EnGenius®

Business Solutions

User Manual

EGS5212FP | EGS7228P | EGS7228FP | EGS7252FP

version 1.0

Layer 2 Managed PoE+ Switch

Neutron Series

IMPORTANT

To install your Switch please refer to the
Quick Installation Guide included in the product packaging.

Table of Contents

Chapter 1

Product Overview

Introduction

The EnGenius EGS series Layer 2 Switch is a device specially designed to support Access Points and IP Surveillance cameras, VOIP phones, and other PoE-Capable devices as well as other Ethernet-based networking equipment or computers.The EGS Switch provides simple, yet powerful PoE manageability with features such as: IEEE 802.3af or IEEE 802.3at/af ports, PoE port management, loopback detection, and IGMP snooping.

Package Contents

Your EGS Layer 2 Switch package will contain the following items:*

- EnGenius Switch
- Quick Installation Guide
- Power Adapter
- Wall Mount Kit
- Ground Screw Kit
- Power Cord
- Rack Mount Kit

*(all items must be in package to issue a refund):

Technical Specifications

Standard:

	EGS5212FP	EGS7928P	EGS7928FP	EGS7252FP
Ports	8	24	24	48
Power budget	Ports 1 - 8, 30 Watts per Port	Ports 1 - 24, 30 Watts per Port	Ports 1 - 24, 30 Watts per Port	Ports 1 - 48, 30 Watts per 24 Ports
Total PoE Budget	130 W	185 W	370 W	740 W
SFP Slots	2	4	4	4
Switching Capacity:	24 Gbps	56 Gbps	56 Gbps	104 Gbps
Forwarding Mode:	Store and Forward			
Flash Memory:	32 MB	32 MB	32 MB	32 MB
SD RAM:	256 MB	256 MB	256 MB	256 MB

Port Functions:

8, 24, or 48 10/100/1000Mbps Ports in the front panel (Depending on model)

2 or 4 100/1000Mbps SFP Ports (Depending on model)

1 RJ 45 Port

PoE Capability:

PoE Standard: Port 1~8, 24, or 48 Support IEEE 802.3at/af

PoE Capable Ports:

Port 1~8, 24, 48 can output up to 30 Watts

LED Indicator

Device:

Power LED x1

Fault LED x1

PoE Max LED x1

LAN Mode LED x1

PoE Mode LED x1

Copper Ports:

LAN/PoE Mode LED x 1

Link/Act LED x 1

SFP Ports:

Link/Act LED x 1

Environment & Mechanical:

Temperature Range

Operating: 32 to 104°F/0 to 40°C

Storage: -40 to 158°F/-40 to 70 °C

Humidity (non-condensing): 5% - 95%

L2 Features:

802.3ad compatible Link Aggregation

802.1D Spanning Tree (STP)

802.1w Rapid Spanning Tree (RSTP)

802.1s Multiple Spanning Tree (MSTP)

IGMP Snooping v1/v2/v3

MLD Snooping

IGMP Fast Leave

Port Trunking

Port Mirroring: One to one and many to one

VLAN Group

Voice VLAN

Queue

CoS based on 802.1p priority

CoS based on physical port

CoS based on TOS

CoS based on DSCP

BootP/DHCP Client

Firmware Burn-Proof

802.1X Port-based Access Control

802.1X Guest VLAN

Port Security

Port Isolation

Storm Control

Attack Prevention

Access Control List (ACL)

Telnet Server

TFTP Client

BootP/DHCP Client

L2 Features Continued:

Web-based support
SNMP v1 support
SNMP v2c support
SNMP v3 support
TFTP upgrade
Command Line Interface (CLI)
SNTP
RMONv1
SYSLOG
Cable Diagnostics
MIB Support
RFC1213
RFC1493
RFC1757
RFC2674

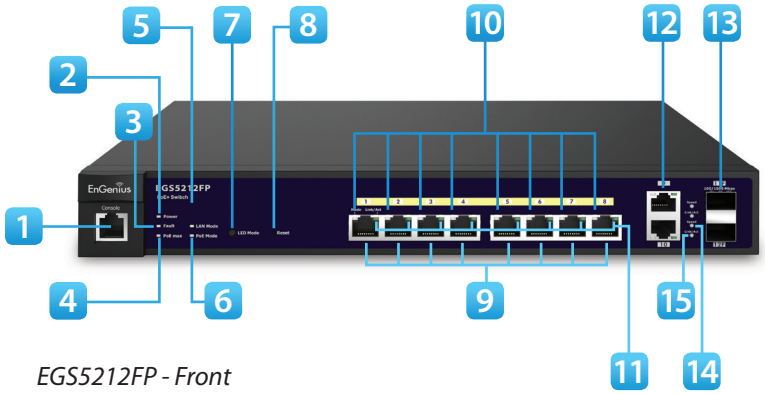
PoE Management
Power on/off per port
Power Class Configuration
Power feeding with priority
User-defined power limit

Physical Interface

Dimensions

EGS5212FP

Width: 13” Length: 9” Height: 1.73”



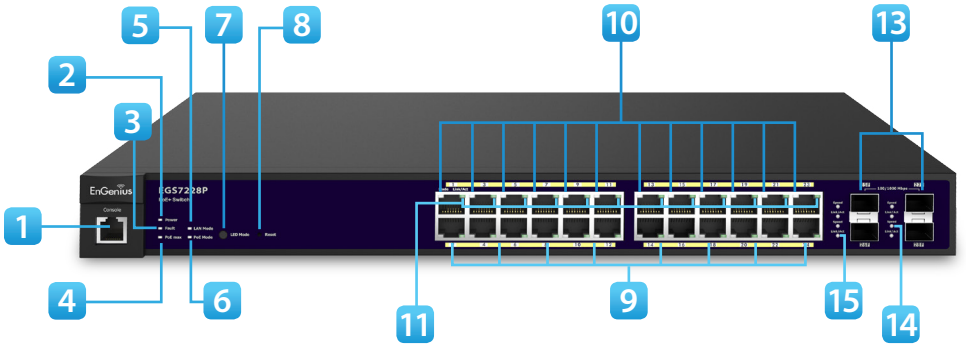
EGS5212FP - Front

EGS5212FP - Back

Dimensions

EGS7228P & EGS7228FP

Width: 9.45” Length: 4.13” Height: 1.06”



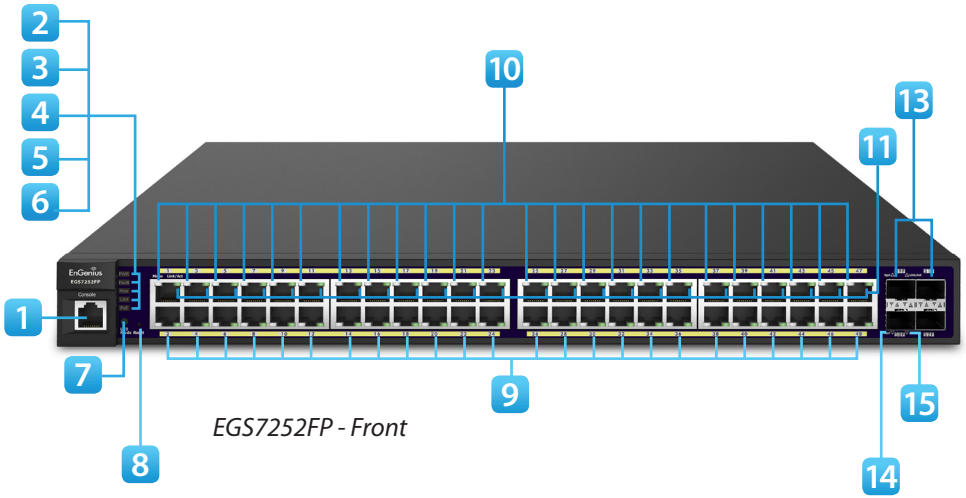
EGS7228P - Front

EGS7228P - Back

Dimensions

EGS7252FP

Width: 17.3” Length: 16.1” Height: 1.7”



EGS7252FP - Front

EGS7252FP -Back

1 **RJ45 Console Port**

2 **Power LED:** Light off = Power off; Solid Light = Power On.

3 **Fault LED:** Light off = Normal Behavior; Solid Light = Error.

4 **PoE Max LED:** Light off = Additional PoE device may still be added; Solid Light = The PoE device’s output power has exceeded total PoE limit. No additional devices can be powered on via PoE.

5 **LAN Mode LED:** Light off = LAN mode is not activated; Solid Light = LAN mode is activated.

6 **PoE Mode LED:** Light off = PoE mode is not activated; Solid Light = PoE mode is activated.

7 **LED Mode Selector:** Press to change between LAN and PoE mode.

8 **Reset Button:** Press to reset the device to factory default settings.

9 **RJ-45 LAN Ports:** 10/100/1000 Mbps RJ-45 LAN ports.

10 **LAN Mode LED (Per Copper Port):** Light off = No link is established on the port; Solid Amber Light = A valid 10/100 Mpbs link is established on the port; Solid Green Light = A valid 1000 Mbps link is established on the port.

11 **Link/Act LED (Per Copper Port):** Light off = No link is established on the port; Solid Light = A valid link is established on the port; Blinking Light = Packet transmission on the port.

12 **Uplink Ports:** Gigabit Ports

13 **SFP Ports:** Small form factor pluggable ports.

14 **Speed LED (Per SFP Port)**

15 **Link/Act LED (Per SFP Port):** Light off = No link is established on the port; Solid Amber Light: A valid 100 Mpbs link is established on the port; Solid Green Light: A valid 1000 Mbps link is established on the port.

16 **Power Connector**

Management Interface

The EGS Layer 2 PoE+ Switch features an embedded Web interface for the monitoring and management of your device.

Connecting the Switch to a Network

Discovery in a Network with a DHCP Server

Use this procedure to setup the Switch within a network that uses DHCP.

1. Connect the supplied Power Adapter (cord) to the Switch and plug the other end into an electrical outlet. Turn the power switch on the back of the device to the **ON** position. Verify the power LED indicator is lit on the Switch.

2. Wait for the Switch to complete booting up. It might take a minute for the Switch to completly boot up.

3. Connect one end of a Category 5/6 Ethernet cable into the Gigabit (10/100/1000) Ethernet port on the Switch front panel and the other end to the Ethernet port on the computer. Verify that the LED on the Ethernet ports of the Switch are **green**.

4. Once your computer is on, ensure that your TCP/IP is set to **On** or **Enabled**. Open **Network Connections** and then click **Local Area Connecton**. Select **Internet Protocol Version 4 (TCP/IPv4)**. If your computer is already on a network, ensure that you have set it to a Static IP Address on the Interface (Example: 192.168.0.10 and the Subnet mask address as 255.255.255.0).

5. Open a web browser on your computer. In the address bar of the web browser, enter **192.168.0.239** and click **Enter**.

6. A login screen will appear. By default, the username is **admin** and the password is **password**. Enter the current password of the Switch and then click **Login**.

7. Once logged in, click **IP Settings** under the System tab and select IPv4 or IPv6. Next,

8. Click **DHCP** under Auto-Configuration.

9. Click **Apply** to save the settings.

10. Connect the Switch to your network (DHCP enabled).

11. On the DHCP server, find and write down the IP address allocated to the device. Use this IP address to access the management interface.

IP Address: _____

Discovery on a Network without a DHCP Server

This section describes how to set up the EGS Layer 2 Switch in a network without a DHCP server. If your network has no DHCP service, you must assign a static IP address to your Switch in order to log in to the web-based Switch management.

1. Connect the supplied Power Adapter (cord) to the Switch and plug the other end into an electrical outlet. Turn the Power Switch on the back of the device to the **ON** Position. Verify the Power LED indicator is lit on the Switch.
2. Wait for the Switch to complete booting up. It might take a minute or so for the Switch to completely boot up.
3. Connect one end of a Category 5/6 Ethernet cable into the Gigabit (10/100/1000) Ethernet port on the Switch front panel and the other end to Ethernet port on the computer. Verify that the LED on Ethernet ports of the Switch are green.
4. Once your computer is on, ensure that your TCP/IP is set to **On** or **Enabled**. Open **Network Connections** and then click **Local Area Connecton**. Select **Internet Protocol Version 4 (TCP/IPv4)**.
5. If your computer is already on a network, ensure that you have set it to a Static IP Address on the Interface (Example: 192.168.0.10 and the Subnet mask address as 255.255.255.0).
6. Open a web browser on your computer. In the address bar of the web browser, enter **192.168.0.239** and click **Enter.**
7. A login screen will appear. By default, the password is **password**. Enter the current password of the Switch and then click **Login**.

   To make access to the web-based management interface more secure, it's highly reccomended that you change the password to something more unique.
8. Once logged in, click **IP Settings** under the **System** menu and select **Static IP** to configure the IP settings of the management interface.
9. Enter the IP address, Subnet mask, and Gateway.
10. Click **Apply** to update the system.

Web Access

Use this procedure to access the management interface through a Web browser for device configuration.

1. Open a Web browser on your computer and enter the following address (default): **http://192.168.0.239**.

2. On the login screen, use the following information: Password: **password**

To make access to the web-based management interface more secure, it's highly reccomended that you change the password to something more unique.

Chapter 2
Management

System

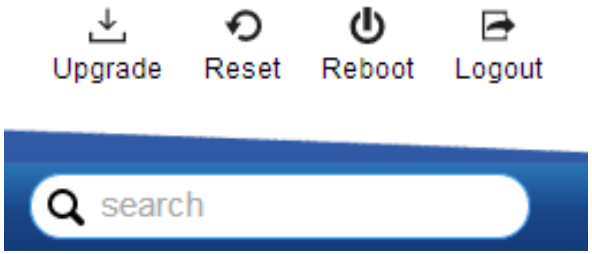
The navigation pane at the left of the Web browser interface contains a System tab that enables you to manage your EGS Layer 2 Switch with features under the following main menu options:

- "System"
- "L2 Features"
- "VLAN"
- "Management"
- "ACL"
- "QoS"
- "Security"
- "Monitoring"
- "Diagnostics"

The description that follows in this chapter describes configuring and managing the system settings within the Switch.

Search Bar

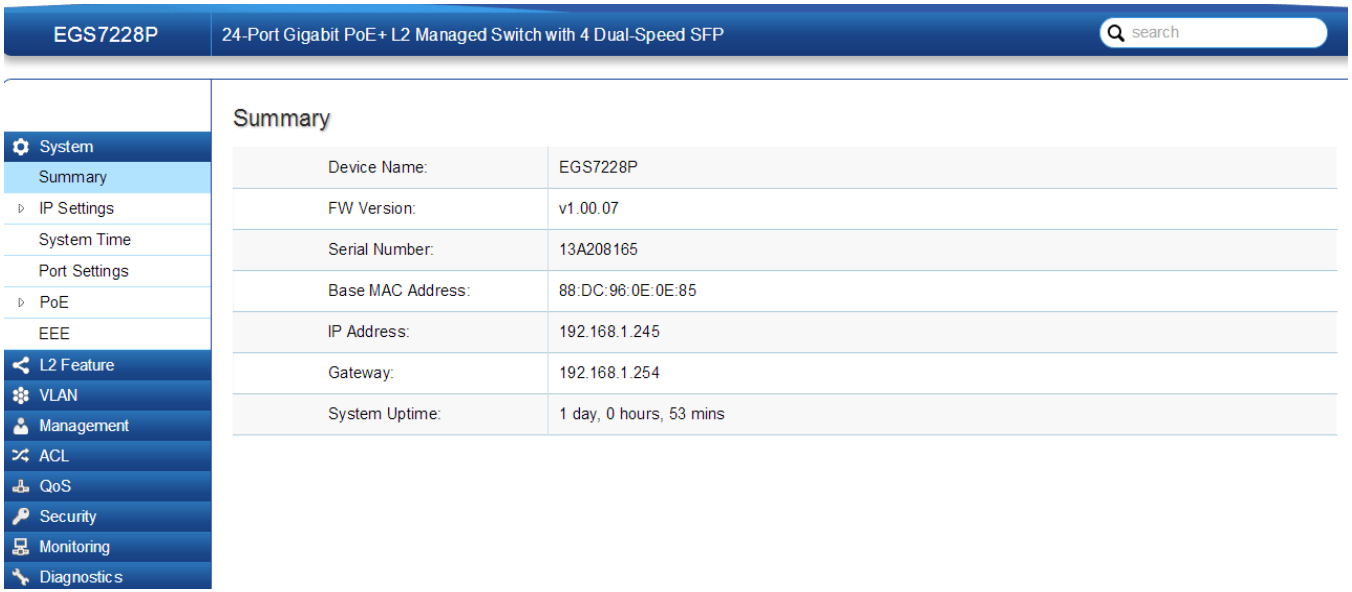
At the top right corner of the Graphical User Interface (GUI) is the search bar which you can use to find and jump to any of the L2 management features. When you type in a word, all possible results for that word in the navigation pane will appear. Click on the results from the drop down list to open that management tab.



Summary

The Summary screen contains general device information about the Switch, including the device name, Firmware version, MAC address, IP address, Gateway, and System Uptime.

Device Name:	Displays the model name of the Switch
FW version:	Displays the installed firmware version of the Switch.
Serial Number:	Displays the serial number of the Switch.
Base MAC address:	Displays the MAC address of the device.
IP Address:	Displays the IP address assigned by DHCP server.
Gateway:	Displays the Gateway of IP interface.
System Uptime:	Displays the amount of time since the most recent device reset. The System Time is displayed in the following format: days, hours, and minutes. For example, the display will read: 3 days, 6 hours, 10 minutes.



IP Settings

The IP Setting screen contains fields for assigning IP addresses. IP addresses are either defined as static or are retrieved using the Dynamic Host Configuration Protocol (DHCP). DHCP assigns dynamic IP addresses to devices on a network. DHCP ensures that network devices can have a different IP address every time the device connects to the network.

Note the following when configuring IP Addresses:

If the device fails to retrieve an IP address through DHCP, the default IP address is **192.168.0.239**.

To access the page, click **IP Settings** under the **System** menu.

IPv4

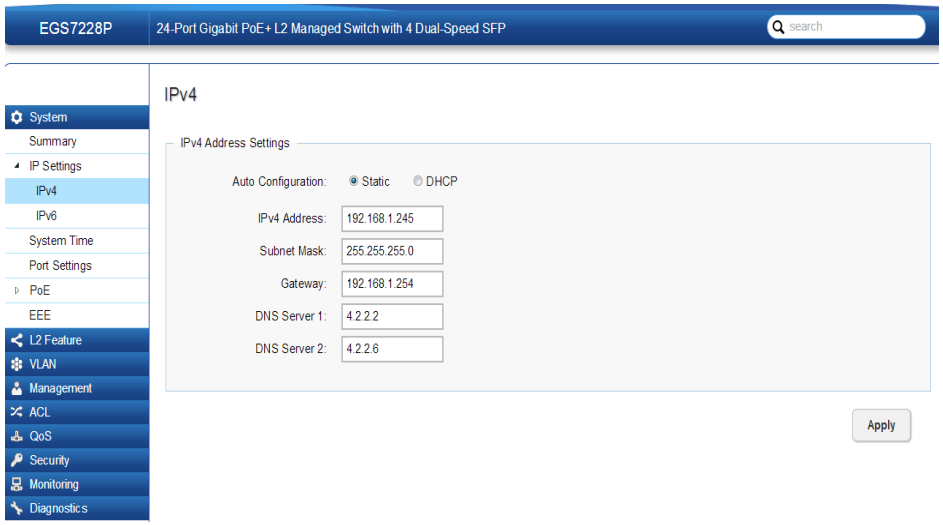
Select whether to you wish to enable **Static** or **DHCP** for Auto-Configuration. Next, enter the information for the IP address, gateway, and DNS servers.

To be managed over the network, the Switch needs an IP Address to be assigned. The IP Settings screen contains fields for assigning IP addresses. IP addresses are either defined as Static or are retrieved using the Dynamic Host Configuration Protocol (DHCP). DHCP assigns dynamic IP addresses to devices on a network. DHCP ensures that network devices have a different IP address every time the device connects to the network.

Important: If the device fails to retrieve an IP address through DHCP, the default IP address is: **192.168.0.239** and the factory default subnet mask is: **255.255.255.0**.

To access the page, click **IPv4** under **IP Settings** in the **System** menu.

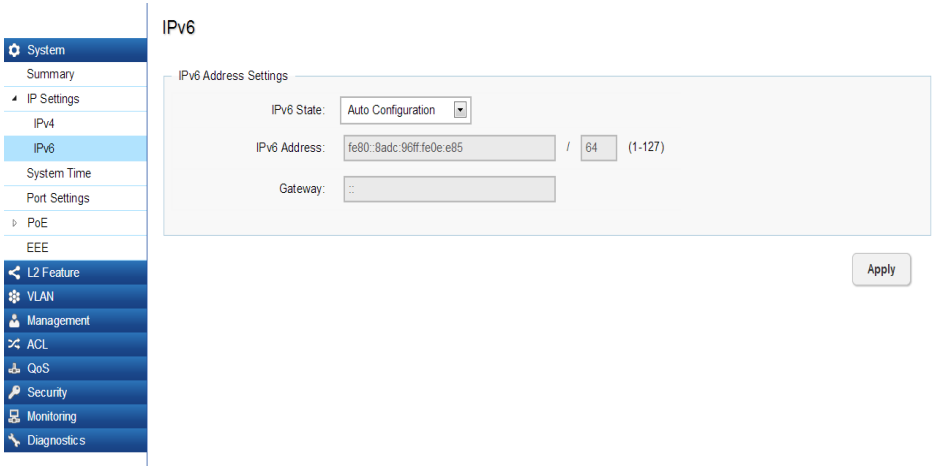
Dynamic IP Address (DHCP):	Enables the IP address to be configured automatically by the DHCP server. Select this option if you have a DHCP server that can assign the Switch an IP address, subnet mask, default gateway IP address, and a domain name server IP address automatically. Selecting this field disables the IP Address, Subnet mask, and Gateway fields.
Static IP Address:	Allows the entry of an IP address, subnet mask, and a default gateway for the Switch. Select this option if you don't have a DHCP server or if you wish to assign a static IP address to the Switch.
IP Address:	This field allows the entry of an IPv4 address to be assigned to this IP interface. Enter the IP address of your Switch in dotted decimal notation. The factory default value is: **192.168.0.239**.
Subnet Mask:	A Bitmask that determines the extent of the subnet that the Switch is on. This should be labeled in the form: xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimals) between 0 and 255. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed. Enter the IP subnet mask of your Switch in dotted decimal notation. The factory default value is: **255.255.255.0**.
Gateway:	Enter an IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an Intranet, or you do not want the Switch to be accessible outside your local network, you can leave this field blank.
DNS Server (Domain Name System):	Used for mapping a domain name to its corresponding IP address and vice versa. Enter a DNS IP address in order to be able to use a domain name to access the Switch instead of using an IP address.



Apply: Click **APPLY** to update the the system settings.

IPv6

IPv6 is a an upgraded version to IPv4, providing more available IP addresses as well as other benefits. To access the switch over an IPv6 network you must first configure it with IPv6 information (IPv6 prefix, prefix length, and default gateway). To configure IPv6 for the Switch, select whether to you wish to enable **Auto-Configuration**, **Static,** or **DHCP** for the IPv6 State. Next, enter the information for the IP address, range, and gateway.



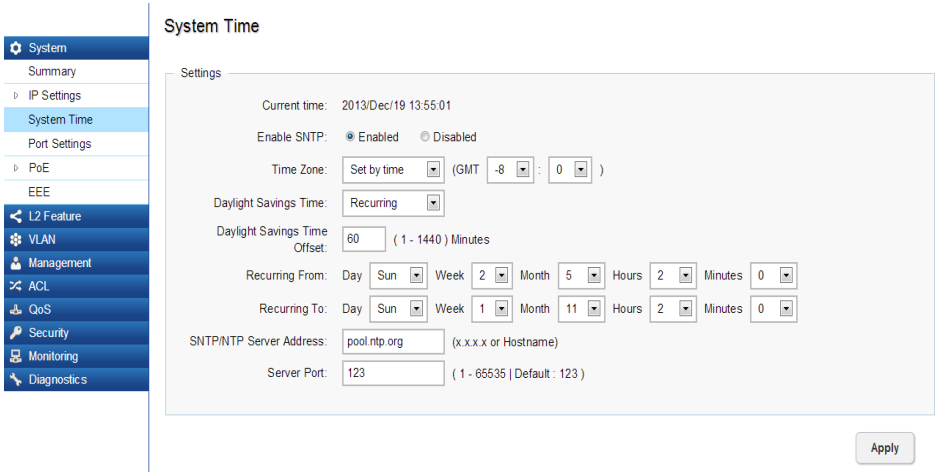
IPv6 State:	Select whether you wish to enable Auto Configuration, DHCPv6 Client, or Static for the IPv6 address.
Auto Configuration:	Use this option to set the IPv6 address for the IPv6 network interface in Auto Configuration. The Switch will automatically generate and use a globally-unique IPv6 address based on the network prefix and its Ethernet MAC address.
DHCPv6 Client:	This enables the IP address to be configured automatically by the DHCP server. Select this option if you have an IPv6 DHCP server that can assign the Switch an IPv6 address/Prefix and a default gateway IP address.
Static:	Allows the entry of an IPv6 address/Prefix and a default gateway for the Switch. Select this option if you wish to assign static IPv6 address information to the Switch.
IPv6 Address:	This field allows the entry of an IPv6 address/Prefix to be assigned to this IP interface.
Gateway:	Set the default gateway IPv6 address for the interface. Enter the default gateway IPv6 address.

Apply: Click **APPLY** to update the system settings.

System Time

Use the System Time screen to view and adjust date and time settings.

The Switch supports Simple Network Time Protocol (SNTP). SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. This software operates only as an SNTP client and cannot provide time services to other systems.



Current time:	Displays the current time.
Enable SNTP:	Select whether to **Enable** or **Disable** the SNTP server. The system time is set via an SNTP sever.
Time Zone:	Select the difference between Greenwich Mean Time (GMT) and local time.
Daylight Savings Time:	Select between **Recurring** or **Non-recurring**.
Daylight Savings Time Offset:	Enter the time of Daylight Savings Time Offset.
Recurring From:	Select the Day, Week, Month, and Hour from the list.
Recurring To:	Select the Day, Week, Month, and Hour from the list.
SNTP/NTP Server Address:	Enter the SNTP or NTP sever IP address or hostname.
Server Port:	Displays the time sever port.

To configure date/time through SNMP:

1. Next to the Enable SNTP, select **Enable**.

2. In the Time Zone Offset list, select by country or by the Coordinated Universal Time (UTC/GMT) time zone in which the Switch is located.

3. Next select **Disabled**, **Recurring**, or **Non-Recurring** for Daylight Savings Time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.

4. In the SNTP/NTP Server Address field, enter the IP address or the host name of the SNTP/NTP server.

5. Finally, enter the port number on the SNTP server to which SNTP requests are sent. The valid range is from 1-65535. The default is: 123.

6. Click **APPLY** to update the system settings.

To configure date/time manually:

1. Next to the Enable SNTP, select **Disable**.

2. In the Manual Time field, use the drop-down boxes to manually select the date and time you wish to set.

3. In the Time Zone Offset list, select by country or by the Coordinated Universal Time (UTC/GMT) time zone in which the Switch is located.

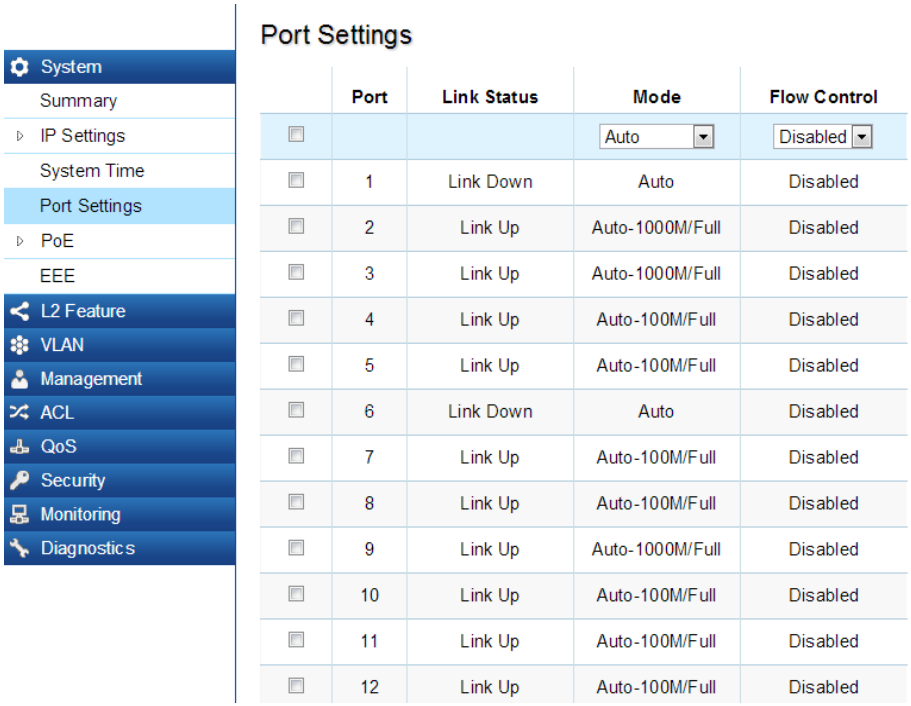
4. Next select **Disabled**, **Recurring** or **Non-recurring** for Daylight Savings Time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.

5. Click **APPLY** to update the system settings.

Port Settings

Use this screen to view and configure Switch port settings. The Port Settings feature lets you change the configuration of the ports on the Switch in order to find the best balance of speed and flow control according to your preferences. Configuring Gigabit ports require additional factors to be considered when arranging your preferences for the Switch compared to 10/100 ports.

To access the page, click **Port Settings** under the **System** menu.



Port:	Displays the port number.
Link Status:	Indicates whether the link is up or down.
Mode:	Select the speed and the duplex mode of the Ethernet connection on this port. Selecting Auto (Auto-Negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the Switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support autoegotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the Switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.

Flow Control:	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port. The Switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later.

Click **APPLY** to update the system settings.

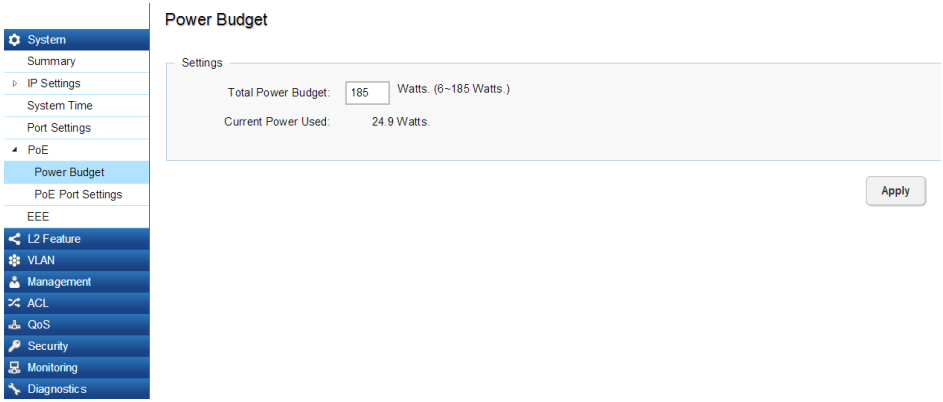
PoE

Power Budget

The PoE Management screen contains system PoE information for monitoring the current power usage and assigns the total amount of power the Switch can provide to all of its PoE ports. Ports 1~8,24, or 48 on the Switch are IEEE802.3at/af compliant ports. Each port is capable of delivering up to 30 Watts and a total PoE budget of either 130, 185, 370 or 740 Watts depending on your model for uninterrupted PoE use. To access the page, click **PoE** under the **System** menu.

	Ports	Power Budget
EWS5912FP	8	130 Watts
EWS7228P	24	185 Watts
EWS7229FP	24	370 Watts
EWS7952FP	48	740 Watts

Total Power Budget:	Enter the amount of power the Switch can provide to all ports.
Current Power Used:	Shows the total amount of power currently being delivered to all ports.



Apply: Click **APPLY** to update the the system settings.

PoE Port Settings

The EnGenius Layer 2 PoE+ Switches supports Power over Ethernet (PoE) as defined by the IEEE 802.3af and 802.3at. All ports can support PoE up to 30W. Ports 1-24 can supply about 48 VDC power to Powered Devices (PDs) over standard UTP Ethernet cables. The Switch follows the standard PSE (Power Sourcing Equipment) pinout, whereby power is sent out over pins 1, 2, 3 and 6.

EGS5212FP: Ports 1-8 supports both IEEE802.3 af and at. The maximum power budget is 130 Watts.

EGS7228P: Ports 1-24 supports both IEEE802.3 af and at. The maximum power budget is 185 Watts.

EGS7228FP: Ports 1-24 supports both IEEE802.3 af and at. The maximum power budget is 370 Watts and 720 Watts when you are using the EnGenius RPS370 external redundant power supply.

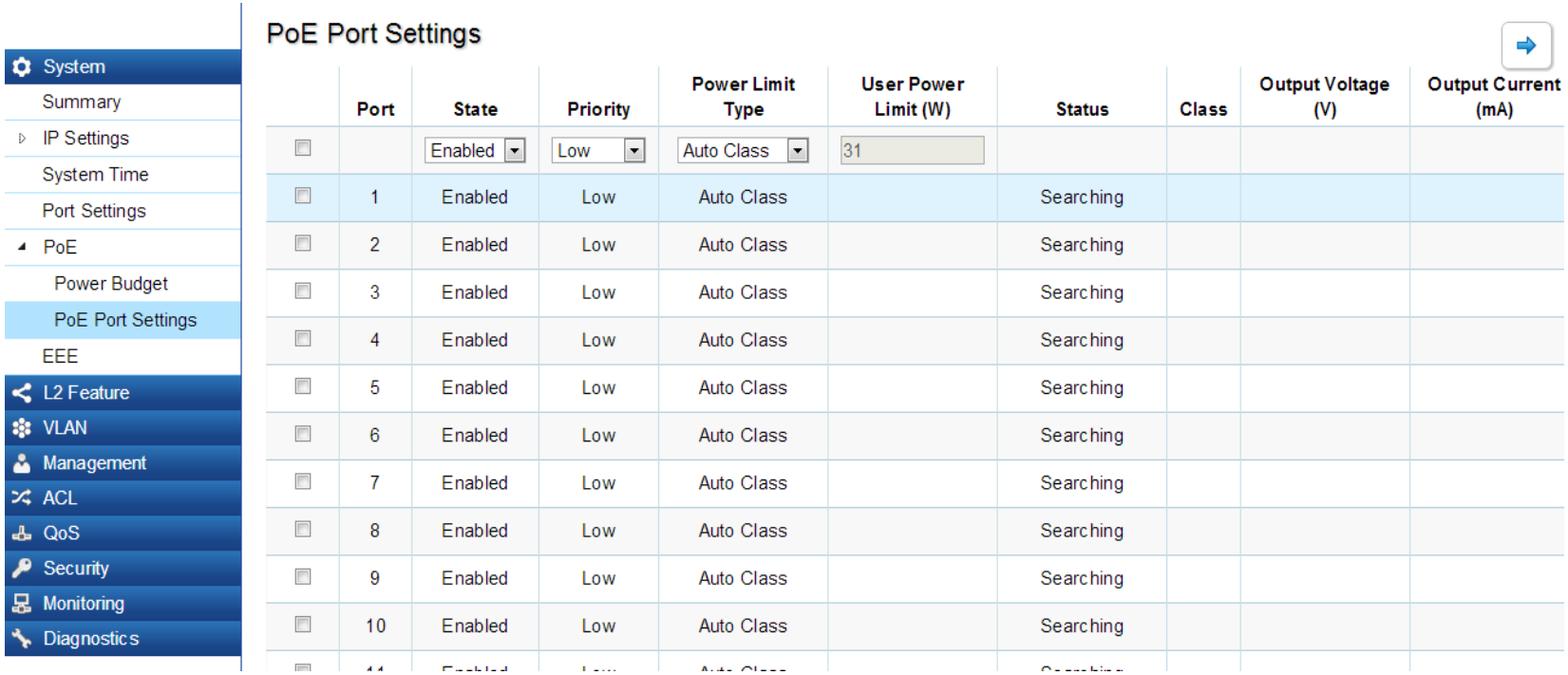
EGS7252FP: Ports 1-48 supports both IEEE802.3 af and at. The maximum power budget is 740 Watts.

To access the page, click **PoE Port Settings** under **PoE** in the **System** Menu. To scroll, click the arrow button at the top right of the screen.

Port:	Displays the specific port for which PoE parameters are defined. PoE parameters are assigned to the powered device that is connected to the selected port.
State:	• **Enable -** Enables the Device Discovery protocol and provides power to the device using the PoE module. The Device Discovery Protocol lets the device discover powered devices attached to device interfaces and learns their classification. • **Disable -** Disables the Device Discovery protocol and halts the power supply delivering power to the device using the PoE module.
Priority:	Select the port priority if the power supply is low. The field default is **Low**. For example, if the power supply is running at 99% usage, and port 1 is prioritized as high, but port 6 is prioritized as low, port 1 is prioritized to receive power and port 6 may be denied power. The possible field values are: **4**. • **Low** - Sets the PoE priority level as low. • **Medium** - Sets the PoE priority level as medium. • **High** - Sets the PoE priority level as high. • **Critical** - Sets the PoE priority level as critical.

Class(Auto):	Shows the classification of the powered device. The class defines the maximum power that can be provided to the powered device. The possible field values are: • **Class 0** – The maximum power level at the Power Sourcing. Equipment is 15.4 Watts. • **Class 1** – The maximum power level at the Power Sourcing. Equipment is 4.0 Watts. • **Class 2** – The maximum power level at the Power Sourcing. Equipment is 7.0 Watts. • **Class 3** – The maximum power level at the Power Sourcing. Equipment is 15.4 Watts. • **Class 4** – The maximum power level at the Power Sourcing. Equipment is 30 Watts.
Class (User	Select this option to base the power limit on the value configured in the User Power Limit field.
User Power Limit:	Sets the maximum amount of power that can be delivered by a port. **Note:** The User Power Limit can only be implemented when the Class value is set to **User-Defined**.

Status:	Shows the port's PoE status. The possible field values are: • **Delivering Power –** The device is enabled to deliver power via the port. • **Disabled –** The device is disabled for delivering power via the port. • **Test Fail –** The powered device test has failed. For example, a port could not be enabled and cannot be used to deliver power to the powered device. • **Testing -** The powered device is being tested. For example, a powered device is tested to confirm it is receiving power from the power supply. • **Searching –**The device is currently searching for a powered device. Searching is the default PoE operational status. • **Fault –** The device has detected a fault on the powered device when the port is forced on. For example; the power supply voltage is out of range, a short short occurs, a communication or there is a communication errorwith PoE devices, or an unknown error occurs.



Apply: Click **APPLY** to update the the system settings.

EEE

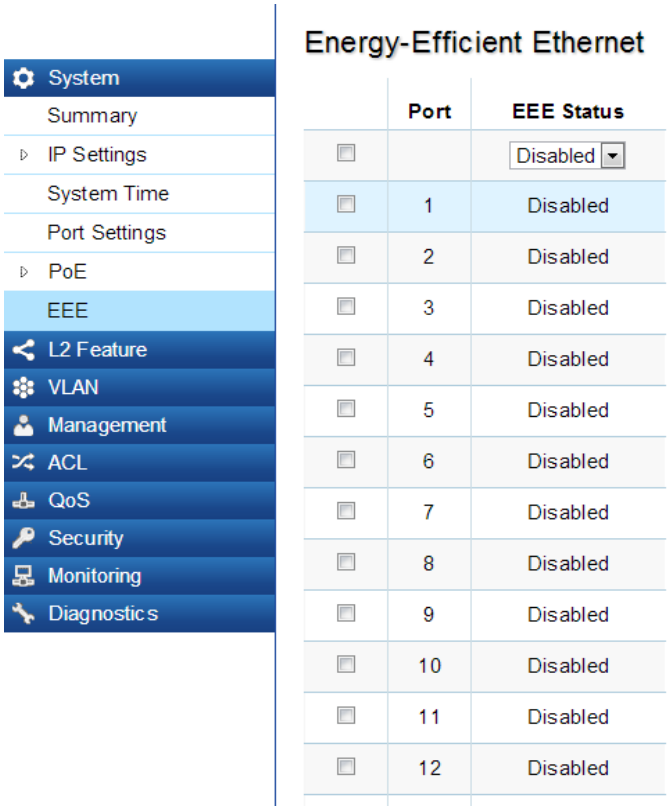
Energy Efficient Ethernet (EEE), an Institute of Electrical and Electronics Engineers (IEEE) 802.3az standard, reduces the power consumption of physical layer devices during periods of low link utilization. EEE saves energy by allowing PHY non-essential circuits shut down when there is no traffic.

Network administrators have long focused on the energy efficiency of their infrastructure, and the EnGenius Layer 2 Switch complies with the IEEE's Energy-Efficient Ethernet (EEE) standard to give you even more control. The EEE-compliant Switch offers users the ability to utilize power that Ethernet links use only during data transmission. Lower Power Idle (LPI) is the method for achieving the power saving during Ethernet idel time.

Use the EEE Configuration page to configure Energy Efficient Ethernet.

Port:	Display the port for which the EEEE setting is displayed.
EEE Status:	**Enable** or **Disable** EEE for the specified port.

Click **APPLY** to update the system settings.



L2 Features

The L2 Feature tab exhibits complete standard-based Layer 2 switching capabilities, including: Link Aggregation, 802.1D single Spanning Tree Protocol, 802.1w Rapid Spanning Tree Protocol, 802.1s Multiple Spanning Tree Protocol, MAC Address Table, Internet Group Management Protocol (IGMP) Snooping, Port Mirroring, 802.1ab Link Layer Discovery Protocol (LLDP), and Multicast Listener Discovery(MLD) snooping. Utilize these features to configure the Switch to your preferences.

Link Aggregation

A Link Aggregation Group (LAG) optimizes port usage by linking a group of ports together to form a single, logical, higher-bandwidth link. Aggregating ports multiplies the bandwidth and increases port flexibility for the Switch. Link Aggregation is most commonly used to link a bandwidth intensive network device (or devices), such as a server, to the backbone of a network.

The participating ports are called Members of a port trunk group. Since all ports of the trunk group must be configured to operate in the same manner, the configuration of the one port of the trunk group is applied to all ports of the trunk group. Thus, you will only need to configure one of any of the ports in a trunk group. A specific data communication packet will always be transmitted over the same port in a trunk group. This ensures the delivery of individual frames of a data communication packet will be received in the correct order. The traffic load of the LAG will be balanced among the ports according to Aggregate Arithmetic. If the connections of one or several ports are broken, the traffic of these ports will be transmitted on the normal ports, so as to guarantee the connection reliability.

When you aggregate ports, the ports and LAG must fulfill the following conditions:

- All ports within a LAG must be the same media/ format type.
- A VLAN is not configured on the port.
- The port is not assigned to another LAG.
- The Auto-negotiation mode is not configured on the port.
- The port is in full-duplex mode.
- All ports in the LAG have the same ingress filter ing and tagged modes.
- All ports in the LAG have the same back pressure and flow control modes.
- All ports in the LAG have the same priority.
- All ports in the LAG have the same transceiver type.
- Ports can be configured as LACP ports only if the ports are not part of a previously configured LAG.

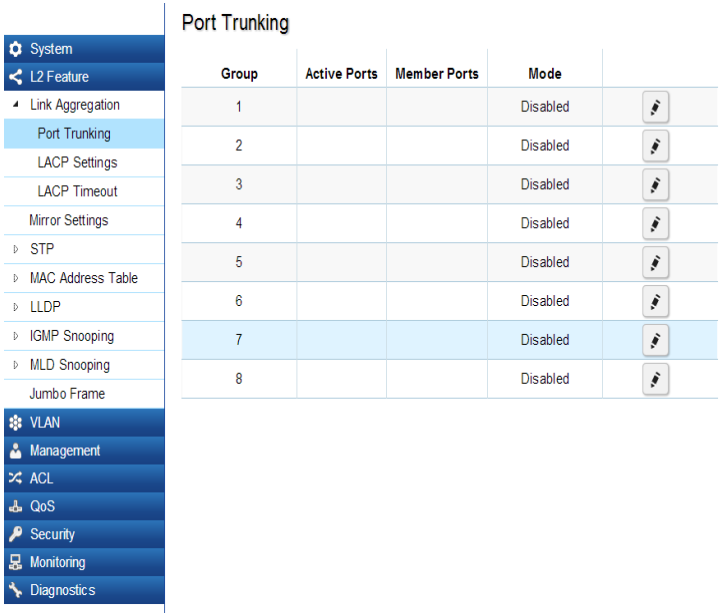
LACP is a dynamic protocol which helps to automate the configuration and maintenance of LAG's. The main purpose of LACP is to automatically configure individual links to an aggregate bundle, while adding new links and helping to recover from link failures if the need arises. LACP can monitor to verify if all the links are connected to the authorized group. LACP is a standard in comput- er networking, hence LACP should be enabled on the Switch's trunk ports initially in order for both the partic- ipating Switches/devices that support the standard, to use it.

Port Trunking

Port Trunking allows you to assign physical links to one logical link that functions as a single, higher-speed link, providing dramatically increased bandwidth. Use Port Trunking to bundle multiple connections and use the combined bandwidth as if it were a single larger "pipe".

Important: You must enable Trunk Mode before you can add a port to a trunk group.

To access the page, click **Port Trunking** under **L2 Features.**



Group:	Displays the number of the given trunk group. You can utilize up to 8 link aggregation groups and each group consisting up to 8 ports on the Switch.
Active Ports:	Displays the active participating members of the trunk group.
Member Port:	Select the ports you wish to add into the trunk group. Up to eight ports per group can be assigned. • **Static** - The Link Aggregation is configured manually for specified trunk group. • **LACP** - The Link Aggregation is configured dynamically for specified trunk group
Mode:	LACP allows for the automatic detection of links in a Port Trunking Group when connected to a LACP-compliant Switch. You will need to ensure both the Switch and device connected to are the same mode in order for them to function, otherwise they will not work. Static configuration is used when connecting to a Switch that does not support LACP.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

LACP Settings

Assign a system priority to run with Link Aggregation Control Protocol (LACP) and is become for a backup link if a link goes down. The lowest system priority is allowed to make decisions about which ports it is actively participating in in case a link goes down. If two or more ports have the same LACP port priority, the port with the lowest physical port number will be selected as the backup port. If a LAG already exists with the maximum number of allowed port members, and LACP is subsequently enabled on another port using a higher priority than an existing member, the newly configured port will replace the existing port member that has a lower priority. A smaller number indicates a higher priority level. The range is from 0-65535 and default is: 32768.

Apply: Click **APPLY** to update the the system settings.

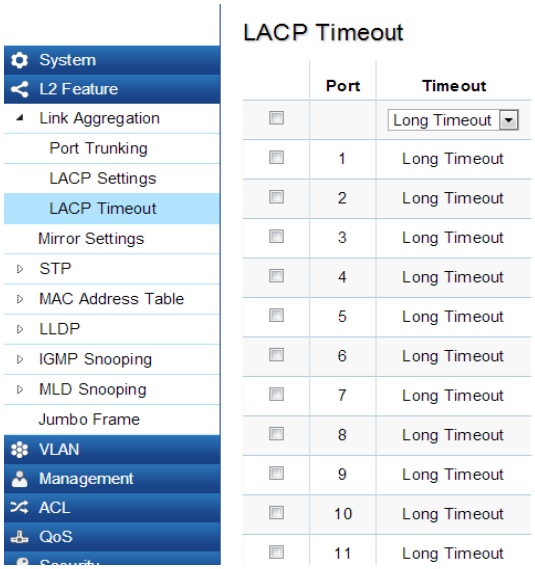
System Priority:	Enter the LACP priority value to the system. The default is 32768 and the range is from 1-65535.

LACP Timeout

Link Aggregation Control Protocol (LACP) allows the exchange of information with regard to the link aggregation between two members of aggregation. The LACP Time Out value is measured in a periodic interval. Check first whether the port in the trunk group is up. When the interval expires, it will be removed from the trunk. Set a Short Timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible. The default value for LACP time out is: Long Timeout.

Timeout:	Select the administrative LACP timeout. • **Long** - Long timeout value. • **Short** - Short timeout value.
Long:	The LACP PDU will be sent for every 30 seconds, and the LACP timeout value is 90 seconds.
Short:	The LACP PDU will be sent every second. The timeout value is 3 seconds.

Apply: Click **APPLY** to update the the system settings.



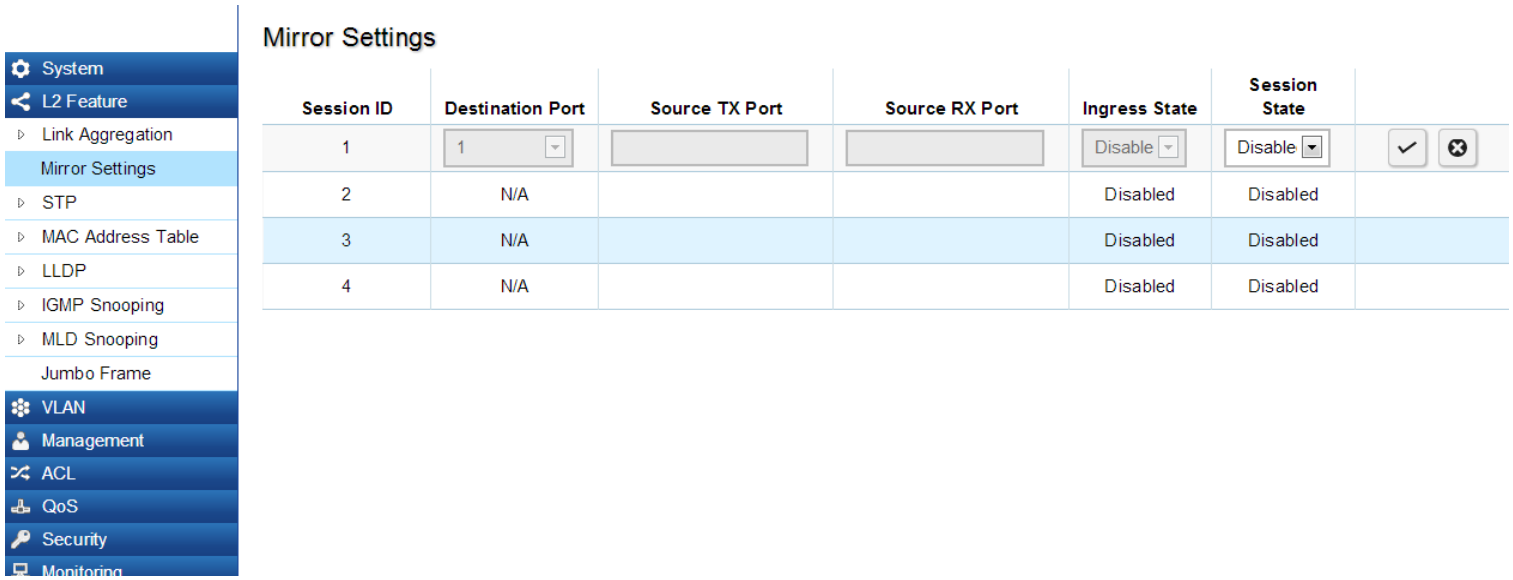
Mirror Settings

Mirrors network traffic by forwarding copies of incoming and outgoing packets from specific ports to a monitoring port. The packet that is copied to the monitoring port will be the same format as the original packet.

Port mirroring is useful for network monitoring and can be used as a diagnostic tool. Use port mirroring to send traffic to applications that analyze traffic for purposes such as monitoring compliance, detecting intrusions, monitoring and predicting traffic patterns, and other correlating events. Port Mirroring is needed for traffic analysis on a Switch because a Switch normally sends packets only to the port to which the destination device is connected. The analyzer captures and evaluates the data without affecting the client on the original port. Port mirroring can consume significant CPU resources while active, so be concious of such usage when configuring the Switch.

.

Mirror ID:	A number identifying the mirror session. This Switch only supports up to 4 mirror sessions.
Port:	Displays the session ID for port mirroring.
Destination Port:	Select the port for traffic purposes from source ports mirrored to this port.
Source TX/RX Port:	Sets the source port from which traffic will be mirrored. **TX Port:** Only frames transmitted from this port are mirrored to the destination port. **RX Port:** Only frames received on this port are mirrored to the destination port. **Both:** Frames received and transmitted on this port are mirrored to the specified destination port. **None:** Disables mirroring for this port.
Ingress State	Select whether to **Enable** or **Disable** ingress traffic forwarding.
Session State:	Select whether to **Enable** or **Disable** port mirroring.



NOTE: You cannot mirror a faster port onto a slower port. For example, if you try to mirror the traffic from a 100 Mbps port onto a 10 Mbps port, this can cause through-put problems. The port you are copying frames from should always support an equal or lower speed than the port to which you are sending the copies. Please note a target port and a source port cannot be the same port.

Click the **Apply** button ✓ to accept the changes or the **Cancel** button ⊗ to discard them.

STP

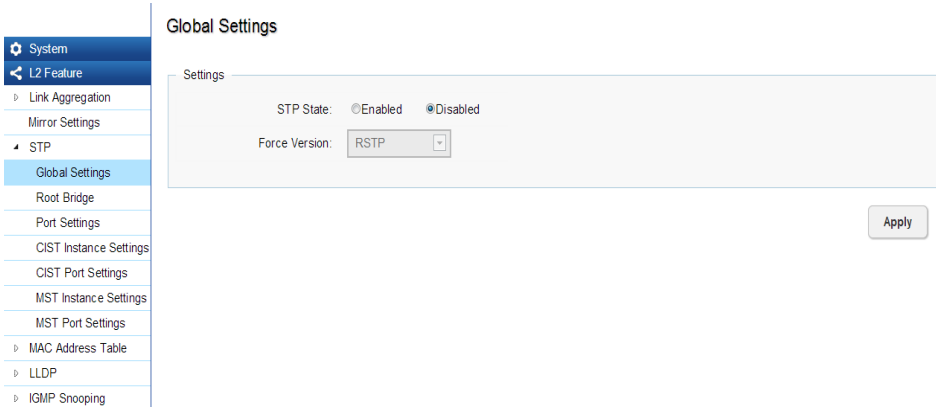
The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between Switches. This allows the Switch to interact with other bridging devices in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

STP provides a tree topology for the Switch. There are different types of Spanning tree verisons, supported, including Spanning Tree Protocol (STP) IEEE802.1D, Multiple Spanning Tree Protocol (MSTP) IEEE802.1w, and Rapid Spanning Tree Protocol (RSTP) IEEE802.1s. Please note that only one spanning tree can be active on the Switch at a time.

Global Settings

Spanning Tree Protocol (STP) is a Layer 2 protocol that runs on Switches. Spanning Tree Protocol (STP) allows you to ensure that you do not create loops when you have redundant paths in the network. STP provides a single active path between two devices on a network in order to prevents loops from being formed when the Switch is interconnected via multiple paths.

STP uses a distributed algorithm to select a bridging device that serves as the root for the spanning tree network. It does this by selecting a root port on each bridging device to incur the lowest path cost when forwarding a packet from that device to the root device. It then selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. Next, all ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, disabling all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops. STP provides a single active path between two devices on a network in order to prevent loops from being formed when the Switch is interconnected via multiple paths.



Once a stable network topology has been established, all bridges listen for Hello Bridge Protocol Data Units (BPDUs) transmitted from the Root Bridge of the Spanning Tree. If a bridge does not receive a Hello BPDU after a predefined interval (known as the Maximum Age), the bridge will assume that the link to the Root Bridge is down and unavailable. This bridge then initiates negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

Spanning Tree Loops

Loops occur when alternate routes exist between hosts. Loops in an extended network can cause the Switch to forward traffic indefinitely, resulting in increased traffic and reducing network efficiency. Once the STP is enabled and configured, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links is also accomplished automatically. STP provides a tree topology and other Spanning tree versions supported include STP, Multiple Spanning Tree Protocol (MSTP), and Rapid Spanning Tree Protocol (RSTP). Please note that only one spanning tree can be active on the Switch at a time. The default setting is: RSTP.

STP:	Select whether to **Enable** or **Disable** the spanning tree operation on the Switch.
Force Version:	Select the Force Protocol Version parameter for the Switch. • **STP** (Spanning Tree Protocol) - IEEE 802.1D. • **RSTP** (Rapid Spanning Tree Protocol) - IEEE 802.1w. • **MSTP** (Multiple Spanning Tree Protocol) - IEEE 802.1s.

Multiple Spanning Tree Protocol (MSTP) defined in IEEE 802.1s, enables multiple VLANs to be mapped to reducethe number of spanning-tree instances needed to support a large number of VLANs. If there is only one VLAN in the network, a single STP works appropriately.

If the network contains more than one VLAN however, the logical network configured by a single STP would work, but it becomes more efficent to use the alternate paths available by using an alternate spanning tree for different VLANs or groups of VLANs. MSTP (which is based on RSTP for fast convergence) is designed to support independent spanning trees based on VLAN groups. MSTP provides multiple forwarding paths for data traffic and enables load balancing.

STP and RSTP prevent loops from forming by ensuring that only one path exists between the end nodes in your network. RSTP is designed as a general replacement for the slower, legacy STP. RSTP is also incorporated into MSTP. With STP, convergence can take up to a minute to complete in a larger network. This can result in the loss of communication between various parts of the network during the convergence process so STP can subsequently can lose data packets during transmission.

RSTP on the other hand is much faster than STP. It can complete a convergence in seconds, so it greatly diminishes the possible impact the process can have on your network compared to STP. RSTP reduces the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails and retain the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

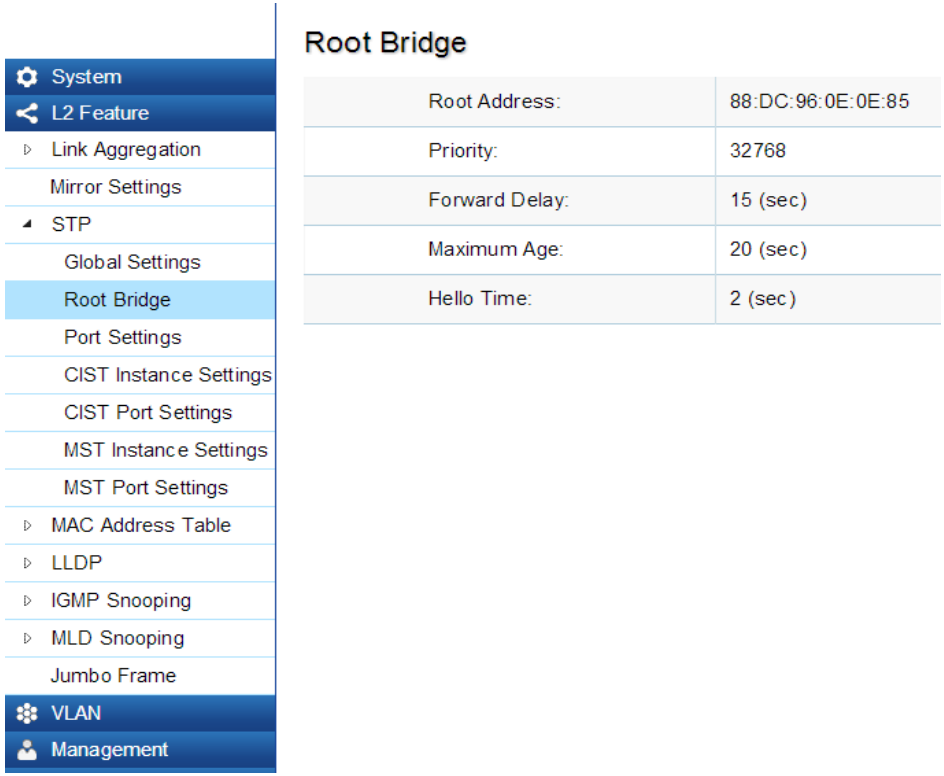
Select whether to **Enable** or **Disable** the Spanning Tree function for the Switch. Next, select whether you wish to enable STP, RSTP, or MSTP. Again, please note that only one Spanning tree function can be active at a time.

Apply: Click **APPLY** to update the the system settings.

Root Bridge

The Root Bridge serves as an administrative point for all Spanning Tree calculations to determine which redundant links to block in order to prevent network loops. From here, you can view all the information regarding the Root Bridge within the STP.

All other decisions in a spanning tree network, such as ports being blocked and ports being put in a forwarding mode, are made regarding a root bridge. The root bridge is the "root" of the constructed "tree" within a spanning tree network. Thus, the root bridge is the bridge with the lowest bridge ID in the spanning tree network. The bridge ID includes two parts; the bridge priority (2 bytes) and the bridge MAC address (6 bytes). The 802.1d default bridge priority is: 32768. STP devices exchange Bridge Protocol Data Units (BPDUs) periodically. All bridges "listen" for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (called the Maximum Age), the bridge assumes that the link to the root bridge is down. The bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

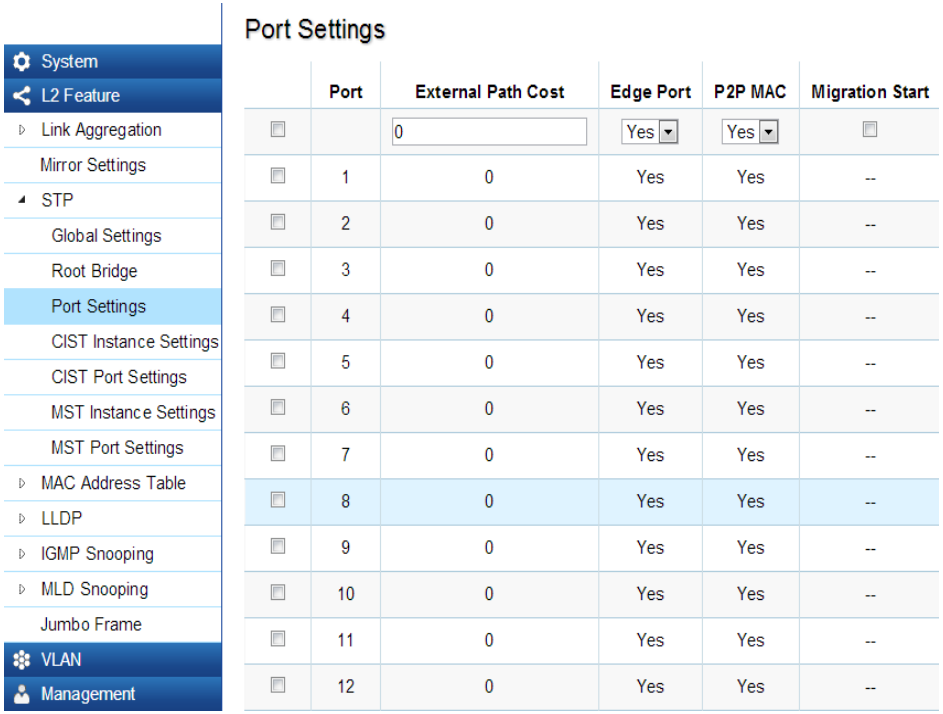


Root Address:	Displays the Root Bridge MAC address. Root in Root Bridge refers to the base of the spanning tree, which the Switch could be configured for.
Priority:	Displays the priority for the bridge. When Switches are running STP, each is assigned a priority. After exchanging BPDUs, the Switch with the lowest priority value becomes the root bridge.
Forward Delay:	Displays the Switch Forward Delay Time. This is the time (in seconds) the Root Switch will wait before changing states (called listening to learning).
Maximum Age:	Displays the bridge Switch Maximum Age Time. This is the amount of time a bridge waits before sending a configuration message. The default is 20 seconds.
Hello Time:	Displays the Switch Hello Time. This is the amount of time a bridge remains in a listening and learning state before forwarding packets. The default is 15 seconds.

Port Settings

STP and RSTP help guard against the formation of loops in an Ethernet network topology. A loop occurs when nodes transmit packets to each other over more than one data path. Packets can become caught in repetitious cycles that needlessly consume network bandwidth which then significantly reduce network performance. With STP, you can set it up on a port per port basis to to further help configure your network topology. The Switch allows each port to have its own spanning tree, and so will require some of its own configuration settings.

Port:	The port or trunked ports you wish to configure.
External Path Cost:	This defines a metric that indicates the relative cost of forwarding packets to the specified port list. The port cost can be set automatically or as a metric value. The default value is 0 (auto). Setting 0 for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. The default port cost for a 100Mbps port is 200,000 and the default port cost for a Gigabit port is 20000. Enter a value between 1 and 200000000 to determine the External Cost. The lower the number, the greater the probability the port will be chosen to forward packets.
Edge Port:	Indicate whether the port is **Enabled** or **Disabled**. •**Yes** - Designates the port as an edge port. • **No** - There is no edge port status.
P2P MAC:	A P2P port must operate in full duplex. Like edge ports, P2P ports transition to a forwarding state rapidly, thus benefiting from RSTP. Enable P2P for the device to establish a point-to-point link, or specify for the device to automatically establish a point-to-point link. Select Yes or No from the list for point-to-point(P2P) . • **Yes** - Restricted in that a P2P port must operate in full-duplex. • **No** -There is no P2P port status.
Migration Start:	When operating in RSTP mode, enable this function to force the port to use the new MST/RST BPDUs and restart the migration delay timer.



Edge Ports

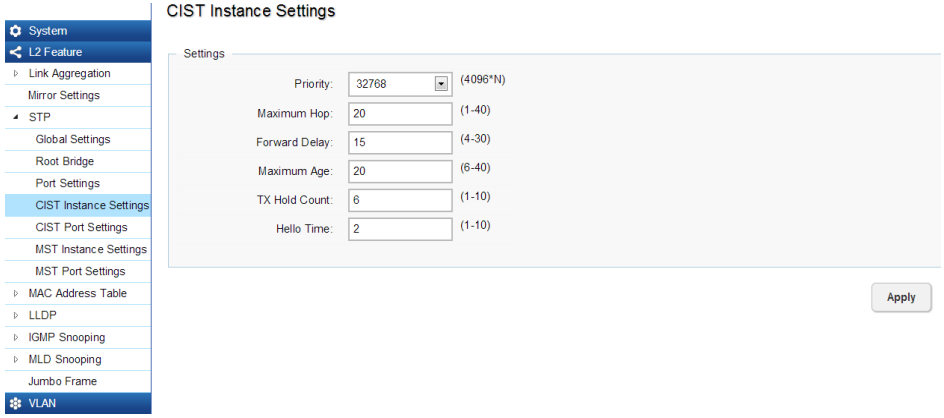
An edge port changes its initial STP port state from a blocking state to a forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Edge Ports are not connected to LANs that have span¬ning tree devices, so Edge Ports do not receive Bridge Protocol Data Units (BPDUs). If an Edge Port starts to receive BPDUs, it is no longer considered an edge port to the Switch.

Apply: Click **APPLY** to update the the system settings.

CIST Instance Settings

The Common Instance Spanning Tree (CIST) protocol is formed by the spanning-tree algorithm running among bridges that support the IEEE 802.1w, IEEE 802.1s, and IEEE 802.1D standard. A Common and Internal Spanning Tree (CIST) represents the connectivity of the entire network and it is equivalent to a spanning tree in an STP/ RSTP.

The CIST inside a Multiple Spanning Tree Instance (MST) region is the same as the CST outside a region. All regions are bound together using a CIST, which is responsible for creating loop-free topology across regions, whereas the MSTI controls topology inside regions. CST instances allow different regions to communicate between themselves. CST is also used for traffic within the region for any VLANs not covered by a MSTI. In an MSTP-enabled network, there is only one CIST that runs between MST regions and single spanning tree devices. A network may contain multiple MST regions and other network segments running RSTP. Multiple regions and other STP bridges are interconnected using a single CST.



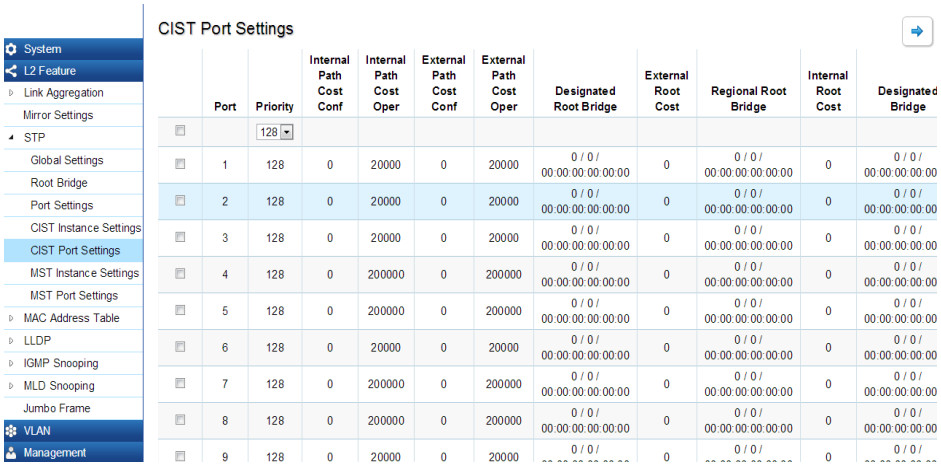
Enter the information to set up CIST for the Switch:

Priority:	Select from the list to specify the priority of the Switch for comparison in the CIST. CIST priority is an important criterion on determining the root bridge. In the same condition, the Switch with the highest priority will be chosen as the root bridge. A lower value has a higher priority. The default value is: 32768 and should be an exact divisor of 4096.
Maximum Hop:	Used to set the number of hops between devices in a spanning tree region before the BPDU packet sent by the Switch is discarded. Each Switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BDPU packet and the information held for the port will age out. The user may set a hop count from 6 to 40. The default value is: 20.
Forward Delay:	Enter the bridge forward delay time, which indicates the amount of time in seconds that a bridge remains in a listening and learning state before forwarding packets. The value must be greater or equal to (Bridge Max Age/2) + 1. The time range is from 4 seconds to 30 seconds. The default value is 15 seconds.
Maximum Age:	The Max Age may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. The user may choose a time between 6 and 40 seconds. The default value is: 20 seconds
TX Hold Count:	Enter the maximum number of Hello packets transmitted per interval. The count can be specified from 1 to 10. The default is: 6.
Hello Time:	Enter the Switch's Hello Time. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to verify that it is the Root Bridge. The Hello Time range is from 1 to 10 seconds. The default Hello Time is: 2 seconds.

Apply: Click **APPLY** to update the the system settings.

CIST Port Settings

Use the CIST Ports Settings page to configure and view STA attributes for interfaces when the spanning tree mode is set to STP or RSTP. You may use a different priority or path cost for ports of the same media type to indicate a preferred path or Edge Port to indicate if the attached device can support fast forwarding or link type to indicate a point-to-point connection or shared-media connection.



MST ID:	Select the MST ID from the list.
Port:	Port or trunked port identifier.
Priority:	Defines the priority used for this port in the Spanning Tree Algorithm. If the path cost for all ports on a Switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Algorithm is detecting network loops. When more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. The range is from 0-240, in steps of 16; and the default is: 128.
Internal Path Cost Conf:	The Internal Path Cost setting allows you to specify the relative cost of sending spanning tree traffic through the interface to adjacent bridges within a spanning tree region.
Internal Path Cost Oper:	The External Path Cost setting is used to calculate the cost of sending spanning tree traffic through the interface to reach an adjacent spanning tree region. The spanning tree algorithm tries to minimize the total path cost between each point of the tree and the root bridge.

Designated Root Bridge:	Displays the Root Bridge for the CST. It is comprised using the bridge priority and the base MAC address of the bridge.
Internal Root Cost:	This is the cost to the CIST regional root in a region.
External Root Cost:	External Root Cost is the cost to the CIST root.
Regional Root Bridge:	This is the bridge identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.
Internal Port Cost:	Enter the cost of the port.
Edge Port Conf:	Displays the Edge Port state.
Designated Bridge:	This is the Bridge Identifier of the bridge of the Designated Port. It is made up using the bridge priority and the base MAC address of the bridge.
Port Role:	Each MST Bridge Port that is enabled is assigned a Port Role within each spanning tree. The port role will be one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port, or Disabled.
Port State:	The Forwarding State of this port. The state parameters are: Discarding, Learning, Forwarding, or Disabled.

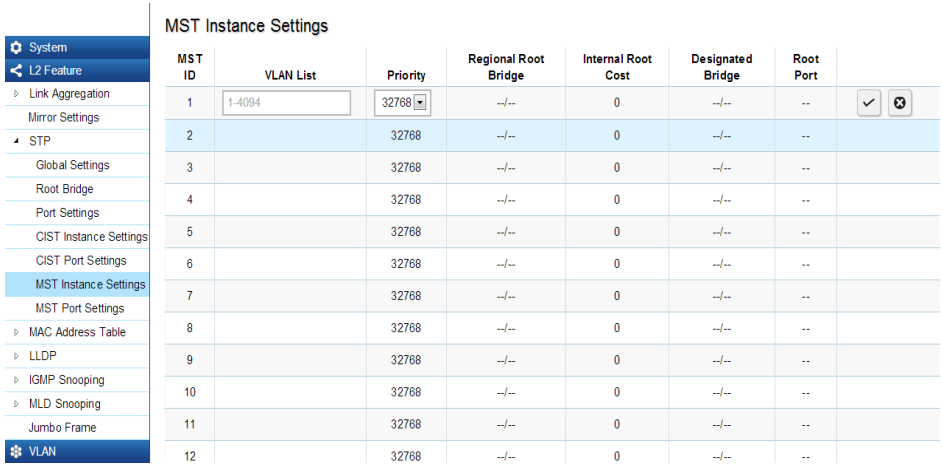
Apply: Click **APPLY** to update the the system settings.

MST Instance Settings

Multiple Spanning Tree Protocol, or MSTP enables the grouping of multiple VLANs with the same topology requirements into one Multiple Spanning Tree Instance (MSTI). MSTP then builds an Internal Spanning Tree (IST) for the region containing commonly configured MSTP bridges. Instances are not supported in STP or RSTP. Instead, they have the same spanning tree in common within the VLAN. MSTP provides the capability to logically divide a Layer 2 network into regions. Every region can contain multiple instances of spanning trees. In MSTP, all of the interconnected bridges that have the same MSTP configuration comprise an MST region.

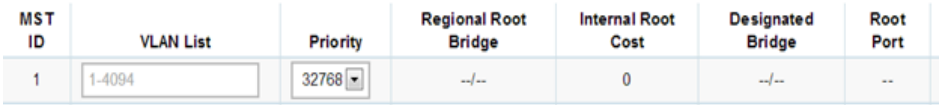
A Common Spanning Tree (CST) interconnects all adjacent MST Regions and acts as a virtual bridge node for communications between STP or RSTP nodes in the global network. MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree (CIST). The CIST is formed as a result of the running spanning tree algorithm between Switches that support STP, RSTP, and MSTP protocols. Once you specify the VLANs you wish to include in a Multiple Spanning Tree Instance (MSTI), the protocol will automatically build an MSTI tree to maintain connectivity among each of the VLANs. MSTP maintains contact with the global network because each instance is treated as an RSTP node in the Common Spanning Tree (CST).

Click the Edit button to configure the MST settings. Next, enter information for the VLAN List and choose the priority you wish to use from the drop-down list.



MST ID:	Displays the ID of the MST group that is created. A maximum of 15 groups can be set for the Switch.
VLAN List:	Enter the VLAN ID range from for the configured VLANs to associate with the MST ID. The VLAN ID number range is from 1 to 4094.
Priority:	Select the bridge priority value for the MST. When Switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the Switch with the lowest priority value becomes the root bridge. The default value is: 32768. The range is from 0-61440. The bridge priority is a multiple of 4096.
Regional Root Bridge:	This is the bridge identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.
Internal Root Cost:	Displays the path cost to the designated root for the MST instance.
Designated Bridge:	Displays the bridge identifier of the bridge with the Designated Port. It is made up using the bridge priority and the base MAC address of the bridge.
Root Port:	Displays the port that accesses the designated root for MST instance.
Configuration Name:	This name uniquely identifies the MSTI (Multiple Spanning Tree Instance). Enter a descriptive name (up to 32 characters) for an MST region. The default is the MAC address name of the device running MSTP.

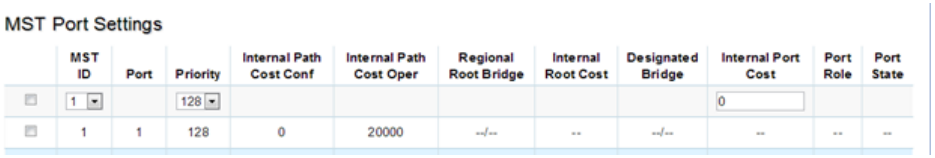
Configuration Reversion:	This value, along with the Configuration Name, identifies the MSTP region configured on the Switch. Devices must have the same revision number to belong to the same region.



Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

MST Port Settings

This page displays the current MSTI configuration information for the Switch. From here you can update the port configuration for an MSTI ID. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for ports you wish to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest MAC address into the forwarding state and other interfaces will be blocked. Note that a lower priority values mean higher priorities for forwarding packets.

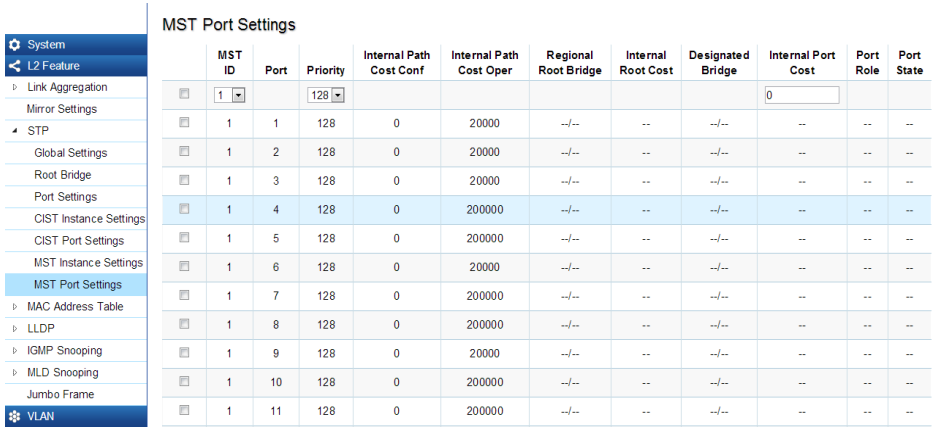

MST Port Settings

	MST ID	Port	Priority	Internal Path Cost Conf	Internal Path Cost Oper	Regional Root Bridge	Internal Root Cost	Designated Bridge	Internal Port Cost	Port Role	Port State
	1		128						0		
	1	1	128	0	20000	--/--	--	--/--	--	--	--

MST ID:	Displays the ID of the MST group that is created. A maximum of 15 groups can be set for the Switch.
Port:	Displays port or trunked port ID.
Priority:	Select the bridge priority value for the MST. When Switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the Switch with the lowest priority value becomes the root bridge. The bridge priority is a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest priority that is a multiple of 4096. For example, if you set the priority to any value from 0 through 4095, the priority is set to 0. The default priority is: 32768. The valid range is from 0-61440.
Internal Path Cost Conf:	The Internal Path Cost setting allows you to specify the relative cost of sending spanning tree traffic through the interface to adjacent bridges within a spanning tree region.
Internal Path Cost Oper:	Displays the operation cost of the path from this bridge to the Root Bridge.
Regional Root Bridge:	This is the bridge identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.

Internal Root Cost:	Displays the path cost to the designated root for the selected MST instance.
Designated Bridge:	Displays the Bridge Identifier of the bridge for the Designated Port. It is made up using the bridge priority and the base MAC address of the bridge.
Internal Port Cost:	This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within an STP instance. Selecting this parameter with a value in the range of 1 to 200000000 will set the quickest route when a loop occurs. A lower internal cost represents a quicker transmission. Selecting 0 (zero) for this parameter will set the quickest optimal route automatically for an interface.
Port Role:	Each MST bridge port that is enabled is assigned a Port Role for each spanning tree. The Port Role is one of the following values: Root, Designated, Alternate, Backup, Master, or Disabled.
Port State:	Displays the state of the selected port.
Edge Port Oper:	Displays the operating Edge Port state.
P2P MAC Conf:	Displays the P2P MAC state.
P2P MAC Oper:	Displays the operating P2P MAC state.
Port Role:	Displays the port role. Shows each MST Bridge Port that is assigned a port role for each spanning tree.
Port State:	Displays the state of the selected port.

Port State:	Indicates the current STP state of a port. If enabled, the Port State determines what forwarding action is taken regarding traffic. The possible port states are: • **Disabled:** STP is disabled on the port. The port forwards traffic while learning MAC addresses. • **Blocking:** The port is blocked and cannot be used to forward traffic or learn MAC addresses. • **Listening:** The port is in listening mode. The port cannot forward traffic or learn MAC addresses in this state. • **Learning:** The port is in learning mode. The port cannot forward traffic. However, it can learn new MAC addresses. • **Forwarding:** The port is in forwarding mode. The port can forward traffic and learn new MAC addresses in this state.



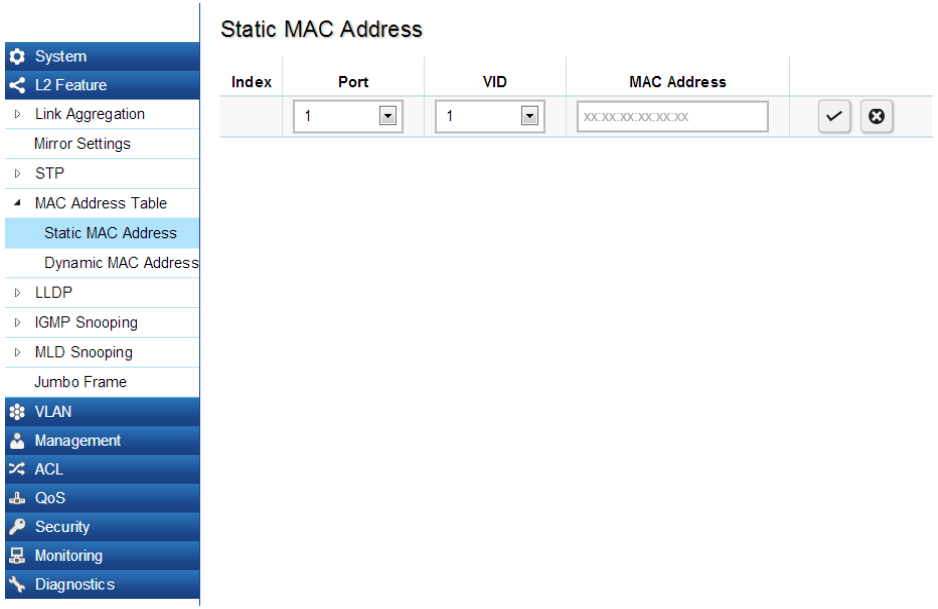
Apply: Click **APPLY** to update the the system settings.

MAC Address Table

The MAC address table contains address information that the Switch uses to forward traffic between the inbound and outbound ports. All MAC addresses in the address table are associated with one or more ports. When the Switch receives traffic on a port, it searches the Ethernet switching table for the MAC address of the destination. If the MAC address is not found, the traffic is flooded out all of the other ports associated with the VLAN. All of the MAC address that the Switch learns by monitoring traffic are stored in the Dynamic address.
A Static address allows you to manually enter a MAC address to configure a specific port and VLAN.

Static MAC Address

The address table lists the destination MAC address, the associated VLAN ID, and port number associated with the address. When you specify a Static MAC address, you are set the MAC address to a VLAN and a port; thus it makes an entry into its forwarding table. These entries are then used to forward packets through the Switch. Static MAC addresses along with the Switch's port security allow only devices in the MAC address table on a port to access the Switch.



To access the page, click **Static MAC Address** under the **L2 Feature** tab.

Index:	Displays the index for the Static MAC Address table.
Port:	Select the port where the MAC address entered in the previous field will be automatically forwarded.
VID:	Enter the VLAN ID on which the IGMP snooping querier is administratively enabled and for which the VLAN exists in the VLAN database.
MAC Address:	Enter a unicast MAC address for which the switch has forwarding or filtering information.

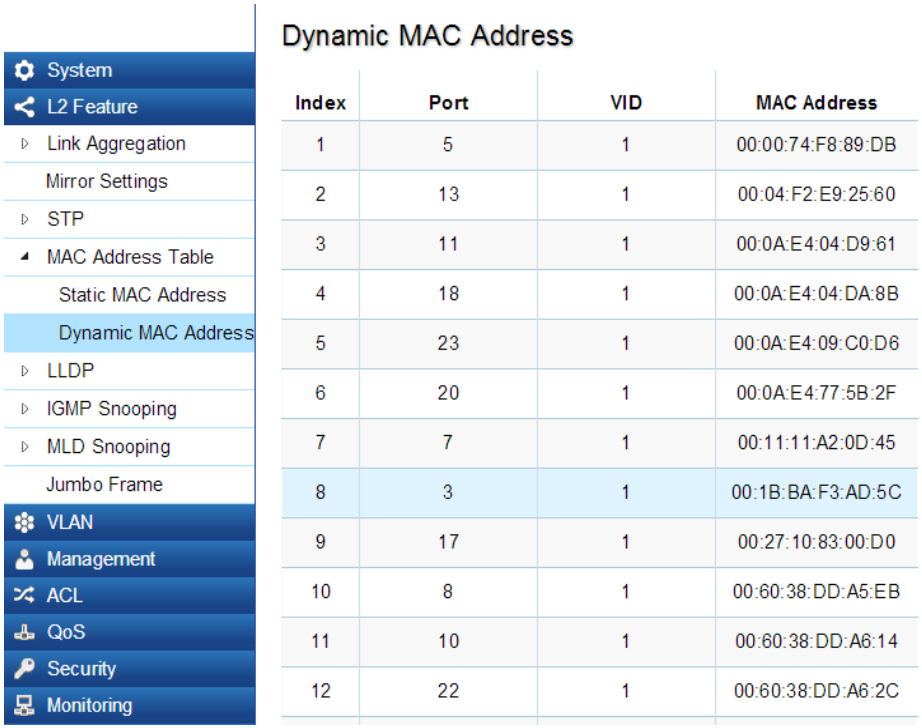
Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Dynamic MAC Address

The Switch will automatically learn the device's MAC address and store it to the Dynamic MAC address table. If there is no packet received from the device within the aging time, the Switch adopts an aging mechanism for updating the tables from which MAC address entries will be removed from related network devices. The Dynamic MAC Address Table shows the MAC addresses and their associated VLANs learned on the selected port.

Index:	Displays the index for the Dynamic MAC Address table.
Port:	Select the port to which the entry refers.
VID:	Displays the VLAN ID for the specified MAC address
MAC Address:	Displays the MAC addresses that the Switch learned from a specific port.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.



Dynamic MAC Address

Index	Port	VID	MAC Address
1	5	1	00:00:74:F8:89:DB
2	13	1	00:04:F2:E9:25:60
3	11	1	00:0A:E4:04:D9:61
4	18	1	00:0A:E4:04:DA:8B
5	23	1	00:0A:E4:09:C0:D6
6	20	1	00:0A:E4:77:5B:2F
7	7	1	00:11:11:A2:0D:45
8	3	1	00:1B:BA:F3:AD:5C
9	17	1	00:27:10:83:00:D0
10	8	1	00:60:38:DD:A5:EB
11	10	1	00:60:38:DD:A6:14
12	22	1	00:60:38:DD:A6:2C

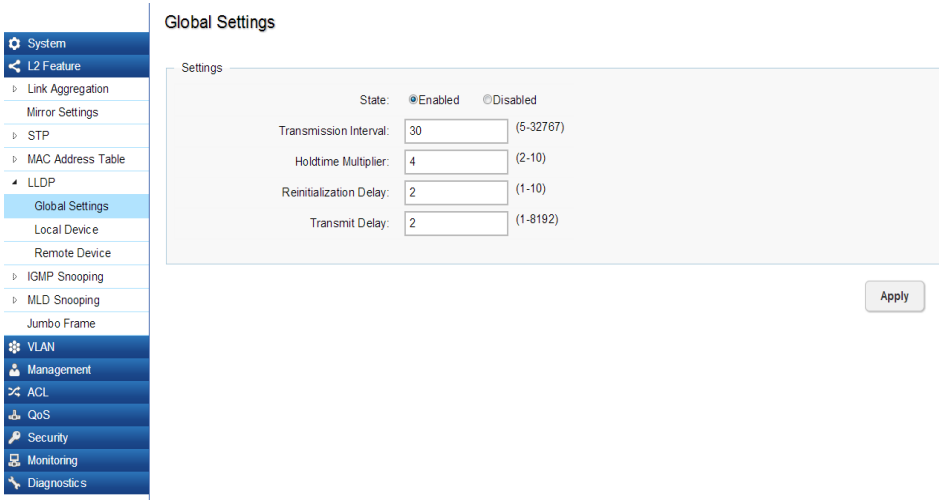
LLDP

Link Layer Discovery Protocol (LLDP) is the IEEE 802.1AB standard for Switches to advertise their identity, major capabilities, and neighbors on the 802 LAN. LLDP allows users to views the discovered information to identify system topology and detect faulty configurations on the LAN. LLDP is essentially a neighbor discovery protocol that uses Ethernet connectivity to advertise information to devices on the same LAN and store information about the network. The information transmitted in LLDP advertisements flow in one direction only; from one device to its neighbors. This information allows the device to quickly identify a variety of other devices, resulting in a LAN that interoperates smoothly and efficiently.

LLDP transmits information as packets called LLDP Data Units (LLDPDUs). A single LLDP Protocol Data Unit (LLDP PDU) is transmitted within a single 802.3 Ethernet frame. A basic LLDPDU consists of a set of Type-Length-Value elements (TLV), each of which contains information about the device. A single LLDPDU contains multiple TLVs. TLVs are short information elements that communicate complex data. Each TLV advertises a single type of information.

Global Settings

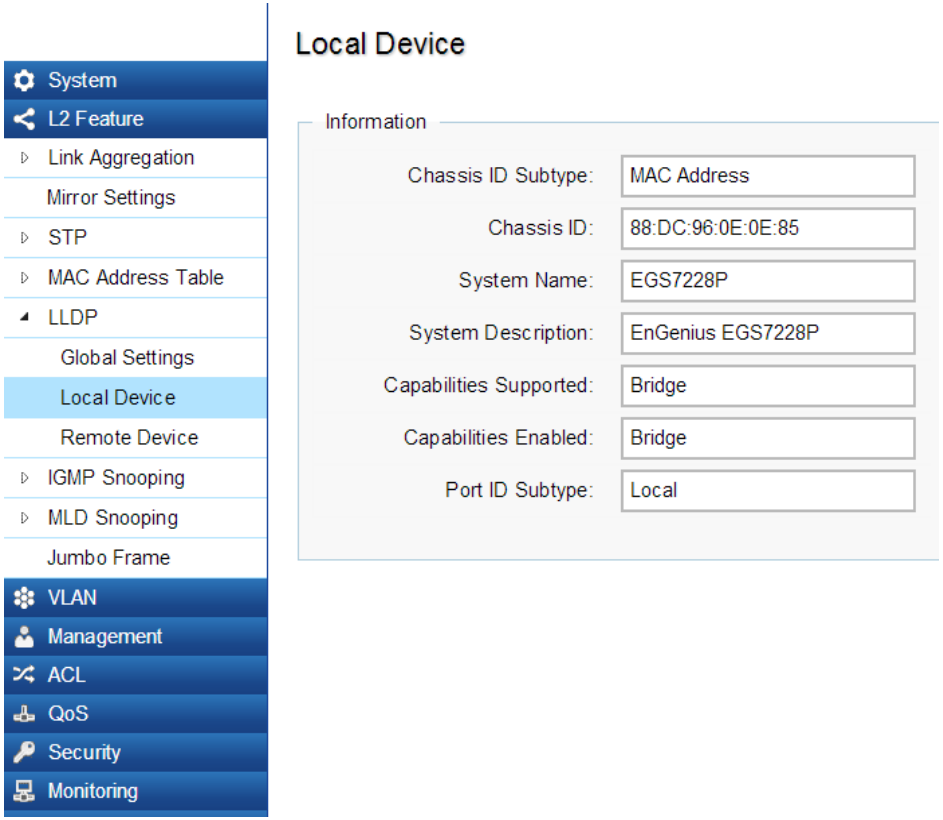
Select whether to **Enable** or **Disable** the LLDP feature on the Switch. Next, enter the Transmission interval, Holdtime Multiplier, Reinitialization Delay parameter, and the Transmit Delay parameter. When finished, click **APPLY** to update the the system settings.



State:	Select **Enabled** or **Disabled** to activate LLDP for the Switch.
Transmission Interval:	Enter the interval at which LLDP advertisement updates are sent. The default value is 30. The range is from 5-32768.
Holdtime Multiplier:	Enter the amount of time that LLDP packets are held before packets are discarded and measured in multiples of the Advertised Interval. The default is 4. The range is from 2-10.
Reinitialization Delay:	Enter the amount of time of delay before reinitializing LLDP. The default is 2. The range is from 1-10.
Transmit Delay:	Enter the amount of time that passes between successive LLDP frame transmissions. The default is 2 seconds. The range is 1-8192 seconds.

Local Device

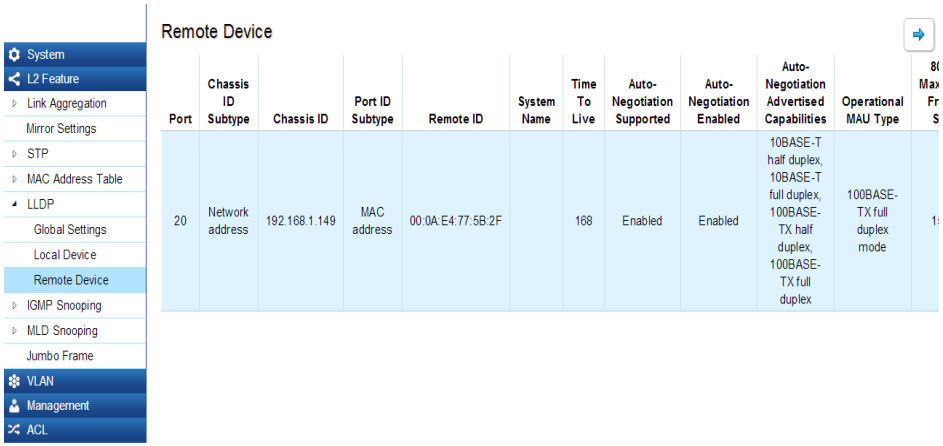
LLDP devices must support chassis and port ID advertisement, as well as the system name, system ID, system description, and system capability advertisements. Here, you can view detailed LLDP information for the EnGenius Switch.



Chassis ID Subtype:	Displays the chassis ID type.
Chassis ID:	Displays the chassis ID of the device transmitting the LLDP frame.
System Name:	Displays the administratively assigned device name.
System Description:	Describes the device.
Capabilities Supported:	Describes the device functions.
Capabilities Enabled:	Describes the device functions.
Port ID Subtype:	Displays the port ID type.

Remote Device

LLDP devices must support chassis and port ID advertisement, as well as the system name, system ID, system description, and system capability advertisements. From here you can viewing detailed LLDP Information for the remote Switch. To scroll, click on the arrow at the top right of the screen.



Port:	Displays the port.
Chassis ID Subtype:	Displays the chassis ID type.
Chassis ID:	Displays the chassis ID of the device that is transmitting the LLDP frame.
Port ID Subtype:	Displays the port ID type.
Remote ID:	Displays the Remote ID.
System Name:	Displays the administratively assigned device name.
Time to Live:	Displays the time.
Auto-Negotiation Supported:	Displays state for the Auto-Negotiation Supported.
Auto-Negotiation Enabled:	Displays state for the Auto-Negotiation Enabled.
Auto-Negotiation Advertised Capabilities:	Displays the type of Auto-Negotiation Advertised Capabilities.
Operational MAU Type:	Displays the type of MAU.
802.3 Maximum Frame Size:	Displays the size of 802.3 Maximum Frame.
802.3 Link Aggregation Capabilities:	Displays the 802.3 Link Aggregation Capabilities.
802.3 Link Aggregation Status:	Displays the status of 802.3 Link Aggregation.
802.3 Link Aggregation Port ID:	Displays the port ID of 802.3 Link Aggregation.

Mode:	Aggregated links can be set up manually or automatically. Select **Static** or **LACP** for the Link Aggregation type. • **Static** - The Link Aggregation is configured manually for the specified trunk group. • **LACP** - The Link Aggregation is configured dynamically for the specified trunk group.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Remote ID	System Name	Time To Live	Auto-Negotiation Supported	Auto-Negotiation Enabled	Auto-Negotiation Advertised Capabilities	Operational MAU Type	802.3 Maximum Frame Size	802.3 Link Aggregation Capability	802.3 Link Aggregation Status	802.3 Link Aggregation Port ID
:0A:E4:77:5B:2F		151	Enabled	Enabled	10BASE-T half duplex, 10BASE-T full duplex, 100BASE-TX half duplex, 100BASE-TX full duplex	100BASE-TX full duplex mode	1522	Not capable of being aggregated	Not currently in aggregation	0

IGMP Snooping

Internet Group Management Protocol (IGMP) Snooping allows a Switch to forward multicast traffic intelligently. Multicasting is used to support real-time applications such as videoconferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any host that wishes to receive the multicast register with their local multicast Switch.

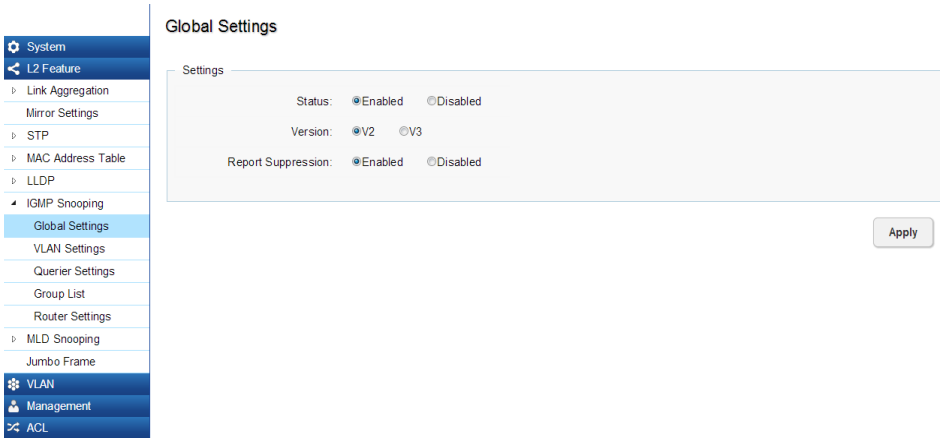
A multicast group is a group of end nodes that want to receive multicast packets from a multicast application. After joining a multicast group, a host node must continue to periodically issue reports to remain a member. Any multicast packets belonging to that multicast group are then forwarded by the Switch from the port.

A Switch supporting IGMP Snooping can passively snoop on IGMP Query, Report, and Leave packets transferred between IP Multicast Switches and IP Multicast hosts to determine the IP Multicast group membership. IGMP Snooping checks IGMP packets passing through the network and configures Multicasting accordingly. Based on the IGMP query and report messages, the Switch forwards traffic only to the ports that request the multicast traffic. It enables the Switch to forward packets of multicast groups to those ports that have validated host nodes. The Switch can also limit flooding of traffic to IGMP designated ports. This improves network performance by restricting the multicast packets only to Switch ports where host nodes are located. IGMP Snooping significantly reduces overall Multicast traffic passing through your Switch. Without IGMP Snooping, Multicast traffic is treated in the same manner as a Broadcast transmission, which forwards packets to all ports on the network.

IGMPv1	Defined in RFC 1112. An explicit join message is sent to the Switch, but a timeout is used to determine when hosts leave a group.
IGMPv2	Defined in RFC 2236. Adds an explicit leave message to the join message so that Switch can more easily determine when a group has no interested listeners on a LAN.
IGMPv3	Defined in RFC 3376. Support for a single source of content for a multicast group.

Global Settings

Click to **Enable** or **Disable** the IGMP Snooping feature for the Switch. Next, select whether you wish to use V2 or V3. Finally, select whether you wish to **Enable** or **Disable** the Report Suppression feature for the Switch.

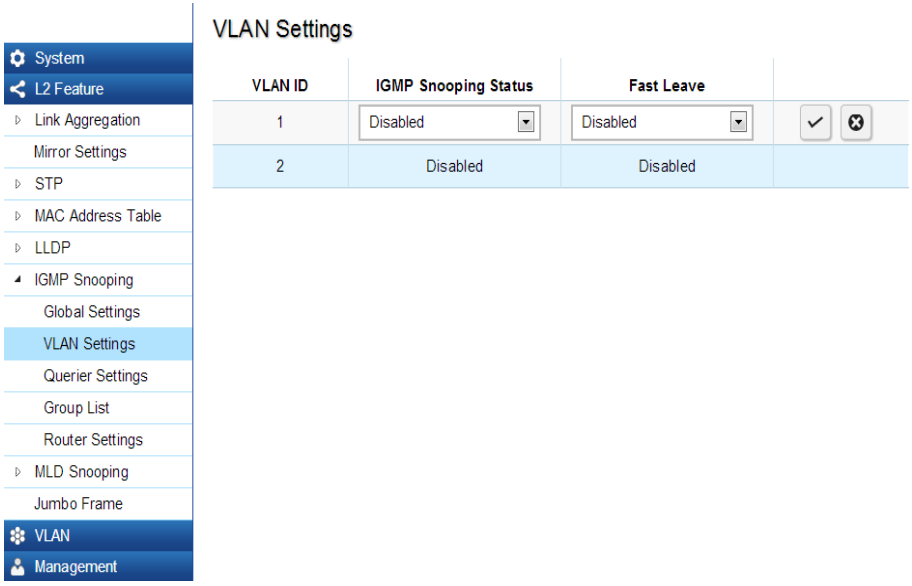


Status:	Select to **Enable** or **Disable** IGMP Snooping on the Switch. The switch snoops all IGMP packets it receives to determine which segments should receive packets directed to the group address when enabled.
Version:	Select the IGMP version you wish to use. If an IGMP packet received by the interface has a version higher than the specified version, this packet will be dropped.
Report Suppression:	Select whether Report Suppression is **Enabled** or **Disabled** for IGMP Snooping. The Report Suppression feature limits the amount of membership reports the member sends to multicast capable routers.

Apply: Click **Apply** to update the system settings.

VLAN Settings

Use the IGMP Snooping VLAN Settings to configure IGMP Snooping settings for VLANs on the system. The Switch performs IGMP Snooping on VLANs that send IGMP packets. You can specify the VLANs that IGMP Snooping should be performed on. Choose from the drop-down box whether to **Enable** or **Disable** IGMP Snooping. Next, choose to **Enable** or **Disable** Fast Leave for the VLAN ID.



Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

VLAN ID:	Displays the VLAN ID.
IGMP Snooping Status:	**Enables** or **Disables** the IGMP snooping feature for the specified VLAN ID.
Fast Leave:	**Enables** or **Disables** the IGMP snooping Fast Leave for the specified VLAN ID. Enabling this feature allows the Switch to immediately remove the Layer 2 LAN port from its forwarding table entry upon receiving an IGMP leave message without first sending out IGMP group-specific (GS) queries to the port.

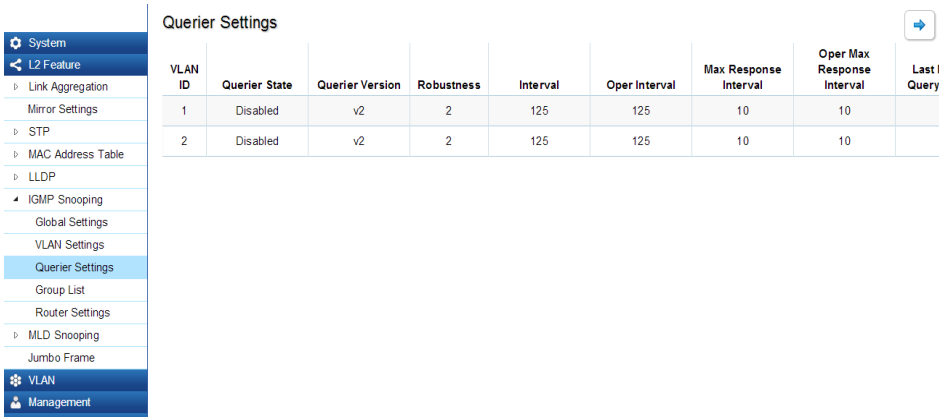
If Fast Leave is not used, a multicast querier will send a GS-query message when an IGMPv2/v3 group leave message is received. The querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period. If Fast Leave is enabled, the Switch assumes that only one host is connected to the port. Therefore, Fast Leave should only be enabled on a port if it is connected to only one IGMP-enabled device.

Fast Leave is supported only with IGMPv2 or IGMPv3 Snooping when IGMP Snooping is enabled. Fast Leave does not apply to a port if the Switch has learned that a multicast querier is attached to it.

Fast Leave can improve bandwidth usage for a network which frequently experiences many IGMP host add and leave requests.

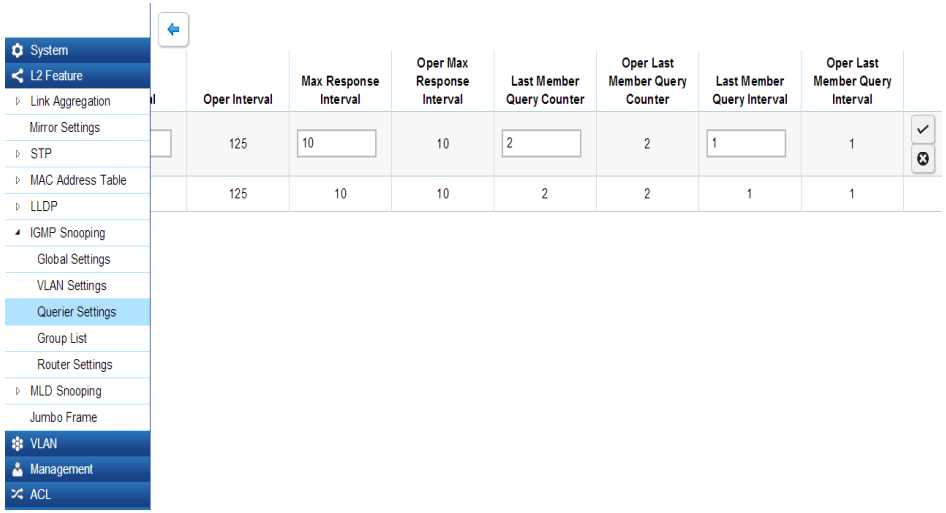
Querier Settings

IGMP snooping requires that one central Switch to periodically query all end devices on the network to announce their Multicast memberships and this central device is the IGMP querier. The snooping Switch sends out periodic queries with a time interval equal to the configured querier query interval. The IGMP query keeps the Switch updated with the current multicast group membership information. If the Switch does not received the updated membership information, then it will stop forwarding multicasts to specified VLANs.



VLAN ID:	Displays the VLAN ID.
Querier State:	Select whether to Enable or Disable the IGMP querier state for the specified VLAN ID. A querier can periodically ask their hosts if they wish to receive multicast traffic. The Querier feature will check whether hosts wish to receive multicast traffic when enabled. An Elected querier will assume the role of querying the LAN for group members, and then propagates the service requests on to any upstream multicast Switch to ensure that it will continue to receive the multicast service. This feature is only supported for IGMPv1 and v2 snooping.
Querier Version:	Enter the version of IGMP packet that will be sent by this port. If an IGMP packet received by the port has a version higher than the specified version, this packet will be dropped.
Robustness:	Provides fine-tuning to allow for expected packet loss on a subnet. It is used in calculating the following IGMP message intervals. The default is 2.

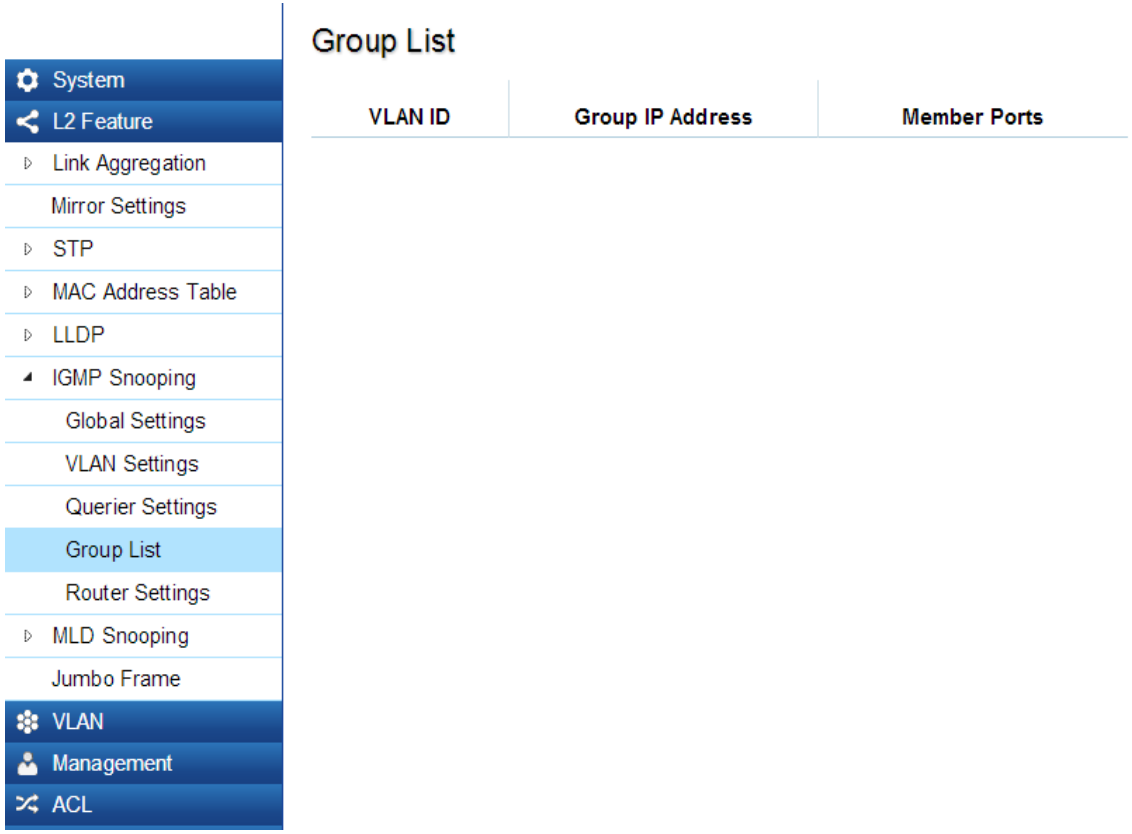
Oper Interval:	Displays the IGMP Interval of the operational querier.
Max Response Interval:	Enter the maximum response time used in the queries that are sent by the snooping querier. The default is 10 seconds.
Oper Max Response Interval:	Display the maximum response time which used in the queries that are sent by the snooping querier.
Last Member Query Counter:	Enter the number of the operational last member querier.
Oper Last Member Query Counter:	Enter the number of IGMP group-specific queries sent before the Switch assumes there are no local members.
Last Member Query Interval:	Displays the Operational Last Member Query Interval sent by the elected querier.
Oper Last Member Query Interval:	Enter the time between two consecutive group-specific queries that are sent by the querier, including those sent in response to leave-group messages. You might lower this interval to reduce the amount of time it takes a querier to detect the loss of the last member of a group.



Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

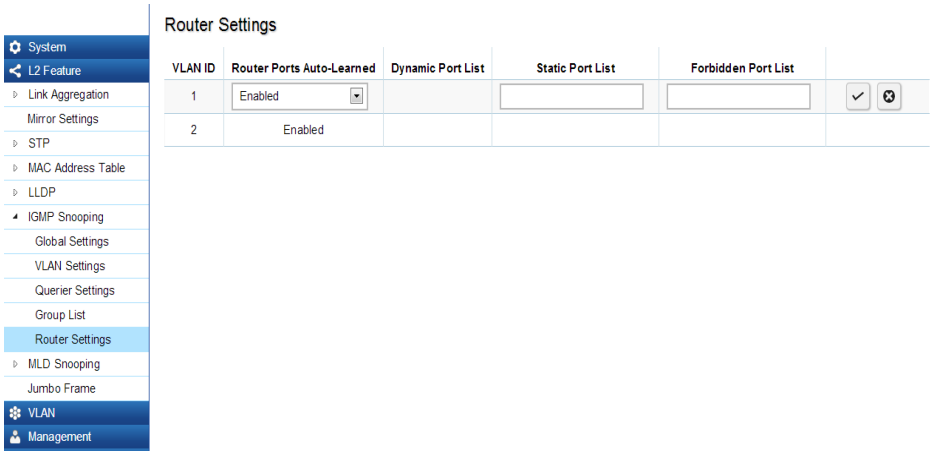
Group List

The Group List displays VLAN ID, Group IP Address, and Members Port in the IGMP Snooping List.



Router Settings

The Router Settings shows the learned multicast router attached port if the port is active and a member of the VLAN. Select the VLAN ID you would like to configure and enter the Static and Forbidden ports for the specified VLAN IDs. All IGMP packets snooped by the Switch will be forwarded to the multicast router reachable from the port.

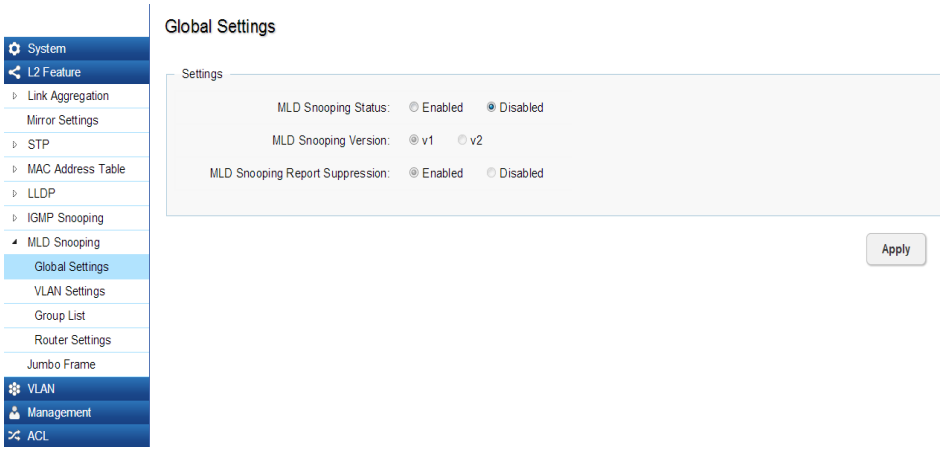


VLAN ID:	Displays the VLAN ID.
Router Ports Auto-Learned:	The Switch will auto detect the prescence of a multicast router and forward IGMP pacets accordingly.
Dynamic Port List:	Displays router ports that have been dynamically configured.
Forbidden Port List:	Designates a range of ports as being disconnected to multicast-enabled routers. Ensures that the forbidden router port will not propagate routing packets out.
Static Port list:	Designates a range of ports as being connected to multicast-enabled routers. Ensures that the all packets will reach the multicast-enabled router

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

MLD Snooping

Multicast Listener Discovery (MLD) Snooping operates on the IPv6 traffic level for discovering multicast listeners on a directly attached port and performs a similar function to IGMP Snooping for IPv4. MLD snooping allows the Switch to examine MLD packets and make forwarding decisions based on content. MLD Snooping limits IPv6 multicast traffic by dynamically configuring the Switch port so that multicast traffic is forwarded only to those ports that wish to receive it. This reduces the flooding of IPv6 multicast packets in the specified VLANs. Both IGMP and MLD Snooping can be active at the same time.



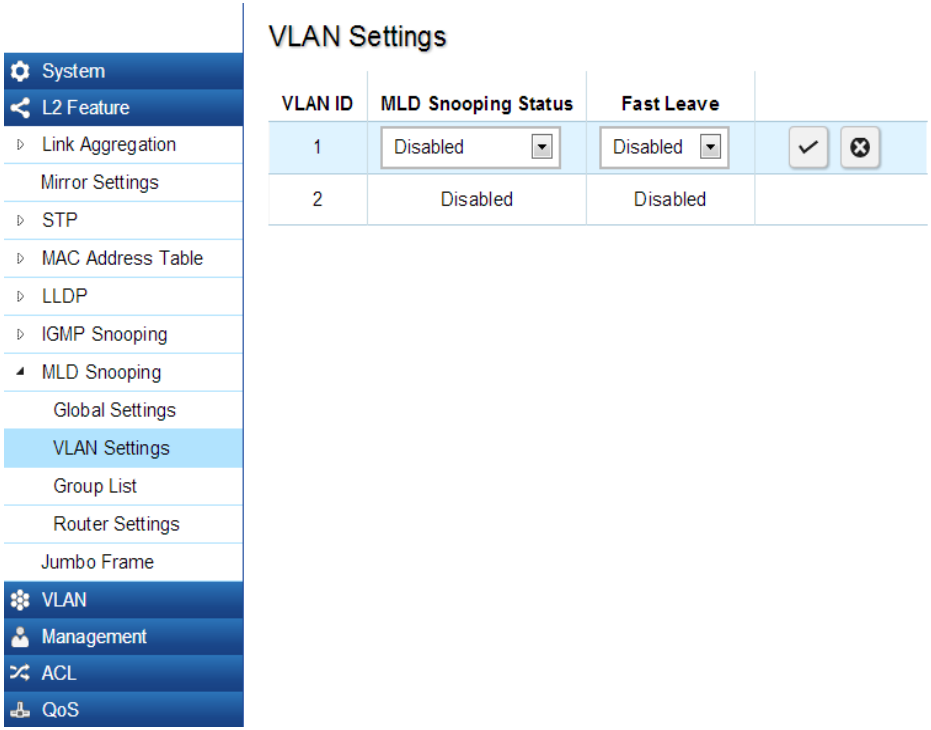
Global Settings

MLD Snooping Status:	Select to **Enable** or **Disable** MLD Snooping on the Switch. The Switch snoops all MLD packets it receives to determine which segments should receive packets directed to the group address when enabled.
MLD Snooping Version:	Select the MLD version you wish to use. If an MLD packet received by the interface has a version higher than the specified version, this packet will be dropped.
MLD Snooping Report Suppression:	The report suppression feature limits the amount of membership reports the member sends to multicast capable routers.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

VLAN Settings

If the Fast Leave feature is not used, a multicast querier will send a GS-query message when an MLD group leave message is received. The querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period. If Fast Leave is enabled, the Switch assumes that only one host is connected to the port. Therefore, Fast Leave should only be enabled on a port if it is connected to only one MLD-enabled device.



Fast Leave can improve bandwidth usage for a network which frequently experiences many MLD host add and leave requests.

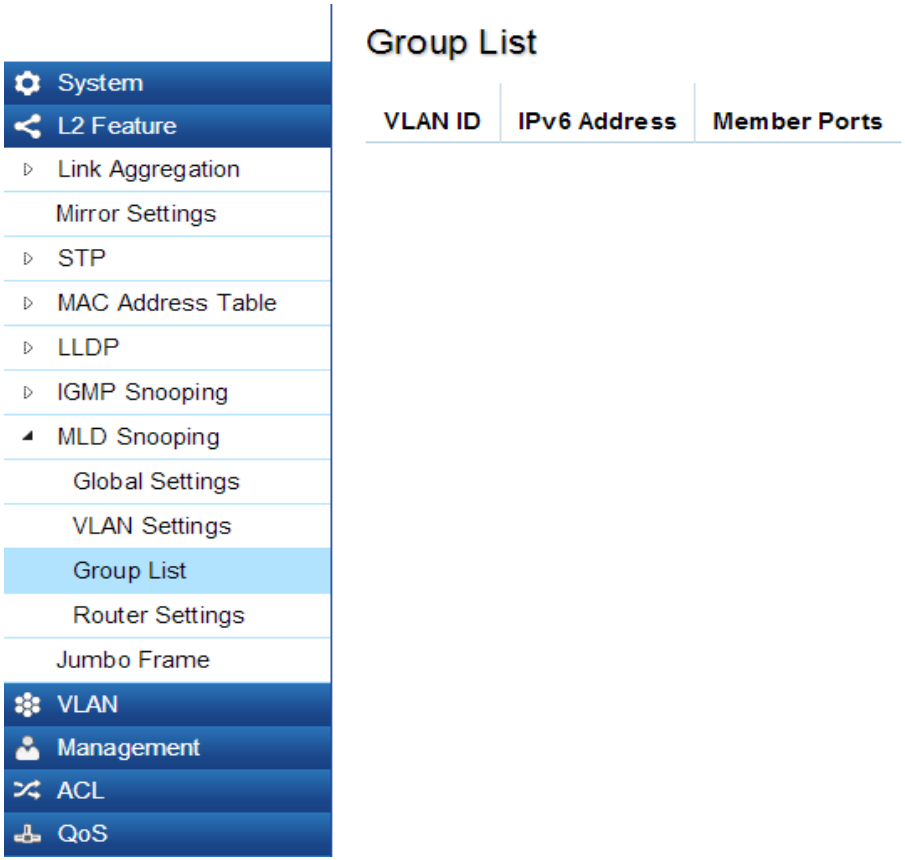
VLAN ID:	Displays the VLAN ID.
MLD Snooping Status:	Select to **Enable** or **Disable** the MLD snooping feature for the specified VLAN ID.
Fast Leave:	**Enables** or **Disables** the MLD snooping Fast Leave for the specified VLAN ID. Enabling this feature allows the Switch to immediately remove the Layer 2 LAN port from its forwarding table entry upon receiving an MLD leave message without first sending out MAC-based general queries to the port.

Select from the drop-down list whether to **Enable** or **Disable** MLD Snooping. Next, select to **Enable** or **Disable** Fast Leave for the specified VLAN ID.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

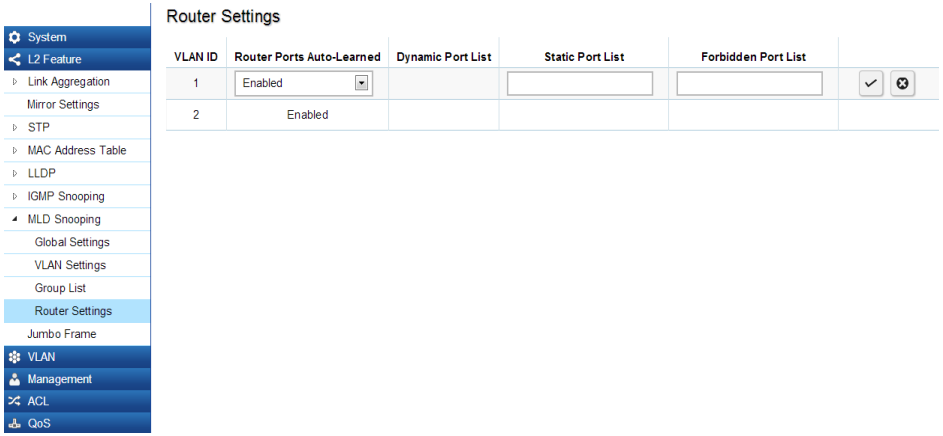
Group List

The Group List displays VLAN ID, IPv6 Address, and Members Port in the MLD Snooping List.



Router Settings

The Router Settings feature shows the learned multicast router attached port if the port is active and a member of the VLAN. Select the VLAN ID you would like to configure and enter the Static and Forbidden ports for the specified VLAN IDs that are utilizing MLD Snooping. All MLD packets snooped by the Switch will be forwarded to the multicast router reachable from the port.



VLAN ID:	Displays the VLAN ID.
Router Ports Au-to-Learned:	The Switch will automatically detect the presence of a multicast router and forward MLD packets accordingly.
Dynamic Port List:	Displays router ports that have been dynamically configured.
Forbidden Port List:	Designates a range of ports as being dis-connected to multicast-enabled routers. Ensure that the forbidden router port will not propagate routing packets out.
Static Port List:	Designates a range of ports as being connected to multicast-enabled routers. Ensure that the all packets will reach the multicast-enabled router.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

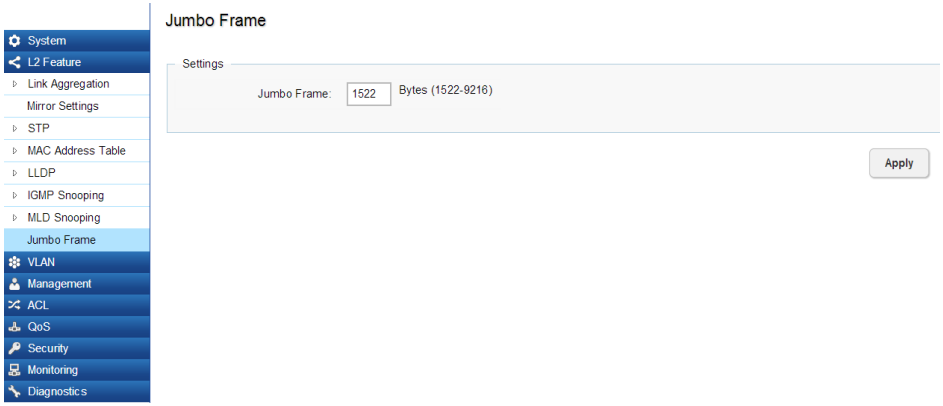
Jumbo Frame

Ethernet has used the 1500 byte frame size since its inception. Jumbo frames are network-layer PDUs that have a size much larger than the typical 1500 byte Ethernet Maximum Transmission Unit (MTU) size. Jumbo frames extend Ethernet to 9000 bytes, making them large enough to carry an 8 KB application datagram plus packet header overhead. If you intend to leave the local area network at high speeds, the dynamics of TCP will require you to use large frame sizes.

The EnGenius Layer 2 Switch supports a Jumbo Frame size of up to 9216 bytes. Jumbo frames need to be configured to work on the ingress and egress port of each device along the end-to-end transmission path. Furthermore, all devices in the network must also be consistent on the maximum Jumbo Frame size, so it is important to do a thorough investigation of all your devices in the communication paths to validate their settings.

Jumbo Frame:	Enter the size of jumbo frame. The range is from 1522-9216 bytes.

Enter the size of jumbo frame. The range is from 1522-9216 bytes. Click **APPLY** to update the the system settings.

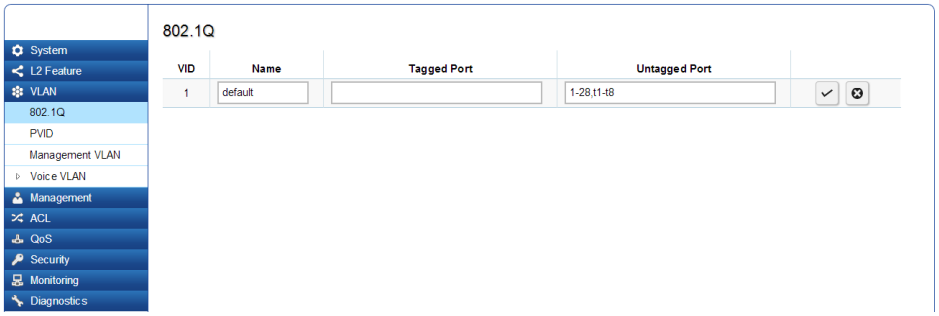


VLAN

A Virtual LAN (VLAN) is a group of ports that form a logical Ethernet segment on a Layer 2 Switch which provides better administration, security, and management of multicast traffic. A VLAN is a network topology configured according to a logical scheme rather than a physical layout. When you use a VLAN, users can be grouped by logical function instead of physical location. All ports that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. VLANs let you logically segment your network into different broadcast domains so that you can group ports with related functions into their own separate, logical LAN segments on the same Switch. This allows broadcast packets to be forwarded only between ports within the VLAN which can avoid broadcast packets being sent to all the ports on a single Switch. A VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. VLANs also improve security by limiting traffic to specific broadcast domains.

802.1Q

Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. The IEEE802.1Q specification establishes a standard method for tagging Ethernet frames with VLAN membership information. The key for IEEE802.1Q to perform its functions is in its tags. 802.1Q-compliant Switch ports can be configured to transmit tagged or untagged frames. A tag field containing VLAN information can be inserted into an Ethernet frame. When using 802.1Q VLAN configuration, you configure ports to be a part of a VLAN group. When a port receives data tagged for a VLAN group, the data is discarded unless the port is a member of the VLAN group.



Enabled:	Enables 802.1Q VLANs. This feature is enabled by default.
VID:	Displays the VLAN ID for which the network policy is defined. The range of the VLAN ID is from 1-494.
Name:	Enter the VLAN name. You can use up to 32 alphanumeric characters.
Tagged Port:	Frames transmitted from this port are tagged with the VLAN ID.
Untagged Port:	Frames transmitted from this port are untagged.

Important: Port-based VLAN and 802.1Q VLAN are mutually exclusive. If you enable port-based VLAN, then 802.1Q VLAN is disabled.

Note: The Switch's default setting is to assign all ports to a single 802.1Q VLAN(VID 1). Please keep this in mind when configuring the VLAN settings for the Switch.

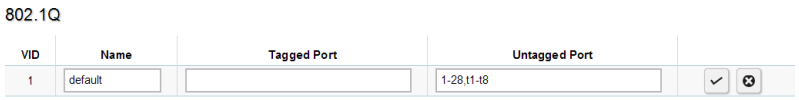
Adding, Editing, and Deleting Items in the List

To add an item to the 802.1Q list, follow these steps:

1. Click the **Add** button 

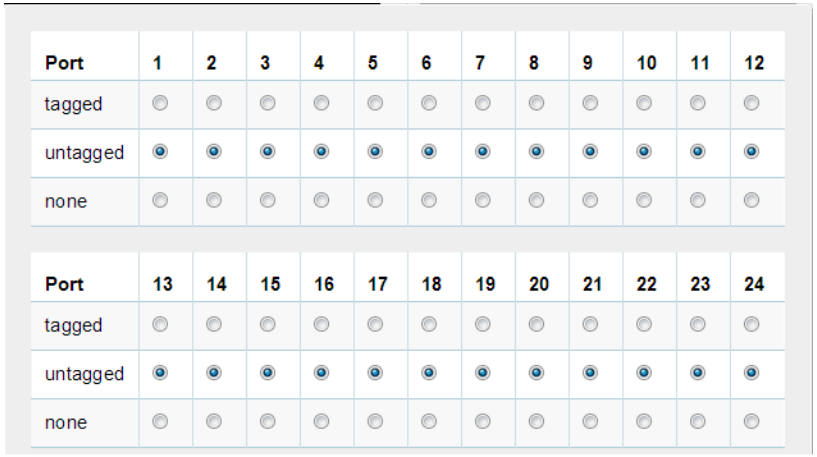
.

2. Enter the VID and name in the the **VID** and **Name** text boxes.



3. Click the **Tagged Ports** text box to show the tagged ports dialog box.

4. Click a radio button in the tagged ports row to select a port.



5. Click the Untagged Ports text box to show the untagged ports dialog box.

6. Click a radio button in the **Untagged Ports** row to select a port.

7. Click **Confirm** to accept the changes or **Cancel** to discard them.

To delete an item in the 802.1Q list, follow these steps:

1. Click the **Delete** button  in the row you want to remove an item from. A confirmation dialog will display.

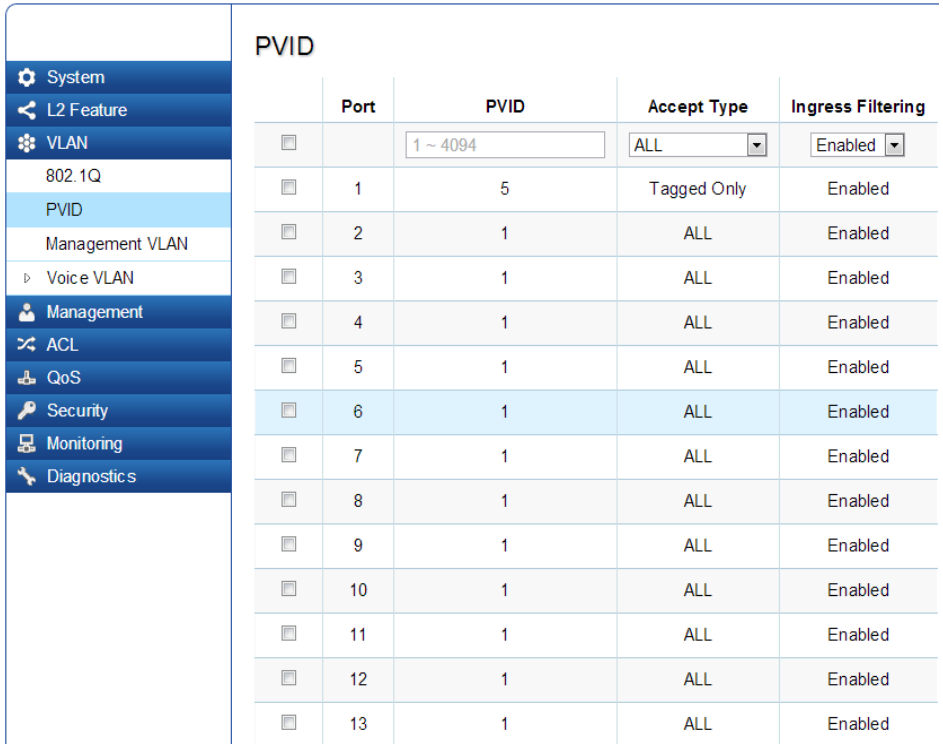
2. Click **OK** to continue or **Cancel** to abort the changes.

PVID

When an Untagged packet enters a Switch port, the PVID (Port VLAN ID) will be attached to the untagged packet and forward frames to a VLAN specified VID part of the PVID. A packet received on a given port would be assigned that port's PVID and then be forwarded to the port that corresponded to the packet's destination address. If the PVID of the port that received the packet is different from the PVID of the port that is to transmit the packet, the Switch will drop the packet. Within the Switch, different PVIDs mean different VLANs, so VLAN identification based upon the PVIDs cannot create VLANs that extend outside a given Switch. If no VLANs are defined on the Switch, all ports are then assigned to a default VLAN with a PVID equal to 1.

Note: To enable PVID functionality, the following requirements must be met:

- All ports must have a defined PVID.
- If no other value is specified, the default VLAN PVID is used.
- If you wish to change the port's default PVID, you must first create a VLAN that includes the port as a member.

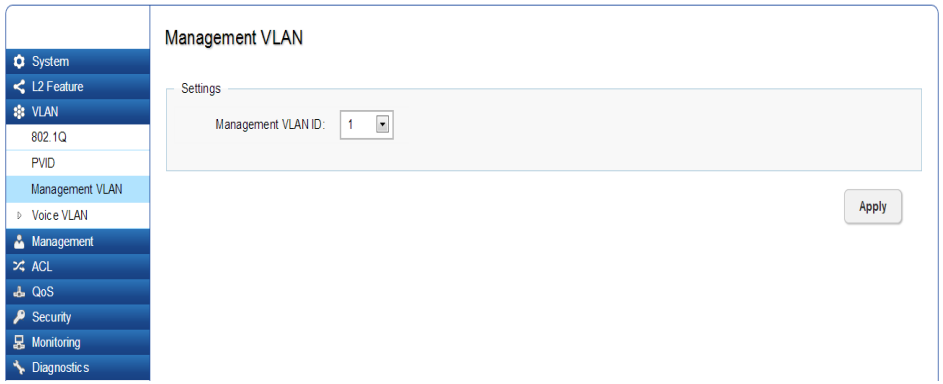


Port:	Displays the VLAN ID to which the PVID tag is assigned. Configure the PVID to assign untagged or tagged frames received on the selected port.
PVID:	Enter the PVID value. The range is from 1-4094.
Accept Type:	Select **Tagged Only** and **Untagged Only** from the list. • **Tagged Only:** The port discards any untagged frames it's receives. The port only accepts tagged frames. • **Untagged Only:** Only untagged frames received on the port are accepted. • **All**: The port accepts both tagged and untagged frames.
Ingress Filtering:	Specify how you wish the port to handle tagged frames. Select **Enabled** or **Disabled** from the list. • **Enabled:** tagged frames are discarded if VID does not match the PVID of the port. • **Disabled:** All frames are forwarded in accordance with the IEEE 802.1Q VLAN.

Click **APPLY** to update the the system settings.

Management VLAN

The Management VLAN allows users to transfer the authority of the Switch from the default VLAN to other VLAN IDs. By default, the active management VLAN ID is 1, which allows an IP connection to be established through any port. When the management VLAN is set to a different VLAN, connectivity through the existing management VLAN is lost and an IP connection can be made only through a port that is part of the management VLAN. It is also mandatory that the port VLAN ID (PVID) of the port to be connected in that management VLAN be the same as the management VLAN ID.



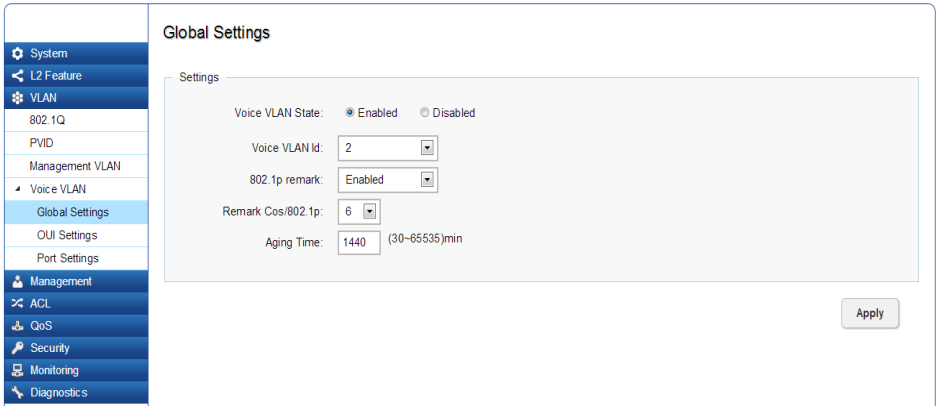
Management VLAN ID:	Select the VLAN ID for allows user to transfer the authority of the Switch.

Apply: Click **Apply** to update the system settings.

Voice VLAN

Enhance your Voice over IP (VoIP) service by configuring ports to carry IP voice traffic from IP phones on a specific VLAN. Voice VLAN provides QoS to VoIP, ensuring that the quality of the call does not deteriorate if the IP traffic is received erratically or unevenly.

Global Settings

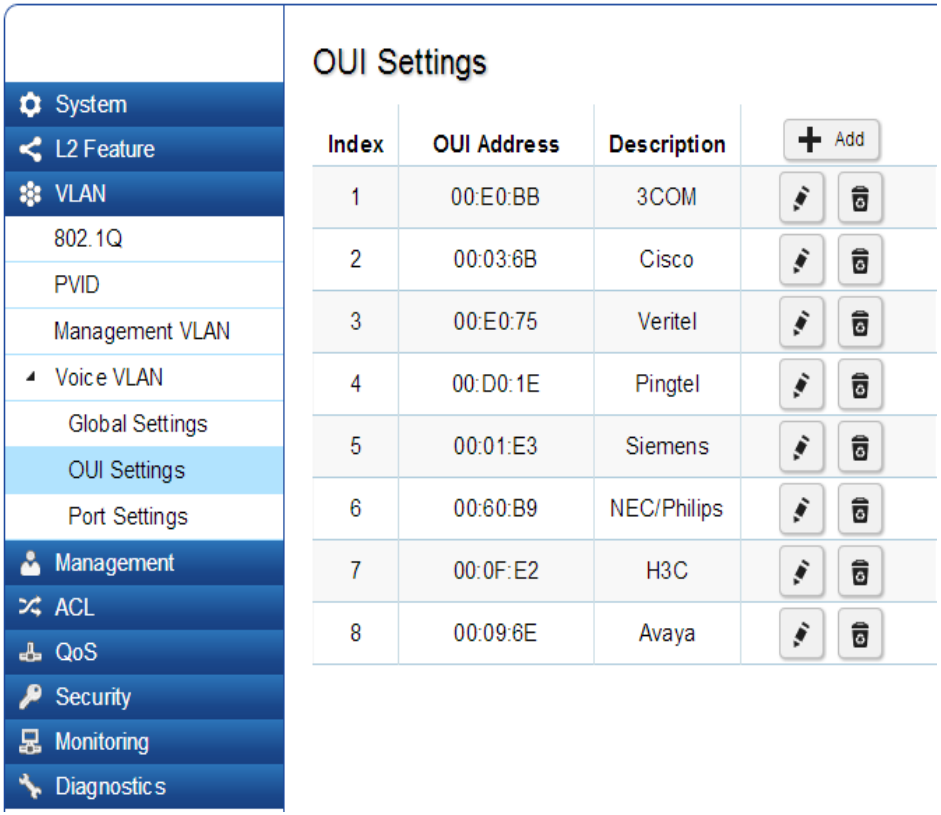


Apply: Click **Apply** to update the system settings.

Voice VLAN State:	Select **Enabled** or **Disabled** for Voice VLAN on the Switch.
Voice VLAN ID:	Sets the Voice VLAN ID for the network. Only one Voice VLAN is supported on the Switch.
802.1p Remark:	Enable this function to have outgoing voice traffic to be marked with the selected CoS value.
Remark CoS/802.1p:	Defines a service priority for traffic on the Voice VLAN. The priority of any received VoIP packet is overwritten with the new priority when the Voice VLAN feature is active on a port. (Range: 0-7; Default: 6)
Aging Time:	The aging time is used to remove a port from voice VLAN if the port is an automatic VLAN member. When the last voice device stops sending traffic and the MAC address of this voice device is aged out, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after expiration of the voice VLAN aging timer. If the voice traffic resumes during the aging time, the aging timer will be reset and stop. The range for aging time is from 1 - 65535 minutes. The default is 1440 minutes.

OUI Settings

The Switches determines whether a received packet is a voice packet by checking its source MAC address. VoIP traffic has a preconfigured Organizationally Unique Identifiers (OUI) prefix in the source MAC address. You can manually add specific manufacturer's MAC addresses and description to the OUI table. All traffic received on the Voice VLAN ports from the specific IP phone with a listed OUI is forwarded on the voice VLAN.



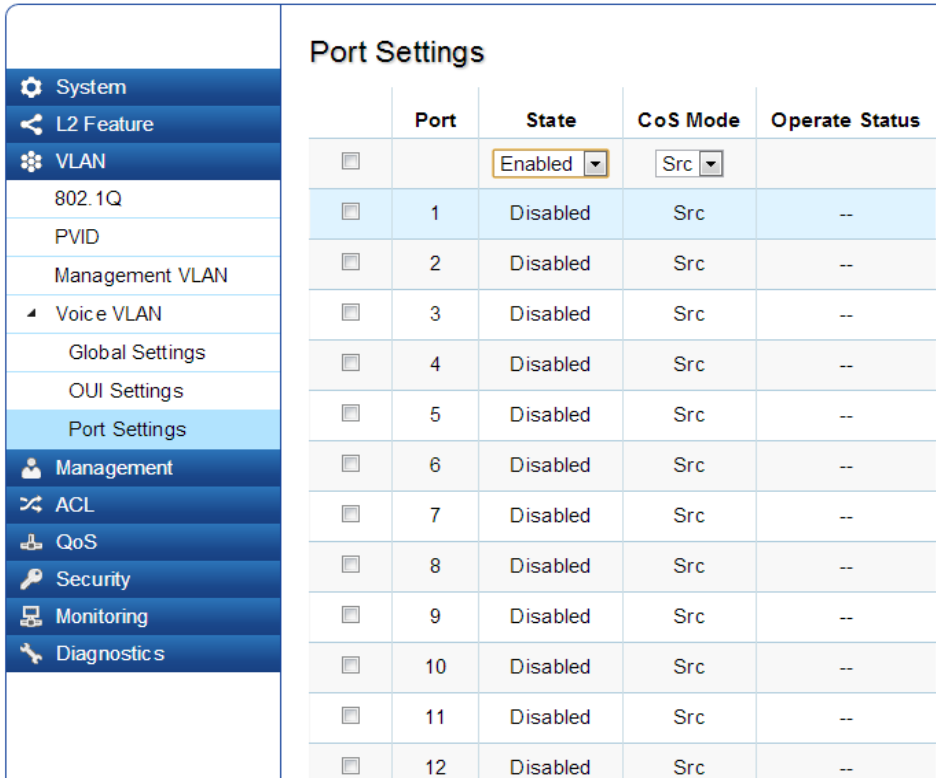
Port:	Enter the OUI to the Voice VLAN. The following OUI are enabled by default. The following OUI are enabled by default. • 00:E0:BB - Assigned to 3COM IP Phones. • 00:03:6B - Assigned to Cisco IP Phones. • 00:E0:75 - Assigned to Veritel IP Phones. • 00:D0:1E - Assigned to Pingtel IP Phones. • 00:01:E3 - Assigned to Siemens IP Phones. • 00:60:B9 - Assigned to NEC/Philips IP Phones. • 00:0F:E2 - Assigned to H3C IP Phones. • 00:09:6E - Assigned to Avaya IP Phones.
Index:	Displays the VoIP sequence ID.
OUI Address:	This is the globally unique ID assigned to a vendor by the IEEE to identify VoIP equipment.
Description:	Displays the ID of the VoIP equipment vendor.

To configure the OUI settings, click the **Edit** button to re-configure the specific entry. Click the **Delete** button to remove the specific entry and click the **Add** button to create a new OUI entry.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Port Settings

Enhance VoIP service by configuring ports to carry IP voice traffic from IP phones on a specific VLAN. Voice VLAN provides QoS to VoIP, ensuring that the quality of voice does not deteriorate if the IP traffic is received unevenly.



Port:	Displays the port to which the Voice VLAN settings are applied.
State:	Select **Enabled** to enhance VoIP quality on the selected port. The default is **Disabled**.
CoS Mode:	Select **Src** or **All** from the list.
Src:	Src QoS attributes are applied to packets with OUIs in the source MAC address.
All:	All QoS attributes are applied to packets that are classified to the Voice VLAN.
Operate Status:	Displays the operating status for the Voice VLAN on the selected port.

Apply: Click **Apply** to update the system settings.

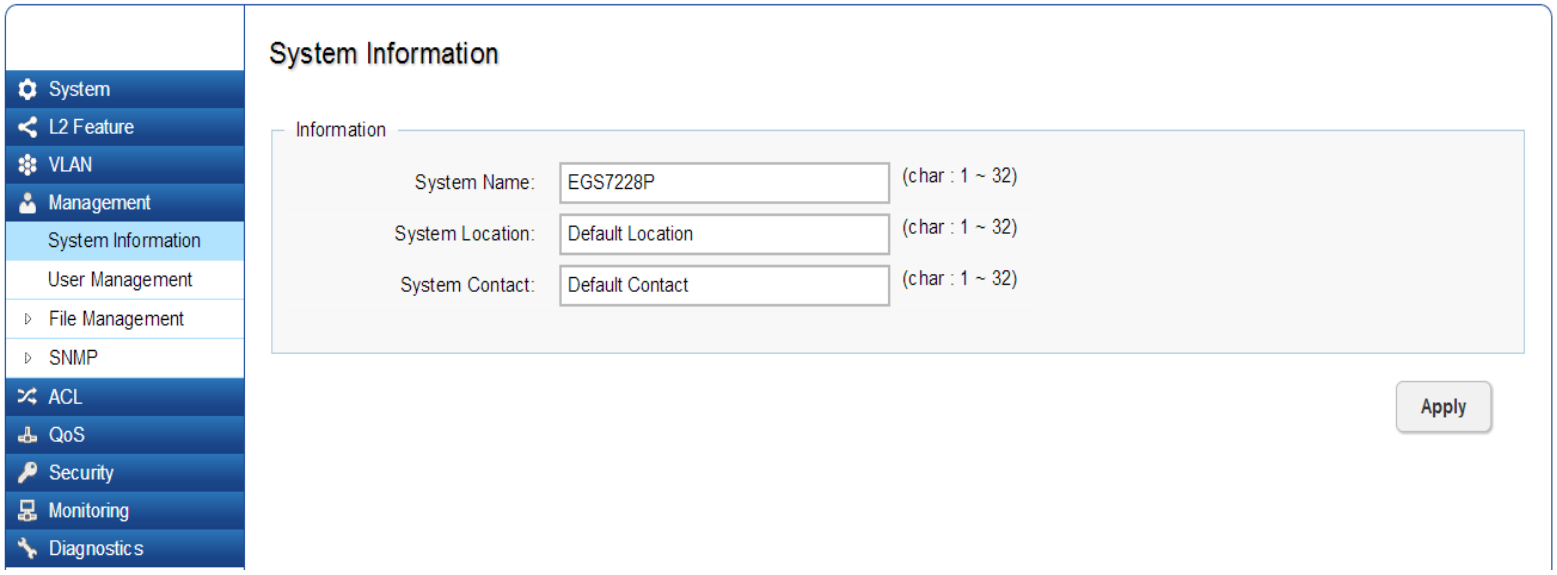
Management

System Information

The System Information screen contains general device information including the system name, system location, and system contact for the Switch.

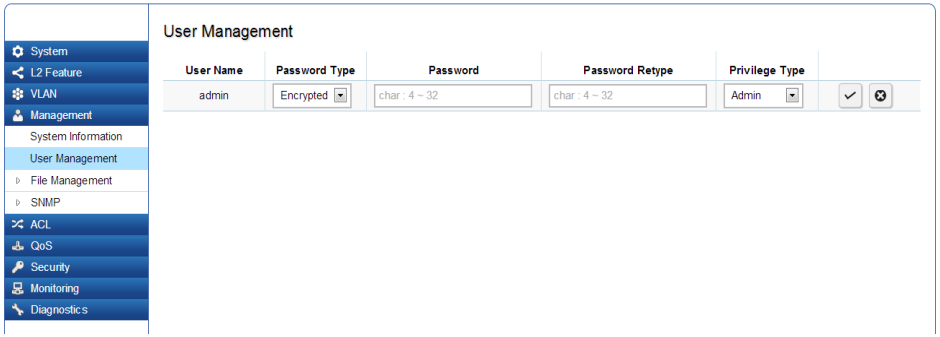
System Name:	Enter the name you wish to use to identify the Switch. You can use up to 32 alphanumeric characters. The factory default name is the name of the Swicth.
System Location:	Enter the location of the Switch. You can use up to 32 alphanumeric characters. The factory default is: **Default Location**.
System Contact:	Enter the contact person for the Switch. You can use up to 160 alphanumeric characters. The factory default is: **Default Location**.

Click **Apply** to save the changes to the system.



User Management

From here, you can add or edit user accounts for the Switch. Click the **Add** button to add an account or the **Edit** button to edit an existing account.



User Name:	Enter a username. You can use up to 18 alphanumeric characters.
Password Type:	Select **Clear Text** or **Encrypted** from the list.
Password:	Enter a new password for accessing the Switch.
Password Retype:	Repeat the new password used to access the Switch.
Privilege Type:	Select **Admin** or **User** from the list to regulate access rights.

Important: Note that Admin users have full access rights to the Switch when determining the authority of the user account.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

File Management

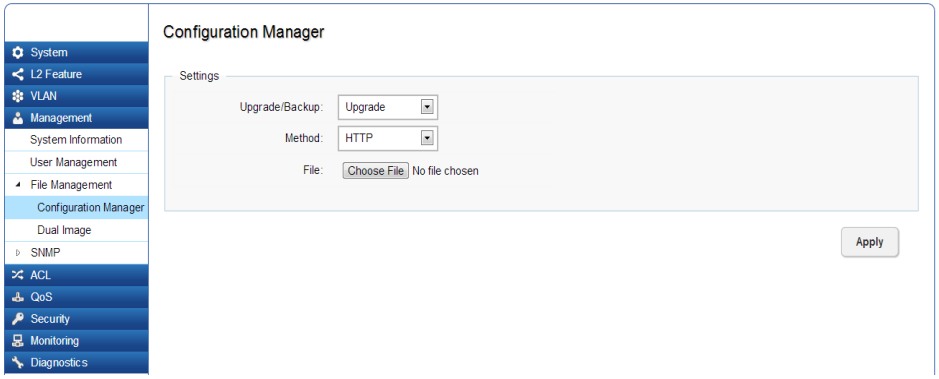
Configuration Manager

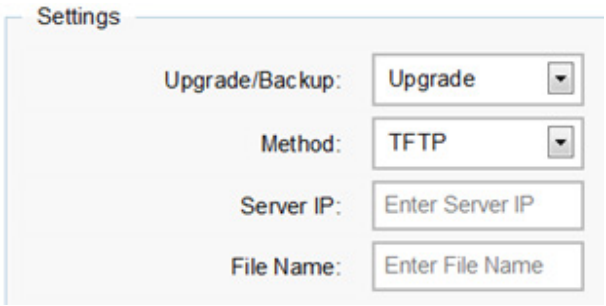
Backup

Download the configuration file from the Switch to TFTP server on the network. Next, download the configuration file from the Switch to your local drive by using an HTTP session.

Upgrade

First, upload the configuration file from a TFTP server to the Switch. Next, upload the configuration file from your local drive to the Switch by using an HTTP session.





Upgrade/Backup:	Select **Upgrade** or **Backup** from the list.
Method:	Two methods can be selected; **HTTP** or **TFTP**.
File:	Click **Browse** to select file to **Upgrade** or **Backup**.
Server IP:	Enter the Server IP address to upload the configuration file from the TFTP server to the Switch.
File Name:	Enter the destination file name to upload from the TFTP server to the Switch.

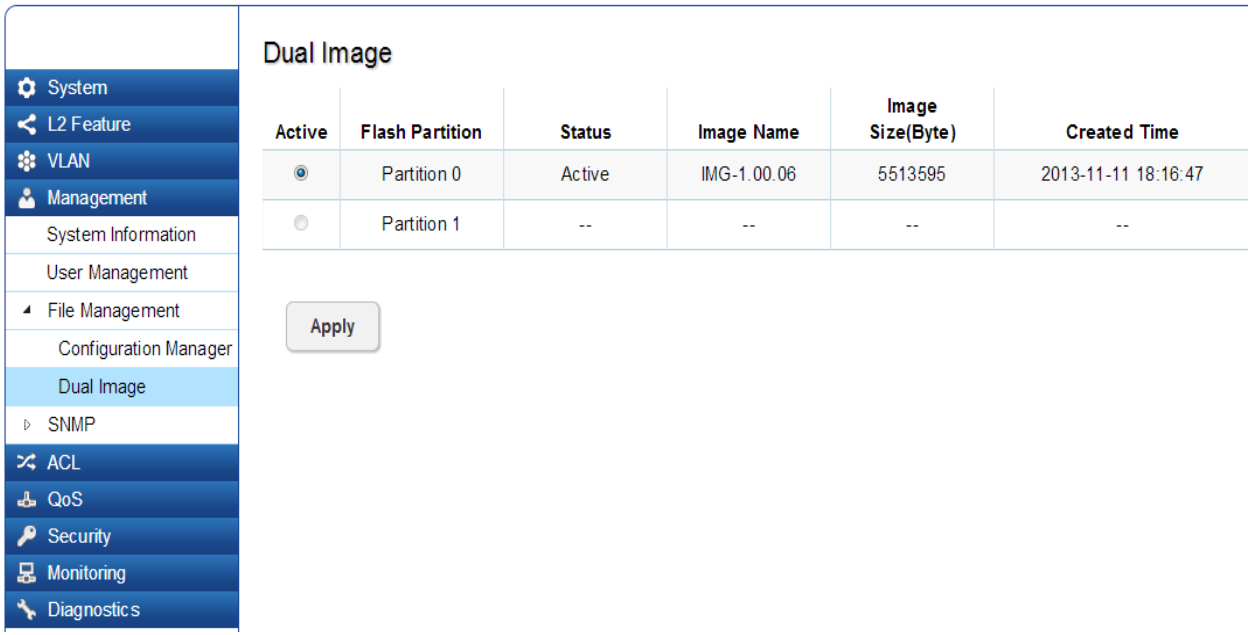
Click **Apply** to save the changes to the system.

Dual Image

The Switch maintains two versions of the Switch image in its permanent storage. One image is the active image, and the second image is the backup image. The Dual Image screen enables the user to select which partition will be set as active after the next reset. The Switch boots and runs from the active image. If the active image is corrupt, the system automatically boots from the non-active image.

Active:	Selects the partition you wish to be active.
Flash Partition:	Displays the number of the partition.
Status:	Displays the partition which is currently active on the Switch.
Image Name:	Displays the name of the image.
Image Size:	Displays the size of the image file.
Created Time:	Displays the time the image was created.

Click **Apply** to save the changes to the system.



SNMP

Simple Network Management Protocol (SNMP) is an Application Layer protocol designed specifically for managing and monitoring network devices. Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is used for collecting information from and configuring network devices such as; servers, printers, hubs, Switches, and routers on an Internet Protocol (IP) network. SNMP is used to exchange management information between a network management system (NMS) and a network device. A manager station can manage and monitor the Switch through their network via SNMPv1, v2c and v3. An SNMP managed network consists of two components; agents and a manager.

An agent translates the local management information from the managed Switch into a form that is compatible with SNMP. SNMP allows a manager and agents to communicate with each other for the purpose of accessing Management Information Bases (MIBs). SNMP uses an extensible design, where the available information is defined by MIBs. MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing Object Identifiers (OID). Each OID identifies a variable that can be read or set via SNMP. The manager is the console through which network administrators perform network management functions.

Several versions of SNMP are supported. They are v1, v2c, and v3. SNMPv1, which is defined in RFC 1157 "A Simple Network Management Protocol (SNMP)", is a standard that defines how communication occurs between SNMP-capable devices and specifies the SNMP message types. Version 1 is the simplest and most basic of versions. There may be times where it's required to support older hardware. SNMPv2c, which is defined in RFC 1901 "Introduction to Community-Based SNMPv2," RFC 1905, "Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)", and RFC 1906 "Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)". SNMPv2c updates protocol operations by introducing a GetBulk request and authentication based on community names. Version 2c adds several enhancements to the protocol, such as support for "Informs". Because of this, v2c has become the most widely used version. Unfortunately, a major weakness of v1 and v2c is security. To combat this, SNMP v3 adds a security features that overcome the weaknesses in v1 and v2c. . If possible, it is recommended that you use v3- especially if you plan to transmit sensitive information across unsecured links. However, the extra security feature makes configuration a little more complex.

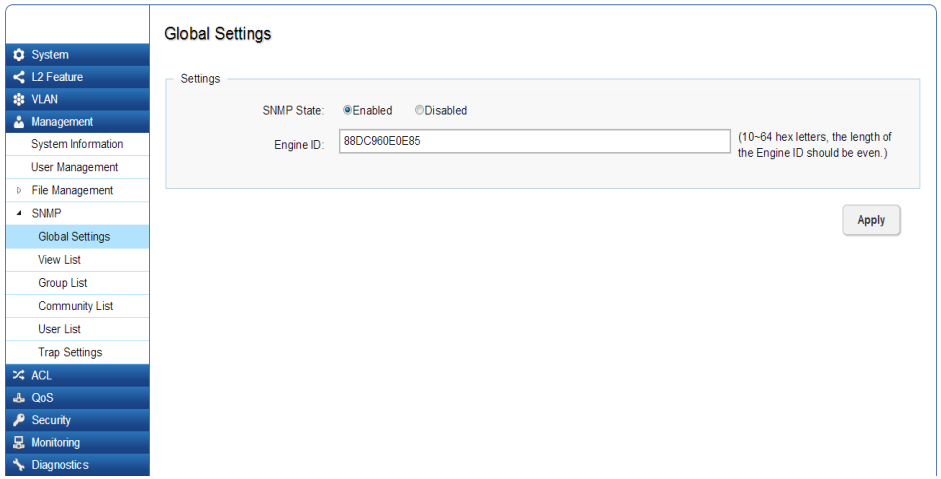
In SNMPv3, User-based Security Model (USM) authentication is implemented along with encryption, allowing you to configure a secure SNMP environment. The SNMPv3 protocol uses different terminology than SNMPv1 and SNMPv2c as well. In the SNMPv1 and SNMPv2c protocols, the terms agent and manager are used. In the SNMPv3 protocol, agents and managers are renamed to entities. With the SNMPv3 protocol, you create users and determine the protocol used for message authentication as well as if data transmitted between two SNMP entities is encrypted.

The SNMPv3 protocol supports two authentication protocols - HMAC-MD5-96 (MD5) and HMAC-SHA-96 (SHA). Both MD5 and SHA use an algorithm to generate a message digest. Each authentication protocol authenticates a user by checking the message digest. In addition, both protocols use keys to perform authentication. The keys for both protocols are generated locally using the Engine ID and the user password to provide even more security.

In SNMPv1 and SNMPv2c, user authentication is accomplished using types of passwords called Community Strings, which are transmitted in clear text and not supported by authentication. Users can assign views to Community Strings that specify which MIB objects can be accessed by a remote SNMP manager.
The default Community Strings for the Switch used for SNMPv1 and SNMPv2c management access for the Switch are public, which allows authorized management stations to retrieve MIB objects, and private, which allow authorized management stations to retrieve and modify MIB objects.

Global Settings

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) protocol designed specifically for managing and monitoring network devices. The SNMP agents maintain a list of variables that are used to manage the device. The variables are defined in the Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent.

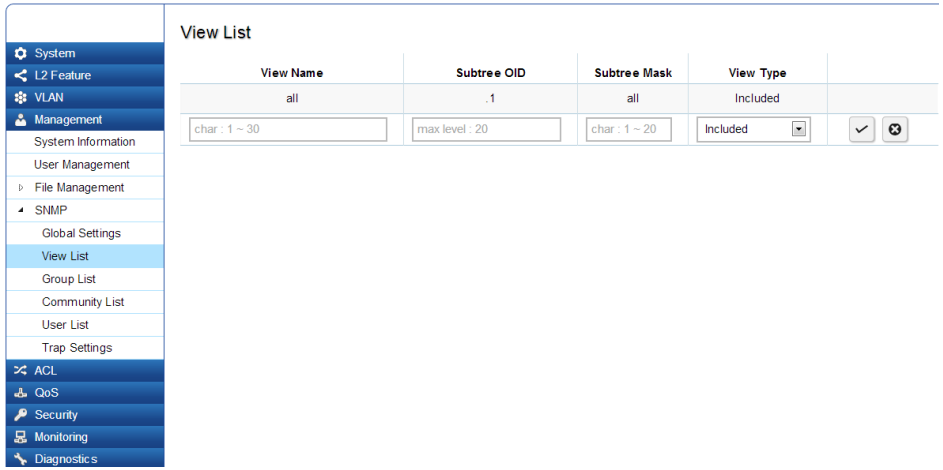


SNMP State:	The default SNMP global state is **Enabled**.
Local Engine ID (10-64 Characters):	Enter the local device Engine ID. The field value is a hexadecimal string.

Click **Apply** to save the changes to the system.

View List

The Switch supports SNMP notification filters based on Object IDs (OIDs). OIDs are used by the system to manage device features. This feature's access is granted via the MIB name or MIB Object ID.

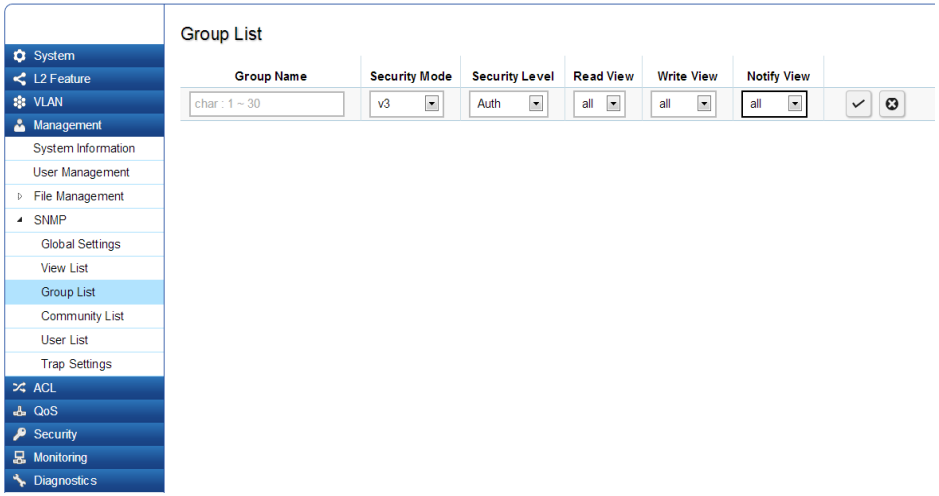


View Name:	Enter the view name. The view name can contain up to 30 alphanumeric characters.
Subtree OID:	Enter the Object Identifier (OID) Subtree for the view. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.
Subtree Mask:	Select 0 or 1 for Subtree mask. The mask of the Subtree OID 1 means this object number "is concerned", amd 0 means "do not concern".
View Type:	Select whether the defined OID branch will be included or excluded from the selected SNMP view.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Group List

Groups allow IT managers to assign access rights to specific device features.

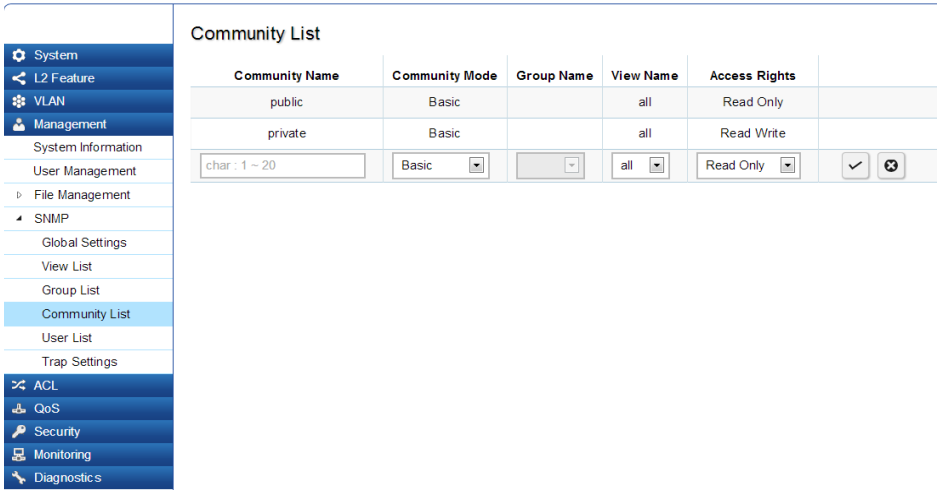


Group Name:	Enter the group name that access control rules are applied to. The group name can contain up to 30 alphanumeric characters.
Security Mode:	Selects the SNMP version (v1, v2c, v3) associated with the group.
Security Level:	Select the security level attached to the group. Security levels apply to SNMPv3 only. • **No Auth** - No authentication is assigned to the group. • **Auth** - Authenticates SNMP messages. • **Priv** - Encrypts SNMP messages.
Read View:	Management access is restricted to read-on-only.
Write View:	Select the group access right. Management access is read-write.
Notify View:	Select the group access rights. This will send traps for the assigned SNMP view.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Community List

Access rights are managed by defining communities. Click Add to add a community list to the Switch. Next, name the community and choose the level of access that will be granted to the specified list from the drop-down boxes.

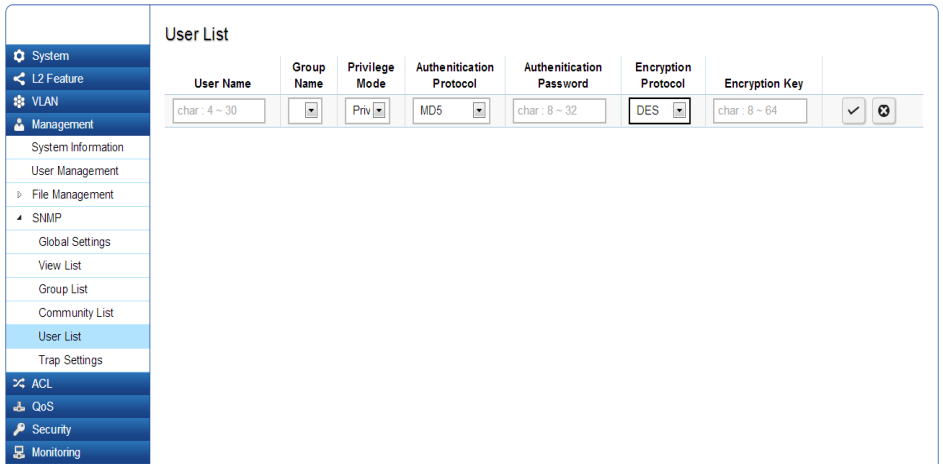


Community Name:	Enter the name of SNMP community string.
Community Mode:	Selected **Basic** or **Advance** from the list. Select the Advance attached to the SNMP group.
Group Name:	Select the SNMP group from a list.
View Name:	Select the view name from a list.
Access Rights:	Specify the level of permission for the MIB objects accessible to the SNMP. Your choices are **Read/write** or **Read-only**.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

User List

From here, you can configure the details pertaining to specific user accounts. Click **Add** to add a new user.



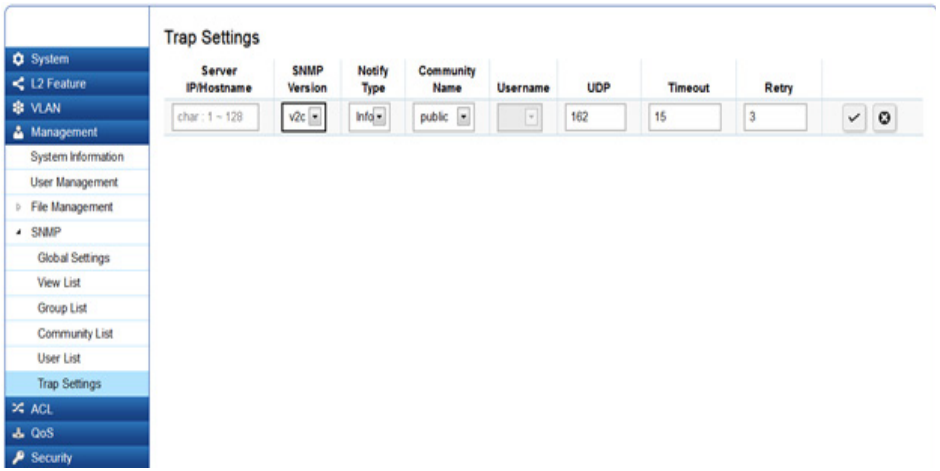
Privilege Mode:	Select **No Auth**, **Auth**, or **Priv** security level from the list. • **No auth -** No authentication are assigned to the group. • **Auth -** Authenticates SNMP messages. • **Priv -** Encrypts SNMP messages.
Authentication Protocol:	Select the method used to authenticate users. • **MD5 -** Using the HMAC-MD5 algorithm. • **SHA -** Using the HMAC-SHA-96 authentication level. Enter the SHA password and the HMAC-SHA-96 password to be used for authentication.
Authentication Password:	Enter MD5 password and the HMAC-MD5-96 password to be used for authentication.
Encryption Protocol:	Select the method used to authenticate users. • **None -** No user authentication is used. • **DES -**Using the Data Encryption Standard algorithm.
Encryption Key:	Enter the Data Encryption Standard key.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Trap Settings

SNMP Traps

A trap is a type of SNMP message. The Switch can send traps to an SNMP manager when an event occurs.
You can restrict user privileges by specifying which portions of the MIBs that a user can view. In this way, you restrict which MIBs a user can display and modify. In addition, you can restrict the types of traps the user can send. You can do this by determining where messages are sent and what types of messages can be sent per user.



Server IP/Hostname:	Enter the Server IP or Hostname. The Hostname can contain up to 128 alpha-numeric characters.
SNMP Version:	Select the SNMP version from the list.
Notify Type:	Select the type of notification to be sent. • **Traps -** Traps are sent. • **Informs -** Informs are sent **ONLY** when v2c is enabled.
Community Name:	Select the Community Name from the list.
UDP:	Enter the UDP port used to send notifications.
Timeout:	Configurable only if the notify type is I**nforms**. Enter the amount of time the device waits before re-sending. The default is 15 seconds.
Retry:	Configurable only if the notify type is **Informs**. Enter the amount of time the device waits before re-sending an inform request. The default is 3 seconds.

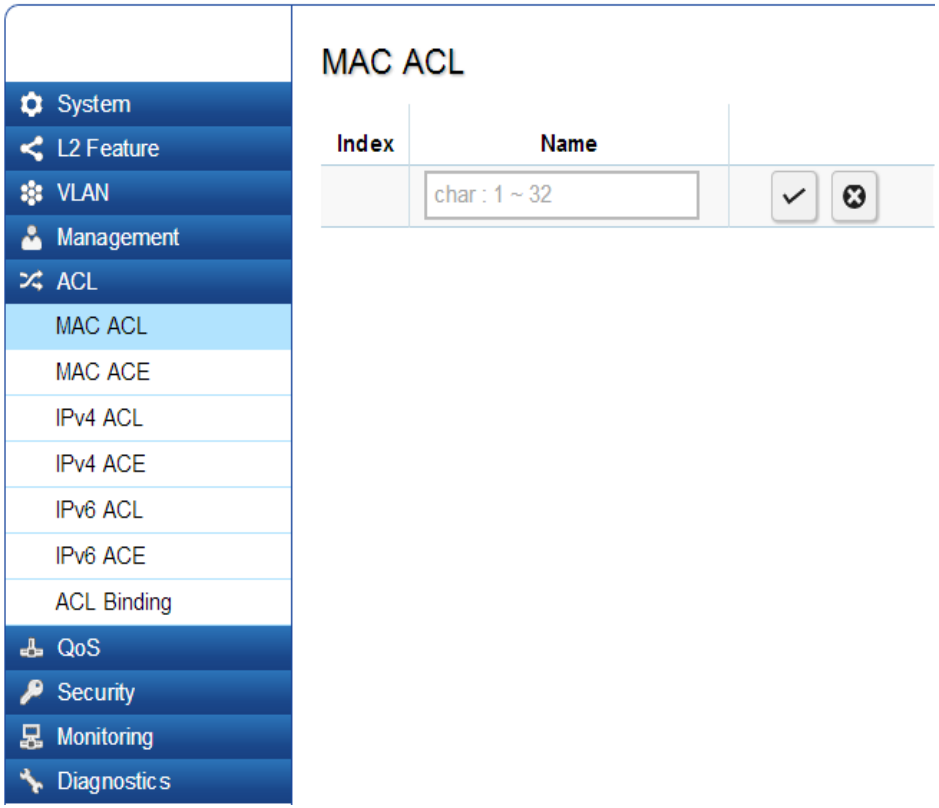
Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

ACL

Access Control List (ACL) allows you to define classifi¬cation rules or establish criteria to provide security to your network by blocking unauthorized users and allowing authorized us¬ers to access specific areas or resources. ACLs can provide basic security for access to the network by controling whether packets are forwarded or blocked at the Switch ports. Access Control Lists (ACLs) are filters that allow you to classify data packets according to a particular content in the packet header, such as the source address, destination address, source port number, destination port number, and more. Packet classifiers identify flows for more efficient processing. Each filter defines the conditions that must match for inclusion in the filter. ACLs are used to provide traffic flow control, restrict contents of routing updates, and determine which types of traffic are forwarded or blocked. This criterion can be specified on a basis of the MAC address or IP address.

MAC ACL

Allows an MAC Based Access Control Lists (ACLs) to be defined. Enter the name of the MAC based ACL name in the index box. You can type up to 32 alphanumeric characters.

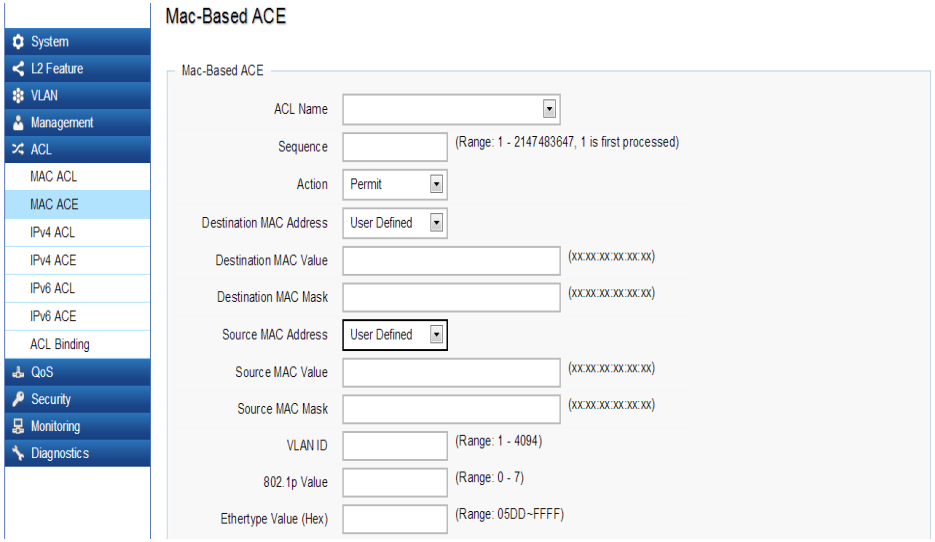


Index:	Displays the current number of ACLs.
Name:	Enter the MAC based ACL name. You can use up to 32 alphanumeric characters.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Mac-Based ACE

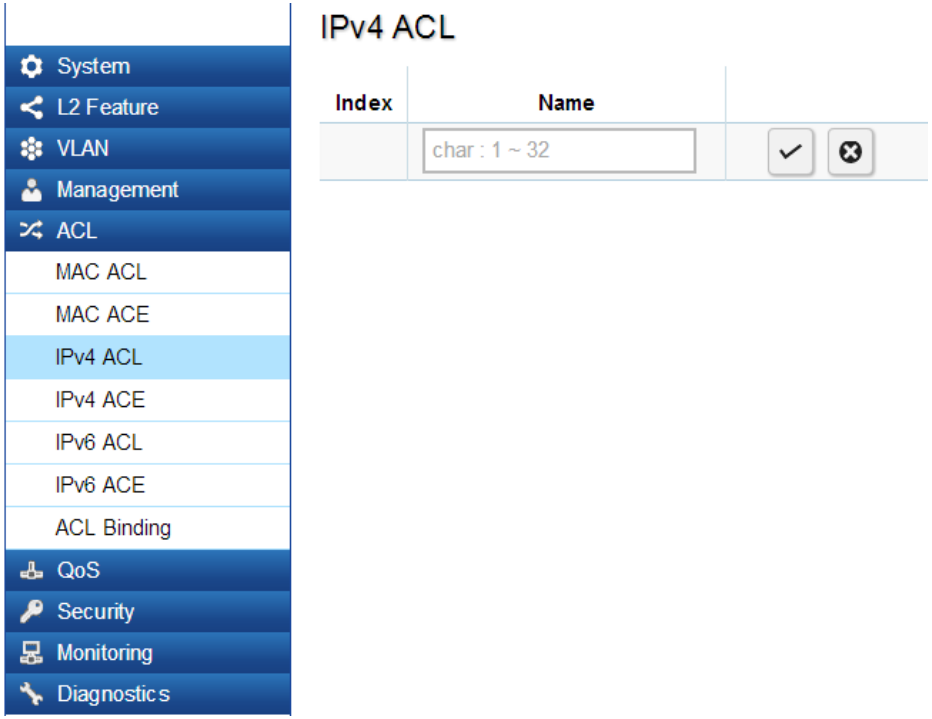
Allows Mac-Based Access Control Entry (ACE) to be defined within a configured ACL.



ACL Name:	Select the ACL from the list.
Sequence:	Enter the sequence number which signifies the order of the specified ACL relative to other ACLs assigned to the selected interface. The valid range is from 1-2147483646, 1 being processed first.
Action:	Select what action taken if a packet matches the criteria. • **Permit** - Forward packets that meet the ACL criteria. • **Deny**- Drops packets that meet the ACL criteria.
Destination MAC Value:	Enter the destination MAC address.
Destination MAC Wildcard Mask:	Enter the mask of the new source MAC address.
Source MAC Value:	Enter the source MAC address.
Source MAC Wildcard Mask:	Enter the mask of the new source MAC address.
VLAN ID:	Enter the VLAN ID to which the MAC address is attached in MAC ACE. The range is from 1-4094.
802.1p Value:	Enter the 802.1p value. The range is from 0-7.
Ethertype Value:	Enter the Ethertype value. The range is from 05DD-FFFF.

IPv4 ACL

Allows the IP Based ACL to be defined.

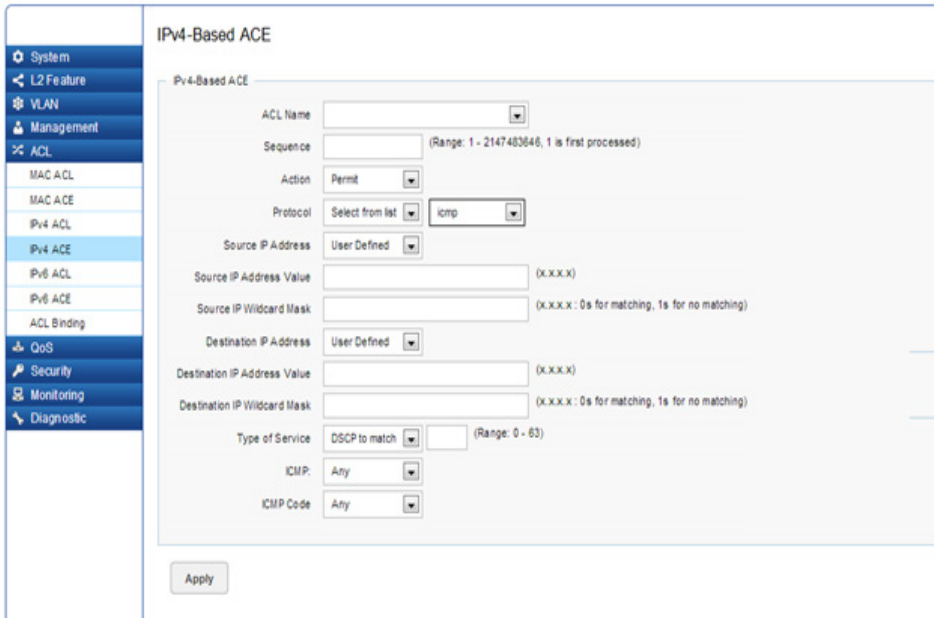


Index:	Displays the current number of ACLs.
Name:	Enter the IP based ACL name. You can use up to 32 alphanumeric characters.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

IPv4-Based ACE

Allows IP Based Access Control Entry (ACE) to be defined within a configured ACL.



ACL Name:	Select the ACL from the list.
Sequence:	Enter the sequence number which signifies the order of the specified ACL relative to other ACLs assigned to the selected interface. The valid range is from 1-2147483646, 1 being processed first.
Action:	Select what action to take if a packet matches the criteria. • **Permit** – Forwards packets that meet the ACL criteria. • **Deny**– Drops packets that meet the ACL criteria.
Protocol:	Select **Any**, **Protocol ID,** or **Select from a List** in the drop down menu. • **Protocol ID** – Enter the protocol in the ACE to which the packet is matched. • **Select from List**–Selects the protocol from the list in the provided field.
Destination IP Address Value:	Enter the destination IP address.
Destination IP Wildcard Mask:	Enter the mask of the new source IP address.
Source IP Address Value:	Enter the source IP address.

Source IP Wildcard Mask:	Enter the mask of the new source IP address.
VLAN ID:	Enter the VLAN ID to which the IP address is attached in IPv4-Based ACE. The range is from 1-4094.
802.1p Value:	Enter the 802.1p value. The range is from 0-7.
Ethertype Value:	Enter the Ethertype value. The range is from 05DD-FFFF.
ICMP:	Select **Any**, **Protocol ID**, or **Select from the List** in drop down menu. • **Protocol ID** – Enter the protocol in the ACE to which the packet is matched. The range is from 0-255. • **Select from List**– Select the ICMP from the list in the provided field.
ICMP Code:	Enter the ICMP code. The range is from 0-255.
Source Port:	Select **Single** or **Range** from the list. Enter the source port that is matched to the packets. The range is from 0-65535.
Destination Port:	Select **Single** or **Range** from the list.Enter the destination port that is matched to the packets. The range is from 0-65535.
Type of Service:	Enter the DSCP. The range is from 0-63.

Click **Apply** to save the changes to the system.

IPv6 ACL

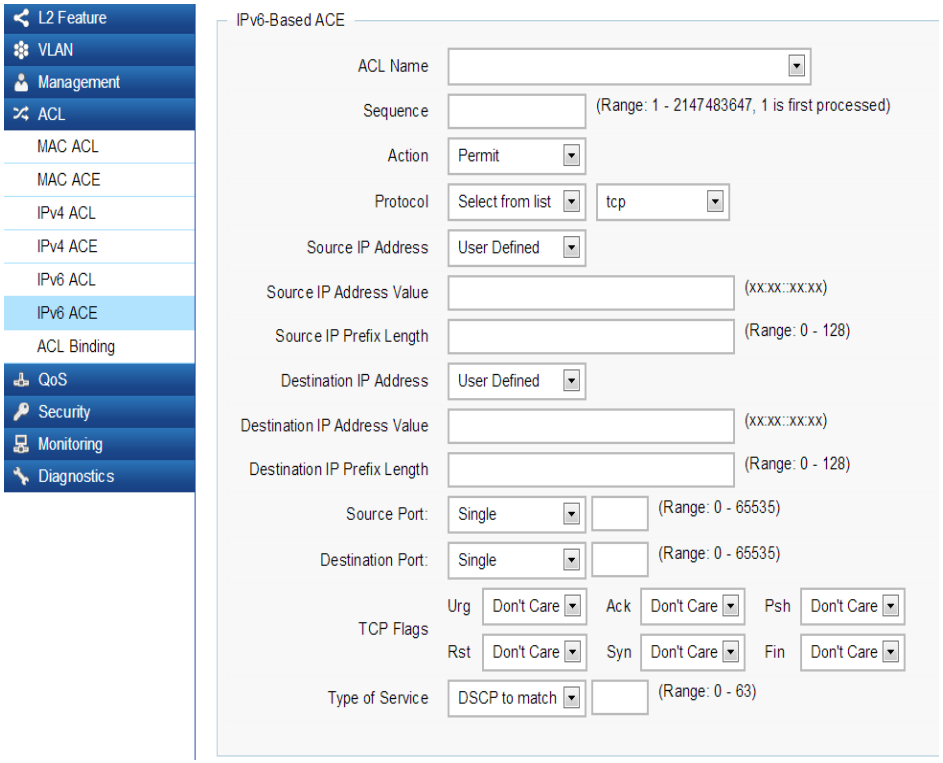
Allows an IPv6 Based ACL to be defined.

Index:	Displays the current number of ACLs.
Name:	Enter the IPv6 based ACL name. You can use up to 32 alphanumeric characters.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

IPv6 Based ACE

Allows IPv6 Based Access Control Entry (ACE) to be defined within a configured ACL.



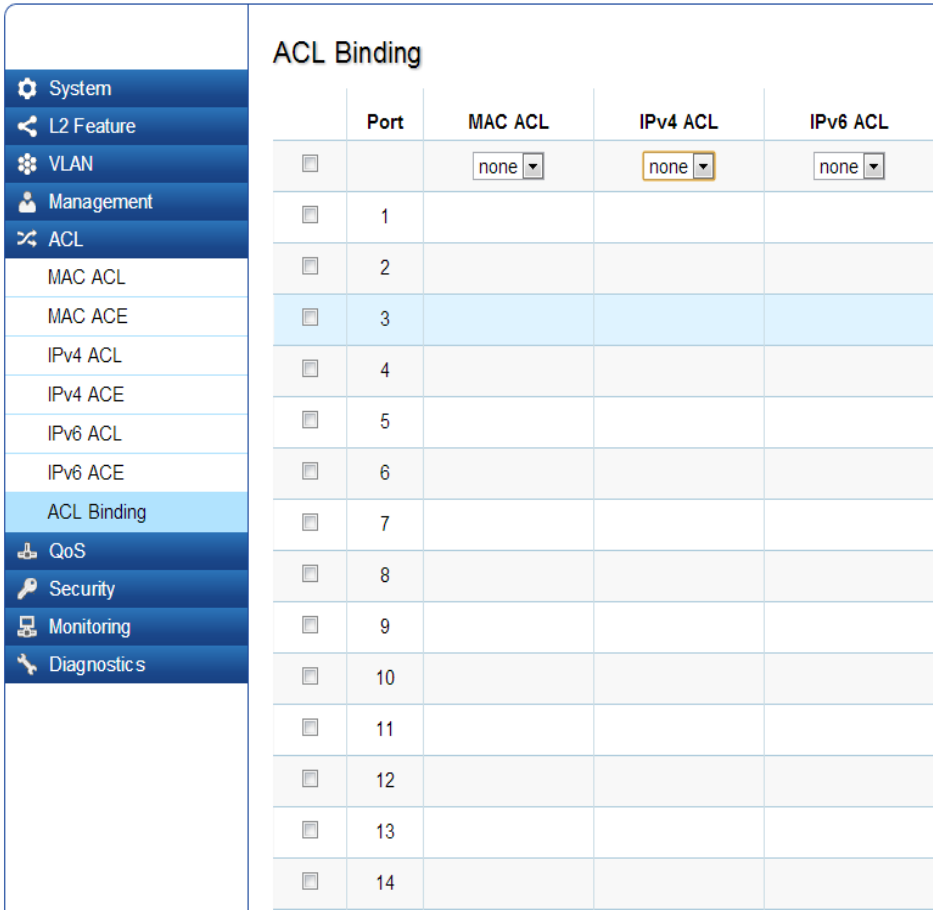
ACL Name:	Select the ACL from the list.
Sequence:	Enter the sequence number which signifies the order of the specified ACL relative to other ACLs assigned to the selected interface. The valid range is from 1-2147483646, 1 being processed first.
Action:	Select what action taken if a packet matches the criteria. • **Permit** – Forward packets that meet the ACL criteria. • **Deny**– Drops packets that meet the ACL criteria.
Protocol:	Select the **Any**, **Protocol ID**, or **Select from List** from drop down menu. • **Protocol ID** – Enter the protocol in the ACE to which the packet is matched. • **Select from List**–Select the protocol from the list in the provided field.
Destination IP Address Value:	Enter the destination IP address.
Destination IP Wildcard Mask:	Enter the mask of the new source IP address.
Source IP Address Value:	Enter the source IP address.
Source IP Wildcard Mask:	Enter the mask of the new source IP address.

VLAN ID:	Enter the VLAN ID to which the IP address is attached in IPv4-Based ACE. The range is from 1-4094.
802.1p Value:	Enter the 802.1p value. The range is from from 0-7.
Ethertype Value:	Enter the Ethertype value. The range is from 05DD-FFFF.
ICMP:	Select **Any**, **Protocol ID**, or **Select from List** from drop down menu. • **Protocol ID** – Enter the protocol in the ACE to which the packet is matched. The range is from 0-255. • **Select from List**– Select the ICMP from the list in the provided field.
ICMP Code:	Enter the ICMP code. The range is from 0-255.
Source Port:	Select **Single** or **Range** from the list. Enter the source port that is matched to packets. The range is from 0-65535.
Destination Port:	Select **Single** or **Range** from the list. Enter the destination port that is matched to packets. The range is from 0-65535.
Type of Service:	Enter the DSCP. The range is from 0-63.

Click **Apply** to save the changes to the system.

ACL Binding

ACL Binding is a configuration setting that allows a user to choose a particular ACL for an ACL check. An ACL check is an additional check used to determine what operations a user can perform regarding particular items or item types.



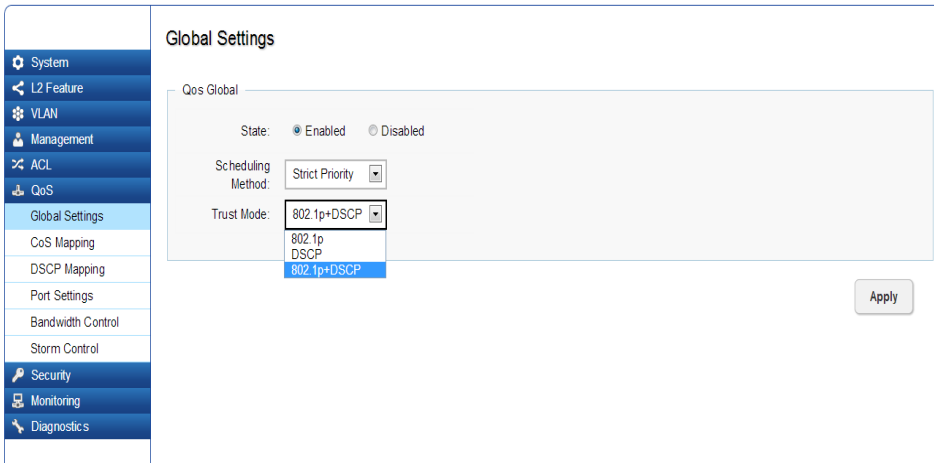
Port:	Select the port for which the ACLs are bound to.
MAC ACL:	The ACL is MAC address based.
IPv4 ACL:	The ACL is IP address based.
IPv6 ACL:	The ACL is IP address based.

Click **Apply** to save the changes to the system.

QoS

Quality of Service (QoS) provides the ability to implement priority queuing within a network. QoS enables traffic to be prioritized, while excessive broadcast and multicast traffic to be avoided. Traffics such as Voice and Video streaming which requires a minimal delay can be assigned to a high priority queue, while other traffic can be assigned to a lower priority queue resulting in uniterrupted actions.

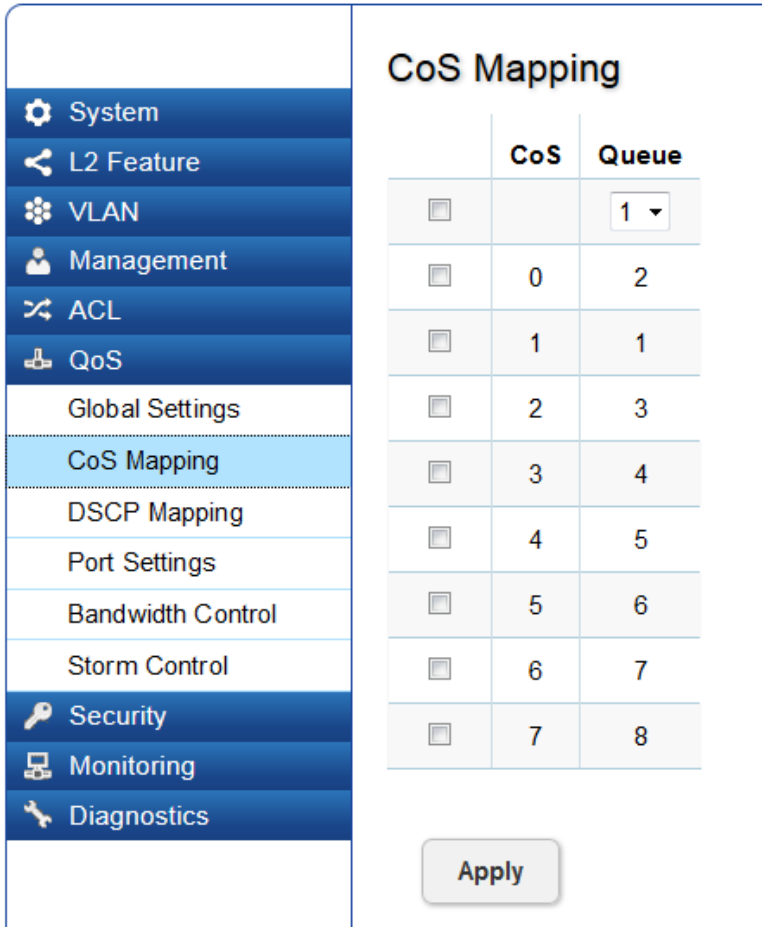
Global Settings



State:	Select whether QoS is enabled or disabled on the switch.
Scheduling Method:	Selects the Strict Priority or WRR to specify the traffic scheduling method. • **Strict Priority -** Specifies traffic scheduling based strictly on the queue priority. • **WRR -** Use the Weighted Round-Robin (WRR) algorithm to handle packets in priority classes of service. It assigns WRR weights to queues.
Trust Mode:	Select which packet fields to use for classifying packets entering the Switch. • **DSCP** - Classify traffic based on the DSCP (Differentiated Services Code Point) tag value. • **1p**-Classify traffic based on the 802.1p. The eight priority tags that are specified in IEEE802.qp are from 1 to 8.

CoS Mapping

Use the Class of Service (CoS) Mapping feature to specify which internal traffic class to map to the corresponding CoS value. CoS allows you to specify which data packets have greater precedence when traffic is buffered due to congestion.

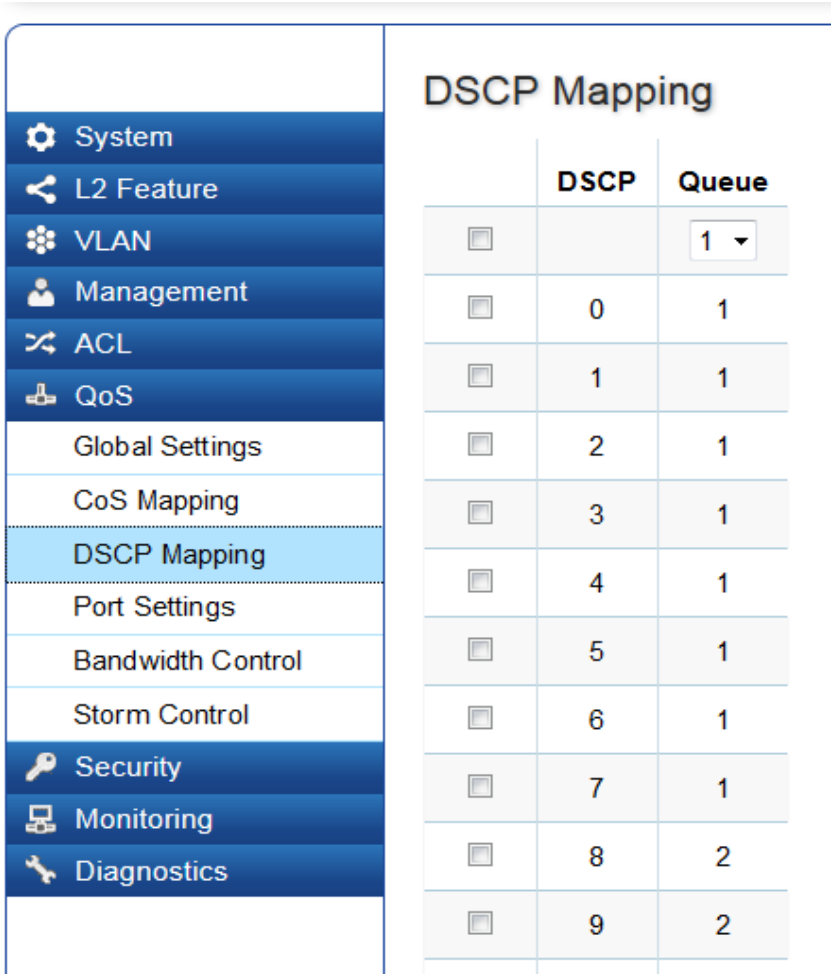


CoS (Class of Service):	Displays the CoS priority tag values, where 0 is the lowest and 7 is the highest.
Queue:	Check the CoS priority tag box and select the Queue values for each CoS value in the provided fields. Eight traffic priority queues are supported and the field values are from 1-8, where one is the lowest priority and eight is the highest priority.

Click **Apply** to save the changes to the system.

DSCP Mapping

Use Differentiated Services Code Point (DSCP) Mapping feature to specify which internal traffic class to map to the corresponding DSCP values. DSCP Mapping increases the number of definable priority levels by reallocating bits of an IP packet for prioritization purposes.



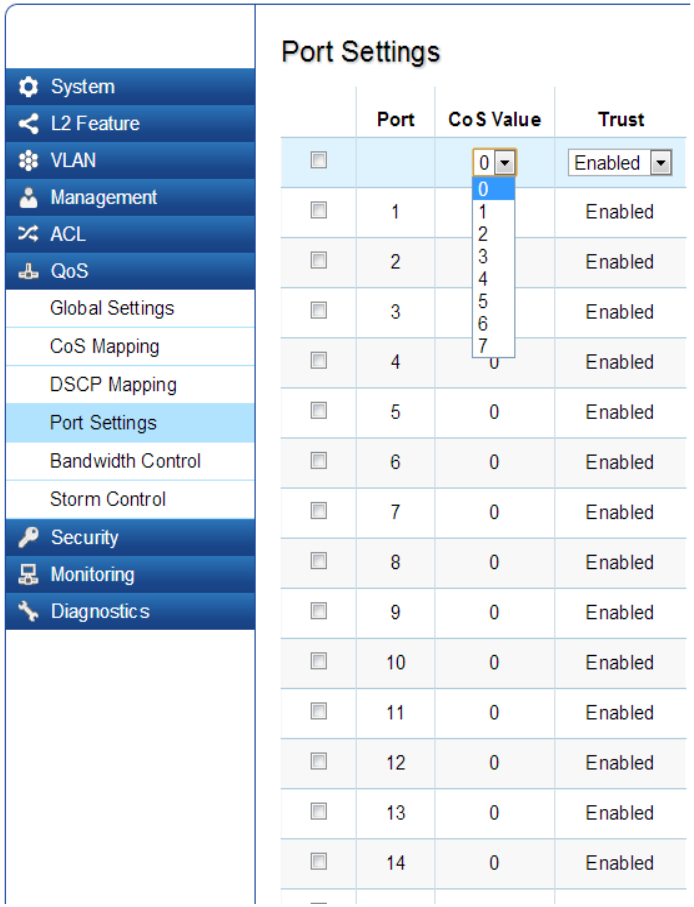
DSCP (Differentiated Services Code Point):	Displays the packet's DSCPvalues, where 0 is the lowest and 10 is the highest.
Queue:	Check the CoS priority tag box and select the Queue values for each DSCP in the provided fields. Eight traffic priority queues are supported and the field values are from 1-8, where one is the lowest priority and eight is the highest priority.

Click **Apply** to save the changes to the system.

Port Settings

From here, you can configure the QoS port settings for the Switch. Select a port you wish to set and choose a CoS value from the drop-down box. Next, Select to **Enable** or **Disable** the Trust setting to let any CoS packet be marked at ingress.

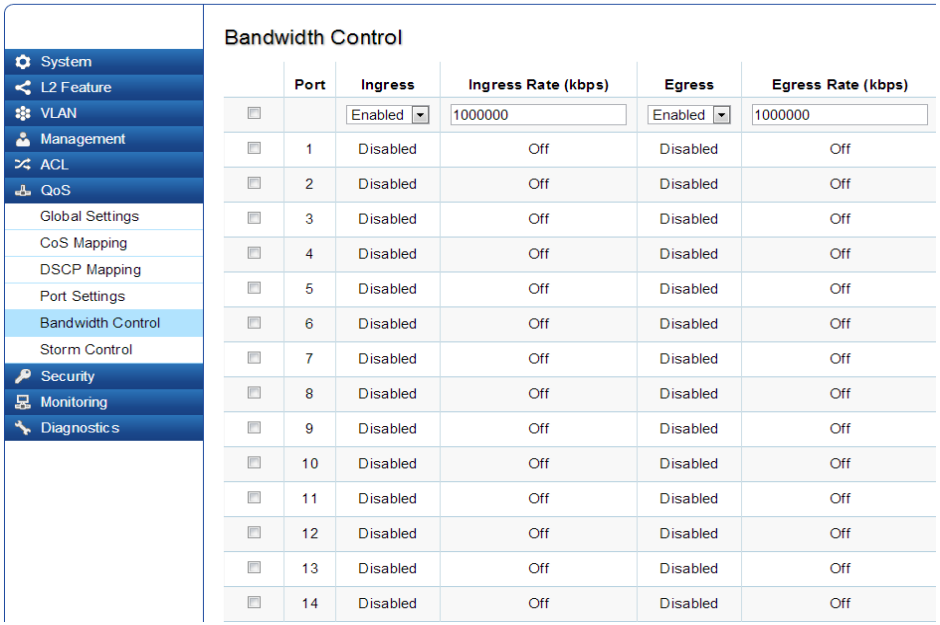
Port:	Displays the ports for which the CoS parameters are defined.
CoS (Class of Service) Value:	Select the CoS priority tag values, where 0 is the lowest and 7 is the highest.
Trust:	Select **Enable** to trust any CoS packet marking at ingress and select **Disable** to not trust any CoS packet marking at ingress.



Click **Apply** to save the changes to the system.

Bandwidth Control

The Bandwidth Control feature allows users to define the bandwidth settings for a specified port's Ingress Rate Limit and Egress Rate.

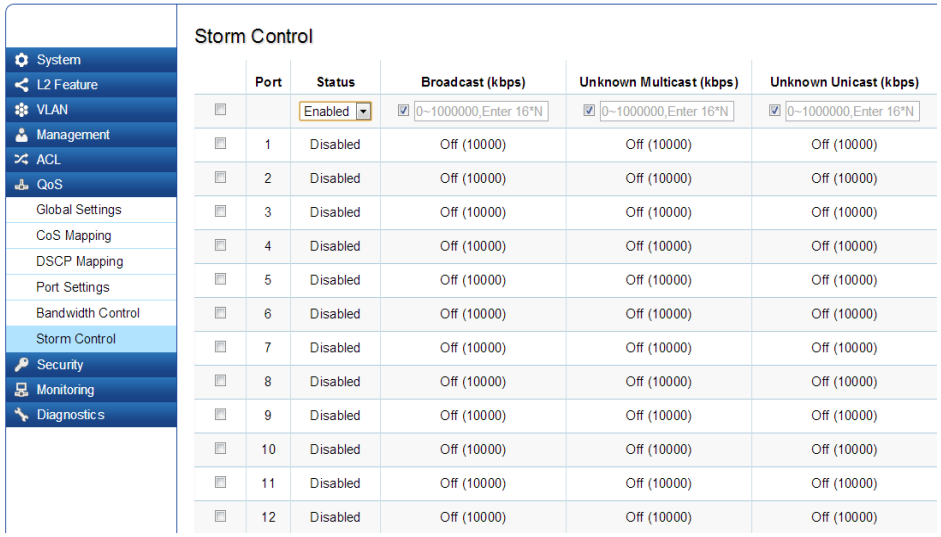


Port:	Displays the ports for which the bandwidth settings are displayed.
Ingress:	Select to **Enable** or **Disable** ingress on the interface.
Ingress Rate:	Enter the ingress rate in kilobits per second. The Gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second.
Egress:	Select from the drop down box to **Enable** or **Disable** egress on the interface .
Egress Rate:	Enter the egress rate in kilobits per second. The Gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second.

Click **Apply** to save the changes to the system.

Storm Control

Storm Control limits the amount of Broadcast, Unknown Multicast, and Unknown Unicast frames accepted and forwarded by the Switch. Storm Control can be enabled per port by defining the packet type and the rate that the packets are transmitted at. The Switch measures the incoming Broadcast, Unknown Multicast, and Unknown Unicast frames rates separately on each port, and discards the frames when the rate exceeds a user-defined rate.



Port:	Displays the ports for which the Storm Control information is displayed.
Status:	Select whether Storm Control is **Enabled** or **Disabled** ingress on the interface.
Broadcast:	Enter the **broadcast** rate in kilobits per second. The Gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second. If the rate of broadcast traffic ingress on the interface increases beyond the configured threshold, the traffic is dropped.
Unknown Multicast:	Enter the Unknown Multicast rate in kilobits per second. The Gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second. If the rate of broadcast traffic ingress on the interface increases beyond the configured threshold, the traffic is dropped.
Unknown Unicast:	Enter the Unknown Unicast rate in kilobits per second. The Gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second. If the rate of broadcast traffic ingress on the interface increases beyond the configured threshold, the traffic is dropped.

Click **Apply** to save the changes to the system.

Security

802.1X

The IEEE-802.1X port-based authentication provides a security standard for network access control with RADIUS servers and holds a network port disconnected until authentication is completed. With 802.1X port-based authentication, the supplicant provides credentials, such as user name, password, or digital certificate to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network. The Switch uses 802.1X to enable or disable port access control, to enable or disable the Guest VLAN, and to enable or disable the forwarding EAPOL (Extensible Authentication Protocol over LANs) frames.

Authenticators:	Specifies the port that is authenticated.
Supplicants:	Specifies the host (Client Device) connected to the authenticated port. performs the authentication on behalf of the authenticator and indicates whether the user is authorized to access system services.

Global Settings

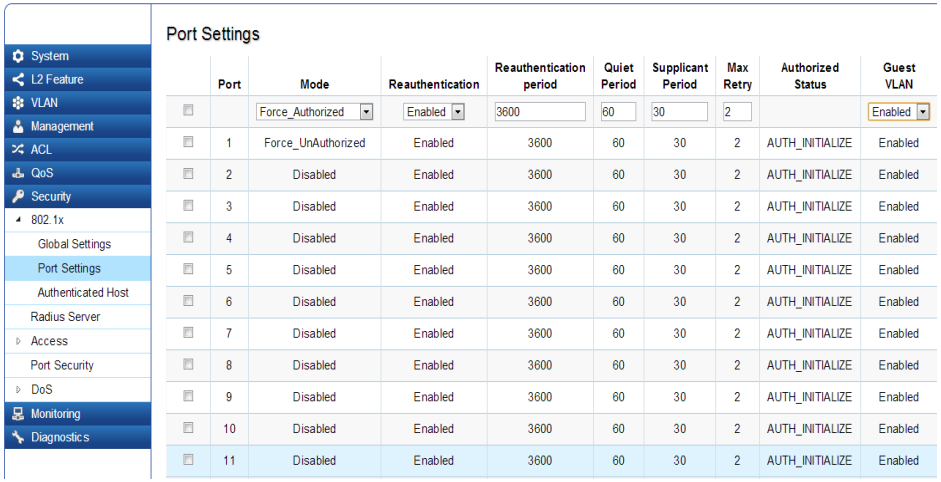
From here, you can select whether to **Enable** or **Disable** 802.1X for the Switch. If enabled, next choose whether to **Enable** or **Disable** the Guest VLAN for the Switch. Finally, select the VLAN ID you wish from the list.

State:	Select whether authentication is **Enabled** or **Disabled** on the Switch.
Guest VLAN:	Select whether Guest VLAN is **Enabled** or **Disabled** on the Switch. The default is **Disabled**.
Guest VLAN ID:	Select the guest VLAN ID from the list of currently defined VLANs.

Click **Apply** to save the changes to the system.

Port Settings

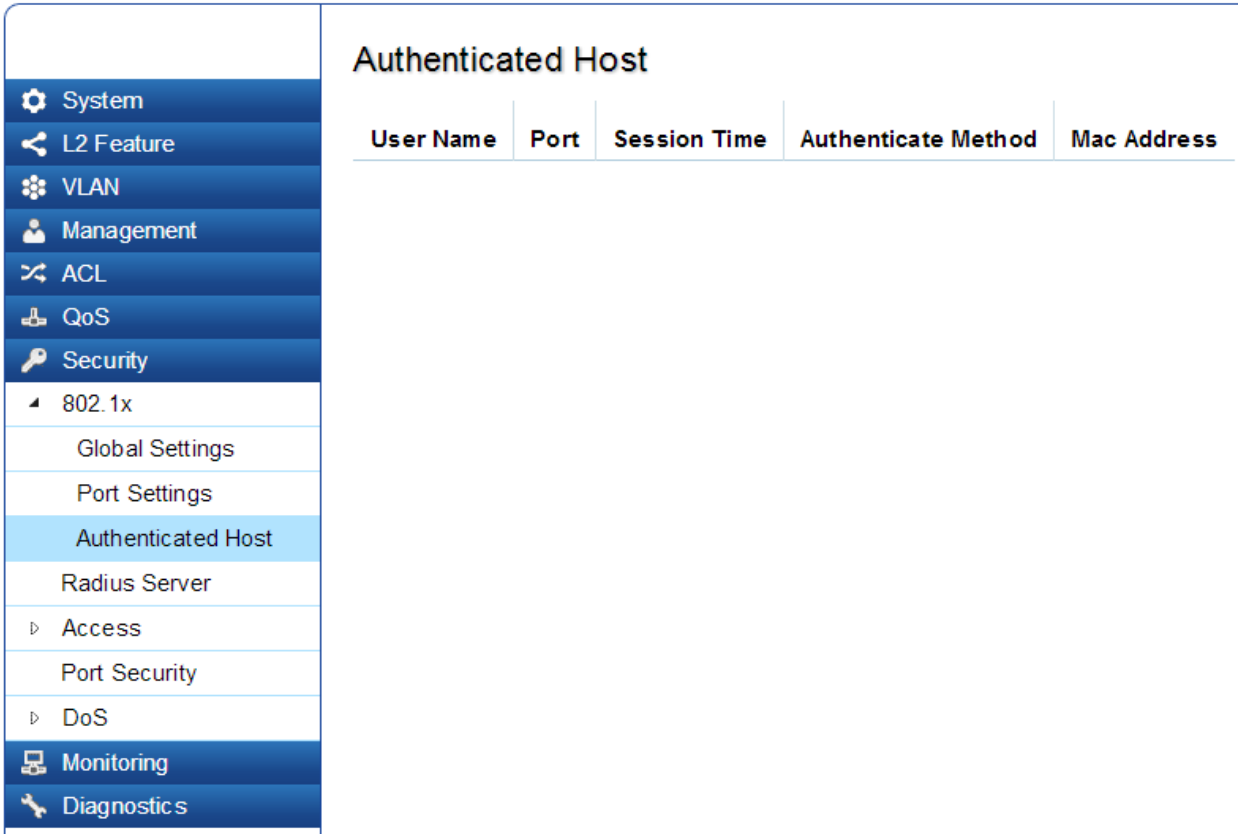
From here, you can configure the port settings as they relate to 802.1X. First, select the mode from the drop-down box. Next, choose whether to **Enable** or **Disable** reauthentification for the port. Enter the amount of time span that you wish to elapse for the Re-authentification period, Quiet Period, and Supplicant Period. After this, enter the Max number of times you wish for the Switch to retransmit and EAP request. Finally, choose whether you wish to **Enable** or **Disable** the VLAN ID.



Port:	Displays the ports for which the 802.1X information is displayed.
Mode:	Select the **Auto** or **Force_UnAuthorized** or **Force_Authorized** mode from the list.
Re-authentication:	Select whether port reauthenticati-on is **Enabled** or **Disabled**.
Re-authentication period:	Enter the time span in which the selected port is reauthenticated. The default is 3600 seconds.
Quiet Period:	Enter the number of the device that remains in the quiet state following a failed authentication exchange. The default is 60 seconds.
Supplicant Period:	Enter the amount of time that lapses before an EAP request is resent to the supplicant. The default is 30 seconds.
Max Retry:	Enter the maximum number of times that the Switch retransmits an EAP request to the client before it times out the authentication session. The default is 2 times.
Guest VLAN ID:	Select whether guest VLAN ID is **Enabled** or **Disabled**.
Authorized Status:	Displays the authorized mode status.

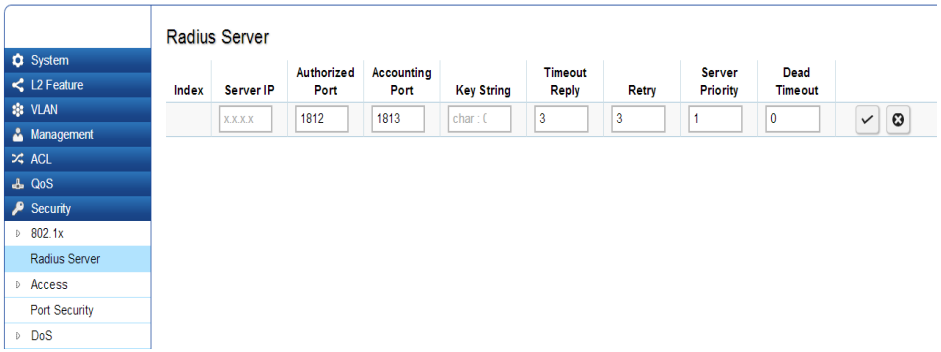
Authenticated Host

The Authenticated Host section displays the authenticated User Name, Port, Session Time, Authenticated Method, and Mac Address.



Radius Server

RADIUS (Remote Authorization Dial-In User Service) servers provide security for networks. Radius servers provide authentication and authorization for networks. The Radius server maintains a user database, which contains authentication information. The Switch passes information to the configured Radius server, which can authenticate a user name and password before authorizing use of the network.



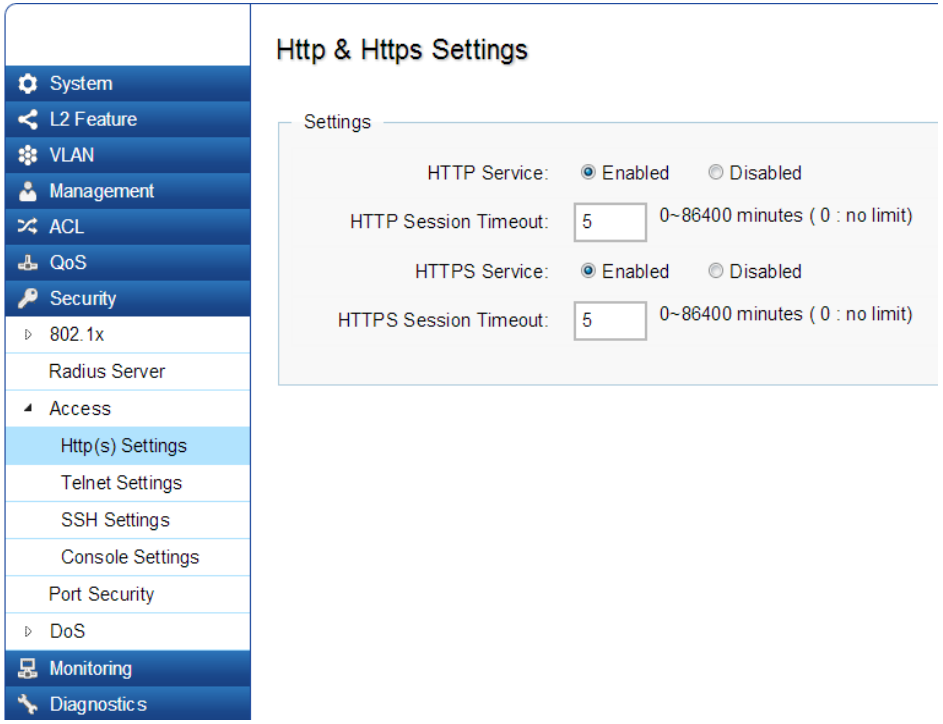
Index:	Displays the index for which RADIUS Server is displayed.
Server IP:	Enter the Radius Server IP address.
Authorized Port:	Enter the authorized port number. The default port is 1812.
Accounting Port:	Enter the name you wish to use to identify this Switch.
Key String:	Enter the Key String used for encrypting all Radius communication between the device and the Radius server.
Timeout Reply:	Enter the amount of time the device waits for an answer from the Radius Server before switching to the next server. The default value is 3.
Retry:	Enter the number of transmitted requests sent to the Radius server before a failure occurs. The default is 3.
Server Priority:	Enter the priority for the Radius server.
Dead Timeout:	Enter the amount of time that the Radius Server is bypassed for service requests. The default value is 0.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Access

Http(s) Settings

The EnGenius Layer 2 PoE+ Switch provides a built-in browser interface that enables you to configure and manage the Switch via Hypertext Transfer Protocol (Http) and Hypertext Transfer Protocol Secure (Https) requests selectivly to help prevent security breaches on the network. You can manage your HTTP and HHTPs settings for the Switch further by choosing the length of session timeouts for HTTP and HTTPs requests. Select whether to **Enable** or **Disable** the HTTP service and enter the HTTP Timeout session. Next, select whether to **Enable** or **Disable** the HTTPS sevice and enter the HTTPS timeout session for the Switch.

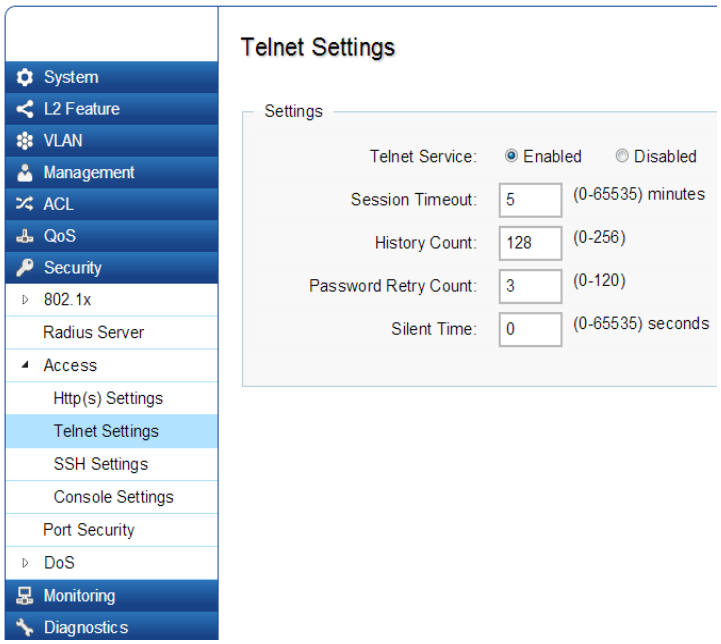


HTTP Service:	Select whether HTTP Service for the Switch is **Enabled** or **Disabled**. This is enabled by default.
HTTP Session Timeout:	Enter the amount of time that elapses before HTTP is timed out. The default is 5 minutes. The range is from 0-86400 minutes.
HTTPs Service:	Select whether the HTTP Service is **Enabled** or **Disabled.** This is disabled by default.
HTTPS Session Timeout:	Enter the amount of time that elapses before HTTPS is timed out. The default is 5 minutes. The range is from from 0-86400 minutes.

Click **Apply** to save the changes to the system.

Telnet Settings

From here, you can configure and manage the Switch's Telnet protocol settings. The Telnet protocol is a standard internet protocol which enables terminals and applications to interface over the Internet with remote hosts by providing Command Line Interface (CLI) communication using a virtual terminal connection. This protocol provides the basic rules for making it possible to link a client to a command interpreter. The Telnet service for the Switch is enabled by default. Please note that for secure communication, it is better to use SSH over Telnet. To enable and configure SSH Settings, please refer to SSH Settings on the next page.

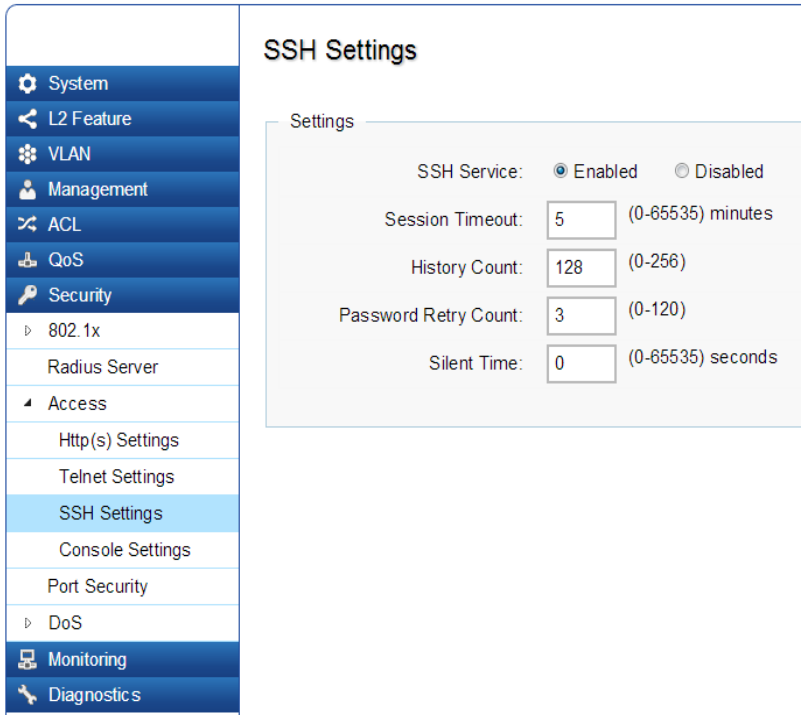


Telnet Service:	Select whether the Telnet Service is **Enabled** or **Disabled**. It is enabled by default.
Session Timeout:	Enter the amount of time that elapses before the Telnet Service is timed out. The default is 5 minutes. The range is from 0-65535 minutes.
History Count:	Enter the entry number for History of Telnet Service. The default is 128. The range is from 0-256.
Password Retry Count:	Enter the number of password request send to Telnet Service. The default is 3. The range is from 0-120.
Silent Time:	Enter the silent time for Telnet Service. The range is from 0-65535 seconds.

Click **Apply** to save the changes to the system.

SSH Settings

Secure Shell (SSH) is a cryptographic network protocol for secure data communication network services. SSH is a way of accessing the command line interface on the network Switch.The traffic is encrypted, so it is difficult to eavesdrop on as it creates a secure connection within an insucure network such as the internet. Even if an attacker was able to view the traffic, the data would be incomprehensible without the correct encryption key to decode it.



SSH Service:	Select whether SSH is **Enabled** or **Disabled**. This is disabled by default.
Session Timeout:	Enter the amount of time that elapses before the SSH Service is timed out. The default is 5 minutes. The range is from 0-65535 minutes.
History Count:	Enter the entry number for History of SSH Service. The default is 128. The range is from 0-256.
Password Retry Count:	Enter the number of password request sent to the SSH Service. The default is 3. The range is from 0-120.
Silent Time:	Enter the silent time for Telnet Service. The range is from 0-65535 seconds.

Click **Apply** to save the changes to the system.

Console Settings

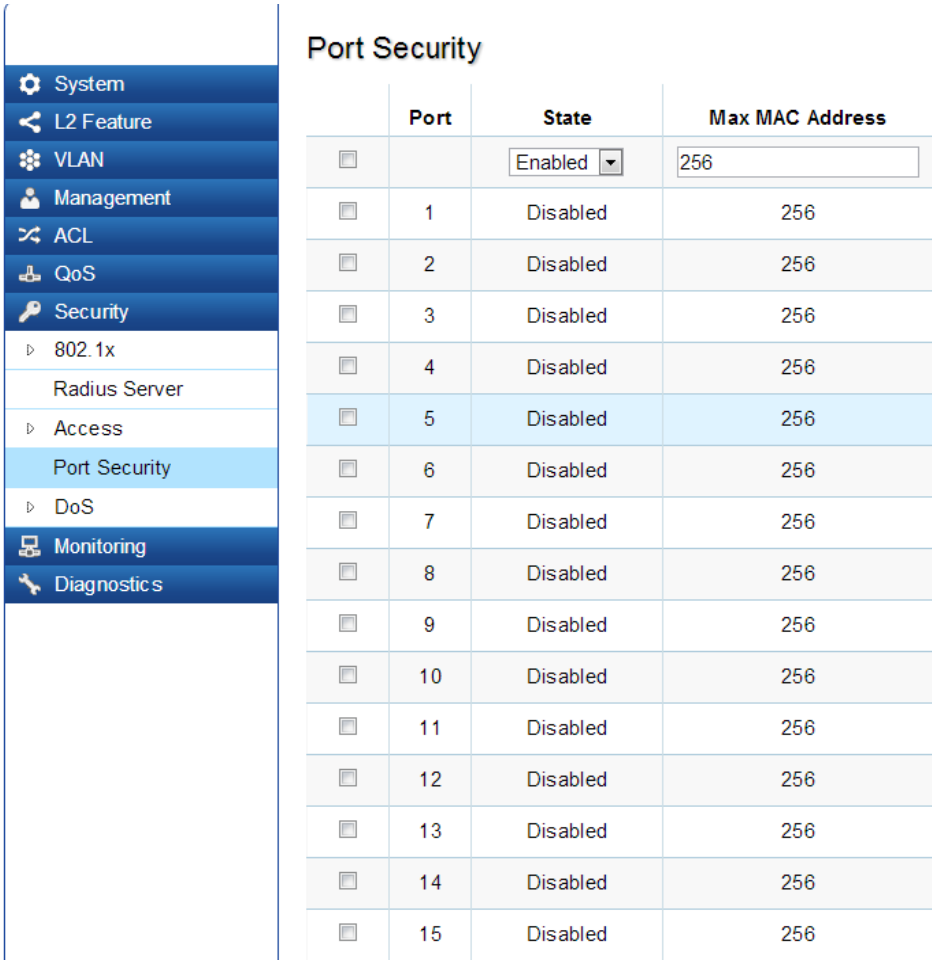
From here, you can configure the Console Service settings for the Switch.

Session Timeout:	Enter the amount of time that elapses before Console Service is timed out. The default is 5 minutes. The range is from 0-65535 minutes.
History Count:	Enter the entry number for History of Console Service. The default is 128. The range is from 0-256.
Password Retry Count:	Enter the number of password requests to send to the Console Service. The default is 3. The range is from 0-120.
Silent Time:	Enter the silent time for Console Service. The range is from 0-65535 seconds.

Click **Apply** to save the changes to the system.

Port Security

Network security can be increased by limiting access on a specific port to users with specific MAC addresses. Port Security prevents unauthorized device to the Switch prior to stopping auto-learning processing.



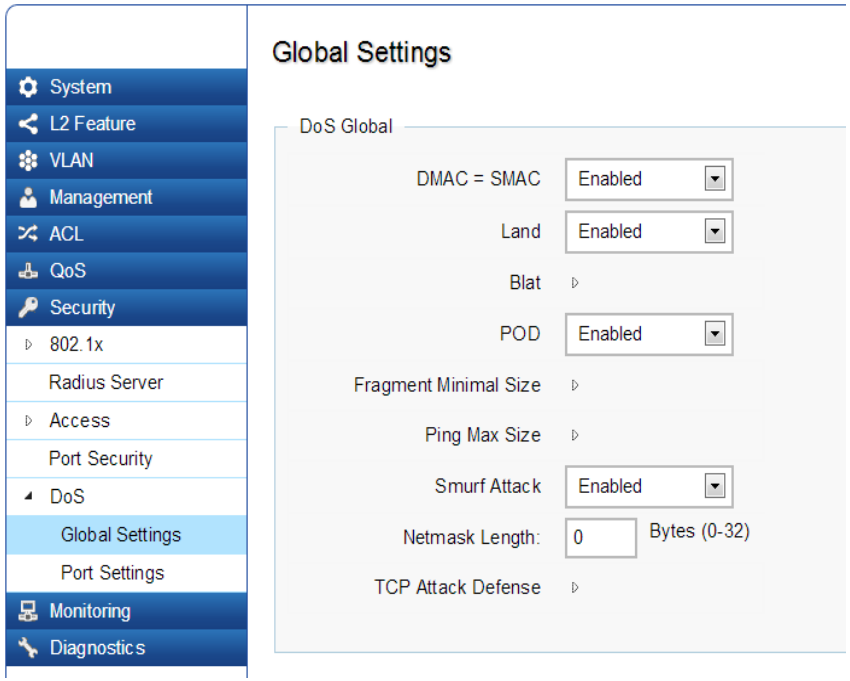
Max MAC Address:	Enter the maximum number of MAC Addresses that can be learned on the port. The range is from 1-256.
Port:	Displays the port for which the port security is defined.
State:	Select **Enabled** or **Disabled** for the port security feature for the selected port.

Click **Apply** to save the changes to the system.

DoS

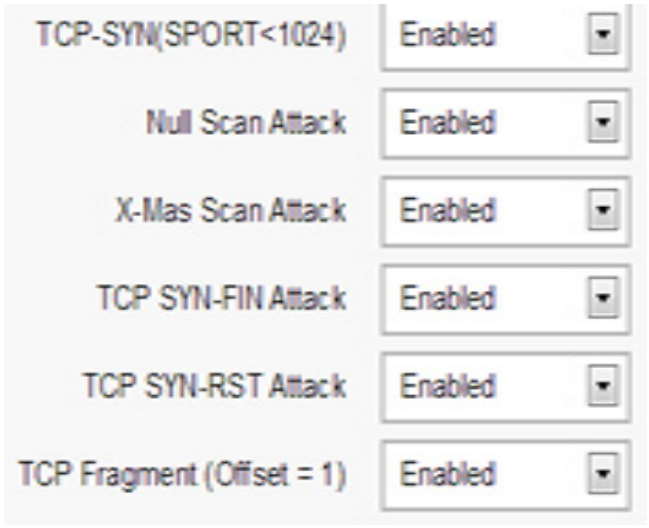
DoS (Denial of Service) is used for classifying and blocking specific types of DoS attacks. From here, you can configure the Switch to monitor and block different types of attacks:

Global Settings



DMAC = SMAC:	Select **Enabled** or **Disabled** from the list.
Land:	Select **Enabled** or **Disabled** from the list.
UDP Blat:	Select **Enabled** or **Disabled** from the list.
TCP Blat:	Select the **Enabled** or **Disabled** from the list.
POD:	Select the **Enabled** or **Disable** from the list.
Fragment Minimal Size:	Enter the minimal size.
IPv6 Min Fragment:	Select **Enabled** or **Disabled** from the list.
Bytes:	Enter the size of IPv6 packets. The range is from 0-65535.
ICMP Fragment:	Select **Enabled** or **Disabled** from the list.

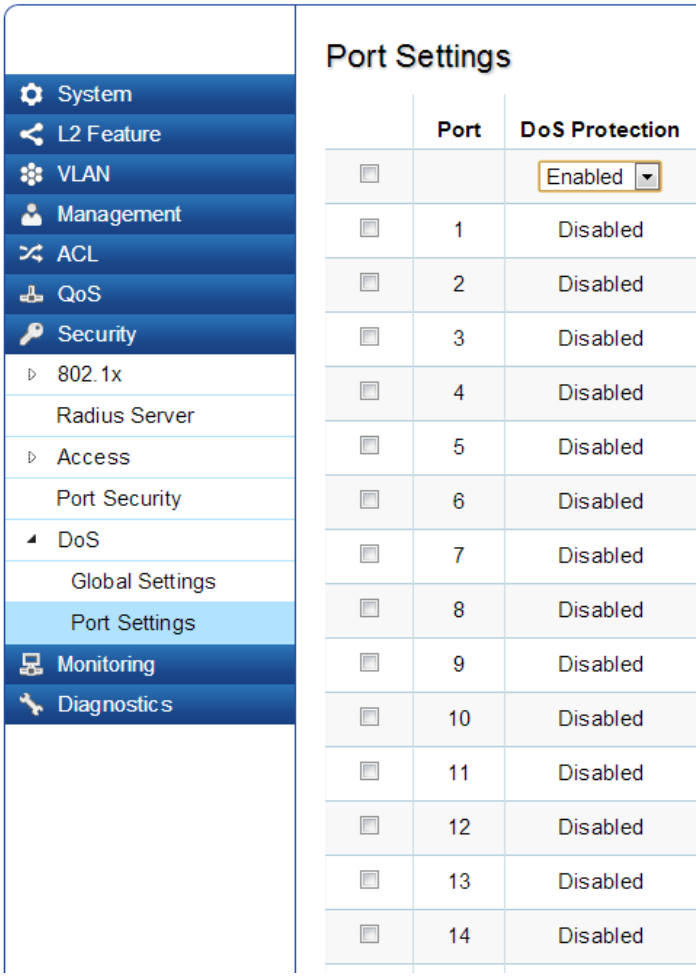
Click **Apply** to save the changes to the system.



DMAC = SMAC:	Select **Enabled** or **Disabled** from the list.
Land:	Select **Enabled** or **Disabled** from the list.
UDP Blat:	Select **Enabled** or **Disabled** from the list.
TCP Blat:	Select the **Enabled** or **Disabled** from the list.
POD:	Select the **Enabled** or **Disable** from the list.
Fragment Minimal Size:	Enter the minimal size.
IPv6 Min Fragment:	Select **Enabled** or **Disabled** from the list.
Bytes:	Enter the size of IPv6 packets. The range is from 0-65535.
ICMP Fragment:	Select **Enabled** or **Disabled** from the list.
Ping Max Size:	Enter the max ping size you wish to use.
IPv4 Ping Max Size:	Select **Enabled** or **Disabled** from the list.
IPv6 Ping Max Size:	Select **Enabled** or **Disabled** from the list.
Ping Max Size Setting:	Enter the max ping size for the ping. The range is from 0-65535.
Smurf Attack:	Select **Enabled** or **Disabled** from the list.
Netmask Length:	Enter the length of the netmask. The range is from 0-32. **TCP-SYN:** Select **Enabled** or **Disabled** from the list.
Null Scan Attack:	Select **Enabled** or **Disabled** from the list.
X-Mas Scan Attack:	Select **Enabled** or **Disabled** from the list.
TCP SYN-FIN Attack:	Select **Enabled** or **Disabled** from the list.

Port Settings

From here you can configure the Port Settings for DoS for the Switch. Select from the drop down list whether you wish to **Enable** or **Disable** DoS Protection for the SWitch.



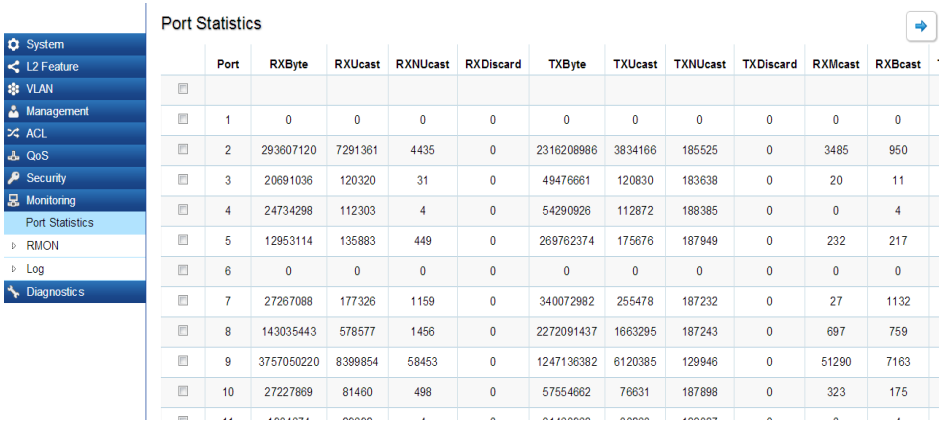
Port:	Displays the port for which the DoS protection is defined.
DoS Protection:	Select **Enabled** or **Disabled** for the DoS Protection feature for the selected port.

Click **Apply** to save the changes to the system.

Monitoring

Port Statistics

The Port Statistics section displays a summary of all port traffic statistics regarding the monitoring features on the Switch.



Port	RXByte	RXUcast	RXNUcast	RXDiscard	TXByte	TXUcast	TXNUcast	TXDiscard	RXMcast	RXBcast
1	0	0	0	0	0	0	0	0	0	0
2	293607120	7291361	4435	0	2316208986	3834166	185525	0	3485	950
3	20691036	120320	31	0	49476661	120830	183638	0	20	11
4	24734298	112303	4	0	54290926	112872	188385	0	0	4
5	12953114	135883	449	0	269762374	175676	187949	0	232	217
6	0	0	0	0	0	0	0	0	0	0
7	27267088	177326	1159	0	340072982	255478	187232	0	27	1132
8	143035443	578577	1456	0	2272091437	1663295	187243	0	697	759
9	3757050220	8399854	58453	0	1247136382	6120385	129946	0	51290	7163
10	27227869	81460	498	0	57554662	76631	187898	0	323	175

Port:	Displays the port for which statistics are displayed.
RXByte:	Displays the number of all packets received on the port.
RXUcast:	Displays the number of Unicast packets received on the port.
RXNUcast:	Displays the number of Unicast packets received on the port.
RXDiscard:	Displays the number of received packets discarded on the port.
TXByte:	Displays the number of all packets transmitted on the port.
TXUcast:	Displays the number of Unicast packets transmitted on port.
TXNUcast:	Displays the number of Unicast packets transmitted on the port.
TXDiscard:	Displays the number of transmitted packets discarded on the port.
RXMcast:	Displays the number of Multicast packets received on the port.
RXBcast:	Displays the number of Broadcast packets received on the port.
TXMcast:	Displays the number of Multicast packets transmitted on the port.
TXBcast:	Displays the number of Broadcast packets transmitted on the port.

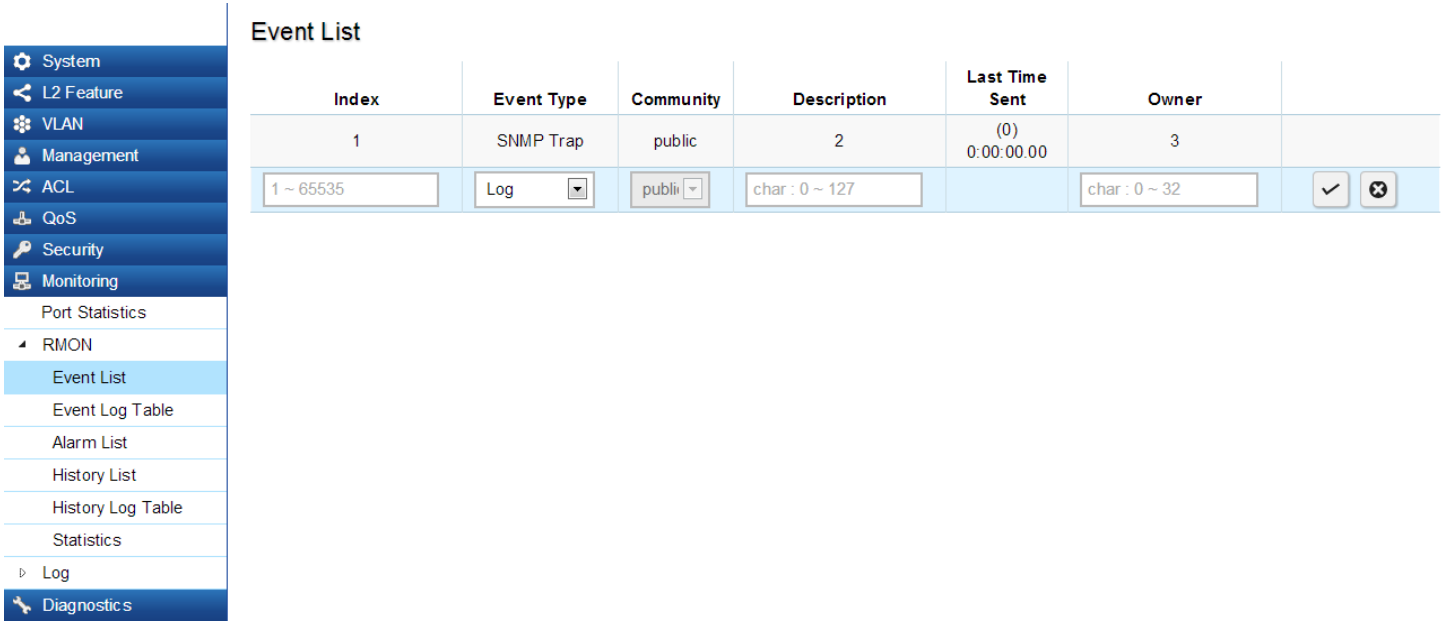
RMON

Remote Network Monitoring, or RMON is used for support monitoring and protocol analysis of LANS by enabling various network monitors and console systems to exchange network-monitoring data through the Switch.

Event List

The Event List defines RMON events on the Switch.

Index:	Enter the entry number for Event.
Event Type:	Select the event type. • **Log** - The event is a log entry. • **SNMP Trap** - The event is a trap. • **Log & Trap** - The event is both a log entry and a trap.
Community:	Enter the community to which the event belogs.
Description:	Displays the number of good broadcast packets received on the interface.
Last Time Sent:	Displays the time that event occurred. Owner: Enter the switch that defined the event.

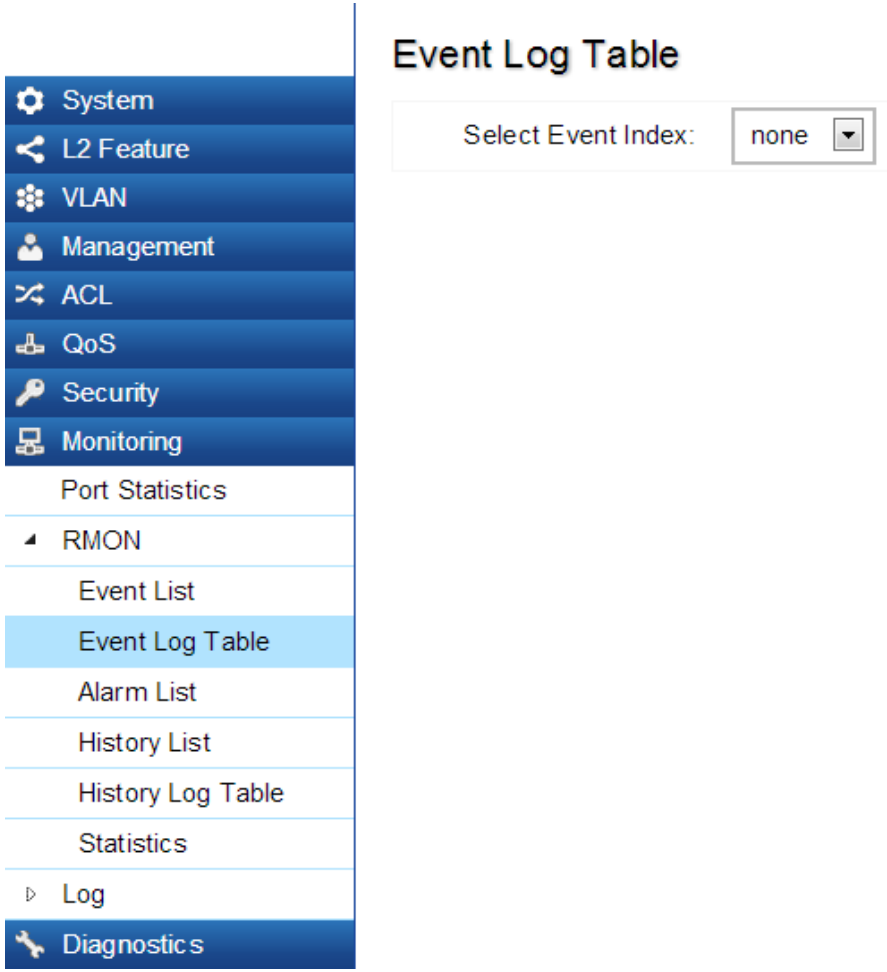


Event Log Table

From here, you can view specific Event logs for the Switch. Choose an Event log you wish to view fromt he drop-down list.

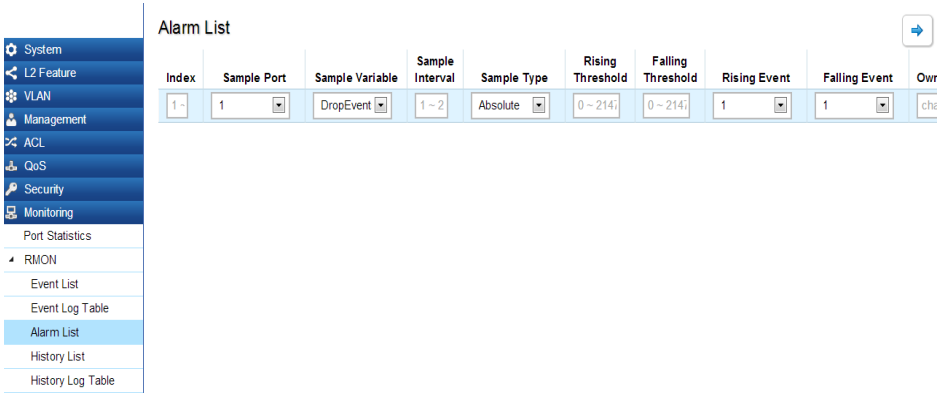
Event Log Table:	Select the index of the Event Log from the list.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.



Alarm List

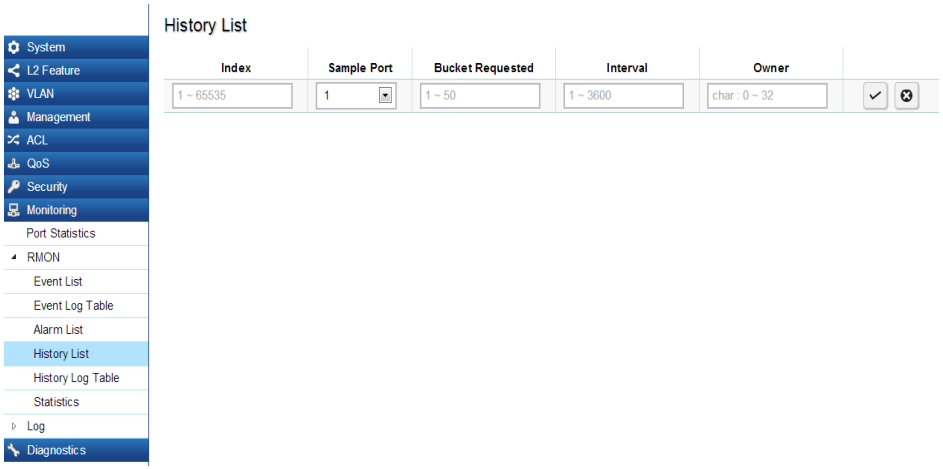
You can configure Network alarms to occur when a network problem is detected. Choose your preferences for the alarm from the drop-down boxes.



Index:	Enter the entry number for the History Log Table. Sample Port: Select the port from which the alarm samples were taken.
Sample Variable:	Select the variable of samples for the specified alarm sample.
Sample Interval:	Enter the alarm interval time.
Sample Type:	Select the sampling method for the selected variable and comparing the value against the thresholds. • **Absolute -** Compares the values with the thresholds at the end of the sampling interval. • **Delta -** Subtracts the last sampled value from the current value.
Rising Threshold:	Enter the rising number that triggers the rising threshold alarm.
Falling Threshold:	Enter the falling number that triggers the falling threshold alarm
Rising Event:	Enter the event number by the falling alarm are reported.
Falling Event:	Enter the event number by the falling alarms are reported.
Owner:	Enter the Switch that defined the alarm.

History List

The RMON History List screen contains information about samples of data taken from the ports.



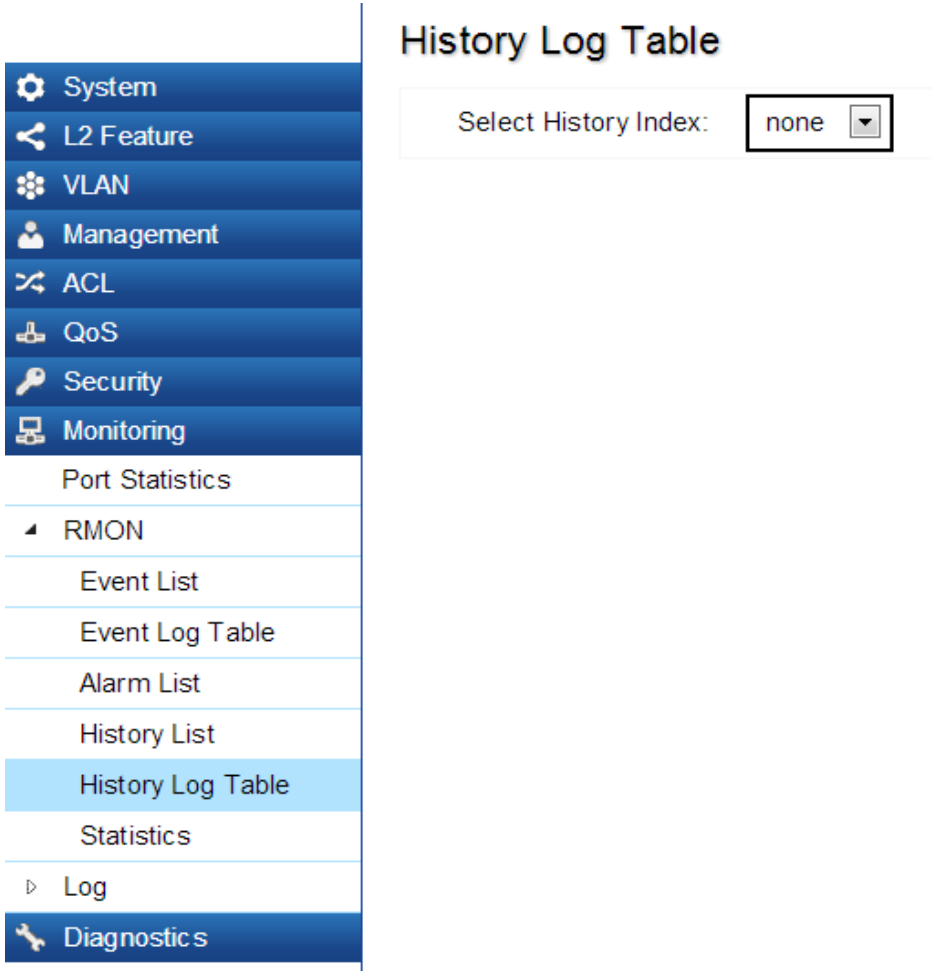
Index:	Enter the entry number for the History Log Table.
Sample Port:	Select the port from which the history samples were taken.
Bucket Requested:	Enter the number of samples to be saved. The range is from 1- 50.
Interval:	Enter the time that samples are taken from the ports. The field range is from 1-3600.
Owner:	Enter the RMON user that requested the RMON information. The range is from 0-32 characters.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

History Log Table

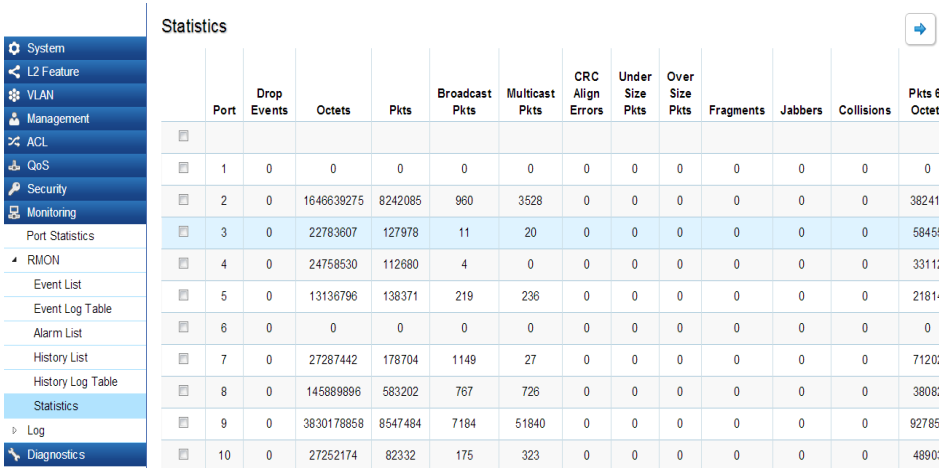
From here, you can view the History Index for History Logs on the Switch. Select a History Index to view from the drop-down box.

History Log Table:	Select the index for the History Log from the list.



Statistics

The Statistics page displays general information about the Switch in terms of its ports and packet transmissions.



Port:	Select the specific port for which RMON statistics are displayed.
Drop Events:	Displays the number of dropped events that have occurred on the port.
Octets:	Displays the sample number from which the statistic taken.
Pkts:	Displays the number of octets received on the port.

Broadcast Pkts:	Displays the number of good broadcast packets received on the port. This number does not include Multicast packets.
Multicast Pkts:	Displays the number of good Multicast packets received on the port.
CRC & Align Errors:	Displays the number of CRC and Align errors that have occurred on the port.
Undersize Pkts:	Displays the number of undersized packets (less than 64 octets) received on the port.
Oversize Pkts:	Displays the number of oversized packets (over 1518 octets) received on the port.
Fragments:	Displays the number of fragments received on the port.
Jabbers:	Displays the total number of received packets that were longer than 1518 octets.
Collisions:	Displays the number of collisions received on the port.
Pkts of 64 Octets:	Displays the number of 64-byte frames received on the port.
Pkts of 65 to 127 Octets:	Displays the number of 65 to 127 byte packets received on the port.
Pkts of 128 to 255 Octets:	Displays the number of 128 to 255 byte packets received on the port.
Pkts of 256 to 511 Octets:	Displays the number of 256 to 511 byte packets received on the port.
Pkts of 512 to 1023 Octets:	Displays the number of 512 to 1023 byte packets received on the port.
Pkts of 1024 to 1522 Octets:	Displays the number of 1024 to 1522 byte packets received on port.

Log

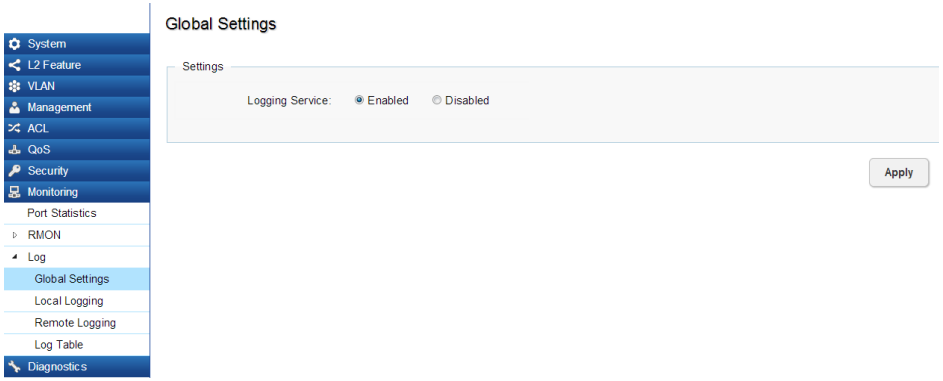
The Syslog Protocol allows devices to send event notification messages in response to events, faults, or errors occurring on the platform as well as changes in configuration or other occurrences across an IP network to syslog servers. It then collects the event messages, providing powerful support for users to monitor network operation and diagnose malfunctions. A Syslog-enabled device can generate a syslog message and send it to a Syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content, and system log related information of Syslog messages. Each Syslog message has a facility and severity level. The Syslog facility identifies a file in the Syslog server. Refer to the documentation of your Syslog program for details. The following table describes the Syslog severity levels.

Code	Severity	Description	General Description
0	Emergency	System is unusable	A emergency condition usually affecting multiple apps/servers/sites. Direct Attention is required.
1	Alert	Actions must be taken immediately	Should be corrected immediately. Notify staff who can fix the problem promptly.
2	Critical	Critical conditions	Should be corrected immediately, but indicates failure in a secondary system.
3	Error	Error conditions	Non-urgent failures, these should be relayed to developers or admins; each item should be resolved promptly.
4	Warning	Warning conditions	Warning message that indicates an error will occur if action is not taken.
5	Notice	Normal but significant conditions	Events that are unusual but not error inducing. No immediate action required.
6	Informational	Informational message	Normal operational status may be gained for reporting procedures.
7	Debug	Debug-level messages	Information useful to developers for debugging applications.

Global Settings

From here, you can **Enable** or **Disable** the Log settings for the Switch.



Logging Service:	Use the radio buttons to enable or disable the system log.
Global Logs:	Select whether to **Enable** or **Disable** the Switch's global logs for Cache, File, and Server Log.

Apply: Click **APPLY** to update the system settings.

Local Logging:

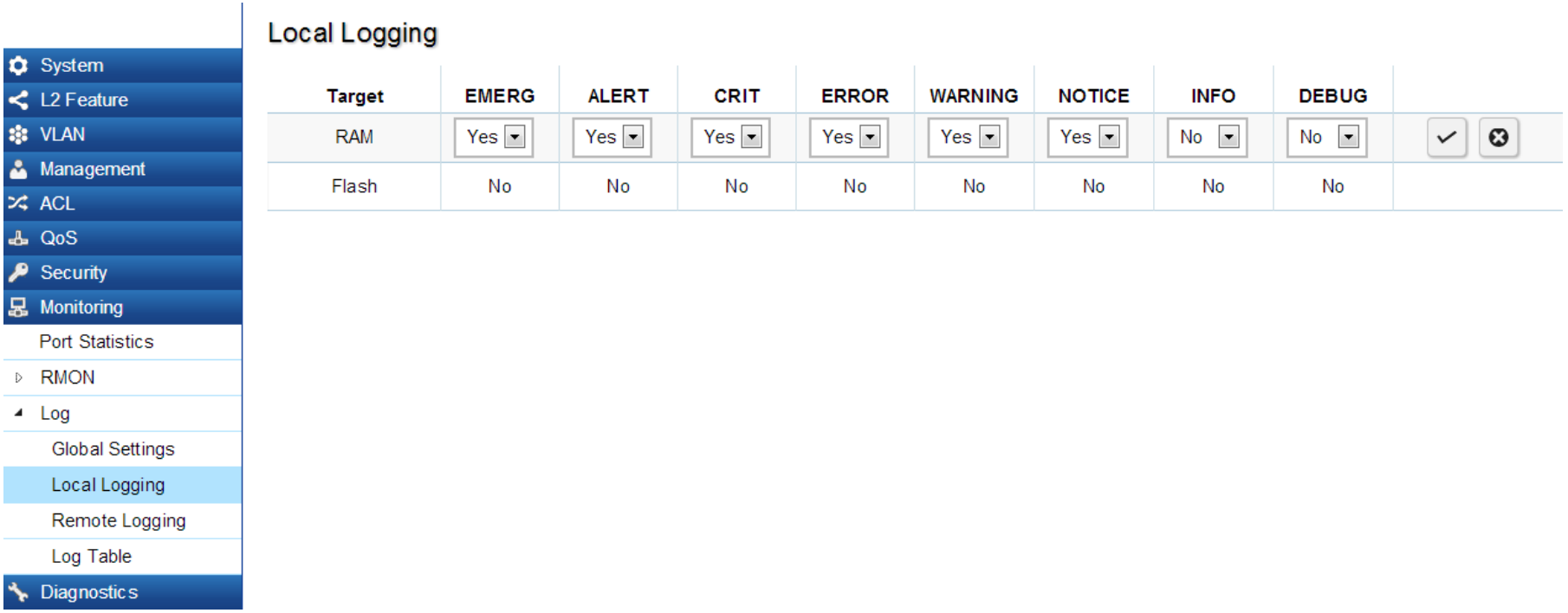
From here, you can discover the paths that a packet takes to a destination.

The Switch supports log output to two directions: **Flash** and **RAM**. The information stored in the system's Flash log will be lost after the Switch is rebooted or powered off, whereas the information stored in the system's RAM will be kept effective even if the Switch is rebooted or powered off.

Target:	The method for saving the switch log, to Flash, RAM or both.
Flash:	Log erased after reboot or power off
RAM:	Log stored in RAM. Will only be erased after system reset.
Severity Level:	Refer to severity level table.

Logs with the selected severity level and all logs of greater severity are sent to the host. For example, if you select **Error**, the logged messages include **Error, Critical, Alert,** and **Emergency.**

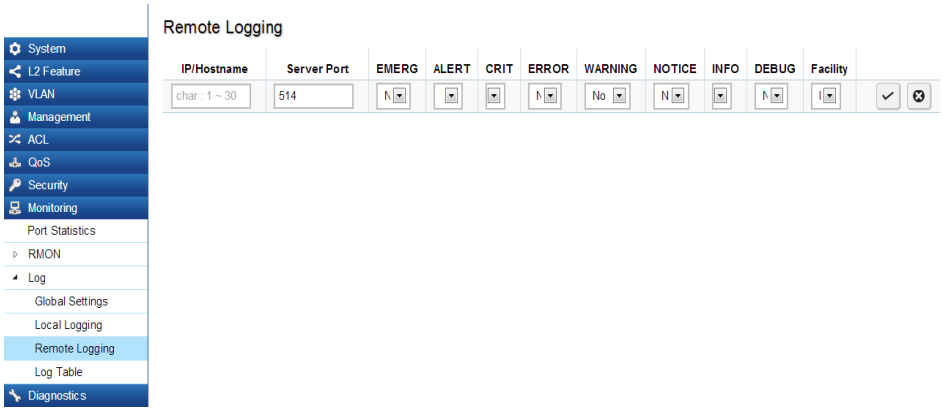
Target:	Select **Yes** or **No** from the list. If the device is not functioning properly, an emergency log message is saved to the specified logging location.
EMERG:	Select **Yes** or **No** from the list. If the Switch is not functioning properly, an emergency log message is saved to the specified logging location.
ALERT:	Select **Yes** or **No** from the list. If there is a serious Switch malfunction, then all Switch features are down.
CRIT:	Select **Yes** or **No** from the list. A critical log is saved if a critical Switch malfunction occurs.
ERROR:	Select **Yes** or **No** from the list. If triggered, a device error has occurred.
WARNING:	Select **Yes** or **No** from the list. The device is functioning, but an operational problem has occurred.
NOTICE:	Select **Yes** or **No** from the list. This will provide information about the Switch.
INFO:	Select **Yes** or **No** from the list. This will provide information about the Switch.
DEBUG:	Select whether the **Yes** or **No** from the list. This will provide a debugging message.



Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

Remote Logging:

From here, you can discover the paths that a packet takes to a destination. Remote logging enables the Switch to send system logs to the Log Server. The Log Server helps to centralize system logs from various devices such as Access Points so that the user can monitor and manage the whole network. Click the **Add** button and select the severity level of events you wish to log.

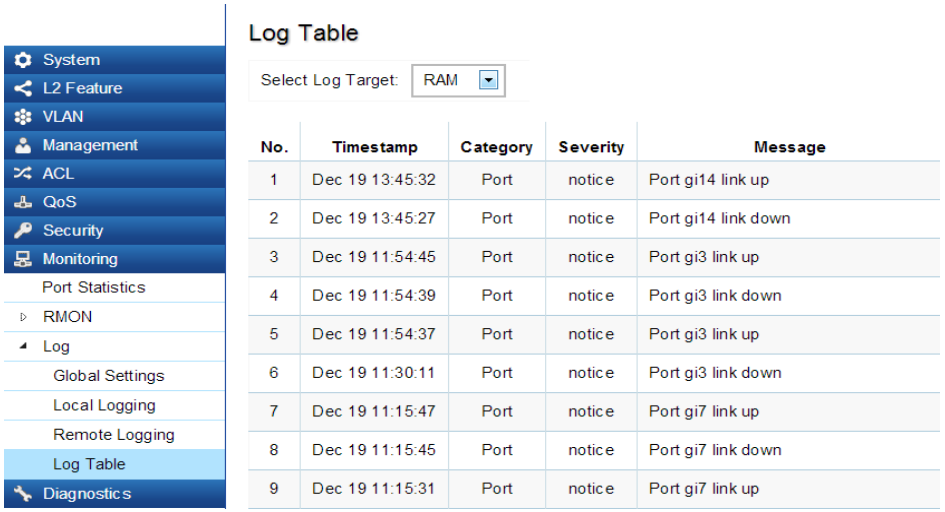


IP/Hostname:	Specify the IP address or host name of the host configured for the Syslog.
Server Port:	Specify the port on the host to which Syslog messages are sent. The default port is 514.
Severity Level:	Refer to severity level table on page 25 or 27. Logs with the selected severity level and all logs of greater severity are sent to the host. For example, if you select Error, the logged messages include Error, Critical, Alert, and Emergency
Facility:	The log facility is used to separate out log messages by application or by function, allowing you to send logs to different files in the syslog server. Use the drop-down menu to select local0, local1, local2, local3, local4, local5, local6, or local7.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

Log Table:

From here, users can view and delete the history log. Select the Log Target you wish to view from the drop-down box.



No.	Timestamp	Category	Severity	Message
1	Dec 19 13:45:32	Port	notice	Port gi14 link up
2	Dec 19 13:45:27	Port	notice	Port gi14 link down
3	Dec 19 11:54:45	Port	notice	Port gi3 link up
4	Dec 19 11:54:39	Port	notice	Port gi3 link down
5	Dec 19 11:54:37	Port	notice	Port gi3 link up
6	Dec 19 11:30:11	Port	notice	Port gi3 link down
7	Dec 19 11:15:47	Port	notice	Port gi7 link up
8	Dec 19 11:15:45	Port	notice	Port gi7 link down
9	Dec 19 11:15:31	Port	notice	Port gi7 link up

No.:	A counter incremented whenever an entry to the Switch's history log is made. It displays the last entry (highest sequence number) first.
Timestamp:	Displays the time of the log entry.
Category:	Displays the category of the history log entry. for example, If the name of a VLAN group is changed, the category will display "VLAN". If a device is connected to the Switch, the category will display "Port".
Severity:	Displays the level of severity of the log entry. Messages are assigned a severity code.
Message:	Displays text describing the event that triggered the history log entry.

Click **CLEAR** to clear the buffered log in the memory.

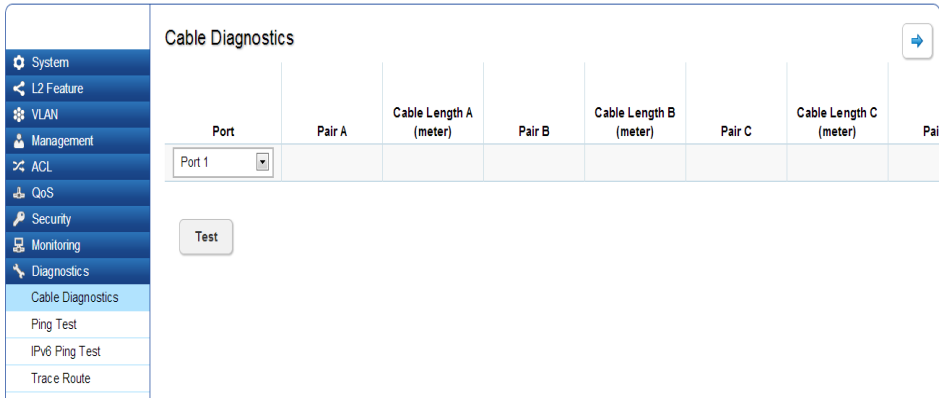
Diagnostics

Cable Diagnostics

Cable Diagnostics helps you to detect whether your cable has connectivity problems provides information about where errors have occurred in the cable. The tests use Time Domain Reflectometry (TDR) technology to test the quality of a copper cable attached to a port. TDR detects a cable fault by sending a signal through the cable and reading the signal that is reflected back. All or part of the signal is reflected back either by cable defects or by the end of the cable when an issue is present. Cables are tested when the ports are in the down state, with the exception of the cable length test.

To verify accuracy of the test, it is reccomended that you run multiple tests in case of a test fault or user error.

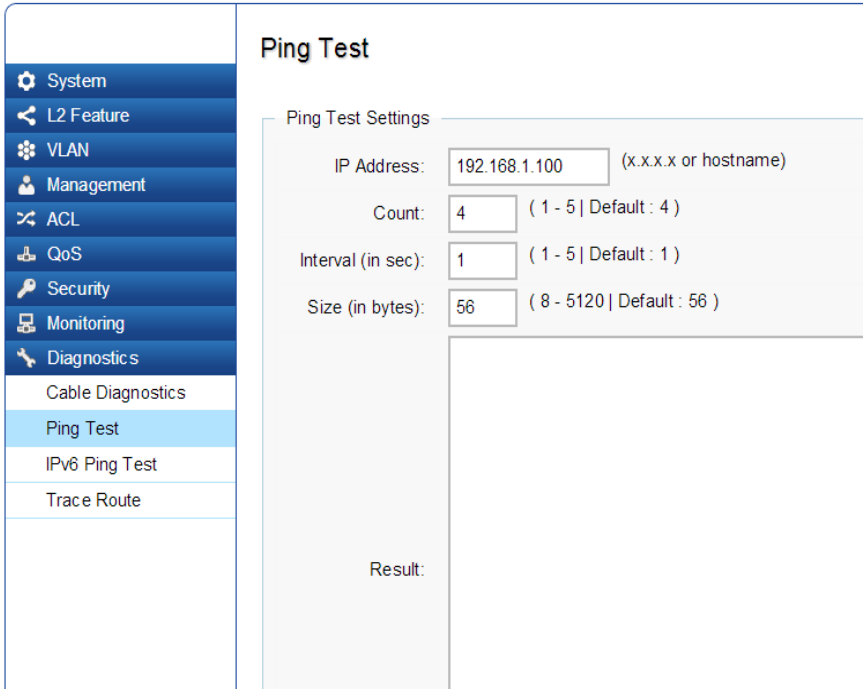
Port:	Select the port to which the cable is connected. Pair (A, B, C, and D): Displays the cable test results. • **Open** - A cable is not connected to the port. • **OK** - A cable is connected to the port.
Cable Length (A, B, C, and D):	Displays the approximate cable length.



Click **Test** to perform the cable tests for the selected port.

Ping Test

The Packet INternet Groper (Ping)Test allows you to verify connectivity to remote hosts. The Ping test operates by sending Internet Control Message Protocol (ICMP) request packets to the tested host and waits for an ICMP response. In the process it measures the time from transmission to reception and records any packet loss.Send a ping request to a specified IPv4 address. Check whether the Switch can communicate with a particular network host before testing.



Ping Test Settings

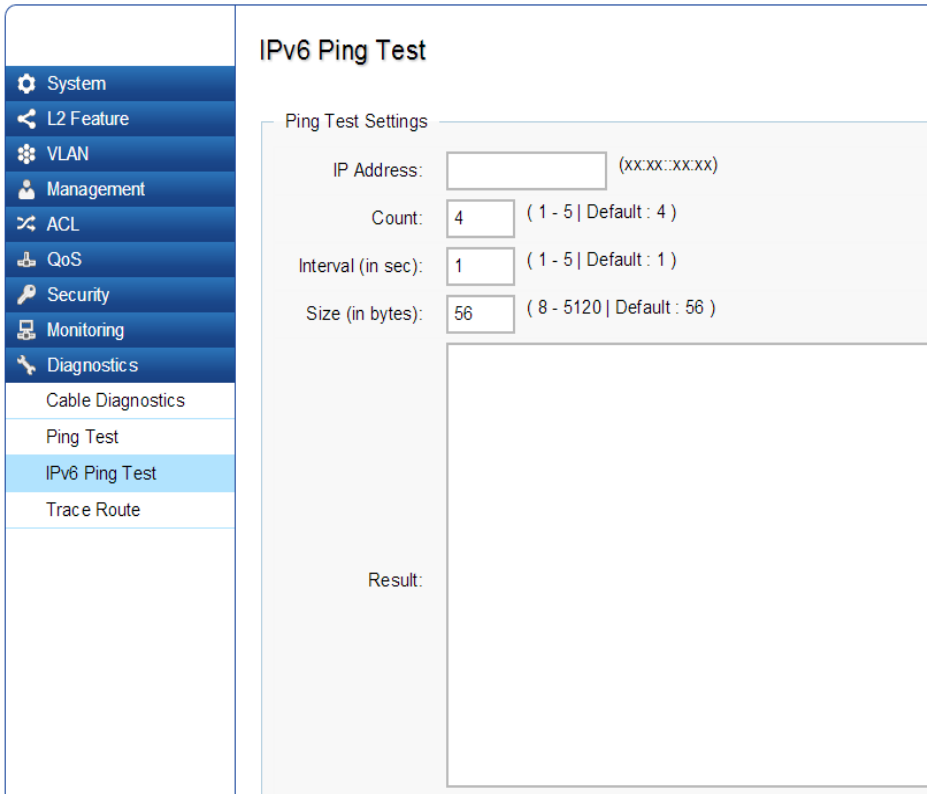
You can vary the test parameters by entering the data in the appropraite boxes. To verify accuracy of the test, it is reccomended that you run multiple tests in case of a test fault or user error.

IP address:	Enter the IP address or the host name of the station you want the Switch to ping to.
Count:	Enter the number of ping to send. The range is from 1-5 and the default is 1.
Interval:	Enter the number of seconds between pings sent. The range is from 1-5 and the default is 4.
Size:	Enter the size of ping packet to send. The range is from 8-5120 and the default is 56.
Result:	Displays the Ping Test results.

Click **Test** to perform the ping tests.

IPv6 Ping Test

Send a ping request to a specified IPv6 address. Check whether the Switch can communicate with a particular network host before testing.



You can vary the test parameters by entering the data in the appropraite boxes. To verify accuracy of the test, it is reccomended that you run multiple tests in case of a test fault or user error.

IP address:	Enter the IPv6 address or the host name of the station you want the Switch to ping to.
Count:	Enter the number of pings to send. The range is from 1-5 and the default is 1.
Interval:	Enter the number of seconds between pings sent. The range is from 1-5 and the default is 4.
Size:	Enter the size of ping packet you wish to send. The range is from 8-5120 and the default is 56.
Result:	Displays the ping test results.

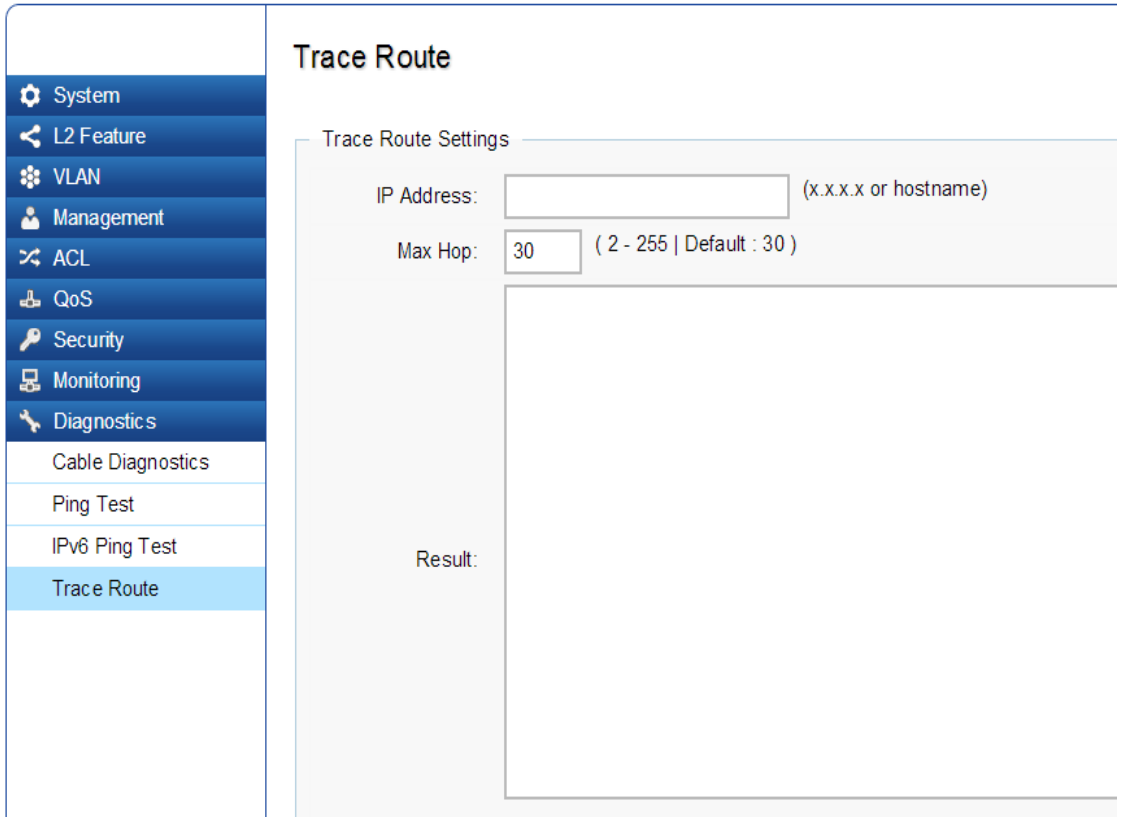
Click **Test** to perform the ping tests.

Trace Route

The traceroute feature is used to discover the routes that packets take when traveling to their destination. It will list all the routers it passes through until it reaches its destination, or fails to reach the destination and is discarded. In testing, it will tell you how long each hop from router to router takes via the trip time of the packets it sends and receives from each successive host in the route.

IP address:	Enter the IP address or the host name of the station you wish the Switch to ping to.
Max Hop:	Enter the maximum number of hops. The range is from 2-255 and the default is 30.
Result:	Displays the trace route results.

Click **Test** to initiate the trace route.



Chapter 3
Maintenance

Maintenance

Maintenance functions are available from the maintenance bar. Maintenance functions include: saving configuration settings, upgrading firmware, resetting the configuration to factory default standards, rebooting the device, and logging out of the interface.

The following represents the Maintenance Menu bar:

Saving Configurations

Important: You must save any setting changes before rebooting. Failure to save results in loss of new configuration changes.

Follow this procedure to save the configuration,

1. Click Save to save the entire configuration changes you have made to the device to Switch.
2. Click **OK**.

Upgrading

WARNING! Backup your configuration information before upgrading to prevent loss of settings information.

Follow this procedure to upgrade the Firmware.

1. Click Upgrade to start upgrading.

1. Click **Choose File**. When a window opens, browse to the location of your new Firmware.

3. Select the new Firmware file and click **OK**.

4. A prompt will displays to confirm the Firmware Upgrade. Click **OK** and follow the on-screen instructions to complete the Firmware Upgrade.

   Note: The Upgrade process may require a few minutes to complete.

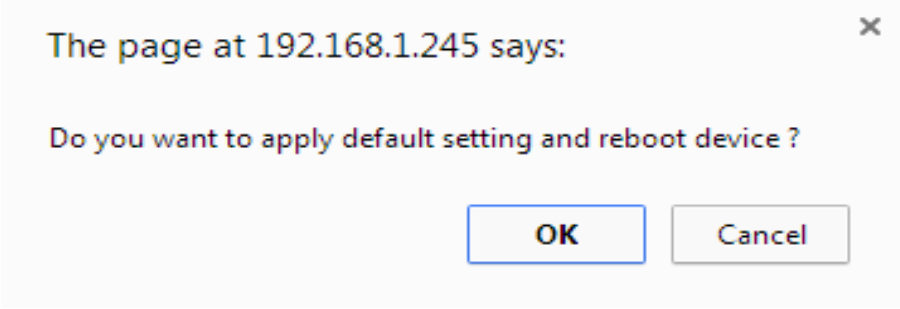
Resetting

WARNING! The Reset function will delete all configuration information from the current device. Backup your information before starting this procedure.

Follow this procedure to reset the Switch back to factory default settings.

1. Click Reset to start the reset process.

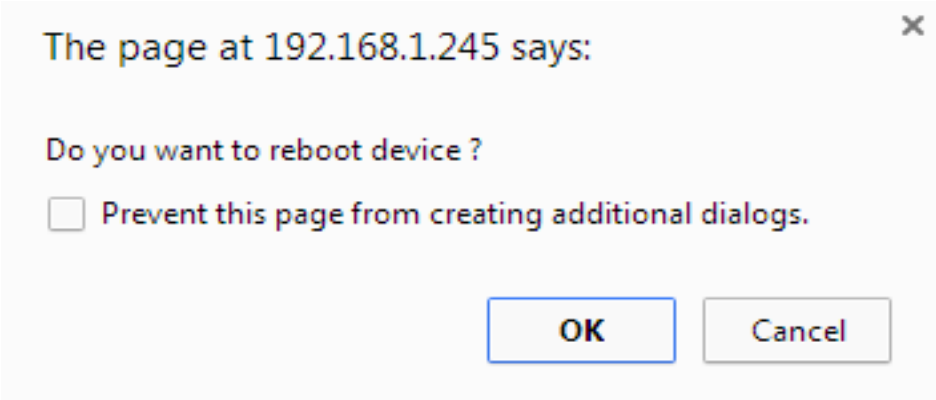
2. When a prompt displays, click **OK** to confirm the reset or **Cancel** to quit the procedure.



Rebooting

Follow this procedure to reboot the Switch.

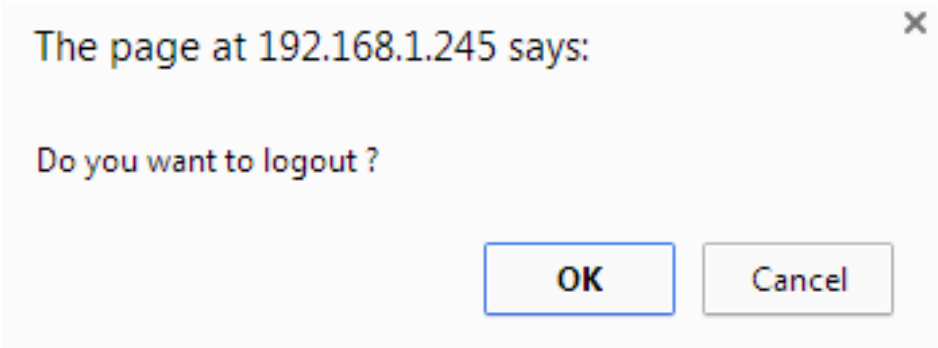
1. Click Reboot to start the reboot process.
2. When a prompt displays, click **OK** to confirm the reboot process or **Cancel** to quit the procedure.



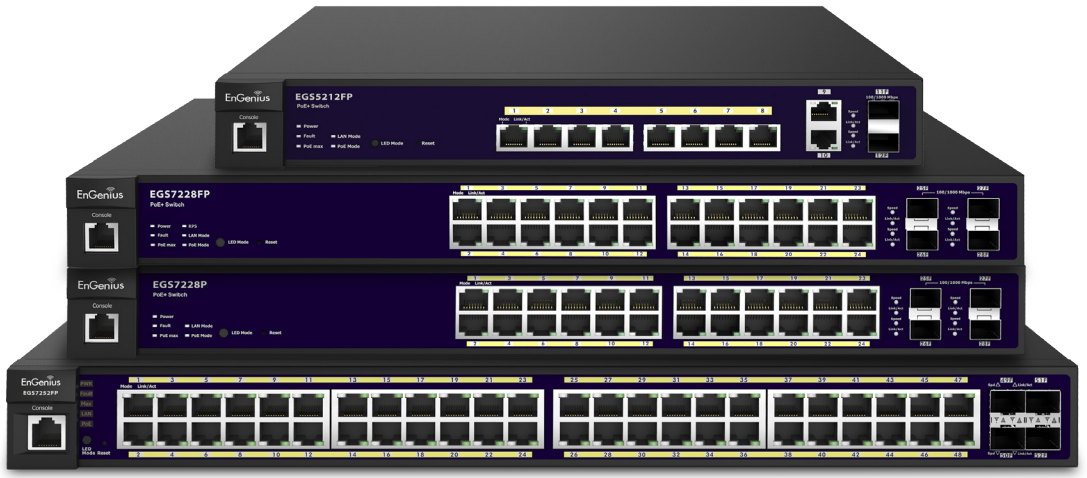
Logging Out

Follow this procedure to log out the current profile from the user interface.

1. Click Logout to log out of the menu.
2. When a prompt shows, click **OK** to confirm logging out or **Cancel** to quit the procedure.



Appendix


EnGenius
EGS5212FP
PoE+ Switch
EnGenius
EGS7228FP
PoE+ Switch
EnGenius
EGS7228P
PoE+ Switch
EnGenius
EGS7252FP

Quick Reference Guide

Hardware Specifications					
Model		**EGS5212FP**	**EGS7228P**	**EGS7228FP**	**EGS7252FP**
Connectors	Gigabit RJ45 Ports	10	24	24	48
	Gigabit SFP Ports	2	4	4	4
	Console Port	1	1	1	1
PoE Features	Standard	IEEE802.3af/at (max 30w per port)			
	PoE Ports	8	24	24	48
	Total PoE Budget	130 W	185 W	370 W	740 W
Power Supply		100-240 VAC, 50/60 Hz			
Environent		Operating Temperature: 32° F~104° F, 0° F -C~40° C Storage Temperature: -40° F~158° F, -40° C~70° C Operating Humidity: 10%~90% (non-condensing) Storage Humidity: 5%~90% (non-condensing)			
Dimensions		330 x 230 x 44mm (13 x 9 x 1.73 inches)	440 x 260 x 44mm (17.3 x 10.2 x 1.7 inches)	440 x 310 x 44mm (17.3 x 12.2 x 1.7 inches)	440 x 410 x 44mm (17.3 x 16.1 x 1.7 inches)"

WARNING!

This switch should be connected only to PoE networks without routing to the outside plant.

Appendix A

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

WARNING!

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the fol- lowing two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Radiation Exposure Statement

WARNING! This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 23cm between the radiator & your body.

Appendix B - IC Interference Statement

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

FOR MOBILE DEVICE USAGE
Radiation Exposure Statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Pour l'utilisation de dispositifs mobiles)
Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20cm de distance entre la source de rayonnement et votre corps.

Appendix C - CE Interference Statement

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- **EN60950-1**
  Safety of Information Technology Equipment
- **EN50385**
  Generic standard to demonstrate the compliance of electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic fields (0 Hz - 300 GHz)
- **EN 300 328**
  Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
- **EN 301 893**
  Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive
- **EN 301 489-1**
  Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements
- **EN 301 489-17**
  Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

This device is a 5GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

CE 0560 !

Česky [Czech]	[Jméno výrobce] tímto prohlašuje, že tento [typ zařízení] je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede [fabrikantens navn] erklærer herved, at følgende udstyr [udstyrets typebetegnelse] overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt [Name des Herstellers], dass sich das Gerät [Gerätetyp] in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab [tootja nimi = name of manufacturer] seadme [seadme tüüp = type of equipment] vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, [name of manufacturer], declares that this [type of equipment] is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente [nombre del fabricante] declara que el [clase de equipo] cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ [name of manufacturer] ΔΗΛΩΝΕΙ ΟΤΙ [type of equipment] ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.

Français [French]	Par la présente [nom du fabricant] déclare que l'appareil [type d'appareil] est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente [nome del costruttore] dichiara che questo [tipo di apparecchio] è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo [name of manufacturer / izgatavotāja nosaukums] deklarē, ka [type of equipment / iekārtas tips] atbilst Direktīvas 1999/ 5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo [manufacturer name] deklaruoja, kad šis [equipment type] atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart [naam van de fabrikant] dat het toestel [type van toestel] in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, [isem tal-manifattur], jiddikjara li dan [il-mudel tal-prodott] jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, [gyártó neve] nyilatkozom, hogy a [... típus] megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym [nazwa producenta] oświadcza, że [nazwa wyrobu] jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	[Nome do fabricante] declara que este [tipo de equipamento] está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	[Ime proizvajalca] izjavlja, da je ta [tip opreme] v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	[Meno výrobcu] týmto vyhlasuje, že [typ zariadenia] spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	[Valmistaja = manufacturer] vakuuttaa täten että [type of equipment = laitteen tyyppimerkintä] tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar [företag] att denna [utrustningstyp] står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.