# CERIO Corporation

# CS-2408G

**8 Port 10/100/1000M Gigabit Web Managed Switch with 4**

**Combo Gigabit Ports**

**User's 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.

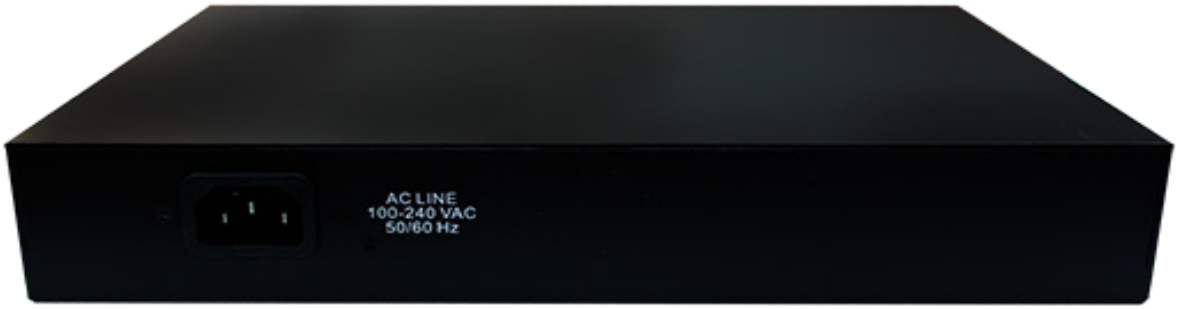
**CE Mark Warning**

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. Introduction

## 1.1 Front Panel


## 1.2 Rear Panel Layout




# 2. Software Configuration

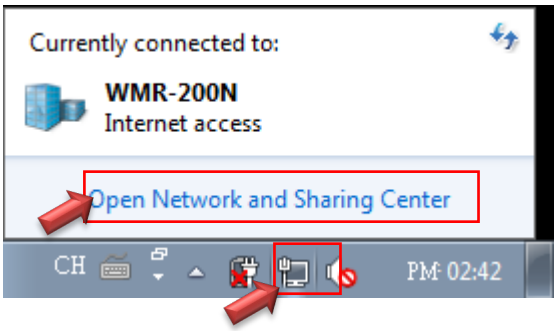
**CS-2408G** supports web-based configuration. Upon the completion of hardware installation, **CS-2408G**can be configured through a PC/NB by using its web browser such as Internet Explorer 6.0 or later.

Set the IP segment of the administrator's computer to be in the same range as **CS-2408G**for accessing the system. Do not duplicate the IP Address used here with IP Address of **CS-2408G**or any other device within the network. **Please refer to the following steps**

## Example of Segment: (Windows 7)

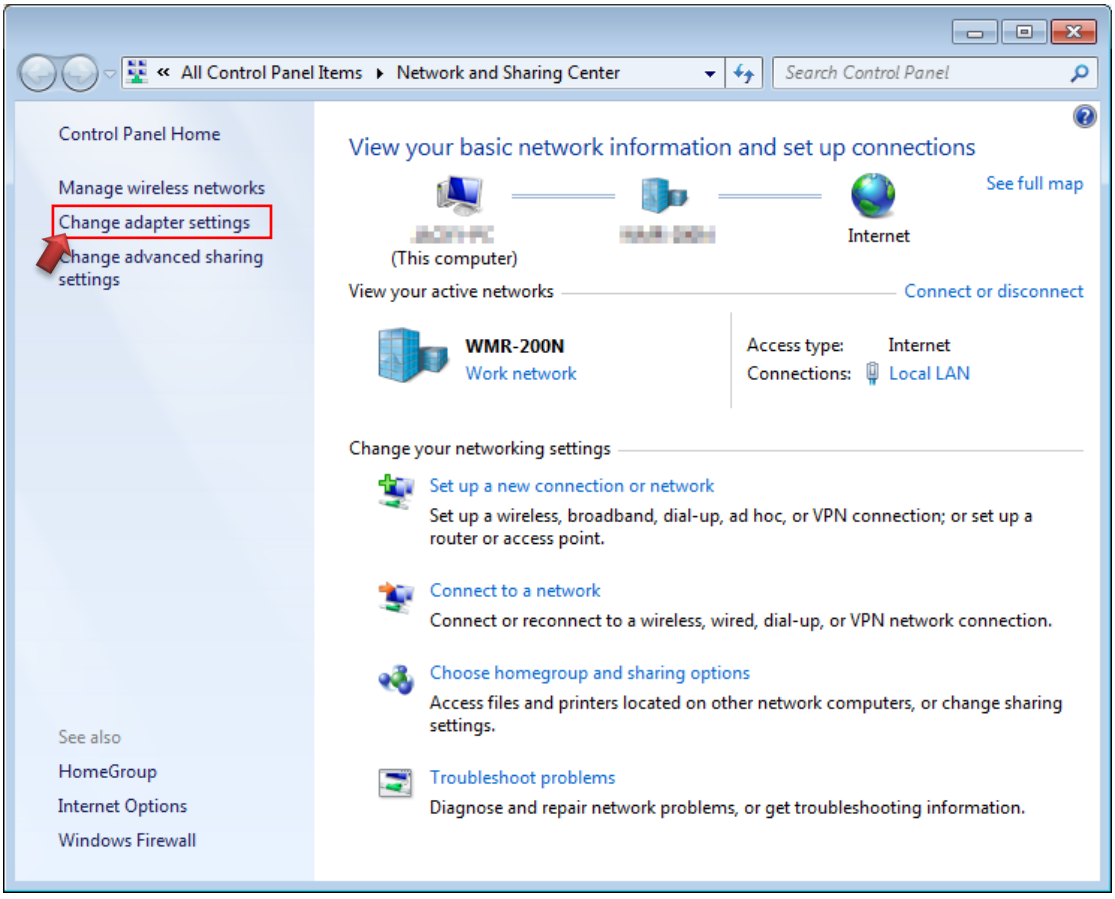
**Step 1 :**

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



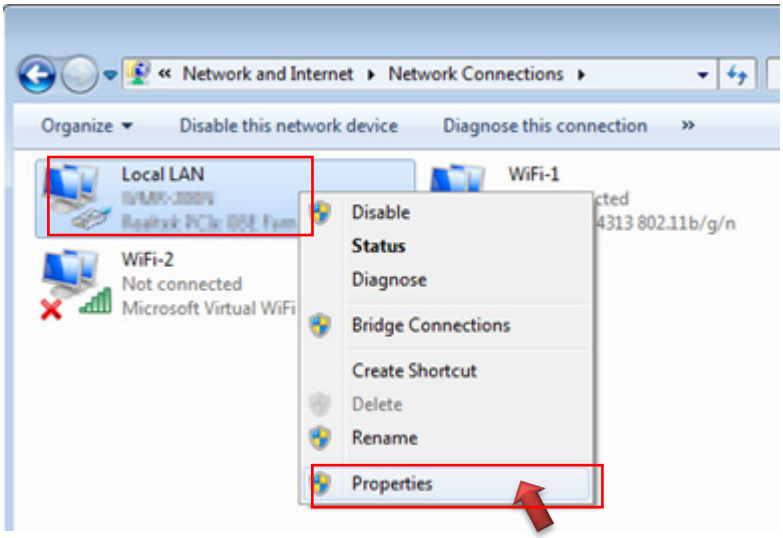

**Step 2 :**

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



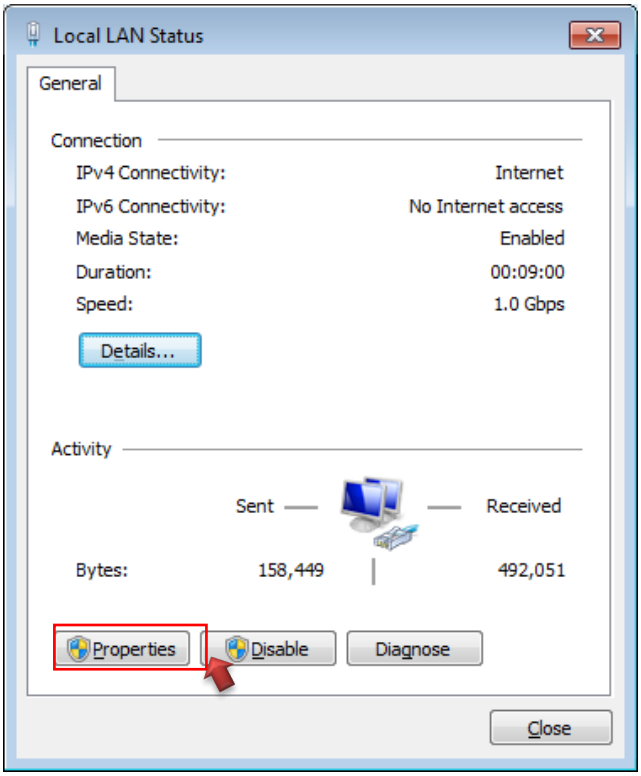
### Step 3 :

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



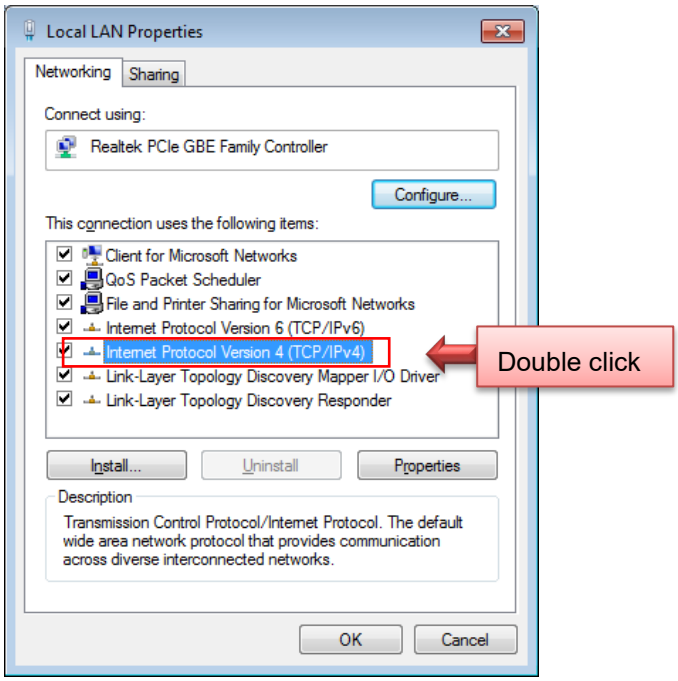

### Step 4 :

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



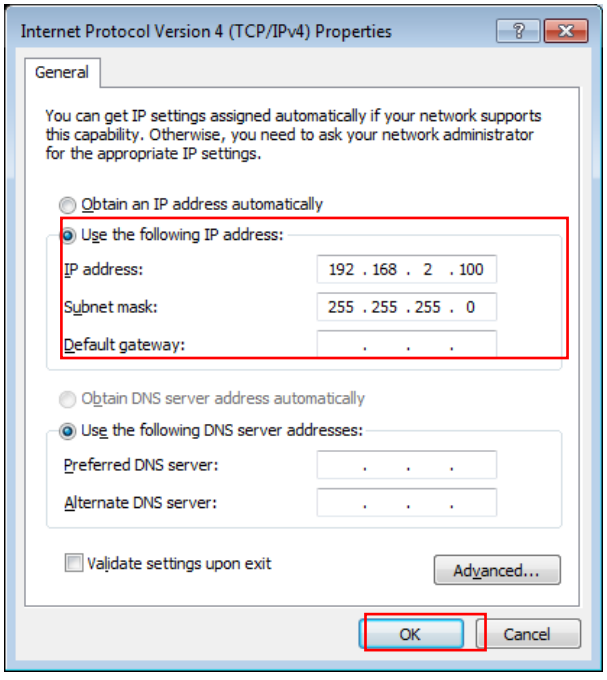

**Step 6 :**

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

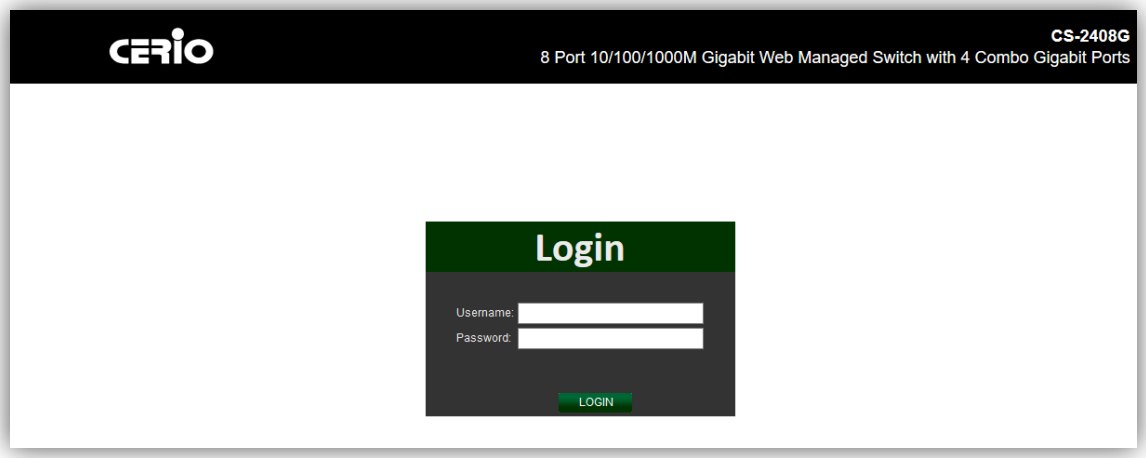
And Click **"OK"** to complete fixing the computer IP settings



**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 (https://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.*

## System login username and password information

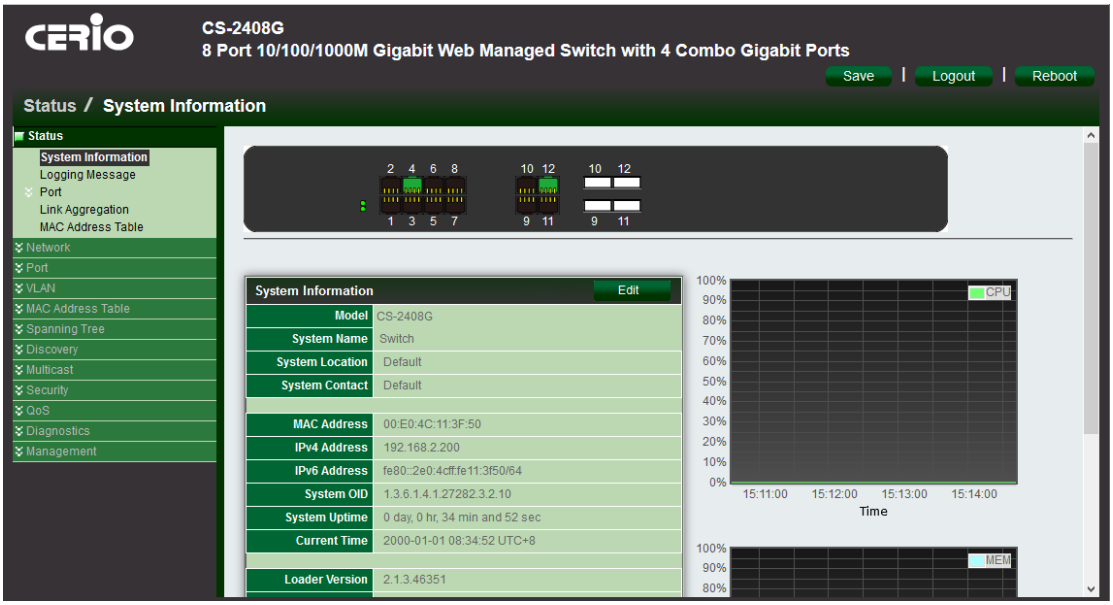
The **CS-2424G** web switch default IP is 192.168.2.200

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 |

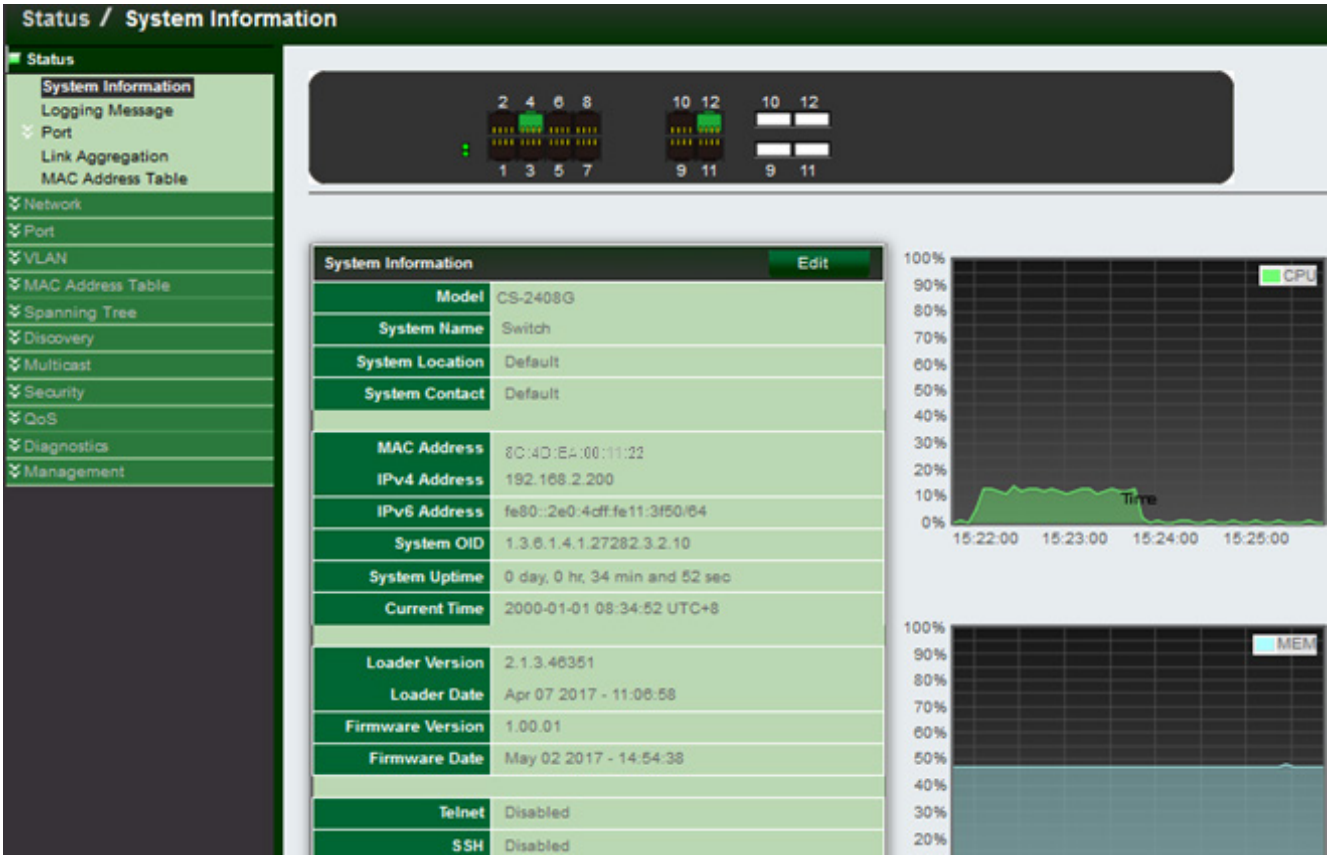
After the authentication procedure, the home page will shows up. Select one of the configurations by clicking the icon.




# 3. Status

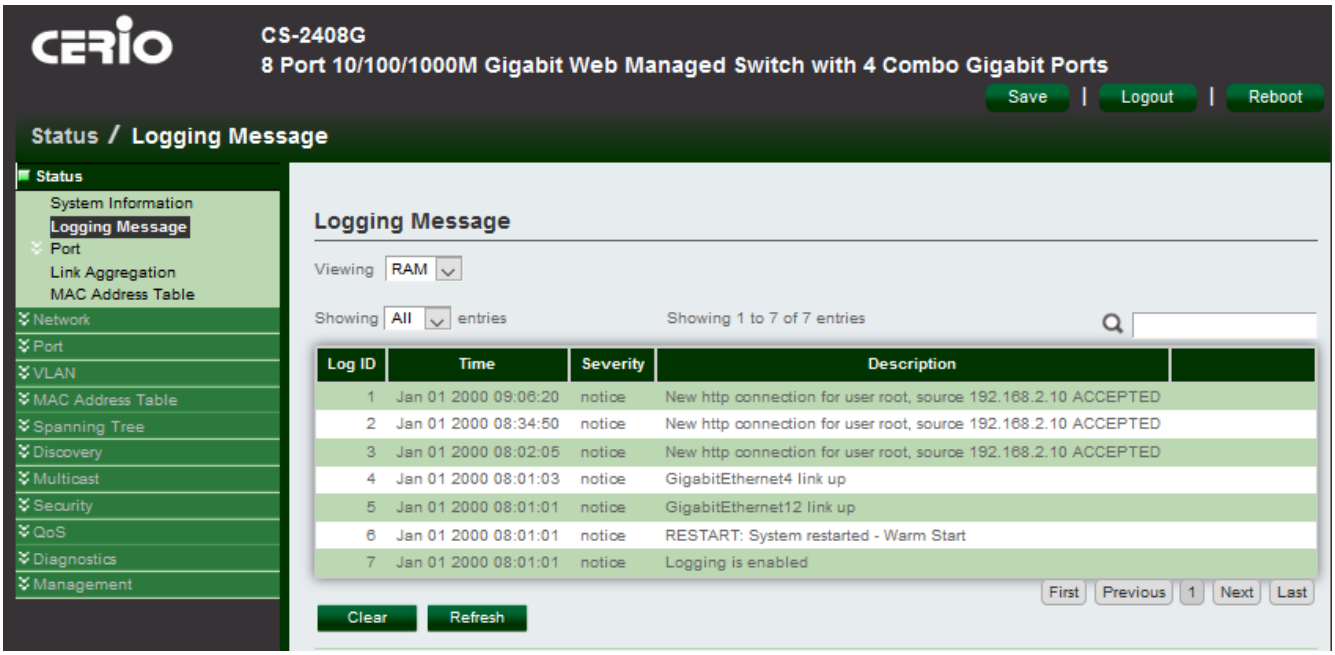
## 3.1 System Information

This administrator can check CS-2408G system information from.



## 3.2 Logging Message

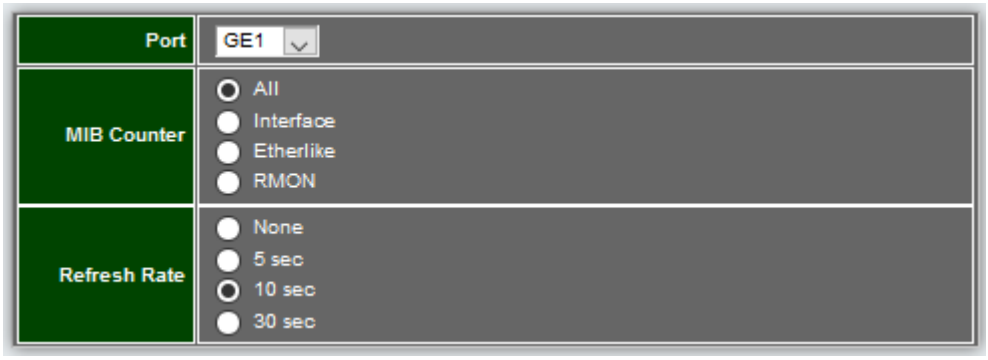
Administrator can viewing RAM or Flash message




## 3.3 Port

### 3.3.1 Statistics

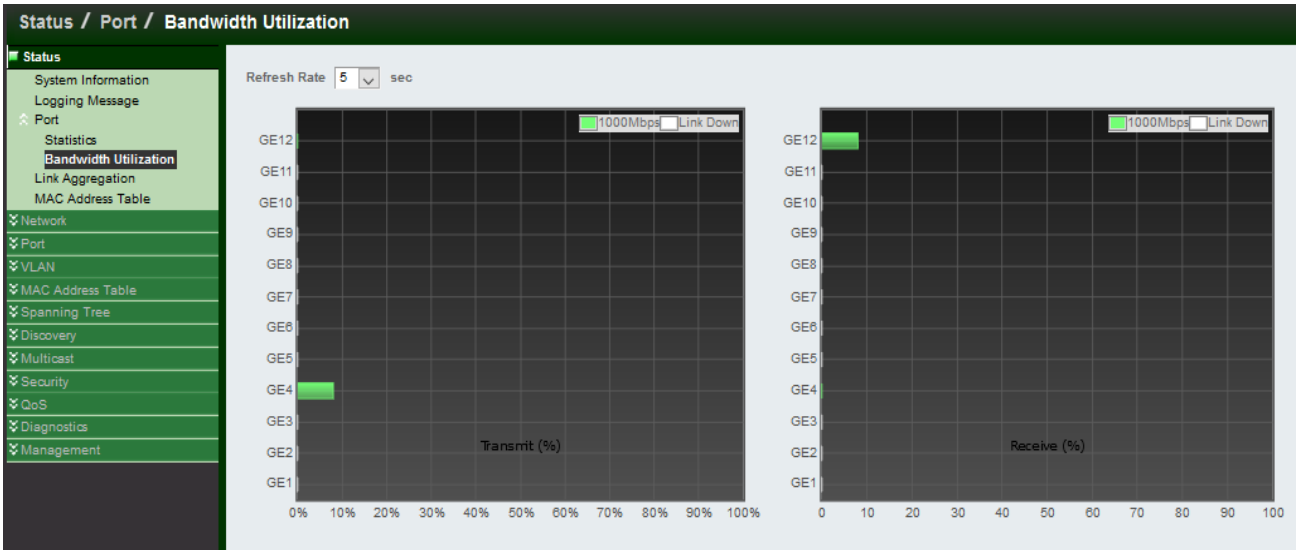
The status support MIB Counter function, Administrator can choose specific port to monitor "Interface", "Etherlike" and "RMON" information.




- **Port:** Administrator can select specific port.
- **MIB Counter:** Administrator can choose MIB type.
- **Refresh Rate:** Administrator can choose seconds to monitor.

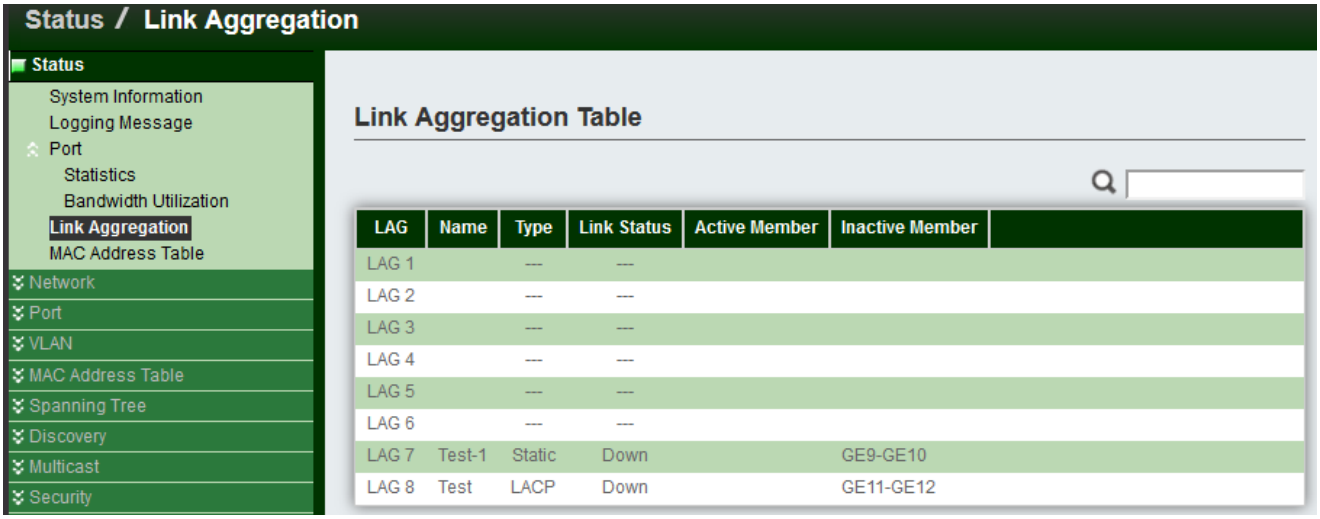
### 3.3.2 Bandwidth Utilization

Administrator can instantly watch TX/RX traffic for all port.




## 3.4 Link Aggregation Table

If administrator have set 5.2 Link Aggregation functions, when can monitor LACP status in this page.

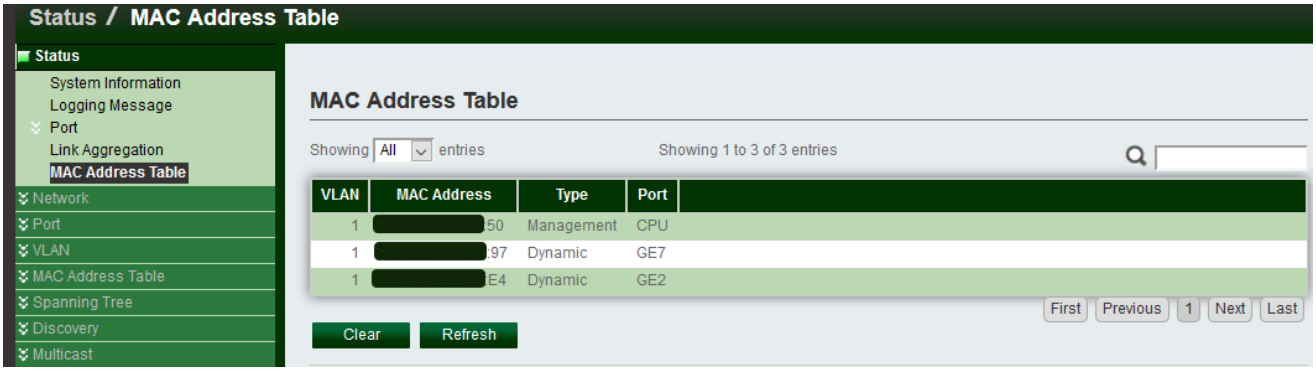



| LAG | Name | Type | Link Status | Active Member | Inactive Member |
|---|---|---|---|---|---|
| LAG 1 | | --- | --- | | |
| LAG 2 | | --- | --- | | |
| LAG 3 | | --- | --- | | |
| LAG 4 | | --- | --- | | |
| LAG 5 | | --- | --- | | |
| LAG 6 | | --- | --- | | |
| LAG 7 | Test-1 | Static | Down | | GE9-GE10 |
| LAG 8 | Test | LACP | Down | | GE11-GE12 |

- **LAG:** Link Aggregation Group.
- **Name:** LAG name.
- **Type:** LAG used type.
- **Link Status:** Display whether it working.
- **Active Member:** Display that active member by sending LACP data units (LACPDUs).
- **Inactive Member:** Display that interfaces member by sending LACP data units (LACPDUs).

## MAC Address Table

Administrator can monitor all connection used MAC address of the port.




- **VLAN:** Display VLAN number.
- **MAC Address:** Display device MAC address information.
- **Type:** Display connected type.
- **Port:** Display port number.

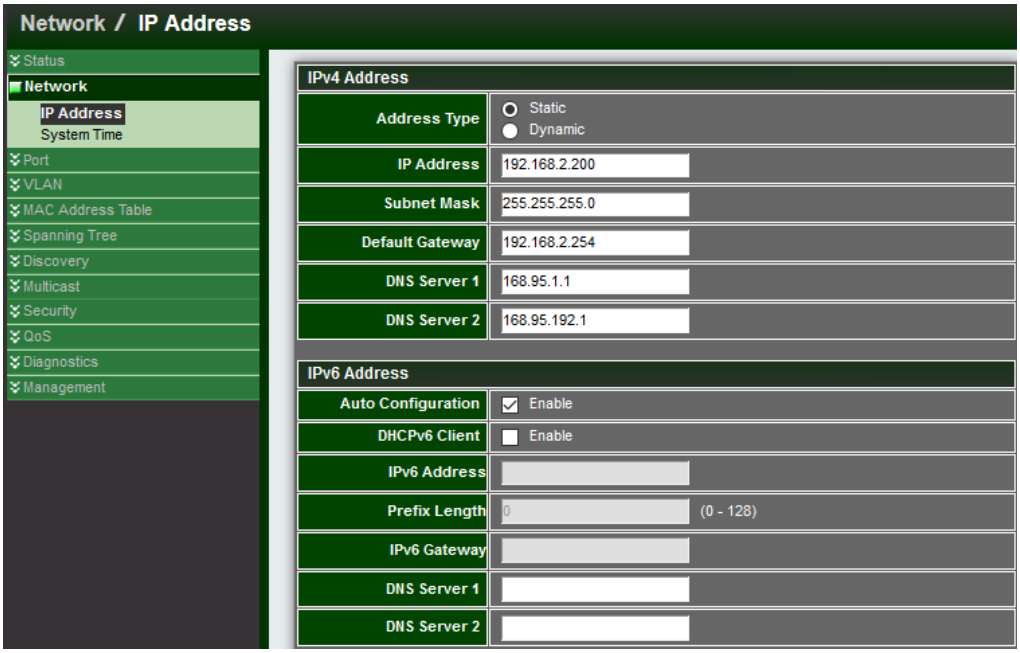
# 4. Network

Administrator can set IPv4/v6 address and system time of the switch.

## 4.1 IP Address

Administrator can set IP address / Subnet Mask / Gateway and DNS in this page.

The Switch default IP address is 192.168.2.200.



**#IPv4 Address:**

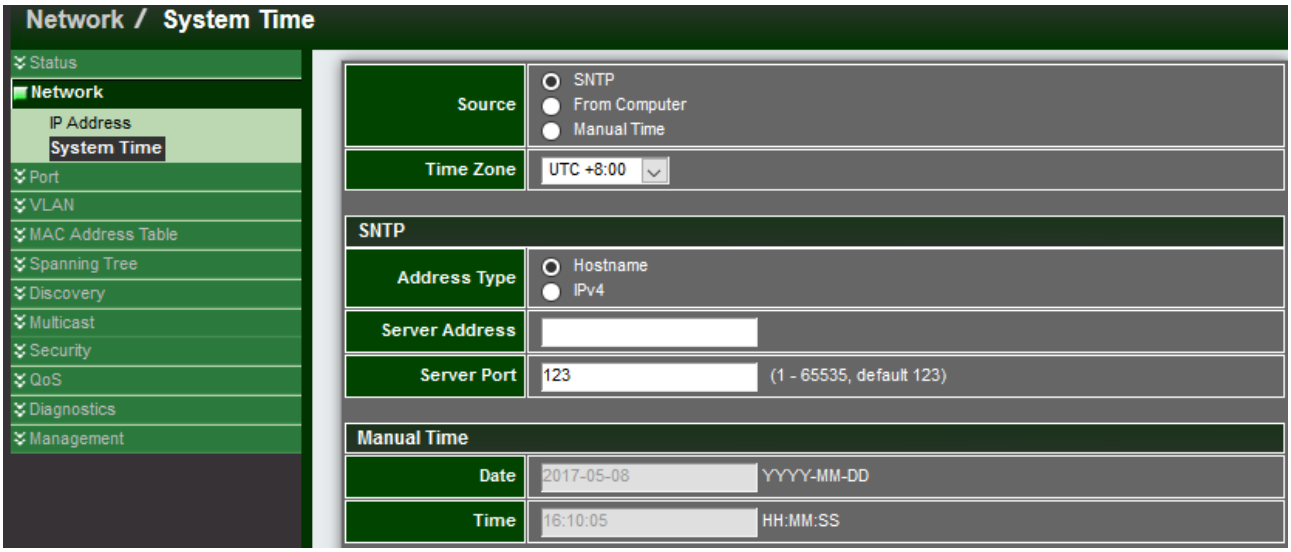
- **Address Type:** Administrator can choose Static or dynamic of the IP address type.
- **IP Address:** Administrator can set IP address of the switch.
- **Subnet Mask:** Set Mask for IP address.
- **Default Gateway:** Set IP address for Gateway.
- **DNS1/2:** Set IP address for DNS.

**#IPv6 Address:**

- **Auto configuration:** Administrator can choose Enable or Disable.
- **DHCP IPv6 client:** Administrator can choose Enable or Disable.
- **IPv6 Address/Prefix Length/IPv6 Gateway:** If administrator to disable "auto configuration" function then administrator can manual set this functions.

## 4.2 System Time

Administrator can set system time for the switch.

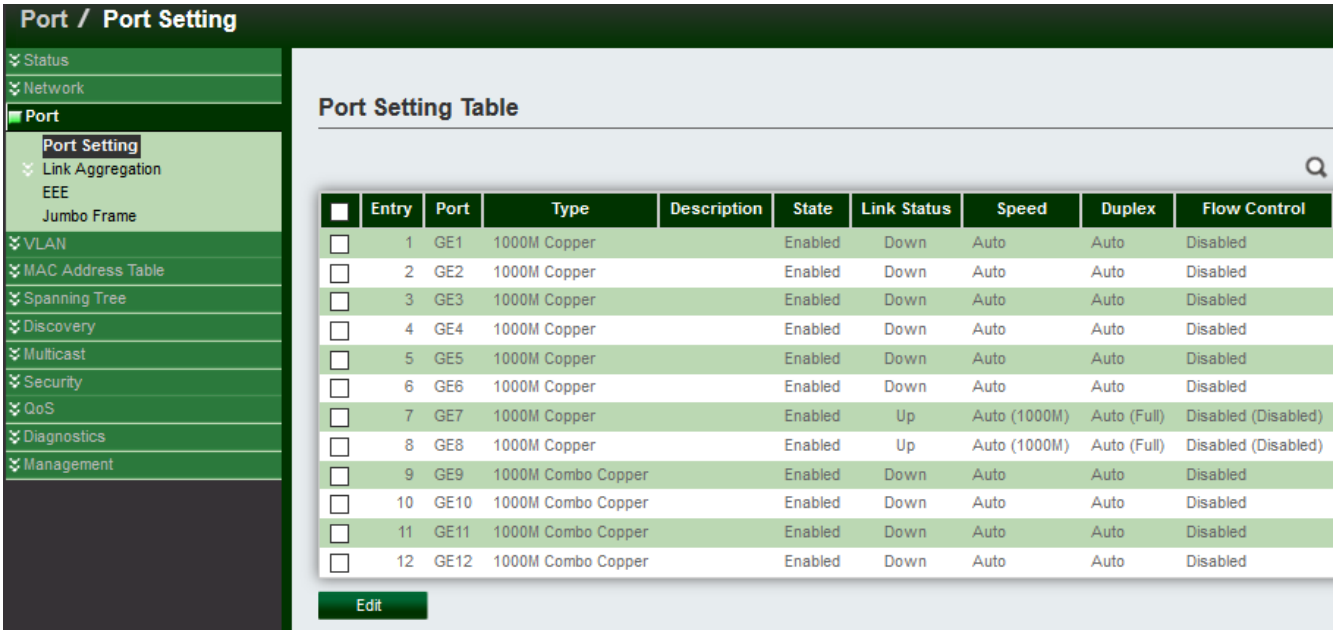


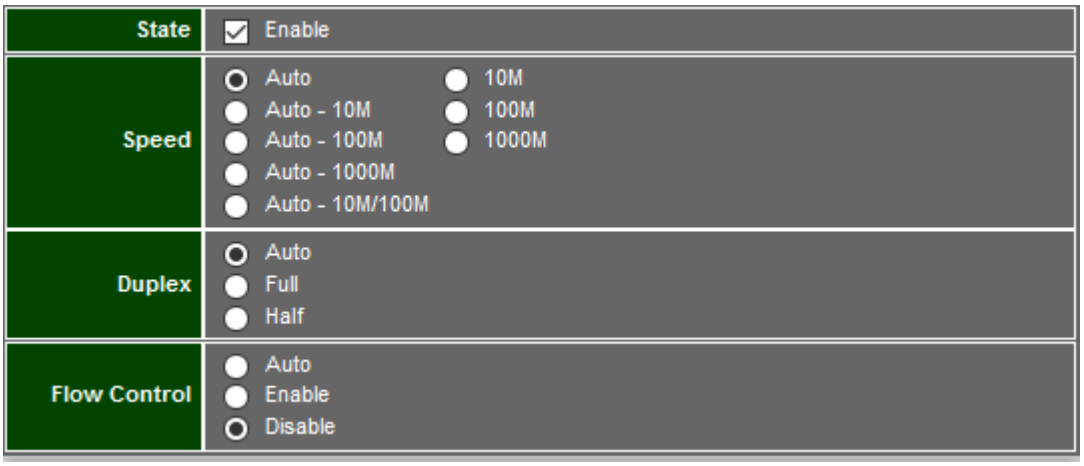

- **Source:** Administrator can choose update time by SNTP / From computer or Manal Time.
- **Time Zone:** Set time zone.
- **SNTP:** If administrator chooses use SNTP mode then need to set time server address.
- **Manual Time:** If administrator chooses to manual time then can manual set this system time.
- **Daylight Saving Time:** Administrator can Disable or Enable daylight saving time function.

# 5. Port

## 5.1 Port setting

Administrator can disable port or set port speed and flow control.



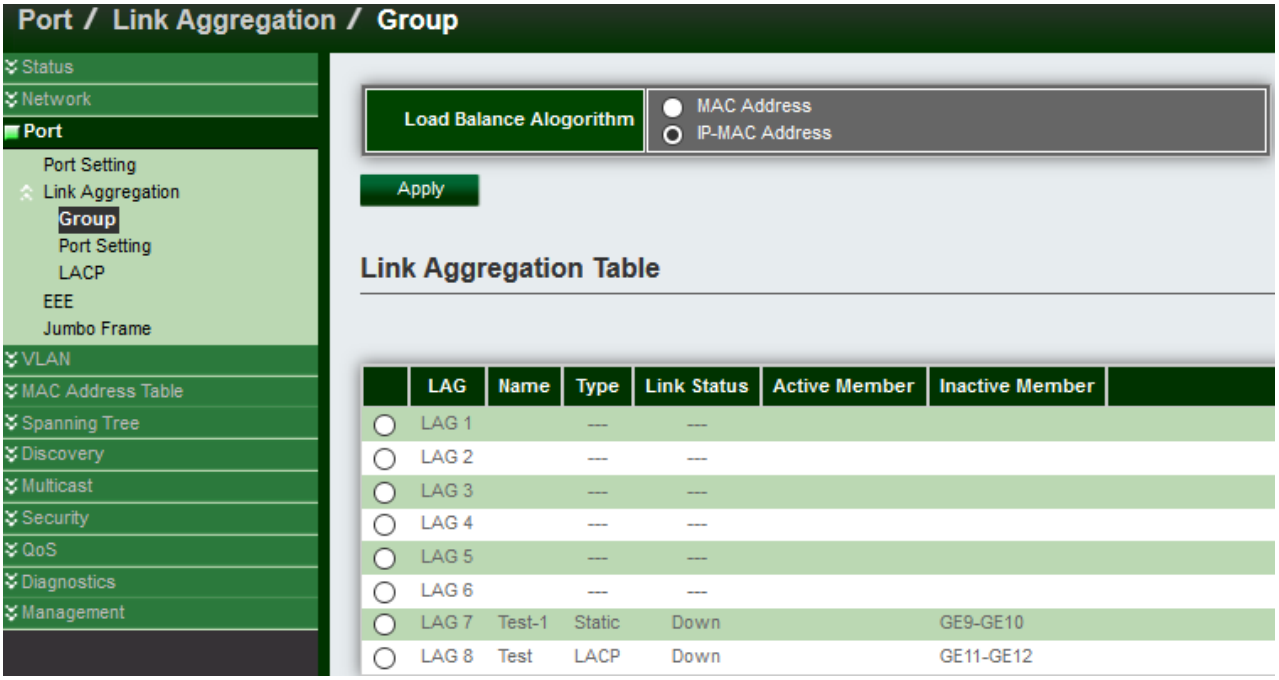




- **State:** Administrator can choose enable or disable Port.
- **Speed:** Administrator can manual set port speed or auto detection.
- **Duplex:** Administrator can manual set full/Half or Auto.
- **Flow Control:** Administrator can choose Enable or Disable or Auto.

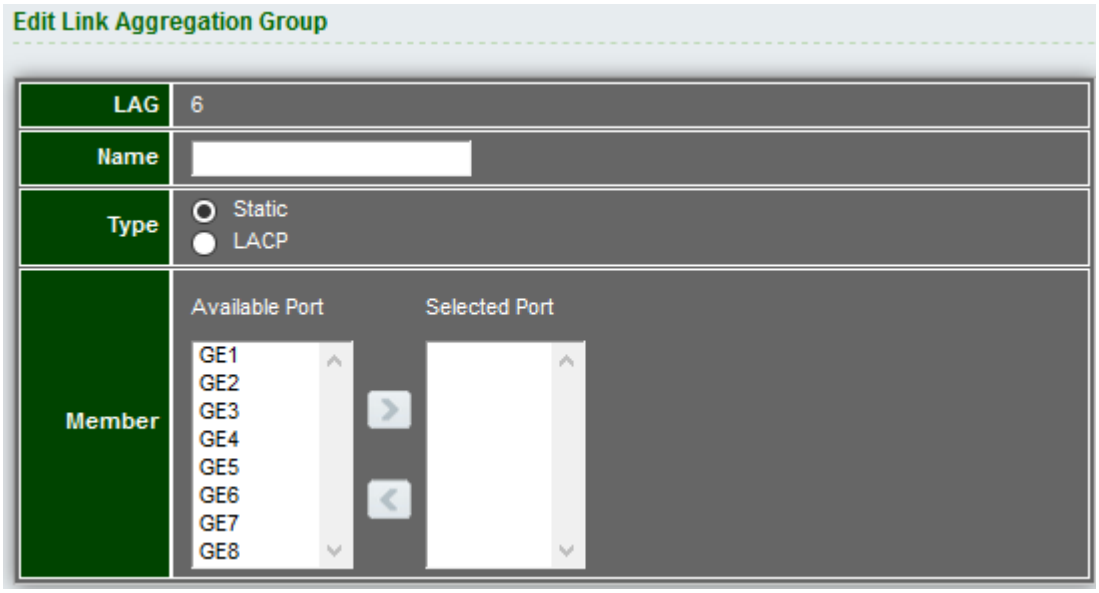
## 5.2 Link Aggregation

### 5.2.1 Group

Administrator can set 8 Link Aggregation Group(LAG)




- **Load Balance Alogorithm:** Administrator can choose Load Balance Alogorithm by MAC or IP Address.

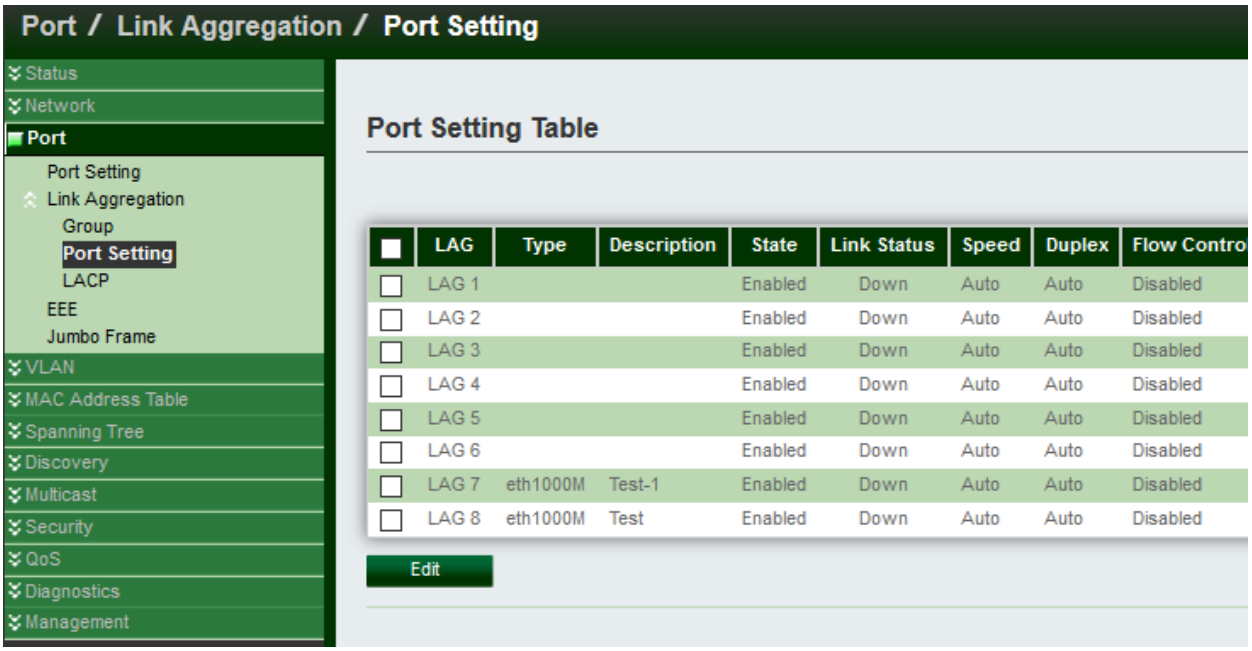


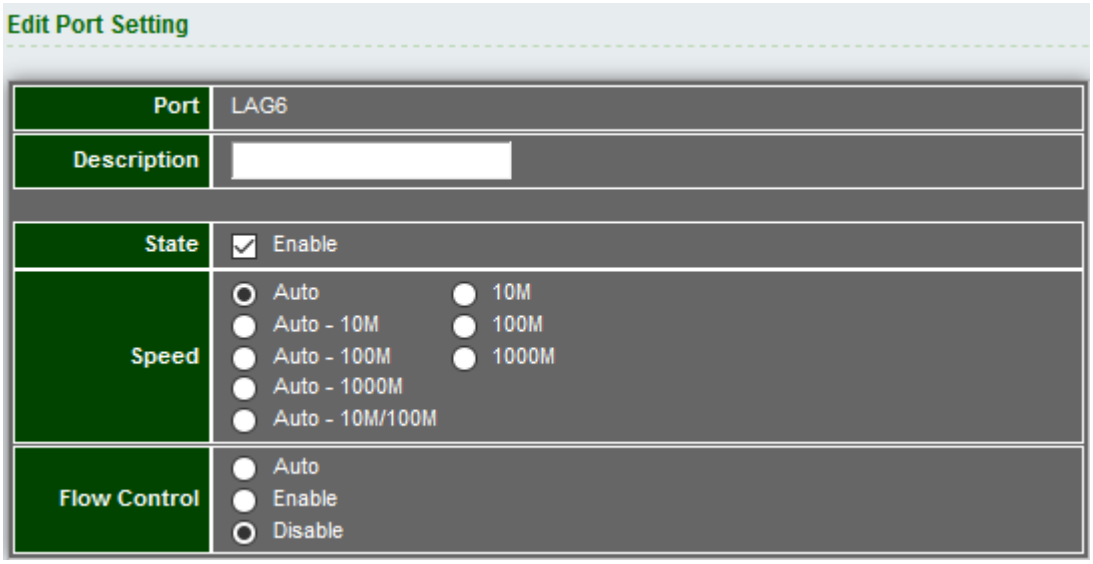

- **LAG:** Display LAG number.
- **Name:** Administrator can set the application name.

- **Type:** Administrator can choose Static or LACP type. 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.
  If both sides of the switch are set LACP mode then both sides of the port will ask to check whether to join the LAG group, if yes then use LACP connection, if no then skip LACP check.
- **Member:** Administrator can choose ports for member.

### 5.2.2 Port Setting

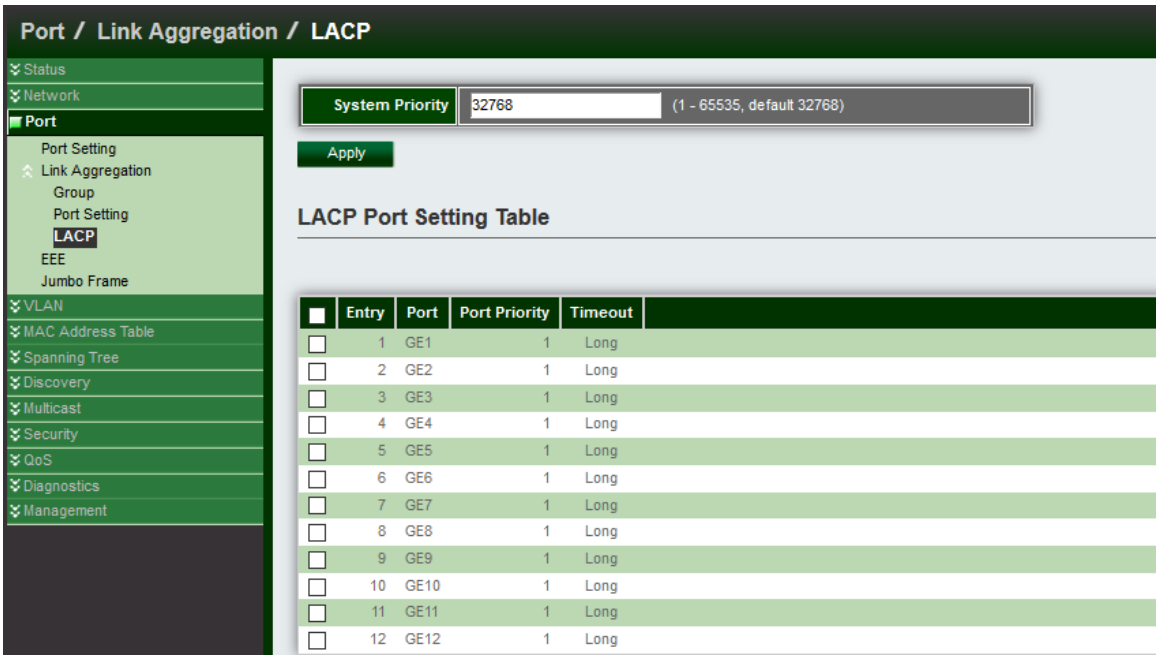
Administrator can set speed and flow control for Link Aggregation Group(LAG).



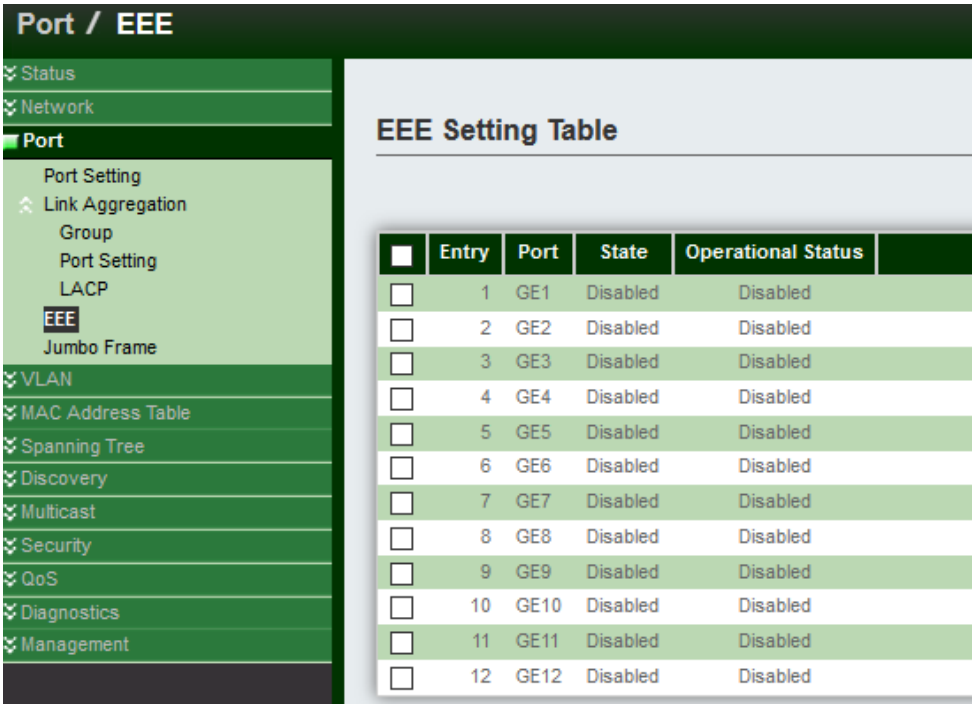
### 5.2.3 LACP

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.



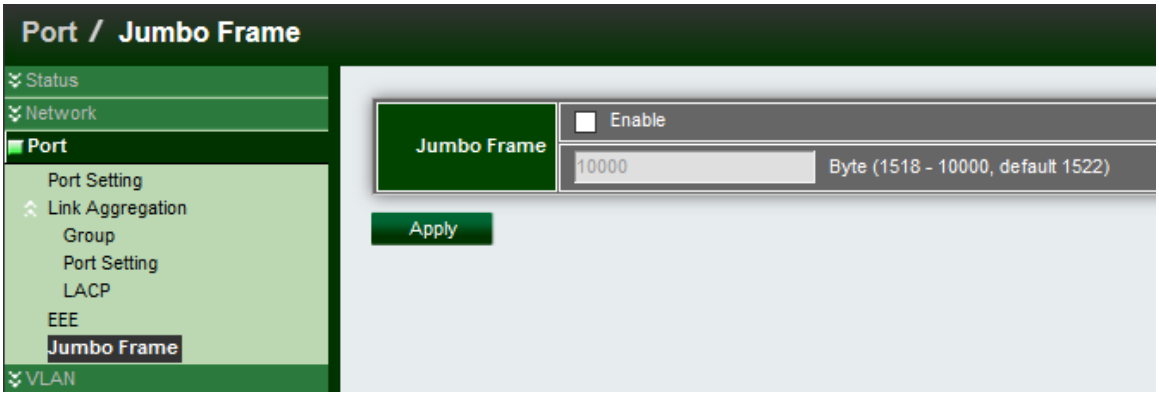

## 5.3 EEE

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



## 5.4 Jumbo Frame

Administrator can set Jumbo Frame for switch.

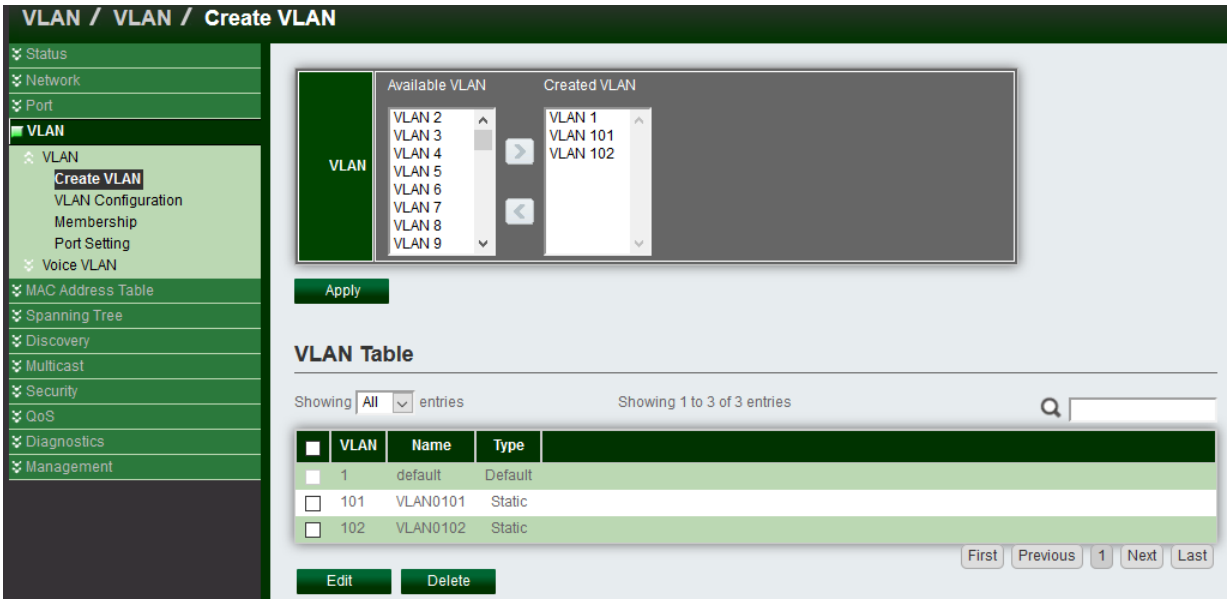



# 6. VLAN

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

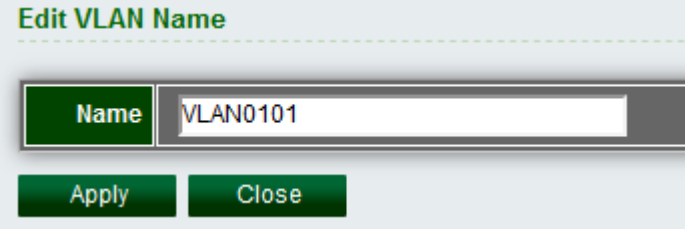
## 6.1 Create VLAN

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.



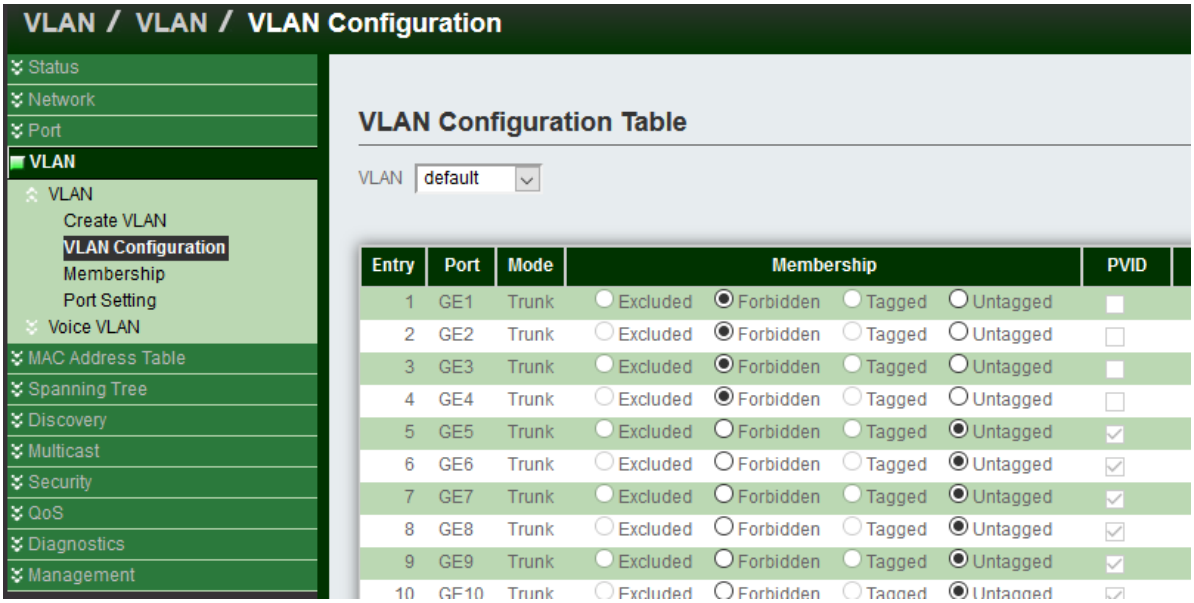

- **VLAN:** Administrator can select VLANs number go to Created VLAN table and click “Apply” button then complete the create VLANs, after complete will display VLANs list in below table.

- **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.




## 6.2 VLAN Configuration Table

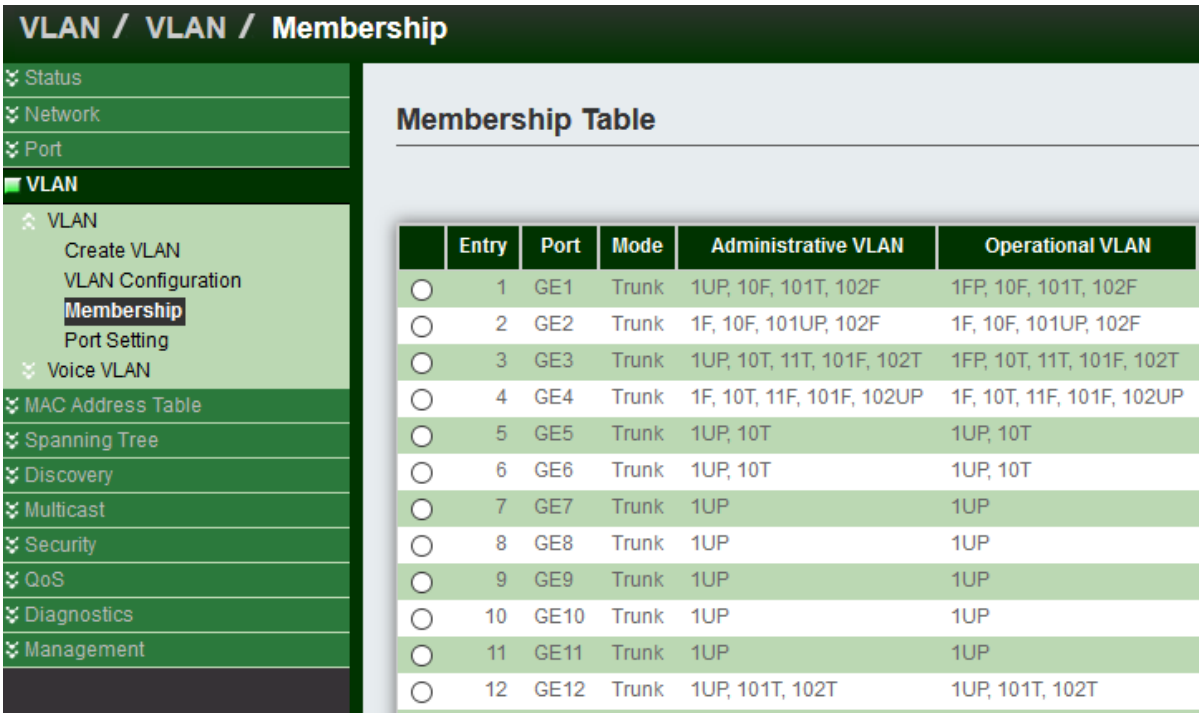
Administrator can choose set Excluded / Forbidden / Tagged / Untagged function in membership table of the Port and LAG.




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

## 6.3 Membership Table

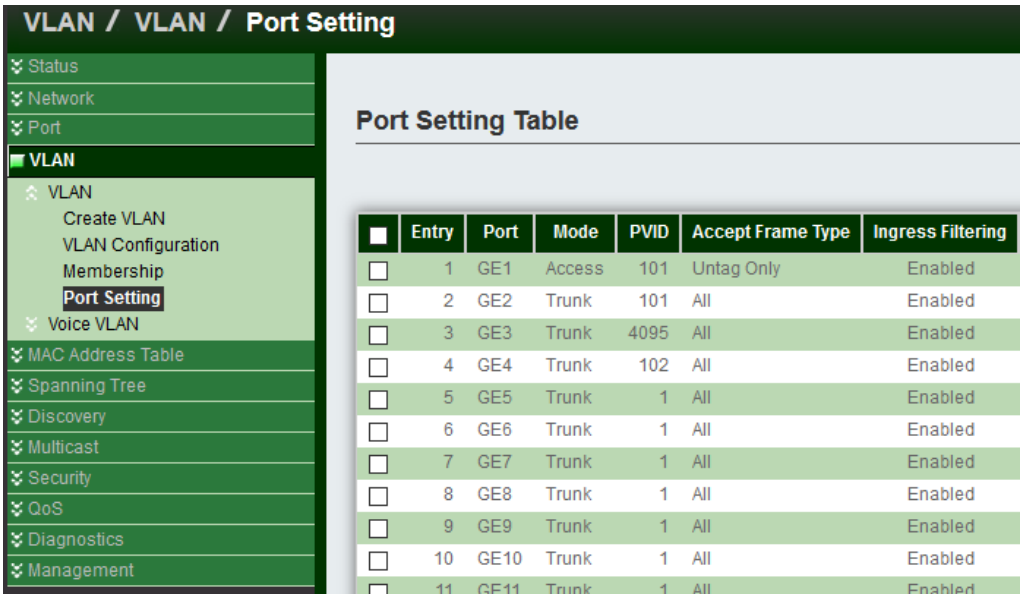
Display all port setting information. Administrator can checkbox and click "**Edit**" button to modify VLAN type. *(Note: Number=VLAN number, F=Forbidden, T=Tagged, U=Untagged, P=PVID)*



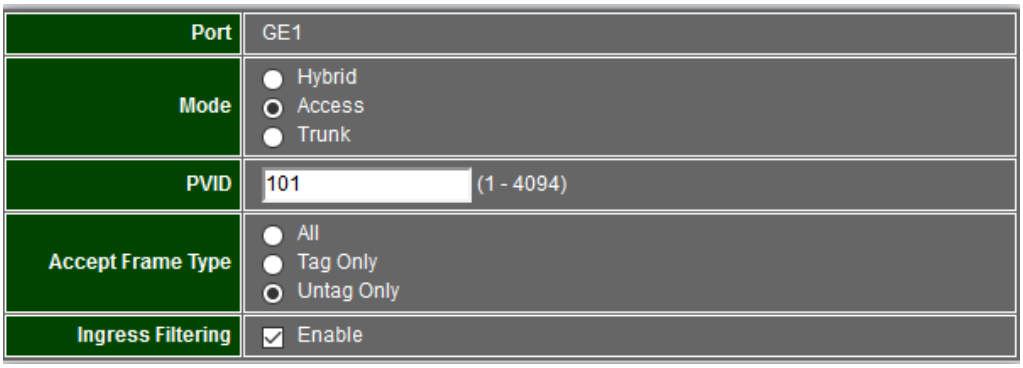

| | Entry | Port | Mode | Administrative VLAN | Operational VLAN |
|---|---|---|---|---|---|
| ○ | 1 | GE1 | Trunk | 1UP, 10F, 101T, 102F | 1FP, 10F, 101T, 102F |
| ○ | 2 | GE2 | Trunk | 1F, 10F, 101UP, 102F | 1F, 10F, 101UP, 102F |
| ○ | 3 | GE3 | Trunk | 1UP, 10T, 11T, 101F, 102T | 1FP, 10T, 11T, 101F, 102T |
| ○ | 4 | GE4 | Trunk | 1F, 10T, 11F, 101F, 102UP | 1F, 10T, 11F, 101F, 102UP |
| ○ | 5 | GE5 | Trunk | 1UP, 10T | 1UP, 10T |
| ○ | 6 | GE6 | Trunk | 1UP, 10T | 1UP, 10T |
| ○ | 7 | GE7 | Trunk | 1UP | 1UP |
| ○ | 8 | GE8 | Trunk | 1UP | 1UP |
| ○ | 9 | GE9 | Trunk | 1UP | 1UP |
| ○ | 10 | GE10 | Trunk | 1UP | 1UP |
| ○ | 11 | GE11 | Trunk | 1UP | 1UP |
| ○ | 12 | GE12 | Trunk | 1UP, 101T, 102T | 1UP, 101T, 102T |

## 6.4 Port Setting

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




| ☐ | Entry | Port | Mode | PVID | Accept Frame Type | Ingress Filtering |
|---|---|---|---|---|---|---|
| ☐ | 1 | GE1 | Access | 101 | Untag Only | Enabled |
| ☐ | 2 | GE2 | Trunk | 101 | All | Enabled |
| ☐ | 3 | GE3 | Trunk | 4095 | All | Enabled |
| ☐ | 4 | GE4 | Trunk | 102 | All | Enabled |
| ☐ | 5 | GE5 | Trunk | 1 | All | Enabled |
| ☐ | 6 | GE6 | Trunk | 1 | All | Enabled |
| ☐ | 7 | GE7 | Trunk | 1 | All | Enabled |
| ☐ | 8 | GE8 | Trunk | 1 | All | Enabled |
| ☐ | 9 | GE9 | Trunk | 1 | All | Enabled |
| ☐ | 10 | GE10 | Trunk | 1 | All | Enabled |
| ☐ | 11 | GE11 | Trunk | 1 | All | Enabled |

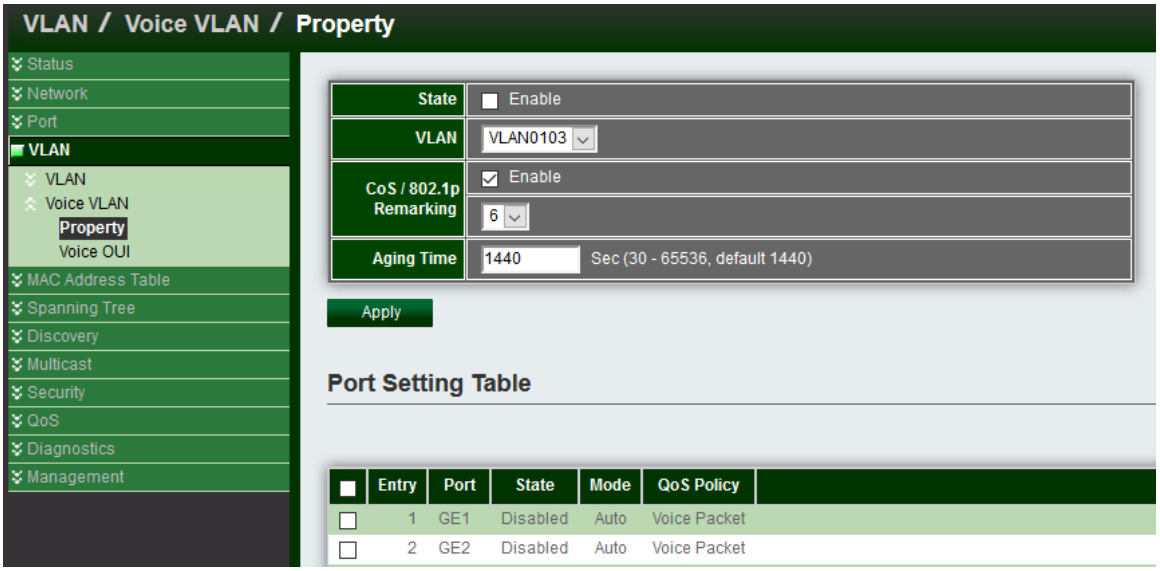



- **Hybrid**: Suitable for the inclusion of not VLANs and VLANs in the network environment.
- **Access**: Suitable for the Switch and device connection in VLAN network environment.
- **Trunk**: Suitable Switch and Switch connection in VLAN network environment.

## 6.5 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.

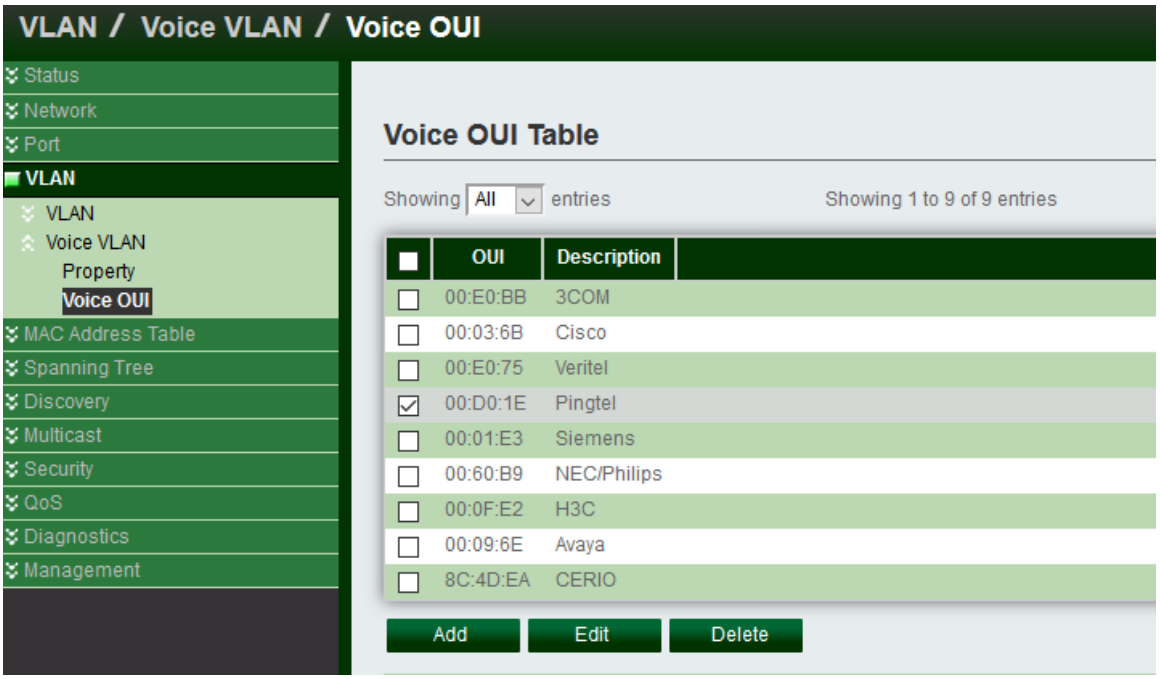
### 6.5.1 Property




- **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.
- **Aging Time:** Administrator can set aging time for this rule.

### 6.5.2 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.

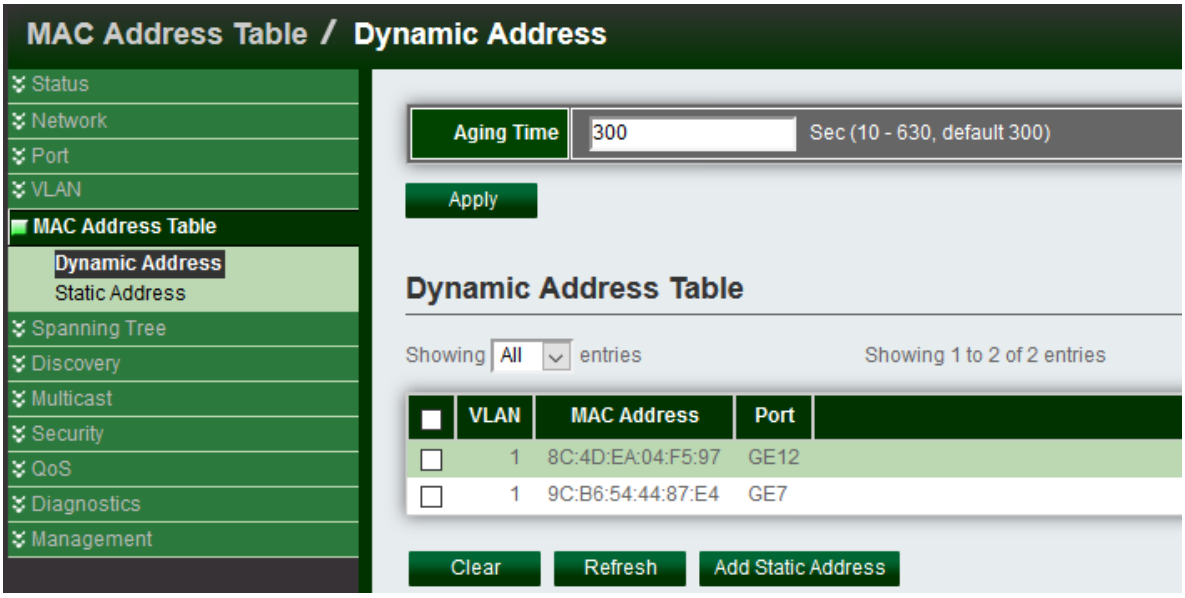
Click “**Edit**” button can modify OUI data.

Click “**Delete**” button can delete OUI data.

# 7. MAC Address Table

## 7.1 Dynamic Address

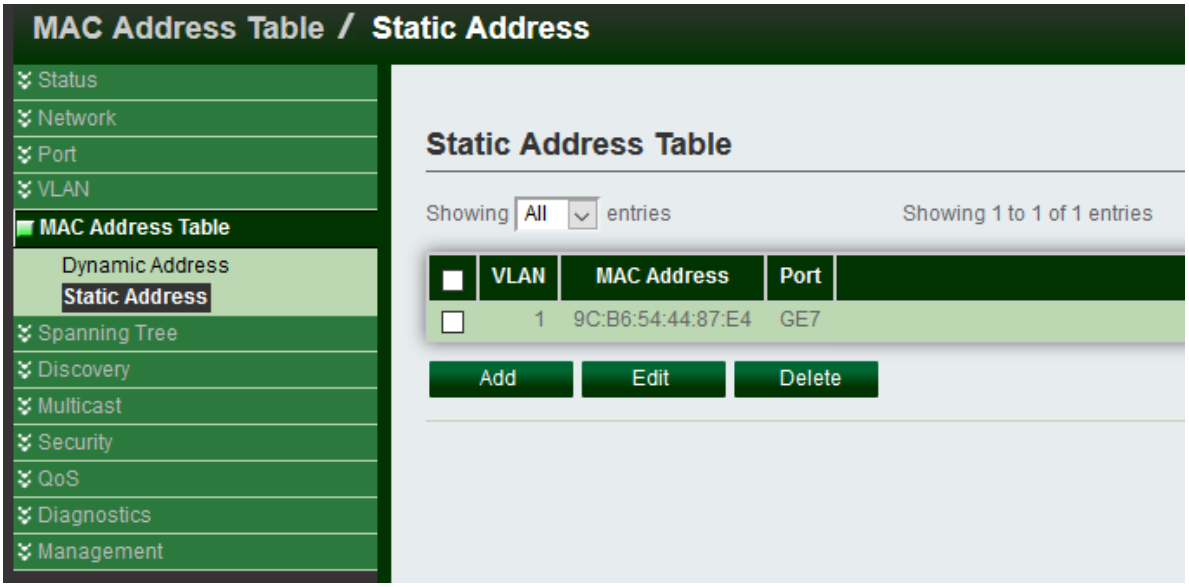
This page can display MAC address for connected device. Administrator can set aging time for connected port.




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

## 7.2 Static Address

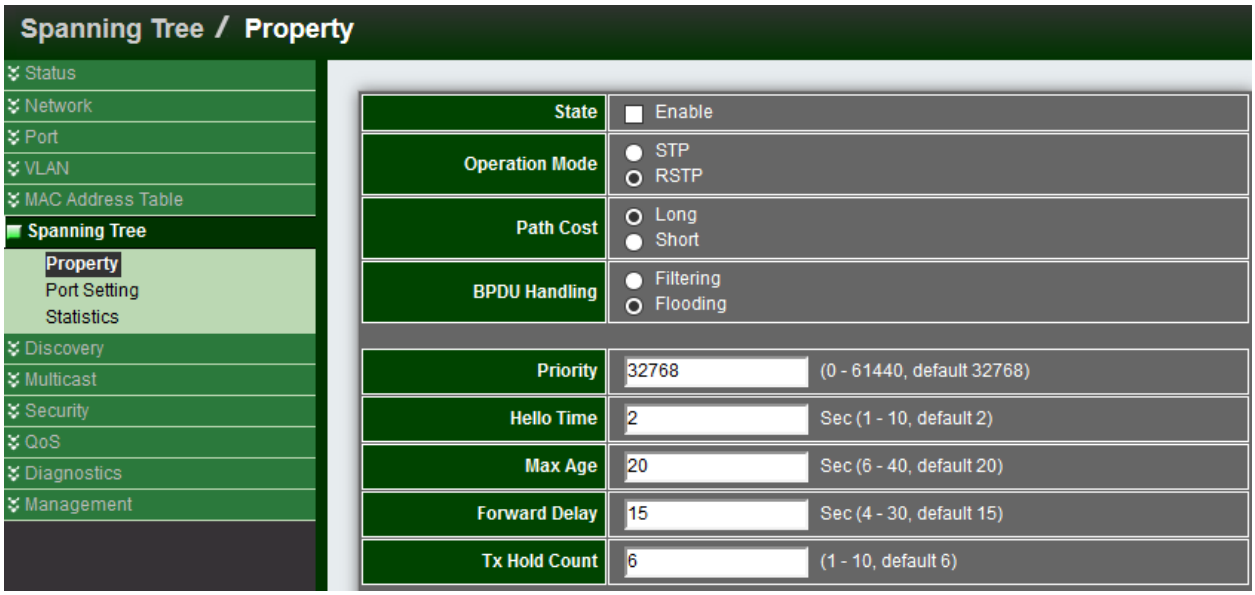
If administrator fixed an MAC address in the port then device MAC address will bind in the port, if device connection other port will can't working only connection bind port.



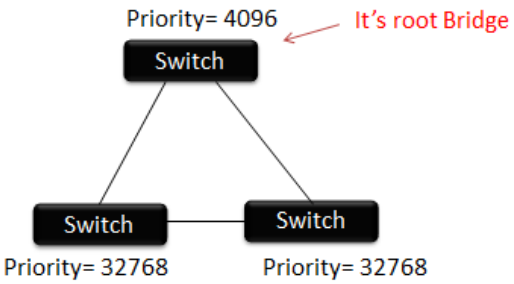
# 8. Spanning Tree

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

## 8.1 Property

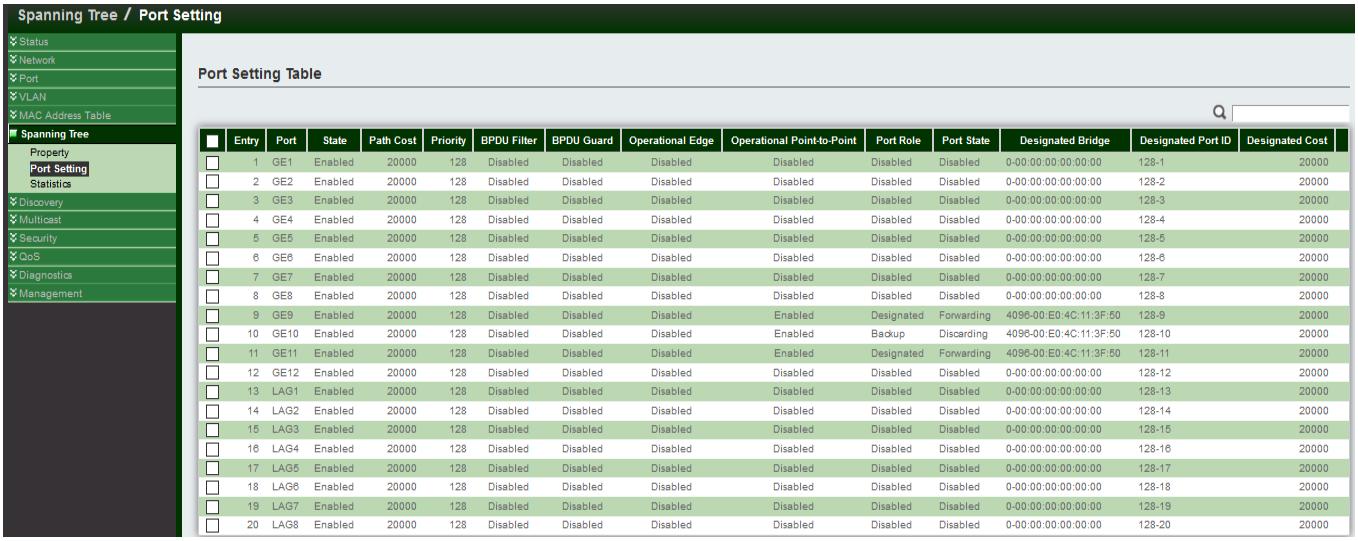



- **State:** Administrator can choose Enable or Disable this function.
- **Operation Mode:** Administrator can choose use STP or RSTP.
- **Path Cost:** Administrator can choose STP judgment use Path cost for Long or Short.
- **BPDU Handling:** When the Switch receives the BPDU frame, Administrator can 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.

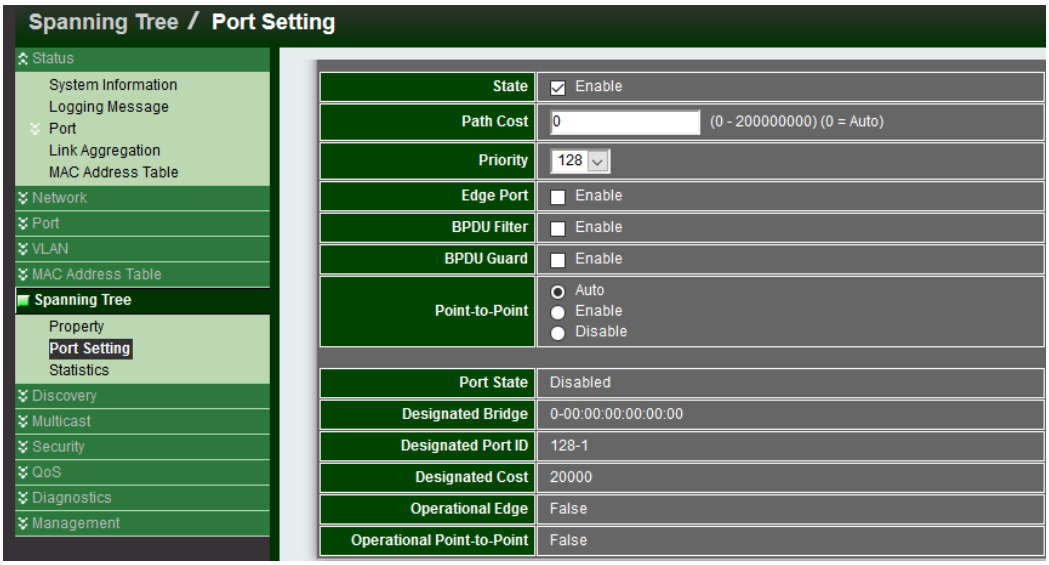


- **Hello Time:** The hello time is the time between each bridge protocol data unit (BPDU) that is sent on a port. This time is equal to 2 seconds (sec) by default, but you can tune the time to be between 1 and 10 sec.
- **Max. Age / Forward delay :** 2*(Forward Delay-1) >= **Max Age** >= 2*(Hello Time+1)
- **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.

## 8.2 Port Setting

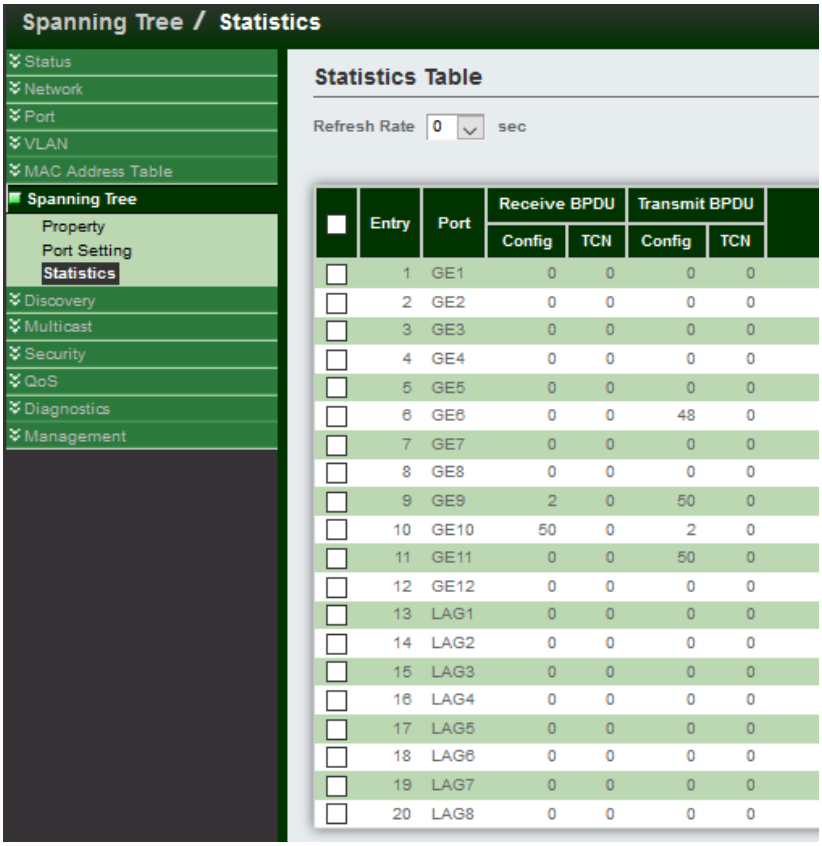



| Entry | Port | State | Path Cost | Priority | BPDU Filter | BPDU Guard | Operational Edge | Operational Point-to-Point | Port Role | Port State | Designated Bridge | Designated Port ID | Designated Cost |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | GE1 | Enabled | 20000 | 128 | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | 0-00:00:00:00:00:00 | 128-1 | 20000 |
| 2 | GE2 | Enabled | 20000 | 128 | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | 0-00:00:00:00:00:00 | 128-2 | 20000 |
| 3 | GE3 | Enabled | 20000 | 128 | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | 0-00:00:00:00:00:00 | 128-3 | 20000 |
| 4 | GE4 | Enabled | 20000 | 128 | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | 0-00:00:00:00:00:00 | 128-4 | 20000 |
| 5 | GE5 | Enabled | 20000 | 128 | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | 0-00:00:00:00:00:00 | 128-5 | 20000 |
| 6 | GE6 | Enabled | 20000 | 128 | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | 0-00:00:00:00:00:00 | 128-6 | 20000 |
| 7 | GE7 | Enabled | 20000 | 128 | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | 0-00:00:00:00:00:00 | 128-7 | 20000 |
| 8 | GE8 | Enabled | 20000 | 128 | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | 0-00:00:00:00:00:00 | 128-8 | 20000 |
| 9 | GE9 | Enabled | 20000 | 128 | Disabled | Disabled | Disabled | Enabled | Designated | Forwarding | 4096-00:E0:4C:11:3F:50 | 128-9 | 20000 |
| 10 | GE10 | Enabled | 20000 | 128 | Disabled | Disabled | Disabled | Enabled | Backup | Discarding | 4096-00:E0:4C:11:3F:50 | 128-10 | 20000 |
| 11 | GE11 | Enabled | 20000 | 128 | Disabled | Disabled | Disabled | Enabled | Designated | Forwarding | 4096-00:E0:4C:11:3F:50 | 128-11 | 20000 |
| 12 | GE12 | Enabled | 20000 | 128 | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | 0-00:00:00:00:00:00 | 128-12 | 20000 |
| 13 | LAG1 | Enabled | 20000 | 128 | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | 0-00:00:00:00:00:00 | 128-13 | 20000 |
| 14 | LAG2 | Enabled | 20000 | 128 | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | 0-00:00:00:00:00:00 | 128-14 | 20000 |
| 15 | LAG3 | Enabled | 20000 | 128 | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | 0-00:00:00:00:00:00 | 128-15 | 20000 |
| 16 | LAG4 | Enabled | 20000 | 128 | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | 0-00:00:00:00:00:00 | 128-16 | 20000 |
| 17 | LAG5 | Enabled | 20000 | 128 | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | 0-00:00:00:00:00:00 | 128-17 | 20000 |
| 18 | LAG6 | Enabled | 20000 | 128 | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | 0-00:00:00:00:00:00 | 128-18 | 20000 |
| 19 | LAG7 | Enabled | 20000 | 128 | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | 0-00:00:00:00:00:00 | 128-19 | 20000 |
| 20 | LAG8 | Enabled | 20000 | 128 | Disabled | Disabled | Disabled | Disabled | Disabled | Disabled | 0-00:00:00:00:00:00 | 128-20 | 20000 |




- **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.

## 8.3 Statistics Table



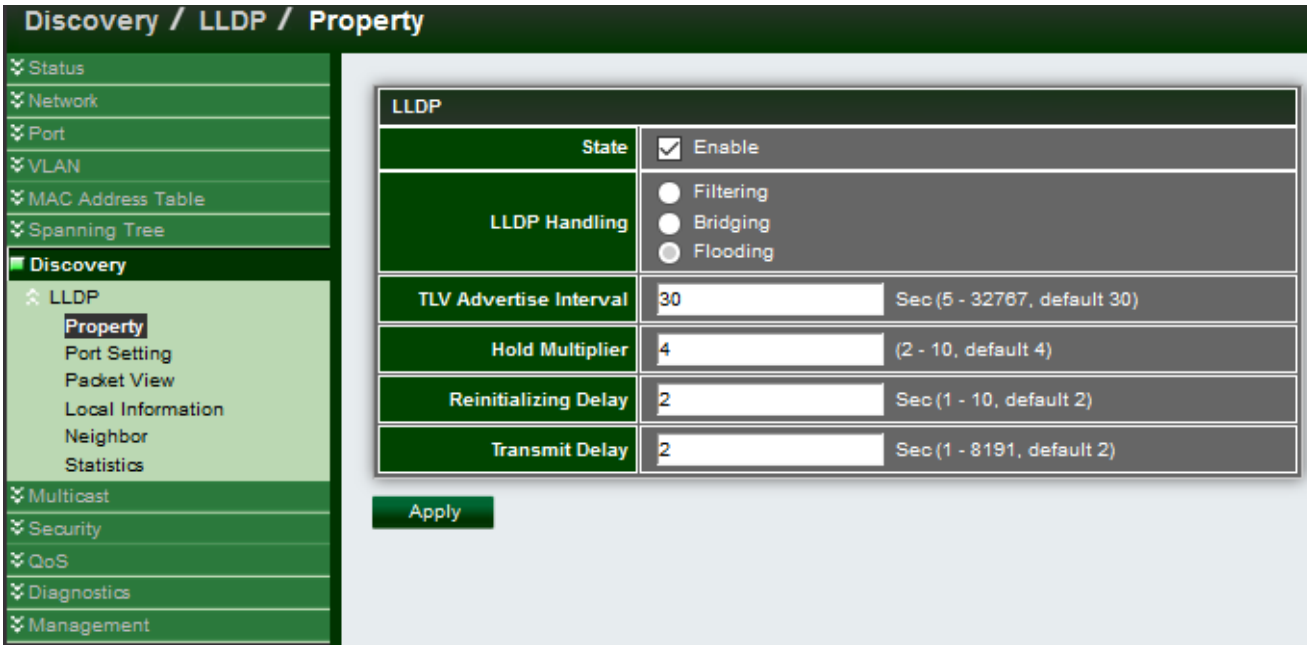

If administrator set “8.1 Property Operation” is STP mode then will display Receive / Transmit BPDU status in the page.

# 9. 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.

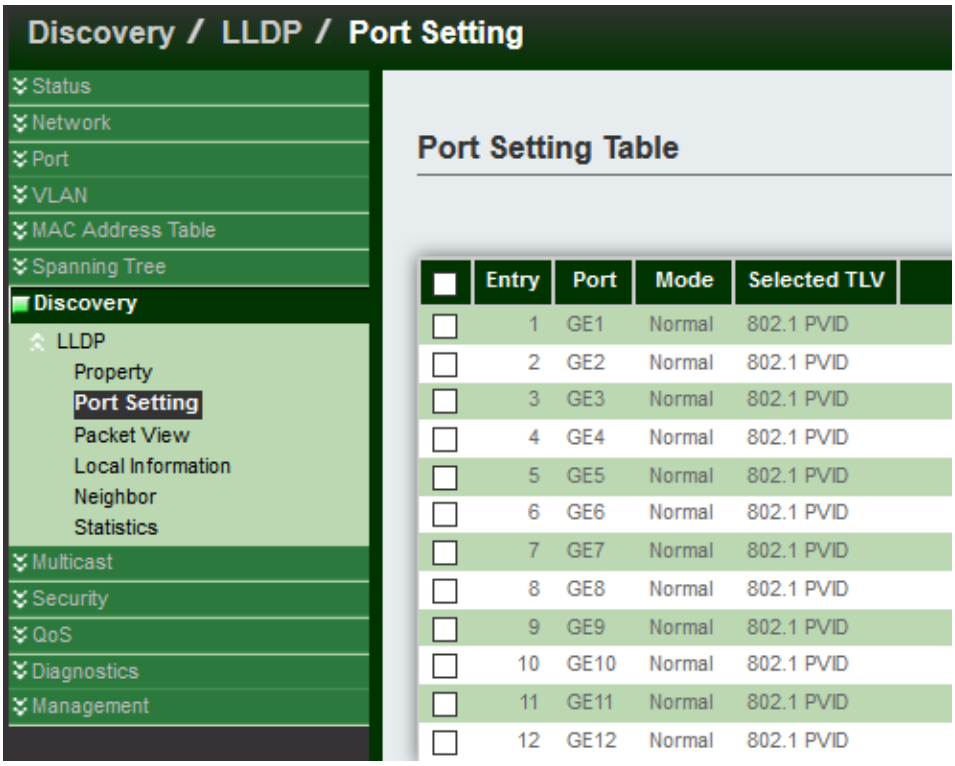
## 9.1 Property

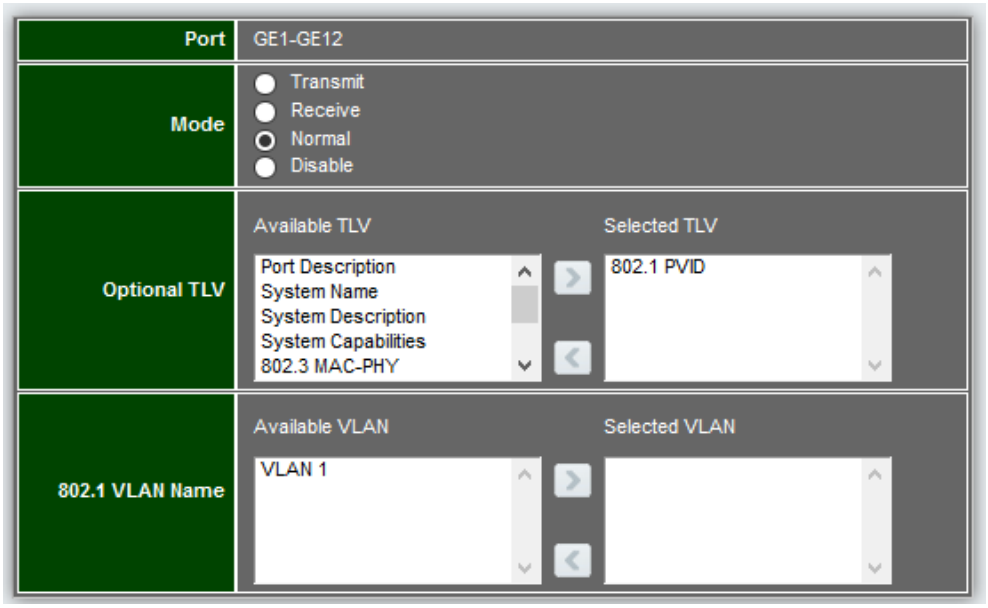



- **State:** Administrator can choose Enable or disable this LLDP function.
- **LLDP Handing:** If cancel checkbox then administrator can choose Filtering / Bridging / Flooding for LLDP handing.
- **TLV Advertise Interval:** Set LLDPDU Send Interval period (range 5-32760, default is 30)
- **Hold Multiplier:**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

## 9.2 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.

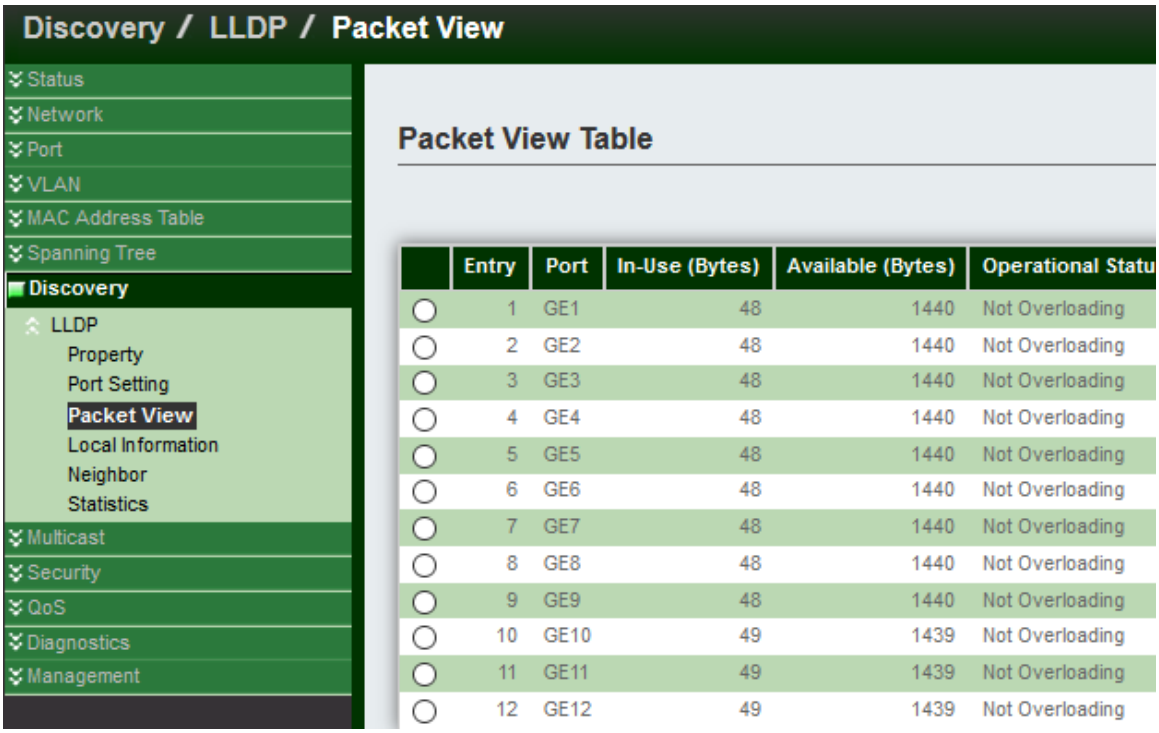



- **Mode:** Administrator can choose Transmit(TX) / Receive(RX) or Normal(TX+RX) and Disable, if choose disable will don't send and receive LLDPDU.
- Optional TLV: Administrator can be configuration information into different TLV, encapsulates LLDPDU and issued to the neighbor device.
- 802.1 VLAN Name: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

## 9.3 Packet View Table

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.




## 9.4 Local Information

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.

| | |
|---|---|
| Chassis ID Subtype | MAC address |
| Chassis ID | 8C:4D:EA:11:22:33 |
| System Name | Switch |
| System Description | 8 Port 10/100/1000M Gigabit Web Managed Switch with 4 Combo Gigabit Ports |
| Supported Capabilities | Bridge |
| Enabled Capabilities | Bridge |
| Port ID | GE2 |
| Port ID Subtype | Local |
| Port Description | |

| Management Address Table | | | | |
|---|---|---|---|---|
| Address Subtype | Address | Interface Subtype | Interface Number | |
| IPv4 | 192.168.2.200 | System Port Number | 0 | |
| IPv6 | fe80::2e0:4cff:fe11:3f50 | System Port Number | 0 | |

| MAC/PHY Detail | |
|---|---|
| Auto-Negotiation Supported | True |
| Auto-Negotiation Enabled | True |
| Auto-Negotiation Advertised Capabilities | 1000baseTFD , 100baseTXFD , 100baseTX , 10baseTFD , 10baseT |
| Operational MAU Type | dot3MauType10GigBaseLX4 |

| 802.3 Detail | |
|---|---|
| 802.3 Maximum Frame Size | 1522 |

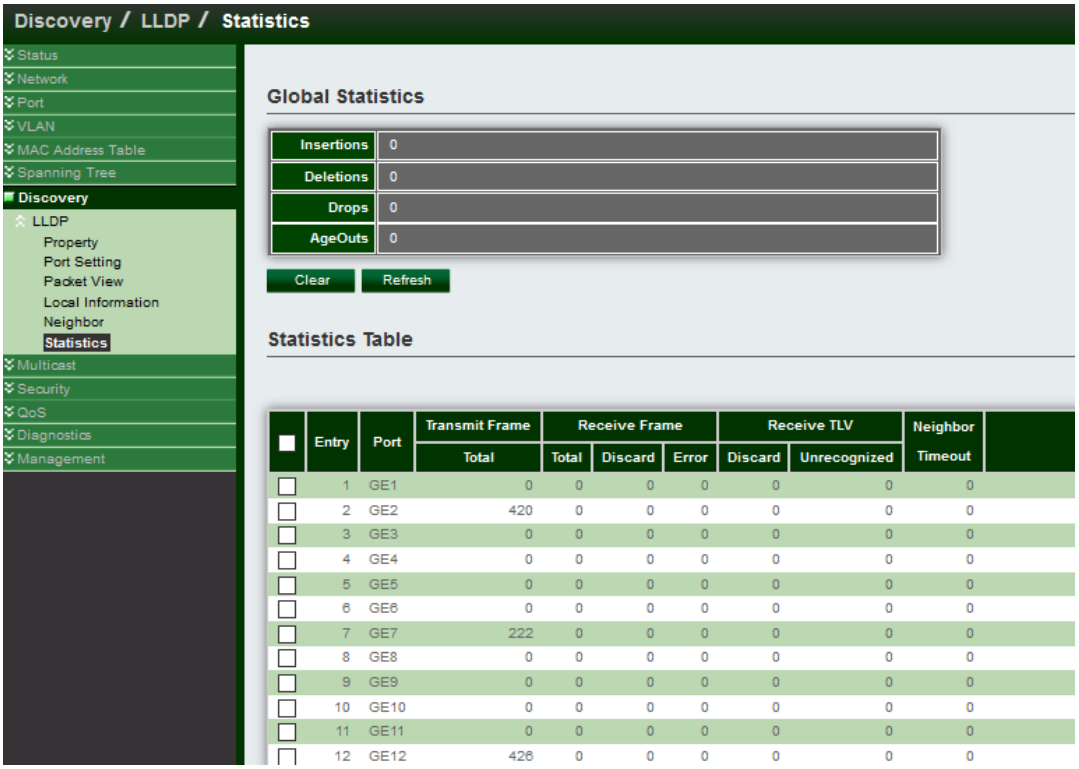
| 802.3 Link Aggregation | |
|---|---|
| Aggregation Capability | Capable |
| Aggregation Status | Not aggregated |
| Aggregation Port ID | 0 |

## 9.5 Neighbor

If use 2 switch and open LLDP function, will identify device for the LLDP neighbors and the neighbors of the summary attribute will show in Neighbor Table.


## 9.6 Statistics

This page can display Transmit / Receive Frame / Receive TLV and Neighbor timeout information's.



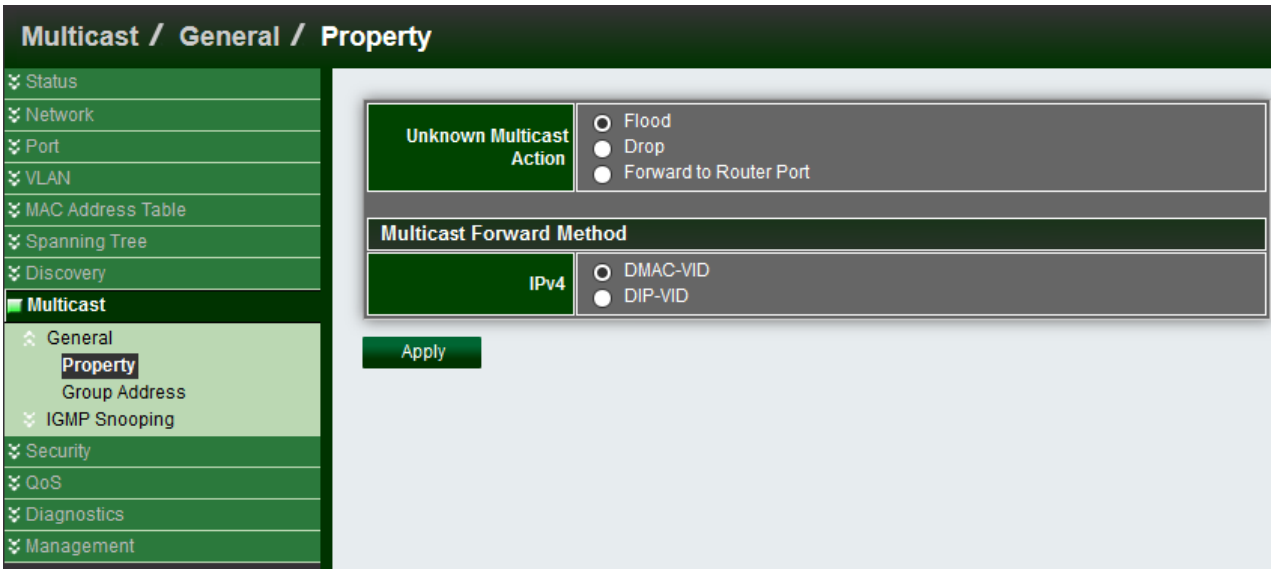
# 10. Multicast

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

## 10.1 General

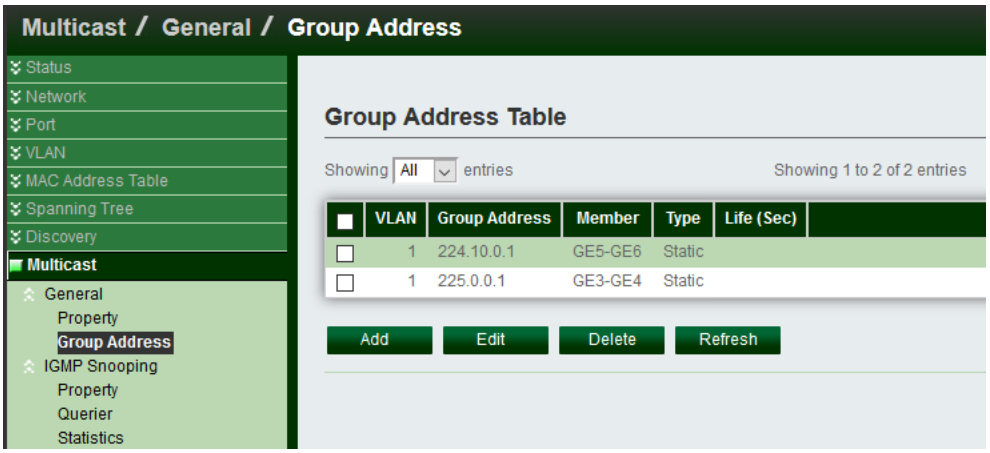
### 10.1.1 Property

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.




### 10.1.2 Group Address

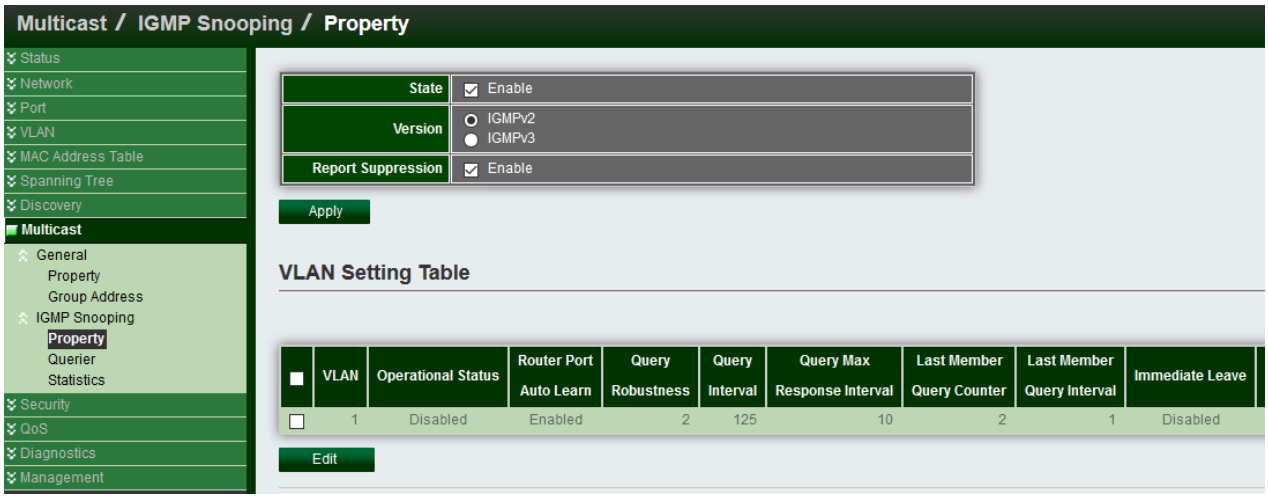
The multicast address range is 224.0.0.0 to 239.255.255.255 and forms the Class D range which is made up of the high order bits 1110 followed by the 28 bit multicast group ID. There is no subletting with these Class D addresses. A multicast group can have a permanently-assigned address or the group may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



## 10.2 IGMP snooping

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

### 10.2.1 Property

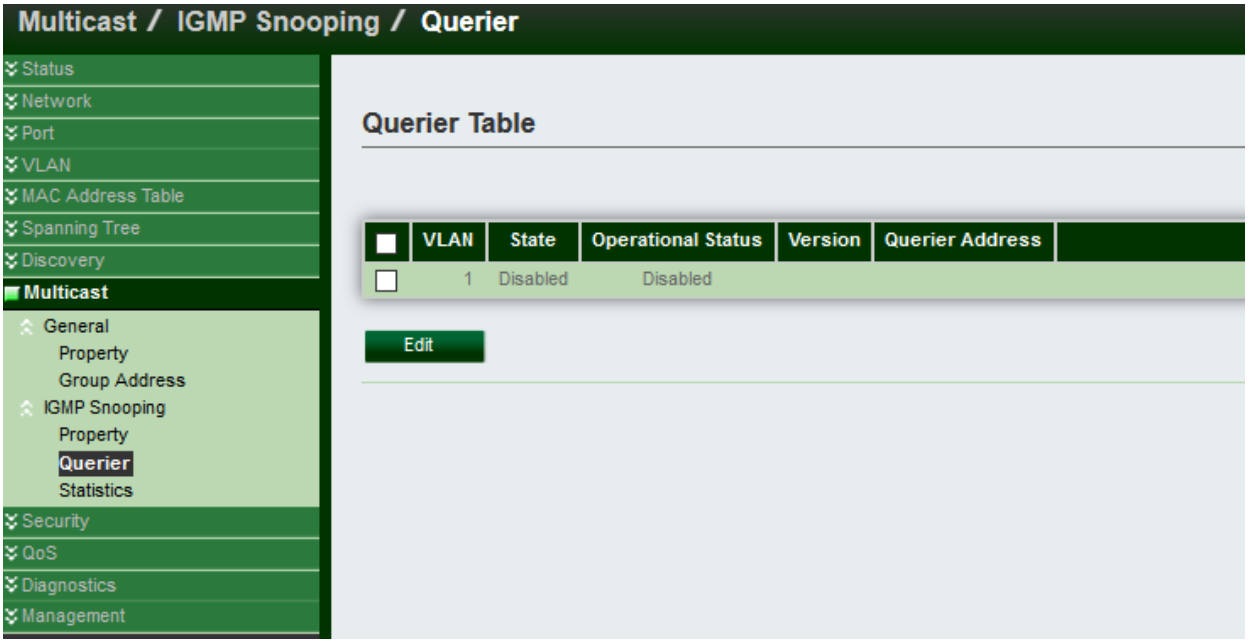



| | |
|---|---|
| VLAN | 1 |
| State | Enable |
| Router Port Auto Learn | Enable |
| Immediate leave | Enable |
| Query Robustness | 2 (1 - 7, default 2) |
| Query Interval | 125 Sec (30 - 18000, default 125) |
| Query Max Response Interval | 10 Sec (5 - 20, default 10) |
| Last Member Query Counter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

- **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.

### 10.2.2 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.



| | |
|---|---|
| VLAN | 1 |
| State | ☐ Enable |
| Version | ◉ IGMPv2<br>○ IGMPv3 |

### 10.2.3 Statistics

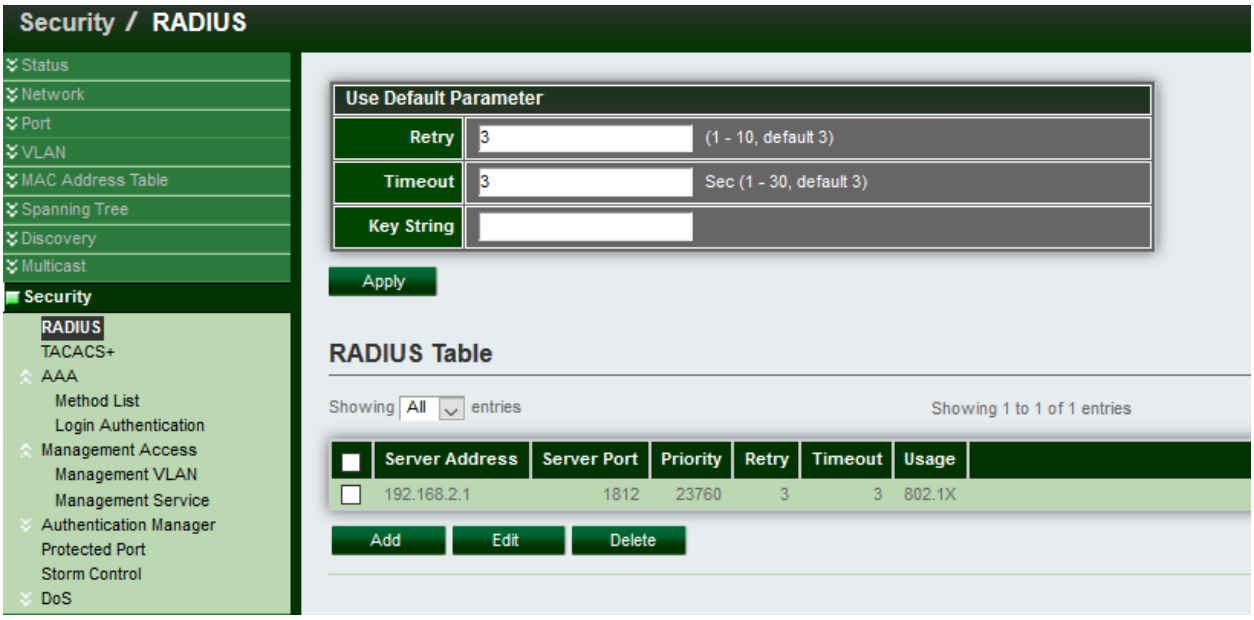
Display Receive / Transmit Packet information of IGMP snooping.

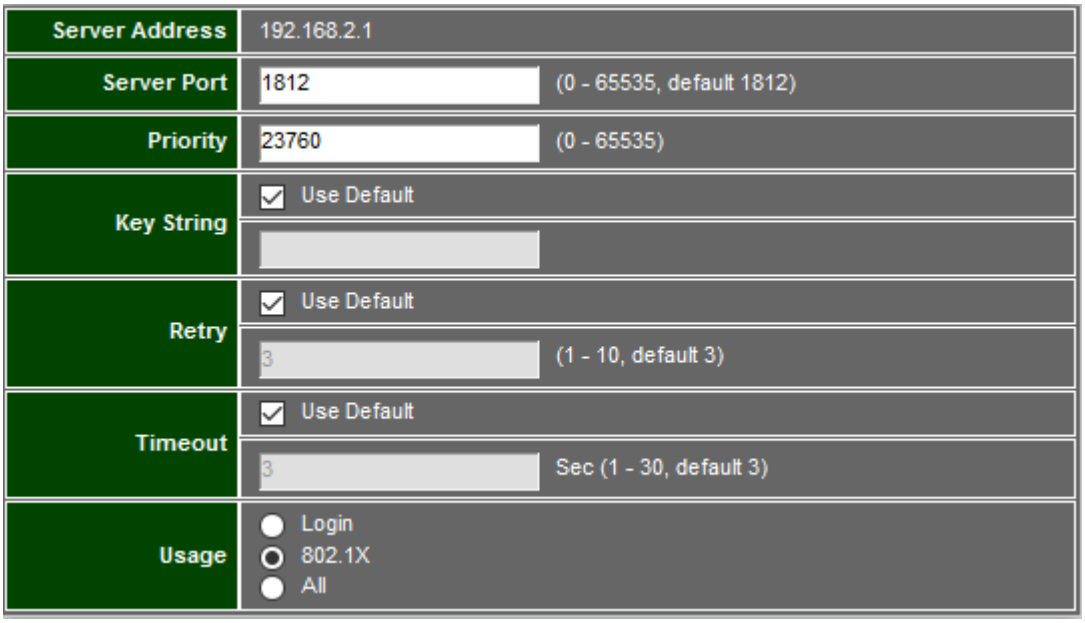
| Receive Packet | |
|---|---|
| Total | 17 |
| Valid | 2 |
| InValid | 15 |
| Other | 0 |
| Leave | 0 |
| Report | 0 |
| General Query | 0 |
| Special Group Query | 0 |
| Source-specific Group Query | 0 |
| **Transmit Packet** | |
| Leave | 0 |
| Report | 0 |
| General Query | 0 |
| Special Group Query | 0 |
| Source-specific Group Query | 0 |

# 11. Security

## 11.1 RADIUS

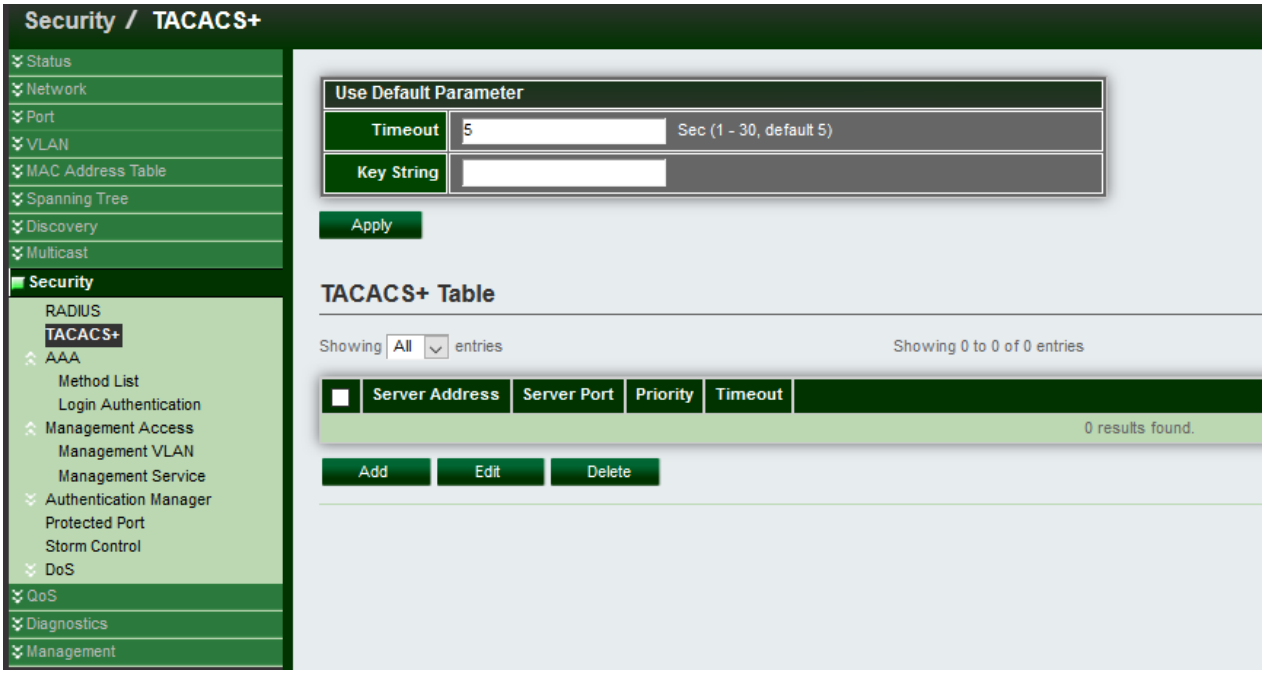
Administrator can be configuration RADIUS to connection RADIUS Server.



## 11.2 TACACS+

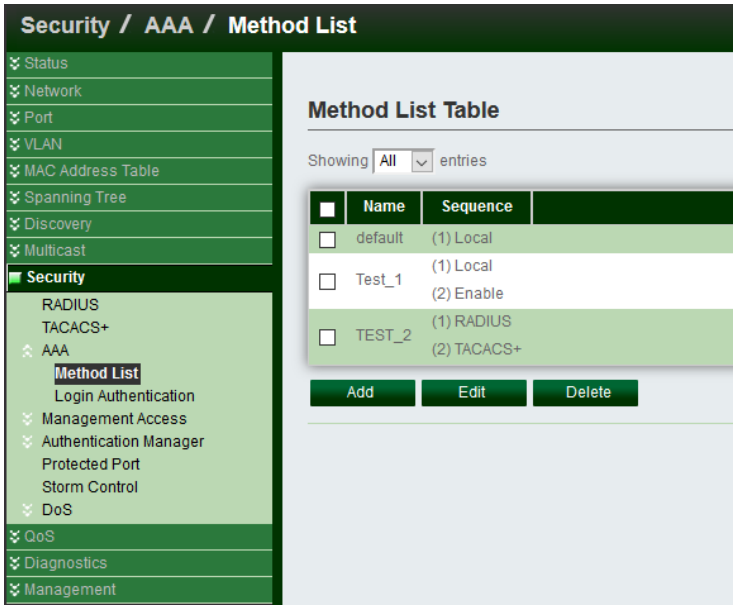
Administrator can be configuration TACACS+ to connection TACACS+ Server.

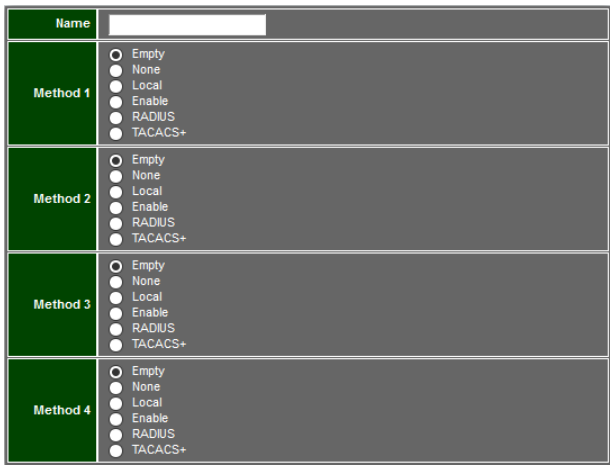



## 11.3 AAA

### 11.3.1 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+

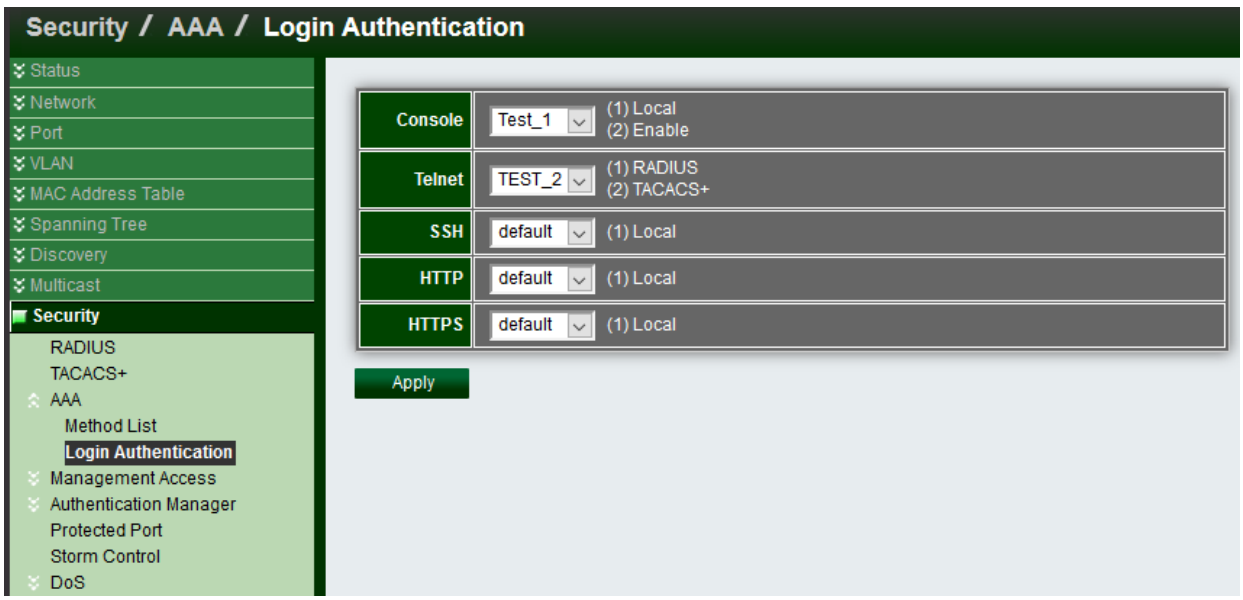





- **Empty:** Close authentication type of this method.
- **None**: Don't use authentication.
- **Local:** System login account use local system authentication in "menu -> management -> user Account".
- **Enable:**
- **RADIUS:** System login account use remote RADIUS server authentication.
- **TACACS+**: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

### 11.3.2 Login Authentication

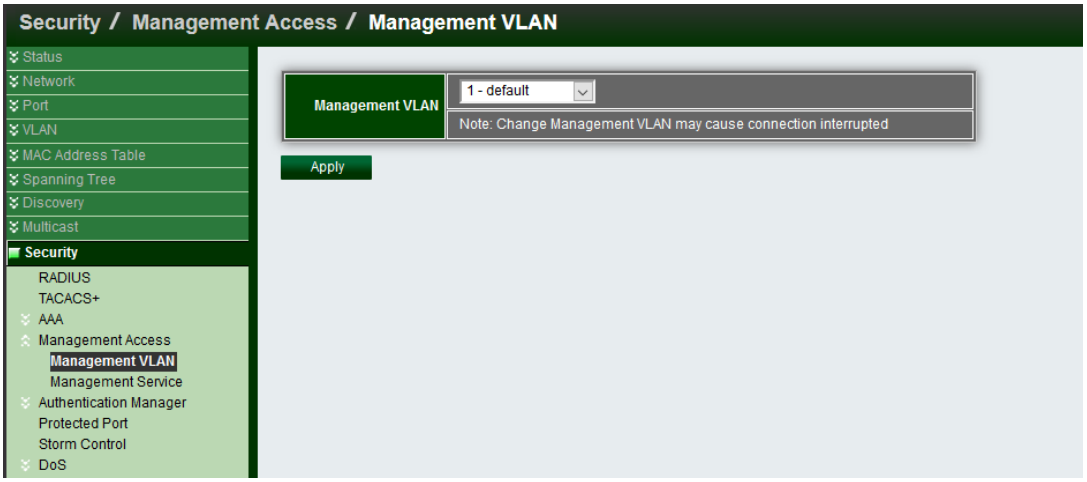
When administrator has created security groups in "AAA=>method" then administrator can select different security group in service port.



## 11.4 Management Access

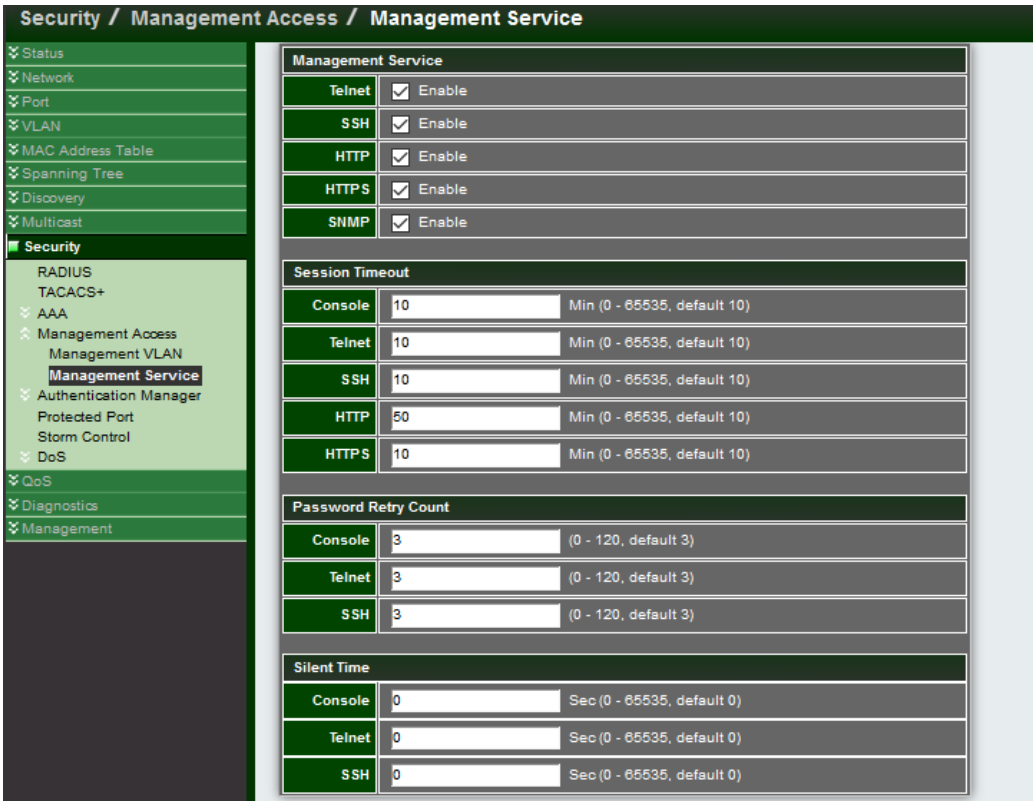
### 11.4.1 Management VLAN

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




### 11.4.2 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.

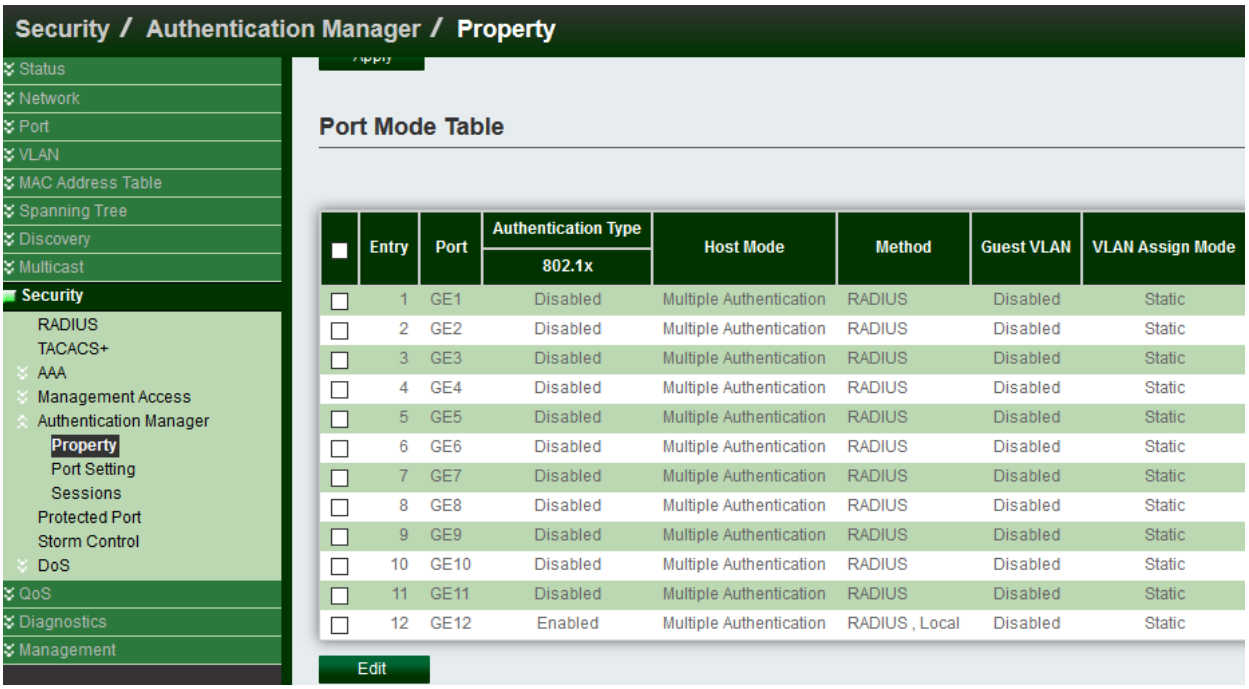


- **Session Timeout:** After login management page, in the set time if not session then system will auto timeout, administrator need re-login.
- **Password Retry Count:** If login error reaches the set value then login page will be kicked out, administrator need reopen the login page.
- **Silent Time:**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

## 11.5 Authentication Manager

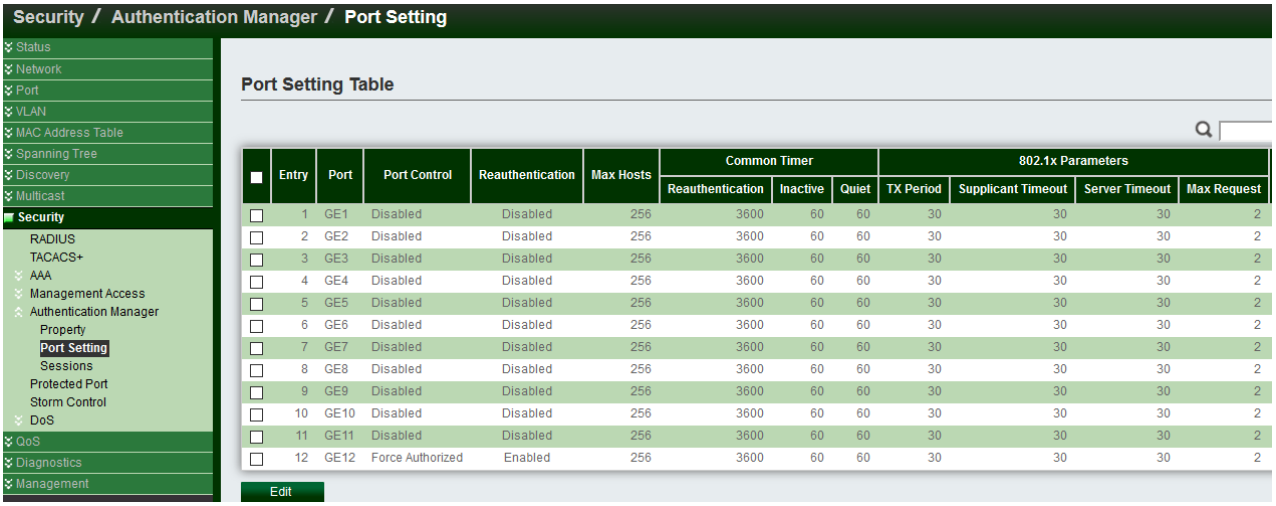
### 11.5.1 Property

Administrator can select use 802.1x authentication.

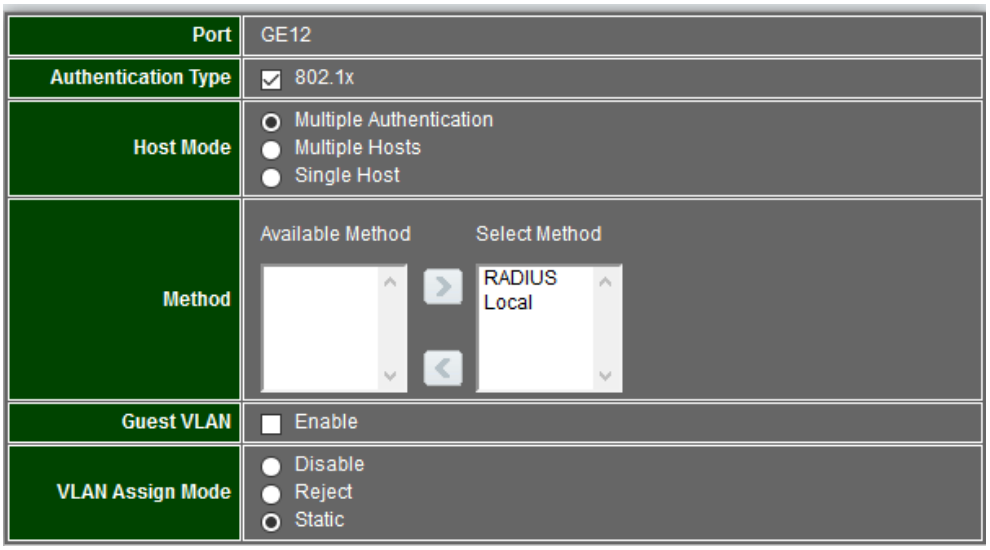


## 11.5.2 Port Setting

Administrator can set authentication method by Ports.



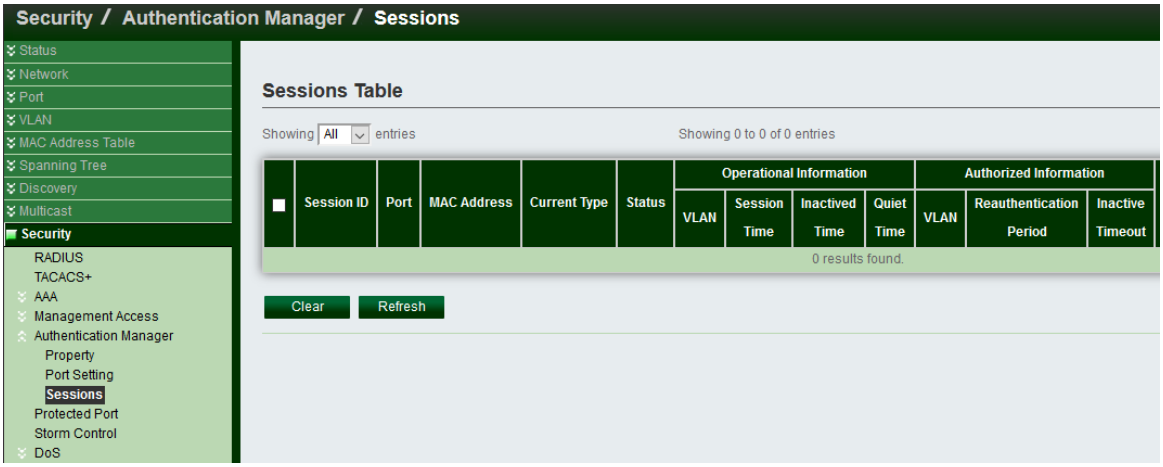

| Entry | Port | Port Control | Reauthentication | Max Hosts | Common Timer | | | 802.1x Parameters | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Reauthentication | Inactive | Quiet | TX Period | Supplicant Timeout | Server Timeout | Max Request |
| 1 | GE1 | Disabled | Disabled | 256 | 3600 | 60 | 60 | 30 | 30 | 30 | 2 |
| 2 | GE2 | Disabled | Disabled | 256 | 3600 | 60 | 60 | 30 | 30 | 30 | 2 |
| 3 | GE3 | Disabled | Disabled | 256 | 3600 | 60 | 60 | 30 | 30 | 30 | 2 |
| 4 | GE4 | Disabled | Disabled | 256 | 3600 | 60 | 60 | 30 | 30 | 30 | 2 |
| 5 | GE5 | Disabled | Disabled | 256 | 3600 | 60 | 60 | 30 | 30 | 30 | 2 |
| 6 | GE6 | Disabled | Disabled | 256 | 3600 | 60 | 60 | 30 | 30 | 30 | 2 |
| 7 | GE7 | Disabled | Disabled | 256 | 3600 | 60 | 60 | 30 | 30 | 30 | 2 |
| 8 | GE8 | Disabled | Disabled | 256 | 3600 | 60 | 60 | 30 | 30 | 30 | 2 |
| 9 | GE9 | Disabled | Disabled | 256 | 3600 | 60 | 60 | 30 | 30 | 30 | 2 |
| 10 | GE10 | Disabled | Disabled | 256 | 3600 | 60 | 60 | 30 | 30 | 30 | 2 |
| 11 | GE11 | Disabled | Disabled | 256 | 3600 | 60 | 60 | 30 | 30 | 30 | 2 |
| 12 | GE12 | Force Authorized | Enabled | 256 | 3600 | 60 | 60 | 30 | 30 | 30 | 2 |




- **Port**: Display selected port number.
- **Authentication Type**: Administrator can enable or disable authentication for 802.1 x protocol.
- **Host Mode:** Administrator has three mode can choose for Multiple Authentication / Multiple Hosts and Single Host.
- **Guest VLAN:** Administrator can enable or disable the Guest VLAN.
- **VLAN Assign Mode:** Administrator can select Reject or Static for VLAN Assign mode or disable the function.

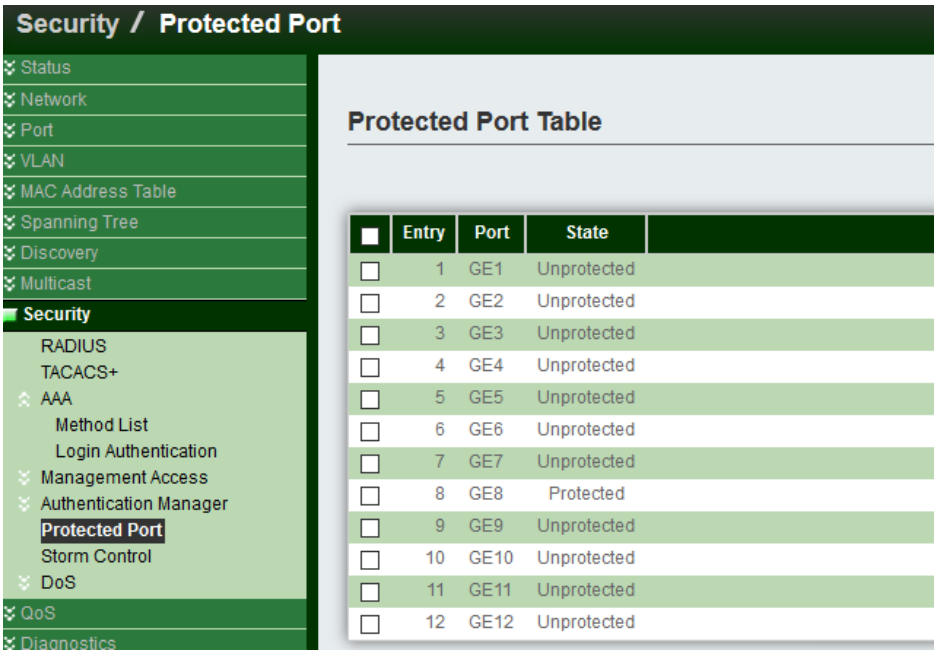
### 11.5.3 Sessions

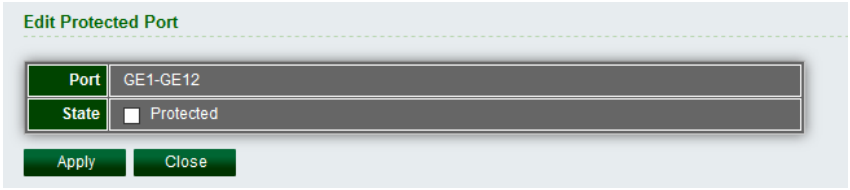
Display session information of authentication.




## 11.6 Protected Port

Administrator can select ports to protected

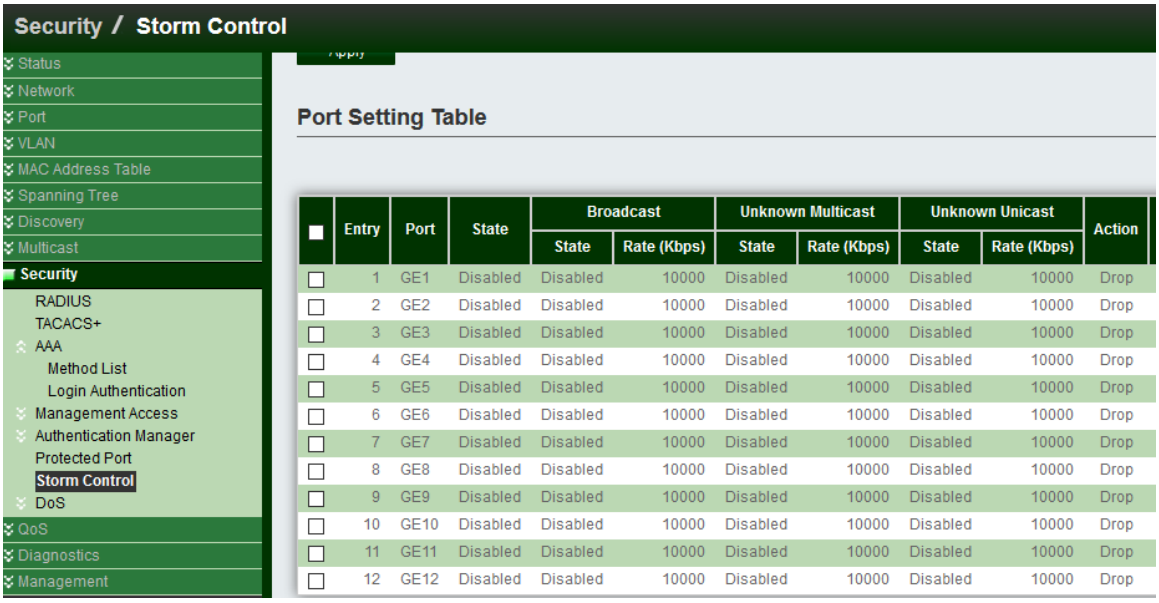


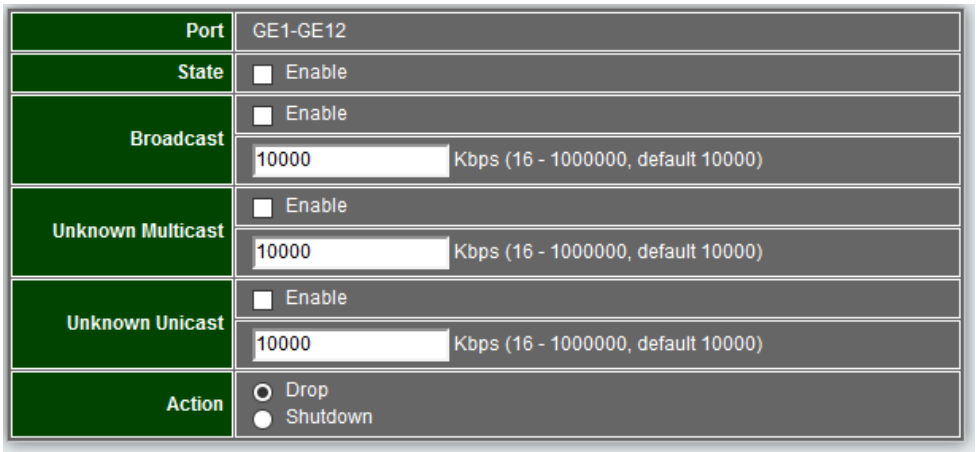




- **State**: Administrator can click checkbox to enable or disable of protected ports.

## 11.7 Storm Control

This function can prevent broadcast storms, administrator can choose ports to enable or disable of prevent storms. When choose enable, administrator can set safe value of broadcast / Multicast / Unicast, if over safety value in ports then system can according to action drop or shutdown this ports.



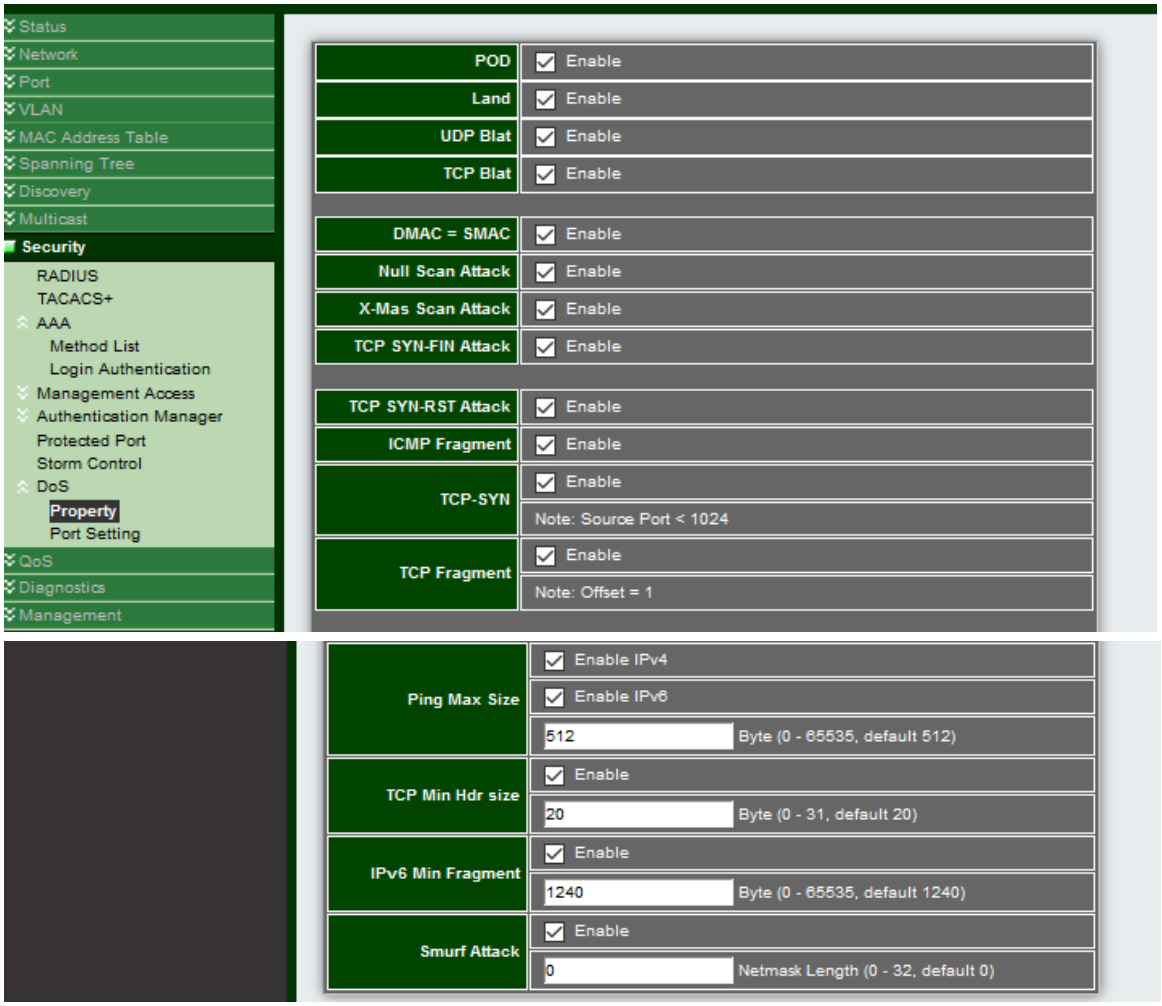




## 11.8 DoS

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.

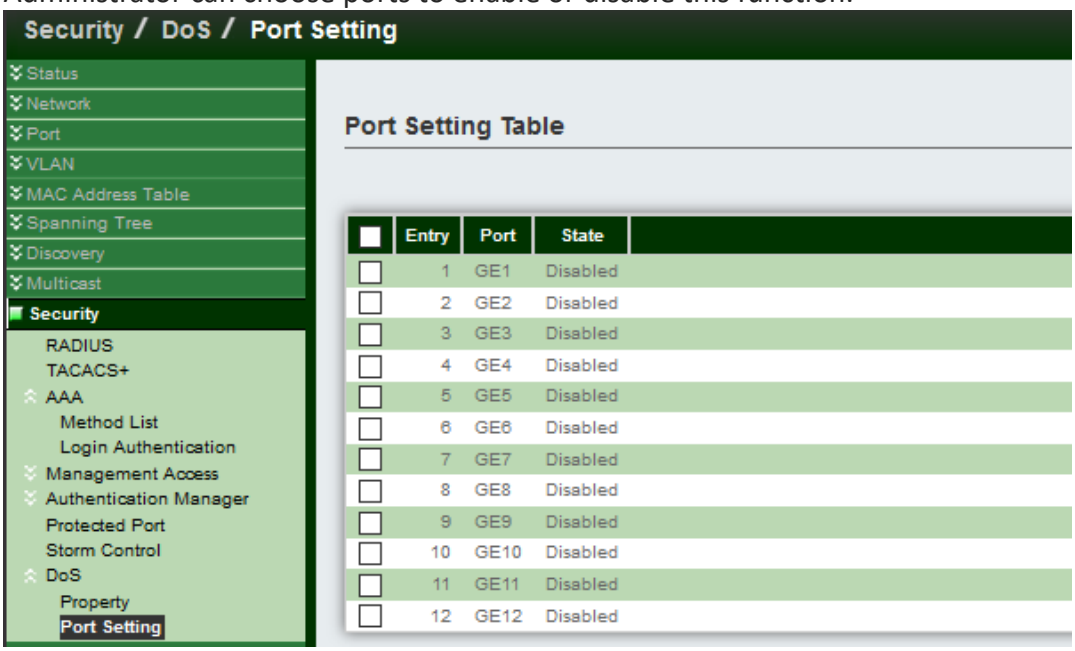
### 11.8.1 Property

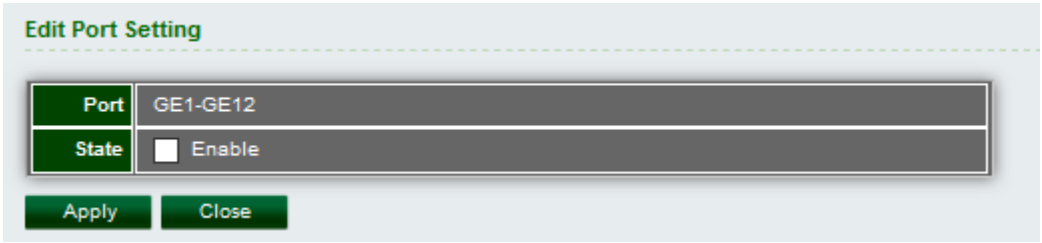
Administrators can enable and set security values to guard against DoS



### 11.8.2 Port Setting

Administrator can choose ports to enable or disable this function.



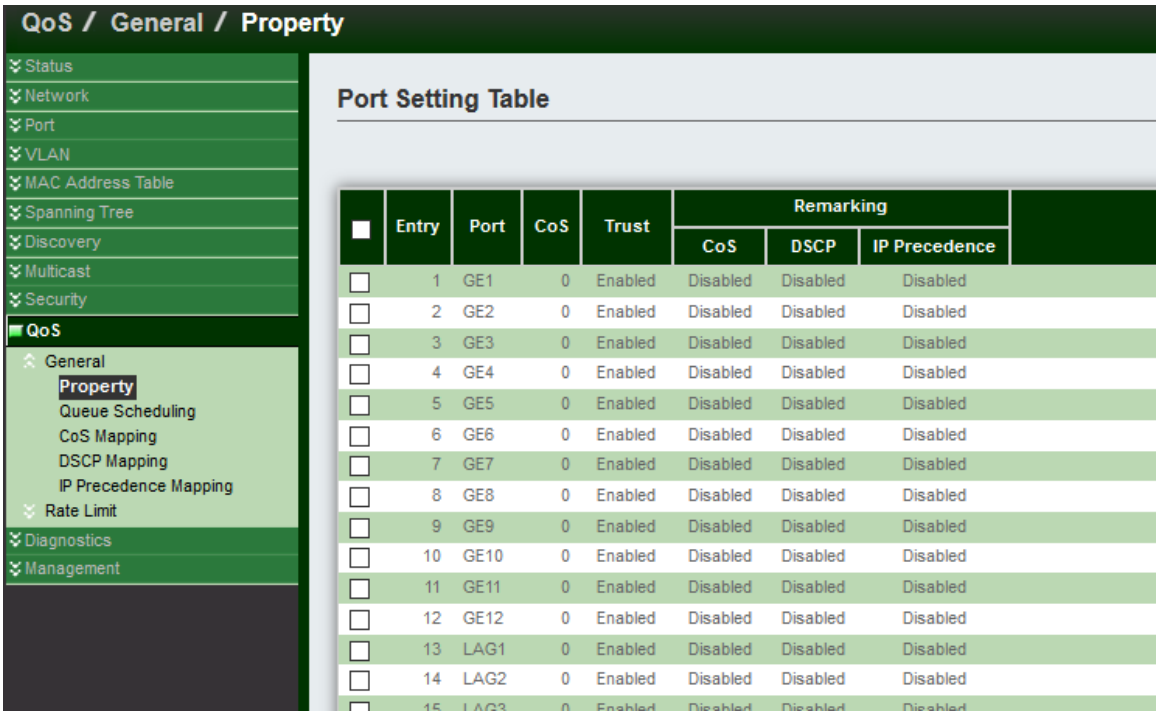



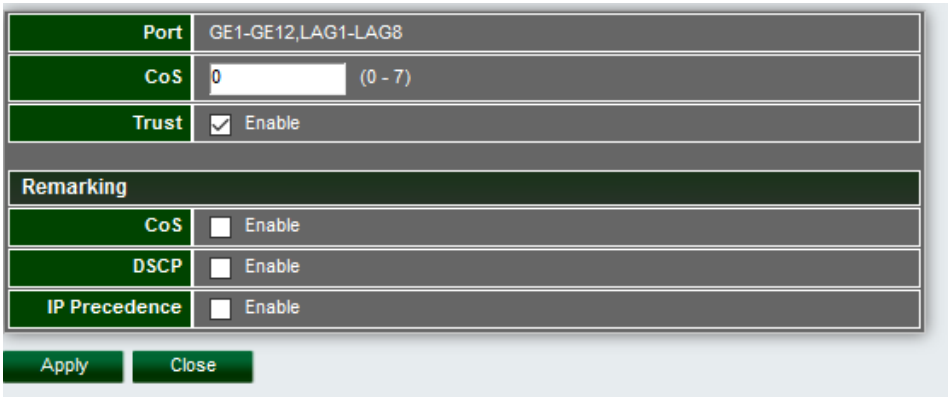

# 12. QoS

Quality of Service (QoS) prioritizes network traffic and manages available bandwidth so that the most important traffic goes first. QoS is implemented as rules or policies that prioritize packets, optionally change information in the packet header, and assign them to outbound port queues based on their priority.

## 12.1 Property

Administrator can set enable or disable QoS function. This switch implements two priority modes based on port, on cos and on DSCP. The port priorities are labeled as CoS0~7.

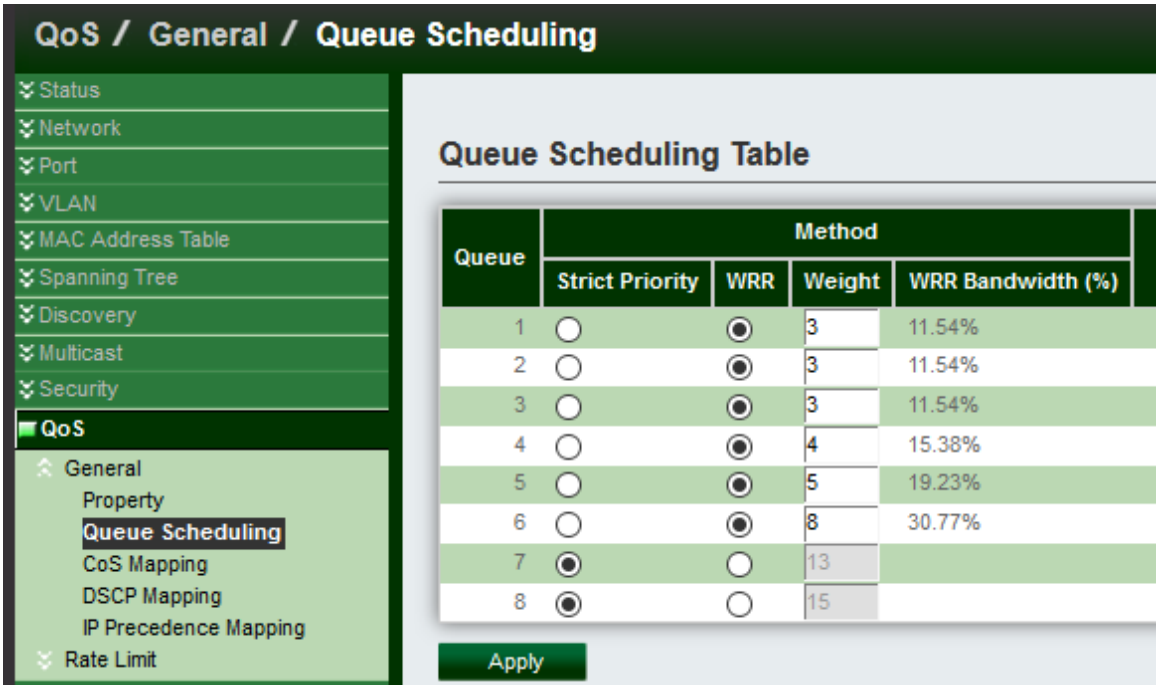



## 12.2 Queue Scheduling

This "**queue scheduling**" function support WRR and Strict Priority two method.

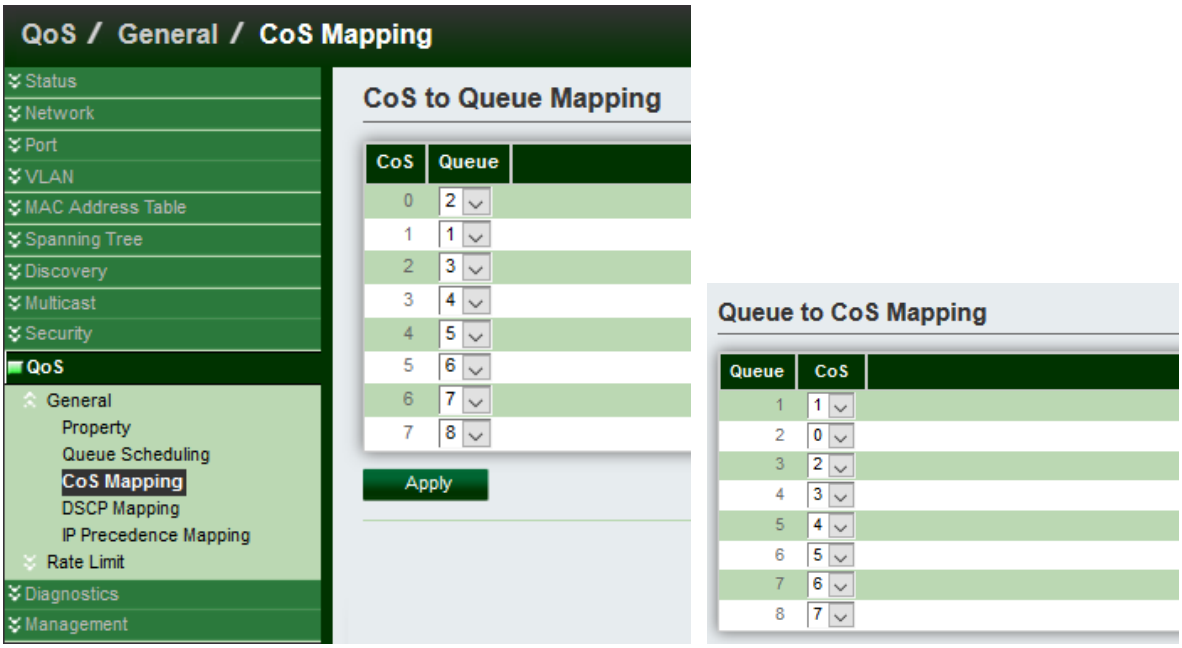
The following picture shows an example description of Queue Scheduling. When you select the combined SP and WRR queueing method, this switch schedules traffic in queue 7 and queue 6 first, based on the strict priority queueing method. When there is no traffic in queue 7 and queue 6, the device schedules 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.

## 12.3 CoS Mapping

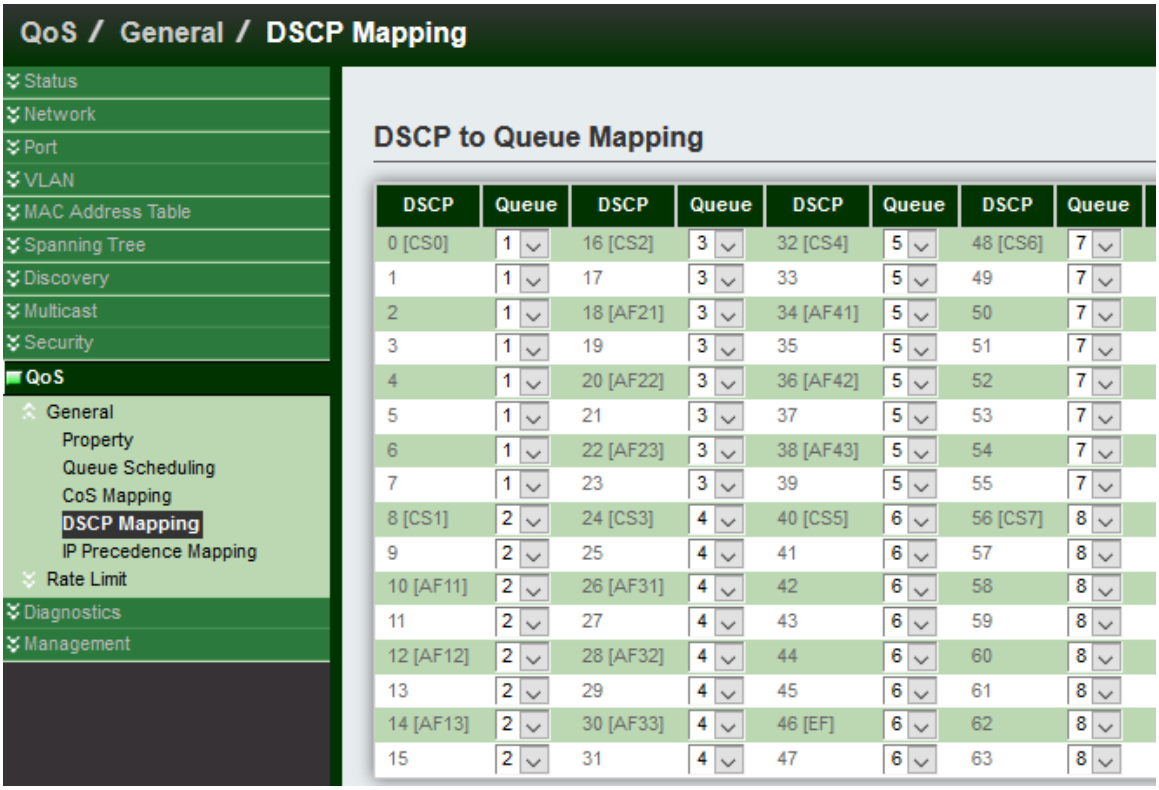
CoS to Queue mapping or Queue to CoS Mapping is queue schedule method and bandwidth allocation, it is possible to achieve the desired QoS in a network.

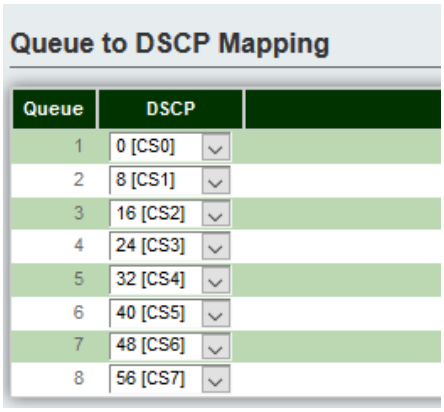



| CoS (0 to 7)<br>7 is highest | Queue(1 to 8)<br>8 is highest priority | Description |
|---|---|---|
| 0 | 2 | Background |
| 1 | 1 | Best Effort |
| 2 | 3 | Excellent Effort |
| 3 | 4 | Critical Application LVS phone SIP |
| 4 | 5 | Video |
| 5 | 6 | Voice Cisco IP phone default |
| 6 | 7 | Interwork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

## 12.4 DSCP Mapping

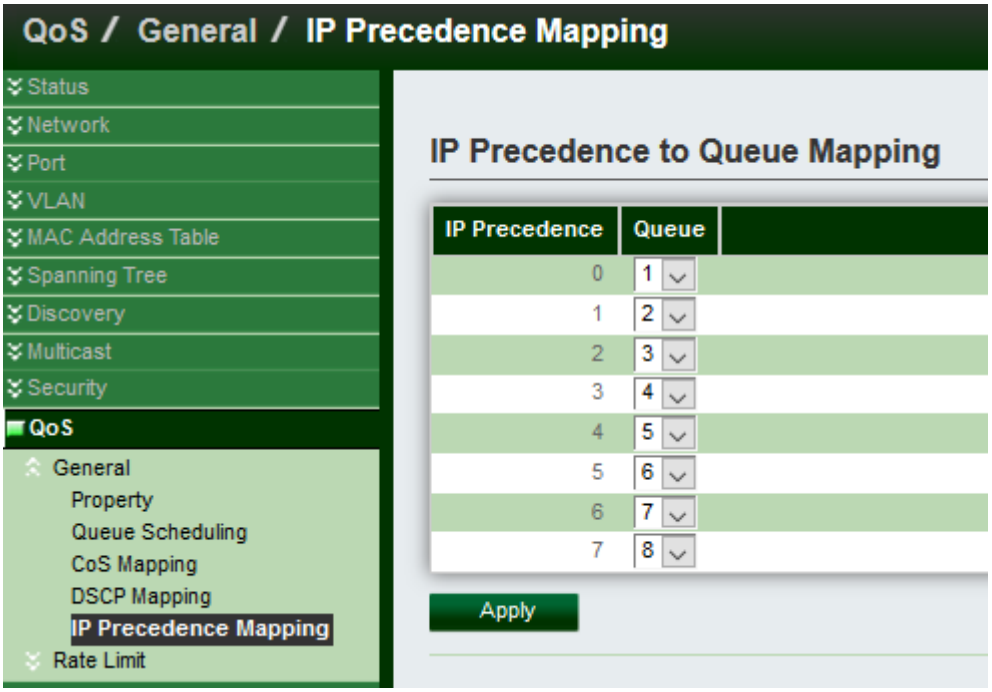
This DSCP values range from 0 through 63, whereas the internal forwarding priority values range from 1 through 8. Any DSCP value within a given range is mapped to the same internal forwarding priority value. These include the CS (Class Selector), AF (Assured Forwarding) and EF (Expedited Forwarding).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



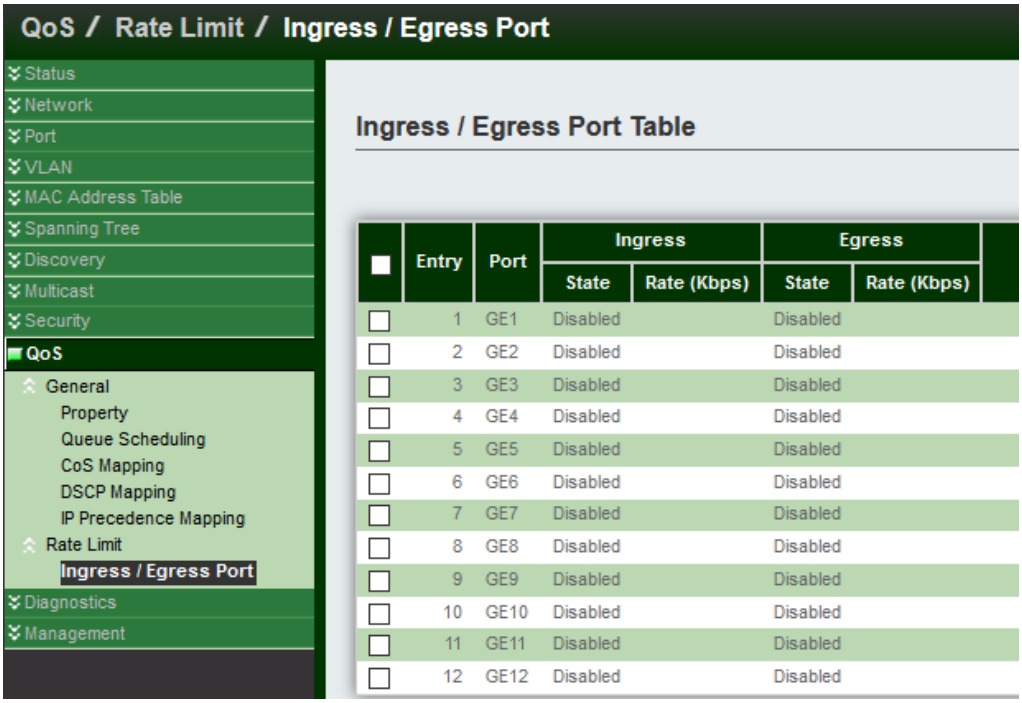

## 12.5 IP Precedence to Queue Mapping

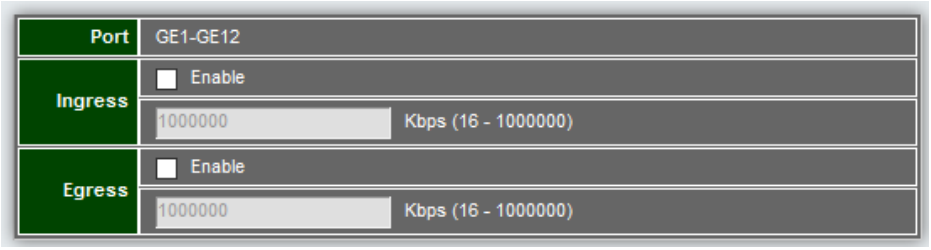
The IP Precedence standard uses the first 3 bits of the ToS byte to mark packets with 8 levels of priority, numbered 0-7, with 0 being the lowest priority and 7 the highest. Because IP Precedence and ToS use different bits in the ToS byte to mark the priority of a packet, they can co-exist in the same packet header without interfering with each other.




## 12.6 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



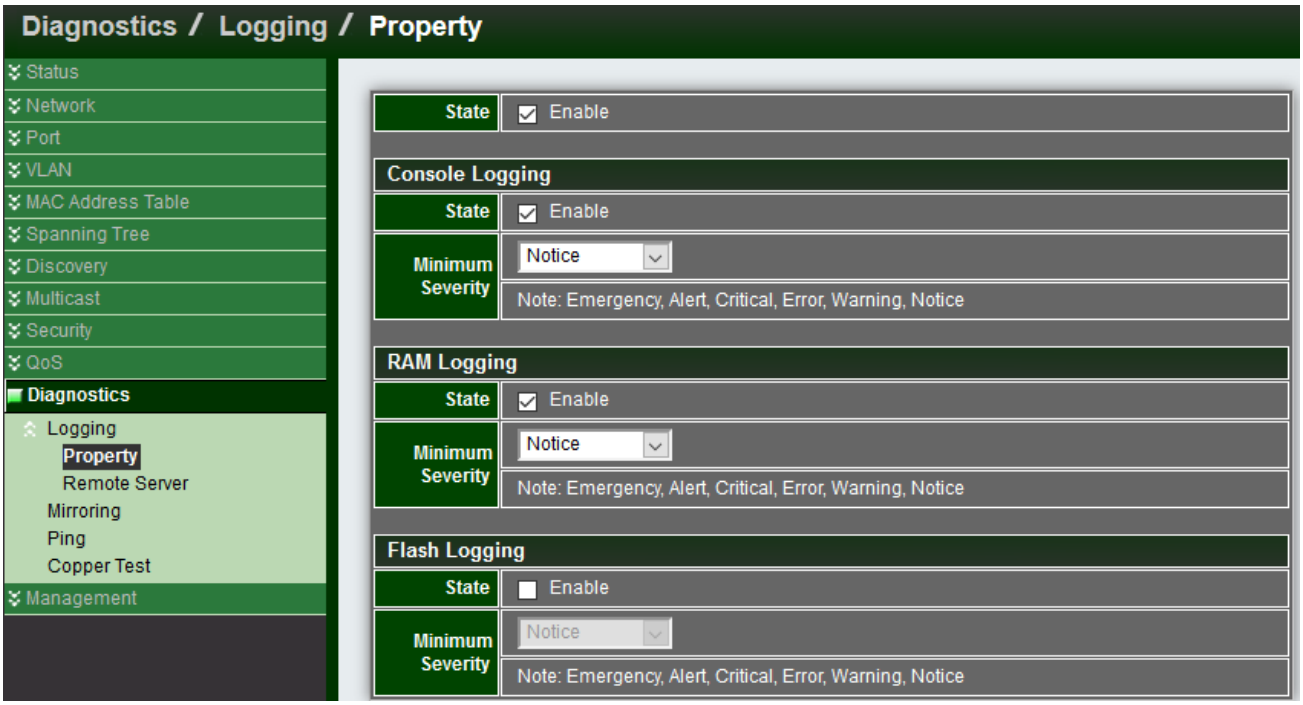



# 13. Diagnostics

## 13.1 Logging

### 13.1.1 Property

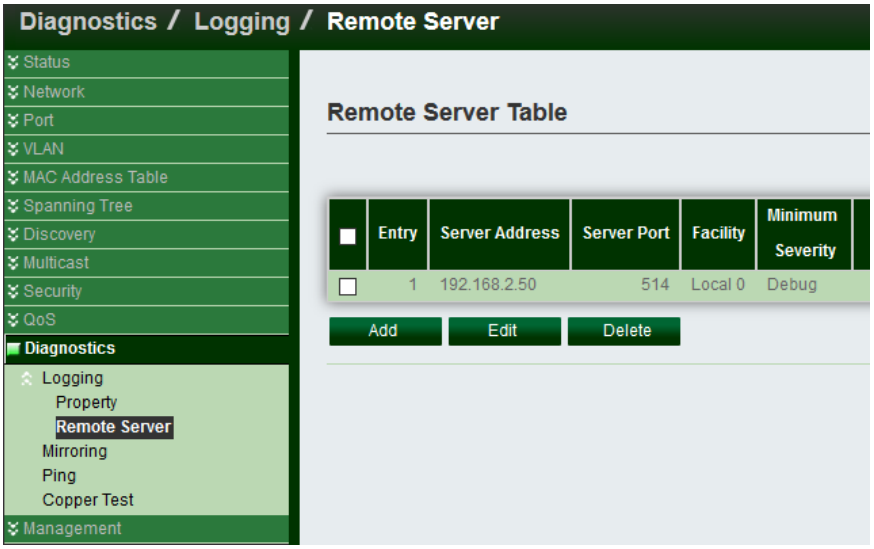
This function support log message includes Console / RAM / Flash message send to remote log server. Administrator can enable or disable this function.




- Minimum Severity: Administrator can choose message type to monitor.

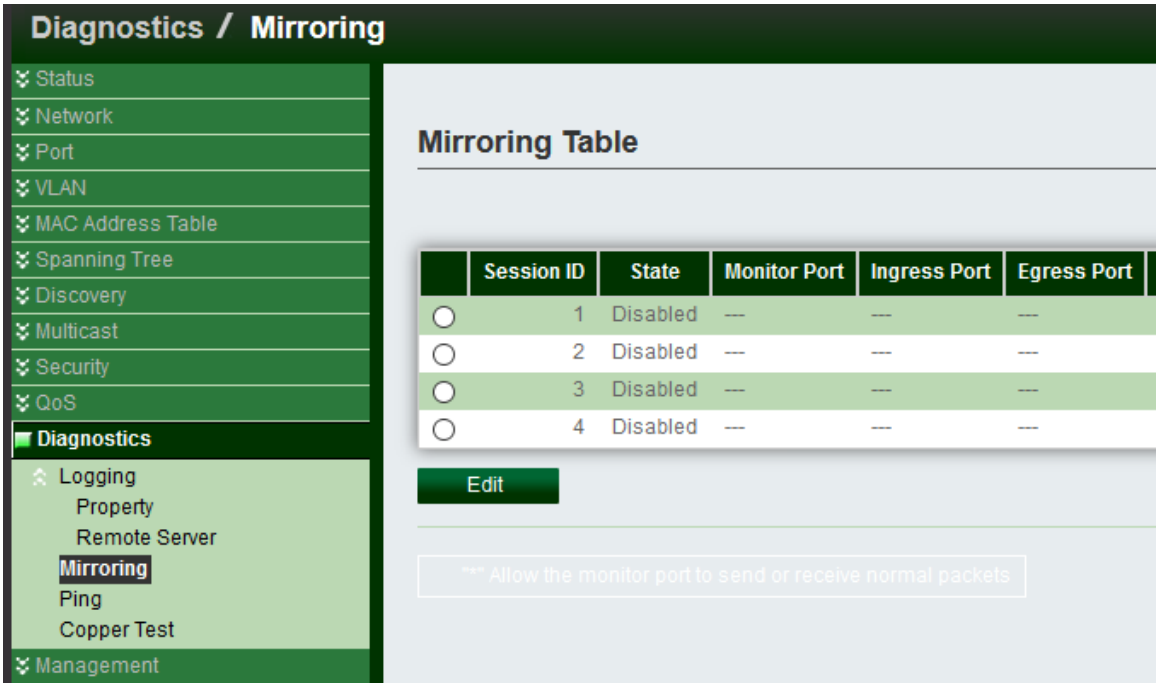
### 13.1.2 Remote Server

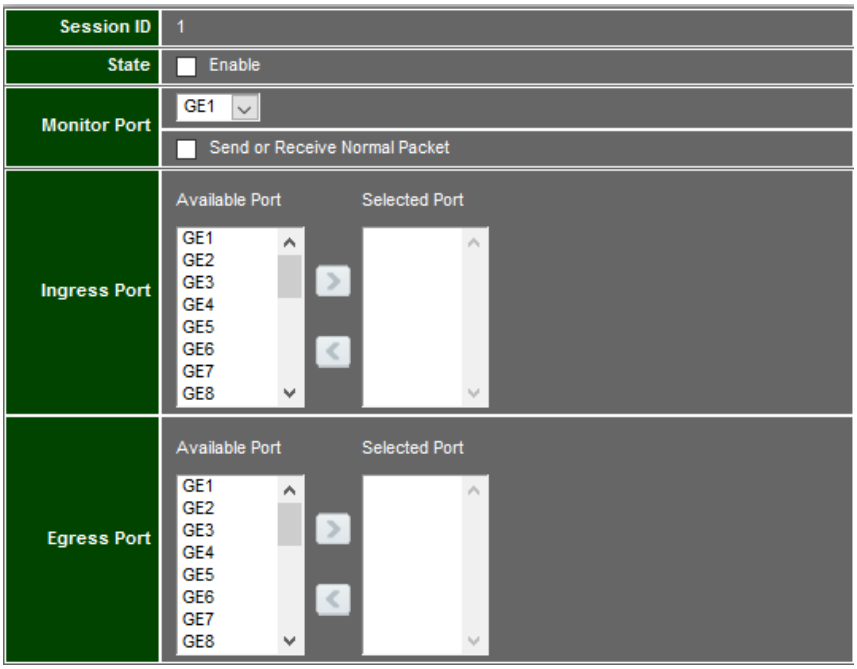
When the creation is complete then system log messages will send to remote log servers.




## 13.2 Mirroring

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

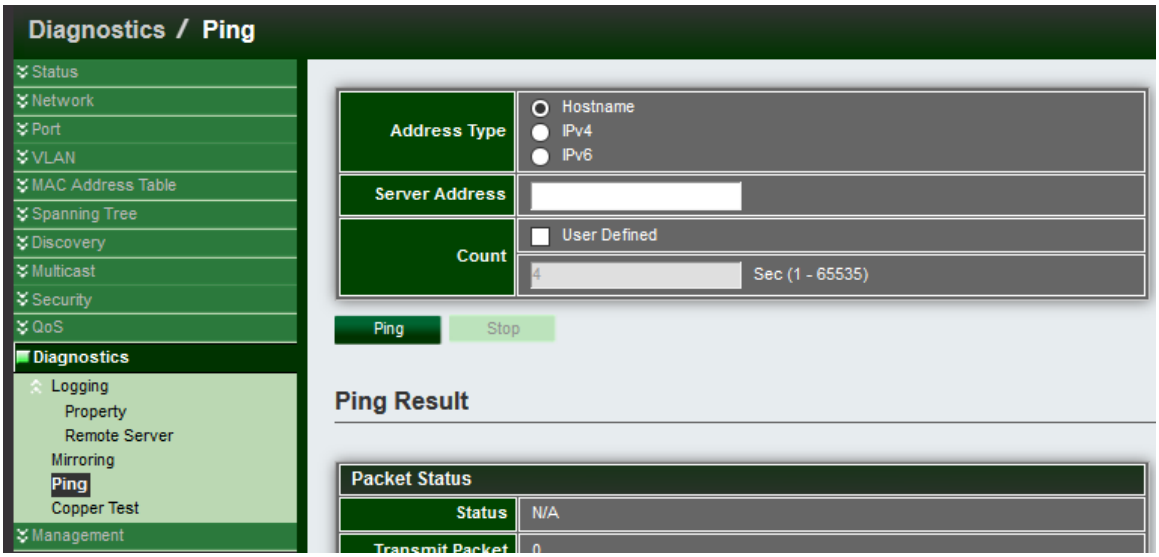





- **Mirroring Port:** Administrator can choose a mirroring Port.
- **Ingress Port:** Administrator can choose mirrored ports for ingress.
- **Egress Port:** Administrator can choose mirrored ports for egress.

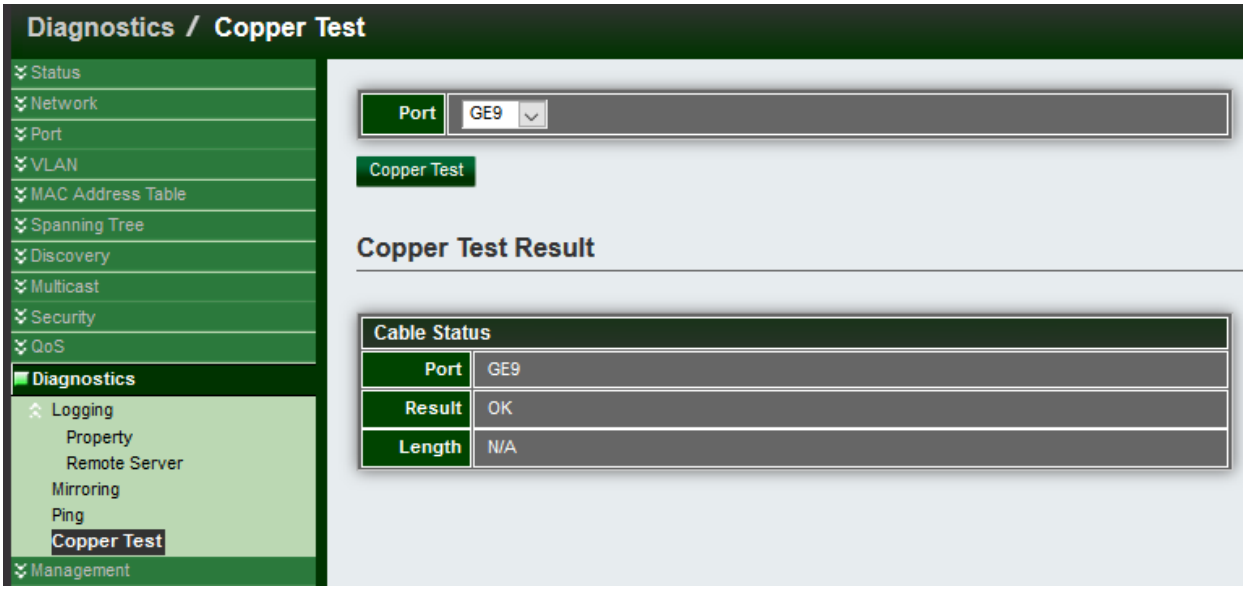
## 13.3 Ping

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



## 13.4 Copper Test

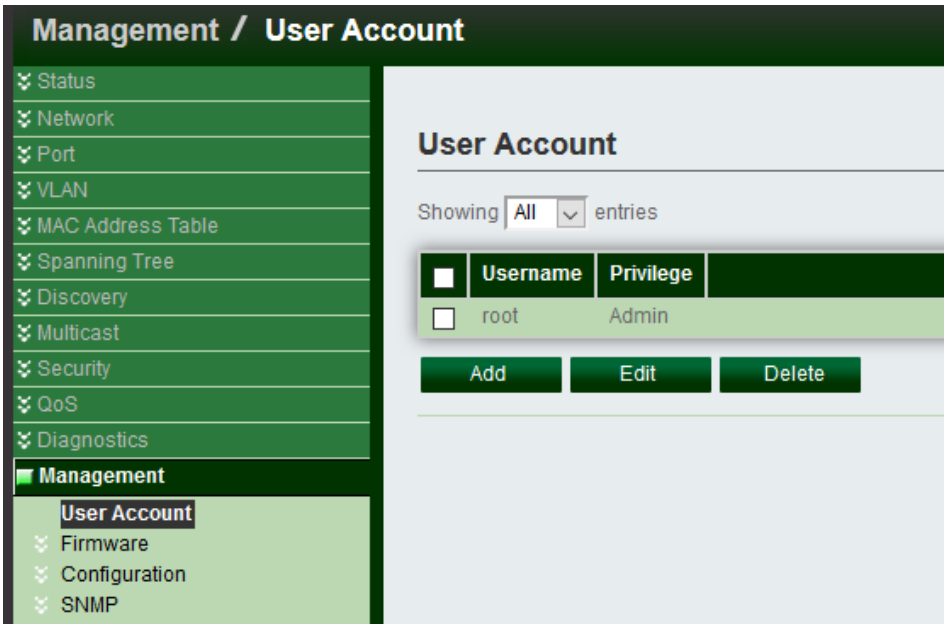
Administrator can use this function check port Result whether is working, if working then display OK.




# 14. Management

## 14.1 User Account

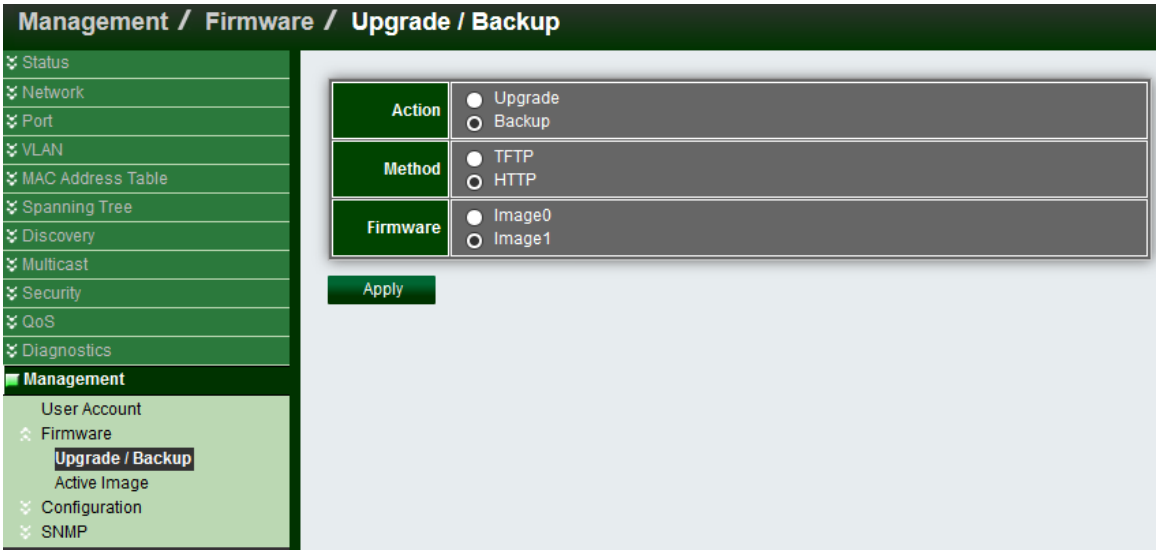
Administrator can added or modify user login account and password.



## 14.2 Firmware

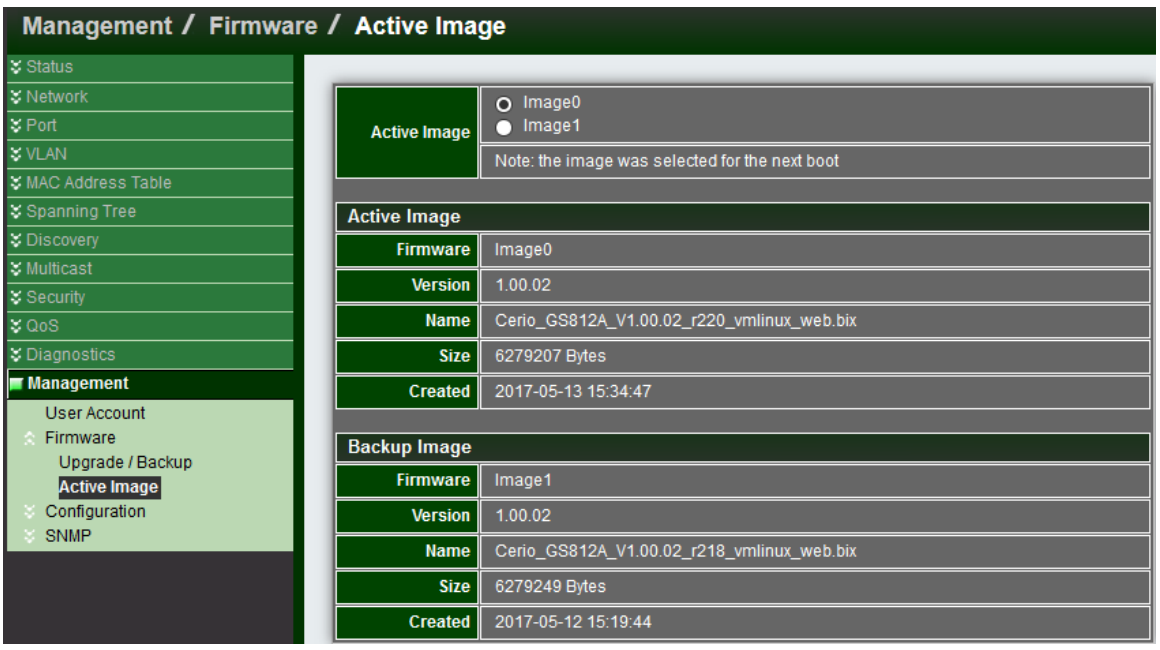
### 14.2.1 Upgrade / Backup

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.




### 14.2.2 Active Image

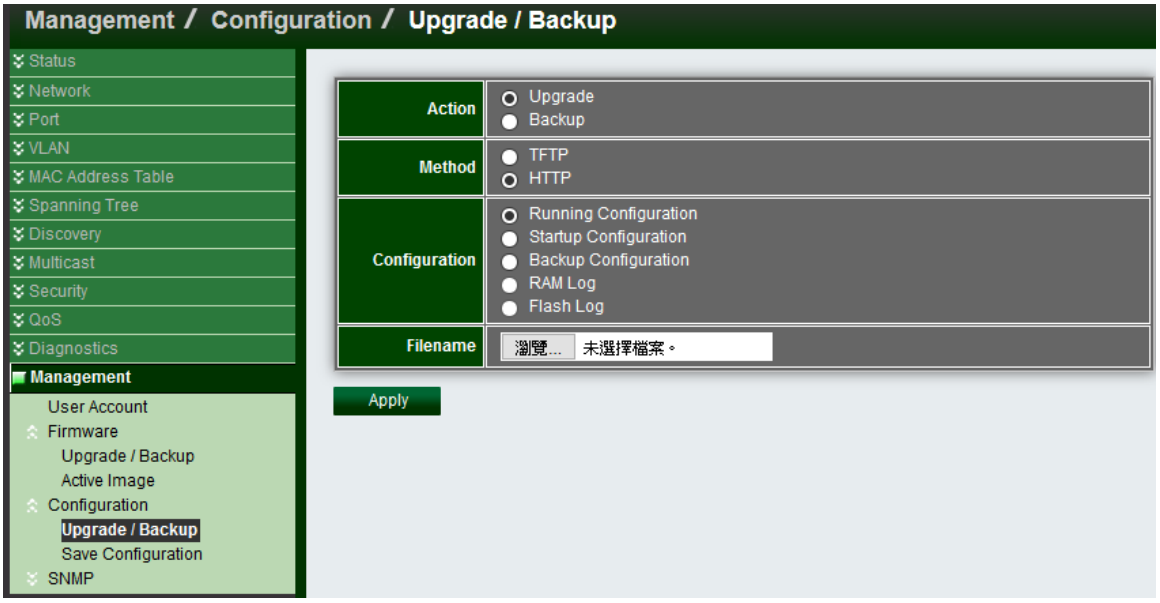
If the Switch has upload multiple firmware in system then administrator can choose a firmware to do system default start.



# 14.3 Configuration

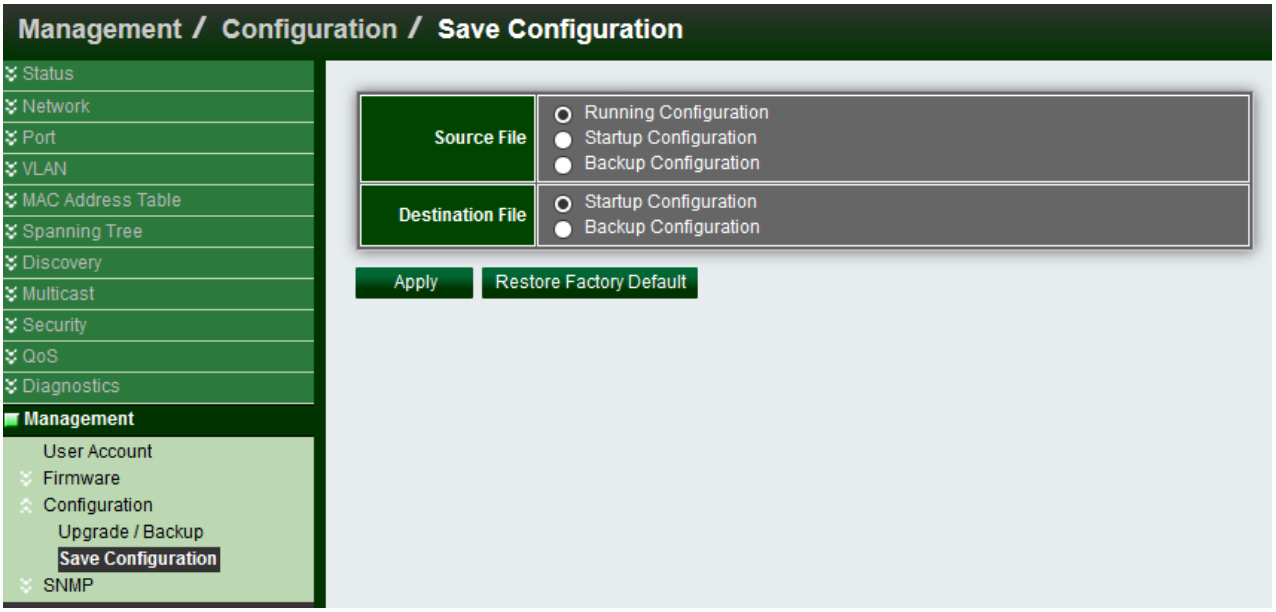
## 14.3.1 Upgrade / Backup

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




## 14.3.2 Save Configuration

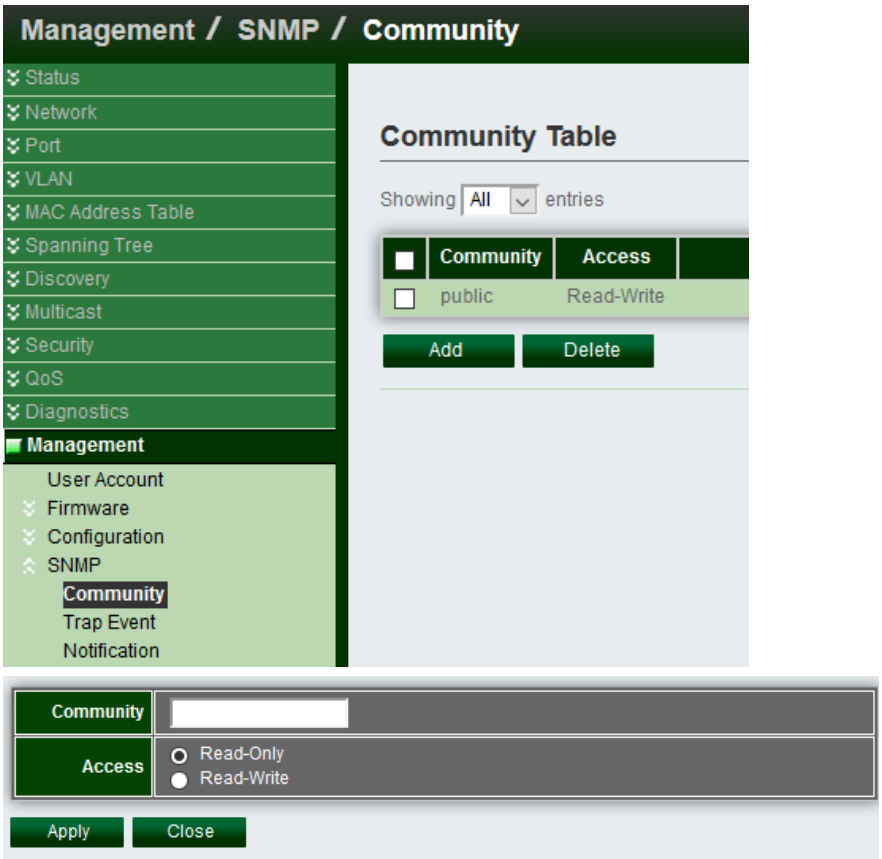
This Functions purpose is to backup current configuration, restore prior configuration or reset back to factory default configurations.



## 14.4 SNMP

### 14.4.1 Community

Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

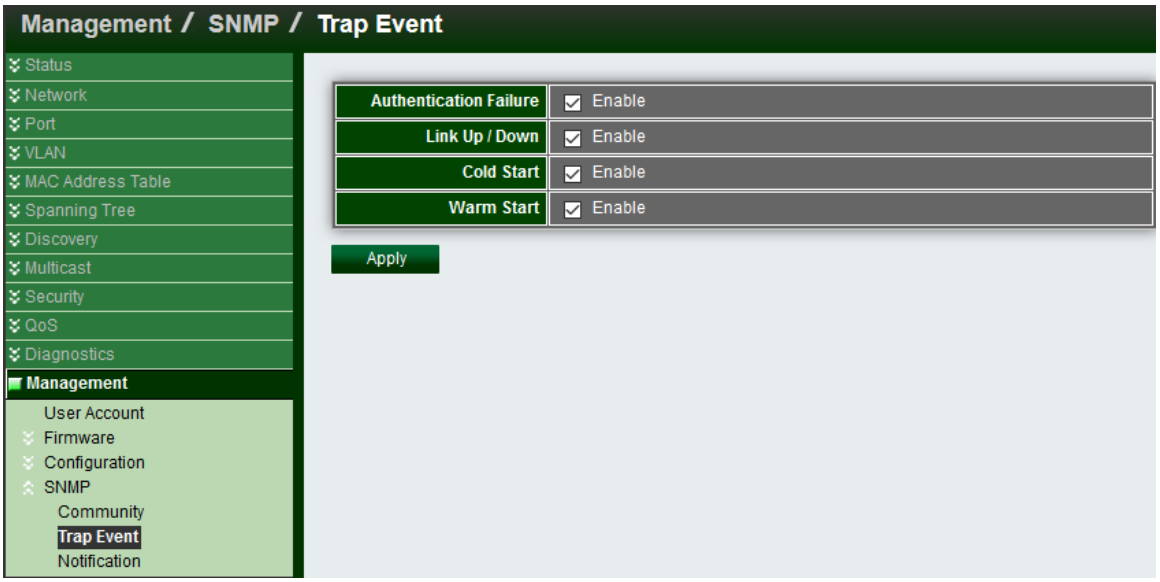



Administrator can create Read-Only or Read-Write of the community in SNMP.

- **Read-Only:** Administrator can enable a remote device to retrieve "read-only" information from a device.
- **Read-Write**: Can be mainly used in requests for information from a device and to modify settings on that device.

### 14.4.2 Trap Event

Administrator can choose SNMP Trap Event Type to monitor




### 14.4.3 Notification

Administrator can configuration SNMPv1 / SNMPv2 and server IP address.