24-PORT POE+ WEB-MANAGED GIGABIT ETHERNET SWITCH WITH 2 SFP PORTS USER MANUAL

MODEL 560559

INTELLINET®
NETWORK SOLUTIONS

INT-560559-UM-0116-1

1 TABLE OF CONTENTS

2 PRODUCT INTRODUCTION

Congratulations on your purchase of the 24-Port PoE+ Web-Managed PoE+ Gigabit Ethernet Switch. Before you install and use this product, read this manual carefully for a full understanding of its functions.

2.1 PRODUCT OVERVIEW

The Web-Managed Gigabit Ethernet Switch provides a seamless network connection. It integrates 1000 Mbps Gigabit Ethernet, 100Mbps Fast Ethernet and 10Mbps Ethernet network capabilities in a highly flexible package. With 24 10/100/1000 Mbps Auto-Negotiation RJ45 ports, all ports support Auto MDI/MDIX function. The switch is a low-cost, easy-to-use, high-performance upgrade from your old network to a 1000 Mbps Gigabit network, essential in helping solve network bottlenecks that frequently develop as more advanced computer users and newer applications continue to demand greater network resources. For efficient management, the switch is equipped with a remote Web interface. The switch can be programmed for advanced switch management functions, such as Port Management, Link Aggregation, VLAN, Spanning Tree, Multicast, QoS, Security, Access Control, MAC Address Table, LLDP, Diagnostics, RMON and Maintenance. Its PoE ports can automatically detect and supply power to IEEE802.3at compliant Powered Devices (PD), such as Wireless Access Points, network cameras or Voice over IP phones.

2.2 FEATURES

- Provides power and data connection for up to 24 PoE network devices
- Save installation cost by delivering data and power over existing network cables
- IEEE 802.3at/af-compliant RJ45 PoE/PoE+ output ports
- PoE power budget of 240 watts
- Power output up to 30 watts per port
- Supports IEEE 802.3at and IEEE 802.3af-compliant PoE devices (wireless access points, VoIP phones, IP cameras)
- Supports IEEE 802.3at/af detection and short circuit, overload and high-voltage protection
- Supports SNMP management
- Two small form-factor pluggable GBIC module slots (SFP)
- Supports VLAN (tag-based and port-based)
- Provides IEEE 802.1x port-based security
- Supports link aggregation (trunking)
- Supports port mirroring
- Supports jumbo frames up to 9 kBytes

- Supports Rapid Spanning Tree/Spanning Tree protocol
- Broadcast storm control with multicast packet rate settings
- Supports two types of QoS: port-based and DSCP
- LEDs for power, link/activity and PoE
- Includes 19" rackmount brackets

2.3 SPECIFICATIONS

Standards

- IEEE 802.1d (Spanning Tree Protocol)
- IEEE 802.1p (Traffic Prioritization)
- IEEE 802.1q (VLAN Tagging)
- IEEE 802.1w (Rapid Spanning Tree Protocol)
- IEEE 802.3 (10Base-T Ethernet)
- IEEE 802.3ab (Twisted Pair Gigabit Ethernet)
- IEEE 802.3ad (Link Aggregation Control Protocol LACP)
- IEEE 802.3af (Power over Ethernet 802.3at Type 1)
- IEEE 802.3at (Power over Ethernet 802.3at Type 2)
- IEEE 802.3u (100Base-TX Fast Ethernet)
- IEEE 802.3x (flow control, for full duplex mode)

Power

- Input: 90 – 260 V AC, 50 – 60 Hz
- Power consumption: 260 watts (maximum)

Environmental

- Metal housing
- Dimensions: 440 (W) x 220 (L) x 44 (H) mm (17.3 x 8.7 x 1.7 in.)
- Weight: 3.1 kg (6.8 lbs.)
- Operating temperature: 0 – 45°C (32 – 113°F)
- Operating humidity: 10 – 90% RH, non-condensing
- Storage temperature: -20 – 90°C (-4 – 194°F)

Package Contents

- 24-Port Gigabit Ethernet PoE+ Web-Managed Switch with 2 SFP Ports
- Power cable
- User manual

2.4 External Component Description

2.4.1 Front Panel

The front panel of the Switch consists of 24 x 10/100/1000 Mbps RJ-45 ports, 2 x SFP ports, 1 x Console port, 1 x Reset button and a series of LED indicators as shown as below.

10/100/1000 Mbps RJ-45 ports (1~24):

Designed to connect to the device with a bandwidth of 10Mbps, 100Mbps or 1000 Mbps. Each has a corresponding 10/100/1000 Mbps LED.

SFP ports (SFP1, SFP2):

Designed to install the SFP module and connect to the device with a bandwidth of 1000 Mbps. Each has a corresponding 1000 Mbps LED.

Console port (Console):

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

Reset button (Reset):

To restore the system factory default settings, press the reset button for 5 seconds while the device is powered on.

LED indicators:

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

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

LED	COLOR	STATUS	STATUS DESCRIPTION
Power	Red	On	Power On
		Off	Power Off
LINK/ACT/Speed (1~24)	10/100 Mbps: Amber	On	A device is connected to the port
		Off	No device is connected to the port
	1000 Mbps: Green		
		Flashing	Sending or receiving data
SFP1 SFP2	Green	On	A device is connected to the port
		Off	No device is connected to the port
		Flashing	Sending or receiving data
POE	Orange	On	An IEEE 802.3af/at compliant powered device (PD) is connected to the port, and the PoE Switch supplies power successfully.
		Off	No powered device is connected to the port.
		Flashing	There may be a short circuit or PoE power overload. Disconnect the device from this port immediately.

2.4.2 Rear Panel

AC Power Connector:

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

Grounding Terminal:

Ground the switch through the PE cable on the AC cord or with a separate ground wire.

2.5 PACKAGE CONTENTS

Before installing the switch, make sure that the following items are enclosed. If any part is missing or damaged, contact your local agent immediately.

- 24-Port Gigabit Ethernet PoE+ Web-Managed Switch with 2 SFP Ports
- Power cable
- Quick Installation Guide
- User manual (on CD)
- Four rubber feet, two mounting ears and eights screws

3 INSTALLING AND CONNECTING THE SWITCH

This part describes how to install your Web-Managed Gigabit Ethernet PoE+ Switch and make connections to it.

3.1 INSTALLATION

The following steps will help prevent damage to the device while also helping to maintain proper security.

- Place the switch on a stable surface or desktop to minimize the chances of falling.
- 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 damage, do not open the switch's chassis even if it fails to receive power.
- Make sure that there is proper heat dissipation from and adequate ventilation around the switch.
- Make sure the surface the switch is placed on can support the weight of the switch and its accessories.

3.1.1 Desktop Installation

When installing the switch on a desktop (if not in a rack), attach the enclosed rubber feet to the bottom corners of the switch to minimize vibration. Allow adequate space for ventilation between the device and the objects around it.

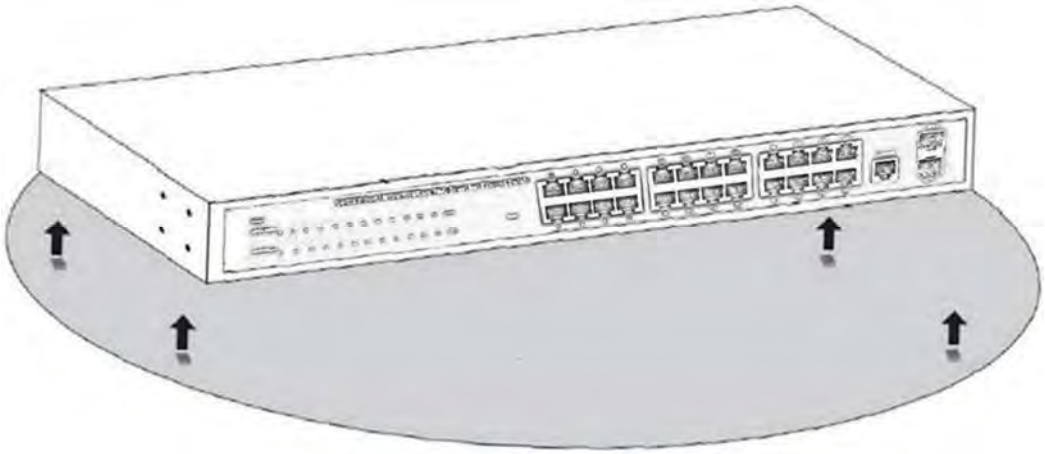


Figure 4 - Desktop Installation

3.1.2 Rack-mountable Installation in 19-inch Cabinet

The switch can be mounted in an EIA standard-sized, 19-inch rack, which can be placed in a wiring closet with other equipment. To install the switch, 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.

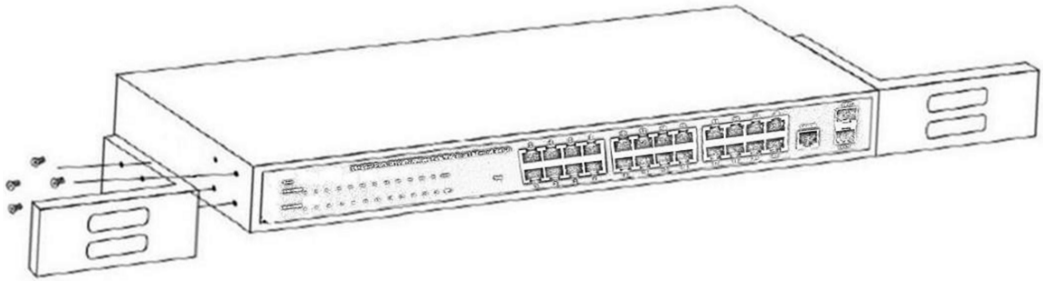


Figure 5 - Bracket Installation

b. Use the screws provided with the equipment rack to mount the switch on the rack and tighten it.

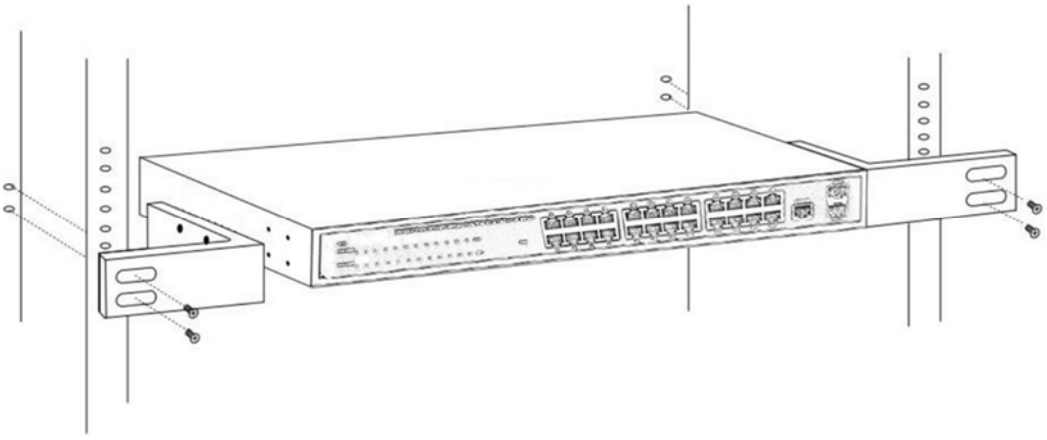


Figure 6 - Rack Installation

3.1.3 Power on the Switch

The switch is powered on by connecting it to an outlet using the AC 100-240V 50/60Hz internal high-performance power supply.

AC Electrical Outlet:

It is recommended to use a single-phase, three-wire receptacle with a neutral outlet or multifunctional computer professional receptacle. Be sure to connect the metal ground connector to the grounding source on the outlet.

AC Power Cord Connection:

Connect the AC power connector on the back panel of the switch to an external receptacle with the included power cord, then check that the power indicator is ON. When it is ON, it indicates the power connection is okay.

4 CONNECTION TO THE SWITCH

4.1 CONNECTING COMPUTER

Use standard Cat5/5e 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 they are connected.

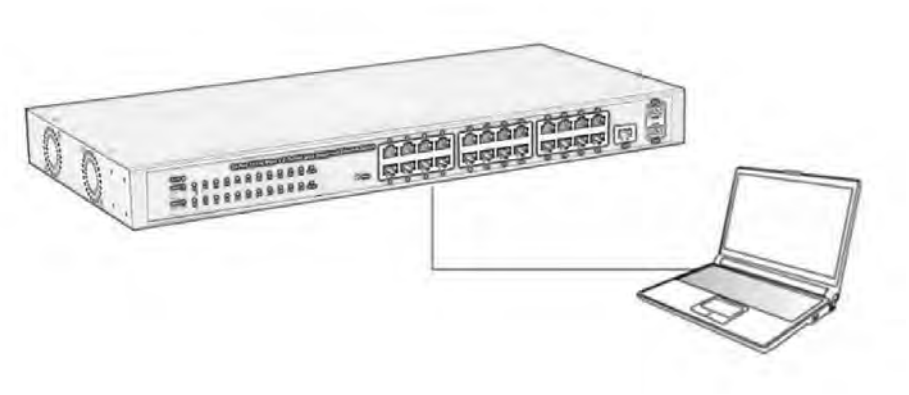


Figure 7 - PC Connect

The LNK/ACT/Speed LEDs for each port light when the link is available.

4.2 HOW TO LOGIN TO 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 Username	admin
Default Password	admin

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

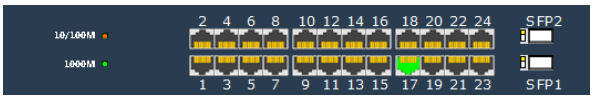
1. Connect the switch with the computer NIC interface.
2. Power on the switch.
3. Check whether the IP address of the computer is within this network segment: 192.168.2.xxx ("xxx" range is 2-254); for example, 192.168.2.100.

4. Open the browser, and go to the URL *http://192.168.2.1*. The switch login window appears, as shown below.

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.

5 SWITCH CONFIGURATION

The PoE+ Web-Managed Gigabit Ethernet Switch software provides rich Layer 2 functionality for switches in your networks. This chapter describes how to use the Web-based management interface (Web UI) for this switch.

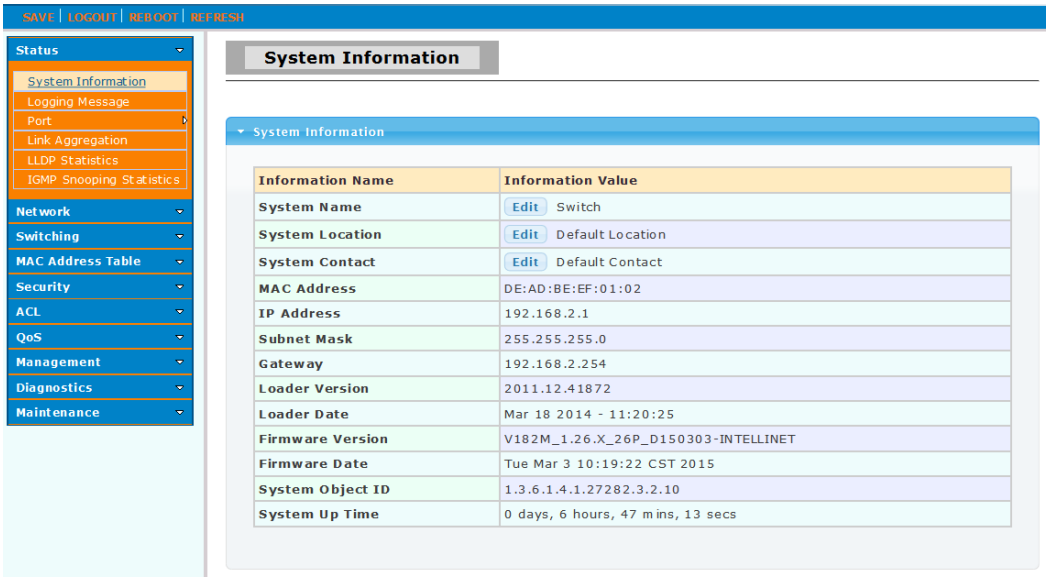


In the Web UI, the left column shows the configuration menu. The top row shows the switch's current link status. Green squares indicate the port link is up (port 17 in the example above), while black squares indicate the port link is down. Below the switch panel, you can find a common toolbar to provide useful functions for users. The rest of the screen area displays the configuration settings.

5.1 STATUS

5.1.1 System Information

This page allows you to configure System-related information and browse information such as MAC address, IP address, firmware version, loader version, among others.



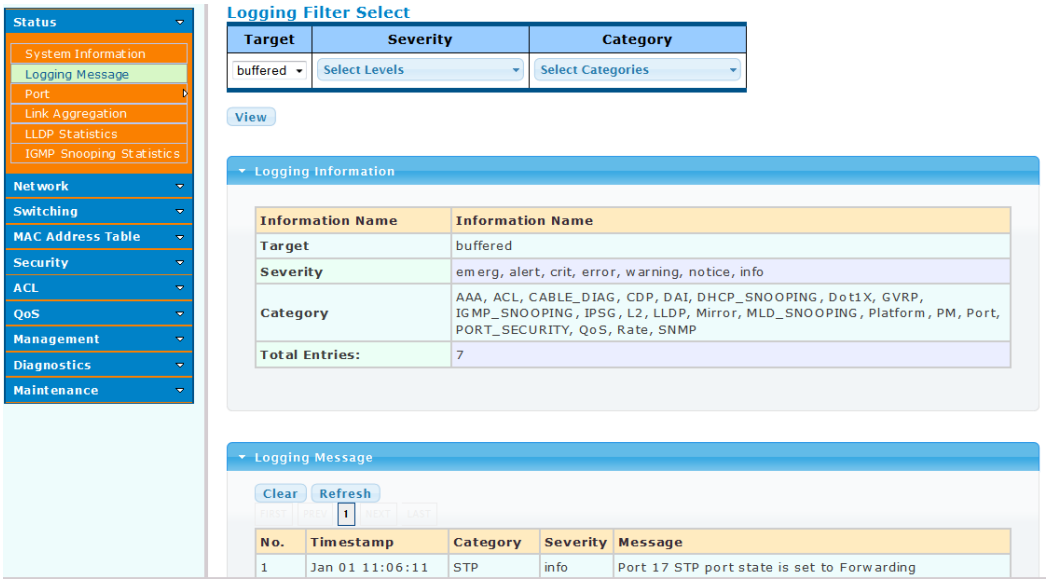
System Name: System name of the switch. This name will also use as CLI prefix of each line. ("Switch>" or "Switch#").

System Location: System location of the switch, e.g., "ServerRoom".

System Contact: System contact of the switch, e.g., the system administrator.

5.1.2 Logging Message

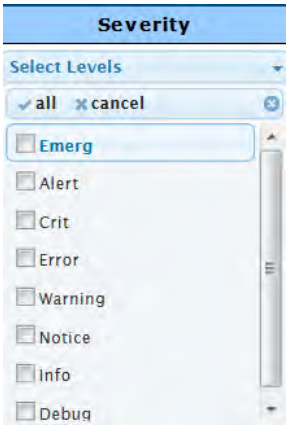
The Intellinet 24-Port Gigabit Ethernet PoE+ Web-Managed Switch is equipped with an extensive logging function. You can define the type of events you wish the switch to log, the level of detail and the target destination for the log.



Target:

- Buffered: The Log information is stored in the RAM. All messages are lost when the switch loses power or is being restarted.
- Flash: Log information is stored in the FLASH memory and will be available after a system restart.

Severity: In a network there are events occurring constantly, and the Intellinet switch can log a great deal of these at runtime. With the severity filter you can define the threshold at which point an event is considered “log worthy”. “Emerg” only logs events which are considered an “Emergency”. That is the kind of event that would get a system administrator out of bed at 4 o’clock in the morning. “Debug” on the other hand is the polar opposite. In this mode there is nothing the switch considered unimportant. Choose whichever level is right for you.



Category: Select what type of events the switch should log, for instance port related events, or events belong to the ACL Access Control List.

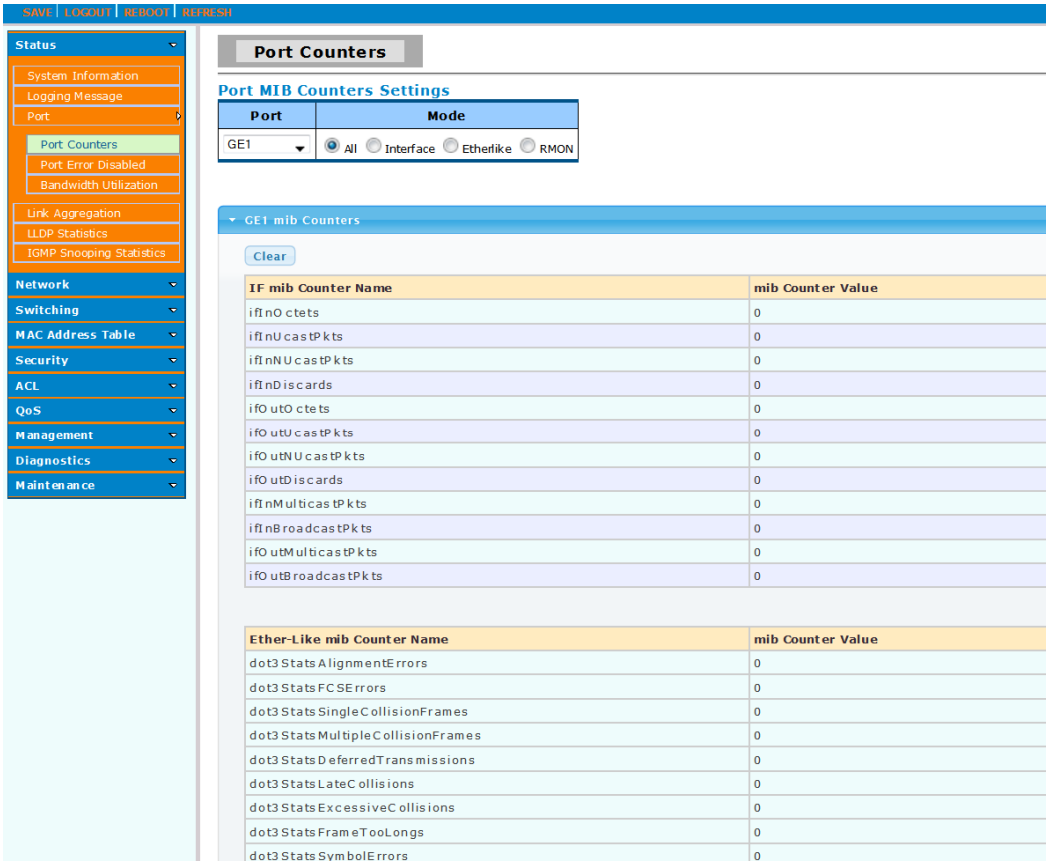
5.1.3 Port

The Port configuration page displays port summary and status information.

5.1.3.1 Port Counters

This page displays standard counters of network traffic using modes like Interface, EtherLike and RMON. Interfaces and EtherLike 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.

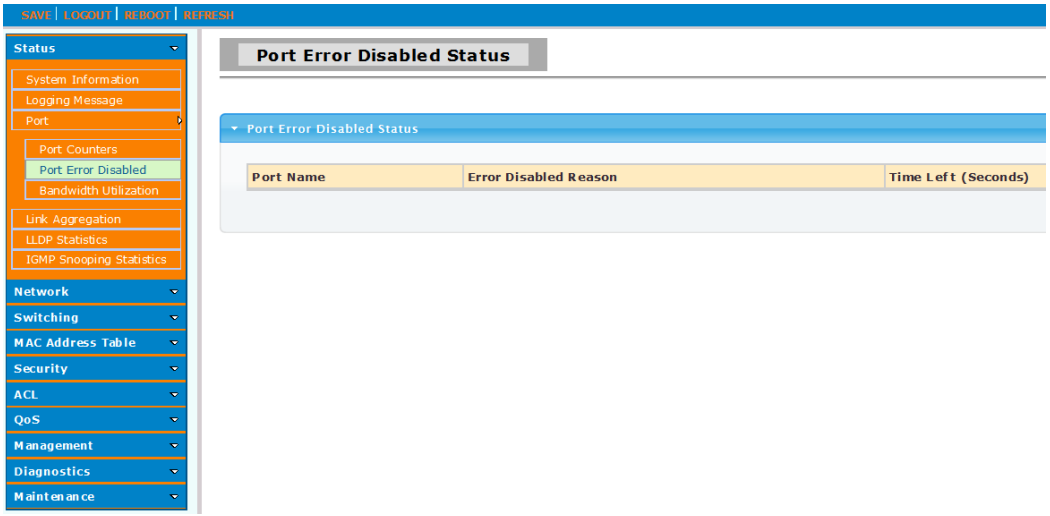
Port: Select any of the 24 RJ45 Gigabit Ethernet Ports (GE), 2 SFP ports, or 8 Link Aggregation Groups (LAG).
Mode: Select the filter you wish to apply to the displayed results.



5.1.3.2 Port Error Disabled

Some protocols such as BPDU Guard, Loop back and UDLD can disable ports to protect the rest of the network, for instance if the switch detects that one of the attached network interface cards is malfunctioning and flooding the network with error packets.

Ideally, you want this screen to look as shown below.

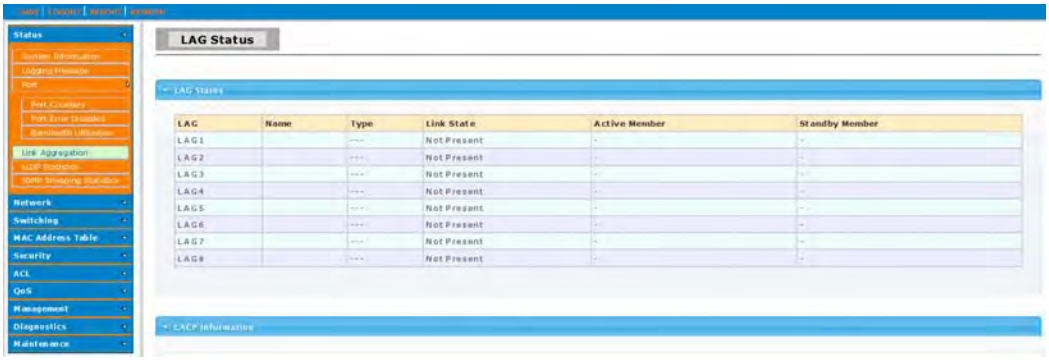


5.1.3.3 Bandwidth Utilization

This page displays the TX (transmit) and RX (receive) bandwidth utilization for each port.

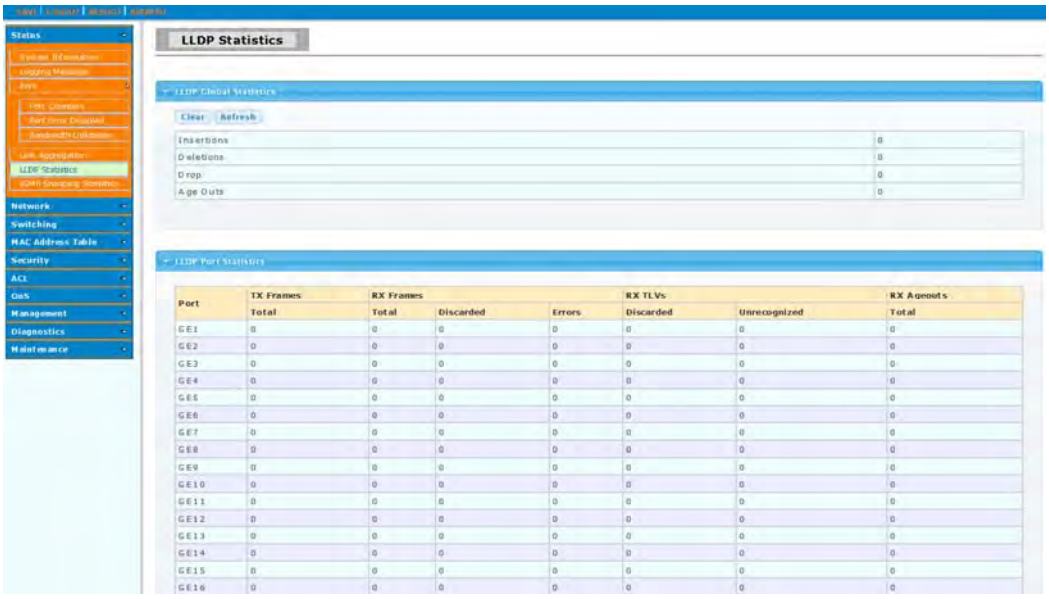
5.1.4 Link Aggregation

Link aggregation is a method of using multiple Ethernet ports in parallel to increase throughput beyond what a single connection could sustain, and to provide redundancy in case one of the links should fail. As this is essentially a grouping of ports into one logical unit, we call them Link Aggregation Groups, or “LAG” for short. Any LAG that is currently defined will be shown on this screen. The configuration of the LAG will be addressed later in the section “Switching”.



5.1.5 LLDP Statistics

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, principally wired Ethernet. The LLDP statistics page displays an overall 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.

5.1.6 IGMP Snooping Statistics

The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships. IGMP is an integral part of IP multicast. IGMP can be used for one-to-many networking applications such as online streaming video and gaming, and allows more efficient use of resources when supporting these types of applications.

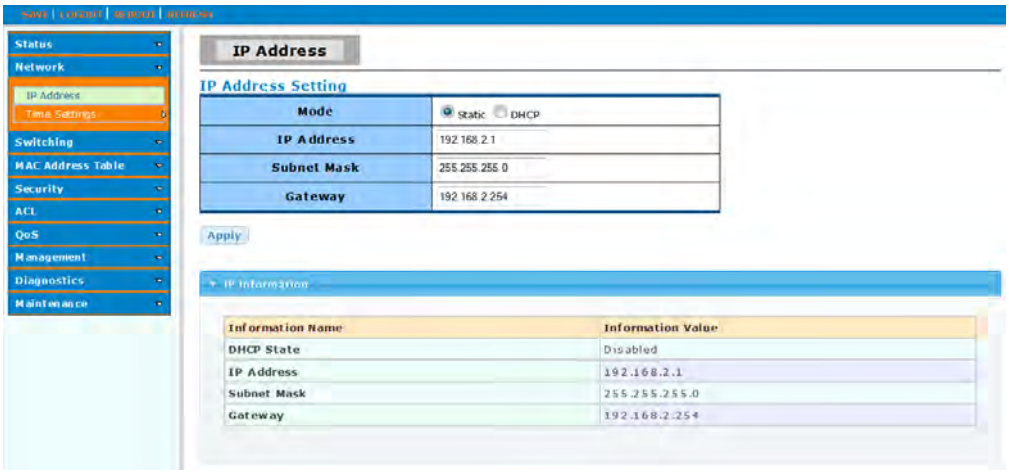
This page displays the IGMP statistics information, also referred to as 'Snooping Statistics'.

5.2 NETWORK

Use the Network page to configure settings for the switch network interface and set up the time related settings.

5.2.1 IP Address

Define the IP address of the switch here.



Mode: Select the mode of network connection.

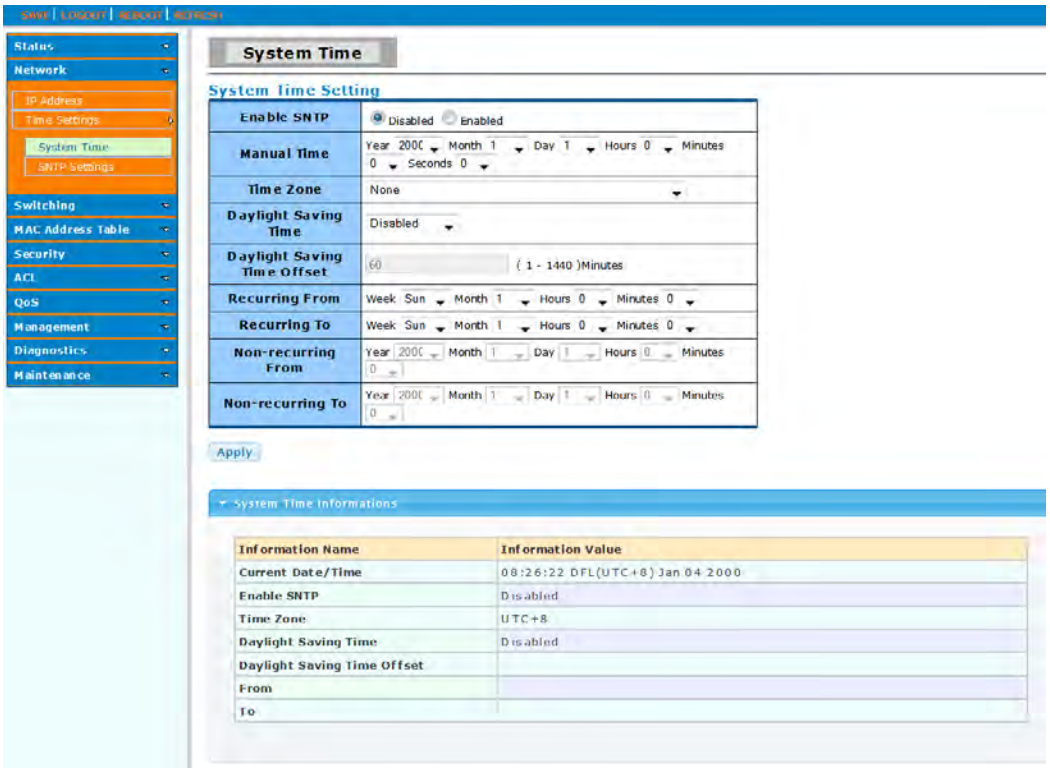
- Static: Define the IP address manually. The IP address, subnet mask and gateway address must be provided.
- DHCP: obtain IP information from a DHCP server on the network.

Note that you have multiple of these switches installed in your network, you must assign a unique IP address to each of them, even if you don't plan on using any of the smart features of the switch. As a reminder, the default IP address of this switch is 192.168.2.1.

5.2.2 Time Settings

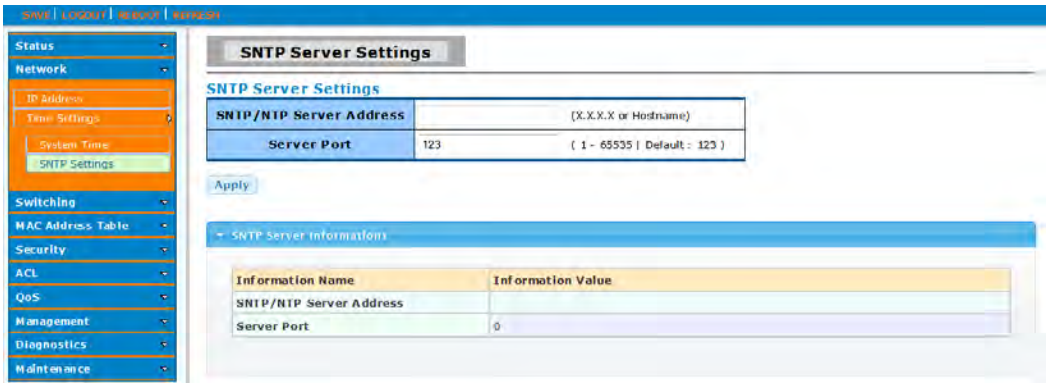
5.2.2.1 *System Time*

For the switch to accurately flag messages with the correct date and time stamp, the switch's system time must be set up first. Set "Enable SNTP" to "Disabled" if you do not want to sync the switch system time with an external time server, but rather want to configure it manually.



5.2.2.2 *SNTP Settings*

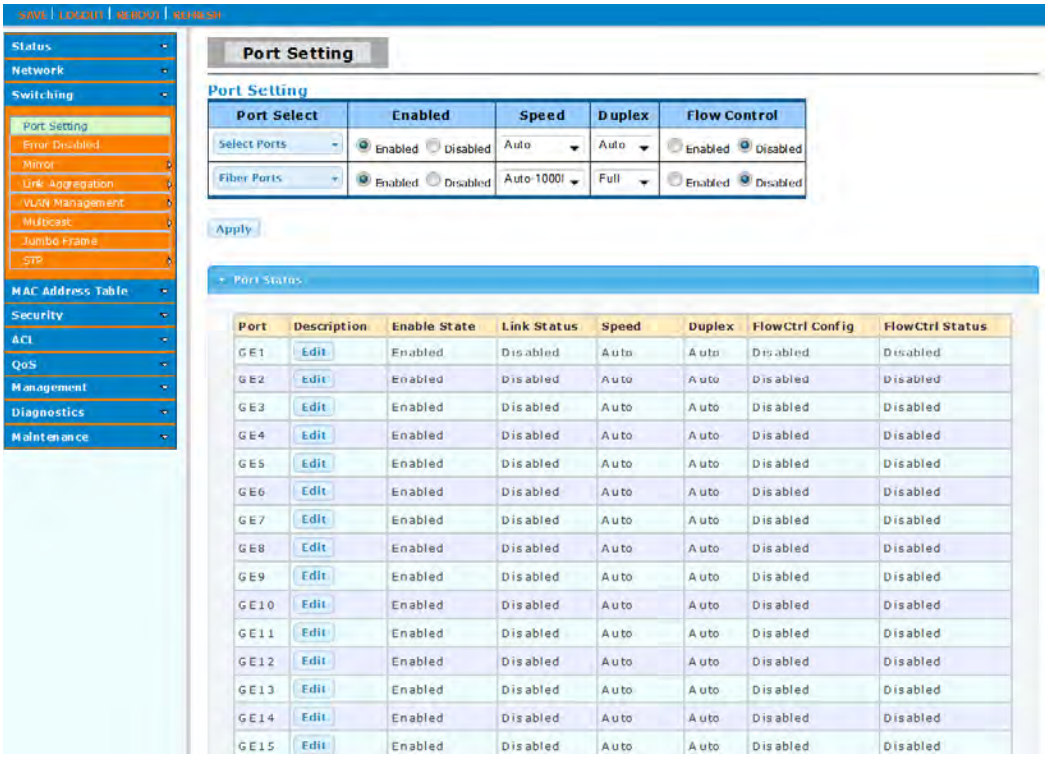
If you wish to synchronize the switch system time with an external time server, also referred to as an NTP or SNTP server, then you can provide the IP address or host name of said server on this screen. Unless you know it to be different, it is recommend to leave the server port as '123'. If you have a NTP server in your LAN, then you can utilize that too, of course.



5.3 SWITCHING

5.3.1 Port Setting

On this screen you can configure basic aspects of each of the ports.

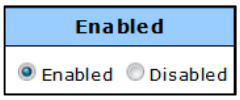


Port Select:

Select one or multiple ports to configure.

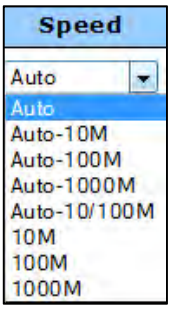
Enabled:

Enable or disable the port. Disabling the power will also cut off power to any connected PoE powered device.



Speed:

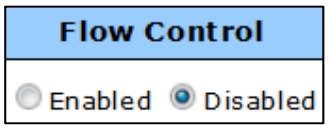
Typically you set to speed to “Auto,” which stands for auto-negotiation. In this mode the connection will be made at the fastest possible speed. In very rare cases, however, this auto-negotiation can fail, and you need to manually adjust the speed to whatever the connecting device is capable of.



Duplex:

In a full duplex system, both parties can communicate to the other simultaneously. An example of a full-duplex device is a telephone; the parties at both ends of a call can speak and be heard by the other party simultaneously. In networking terms, full duplex allows receiving and transmitting of data at the same time, whereas half duplex does not. If the telephone is an example for full duplex, then a push-to-talk CB radio or 'walkie-talkie' represents half duplex. The switch can either receive or send data, but it can never happen simultaneously. Unless you have any specific reason not to do so, this should be left in "Auto" mode.

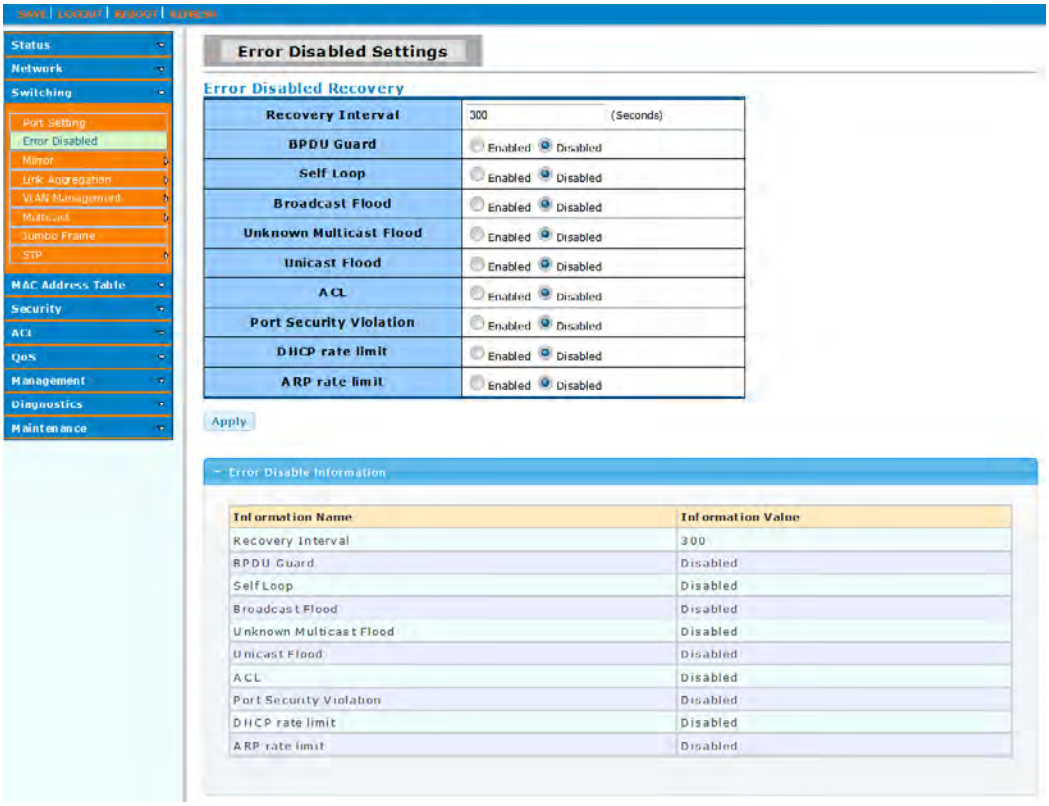
Flow Control:



IEEE 802.3x flow control is the process of managing the rate of data transmission between two nodes, i.E. the switch and a connected network client, to prevent a fast sender from overwhelming a slow receiver. It provides a mechanism for the receiver to control the transmission speed, so that the receiving node is not overwhelmed with data from transmitting node. That sounds like it is a good thing, and it is, but why then is the option by default set to "disabled" you might ask. The short answer is: Because you normally don't need it, and because it can in very rare circumstances have a negative impact on the overall performance in your network. The TCP protocol already provides its own flow control mechanism, allowing a sender to throttle back the speed if the receiver is having problems keeping up.

5.3.2 Error Disabled

This page allows you to define the parameters for the automatic port disable function.



Recovery Interval: The switch will automatically re-enable ports that have been previously disabled, after the recovery interval time has elapsed.

BPDU Guard: BPDUs are sent out as multicast frames to which only other layer 2 switches or bridges are listening. If any loops (multiple possible paths between switches) are found in the network topology, the switches will co-operate to disable a port or ports to ensure that there are no loops.

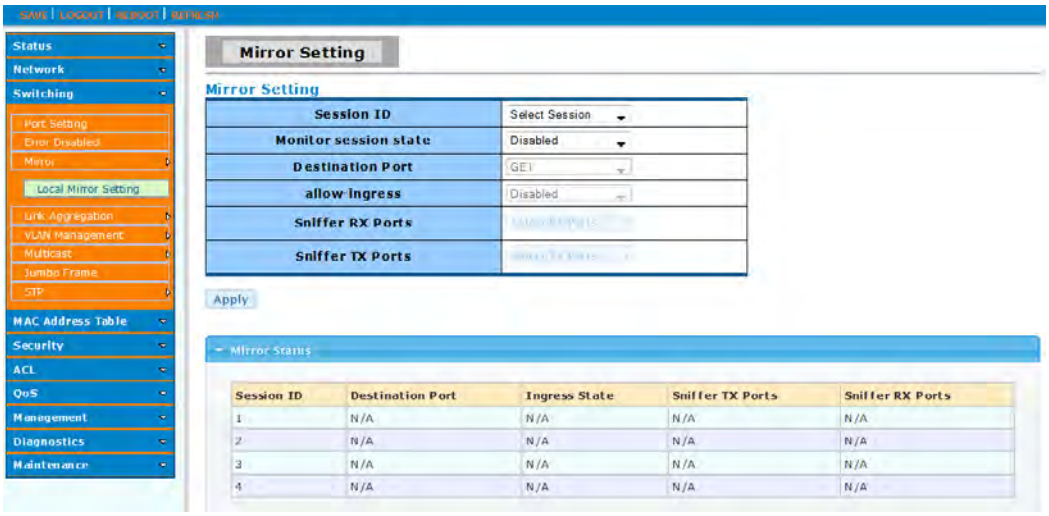
Flood: The network can get overwhelmed by a large amount of unicast packets that can literally flood the entire network and can consume sufficient network resources so as to render the network unable to transport normal traffic.

ACL/Port Security Violation: Security related threads that violate the Access Control List settings can be caught by the switch, and drastic measures can be taken, namely disable the port from which the packets originate.

DHCP/ARP Rate Limit: Ports are disabled that exceed the DHCP request and ARP rate limits.

5.3.3 Traffic Mirroring

Port mirroring is the ability of a network switch to send a copy of network packets seen on a switch port or ports to a network-monitoring device connected to another switch port, i.e., a computer equipped with a packet sniffer utility.



Session ID: The Intellinet switch supports up to 4 session IDs.

Monitor Session State: Disables or enables port mirroring for this session.

Destination Port: The port to which the mirrored packets are sent, which is the port to which you connect your network monitoring station. This port will no longer function as a regular port, and it cannot be assigned to any LAG or VLAN group.

Allow-Ingress: Enable or Disable ingress traffic forwarding. An example for ingress traffic is the information returned by a web site to the local user's request. Egress, on the other hand, would be the request by the local user to the web site. Simply speaking, from the standpoint of your network, ingress traffic can be consider incoming or inbound traffic, whereas egress traffic is outgoing or outbound traffic.

Sniffer RX/TX Ports: Defines the source ports from which traffic will be mirrored.

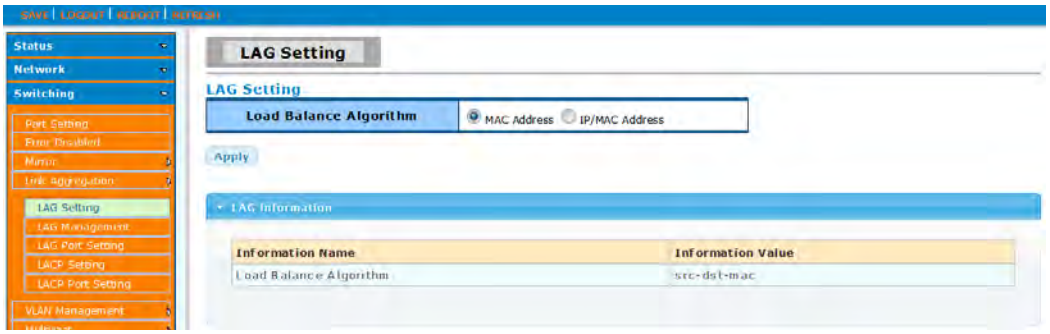
TX Ports: Only traffic transmitted originating from these ports will be mirrored to the destination port.

RX Port: Only traffic received by these ports will be mirrored to the destination port.

5.3.4 Link Aggregation

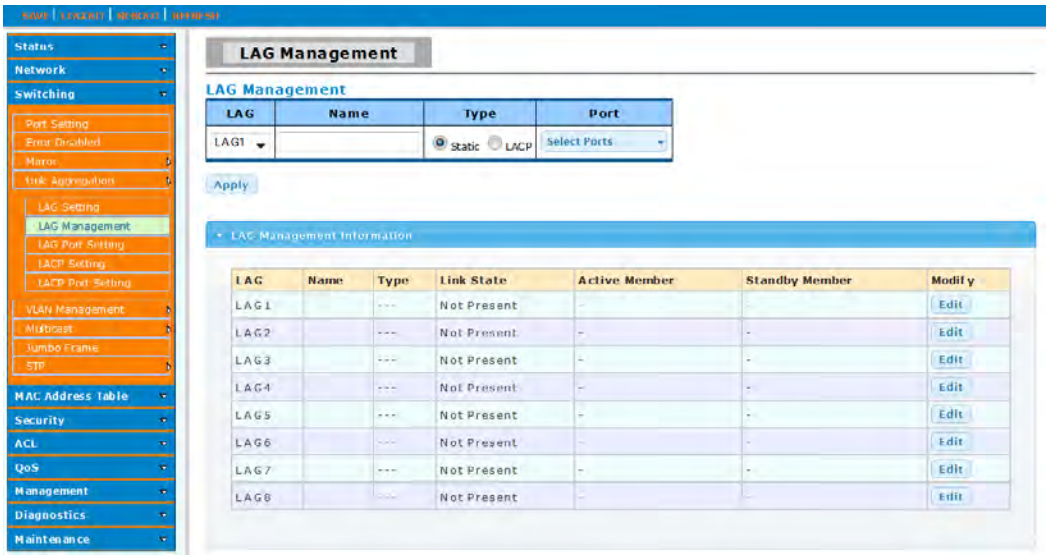
5.3.4.1 *LAG Setting*

Besides providing a higher speed connection to another port by grouping ports together into la logical unit, Link Aggregation (LAG) also provides a load balancing feature. On this screen you define whether LAG that is depended on the MAC address or IP/MAC address.



5.3.4.2 *LAG Management*

This page is used to set up LAG groups. You can create up to 8 different LAG groups, each can have up to 8 member ports. Each LAG can be given a custom name, and you must select the ports for the LAG.



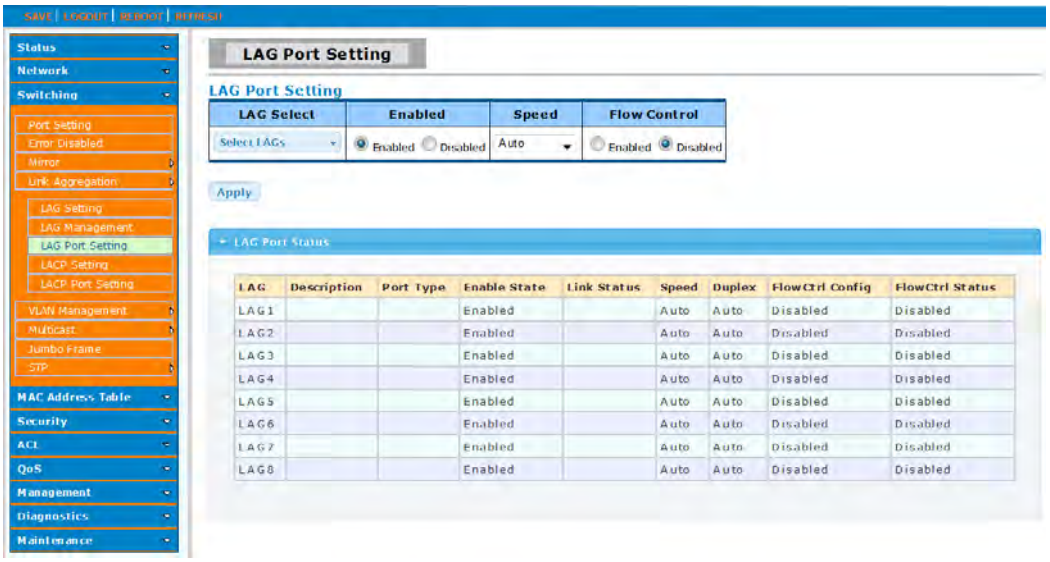
As for the type, there are two choices: Static and LACP.

Static: All configuration settings must be set up manually exactly the same way on the participating LAG device, i.e., the other Intellinet 24 Port PoE+ Web Managed Gigabit Switch. There is no problem with doing this of course. Even the static method provides link redundancy, should one or more of the links in the trunk fail. However, if media converters are used, it can happen that the link on the switch#1 is up, but the connection to the switch#2 at the other end is interrupted, for example because of a cable malfunction. In this case, switch#1 keeps sending data via this connection, because on this end there are no interruptions. The data transfer is therefore interrupted.

LACP: Link Aggregation Control Protocol (LACP) allows the dynamic exchange of information with regard to the link aggregation between the two members of said aggregation. It allows for the automatic detection of links in an LAG group when connected to another LACP-compliant Switch. Both switch#1 and switch#2 need to be set to the same mode for this to work. The data between the two switches is packetized in Link Aggregation Control Protocol Data Units (LACDUs). Should any of these packets fail to arrive, for instance due to an interruption one side of the media converter, the switches will quickly remove the LAG group port causing the problem from the LAG group. No data is lost.

5.3.4.3 *LAG Port Setting*

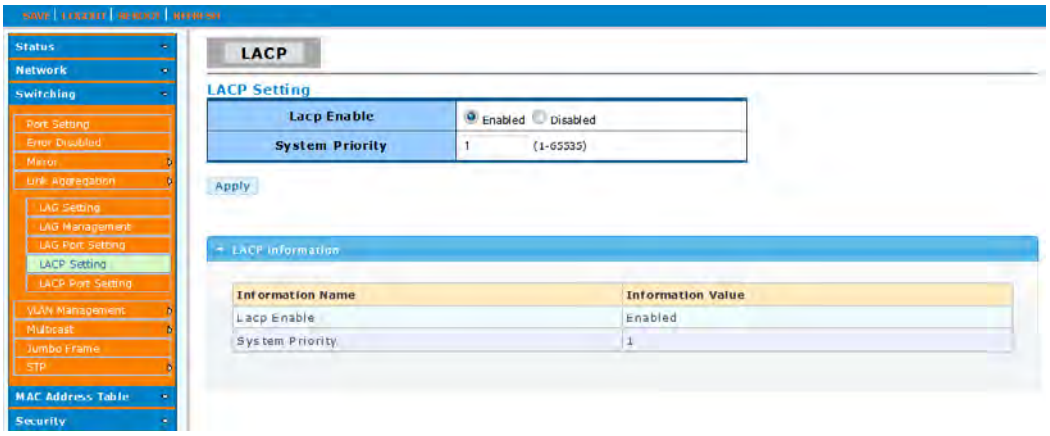
On this page you define additional settings for the LAG groups.



You can enable or disable the entire group, set the speed to manual values from 10 to 1000 Mbps, or auto, and you can enable or disable flow control.

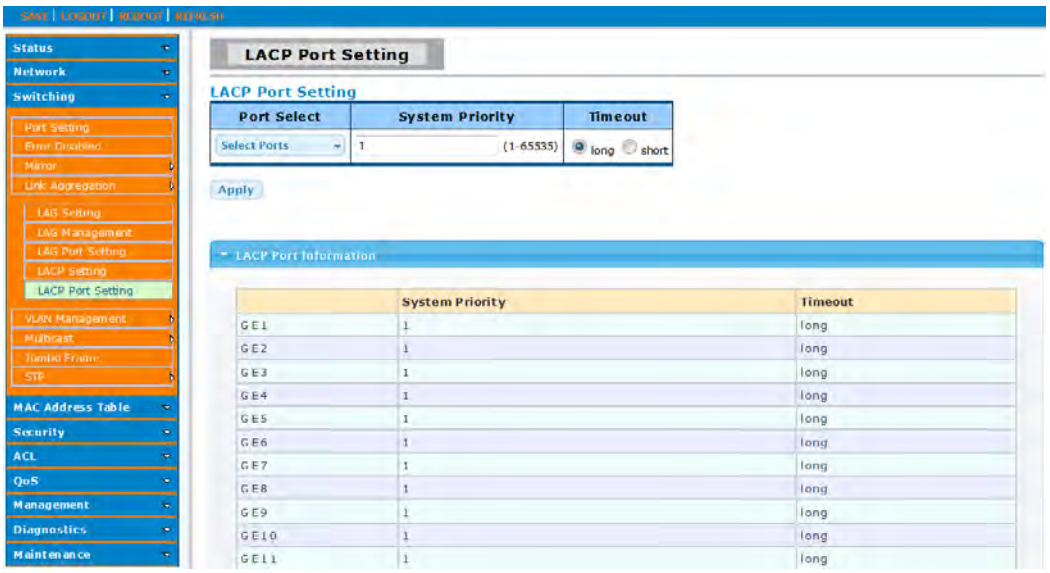
5.3.4.4 *LACP Setting*

This page is used to configure the system LACP system priority, which determines which switch (switch #1 or switch #2) in an LACP link controls port priorities. If both switches are set to the default value "1," then the LACP system ID (MAC address of the switch) determines which of the switches is in charge. Other than that, the switch with the lowest system priority number is in control.



5.3.4.5 *LACP Port Setting*

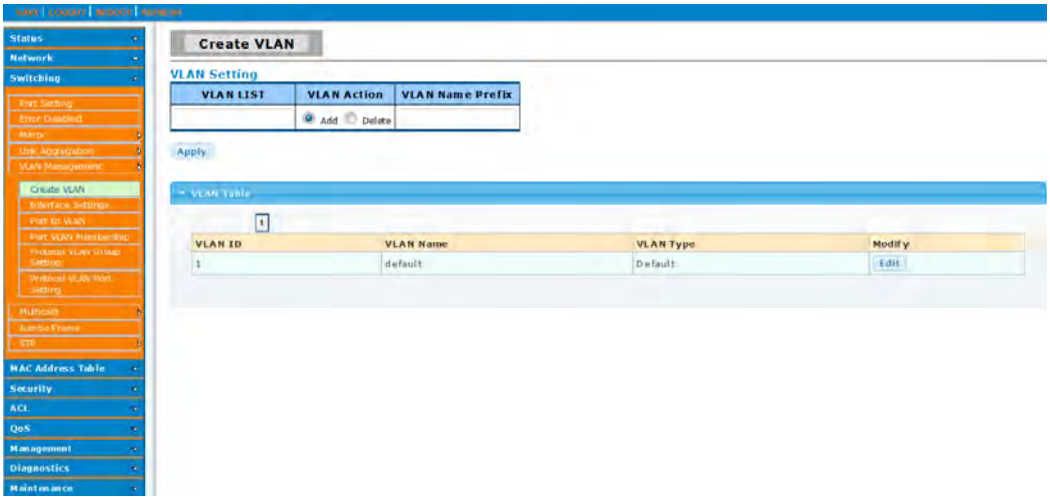
This page is used to set the priority for the LACP member ports. While the system priority defines, which switch is in charge in the LACP setup, the port priority is used to determine, how the ports in the LACP group are used, based on which port priority. The lowest number value has the highest priority, and if all are left at default, then the actual port number defines the priority.


SAVE | LOGOUT | REBOOT | REFRESH
Status
Network
Switching
Port Setting
Error Disabled
Mirror
Link Aggregation
LAG Setting
LAG Management
LAG Port Setting
LACP Setting
LACP Port Setting
VLAN Management
Multicast
Jumbo Frame
STP
MAC Address Table
Security
ACL
QoS
Management
Diagnostics
Maintenance
LACP Port Setting
LACP Port Setting
Port Select
System Priority
Timeout
Select Ports
1
(1-65535)
long
short
Apply
LACP Port Information
System Priority
Timeout
GE1 1 long
GE2 1 long
GE3 1 long
GE4 1 long
GE5 1 long
GE6 1 long
GE7 1 long
GE8 1 long
GE9 1 long
GE10 1 long
GE11 1 long

5.3.5 VLAN Management

5.3.5.1 *Create VLAN*

This page allows adding, deleting or editing the switch's VLAN settings.

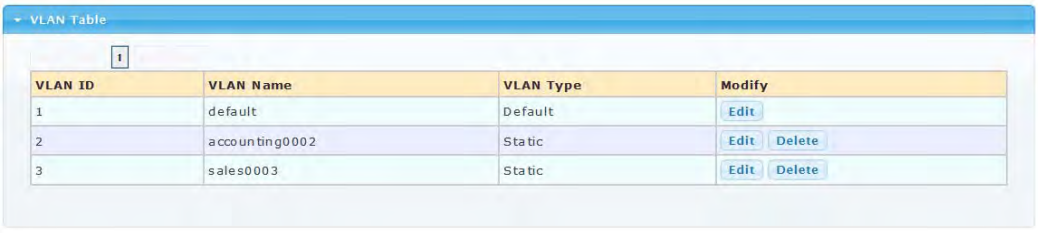


VLAN LIST: This is he ID for the new VLAN.

VLAN Action: Add or delete the VLAN.

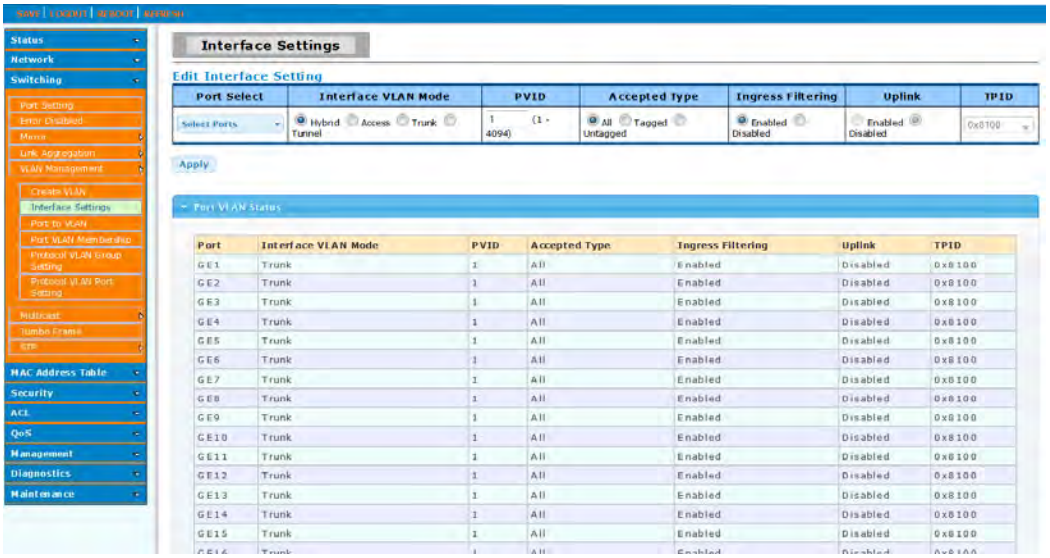
VLAN Name Prefix: VLAN Name Prefix for the new VLAN.

Below is a real-world example:



5.3.5.2 *Interface Settings*

This page allows the user to set the port type of vlan, common have access and trunk, dot1q - tunnel three modes and native VLAN choose whether the port TX,RX should have a tag.



Port Select : Select one or multipleports 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.

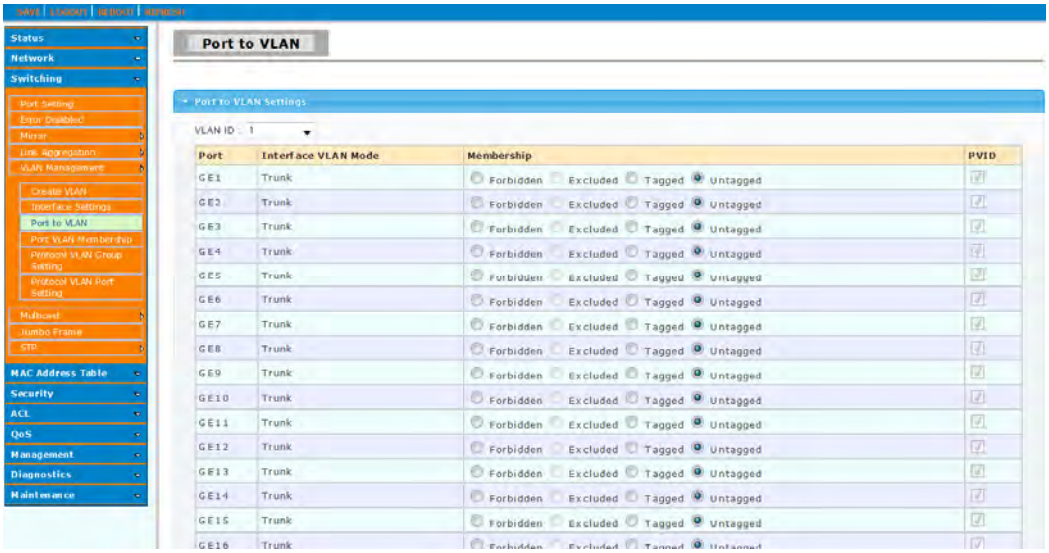
Ingress Filtering: Choose filter port open and close.

Uplink: Select port Uplink open or close.

5.3.5.3 *Port to VLAN*

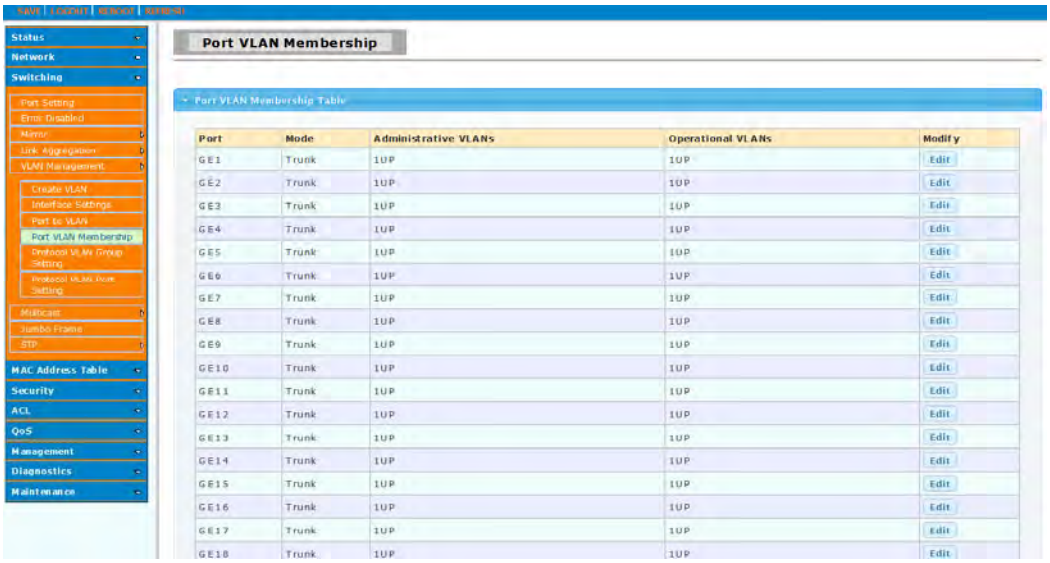
To display Port to VLAN web page, **click Switching > VLAN Management > Port to VLAN**

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



5.3.5.4 *Port VLAN Membership*

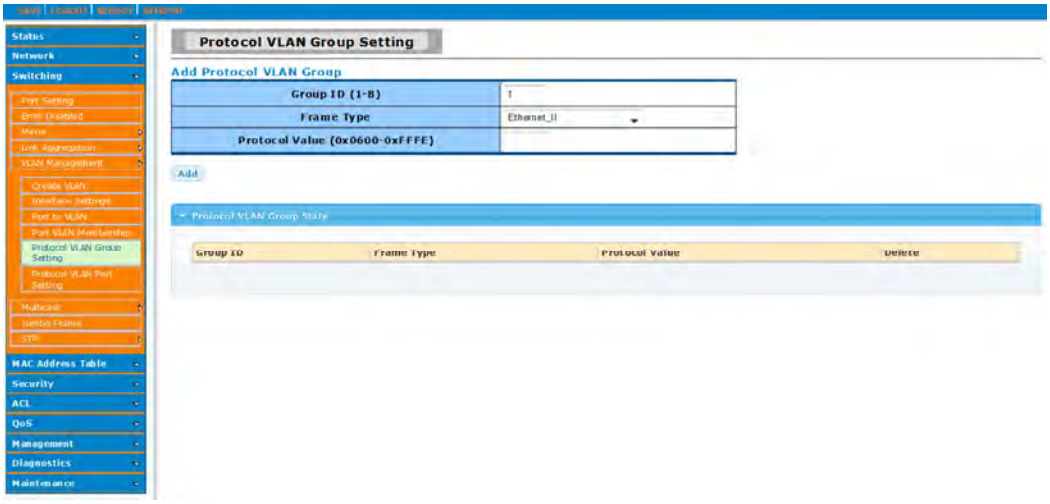
To display Port VLAN Membership web page, **click Switching > VLAN Management > Port VLAN Membership**



5.3.5.5 *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.

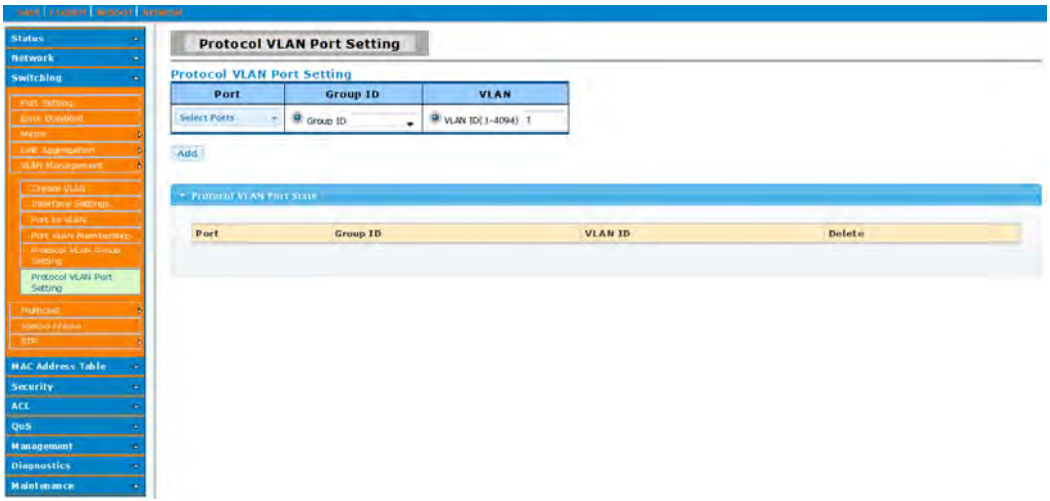
RFC_1042: packet type is RFC 1042 packet.

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

5.3.5.6 *Protocol VLAN Port Setting*

To display 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.

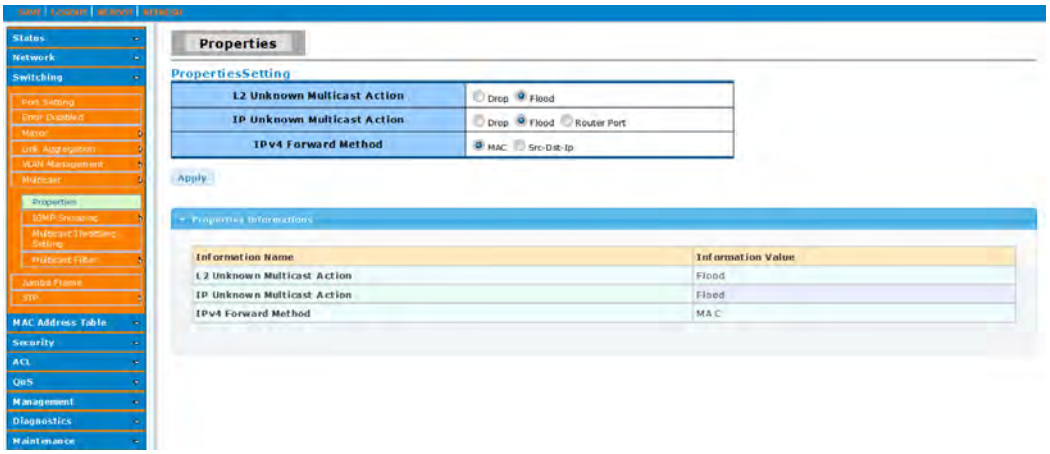
VLAN : Click the corresponding radio button to select a previously configured VLAN ID or VLAN Name.

5.3.6 Multicast

5.3.6.1 *Properties*

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

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

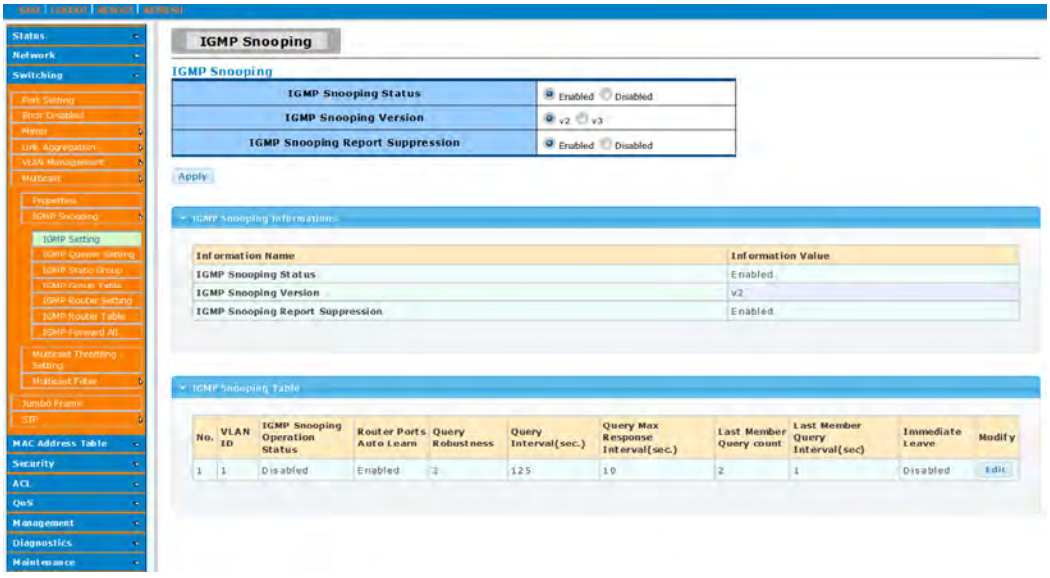


5.3.6.2 *IGMP Snooping*

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

IGMP Setting

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



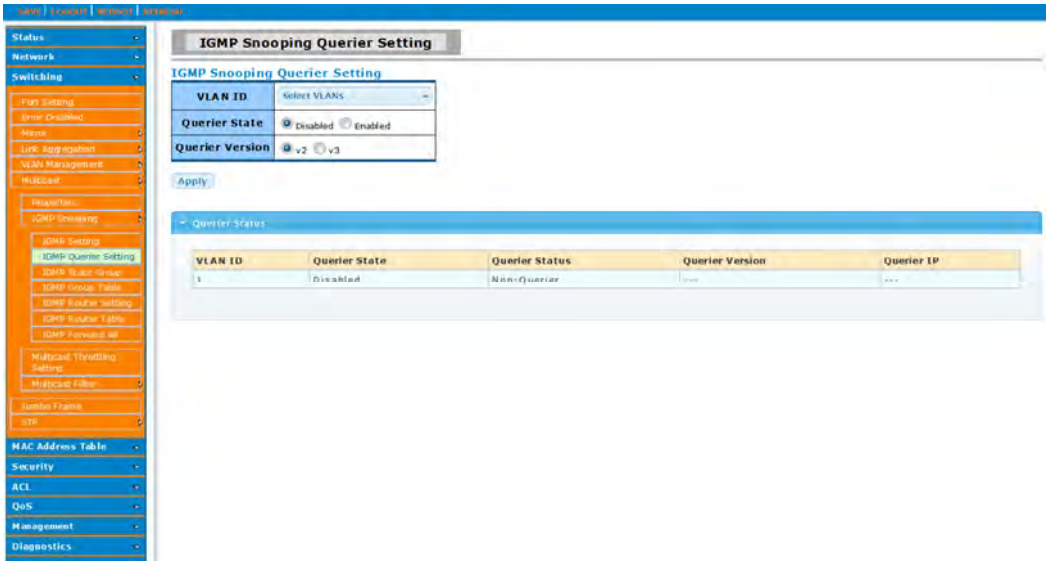
IGMP Snooping: Select the IGMP Snooping enable or disable.

IGMP Snooping Version: Select the IGMP Snooping Version,IGMPv2 or IGMPv3.

IGMP Snooping Report Suppression: Select the IGMP Snooping Report Suppression enable or disable.

IGMP Snooping Querier Setting

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

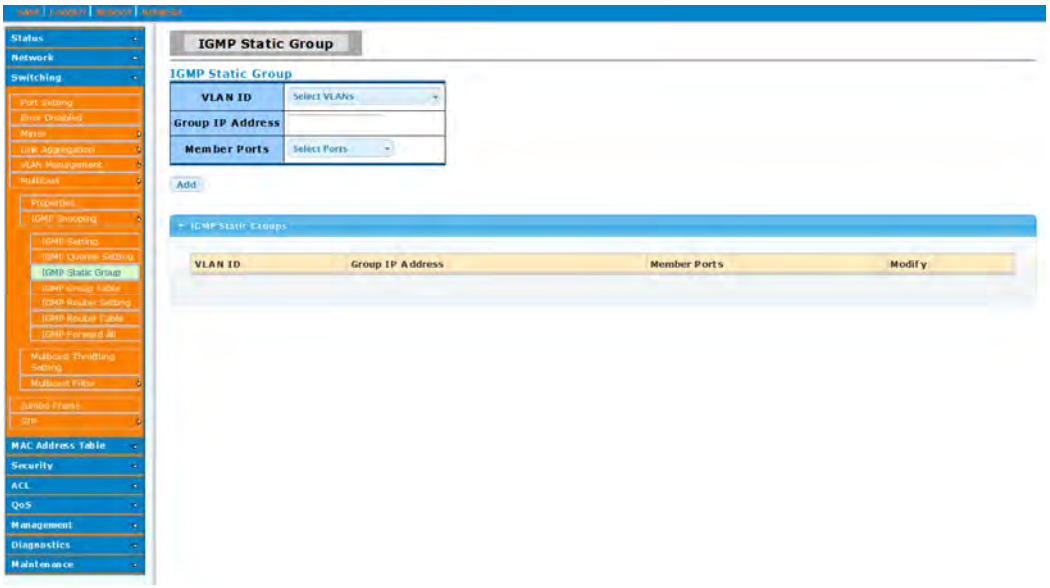
Disable: Disable IGMP Querier Election.

Version: Select the Querier Version,IGMPv2 or IGMPv3

IGMP Static Group

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

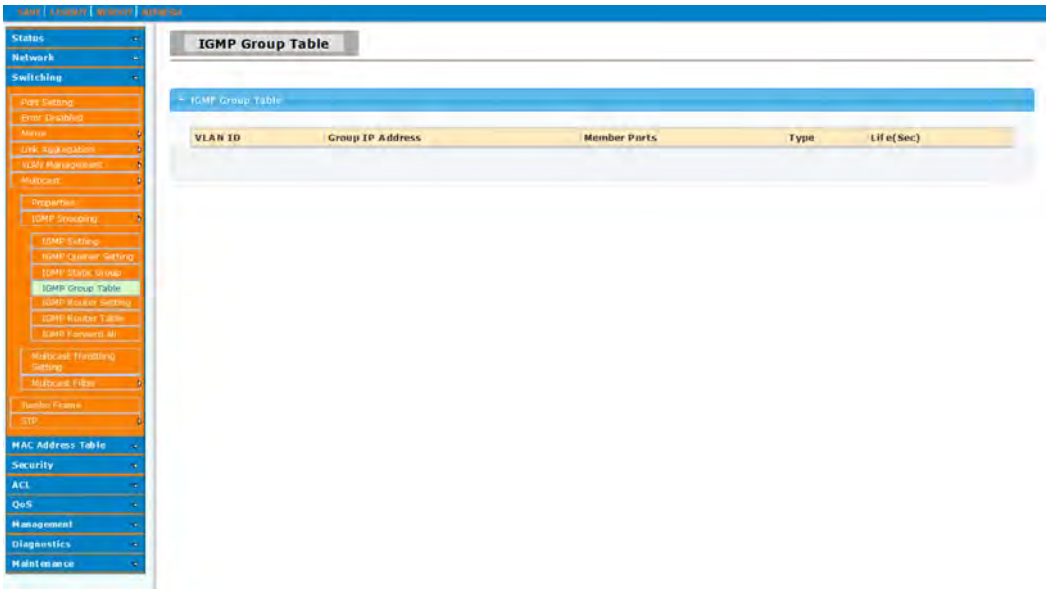
This page is used to configure specified ports as static member ports.



IGMP Group Table

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

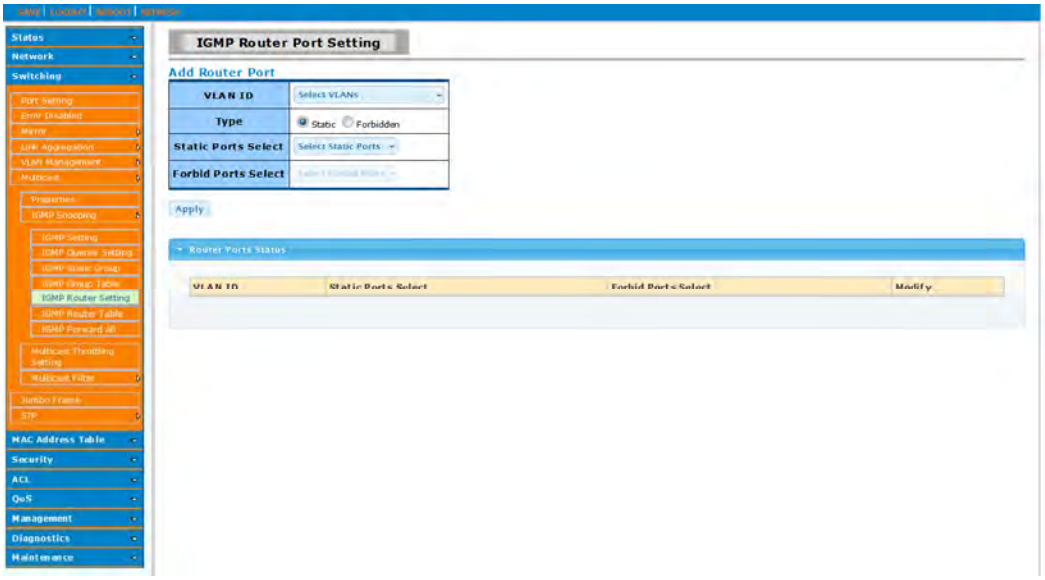
This page is used to display IGMP Group Table statistics information.



IGMP Router Port Setting

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

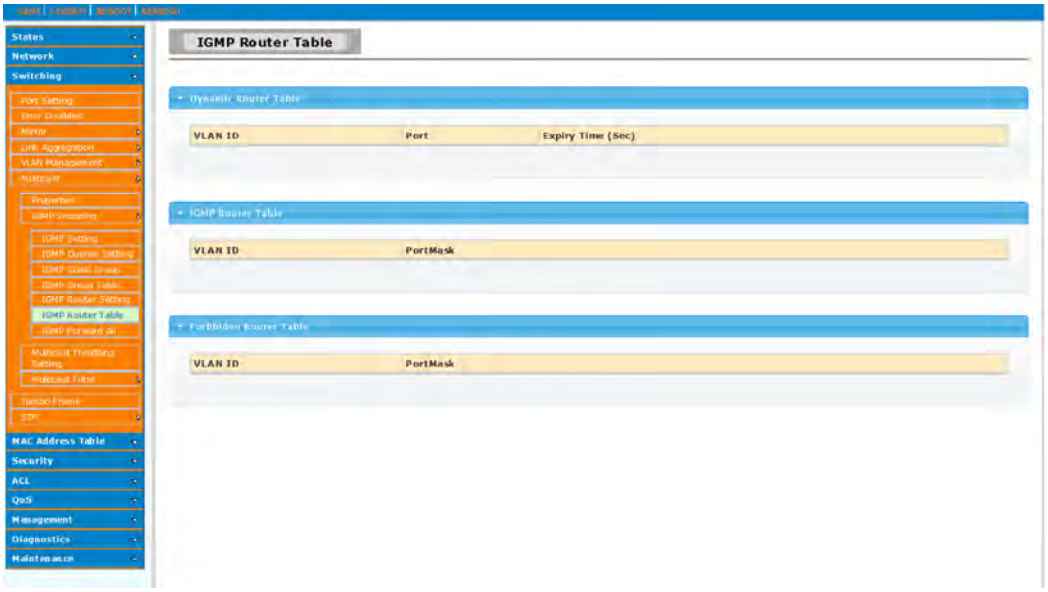
This page is used to configure specified ports as static route ports.



IGMP Router Table

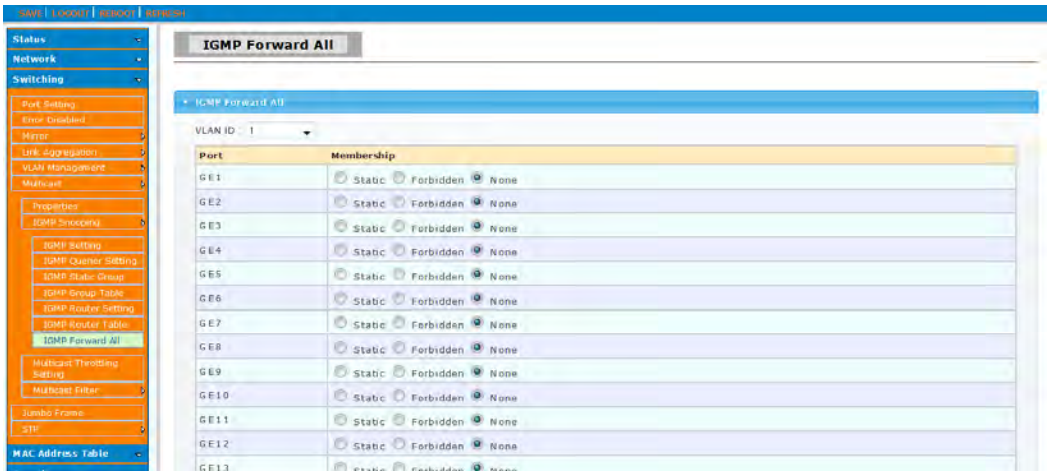
To display IGMP Router Table web page, click **Switching > Multicast > IGMP Snooping > IGMP Router Table**

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



IGMP Forward All

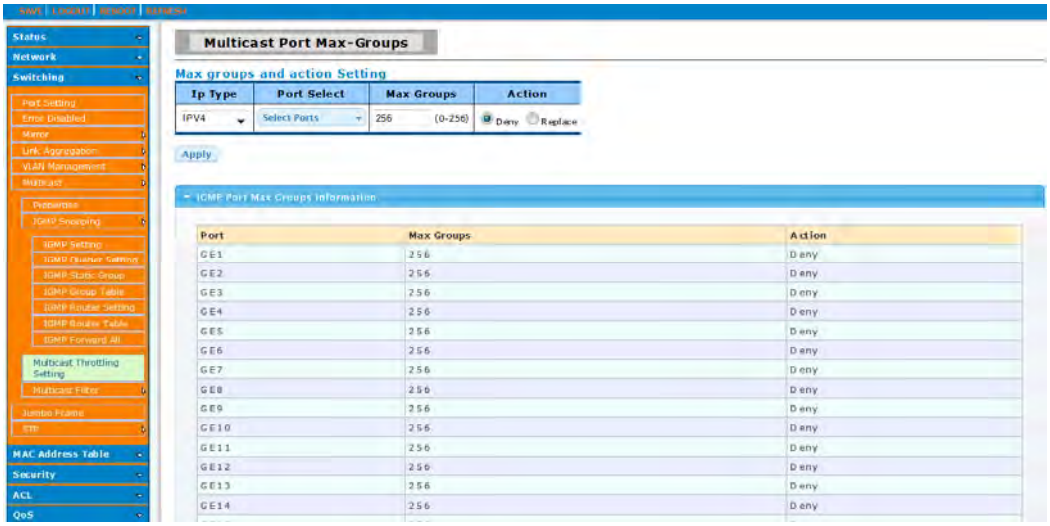
To display IGMP Forward All web page, click **Switching > Multicast > IGMP Snooping > IGMP Forward All**



5.3.6.3 *Multicast Port Max-Groups*

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

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

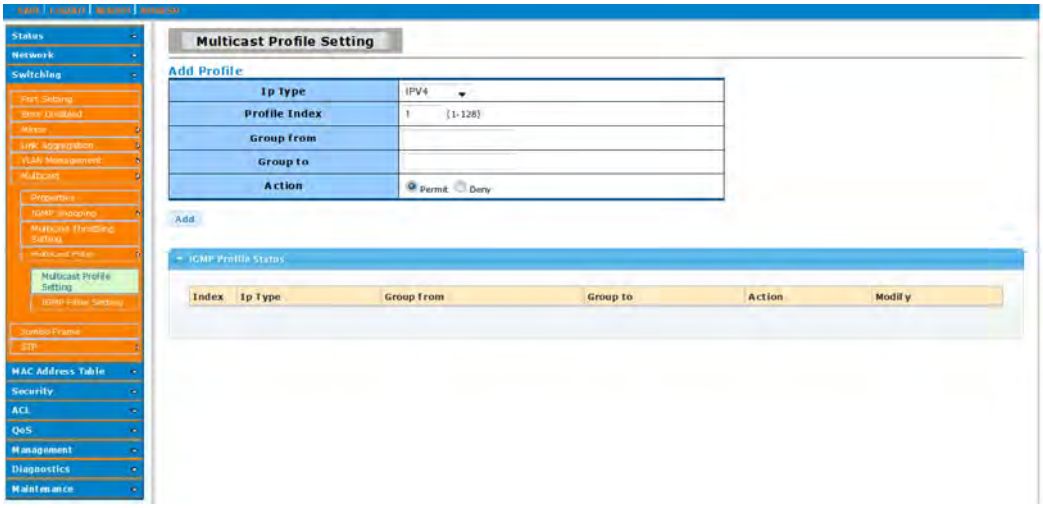


Multicast Filter

This page allow user to Create filter instance.

Multicast Profile Setting

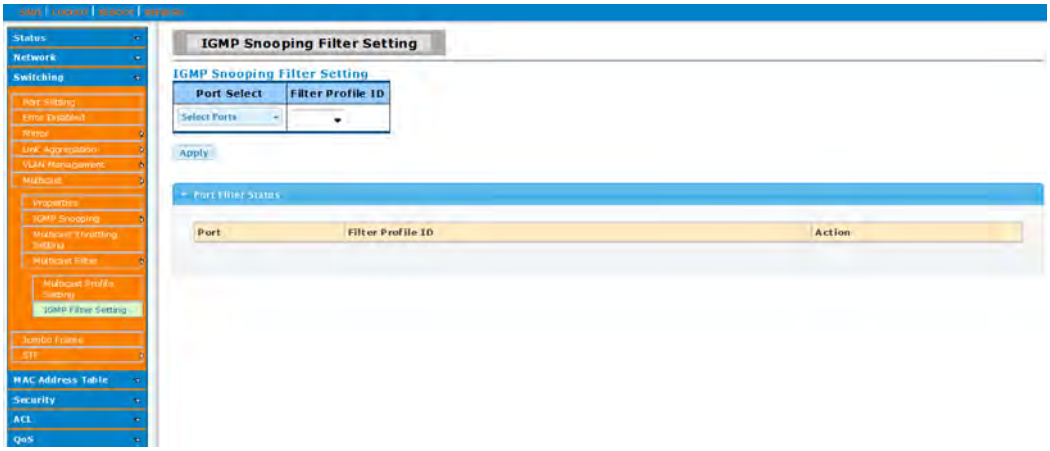
To display Multicast Profile Setting web page, click **Switching > Multicast >Multicast Filter > Multicast Profile Setting**



Multicast Profile Setting

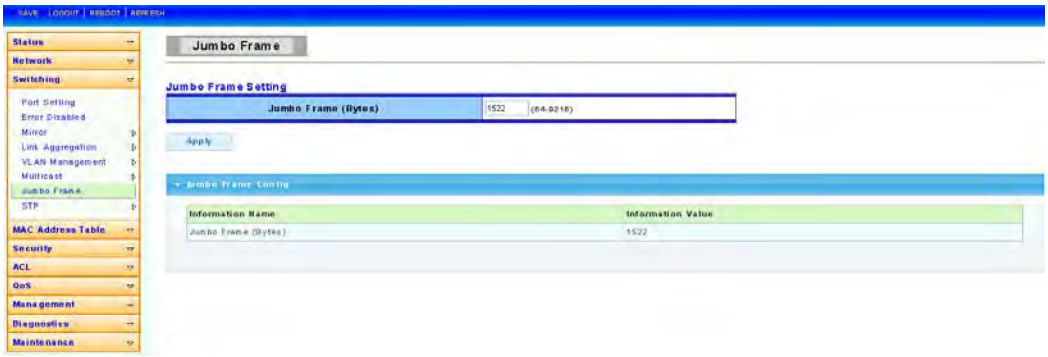
To display IGMP Filter Setting web page, click **Switching > Multicast > Multicast Filter >** IGMP Filter Setting

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



5.3.7 Jumbo Frame

To display Jum bo Frame web page, click **Switching > Jumbo Frame**



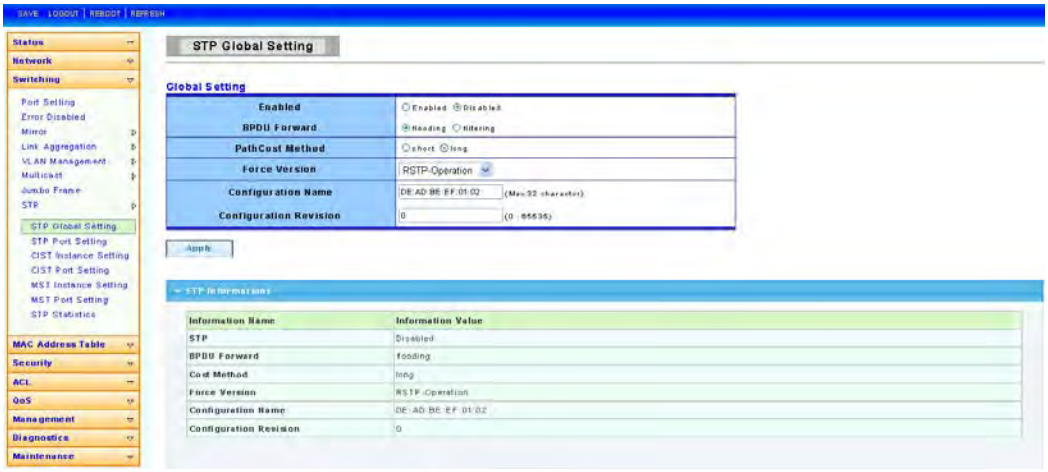
Jumbo Frame: Jumbo frame size. The valid range is 0 bytes – 9216 bytes.

STP

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

STP Global Setting

To display 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.

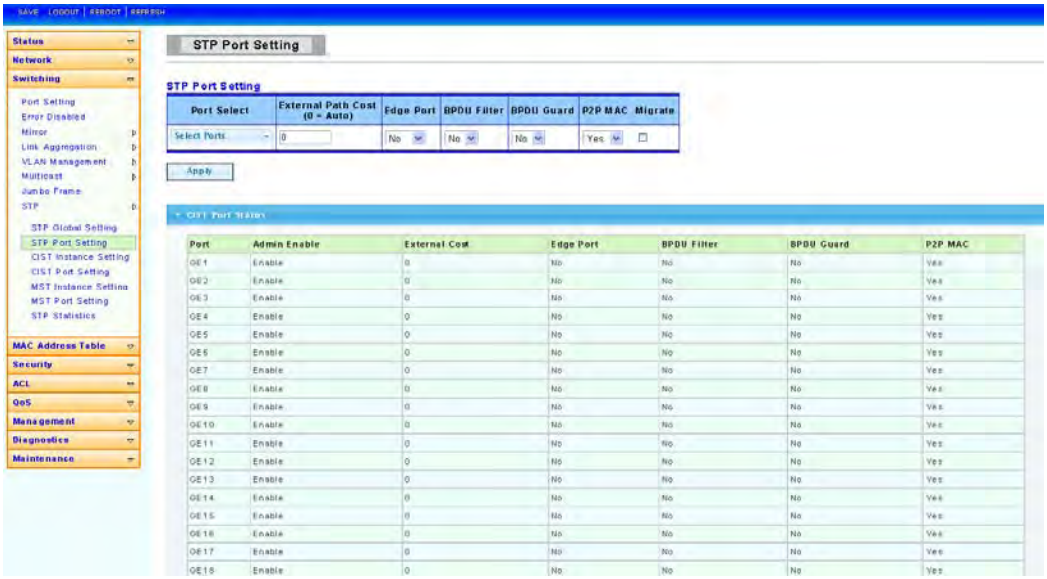
RSTP-Operation: 802.1w operation.

MSTP-Operation: 802.1s operation.

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

STP Port Setting

To display 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.

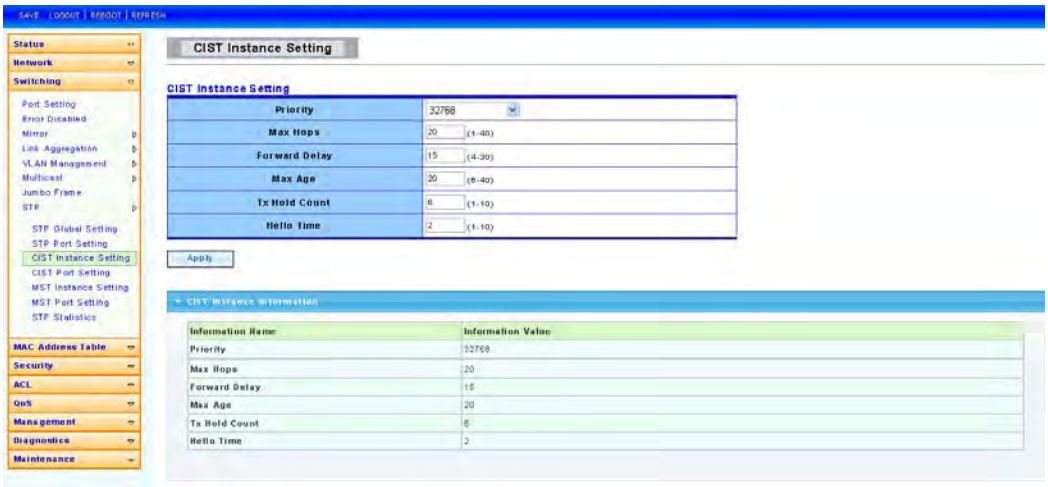
No: Force to false state.

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).

CIST Instance Setting

To display 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.

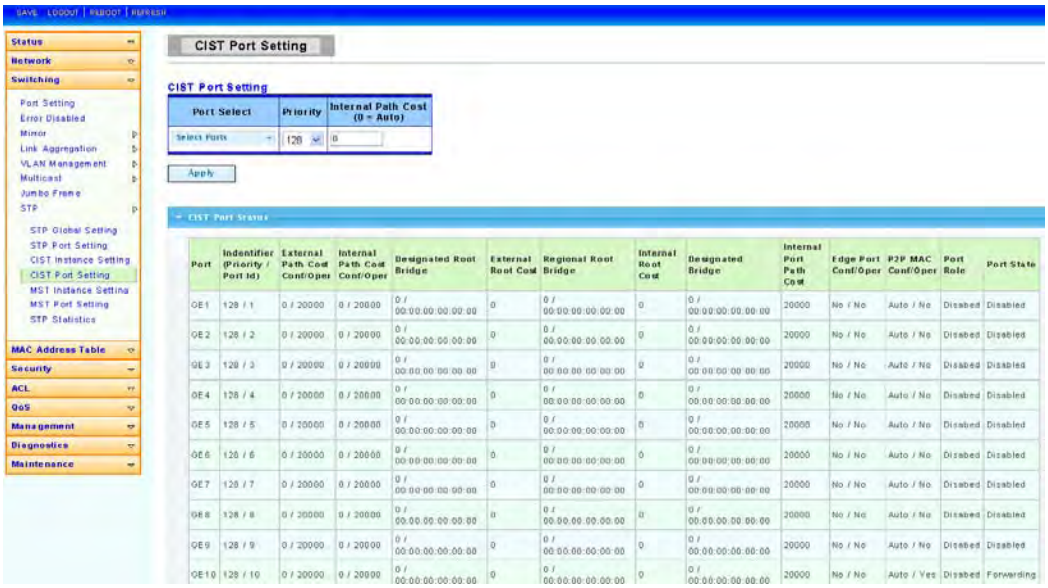
Max Age: Set the time any switch should wait before trying to change the STP topology after unhearing Hello BPDU.

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.

CIST Port Setting

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



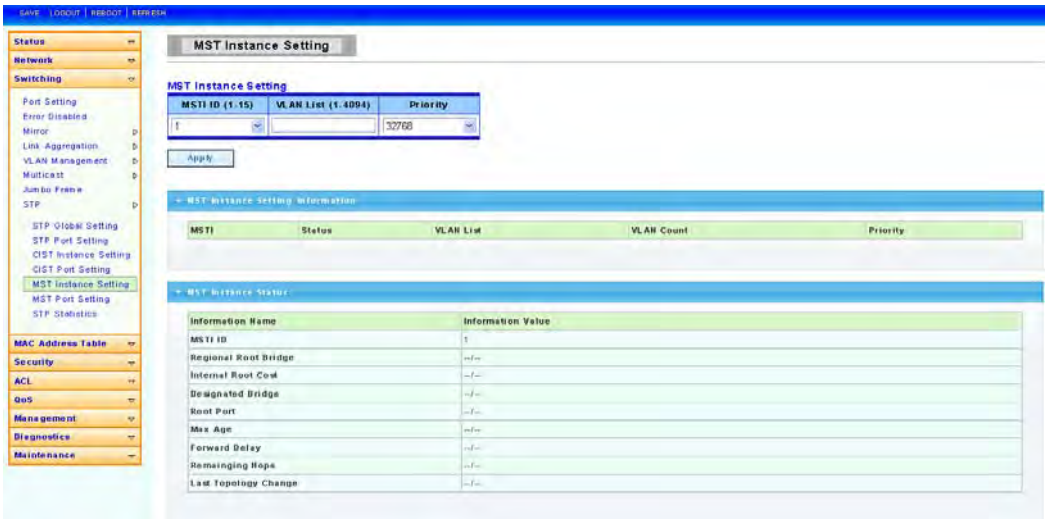
Port Select : Select the port list to specify which ports should apply this setting.

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`)

MST Instance Setting

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



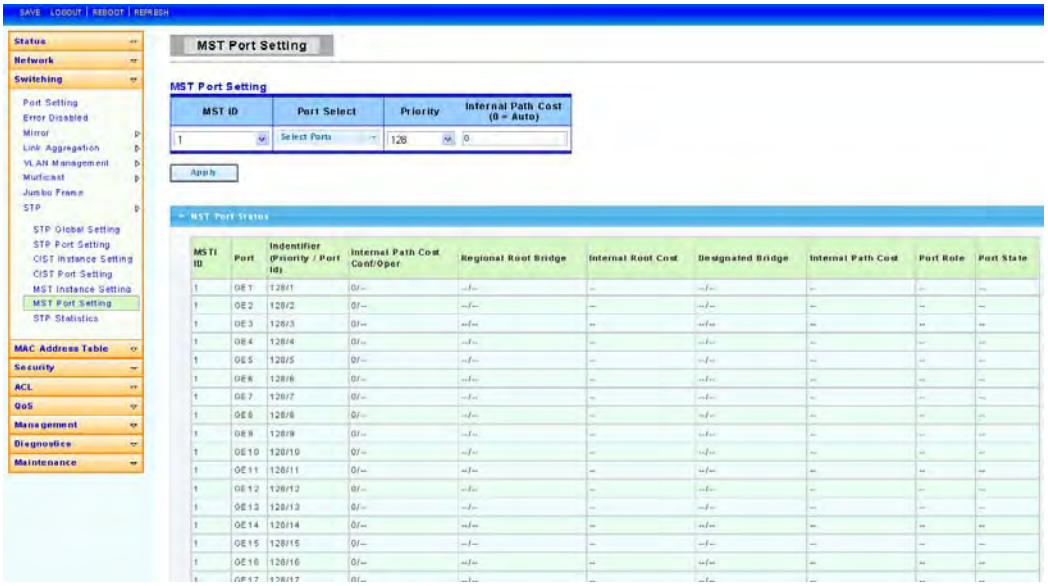
MSTI ID: Set the MSTI ID to specified the MST instance.

VLAN List: Set the VLAN List.

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

MST Port Setting

To display 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`)

STP Statistics

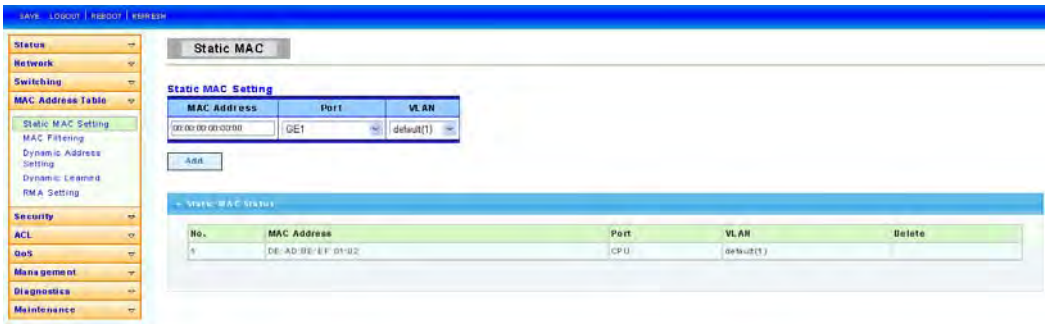
To display STP Statistics web page, click **Switching > STP > STP Statistics**


SAVE | LOGOUT | REBOOT | REFRESH
Status
Network
Switching
Port Setting
Error Disabled
Mirror
Link Aggregation
VLAN Management
Multicast
Jumbo Frame
STP
STP Global Setting
STP Port Setting
CIST Instance Setting
CIST Port Setting
MST Instance Setting
MST Port Setting
STP Statistics
MAC Address Table
Security
ACL
QoS
Management
Diagnostics
Maintenance
STP Statistics
STP Statistics
Port
Configuration BDPUs Received
TCN BDPUs Received
MSTP BDPUs Received
Configuration BDPUs Transmitted
TCN BDPUs Transmitted
MSTP BDPUs Transmitted
GE1 0 0 0 0 0 0
GE2 0 0 0 0 0 0
GE3 0 0 0 0 0 0
GE4 0 0 0 0 0 0
GE5 0 0 0 0 0 0
GE6 0 0 0 0 0 0
GE7 0 0 0 0 0 0
GE8 0 0 0 0 0 0
GE9 0 0 0 0 0 0
GE10 0 0 0 0 0 0
GE11 0 0 0 0 0 0
GE12 0 0 0 0 0 0
GE13 0 0 0 0 0 0
GE14 0 0 0 0 0 0
GE15 0 0 0 0 0 0
GE16 0 0 0 0 0 0
GE17 0 0 0 0 0 0
GE18 0 0 0 0 0 0
GE19 0 0 0 0 0 0
GE20 0 0 0 0 0 0
GE21 0 0 0 0 0 0
GE22 0 0 0 0 0 0
GE23 0 0 0 0 0 0
GE24 0 0 0 0 0 0

5.4 MAC ADDRESS TABLE

Static Mac Setting

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



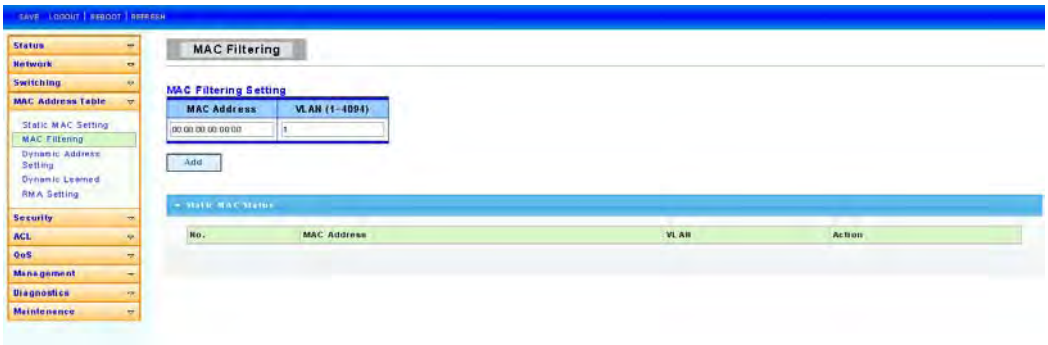
MAC Address: The MAC address to which packets will be statically forwarded. If Type is unicast, enter unicast MAC address in this field;If Type is multicast, enter multicast MAC address in this field.

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.

MAC Filtering

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



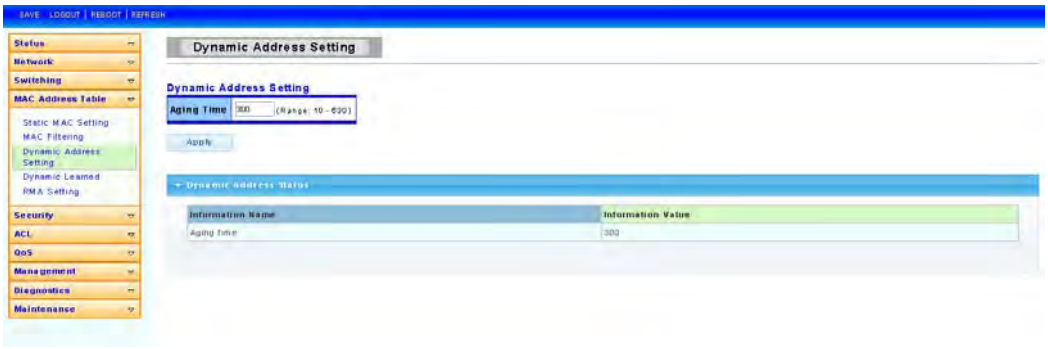
MAC Address: The MAC address to which packets will be filtered. This must be a unicast MAC address.

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

Dynamic Address Setting

To display 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

Dynamic Learned

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

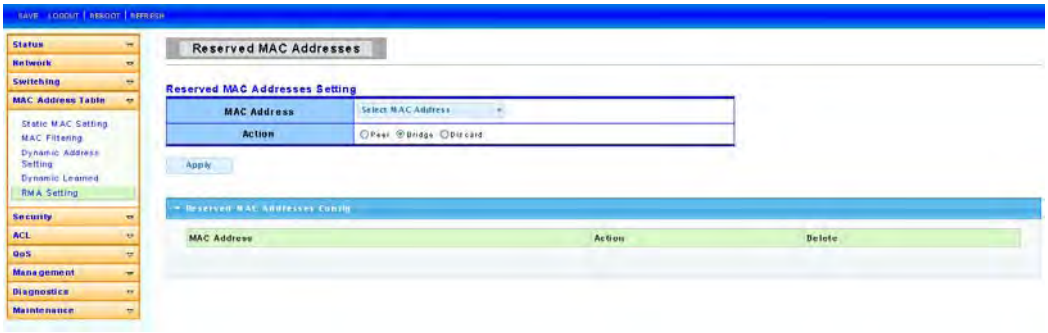
Port: Select the port number to show or clear dynamic MAC entries. If not select any port, VLAN and MAC address, the whole dynamic MAC table will be displayed or cleared.

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.

RMA MAC Address

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


SAVE | LOGOUT | REBOOT | REFRESH
Status
Network
Switching
MAC Address Table
Static MAC Setting
MAC Filtering
Dynamic Address Setting
Dynamic Learned
RMA Setting
Security
ACL
QoS
Management
Diagnostics
Maintenance
Reserved MAC Addresses
Reserved MAC Addresses Setting
MAC Address
Select MAC Address
Action
Peer
Bridge
Discard
Apply
Reserved MAC Addresses Config
MAC Address
Action
Delete

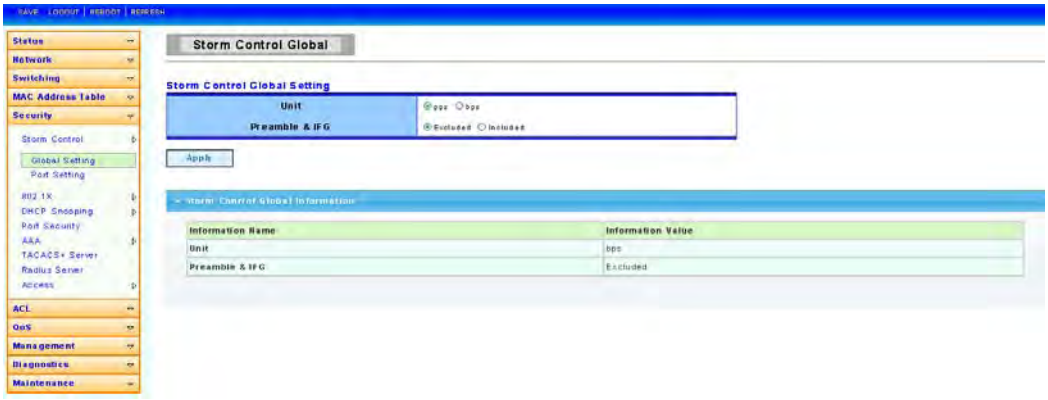
5.5 SECURITY

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

Storm Control

Global Setting

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



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

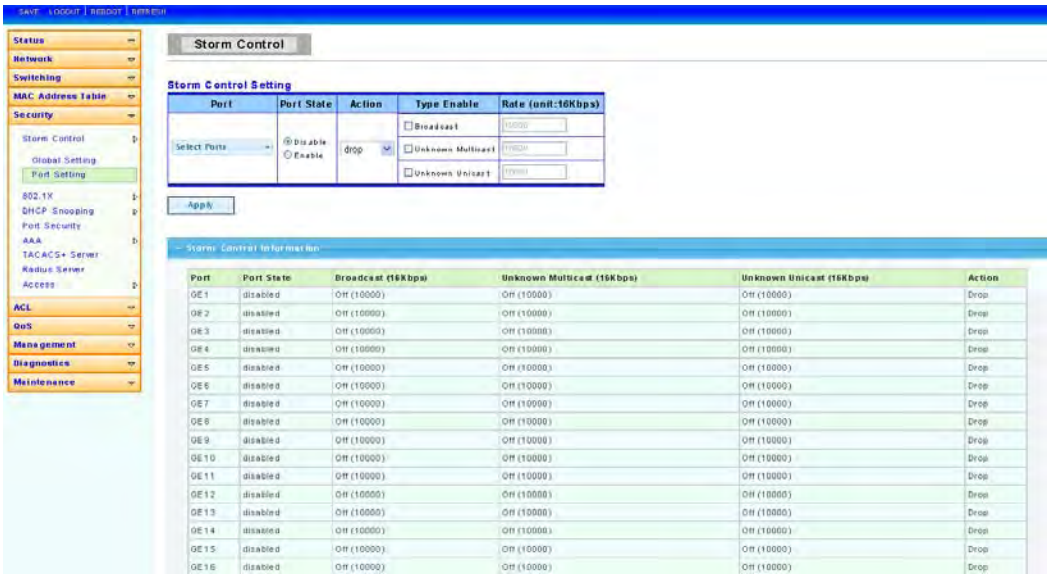
Preamble & IFG: Select the rate calculates w/o preamble & IFG (20 bytes).

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

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

Port Setting

To display Port Setting 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.

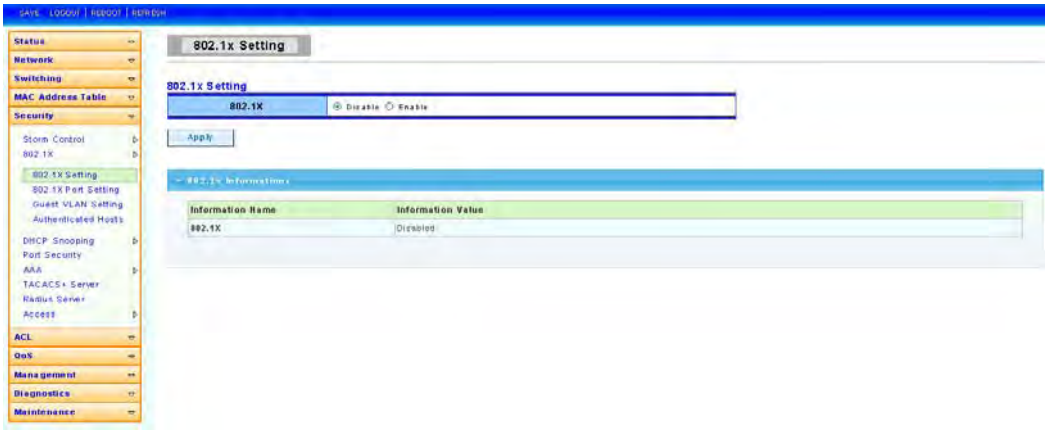
Rate: Value of storm control rate, Unit: pps (packet per-second) or Kbps (Kbits per-second) depends on global mode setting. The range is from 0 to 1000000.

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.

802.1X Setting

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



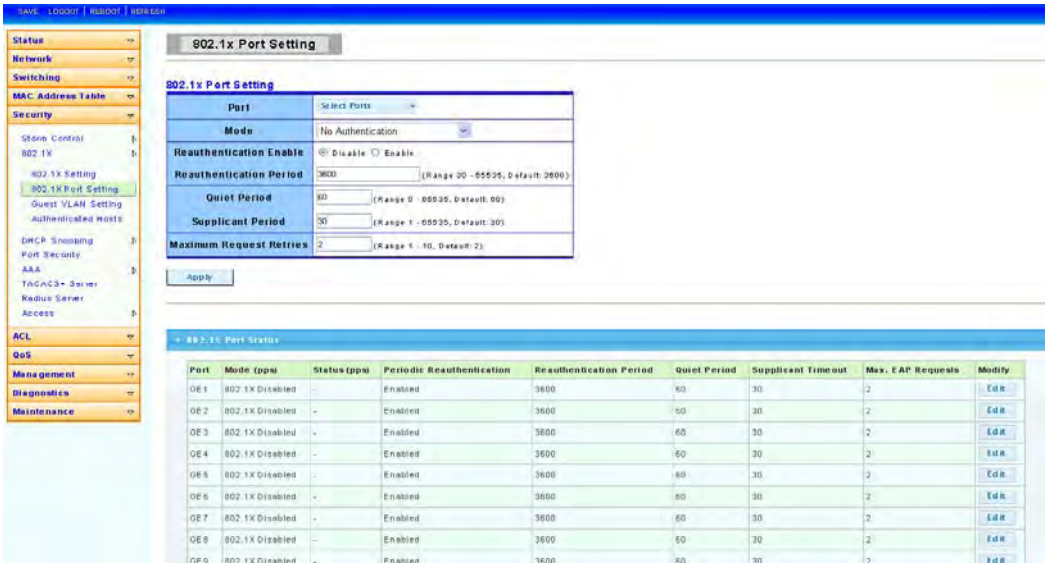
802.1X: Set the enabling status of 802.1X functionality.

Enable: Enable 802.1X.

Disable: Disable 802.1X.

802.1X Port Setting

To display 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.

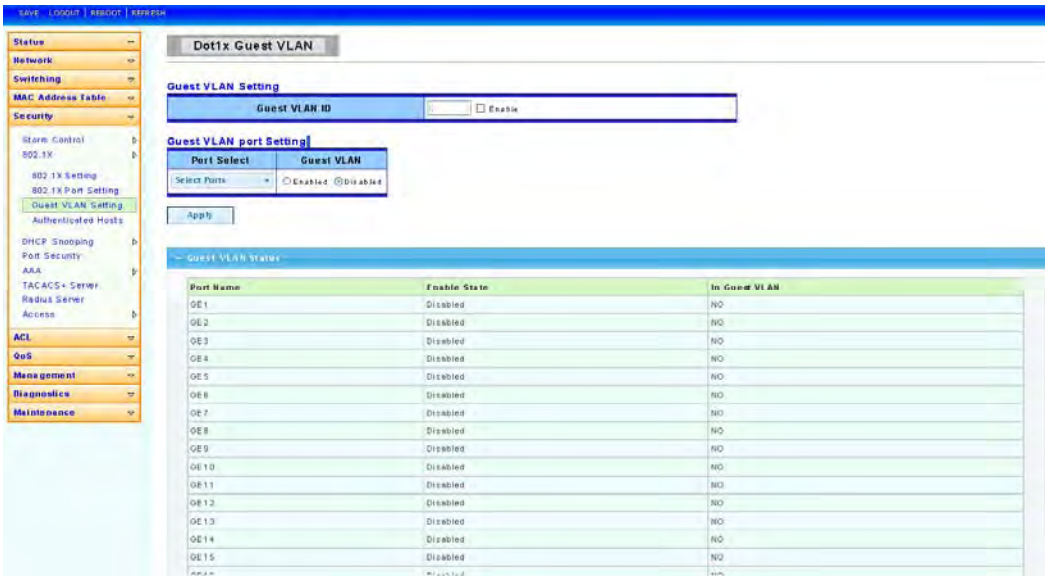
No Authentication:802.1X disabled.

Reauthentication Enable: Set the enabling status of802.1X reauthentication.

Reauthentication Period: Set the reauthentication period of 802.1X if reauthentication is enabled.

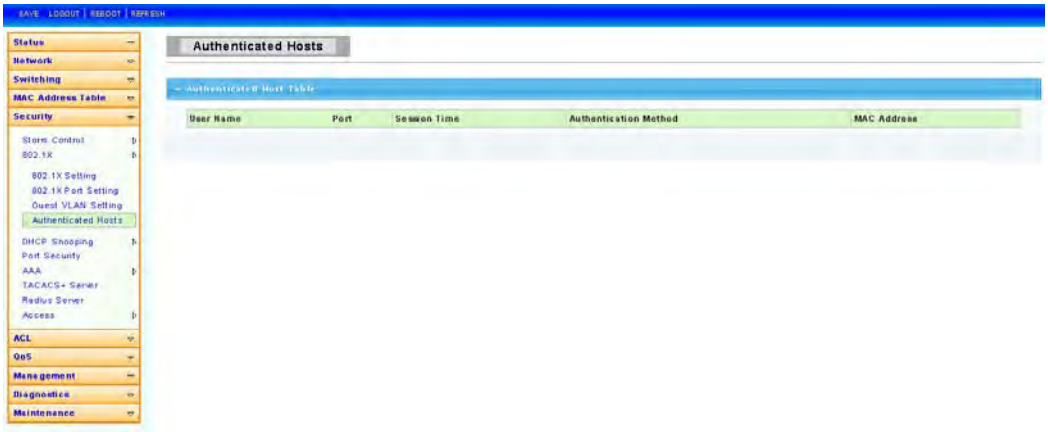
Guest VLAN Setting

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



Authenticated Hosts

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



DHCP Snooping

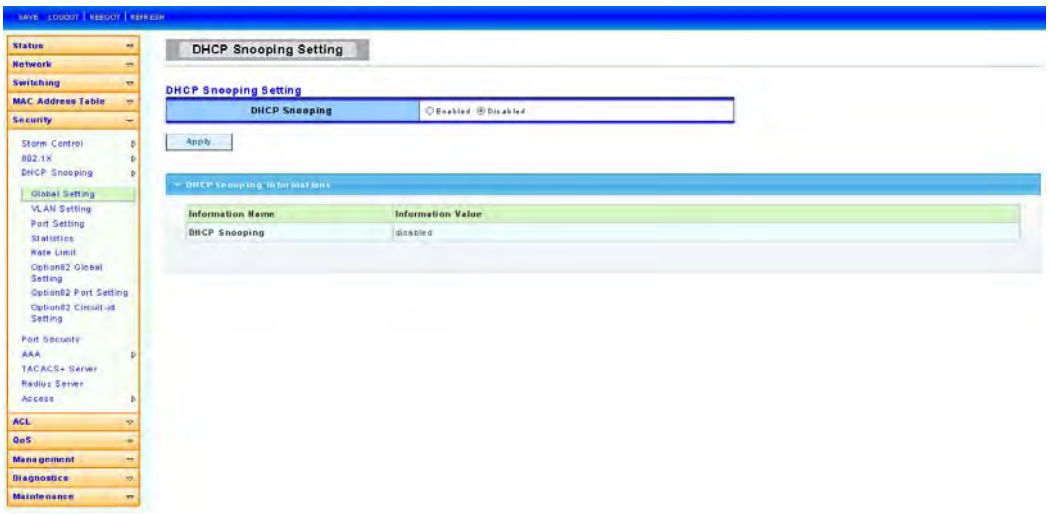
When the switch opens DHCP-Snooping, it will snoop DHCP message and receive DHCP Request and abstract and record the IP address and MAC address from DHCP ACK message. Besides, DHCP-Snooping admits one physical port setting as creditable port or discreditable ports. Creditable

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.

Global Setting

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

This page is used to open DHCP Snooping function

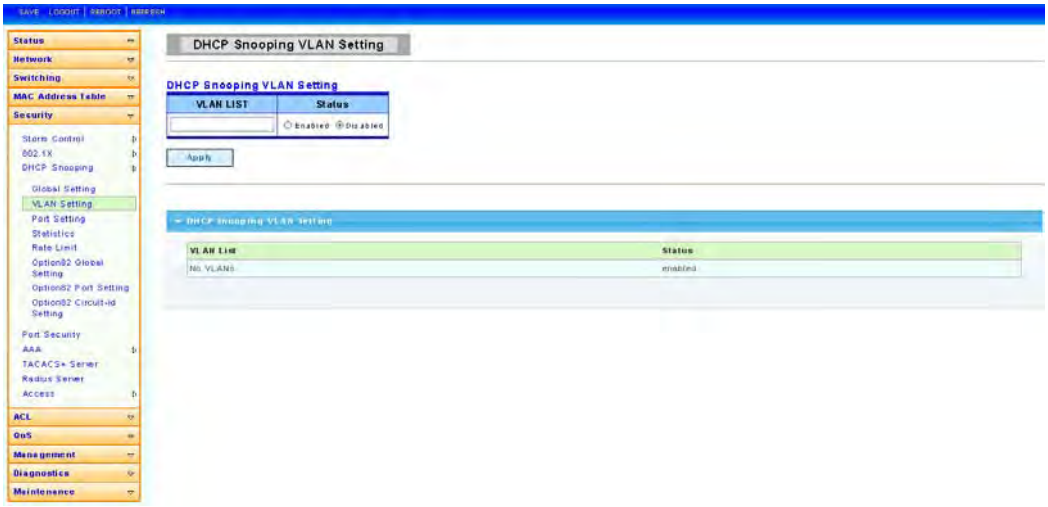


DHCP Snooping: enable or disable DHCP Snooping function

VLAN Setting

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

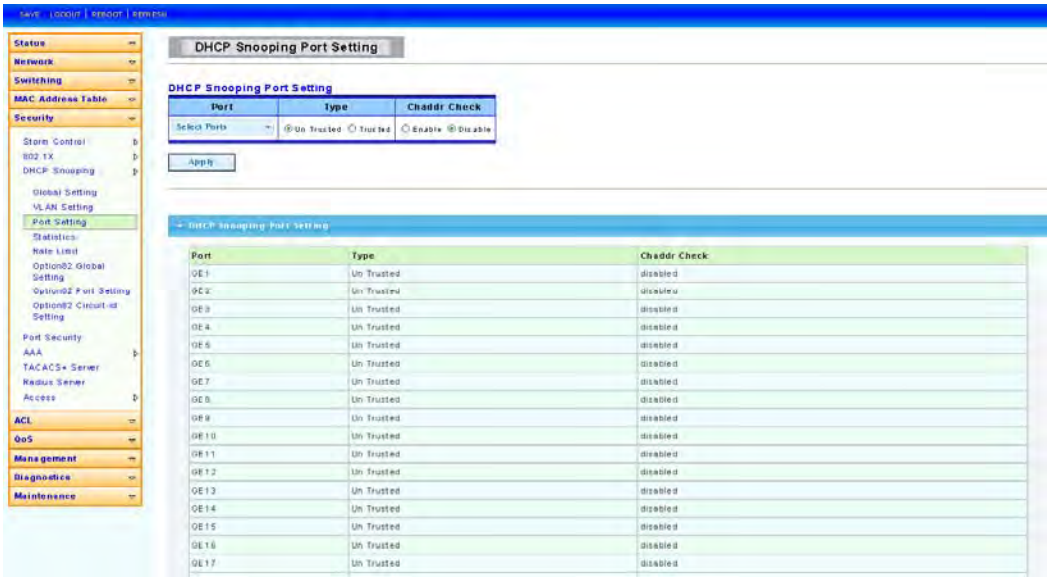
Specific VLAN starts DHCP Snooping



Port Setting

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

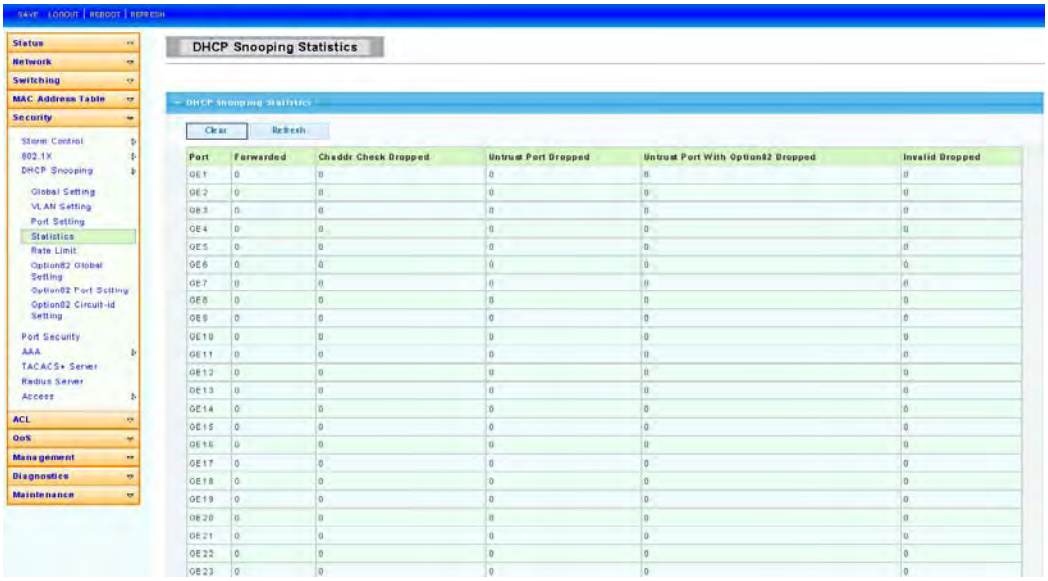
This page allow user to make the specific port is configured for DHCP Snooping trust port.



Statistics

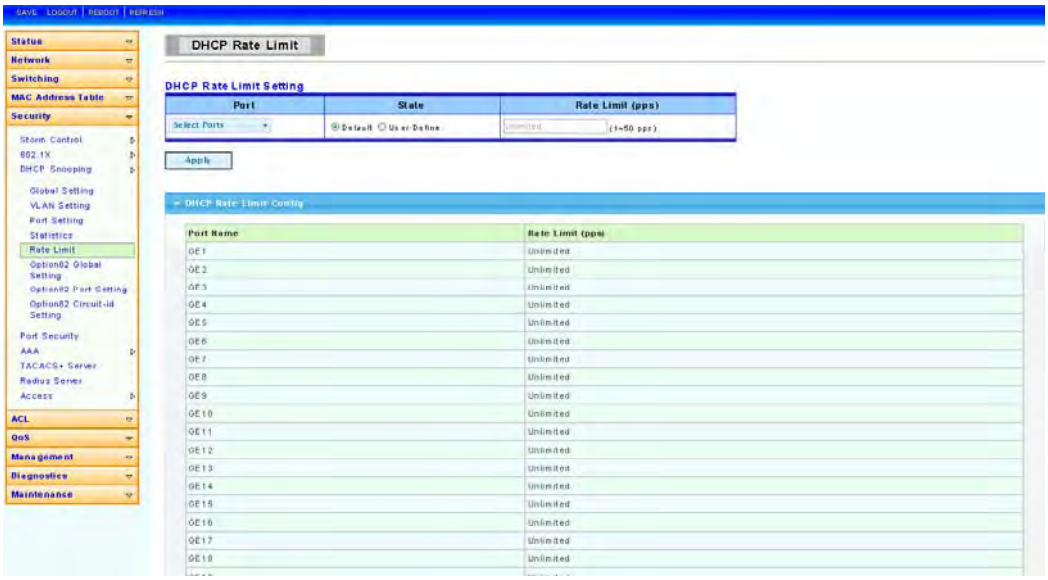
To display Statistics web page, click **Security > DHCP Snooping > Statistics**

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



Rate Limit

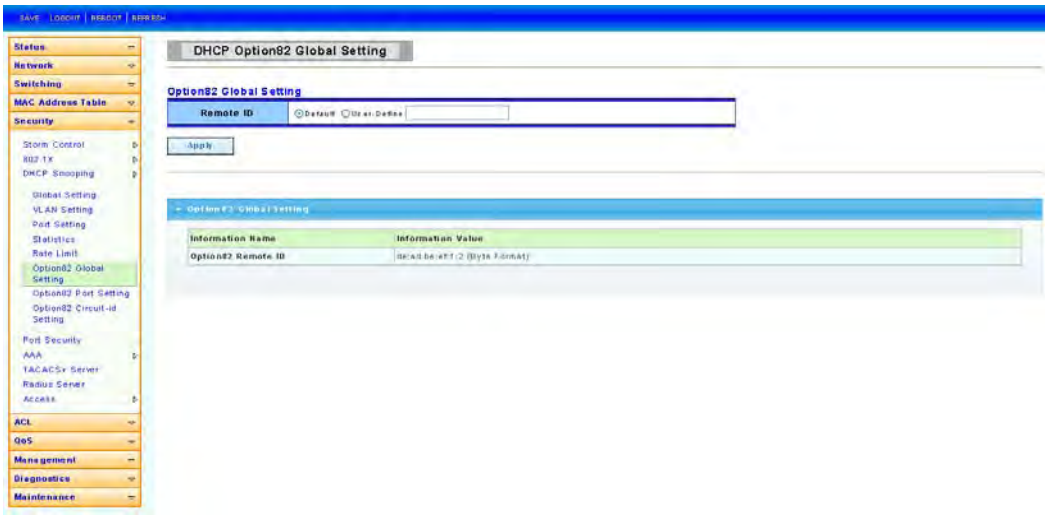
To display Rate Limit web page, click **Security > DHCP Snooping > Rate Limit**



Option82 Global Setting

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

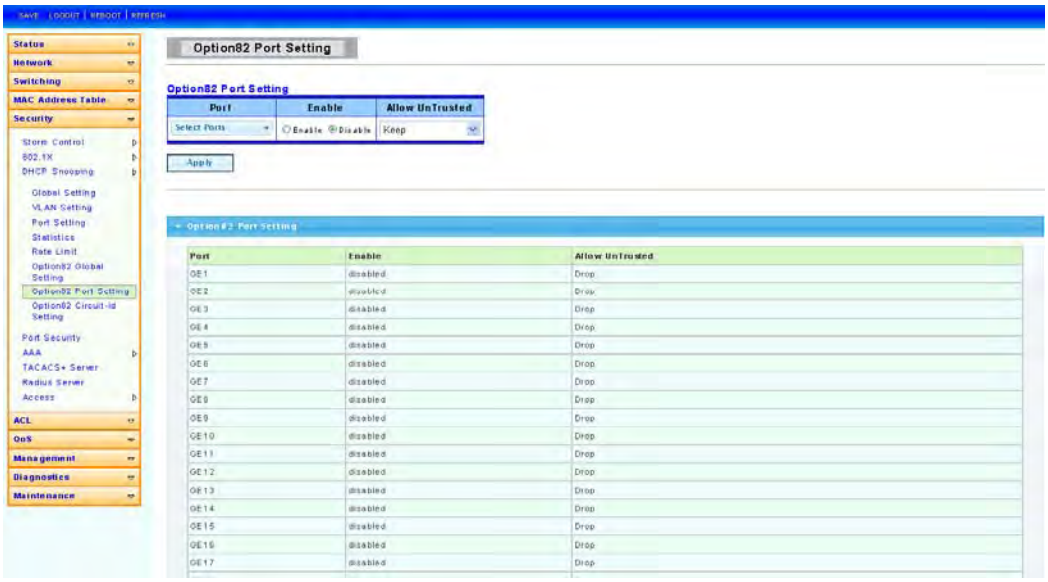
This page is used to configure DHCP Snooping support Option82 strategy.



Option82 Port Setting

To display 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.



Option82 Circuit-ID Setting

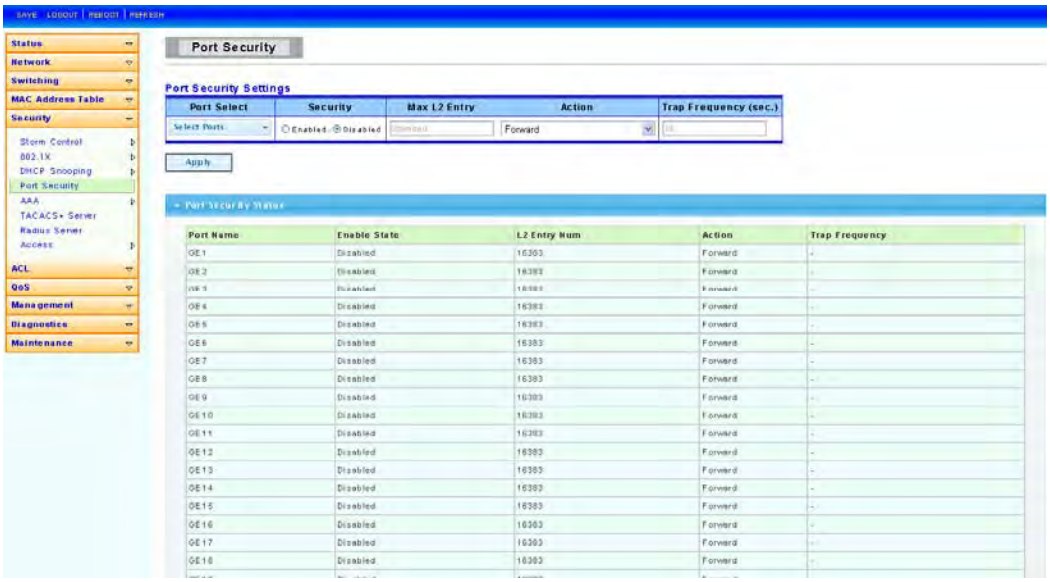
To display Option82 Circuit-ID Setting web page, click **Security> DHCP Snooping > Option82 Circuit-ID Setting**

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

Port Security

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

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



Port Select: Select one or multipleports 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.

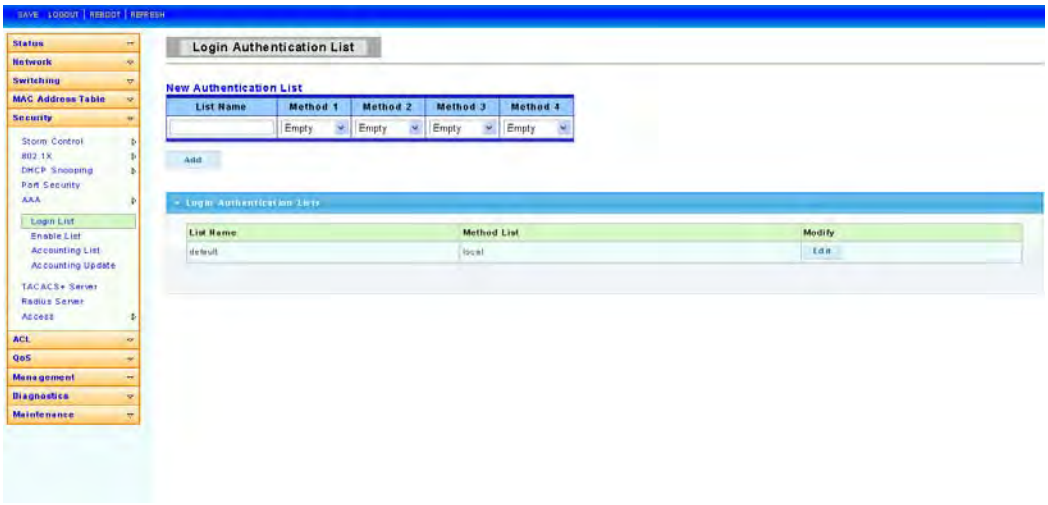
Max L2 Entry: The total number of MAC addresses entry which can be learn by a port.

AAA

Login List

To display Login 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 besupported 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 besupported 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 besupported 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.

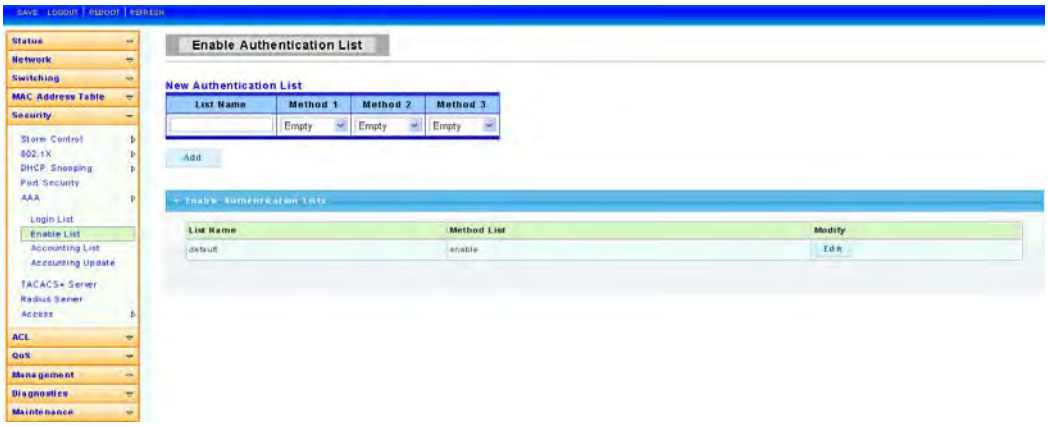
Radius: Use remote Radius server to authenticate. Not supported now, it will besupported in the future.

Enable: Use local enable password to authenticate

Enable List

To display Login 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 besupported 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 besupported in the future.

Method 3: Select third priority of enable authentication method.

Enable: Use local enable password to authenticate.

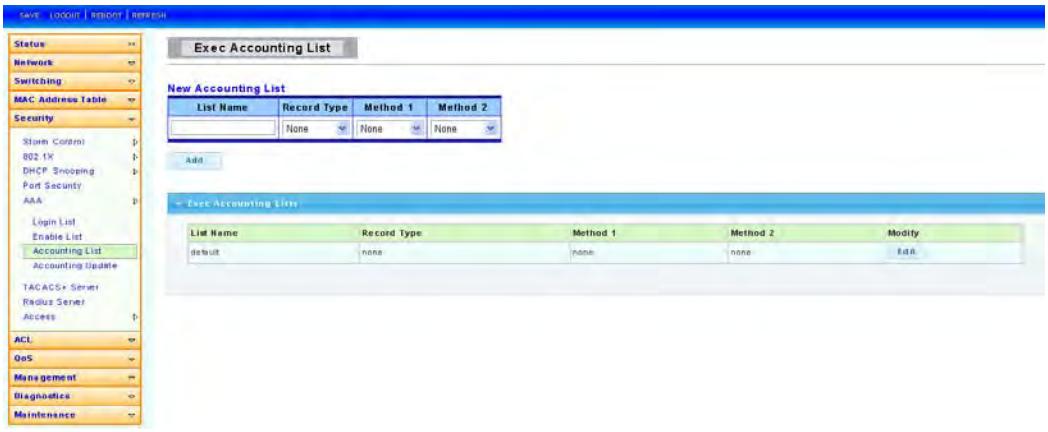
Tacacs+: Use remote TACACS+ server to authenticate.

Radius: Use remote Radius server to authenticate. Not supported now, it will besupported in the future.

Accounting List

To display 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 ofexec accounting method.

Tacacs+: Use remote TACACS+ server to accounting.

Radius: Use remote Radius server to accounting. Not supported now, it will besupported in the future.

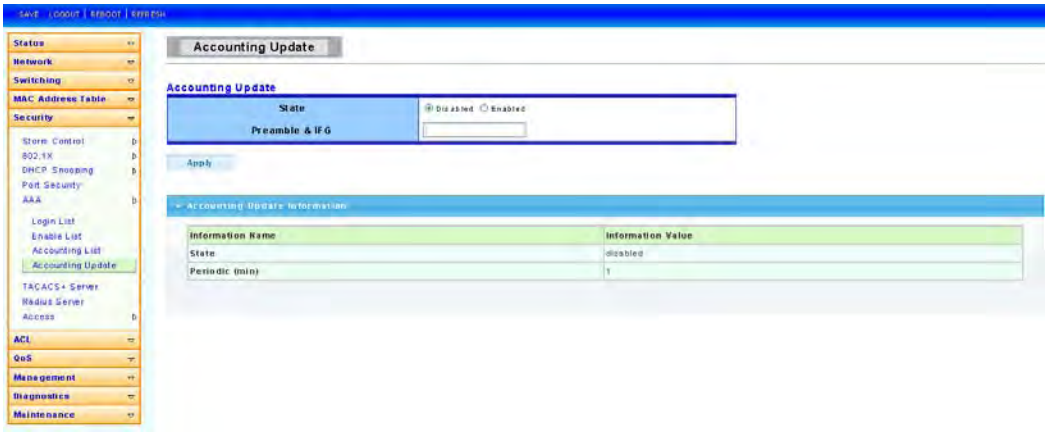
Method 2: Select second priority ofexec accounting method.

Tacacs+: Use remote TACACS+ server to accounting.

Radius: Use remote Radius server to accounting. Not supported now, it will besupported in the future.

Accounting Update

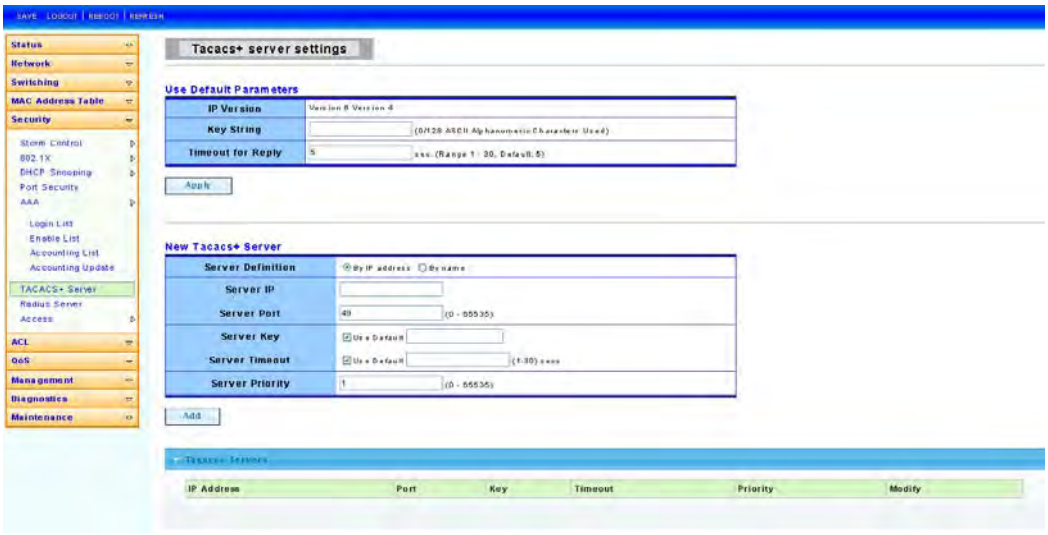
To display Accounting Update web page, click **Security> AAA > Accounting Update**



Tacacs+ Server

To display Tacacs+ server web page, click **Security> AAA >Tacacs+ server**

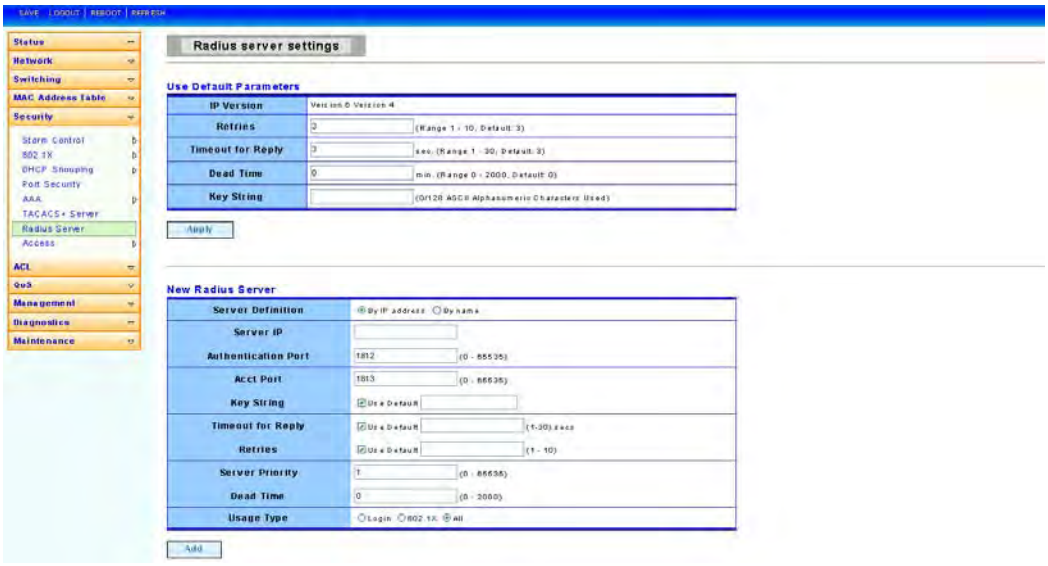
This page allow user to add, edit or delete TACACS+ server settings.



Radius server

To display Radius server web page, click **Security > AAA > Radius server**

This page is used to set about radius server.

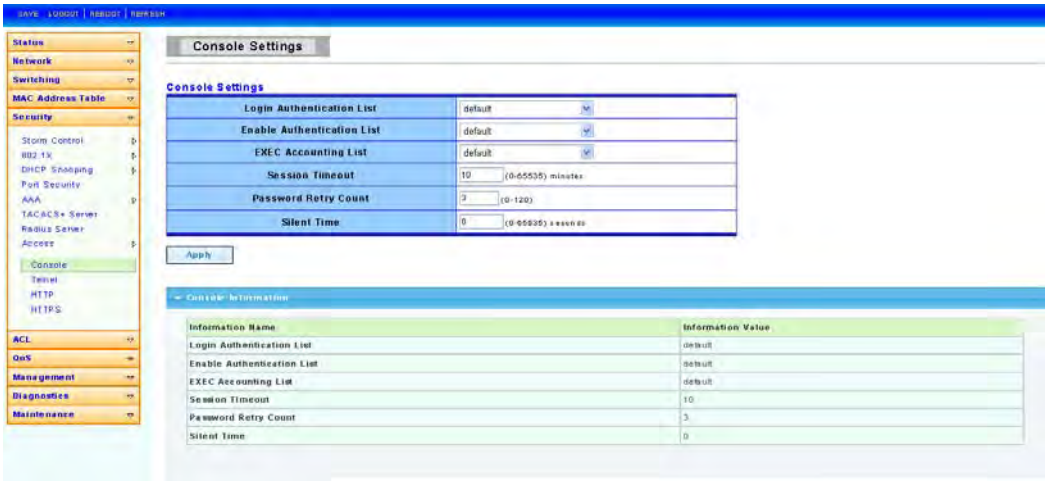


Access

Console

To display Console 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 Authorization List: Select one of the EXEC authorization lists we configured in “EXEC List” page.

Commands Authorization List: Select one of the commands authorization lists we configured in “Commands List” page.

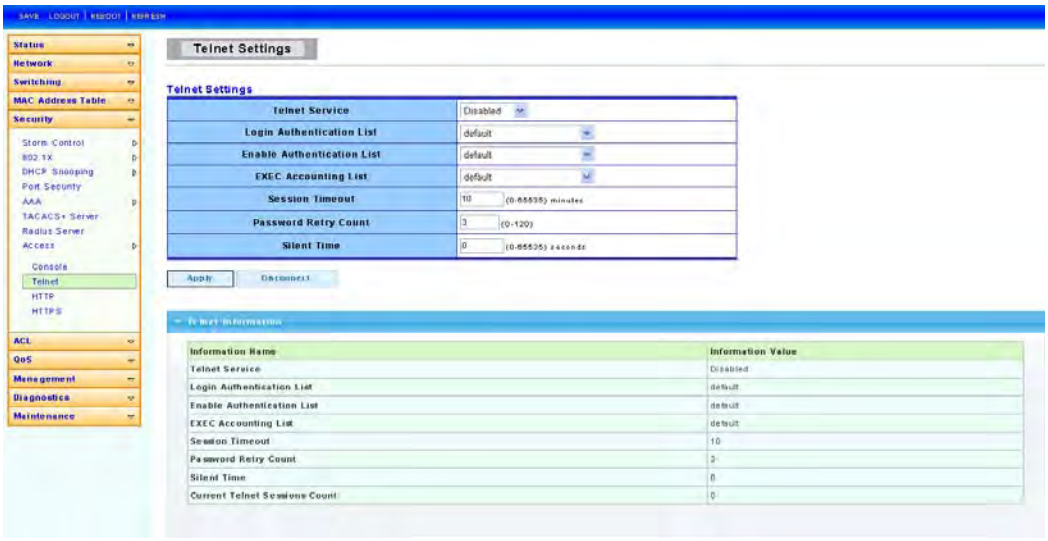
EXEC Accounting List: Select one of the EXEC accounting lists we configured in “Accounting List” page.

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.

Telnet

To display Telnet 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.

Commands Authorization List: Select one of the commands authorization lists we configured in “Commands List” page.

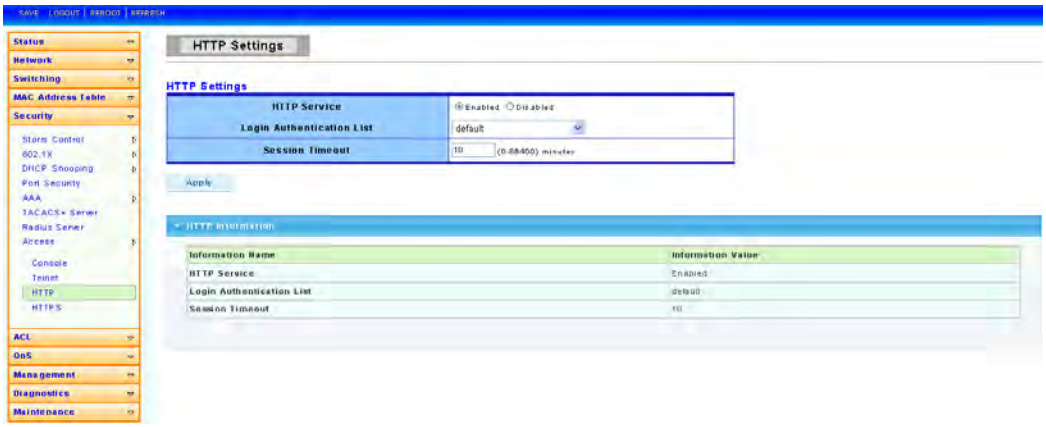
EXEC Accounting List: Select one of the EXEC accounting lists we configured in “Accounting List” page.

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

HTTP

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

This page allow user to combine all kinds of AAA lists to HTTP line. The user accesses switch WEBUI 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

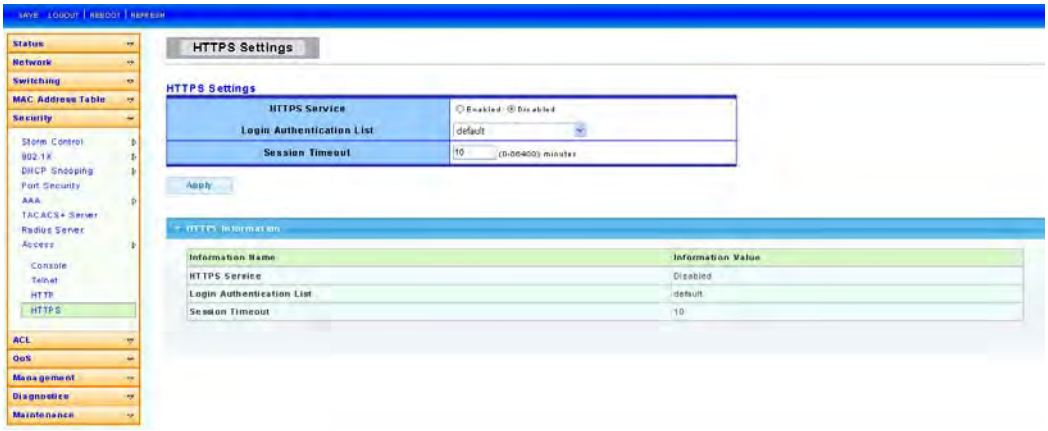
“Login List” page.

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.

HTTPS

To display HTTPS 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.

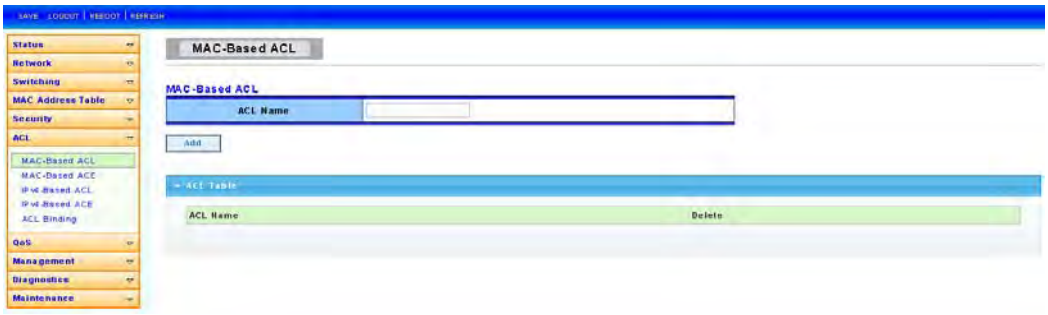
Session Timeout: Set session timeout minutes for user access WEB from HTTPS protocol. If user does not response after session timeout minute, WEBUI will logout automatically. 0 minutes means never timeout.

5.6 ACL

MAC-Based ACL

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

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

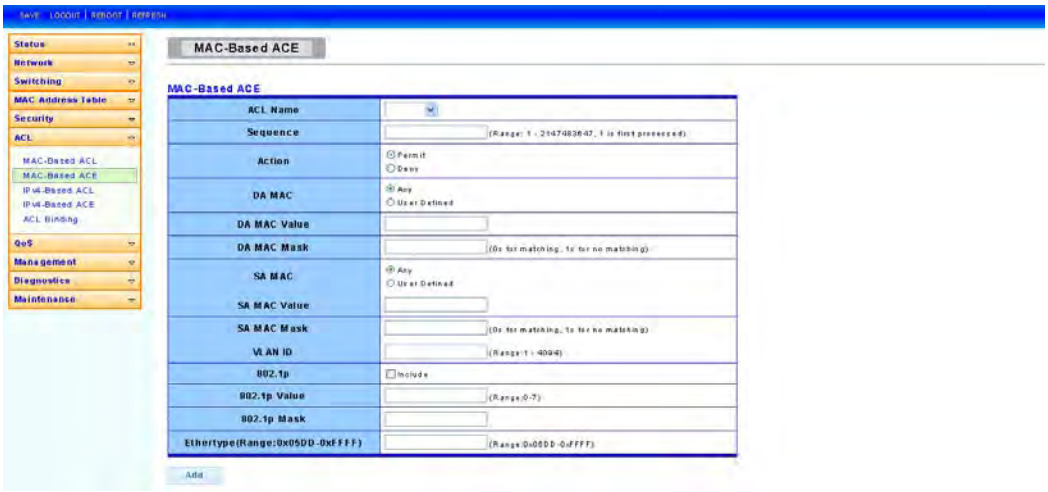


ACL Name: Enter ACL name in this field.

MAC-Based ACE

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

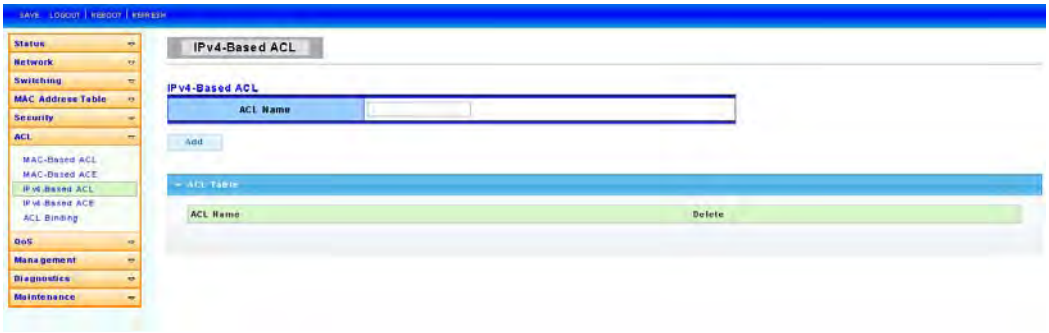
This page allow user to set Based on MAC address expanding ACL list, matching corresponding MAC and setting the ports as drop or forward.



IPv4-Based ACL

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

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



IPv4-Based ACE

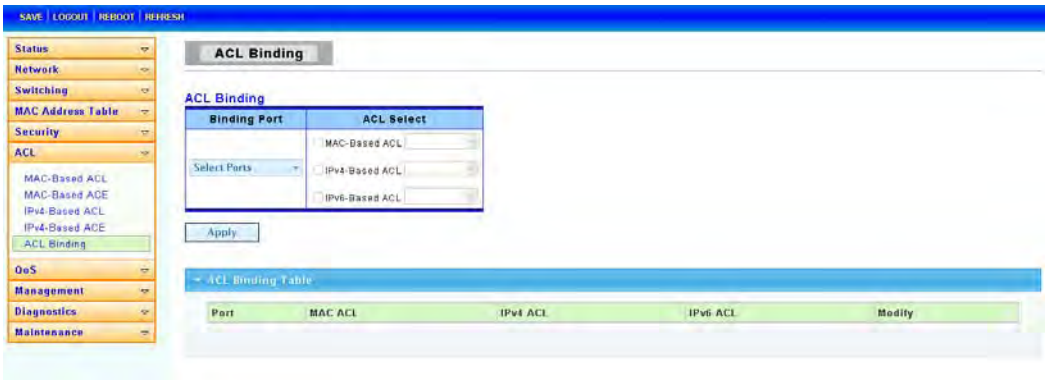
To display IPv4-Based ACE web page, click **ACL > IPv4-Based ACE**

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.

ACL Binding

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

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


SAVE | LOGOUT | REBOOT | REFRESH
Status
Network
Switching
MAC Address Table
Security
ACL
MAC-Based ACL
MAC-Based ACE
IPv4-Based ACL
IPv4-Based ACE
ACL Binding
QoS
Management
Diagnostics
Maintenance
ACL Binding
ACL Binding
Binding Port
ACL Select
Select Ports
MAC-Based ACL
IPv4-Based ACL
IPv6-Based ACL
Apply
ACL Binding Table
Port
MAC ACL
IPv4 ACL
IPv6 ACL
Modify

5.7 QoS

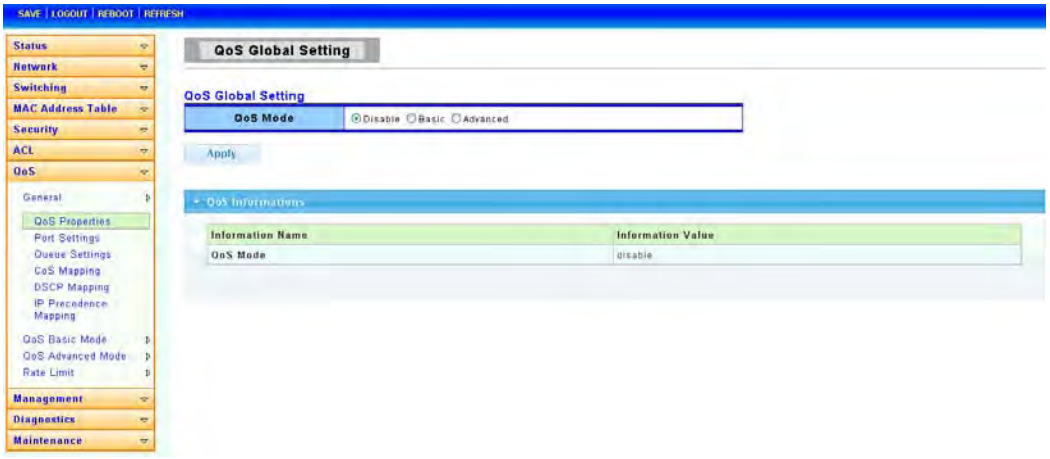
Use the QoS pages to configure settings for the switch QoS interface and how the switch connects to a remote server to get services.

General

QoS Properties

To display QoS properties web page, click **QoS > General > QoS properties**

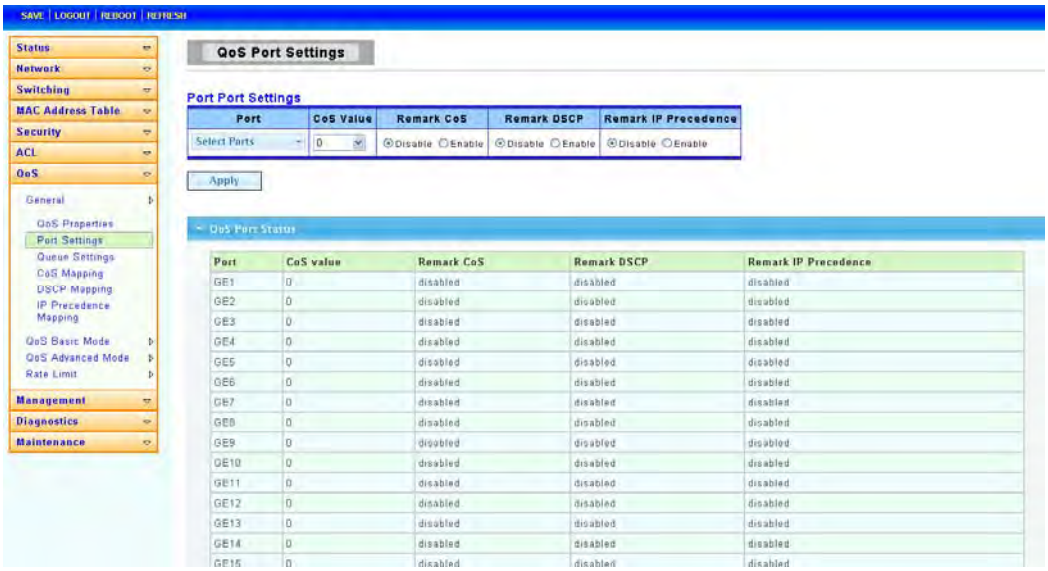
This page allow user to set QoS mode such basic or advanced.



Port Settings

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

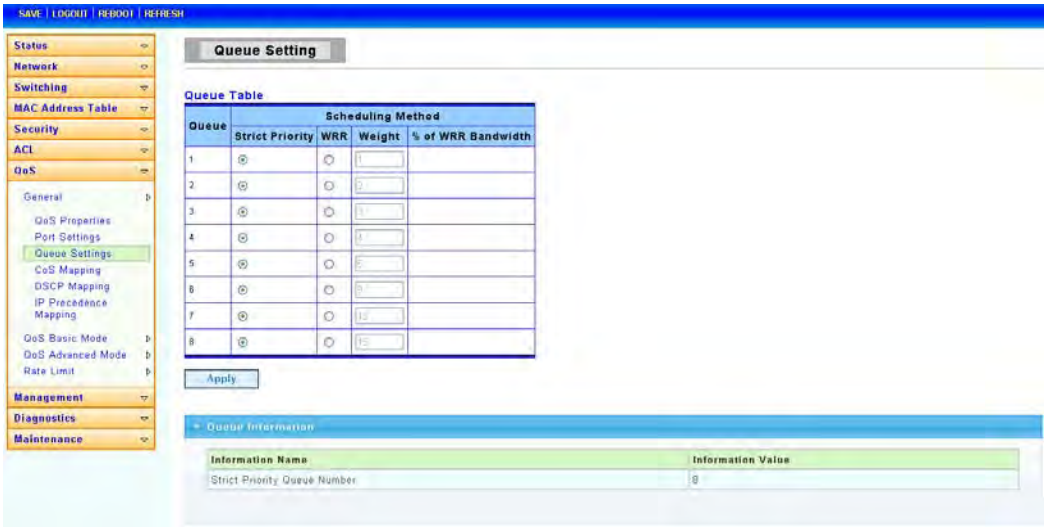
This page is used to give the QoS instance port configuration.



Queue Settings

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

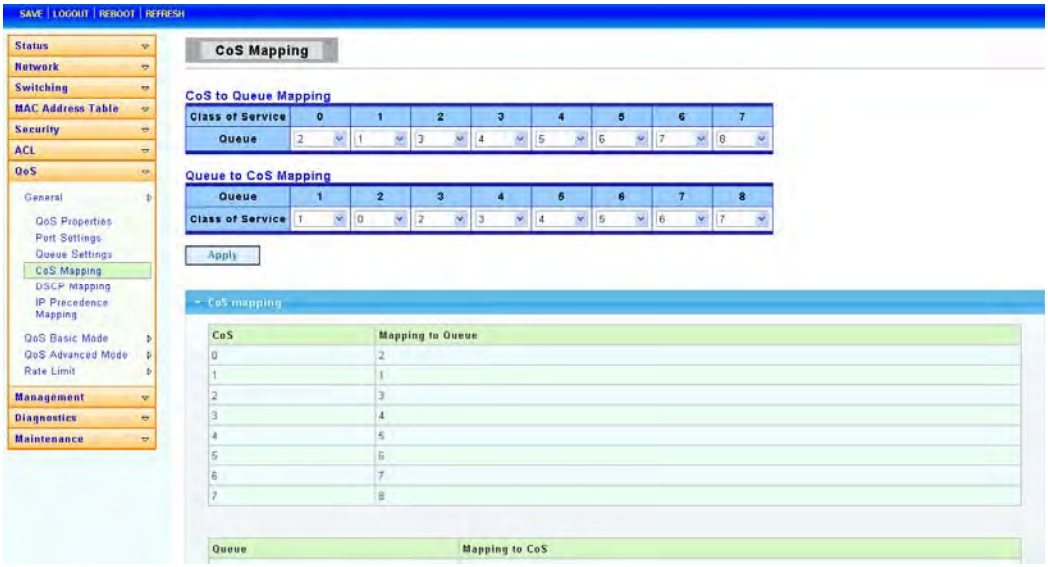
This page allow user to set Set the QoS instance queue scheduling model.



COS Mapping

To display COS Mapping web page, click **QoS > General > COS Mapping**

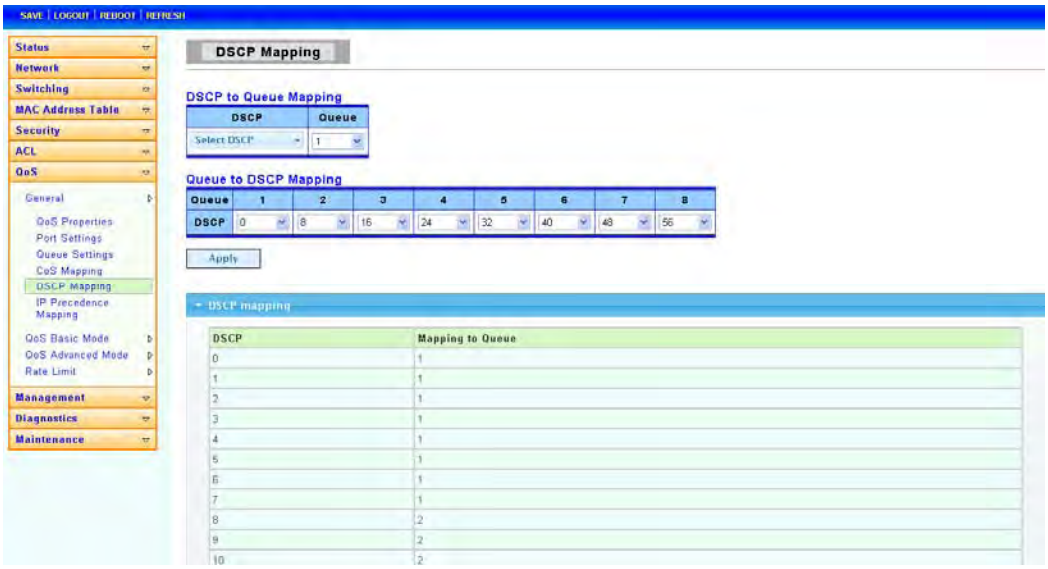
The page allow user to set QoS instance of COS Mapping.



DSCP Mapping

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

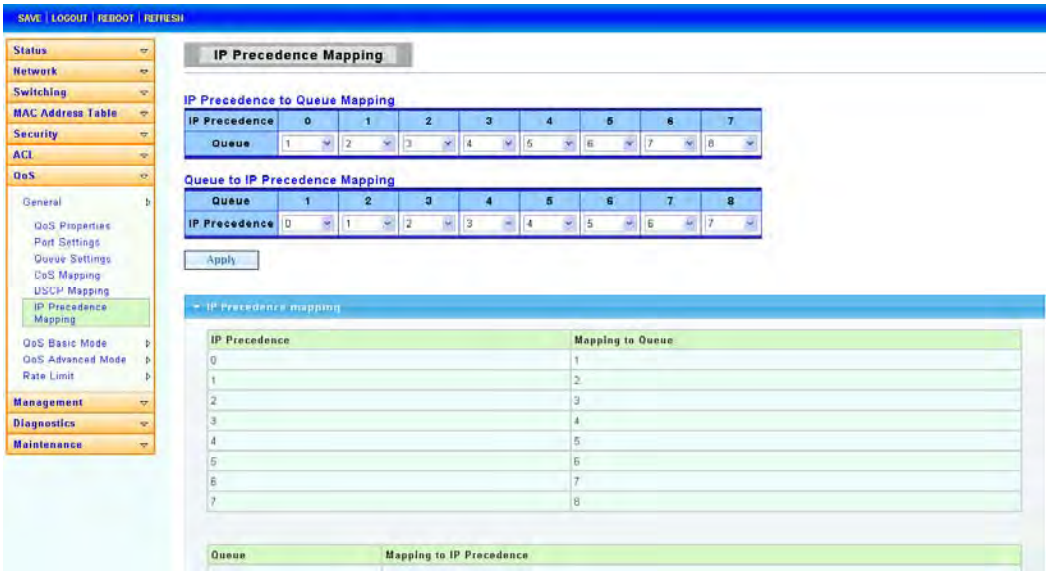
The page allow user to set QoS instance of DSCP Mapping.



IP Precedence Mapping

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

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

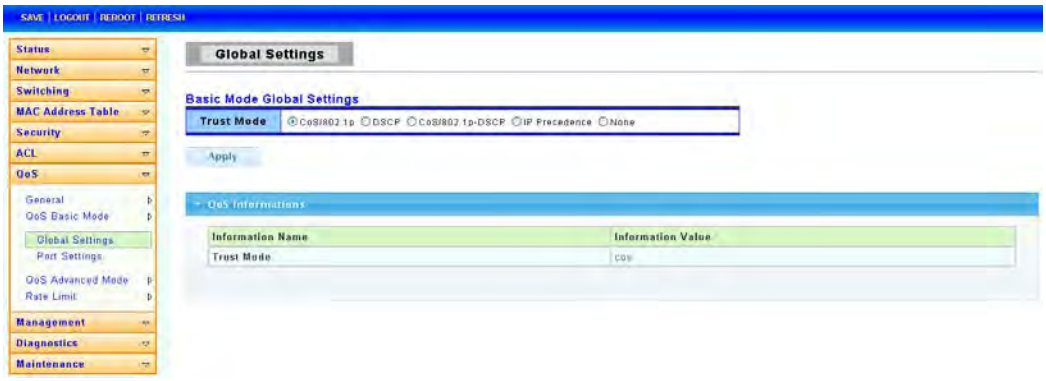


QoS Basic Mode

Global Settings

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

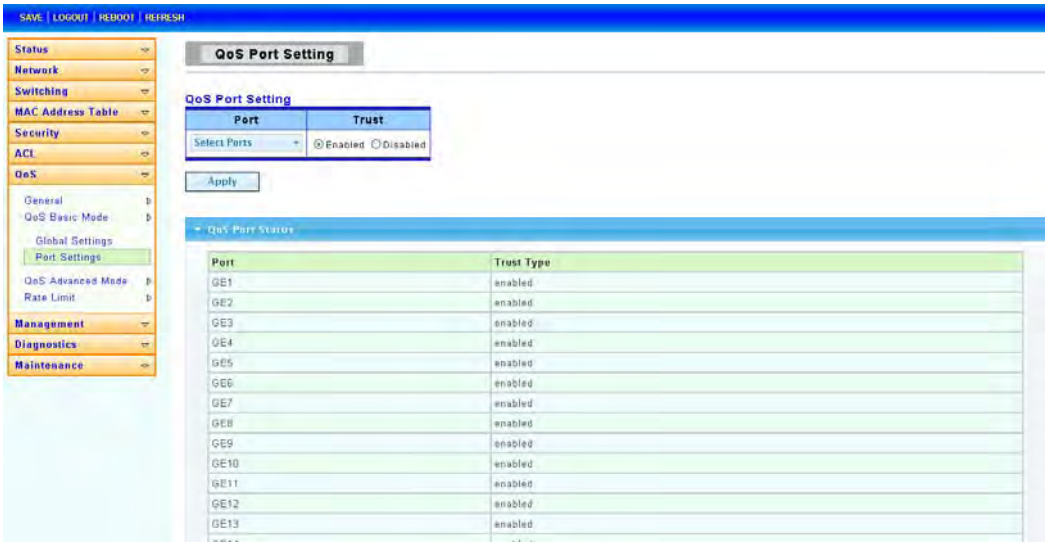
This page allow user to set QoS for trust mode on basic mode global settings.



Port Settings

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

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

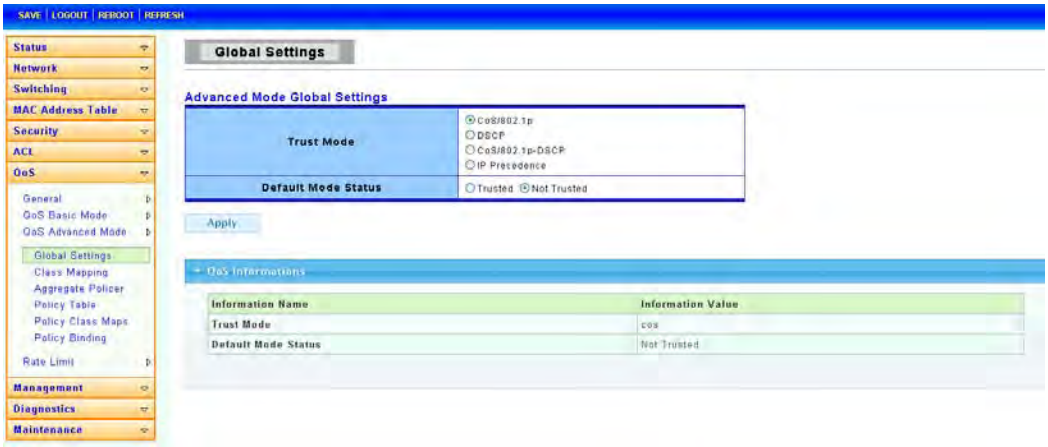


QoS Advanced Mode

Global Settings

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

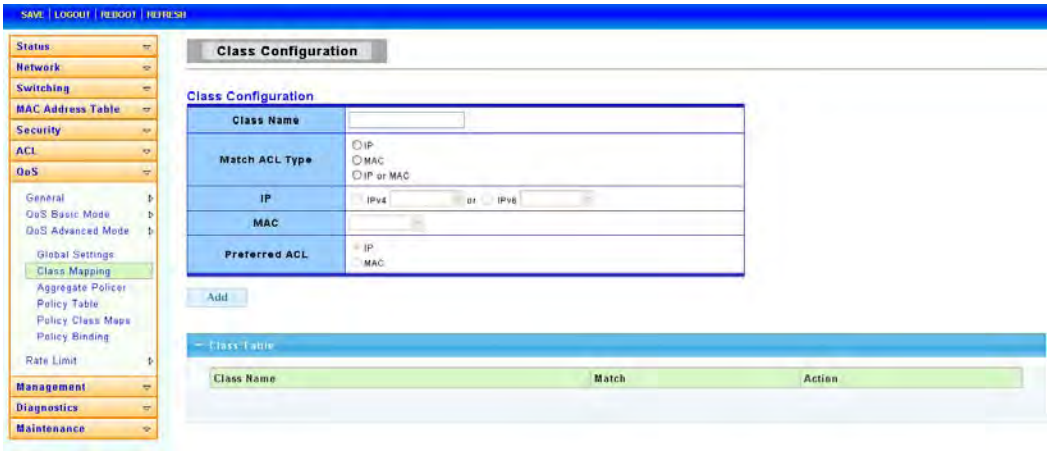
This page allow user to set the default QoS mode state under advanced mode global settings trust mode.



Class Mapping

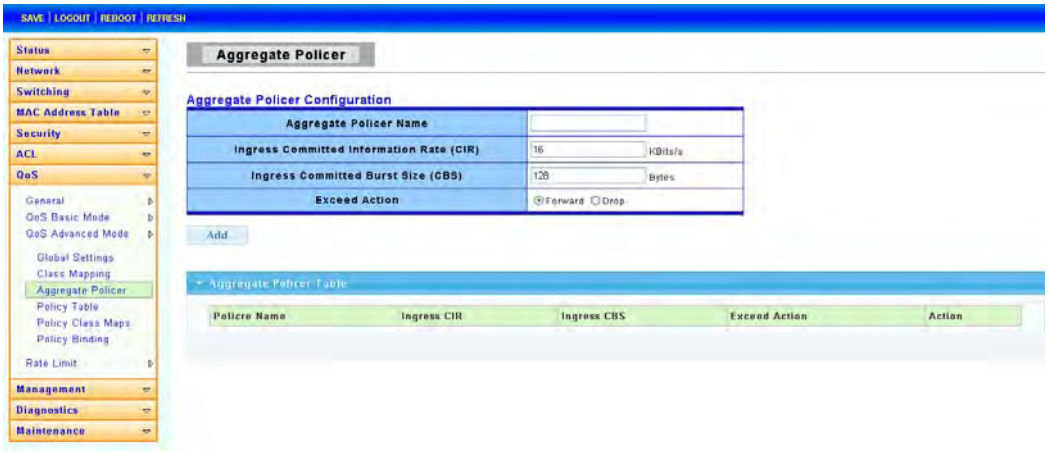
To display Class Mapping web page, click **QoS > QoS Advanced Mode > Class Mapping**

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



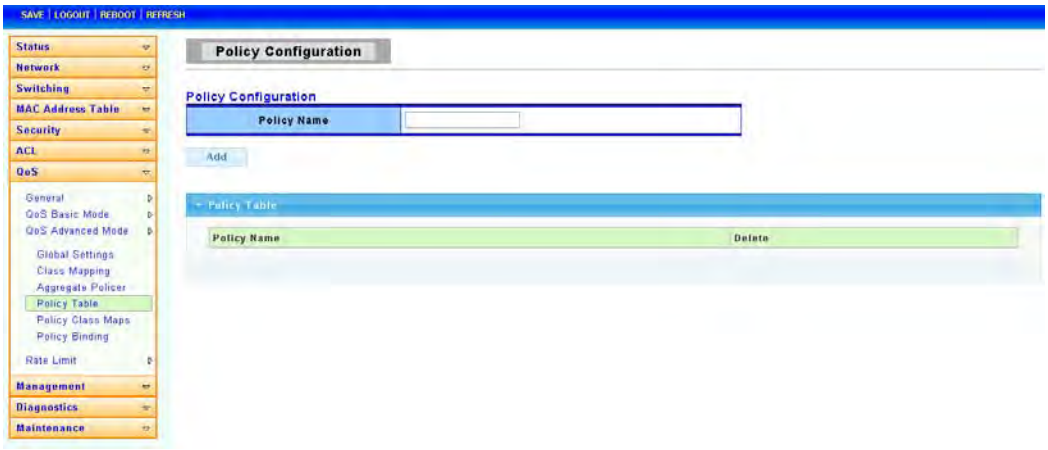
Aggregate Policer

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



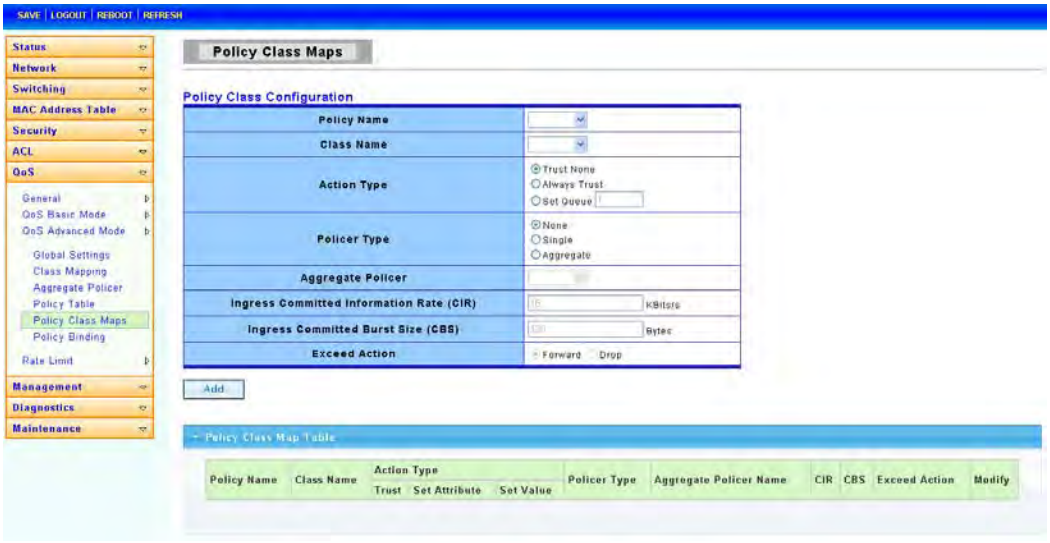
Policy Table

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



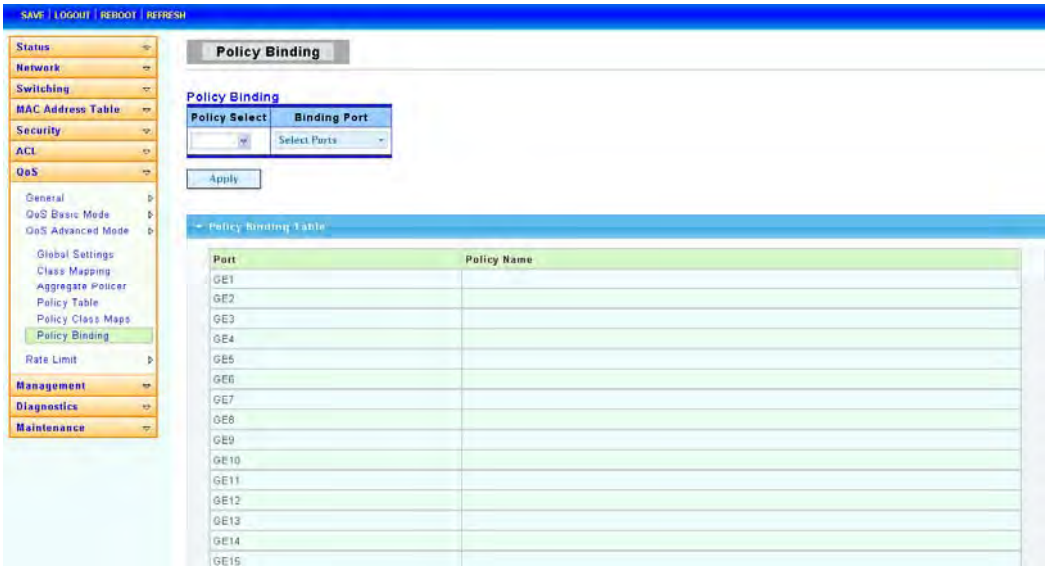
Policy Class Maps

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



Policy Binding

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

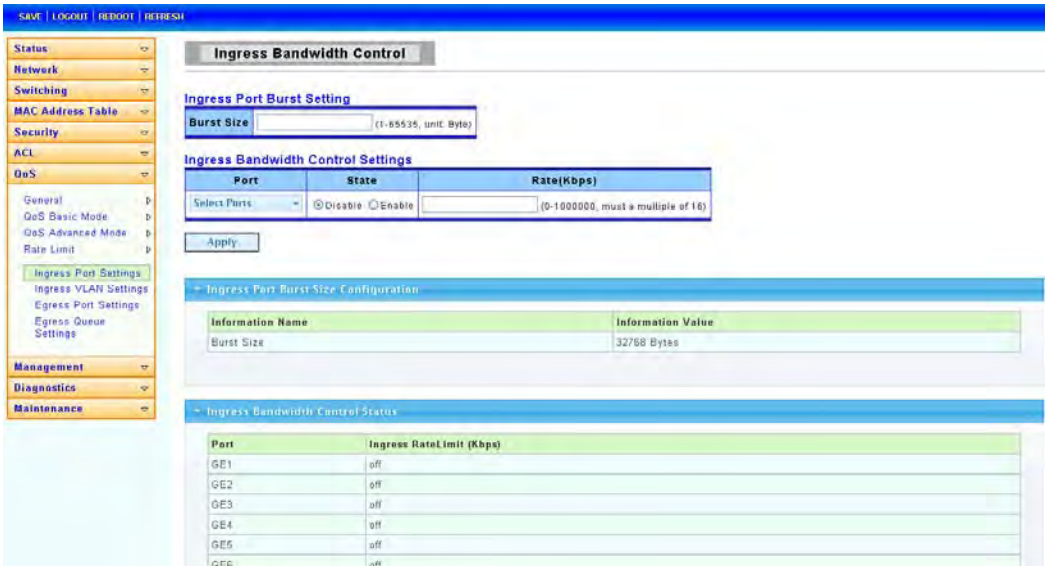


Rate Limit

Ingress Port Settings

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

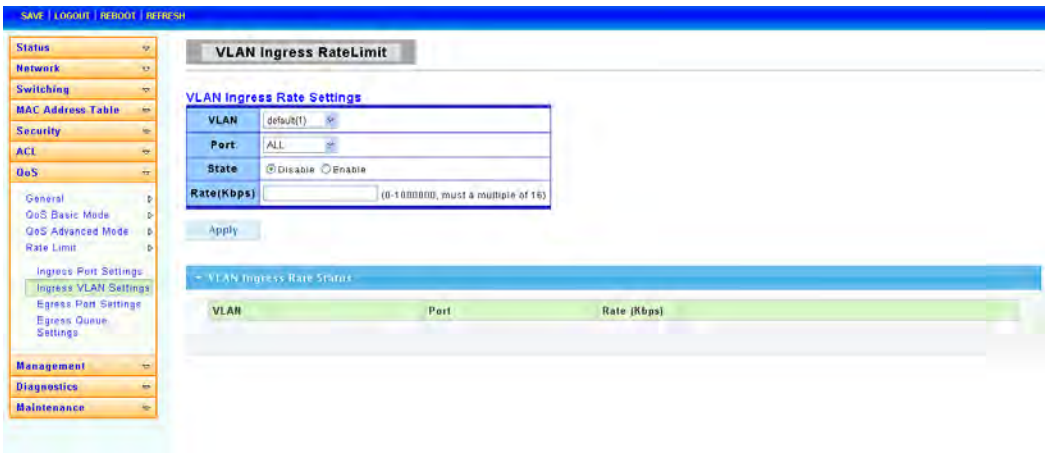
This page allow user to set ingress port monitor.



Ingress VLAN Settings

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

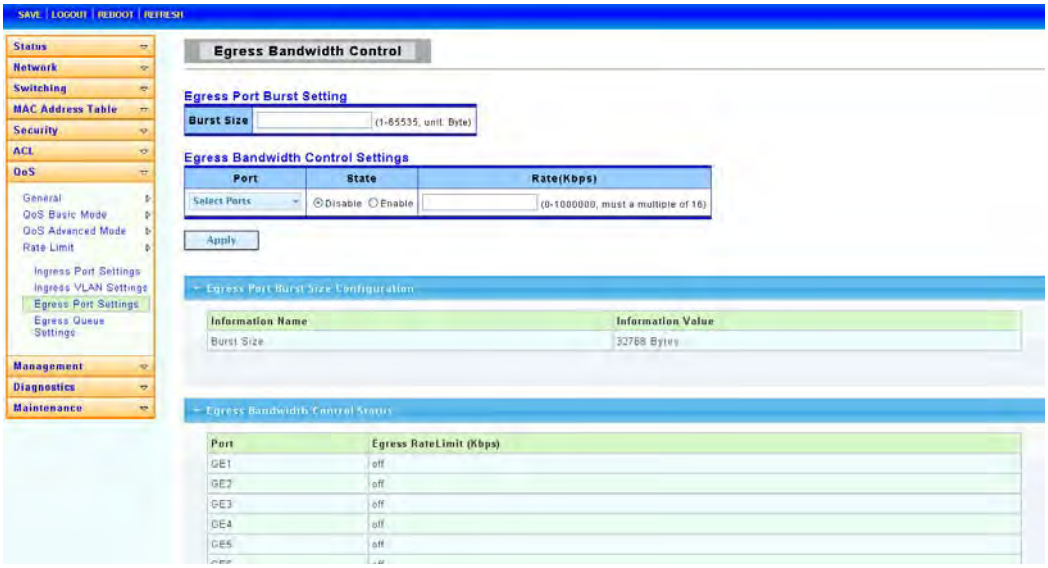
This page is used to set the bandwidth of the VLAN entry control.



Egress Port Settings

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

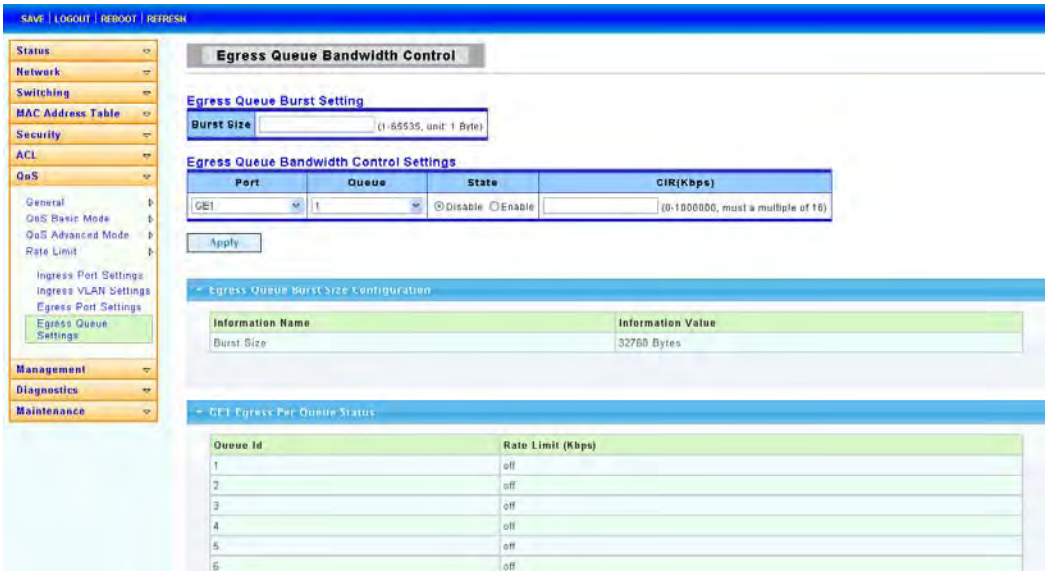
This page is used to set the egress port monitor.



Egress Queue Settings

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

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



5.8 MANAGEMENT

POE

POE Global Setting

To display POE Global Setting web page, click **Management > POE > POE Global Setting**

This page is used to check POE Status, you can set Max Available Power here.

MAX Available Power: Switch configuration can provide maximum power.

System Operation Status： display POE operation status on or off

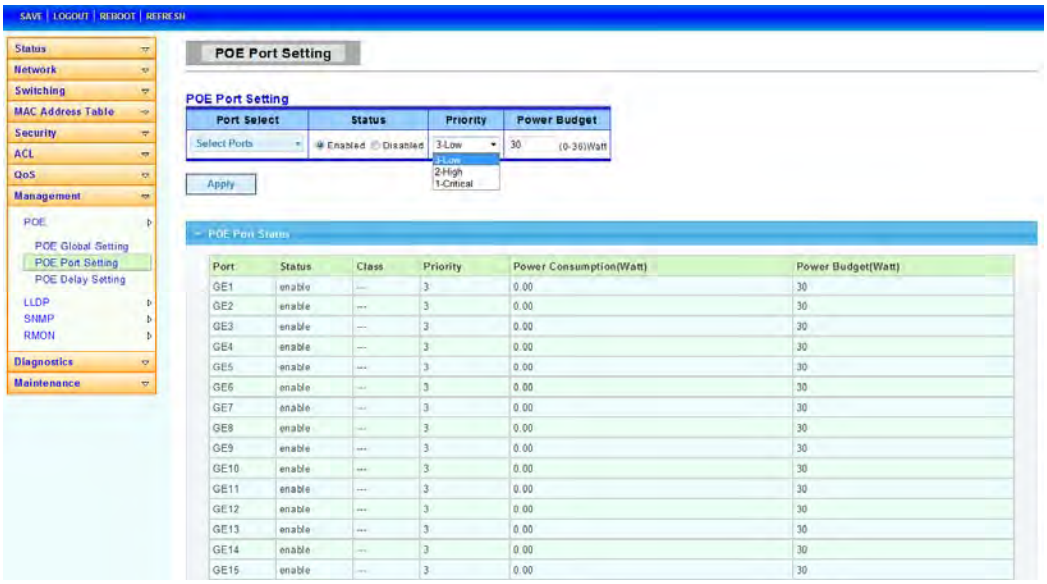
Main Power Consumption: configure main power consumption

Device Temperature: display the temperature of device.

POE Port Setting

To display POE Global Setting web page, click **Management > POE > POE Port Setting**

This page allow user to configure POE setting.



Port Select: Select specific ports.

Priority: Setting the priority of POE.

Critical

High

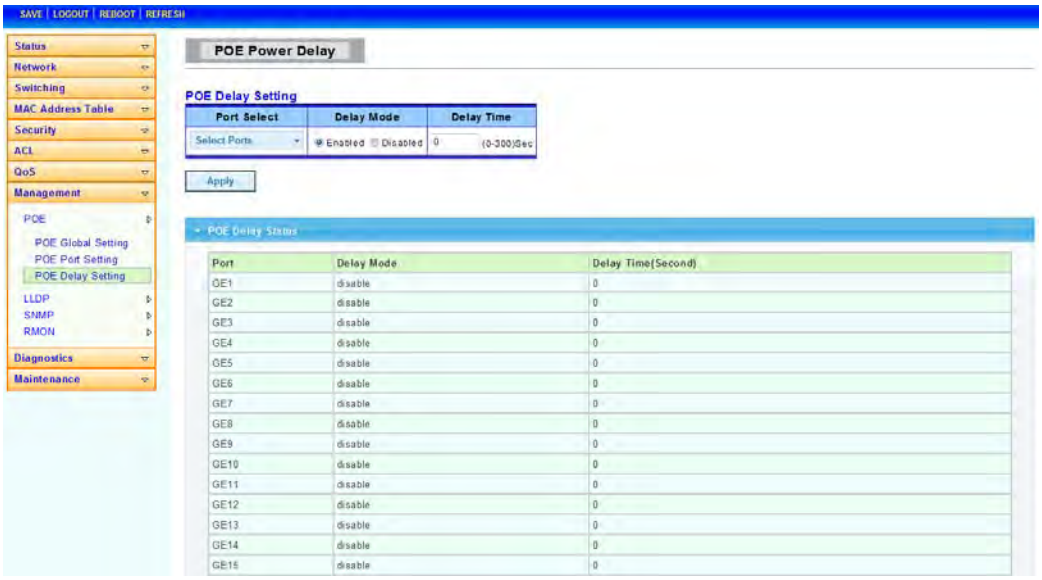
Low

Power Budget: POE port estimation can provide power.

POE Delay Setting

To display POE Global Setting web page, click **Management > POE > POE Delay Setting**

This page is for setting POE Power Delay.



Port Select: Select specific ports.

Delay Mode: enable or disable delay mode.

Delay Time: Configuration delay time.

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.

LLDP Global Settings

To display LLDP Global Settings web page, click **Management > LLDP > LLDP Global Settings**

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.

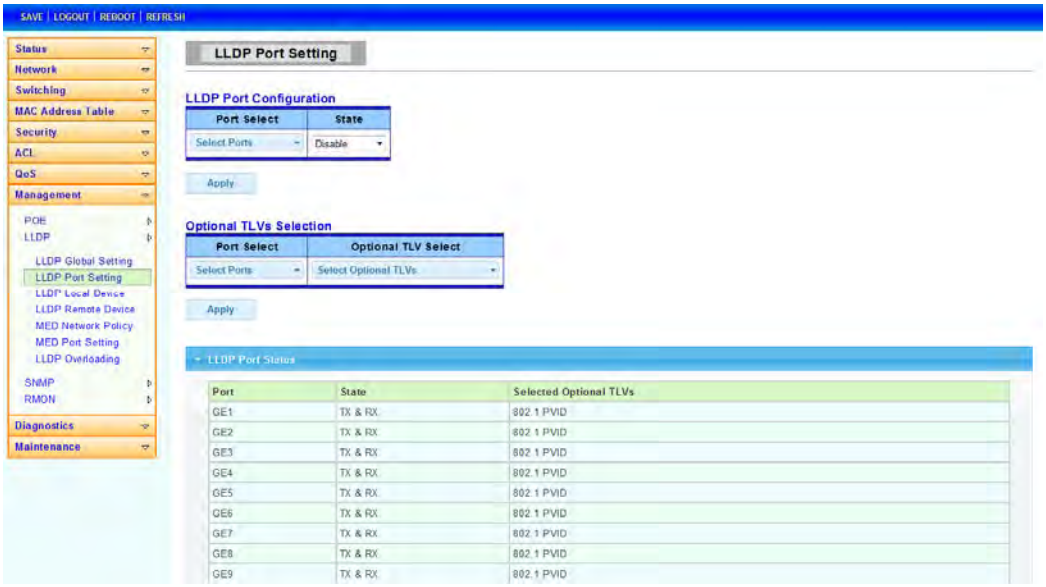
Holdtime Multiplier: Select the multiplier onthe transmit interval to assign to TTL

(range 2–10, default = 4).

Reinitialization Delay: Select the delay before a re-initialization (range 1–10 seconds, default = 2).

LLDP Port Settings

To display LLDP Port Settings web page, click **Management > LLDP > LLDP Port Settings**



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.

LLDP Local Device

To display 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.

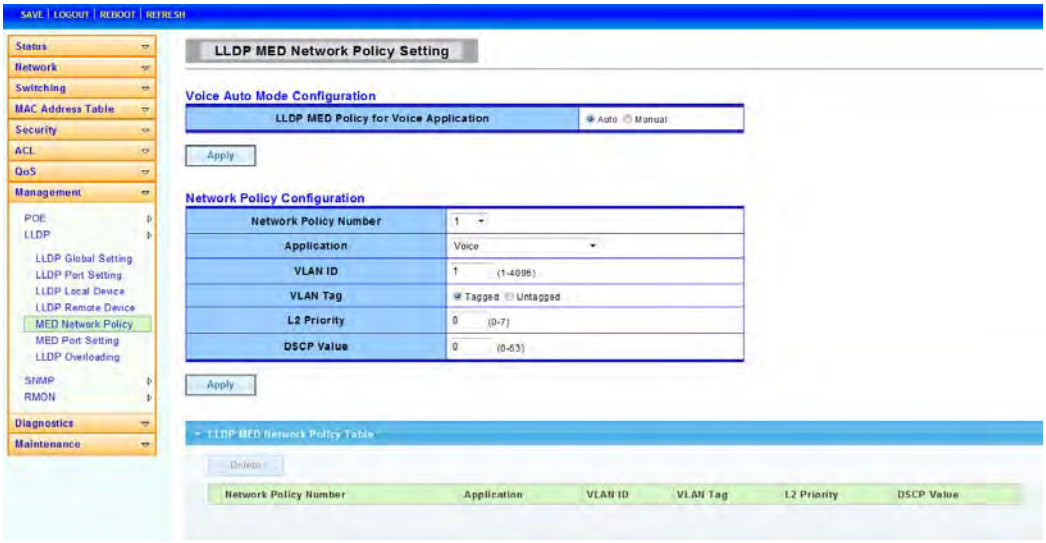
LLDP Remote Device

To display 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.

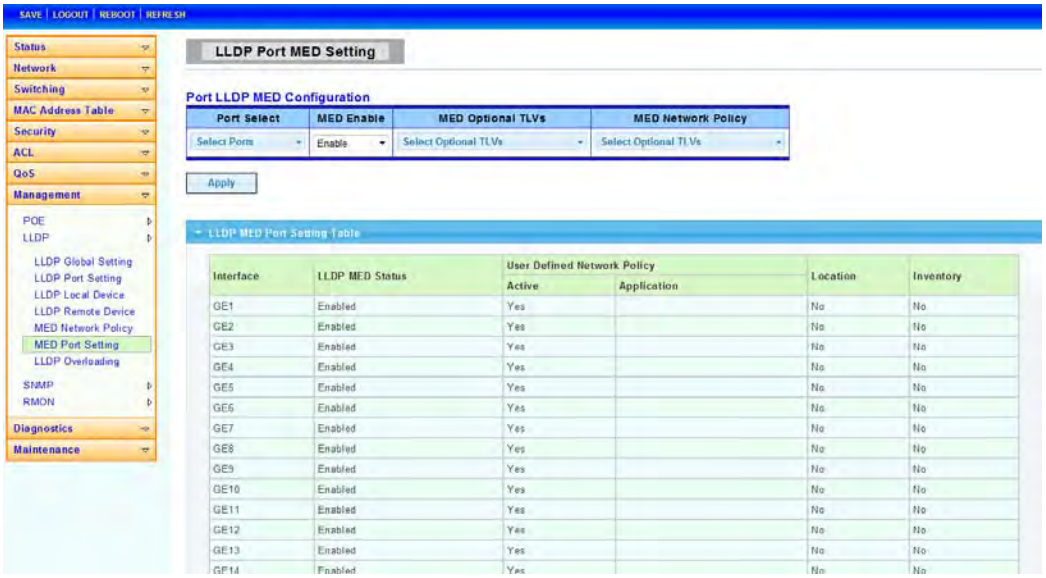
LLDP Network Policy

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



MED Port Setting

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



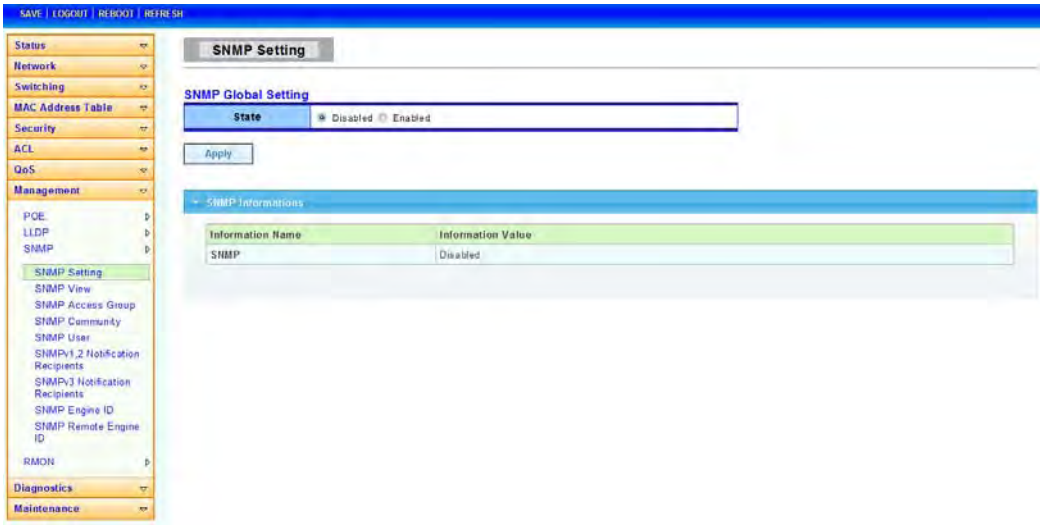
LLDP Overloading

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

SNMP

SNMP Setting

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



State: SNMP daemon state

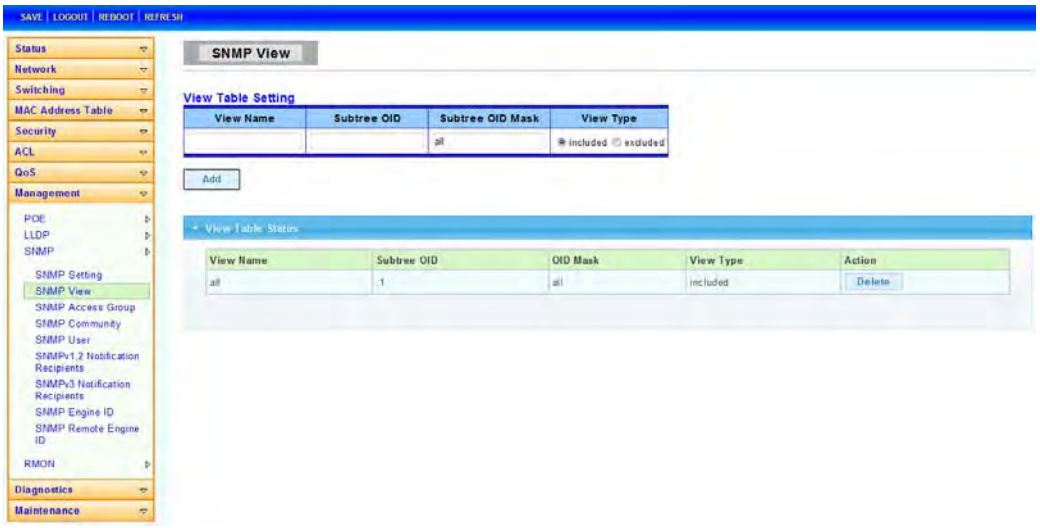
Enabled: Enable SNMP daemon

Disabled: Disable SNMP daemon

SNMP View

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

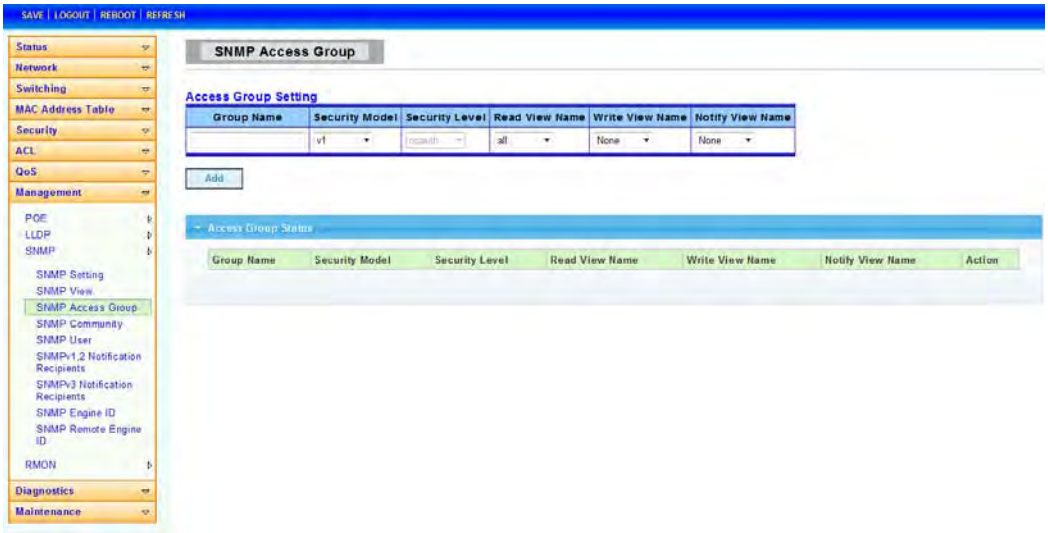
This page is used to configure SNMP view.Used in the SNMP message Management variables (OID) to describe the switch in the Management object,MIB (Management Information Base,Management Information Base) is a set of the monitoring network equipment Management variables.View is used to control variable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



SNMP Access Group

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

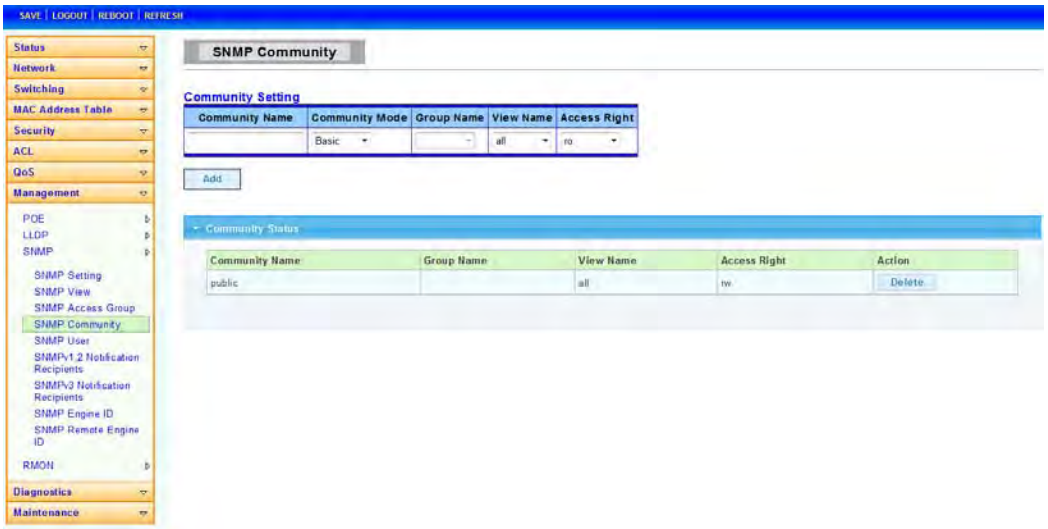
This page is used to configure SNMP group ,Within the group by the user read-only, only write, inform the view to achieve the goal of access control.



SNMP Community

To display 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.



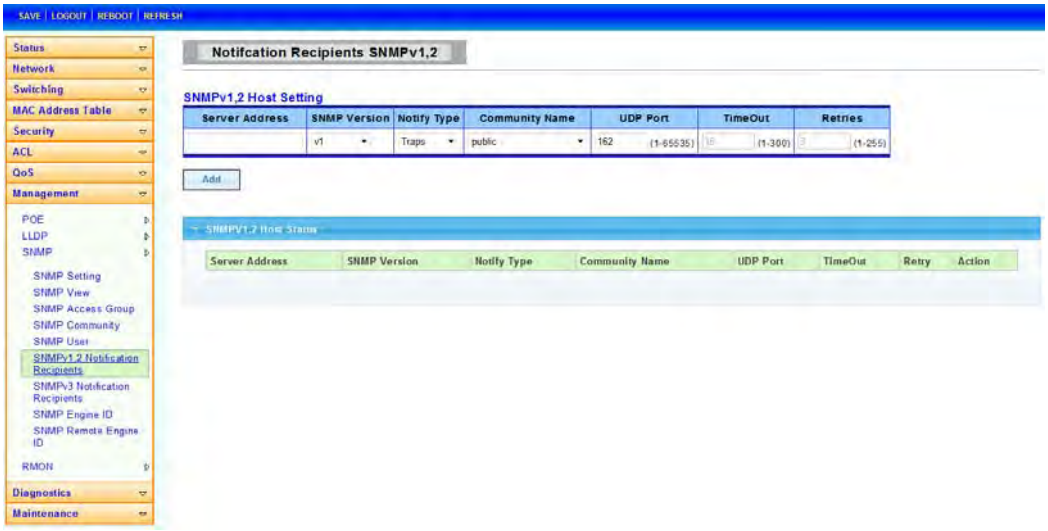
SNMP User

To display SNMP User 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.

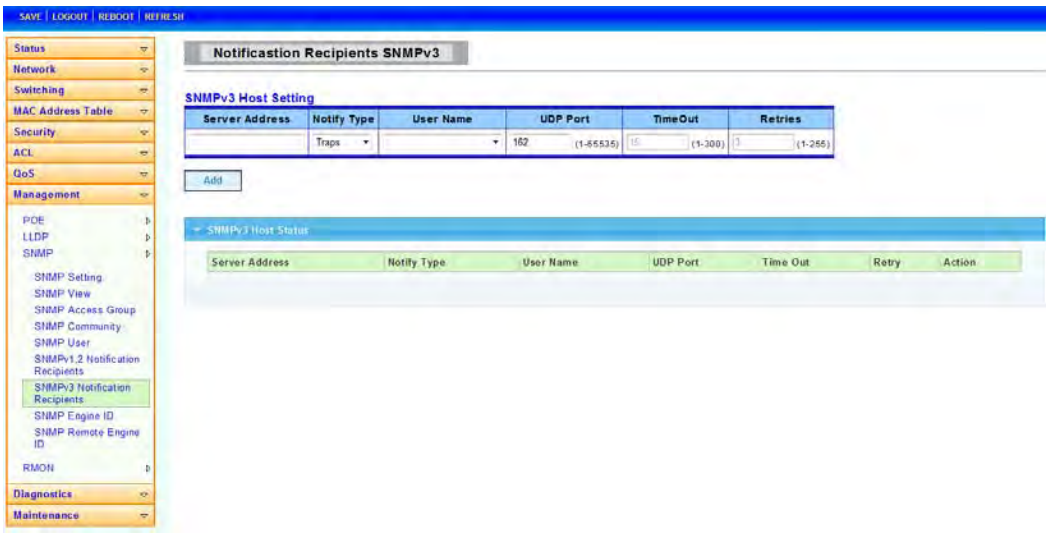
SNMPv1,2 Notifcation Recipients

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



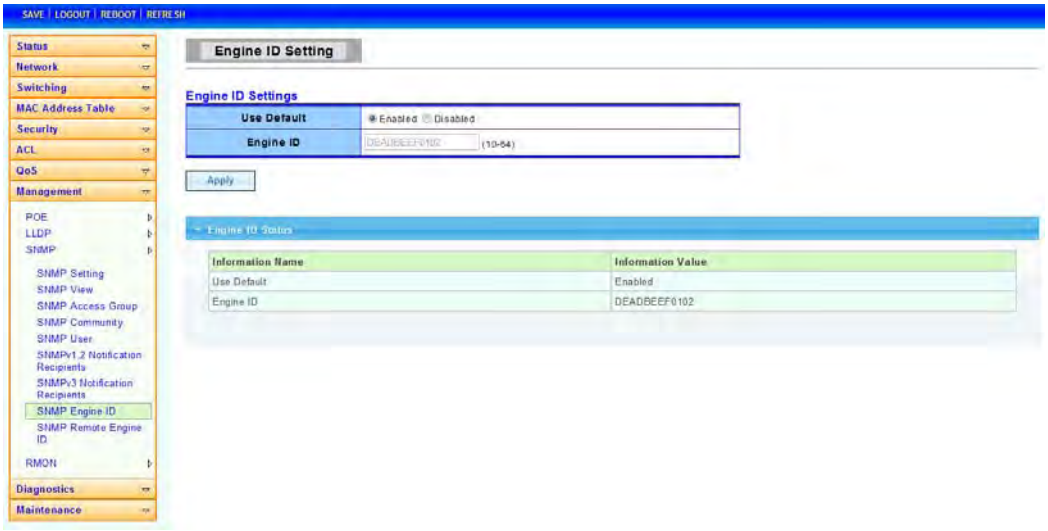
SNMPv3 Notification Recipients

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



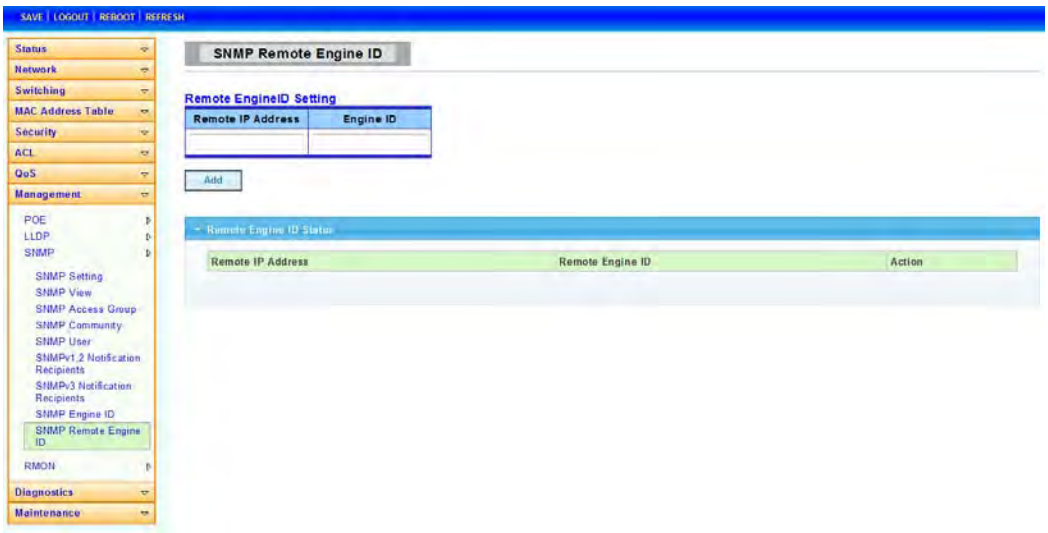
SNMP Engine ID

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



SNMP Remote Engine ID

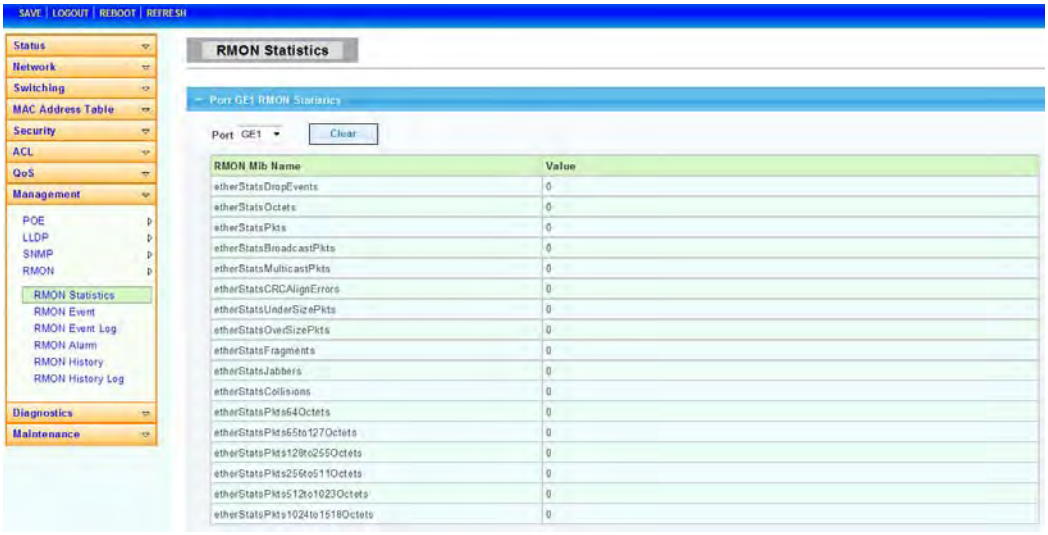
To display SNMP Remote Engine ID web page, click **Management > SNMP > SNMP Remote Engine ID**



RMON

RMON Statistics

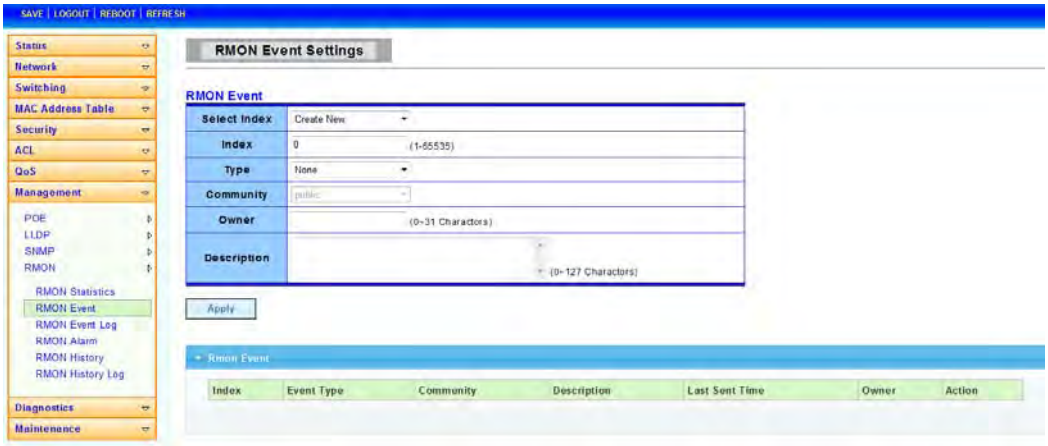
To display RMON Statistics web page, click **Management > RMON > RMON Statistics**



RMON Event

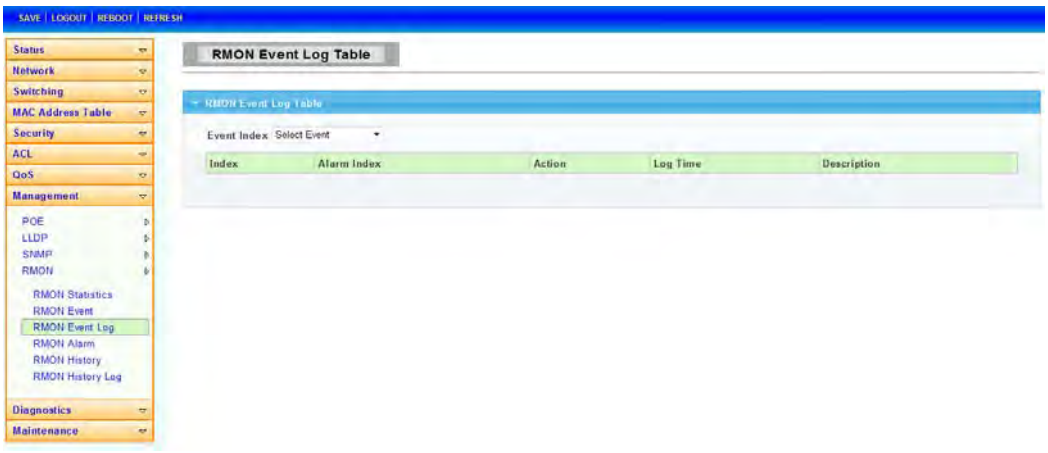
To display RMON Event web page, click **Management > RMON > RMON Event**

This page is used to configure RMON event group.



RMON Event Log

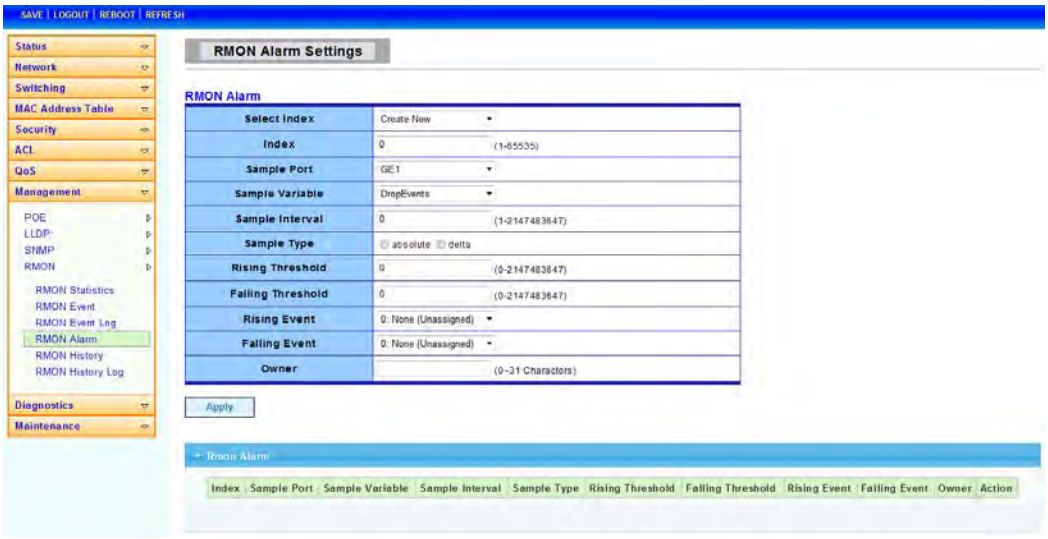
To display RMON Event Logweb page, click **Management > RMON > RMON Event Log**



RMON Alarm

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

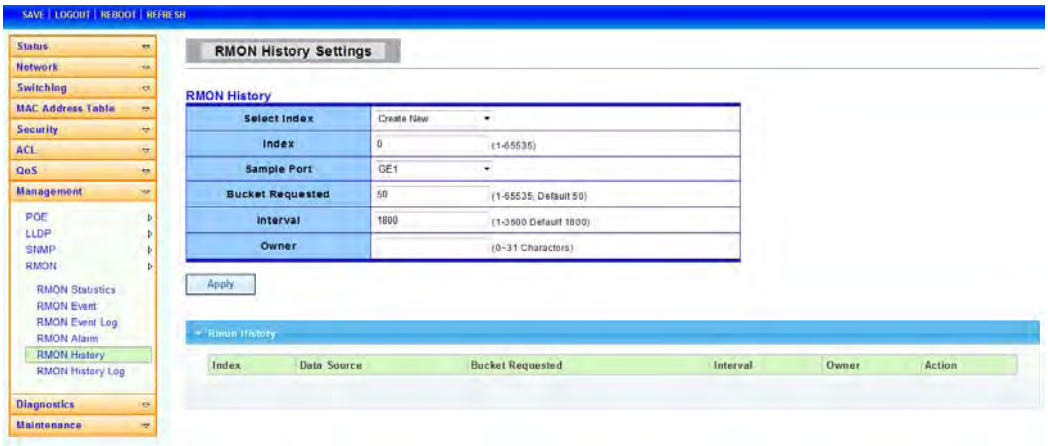
This page is used to configure RMON statistics group and alarm group.



RMON History

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

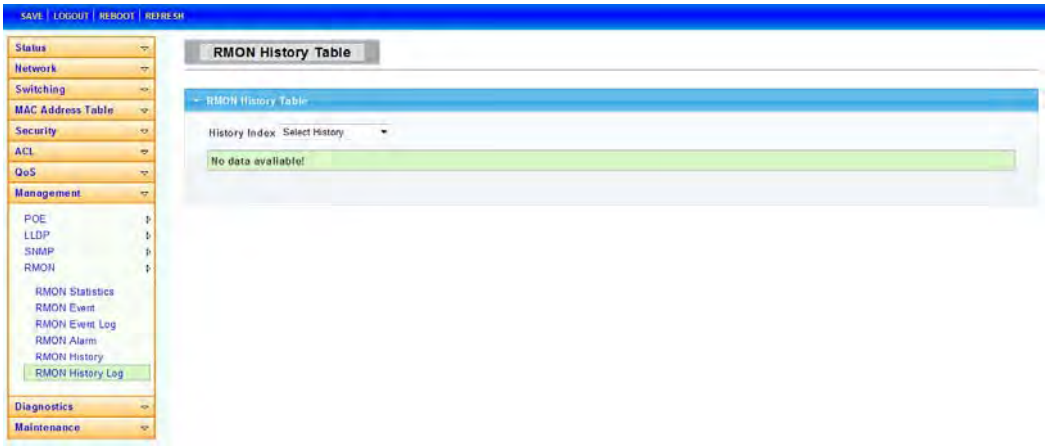
This page is used to configure the PMON history group.



RMON History Log

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

Log



5.9 DIAGNOSTICS

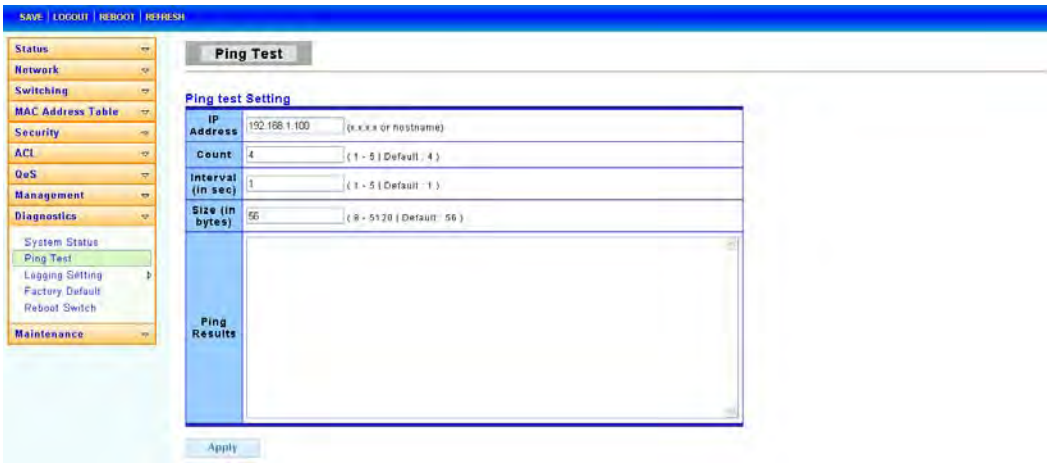
Use the Diagnostics pages to configure settings for the switch diagnostics feature or operating diagnostic utilities.

System Status

To display System Status Log web page, click **Diagnostics > System Status**

Ping Test

To display Ping Test Log 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.

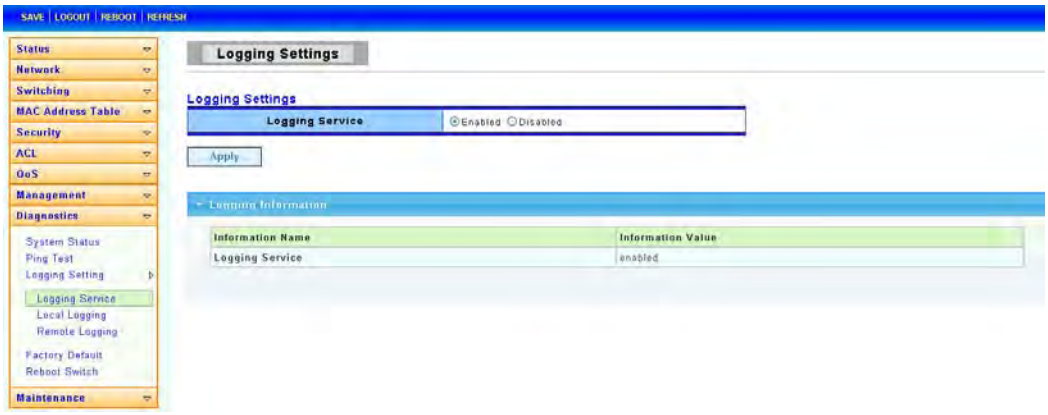
Size: The size of ping packet.

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

Logging Setting

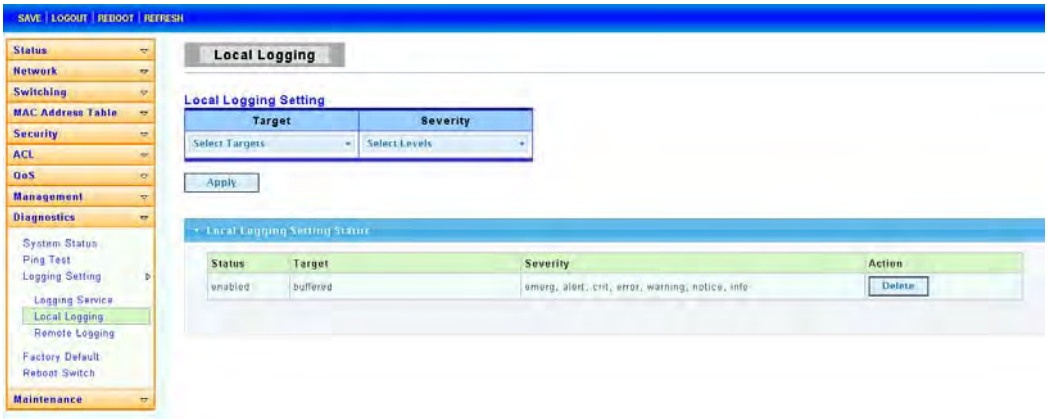
Logging Service

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



Local Logging

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



Target: Select the target to store log message

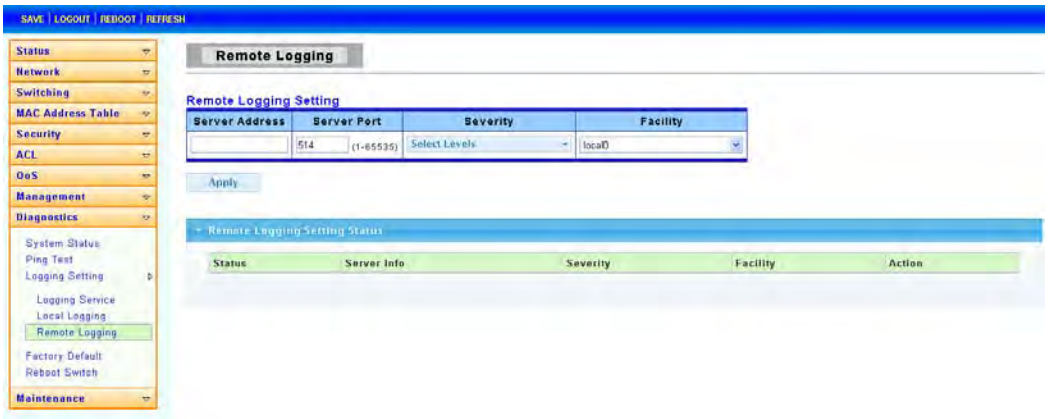
RAM: Store log messages in RAM disk. All log messages will disappear after system reboot.

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.

Remote Logging

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



Server Address: The IP address of remote log server.

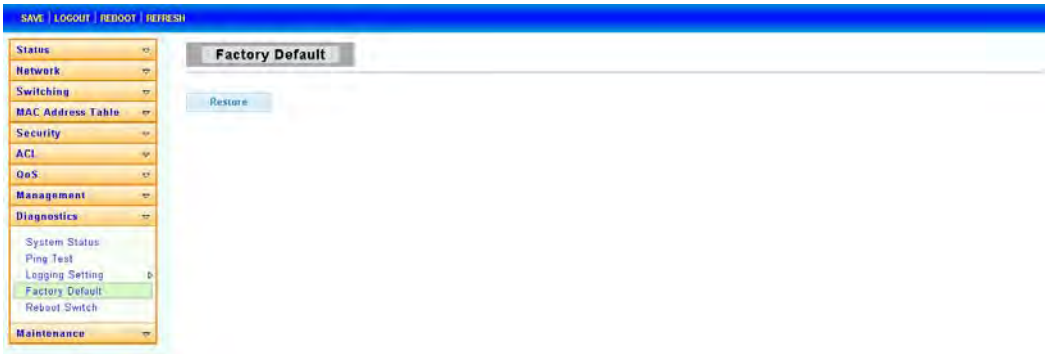
Server Port: The Port number of remote log server.

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

Factory Default

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

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



Reboot Switch

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

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

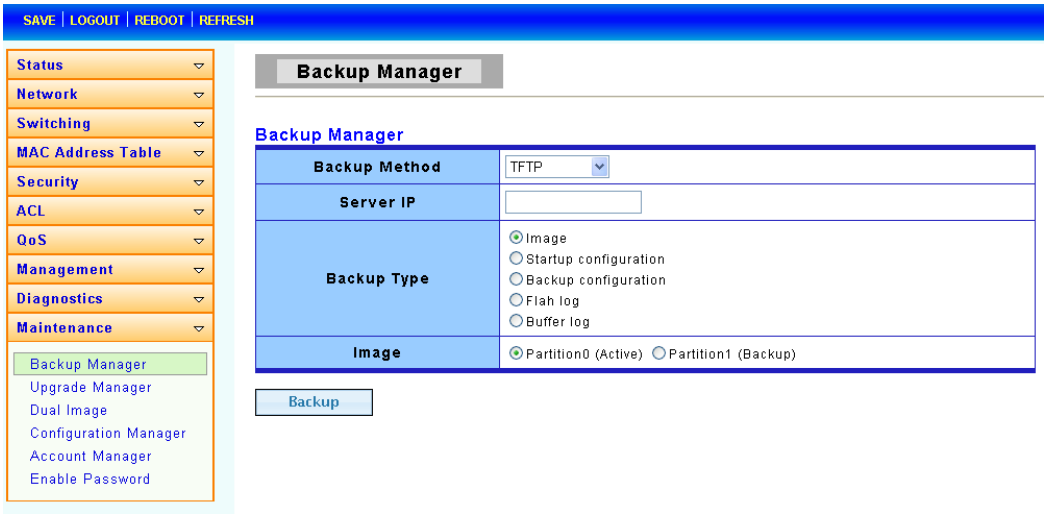
5.10 MAINTENANCE

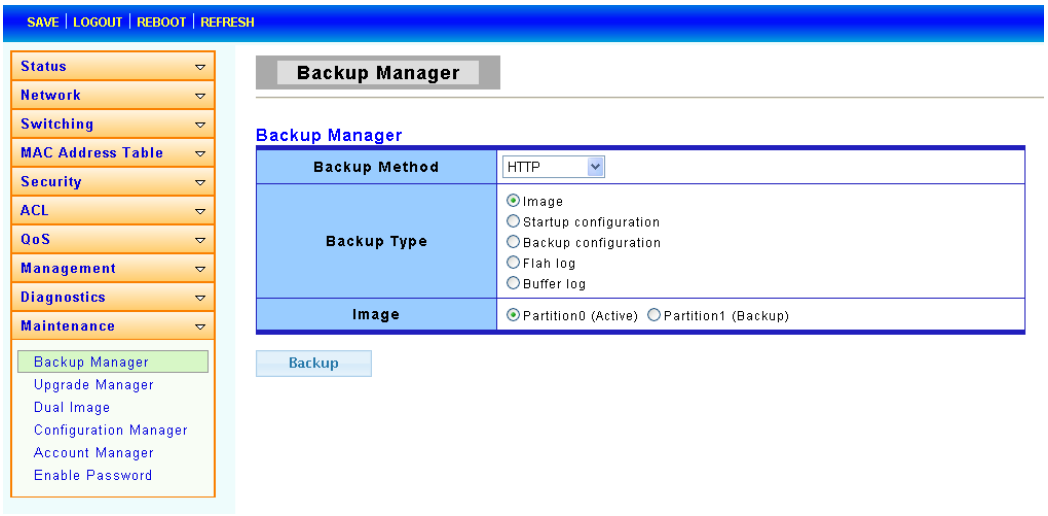
Use the Maintenance pages to configure settings for the switch network interface and how the switch connects to a remote server to get services.

Backup Manager

To display 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

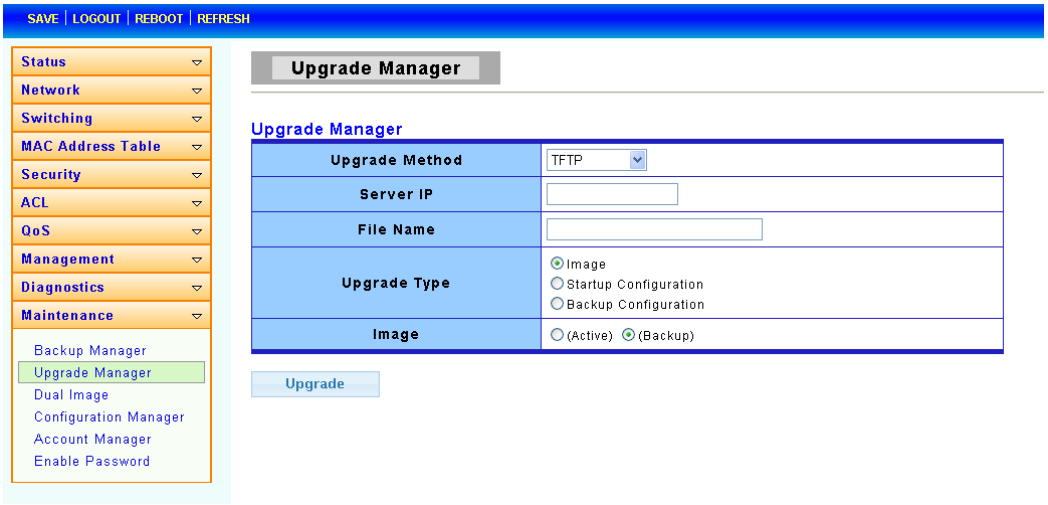
Server IP: IP address of the TFTP server. If the TFTP backup method is selected, the IP address of the TFTP server must be assigned.

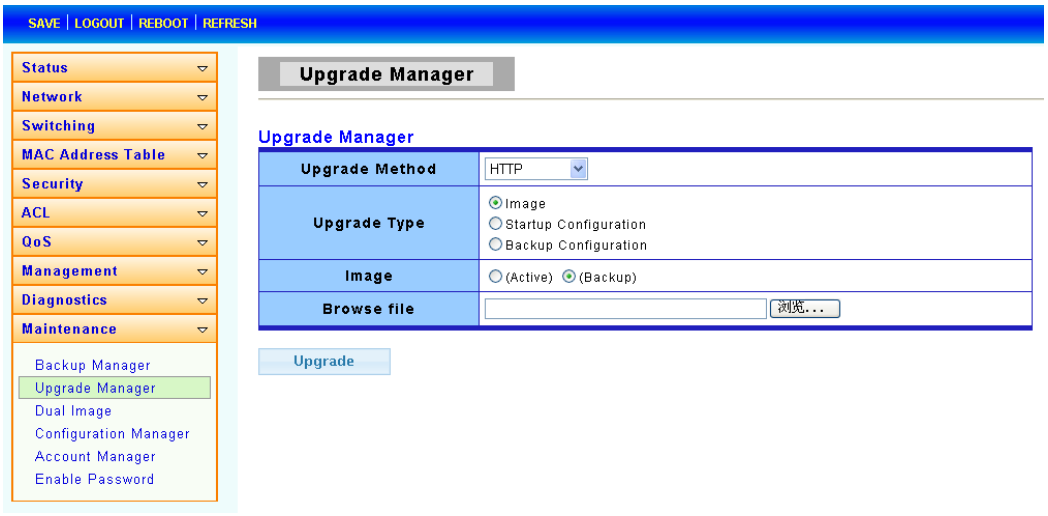
Backup Type: Select Backup Type

Upgrade Manager

To display 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.

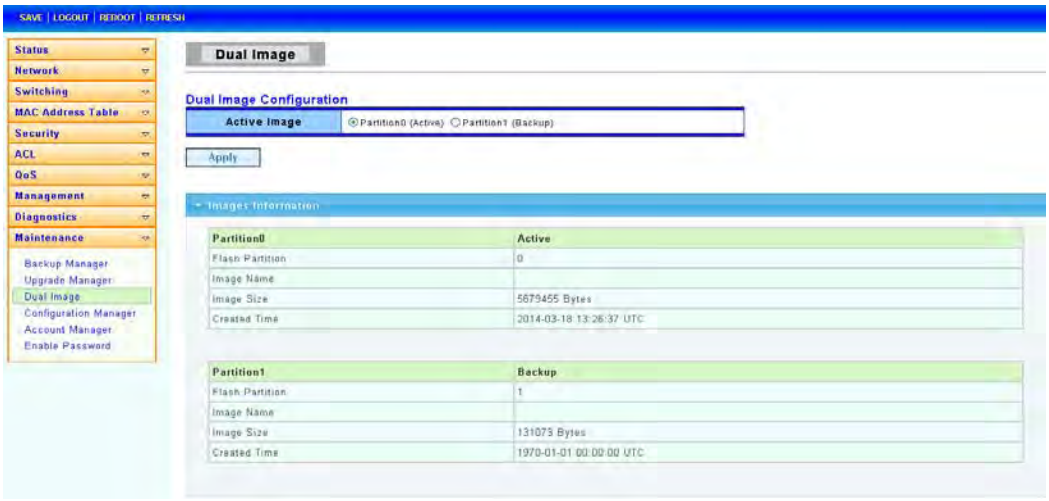
File Name: Firmware image or configuration file name on remote TFTP server. If the TFTP upgrade method is selected, the file name must be specified.

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

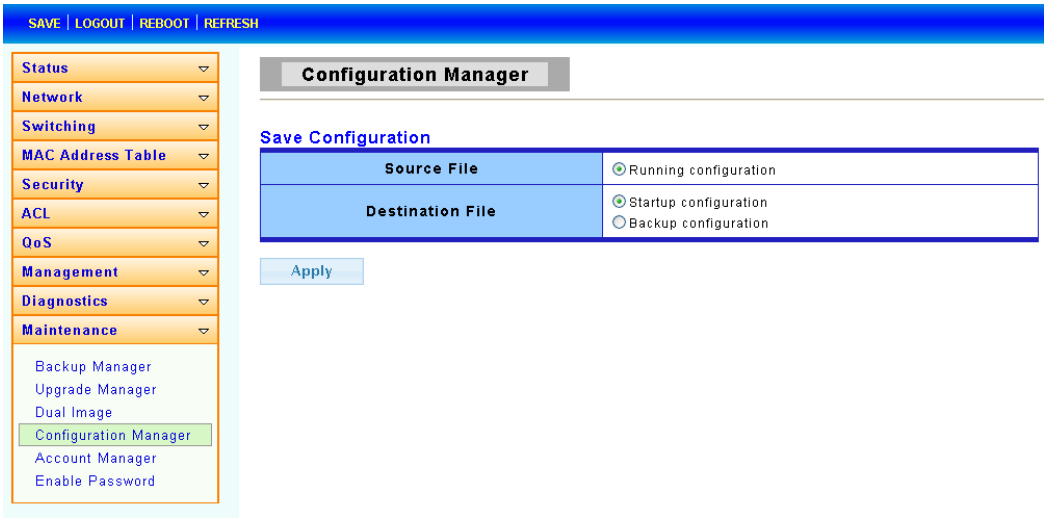
Dual Image

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



Configuration Manager

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



Account Manager

To display Account Manager 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.

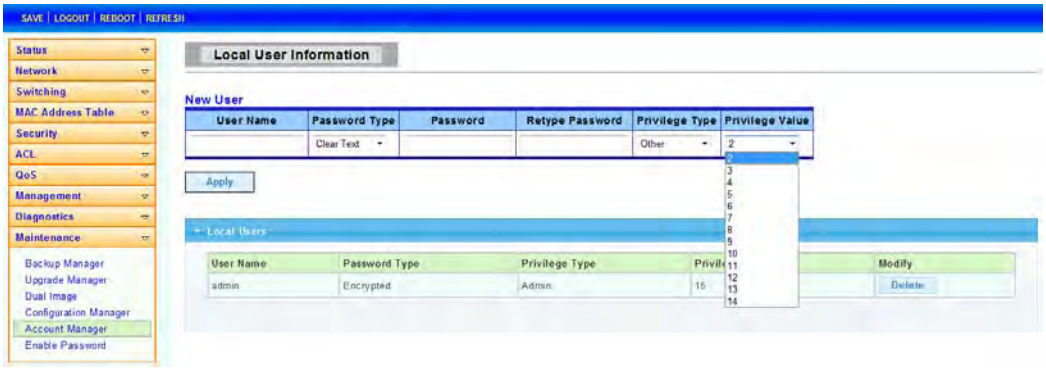
Retype Password: Retype password to make sure the password is exactly you typed before in “Password” field.

Privilege Type: Select privilege level for new account.

Admin: Allow to change switch settings.

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

If AAA feature is enabled, we have one more privilege type to allow user adding privilege value for this account.



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.

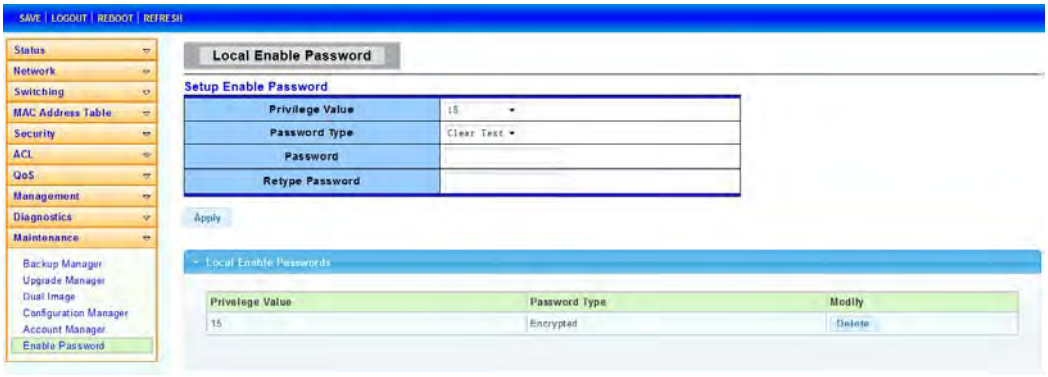
Other: Assign privilege level value in Privilege value field.

Privilege Value: If the account privilege type is “Other”, set the privilege level for this account here. The valid privilege level is from 2 to 14.

Enable Password

To display 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.