WATERS NETWORK SYSTEMS™

OPERATING MANUAL

MS1008-2G-4POE/PSX1008-2G-4PoE Switch

Managed Switch with Eight 10/100/1000Base-TX Ports

Plus One Mini GBIC slot for 1000Base-SX or LX fiber

or one 10/100/1000Base-TX port

Four PoE Ports

CORPORATE HEADQUATERS

5001 American Blvd. W., Suite 605

Bloomington, MN 55437

Phone: 800.441.5319

Phone: 952.831.5603

Fax: 952.831.5605

MANUFACTURING/CUSTOMER SERVICE

945 37th Avenue, NW

Rochester, MN 55901

Phone: 800.328.2275

Phone: 507.252.1951

Fax: 507.285.1952

Web site: http://www.watersnet.com

Table of Contents

1.0 Specifications

OPERATIONAL CHARACTERISTICS:

MAC Address Table:	8k
Switching Mode:	Store-and-forward
Bandwidth:	Up to 18Gbps
System Throughput:	Up to 26.7Mbps (64bytes packet length)
Memory Buffer Size:	1Mb
Performance:	Non-blocking wire speed

MANAGEMENT FEATURES:

Web-based, Telnet and console
SNMP
SNMP IP security (supports 4 IP accounts)
RMON
Port setting for duplex and speed
Port trunking (3 groups)
Port based and tagged VLANs (up to 256)
QoS
IGMP (Supports 256 IGMP groups and IGMP query)
GVRP (256 groups)
Port security
Port mirroring
Broadcast storm
Spanning Tree
SMTP
System Log
DHCP
SNTP

NETWORK STANDARDS:

IEEE 802.3
IEEE 802.3u
IEEE 802.3z
IEEE 802.3x
IEEE 802.3ab
IEEE 802.3ad
IEEE 802.1d
IEEE 802.1s

IEEE 802.1w
IEEE 802.1d
IEEE 802.1p
IEEE 802.1q
IEEE 802.1x

EMI/SAFETY COMPLIANCE:

FCC Class A, CE, UL cUL, CE/EN60950

NETWORK CABLE CONNECTORS

RJ45 shielded female ports
10/100Mbps: CAT5 UTP or better
Multimode: LC
Singlemode: LC

POWER SUPPLY:

Input Voltage
90 to 240 VAC, 50 to 60Hz

Power Consumption

10 watts maximum

OPERATING ENVIRONMENT:

Ambient Temperature:
32° to 140°F (0° to 60°C)
Storage:
14° to 158°F (-10°to 70°C)
Ambient relative humidity:
5% to 90% (non-condensing)

MECHANICAL:

Enclosure:
Rugged high-strength sheet metal suitable for stand-alone, wall or tabletop mounting
Cooling Method: Internal fan

PHYSICAL CHARACTERISTICS:

GSM2109:
Dimensions:
8.5 x 5.5 x 1.75 in (216 x 140 x 45mm)
Weight:
2 lbs (.91kg)

GSM1009-1SFP:
Dimensions:
11 x 10.5 x 2 in (279 x 267 x 51mm)
Weight:
3.7lbs (1.68kg)

Warranty:

Limited Lifetime

2.0 Package Contents

Examine the shipping container for obvious damage prior to installing this product. Notify the carrier of any damage that you believe occurred during shipment. Ensure that the items listed below are included. If an item is missing, please contact your supplier. Both the MS1008-2G-4PoE and PSX1008-2G-4PoE switch package contains the following:

- Switch
- Power Cord
- Four Rubber Feet
- RS-232 cable
- User's Guide

3.0 Introduction

In our modern society, communication and sharing information is essential to our lives. Computer networks have proven to be one of the fastest methods of communication.

The switch is a compact desktop size switch that is an ideal solution for any network user. The switch provides high-performance managed switching functions with low-cost connectivity. The switch features store-and-forward switching and will auto-learn and store source addresses with an 8K-entry MAC address table.

Figure 3.1 - PSX1008-2G-4PoE switch

The switch provides eight switched auto-sensing 10/100Base-TX RJ45 ports plus one mini GBIC and one 10/100/1000Base-TX port. The switch provides nine usable ports.

The ninth port can be used for 1000Base-SX fiber connectivity or for 10/100/1000Base-TX connectivity.

Four of the 10/100Base-TX ports provide Power over Ethernet (PoE) connectivity. The PoE ports eliminates the need to run 110/220 VAC power to other devices on the LAN. The same CAT5 Ethernet cable that carries data to each device can also deliver power over the same cable. This allows greater flexibility in the location of network devices and can help reduce installation costs.

There are two system components for PoE: the power sourcing equipment (PSE) which initiates the connection to the second component--the powered device (PD). The current is transmitted over two of the four twisted pairs of wires in a CAT5 cable.

The PoE ports follow the IEEE 802.3af standard and are completely compatible with existing Ethernet switches and networked devices. Because the PSE tests whether a networked device is PoE-capable, power is never transmitted unless a PD is located at other end of the cable. It also continues to monitor the channel. If the PD does not draw a minimum current because it has been unplugged or physically turned off, the PSE shuts down the power to that port. Optionally, the standard permits PDs to send a signal to the PSEs for their power requirement.

The switch will automatically detect the speed of connected devices to accommodate 10, 100, 1000Mbps on the RJ45 ports. All RJ45 ports support the **Auto MDI/MDIX** function. With the built-in Web-based management functionality, managing and configuring the switch is easy. From cabinet management to port-level control and monitoring, you can visually configure and manage your network via your Web Browser. The switch can be managed via a web browser, Telnet, CLI (command line interface) commands or SNMP Management.

Ethernet switching technology dramatically boosted the total bandwidth of a network,

eliminating congestion problems inherent with the carrier sense multiple access with the collision detection (CSMA/CD) protocol and greatly reduced unnecessary transmissions.

This revolutionized networking. First, by allowing two-way, simultaneous transmissions over the same port (full-duplex), bandwidth was essentially doubled. Second, by reducing the collision domain to a single switch-port, the need for carrier sensing was eliminated. Third, by using the store-and-forward technology's approach of inspecting each packet to intercept corrupt or redundant data, switching eliminated unnecessary transmissions that slow down network traffic.

Auto-negotiation regulates the speed and duplex of each port, based on the capability of both devices. Flow-control allows transmission from a 100Mbps node to a 10Mbps node without loss of data. Auto-negotiation and flow-control may have to be disabled for some networking operations that involve legacy equipment. Disabling the auto-negotiation is accomplished by hard setting the speed or duplex mode of a port.

3.1 Switch Features

- 8-port 10/100Base-TX RJ45 ports
- One mini GBIC slot for SFP module for 1000Base-SX or LX fiber connectivity or one 10/100/1000Base-TX port
- Embedded 4-port PoE inject function
- Conforms to IEEE 802.3, 802.3u, 802.3x, 802.3z, and 802.3ab Ethernet Standards
- Auto-sensing 10/100/1000Base-TX RJ45 port ports
- Automatic MDI/MDIX crossover for each 10/100Base-TX port
- Console port on front side for system configuration
- Half-duplex mode for backpressure
- Full-duplex for flow control
- Store-and-forward switching architecture
- Automatic address learning, address migration
- 8K-entry MAC address table

- 5.6Gbps switch bandwidth
- IGMP snooping
- GVRP function
- 802.1x user authentication
- 802.1p CoS per port 4 queues
- Port based VLAN 802.1q VLAN
- 802.3ad port trunk with LACP
- STP/RSTP
- QoS
    - Port based / tag based
    - IPv4 Tos/Ipv4, Ipv6 DiffServe
- Port mirror and bandwidth control
- 802.1x user authentication
- GVRP and MVR function
- Broadcast storm filter
- DHCP client, relay, server
- SNTP and SMTP
- Management IP address security
- MAC address security
- System log
- SNMP trap support
- TFTP firmware update
- Web/SNMP/Telnet/CLI//MenuDrivenRMON
- Performs non-blocking full wire speed
- Configuration upload and download
- Supports X-ring function

3.2 Software Features

RFC Standard	RFC2233 MIBII, RFC 1157 SNMP MIB, RFC 1493 Bridge MIB, RFC 2674 VLAN MIB, RFC 2665 Ethernet like MIB, RFC1215 Trap MIB, RFC 2819 RMON MIB, Private MIB, RFC2030 SNTP, RFC 2821 SMTP, RFC 1757 RMON1 MIB, RFC 1215 Trap
Management	SNMP v1, SNMP v2c, SNMP v3, Telnet, Console (CLI), Web management and menu driven
SNMP Trap	Cold start, warm start, link down, link up, authorization fail, Trap station up to 3.
Port Trunk	Supports IEEE802.3ad with LACP function. Up to 3 trunk groups and maximum group member up to 4 ports.
Class of Service	Per port supports 4 queues. Weight round ratio (WRR): High: Mid-High: Mid-Low: Low (8:4:2:1)
QoS	Port based, Tag based, IPv4 Type of service, Ipv6 Different service.
VLAN	Port based VLAN Double Tag VLAN for management IEEE802.1Q Tag VLAN. Static VLAN groups up to 256 Dynamic VLAN groups up to 2048 VLAN ID can be assigned from 1 to 4094. GVRP function supports 256 groups.
IGMP	IGMP v1 and v2 compliance and also supports 256 IGMP groups and support query mode.

Port Security	Supports ingress and egress MAC address filter and static source MAC address lock.
Port Mirror	Global system supports 3 mirroring types: “RX, TX and Both packet”. The maximum of port mirror entries is 8.
Bandwidth Control	Ingress rate limiting packet type: all of frames, broadcast, multicast, unknown unicast and broadcast packet. Egress rate shaping supports all of packet. Rate limiting levels: 64kbps to 64Mbits or up to 256Mbits for Gigabit port.
User Authentication	Support IEEE802.1x User-Authentication and can report to RADIUS server. ▪ Reject ▪ Accept ▪ Authorize ▪ Disable
DHCP	DHCP Client, DHCP relay and DHCP Server. DHCP server provides global IP pool for DHCP server.
Packet filter	Broadcast storm packet filter by 5%, 10%, 15% and 25%.
Port Security	Supports ingress and egress MAC address filter and static source MAC address lock
System log	Provide 1000 log entries and supports remote storage function.
SNMP IP security	Supports 10 IP address accounts for system management security for web, SNMP, Telnet to prevent intruders.
SMTP	6 mail accounts.
SNTP	Supports RFC2030 simple network time protocol

Configuration upload and download	Support binary format configuration file for system quick configuration.
Spanning Tree	IEEE802.1d Spanning tree IEEE802.1w Rapid spanning tree
X-ring	Provides X-ring, dual homing and coupling ring. Provides redundant backup feature and recovery time below 300ms
PoE management	PoE Enable/Disable; Power limit by classification: Enable/ Disable PD power classification and output power will be limited by PD's classification. Power limit by management: Enable power feeding priority Priority: Per port power feeding priority setting. Once current power output is out of switch's ability, power will be shut down. Detect Legacy Signature: The goal of Detect Legacy Signature is to identify these devices based on their unique electrical signatures (resistive and capacitive) and power them up as selectively as possible. Some of CISCO PD devices are pre-standard and do not follow 802.3af with exactly electrical signature. If that is the case, this function should be enabled.

Table 3.1 – Software Features

3.3 Management Methods

The switch supports following management methods:

- Console and Telnet Management
- Web-based Management
- SNMP Network Management

3.3.1 Console and Telnet Management

Console Management is done through the RS-232 Console Port. Use the RS-232 cable supplied in your package to connect directly to a workstation from your switch. Use the default IP **192.168.16.1** to use Telnet or Web Management to login to the switch and modify the configuration.

3.3.2 Web-based Management

The switch provides an embedded HTML web site residing in flash memory. It offers advanced management features and allow users to manage the switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

3.3.3 SNMP Network Management

SNMP (Simple Network Management Protocol) provides a means to monitor and control network devices, manage configurations, collect statistics, performance and security information.

3.4 Hardware Description

Front Panel

The front panel of the switch consists of eight auto-sensing 10/100Base-TX RJ45 (Ports 5-8 PoE ports) ports, one mini GBIC slot and one 10/100/1000Base-TX port. The ninth 10/100/1000Base-TX port shares the slot with the mini GBIC. So, if the GBIC is used, the ninth 10/100/1000Bse-TX port is inactive. Therefore, the switch provides nine usable ports. You have the choice of using the ninth port in copper or fiber. The LED indicators are also located on the front panel of the switch.

The console connection is also on the front panel of the switch. The console port can be used to perform management functions. Console connection requires a direct connection between the switch and a workstation with a RS-232 cable.

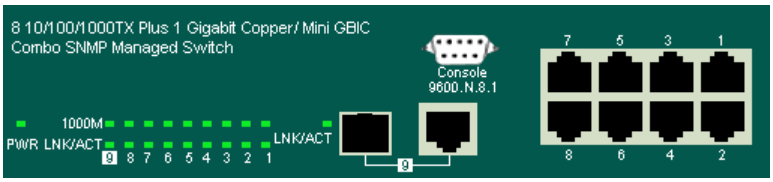


Figure 3.2 - Front Panel

Rear Panel

A three-pronged AC power plug is located on the rear panel of the switch. The switch operates in the range 100-240V AC, 50-60Hz.

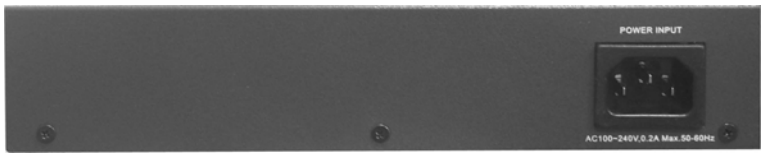


Figure 3.3 - Rear Panel

Hardware Ports

- One slot for mini GBIC
- One 10/100/1000Base-TX port
- Eight 10/100Base-TX connections. MDI allows you to connect to another hub or switch and MDIX allows you to connect to a workstation or PC. Therefore, **Auto MDI/MDIX** means that you can connect to another switch or workstation without a crossover cable.

3.5 LED Indicators

The following table provides the status and description of the LEDs. The LEDs provide a real-time indication of systematic operation status.

LED	Status	Color	Description
Power	On	Green	Power On
1000M (Port 9)	On	Green	The port is operating at 1000Mbps.
	On	Orange	The port is operating at 100Mbps
	Off		No device attached
FWD (Ports 5-8)	On	Green	The port is supplying power to the powered device.
	Off		No powered device is attached or power failed.
100M (Ports 1-9)	On	Green	The port is operating at 100Mbps.
	Off		No device attached.
LNK/ ACT	On	Green	The port is connecting with the device.
	Blinks	Green	The port is receiving or transmitting data.
	Off		No device attached.
FDX/ COL	On	Orange	The port is operating in full-duplex mode.
	Blinks	Green	Packet collisions occurring.
	Off		The port is operating in half-duplex mode.

Table 3.2 - LED Description

3.6 Desktop Installation

Choose a surface for your switch that is clean, smooth, level, sturdy and with a power outlet nearby. Make sure there is enough clearance around the switch to allow attachment of cables, power cord and air circulation.

3.6.1 Attaching Rubber Feet

1. Make sure the mounting surface on the bottom of the switch is free of grease and dust.
2. Remove adhesive backing from the rubber feet.
3. Apply the rubber feet to each corner on the bottom of the switch.

3.6.2 Power On

Connect the power cord to the AC power socket on the rear panel of the switch. Check the power indicator on the front panel to see if power is properly supplied.

4.0 Network Applications

This section provides samples of network topology in which the GSM2109/1009 switch can be used. This model switch is generally used as a desktop, workgroup or edge segment switch.

Desktop Application

The switch provides an ideal solution for small workgroups. The switch can be used as a standalone switch to which personal computers, servers, and print servers are directly connected to form a small workgroup.

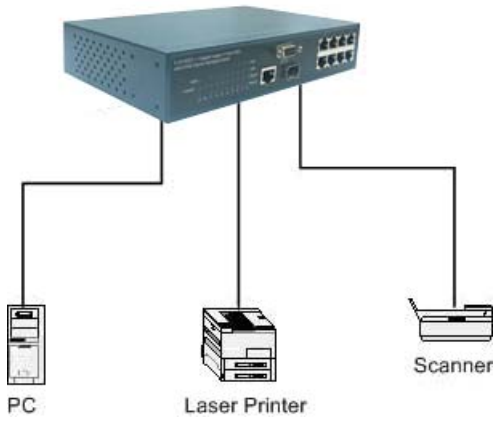


Figure 4.1 – Workgroup/Classroom Application

Segment Application

For enterprise networks where large data packets are constantly processed, this switch is suitable for department users to connect to the corporate backbone. The switch automatically learns node addresses, which are subsequently used to filter and forward all traffic based on the destination address. You can use any of the copper ports or the mini GBIC port to connect with another switch to interconnect each of your small-switched workgroups to form a larger switched network.

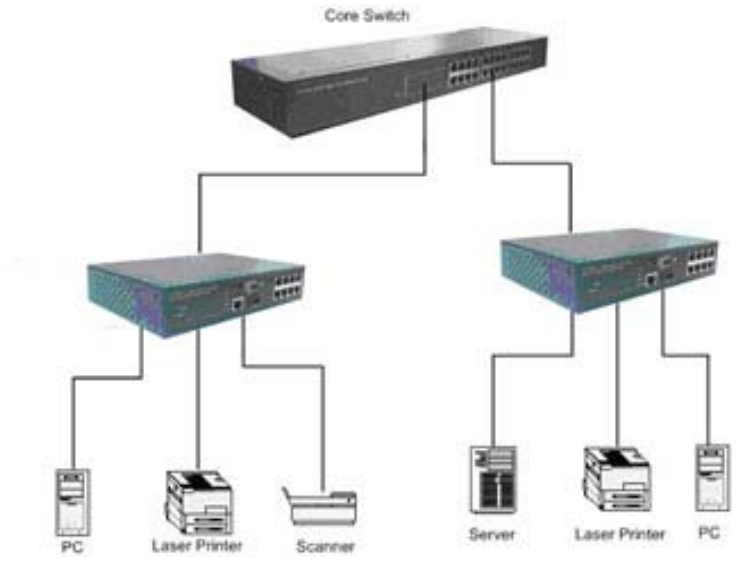


Figure 4.2 – Segment Application

PoE

The four-port PoE switch provides power to the powered devices that follow the IEEE 802.3af standard on the network. The following figure provides an example of a network application for PoE.

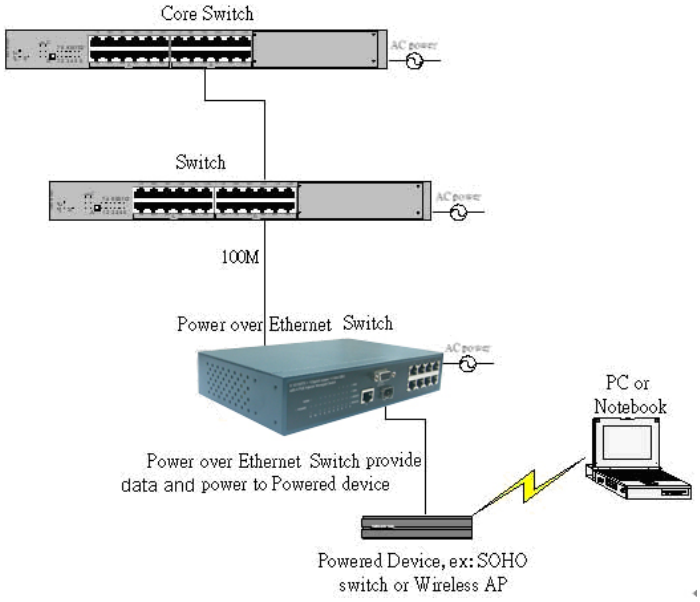


Figure 4.3 – PoE Switch with Wireless Powered Device

4.1 Network Configuration

This section explains how to configure console management via a direct connection to the console port of the switch. Console management involves the administration of the switch via a direct connection to the RS-232 console port. This port is a female DB-9 connector. From the **Main Console Management Menu,** you have access to all of the management functions of the switch.

Connecting a Terminal or PC to the Console Port

Use the supplied RS-232 cable to connect a terminal or PC to the console port. The terminal or PC to be connected must support the terminal emulation program.

After the connection between switch and PC is made, run a **terminal emulation program** or **Hyper Terminal** to match the following default characteristics of the console port:

Baud Rate:	**9600 bps**
Data Bits:	**8**
Parity:	**None**
Stop Bit:	**1**
Flow Control:	**None**

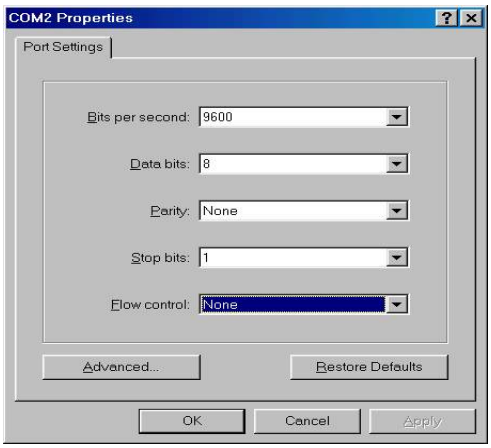


Figure 4.4 - Communication Parameters

1. Press **Enter** once you have entered the parameters listed above.
2. Turn on the switch. The switch will display a series of messages as it performs a self test. Once the self test is completed, the login screen will be displayed.

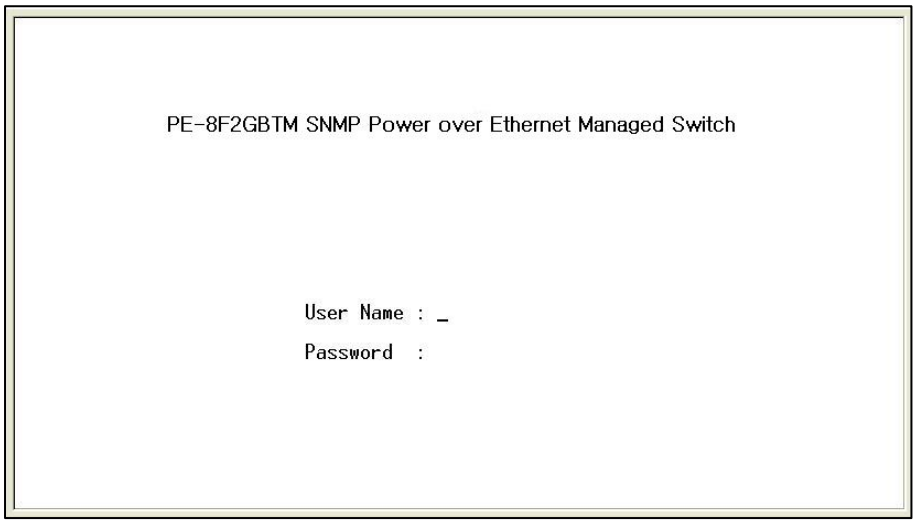


Figure 4.5 - Console Login Interface

3. Enter the user name and password.
4. The default user name is **root**, and the default password is **root**. You may change the login identification to make it more secure for your network in the **System Configuration** menu.
5. Once you have logged into the system, a command prompt will be displayed. The switch provides CLI (command line interface) console management. Once you have logged into the switch, you can begin entering CLI commands. **Section 6.0** lists the commands and their descriptions.

5.0 Web Based Management

This section covers the functions of web based management. There is an embedded HTML web site residing in flash memory in the CPU board of the switch. Web based management provides advanced management features for the network administrator that can be accessed from anywhere on the network through a standard web browser such as Microsoft Internet Explorer (IE).

The web based management supports IE 5.0. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

Note: By default, IE5.0 or later versions do not allow Java Applets to open sockets. The browser settings should be modified to enable Java Applets to use network ports.

5.1 Workstation Settings for Web Management

Before the management functions can be accessed via the web, use the console connection to login to the switch to check the IP address of the switch. The default IP address is:

- **IP Address**: 192.168.16.1
- **Subnet Mask**: 255.255.255.0
- **Default Gateway**: 192.168.16.254
- **User Name**: root
- **Password**: root

5.2 Login via the Web

1. Launch **IE**.
2. Enter the **IP address** of the switch and press **Enter.**
   Example: http://192.168.16.1
3. The login screen will be displayed.
4. Enter the user name and password. The default user name and password is **root**.
5. Click **Enter** or **OK**.

6. The main menu of for web based management will be displayed.

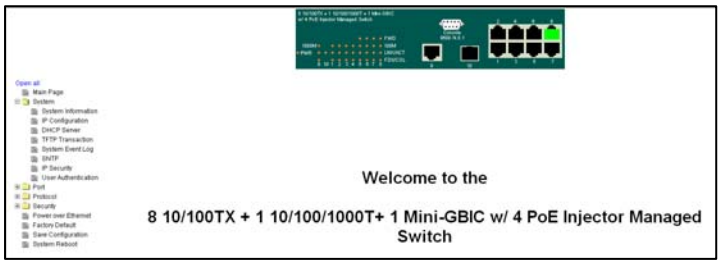


Figure 5.1 - Web Management Opening Screen

5.3 System Information

Use the **System Information** menu to enter the following system information:

- **System Name** - assign a name for the switch. The maximum length is 64 bytes.
- **System Description** - displays the description for the switch. The information is **read only** and cannot be modified.
- **System Location** - assign the physical location for the switch. The maximum length is 64 bytes.
- **System Contact** – assign a contact for the switch.

The following information is displayed on this screen:

- **Firmware Version** - displays the firmware version for the switch.
- **Kernel Version** - displays the kernel software version.
- **MAC Address** - displays the unique hardware address assigned by manufacturer (default).

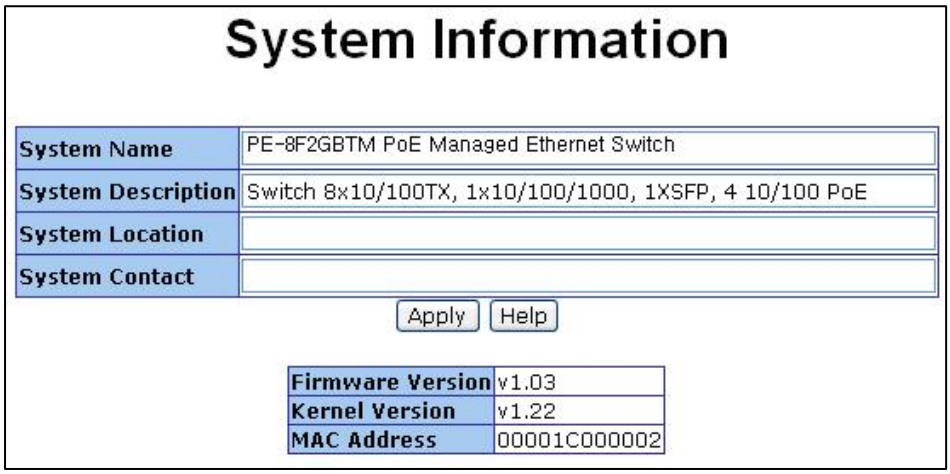


Figure 5.2 - System Information Screen

5.4 IP Configuration

This menu allows you to change the **IP address** for the switch as well as reconfigure IP settings. Once the IP address has been set, the switch must be rebooted. DHCP Client is disabled by default.

- **IP Address** – Use this option to assign the switch IP address. The default IP address is 192.168.16.1.
- **Subnet Mask** - Use this option to assign the switch IP subnet mask.
- **Gateway** – Use this option to assign the switch gateway. The default gateway value is 192.168.16.254.
- **DNS1** – DNS1 is short for Domain Name Server. DNS is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember, however, the Internet is based on IP addresses. Each time a user accesses the domain name of a web page, a DNS service must translate the name into the corresponding IP address. For example, the domain name **www.net.com** might translate to **192.168.1.1**.
- **DNS2** - DNS2 is the backup for DNS1. If the DNS1 cannot function, the DNS2 will replace DNS1.

Figure 5.3 – IP Configuration

5.5 DHCP Server

Dynamic Host Configuration Protocol (DHCP) is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device may have a different IP address every time it connects to the network. In some systems, the IP address may change while connected. DHCP supports a combination of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than an administrator managing this task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

5.5.1 DHCP Server Configuration

The switch provides the following DHCP server functions once DHCP has been enabled.

- **DHCP Server** - Enable or Disable the DHCP Server function. If enabled, the switch will be the DHCP server on your LAN.
- **Low IP Address** – Low IP address is the first of the dynamic IP numbers to be assigned. For example, if the dynamic IP assign range is from *192.168.1.100 ~ 192.168.1.200*, 192.168.1.100 will be the Low IP address.
- **High IP Address** - High IP address is the last of the dynamic IP numbers to be assigned. In the example listed above, the High IP address would be 192.168.1.200.

- **Subnet Mask** - The dynamic IP assigned range for subnet mask.
- **Gateway** - The gateway of your network.
- **DNS** – The Domain Name Server IP Address of your network.
- **Lease Time (sec)** – Specifies in seconds the time period that the system will reset the dynamic IP assignment.

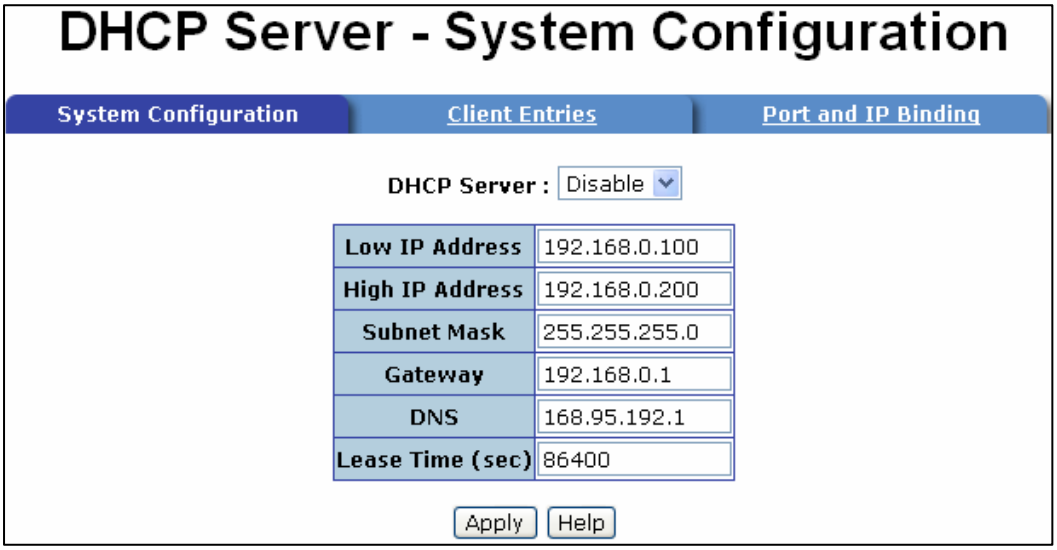


Figure 5.4 - DHCP Server Configuration

When the DHCP server function is enabled, the system will collect DHCP client information which will be displayed in the DHCP Client Entry screen.

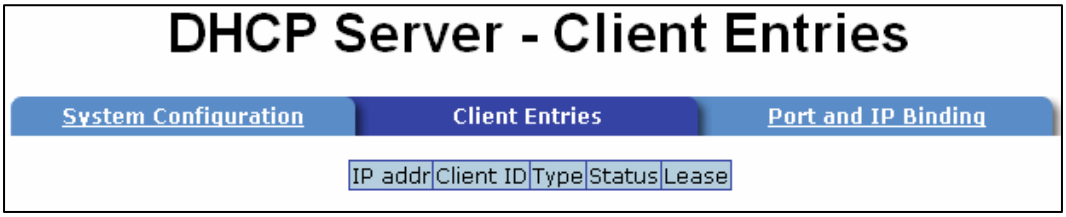


Figure 5.5 - DHCP Client Entries Screen

5.6 Port and IP Bindings

The switch allows you to assign a specific IP address that is in the dynamic IP range to a specific port. When the device is connecting to the port and requests a dynamic IP assignment, the system will assign the IP address that has been previously assigned to the connected device.

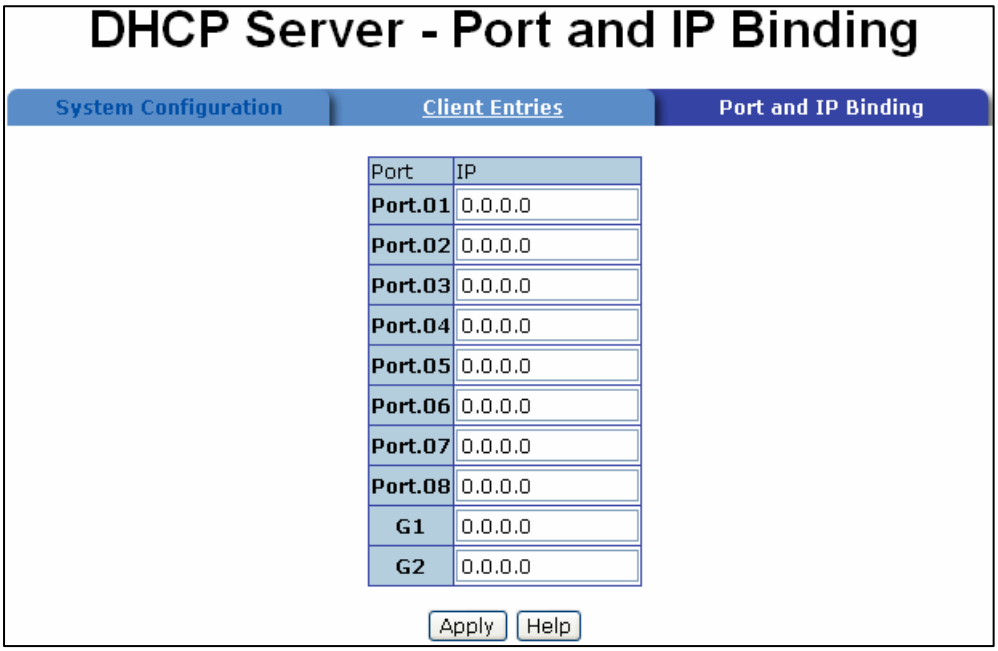


Figure 5.6 - Port and IP Bindings Screen

5.7 TFTP Transaction

The **TFTP Transaction** Menu allows you to update the switch firmware, restore EEPROM value or backup current EEPROM value.

1. Start the **TFTP server**.
2. Copy the new firmware version image file to the **TFTP server**.
3. Enter the **IP address** of the TFTP server.
4. Click **Apply** to proceed with the update.

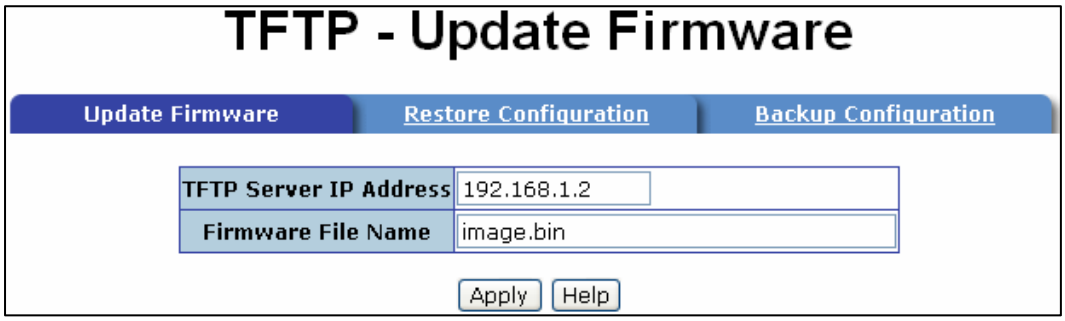


Figure 5.7 - Update Firmware Screen

5.8 Restore Configuration

You can restore the EEPROM value from the TFTP server:

1. Fill in the **TFTP server IP address**.
2. Enter the correct **Restore File Name**.
3. Click **Apply** to proceed.

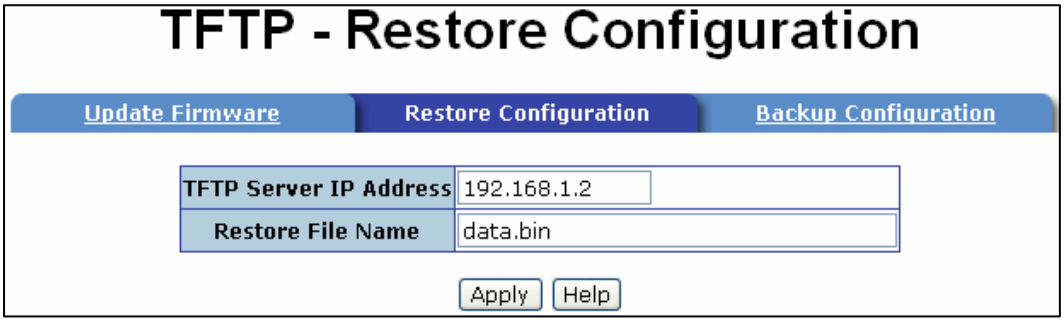


Figure 5-8 - Restore Configuration Screen

5.9 Backup Configuration

This menu allows you to save the current EEPROM value from the switch to the TFTP server.

1. Fill in the **TFTP server IP address**.
2. Enter the correct **Backup File Name**.
3. Click **Apply** to proceed.

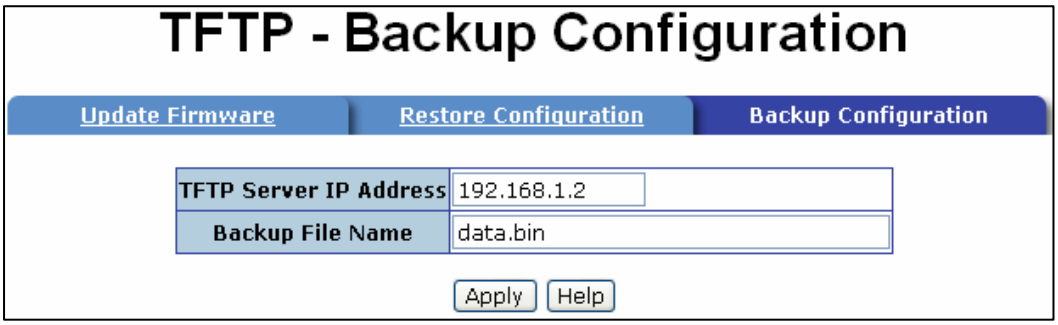


Figure 5.9 - Backup Configuration Screen

5.10 System Event Log Menu

The **System Event Log** Menu allows you to configure the switch so you can collect and view system events.

1. Select the **System Log Mode**: client only, server only, or both client and server.
2. Assign the **system log server IP**.
3. Click **Reload** to refresh the events log.
4. Click **Clear** to clear the current events log.

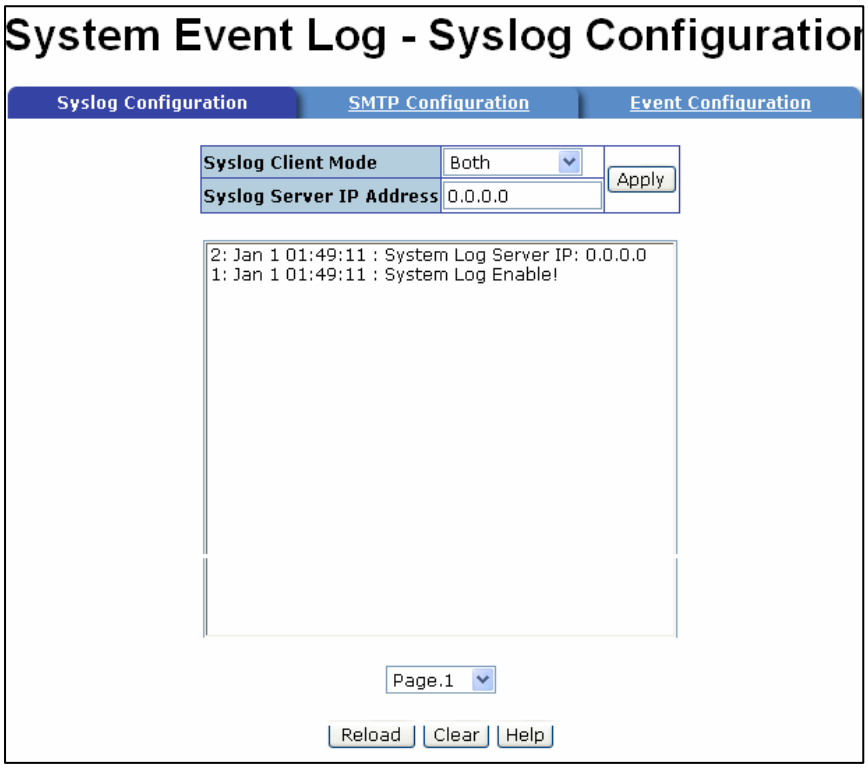


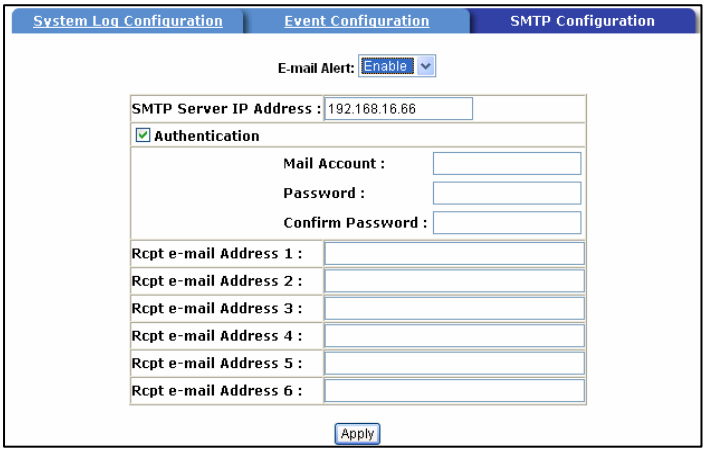
Figure 5.10 – System Log Configuration

5.11 SMTP Configuration

The system can be configured to send an alert to an email account when specific events occur. The following options can be configured for event notification:

- **Email alert** – enable or disable the email alert function
- **SMTP Server IP** – assign the mail server IP address. (When the Email Alert is enabled, this function will be available.)
- **Authentication** –enable and configure the email account and password for authentication. (When the Email Alert is enabled, this function will be available.)
- **Mail Account** – configure email account to receive the alerts. Ex: johnadmin@123.com. The email account must exist on the mail server configured in **SMTP Server IP Address** column.
- **Password** - email account password

- **Confirm Password** - confirm password
- **Rcpt email address 1 ~ 6** – up to six email accounts can be assigned to receive the alert.



5.11 - SMTP Configuration Screen

5.12 Event Configuration

The **Event Configuration** allows you to select SMTP events. When selected events occur, the system will send out the log information or alerts. Per port log and SMTP events can also be selected.

- **Device cold start** – the system will produce a log event when the device executes a cold start action.
- **Device warm start** – the system will produce a log event when the device executes a warm start.
- **Authentication Failure** – the system will produce a log event when the SNMP authentication fails.
- **X-ring topology change** - – the system will produce a log event when the X-ring topology changes.

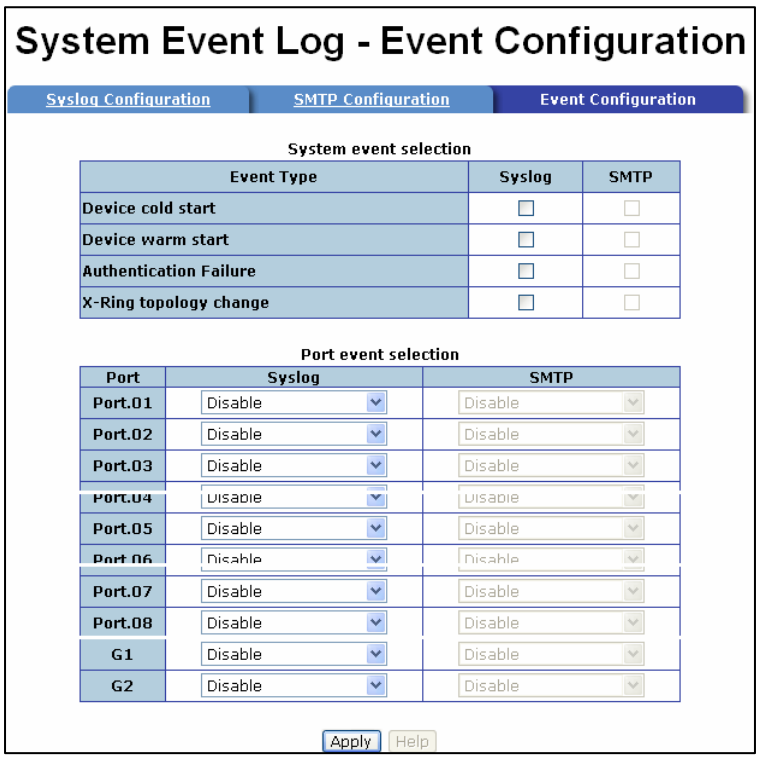


Figure 5.12 - Event Configuration Screen

- **Port Event Selection** – There are three choices for per port events and per port SMTP events. Disabled indicates that no event is selected.
    - **Link Up** - the system will produce a log message when port connection is up only.
    - **Link Down** - the system will produce a log message when port connection is down only.
    - **Link Up & Link Down** - the system will produce a log message when port connection is up and down.

5.13 SNTP Configuration

Use this menu to configure the Simple Network Time Protocol (SNTP) settings. The SNTP synchronizes the switch clock with the Internet.

- **SNTP Client** – set the SNTP function to enable or disable**. SNTP** is disabled by default.
- **Daylight Savings Time** - enable or disable the daylight savings time function. When daylight saving time is enabled, you must also set the daylight savings time period.
- **UTC Timezone** - set the switch location time zone. Use the following table as a reference for the different time zone locations.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian	+10 hours	10 pm

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
Standard GST Guam Standard, USSR Zone 9		
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

Table 5.1 – Time Zone Information

- **SNTP Sever URL** - set the SNTP server IP address.
- **Daylight Saving Period** – enter the start and end period for daylight savings time. The daylight savings ending time will different in every year.
- **Daylight Saving Offset (mins)** - set the offset time.
- Switch Timer - displays the switch current time.

Click **Apply** to save the configuration.

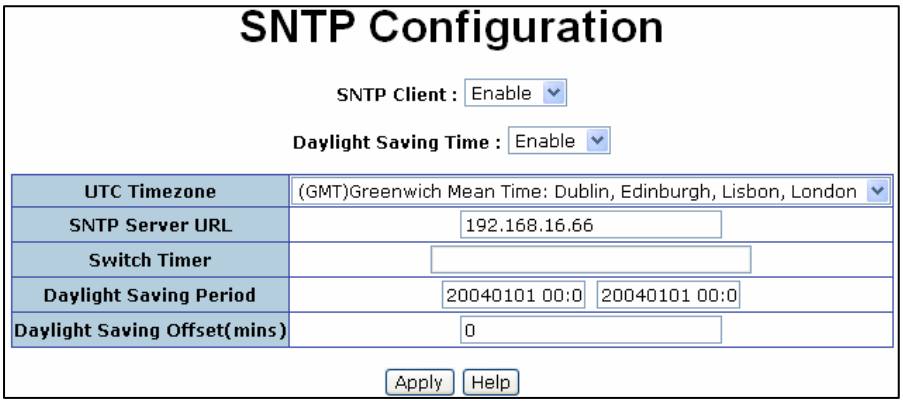


Figure 5.13 – SNTP Configuration

5.14 IP Security

IP security allows you to assign ten specific IP addresses that have permission to access the switch through the web browser for secure switch management. The following lists the functions for IP security:

- **IP Security Mode** – The IP Security mode must be enabled in order to configure the HTTP server and the Telnet server.
- **Enable HTTP Server** – Once this is enabled, the ten IP addresses will be able to access the management functions via the web.
- **Enable Telnet Server** - Once this is enabled, the ten IP addresses will be able to access the management functions via Telnet.
- **Security IP 1 ~ 10** – Assign up to ten specific IP addresses. Only those ten IP addresses can access and management the switch through the web browser.

Click **Apply** to save the configuration.

Note: Remember to execute **Save Configuration** to save the new settings.

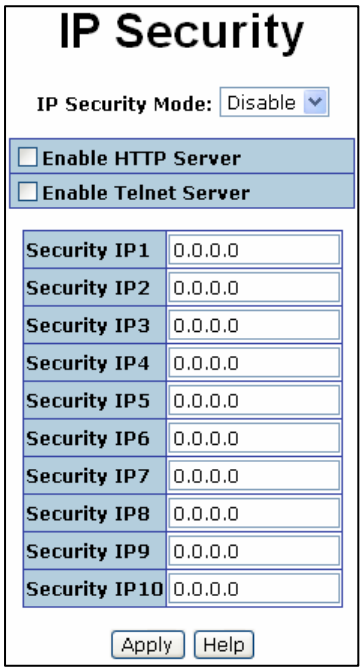


Figure 5.14 – IP Security Settings

5.15 User Authentication

User authentication is used to modify login user name and password:

- **User name** – key in the new user name. The default is **root**.
- **Password** - key in the new password. The default is **root**.
- **Confirm password** - Retype the new password for confirmation.

Click **Apply** to save the configuration.

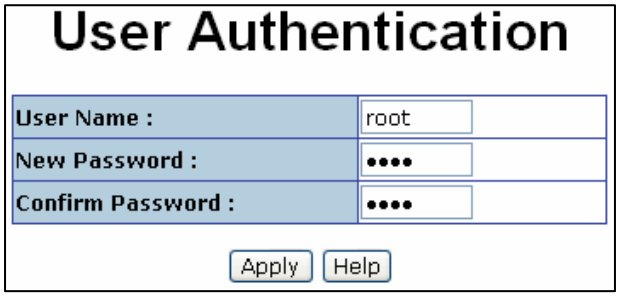
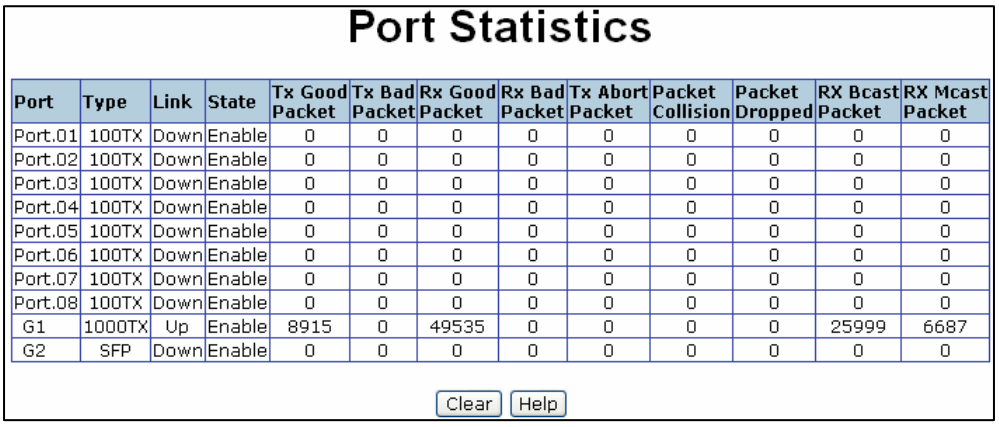


Figure 5.15 – User Authentication

5.16 Port Menu

This menu provides information for all switch ports.

The **Port Statistics** screen provides statistics for current port traffic. You can use the Clear button to clean out off of the counts.



Port	Type	Link	State	Tx Good Packet	Tx Bad Packet	Rx Good Packet	Rx Bad Packet	Tx Abort Packet	Packet Collision	Packet Dropped	RX Bcast Packet	RX Mcast Packet
Port.01	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.02	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.03	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.04	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.05	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.06	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.07	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.08	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
G1	1000TX	Up	Enable	8915	0	49535	0	0	0	0	25999	6687
G2	SFP	Down	Enable	0	0	0	0	0	0	0	0	0

Figure 5.16 – Port Statistics

5.17 Port Control Menu

The section of this screen is used to configure each port. The bottom section displays the current settings for each port.

- **Port** - Select the port that you want to configure.
- **State** - Current port status. The port can be set to disable or enable mode. If a port is set to **disable**, it will not be able to receive or transmit packets.
- **Negotiation** - Set auto negotiation status of the port. There are two choices, **auto** and **force**. If you set negotiation to **force**, the following settings must be made:
  - **Speed** – Hard set the speed to either 10 or 100 for ports 1-8. The Gigabit ports can be set at either 10, 100 or 1000.
  - **Duplex** – Choose between full-duplex or half-duplex.
- **Flow Control** – The default for flow control is Disable. Flow control is **Symmetric** or **Asymmetric** in Full Duplex mode.
- **Security** – The default for security is **Off**. When turned **On**, the port will accept only one MAC address.

Click **Apply** to save the configuration.

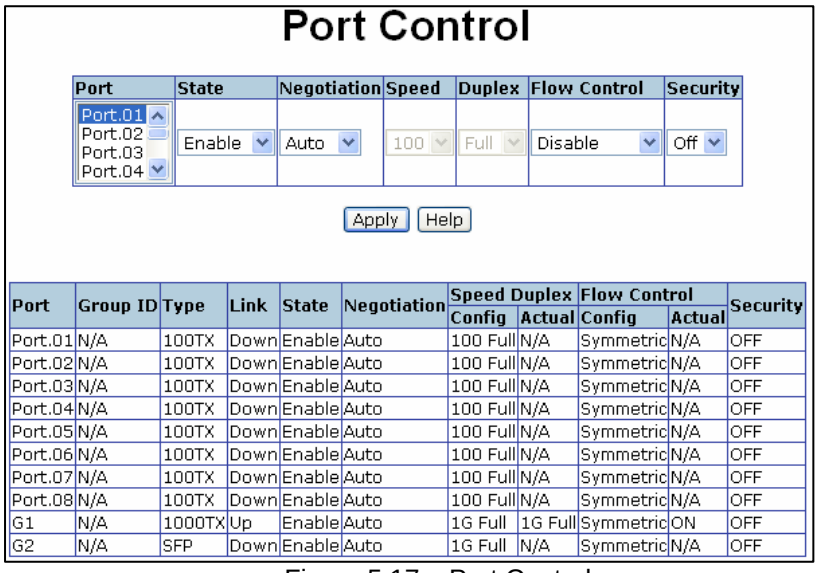


Figure 5.17 – Port Control

To view the status of a single port, click on the **port** displayed on the switch panel at the top of your web management screen. Single port information will be displayed as shown in Figure 5.18.

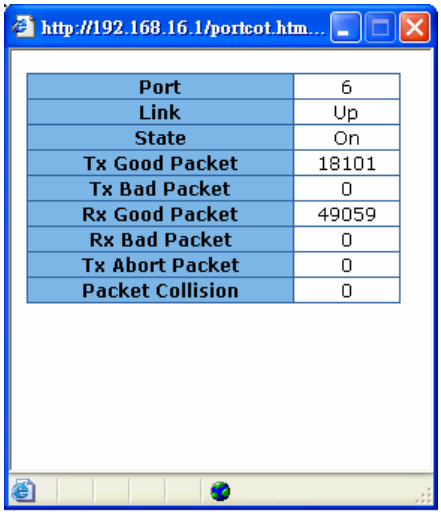


Figure 5.18 – Single port status

5.18 Port Trunking

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between partner systems. The systems have to reach an agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group and enable its transmission and reception functions. Link aggregation allows you to group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. LACP operation requires **full duplex** mode. Aggregator setting involves the following:

- **System priority** – a value used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.
- **Group ID** – There are three trunk groups for configuration.
- **LACP** – When enabled, the group is LACP static trunk group. If disabled, the group is local static trunk group. All ports support LACP dynamic trunk group. If connecting to a device that also supports LACP, the LACP dynamic trunk group will be created automatically.
- **Work Ports** – A maximum of four ports can be aggregated at the same time.
  - **Select** the ports to join the trunk group. A maximum of four ports can be aggregated at the same time. Use the **Add** button to add the port. To remove unwanted ports, select the port and click **Remove**.
- If LACP is enabled, you can configure the LACP Active/Passive status in each port on the state activity page.
- Click **apply** to confirm the setting.
- The Trunk Group can be deleted by selecting the **Group ID** and clicking **Delete**.

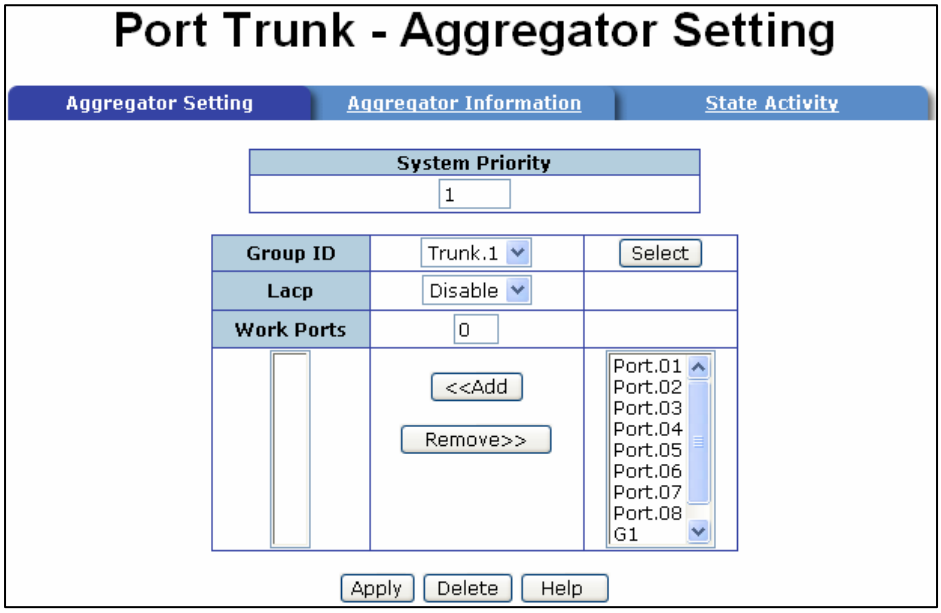


Figure 5.19 – Port Trunk Aggregator Setting

Once the **LACP aggregator** has been configured, the information can be displayed through the **Aggregator Information** screen.

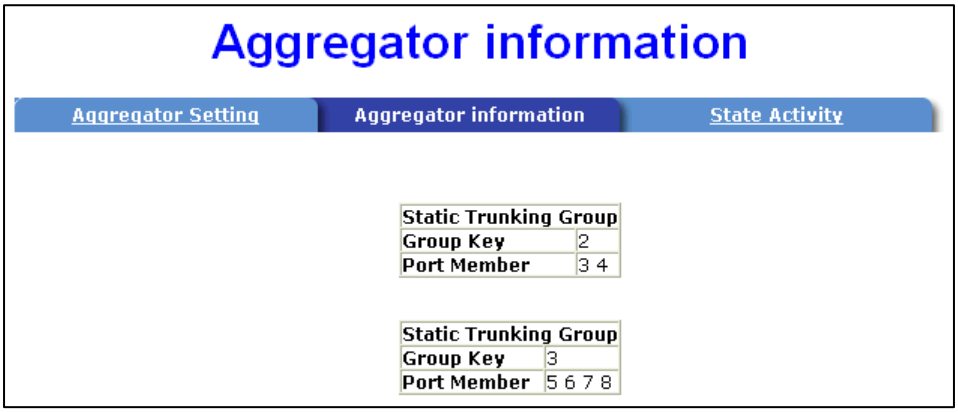


Figure 5.20 - Aggregator Information screen

5.19 State Activity

Once the LACP aggregator has been configured, you can configure the port state activity. Port state activity can be set to **active** or **passive**.

- **Active** – port automatically sends LACP protocol packets
- **Passive** – port does not automatically send LACP protocol packets and responds only if it receives LACP protocol packets from the opposite device.

Note: A link having either two active LACP ports or one active port can perform dynamic LACP trunking. A link with two passive LACP ports will not perform dynamic LACP trunking because both ports are waiting for the LACP protocol packet from the opposite device. The active status will be created automatically if you are the active LACP's actor when selecting the trunking port.

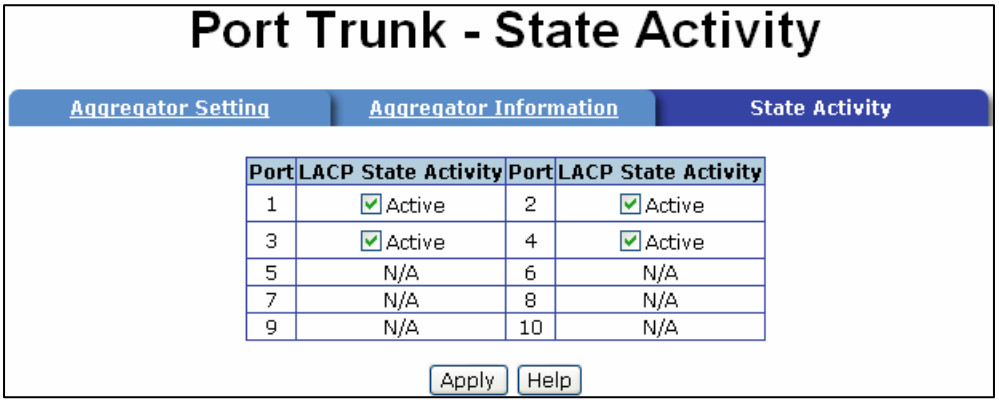


Figure 5.21 - State Activity Screen

5.20 Port Mirroring

Port mirroring is a method used to monitor the traffic on a switched network. A specific port can monitor traffic through mirrored ports. The in and out traffic of a monitored port will be duplicated into the mirrored port.

- **Destination port** – mirror port can be used to see all monitor port traffic. You can connect mirror port to LAN analyzer or Netxray. Select the mirroring port state:
    - **RX** – RX packet only
    - **TX** – TX packet only

- **Both** – RX and TX packet

- **Source port** – select the ports to be monitored. All monitored port traffic will be copied to the mirror port. You can select a maximum of 10 monitor ports in the switch. You can choose the port to monitor in only one mirror mode. Select the mirroring port state:
  - **RX** – RX packet only
  - **TX** – TX packet only
  - **Both** – RX and TX packet
- Click **Apply** to confirm the settings.

Note: To disable the function, set the monitor port to **none**.

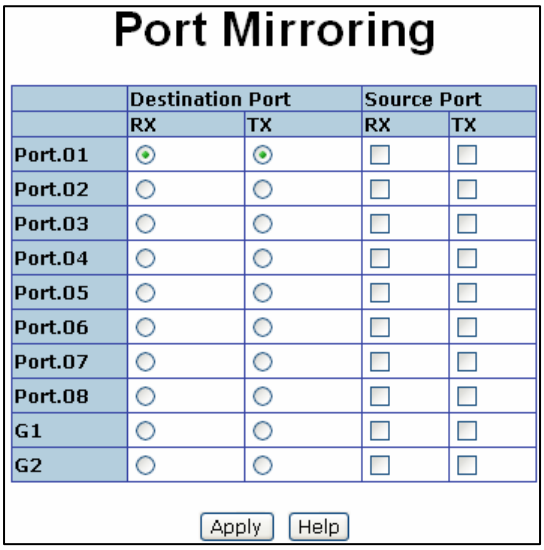


Figure 5.22 - Port Mirroring Screen

5.21 Rate Limiting

Rate limiting allows you to set up the bandwidth rate and packet limitation type per port.

- **Ingress Limit Packet Type** – select the packet type to be filtered. The packet types include all types of packets: broadcast/multicast/unknown unicast packets; broadcast/ multicast packets; broadcast packets only. The broadcast/multicast/unknown unicast packets, broadcast/multicast packets and broadcast packets only used ingress packets. The egress rate supports all types of packets.
- All ports support port ingress and egress rate control. For example, if Port 1 is 10Mpbs, users can set its effective egress rate at 1Mbps and ingress rate is 500kbps. The switch performs the ingress rate by packet counter to meet the specified rate.
- **Ingress** – enter the port effective ingress rate. The default value is **0**.
- **Egress** – enter the port effective egress rate. The default value is **0**.
- Click **Apply** to confirm the settings.

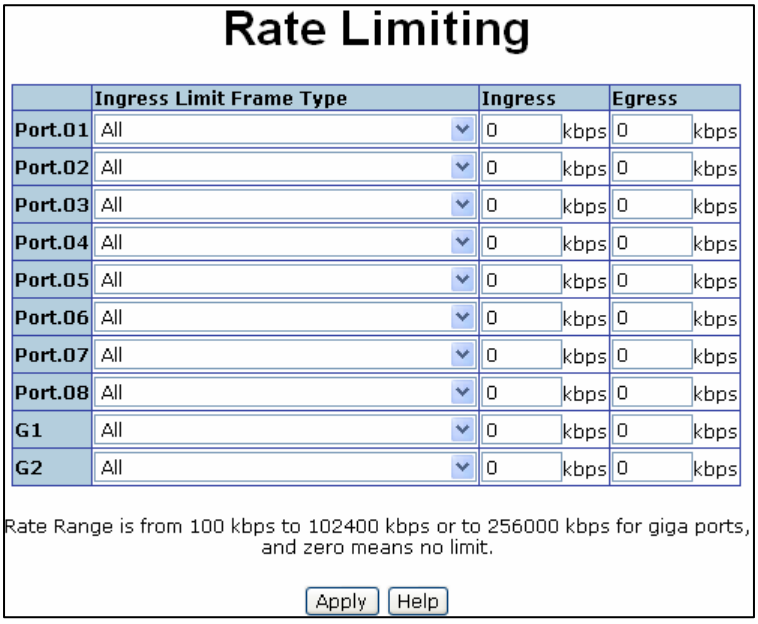


Figure 5.23 – Rate Limiting

5.22 Protocol Menu Options

5.22.1 VLANs

Virtual Local Area Networks (VLANs) are logical network groups that limit the broadcast domain. VLANs allows you to isolate network traffic so only members of the VLAN receive traffic from the other VLAN members and not from everyone on the network. Basically, creating a VLAN is the equivalent of reconnecting a group of network devices to another physical switch. However, all the network devices are still connected to the same physical switch.

The **VLAN Configuration** provides two VLAN modes:

- Port based
- 802.1Q

VLAN support is **disabled** by default.

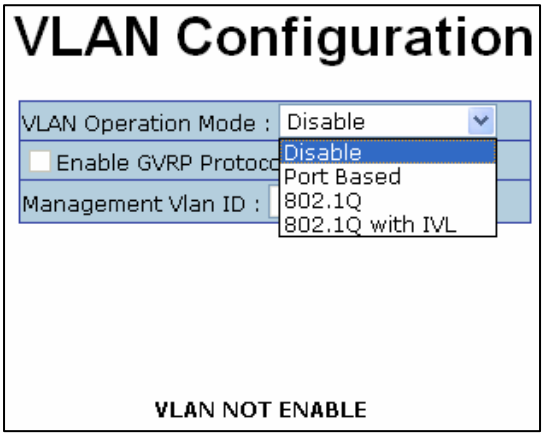


Figure 5.24 - VLAN Configuration

5.22.2 Port Based VLAN Configuration

When a port is configured in a VLAN, packets can travel only among members of the same VLAN group. All unselected ports belong to another single VLAN. If the port-based VLAN is enabled, VLAN-tagging is ignored.

In order for an end station to send packets to different VLANs, it has to be either capable of sending tagged or attached to a VLAN-aware bridge that is capable of classifying and tagging the packet with a different VLAN ID based on not only default PVID but also other information about the packet, such as the protocol.

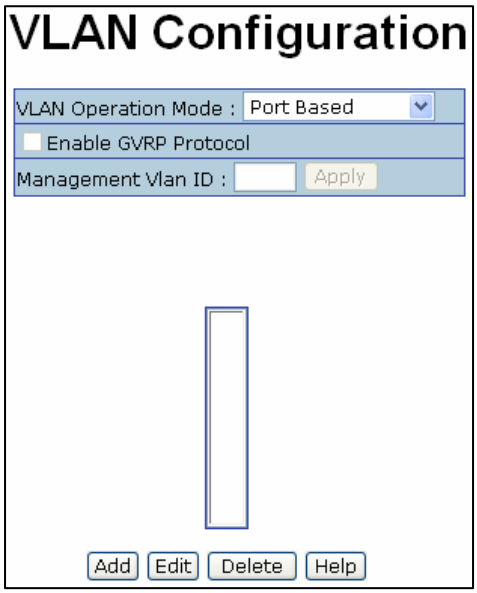


Figure 5.25 – VLAN Configuration

1. Click **Add** to create a new VLAN group.
2. Enter the **Group Name** and **VLAN ID**.
3. Select the **members of the VLAN group**.
4. Click **apply**.

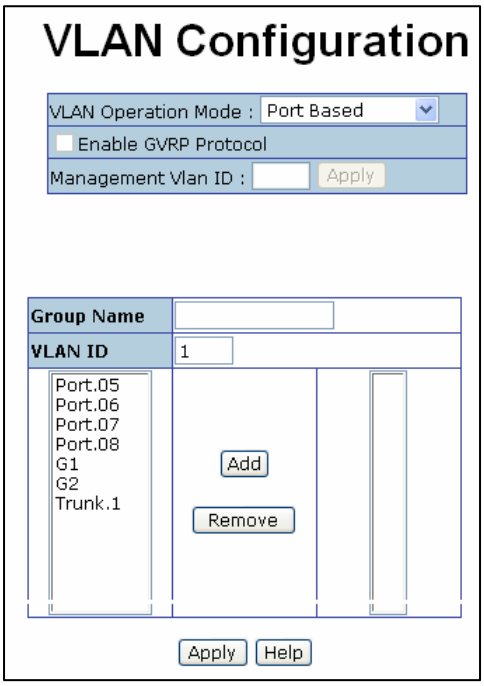


Figure 5.26 – VLAN Configuration Screen

5. The VLANs will be displayed.
6. Use the **Delete** button to remove VLANs.
7. Use the **Edit** button to modify existing VLANs.

5.22.3 802.1q VLAN

The IEEE 802.1q specification covers tagged-based. Therefore, it is possible to create a VLAN across devices from different switch venders. IEEE 802.1Q VLAN uses a technique to insert a “tag” into the Ethernet frames. The tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.

From this menu, you can create a tag-based VLAN, and enable or disable the Generic Attribute Registration Protocol (**GVRP**) protocol. There are 256 VLAN groups available for configuration. Once 802.1q is enabled, all the ports on the switch belong to default VLAN, VID is 1. The default VLAN cannot be deleted.

Each member port of an 802.1 VLAN port is configured as an **Access**, **Trunk**, or **Hybrid Link**. Frames on an **Access Link** carry no VLAN identification. Conversely, frames

on a **Trunk Link** are VLAN-tagged. A **Hybrid Link** can carry both VLAN-tagged frames and untagged frames.

The technique of 802.1q tagging inserts a 4-byte tag, including the VLAN ID of the destination port—PVID in the frame. With the combination of Access, Trunk and Hybrid Links, communication across switches allows the packets to be sent through tagged and untagged ports.

GVRP allows automatic VLAN configuration between the switch and nodes. If the switch is connected to a device with GVRP enabled, you can send a GVRP request using the VID of a VLAN defined on the switch; the switch will automatically add that device to the existing VLAN.

1. To **enable** the GVRP protocol, check box to enable GVRP protocol.
2. Select the ports to be configured.
3. There are three link types.
   - **Access Link**
   - **Trunk Link**
   - **Hybrid Link**
4. Assign the **Untagged VID**.
5. Assign the **Tagged VID**.
6. Click **apply**. Figure 5.27 displays the settings.

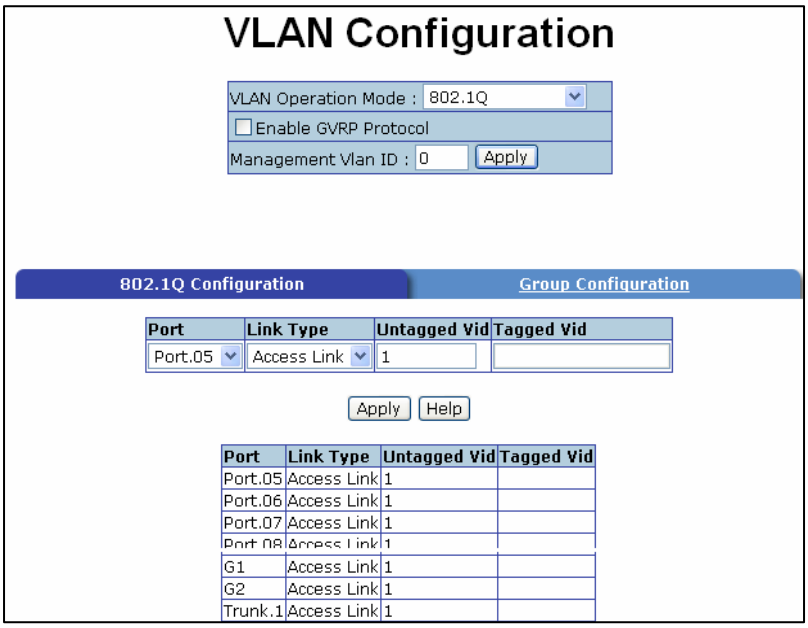


Figure 5.27 – VLAN 802.1q Configuration Screen

Group Configuration

To edit the existing VLAN Group:

1. Select the VLAN group in the table list.
2. Click **apply**.

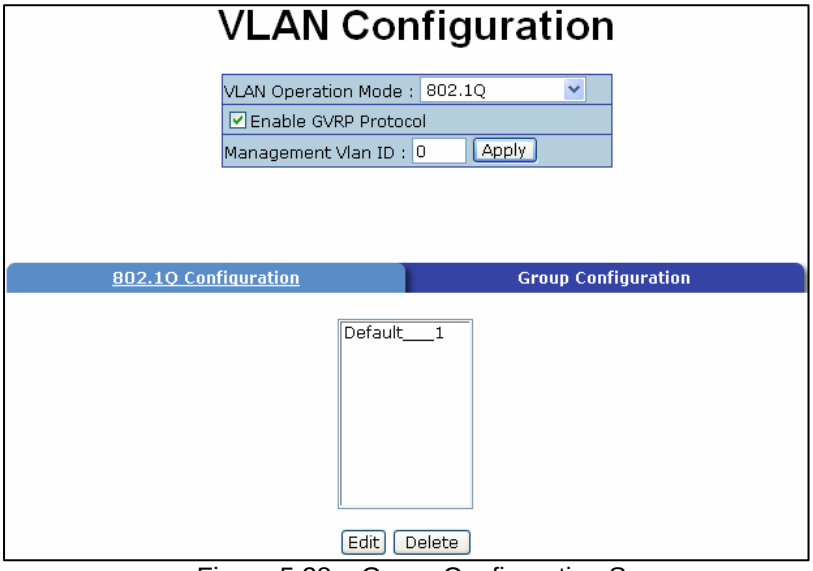


Figure 5.28 – Group Configuration Screen

3. You can change the VLAN group name and VLAN ID.
4. Once you have made the changes, click **apply** to save the changes.

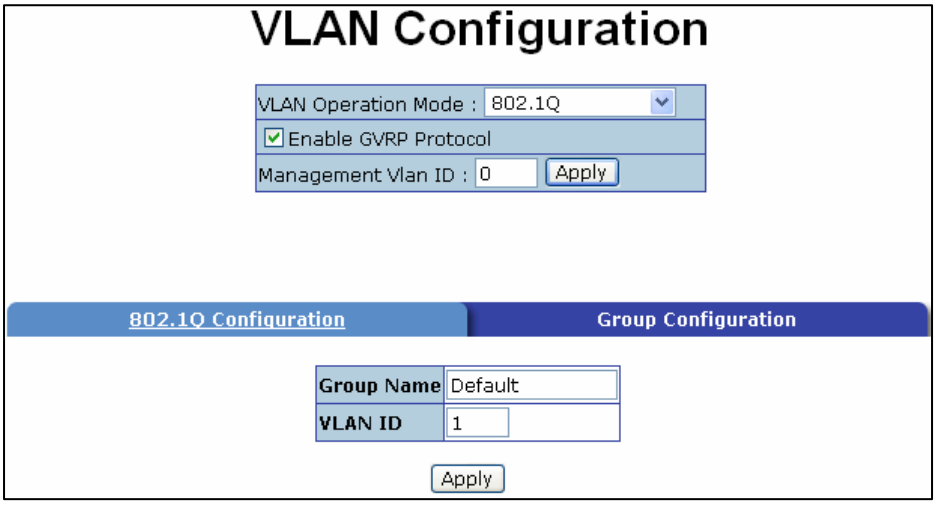


Figure 5.29 – Group Configuration Screen

5.23 RSTP (Rapid Spanning Tree Protocol) Menu

RSTP is an evolution of the Spanning Tree Protocol and provides faster spanning tree convergence once a topology change has been made. This switch supports both STP and RSTP. The switch will auto detect the connected device that is running STP or RSTP protocol.

5.23.1 RSTP Configuration

1. Spanning tree information about the Root Bridge can be viewed here.
2. Use this menu option to modify RSTP state. Remember to use the **apply** button to save the configuration. The following lists information about spanning tree settings.
   - **RSTP mode** – RSTP must **enabled** before RSTP functions can be configured. RSTP is **disabled** by default.
   - **Priority (0-61440)** - a value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If you change the value, you must reboot the switch to assign the new path priority number. The value must be multiple of 4096 according to the protocol standard rule.

- **Max Age (6-40)** - the number of seconds a bridge waits without receiving STP configuration messages before attempting a reconfiguration. Enter a value between 6 through 40.
- **Hello Time (1-10)** - Determines how often the switch broadcasts its hello message to other switches to check RSTP current status. Enter a value between 1 through 10.
- **Forward Delay Time (4-30)** - the number of seconds a port waits before changing from its RSTP learning and listening states to the forwarding state. Enter a value between 4 through 30.

Note: Follow the rule to configure the MAX age, hello time and forward delay time:
2 x (Forward Delay Time value –1) > = Max Age value >= 2 x (Hello Time value +1)

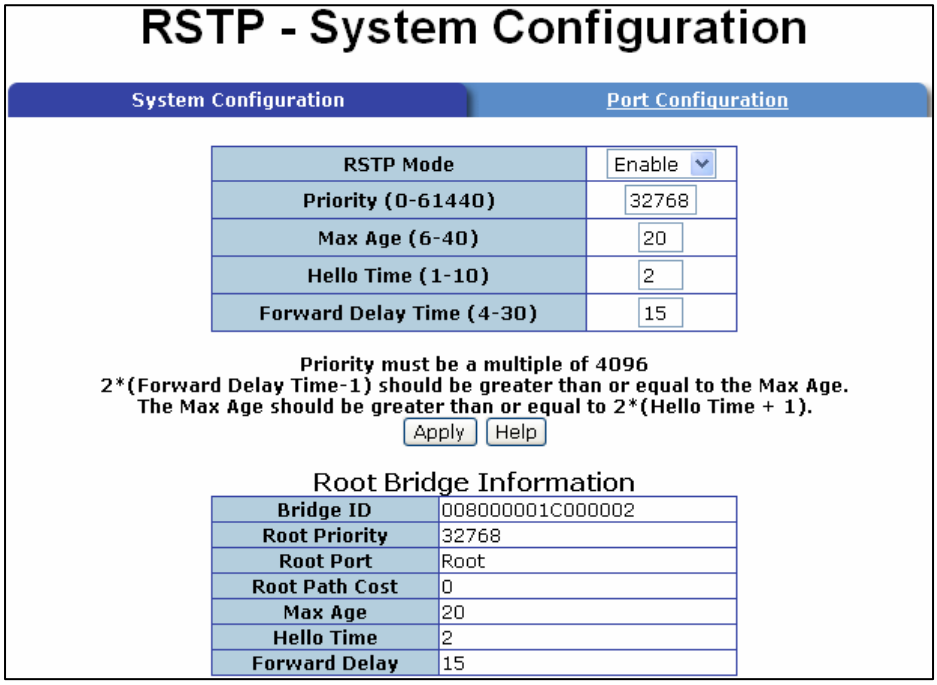


Figure 5.30 - RSTP System Configuration

5.23.2 Port Configuration

The RSTP port configuration allows you to set the path cost and priority of each port.

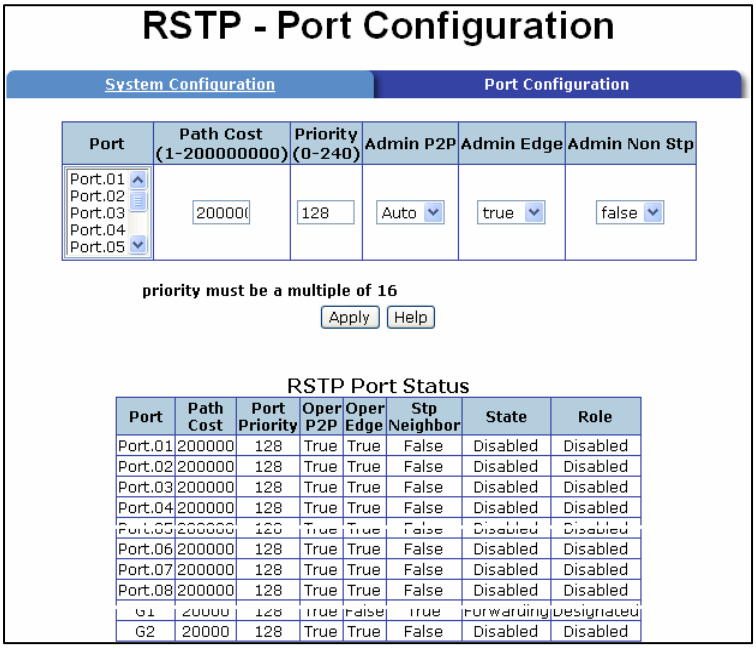


Figure 5.31 – RSTP – Port Configuration

1. Select the port from the port column.
    a. **Path Cost** – the cost of the path to the other bridge from the transmitting bridge at the specified port. Enter a number 1 through 200000000.
    b. **Priority** - decide which port should be blocked by priority in LAN. Enter a number 0 through 240. The value of priority must be a multiple of 16.
2. **Admin P2P** - some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. **True** equals P2P **enabled**. **False** equals P2P **disabled**.
3. **Admin Edge** - the port directly connected to end stations cannot create a bridging loop in the network. To configure the port as an edge port, set the port to **True**.
4. **Admin Non STP** - the port includes the STP mathematic calculation. **True** does not

include STP mathematic calculation. **False** includes the STP mathematic calculation.

5. Click **Apply**.

5.24 SNMP Configuration

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management provides a system to learn of problems by receiving traps or change notices from network devices implementing SNMP.

5.24.1 System Configuration Menu

The **System Configuration** Menu allows you to define a new community string set and remove unwanted community strings.

- **String** – enter the name of the string.
- **Attribute** – enable access rights for the community string.
  - **Read only** – enables requests accompanied by this string to display MIB-object information
  - **Read/write** – enables requests accompanied by this string to display MIB-object information and set MIB objects
- Click **Add**.
- To **remove** the community string, select the community string to be removed, and click **Remove**. You cannot remove the default community string set.
- **Agent Mode** - select the SNMP version that you want to use.
- Click **Change** to switch to the selected SNMP version mode.

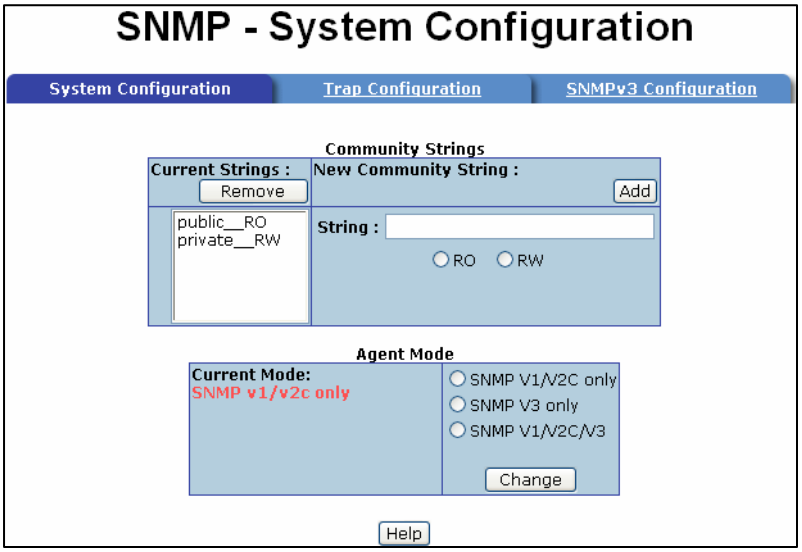


Figure 5.32 – SNMP Configuration

5.24.2 Trap Configuration

A trap manager is a management station that receives traps or system alerts generated by the switch. If a trap manager is not defined, no traps received. Create a trap manager by entering the IP address of the station and a community string. To define a trap manager, enter the following information.

- **IP Address** - enter the IP address of the trap manager.
- **Community** - enter the community string.
- **Trap Version** - select the SNMP version – v 1 or v2.
- Click **Add** - to save the settings.
- To remove the community string, select the community string to be removed and click **Remove**. The default community string cannot be removed.

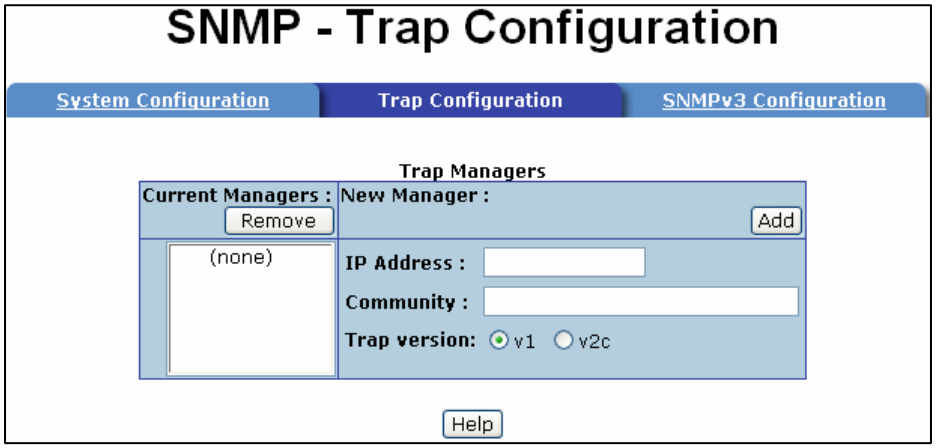


Figure 5.33 – Trap Configuration

5.24.3 SNMPV3 Configuration

To configure the SNMP V3 function, the following tasks should be done. See Figure 5.32 – SNMP V3 Configuration Interface.

Configure the **Context Table**.

- Assign the context name of the context table.
- Click **Add**.
- Click **Remove** to remove an unwanted context name.

Configure **User SNMP v3 User Table**.

- **User ID** – Enter a user name.
- **Authentication Password** – Enter an authentication password.
- **Privacy Password** – Enter a private password.
- Click **Add** to add the password.
- Click **Remove** to remove an unwanted password.

Configure **SNMP V3 Group Table**.

- **Security Name (User ID)** – assign the user name that you set up in user table.
- **Group Name** – set up the group name.
- Click **Add** to add the group information.
- Click **Remove** to remove group information.

Configure **SNMP V3 Access Table**

- **Context Prefix** – set up the context name.
- **Group Name** – set up the group
- **Security Level** – select the access level between the following choices:
    - NoAuthNoPriv
    - AuthNoPriv
    - AuthPriv
- **Read View Name** – set the read view
- **Write View Name** – set up the write view.
- **Notify View Name** – set up the notify view.
- Click **Add** to add the access table information.
- Click **Remove** to remove the access table information

Configure **MIBview Table**.

- **ViewName**- set up the name.
- **Sub-Oid Tree** – enter the Sub Oid
- **Type** – select excluded or included
- Click **Add** to configure the **MIBview Table**.
- Click **Remove** to remove the **MIBview Table**.

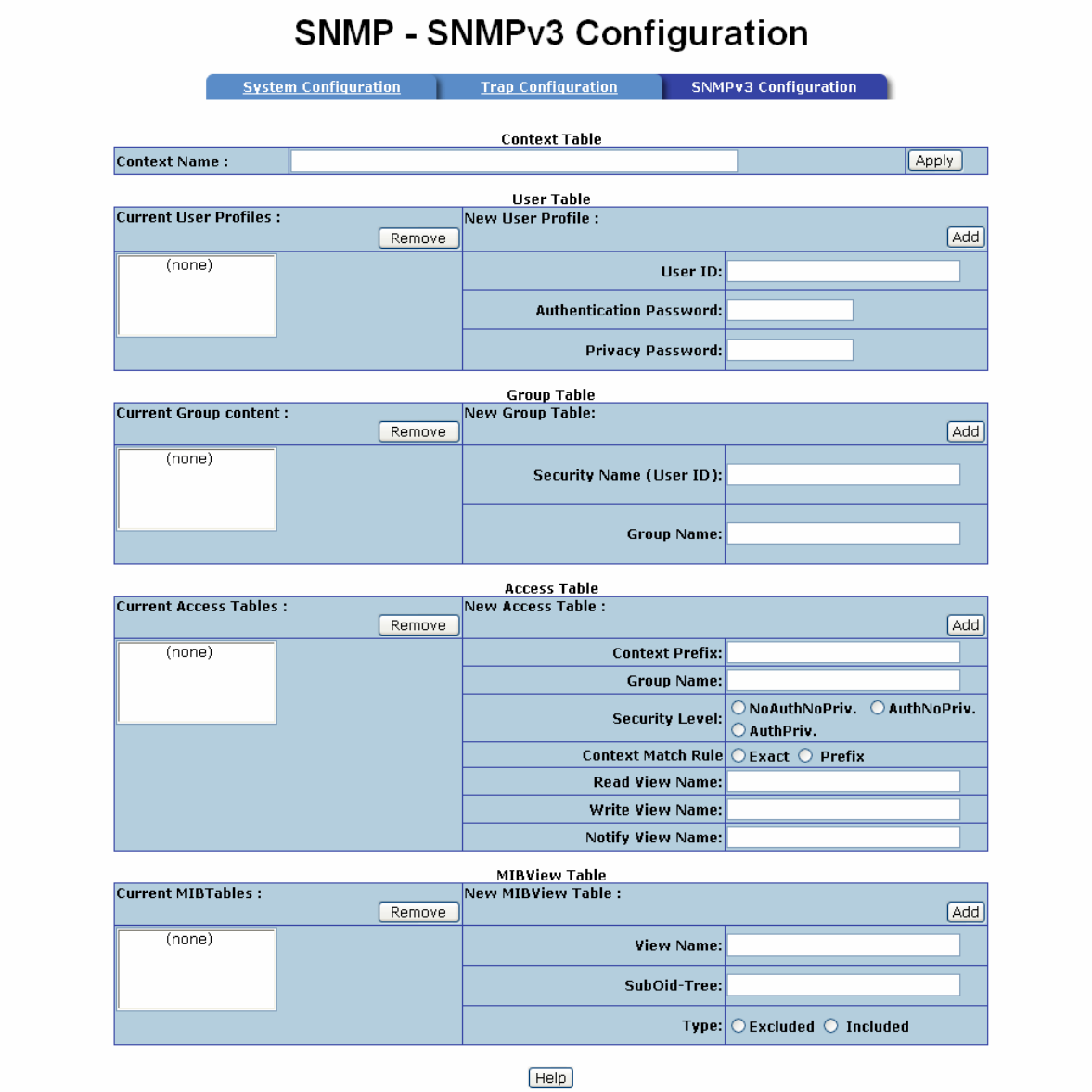


Figure 5.34 – SNMP V3 Interface

5.25 QoS Configuration

Use the QoS configuration menus to configure the following:

- QoS policy
- Priority setting
- Per port priority setting
- COS
- TOS

QoS Policy and Priority TYpe

- **QoS Policy** – select the QoS policy rule.
  - **8,4,2,1 weight fair queue scheme** - the switch will follow the 8:4:2:1 rate to process priority queue from highest to lowest queue. For example, the system will process 80 percent high queue traffic, four middle queue traffic, two low queue traffic and the lowest (one) queue traffic at the same time.
  - **Use the strict priority scheme** – higher queue priority will be processed first unless the higher queue is empty.
- **Select the Priority Type** – each port has five priority type selections. Disable indicates that no priority type is selected.
  - **Port-based** - port priority follows the **default port priority** that you have assigned: high, middle, low, or lowest.
  - **COS only** - the port priority follows the **COS priority** that has been assigned.
  - **TOS only** - the port priority follows the **TOS priority** that has been assigned.
  - **COS first** - the port priority follows the COS priority first and other priority rules next.
  - **TOS first** - the port priority follows the TOS priority first and other priority rules next.

Click **Apply** to save the configuration.

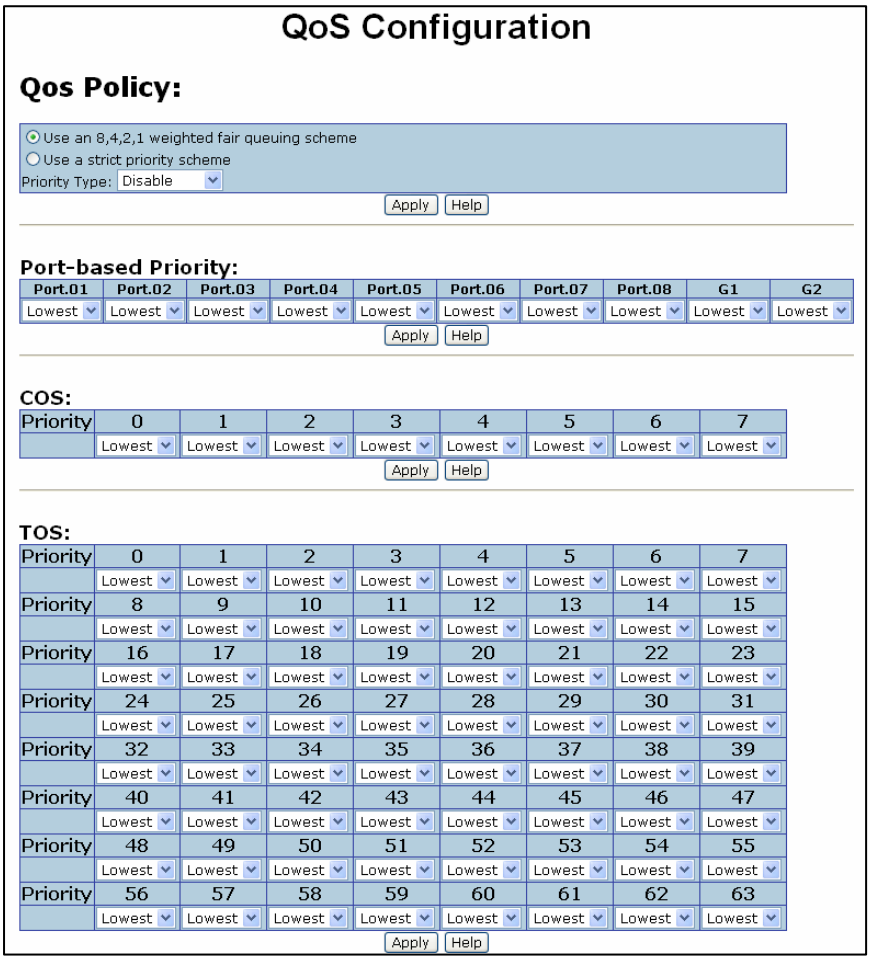


Figure 5.35 – QoS Configuration

Port Based Priority

Use this section of the screen to configure the priority level per port.

- **Port 1 ~ G1 & G2** – each port has four priority levels – High, Middle, Low and Lowest.
- Click **Apply** to save the configuration.

COS Configuration

Use this section of the screen to set the COS priority level.

- **COS priority** - set the COS priority level 0~7: High, Middle, Low, Lowest.
- Click **Apply** to save the configuration.

TOS Configuration

Use this section of the screen to set the TOS priority level.

- **TOS priority** - the system provides 0~63 TOS priority levels. Each level has four types of priority – high, mid, low, and lowest. The default value is the **lowest** priority for each level. When the IP packet is received, the system will check the TOS level value in the IP packet that has been received. For example: TOS level is set to 25. Port 1 will follow the TOS priority policy only. When the packet for port 1 is received, the system will check the TOS value of the received IP packet. If the TOS value of the received IP packet is 25 (priority = high), the packet priority will have highest priority.
- Click **Apply** to save the configuration.

5.26 IGMP Configuration

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP). IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries and report packets as well as manage IP multicast traffic through the switch. IGMP provides the following three fundamental types of messages:

Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host is no longer a member of a specific multicast group.

Table 5.2 – IGMP Messages

IGMP Configuration

IGMP is **disabled** by default. Use the **IGMP Configuration** menu to enable IGMP. IP multicast addresses range from 224.0.0.0 to 239.255.255.255.

- **IGMP Protocol** - enable or disable the IGMP protocol.
- **IGMP Query** - enable or disable the IGMP query function. The IGMP query information will be display in the IGMP status section.
- Click **Apply** to save the configuration.

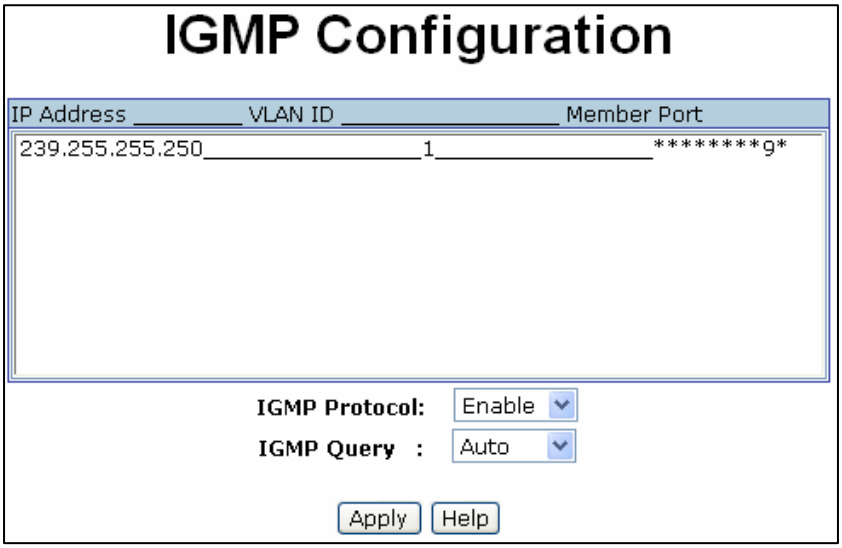


Figure 5.36 – IGMP Configuration

5.27 X-ring

X-ring provides a faster redundant recovery than the spanning tree topology. The action is similar to STP and RSTP, but the algorithms that are used are not the same.

To use the X-ring topology, the X-ring function must be **enabled** and the switch must assign two member ports in the ring. One switch in the X-ring group should be set as a backup switch that one of two member ports will be blocking. That switch is the backup port, and the other port is the working port. The other switches are working switches and their two member ports are working ports. If there is a network connection failure, the backup port will automatically become a working port to recover the failure.

The switch can be set as the ring master or slave. The ring master has the rights to negotiate and send commands to other switches in the X-ring group. If there are two or more switches are in master mode, then the software will select the switch with lowest MAC address as the ring master.

The system also supports a coupling ring that can connect two or more X-ring groups for redundant backup.

- **Enable X-ring** – use to enable the X-ring function.
- **Enable Ring Master** - enable sets the switch as the ring master. Disable sets the switch as the slave.
- **1st & 2nd Ring Ports** - select two ports as member ports. One port will be the working port and one port will be the backup port. The system will automatically decide which port is the working port and which port is the backup port.
- **Enable Coupling Ring** – use to enable the coupling ring function.
- **Coupling Port** - select the member port.
- **Control Port** - select the switch as the master switch in the coupling ring.

  Enable Dual Homing – Dual homing only works when **X-ring** is enabled. To enable the **dual homing** function, set up one port as the dual homing port. Only one port can be the dual homing port. Dual-homing provides reliability for your network by allowing a device to be connected to the network by way of two independent connection points. One access point is the operating connection and the other is a standby or back up connection that is activated in case the operating connection fails.
- Click **Apply** to save the configuration.

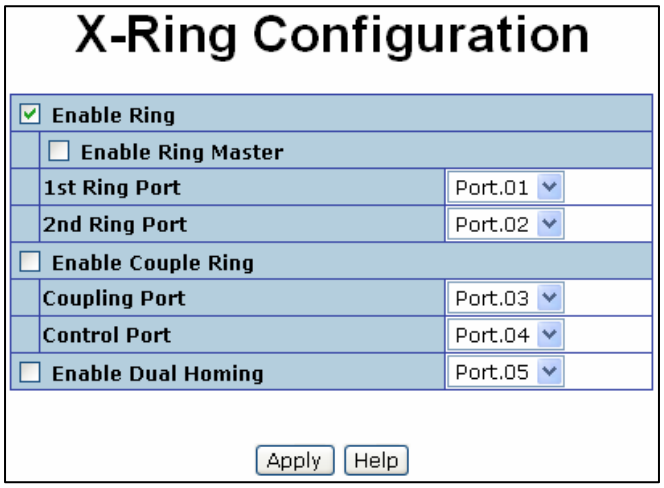


Figure 5.37 - X-ring Interface

Note: When the X-ring function is enabled, RSTP must be disabled. The X-ring function cannot exist at the same time as RSTP.

5.28 Security Menu

Use the **Security** menu to configure 802.1x and port security by MAC address. 802.1x is an IEEE network standard that allows a client to connect to a wireless access point or wired switch, but prevents the client from gaining access to the Internet until proper authentication has taken place. Authentication is supplied through user name and password which are verified by a separate server.

802.1x/Radius - System Configuration

Once the 802.1x function has been enabled, you are ready to configure the parameters for this function.

- **IEEE 802.1x protocol** - enable or disable 802.1x protocol.
- **Radius Server IP** - set the Radius Server IP address.
- **Server Port** - set the UDP destination port for authentication requests to the specified Radius Server.
- **Accounting Port** - set the UDP destination port for accounting requests to the specified Radius Server.

- **Shared Key** - set an encryption key to be used during authentication sessions with the specified radius server. This key must match the encryption key used on the Radius Server.
- **NAS, Identifier** - set the identifier for the radius client.
- Click **Apply** to save the configuration.

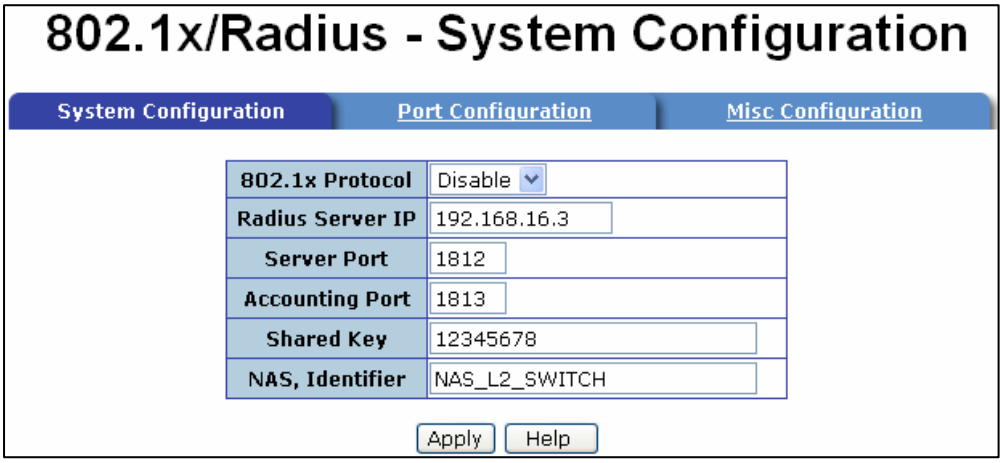


Figure 5.38 – 802.1x System Configuration

802.1x Port Configuration

The 802.1x authentication state can be configured for each port. The **State** provides the following conditions. Use the **Space** bar to change the state value.

- **Reject** - the specified port is required to be held in the **unauthorized** state.
- **Accept** - the specified port is required to be held in the **authorized** state.
- **Authorized** - the specified port is set to the **authorized** or **unauthorized** state in accordance with the outcome of an authentication exchange between the supplicant and the authentication server.
- **Disable** - the specified port is required to be held in the **authorized** state
- Click **Apply** to save the configuration.

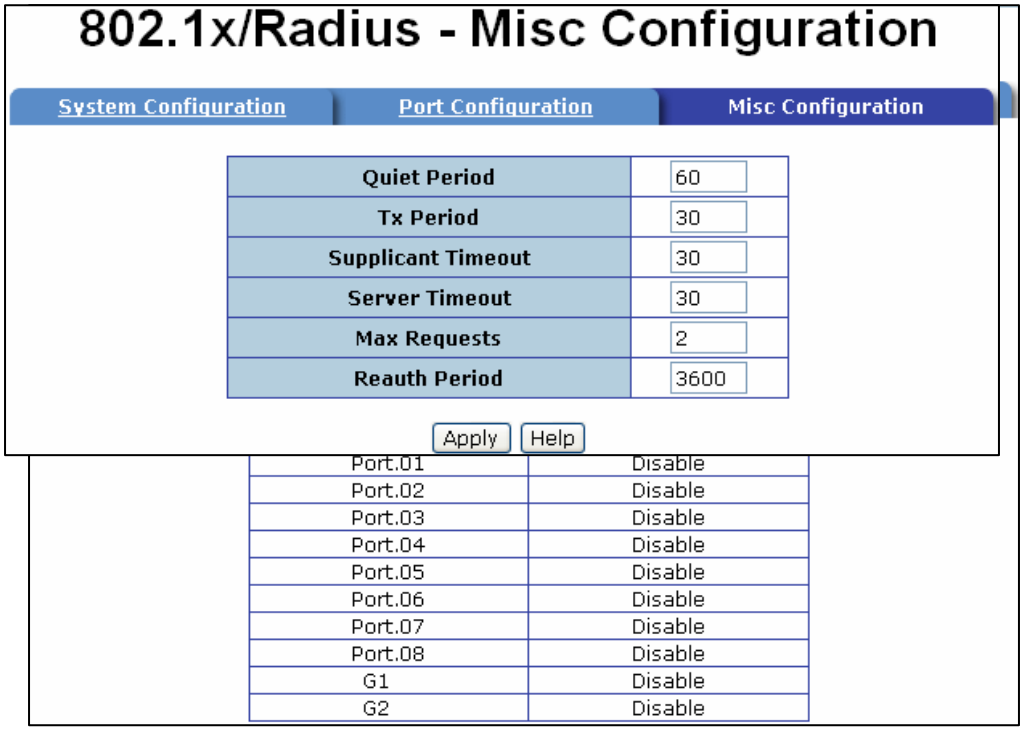


Figure 5.39 – 802.1x Per Port Setting Interface

Miscellaneous Configuration

- **Quiet Period** - set the period during which the port doesn't try to acquire a supplicant.
- **TX Period** - set the period the port waits for retransmit (next EAPOL PDU) during an authentication session.
- **Supplicant Timeout** - set the period of time the switch waits for a supplicant response to an EAP request.
- **Server Timeout** - set the period of time the switch waits for a server response to an authentication request.
- **Max Requests** - set the number of authentication requests that must time-out before authentication fails and the authentication session ends.
- **Reauth period** - set the period of time after which clients connected must be re-authenticated.
- Select **Apply** to save the configuration.

Figure 5.40 – 802.1x Miscellaneous Configuration

5.29 MAC Address Table

In addition to the 802.1x security, the **Port Security Configuration** uses MAC addresses to ensure additional port security.

Static MAC Address

The **Port Security Configuration** menu allows you to add a static MAC address. The static MAC address will remain in the switch's address table, regardless of whether or not the device is physically connected to the switch. This eliminates the need for the switch to re-learn a device's MAC address when the disconnected or powered-off device once again becomes active on the network. You can **add/modify/delete** a static MAC address.

To add a static MAC address in switch MAC table, follow this procedure:

1. **MAC Address** - enter the MAC address of the port that should permanently forward traffic, regardless of device activity.
2. **Port No.** – use the **Space** bar to select the port number.
3. **VLAN ID** - enter the MAC address, and VLAN ID (if that MAC address belongs to a VLAN group).
4. Click **Add** to save the configuration.

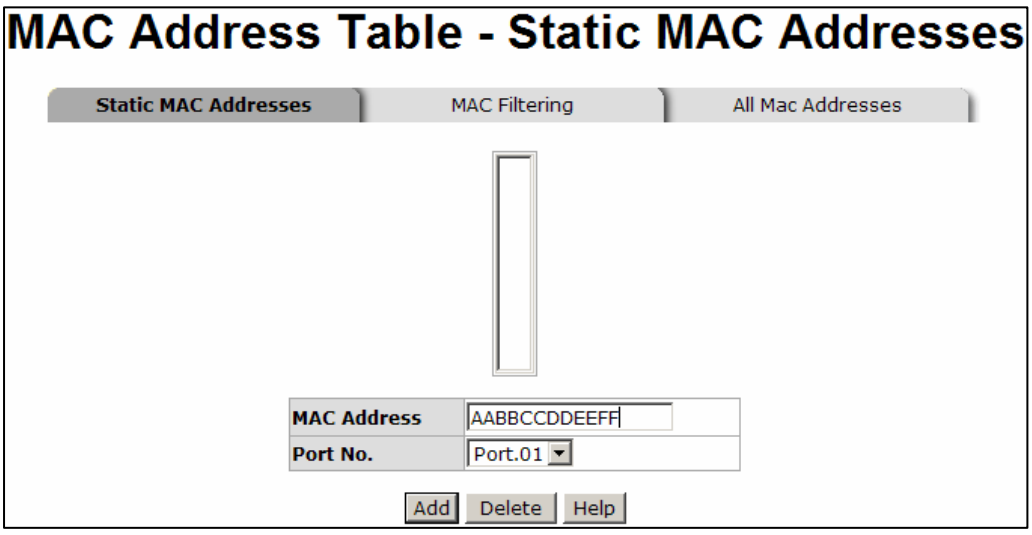


Figure 5.41 – Static MAC Address Interface

MAX Filtering

By filtering MAC addresses, you can enhance the security on your network. The **MAC Filtering** screen allows you to add and delete MAC addresses.

To add a **MAC Address** for filtering:

1. **MAC Address** - Enter the MAC address to be filtered.
2. **VID** – If the MAC address belongs to a VLAN group, enter the VLAN ID for the MAC address.
3. Click **Add** to save the configuration.
4. The MAC address will be displayed in the table. You can delete a MAC address from the filtering table by selecting the MAC address and clicking **Delete**.

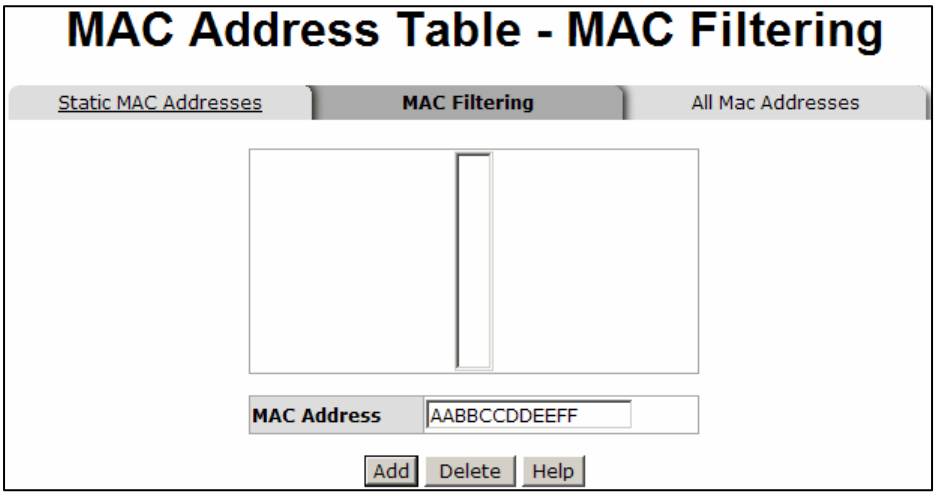


Figure 5.42 – Filter MAC Address Interface

All MAC Addresses

You can view the MAC address and the related devices' MAC address connected to the port.

1. Select the **port**.
2. The selected port for static MAC address information will be displayed.
3. Select **Clear MAC Table** to clear the current port static MAC address information.

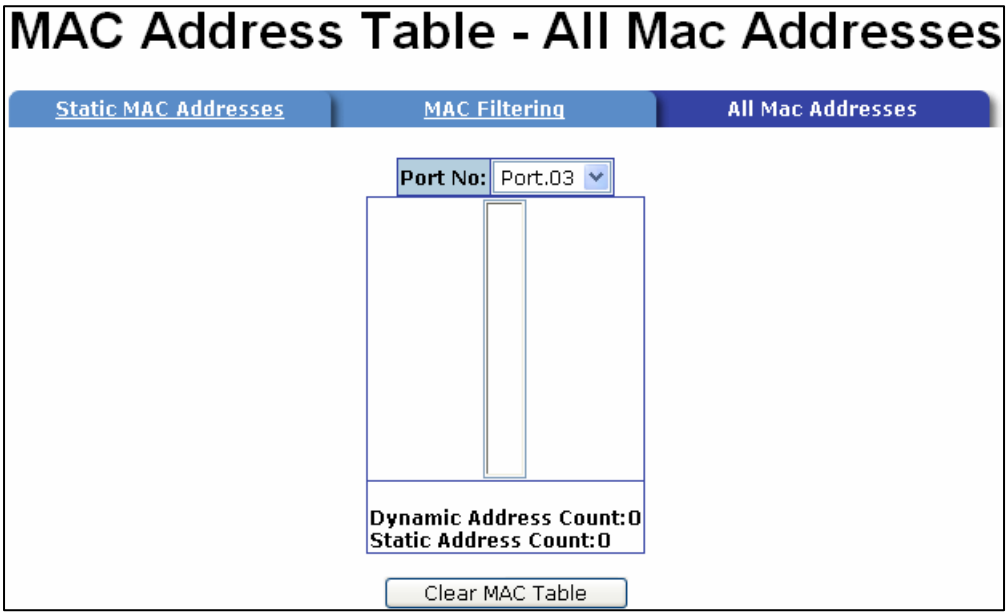


Figure 5.43 – All MAC Address Interface

5.30 Power over Ethernet (PoE)

The following list describes the PoE settings for the switch.

- **Maximum Power Available** - Displays the maximum watts.
- **Actual Power Consumption** – Real-time total power consumption.
- **Power Source** – Displays the supplying power source.
- **Power Source 1 (AC)** – Displays the supplying power of power source 1.
- **Power Source 2 (AC+DC)** – Displays the supplying power of power source 2 (may vary by model.)
- **Firmware Version** – Displays the firmware version.
- **AC Disconnect** - Use this setting to disable AC input.
- **Capacitive Detection** - Used to detect the power consumption of the powered device.
- Click **Apply** to confirm/save changes.
- Use the **Refresh** button to renew the states.
- **Port** – Displays the index of PoE ports.

- **Enable State** – PoE is **enabled** by default. You can check this box to disable the PoE function to the port.
- **Power Limit From** – Choose the power limit method.
  - Classification: The system will limit the power supply to the powered device in accordance with the related class.
  - Management: You can assign the power limit manually.
- **Legacy** – Used to support legacy power devices.
- **Priority** – Used to choose the priority of power supply.
- **Power Limit (<15400) mW** - While **Power Limit From** is in **Management** mode, you can enter the power limit value (under 15.4 Watts).
- **Mode** - Displays the operating mode of the port.
- **Current (mA)** - Displays the operating current of the port.
- **Voltage (V)** - Displays the operating voltage of the port.
- **Power (mW)** - Displays the power consumption of the port.
- **Determined Class** – Displays the power limit class.
- Click **Apply** to apply changes.

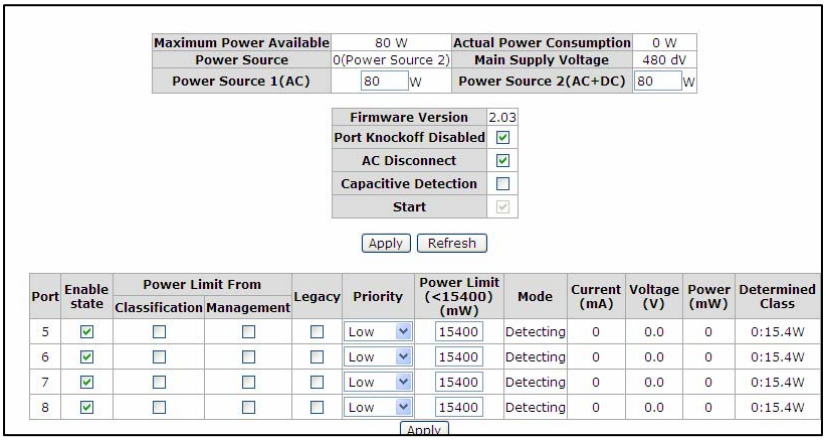


Figure 5.44 – PoE Settings

5.31 Factory Default Settings

You can return the factory default settings by choosing **Factory Default** from the **Main Menu**.

- **Keep current IP address setting** – You may either keep the current IP address or reset the IP to the default IP address. Use the **Space** key to make the change.
- **Keep current username and password** – You may either keep the current username and password or reset to default username and password (**root/root**). Use the **Space** key to make the change.
- Once you have checked the appropriate settings, click **Default** to reset.

Figure 5.45 – Factory Default Interface

5.32 Save Configuration

Once you have made changes to the system, you must use **Save All Configuration** from the **Main Menu** to ensure that all changes are saved.

1. Click on **Save Configuration**.
2. Click on **Save** to save the configuration to the flash memory.

5.33 Reboot the System

Once changes have been made, the system should be rebooted to apply the changes.

1. Choose **Reboot System** from the **Main Menu**.
2. Click on **Reboot** to reboot the system.

6.0 CLI Commands

To use the CLI commands, enter **enable** once you have logged into the switch.

The following table lists the **Command** level of the CLI commands.

Command	Description	Prompt	Access Method	Exit Method
User EXEC	This command is a subset of the commands available at the privileged level. Use this command to: ▪ Perform basic tests ▪ Display system information	switch>	Begin a session with the switch	Logout or quit
Privileged EXEC	The privileged command is in advanced mode. Use this command to: ▪ Display advanced status functions ▪ Save configuration	switch#	Enter the **enable** command while in EXEC mode. Enable takes you into the privileged mode.	Disable
Global configuration	Use this command to configure parameters that will apply to the switch as a whole	switch (config) #	Enter the configure command while in privileged mode	Exit or end
VLAN database	Use this command to configure VLAN specific parameters	switch (vlan)#	Enter the VLAN database command while in privileged EXEC mode	Exit
Interface configuration	Use this mode to configure parameters	switch (config-i	Enter the interface	Exit

		f)#	command (with a specific interface) while in the global configuration mode	

Commands Set List – Used in Next Table

User EXEC	E
Privileged EXEC	P
Global configuration	G
VLAN database	V
Interface Configuration	I

The following table lists the **System Commands**.

Command	Level	Description	Example
show config	E	Displays switch configuration	switch>show config
show terminal	P	Displays console information	switch>show terminal
menu	E	Enters menu mode	switch>menu
write memory	G	Saves user configuration into permanent memory (flash ROM)	switch#write memory
system name [system name}	G	Configure the system name	switch (config)# system name xxx
system location [system location]	G	Configure switch location	switch(config)#system location xxx
system	G	Set switch system description string	switch(config)#system description xxx

Command	Level	Description	Example
description [system description]			
system contact [system contact]	G	Set switch system contact window string	switch(config)#system contact xxx
show system-info	E	Show system information	switch>show system-info
ip address] [Ip-address] [Subnet-mask] [Gateway]	G	Configure the IP address of switch	switch(config)#ip address 192.168.1.1 255.255.255.0 192.168.1.254
ip dhcp	G	Enable DHCP client function of switch	switch(config)#ip dhcp
show ip	P	Show IP information of switch	switch#show ip
no ip dhcp	G	Disable DHCP client function of switch	switch(config)#no ip dhcp
reload	G	Halt and perform a cold restart	switch(config)#reload
default	G	Restore to default settings	switch(config)#default
admin username [username]	G	Changes a login username. (maximum 10 characters)	switch(config)#admin username xxxxxx
admin password [password]	G	Specifies a password (maximum 10 characters)	switch(config)#admin password xxxxxx
show admin	P	Displays administrator information	switch#show admin
dhcpserver enable	G	Enables DHCP Server	switch(config)#dhcpserver enable
dhcpserver lowip	G	Configures low IP address number for IP pool	switch(config)# dhcpserver lowip 192.168.1.1

Command	Level	Description	Example
[low ip]			
dhcpserver highip [high ip]	G	Configures high IP address number for IP pool	switch(config)# dhcpserver highip 192.168.1.50
dhcpserver subnetmask [subnet mask]	G	Configures subnet mask for DHCP clients	switch(config)#dhcpserver subnetmask 255.255.255.0
dhcpserver gateway [gateway]	G	Configures gateway for DHCP clients	switch(config)#dhcpserver gateway 192.168.1.254
dhcpserver dnsip [dns ip]	G	Configures DNS IP for DHCP clients	switch(config)# dhcpserver dnsip 192.168.1.1
dhcpserver leasetime [hours]	G	Configures lease time (in hours)	switch(config)#dhcpserver leasetime 1
dhcpserver ipbinding	I	Set static IP for DHCP clients by port	switch(config)#interface fastEthernet 2 switch(config-if)# dhcpserver ipbinding 192.168.1.1
show dhcpserver configuration	P	Displays configuration of DHCP server	switch#show dhcpserver configuration
show dhcpserver clients	P	DIsplays client entries of DHCP server	switch#show dhcpserver clinets
show dhcpserver ip-binding	P	Displays IP-Binding information of DHCP server	switch#show dhcpserver ip-binding
no dhcpserver	G	Disables DHCP server function	switch(config)#no dhcpserver
security enable	G	Enables IP security function	switch(config)#security enable
security http	G	Enables IP security of HTTP	switch(config)#security http

Command	Level	Description	Example
		server	
security telnet	G	Enables IP security of telnet server	switch(config)#security telnet
security ip [Index(1..10)] [IP Address]	G	Set the IP security list	switch(config)#security ip 1.192.168.1.55
show security	P	Displays IP security information	switch#show security
no security	G	Disables IP security function	switch(config)#no security
no security http	G	Disables IP security for HTTP server	switch(config)#no security http
no security telnet	G	Disables IP security of telnet server	switch(config)#no security telnet

The following table lists the **Port Commands**.

Command	Level	Description	Example
interface fastEthernet [portid}	G	Choose the port for modification	switch(config)#interface fastEthernet 2
duplex [full | half]	I	Use the duplex command to specify the duplex mode for the Fast Ethernet ports	switch(config)#interface fastEthernet 2 switch(config-if)#duplex full
speed [10|100|1000| auto]	I	Use the speed configuration command to specify the speed mode for operation of the Fast Ethernet ports.	switch(config)#interface fastEthernet 2 switch(config-if)#speed 100
flowcontrol mode [symmetric| asymmetric]	I	Use the flow control configuration command to control traffic rates when there is congestion.	switch(config)#interface fastEthernet 2 switch(config-if)#flowcontrol mode Asymmetric
no flowcontrol	I	Disable flow control	switch(config-if)#no flowcontrol
security enable	I	Enable security	switch(config)#interface fastEthernet 2 h(config-if)#security enable
no security	I	Disable security	switch(config)#interface fastEthernet 2 switch(config-if)#no security

Command	Level	Description	Example
bandwidth type all	I	Set interface ingress limit frame type to “accept all frame”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type all
bandwidth type broadcast-multicast-flooded-unicast	I	Set interface ingress limit frame type to “accept broadcast, multicast, and flooded unicast frame”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast-flooded-unicast
bandwidth type broadcast-multicast	I	Set interface ingress limit frame type to “accept broadcast and multicast” frame	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast
bandwidth type broadcast-only	I	Set interface ingress limit frame type to “only accept broadcast frame”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-only
bandwidth in [value]	I	Set interface input bandwidth. Rate range is from 100kbps to 102400kbps or to 256000 kbps for Giga ports. Zero means no limit.	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth in 100
bandwidth out	I	Set interface output bandwidth. Rate range is from 100kbps to 102400kbps or to 256000 kbps for Giga ports. Zero means no limit.	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth out 100
show bandwidth	I	Displays interfaces bandwidth control	switch(config)#interface fastEthernet 2 switch(config-if)#show bandwidth
state [enable | disable]	I	Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disable form of this command to disable the port.	switch(config)#interface fastEthernet 2 (config-if)#state Disable
show interface configuration	I	Displays the status of the interface configuration	switch(config)#interface fastEthernet 2 switch(config-if)#show

Command	Level	Description	Example
			interface configuration
show interface status	I	Displays the actual status of the interface	switch(config)#interface fastEthernet 2 switch(config-if)#show interface status
show interface accounting	I	Displaces statistic counter of interface	switch(config)#interface fastEthernet 2 switch(config-if)#show interface accounting
no accounting	I	Clears interface accounting information	switch(config)#interface fastEthernet 2 switch(config-if)#no accounting

The following table lists the **Trunk Commands**.

Command	Level	Description	Example
aggregator priority [1~65535]	G	Set port group system priority	switch(config)#aggregator priority 22
aggregator activityport [Port Numbers]	G	Set activity port	switch(config)#aggregator activityport 2
aggregator group [GroupID] [Port-list] lacp workp [Workport]	G	Assign a trunk group with LACP active. [GroupID] :1~3 [Port-list]: Member port list, This parameter could be a port range (ex.1-4) or a port list separated by a comma (ex.2, 3, 6) [Workport]: The number of work ports which cannot be less than zero or be larger than the number of member ports.	switch(config)#aggregator group 1 1-4 lacp workp 2 or switch(config)#aggregator group 2 1,4,3 lacp workp 3
aggregator group [GroupID] [Port-list] nolacp	G	Assign a static trunk group. [GroupID] :1~3 [Port-list]: Member port list. This parameter could be a port range (ex.1-4) or a port	switch(config)#aggregator group 1 2-4 nolacp or switch(config)#aggregator group 1 3,1,2 nolacp

Command	Level	Description	Example
		list separate by a comma (ex.2, 3, 6)	
show aggregator	P	Displays the information of trunk group	switch#show aggregator
no aggregator lacp [GroupID]	G	Disable the LACP function of trunk group	switch(config)#no aggregator lacp 1
no aggregator group [GroupID]	G	Remove a trunk group	switch(config)#no aggreator group 2

The following table lists the **VLAN Commands**.

Command	Level	Description	Example
vlan database	P	Enter VLAN configure mode	switch#vlan database
vlanmode [portbase| 802.1q | gvrp]	V	Used to set VLAN mode.	switch(vlan)# vlanmode portbase or switch(vlan)# vlanmode 802.1q or switch(vlan)# vlanmode gvrp
no vlan	V	Used to disable VLAN	
Port based VLAN configuration			
vlan port-based grpname [Group Name] grpid [GroupID] port [PortNumbers]	V	Add new port to port-based VLAN	switch(vlan)# vlan port-based grpname test grpid 2 port 2-4
show vlan [GroupID] or show vlan	V	Displays VLAN information	switch(vlan)#show vlan 23
no vlan group [GroupID]	V	Delete port-based group ID	switch(vlan)#no vlan group 2
IEEE 802.1Q VLAN			
vlan 8021q	V	Modify the name of VLAN	switch(vlan)#vlan 8021q test

Command	Level	Description	Example
name [GroupName] vid [VID]		group. If there is no group, this command can't be applied.	vid 22
vlan 8021q port [PortNumber] access-link untag [UntaggedVID]	V	Assign an access link for VLAN by port. If the port belongs to a trunk group, this command can't be applied.	switch(vlan)#vlan 8021q port 3 access-link untag 33
vlan 8021q port [PortNumber] trunk-link tag [TaggedVID List]	V	Assign a trunk link for a VLAN by port. If the port belongs to a trunk group, this command can't be applied.	switch(vlan)#vlan 8021q port 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q port 3 trunk-link tag 3-20
vlan 8021q port [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]	V	Assign a hybrid link for a VLAN by port. If the port belongs to a trunk group, this command can't be applied.	switch(vlan)# vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q port 3 hybrid-link untag 5 tag 6-8
vlan 8021q trunk [PortNumber] access-link untag [UntaggedVID]	V	Assign a access link for VLAN by trunk group	switch(vlan)#vlan 8021q trunk 3 access-link untag 33
vlan 8021q trunk [PortNumber] trunk-link tag [TaggedVID List]	V	Assign a trunk link for a VLAN by trunk group	switch(vlan)#vlan 8021q trunk 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q trunk 3 trunk-link tag 3-20
vlan 8021q trunk [PortNumber] hybrid-link untag	V	Assign a hybrid link for VLAN by trunk group	switch(vlan)# vlan 8021q trunk 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q

Command	Level	Description	Example
[UntaggedVID] tag [TaggedVID List]			trunk 3 hybrid-link untag 5 tag 6-8
show vlan [GroupID] or show vlan	V	Show VLAN information	switch(vlan)#show vlan 23
no vlan group [GroupID]	V	Delete port based group ID	switch(vlan)#no vlan group 2

The following table lists the Spanning Tree Commands.

Command	Level	Description	Example
spanning-tree enable	G	Enable spanning tree	switch(config)#spanning-tree enable
spanning-tree priority [0~61440]	G	Configure spanning tree priority parameter	switch(config)#spanning-tree priority 32767
spanning-tree max-age [seconds]	G	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it will recompute the Spanning Tree Protocol (STP) topology.	switch(config)# spanning-tree max-age 15
spanning-tree hello-time [seconds]	G	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#spanning-tree hello-time 3
spanning-tree forward-time [seconds]	G	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding	switch(config)# spanning-tree forward-time 20

Command	Level	Description	Example
		time determines how long each of the listening and learning states last before the port begins forwarding.	
stp-path-cost [1~200000000]	I	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state.	switch(config)#interface fastEthernet 2 switch(config-if)#stp-path-cost 20
stp-path-priority [Port Priority]	I	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-path-priority 127
stp-admin-p2p [Auto|True|False]	I	Admin P2P of STP priority.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-p2p Auto
stp-admin-edge [True|False]	I	Admin Edge of STP priority.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-edge True
stp-admin-non-stp [True|False]	I	Admin NonSTP of STP priority.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-non-stp False
show spanning-tree	E	Display a summary of the spanning-tree states.	switch>show spanning-tree
no spanning-tree	G	Disable spanning-tree.	switch(config)#no spanning-tree

The following table lists the **QoS Commands**.

Command	Level	Description	Example
qos policy [weighted-fair|strict]	G	Select QOS policy scheduling	switch(config)#qos policy weighted-fair
qos prioritytype [port-based|cos-only|tos-only|cos-first|tos-first]	G	Use this command to set QOS priority type	switch(config)#qos prioritytype
qos priority portbased [Port] [lowest|low|middle|high]	G	Use this command to configure port-based priority	switch(config)#qos priority portbased 1 low
qos priority cos [Priority][lowest|low|middle|high]	G	Use this command to configure COS priority	switch(config)#qos priority cos 22 middle
qos priority tos [Priority][lowest|low|middle|high]	G	Configure TOS priority	switch(config)#qos priority tos 3 high
show qos	P	Displays the QoS configuration	switch>show qos
no qos	G	Disables QoS function	switch(config)#no qos

The following table lists the IGMP Commands.

Command	Level	Description	Example
igmp enable	G	Enables IGMP snooping function	switch(config)#igmp enable
Igmp-query auto	G	Set IGMP query to auto mode	switch(config)#Igmp-query auto
Igmp-query force	G	Set IGMP query to force mode	switch(config)#Igmp-query force
show igmp configuration	P	Displays the details of the IGMP configuration.	switch#show igmp configuration
show igmp multi	P	Displays the details of the IGMP snooping entries.	switch#show igmp multi
no igmp	G	Disables IGMP snooping function	switch(config)#no igmp

no igmp-query	G	Disable IGMP query	switch#no igmp-query

The following table lists the **MAC/Filter Table Commands**.

Command	Level	Description	Example
mac-address-table static hwaddr [MAC]	I	Configure static MAC address table.	switch(config)#interface fastEthernet 2 switch(config-if)#mac-address-table static hwaddr 000012345678
mac-address-table filter hwaddr [MAC]	G	Configure filter MAC address table.	switch(config)#mac-address-table filter hwaddr 000012348678
show mac-address-table	P	Display MAC address table (all)	switch#show mac-address-table
show mac-address-table static	P	Display static MAC address table	switch#show mac-address-table static
show mac-address-table filter	P	Display filter MAC address table.	switch#show mac-address-table filter
no mac-address-table static hwaddr [MAC]	I	Remove static entry of MAC address table	switch(config)#interface fastEthernet 2 switch(config-if)#no mac-address-table static hwaddr 000012345678
no mac-address-table filter hwaddr [MAC]	G	Remove filter entry of MAC address table	switch(config)#no mac-address-table filter hwaddr 000012348678
no mac-address-table	G	Remove dynamic entry of MAC address table	switch(config)#no mac-address-table

The following table lists **SNMP Commands**.

Command	Level	Description	Example
snmp system-name [System Name]	G	Set SNMP agent system name	switch(config)#snmp system-name l2switch
snmp system-location	G	Set SNMP agent system location	switch(config)#snmp system-location lab

Command	Level	Description	Example
[System Location]			
snmp system-contact [System Contact]	G	Set SNMP agent system contact	switch(config)#snmp system-contact where
snmp agent-mode [v1v2c|v3|v1v2cv3]	G	Select the agent mode of SNMP	switch(config)#snmp agent-mode v1v2cv3
snmp community-strings [Community] right [RO/RW]	G	Enter the SNMP community string.	switch(config)#snmp community-strings public right rw
snmp-server host [IP address] community [Community-string] trap-version [v1|v2c]	G	Configure SNMP server host and community string	switch(config)#snmp-server host 192.168.1.50 community public trap-version v1 (remove) Switch(config)# no snmp-server host 192.168.1.50
snmpv3 context-name [Context Name]	G	Configure the context name	switch(config)#snmpv3 context-name Test
snmpv3 user [User Name] group [Group Name] password [Authentication Password] [Privacy Password]	G	Configure the user profile for SNMPV3 agent. Privacy password can be left empty.	switch(config)#snmpv3 user test01 group G1 password AuthPW PrivPW
snmpv3 access context-name [Context Name] group	G	Configure the access table of SNMPV3 agent	switch(config)#snmpv3 access context-name Test group G1 security-level AuthPriv match-rule Exact views V1

Command	Level	Description	Example
[Group Name] security-level [NoAuthNoPriv| AuthNoPriv| AuthPriv] match-rule [Exact|Prifix] views [Read View Name] [Write View Name] [Notify View Name]			V1 V1
snmpv3 mibview view [View Name] type [Excluded| Included] sub-oid [OID]	G	Configure the mibview table of SNMPV3 agent	switch(config)#snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1
show snmp	P	Displays the SNMP configuration	switch#show snmp
no snmp community-strings [Community]	G	Remove the specified community.	switch(config)#no snmp community-strings public
no snmp-server host [Host-address]	G	Remove the SNMP server host.	switch(config)#no snmp-server 192.168.1.50
no snmp-server host [Host-address]	G	Remove the SNMP server host.	switch(config)#no snmp-server 192.168.1.50
no snmpv3 user [User Name]	G	Remove specified user of SNMPv3 agent.	switch(config)#no snmpv3 user Test
no snmpv3 access context-name [Context Name] group	G	Remove specified access table of SNMPv3 agent.	switch(config)#no snmpv3 access context-name Test group G1 security-level AuthPr iv match-rule Exact views V1 V1 V1

Command	Level	Description	Example
[Group Name] security-level [NoAuthNo Priv|AuthNoPriv |AuthPriv] match-rule [Exact|Prifix] views [Read View Name] [Write View Name] [Notify View Name]			
no snmpv3 mibview view [View Name] type [Excluded| Included] sub-oid [OID]	G	Remove specified mibview table of SNMPV3 agent.	switch(config)#no snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1

The following table lists the commands for **Port Mirroring**.

Command	Level	Description	Example
monitor rx	G	Set RX destination port for monitor function	switch(config)#monitor rx
monitor tx	G	Set TX destination port for monitor function	switch(config)#monitor tx
show monitor	P	Displays port monitor information	switch#show monitor
monitor [RX|TX|Both]	I	Configure source port for monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#monitor RX
show monitor	I	Displays port monitor information	switch(config)#interface fastEthernet 2 switch(config-if)#show monitor
no monitor	I	Disables source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#no monitor

The following table lists the commands for the **802.1x Security functions**.

Command	Level	Description	Example
8021x enable	G	The 802.1x global configuration command is used to enable 802.1x protocols.	switch(config)# 8021x enable
8021x system radiusip [IP address]	G	The 802.1x system radius IP global configuration command is used to change the radius server IP.	switch(config)# 8021x system radiusip 192.168.1.1
8021x system serverport [port ID]	G	The 802.1x system server port global configuration command is used to change the radius server port	switch(config)# 8021x system serverport 1815
8021x system accountport [port ID]	G	The 802.1x system account port global configuration command is used to change the accounting port	switch(config)# 8021x system accountport 1816
8021x system sharekey [ID]	G	The 802.1x system share key global configuration command is used to change the shared key value.	switch(config)# 8021x system sharekey 123456
8021x system nasid [words]	G	The 802.1x system nasid global configuration command is used to change the NAS ID	switch(config)# 8021x system nasid test1
8021x misc quietperiod [sec.]	G	The 802.1x misc quiet period global configuration command is used to specify the quiet period value of the switch.	switch(config)# 8021x misc quietperiod 10
8021x misc txperiod [sec.]	G	The 802.1x misc TX period global configuration command is used to set the TX period.	switch(config)# 8021x misc txperiod 5
8021x misc supportimeout [sec.]	G	The 802.1x misc supp timeout global configuration command is used to set the supplicant timeout.	switch(config)# 8021x misc supportimeout 20
8021x misc servertimeout [sec.]	G	The 802.1x misc server timeout global configuration command is used to set the	switch(config)#8021x misc servertimeout 20

Command	Level	Description	Example
		server timeout.	
8021x misc maxrequest [number]	G	The 802.1x misc max request global configuration command is used to set the MAX requests.	switch(config)# 8021x misc maxrequest 3
8021x misc reauthperiod [sec.]	G	The 802.1x misc reauth period global configuration command is used to set the reauth period.	switch(config)# 8021x misc reauthperiod 3000
8021x portstate [disable | reject | accept | authorize]	I	The 802.1x port state interface configuration command is used to set the state of the selected port.	switch(config)#interface fastethernet 3 switch(config-if)#8021x portstate accept
show 8021x	E	Displays a summary of the 802.1x properties and the port states.	switch>show 8021x
no 8021x	G	Disable 802.1x function	switch(config)#no 8021x

The following table lists the **TFTP Commands**.

Command	Level	Description	Example
backup flash:backup_ cfg	G	Save configuration to TFTP server. Must specify the IP address of the TFTP server and the file name.	switch(config)#backup flash:backup_cfg
restore flash:restore_ cfg	G	Upload configuration from TFTP server. Must specify the IP address of the TFTP server and the file name.	switch(config)#restore flash:restore_cfg
upgrade flash:upgrade_ fw	G	Upgrade firmware from the TFTP server. Must specify the IP address of TFTP server and the file name.	switch(config)#upgrade lash:upgrade_fw

The following table lists the **SystemLog, SMTP and Events** Commands.

Command	Level	Description	Example
systemlog ip [IP address]	G	Set IP address of system log server	switch(config)#systemlog ip 192.168.1.100
systemlog mode [client|server|both]	G	Specify the log mode	switch(config)#systemlog mode both
show systemlog	E	Display system log	Switch>show systemlog
show systemlog	P	Display system log, client and server information	switch#show systemlog
no systemlog	G	Disable system log function	switch(config)#no systemlog
smtp enable	G	Enable SMTP function	switch(config)#smtp enable
smtp serverip [IP address]	G	Configure SMTP server IP	switch(config)#smtp serverip 192.168.1.5
smtp authentication	G	Enable SMTP authentication	switch(config)#smtp authentication
smtp account [account]	G	Configure authentication account	switch(config)#smtp account user
smtp password [password]	G	Configure authentication password	switch(config)#smtp password
smtp rcptemail [Index] [Email address]	G	Configure e-mail address for receipt of alerts	switch(config)#smtp rcptemail 1 alert@test.com
show smtp	P	Display SMTP information	switch#show smtp
no smtp	G	Disable SMTP function	switch(config)#no smtp
event device-cold-start [Systemlog|SMTP|Both]	G	Set cold start event type	switch(config)#event device-cold-start both
event authentication-failure [Systemlog|SMTP|Both]	G	Set authentication failure event type	switch(config)#event authentication-failure both
event X --ring-topology-change	G	Set X-ring topology event type	switch(config)#event X --ring-topology-change both

Command	Level	Description	Example
[Systemlog| SMTP|Both]			
event systemlog [Link-UP|Link-Down|Both]	I	Set port event for system log	switch(config)#interface fastethernet 3 switch(config-if)#event systemlog both
event smtp [Link-UP|Link-Down|Both]	I	Set port event for SMTP	switch(config)#interface fastethernet 3 switch(config-if)#event smtp both
show event	P	Display event selection	switch#show event
no event device-cold-start	G	Disable cold start event type	switch(config)#no event device-cold-start
no event authentication-failure	G	Disable authentication failure event type	switch(config)#no event authentication-failure
no event X- -ring-topology-change	G	Disable X- ring topology event	switch(config)#no event X- -ring-topology-change
no event systemlog	I	Disable port event for system log	switch(config)#interface fastethernet 3 switch(config-if)#no event systemlog
no event smpt	I	Disable port event for SMTP	switch(config)#interface fastethernet 3 switch(config-if)#no event smtp
show systemlog	P	Display system log client & server information	switch#show systemlog

The following table lists the **SNTP Commands**.

Command	Level	Description	Example
sntp enable	G	Enable SNTP function	switch(config)#sntp enable
sntp daylight	G	Enable daylight savings time. If SNTP function is disabled, this command can't be applied.	switch(config)#sntp daylight
sntp daylight-period	G	Set period of daylight savings time. If SNTP function is	switch(config)# sntp daylight-period

Command	Level	Description	Example
[Start time] [End time]		disabled, this command can't be applied. Parameter format: [yyyymmdd-hh:mm]	20060101-01:01 20060202-01-01
sntp daylight-offset [Minute]	G	Set offset of daylight saving time. If SNTP function is disabled, this command can't be applied.	switch(config)#sntp daylight-offset 3
sntp ip [IP]	G	Set SNTP server IP. If SNTP function is disabled, this command can't be applied.	switch(config)#sntp ip 192.169.1.1
sntp timezone [Timezone]	G	Set timezone index, use the show sntp timzezone command to obtain more information of the index number	switch(config)#sntp timezone 22
show sntp	P	Displays SNTP information	switch#show sntp
show sntp timezone	P	Displays index number of time zone list	switch#show sntp timezone
no sntp	G	Disable SNTP function	switch(config)#no sntp
no sntp daylight	G	Disable daylight savings time	switch(config)#no sntp daylight

The following table lists the **X-Ring Commands**.

Command	Level	Description	Example
X - ring enable	G	Enable X-ring	switch(config)#Xring enable
X - ring master	G	Enable ring master	switch(config)#Xring master
X - ring couplering	G	Enable couple ring	switch(config)#Xring couplering
X - ring dualhoming	G	Enable dual homing	switch(config)#Xring dualhoming
X - ring ringport [1st Ring Port] [2nd Ring Port]	G	Configure first and second ring port	switch(config)#Xring ringport 7 8
X - ring couplingport [Coupling Port]	G	Configure coupling port	switch(config)#Xring couplingport 1
X - ring controlport	G	Configure control port	switch(config)#Xring controlport 2

Command	Level	Description	Example
[Control Port]			
X - ring homingport [Dual Homing Port]	G	Configure dual homing port	switch(config)#Xring homingport 3
show X - ring	P	Display X-ring information	switch#show Xring
no X - ring	G	Disable X-ring	switch(config)#no X ring
no X - ring master	G	Disable ring master	switch(config)# no Xring master
no X - ring couplering	G	Disable coupling ring	switch(config)# no Xring couplering
no X - ring dualhoming	G	Disable dual homing	switch(config)# no Xring dualhoming

7.0 Troubleshooting

All Waters' switching products are designed to provide reliability and consistently high performance in all network environments. The installation of Waters' MS1008-2G-4POE/PSX1008-2G-4PoE switch is a straightforward procedure (See Sections 3-5). Should problems develop during installation or operation, this section is intended to help locate, identify and correct these types of problems. Please follow the suggestions listed below prior to contacting your supplier. However, if you are unsure of the procedures described in this section or if the Waters' switch is not performing as expected, do not attempt to repair the unit; instead contact your supplier for assistance or contact Waters Network Systems' Customer Support Center at **800.328.2275** or email carolynl@watersnet.com.

7.1 Before Calling for Assistance

1. If difficulty is encountered when installing or operating the unit, refer back to the Installation Section of this manual. Also check to make sure that the various components of the network are operational and compatible.
2. Check the cables and connectors to ensure that they have been properly connected and the cables/wires have not been crimped or in some way impaired during installation. (About 90% of network downtime can be attributed to wiring and connector problems.)
3. Make sure that an AC power cord is properly attached to the switch.
4. Be certain that each AC power cord is plugged into a functioning electrical outlet. Use the PWR LEDs to verify each unit is receiving power.
5. If the problem is isolated to a network device other than the Waters' switch, it is recommended that the problem device be replaced with a known good device. Verify whether or not the problem is corrected. If not, go to next step. If the problem is corrected, the Waters' switch and its associated cables are functioning properly.
6. If the problem continues, contact Waters Network Systems Customer Service at

800.328.2275 or email carolynl@watersnet.com for assistance.

When Calling for Assistance

Please be prepared to provide the following information.

1. A complete description of the problem, including the following:
    a. The nature and duration of the problem
    b. Situations when the problem occurs
    c. The components involved in the problem
    d. Any particular application that, when used, appears to create the problem
2. An accurate list of Waters Network Systems product model(s) involved. Include the date(s) that you purchased the products from your supplier.
3. It is useful to include other network equipment models and related hardware, including personal computers, workstations, terminals and printers; plus, the various network media types being used.
4. A record of changes that have been made to your network configuration prior to the occurrence of the problem. Any changes to system administration procedures should all be noted in this record.

7.2 Return Material Authorization (RMA) Procedure

All returns for repair must be accompanied by a Return Material Authorization (RMA) number. To obtain an RMA number, call Waters Network Systems Customer Service at 800.328.2275 during business hours of 8:00 am to 5:00 pm (CT) or email carolynl@watersnet.com. When calling, please have the following information readily available:

- Name and phone number of your contact person
- Name of your company/institution
- Your shipping address
- Product name
- Failure symptoms, including a full description of the problem
- Waters Network Systems will carefully test and evaluate all returned products, will

repair products that are under warranty at no charge, and will return the warranty-repaired units to the sender with shipping charges prepaid (see Warranty Information at the end of this manual for complete details). However, if Waters cannot duplicate the problem or condition causing the return, the unit will be returned as: **No Problem Found**.

Waters Network Systems reserves the right to charge for the testing of non-defective units under warranty. Testing and repair of product that is not under warranty will result in a customer (user) charge.

7.3 Shipping and Packaging Information

Should you need to ship the unit back to Waters Network Systems, please follow these instructions: Package the unit carefully. It is recommended that you use the original container if available. Units should be wrapped in a "bubble-wrap" plastic sheet or bag for shipping protection. (You may retain all connectors and this Installation Guide.)

CAUTION: Do not pack the unit in Styrofoam "popcorn" type packing material. This material may cause electro-static shock damage to the unit.

Clearly mark the Return Material Authorization (RMA) number on the outside of the shipping container. Waters Network Systems is not responsible for your return shipping charges.

Ship the package to:

Waters Network Systems
Attention: Customer Service
945 37th Avenue, NW
Rochester, MN 55901

8.0 Warranty

Waters Network Systems'

Warranty Statement

Waters Network Systems' products are warranted against defects in materials and workmanship. The warranty period for each product will be provided upon request at the time of purchase. Unless otherwise stated, the warranty period is for the useable life of the product.

In the event of a malfunction or other indication of product failure attributable directly to faulty materials and/or workmanship, Waters Network Systems will, at its option, repair or replace the defective products or components at no additional charge as set for herein. This limited warranty does not include service to repair damage resulting from accident, disaster, misuse, neglect, lightning, acts of God, tampering or product modification.

If a product does not operate as warranted during the applicable warranty period, Waters shall, at its option and expense, repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item. All products that are replaced will become the property of Waters. Replacement products may be new or reconditioned. Any replaced or repaired product or part has a ninety (90) day warranty or the remainder of the initial warranty period, whichever is longer.

Waters shall not be responsible for any custom software or firmware, configuration information, or memory data of Customer contained in, stored on, or integrated with any products returned to Waters pursuant to any warranty.

Service under the warranty may be obtained by contacting Waters Network Systems and receiving a Return Material Authorization (RMA) number from Waters Network

Systems. Returned product accompanied with the issued RMA number and prepaid shipping will be repaired or replaced by Waters Network Systems. Repaired or replaced products will be returned at no cost to the original Buyer and shipped via the carrier and method of delivery chosen by Waters Network Systems.

A product's lifetime ends when service and repair for the product can no longer be obtained from the original manufacturer or its direct successor or assignee.
Specific warranty by product family is as follows:

ProSwitch-FixPort: Limited Lifetime
ProSwitch-FlexPort: Limited Lifetime
ProSwitch-GS Series Limited Lifetime
ProSwitch-Lite: 3 Years from date of manufacture (see note)
ProSwitch-POE Series Limited Lifetime
ProSwitch-Secure: Limited Lifetime (see note)
ProSwitch-SecureAir+: Limited Lifetime
ProSwitch-Xpress: Limited Lifetime
ProSwitch-Xtreme: Limited Lifetime (see note)
ProSwitch-CS and CSX 3 Years from date of manufacture (see note)
ProMedia Converters 3 Years from date of manufacture (see note)

Note: Warranty period for any and all external power supplies is one (1) year from date of purchase.

EXCEPT FOR THE EXPRESS WARRANTY SET FORTH ABOVE, *WATERS NETWORK SYSTEMS* GRANTS NO OTHER WARRANTIES, EXPRESSED OR IMPLIED, BY STATUTE OR OTHERWISE, REGARDING THE PRODUCTS, THEIR FITNESS FOR ANY PURPOSE, THEIR QUALITY, THEIR MERCHANTABILITY, OR OTHERWISE.

WATERS NETWORK SYSTEMS' LIABILITY UNDER THE WARRANTY SHALL BE LIMITED TO PRODUCT REPAIR, OR REPLACEMENT OF THE BUYER'S PURCHASE PRICE. IN NO EVENT SHALL *WATERS NETWORK SYSTEMS* BE LIABLE FOR THE COST OF PROCUREMENT OF SUBSTITUTE GOODS BY THE CUSTOMER OR FOR ANY CONSEQENTIAL OR INCIDENTAL DAMAGES FOR BREACH OR WARRANTY.

SOFTWARE: WATERS WARRANTS THAT THE SOFTWARE PROGRAMS LICENSED FROM IT WILL PERFORM IN SUBSTANTIAL CONFORMANCE TO THE PROGRAM SPECIFICATIONS THEREFORE FOR A PERIOD OF NINETY (90) DAYS FROM THE DATE OF SHIPMENT FROM WATERS OR ITS AUTHORIZED SALES AGENT. WATERS WARRANTS THE MAGNETIC MEDIA CONTAINING SOFTWARE AGAINST FAILURE DURING THE WARRANTY PERIOD. NO UPDATES ARE PROVIDED. WATERS SOLE OBLIGATION HEREUNDER SHALL BE (AT WATERS DISCRETION) TO REFUND THE PURCHASE PRICE PAID BY CUSTOMER FOR ANY DEFECTIVE SOFTWARE PRODUCTS OR TO REPLACE ANY DEFECTIVE MEDIA WITH SOFTWARE WHICH SUBSTANTIALLY CONFORMS TO WATERS APPLICABLE PUBLISHED SPECIFICATIONS. CUSTOMER ASSUMES RESPONSIBILITY FOR THE SELECTION OF THE APPROPRIATE APPLICATIONS PROGRAM AND ASSOCIATED REFERENCE MATERIALS. WATERS MAKES NO WARRANTY THAT ITS SOFTWARE PRODUCTS WILL WORK IN COMBINATION WITH ANY HARDWARE OR APPLICATIONS SOFTWARE PRODUCTS PROVIDED BY THIRD PARTIES, THAT THE OPERATION OF THE SOFTWARE PRODUCTS WILL BE UNINTERRUPTED OR ERROR FREE, OR THAT ALL DEFECTS IN THE SOFTWARE PRODUCTS WILL BE CORRECTED. FOR ANY THIRD PARTY PRODUCTS LISTED IN THE WATERS SOFTWARE PRODUCT DOCUMENTATION OR SPECIFICATIONS AS BEING COMPATIBLE, WATERS

WILL MAKE REASONABLE EFFORTS TO PROVE COMPATIBILITY, EXCEPT WHERE THE NON-COMPATIBILITY IS CAUSED BY A “BUG” OR DEFECT IN THE THIRD PARTY’S PRODUCT.

WARRANTIES EXCLUSIVE: IF A WATERS PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER’S SOLE REMEDY SHALL BE REPAIR, OR REPLACEMENT, AT WATERS OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. WATERS NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

WATERS SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER’S OR ANY THIRD PERSON’S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE) SHALL WATERS BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH

THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF WATERS OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. NOTHING HEREIN SHALL HAVE THE EFFECT OF LIMITING OR EXCLUDING WATERS'S LIABILITY FOR DEATH OR PERSONAL INJURY CAUSED BY NEGLIGENCE.

Waters Network Systems, LLC
5001 American Blvd. West, Suite 605
Minneapolis, MN 55437
Phone Number: 952.831.5604
Fax Number: 952.831.5605