CERIO Corporation

CS-2424G-24P_A2

PoE CS-2000 Series - 24 Port 10/100/1000M Gigabit Web Managed PoE+ Switch with 4 SFP Ports (400Watt Power)

User Manual

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 8
1.1 Front Panel 8
1.2 Rear Panel Layout 8
2. Software Configuration 8
2.1 Example of Segment: (Windows OS) 9
2.2 System login username and password information 12
3. System Status 13
3.1 Device Information 13
3.2 Logging Message 14
3.3 Port 15
3.3.1 Statistics 15
3.3.2 Error Disabled 17
3.3.3 Bandwidth Utilization 17
3.4 Link Aggregation 18
3.5 MAC Address Table 19
4. Network 19
4.1 IP Address 19
4.2 System Time 21
5. Port 22
5.1 Port setting 22
5.2 Error Disabled 23
5.3 Link Aggregation setup 24
5.3.1 Group Configuration 24
5.3.2 Port Setting 25
5.3.3 LACP 26
5.4 EEE 27
5.5 Jumbo Frame 27
6. PoE 28
6.1 Global Setting 28
6.2 Priority Setting 28
6.3 Power Limit 29
6.4 Power Show 29
6.5 PD Alive Check 30
7. VLAN 31
7.1 Create VLAN 31
7.2 VLAN Configuration 32
7.3 Membership 33

7.4 Port Setting 34
7.5 Voice VLAN 35
7.5.1 Property 35
7.5.2 Voice OUI 36
7.6 MAC VLAN 36
7.7 GVRP 37
7.7.1 Property 38
7.7.2 Member ship 39
8. MAC Address Table 41
8.1 Dynamic Address 41
8.2 Static Address 41
8.3 Filtering Address 42
9. Spanning Tree 42
9.1 Property 42
9.2 Port Setting 44
9.3 MST Instance 45
9.4 MST Port Setting 46
9.5 Statistics 47
10. Discovery(LLDP) 48
10.1 Property 48
10.2 Port Setting 49
10.3 Packet View 50
10.4 Local Information 52
10.5 Neighbor 55
10.6 Statistics 56
11. Multicast 57
11.1 General 57
11.1.1 Property 57
11.1.2 Group Address 57
11.1.3 Router Port 58
11.1.4 Forward All 59
11.1.5 Filtering Profile 60
11.1.6 Filtering Binding 60
11.2 IGMP Snooping 61
11.2.1 Property 61
11.2.2 Querier 63
11.2.3 Statistics 63

11.3 MLD Snooping 64
11.3.1 Property 64
11.3.2 Statistics 66
11.4 MVR 66
11.4.1 Property 67
11.4.2 Port Setting 67
11.4.3 Group Address 68
12. Security 69
12.1 RADIUS 69
12.2 TACACS+ 71
12.3 AAA 72
12.3.1 Method List 72
12.3.2 Login Authentication 73
12.4 Management Access 74
12.4.1 Management VLAN 74
12.4.2 Management Service 74
12.4.3 Management ACL 75
12.4.4 Management ACE 76
12.5 Port Security 77
12.6 Protected Port 78
12.7 Storm Control 78
12.8 DoS 80
12.8.1 Property 80
12.8.2 Port Setting 81
12.9 Dynamic ARP Inspection 81
12.9.1 Property 81
12.9.2 Statistics 83
12.10 DHCP Snooping 84
12.10.1 Property 84
12.10.2 Statistics 85
12.10.3 Option82 Property 85
12.10.4 Option82 Circuit ID 86
12.11 IP Source Guard 87
12.11.1 Port Setting 87
12.11.2 IMPV Binding 88
12.11.3 Save Databases 88
13. ACL 89

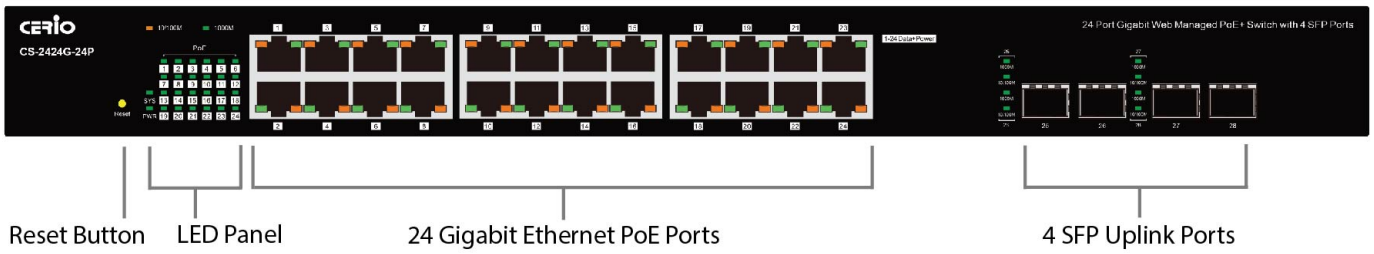
13.1 MAC ACL 89
13.2 MAC ACE 90
13.3 IPv4 ACL 91
13.4 IPv4 ACE 92
13.5 IPv6 ACL 94
13.6 IPv6 ACE 94
13.7 ACL Binding 96
14. QoS 97
14.1 Property 97
14.2 Queue Scheduling 98
14.3 CoS Mapping 99
14.4 DSCP Mapping 100
14.5 IP Precedence to Queue Mapping 101
14.6 Rate Limit 101
15. Diagnostics 102
15.1 Logging 102
15.2 Mirroring 103
15.3 Ping 104
15.4 Traceroute 105
15.5 Copper Test 105
15.6 Fiber Module 106
16. Management 106
16.1 User Account 106
16.2 Firmware 107
16.2.1 Upgrade / Backup 107
16.2.2 Active Image 107
16.3 Configuration 108
16.3.1 Upgrade / Backup 108
16.3.2 Save Configuration 108
16.4 SNMP 109
16.4.1 View 109
16.4.2 Group 110
16.4.3 Community 110
16.4.4 User 111
16.4.5 Engine ID 112
16.4.6 Trap Event 112
16.4.7 Notification 113

16.5 RMON 114
16.5.1 Statistics 114
16.5.2 History 114
16.5.3 Event 115
16.5.4 Alarm 115
16.6 Time Range 116

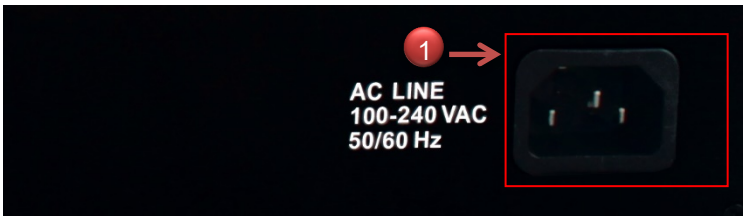
1. Exterior

1.1 Front Panel

Status LED lights for 24 Port 10/100/1000Mps with 4 SFP Port



1.2 Rear Panel Layout



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

2. Software Configuration

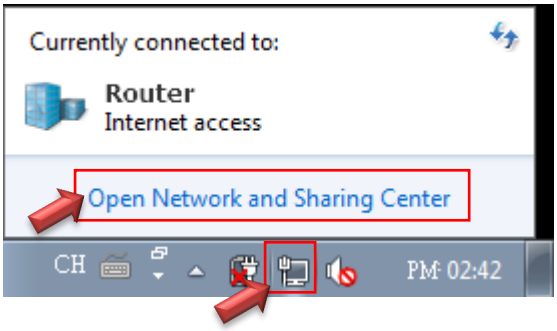
CS-2424G-24P_A2 supports web-based configuration. Upon the completion of hardware installation, **CS-2424G-24P_A2** can be configured through a PC/NB by using its web browser such as Internet Explorer 6.0 or later.

Set the IP segment of the administrator's computer to be in the same range as **CS-2424G-24P_A2** for accessing the system. Do not duplicate the IP Address used here with IP Address of **CS-2424G-24P_A2** or any other device within the network. ***Please refer to the following steps***

2.1 Example of Segment: (Windows OS)

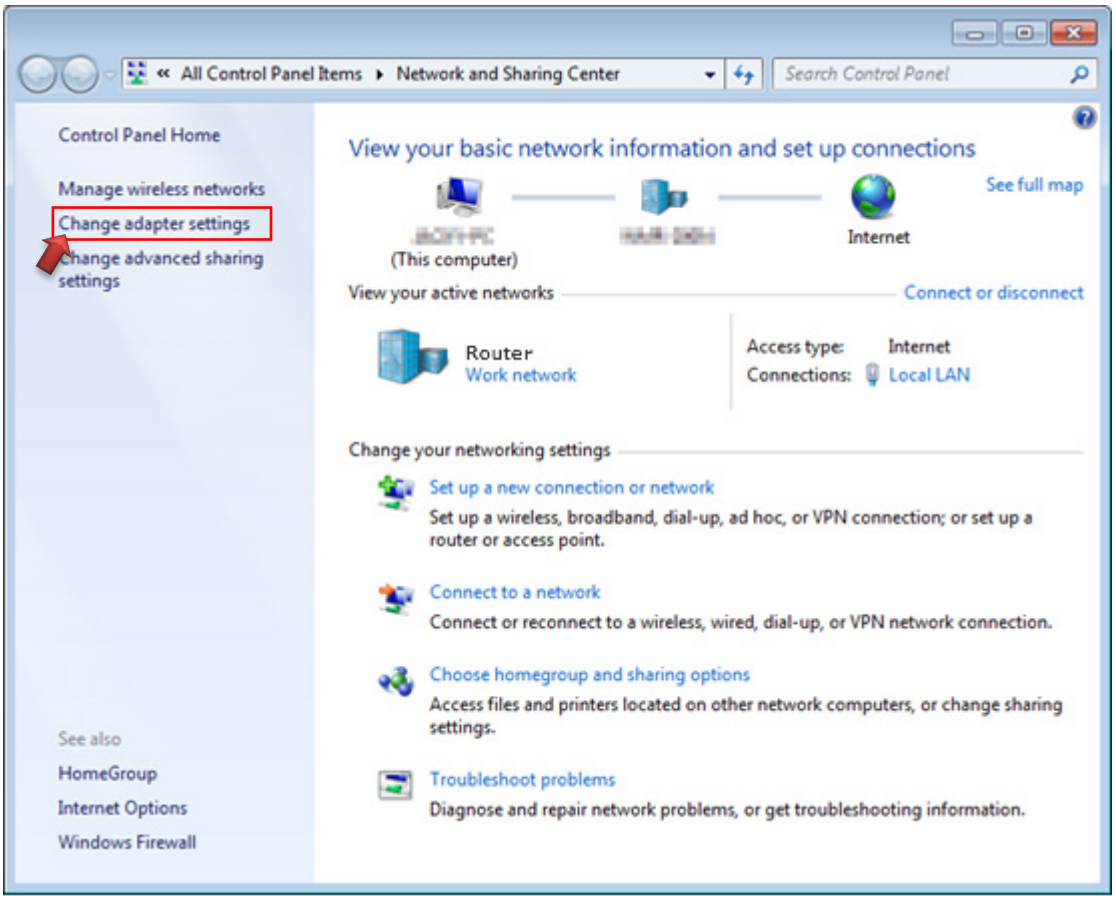
Step 1 :

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



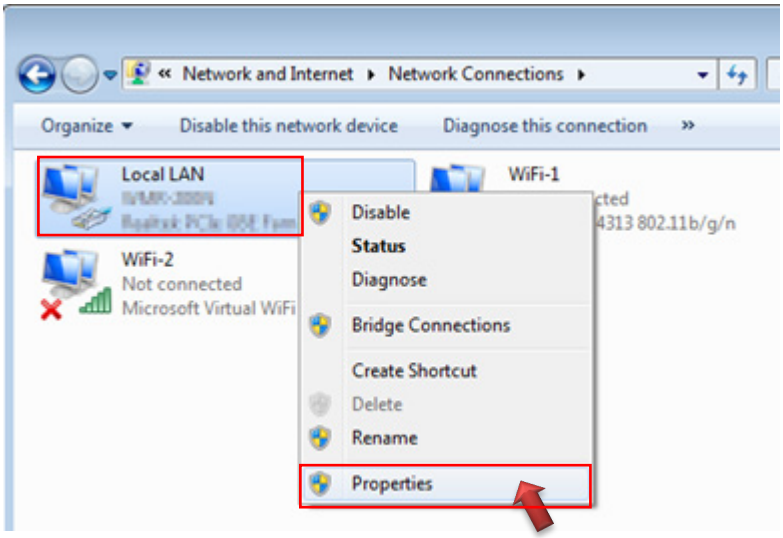
Step 2 :

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



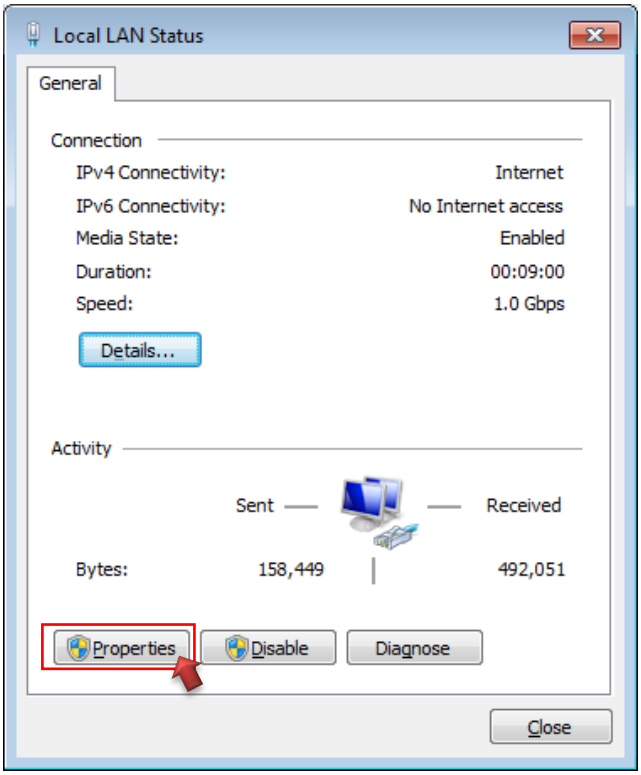
Step 3 :

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



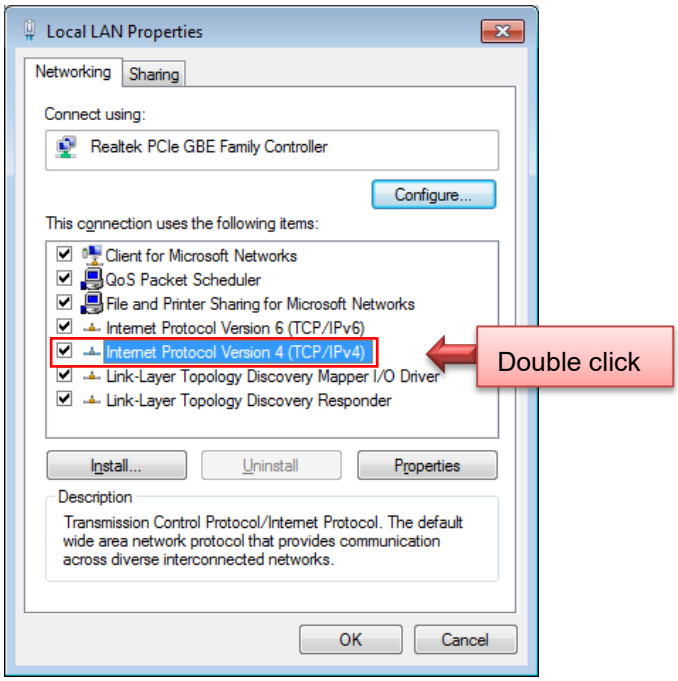
Step 4 :

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



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



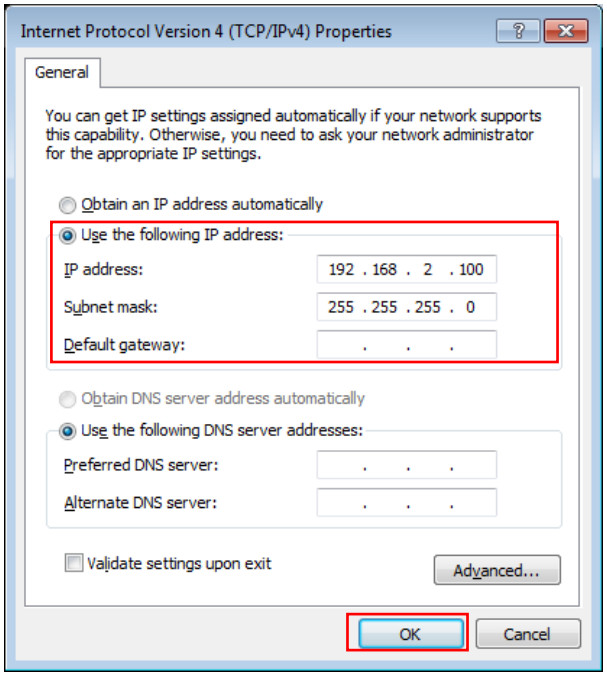
Step 6 :

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



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.

System login Overview page will appear after successful login.

2.2 System login username and password information

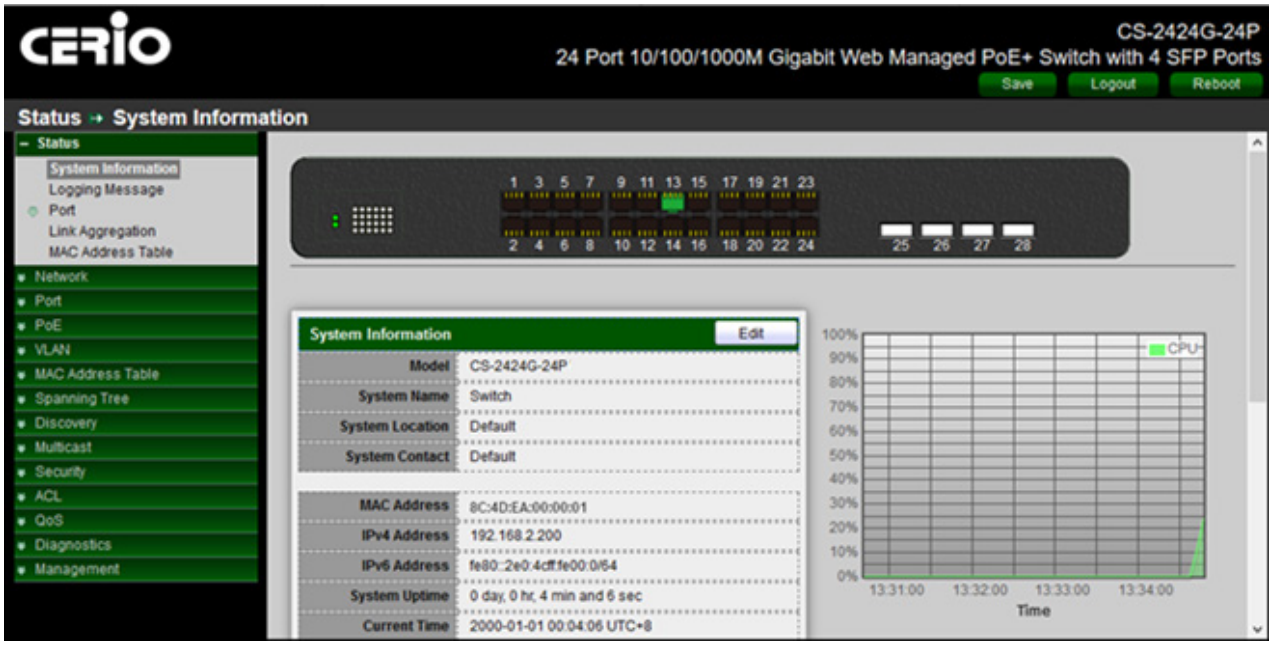
The **CS-2424G-24P_A2** web switch default IP is 192.168.2.200

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

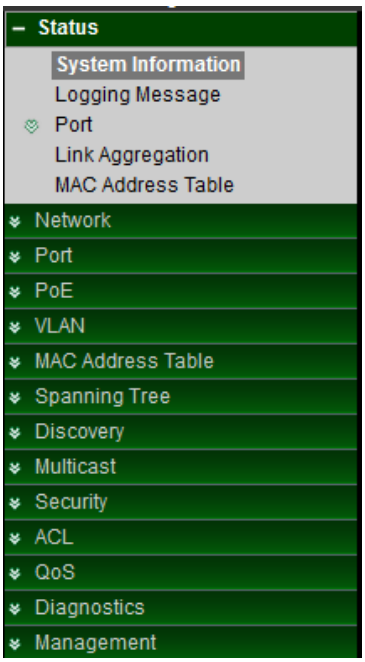
After the authentication procedure, the home page will show up. Select one of the configurations by clicking the icon.

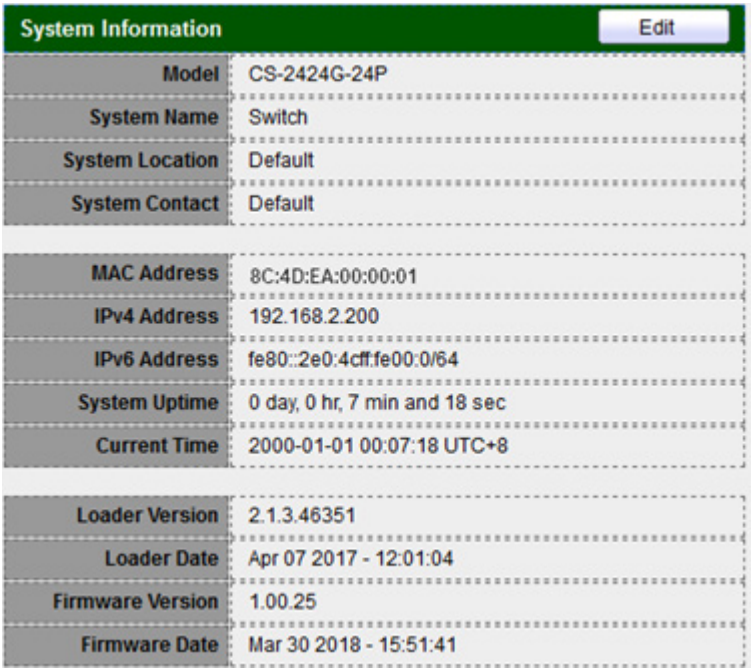


3. System Status

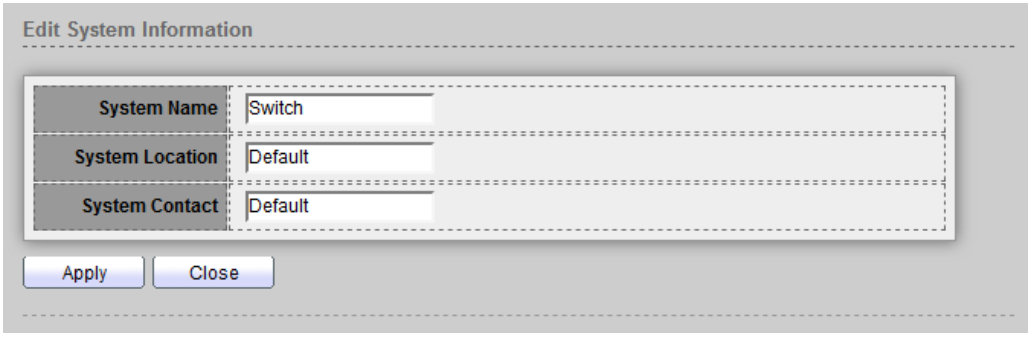
3.1 Device Information

This administrator can check device system information in the “Device Information” tab





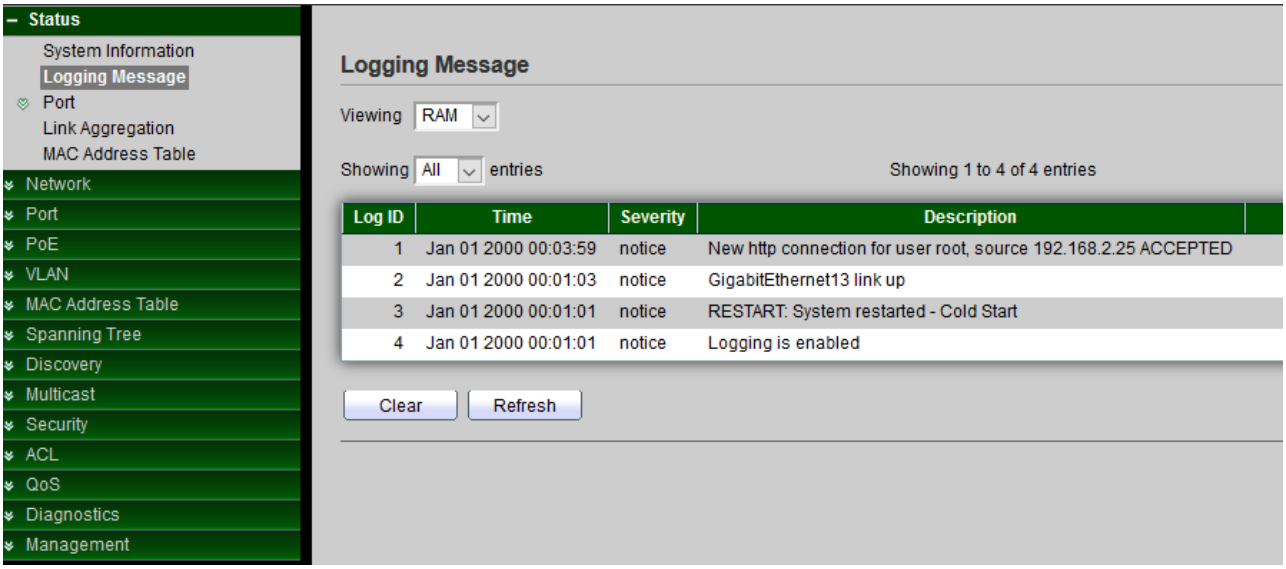
- **Model:** Display model name of the switch.



- **System Name/ Location/ Contact:** Display system name of the switch. When administrator click Edit button then can modify the system information.
- **MAC Address:** Display system use MAC address.
- **IPv4/v6 Address:** Display system use IP address.
- **System Uptime:** Display system operating time.
- **System Current:** Display system time.
- **Loader Version:** Display system loader version.
- **Loader Time:** Display loader time
- **Firmware Version:** Display system firmware version.
- **Firmware Date:** Display firmware time.
- **Telnet / SSH / HTTP / HTTPs / SNMP:** Display system enable or disable the services information.

3.2 Logging Message

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



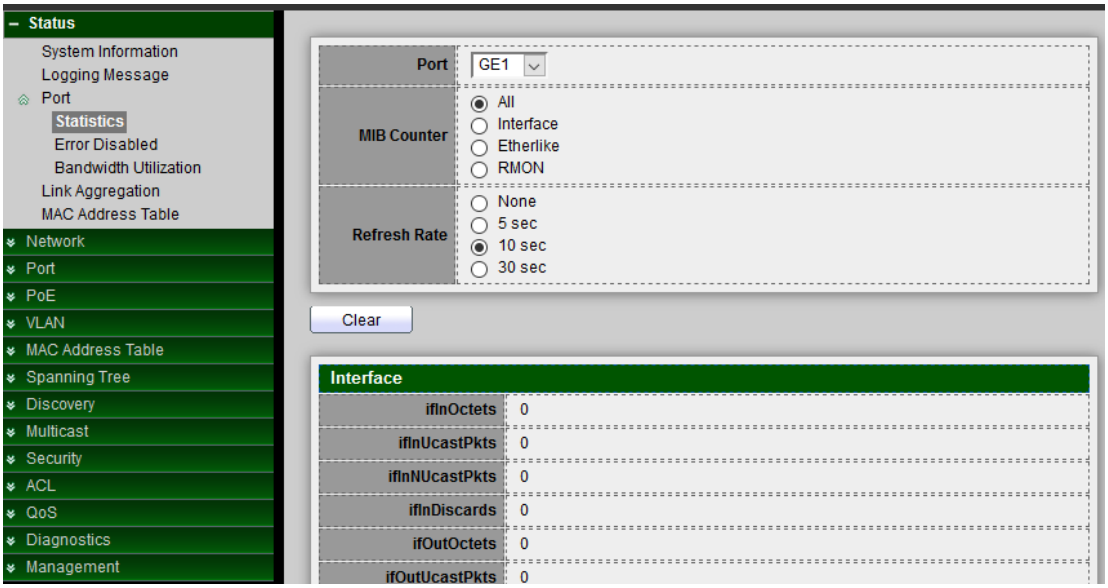
- **Viewing:** Administrator can select RAM or Flash.
- **Showing:** Administrator can set pen display.

3.3 Port

Display detailed information for each port.

3.3.1 Statistics

Administration can choose to view specified GE or LAG information.(contain Interface/ Etherlike/ RMON information) or set auto refresh time of information page.



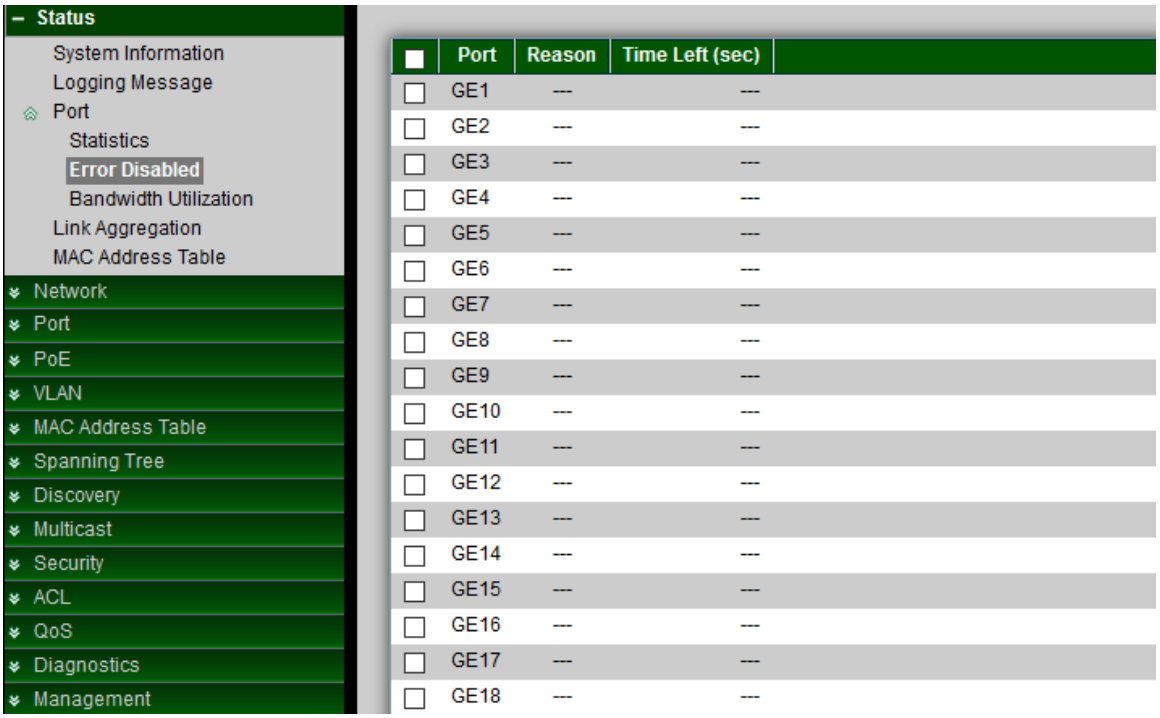
Interface	
ifInOctets	1226044
ifInUcastPkts	8677
ifInNUcastPkts	343
ifInDiscards	0
ifOutOctets	2813449
ifOutUcastPkts	5587
ifOutNUcastPkts	194
ifOutDiscards	0
ifInMulticastPkts	226
ifInBroadcastPkts	117
ifOutMulticastPkts	194
ifOutBroadcastPkts	0

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

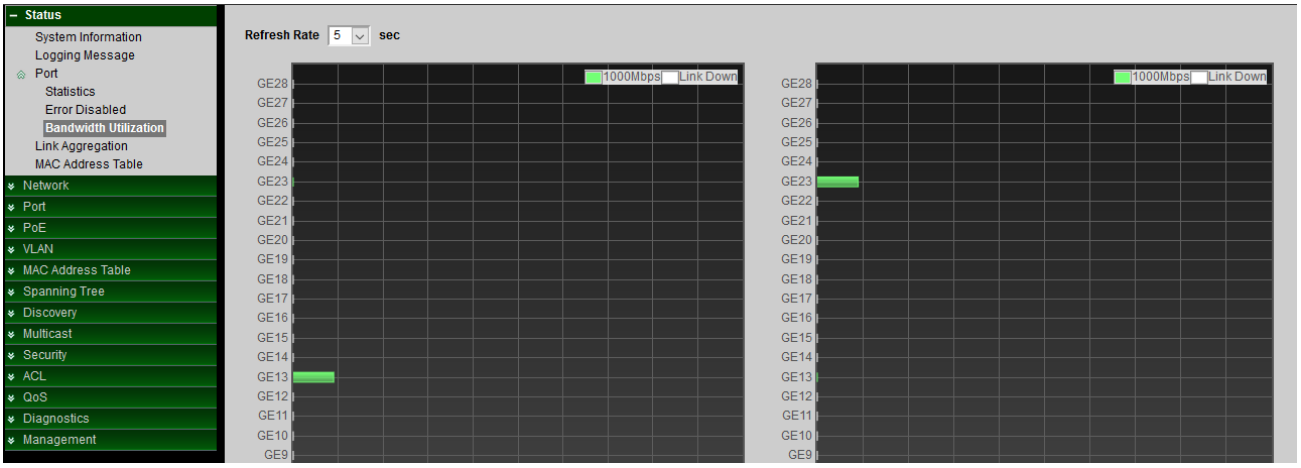
3.3.2 Error Disabled

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



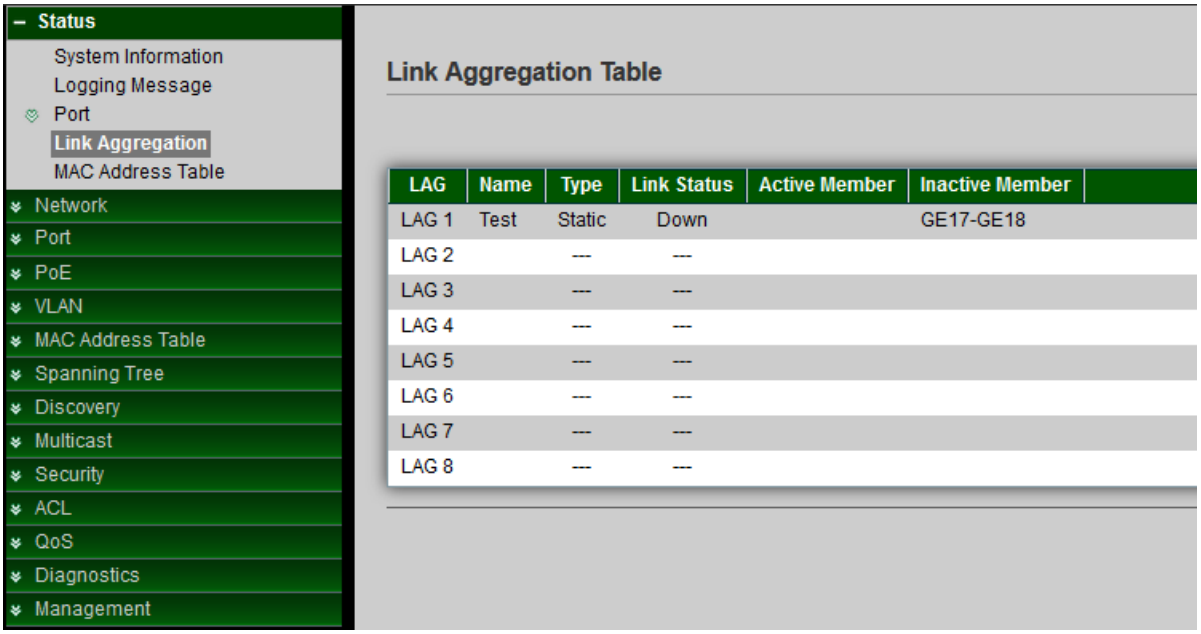
3.3.3 Bandwidth Utilization

This page can display Tx / Rx Real-time bandwidth information of each port. (Instant used rate per port).



3.4 Link Aggregation

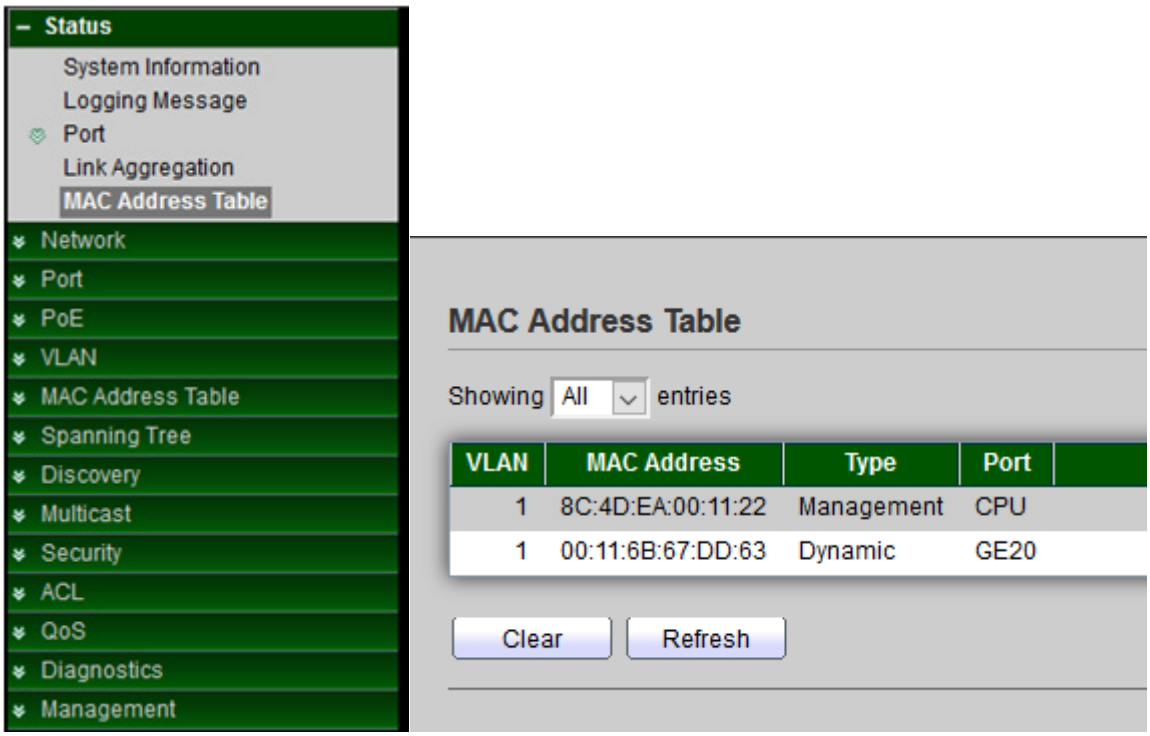
If administrator has set LACP function then this can display LACP information.



- **LAG 1~8:** This system have support 8 Link Aggregation group. Administrator can enable 8 LAG.
- **Name:** Disable LAGs name.
- **Type:** Display Link Aggregation used Static or LACP mode.
- **Link Status:** Display LA status.
- **Active / inactive Member:** Display LA active or inactive member.

3.5 MAC Address Table

Display each port of MAC address and VLAN information.

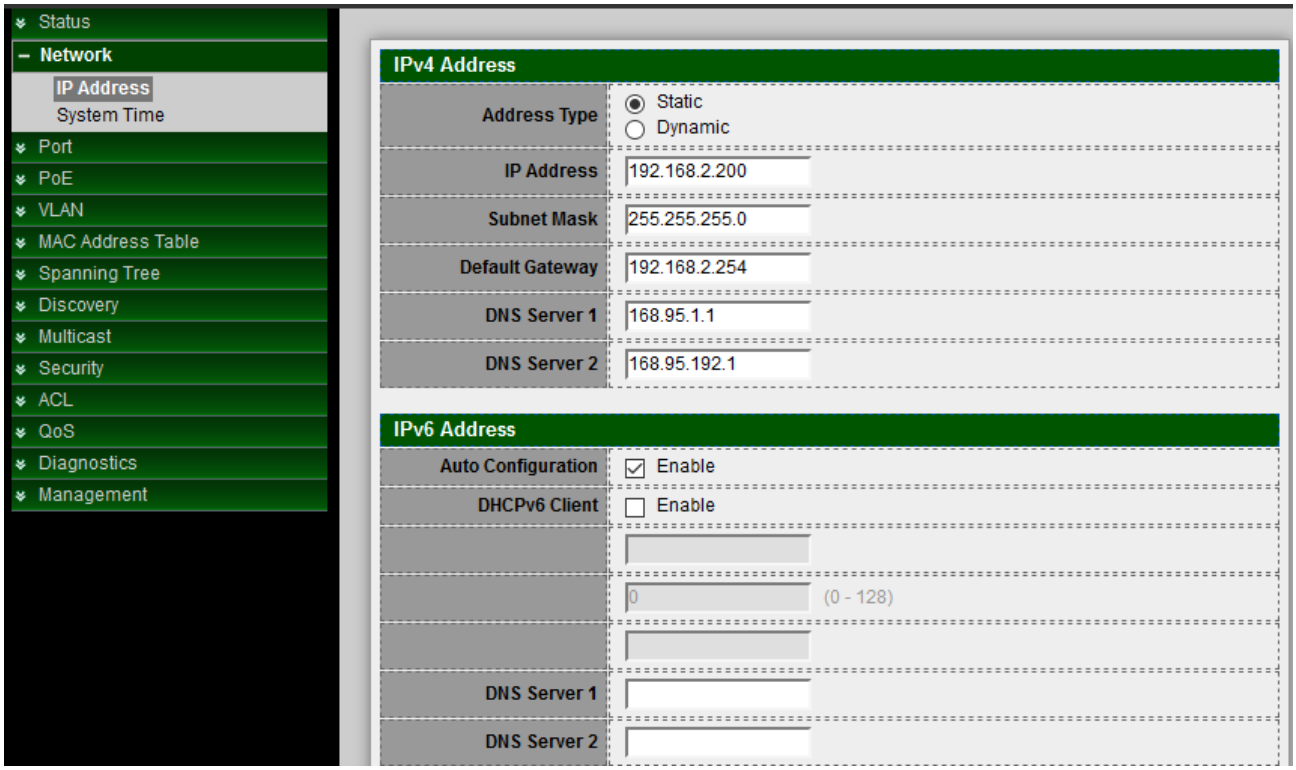


- **VLAN:** Display each port used VLAN number.
- **MAC Address:** Display device use MAC address information.
- **Type:** Display each port used type for Dynamic or Static.
- **Port:** Display Port number.

4. Network

4.1 IP Address

Administrator can set IP address for the system. The IP address support IPv4 & IPv6 protocol, if switch device must want to internet, administrator can set gateway IP address in the page.



IPv4 Address

- **Address Type:** Administrator can select use static or Dynamic IP address in system. If administrator chooses use Dynamic type then switch IP address will be dispatched by the DHCP server.
- **IPv4 Address / subnet / Gateway / DNS1-2:** If used static IP address then administrator can modify this IP address and subnet and gateway and DNS IP address of the system.

IPv6 Address

- **IPv6 Address:** Administrator can choose use Auto Configuration or DHCP Client mode to set IPv6 address.

  If administrator disables Auto Configuration or DHCP Client mode then administrator can manual setting IPv6 address.

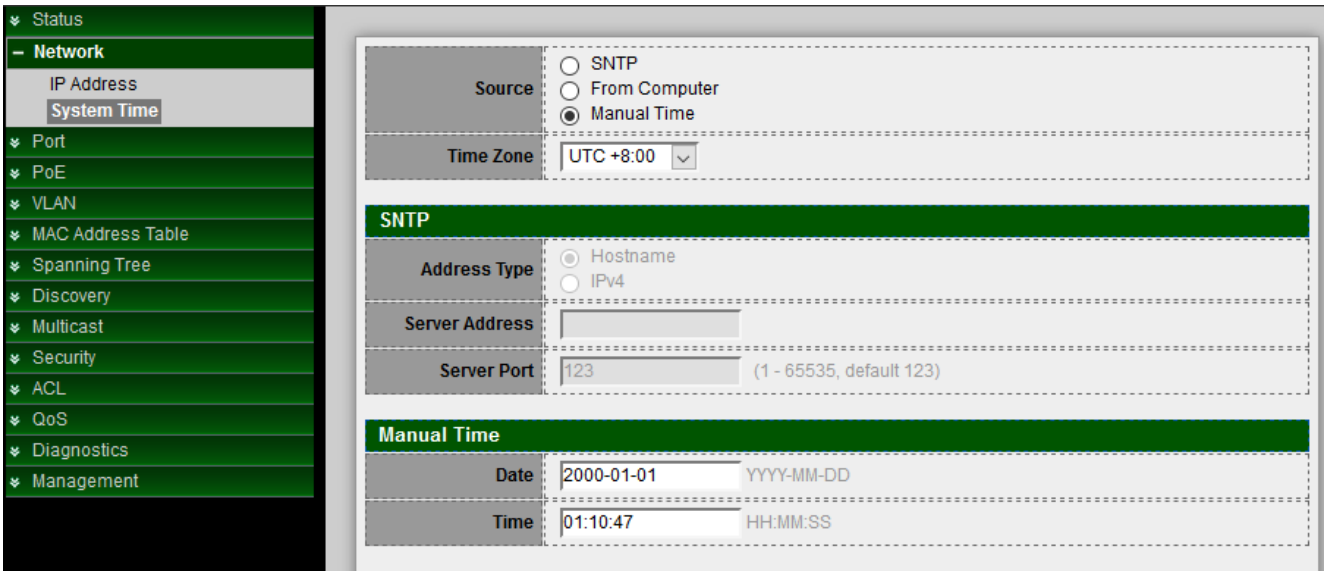
Operational Status

This information can display the current used IPv4/v6 address and gateway of the switch.

4.2 System Time

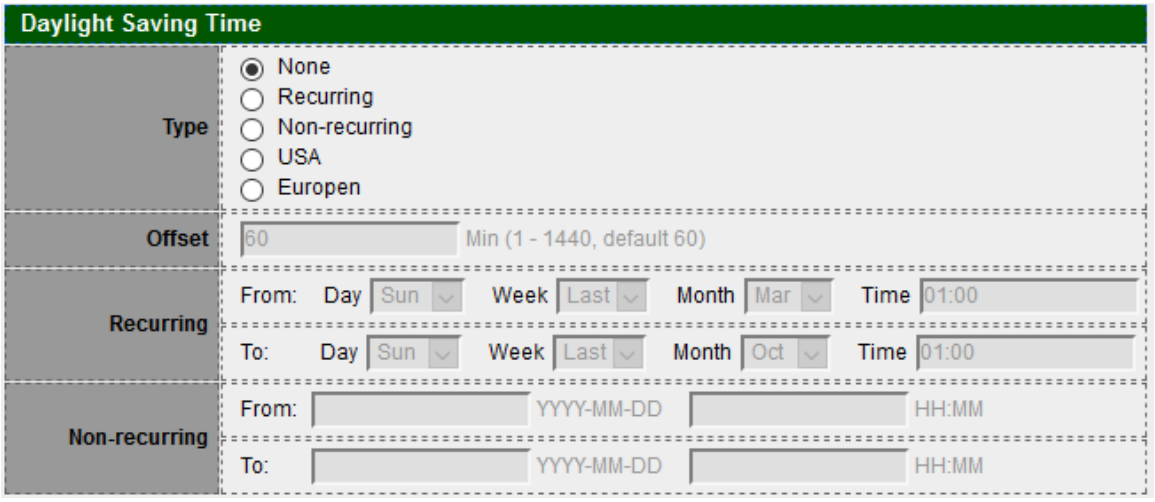
System time can be configured via this page. Administrator can select SNTP Server or from computer to update the system time or administration can use manual setting the system time.

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.



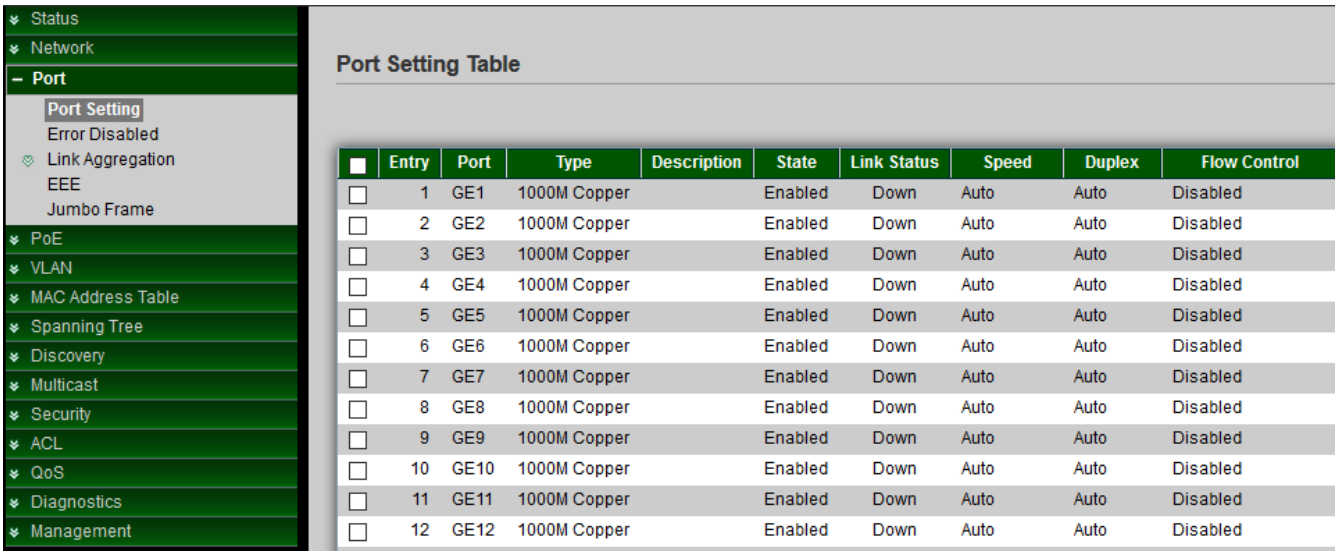
Daylight Saving Time

The L2 Switch support Daylight saving time function, if administrator need enable and set the Daylight saving time function will can be enable this function.



5. Port

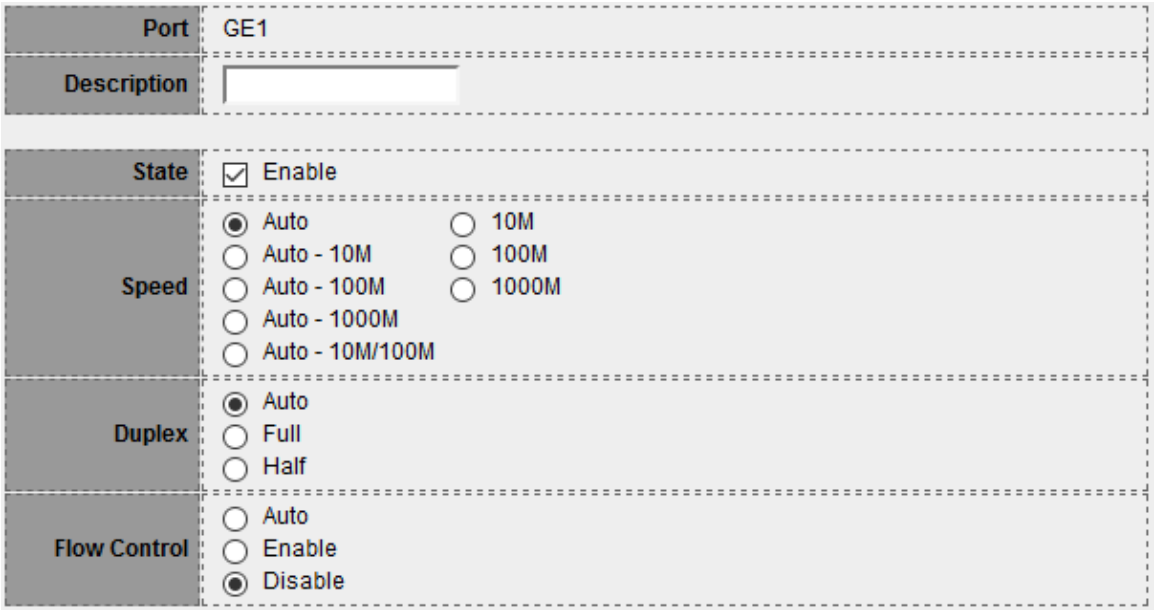
5.1 Port setting



Entry	Port	Type	Description	State	Link Status	Speed	Duplex	Flow Control
1	GE1	1000M Copper		Enabled	Down	Auto	Auto	Disabled
2	GE2	1000M Copper		Enabled	Down	Auto	Auto	Disabled
3	GE3	1000M Copper		Enabled	Down	Auto	Auto	Disabled
4	GE4	1000M Copper		Enabled	Down	Auto	Auto	Disabled
5	GE5	1000M Copper		Enabled	Down	Auto	Auto	Disabled
6	GE6	1000M Copper		Enabled	Down	Auto	Auto	Disabled
7	GE7	1000M Copper		Enabled	Down	Auto	Auto	Disabled
8	GE8	1000M Copper		Enabled	Down	Auto	Auto	Disabled
9	GE9	1000M Copper		Enabled	Down	Auto	Auto	Disabled
10	GE10	1000M Copper		Enabled	Down	Auto	Auto	Disabled
11	GE11	1000M Copper		Enabled	Down	Auto	Auto	Disabled
12	GE12	1000M Copper		Enabled	Down	Auto	Auto	Disabled

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

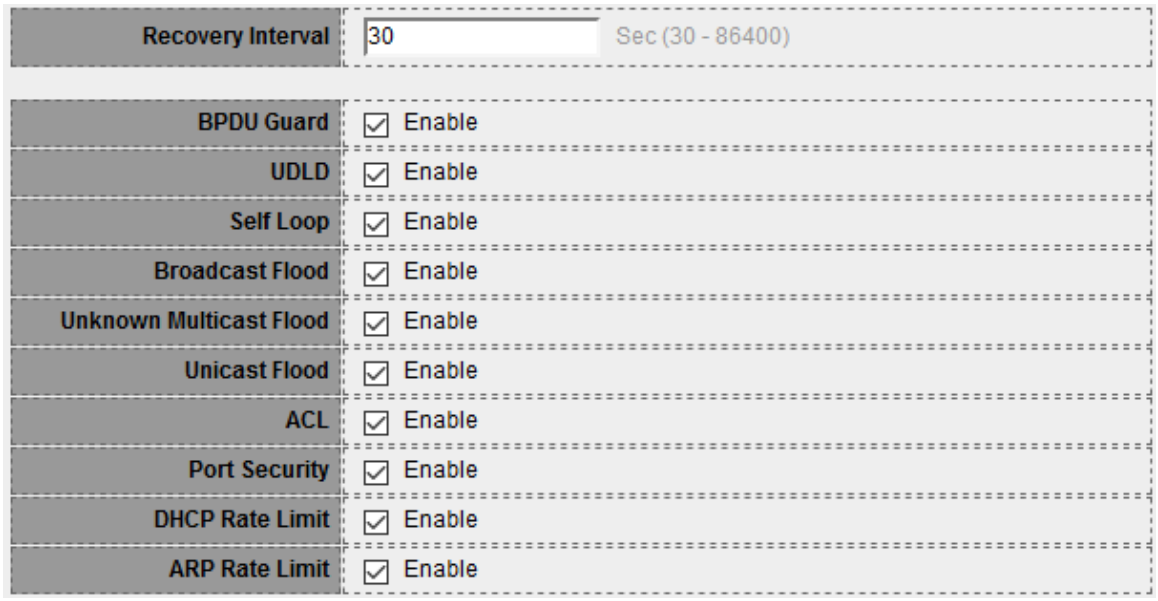
Please select port number in checkbox and click apply button to set speed / Duplex / Flow Control of each port.



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.

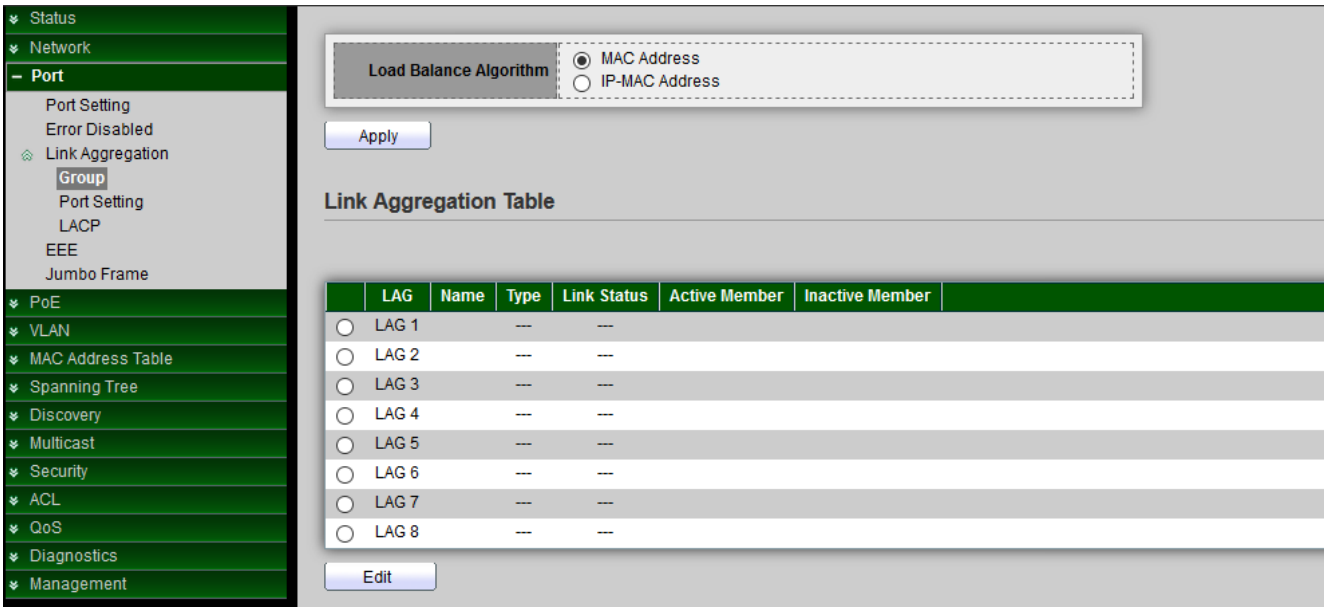
After administrator enable this functions, if occur error in table functions then system will auto immediate block of faulty operation until the after the set time, system will auto re-enable.



- **Recovery Interval**: Administrator can set time of auto recovery interval.

5.3 Link Aggregation setup

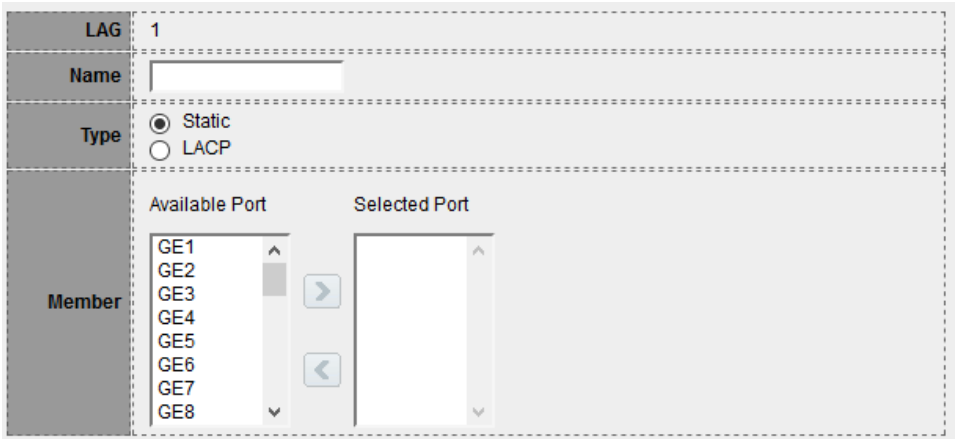
Link Aggregation is also referred to as link aggregation, teaming port, and port trunk for 802.3ad (LACP, Link Aggregation Control Protocol), The Port Aggregation can aggregate multiple Ethernet ports together to form a logical aggregation group. To upper layer entities, all the physical links in an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



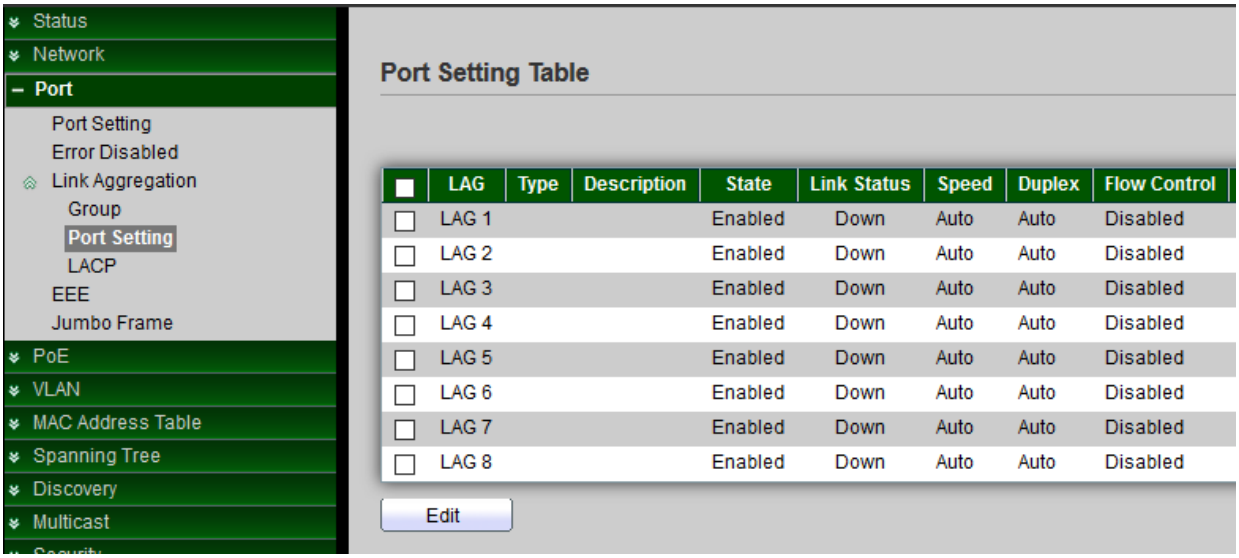
- **Type:** LDAP function support Static and LACP (Dynamic) 2 types.
  - **Static:** If used “static” the number of ports on both sides of the switch is fixed, every entity network connection can't error, and otherwise it will not be able to connect successfully.

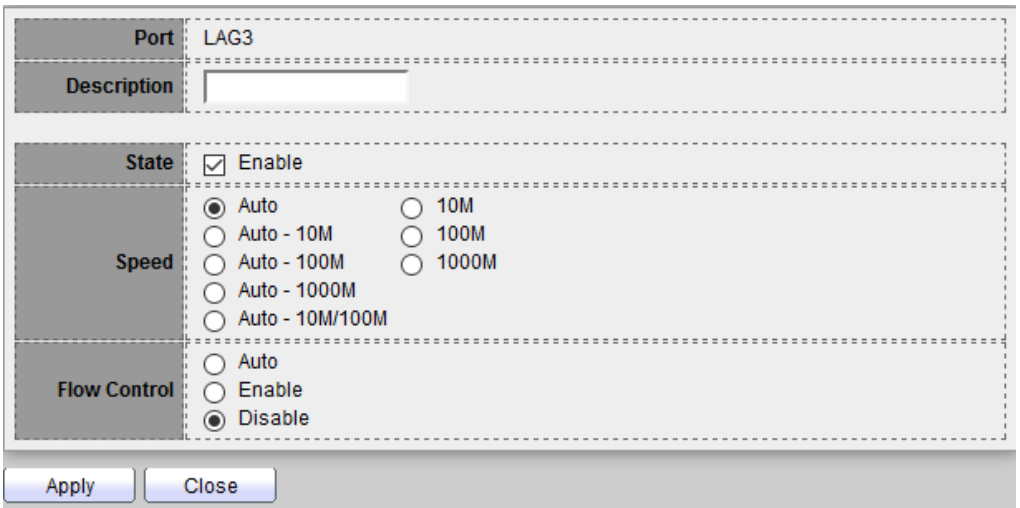
- **LACP:** LACP is IEEE Standard, When LACP mode is set on both sides of the switch, both ports will check whether joining LAG group through the query, if both used LACP mode then enable LACP function, otherwise they will skip the LACP connection.

➢ **Member:** Administrator need choose posts in the LA group.

5.3.2 Port Setting

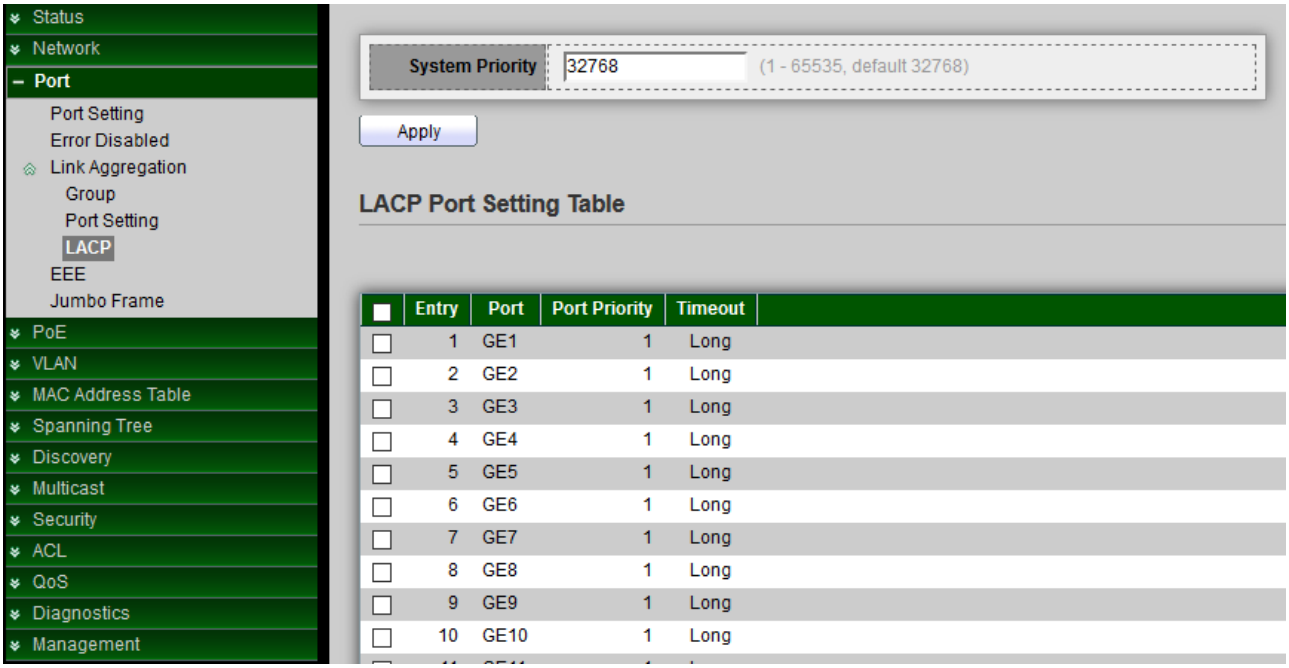
Administrator can set speed and flow control for Link Aggregation Group (LAG).





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.

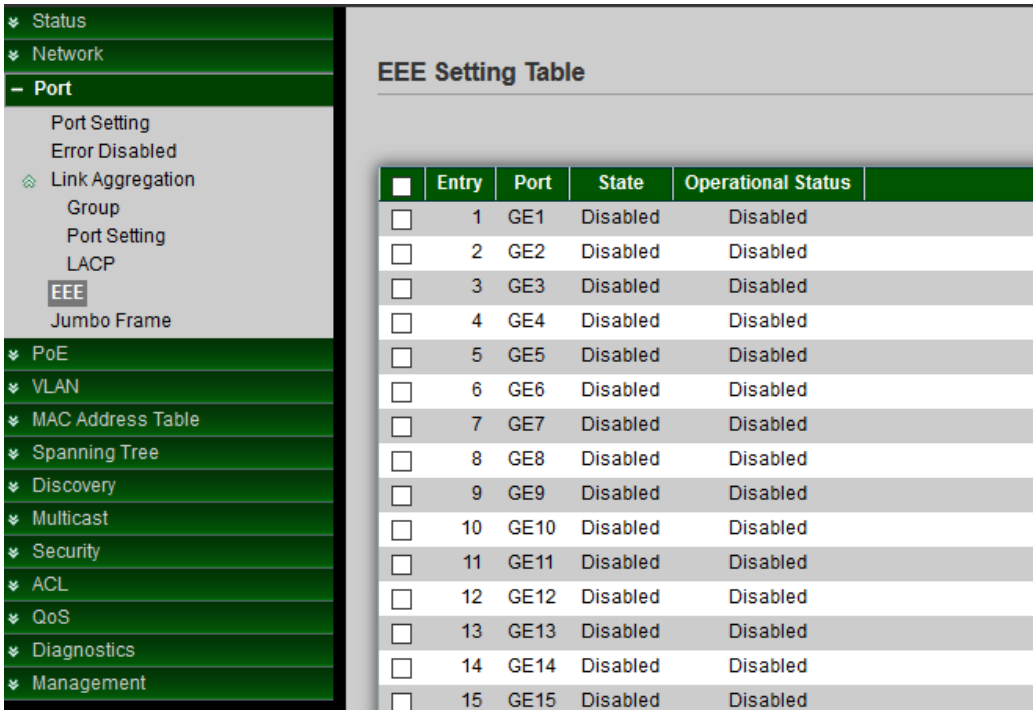


- **System Priority:** Administrator configures the LACP system priority on each switch running LACP. LACP uses the system priority with the switch MAC address to form the system ID and also during negotiation with other switches.

  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.

5.4 EEE

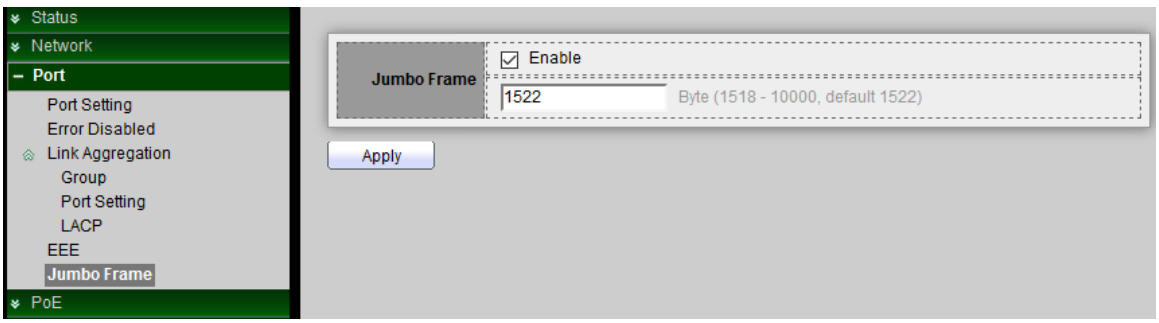
This switch support Energy-effcient Ethernet(EEE) function. Administrator can choose Enable or Disable EEE function. The default is “Disable”.



5.5 Jumbo Frame

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

Note	Adjust frames size: (This frame control is always “Enable”) 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".



6. PoE

6.1 Global Setting

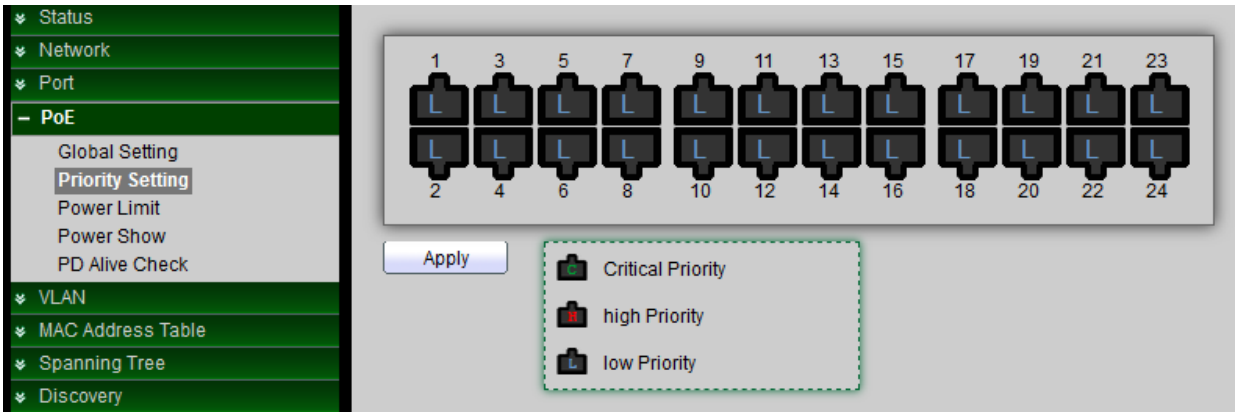
This page system can calculate PoE used nominal power / Consuming Power / Remaining Power and administrator can set PoE enable / disable by schedule.

	Index	Name	Port List	Schedule Status
☐	1	Test	gi2,gi4,gi12,gi22	Enable
☐	2	None		Disable
☐	3	None		Disable
☐	4	None		Disable
☐	5	None		Disable
☐	6	None		Disable
☐	7	None		Disable
☐	8	None		Disable
☐	9	None		Disable

System supports 24 time schedule. If administrator need enable time schedule then must go to "**Management**" ➔ "**Time Range**" create and set time policy first.

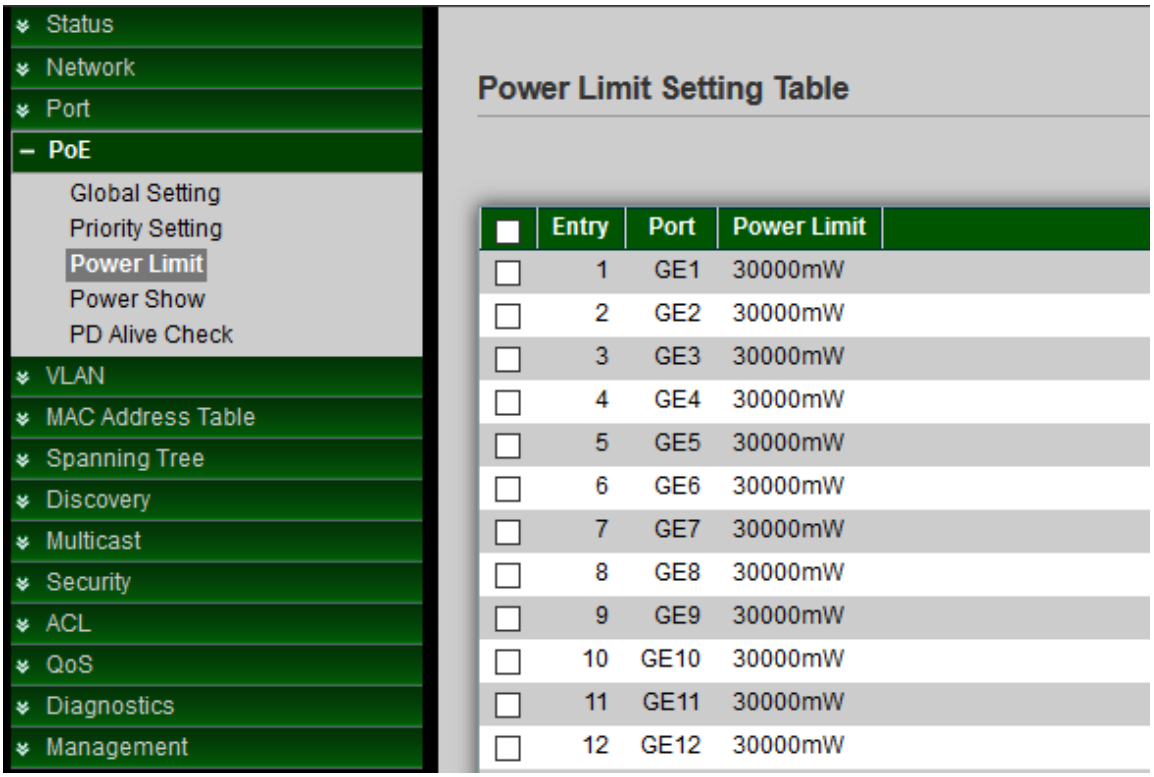
6.2 Priority Setting

The PoE priority default is priority 3, administrator can set priority 1-3 for the Critical/High/Low.
If the function setting prioritizes the power allocation to the ports that present a PD power demand. This system will remove power from one or more lower-priority ports to meet the power demand on other, higher-priority ports.



6.3 Power Limit

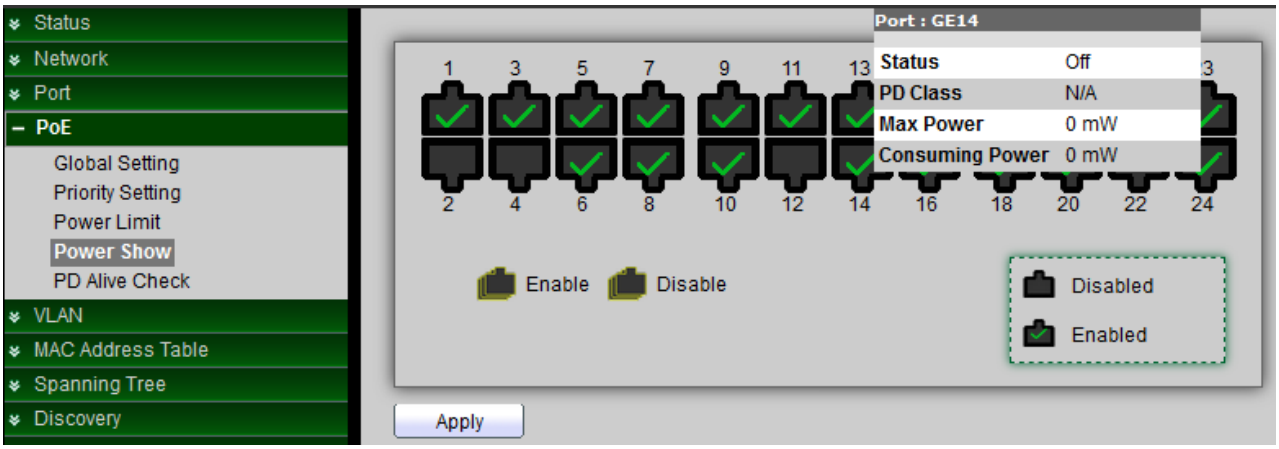
Administrator can set output power limit of each ports. Default is 30W



	Entry	Port	Power Limit
☐	1	GE1	30000mW
☐	2	GE2	30000mW
☐	3	GE3	30000mW
☐	4	GE4	30000mW
☐	5	GE5	30000mW
☐	6	GE6	30000mW
☐	7	GE7	30000mW
☐	8	GE8	30000mW
☐	9	GE9	30000mW
☐	10	GE10	30000mW
☐	11	GE11	30000mW
☐	12	GE12	30000mW

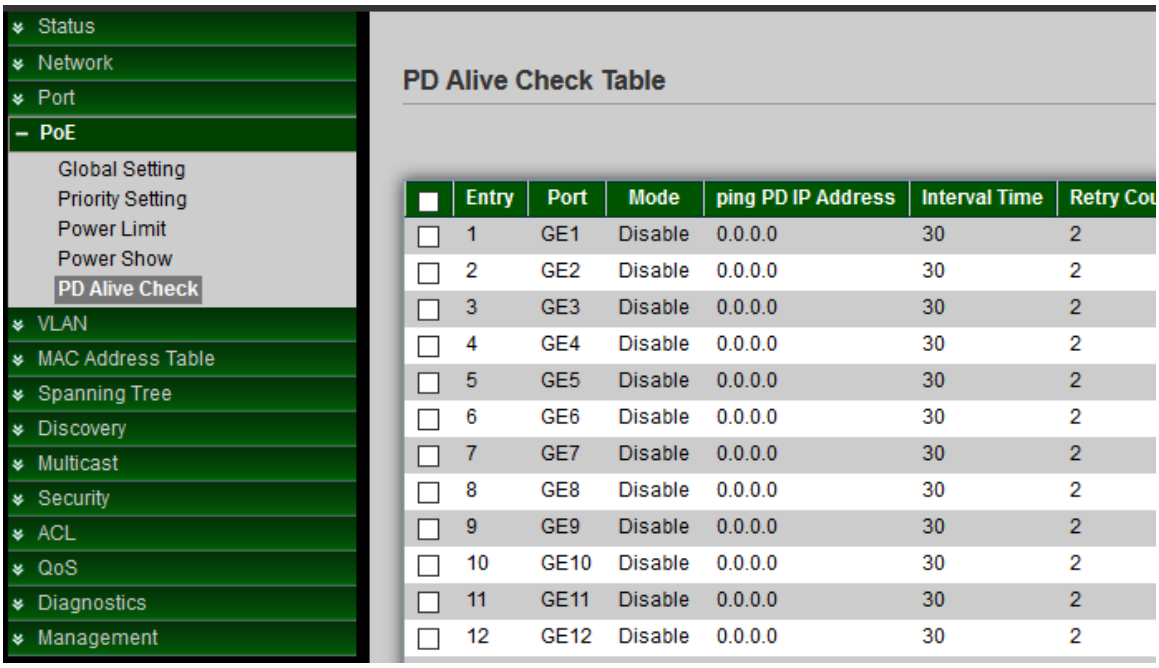
6.4 Power Show

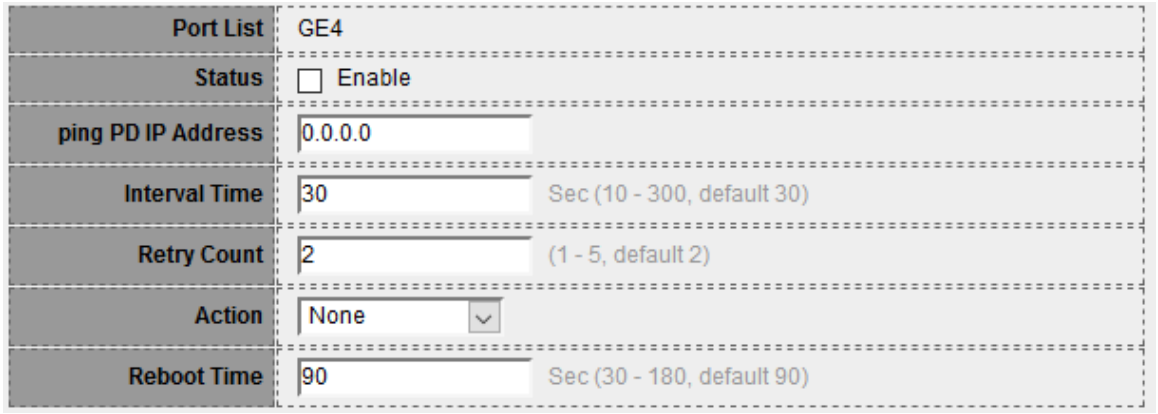
This page can display PoE on/off and PoE used power (mW)



6.5 PD Alive Check

The function can detection PD device whether alive and support ping tools.
Administrator can set IP address of device, let the system automatically ping to device, if device not response then system can auto take PoE off and re-power PoE.



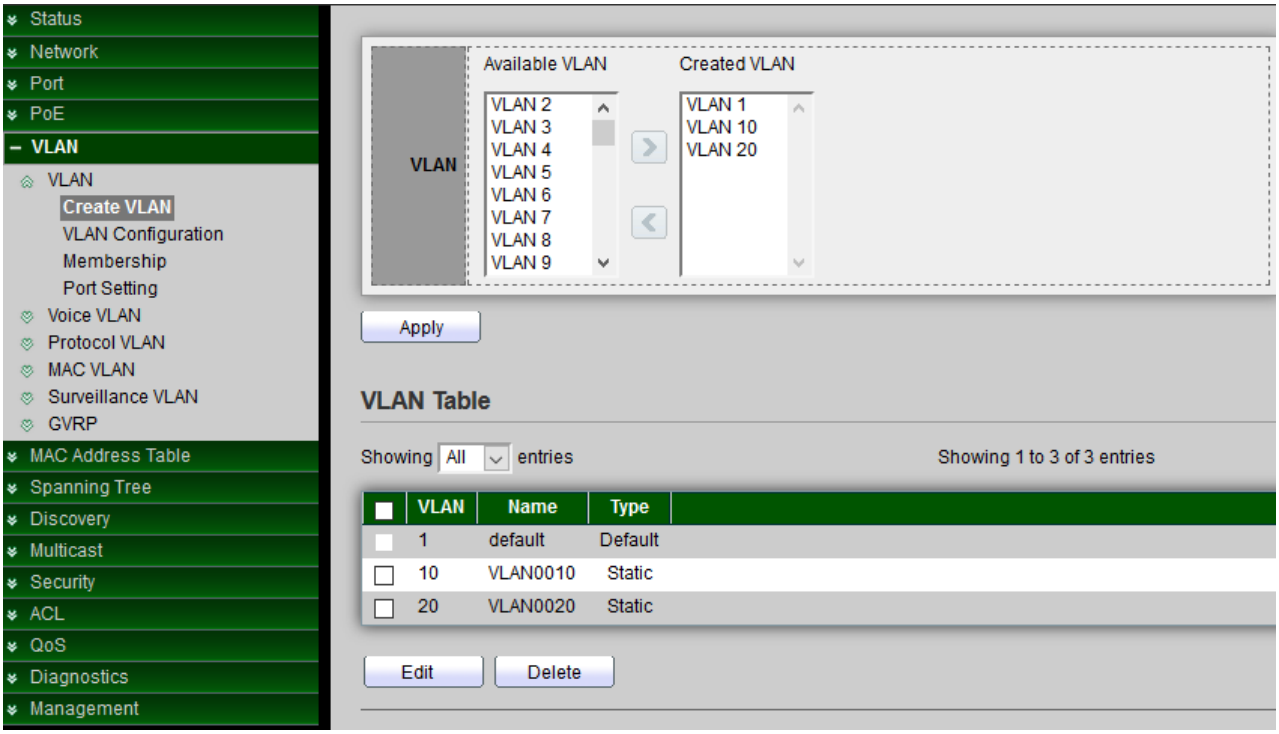


7. VLAN

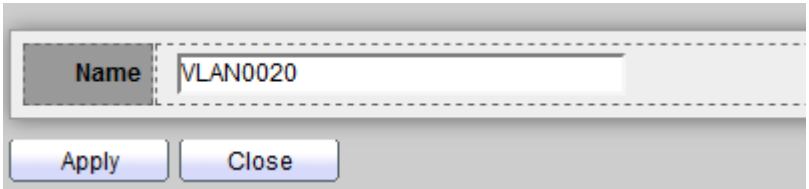
Administrator can set IEEE 802.1q Tag Based VLAN or Port Based VLAN. System default is VLAN1 Port based (PVID).

7.1 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.

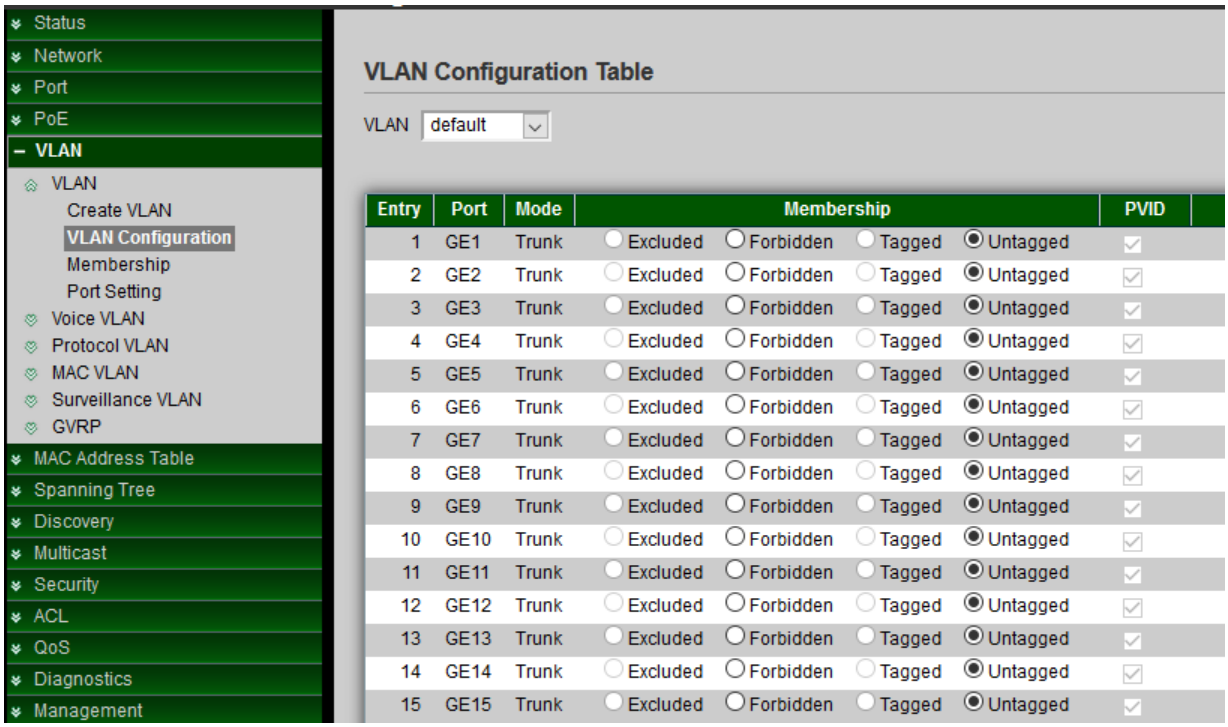


- **VLAN:** Administrator can select VLANs number in "Available VLAN" table and move to "Created VLAN" table will complete the 802.1q VLAN.
- **VLAN Table:** Administrator can checkbox VLAN to edit or delete, if check and click "Edit" button then administrator can manual modify name description for this VLAN.



7.2 VLAN Configuration

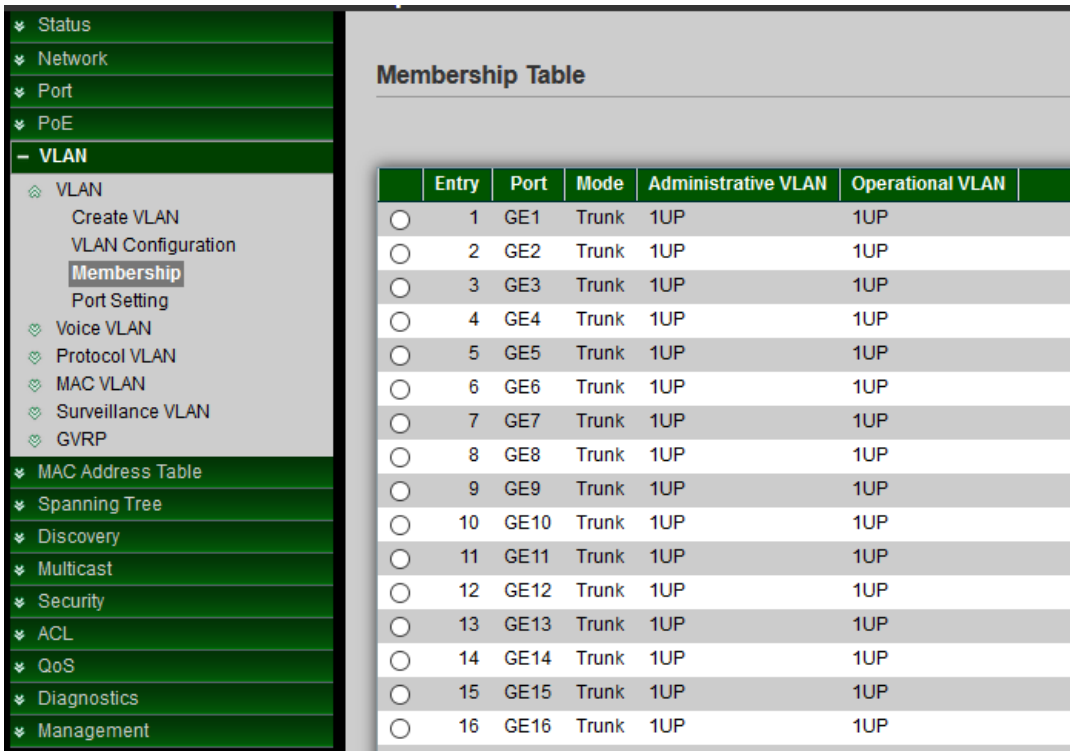
Administrator can choose set Excluded / Forbidden / Tagged / Untagged function in membership table of the Port and LAG.

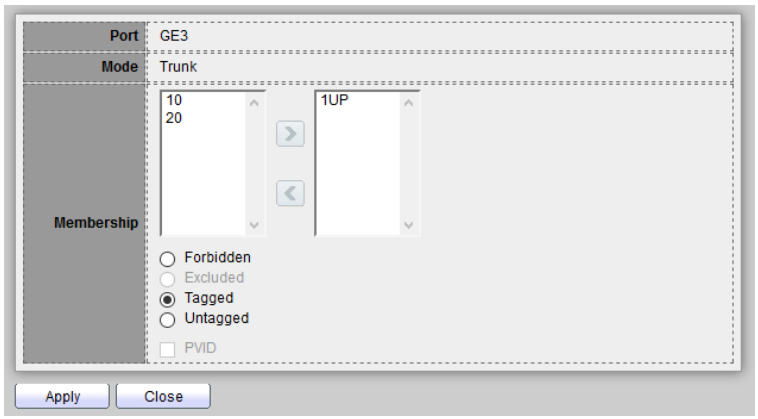


- **VLAN:** Administrator can click drop down menu to choose VLAN and set.
  - **Excluded:** This interface is currently not a member of the VLAN. This is the default for all the ports and LAGs.
  - **Tagged**: This interface is a tagged member of the VLAN.
  - **Untagged**: This interface is an untagged 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.

7.3 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.

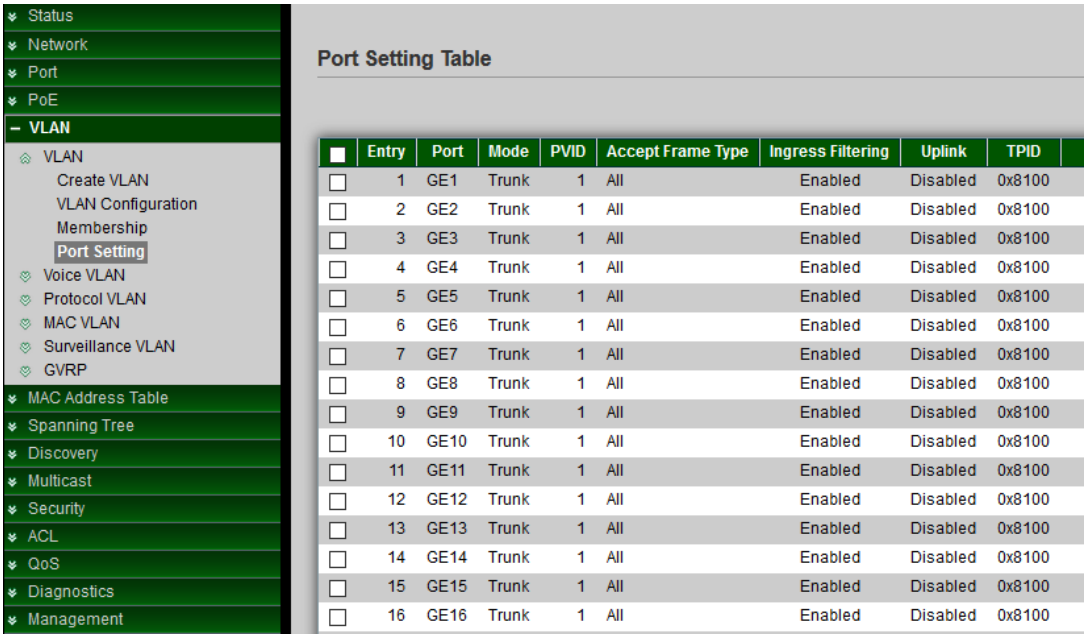


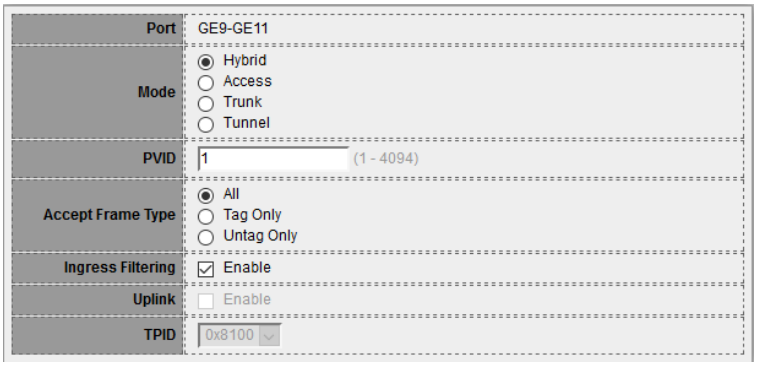


- **Port:** Display selected port number.
- **Mode:** Displays the port VLAN mode that was selected on the Interface Settings page.
- **Membership:** Move the VLAN IDs from the left list to the right list by using the arrow buttons. The default VLAN might appear in the right list if it is tagged, but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

7.4 Port Setting

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





- **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.

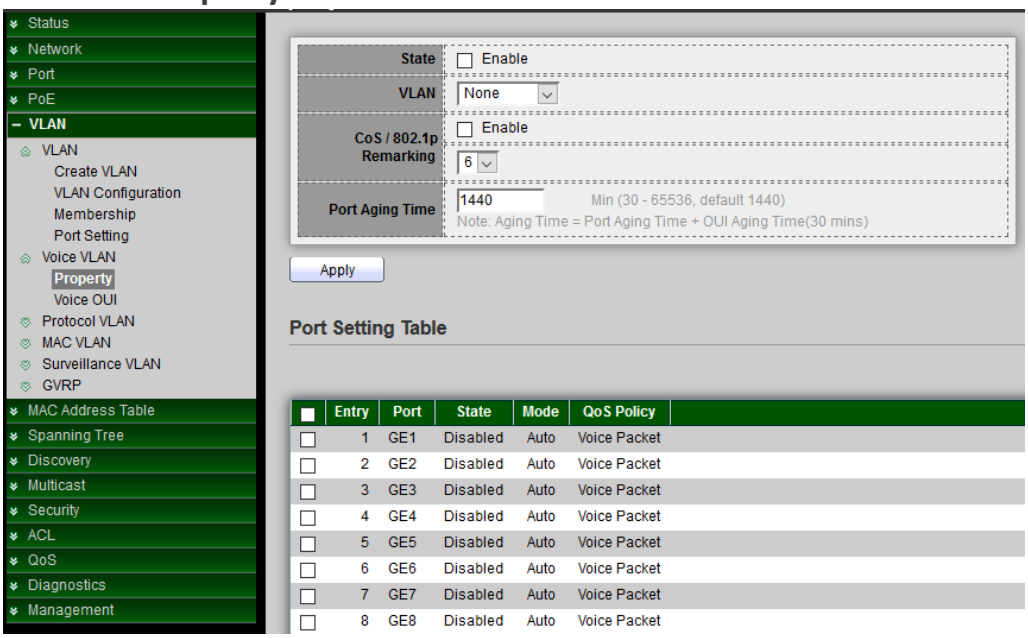
➢ **Uplink:** Administrator can check **Enable** to set the interface as an uplink port.

➢ **TPID:** If Unlink is enabled, select the Modified Tag Protocol Identifier (TPID) value for the interface.

7.5 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.

7.5.1 Property



➢ **State:** Administrator can choose Enable or Disable this function.

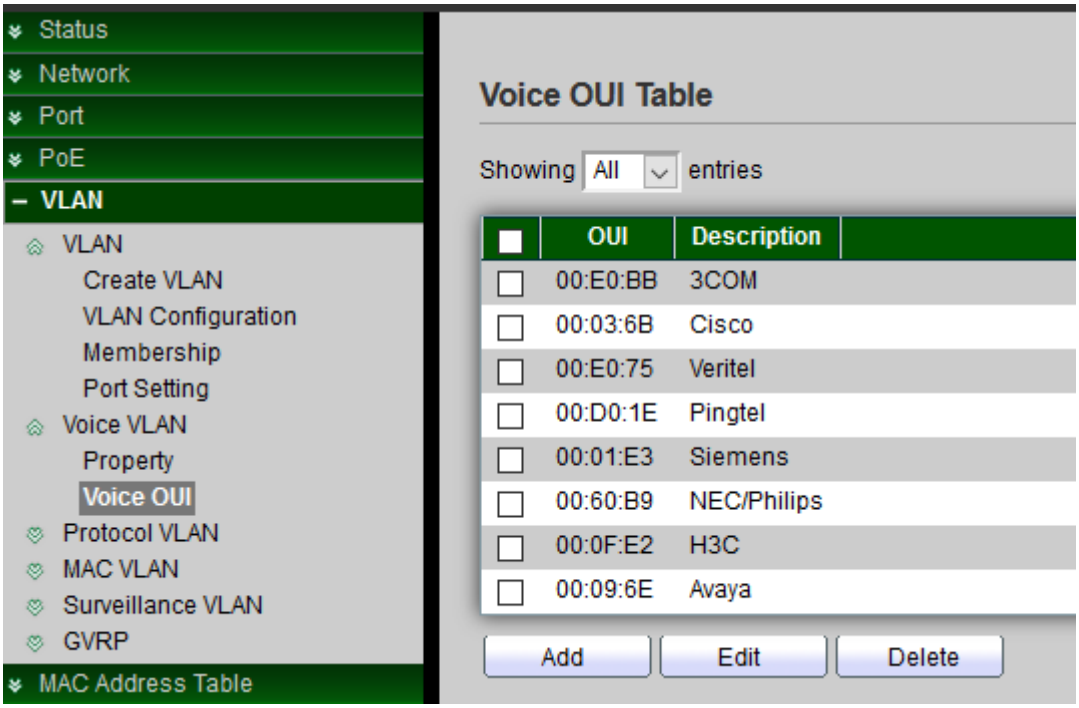
➢ **VLAN:** Administrator can choose VLAN.

➢ **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.

7.5.2 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.



Administrator can create new OUI or modify or delete OUI in table

Click **"Add"** button can create new OUI.

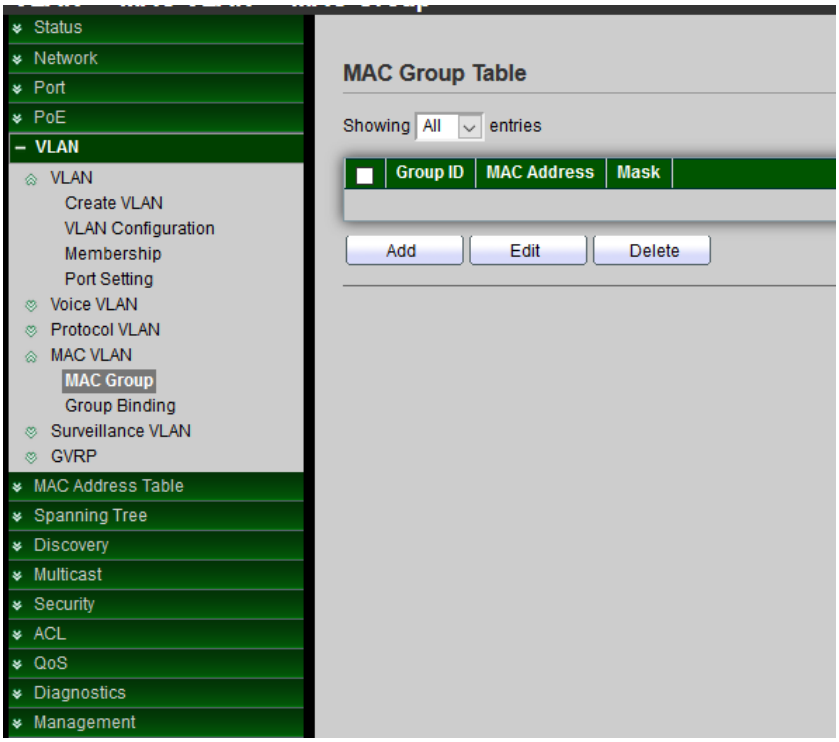
Click "**Edit**" button can modify OUI data.

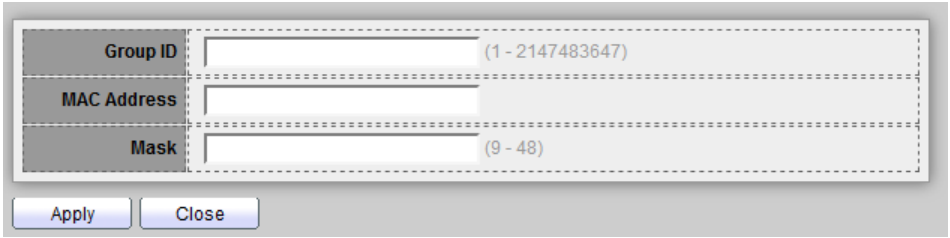
Click "**Delete**" button can delete OUI data.

7.6 MAC VLAN

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.





7.7 GVRP

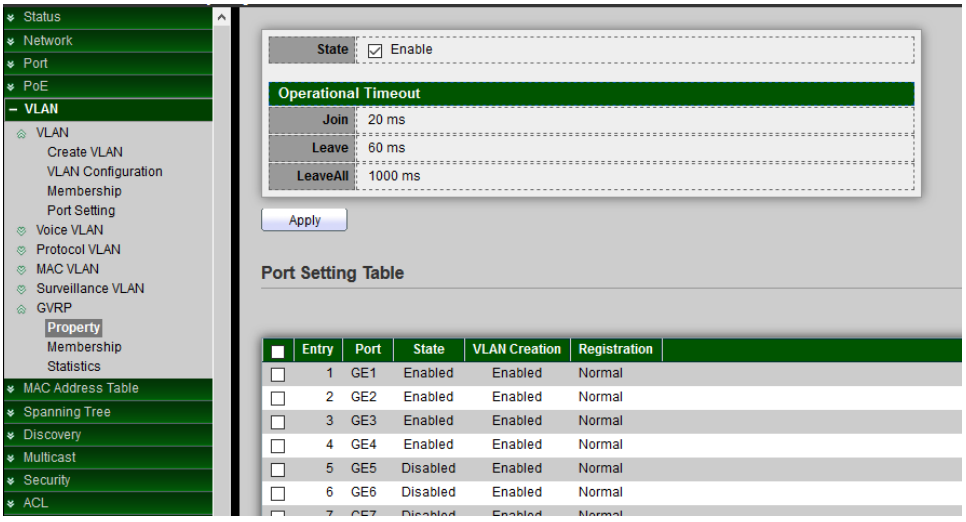
The GVRP (Generic VLAN Registration Protocol) is described in the IEEE 802.1p standard; It's an IEEE 802.1Q-compliant method for facilitating automatic (dynamic) VLAN membership configuration. GVRP-enabled switches can exchange VLAN configuration information with other GVRP-enabled switches.

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.

7.7.1 Property

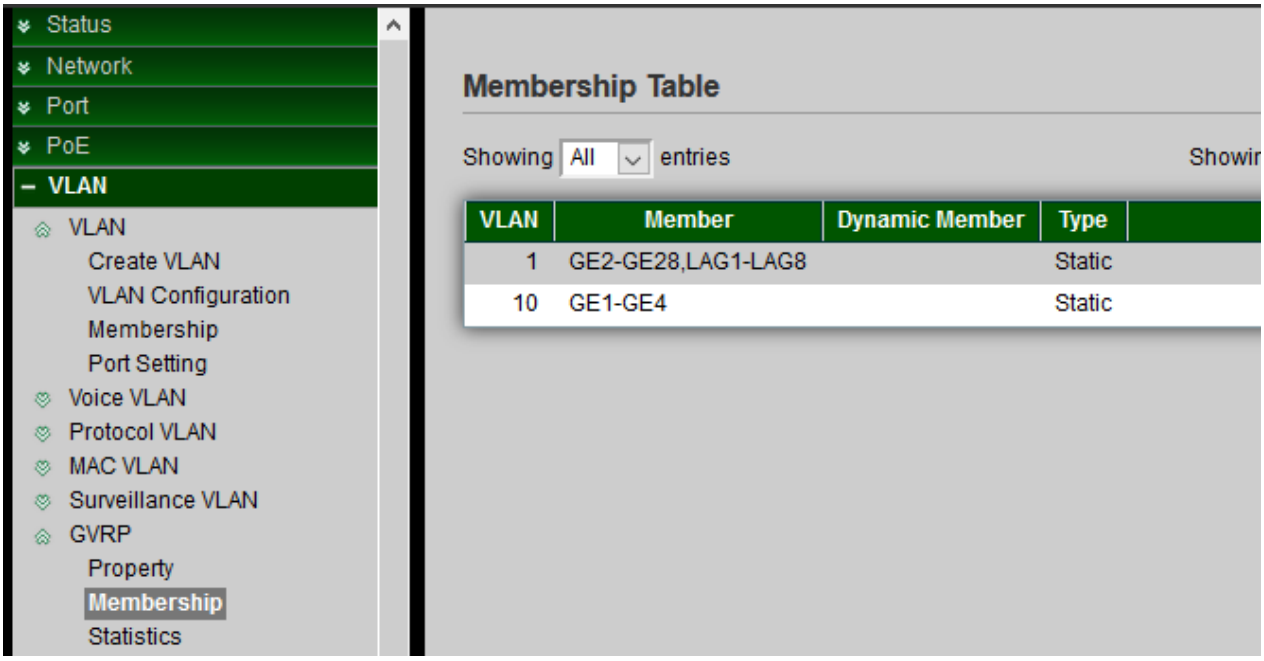
Administrator can enable GVRP function and set every port registration on GVRP.



- **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.

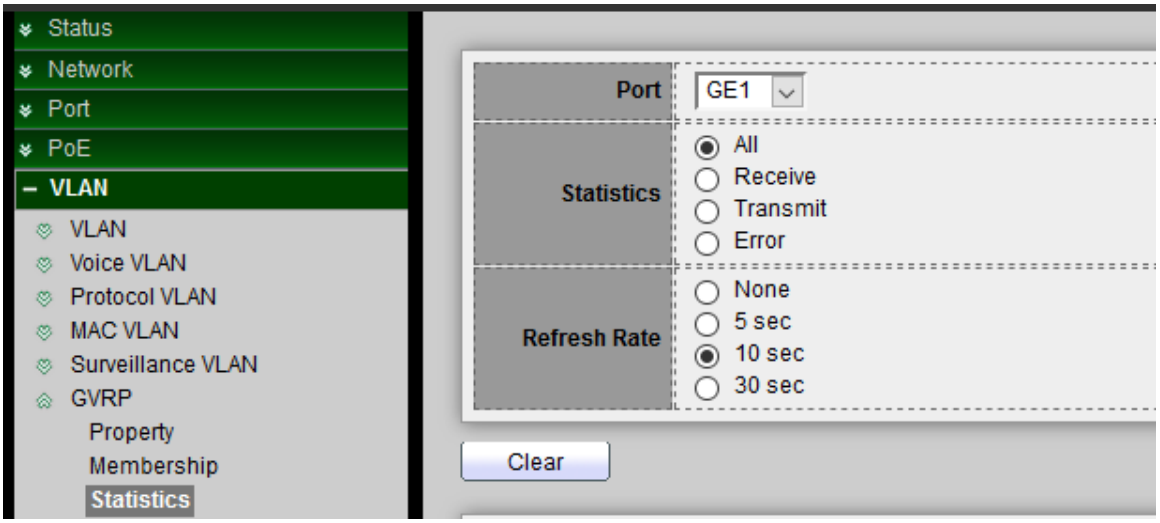
7.7.2 Member ship

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



7.7.3 Statistics

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



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

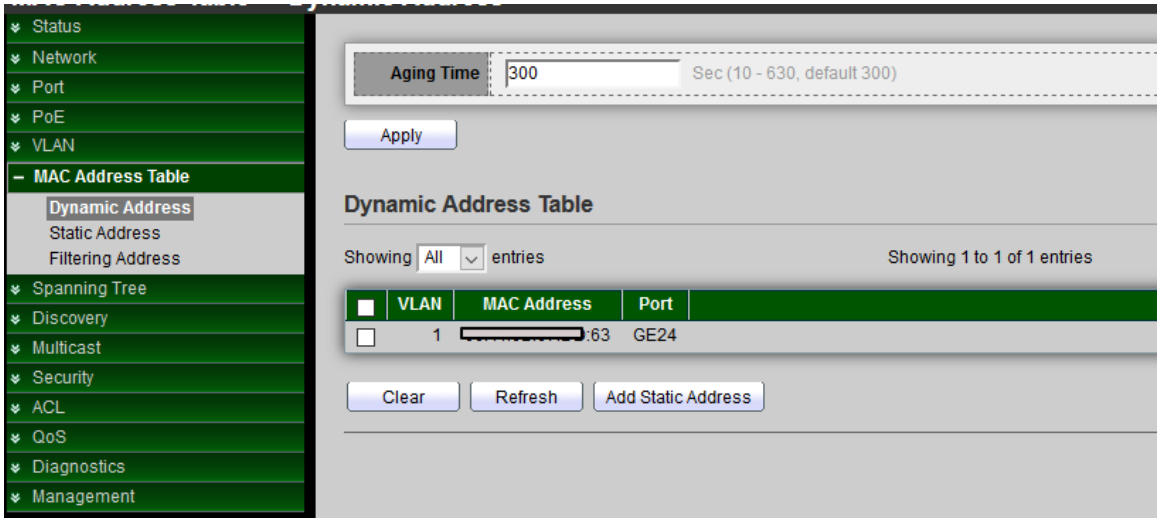
Transmit	
Join empty	0
Empty	0
Leave Empty	0
Join In	0
Leave In	0
Leave All	188

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

8. MAC Address Table

8.1 Dynamic Address

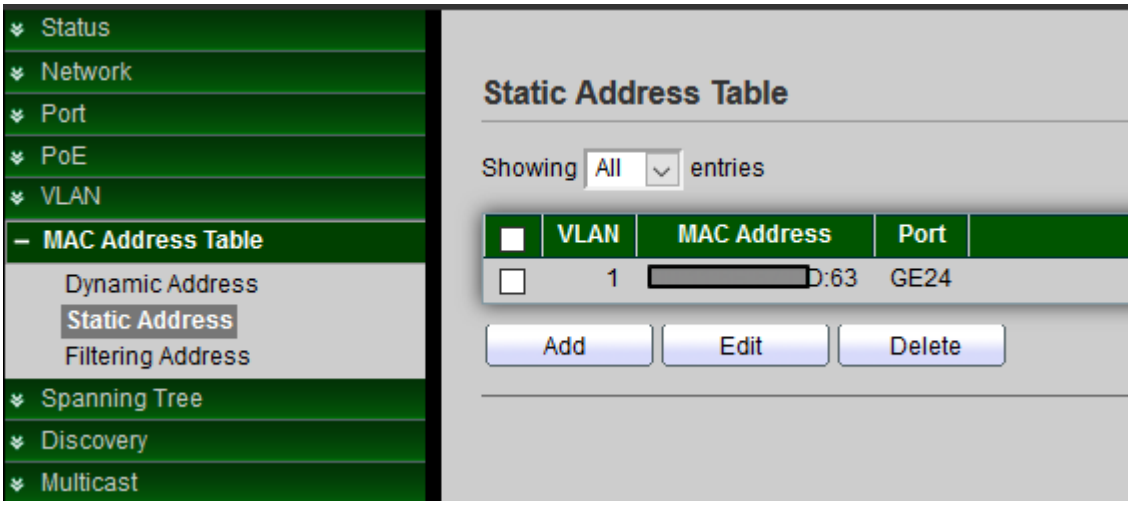
This page can display MAC address for connected device. Administrator can set aging time for connected port.



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

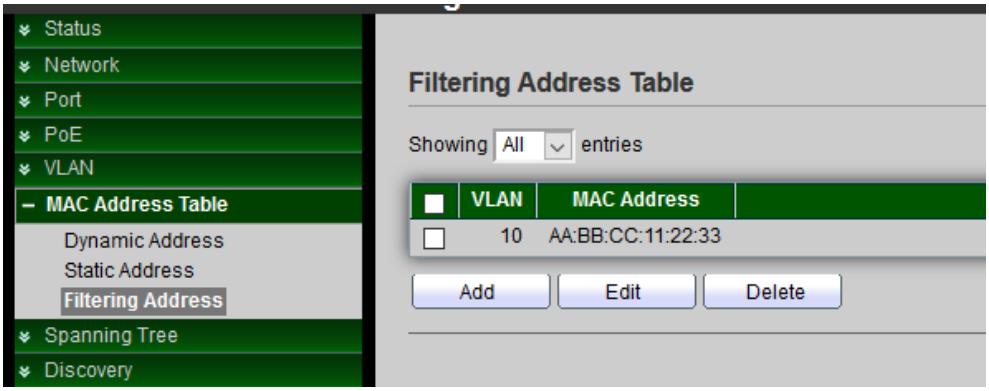
8.2 Static Address

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.



8.3 Filtering Address

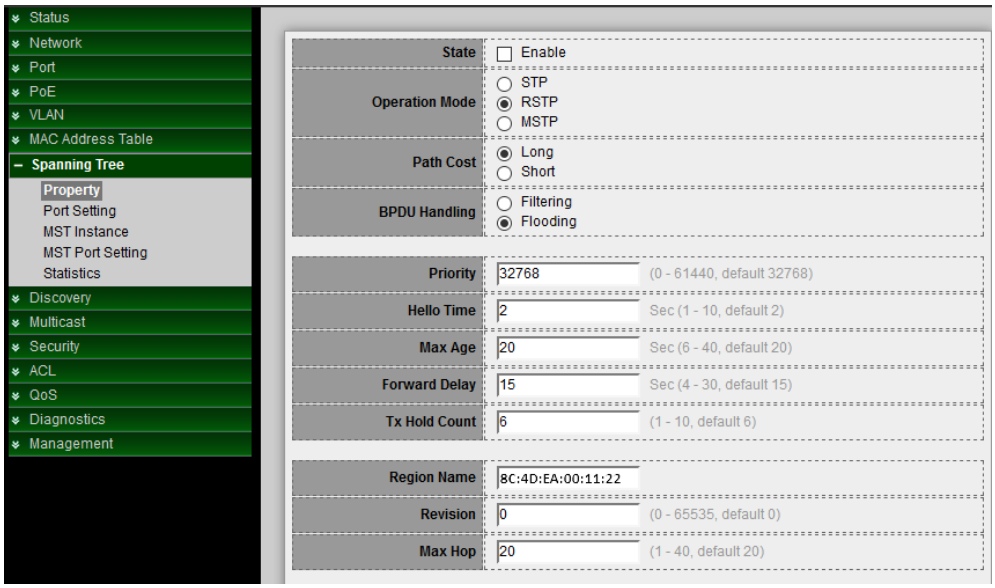
Administrator can set need filtering MAC address in the MAC table. If MAC is added on table this MAC will be blocked



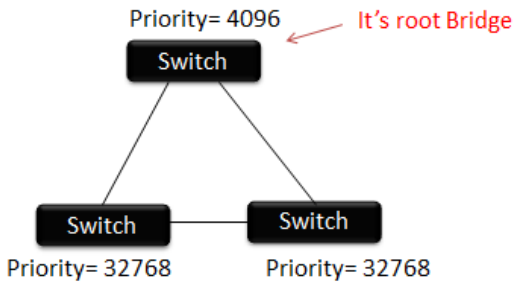
9. Spanning Tree

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.

9.1 Property

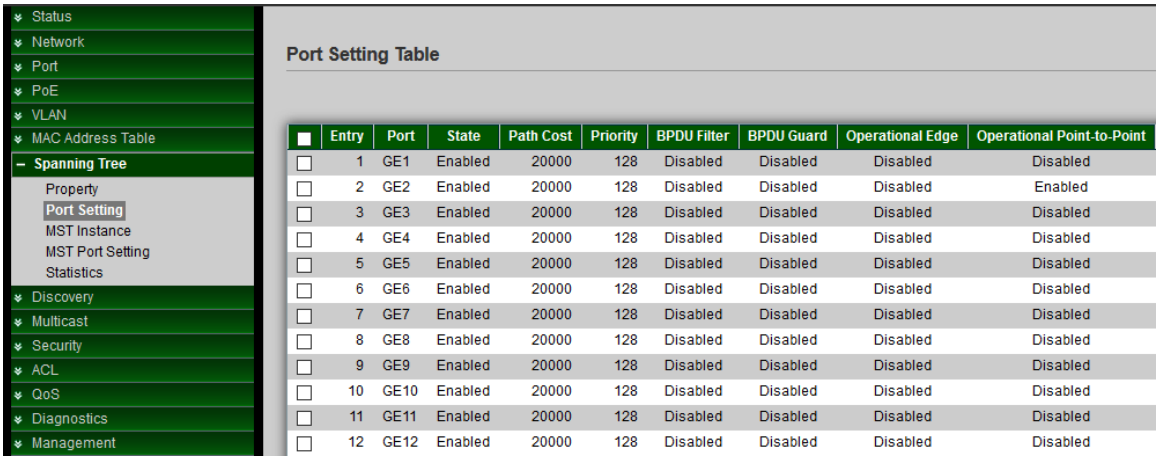


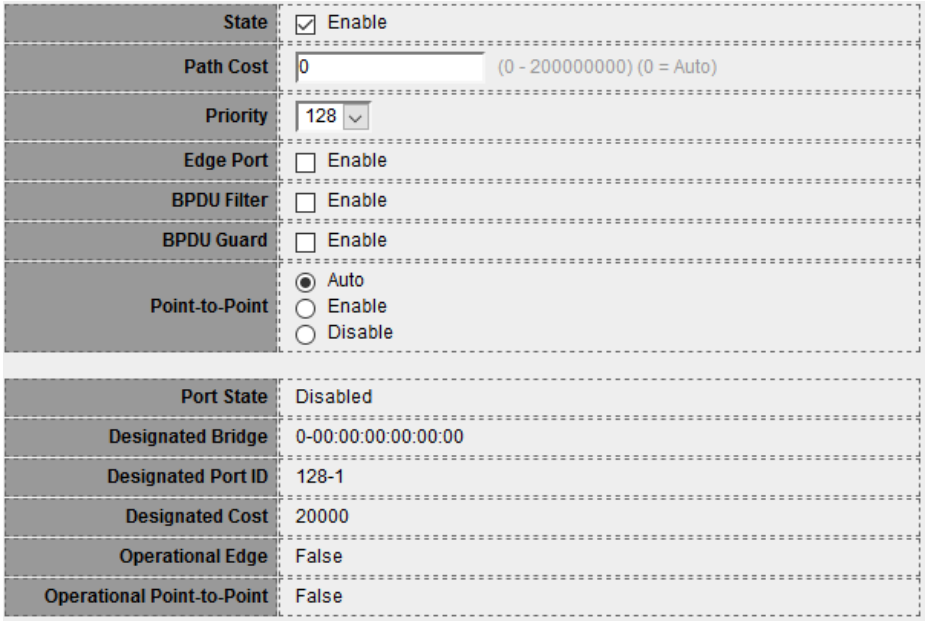
- **State:** Administrator can choose Enable or Disable this function.
- **Operation Mode:** Administrator can choose use STP or RSTP.
- **Path Cost:** Administrator can choose STP judgment use Path cost for Long or Short.
- **BPDU Handling:** When the Switch receives the BPDU frame, Administrator can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



- **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)*
- **TX hold Count:** When STP/RSTP use Tx hold count to configure the BPDU burst size by specifying the transmit hold count value. Default is before pausing for 6 second, administrator can set range 1~10.
- **Region Name:** If Switch set same Region will only process BPDU information in the same Region to calculate Topology. To determine if you are in the same Region, Switch will compare the 3 parameters in the spanning-tree mst configuration. All three parameters are the same Region. Administrator can use MAC address will set a name.
- **Revision:** Administrator every time change MST value, customary "Revision" to add 1 value.
- **Max. Hop:** Set max. hop of switch.

9.2 Port Setting



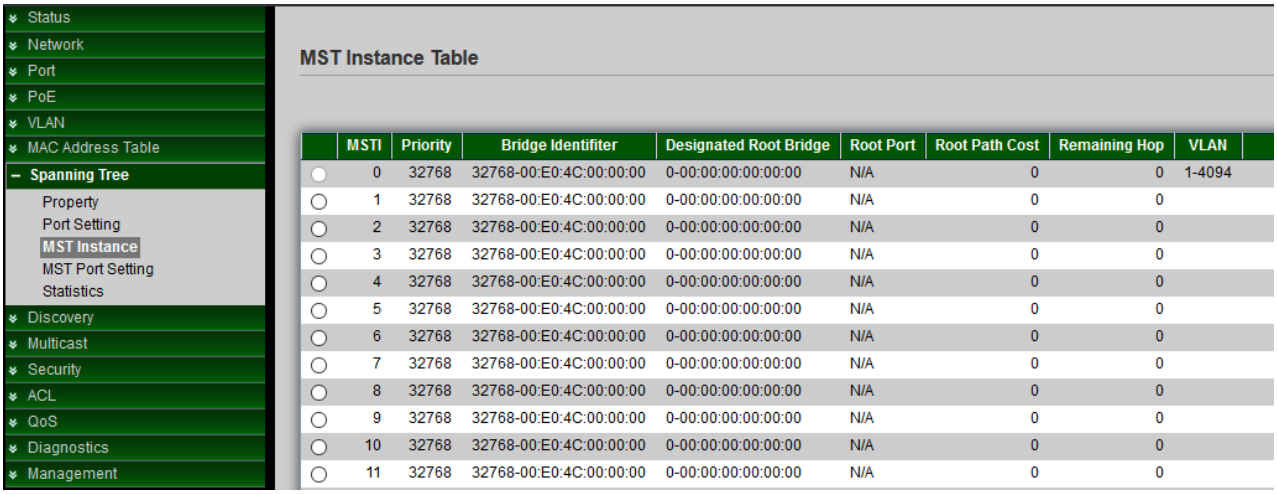


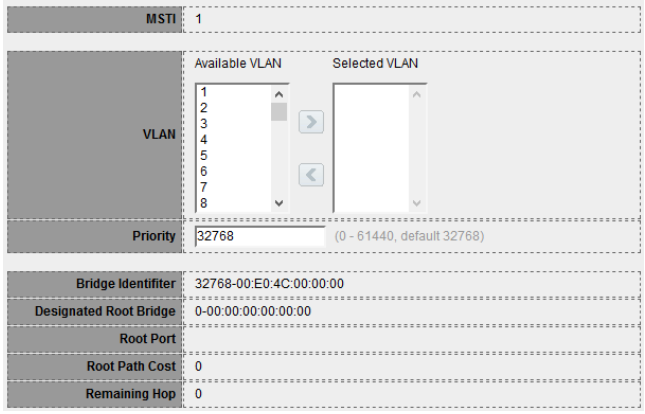
- **State:** Administrator can set Enable or Disable.
- **Path Cost:** Path Cost (1-200000000) This parameter is used determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost 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:** Use portfast, if this port connection end-station of device then administrator can enable the function will be can't receive BPDU.

- **BPDU Filter / BPDU Guard:** If this port has set Trunk function then this port can't be enabled Edge Port / BPDU Filter / BPDU Guard otherwise Trunk will not working normally.

9.3 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.

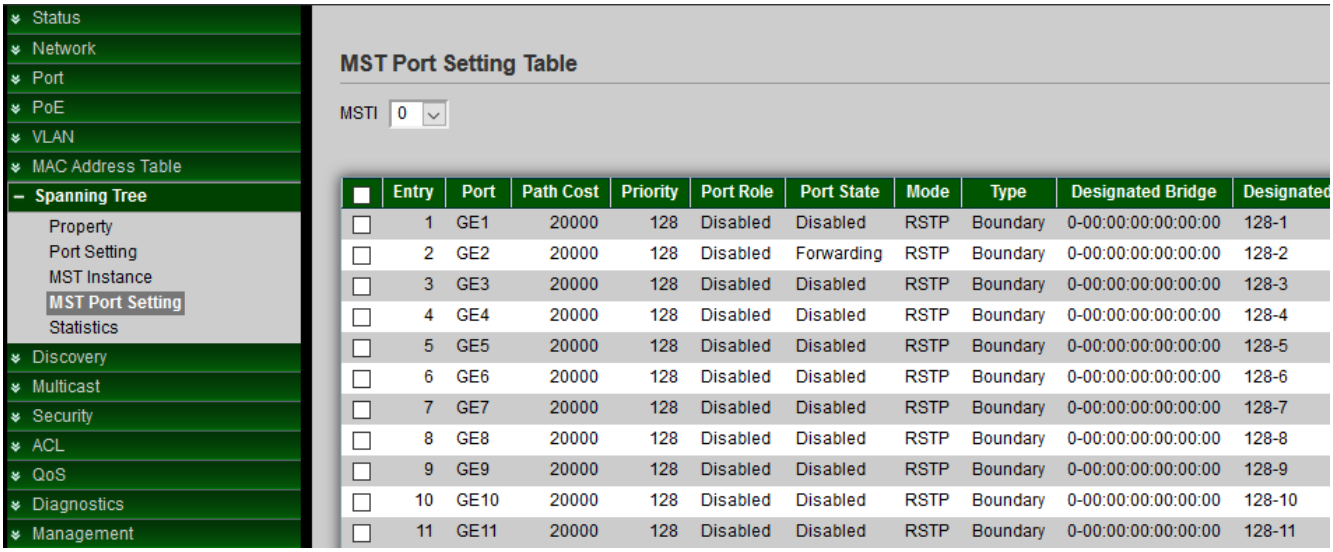




- **MSTI:** Select the MSTP instance to be configured.
- **VLAN:** Displays the VLANs mapped to the selected MSTP instance.
- **Priority:** Enter the priority of this bridge for the selected MST instance.
- **Bridge Identifier:** Displays the priority and MAC address of the Root Bridge for the selected 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.

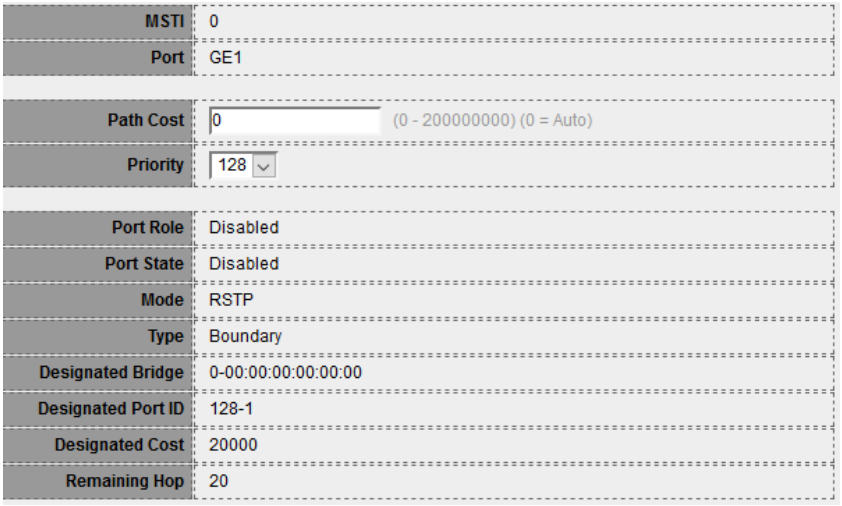
9.4 MST Port Setting

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.



Entry	Port	Path Cost	Priority	Port Role	Port State	Mode	Type	Designated Bridge	Designated
1	GE1	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-1
2	GE2	20000	128	Disabled	Forwarding	RSTP	Boundary	0-00:00:00:00:00:00	128-2
3	GE3	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-3
4	GE4	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-4
5	GE5	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-5
6	GE6	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-6
7	GE7	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-7
8	GE8	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-8
9	GE9	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-9
10	GE10	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-10
11	GE11	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-11

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.

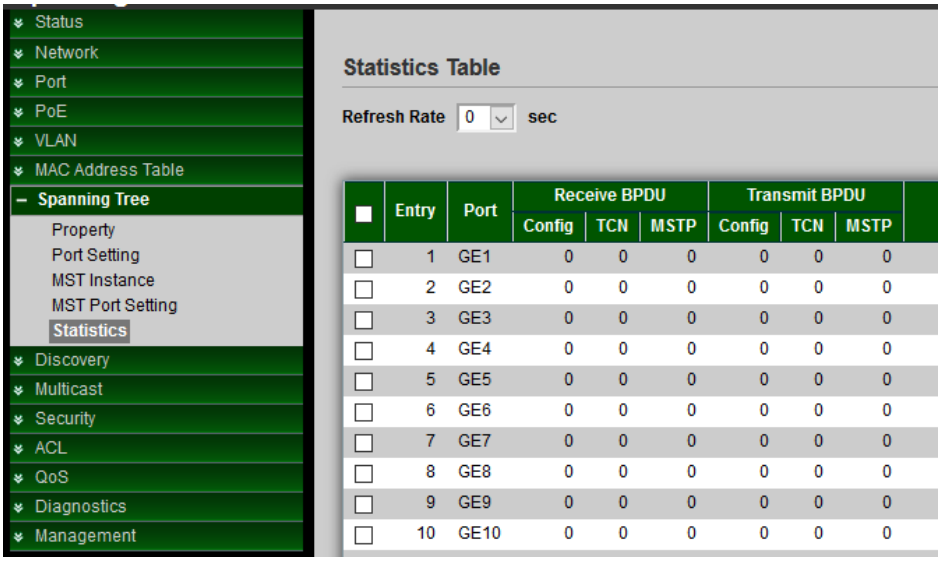


- **Path Cost:** Path cost default value is 0 (auto) depends on source device rate.
  If network is a loop occurs, the MST uses cost when selecting an interface to put in the forwarding state. Administrator can assign lower cost values to interfaces that you want selected first and higher cost values 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:** 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.
- **Port State:** Displays the MSTP status of the port.
- **Mode:** Displays the current Spanning Tree mode.
  - **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.
  - **Boundary:** A Boundary port attaches MSTP bridges to a LAN in an outlying region. If the port is a boundary port, it also indicates whether the device on the other side of the link is working in RSTP or STP mode.
  - **Internal:** The port is an internal port.
- **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.

9.5 Statistics

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



Port	GE1
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

10. 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.

10.1 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)

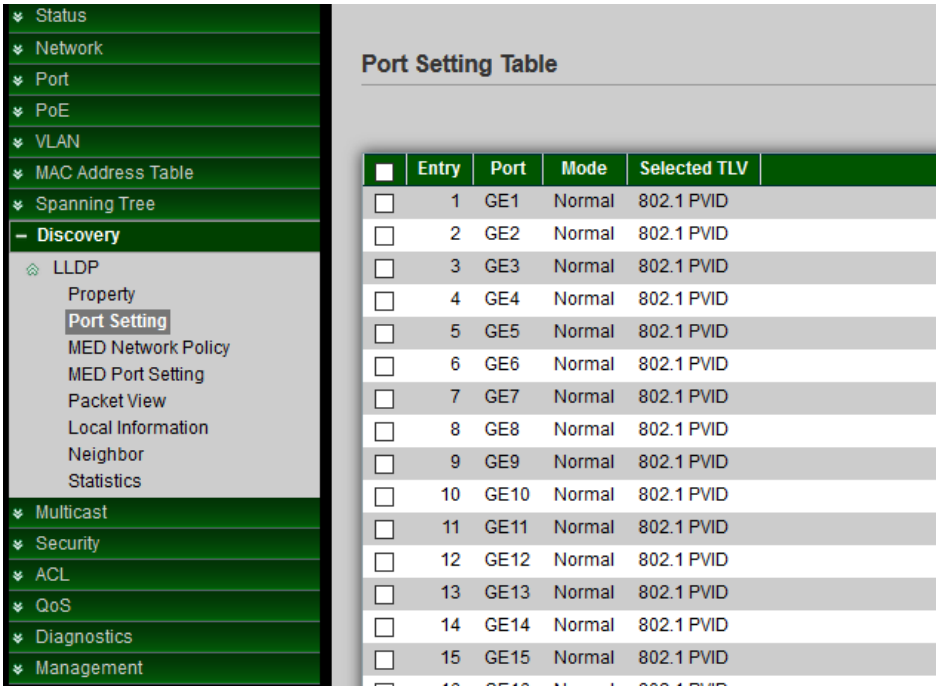
LLDP-MED	
Fast Start Repeat Count	3 (1 - 10, default 3)

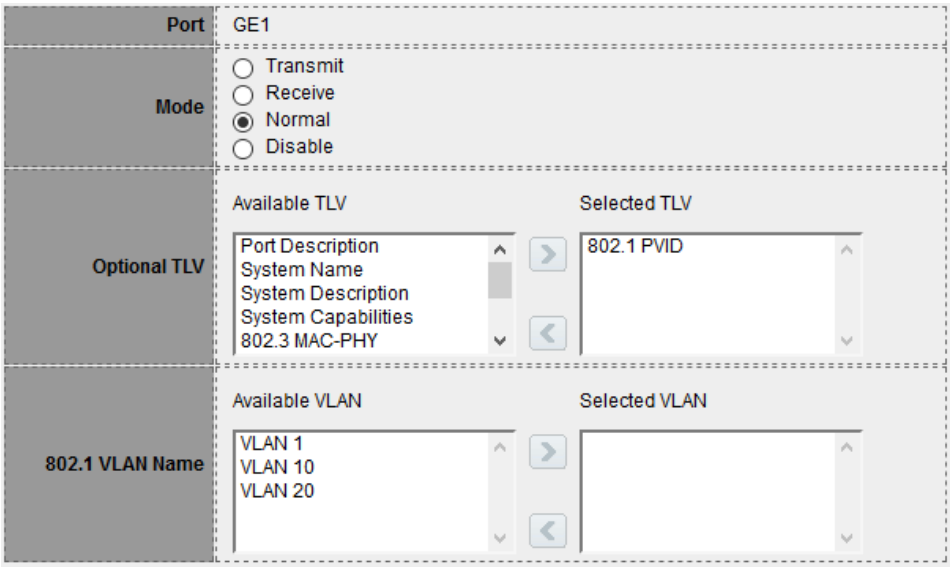
- **State:** Administrator can choose Enable or disable this LLDP function.
- **LLDP Handing:** If cancel checkbox then administrator can choose Filtering / Bridging / Flooding for LLDP handing.
- **TLV Advertise Interval:** Set LLDPDU Send Interval period (range 5-32760, default is 30)

- **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:** Set this value will be delayed for a period of time to be initialized, to avoid frequent changed when the port use LLDP mode, default value is 2.
- **Transmit Delay:** Set this value main purpose is to be local device to send LLDPDU delay time to a neighbor device. To avoid frequent changes in local configuration caused by frequent transmission of LLDPDUs, default value is 2.
- **Fast Start Repeat Count:** Administrator can set 1~10 number of Fast Start Repeat Count. This LLDP packets will sent when the mechanism is initialized. This event occurs when a new media endpoint device links to the switch, the system default is 3.

10.2 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.

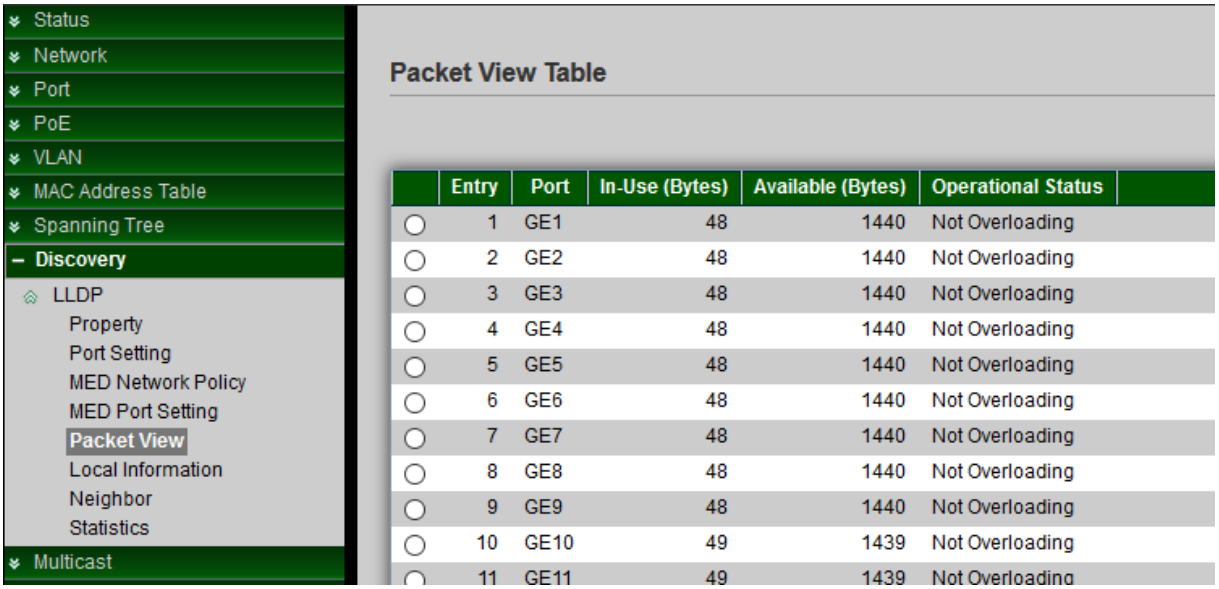




- **Mode:** Administrator can choose Transmit(TX) / Receive(RX) or Normal(TX+RX) and Disable, if choose disable will don't send and receive LLDPDU.
- **Optional TLV:** Administrator can be configuration information into different TLV, encapsulates LLDPDU and issued to the neighbor device.
- **802.1 VLAN Name:** Administrator can choose VLAN group.

10.3 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.



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)	10
Operational Status	Transmitted

Mandatory TLVs:

- **Size(Bytes):** Display total mandatory TLV byte size.
- **Operational Status:** If TLV is transmitting or overloaded will display on this table.

MED Capabilities

- **Size(Bytes):** Display total LLDP MED capabilities packets byte size.
- **Operational Status:** Display the LLDP MED capabilities packets whether were transmitted or they were overloaded.

MED Location

- **Size(Bytes):** Display total LLDP MED location packets byte size.
- **Operational Status:** Display the MED location packets whether were transmitted or they were overloaded.

MED Network Policy

- **Size(Bytes):** Display total LLDP MED Network Policy packets byte size.
- **Operational Status:** Display the MED Network Policy whether were transmitted or they were overloaded.

MED Inventory

- **Size(Bytes):** Display total LLDP MED Inventory packets byte size.
- **Operational Status:** Display the MED Inventory whether were transmitted or they were overloaded.

MED Extended Power via MDI

- **Size(Bytes):** Display total LLDP MED extended power via MDI packets byte size.
- **Operational Status:** Display the MED extended power via MDI whether were transmitted or they were overloaded.

802.3 TLVs

- **Size(Bytes):** Display total LLDP MED 802.3 TLVs packets byte size.
- **Operational Status:** Display the MED 802.3 TLVs whether were transmitted or they were overloaded.

Optional TLVs

- **Size(Bytes):** Display total LLDP MED optional TLVs packets byte size.
- **Operational Status:** Display the MED optional TLVs whether were transmitted or they were overloaded.

802.1 TLVs

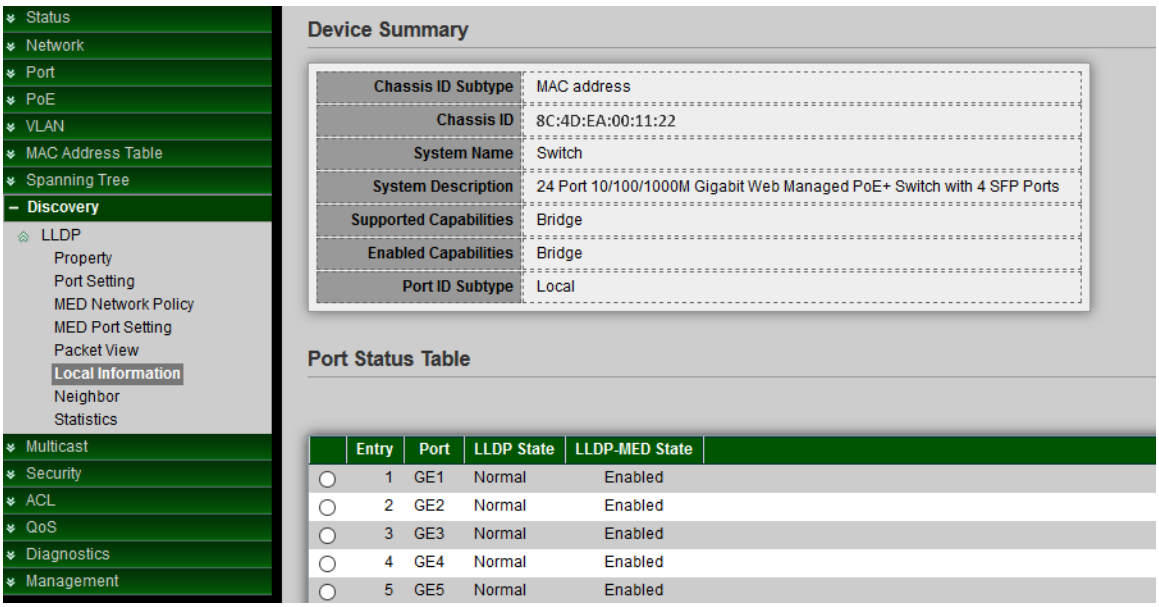
- **Size(Bytes):** Display total LLDP MED 802.1 TLVs packets byte size.
- **Operational Status:** Display the MED 802.1 TLVs whether were transmitted or they were overloaded.

Total

- **In-Use(Bytes):** Display total bytes of LLDP information.
- **Available(Bytes):** Display total available bytes left for additional LLDP information in each packet.

10.4 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.



Management Address Table			
Address Subtype	Address	Interface Subtype	Interface Number
0 results found.			

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

802.3 Detail	
802.3 Maximum Frame Size	N/A

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

Management Address Table: This table will display local LLDP agent.

- **Address Subtype:** Display management IP address type.
- Address: Returned address most appropriate for management use, typically a Layer 3 address.
- Interface Subtype: Numbering method used for defining the interface number.
- 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

- **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	N/A

- **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

- **Aggregation Capability**: Indicates whether the interface can be aggregated.
- **Aggregation Status**: Indicates whether the interface is aggregated.
- **Aggregation Port ID**: Advertised aggregated interface ID.

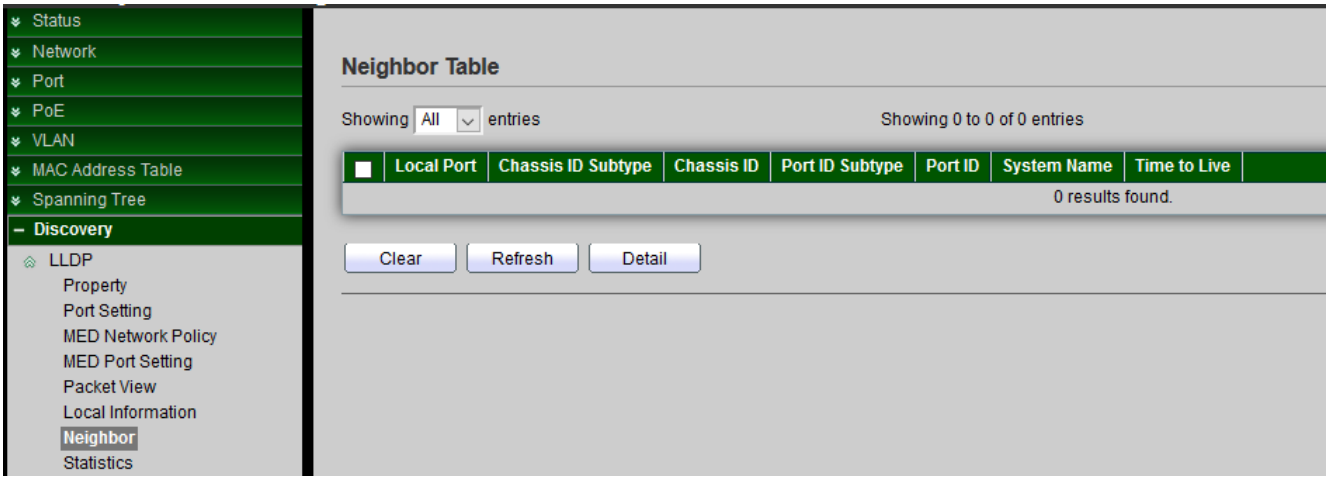
EMD Detail

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

- **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.
- **PoE Power Source**: Port power source.
- **PoE Power Priority:** Port power priority.
- **PoE Power Value**: Port power value.
- **Hardware Revision**: Hardware version.
- **Firmware Revision**: Firmware version.
- **Software Revision**: Software version.
- **Serial Number**: Device serial number.
- **Manufacturer Name:** Device manufacturer name.
- **Model Name:** Device model name.
- **Asset ID**: Asset ID.

10.5 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).



- **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.

10.6 Statistics

This page displays LLDP statistical information per port.

- **Port**: Port identifier.
- **Transmit Frames Total:** Total number of transmitted frames.
- **Receive Frames:**
  - **Total:** Number of received frames.
  - **Discarded:** Total number of received frames that were discarded.
  - **Errors:** Total number of received frames with errors.
- **Receive TLV:**
  - **Discarded:** Total number of received TLV that were discarded.
  - **Unrecognized:** Total number of received TLV that was unrecognized.
- **Neighbor Timeout:** Number of neighbor Timeout on the port.

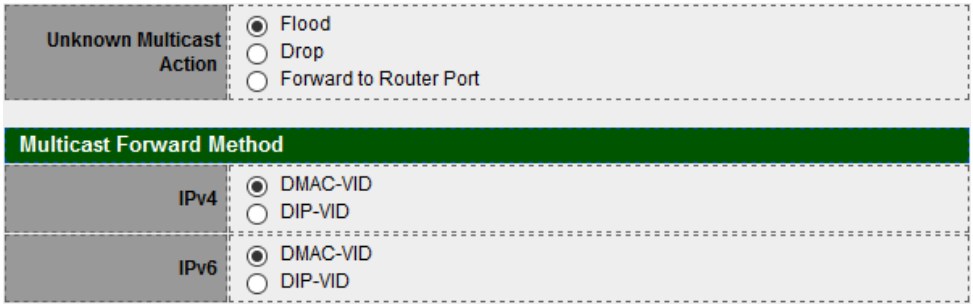
11. Multicast

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

11.1 General

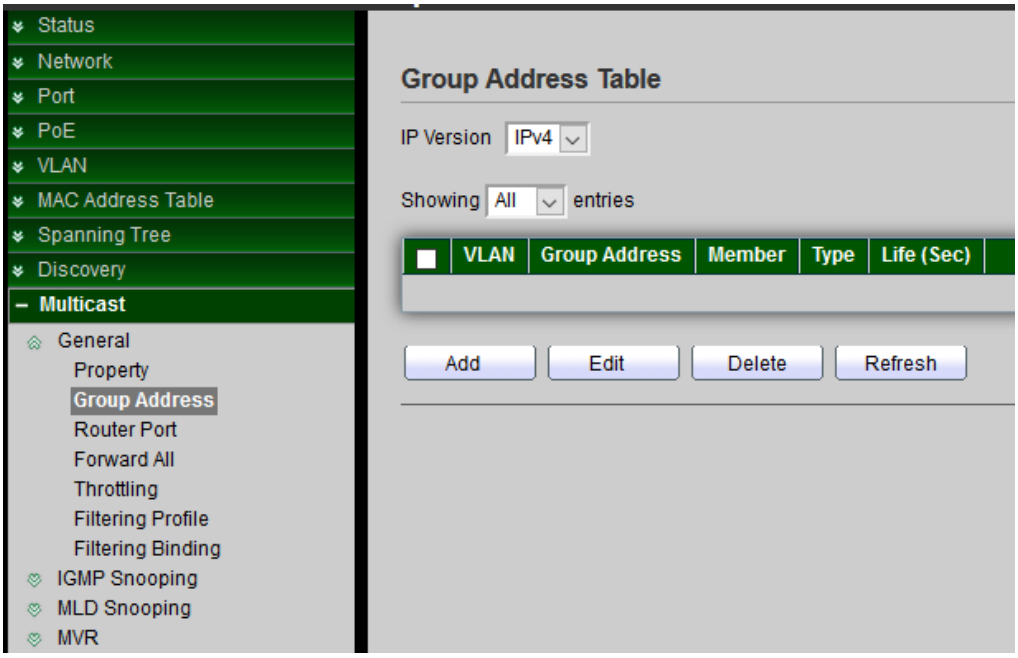
11.1.1 Property

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.



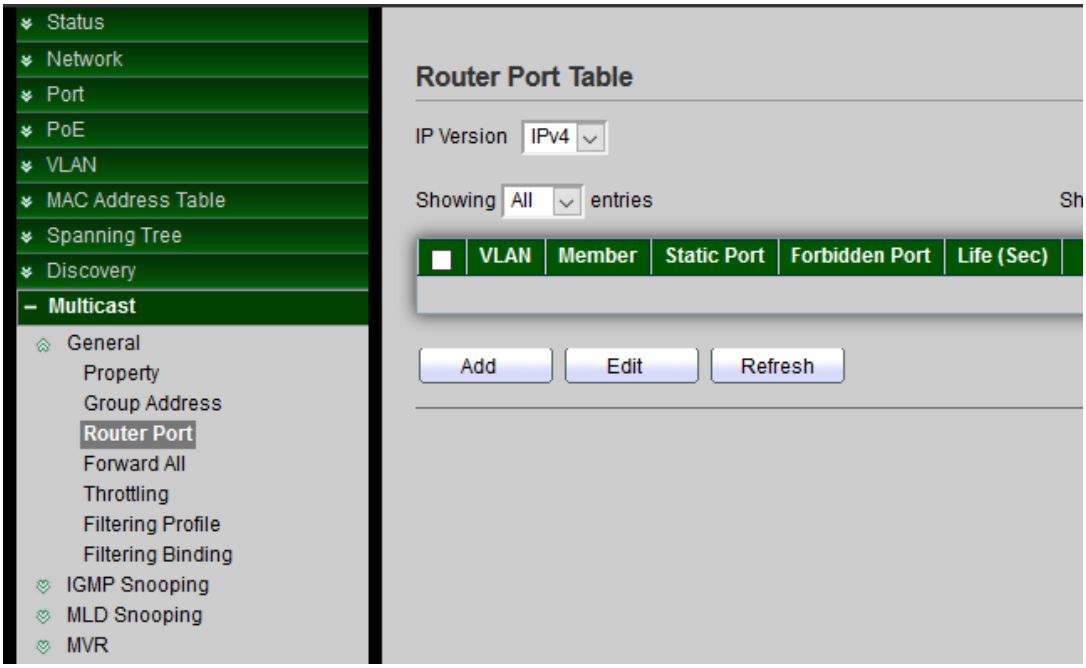
11.1.2 Group Address

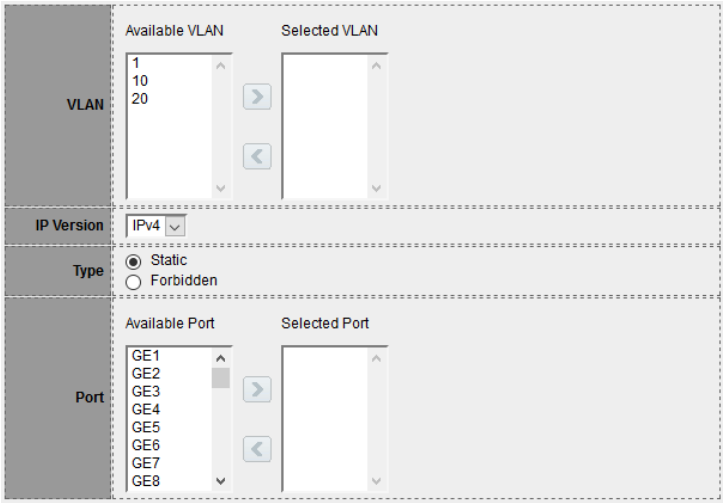
The multicast address range is 224.0.0.0 to 239.255.255.255 and forms the Class D range which is made up of the high order bits 1110 followed by the 28 bit multicast group ID. There is no subletting with these Class D addresses. A multicast group can have a permanently-assigned address or the group may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



11.1.3 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 MRouter(s) can, in turn; forward the Multicast streams and propagate the registration messages to other subnets.



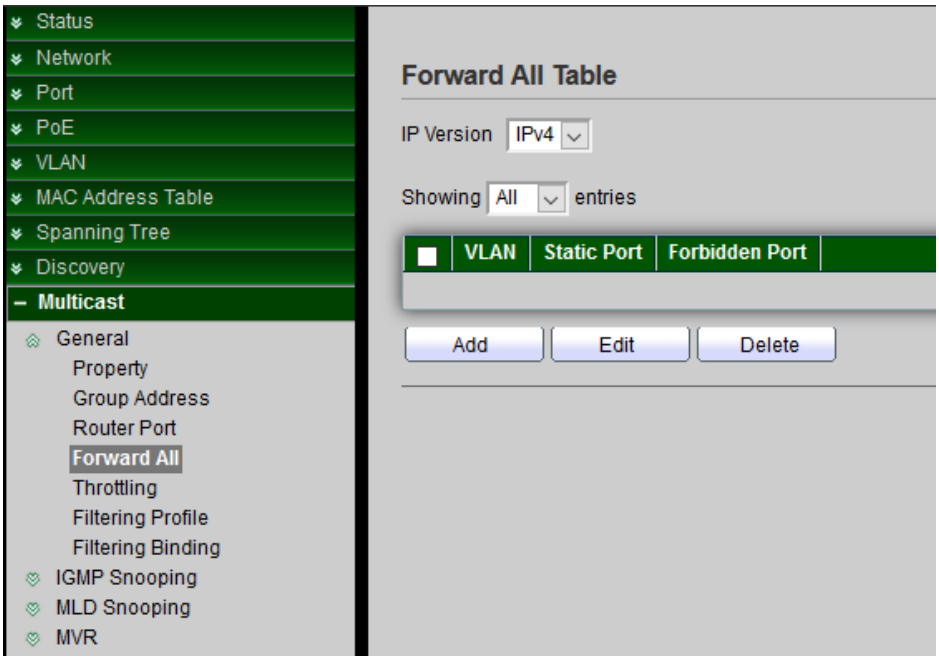


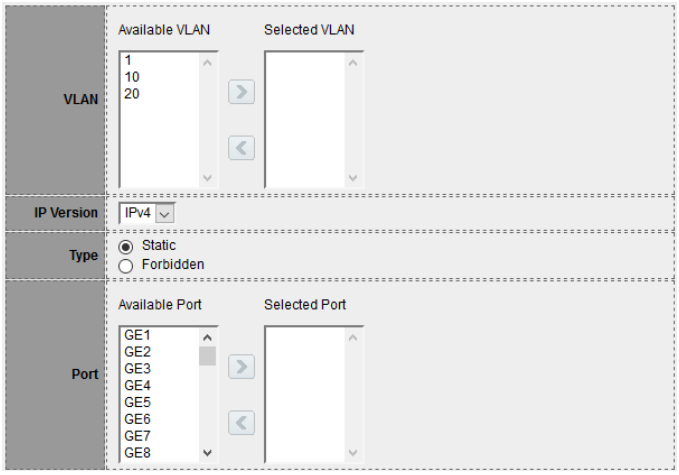
- **VLAN:** Select VLAN in available VLAN table.
- **IP Version:** Select either **Version 4** or **Version 6** that the Multicast router supports.
- **Type:** Select the type for the Static or Forbidden.
  - **Static:** The port is statically configured as a Multicast router port.
  - **Forbidden:** This port is not to be configured as a Multicast router port, even if IGMP or MLD queries are received on this port.
- **Port:** Select ports member.

11.1.4 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.

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

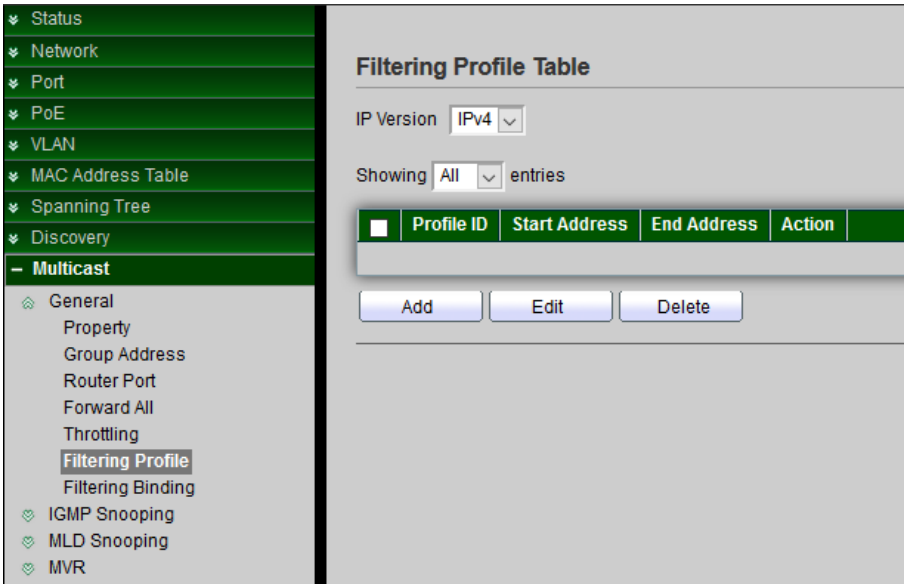




- **VLAN:** Select VLAN in available VLAN table.
- **IP Version:** Select either **Version 4** or **Version 6** that the Multicast router supports.
- **Type:** Select the type for the Static or Forbidden.
  - **Static:** The port is statically configured as a Multicast router port.
  - **Forbidden:** This port is not to be configured as a Multicast Router port, even if IGMP or MLD queries are received on this port.
- **Port:** Select ports member.

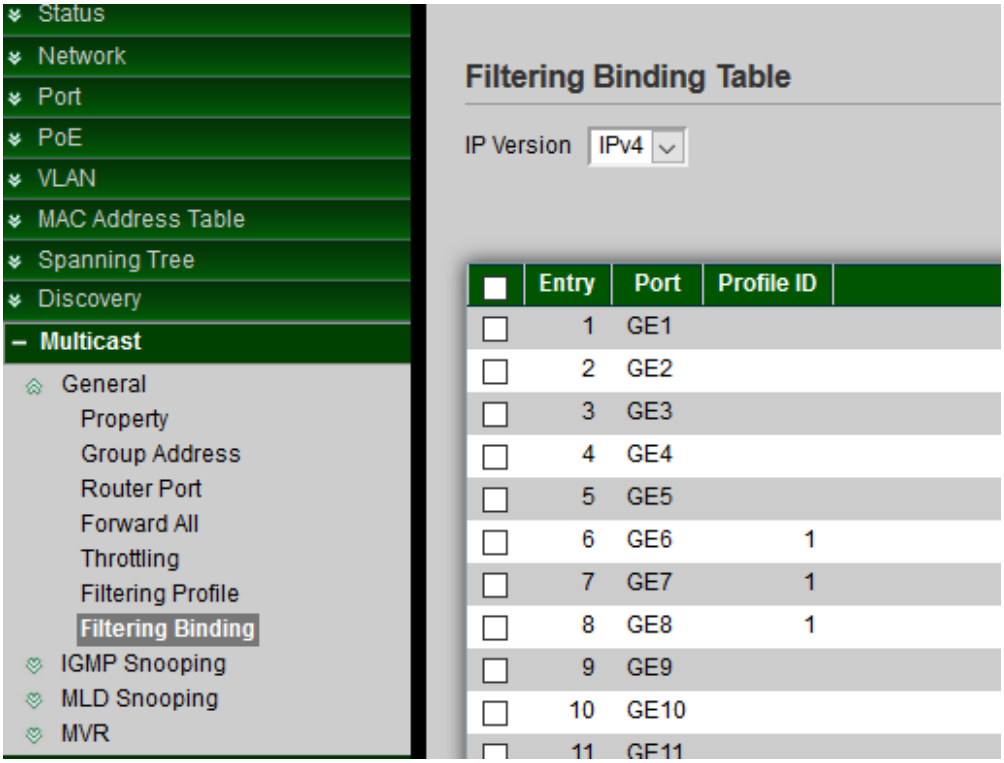
11.1.5 Filtering Profile

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



11.1.6 Filtering Binding

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

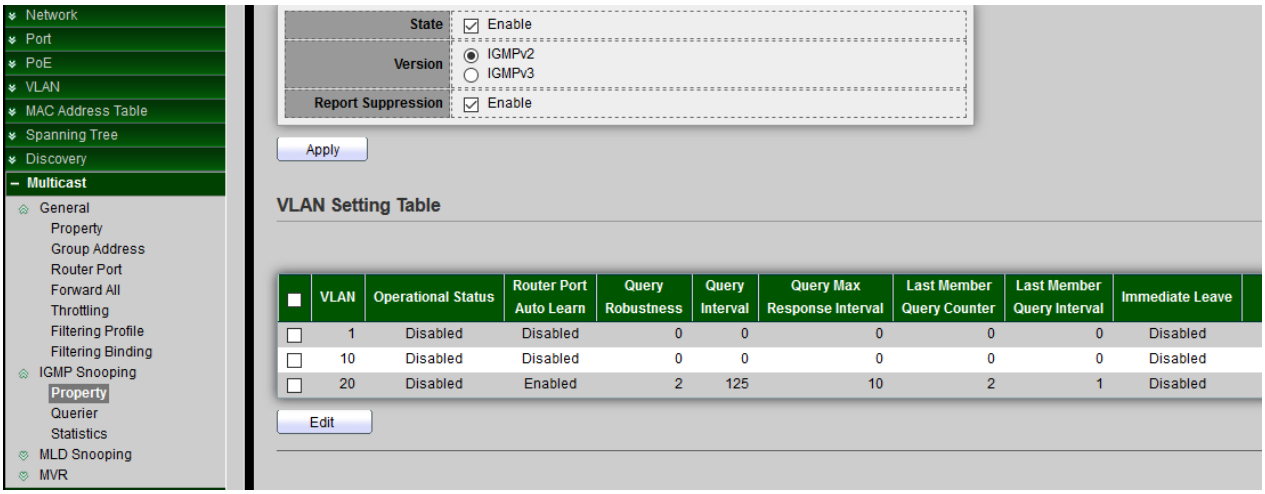


11.2 IGMP Snooping

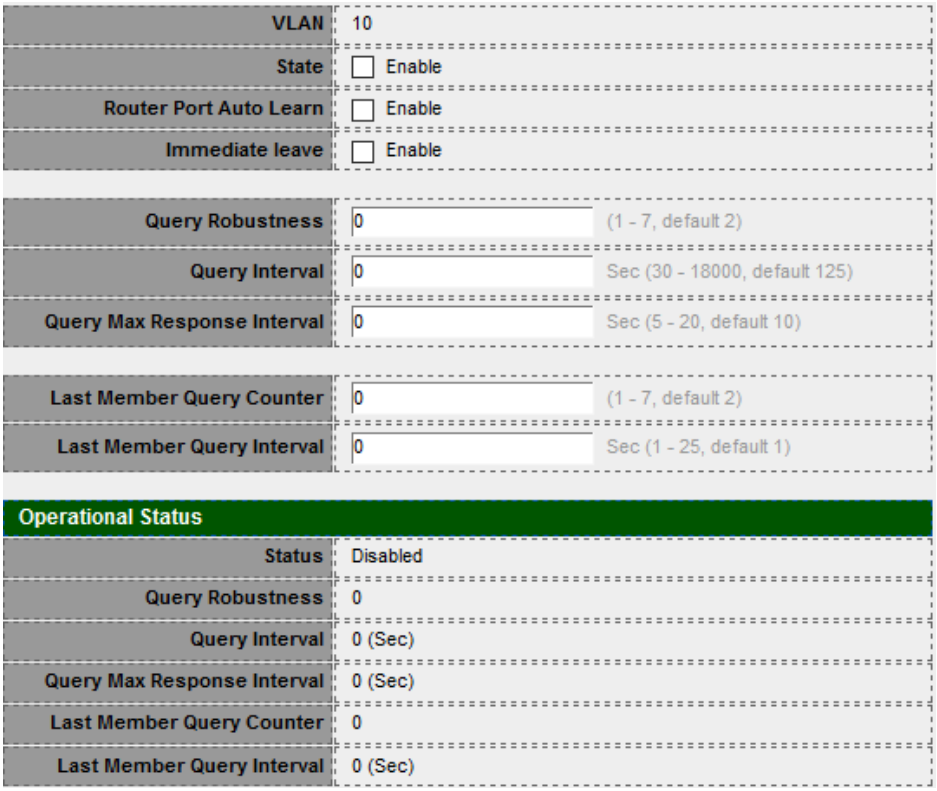
IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast 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.

11.2.1 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.



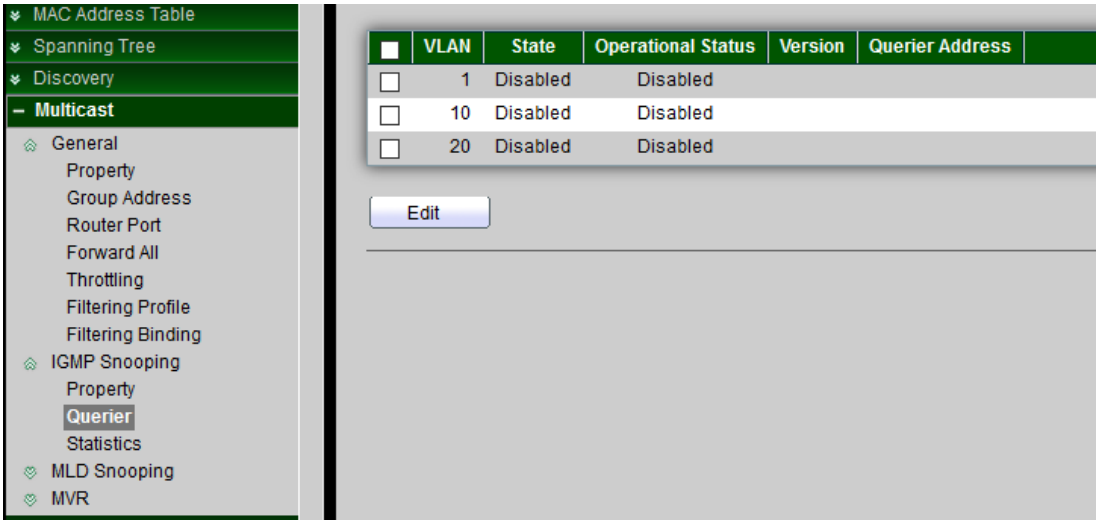
- **State:** Administrator can select Enable or Un-enable.
- **Version:** Select either IGMPv2 or IGMPv3.
- **Report Suppression:** Enable or disable IGMP report suppression. If administrator select disabling this feature will forward all IGMP reports to Multicast routers.

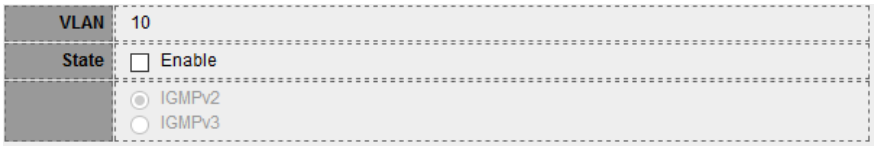


- **State:** Administrator can choose Enable or Disable this function.
- **Router Port Auto Learn:** Administrator can enable Router Port Auto Learn.
- **Immediate leave:** Immediate leave for the specified VLAN. Administrator enable immediate leave will host tracking is started, which allows the switch to track the hosts that send membership reports. The switch can then determine when the last host on an interface leaves the multicast group and immediately stop forwarding multicast traffic to the interface.
- **Query Robustness:** Administrator can configure IGMP Snooping for Query Robustness.
- **Query Interval**: Administrator can configure IGMP Snooping for Query Interval.
- **Query Max Response Interval:** Administrator can configure IGMP Snooping for Query Max Response Interval
- **Last Member Query Counter:** The number of times, from 1 through 7, that the router sends group- or group-source-specific queries upon receipt of a message indicating a leave.
- **Last Member Query Interval**: Last Member Query Interval set 1 is average of about 150 milliseconds. Administrator can configure value 1~25. This Last Member Query Interval is in order to avoid the impact of higher rates of IGMP leave messages.
- **Operational Status:** Display IGMP snooping configuration information.

11.2.2 Querier

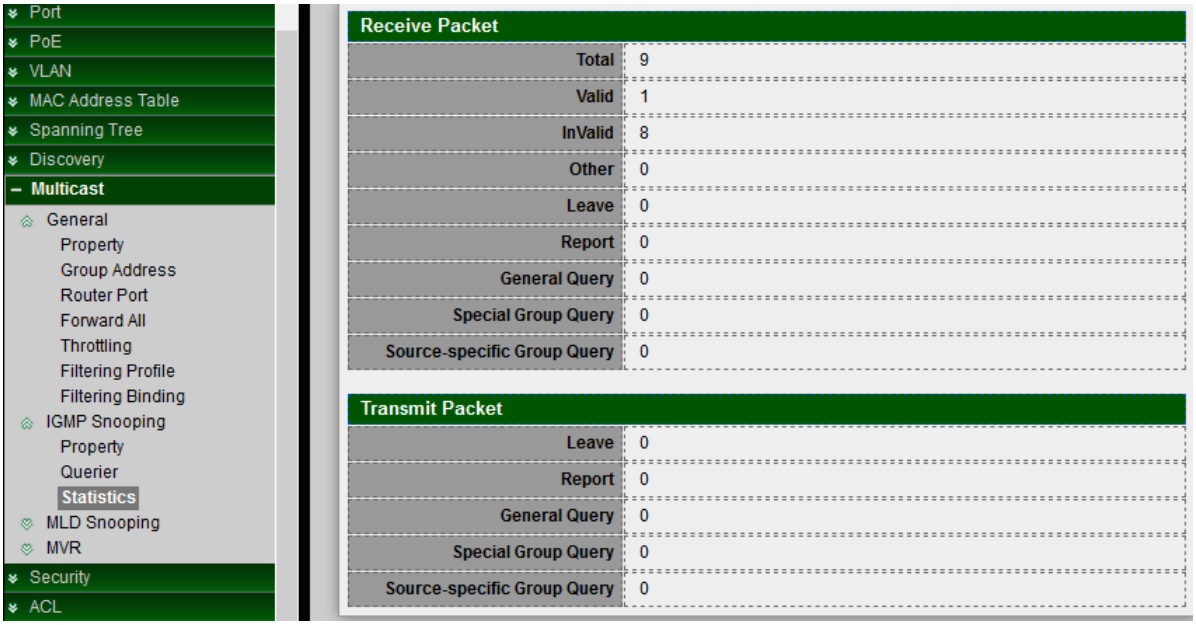
Administrator can choose created VLAN to enable or disable the IGMP Snooping query function. When select checkbox and click "**Edit**" button will be go to set IGMP Snooping version, this function can get IGMP Snooping query device regularly to VLAN local segments in all hosts and routers send IGMP Snooping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





11.2.3 Statistics

Display Receive / Transmit Packet information of IGMP snooping.

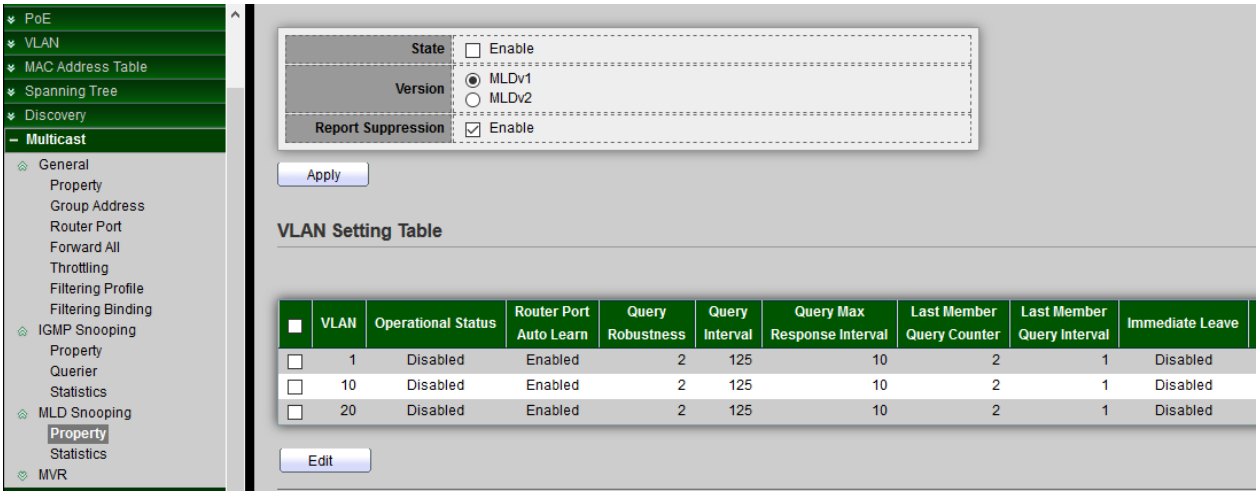


11.3 MLD Snooping

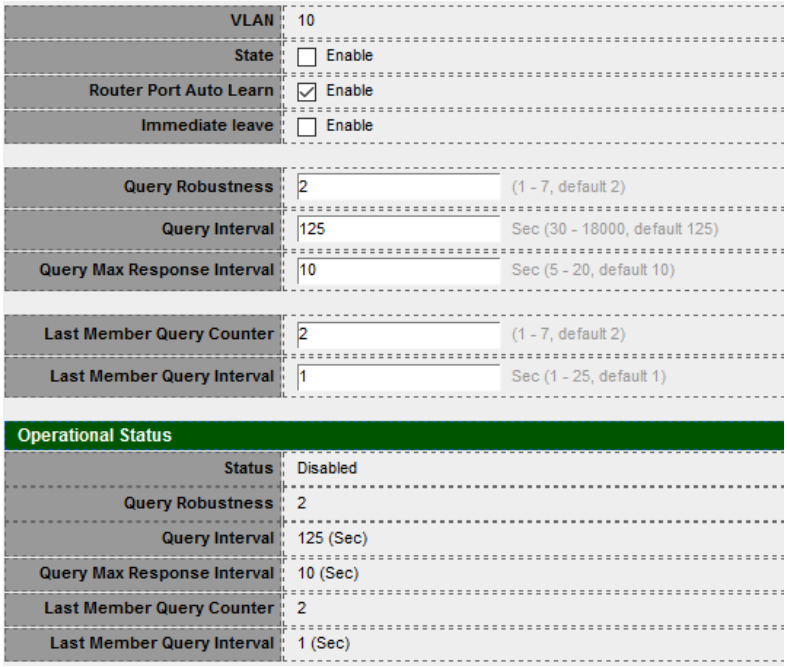
The function support selective Multicast forwarding (IPv6), MLD Snooping must be enabled globally and for each relevant VLAN. The switch supports MLD Snooping on both static and dynamic VLANs. Hosts use the MLD protocol to report their participation in Multicast sessions, and the switch uses MLD Snooping 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.

11.3.1 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.



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



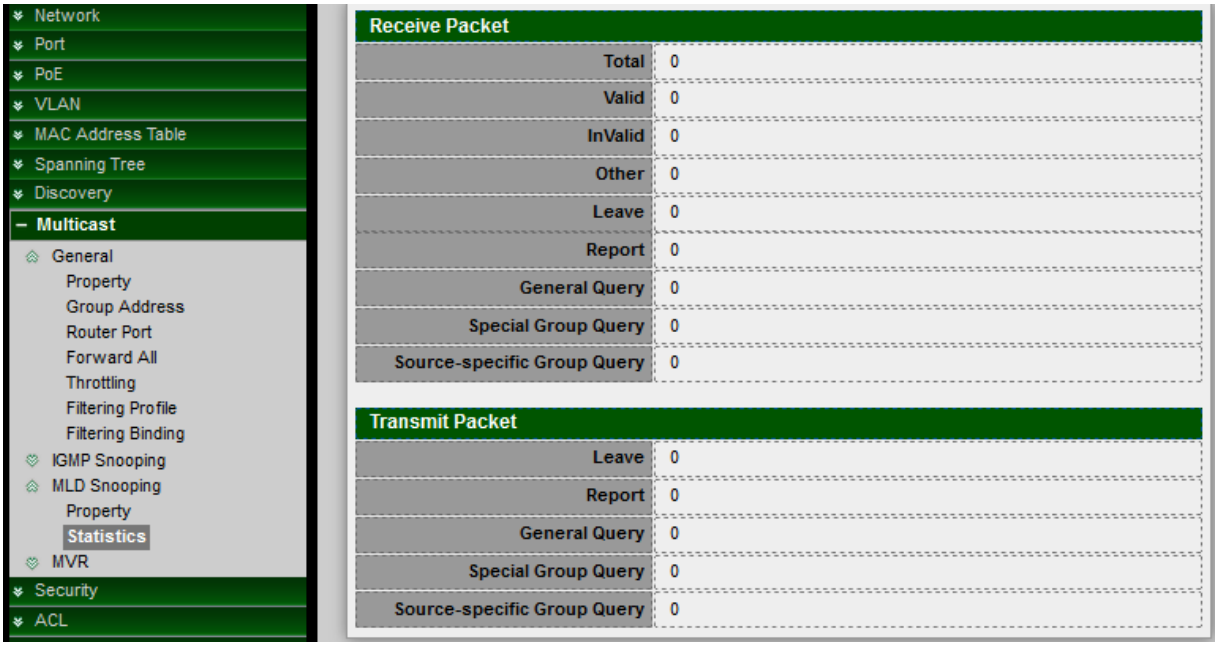
VLAN	10
State	☐ Enable
Router Port Auto Learn	☑ Enable
Immediate leave	☐ Enable
Query Robustness	2 (1 - 7, default 2)
Query Interval	125 Sec (30 - 18000, default 125)
Query Max Response Interval	10 Sec (5 - 20, default 10)
Last Member Query Counter	2 (1 - 7, default 2)
Last Member Query Interval	1 Sec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

- **State:** Administrator can Enable or Un-Enable MLD Snooping on the VLAN. The switch monitors network traffic to determine which hosts have asked to be sent Multicast traffic. The switch performs MLD Snooping only when MLD Snooping is enabled globally and on the VLAN.
- **Router Ports Auto Learn**: Enable or Un-Enable auto learning of the Multicast router.
- **Query Robustness**—Enter the robustness variable value to be used if the switch cannot read this value from messages sent by the elected Querier.
- **Query Interval**—Enter the query interval value to be used by the switch if the switch cannot derive the value from the messages sent by the elected Querier.
- **Query Max Response Interval**—Enter the query maximum response delay to be used if the switch cannot read the maximum response time value from general queries sent by the elected Querier.
- **Last Member Query Counter**—Enter the last member query count to be used if the switch cannot derive the value from the messages sent by the elected Querier.
- **Last Member Query Interval**—Enter the maximum response delay to be used if the switch cannot read maximum response time value from group-specific queries sent by the elected Querier.

11.3.2 Statistics

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

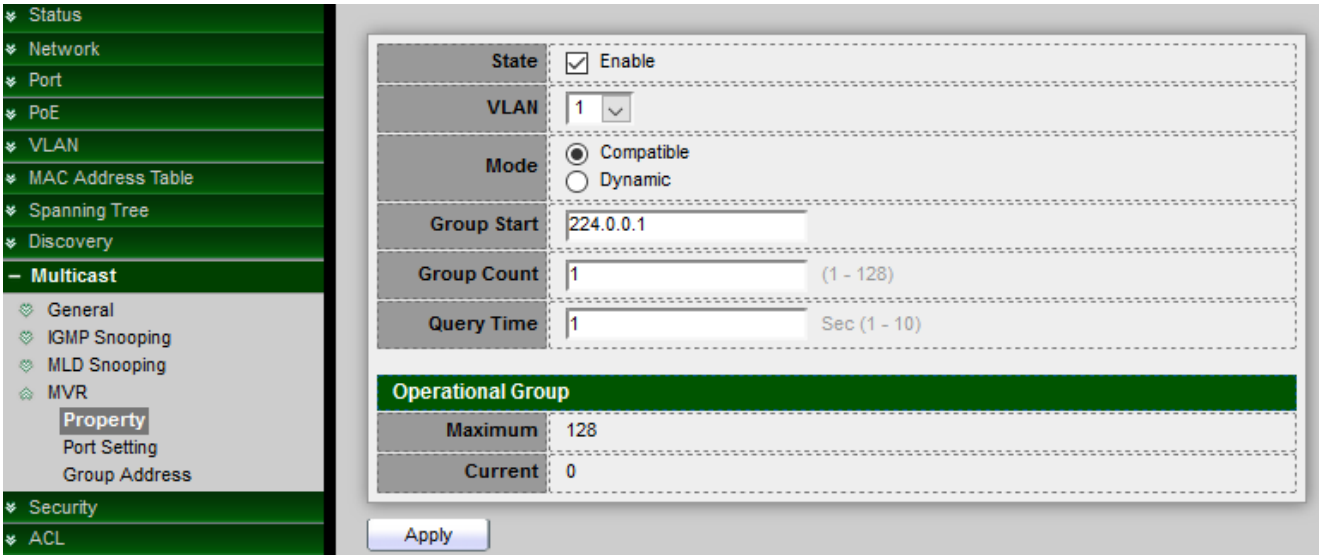


11.4 MVR

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.

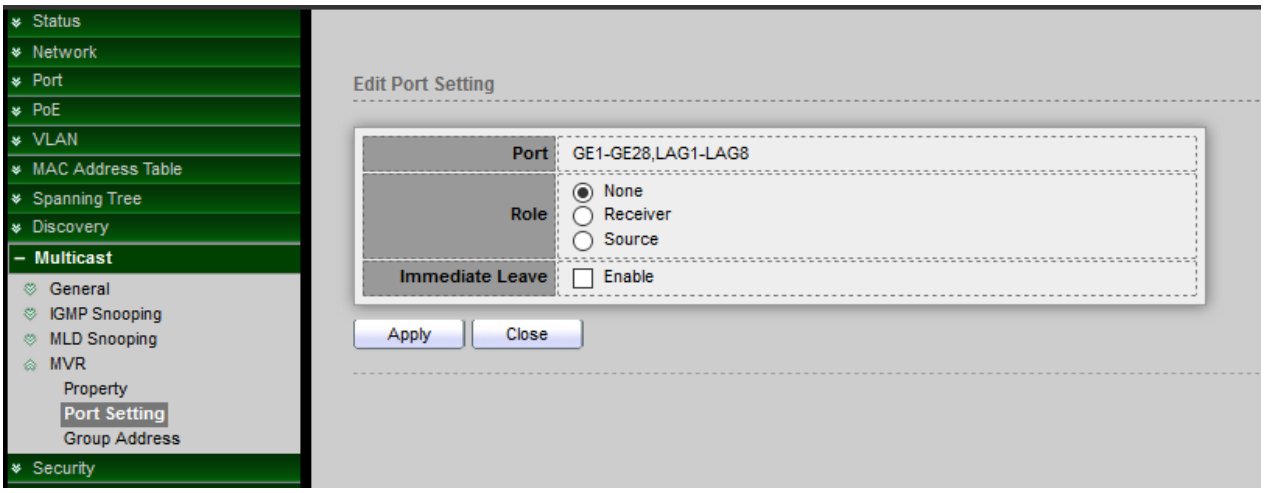
11.4.1 Property



- **State:** Administrator can Enable or Un-Enable MVR function.
- **VLAN:** Select VLAN ID.
- **Mode:** Select use Compatible or Dynamic mode.
- **Group Start:** Administrator can set range is 224.0.0.0 to 239.255.255.255.
- **Group 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:** 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.

11.4.2 Port Setting

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

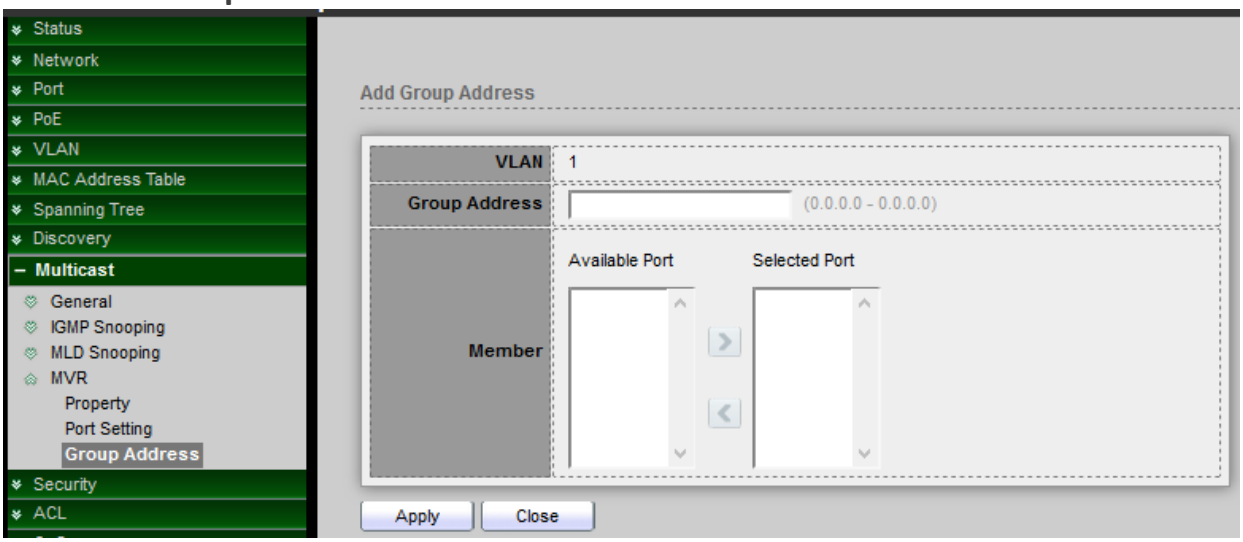


- **Receiver:** Configures a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group, either statically or by using IGMP leave and join messages. Receiver ports cannot belong to the multicast VLAN.
- **Source:** 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:** 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.

11.4.3 Group Address



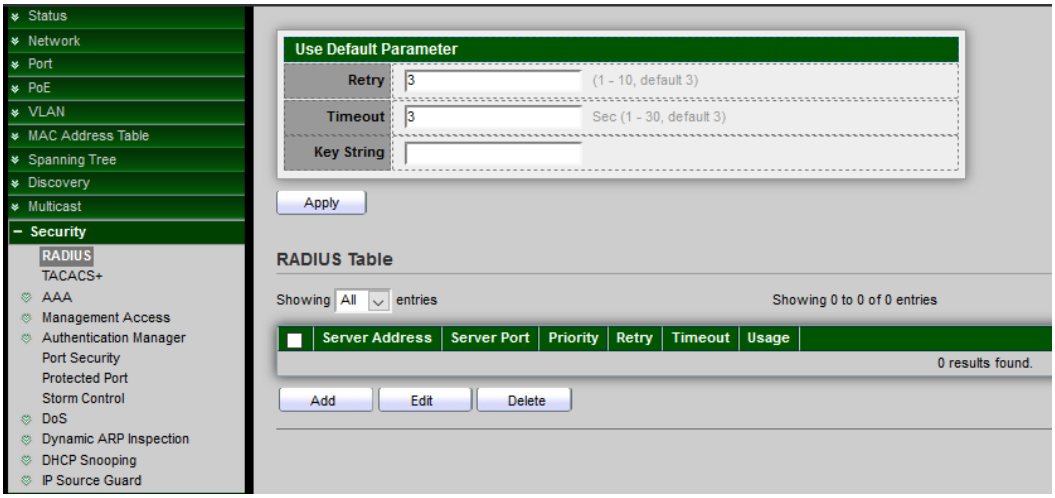
- **Group Address:** Administrator can set MVR multicast group addresses on the switch. (The address range is 224.0.0.0 to 239.255.255.255)
- **Member:** Select Ports in the MVR Group.

12. Security

12.1 RADIUS

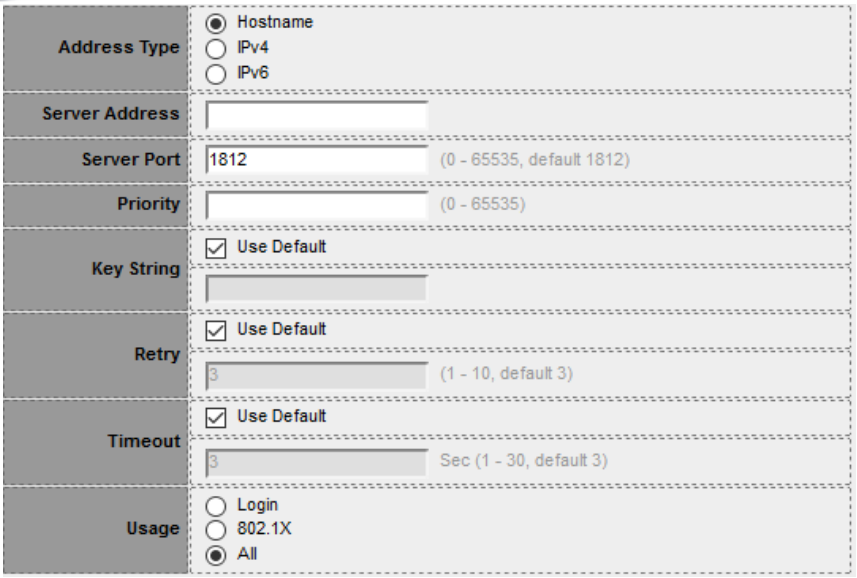
Network architecture can establish a Remote Authorization login Service (RADIUS) server to provide a centralized 802.1X or MAC-based network access control for all of its devices. This switch can act as a RADIUS client that uses the RADIUS server to provide centralized security and authorization and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

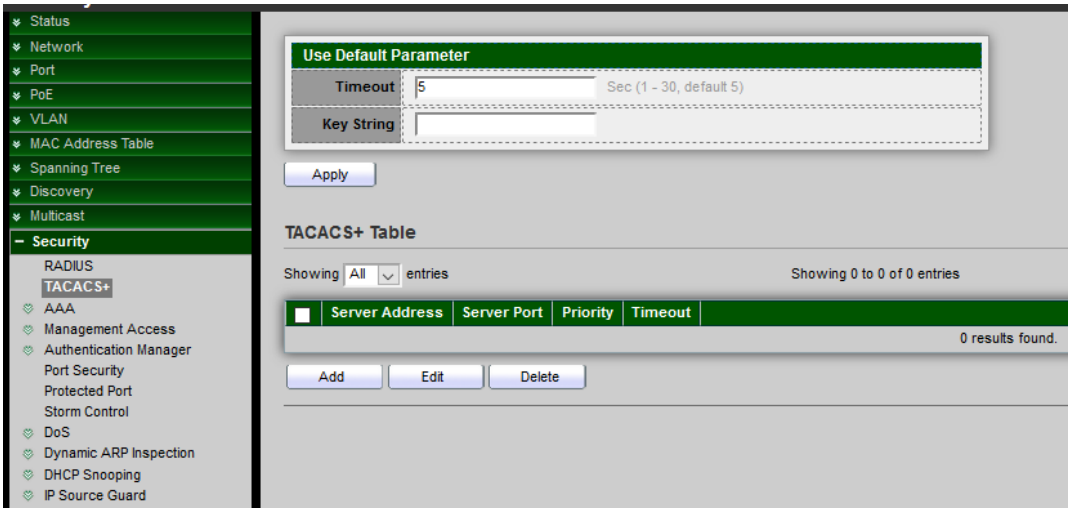
- **Retry:** Enter the number of transmitted requests that are sent to the RADIUS server before a failure is considered to have occurred. Default is 3
- **Timeout:** Enter the number of seconds that the switch waits for an answer from the RADIUS server before retrying the query, or switching to the next server. Default is 3
- **Key String:** 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.



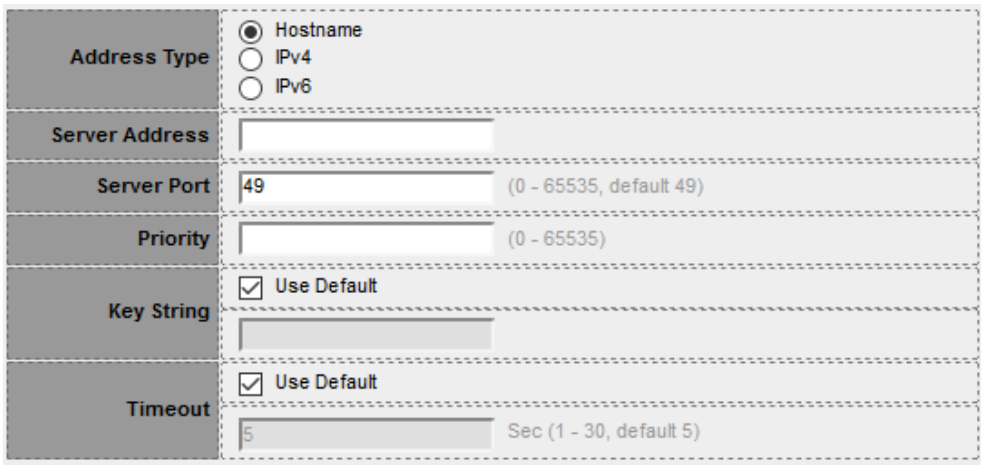
- **Address Type:** Select IP Version 4 / 6 or use Hostname type.
- **Server Address:** Please enter the IP address or hostname of the RADIUS server.
- **Server Port:** Set port of RADIUS server.
- **Priority:** Administrator can enter the priority of the server. The priority determines the order that the switch attempts to contact the servers to authenticate users. The switch first starts with the highest priority server. 0 is the high priority.
- **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.

12.2 TACACS+

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



- **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.
  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.



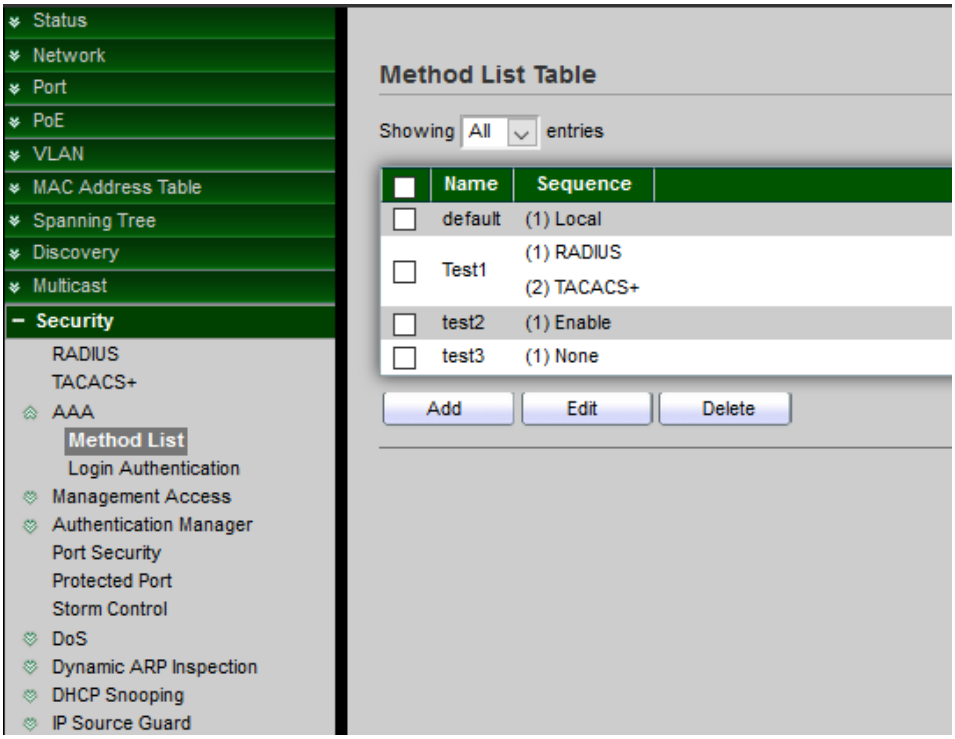
- **Address Type:** Select IP Version 4 / 6 or use Hostname type.
- **Server Address:** Please enter the IP address or hostname of the TACACS+ server.
- **Server Port:** Set port of RADIUS server.

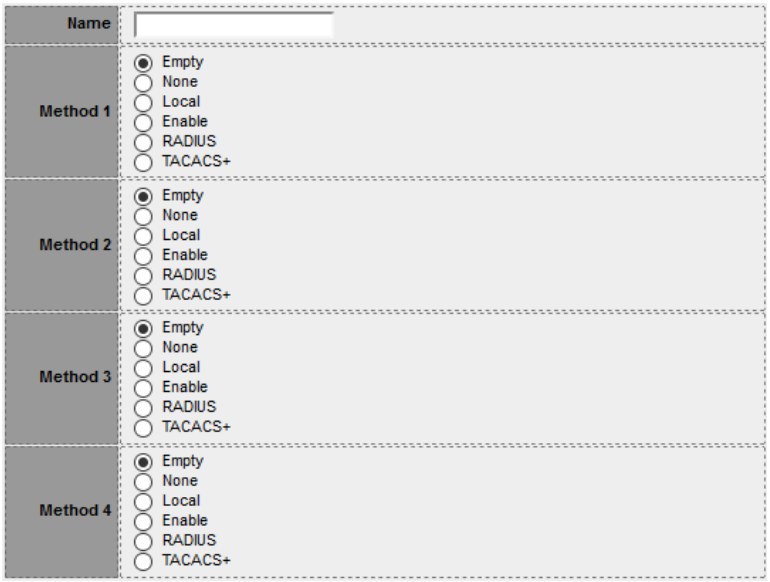
- **Priority:** Administrator can enter the priority of the server. The priority determines the order that the switch attempts to contact the servers to authenticate users. The switch first starts with the highest priority server. 0 is the high priority.
- **Key String:** Administrator can select user 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:** Select User Defined to enter the number of seconds that the switch waits for an answer from the TACACS+ server before retrying the query or switching to the next server, or select Use Default to use the default value.

12.3 AAA

12.3.1 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+

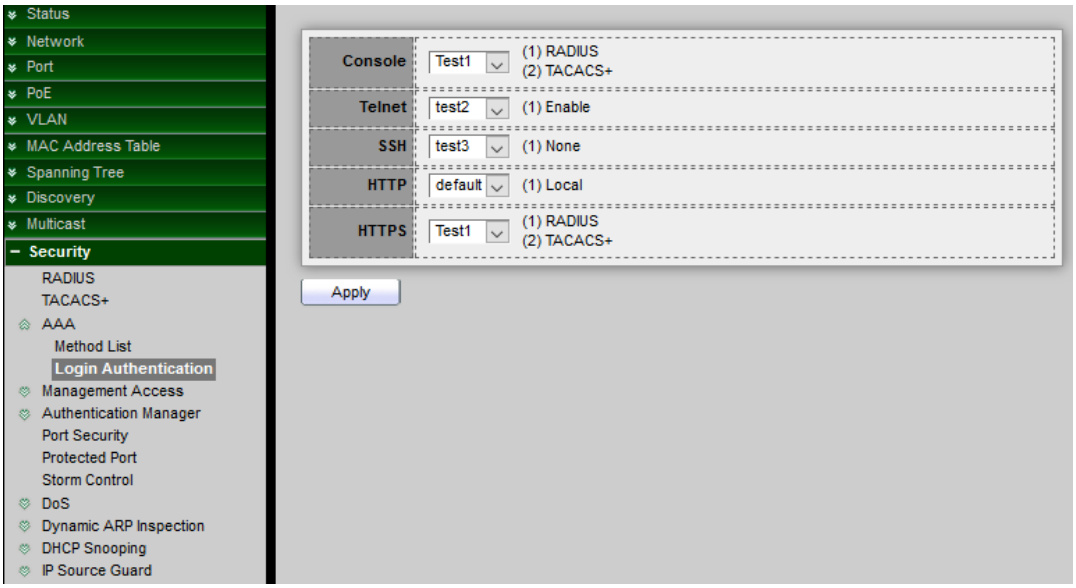




- **Empty:** Close authentication type of this method.
- **None**: Don't use authentication.
- **Local:** System login account use local system authentication in "menu -> management -> user Account".
- **Enable:**
- **RADIUS:** System login account use remote RADIUS server authentication.
- **TACACS+**: System login account use remote TACACS+ server authentication.

12.3.2 Login Authentication

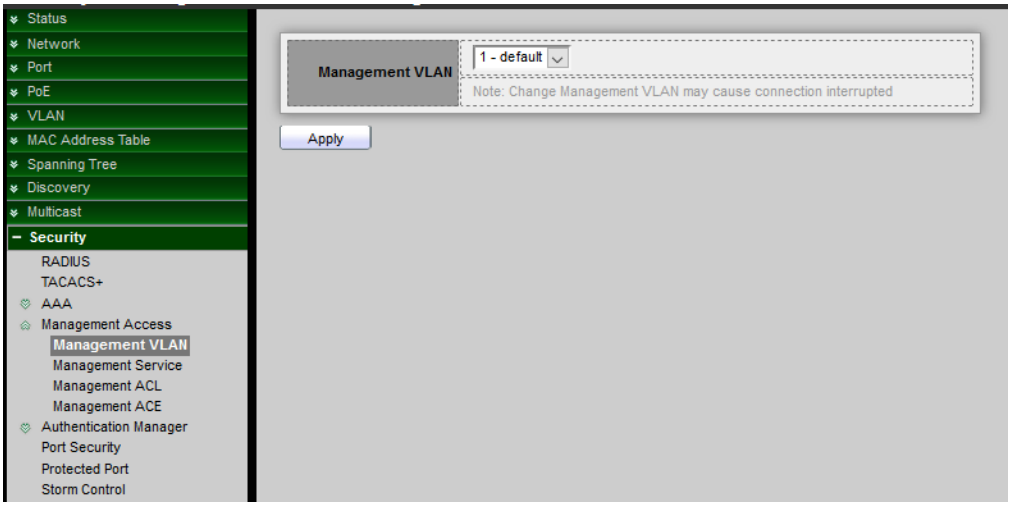
When administrator has created security groups in "AAA➔method" then administrator can select different security group in service port.



12.4 Management Access

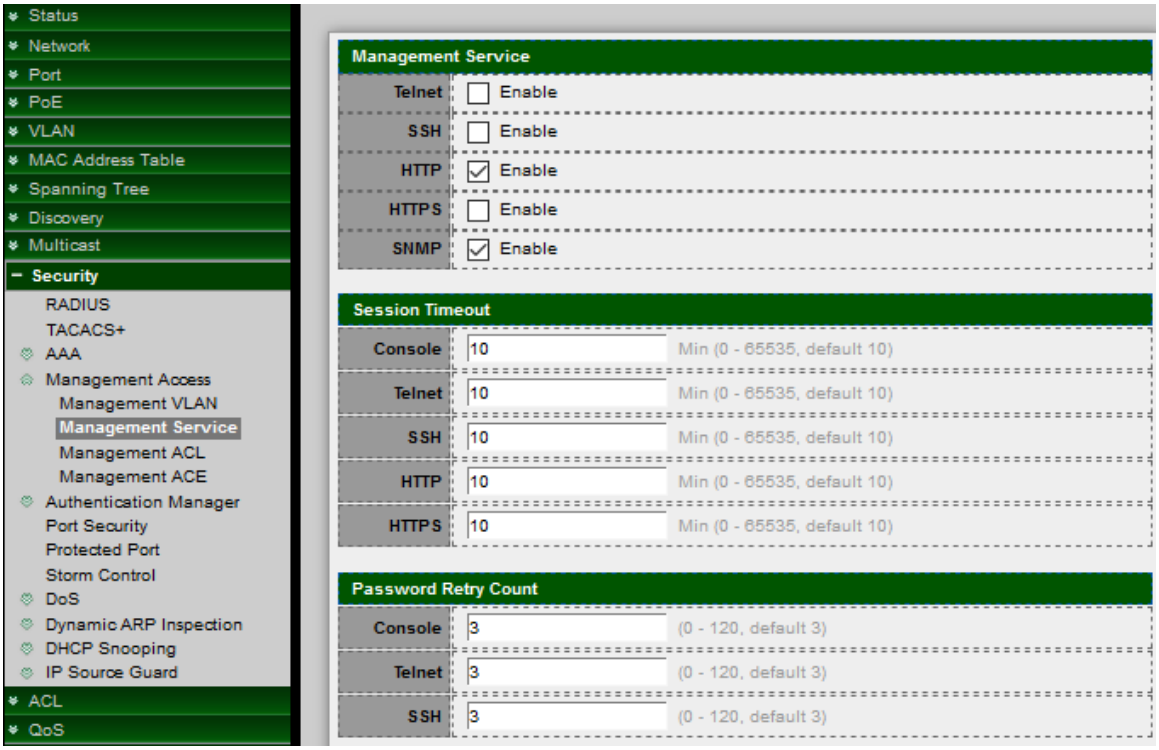
12.4.1 Management VLAN

When created VLAN function then administrator can select a specific VLAN, only allow this VLAN can to enter the UI management page.



12.4.2 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.



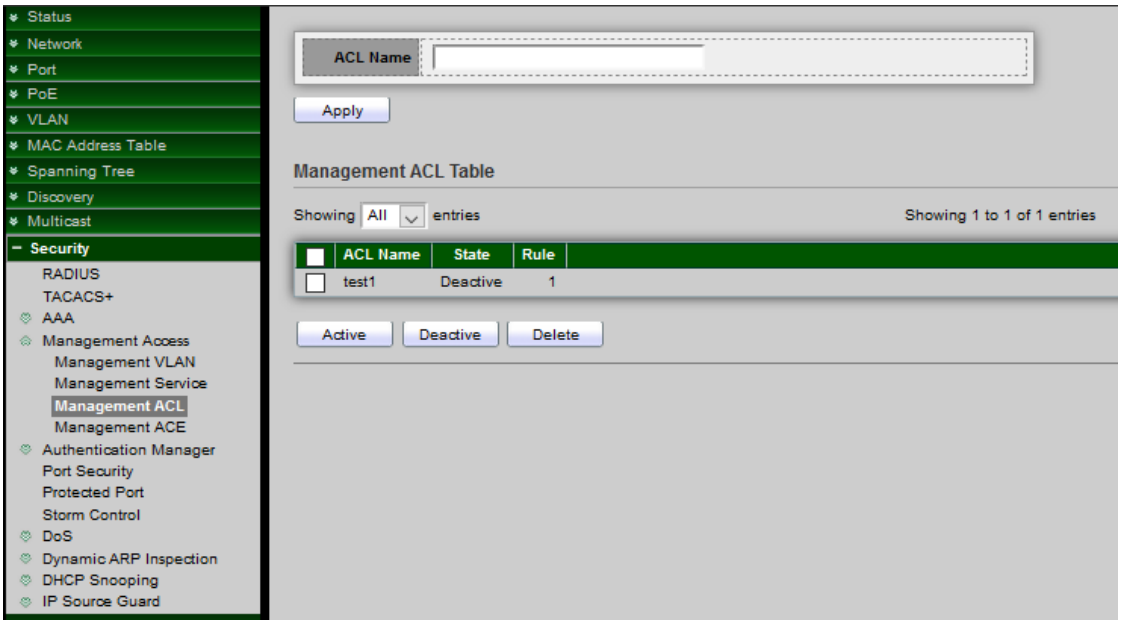
- **Session Timeout:** After login management page, in the set time if not session then system will auto timeout, administrator need re-login.
- **Password Retry Count:** If login error reaches the set value then login page will be kicked out, administrator need reopen the login page.
- **Silent Time:** 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.

12.4.3 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.

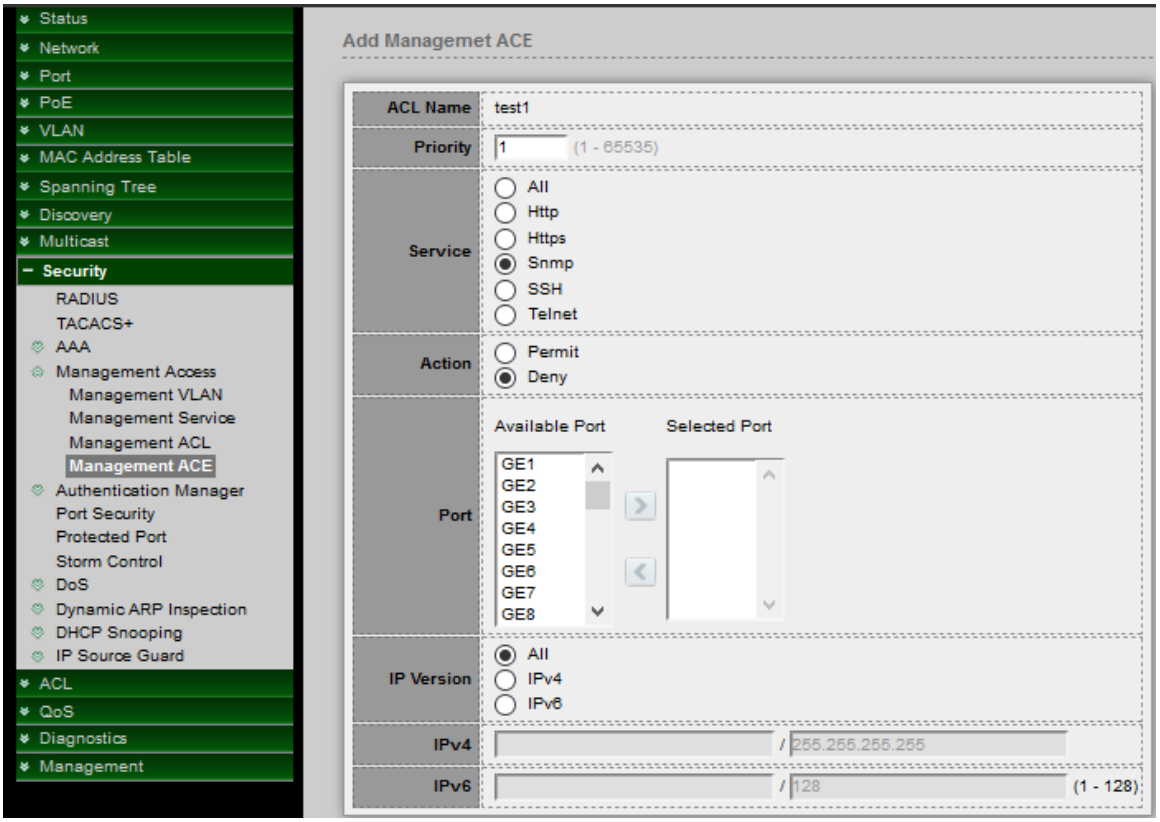
Note	If only create one ACL Profile and click Active then these all ports and services will are all denied.



12.4.4 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.

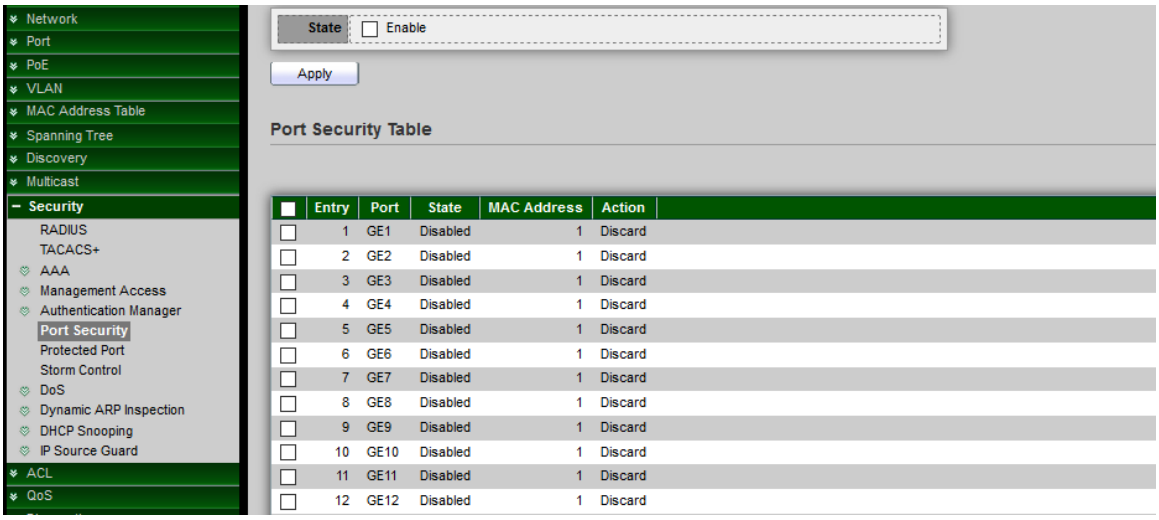
Administrator can go to "management ACL" page click "Active" button to enable the rule. After active the rule, this management page will can't operating only use Telnet protocol to management.



- **Priority:** Set this rule priority.
- **Service:** Select the service want to login management.
- **Action:** Select Permit or Deny.
- **Port:** Select managed ports.
- **IP Version:** Select IPv4 or IPv6.

12.5 Port Security

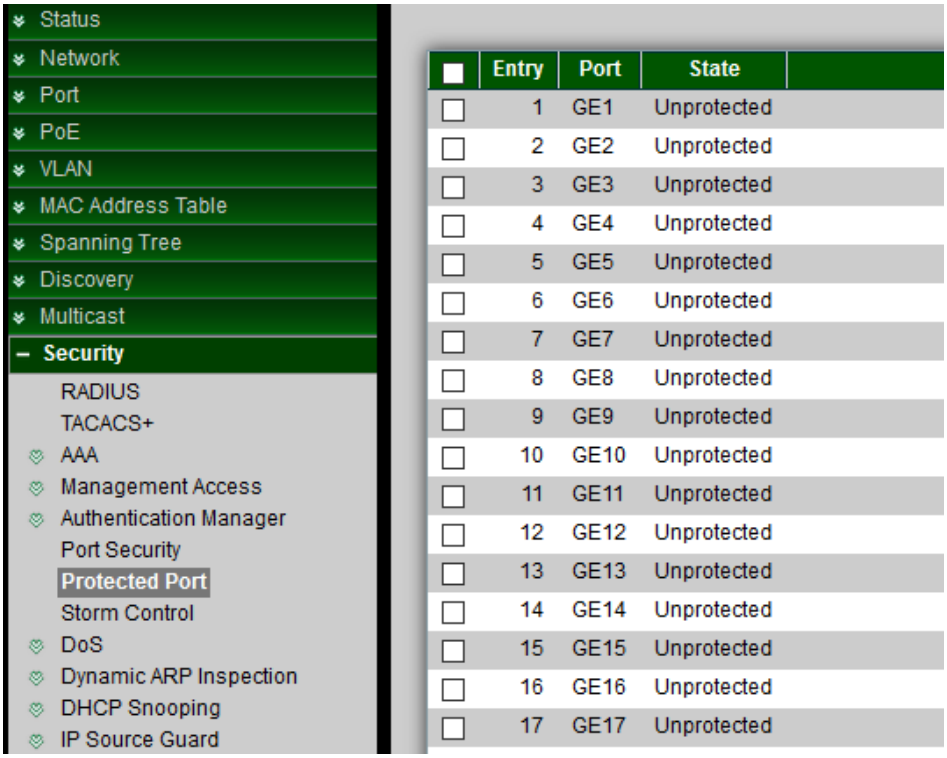
Port security monitors received and learned packets. Access to locked ports is limited to users with specific MAC addresses.



- **Port:** Displays selected port number.
- **State:** Enable or Un-Enable the port security.
- **MAC Address:** Enter the maximum number of MAC addresses that can be learned on the interface if Limited Dynamic Lock learning mode is selected. The range is 1 to 256 and the default is 1.
- **Action:** If Interface Status is locked, select an action to be applied to packets arriving on a locked interface.
  - **Forward:** Forwards packets from an unknown source without learning the MAC address.
  - **Discard:** Discards packets from any unlearned source, shuts down the interface, logs the events, and sends traps to the specified trap receivers.
  - **Shutdown:** Discards packets from any unlearned source, shuts down the interface, logs the events, and sends traps to the specified trap receivers. The interface remains shut down until reactivated, or until the switch is rebooted.

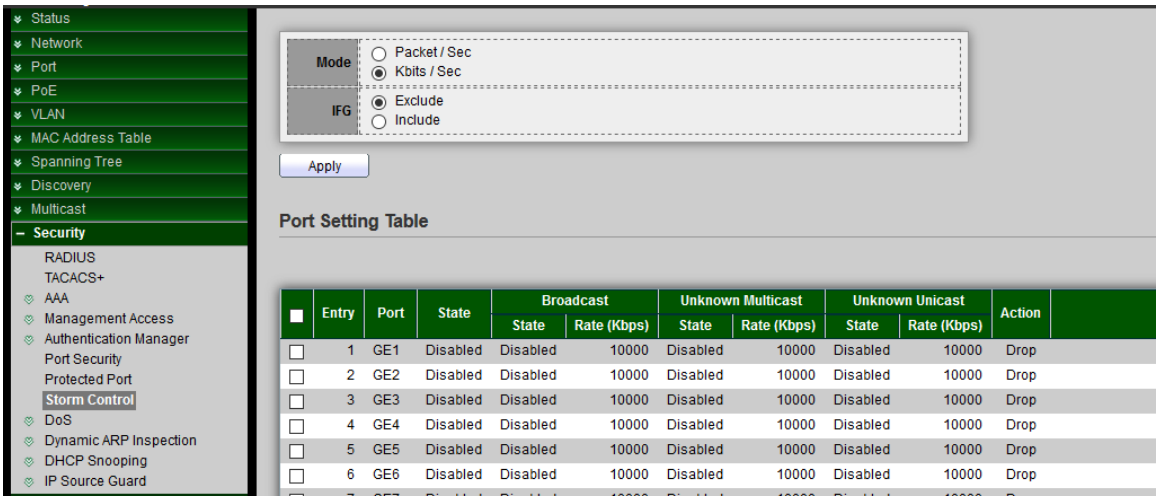
12.6 Protected Port

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.

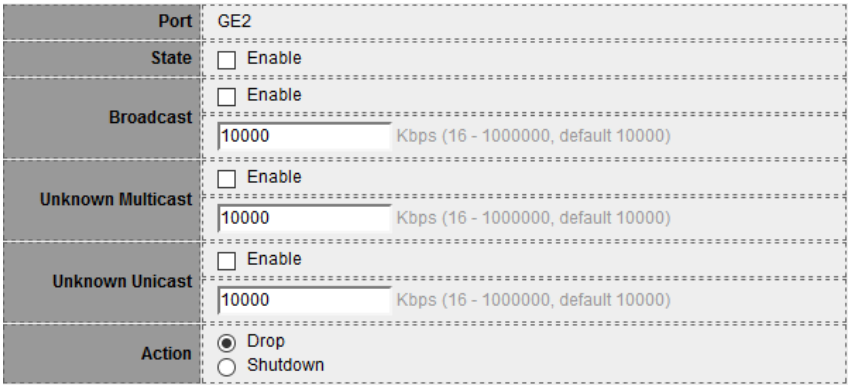


12.7 Storm Control

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.



- **Mode:** Select use Packets/second or Kbits/sec of the rate threshold
- **IFG:** Inter frame gap is 20 Bytes
  - **Excluded:** Not count the Broadcast / unknown Multicast or unknown Unicast frames. (excluding preamble and IFG)
  - **Include:** Count the Broadcast / unknown Multicast or unknown Unicast frames. (including preamble and IFG)



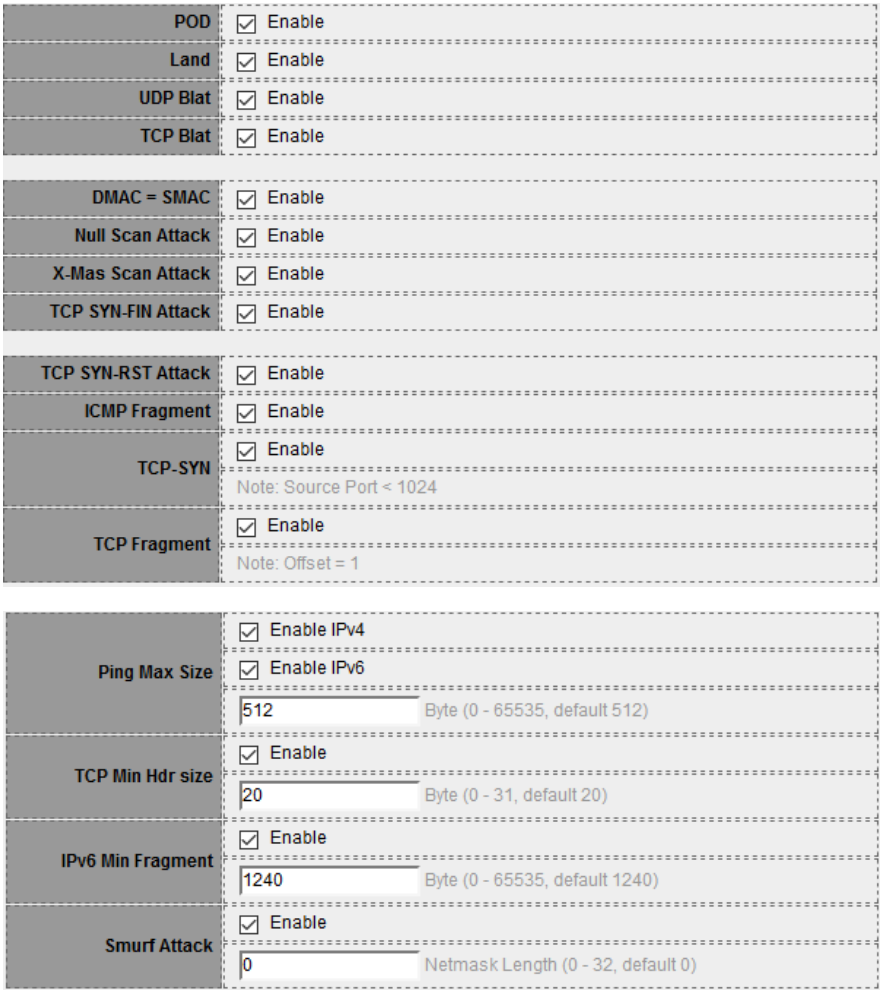
- **Port:** Display selected Port number.
- **State:** Enable or Un-Enable the function.
- **Broadcast:** If enable storm control for Broadcast traffic will count Broadcast traffic towards the bandwidth threshold.
- **Unknown Multicast:** If enable storm control for unknown Multicast will count unknown Multicast traffic towards the bandwidth threshold.
- **Unknown Unicast:** If enable storm control for unknown Unicast will count unknown Unicast traffic towards the bandwidth threshold.
- **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.
  - **Shutdown:** Received beyond the threshold will shut down the port.

12.8 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.

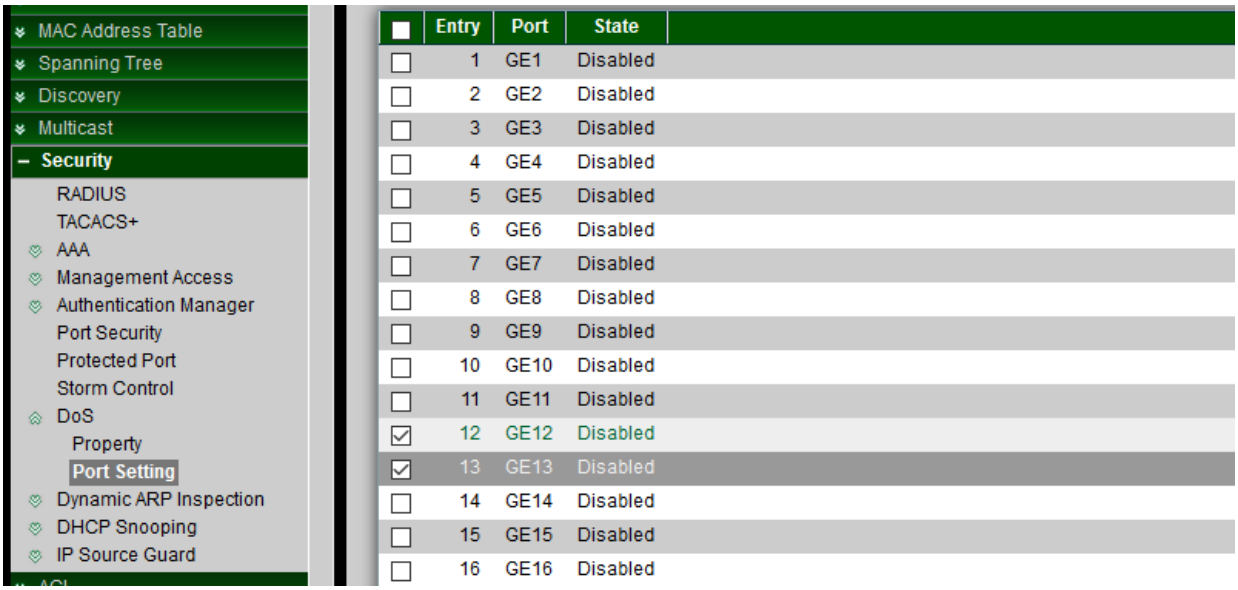
12.8.1 Property

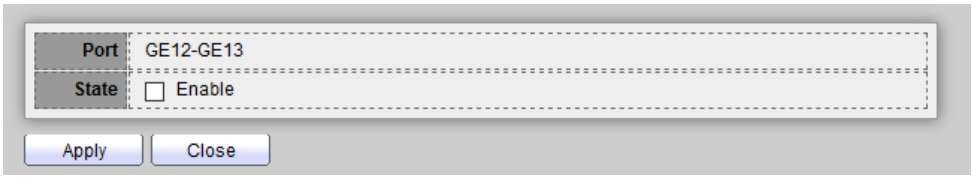
This default is enabled all DoS protection feature and SYN-FIN / SYN-RST protections. The default threshold is 60 SYN packets per second. The default period of port recovery is 60 seconds.



12.8.2 Port Setting

Administrator can choose protected ports.

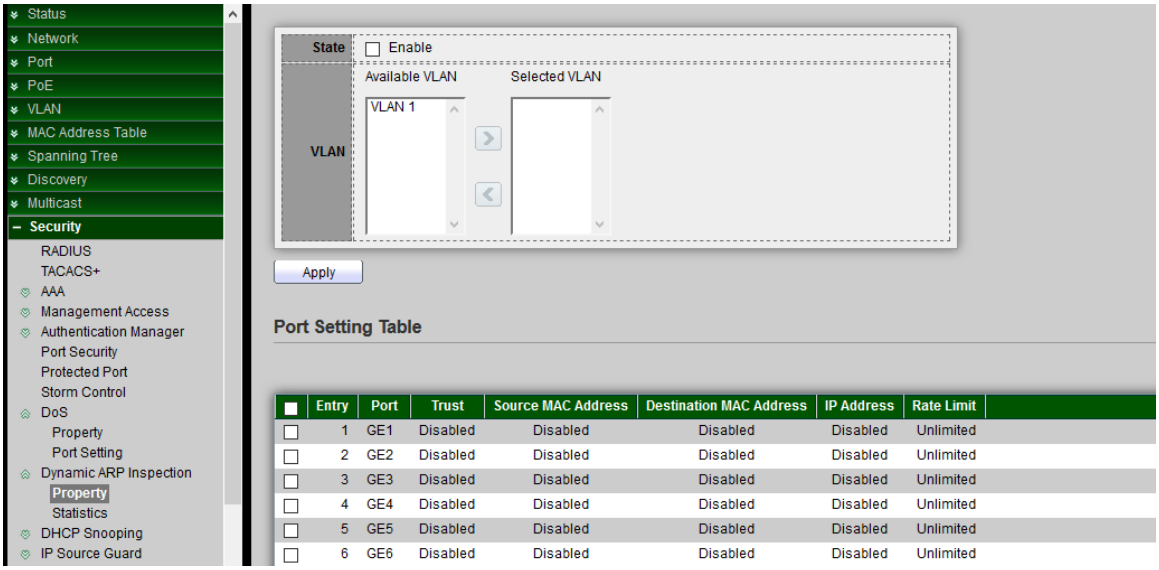




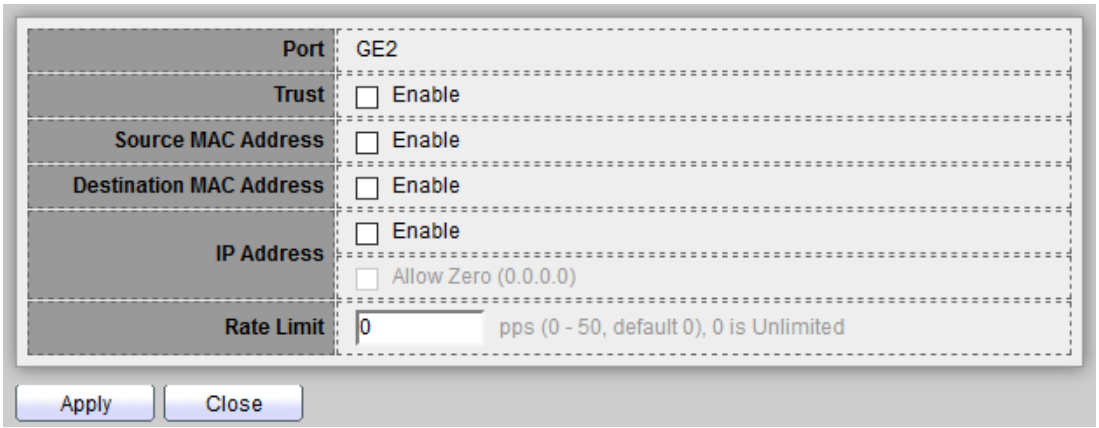
12.9 Dynamic ARP Inspection

Dynamic Address Resolution Protocol (ARP) is a TCP/IP protocol for translating IP addresses into MAC addresses.

12.9.1 Property



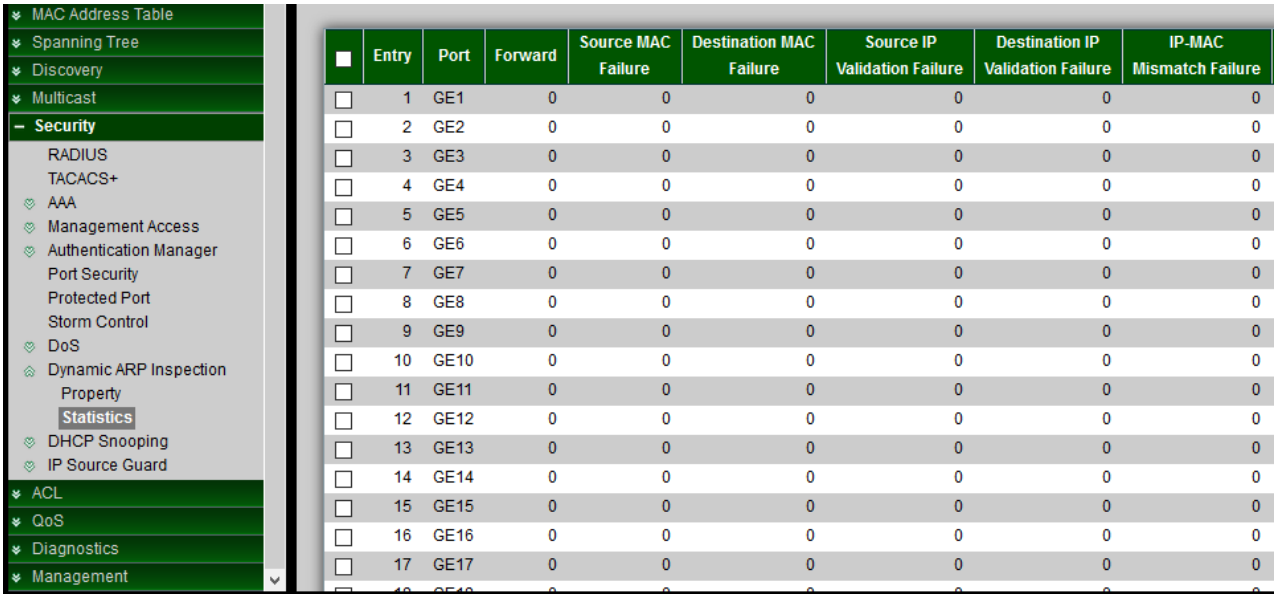
- **State:** Administrator can enable or disable this Dynamic ARP Inspection.
- **VLAN:** In the Enabled VLAN table, users assign static ARP Inspection lists to enabled VLANs. When a packet passes through an untrusted interface that is enabled for ARP Inspection switch will performs the checks.



- **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.
- **Destination MAC Address:** Check Enable to validate the destination MAC addresses in ARP replies.
- **IP Address:** Check Enable to validate the IP addresses in ARP requests and replies.
  - **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 300 pps and the default is 0 Unlimited.

12.9.2 Statistics

The Statistics page will displays the statistical information for ARP Inspection.



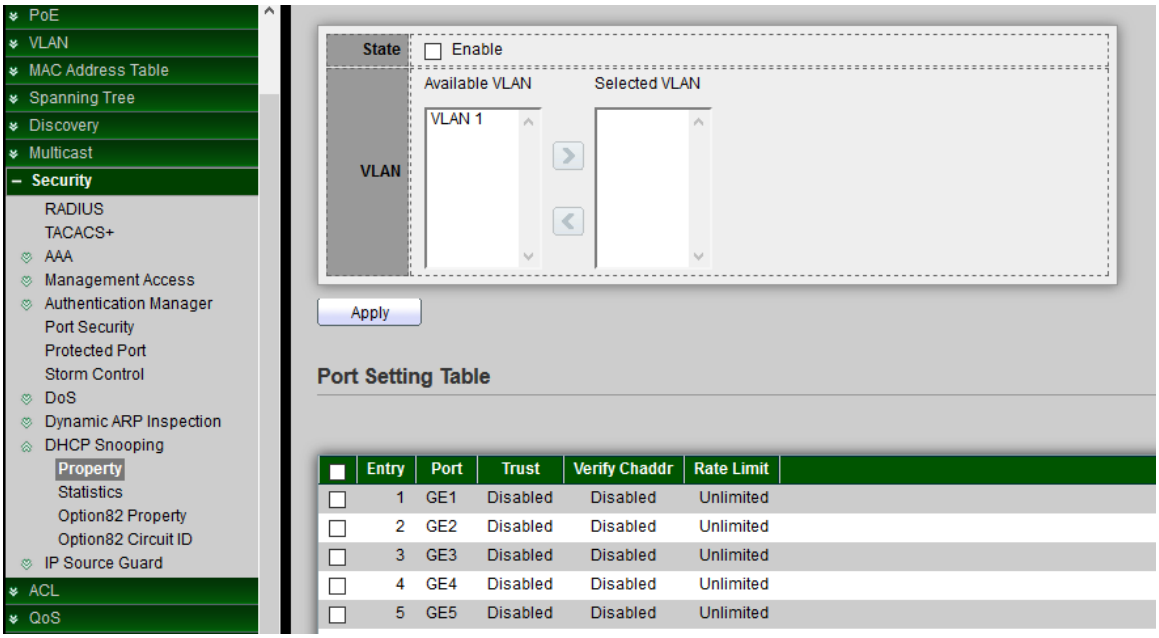
Entry	Port	Forward	Source MAC Failure	Destination MAC Failure	Source IP Validation Failure	Destination IP Validation Failure	IP-MAC Mismatch Failure
1	GE1	0	0	0	0	0	0
2	GE2	0	0	0	0	0	0
3	GE3	0	0	0	0	0	0
4	GE4	0	0	0	0	0	0
5	GE5	0	0	0	0	0	0
6	GE6	0	0	0	0	0	0
7	GE7	0	0	0	0	0	0
8	GE8	0	0	0	0	0	0
9	GE9	0	0	0	0	0	0
10	GE10	0	0	0	0	0	0
11	GE11	0	0	0	0	0	0
12	GE12	0	0	0	0	0	0
13	GE13	0	0	0	0	0	0
14	GE14	0	0	0	0	0	0
15	GE15	0	0	0	0	0	0
16	GE16	0	0	0	0	0	0
17	GE17	0	0	0	0	0	0

- **Entry:** Display list entry.
- **Port:** Display all port number.
- **Forward:** Display total number of ARP packets forwarded by the VLAN.
- **Source MAC Failure:** Display total number of ARP packets that include wrong source MAC addresses.
- **Destination MAC Failure:** Display total number of ARP packets that include wrong destination MAC addresses.
- **Source IP Address Validation Failures:** Display total number of ARP packets that the source IP address validation fails.
- **Destination IP Address Validation Failures:** Display total number of ARP packets that the destination IP address validation fails.
- **IP-MAC Mismatch Failures:** Display total number of ARP packets that the IP address does not match the MAC address.

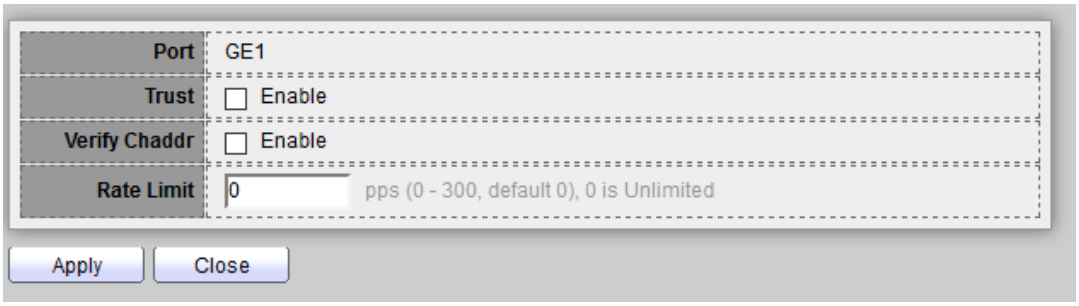
12.10 DHCP Snooping

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.

12.10.1 Property

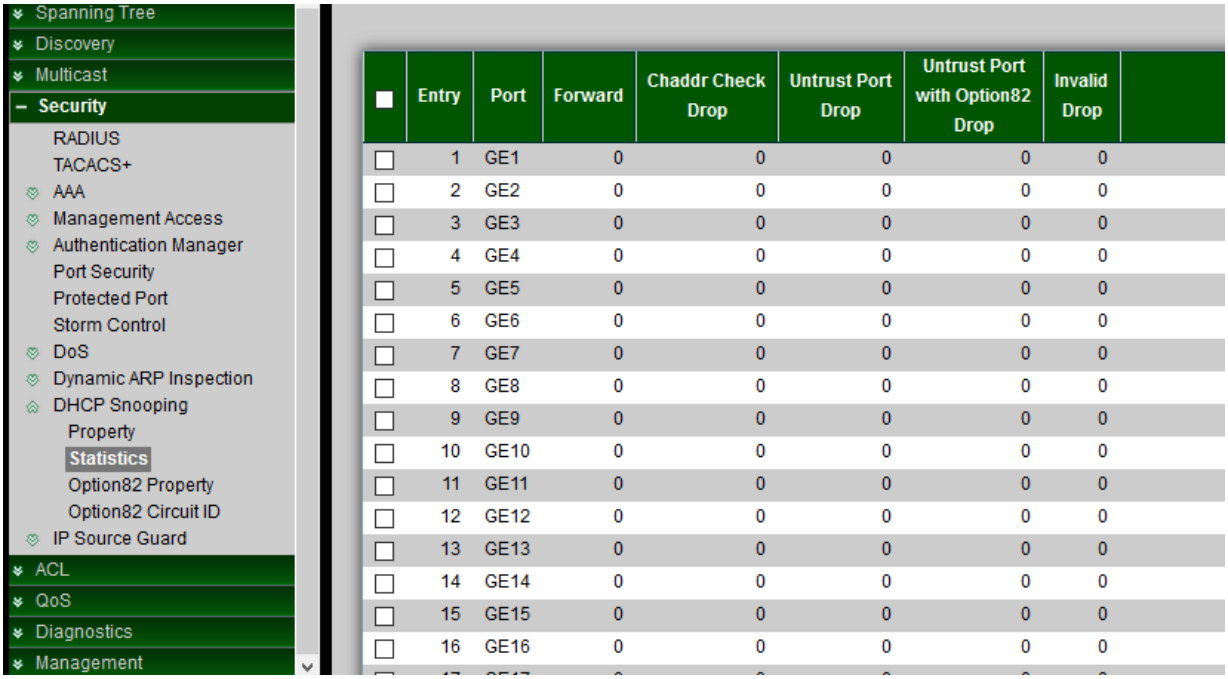


- **State:** Administrator can enable or Un-Enable DHCP Snooping.
- **VLAN:** Administrator can to enable DHCP Snooping on a VLAN, ensure that DHCP Snooping is globally enabled on the switch.



- **Port:** Display selected Port number.
- **Trust:** If check Enable will connected to a DHCP server or to other switches or routers as trusted ports.
- **Verify Chaddr:** Whether enable verify chaddr.
- **Rate Limit:** Check Enable to limit the rate on the interface. If rate limit is enabled, enter the maximum number of rate that can be allowed on the interface, default is 0 unlimited.

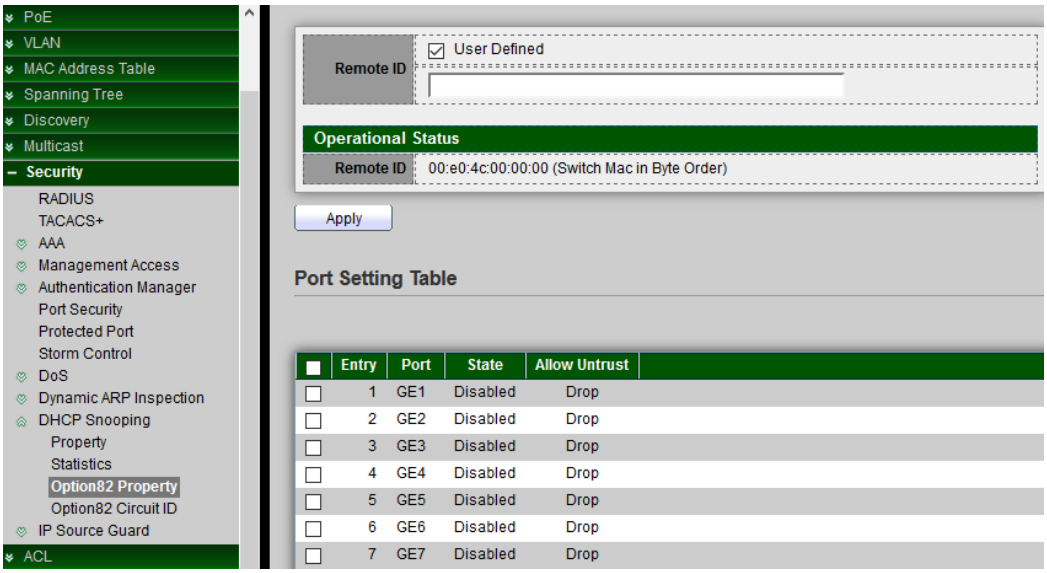
12.10.2 Statistics



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

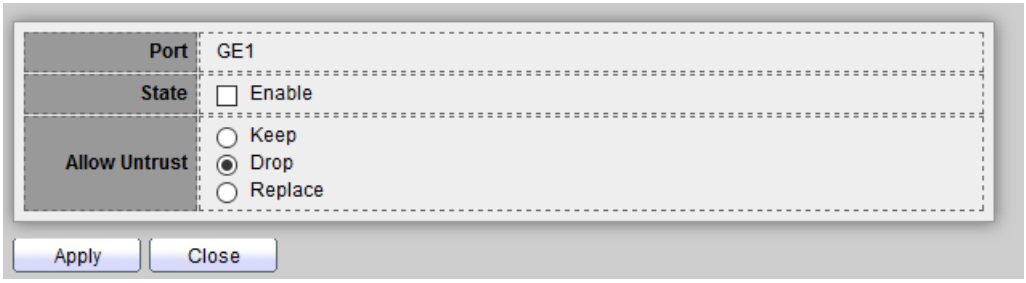
- **Entry:** Display list entry.
- **Port:** Display all port number.
- **Forward:** Display total number of forwarded packets.
- **Chaddr Check Drop:** Display total number of packets that are dropped by Chaddr check.
- **Untrust Port Drop:** Display total number of packets that are dropped by Untrust check.
- **Untrust Port With Option82 Drop:** Display total number of packets that are dropped by untrusted ports that enable Option 82.
- **Invalid Drop:** Display total number of packets that are dropped due to invalid.

12.10.3 Option82 Property



Entry	Port	State	Allow Untrust
1	GE1	Disabled	Drop
2	GE2	Disabled	Drop
3	GE3	Disabled	Drop
4	GE4	Disabled	Drop
5	GE5	Disabled	Drop
6	GE6	Disabled	Drop
7	GE7	Disabled	Drop

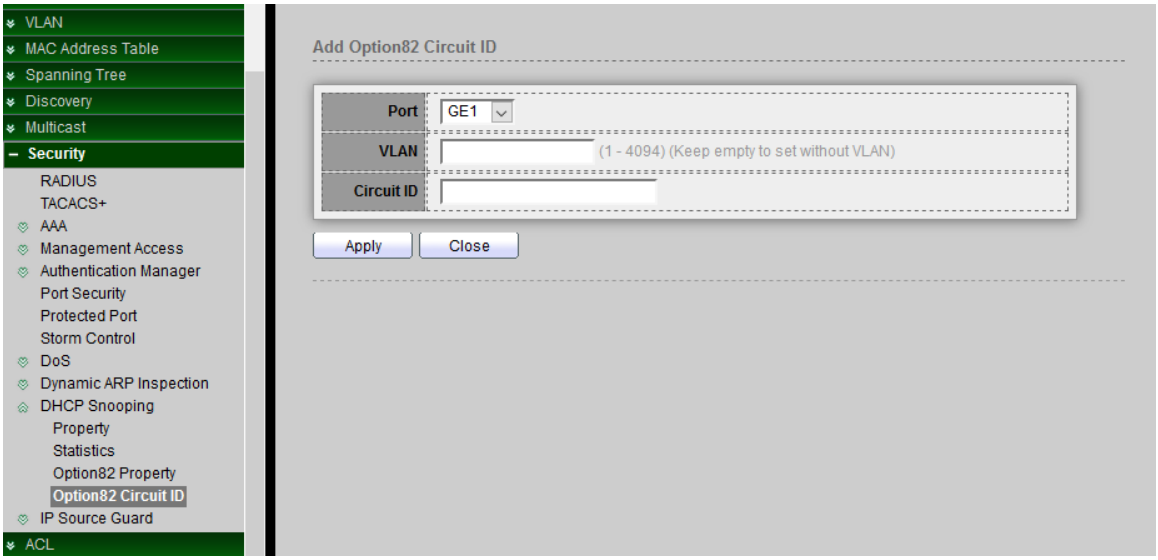
- **Remote ID:** If Option 82 is enabled, select User Defined to manually enter the format remote ID.
- **Operational Status:** Display remote ID information.



- **Port:** Display selected Port number.
- **State:** Check Enable or Un-Enable.
- **Allow Untrust:** When untrusted port receives DHCP packets administrator can select setting Keep / Drop / or Replace action.
  - **Keep:** Keeps DHCP packets with Option 82 information.
  - **Drop:** Drops DHCP packets with Option 82 information.
  - **Replace:** Replaces DHCP packets with Option 82 information.

12.10.4 Option82 Circuit ID

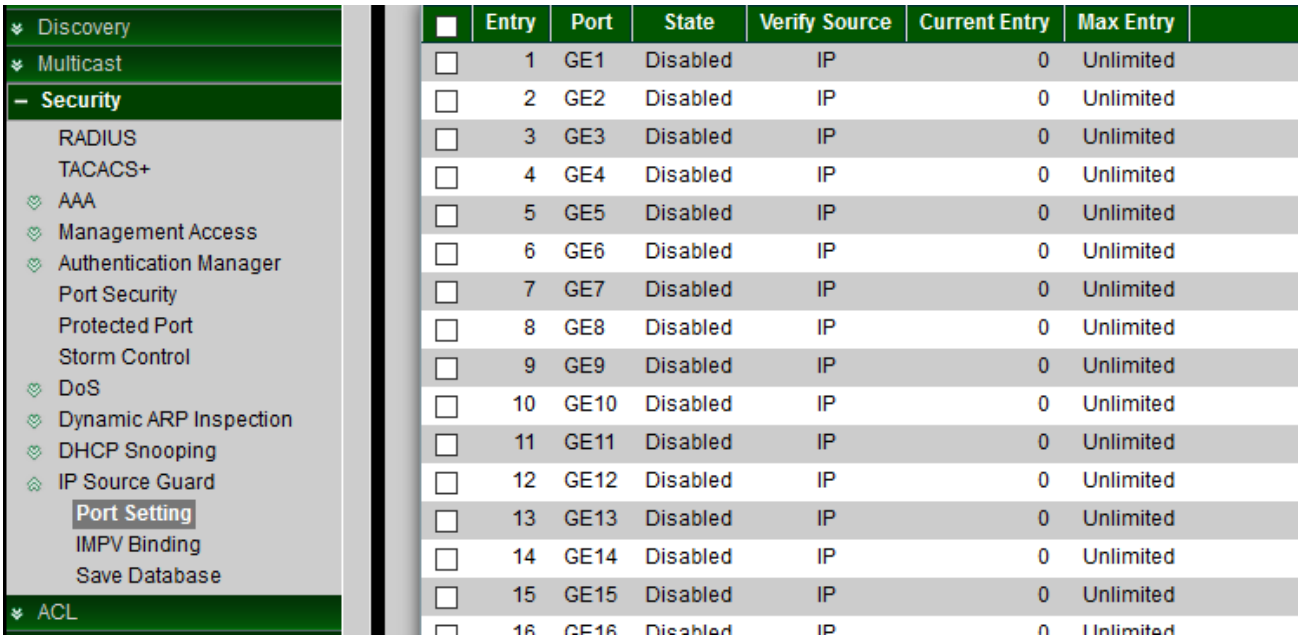
Administrator can use the Option82 Port CID Settings page to configure the Option 82 circuit-ID.



- **Port:** Select a Port number.
- **VLAN:** Set a VALN number to use circuit ID.
- Dircuit ID: Using from 1 to 64 ASCII characters (no spaces). When the Option 82 feature is enabled, the default circuit-ID suboption is the switch VLAN and port identifier, in the format of vlan-mod-port.

12.11 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.

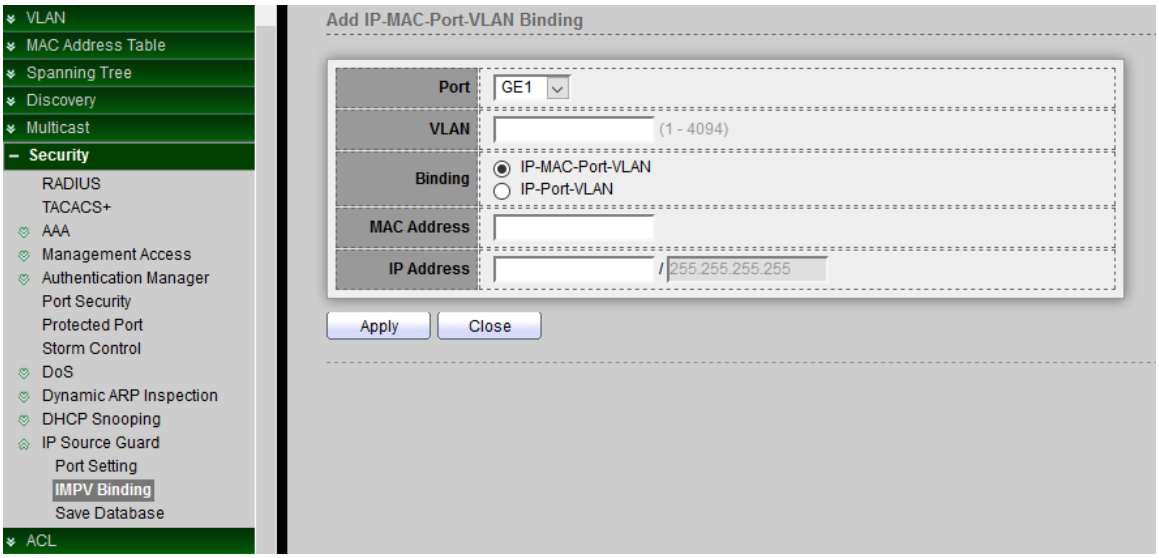


12.11.1 Port Setting

- **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.
- **Verify Source:** Administrator can select IP only or MAC and IP type of source traffic to be verified.
- **Max Entry:** Administrator need enter the maximum number of IP source binding rules. The range is 0 to 50, and 0 is Unlimited.

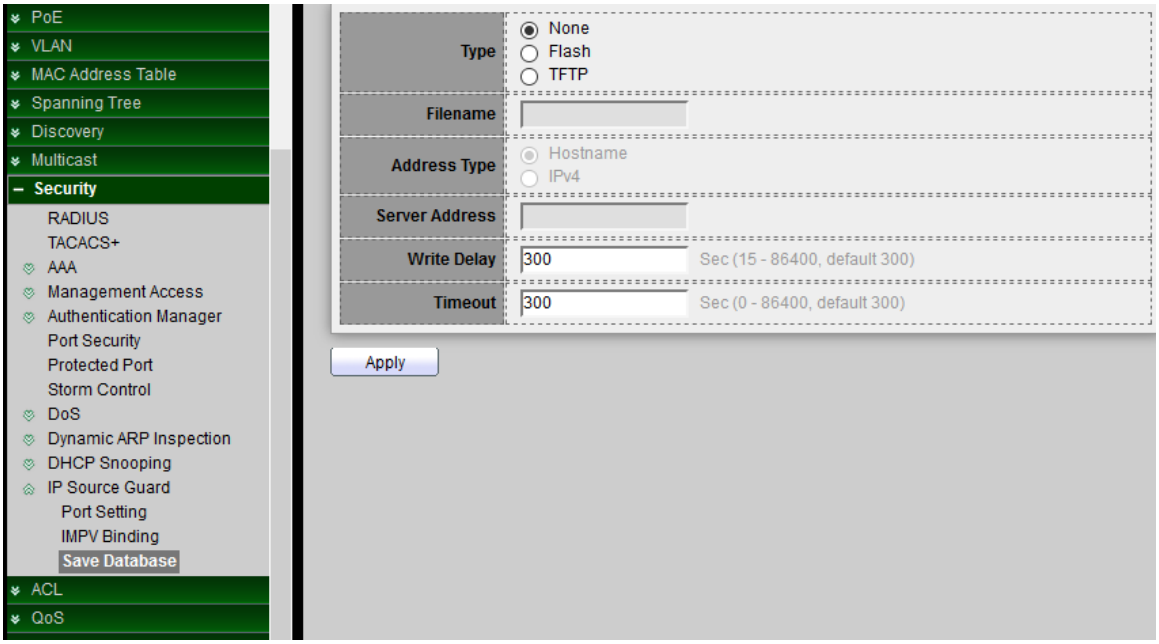
12.11.2 IMPV Binding

Use the Binding to query and view information about inactive addresses recorded in the IP Source Guard database.



- **Port:** Administrator can select port number.
- **VLAN:** Set VLAN with which the IP address is associated.
- **Binding:** Select “IP/MAC/Port/VLAN or IP/ Port/VLAN binding.
- **MAC Address:** Set MAC address of the interface.
- **IP Address:** Set IP address of the interface.

12.11.3 Save Databases



- **Type:** System can access the database by local Flash or TFTP server.
- **Filename:** Set file name of TFTP server.
- **Address Type:** Select use Host name or IP address to connection TFTP server.
- **Server Address:** Set TFTP address. If use host name then need enter host name. If use IPv4 then need IP Address.
- **Write Delay:** Set connected delay time.
- **Timeout:** Set connected timeout.

13. ACL

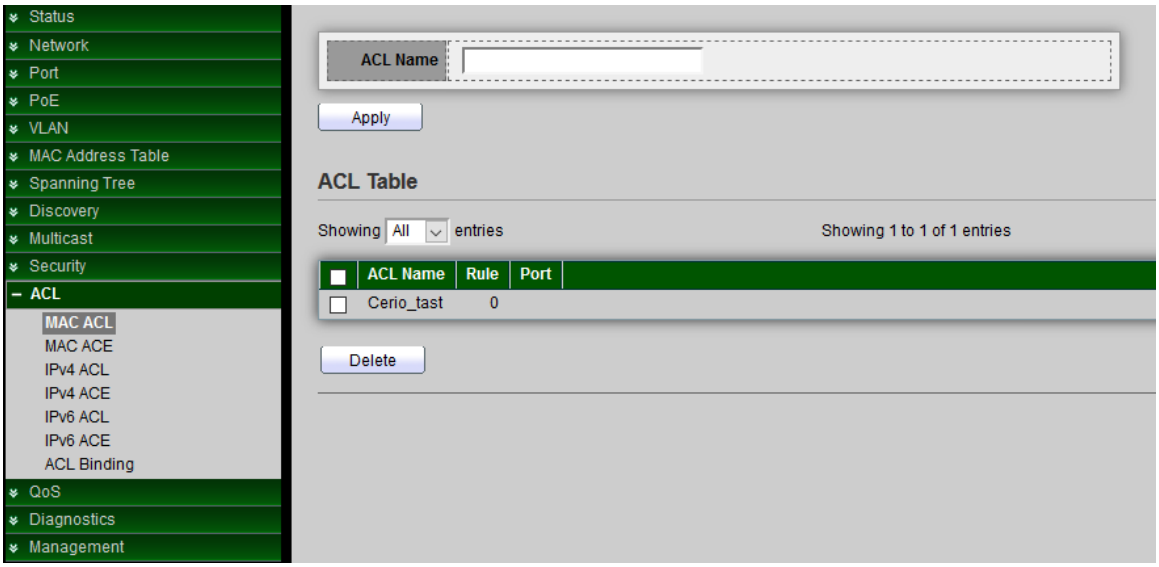
ACL (Access Control List) is an ordered list of classification filters and actions. Each single classification rule, together with its action, is called an Access Control Element (ACE). Each ACE is made up of filters that distinguish traffic groups and associated actions. A single ACL may contain one 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.

13.1 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.

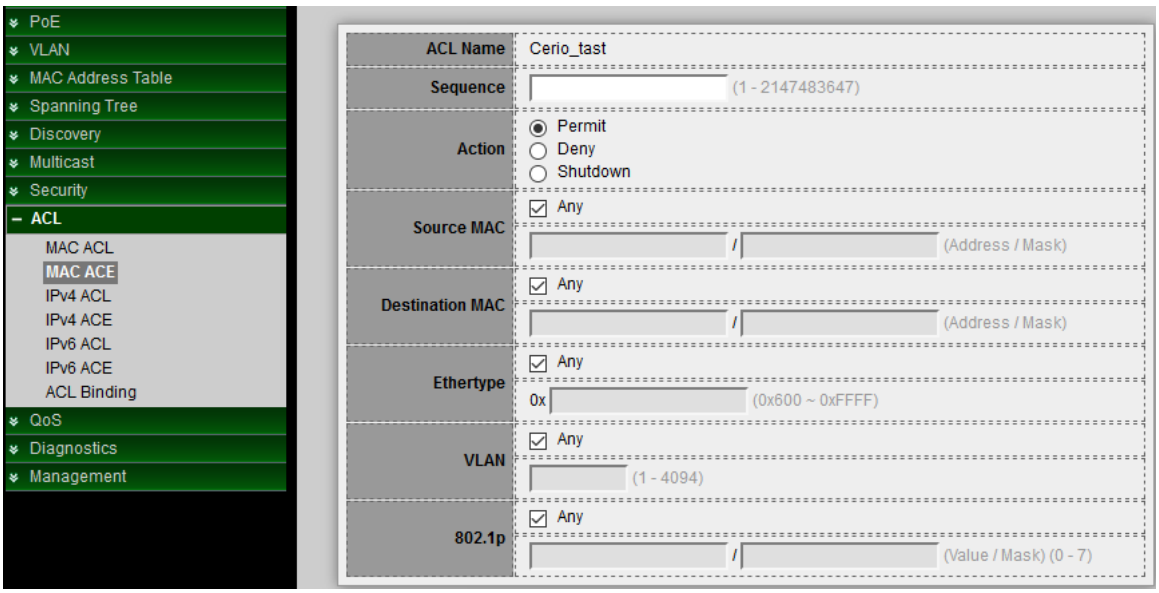
Note	A port can be either secured with ACLs or configured with advanced QoS policy, but not both.



- **ACL Name:** Create a name of ACL.
- **ACL Table:** Display created MAC ACL name list.
- **ACL Name:** Display ACL name.
- **Rule:** Display the number of conditions.

13.2 MAC ACE

MAC ACEs will check all frames for a match.



- **ACL Name:** Displays selected MAC ACL name.
- **Sequence:** This sequence is priority of ACE rule. ACEs with higher priority are processed first. 1 is the highest priority.
- **Action:** Administrator can select the action taken upon a match.

- **Permit:** This is forwards packets that meet the ACE criteria.
- **Deny:** This is drops packets that meet the ACE criteria.
- **Shutdown:** This is disables the port from where the packets were received.

➢ **Source MAC:** If select any then all source addresses are acceptable or select administrator defined to enter a source MAC address or a range of source MAC addresses.

➢ **Destination MAC:** If select any then all destination addresses are acceptable, or select administrator defined to enter a destination MAC address or a range of destination MAC addresses.

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).

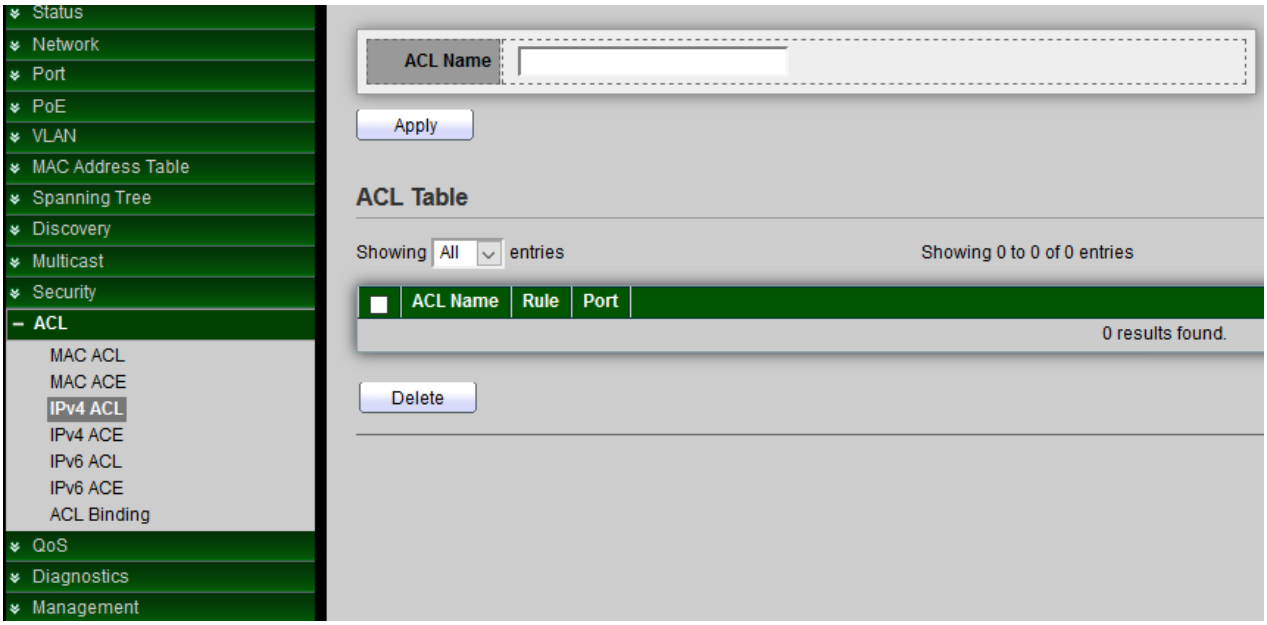
➢ **Ethertype:** Enter the frame Ethernet type to be matched.

➢ **VLAN:** Enter the number of the VLAN tag to match.

➢ **802.1p:** Check Include to use 802.1p, administrator need enter the 802.1p value to be added to the VPT tag and set mask.

13.3 IPv4 ACL

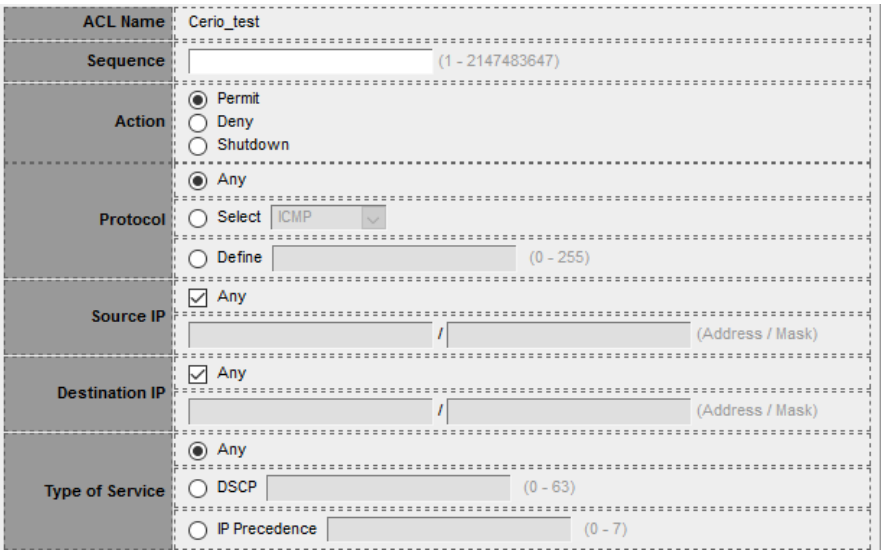
This page mainly creates IPv4 ACLs profile. The IPv4 ACLs are used to check IPv4 packets, while other types of frames, such as ARPs, are not checked.



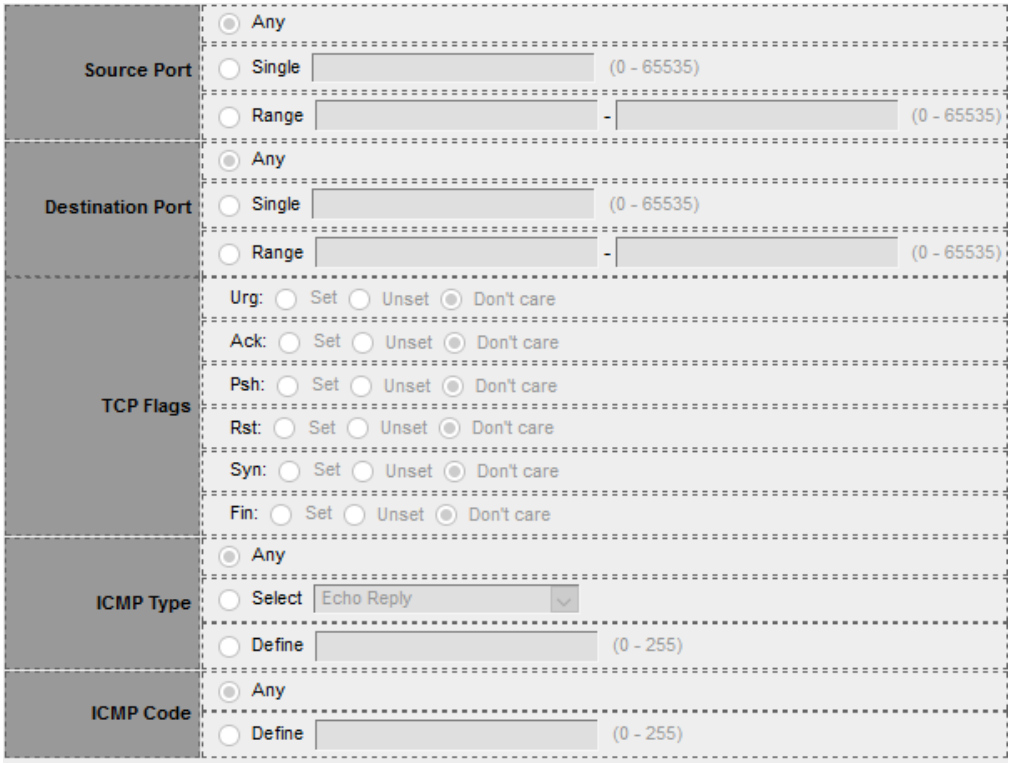
➢ **ACL Name:** Create a name of ACL.

➢ **ACL Table:** Display created IPv4 ACL name list.

13.4 IPv4 ACE



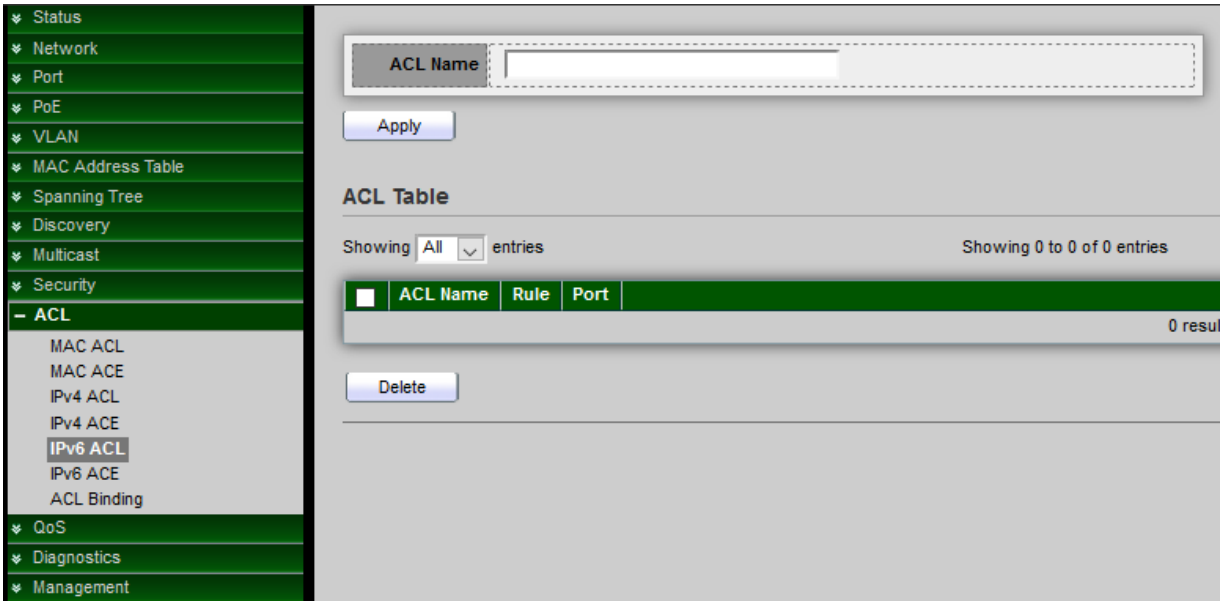
- **ACL Name:** Displays selected IPv4 ACL name.
- **Sequence:** This sequence is priority of ACE rule. ACEs with higher priority are processed first. 1 is the highest priority.
- **Action:** Administrator can select the action taken upon a match.
  - **Permit:** This is forwards packets that meet the ACE criteria.
  - **Deny:** This is drops packets that meet the ACE criteria.
  - **Shutdown:** This is disables the port from where the packets were received.
- **Protocol:** Creates an ACE based on a specific protocol.
  - **Any:** Select to accept all service protocols.
  - **Select:** Administrator can from the drop-down select ICMP/IP in IP/TCP/EGP/IGP/UDP/HMP/RDP/IPV6/IPV6:ROUT(Matches packets belonging to the IPv6 over IPv4 route through a gateway)/IPV6:FRAG(Matches packets belonging to the IPv6 over IPv4 Fragment Header)/RSVP/IPV6:ICMP/OSPF/PIM/L2TP protocols.
- **Source IP:** If administrator select any then all source addresses are acceptable, or select User Defined to enter a source address or a range of source addresses.
- **Destination IP:** If administrator select any then all destination address are acceptable, or select User Defined to enter a destination address or a range of destination addresses.
- **Type of Service:** Select the service type of IP packets.
  - Any: Any service type.
  - DSCP: Differentiated Serves Code Point (DSCP) to match.
  - IP Precedence: IP precedence is a model of TOS (type of service) that the network uses to help provide the appropriate QoS commitments. This model uses the 3 most significant bits of the service type byte in the IP header, as described in RFC 791 and RFC 1349.



- **Source Port:** If administrator select use TCP/UDP protocol will can definition source port.
  - **Any:** Match to all source ports.
  - **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:** If administrator selects use TCP/UDP protocol will can definition destination port.
- **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.
  - **Set:** Match if the flag is SET.
  - **Unset:** Match if the flag is Not SET.
  - **Don't care:** Ignore the TCP flag.
- **ICMP Type:** If the IP protocol of the ACL is ICMP, select the ICMP message type used for filtering purposes.
  - **Any:** All message types are accepted.
  - **Select:** Select message type by name.
  - **Define:** Enter the number of message type to be used for filtering purposes.
- **ICMP Code: T**he ICMP messages can have a code field that indicates how to handle the message. Select any to accept all codes, or select User Defined to enter an ICMP code for filtering purposes.

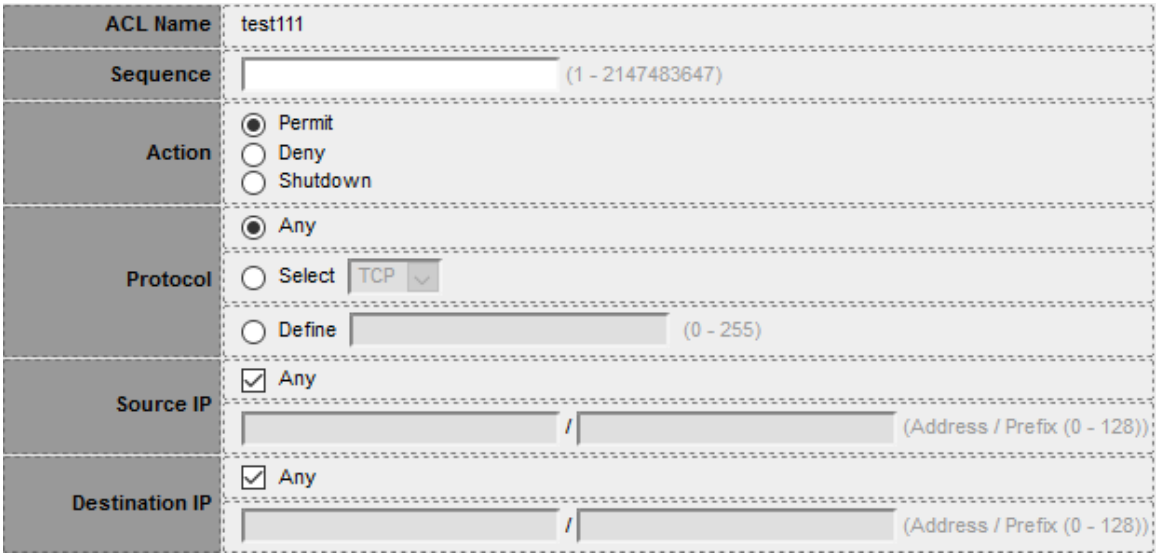
13.5 IPv6 ACL

Use the IPv6 Based ACL page to create IPv6-based ACLs, which check pure IPv6-based traffic. IPv6 based ACLs do not check IPv6-over-IPv4 or ARP packets.



- **ACL Name:** Create a name of ACL.
- **ACL Table:** Display created IPv6 ACL name list.

13.6 IPv6 ACE

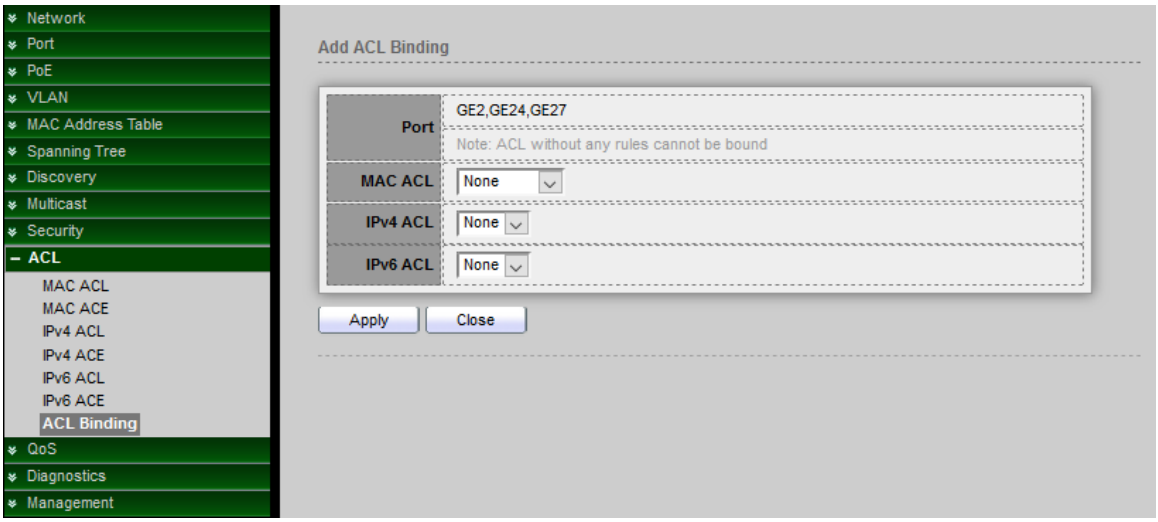


- **ACL Name:** Displays selected IPv6 ACL name.

- **Sequence:** This sequence is priority of ACE rule. ACEs with higher priority are processed first. 1 is the highest priority.
- **Action:** Administrator can select the action taken upon a match.
  - **Permit:** This is forwards packets that meet the ACE criteria.
  - **Deny:** This is drops packets that meet the ACE criteria.
  - **Shutdown:** This is disables the port from where the packets were received.
- **Protocol:** Creates this ACE based on a specific protocol or protocol ID.
  - **Any:** Select to accept all service protocols.
  - **Select:** Administrator can from the drop-down select TCP/UDP and ICMP protocols.
- **Source IP:** If administrator select any then all source address are acceptable, or select User Defined to enter a source address or a range of source addresses.
- **Destination IP:** If administrator select any then all destination address are acceptable, or select User Defined to enter a destination address or a range of destination addresses.
- **Type of Service:** Select the service type of IP packets.
  - **Any:** Any service type.
  - **DSCP:** Differentiated Serves Code Point (DSCP) to match.
  - **IP Precedence:** IP precedence is a model of TOS (type of service) that the network uses to help provide the appropriate QoS commitments. This model uses the 3 most significant bits of the service type byte in the IP header, as described in RFC 791 and RFC 1349.
- **Source Port**
  - **Any:** Match to all source ports.
  - **Single:** Enter a single TCP/UDP source port to which packets are matched. This field is active only if TCP or UDP is selected from the Select from list drop-down menu.
  - **Range:** Select a range of TCP/UDP source ports to which the packet is matched.
- **Destination Port:** Select one of the available values. (They are the same as for the **Source Port** field.)
- **TCP Flags:** Select one of 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.
  - **Set:** Match if the flag is SET.
  - **Unset:** Match if the flag is Not SET.
  - **Don't care:** Ignore the TCP flag.
- **ICMP Type:** If the ACL is based on ICMP, select the ICMP message type that will be used for filtering purposes.
- **ICMP Code:** The ICMP messages may have a code field that indicates how to handle the message. Select any to accept all codes, or select User Defined to enter an ICMP code for filtering purposes.

13.7 ACL Binding

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.



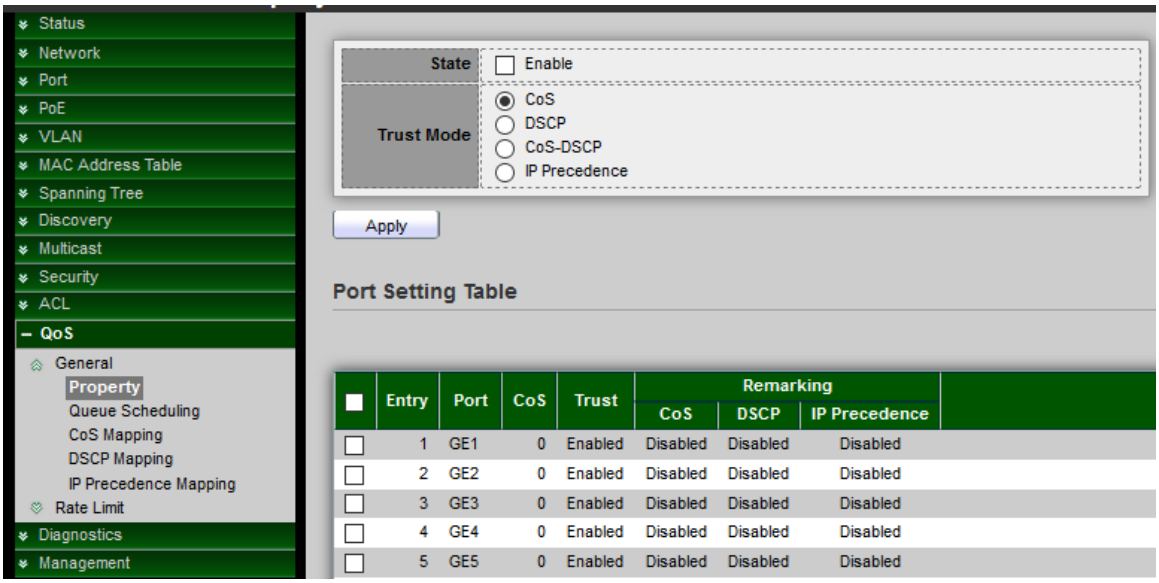
- **Port:** Displays selected Port number.
- **MAC ACL:** MAC ACLs that are bound to the interface.
- **IPv4 ACL:** IPv4 ACLs that are bound to the interface.
- **IPv6 ACL:** IPv6 ACLs that are bound to the interface.

14. QoS

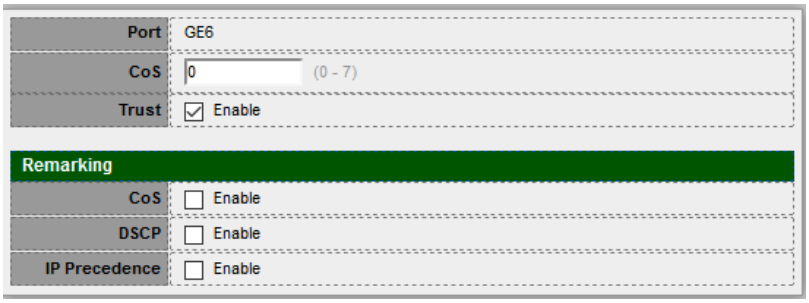
The quality of service (QoS) feature is applied throughout the network to ensure that network traffic is prioritized according to required criteria and the desired traffic receives preferential treatment.

14.1 Property

The QoS feature is used to optimize network performance.



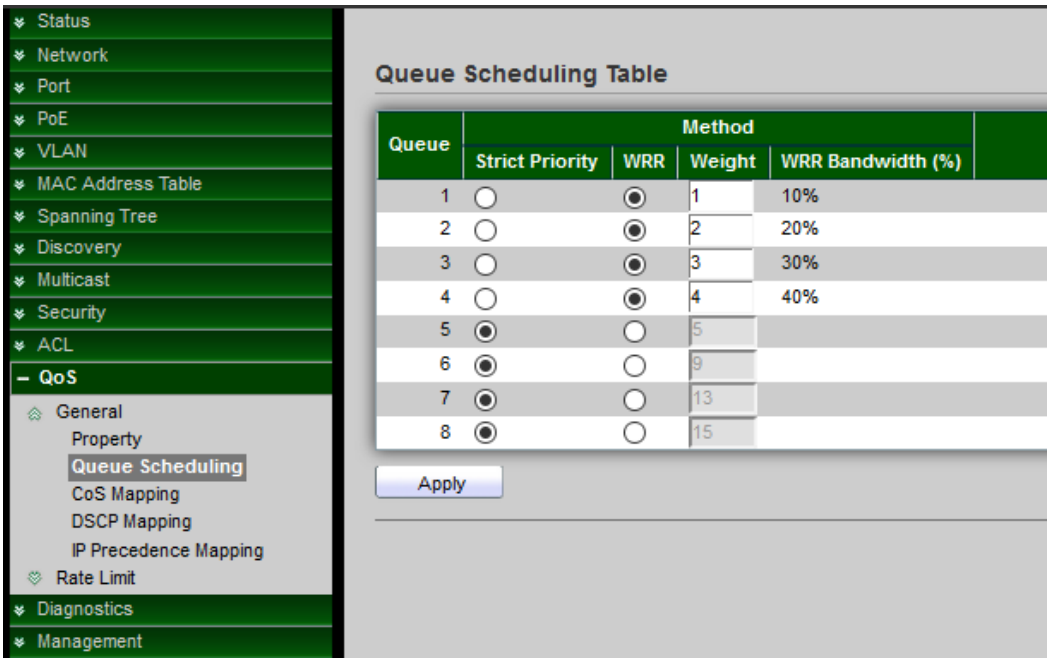
- **State:** Administrator can enable or disable this QoS Feature.
- **Trust Mode:** Administrator can select CoS / DSCP / CoS-DSCP and IP Precedence mode.
  - **CoS:** Traffic is mapped to queues based on the VPT field in the VLAN tag, or based on the per-port default CoS value (if there is no VLAN tag on the incoming packet), the actual mapping of the VPT to queue can be configured on the CoS to Queue page.
  - **DSCP:** 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:** 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.
  - **CoS-DSCP:** Select to use Trust CoS mode for non-IP traffic and Trust DSCP mode for IP traffic.



- **Port:** Displays selected port number.
- **CoS:** 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:** Select the trust mode when the switch is in QoS basic mode.
- **Remarking:**
  - **CoS:** 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:** 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:** 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.

14.2 Queue Scheduling

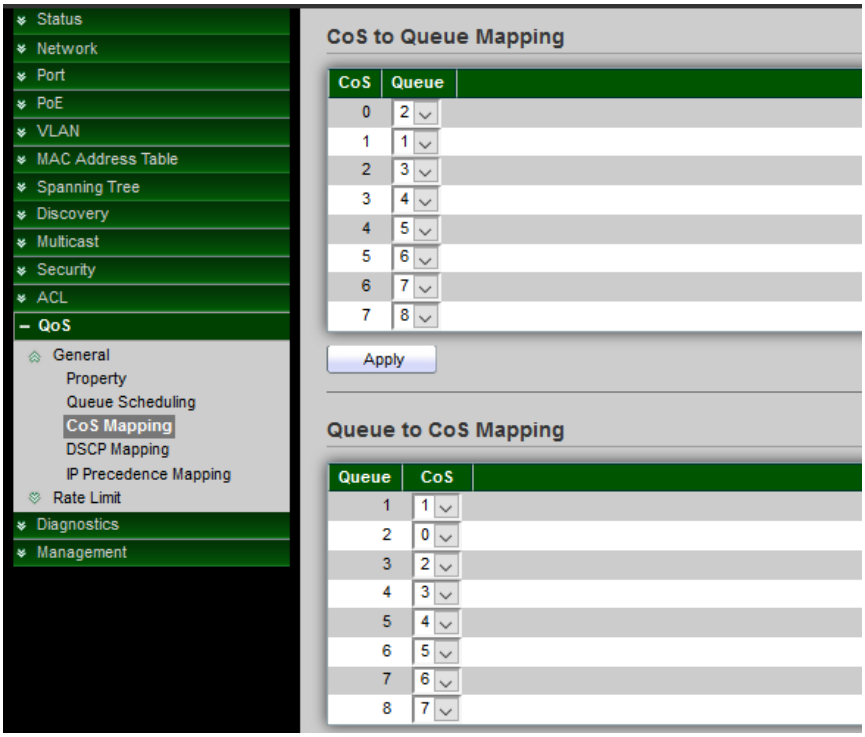
This "**Queue scheduling**" function support WRR and Strict Priority two method.
The following picture shows an example description of Queue Scheduling. When you select the combined SP and WRR queueing method, this switch schedules traffic in queue 7 and queue 6 first, based on the strict priority queueing method. When there is no traffic in queue 7 and queue 6, the device schedules the other queues in round-robin fashion from the highest priority queue to the lowest priority queue (Q0 through Q5).



- **Strict Priority:** The function assigns the maximum weights to each queue, to cause the queuing mechanism to serve as many packets in one queue as possible before moving to a lower queue.
- **WRR:** Weight Round Robin Scheduling is like waiting in line, Packets in all the queues are sent in order based on the weight value for each queue.
- **Weight:** Administrator can set weight priority queue.

14.3 CoS Mapping

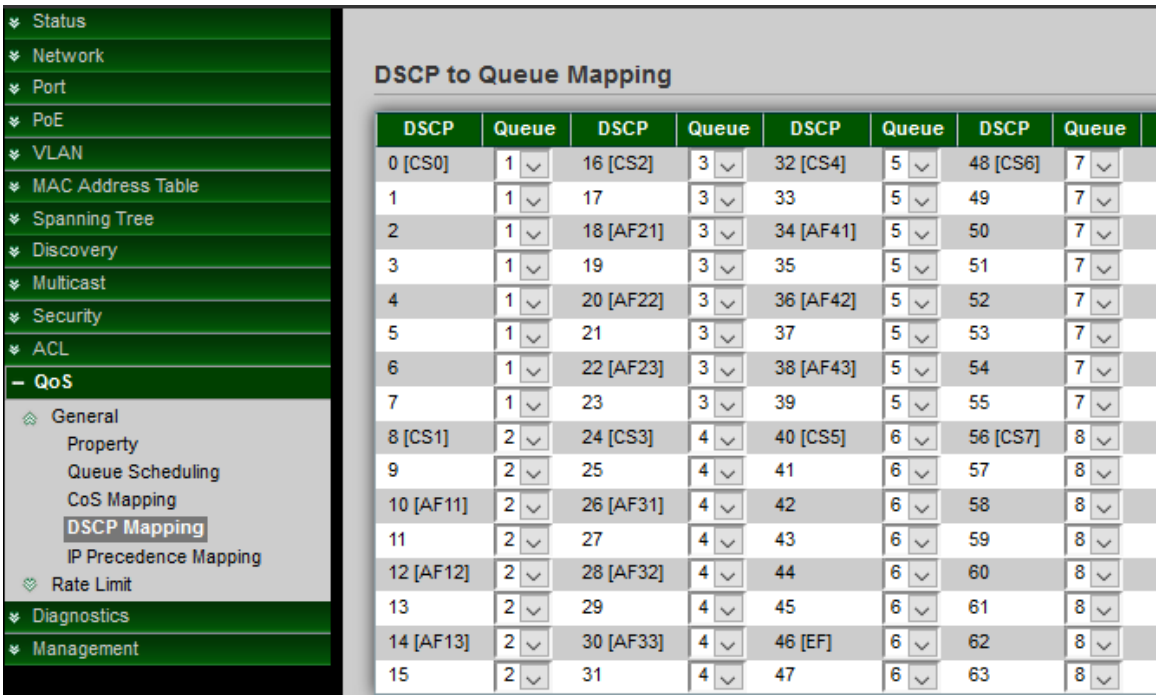
CoS to Queue mapping or Queue to CoS Mapping is queue schedule method and bandwidth allocation, it is possible to achieve the desired QoS in a network.

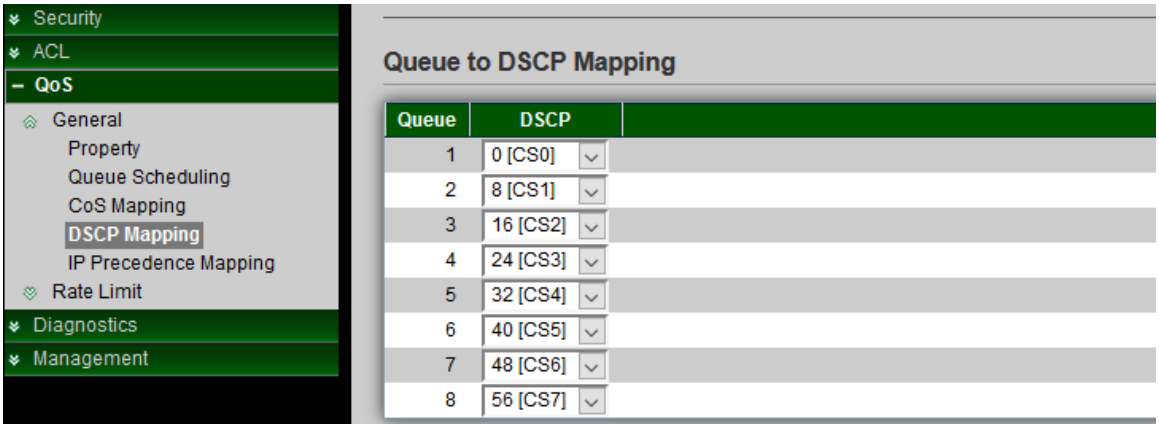


CoS (0 to 7) 7 is highest	Queue(1 to 8) 8 is highest priority	Description
0	2	Background
1	1	Best Effort
2	3	Excellent Effort
3	4	Critical Application LVS phone SIP
4	5	Video
5	6	Voice IP phone default
6	7	Interwork Control LVS phone RTP
7	8	Network Control

14.4 DSCP Mapping

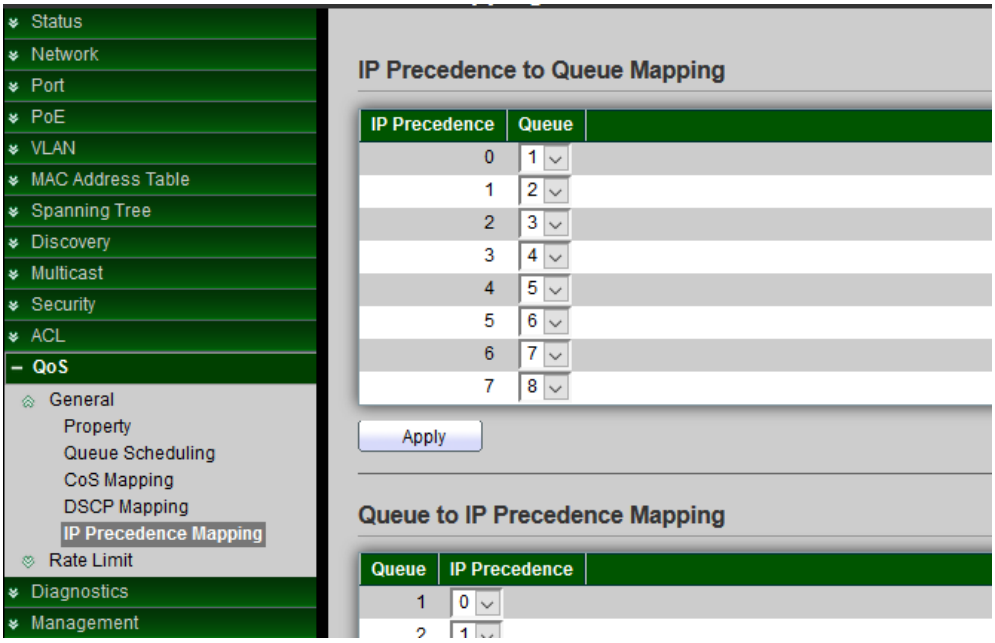
This DSCP values range from 0 through 63, whereas the internal forwarding priority values range from 1 through 8. Any DSCP value within a given range is mapped to the same internal forwarding priority value. These include the CS (Class Selector), AF (Assured Forwarding) and EF (Expedited Forwarding). For example, a packet with a DSCP tag value of 1 can be assigned to the High queue.





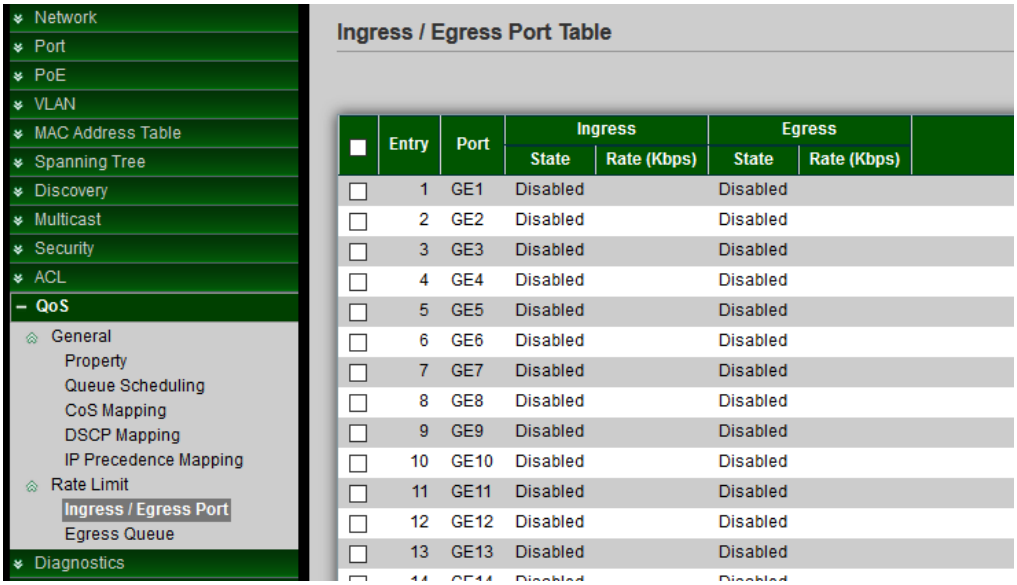
14.5 IP Precedence to Queue Mapping

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.



14.6 Rate Limit

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 1000000 Kbps

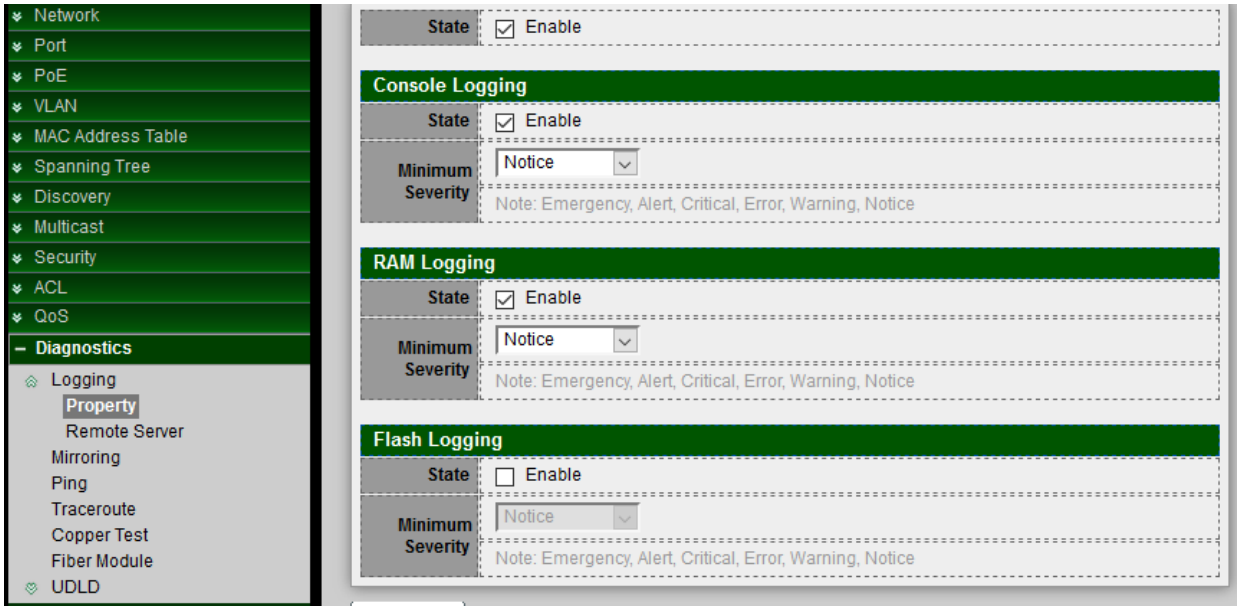


15. Diagnostics

15.1 Logging

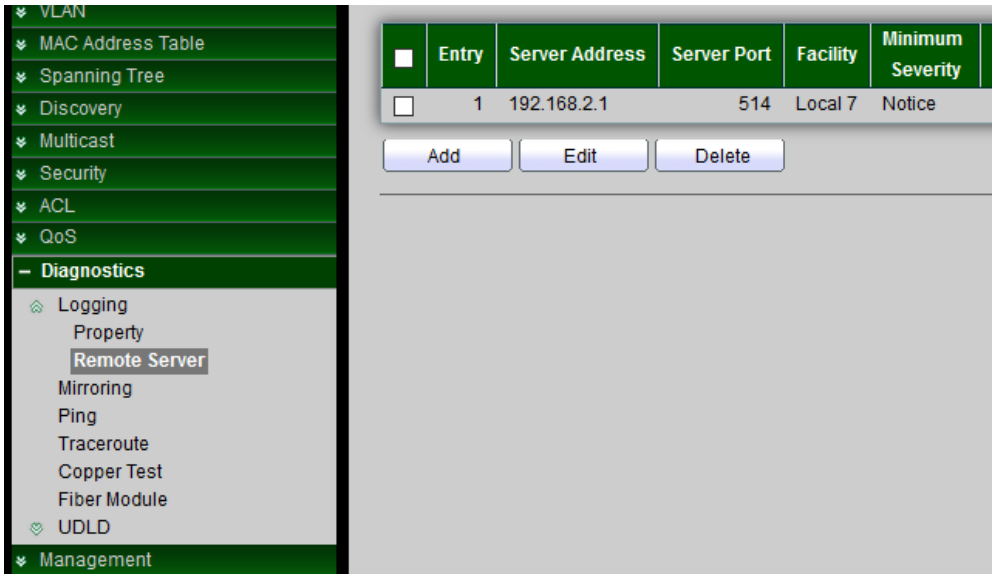
This function support log message includes Console / RAM / Flash message send to remote log server. Administrator can enable or disable this function.

Property



Remote Server

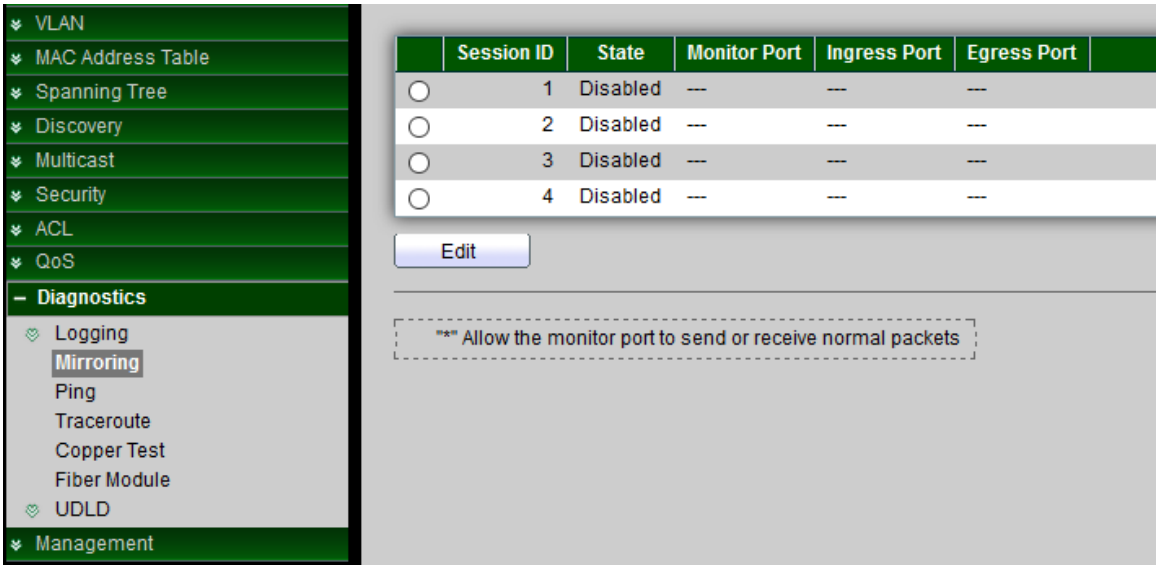
Use the Remote Log Servers page to define the remote SYSLOG servers where log messages are sent (using the SYSLOG protocol). For each server, you can configure the severity of the messages that it receives.

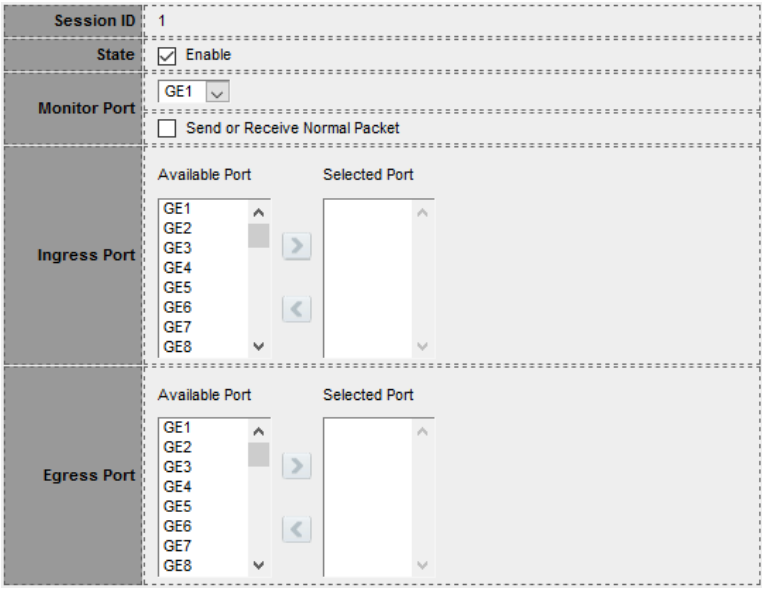


- **Address Type:** Administrator can select use Hostname or IPv4/6 connection remote log server.
- **Server Port:** Enter service port to which the log messages are sent.
- **Facility:** Select a facility from which system logs are sent to the remote server. Only one facility can be assigned to a server.
- **Minimum Severity:** Select the minimum level of system log messages to be sent to the server.

15.2 Mirroring

Mirroring function can mirror Rx/Tx traffic, Packet can mirror to destination port and for analysis.

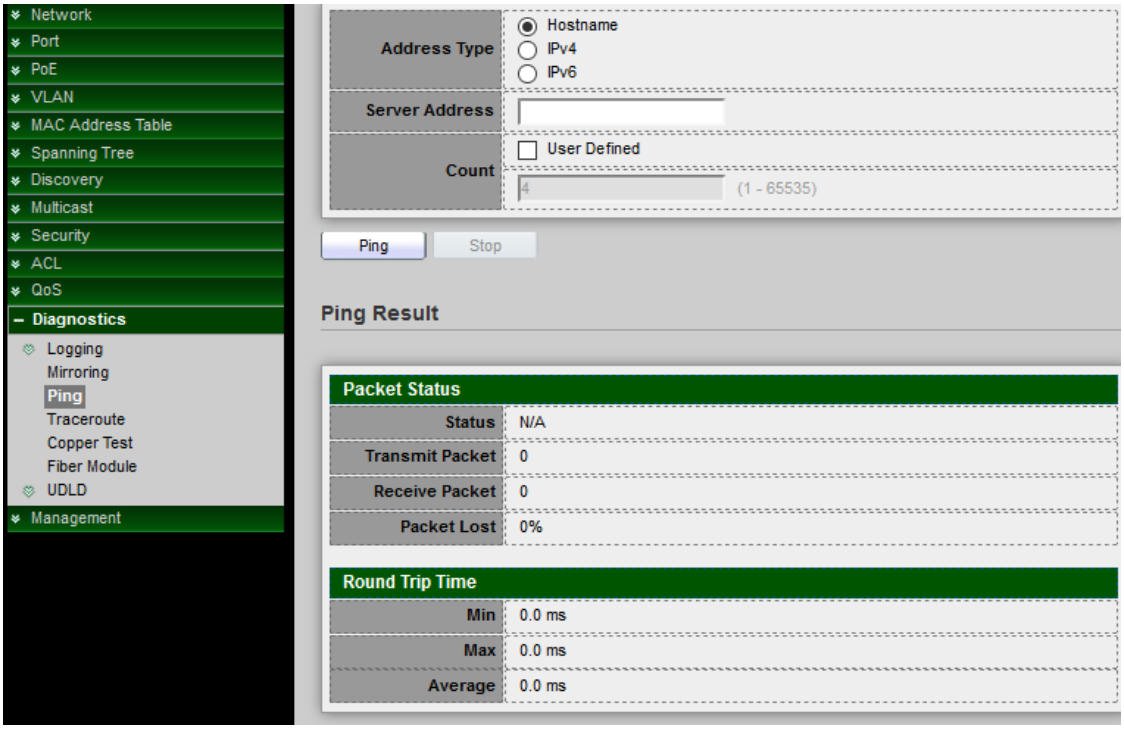




- **Mirroring Port:** Administrator can choose a mirroring Port.
- **Ingress Port:** Administrator can choose mirrored ports for ingress.
- **Egress Port:** Administrator can choose mirrored ports for egress.

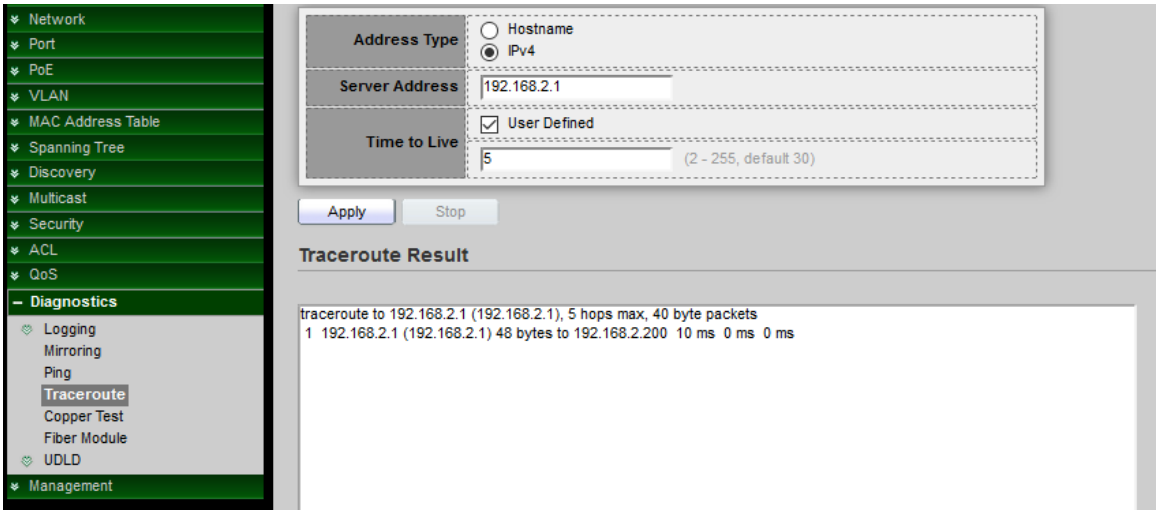
15.3 Ping

Administrators can use this ping function to check connected device whether is active. This ping function support IPv4 and IPv6 protocol.



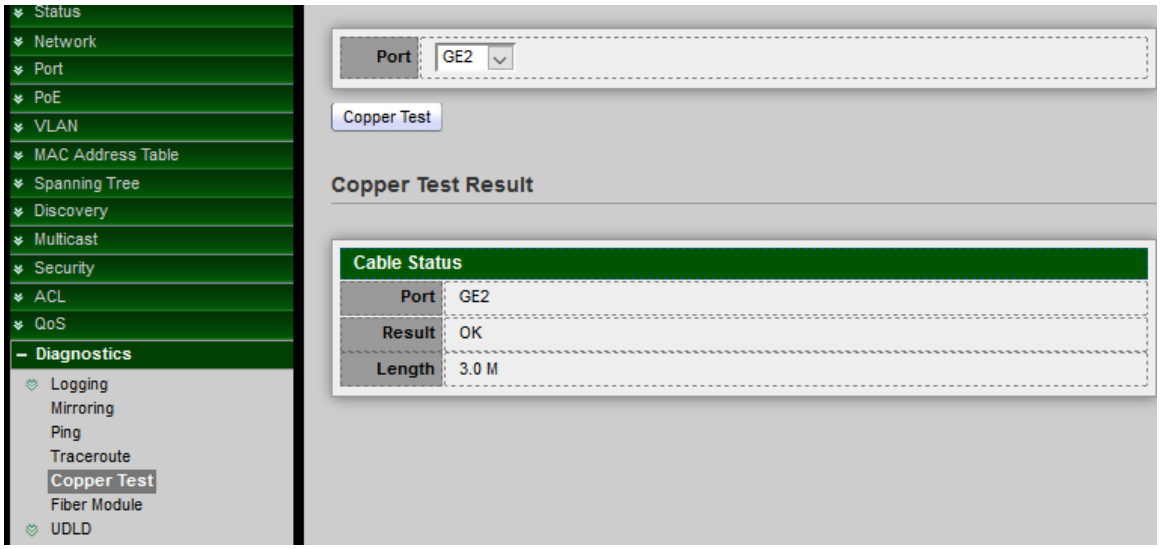
15.4 Traceroute

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.



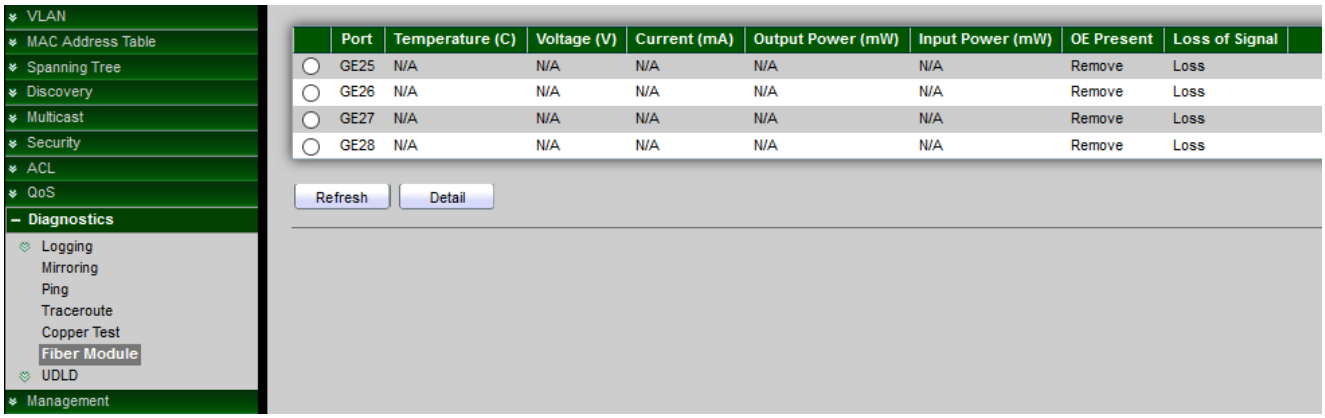
15.5 Copper Test

Administrator can use this function check port Result whether is working, if working then display OK.



15.6 Fiber Module

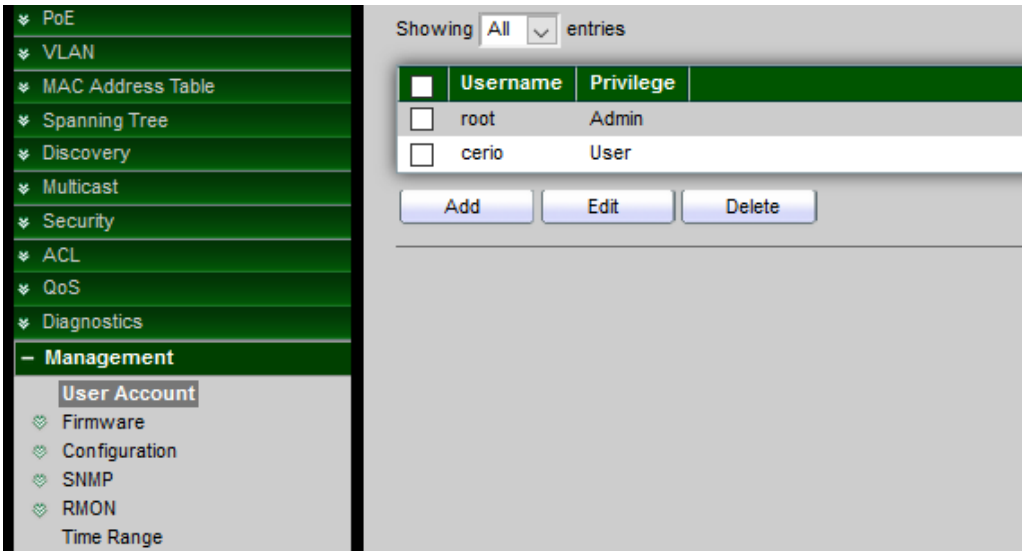
Display Fiber module messenger.



16. Management

16.1 User Account

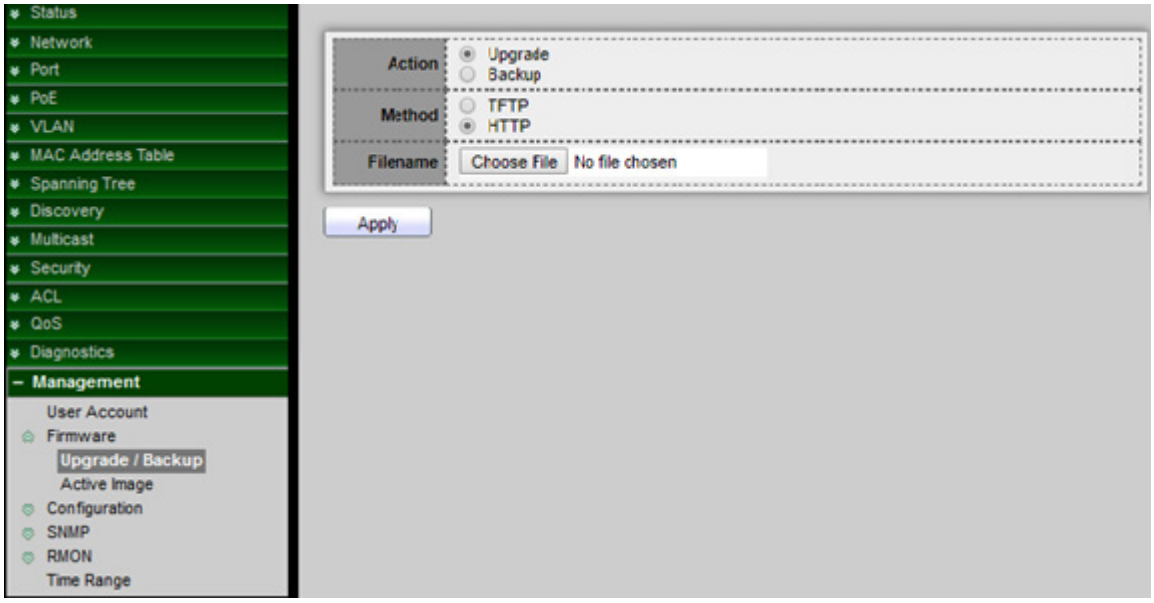
The default username/password is root/default. Administrator can modify login password or create new username / password and defined Privilege.



16.2 Firmware

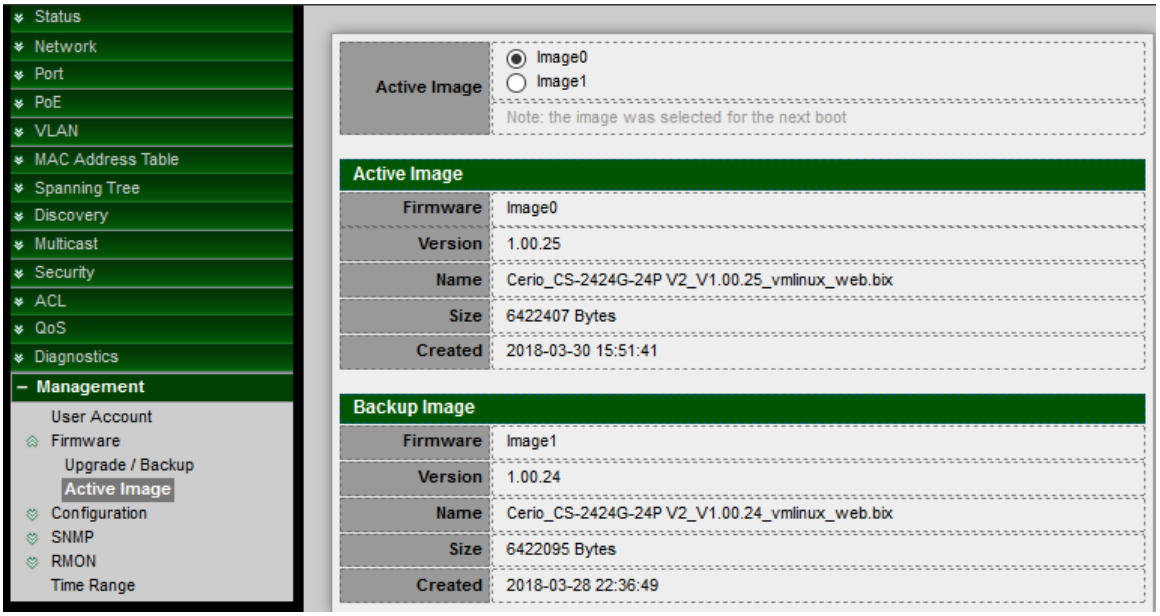
16.2.1 Upgrade / Backup

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.



16.2.2 Active Image

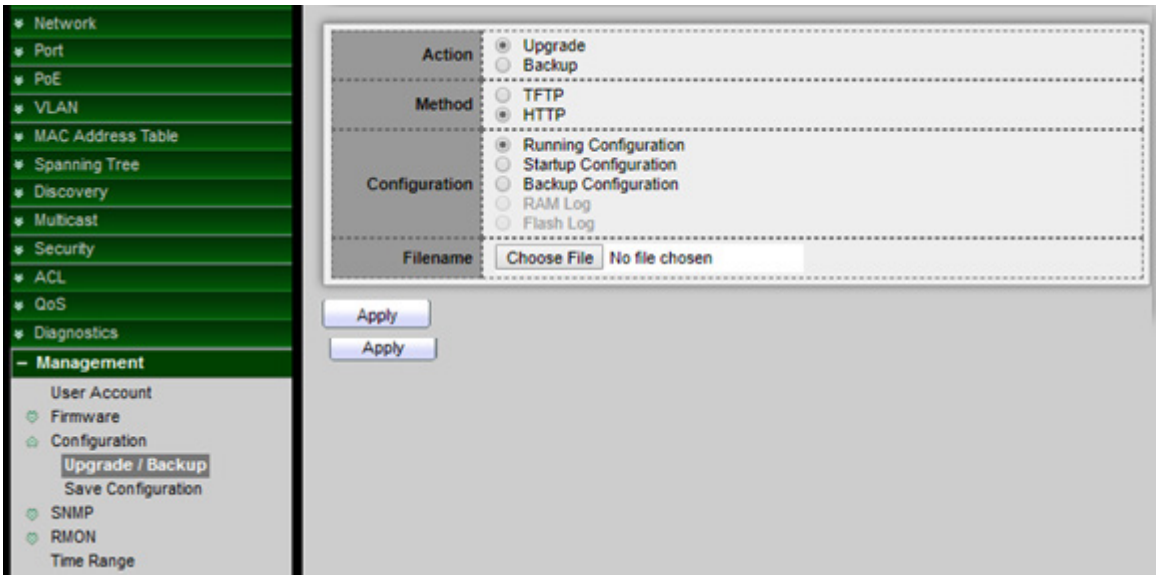
If the Switch has upload multiple firmware in system then administrator can choose a firmware to do system default start.



16.3 Configuration

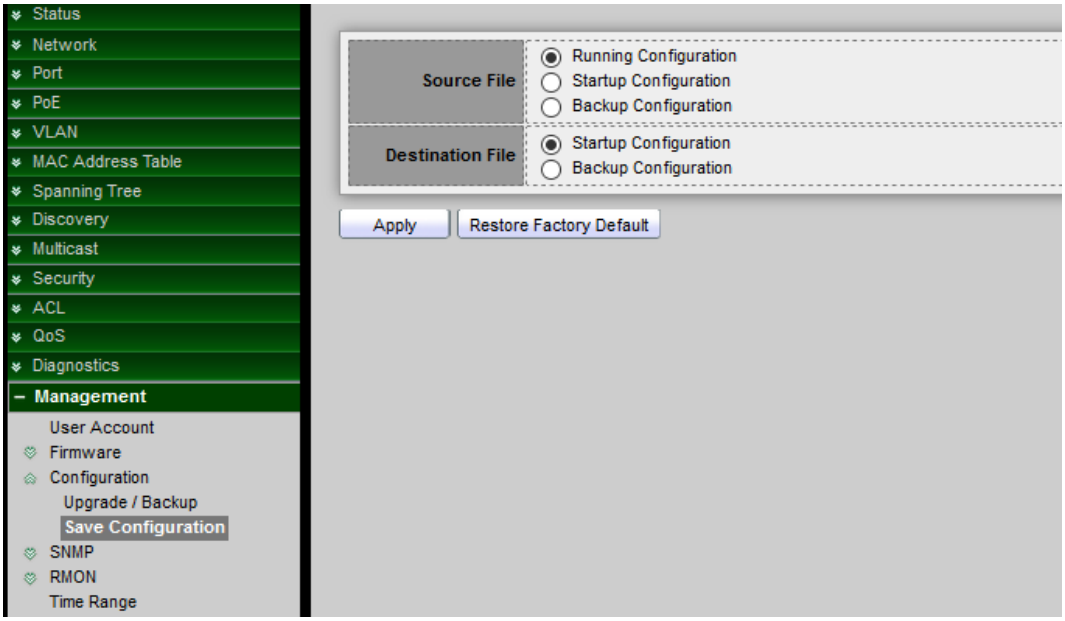
16.3.1 Upgrade / Backup

Administrator can backup system configuration file to PC or upload configuration file to Switch system.



16.3.2 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.



Source File

- Running Configuration to the Running Configuration, Startup Configuration or Backup Configuration.
- Startup Configuration to the Running Configuration, Startup Configuration, or Backup Configuration.
- Backup Configuration to the Running Configuration, Startup Configuration, or Backup Configuration.

Destination File

Select the configuration file type to be overwritten by the source file

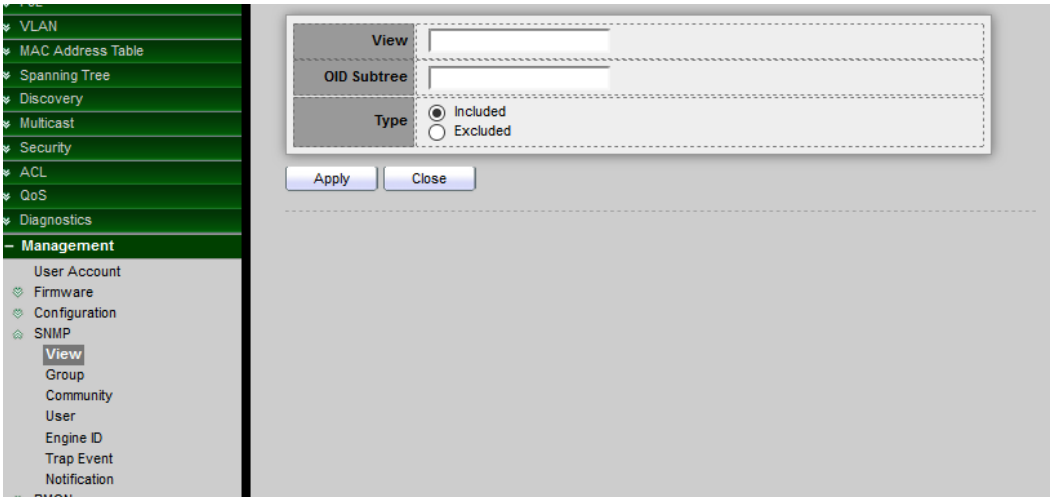
- Restore Factory Default button is reset system to default.

16.4 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.

16.4.1 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.



- **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.

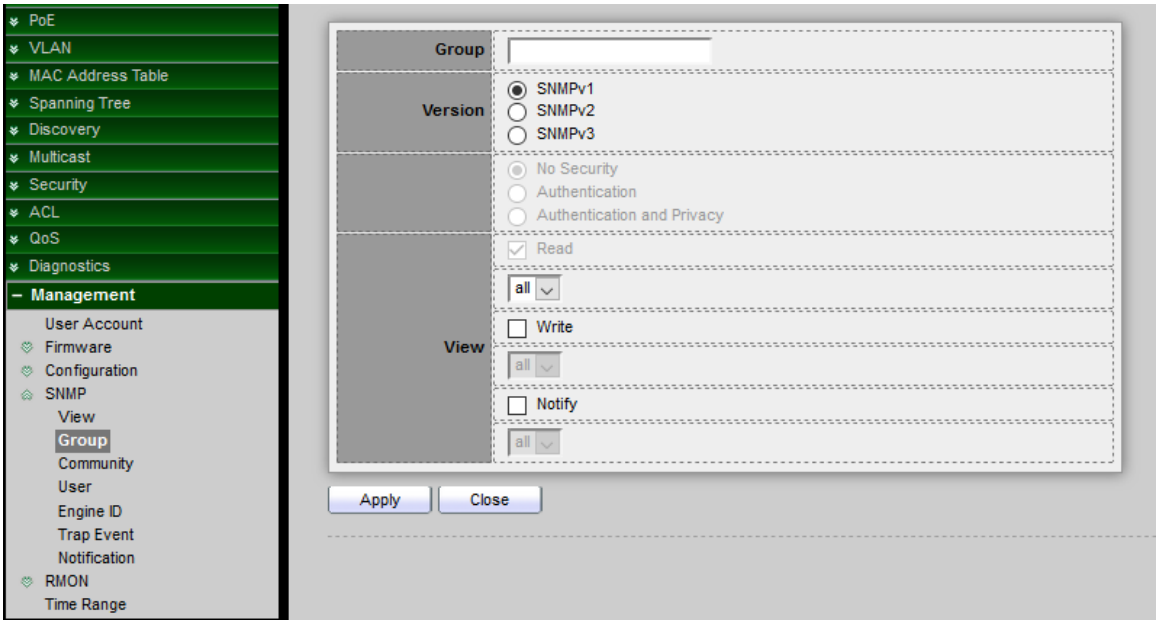
➢ **Type:**

Include: Check to include the selected MIBs in this view

Excluded: Check to Excluded the selected MIBs in this view

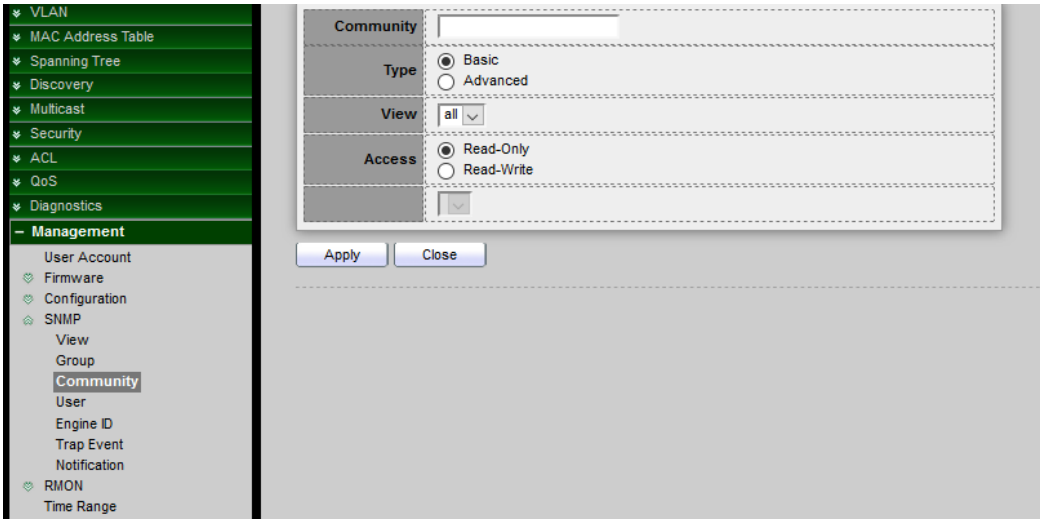
16.4.2 Group

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.



16.4.3 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.



- **Type:**

  Basic: 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: 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.

- **Access:**

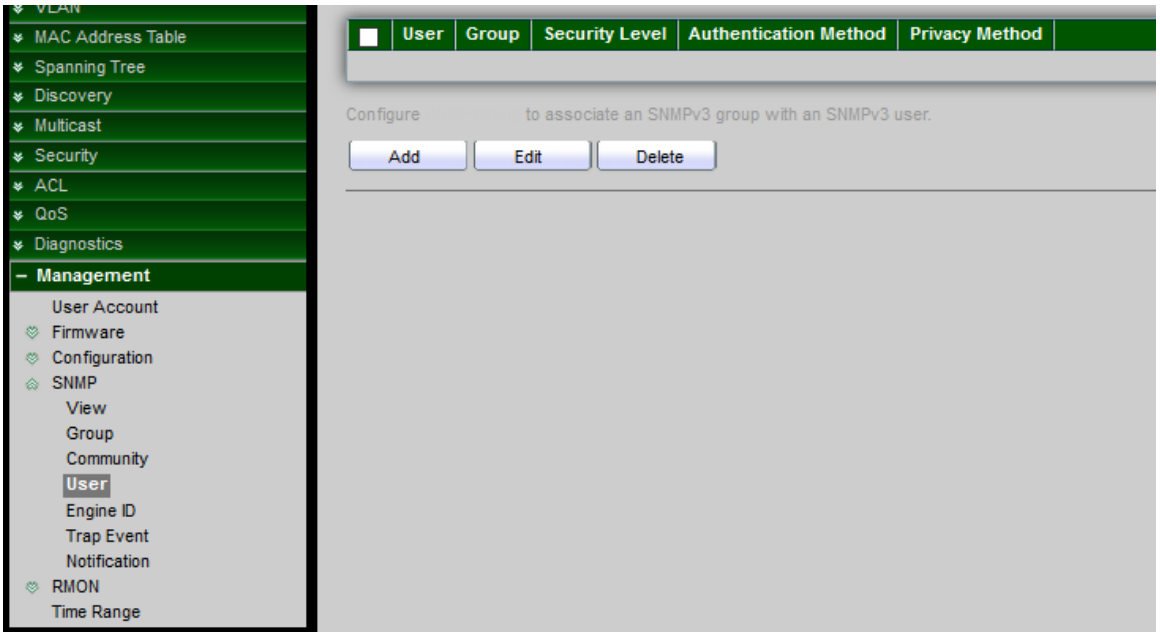
  Read Only: Management access is restricted to read-only. Changes cannot be made to the community.

  Read Write: Management access is read-write. Changes can be made to the switch configuration, but not to the community.

16.4.4 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.

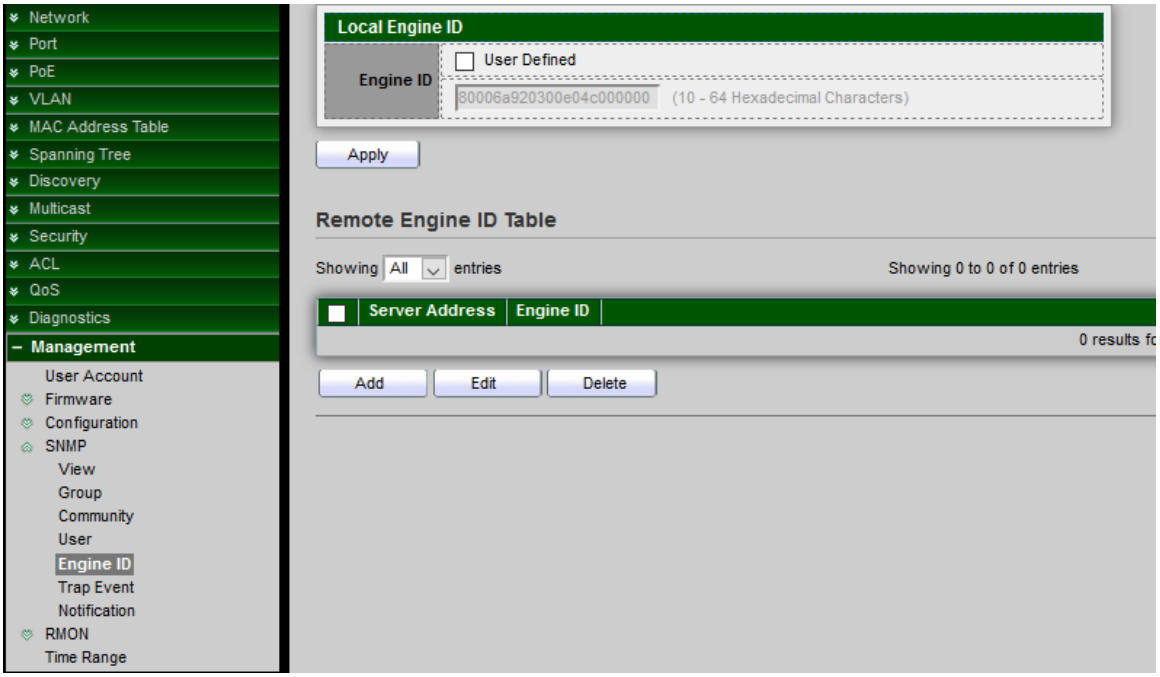
Groups enable network managers to assign access rights to a group of users, instead of a single user. A user can only be a member of a single group.
Administrator need to create a SNMPv3 user, a SNMPv3 group must be available.



16.4.5 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.

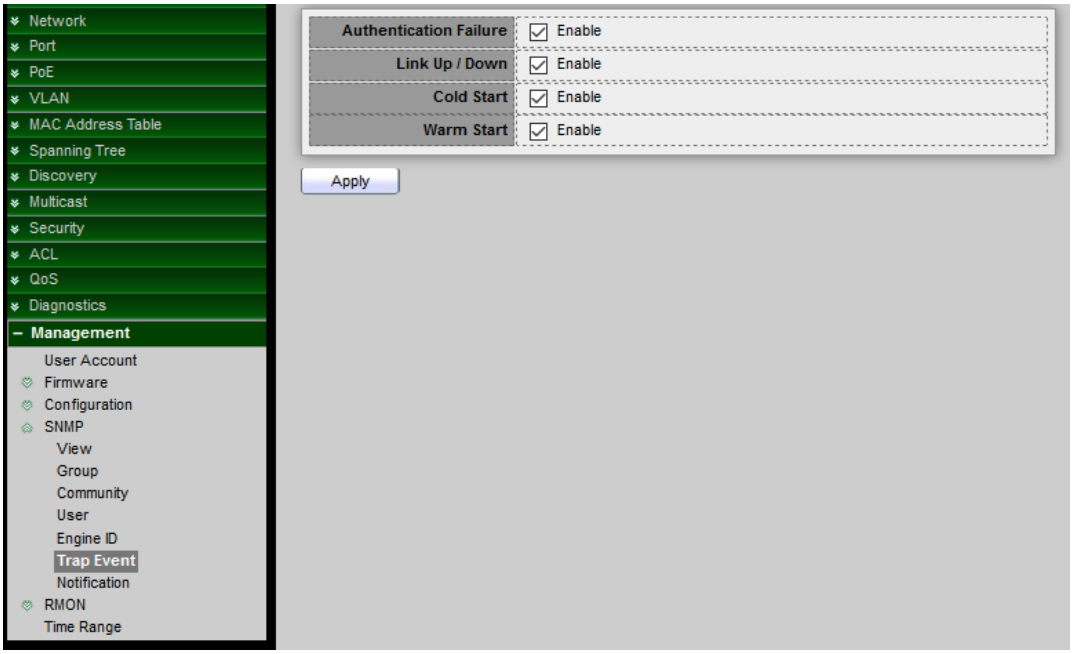


- **User Defined:** The field value is a hexadecimal string (range: 10 to 64). Each byte in the hexadecimal character strings is represented by two hexadecimal digits.

16.4.6 Trap Event

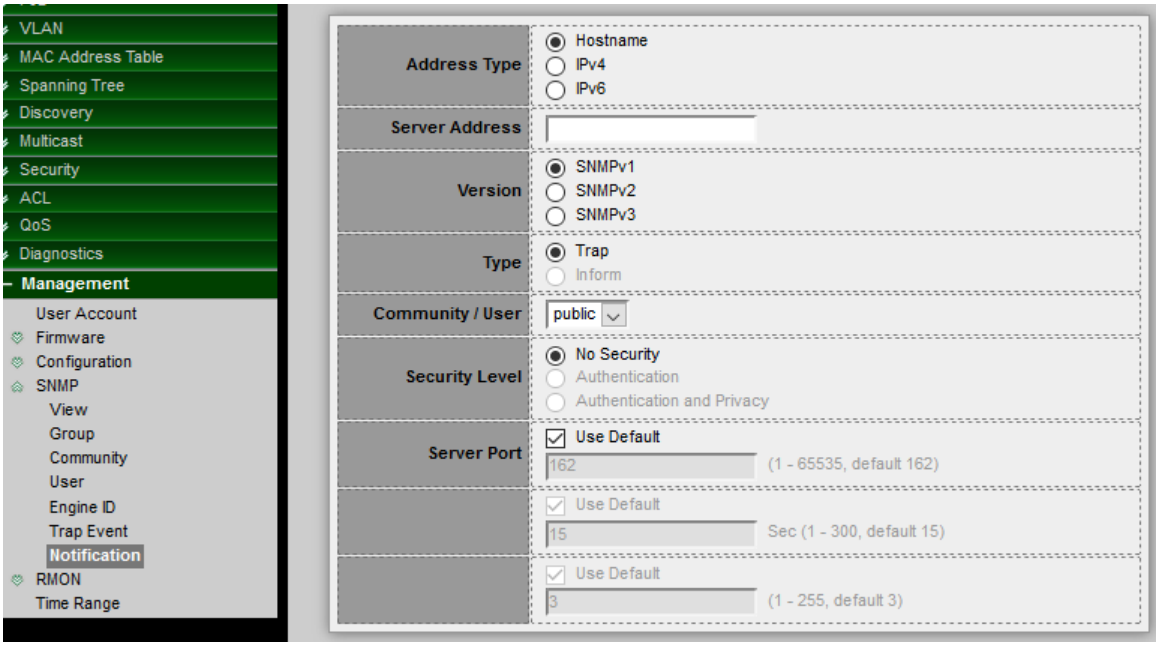
Administrator can choose SNMP Trap Event Type to monitor

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.



16.4.7 Notification

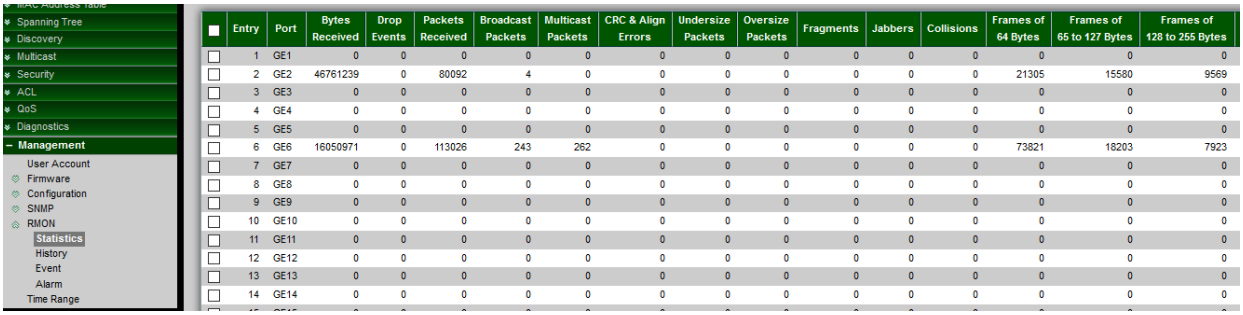
Notification is network nodes where the trap messages are sent by the switch. A list of notification recipients are defined as the targets of trap messages. A trap receiver entry contains the IP address of the node and the SNMP credentials corresponding to the version that will be included in the trap 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.



16.5 RMON

16.5.1 Statistics

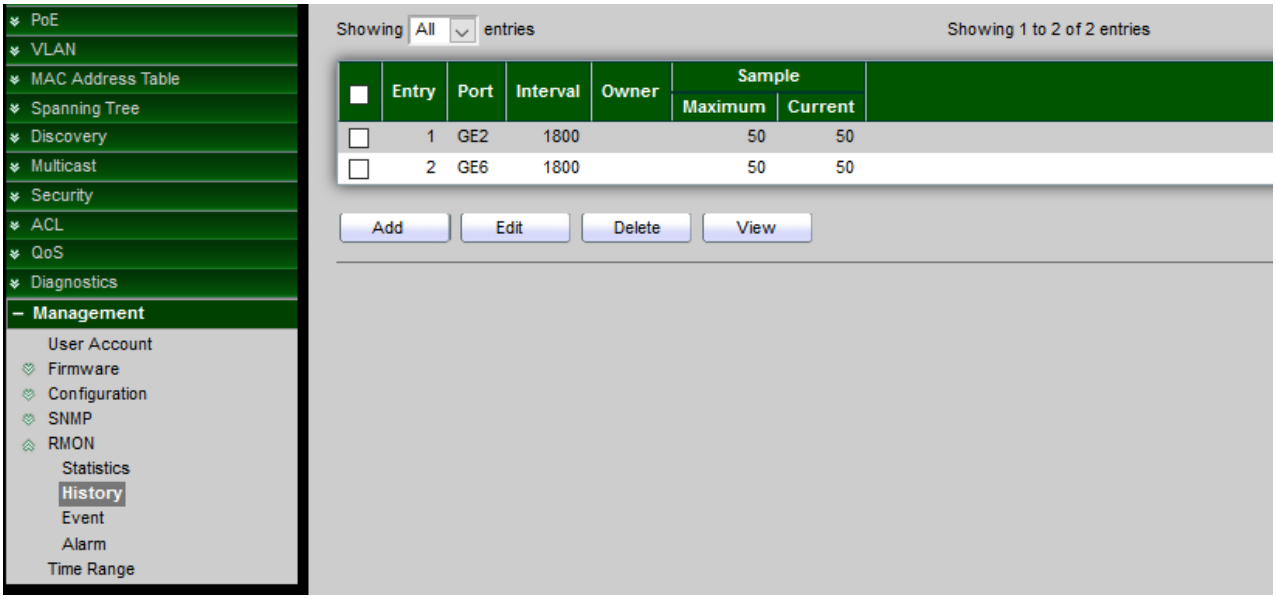
The page displays traffic statistics per interface. The refresh rate of the information can be selected. This page is useful for analyzing the amount of traffic that is both sent and received and its dispersion (Unicast, Multicast, and Broadcast).



Entry	Port	Bytes Received	Drop Events	Packets Received	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets	Oversize Packets	Fragments	Jabbers	Collisions	Frames of 64 Bytes	Frames of 65 to 127 Bytes	Frames of 128 to 255 Bytes
1	GE1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	GE2	46761239	0	80092	4	0	0	0	0	0	0	0	21305	15580	9569
3	GE3	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	GE4	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	GE5	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	GE6	16050971	0	113026	243	262	0	0	0	0	0	0	73821	18203	7923
7	GE7	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	GE8	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	GE9	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	GE10	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	GE11	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	GE12	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	GE13	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	GE14	0	0	0	0	0	0	0	0	0	0	0	0	0	0

16.5.2 History

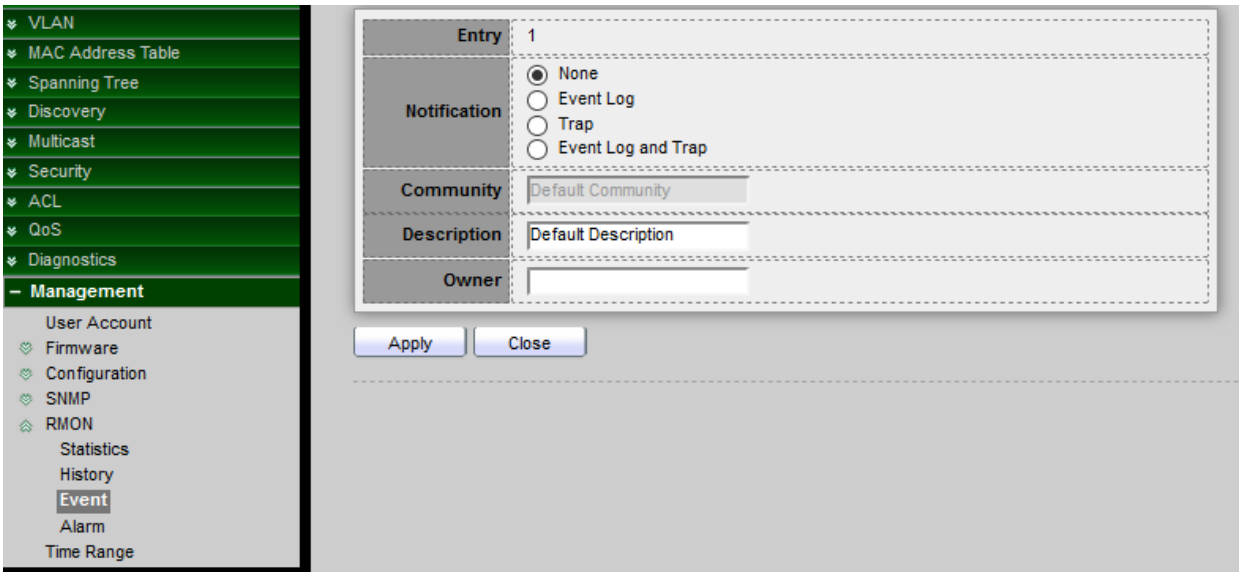
Use the History Control Table page to define the sampling frequency, amount of samples to store, and the interface from where to gather the data. After the data is sampled and stored, it appears on the History Table page that can be viewed by clicking History Table.



- **Max Sample:** Enter the number of samples to store.
- **Interval:** Enter the time in seconds that samples were collected from the interface.
- **Owner:** Enter the RMON station or user that requested the RMON information.

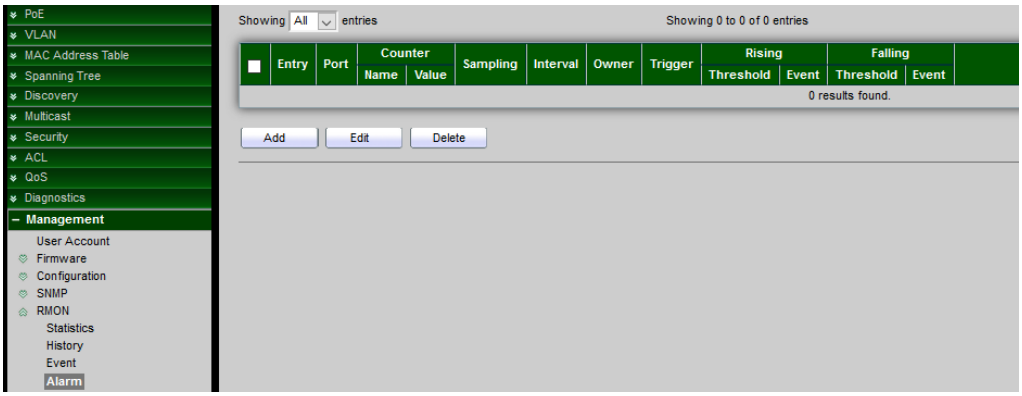
16.5.3 Event

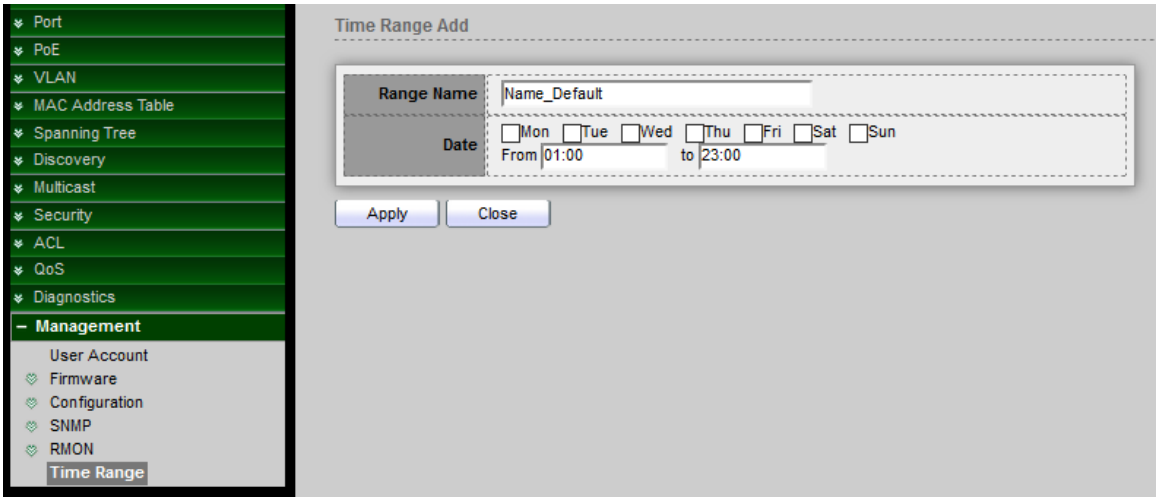
Events page to configure events that are actions performed when an alarm is generated (alarms are defined on the Alarms page). An event can be any combination of logs and traps. If the action includes logging of the events, they are displayed on the Event Log Table page.



16.5.4 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.



16.6 Time Range

Administrator can set time rule in page.