CERIO Corporation

CS-3008XG

8 SFP+ 10Gigabit Port Managed Fiber Optical Switch

User Manual

Default IP / Login Information	
IP Address	192.168.2.200
User Name	root
Password	default

FCC Warning

This device has been tested and found to comply with limits for a Class A digital device, pursuant to Part 2 and 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiates radio frequency energy and, if not installed and used in accordance with the user's manual, may cause interference in which case user will be required to correct the interference at his own expense.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user many be required to take adequate measures.

1. Exterior 9
1.1 Front Panel 9
1.2 Rear Panel Layout 9
2. Software Configuration 10
2.1 Example of Segment: (Windows OS) 10
2.2 System login information and IP / Gateway Setting instructions 13
3. Status 15
3.1 System Information 15
3.2 Logging Message 17
3.3 Port 18
3.3.1 Statistics 18
3.3.2 Error Disabled 21
3.3.3 Bandwidth Utilization 21
3.4 Link Aggregation 22
3.5 MAC Address Table 23
4. Network 25
4.1 DNS 25
4.2 Host 27
4.3 System Time 29
5. Port 31
5.1 Port setting 31
5.2 Error Disabled 33
5.3 Link Aggregation 34
5.3.1 Group Configuration 34
5.3.2 Port Setting 36
5.3.3 LACP 39
5.4 EEE 41
5.5 Jumbo Frame 42
6. VLAN 43
6.1 VLAN 43
6.1.1 Create VLAN 43
6.1.2 VLAN Configuration 45
6.1.3 Membership 46
6.1.4 Port Setting 47

6.2 Voice VLAN 50
6.2.1 Property 50
6.2.2 Voice OUI 51
6.3 Protocol VLAN 53
6.3.1 Protocol Group 53
6.3.2 Group Binding 54
6.4 MAC VLAN 55
6.4.1 MAC Group 55
6.4.2 Group Binding 57
6.5 Surveillance VLAN 58
6.5.1 Property 58
6.5.2 Surveillance OUI 61
6.6 GVRP 62
6.6.1 Property 63
6.6.2 Member ship 64
6.6.3 Statistics 65
7. MAC Address Table 67
7.1 Dynamic Address 67
7.2 Static Address 68
7.3 Filtering Address 69
7.4 Port Security Address 70
8. Spanning Tree 71
8.1 Property 72
8.2 Port Setting 74
8.3 MST Instance 76
8.4 MST Port Setting 78
8.5 Statistics 81
9. ERPS 83
9.1 Propely 86
9.2 ERPS Instance Setting 87
10. Loopback 93
10.1 Loopback Config 93
11. Discovery(LLDP) 95
11.1 Property 95

11.2 Port Setting 97

11.3 MED Network Policy 99

11.4 MED Port Setting 101

11.5 Packet View 103

11.6 Local Information 105

11.7 Neighbor 111

11.8 Statistics 114

12. DHCP 116

12.1 Property 116

12.2 IP Pool Setting 117

12.3 VLAN IF Address Group Setting 120

12.4 Client List 121

12.5 Client Static Binding Table 122

12.6 Client Static Port Binding Table 123

13. Multicast 124

13.1 General 124

13.1.1 Property 124

13.1.2 Group Address 125

13.1.3 Router Port 127

13.1.4 Forward All 129

13.1.5 Throttling 131

13.1.6 Filtering Profile 132

13.1.7 Filtering Binding 133

13.2 IGMP Snooping 135

13.2.1 Property 135

13.2.2 Querier 138

13.2.3 Statistics 139

13.3 MLD Snooping 141

13.3.1 Property 141

13.3.2 Statistics 144

13.4 MVR 145

13.4.1 Property 146

13.4.2 Port Setting 147

13.4.3 Group Address 148

14. IP Configuration 150
14.1 IPv4 Management and Interfaces 150
14.1.1 IPv4 Interface & Default IP Configure 150
14.1.2 IPv4 Routes & Default Route Configure 154
14.1.3 ARP 161
14.2 IPv6 Management and Interfaces 163
14.2.1 IPv6 Interface 163
14.2.2 IPv6 Addresses 165
14.2.3 IPv6 Routes 168
14.2.4 IPv6 Neighbors 171
14.3 RIP Routes Setting 173
14.3.1 Rip Routes Setting 173
14.4 OSPF Routes Management 174
14.4.1 Ospf Routes Setting 174
14.5 VRRP Management 176
14.5.1 VRRP Interfaces Setting 176
15. Security 179
15.1 RADIUS 179
15.2 TACACS+ 182
15.3 AAA 185
15.3.1 Method List 185
15.3.2 Login Authentication 187
15.4 Management Access 188
15.4.1 Management Service 188
15.4.2 Management ACL 189
15.4.3 Management ACE 190
15.5 Authentication Manager 193
15.5.1 Property 193
15.5.2 Port Setting 198
15.5.3 MAC-Based Local Account 203
15.5.4 WEB-Based Local Account 205
15.5.5 Sessions 206
15.6 Port Security 208
15.7 Protected Port 211

15.8 Storm Control 212
15.9 DoS 215
15.9.1 Property 215
15.9.2 Port Setting 217
15.10 Dynamic ARP Inspection 218
15.10.1 Property 218
15.10.2 Statistics 220
15.11 DHCP Snooping 221
15.11.1 Property 221
15.11.2 Statistics 223
15.11.3 Option82 Property 225
15.11.4 Option82 Circuit ID 226
15.12 IP Source Guard 228
15.12.1 Port Setting 228
15.12.2 IMPV Binding 229
15.12.3 Save Databases 231
16. ACL 233
16.1 MAC ACL 233
16.2 MAC ACE 234
16.3 IPv4 ACL 237
16.4 IPv4 ACE 238
16.5 IPv6 ACL 242
16.6 IPv6 ACE 243
16.7 ACL Binding 247
17. QoS 249
17.1 Property 249
17.2 Queue Scheduling 252
17.3 CoS Mapping 253
17.4 DSCP Mapping 255
17.5 IP Precedence to Queue Mapping 257
17.6 Rate Limit 258
17.6.1 Ingress / Egress Port 258
17.6.2 Egress Queue 259
18. Diagnostics 262

18.1 Logging 262

18.1.1 Property 262

18.1.2 Remote Server 264

18.2 Mirroring 266

18.3 Ping 268

18.4 Traceroute 269

18.5 Fiber Module 270

18.6 UDLD 271

18.6.1 Property 271

18.6.2 Neighbor 272

19. Management 274

19.1 User Account 274

19.2 Firmware 275

19.2.1 Upgrade / Backup 275

19.2.2 Active Image 277

19.3 Configuration 278

19.3.1 Upgrade / Backup 278

19.3.2 Save Configuration 279

19.4 SNMP 280

19.4.1 View 280

19.4.2 Group 282

19.4.3 Community 284

19.4.4 User 286

19.4.5 Engine ID 288

19.4.6 Trap Event 290

19.4.7 Notification 291

19.5 RMON 294

19.5.1 Statistics 294

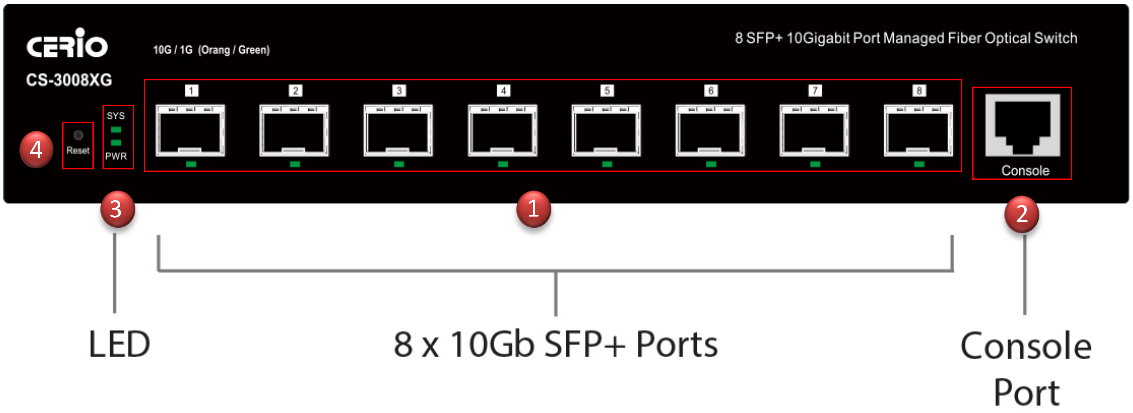
19.5.2 History 296

19.5.3 Event 298

19.5.4 Alarm 300

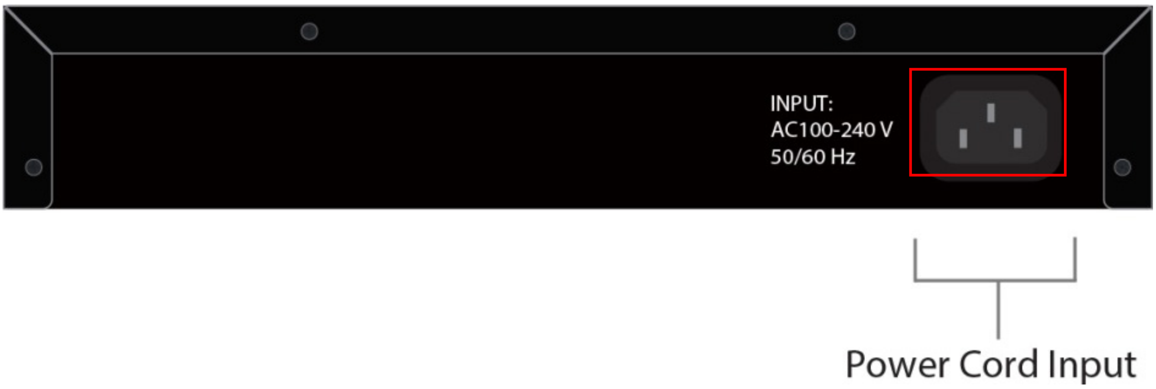
1. Exterior

1.1 Front Panel



1) 8 x SFP + 10Gigabit Ethernet Ports(RJ-45) with 10G (Orange)/1G(Green) Ethernet Link/ACT LED
2) Console Port.
3) Power and Sys standby LED light.
4) Reset to default button. (Long press the “Reset” button with a pin for 10 seconds, if the LEDs start to flash, the reset process starts.)

1.2 Rear Panel Layout



1) AC input (100-240V/AC, 50-60Hz) UL Safety

2. Software Configuration

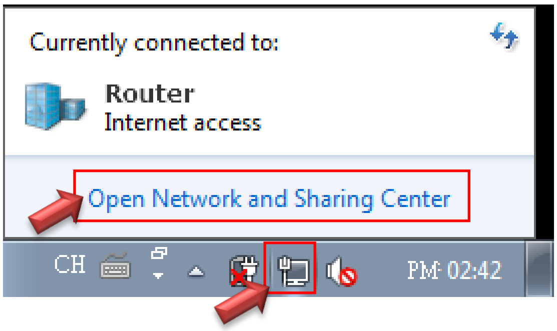
CS-3008XG supports web-based configuration. Upon the completion of hardware installation, The Switch can be configured through a PC/NB by using its web browser such as Internet Explorer 6.0 or later.

Set the IP segment of the administrator's computer to be in the same range as **CS-3008XG** for accessing the system. Do not duplicate the IP Address used here with IP Address of **CS-3008XG** or any other device within the network. ***Please refer to the following steps***

2.1 Example of Segment: (Windows OS)

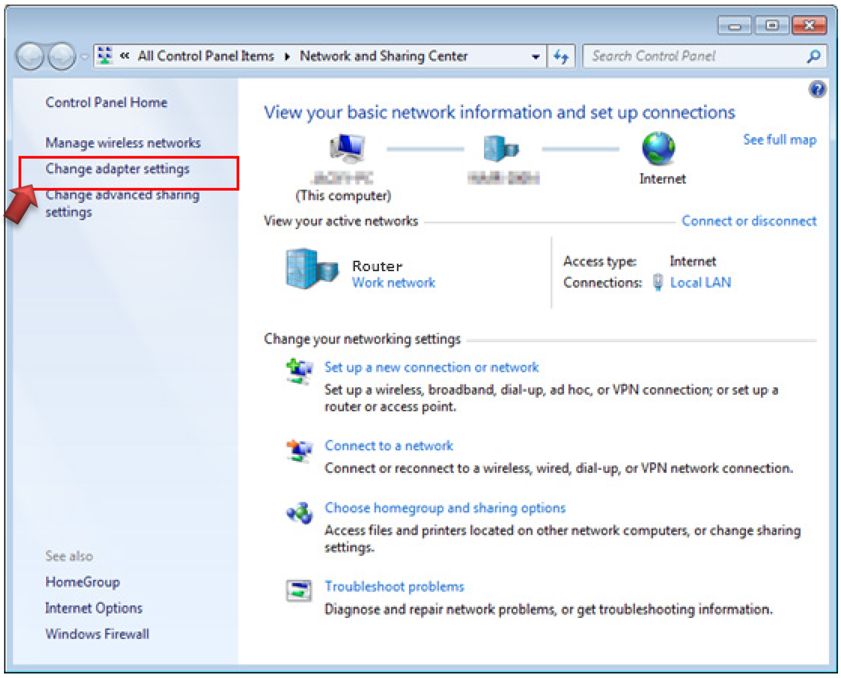
Step 1 :

Please click on the computer icon in the bottom right window, and click **"Open Network and Sharing Center"**



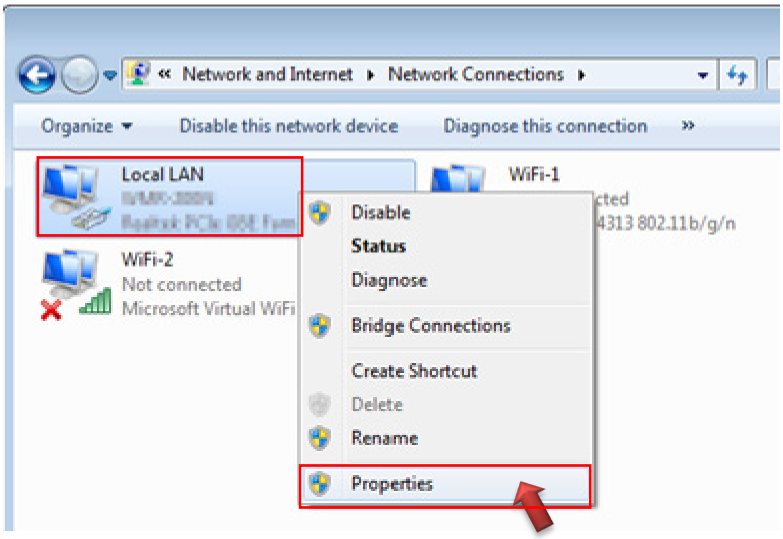
Step 2 :

In the Network and Sharing Center page, click on the left side of **"Change adapter setting"** button


All Control Panel Items ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
See also
HomeGroup
Internet Options
Windows Firewall
View your basic network information and set up connections
See full map
(This computer)
Internet
View your active networks
Connect or disconnect
Router
Work network
Access type: Internet
Connections: Local LAN
Change your networking settings
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.
Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

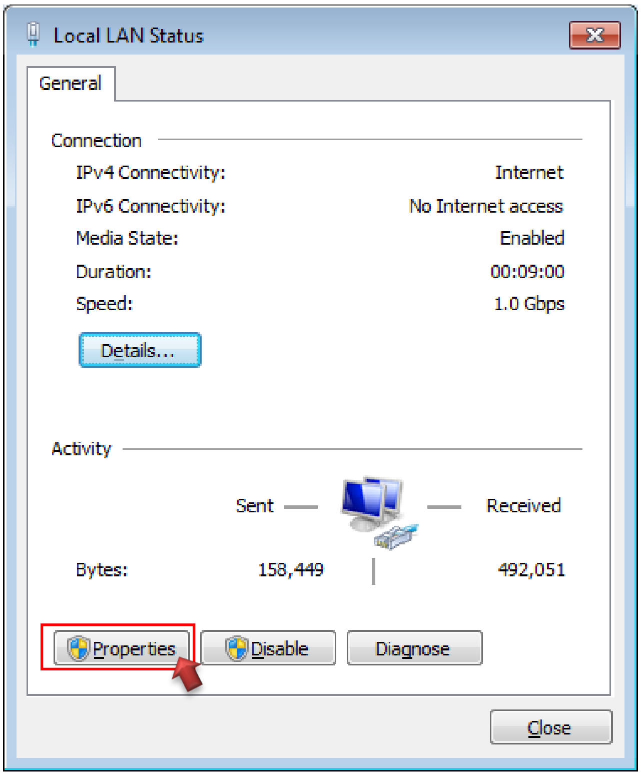
Step 3 :

In **“Change adapter setting”** Page, right click on Local LAN then select **“Properties”**



Step 4 :

In the **“Properties”** page, click the **“Properties”** button to open TCP/IP setting


Local LAN Status

General

Connection

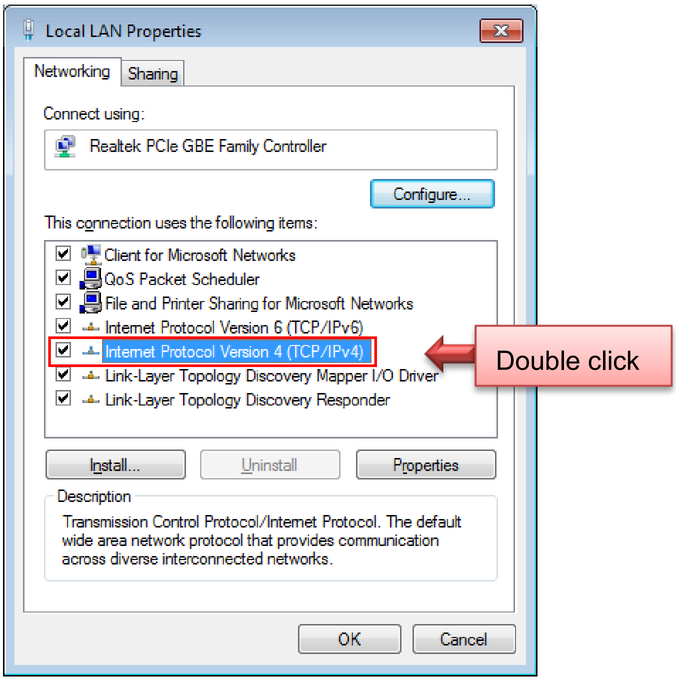
IPv4 Connectivity: Internet
IPv6 Connectivity: No Internet access
Media State: Enabled
Duration: 00:09:00
Speed: 1.0 Gbps

Activity

Sent — Received
Bytes: 158,449 492,051

Step 5 :

In Properties page for setting IP addresses, find **“Internet Protocol Version 4 (TCP/IPv4)”** and double click to open TCP/IPv4 Properties window



Local LAN Properties

Networking | Sharing

Connect using:

Realtek PCIe GBE Family Controller

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Install... | Uninstall | Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK | Cancel

Double click

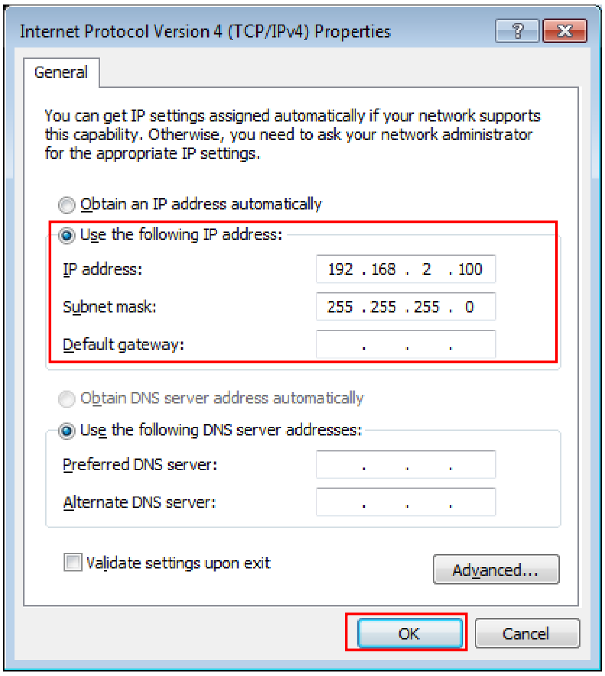
Step 6 :

Select **“Use the following IP address”**, and fix in IP Address to: 192.168.2.X

ex. The X is any number from 1 to 253

Subnet mask : 255.255.255.0

And Click **"OK"** to complete fixing the computer IP settings



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 2 . 100
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	. . .
Alternate DNS server:	. . .

□ Validate settings upon exit

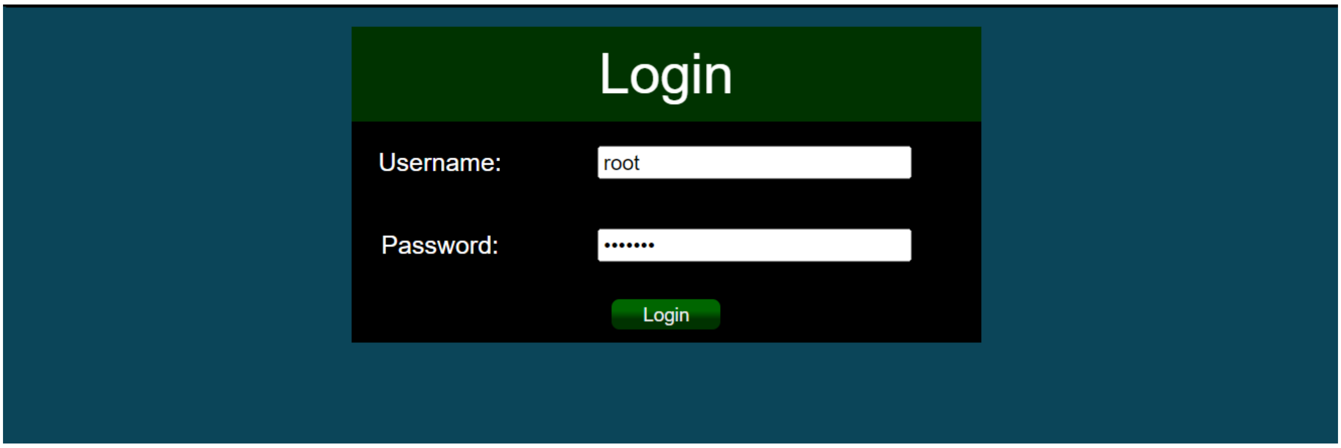
Advanced...

OK | Cancel

Step 7 :

Open Web Browser

Without a valid certificate, users may encounter the following problem in IE7 when they try to access system's WMI (http://192.168.2.200). There will be a “Certificate Error”, because the browser treats system as an illegal website.



Login

Username: root

Password: •••••••

System login Overview page will appear after successful login.

2.2 System login information and IP / Gateway Setting instructions

The **CS-3008XG** web switch default IP is 192.168.2.200

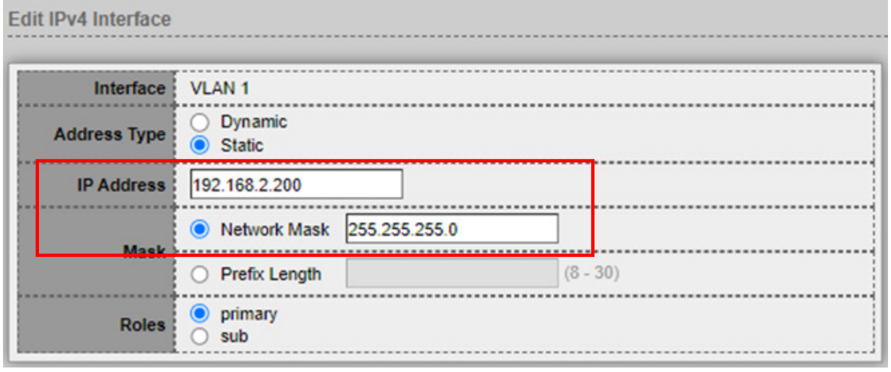
Into the management page as follows, please enter Username and password

- **Default IP Address**: 192.168.2.200
- **Default Username and Password**

Management Account	Root Account
Username	root
Password	default

After the authentication procedure, the home page will show up. Select one of the configurations by clicking the icon.

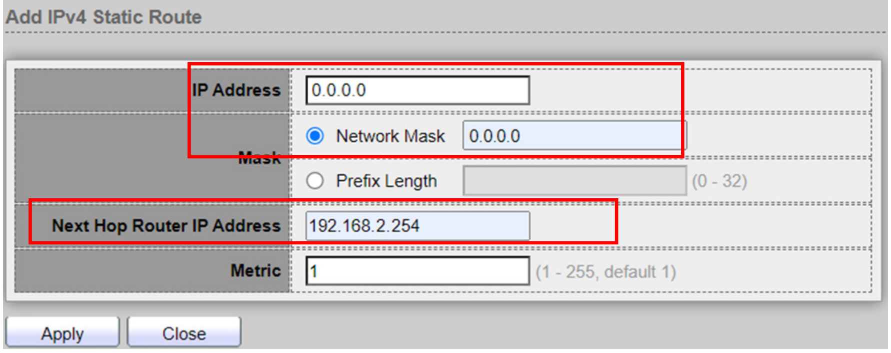
Default IP Configure:


Edit IPv4 Interface

Interface	VLAN 1
Address Type	○ Dynamic ● Static
IP Address	192.168.2.200
Mask	● Network Mask 255.255.255.0 ○ Prefix Length (8 - 30)
Roles	● primary ○ sub

Note	If you want to change the default IP (VLAN IP) address of the Fiber Optical Switch, please refer to the chapter : 14.1.1. for ” IP Configuration > IPv4 Interface & Default IP Configure >” (Please refer to page 149)

Layer 3 Default Route Configure: **(This function is the same as the "Default Gateway Configure " of the Layer 2 switch)**


Add IPv4 Static Route

IP Address	0.0.0.0
Mask	● Network Mask 0.0.0.0 ○ Prefix Length (0 - 32)
Next Hop Router IP Address	192.168.2.254
Metric	1 (1 - 255, default 1)

Note	If you want to make default Route IP address of the L3 Fiber Optical Switch, please refer to the chapter : 14.1.2. for ” IP Configuration > IPv4 Routes & Default Route Configure >” (Please refer to page 153)

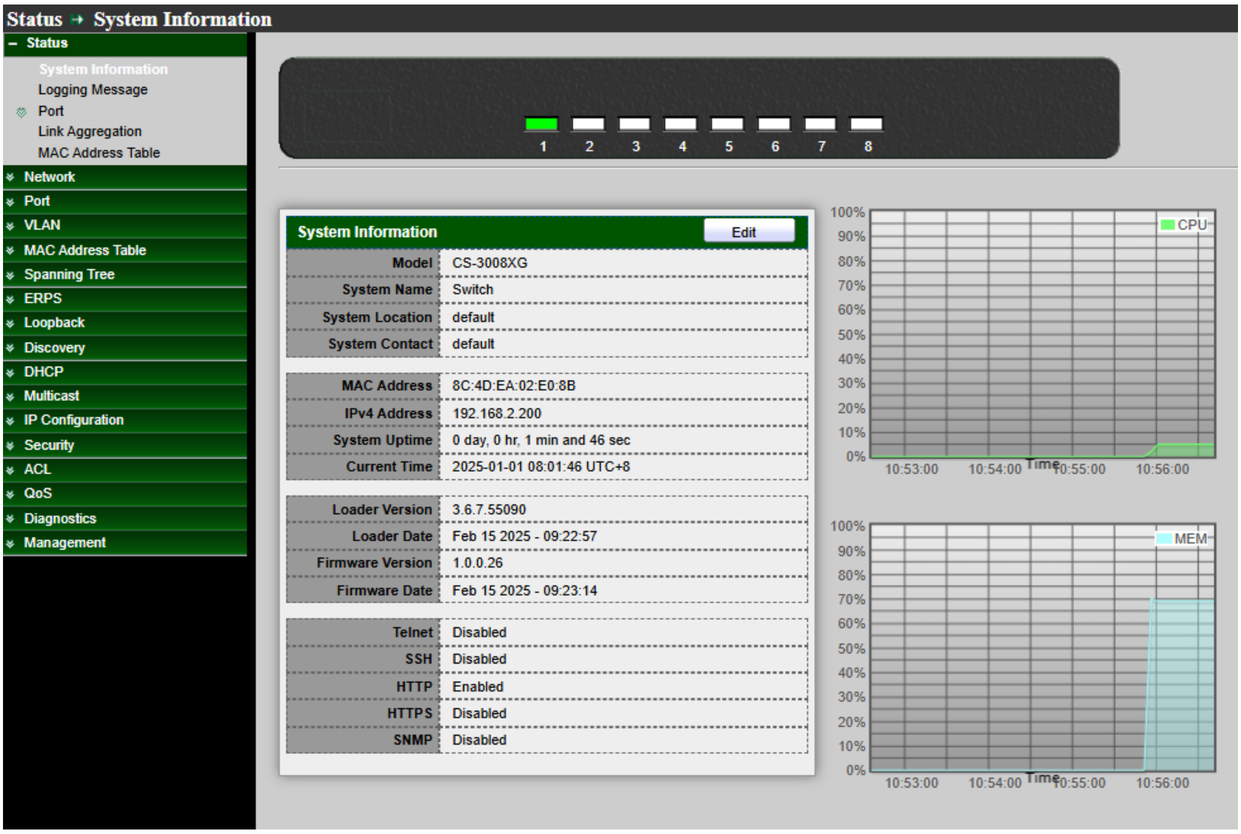
3. Status

3.1 System Information

Administrator can check this page shows switch panel, CPU utilization, Memory utilization and other

system current information. It also allows user to edit some system information.

Note	In the Web UI, the left column shows the configuration menu. The top row shows the switch's current link status. Green squares indicate the port link is up, while black squares indicate the port link is down. Below the switch panel, you can find a common toolbar to provide useful functions for users. The rest of the screen area displays the configuration settings.



System Information

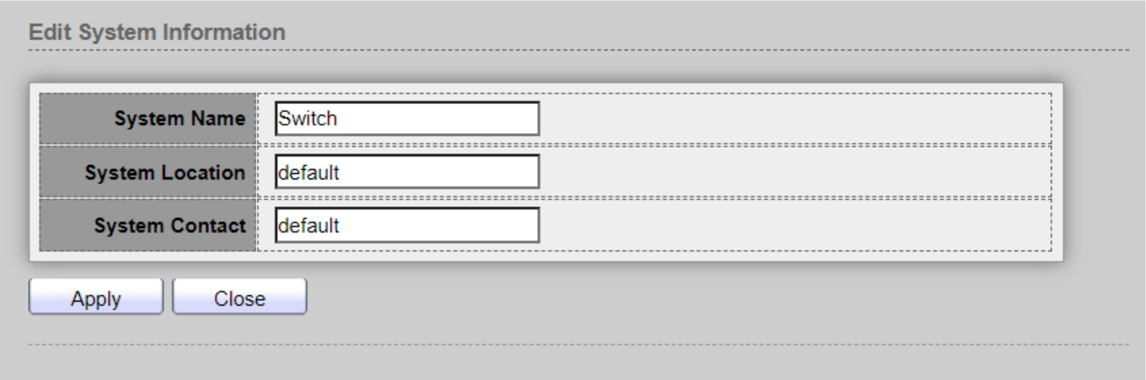
Model	CS-3008XG
System Name	Switch
System Location	default
System Contact	default
MAC Address	8C:4D:EA:02:E0:8B
IPv4 Address	192.168.2.200
System Uptime	0 day, 0 hr, 1 min and 46 sec
Current Time	2025-01-01 08:01:46 UTC+8
Loader Version	3.6.7.55090
Loader Date	Feb 15 2025 - 09:22:57
Firmware Version	1.0.0.26
Firmware Date	Feb 15 2025 - 09:23:14
Telnet	Disabled
SSH	Disabled
HTTP	Enabled
HTTPS	Disabled
SNMP	Disabled

Field	Description
Model	Model name of the switch.
System Name	System name of the switch. This name will also use as CLI prefix of each line. ("Switch>" or "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.

Edit System Information

Administrator can click “Edit” button on the table title to edit following system information.


Edit System Information

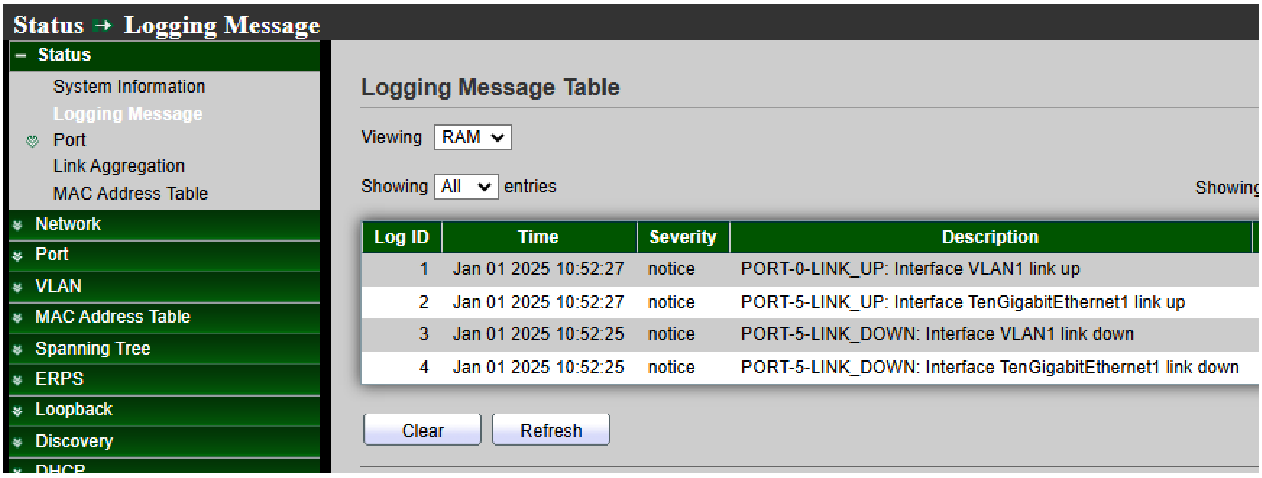
System Name	Switch
System Location	default
System Contact	default

- **System Name:** System name of the switch. This name will also use as CLI prefix of each line. (“Switch>” or “Switch#”).
- **System Location:** Location Location information of the switch.
- **System Contact:** Contact information of the switch.

*Click the **“Apply”** button to save your changes or **“Close”** the button to close settings.*

3.2 Logging Message

Administrator can use this tools page to Inspection of system RAM and Flash status.



Logging Message Table

Viewing RAM

Showing All entries

Showing

Log ID	Time	Severity	Description
1	Jan 01 2025 10:52:27	notice	PORT-0-LINK_UP: Interface VLAN1 link up
2	Jan 01 2025 10:52:27	notice	PORT-5-LINK_UP: Interface TenGigabitEthernet1 link up
3	Jan 01 2025 10:52:25	notice	PORT-5-LINK_DOWN: Interface VLAN1 link down
4	Jan 01 2025 10:52:25	notice	PORT-5-LINK_DOWN: Interface TenGigabitEthernet1 link down

- **Viewing:** The logging view including:
  - **RAM:** Show the logging messages stored on the RAM.
  - **Flash:** Show the logging messages stored on the 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.

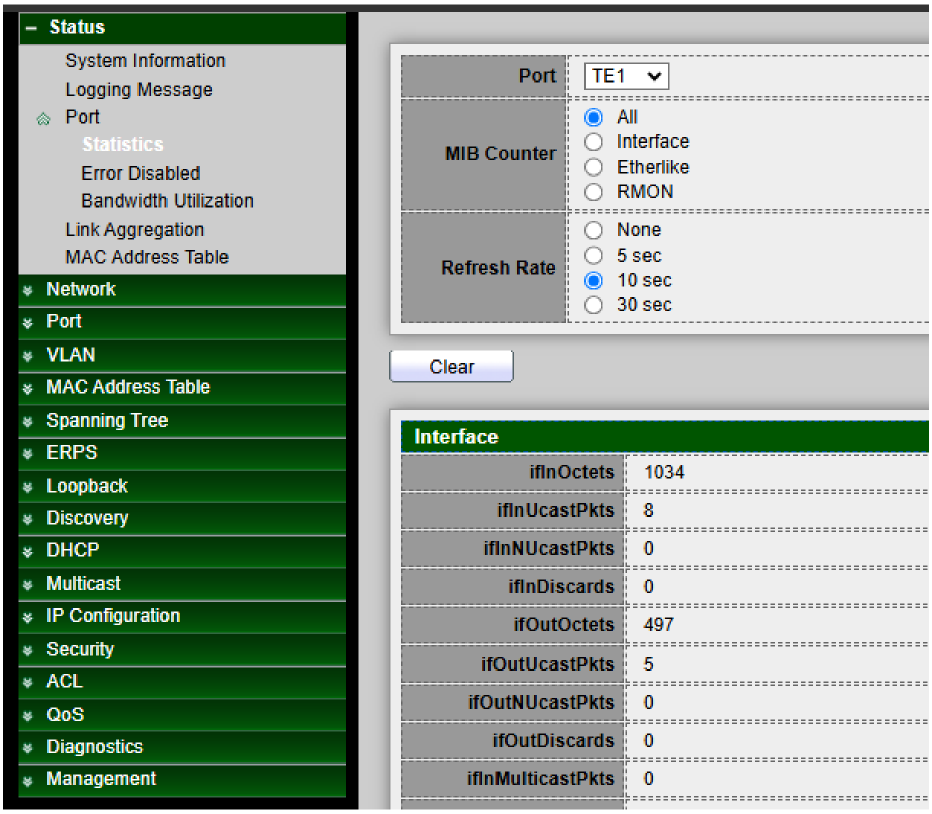
*Click the **"Clear"** button to clear this page or click the **"Refresh"** button to refresh the page .*

3.3 Port

Display detailed port summary and status information for each port.

3.3.1 Statistics

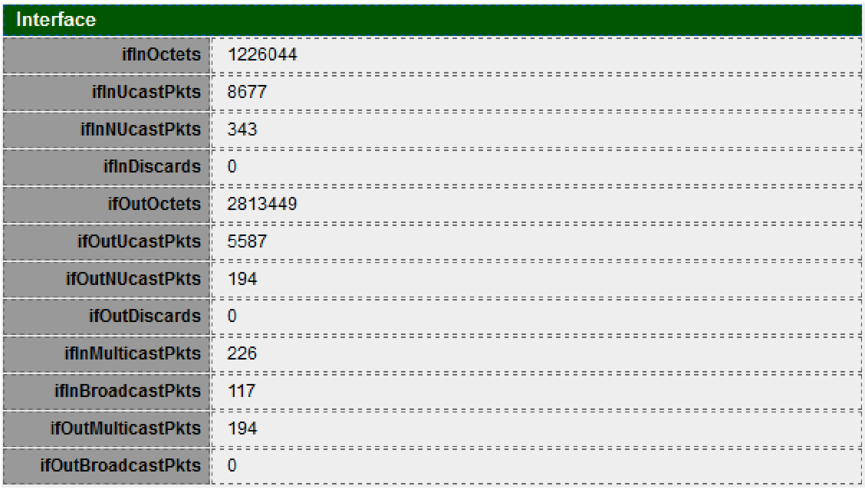
Administration can choose to view displays standard counters on network traffic form the Interfaces, Ethernet-like and RMON MIB. Interfaces and Ethernet-like counters display errors on the traffic passing through each port. RMON counters provide a total count of different frame types and sizes passing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



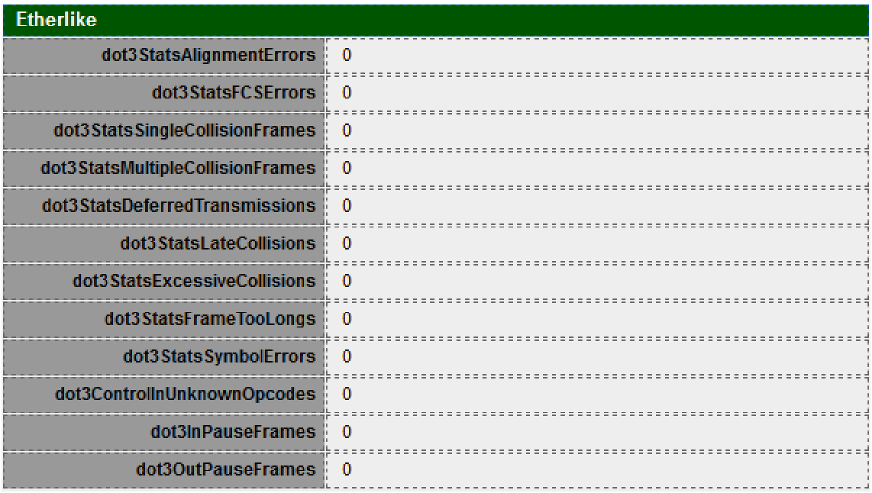
Port	TE1
MIB Counter	● All ○ Interface ○ Etherlike ○ RMON
Refresh Rate	○ None ○ 5 sec ● 10 sec ○ 30 sec

Interface	
ifInOctets	1034
ifInUcastPkts	8
ifInNUcastPkts	0
ifInDiscards	0
ifOutOctets	497
ifOutUcastPkts	5
ifOutNUcastPkts	0
ifOutDiscards	0
ifInMulticastPkts	0

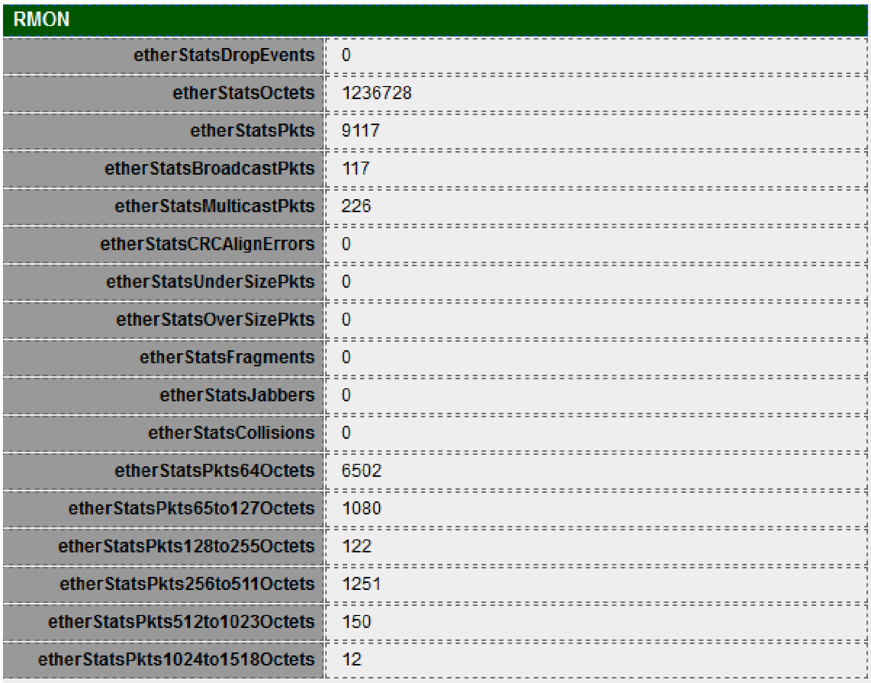
*Click the **"Clear"** button to clear this page.*



Interface	
ifInOctets	1226044
ifInUcastPkts	8677
ifInNUcastPkts	343
ifInDiscards	0
ifOutOctets	2813449
ifOutUcastPkts	5587
ifOutNUcastPkts	194
ifOutDiscards	0
ifInMulticastPkts	226
ifInBroadcastPkts	117
ifOutMulticastPkts	194
ifOutBroadcastPkts	0



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

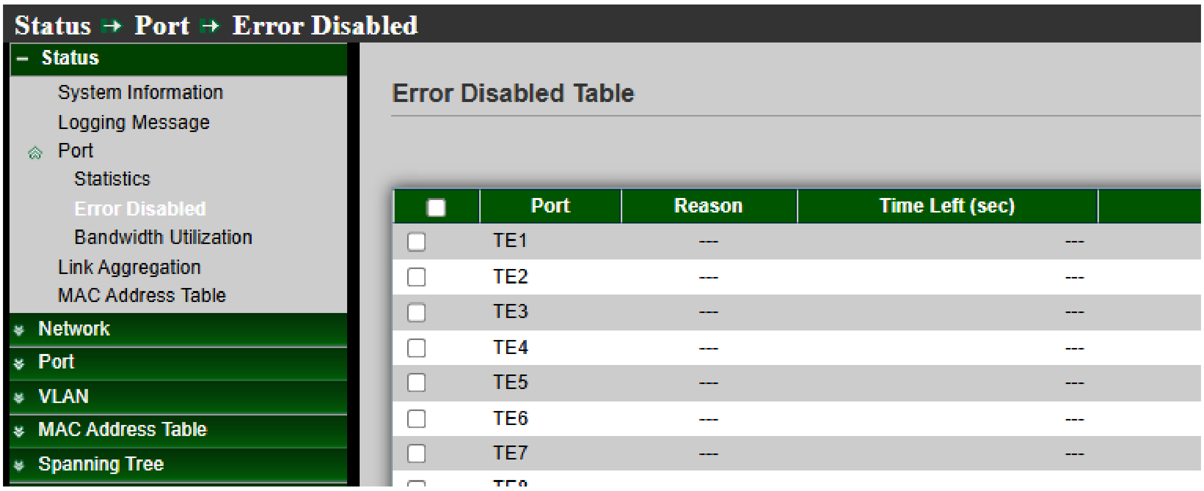


RMON	
etherStatsDropEvents	0
etherStatsOctets	1236728
etherStatsPkts	9117
etherStatsBroadcastPkts	117
etherStatsMulticastPkts	226
etherStatsCRCAlignErrors	0
etherStatsUnderSizePkts	0
etherStatsOverSizePkts	0
etherStatsFragments	0
etherStatsJabbers	0
etherStatsCollisions	0
etherStatsPkts64Octets	6502
etherStatsPkts65to127Octets	1080
etherStatsPkts128to255Octets	122
etherStatsPkts256to511Octets	1251
etherStatsPkts512to1023Octets	150
etherStatsPkts1024to1518Octets	12

- **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 “None , 5 sec , 10 sec , 30 sec “seconds base to get new counter of specified port.

3.3.2 Error Disabled

If administrator has set Error disabled functions then can monitor information in page.



Status ➝ Port ➝ Error Disabled

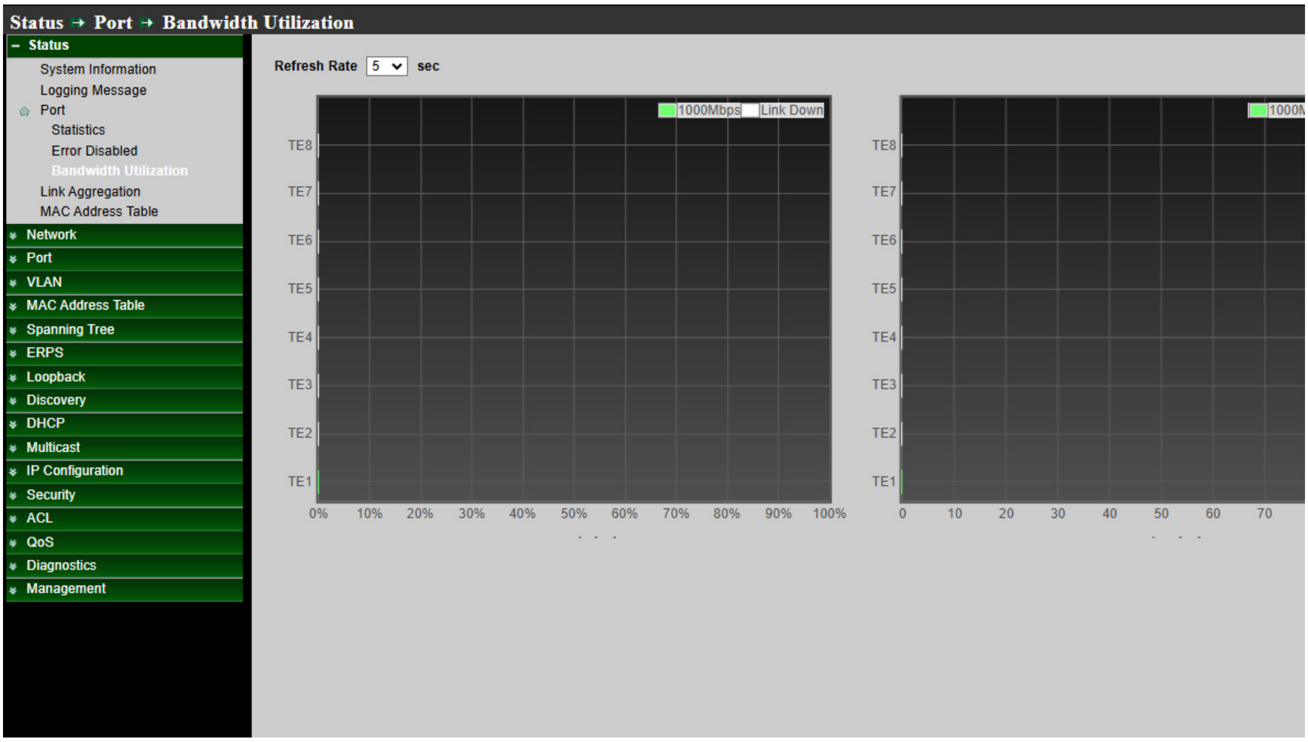
Error Disabled Table

□	Port	Reason	Time Left (sec)
□	TE1	---	---
□	TE2	---	---
□	TE3	---	---
□	TE4	---	---
□	TE5	---	---
□	TE6	---	---
□	TE7	---	---

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

3.3.3 Bandwidth Utilization

This page can display Tx / Rx Real-time bandwidth information of each port. (Instant used rate per port and this page will refresh automatically in every refresh period)



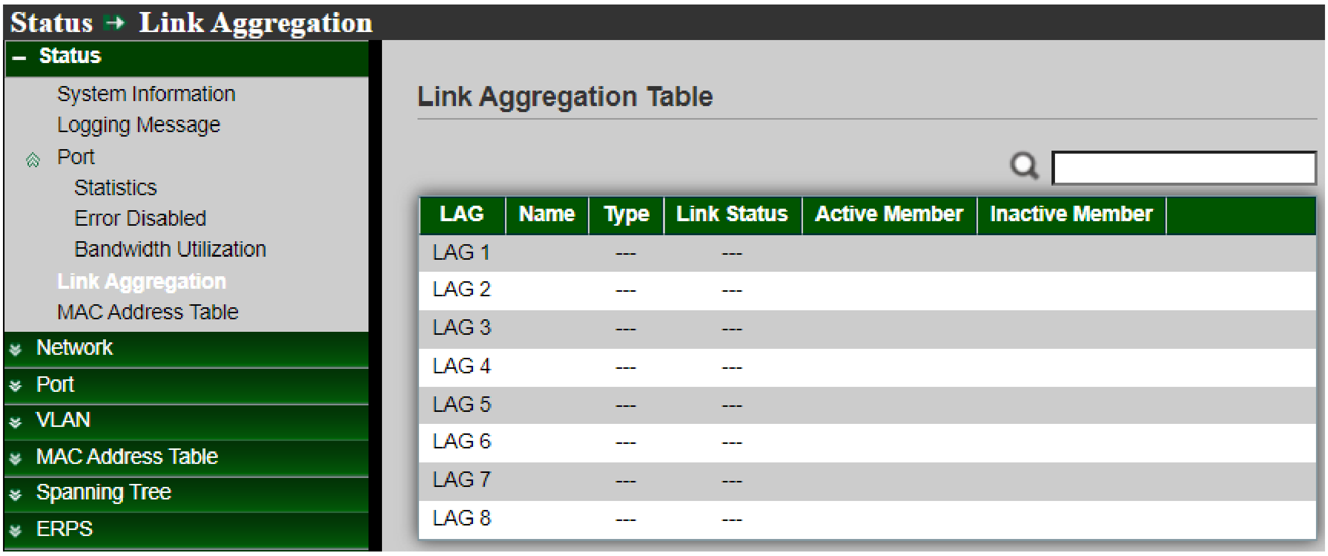
Refresh Rate 5 sec

- **Refresh Rate:** Refresh the web page every period of seconds to get new bandwidth utilization Rata.
  - **2 :** Select the 2 second cycle from the drop-down menu to refresh the display page.
  - **5 :** Select the 5 second cycle from the drop-down menu to refresh the display page.

10 : Select the 10 second cycle from the drop-down menu to refresh the display page.

3.4 Link Aggregation

If administrator has set LACP function then this can display LACP information. This system have support 8 Link Aggregation group. Administrator can enable 8 LAG.



Link Aggregation Table

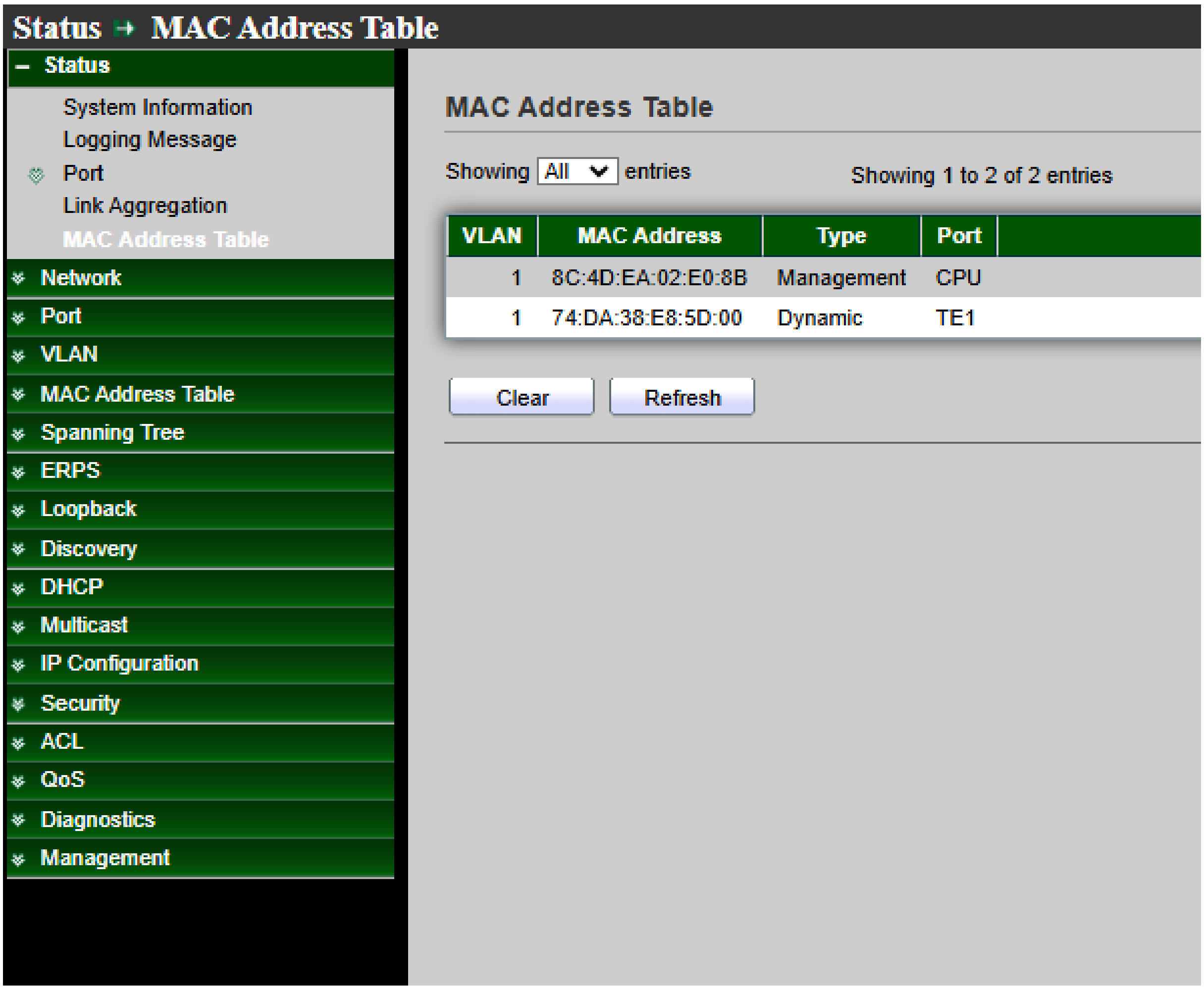
LAG	Name	Type	Link Status	Active Member	Inactive Member
LAG 1		---	---		
LAG 2		---	---		
LAG 3		---	---		
LAG 4		---	---		
LAG 5		---	---		
LAG 6		---	---		
LAG 7		---	---		
LAG 8		---	---		

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

3.5 MAC Address Table

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

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



MAC Address Table

Showing All entries Showing 1 to 2 of 2 entries

VLAN	MAC Address	Type	Port
1	8C:4D:EA:02:E0:8B	Management	CPU
1	74:DA:38:E8:5D:00	Dynamic	TE1

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

*Click the **"Clear"** button to clear this page or click the **"Refresh"** button to refresh the page .*

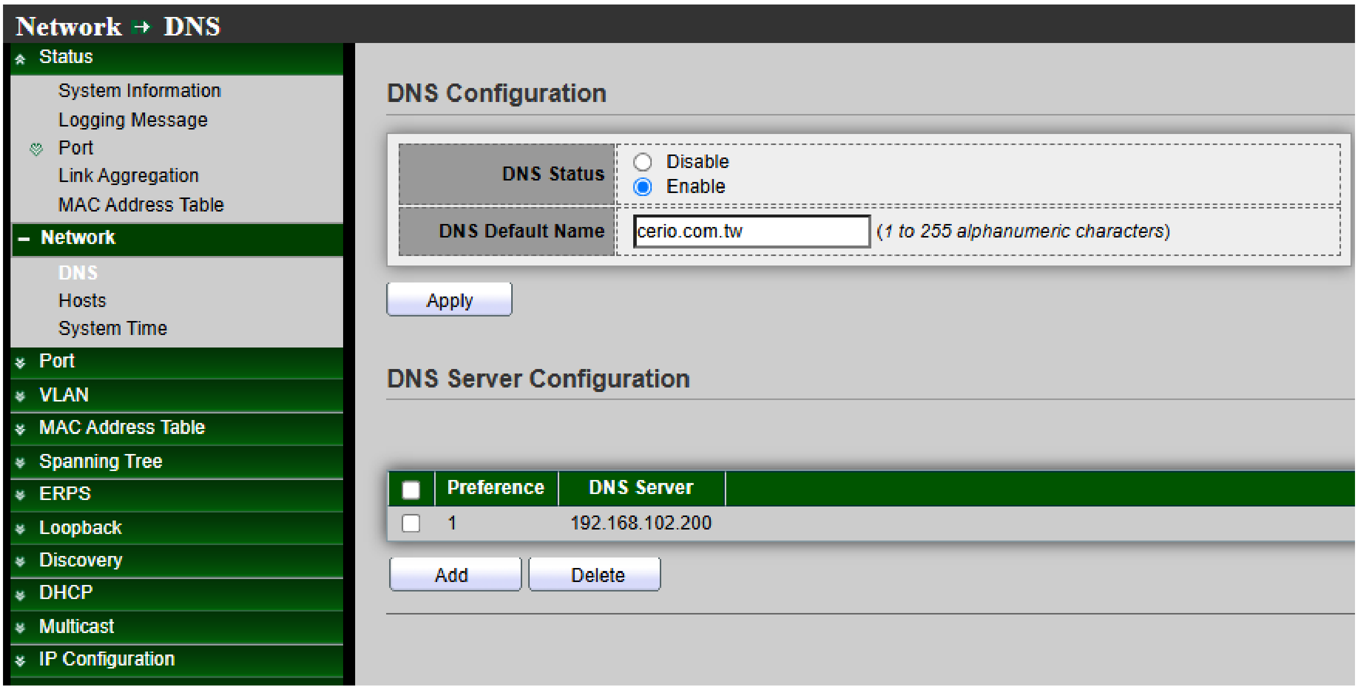
4. Network

4.1 DNS

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. Use the DNS screen to configure and view the default DNS servers on the Switch.
Use these pages to configure information about which DNS servers your network uses and how the switch operates as a DNS client.

DNS service on this switch allows host names to be mapped to IP addresses using static table entries or by redirection to other name servers on the network. When a client device designates this switch as a DNS server, the client will attempt to resolve host names into IP addresses by forwarding DNS queries to the switch, and waiting for a response.
You can manually configure entries in the DNS table used for mapping domain names to IP addresses, configure default domain names, or specify one or more name servers to use for domain name to address translation.

You can use these pages to configure information about DNS servers the network uses and how the switch operates as a DNS client.
Use this page to configure global DNS settings and DNS server information.



DNS Configuration

DNS Status	○ Disable ● Enable
DNS Default Name	cerio.com.tw (1 to 255 alphanumeric characters)

DNS Server Configuration

□	Preference	DNS Server
□	1	192.168.102.200

DNS Configuration

Select the Disable or Enable button to specify whether to disable or enable the administrative state of the DNS client:

- **DNS Status:**
  - **Disable：** Prevent the switch from sending DNS queries.
  - **Enable：** Allow the switch to send DNS queries to a DNS server to resolve a DNS domain name.
- **DNS Default Name：** Enter the default DNS domain name to include in DNS queries.

Note	When the system is performing a lookup on an unqualified host name, this field is provides the domain name (for example, if default domain name is cerio.cc and the user enters oem, then "oem" is changed to oem.cerio.cc to resolve the name). The name must not be longer than 255 alphanumeeric characters.

*Click the **"Apply"** button to save your changes.*

DNS Server Configuration

Administrator can configure this DNS Server Setting **"add"** and " Delete " function management.

Field	Description
Preference	The Preference field displays the server preference order. The preference is set in the order in which preferences were entered.
DNS Server	Shows the server is added to the list.

Note	The "preference" of the DNS server. The preferences are determined by the order in which they were entered. You can specify up to eight DNS servers.

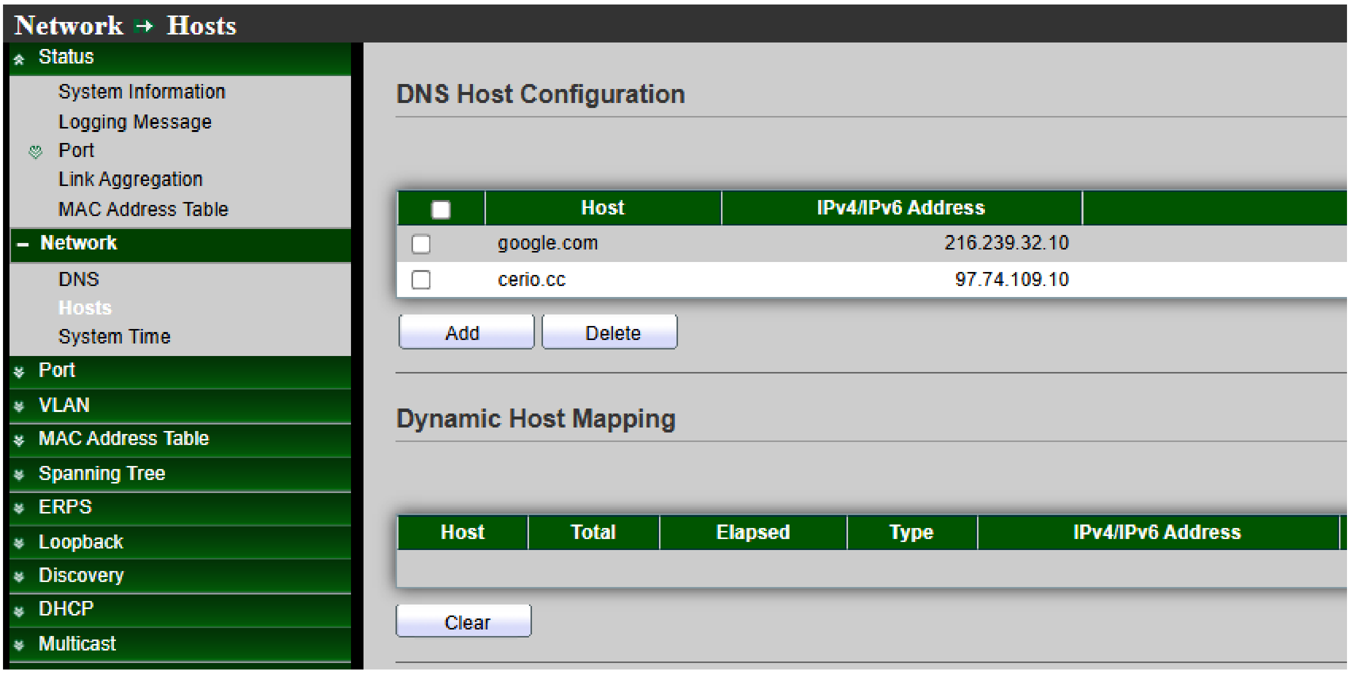
- **Add** ：To specify the DNS server to which the switch sends DNS queries, enter an IP address in standard IPv4 dot notation in the DNS Server Address and click Add. The server appears in the list below. You can specify up to eight DNS servers. The preference is set in the order created.
- **Delete** ：To remove a DNS server from the list, select the check box next to the server you want to remove and click Delete. If no DNS server is specified, the check box is global and will delete all the DNS servers listed.

Administrator can configure this DNS Server Configuration **“Apply”** and “ **Cancel** “on the screen and

reset the data on the screen to the latest value of the switch.

4.2 Host

This page provide administrator to view Host Name to IP Address Information, Administrator can set this page to manually map host names to IP addresses or to view dynamic host mappings.



DNS Host Configuration

□	Host	IPv4/IPv6 Address
□	google.com	216.239.32.10
□	cerio.cc	97.74.109.10

Dynamic Host Mapping

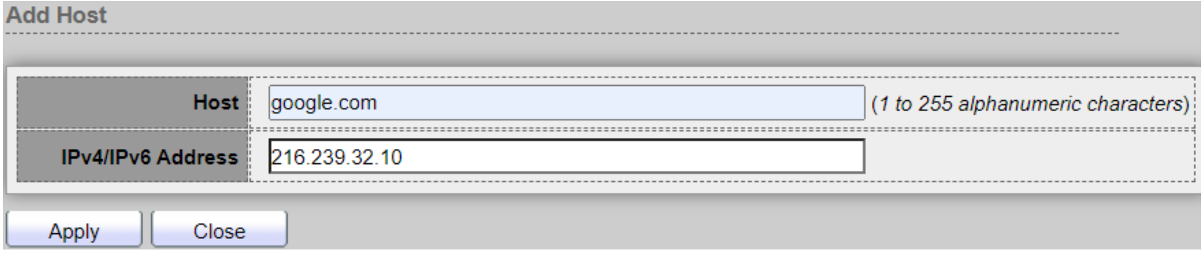
Host	Total	Elapsed	Type	IPv4/IPv6 Address

*Click the **“Clear”** button to clear this page*

DNS Host Configuration

Administrator can configure **“add”** and “ Delete “ for a static entry to the local dynamic host mapping Table function management.

Field	Description
Host	Show “host name” that for you assign to the specified IP address.
IPv4/IPv6 Address	The IP address associated with the “host name”.



Add Host

Host	google.com	(1 to 255 alphanumeric characters)
IPv4/IPv6 Address	216.239.32.10	

- **Host:** Administrator can set the Host Name field, specify the static host name to add.
- **IPv4/IPv6 Address:** Enter the IP address to associate with the host name to this " IPv4/IPv6 Address" field, The entry is displayed in the list on the page after **"Apply"** creation.

Note	For Host Name field, Must be follow 1 to 255 alphanumeric characters, Its length cannot exceed 158 characters and it is a required field.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

Dynamic Host Mapping

Administrator can clear all the dynamic host name entries from the list, click the Clear button.

The Dynamic Host Mapping table shows host name-to-IP address entries that the switch learned.

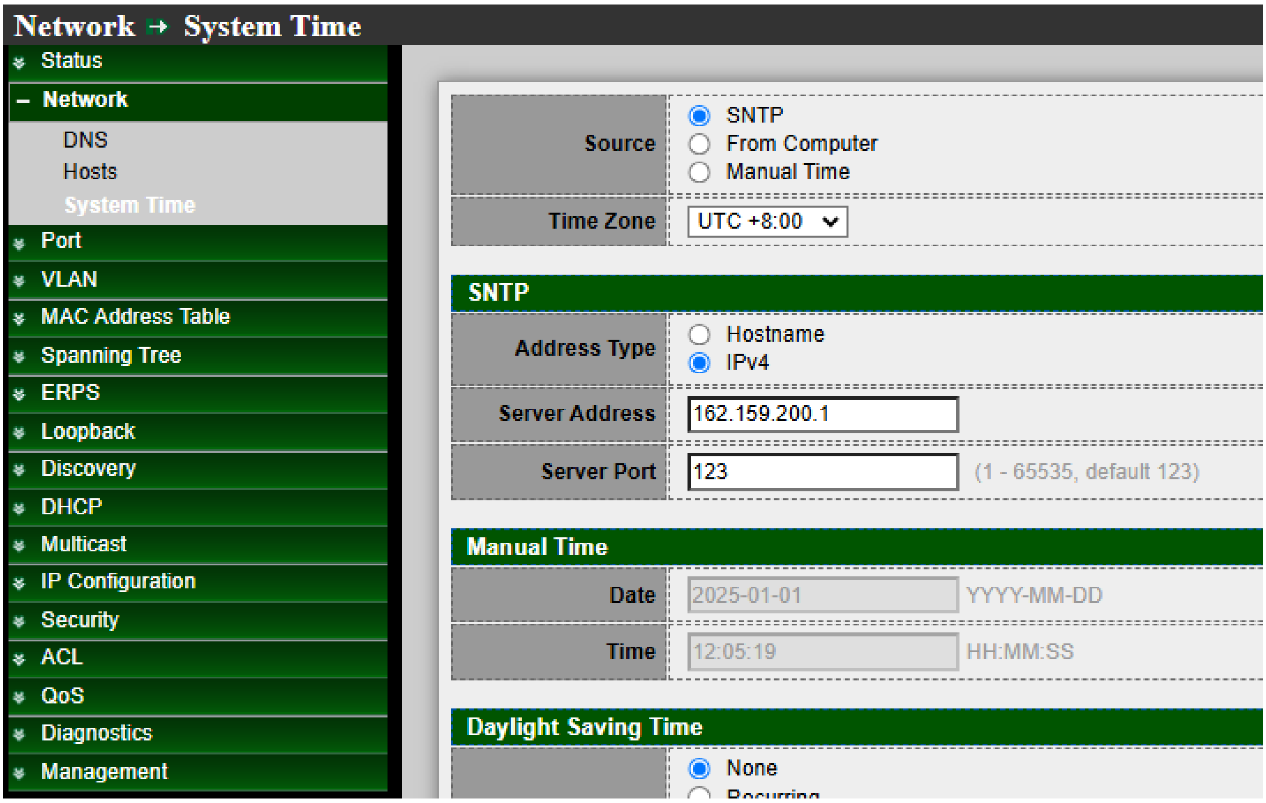
Field	Description
Host	Displays the lists the host name you assign to the specified IP address.
Total	Displays the amount of time since the dynamic entry was first added to the table.
Elapsed	Displays the amount of time since the dynamic entry was last updated.
Type	Displays the type of the dynamic entry.
IPv4/IPv6 Address	Displays the lists the IPv4 or IPv6 addresses associated with the host name.

*Click the **"Apply"** button to save your changes or click the **"Clear"** button to refresh the page .*

4.3 System Time

System time can be configured via this page. Administrator can select SNTP Server or from computer to update the system time or administration can use manual setting the system time.

Note. If administrator chooses SNTP Server to synchronization update time then must confirm system gateway and DNS is correct and switch system must be able to connect to the SNTP Server.



Source	● SNTP ○ From Computer ○ Manual Time
Time Zone	UTC +8:00

SNTP

Address Type	○ Hostname ● IPv4
Server Address	162.159.200.1
Server Port	123 (1 - 65535, default 123)

Manual Time

Date	2025-01-01 YYYY-MM-DD
Time	12:05:19 HH:MM:SS

Daylight Saving Time

● None
○ Recurring

System Time

- ➢ **Source:** Select the time source.
  - **SNTP:** Time sync from NTP server.
  - **From Computer:** Time set from browser host.
  - **Manual Time:** Time set by manually configure.
- ➢ **Time Zone:** Select a time zone difference from listing district.

SNTP

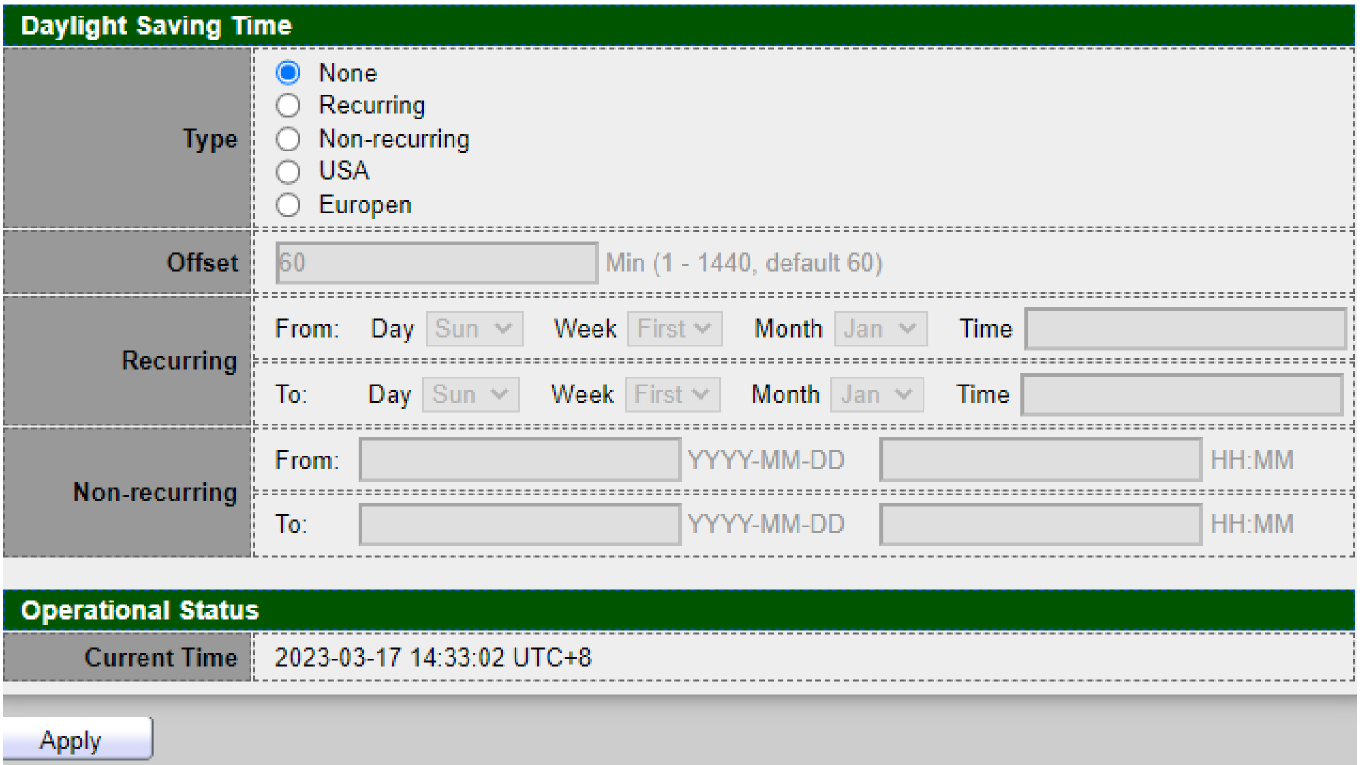
- ➢ **Address Type:** Select the address type of NTP server. This is enabled when time source is SNTP.
- ➢ **Server Address:** Input IPv4 address or hostname for NTP server. This is enabled when time Source is SNTP.
- ➢ **IPv6 Address:** Input NTP port for NTP server. Default is 123. This is enabled when time source is SNTP.

Manual Time

- **Date:** Input manual date. This is enabled when time source is manual.
- **Time:** Input manual time. This is enabled when time source is manual.

Daylight Saving Time

The Switch support Daylight saving time function, if administrator need enable and set the Daylight saving time function will can be enable this function.



Daylight Saving Time

Type	● None ○ Recurring ○ Non-recurring ○ USA ○ Europen
Offset	60 Min (1 - 1440, default 60)
Recurring	From: Day Sun Week First Month Jan Time
	To: Day Sun Week First Month Jan Time
Non-recurring	From: YYYY-MM-DD HH:MM
	To: YYYY-MM-DD HH:MM

Operational Status

Current Time	2023-03-17 14:33:02 UTC+8

- **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.
- **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.

Operational Status

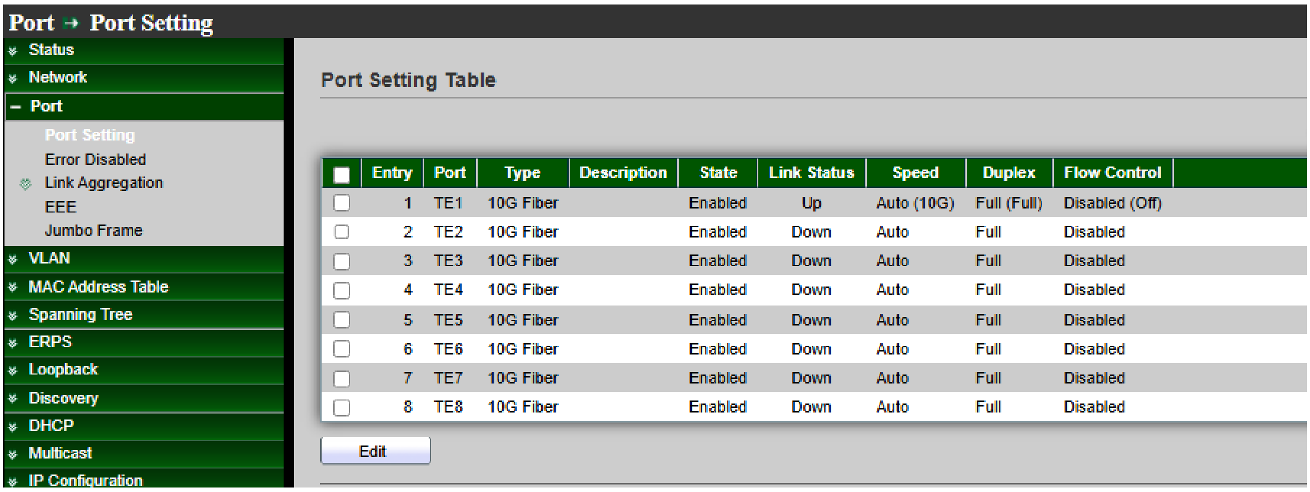
Current Time: Display the current operating time

*Click the **“Apply”** button to save your changes settings.*

5. Port

5.1 Port setting

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



Port Setting Table

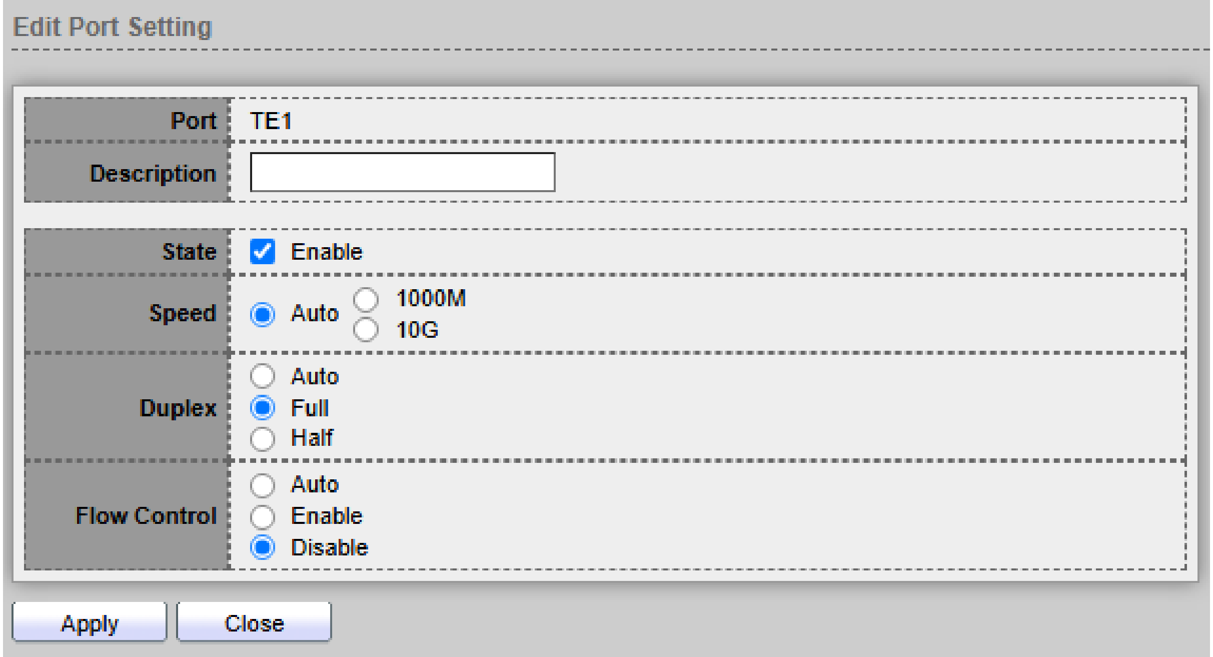
□	Entry	Port	Type	Description	State	Link Status	Speed	Duplex	Flow Control
□	1	TE1	10G Fiber		Enabled	Up	Auto (10G)	Full (Full)	Disabled (Off)
□	2	TE2	10G Fiber		Enabled	Down	Auto	Full	Disabled
□	3	TE3	10G Fiber		Enabled	Down	Auto	Full	Disabled
□	4	TE4	10G Fiber		Enabled	Down	Auto	Full	Disabled
□	5	TE5	10G Fiber		Enabled	Down	Auto	Full	Disabled
□	6	TE6	10G Fiber		Enabled	Down	Auto	Full	Disabled
□	7	TE7	10G Fiber		Enabled	Down	Auto	Full	Disabled
□	8	TE8	10G Fiber		Enabled	Down	Auto	Full	Disabled

Field	Description
Port	Display for Port Name.
Type	Display for Port media type.
Description	Display custom port description.
State	Display for Port admin state. • **Enabled:** Enable the port. • **Disabled:** Disable the port.
Link Status	Current port link status. • **Up:** Port is link up. • **Down:** Port is link down.

Speed	Current port speed configuration and link speed status.
Duplex	Current port duplex configuration and link duplex status.
Flow Control	Current port flow control configuration and link flow control status.

Administrator can set speed / Duplex / Flow Control by each port.

Please select port number in checkbox and click apply button to set speed / Duplex / Flow Control of each port.



Edit Port Setting

Port	TE1
Description	
State	☑ Enable
Speed	● Auto ○ 1000M ○ 10G
Duplex	○ Auto ● Full ○ Half
Flow Control	○ Auto ○ Enable ● Disable

- **Port:** Selected port list.
- **Description:** Custom port description
- **State:** Port admin state.
  - **Enabled:** Enable the port.
  - **Disabled:** Disable the port.
- **Speed :** Port speed capabilities.
  - **Auto:** Auto speed with all capabilities
  - **1000M:** Force speed with 1000M ability
  - **10G:** Force speed with 10G ability
- **Duplex:** Port duplex capabilities.
  - **Auto:** Auto duplex with all capabilities
  - **Half:** Auto speed with 10M and 100M ability only
  - **Full:** Auto speed with 10M/100M/1000M ability only
- **Flow Control:** Port flow control.

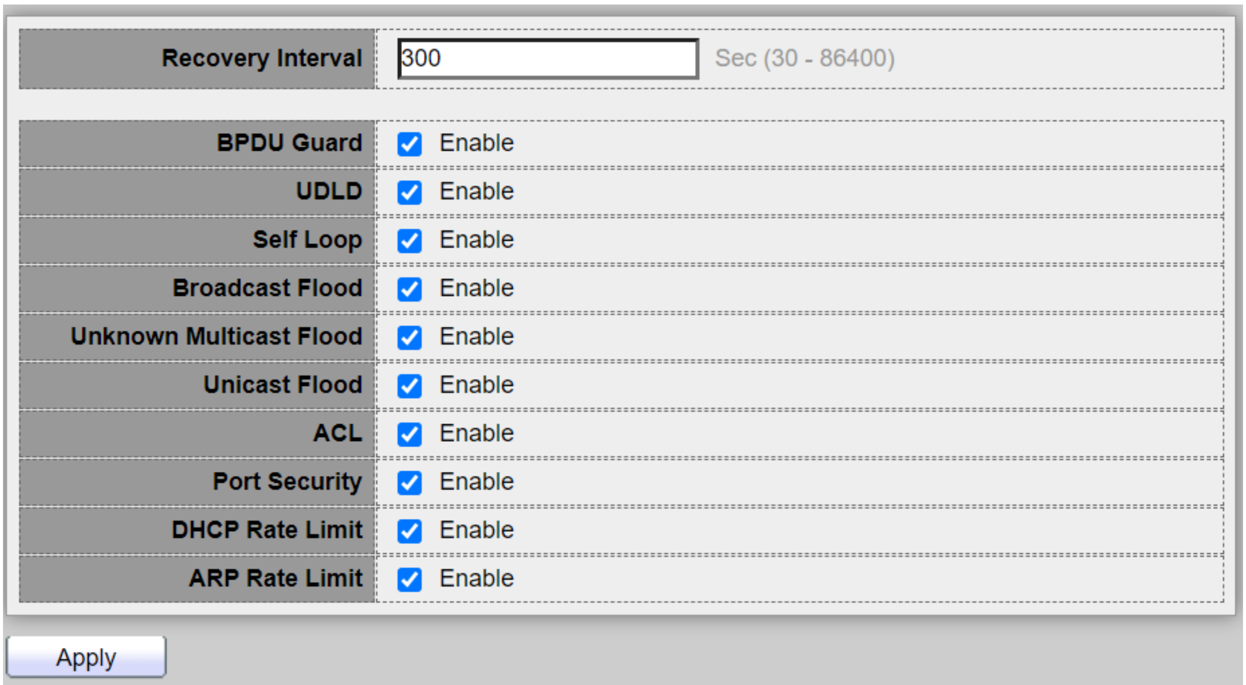
- **Auto:** Auto flow control by negotiation
- **Enabled:** Enable flow control ability
- **Disabled:** Disable flow control ability

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

5.2 Error Disabled

This function can block of faulty operation, including EPDU Guard / UDLD / Self Loop / Broadcast Flood / Unknown Multicast Flood / Unicast Flood / ACL / Port Security / DHCP Rate Limit / ARP Rate Limit etc.

After administrator enable this functions, if occur error in table functions then system will auto immediate block of faulty operation until the after the set time, system will auto re-enable.



Recovery Interval	300 Sec (30 - 86400)
BPDU Guard	☑ Enable
UDLD	☑ Enable
Self Loop	☑ Enable
Broadcast Flood	☑ Enable
Unknown Multicast Flood	☑ Enable
Unicast Flood	☑ Enable
ACL	☑ Enable
Port Security	☑ Enable
DHCP Rate Limit	☑ Enable
ARP Rate Limit	☑ Enable

- ➢ **Recovery Interval:** Auto recovery after this interval for error disabled port.
- ➢ **BPDU Guard:** Enabled to auto shutdown port when BPDU Guard reason occur.
  *This reason caused by STP BPDU Guard mechanism.
- ➢ **UDLD:** Enabled to auto shutdown port when UDLD violation occur.
- ➢ **Self Loop:** Enabled to auto shutdown port when Self Loop reason occur.
- ➢ **Broadcast Flood:** Enabled to auto shutdown port when Broadcast Flood reason occur.
  *This reason caused by broadcast rate exceed broadcast storm control rate.
- ➢ **Unknown Multicast Flood:** Enabled to auto shutdown port when Unknown Multicast Flood

reason occur. This reason caused by unknown multicast rate exceed unknown multicast storm control rate.

- **Unicast Flood:** Enabled to auto shutdown port when Unicast Flood reason occur.
  *This reason caused by unicast rate exceed unicast storm control rate.
- **ACL:** Enabled to auto shutdown port when ACL shutdown port reason occur.
  ***** This reason caused packet match the ACL shutdown port action**.**
- **Port Security:** Enabled to auto shutdown port when Port Security Violation reason occur.
  *****This reason caused by violation port security rules.
- **DHCP rate limit:** Enabled to auto shutdown port when DHCP rate limit reason occur.
  *****This reason caused by DHCP packet rate exceed DHCP rate limit.
- **ARP rate limit:** Enabled to auto shutdown port when ARP rate limit reason occur.
  *****This reason caused by DHCP packet rate exceed ARP rate limit.

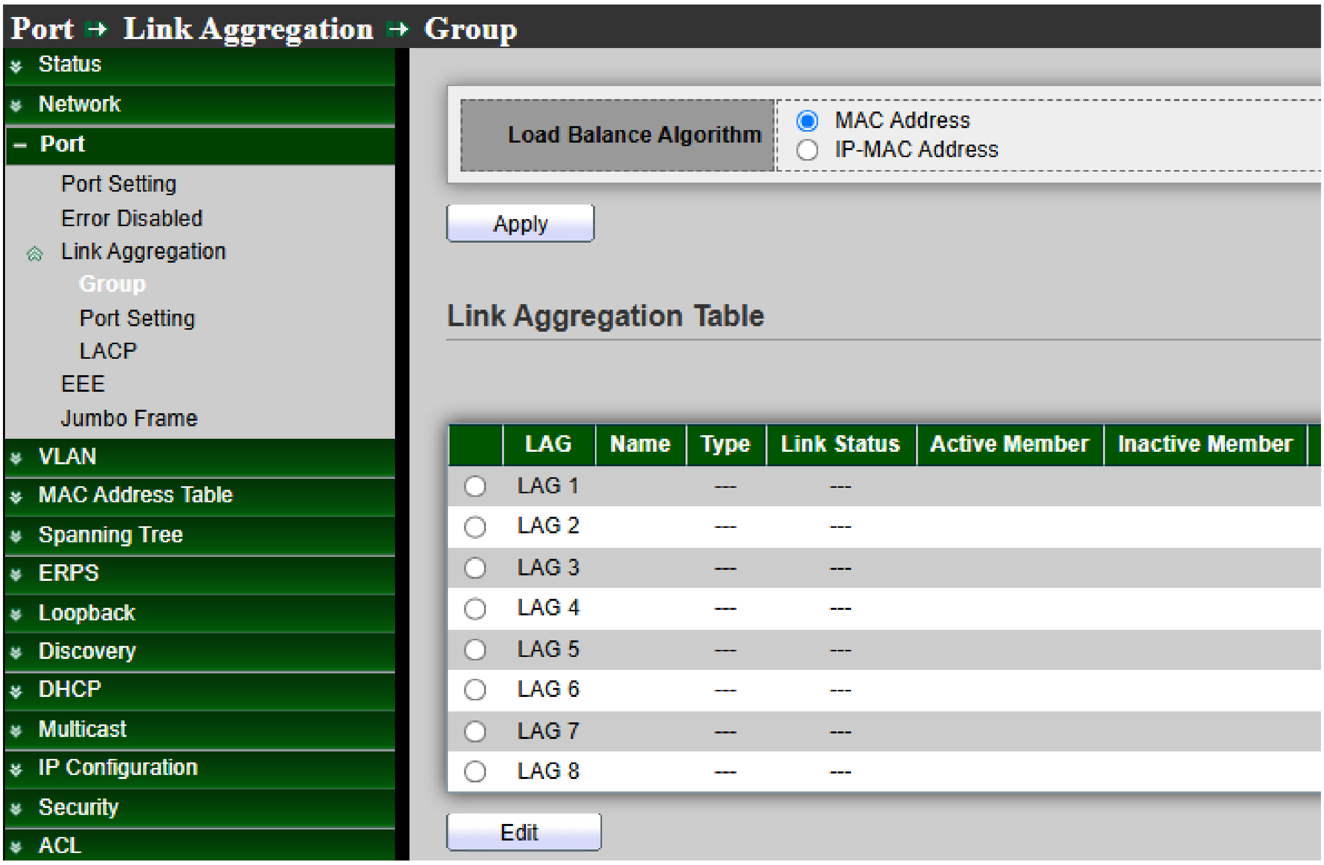
*Click the **"Apply"** button to save your changes settings.*

5.3 Link Aggregation

Link Aggregation is also referred to as link aggregation, teaming port, and port trunk for 802.3ad (LACP, Link Aggregation Control Protocol), The Port Aggregation can aggregate multiple Ethernet ports together to form a logical aggregation group. To upper layer entities, all the physical links in an aggregation group are a single logical link.

5.3.1 Group Configuration

Administrator can select use MAC Address or IP-MAC address of load balance Algorithm.
This system default can set 8 LA group, administrator can select LAG number and click Edit button go to set LA used ports.



Port → Link Aggregation → Group

Load Balance Algorithm: ● MAC Address ○ IP-MAC Address

Link Aggregation Table

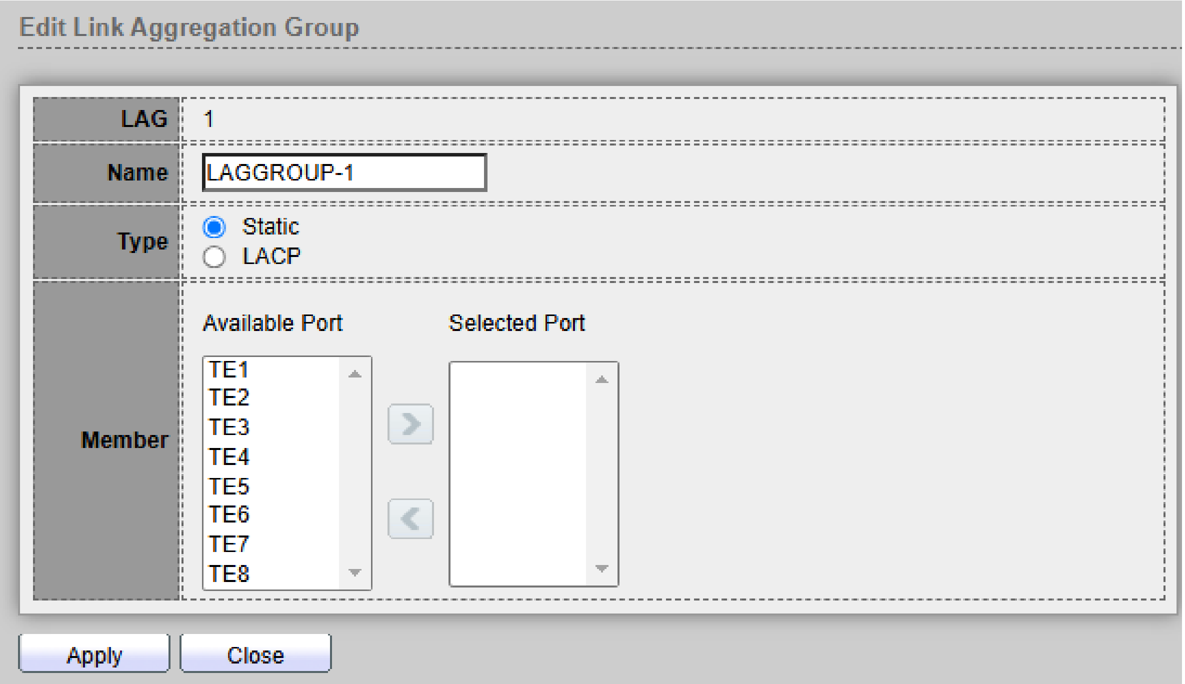
	LAG	Name	Type	Link Status	Active Member	Inactive Member
○	LAG 1		---	---		
○	LAG 2		---	---		
○	LAG 3		---	---		
○	LAG 4		---	---		
○	LAG 5		---	---		
○	LAG 6		---	---		
○	LAG 7		---	---		
○	LAG 8		---	---		

- **Load Balance Algorithm:** LAG load balance distribution algorithm.
  - **MAC Address:** Based on MAC address.
  - **IP-MAC Address:** Based on MAC address and IP address.

*Click the **"Apply"** button to save your changes settings.*

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.


Edit Link Aggregation Group

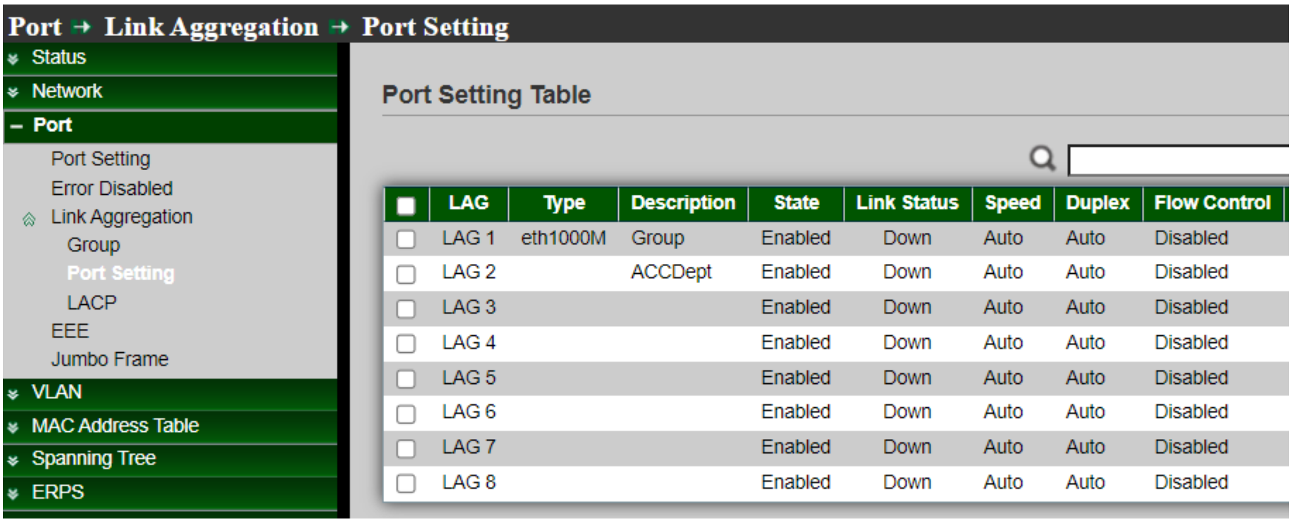
LAG	1
Name	LAGGROUP-1
Type	● Static ○ LACP
Member	Available Port: TE1, TE2, TE3, TE4, TE5, TE6, TE7, TE8 Selected Port:

- **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.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

5.3.2 Port Setting

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

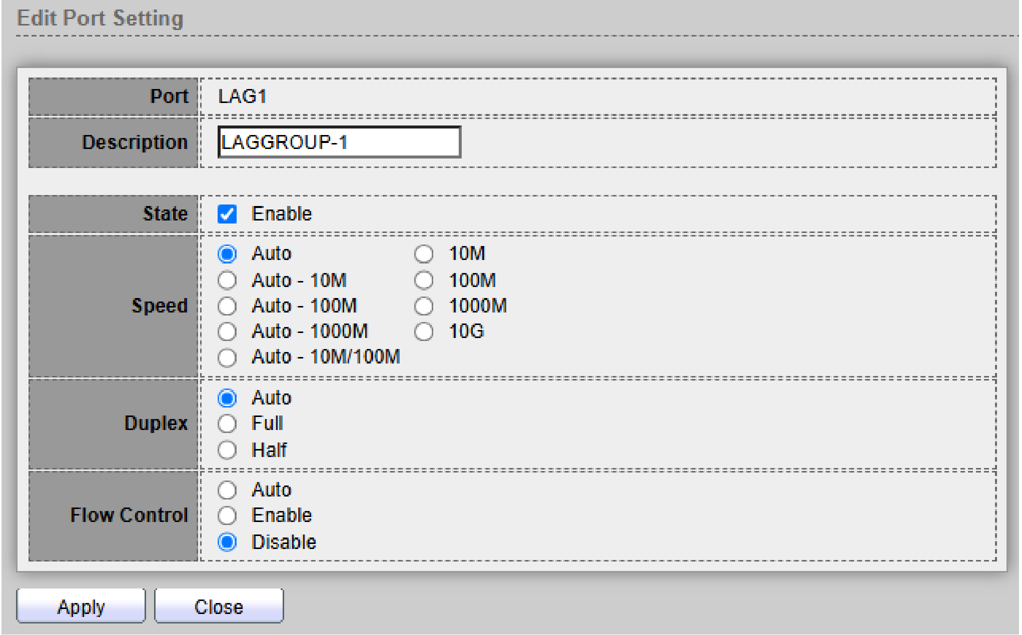


Port → Link Aggregation → Port Setting

Port Setting Table

□	LAG	Type	Description	State	Link Status	Speed	Duplex	Flow Control
□	LAG 1	eth1000M	Group	Enabled	Down	Auto	Auto	Disabled
□	LAG 2		ACCDept	Enabled	Down	Auto	Auto	Disabled
□	LAG 3			Enabled	Down	Auto	Auto	Disabled
□	LAG 4			Enabled	Down	Auto	Auto	Disabled
□	LAG 5			Enabled	Down	Auto	Auto	Disabled
□	LAG 6			Enabled	Down	Auto	Auto	Disabled
□	LAG 7			Enabled	Down	Auto	Auto	Disabled
□	LAG 8			Enabled	Down	Auto	Auto	Disabled

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



Edit Port Setting

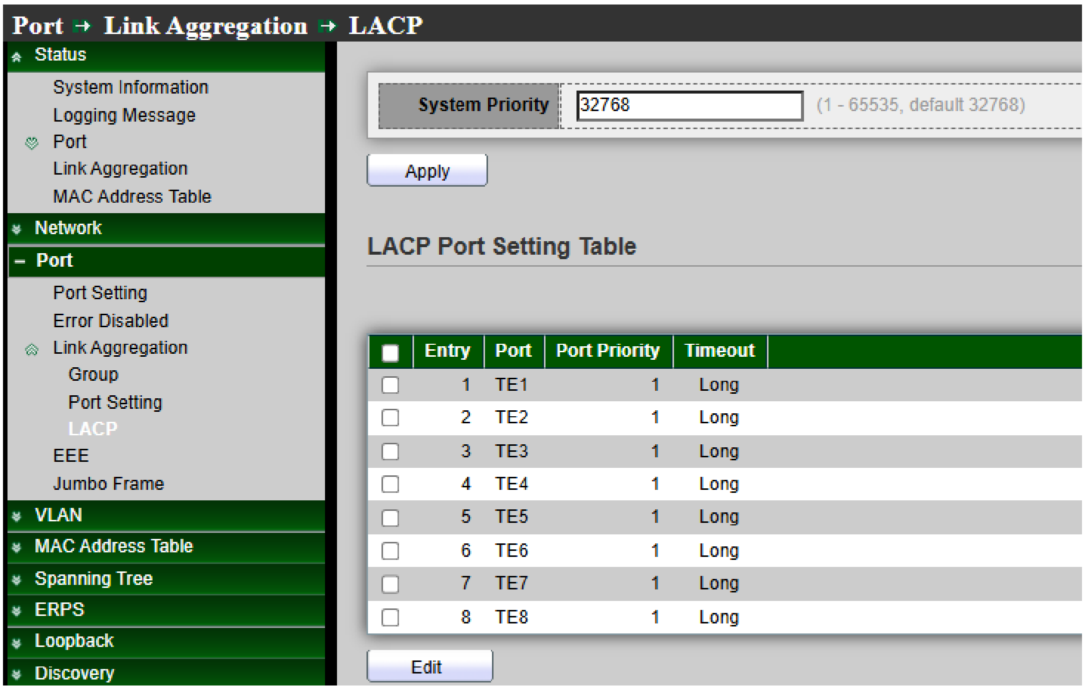
Port	LAG1
Description	LAGGROUP-1
State	☑ Enable
Speed	● Auto ○ 10M ○ Auto - 10M ○ 100M ○ Auto - 100M ○ 1000M ○ Auto - 1000M ○ 10G ○ Auto - 10M/100M
Duplex	● Auto ○ Full ○ Half
Flow Control	○ Auto ○ Enable ● Disable

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

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

5.3.3 LACP

The LACP can aggregate multiple Ethernet ports together to form a logical aggregation group. To upper layer entities, all the physical links in an aggregation group are a single logical link. Administrator can to configure LACP global and port configurations. Select ports and click "Edit" button to edit port configuration.



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

LACP Port Setting Table

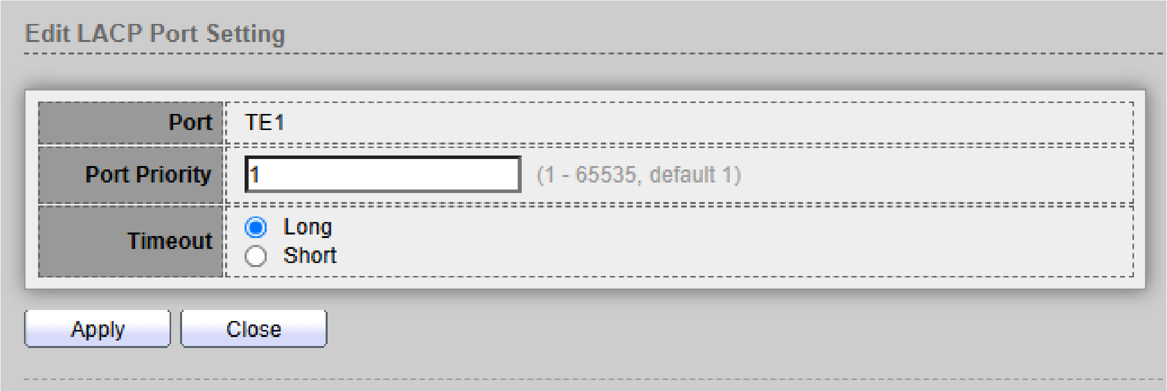
□	Entry	Port	Port Priority	Timeout
□	1	TE1	1	Long
□	2	TE2	1	Long
□	3	TE3	1	Long
□	4	TE4	1	Long
□	5	TE5	1	Long
□	6	TE6	1	Long
□	7	TE7	1	Long
□	8	TE8	1	Long

- **System Priority:** Administrator configures the LACP system priority on each switch running LACP. LACP uses the system priority with the switch MAC address to form the system ID and also during negotiation with other switches. This decides the system priority field in LACP PDU.

*Click the **"Apply"** button to save your changes settings.*

Note	The function with the lower system priority value determines which links between LACP partner devices are active and which are in standby for each LACP group. The device on the controlling end of the link uses port priorities to determine which ports are bundled into the aggregated bundle and which ports are put in standby mode. Port priorities on the other device (the no controlling end of the link) are ignored. In priority comparisons, numerically lower values have higher priority. Therefore, the system with the numerically lower value (higher priority value) for LACP system priority becomes the controlling system. If both devices have the same LACP system priority (for example, they are both configured with the default setting of 32768), the device MAC address determines which switch is in control.

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



Edit LACP Port Setting

Port	TE1
Port Priority	1 (1 - 65535, default 1)
Timeout	● Long ○ Short

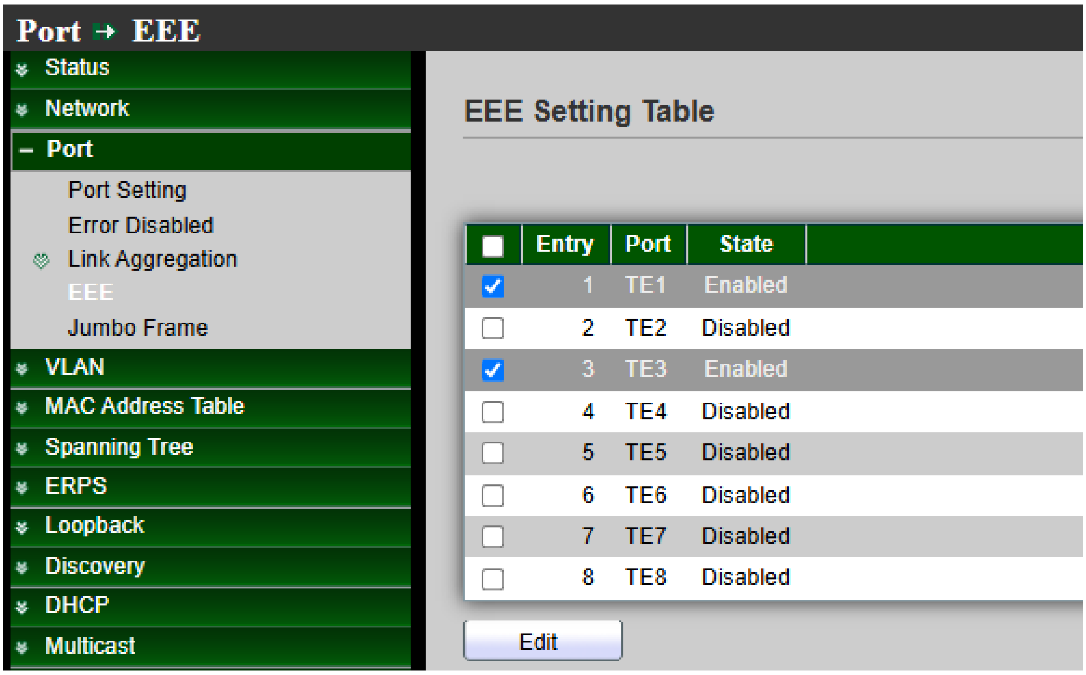
- **Port:** Selected port list.
- **Port Priority:** Enter the LACP priority value of the port.
- **Timeout:** The periodic transmissions type of LACP PDUs.
  - **Long:** Transmit LACP PDU with slow periodic (30s).
  - **Short:** Transmit LACPP DU with fast periodic (1s).

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

5.4 EEE

Energy Efficient Ethernet (EEE) combines the MAC with a family of physical layers that support operation in a low power mode. It is defined by IEEE 802.3az Energy Efficient Task Force. Lower power mode enables both the send and receive sides of the link to disable some functionality for power savings when lightly loaded. Transition to low power mode does not change the link status. Frames in transit are not dropped or corrupted in transition to and from low power mode. Transition time is transparent to upper layer protocols and applications.

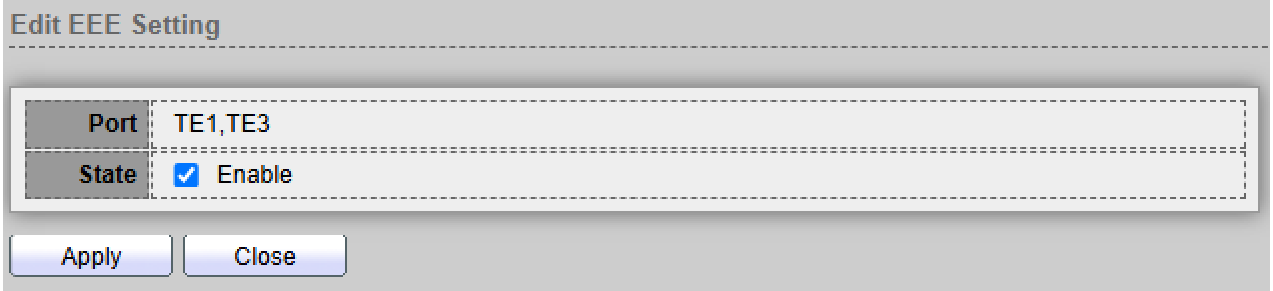
This switch support Energy-effcient Ethernet(EEE) function. Administrator can by ports to setting Enable or Disable for the EEE function. The default is “Disable”.



EEE Setting Table

□	Entry	Port	State
☑	1	TE1	Enabled
□	2	TE2	Disabled
☑	3	TE3	Enabled
□	4	TE4	Disabled
□	5	TE5	Disabled
□	6	TE6	Disabled
□	7	TE7	Disabled
□	8	TE8	Disabled

Field	Description
Port	Port Name
State/Operational Status	Port EEE admin state. • **Enabled:** EEE is enabled/ is operating • **Disabled:** EEE is disabled/ is no operating



Edit EEE Setting

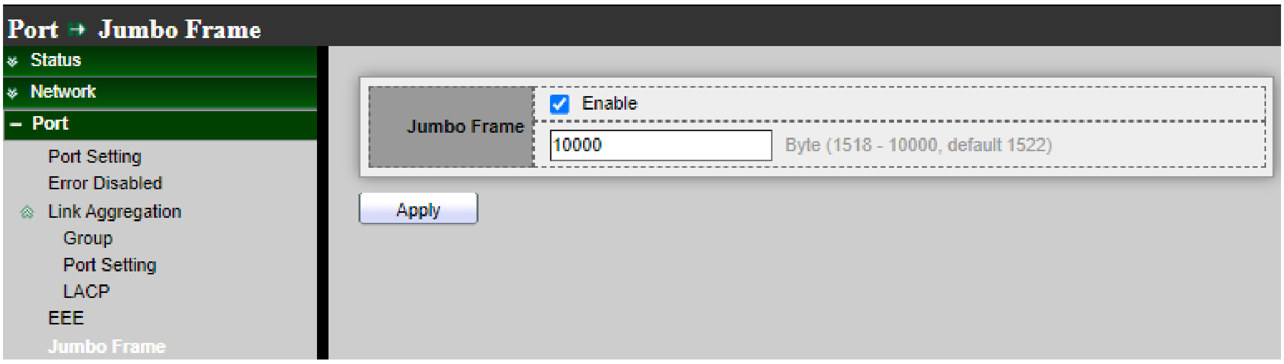
Port	TE1,TE3
State	☑ Enable

- **Port:** Selected port list.
- **State:** Port EEE admin state.
  - **Enable:** Enable EEE
  - **Disable:** Disable EEE

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

5.5 Jumbo Frame

The administrator can set the Jumbo Frame size and display it on this page.



Port → Jumbo Frame

Jumbo Frame	☑ Enable
	10000 Byte (1518 - 10000, default 1522)

- **Jumbo Frame:** Enable or disable jumbo frame. When jumbo frame is enabled, switch max frame size is allowed to configure. When jumbo frame is disabled, default frame size 1522 will be used.

Note	When jumbo frames are required, the maximum frame size (10000) of the switch is allowed to be configured. Uncheck to apply : When you click uncheck to **"Apply"** , The switch will back to default regular frame size "1522".

*Click the **"Apply"** button to save your changes settings.*

6. VLAN

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

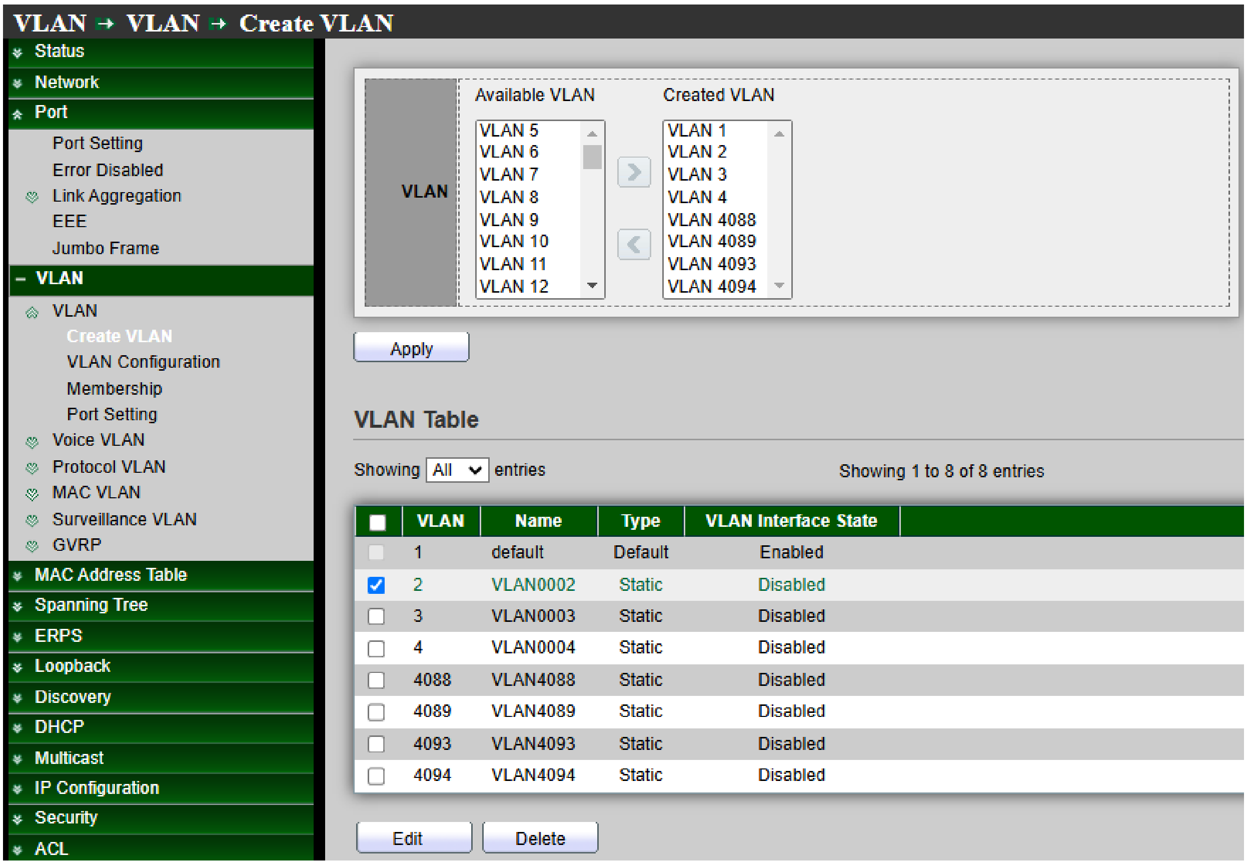
The **CS-3008XG** adding Virtual LAN (VLAN) support to a Layer 2 switch offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast, and like a router, it partitions the network into logical segments, which provides better administration, security and management of multicast traffic.

Administrator can set IEEE 802.1q Tag Based VLAN or Port Based VLAN. System default is VLAN1 Port based (PVID).

6.1 VLAN

6.1.1 Create VLAN

Administrator can select VLAN number in Available VLAN list, this VLAN number based on IEEE 802.1q standard. Available VLAN list can be multiple choices.



	Available VLAN	Created VLAN
VLAN	VLAN 5 VLAN 6 VLAN 7 VLAN 8 VLAN 9 VLAN 10 VLAN 11 VLAN 12	VLAN 1 VLAN 2 VLAN 3 VLAN 4 VLAN 4088 VLAN 4089 VLAN 4093 VLAN 4094

VLAN Table

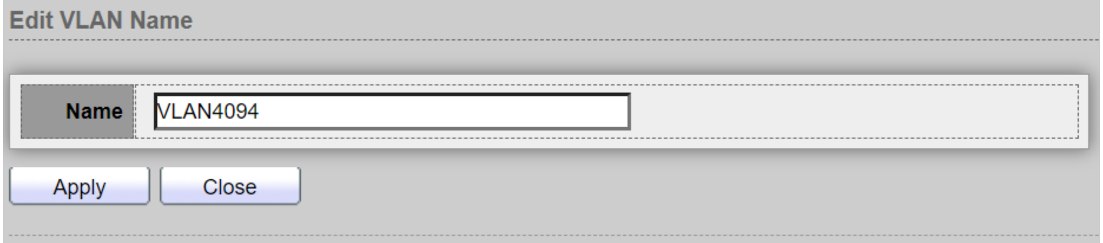
Showing All entries Showing 1 to 8 of 8 entries

□	VLAN	Name	Type	VLAN Interface State
□	1	default	Default	Enabled
☑	2	VLAN0002	Static	Disabled
□	3	VLAN0003	Static	Disabled
□	4	VLAN0004	Static	Disabled
□	4088	VLAN4088	Static	Disabled
□	4089	VLAN4089	Static	Disabled
□	4093	VLAN4093	Static	Disabled
□	4094	VLAN4094	Static	Disabled

- **VLAN:** Administrator can select VLANs number in "Available VLAN" table and move to "Created VLAN" table will complete the 802.1q VLAN.

*Click the **"Apply"** button to save your changes settings.*

VLAN Table: Administrator can checkbox VLAN to edit or delete, if check and click "Edit" button then administrator can manual modify name description for this VLAN.



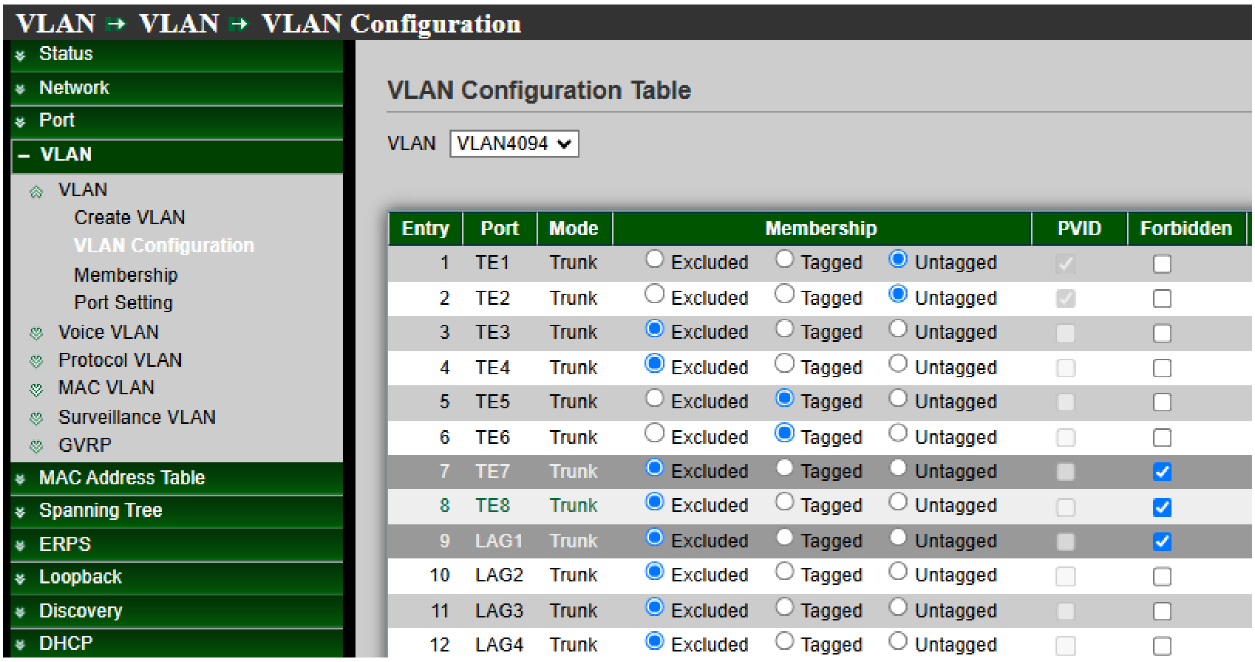
Edit VLAN Name

Name: VLAN4094

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

6.1.2 VLAN Configuration

Administrator can choose set Excluded / Forbidden / Tagged / Untagged function in membership table of the Port and LAG.



VLAN Configuration Table

VLAN VLAN4094

Entry	Port	Mode	Membership			PVID	Forbidden
1	TE1	Trunk	○ Excluded	○ Tagged	● Untagged	☑	□
2	TE2	Trunk	○ Excluded	○ Tagged	● Untagged	☑	□
3	TE3	Trunk	● Excluded	○ Tagged	○ Untagged	□	□
4	TE4	Trunk	● Excluded	○ Tagged	○ Untagged	□	□
5	TE5	Trunk	○ Excluded	● Tagged	○ Untagged	□	□
6	TE6	Trunk	○ Excluded	● Tagged	○ Untagged	□	□
7	TE7	Trunk	● Excluded	○ Tagged	○ Untagged	□	☑
8	TE8	Trunk	● Excluded	○ Tagged	○ Untagged	□	☑
9	LAG1	Trunk	● Excluded	○ Tagged	○ Untagged	□	☑
10	LAG2	Trunk	● Excluded	○ Tagged	○ Untagged	□	□
11	LAG3	Trunk	● Excluded	○ Tagged	○ Untagged	□	□
12	LAG4	Trunk	● Excluded	○ Tagged	○ Untagged	□	□

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

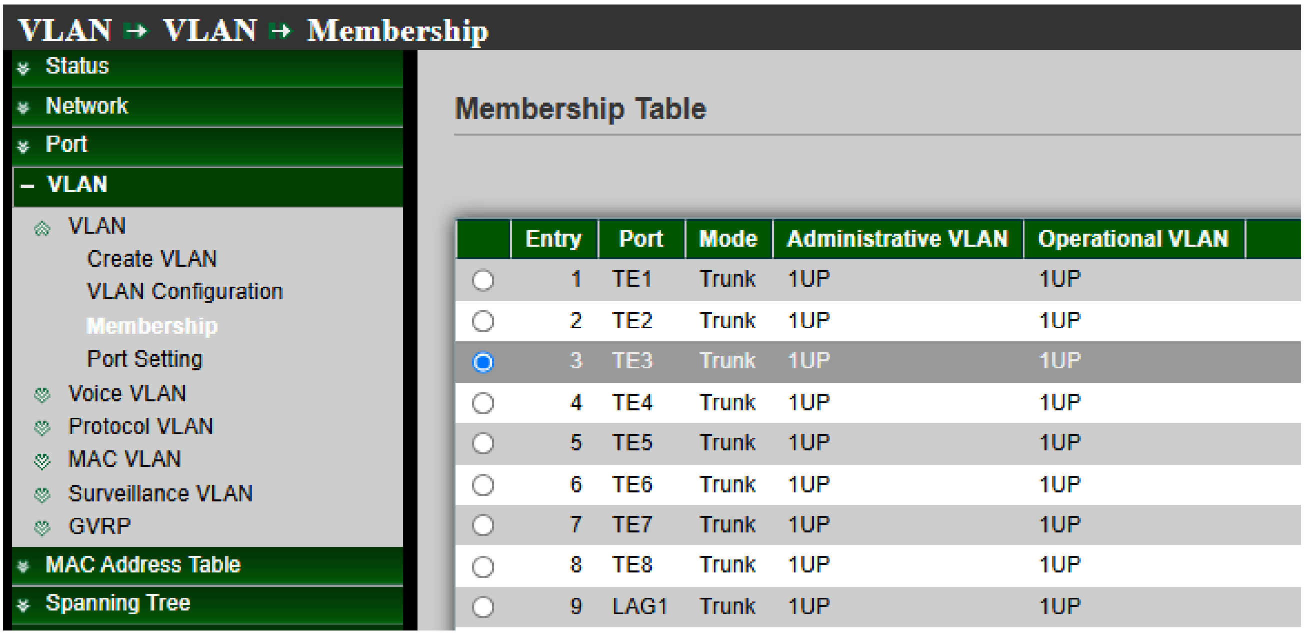
➢ **VLAN:** Administrator can click drop down menu to choose VLAN and set.

- **Excluded:** This interface is currently not a member of the VLAN. This is the default for all the ports and LAGs.
- **Tagged**: This interface is a tagged member of the VLAN.

- **Untagged**: This interface is an untagged member of the VLAN. Frames of the VLAN are sent untagged to the interface VLAN.
- **PVID**: Check to set the PVID of the interface to the VID of the VLAN. PVID is a per-port setting.
- **Forbidden:** Select for this specified port of the Forbidden.

6.1.3 Membership

Display all port setting information. Administrator can checkbox and click "**Edit**" button to modify VLAN type. *(Note: Number=VLAN number, F=Forbidden, T=Tagged, U=Untagged, P=PVID)*
When a port is forbidden default VLAN membership, that port is not allowed membership in any other VLAN. An internal VID of 4095 is assigned to the port. This PVID on the ports between the two devices must be the same if the ports are to send and receive untagged packets to and from the VLAN. Otherwise, traffic might leak from one VLAN to another.

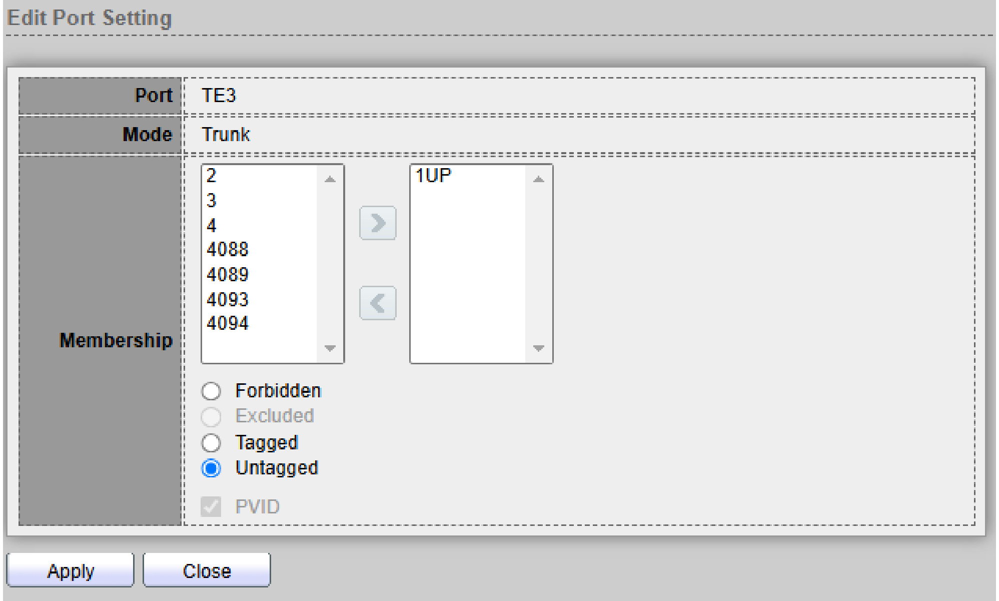


Membership Table

	Entry	Port	Mode	Administrative VLAN	Operational VLAN
○	1	TE1	Trunk	1UP	1UP
○	2	TE2	Trunk	1UP	1UP
●	3	TE3	Trunk	1UP	1UP
○	4	TE4	Trunk	1UP	1UP
○	5	TE5	Trunk	1UP	1UP
○	6	TE6	Trunk	1UP	1UP
○	7	TE7	Trunk	1UP	1UP
○	8	TE8	Trunk	1UP	1UP
○	9	LAG1	Trunk	1UP	1UP

Field	Description
Port	Display the interface of port entry.
Mode	Display the interface VLAN mode of port.
Administrative VLAN	Display the administrative VLAN list of this port.

Operational VLAN	Display the operational VLAN list of this port. Operational VLAN means the VLAN status that really runs in device. It may different to administrative VLAN.



Edit Port Setting

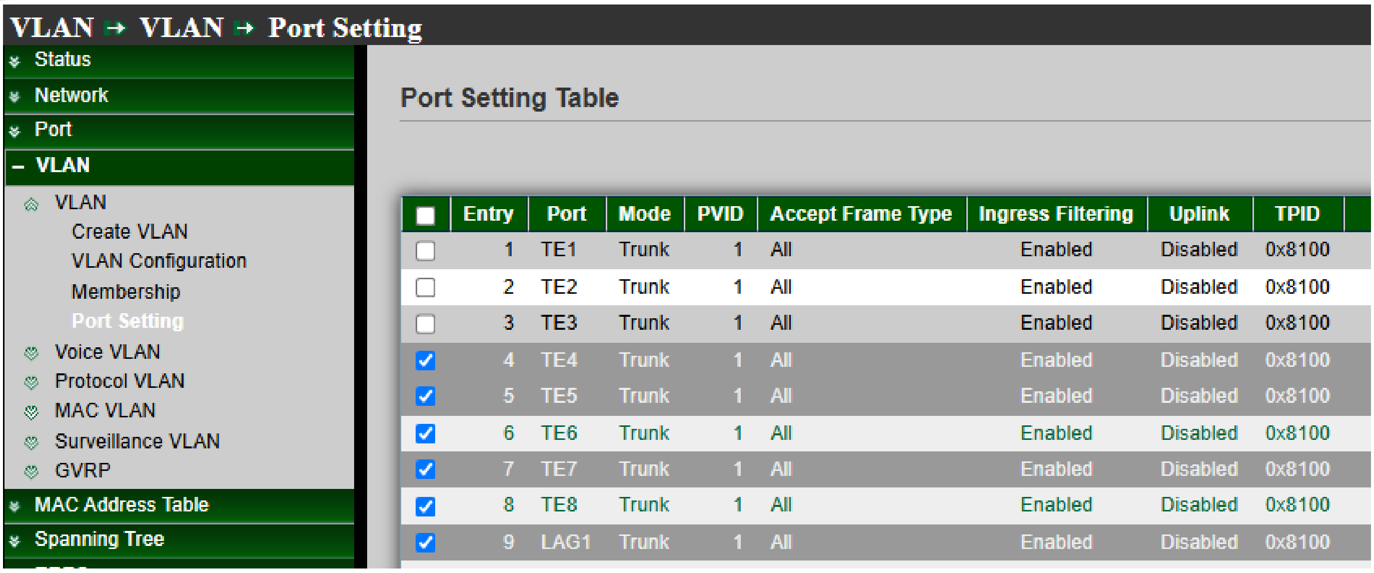
Port	TE3
Mode	Trunk
Membership	2 3 4 4088 4089 4093 4094 1UP ○ Forbidden ○ Excluded ○ Tagged ● Untagged ☑ PVID

- **Port:** Display selected port number.
- **Mode:** Displays the port VLAN mode that was selected on the Interface Settings page.
- **Membership:** Move the VLAN IDs from the left list to the right list by using the arrow buttons. The default VLAN might appear in the right list if it is tagged, but it cannot be selected.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

6.1.4 Port Setting

Administrator can set Access / Trunk / Hybrid for VLAN mode.

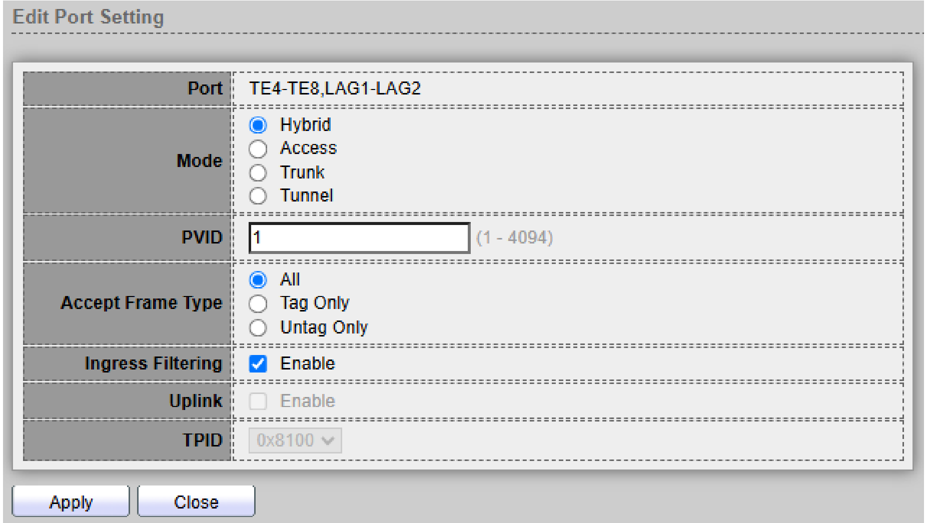


VLAN → VLAN → Port Setting

Port Setting Table

■	Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
□	1	TE1	Trunk	1	All	Enabled	Disabled	0x8100
□	2	TE2	Trunk	1	All	Enabled	Disabled	0x8100
□	3	TE3	Trunk	1	All	Enabled	Disabled	0x8100
☑	4	TE4	Trunk	1	All	Enabled	Disabled	0x8100
☑	5	TE5	Trunk	1	All	Enabled	Disabled	0x8100
☑	6	TE6	Trunk	1	All	Enabled	Disabled	0x8100
☑	7	TE7	Trunk	1	All	Enabled	Disabled	0x8100
☑	8	TE8	Trunk	1	All	Enabled	Disabled	0x8100
☑	9	LAG1	Trunk	1	All	Enabled	Disabled	0x8100

Field	Description
Port	Display the interface.
Mode	Display the VLAN mode for Hybrid/Access/Trunk/Tunnel mode of port.
PVID	Display the Port-based VLAN ID of port.
Accept Frame Type	Display accept frame type of port.
Ingress Filtering	Display ingress filter status of port.
Uplink	Display uplink status.
TPID	Display TPID used of interface.



Edit Port Setting

Port	TE4-TE8,LAG1-LAG2
Mode	● Hybrid ○ Access ○ Trunk ○ Tunnel
PVID	1 (1 - 4094)
Accept Frame Type	● All ○ Tag Only ○ Untag Only
Ingress Filtering	☑ Enable
Uplink	□ Enable
TPID	0x8100

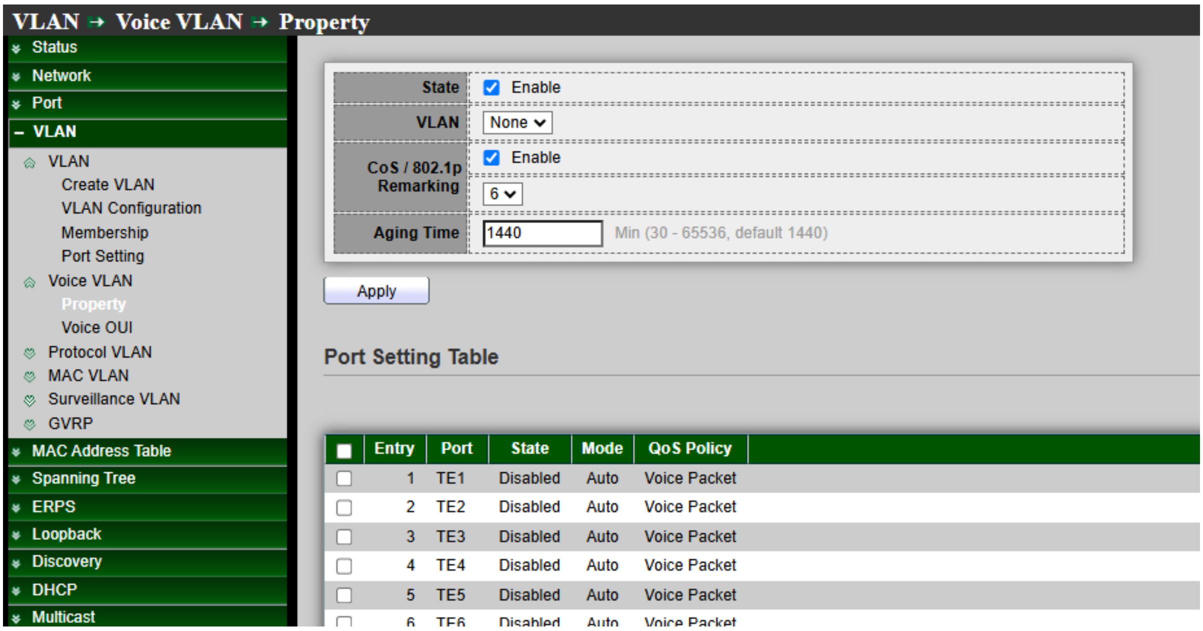
- **Hybrid:** The interface can be a tagged or untagged member of one or more VLANs.
- **Access:** The interface is an untagged member of a single VLAN. A port configured in this mode is known as an access port.
- **Trunk:** The interface is an untagged member of one VLAN at most, and is a tagged member of zero or more VLANs. A port configured in this mode is known as a trunk port.
- **Tunnel:** This enables the user to use own VLAN arrangements (PVID) across the provider network.
- **PVID:** Enter the Port VLAN ID (PVID) of the VLAN to which incoming untagged and priority tagged frames are classified.
- **Accept Frame Type:** Select the type of frame that the interface can receive. Frames that are not of the configured frame type are discarded at ingress. These frame types are only available in General mode. As follow.
  - **All:** The interface accepts all types of frames: untagged frames, tagged frames, and priority tagged frames.
  - **Tag Only:** The interface accepts only tagged frames.
  - **Untag Only:** The interface accepts only untagged and priority frames.
- **Ingress Filtering:** Administrator can check Enable to enable ingress filtering. When an interface is ingress filtering enabled, the interface discards all incoming frames that are classified as VLANs of which the interface is not a member. Ingress filtering can be disabled or enabled on general ports. It is always enabled on access ports and trunk ports.
- **Uplink:** Administrator can check **Enable** to set the interface as an uplink port.
- **TPID:** If Unlink is enabled, select the Modified Tag Protocol Identifier (TPID) value for the interface.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

6.2 Voice VLAN

Voice VLAN allows you to enhance VoIP service by configuring ports to carry IP Voice traffic from IP phones on a specific VLAN. VoIP traffic has a preconfigured OUI prefix in the source MAC address. Administrator can set VLAN ID in the range of 1 to 4094.

6.2.1 Property



VLAN → Voice VLAN → Property

State	☑ Enable
VLAN	None
CoS / 802.1p Remarking	☑ Enable 6
Aging Time	1440 Min (30 - 65536, default 1440)

Apply

Port Setting Table

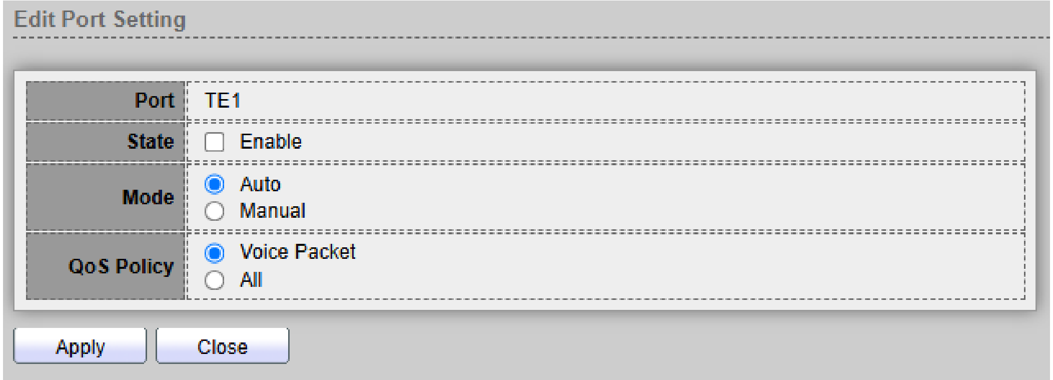
□	Entry	Port	State	Mode	QoS Policy
□	1	TE1	Disabled	Auto	Voice Packet
□	2	TE2	Disabled	Auto	Voice Packet
□	3	TE3	Disabled	Auto	Voice Packet
□	4	TE4	Disabled	Auto	Voice Packet
□	5	TE5	Disabled	Auto	Voice Packet
□	6	TE6	Disabled	Auto	Voice Packet

- **State:** Administrator can choose Enable or Disable this function.
- **VLAN:** Administrator can choose VLAN.
- **CoS / 802.1P Remarking**: Administrator can set CoS 802.1p priority level for the VLAN.
- **Port Aging Time:** Administrator can set aging time for this rule.

*Click the **"Apply"** button to save your changes settings.*

Field	Description
Port	Display port entry.
State	Display enable/disabled status of interface.
Mode	Display voice VLAN mode.

QoS Policy	Display voice VLAN remark will effect which kind of packet.



Edit Port Setting

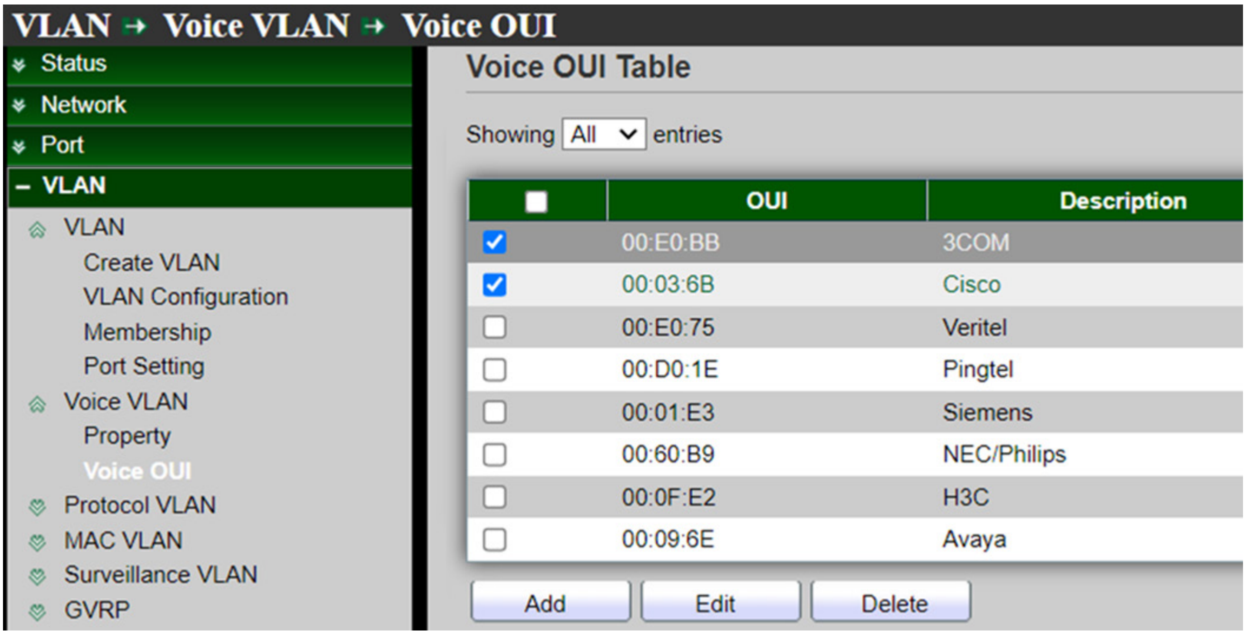
Port	TE1
State	□ Enable
Mode	● Auto ○ Manual
QoS Policy	● Voice Packet ○ All

- **Port:** Display port entry.
- **State:** Enable/disabled status of interface.
- **Mode**: Choose voice VLAN mode.
- **Qos Policy**: Choose voice VLAN remark will effect which kind of packet.

Click t*he* ***"Apply"*** *button to save your changes or* ***"Close"*** *the button to close settings.*

6.2.2 Voice OUI

Organizationally Unique Identifiers (OUI) is the first three bytes of a MAC Address, while the last three bytes contain a unique station ID. Administrator can add a specific manufacturer with the OUI. Once the OUI is added, all traffic received on voice VLAN ports from the specific IP phone with a listed OUI is forwarded on the voice VLAN. Unlike the telephony OUI mode that detects voice devices based on telephony OUI, Auto Voice VLAN mode depends on auto smart port to dynamically add the ports to the voice VLAN. The default has set 8 companies for the voice phone.



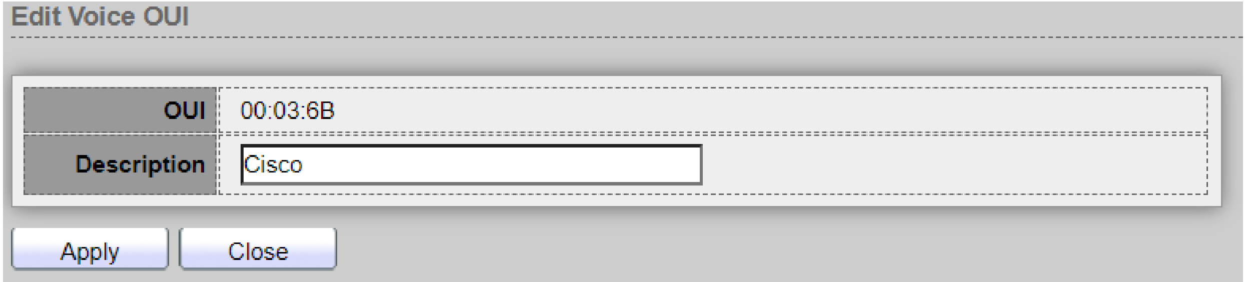
VLAN → Voice VLAN → Voice OUI

Voice OUI Table

Showing All entries

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

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



Edit Voice OUI

OUI	00:03:6B
Description	Cisco

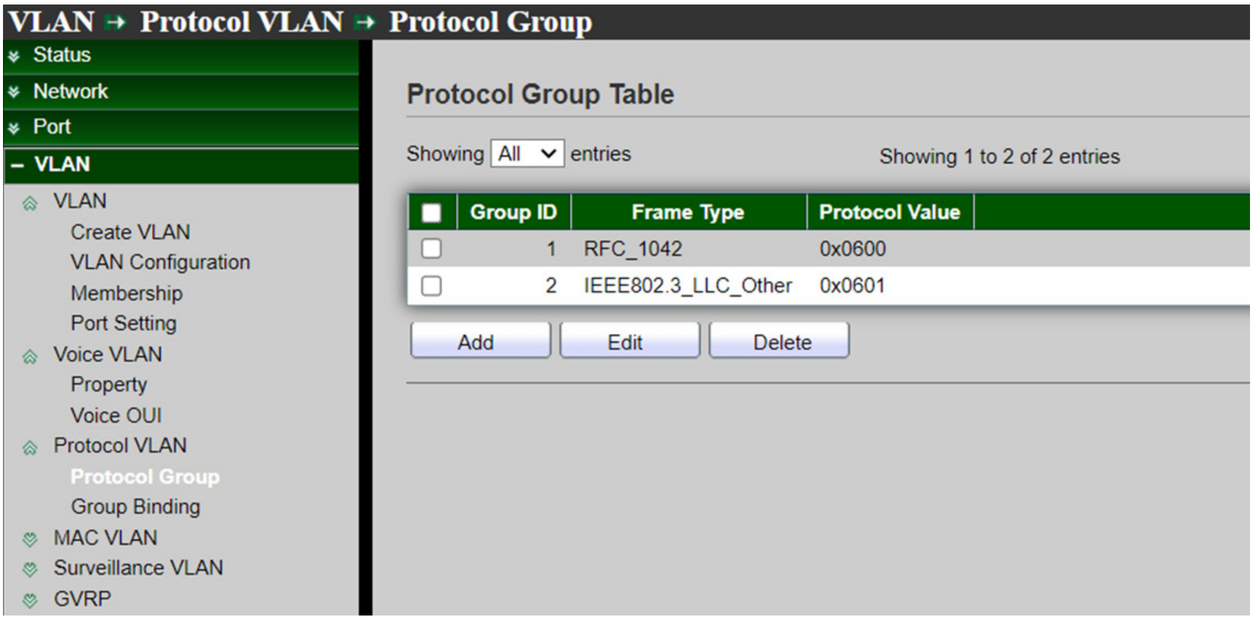
Administrator can create new OUI or modify or delete OUI in table
Click **“add”** button can create new OUI.
Click “**Edit**” button can modify OUI data.
Click **“Delete”** button can delete OUI data.

*Click the **“Apply”** button to save your changes or **“Close”** the button to close settings.*

6.3 Protocol VLAN

6.3.1 Protocol Group

Administrator can configure this page to add or edit groups settings of protocol VLAN, Setting **“add”** and “Edit” and **“Delete”** function for this management.

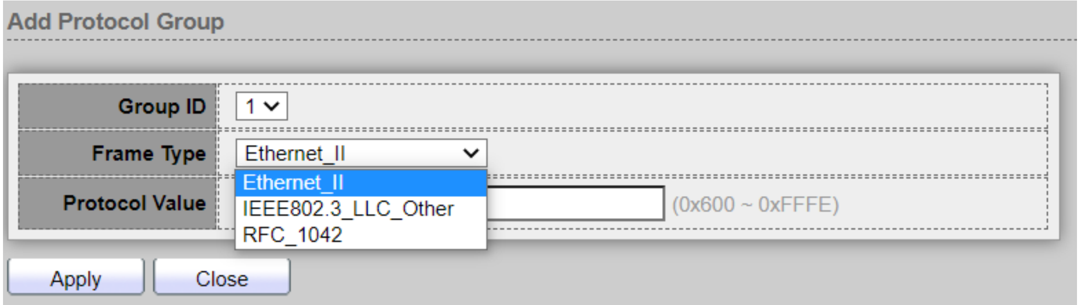


Protocol Group Table

Showing All entries   Showing 1 to 2 of 2 entries

□	Group ID	Frame Type	Protocol Value
□	1	RFC_1042	0x0600
□	2	IEEE802.3_LLC_Other	0x0601

Field	Description
Group ID	Display group ID of entry.
Frame Type	Display frame type of entry.
Protocol Value	Display protocol value of entry.



Add Protocol Group

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

- **Group ID :** Select group ID of list. The range from 1 to 8.
- **Frame Type :** Select frame type of list that maps packets to protocol-defined VLANs by

examining the type octet within the packet header to discover the type of protocol associated with it.

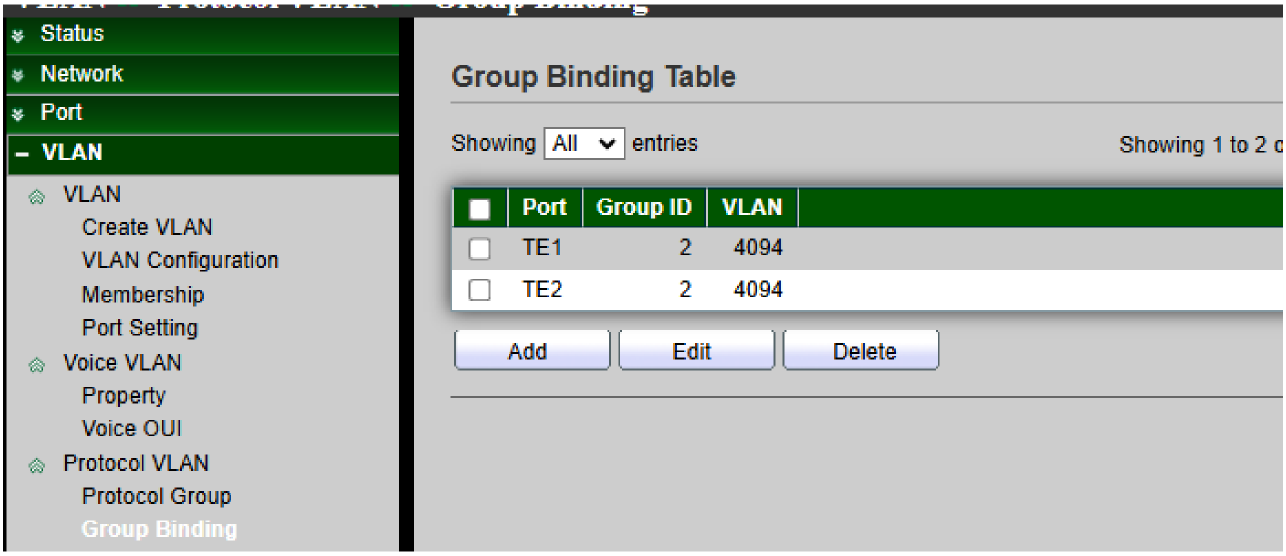
- **Ethernet_II :** packet type is Ethernet version 2.
- **IEEE802.3_LLC_Other :** packet type is 802.3 packet with LLC other header.
- **RFC_1042 :** packet type is rfc 1042 packet.

➢ **Protocol Value :** Input protocol value of the target protocol. Packets match this protocol value classified to specified VLAN ID.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

6.3.2 Group Binding

Administrator can configure this bind protocol VLAN group to each port with VLAN ID, Setting **"add"** and "Edit" and **"Delete"** function for this management.

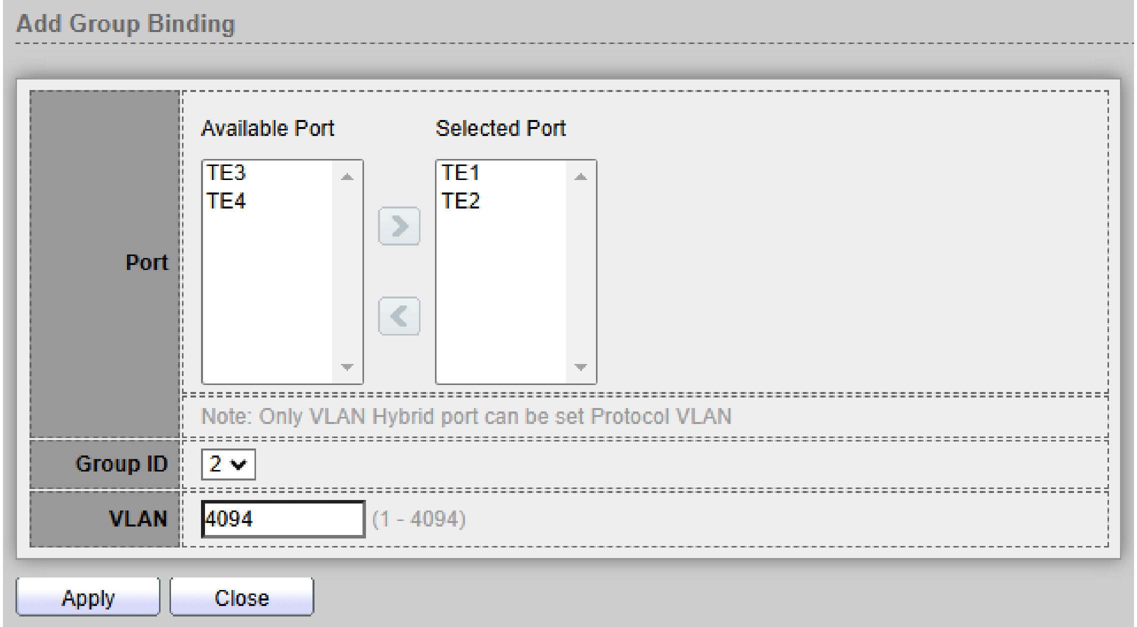


Group Binding Table

Showing All entries Showing 1 to 2 o

□	Port	Group ID	VLAN
□	TE1	2	4094
□	TE2	2	4094

Field	Description
Port	Display port ID that binding with protocol group entry.
Group ID	Display group ID that port binding with.
VLAN	Display VLAN ID that assign to packets which match protocol group.



Add Group Binding

Port	Available Port: TE3 TE4 Selected Port: TE1 TE2 Note: Only VLAN Hybrid port can be set Protocol VLAN
Group ID	2
VLAN	4094 (1 - 4094)

- **Port :** Select ports in left box then move to right to binding with protocol group. Or select ports in right box then move to left to unbind with protocol group. Only interface has hybrid VLAN mode can be selected and bound with protocol group. Only available on Add dialog.   .
- **Group ID :** Select a Group ID to associate with port. Only available on Add dialog.
- **VLAN :** Input VLAN ID that will assign to packets which match protocol group.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

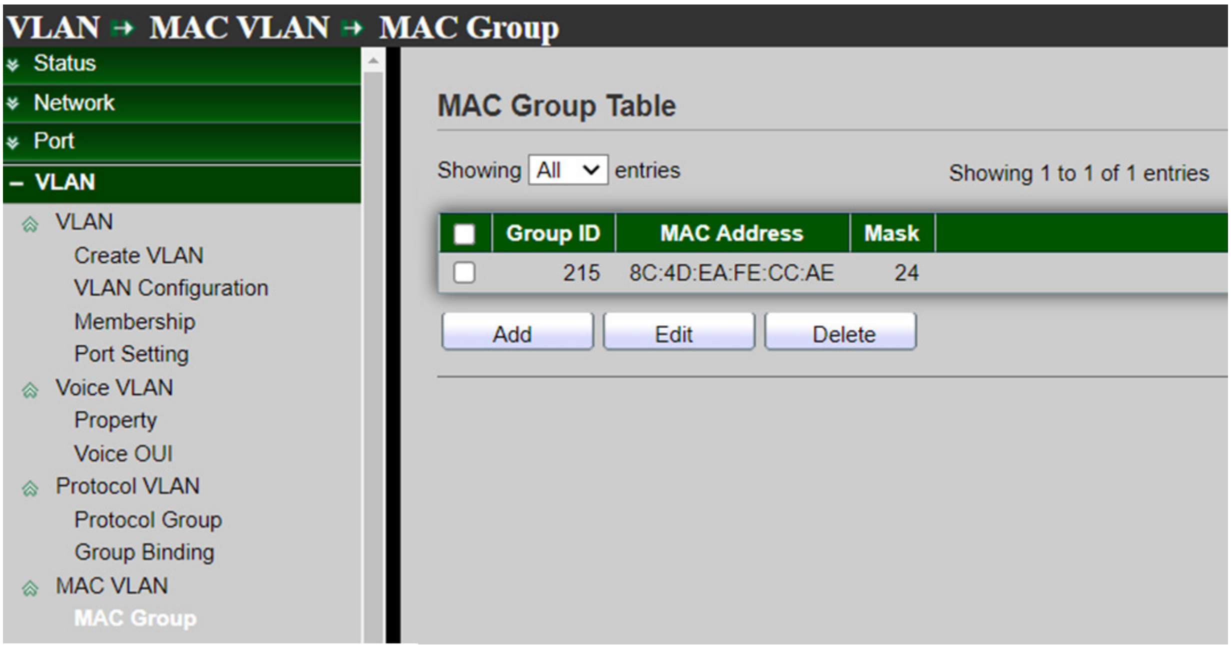
6.4 MAC VLAN

6.4.1 MAC Group

The MAC VLAN feature allows incoming untagged packets to be assigned to a VLAN and thus classify traffic based on the source MAC address of the packet. You define a MAC to VLAN mapping by configuring an entry in the MAC to VLAN table. An entry is specified using a source MAC address and the appropriate VLAN ID. The MAC to VLAN configurations are shared across all ports of the device (i.e., there is a system-wide table that has MAC address to VLAN ID mappings).

When untagged or priority tagged packets arrive at the switch and entries exist in the MAC to VLAN table, the source MAC address of the packet is looked up. If an entry is found, the corresponding VLAN ID is assigned to the packet. If the packet is already priority tagged it will maintain this value;

otherwise, the priority will be set to 0 (zero). The assigned VLAN ID is verified against the VLAN table. If the VLAN is valid, ingress processing on the packet continues; otherwise, the packet is dropped. This implies that you can configure a MAC address mapping to a VLAN that has not been created on the system, Setting **"add"** and "Edit" and **"Delete"** function for this management.

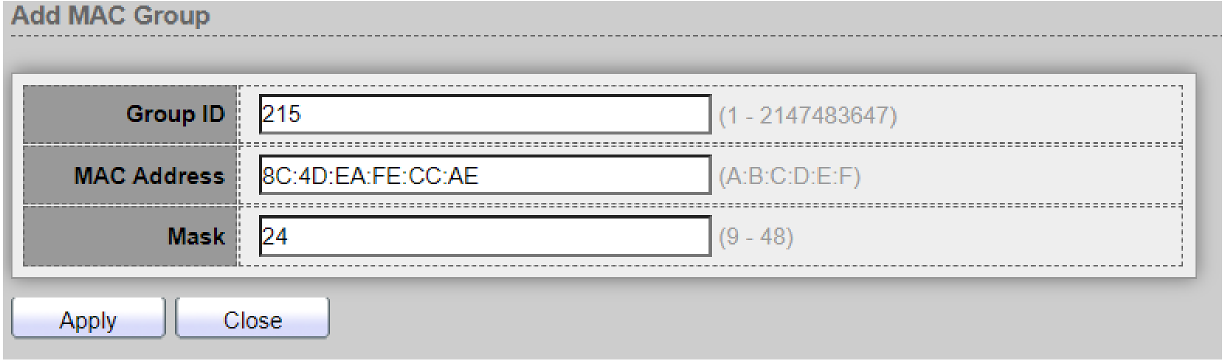


MAC Group Table

Showing All entries   Showing 1 to 1 of 1 entries

□	Group ID	MAC Address	Mask
□	215	8C:4D:EA:FE:CC:AE	24

Field	Description
Group ID	Display group ID of entry.
MAC Address	Display mac address of entry.
Mask	Display mask of mac address for classified packet.



Add MAC Group

Group ID	215	(1 - 2147483647)
MAC Address	8C:4D:EA:FE:CC:AE	(A:B:C:D:E:F)
Mask	24	(9 - 48)

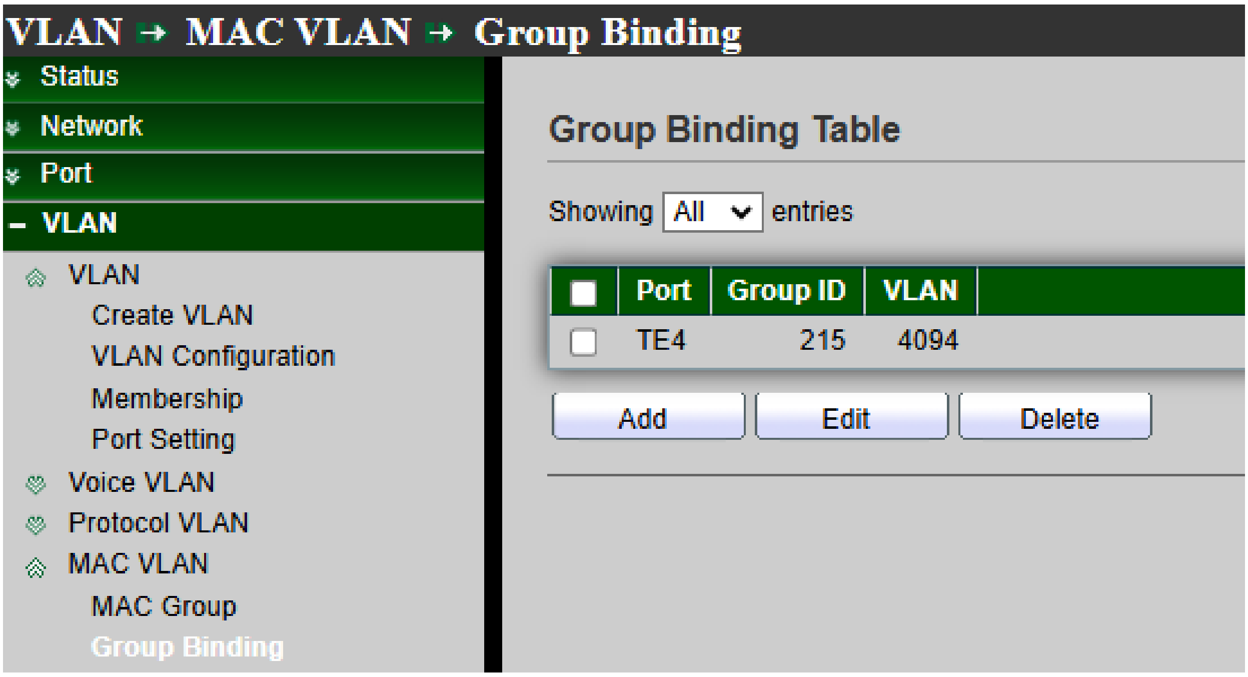
- **Group ID:** Add a Group ID number.

- **MAC Address :** Enter the MAC Address.
- **Mask**: Enter the mask of mac address for classified packet..

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

6.4.2 Group Binding

The Group Binding allows user to bind MAC VLAN group to each port with VLAN ID, Setting **"add"** and "Edit" and **"Delete"** function for this management.



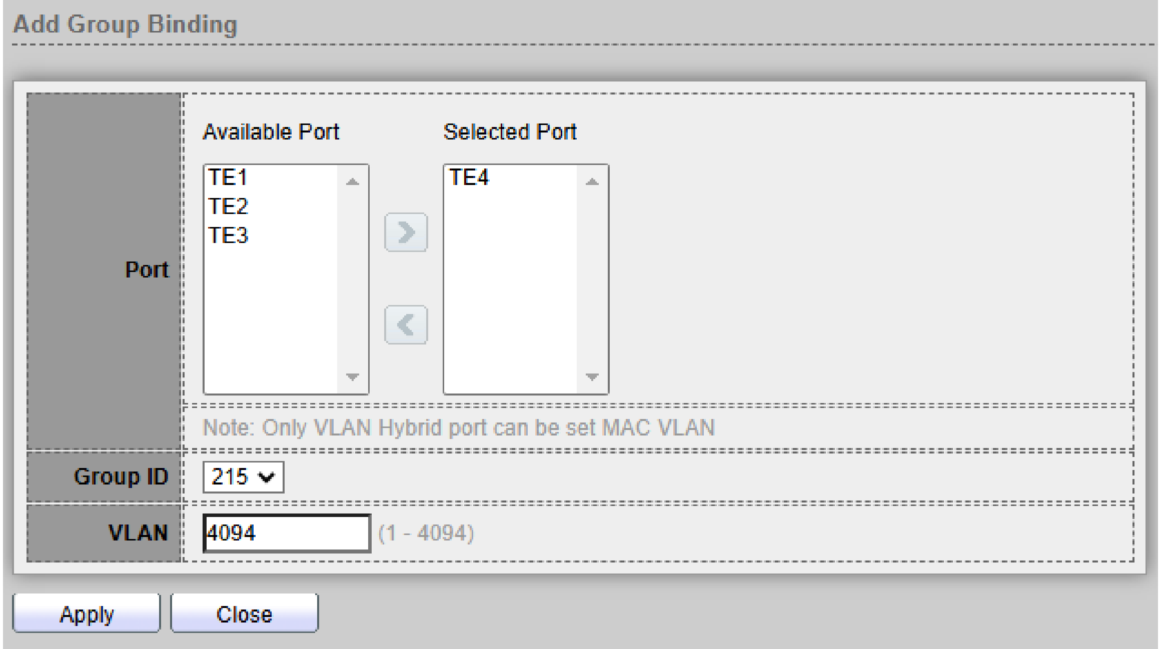
VLAN → MAC VLAN → Group Binding

Group Binding Table

Showing All entries

□	Port	Group ID	VLAN
□	TE4	215	4094

Field	Description
Field	Description.
Port	Display port ID that binding with protocol group entry.
Group ID	Display group ID that port binding with.
VLAN	Display VLAN ID that assign to packets which match protocol group.



Add Group Binding

Port	Available Port: TE1 TE2 TE3 Selected Port: TE4
	Note: Only VLAN Hybrid port can be set MAC VLAN
Group ID	215
VLAN	4094 (1 - 4094)

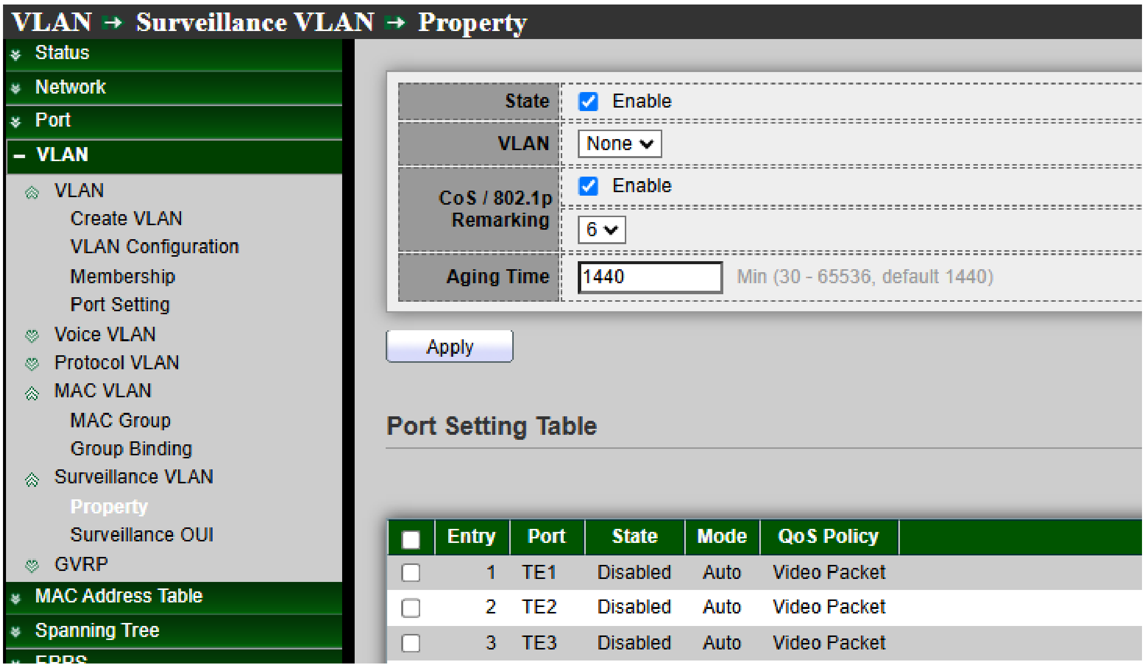
- **Port:** Select the port in the left frame and move to the right to bind to the mac group; or select the port in the right frame and move to the left to bind to the mac group. Only interfaces with mixed VLAN mode can be selected and bound to the protocol group.
- **Group ID:** Choose a Group ID associated with the port.
- **VLAN**: Enter the VLAN ID that will be assigned to packets matching the MAC Group.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

6.5 Surveillance VLAN

6.5.1 Property

Administrator can configure this page to configure global and per interface settings of urveillance VLAN.



VLAN → Surveillance VLAN → Property

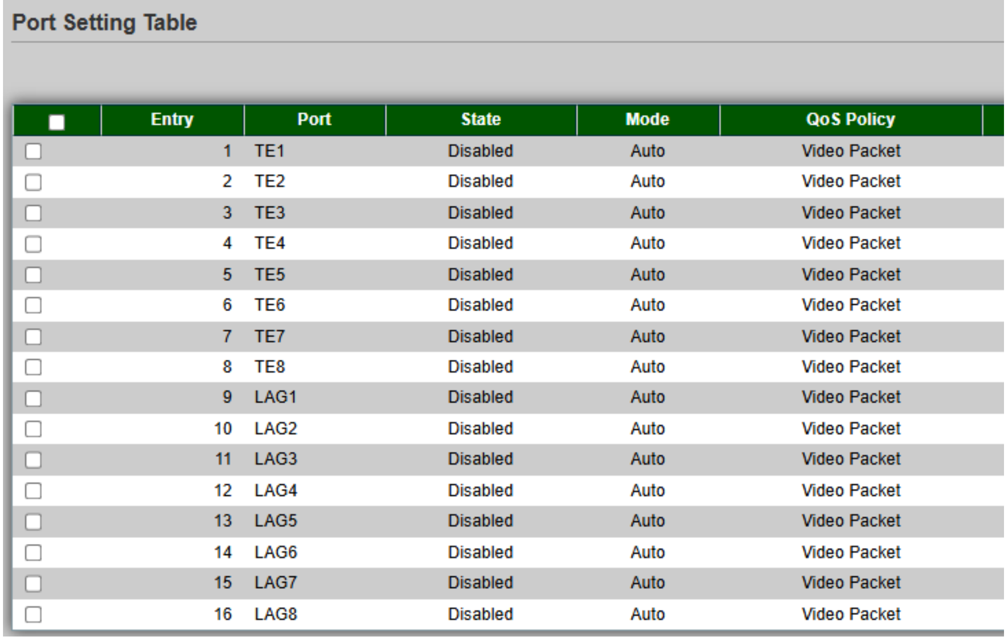
State	☑ Enable
VLAN	None
CoS / 802.1p Remarking	☑ Enable 6
Aging Time	1440 Min (30 - 65536, default 1440)

Port Setting Table

□	Entry	Port	State	Mode	QoS Policy
□	1	TE1	Disabled	Auto	Video Packet
□	2	TE2	Disabled	Auto	Video Packet
□	3	TE3	Disabled	Auto	Video Packet

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

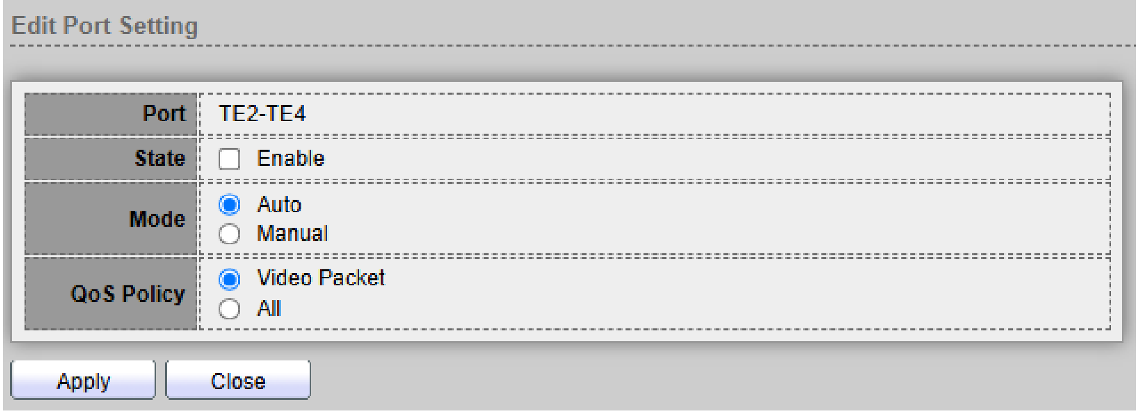
*Click the **"Apply"** button to save your changes settings.*



Port Setting Table

■	Entry	Port	State	Mode	QoS Policy
☐	1	TE1	Disabled	Auto	Video Packet
☐	2	TE2	Disabled	Auto	Video Packet
☐	3	TE3	Disabled	Auto	Video Packet
☐	4	TE4	Disabled	Auto	Video Packet
☐	5	TE5	Disabled	Auto	Video Packet
☐	6	TE6	Disabled	Auto	Video Packet
☐	7	TE7	Disabled	Auto	Video Packet
☐	8	TE8	Disabled	Auto	Video Packet
☐	9	LAG1	Disabled	Auto	Video Packet
☐	10	LAG2	Disabled	Auto	Video Packet
☐	11	LAG3	Disabled	Auto	Video Packet
☐	12	LAG4	Disabled	Auto	Video Packet
☐	13	LAG5	Disabled	Auto	Video Packet
☐	14	LAG6	Disabled	Auto	Video Packet
☐	15	LAG7	Disabled	Auto	Video Packet
☐	16	LAG8	Disabled	Auto	Video Packet

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



Edit Port Setting

Port	TE2-TE4
State	☐ Enable
Mode	● Auto ○ Manual
QoS Policy	● Video Packet ○ All

- **Port :** Display selected port to be edited.
- **State :** Set checkbox to enable/disabled Surveillance VLAN function of interface.
- **Mode :** Select port Surveillance VLAN mode.

- **Auto :** Video VLAN auto detect packets that match OUI table and add received port into surveillance VLAN ID tagged member.
- **Manual :** User need add interface to VLAN ID tagged member manually.

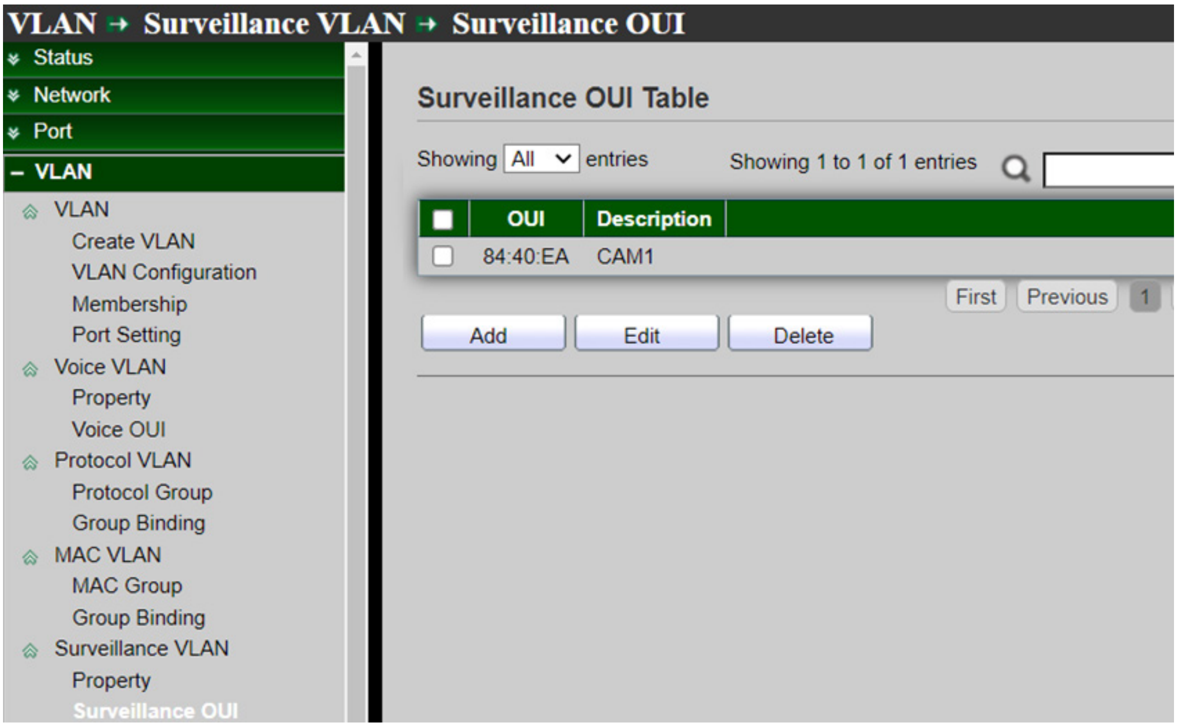
➢ **QoS Policy :** Select port QoS Policy mode.

- **Video Packet :** 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 Surveillance VLAN.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

6.5.2 Surveillance OUI

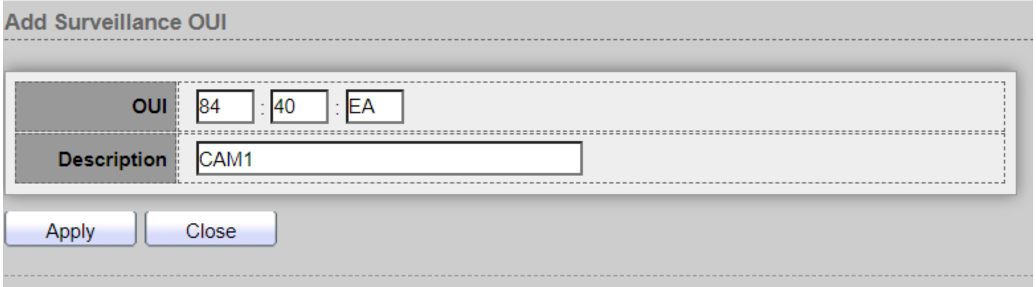
Administrator can configure this page to add, edit or delete OUI MAC addresses, Setting **"add"** and "Edit" and **"Delete"** function for this management.



□	OUI	Description
□	84:40:EA	CAM1

Field	Description
OUI	Display OUI MAC address.

Description	Display description of OUI entry.



Add Surveillance OUI

OUI	84 : 40 : EA
Description	CAM1

- **OUI :** Input OUI MAC address. Can't be edited in edit dialog.   .
- **Description :** Input description of the specified MAC address to the Surveillance VLAN OUI table.

  *Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

6.6 GVRP

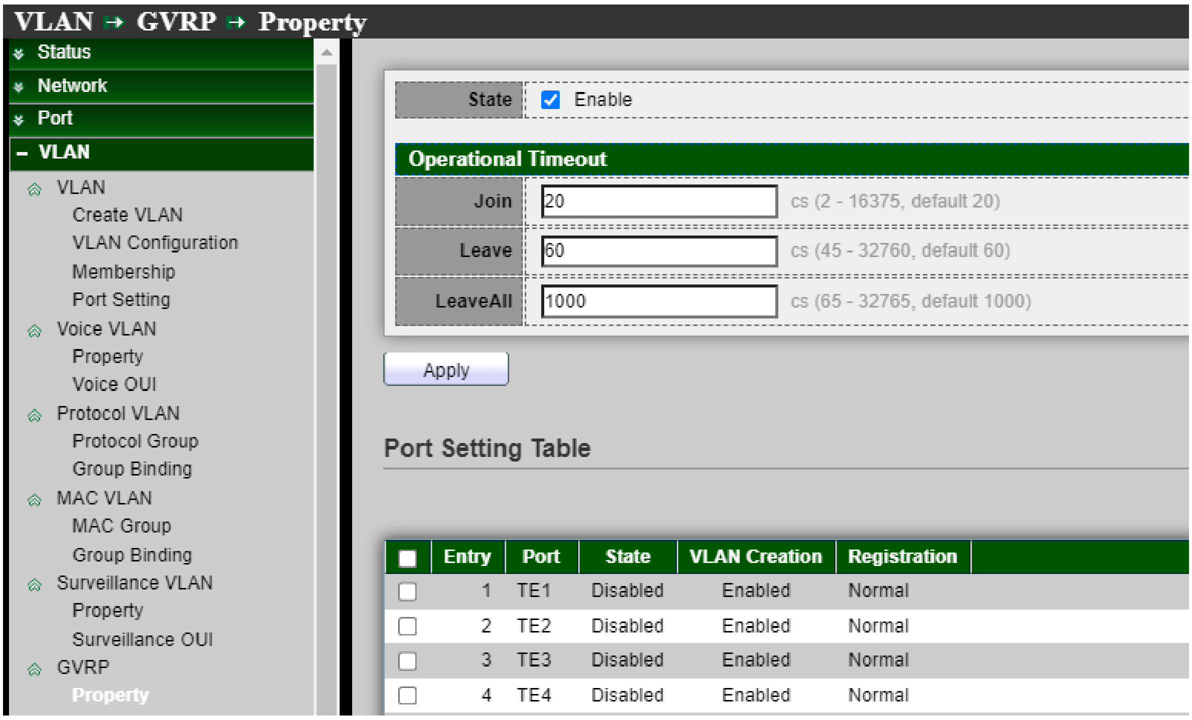
The GVRP (Generic VLAN Registration Protocol) is described in the IEEE 802.1p standard; It's an IEEE 802.1Q-compliant method for facilitating automatic (dynamic) VLAN membership configuration. GVRP-enabled switches can exchange VLAN configuration information with other GVRP-enabled switches.

Policy rules or other network management methods can determine who is admitted to a VLAN. When a node requests admission to a specific VLAN, GVRP handles the registration of the node with GVRP-enabled switches and maintains that information.

GVRP reduces the chance of errors in VLAN configuration by automatically providing VLAN ID (VID) consistency across the network. In addition, you can use GVRP to dynamically enable port membership in static VLANs configured on a switch. Once GVRP creates a dynamic VLAN will can also reduce unnecessary broadcast traffic and unicast traffic.

6.6.1 Property

Administrator can enable GVRP function and set every port registration on GVRP.



VLAN → GVRP → Property

State ☑ Enable

Operational Timeout

Join	20	cs (2 - 16375, default 20)
Leave	60	cs (45 - 32760, default 60)
LeaveAll	1000	cs (65 - 32765, default 1000)

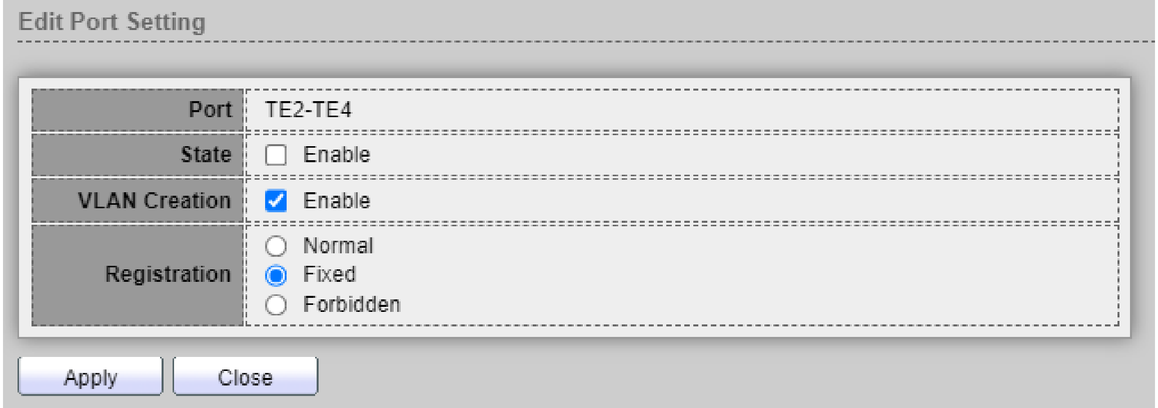
Port Setting Table

□	Entry	Port	State	VLAN Creation	Registration
□	1	TE1	Disabled	Enabled	Normal
□	2	TE2	Disabled	Enabled	Normal
□	3	TE3	Disabled	Enabled	Normal
□	4	TE4	Disabled	Enabled	Normal

- **State :** Set the enabling status of GVRP functionality
  - **Enable:** if Checked Enable GVRP, else is Disable GVRP.
- **Operational Timeout:** The port will not learn any dynamic VLAN. Only send static VLAN information to
  - **Join.:** GVRP Join time out.
  - **Leave:** GVRP leave time out.

*Click the **"Apply"** button to save your changes settings.*

Field	Description
Port	Port Name.
State	Display port GVRP state.
VLAN Creation	Display port GVRP creation VLAN state.
Registration	Display port GVRP registration mode.



Edit Port Setting

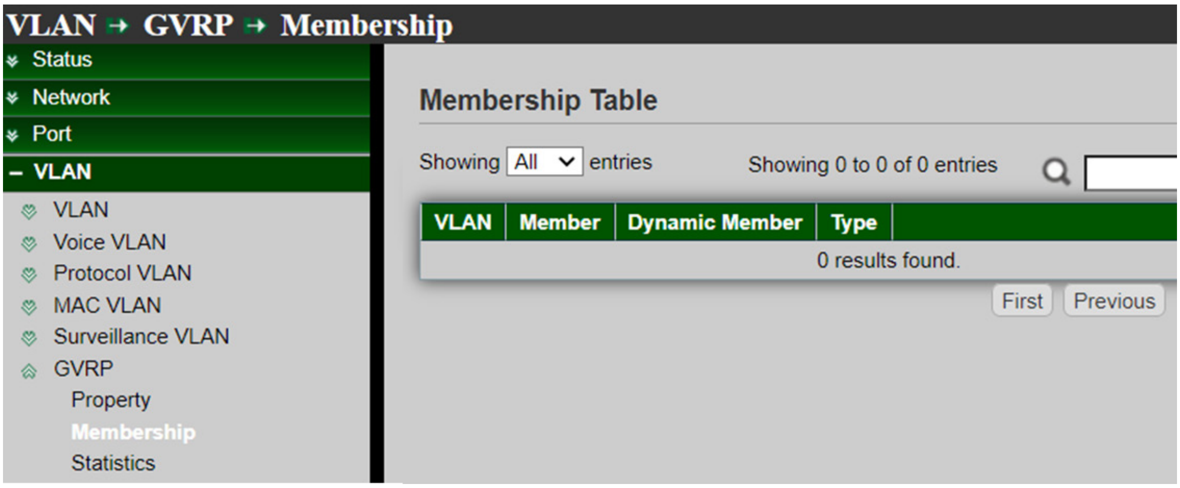
Port	TE2-TE4
State	□ Enable
VLAN Creation	☑ Enable
Registration	○ Normal ● Fixed ○ Forbidden

- **Port:** Display port number.
- **State:** Displays whether GVRP is enabled or disabled on the interface.
- **VLAN Creation:** Displays whether Dynamic VLAN creation is enabled or disabled on the interface. If it is disabled, GVRP can operate but new VLANs are not created.
- **Registration:** Displays the VLAN registration mode on the interface.
  - **Normal: Normal mode.**.
  - **Fixed:** The port will not learn any dynamic VLAN. Only send static VLAN information to neighbor and allow static VLAN packet pass..
  - **Forbidden:** The port will not learn any dynamic VLAN and only allow default VLAN packet pass.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

6.6.2 Member ship

When enable GVRP function and state ports in GVRP then administrator can check GVRP member information.



Membership Table

Showing All entries

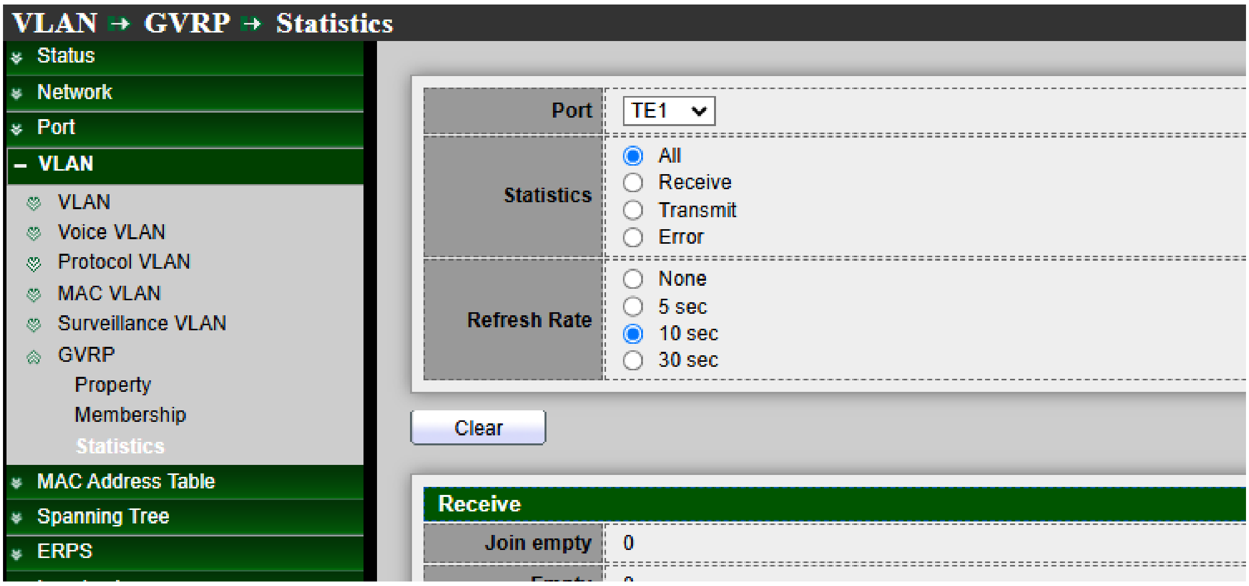
Showing 0 to 0 of 0 entries

VLAN	Member	Dynamic Member	Type
0 results found.			

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

6.6.3 Statistics

When enable and set GVRP function then administrator can check every port in GVRP include Receive / Transmit and Error information.



Port: TE1

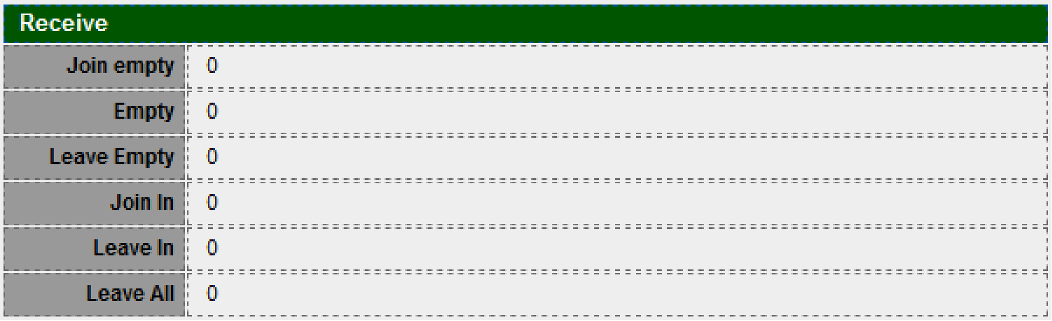
Statistics: ● All ○ Receive ○ Transmit ○ Error

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

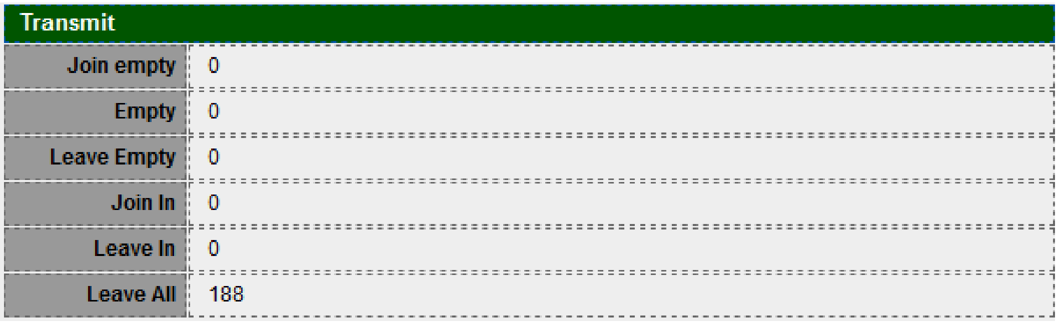
Receive

Join empty	0
Empty	0

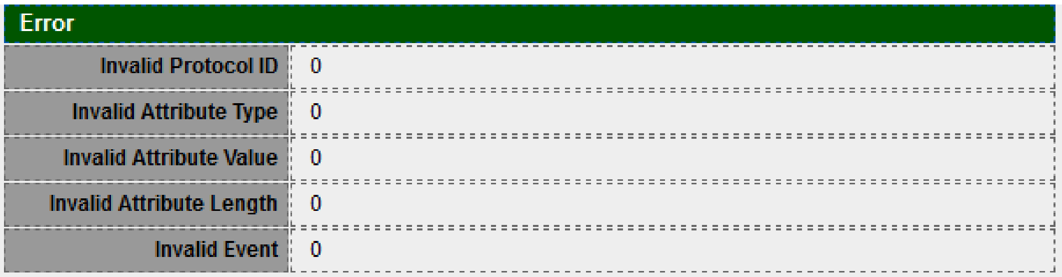
Click the ***"Clear"*** *button to clear this page.*



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	188



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

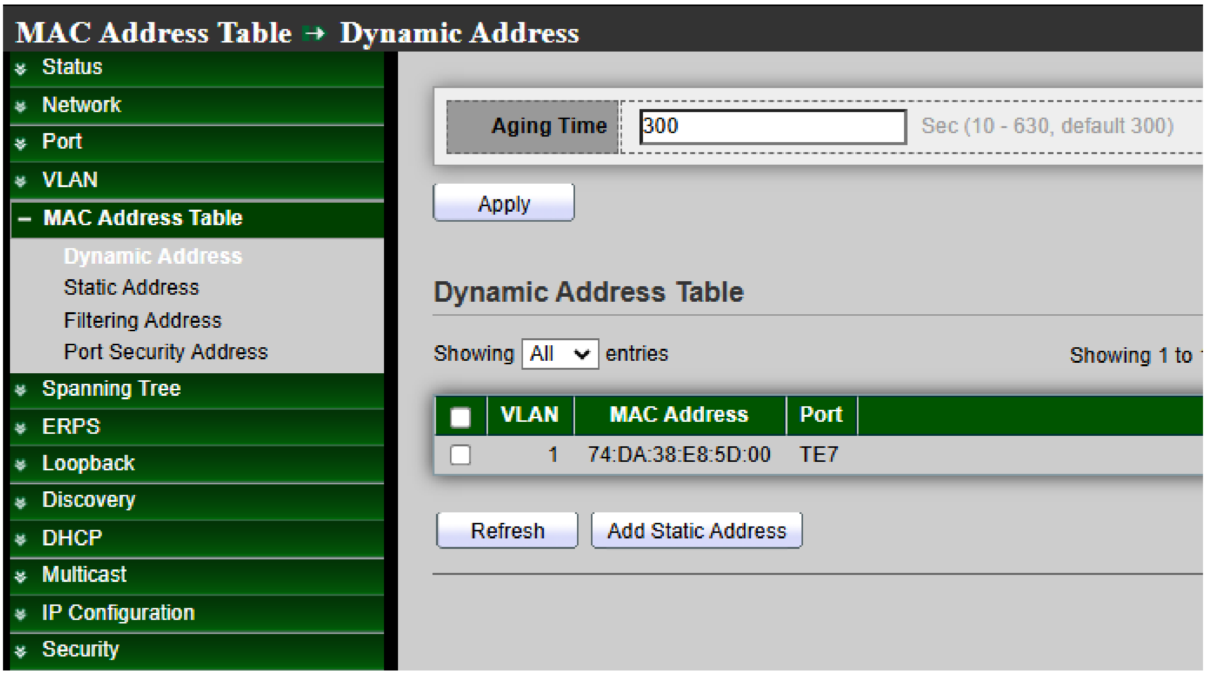
Field	Description
Join empty	The number of Receive or Transmit Join empty attribute value.
Empty	The number of Receive or Transmit Empty attribute value.
Leave Empty	The number of Receive or Transmit Leave Empty attribute value.
Join In	The number of Receive or Transmit Join In attribute value.
Leave In	The number of Receive or Transmit Leave In empty attribute value.
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.

7. MAC Address Table

7.1 Dynamic Address

This page can display MAC address for connected device. Administrator can set aging time for connected port.


MAC Address Table → Dynamic Address

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

Dynamic Address Table

Showing All entries   Showing 1 to

□	VLAN	MAC Address	Port
□	1	74:DA:38:E8:5D:00	TE7

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

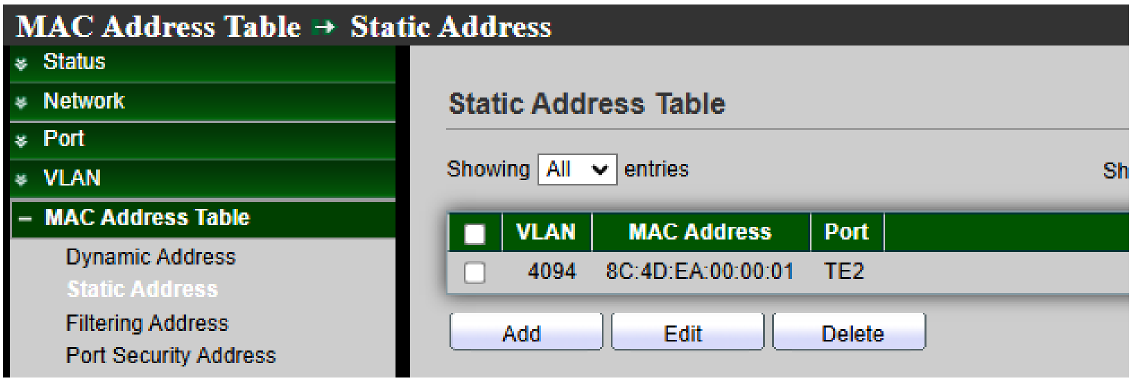
*Click the **“Apply”** button to save your changes settings.*

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

When administrator select checkbox MACs address and click "**Add Static Address**" button then selected MAC address will move to "**Static Address**" function.

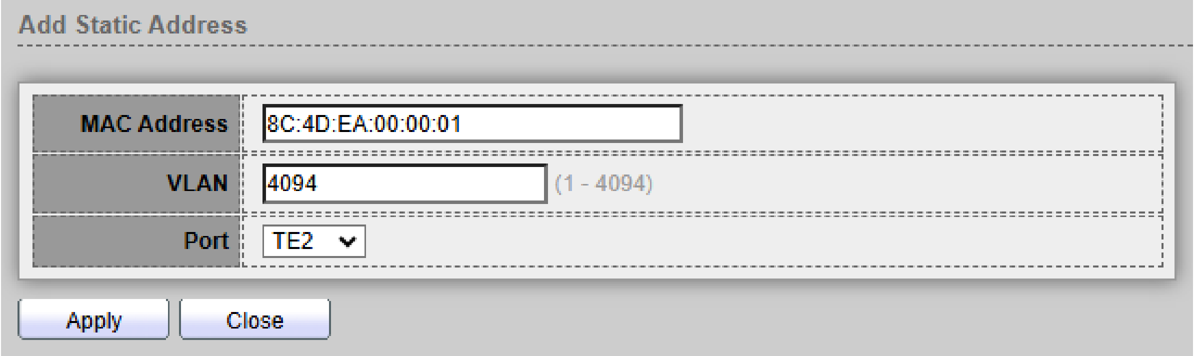
7.2 Static Address

If administrator fixed an MAC address in the port then device MAC address will bind in the port, if device connection other port will can't working only connection bind port, Setting **"add"** and "Edit" and **"Delete"** function for this management.



□	VLAN	MAC Address	Port
□	4094	8C:4D:EA:00:00:01	TE2

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



Add Static Address

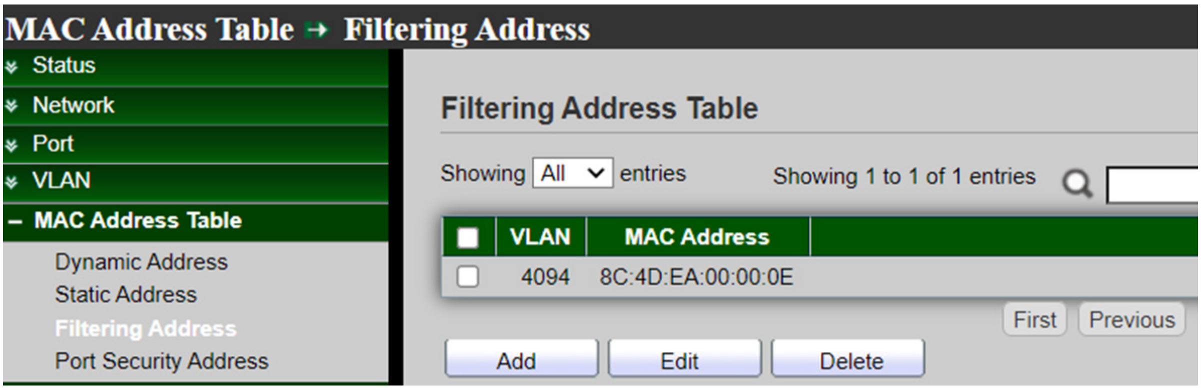
MAC Address	8C:4D:EA:00:00:01
VLAN	4094 (1 - 4094)
Port	TE2

- **MAC Address :** Enter the MAC address to which packets will be statically forwarded.
- **VLAN :** Enter the Specify the VLAN ID
- **Port :** Select an interface or port number.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

7.3 Filtering Address

Administrator can set need filtering MAC address in the MAC table. If MAC is added on table this MAC will be blocked, Setting **"add"** and "Edit" and **"Delete"** function for this management.



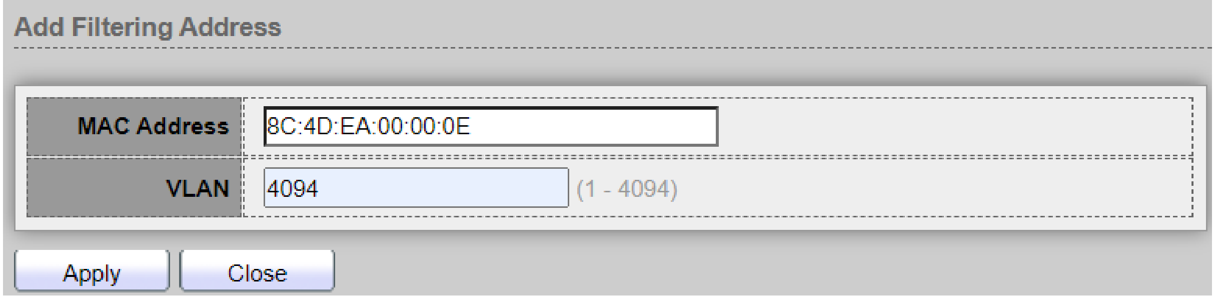
MAC Address Table → Filtering Address

Filtering Address Table

Showing All entries   Showing 1 to 1 of 1 entries

□	VLAN	MAC Address
□	4094	8C:4D:EA:00:00:0E

Field	Description
MAC Address	Specify unicast MAC address in the packets to be dropped.
VLAN	Specify the VLAN ID for the specific MAC address.



Add Filtering Address

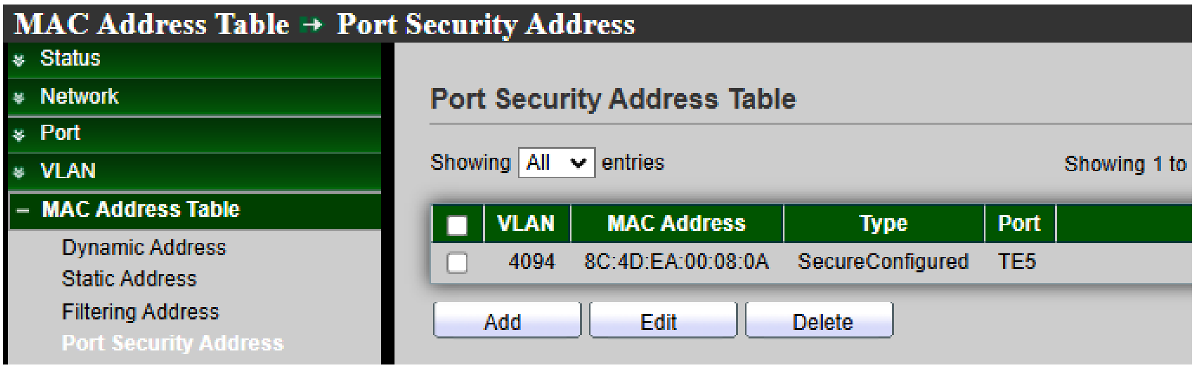
MAC Address	8C:4D:EA:00:00:0E
VLAN	4094 (1 - 4094)

- **MAC Address :** Enter to specify the unicast MAC address in the packets to be dropped.
- **VLAN :** Enter a VLAN ID that specifies a specific MAC address.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

7.4 Port Security Address

Administrator can set this Port Security Address function, Setting **"add"** and "Edit" and **"Delete"** function for this management.



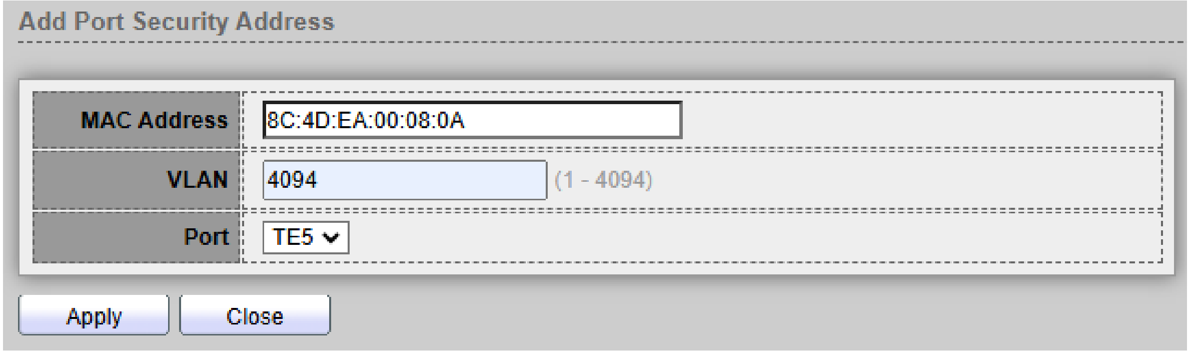
MAC Address Table → Port Security Address

Port Security Address Table

Showing All entries Showing 1 to

□	VLAN	MAC Address	Type	Port
□	4094	8C:4D:EA:00:08:0A	SecureConfigured	TE5

Field	Description
VLAN	Specify the VLAN to show port security.
MAC Address	Specify the MAC address for port security.
Type	Specify the Type for port security.
Port	Interface or port number.



Add Port Security Address

MAC Address	8C:4D:EA:00:08:0A
VLAN	4094 (1 - 4094)
Port	TE5

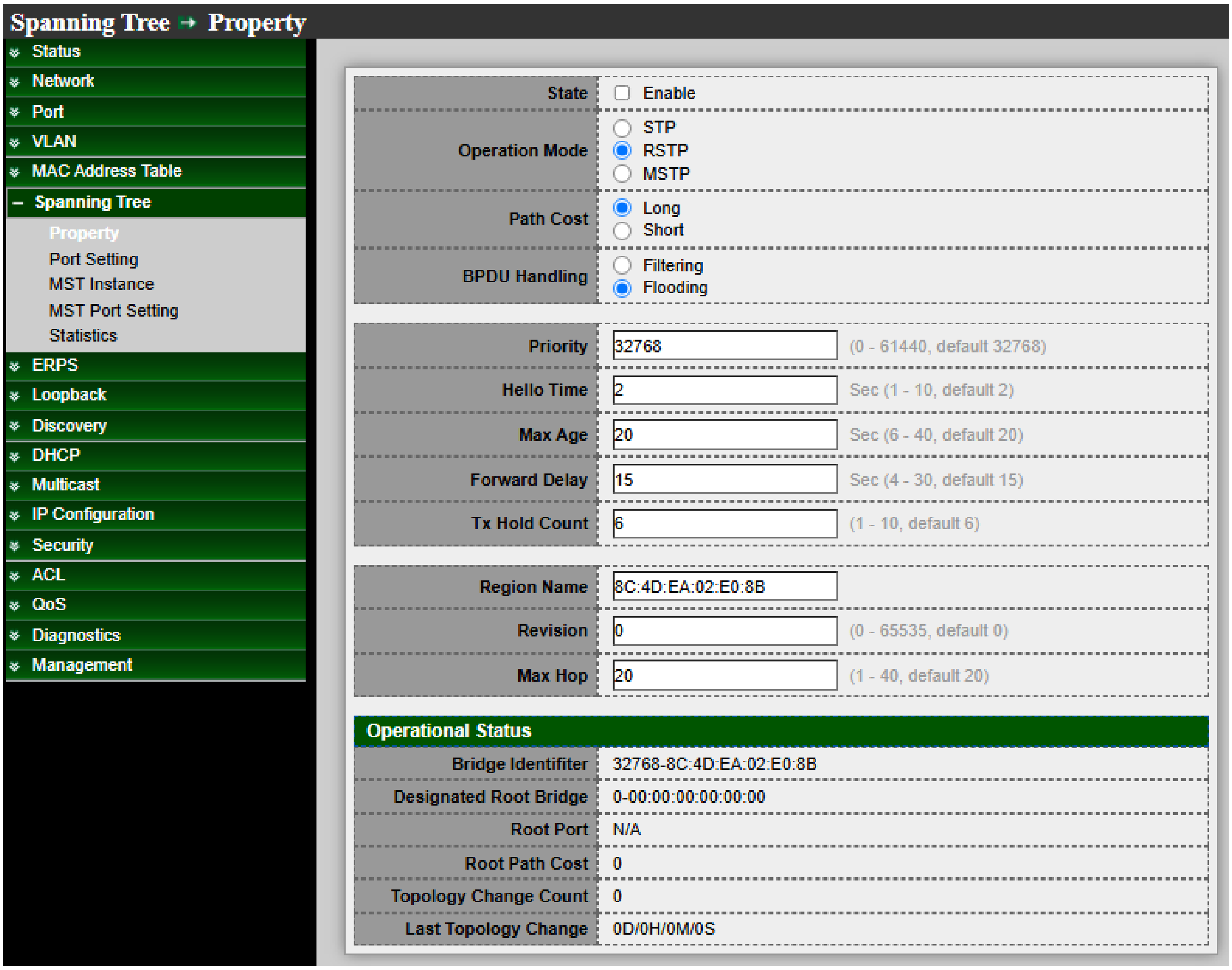
- **MAC Address :** Enter the MAC address for port security.
- **VLAN :** Enter the Specify the VLAN ID
- **Port :** Select an interface or port number.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

8. Spanning Tree

Spanning Tree function allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail. If Spanning Tree costs change, or if one network segment in the Spanning Tree becomes unreachable, the spanning tree algorithm reconfigures the spanning tree topology and reestablishes the link by activating the standby path. Without spanning tree in place, it is possible that both connections may be simultaneously live, which could result in an endless loop of traffic on the LAN.

8.1 Property



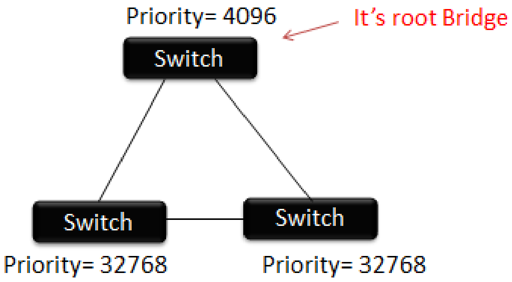
State	□ Enable
Operation Mode	○ STP ● RSTP ○ MSTP
Path Cost	● Long ○ Short
BPDU Handling	○ Filtering ● Flooding
Priority	32768 (0 - 61440, default 32768)
Hello Time	2 Sec (1 - 10, default 2)
Max Age	20 Sec (6 - 40, default 20)
Forward Delay	15 Sec (4 - 30, default 15)
Tx Hold Count	6 (1 - 10, default 6)
Region Name	8C:4D:EA:02:E0:8B
Revision	0 (0 - 65535, default 0)
Max Hop	20 (1 - 40, default 20)

Operational Status

Bridge Identifier	32768-8C:4D:EA:02:E0:8B
Designated Root Bridge	0-00:00:00:00:00:00
Root Port	N/A
Root Path Cost	0
Topology Change Count	0
Last Topology Change	0D/0H/0M/0S

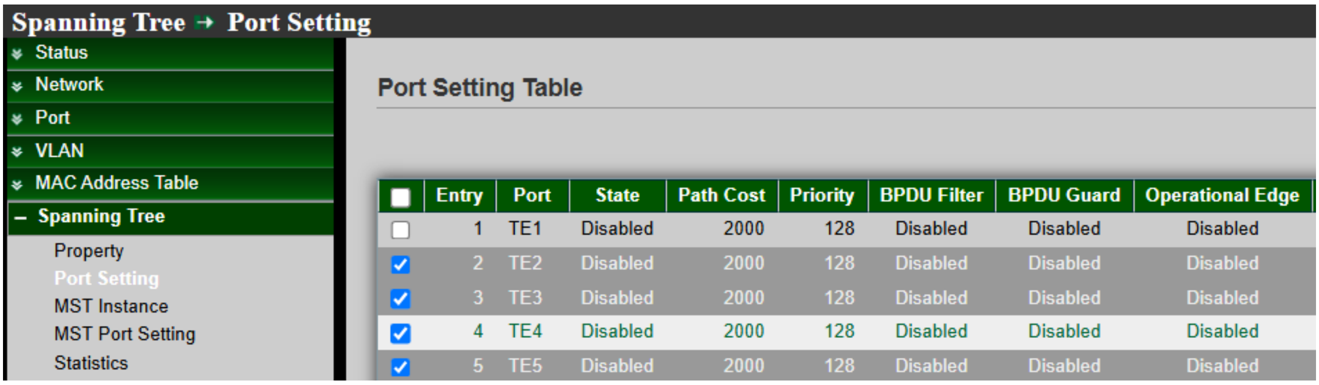
- **State:** Administrator can choose Enable or Disable this function.
- **Operation Mode:** Administrator can choose use Spanning Tree (STP) or Rapid Spanning Tree (RSTP) or Multiple Spanning Tree (MSTP).
- **Path Cost:** Administrator can choose STP judgment use Path cost for Long or Short.
  - **Long :** 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:** When the Switch receives the BPDU frame, Administrator can choose the BPDU Handling mode for Filtering or Flooding. 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:** Administrator can set bridge priority, default is 32768. The lower value (priority) is the

root bridge. Specify the bridge priority. The valid range is from 0 to 61440, and the value should be the multiple of 4096. It ensures the probability that the switch is selected as the root bridge, and the lower value has the higher priority for the switch to be selected as the root bridge of the topology.



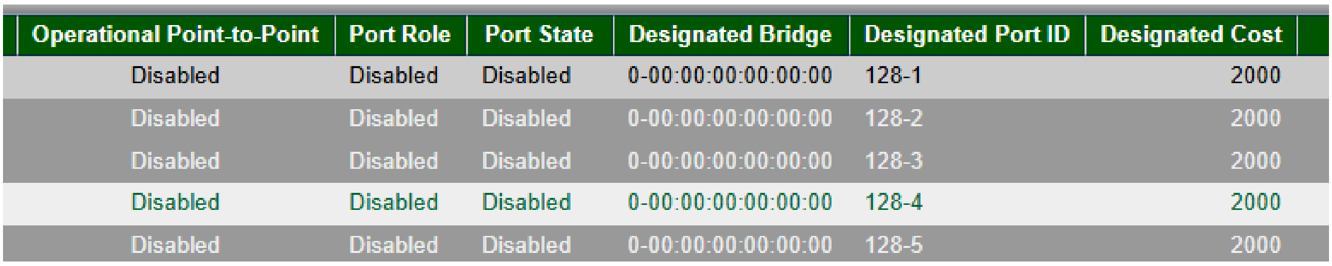
- **Hello Time:** The hello time is the time between each bridge protocol data unit (BPDU) that is sent on a port. This time is equal to 2 seconds (sec) by default, but you can tune the time to be between 1 and 10 sec.
- **Max. Age / Forward delay :** *2*(Forward Delay-1) >= **Max Age** >= 2*(Hello Time+1),* the time interval in seconds for a switch to wait the configuration messages, without attempting to redefine its own configuration.
- **Forward Delay :** Specify the STP forward delay time, which is the amount of time that a port remains in the Listening and Learning states before it enters the Forwarding state. Its valid range is from 4 to 10 seconds.
- **TX hold Count:** Specify the tx-hold-count used to limit the maximum numbers of packets transmission per second. The valid range is from 1 to 10.
- **Region Name:** The MSTP instance name. Its maximum length is 32 characters. The default value is the MAC address of the switch.
- **Revision:** Administrator every time change MST value, customary "Revision" to add 1 value. The MSTP revision number. Its valid rage is from 0 to 65535.
- **Max. Hop:** Set max. hop of switch. Specify the number of hops in an MSTP region before the BPDU is discarded. The valid range is 1 to 40.

8.2 Port Setting



Port Setting Table

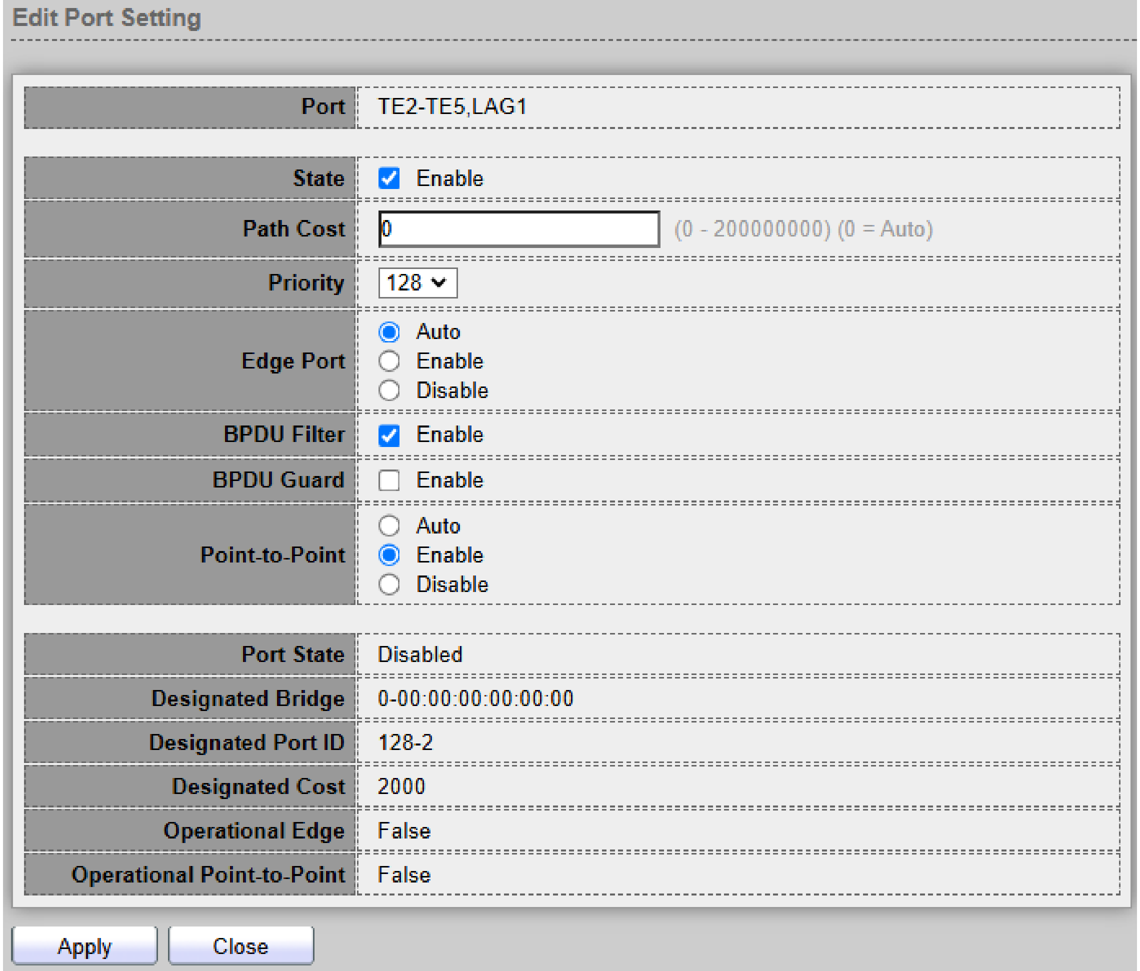
□	Entry	Port	State	Path Cost	Priority	BPDU Filter	BPDU Guard	Operational Edge
□	1	TE1	Disabled	2000	128	Disabled	Disabled	Disabled
☑	2	TE2	Disabled	2000	128	Disabled	Disabled	Disabled
☑	3	TE3	Disabled	2000	128	Disabled	Disabled	Disabled
☑	4	TE4	Disabled	2000	128	Disabled	Disabled	Disabled
☑	5	TE5	Disabled	2000	128	Disabled	Disabled	Disabled



Operational Point-to-Point	Port Role	Port State	Designated Bridge	Designated Port ID	Designated Cost
Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-1	2000
Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-2	2000
Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-3	2000
Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-4	2000
Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-5	2000

Field	Description
Port	Specify the interface ID or the list of interface IDs.
State	The operational state on the specified port.
Path Cost	STP path cost on the specified port.
Priority	STP priority on the specified port.
BPDU Filter	The states of BPDU filter on the specified port.
BPDU Guard	The states of 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. The possible values are: “Disabled”, “Master”, “Root”, “Designated”, “Alternative”, and Backup”.
Port State	The current port state on the specified port. The possible values are: “Disabled”, “Discarding”, “Learning”, and “Forwarding”.

Designated Bridge	The bridge ID of the designated bridge.
Designated Port ID	The designated port ID on the switch.
Designated Cost	The path cost of the designated port on the switch



Edit Port Setting

Port	TE2-TE5,LAG1
State	☑ Enable
Path Cost	0 (0 - 200000000) (0 = Auto)
Priority	128
Edge Port	● Auto ○ Enable ○ Disable
BPDU Filter	☑ Enable
BPDU Guard	□ Enable
Point-to-Point	○ Auto ● Enable ○ Disable
Port State	Disabled
Designated Bridge	0-00:00:00:00:00:00
Designated Port ID	128-2
Designated Cost	2000
Operational Edge	False
Operational Point-to-Point	False

- **State:** Administrator can set Enable or Disable.
- **Path Cost:** Path Cost (1-200000000) This parameter is used determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short, the maximum path cost is 65,535. Range: 1-200000000, (set 0 = Auto, default is 0).
- **Priority:** If the path cost for all ports on a switch is the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

Range: 0-240, default is 128.

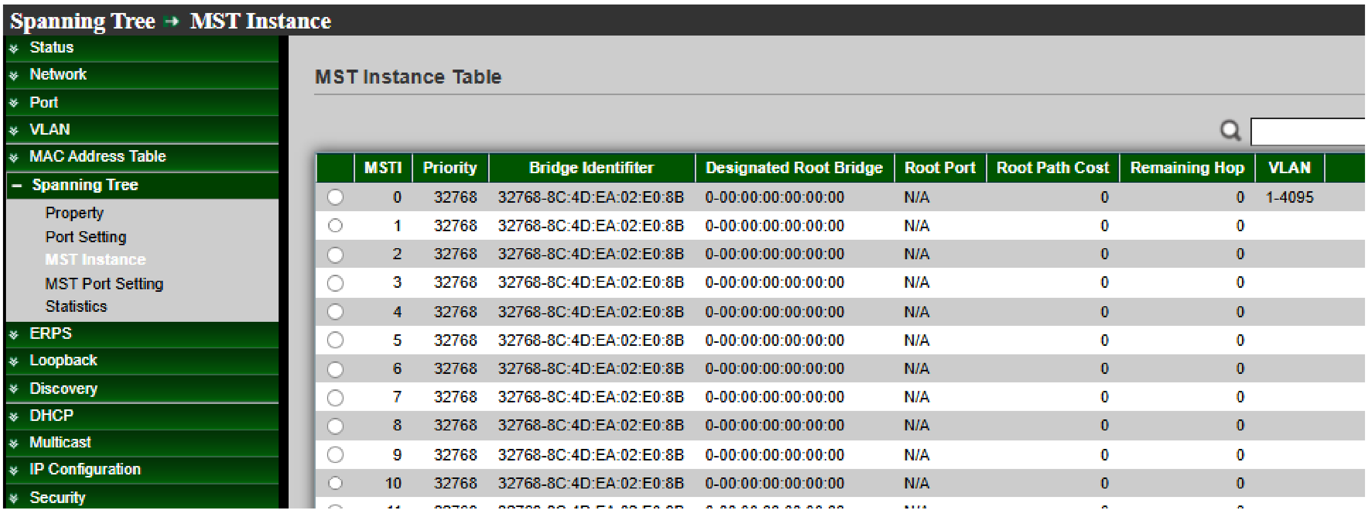
- **Edge Port:** Specify the edge mode..
  - **Enable :** Force to true state (as link to a host).
  - **Disable :** Force to false state (as link to a bridge).

  In the edge mode, the interface would be put into the Forwarding state immediately upon link up. If the edge mode is enabled for the interface and there are BPDUs received on the interface, the loop might be occurred in the short time before the STP state change.
- **BPDU Filter :** The BPDU Filter configuration avoids receiving/transmitting BPDU from the specified ports.
  - **Enable :** Enable BPDU filter function.
  - **Disable :** Disable BPDU filter function.
- **BPDU Filter :** 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 :** The state is depended on the duplex setting of the port.
  - **Enable :** Force to true state.
  - **Disable:** Force to false state.
- **Port State :** The current port state on the specified port. The possible values are : “Disabled”, “Discarding”, “Learning”, and “Forwarding”.
- **Designated Bridge :** The bridge ID of the designated bridge.
- **Designated Port ID :** The designated port ID on the switch.
- **Designated Cost :** The path cost of the designated port on the switch.
- **Operational Edge :** Show the “false” and “true” status.
- **Operational Point-to-Point :** Show the “false” and “true” status.

*Click the **“Apply”** button to save your changes or **“Close”** the button to close settings.*

8.3 MST Instance

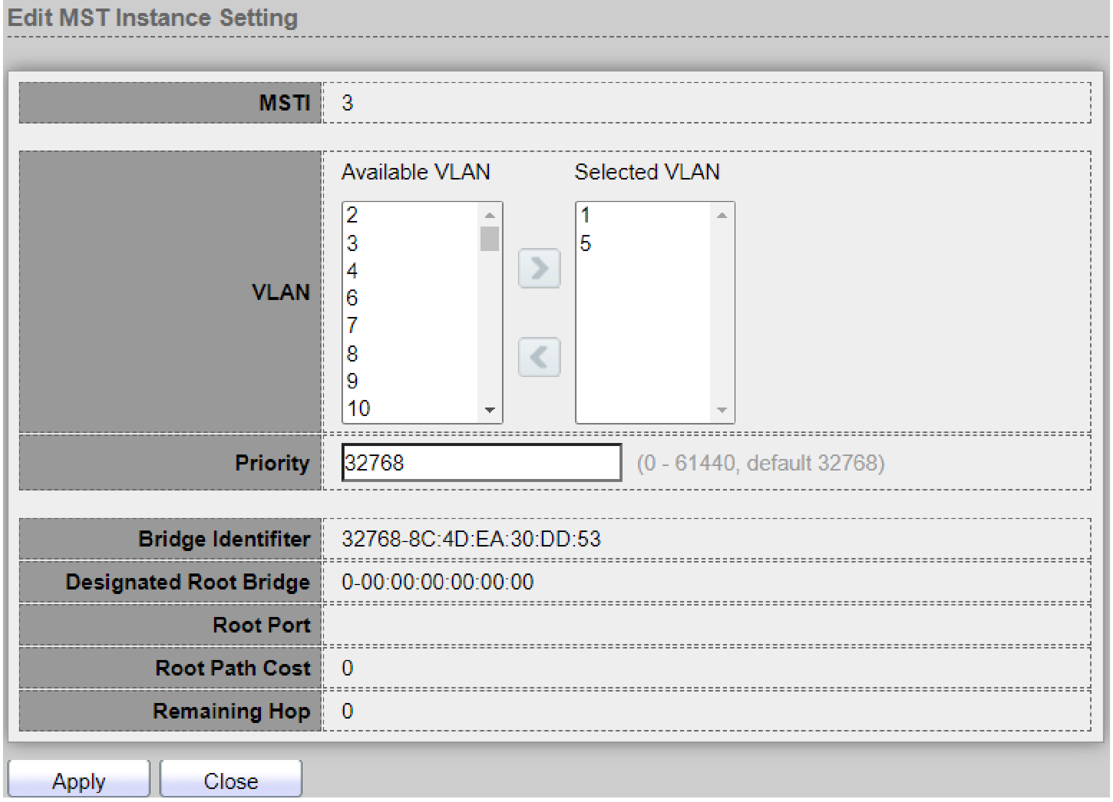
MST can have multiple sets of STP instances. Each instance is independently formed as a logical spanning tree. And instance has its own VLAN and port state, can independently set the priority of each port.



MST Instance Table

	MSTI	Priority	Bridge Identifier	Designated Root Bridge	Root Port	Root Path Cost	Remaining Hop	VLAN
○	0	32768	32768-8C:4D:EA:02:E0:8B	0-00:00:00:00:00:00	N/A	0	0	1-4095
○	1	32768	32768-8C:4D:EA:02:E0:8B	0-00:00:00:00:00:00	N/A	0	0	
○	2	32768	32768-8C:4D:EA:02:E0:8B	0-00:00:00:00:00:00	N/A	0	0	
○	3	32768	32768-8C:4D:EA:02:E0:8B	0-00:00:00:00:00:00	N/A	0	0	
○	4	32768	32768-8C:4D:EA:02:E0:8B	0-00:00:00:00:00:00	N/A	0	0	
○	5	32768	32768-8C:4D:EA:02:E0:8B	0-00:00:00:00:00:00	N/A	0	0	
○	6	32768	32768-8C:4D:EA:02:E0:8B	0-00:00:00:00:00:00	N/A	0	0	
○	7	32768	32768-8C:4D:EA:02:E0:8B	0-00:00:00:00:00:00	N/A	0	0	
○	8	32768	32768-8C:4D:EA:02:E0:8B	0-00:00:00:00:00:00	N/A	0	0	
○	9	32768	32768-8C:4D:EA:02:E0:8B	0-00:00:00:00:00:00	N/A	0	0	
○	10	32768	32768-8C:4D:EA:02:E0:8B	0-00:00:00:00:00:00	N/A	0	0	

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 configuration of remaining hop on the specified MSTI.
VLAN	The VLAN configuration on the specified MSTI.



Edit MST Instance Setting

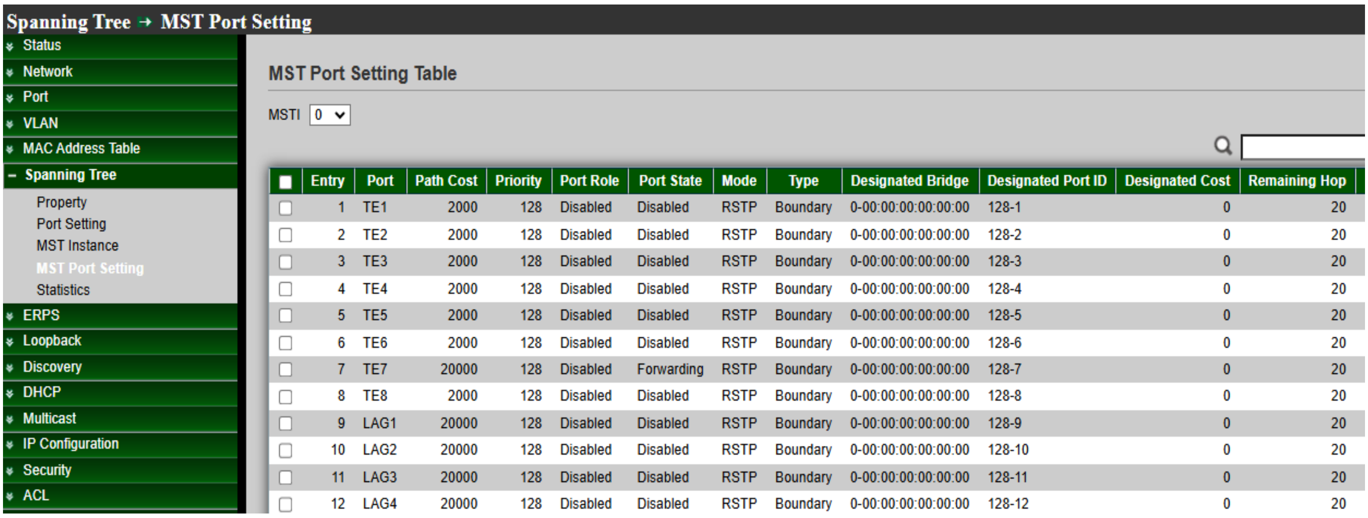
MSTI	3
VLAN	Available VLAN: 2, 3, 4, 6, 7, 8, 9, 10 Selected VLAN: 1, 5
Priority	32768 (0 - 61440, default 32768)
Bridge Identifiter	32768-8C:4D:EA:30:DD:53
Designated Root Bridge	0-00:00:00:00:00:00
Root Port	
Root Path Cost	0
Remaining Hop	0

- **VLAN :** Select the VLAN list for the specified MSTI.
- **Priority:** Specify the bridge priority on the specified MSTI. The valid range is from 0 to 61440, and the value must be the multiple of 4096. It ensures the probability that the switch is selected as the root bridge, and the lower values has the higher priority for the switch to be selected as the root bridge of the STP topology.
- **Bridge Identifier:** Displays the priority and MAC address of the Root Bridge for the selected MST instance.
- **Root Port:** Displays the root port of the selected MST instance.
- **Root Path Cost:** Displays the root path cost of the selected MST instance.
- **Remaining Hops:** Displays the number of hops remaining to the next destination.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

8.4 MST Port Setting

MST (Multiple Spanning Tree) is an extension to RST (Rapid Spanning Tree). MST further develops the usefulness of VLANs. MST configures a separate spanning tree for each VLAN group and blocks all but one possible alternate path within each spanning tree. A Multiple Spanning Tree Instance (MSTI) calculates and builds a loop-free topology to bridge packets from the VLANs that map to the instance.



MST Port Setting Table

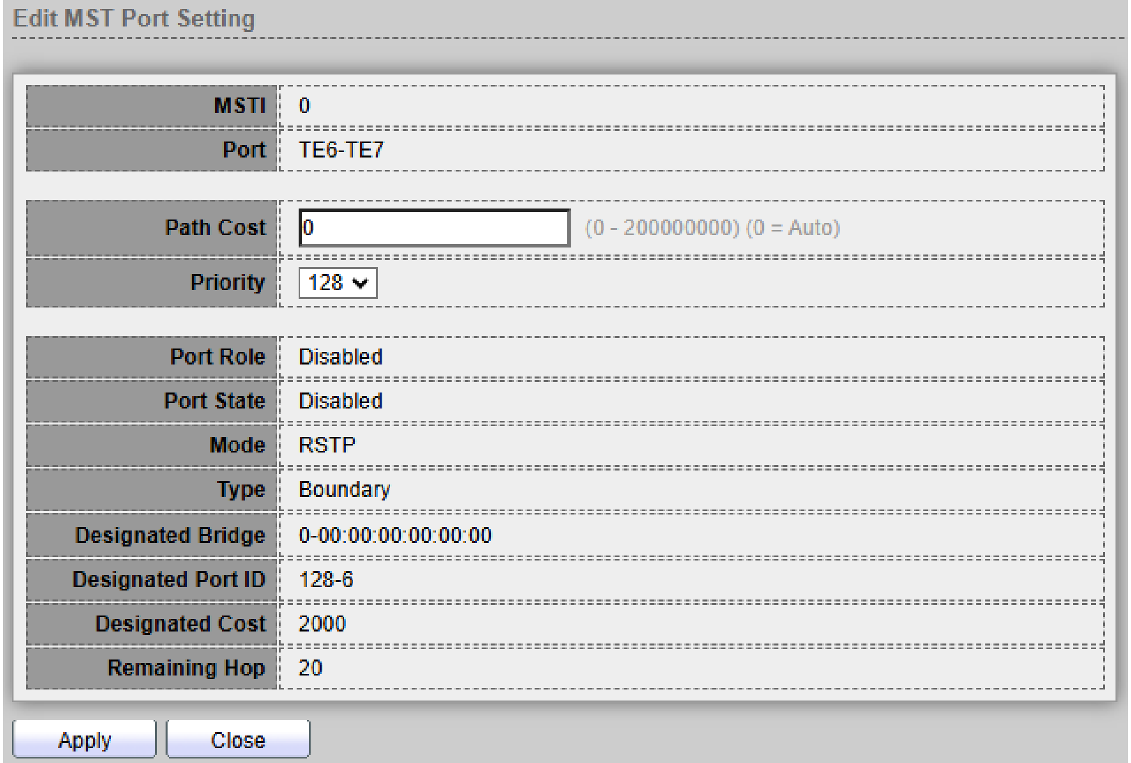
MSTI 0

□	Entry	Port	Path Cost	Priority	Port Role	Port State	Mode	Type	Designated Bridge	Designated Port ID	Designated Cost	Remaining Hop
□	1	TE1	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-1	0	20
□	2	TE2	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-2	0	20
□	3	TE3	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-3	0	20
□	4	TE4	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-4	0	20
□	5	TE5	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-5	0	20
□	6	TE6	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-6	0	20
□	7	TE7	20000	128	Disabled	Forwarding	RSTP	Boundary	0-00:00:00:00:00:00	128-7	0	20
□	8	TE8	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-8	0	20
□	9	LAG1	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-9	0	20
□	10	LAG2	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-10	0	20
□	11	LAG3	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-11	0	20
□	12	LAG4	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-12	0	20

MST Port Settings is used to configure the port MSTP settings for every MST instance. It is also used to view statistics that have been learned from the protocol.

Field	Description
MSTI	Specify the port setting on the specified MSTI
Port	Specify the interface ID or the list of interface IDs.
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. The possible values are: “Disabled”, “Master”, “Root”, “Designated”, “Alternative”, and “Backup”.
Port State	The current port state on the specified port. The possible values are: “Disabled”, “Discarding”, “Learning”, and “Forwarding”.
Mode	The operational STP mode on the specified port.
Type	The possible value for the port type are: • **Boundary**: The port 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 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.
Remaining Hop	The remaining hops count on the specified port.



Edit MST Port Setting

MSTI	0
Port	TE6-TE7
Path Cost	0 (0 - 200000000) (0 = Auto)
Priority	128
Port Role	Disabled
Port State	Disabled
Mode	RSTP
Type	Boundary
Designated Bridge	0-00:00:00:00:00:00
Designated Port ID	128-6
Designated Cost	2000
Remaining Hop	20

- **MTSI :** Specify the port setting on the specified MSTI.
- **Port :** Specify the interface ID or the list of interface IDs..
- **Path Cost:** Specify the STP port path cost on the specified MSTI,Path cost default value is 0 (auto) depends on source device rate.

  If network is a loop occurs, the MST uses cost when selecting an interface to put in the forwarding state. Administrator can assign lower cost values to interfaces that you want selected first and higher cost values that you want selected last. If all interfaces have the same cost value, the MST puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.
- **Priority:** Specify the STP port priority on the specified MSTI,Administrator can configure the MTP priority and make it more likely that the switch will be chosen as the root switch.
- **Port Role:** Displays the port role per instance, assigned by the MSTP algorithm to provide STP paths. The current port role on the specified port. The possible values are :

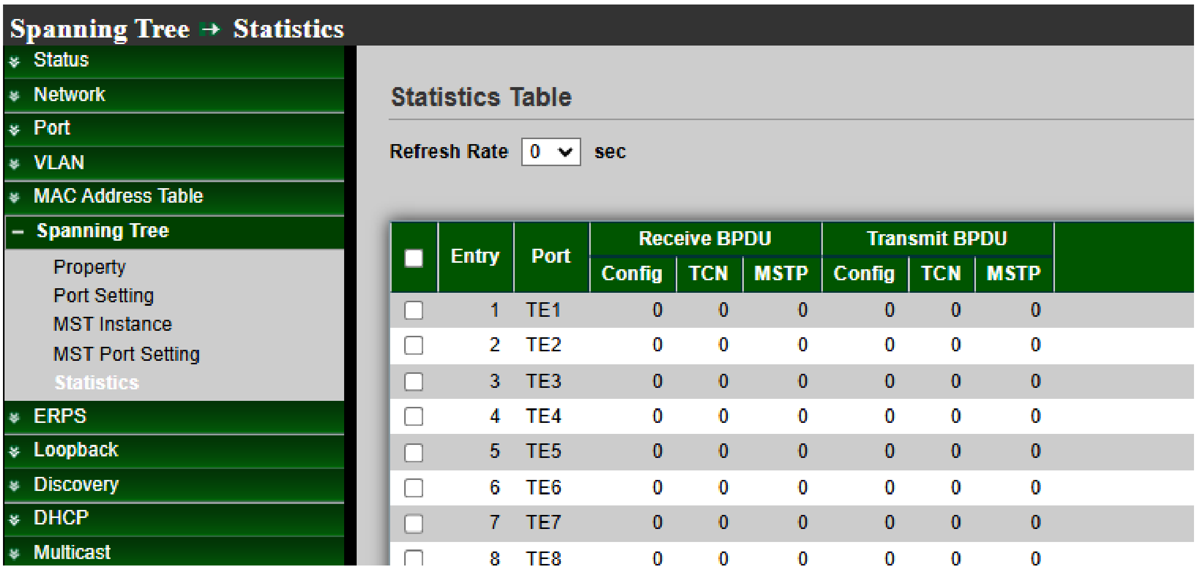
"Disabled", "Master", "Root", "Designated", "Alternative", and "Backup".

- ➢ **Port State:** The current port state on the specified port. The possible values are: **"Disabled", "Discarding", "Learning", and "Forwarding".**
- ➢ **Mode:** The operational STP mode on the specified port.
  - ● **RSTP:** RSTP is enabled on the port.
  - ● **STP:** Classic STP is enabled on the port.
  - ● **MSTP:** MSTP is enabled on the port.
- ➢ **Type :** Displays the MSTP type of the port. The possible value for the port type are :
  - ● **Boundary :** The port 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:** Displays the bridge ID number that connects the link or shared LAN to the root.
- ➢ **Designated Port ID:** Displays the priority and port ID on the designated bridge that connects the link or the shared LAN to the root.
- ➢ **Designated Cost:** Displays the cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
- ➢ **Remaining Hops :** Displays the hops remaining to the next destination.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

8.5 Statistics

This page can check Receive / Transmit BPDU information of the STP Port.

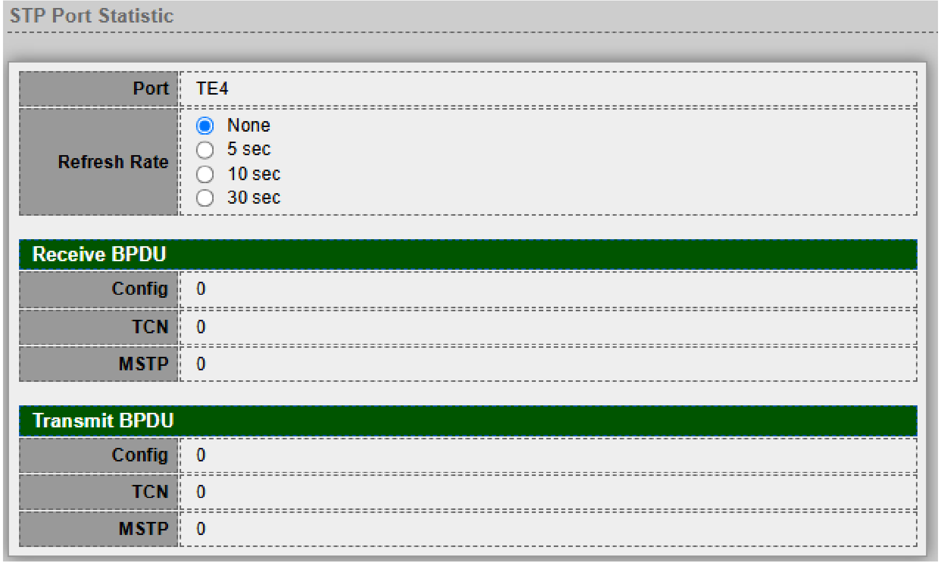


Statistics Table

Refresh Rate 0 sec

☐	Entry	Port	Receive BPDU			Transmit BPDU		
			Config	TCN	MSTP	Config	TCN	MSTP
☐	1	TE1	0	0	0	0	0	0
☐	2	TE2	0	0	0	0	0	0
☐	3	TE3	0	0	0	0	0	0
☐	4	TE4	0	0	0	0	0	0
☐	5	TE5	0	0	0	0	0	0
☐	6	TE6	0	0	0	0	0	0
☐	7	TE7	0	0	0	0	0	0
☐	8	TE8	0	0	0	0	0	0

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



STP Port Statistic

Port	TE4
Refresh Rate	● None ○ 5 sec ○ 10 sec ○ 30 sec
Receive BPDU	
Config	0
TCN	0
MSTP	0
Transmit BPDU	
Config	0
TCN	0
MSTP	0

- **Refresh Rate :** The option to refresh the statistics automatically : None , 5 sec , 10 sec , 30sec for refresh level.
- **Clear :** Clear the statistics for the selected interfaces.

9. ERPS

ERPS (Ethernet Ring Protection Switching) : In Ethernet switching networks such as ring networks, redundant links are generally used to provide link backup and enhance network reliability. However, using redundant links can create network loops, cause broadcast storms, and cause MAC address table instability. As a result, communication quality deteriorates, and even communication services are interrupted.

STP (Spanning Tree Protocol), RSTP (Rapid Spanning Tree Protocol), and MSTP (Multiple Spanning Tree Protocol) can also meet the reliability requirements of the network, but the convergence speed is slow and does not meet the industry standard requirements.

The first industrial standard Ethernet ring redundancy protocol (ITU-T G.8032), used for link backup, improving network reliability, Ethernet networks need faster ERPS function protection switch. Complementary STP cannot meet the requirement of fast convergence. ERPS is an ITU-T standard protocol used to prevent ring network loops. It optimizes detection and performs fast convergence. ERPS allows all ERPS-capable devices on the ring network to communicate.

As shown in Figure sample-1 => Typical networking

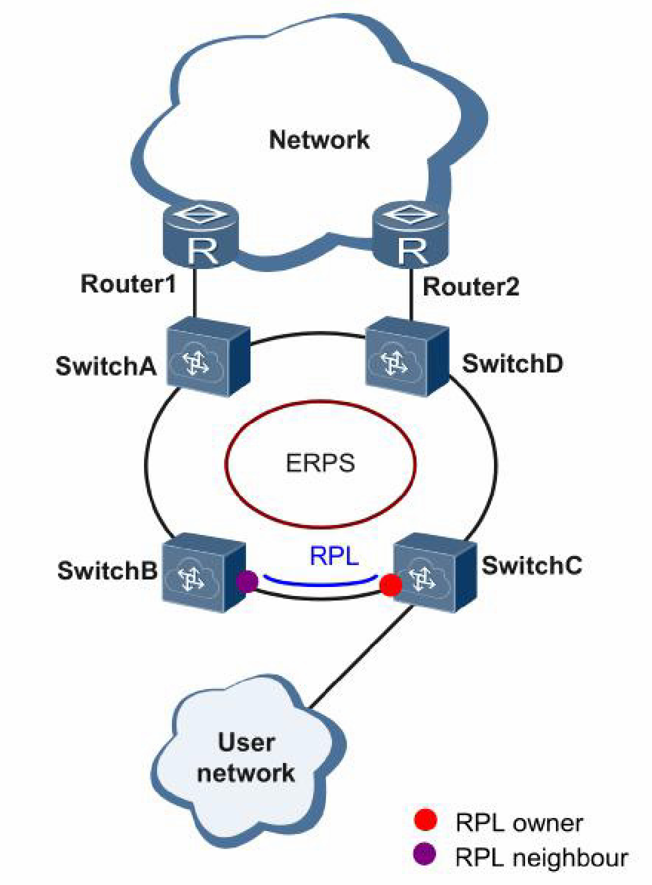


Figure sample ERPS link is normal

ERPS is a standard ring network protocol dedicated to the Ethernet link layer, with the ERPS ring as the basic unit. Only two ports on each Layer 2 switching device can join the same ERPS ring. In the ERPS ring, in order to prevent loops, you can start the loop breaking mechanism, block the RPL owner port, and eliminate the loop. When a link failure occurs on the ring network, the device running the ERPS protocol can quickly unblock the blocked port and perform link protection switching..

As shown in Figure sample-2 => Typical networking

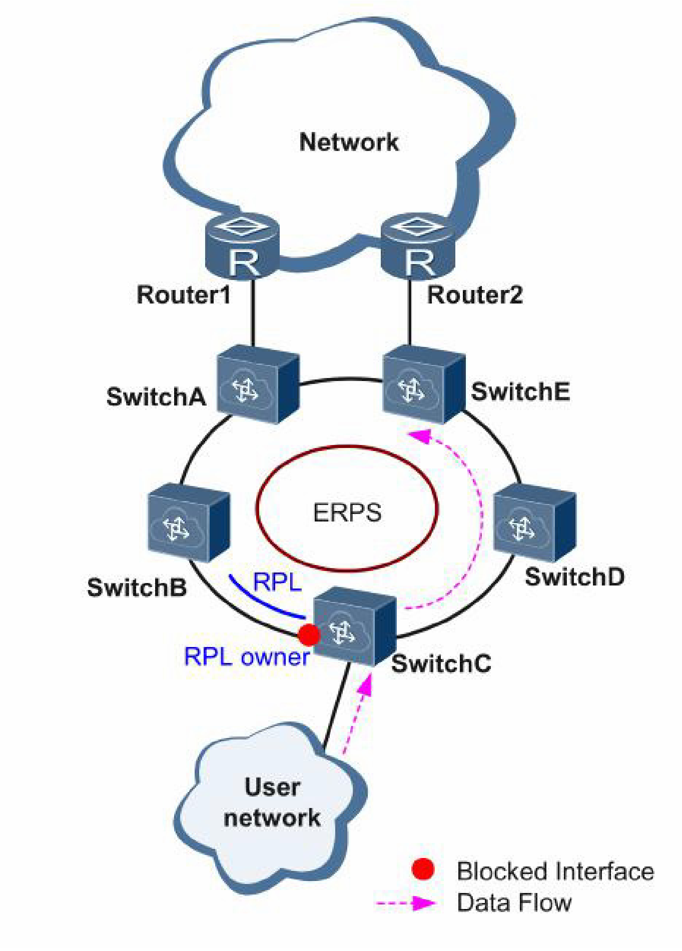


Figure sample ERPS link is normal

All devices on the ring consisting of Switch A to Switch E communicate normally.
To prevent loops, ERPS will first block the RPL owner port. If an RPL neighbor port is configured, this port will also be blocked, and other ports can forward service traffic normally.

As shown in Figure sample-3 => The link is failure

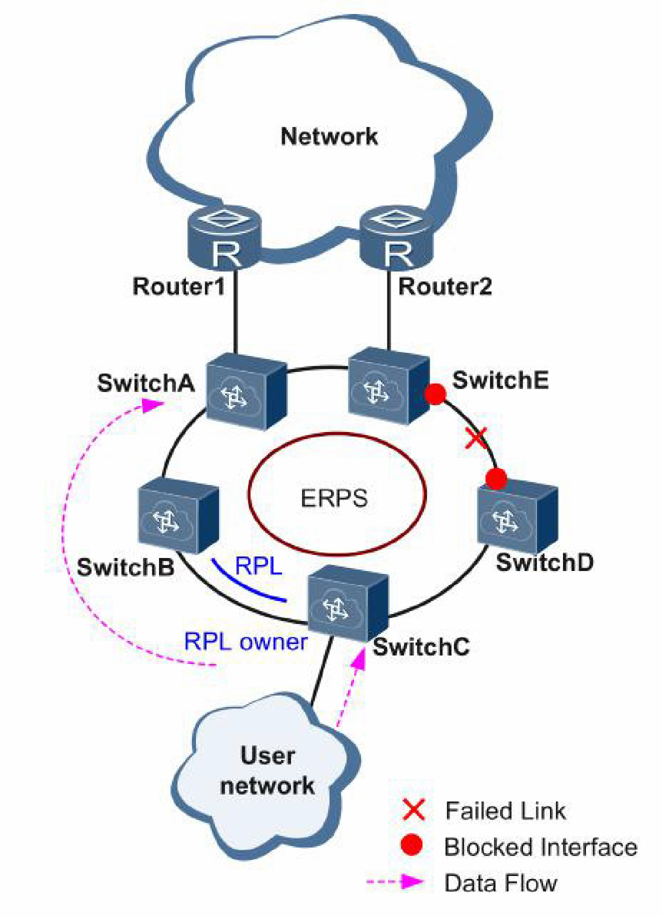


Figure sample ERPS link is failure

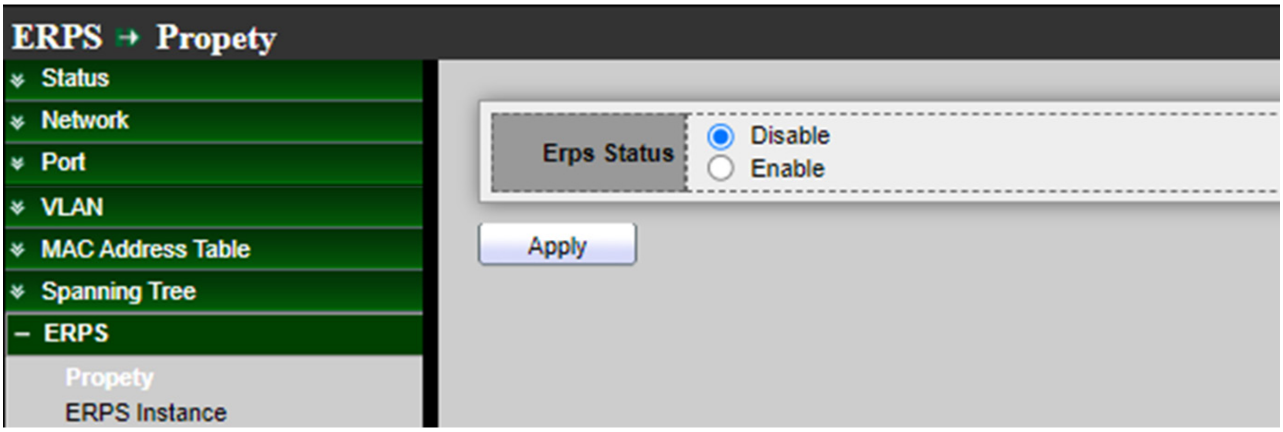
When the link between Switch D and Switch E fails, the ERPS protocol starts the protection switching mechanism, blocks the ports at both ends of the faulty link, and releases the RPL owner port. The port resumes receiving and sending user traffic, thus ensuring uninterrupted traffic.

Note	After the link returns to normal, the ERPS ring is configured in switchback mode by default. The device where the RPL owner port is located will block the traffic on the RPL link again, and the original faulty link will be used to complete the transmission of user traffic.

9.1 Propely

In a network with ring topology that runs ERPS, only one switch is assigned as an "owner" that is responsible for blocking traffic in RPL so as to avoid loops. The switch adjacent to the RPL owner is called the RPL "neighbor" node that is responsible for blocking its end of the RPL under normal condition. Other participating switches adjacent to the RPL owner or neighbor in a ring are members or RPL next-neighbor nodes to this topology and normally forward receive traffic.
ERPS, like STP, provides a loop-free network by using polling packets to detect faults. When a fault occurs, ERPS heals itself by sending traffic over a protected reverse path less than 50ms and recover quickly to forward traffic. Because of this fault detection mechanism, the network broadcast storm problem could be avoided as well.
Ethernet Ring Protection Switch (ERPS) is an Ethernet ring protection protocol which is used to prevent forming the loop in LAN, thus, the Broadcast Storm problem could be avoided. The loop avoidance mechanism ensures the traffic flows on all but the RPL ring link. In order to achieve the loop-avoidance mechanism, ITU-T G.8032 defines three roles in ERPS, which are "RPL Owner Node", "RPL Neighbor Node", and "None Node".

Administrator can configure this "ERPS "for Enable / Disable ERPS function.

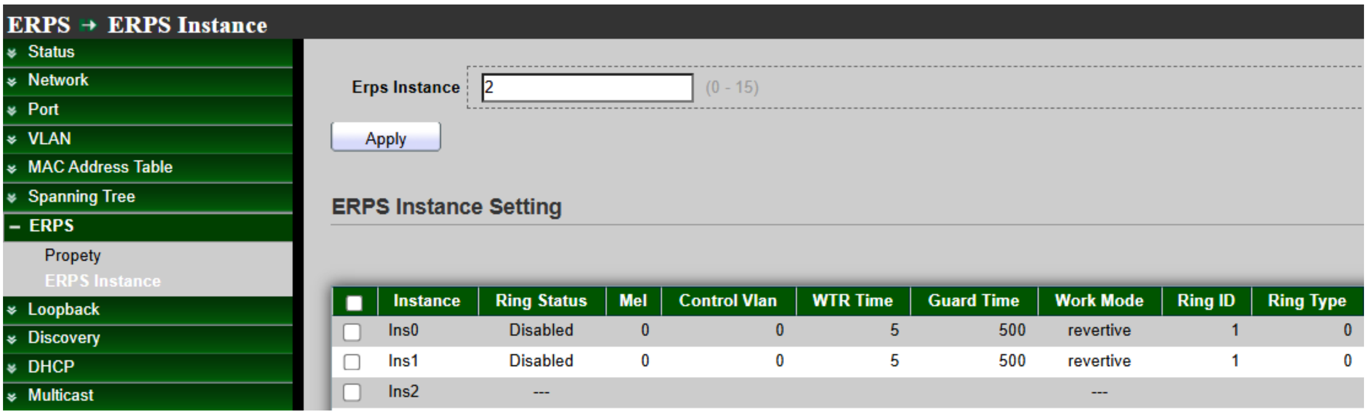


Erps Status: ● Disable ○ Enable

*Click the **"Apply"** button to save your changes settings.*

9.2 ERPS Instance Setting

Below, Chick and edit to configuration interface “ Ins” Setting.
Administrator can configure this “ERPS Instance“for Ring Instane config function.

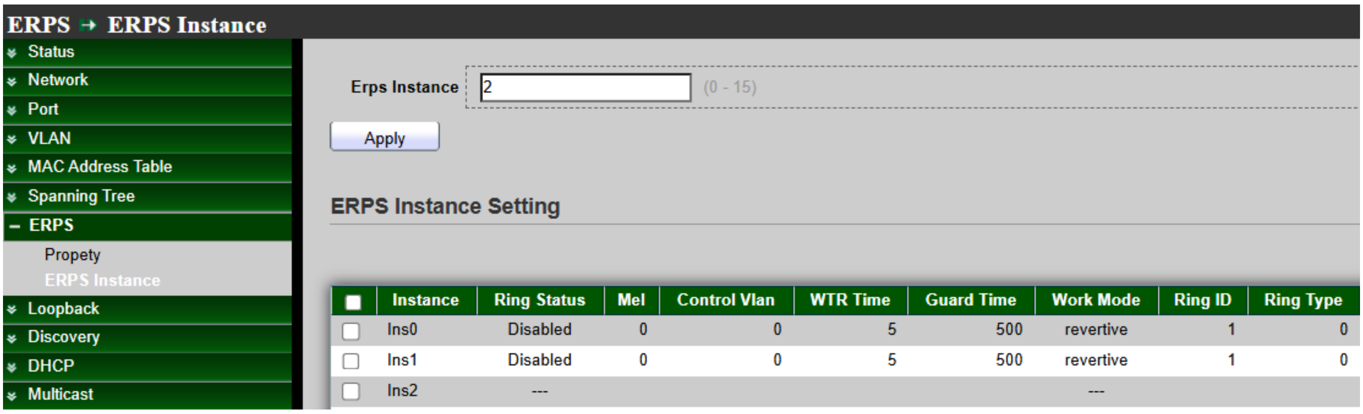


Erps Instance: 2 (0 - 15)

ERPS Instance Setting

□	Instance	Ring Status	Mel	Control Vlan	WTR Time	Guard Time	Work Mode	Ring ID	Ring Type
□	Ins0	Disabled	0	0	5	500	revertive	1	0
□	Ins1	Disabled	0	0	5	500	revertive	1	0
□	Ins2	---					---		

Note	Before configuring ERPS, the rapid spanning tree protocol (RSTP), or multiple spanning tree protocol is required to disabled, due to only one protocol is exclusive running within a switch.

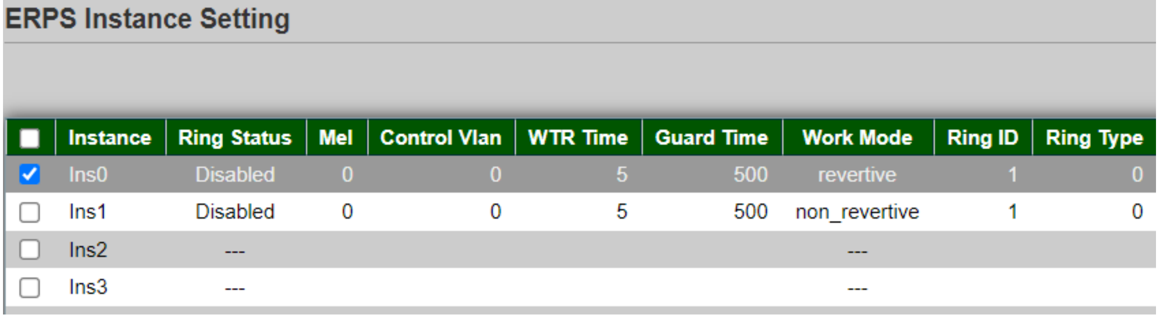

Erps Instance: 2 (0 - 15)

ERPS Instance Setting

□	Instance	Ring Status	Mel	Control Vlan	WTR Time	Guard Time	Work Mode	Ring ID	Ring Type
□	Ins0	Disabled	0	0	5	500	revertive	1	0
□	Ins1	Disabled	0	0	5	500	revertive	1	0
□	Ins2	---					---		

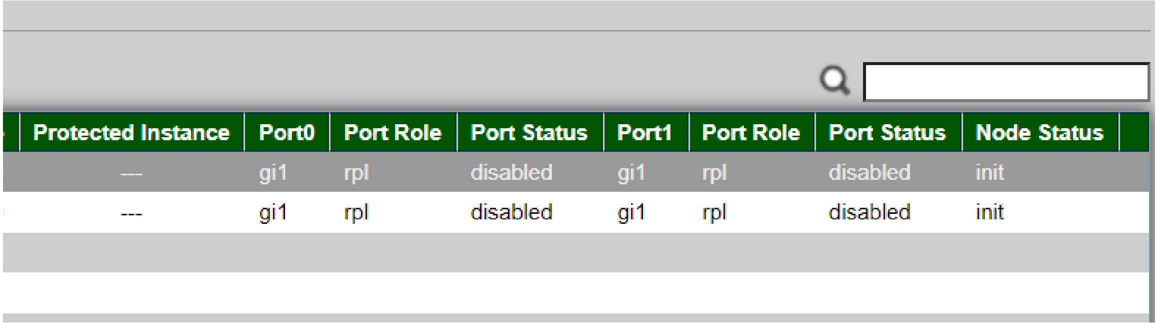
- **ERPS Instance:** The ID of the ERPS interface.

*Click the **“Apply”** button to save your changes settings.*



ERPS Instance Setting

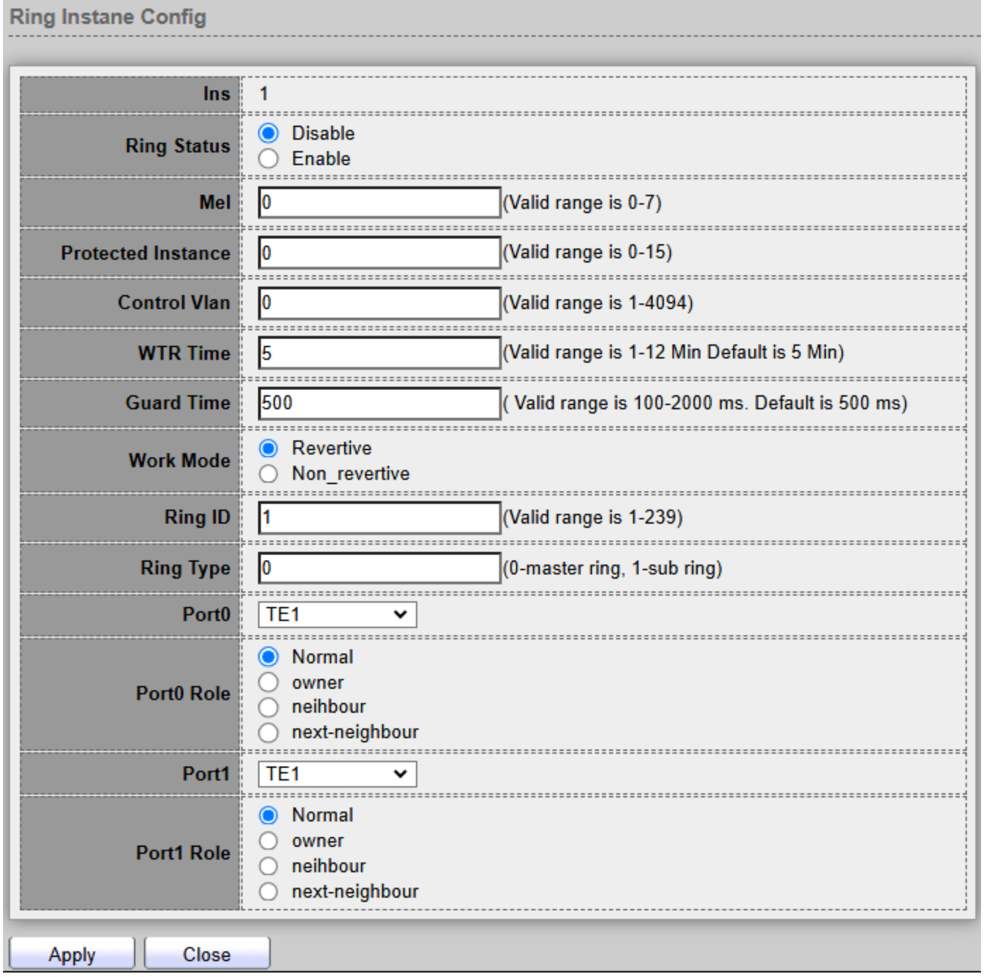
☐	Instance	Ring Status	Mel	Control Vlan	WTR Time	Guard Time	Work Mode	Ring ID	Ring Type
☑	Ins0	Disabled	0	0	5	500	revertive	1	0
☐	Ins1	Disabled	0	0	5	500	non_revertive	1	0
☐	Ins2	---					---		
☐	Ins3	---					---		



	Protected Instance	Port0	Port Role	Port Status	Port1	Port Role	Port Status	Node Status
	---	gi1	rpl	disabled	gi1	rpl	disabled	init
	---	gi1	rpl	disabled	gi1	rpl	disabled	init

Field	Description
Instance	The ID of the ERPS , The ID of the Protection group.
Ring Status	Display Enable or Disable the Ring.
Mel	Display MEL for the Ring.
Control VLAN	Display the control VLAN ID.
WTR Time	The Wait To Restore timing value to be used in revertive switching. The period of the WTR time can be configured by the operator in 1 minute steps between 5 and 12 minutes with a default value of 5 minutes.
Guard Time	Guard timeout value to be used to prevent ring nodes from receiving outdated R-APS messages. The period of the guard timer can be configured in 100 ms steps between 100 ms and 2000ms(2 seconds), with a default value of 500 ms
Work Mode	Display Revertive or Non_revertive mode. • **In Revertive mode :** after the conditions causing a protection switch has cleared,the traffic channel is restored to the working transport entity, i.e., blocked on the RPL

	• **In Non-Revertive mode :** the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared.
Ring ID	Display ring ID
Ring Type	Display ring type "0" for Master-ring or "1" for Sub-ring.
Protected Instance	Protection instance of ERPS ring instance.
Prot0	The port0(left port) for this node.
Port Role	Current port0 rule status.
Port Status	Display the port0 port(left port) status.
Port1	The port1(light port) for this node.
Port Role	Current port1 rule status.
Port Status	Display the port1 port(light port)status.
Node Status	Shows the following ERPS states: **Init :** The ERPS ring has started but has not yet determined the status of the ring. **Idle :** If all nodes in a ring are in this state, it means that all the links in the ring are up. This state will switch to protection state if a link failure occurs. **Protection :** If a node in this state, it means that a link failure has occurred. This state will switch to idle state if all the failed links recover.



Ring Instane Config

Ins	1
Ring Status	● Disable ○ Enable
Mel	0 (Valid range is 0-7)
Protected Instance	0 (Valid range is 0-15)
Control Vlan	0 (Valid range is 1-4094)
WTR Time	5 (Valid range is 1-12 Min Default is 5 Min)
Guard Time	500 (Valid range is 100-2000 ms. Default is 500 ms)
Work Mode	● Revertive ○ Non_revertive
Ring ID	1 (Valid range is 1-239)
Ring Type	0 (0-master ring, 1-sub ring)
Port0	TE1
Port0 Role	● Normal ○ owner ○ neihbour ○ next-neighbour
Port1	TE1
Port1 Role	● Normal ○ owner ○ neihbour ○ next-neighbour

- **Ring Status :** Enables/disables the ring status.
  - **Disable :** Disable the Ins for ERPS protocol.
  - **Enable :** Enable the Ins for ERPS protocol.
- **Mel :** Configures the control MEL for the ring. Valid values are from 0 to 7, Default is 0.

Note	The ring maintenance entity group level (MEL) provides a communication channel for ring automatic protecting switching (R-APS) information. On a layer 2 network running ERPS, if another fault detection protocol is enabled, the MEL field in the RAPS PDU will determine whether these packets can be forwarded. If the MEL value of the ERPS ring is less than the MEL value of the fault detection protocol, the data packet has a lower priority and is discarded. In addition, the MEL value can also be used to facilitate communication with equipment from different vendors in the ERPS ring. The same MEL value can ensure smooth communication between multi-vendor devices. The recommended setting for MEL is 7. In networks that have a main ring and a sub ring, the MEL for both rings should be set to 7.

- **Protected Instance :** The valid 0-15 protected-instance setting to configures Ethernet ring protection (ERP) instances in an ERPS ring.
- **Control VLAN :** The control VLAN of the instance should be the same as it is under Control VLAN,ERPS Control VLAN ID, ranges from 1 to 4094. It's aVLAN ID to send PDUs of ERPS.

Note	In the ERPS ring, the control VLAN is only used to forward RAPS PDUs, thereby improving the security of the ERPS protocol. All devices in the ERPS ring must be configured with the same control VLAN. Other VLANs cannot use the same ID as the control VLAN. For example, if the standard VLAN 20 already exists in the VLAN configuration, you cannot set VLAN 20 as the control VLAN of the ERPS ring.

- **WTR Time :** Configures the WTR time for the ring. Valid values are between 1 and 12 (min) , Default is 5min.
- **Guard Time :** Configures the guard time for the ring. Valid values are between 100 and 2000 (ms), Default is500ms.
- **Work Mode :** Select the reversion mode or not.
  - **Revertive :** Enables and select the reversion mode.

Note	After learning of the ring network fault restored, the RPL owner node will restore the blockade status of RPL and make the network flow transmission path restore to the link before the fault

  - **Non_revertive :** Disable and select the reversion mode.

Note	After learning of the ring network fault restored, the RPL owner node will not block the RPL, the network flow transmission path is same as before.

- **Ring ID :** ERPS ring ID, Configures the ring. Valid value are from 1 to 239 Ring ID distinguishes different Ring topology.
- **Ring Type :** Configures the Ring Type value to "0" for Master-ring or "1" for Sub-ring, Default is 0.

Note	Master-ring (if the value is set to "1")：It is the ring which connects the two ports on the interconnection node. Sub-ring (if the value is set to "0")：It is the ring which connects to other network through two interconnection nodes,it is not a ring network, it will make up a ring network only when connect it through the interconnection node.

- **Port0 :** ERPS ring port 0, it could be map to real switch port1 (GE1) – port 24(GE24)

Note	Do not set the same as Ring port1.

- **Port0 Role :** Set the ERPS port0 role as Normal or Owner, Neighbour or Next-Neighbour.
  - **Normal:** Besides Owner and Neighbor node, the rest of nodes are defined as This Normal node..
  - **Owner :** In charge of blocking one side of RPL link. It will prevent the packet flow from its blocked port.
  - **Neighbour:** In charge of blocking one side of RPL link. It will prevent the packet flow from its blocked port.
  - **Next-Neighbour:** In charge next of blocking one side of RPL link. It will prevent the packet flow from its blocked port.

- **Port1:** ERPS ring port 1, it could be map to real switch port1 (GE1) – port 24(GE24).

Note	Do not set the same as Ring port0.

- **Port1 Role :** Set the ERPS port1 role as Normal or Owner, Neighbour or Next-Neighbour..
  - **Normal:** Besides Owner and Neighbor node, the rest of nodes are defined as This Normal node..
  - **Owner :** In charge of blocking one side of RPL link. It will prevent the packet flow from its blocked port.
  - **Neighbour:** In charge of blocking one side of RPL link. It will prevent the packet flow from its blocked port.
  - **Next-Neighbour:** In charge next of blocking one side of RPL link. It will prevent the packet flow from its blocked port

Note	Do not connect all switches to form a loop (ring) network until you have enabled any ERPS protocol on any ring node. There should be at least one ring port unplugged until all nodes in the topology are ready.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

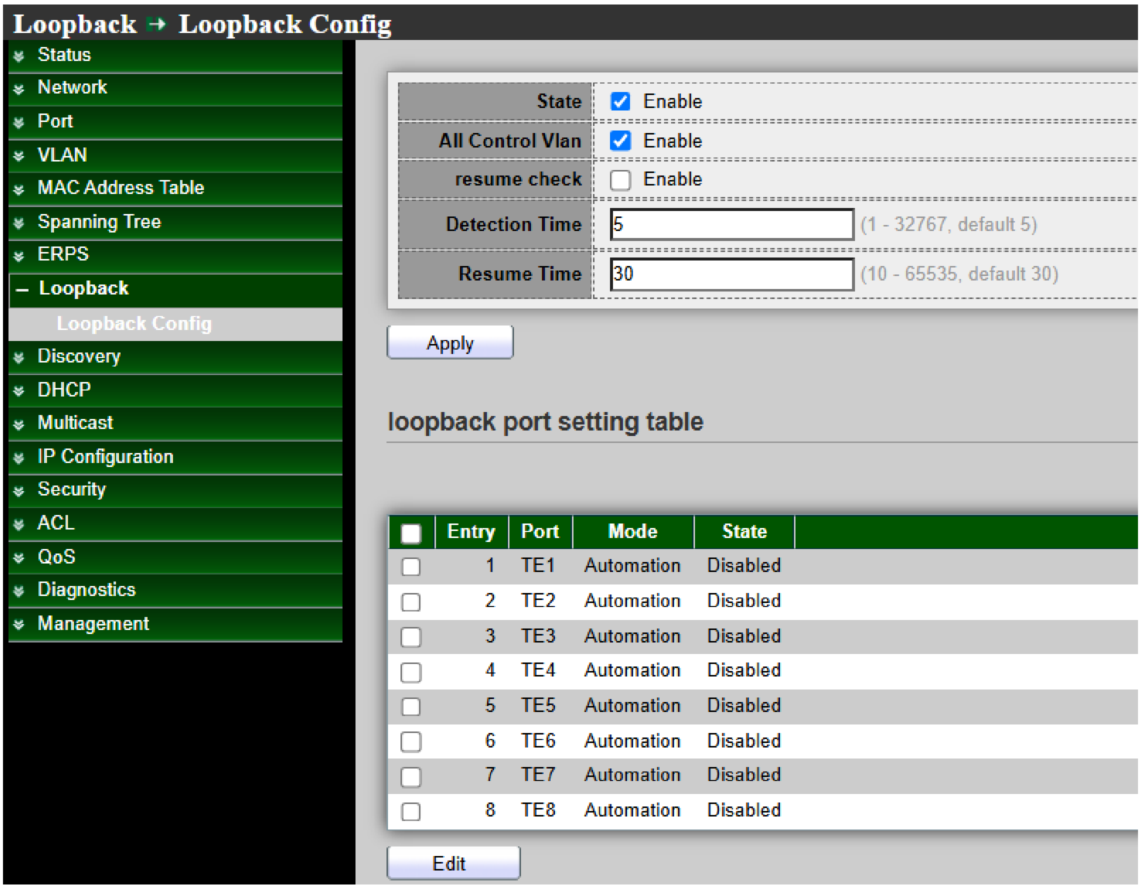
10. Loopback

Loops in the network can lead to a waste of network resources or even network paralysis. In order to detect loops in the network in a timely manner and avoid serious impact on the entire network, we provide behavior detection technology (Loopback) that sends the network packet data stream back to the sender as it is, so that when a loop occurs in the network, users can promptly carry out basic network security countermeasures and inspections to avoid possible paralysis caused by loops and obtain the lowest possible shutdown control state.

Loopback is exactly such a detection technology. It periodically transmits monitoring packets from the interface to check whether the packet is returned to the original device intact, and then determines whether there is a loop between the network device or the network interface. After a loop is discovered, the interface can be processed according to the user's prior settings (such as the default close port interface) to keep the interface under control and reduce the possible impact of the loop on the device or even the entire network.

10.1 Loopback Config

Administrator can configure this page edit port settings of Loopback, Setting **"Apply"** function for this management.



State	☑ Enable
All Control Vlan	☑ Enable
resume check	□ Enable
Detection Time	5 (1 - 32767, default 5)
Resume Time	30 (10 - 65535, default 30)

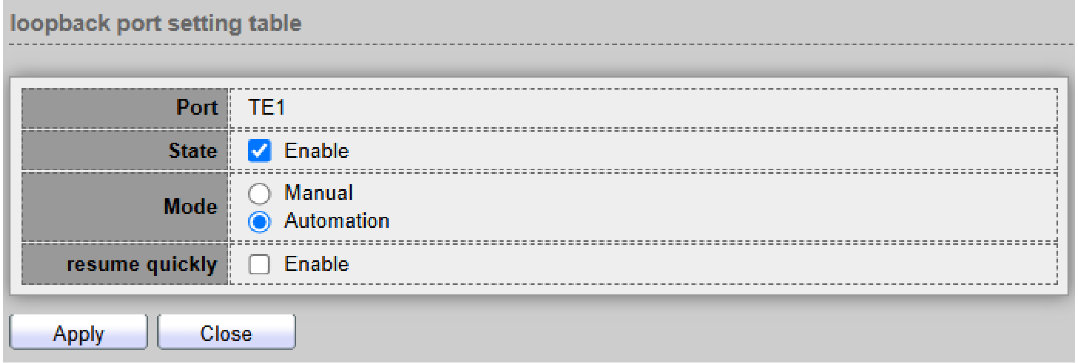
loopback port setting table

□	Entry	Port	Mode	State
□	1	TE1	Automation	Disabled
□	2	TE2	Automation	Disabled
□	3	TE3	Automation	Disabled
□	4	TE4	Automation	Disabled
□	5	TE5	Automation	Disabled
□	6	TE6	Automation	Disabled
□	7	TE7	Automation	Disabled
□	8	TE8	Automation	Disabled

- **State :** Set the enabling status of loopback-detection
- **All Control Vlan :** Enable loop detection for global vlan
- **Resume check :** Set loopback resume Advance detection.
- **Detection Time :** Administrator can set the loop time intervals for 1~32767 sec.
- **Resume Tmie :** Administrator can set the loop recovery time for 10~65535 sec.

*Click the **"Apply"** button to save your changes settings.*

Field	Description
Entry	Display number of entry
Port	Display the number of port
Mode	The response mode selected for the port: Manual or Automation
State	Display the status of port loopback detection



loopback port setting table

Port	TE1
State	☑ Enable
Mode	○ Manual ● Automation
resume quickly	□ Enable

- **Port :** The port to be edited.
- **State :** Click the check box to enable the loopback detection feature of the interface.
- **Mode :** Selects the action when the port detects a loopback

- **Manual :** In manual mode, When a network loop is detected on the network port, in addition to the abnormal flashing of the indicator light of the network port that generated the loop for identification, the network port's transmission capability will be in a block prevention state that stops transmission. Under this Manual mode setting, the network port that generated the loop will need to be manually restored to the usable state. This function can be turned off and on again before normal operation can be restored. (The closing and reopening of this Manual mode requires human judgment to determine whether the network port has indeed eliminated loopback before it can function normally).

- **Automation :** In Automation mode. When a network loop is detected on the network port, in addition to the abnormal flashing of the indicator light of the network port causing the loop for identification, the network port's transmission capability will be in a block prevention state that stops transmission and is turned off. Under this Automation mode setting, the system will automatically continue to detect in a 5-second cycle and automatically return to the available state. (When no loop is found within 5 seconds, the network port of the loop will automatically switch from the block state to the normal state that is available}

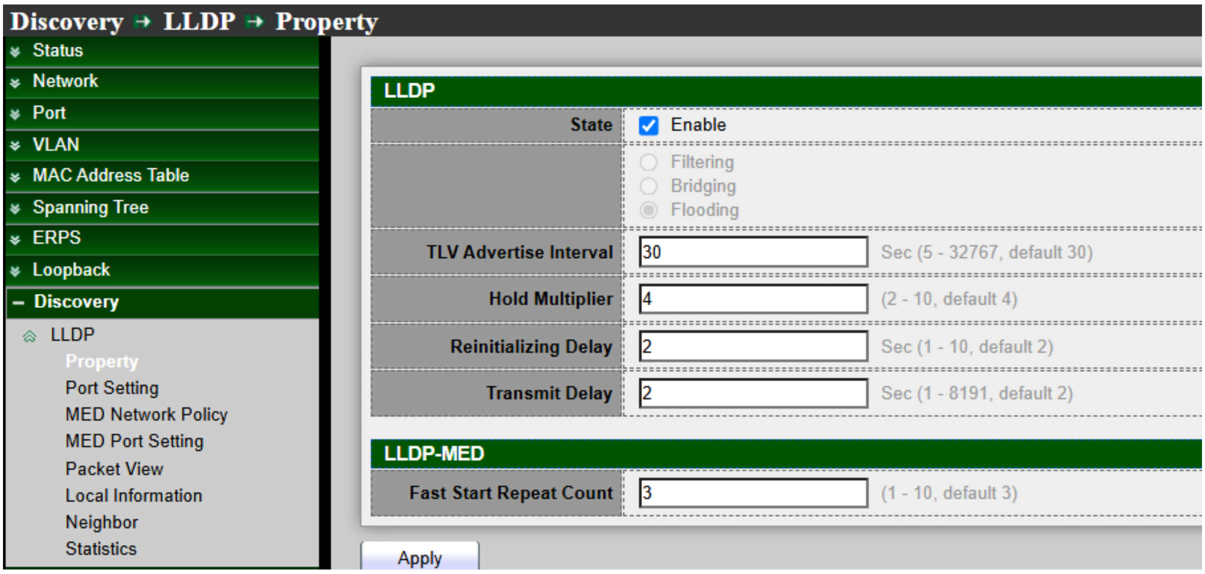
- **Resume quickly :** Set loopback Immediate recovery.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

11. Discovery(LLDP)

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, principally wired Ethernet.
LLDP information is sent by devices from each of their interfaces at a fixed interval, in the form of an Ethernet frame. Each frame contains one LLDP Data Unit (LLDPDU). Each LLDPDU is a sequence of type-length-value (TLV) structures.

11.1 Property



LLDP

State	☑ Enable	
	○ Filtering ○ Bridging ● Flooding	
TLV Advertise Interval	30	Sec (5 - 32767, default 30)
Hold Multiplier	4	(2 - 10, default 4)
Reinitializing Delay	2	Sec (1 - 10, default 2)
Transmit Delay	2	Sec (1 - 8191, default 2)

LLDP-MED

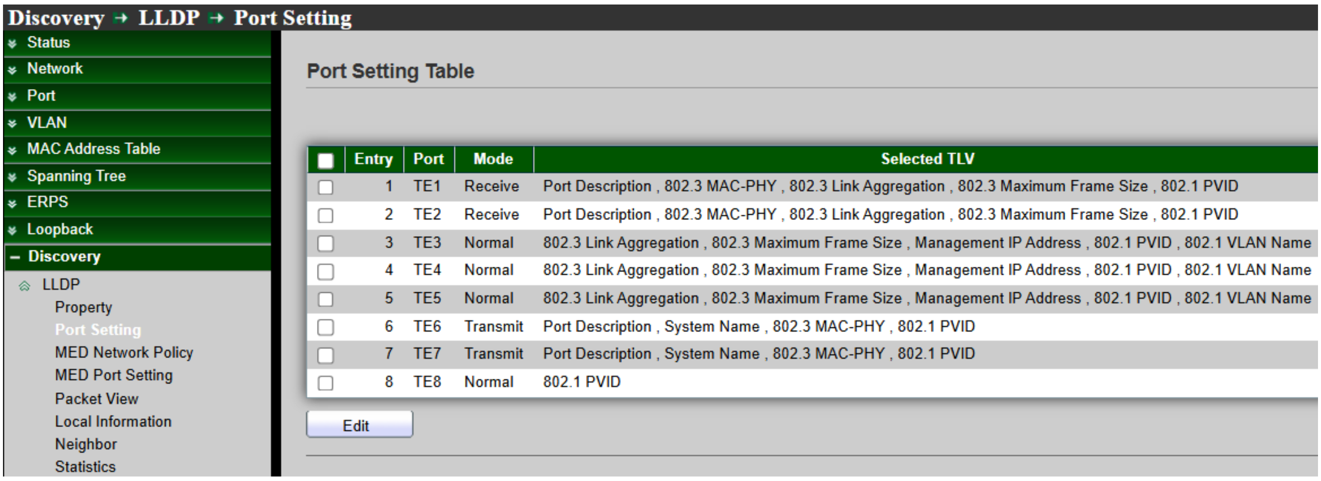
Fast Start Repeat Count	3	(1 - 10, default 3)

- **State:** Administrator can choose Enable or disable this LLDP function.
- **LLDP Handing:** If cancel checkbox then administrator can choose Filtering / Bridging / Flooding for LLDP handing. Select LLDP PDU handling action to be filtered, bridging or flooded when LLDP is globally disabled
  - **Filtering:** Deletes the packet.
  - **Bridging:** (VLAN-aware flooding) Forwards the packet to all VLAN members.
  - **Flooding:** Forwards the packet to all ports
- **TLV Advertise Interval:** Select the interval at which frames are transmitted. (range 5-32760, default is 30)
- **Hold Multiplier:** Set Hold value (Range 2-10, default is 4). Administrator can control the aging time of local information on the neighbor device by configuring the value of the Hold multiplier. *TTL=Hold multiplier * TLV Advertise Interval.*
- **Reinitializing Delay:** S Select the delay before a re-initialization (range 1–10 seconds, default = 2)..
- **Transmit Delay:** Select the delay after an LLDP frame is sent (range 1–8191 seconds, default = 3).
- **Fast Start Repeat Count:** The fast start repeat count when port link up(range 1–10,default = 3).

*Click the **"Apply"** button to save your changes settings.*

11.2 Port Setting

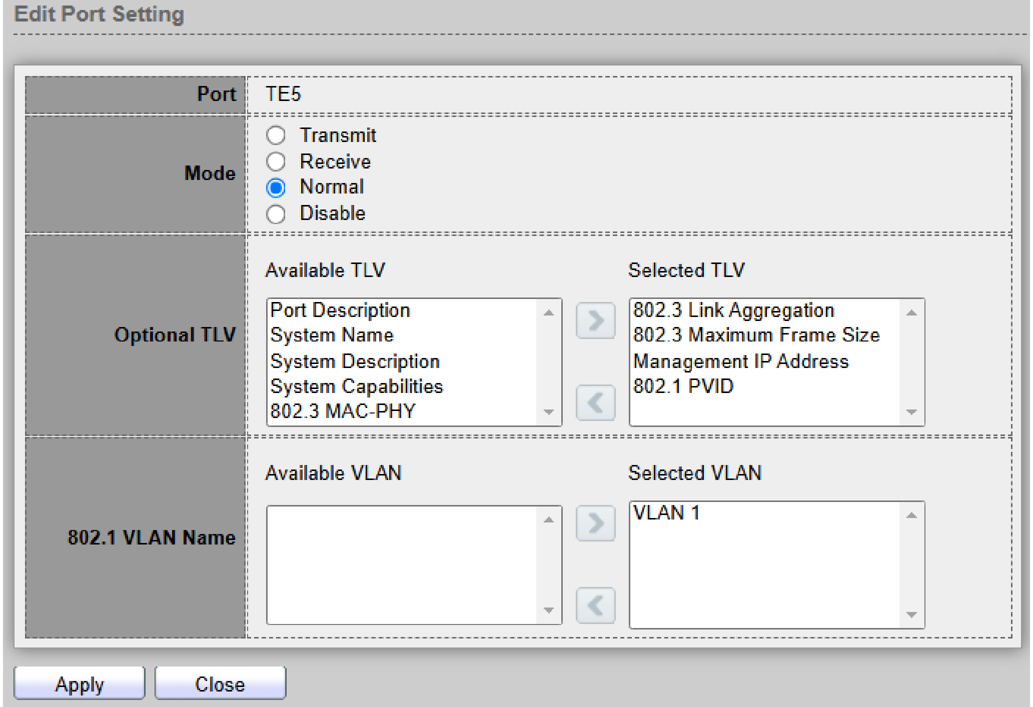
Administrator can configure each port of the LLDPDU Transmit / Receive / Normal or Disable the mode and choose from "Optional TLV" list send the TLV type of port.



Port Setting Table

□	Entry	Port	Mode	Selected TLV
□	1	TE1	Receive	Port Description , 802.3 MAC-PHY , 802.3 Link Aggregation , 802.3 Maximum Frame Size , 802.1 PVID
□	2	TE2	Receive	Port Description , 802.3 MAC-PHY , 802.3 Link Aggregation , 802.3 Maximum Frame Size , 802.1 PVID
□	3	TE3	Normal	802.3 Link Aggregation , 802.3 Maximum Frame Size , Management IP Address , 802.1 PVID , 802.1 VLAN Name
□	4	TE4	Normal	802.3 Link Aggregation , 802.3 Maximum Frame Size , Management IP Address , 802.1 PVID , 802.1 VLAN Name
□	5	TE5	Normal	802.3 Link Aggregation , 802.3 Maximum Frame Size , Management IP Address , 802.1 PVID , 802.1 VLAN Name
□	6	TE6	Transmit	Port Description , System Name , 802.3 MAC-PHY , 802.1 PVID
□	7	TE7	Transmit	Port Description , System Name , 802.3 MAC-PHY , 802.1 PVID
□	8	TE8	Normal	802.1 PVID

Field	Description
Port	Display the port of LLDP state.
Mode	Display the Transmit (TX Only),Receive (RX Only),Normal (TX And RX),Disable
Selected TLV	Display the TLVs for your selected.



Edit Port Setting

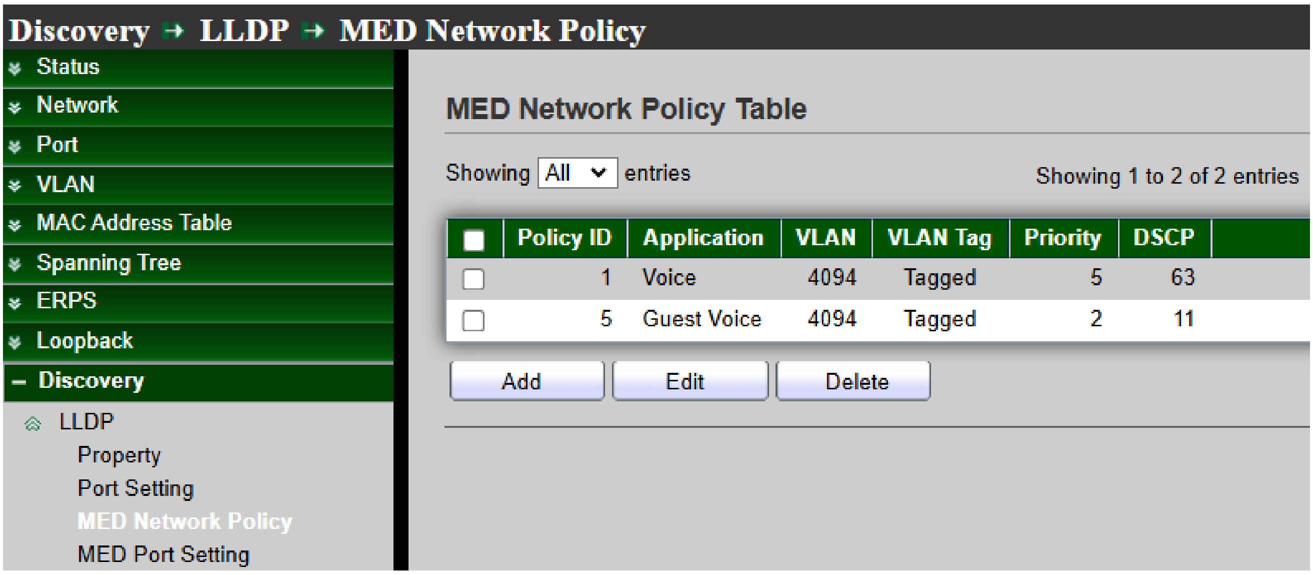
Port	TE5
Mode	○ Transmit ○ Receive ● Normal ○ Disable
Optional TLV	Available TLV: Port Description, System Name, System Description, System Capabilities, 802.3 MAC-PHY Selected TLV: 802.3 Link Aggregation, 802.3 Maximum Frame Size, Management IP Address, 802.1 PVID
802.1 VLAN Name	Available VLAN: Selected VLAN: VLAN 1

- **Mode :** Administrator can choose Transmit(TX) / Receive(RX) or Normal(TX+RX) and Disable, if choose disable will don't send and receive LLDPDU.
  - Transmit (TX Only): Transmit LLDP PDUs only.
  - Receive (RX Only): Receive LLDP PDUs only.
  - Normal (TX And RX): Transmit and receive LLDP PDUs both
  - Disable : Disable the transmission of LLDP PDUs
- **Optional TLV :** Administrator can be configuration information into different TLV, encapsulates LLDPDU and issued to the neighbor device.
  - 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 to be carried (multiple selection is allowed).

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

11.3 MED Network Policy

Administrator can see the display for LLDP MED Network Policy Setting, Setting **"add"** and "Edit" and **"Delete"** function for this management.

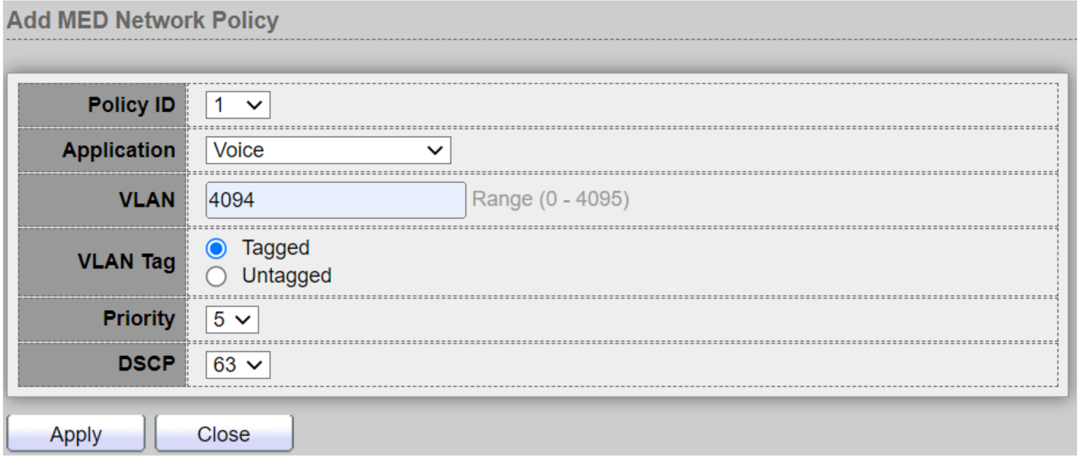


MED Network Policy Table

Showing All entries Showing 1 to 2 of 2 entries

□	Policy ID	Application	VLAN	VLAN Tag	Priority	DSCP
□	1	Voice	4094	Tagged	5	63
□	5	Guest Voice	4094	Tagged	2	11

Field	Description
Policy ID	Display the policy ID.
Application	Display the network policy type.
VLAN	Display the VLAN ID.
VLAN Tag	Display the VLAN tag status.
Priority	Display the L2 priority.
DSCP	Display the DSCP value.



Add MED Network Policy

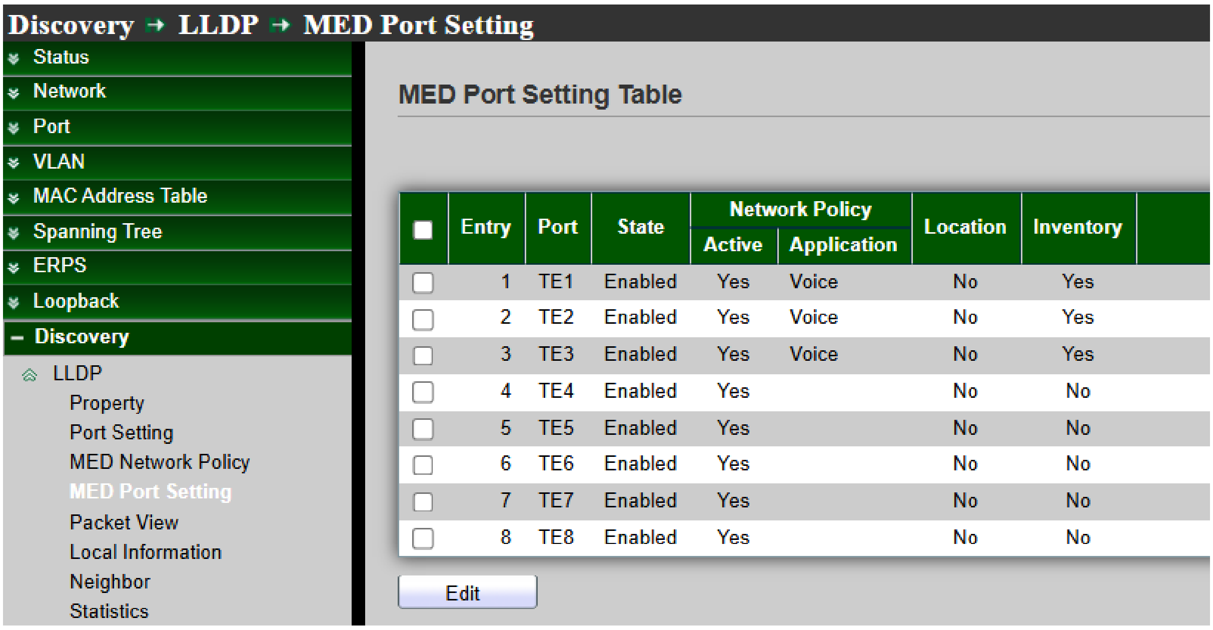
Policy ID	1
Application	Voice
VLAN	4094 Range (0 - 4095)
VLAN Tag	● Tagged ○ Untagged
Priority	5
DSCP	63

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

*Click the **“Apply”** button to save your changes or **“Close”** the button to close settings.*

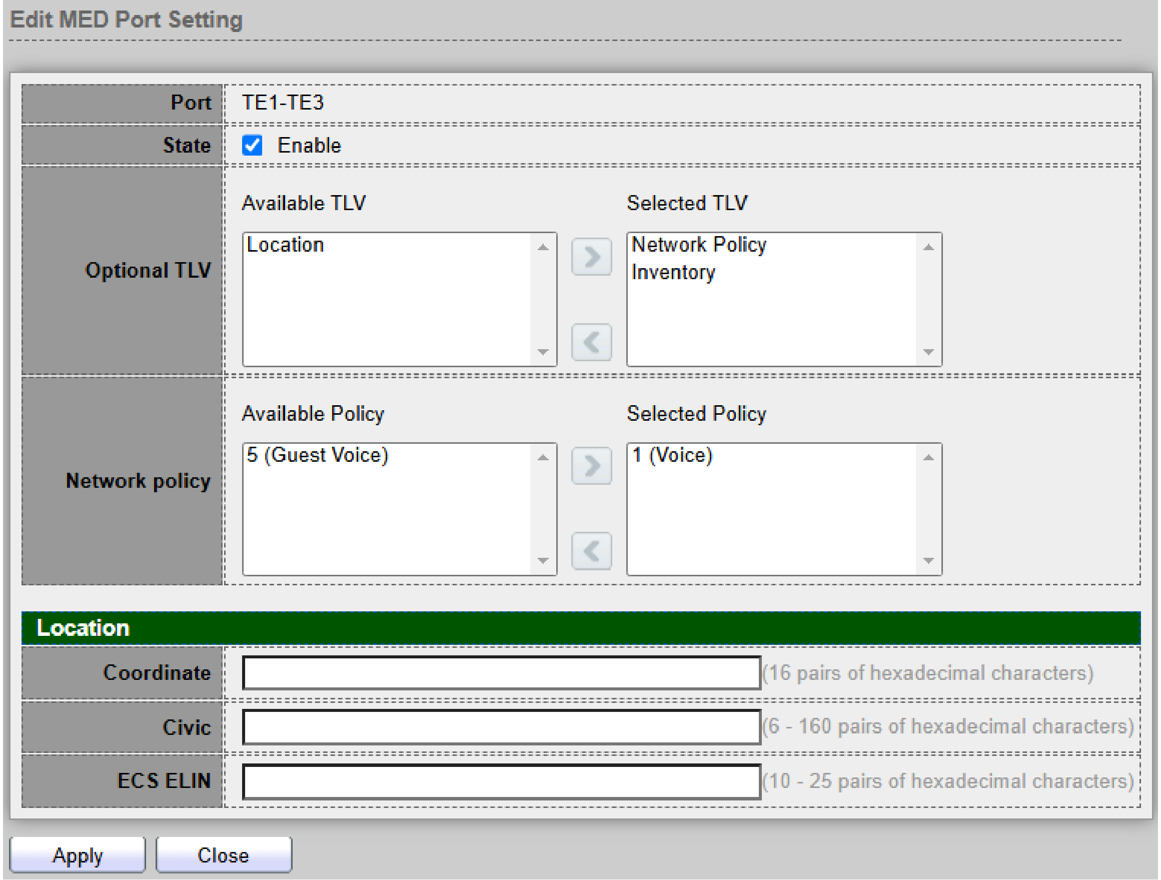
11.4 MED Port Setting

Administrator can see the display for LLDP MED Port Setting.



□	Entry	Port	State	Network Policy		Location	Inventory
				Active	Application		
□	1	TE1	Enabled	Yes	Voice	No	Yes
□	2	TE2	Enabled	Yes	Voice	No	Yes
□	3	TE3	Enabled	Yes	Voice	No	Yes
□	4	TE4	Enabled	Yes		No	No
□	5	TE5	Enabled	Yes		No	No
□	6	TE6	Enabled	Yes		No	No
□	7	TE7	Enabled	Yes		No	No
□	8	TE8	Enabled	Yes		No	No

Field	Description
Port	Display the LLDP MED specified port.
State	Display the LLDP MED status
Optional TLV	Display the LLDP MED optional TLVs.
Network Policy	Display the LLDP MED network policy Active and Application IDs.
Location	Display the location status.
Inventory	Display the inventory by yes or no.



Edit MED Port Setting

Port	TE1-TE3
State	☑ Enable
Optional TLV	Available TLV: Location Selected TLV: Network Policy, Inventory
Network policy	Available Policy: 5 (Guest Voice) Selected Policy: 1 (Voice)

Location

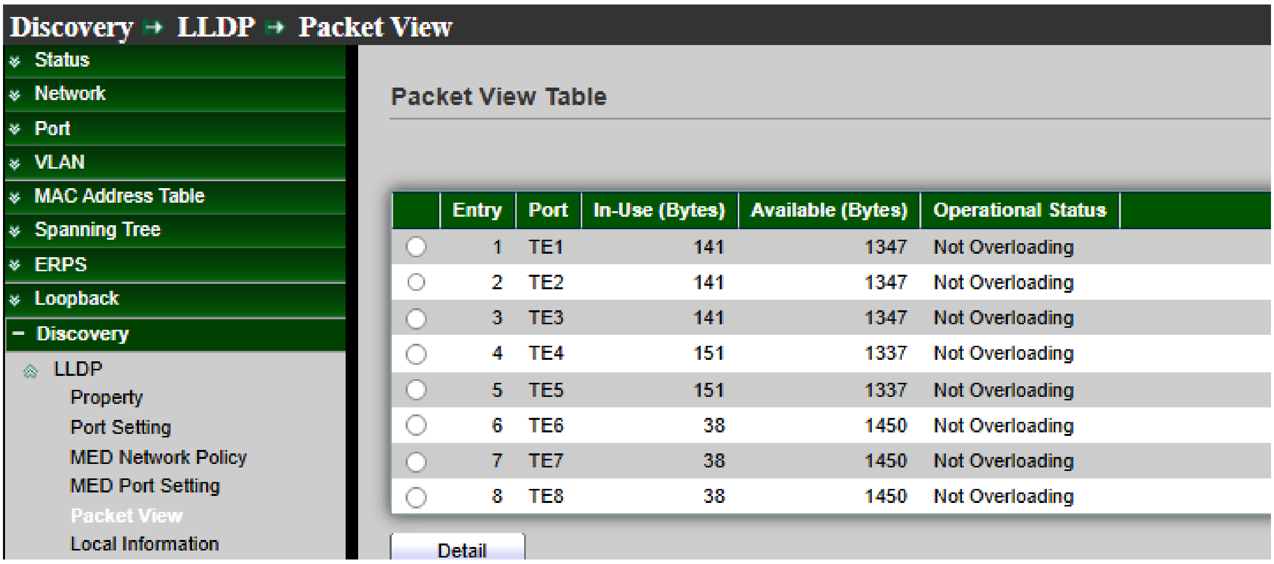
Coordinate	(16 pairs of hexadecimal characters)
Civic	(6 - 160 pairs of hexadecimal characters)
ECS ELIN	(10 - 25 pairs of hexadecimal characters)

- **Port :** Select specified port or all ports to configure LLDP MED.
- **State :** Select LLDP MED enable status
- **Optional TLV :** Select LLDP MED optional TLVs (multiple selection is allowed).
  - Network Policy
  - Location
  - Inventory
- **Network Policy :** Select the network policy IDs to be bound to ports. The network policy should be created in MED Network Policy page at first.
- **Location:**
  - **Coordinate : Set Coordinate**
  - **Civic : Set Civic**
  - **ECS ELIN : Set ECS ELIN**

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

11.5 Packet View

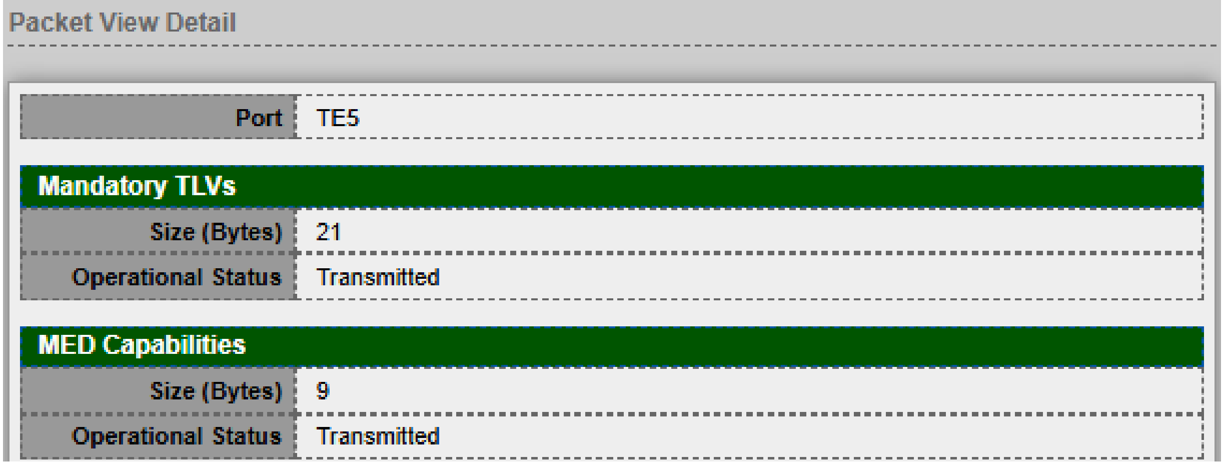
Administrator can select which port to view and click on the "**Detail**" button to view the information of the LLDP packet on the selected port.



Packet View Table

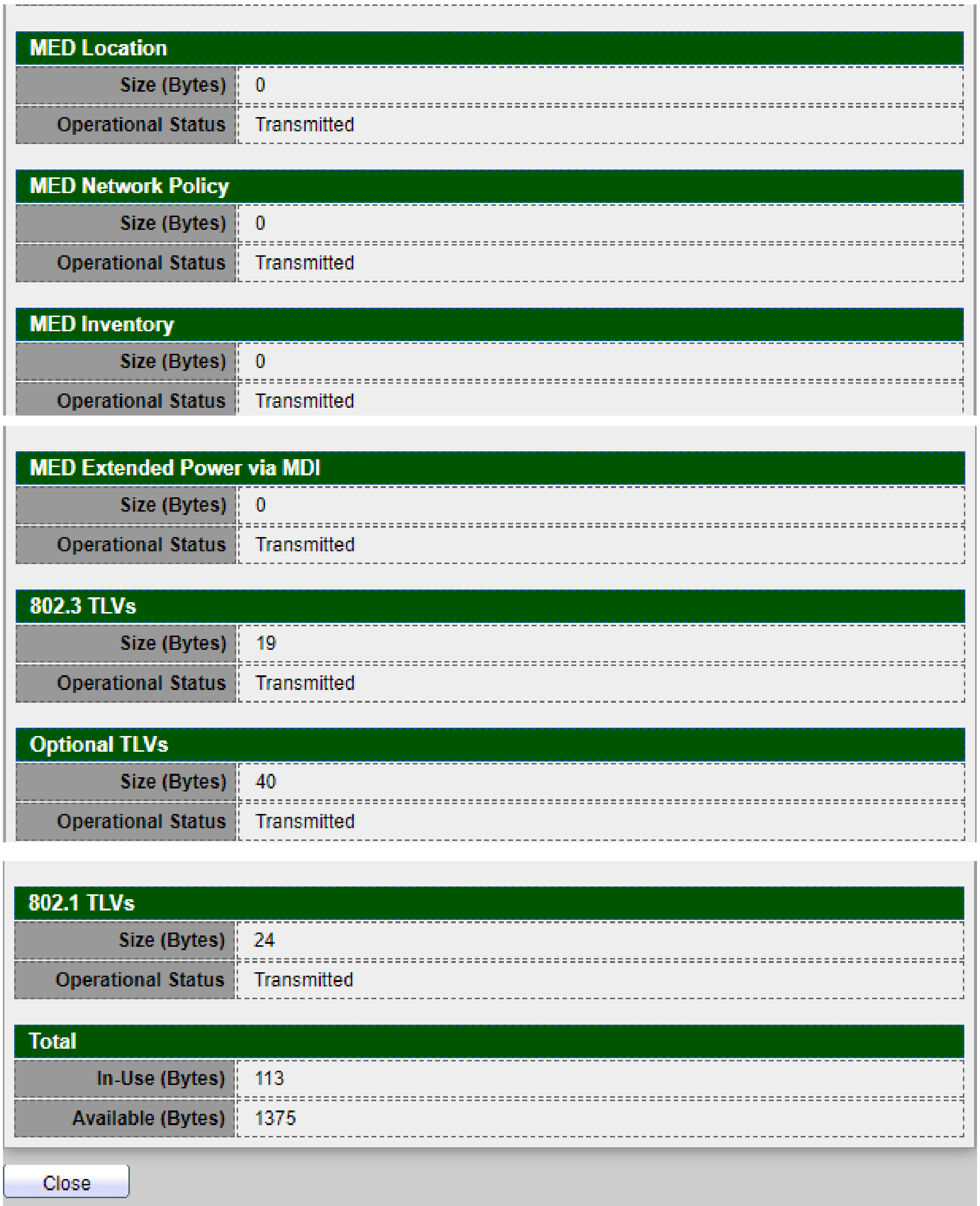
	Entry	Port	In-Use (Bytes)	Available (Bytes)	Operational Status
○	1	TE1	141	1347	Not Overloading
○	2	TE2	141	1347	Not Overloading
○	3	TE3	141	1347	Not Overloading
○	4	TE4	151	1337	Not Overloading
○	5	TE5	151	1337	Not Overloading
○	6	TE6	38	1450	Not Overloading
○	7	TE7	38	1450	Not Overloading
○	8	TE8	38	1450	Not Overloading

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



Packet View Detail

Port	TE5
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)	19
Operational Status	Transmitted

Optional TLVs	
Size (Bytes)	40
Operational Status	Transmitted

802.1 TLVs	
Size (Bytes)	24
Operational Status	Transmitted

Total	
In-Use (Bytes)	113
Available (Bytes)	1375

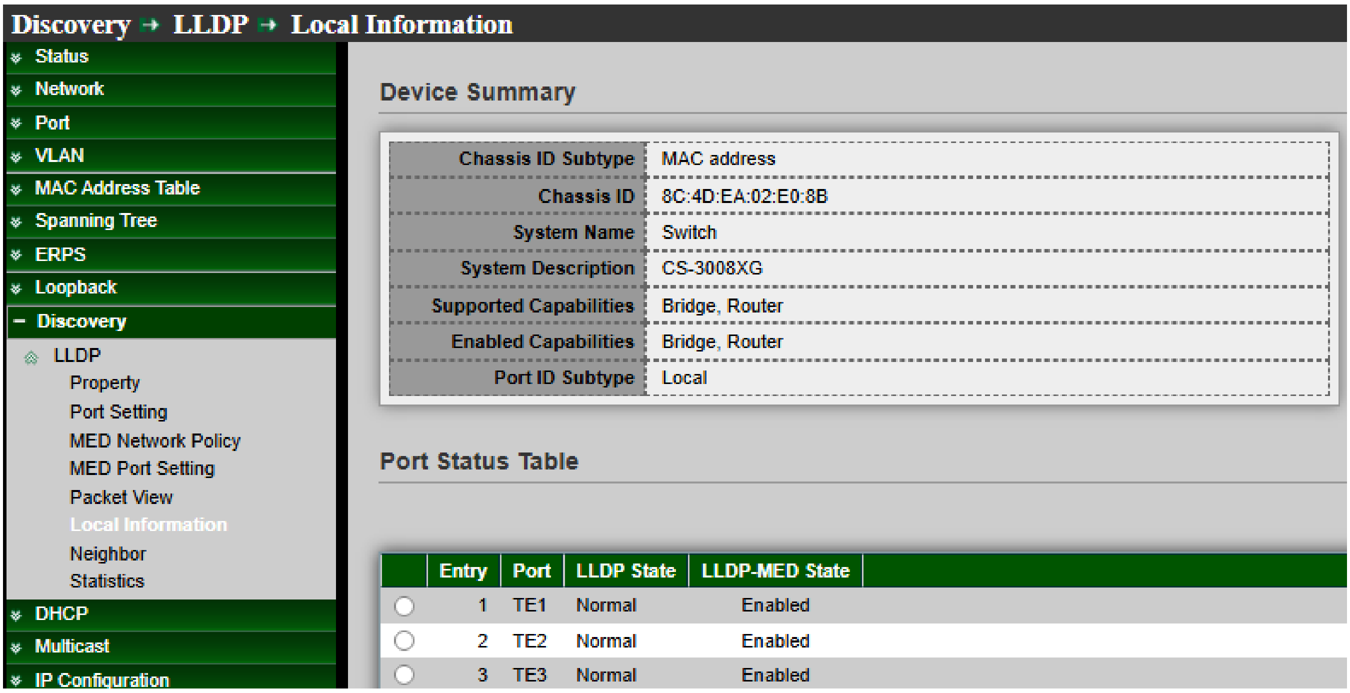
*Click the **“Close”** button to close the view detail page.*

Field	Description
Port	Port Name
Mandatory TLVs	Total mandatory TLV byte size. Status is sent or overloading.
MED Capabilities	Total MED Capabilities TLV byte size. Status is sent or overloading.

MED Location	Total MED Location byte size. Status is sent or overloading.
MED Network Policy	Total MED Network Policy byte size. Status is sent or overloading.
MED Inventory	Total MED Inventory byte size. Status is sent or overloading.
MED Extended Power via MDI	Total MED Extended Power via MDI byte size. Status is sent or overloading.
802.3 TLVs	Total 802.3 TLVs byte size. Status is sent or overloading.
Optional TLVs	Total Optional TLV byte size. Status is sent or overloading.
802.1 TLVs	Total 802.1 TLVs byte size. Status is sent or overloading.
Total	Total number of bytes of LLDP information in each packet.

11.6 Local Information

Displays switch summary and every port status of LLDP. Administrator can select which port to view and click on the "**detail**" button to view the information of the local device as well as the information of selected port LLDP property.



Device Summary

Chassis ID Subtype	MAC address
Chassis ID	8C:4D:EA:02:E0:8B
System Name	Switch
System Description	CS-3008XG
Supported Capabilities	Bridge, Router
Enabled Capabilities	Bridge, Router
Port ID Subtype	Local

Port Status Table

	Entry	Port	LLDP State	LLDP-MED State
○	1	TE1	Normal	Enabled
○	2	TE2	Normal	Enabled
○	3	TE3	Normal	Enabled

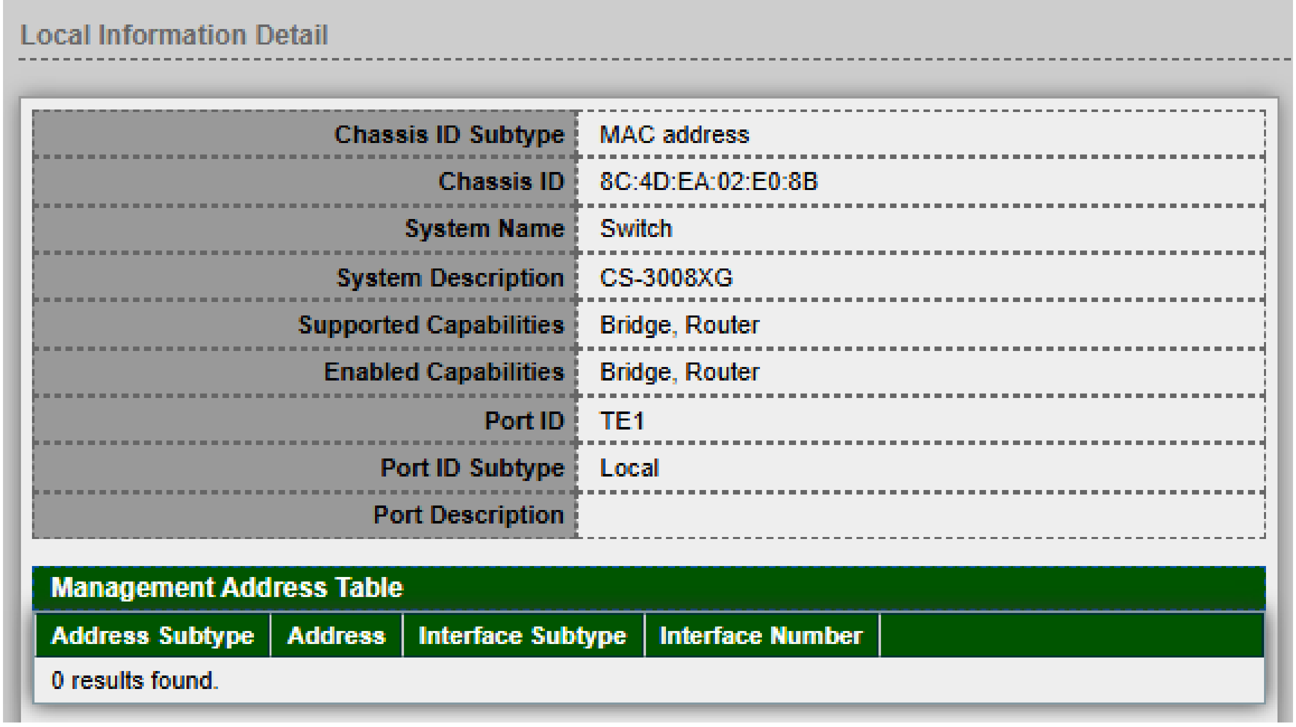
Device Summary

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

Port Status Table

Field	Description
Port	Type of the port number
LLDP Status	LLDP Tx and Rx abilities.
LLDP Med Status	LLDP MED enable state.

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



Local Information Detail

Chassis ID Subtype	MAC address
Chassis ID	8C:4D:EA:02:E0:8B
System Name	Switch
System Description	CS-3008XG
Supported Capabilities	Bridge, Router
Enabled Capabilities	Bridge, Router
Port ID	TE1
Port ID Subtype	Local
Port Description	

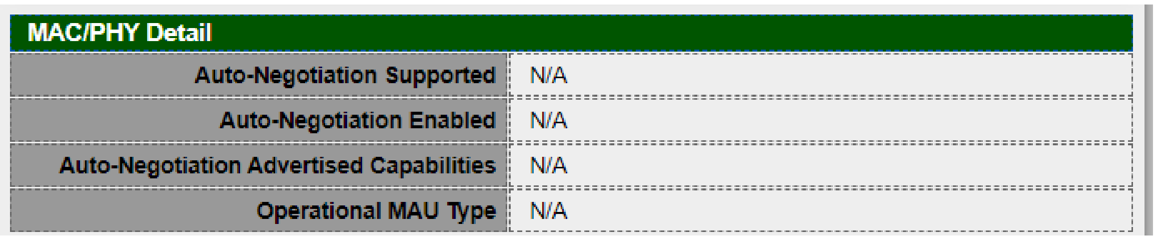
Management Address Table

Address Subtype	Address	Interface Subtype	Interface Number
0 results found.			

Management Address Table

Field	Description
Address Subtype	Type of the port number
Address	Display management IP address type.
Interface Subtype	Returned address most appropriate for management use, typically a Layer 3 address.
Interface number	Specific interface associated with this management address.

MAC/PHY Details

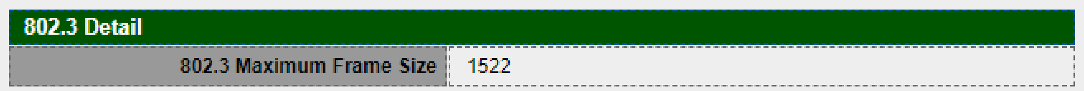


MAC/PHY Detail

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

Field	Description
Auto-Negotiation Supported	Port speed auto-negotiation support status.
Auto-Negotiation Enabled	Port speed auto-negotiation active status.
Auto-Negotiation Advertised Capabilities	Port speed auto-negotiation capabilities, for example, 1000BASE-T half-duplex mode, 100BASE-TX full-duplex mode.
Operational MAU Type	Medium Attachment Unit (MAU) type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interfaces' collision detection and bit injection into the network, for example, 100BASE-TX full duplex mode.

802.3 Detail

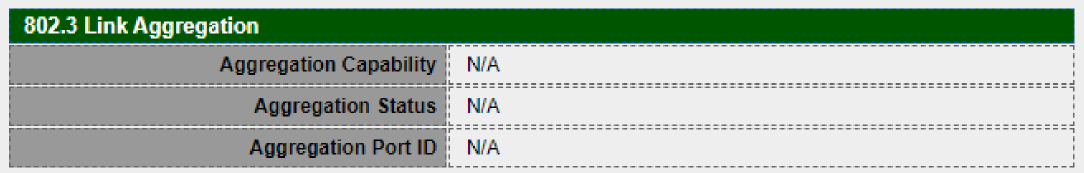


802.3 Detail

802.3 Maximum Frame Size	1522

Field	Description
802.3 Maximum Frame Size	The maximum supported IEEE 802.3 frame size.

802.3 Link Aggregation

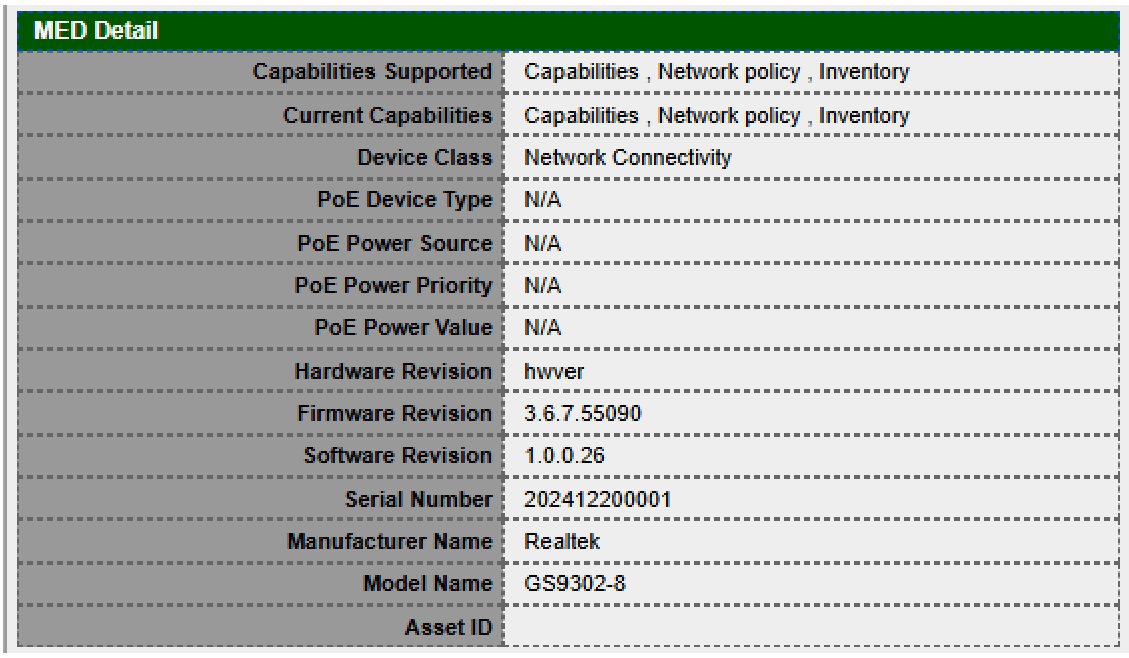


802.3 Link Aggregation

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

Field	Description
Aggregation Capability	Indicates whether the interface can be aggregated.
Aggregation Status	Indicates whether the interface is aggregated.
Aggregation Port ID	Advertised aggregated interface ID.

MED Detail

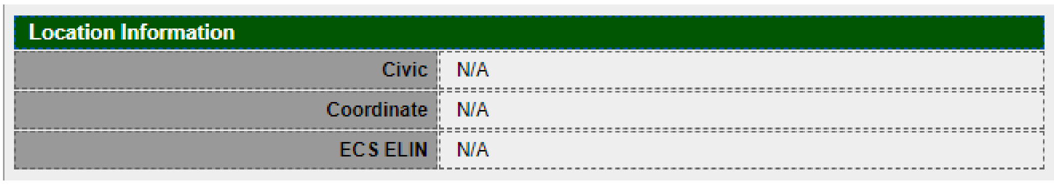


MED Detail	
Capabilities Supported	Capabilities , Network policy , Inventory
Current Capabilities	Capabilities , Network policy , Inventory
Device Class	Network Connectivity
PoE Device Type	N/A
PoE Power Source	N/A
PoE Power Priority	N/A
PoE Power Value	N/A
Hardware Revision	hwver
Firmware Revision	3.6.7.55090
Software Revision	1.0.0.26
Serial Number	202412200001
Manufacturer Name	Realtek
Model Name	GS9302-8
Asset ID	

Field	Description
Capabilities Supported	MED capabilities supported on the port.
Current Capabilities	MED capabilities enabled on the port.
Device Class	LLDP MED endpoint device class.
PoE Device Type	Port PoE type, for example, powered. (Only POE model are supported.)
PoE Power Source	Port power source. (Only POE model are supported.)
PoE Power Priority	Port power priority. (Only POE model are supported.)
PoE Power Value	Port power value. (Only POE model are supported.)
Hardware Revision	Hardware version.
Firmware Revision	Firmware version.
Software	Software version.

Revision	
Serial Number	Device serial number.
Manufacturer Name	Device chipset IC manufacturer name.
Model Name	Device chipset IC model name.
Asset ID	Asset ID.

Location Information

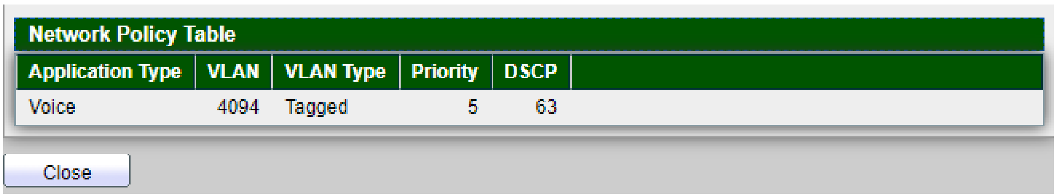


Location Information

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

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

Network Policy Table



Network Policy Table

Application Type	VLAN	VLAN Type	Priority	DSCP
Voice	4094	Tagged	5	63

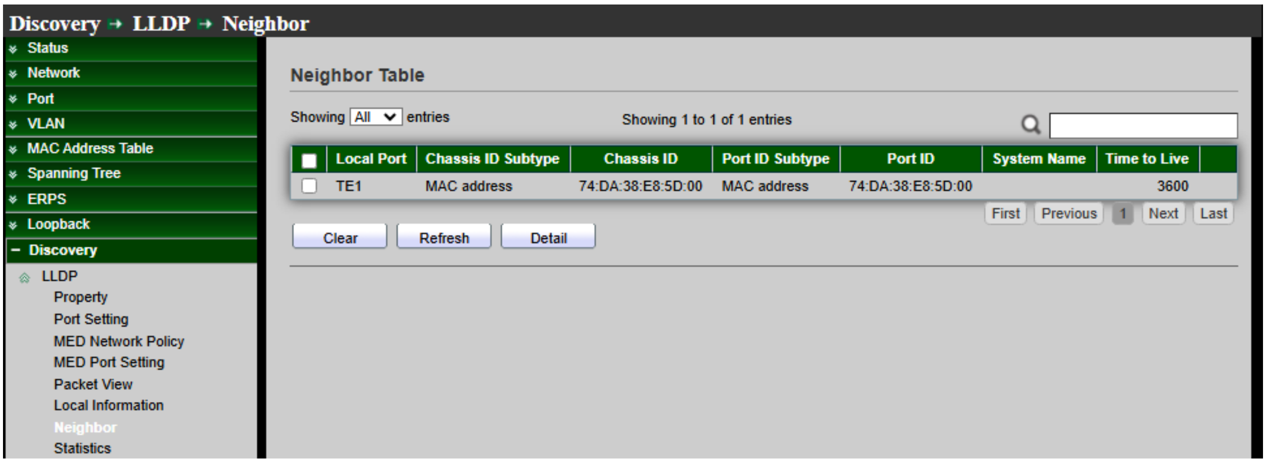
Field	Description
Application	Display the network policy application type. ● Voice ● Voice Signaling ● Guest Voice ● Guest Voice Signaling ● Softphone Voice ● Video Conferencing

	● App Streaming Video ● VideoSignaling
VLAN	Display the VLAN ID.
VLAN Type	VLAN tag status.**D**isplay the network policy application Traffic is tagged or Traffic is untagged type.
Priority	Display the L2 priority.
DSCP	Display the DSCP value.

*Click the **"Close"** button to close the information page.*

11.7 Neighbor

The page displays information that was received using the LLDP protocol from neighboring devices. After timeout the information is deleted. (Based on the value received from the neighbor time to Live TLV during which no LLDP PDU was received from a neighbor), Setting **"add"** and "Edit" and **"Delete"** function for this management.



Neighbor Table

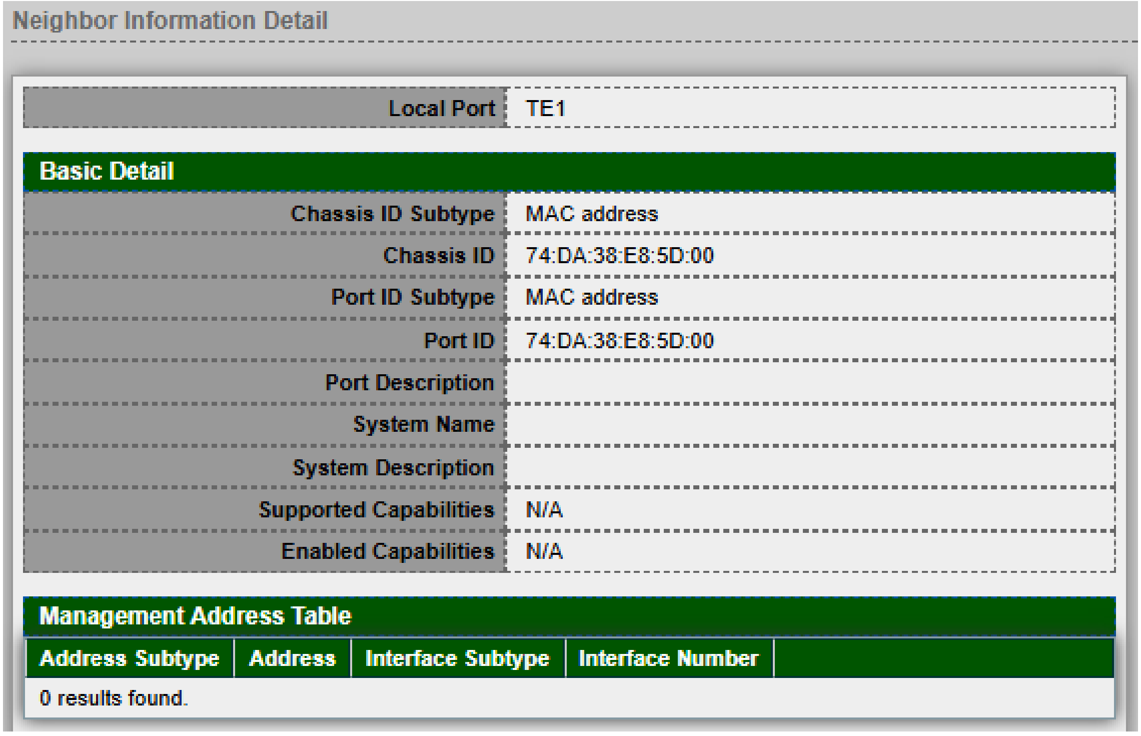
Showing All entries Showing 1 to 1 of 1 entries

□	Local Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	System Name	Time to Live
□	TE1	MAC address	74:DA:38:E8:5D:00	MAC address	74:DA:38:E8:5D:00		3600

Field	Description
Local Port	Number of the local port to which the neighbor is connected.
Chassis ID Subtype	Type of chassis ID (for example, MAC address).
Chassis ID	Identifier of the 802 LAN neighboring device's chassis.

Port ID Subtype	Type of the port identifier that is shown.
Port ID	Identifier of port.
System Name	Published name of the switch.
Time to Live	Time interval in seconds after which the information for this neighbor is deleted.

Click "detail" to view selected neighbor detail information.



Neighbor Information Detail

Local Port	TE1

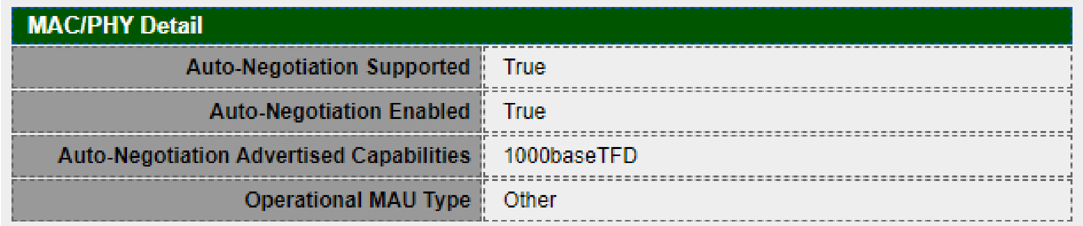
Basic Detail

Chassis ID Subtype	MAC address
Chassis ID	74:DA:38:E8:5D:00
Port ID Subtype	MAC address
Port ID	74:DA:38:E8:5D:00
Port Description	
System Name	
System Description	
Supported Capabilities	N/A
Enabled Capabilities	N/A

Management Address Table

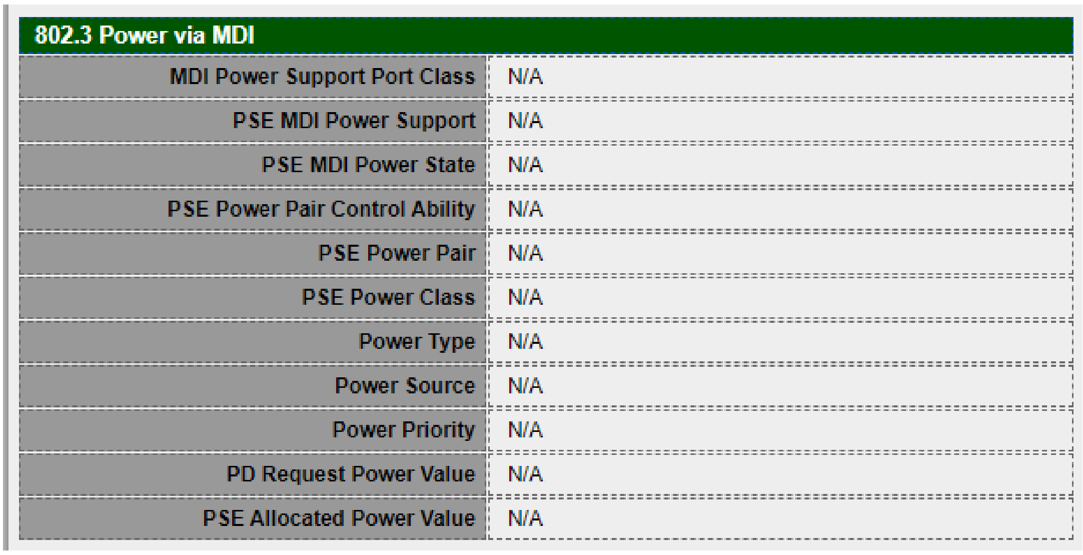
Address Subtype	Address	Interface Subtype	Interface Number

0 results found.

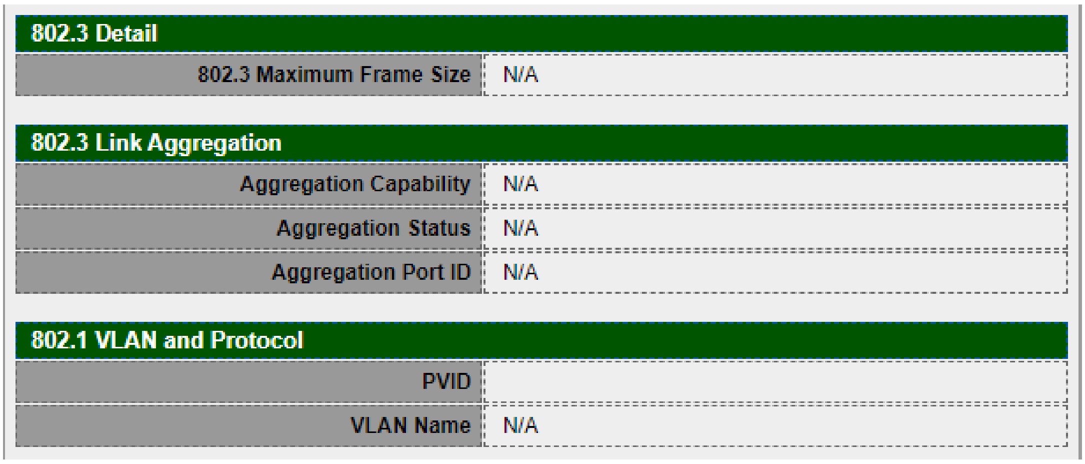


MAC/PHY Detail

Auto-Negotiation Supported	True
Auto-Negotiation Enabled	True
Auto-Negotiation Advertised Capabilities	1000baseTFD
Operational MAU Type	Other



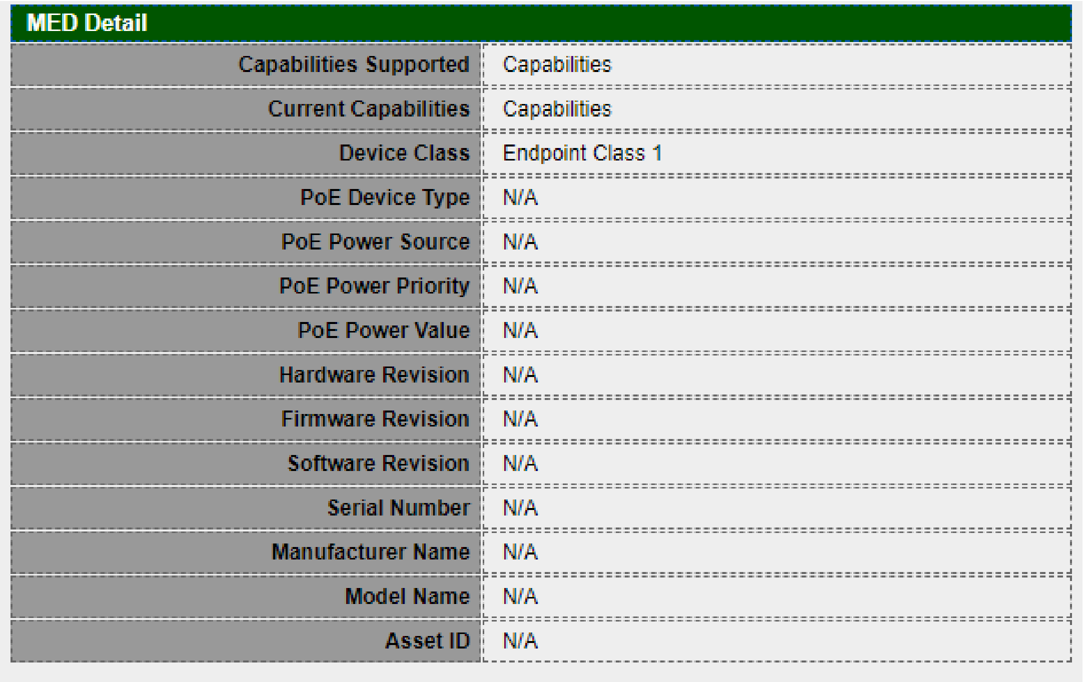
802.3 Power via MDI	
MDI Power Support Port Class	N/A
PSE MDI Power Support	N/A
PSE MDI Power State	N/A
PSE Power Pair Control Ability	N/A
PSE Power Pair	N/A
PSE Power Class	N/A
Power Type	N/A
Power Source	N/A
Power Priority	N/A
PD Request Power Value	N/A
PSE Allocated Power Value	N/A



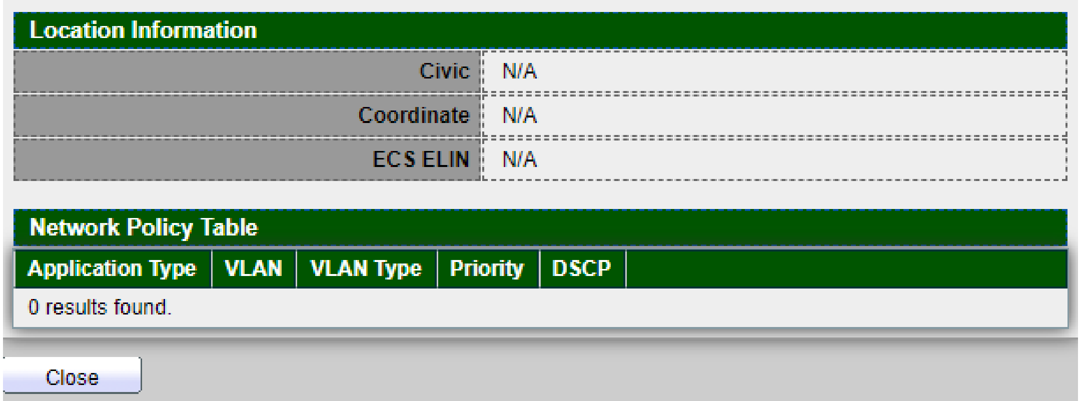
802.3 Detail	
802.3 Maximum Frame Size	N/A

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

802.1 VLAN and Protocol	
PVID	
VLAN Name	N/A



MED Detail	
Capabilities Supported	Capabilities
Current Capabilities	Capabilities
Device Class	Endpoint Class 1
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

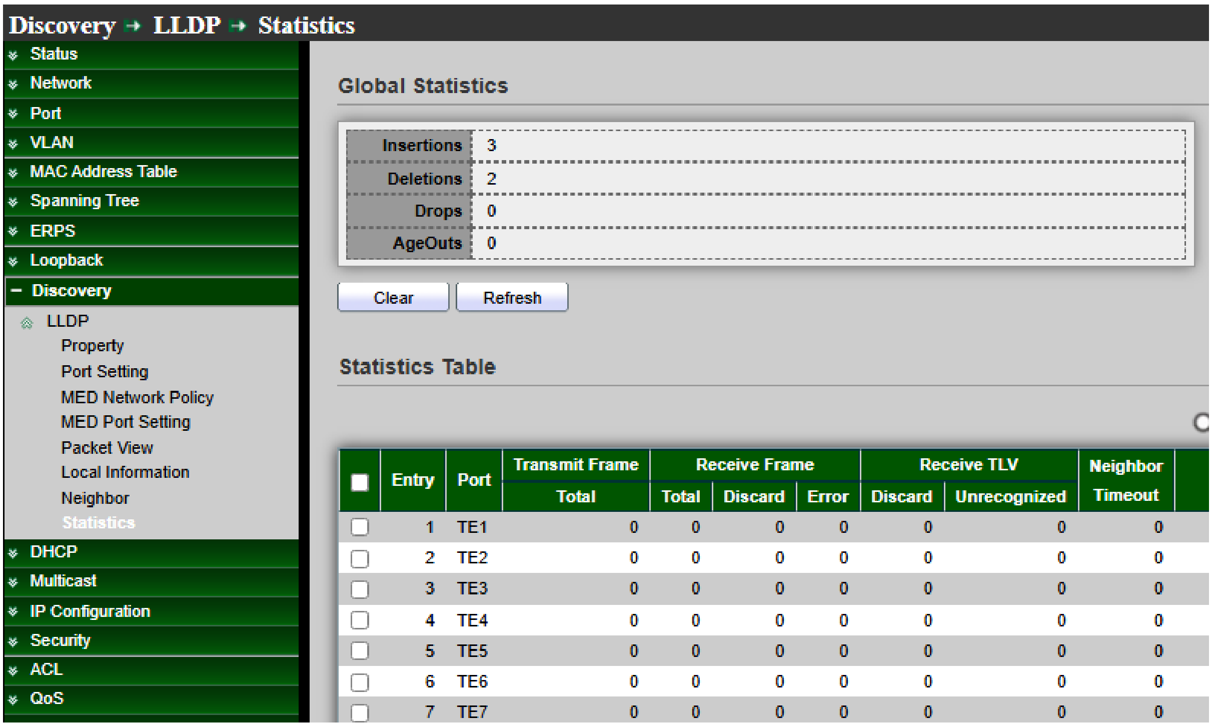
Network Policy Table

Application Type	VLAN	VLAN Type	Priority	DSCP
0 results found.				

Click the ***"Close"*** *button to close the information page.*

11.8 Statistics

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



Global Statistics

Insertions	3
Deletions	2
Drops	0
AgeOuts	0

Statistics Table

□	Entry	Port	Transmit Frame	Receive Frame			Receive TLV		Neighbor
			Total	Total	Discard	Error	Discard	Unrecognized	Timeout
□	1	TE1	0	0	0	0	0	0	0
□	2	TE2	0	0	0	0	0	0	0
□	3	TE3	0	0	0	0	0	0	0
□	4	TE4	0	0	0	0	0	0	0
□	5	TE5	0	0	0	0	0	0	0
□	6	TE6	0	0	0	0	0	0	0
□	7	TE7	0	0	0	0	0	0	0

Global 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.

*Click the **"Clear"** button to clear this page or click the **"Refresh"** button to refresh the page .*

Statistics Table

Field	Description
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 ● **Discarded:** Number of LLDP frames discarded for any reason by the LLDP agent on the corresponding port. ● **Errors:** Number of invalid LLDP frames received by the LLDP agent on the corresponding port, while the LLDP agent is enabled.
Receive TLV	● **Discarded:** Number of TLVs of LLDP frames discarded for any reason by the LLDP agent on the corresponding port. ● **Unrecognized:** Number of TLVs of LLDP frames that are unrecognied while the LLDP agent is enabled ● **Neighbor Timeout:** Number of TLVs of LLDP frames that are unrecognied while the LLDP agent is enabled
Neighbor Timeout	Number of age out LLDP frames.

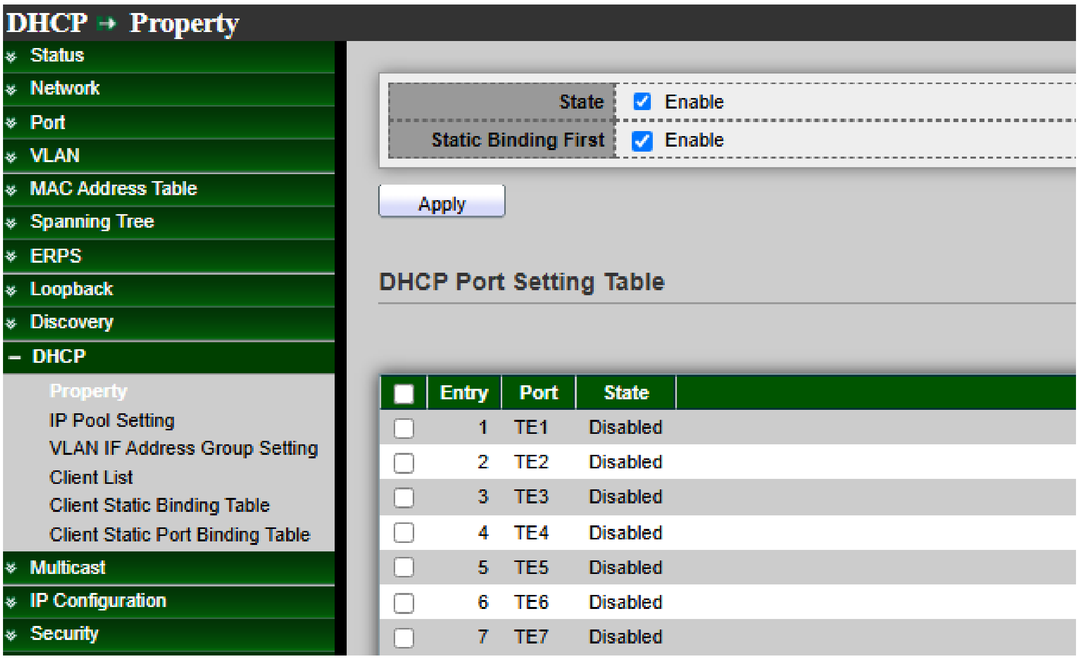
12. DHCP

The protocol operates on a client-server model. When DHCP clients connect to the network, they send broadcast queries to request the necessary information from the DHCP server. A DHCP server manages a pool of IP addresses and network configuration information. If they receive a query from a DHCP client, they will automatically be assigned an IP address and network parameters.

Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol. It is used in Internet Protocol (IP) networks to dynamically distribute network configuration parameters. For example, a device can request an IP address for an interface from a DHCP server. Using DHCP also reduces the need for network administrators or users to manually configure these settings.

12.1 Property

Administrator can configure this “DHCP port Setting Table “for Enable / Disable DHCP Server function.



State ☑ Enable
Static Binding First ☑ Enable

DHCP Port Setting Table

□	Entry	Port	State
□	1	TE1	Disabled
□	2	TE2	Disabled
□	3	TE3	Disabled
□	4	TE4	Disabled
□	5	TE5	Disabled
□	6	TE6	Disabled
□	7	TE7	Disabled

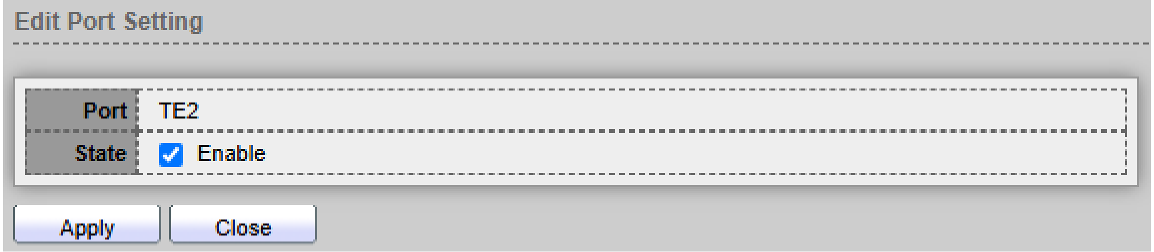
Use this section to enable the DHCP Server function on the switch. Also can select DHCP "Static Binding First" function to ticking “enable” for your configuration.

*Click the **“Apply”** button to save your changes settings.*

Field	Description
Port	Display the DHCP of port entry.
State	Show the DHCP Enable or DHCP Display Status.

Edit Port Setting :

You can select the port form GE1 - GE28 (Ports) and LAG1~LAG8 (Groups) to be set, and click "Edit" to edit DHCP port   to ticking “enable” for your configuration.



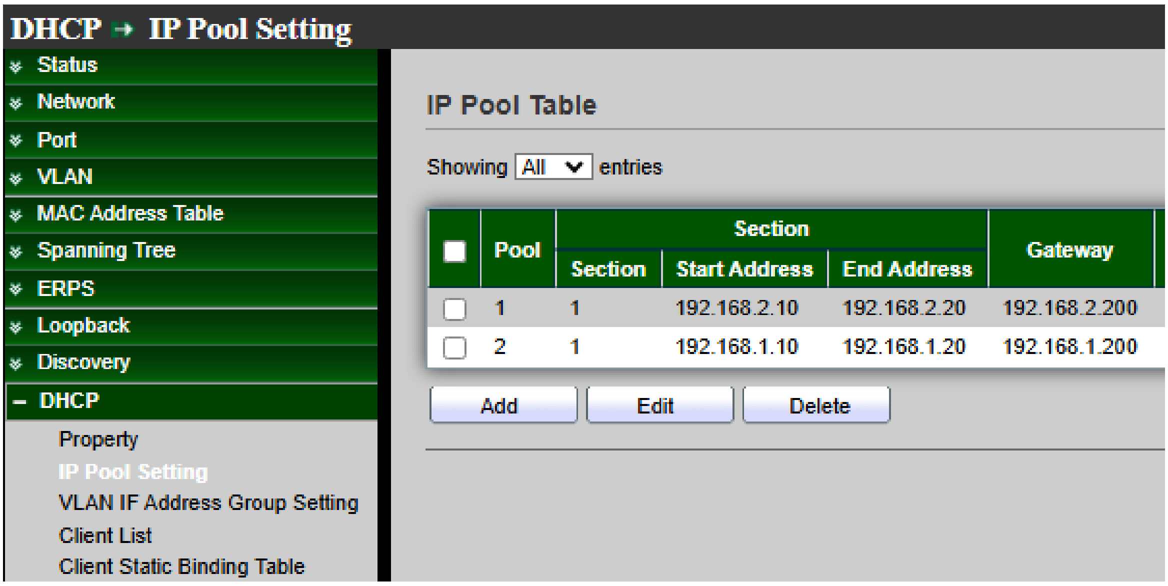
Edit Port Setting

Port	TE2
State	☑ Enable

*Click the **“Apply”** button to save your changes or **“Close”** the button to close settings.*

12.2 IP Pool Setting

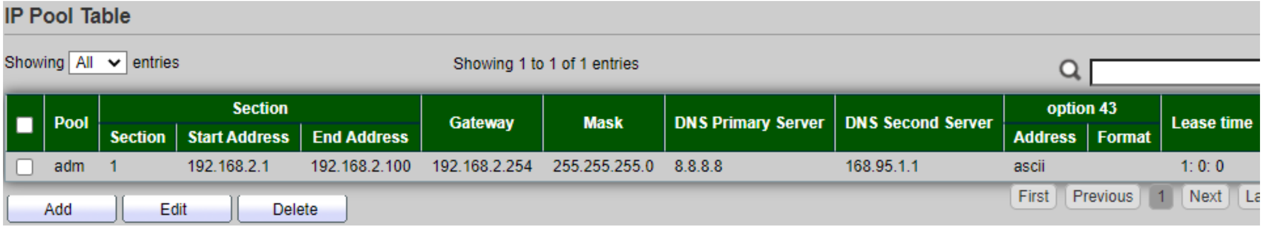
Administrator can configure this IP Pool Table Setting **“add”** and “Edit” and **“Delete”** function management.



IP Pool Table

Showing All entries

□	Pool	Section			Gateway
		Section	Start Address	End Address	
□	1	1	192.168.2.10	192.168.2.20	192.168.2.200
□	2	1	192.168.1.10	192.168.1.20	192.168.1.200

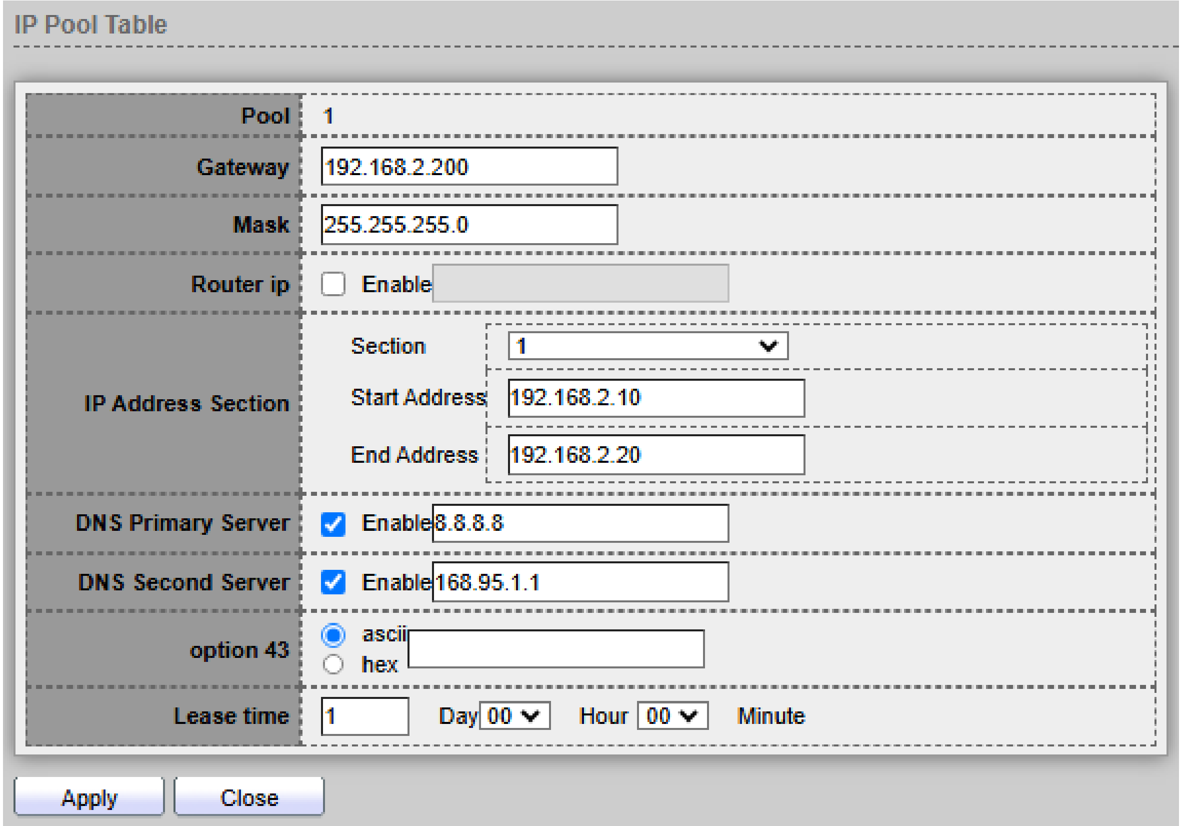


IP Pool Table

Showing All entries   Showing 1 to 1 of 1 entries

□	Pool	Section			Gateway	Mask	DNS Primary Server	DNS Second Server	option 43		Lease time
		Section	Start Address	End Address					Address	Format	
□	adm	1	192.168.2.1	192.168.2.100	192.168.2.254	255.255.255.0	8.8.8.8	168.95.1.1	ascii		1: 0: 0

Field	Description
Pool	Display the Pool Name.
Section	• **Section :** Section entry. • **Start Address :** Displays the starting IP address of the IP address pool configured for this DHCP server instance. • **End Address :** Displays the last IP address of the IP address pool configured for this DHCP server instance.
Gateway	Displays the default gateway value sent to clients from this DHCP server instance.
Mask	Displays the subnet mask value sent to clients from this DHCP server instance.
DNS Primary Server	Displays the primary DNS server value sent to clients from this DHCP server instance.
DNS Second Server	Displays the secondary DNS server value sent to clients from this DHCP server instance.
Option43	• **Address :** Displays of option 43 address. • **Format :** Displays of option 43 format type.
Lease time	This field displays the amount of time that the IP address is valid.



IP Pool Table

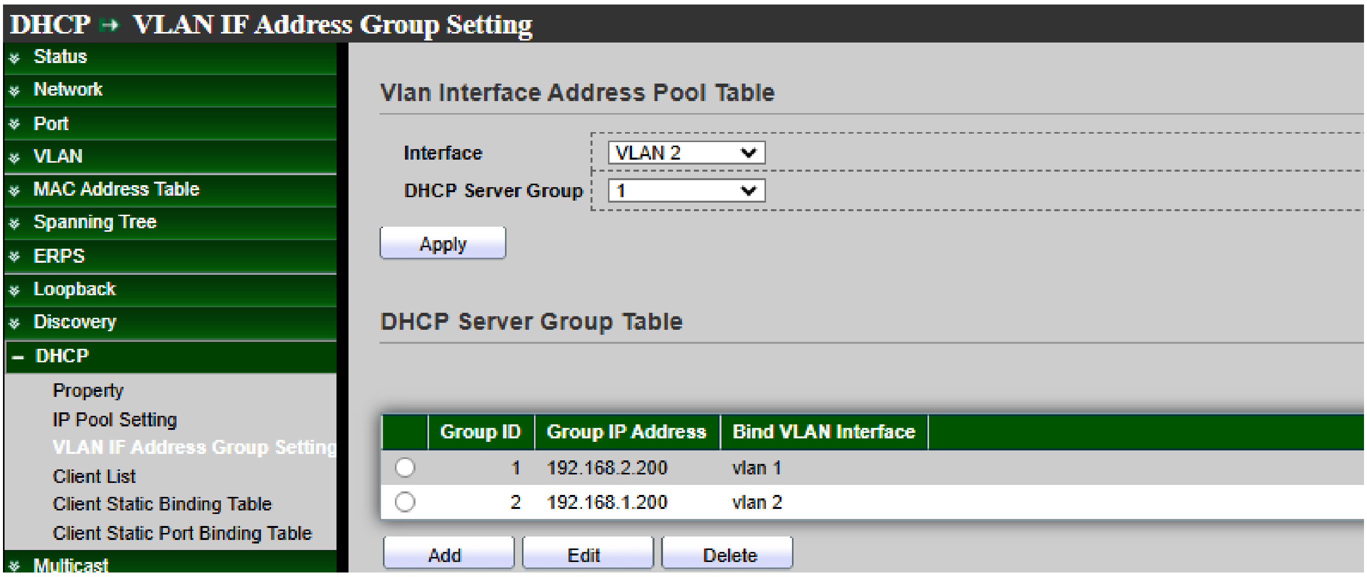
Pool	1
Gateway	192.168.2.200
Mask	255.255.255.0
Router ip	□ Enable
IP Address Section	Section: 1 Start Address: 192.168.2.10 End Address: 192.168.2.20
DNS Primary Server	☑ Enable 8.8.8.8
DNS Second Server	☑ Enable 168.95.1.1
option 43	● ascii ○ hex
Lease time	1 Day 00 Hour 00 Minute

- **Pool :** Select Add New Pool and enter a name for the DHCP Pool.
- **Gateway :** Enter the IP address of the gateway, which is the host on the LAN that relays all traffic coming into and going out of the LAN.
- **Mask :** Assign the subnet mask of IP address.
- **Router ip :** Select to specify another routing gateway address for the DHCP client.
- **IP Address Section :**
  - **Section :** Select the Section number.
  - **Start Address :** Enter the starting point for the DHCP server to assign IP address for the device connected.
  - **End Address :** Enter the ending point for the DHCP server to assign IP address for the device connected.
- **DNS Primary Server :** Select “enable“ and fill in the for your primary DNS IP address.
- **DNS Second Server :** Select “enable“ and fill in the for your second DNS IP address.
- **Option 43 :** Configure option 43 character string with “ASCII” format and configure option 43 character string with “HEX” format in IP DHCP pool mode.
- **Lease time :** A controllable time period that DHCP server will reclaim IP addresses,Set the time value if set time is selected as Day / Hour / Minute.

*Click the **“Apply”** button to save your changes or **“Close”** the button to close settings.*

12.3 VLAN IF Address Group Setting

Administrator can configure select the drop down list of "VLAN Interface" and ""DHCP server group " in the VLAN interface address pool table.



DHCP ➔ VLAN IF Address Group Setting

Vlan Interface Address Pool Table

Interface: VLAN 2

DHCP Server Group: 1

DHCP Server Group Table

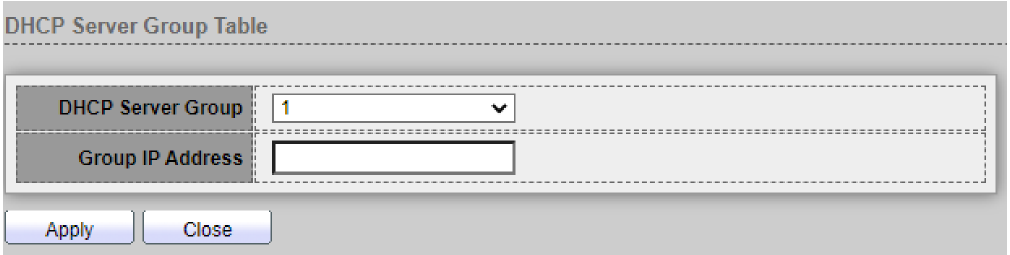
	Group ID	Group IP Address	Bind VLAN Interface
○	1	192.168.2.200	vlan 1
○	2	192.168.1.200	vlan 2

- ➢ **Interface :** Select a VLAN interface.
- ➢ **DHCP Sever Group :** Select a DHCP Sever Group.

*Click the **"Apply"** button to save your changes settings.*

Administrator can configure this "DHCP Server Group Table "page setting for **"add"** and **"Edit"** and **"Delete"** function management.

Field	Description
Group ID	Displays the DHCP Server Group ID
Group IP Address	Displays the DHCP Server Group IP Address
Bind VLAN Interface	Displays the DHCP Server Bind VLAN Interface



DHCP Server Group Table

DHCP Server Group: 1

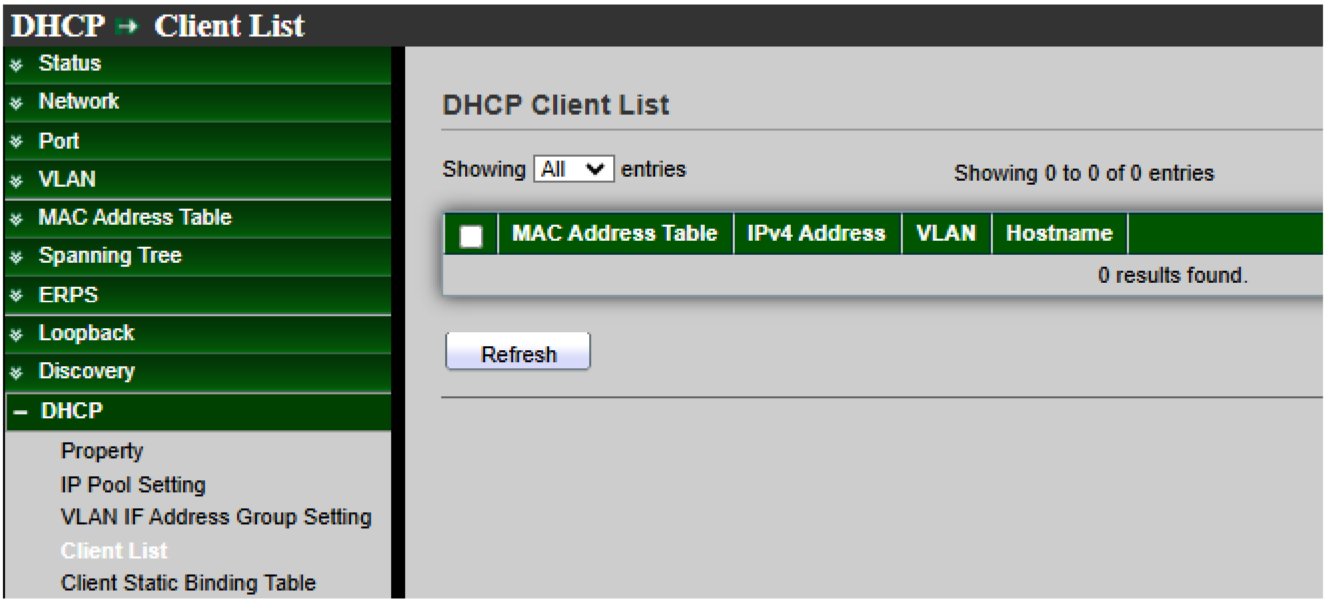
Group IP Address:

- **DHCP Server Group :** Administrator can be select **"DHCP Server Group"** in the drop-down box, and then confirm the grouping function to be set.
- **Group IP Address :** Administrator can fill in Group IP address.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

12.4 Client List

This page can displayed DHCP Client List show" MAC Address Table" and show "IPv4 Address" and show "VLAN" and show "Hostname" information .



DHCP Client List

Showing All entries Showing 0 to 0 of 0 entries

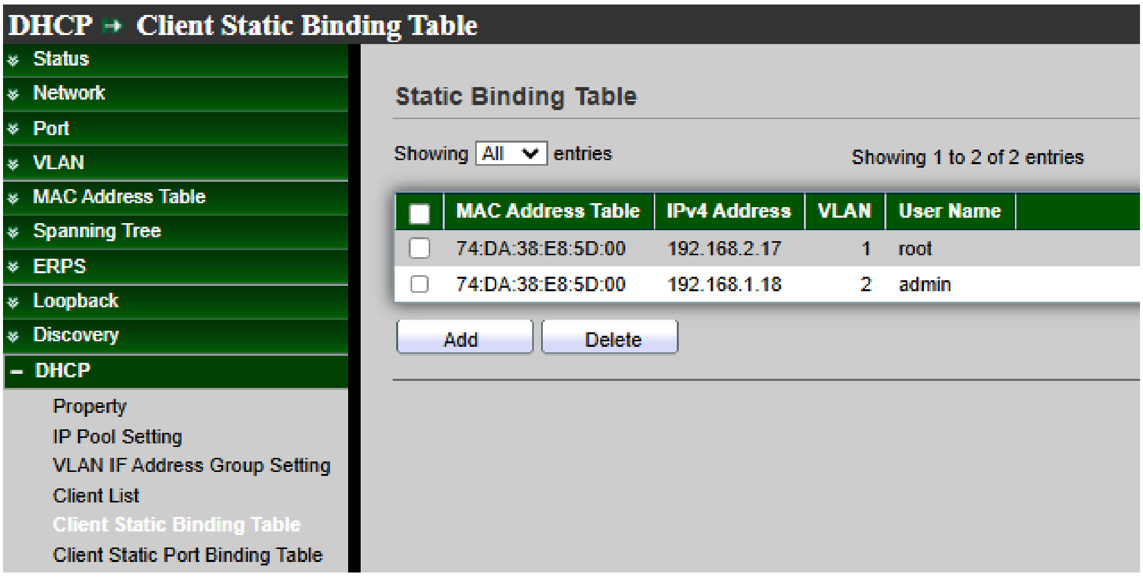
□	MAC Address Table	IPv4 Address	VLAN	Hostname
0 results found.				

Field	Description
MAC Address Table	Display the MAC address of the client device.
IPv4 Address	Display the IP address sent to the client device.
VLAN	Display the VLAN ID of the DHCP client.
Hostname	Displays the hostname of the DHCP client.

*Click **"Refresh"** to refresh the "Client List" statistics .*

12.5 Client Static Binding Table

Administrator can configure this "Static Binding Table "setting for **"add"** and **"Delete"** function management. And this page can displayed "Static Binding Table " show" MAC Address Table" and show "IPv4 Address" and show "VLAN" and show "User Name" information .

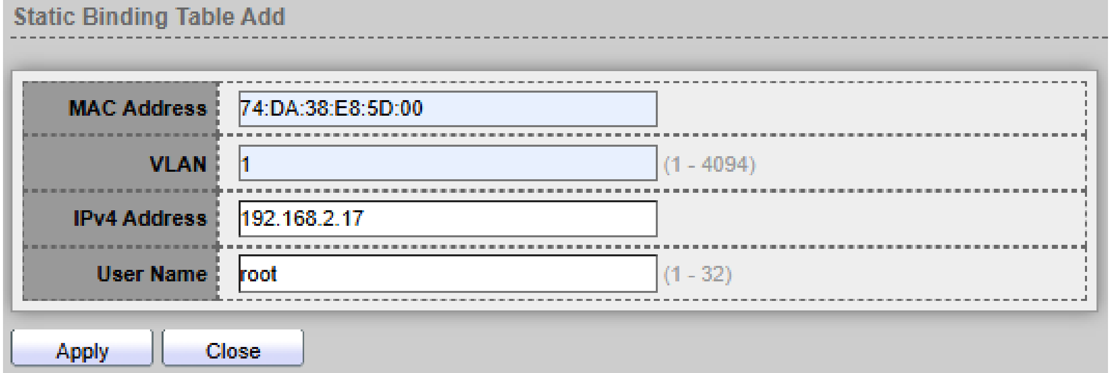

DHCP → Client Static Binding Table
Status
Network
Port
VLAN
MAC Address Table
Spanning Tree
ERPS
Loopback
Discovery
DHCP
Property
IP Pool Setting
VLAN IF Address Group Setting
Client List
Client Static Binding Table
Client Static Port Binding Table
Add
Delete

Static Binding Table

Showing All entries Showing 1 to 2 of 2 entries

□	MAC Address Table	IPv4 Address	VLAN	User Name
□	74:DA:38:E8:5D:00	192.168.2.17	1	root
□	74:DA:38:E8:5D:00	192.168.1.18	2	admin

Field	Description
MAC Address Table	Display the MAC address of the client device.
IPv4 Address	Display the IP address sent to the client device.
VLAN	Display the VLAN ID of the DHCP client.
Users Name	Displays the Users Name of the DHCP client.



Static Binding Table Add

MAC Address	74:DA:38:E8:5D:00	
VLAN	1	(1 - 4094)
IPv4 Address	192.168.2.17	
User Name	root	(1 - 32)

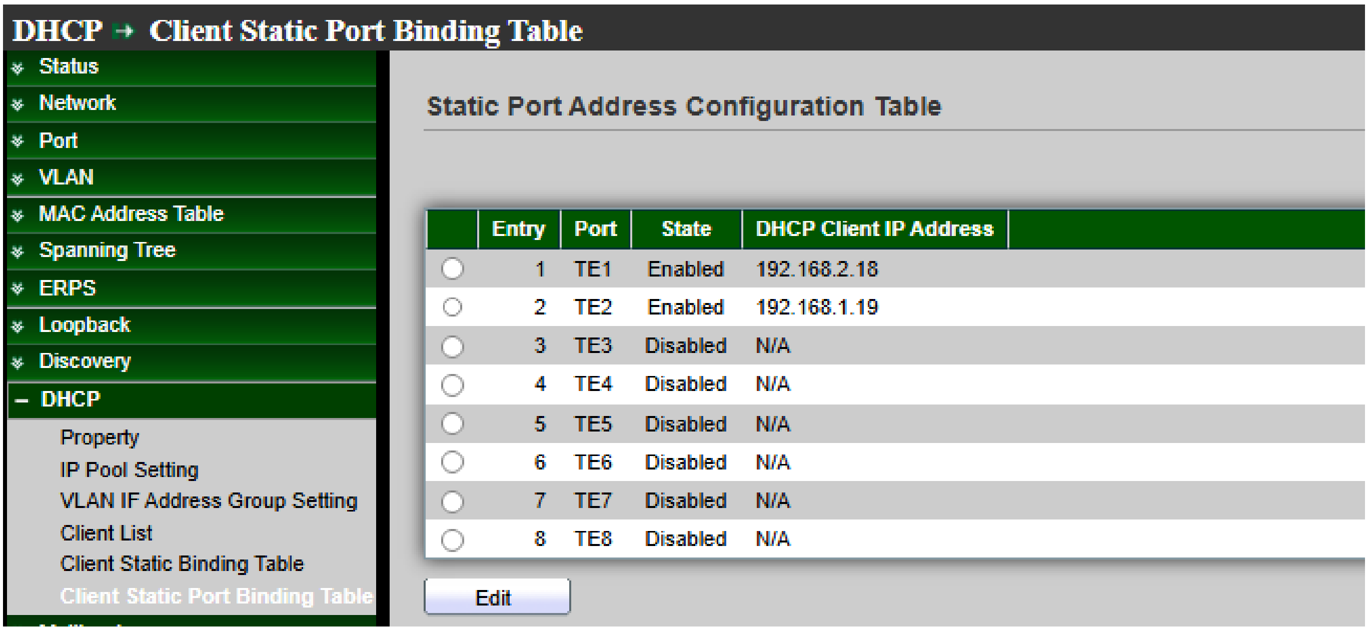
- **MAC Address :** The MAC address of the device that wishes binding.

- **VLAN :** Administrator can be configuration the DHCP VLAN ID.
- **IPv4 Address :** The IP address that will assign to the device with Binding MAC address.
- **User Name :** Generates a username for this binding rule.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

12.6 Client Static Port Binding Table

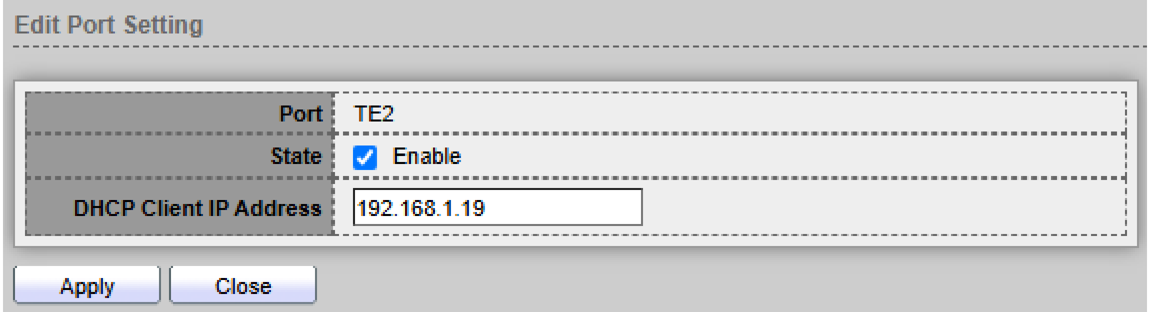
Administrator can configure this "Static Port Address Configuration Table "setting for **"Edit"** function management. And this page can displayed " Entry" ,"Port" ,"State" and "DHCP Client IP Address" information .


DHCP → Client Static Port Binding Table
Status
Network
Port
VLAN
MAC Address Table
Spanning Tree
ERPS
Loopback
Discovery
– DHCP
Property
IP Pool Setting
VLAN IF Address Group Setting
Client List
Client Static Binding Table
Client Static Port Binding Table
Edit

Static Port Address Configuration Table

	Entry	Port	State	DHCP Client IP Address
○	1	TE1	Enabled	192.168.2.18
○	2	TE2	Enabled	192.168.1.19
○	3	TE3	Disabled	N/A
○	4	TE4	Disabled	N/A
○	5	TE5	Disabled	N/A
○	6	TE6	Disabled	N/A
○	7	TE7	Disabled	N/A
○	8	TE8	Disabled	N/A

Field	Description
Entry	Display the number of entry
Port	Display the number of port
State	Display the enabled state of DHCP static port binding
DHCP Client IP Address	Display the IP address of DHCP static port binding



Edit Port Setting

Port	TE2
State	☑ Enable
DHCP Client IP Address	192.168.1.19

- **Port :** Select static binding port.
- **State :** Select whether to enable the DHCP static binding function of the port.
- **DHCP Client IP Address :** Set the DHCP client IP address for the static binding port.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

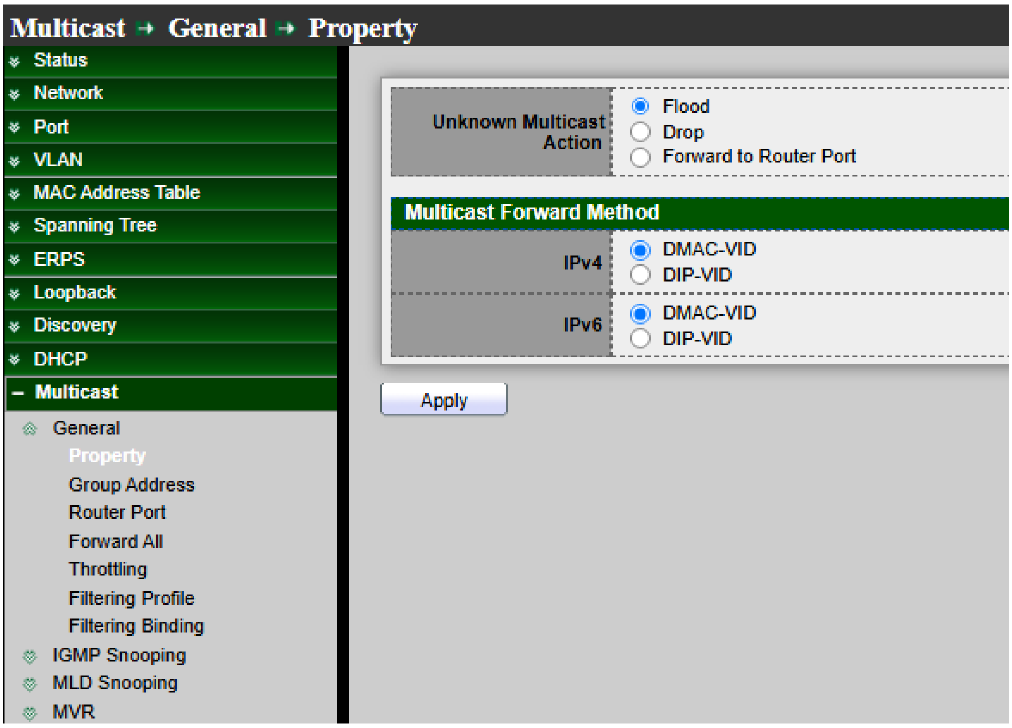
13. Multicast

Multicast is the only type of IPv4 multicast that is supported by the Ethernet gateway.

13.1 General

13.1.1 Property

This page can be configured with unknown multicast action, administrator can set the forwarding method is based on the DMAC or the DIP, the function implements high performance data transfer from point to multipoint in network will be reduce the loading on the network.



Multicast → General → Property

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

Multicast Forward Method

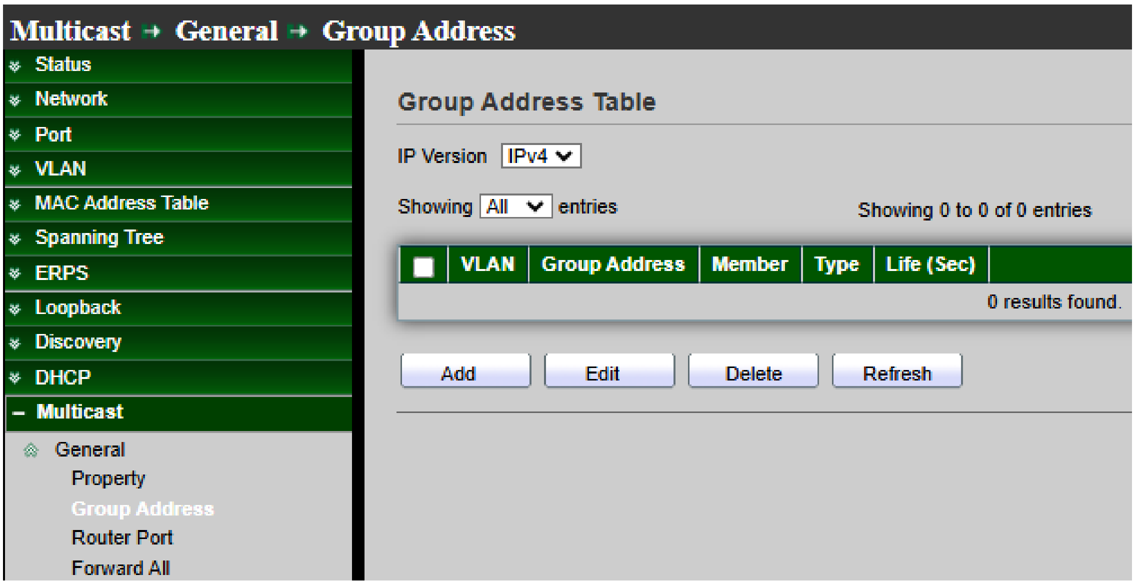
IPv4	● DMAC-VID ○ DIP-VID
IPv6	● DMAC-VID ○ DIP-VID

- **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.
- **Multicast Forward Method :** Assign the subnet mask of IP address.
- **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).

*Click the **"Apply"** button to save your changes settings.*

13.1.2 Group Address

The multicast address range is 224.0.0.0 to 239.255.255.255 and forms the Class D range which is made up of the high order bits 1110 followed by the 28 bit multicast group ID. There is no subletting with these Class D addresses. A multicast group can have a permanently-assigned address or the group may be Transient. Setting **"add"** and **"Edit"** and **"Delete"** and **"Refresh"** function for this management.



Group Address Table

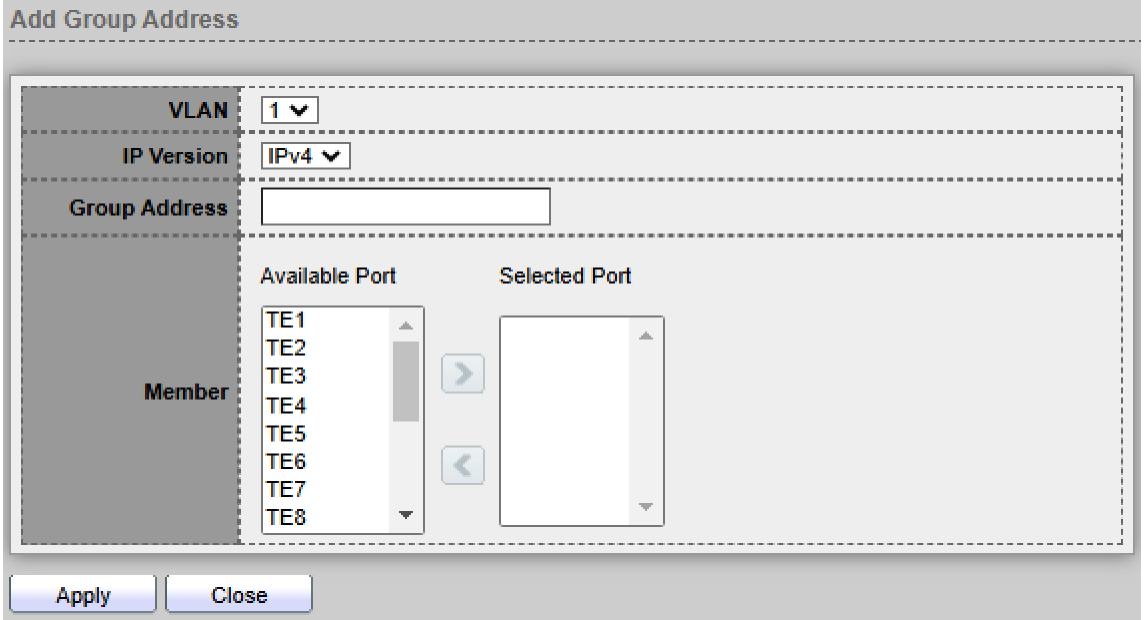
IP Version: IPv4

Showing All entries — Showing 0 to 0 of 0 entries

□	VLAN	Group Address	Member	Type	Life (Sec)
					0 results found.

- **IPV4 Version :** Select the IP Version.
  - **IPv4 :** ipv4 multicast group.
  - **IPv6 :** ipv6 multicast group.

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



Add Group Address

VLAN: 1

IP Version: IPv4

Group Address:

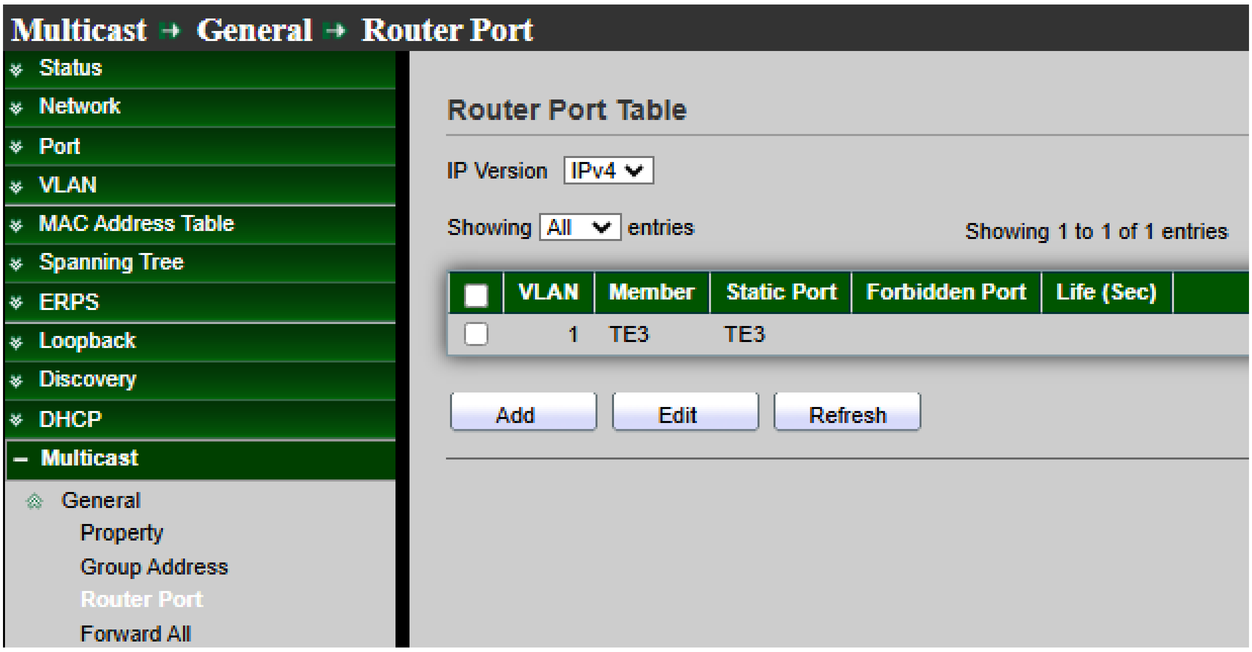
Member: Available Port: TE1, TE2, TE3, TE4, TE5, TE6, TE7, TE8 / Selected Port:

- **VLAN :** The VLAN ID of group.
- **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.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

13.1.3 Router Port

A Multicast Router (MRouter) port is a port that connects to a Multicast router. The switch includes the MRouter port(s) when it forwards Multicast streams and IGMP/ MLD registration messages. It is required in order for all Router(s) can, in turn; forward the Multicast streams and propagate the registration messages to other subnets, Setting **“add”** and **“Edit”** and **“Delete”** function for this management.



Router Port Table

IP Version IPv4

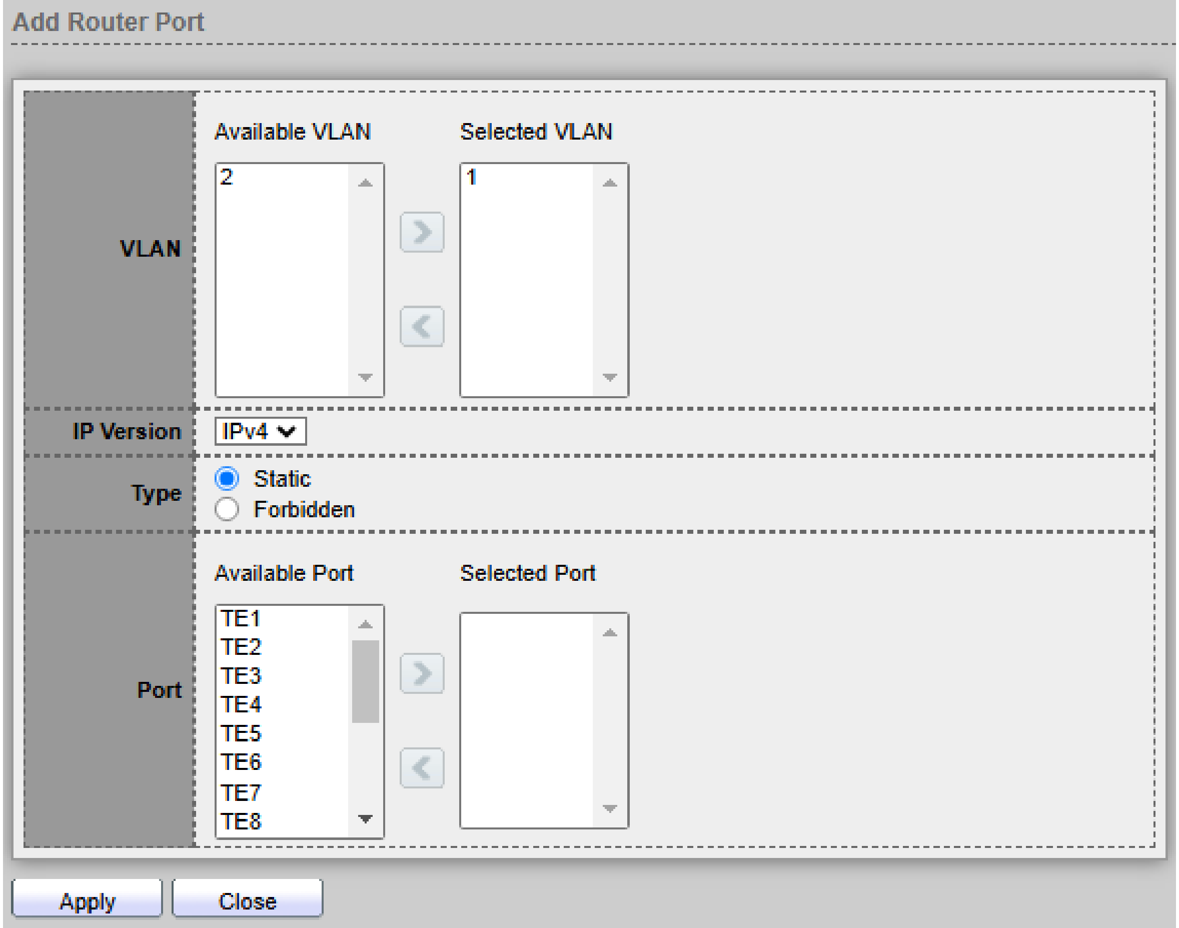
Showing All entries

Showing 1 to 1 of 1 entries

□	VLAN	Member	Static Port	Forbidden Port	Life (Sec)
□	1	TE3	TE3		

- **IPV4 Version :** Select the IP Version.
  - **IPv4 :** ipv4 multicast router.
  - **IPv6 :** ipv6 multicast router.

Field	Description
VLAN	The VLAN ID router entry.
Member	Router Port member (include 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.



Add Router Port

VLAN: Available VLAN: 2; Selected VLAN: 1

IP Version: IPv4

Type: ● Static ○ Forbidden

Port: Available Port: TE1, TE2, TE3, TE4, TE5, TE6, TE7, TE8; Selected Port:

- **VLAN :** The VLAN ID of group.
  - **Available VLAN:** Optional VLAN member.
  - **Selected VLAN**: Selected VLAN member.
- **IP Version :**
  - **IPv4 :** IPv4 multicast router.
  - **IPv6 :** IPv6 multicast router.

Type : The router port type:

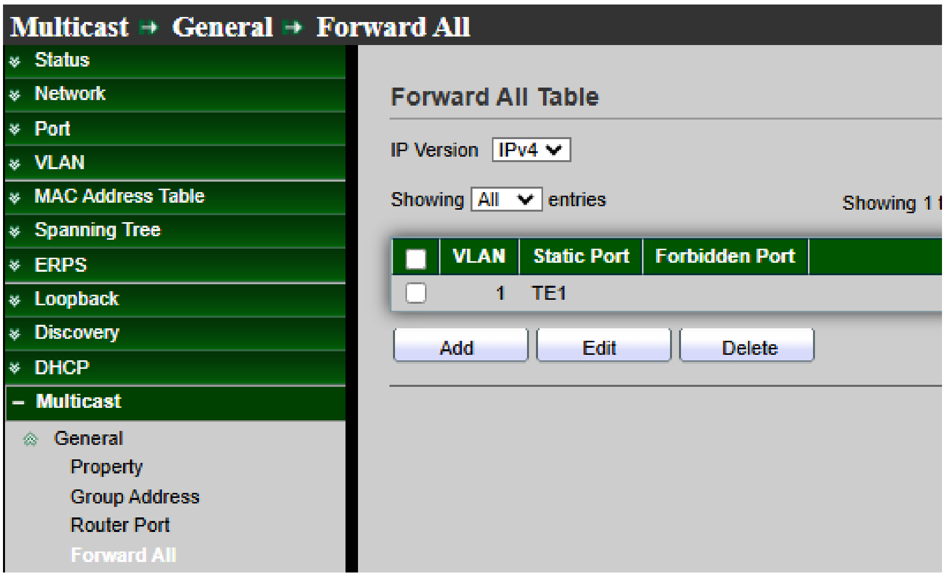
  - **Static :** Static router port.
  - **Forbidden :** forbidden router port, can’t learn dynamic router port member.
- **Port :** The member ports of Router entry.
  - **Available Port:** Optional router port member.
  - **Selected Port**: Selected router port member.

*Click the **“Apply”** button to save your changes or **“Close”** the button to close settings.*

13.1.4 Forward All

Configure ports or LAGs to receive Multicast streams from a specific VLAN. Administrator can statically configure a port to Forward All if the devices connecting to the port do not support IGMP or MLD, Setting **"add"** and **"Edit"** and **"Delete"** function for this management.

Note	The configuration affects only the ports that are members of the selected VLAN.



Forward All Table

IP Version IPv4

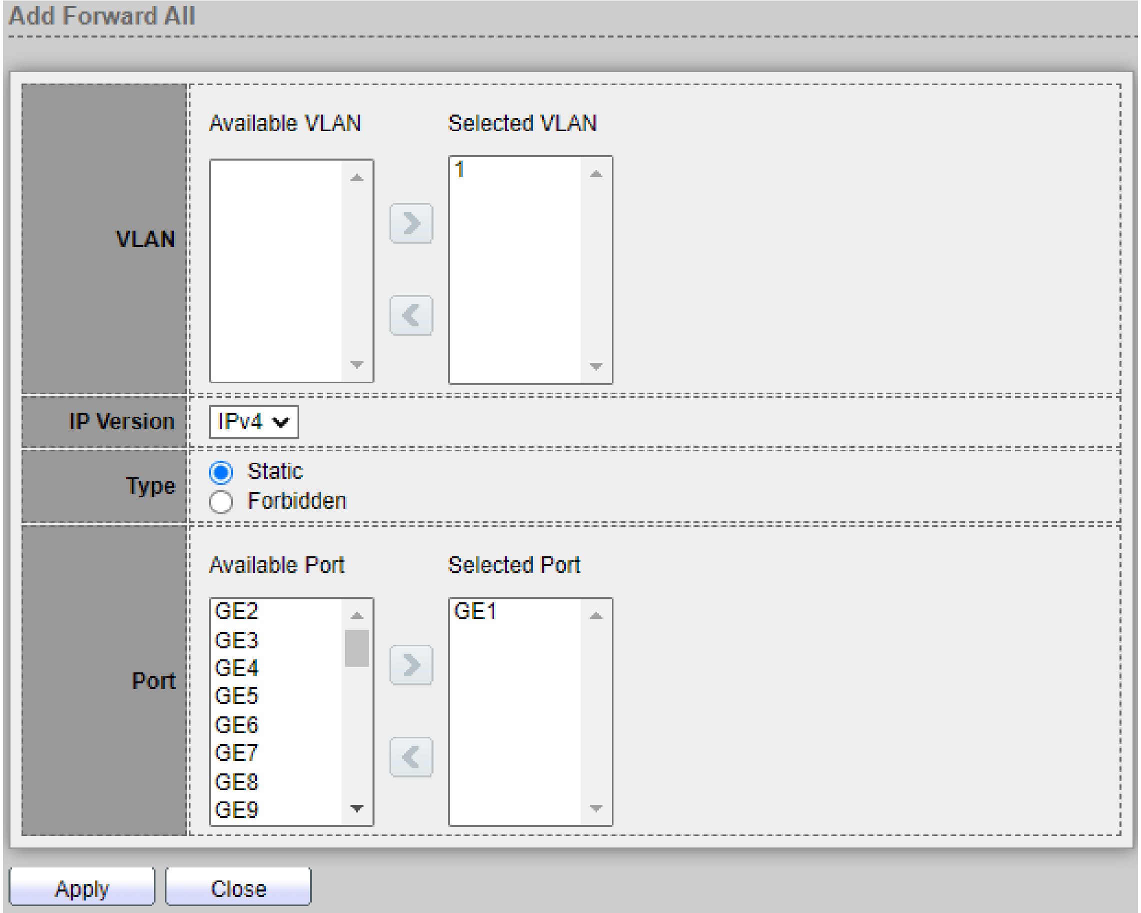
Showing All entries

Showing 1

□	VLAN	Static Port	Forbidden Port
□	1	TE1	

- **IPV4 Version :** Select the IP Version.
  - **IPv4 :** IPv4 multicast forward all.
  - **IPv6 :** IPv6 multicast forward all.

Field	Description
VLAN	VLAN ID of forward all entry
Static Port	Known multicast group always forward port member
Forbidden Port	Known multicast group always not forward port member



Add Forward All

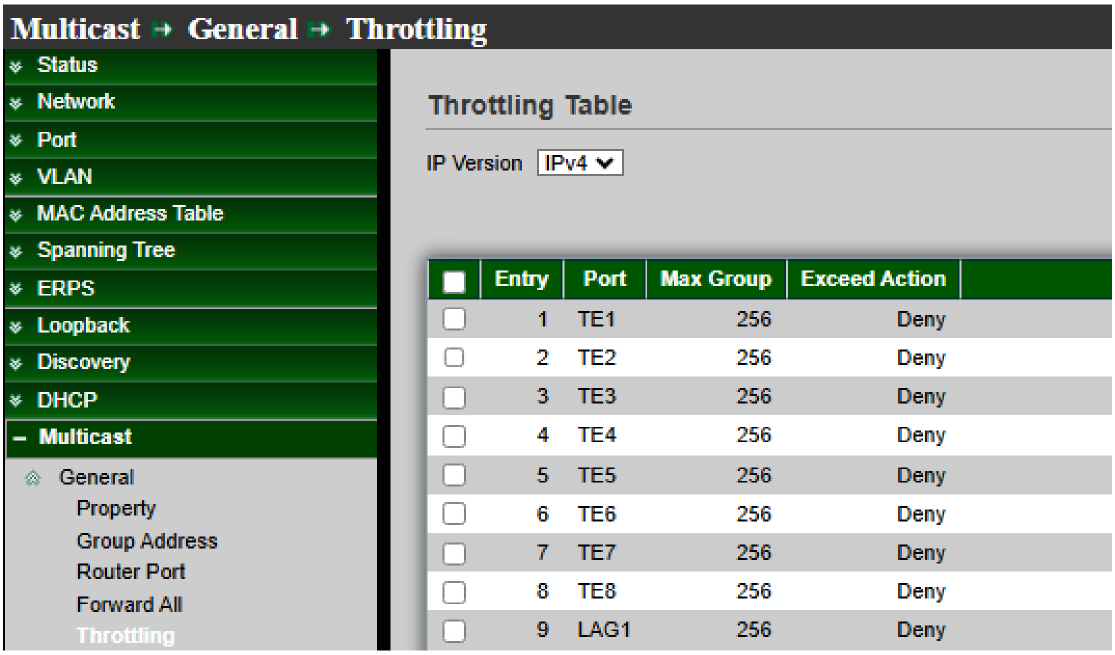
VLAN	Available VLAN: (empty) Selected VLAN: 1
IP Version	IPv4
Type	● Static ○ Forbidden
Port	Available Port: GE2, GE3, GE4, GE5, GE6, GE7, GE8, GE9 Selected Port: GE1

- **VLAN :** The VLAN ID of forward all entry.
  - **Available VLAN:** Optional VLAN member.
  - **Selected VLAN**: Selected VLAN member.
- **IP Version :**
  - **IPv4 :** IPv4 multicast forward all.
  - **IPv6 :** IPv6 multicast forward all.
- **Type :** The forward all port type
  - **Static :** Static forward all port. The port is statically configured as a Multicast router port.
  - **Forbidden :** Forbidden forward all port. This port is not to be configured as a Multicast Router port, even if IGMP or MLD queries are received on this port.
- **Port :** The member ports of forward all.
  - **Available Port:** Optional router port member.
  - **Selected Port**: Selected router port member.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

13.1.5 Throttling

This page allow user to configure port can learned max group number and if port group number arrived max group number action.



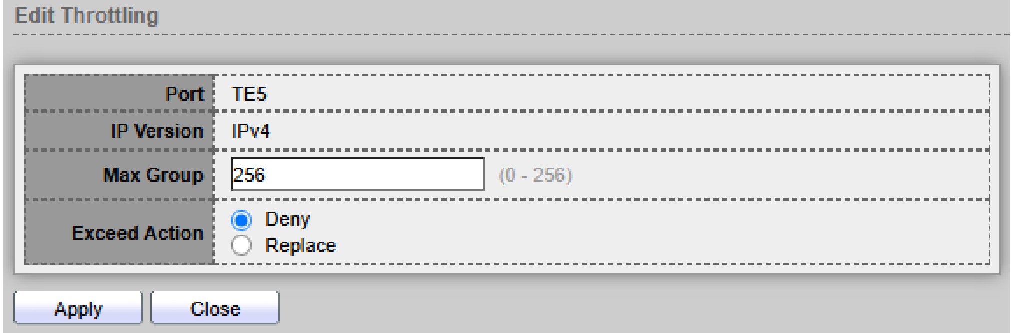
Throttling Table

IP Version IPv4

□	Entry	Port	Max Group	Exceed Action
□	1	TE1	256	Deny
□	2	TE2	256	Deny
□	3	TE3	256	Deny
□	4	TE4	256	Deny
□	5	TE5	256	Deny
□	6	TE6	256	Deny
□	7	TE7	256	Deny
□	8	TE8	256	Deny
□	9	LAG1	256	Deny

- **IPV4 Version :** Select the IP Version.
  - **IPv4 :** IPv4 for IGMP snooping throttling.
  - **IPv6 :** IPv6 for MLD snooping throttling.

Field	Description
Port	Display the Port Name
Max Group	Display the Max number of group for port
Exceed Action	Display the port exceed max number group learning group action



Edit Throttling

Port	TE5
IP Version	IPv4
Max Group	256 (0 - 256)
Exceed Action	● Deny ○ Replace

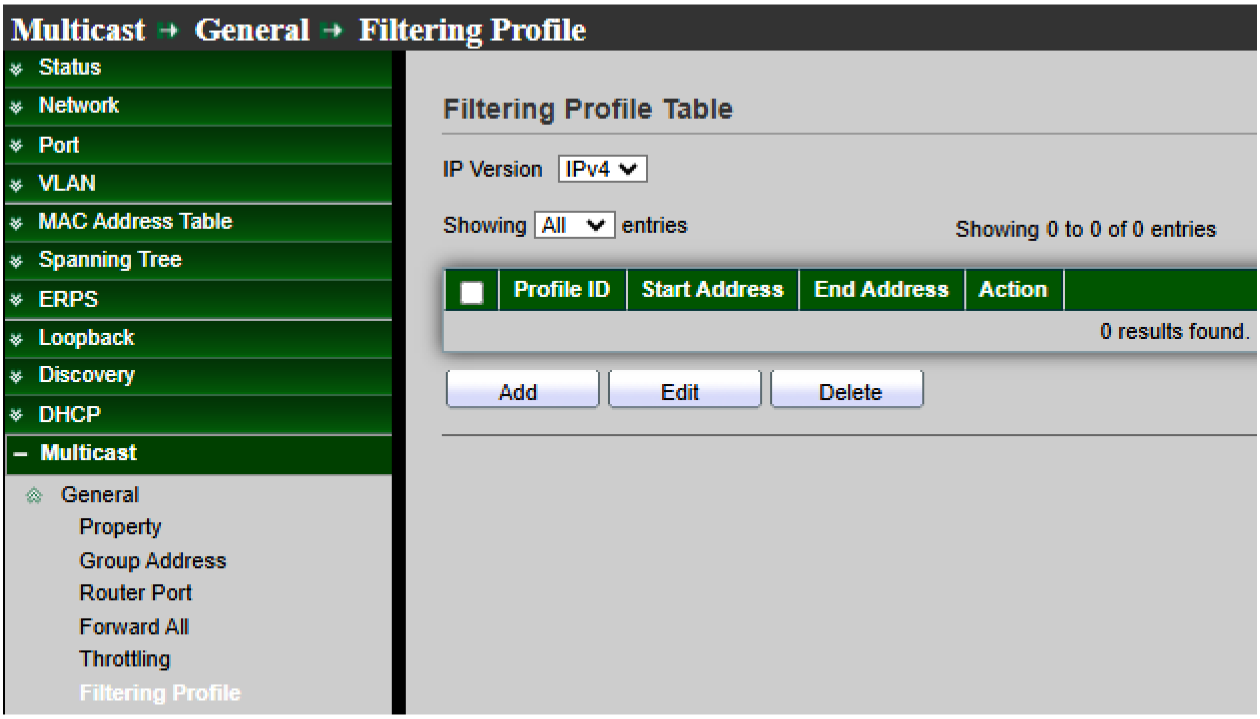
- **Port :** Display the selected port list.
- **IP Version :** Display the selected IP version

- **Max Group :** Max number of group for port
- **Exceed Action :** Excess Max number of port learning group action.
  - **Deny:** do not learning group.
  - **Replace:** random replace one exist group.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

13.1.6 Filtering Profile

Filter profile permits or denies a range of Multicast groups to be learned when the join group matches the filter profile IP group range, Setting **"add"** and **"Edit"** and **"Delete"** function for this management.



IP Version IPv4

Showing All entries   Showing 0 to 0 of 0 entries

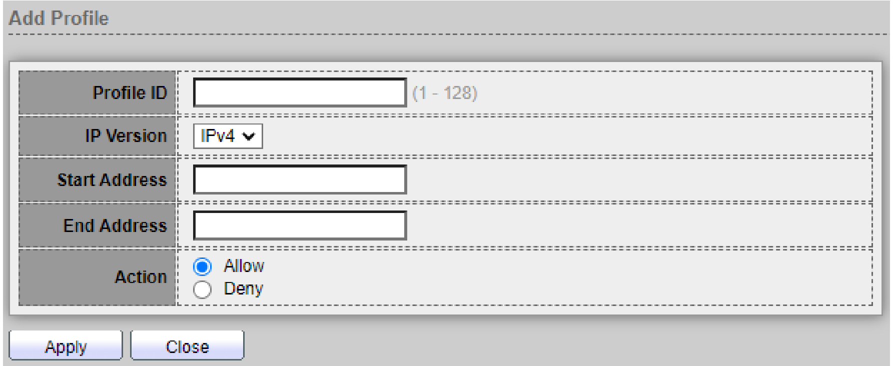
□	Profile ID	Start Address	End Address	Action

0 results found.

- **IPV4 Version :** Select the IP Version.
  - **IPv4 :** IPv4 for IGMP snooping profile.
  - **IPv6 :** IPv6 for MLD snooping profile.

Field	Description
Profile ID	Display profile ID
Start Address	The start group address of profile
End Address	The end group address of profile

Action	Display profile action



Add Profile

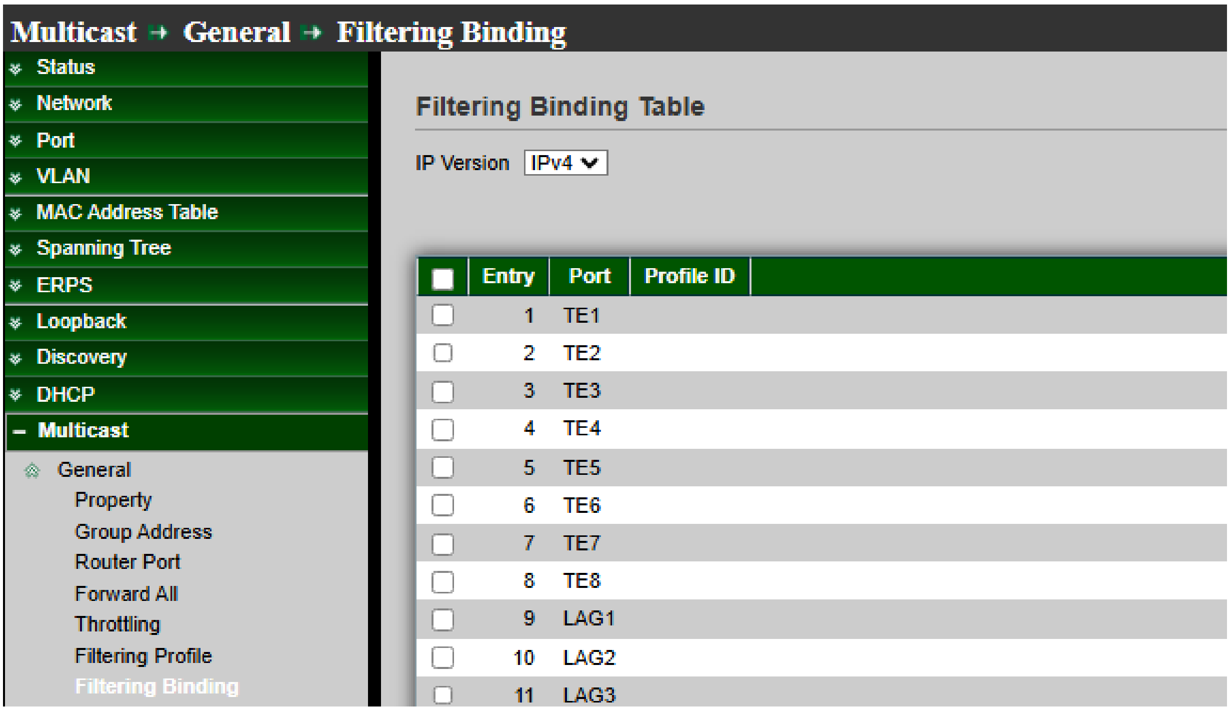
Profile ID	(1 - 128)
IP Version	IPv4
Start Address	
End Address	
Action	● Allow ○ Deny

- **Profile ID: Profile ID**.
- **IP Version :** Display the selected IP version
  - **IPv4:** IGMP snooping profile.
  - **IPv6:** MLD snooping profile.
- **Start Address:** The start group address of profile.
- **End Address :** The end group address of profile.
- **Action:** The action of profile:
  - **Allow:** permit all packets that match the profile.
  - **Deny:** deny all packets that match the profile.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

13.1.7 Filtering Binding

When the setting is completed of Filtering Profile, administrator can select ports to set filtering binding.



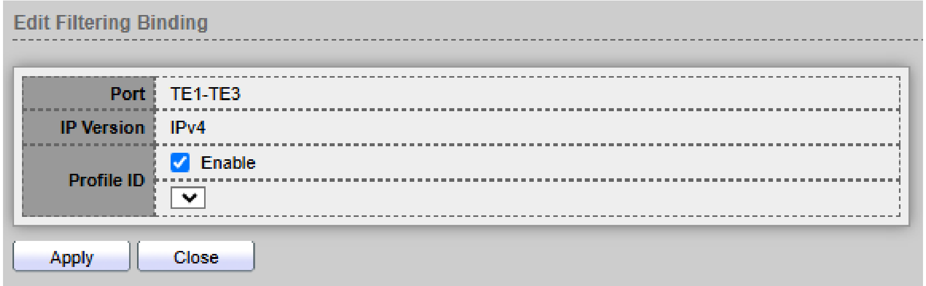
Filtering Binding Table

IP Version: IPv4

□	Entry	Port	Profile ID
□	1	TE1	
□	2	TE2	
□	3	TE3	
□	4	TE4	
□	5	TE5	
□	6	TE6	
□	7	TE7	
□	8	TE8	
□	9	LAG1	
□	10	LAG2	
□	11	LAG3	

- **IPV4 Version :** Select the IP Version.
  - **IPv4 :** IPv4 for IGMP snooping throttling.
  - **IPv6 :** IPv6 for MLD snooping throttling.

Field	Description
Entry	Entry of number
Port	Port Name
Profile ID	Port binding Profile ID


Edit Filtering Binding

Port	TE1-TE3
IP Version	IPv4
Profile ID	☑ Enable

- **Port:** Selected Port List.
- **IP Version :** Display Selected Port filtering IP version.
- **Profile ID:** If check Enable, can select or change profile ID, Else it will delete port filter profile *binding.*

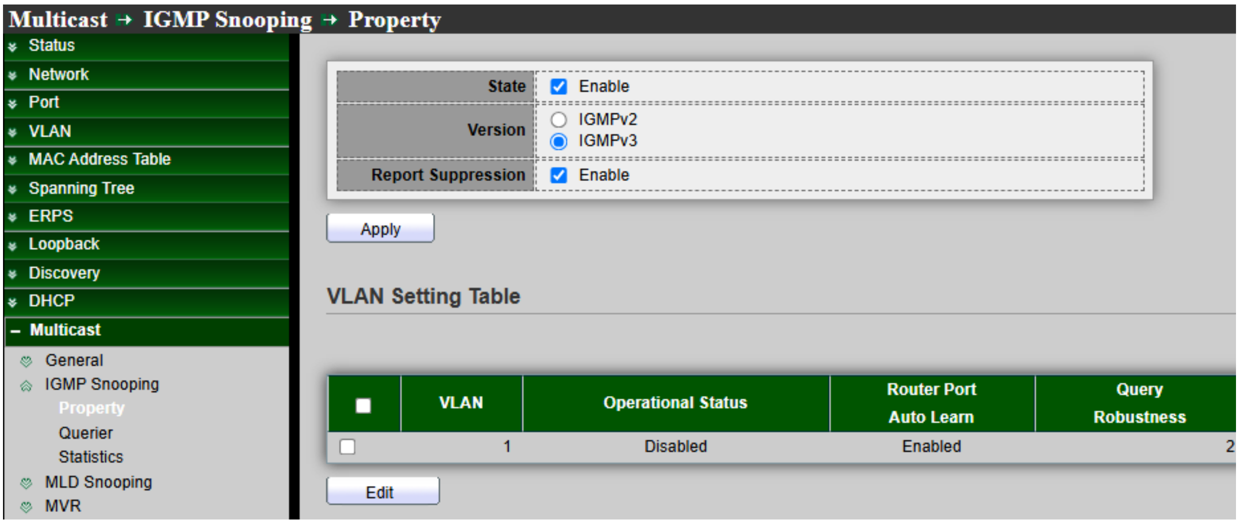
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

13.2 IGMP Snooping

IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic. The IGMP snooping support v2 & v3, administrator can forward or drop Unknown Multicast.

13.2.1 Property

When IGMP Snooping is enabled globally or on a VLAN, all IGMP packets are forwarded to the CPU. The CPU analyzes select of ports are asking to join Multicast groups on VLAN or routers that are generating IGMP queries, or receiving PIM / OSFP / DVMRP / IGMP query protocols incoming packets.



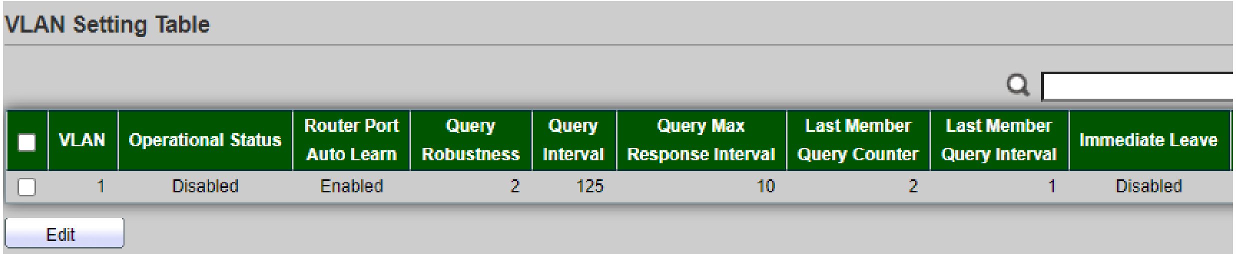
State: ☑ Enable
Version: ○ IGMPv2 ● IGMPv3
Report Suppression: ☑ Enable

VLAN Setting Table

□	VLAN	Operational Status	Router Port Auto Learn	Query Robustness
□	1	Disabled	Enabled	2

- **State:** Administrator can select Enable or Un-enable, Set the enabling status of IGMP Snooping functionality.
  - **Enable:** If Checked Enable IGMP Snooping, else is Disabled IGMP Snooping.
- **Version:** Select either IGMPv2 or IGMPv3,Set the igmp snooping version.
  - **IGMPv2:** Only support process igmp v2 packet.
  - **IGMPv3:** Support v3 basic and v2.
- **Report Suppression:** Enable or disable IGMP report suppression. If administrator select disabling this feature will forward all IGMP reports to Multicast routers, Set the enabling status of IGMP v2 report suppression.
  - **Enable:** If Checked Enable IGMP Snooping v2 report suppression, else Disable the report suppression function.

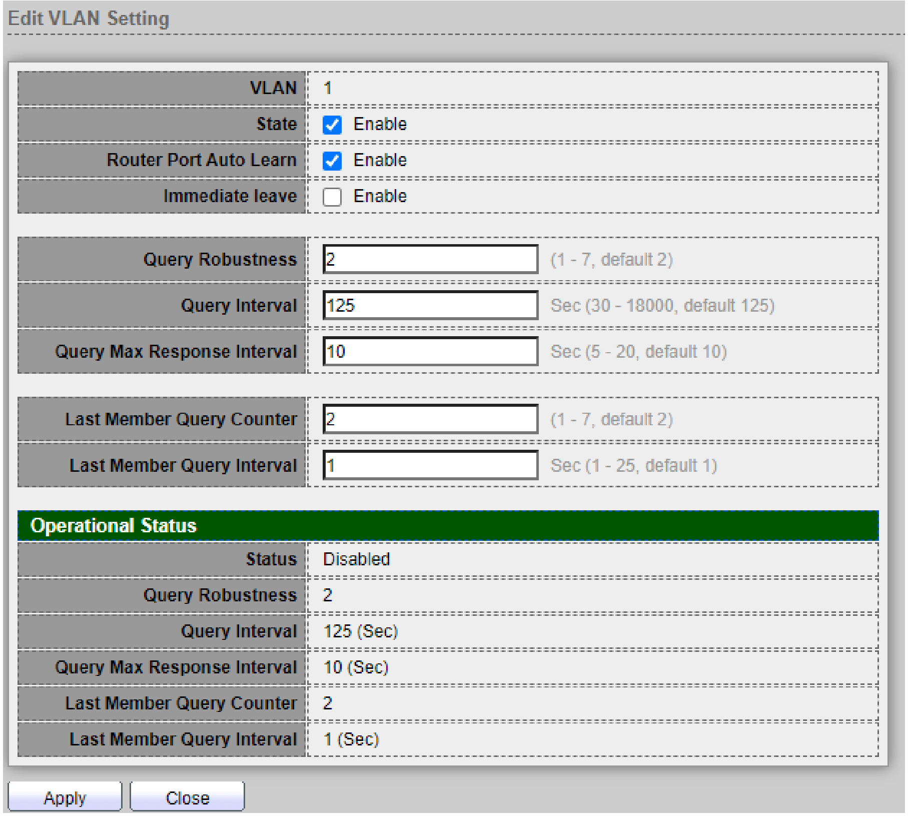
*Click the **"Apply"** button to save your changes.*



VLAN Setting Table

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

Field	Description
VLAN	The IGMP entry VLAN ID
Operation Status	The enable status of IGMP snooping VLAN functionality
Router Port Auto Learn	The enabling status of IGMP snooping router port auto learning
Query Robustness	The Query Robustness allows tuning for the expected packet loss on a subnet.
Query Interval	The interval of querier to send general query
Query Max Response Interval	In Membership Query Messages, it specifies the maximum allowed time before sending a responding report in units of 1/10 second.
Last Member Query count	The count that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Last Member Query Interval	The interval that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Immediate leave	The immediate leave status of the group will immediate leave when receive IGMP Leave message.



Edit VLAN Setting

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

Operational Status

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

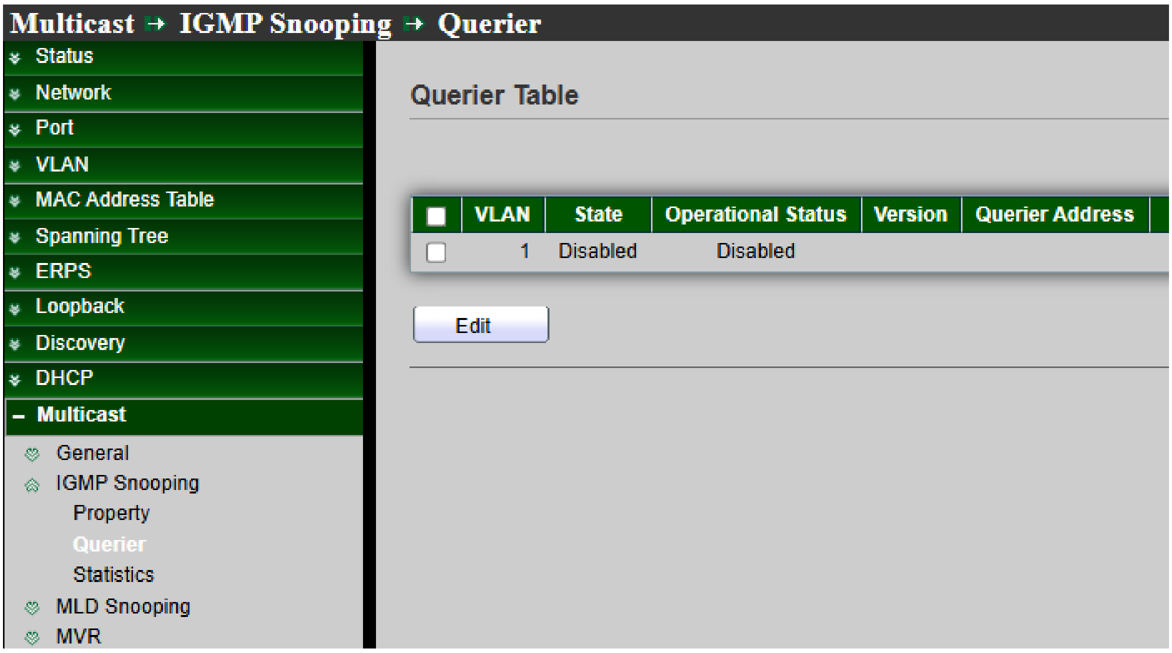
- **VLAN:** The VLAN ID of IGMP Snooping.
- **State:** Set the enabling status of IGMP Snooping VLAN functionality.
  - **Enable: Enable:** If Checked Enable IGMP Snooping VLAN, else is Disabled IGMP Snooping VLAN.
- **Router Port Auto Learn:** Set the enabling status of IGMP Snooping router port learning.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

- **Operational Status:** Set the enabling status of IGMP Snooping router port learning.
  - **Status:** Operational IGMP snooping status， must both IGMP snooping global and IGMP snooping enable the status will be enable.
  - **Query Robustness:** Operational Query Robustness.
  - **Query Interval:** Operational Query Interval.
  - **Query Max Response Interval:** Operational Query Max Response Interval.
  - **Last Member Query Counter:** Operational Last Member Query Count.
  - **Last Member Query Interval:** Operational Last Member Query Interval.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

13.2.2 Querier

Administrator can choose created VLAN to enable or disable the IGMP Snooping query function. When select checkbox and click "**Edit**" button will be go to set IGMP Snooping version, this function can get IGMP Snooping query device regularly to VLAN local segments in all hosts and routers send IGMP Snooping general query packets, to the query segment which multicast group members.

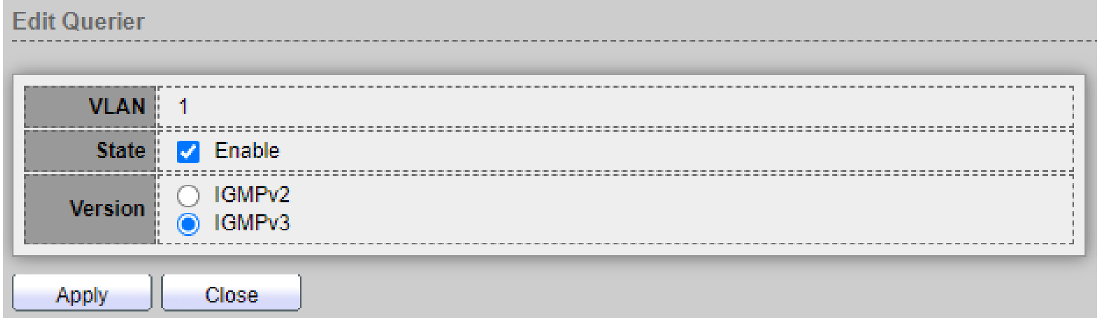


Querier Table

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

Field	Description
VLAN	IGMP Snooping querier entry VLAN ID
State	The IGMP Snooping querier Admin State.

Operational Status	The IGMP Snooping querier operational status
Querier Version	The IGMP Snooping querier operational version.
Querier IP	The operational Querier IP address on the VLAN


Edit Querier

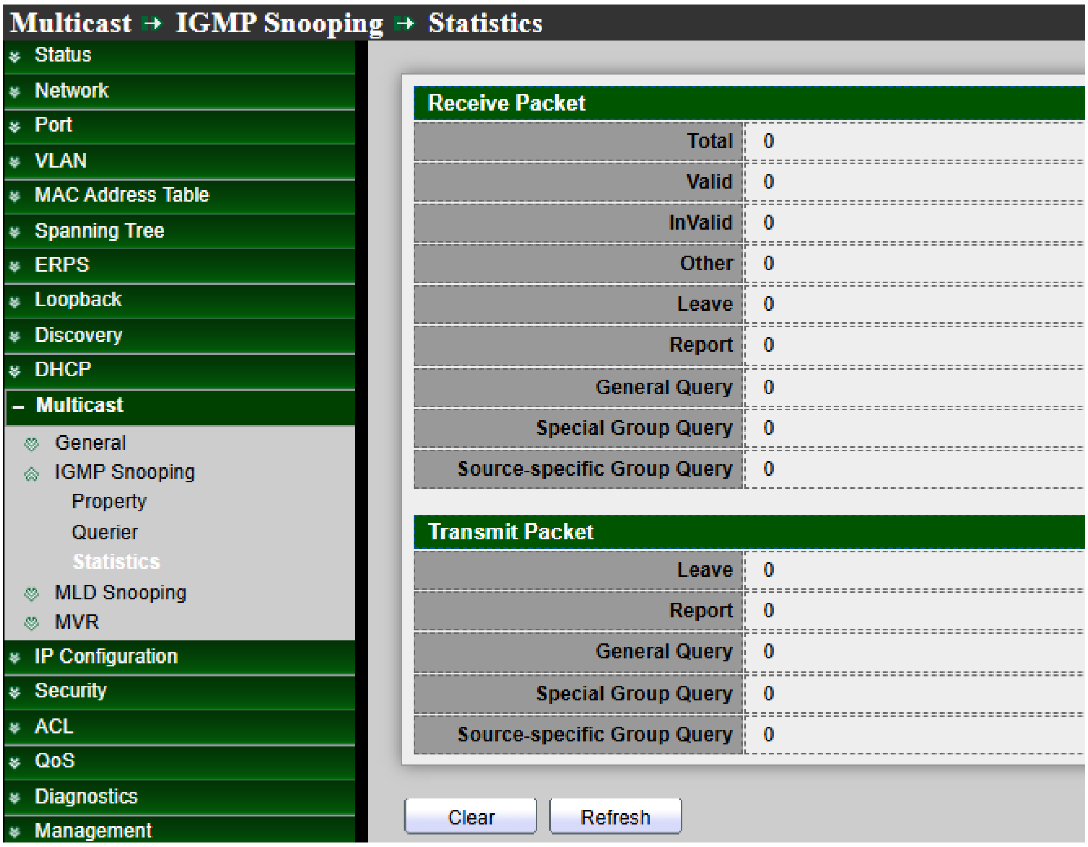
VLAN	1
State	☑ Enable
Version	○ IGMPv2 ● IGMPv3

- **VLAN:** The Selected Edit IGMP Snooping querier VLAN List.
- **State :** Set the enabling status of IGMP Querier Election on the chose VLANs.
  - **Enabled:** if checked Enable IGMP Querier else Disable IGMP Querier.
- **Version :** Set the query version of IGMP Querier Election on the chose VLANs.
  - **IGMPv2:** Querier version 2.
  - **IGMPv3:** Querier version 3. (IGMP Snooping version should be IGMPv3).

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

13.2.3 Statistics

Display Receive / Transmit Packet information of IGMP snooping.



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

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

Field	Description
Receive Packet	● **Total:** Total RX igmp packet, include ipv4 multicast data to CPU. ● **Valid:** The valid igmp snooping process packet. ● **InValid:** The invalid igmp snooping process packet. ● **Other:** The ICMP protocol is not 2, and is not ipv4 multicast data packet. ● **Leave:** IGMP leave packet. ● **Report:** IGMP join and report packet. ● **General Query:** IGMP General Query packet. ● **Special Group Query:** IGMP Special Group General Query packet. ● **Source-specific Group Query:** IGMP Special Source and Group General Query packet.
Transmit Packet	● **Leave:** IGMP leave packet. ● **Report:** IGMP join and report packet. ● **General Query:** IGMP general query packet include

	querier transmit general query packet ● **Special Group Query:** IGMP special group query packet include querier transmit special group query packet. ● **Source-specific Group Query:** IGMP Special Source and Group General Query packet.

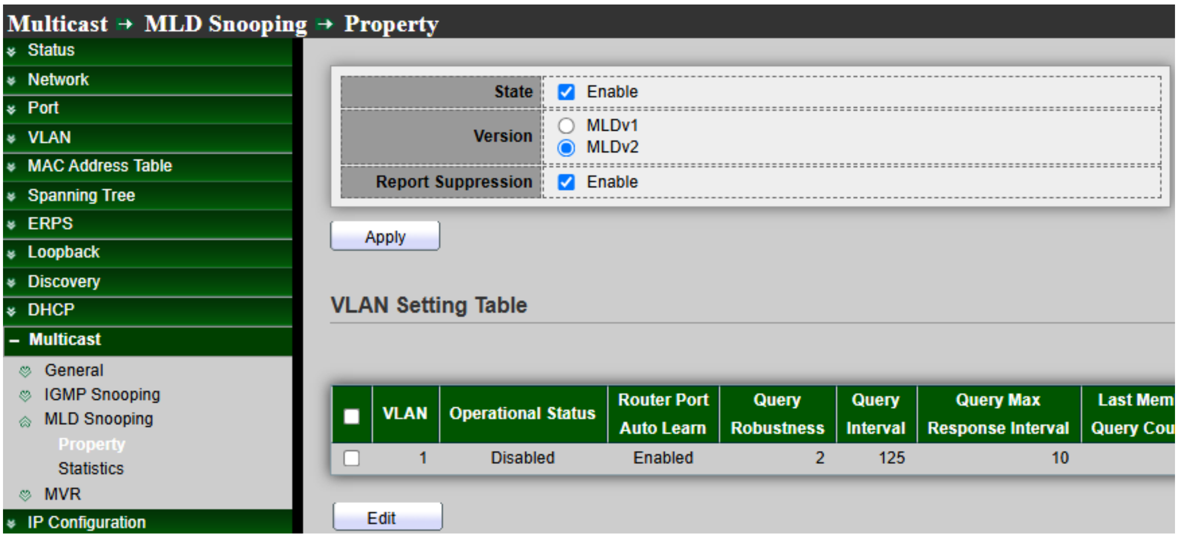
*Click the **"Clear"** button to clear this page or click the **"Refresh"** button to refresh the page .*

13.3 MLD Snooping

The function support selective Multicast forwarding (IPv6), MLD Snooping must be enabled globally and for each relevant VLAN. The switch supports MLD Snooping on both static and dynamic VLANs. Hosts use the MLD protocol to report their participation in Multicast sessions, and the switch uses MLD Snooping to build Multicast membership lists. It uses these lists to forward Multicast packets only to switch ports where there are host nodes that are members of the Multicast groups. The switch does not support MLD Querier.

13.3.1 Property

Administrator to enable MLD Snooping in addition to the manually configured Multicast groups, the result is a union of the Multicast groups and port memberships derived from the manual setup and the dynamic discovery by MLD Snooping. However, only the static definitions are preserved when the switch is rebooted.



State	☑ Enable
Version	○ MLDv1 ● MLDv2
Report Suppression	☑ Enable

VLAN Setting Table

□	VLAN	Operational Status	Router Port Auto Learn	Query Robustness	Query Interval	Query Max Response Interval	Last Mem Query Cou
□	1	Disabled	Enabled	2	125	10	

➢ **State:** Administrator can select Enable or Un-enable, Set the enabling status of IGMP Snooping functionality.

- **Enable:** If Checked Enable IGMP Snooping, else is Disabled IGMP Snooping.

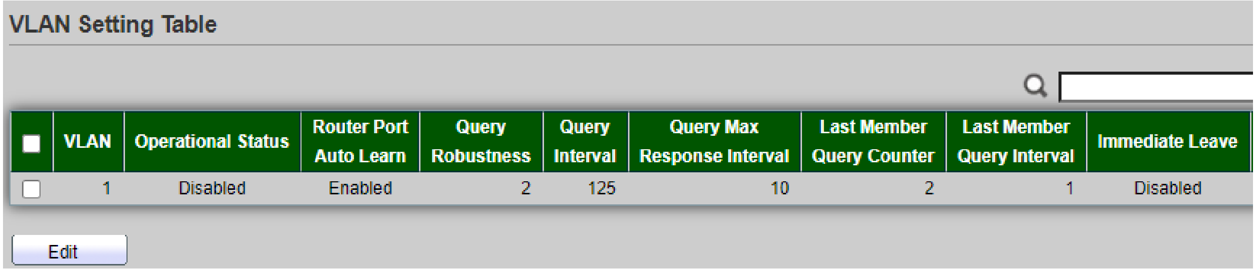
➢ **Version:** Select either MLDv1 or MLDv2, Set the MLD snooping version.

- **MLDv1:** Only support process MLD v1 packet.
- **MLDv2:** Support v2 basic and v1.

➢ **Report Suppression:** Set the enabling status of MLD v1 report suppression.

- **Enable:** If Checked Enable MLD Snooping v1 report suppression, else Disable the report suppression function.

*Click the **"Apply"** button to save your changes.*

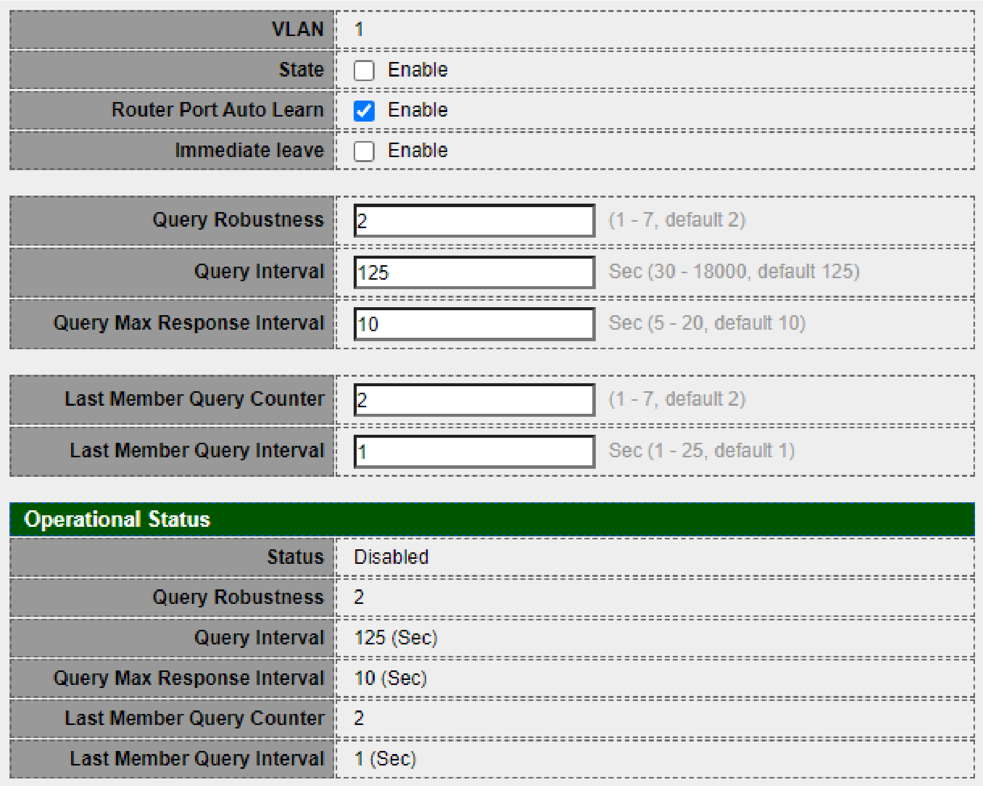


VLAN Setting Table

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

Field	Description
VLAN	The MLD entry VLAN ID
Operation Status	The enable status of MLD snooping VLAN functionality
Router Port Auto Learn	The enabling status of 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	In Membership Query Messages, it specifies the maximum allowed time before sending a responding report in units of 1/10 second.
Query Max Response Interval	The count that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Last Member Query Interval	The interval that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Immediate leave	The immediate leave status of the group will immediate leave when receive MLD Leave message.

Administrator can select VLAN in checkbox and click “Edit” button to set MLD Snooping.



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

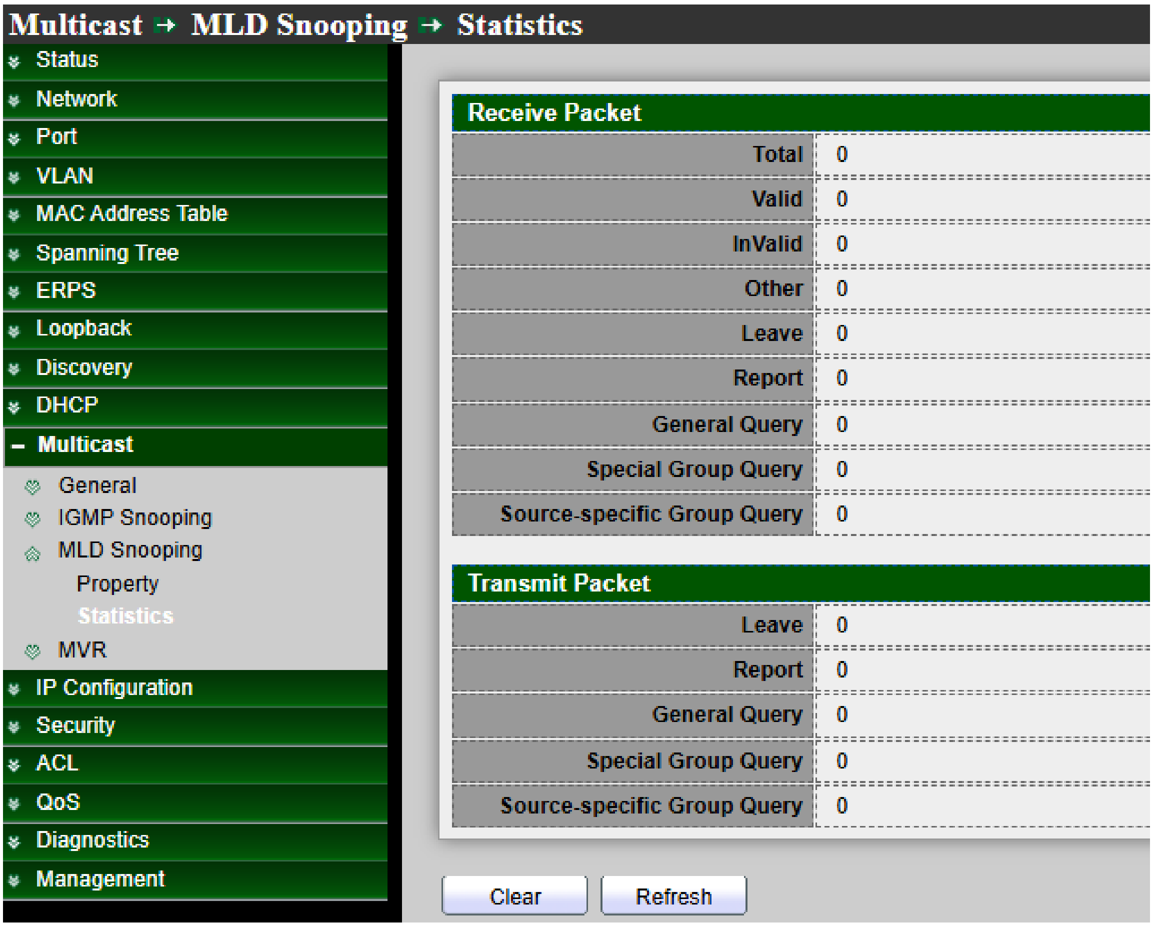
Operational Status	
Status	Disabled
Query Robustness	2
Query Interval	125 (Sec)
Query Max Response Interval	10 (Sec)
Last Member Query Counter	2
Last Member Query Interval	1 (Sec)

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

- **Operational Status:** Set the enabling status of MLD Snooping router port learning.
  - **Status:** Operational MLD snooping status,must both MLD snooping global and MLD snooping enable the status will be enable.
  - **Query Robustness:** Operational Query Robustness.
  - **Query Interval:** Operational Query Interval.
  - **Query Max Response Interval:** Operational Query Max Response Interval.
  - **Last Member Query Counter:** Operational Last Member Query Count.
  - **Last Member Query Interval:** Operational Last Member Query Interval.

13.3.2 Statistics

If administrator to enable MLD snooping, the page will display Receive / Transmit Packet information of MLD Snooping.



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

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

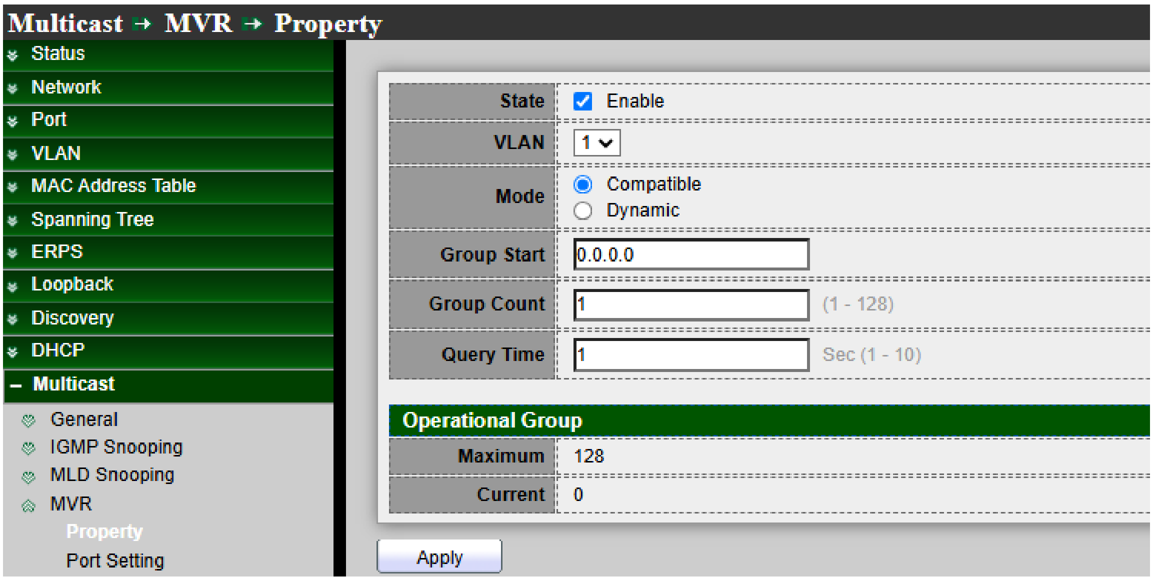
Field	Description
Receive Packet	● **Total:** Total RX MLD packet, include ipv4 multicast data to CPU. ● **Valid:** The valid MLD snooping process packet. ● **InValid:** The invalid MLD snooping process packet. ● **Other:** The ICMPV6 type is not MLD, and is not ipv6 multicast data packet and is not IPV6 router protocol. ● **Leave:** MLD leave packet. ● **Report:** MLD join and report packet. ● **General Query:** MLD General Query packet. ● **Special Group Query:** MLD Special Group General Query packet. ● **Source-specific Group Query:** MLD Special Source and Group General Query packet.
Transmit Packet	● **Leave:** MLD leave packet. ● **Report:** MLD join and report packet. ● **General Query:** MLD general query packet. ● **Special Group Query:** MLD special group query packet. ● **Source-specific Group Query:** MLD Special Source and Group General Query packet.

*Click the **"Clear"** button to clear this page or click the **"Refresh"** button to refresh the page .*

13.4 MVR

MVR (Multicast VLAN Registration) is designed for applications that use wide-scale deployment of multicast traffic across an Ethernet ring-based service-provider network (for example, the broadcast of multiple television channels over a service-provider network). MVR allows a subscriber on a port to subscribe and unsubscribe to a multicast stream on the network-wide multicast VLAN.
It allows the single multicast VLAN to be shared in the network while subscribers remain in separate VLANs. MVR provides the ability to continuously send multicast streams in the multicast VLAN, but to isolate the streams from the subscriber VLANs for bandwidth and security reasons.

13.4.1 Property



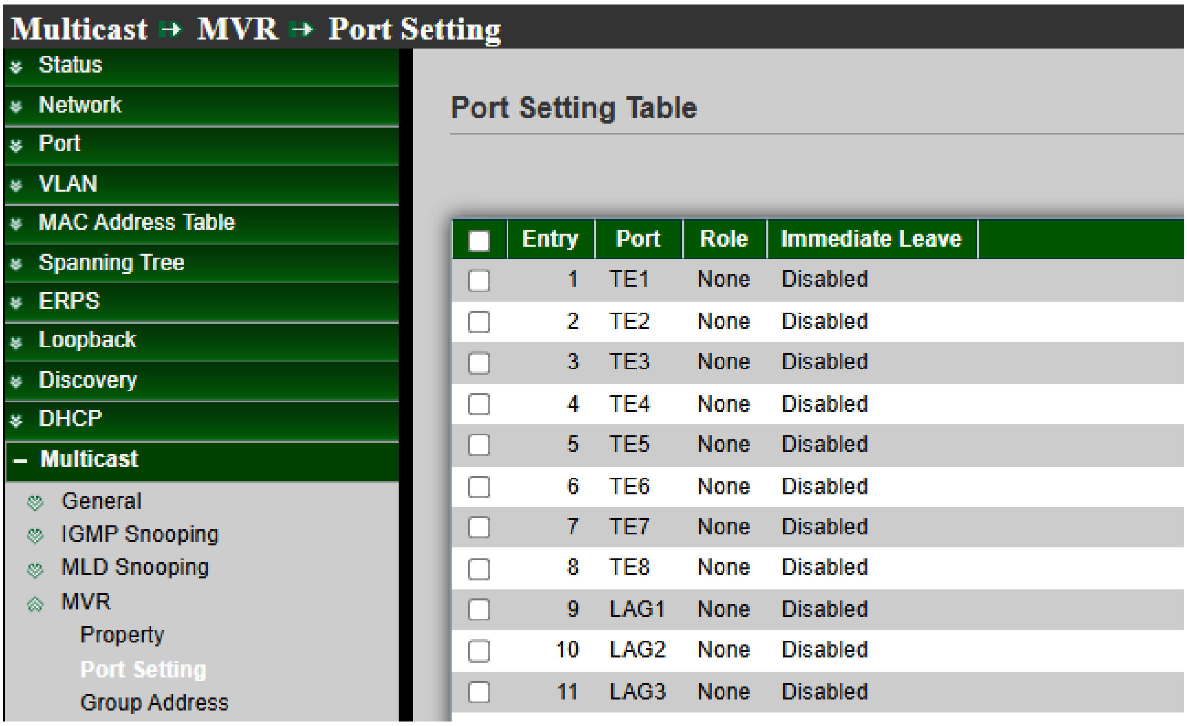
State	☑ Enable
VLAN	1
Mode	● Compatible ○ Dynamic
Group Start	0.0.0.0
Group Count	1 (1 - 128)
Query Time	1 Sec (1 - 10)
Operational Group	
Maximum	128
Current	0

- **State:** Administrator can select Enable or Un-enable, Set the enabling status of MVR functionality.
  - **Enable:** if checked enable the MVR state, else disable the MVR state.
- **VLAN:** Select the MVR VLAN ID.
- **Mode:** Set the MVR mode.
  - **Compatible:** compatible mode.
  - **Dynamic:** dynamic mode, will learn group member on source port.
- **Group Start:** Administrator can set range is 224.0.0.0 to 239.255.255.255,MVR group range start.
- **Group Count:** MVR group continue count, Uses the count parameter to configure a contiguous series of MVR group addresses (the range for count is 1 to 128; the default is 1).
- **Query Time:** MVR query time when receive MVR leave MVR group packet,Administrator can defines the maximum time to wait for IGMP report memberships on a receiver port before removing the port from multicast group membership. The value is in units of second. The range is 1 to 10, and the default is 1 second.
- **Operational Group:**
  - **Maximum:** The max number of MVR group database.
  - **Current:** The learned MVR group current time.

*Click the **"Apply"** button to save your changes settings.*

13.4.2 Port Setting

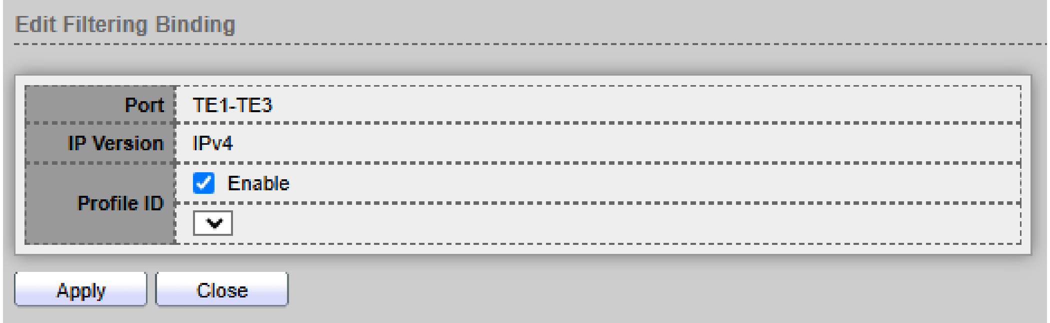
Administrator can select ports to set role and immediate of MVR.



Port Setting Table

☐	Entry	Port	Role	Immediate Leave
☐	1	TE1	None	Disabled
☐	2	TE2	None	Disabled
☐	3	TE3	None	Disabled
☐	4	TE4	None	Disabled
☐	5	TE5	None	Disabled
☐	6	TE6	None	Disabled
☐	7	TE7	None	Disabled
☐	8	TE8	None	Disabled
☐	9	LAG1	None	Disabled
☐	10	LAG2	None	Disabled
☐	11	LAG3	None	Disabled

Field	Description
Port	Port Name
Role	Port Role for MVR, the type is None/Receiver/Source
Immediate Leave	Status of immediate leave



Edit Filtering Binding

Port	TE1-TE3
IP Version	IPv4
Profile ID	☑ Enable ⌄

- **Port:** Display the selected port list.
- **Role:** MVR port role.
  - **None:** port role is none.
  - **Receiver:** port role is receiver, Configures a port as a receiver port if it is a subscriber port

and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group, either statically or by using IGMP leave and join messages. Receiver ports cannot belong to the multicast VLAN.

- **Source:** port role is source, Configures uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports. All source ports on a switch belong to the single multicast VLAN.

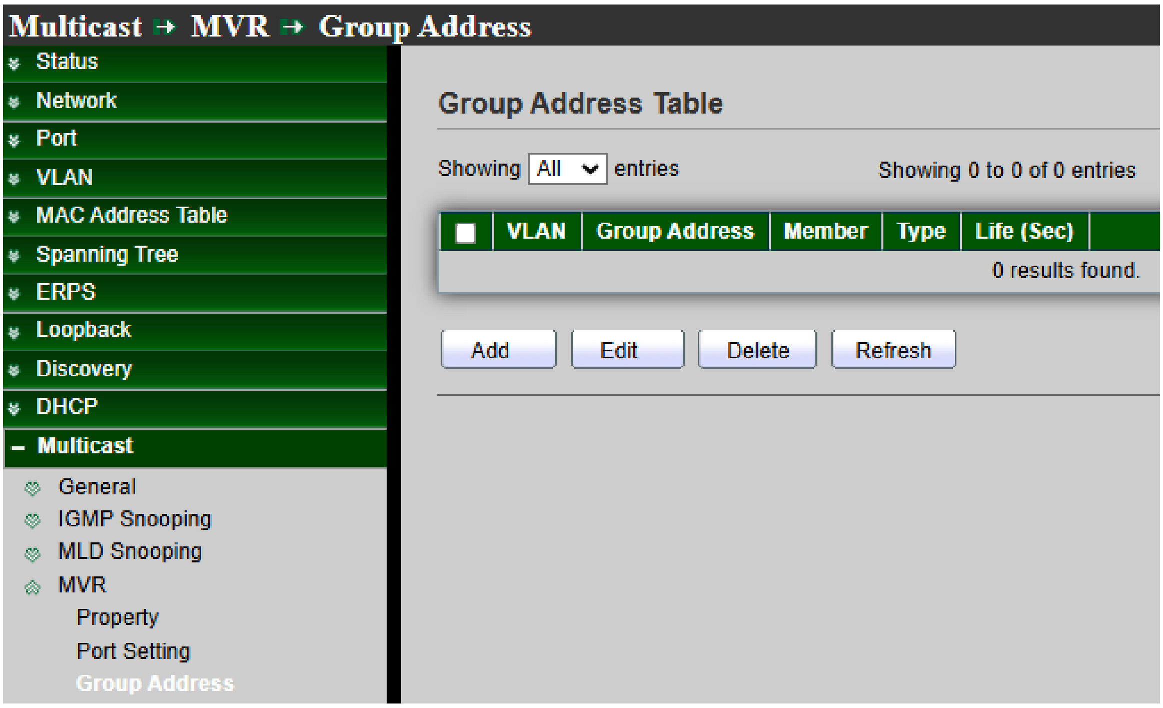
Note	If administrator to set a non-MVR port with MVR characteristics is operation fails. The default configuration is as a non-MVR port.

- **Immediate Leave:** MVR Port immediate leave
  - **Enable:** if checked is enable immediate leave, else disable immediate leave, This function only be enabled on receiver ports to which a single receiver device is connected. When Enables the Immediate Leave feature of MVR on the port. The Immediate Leave feature is disabled by default

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

13.4.3 Group Address

Setting **"add"** and **"Edit"** and **"Delete"** and **"Refresh"** function for this management.

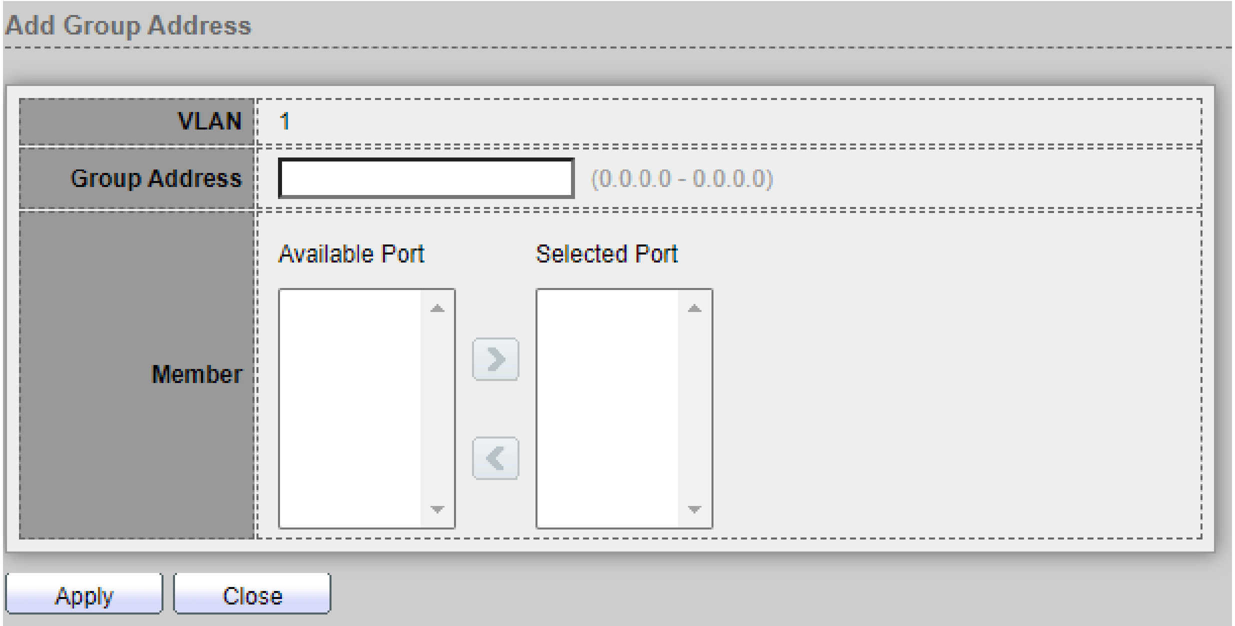


Group Address Table

Showing All entries — Showing 0 to 0 of 0 entries

□	VLAN	Group Address	Member	Type	Life (Sec)
					0 results found.

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


Add Group Address

VLAN	1
Group Address	(0.0.0.0 - 0.0.0.0)
Member	Available Port / Selected Port

- **VLAN:** The VLAN ID of MVR group.
- **Group Address:** MVR group IP address ,Administrator can set MVR multicast group addresses on the switch.(The address range is 224.0.0.0 to 239.255.255.255)
- **Member:** Select Ports in the MVR Group.
  - **Available Port :** Optional port member, it is only receiver port when MVR mode is compatible, it include source port when mode is dynamic.
  - **Selected Port** : Selected port member.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

14. IP Configuration

By default all ports belong to the same VLAN and the switch only provides Layer 2 Function. To segment connected networks, first create a VLAN for each unique network user group or application traffic, assign all ports belonging to the same group to these VLANs, and assign an IP interface to each VLAN. By dividing the network into Different VLANs, which can be divided into subnets that are disconnected at the layer2. Network traffic within the same subnet is still switched using Layer 2 switching. and VLANs can now (as required) be interconnected with Layer 3 switching.
Each VLAN represents a layer 3 virtual interface. You only need to provide Network address for each virtual interface, and traffic between different interfaces Subnets will be routed through Layer 3 switching.

14.1 IPv4 Management and Interfaces

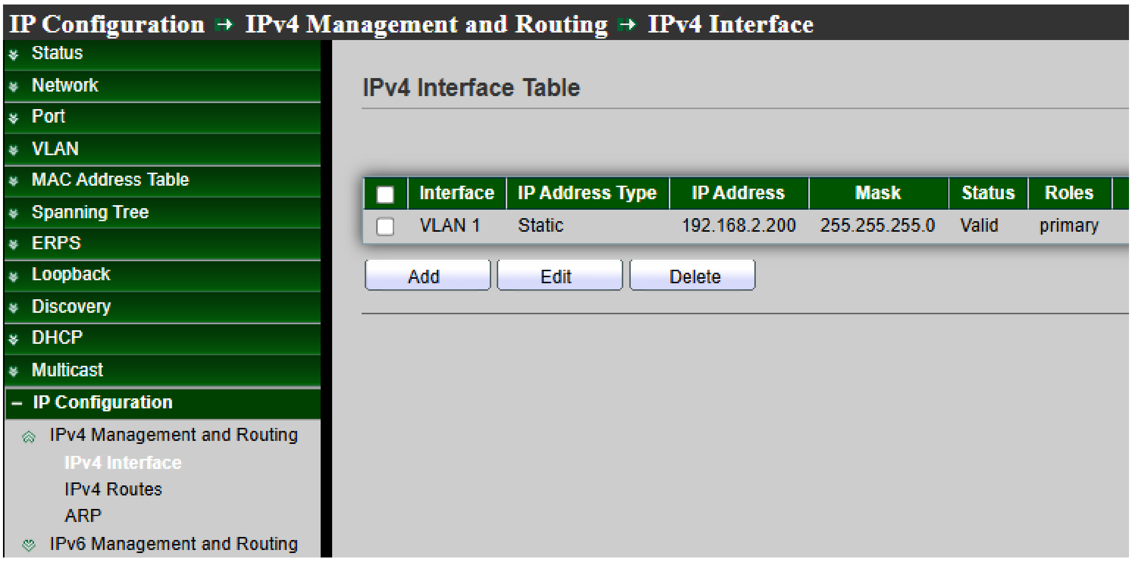
This chapter describes how to configure the IP interface for management access
Switch over the network. The switch supports IP version 4 and version 6,
And can be managed simultaneously by any of these address types. You can manually configure specific IPv4 or IPv6 addresses, or instruct the switch to obtain an IPv4 address from a BOOTP or DHCP server. An IPv6 address can only be configured manually.

IPv4 Configuration – Set the IPv4 address for management access.

An IPv4 address default IP is **'192.168.2.200'** To configure a static address, To configure a static address, you need to change the switch's default settings to values that are compatible with your network. **You may also need to a establish a default gateway between the switch and management stations that exist on another network segment (if no routing protocols are enabled).**
You can direct the device to obtain an address from a BOOTP or DHCP server, or manually configure a static IP address. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything other than this format will not be accepted.

14.1.1 IPv4 Interface & Default IP Configure

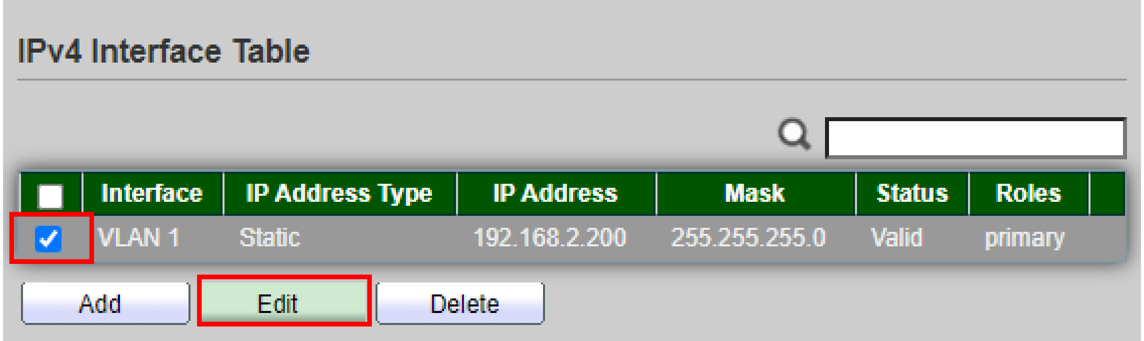
Administrator can configure this drop down list to specify the VLAN ID number of the IPv4 interface through which the IPv4 packets are forwarded and The Switch supports the VLAN interface type and Loopback interface type,Setting **"add"** and **"Edit"** and **"Delete"** function for this management.



IP Configuration → IPv4 Management and Routing → IPv4 Interface

IPv4 Interface Table

□	Interface	IP Address Type	IP Address	Mask	Status	Roles
□	VLAN 1	Static	192.168.2.200	255.255.255.0	Valid	primary

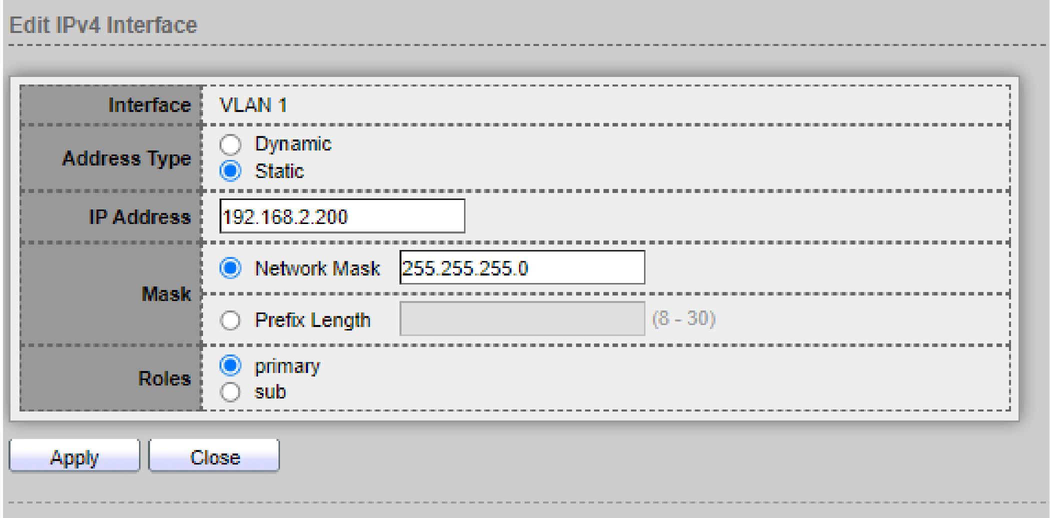


IPv4 Interface Table

□	Interface	IP Address Type	IP Address	Mask	Status	Roles
☑	VLAN 1	Static	192.168.2.200	255.255.255.0	Valid	primary

Configure VLAN1 (Default VLAN) IP address for your Fiber Optical Switch

And 'Save running configuration to startup configuration'



Edit IPv4 Interface

Interface	VLAN 1
Address Type	○ Dynamic ● Static
IP Address	192.168.2.200
Mask	● Network Mask 255.255.255.0 ○ Prefix Length (8 - 30)
Roles	● primary ○ sub

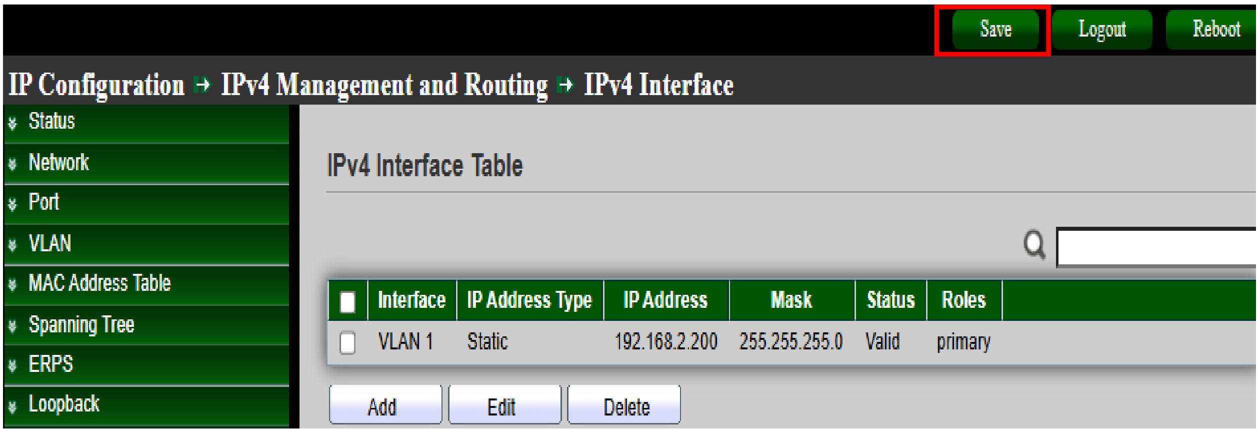
- **Address Type :**
  - **Dynamic :** Select to set as "Dynamic" type.
  - **Static :** Select to set as "Static" type.

Note	If set the "Dynamic" type，The IP settings will be obtained from other DHCP server assignments.

- **IP Address :** IP Address of the VLAN. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. **(Default IP is : 192.168.2.200).**
- **Mask :**
  - **Network Mask :** This mask identifies the host address bits used for routing to specific subnets. **(Default Network Mask is : 255.255.255.0)**
  - **Prefix Length :** In the Prefix Length field, define the Prefix Length of the Routing IPv4 Interface.
- **Roles :**
  - **Primary :** In the Primary field, Select the setting defined as the primary roles.
  - **Sub :** In the Sub field, Select the setting defined as the secondary roles.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

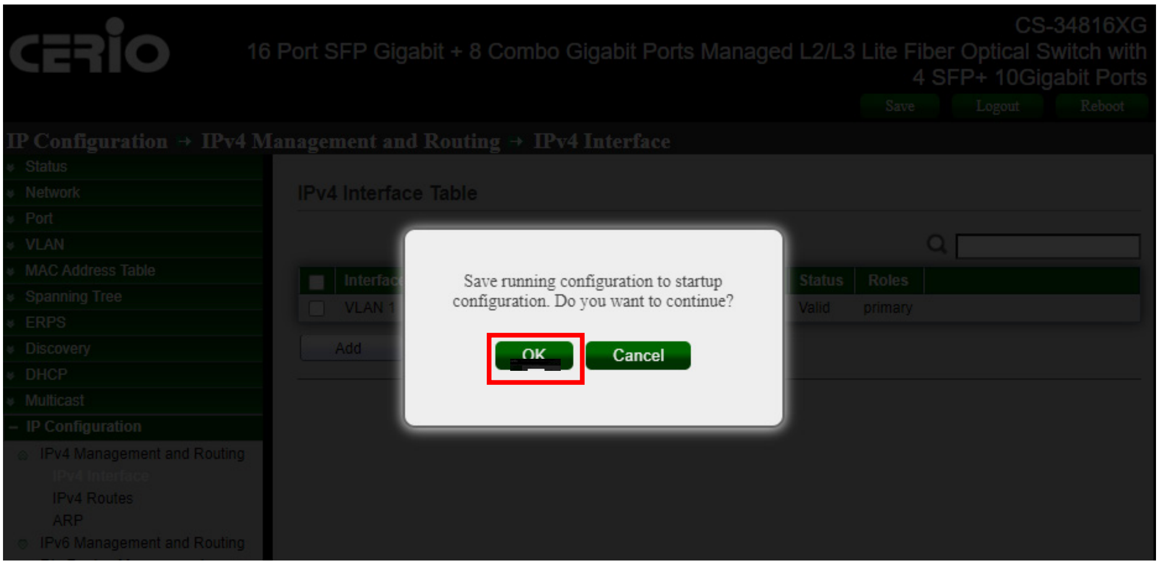
'Save running configuration to startup configuration'



IPv4 Interface Table

□	Interface	IP Address Type	IP Address	Mask	Status	Roles
□	VLAN 1	Static	192.168.2.200	255.255.255.0	Valid	primary

After successfully changing the new IP, execute "Save running configuration to startup configuration" to make the new IP setting of Fiber Optical Switch take effect every time it is started.

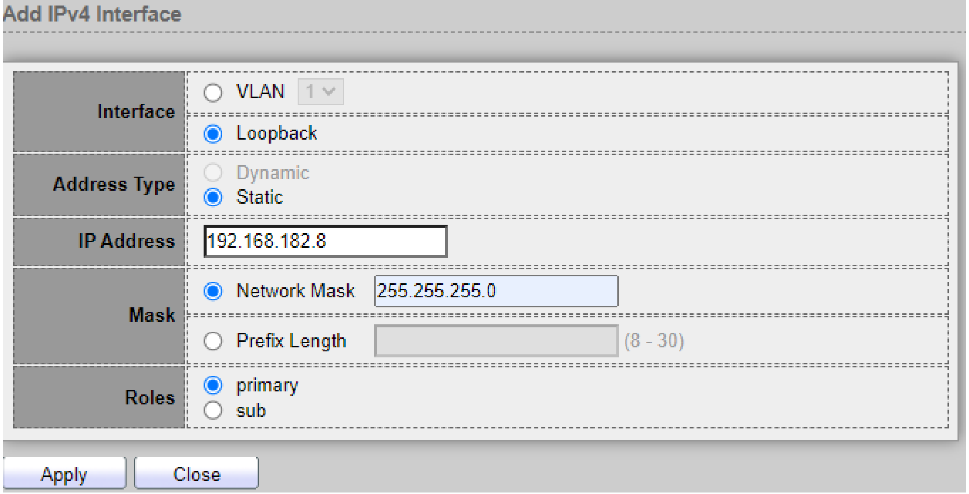

CS-34816XG
16 Port SFP Gigabit + 8 Combo Gigabit Ports Managed L2/L3 Lite Fiber Optical Switch with 4 SFP+ 10Gigabit Ports
Save
Logout
Reboot
IP Configuration → IPv4 Management and Routing → IPv4 Interface
Status
Network
Port
VLAN
MAC Address Table
Spanning Tree
ERPS
Discovery
DHCP
Multicast
IP Configuration
IPv4 Management and Routing
IPv4 Interface
IPv4 Routes
ARP
IPv6 Management and Routing
IPv4 Interface Table
Interface
Status
Roles
VLAN 1
Valid
primary
Add

Save running configuration to startup configuration. Do you want to continue?

OK Cancel

Click the "ok" button to save 'Save running configuration to startup configuration'.

Add New VLAN IP address setting on 'Loopback'



Add IPv4 Interface

Interface	○ VLAN 1 ● Loopback
Address Type	○ Dynamic ● Static
IP Address	192.168.182.8
Mask	● Network Mask 255.255.255.0 ○ Prefix Length (8 - 30)
Roles	● primary ○ sub

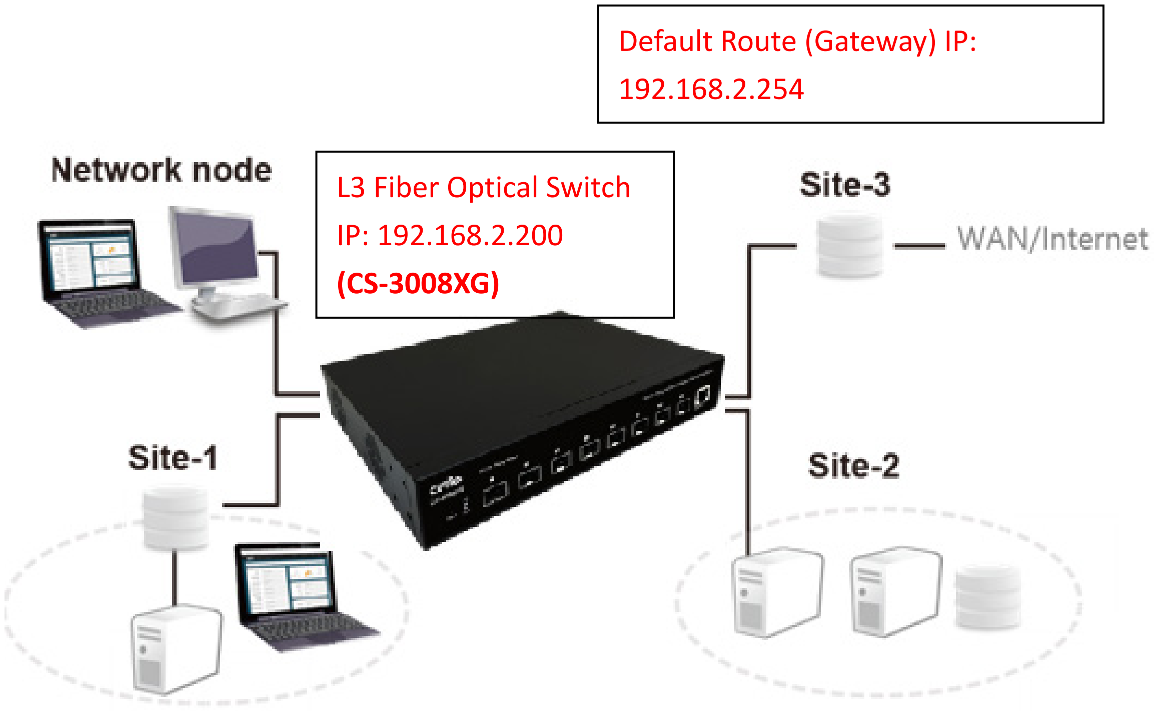
Apply Close

- **Address Type :** The Interface for Loopback only provides settings as "static" type.
- **IP Address :** In the IP Address field, define the IP address of the Routing IPv4 Interface.
- **Mask :**
  - **Network Mask :** In the Network Mask field, define the Subnet Mask of the Routing IPv4 Interface.
- **Prefix Length :** In the Prefix Length field, define the Prefix Length of the Routing IPv4
- **Roles :**
  - **Primary :** In the Primary field, Select the setting defined as the primary roles.
  - **Sub :** In the Sub field, Select the setting defined as the secondary roles.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

14.1.2 IPv4 Routes & Default Route Configure

You can enter static routes in the routing table using the IP > Static Routes (Add) page. Static routes may be required to force the use of a specific route to a subnet. Static routes do not automatically change in response to changes in network topology , so you should only configure a small number of stable routes to ensure network



Default Route (Gateway) IP: 192.168.2.254

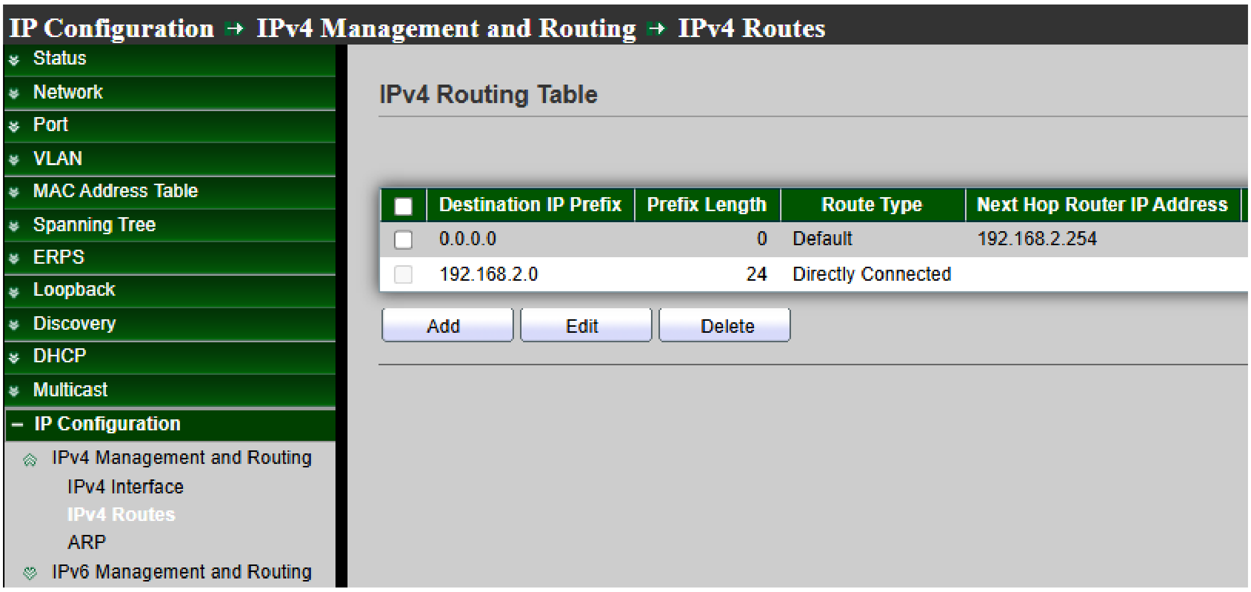
L3 Fiber Optical Switch
IP: 192.168.2.200
(CS-3008XG)

The Switch usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. In the network, the router selects an appropriate path according to the destination address of the received data, and forwards the data to the next router. The last router in the path is responsible for forwarding the packet to the destination host.

For example, the traffic from “Network node” to the Internet through the Switch’s default Route (default Gateway) (Site-3). You create one static route to connect to services offered by your ISP behind router (Site-2).

You create another static route to communicate with a separate network behind a router (Site-1)connected to the Switch.

Administrator can configure this “IPv4 Routing Table “page setting for **“add”** and “Edit” and **“Delete”** function management.



IPv4 Routing Table

□	Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address
□	0.0.0.0	0	Default	192.168.2.254
□	192.168.2.0	24	Directly Connected	

Configure next hop route of the Gateway IP forwarded packet in "Default Route", for LAN device to access the Internet.

And 'Save running configuration to startup configuration'

Default routes in hosts are often called default gateways. The **default gateway** is usually a filtering device such as a NAT gateway router, firewall, or proxy server.

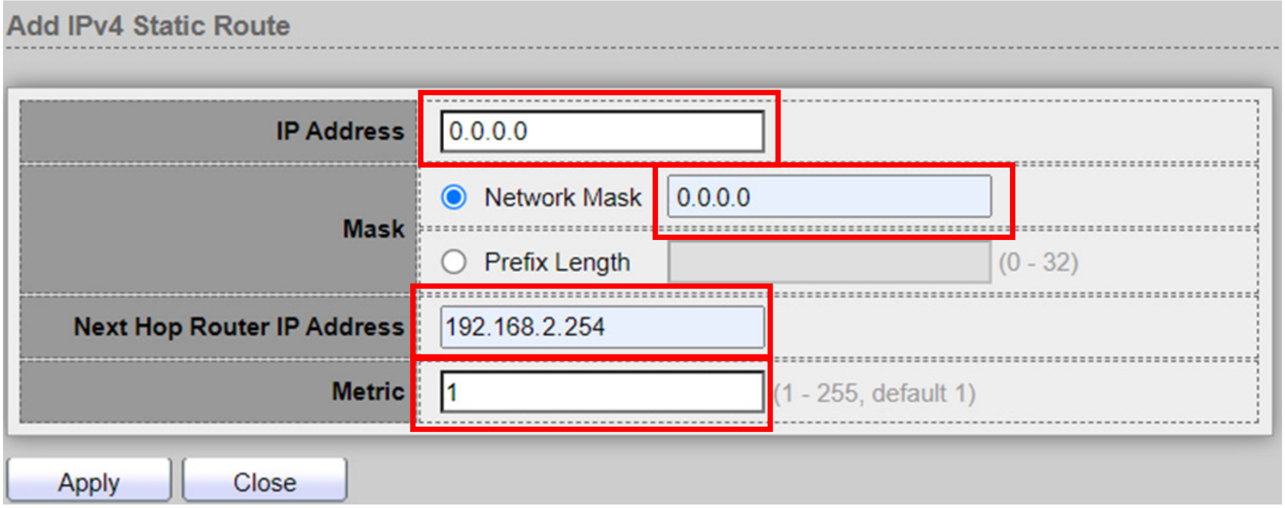
"Default route" is the route selected by the router when no other existing route can be found for the destination address in the IP packet. All packets whose destination is not in the router's routing table will use the default route. The route usually leads to another router that also handles the packet: if it knows how to route the packet, it forwards the packet to the known route; otherwise, the packet is forwarded to the default route. Route to another router. With each forwarding, the route increases the distance by one hop.

Note	CS-3008XG is a switch with route function. "Default Route" this feature is often referred to as "Default Gateway Configure" when operating in a Layer 2 switch environments. These settings for L2 and L3 have the same purpose, which is to set the default transmission destination for unknown IP data.

The default route in a TCP/IP network is a setting that tells the device how to forward the packet when the destination IP of the packet is not on the same subnet as the device, in order to achieve smooth access to the Internet. Use static routing settings to determine the gateway IP address to designate as the next hop.

Configure the "default route" (Gateway IP) of the Fiber Optical Switch . Please refer to the following .

Default Route (Gateway IP)Configure Sample:



Add IPv4 Static Route

IP Address	0.0.0.0		
Mask	● Network Mask	0.0.0.0	
	○ Prefix Length		(0 - 32)
Next Hop Router IP Address	192.168.2.254		
Metric	1	(1 - 255, default 1)	

The default route setting Sample destination IP address and Mask IP Address are “0.0.0.0 “(Means any IP), Gateway Router IP Address is “192.168.2.254”, Metric is “1” .

Note	The destination IP and netmask 0.0.0.0 (Means any IP) represents any destination IP address that does not match other route entries. According to this preset route, all traffic to the Internet will be forwarded to the gateway router (192.168.2.254).This will allow you to successfully access the Internet. (Distance is an optional parameter, in this case we can leave it as default or set it to 1) .

➢ **IP Address / Destination IP :** In the Destination IP field, specify the IP address for the destination.

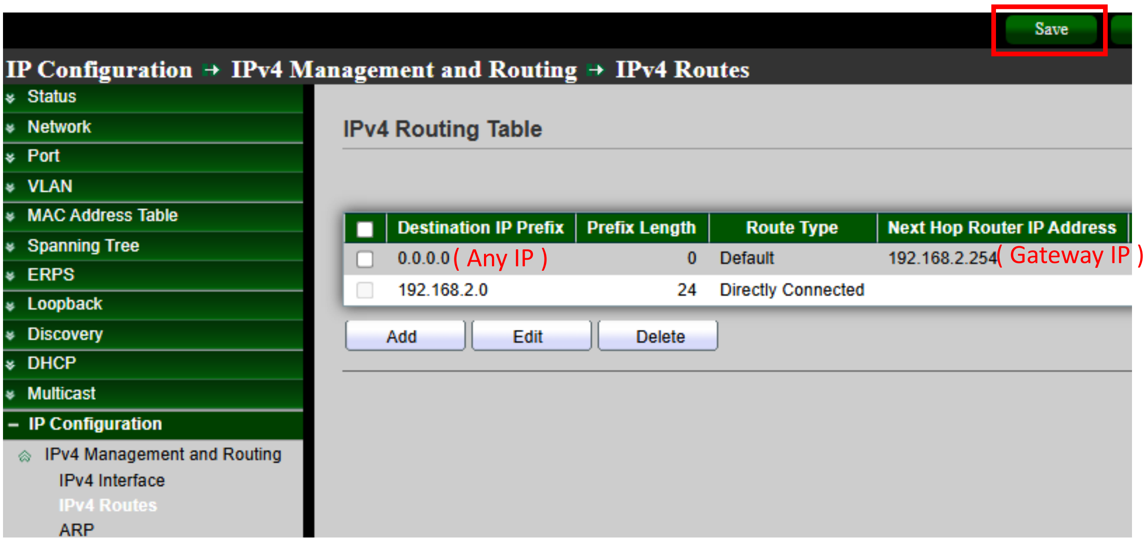
➢ **Mask :**

- **Network Mask :** Specify the subnet mask for the attached network.
- **Prefix Length :** In the IPv4 Prefix Length field, specify the IPv4 prefix length for the destination.

- **Next Hop Router IP Address :** In the Next Hop IP Address field, specify the outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.
- **Metric :** Please fill in the cost (hop count) of transmission you want to apply for routing purposes.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

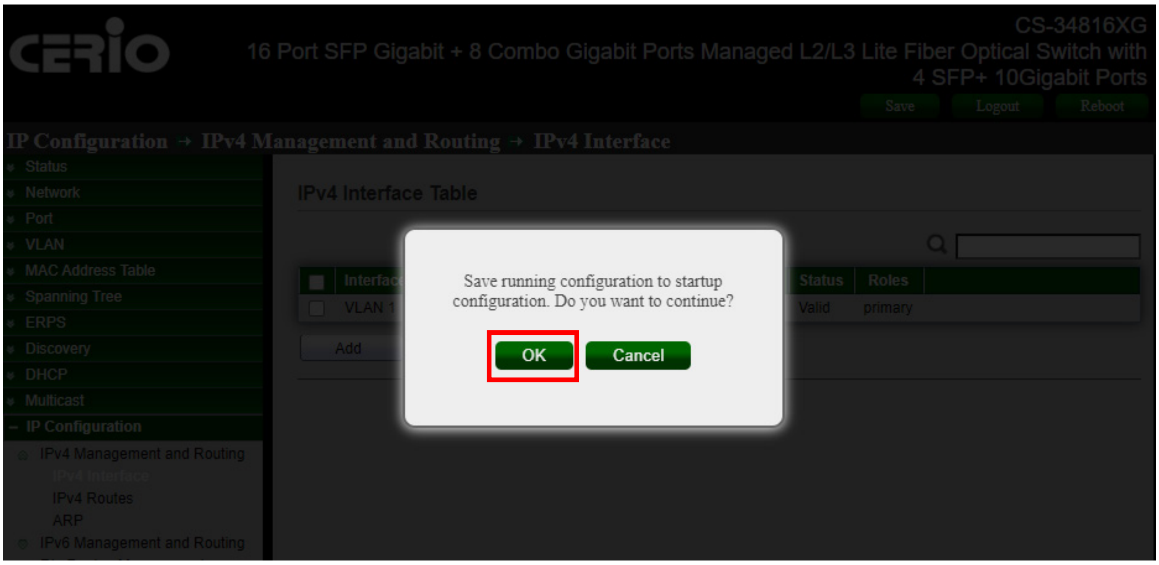
'Save running configuration to startup configuration'



IPv4 Routing Table

☐	Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address
☐	0.0.0.0(Any IP)	0	Default	192.168.2.254(Gateway IP)
☐	192.168.2.0	24	Directly Connected	

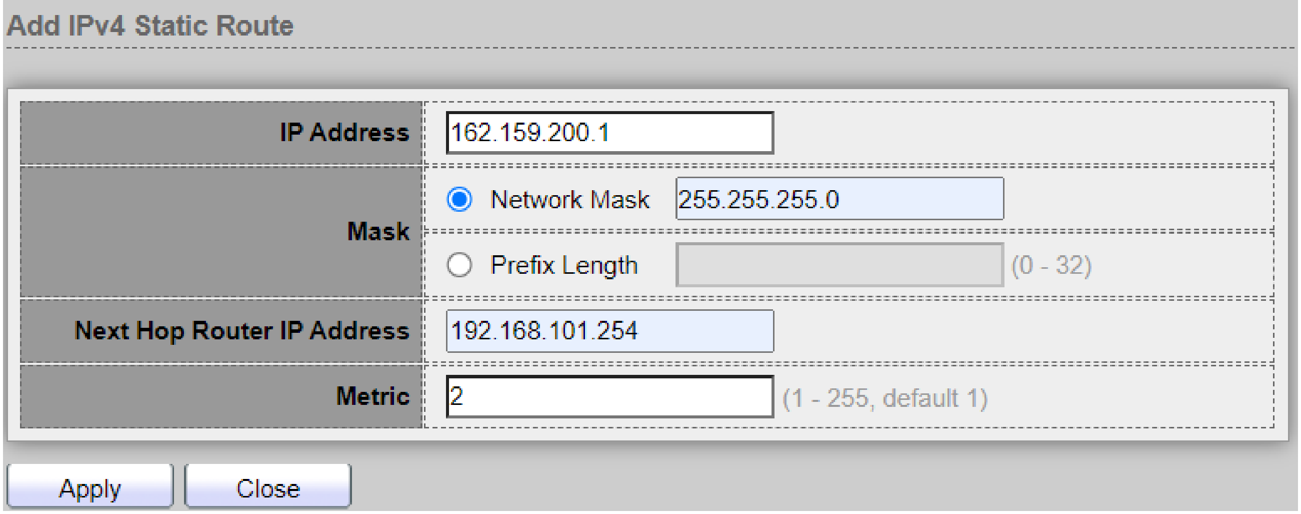
After successfully changing the new IP, execute "Save running configuration to startup configuration" to make the Gateway IP setting of Fiber Optical Switch take effect every time it is started.


CS-34816XG
16 Port SFP Gigabit + 8 Combo Gigabit Ports Managed L2/L3 Lite Fiber Optical Switch with 4 SFP+ 10Gigabit Ports
Save
Logout
Reboot
IP Configuration → IPv4 Management and Routing → IPv4 Interface
Status
Network
Port
VLAN
MAC Address Table
Spanning Tree
ERPS
Discovery
DHCP
Multicast
IP Configuration
IPv4 Management and Routing
IPv4 Interface
IPv4 Routes
ARP
IPv6 Management and Routing
IPv4 Interface Table
Interface
Status
Roles
VLAN 1
Valid
primary
Add
OK
Cancel

Save running configuration to startup configuration. Do you want to continue?

Click the "ok" button to save 'Save running configuration to startup configuration'.

Static Route Configure Sample:



Add IPv4 Static Route

IP Address	162.159.200.1
Mask	● Network Mask 255.255.255.0 ○ Prefix Length (0 - 32)
Next Hop Router IP Address	192.168.101.254
Metric	2 (1 - 255, default 1)

The Static Route Sample IP Address is 162.159.200.1

Gateway Router IP Address is 192.168.101.254

- **IP Address / Destination IP :** In the Destination IP field, specify the IP address for the destination.

Note	This parameter specifies the IP network address of the final destination. Routing is always based on network numbers. If you need to specify a route to a single host, use the subnet mask 255.255.255.255 in the Subnet Mask field to force the network number to be the same as the host ID.

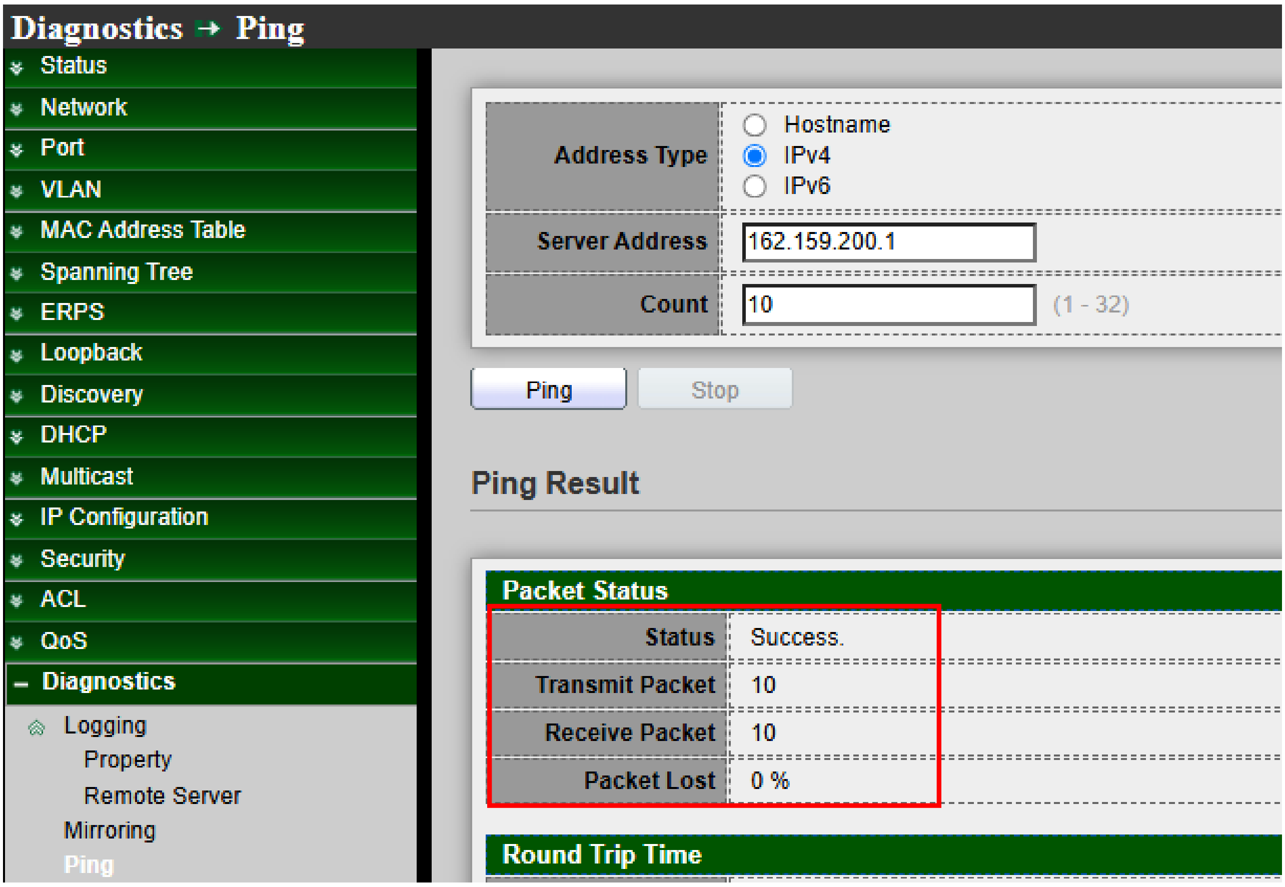
- **Mask :**
  - **Network Mask :** Specify the subnet mask for the attached network.
  - **Prefix Length :** In the IPv4 Prefix Length field, specify the IPv4 prefix length for the destination.
- **Next Hop Router IP Address :** In the Next Hop IP Address field, specify the outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.

Note	The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly attached network.

- **Metric :** Please fill in the cost (hop count) of transmission you want to apply for routing purposes.

Note	This metric represents the "cost" of transmission for routing purposes. IP routing uses "hop count" as a measure of cost, with a minimum value of 1 for directly connected networks. Enter a number that approximates the cost of this link. The number does not need to be exact, but must be between 1 and 255. In fact, 1 or 2 or 3 is usually suggested here to fill in the frequently used numbers.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

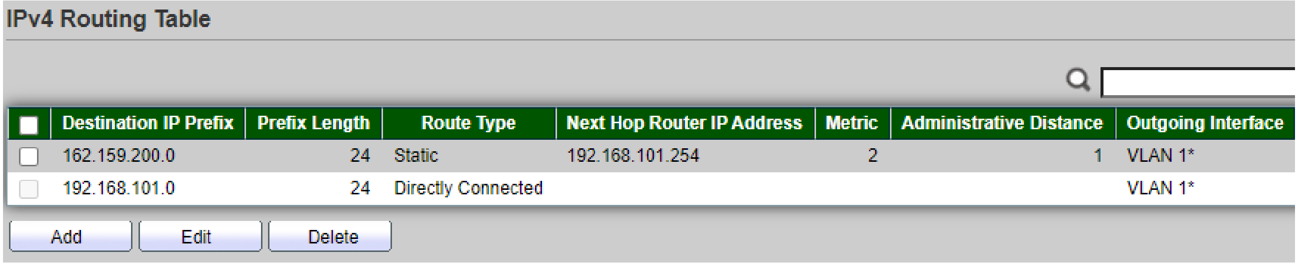


Address Type	○ Hostname ● IPv4 ○ IPv6
Server Address	162.159.200.1
Count	10 (1 - 32)

Packet Status

Status	Success.
Transmit Packet	10
Receive Packet	10
Packet Lost	0 %

For the Static Route Sample IP Address Enter to " 162.159.200.1", If the setting is successful, you can test and verify it through the "Diagnostics> Ping tool.



IPv4 Routing Table

□	Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address	Metric	Administrative Distance	Outgoing Interface
□	162.159.200.0	24	Static	192.168.101.254	2	1	VLAN 1*
□	192.168.101.0	24	Directly Connected				VLAN 1*

Field	Description
Destination IP Prefix	The IP Prefix for the destination
Prefix Length	The prefix length for the active route.
Router Type	The type of route: Static or Dynamic, depending on how the route was added.
Next Hop Router IP Address	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination. The next router **(ex. Your Gateway site IP address)** is always one of the adjacent neighbors or the IP address of the local interface for a directly attached network.
Metric	The Metric value for the configured next hop. Specify the Metric (sometimes called administrative distance), which is an integer value from 1 to 255.
Administrative Distance	The route administrative distance of the configured route.
Outgoing Interface	The outgoing interface of the route active or inactive.

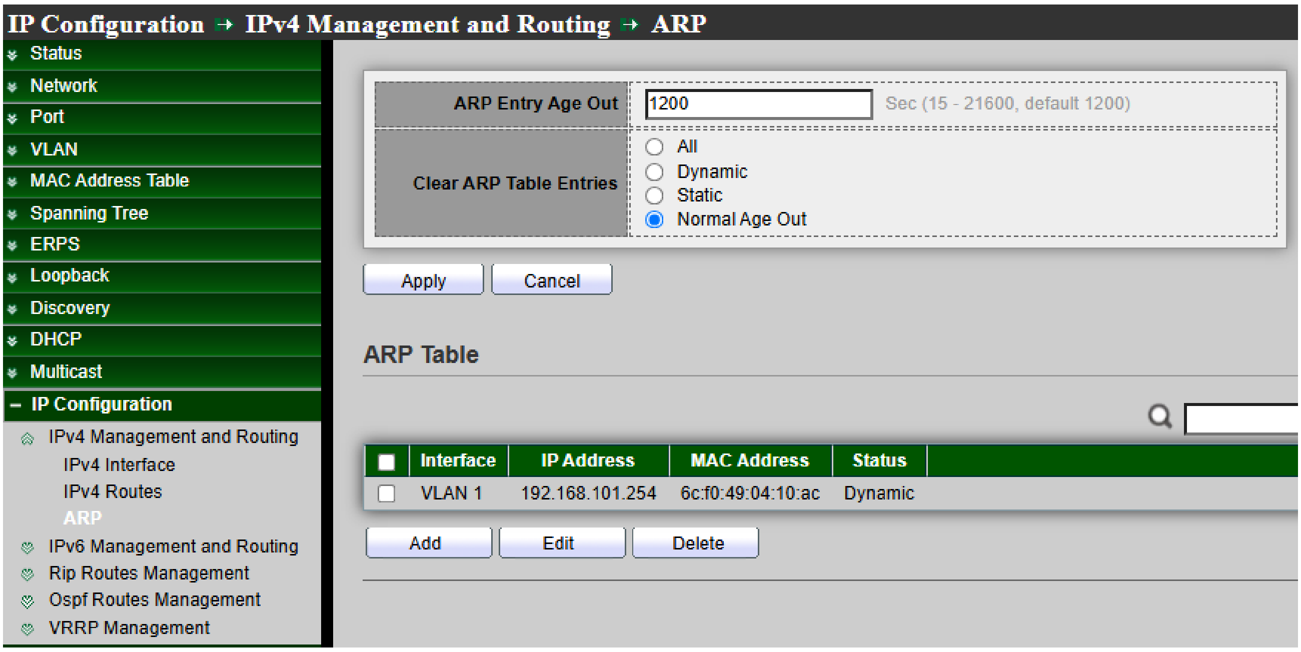
14.1.3 ARP

ARP (Address Resolution Protocol, Address Resolution Protocol) is a protocol that resolves an IP address into an Ethernet MAC address (or physical address). In a local area network, when a host or other network device has data to send to another host or device, it must know the other party's network layer and IP address. But just having an IP address is not enough, because IP data must be encapsulated into a frame to be sent through the physical network, so the sending station must also have the physical address of the receiving station, so the address needs to be mapped from the IP to the physical address. ARP is the protocol to achieve this function.

ARP table (ARP Cache page)

After the device resolves the destination MAC address through ARP, it will add an IP address-to-MAC address mapping entry in its own ARP table for subsequent data forwarding to the same destination. ARP table are divided into “dynamic ARP table” and “static ARP table”.

Use the **ARP Table** (ARP Cache page) to view entries in the table, a table of the remote connections most recently seen by this switch.



ARP Entry Age Out	1200 Sec (15 - 21600, default 1200)
Clear ARP Table Entries	○ All ○ Dynamic ○ Static ● Normal Age Out

ARP Table

□	Interface	IP Address	MAC Address	Status
□	VLAN 1	192.168.101.254	6c:f0:49:04:10:ac	Dynamic

- **ARP Entry Age Out :** The setting of ARP aging time can be set from 15 seconds to 21600 seconds, and the default is 1200 seconds.
- **Clear ARP Table Entries :** Administrator can configure this “ARP Table for Clean ARP Table Entries by “All” and “Dynamic” and “Static” and by “Normal Age Out” (ARP aging set time) management.

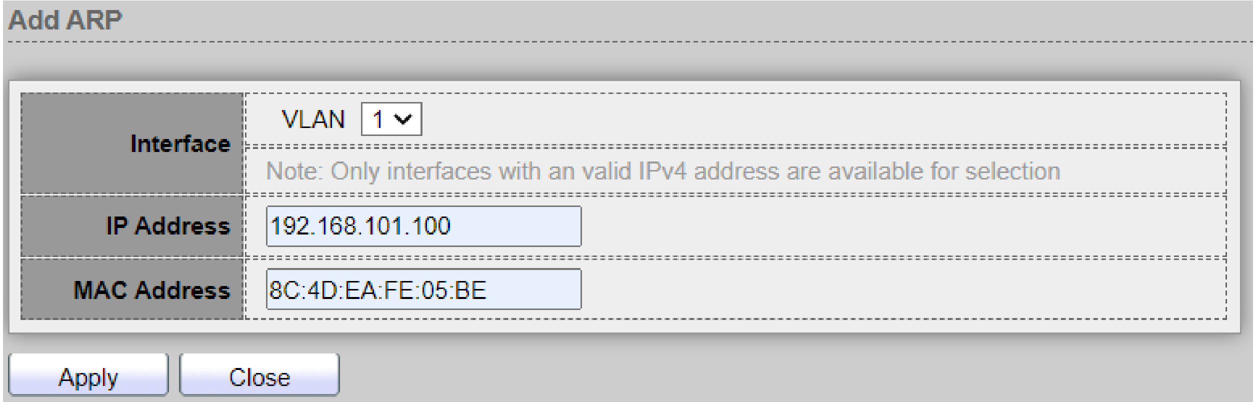
Note	1. Dynamic ARP Table : Dynamic ARP Table are automatically generated and maintained by the ARP protocol through ARP aging-out time , and can be outdated and invalid, updated by new ARP table , or overwritten by static ARP Table. When the invalid time expires and the interface is disabled, the corresponding dynamic ARP Table will be deleted automatically. 2. Static ARP Table : Static ARP Table are manually configured and maintained, and will not be invalidated or overwritten by dynamic ARP Table.

*Click the **"Apply"** button to save your changes or "**Cancel**" the button to cancel settings.*

ARP Table

Administrator can configure this "ARP "page setting for **"add"** and "Edit" and **"Delete"** function management.

Field	Description
Interface	The routing interface associated with the ARP entry.
IP Address	Displays the IP address of the device (on a subnet) that is attached an existing routing interface of the switch.
MAC Address	Displays the unicast MAC address of the attached device. The address is six two-digit hexadecimal numbers separated by colons, for example, 40:bo:34:54:97:82
Status	The type of ARP entry. Possible values are as follows: • **Local :** An ARP entry associated with one of the switch's routing interface's MAC addresses. • **Gateway :** A dynamic ARP entry whose IP address is that of a router. • **Static :** An ARP entry that was manually configured. • **Dynamic :** An ARP entry that was learned by the router.



Add ARP

Interface	VLAN 1 Note: Only interfaces with an valid IPv4 address are available for selection
IP Address	192.168.101.100
MAC Address	8C:4D:EA:FE:05:BE

- **Interface :** Administrator can select VLAN interface.
- **IP Address :** Enter the IPv4 address of add ARP table.
- **MAC Address :** Enter the MAC address of add ARP table.

Note	Configuring a static ARP table can improve communication security. Static ARP Table restricts the use of specified MAC addresses when communicating with devices with specified IP addresses. At this time, the harmful network transmission cannot modify the mapping relationship between the IP address and the MAC address of the entry, so as to protect the communication between the device and the specified device. Normal communication.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

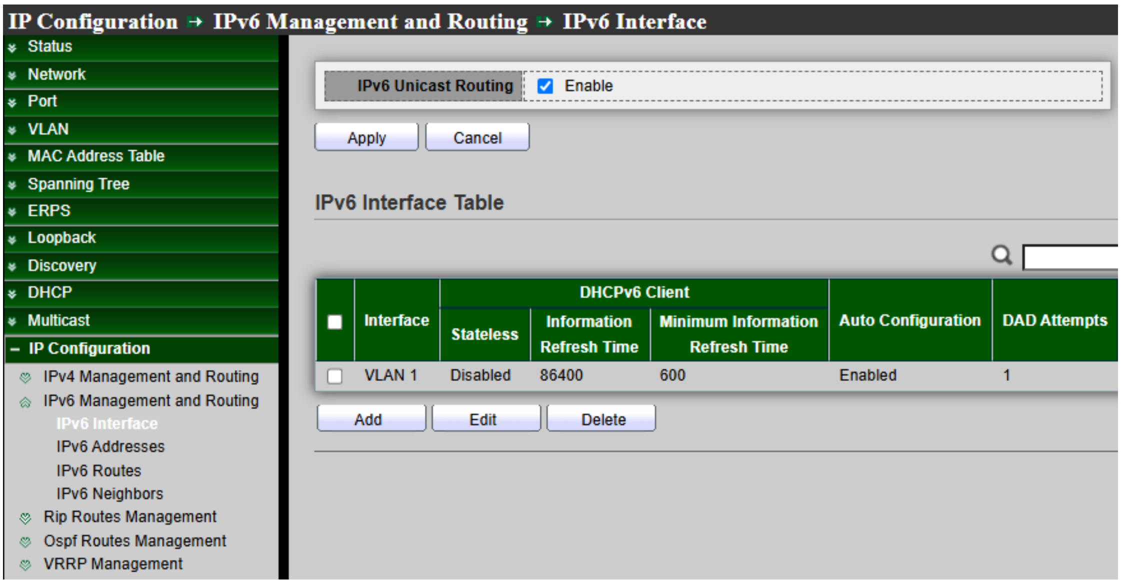
14.2 IPv6 Management and Interfaces

This chapter describes how to configure the IP interface for management access
Switch over the network. The switch supports IP version 4 and version 6,
And can be managed simultaneously by any of these address types. You can manually configure specific IPv4 or IPv6 addresses, or instruct the switch to obtain an IPv4 address from a BOOTP or DHCP server. An IPv6 address can only be configured manually.

IPv6 Configuration – Set the IPv6 address for management access.

14.2.1 IPv6 Interface

Administrator can configure this "IPv6 Interface Table "page setting for **"add"** and "Edit" and **"Delete"** function management.



IP Configuration → IPv6 Management and Routing → IPv6 Interface

IPv6 Unicast Routing ☑ Enable

IPv6 Interface Table

☐	Interface	DHCPv6 Client			Auto Configuration	DAD Attempts
		Stateless	Information Refresh Time	Minimum Information Refresh Time		
☐	VLAN 1	Disabled	86400	600	Enabled	1

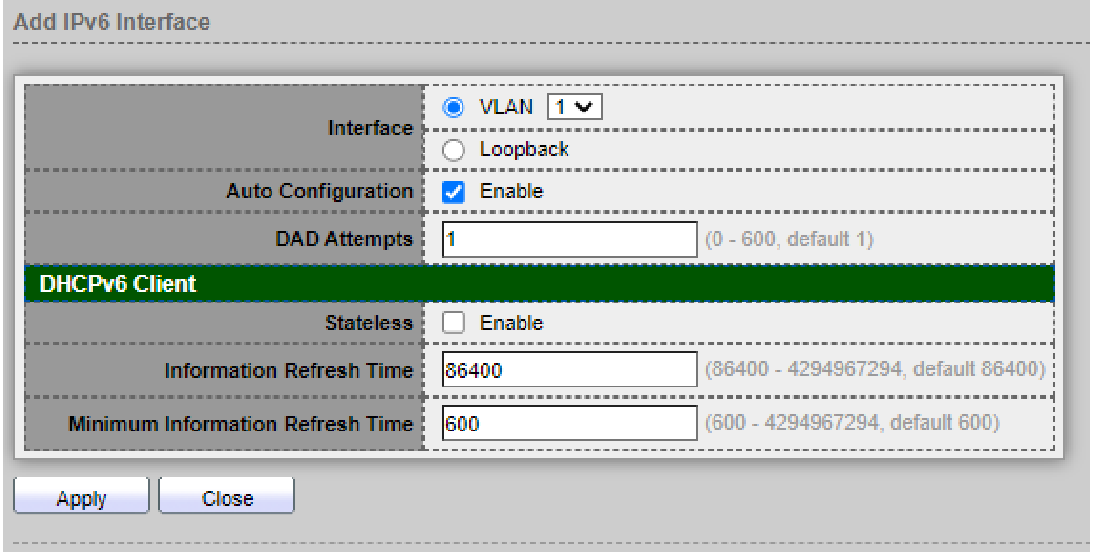
IPv6 Unicast Routing : Administrator can configure “Enable” this IPv6 Unicast Routing function.

Note	Next to IPv6 Unicast Routing, specify whether IPv6 unicast routing is globally enabled by selecting the Enable radio button or the Disable radio button.

*Click the **“Apply”** button to save your changes or “**Cancel**” the button to cancel settings.*

Select the type of the IPv6 interface through which the IPv6 packets are forwarded.
The Switch supports the VLAN interface type and Loopback interface type .

<u>Configuration” Interface” setting on “VLAN“ :</u>



Add IPv6 Interface

Interface	● VLAN 1 ○ Loopback
Auto Configuration	☑ Enable
DAD Attempts	1 (0 - 600, default 1)
DHCPv6 Client	
Stateless	☐ Enable
Information Refresh Time	86400 (86400 - 4294967294, default 86400)
Minimum Information Refresh Time	600 (600 - 4294967294, default 600)

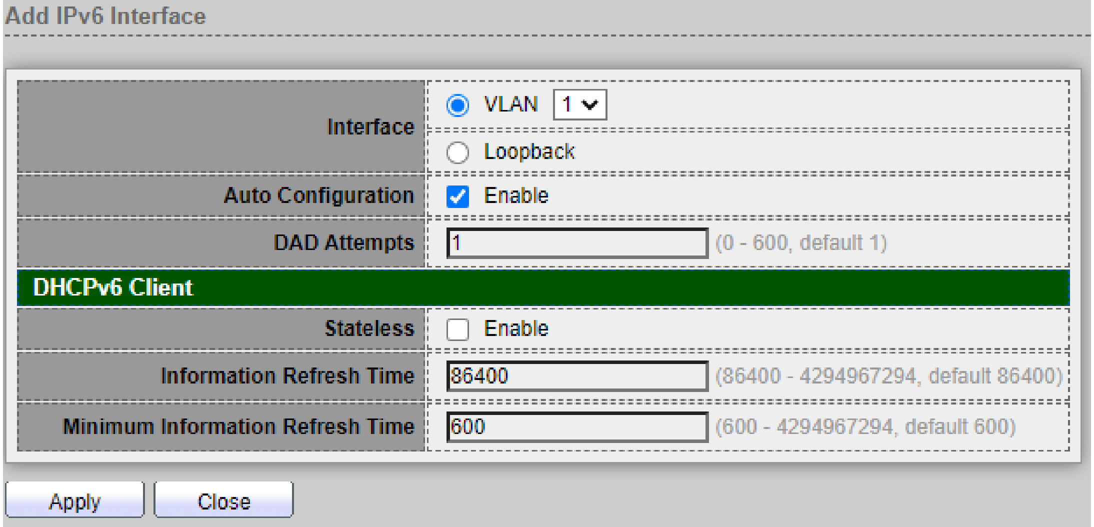
- **Auto Configuration :** The IPv6 address autoconfiguration automatically creates new IPv6 interfaces for a given line description, and assigns IPv6 addresses for the interfaces.
- **DAD Attempts :** Configures the number of neighbor solicitations to be sent when performing duplicate address detection (DAD) for a unicast address configured on an interface. The no form of this command sets the number of attempts to the default value.

DHCP6 Client :

- **Stateless :** IPv6 stateLess AddressAutoConfiguration(SLAAC) function
- **Information Refresh Time :** 86400 by default
- **Minimum Information Refresh Time :** 600 by default

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

<u>Configuration" Interface" setting on "Loopback" :</u>



Add IPv6 Interface

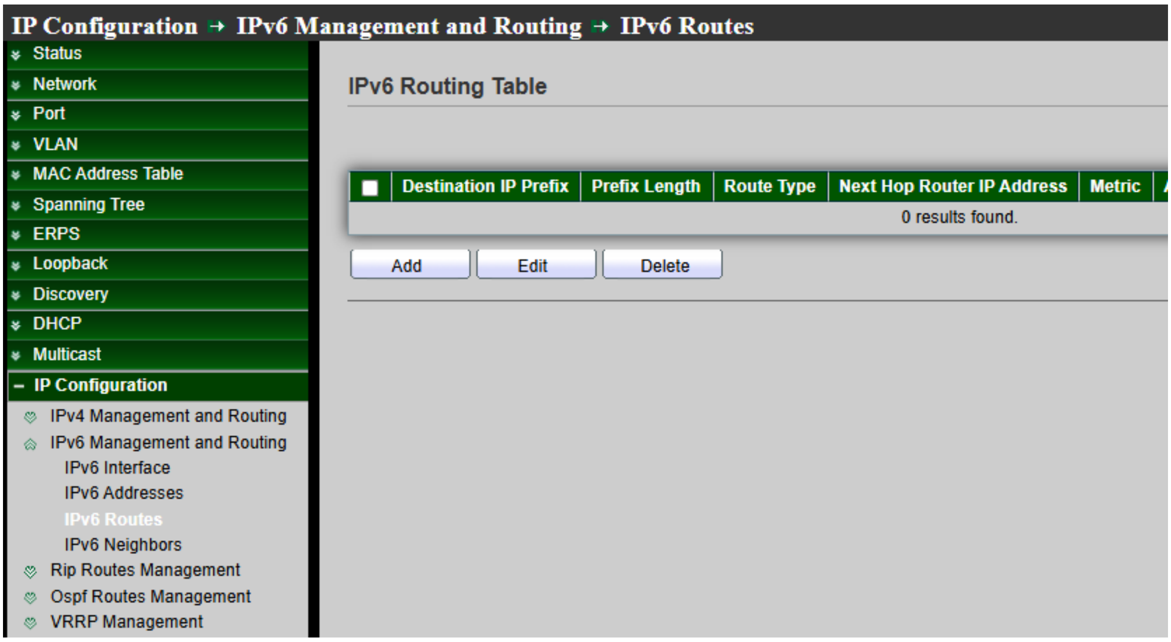
Interface	● VLAN 1 ○ Loopback
Auto Configuration	☑ Enable
DAD Attempts	1 (0 - 600, default 1)
DHCPv6 Client	
Stateless	□ Enable
Information Refresh Time	86400 (86400 - 4294967294, default 86400)
Minimum Information Refresh Time	600 (600 - 4294967294, default 600)

Loopback : The loopback address may be used by a node to send an IPv6 packet to itself.
It must not be assigned to a physical or virtual interface.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

14.2.2 IPv6 Addresses

Administrator can configure this "IPv6 Address Table "page setting for **"add"** and **"Delete"** function management.



IP Configuration → IPv6 Management and Routing → IPv6 Routes

IPv6 Routing Table

□	Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address	Metric
0 results found.					

IPv6 Address Table

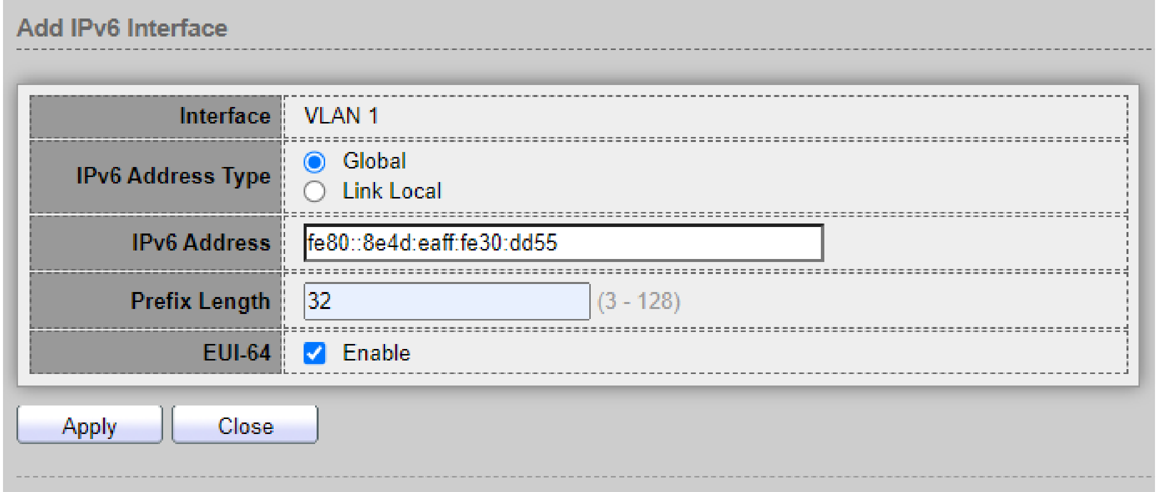
- **Interface :** From the Interface menu, Administrator can select the VLAN for the IPv6 Interface Selection page displays. The page also shows the IPv6 Interface Configuration table.

Field	Description
IPv6 Address Type	The IP Prefix for the destination
IPv6 Address	The prefix length for the active route.
IPv6 Prefix Length	The type of route: Static or Dynamic, depending on how the route was added.
DAD status	Shows the state of the IPv6 address. The state can be one of the following • **Tent :** Routing is disabled or the address does not work because of a “duplicate address detection” (DAD) condition**.** • **Active :** The IPv6 address is valid and active. • **Preferred :** The IPv6 address was verified to be unique, valid, and active.

Select the type of the IPv6 Address through which the IPv6 format are use.

The Switch supports the Global type and Link Local type .

<u>Configuration" IPv6 Address Type" setting on "Global " :</u>



Add IPv6 Interface

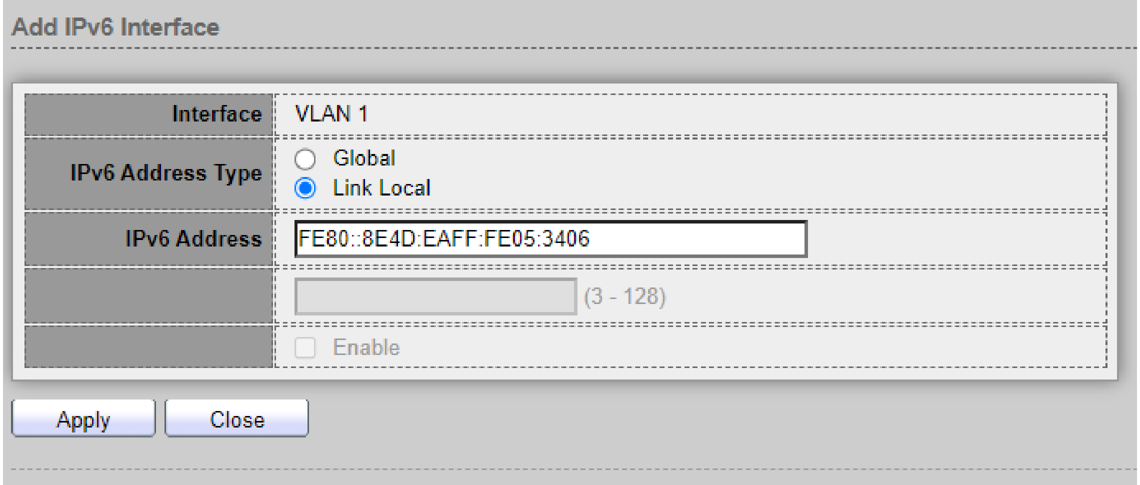
Interface	VLAN 1
IPv6 Address Type	● Global ○ Link Local
IPv6 Address	fe80::8e4d:eaff:fe30:dd55
Prefix Length	32 (3 - 128)
EUI-64	☑ Enable

- **IPv6 Address Type :**
  - **Global :** Configures an IPv6 global unicast address with a full IPv6 address including the network prefix and host address bits, followed by a forward slash, and a decimal value indicating how many contiguous bits of the address comprise the prefix.
  - **Link Local :** Configures an IPv6 link-local address. The address prefix must be in the range of FE80 to FEBF. and you can configure only one link-local address per interface.(The specified address replaces a link-local address that was automatically generated for the interface).
- **IPv6 Address :** Full in your IPv6 address . Example of IPv6 input network range: 2001: 8E4D: EAFF: FE01: 0000: 0000: 0000: 0002 ~ FFFF: FFFF: FFFF: FFFE. (For IPv6 IP acquisition, May please contact your ISP provider).
- **Prefix Length :** The Prefix Length of the IPv6 address of the Switch .
- **EUI-64 :** Use this section to tick the Enable for EUI-64 format IPv6 configuration, Configures an IPv6 address for an interface using an EUI-64 interface ID in the low order 64 bits.

Note	The switch must be configured with a link-local address. Therefore, any configuration process that enables IPv6 functionality, including address auto configuration, explicitly enabling IPv6 or manually assigning a global unicast address will also automatically generate a link-local unicast address. The prefix length for a link local address is fixed at 64 bits, and the host portion of the default address is based on the modified EUI-64 (Extended Universal Identifier) form of the interface identifier.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

<u>Configuration" IPv6 Address Type" setting on "Link Local" :</u>



Add IPv6 Interface

Interface	VLAN 1
IPv6 Address Type	○ Global ● Link Local
IPv6 Address	FE80::8E4D:EAFF:FE05:3406
	(3 - 128)
	□ Enable

- **IPv6 Addrress :** This section uses the Link Local address of the local identifier interface required by the IPv6 mode address operation specification, for example, it is as "FE80::8E4D:EAFF:FE05:3406".

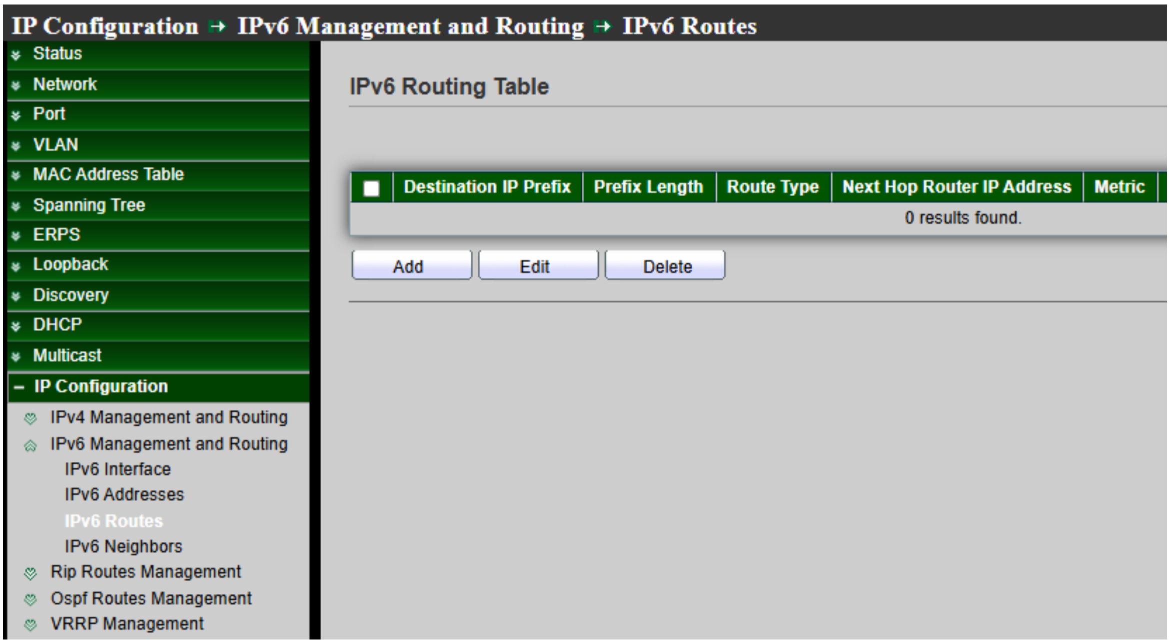
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

14.2.3 IPv6 Routes

You can enter static routes in the routing table using the IP > Static Routes (Add) page. Static routes may be required to force the use of a specific route to a subnet. Static routes do not automatically change in response to changes in network topology , so you should only configure a small number of stable routes to ensure network

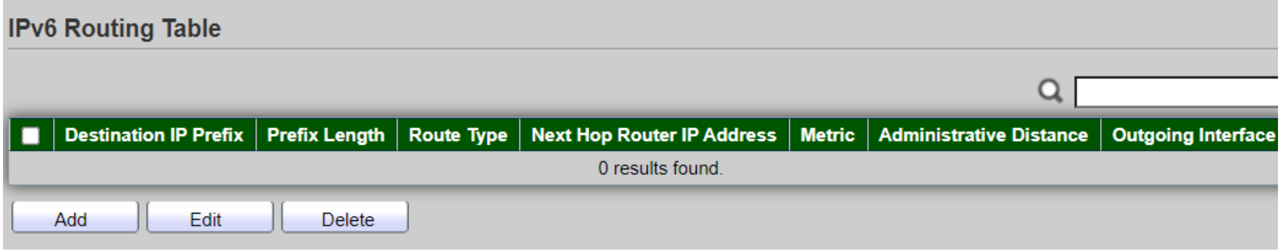
This page system can displayed IPv6 Routing Table for "Destination IP Prefix" / Prefix Length / Route Type / Next Hop Router IP Address / Metric / Administrative Distance / Outgoing Interface information.

Administrator can configure this "IPv6 Routing Table" page setting for **"add"** and "Edit" and **"Delete"** function management.



IPv6 Routing Table

□	Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address	Metric
0 results found.					

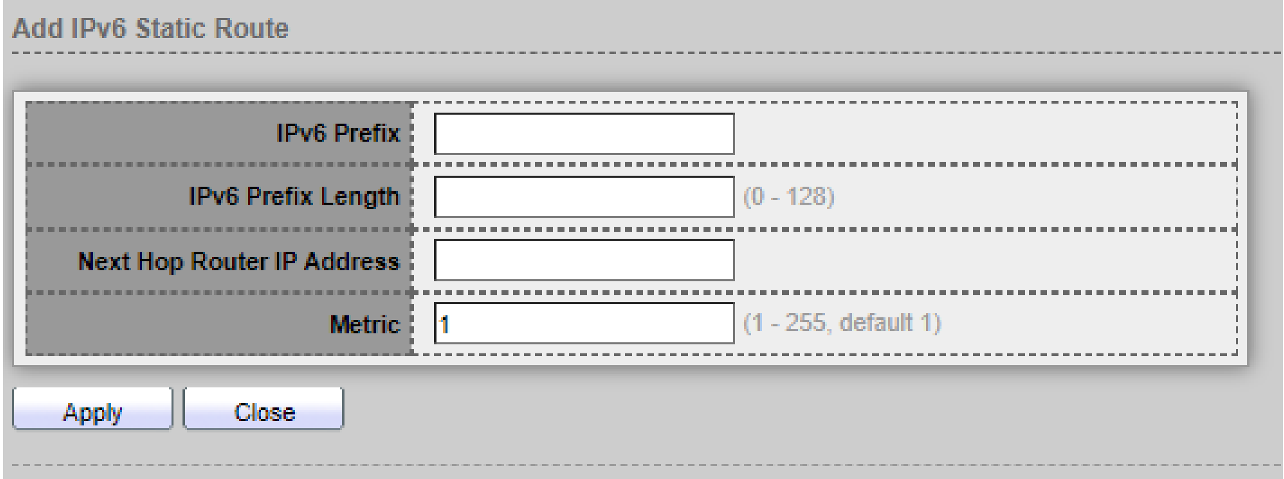


IPv6 Routing Table

□	Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address	Metric	Administrative Distance	Outgoing Interface
0 results found.							

Field	Description
Destination IP Prefix	The IP Prefix for the destination
Prefix Length	The prefix length for the active route.
Route Type	The type of protocol for the active route: • Static. The route was manually defined. • ND (Neighbor Discovery). The route was discovered through the ND protocol. • Connected. The route was derived from a manually configured IPv6 address.
Next Hop Router IP Address	The next hop IPv6 address for the active route.

Metric	The Metric value for the configured next hop. Specify the Metric (sometimes called administrative distance), which is an integer value from 1 to 255.
Administrative Distance	The route administrative distance of the configured route.
Outgoing Interface	The outgoing interface of the route active or inactive.



Add IPv6 Static Route

IPv6 Prefix	
IPv6 Prefix Length	(0 - 128)
Next Hop Router IP Address	
Metric	1 (1 - 255, default 1)

- **IPv6 Prefix :** In the IPv6 Prefix field, specify the IPv6 network prefix for the destination..
- **IPv6 Prefix Length :** In the IPv6 Prefix Length field, specify the IPv6 prefix length for the destination..
- **Next Hop Router IP Address :** In the Next Hop IPv6 Address field, specify the outgoing router IPv6 address to use when forwarding traffic to the next router (if any) in the path toward the destination.

Note	The next router is always one of the adjacent neighbors or the IPv6 address of the local interface for a directly attached network.

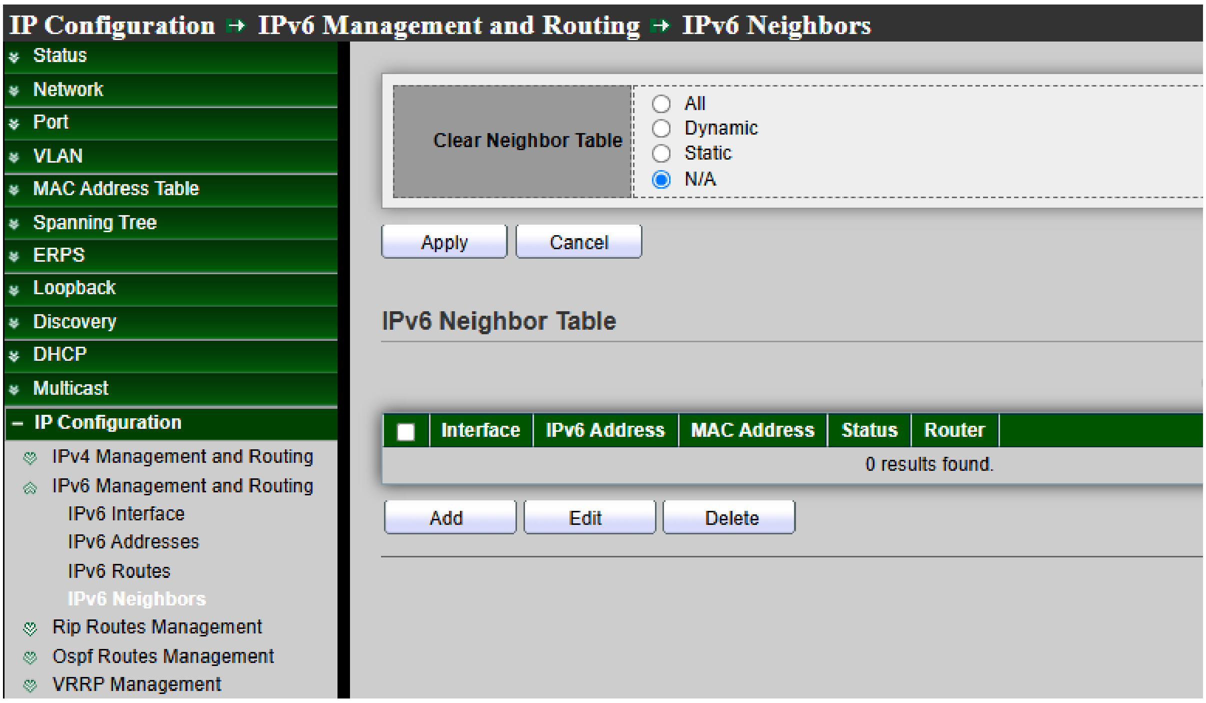
- **Metric :** Please fill in the cost (hop count) of transmission you want to apply for routing purposes.

Note	This metric represents the "cost" of transmission for routing purposes. IP routing uses "hop count" as a measure of cost, with a minimum value of 1 for directly connected networks. Enter a number that approximates the cost of this link. The number does not need to be exact, but must be between 1 and 255. In fact, 1 or 2 or 3 is usually suggested here to fill in the frequently used numbers.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

14.2.4 IPv6 Neighbors

Administrator can configure this “IPv6 Neighbor Table “page setting for **“add”** and “Edit” and **“Delete”** function management.

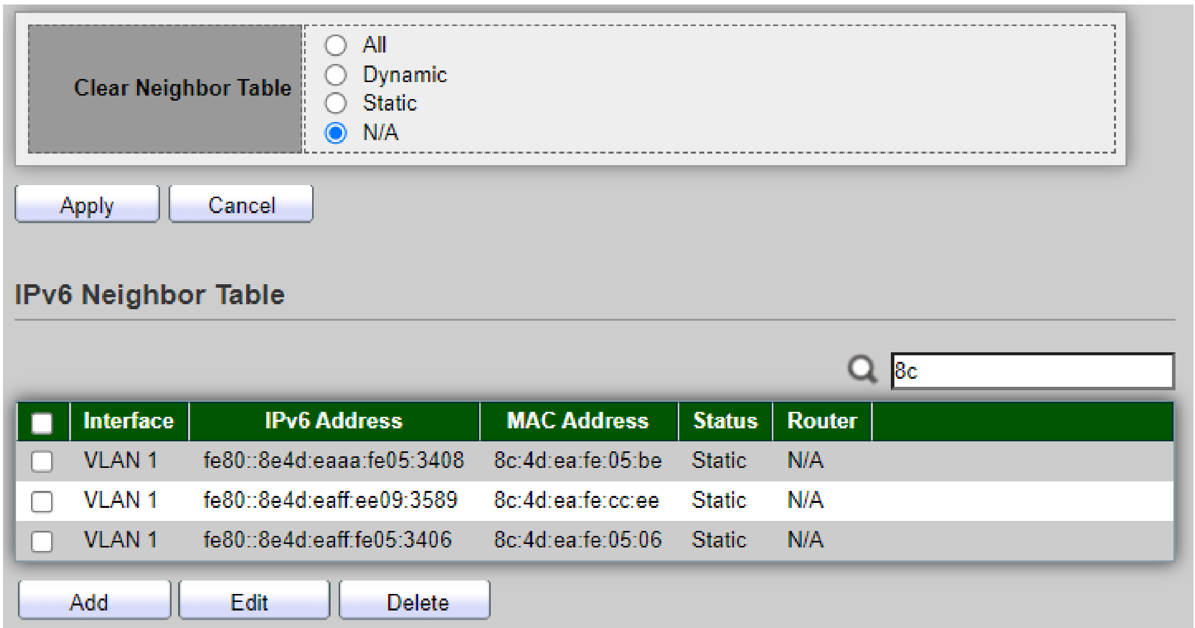


Clear Neighbor Table: ○ All ○ Dynamic ○ Static ● N/A

IPv6 Neighbor Table

□	Interface	IPv6 Address	MAC Address	Status	Router

0 results found.



Clear Neighbor Table: ○ All ○ Dynamic ○ Static ● N/A

IPv6 Neighbor Table

Search: 8c

□	Interface	IPv6 Address	MAC Address	Status	Router
□	VLAN 1	fe80::8e4d:eaaa:fe05:3408	8c:4d:ea:fe:05:be	Static	N/A
□	VLAN 1	fe80::8e4d:eaff:ee09:3589	8c:4d:ea:fe:cc:ee	Static	N/A
□	VLAN 1	fe80::8e4d:eaff:fe05:3406	8c:4d:ea:fe:05:06	Static	N/A

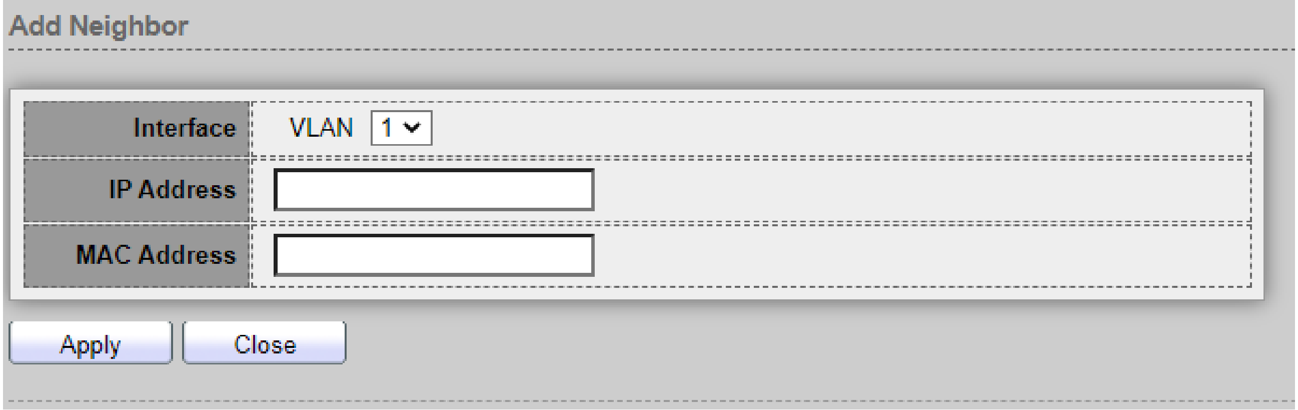
Clear Neighbor Table

The administrator can select the filter Status type including by “All” or “Dynamic” or “Static” or “N/A “to quickly select batches to clear the "IPv6 Neighbor Table".

Use the "Search" menu to consult the list.

Search by "Keyword" using the Search menu and field. For example, '8c'. Then click the Search icon button. If the address exists, show the entry.

Field	Description
Interface	The interface whose settings are displayed in the current table row. This field displays the ID number of the IPv6 interface on which the IPv6 address is created or through which the neighboring device can be reached.
IPv6 Address	The IPv6 address of the neighbor or interface.
MAC Address	This field displays the MAC address of the IPv6 interface on which the IPv6 address is configure or the MAC address of the neighboring device.
Status	The state of the neighbor cache entry. The states for "dynamic entries" or "Static entries"in the IPv6 neighbor discovery cach.
Router	Neighbor for the active route.


Add Neighbor

Interface	VLAN 1
IP Address	
MAC Address	

- **Interface :** Select the type of IPv6 interface for VLAN ID configure.
- **IP Address :** Specify the IPv6 address of the neighboring device which can be reached through the interface.
- **MAC Adderss :** Specify the MAC address of the neighboring device which can be reached through the interface.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

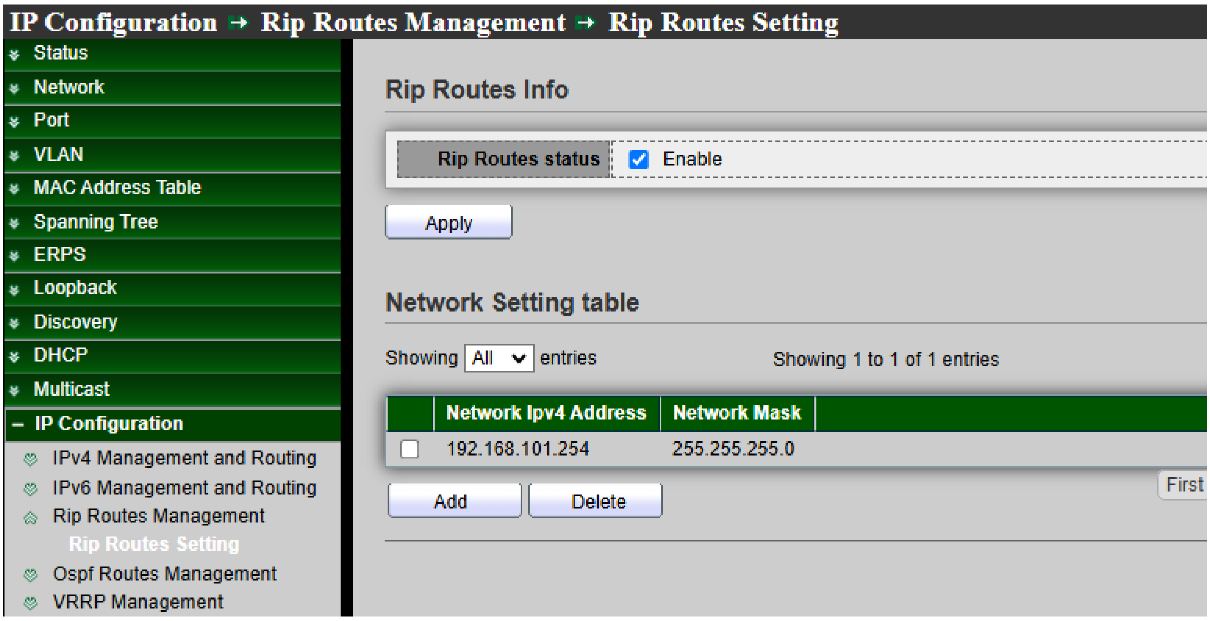
14.3 RIP Routes Setting

This Switch IPv4 routing, Support versions of RIPv2. and RIP v2 uses multicast to send routing table updates.Routing Information Protocol (RIP) is used to manage router information in a self-contained network, such as a corporate LAN or a private WAN. With RIP, a gateway host sends its routing table to the closest router each 30 seconds. This router, then sends the contents of its routing tables to neighboring routers.

RIP is best for small networks. This is because the transmission of the full routing table each 30 seconds can put a large traffic load on the network, and because RIP tables are limited to 15 hops. So, OSPF is a better alternative for larger networks.

14.3.1 Rip Routes Setting

Administrator can configure Enable or disable for this “Rip Routes status“ management.



IP Configuration → Rip Routes Management → Rip Routes Setting

Rip Routes Info

Rip Routes status ☑ Enable

Network Setting table

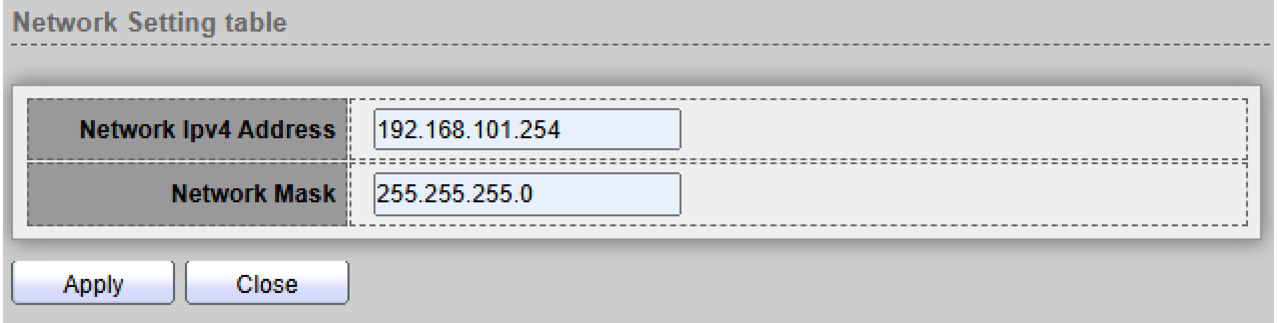
Showing All entries   Showing 1 to 1 of 1 entries

	Network Ipv4 Address	Network Mask
□	192.168.101.254	255.255.255.0

Administrator can configure this “Rip Routes Info “page setting for **“add”** and **“Delete”** table management.

Field	Description
Network IPv4 Address	Displays the routing IPv4 IP address to be added to the advertised RIP v2 protocol Routes.

Network Mask	Displays the routing mask to be added to the advertised RIP v2 protocol Routes.



Network Setting table

Network Ipv4 Address	192.168.101.254
Network Mask	255.255.255.0

- **Network IPv4 Address :** The IPv4 address to be announced to visit the Routing RIP v2 protocol.
- **Network Mask :** The Mask to be announced to visit the Routing the Routing RIP v2 protocol.

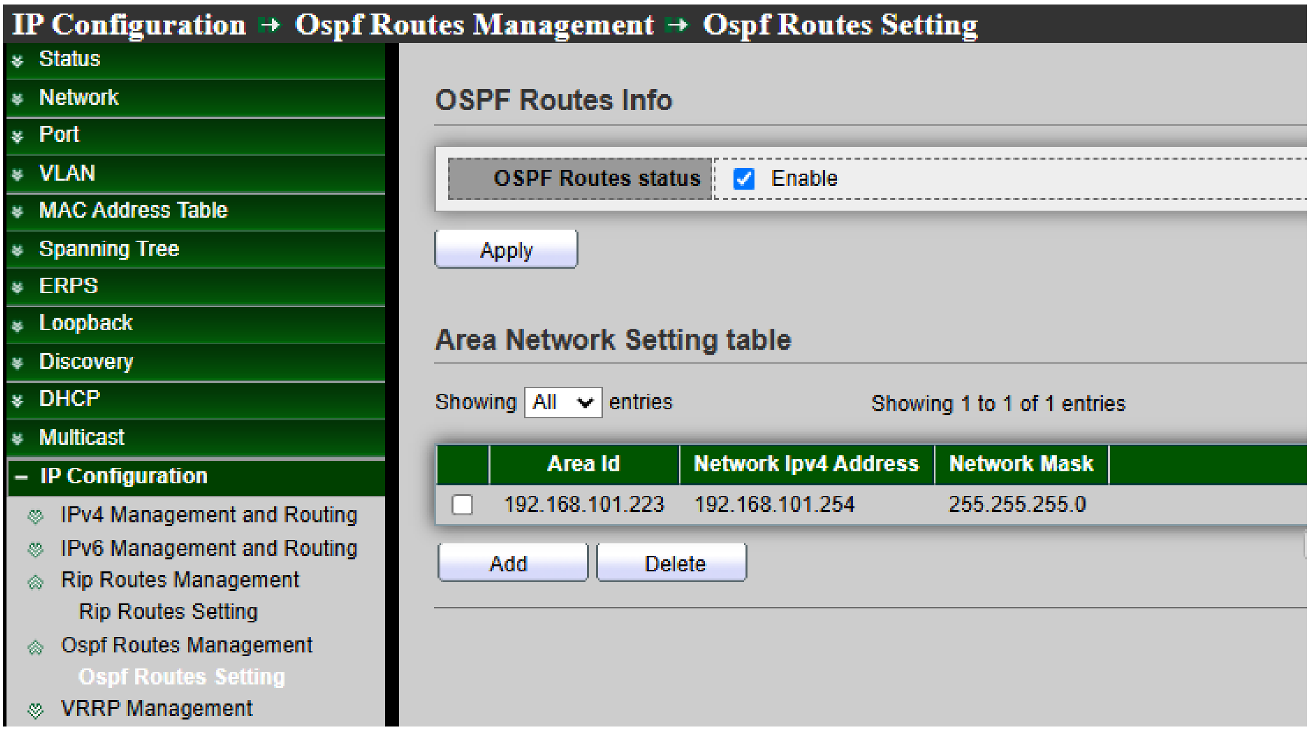
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

14.4 OSPF Routes Management

On the Areas tab, Add an Area ID for the area in x.x.x.x format. This is the identifier that each neighbor must accept to be part of the same area.OSPF determines routes dynamically by obtaining information from other routers and advertising routes to other routers by way of Link State Advertisements (LSAs). The router keeps information about the links between it and the destination and can make highly efficient routing decisions. A cost is assigned to each router interface, and the best routes are determined to be those with the lowest costs, when summed over all the encountered outbound router interfaces and the interface receiving the LSA.
Hierarchical techniques are used to limit the number of routes that must be advertised and the associated LSAs. Because OSPF dynamically processes a considerable amount of route information, it has greater processor and memory requirements than does RIP.

14.4.1 Ospf Routes Setting

Administrator can configure Enable or disable for this "OSPF Routes status " management.



IP Configuration → Ospf Routes Management → Ospf Routes Setting

OSPF Routes Info

OSPF Routes status ☑ Enable

Area Network Setting table

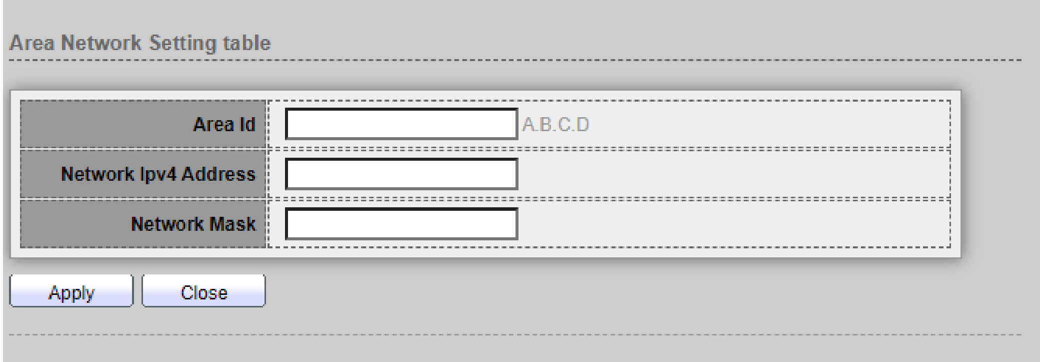
Showing All entries

Showing 1 to 1 of 1 entries

	Area Id	Network Ipv4 Address	Network Mask
□	192.168.101.223	192.168.101.254	255.255.255.0

Administrator can configure this “OSPF Routes Info “page setting for **“add”** and **“Delete”** table management.

Field	**Description**
Area Id	Displays the routing Area Id of A,B,C,D to be added to the advertised OSPF v2 protocol Routes, On the Areas tab, Add an Area ID for the area in x.x.x.x format. This is the identifier that each neighbor must accept to be part of the same area.
Network IPv4 Address	Displays the routing IPv4 IP address to be added to the advertised OSPF v2 protocol Routes.
Network Mask	Displays the routing mask to be added to the advertised OSPF v2 protocol Routes.



Area Network Setting table

Area Id	A.B.C.D
Network Ipv4 Address	
Network Mask	

- **Ared Id :** The Ared Id of A,B,C,D to be announced to visit the Routing OSPF v2 protocol.
- **Network IPv4 Address :** The IPv4 address to be announced to visit the Routing OSPF v2 protocol.
- **Network Mask :** The Mask to be announced to visit the Routing the Routing OSPF v2 protocol.

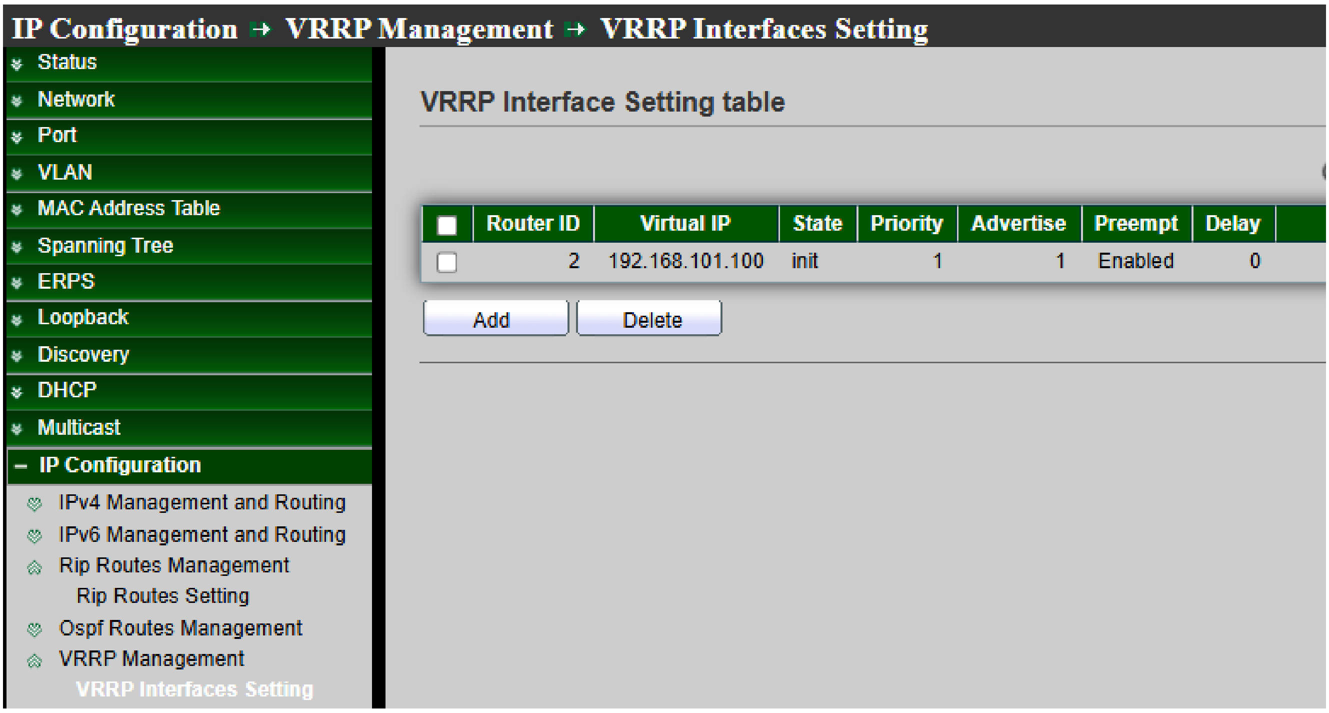
*Click the **“Apply”** button to save your changes or **“Close”** the button to close settings.*

14.5 VRRP Management

VRRP creates a virtual router, known as a default gateway, which acts as a backup if the main router fails. The master router sends out advertisements at regular intervals. Backup routers monitor these advertisements to determine the status of the master router. If the master router fails, the backup router with the highest priority becomes the new master router,
The Virtual Router Redundancy V2 Protocol (VRRP) is a computer networking protocol that increases the availability of the default gateway servicing hosts on a wireless LAN. This protocol operates by establishing a virtual router, an abstract representation of multiple routers acting as a group. The group presents itself as a single default gateway to the hosts on the subnet.
The virtual router’s member possessing the highest priority becomes the master and forwards packets sent to the virtual router’s IP address. The remaining members operate in standby, ready to take over should the master become unavailable. Thus, the Virtual Router Redundancy Protocol enhances network reliability through router redundancy.

14.5.1 VRRP Interfaces Setting

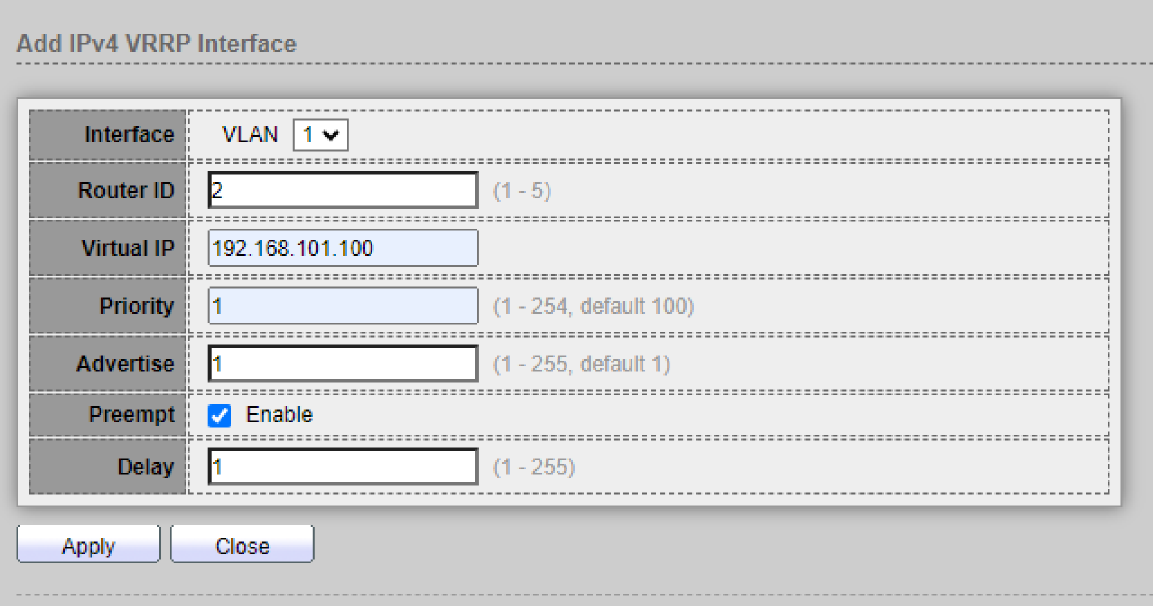
Administrator can configure this “VRRP Interface Setting“page setting for **“add”** and **“Delete”** function management.



VRRP Interface Setting table

□	Router ID	Virtual IP	State	Priority	Advertise	Preempt	Delay
□	2	192.168.101.100	init	1	1	Enabled	0

Field	Description
Router Id	Displays the ID number of the virtual router.
Virtual IP	Displays the IP address and of an IP routing domain that is associated to a virtual router.
State	Displays the status of the virtual router. ● **Master:** This switch functions as the master router. ● **Backup:** This switch functions as a backup router. ● **Init:** This Switch is initiating the VRRP protocol or when the Uplink Status field displays Dead.
Priority	Displays the Switch Virtual Router Redundancy Protocol (VRRP) priority level (1 to 255) of the entry.
Advertise	Displays the Switch Virtual Router Redundancy Protocol (VRRP) Advertisement Interval.
Preempt	Displays the Switch Virtual Router Redundancy Protocol (VRRP) preempt Enable or Disable status.
Delay	Displays the Switch Virtual Router Redundancy Protocol (VRRP) preempt Preempt delay time.



Add IPv4 VRRP Interface

Interface	VLAN 1
Router ID	2 (1 - 5)
Virtual IP	192.168.101.100
Priority	1 (1 - 254, default 100)
Advertise	1 (1 - 255, default 1)
Preempt	☑ Enable
Delay	1 (1 - 255)

- **Interface :** Select a VLAN interface.
- **Router ID :** Select a virtual router number (1 to 5) for which this VRRP entry is created. You can configure up to five virtual routers for one network..
- **Virtual IP :** Enter the IP address of the virtual router .
- **Priority :** Enter a number (between 1 and 254) to set the priority level. The bigger the number, the higher the priority. The default is 100.

Note	Configure the priority level (1 to 254) to set which backup router to take over in case the master router goes down. The backup router with the highest priority will take over..

- **Advertise :** Specify the number of seconds between Hello message transmissions. The default is 1. All routers participating in the virtual router must use the same advertisement Interval.

Note	The master router sends out Hello messages to let the other backup routers know that it is still up and running. The time interval between sending the Hello messages is the advertisement interval.

- **Preempt :** Select this option to activate preempt mode.
- **Delay :** Enter a delay time (between 1 and 255) .

Note	If the master router is unavailable, a backup router assumes the role of the master router. However, when another backup router with a higher priority joins the network, it will preempt the lower priority backup router that is the master. Disable preempt mode to prevent this from happening. A layer 3 device with the same IP address as the virtual router will become the master router regardless of the preempt mode.

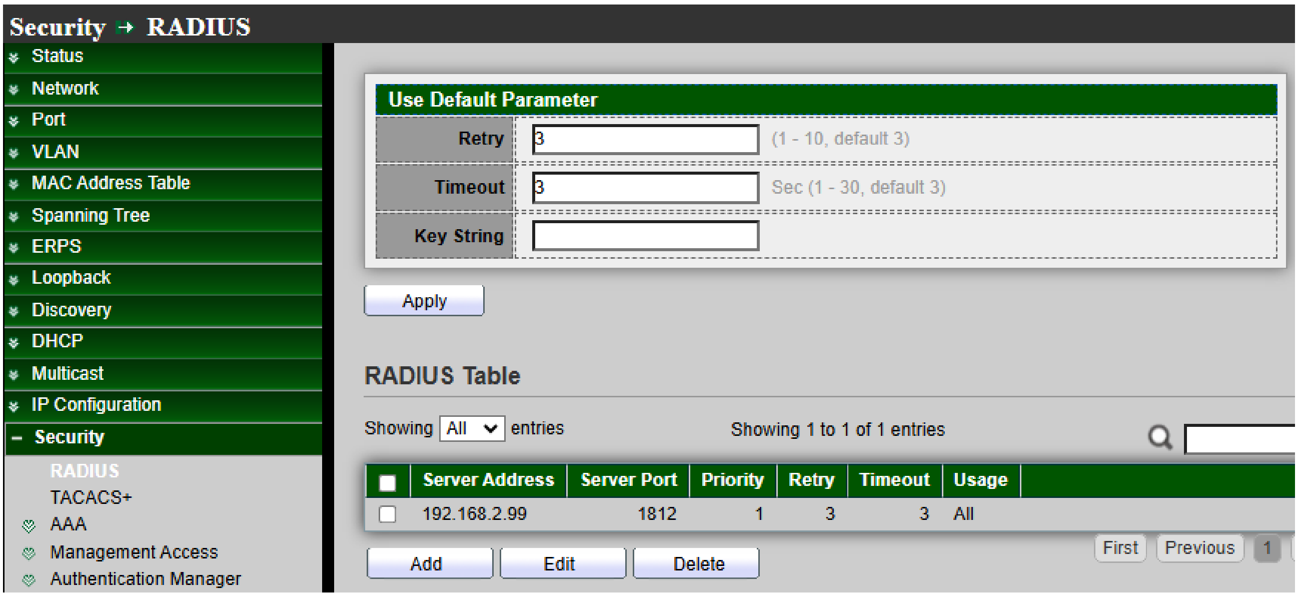
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

15. Security

15.1 RADIUS

Network architecture can establish a Remote Authorization login Service (RADIUS) server to provide a centralized 802.1X or MAC-based network access control for all of its devices. This switch can act as a RADIUS client that uses the RADIUS server to provide centralized security and authorization and user authentication.

Administrator can set account for the switch on the RADIUS server, and configure that RADIUS server along with the other parameters on the RADIUS page.



Use Default Parameter

Retry	3	(1 - 10, default 3)
Timeout	3	Sec (1 - 30, default 3)
Key String		

RADIUS Table

Showing All entries Showing 1 to 1 of 1 entries

□	Server Address	Server Port	Priority	Retry	Timeout	Usage
□	192.168.2.99	1812	1	3	3	All

- **Use Default Parameters :**

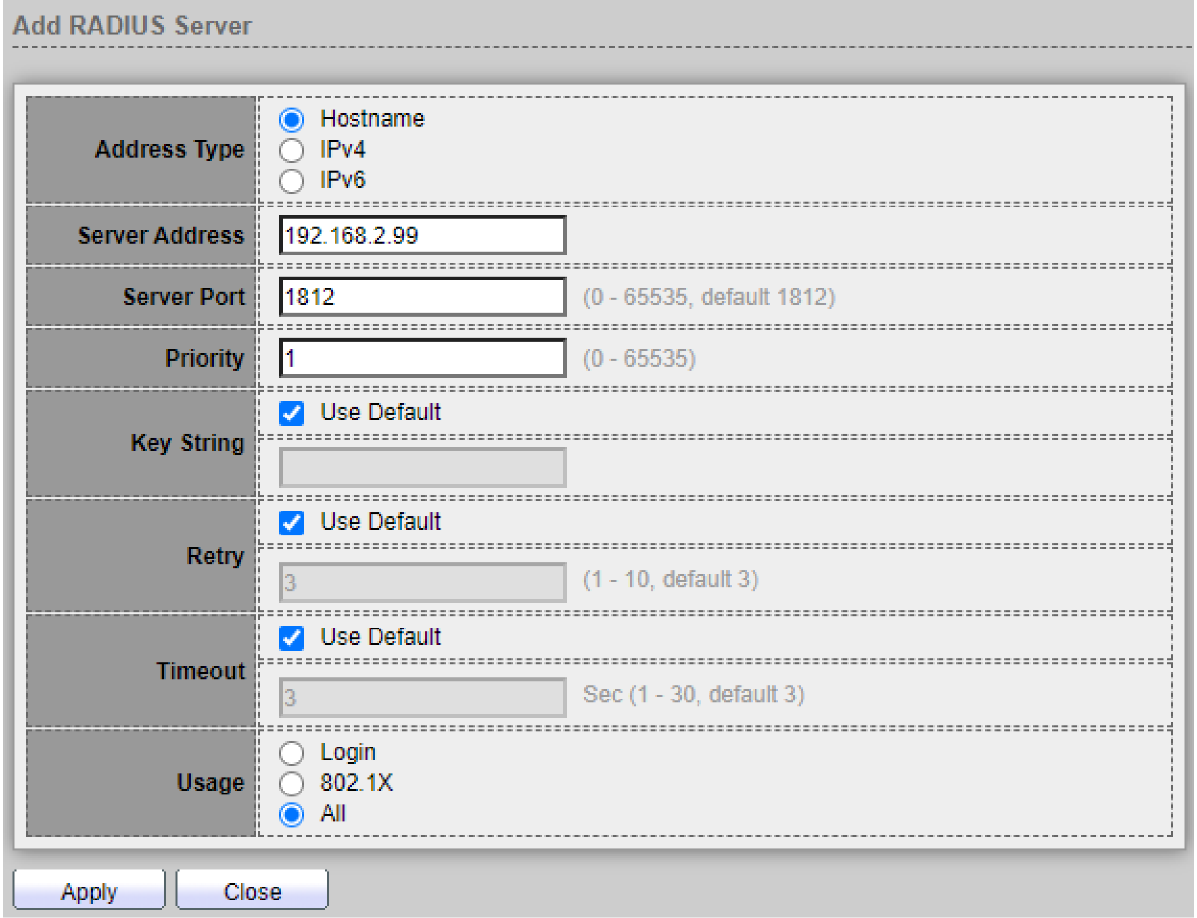
- **Retry:** Set default retry number ,Enter the number of transmitted requests that are sent to the RADIUS server before a failure is considered to have occurred. Default is 3.
- **Timeout:** Set default timeout value ,Enter the number of seconds that the switch waits for

an answer from the RADIUS server before retrying the query, or switching to the next server. Default is 3.

- **Key String:** Set default RADIUS key string ,The key string used security communications between the switch and the RADIUS server by MD5.This key must match the key configured on the RADIUS server. If don't have an encrypted key string (from other device), please enter the key string in plaintext form.

*Click the “**Apply**” button to save your changes settings.*

Field	Description
Server Address	RADIUS server address.
Server Port	RADIUS server port.
Priority	RADIUS server priority (smaller value has higher priority). RADIUS session will try to establish with the server setting which has highest priority. If failed, it will try to connect to the server with next higher priority.
Retry	RADIUS server retry value. If it is fail to connect to server, it will keep trying until timeout with retry times.
Timeout	RADIUS server timeout value. The time that the waits for the RADIUS server to reply before retransmitting or switching to the next server.
Usage	RADIUS server usage type • **Login:** For login authentication. • **802.1x:** For 802.1x authentication. • **All:** For alltypes.



Add RADIUS Server

Address Type	● Hostname ○ IPv4 ○ IPv6
Server Address	192.168.2.99
Server Port	1812 (0 - 65535, default 1812)
Priority	1 (0 - 65535)
Key String	☑ Use Default
Retry	☑ Use Default 3 (1 - 10, default 3)
Timeout	☑ Use Default 3 Sec (1 - 30, default 3)
Usage	○ Login ○ 802.1X ● All

- **Address Type:** Select IP Version 4 / 6 or use Hostname typem, In add dialog, user need to specify server Address Type
  - **Hostname:** Use domain name as server address.
  - **IPv4:** Use IPv4 as server address.
  - **IPv6:** Use IPv6 as server address.
- **Server Address:** Please enter the IP address or hostname of the RADIUS server. In add dialog, user need to input server address based on address type. In edit dialog, it shows current edit server address.
- **Server Port:** Set port of RADIUS server.
- **Priority:** Administrator can enter the priority of the server. The priority determines the order that the switch attempts to contact the servers to authenticate users. The switch first starts with the highest priority server. 0 is the high priority, Set RADIUS server priority (smaller value has higher priority). RADIUS session will try to establish with the server setting which has highest priority. If failed, it will try to connect to the server with next higher priority.
- **Key String:** Administrator can select user defined Encrypted or Plaintext to enter the key string form used for authenticating and encrypting the communication between the switch and the

RADIUS server. This key must match the key configured on the RADIUS server. If administrator select use default (checked in checkbox) will use the default key string.

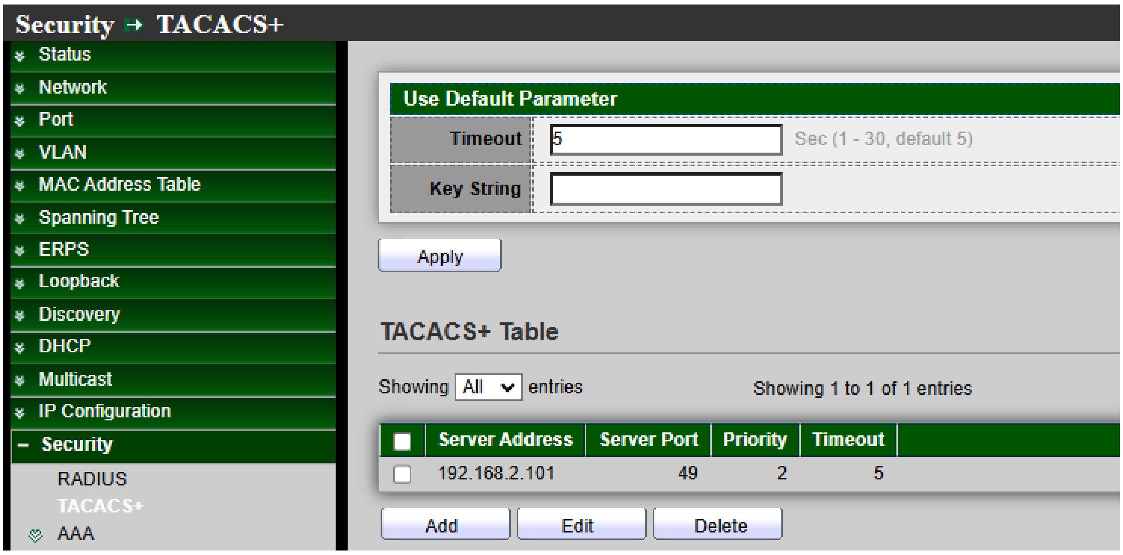
- **Retry:** Select User Defined to enter the number of requests that are sent to the RADIUS server before a failure is considered to have occurred, or select Use Default to use the default value.
- **Timeout:** Select User Defined to enter the number of seconds that the switch waits for an answer from the RADIUS server before retrying the query or switching to the next server, or select Use Default to use the default value.
- **Usage:** Select the RADIUS server authentication type.
  - **Login:** RADIUS server is used for authenticating users that want to administer the switch.
  - **802.1X:** RADIUS server is used for authentication in 802.1X access control.
  - **All:** RADIUS server is used for authenticating user that wants to administer the switch and for authentication in 802.1X access control.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

15.2 TACACS+

Administrator can be configuration TACACS+ to connection TACACS+ Server to provide authentication and authorization for all devices in the organization.

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



Use Default Parameter

Timeout	5	Sec (1 - 30, default 5)
Key String		

TACACS+ Table

Showing All entries Showing 1 to 1 of 1 entries

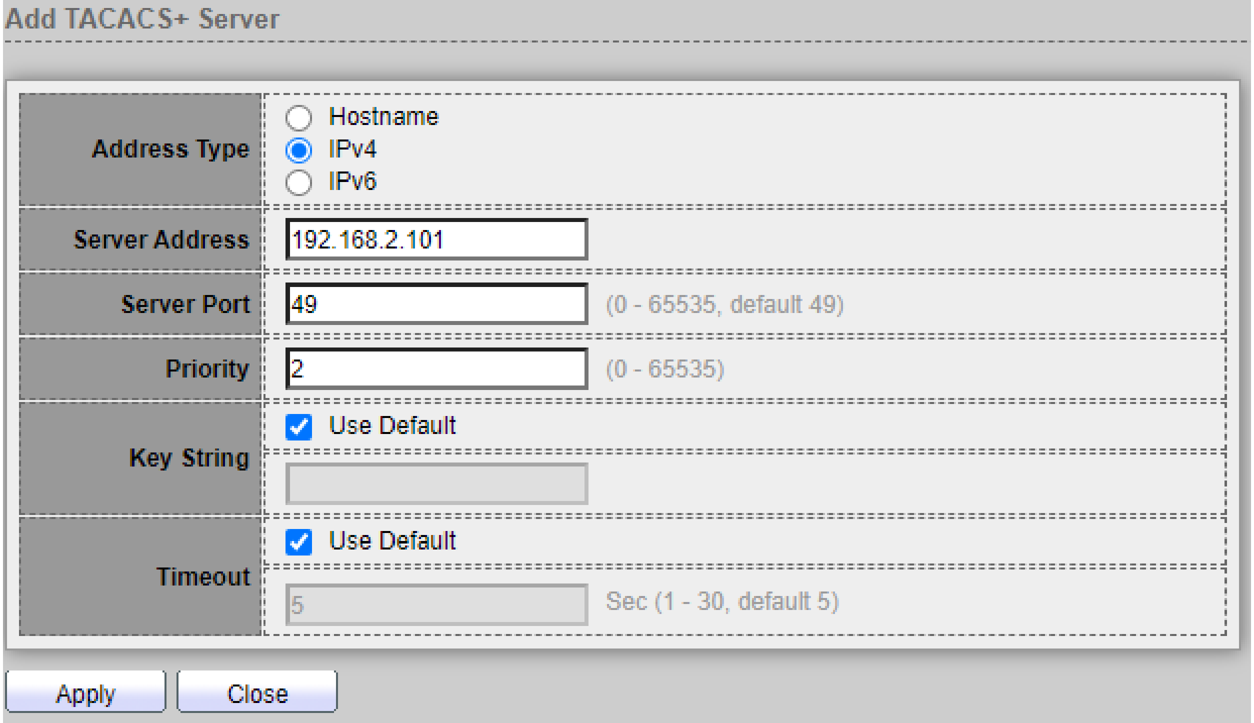
□	Server Address	Server Port	Priority	Timeout
□	192.168.2.101	49	2	5

- **Use Default Parameters :**
  - **Timeout:** Enter the amount of time in seconds that passes before the connection between the switch and the TACACS+ server times out. If a value is not entered for an individual server, the value is taken from this field, default is 5.
  - **Key String:** Enter the default key string in encrypted or plaintext form used for communicating with all TACACS+ servers.

Note	If administrator don't enter the default key string here, the key entered on the Add page must match the encryption key used by the TACACS+ server or enter the default key string here and a key string for an individual TACACS+ server, the key string configured for the individual TACACS+ server takes precedence.

*Click the **"Apply"** button to save your changes settings.*

Field	Description
Server Address	TACACS+ server address.
Server Port	TACACS+ server port.
Priority	TACACS+ server priority (smaller value has higher priority). TACACS+ session will try to establish with the server setting which has highest priority. If failed, it will try to connect to the server with next higher priority.
Timeout	TACACS+ server timeout value. If it is fail to connect to server, it will keep trying until timeout.



Add TACACS+ Server

Address Type	○ Hostname ● IPv4 ○ IPv6
Server Address	192.168.2.101
Server Port	49 (0 - 65535, default 49)
Priority	2 (0 - 65535)
Key String	☑ Use Default
Timeout	☑ Use Default 5 Sec (1 - 30, default 5)

- **Address Type:** Select IP Version 4 / 6 or use Hostname typem, In add dialog, user need to specify server Address Type
  - **Hostname:** Use domain name as server address.
  - **IPv4:** Use IPv4 as server address.
  - **IPv6:** Use IPv6 as server address.
- **Server Address:** In add dialog, user need to input server address based on address type. In edit dialog, it shows current edit server address.
- **Server Port:** Set TACACS+ server port.
- **Priority:** Administrator can enter the priority of the server. The priority determines the order that the switch attempts to contact the servers to authenticate users. The switch first starts with the highest priority server. 0 is the high priority, Set TACACS+ server priority (smaller value has higher priority). TACACS+ session will try to establish with the server setting which has highest priority. If failed, it will try to connect to the server with next higher priority.
- **Key String:** Administrator can select user defined Encrypted or Plaintext to enter the key string form used for authenticating and encrypting the communication between the switch and the TACACS+ server. This key must match the key configured on the TACACS+ server. If administrator select use default (checked in checkbox) will use the default key string.
- **Timeout:** Set TACACS+ server timeout value. If it is fail to connect to server,it will keep trying until timeout.

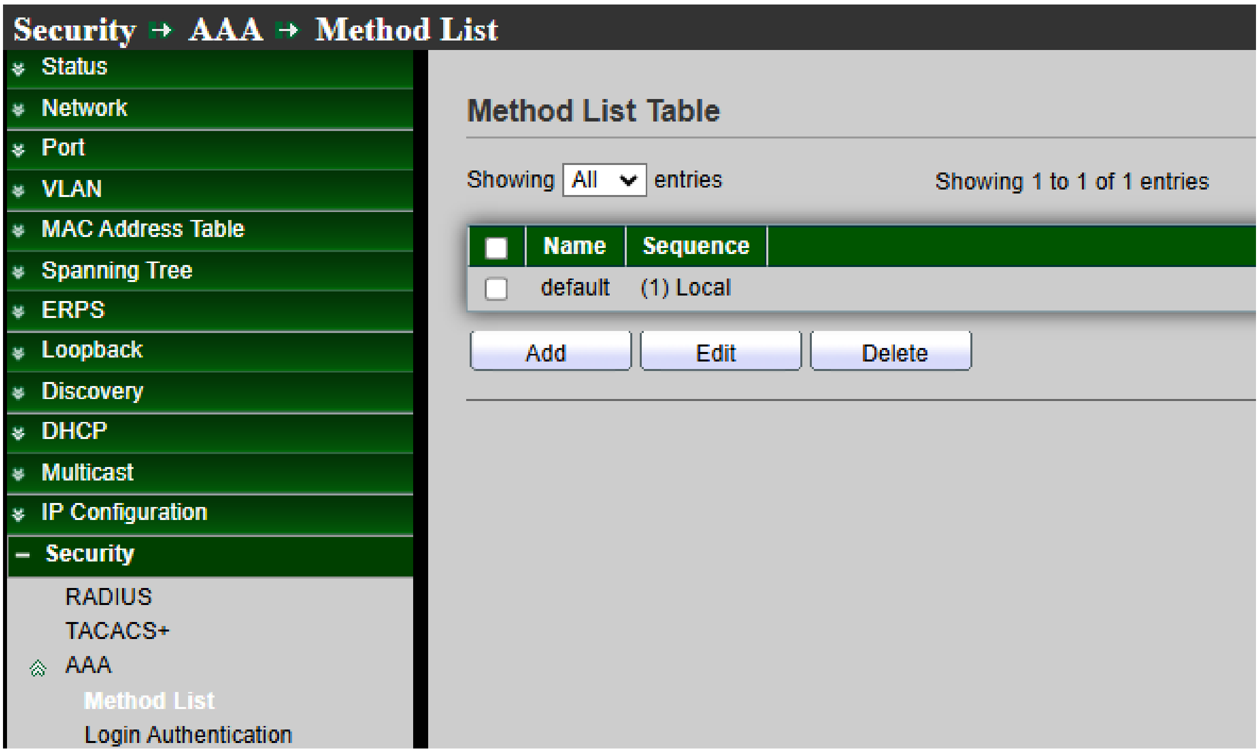
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

15.3 AAA

15.3.1 Method List

Administrator can set groups of AAA security, each group have 4 method table, each method can select 1 of 6 type which contains Empty / None / Local / Enable / RADIUS and TACACS+.

This page allow user to add, edit or delete login authentication list settings (The "default" list cannot be deleted.). The line combined to this list will authenticate login user by methods in this list. If the first method is failed, it will try to use the next priority method to authenticate if it exists.With RADIUS and TACACS+ methods, the failed means connecting to server fail. With Local method, the failed means cannot find the user in local database.

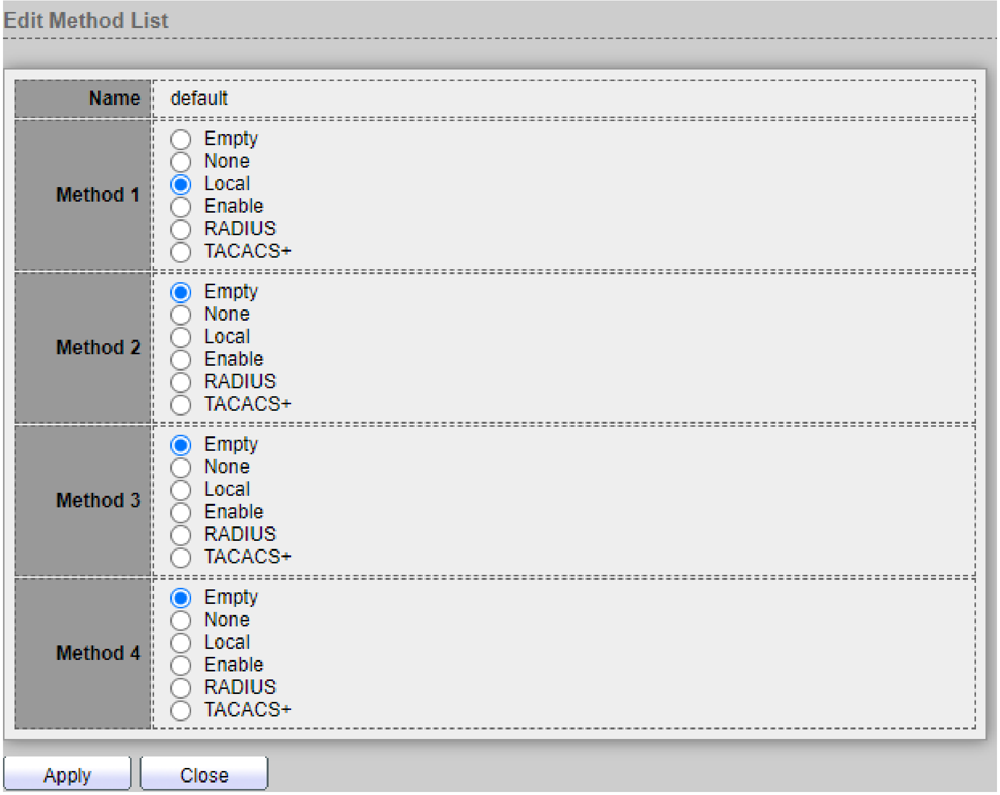


Showing All entries Showing 1 to 1 of 1 entries

□	Name	Sequence
□	default	(1) Local

Field	Description
Name	Login authentication list name. This name should be different from other existing lists.

Sequence	Priority of login authentication method. • **None:** Authenticated with any condition. • **Local:** Use local accounts database to authenticate • **TACACS+:** Use remote TACACS+ server to authenticate. • **RADIUS:** Use remote Radius server to authenticate. • **Enable:** Use local enable password to authenticate



Edit Method List

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

- **Name:** Login authentication list name. This name should be different from other existing lists.
- **Method 1:** Select first priority of login authentication method.
  - **None:** Authenticated with any condition.
  - **Local:** Use local accounts database to authenticate
  - **TACACS+:** Use remote TACACS+ server to authenticate.
  - **RADIUS:** Use remote Radius server to authenticate.
  - **Enable:** Use local enable password to authenticate.
- **Method 2:** Select first priority of login authentication method.
  - **None:** Authenticated with any condition.
  - **Local:** Use local accounts database to authenticate
  - **TACACS+:** Use remote TACACS+ server to authenticate.
  - **RADIUS:** Use remote Radius server to authenticate.

- **Enable:** Use local enable password to authenticate.

➢ **Method 3:** Select first priority of login authentication method.

- **None:** Authenticated with any condition.
- **Local:** Use local accounts database to authenticate
- **TACACS+:** Use remote TACACS+ server to authenticate.
- **RADIUS:** Use remote Radius server to authenticate.
- **Enable:** Use local enable password to authenticate.

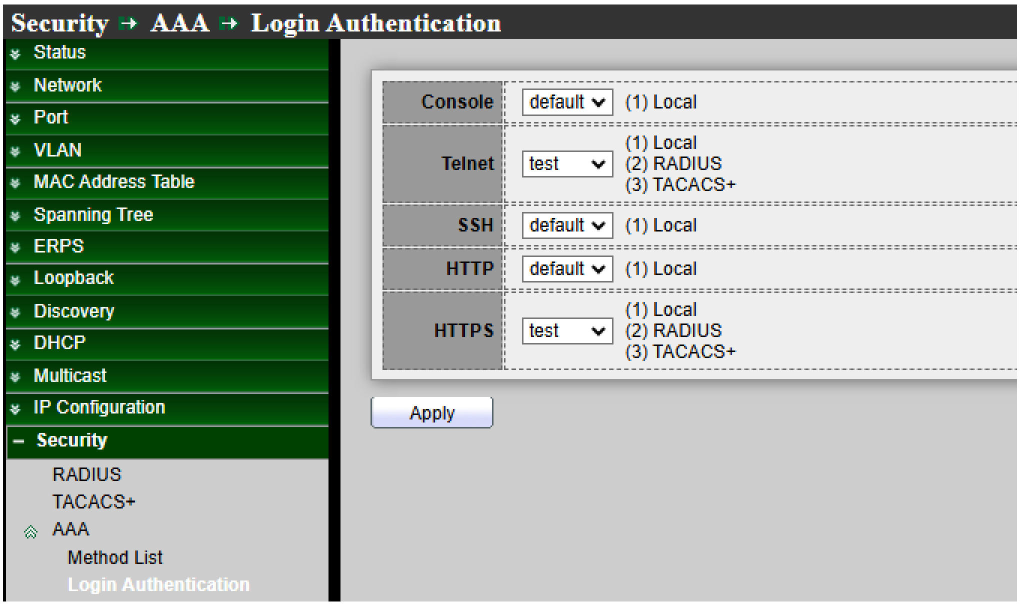
➢ **Method 4:** Select first priority of login authentication method.

- **None:** Authenticated with any condition.
- **Local:** Use local accounts database to authenticate
- **TACACS+:** Use remote TACACS+ server to authenticate.
- **RADIUS:** Use remote Radius server to authenticate.
- **Enable:** Use local enable password to authenticate.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

15.3.2 Login Authentication

When administrator has created security groups in "AAA➔method" then administrator can select different security group in service port.



Security ➔ AAA ➔ Login Authentication

Console	default	(1) Local
Telnet	test	(1) Local (2) RADIUS (3) TACACS+
SSH	default	(1) Local
HTTP	default	(1) Local
HTTPS	test	(1) Local (2) RADIUS (3) TACACS+

Field	Description
Console	Specify login authentication list combined on console

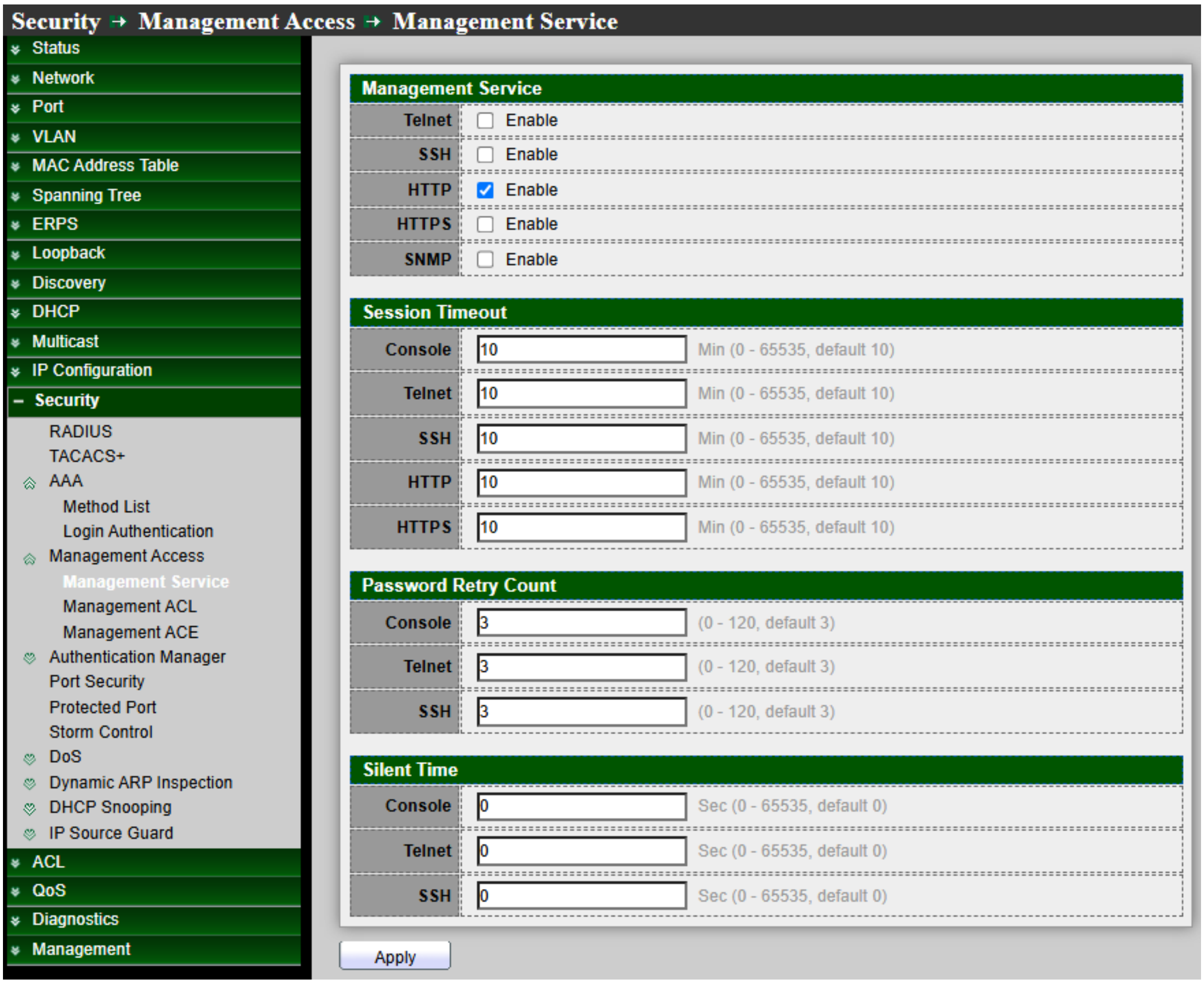
Telnet	Specify login authentication list combined on Telnet
SSH	Specify login authentication list combined on SSH
HTTPS	Specify login authentication list combined on HTTPS

*Click the "**Apply**" button to save your changes settings.*

15.4 Management Access

15.4.1 Management Service

Administrator can select enable Telnet / SSH / HTTP / HTTPS / SNMP by different protocol to login service and configuration login timeout limit and password error retry count limit.



Management Service

Telnet	☐ Enable
SSH	☐ Enable
HTTP	☑ Enable
HTTPS	☐ Enable
SNMP	☐ Enable

Session Timeout

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

Password Retry Count

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

Silent Time

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

➢ **Management Service:** Management service admin state.

- **Telnet:** Connect CLI through telnet.
- **SSH:** Connect CLI through SSH.

- **HTTP:** Connect WEBUI through HTTP.
- **HTTPS:** Connect WEBUI through HTTPS.
- **SNMP:** Manage switch trough SNMP.

➢ **Session Timeout:** Set session timeout minutes for user access to user interface. 0 minutes means never timeout, After login management page, in the set time if not session then system will auto timeout, administrator need re-login.

- **Console:** Set console for session timeout 0~65535 minutes.
- **Telnet:** Set Telnet for session timeout 0~65535 minutes.
- **SSH:** Set SSH for session timeout 0~65535 minutes.
- **HTTP:** Set HTTP for session timeout 0~65535 minutes.
- **HTTPS:** Set HTTPS for session timeout 0~65535 minutes.

➢ **Password Retry Count:** Retry count is the number which CLI password input error tolerance count. After input error password exceeds this count, the CLI will freeze after silent time, If login error reaches the set value then login page will be kicked out, administrator need reopen the login page.

- **Console:** Set console for password Retry count of 0~120 .
- **Telnet:** Set Telnet for password Retry count of 0~120 .
- **SSH:** Set SSH for password Retry count of 0~120 .

➢ **Silent Time:** This function to be matched "Password Retry Count" function, if login error reaches the set value within then set value of silent time will can't be reopen login page until the set time end ,After input error password exceeds password retry count, the CLI will freeze after silent time.

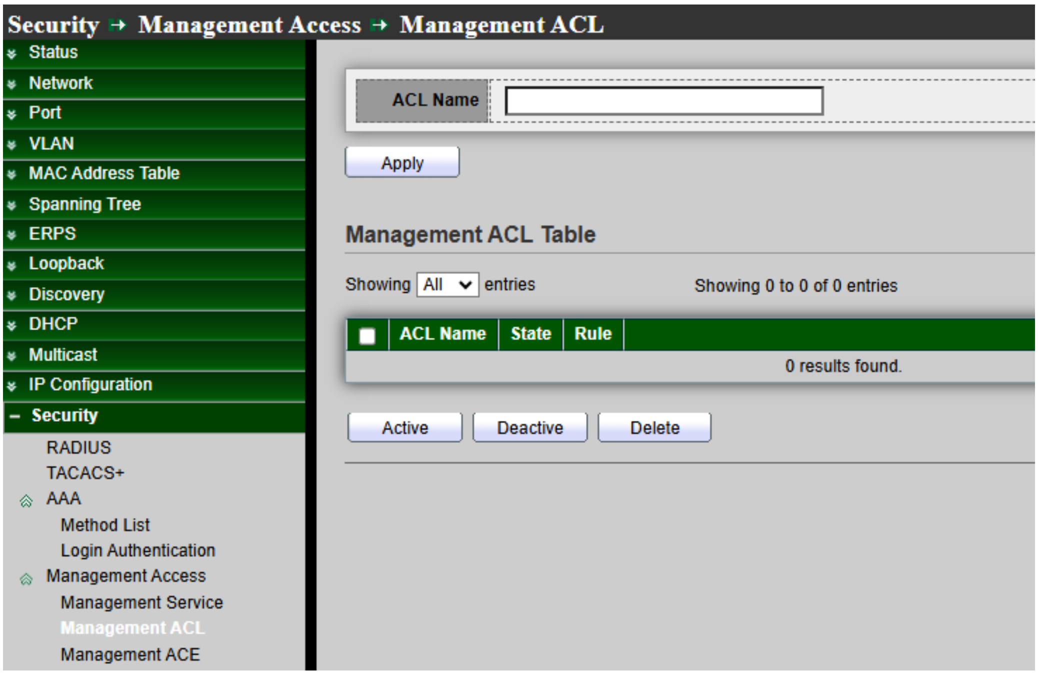
- **Console:** Set console for Silent Time of 0~65535 minutes .
- **Telnet:** Set Telnet for Silent Time of 0~65535 minutes .
- **SSH:** Set SSH for for Silent Time of 0~65535 minutes .

15.4.2 Management ACL

Administrator can create ACL and set Active or Deactive the rules.

If administrator set "Active" will be apply "Management ACE" rules. ACL can set which ports is Permit or Deny connection to which services of the switch management interface.

Note	If only create one ACL Profile and click Active then these all ports and services will are all denied.



- **ACL Name:** Input MAC ACL name.

*Click the "**Apply**" button to save your changes settings.*

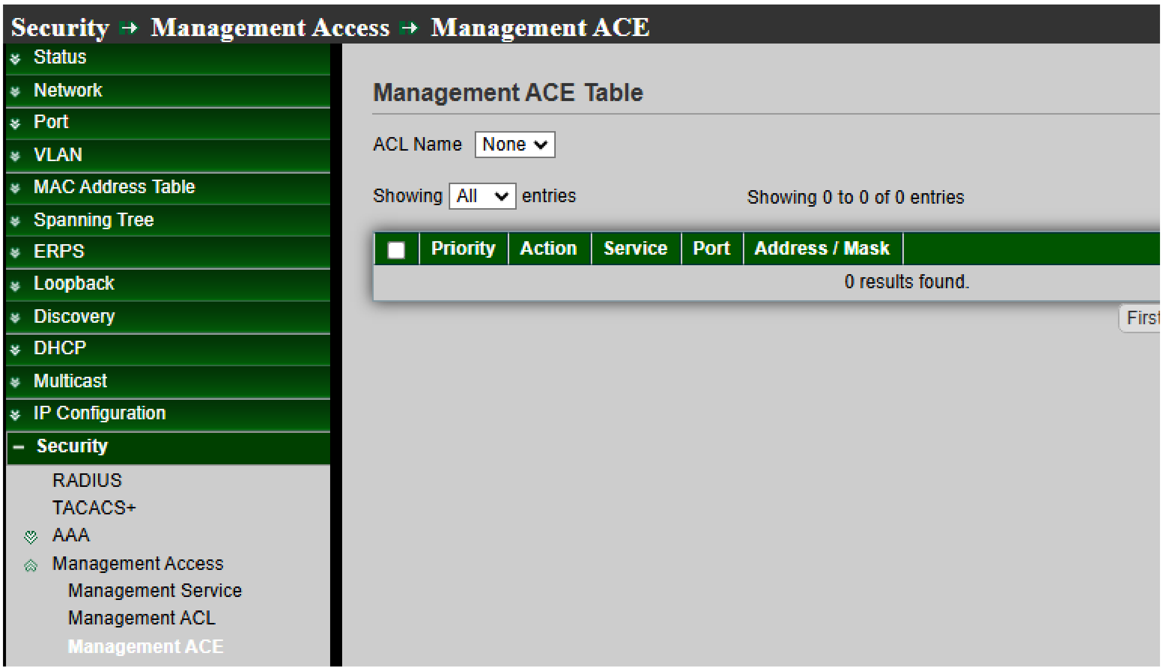
Field	Description
ACL Name	Display Management ACL name
State	Display Management ACL whether active.
Rule	Display the number Management ACE rule of ACL

*Set the **"Active"** and **"Deactive"** and **"Delete"** for this table management.*

15.4.3 Management ACE

This management ACE page is to create an ACL profile rule. Administrator can select an created ACL profile to set security rule. If set the ACE only use Telnet a single rule. After confirmation the rule will apply to ACL profile.

Administrator can go to "management ACL" page click "Active" button to enable the rule. After active the rule, this management page will can't operating only use Telnet protocol to management, Setting **"add"** and **"Edit"** and **"Delete"** function for this management.



Management ACE Table

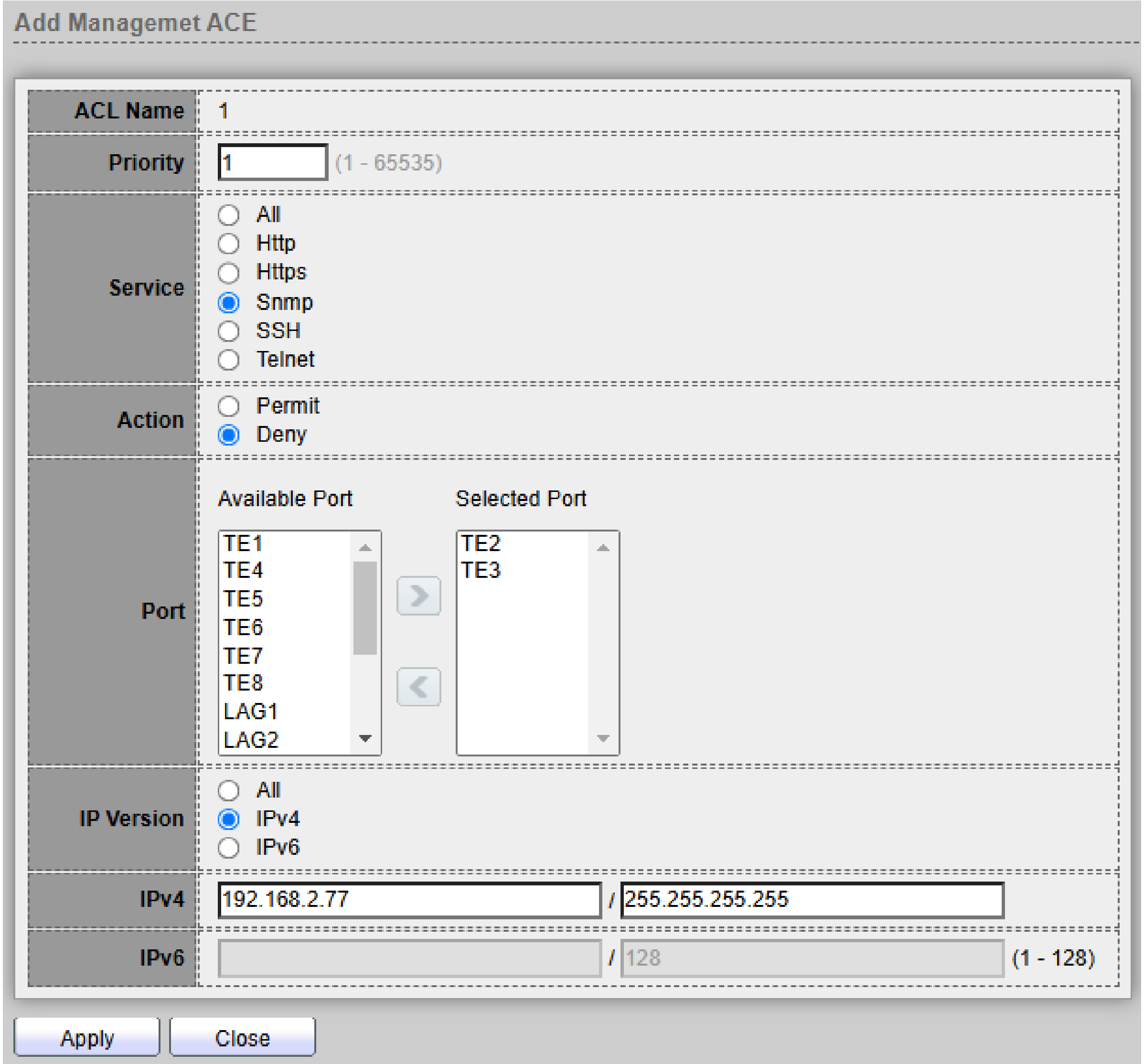
ACL Name: None

Showing All entries — Showing 0 to 0 of 0 entries

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

- **ACL Name:** Select the ACL name to which an ACE is being added.

Field	Description
Priority	Display the priority of ACE.
Action	Display the action of ACE
Service	Display the service ACE.
Port	Display the port list of ACE.
Address / Mask	Display the source IP address and mask of ACE.



Add Managemet ACE

ACL Name	1
Priority	1 (1 - 65535)
Service	○ All ○ Http ○ Https ● Snmp ○ SSH ○ Telnet
Action	○ Permit ● Deny
Port	Available Port: TE1, TE4, TE5, TE6, TE7, TE8, LAG1, LAG2 Selected Port: TE2, TE3
IP Version	○ All ● IPv4 ○ IPv6
IPv4	192.168.2.77 / 255.255.255.255
IPv6	/ 128 (1 - 128)

- **ACL Name**: Display the ACL name to which an ACE is being added.
- **Priority**: Set this rule priority, Specify the priority of the ACE. ACEs with higher sequence are processed first (1 is the highest priority). Only available on Add Dialog.
- **Service:** Select the type service of rule.
  - **All**: All services .
  - **HTTP**: Only HTTP service .
  - **HTTPs**: Only HTTPs service.
  - **SNMP**: Only SNMP service.
  - **SSH:** Only SSH service.
  - **Telnet**: Only Telnet service
- **Action:** Select the action after ACE match packet.
  - **Permit**: Forward packets that meet the ACE criteria.
  - **Deny**: Drop packets that meet the ACE criteria.

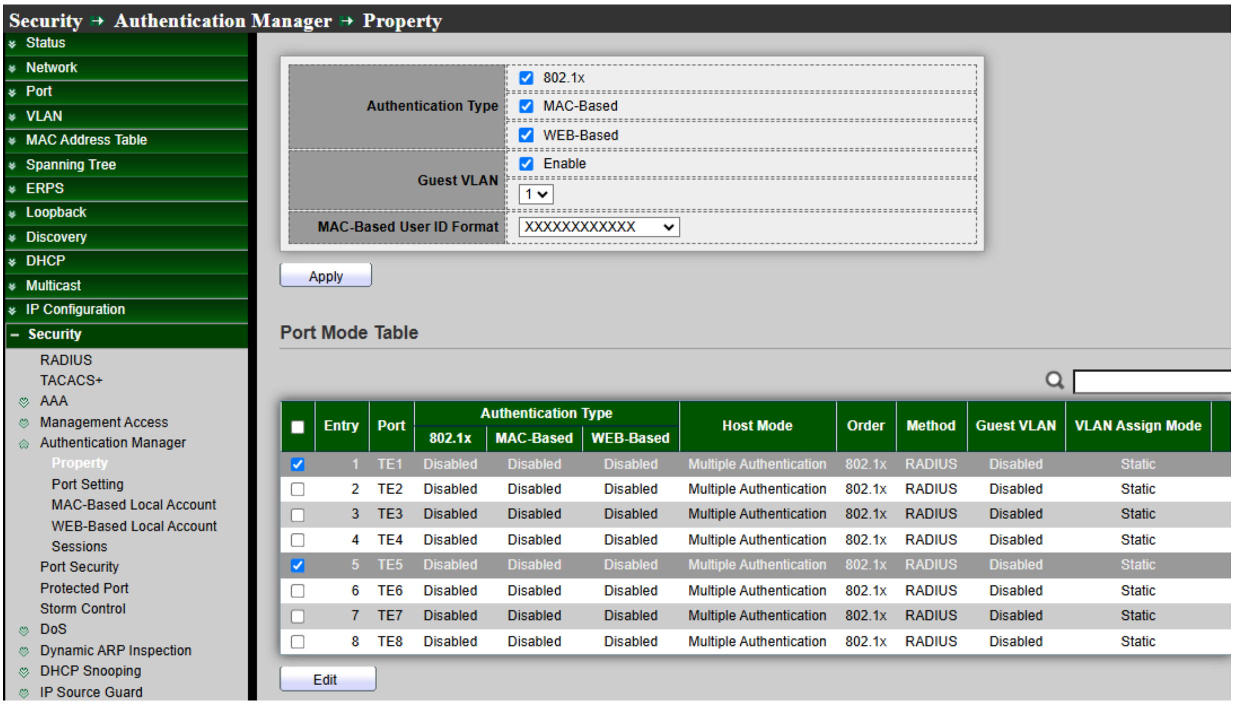
- **Port:** Select ports which will be matched.
- **IP Version:** Select the type of source IP address.
  - **All**: All IP addresses can access.
  - **IPv4**: Specify IPv4 address ca access.
  - **IPv6**: Specify IPv6 address ca access
- **IPv4:** Enter the source IPv4 address value and mask to which will be matched.
- **IPv6:** Enter the source IPv6 address value and mask to which will be matched.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

15.5 Authentication Manager

15.5.1 Property

This page allow user to edit authentication global settings and some port mods' configurations, Administrator can edit authentication global settings and some port mods' configurations.



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

Guest VLAN: ☑ Enable; 1

MAC-Based User ID Format: XXXXXXXXXXXX

Port Mode Table

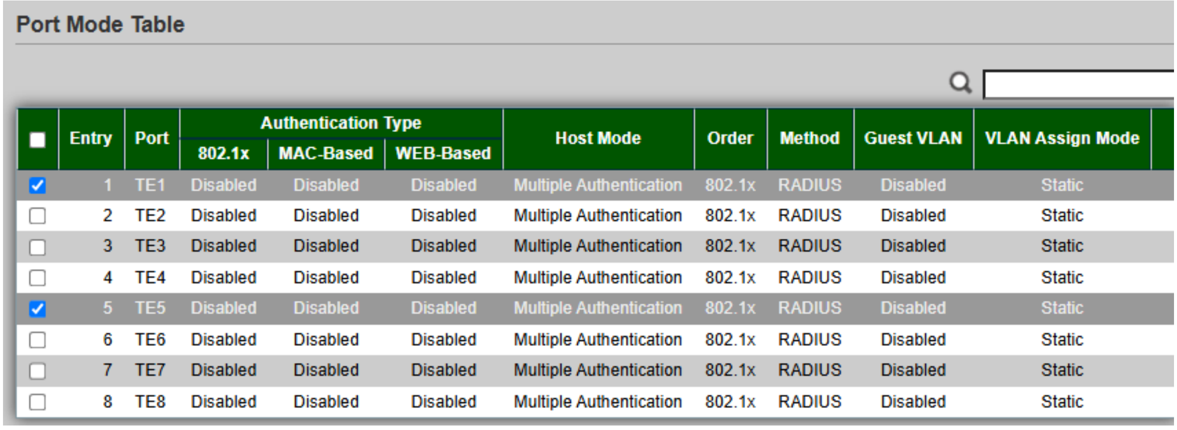
□	Entry	Port	Authentication Type			Host Mode	Order	Method	Guest VLAN	VLAN Assign Mode
			802.1x	MAC-Based	WEB-Based					
☑	1	TE1	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
□	2	TE2	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
□	3	TE3	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
□	4	TE4	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
☑	5	TE5	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
□	6	TE6	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
□	7	TE7	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
□	8	TE8	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static

- **Authentication Type :** Set checkbox to enable/disable following authentication types
  - 802.1x: Use IEEE 802.1x to do authentication
  - MAC-Based: Use MAC address to do authentication
  - WEB-Based: Prompt authentication web page for user to do authentication
- **Guest VLAN :** Set checkbox to enable/disable guest VLAN, if guest VLAN is enabled, you

need to select one available VLAN ID to be guest VID.

- **MAC-Based User ID Format :** Select mac-based authentication RADIUS username/password ID format.
  - XXXXXXXXXXXX
  - xxxxxxxxxxxx
  - XX:XX:XX:XX:XX:XX
  - xx:xx:xx:xx:xx:xx
  - XX-XX-XX-XX-XX-XX
  - xx-xx-xx-xx-xx-xx
  - XX.XX.XX.XX.XX.XX
  - xx.xx.xx.xx.xx.xx
  - XXXX:XXXX:XXXX
  - xxxx:xxxx:xxxx
  - XXXX-XXXX-XXXX
  - xxxx-xxxx-xxxx
  - XXXX.XXXX.XXXX
  - xxxx.xxxx.xxxx
  - XXXXXX:XXXXXX
  - xxxxxx:xxxxxx
  - XXXXXX-XXXXX
  - xxxxxx-xxxxxx

*Click the **"Apply"** button to save your changes settings.*

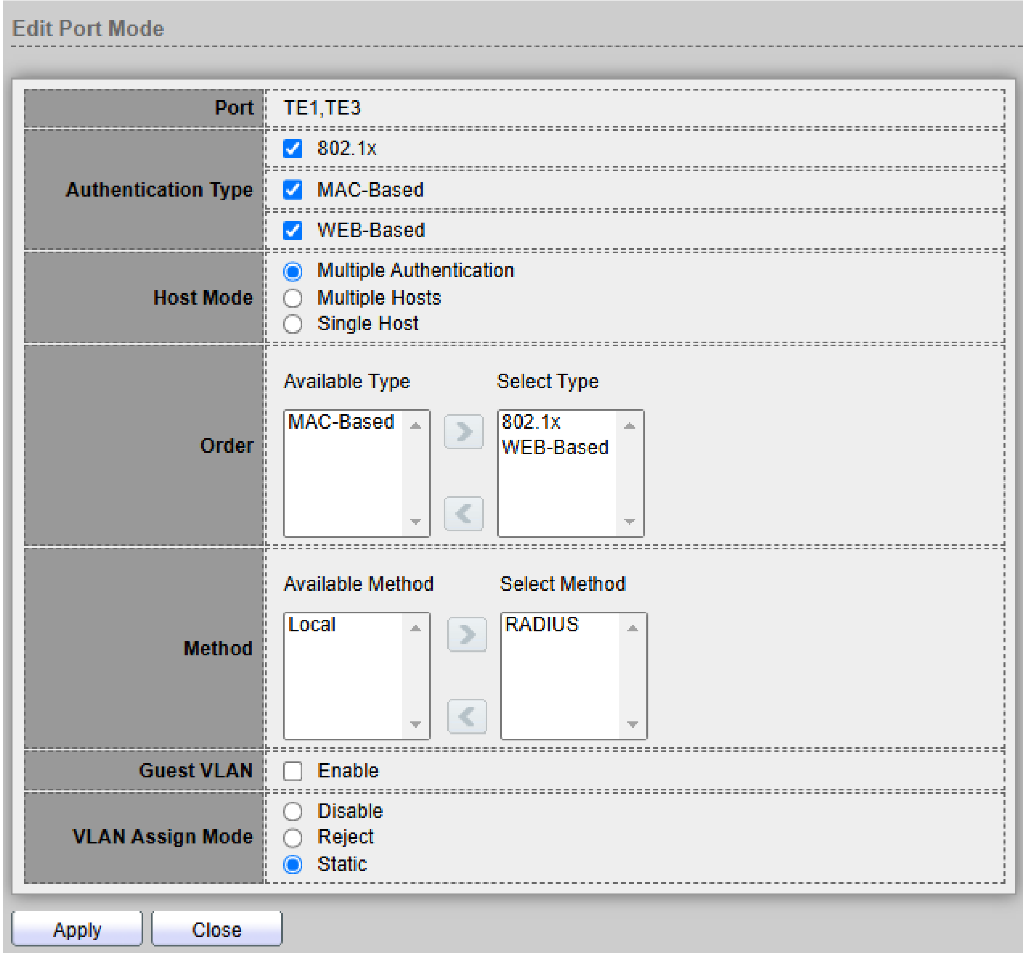


Port Mode Table

□	Entry	Port	Authentication Type			Host Mode	Order	Method	Guest VLAN	VLAN Assign Mode
			802.1x	MAC-Based	WEB-Based					
☑	1	TE1	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
□	2	TE2	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
□	3	TE3	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
□	4	TE4	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
☑	5	TE5	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
□	6	TE6	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
□	7	TE7	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
□	8	TE8	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static

Field	Description
Port	Port name
Authentication Type (802.1X)	802.1 X authentication type state • **Enabled:** 802.1X is enabled • **Disabled:** 802.1X is disabled
Authentication Type (MAC-Based)	MAC-Based authentication type state • **Enabled:** MAC-Based authentication is enabled • **Disabled:** MAC-Based authentication is disabled
Authentication Type (WEB-Based)	WEB-Based authentication type state • **Enabled:** WEB-Based authentication is enabled • **Disabled:** WEB-Based authentication is disabled
Host Mode	Authenticating host mode • **Multiple Authentication:** In this mode, every client need to pass authenticate procedure individually. • **Multiple Hosts:** In this mode, only one client need to be authenticated and other clients will get the same access accessibility. Web-auth cannot be enabled in this mode. • **Single Host:** In this mode, only one host is allowed to be authenticated. It is the same as Multi-auth mode with max hosts number configure to be 1.
Order	Support following authentication type order combinations. Web Authentication should always be the last type. The authentication manager will go to next type if current type is not enabled or authenticated fail. • **802.1x** • **MAC-Based** • **WEB-Based** • **802.1x MAC-Based** • **802.1x WEB-Based** • **MAC-Based 802.1x** • **WEB-Based 802.1x** • **802.1x MAC-Based WEB-Based** • **802.1x WEB-Based MAC-Based**

Method	Support following authentication method order combinations. These orders only available on MAC-Based authentication and WEB-Based authentication. 802.1x only support Radius method. • **Local:** Use DUT's local database to do authentication • **Radius:** Use remote RADIUS server to do authentication • **Local Radius** • **Radius Local**
Guest VLAN	Port guest VLAN enable state • **Enabled:** Guest VLAN is enabled on port • **Disabled:** Guest VLAN is disabled on port
VLAN Assign Mode	Support following VLAN assign mode and only apply when source is RADIUS • **Disable:** Ignore the VLAN authorization result and keep original VLAN of host. • **Reject:** If get VLAN authorized information, just use it. However, if there is no VLAN authorized information, reject the host and make it unauthorized. • **Static:** If get VLAN authorized information, just use it. If there is no VLAN authorized information, keep original VLAN of host.



Edit Port Mode

Port	TE1,TE3
Authentication Type	☑ 802.1x ☑ MAC-Based ☑ WEB-Based
Host Mode	● Multiple Authentication ○ Multiple Hosts ○ Single Host
Order	Available Type: MAC-Based Select Type: 802.1x WEB-Based
Method	Available Method: Local Select Method: RADIUS
Guest VLAN	□ Enable
VLAN Assign Mode	○ Disable ○ Reject ● Static

- **Port :** Display selected Port number.
- **Authentication Type :** Set checkbox to enable/disable authentication types.
  - **802.1x :** Use IEEE 802.1x to do authentication
  - **MAC-Based :** Use MAC address to do authentication
  - **WEB-Based :** Prompt authentication web page for user to do authentication
- **Host Mode :** Select authenticating host mode.
  - **Multiple Authentication :** In this mode, every client need to pass authenticate procedure individually
  - **Multiple Hosts :** In this mode, only one client need to be authenticated and other clients will get the same access accessibility. Web-auth cannot be enabled in this mode.
  - **Single Host :** In this mode, only one host is allowed to be authenticated. It is the same as Multi-auth mode with max hosts number configure to be 1.
- **Order :** Support following authentication type order combinations. Web Authentication should always be the last type. The authentication manager will go to next type if current

type is not enabled or authenticated fail.

- 802.1x
- MAC-Based
- WEB-Based
- 802.1x MAC-Based
- 802.1x WEB-Based
- MAC-Based 802.1x
- WEB-Based 802.1x
- 802.1x MAC-Based WEB-Based
- 802.1x WEB-Based MAC-Based

➢ **Method :** Support following authentication method order combinations.These orders only available on MAC-Based authentication and WEB-Based authentication. 802.1x only support Radius method.

- **Local :** Use DUT's local database to do authentication
- **Radius :** Use remote RADIUS server to do authentication

➢ **Guest VLAN :** Set checkbox to enable/disable guest VLAN.

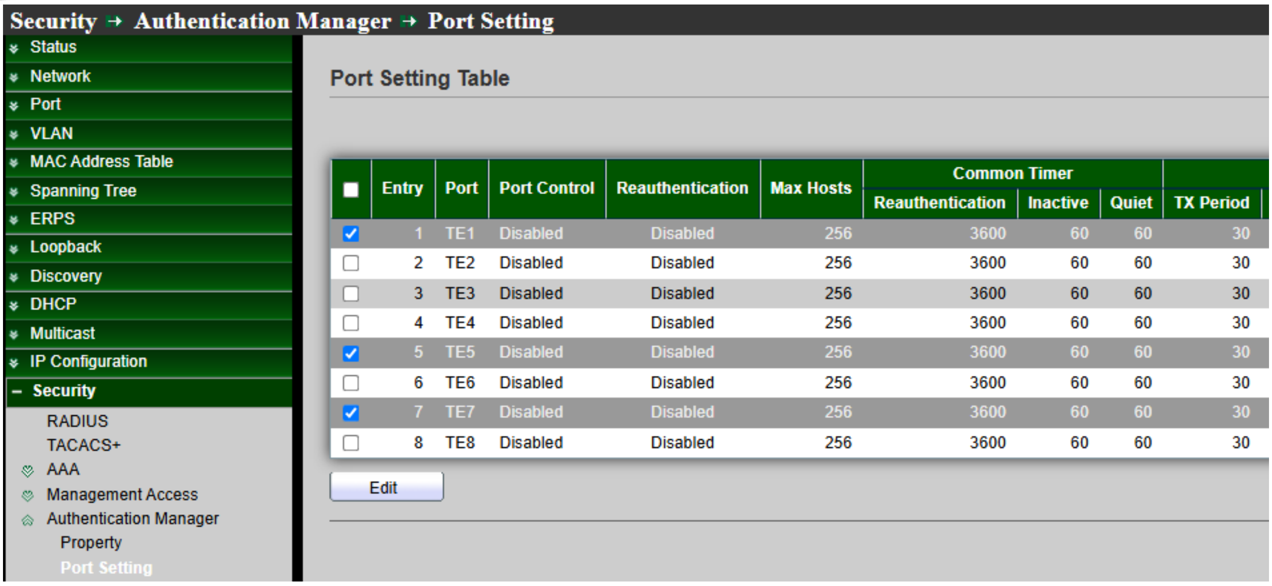
➢ **VLAN Assign Mode :** Support following VLAN assign mode and only apply when source is RADIUS.

- **Disable**: Ignore the VLAN authorization result and keep original VLAN of host.
- **Reject**: If get VLAN authorized information, just use it. However, if there is no VLAN authorized information, reject the host and make it unauthorized.Local Radius.
- **Static**: If get VLAN authorized information, just use it. If there is no VLAN authorized information, keep original VLAN of host.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

15.5.2 Port Setting

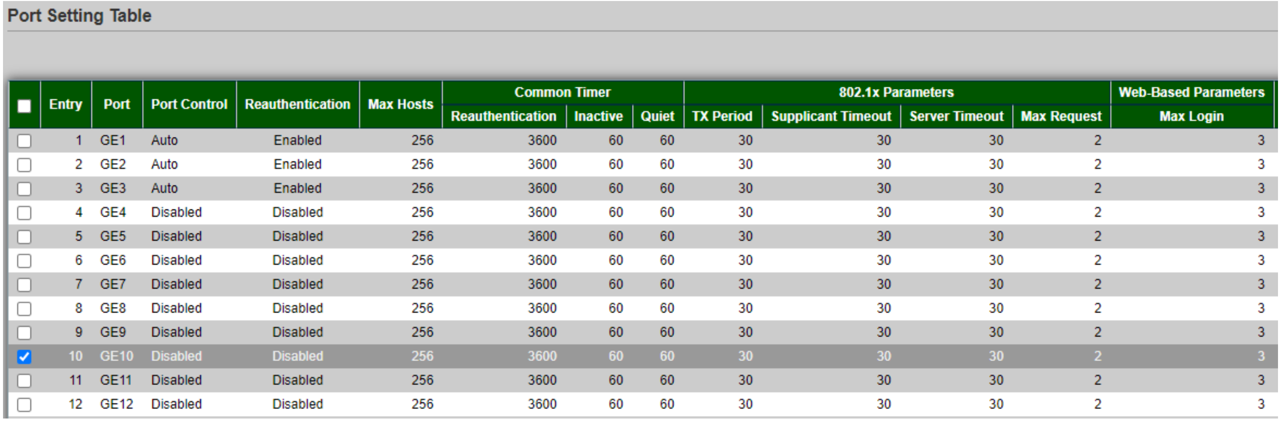
Administrator can configure authentication manger port settings,This page allow user to configure authentication manger port settings



Security → Authentication Manager → Port Setting

Port Setting Table

□	Entry	Port	Port Control	Reauthentication	Max Hosts	Common Timer			
						Reauthentication	Inactive	Quiet	TX Period
☑	1	TE1	Disabled	Disabled	256	3600	60	60	30
□	2	TE2	Disabled	Disabled	256	3600	60	60	30
□	3	TE3	Disabled	Disabled	256	3600	60	60	30
□	4	TE4	Disabled	Disabled	256	3600	60	60	30
☑	5	TE5	Disabled	Disabled	256	3600	60	60	30
□	6	TE6	Disabled	Disabled	256	3600	60	60	30
☑	7	TE7	Disabled	Disabled	256	3600	60	60	30
□	8	TE8	Disabled	Disabled	256	3600	60	60	30

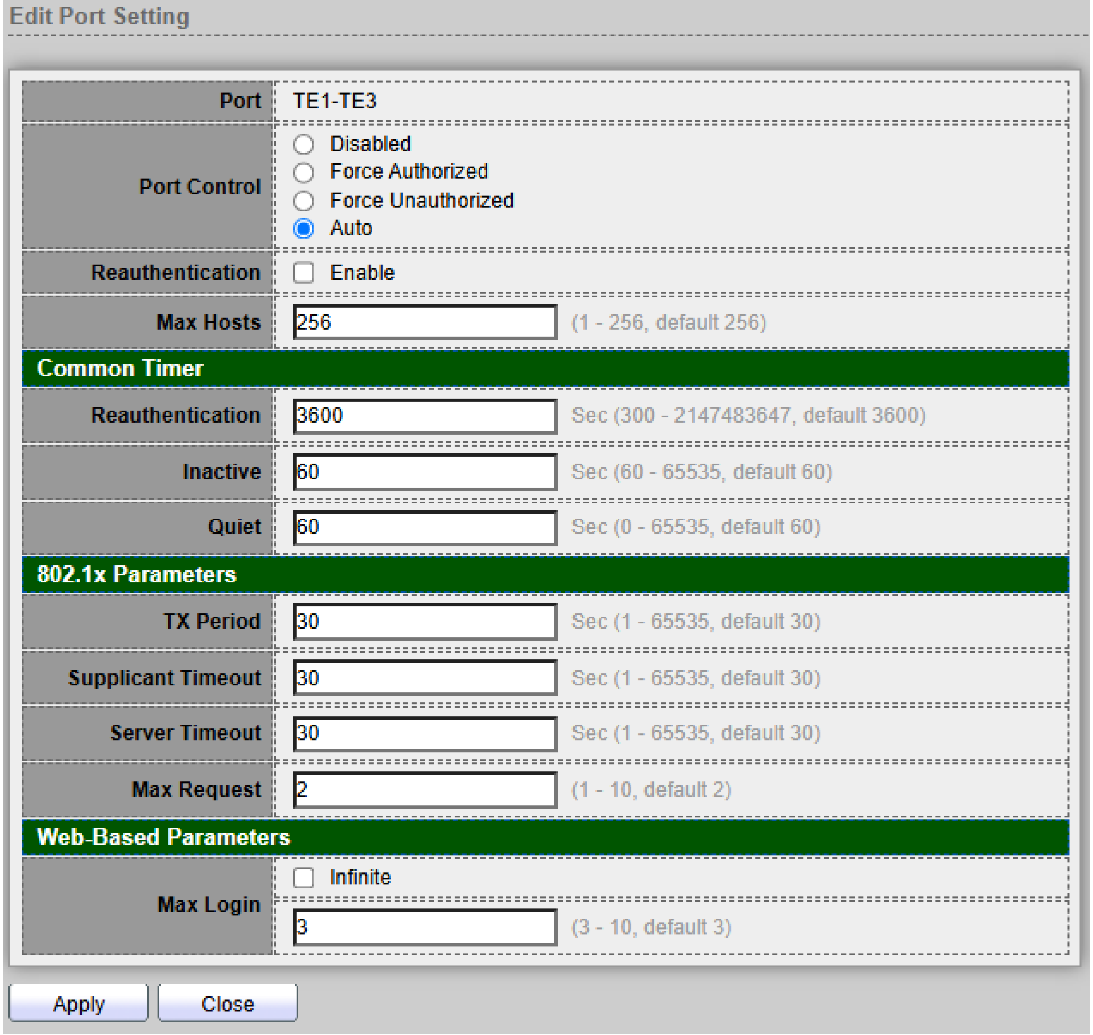


Port Setting Table

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

Field	Description
Port	Port name
Port Control	Support following authentication port control types. • **Disable:** Disable authentication function and all clients have network accessibility. • **Force Authorized:** Port is force authorized and all clients have network accessibility. • **Force Unauthorized:** Port is force unauthorized and all clients have no network accessibility. • **Auto:** Need passing authentication procedure to get network accessibility.
Reauthentication	Reautheticate state • **Enabled:** Host will be reauthenticated after reauthentication period

	• **Disabled:** Host will not be reauthenticated after reauthentication period.
Max Hosts	In Multiple Authentication mode, total host number cannot not exceed max hosts number
Common Timer	• **Reauthentication:** After re-authenticate period, host will return to initial state and need to pass authentication procedure again. • **Inactive:** If no packet from the authenticated host, the inactive timer will increase. After inactive timeout, the host will be unauthorized and corresponding session will be deleted. In multi-host mode, the packet is counting on the authorized host only and not all packets on the port. • **Quiet:** When port is in Locked state after authenticating fail several times, the host will be locked in quiet period. After this quiet period, the host is allowed to authenticate again.
802.1X Params	• **TX Period:** Number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the supplicant (client) before resending the request. • **Supplicant Timeout:** Number of seconds that lapses before EAP requests are resent to the supplicant. • **Server Timeout:** Number of seconds that lapses before the switch resends a request to the authentication server. • **Max Request:** The maximum number of EAP requests that can be sent. If a response is not received after the defined period (supplicant timeout), the authentication process is restarted.
Web-Based Param (Max Login)	Allow user login fail number. After login fail number exceed, the host will enter Lock state and is not able to authenticate until quiet period exceed.



Edit Port Setting

Port	TE1-TE3
Port Control	○ Disabled ○ Force Authorized ○ Force Unauthorized ● Auto
Reauthentication	□ Enable
Max Hosts	256 (1 - 256, default 256)
Common Timer	
Reauthentication	3600 Sec (300 - 2147483647, default 3600)
Inactive	60 Sec (60 - 65535, default 60)
Quiet	60 Sec (0 - 65535, default 60)
802.1x Parameters	
TX Period	30 Sec (1 - 65535, default 30)
Supplicant Timeout	30 Sec (1 - 65535, default 30)
Server Timeout	30 Sec (1 - 65535, default 30)
Max Request	2 (1 - 10, default 2)
Web-Based Parameters	
Max Login	□ Infinite 3 (3 - 10, default 3)

- **Port :** Display selected Port number.
- **Port Control :** Support following authentication port control types.
  - **Disable :** Disable authentication function and all clients have network accessibility.
  - **Force Authorized :** Port is force authorized and all clients have network accessibility.
  - **Force Unauthorized :** Port is force unauthorized and all clients have no network accessibility.
  - **Auto :** Need passing authentication procedure to get network accessibility.
- **Reauthentication :** Set checkbox to enable/disable reuauthentication.
- **Max Hosts :** In Multiple Authentication mode, total host number cannot not exceed max hosts number.
- **Common Timer:**
  - **Reauthentication :** After re-authenticate period, host will return to initial state and need to pass authentication procedure again.

- **Inactive :** If no packet from the authenticated host, the inactive timer will increase. After inactive timeout, the host will be unauthorized and corresponding session will be deleted. In multi-host mode, the packet is counting on the authorized host only and not all packets on the port.
- **Quiet :** When port is in Locked state after authenticating fail several times, the host will be locked in quiet period. After this quiet period, the host is allowed to authenticate again.

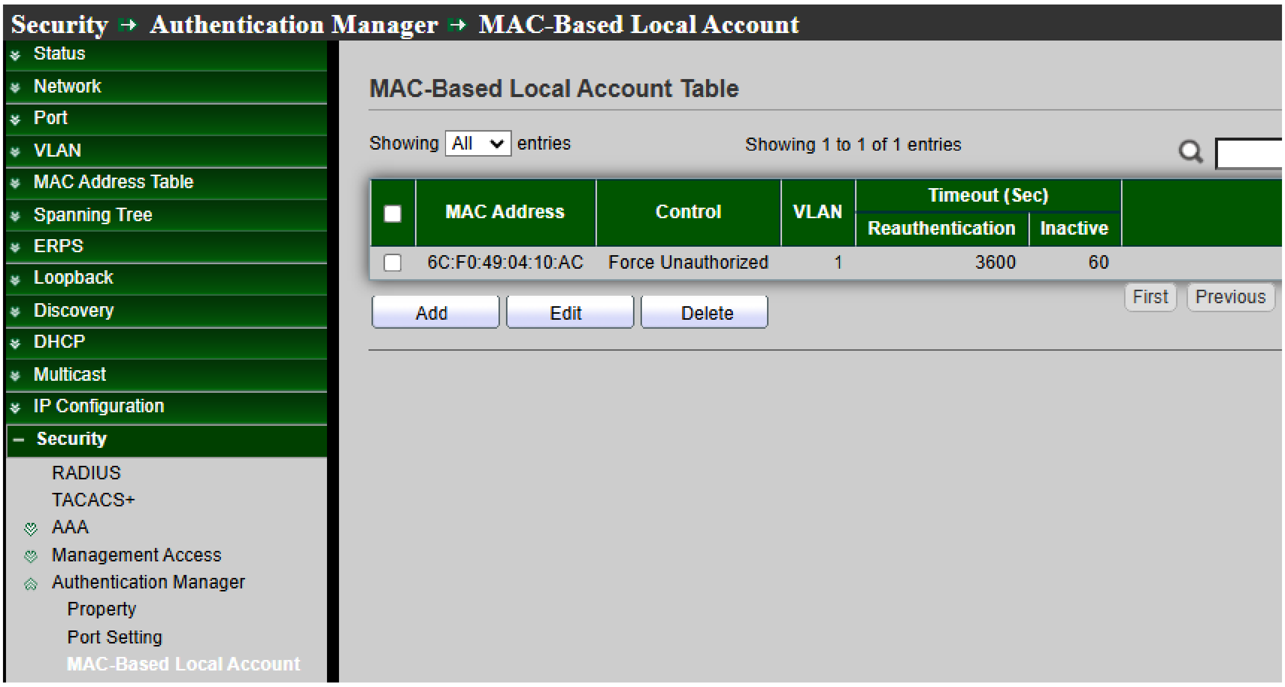
➢ **802.1X Params :**

- **TX Period :** Number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the supplicant (client) before resending the request.
- **Supplicant Timeout :** Number of seconds that lapses before EAP requests are resent to the supplicant.
- **Server Timeout:** Number of seconds that lapses before the switch resends a request to the authentication server.
- **Max Request :** The maximum number of EAP requests that can be sent. If a response is not received after the defined period (supplicant timeout), the authentication process is restarted.
- **Max Login :** Set checkbox to set max login number to be infinite or specify max login number.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

15.5.3 MAC-Based Local Account

Administrator can allow to add/edit/delete MAC-Based authentication local accounts, Setting **“add”** and **“Edit”** and **“Delete”** function for this management.



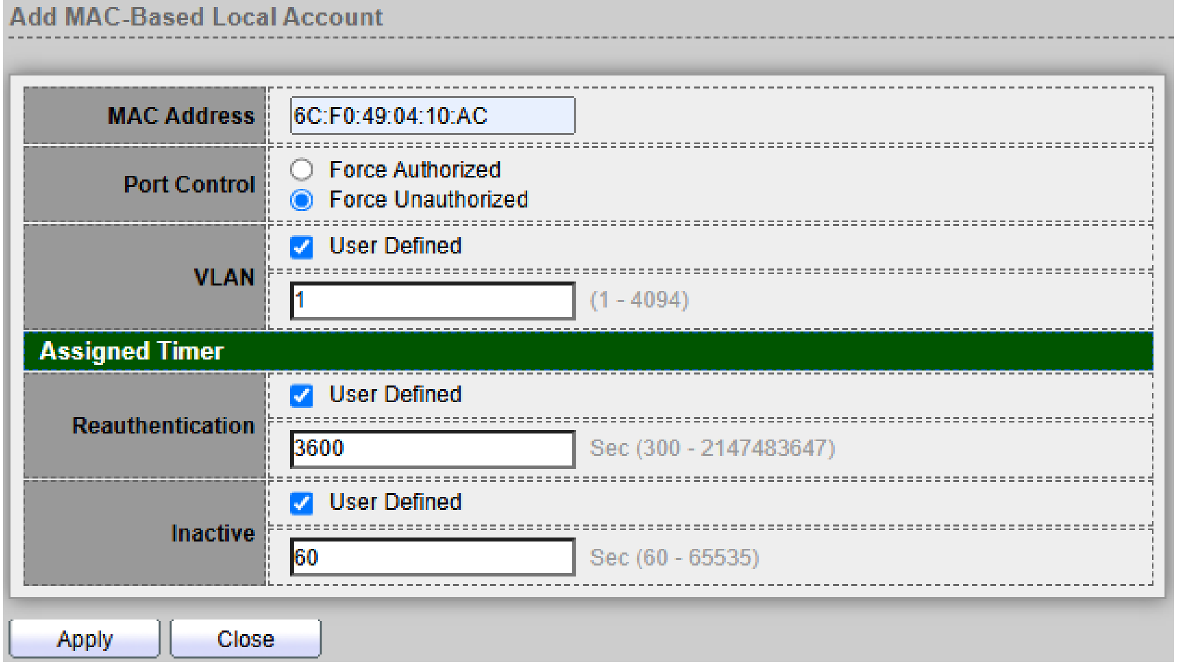
MAC-Based Local Account Table

Showing All entries

Showing 1 to 1 of 1 entries

□	MAC Address	Control	VLAN	Timeout (Sec)	
				Reauthentication	Inactive
□	6C:F0:49:04:10:AC	Force Unauthorized	1	3600	60

Field	Description
MAC Address	Authenticated host MAC address, and each MAC allow only one entry in local database.
Control	Control Type • **Force Authorized:** Host will be force authorized. • **Force Unauthorized:** Host will be force unauthorized.
VLAN	Assigned VLAN ID for the authenticated host.
Timeout	• **Reauthentication:** Assigned reauthentication period for the authenticated host. • **Inactive:** Assigned inactive timeout for the authenticated host.



Add MAC-Based Local Account

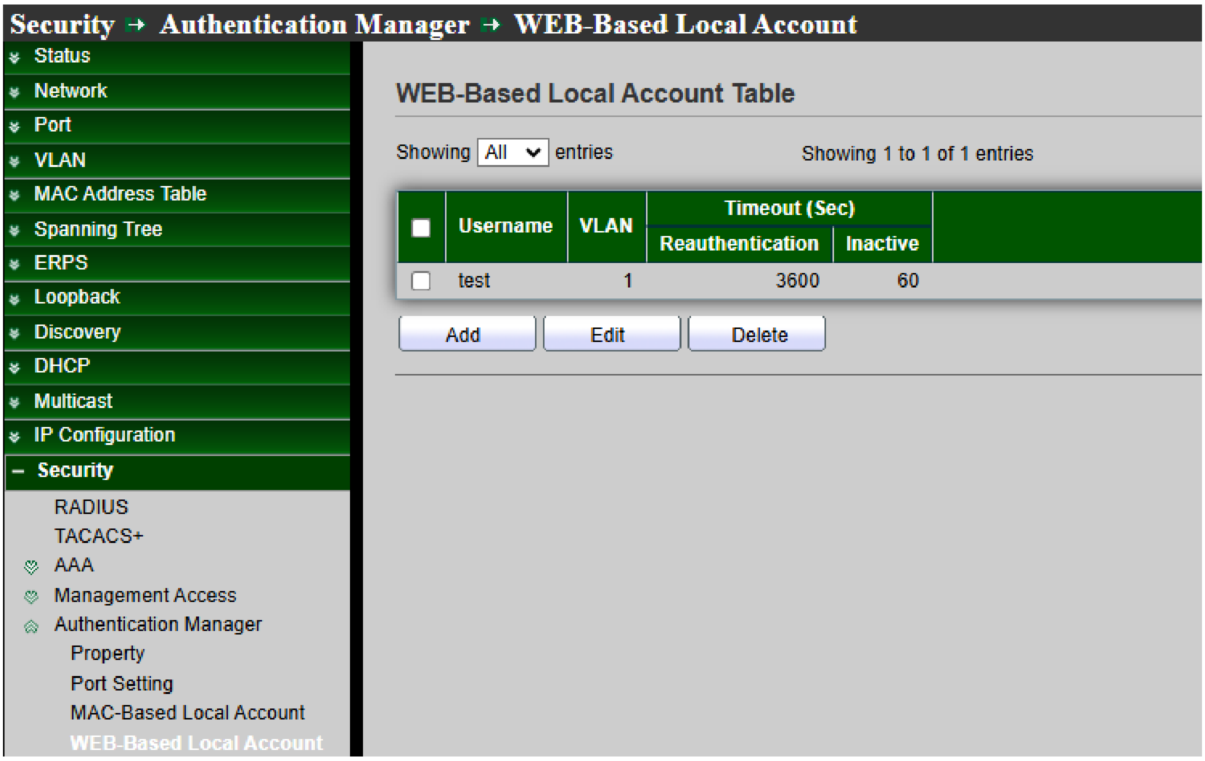
MAC Address	6C:F0:49:04:10:AC
Port Control	○ Force Authorized ● Force Unauthorized
VLAN	☑ User Defined 1 (1 - 4094)
Assigned Timer	
Reauthentication	☑ User Defined 3600 Sec (300 - 2147483647)
Inactive	☑ User Defined 60 Sec (60 - 65535)

- **MAC Address :** Authenticated host MAC address, and each MAC allow only one entry in local database.
- **Port Control :** Support following authentication port control types.
  - **Force Authorized:** Host will be force authorized.
  - **Force Authorized :** Host will be force unauthorized.
- **VLAN :** Assigned VLAN ID for the authenticated host.
- **Assigned Timer:**
  - **Timeout (Reauthentication) :** Assigned reauthentication period for the authenticated host.
  - **Timeout (Inactive) :** Assigned inactive timeout for the authenticated host.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

15.5.4 WEB-Based Local Account

Administrator can allow to add/edit/delete WEB-Based authentication local accounts, Setting **"add"** and **"Edit"** and **"Delete"** function for this management.



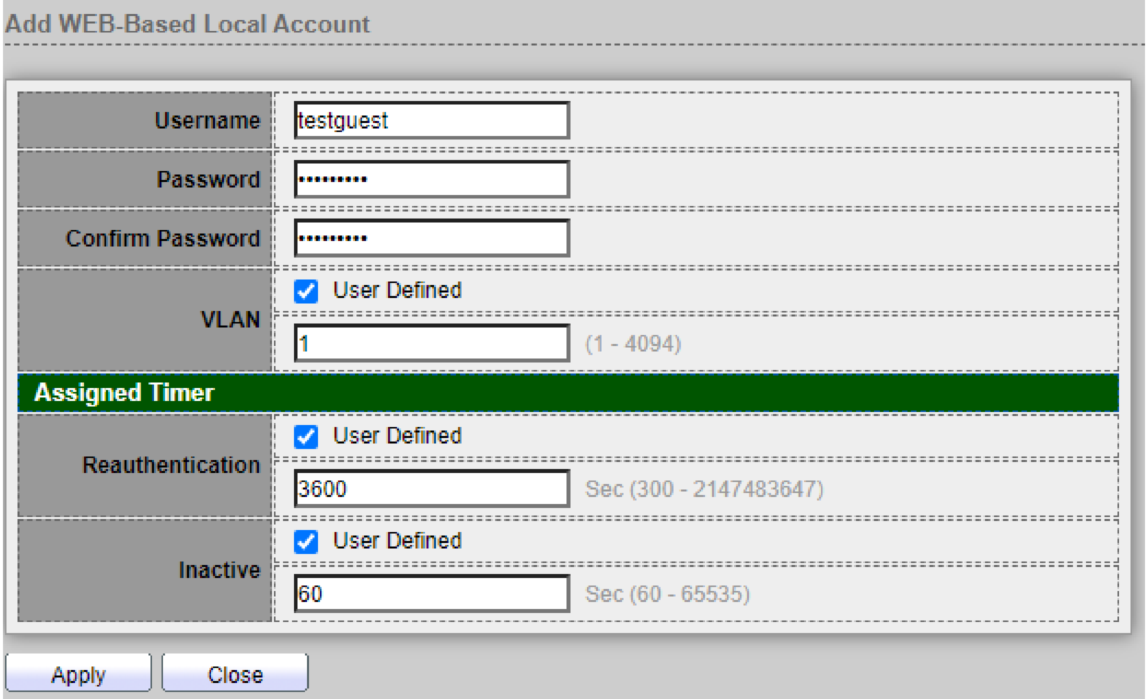
Security → Authentication Manager → WEB-Based Local Account

WEB-Based Local Account Table

Showing All entries   Showing 1 to 1 of 1 entries

□	Username	VLAN	Timeout (Sec)	
			Reauthentication	Inactive
□	test	1	3600	60

Field	Description
Username	Authenticating account user name
VLAN	Assigned VLAN ID for the authenticated host.
Timeout(Sec)	• **Reauthentication:** Assigned reauthentication period for the authenticated host. • **Inactive:** Assigned inactive timeout for the authenticated host.



Add WEB-Based Local Account

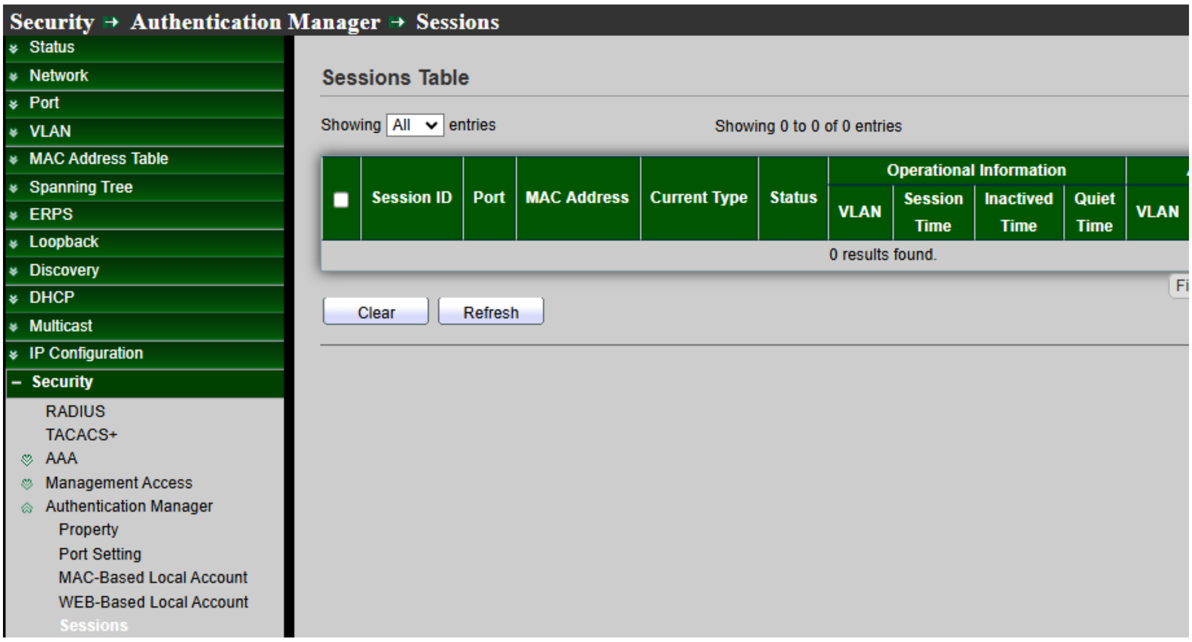
Username	testguest
Password	••••••••••
Confirm Password	••••••••••
VLAN	☑ User Defined 1 (1 - 4094)
Assigned Timer	
Reauthentication	☑ User Defined 3600 Sec (300 - 2147483647)
Inactive	☑ User Defined 60 Sec (60 - 65535)

- **Username :** Authenticating account user name.
- **Password :** Authenticating account password.
- **Confirm Password :** Confirm authenticating account password.
- **VLAN :** Assigned VLAN ID for the authenticated host.
- **Assigned Timer:**
  - **Timeout (Reauthentication) :** Assigned reauthentication period for the authenticated host.
  - **Timeout (Inactive) :** Assigned inactive timeout for the authenticated host.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

15.5.5 Sessions

Administrator can check all detail information of authentication sessions and allow user to select specific session to delete by clicking **"Clear "** button.

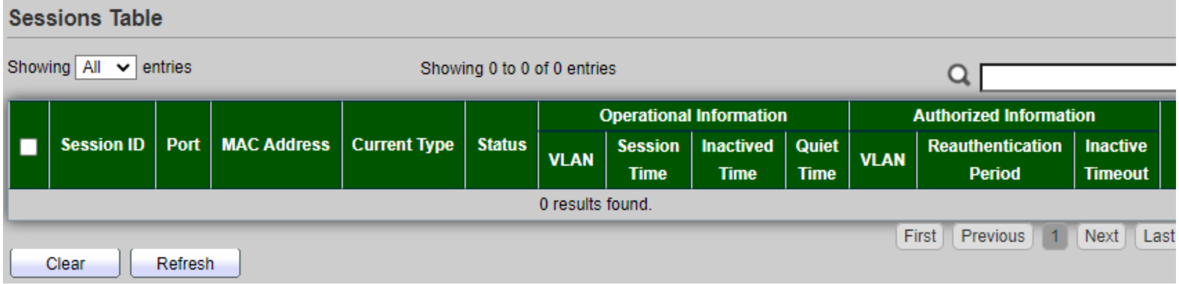


Security → Authentication Manager → Sessions

Sessions Table

Showing All entries Showing 0 to 0 of 0 entries

□	Session ID	Port	MAC Address	Current Type	Status	Operational Information				
						VLAN	Session Time	Inactived Time	Quiet Time	VLAN
0 results found.										



Sessions Table

Showing All entries Showing 0 to 0 of 0 entries

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

Field	Description
Session ID	Session ID is unique of each session
Port	Port name which the host located
MAC Address	Host MAC address
Current Type	Show current authenticating type • **802.1x:** Use IEEE 802.1X to do authenticating • **MAC-Based:** Use MAC-Based authentication to do authenticating • **WEB-Based:** Use WEB-Based authentication to do authenticating

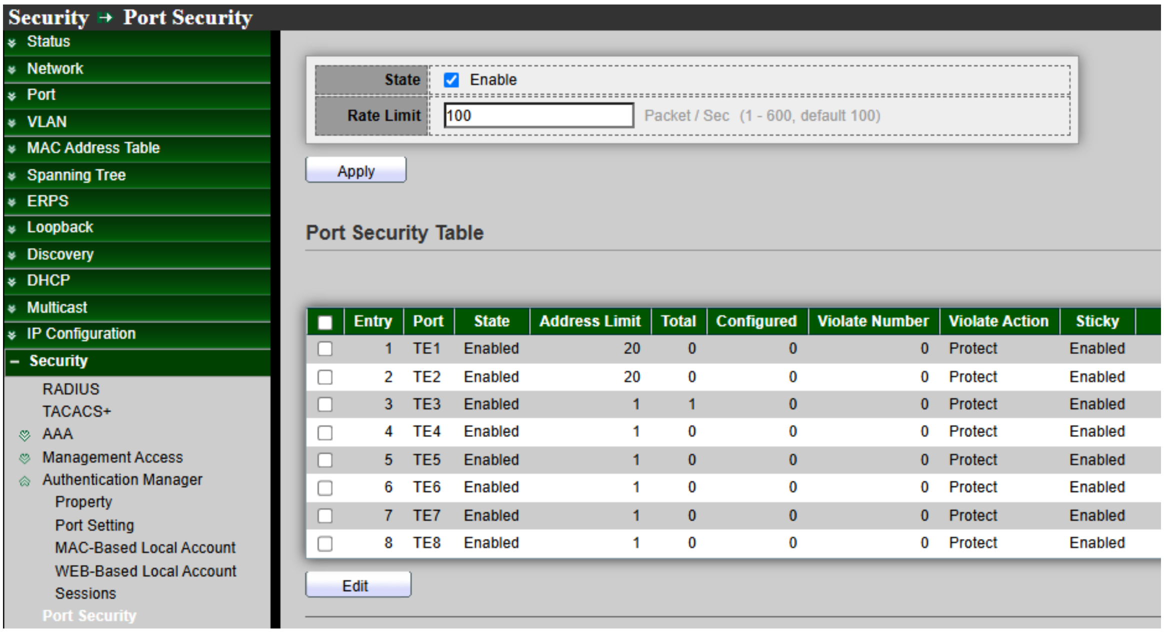
Status	Show host authentication session status • **Disable:** This session is ready to be deleted • **Running:** Authentication process is running • **Authorized:** Authentication is passed and getting network accessibility. • **UnAuthorized:** Authentication is not passed and not getting network accessibility. • **Locked:** Host is locked and do not allow to do authenticating until quiet period. • **Guest:** Host is in the guest VLAN.
Operationl	• **VLAN:** Shows host operational VLAN ID. • **Session Time:** In "Authorized" state, it shows total time after authorized. • **Inactived:** In "Authorized" state, it shows how long the host do not send any packet. • **Quiet Time:** In "Locked" state, it shows total time after locked. • **Locked:** Host is locked and do not allow to do authenticating until quiet period.
Authorized	• **VLAN:** Shows VLAN ID given from authorized procedure. • **Reauthentication Period:** Shows reauthentication period given from authorized procedure. • **Inactive Timeouts:** Shows inactive timeout given from authorized procedure.

*Click the **"Clear"** button to clear this page or click the **"Refresh"** button to refresh the page .*

15.6 Port Security

Port security examines all traffic received by secure ports to detect violations or to recognize and secure new MAC addresses. When the shutdown violation mode is configured, traffic cannot enter the secure port after a violation has been detected, which removes the possibility that violations might cause excessive CPU load.

Port security monitors received packets. Access to locked ports is limited to users with specific MAC addresses, This page allow user to configure port security settings for each interface. When port security is enabled on interface, action will be perform once MAC address over.



State ☑ Enable

Rate Limit 100 Packet / Sec (1 - 600, default 100)

Port Security Table

☐	Entry	Port	State	Address Limit	Total	Configured	Violate Number	Violate Action	Sticky
☐	1	TE1	Enabled	20	0	0	0	Protect	Enabled
☐	2	TE2	Enabled	20	0	0	0	Protect	Enabled
☐	3	TE3	Enabled	1	1	0	0	Protect	Enabled
☐	4	TE4	Enabled	1	0	0	0	Protect	Enabled
☐	5	TE5	Enabled	1	0	0	0	Protect	Enabled
☐	6	TE6	Enabled	1	0	0	0	Protect	Enabled
☐	7	TE7	Enabled	1	0	0	0	Protect	Enabled
☐	8	TE8	Enabled	1	0	0	0	Protect	Enabled

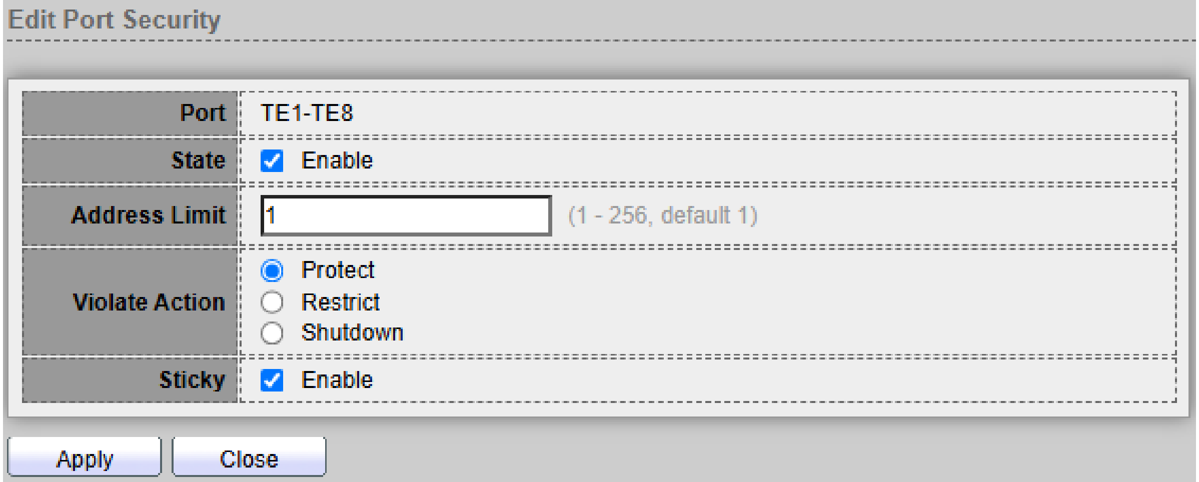
- **State:** Select the status of port security
  - **Disable:** Disable port security function.
  - **Enable:** Enable port security function.
- **Rate Limit :** Set rate limit of 1-600 packets per second.

Note	When the protect or restrict violation modes are configured, port security continues to process traffic after a violation occurs, which might cause excessive CPU load. Configure the port security rate limiter to protect the CPU against excessive load when the protect or restrict violation modes are configured.

*Click the **"Apply"** button to save your changes settings.*

Field	Description
Port	Port name which the port security.
State	Display port security of Enable or Disable state.
Addres Limie	Displays the maximum number of port security of MAC addresses that can be configured on the port.
Total	Displays the number of all port security total MAC addresses on the port.

Configured	Displays the number of all port security MAC addresses configured on the port.
Violate Active	Displays the operational state that the interface applies to packets arriving on the locked interface. • **Protect.** • **Restrict.** • **Shutdown.**
Sticky	Display port security sticky of Enable or Disable.



Edit Port Security

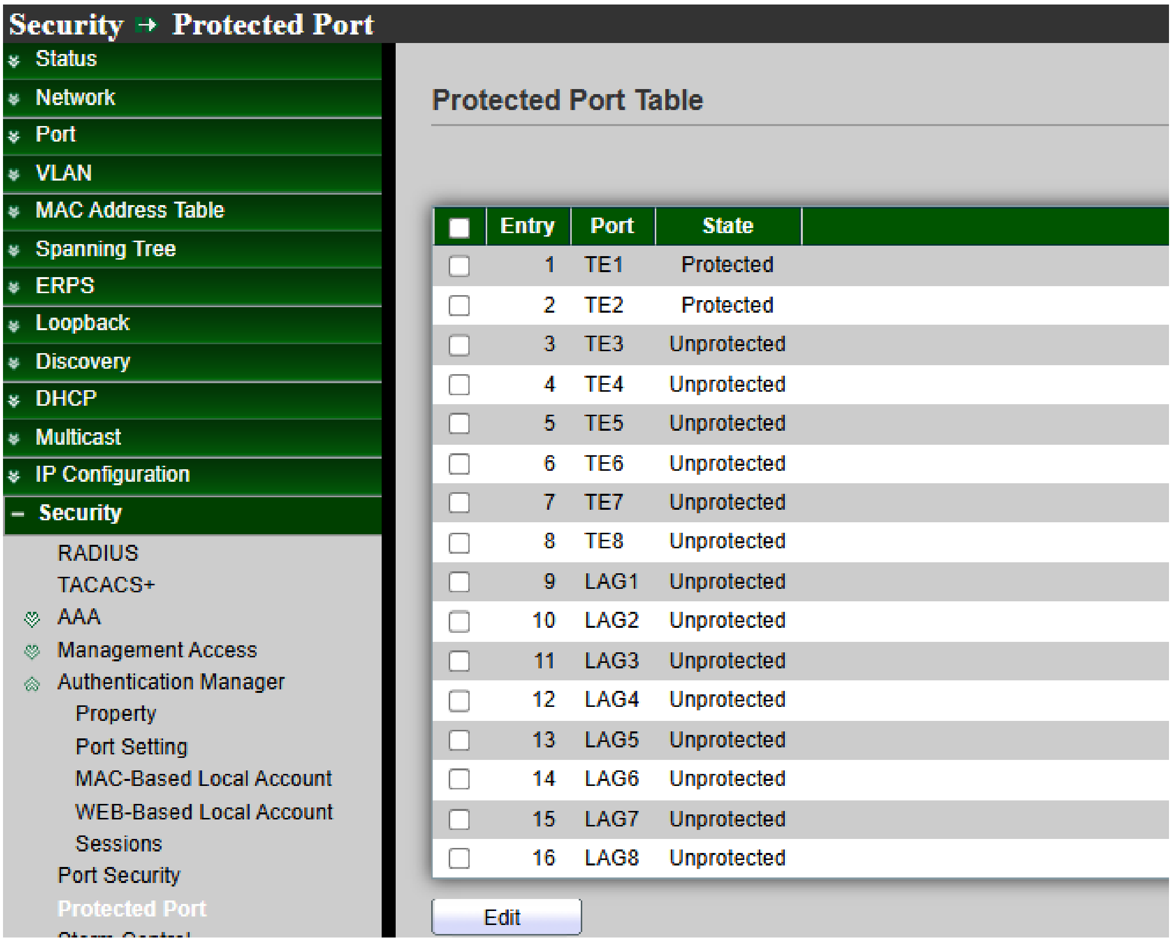
Port	TE1-TE8
State	☑ Enable
Address Limit	1 (1 - 256, default 1)
Violate Action	● Protect ○ Restrict ○ Shutdown
Sticky	☑ Enable

- **Port:** Display selected Port number.
- **State:** Enable or Un-Enable the port security.
- **Address Limit:** When configuring port security, the maximum number of secure MAC addresses that can be configured in the switch, A secure port has a default of one MAC address. The default can be changed to any value between 1 and 256. The upper limit of 256 guarantees one MAC address per port.
- **Violate Action:** Select the action if learned mac addresses, If Interface Status is locked, select an action to be applied to packets arriving on a locked interface.
  - **Protect:** Drop packets with invalid MAC address.
  - **Restrict:** Drop packets with invalid MAC address and log the event.
  - **Shutdown:** Drop packets with invalid MAC address and shut down the interface of port, and log the event.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

15.7 Protected Port

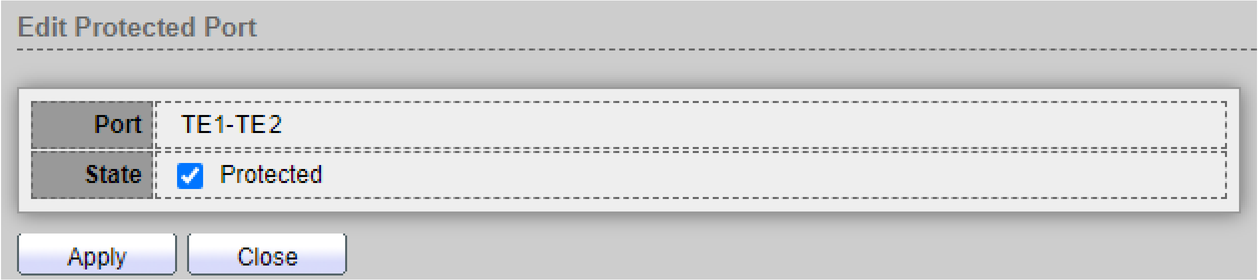
This page allow user to configure protected port setting to prevent the selected ports from communication with each other. Protected port is only allowed to communicate with unprotected port. In other words, protected port is not allowed to communicate with another protected port. If administrators check enable to make this a protected port. A protected port is also referred as a Private VLAN Edge. It's provide Layer 2 isolation between interfaces (Ethernet ports and Link Aggregation Groups) that share the same Broadcast domain (VLAN).After enable protected port, packets received from protected ports can be forwarded only to unprotected egress ports and unrestricted by VLAN members.



Protected Port Table

□	Entry	Port	State
□	1	TE1	Protected
□	2	TE2	Protected
□	3	TE3	Unprotected
□	4	TE4	Unprotected
□	5	TE5	Unprotected
□	6	TE6	Unprotected
□	7	TE7	Unprotected
□	8	TE8	Unprotected
□	9	LAG1	Unprotected
□	10	LAG2	Unprotected
□	11	LAG3	Unprotected
□	12	LAG4	Unprotected
□	13	LAG5	Unprotected
□	14	LAG6	Unprotected
□	15	LAG7	Unprotected
□	16	LAG8	Unprotected

Field	Description
Port	Port Name
State	Port protected admin state. • **Protected:** Port is protected. • **Unprotected:** Port is unprotected


Edit Protected Port

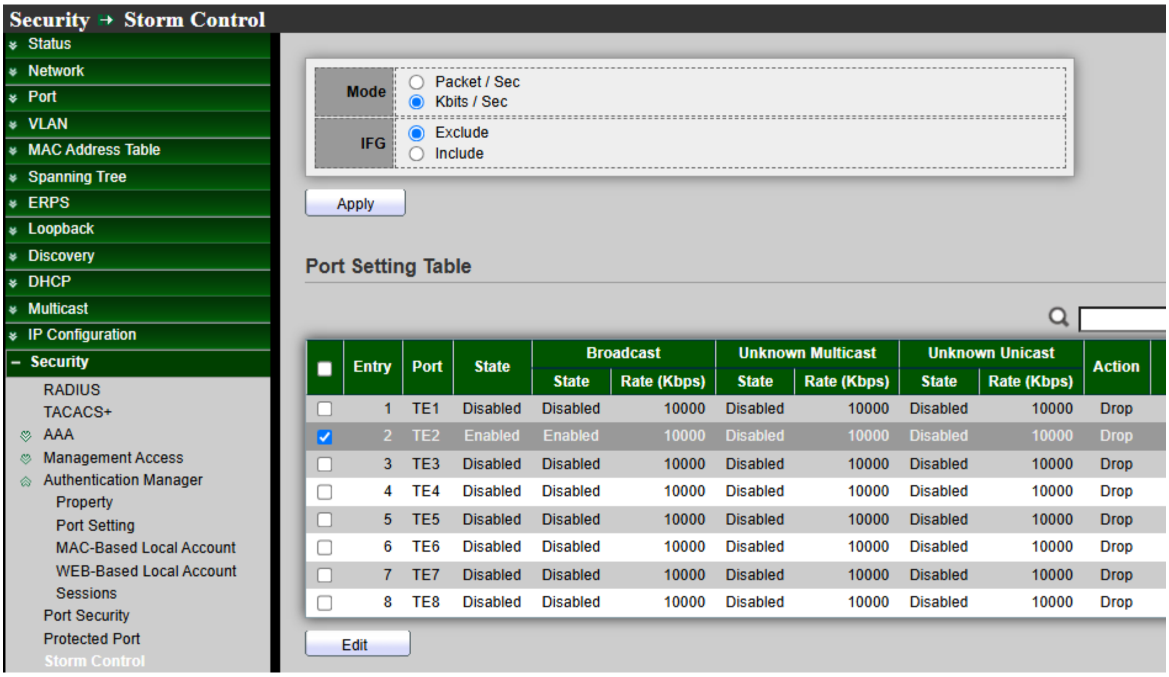
Port	TE1-TE2
State	☑ Protected

- ➢ **Port:** Display selected Port number.
- ➢ **State:** Port protected admin state.
  - **Protected:** Enable protecting function.
  - **Unprotected (deselect):** Disable protecting function

*Click the **"Apply"** button to save your changes or "**Close**" the button to close settings.*

15.8 Storm Control

When the rate of Broadcast / unknown Multicast or unknown Unicast frames is higher than the user-defined threshold, this function can to limit the number of frames entering the switch and to define the types of frames that are counted towards this limit. Will be the frames received beyond the threshold are discarded or the interface shuts down.


Security → Storm Control

Mode	○ Packet / Sec ● Kbits / Sec
IFG	● Exclude ○ Include

Port Setting Table

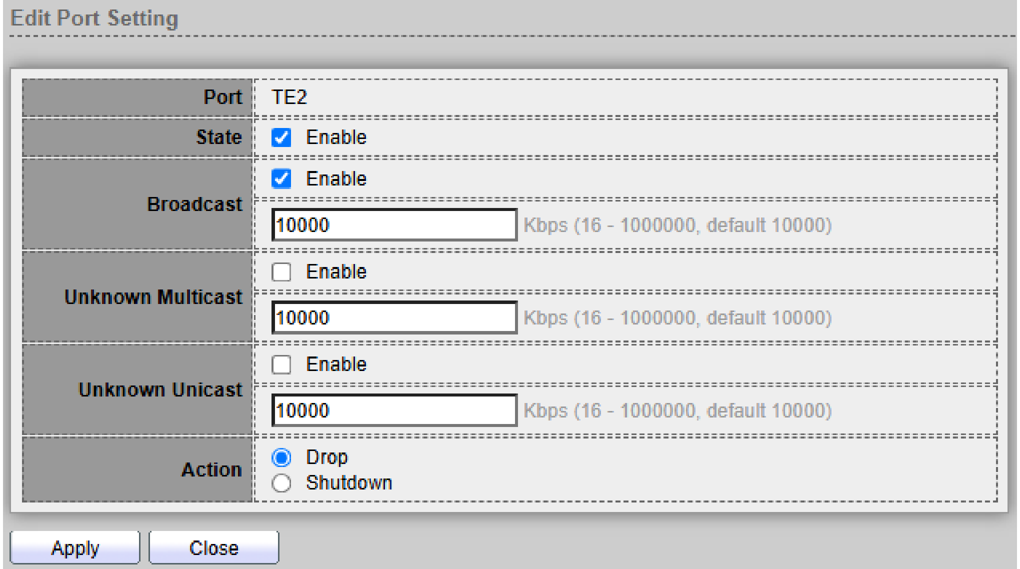
□	Entry	Port	State	Broadcast		Unknown Multicast		Unknown Unicast		Action
				State	Rate (Kbps)	State	Rate (Kbps)	State	Rate (Kbps)	
□	1	TE1	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☑	2	TE2	Enabled	Enabled	10000	Disabled	10000	Disabled	10000	Drop
□	3	TE3	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
□	4	TE4	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
□	5	TE5	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
□	6	TE6	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
□	7	TE7	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
□	8	TE8	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop

- ➢ **Mode:** Select the unit of storm control.
  - **Packets/sec:** Select by Packets/second of the rate threshold.
  - **Kbits/sec:** Select by Kbits/second of the rate threshold.

- **IFG:** Select the rate calculates w/o preamble & IFG (20 bytes).
  - **Excluded:** exclude preamble & IFG (20 bytes) when count ingress storm control rate.
  - **Include:** include preamble & IFG (20 bytes) when count ingress storm control rate.

*Click the **"Apply"** button to save your changes settings.*

Field	Description
Port	Port name which the host located.
State	Display enable or disable the storm control function.
Broadcast	Show the storm control for the Broadcast packets. • **State:** Display enable or disable the storm control for broadcast packets. • **Rate(Kpps):** Displays the bandwidth threshold for broadcast packets.
Unknown Multicast	Show the storm control for the unknown Multicast packets. • **State:** Display enable or disable the storm control for unknown Multicast packets . • **Rate(Kpps):** Displays the bandwidth threshold for unknown Multicast packets.
Unknown Unicast	Show the storm control for the unknown Unicast packets. • **State:** Display enable or disable the storm control for unknown Unicast packets . • **Rate(Kpps):** Displays the bandwidth threshold for unknown Unicast packets.
Action	• **Drop:** Received beyond the threshold will discard the frames, Packets exceed storm control rate will be dropped. • **Shutdown:** Received beyond the threshold will shut down the port, Port will be shutdown when packets exceed storm control rate.



Edit Port Setting

Port	TE2
State	☑ Enable
Broadcast	☑ Enable 10000 Kbps (16 - 1000000, default 10000)
Unknown Multicast	□ Enable 10000 Kbps (16 - 1000000, default 10000)
Unknown Unicast	□ Enable 10000 Kbps (16 - 1000000, default 10000)
Action	● Drop ○ Shutdown

- **Port:** Display selected Port number.
- **State:** Select the state of setting.
  - **Enable:** Enable the storm control function.
- **Broadcast:** If enable storm control for Broadcast traffic will count Broadcast traffic towards the bandwidth threshold.
  - **Enable:** Enable the storm control function of Broadcast packet, Value of storm control rate, Unit: Kbps (Kbits per-second, range16 - 1000000) depends on global mode setting.
- **Unknown Multicast:** If enable storm control for unknown Multicast will count unknown Multicast traffic towards the bandwidth threshold.
  - **Enable:** Enable the storm control function of Unknown Multicast packet, Value of storm control rate, Unit: Kbps (Kbits per-second, range16 - 1000000) depends on global mode setting.
- **Unknown Unicast:** If enable storm control for unknown Unicast will count unknown Unicast traffic towards the bandwidth threshold.
  - **Enable:** Enable the storm control function of Unknown Unicast packet, Value of storm control rate, Unit: Kbps (Kbits per-second, range16 - 1000000) depends on global mode setting.
- **Action:** Administrator can select Drop or Shutdown will Broadcast / unknown Multicast or unknown Unicast frames is higher than the user-defined threshold.
  - **Drop:** Received beyond the threshold will discard the frames, Packets exceed storm control rate will be dropped
  - **Shutdown:** Received beyond the threshold will shut down the port, Port will be shutdown when packets exceed storm control rate.

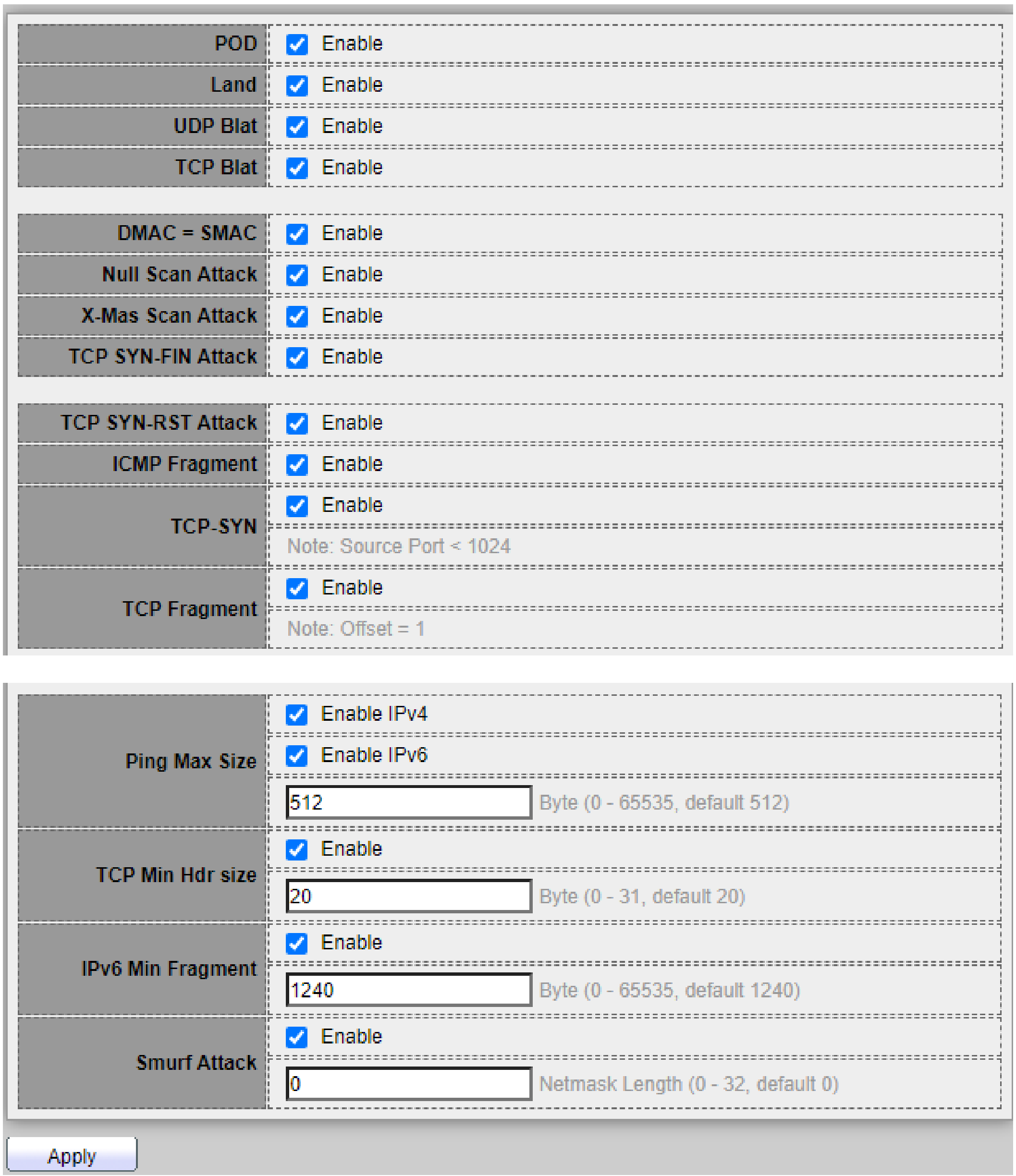
*Click the **"Apply"** button to save your changes or "**Close**" the button to close settings.*

15.9 DoS

DoS attack (denial-of-service) is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

15.9.1 Property

This default is enabled all DoS protection feature and SYN-FIN / SYN-RST protections. The default threshold is 60 SYN packets per second. The default period of port recovery is 60 seconds.



POD	☑ Enable
Land	☑ Enable
UDP Blat	☑ Enable
TCP Blat	☑ Enable
DMAC = SMAC	☑ Enable
Null Scan Attack	☑ Enable
X-Mas Scan Attack	☑ Enable
TCP SYN-FIN Attack	☑ Enable
TCP SYN-RST Attack	☑ Enable
ICMP Fragment	☑ Enable
TCP-SYN	☑ Enable Note: Source Port < 1024
TCP Fragment	☑ Enable Note: Offset = 1
Ping Max Size	☑ Enable IPv4 ☑ Enable IPv6 512 Byte (0 - 65535, default 512)
TCP Min Hdr size	☑ Enable 20 Byte (0 - 31, default 20)
IPv6 Min Fragment	☑ Enable 1240 Byte (0 - 65535, default 1240)
Smurf Attack	☑ Enable 0 Netmask Length (0 - 32, default 0)

- **POD:**
  - **Enable:** Enable the function of of avoids ping of death attack.
- **Land:**
  - **Enable:** Enable the function of drops the packets if the source IP address is equal to the destination IP address.
- **UDP Blat:**
  - **Enable:** Enable the function of drops the packets if the UDP source port equals to the UDP destination port.
- **TCP Blat:**
  - **Enable:** Enable the function of drops the packages if the TCP source port is equal to the TCP destination port.
- **DMAC = SMAC:**
  - **Enable:** Enable the function of drops the packets if the destination MAC address is equal to the source MAC address.
- **Null Scan Attach:**
  - **Enable:** Enable the function of drops the packets with NULL scan.
- **X-Mas Scan Attack:**
  - **Enable:** Enable the function of drops the packets if the sequence number is zero, and the FIN, URG and PSH bits are set.
- **TCP SYN-FIN Attack:**
  - **Enable:** Enable the function of drops the packets with SYN and FIN bits set.
- **TCP SYN-RST Attack:**
  - **Enable:** Enable the function of drops the packets with SYN and RST bits set.
- **ICMP Flagment:**
  - **Drop:** Enable the function of drops the fragmented ICMP packets.
- **TCP- SYN (SPORT<1024):**
  - **Enable:** Enable the function of drops SYN packets with sport less than 1024.
- **TCP Fragment (Offset = 1):**
  - **Enable:** Enable the function of drops the TCP fragment packets with offset equals to one.
- **Ping Max Size:**
  - **Enable:** Enable the function of specify the maximum size of the ICMPv4/ICMPv6 ping packets. The valid range is from 0 to 65535 bytes, and the default value is 512 bytes.
- **IPv4 Ping Max Size:**
  - **Enable:** Enable the function of checks the maximum size of ICMP ping packets, and drops the packets larger than the maximum packet size.
- **IPv6 Ping Max Size:**

- **Enable:** Enable the function of checks the maximum size of ICMPv6 ping packets, and drops the packets larger than the maximum packet size.

➢ **TCP Min Hdr Size:**

- **Enable:** Enable the function of checks the minimum TCP header and drops the TCP packets with the header smaller than the minimum size. The length range is from 0 to 31 bytes, and default length is 20 bytes.

➢ **IPv6 Min Flagment:**

- **Enable:** Enable the function of checks the minimum size of IPv6 fragments, and drops the packets smaller than the minimum size. The valid range is from 0 to 65535 bytes, and default value is 1240 bytes.

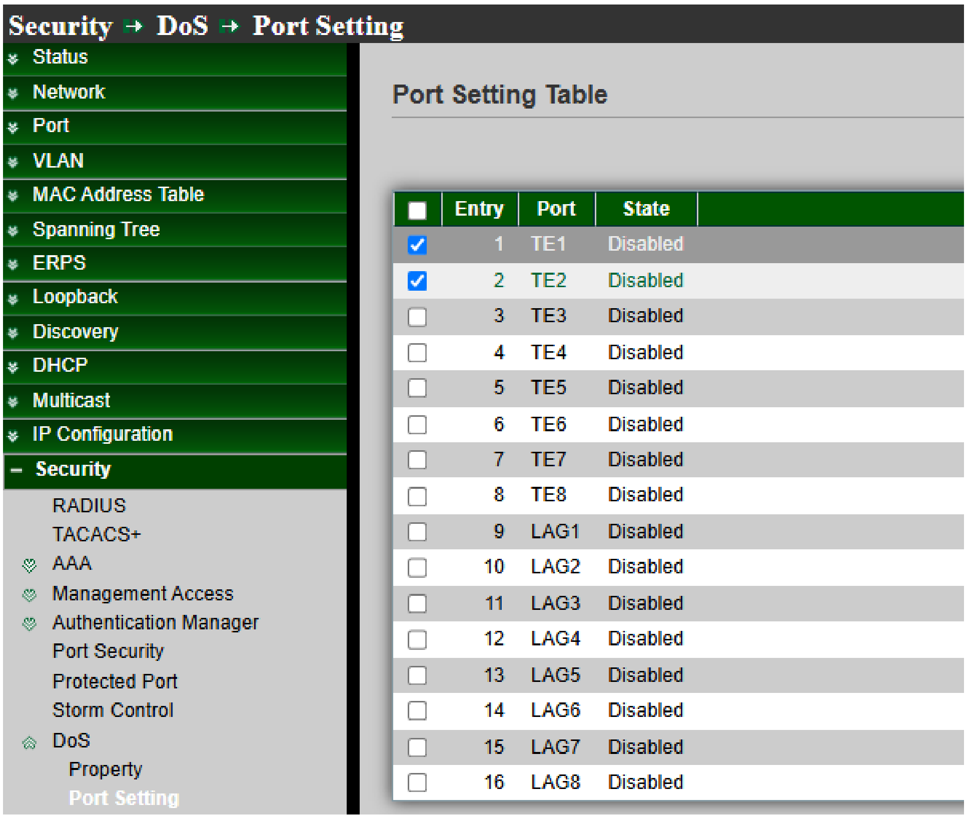
➢ **Smurf Attack:**

- **Enable:** Enable the function of avoids smurf attack. The length range of the netmask is from 0 to 323 bytes, and default length is 0 bytes.

*Click the **“Apply”** button to save your changes settings*

15.9.2 Port Setting

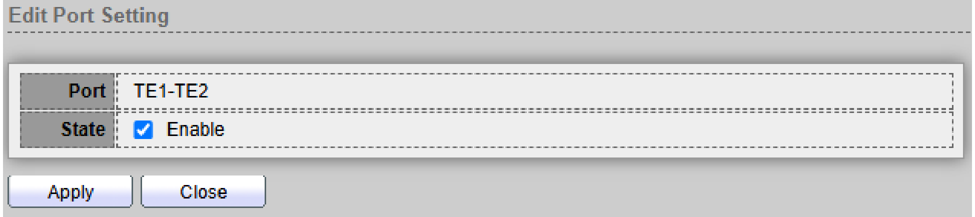
Administrator can choose protected ports.



Port Setting Table

☐	Entry	Port	State
☑	1	TE1	Disabled
☑	2	TE2	Disabled
☐	3	TE3	Disabled
☐	4	TE4	Disabled
☐	5	TE5	Disabled
☐	6	TE6	Disabled
☐	7	TE7	Disabled
☐	8	TE8	Disabled
☐	9	LAG1	Disabled
☐	10	LAG2	Disabled
☐	11	LAG3	Disabled
☐	12	LAG4	Disabled
☐	13	LAG5	Disabled
☐	14	LAG6	Disabled
☐	15	LAG7	Disabled
☐	16	LAG8	Disabled

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



Edit Port Setting

Port	TE1-TE2
State	☑ Enable

- **Port:** Display selected Port number.
- **State:** Select the state of setting.
  - **Enable:** Enable the DoS protection function.

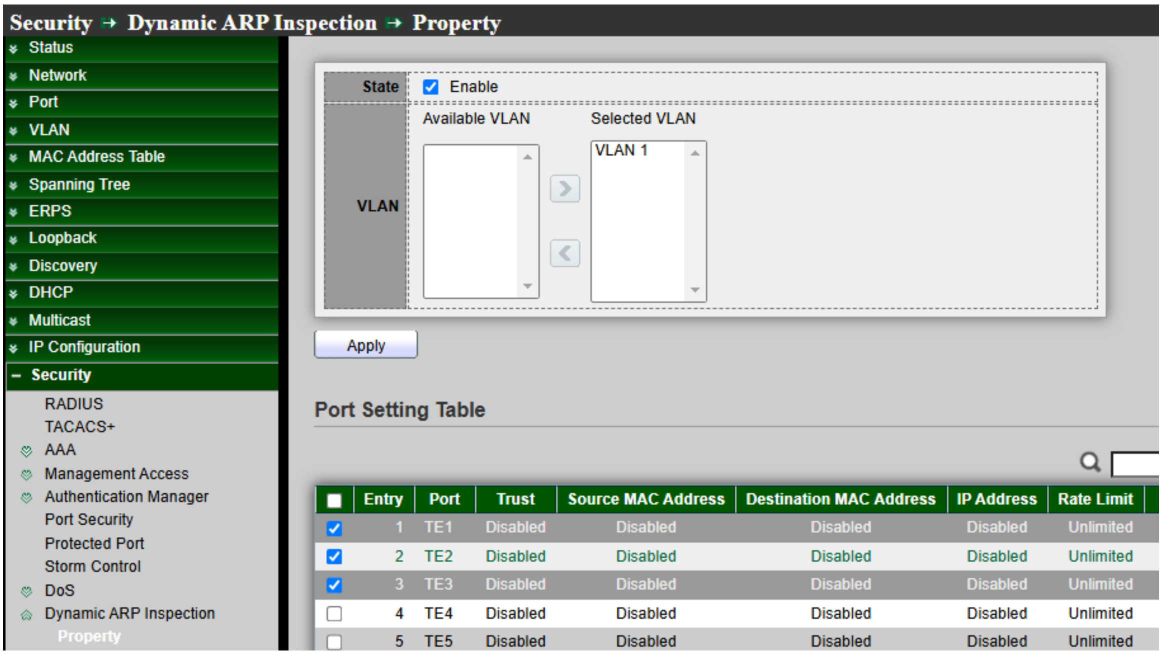
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

15.10 Dynamic ARP Inspection

Dynamic Address Resolution Protocol (ARP) is a TCP/IP protocol for translating IP addresses into MAC addresses. Use the Dynamic ARP Inspection pages to configure settings of Dynamic ARP Inspection.

15.10.1 Property

This page allow user to configure global and per interface settings of Dynamic ARP Inspection.



State: ☑ Enable

VLAN: Available VLAN — Selected VLAN: VLAN 1

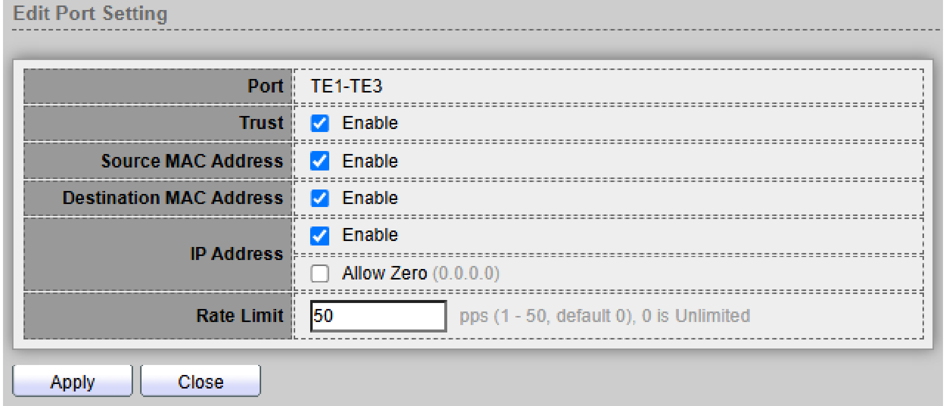
Port Setting Table

□	Entry	Port	Trust	Source MAC Address	Destination MAC Address	IP Address	Rate Limit
☑	1	TE1	Disabled	Disabled	Disabled	Disabled	Unlimited
☑	2	TE2	Disabled	Disabled	Disabled	Disabled	Unlimited
☑	3	TE3	Disabled	Disabled	Disabled	Disabled	Unlimited
□	4	TE4	Disabled	Disabled	Disabled	Disabled	Unlimited
□	5	TE5	Disabled	Disabled	Disabled	Disabled	Unlimited

- **State:** Administrator can enable or disable this Dynamic ARP Inspection. Set checkbox to enable/disable Dynamic ARP Inspection function.
- **VLAN:** In the Enabled VLAN table, users assign static ARP Inspection lists to enabled VLANs. When a packet passes through an untrusted interface that is enabled for ARP Inspection switch will performs the checks, Select VLANs in left box then move to right to enable Dynamic ARP Inspection. Or select VLANs in right box then move to left to disable Dynamic ARP Inspection.

*Click the **"Apply"** button to save your changes settings*

Field	Description
Port	Port the port ID.
Trust	Display enable/disabled trust attribute of interface.
Source MAC Address	Display enable/disabled source mac address validation attribute of interface.
Destination MAC Address	Display enable/disabled destination mac address validation attribute of interface.
IP Address	Display enable/disabled IP address validation attribute of interface, Allow zero which means allow 0.0.0.0 IP address.
Rate Limit	Display rate limitation value of interface.



Edit Port Setting

Port	TE1-TE3
Trust	☑ Enable
Source MAC Address	☑ Enable
Destination MAC Address	☑ Enable
IP Address	☑ Enable □ Allow Zero (0.0.0.0)
Rate Limit	50 pps (1 - 50, default 0), 0 is Unlimited

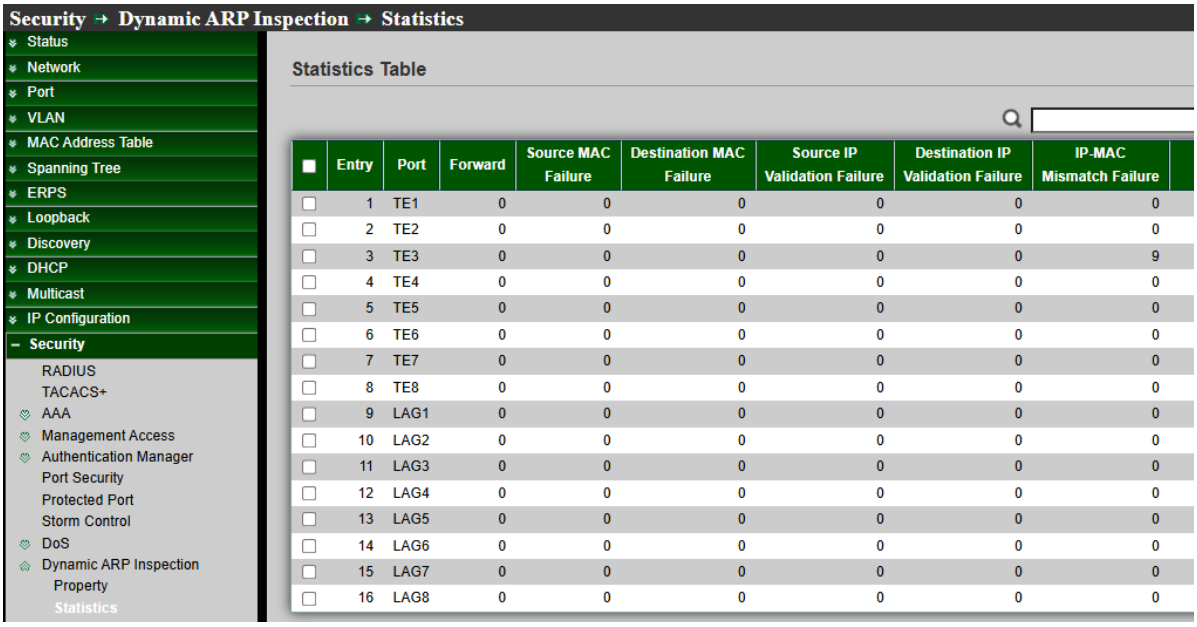
- **Port:** Display selected Port number.
- **Trust:** If enabled, the port or LAG is a trusted interface, and ARP inspection is not performed on the ARP requests or replies sent to or from the interface. If Un-Enable, the port or LAG is not a trusted interface, and ARP inspection is performed on the ARP requests or replies sent to or from the interface. By default, it is disabled.

- **Source MAC Address:** Check Enable to validate the source MAC addresses in ARP requests and replies, Set checkbox to enable or disable source mac address validation of interface. All ARP packets will be checked whether sender mac is same as source mac in Ethernet header if enable source mac address validation. Default is disabled.
- **Destination MAC Address:** Check Enable to validate the destination MAC addresses in ARP replies, Set checkbox to enable or disable destination mac address validation of interface. All ARP packets will be checked whether target mac is same as destination mac in Ethernet header if enable destination mac address validation. Default is disabled.
- **IP Address:** Set checkbox to enable or disable IP address validation of interface. All ARP packets will be checked whether IP address is 0.0.0.0,255.255.255.255 or multicast address. Default is disabled.
  - **Allow all-zeros IP:** If IP address validation is enabled, check Enable to allow 0.0.0.0 the IP address.
- **Rate Limit:** Enter the maximum rate that is allowed on the interface. The range is 1 to 50pps and the default is 0 Unlimited.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

15.10.2 Statistics

The Statistics page will displays the statistical information for ARP Inspection.



Statistics Table

☐	Entry	Port	Forward	Source MAC Failure	Destination MAC Failure	Source IP Validation Failure	Destination IP Validation Failure	IP-MAC Mismatch Failure
☐	1	TE1	0	0	0	0	0	0
☐	2	TE2	0	0	0	0	0	0
☐	3	TE3	0	0	0	0	0	9
☐	4	TE4	0	0	0	0	0	0
☐	5	TE5	0	0	0	0	0	0
☐	6	TE6	0	0	0	0	0	0
☐	7	TE7	0	0	0	0	0	0
☐	8	TE8	0	0	0	0	0	0
☐	9	LAG1	0	0	0	0	0	0
☐	10	LAG2	0	0	0	0	0	0
☐	11	LAG3	0	0	0	0	0	0
☐	12	LAG4	0	0	0	0	0	0
☐	13	LAG5	0	0	0	0	0	0
☐	14	LAG6	0	0	0	0	0	0
☐	15	LAG7	0	0	0	0	0	0
☐	16	LAG8	0	0	0	0	0	0

Field	Description
Port	Interface of port number.

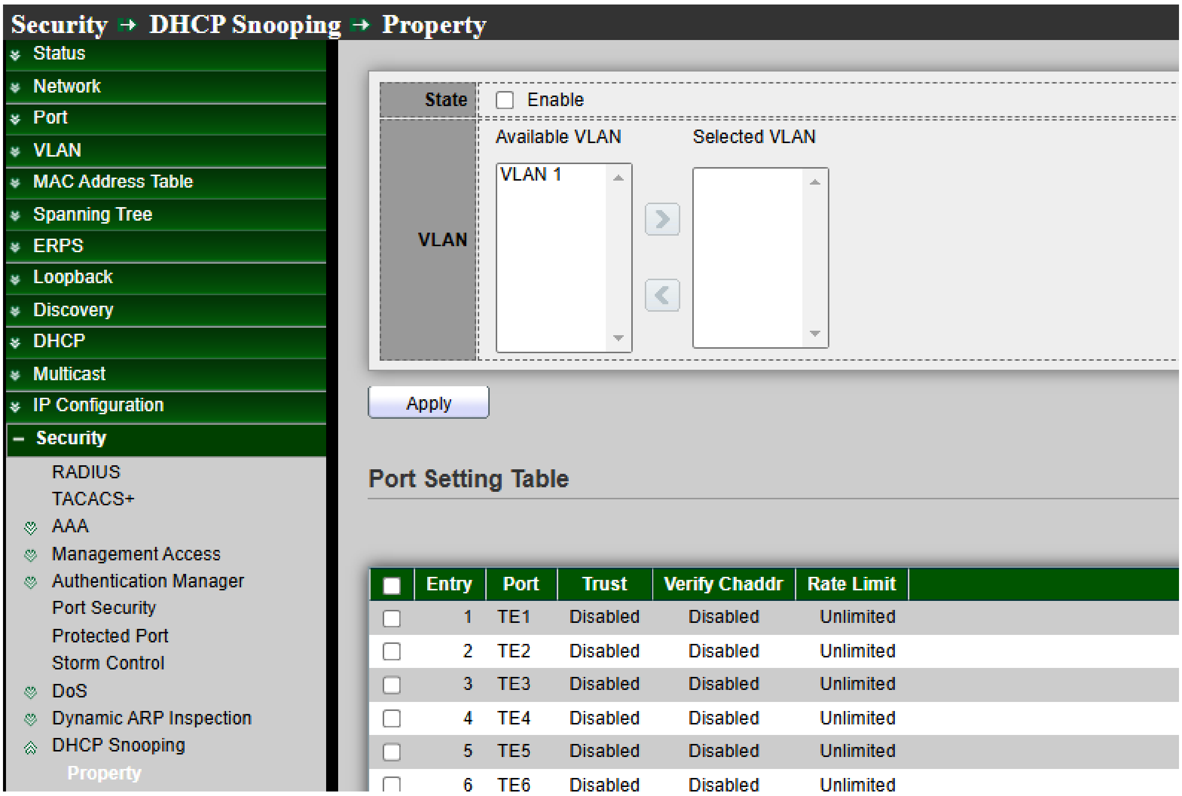
Forward	Display how many packets forwarded normally.
Source MAC Failure	Display how many packets dropped by source MAC validation.
Destination MAC Failure	Display how many packets dropped by destination MAC validation.
Source IP Address Validation Failures	Display how many packets dropped by source IP validation.
Destination IP Address Validation Failures	Display how many packets dropped by destination IP validation.
IP-MAC Mismatch Failures	Display how many packets dropped by IP-MAC doesn’t match in IP Source Guard binding table.

15.11 DHCP Snooping

Administrator can use DHCP snooping to help avoid the Denial of Service attacks that result from unauthorized users adding a DHCP server to the network that then provides invalid configuration data to other DHCP clients on the network. DHCP packets received on other switch ports are inspected before being forwarded. Packets from untrusted sources are dropped.

15.11.1 Property

This page allow user to configure global and per interface settings of DHCP Snooping.



State: □ Enable

VLAN: Available VLAN: VLAN 1 | Selected VLAN:

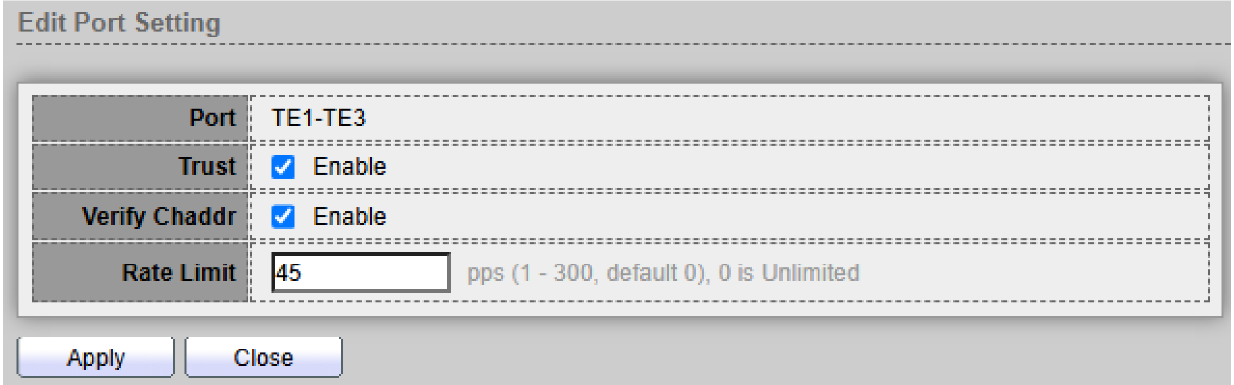
Port Setting Table

□	Entry	Port	Trust	Verify Chaddr	Rate Limit
□	1	TE1	Disabled	Disabled	Unlimited
□	2	TE2	Disabled	Disabled	Unlimited
□	3	TE3	Disabled	Disabled	Unlimited
□	4	TE4	Disabled	Disabled	Unlimited
□	5	TE5	Disabled	Disabled	Unlimited
□	6	TE6	Disabled	Disabled	Unlimited

- **State:** Administrator can enable or Un-Enable DHCP Snooping, Set checkbox to enable/disable DHCP Snooping function.
- **VLAN:** Administrator can to enable DHCP Snooping on a VLAN, ensure that DHCP Snooping is globally enabled on the switch, Select VLANs in left box then move to right to enable DHCP Snooping. Or select VLANs in right box then move to left to disable DHCP Snooping.

*Click the **"Apply"** button to save your changes settings.*

Field	Description
Port	Interface of port number.
Trust	Display enable/disabled trust attribute of interface.
Verify Chaddr	Display enable/disabled chaddr validation attribute of interface.
Rate Limit	Display rate limitation value of interface.



Edit Port Setting

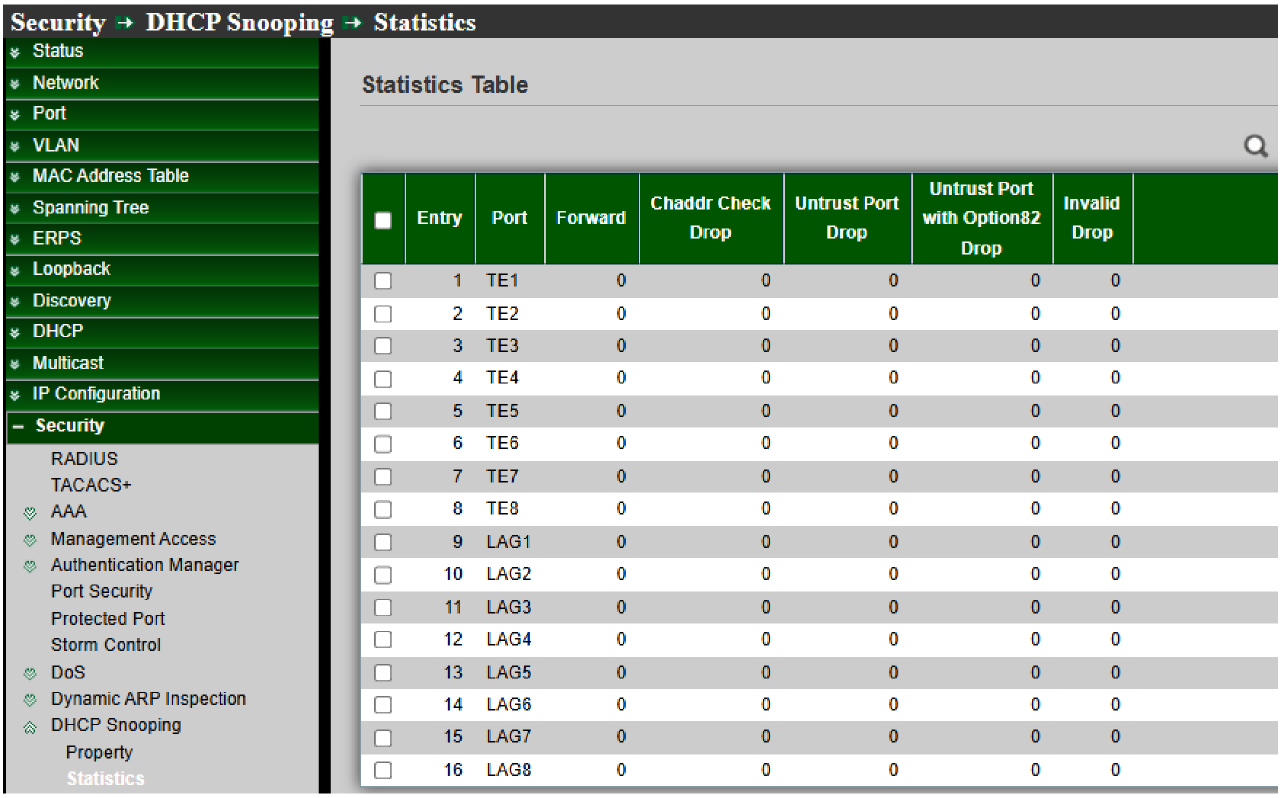
Port	TE1-TE3
Trust	☑ Enable
Verify Chaddr	☑ Enable
Rate Limit	45 pps (1 - 300, default 0), 0 is Unlimited

- **Port:** Display selected Port number.
- **Trust:** If check Enable will connected to a DHCP server or to other switches or routers as trusted ports, Set checkbox to enable/disabled trust of interface. All DHCP packet will be forward directly if enable trust. Default is disabled
- **Verify Chaddr:** Set checkbox to enable or disable chaddr validation of interface. All DHCP packets will be checked whether client hardware mac address is same as source mac in Ethernet header if enable chaddr validation. Default is disabled.
- **Rate Limit:** Enter the maximum rate that is allowed on the interface. The range is 1 to 300pps and the default is 0 Unlimited.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

15.11.2 Statistics

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



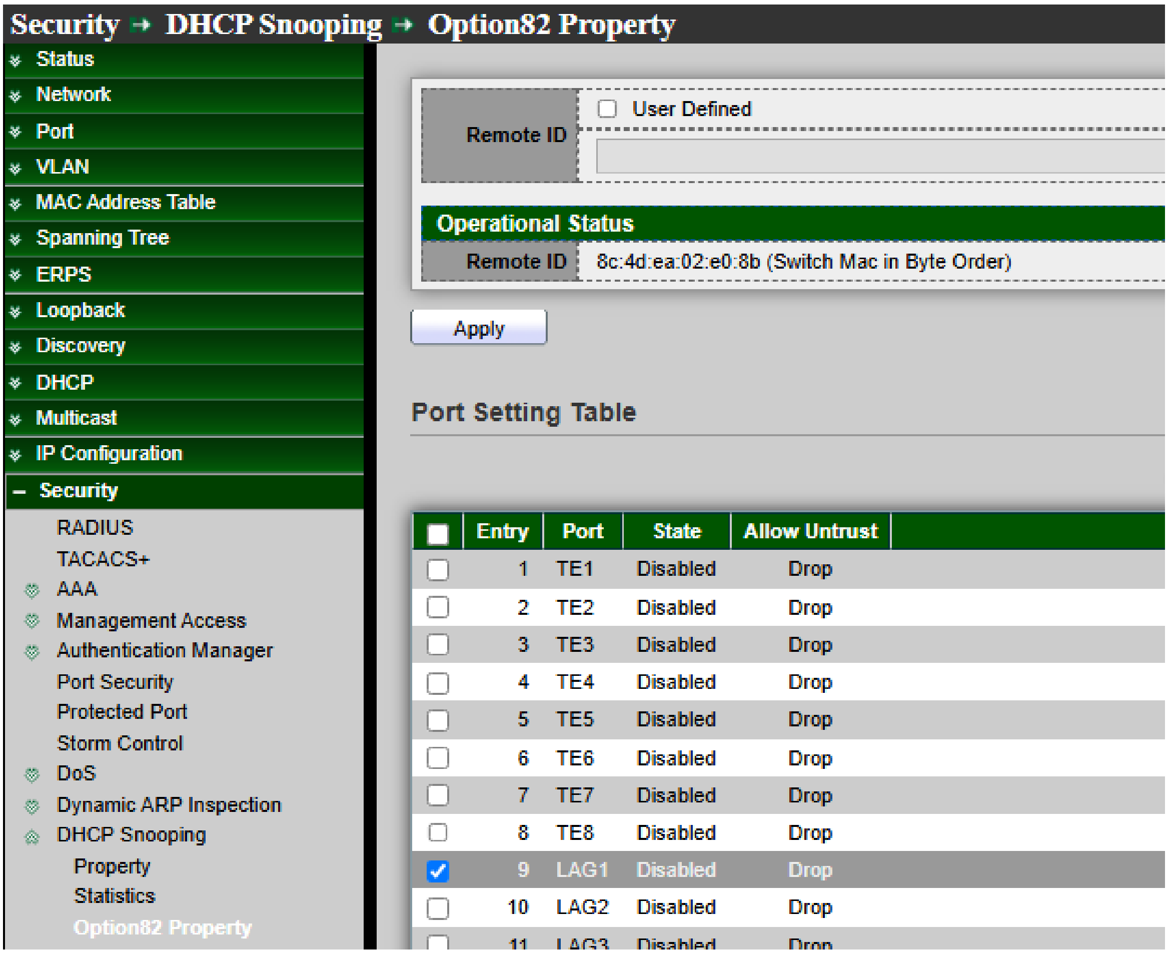
Statistics Table

□	Entry	Port	Forward	Chaddr Check Drop	Untrust Port Drop	Untrust Port with Option82 Drop	Invalid Drop
□	1	TE1	0	0	0	0	0
□	2	TE2	0	0	0	0	0
□	3	TE3	0	0	0	0	0
□	4	TE4	0	0	0	0	0
□	5	TE5	0	0	0	0	0
□	6	TE6	0	0	0	0	0
□	7	TE7	0	0	0	0	0
□	8	TE8	0	0	0	0	0
□	9	LAG1	0	0	0	0	0
□	10	LAG2	0	0	0	0	0
□	11	LAG3	0	0	0	0	0
□	12	LAG4	0	0	0	0	0
□	13	LAG5	0	0	0	0	0
□	14	LAG6	0	0	0	0	0
□	15	LAG7	0	0	0	0	0
□	16	LAG8	0	0	0	0	0

Field	Description
Port	Interface of port number.
Forward	Display how many packets forwarded normally.
Chaddr Check Drop	Display how many packets dropped by chaddr validation.
Untrusted Port Drop	Display how many DHCP server packets that are received by untrusted port dropped.
Untrusted Port with Option82 Drop	Display how many packets dropped by untrusted port with option82 checking.
Invalid Drop	Display how many packets dropped by invalid checking.

15.11.3 Option82 Property

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



Remote ID	□ User Defined

Operational Status

Remote ID	8c:4d:ea:02:e0:8b (Switch Mac in Byte Order)

Port Setting Table

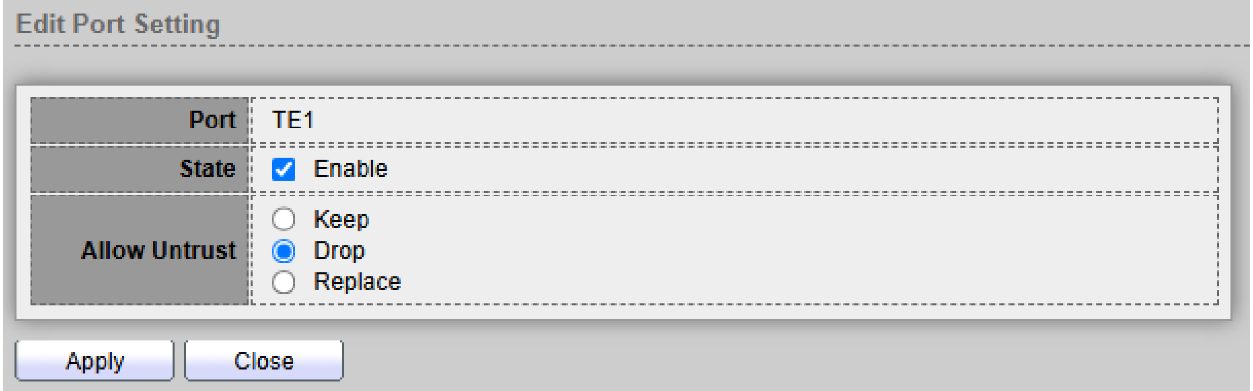
□	Entry	Port	State	Allow Untrust
□	1	TE1	Disabled	Drop
□	2	TE2	Disabled	Drop
□	3	TE3	Disabled	Drop
□	4	TE4	Disabled	Drop
□	5	TE5	Disabled	Drop
□	6	TE6	Disabled	Drop
□	7	TE7	Disabled	Drop
□	8	TE8	Disabled	Drop
☑	9	LAG1	Disabled	Drop
□	10	LAG2	Disabled	Drop
□	11	LAG3	Disabled	Drop

- **Remote ID:** If Option 82 is enabled, select User Defined to manually enter the format remote ID, Set checkbox to enable user-defined remote-ID. By default, remote ID is switch mac in byte order.
  Input user-defined remote ID. Only available when enable user-define remote ID.

Field	Description
Operational Status	Display remote ID information.

*Click the **"Apply"** button to save your changes settings.*

Field	Description
Port	Interface of port number.
State	Set checkbox to enable/disable option82 function of interface.
Allow untrusted	Display allow untrusted action of interface.



Edit Port Setting

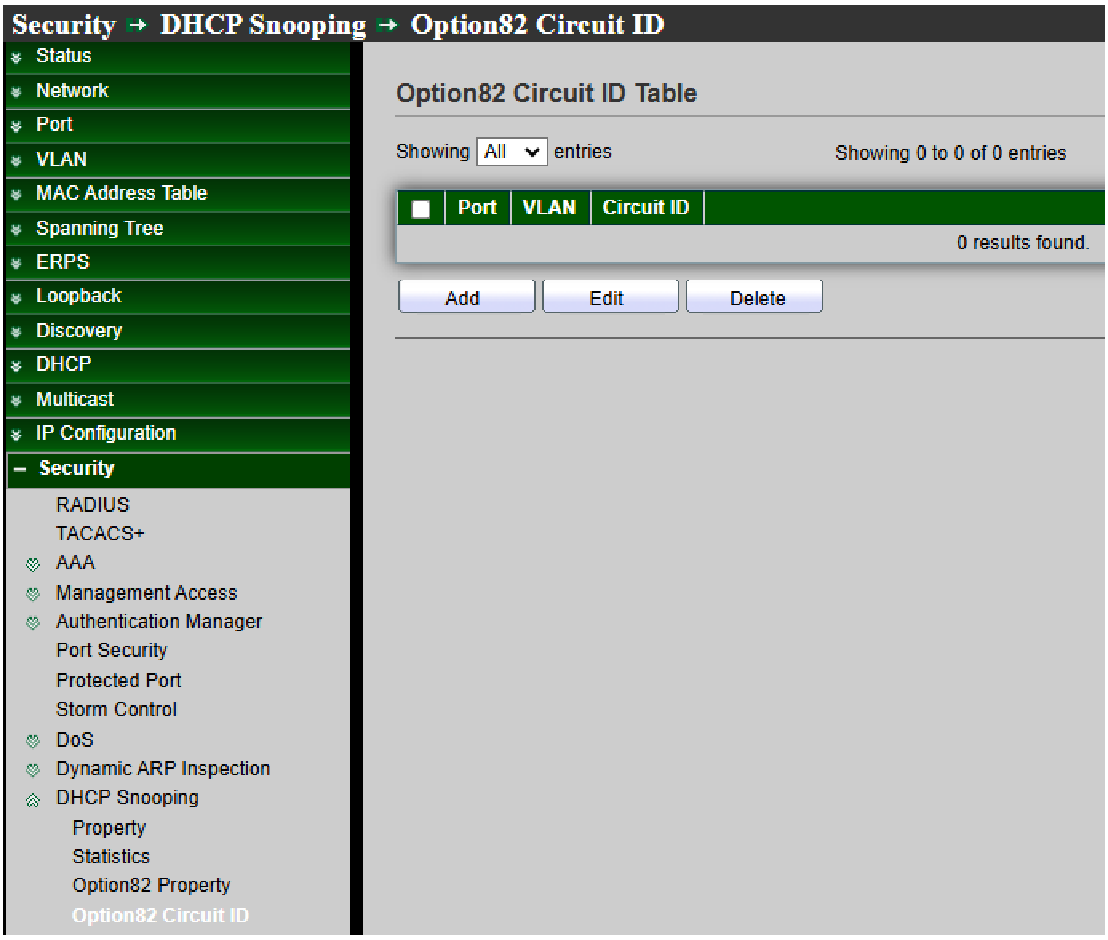
Port	TE1
State	☑ Enable
Allow Untrust	○ Keep ● Drop ○ Replace

- **Port:** Display selected Port number.
- **State:** Check Enable or Un-Enable, Display option82 enable/disable status of interface.
- **Allow untrusted:** Select the action perform when untrusted port receive DHCP packet has option82 filed. Default is drop.
  - **Keep:** Keep original option82 content.
  - **Drop:** Drop packets with option82.
  - **Replace:** Replace option82 content by switch setting.

*Click the **“Apply”** button to save your changes or **“Close”** the button to close settings.*

15.11.4 Option82 Circuit ID

Administrator can use the Option82 Port CID Settings page to configure the Option 82 circuit-ID Setting **“add”** and “Edit” and **“Delete”** function management, This page allow user to set string of DHCP option82 circuit ID filed. The string will attach in option82 if option inserted.



Security → DHCP Snooping → Option82 Circuit ID

Option82 Circuit ID Table

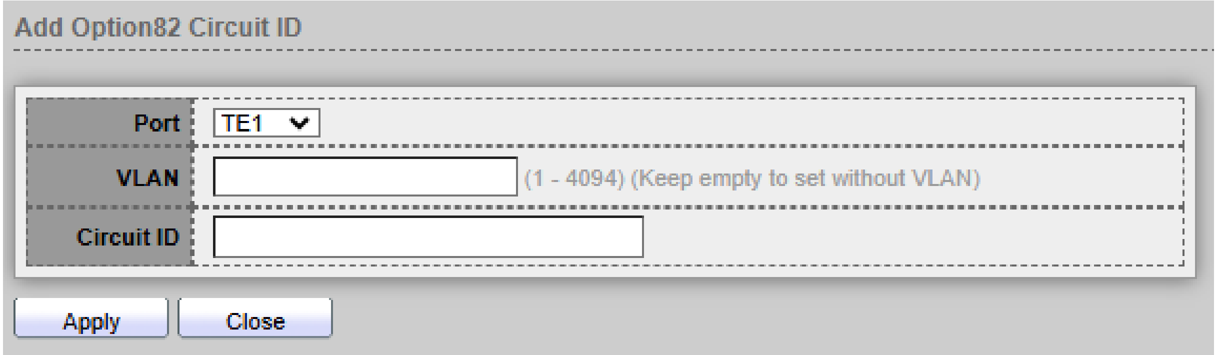
Showing All entries

Showing 0 to 0 of 0 entries

□	Port	VLAN	Circuit ID

0 results found.

Field	Description
Port	Display port ID of entry.
VLAN	Display associate VLAN of entry.
Circuit ID	Display circuit ID string of entry.



Add Option82 Circuit ID

Port	TE1
VLAN	(1 - 4094) (Keep empty to set without VLAN)
Circuit ID	

- **Port:** Select port from list to associate to CID entry. Only available on Add dialog.
- **VLAN:** Input VLAN ID to associate to circuit ID entry. VLAN ID is not mandatory. Only available on Add dialog.

- ➢ **Dircuit ID:** Input String as circuit ID. Packets match port and VLAN will be inserted circuit ID.

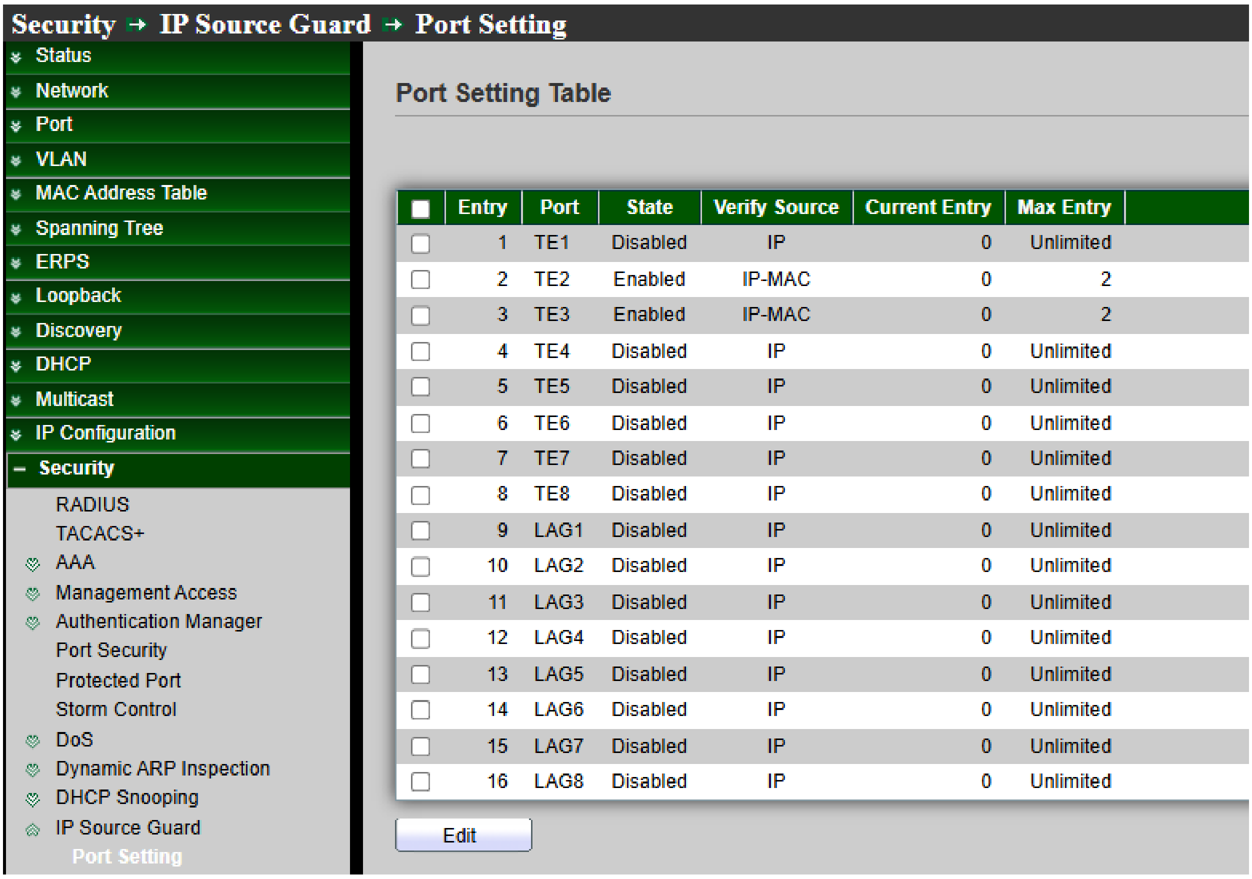
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

15.12 IP Source Guard

IP Source Guard restricts the client IP traffic to those source IP addresses configured in the IP Source binding database, mainly can prevent traffic attacks caused when a host tries to use the IP address of its neighbor.

15.12.1 Port Setting

This page allow user to configure per port settings of IP Source Guard.

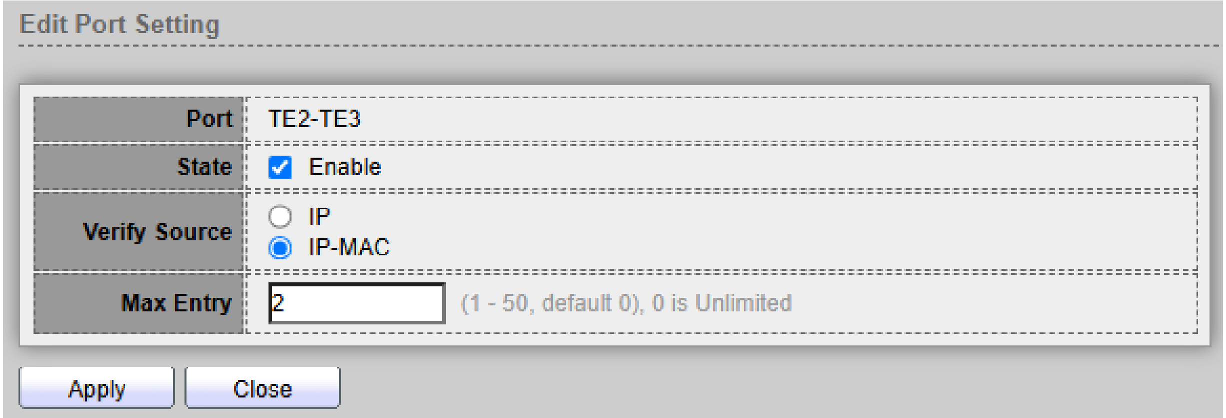


Port Setting Table

□	Entry	Port	State	Verify Source	Current Entry	Max Entry
□	1	TE1	Disabled	IP	0	Unlimited
□	2	TE2	Enabled	IP-MAC	0	2
□	3	TE3	Enabled	IP-MAC	0	2
□	4	TE4	Disabled	IP	0	Unlimited
□	5	TE5	Disabled	IP	0	Unlimited
□	6	TE6	Disabled	IP	0	Unlimited
□	7	TE7	Disabled	IP	0	Unlimited
□	8	TE8	Disabled	IP	0	Unlimited
□	9	LAG1	Disabled	IP	0	Unlimited
□	10	LAG2	Disabled	IP	0	Unlimited
□	11	LAG3	Disabled	IP	0	Unlimited
□	12	LAG4	Disabled	IP	0	Unlimited
□	13	LAG5	Disabled	IP	0	Unlimited
□	14	LAG6	Disabled	IP	0	Unlimited
□	15	LAG7	Disabled	IP	0	Unlimited
□	16	LAG8	Disabled	IP	0	Unlimited

Field	Description
Port	Interface of port number.
State	Display IP Source Guard enable/disable status of interface.
Verify Source	Display mode of IP Source Guard verification.

Current Binding Entry	Display current binding entries of a interface.
Max Binding Entry	Display the number of maximum binding entry of interface.



Edit Port Setting

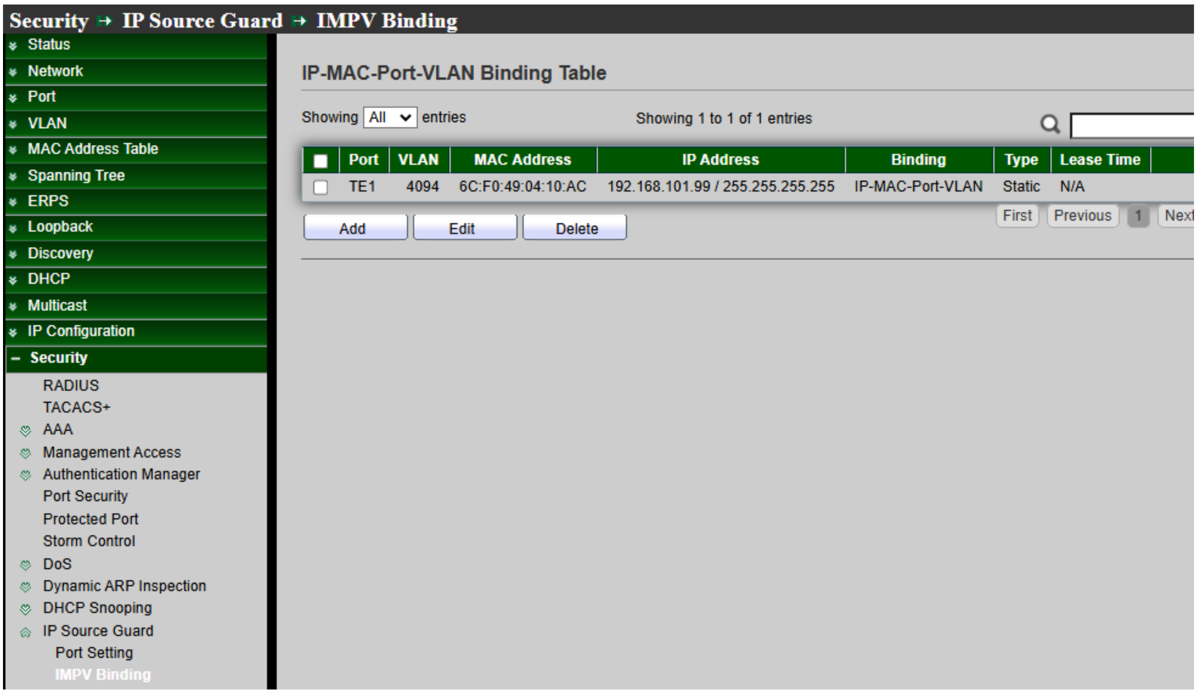
Port	TE2-TE3
State	☑ Enable
Verify Source	○ IP ● IP-MAC
Max Entry	2 (1 - 50, default 0), 0 is Unlimited

- **Port:** Display selected Port number.
- **State:** Check Enable or Un-Enable this IP Source Guard. Mainly restricts the client IP traffic to those source IP addresses configured Check Enable to enable IP Source Guard on the interface. Administrator can disable this feature, Default is disabled.
- **Verify Source:** Administrator can select IP only or MAC and IP type of source traffic to be verified.
  - **IP:** Only verify source IP address of packet.
  - **IP-MAC:** Verify source IP and source MAC address of packet
- **Max Entry:** Administrator need enter the maximum number of IP source binding rules. The range is 0 to 50, and 0 is Unlimited.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

15.12.2 IMPV Binding

Use the Binding to query and view information about inactive addresses recorded in the IP Source Guard database, This page allow user to add static IP source guard entry and browse all IP source guard entries that learned by DHCP snooping or statically create by user, Setting **"add"** and "Edit" and **"Delete"** for this function management.



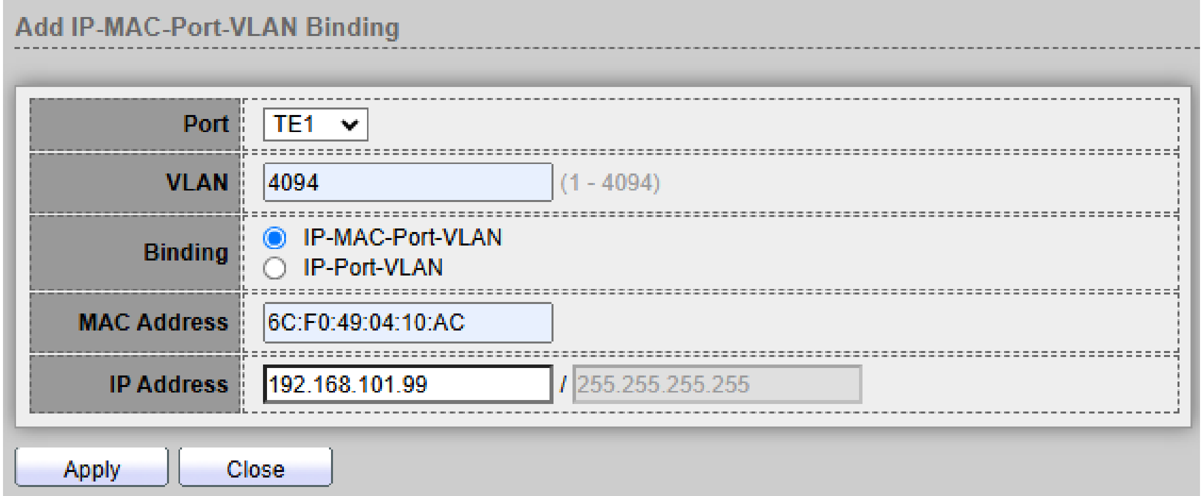
Security → IP Source Guard → IMPV Binding

IP-MAC-Port-VLAN Binding Table

Showing All entries   Showing 1 to 1 of 1 entries

□	Port	VLAN	MAC Address	IP Address	Binding	Type	Lease Time
□	TE1	4094	6C:F0:49:04:10:AC	192.168.101.99 / 255.255.255.255	IP-MAC-Port-VLAN	Static	N/A

Field	Description
Port	Display port ID of entry.
VLAN	Display VLAN ID of entry.
MAC Address	Display MAC address of entry. Only available of IP-MAC binding entry.
IP Address	Display IP address of entry. Mask always to be 255.255.255.255 for IP-MAC binding. IP binding entry display user input
Binding	Display binding type of entry.
Status	Type of existing binding entry: • **Static :** Entry added by user manually configured. • **Dynamic :** Entry learned by DHCP snooping.
Lease Time	Lease time of DHCP Snooping learned entry. After lease time entry will be deleted. Only available of dynamic entry.



Add IP-MAC-Port-VLAN Binding

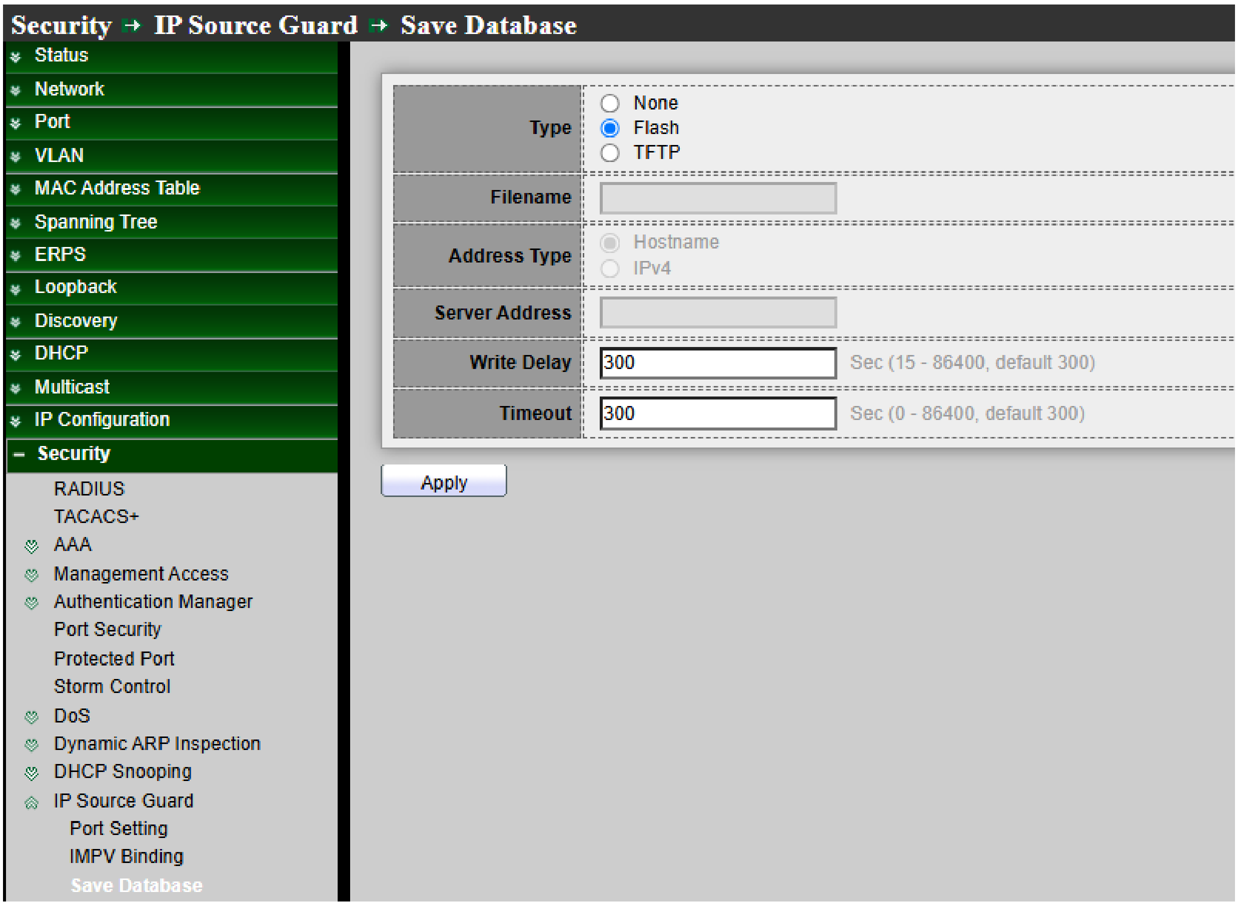
Port	TE1
VLAN	4094 (1 - 4094)
Binding	● IP-MAC-Port-VLAN ○ IP-Port-VLAN
MAC Address	6C:F0:49:04:10:AC
IP Address	192.168.101.99 / 255.255.255.255

- **Port:** Administrator can select port from list of a binding entry.
- **VLAN:** Specify a VLAN ID of a binding entry.
- **Binding:** Administrator can select matching mode of 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:** Input MAC address. Only available on IP-MAC-Port-VLAN mode.
- **IP Address:** Input IP address and mask. Mask only available on IP-MAC-Port mode.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

15.12.3 Save Databases

This page allow user to configure DHCP snooping database which can backup and restore dynamic DHCP snooping entries



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

- **Type:** Administrator can select the type of database agent.
  - **None:** Disable database agent service.
  - **Flash:** Save DHCP dynamic binding entries to flash.
  - **TFTP:** Save DHCP dynamic binding entries to remote TFTP server.
- **Filename:** Set file name of TFTP server, Input filename for backup file. Only available when selecting type “flash” and “TFTP”.
- **Address Type:** Select use Host name or IP address to connection TFTP server.
  - **Hostname:** TFTP server address is hostname.
  - **IPv4:** TFTP server address is IPv4 address.
- **Server Address:** Input remote TFTP server hostname or IP address. Only available when selecting type “TFTP.
- **Write Delay:** Input delay timer for doing backup after change happened. Default is 300 seconds.
- **Timeout:** Input aborts timeout for doing backup failure. Default is 300 seconds.

*Click the **“Apply”** button to save your changes settings.*

16. ACL

ACL (Access Control List) is an ordered list of classification filters and actions. Each single classification rule, together with its action, is called an Access Control Element (ACE). Each ACE is made up of filters that distinguish traffic groups and associated actions. A single ACL may contain one or more ACEs, which are matched against the contents of incoming frames. Either a DENY or PERMIT action is applied to frames whose contents match the filter.

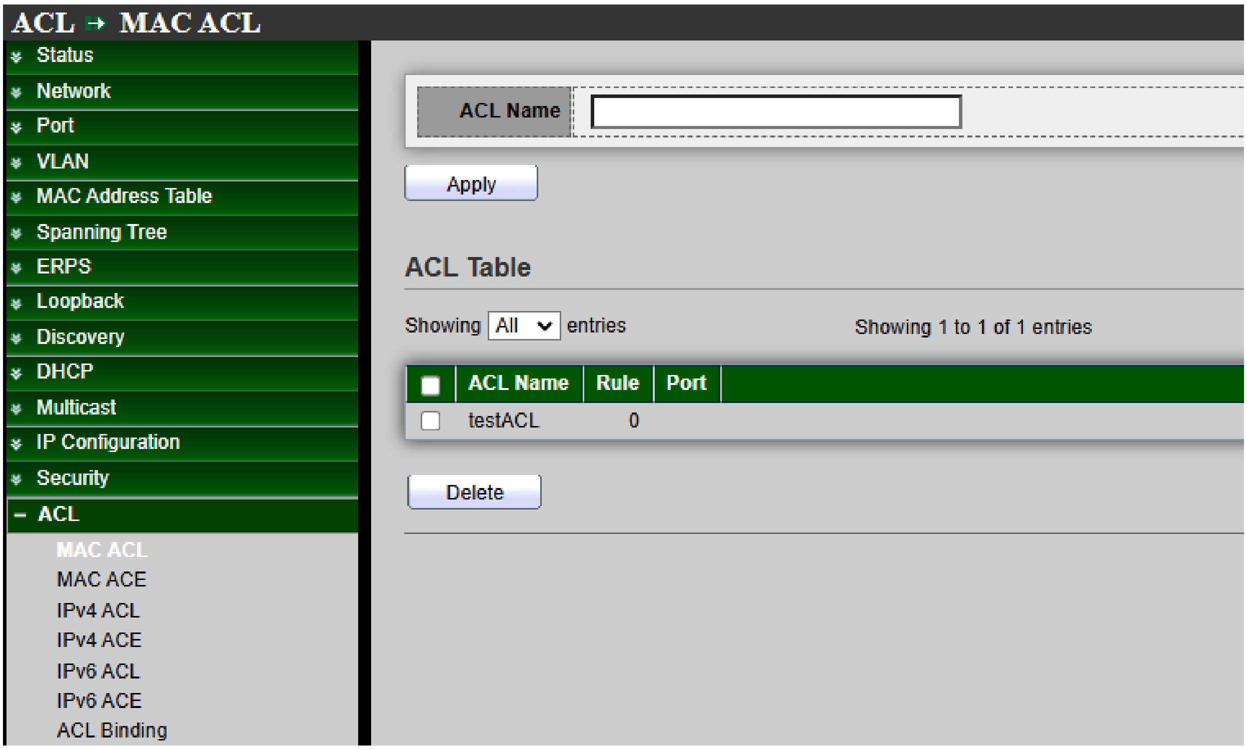
Note	When a packet matches an ACE filter, the ACE action is taken and that ACL processing is stopped. If the packet does not match the ACE filter, the next ACE is processed. If all ACEs of an ACL have been processed without finding a match, and if another ACL exists, it is processed in a similar manner. If no match is found to any ACE in all relevant ACLs then ACL default action will dropped the packet.

16.1 MAC ACL

This page mainly creates MAC ACLs profile. The MAC ACLs are used to filter traffic based on Layer 2 fields and defined on the MAC ACE page.

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

Note	A port can be either secured with ACLs or configured with advanced QoS policy, but not both.



ACL Name

ACL Table

Showing All entries   Showing 1 to 1 of 1 entries

□	ACL Name	Rule	Port
□	testACL	0	

- **ACL Name:** Create a name of ACL.

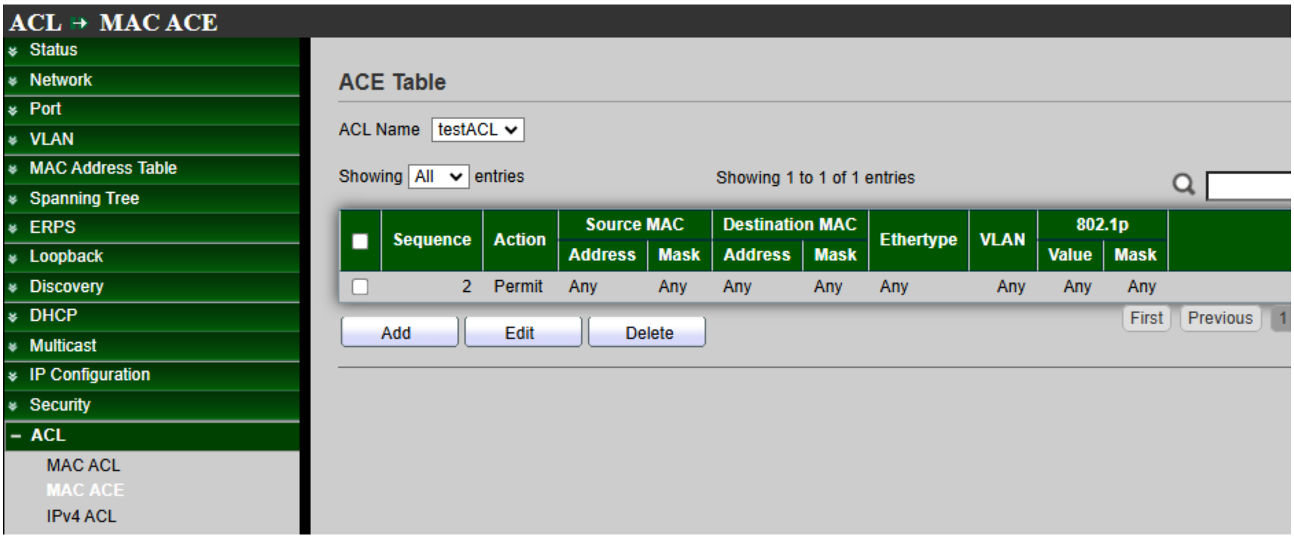
Click the ***"Apply"*** *button to save your changes settings.*

Field	Description
ACL Name	Display MAC ACL name.
Rule	Display the number ACE rule of ACL..
Port	Display the port list that bind this ACL.

Click the ***"Delete"*** *button to delete ACL table list.*

16.2 MAC ACE

MAC ACE will check all frames for a match. Setting **"add"** and "Edit" and **"Delete"** for this function management, This page allow user to add, edit or delete ACE rule. An ACE rule cannot be edited or deleted if ACL under binding. New ACE cannot be added if ACL under binding .



ACE Table

ACL Name: testACL

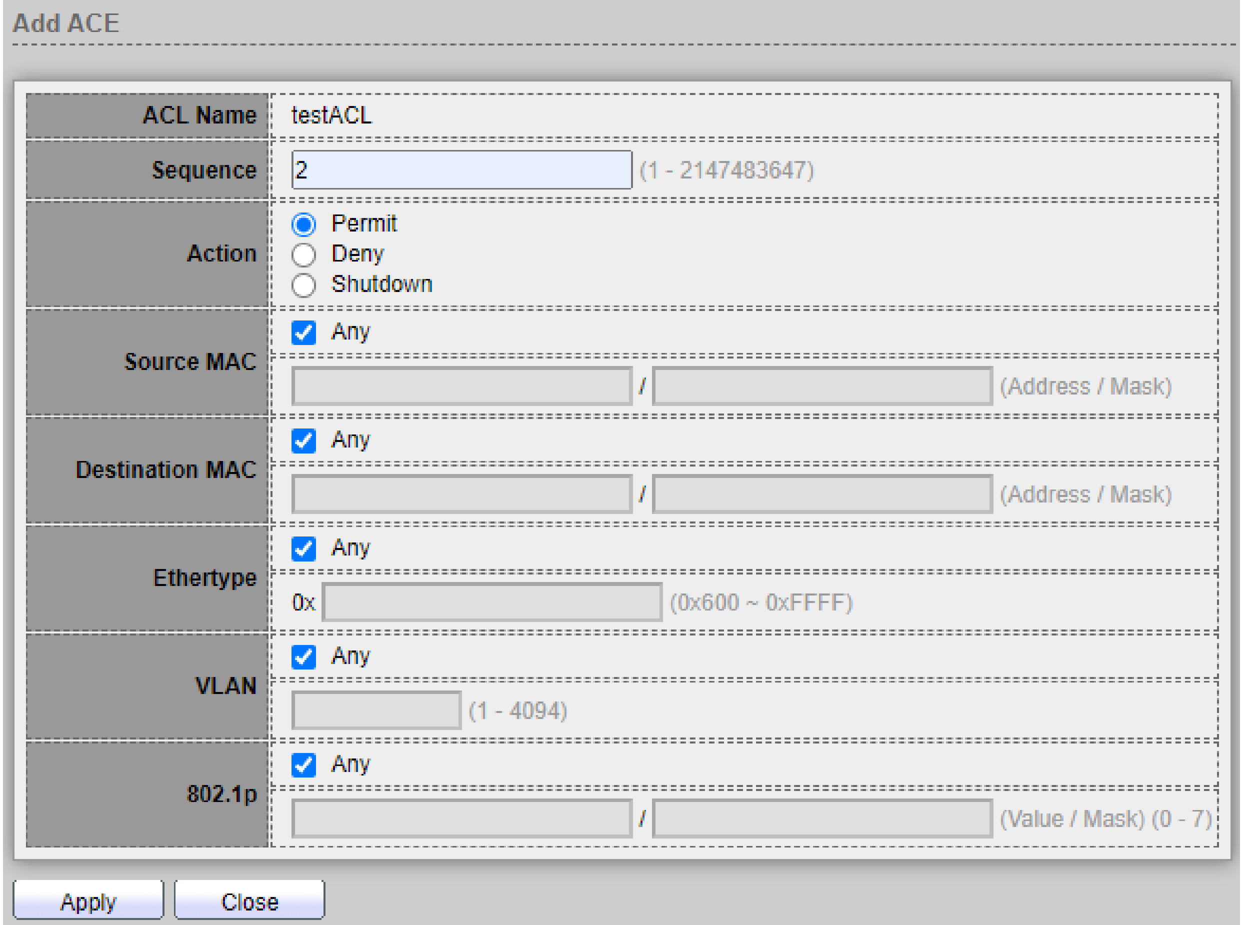
Showing All entries

Showing 1 to 1 of 1 entries

□	Sequence	Action	Source MAC		Destination MAC		Ethertype	VLAN	802.1p	
			Address	Mask	Address	Mask			Value	Mask
□	2	Permit	Any	Any	Any	Any	Any	Any	Any	Any

- **ACL Name:** Select the ACL name to which an ACE is being added.

Field	Description
Sequence	Display the sequence of ACE.
Action	Display the action of ACE
Source MAC	Display the source MAC address and mask of ACE.
Destination MAC	Display the destination MAC address and mask of ACE.
Ethertype	Display the Ethernet frame type of ACE.
VLAN ID	Display the VLAN ID of ACE
802.1p Value	Display the 802.1p value of ACE.
802.1p Mask	Display the 802.1p mask of ACE.



Add ACE

ACL Name	testACL
Sequence	2 (1 - 2147483647)
Action	● Permit ○ Deny ○ Shutdown
Source MAC	☑ Any / (Address / Mask)
Destination MAC	☑ Any / (Address / Mask)
Ethertype	☑ Any 0x (0x600 ~ 0xFFFF)
VLAN	☑ Any (1 - 4094)
802.1p	☑ Any / (Value / Mask) (0 - 7)

- **ACL Name:** Display the ACL name to which an ACE is being added.

- **Sequence:** ACEs with higher sequence are processed first (1 is the highest priority). Only available on Add Dialog.
- **Action:** Administrator can select the action after ACE match packet.
  - **Permit:** Forward packets that meet the ACE criteria.
  - **Deny:** Drop packets that meet the ACE criteria.
  - **Shutdown:** Drop packets that meet the ACE criteria, and disable the port from where the packets were received. Such ports can be reactivated from the Port Settings page.
- **Source MAC:** Select the type for source MAC address.
  - **Any:** All source addresses are acceptable.
  - **User Defined:** Only a source address or a range of source addresses which users define are acceptable. Enter the source MAC address and mask to which will be matched.
- **Destination MAC:** Destination MAC Select the type for Destination MAC address.
  - **Any:** All destination addresses are acceptable.
  - **User Defined:** Only a destination address or a range of destination addresses which users define are acceptable. Enter the destination MAC address and mask to which will be matched.

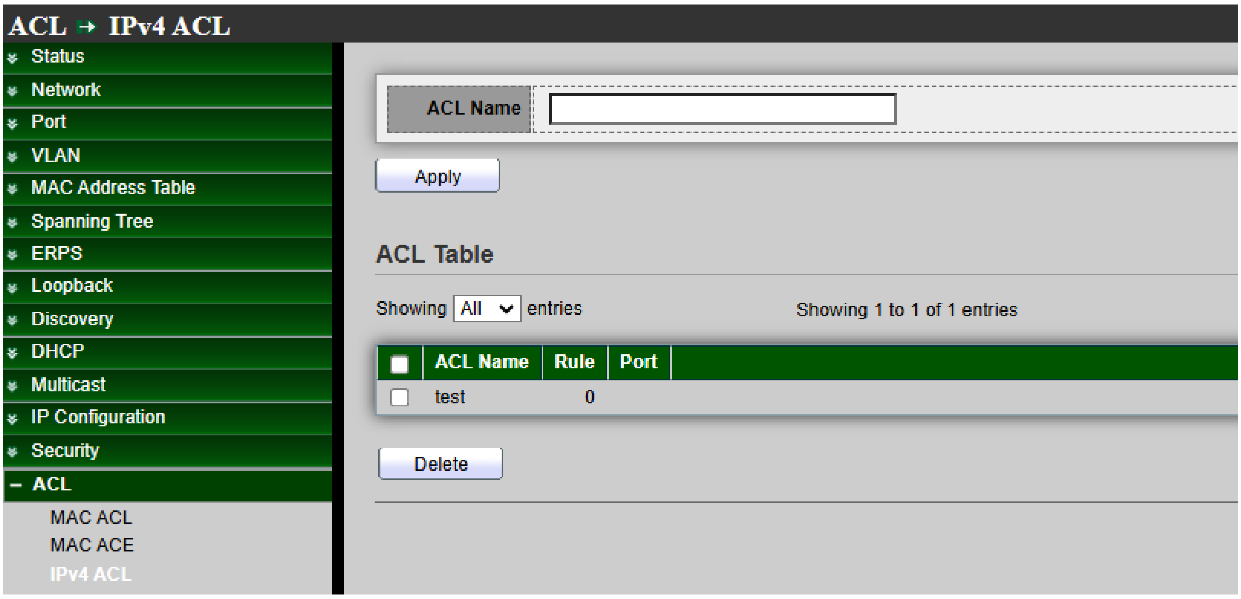
Note	Set F is show value, 0 is mask value, E.g. If an MAC is 8C:4D:EA:11:22:33 the mask value FF:FF:FF:00:00:00 indicates that only the first three bytes of the destination MAC address are used(8C:4D:EA).

- **Ethertype:** Select the type for Ethernet frame type.
  - **Any:** All Ethernet frame type is acceptable.
  - **User Defined:** Only an Ethernet frame type which users define is acceptable. Enter the Ethernet frame type value to which will be matched.
- **VLAN ID:** Select the type for VLAN ID.
  - **Any:** All VLAN ID is acceptable.
  - **User Defined:** User Defined: Only a VLAN ID which users define is acceptable. Enter the VLAN ID to which will be matched.
- **802.1p:** Select the type for 802.1p value.
  - **Any:** All 802.1p value is acceptable.
  - **User Defined:** User Defined: Only an 802.1p value or a range of 802.1p value which users define is acceptable. Enter the 802.1p value and mask to which will be matched.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

16.3 IPv4 ACL

Mainly creates IPv4 ACLs profile. The IPv4 ACLs are used to check IPv4 packets, This page allow user to add or delete Ipv4 ACL rule. A rule cannot be deleted if under binding.



ACL Name

ACL Table

Showing All entries Showing 1 to 1 of 1 entries

□	ACL Name	Rule	Port
□	test	0	

- **ACL Name:** Create a name of ACL.

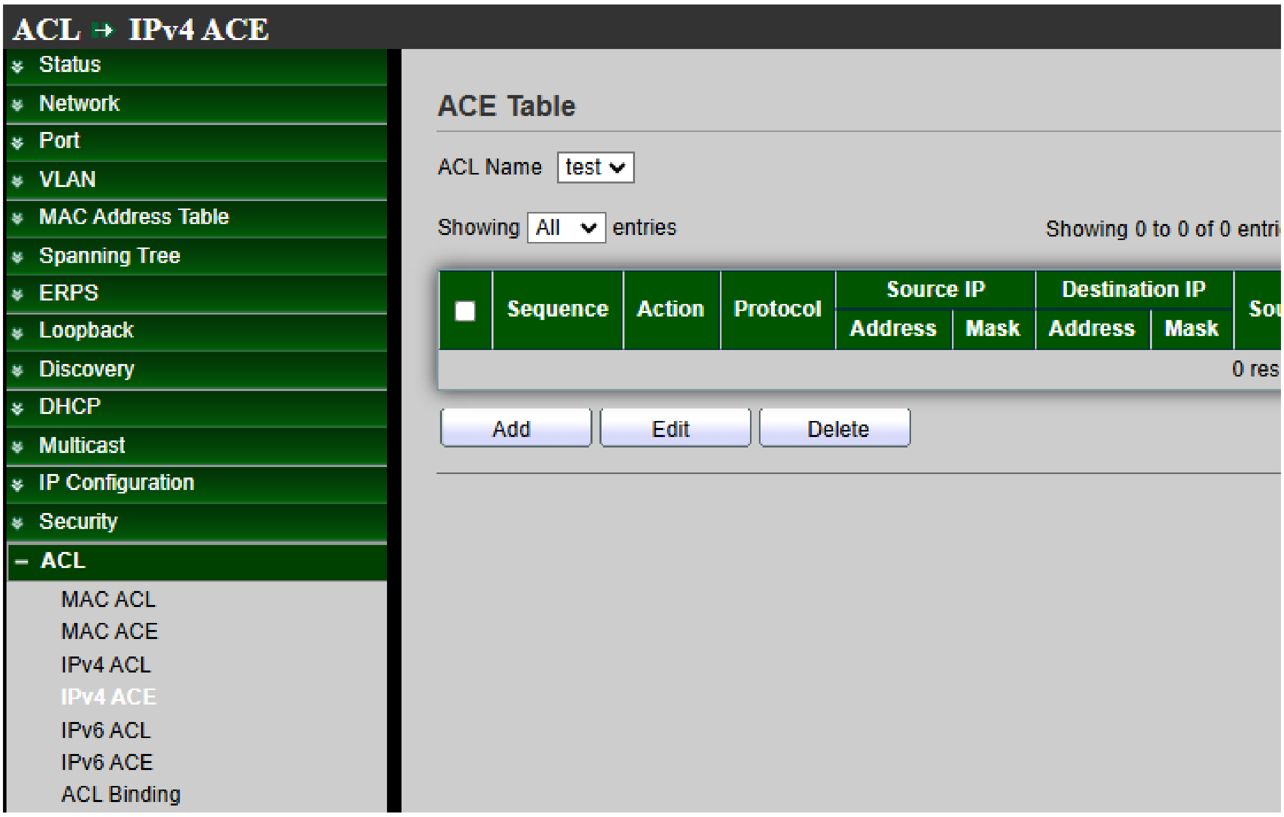
*Click the **"Apply"** button to save your changes settings.*

Field	Description
ACL Name	Display IPv4 ACL name
Rule	Display the number ACE rule of ACL
Port	Display the port list that bind this ACL

*Click the **"Delete"** button to delete the table list.*

16.4 IPv4 ACE

This page allow user to add, edit or delete ACE rule. An ACE rule cannot be edited or deleted if ACL under binding. New ACE cannot be added if ACL under binding, Setting **"add"** and "Edit" and **"Delete"** for this function management.



ACE Table

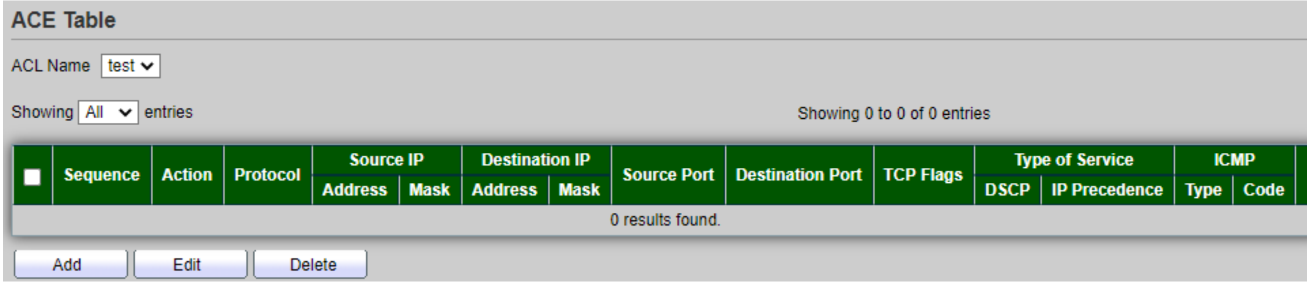
ACL Name: test

Showing All entries

Showing 0 to 0 of 0 entri

□	Sequence	Action	Protocol	Source IP		Destination IP		Sou
				Address	Mask	Address	Mask	
0 res								

- **ACL Name:** Select the ACL name to which an ACE is being added.



ACE Table

ACL Name: test

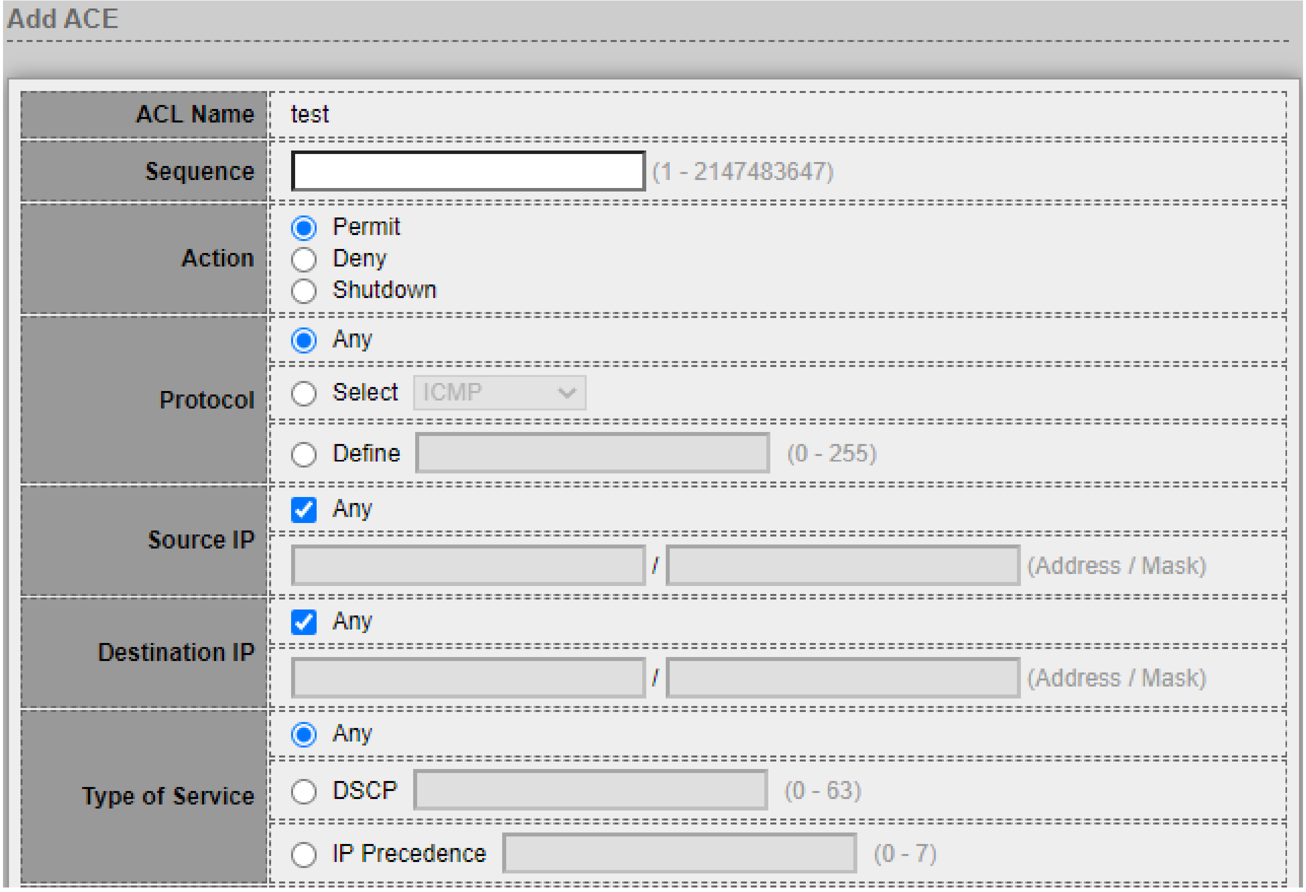
Showing All entries

Showing 0 to 0 of 0 entries

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

Field	Description
Sequence	Display the sequence of ACE.
Action	Display the action of ACE.
Protocol	Display the protocol value of ACE.

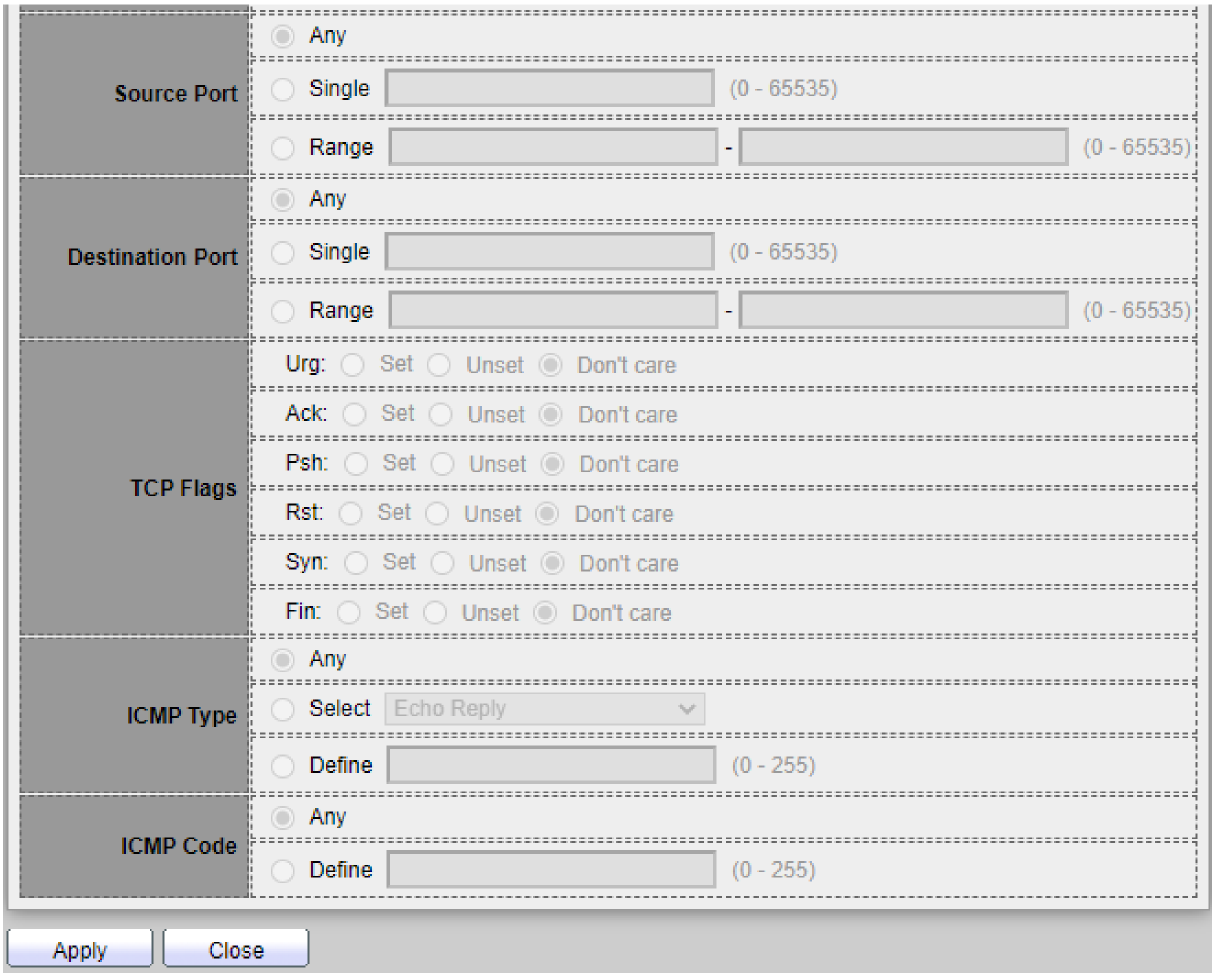
Source IP	Display the source IP address and mask of ACE: • **Address:** Display for the IPv4 IP address. • **Mask :** Display for the Mask address.
Destination IP	Display the destination IP address and mask of ACE: • **Address:** Display for the IPv4 IP address. • **Mask :** Display for the Mask address.
Source Port	Display single source port or a range of source ports of ACE. Only available when protocol is TCP or UDP.
Destination Port	Display single destination port or a range of destination ports of ACE. Only available when protocol is TCP or UDP.
TCP Flags	Display the TCP flag value if ACE. Only available when protocol is TCP.
Type of Service	Display the ToS value of ACE which could be DSCP or IP Precedence.
ICMP	Display the ICMP type and code of ACE. Only available when protocol is ICMP.



Add ACE

ACL Name	test
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)

- **ACL Name:** Display the ACL name to which an ACE is being added.
- **Sequence:** Specify the sequence of the ACE ,ACEs with higher sequence are processed first (1 is the highest priority). Only available on Add Dialog.
- **Action:** Administrator can select the action for a match.
  - **Permit:** Forward packets that meet the ACE criteria.
  - **Deny:** Drop packets that meet the ACE criteria.
  - **Shutdown:** Drop packets that meet the ACE criteria, and disable the port from where the packets were received. Such ports can be reactivated from the Port Settings page.
- **Protocol:** Administrator can select the type of protocol for a match.
  - **Any (IP):** All IP protocols are acceptable.
  - **Select from list:** Select one of the following protocols from the drop-down 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 the protocol ID.
- **Source IP:** Select the type for source IP address.
  - **Any:** All source addresses are acceptable.
  - **User Defined:** Only a source address or a range of source addresses which users define are acceptable. Enter the source IP address value and mask to which will be matched.
- **Destination IP:** Select the type for destination IP address..
  - **Any:** All destination addresses are acceptable.
  - **User Defined:** Only a destination address or a range of destination addresses which users define are acceptable. Enter the destination IP address value and mask to which will be matched.
- **Type of Service:** Select the type of service for a match.
  - **Any:** All types of service are acceptable.
  - **DSCP to match:** Enter a Differentiated Serves Code Point (DSCP) to match.
  - **IP Precedence to match:** Enter a IP Precedence to match.



Source Port	● Any ○ Single ____ (0 - 65535) ○ Range ____ - ____ (0 - 65535)
Destination Port	● Any ○ Single ____ (0 - 65535) ○ Range ____ - ____ (0 - 65535)
TCP Flags	Urg: ○ Set ○ Unset ● Don't care Ack: ○ Set ○ Unset ● Don't care Psh: ○ Set ○ Unset ● Don't care Rst: ○ Set ○ Unset ● Don't care Syn: ○ Set ○ Unset ● Don't care Fin: ○ Set ○ Unset ● Don't care
ICMP Type	● Any ○ Select Echo Reply ○ Define ____ (0 - 255)
ICMP Code	● Any ○ Define ____ (0 - 255)

- **Source Port:** Select the type of protocol for a match. Only available when protocol is TCP or UDP.
  - **Any:** All source ports are acceptable.
  - **Single:** Enter a single TCP/UDP source port to which packets are matched.
  - **Range:** Select a range of TCP/UDP source ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.
- **Destination Port:** Select the type of protocol for a match. Only available when protocol is TCP or UDP.
  - **Any:** All source ports are acceptable.
  - **Single:** Enter a single TCP/UDP source port to which packets are matched.
  - **Range:** Select a range of TCP/UDP destination ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.
- **TCP Flags:** Select one or more TCP flags with which to filter packets. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security. Only available when protocol is TCP.

- **Set:** Match if the flag is SET.
- **Unset:** Match if the flag is Not SET.
- **Don't care:** Ignore the TCP flag.

➢ **ICMP Type:** Either select the message type by name or enter the message type number. Only available when protocol is ICMP.

- **Any:** All message types are acceptable.
- **Select from list:** Select message type by name.
- **Protocol ID to match:** Enter the number of message type.

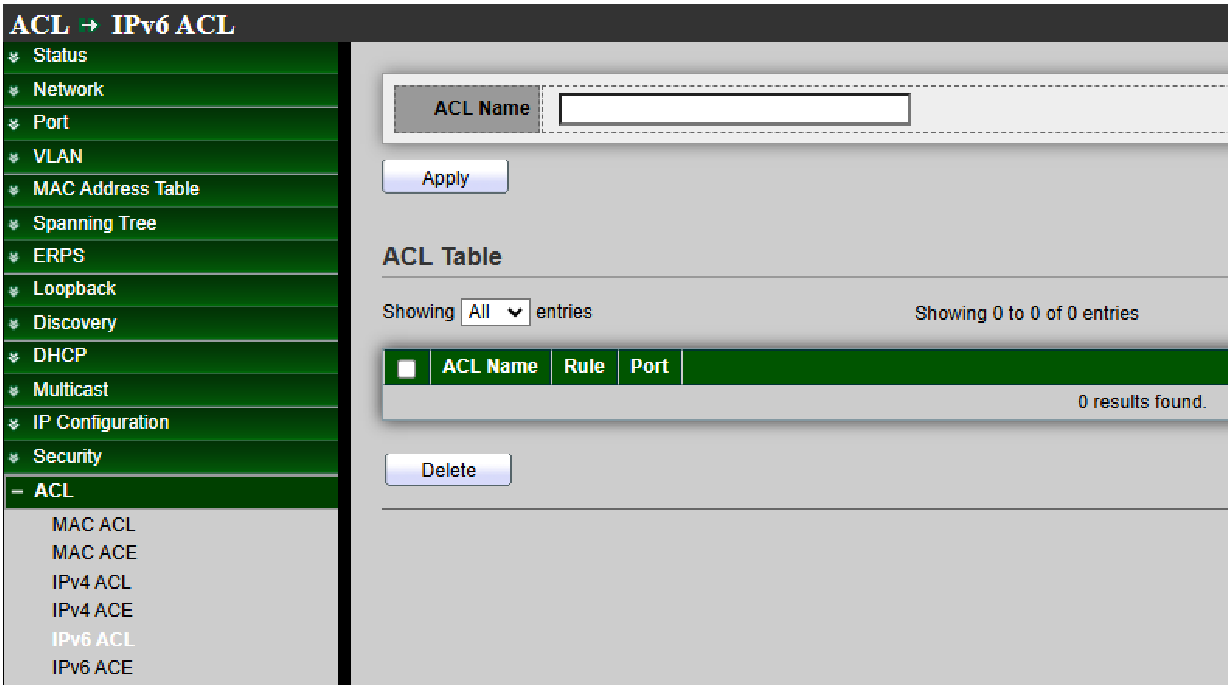
➢ **ICMP Code:** Select the type for ICMP code. Only available when protocol is ICMP.

- **Any:** All codes are acceptable.
- **User Defined:** Enter an ICMP code to match.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

16.5 IPv6 ACL

Mainly creates IPv6 ACLs profile. The IPv6 ACLs are used to check IPv6 packets, This page allow user to add or delete Ipv6 ACL rule. A rule cannot be deleted if under binding.



ACL Name

ACL Table

Showing All entries   Showing 0 to 0 of 0 entries

☐	ACL Name	Rule	Port

0 results found.

➢ **ACL Name:** Create a name of ACL.

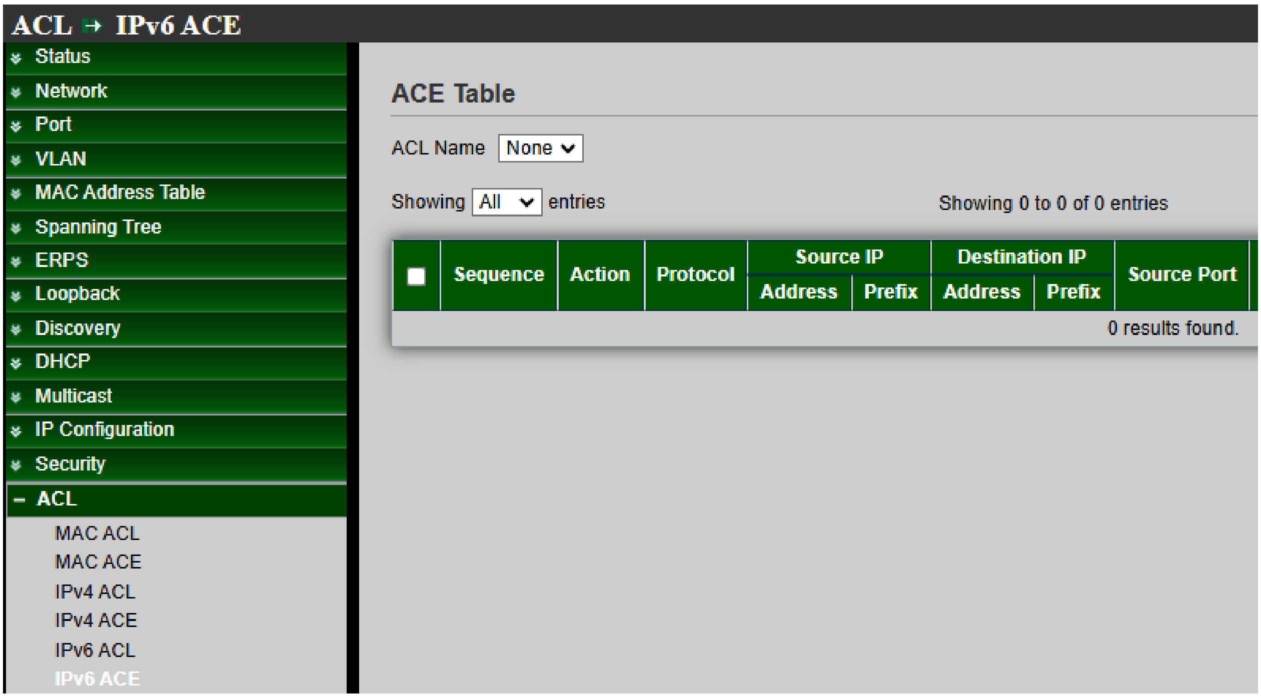
*Click the **"Apply"** button to save your changes settings.*

Field	Description
ACL Name	Display IPv6 ACL name
Rule	Display the number ACE rule of ACL
Port	Display the port list that bind this ACL

*Click the **"Delete"** button to delete the table list.*

16.6 IPv6 ACE

This page allow user to add, edit or delete ACE rule. An ACE rule cannot be edited or deleted if ACL under binding. New ACE cannot be added if ACL under binding, Setting **"add"** and "Edit" and **"Delete"** for this function management.



ACL → IPv6 ACE

ACE Table

ACL Name: None

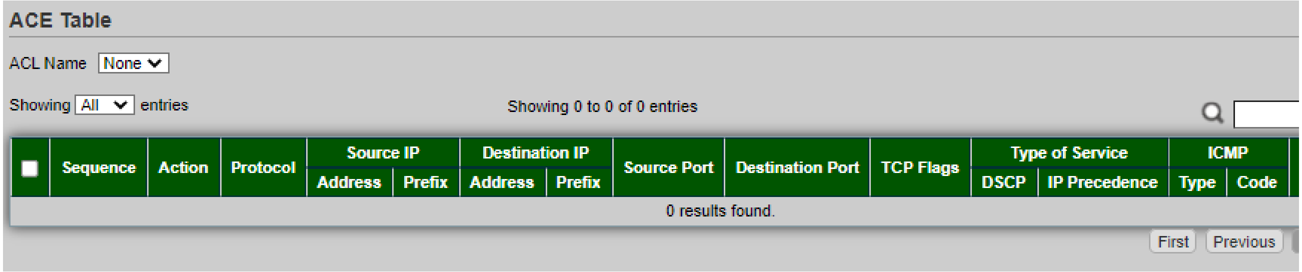
Showing All entries

Showing 0 to 0 of 0 entries

☐	Sequence	Action	Protocol	Source IP		Destination IP		Source Port
				Address	Prefix	Address	Prefix	

0 results found.

- ➢ **ACL Name:** Select the ACL name to which an ACE is being added.



ACE Table

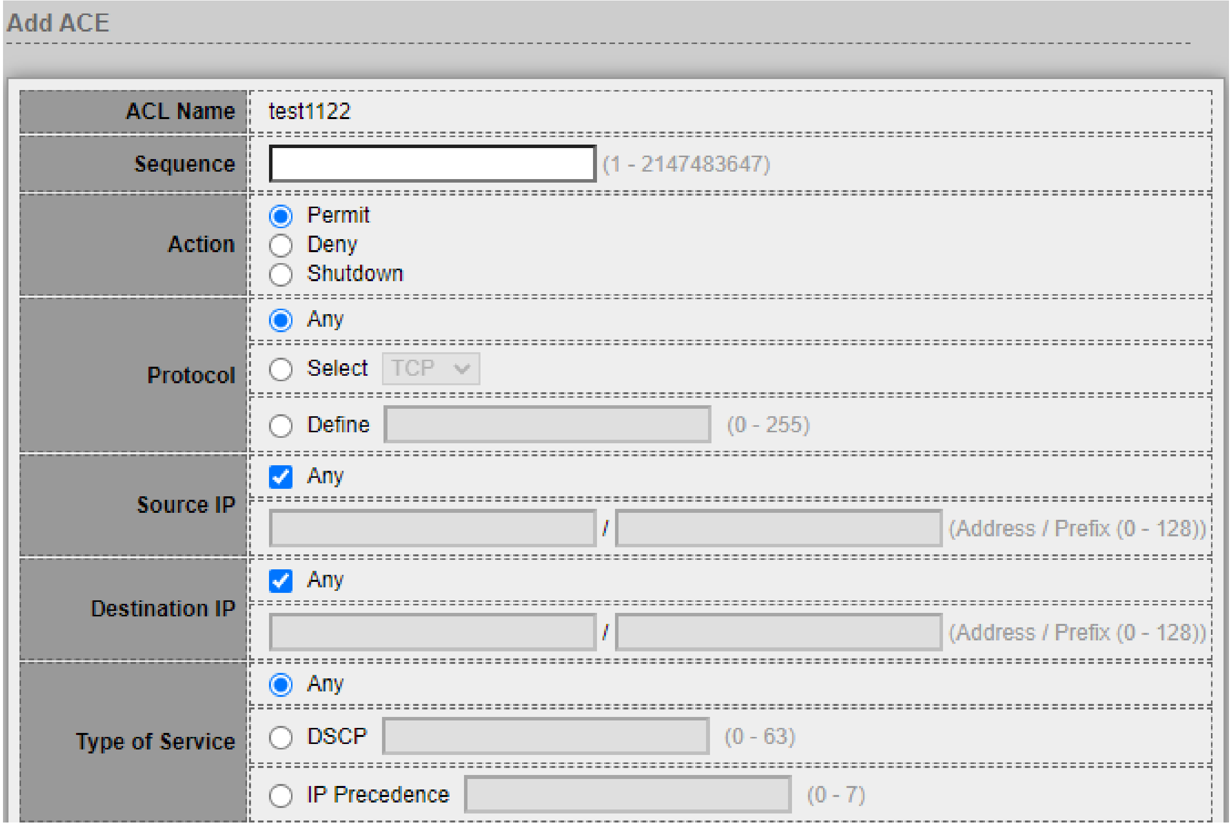
ACL Name None

Showing All entries

Showing 0 to 0 of 0 entries

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

Field	Description
Sequence	Display the sequence of ACE.
Action	Display the action of ACE.
Protocol	Display the protocol value of ACE.
Source IP	Display the source IP address and mask of ACE: • **Address:** Display for the IPv6 IP address. • **Mask :** Display for the Mask address.
Destination IP	Display the destination IP address and mask of ACE: • **Address:** Display for the IPv6 IP address. • **Mask :** Display for the Mask address.
Source Port	Display single source port or a range of source ports of ACE. Only available when protocol is TCP or UDP.
Destination Port	Display single destination port or a range of destination ports of ACE. Only available when protocol is TCP or UDP.
TCP Flags	Display the TCP flag value if ACE. Only available when protocol is TCP.
Type of Service	Display the ToS value of ACE which could be DSCP or IP Precedence.
ICMP	Display the ICMP type and code of ACE. Only available when protocol is ICMP.

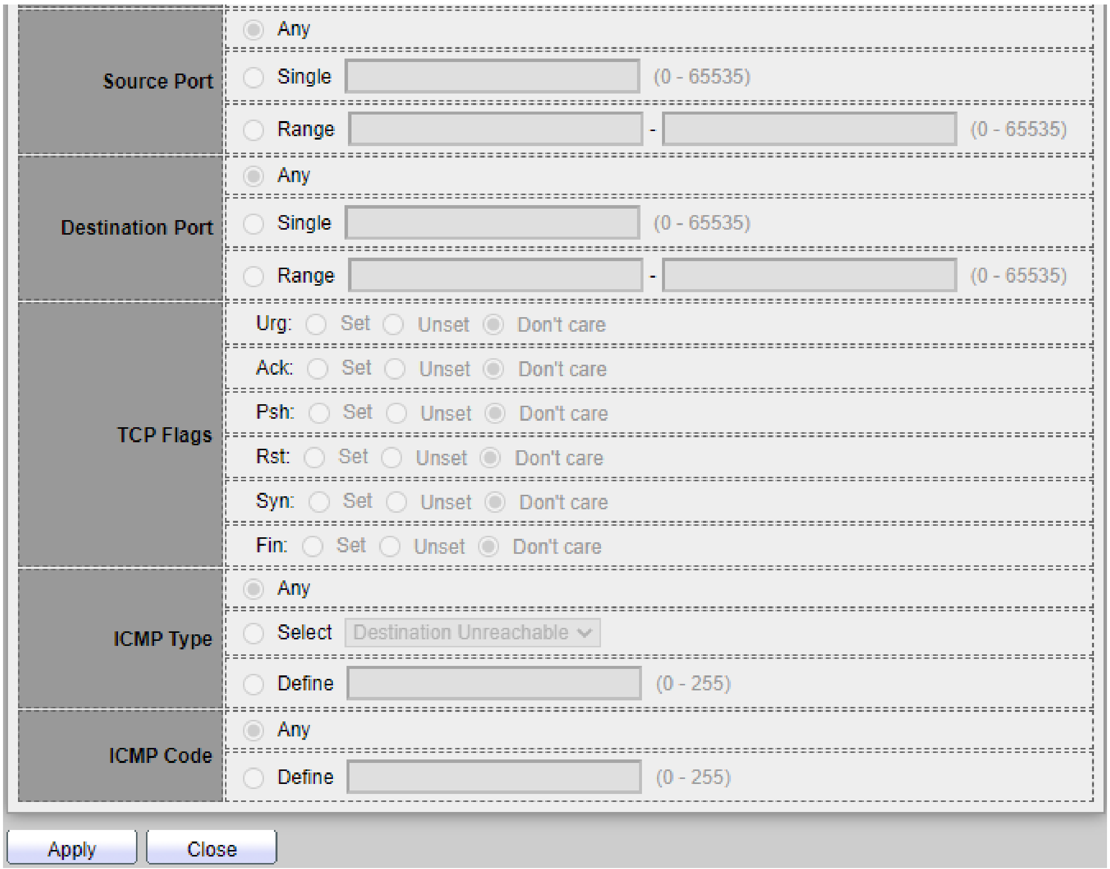


Add ACE

ACL Name	test1122
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)

- **ACL Name:** Display the ACL name to which an ACE is being added.
- **Sequence:** Specify the sequence of the ACE ,ACEs with higher sequence are processed first (1 is the highest priority). Only available on Add Dialog.
- **Action:** Administrator can select the action for a match.
  - **Permit:** Forward packets that meet the ACE criteria.
  - **Deny:** Drop packets that meet the ACE criteria.
  - **Shutdown:** Drop packets that meet the ACE criteria, and disable the port from where the packets were received. Such ports can be reactivated from the Port Settings page.
- **Protocol:** Administrator can select the type of protocol for a match.
  - **Any (IP):** All IP protocols are acceptable.
  - **Select from list:** Select one of the following protocols from the drop-down 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 the protocol ID.
- **Source IP:** Select the type for source IP address.
  - **Any:** All source addresses are acceptable.
  - **User Defined:** Only a source address or a range of source addresses which users define are acceptable. Enter the source IP address value and mask to which will be matched.

- **Destination IP:** Select the type for destination IP address..
  - **Any:** All destination addresses are acceptable.
  - **User Defined:** Only a destination address or a range of destination addresses which users define are acceptable. Enter the destination IP address value and prefix to which will be matched.
- **Type of Service:** Select the type of service for a match.
  - **Any:** All types of service are acceptable.
  - **DSCP to match:** Enter a Differentiated Serves Code Point (DSCP) to match.
  - **IP Precedence to match:** Enter a IP Precedence to match.



Source Port	● 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)

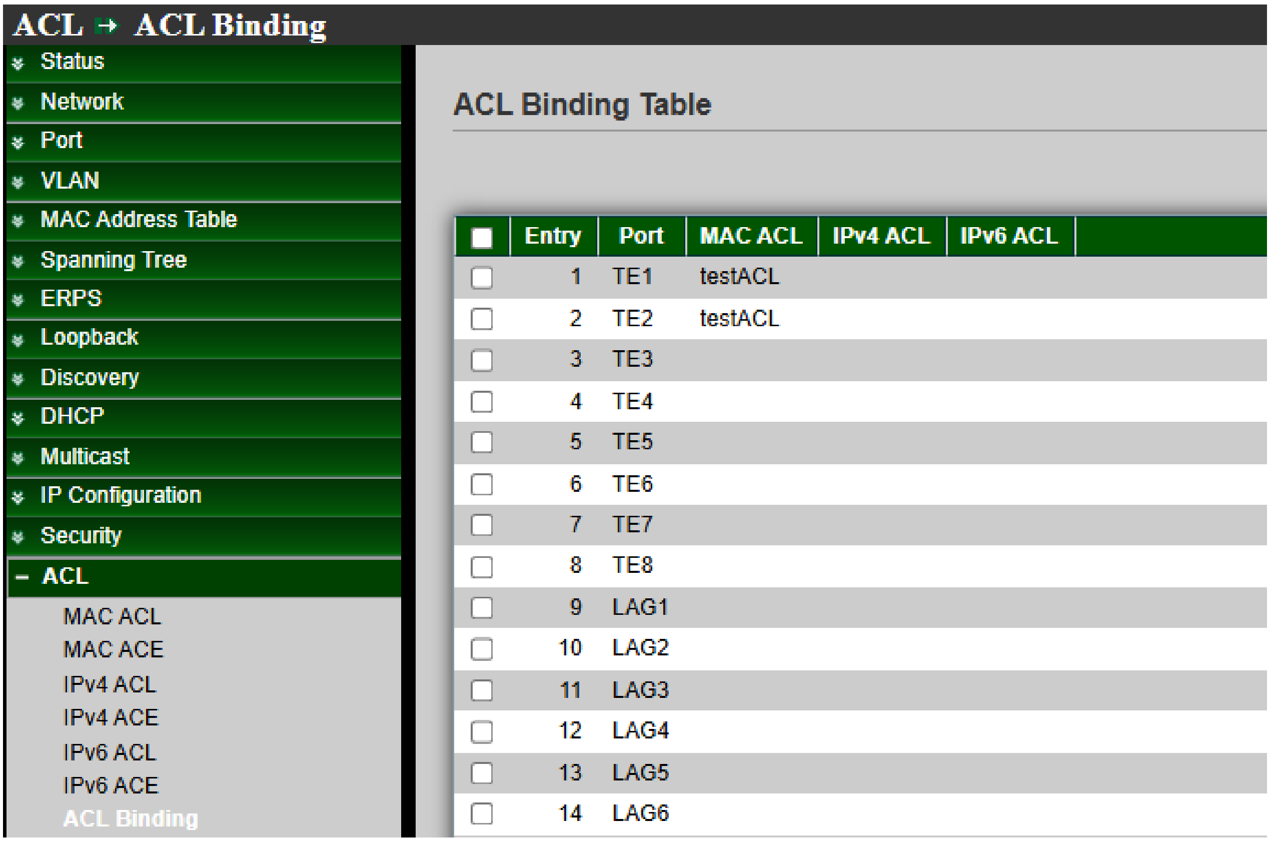
- **Source Port:** Select the type of protocol for a match. Only available when protocol is TCP or UDP.
  - **Any:** All source ports are acceptable.
  - **Single:** Enter a single TCP/UDP source port to which packets are matched.
  - **Range:** Select a range of TCP/UDP source ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.
- **Destination Port:** Select the type of protocol for a match. Only available when protocol is TCP or UDP.

  - **Any:** All destination ports are acceptable.
  - **Single:** Enter a single TCP/UDP destination port to which packets are matched.
  - **Range:** Select a range of TCP/UDP destination ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.
- **TCP Flags:** Select one or more TCP flags with which to filter packets. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security. Only available when protocol is TCP.
  - **Set:** Match if the flag is SET.
  - **Unset:** Match if the flag is Not SET.
  - **Don't care:** Ignore the TCP flag.
- **ICMP Type:** Either select the message type by name or enter the message type number. Only available when protocol is ICMP.
  - **Any:** All message types are acceptable.
  - **Select from list:** Select message type by name.
  - **Protocol ID to match:** Enter the number of message type.
- **ICMP Code:** Select the type for ICMP code. Only available when protocol is ICMP.
  - **Any:** All codes are acceptable.
  - **User Defined:** Enter an ICMP code to match.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

16.7 ACL Binding

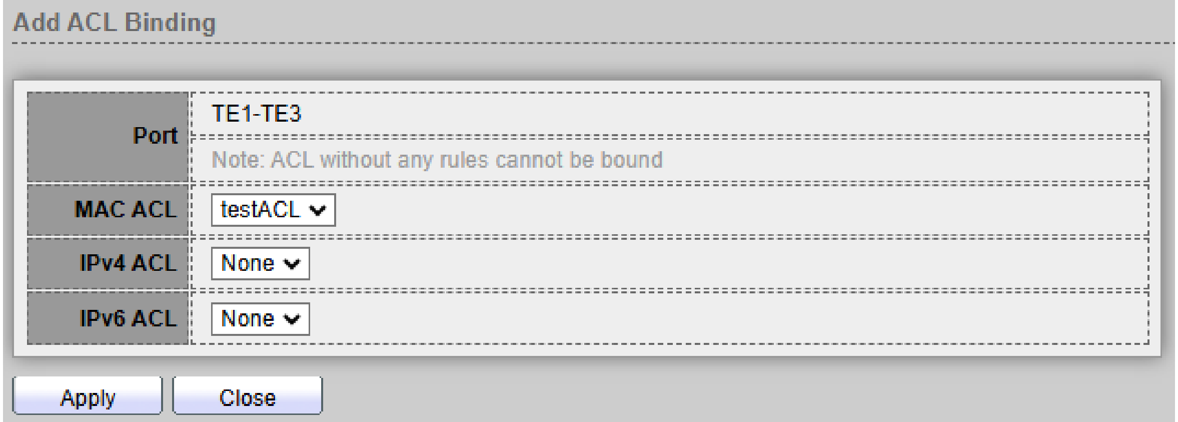
This page allow user to bind or unbind ACL rule to or from interface. IPv4 and Ipv6 ACL cannot be bound to the same port simultaneously , Administrator can from ACL Binding Table to select ports. When an ACL is bound to an interface, its ACE rules are applied to packets arriving at that interface. Packets that do not match any of the ACEs in the ACL are matched to a default rule, whose action is to drop unmatched packets.



ACL Binding Table

□	Entry	Port	MAC ACL	IPv4 ACL	IPv6 ACL
□	1	TE1	testACL		
□	2	TE2	testACL		
□	3	TE3			
□	4	TE4			
□	5	TE5			
□	6	TE6			
□	7	TE7			
□	8	TE8			
□	9	LAG1			
□	10	LAG2			
□	11	LAG3			
□	12	LAG4			
□	13	LAG5			
□	14	LAG6			

Field	Description
Port	Display port entry ID.
MAC ACL	Display mac ACL name that bound of interface. Empty means no rule bound.
IPv4 ACL	Display ipv4 ACL name that bound of interface. Empty means no rule bound.
IPv6 ACL	Display ipv6 ACL name that bound of interface. Empty means no rule bound.



Add ACL Binding

Port	TE1-TE3 Note: ACL without any rules cannot be bound
MAC ACL	testACL
IPv4 ACL	None
IPv6 ACL	None

- **Port:** Displays selected Port number.
- **MAC ACL:** MAC ACLs that are bound to the interface, Select mac ACL name from list to bind.
- **IPv4 ACL:** IPv4 ACLs that are bound to the interface, Select IPv4 ACL name from list to bind.
- **IPv6 ACL:** IPv6 ACLs that are bound to the interface, Select IPv6 ACL name from list to bind.

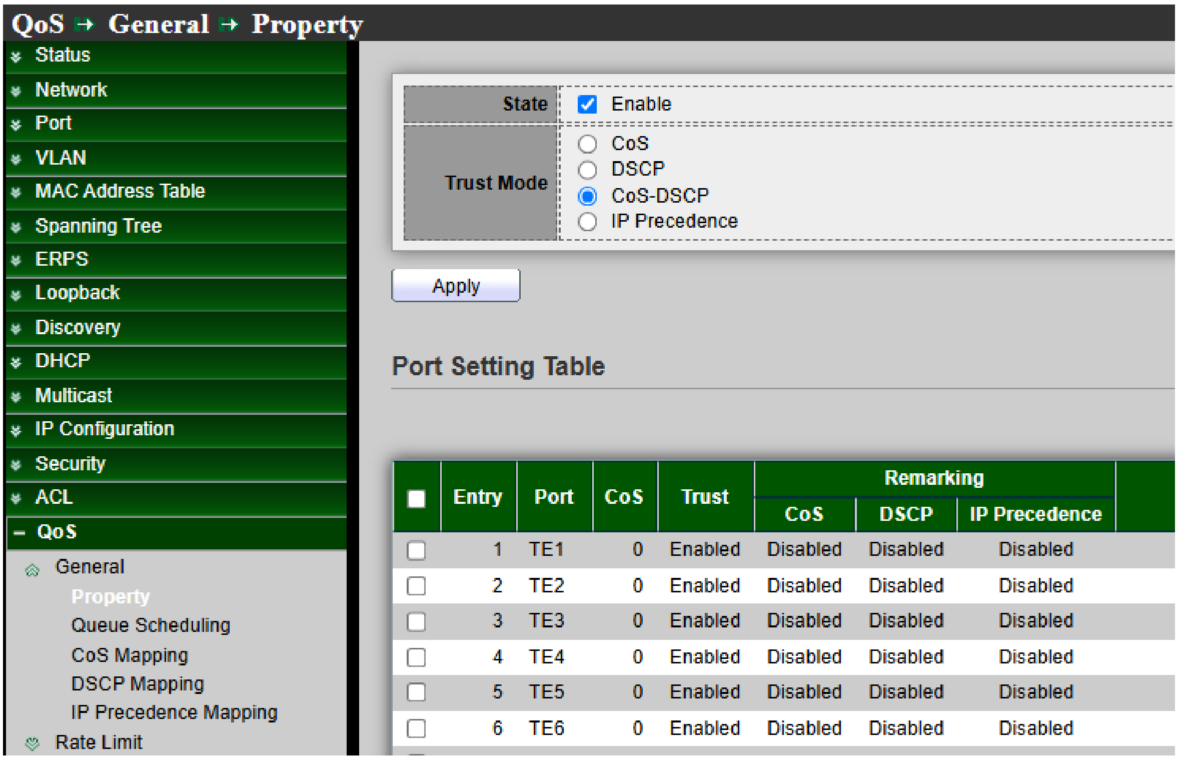
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

17. QoS

The quality of service (QoS) feature is applied throughout the network to ensure that network traffic is prioritized according to required criteria and the desired traffic receives preferential treatment.

17.1 Property

The QoS feature is used to optimize network performance, Use the QoS general pages to configure settings for general purpose



QoS → General → Property

State: ☑ Enable

Trust Mode: ○ CoS ○ DSCP ● CoS-DSCP ○ IP Precedence

Port Setting Table

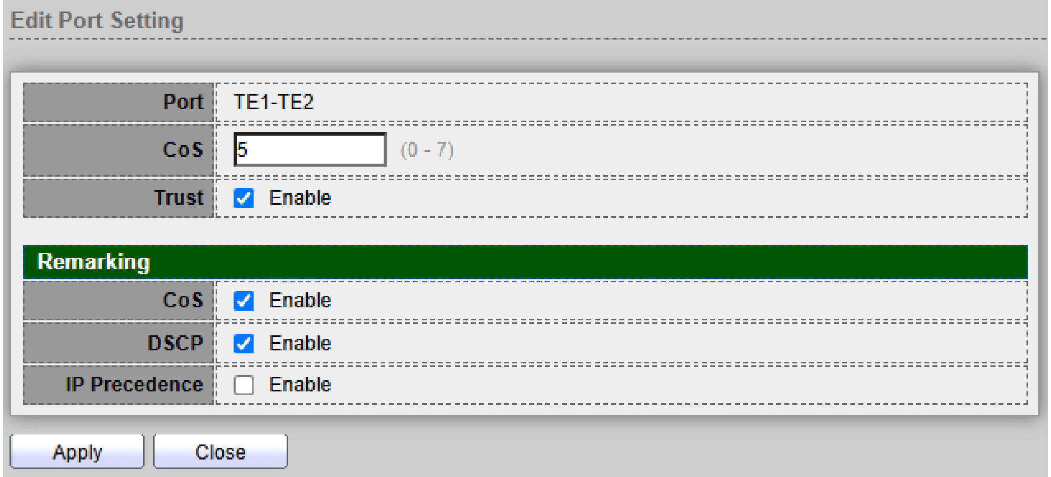
□	Entry	Port	CoS	Trust	Remarking		
					CoS	DSCP	IP Precedence
□	1	TE1	0	Enabled	Disabled	Disabled	Disabled
□	2	TE2	0	Enabled	Disabled	Disabled	Disabled
□	3	TE3	0	Enabled	Disabled	Disabled	Disabled
□	4	TE4	0	Enabled	Disabled	Disabled	Disabled
□	5	TE5	0	Enabled	Disabled	Disabled	Disabled
□	6	TE6	0	Enabled	Disabled	Disabled	Disabled

- **State:** Administrator can enable or disable this QoS Feature.
- **Trust Mode:** Administrator can select CoS / DSCP / CoS-DSCP and IP Precedence mode.
  - **CoS:** Traffic is mapped to queues based on the CoS field in the VLAN tag, or based on the per-port default CoS value (if there is no VLAN tag on the incoming packet), the actual mapping of the CoS to queue can be configured on port setting dialog.
  - **DSCP:** All IP traffic is mapped to queues based on the DSCP field in the IP header. The actual mapping of the DSCP to queue can be configured on the DSCP mapping page. If traffic is not IP traffic, it is mapped to the best effort queue..
  - **CoS-DSCP:** Select to use Trust CoS mode for non-IP traffic and Trust DSCP mode for IP traffic.
  - **IP Precedence:** Traffic is mapped to queues based on the IP precedence. The actual mapping of the IP precedence to queue can be configured on the IP Precedence mapping page.

*Click the **"Apply"** button to save your changes settings.*

Field	Description
Port	Interface of port name.
CoS	Port default CoS priority value for the selected ports.

Trust	Port trust state: • **Enabled:** Traffic will follow trust mode in global setting. • **Disabled:** Traffic will always use best efforts.
Remarking (CoS)	Remarking (CoS) Port CoS remaking admin state: • **Enabled:** CoS remarking is enabled. • **Disabled:** CoS remarking is disabled.
Remarking (DSCP)	Port DSCP remaking admin state: • **Enabled:** DSCP remarking is enabled. • **Disabled:** DSCP remarking is disabled.



Edit Port Setting

Port	TE1-TE2
CoS	5 (0 - 7)
Trust	☑ Enable

Remarking

CoS	☑ Enable
DSCP	☑ Enable
IP Precedence	□ Enable

- **Port:** Displays selected port number.
- **CoS:** Set default CoS/802.1p priority value for the selected ports,Set the default CoS value to be assigned for incoming packets (that do not have a VLAN tag). The range is 0 to 7.
- **Trust:** Set checkbox to enable/disable port trust state.
- **Remarking:**
  - **CoS:** Set checkbox to enable/disable port CoS remarking, Traffic is mapped to queues based on the VPT field in the VLAN tag, or based on the per-port default CoS value (if there is no VLAN tag on the incoming packet), the actual mapping of the VPT to queue can be configured on the CoS to Queue page.
  - **DSCP:** Set checkbox to enable/disable port DSCP remarking,All IP traffic is mapped to queues based on the DSCP field in the IP header. The actual mapping of the DSCP to queue can be configured on the DSCP to Queue page. If traffic is not IP traffic, it is mapped to the best effort queue.
  - **IP Precedence:** Set checkbox to enable/disable port IP Precedence remarking, Traffic is mapped to queues based on the IP precedence. The actual mapping of the IP precedence to queue can be configured on the IP Precedence to Queue page.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

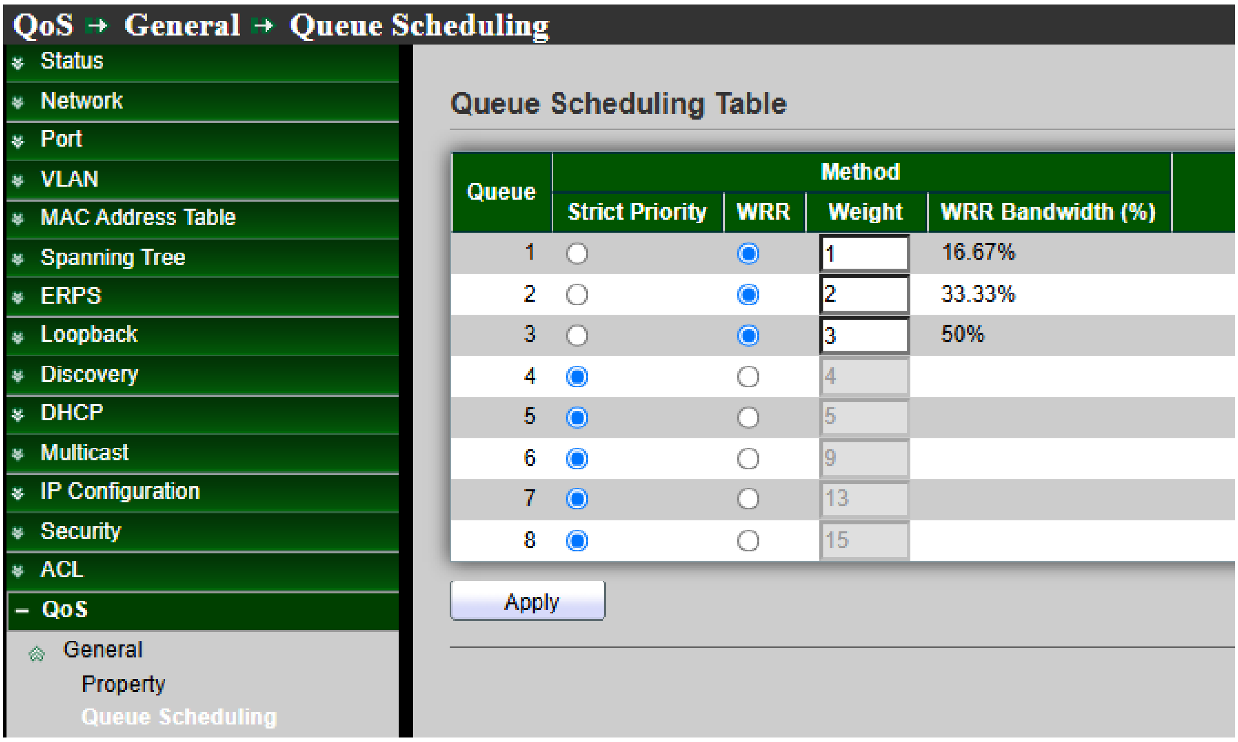
17.2 Queue Scheduling

The switch supports eight queues for each interface. Queue number 8 is the highest priority queue. Queue number 1 is the lowest priority queue. There are two ways of determining how traffic in queues is handled, Strict Priority (SP) and Weighted Round Robin (WRR).

- Strict Priority (SP)—Egress traffic from the highest priority queue is transmitted first. Traffic from the lower queues is processed only after the highest queue has been transmitted, which provide the highest level of priority of traffic to the highest numbered queue.
- Weighted Round Robin (WRR)—In WRR mode the number of packets sent from the queue is proportional to the weight of the queue (the higher the weight, the more frames are sent).

The queuing modes can be selected on the Queue page.When the queuing mode is by Strict Priority, the priority sets the order in which queues are serviced, starting with queue_8 (the highest priority queue) and going to the next lower queue when each queue is completed.

When the queuing mode is Weighted Round Robin, queues are serviced until their quota has been used up and then another queue is serviced. It is also possible to assign some of the lower queues to WRR, while keeping some of the higher queues in Strict Priority. In this case traffic for the SP queues is always sent before traffic from the WRR queues. After the SP queues have been emptied, traffic from the WRR queues is forwarded. (The relative portion from each WRR queue depends on its weight).



Queue Scheduling Table

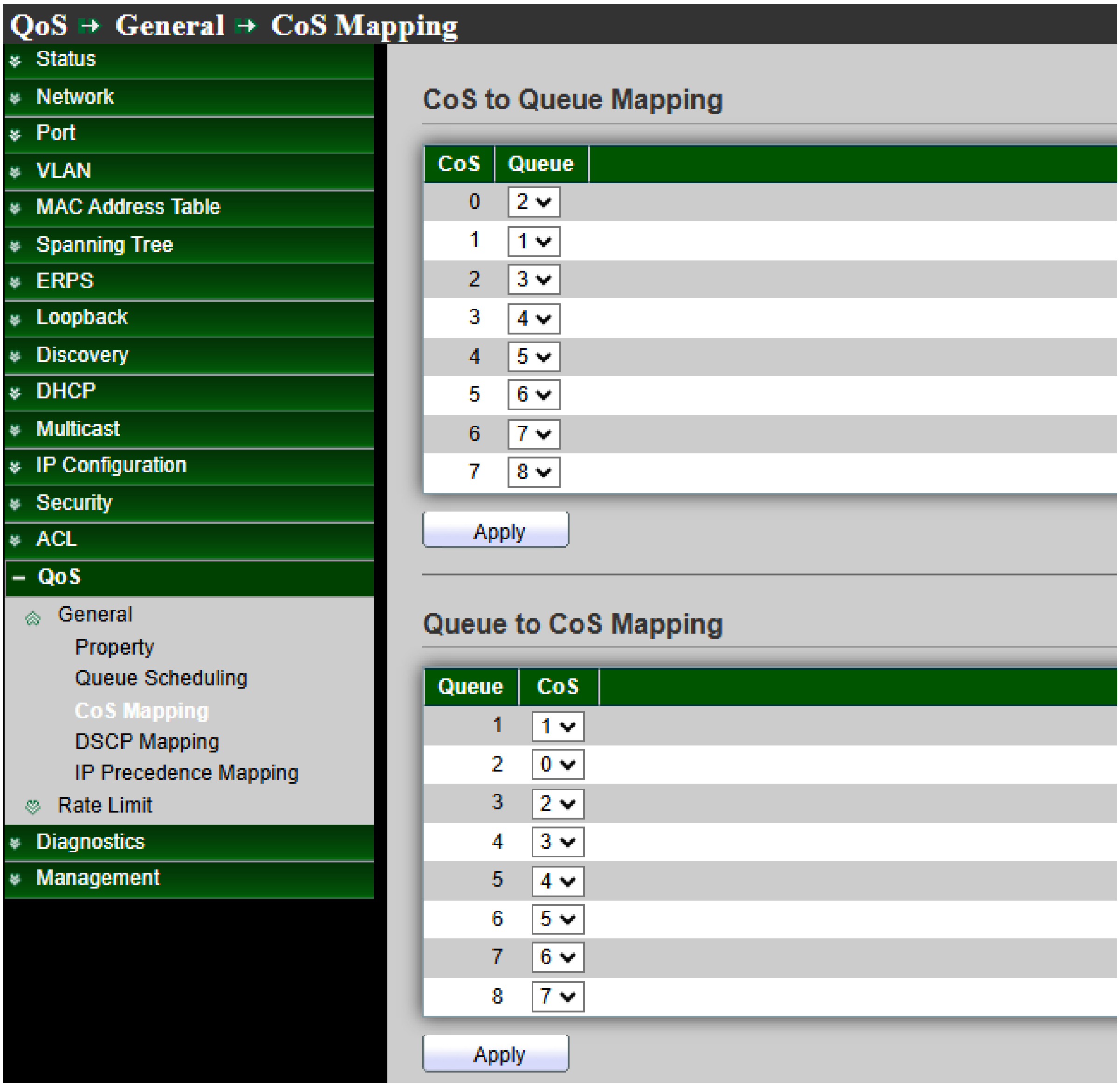
Queue	Method			
	Strict Priority	WRR	Weight	WRR Bandwidth (%)
1	○	●	1	16.67%
2	○	●	2	33.33%
3	○	●	3	50%
4	●	○	4	
5	●	○	5	
6	●	○	9	
7	●	○	13	
8	●	○	15	

Field	Description
Queue	Queue ID to configure
Strict Priority	Set queue to strict priority type
WRR	Set queue to Weight round robin type
Weight	If the queue type is WRR, set the queue weight for the queue.
WRR Bandwidth	Percentage of WRR queue bandwidth

*Click the **"Apply"** button to save your changes settings.*

17.3 CoS Mapping

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



QoS → General → CoS Mapping

CoS to Queue Mapping

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

Queue to CoS Mapping

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

CoS to Queue Mapping

- **CoS:** CoS value.
- **Queue:** Select queue id for the CoS value.

*Click the **"Apply"** button to save your changes settings.*

Queue to CoS Mapping

- **Queue:** Queue ID.
- **Cos:** Select CoS value for the queue id.

*Click the **"Apply"** button to save your changes settings.*

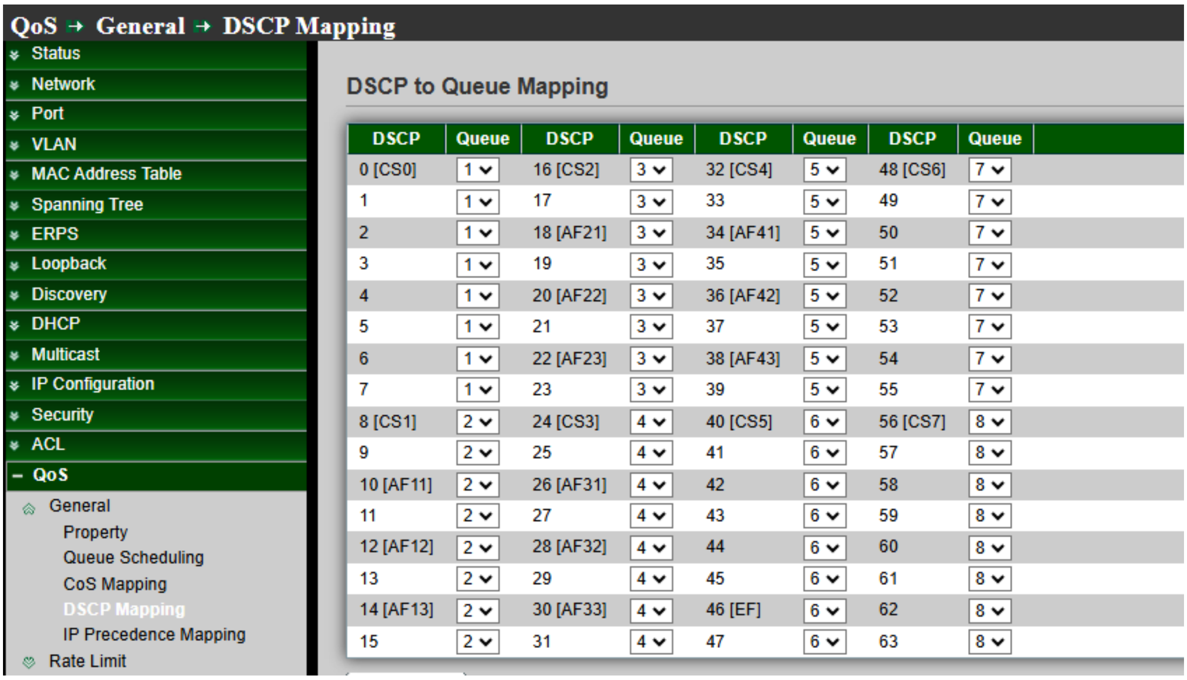
CoS (0 to 7) 7 is highest	Queue(1 to 8) 8 is highest priority	Description
0	2	Background
1	1	Best Effort
2	3	Excellent Effort
3	4	Critical Application LVS phone SIP
4	5	Video
5	6	Voice IP phone default
6	7	Interwork Control LVS phone RTP
7	8	Network Control

17.4 DSCP Mapping

The DSCP to Queue table determines the egress queues of the incoming IP packets based on their DSCP values. The original VLAN Priority Tag (VPT) of the packet is unchanged.

This DSCP values range from 0 through 63, whereas the internal forwarding priority values range from 1 through 8. Any DSCP value within a given range is mapped to the same internal forwarding priority value. These include the CS (Class Selector), AF (Assured Forwarding) and EF (Expedited Forwarding). For example, a packet with a DSCP tag value of 1 can be assigned to the High queue.

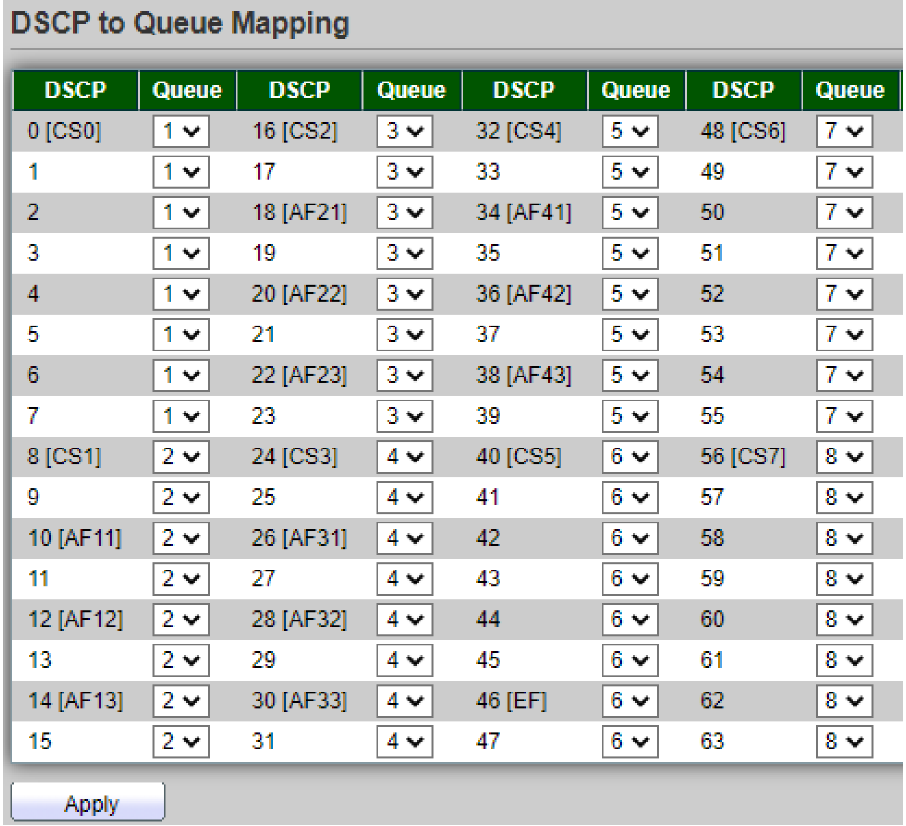
Use the Queues to DSCP page to remark DSCP value for egress traffic from each queue.



DSCP to Queue Mapping

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

DSCP to Queue Mapping



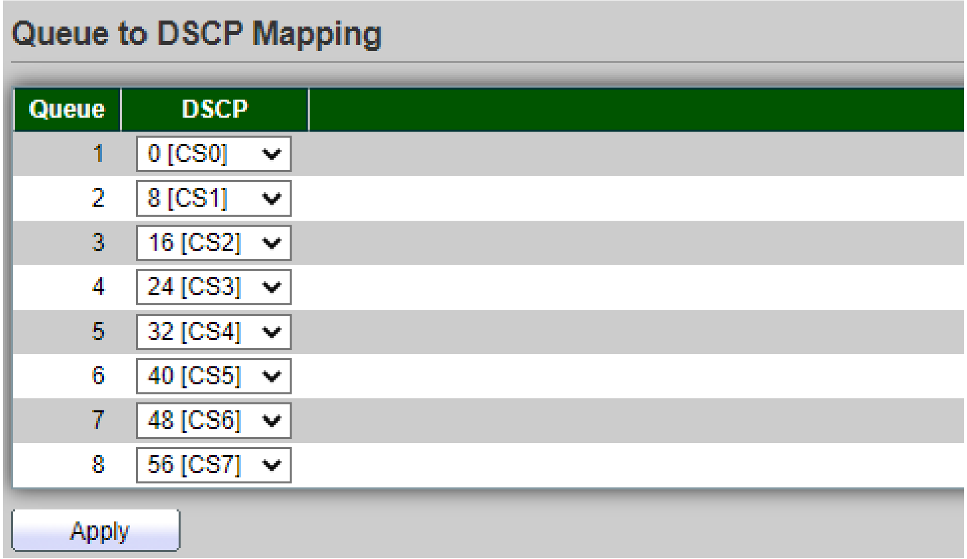
DSCP to Queue Mapping

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

- **DSCP:** DSCP value.
- **Queue:** Select queue id for DSCP value.

*Click the “**Apply**” button to save your changes settings.*

Queue to DSCP Mapping



Queue to DSCP Mapping

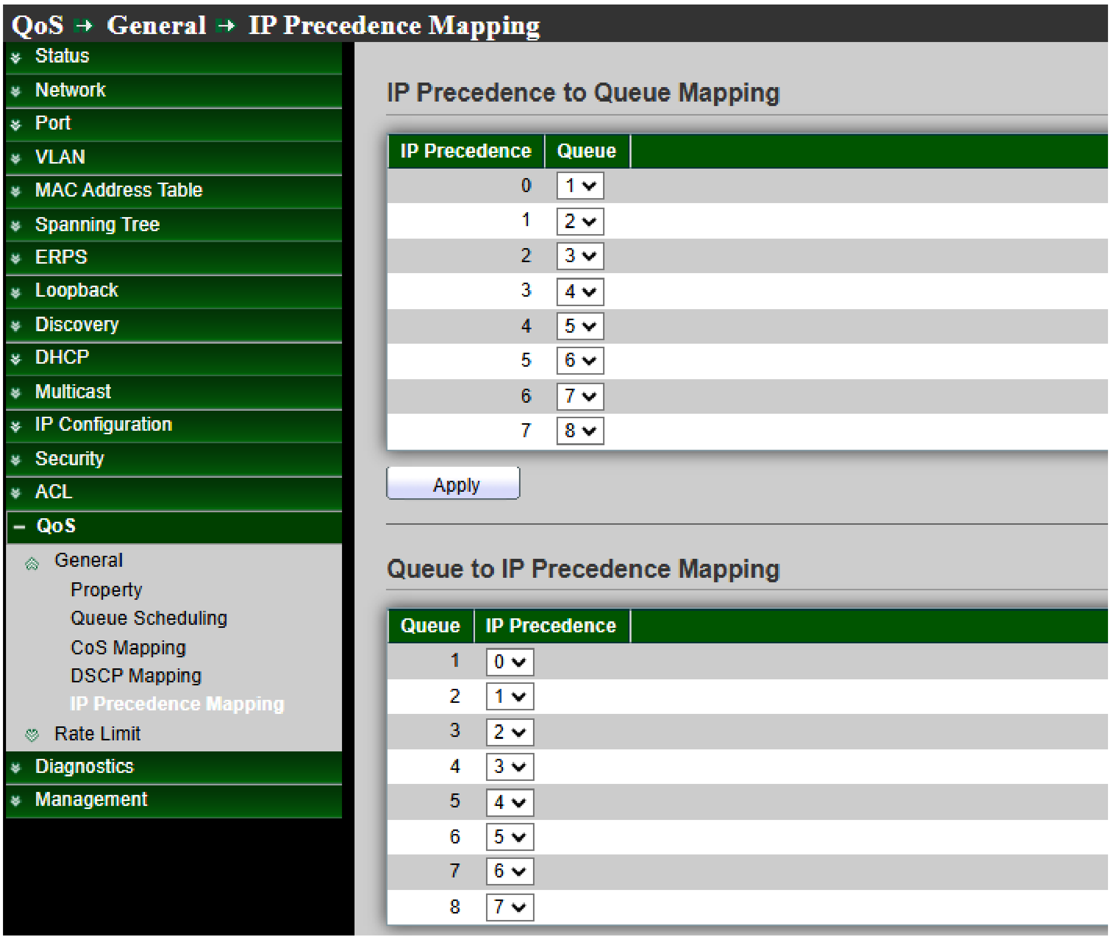
Queue	DSCP
1	0 [CS0]
2	8 [CS1]
3	16 [CS2]
4	24 [CS3]
5	32 [CS4]
6	40 [CS5]
7	48 [CS6]
8	56 [CS7]

- **Queue:** DSCP value.
- **DSCP:** Select DSCP value for queue id.

*Click the “**Apply**” button to save your changes settings.*

17.5 IP Precedence to Queue Mapping

This page allow user to configure IP Precedence to Queue mapping and Queue to IP Precedence mapping , The IP Precedence standard uses the first 3 bits of the ToS byte to mark packets with 8 levels of priority, numbered 0-7, with 0 being the lowest priority and 7 the highest. Because IP Precedence and ToS use different bits in the ToS byte to mark the priority of a packet, they can co-exist in the same packet header without interfering with each other.



IP Precedence to Queue Mapping

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

Queue to IP Precedence Mapping

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

IP Precedence to Queue mapping

- **IP Precedence:** IP Precedence value.
- **Queue:** Queue value which IP Precedence is mapped.

Click the ***"Apply"*** *button to save your changes settings.*

Queue to IP Precedence mapping

- **Queue:** Queue ID.
- **IP Precedence:** IP Precedence value which queue is mapped.

Click the ***"Apply"*** *button to save your changes settings.*

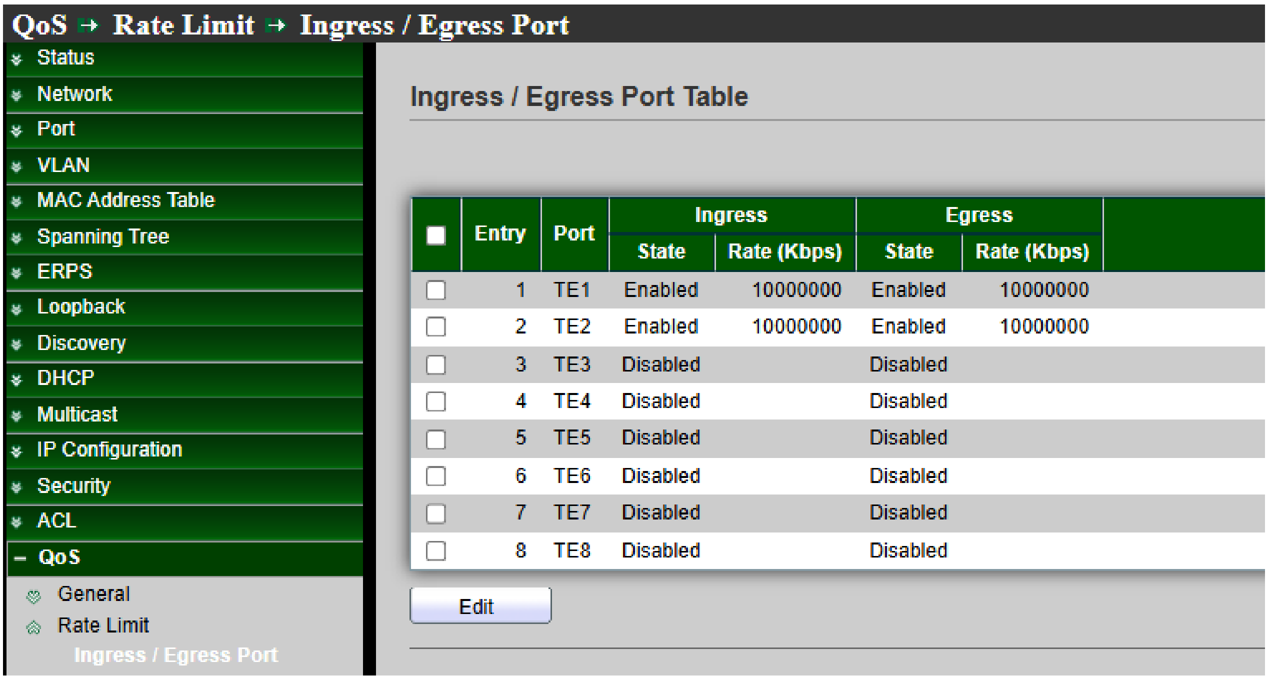
17.6 Rate Limit

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

17.6.1 Ingress / Egress Port

The rate limiting function can be configured to limit of Ingress/Egress traffic on a particular interface.

Administrator can set Ingress/Egress rate limiting in Ports. The usage rate is 16 to 10000000 Kbps

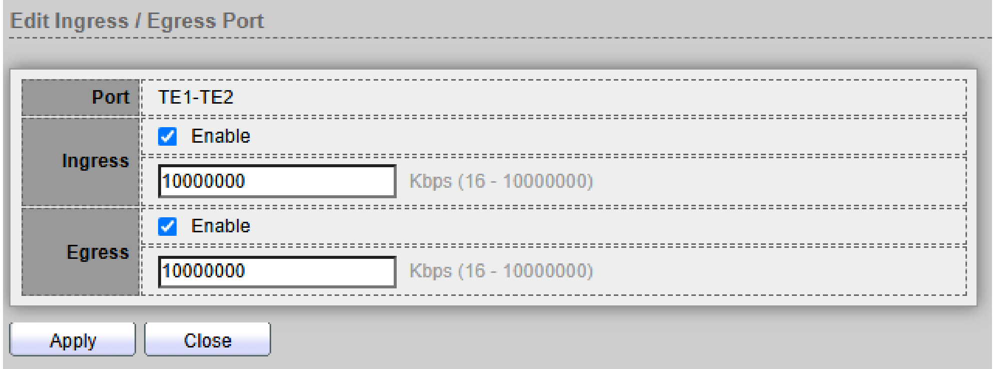


Ingress / Egress Port Table

□	Entry	Port	Ingress		Egress	
			State	Rate (Kbps)	State	Rate (Kbps)
□	1	TE1	Enabled	10000000	Enabled	10000000
□	2	TE2	Enabled	10000000	Enabled	10000000
□	3	TE3	Disabled		Disabled	
□	4	TE4	Disabled		Disabled	
□	5	TE5	Disabled		Disabled	
□	6	TE6	Disabled		Disabled	
□	7	TE7	Disabled		Disabled	
□	8	TE8	Disabled		Disabled	

Field	Description
Port	Port name.

Trust	Port ingress rate limit state: • **Enabled:** To enabled Ingress rate limit function. • **Disabled:** To disabled the Ingress rate limit function.
Ingress (Rate)	Port ingress rate limit value if ingress rate state is enabled.
Trust	Port egress rate limit state: • **Enabled:** To enabled Egress rate limit function. • **Disabled:** To disabled Egress rate limit function.
Egress (Rate)	Port egress rate limit value if egress rate state is enabled.



Edit Ingress / Egress Port

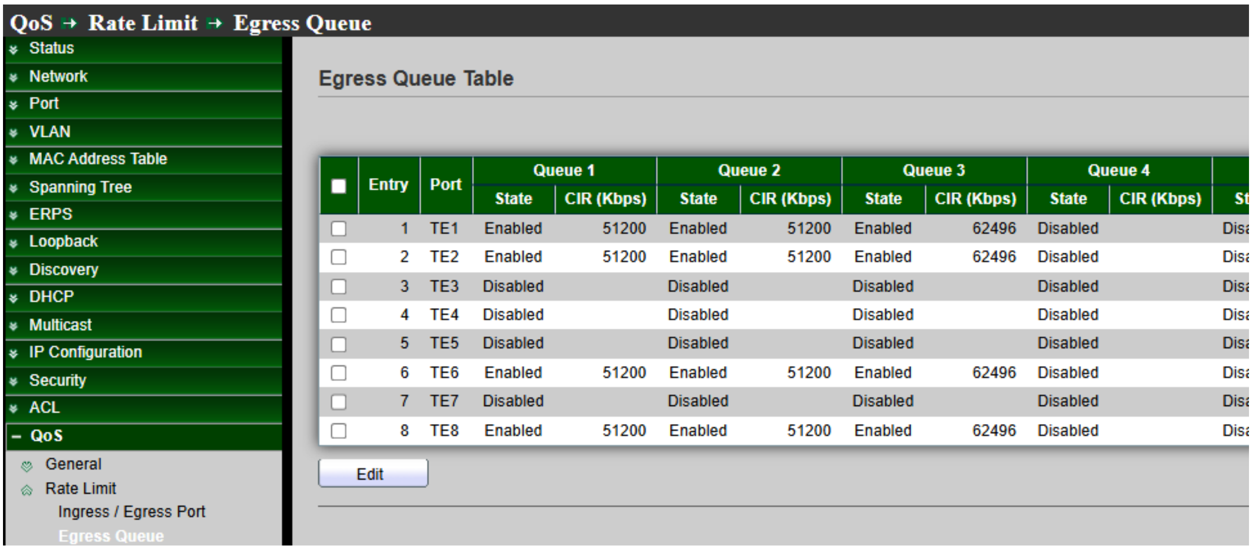
Port	TE1-TE2
Ingress	☑ Enable
	10000000 Kbps (16 - 10000000)
Egress	☑ Enable
	10000000 Kbps (16 - 10000000)

- **Port:** Select the checkbox for port list.
- **Ingress :** Set checkbox to enable/disable ingress rate limit. If ingress rate limit is enabled, rate limit value need to be assigned, The control Range is “16-10000000 Kbps”.
- **Egress :** Set checkbox to enable/disable egress rate limit. If egress rate limit is enabled, rate limit value need to be assigned, The control Range is “16-10000000 Kbps”.

*Click the **“Apply”** button to save your changes or **“Close”** the button to close settings.*

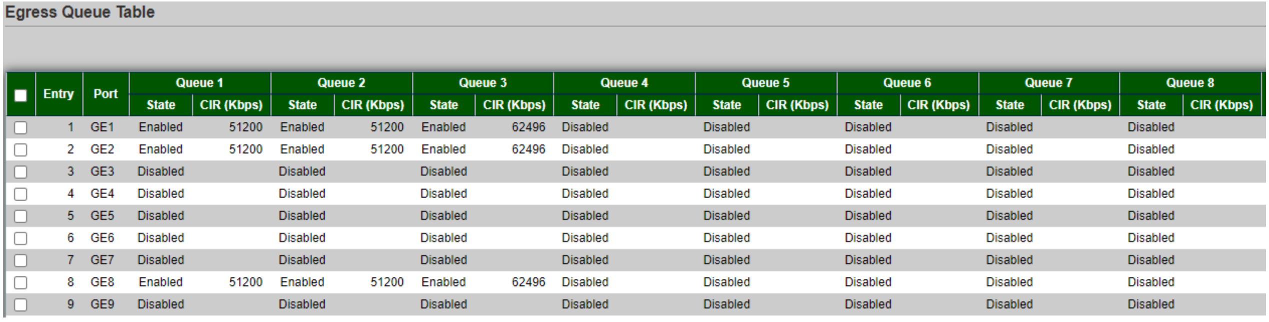
17.6.2 Egress Queue

The Egress Queue function can be configured priority Queue by QoS. Egress rate limiting is performed by shaping the output load.Administrator can set Ingress Queue by limiting QoS . The usage rate is 16 to 1000000 Kbps, Please Click "Edit" button to set the Egress Queue Port menu.



Egress Queue Table

□	Entry	Port	Queue 1		Queue 2		Queue 3		Queue 4		
			State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	St
□	1	TE1	Enabled	51200	Enabled	51200	Enabled	62496	Disabled		Disa
□	2	TE2	Enabled	51200	Enabled	51200	Enabled	62496	Disabled		Disa
□	3	TE3	Disabled		Disabled		Disabled		Disabled		Disa
□	4	TE4	Disabled		Disabled		Disabled		Disabled		Disa
□	5	TE5	Disabled		Disabled		Disabled		Disabled		Disa
□	6	TE6	Enabled	51200	Enabled	51200	Enabled	62496	Disabled		Disa
□	7	TE7	Disabled		Disabled		Disabled		Disabled		Disa
□	8	TE8	Enabled	51200	Enabled	51200	Enabled	62496	Disabled		Disa

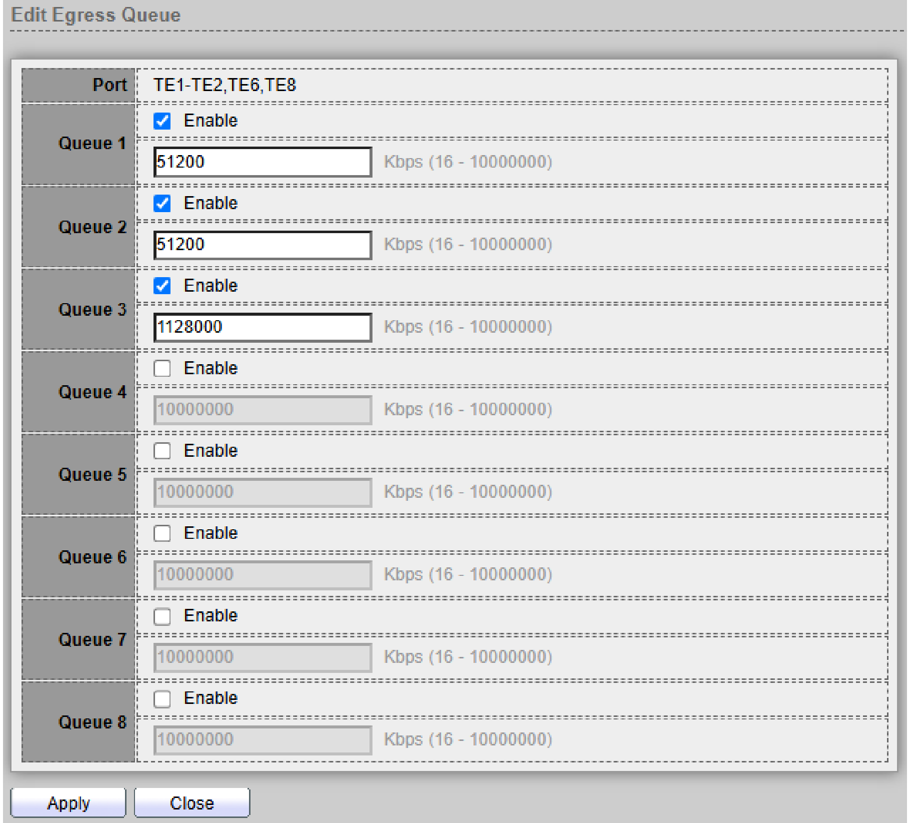


Egress Queue Table

□	Entry	Port	Queue 1		Queue 2		Queue 3		Queue 4		Queue 5		Queue 6		Queue 7		Queue 8	
			State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)
□	1	GE1	Enabled	51200	Enabled	51200	Enabled	62496	Disabled		Disabled		Disabled		Disabled		Disabled	
□	2	GE2	Enabled	51200	Enabled	51200	Enabled	62496	Disabled		Disabled		Disabled		Disabled		Disabled	
□	3	GE3	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	4	GE4	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	5	GE5	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	6	GE6	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	7	GE7	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	8	GE8	Enabled	51200	Enabled	51200	Enabled	62496	Disabled		Disabled		Disabled		Disabled		Disabled	
□	9	GE9	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	

Field	Description
Port	Interface of port number.
Queue 1 (State)	Port egress queue 1 rate limit state • **Enabled:** Egress queue rate limit is enabled. • **Disabled:** Egress queue rate limit is disabled.
Queue 1 (CIR)	Queue 1 egress committed information rate.
Queue 2 (State)	Port egress queue 2 rate limit state. • **Enabled:** Egress queue rate limit is enabled. • **Disabled:** Egress queue rate limit is disabled.
Queue 2 (CIR)	Queue 2 egress committed information rate.
Queue 3 (State)	Port egress queue 3 rate limit state. • **Enabled:** Egress queue rate limit is enabled. • **Disabled:** Egress queue rate limit is disabled.
Queue 3 (CIR)	Queue 3 egress committed information rate.

Queue 4 (State)	Port egress queue 4 rate limit state. - **Enabled:** Egress queue rate limit is enabled. - **Disabled:** Egress queue rate limit is disabled.
Queue 4 (CIR)	Queue 4 egress committed information rate.
Queue 5 (State)	Port egress queue 5 rate limit state. - **Enabled:** Egress queue rate limit is enabled. - **Disabled:** Egress queue rate limit is disabled.
Queue 5 (CIR)	Queue 5 egress committed information rate.
Queue 6 (State)	Port egress queue 6 rate limit state. - **Enabled:** Egress queue rate limit is enabled. - **Disabled:** Egress queue rate limit is disabled
Queue 6 (CIR)	Queue 6 egress committed information rate.
Queue 7 (State)	Port egress queue 7 rate limit state. - **Enabled:** Egress queue rate limit is enabled. - **Disabled:** Egress queue rate limit is disabled.



Edit Egress Queue

Port	TE1-TE2,TE6,TE8
Queue 1	☑ Enable 51200 Kbps (16 - 10000000)
Queue 2	☑ Enable 51200 Kbps (16 - 10000000)
Queue 3	☑ Enable 1128000 Kbps (16 - 10000000)
Queue 4	□ Enable 10000000 Kbps (16 - 10000000)
Queue 5	□ Enable 10000000 Kbps (16 - 10000000)
Queue 6	□ Enable 10000000 Kbps (16 - 10000000)
Queue 7	□ Enable 10000000 Kbps (16 - 10000000)
Queue 8	□ Enable 10000000 Kbps (16 - 10000000)

Set checkbox to enable/disable ingress priority queue 1 to~ queue 8 level , The control range is “16-1000000 Kbps”

- **Port:** Select one or multiple ports for the configure.
- **Queue 1:** Set checkbox to enable/disable egress queue 1 rate limit.
  - **Enable:** If egress rate limit is enabled, rate limit value need to be assigned.
- **Queue 2:** Set checkbox to enable/disable egress queue 2 rate limit.
  - **Enable:** If egress rate limit is enabled, rate limit value need to be assigned.
- **Queue 3:** Set checkbox to enable/disable egress queue 3 rate limit.
  - **Enable:** If egress rate limit is enabled, rate limit value need to be assigned.
- **Queue 4:** Set checkbox to enable/disable egress queue 4 rate limit.
  - **Enable:** If egress rate limit is enabled, rate limit value need to be assigned.
- **Queue 5:** Set checkbox to enable/disable egress queue 5 rate limit.
  - **Enable:** If egress rate limit is enabled, rate limit value need to be assigned.
- **Queue 6:** Set checkbox to enable/disable egress queue 6 rate limit.
  - **Enable:** If egress rate limit is enabled, rate limit value need to be assigned.
- **Queue 7:** Set checkbox to enable/disable egress queue 7 rate limit.
  - **Enable:** If egress rate limit is enabled, rate limit value need to be assigned.
- **Queue 8:** Set checkbox to enable/disable egress queue 8 rate limit.
  - **Enable:** If egress rate limit is enabled, rate limit value need to be assigned.

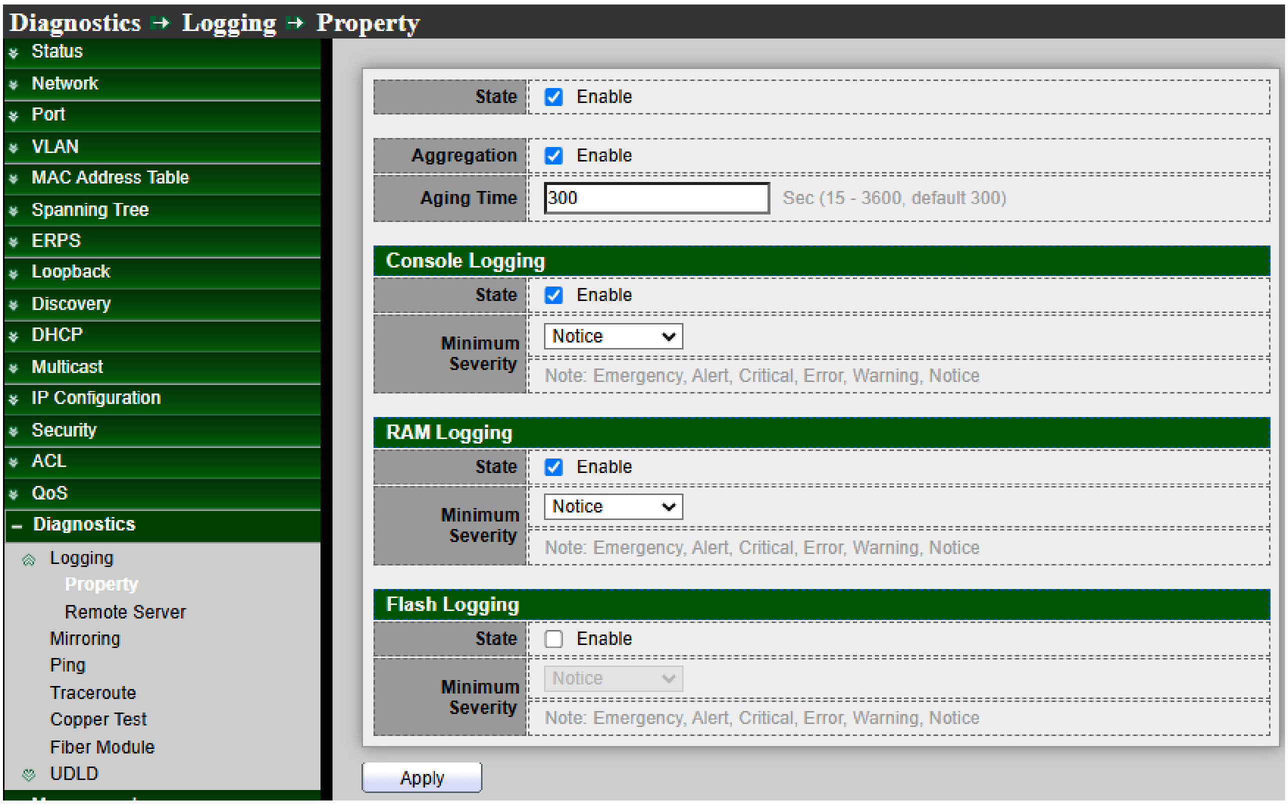
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

18. Diagnostics

18.1 Logging

18.1.1 Property

This function support log message includes Console / RAM / Flash message send to remote log server. Administrator can enable or disable this function. Use the Diagnostics pages to configure settings for the switch diagnostics feature or operating diagnostic utilities.



State ☑ Enable

Aggregation ☑ Enable

Aging Time 300 Sec (15 - 3600, default 300)

Console Logging

State ☑ Enable

Minimum Severity Notice

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

RAM Logging

State ☑ Enable

Minimum Severity Notice

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

Flash Logging

State □ Enable

Minimum Severity Notice

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

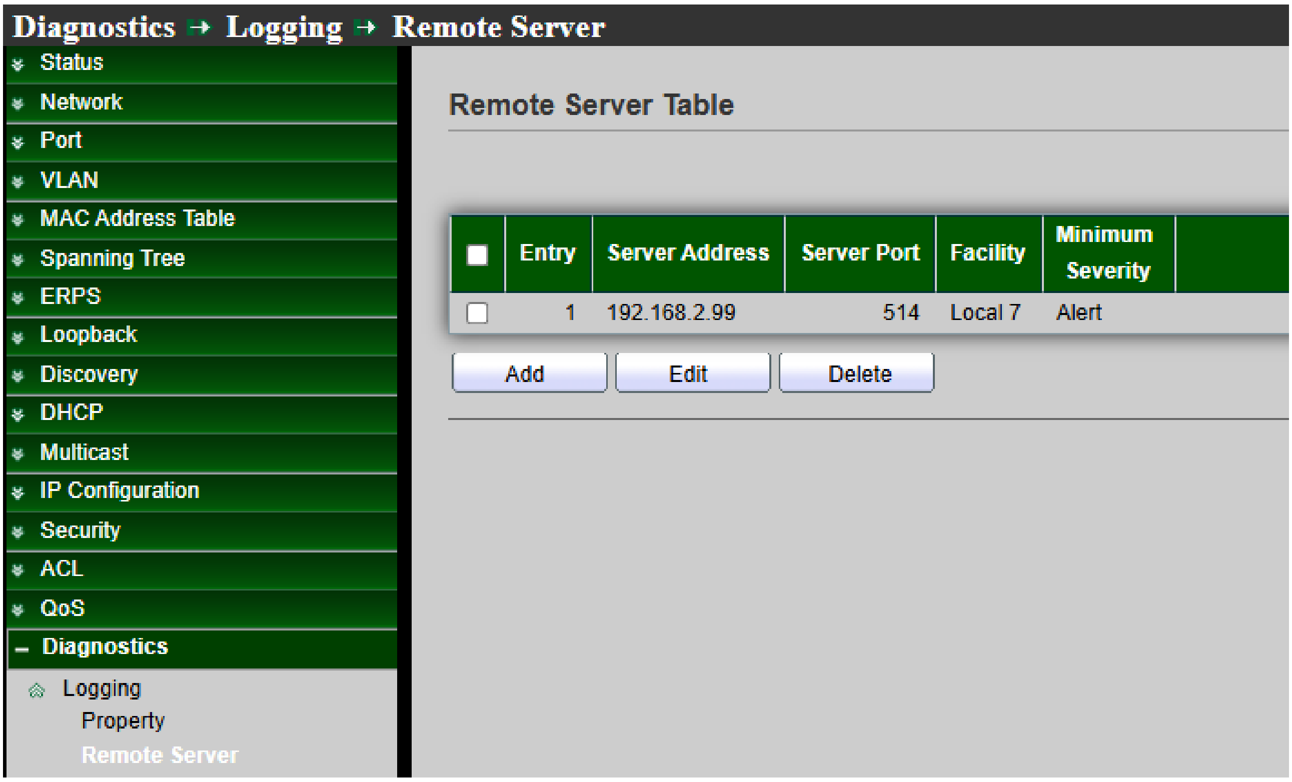
- **State:** When the logging service is enabled, logging configuration of each destination rule can be individually configured. If the logging service is disabled, no messages will be sent to these destinations.
  - **Enable:** Enable/Disable the global logging services.
- **Aggregation:**
  - **Enable:** Enable/Disable the aggregation services.
  - **Aging:** 15~3600 Second. The default is 300 second.
- **Console Logging:**
  - **State:** Enable/Disable the Console Logging services.
  - **Minimum Severity:** The minimum severity for the Console Logging. Including selection of events such as Emergency, Alert, Critical, Error, Warning, Notice, Information, Debug, etc.
- **RAM Loggong:**
  - **State:** Enable/Disable the RAM Loggong services.
  - **Minimum Severity:** The minimum severity for the RAM logging. Including selection of events such as Emergency, Alert, Critical, Error, Warning, Notice, Information, Debug, etc.
- **Flash Loggong:**
  - **State:** Enable/Disable the Flash Loggong services.
  - **Minimum Severity:** The minimum severity for the flash logging. Including selection of events such as Emergency, Alert, Critical, Error, Warning, Notice, Information, Debug, etc.

Note	• Emergency—System is not usable. • Alert—Action is needed. • Critical—System is in a critical condition. • Error—System is in error condition. • Warning—System warning has occurred. • Notice—System is functioning properly, but a system notice has occurred. • Informational—Device information. • Debug—Detailed information about an event.

*Click the **"Apply"** button to save your changes settings.*

18.1.2 Remote Server

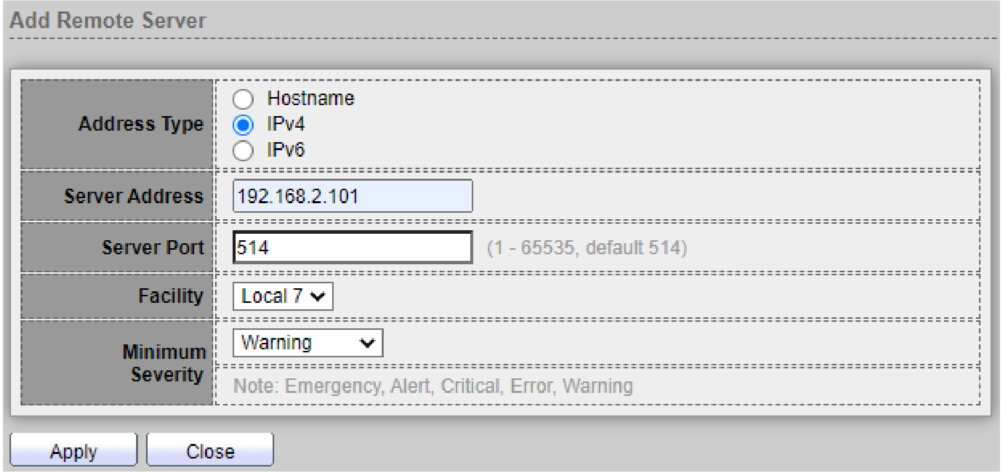
Use the Remote Log Servers page to define the remote SYSLOG servers where log messages are sent (using the SYSLOG protocol). For each server, you can configure the severity of the messages that it receives, Setting **"add"** and "Edit" and **"Delete"** for this function management.



Remote Server Table

□	Entry	Server Address	Server Port	Facility	Minimum Severity
□	1	192.168.2.99	514	Local 7	Alert

Field	Description
Server Address	The IP address of the remote logging server.
Server Ports	The port number of the remote logging server.
Facility	The facility of the logging messages. It can be one of the following values: local0, local1, local2, local3, local4, local5, local6, and l7.
Minimum Severity	The minimum severity. • **Emergence:** System is not usable. • **Alert:** Immediate action is needed. • **Critical:** System is in the critical condition. • **Error:** System is in error condition. • **Warning:** System warning has occurred. • **Notice:** System is functioning properly, but a system notice has occurred. • **Informational:** Device information. • **Debug:** Provides detailed information about an event.



Add Remote Server

Address Type	○ Hostname ● IPv4 ○ IPv6
Server Address	192.168.2.101
Server Port	514 (1 - 65535, default 514)
Facility	Local 7
Minimum Severity	Warning Note: Emergency, Alert, Critical, Error, Warning

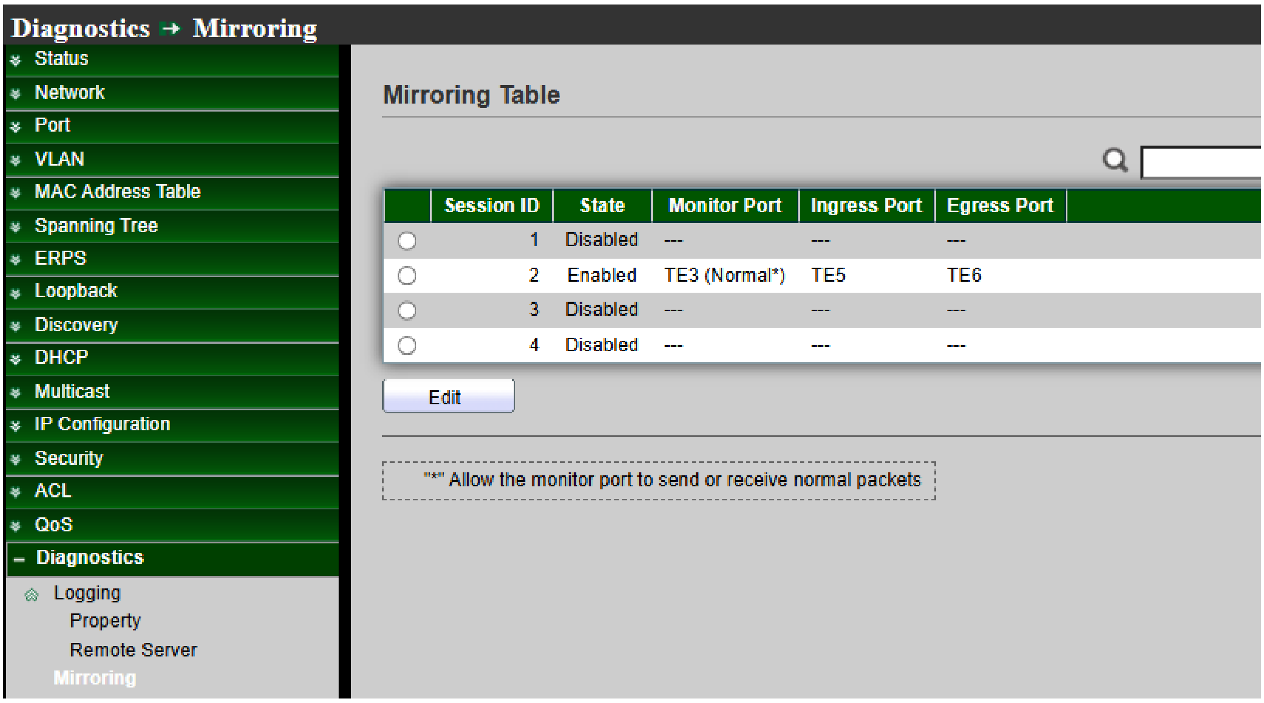
- **Address Type:** Administrator can select use Hostname or IPv4/6 connection remote log server.
- **Server Address:** Enter the IP address of the server.
- **Server Port:** Enter service port to which the log messages are sent.
- **Facility:** Select a facility from which system logs are sent to the remote server. Only one facility can be assigned to a server.
- **Minimum Severity:** Select the minimum level of system log messages to be sent to the server.

- **Emergence:** System is not usable.
- **Alert:** Immediate action is needed.
- **Critical:** System is in the critical condition.
- **Error:** System is in error condition.
- **Warning:** System warning has occurred.
- **Notice:** System is functioning properly, but a system notice has occurred.
- **Informational:** Device information.
- **Debug:** Provides detailed information about an event..

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

18.2 Mirroring

Mirroring function can mirror Rx/Tx traffic, Packet can mirror to destination port and for analysis.



Mirroring Table

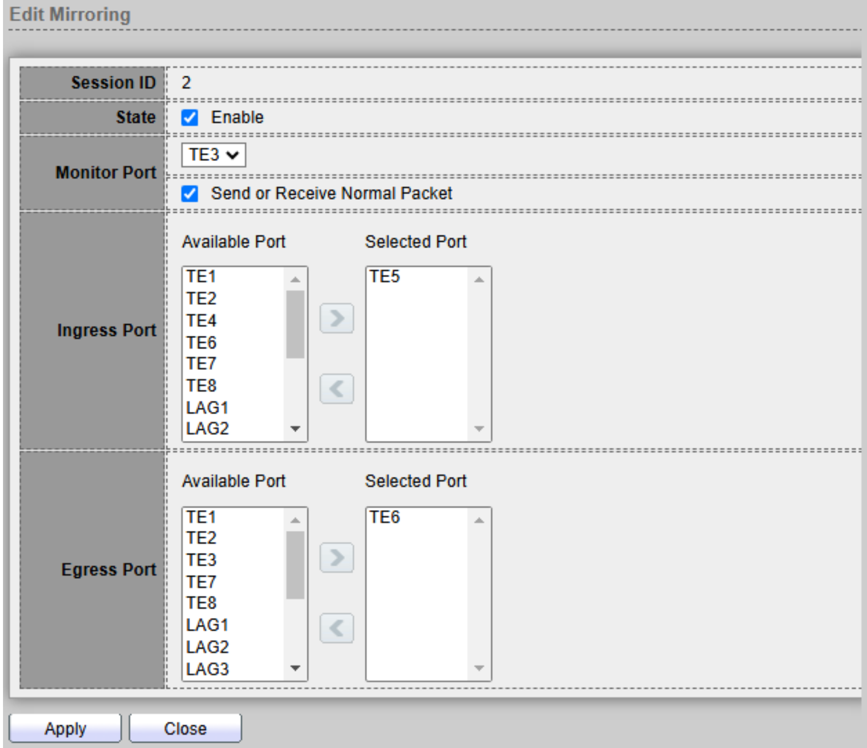
	Session ID	State	Monitor Port	Ingress Port	Egress Port
○	1	Disabled	---	---	---
○	2	Enabled	TE3 (Normal*)	TE5	TE6
○	3	Disabled	---	---	---
○	4	Disabled	---	---	---

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

Field	Description
Session ID	Select mirror session ID

State	Select mirror session state : port-base mirror or disable • **Enabled:** Enable port based mirror • **Disabled:** Disable mirror.
Monitor Port	Select mirror session monitor port, and select whether normal packet could be sent or received by monitor port.
Ingress port	Select mirror session source rx ports
Egress ports	Select mirror session source tx ports

*Click the "**Edit**" button to edit your settings.*



Edit Mirroring

Session ID	2
State	☑ Enable
Monitor Port	TE3 ☑ Send or Receive Normal Packet
Ingress Port	Available Port: TE1, TE2, TE4, TE6, TE7, TE8, LAG1, LAG2 Selected Port: TE5
Egress Port	Available Port: TE1, TE2, TE3, TE7, TE8, LAG1, LAG2, LAG3 Selected Port: TE6

➢ **Session ID:** Display selected mirror session ID.

➢ **State:**

- **Enable:** Enable/Disable the mirroring function.

➢ **Mirroring Port:** Administrator can choose a mirroring Port.

➢ **Ingress Port:** Administrator can choose mirrored ports for ingress.

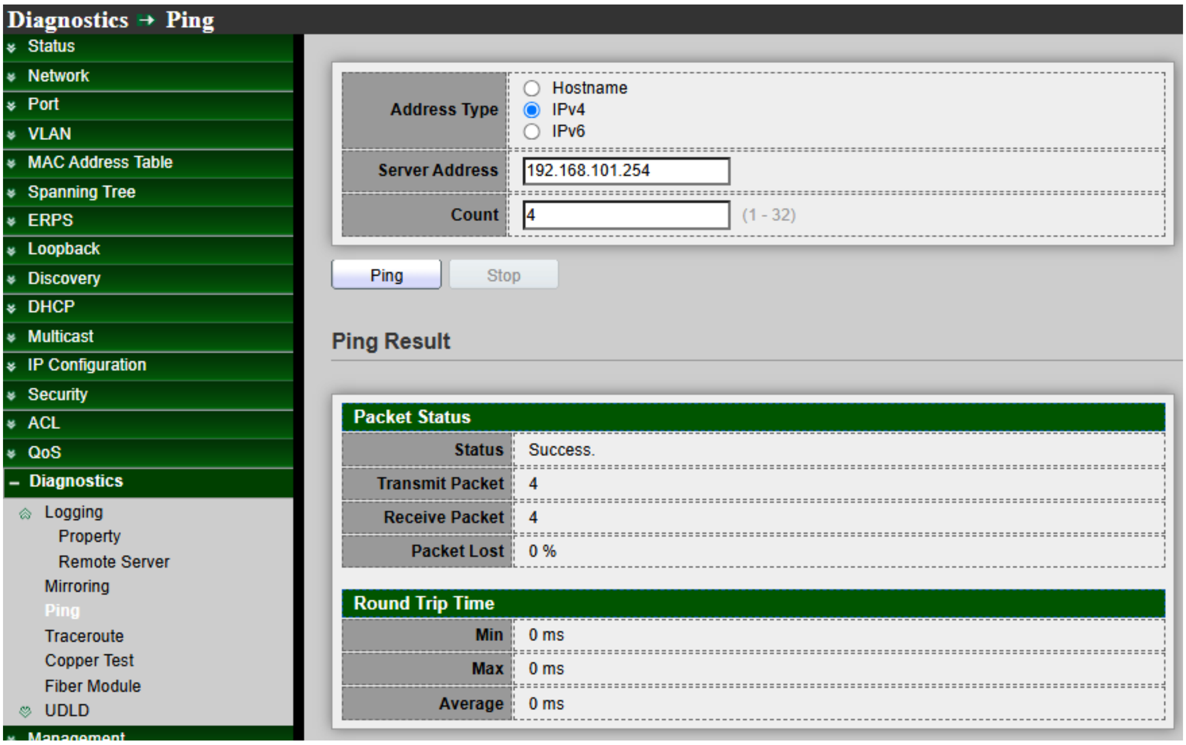
➢ **Egress Port:** Administrator can choose mirrored ports for egress

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

18.3 Ping

The Ping utility tests if a remote host can be reached and measures the round-trip time for packets sent from the device to a destination device.

Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP response, sometimes called a pong. It measures the round-trip time and records any packet loss, Administrators can use this ping function to check connected device whether is active. This ping function support IPv4 and IPv6 protocol.



Address Type: ○ Hostname ● IPv4 ○ IPv6

Server Address: 192.168.101.254

Count: 4 (1 - 32)

Ping Result

Packet Status	
Status	Success.
Transmit Packet	4
Receive Packet	4
Packet Lost	0 %

Round Trip Time	
Min	0 ms
Max	0 ms
Average	0 ms

- **Address Type:** Specify the address type to "Hostname", "IPv6", or "IPv4".
- **Server Address:** Specify the Hostname/IPv4/IPv6 address for the remote logging server.
- **Count:** Specify the numbers of each ICMP ping request.

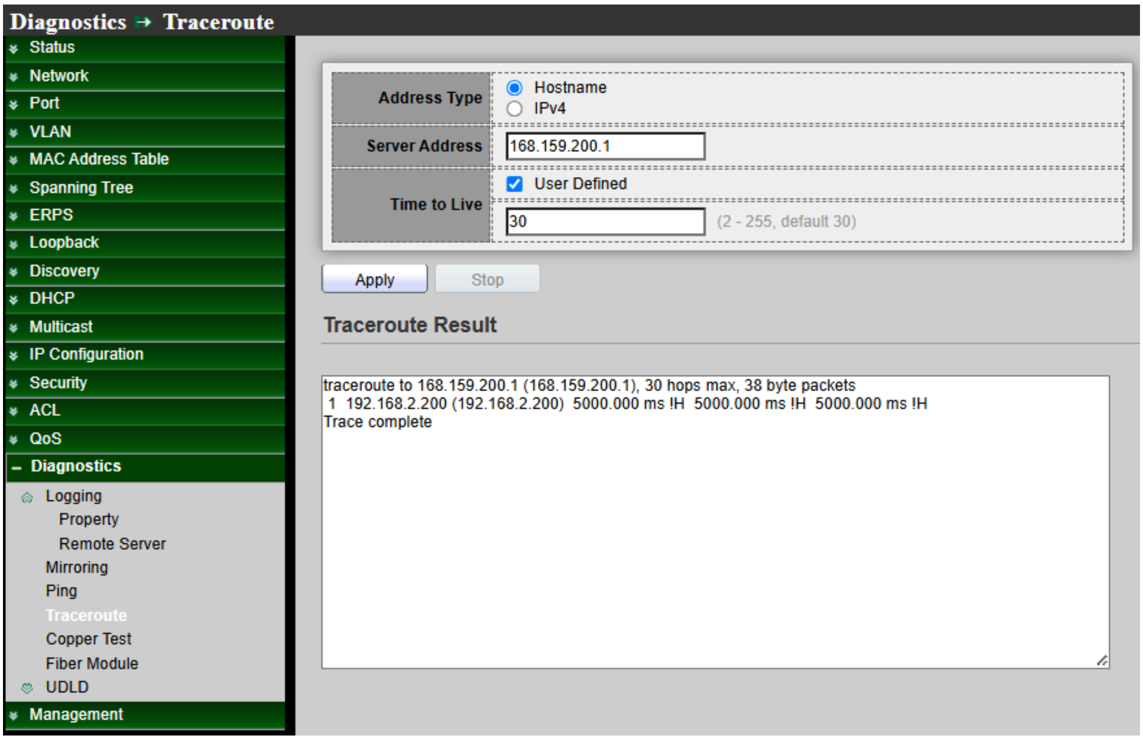
*Click the **"Ping"** button to ping result appears.*

Field	Description
Packet Status	Displays whether the ping succeeded or failed. • **Status:** Displays the ping result status of " Success" or "Ping failed (timeout)". • **Transmit Packet:** Number of packets sent by ping.

	• **Receive Packet:** Number of packets received by ping. • **Packet Lost:** Percentage of packets lost in ping process.
Round Trip Time	Displays the ping **round trip time.** • **Min:** Shortest time for packet to return. • **Max:** Longest time for packet to return. • **Average:** Average time for packet to return

18.4 Traceroute

Traceroute discovers the IP routes along which packets were forwarded by sending an IP packet to the target host and back to the switch. The Traceroute page displays each hop between the switch and a target host and the round-trip time to each hop.



Diagnostics → Traceroute

Address Type	● Hostname ○ IPv4
Server Address	168.159.200.1
Time to Live	☑ User Defined 30 (2 - 255, default 30)

Traceroute Result

```
traceroute to 168.159.200.1 (168.159.200.1), 30 hops max, 38 byte packets
 1  192.168.2.200 (192.168.2.200)  5000.000 ms !H  5000.000 ms !H  5000.000 ms !H
Trace complete
```

➢ **Address Type:** Specify the address type to "Hostname", or "IPv4".

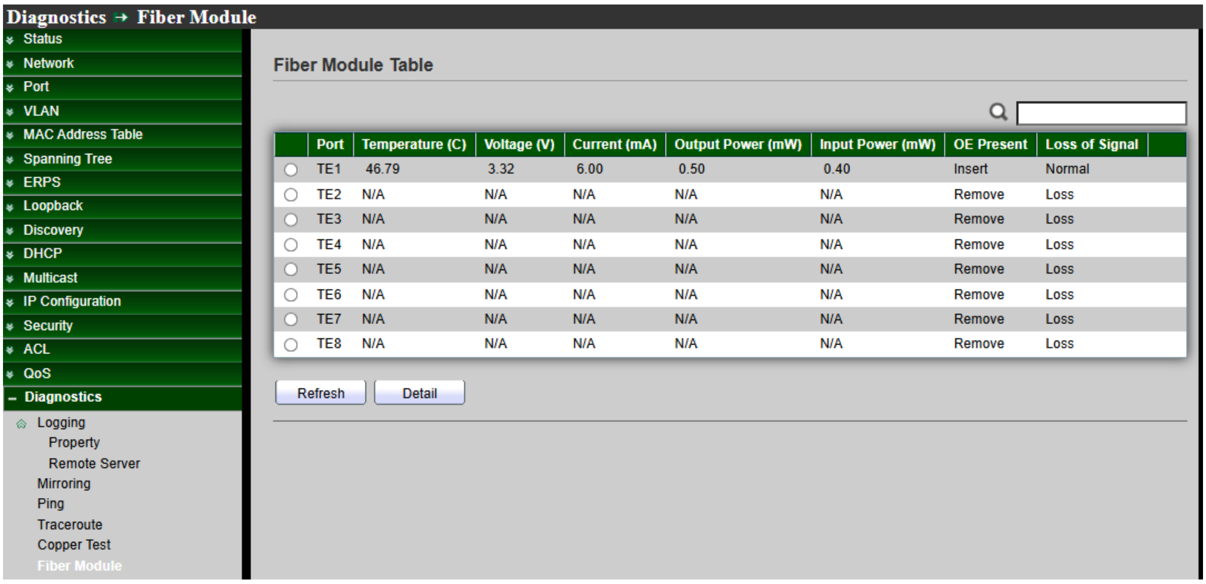
➢ **Server Address:** Specify the Hostname/IPv4 address for the remote logging server.

➢ **Time to Live :**Enter the maximum number of hops that Traceroute permits. This is used to prevent a case where the sent frame gets into an endless loop. The Traceroute command terminates when the destination is reached or when this value is reached. To use the default value (30), select Use Default.

*Click the **"Apply"** button to Traceroute result appears.*

18.5 Fiber Module

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



	Port	Temperature (C)	Voltage (V)	Current (mA)	Output Power (mW)	Input Power (mW)	OE Present	Loss of Signal
○	TE1	46.79	3.32	6.00	0.50	0.40	Insert	Normal
○	TE2	N/A	N/A	N/A	N/A	N/A	Remove	Loss
○	TE3	N/A	N/A	N/A	N/A	N/A	Remove	Loss
○	TE4	N/A	N/A	N/A	N/A	N/A	Remove	Loss
○	TE5	N/A	N/A	N/A	N/A	N/A	Remove	Loss
○	TE6	N/A	N/A	N/A	N/A	N/A	Remove	Loss
○	TE7	N/A	N/A	N/A	N/A	N/A	Remove	Loss
○	TE8	N/A	N/A	N/A	N/A	N/A	Remove	Loss

Field	Description
Port	Interface or port number.
Temperature	Internally measured transceiver temperature.
Voltage	Internally measured supply voltage.
Current	Measured TX bias current.
Output Power	Measured TX output power in mill watts.
Input Power	Measured RX received power in mill watts.
Transmitter Fault	State of TX fault.
OE Present	Indicate transceiver has achieved power up and data is ready.
Loss of Signal	Loss of signal.

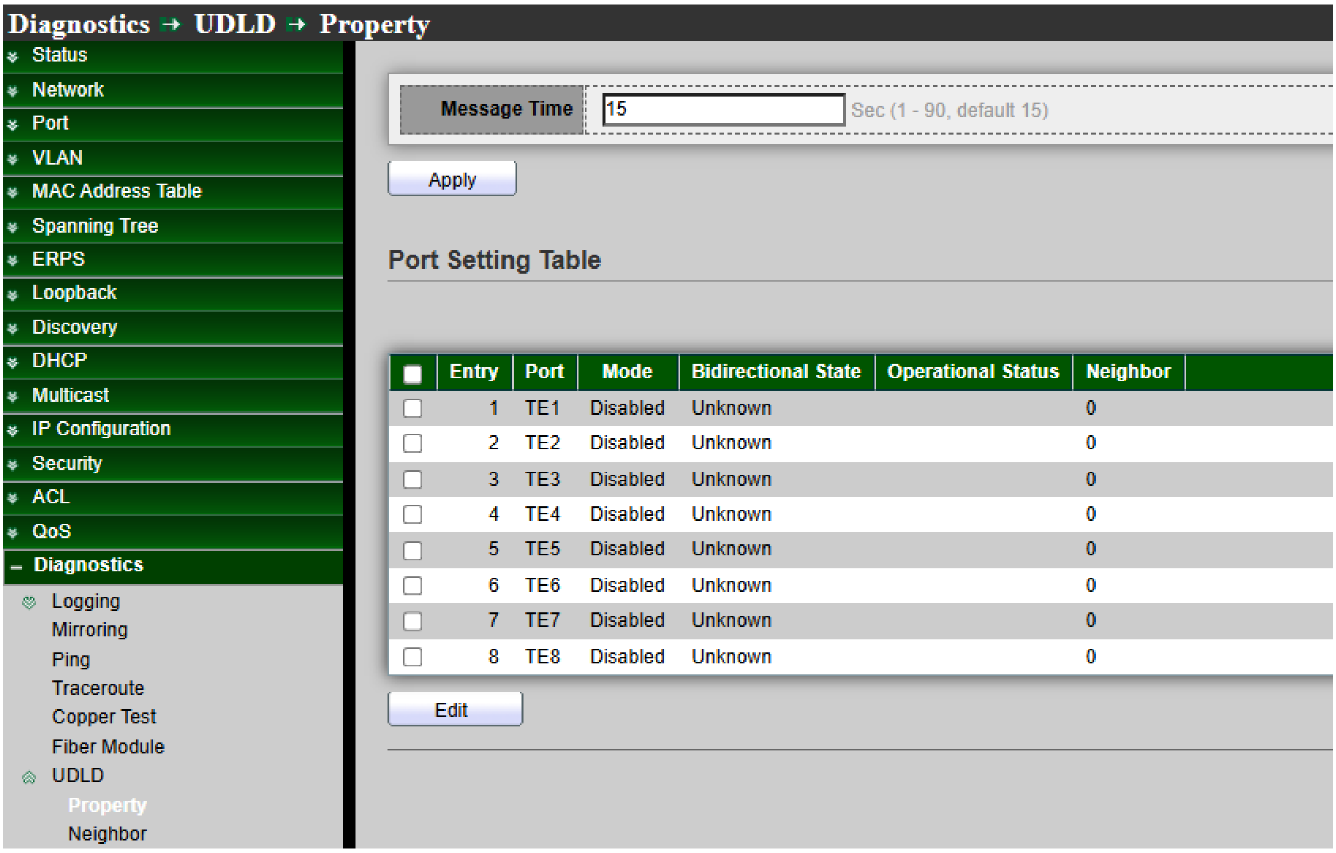
*Click the **"Refresh"** button to refresh this page or click the **"Detail"** button to check detail information.*

18.6 UDLD

Uni-Directional Link Detection (UDLD) monitors a link between two devices and brings the ports on both ends of the link down if the link goes down at any point between the two devices, Use the UDLD pages to configure settings of UDLD function.

18.6.1 Property

This page allow user to configure global and per interface settings of UDLD.



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

Port Setting Table

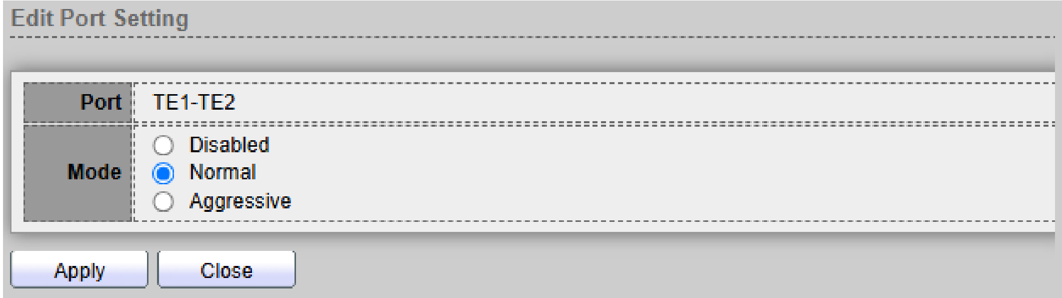
□	Entry	Port	Mode	Bidirectional State	Operational Status	Neighbor
□	1	TE1	Disabled	Unknown		0
□	2	TE2	Disabled	Unknown		0
□	3	TE3	Disabled	Unknown		0
□	4	TE4	Disabled	Unknown		0
□	5	TE5	Disabled	Unknown		0
□	6	TE6	Disabled	Unknown		0
□	7	TE7	Disabled	Unknown		0
□	8	TE8	Disabled	Unknown		0

- **Message Time:** To use the UDLD protocol all connected switches and interfaces have to be configured for it. A UDLD configured switch sends UDLD advertisements, "hello" packets to its neighbors and expects to receive one in the designated hold time (the default hold time is 15mins). If this doesn't happen the UDLD disables the unresponsive interface..

*Click the **"Apply"** button to save your changes settings.*

Field	Description
Port	Display port ID of entry.

Mode	Display UDLD running mode of interface.
Bidirectional State	Display bidirectional state of interface.
Operational Status	Display operational status of interface
Neighbor	Display the number of neighbor of interface



Edit Port Setting

Port	TE1-TE2
Mode	○ Disabled ● Normal ○ Aggressive

- **Port:** Select one or multiple ports for the configure.
- **Mode:** Select UDLD running mode of interface.
  - **Disabled:** Disable UDLD function.
  - **Normal:** Running on normal mode that port goes to Link Up One phase after last neighbor ages out.
  - **Aggressive:** Running on aggressive mode that port goes to Re-Establish phase after last neighbor ages out.

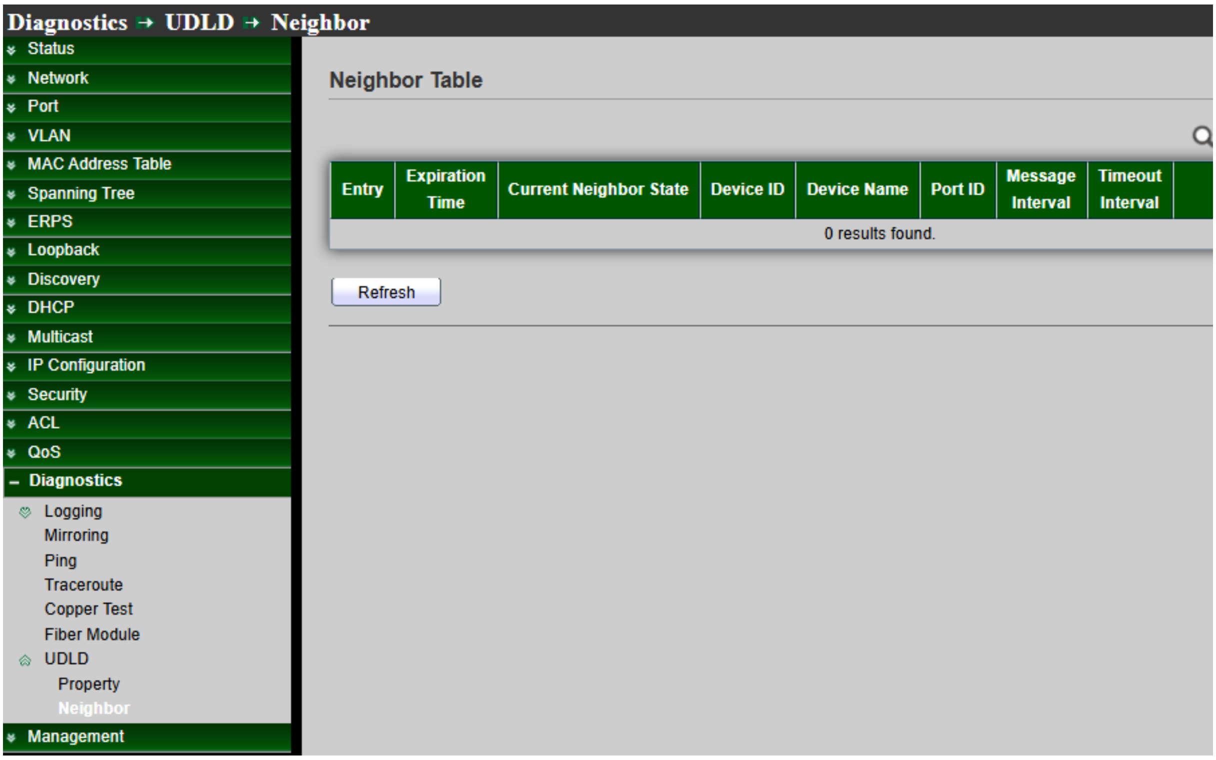
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

18.6.2 Neighbor

Each switch port that is configured for UDLD exchanges UDLD protocol packets that include information about the port's device and port ID, and the port also sends the same device and port ID information that it knows about its connected neighbor.

Because of this, a port should receive its own device and port ID information from its neighbor if the link is bi-directional. If a port does not receive information about its own device and port ID from its neighbor, the link is considered to be unidirectional.

This can occur when the link is up on both sides, but one side is not receiving packets, or when wiring mistakes occur, causing the transmit and receive wires to not be connected to the same ports on both ends of a link.



Diagnostics → UDLD → Neighbor

Neighbor Table

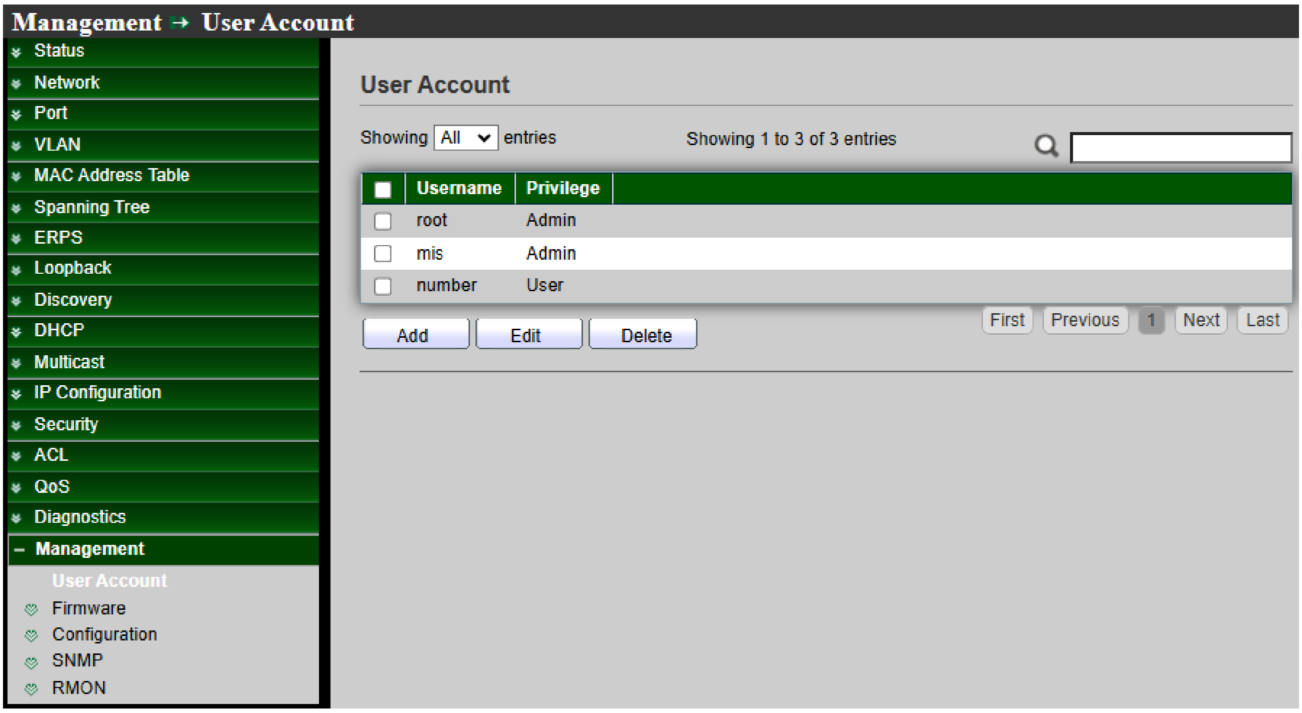
Entry	Expiration Time	Current Neighbor State	Device ID	Device Name	Port ID	Message Interval	Timeout Interval
0 results found.							

Field	Description
Entry	Display entry index.
Expiration Time	Display expiration time before age out.
Current Neighbor State	Display neighbor current state
Device ID	Display neighbor device ID.
Device Name	Display neighbor device name.
Port ID	Display neighbor port ID that connected.
Message Interval	Display neighbor message interval.
Timeout Interval	Display neighbor timeout interval

19. Management

19.1 User Account

The default username/password is root/default. Administrator can modify login password or create new username / password and defined Privilege, Setting **“add”** and “Edit” and **“Delete”** function for this management.



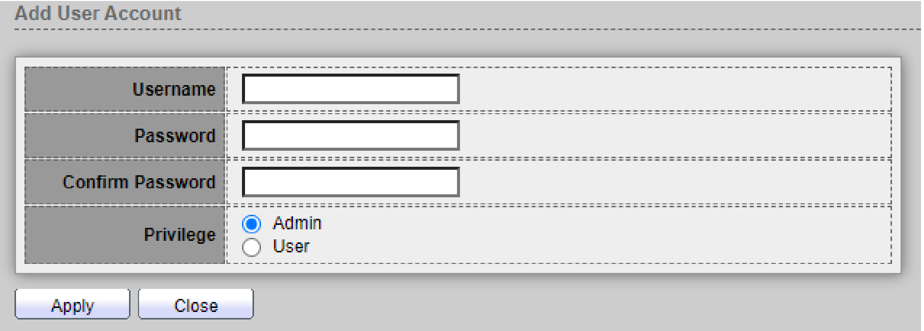
User Account

Showing All entries

Showing 1 to 3 of 3 entries

□	Username	Privilege
□	root	Admin
□	mis	Admin
□	number	User

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



Add User Account

Username	
Password	
Confirm Password	
Privilege	● Admin ○ User

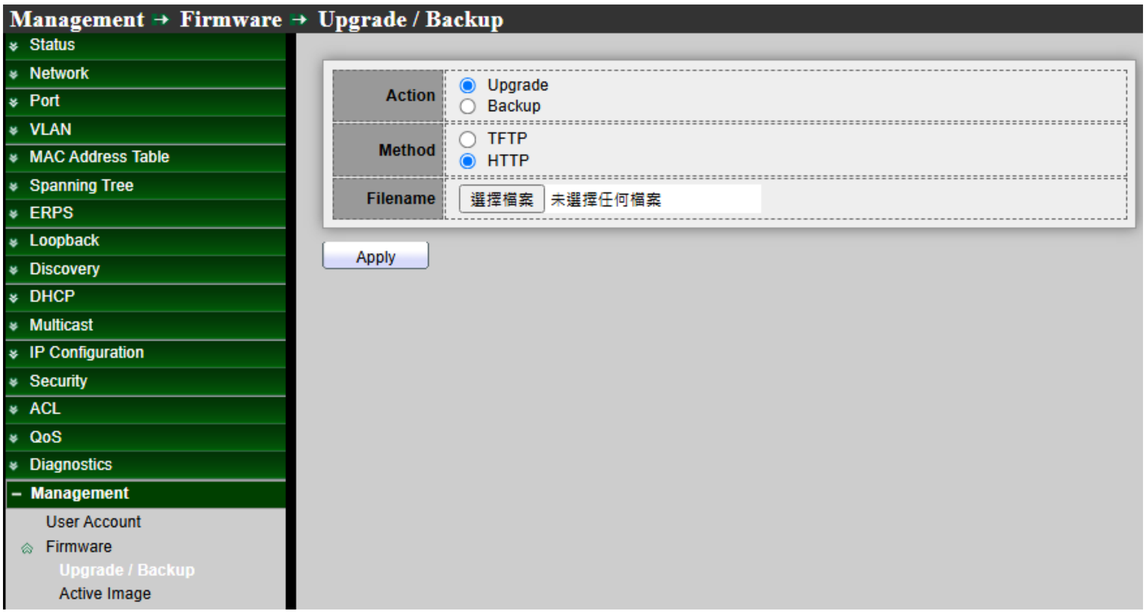
- **Username:** User name of the account.
- **Password:** Set password of the account.
- **Confirm Password:** Set the same password of the account as in “Password” field.
- **Privilege:** Select privilege level for new account.
  - **Admin:** Allow to change switch settings. Privilege value equals to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

*Click the **“Apply”** button to save your changes or **“Close”** the button to close settings.*

19.2 Firmware

19.2.1 Upgrade / Backup

Administrator can upgrade or backup firmware, method can choose use TFTP or HTTP protocol. If choose backup then administrator can choose firmware image to backup.



Management → Firmware → Upgrade / Backup

Action	● Upgrade ○ Backup
Method	○ TFTP ● HTTP
Filename	選擇檔案 未選擇任何檔案

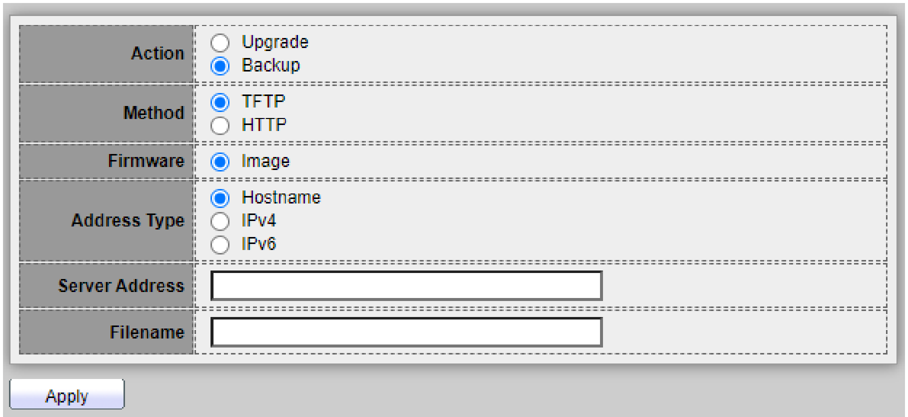
- **Action:** Firmware operations.
  - **Upgrade:** Upgrade firmware from remote host to DUT.

- **Backup:** Backup firmware image from DUT to remote host.

- **Method:** Firmware upgrade / backup method.
  - **TFTP:** Using TFTP to upgrade/backup firmware.
  - **HTTP:** Using WEB browser to upgrade/backup firmware.
- **Filename:** Use browser to upgrade firmware, you should select firmware image file on your host PC.

Note	When the system is updated, the default value is upgrade always to Image1.

*Click the **"Apply"** button to save your changes settings.*



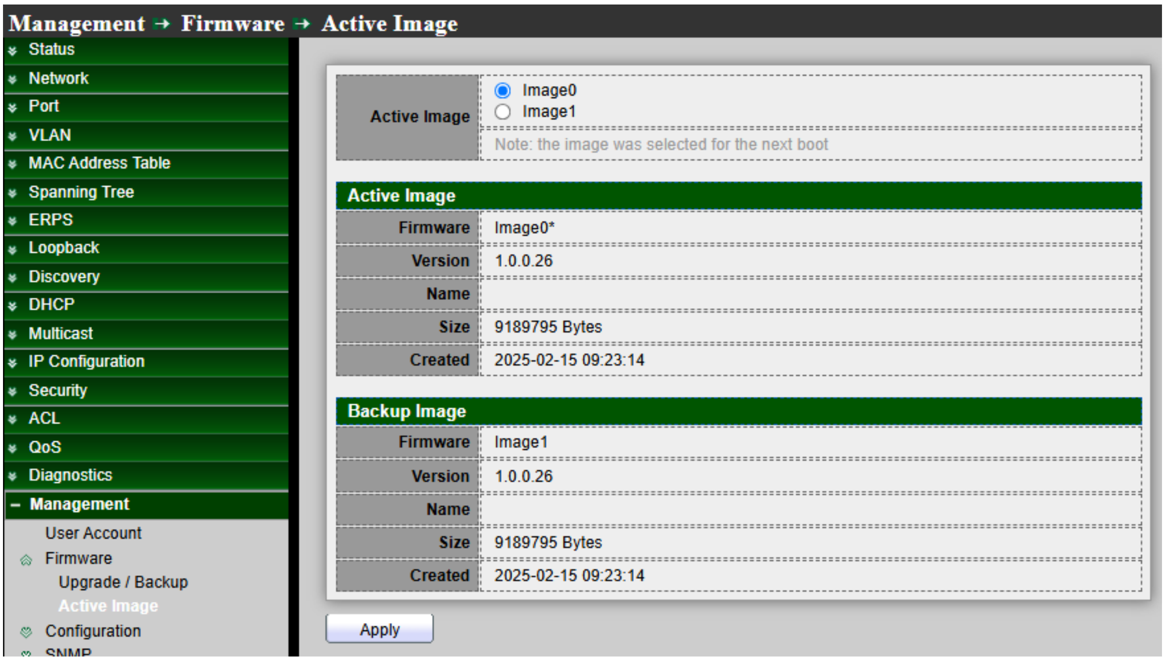
Action	○ Upgrade ● Backup
Method	● TFTP ○ HTTP
Firmware	● Image
Address Type	● Hostname ○ IPv4 ○ IPv6
Server Address	
Filename	

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

*Click the **"Apply"** button to save your changes settings.*

19.2.2 Active Image

This page allows user to select firmware image on next booting and show firmware information on both flash partitions, If the Switch has upload multiple firmware in system then administrator can choose a firmware to do system default start.



Active Image: ● Image0 ○ Image1

Note: the image was selected for the next boot

Active Image

Firmware	Image0*
Version	1.0.0.26
Name	
Size	9189795 Bytes
Created	2025-02-15 09:23:14

Backup Image

Firmware	Image1
Version	1.0.0.26
Name	
Size	9189795 Bytes
Created	2025-02-15 09:23:14

➢ **Active Image:** Select firmware image to use on next booting.

- **Image0:** Select the flash partition 0 for Firmware image0 to active.
- **Image1:** Select the flash partition 1 for Firmware image1 to active.

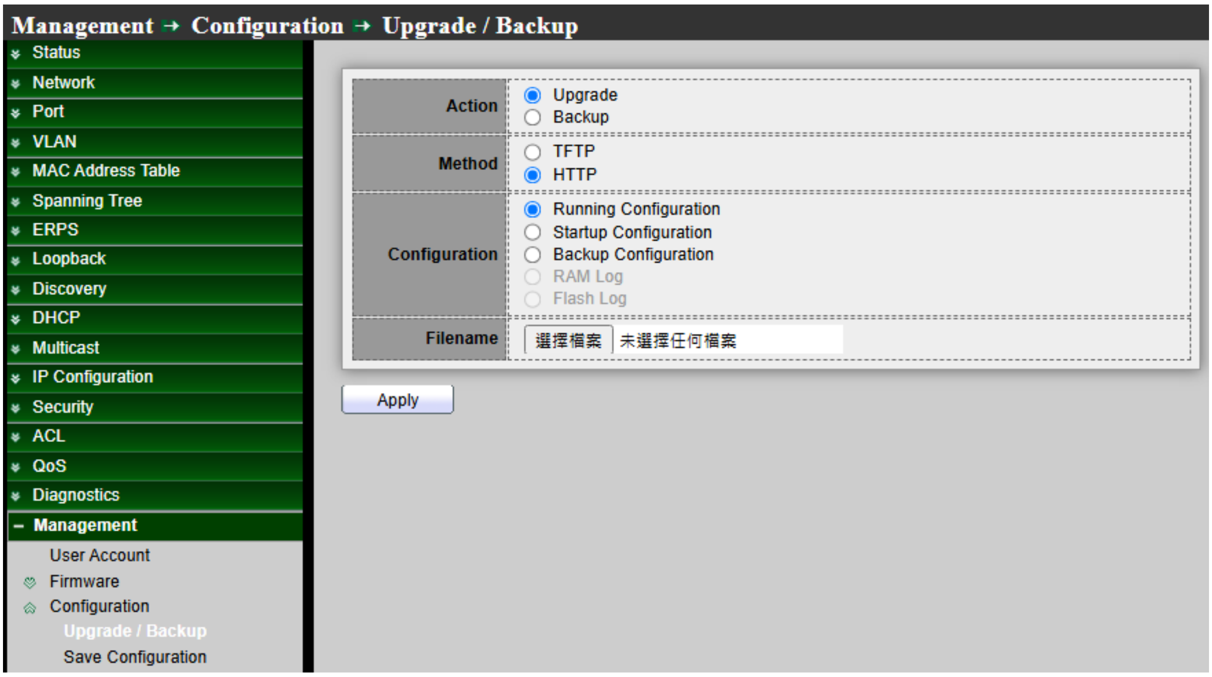
Field	Description
Active Image	• **Firmware:** Firmware image. • **Version:** Firmware version.. • Name: Firmware name. • **Size:** Firmware image size. • **Created:** Firmware image created date.
Backup Image	• **Firmware:** Firmware image. • **Version:** Firmware version.. • Name: Firmware name. • **Size:** Firmware image size. • **Created:** Firmware image created date.

*Click the **"Apply"** button to save your changes settings.*

19.3 Configuration

19.3.1 Upgrade / Backup

Administrator can backup system configuration file to PC or upload configuration file to Switch system, This page allow user to upgrade or backup firmware image through HTTP or TFTP server.



Management → Configuration → Upgrade / Backup

Action	● Upgrade ○ Backup
Method	○ TFTP ● HTTP
Configuration	● Running Configuration ○ Startup Configuration ○ Backup Configuration ○ RAM Log ○ Flash Log
Filename	選擇檔案 未選擇任何檔案

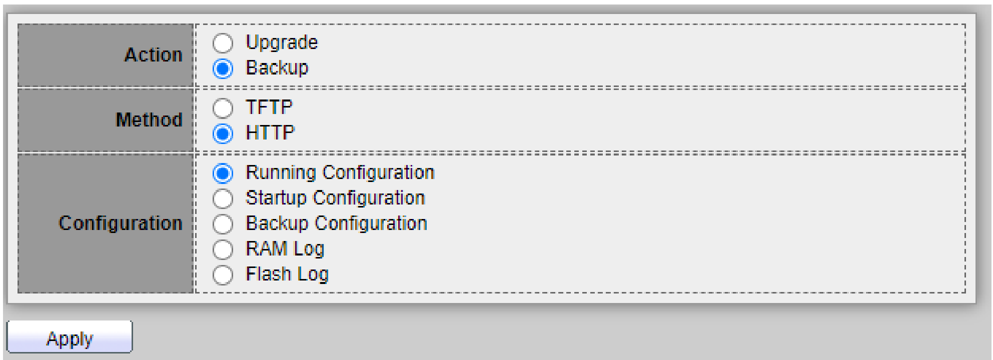
Upgrade Configuration

- **Action:** Configuration operations.
  - **Upgrade:** Upgrade firmware from remote host to DUT.
  - **Backup:** Backup firmware image from DUT to remote host.
- **Method:** Configuration upgrade method.
  - **TFTP:** Using TFTP to upgrade firmware.
  - **HTTP:** Using WEB browser to upgrade firmware.
- Configuration: Configuration Type.
  - **Running Configuration:** Merge to current running configuration file.
  - **Startup Configuration:** Replace startup configuration file.
  - **Backup Configuration:** Replace backup configuration file.
- **Address Type:** Specify TFTP server address type
  - **Hostname:** Use domain name as server address.
  - **IPv4:** Use IPv4 as server address.
  - **IPv6:** Use IPv6 as server address

- **Server Address:** Specify TFTP server address.
- **Filename:** Configuration file name on remote TFTP server.

*Click the **"Apply"** button to save your changes settings.*

Backup Configuration



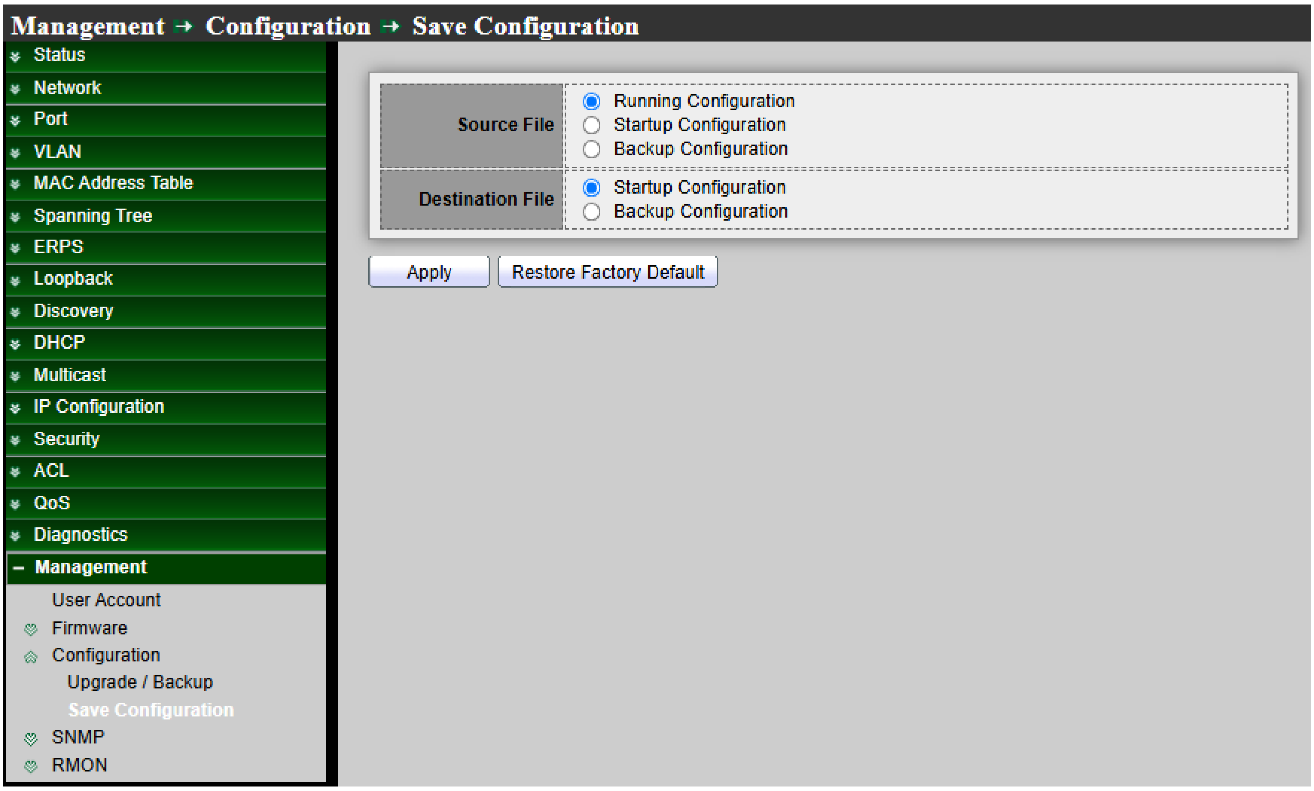
Action	○ Upgrade ● Backup
Method	○ TFTP ● HTTP
Configuration	● Running Configuration ○ Startup Configuration ○ Backup Configuration ○ RAM Log ○ Flash Log

- **Action:** Configuration operations.
  - **Upgrade:** Upgrade firmware from remote host to DUT.
  - **Backup:** Backup firmware image from DUT to remote host.
- **Method:** Configuration backup method.
  - **TFTP:** Using TFTP to backup firmware.
  - **HTTP:** Using WEB browser to backup firmware.
- Configuration: Configuration Type.
  - **Running Configuration:** Backup running configuration file.
  - **Startup Configuration:** Backup start configuration file.
  - **Backup Configuration:** Backup backup configuration file.
  - **RAM Log:** Backup log file stored in RAM.
  - **Flash Log:** Backup log files store in Flash.

*Click the **"Apply"** button to save your changes settings.*

19.3.2 Save Configuration

When administrator to click Apply on any window, changes that you made to the switch configuration settings are stored only in the Running Configuration. To preserve the parameters in the Running Configuration, the Running Configuration must be copied to another configuration type or saved as a file on another device, This page allow user to manage configuration file saved on DUT and click “Restore Factory Default” button to restore factory defaults.



Management → Configuration → Save Configuration

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

Destination File: ● Startup Configuration ○ Backup Configuration

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

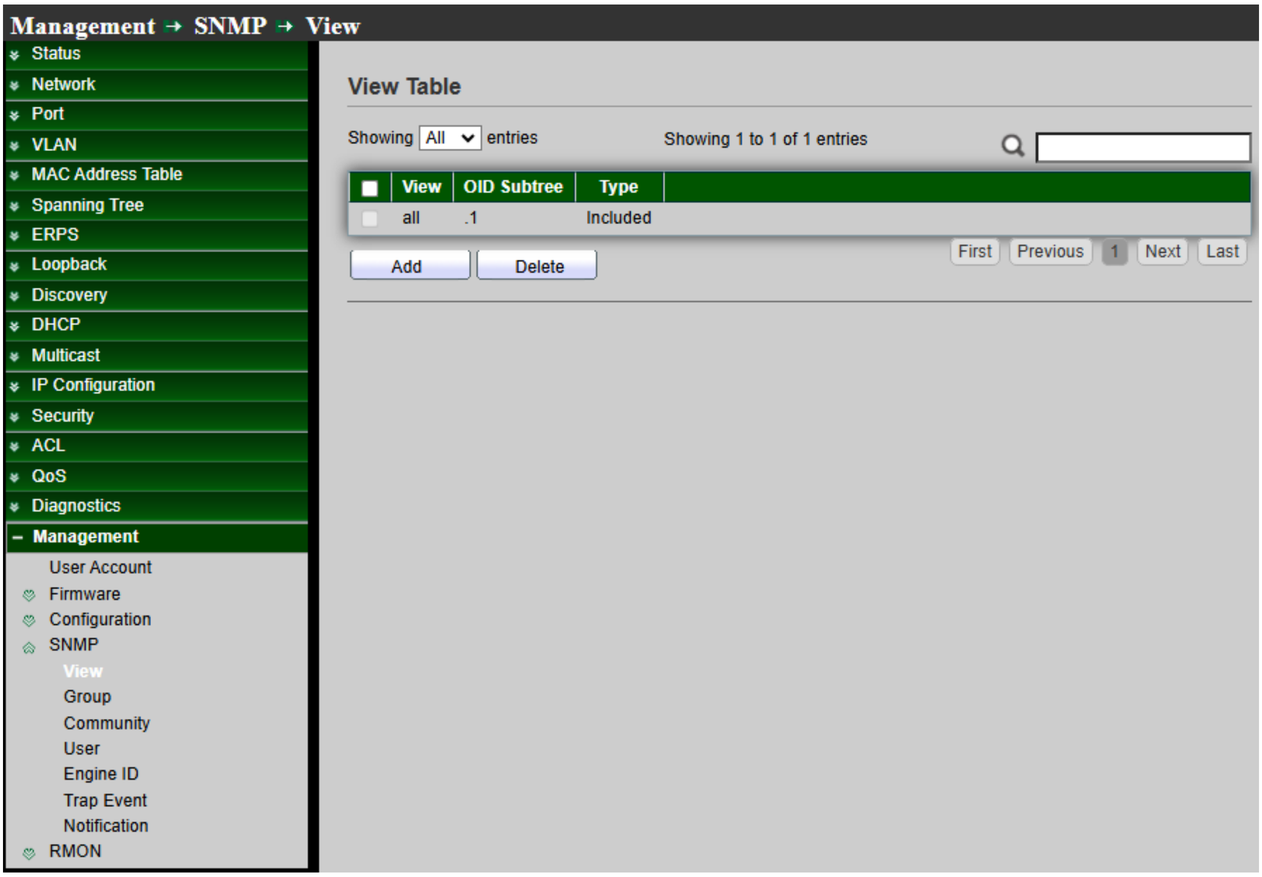
*Click the **“Apply”** button to save your changes or Chick “**Restore Factory Default**” the button to back to factory default setting.*

19.4 SNMP

The SNMP supports SNMP v1, v2, and v3. It also reports system events to trap receivers using the traps defined in the Management Information Base (MIB) that it supports.

19.4.1 View

A view is a user-defined label for a collection of MIB tree subtrees. Each subtree ID is defined by the OID of the root of the relevant subtrees. You can either use well-known names to specify the root of the desired subtree or enter an OID. Setting **“add”** or **“Delete”** to management.



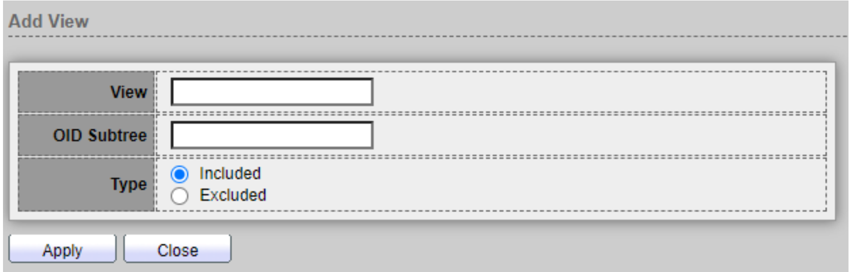
View Table

Showing All entries

Showing 1 to 1 of 1 entries

□	View	OID Subtree	Type
□	all	.1	Included

Field	Description
View	The SNMP view name. Its maximum length is 30 characters.
Subtree OID	Specify the ASN.1 subtree object identifier (OID) to be included or excluded from the SNMP view.
View Type	Include or exclude the selected MIBs in the view.



Add View

View	
OID Subtree	
Type	● Included ○ Excluded

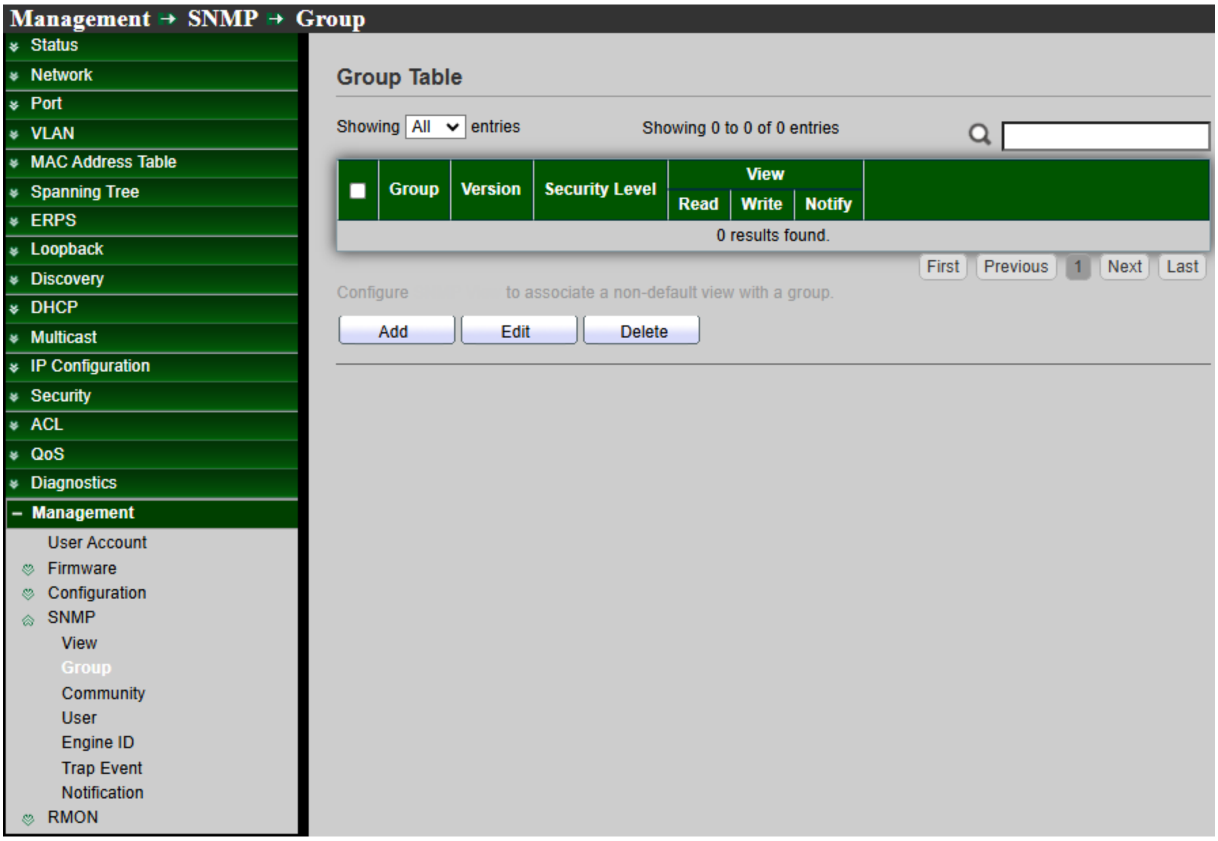
- **View:** Enter a unique view name.
- **Object Subtree:** Select User Defined to manually define an OID, or select an existing OID from the list. All descendent of this node will be included or excluded in the view.
- **Type:**

  Include: Check to include the selected MIBs in this view.

  Excluded: Check to Excluded the selected MIBs in this view.

19.4.2 Group

In SNMPv1 and SNMPv2, a community string is sent along with the SNMP frames. The community string acts as a password to gain access to an SNMP agent. However, neither the frames nor the community string are encrypted. So SNMPv1 and SNMPv2 are not secure. In SNMPv3 can configure Authentication and Privacy is more secure. Setting **“add”** and “Edit” and **“Delete”** function for this management



Group Table

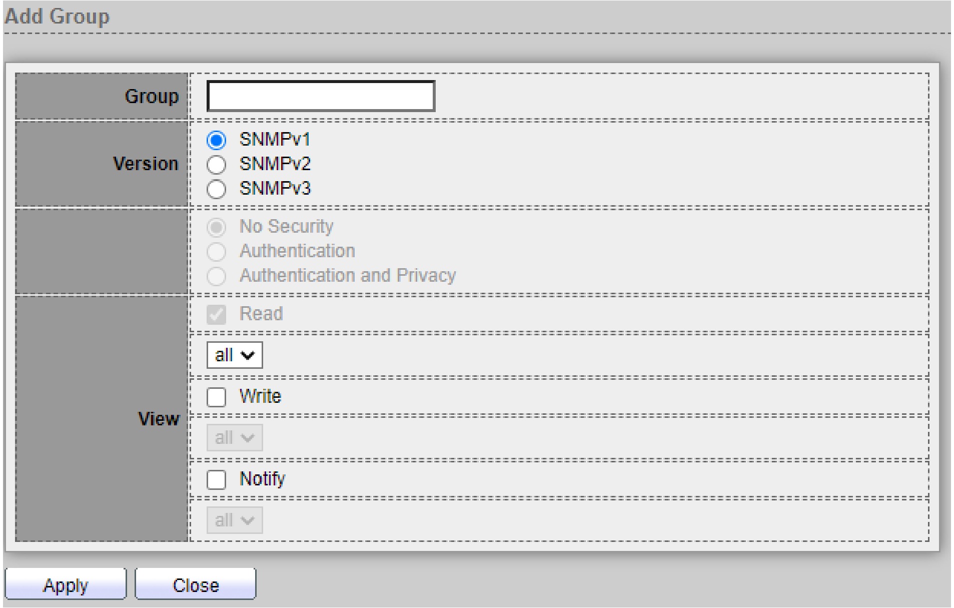
Showing All entries Showing 0 to 0 of 0 entries

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

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

Field	Description
Group	Specify SNMP group name, and the maximum length is 30 characters.

Version	Spedify SNMP version • **SNMPv1:** SNMP Version 1. • **SNMPv2:** Community-based SNMP Version 2c. • **SNMPv3:** User security model SNMP version 3.
Security Level	Specify SNMP security level • **No Security :** Specify that no packet authentication is performed. • **Authentication:** Specify that packet authentication without encryption is performed. • **Authentication and Privacy:** Specify that packet authentication with encryption is performed.
View	Spedify SNMP version • **Read:** Group read view name.. • **Write:** Group write view name. • **Notify:** The view name that sends only traps with contents that is included in SNMP view selected for notification.



Add Group

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

- **Group:** Specify SNMP group name, and the maximum length is 30 characters.
- **Version:** Specify SNMP version.
  - **SNMPv1:** SNMP Version 1.
  - **SNMPv2:** Community-based SNMP Version 2c.
  - **SNMPv3:** User security model SNMP version 3.
- **Security Level:** Specify SNMP security level.

- **No Security :** Specify that no packet authentication is performed.
- **Authentication:** Specify that packet authentication without encryption is performed.
- **Authentication and Privacy:** Specify that packet authentication with entryption is performed.

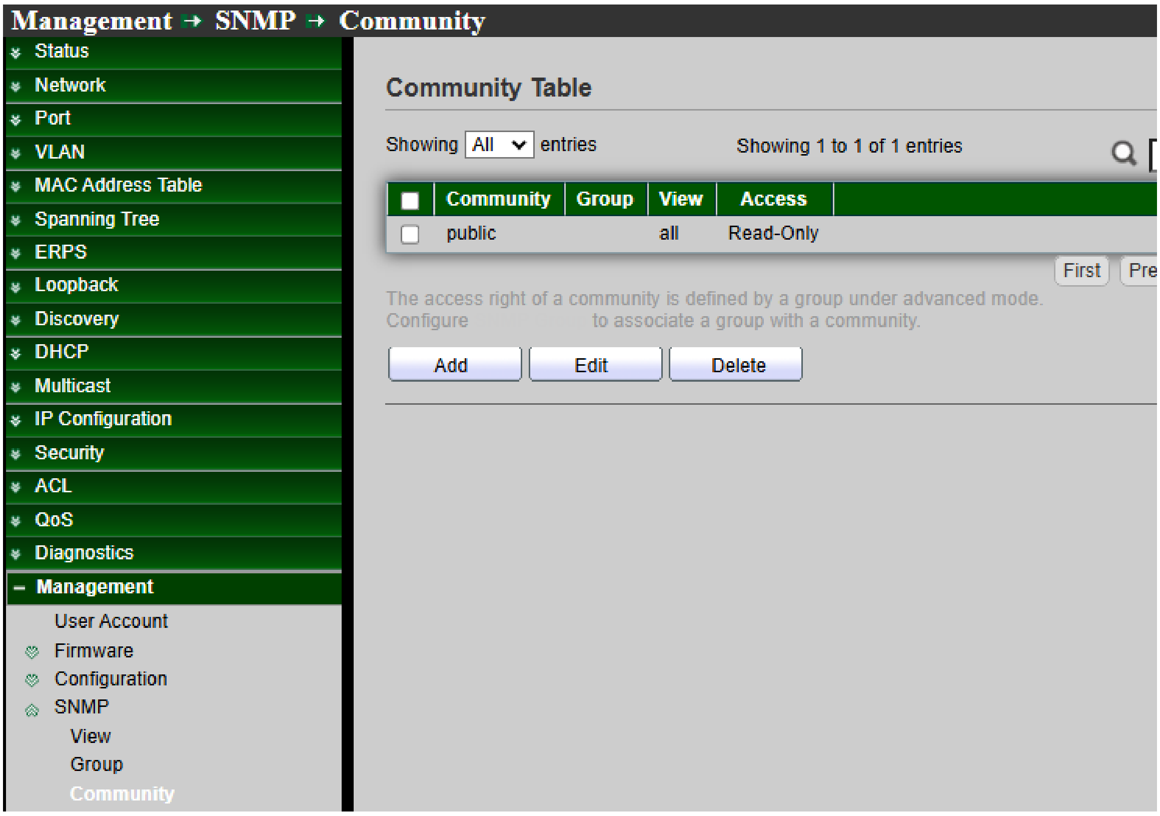
➢ **View:**

- **Read :** Select read view name if Read is checked.
- **Write:** Select write view name, if Write is checked.
- **Notify:** Select notify view name, if Notify is checked.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

19.4.3 Community

Communities are only defined in SNMPv1 and v2 because SNMPv3 works with users instead of communities. The users belong to groups that have access rights assigned to them, Setting **"add"** and "Edit" and **"Delete"** function for this management.



Community Table

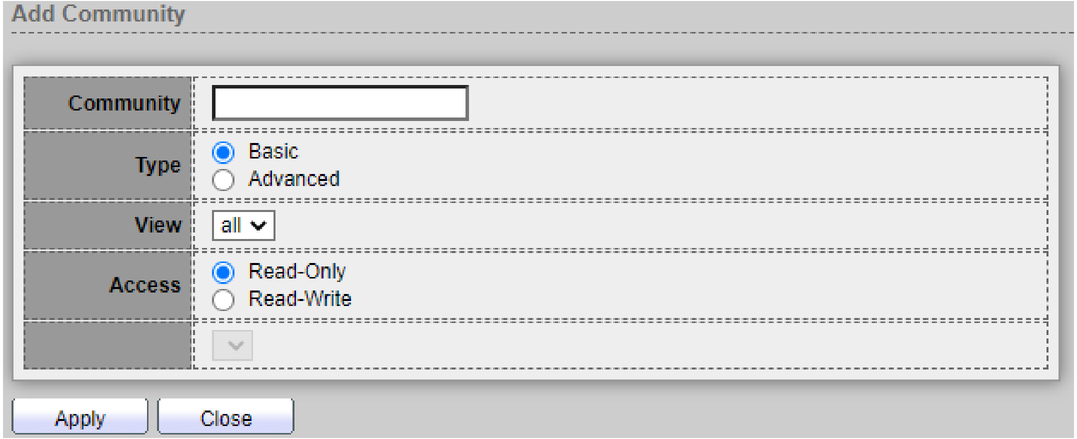
Showing All entries Showing 1 to 1 of 1 entries

□	Community	Group	View	Access
□	public		all	Read-Only

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

Field	Description

Community	The SNMP community name. Its maximum length is 20 characters.
Community	SNMP Community mode. • **Basic:** snmp community specifies view and access right. • **Advanced:** snmp community specifies group.
Group	Specify the SNMP group configured by the command **SNMP group** to define the object available to the community.
View	Specify the SNMP view to define the object available to the community.
Access	SNMP access mode • **Read-Only:** Read only. • **Read-Write:** Read and write.



Add Community

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

- **Community:** The SNMP community name. Its maximum length is 20 characters.
- **Type:** Specify SNMP version.
  - **Basic:** SNMP community specifies view and access right ,The access rights of a community can configure with Read Only or Read Write. In addition, Administrator can restrict the access to the community to only certain MIB objects by selecting a view.
  - **Advanced:** SNMP community specifies group, The access rights of a community are defined by a group. You can configure the group with a specific security model. The access rights of a group are Read, Write, and Notify.
- **View:** Specify the SNMP view to define the object available to the community.
- **Access:** SNMP access mode.
  - **Read Only:** Read only , Management access is restricted to read-only. Changes cannot be made to the community.
  - **Read Write:** Read and write , Management access is read-write. Changes can be made to the switch configuration, but not to the community.

- **Group:** If set Type for specify SNMP version to "Advanced" type, Must be set specify the SNMP group configured by user to define the object available to the community.

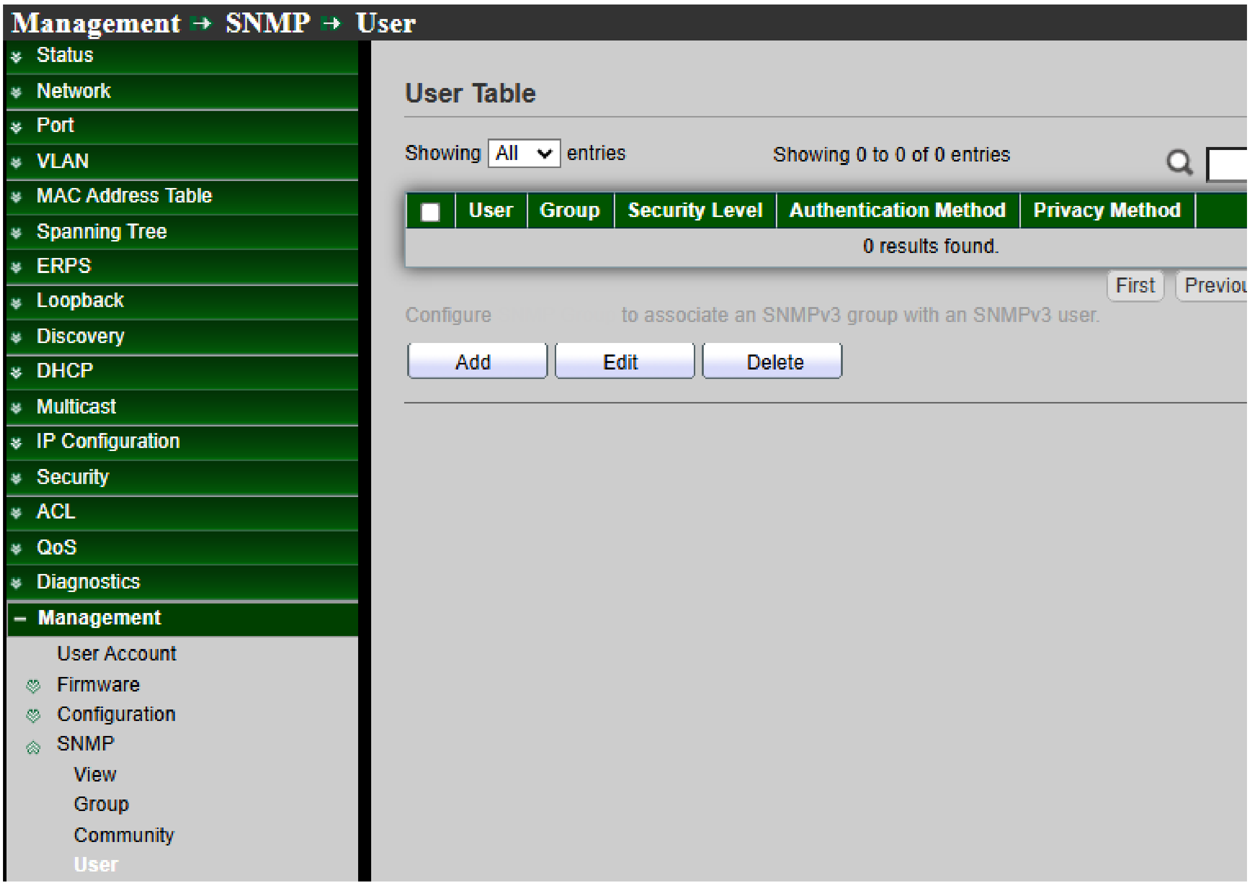
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

19.4.4 User

An SNMP user is defined by the login credentials (username, passwords, and authentication method) and by the context and scope in which it operates by association with a group and an Engine ID. The configured user has the attributes of its group, having the access privileges configured within the associated view.

Groups enable network managers to assign access rights to a group of users, instead of a single user. A user can only be a member of a single group.

Administrator need to create a SNMPv3 user, a SNMPv3 group must be available, Setting **"add"** and "Edit" and **"Delete"** function for this management.



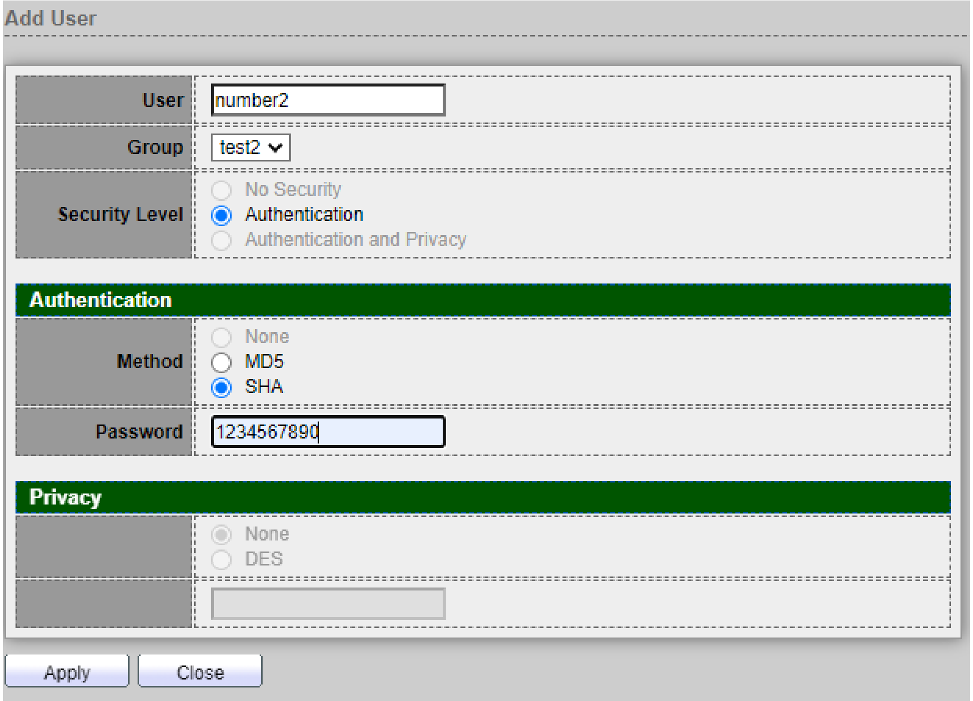
User Table

Showing All entries   Showing 0 to 0 of 0 entries

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

Configure to associate an SNMPv3 group with an SNMPv3 user.

Field	Description
User	Specify the SNMP user name on the host that connects to the SNMP agent. The max character is 30 characters. For the SNMP v1 or v2c, the user name must match the community name
Group	Specify the SNMP group to which the SNMP user belongs.
Security Level	SNMP privilege mode • **No Security :** Specify that no packet authentication is performed. • **Authentication:** Specify that packet authentication without encryption is performed. • **Authentication and Privacy:** Specify that packet authentication with encryption is performed.
Authentication Method	Authentication Protocol which is available when Privilege Mode is **Authentication** or **Authentication and Privacy**. • **None:** No authentication required. • **MD5:** Specify the HMAC-MD5-96 authentication protocol. • **SHA:** Specify the HMAC-SHA-96 authentication protocol.
Privacy Method	Encryption Protocol • **None:** No privacy required. • **DES:** DES gorithm



Add User

User	number2
Group	test2
Security Level	○ No Security ● Authentication ○ Authentication and Privacy

Authentication

Method	○ None ○ MD5 ● SHA
Password	1234567890

Privacy

	● None ○ DES

- **User:** Specify the SNMP user name on the host that connects to the SNMP agent. The max character is 30 characters.
- **Security Level:** SNMP privilege mode.
  - **No Security:** Specify that no packet authentication is performed.
  - **Authentication:** Specify that packet authentication without encryption is performed.
  - **Authentication and Privacy:** Specify that packet authentication with encryption is performed.

Authentication

- **Method:** Authentication Protocol which is available when Privilege Mode is Authentication or Authentication and Privacy**.**
  - **None:** No authentication required.
  - **MD5:** Specify the HMAC-MD5-96 authentication protocol.
  - **SHA:** Specify the HMAC-SHA-96 authentication protocol.
- **Password:** The authentication password, The number of character range is 8 to 32 characters.

Privacy

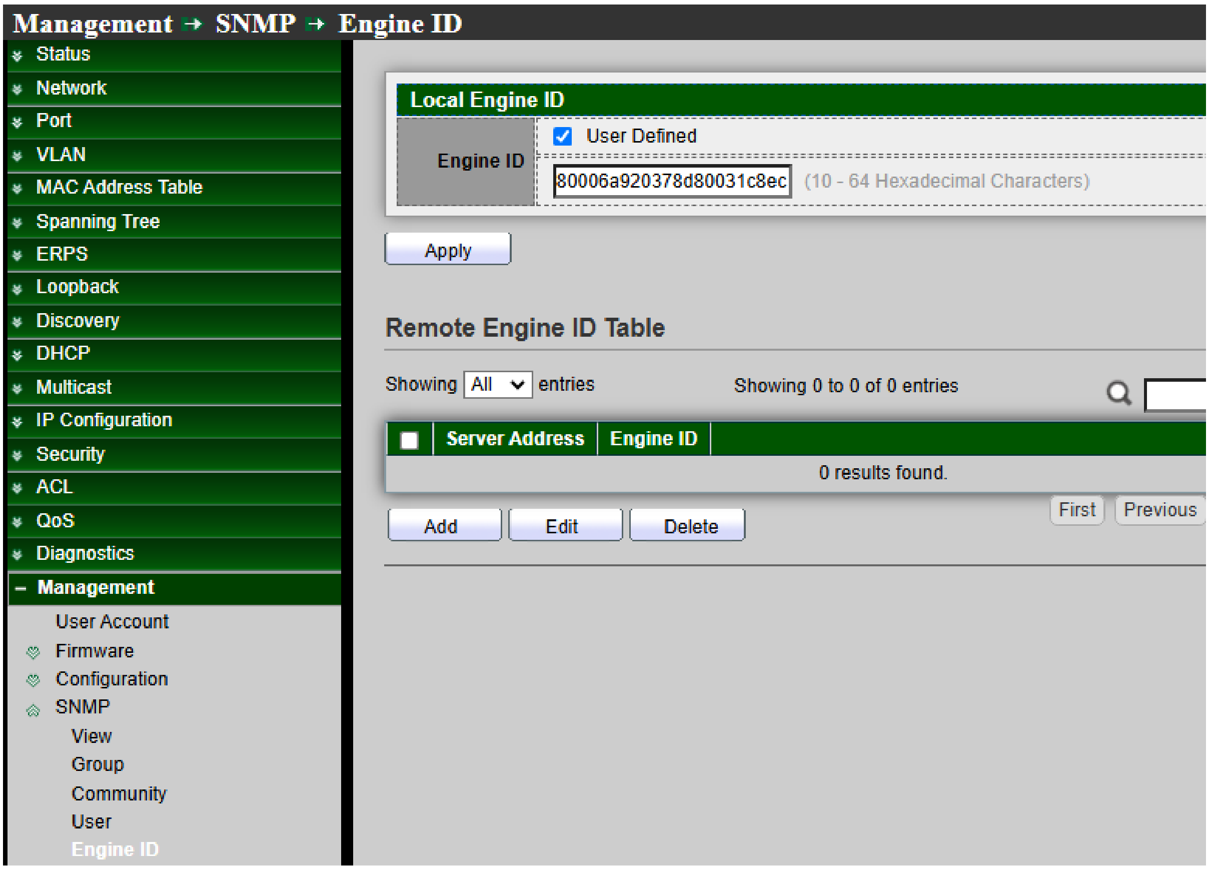
- **Method:** Encryption Protocol**.**
  - **None:** No privacy required.
  - **DES:** DES algorithm.
  - **SHA:** Specify the HMAC-SHA-96 authentication protocol.
- **Password:** The privacy password, The number of character range is 8 to 64 characters.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

19.4.5 Engine ID

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

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



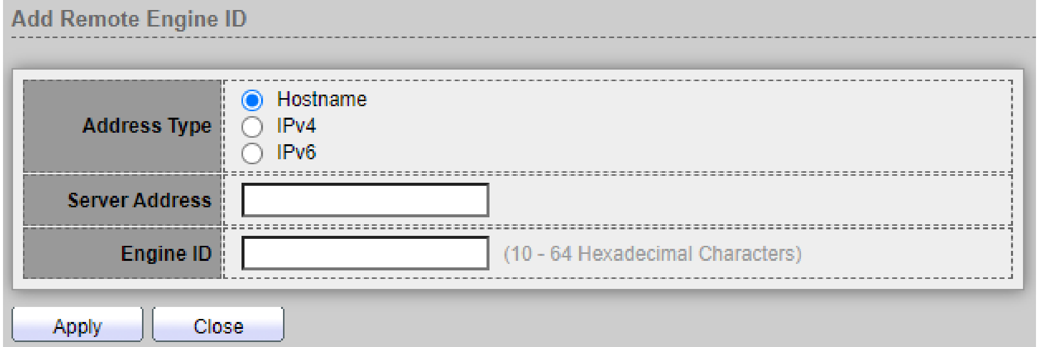
Local Engine ID

- **Engine ID:** If checked "User Defined", the local engine ID is configure by user, else use the default Engine ID which is made up of MAC and Enterprise ID**,** The user defined engine ID is range 10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.

*Click the **"Apply"** button to save your changes settings.*

Remote Engine ID Table

Field	Description
Server Address	Remote host.
Engine ID	Specify Remote SNMP engine ID. The engine ID is range10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.



Add Remote Engine ID

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

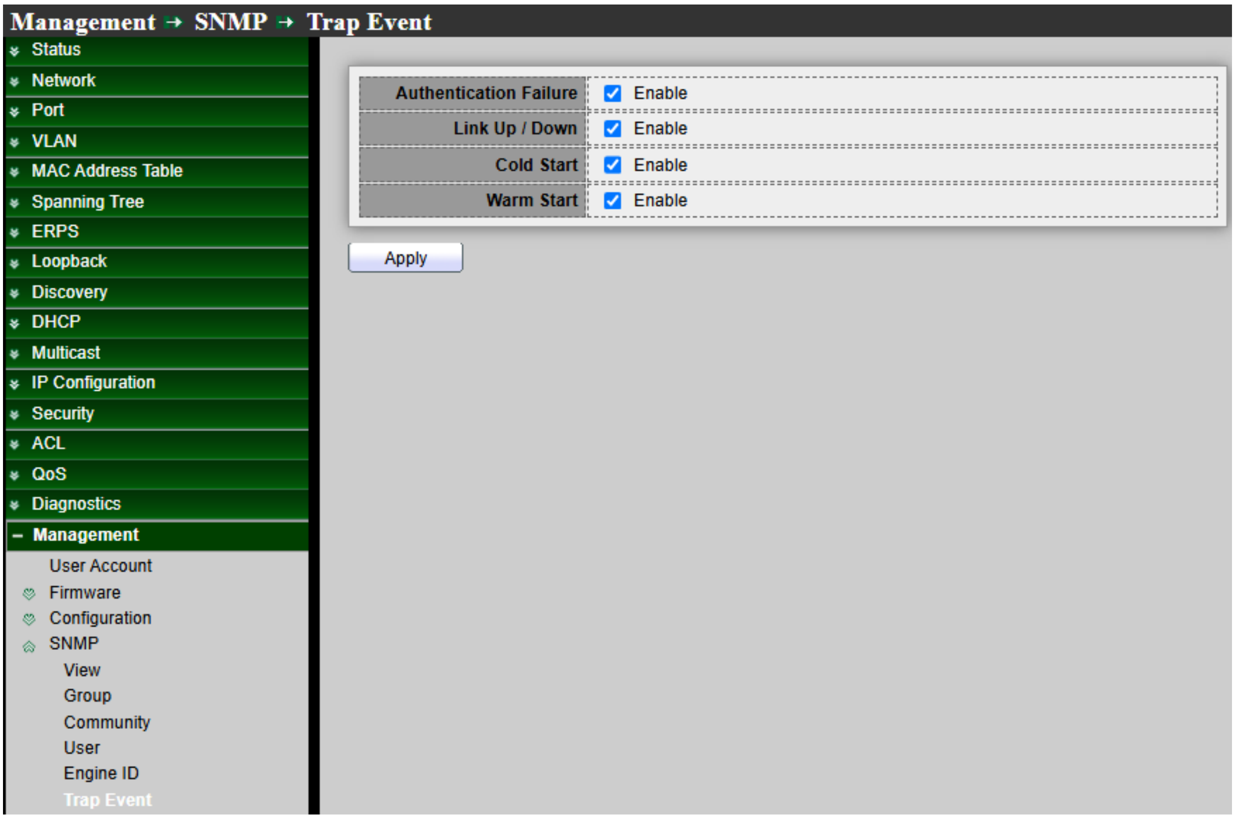
- **Address Type:** Remote host address type for Hostname/IPv4/IPv6.
- **Server Address:** Remote host.
- **Engine ID:** Specify Remote SNMP engine ID. The engine ID is range10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

19.4.6 Trap Event

Administrator can choose SNMP Trap Event Type to monitor

Trap messages are generated to report system events, as defined in RFC 1215. The system can generate traps defined in the MIB that it supports.



Management → SNMP → Trap Event

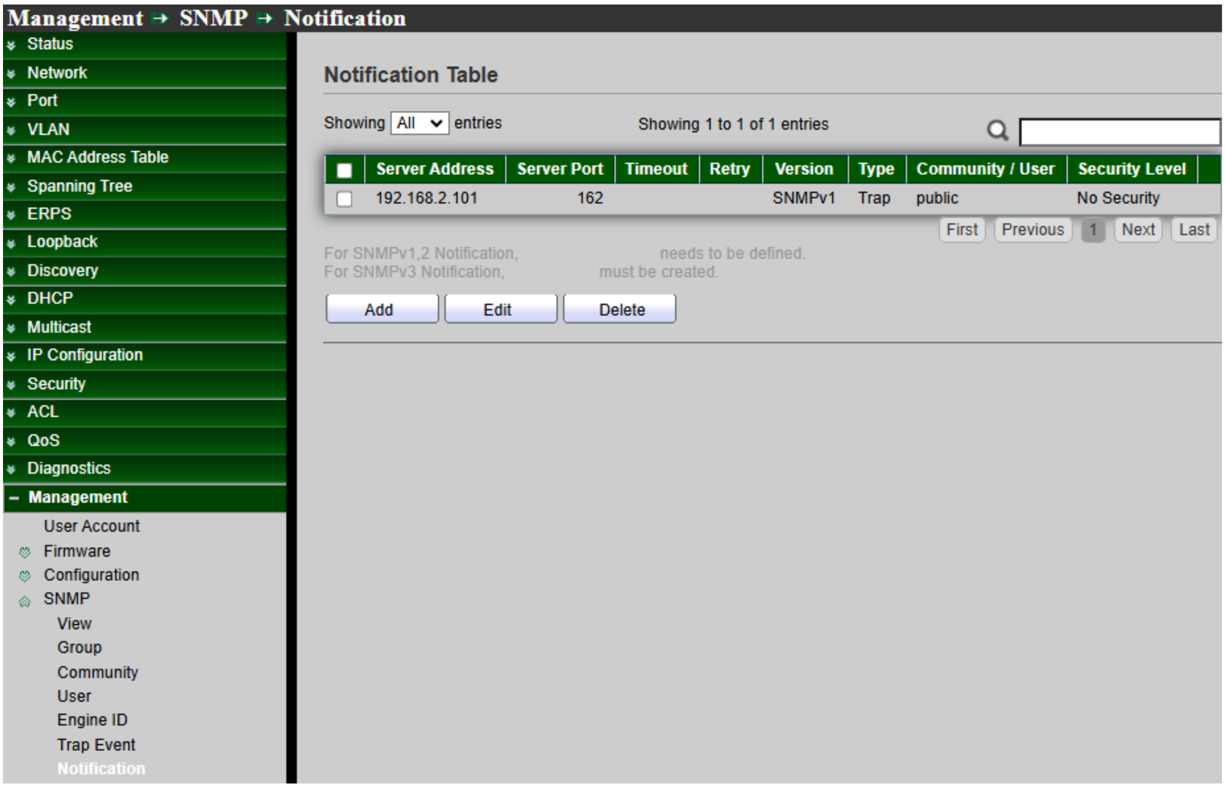
Authentication Failure	☑ Enable
Link Up / Down	☑ Enable
Cold Start	☑ Enable
Warm Start	☑ Enable

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

*Click the **"Apply"** button to save your changes settings.*

19.4.7 Notification

Notification is network nodes where the trap messages are sent by the switch. A list of notification recipients are defined as the targets of trap messages. A trap receiver entry contains the IP address of the node and the SNMP credentials corresponding to the version that will be included in the trap message. When an event arises that requires a trap message to be sent, it is sent to every node listed in the Notification Recipient Table, , Setting **"add"** and "Edit" and **"Delete"** function for this management.



Notification Table

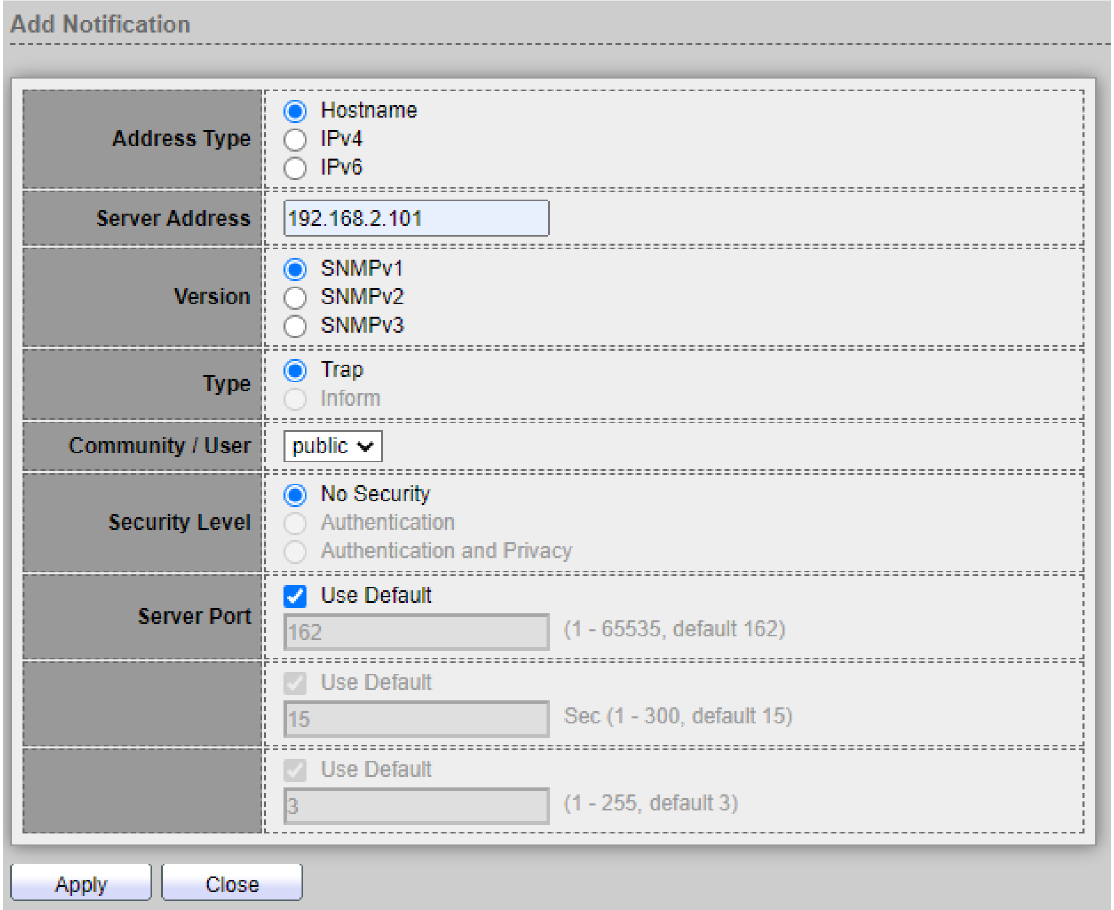
Showing All entries　　Showing 1 to 1 of 1 entries

□	Server Address	Server Port	Timeout	Retry	Version	Type	Community / User	Security Level
□	192.168.2.101	162			SNMPv1	Trap	public	No Security

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

Field	Description
Server Address	IP address or the hostname of the SNMP trap recipients.
Server Port	Recipients server UDP port number
Timeout	Specify the SNMP informs timeout
Retry	Specify the retry counter of the SNMP informs.
Version	Specify SNMP notification version • **SNMPv1:** SNMP Version 1 notification. • **SNMPv2:** SNMP Version 2 notification. • **SNMPv3:** SNMP Version 3 notification.
Type	Notification Type • **Trap:** Send SNMP traps to the host. • **Inform:** Send SNMP informs to the host.
Community/User	SNMP community/user name for notification. If version is SNMPv3 the name is user name, else is community name
Security Level	SNMP trap packet security level • **No Security:** Specify that no packet authentication is performed.

- **Authentication:** Specify that packet authentication without encryption is performed.
- **Authentication and Privacy:** Specify that packet authentication with encryption is performed.



Add Notification

Address Type	● Hostname ○ IPv4 ○ IPv6
Server Address	192.168.2.101
Version	● SNMPv1 ○ SNMPv2 ○ SNMPv3
Type	● Trap ○ Inform
Community / User	public
Security Level	● No Security ○ Authentication ○ Authentication and Privacy
Server Port	☑ Use Default 162 (1 - 65535, default 162)
	☑ Use Default 15 Sec (1 - 300, default 15)
	☑ Use Default 3 (1 - 255, default 3)

➢ **Address Type:** Remote host address type for Hostname/IPv4/IPv6.

➢ **Server Address:** IP address or the hostname of the SNMP trap recipients.

➢ **Version:** Specify SNMP notification version.

- **SNMPv1:** SNMP Version 1 notification.
- **SNMPv2:** SNMP Version 2 notification.
- **SNMPv3:** SNMP Version 3 notification.

➢ **Type:** Notification Type**.**

- **Trap:** Send SNMP traps to the host.
- **Inform:** Send SNMP informs to the host.(version 1 have no inform).

➢ **Community/User:** SNMP community/user name for notification. If version is SNMPv3 the name is user name, else is community name.

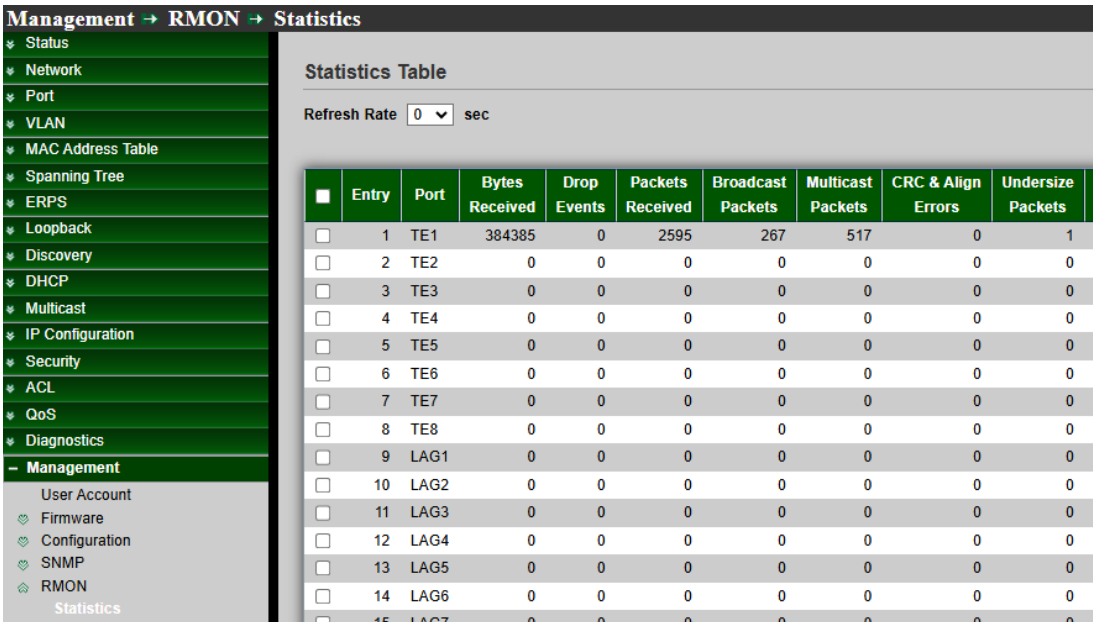
- **Security Level:** SNMP notification packet security level, the security level must less than or equal to the community/user name**.**
  - **No Security:** Specify that no packet authentication is performed.
  - **Authentication:** Specify that packet authentication without encryption is performed.
  - **Authentication and Privacy:** Specify that packet authentication with encryption is performed.
- **Server Port:** Recipients server UDP port number, if “use default” checked the value is 162, else user configure.
- **Timeout:** Specify the SNMP informs timeout, if “use default” checked the value is 15, else user configure.
- **Retry:** Specify the SNMP informs retry count, if “use default” checked the value is 3, else user configure.

*Click the **“Apply”** button to save your changes or **“Close”** the button to close settings.*

19.5 RMON

19.5.1 Statistics

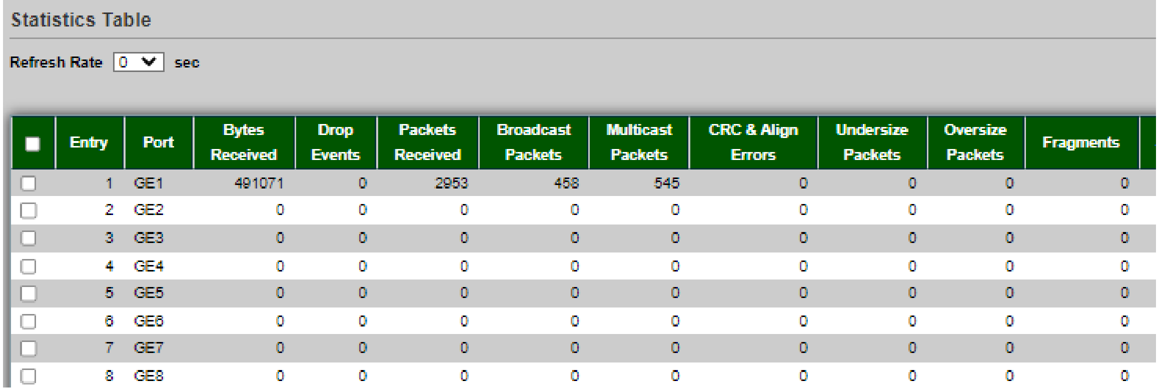
The page displays traffic statistics per interface. The refresh rate of the information can be selected. This page is useful for analyzing the amount of traffic that is both sent and received and its dispersion (Unicast, Multicast, and Broadcast) *Click the **“Clear”** button to clear this page or click the **“Refresh”** button to refresh and chick the **“View”** button to view the page .*



Statistics Table

Refresh Rate 0 sec

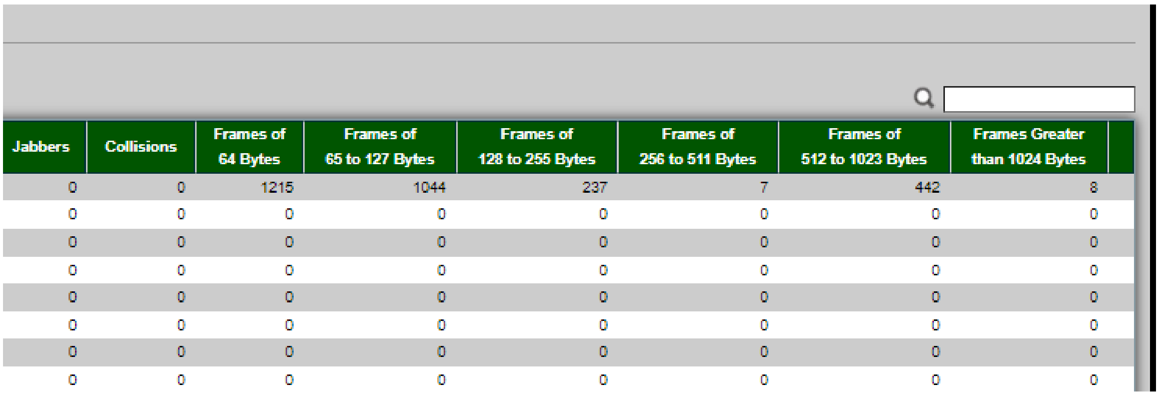
□	Entry	Port	Bytes Received	Drop Events	Packets Received	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets
□	1	TE1	384385	0	2595	267	517	0	1
□	2	TE2	0	0	0	0	0	0	0
□	3	TE3	0	0	0	0	0	0	0
□	4	TE4	0	0	0	0	0	0	0
□	5	TE5	0	0	0	0	0	0	0
□	6	TE6	0	0	0	0	0	0	0
□	7	TE7	0	0	0	0	0	0	0
□	8	TE8	0	0	0	0	0	0	0
□	9	LAG1	0	0	0	0	0	0	0
□	10	LAG2	0	0	0	0	0	0	0
□	11	LAG3	0	0	0	0	0	0	0
□	12	LAG4	0	0	0	0	0	0	0
□	13	LAG5	0	0	0	0	0	0	0
□	14	LAG6	0	0	0	0	0	0	0
□	15	LAG7	0	0	0	0	0	0	0



Statistics Table

Refresh Rate 0 sec

□	Entry	Port	Bytes Received	Drop Events	Packets Received	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets	Oversize Packets	Fragments
□	1	GE1	491071	0	2953	458	545	0	0	0	0
□	2	GE2	0	0	0	0	0	0	0	0	0
□	3	GE3	0	0	0	0	0	0	0	0	0
□	4	GE4	0	0	0	0	0	0	0	0	0
□	5	GE5	0	0	0	0	0	0	0	0	0
□	6	GE6	0	0	0	0	0	0	0	0	0
□	7	GE7	0	0	0	0	0	0	0	0	0
□	8	GE8	0	0	0	0	0	0	0	0	0



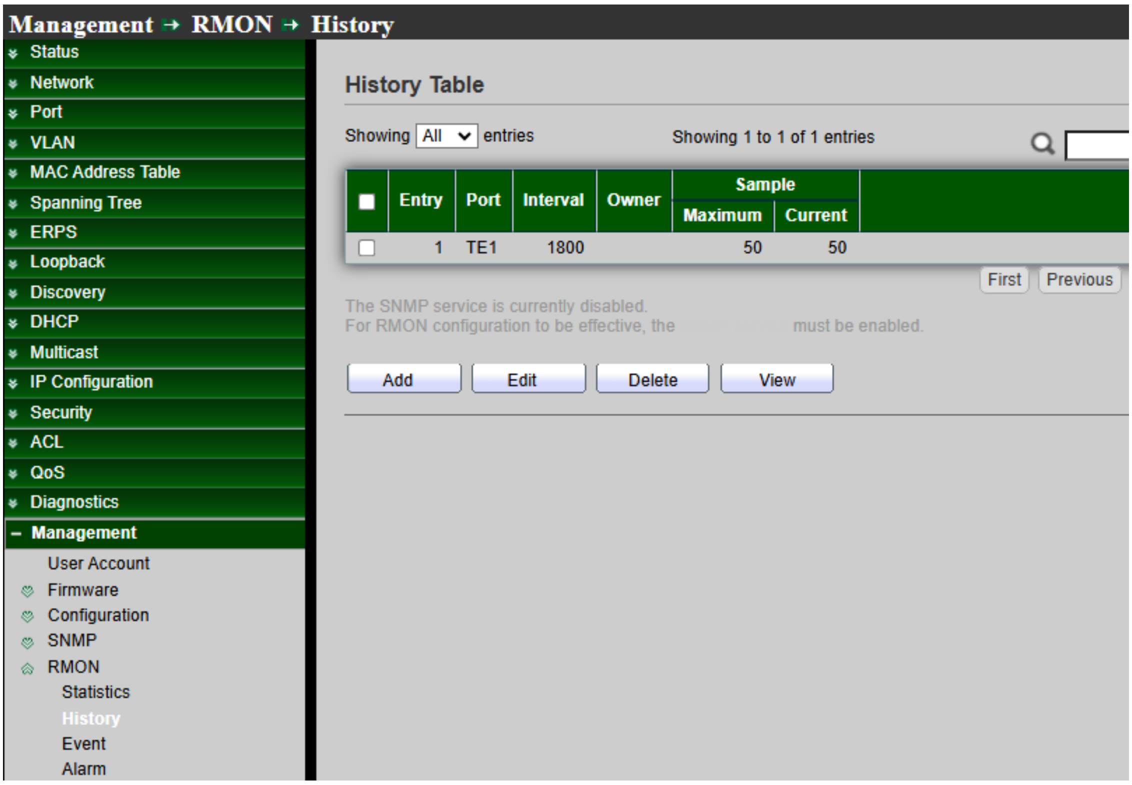
Jabbers	Collisions	Frames of 64 Bytes	Frames of 65 to 127 Bytes	Frames of 128 to 255 Bytes	Frames of 256 to 511 Bytes	Frames of 512 to 1023 Bytes	Frames Greater than 1024 Bytes
0	0	1215	1044	237	7	442	8
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Field	Description
Port	The port for the RMON statistics.
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. This number does not include Multicast packets.
Multicast Packets	Number of good Multicast packets received.
CRC & Align Errors	Number of CRC and Align errors that have occurred.
Undersize Packages	Number of undersized packets (less than 64 octets) received.

Oversize Packages	Number of oversized packets (over 1518 octets) received.
Fragments	Number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received.
Jabbers	Number of received packets that were longer than 1632 octets. This number excludes frame bits, but includes FCS octets that had either a bad FCS (Frame Check Sequence) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. A Jabber packet is defined as an Ethernet frame that satisfies the following criteria: • Packet data length is greater than MRU. • Packet has an invalid CRC. • RX error event has not been detected.
Collision	Number of collisions received. If Jumbo Frames are enabled, the threshold of Jabber Frames is raised to the maximum size of Jumbo Frames.
Frames of 64 Bytes	Number of frames, containing 64 bytes that were received.
Frames of 65 to 127 Bytes	Number of frames, containing 65 to 127 bytes that were received.
Frames of 128 to 255 Bytes	Number of frames, containing 128 to 255 bytes that were received.
Frames of 256 to 511 Bytes	Number of frames, containing 256 to 511 bytes that were received.
Frames of 512 to 1023 Bytes	Number of frames, containing 512 to 1023 bytes that were received.
FramesGreater than 1024 Bytes	Number of frames, containing 1024 to 1518 bytes that were received

19.5.2 History

Use the History Control Table page to define the sampling frequency, amount of samples to store, and the interface from where to gather the data. After the data is sampled and stored, it appears on the History Table page that can be viewed by clicking History Table, , Setting **“add”** and “Edit” and **“Delete”** and “View” function for this management.



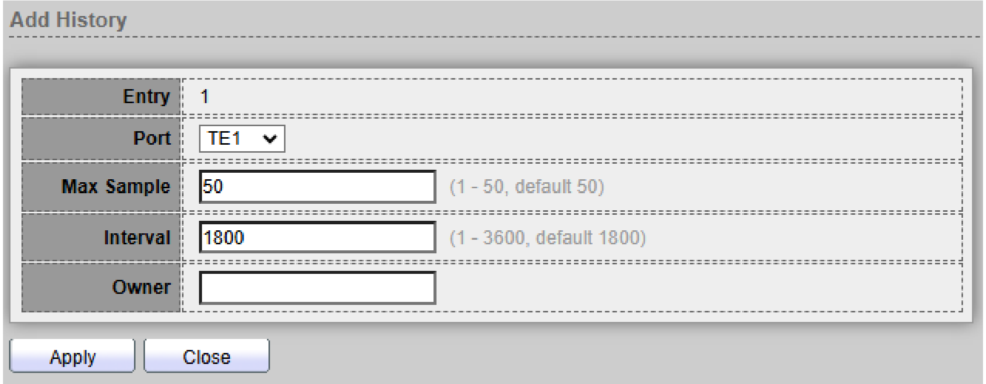
History Table

Showing All entries Showing 1 to 1 of 1 entries

□	Entry	Port	Interval	Owner	Sample	
					Maximum	Current
□	1	TE1	1800		50	50

The SNMP service is currently disabled.
For RMON configuration to be effective, the must be enabled.

Field	Description
Port	The port for the RMON history.
Interval	The number of seconds for each sample.
Owner	The owner name of event (0~31 characters).
Sample	The maximum number of buckets. • **Maximum :** The maximum number of buckets. • **Current:** The current number of buckets.



Add History

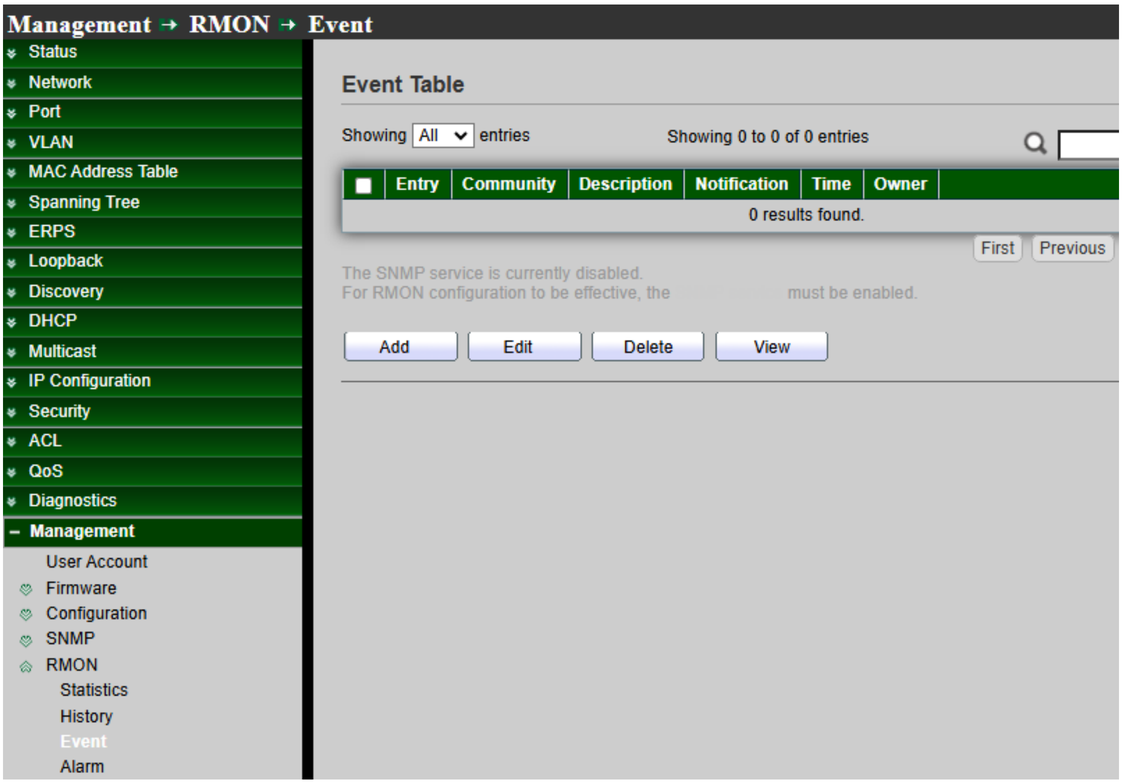
Entry	1
Port	TE1
Max Sample	50 (1 - 50, default 50)
Interval	1800 (1 - 3600, default 1800)
Owner	

- **Port:** Select ports for the configure.
- **Max Sample:** Specify the maximum number of buckets.
- **Interval:** Enter the time in seconds that samples were collected from the interface, Specify the number of seconds for each sample
- **Owner:** Enter the RMON station or user that requested the RMON information, Specify the owner name of event (0~31 characters).

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

19.5.3 Event

Events page to configure events that are actions performed when an alarm is generated (alarms are defined on the Alarms page). An event can be any combination of logs and traps. If the action includes logging of the events, they are displayed on the Event Log Table page, Setting **"add"** and "Edit" and **"Delete"** and "View" function for this management.



Management → RMON → Event

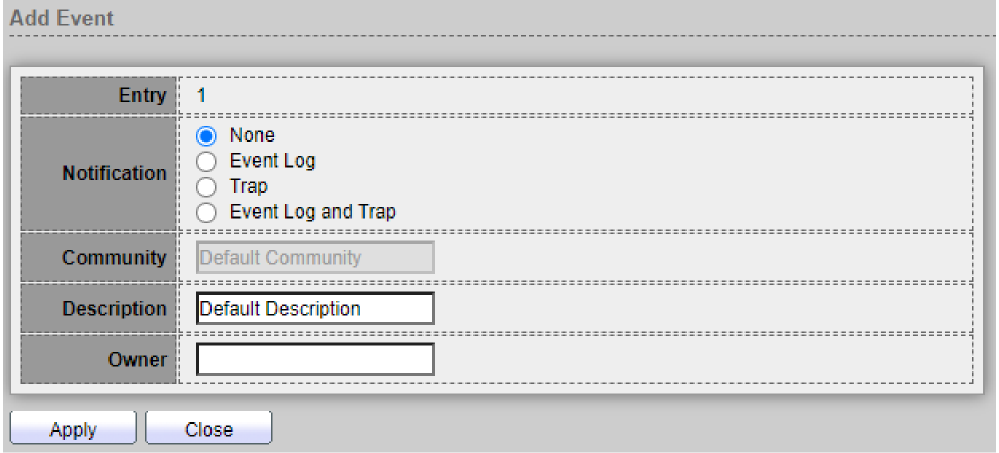
Event Table

Showing All entries Showing 0 to 0 of 0 entries

□	Entry	Community	Description	Notification	Time	Owner
0 results found.						

The SNMP service is currently disabled.
For RMON configuration to be effective, the must be enabled.

Field	Description
Entry	The entry of event.
Community	The specified community.
Description	The description for the event.
Notification	The notification type for the event : None/Event Log/Trap/Event Log and Trap.
Time	The number of seconds for each sample.
Owner	The owner name of event (0~31 characters).


Add Event

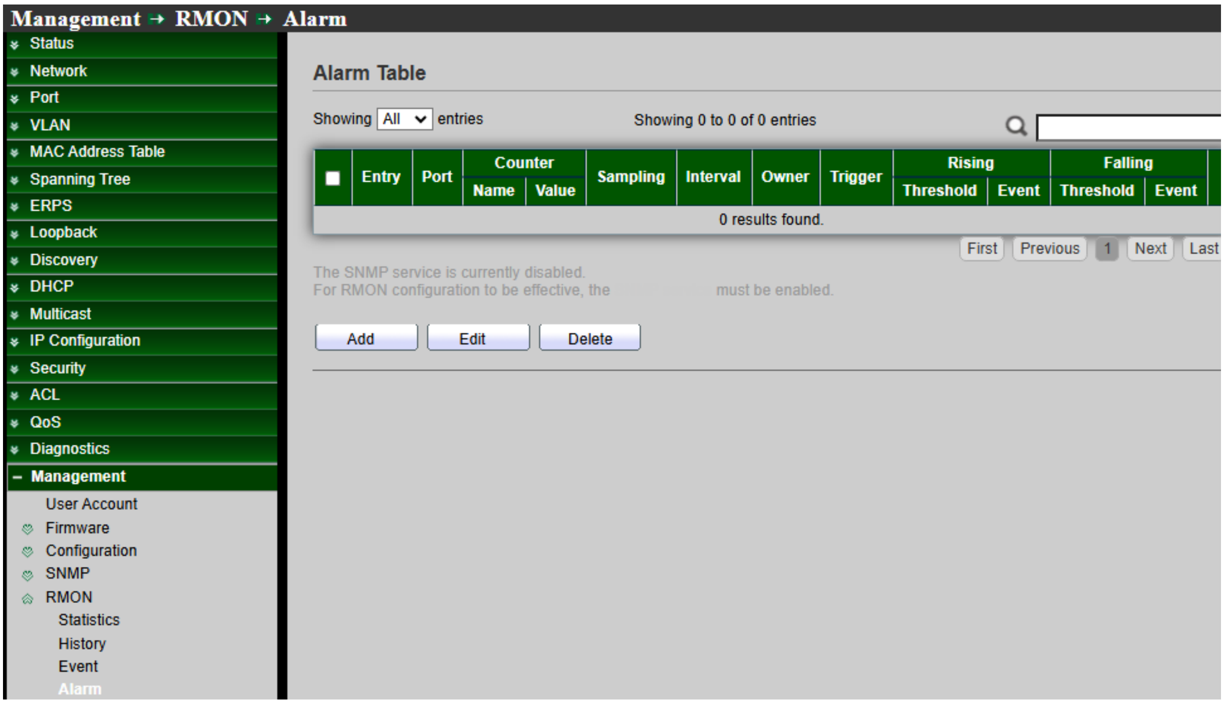
Entry	1
Notification	● None ○ Event Log ○ Trap ○ Event Log and Trap
Community	Default Community
Description	Default Description
Owner	

- **Entry:** Display the entry corresponding to the event.
- **Notification:** Specify the notification type for the event, and the possible value are.
  - **None:** Nothing for notification.
  - **Event Log:** Logging the event in the RMON Event Log table.
  - **Trap:** Send a SNMP trap.
  - **Event Log and Trap:** Logging the event and send the SNMP trap
- **Community:** Specify the SNMP community when the notification type is specified as “Trap” and “Event Log and Trap”.
- **Description:** Specify the description for the event.
- **Owner:** Specify owner for the event.

*Click the **“Apply”** button to save your changes or **“Close”** the button to close settings.*

19.5.4 Alarm

RMON alarms provide a mechanism for setting thresholds and sampling intervals to generate exception events on any counter or any other SNMP object counter maintained by the agent. Both the rising and falling thresholds must be configured in the alarm. After a rising threshold is crossed, no rising events are generated until the companion falling threshold is crossed. After a falling alarm is issued, the next alarm is issued when a rising threshold is crossed, Setting **“add”** and “Edit” and **“Delete”** function for this management.



Management → RMON → Alarm

Alarm Table

Showing All entries Showing 0 to 0 of 0 entries

□	Entry	Port	Counter		Sampling	Interval	Owner	Trigger	Rising		Falling	
			Name	Value					Threshold	Event	Threshold	Event
0 results found.												

The SNMP service is currently disabled.
For RMON configuration to be effective, the [illegible] must be enabled.

Field	Description
Port	The port configuration for the RMON alarm.
Counter	The counter for sampling • **DropEvents (Drop Event)**: Total number of events received in which the packets were dropped. • **Octes (Received Bytes)**: Number of Octets. • **Pkts (Received Packets):** Number of packets. • **BroadcastPkts (Broadcast Packets Received)**: Broadcast packets. • **MulticastPkts (Multicast Packets Received)**: Multicast packets. • **CRCAlignError (CRC and Align Error)**: CRC alignment error. • **UndersizePkts (Undersize Packets)**: Number of undersized packets. • **OversizePkts (Oversize Packets)**: Number of oversized packets. • **Fragments (Fragments)**: Total number of packet fragment. • **Jabbers (Jabbers)**: Total number of packet jabber. • **Collisions (Collisions)**: Collision. • **Pkts64Octetes (Frames of 64 Bytes)**: Number of packets size 64 octets. • **Pkts65to127Octetes (Frames of 65 to 127 Bytes)**: Number of packets size 65 to 127 octets. • **Pkts128to255Octetes (Frames of 128 to 255 Bytes)**: Number of

	packets size 128 to 255 octets. • **Pkts256to511Octetes (Frames of 256 to 511 Bytes)**: Number of packets size 256 to 511 octets. • **Pkts512to1023Octetes (Frames of 512 to 1023 Bytes)**: Number of packets size 512 to 1023 octets. • **Pkts1024to1518Octets (Frames Greater than 1024 Bytes)**: Number of packets size 1024 to 1518 octets.
Version	The sampling type including: • **Absolute:** The selected variable value is compared directly with the thresholds at the end of the sampling interval • **Delta:** The selected variable value of the last sample is subtracted from the current value and the difference is compared with the thresholds.
Interval	The number of seconds for each sample.
Owner	The owner for the alarm entry.
Trigger	The type of event triggering.
Rising Threshold	The threshold for firing rising event.
Rising Event	The rising event when alarm was fired.
Falling Threshold	The threshold for firing falling event.
Falling Event	The falling event when alarm was fired.