8+2SFP Port 10/100/1000Mbps
PoE Web Smart Ethernet Switch

User Manual

Version 1.0 | 1/6/2015

Table of Contents

Chapter 1 Product Introduction

Congratulations on your purchasing of the PoE Web Smart Ethernet Switch. Before you install and use this product, please read this manual carefully for full exploiting the functions of this product.

1.1 Product Overview

The 8-port + 2SFP 10/100/1000M PoE Web Smart Ethernet Switch provides the seamless network connection. It integrates 10/100/1000Mbps Ethernet network capabilities. These PoE ports can automatically detect and supply power with those IEEE 802.3at compliant Powered Devices (PDs). In this situation, the electrical power is transmitted along with data in one single cable allowing you to expand your network where there are no power lines or outlets, where you wish to fix devices such as APs, IP Cameras or IP Phones, etc.

The Web Smart Ethernet Switch, and can be configured by web based interface. Including administrator, port management, VLAN setting, each port statistics, trunking setting, QoS setting, security filter, configuration/ backup/recovery, log out, and so on.

1.2 Features

- Complies with IEEE802.3, IEEE 802.3u, IEEE 802.3ab standards
- 8 x 10/100/1000Mbps Auto-Negotiation RJ45 ports supporting Auto-MDI/MDIX
- Supports PoE power up to 30W for each PoE port
- Supports All power up to 140W
- Support the Console port management
- Supports PoE IEEE802.3at compliant PDs
- Supports IEEE802.3x flow control for Full-duplex Mode and backpressure for Half-duplex Mode
- 8K entry MAC address table of the Switch with auto-learning and auto-aging
- Supports WEB management interface
- LED indicators for monitoring power, link, activity and speed
- Internal power adapter supply

1.3 External Component Description

1.3.1 Front Panel

The front panel of the Switch consists of 8 x 10/100/1000Mbps RJ-45 ports, 1 x Console port, 2 x SFP ports, 1 x Reset button and a series of LED indicators as shown as below.

Figure 1 - Front Panel

10/100/1000Mbps RJ-45 ports (1~8):
Designed to connect to the device with a bandwidth of 10Mbps, 100Mbps or 1000Mbps. Each has a corresponding 10/100/1000Mbps LED.

Console port (Console):
Designed to connect with the serial port of a computer or terminal for monitoring and configuring the Switch.

SFP ports (SFP1, SFP2):
Designed to install the SFP module and connect to the device with a bandwidth of 1000Mbps. Each has a corresponding 1000Mbps LED.

Reset button (Reset):
Keep the device powered on and push a paper clip into the hole.
Press down the button for 2 seconds to reboot the Switch, Press down the button for 5 seconds to restore the Switch to its original factory default settings.

LED indicators:
The LED Indicators will allow you to monitor, diagnose and troubleshoot any potential problem with the Switch, connection or attached devices.

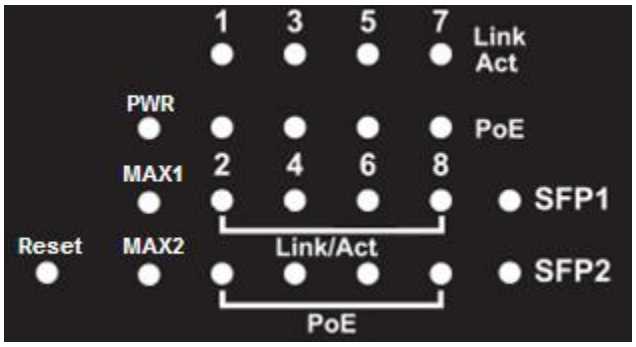


Figure 2 - LED Indicators

The following chart shows the LED indicators of the Switch along with explanation of each indicator.

LED	COLOR	STATUS	STATUS DESCRIPTION
PWR	Green	On	Power On
		Off	Power Off

Link/Act (1-8)	10/100M: Orange 1000M: Green	On	A device is connected to the port
		Off	A device is disconnected to the port
		Flashing	Sending or receiving data
PoE	Green	On	A Powered Device is connected to the port, which supply power successfully.
		Off	No PD is connected to the corresponding port, or no power is supplied according to the power limits of the port.
		Flashing	The PoE power circuit may be in short or the power current may be overloaded.
Max 1 (1-4Ports)	Green	On	When the power which output to PDs has reached the maximum power budget(The power of all the connected PoE ports is ≥55W). No power may be supplied if additional PDs are connected.
		Off	The power of all the connected PoE ports is <55W, or No PD connected to the corresponding port.
		Flashing	When the power which output to PDs has exceeded the maximum power budget(The power of all the connected PoE port is ≥70W).
Max 2 (5-8Ports)	Green	On	When the power which output to PDs has reached the maximum power budget(The power of all the connected PoE ports is ≥55W). No power may be supplied if additional PDs are connected.
		Off	The power of all the connected PoE ports is <55W, or No PD connected to the corresponding port.
		Flashing	When the power which output to PDs has exceeded the maximum power budget (The power of all the connected PoE port is ≥70W).
SFP1 SFP2	Green	On	A device is connected to the port
		Off	A device is disconnected to the port
		Flashing	Sending or receiving data

1.3.2 Rear Panel

The rear panel of the Switch contains AC power connector and one marker shown as below.

Figure 3 - Rear Panel

AC Power Connector:

Power is supplied through an external AC power adapter. It supports AC 100~240V, 50/60Hz.

1.4 Package Contents

Before installing the Switch, make sure that the following the "packing list" listed OK. If any part is lost and damaged, please contact your local agent immediately. In addition, make sure that you have the tools install switches and cables by your hands.

- One PoE Web Smart Ethernet Switch
- Four rubber feet, two mounting ears and eights screws
- One AC power cord
- One Quick Installation Guide

Chapter 2 Installing and Connecting the Switch

This part describes how to install your PoE Ethernet Switch and make connections to it. Please read the following topics and perform the procedures in the order being presented.

2.1 Installation

Please follow the following instructions in avoid of incorrect installation causing device damage and security threat.

- Put the Switch on stable place or desktop in case of falling damage.
- Make sure the Switch works in the proper AC input range and matches the voltage labeled on the Switch.
- To keep the Switch free from lightning, do not open the Switch's shell even in power failure.
- Make sure that there is proper heat dissipation from and adequate ventilation around the Switch.
- Make sure the cabinet to enough back up the weight of the Switch and its accessories.

2.1.1 Desktop Installation

Sometimes users are not equipped with the 11-inch standard cabinet. So when installing the Switch on a desktop, please attach these cushioning rubber feet provided on the bottom at each corner of the Switch in case of the external vibration. Allow adequate space for ventilation between the device and the objects around it.

2.1.2 Rack-mountable Installation in 11-inch Cabinet

The Switch can be mounted in an EIA standard-sized, 11-inch rack, which can be placed in a wiring closet with other equipment. To install the Switch, please follow these steps:

a. attach the mounting brackets on the Switch's side panels (one on each side) and secure them with the screws provided.

Figure 4 - Bracket Installation

b. use the screws provided with the equipment rack to mount the Switch on the rack and

tighten it.

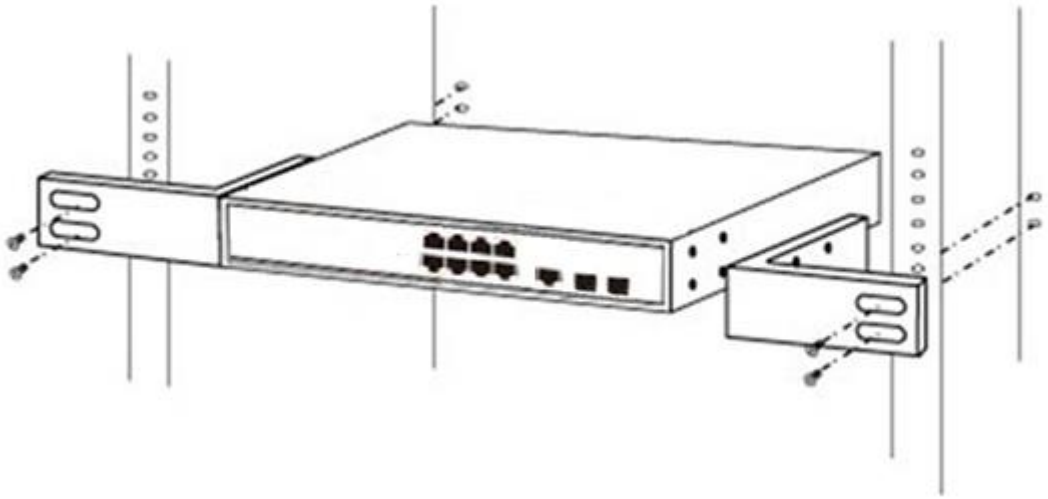


Figure 5 - Rack Installation

2.1.3 Power on the Switch

The Switch is powered on by the AC 100-240V 50/60Hz internal high-performance power supply. Please follow the next tips to connect:

AC Electrical Outlet:
It is recommended to use single-phase three-wire receptacle with neutral outlet or multifunctional computer professional receptacle. Please make sure to connect the metal ground connector to the grounding source on the outlet.

AC Power Cord Connection:
Connect the AC power connector in the back panel of the Switch to external receptacle with the included power cord, and check the power indicator is ON or not. When it is ON, it indicates the power connection is OK.

2.2 Connect Computer (NIC) to the Switch

Please insert the NIC into the computer, after installing network card driver, please connect one end of the twisted pair to RJ-45 jack of your computer, the other end will be connected to any RJ-45 port of the Switch, the distance between Switch and computer is around 100 meters. Once the connection is OK and the devices are power on normally, the LINK/ACT/Speed status indicator lights corresponding ports of the Switch.

2.3 Switch connection to the PD

1-8 ports of the Switch have PoE power supply function, the maximum output power up to 30W each port, it can make PD devices, such as internet phone, network camera, wireless access point work. You only need to connect the Switch PoE port directly connected to the PD port by network cable.

Chapter 3 How to Login the Switch

3.1 Switch to End Node

Use standard Cat.5/5e Ethernet cable (UTP/STP) to connect the Switch to end nodes as described below. Switch ports will automatically adjust to the characteristics (MDI/MDI-X, speed, duplex) of the device to which is connected.

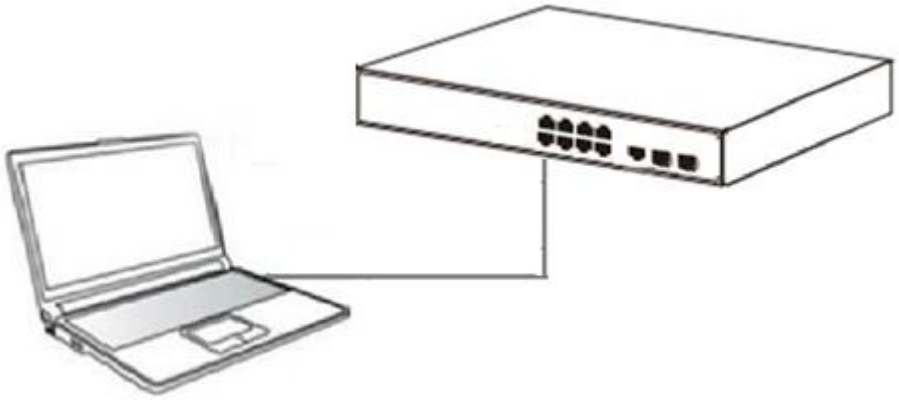


Figure 6 - PC Connect

Please refer to the **LED Indicators.** The LINK/ACT/Speed LEDs for each port lights on when the link is available.

3.2 How to Login the Switch

As the Switch provides Web-based management login, you can configure your computer's IP address manually to log on to the Switch. The default settings of the Switch are shown below.

Parameter	Default Value
Default IP address	192.168.2.1
Default user name	admin
Default password	admin

You can log on to the configuration window of the Switch through following steps:

1. Connect the Switch with the computer NIC interface.
2. Power on the Switch.
3. Check whether the IP address of the computer is within this network segment: 192.168.2.xxx ("xxx" ranges 2~254), for example, 192.168.2.100.
4. Open the browser, and enter *http://192.168.2.1* and then press "Enter". The Switch login window appears, as shown below.

Figure 7- Login Windows

5. Enter the Username and Password (The factory default Username is **admin** and Password is **admin**), and then click “LOGIN” to log in to the Switch configuration window as below.

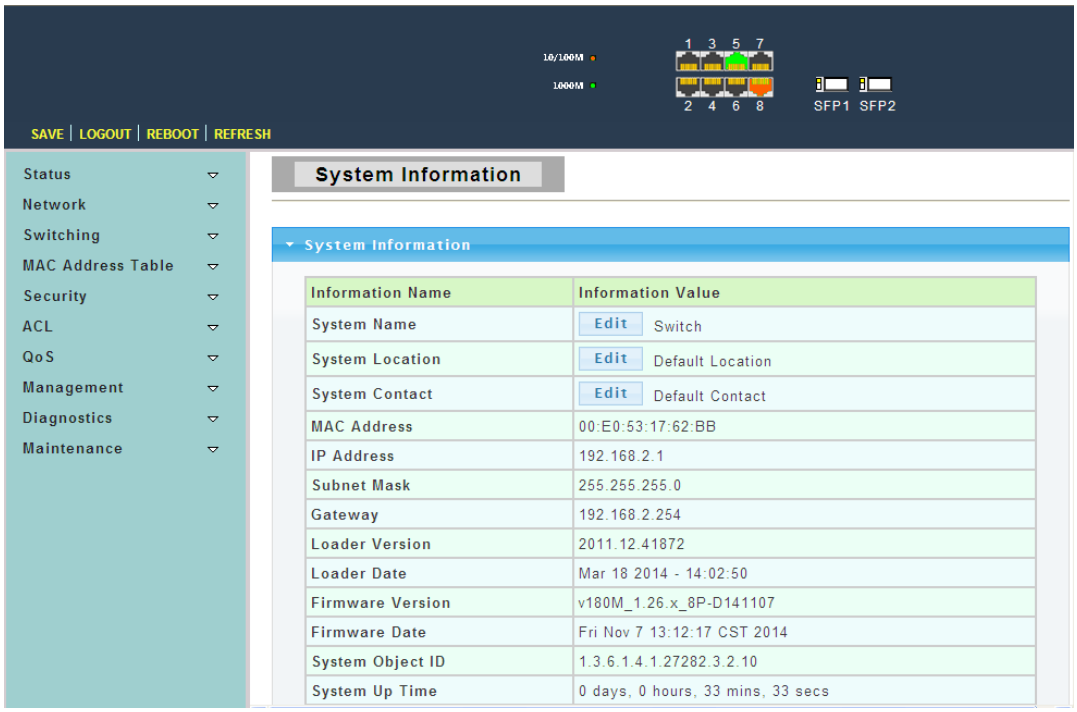
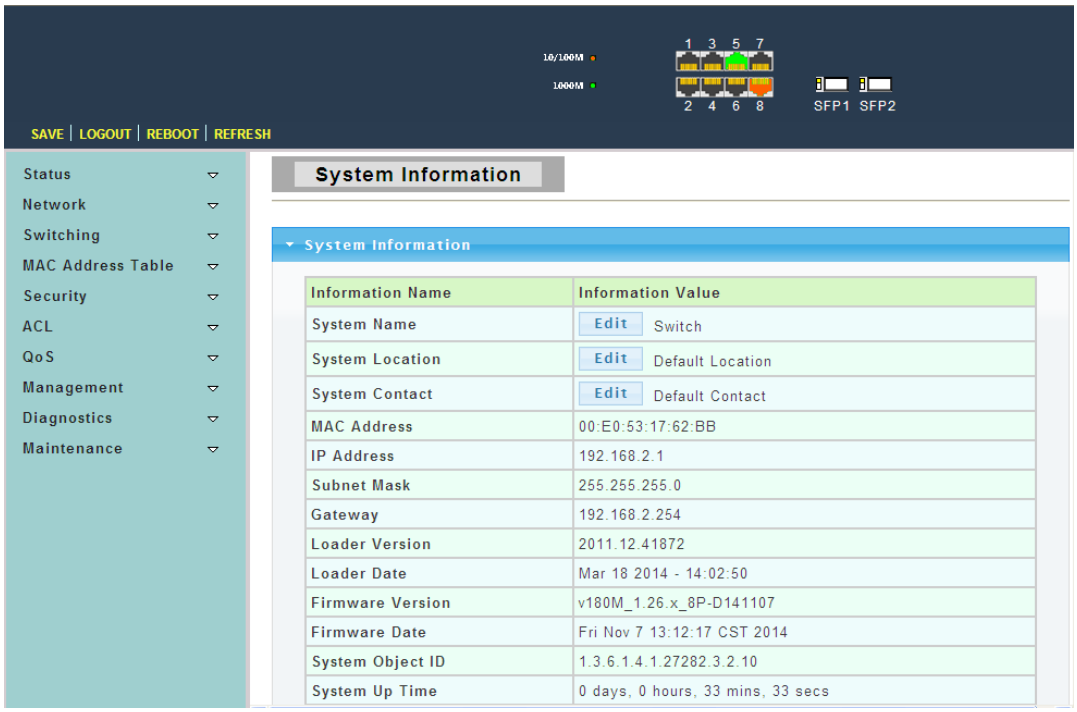


Figure 8 - Configuration Windows

Chapter 4 Switch Configuration

Web Smart Ethernet Switch Managed switch software provides rich layer 2 functionality for switches in your networks. This chapter describes how to use Web-based management interface (Web UI) to this switch configure managed switch software features.

In the Web UI, the left column shows the configuration menu. The top row shows the switch's current link status.Display port connection speed of 10/100 m the orange square, green square display port connection speed of 1000 m, while black square display port is not connected. Below the switch panel, you can find a common toolbar to provide useful functions for users. The rest of the screen area displays the configuration settings.



4.1 Tool

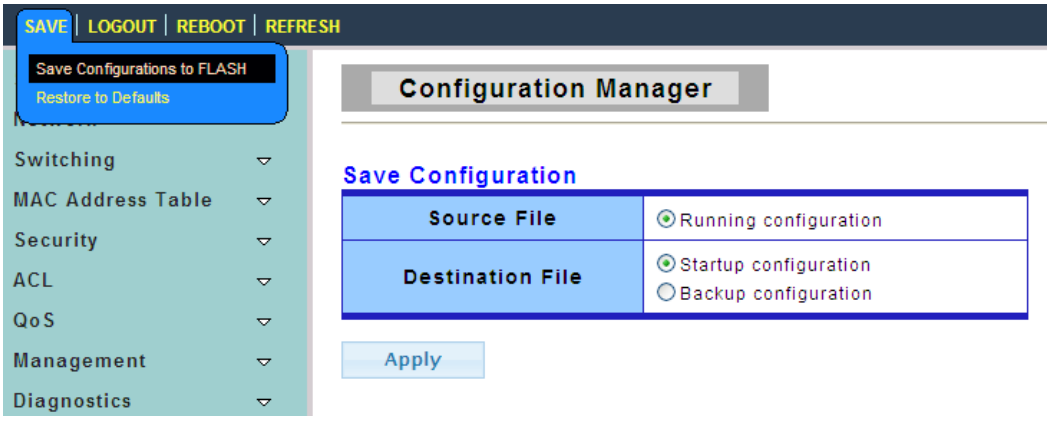
There are "SAVE", "LOGOUT", "REBOOT" and "REFRESH" configuration web pages in this section.

4.1.1 SAVE

4.1.1.1 Save Configurations to FlASH

To display theConfiguration Manager web page, click **SAVE > Save Configurations to FLASH**

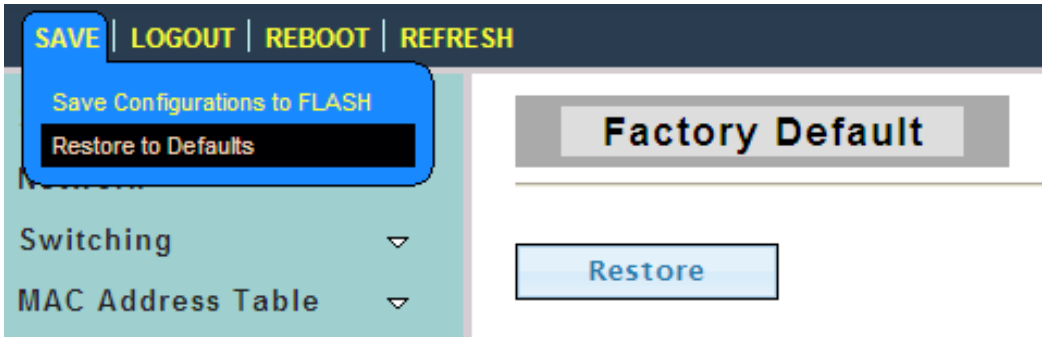
Click the "Apply" button and confirm to save all settings of the switch. If you don't save the settings, the switch will use the values you have saved last time after rebooted.



4.1.1.2 Restore to Defaults

To display the Factory Default web page, click **SAVE > Restore to Defaults**

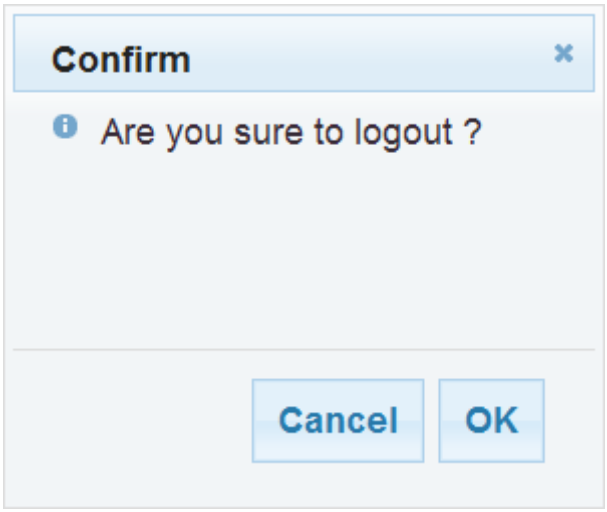
This page allow user to restore switch to factory default by click the “Restore” button.



4.1.2 LOGOUT

To display the LOGOUT web page, click **LOGOUT**

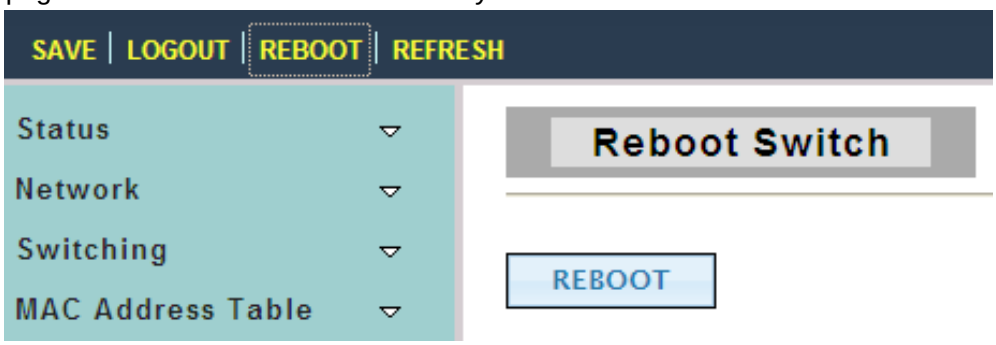
Click the “OK” button to immediately exit the switch.



4.1.3 Reboot

To display the Reboot Switch web page, click **Reboot**

This page allow user to reboot the switch by click the “Reboot” button.



4.1.4 REFRESH

YOU can click the “REFRESH” button to refresh the screen.

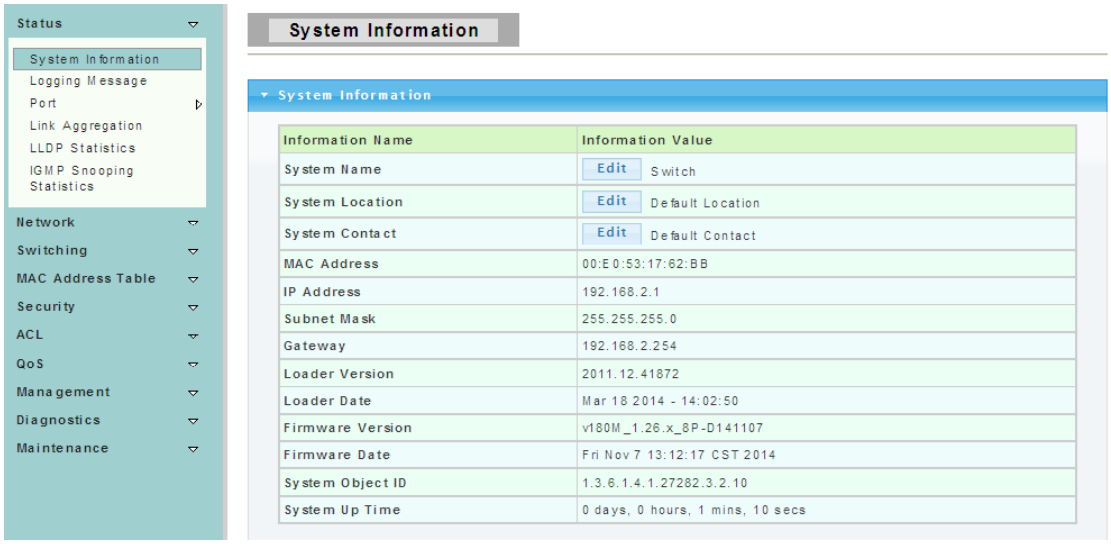
4.2 Status

Use the Status pages to view system information and status.

4.2.1 System Information

To display the System Information web page, click **Status > System Information**

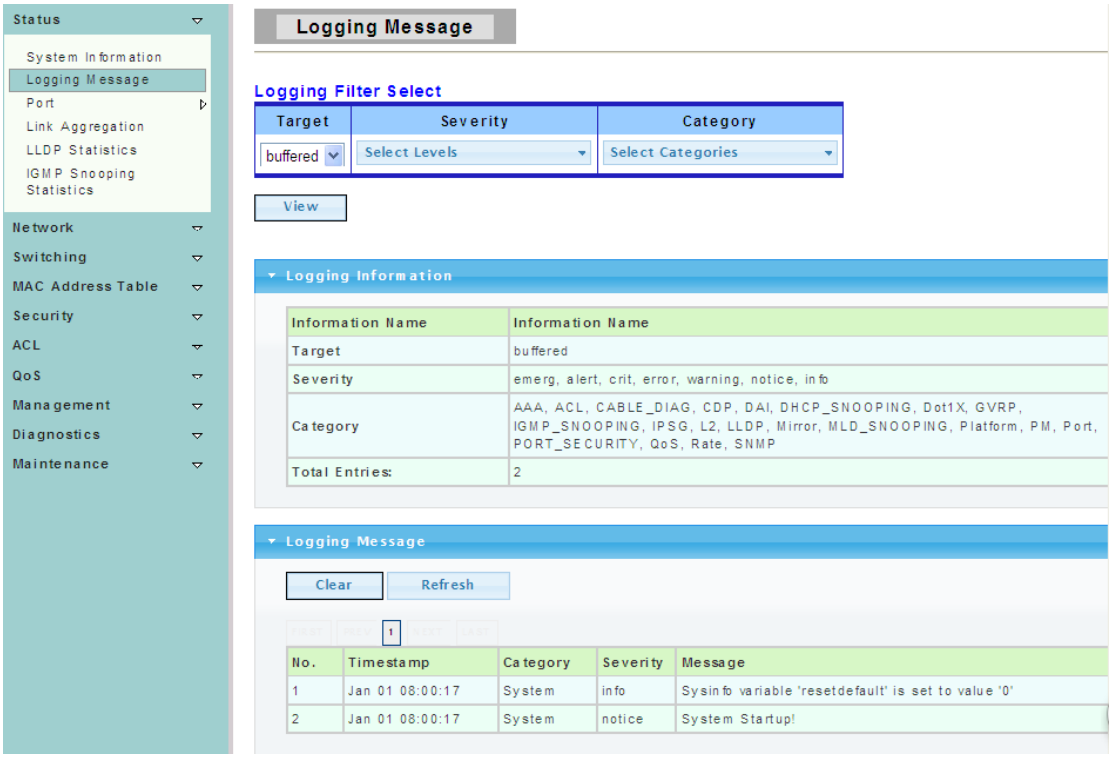
This page allows user to configure System related information and browse some system information such as MAC address, IP address, firmware version, loader version …… etc.



System Name: Enter a system name for the Switch, if so desired. This name will identify it in the Switch network.
System Location: Enter the location of the Switch, if so desired.
System Contact: Enter a contact name for the Switch, if so desired.

4.2.2 Logging Message

To display the Logging Message web page, click **Status > Logging Message**



Target: Select the log message source to show on the table.

- buffered: Logs store in the buffered.
- flash: Logs store in the flash.

Severity: Select severity to filter log messages.

Category: Select category to filter log messages.

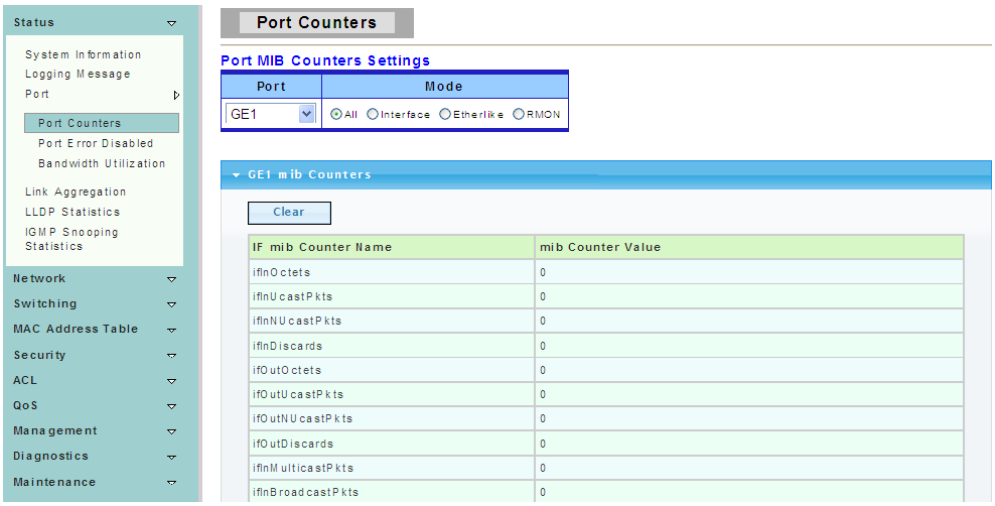
4.2.3 Port

The Port configuration page displays port summary and status information.

4.2.3.1 Port Counters

To display the Port Counters web page, click **Status > Port > Port Counters**

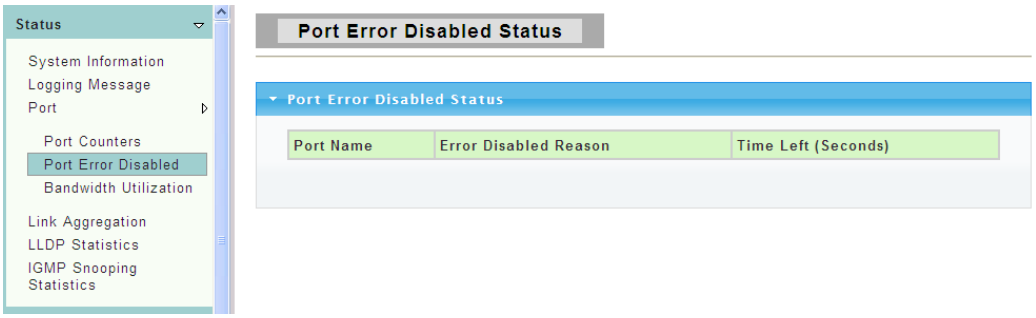
This page displays standard counters on network traffic form the Interfaces, Ethernet-like and RMON MIB. Interfaces and Ethernet-like counters display errors on the traffic passing through each port. RMON counters provide a total count of different frame types and sizes passing through each port.



4.2.3.2 Port Error Disabled

To display the Port Error Disabled web page, click **Status > Port > Port Error Disabled**

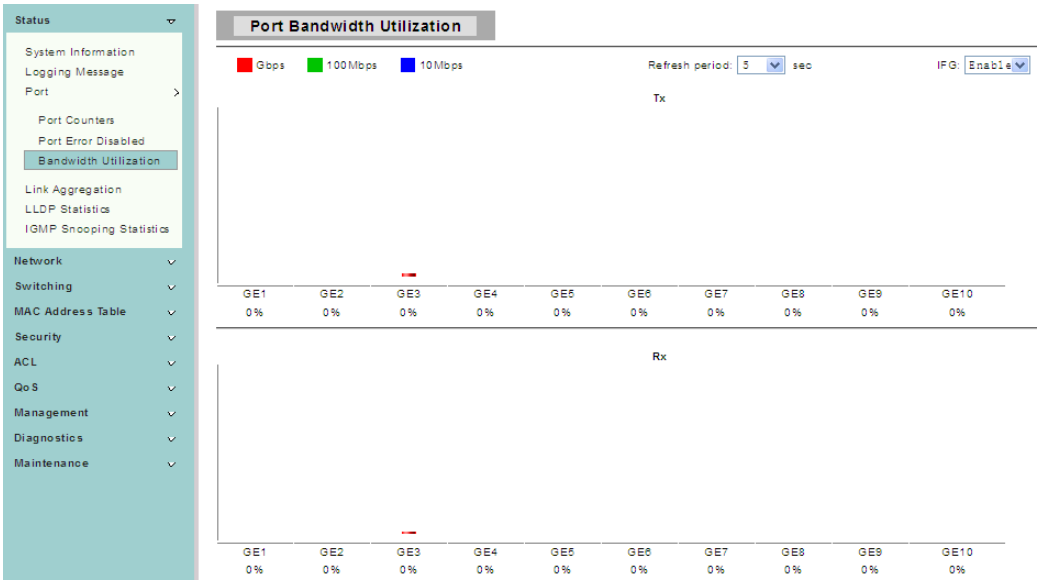
This page allow user to browse ports which disabled by some protocols such as BPDU Guard, Loop back and UDLD.



4.2.3.3 Bandwidth Utilization

To display the Bandwidth Utilization web page, click **Status > Port > Bandwidth Utilization**

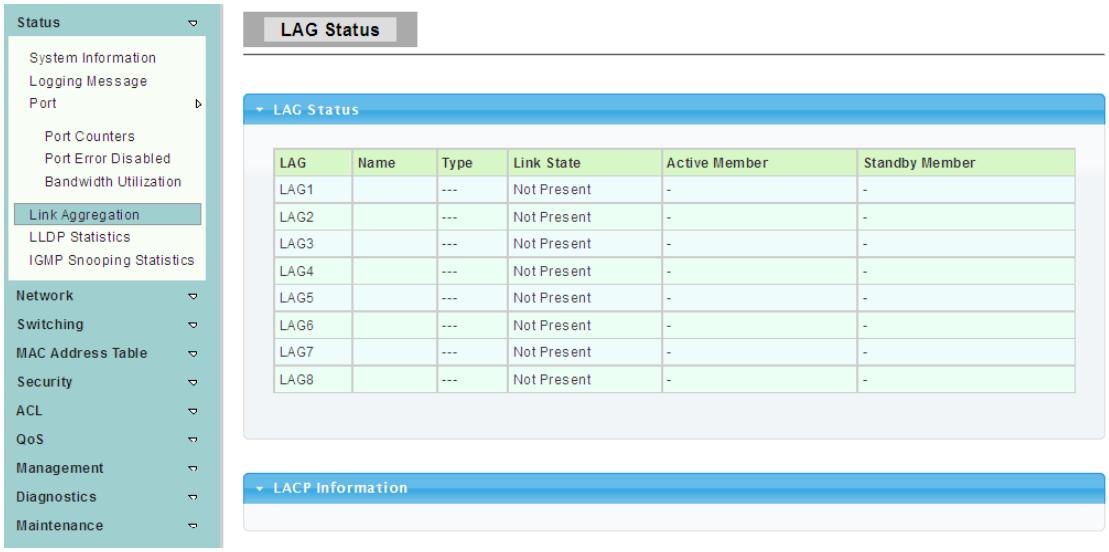
This page is used to visual display switch each port TX and RX bandwidth utilization.



4.2.4 Link Aggregation

To display the Link Aggregation web page, click **Status > Link Aggregation**

This page displays trunk information, report trunk situation, functional ports and alternative ports.

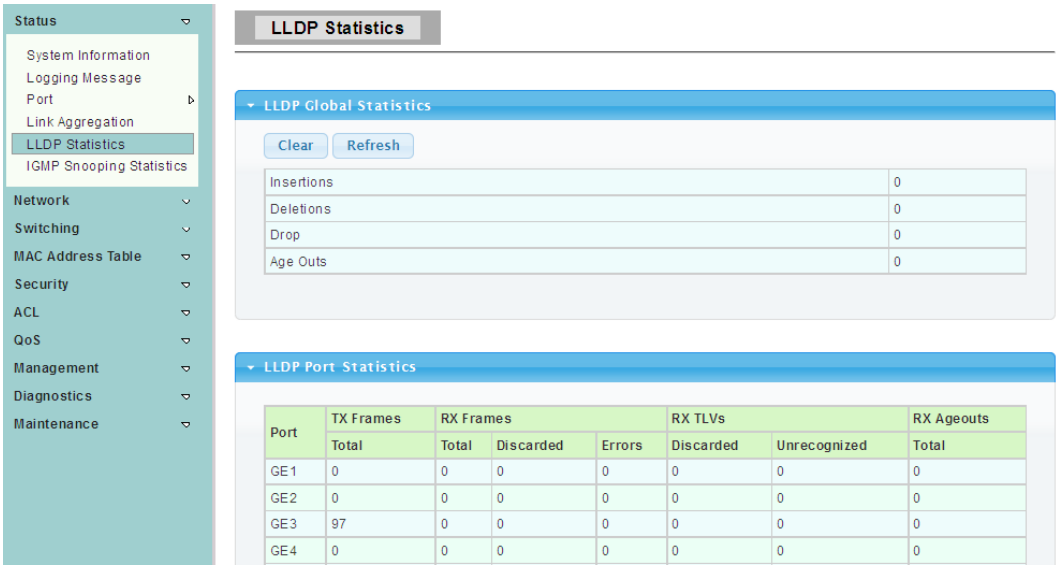


LAG: LAG ID.
Name: LAG Name.
Type: The type of the LAG group: static LAG or LACP LAG.

4.2.5 LLDP Statistics

To display the LLDP Statistics web page, click **Status > LLDP Statistics**

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



Insertions: The number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) has been inserted into tables associated

with the remote systems.

Deletions: The number of times the complete set of information advertised by MSAP has been deleted from tables associated with the remote systems.

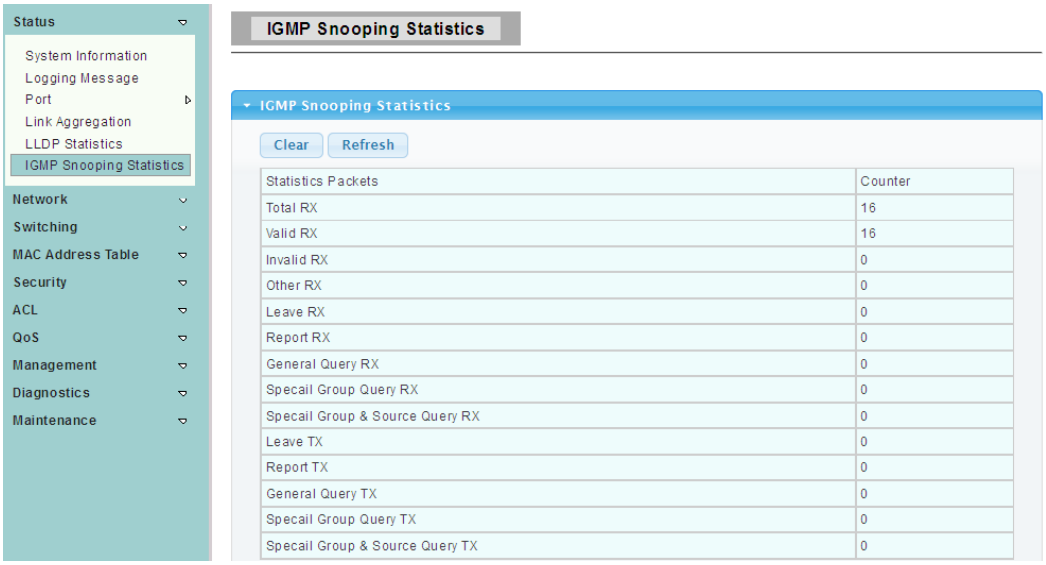
Drops: The number of times the complete set of information advertised by MSAP could not be entered into tables associated with the remote systems because of insufficient resources.

Age Outs: The number of times the complete set of information advertised by MSAP has been deleted from tables associated with the remote systems because the information timeliness interval has expired.

4.2.6 IGMP Snooping Statistics

To display the IGMP Snooping Statistics web page, click **Status > IGMP Snooping Statistics**

This page is used to display IGMP Snooping statistics information.



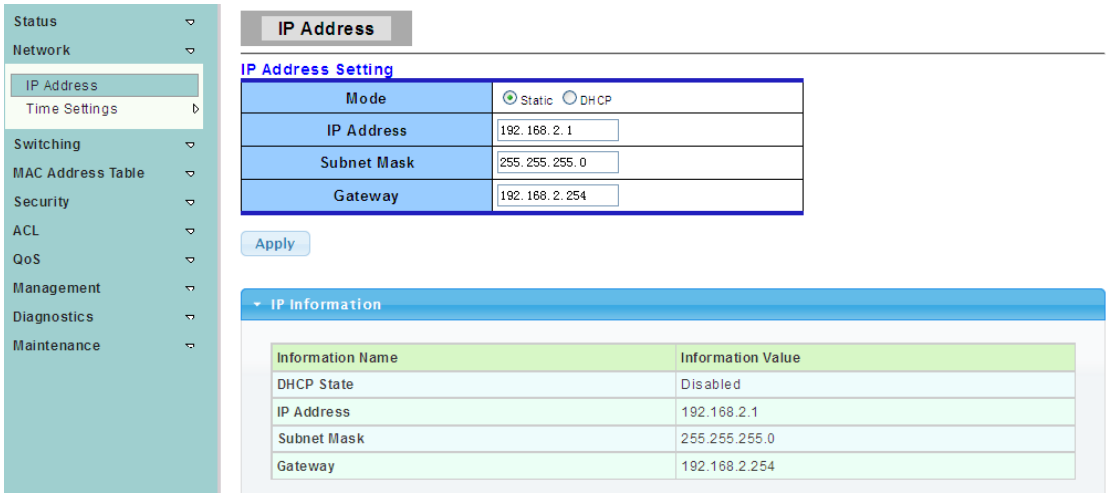
4.3 Network

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

4.3.1 IP Address

To display the IP Address web page, click **Network > IP Address**

This page allow user to edit IP address, Subnet Mask and Gateway.



Mode: Select the mode of network connection.

- Static: Enable static IP address.
- DHCP: Enable DHCP to obtain IP information from a DHCP server on the network.

IP Address: If static mode is enabled, enter IP address in this field.

Subnet Mask: If static mode is enabled, enter subnet mask in this field.

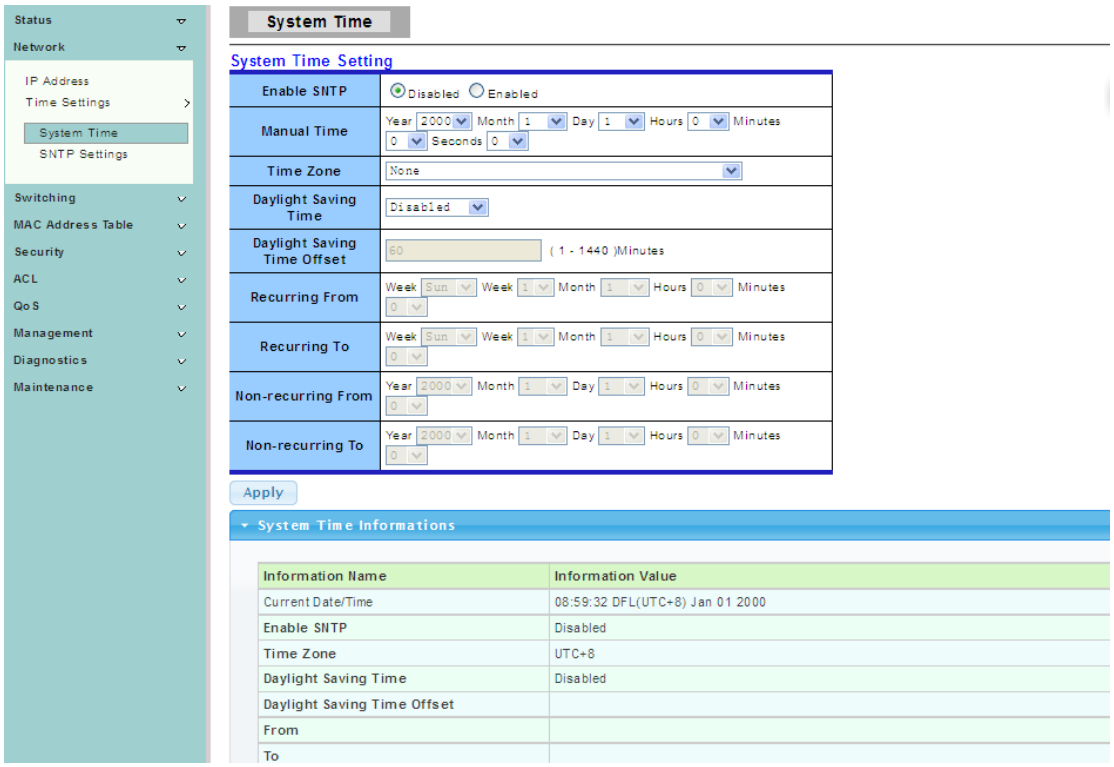
Gateway: If static mode is enabled, enter gateway address in this field.

4.3.2 Time Settings

4.3.2.1 System Time

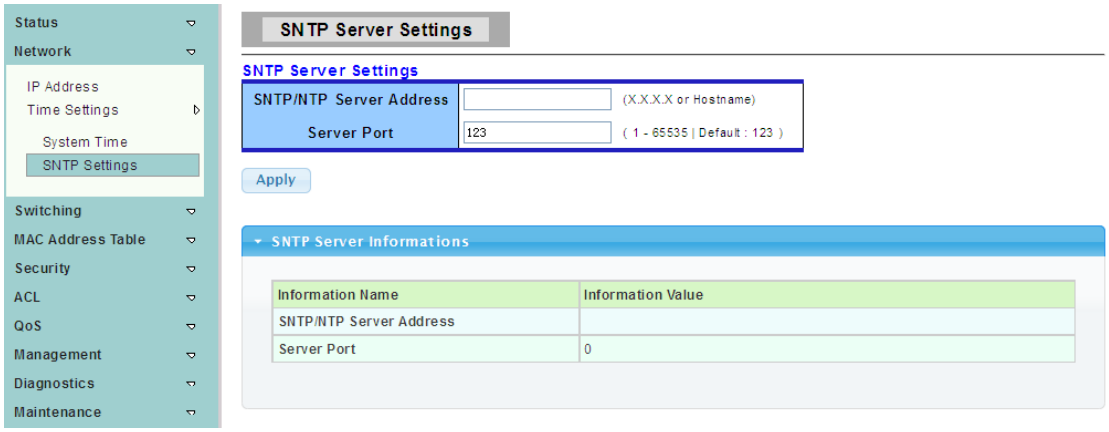
To display the System Time web page, click **Network > Time Settings > System Time**

System time setting, that is set time zone,time servicer, get the time and daylight saving time automatically.



4.3.2.2 SNTP Settings

To display the SNTP Settings web page, click **Network > Time Settings > SNTP Settings**



SNTP Server Address: The IP address of SNTP/NTP server.
Server Port: The Port Number of SNTP/NTP server.

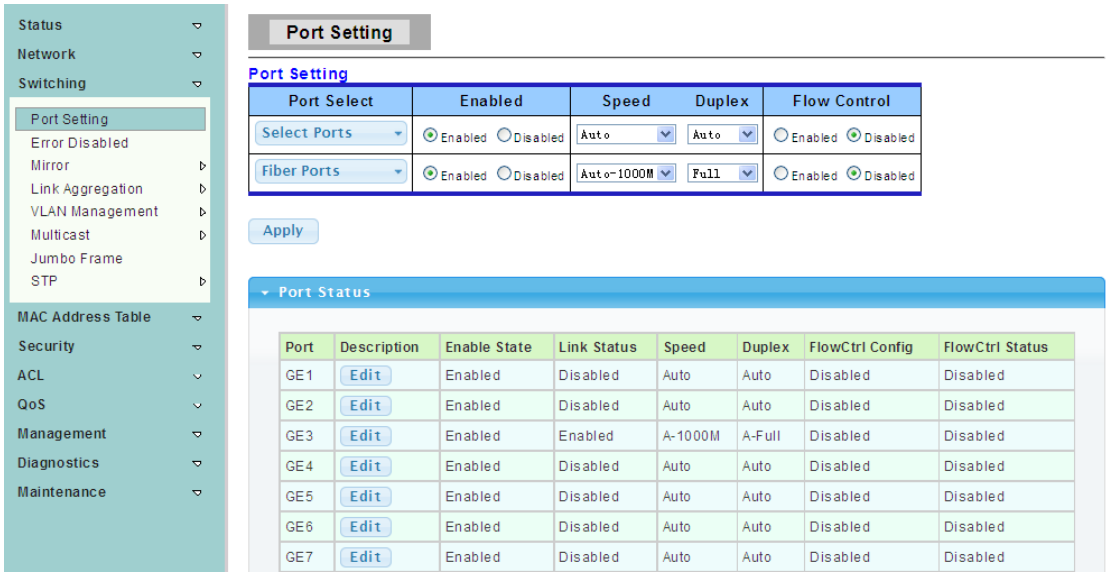
4.4 Switching

Use the Switching pages to configure settings for the switch ports, trunk, layer 2 protocols and other switch features.

4.4.1 Port Setting

To display the Port Setting web page, click **Switching > Port Setting**

Port Setting, that is set ports status, speed, duplex mode and flow control function.



Port Select: Select one or multiple ports to configure.
Enabled: Port admin state.

- Enabled: Enable the port.
- Disabled: Disable the port.

Speed: Port speed capabilities.

- Auto: Auto speed with all capabilities.
- Auto-10M: Auto speed with 10M ability only.
- Auto-100M: Auto speed with 100M ability only.
- Auto-1000M: Auto speed with 1000M ability only.
- Auto-10M/100M: Auto speed with 10M/100M abilities.
- 10M: Force speed with 10M ability.
- 100M: Force speed with 100M ability.
- 1000M: Force speed with 1000M ability.

Duplex: Port duplex capabilities.

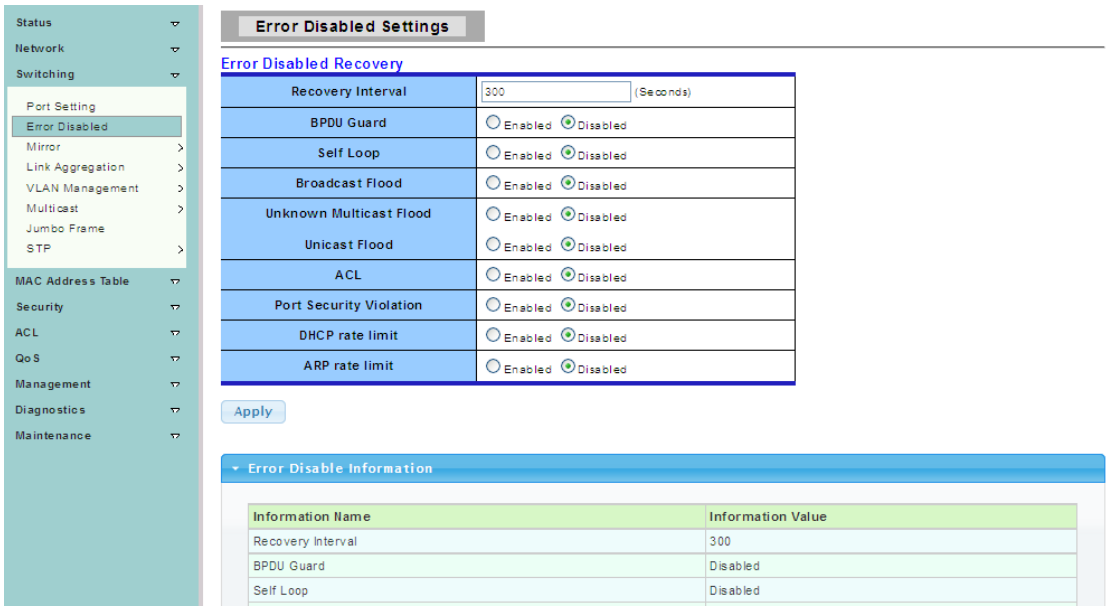
- Auto: Auto duplex with all capabilities.
- Full: Auto speed with full duplex ability only.
- Half: Auto speed with half duplex ability only.

Flow Control: Port flow control.

- Enable: Enable flow control ability.
- Disabled: Disable flow control ability.

4.4.2 Error Disabled

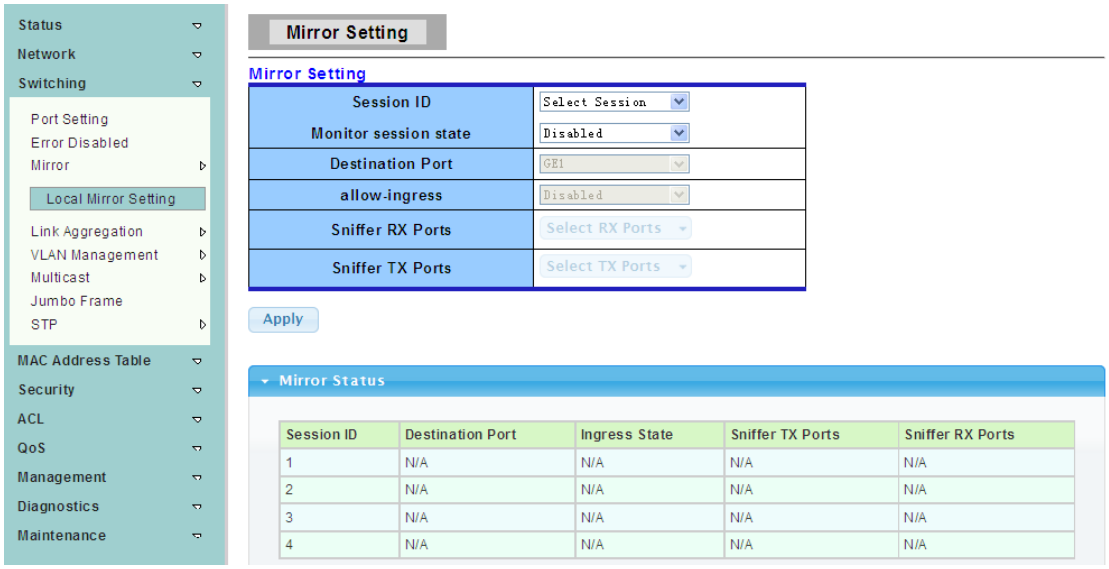
To display the Error Disabled web page, click **Switching > Error Disabled**



4.4.3 Mirror

To display the Local Mirror Setting web page, click **Switching > Mirror > Local Mirror Setting**

Port mirroring, that is copy the TX/RX data flow from the source port to the Destination Port, commonly used in port mirroring.



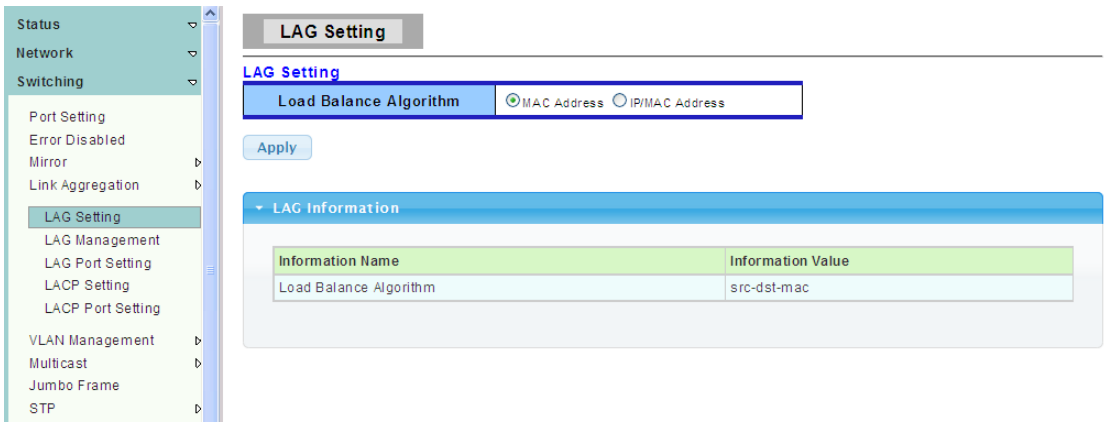
4.4.4 Link Aggregation

Link aggregation, that is multiple Ethernet ports together to form a logical port, it supports static allocation or LACP.

4.4.4.1 LAG Setting

To display the LAG Setting web page, click **Switching > Link Aggregation > LAG Setting**

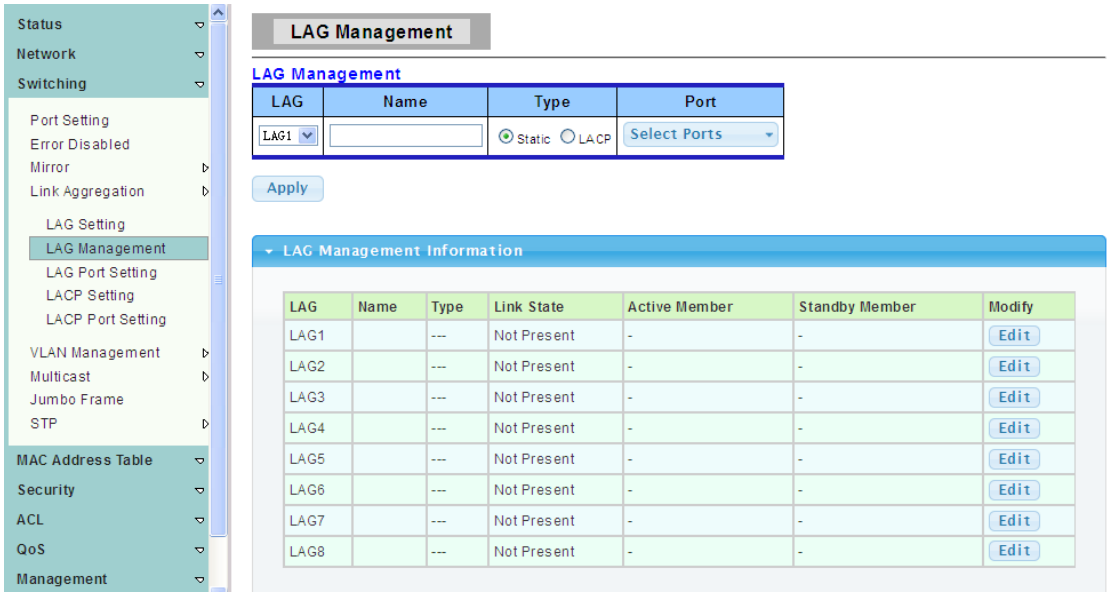
This page allow user to configure Ports aggregation rules that is depended on MAC Address or IP/MAC Address.



4.4.4.2 LAG Management

To display the LAG Management web page, click **Switching > Link Aggregation > LAG Management**

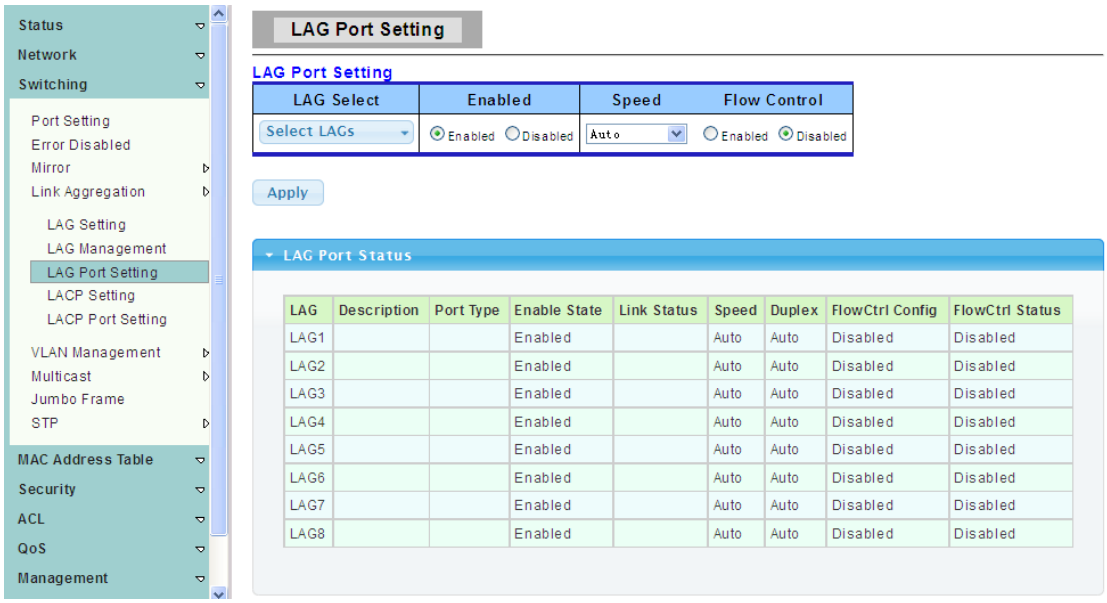
This page is used to create new LAG, configure ports aggregation type,and select member ports.



4.4.4.3 LAG Port Setting

To display the LAG Port setting web page, click **Switching > Link Aggregation > LAG Port Setting**

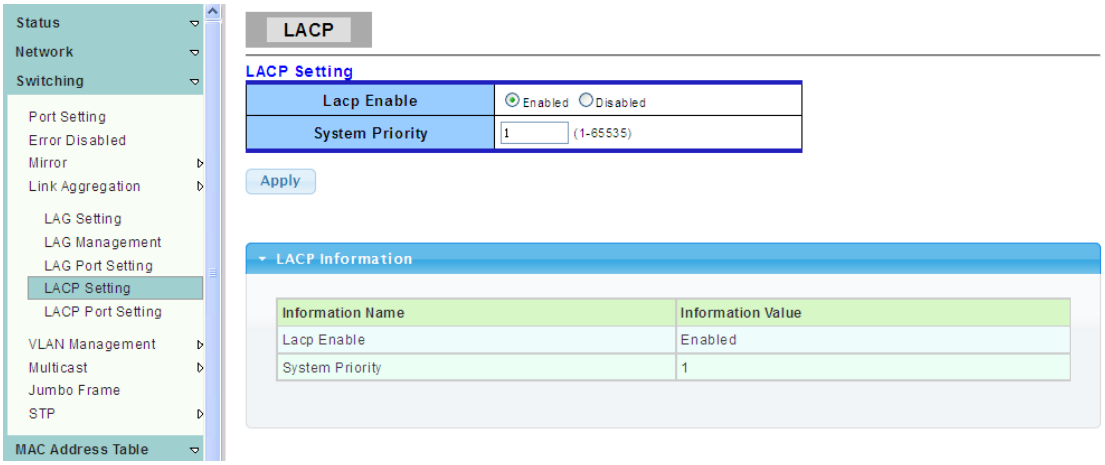
This page is used to set LAG status, speed and flow control function.



4.4.4.4 LACP Setting

To display the LACP Setting web page, click **Switching > Link Aggregation > LACP Setting**

This page is used to configure the system Priority of LACP.

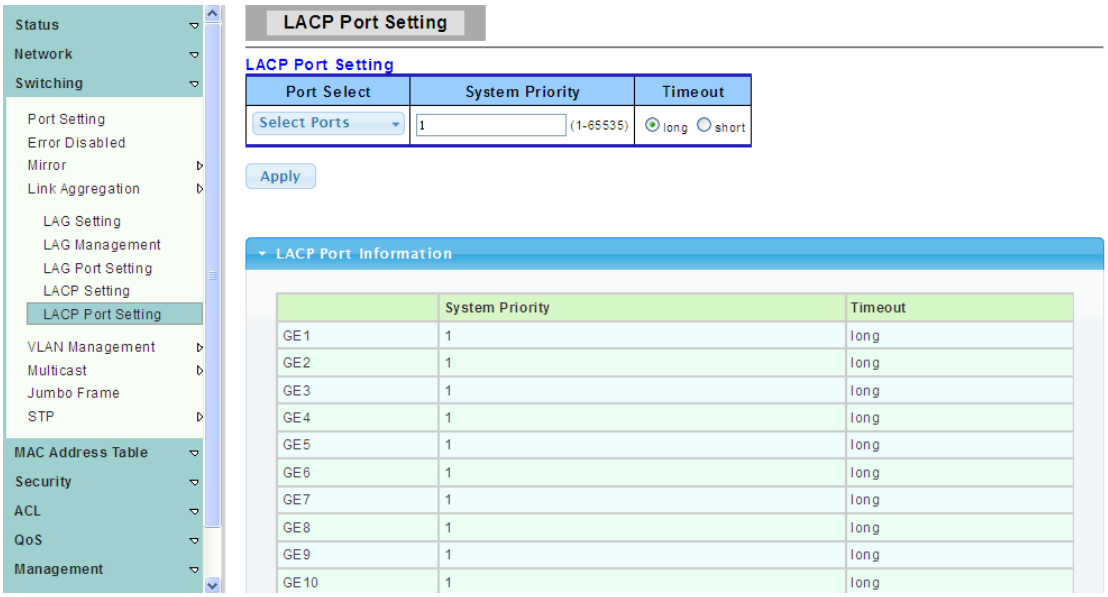


System Priority: Configure the system priority of LACP. This decides the system priority field in LACPDU.

4.4.4.5 LACP Port Setting

To display the LACP Port Setting web page, click **Switching > Link Aggregation > LACP Port Setting**

This page is used to set LACP member ports.

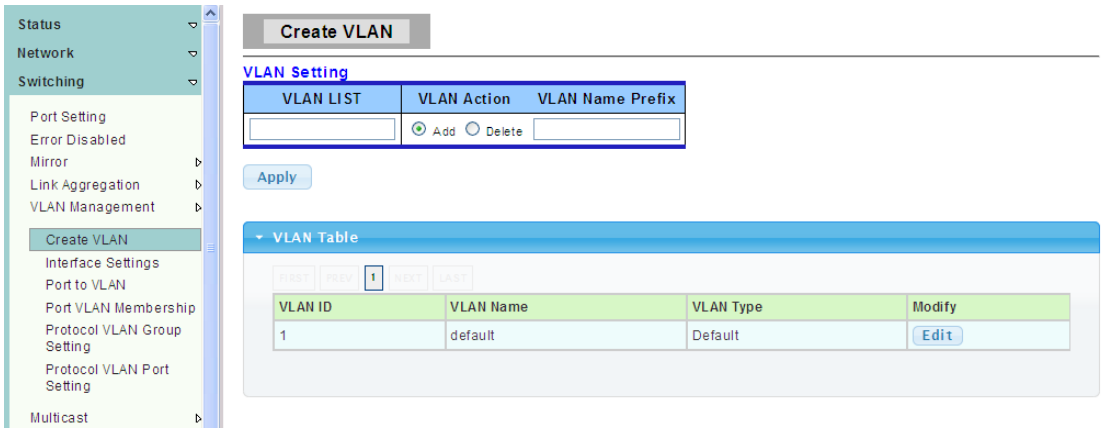


4.4.5 VLAN Management

4.4.5.1 Create VLAN

To display the Create VLAN web page, click **Switching > VLAN Management > Create VLAN**

This page allow user to add, delete or edit VLAN settings.

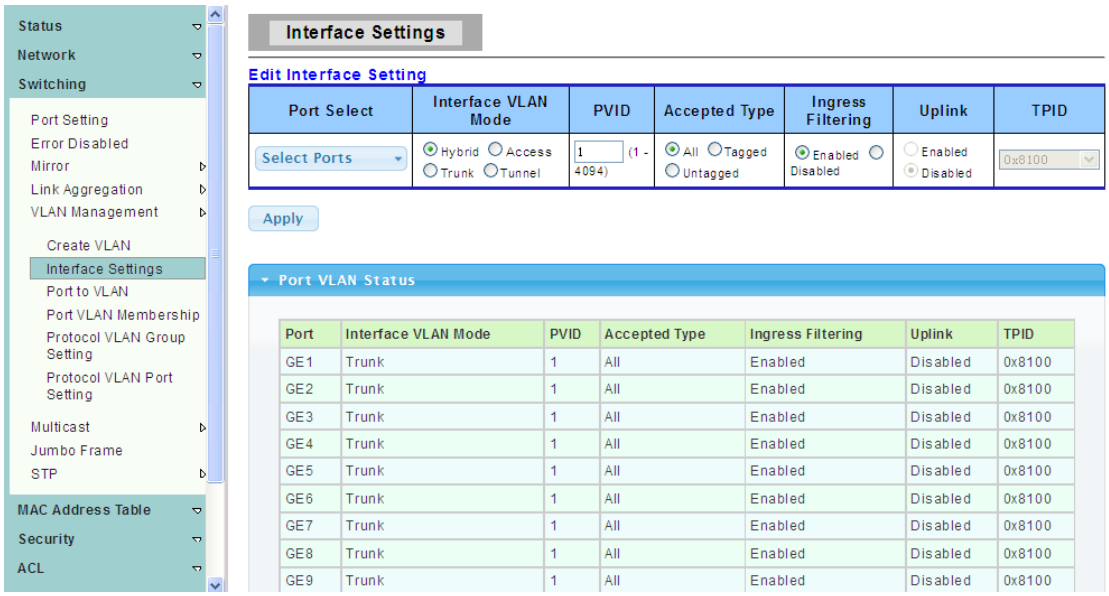


VLAN LIST: VLAN LIST for the new VLAN.
VLAN Action: Add or delete VLAN.
VLAN Name Prefix: VLAN Name Prefix for the new VLAN.

4.4.5.2 Interface Settings

To display the VLAN Interface Settings web page, **click Switching > VLAN Management > Interface Settings**

This page allows the user to set the port type of vlan.



Port Select : Select one or multiple ports to configure.
Interface VLAN Mode: VLAN port mode

- Hybrid: Port hybrid model.
- Access: Port hybrid model.
- Trunk: Port hybrid model.
- Tunnel: Port hybrid model.

PVID: VLAN ID for the selected ports.
Accepted Type: Port accepted type.

- All: Accept tagged and untagged frames.
- Tag Only: Only accept tagged frame.

- Untag Only: Only accept untagged frame.

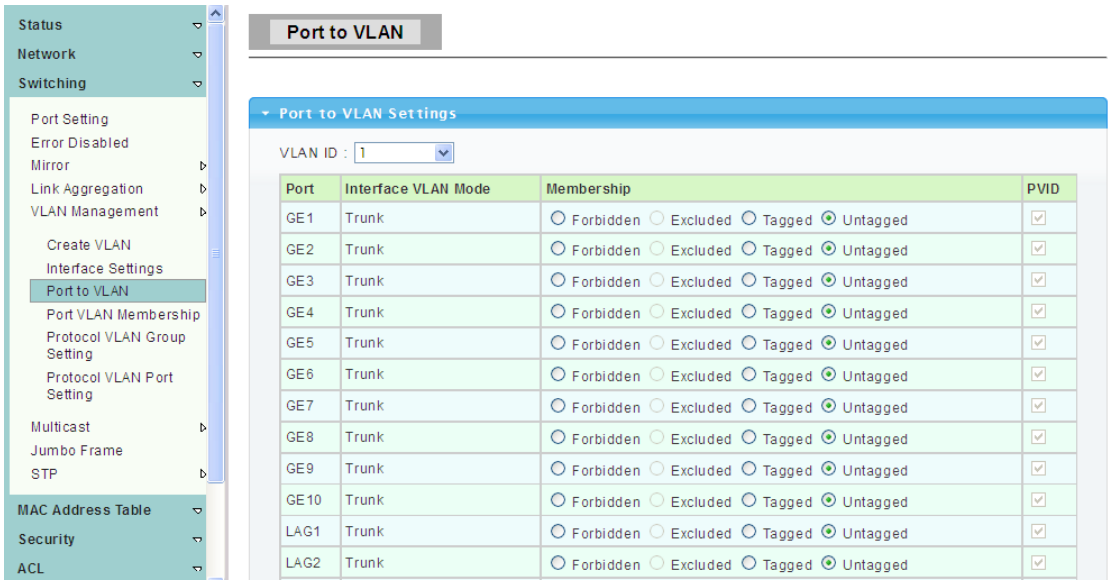
Ingress Filtering: Choose filter port open and close.

Uplink: Select port Uplink open or close.

4.4.5.3 Port to VLAN

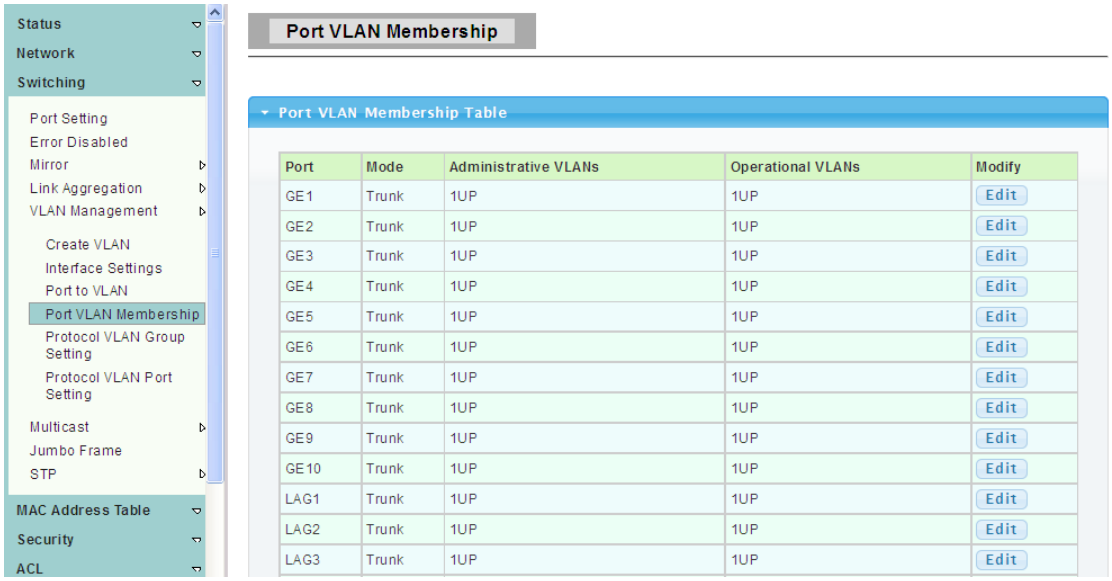
To display the Port to VLAN web page, click **Switching > VLAN Management > Port to VLAN**

Make port add to VLAN, select the port's different behaviors when it works under the VLAN.



4.4.5.4 Port VLAN Membership

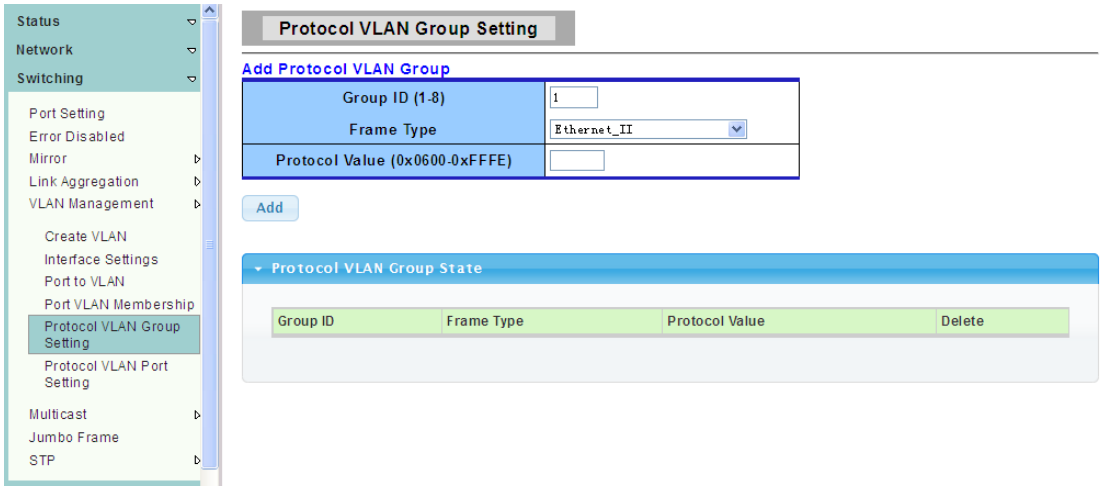
To display the Port VLAN Membership web page, click **Switching > VLAN Management > Port VLAN Membership**



4.4.5.5 Protocol VLAN Group Setting

To display Protocol VLAN Group Setting web page, click **Switching > VLAN > Protocol VLAN Group Setting**

The VLAN group setting, that is sets the same type message as a group and transmit it in the specific VLAN.



Group ID(1-8) : Enter an ID number of the group, between 1 and 8.

Group Name: This is used to identify the new Protocol VLAN group.Type an alphanumeric string of up to 16 characters.

Frame Type : This function maps packets to protocol-defined VLAN by examining the type octet within the packet header to discover the type of protocol associated with it.

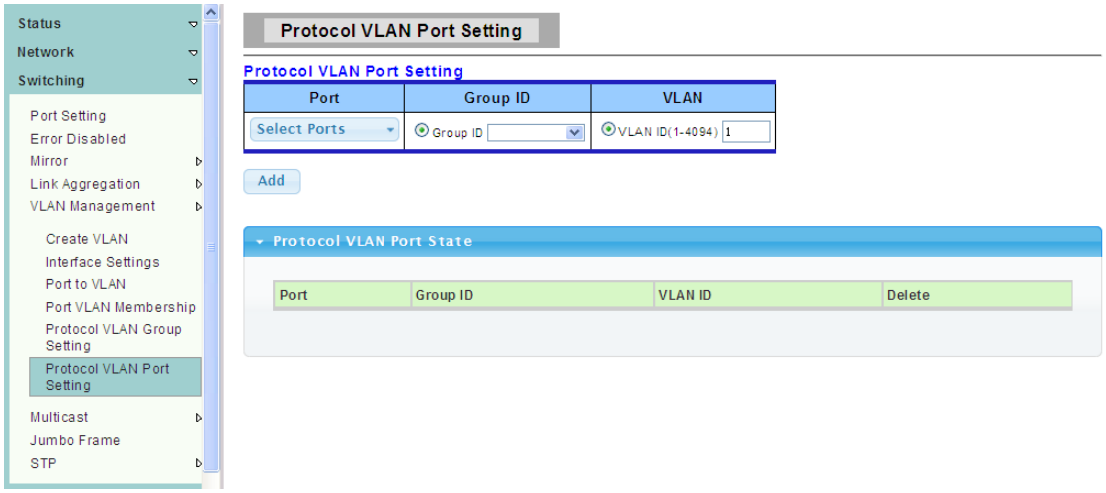
- Ethernet_II: packet type is Ethernet version 2.
- IEEE802.3_LLC_Other: packet type is 802.3 packet with LLC other header.
- RFC_1042: packet type is RFC 1042 packet.

Protocol Value (0x0600-0xFFFE): Enter the Ether type of the target protocol.

4.4.5.6 Protocol VLAN Port Setting

To display the Protocol VLAN Port Setting web page, click **Switching > VLAN > Protocol VLAN Port Setting**

This page is used to divide the port into groups and map it to the VLAN.



Port: Select the specified ports you wish to configure by selecting the port in this list.

Group: Click the corresponding radio button to select a previously configured Group ID or Group Name.

VLAN : Click the corresponding radio button to select a previously configured VLAN ID or VLAN Name.

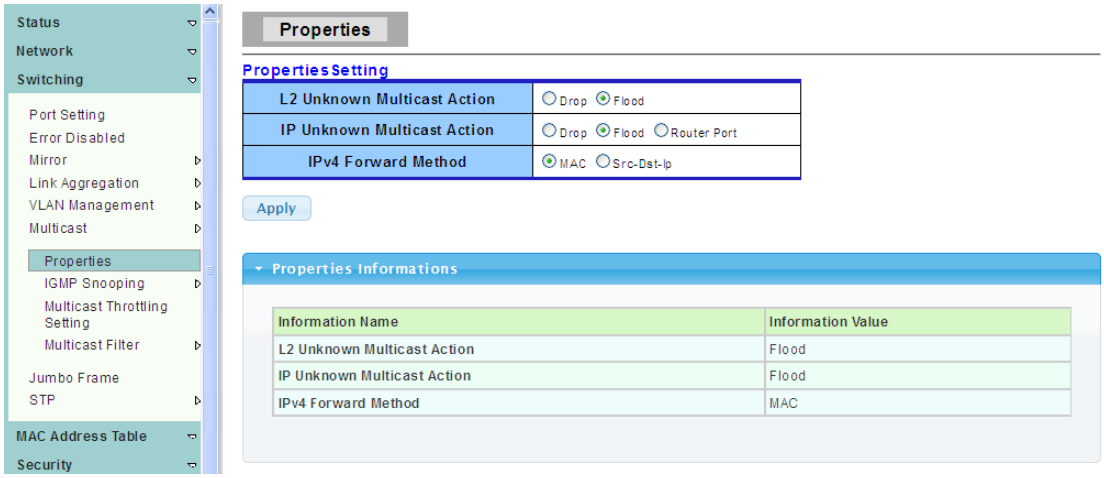
4.4.6 Multicast

IP multicasting is a bandwidth-conserving technology that reduces traffic because it simultaneously delivers a single stream of information to thousands of corporate recipients and homes. Applications that take advantage of multicast include video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news.

4.4.6.1 Properties

To display the Properties web page, click **Switching > Multicast > Properties**

This page is used to Set message behavior and iPv4 message forwarding rules.

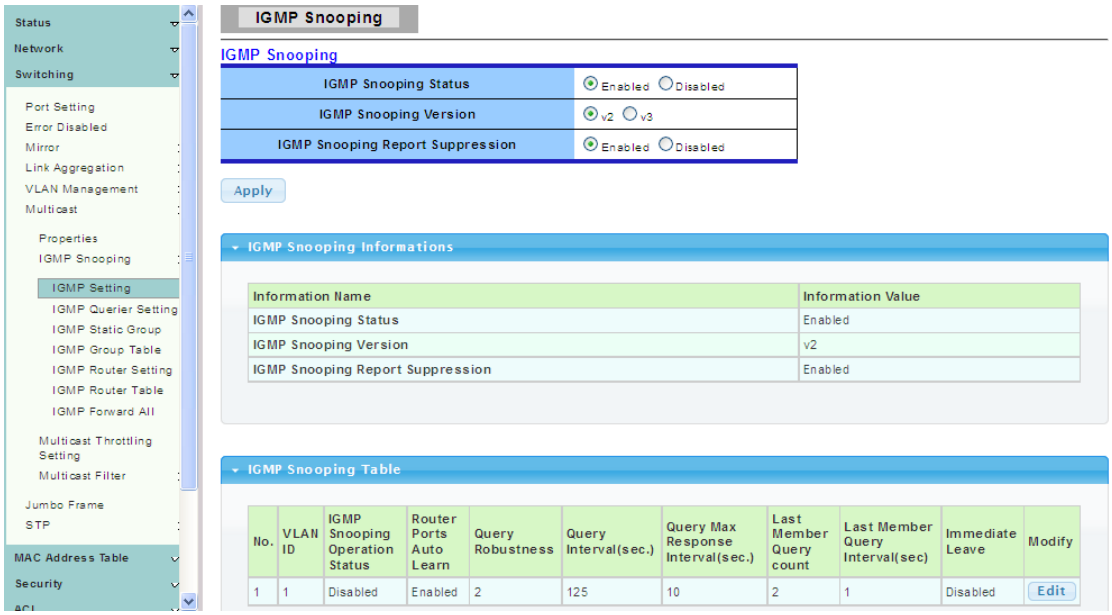


4.4.6.2 IGMP Snooping

IGMP snooping, as implied by the name, is a feature that allows the switch to "listen in" on the IGMP conversation between hosts and routers.

1. IGMP Setting

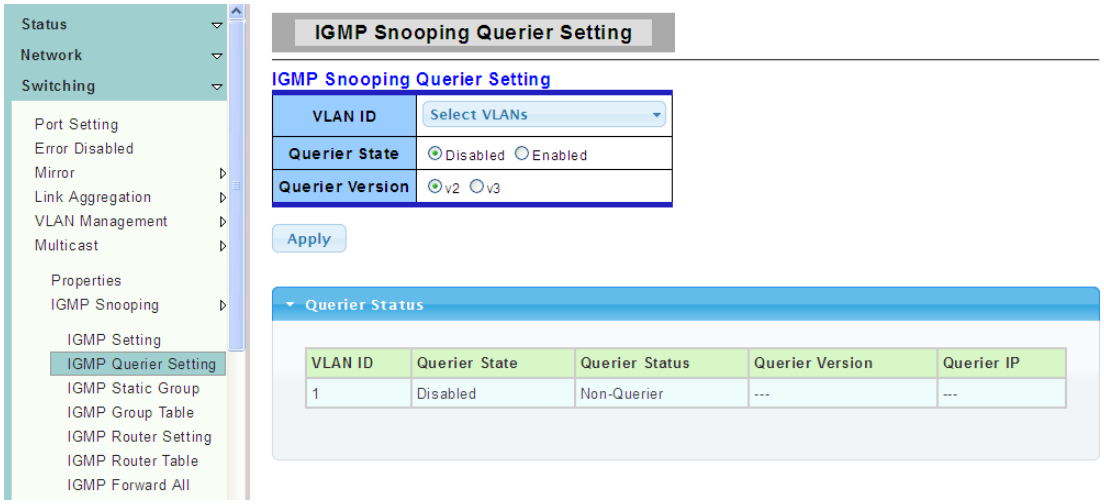
To display the IGMP Setting web page, click **Switching > Multicast > IGMP Snooping > IGMP Setting**



IGMP Snooping: Select the IGMP Snooping enable or disable.
IGMP Snooping Version: Select the IGMP Snooping Version, IGMPv2 or IGMPv3.
IGMP Snooping Report Suppression: Select the IGMP Snooping Report Suppression enable or disable.

2. IGMP Querier Setting

To display the IGMP Snooping Querier Setting web page, click **Switching > Multicast > IGMP Snooping > IGMP Querier Setting**



VLAN ID: Select the VLANs to configure.
Querier State: Set the enabling status of IGMP Querier Election on the chose VLANs.

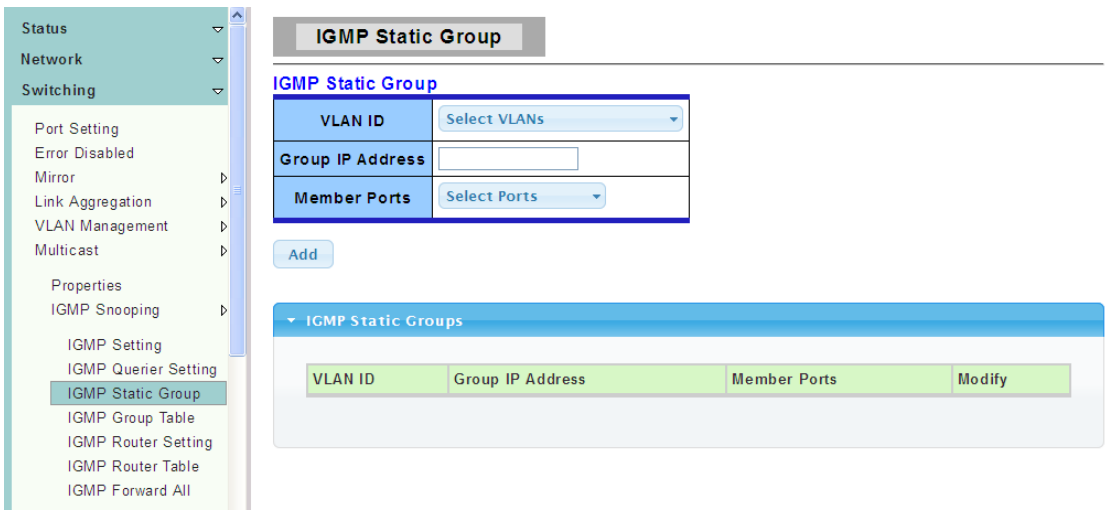
- Enable: Enable IGMP Querier Election.
- Disable: Disable IGMP Querier Election.

Version: Select the Querier Version, IGMPv2 or IGMPv3

3. IGMP Static Group

To display the IGMP Static Setting web page, click **Switching > Multicast > IGMP Snooping > IGMP Static Group**

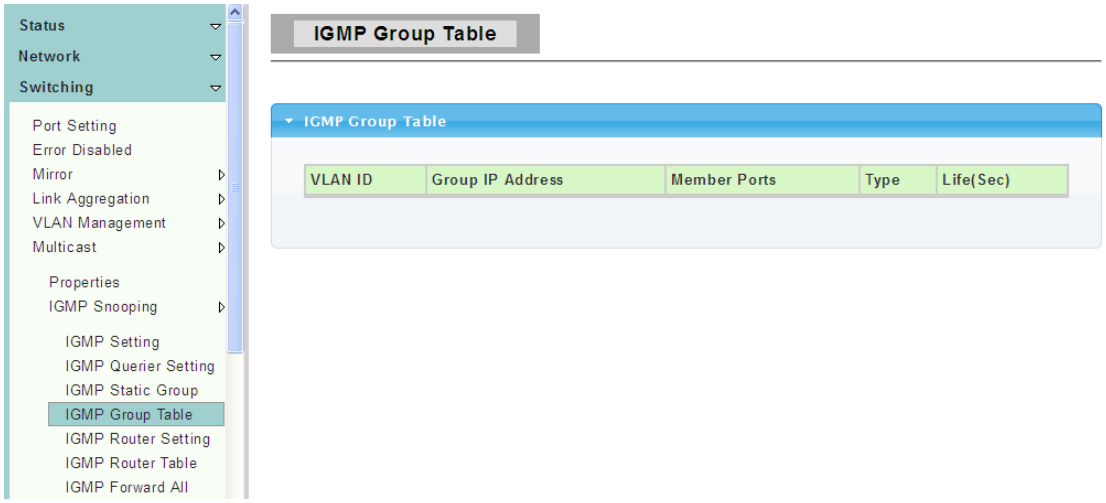
This page is used to configure specified ports as static member ports.



4. IGMP Group Table

To display the IGMP Group Table web page, click **Switching > Multicast > IGMP Snooping > IGMP Group Table**

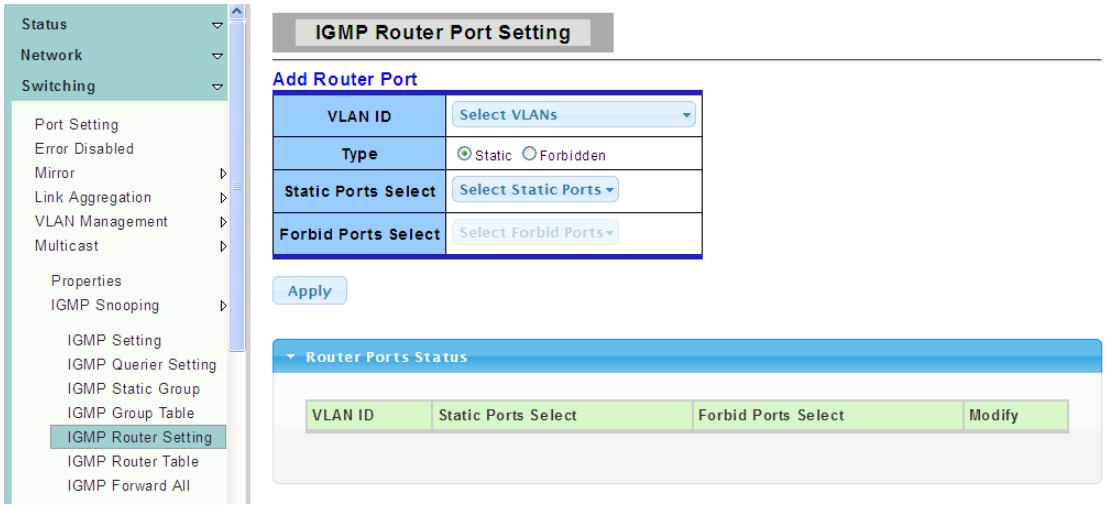
This page is used to display IGMP Group Table statistics information.



5. IGMP Router Setting

To display the IGMP Router Port Setting web page, click **Switching > Multicast > IGMP Snooping > IGMP Router Setting**

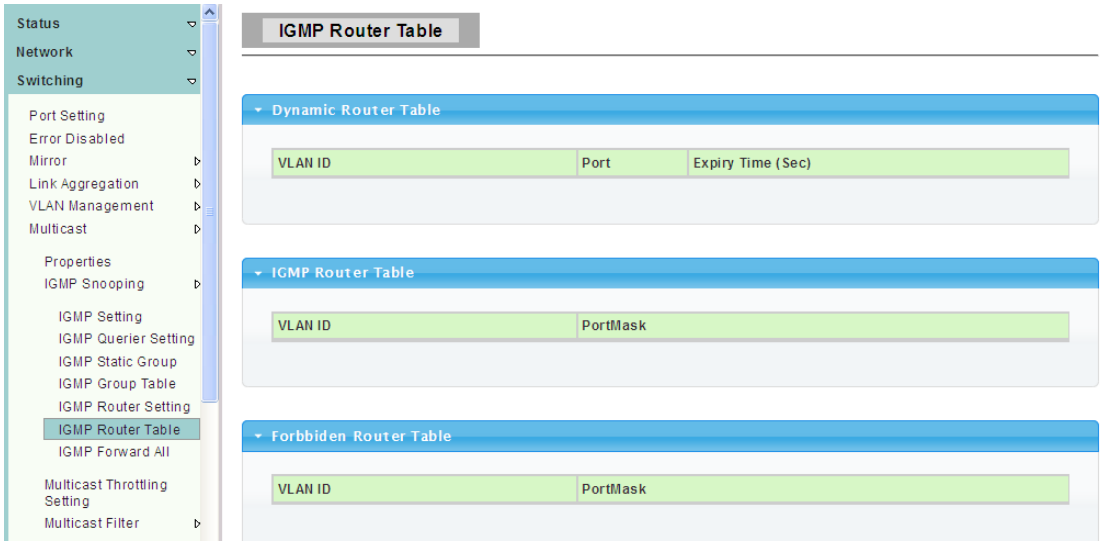
This page is used to configure specified ports as static route ports.



6. IGMP Router Table

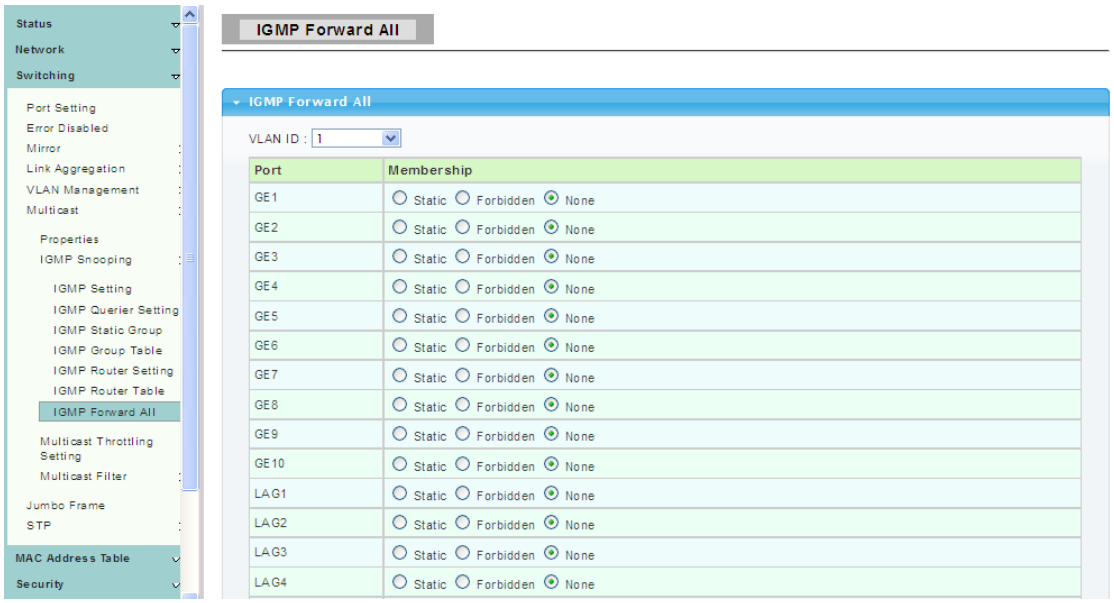
To display the IGMP Router Table web page, click **Switching > Multicast > IGMP Snooping > IGMP Router Table**

This page is used to display IGMP Router Table statistics information.



7. IGMP Forward All

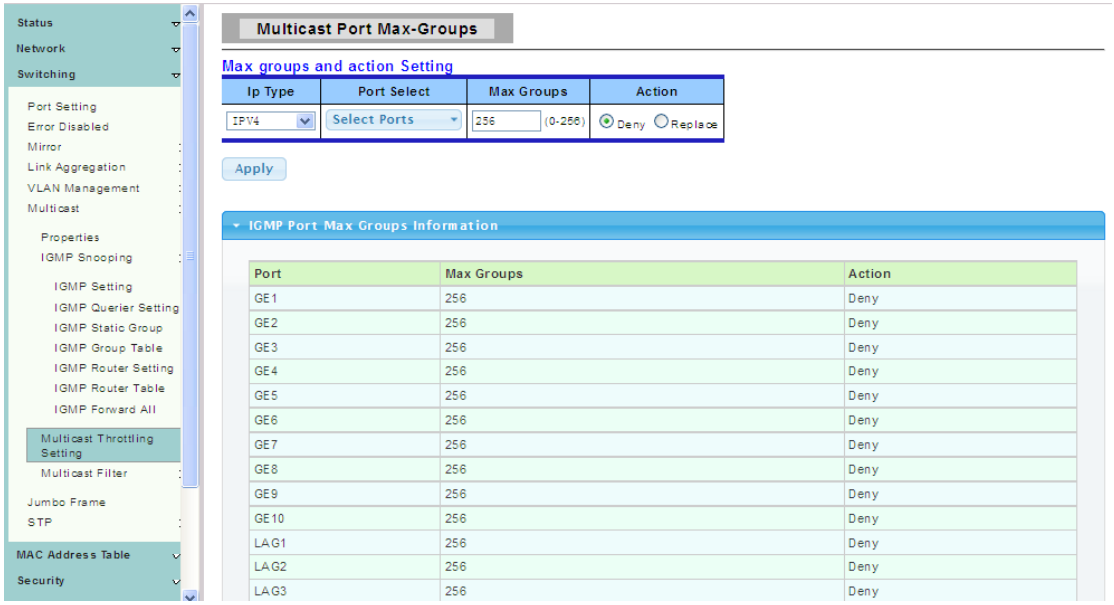
To display the IGMP Forward All web page, click **Switching > Multicast > IGMP Snooping > IGMP Forward All**



4.4.6.3 Multicast Throtting Setting

To display the Multicast Port Max-Groups web page, click **Switching > Multicast >Multicast Throtting Setting**

This page is used to Limit the port can join one of the biggest Multicast instance.

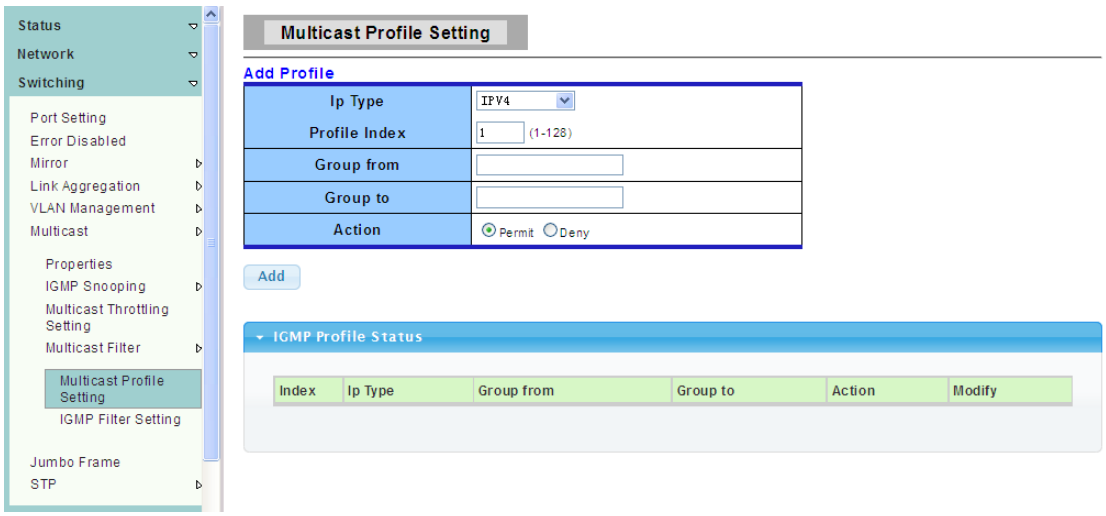


4.4.6.4 Multicast Filter

This page allow user to create filter instance.

1. Multicast Profile Setting

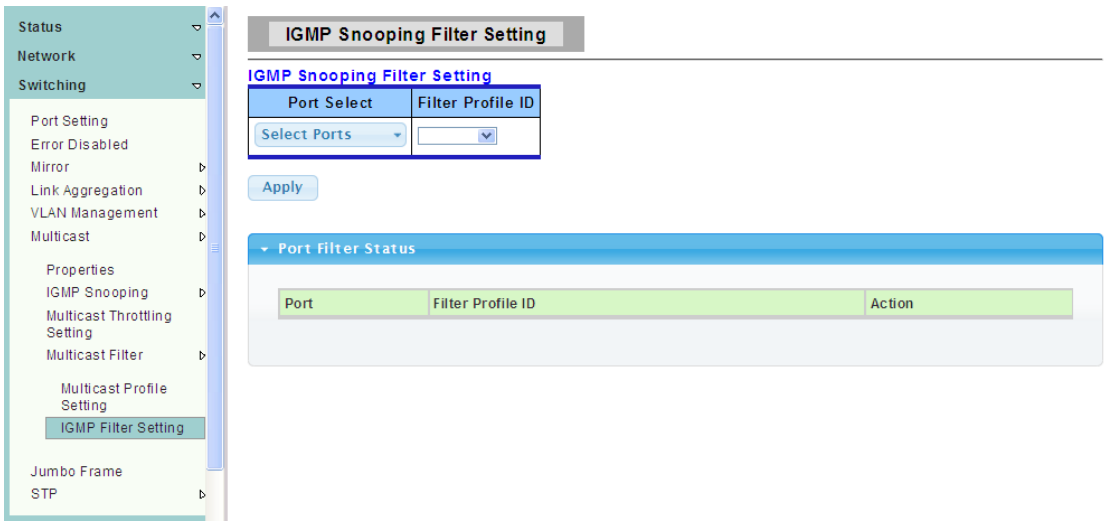
To display the Multicast Profile Setting web page, click **Switching > Multicast >Multicast Filter > Multicast Profile Setting**



2. IGMP Filter Setting

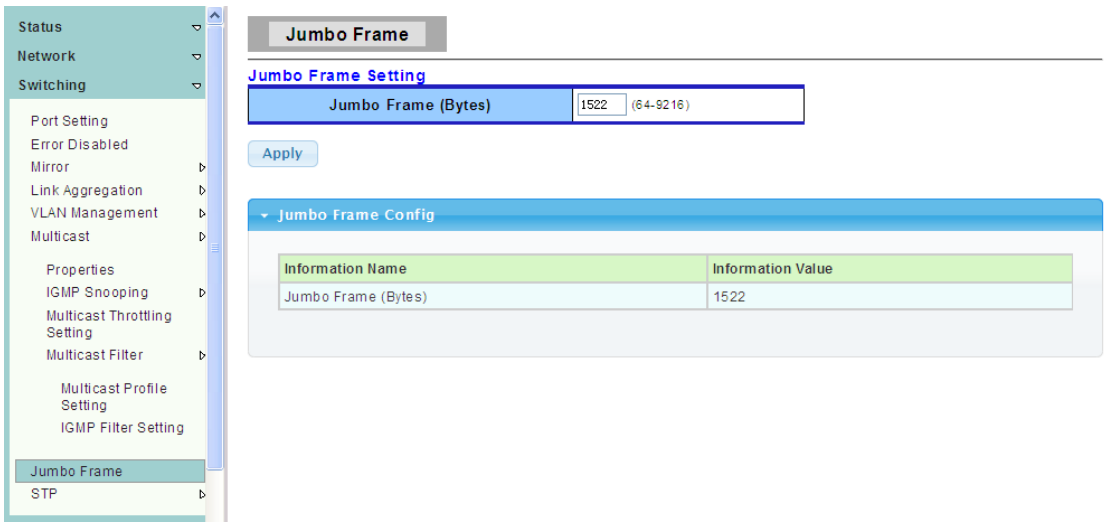
To display IGMP Snooping Filter Setting web page, click **Switching > Multicast > Multicast Filter > IGMP Filter Setting**

This page is used to Filter on the port to bind to that instance.



4.4.7 Jumbo Frame

To display the Jumbo Frame web page, click **Switching > Jumbo Frame**



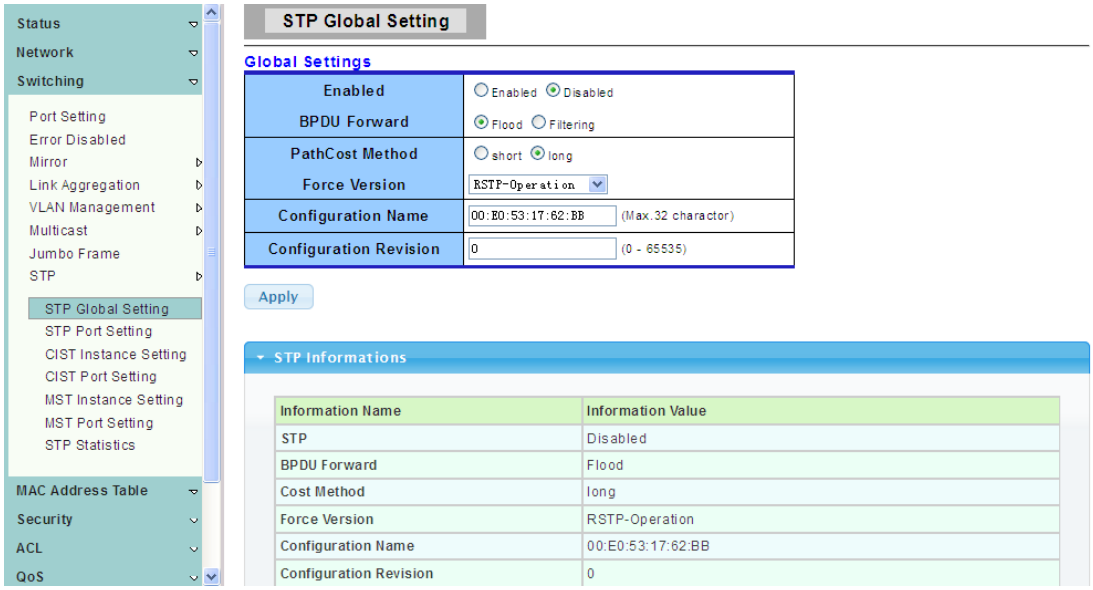
Jumbo Frame: Jumbo frame size. The valid range is 64 bytes – 9216 bytes.

4.4.8 STP

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

4.4.8.1 STP Global Setting

To display the STP Global Setting web page, click **Switching > STP > STP Global Setting**



Enabled: Set the STP status to be enabled/disabled on the Switch.

BPDU Forward: Choose BPDU packets is a flood or filtering

Path Cost Method: Choose the path overhead is short or long

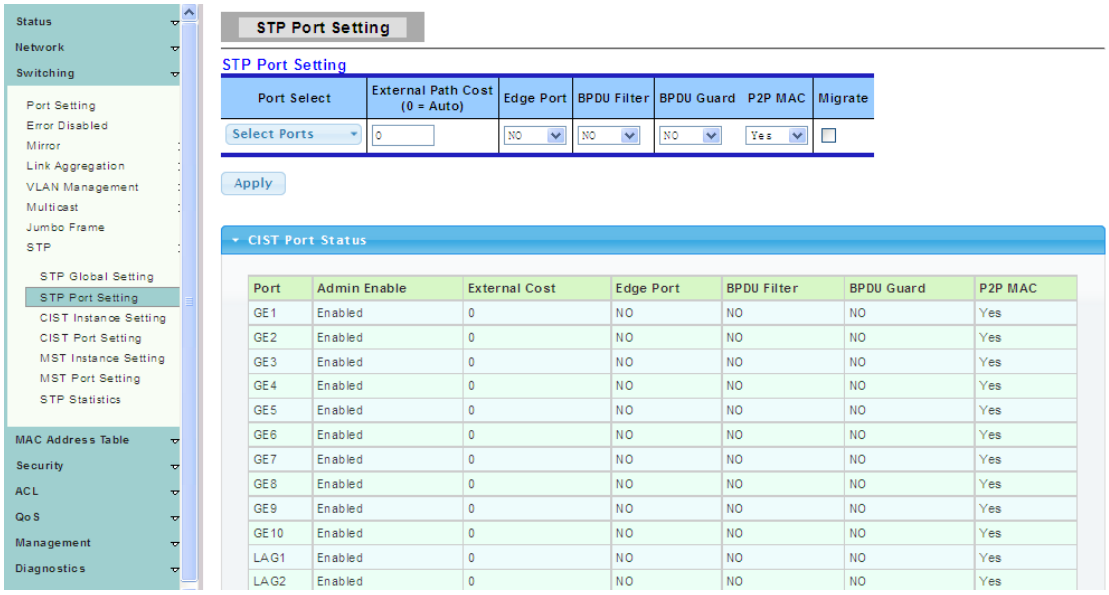
Force Version: Select the operating mode of STP.

- STP-Compatible: 802.1D STP operation.
- RSTP-Operation: 802.1w operation.
- MSTP-Operation: 802.1s operation.

Configuration Revision: Set the Revision of the Configuration Identification. (Range:0-65535).

4.4.8.2 STP Port Setting

To display the STP Port Setting web page, click **Switching > STP > STP Port Setting**



Port Select: Select the port list to specify which ports should apply this setting.

External Path: Cost Set the port's contribution, when it is the Root Port, to the Root Path Cost for the Bridge. (0 means `Auto`).

Edge Port: Set the edge port configuration.

- No: Force to false state (as link to a bridge).
- Yes: Force to true state (as link to a host).

BPDU Filter: Set the BPDU Filter configuration.

- No: Disable BPDU filter function.
- Yes: Enable BPDU filter function.

To avoid transmitting BPDU from the specified ports.

BPDU Guard: Set the BPDU Guard configuration.

- No: Disable BPDU guard function.
- Yes: Enable BPDU filter function.

To drop directly the received BPDU from the specified ports.

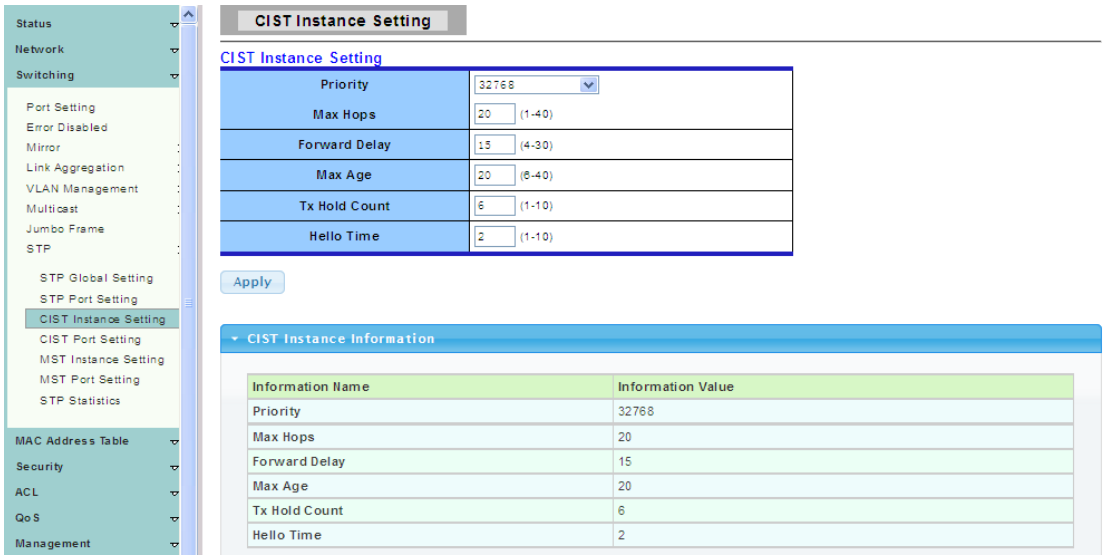
P2P MAC: Set the Point-to-Point port configuration.

- No: Force to false state.
- Yes: Force to true state.

Migrate: Force to try to use the new MST/RST BPDUs, and hence to test the hypothesis that all legacy systems that do not understand the new BPDU formats have been removed from the LAN segment on the port(s).

4.4.8.3 CIST Instance Setting

To display the CIST Instance Setting web page, click **Switching > STP > CIST Instance Setting**



Priority: Set the Bridge Priority in the specified CIST instance.

Max Hops: Set the value of the maximum number of hops in the region.

Forward Delay: Set the delay time an interface takes to converge from blocking state to forwarding state.

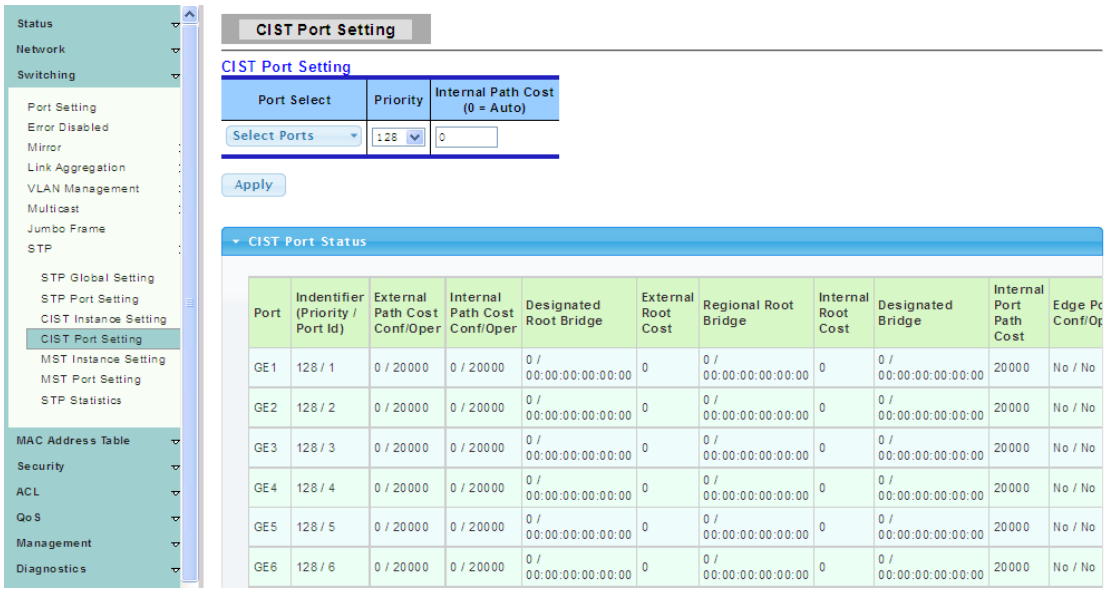
Max Age: Set the time any switch should wait before trying to change the STP topology after unhearing Hello BPDU.

Tx Hold Count: Set the Transmit Hold Count used to limit BPDIU transmission rate.

Hello Time: Set the interval between periodic transmissions of BPDU by Designated Ports.

4.4.8.4 CIST Port Setting

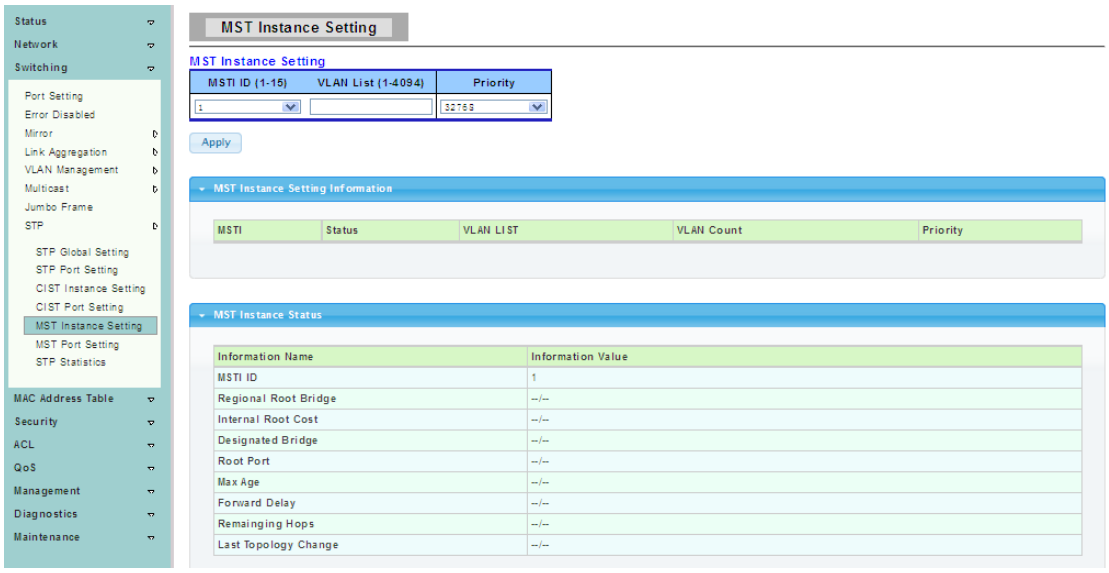
To display the CIST Port Setting web page, click **Switching > STP > CIST Port Setting**



Port Select : Select the port list to specify which ports should apply this setting.
Priority: Set the Port Priority to the selected ports in the specified CIST instance.
Internal Path Cost: Set the Internal Path Cost to the selected ports in the specified CIST instance. (0 means `Auto`)

4.4.8.5 MST Instance Setting

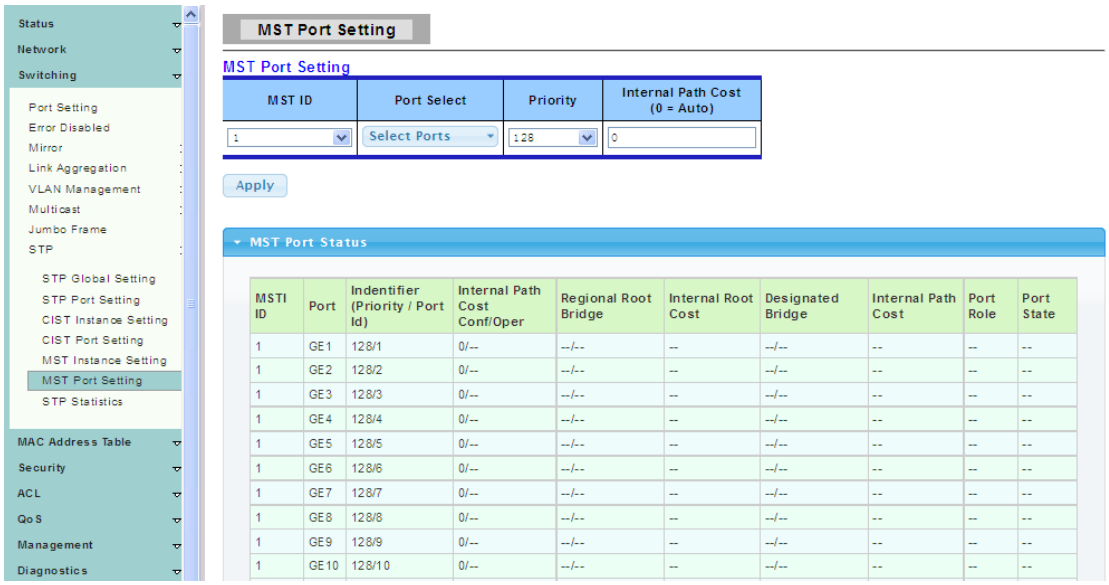
To display the MST Instance Setting web page, click **Switching > STP > MST Instance Setting**



MSTI ID: Set the MSTI ID to specified the MST instance.
VLAN List: Set the VLAN List.
Priority: Set the Bridge Priority in the specified MST instance.

4.4.8.6 MST Port Setting

To display the MST Port Setting web page, click **Switching > STP > MST Port Setting**



MST ID: Set the MSTI ID to specify MST instance.

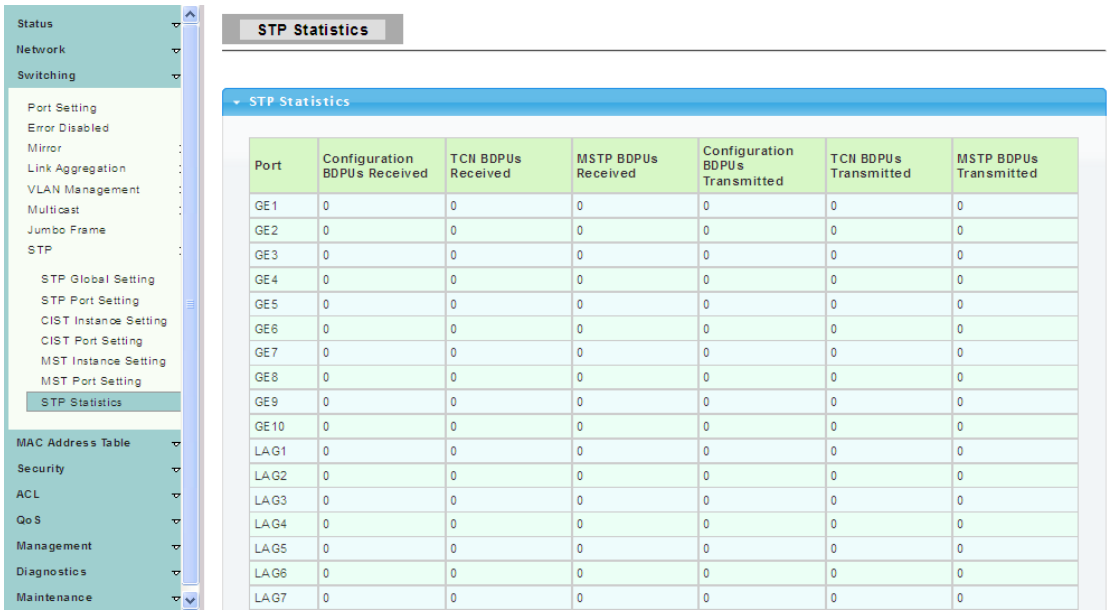
Port Select : Select the port list to specify which ports should apply this setting.

Priority: Set the Port Priority to the selected ports in the specified MST instance.

Internal Path Cost: Set the Internal Path Cost tot he selected ports in the specified MST instance. (0 means `Auto`)

4.4.8.7 STP Statistics

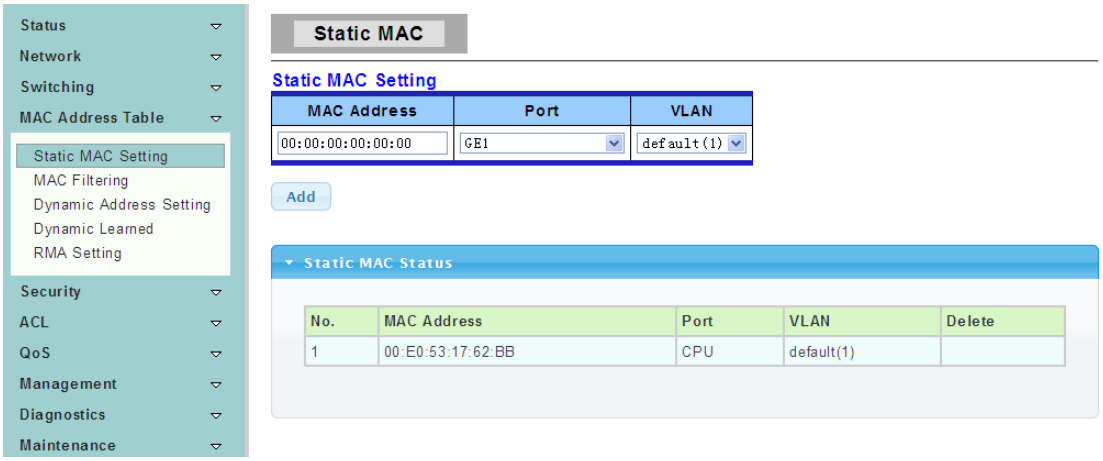
To display the STP Statistics web page, click **Switching > STP > STP Statistics**



4.5 Mac Address Table

4.5.1 Static Mac Setting

To display the Static Mac web page, click **Mac Address Table > Static Mac Setting**



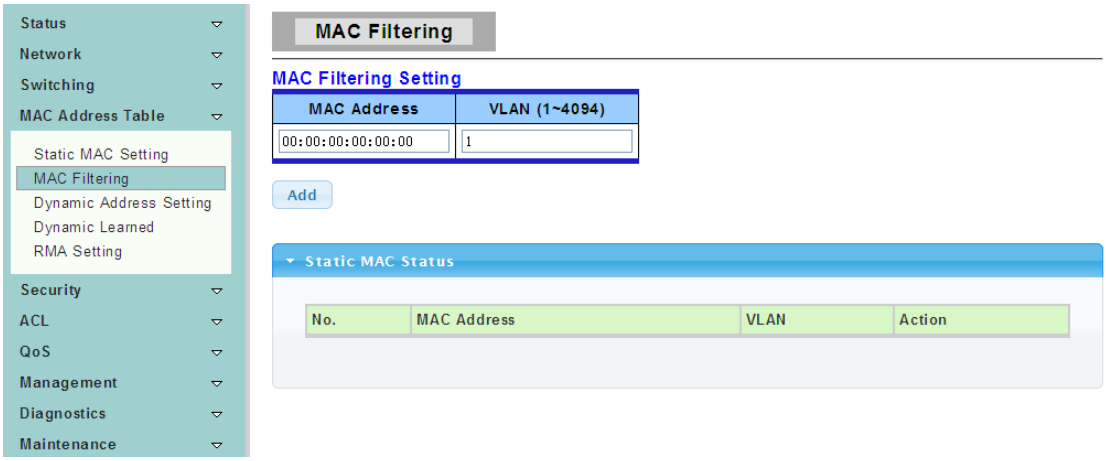
MAC Address: The MAC address to which packets will be statically forwarded. If Type is unicast, enter unicast MAC address in this field; If Type is multicast, enter multicast MAC address in this field.

Port: If Type is unicast, select the port number of the MAC entry; If Type is multicast, select the port list of the MAC entry.

VLAN: The VLAN ID number of the VLAN on which the above MAC address resides.

4.5.2 MAC Filtering

To display the MAC Filtering web page, click **Mac Address Table > MAC Filtering**



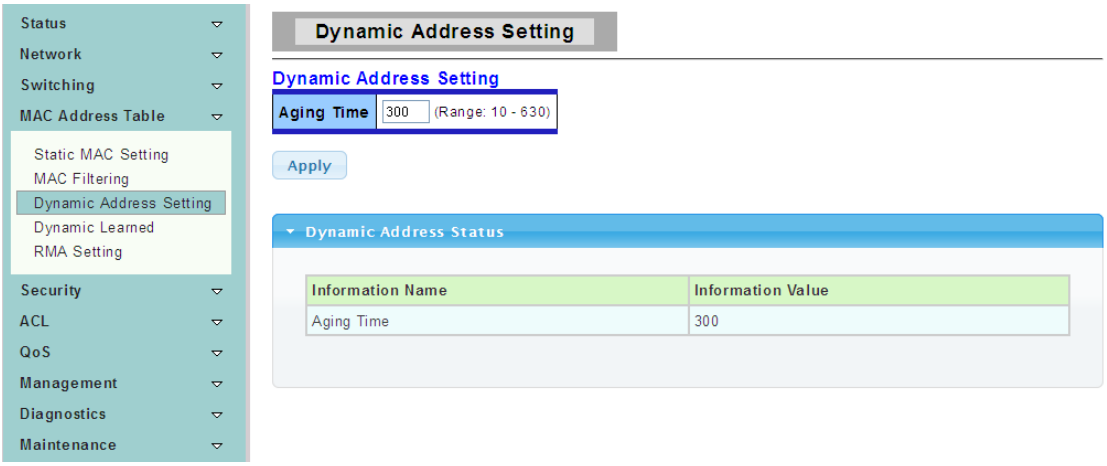
MAC Address: The MAC address to which packets will be filtered. This must be a unicast MAC address.

VLAN: The VLAN ID number of the VLAN on which the above MAC address resides.

4.5.3 Dynamic Address Setting

To display the Dynamic Address Setting web page, click **Mac Address Table > Dynamic Address Setting**

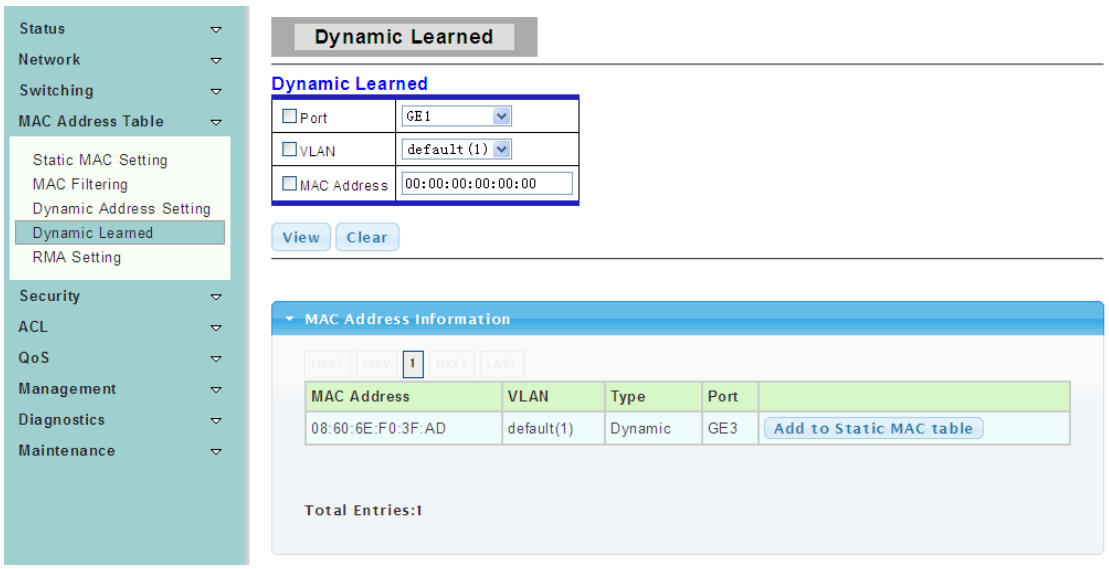
This page is used to set the MAC address of the aging time to study.



Aging Time: Set the time needed for aging

4.5.4 Dynamic Learned

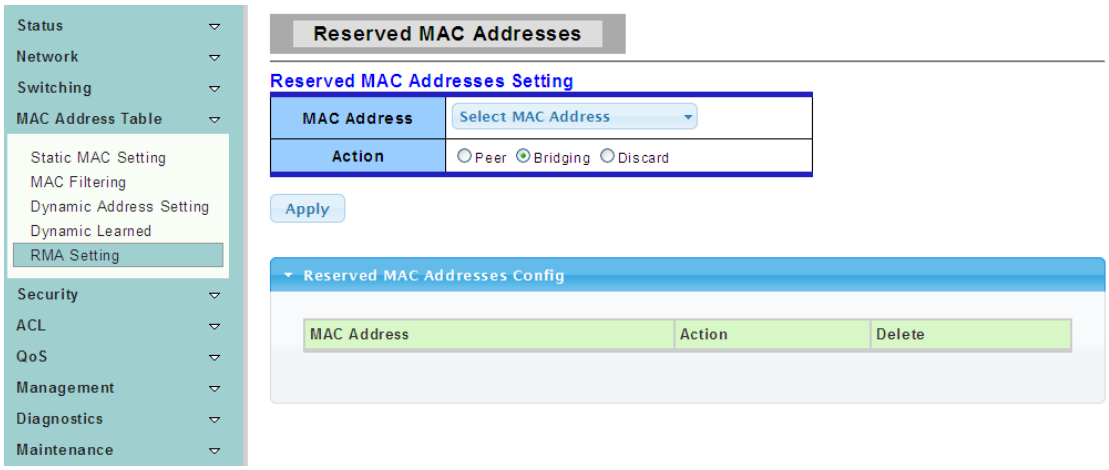
To display the Dynamic Learned web page, click **Mac Address Table > Dynamic Learned**



Port: Select the port number to show or clear dynamic MAC entries. If not select any port, VLAN and MAC address, the whole dynamic MAC table will be displayed or cleared.
VLAN: Select the VLAN to show or clear dynamic MAC entries. If not select any port, VLAN and MAC address, the whole dynamic MAC table will be displayed or cleared.
MAC Address: Select the MAC address to show or clear dynamic MAC entries. If not select any port, VLAN and MAC address, the whole dynamic MAC table will be displayed or cleared.

4.5.5 RMA Setting

To display the Reserved MAC Addresses web page, click **Mac Address Table > RMA Setting**



4.6 Security

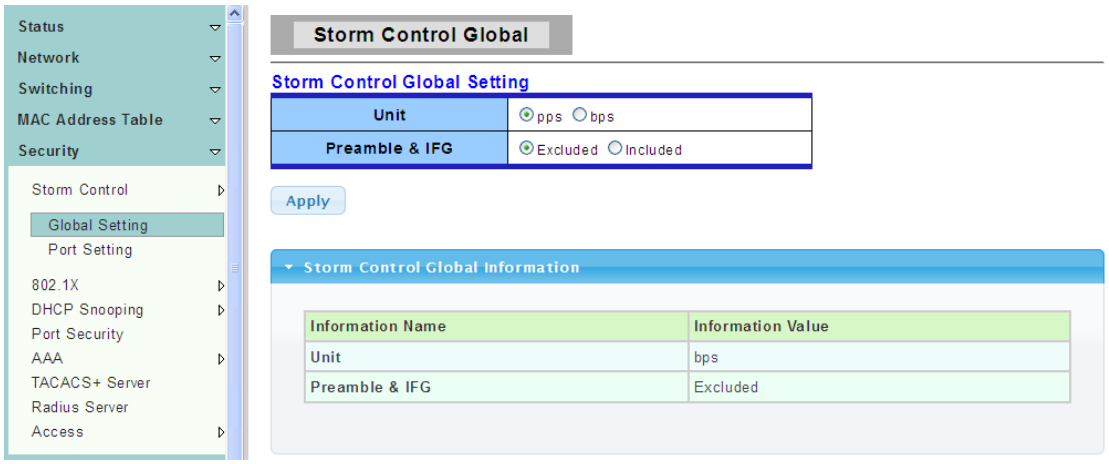
Use the Security pages to configure settings for the switch security features.

4.6.1 Storm Control

Storm control prevents LAN interfaces from being disrupted by a broadcast storm. A broadcast storm occurs when broadcast packets flood the subnet, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation or in the network configuration can cause a broadcast storm.

4.6.1.1 Global Setting

To display the Storm Control Global web page, click **Security > Storm Control > Global Setting**



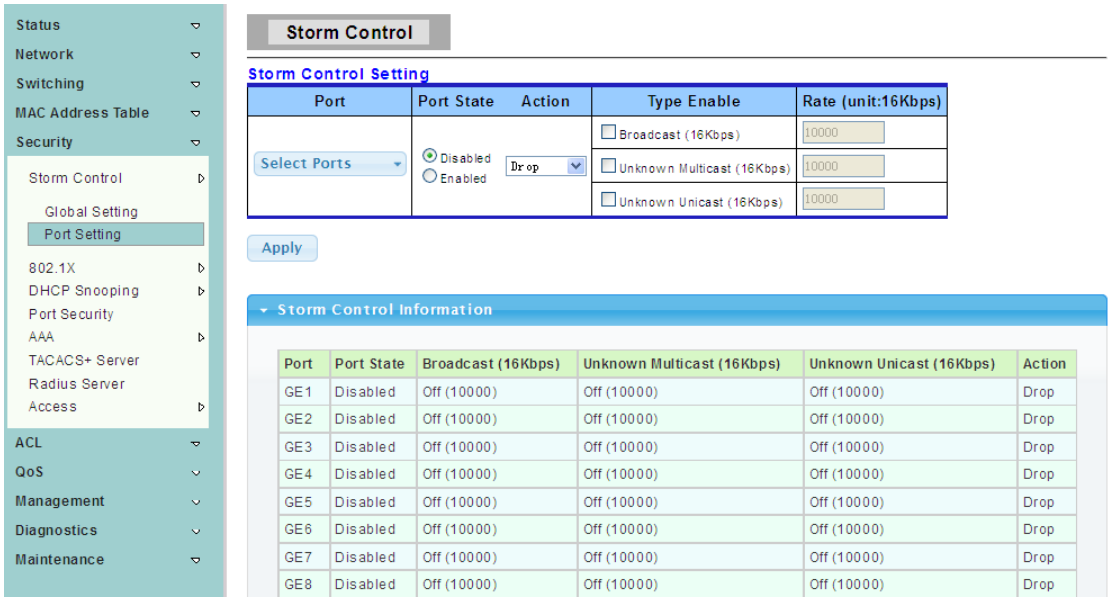
Unit: Choose to storm control unit is the pps or bps

Preamble & IFG: Select the rate calculates w/o preamble & IFG (20 bytes).

- Excluded: exclude preamble & IFG (20 bytes) when count ingress storm control rate.
- Included: include preamble & IFG (20 bytes) when count ingress storm control rate.

4.6.1.2 Port Setting

To display the Strom Control web page, click **Security > Storm Control > Port Setting**



Port: Select the setting ports.

Type Enable: Select the type of storm control.

- Broadcast: Broadcast packet.
- Unknown Multicast: Unknown multicast packet State.
- Unknown Unicast: Unknown unicast packet.

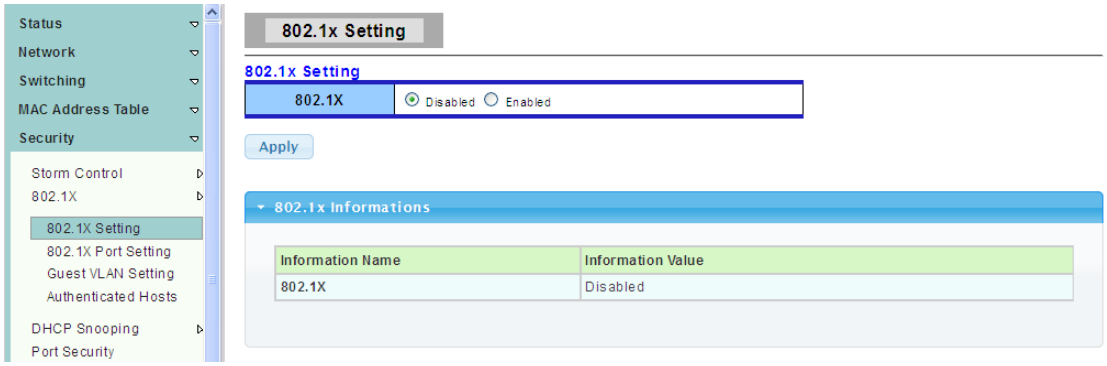
Rate: Value of storm control rate, Unit: pps (packet per-second) or Kbps (Kbits per-second) depends on global mode setting. The range is from 0 to 1000000.

4.6.2 802.1X

802.1x is based on the Client/Server access control and authentication protocol. It can restrict the unauthorized users or devices to connect the access port visit the LAN/WLAN. Before getting the mission from the switch or LAN, the 802.1x will check the users or devices that connect with the switch ports. Before the devices or users pass the exam, it only accept the EAPoL data connect with the switch; but after it passes it, the ordinary data all can be transmitted through Ethernet ports.

4.6.2.1 802.1X Setting

To display the 802.1x Setting web page, click **Security > 802.1X > 802.1X Setting**

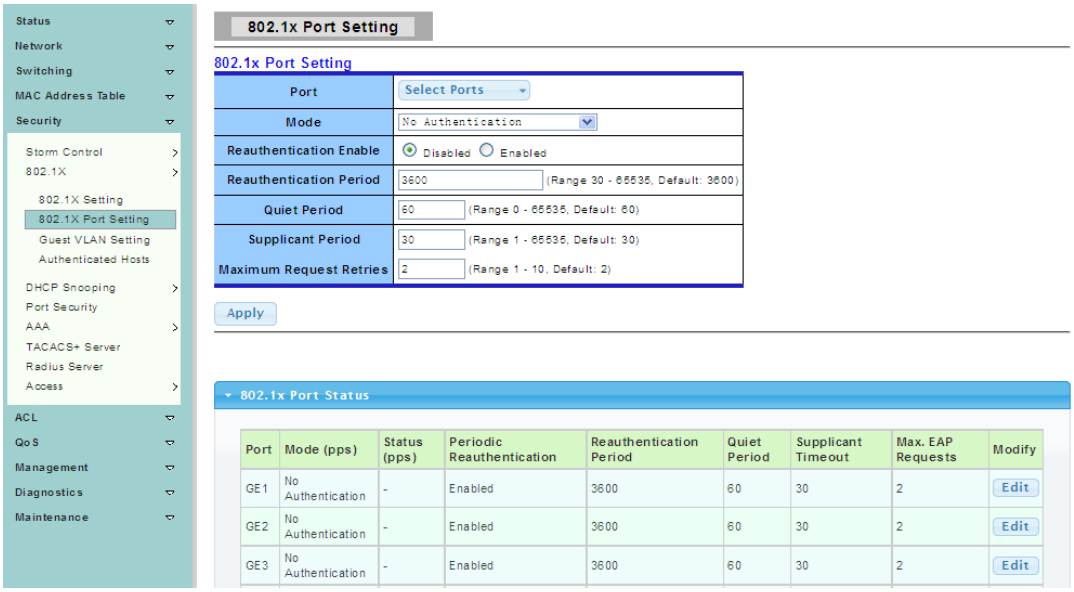


802.1X: Set the enabling status of 802.1X functionality.

- Enable: Enable 802.1X.
- Disable: Disable 802.1X.

4.6.2.2 802.1X Port Setting

To display the 802.1X Port Setting web page, click **Security > 802.1X > 802.1X Port Setting**



Port: Select the ports to configure their authentication mode.

Mode: The authentication mode.

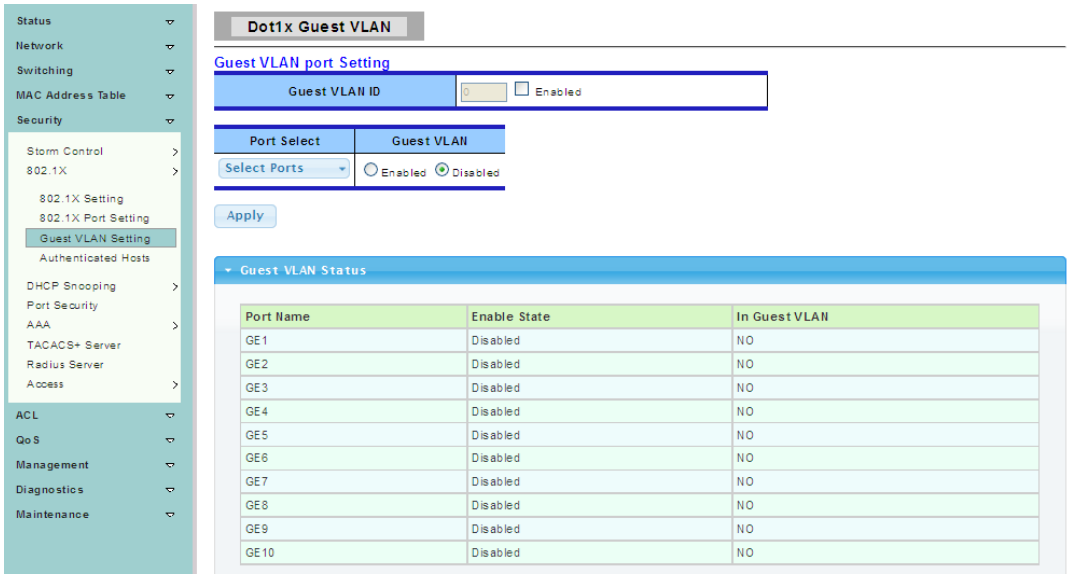
- Force Unauthorized: Force this port to be unconditional unauthorized.
- Force Authorized: Force this port to be unconditional authorized.
- Authentication: 802.1X authentication.
- No Authentication:802.1X disabled.

Re authentication Enable: Set the enabling status of802.1X re authentication.

Re authentication Period: Set the re authentication period of 802.1X if re authentication is enabled.

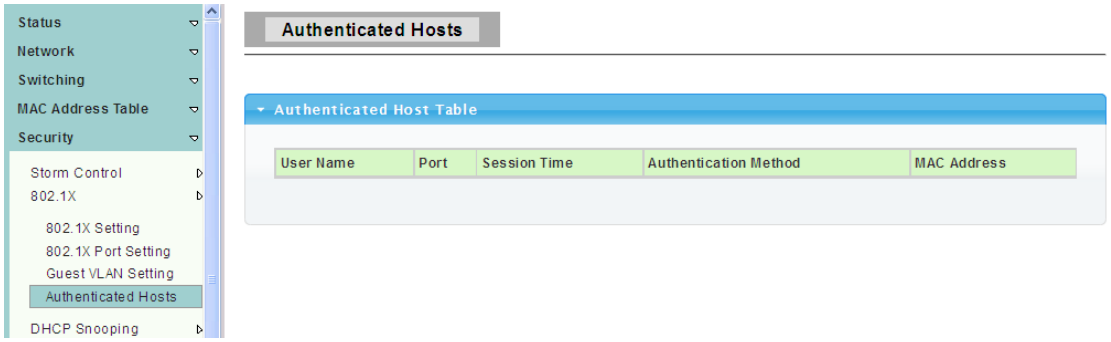
4.6.2.3 Guest VLAN Setting

To display the Dot1x Guest VLAN web page, click **Security > 802.1X > Guest VLAN Setting**



4.6.2.4 Authenticated Hosts

To display the Authenticated Hosts web page, click **Security > 802.1X > Authenticated Hosts**



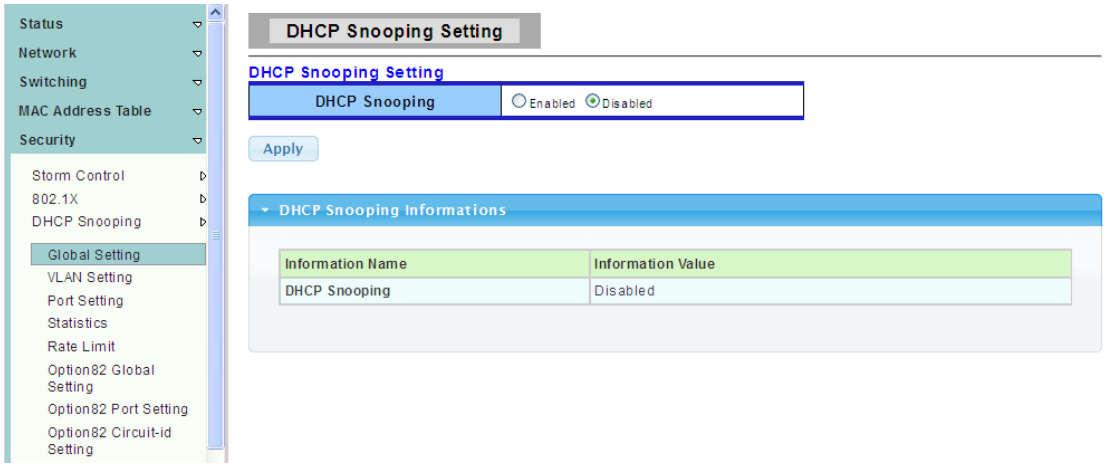
4.6.3 DHCP Snooping

When the switch opens DHCP-Snooping, it will snoop DHCP message and receive DHCP Request and abstract and record the IP address and MAC address from DHCP ACK message. Besides, DHCP-Snooping admits one physical port setting as creditable port or discreditable ports. Creditable ports can receive and forward the DHCP Offer message, on the contrary, the discreditable port will lose the DHCP Offer message. In that way, the switch can pick out the fake DHCP Server and make sure that the client gets legal IP address from DHCP Server.

4.6.3.1 Global Setting

To display the DHCP Snooping Setting web page, click **Security > DHCP Snooping > Global Setting**

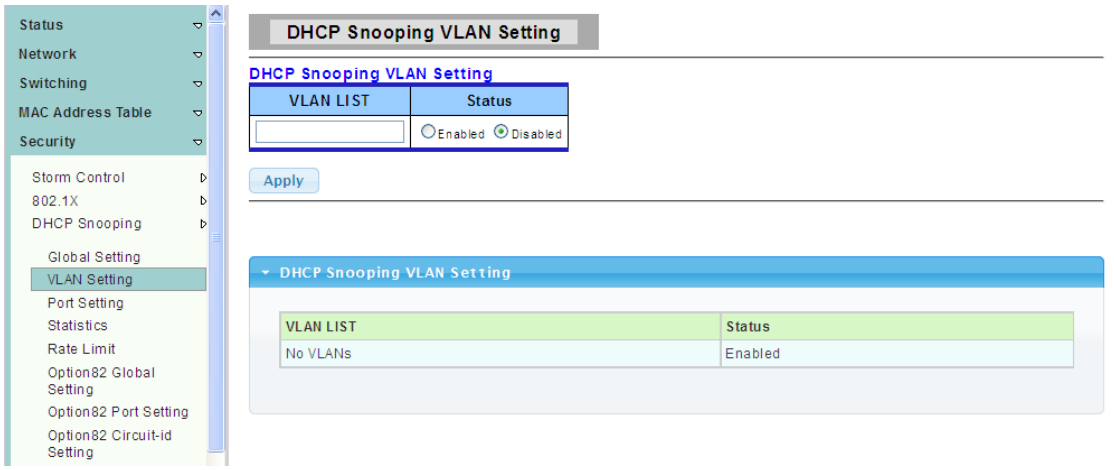
This page is used to open DHCP Snooping function.



DHCP Snooping: enable or disable DHCP Snooping function.

4.6.3.2 VLAN Setting

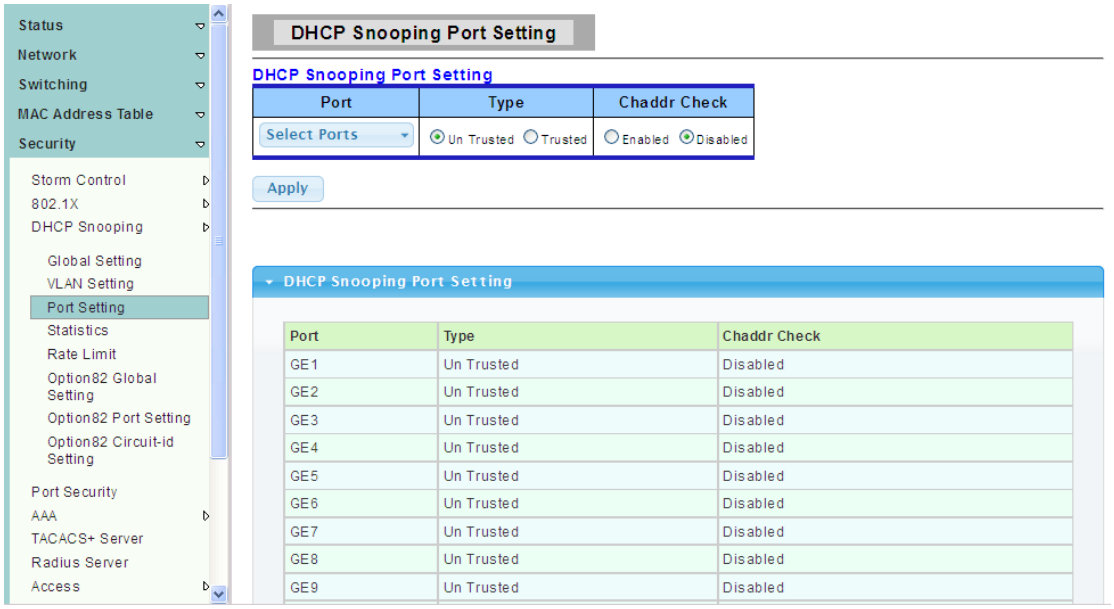
To display the DHCP Snooping VLAN Setting web page, click **Security > DHCP Snooping > VLAN Setting**



4.6.3.3 Port Setting

To display the DHCP Snooping Port Setting web page, click **Security > DHCP Snooping > Port Setting**

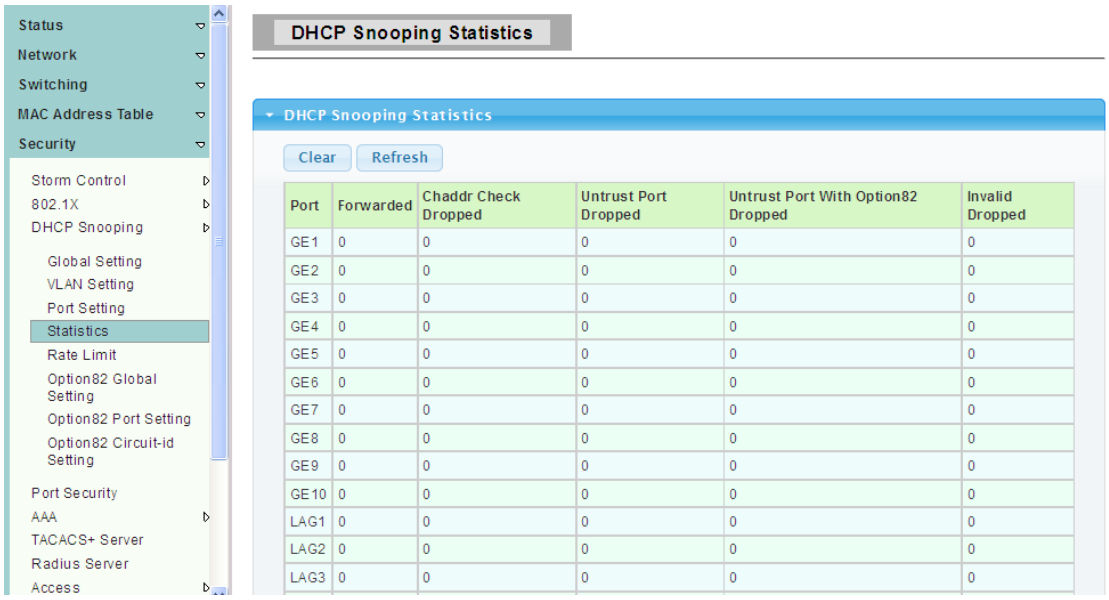
This page allow user to make the specific port is configured for DHCP Snooping trust port.



4.6.3.4 Statistics

To display the DHCP Snooping Statistics web page, click **Security > DHCP Snooping > Statistics**

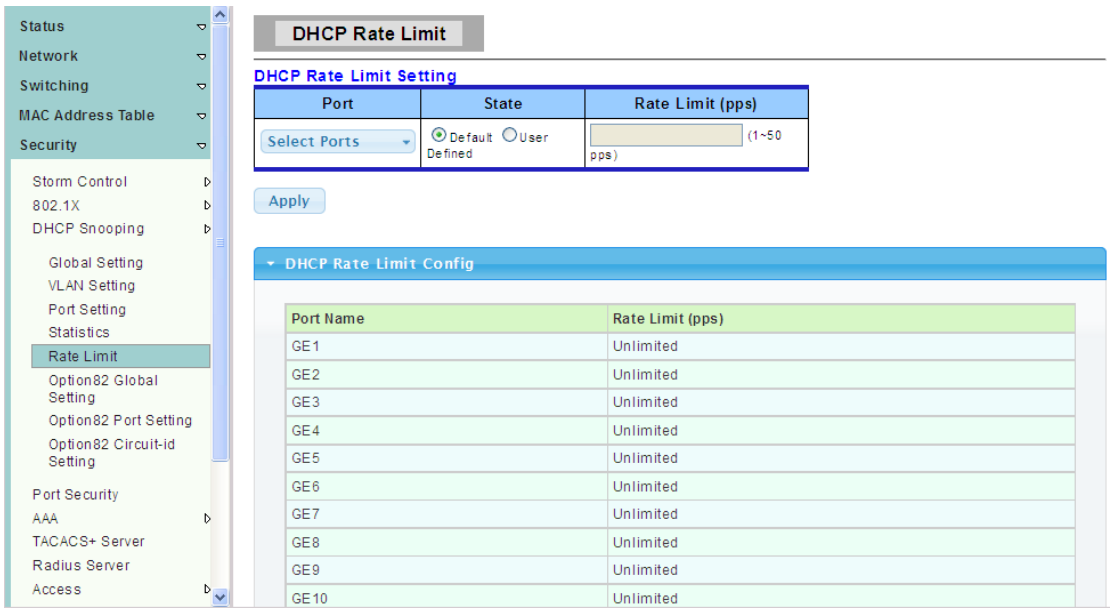
This page statistics of each port of DHCP Snooping state information.



4.6.3.5 Rate Limit

To display the DHCP Rate Limit web page, click **Security > DHCP Snooping > Rate Limit**

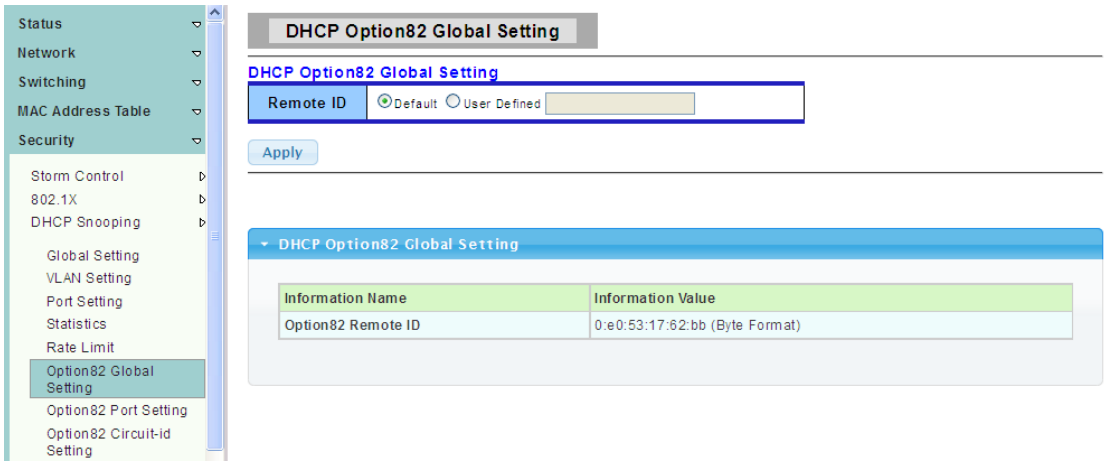
DHCP Snooping on each port traffic control, can restrict access to the switch port access to access networks.



4.6.3.6 Option82 Global Setting

To display the DHCP Option82 Global Setting web page, click **Security > DHCP Snooping > Option82 Global Setting**

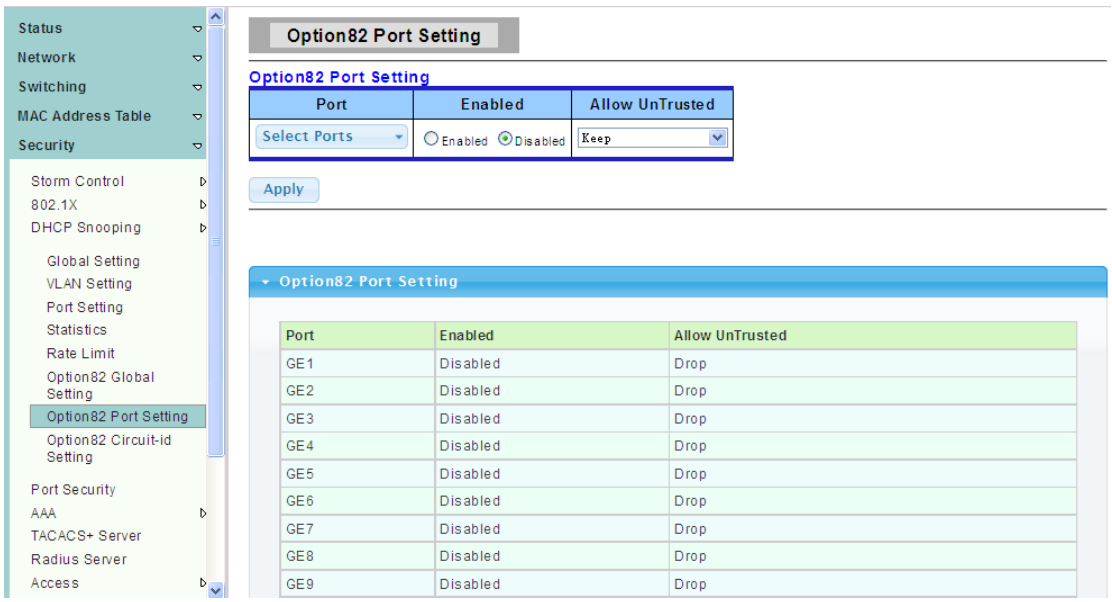
This page is used to configure DHCP Snooping support Option82 strategy.



4.6.3.7 Option82 Port Setting

To display the Option82 Port Setting web page, click **Security > DHCP Snooping > Option82 Port Setting**

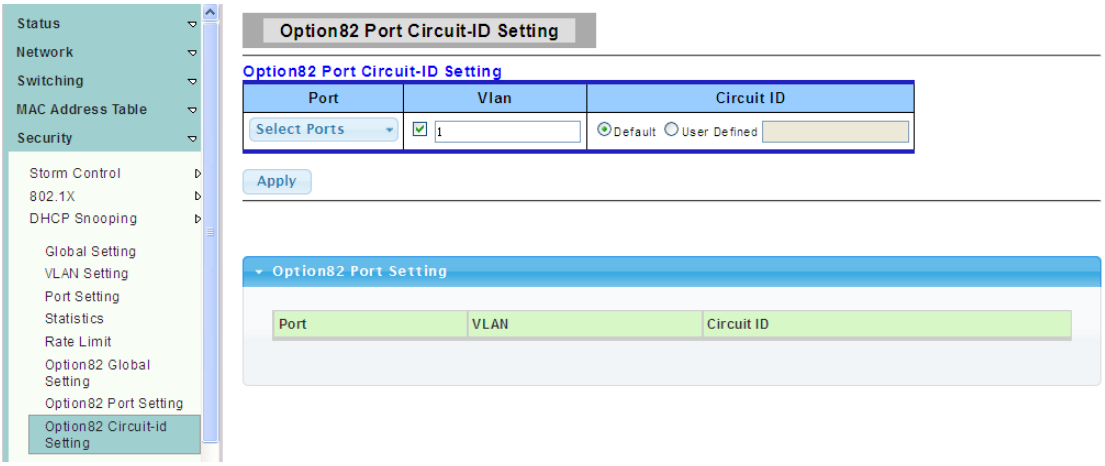
To the specified port configuration of receiving containing Option 82 options request packet port handling strategy.



4.6.3.8 Option82 Circuit-ID Setting

To display the Option82 Port Circuit-ID Setting web page, click **Security > DHCP Snooping > Option82 Circuit-ID Setting**

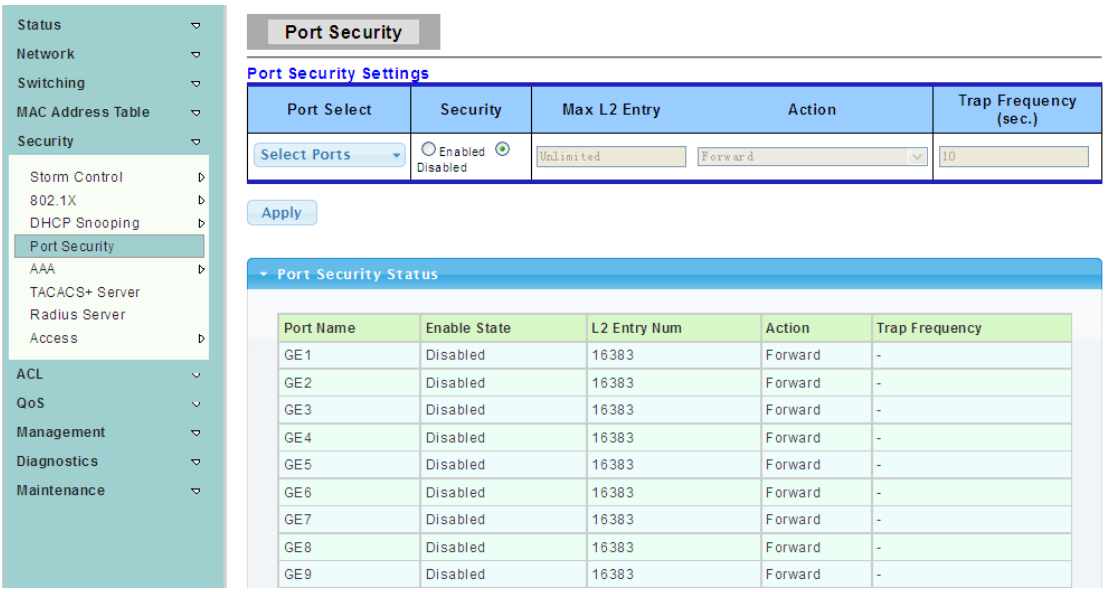
This page allow user to edit circuit ID content in the option82.



4.6.4 Port Security

To display the Port Security web page, click **Security > Port Security**

Ports Security, it can set port isolation and specific behavior.



Port Select: Select one or multiple ports to configure.
Security: Port security function. It constraint how many MAC addresses can be learned by a port and drop new one when reach the limitation.

- Enable: Enable port security function.
- Disable: Disable port security function.

Max L2 Entry: The total number of MAC addresses entry which can be learn by a port.

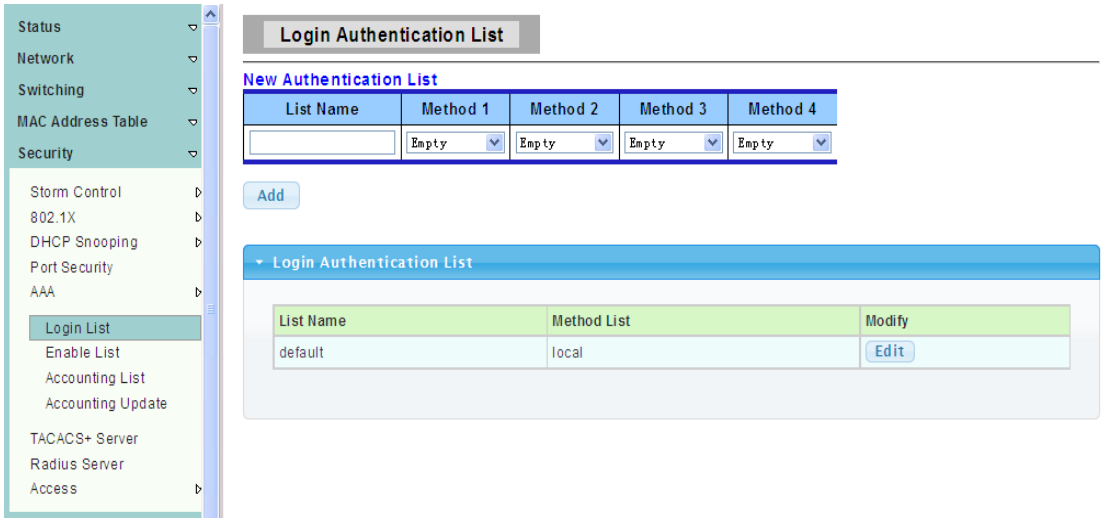
4.6.5 AAA

AAA enables the ASA to determine who the user is (authentication), what the user can do (authorization), and what the user did (accounting).

4.6.5.1 Login List

To display the Login Authentication List web page, click **Security > AAA > Login List**

This page allow user to add, edit delete login authentication list settings (The“default” list cannot be deleted.).The line combined to this list will authenticate login user by methods in this list. If the first method is failed, it will try to use the next priority method to authenticate if it exists.



List Name: New login authentication list name. This name should be different from other existing lists.

Method 1: Select first priority of login authentication method.

- Local: Use local accounts database to authenticate.
- Tacacs+: Use remote TACACS+ server to authenticate.
- Radius: Use remote Radius server to authenticate. Not supported now, it will be supported in the future.
- Enable: Use local enable password to authenticate.

Method 2: Select second priority of login authentication method.

- Local: Use local accounts database to authenticate.
- Tacacs+: Use remote TACACS+ server to authenticate.
- Radius: Use remote Radius server to authenticate. Not supported now, it will be supported in the future.
- Enable: Use local enable password to authenticate.

Method 3: Select third priority of login authentication method.

- Local: Use local accounts database to authenticate.
- Tacacs+: Use remote TACACS+ server to authenticate.
- Radius: Use remote Radius server to authenticate. Not supported now, it will be supported in the future.
- Enable: Use local enable password to authenticate.

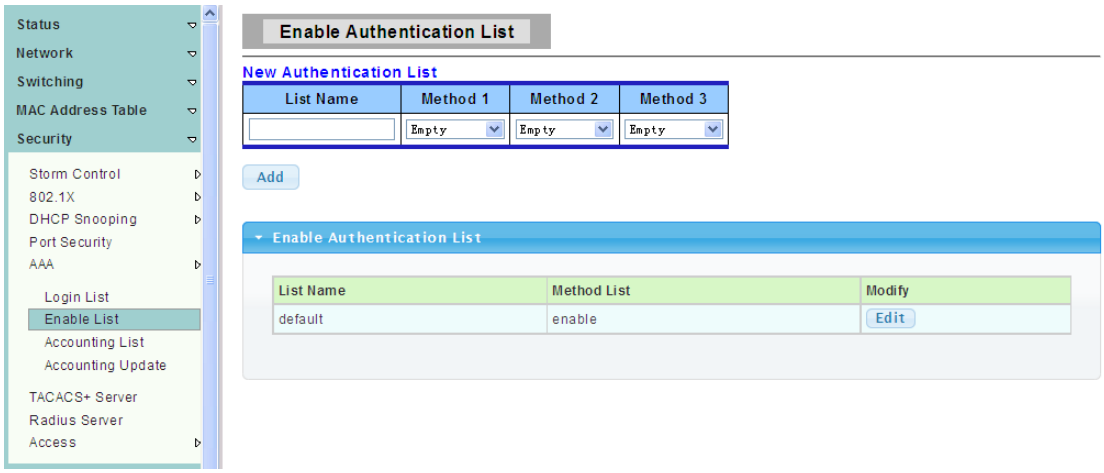
Method 4: Select forth priority of login authentication method.

- Local: Use local accounts database to authenticate
- Tacacs+: Use remote TACACS+ server to authenticate.
- Radius: Use remote Radius server to authenticate. Not supported now, it will be supported in the future.
- Enable: Use local enable password to authenticate.

4.6.5.2 Enable List

To display the Enable Authentication List web page, click **Security > AAA > Enable List**

This page allow user to add, editor delete enable authentication list settings (The “default” list cannot be deleted.). The line combined to this list will authenticate user who issuing the ‘enable’ command by methods in this list. If the first method is failed, it will try to use the next priority method to authenticate if it exists.



List Name: New enable authentication list name. This name should be. different from other existing lists.

Method 1: Select first priority of enable authentication method.

- Enable: Use local enable password to authenticate
- Tacacs+: Use remote TACACS+ server to authenticate.
- Radius: Use remote Radius server to authenticate. Not supported now, it will be supported in the future.

Method 2: Select second priority of enable authentication method.

- Enable: Use local enable password to authenticate
- Tacacs+: Use remote TACACS+ server to authenticate.
- Radius: Use remote Radius server to authenticate. Not supported now, it will be supported in the future.

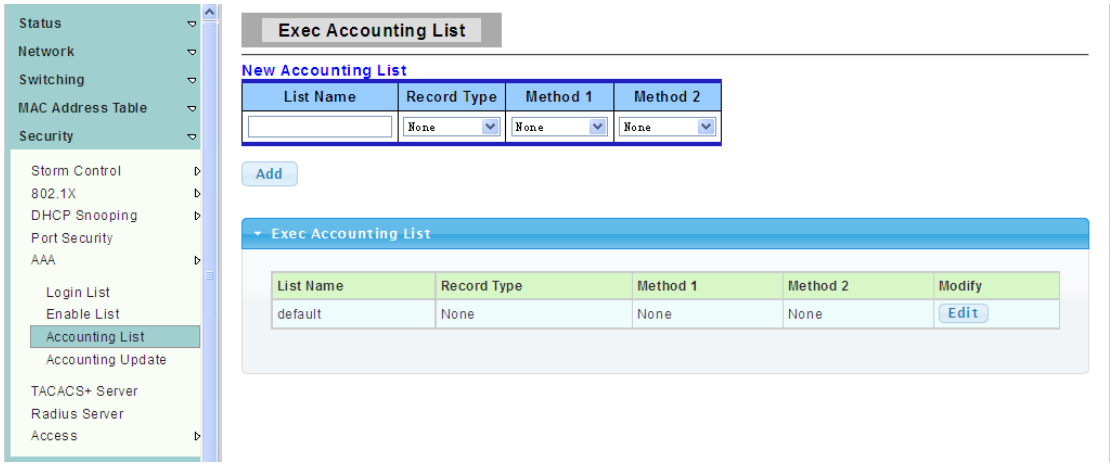
Method 3: Select third priority of enable authentication method.

- Enable: Use local enable password to authenticate.
- Tacacs+: Use remote TACACS+ server to authenticate.
- Radius: Use remote Radius server to authenticate. Not supported now, it will be supported in the future.

4.6.5.3 Accounting List

To display the Exec Accounting List web page, click **Security > AAA > Accounting List**

This page allow user to add, editor delete accounting list settings (The “default” list cannot be deleted.). The line combined to this list will accounting user who entering CLI shell by methods in this list. If the first method is failed, it will try to use the next priority method to accounting if it exists.



List Name: New accounting list name. This name should be different from other existing lists.

Record Type: Select accounting record type.

- none: No accounting.
- start-stop: Record start and stop without waiting.
- stop-only: Record stop when service terminates.

Method 1: Select first priority of exec accounting method.

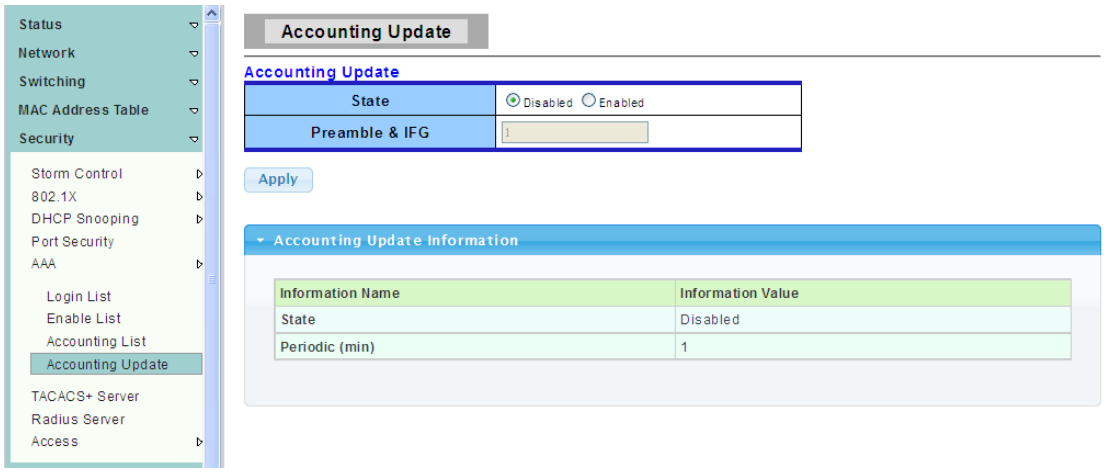
- Tacacs+: Use remote TACACS+ server to accounting.
- Radius: Use remote Radius server to accounting. Not supported now, it will be supported in the future.

Method 2: Select second priority of exec accounting method.

- Tacacs+: Use remote TACACS+ server to accounting.
- Radius: Use remote Radius server to accounting. Not supported now, it will be supported in the future.

4.6.5.4 Accounting Update

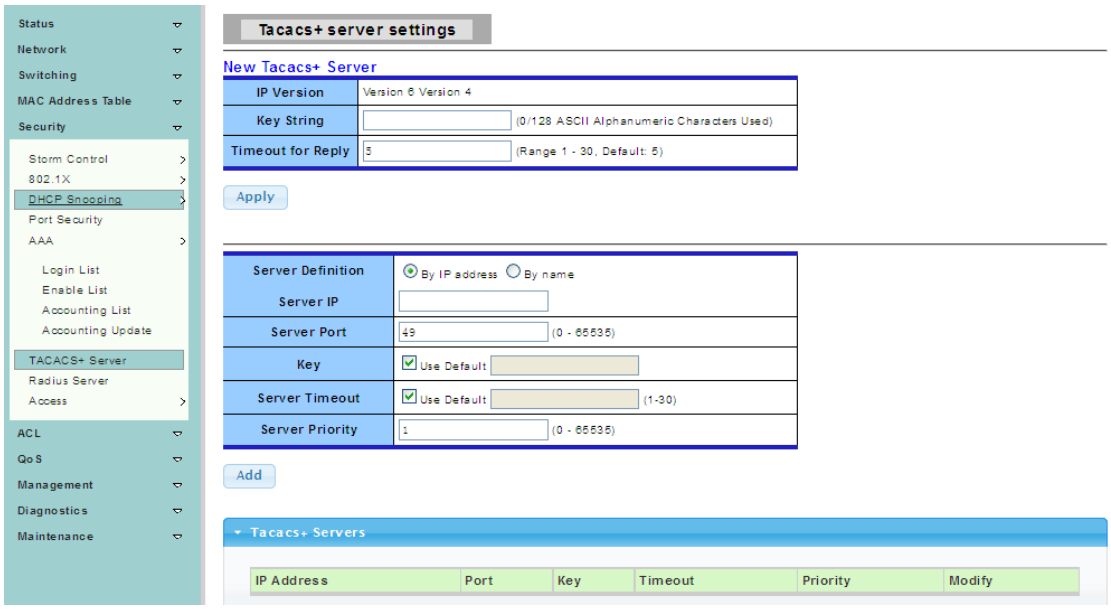
To display the Accounting Update web page, click **Security > AAA > Accounting Update**



4.6.6 TACACS+ Server

To display the TACACS+ server settings web page, click **Security > TACACS+ Server**

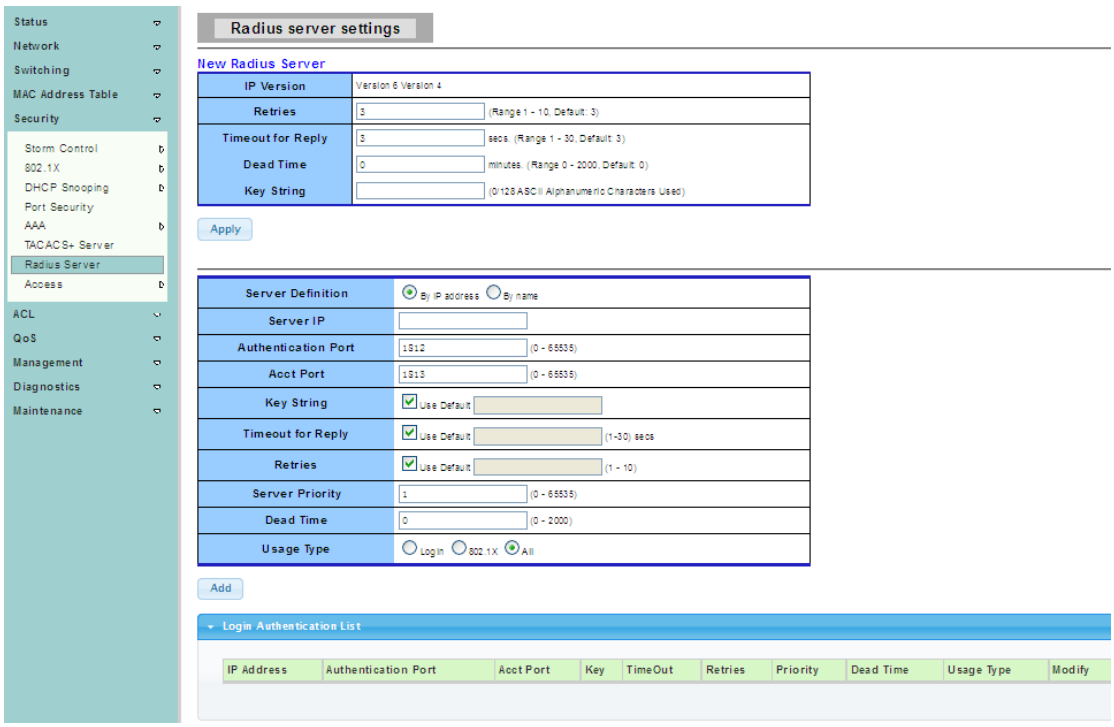
This page allow user to add, edit or delete TACACS+ server settings.



4.6.7 Radius server

To display the Radius server settings web page, click **Security > Radius Server**

This page is used to set about radius server.



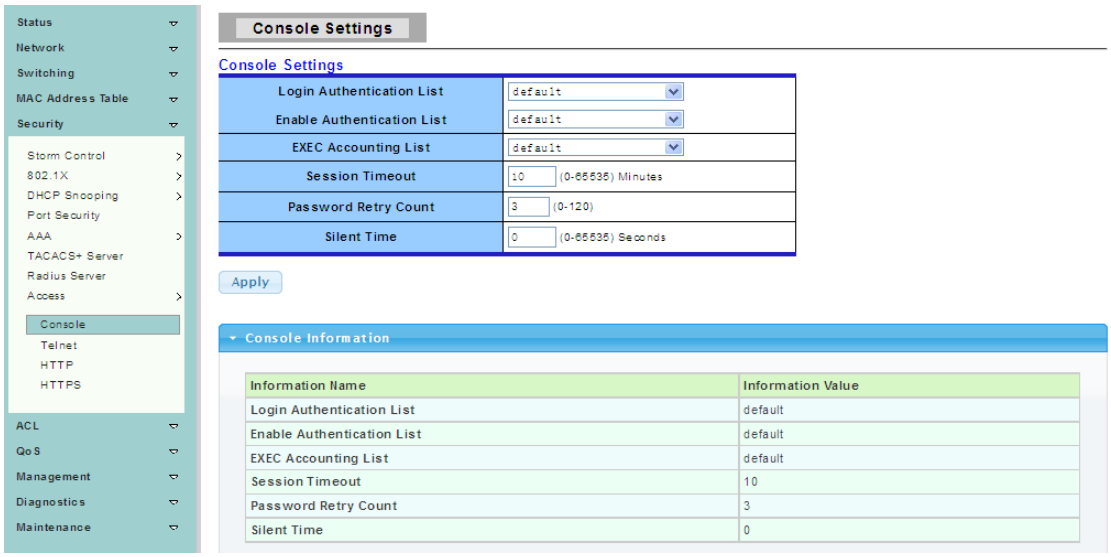
4.6.8 Access

4.6.8.1 Console

To display the Console Settings web page, click **Security > Access > Console**

This page allow user to combine all kinds of AAA lists to console line. The user accesses

switch from console will be authenticated, authorized and accounted by AAA lists we combined here.



Login Authentication List: Select one of the login authentication lists we configured in "Login List" page.

Enable Authentication List: Select one of the enable authentication lists we configured in "Enable List" page.

EXEC Accounting List: Select one of the EXEC accounting lists we configured in "Accounting List" page.

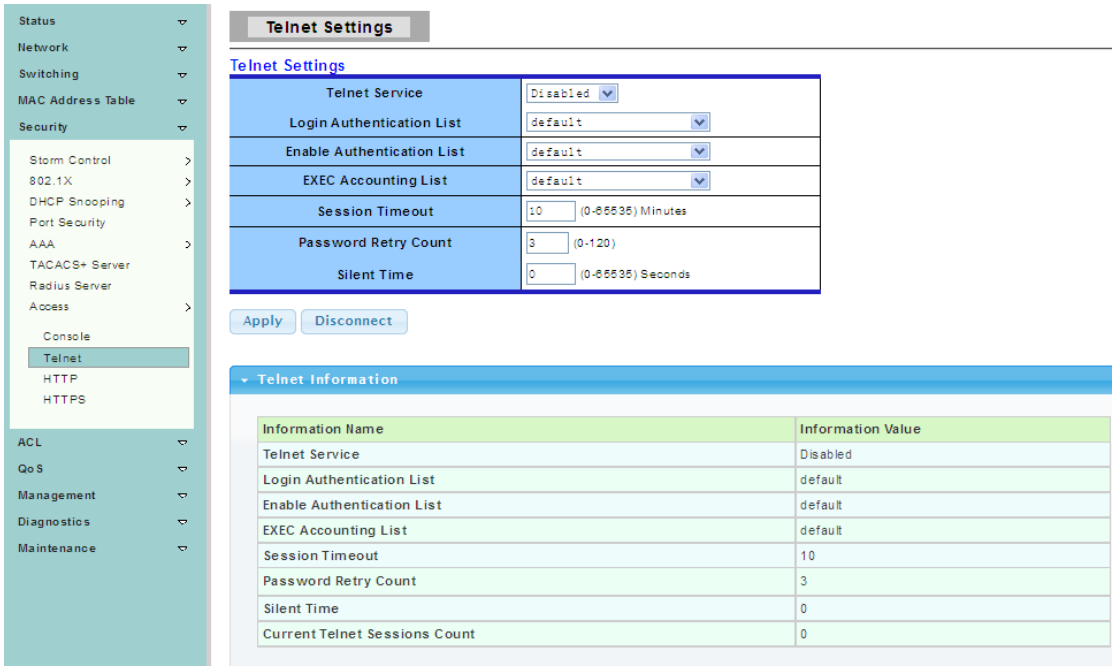
Session Timeout: Set session timeout minutes for user access CLI from console line. If user does not response after session timeout minute, CLI will logout automatically. 0 minutes means never timeout.

Password Retry Count: limit the number of repeat input error password.

4.6.8.2 Telnet

To display the Telnet Settings web page, click **Security > Access > Telnet**

This page allow user to combine all kinds of AAA lists to telnet line. The user accesses switch from telnet will be authenticated, authorized and accounted by AAA lists we combined here.



Telnet Service: Set remote service disable or enable.

Login Authentication List: Select one of the login authentication lists we configured in "Login List" page.

Enable Authentication List: Select one of the enable authentication lists we configured in "Enable List" page.

EXEC Authorization List: Select one of the EXEC authorization lists we configured in "EXEC List" page.

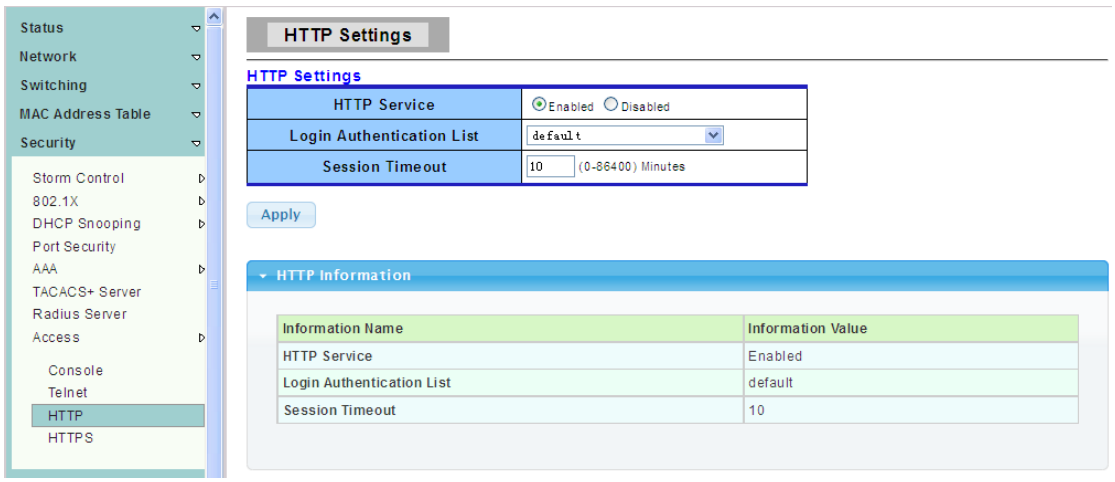
Session Timeout: Set session timeout minutes for user access CLI from telnet line. If user does not response after session timeout minute, CLI will logout automatically.

Password Retry Count: limit the number of repeat input error password.

4.6.8.3 HTTP

To display the HTTP Settings web page, click **Security > Access > HTTP**

This page allow user to combine all kinds of AAA lists to HTTP line. The user accesses switch WEB UI from HTTP will be authenticated by AAA lists we combined here.

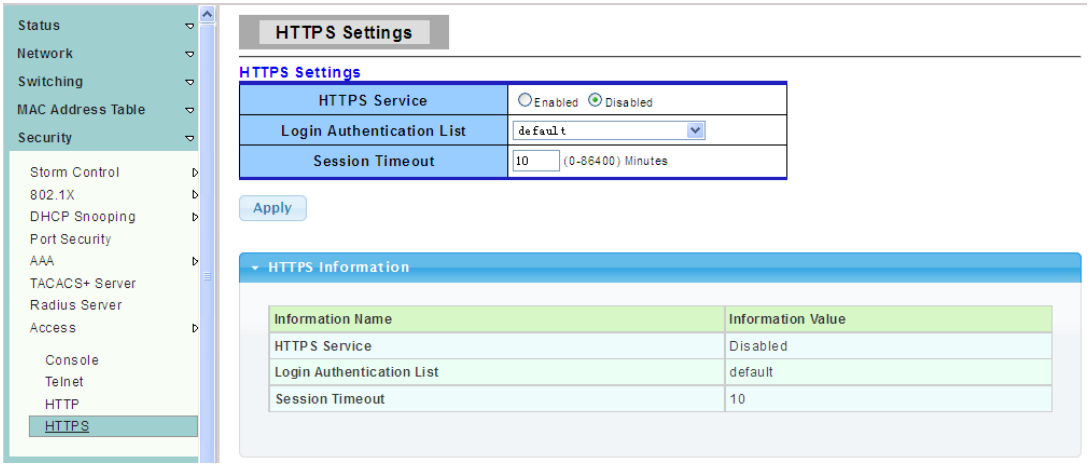


HTTP Server：Set HTTP Server disable or enable.
Login Authentication List: Select one of the login authentication lists we configured in “Login List” page.
Session Timeout: Set session timeout minutes for user access WEB from HTTP protocol. If user does not response after session timeout minute, WEBUI will logout automatically. 0 minutes means never timeout.

4.6.8.4 HTTPS

To display the HTTPS Settings web page, click **Security > Access > HTTPS**

This page allow user to combine all kinds of AAA lists to HTTPS line. The user accesses switch WEBUI from HTTPS will be authenticated by AAA lists we combined here.



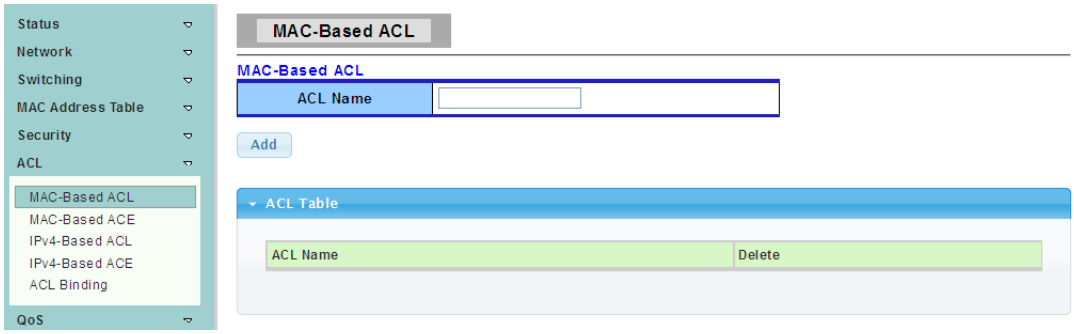
HTTPS Server: Set HTTPS Server disable or enable.
Login Authentication List: Select one of the login authentication lists we configured in “Login List” page.
Session Timeout: Set session timeout minutes for user access WEB from HTTPS protocol. If user does not response after session timeout minute, WEBUI will logout automatically. 0 minutes means never timeout.

4.7 ACL

4.7.1 MAC-Based ACL

To display the MAC-Based ACL web page, click **ACL > MAC-Based ACL**

This page allow user to set name for MAC-Based ACL.

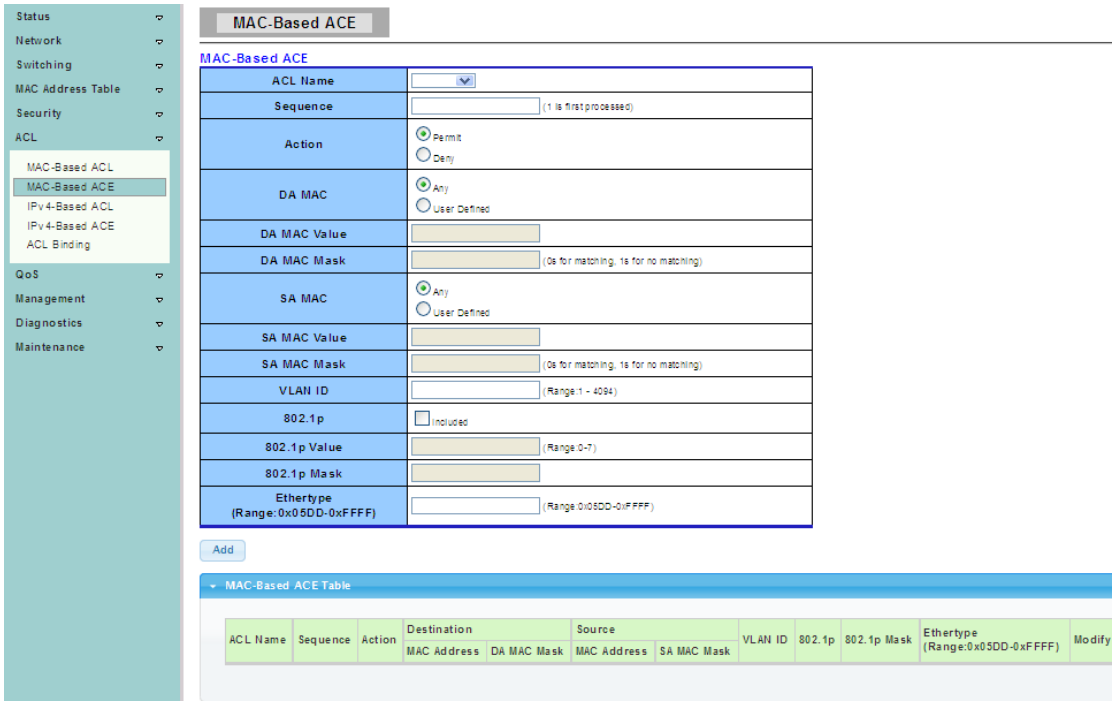


ACL Name: Enter ACL name in this field.

4.7.2 MAC-Based ACE

To display the MAC-Based ACE web page, click **ACL > MAC-Based ACE**

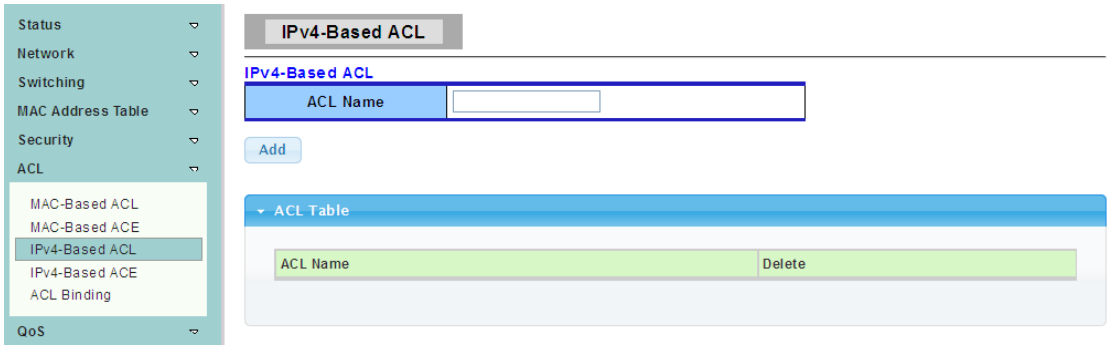
This page allow user to set Based on MAC address expanding ACL list, matching corresponding MAC and setting the ports as drop or forward.



4.7.3 IPv4-Based ACL

To display the IPv4-Based ACL web page, click **ACL > IPv4-Based ACL**

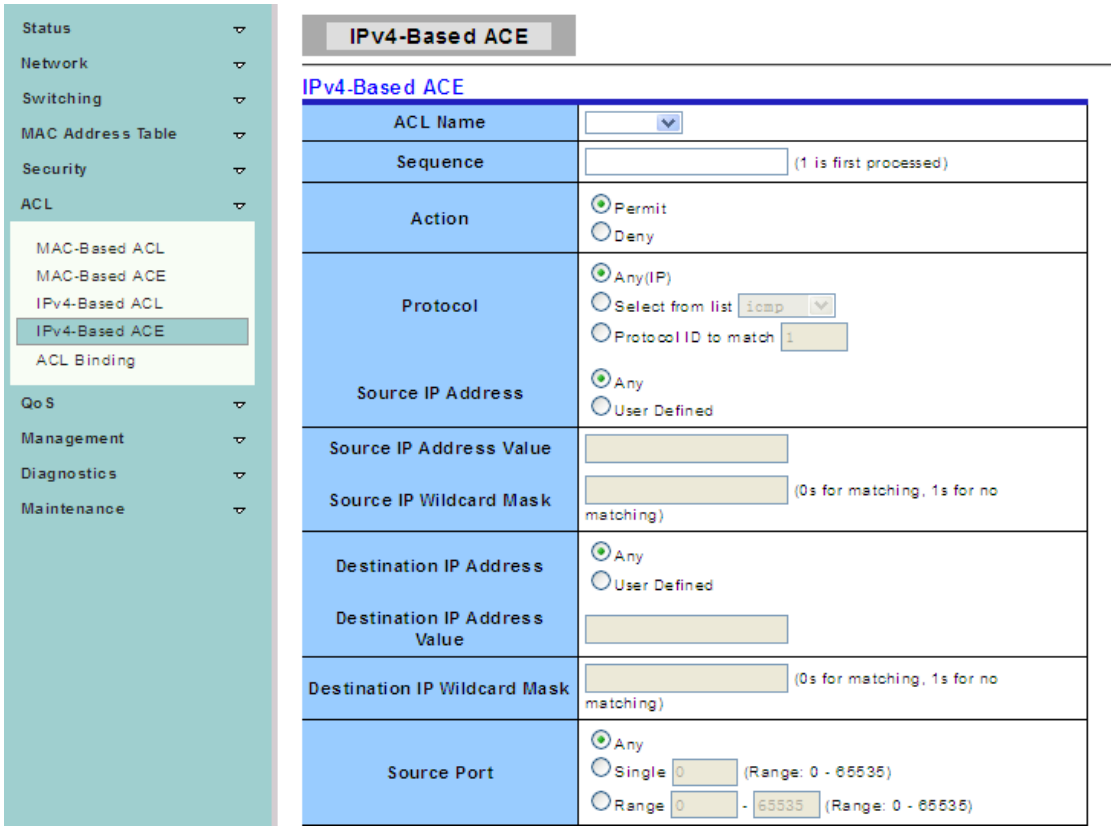
This page allow user to set name for IPv4-Based ACL.



4.7.4 IPv4-Based ACE

To display the IPv4-Based ACE web page, click **ACL > IPv4-Based ACE**

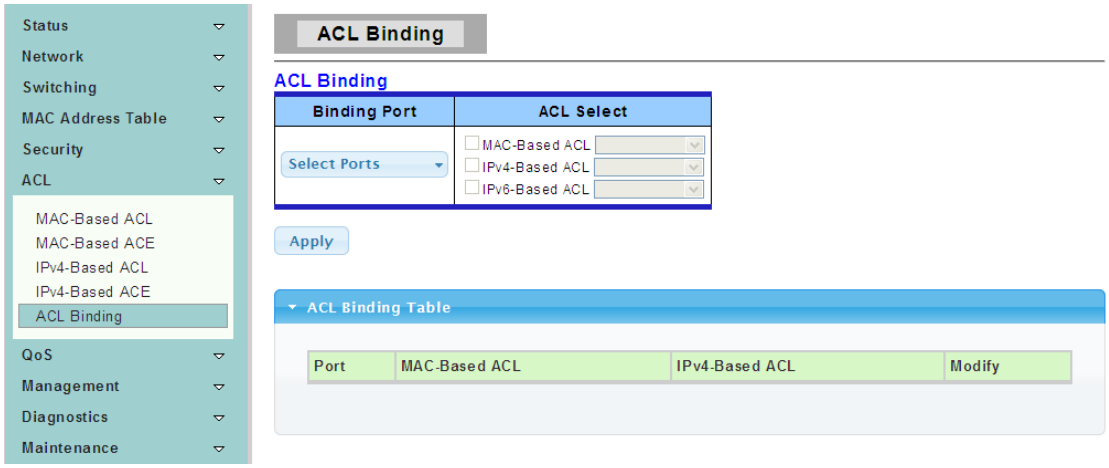
This page allow user to set Based on IPv4 expanding ACL Peer Guardian and matching corresponding IP and setting the port as drop or forward.



4.7.5 ACL Binding

To display the ACL Binding web page, click **ACL > ACL Binding**

This page allow user to Bounding with accordingly ACL rules, port bounding ACL rules.



4.8 QoS

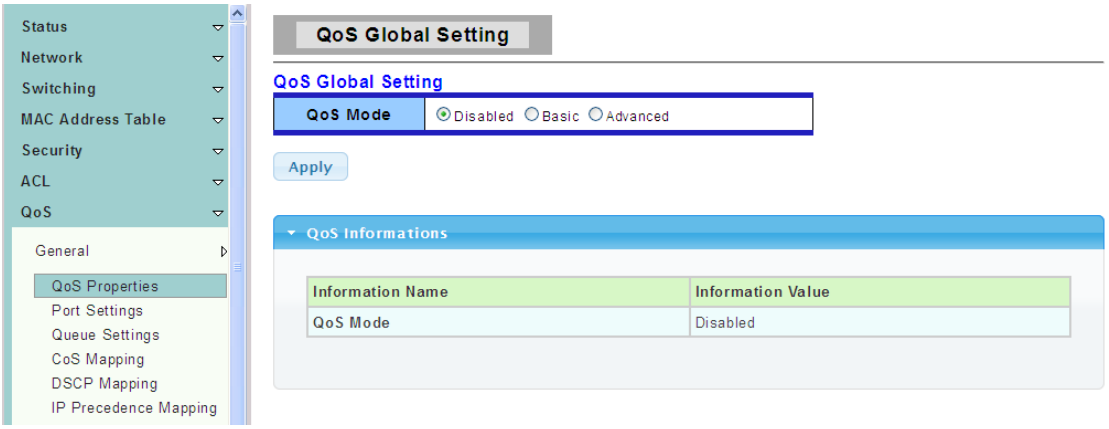
Use the QoS pages to configure settings for the switch QoS interface and how the switch connects to a remote server to get services.

4.8.1 General

4.8.1.1 QoS Properties

To display the QoS Global Setting web page, click **QoS > General > QoS properties**

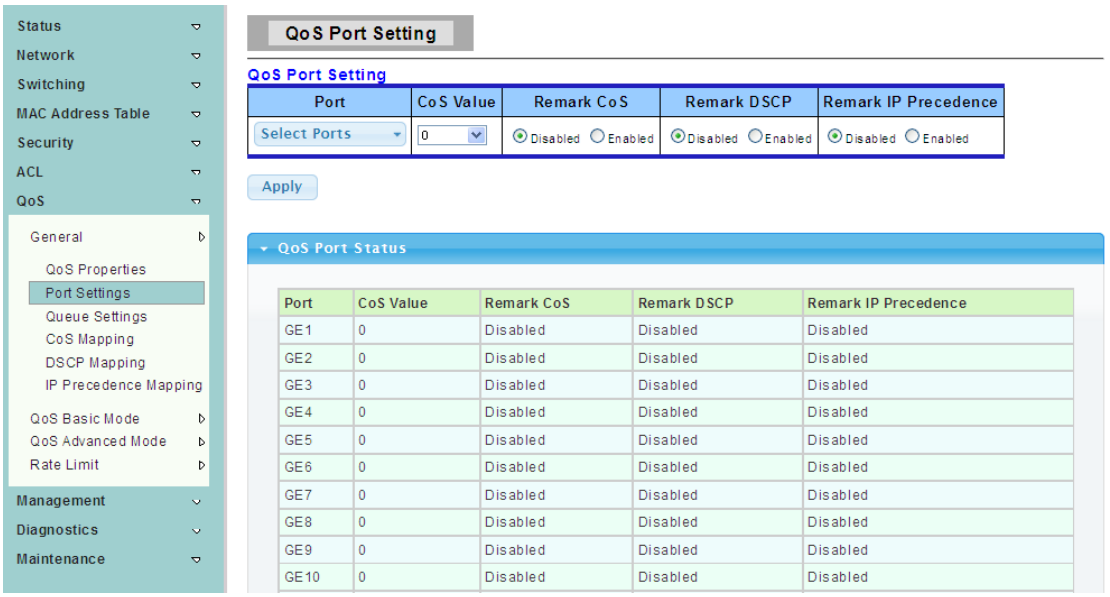
This page allow user to set QoS mode such basic or advanced.



4.8.1.2 Port Settings

To display the QoS Port Settings web page, click **QoS > General > Port Settings**

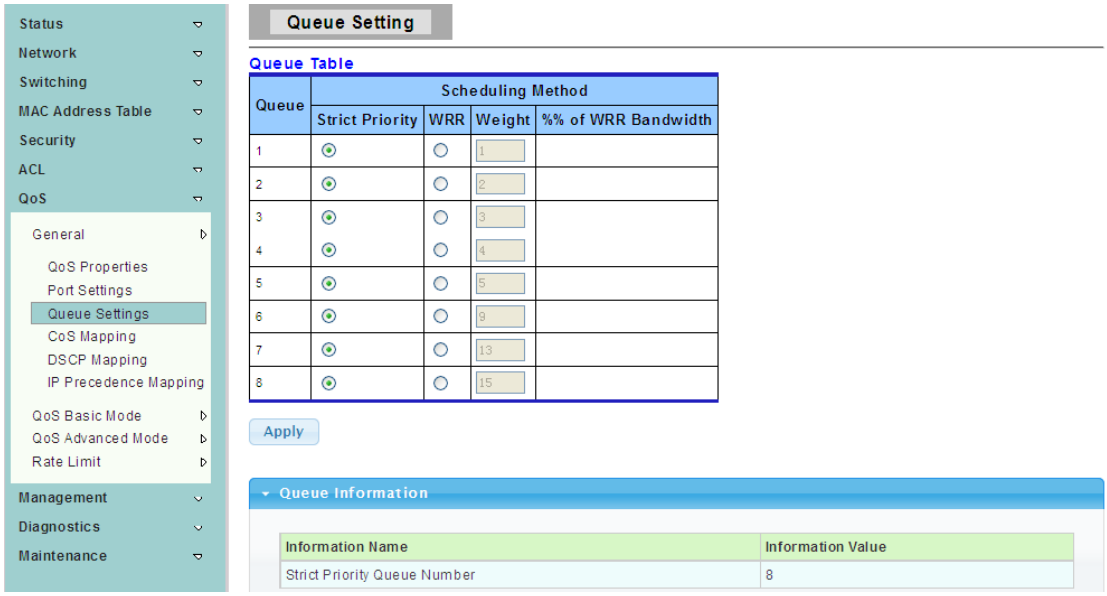
This page is used to give the QoS instance port configuration.



4.8.1.3 Queue Settings

To display the Queue Setting web page, click **QoS > General > Queue Settings**

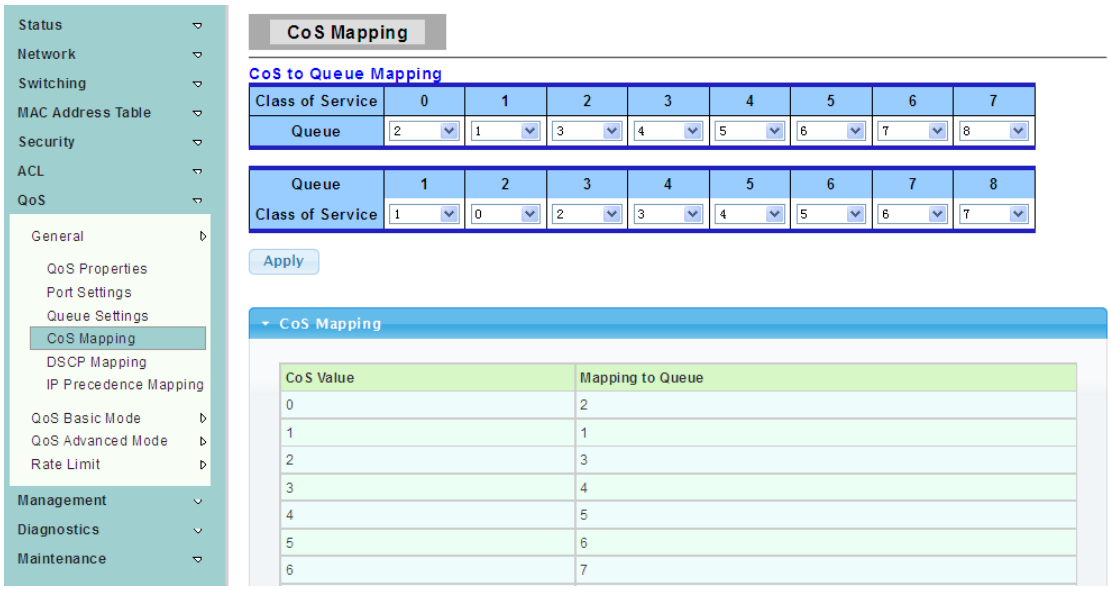
This page allow user to set Set the QoS instance queue scheduling model.



4.8.1.4 CoS Mapping

To display the CoS Mapping web page, click **QoS > General > CoS Mapping**

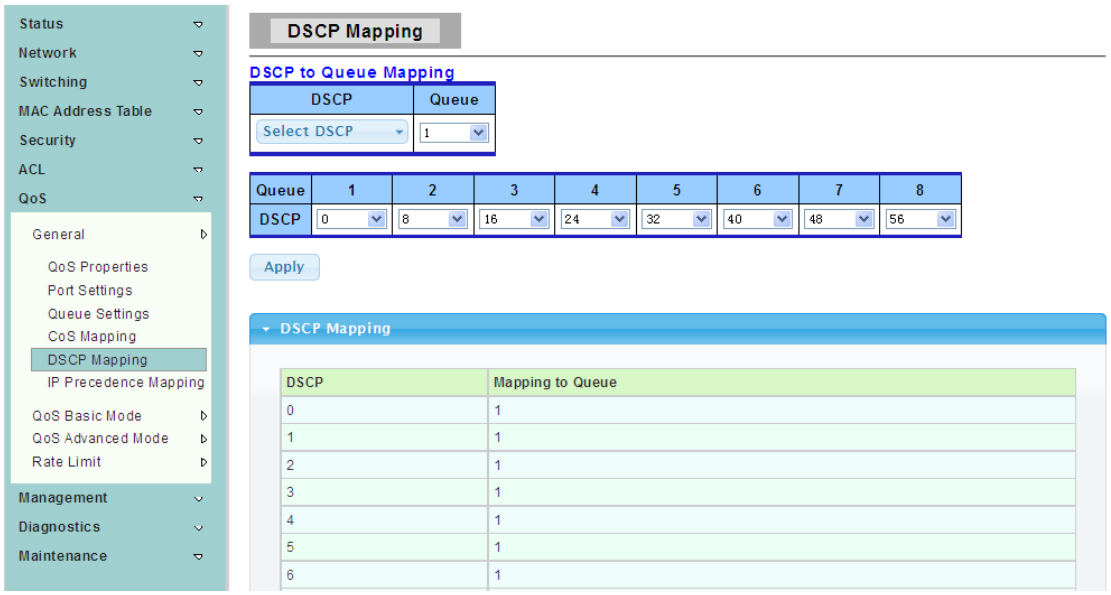
The page allow user to set QoS instance of CoS Mapping.



4.8.1.5 DSCP Mapping

To display the DSCP Mapping web page, click **QoS > General > DSCP Mapping**

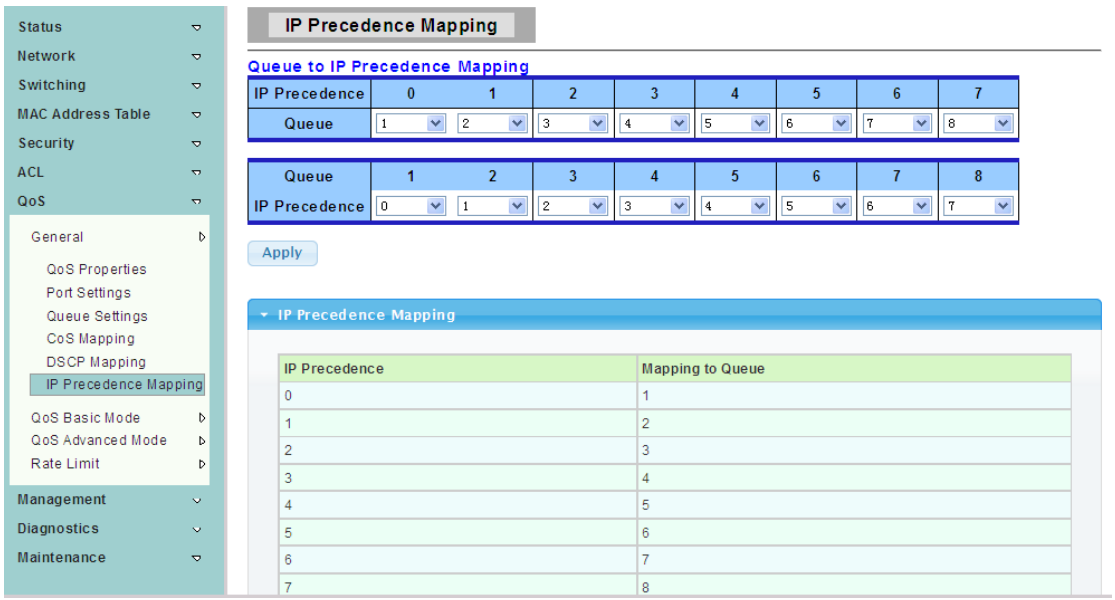
The page allow user to set QoS instance of DSCP Mapping.



4.8.1.6 IP Precedence Mapping

To display the IP Precedence Mapping web page, click **QoS > General > IP Precedence Mapping**

The page allow user to set QoS instance of IP Precedence Mapping.

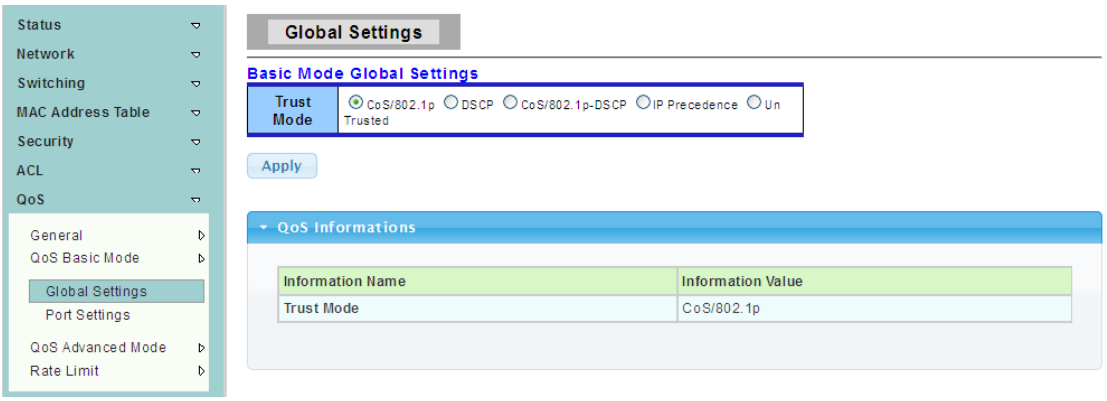


4.8.2 QoS Basic Mode

4.8.2.1 Global Settings

To display the Global Settings web page, click **QoS > QoS Basic Mode > Global Settings**

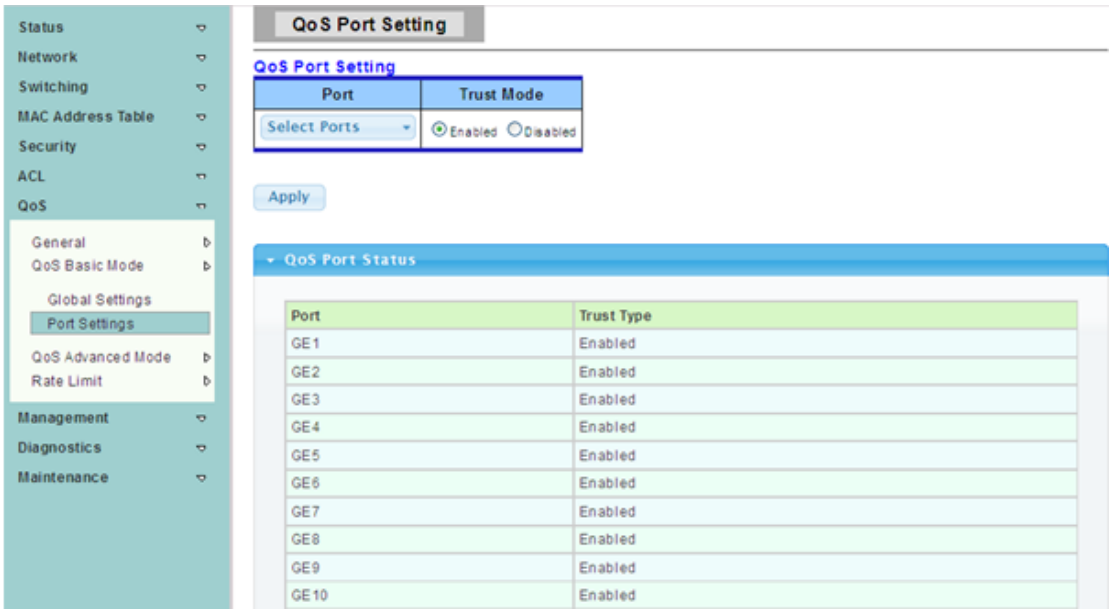
This page allow user to set QoS for trust mode on basic mode global settings.



4.8.2.2 Port Settings

To display the QoS Port Settings web page, click **QoS > QoS Basic Mode > Port Settings**

This page allow user to set QoS port setting enabled or disabled.

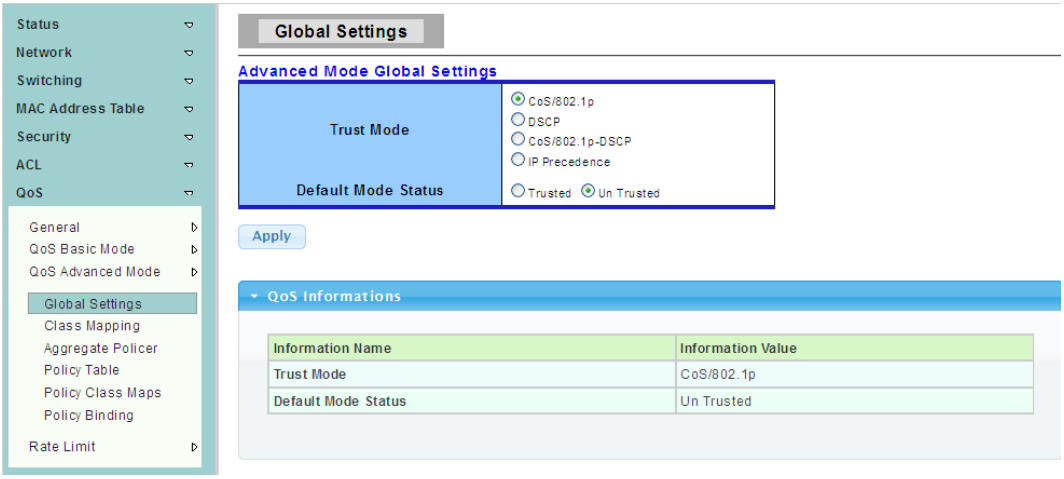


4.8.3 QoS Advanced Mode

4.8.3.1 Global Settings

To display the Global Settings web page, click **QoS > QoS Advanced Mode > Global Settings**

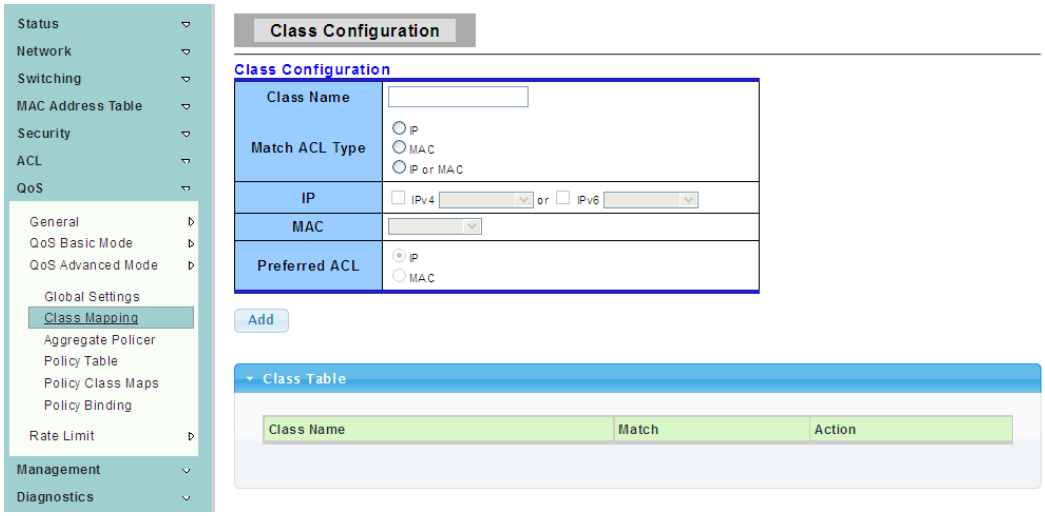
This page allow user to set the default QoS mode state under advanced mode global settings trust mode.



4.8.3.2 Class Mapping

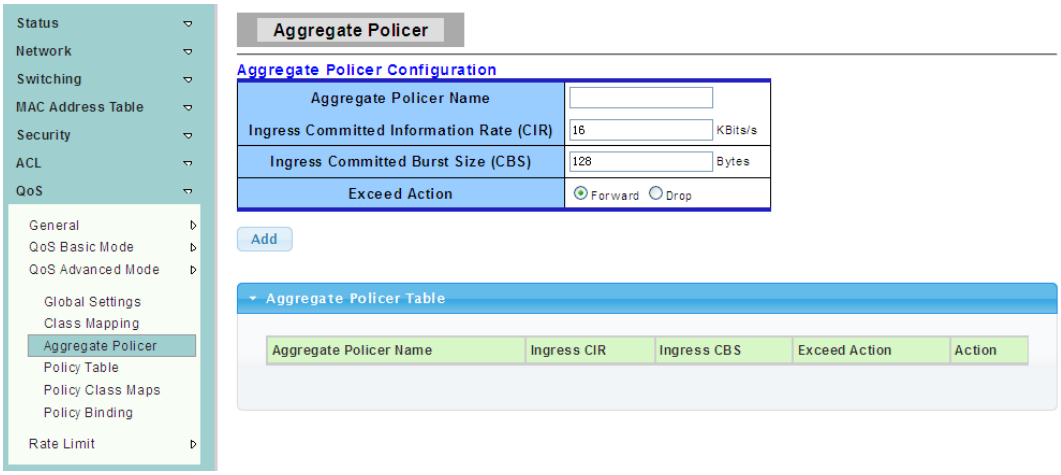
To display the Class Configuration web page, click **QoS > QoS Advanced Mode > Class Mapping**

This page allow user to create a QoS class which is used to link the ACL.



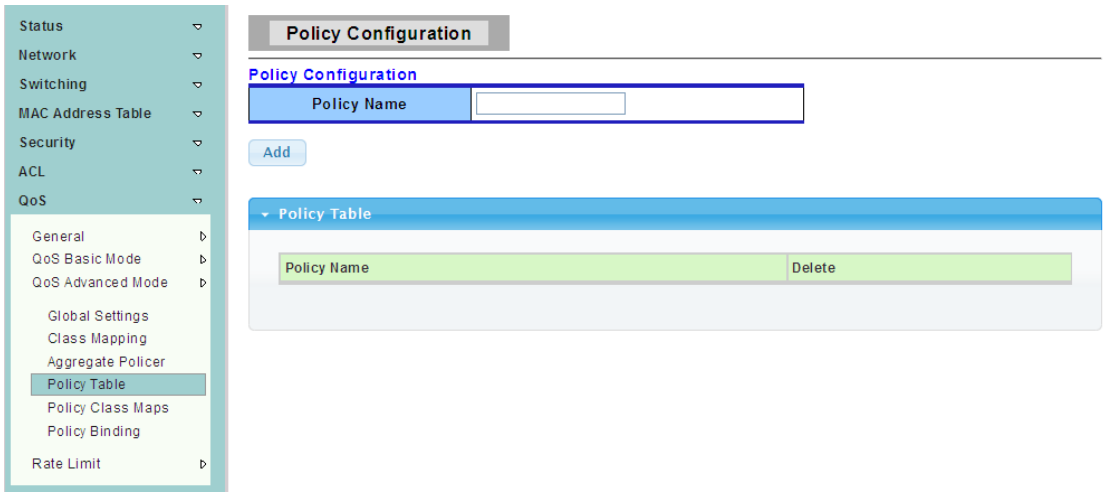
4.8.3.3 Aggregate Policer

To display the Aggregate Policer web page, click **QoS > QoS Advanced Mode > Aggregate Policer**



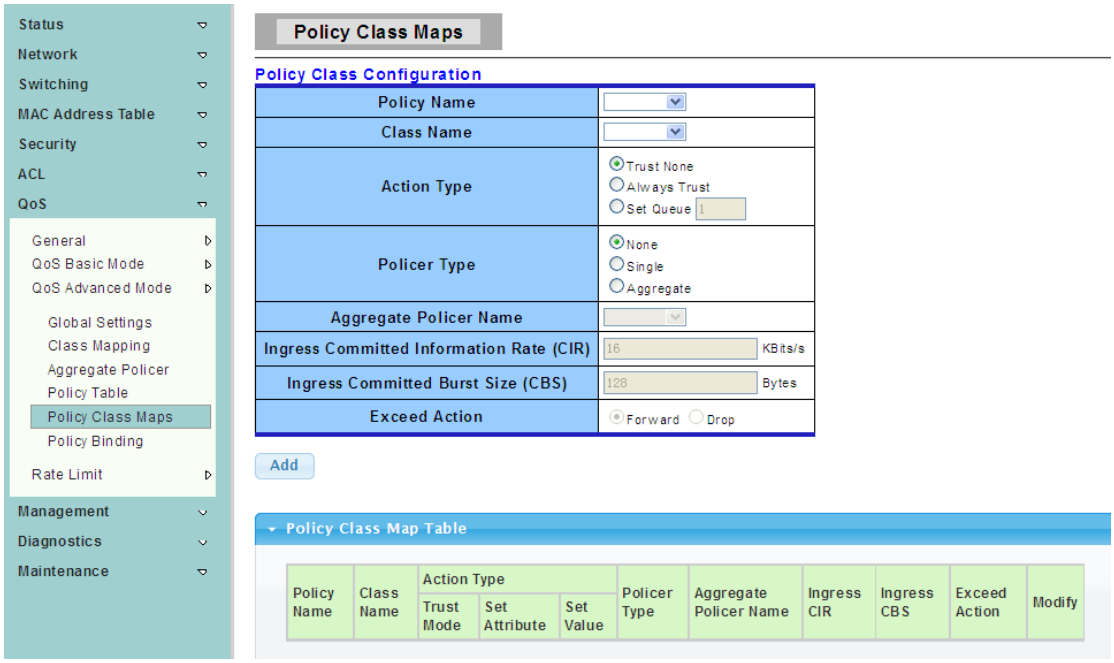
4.8.3.4 Policy Table

To display the Policy Configuration web page, click **QoS > QoS Advanced Mode > Policy Table**



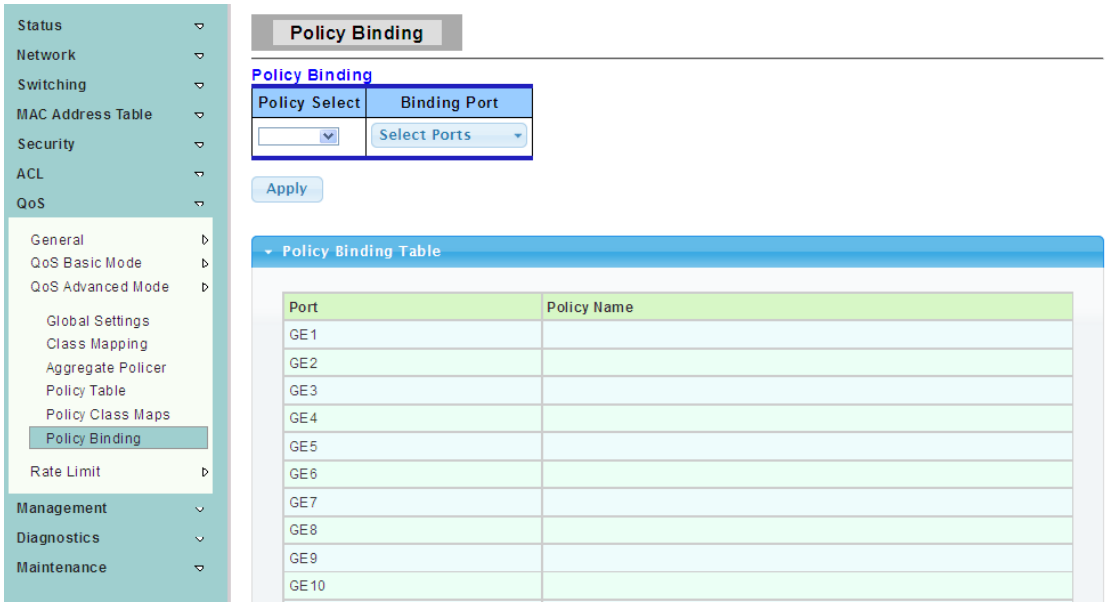
4.8.3.5 Policy Class Maps

To display the Policy Class Maps web page, click **QoS > QoS Advanced Mode > Policy Class Maps**



4.8.3.6 Policy Binding

To display the Policy Binding web page, click **QoS > QoS Advanced Mode > Policy Binding**

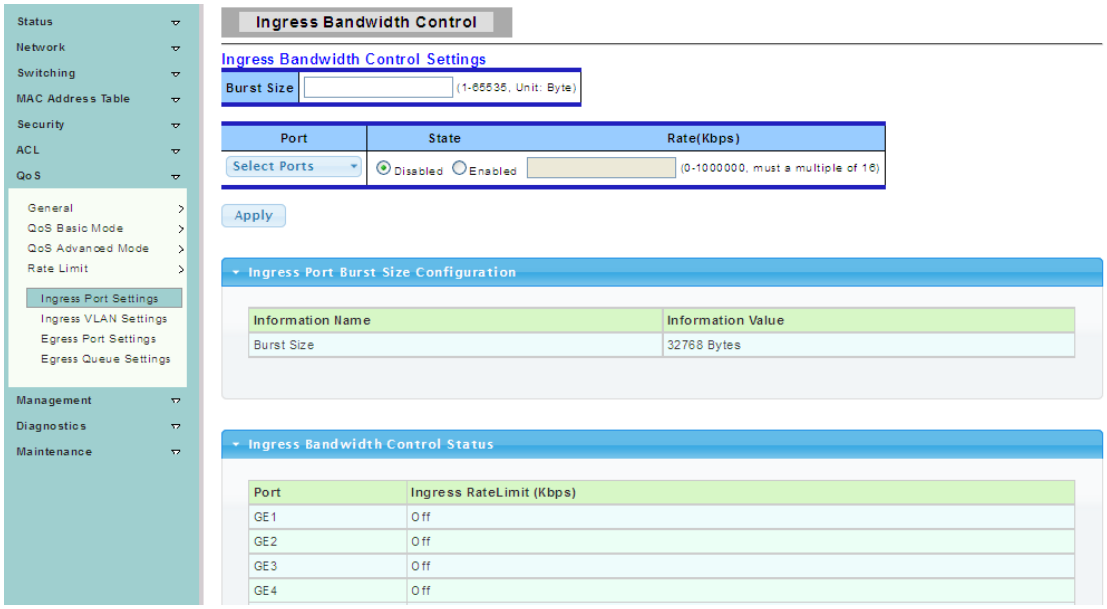


4.8.4 Rate Limit

4.8.4.1 Ingress Port Settings

To display the Ingress Bandwidth Control web page, click **QoS > Rate Limit > Ingress Port Settings**

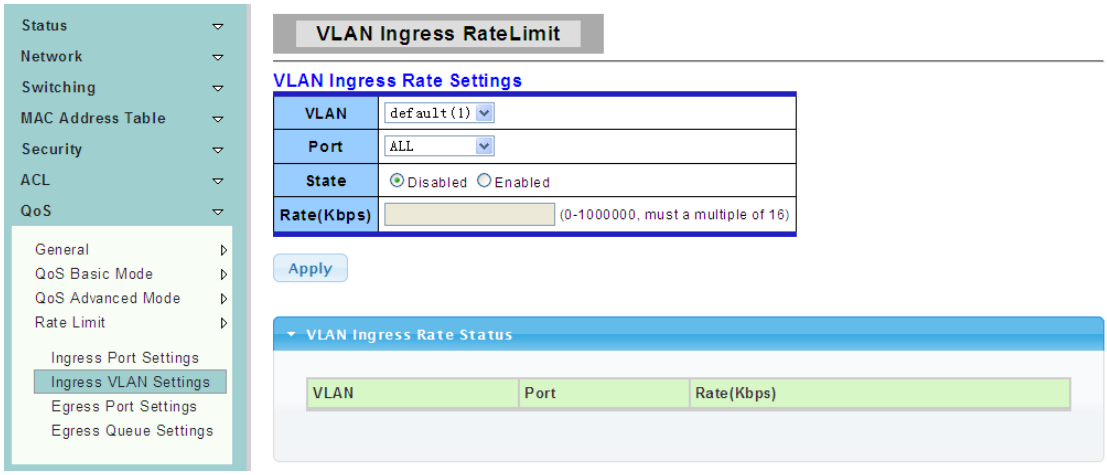
This page allow user to set ingress port monitor.



4.8.4.2 Ingress VLAN Settings

To display the VLAN Ingress RateLimit web page, click **QoS > Rate Limit > Ingress VLAN Settings**

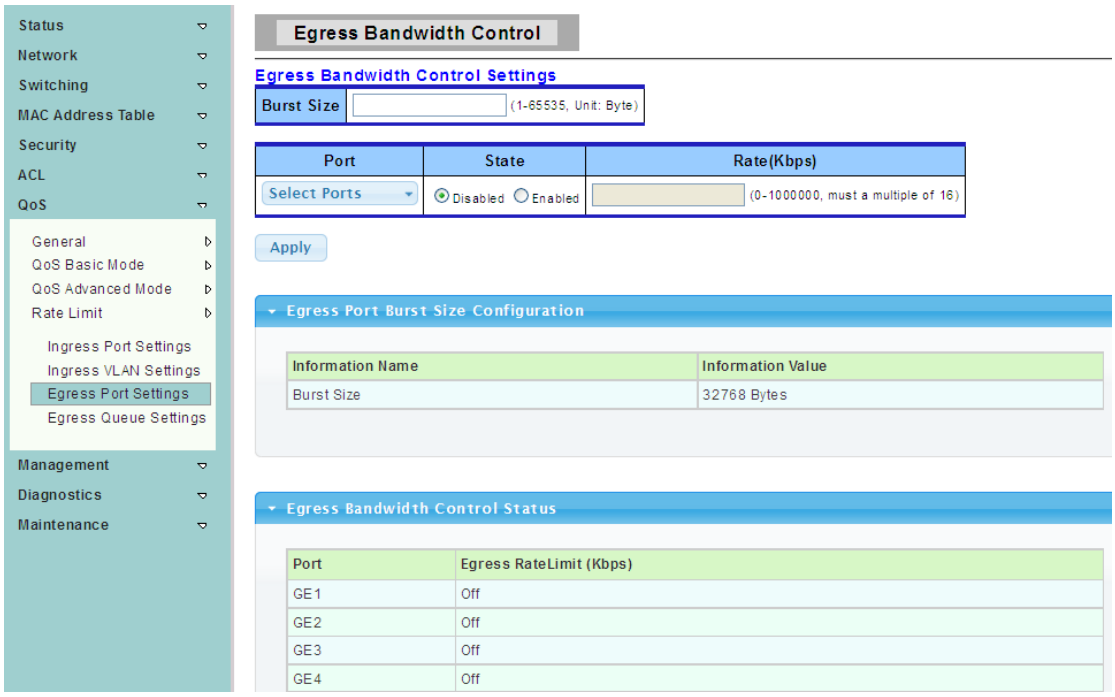
This page is used to set the bandwidth of the VLAN entry control**.**



4.8.4.3 Egress Port Settings

To display the Egress Bandwidth Control web page, click **QoS > Rate Limit > Egress Port Settings**

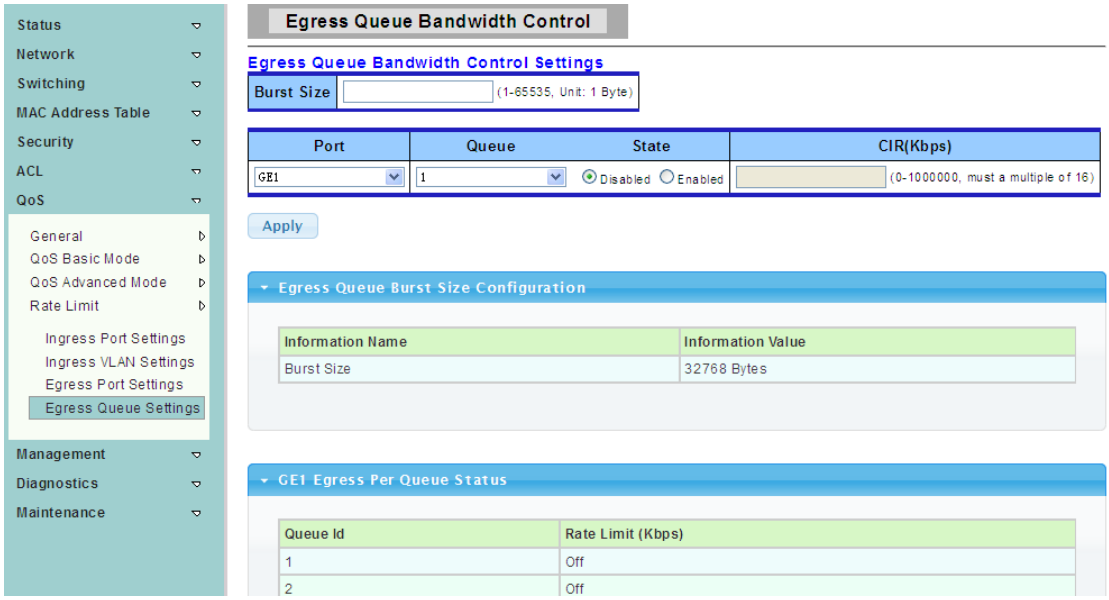
This page is used to set the egress port monitor.



4.8.4.4 Egress Queue Settings

To display the Egress Queue Bandwidth Control web page, click **QoS > Rate Limit > Egress Queue Settings**

The page is used to set the egress lined up bandwidth monitor.



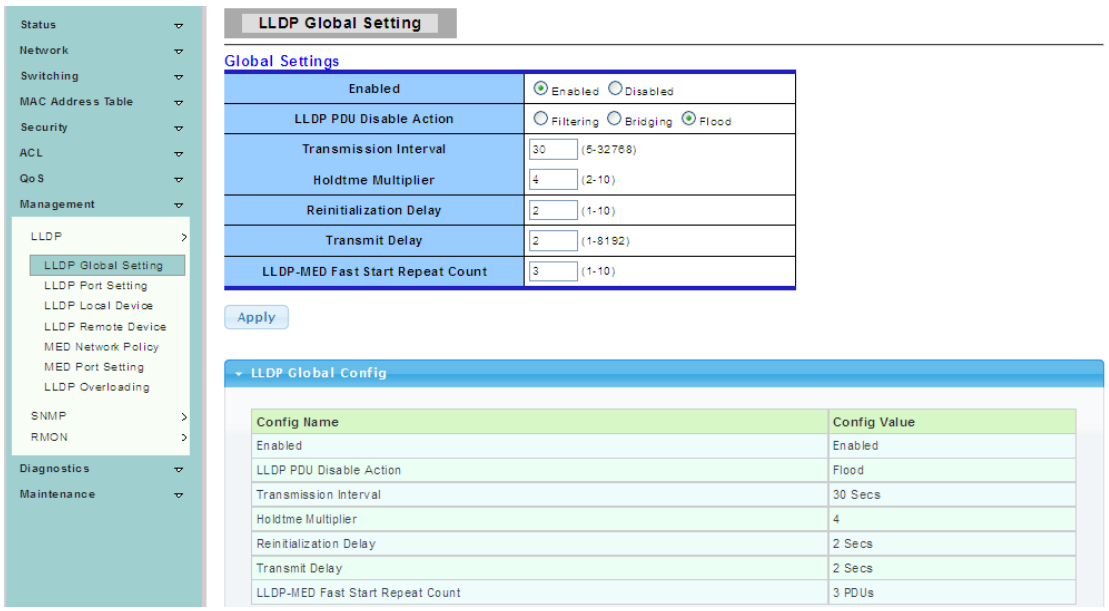
4.9 Management

4.9.1 LLDP

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

4.9.1.1 LLDP Global Setting

To display the LLDP Global Setting web page, click **Management > LLDP > LLDP Global Setting**



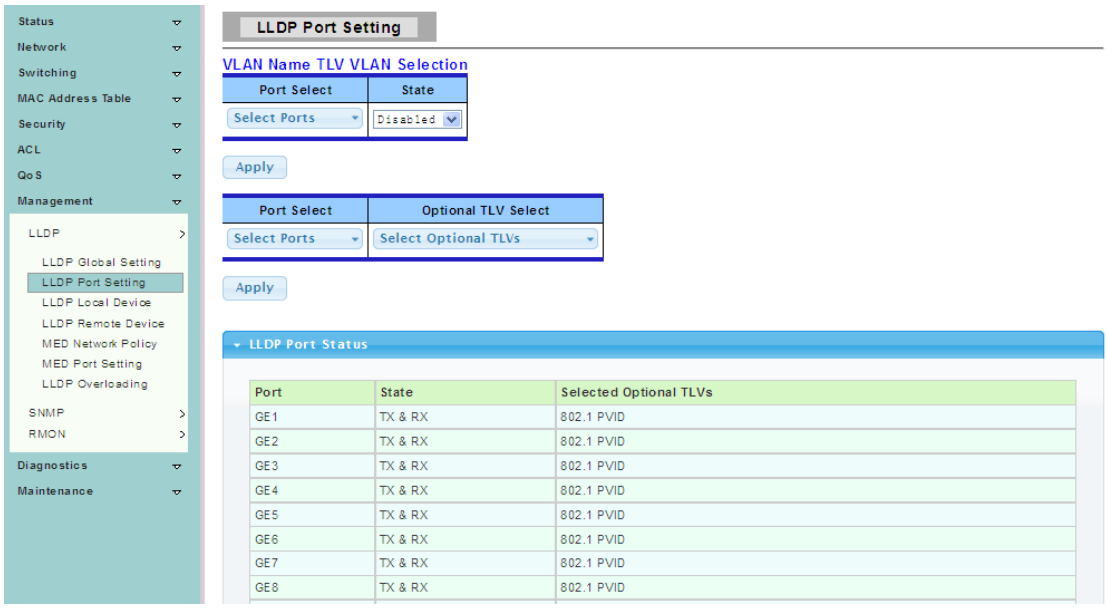
Enabled: Enable/Disable LLDP protocol on this switch.

Transmission Interval: Select the interval at which frames are transmitted. Thedefault is 30 seconds, and the valid range is 5–32768 seconds.

Holdtime Multiplier: Select the multiplier onthe transmit interval to assign to TTL (range 2–10, default = 4).
Reinitialization Delay: Select the delay before a re-initialization (range 1–10 seconds, default = 2).

4.9.1.2 LLDP Port Setting

To display the LLDP Port Setting web page, click **Management > LLDP > LLDP Port Setting**



Port Select: Select specified port or all ports to configure transmission state.
State: Select the transmission state of LLDP port interface.

- Disable: Disable the transmission of LLDP PDUs.
- RX Only: Receive LLDP PDUs only.
- TX Only: Transmit LLDP PDUs only.
- TX And RX: Transmit and receive LLDP PDUs both Select specified port or all port.

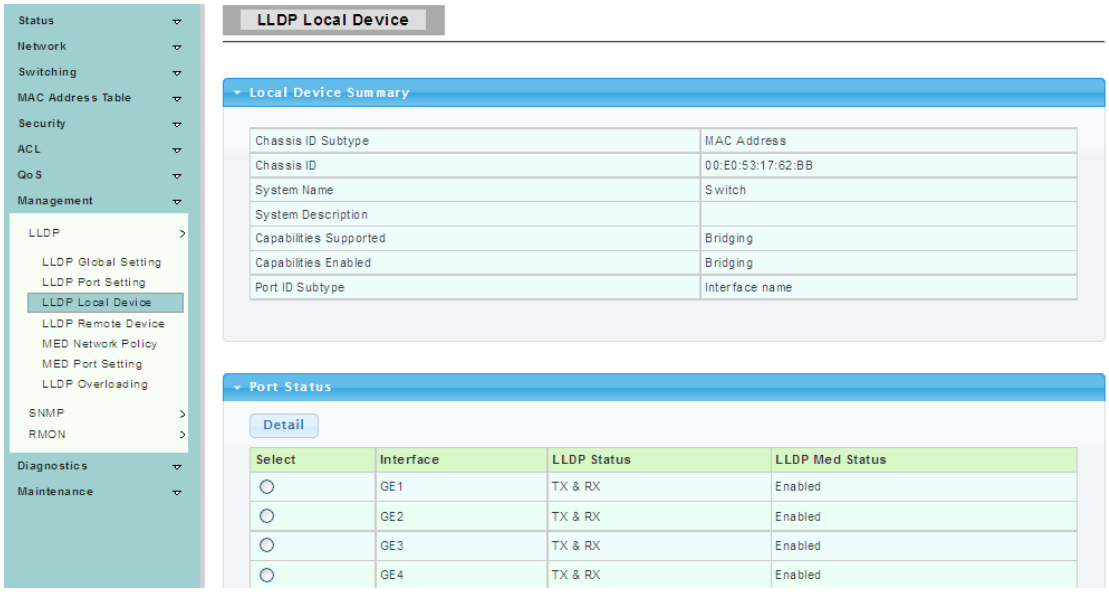
configure transmission state.

Port Select: Select specific ports.
Optional TLV Select: Select Optional TLVs.

4.9.1.3 LLDP Local Device

To display the LLDP Local Device web page, click **Management > LLDP > LLDP Local Device**

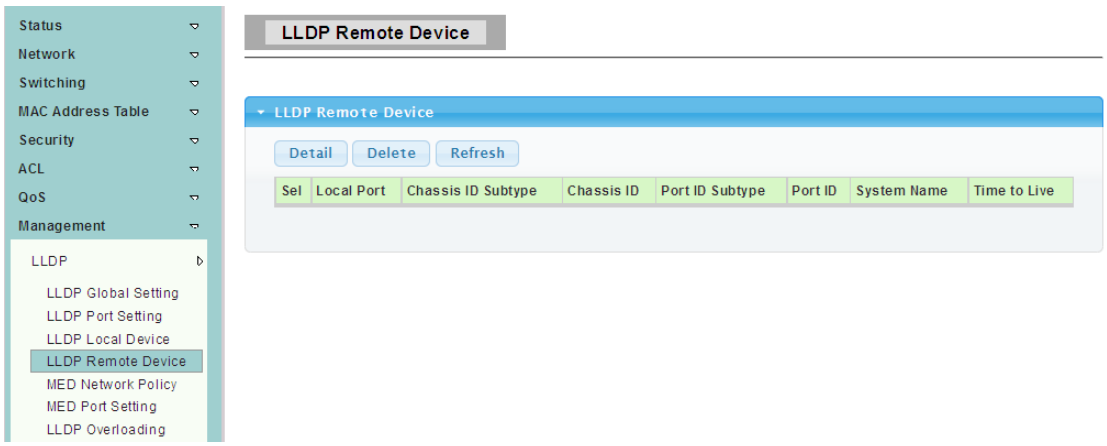
Use the LLDP Local Device page to view information about devices on the network for which the switch has received LLDP information.



4.9.1.4 LLDP Remote Device

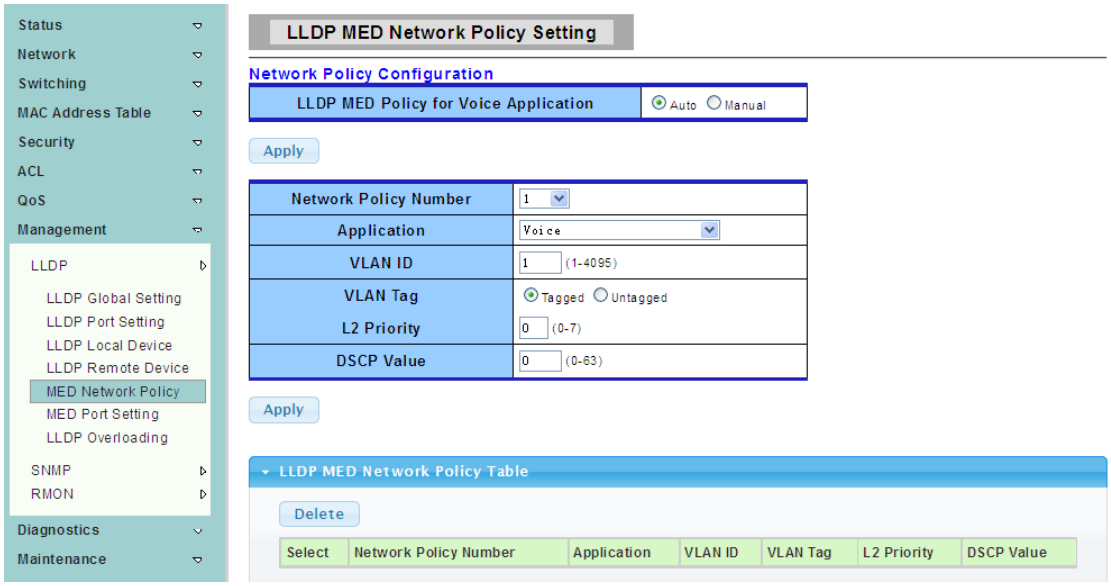
To display the LLDP Remote Device web page, click **Management > LLDP > LLDP Remote Device**

Use the LLDP Remote Device page to view information about remote devices for which the switch has received LLDP information.



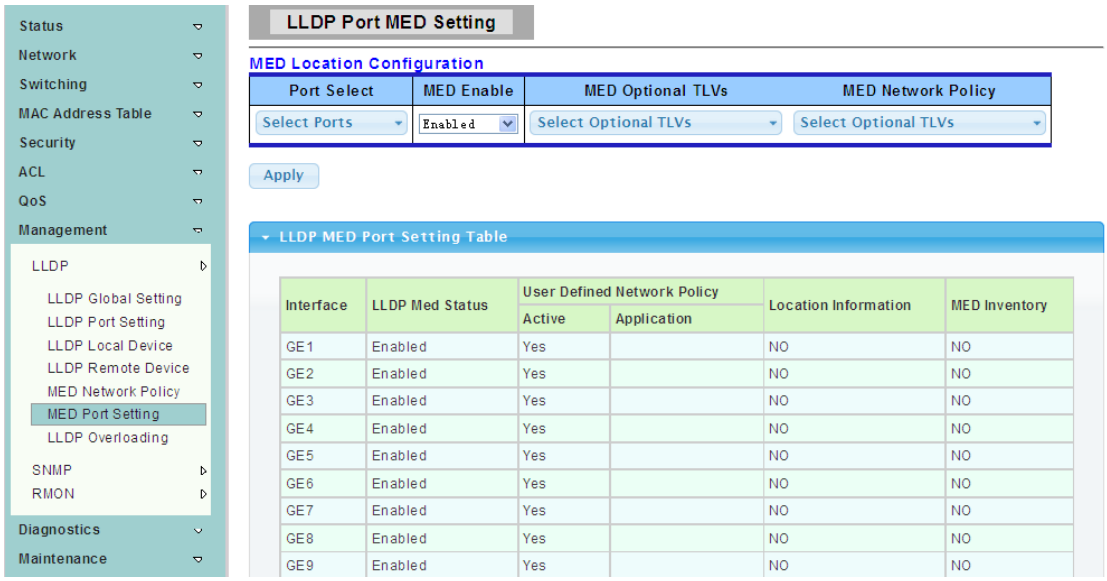
4.9.1.5 MED Network Policy

To display the LLDP MED Network Policy Setting web page, click **Management > LLDP > MED Network Policy**



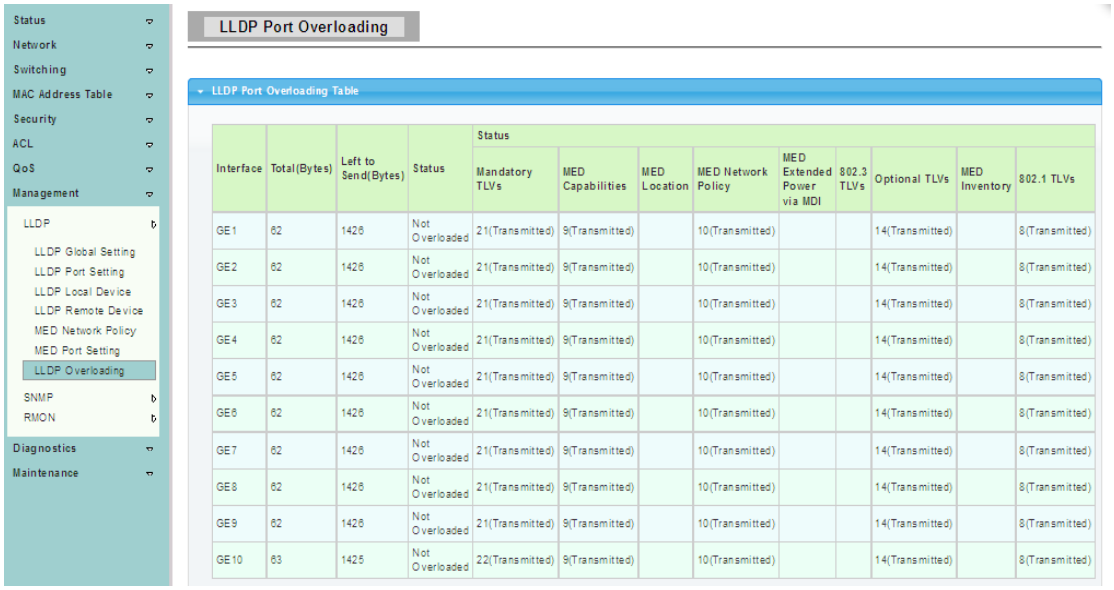
4.9.1.6 MED Port Setting

To display the LLDP Port MED Setting web page, click **Management > LLDP > MED Port Setting**



4.9.1.7 LLDP Overloading

To display the LLDP Port Overloading web page, click **Management > LLDP > LLDP Overloading**



Interface	Total(Bytes)	Left to Send(Bytes)	Status	Status								
				Mandatory TLVs	MED Capabilities	MED Location	MED Network Policy	MED Extended Power via MDI	802.3 TLVs	Optional TLVs	MED Inventory	802.1 TLVs
GE1	62	1426	Not Overloaded	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE2	62	1426	Not Overloaded	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE3	62	1426	Not Overloaded	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE4	62	1426	Not Overloaded	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE5	62	1426	Not Overloaded	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE6	62	1426	Not Overloaded	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE7	62	1426	Not Overloaded	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE8	62	1426	Not Overloaded	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE9	62	1426	Not Overloaded	21(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)
GE10	63	1425	Not Overloaded	22(Transmitted)	9(Transmitted)		10(Transmitted)			14(Transmitted)		8(Transmitted)

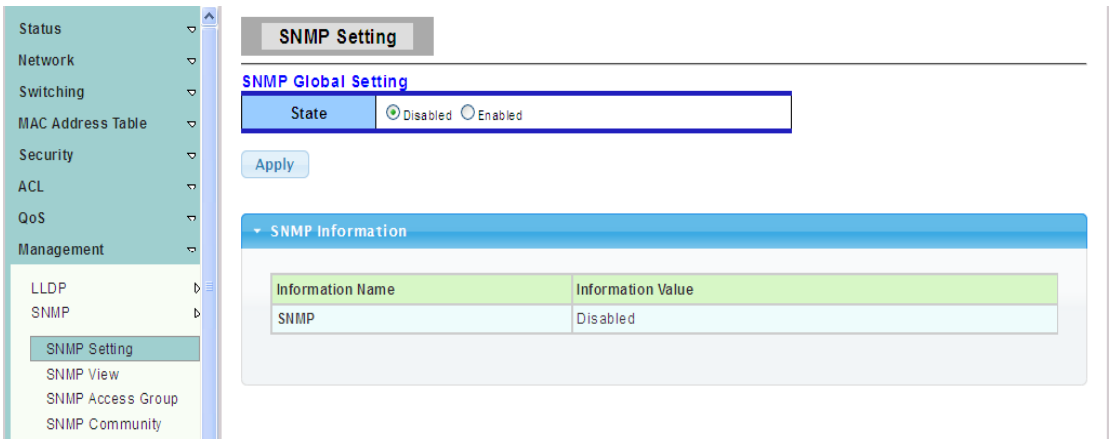
Total (Bytes): Total number of bytes of LLDP information in each packet.
Left to Send (Bytes): Total number of available bytes left for additional LLDP information in each packet.
Status: Whether TLVs are being transmitted or if they are overloaded.

4.9.2 SNMP

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the Switch, switch group or network.

4.9.2.1 SNMP Setting

To display the SNMP Setting web page, click **Management > SNMP > SNMP Setting**



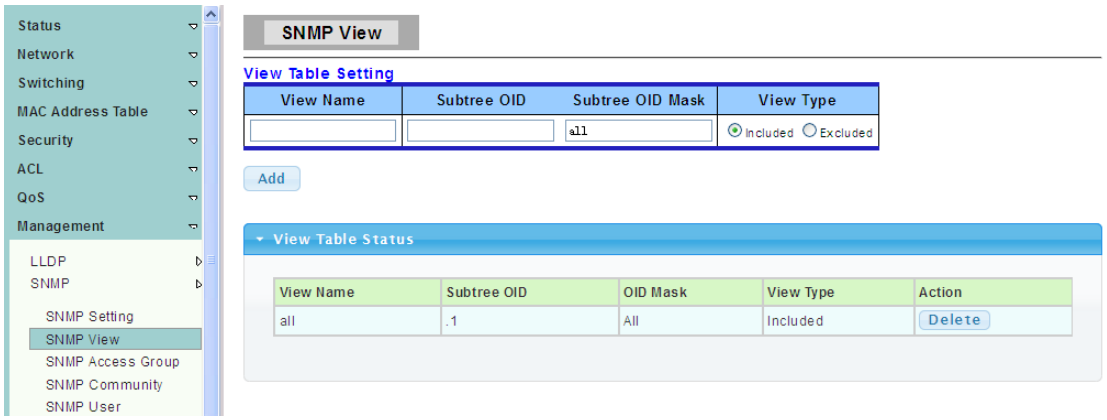
State: SNMP daemon state

- Enabled: Enable SNMP daemon
- Disabled: Disable SNMP daemon

4.9.2.2 SNMP View

To display the SNMP View web page, click **Management > SNMP > SNMP View**

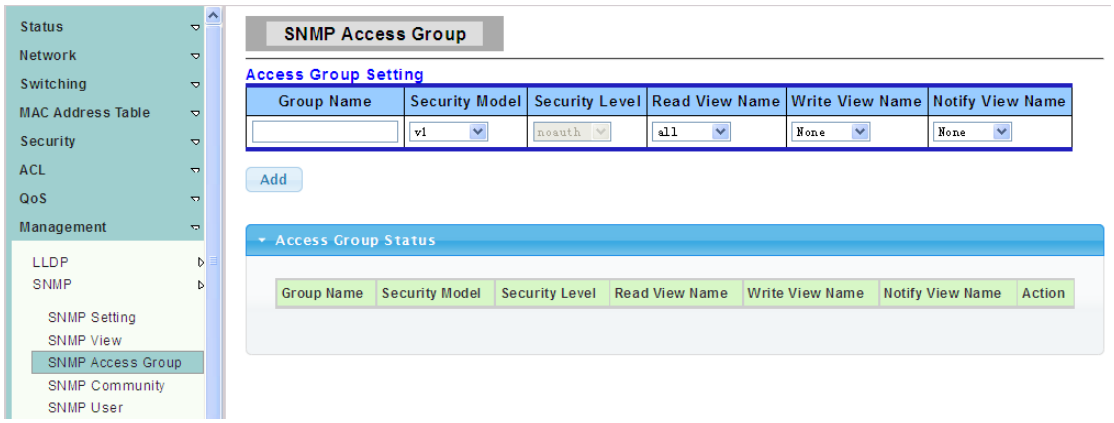
This page is used to configure SNMP view. Used in the SNMP message Management variables (OID) to describe the switch in the Management object, MIB (Management Information Base, Management Information Base) is a set of the monitoring network equipment Management variables. View is used to control variable is how to be managed.



4.9.2.3 SNMP Access Group

To display the SNMP Access Group web page, click **Management > SNMP > SNMP Access Group**

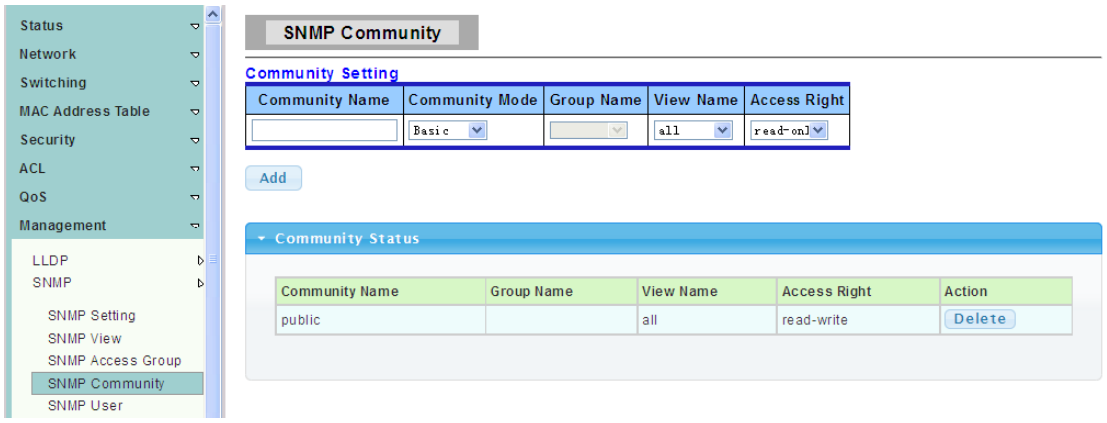
This page is used to configure SNMP group, Within the group by the user read-only, only write, inform the view to achieve the goal of access control.



4.9.2.4 SNMP Community

To display the SNMP Community web page, click **Management > SNMP > SNMP Community**

SNMP v1 and the SNMP v2c USES the group Name (Community Name) certification, the group has played a role similar to the password. If use SNMP v1 and SNMP v2c, after configuration view, can be directly on this page to configure SNMP community.



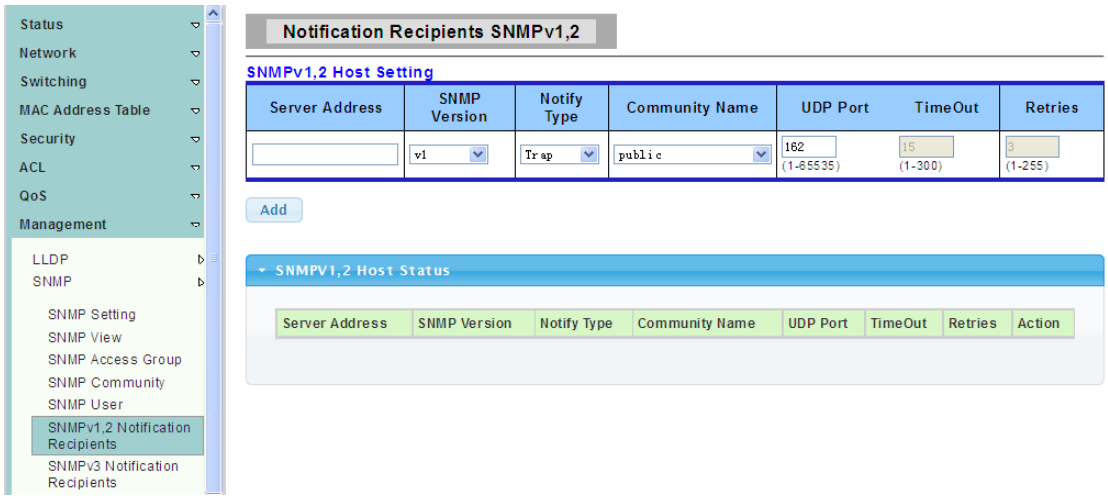
4.9.2.5 SNMP User

To display the SNMP User Table web page, click **Management > SNMP > SNMP User**

This page is used to create SNMP user under the group, And the group with the same level of security and access control permissions.

4.9.2.6 SNMPv1,2 Notification Recipients

To display the Notification Recipients SNMPv1,2 web page, click **Management > SNMP > SNMPv1,2 Notification Recipients**

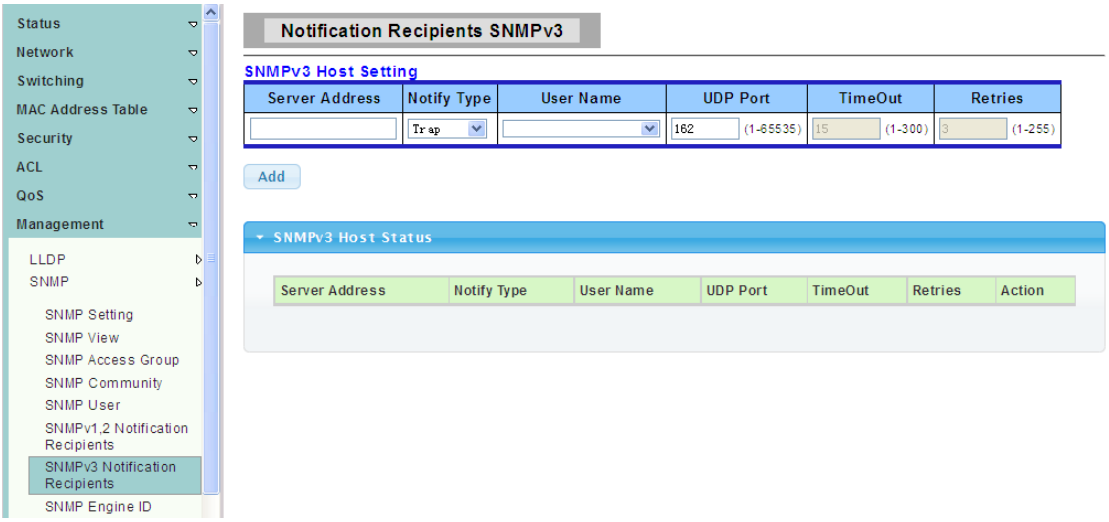


SNMPv1,2 version notification event receiving host related configuration, you can configure to inform the host in the form of the trap message or log information about the

current equipment, can be set up group name, UDP port number and message of the timeout.

4.9.2.7 SNMPv3 Notification Recipients

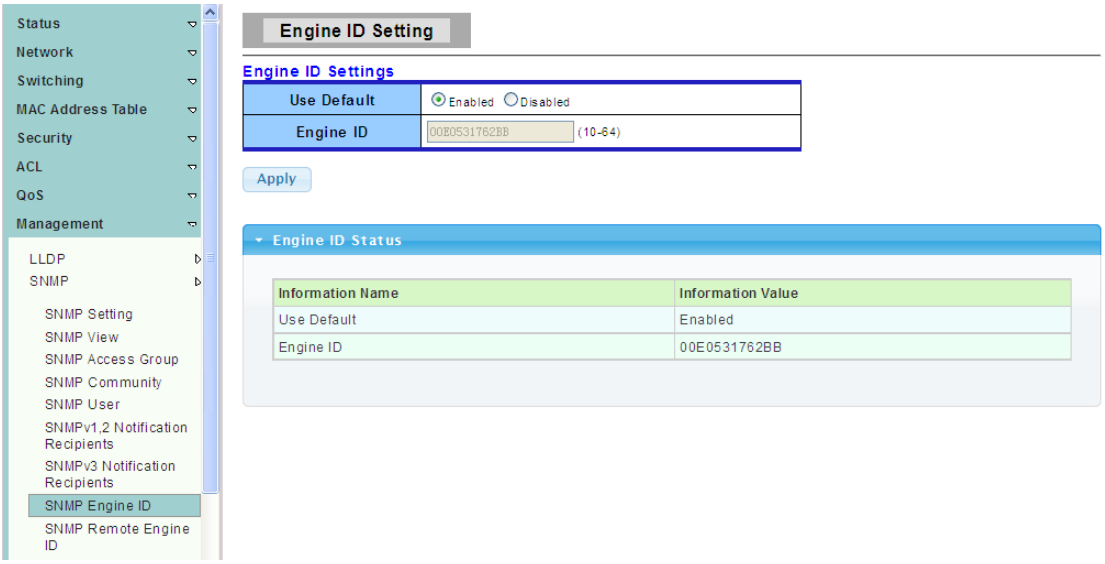
To display the Notification Recipients SNMPv3 web page, click **Management > SNMP > SNMPv3 Notification Recipients**



SNMPv3 version notification event receiving host related configuration, you can configure to inform the host in the form of the trap message or log information about the current equipment, can be set up group name, UDP port number and message of the timeout.

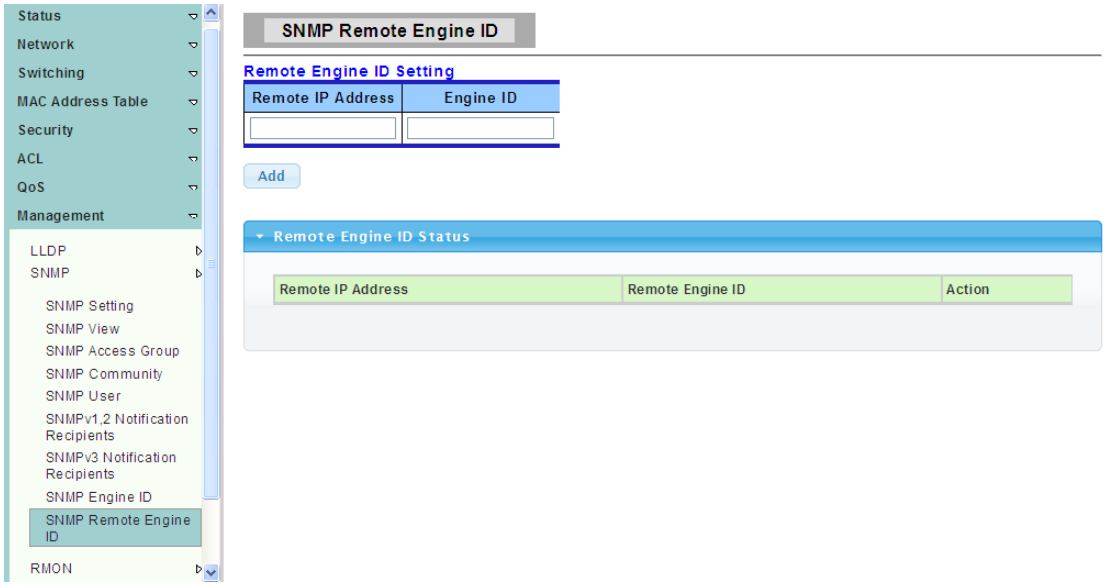
4.9.2.8 SNMP Engine ID

To display the Engine ID Setting web page, click **Management > SNMP > SNMP Engine ID**



4.9.2.9 SNMP Remote Engine ID

To display the SNMP Remote Engine ID web page, click **Management > SNMP > SNMP Remote Engine ID**



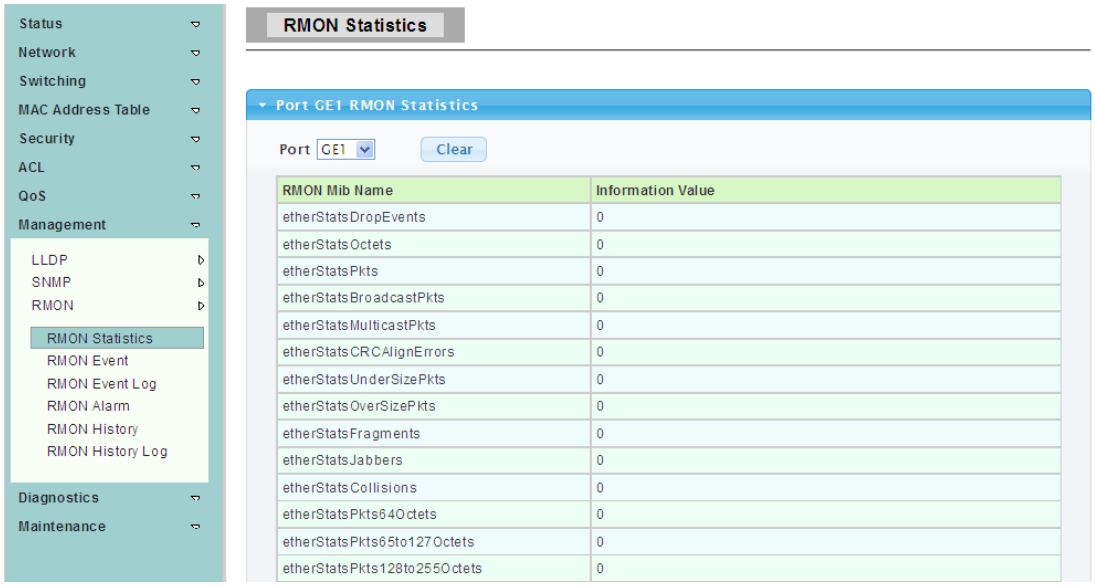
4.9.3 RMON

Remote Monitoring. A subset of SNMP MIB II that allows monitoring and management capabilities by addressing up to ten different groups of information.

4.9.3.1 RMON Statistics

To display the RMON Statistics web page, click **Management > RMON > RMON Statistics**

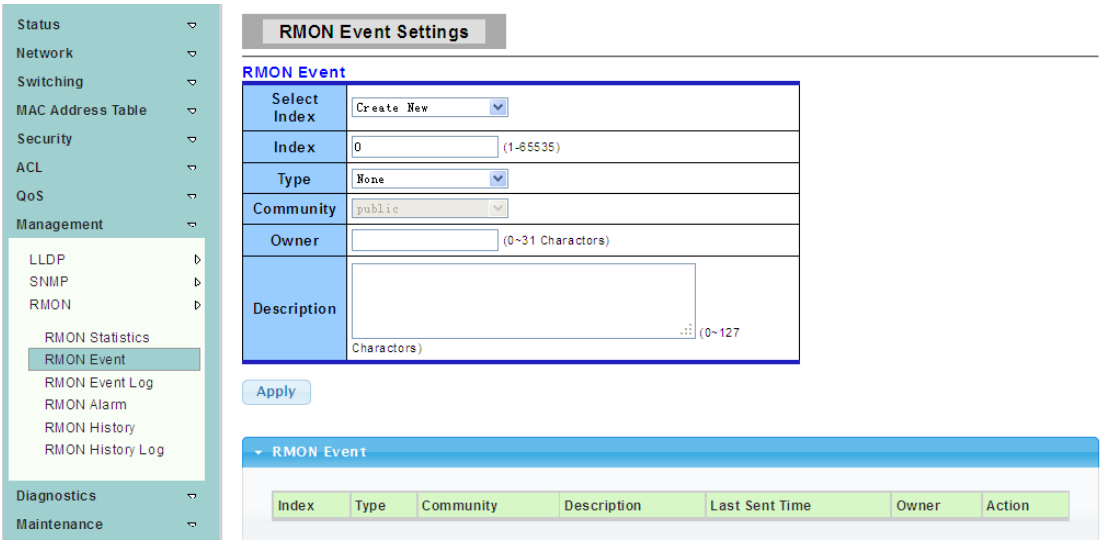
The Statistics page displays detailed information regarding packet sizes and information regarding physical layer errors. The information displayed is according to the RMON standard.



4.9.3.2 RMON Event

To display the RMON Event Settings web page, click **Management > RMON > RMON Event**

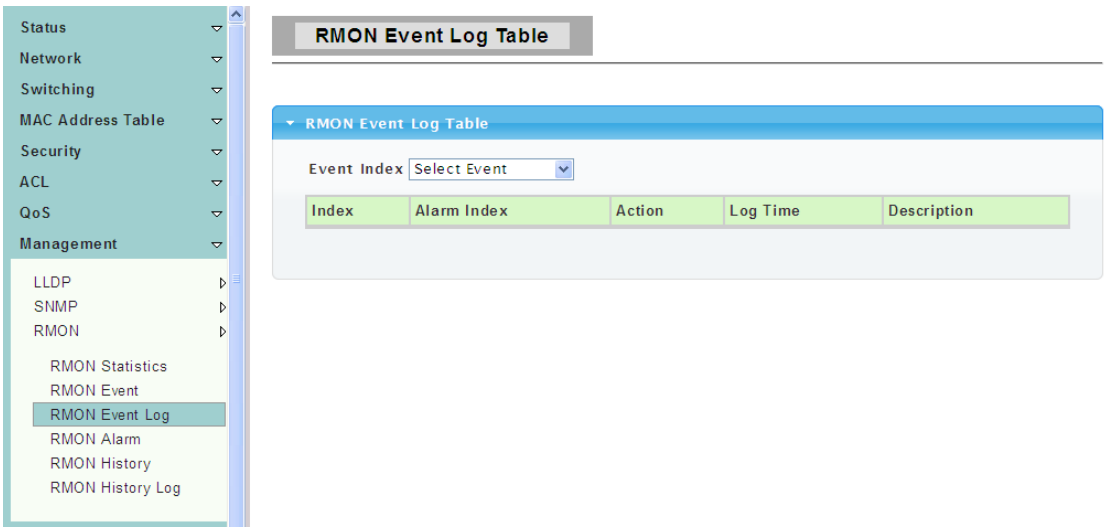
This page is used to configure RMON event group.



4.9.3.3 RMON Event Log

To display the RMON Event Log Table web page, click **Management > RMON > RMON Event Log**

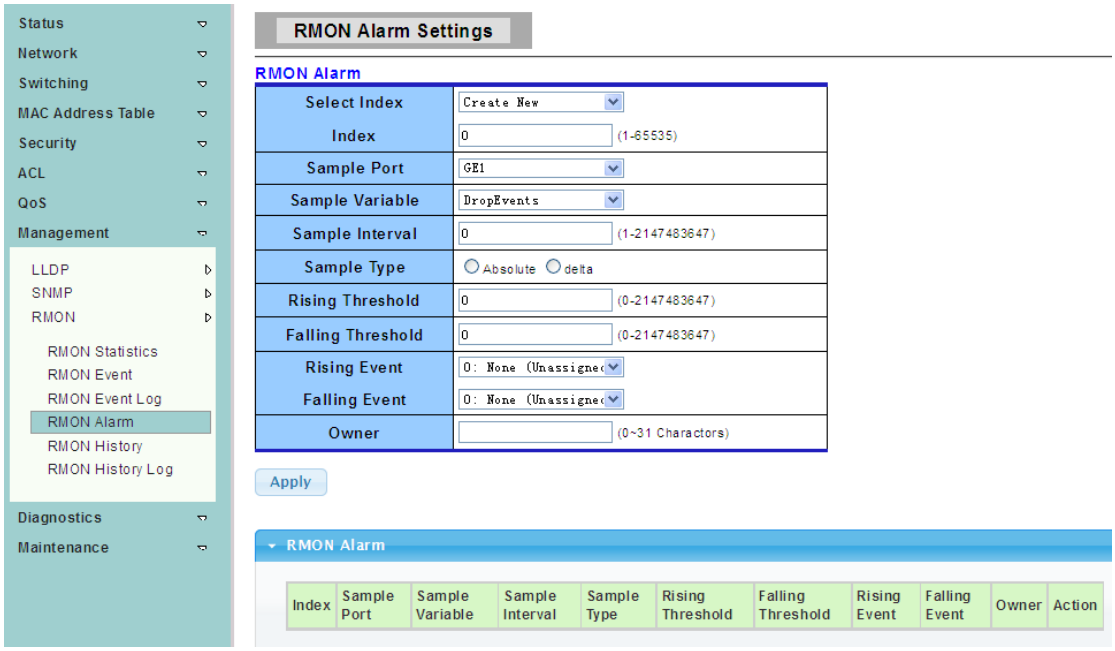
The Event Log Table page displays the log of events(actions) that occurred. Two types of events can be logged: Log or Log and Trap. The action in the event is performed when the event is bound to an alarm(see the Alarms page) and the conditions of the alarm have occurred.



4.9.3.4 RMON Alarm

To display the RMON Alarm Settings web page, click **Management > RMON > RMON Alarm**

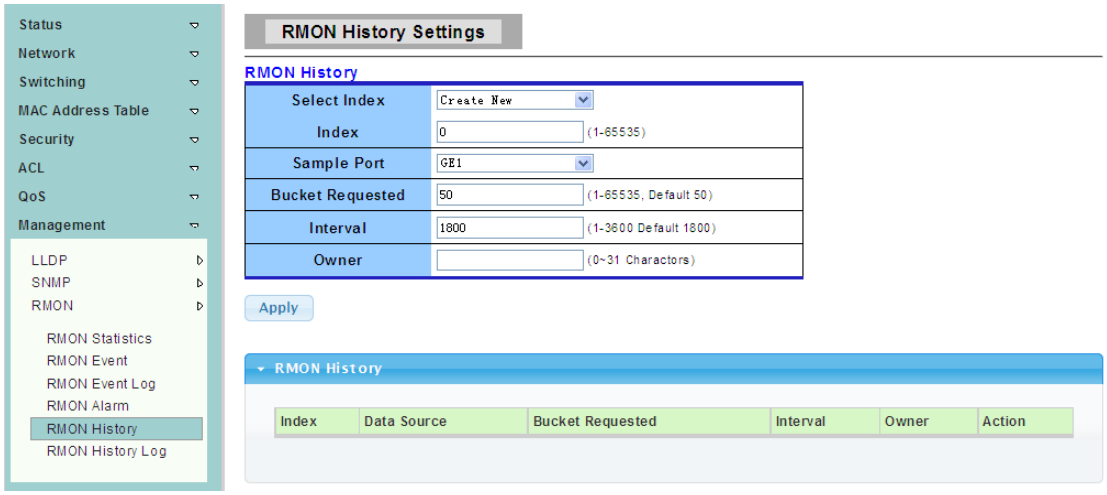
This page is used to configure RMON statistics group and alarm group.



4.9.3.5 RMON History

To display the RMON History Settings web page, click **Management > RMON > RMON History**

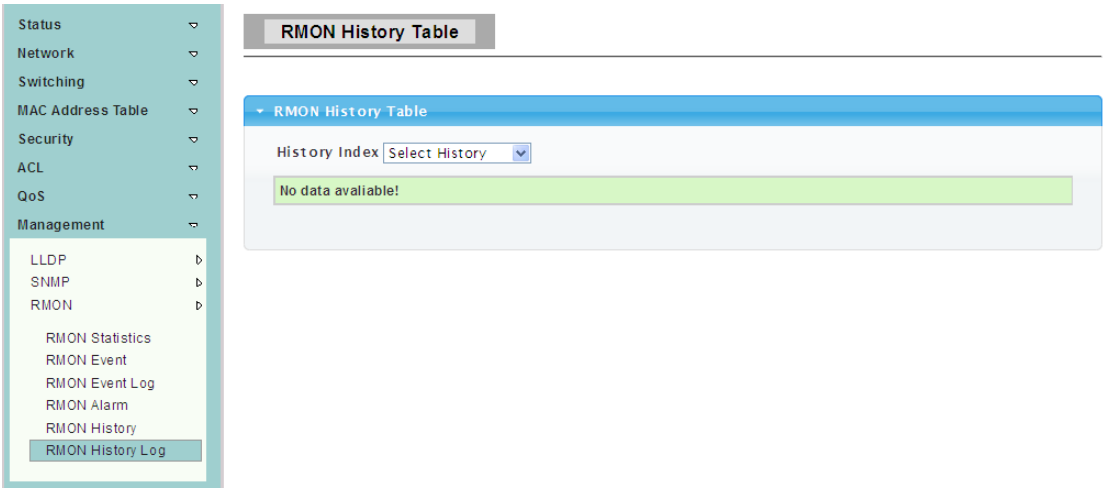
This page is used to configure the PMON history group.



4.9.3.6 RMON History Log

To display the RMON History Table web page, click **Management > RMON > RMON History Log**

The RMON History Log Table page displays interface-specific statistical network sampling. The samples were configured in the History Control table described above.



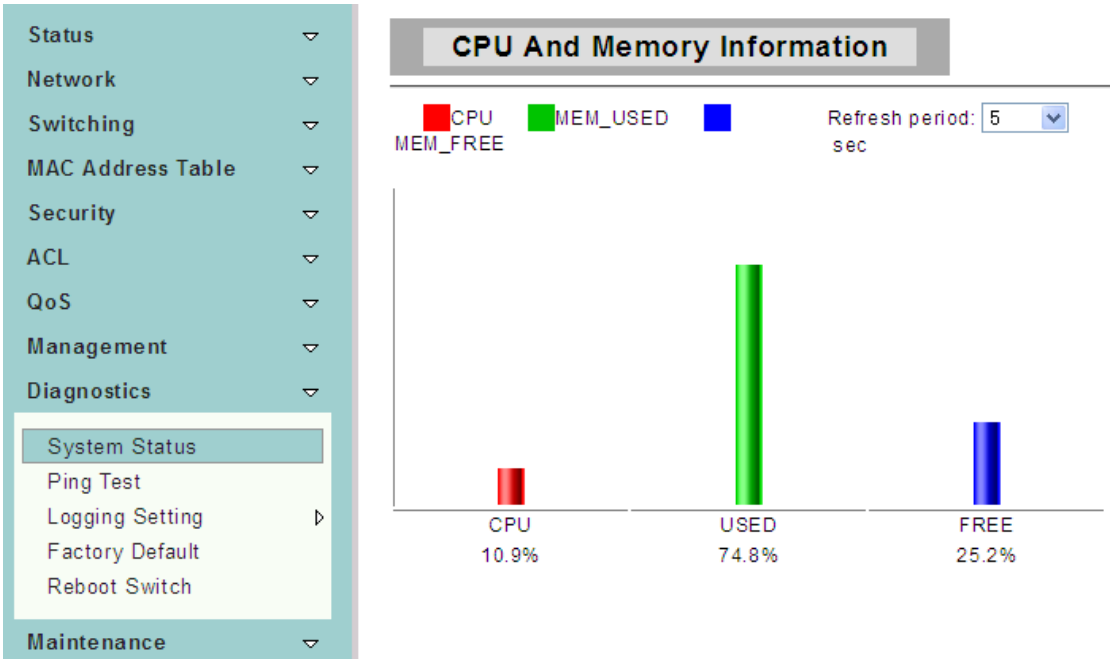
4.10 Diagnostics

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

4.10.1 System Status

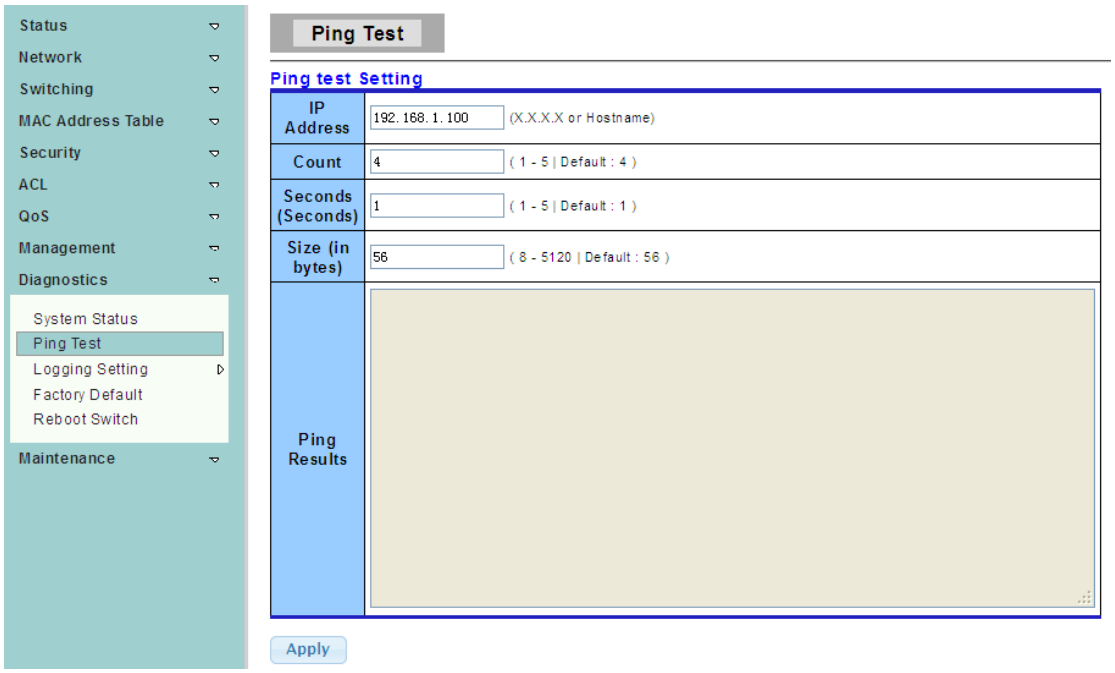
To display the CPU And Memory Information web page, click **Diagnostics > System Status**

This page is used to display the state of the system operation, CPU resource utilization, used memory and free memory rate, and set the refresh time.



4.10.2 Ping Test

To display the Ping Test web page, click **Diagnostics > Ping Test**



IP Address: The IP address of ping target.

Count: How many times to send ping request packet.

Interval: Time interval between each ping request packet.

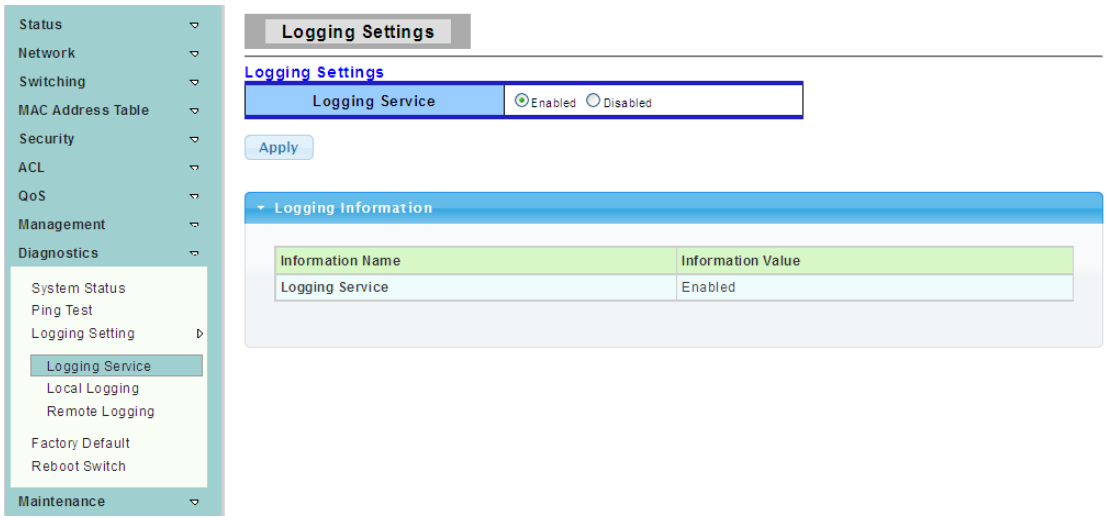
Size: The size of ping packet.

Ping Results: After ping finished, results will show in this field.

4.10.3 Logging Setting

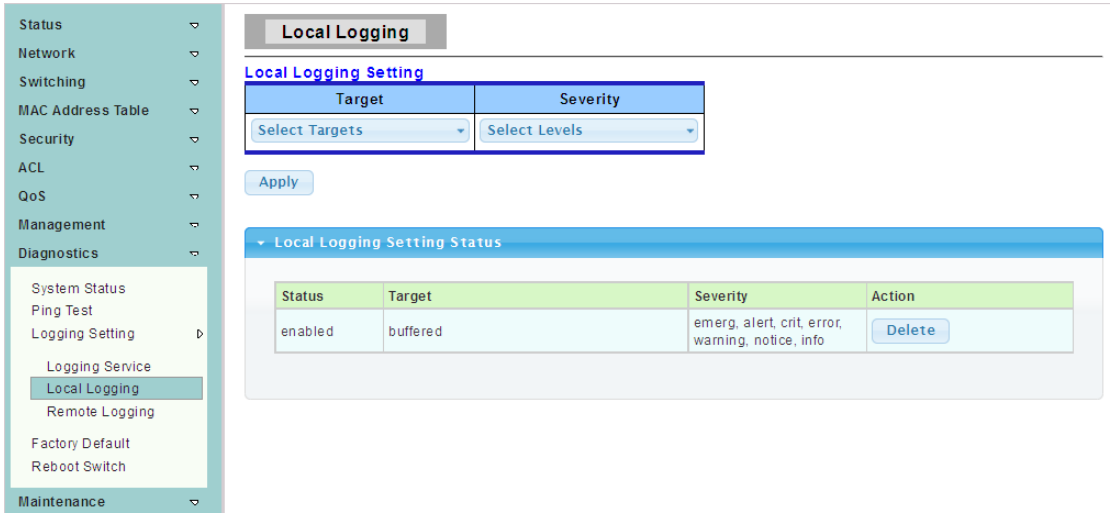
4.10.3.1 Logging Service

To display the Logging Settings web page, click **Diagnostics > Logging Setting > Logging Service**



4.10.3.2 Local Logging

To display the Local Logging web page, click **Diagnostics > Logging Setting > Local Logging**



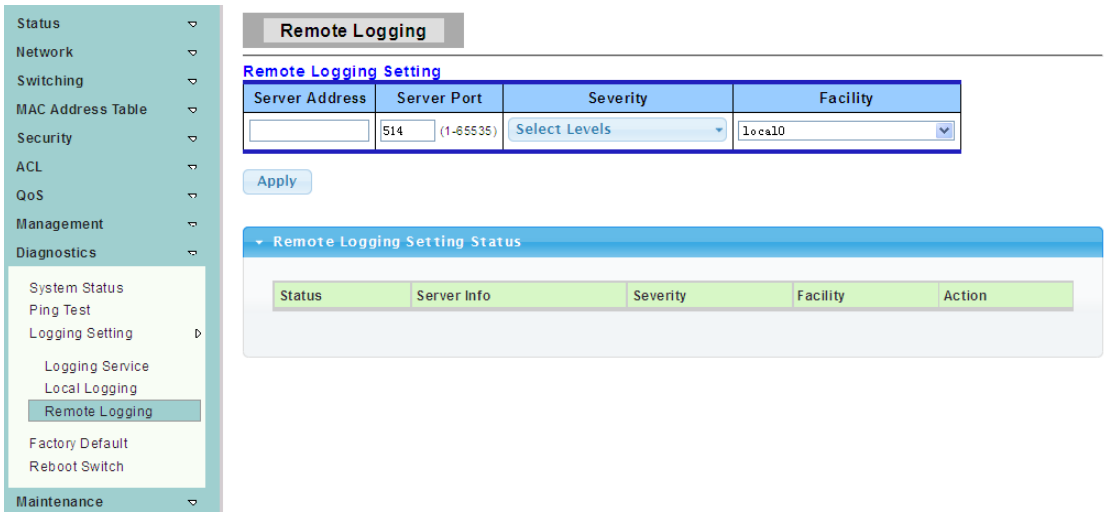
Target: Select the target to store log message.

- buffered: Store log messages in buffered. All log messages will disappear after system reboot.
- flash: Store log messages in flash. All log messages will not disappear after system reboot.

Severity: Select severity of log messages which will be stored.

4.10.3.3 Remote Logging

To display the Remote Logging web page, click **Diagnostics > Logging Setting > Remote Logging**



Server Address: The IP address of remote log server.
Server Port: The Port number of remote log server.
Severity: Select severity of log messages which will be sent.

4.10.4 Factory Default

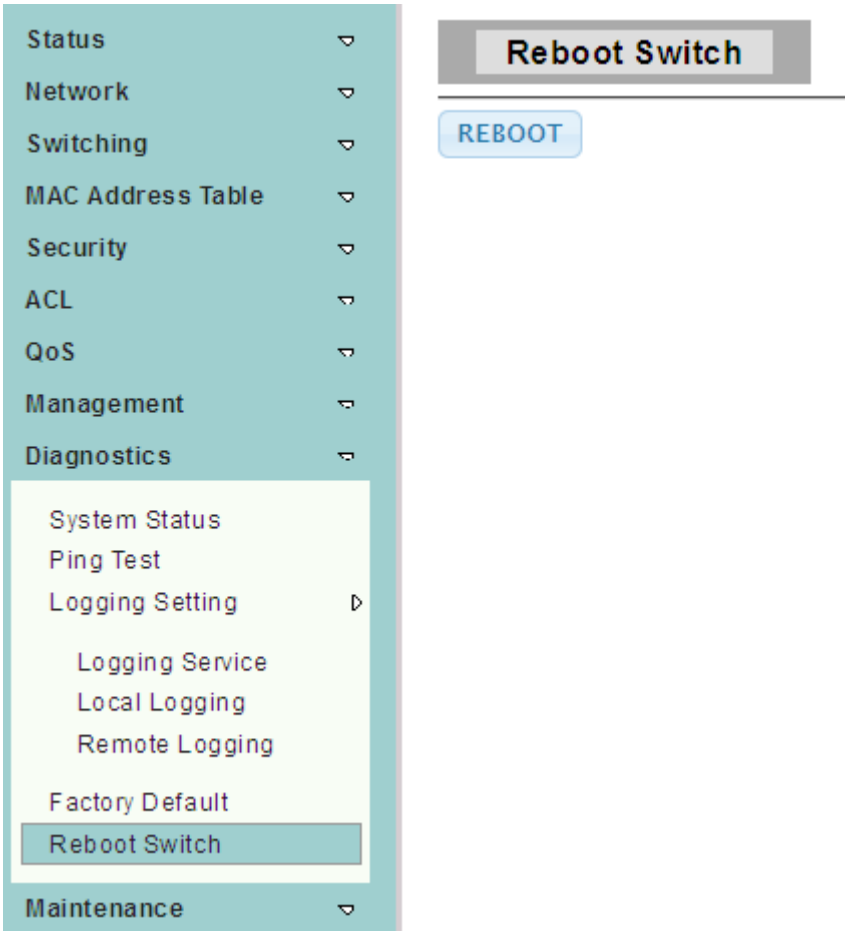
To display the Factory Default web page, click **Diagnostics > Factory Default**

This page allow user to restore switch to factory default by click the “Restore” button.

4.10.5 Reboot Switch

To display the Reboot Switch web page, click **Diagnostics > Reboot Switch**

This page allow user to reboot the switch by click the “Reboot” button.



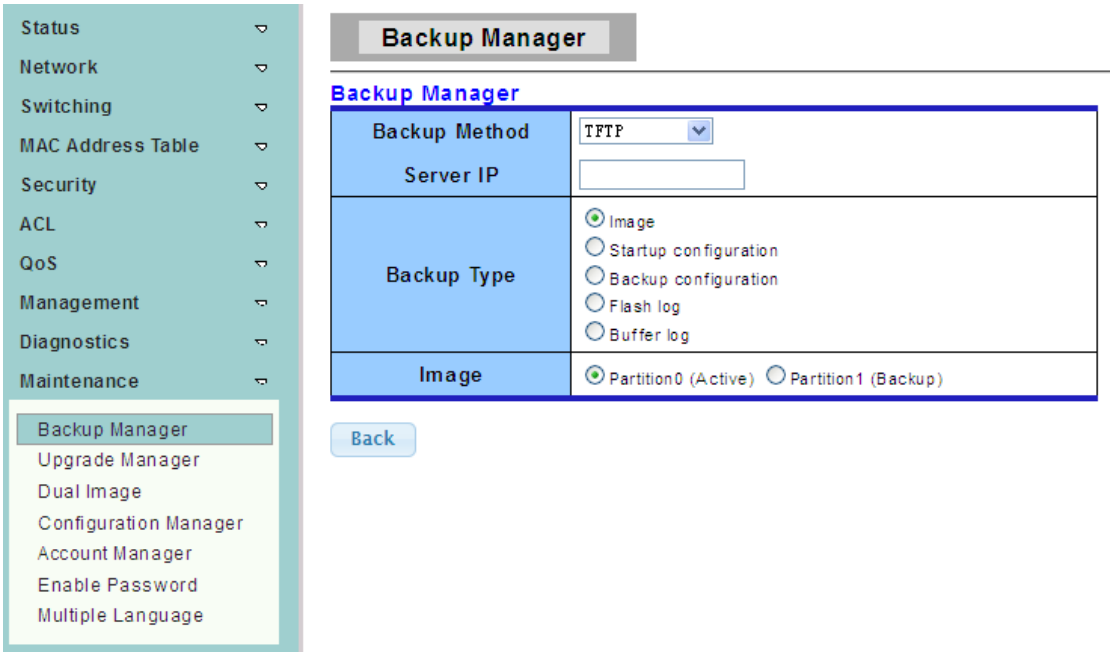
4.11 Maintenance

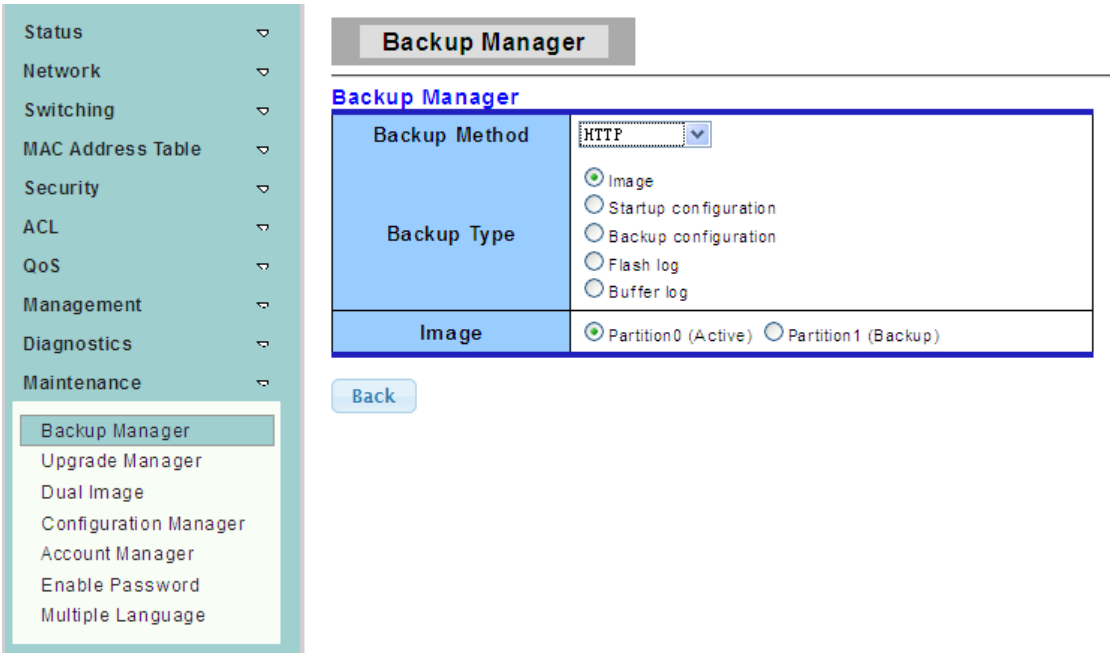
Use the Maintenance pages to configure settings for the switch network interface and how the switch connects to a remote server to get services.

4.11.1 Backup Manager

To display the Backup Manager web page, click **Maintenance > Backup Manager**

This page allow user to backup the firmware image or configuration file on the switch to remote TFTP server or host file system through HTTP protocol.





Backup Method: Select backup method.

- TFTP: Use TFTP to backup
- HTTP: Use HTTP to backup

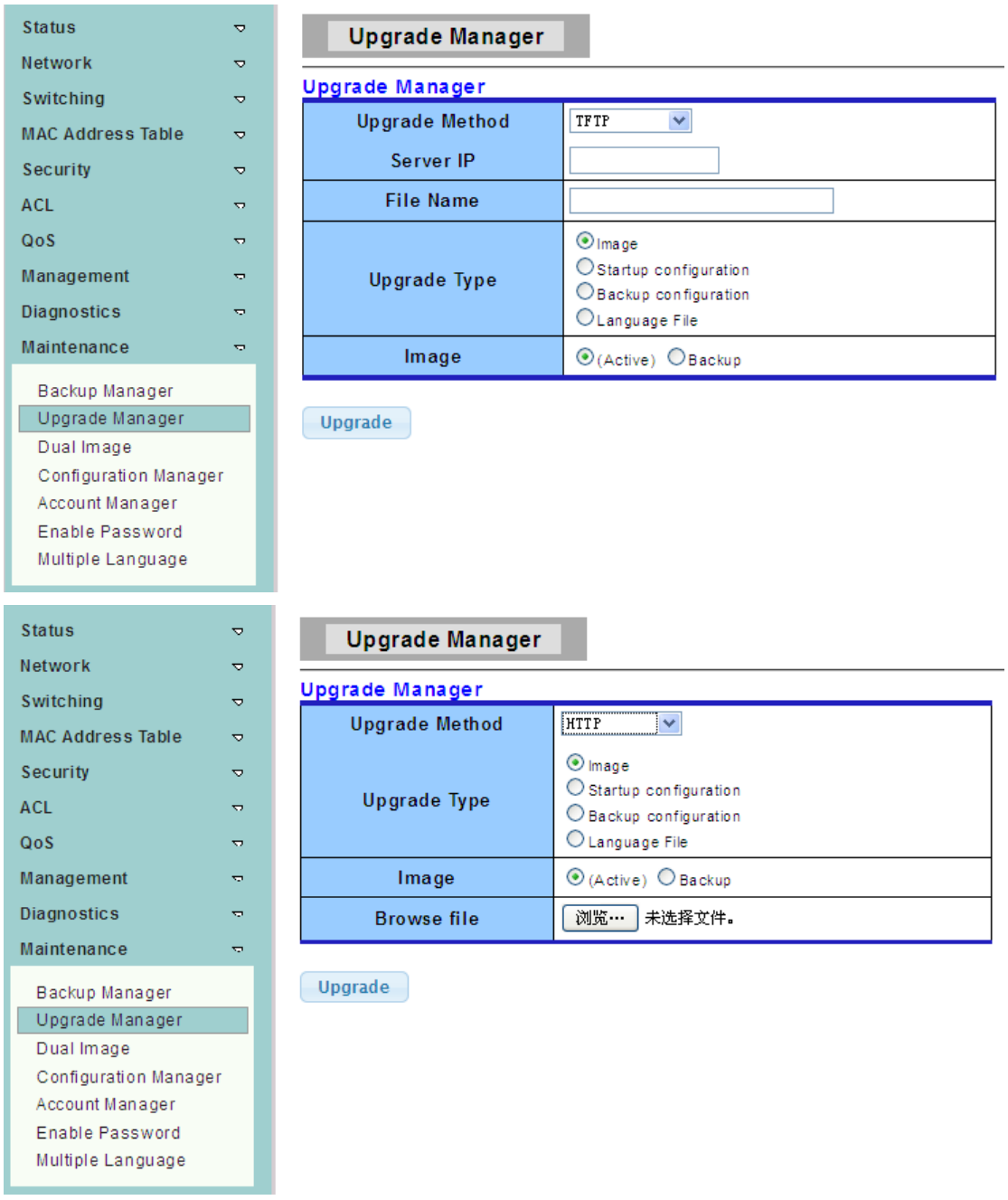
Server IP: IP address of the TFTP server. If the TFTP backup method is selected, the IP address of the TFTP server must be assigned.

Backup Type: Select Backup Type.

4.11.2 Upgrade Manager

To display the Upgrade Manager web page, click **Maintenance > Upgrade Manager**

This page allow user to upgrade new firmware image or configuration file to the switch from remote TFTP server or select file from web browser.



Upgrade Method: Select upgrade method.

- TFTP: Use TFTP to upgrade
- HTTP: Use HTTP to upgrade

Server IP: IP address of the TFTP server. If the TFTP upgrade method is selected, the IP address of the TFTP server must be assigned.

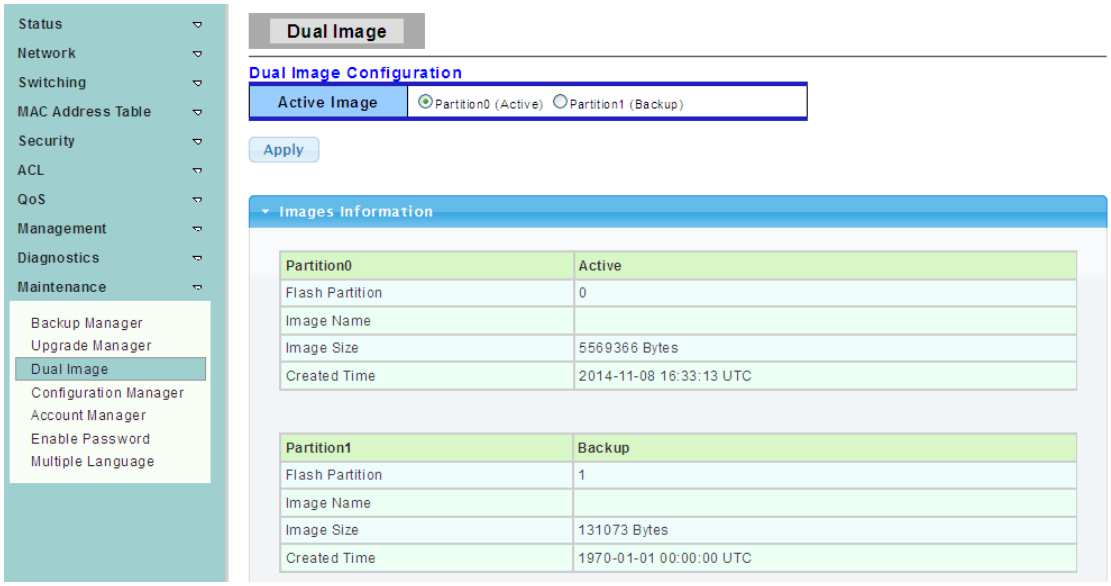
File Name: Firmware image or configuration file name on remote TFTP server. If the TFTP upgrade method is selected, the file name must be specified.

Browse file: If the HTTP upgrade method is selected, the browse file field allow you to select any file on host operating system.

Upgrade Type: Select Backup Type.

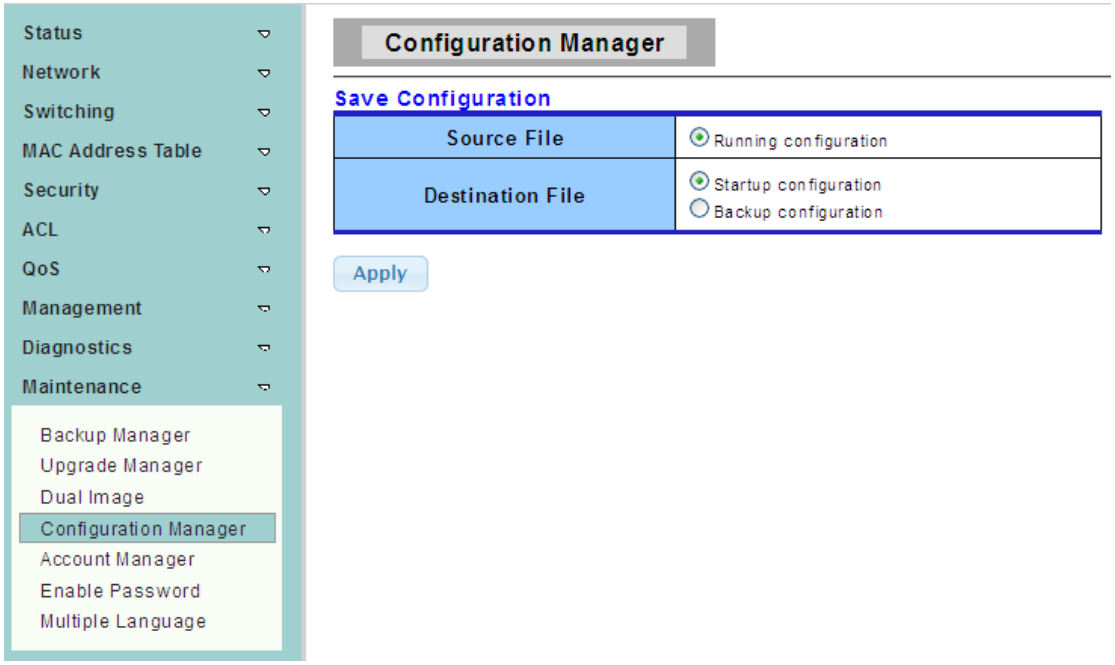
4.11.3 Dual Image

To display Dual Image web page, click **Maintenance > Dual Image**



4.11.4 Configuration Manager

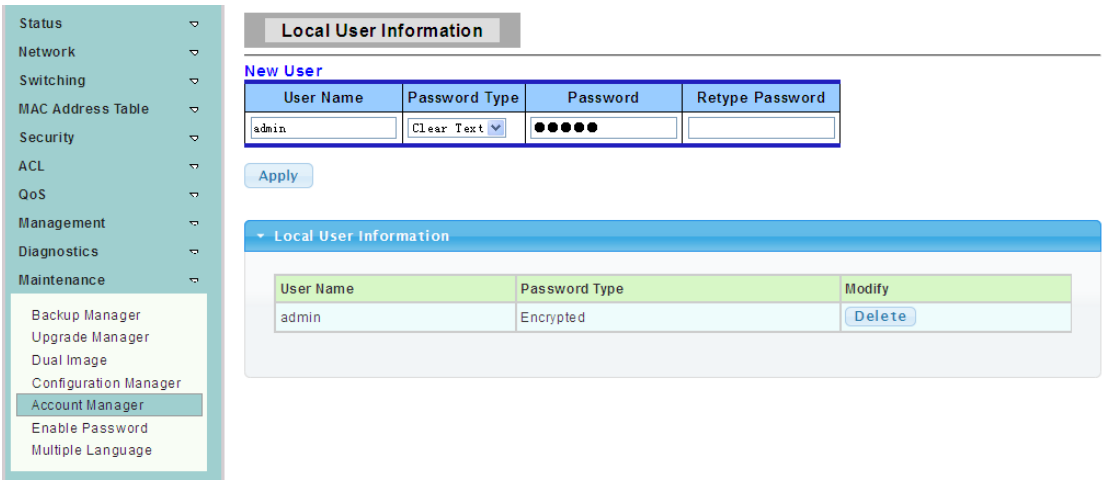
To display the Configuration Manager web page, click **Maintenance > Configuration Manager**



4.11.5 Account Manager

To display the Local User Informaion web page, click **Maintenance > Account Manager**

This page allow user to add or delete switch local user database for authenticating.



User Name: User name for new account.

Password Type: Select password type for new account.

- Clear Text: Password without encryption.
- Encrypted: Password with encryption.
- No Password: No password for the new account.

Password: If the password type is not “No Password”, the password must be specified.

Retype Password: Retype password to make sure the password is exactly you typed before in “Password” field.

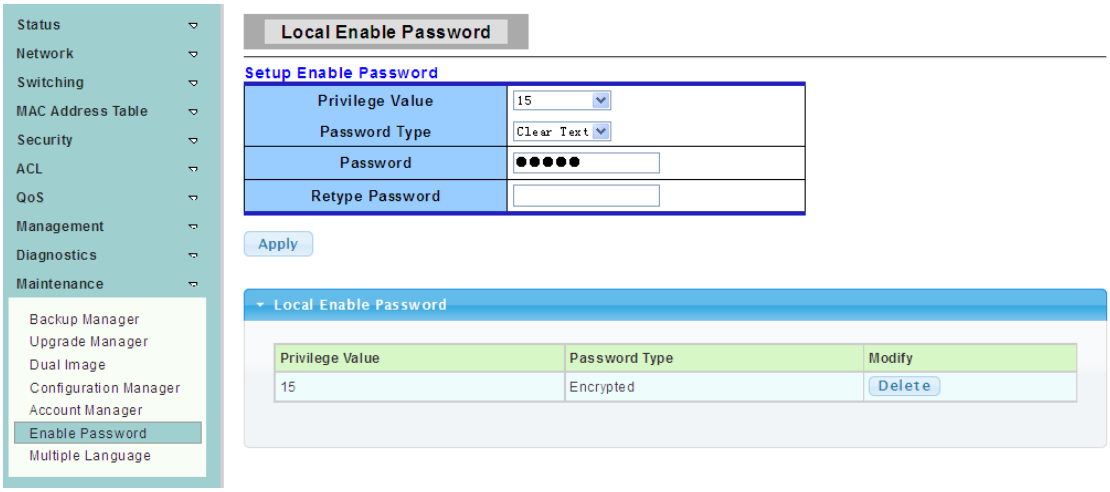
Privilege Type: Select privilege level for new account.

- Admin: Allow to change switch settings.
- User: See switch settings only. Not allow to change it.

4.11.6 Enable Password

To display the Local Enable Password web page, click **Maintenance > Enable Password**

This page allow user to modifythe enable password. In command line interface, user can use “enable” command to changetheir privilege level to “Admin”. After “enable” command is issued, user need to type the enable password to change their privilege level.



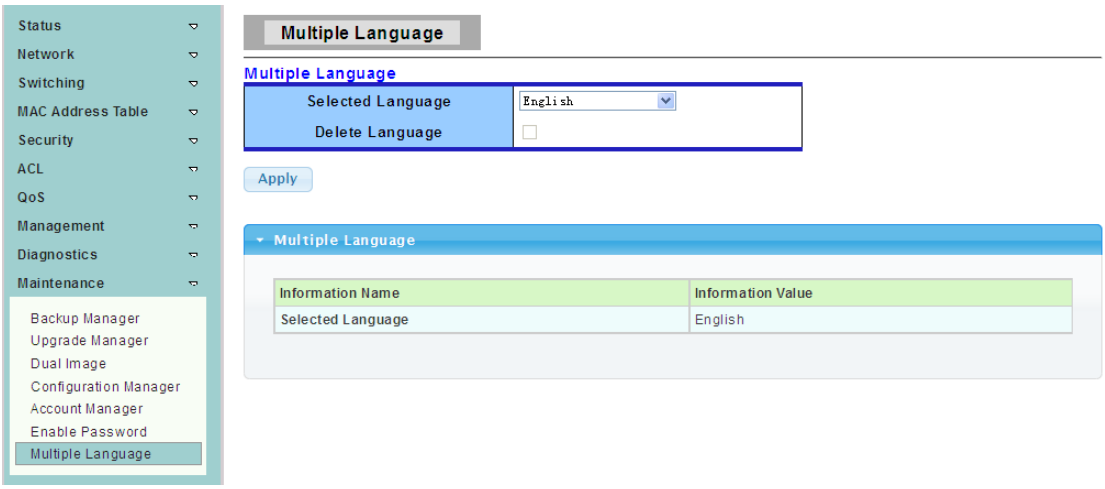
Password Type: Select password type for enable password.

- Clear Text: Password without encryption
- Encrypted: Password with encryption

Password: Password string.
Retype Password: Retype password to make sure the password is exactly you typed before in “Password” field.

4.11.7 Multiple Language

To display Multiple Language web page, click **Maintenance > Multiple Language**



Selected Language:can choose English or Chinese.
Delete Language: Select to delete the language.

Appendix: Technical Specifications

Standards		IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3x, IEEE 802.1q, IEEE 802.1p, IEEE 802.3at, IEEE 802.3af
Network Media (Cable)		10BASE-T: UTP category 3,4,5 cable (maximum 100m) 100BASE-T: UTP category 5, 5e cable (maximum 100m) 1000Base-T: UTP category 5e, 6 cable (maximum 100m)
Number of Ports		8 x 10/100/1000Mbps Auto-Negotiation ports
LED indicators	Port	Link/Act
	PoE	PoE
	Other	Power
Transfer Method		Store-and-Forward
MAC Address Table		8K
Switching Capacity		20 Gbps
Frame Filtering and Forward Rate		10Mbps: 14880pps 100Mbps: 148800pps 1000Mbps: 1488000pps
Dimensions (L × W × H)		280*180*44 mm
Environment		Operating Temperature: 0℃~40℃ Storage Temperature: -10℃~70℃ Operating Humidity: 10%~90% non-condensing Storage humidity: 5%~90% non-condensing