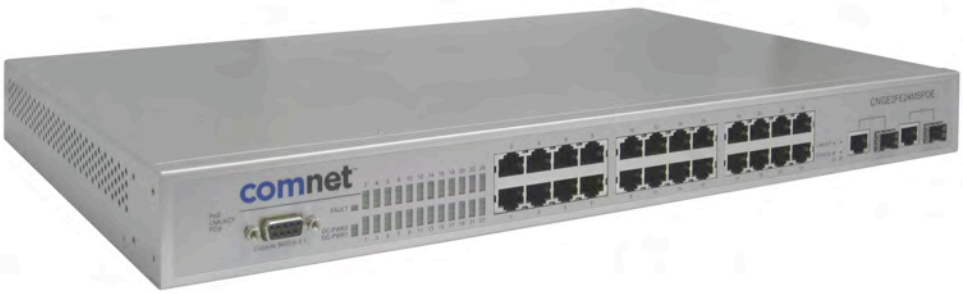
comnet
Communication Networks



INSTALLATION AND OPERATION MANUAL

CNGE2FE24MSPOE

ENVIRONMENTALLY HARDENED MANAGED ETHERNET SWITCH WITH (24) 10/100TX + (2) 10/100/1000FX RJ45 or 1000FX SFP PORTS

V1.02 – October 2009

The ComNet™ CNGE2FE24MSPoE Managed Ethernet Switch provides transmission of (24) 10/100 BASE-TX and (2) 10/100/1000TX or 1000FX combo ports. Unlike most Ethernet switches, these environmentally hardened units are designed for deployment in difficult operating environments, and are available for use with either conventional CAT-5e copper or optical transmission media. The 24 electrical ports support the 10/100 Mbps Ethernet IEEE 802.3 protocol, and auto-negotiating and auto-MDI/MDIX features are provided for simplicity and ease of installation. All 24 ports support IEEE.802.3af based POE. 2 ports are 10/100/1000 configurable for copper or fiber media for use with multimode or single mode optical fiber, selected by optional SFP modules. These network managed layer 2 switches are optically (1000 BASE-FX) and electrically compatible with any IEEE 802.3 compliant Ethernet devices. Plug-and-play design ensures ease of installation, and no electrical or optical adjustments are ever required. The CNGE2FE24MSPoE incorporates LED indicators for monitoring the operating status of the managed switch and network. These units are rack mountable.

Notice

The contents of this manual are based on the table below listing firmware version, software kernel version, and hardware version. If the switch functions are different from the description of contents of manual, please contact your local representative for more information.

Firmware Version	V2.10
Kernel Version	V5.57
Hardware Version	----------

FCC Warning

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

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

CE Mark Warning

This is a Class-A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Content

1 Introduction

The CNGE2FE24MSPOE Managed Industrial PoE Switch is a cost-effective solution and meets the high reliability requirements demanded by industrial applications. Using the fiber ports can extend the connection distance that increases the network elasticity and performance. The industrial switch provides the PoE function for Powered Devices to receive power as well as data over the RJ45 cable.

1.1 Hardware Features

IEEE Standard	IEEE 802.3 10Base-T Ethernet IEEE 802.3u 100Base-TX / 100Base-FX IEEE802.3z Gigabit fiber IEEE802.3ab 1000Base-T IEEE802.3x Flow Control and Back Pressure IEEE802.3ad Port trunk with LACP IEEE802.1d Spanning Tree/ IEEE802.1w Rapid Spanning Tree IEEE802.1p Class of Service IEEE802.1Q VLAN Tag IEEE 802.1x User Authentication (Radius) IEEE802.3af Power over Ethernet IEEE802.1ab LLDP
Switch Architecture	Back-plane (Switching Fabric): 8.8Gbps Packet throughput ability (Full-Duplex): 13.1Mpps@64bytes

Transfer Rate	14,880 pps for 10Base-T Ethernet port 148,800 pps for 100Base-TX/FX Fast Ethernet port 1,488,000 pps for Gigabit Fiber Ethernet port
Packet Buffer	4Mbits
MAC address	8K MAC address table
Flash ROM	4Mbytes
DRAM	32Mbytes
Jumbo Frame	9022bytes (for Gigabit Ports)
Connector	(Front) RS-232 : Female DB-9 (for Console) (Rear) RS-232: Male DB-9 (for UPWM) 10/100TX: 24 x RJ45 10/100/1000T/ Mini-GBIC Combo: 2 x RJ45 + 2 x SFP sockets
LED	**System Power** (Green) **Gigabit Fiber**: Link/Activity (Green) **Gigabit Copper:** Link/Activity (Green), Full duplex/collision (Yellow), Mini-GBIC [(Link/Activity) Green]
Network Cable	10Base-T: 2-pair UTP/STP Cat. 3, 4, 5, 5e cable EIA/TIA-568 100-ohm (100m) 100Base-TX: 2-pair UTP/STP Cat. 5/5e cable EIA/TIA-568 100-ohm (100m) 1000Base-T: 2-pair UTP/STP Cat. 5e cable EIA/TIA-568 100-ohm (100m)

Power Supply	DC 48V A readily accessible disconnect device as part of the building installation shall be incorporated into the fixed wiring. Moreover, The disconnect device (appropriate circuit breaker) must be included in the ungrounded supply conductor.
Redundant Power Supply	DC 48V
Power Consumption	335 Watts
Operating Temp.	-40°C to +75°C
Operation Humidity	5% to 95% (Non-condensing)
Storage Temperature	-40°C to 85°C
Fan	Fanless
Case Dimension	440mm (W) x 280mm (D) x 44mm (H)
Installation	19” Rack mount
EMI	FCC Class A CE EN61000-4-2/3/4/6/8, CE EN61000-6-2, CE EN61000-6-4
Safety	UL cUL CE/EN60950-1

Stability testing	IEC60068-2-32 (Free fall) IEC60068-2-27 (Shock) IEC60068-2-6 (Vibration)

1.2 Software Feature

Management	SNMP v1 SNMP v2c SNMP v3 Web/Telnet/Console (CLI)
SNMP MIB	RFC 2418 SNMP MIB, RFC 1213 MIBII, RFC 2011 SNMP V2 MIB, RFC 1493 Bridge MIB, RFC 2674 VLAN MIB, RFC 1215 Trap MIB, RFC 1643 Ethernet Like, RFC 1757 RMON1, RSTP MIB, PoE MIB, UPS MIB, LLDP MIB, Private MIB
VLAN	Port based VLAN, up to 24 groups IEEE802.1Q Tag VLAN Static VLAN groups up to 256, Dynamic VLAN group up to 2048, VLAN ID from 1 to 4094. GVRP up to 256 groups.
Port Trunk with LACP	LACP Port Trunk: 13 Trunk groups/Maximum 4 trunk members

LLDP	Supports LLDP to allow switch to advertise its identification and capability on the LAN
Spanning Tree	Supports IEEE802.1d Spanning Tree and IEEE802.1w Rapid Spanning Tree
X-Ring	Supports X-Ring, Dual Homing, Couple Ring and Central Ring topology Provides redundant backup feature and the recovery time below 20ms
Quality of service	The quality of service determined by port, Tag and IPv4 Type of service, IPv4 Different Service
Class of Service	Supports IEEE802.1p class of service, per port provides 4 priority queues
Port Security	Supports 50 entries of MAC address for static MAC and another 50 for MAC filter
Port Mirror	Supports 3 mirroring types: “RX, TX and Both packet”
IGMP	Supports IGMP snooping v1, v2 256 multicast groups and IGMP query
IP Security	Supports 10 IP addresses that have permission to access the switch management and to prevent unauthorized intruder
Login Security	Supports IEEE802.1X Authentication/RADIUS
Access Control List (ACL)	Supports up to 255 Policy

Bandwidth Control	Support ingress packet filter and egress packet limit The egress rate control supports all of packet type and the limit rates are 0~100Mbps Ingress filter packet type combination rules are Broadcast/Multicast/Unknown Unicast packet, Broadcast/Multicast packet, Broadcast packet only and all of packet. The packet filter rate can be set from 0 to 100Mbps
Flow Control	Supports Flow Control for Full-duplex and Back Pressure for Half-duplex
System log	Supports System log record and remote system log server
SMTP	Supports 1 SMTP Server and 6 e-mail accounts for receiving event alert
Relay Alarm	Provides one relay output for port breakdown and power failure. Alarm Relay current carry ability: 1A @ DC 24V
SNMP Trap	1. Device cold start, 2. Authorization failure, 3. X-Ring topology changed. 4. Port link up/ link down. 5. DC disconnect trap-PoE port Event Trap station up to 3
DHCP	Provides DHCP Client/DHCP Server/IP Relay functions
DNS	Provides DNS client feature Supports Primary and Secondary DNS server

SNTP	Supports SNTP to synchronize system clock in Internet
Firmware Upgrade	Supports TFTP & Console firmware update
Configuration Upload and Download	Supports binary format configuration file for system quick installation (TFTP backup and restore)
ifAlias	Each port allows importing 128bit of alphabetic string of word on SNMP and CLI interface.

1.3 **Package Contents**

Please refer to the package contents list below to verify them against the checklist.

- CNGE2FE24MSPOE Managed Industrial PoE Switch x 1
- User manual x 1
- Pluggable Terminal Block x 1
- Mounting plate x 2
- DB-9P/F TO DB-9P/M 150cm RoHS cable x 1
- Rubber feet x 4

Compare the contents with the standard checklist above. If any item is damaged or missing, please contact your local representative for service.

2 Hardware Description

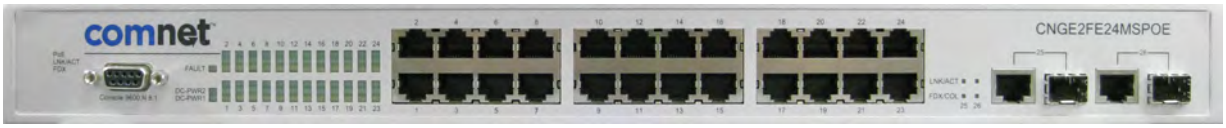
In this paragraph, the Industrial switch's hardware spec, port, cabling information, and wiring installation will be described.

2.1 Physical Dimension

CNGE2FE24MSPOE Managed Industrial PoE Switch dimensions (W x D x H) are **440mm x 280mm x 44mm**

2.2 Front Panel

The Front Panel of the CNGE2FE24MSPOE Managed Industrial PoE Switch is shown below:



Front Panel of the CNGE2FE24MSPOE Industrial Switch

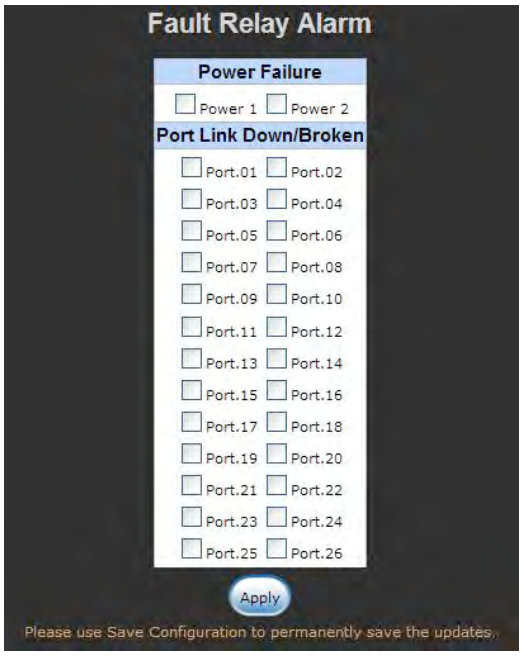
2.3 Rear Panel

The rear panel of the CNGE2FE24MSPOE Managed Industrial PoE Switch has one terminal block connector. The ten-pin screw clamp terminal strip is for power supply connections and connections to the fault relay. Redundant power sources may be used.

The fault relay can be configured to change from its normally open state in response to any or all of the following conditions using the GUI check boxes shown in the image below:

- failure of power supply 1
- failure of power supply 2

- failure or a port
- failure of a link to the port



Pin-outs follow:

PWR1

Pin 1 or Pin 2 = +48 VDC

Pin 3 or Pin 4 = -48 VDC

PWR2

Pin 7 or Pin 8 = +48 VDC

Pin 9 or Pin 10 = -48 VDC

Fault

Pin 5 and Pin 6 = normally open relay secondary, contacts rated at 24 VDC 1A max, resistive loads only

Rear panel of the CNGE2FE24MSPOE Industrial Switch

2.4 LED Indicators

The diagnostic LEDs located on the front panel of the industrial switch provide real-time information of the system and optional status. The following table provides the description of the LED status and their meanings for the switch.

LED	Status	Description
Fault	Red	DC power input 1 or 2 is inactive or port link down
	Off	DC power 1/DC Power 2/port linking are all active, or no power inputs
DC-PWR1	Green	DC power input 1 is active
	Off	DC power input 1 is inactive
DC-PWR2	Green	DC power input 2 is active
	Off	DC power input 2 is active
PoE	Green	A powered device is connected utilizing Power over Ethernet on the port
	Off	No device is connected or power forwarding fails
LNK/ACT	Green	The port is connecting with the device.
	Blink	The port is receiving or transmitting data.
	Off	No device attached.
FDX	Amber	The port is operating in Full-duplex mode.
	Off	In Half-duplex mode
LNK/ACT (Gigabit	Green	The port is connecting with the device.

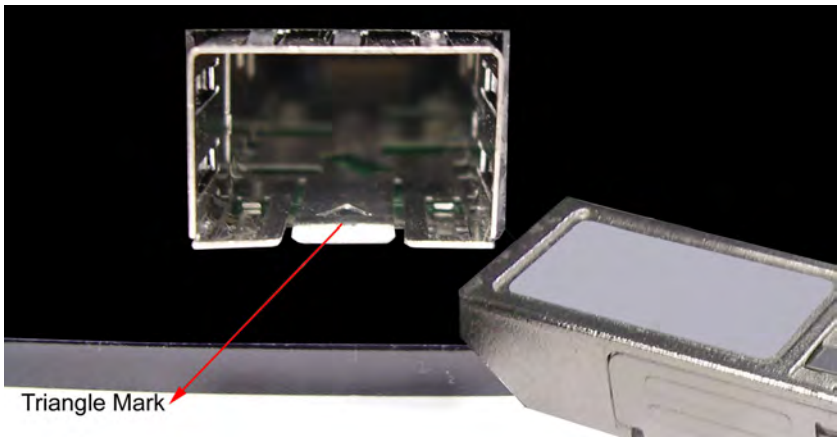
port) **25/26 port**	Blink	The port is receiving or transmitting data.
	Off	No device attached
FDX/COL (Gigabit port) **25/26 port**	Amber	The port is operating in Full-duplex mode
	Blink	Collision of Packets occurs in the port
	Off	In Half-duplex mode

2.5 Cabling

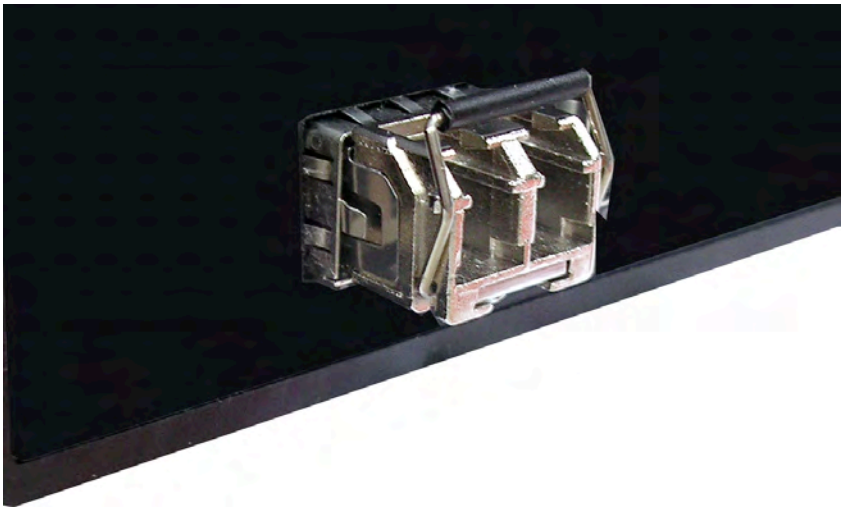
- Use four twisted-pair, Category 5e or above cabling for RJ45 port connection. The cable between the switch and the link partner (switch, hub, workstation, etc.) must be less than 100 meters (328 ft.) long.
- Use fiber optic cabling and connectors which are suitable for the selected SFP fiber module installed. The maximum transmission distance will be determined by the selected SFP module.

To connect the SFP transceiver using LC connectors, please follow the steps shown below:

First, insert the transceiver into the SFP module. Notice that the triangle mark is the bottom of the module.

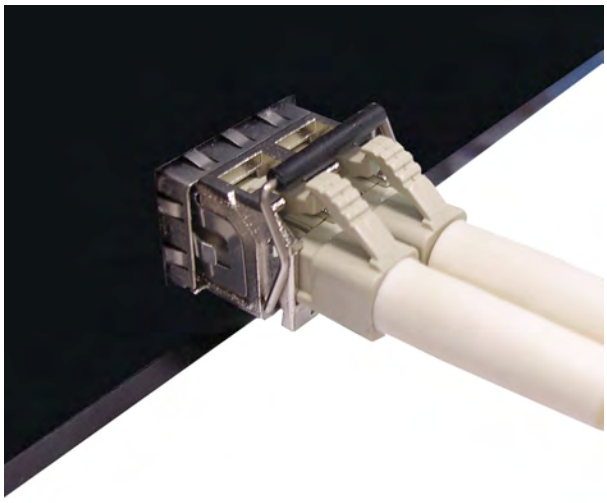


Transceiver to the SFP module



Transceiver Inserted

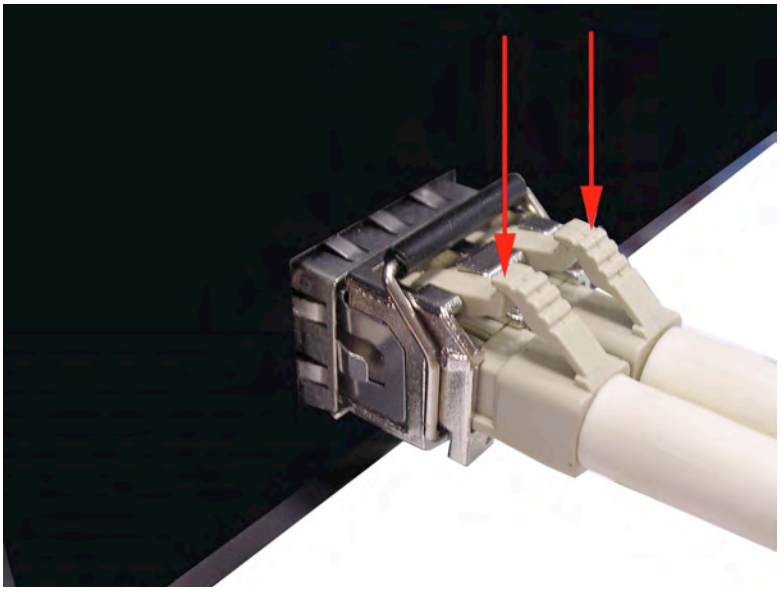
Second, insert the fiber cables LC connector into the transceiver.



LC connector to the transceiver

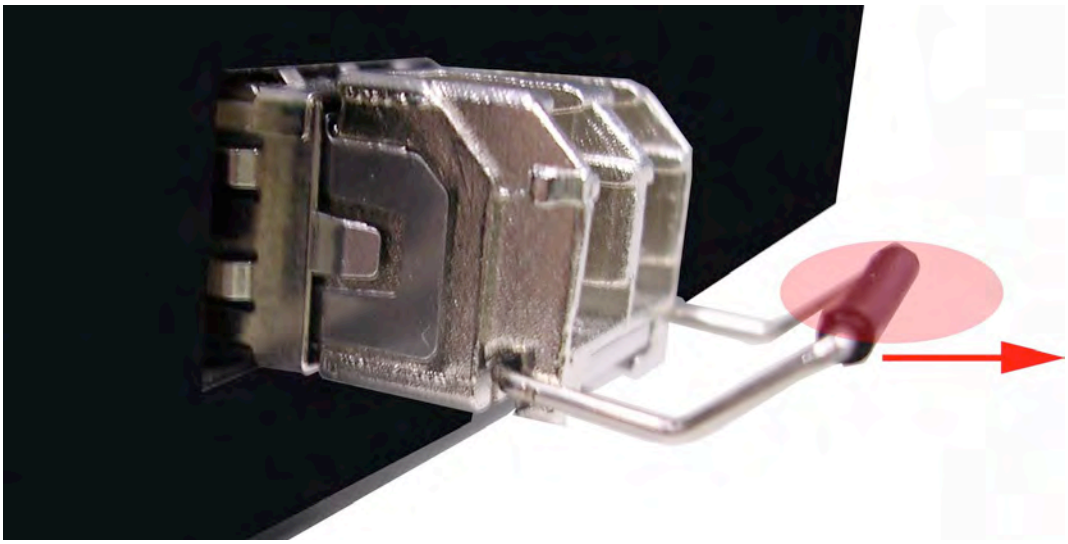
To remove the LC connector from the transceiver, please follow the steps shown below:

First, press the upper side of the LC connector to release from the transceiver and pull it out.



Remove LC connector

Second, push down the metal loop and pull the transceiver out by the plastic handle.



Pull out from the transceiver

2.6 Desktop Installation

Set the switch on a sufficiently large flat space with a power outlet nearby. The surface where you put your switch should be clean, smooth, level and sturdy.

Make sure there is enough clearance around the switch to allow attachment of cables, power cord and allow air circulation.

2.6.1 **Attaching Rubber Feet**

A. Make sure mounting surface on the bottom of the switch is grease and dust free.
B. Remove adhesive backing from your Rubber Feet.
C. Apply the Rubber Feet to each corner on the bottom of the switch. These footpads can help prevent shock/vibration.

Attaching Rubber Feet to each corner on the bottom of the Switch

2.7 Rack-mounted Installation

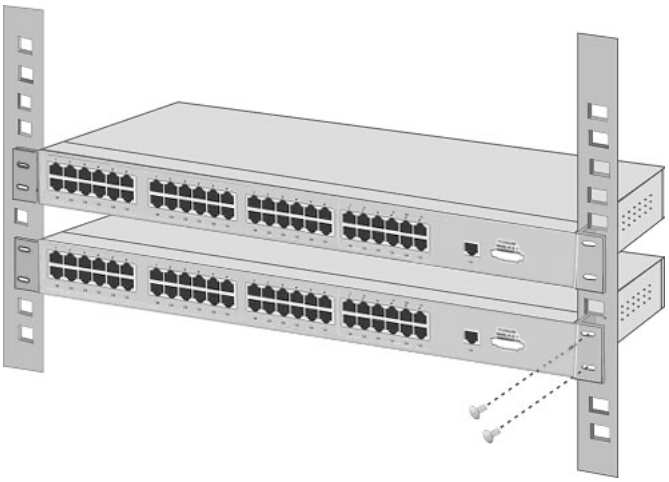
The Switch comes with a rack-mounted kit and can be mounted in an EIA standard size, 19-inch Rack. It can be placed in a wiring closet with other equipment.

Perform the following steps to rack-mount the switch:

A. Position one plate to align with the holes on one side of the hub and secure it with the smaller plate screws. Then, attach the remaining plate to the other side of the switch.

Attach mounting plates with screws

B. After attaching both mounting plates, position the switch in the rack by lining up the holes in the plates with the appropriate holes on the rack. Secure the switch to the rack with a screwdriver and suitable rack-mounting screws.

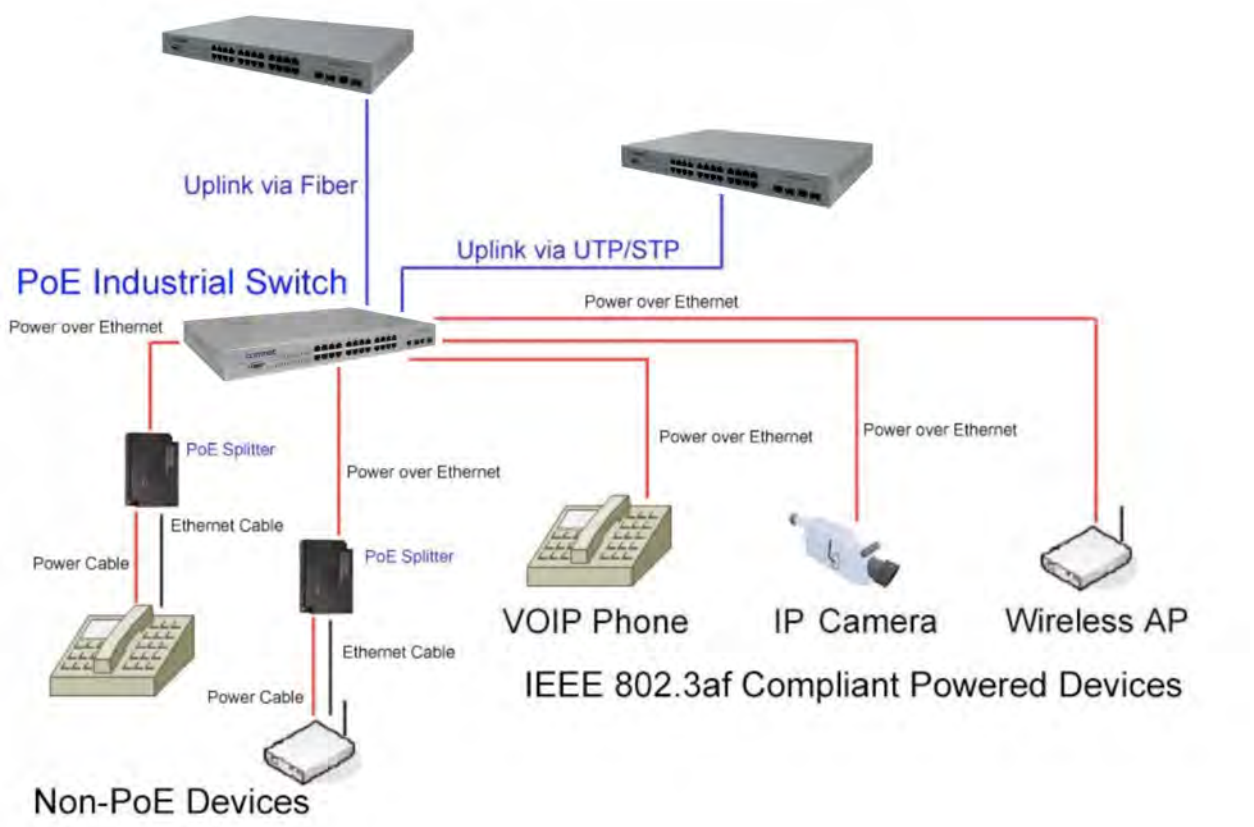


Mount the Switch in an EIA standard 19-inch Rack

Note: For proper ventilation, allow at least 4 inches (10 cm) of clearance on the front and 3.4 inches (8 cm) on the back of the switch. This is especially important for enclosed rack installation.

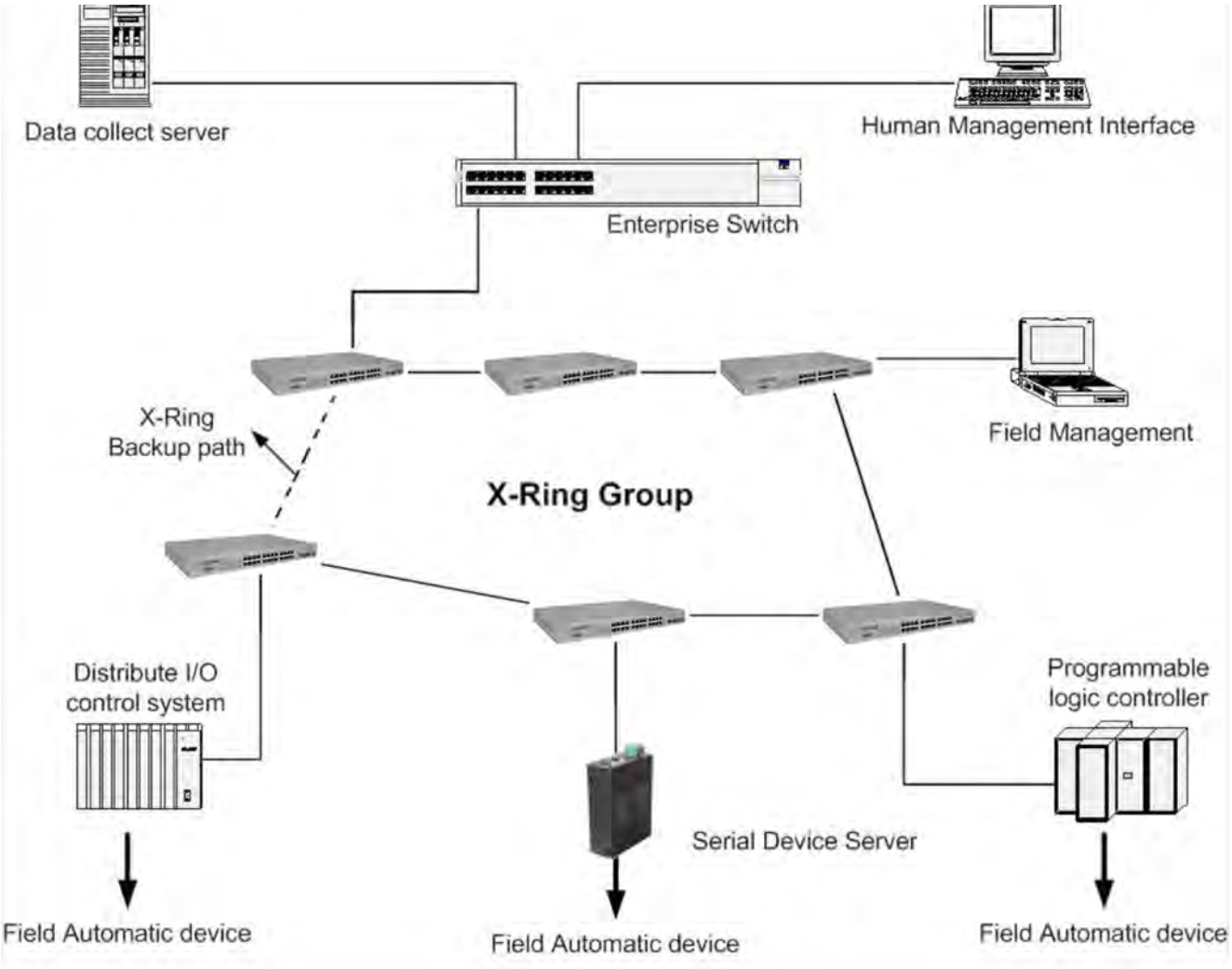
3 Network Application

This segment provides samples to help the user understand industrial switch applications. For sample applications of the industrial switch, see the figures below.



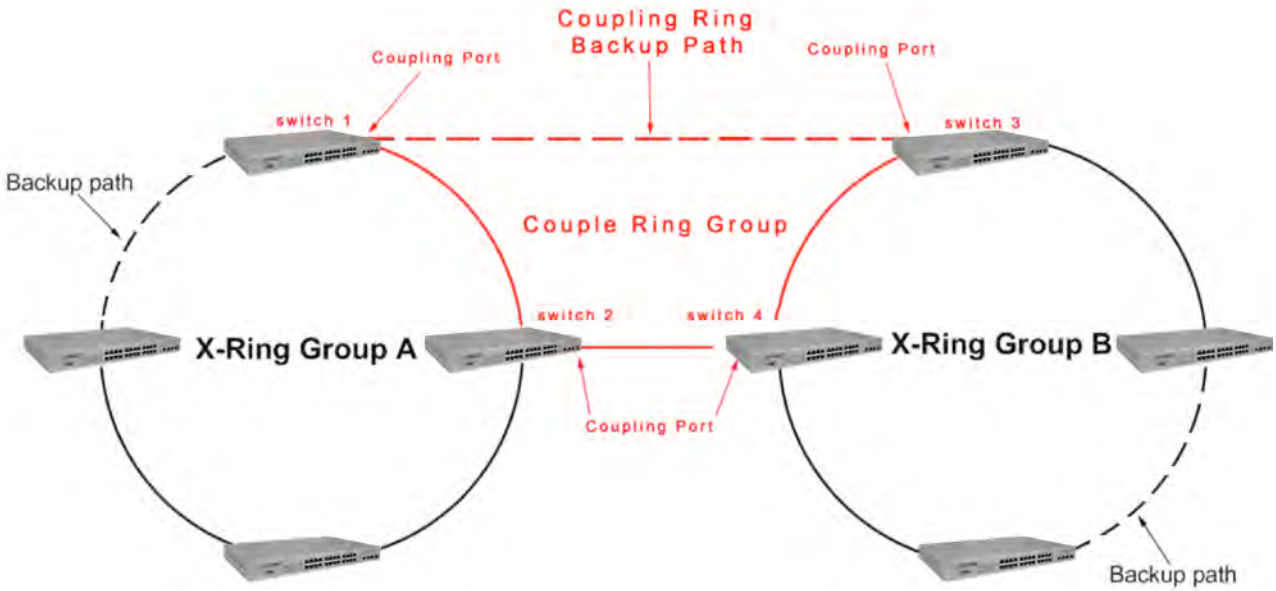
3.1 X-Ring Application

The industrial switch supports the X-Ring protocol that can help the network system to recover from network connection failure within 20ms or less, and make the network system more reliable. The X-Ring algorithm is similar to Spanning Tree Protocol (STP) and Rapid STP (RSTP) algorithm but its recovery time is less than STP/RSTP. The figure below is a sample of an X-Ring application.



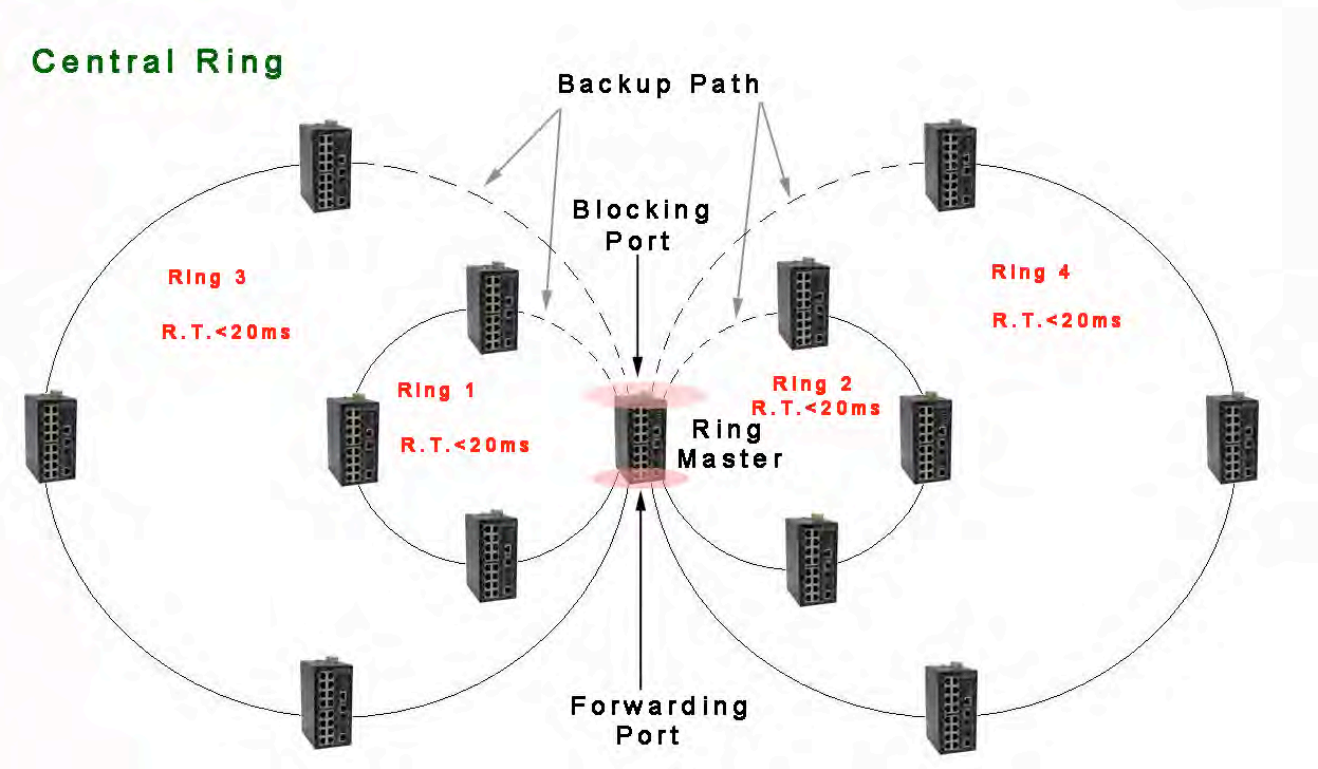
3.2 Couple Ring Application

In the network, it may have more than one X-Ring group. Using the coupling ring function can connect each X-Ring for redundant backup. It can ensure the transmissions between two ring groups do not fail. The following figure is a sample of coupling ring application.



3.3 Central Ring Application

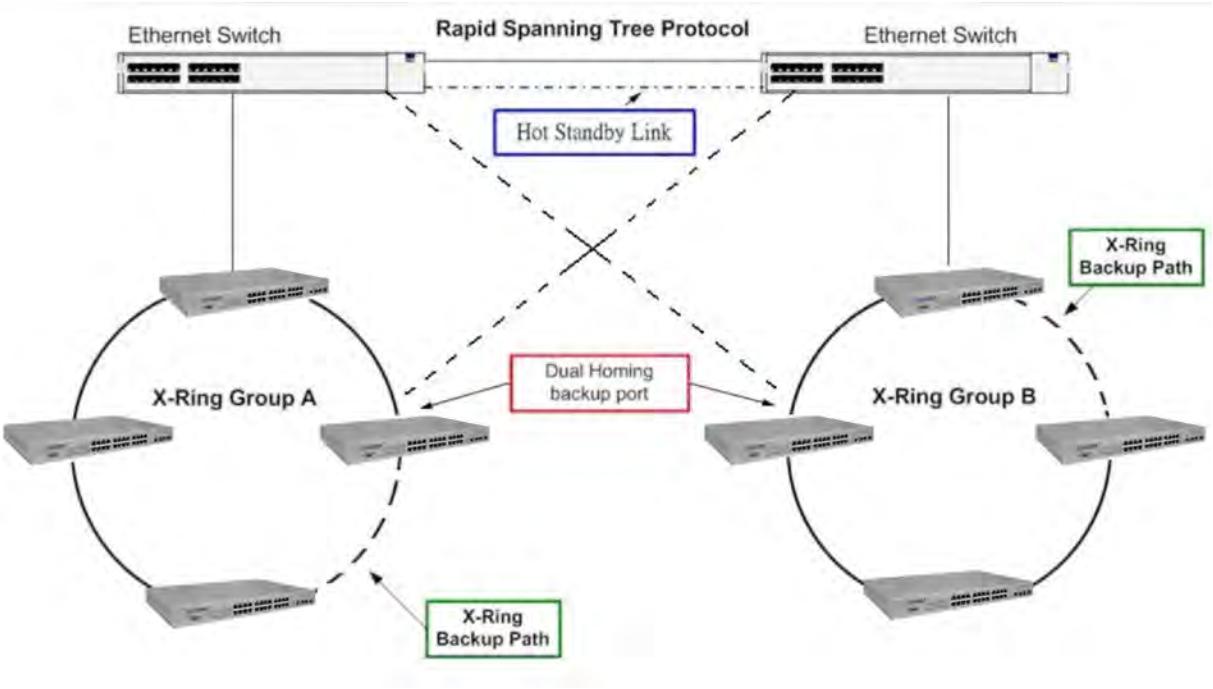
Central Ring is an advanced function which supports backup connection for redundant transmission. When the connection fails, the system will recover from failure within 20 milliseconds. Central Ring can also handle up to 4 rings by configuring a single switch only as the ring master switch.



3.4 Dual Homing Application

Dual Homing function is to prevent a connection loss between X-Ring group(s) and upper level/core switches. Assign one port to be the Dual Homing port that is the backup port in the X-Ring group. The Dual Homing function only works when the X-Ring function is active. Each X-Ring group only has one Dual Homing port.

[NOTE] In Dual Homing application architecture, the upper level switches need to enable the Rapid Spanning Tree protocol.



4 Console Management

4.1 Connecting to the Console Port

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

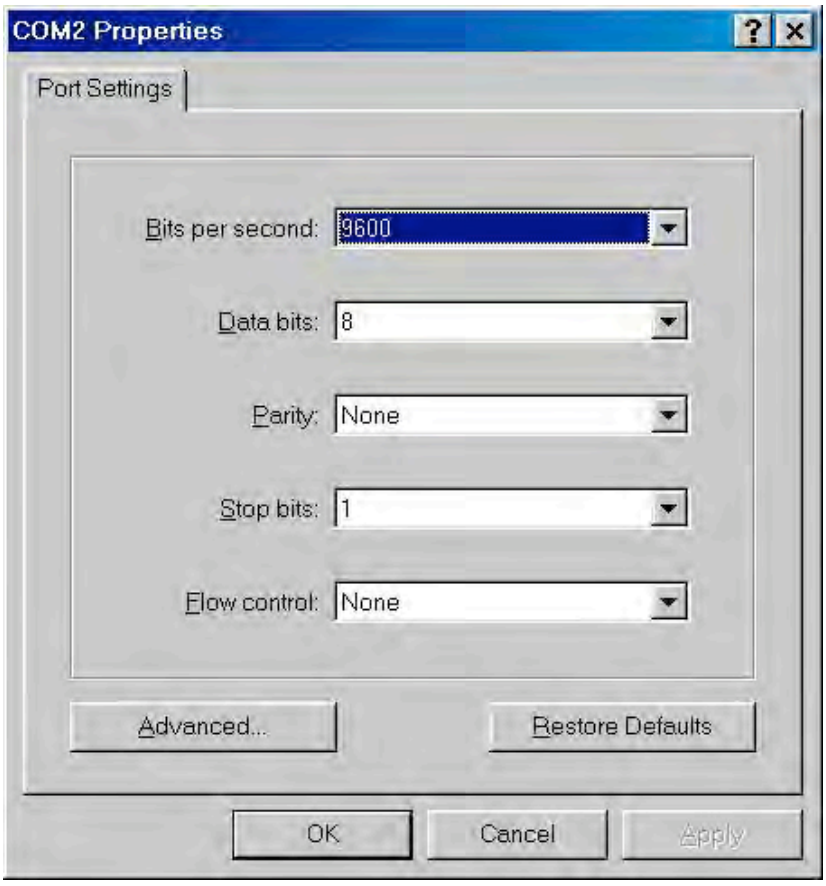
Connecting the switch to a terminal via RS-232 cable

4.2 Login in the Console Interface

When the connection between Switch and PC is ready, turn on the PC and run a terminal emulation program or **Hyper Terminal** and configure its **communication parameters** to match the following default characteristics of the console port:

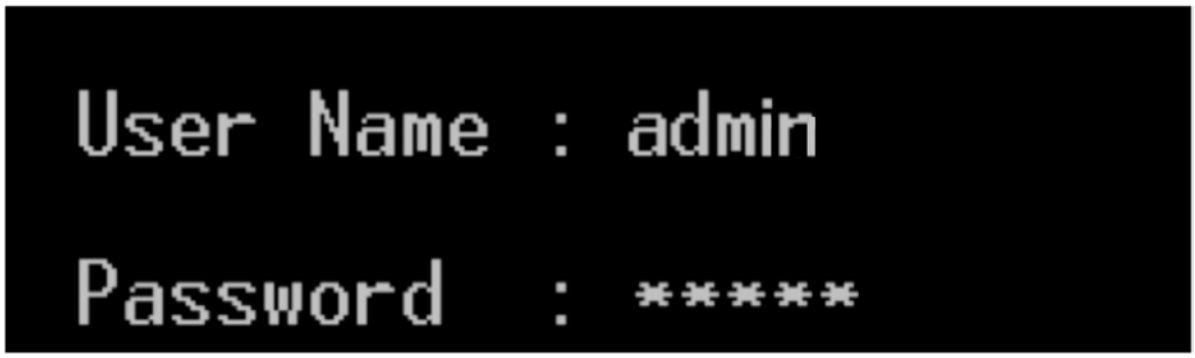
Baud Rate: 9600 bps
Data Bits: 8
Parity: none
Stop Bit: 1

Flow control: None



The settings of communication parameters

After finishing the parameter settings, select '**OK'**. When the blank screen shows up, press **Enter** key to bring out the login prompt. Key in '**admin**' (default value) for both User name and Password (use **Enter** key to switch), then press **Enter** key and the Main Menu of console management appears.



Console login interface

4.3 CLI Management

The system supports the console management—CLI command. After you log in on the system, you will see a command prompt. To enter CLI management interface, type in "**enable**" command.

CLI command interface

The following table lists the CLI commands and description.

Modes	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with your switch.	switch>	Enter **logout** or **quit**.	The user commands available at the user level are a subset of those available at the privileged level. Use this mode to • Perform basic tests. • Display system information.
Privileged EXEC	Enter the **enable** command while in User EXEC mode.	switch#	Enter **disable** to exit.	The privileged command is the advanced mode. Use this mode to • Display advanced function status • Save configuration

Global Configuration	Enter the **configure** command while in privileged EXEC mode.	switch (config)#	To exit to privileged EXEC mode, enter **exit** or **end**	Use this mode to configure those parameters that are going to be applied to your switch.
VLAN database	Enter the **vlan database** command while in privileged EXEC mode.	switch (vlan)#	To exit to user EXEC mode, enter **exit**.	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the **interface** of fast Ethernet command (with a specific interface) while in global configuration mode	switch (config-if)#	To exit to global configuration mode, enter **exit**. To exit to privileged EXEC mode, enter **exit** or **end**.	Use this mode to configure parameters for the switch and Ethernet ports.

5 Web-Based Management

This section introduces the configuration and functions of the Web-Based management.

5.1 About Web-based Management

There is an embedded HTML web site residing in flash memory on the CPU board of the switch, which offers advanced management features and allows users to manage the switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The Web-Based Management supports Internet Explorer 6.0 or later version. And, it is applied for Java Applets for reducing network bandwidth consumption, enhance access speed and present an easy viewing screen.

5.2 Preparing for Web Management

Before using the web management, install the industrial switch on the network and make sure that any one of the PCs on the network can connect with the industrial switch through the web browser. The industrial switch default value of IP, subnet mask, username and password are listed as below:

- IP Address: **192.168.10.1**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.168.10.254**
- User Name: **admin**
- Password: **admin**

5.3 System Login

1. Launch Internet Explorer on the PC
2. Key in “http:// then enter the IP address of the switch, and then Press “**Enter**”.

3. The login screen will appear right after.
4. Key in the user name and password. The default user name and password are the same as ‘**admin’**
5. Press **Enter** or select **OK**, and then the home screen of the Web-based management shows up.

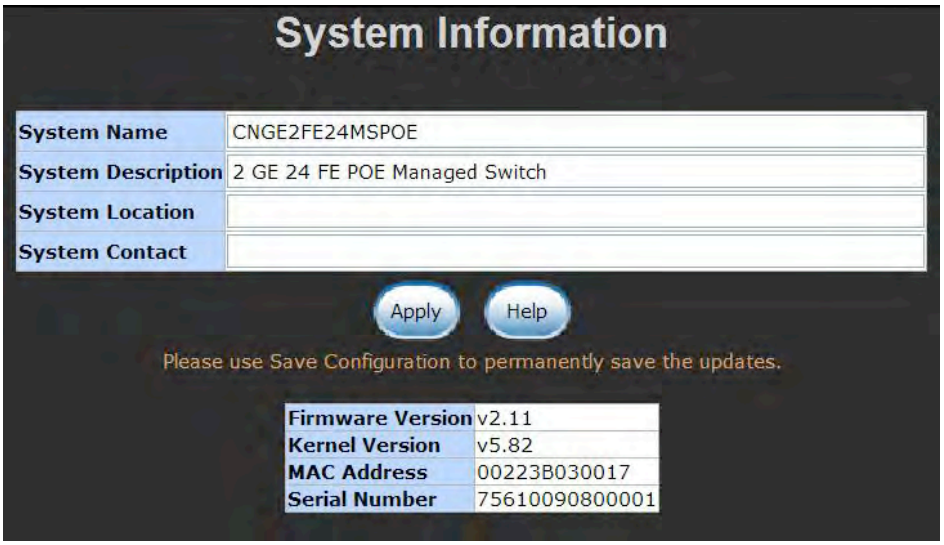
6 System

6.1 System Information

Assign the system name and location and view the system information.

- **System Name:** Assign the system name of the switch (The maximum length is 64 bytes)
- **System Description:** Describes the switch.
- **System Location:** Assign the switch physical location (The maximum length is 64 bytes).
- **System Contact:** Enter the name of contact person or organization.
- **Firmware Version:** Displays the switch's firmware version.
- **Kernel Version:** Displays the kernel software version.
- **MAC Address:** Displays the unique hardware address assigned by manufacturer (default).
- And then, select 

.



System information interface

6.2 IP Configuration

User can configure the IP Settings and DHCP client function here.

- **DHCP Client:** Enable or disable the DHCP client function. When DHCP client function is enabled, the industrial switch will be assigned an IP address from the network DHCP server. The default IP address will be replaced by the assigned IP address from the DHCP server. After user selects **Apply**, a popup dialog box shows up. It is to inform the user that when the DHCP client is enabled, the current IP address will be lost and the user should find the new IP address on the DHCP server.
- **IP Address:** Assign the IP address that the network is using. If DHCP client function is enabled, then the user does not need to assign the IP address. The network DHCP server will assign the IP address displaying it in this column for the industrial switch. The default IP is 192.168.10.1.
- **Subnet Mask:** Assign the subnet mask to the IP address. If DHCP client function is enabled, and then the user does not have to assign the subnet mask.
- **Gateway:** Assign the network gateway for the industrial switch. The default gateway is 192.168.10.254.
- **DNS1:** Assign the primary DNS IP address.
- **DNS2:** Assign the secondary DNS IP address.
- And then, select 

.

IP configuration interface

6.3 DHCP Server – System configuration

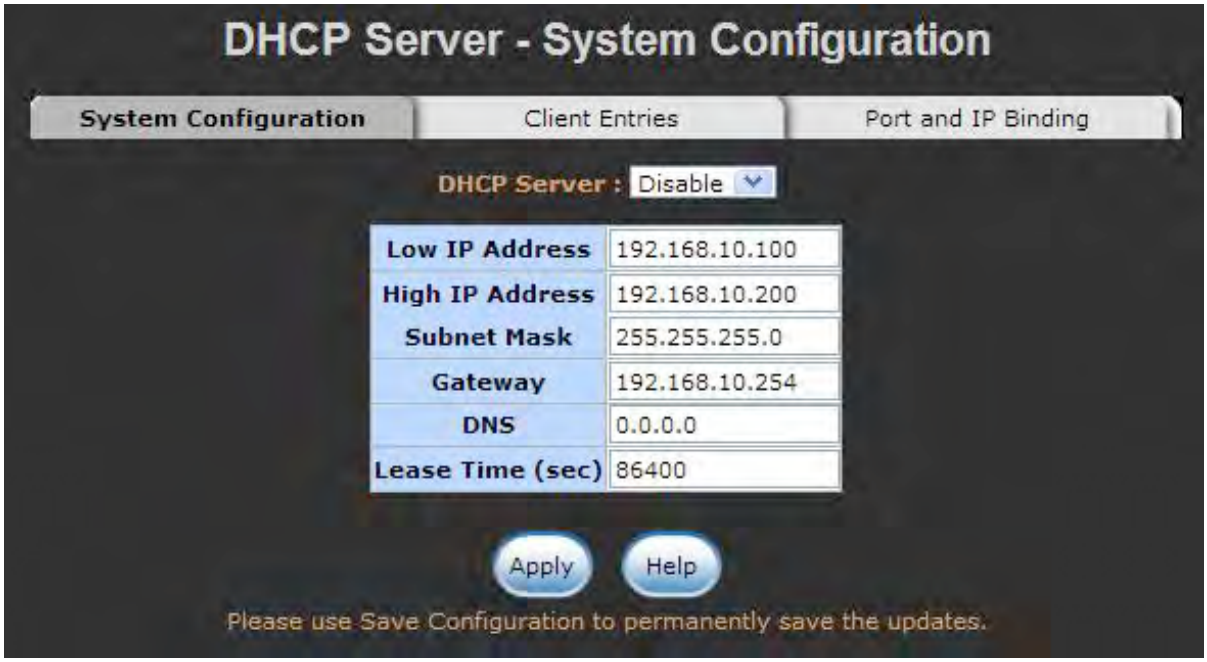
DHCP is the abbreviation of Dynamic Host Configuration Protocol that is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change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

The system provides the DHCP server function. Enable the DHCP server function, the switch system will be a DHCP server.

- **DHCP Server:** Enable or Disable the DHCP Server function. Enable—the switch will be the DHCP server on your local network.
- **Low IP Address:** Type in an IP address. Low IP address is the beginning of the dynamic IP range. For example, dynamic IP is in the range between 192.168.1.100 ~ 192.168.1.200. In contrast, 192.168.1.100 is the Low IP address.
- **High IP Address:** Type in an IP address. High IP address is the end of the dynamic IP range. For example, dynamic IP is in the range between 192.168.1.100 ~

192.168.1.200. In contrast, 192.168.1.200 is the High IP address.

- **Subnet Mask:** Type in the subnet mask of the IP configuration.
- **Gateway:** Type in the IP address of the gateway in your network.
- **DNS:** Type in the Domain Name Server IP Address in your network.
- **Lease Time (sec):** It is the time period that system will reset the dynamic IP assignment to ensure the dynamic IP will not been occupied for a long time or the server does not know that the dynamic IP is idle.
- And then, select 



DHCP Server Configuration interface

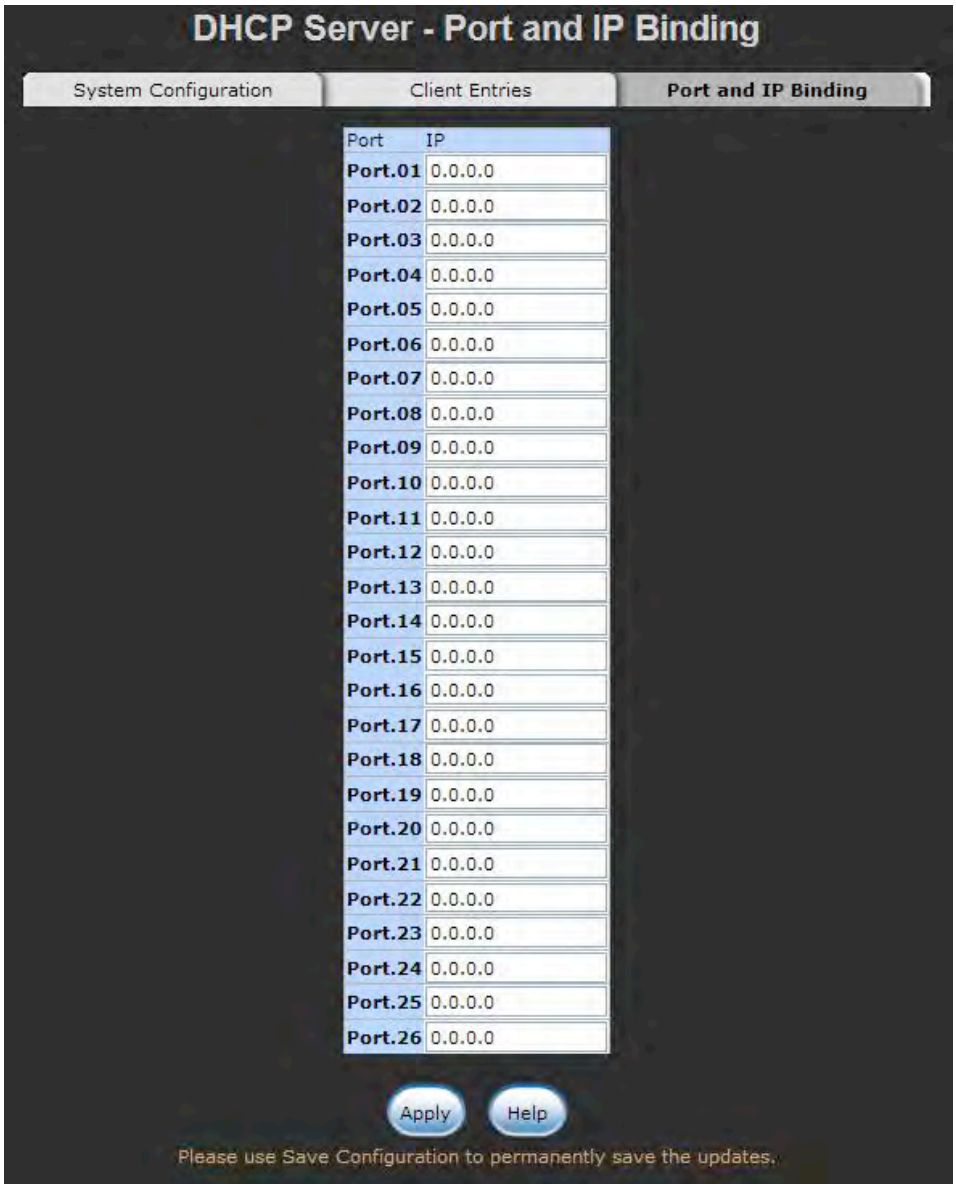
6.4 DHCP Server – Client Entries

When the DHCP server function is active, the system will collect the DHCP client information and displays it at this tab.

DHCP Client Entries interface

6.5 DHCP Server - Port and IP Binding

Assign the dynamic IP address to the port. When the device is connecting to the port and asks for IP assigning, the system will assign the IP address that has been assigned before to the connected device.

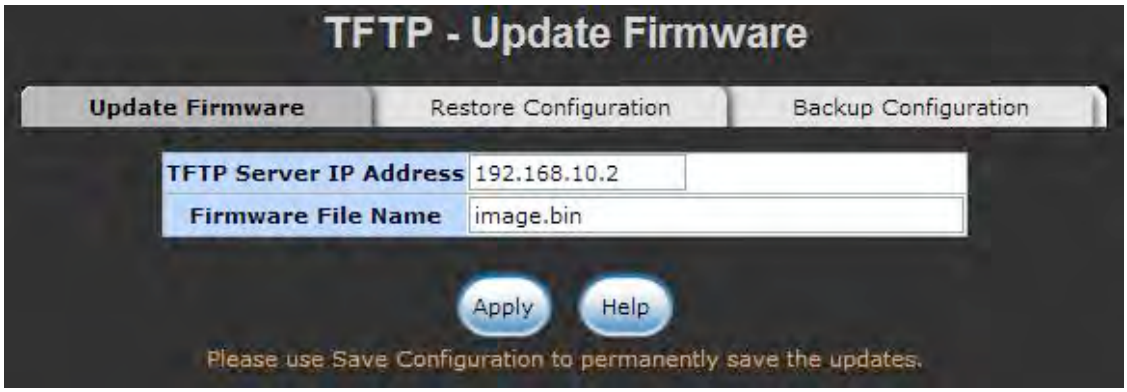


Port and IP Bindings interface

6.6 TFTP - Update Firmware

It provides the functions that allow user to update the switch firmware. Before updating, make sure the TFTP server is ready and the firmware image is located on the TFTP server.

1. **TFTP Server IP Address:** Type in your TFTP server IP.
2. **Firmware File Name:** Type in the name of firmware image.
3. Select Apply.

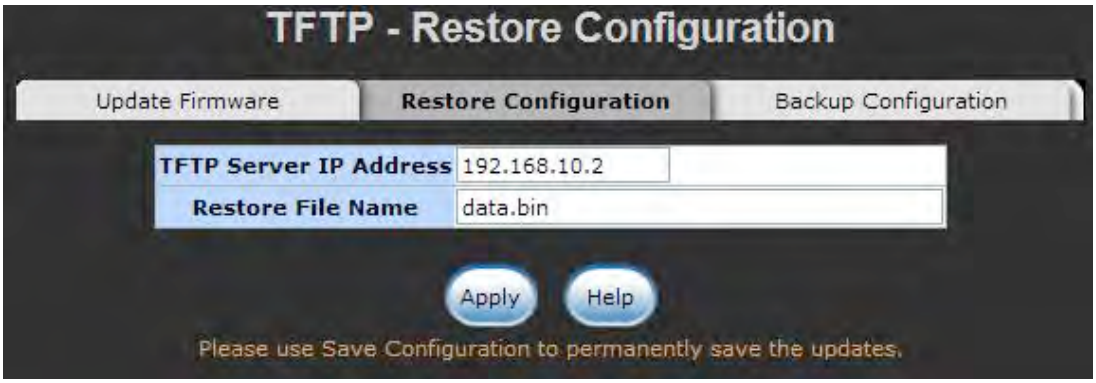


Update Firmware interface

6.7 TFTP – Restore Configuration

You can restore the configuration from TFTP server. Before doing that, you must put the image file on the TFTP server first and the switch will download back the flash image.

1. **TFTP Server IP Address:** Type in the TFTP server IP.
2. **Restore File Name:** Type in the correct file name for restoring.
3. Select Apply.

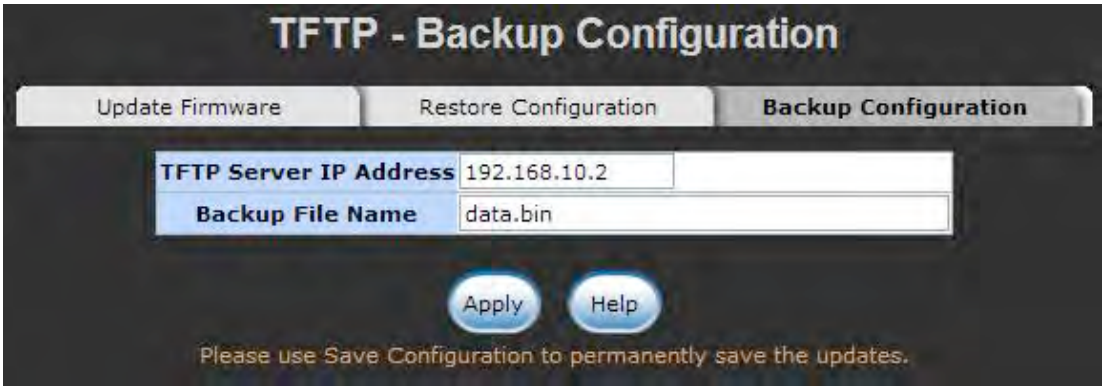


Restore Configuration interface

6.8 TFTP - Backup Configuration

You can save the current configuration from flash ROM to TFTP server for restoring later.

1. **TFTP Server IP Address:** Type in the TFTP server IP.
2. **Backup File Name:** Type in the file name.
3. Select Apply.



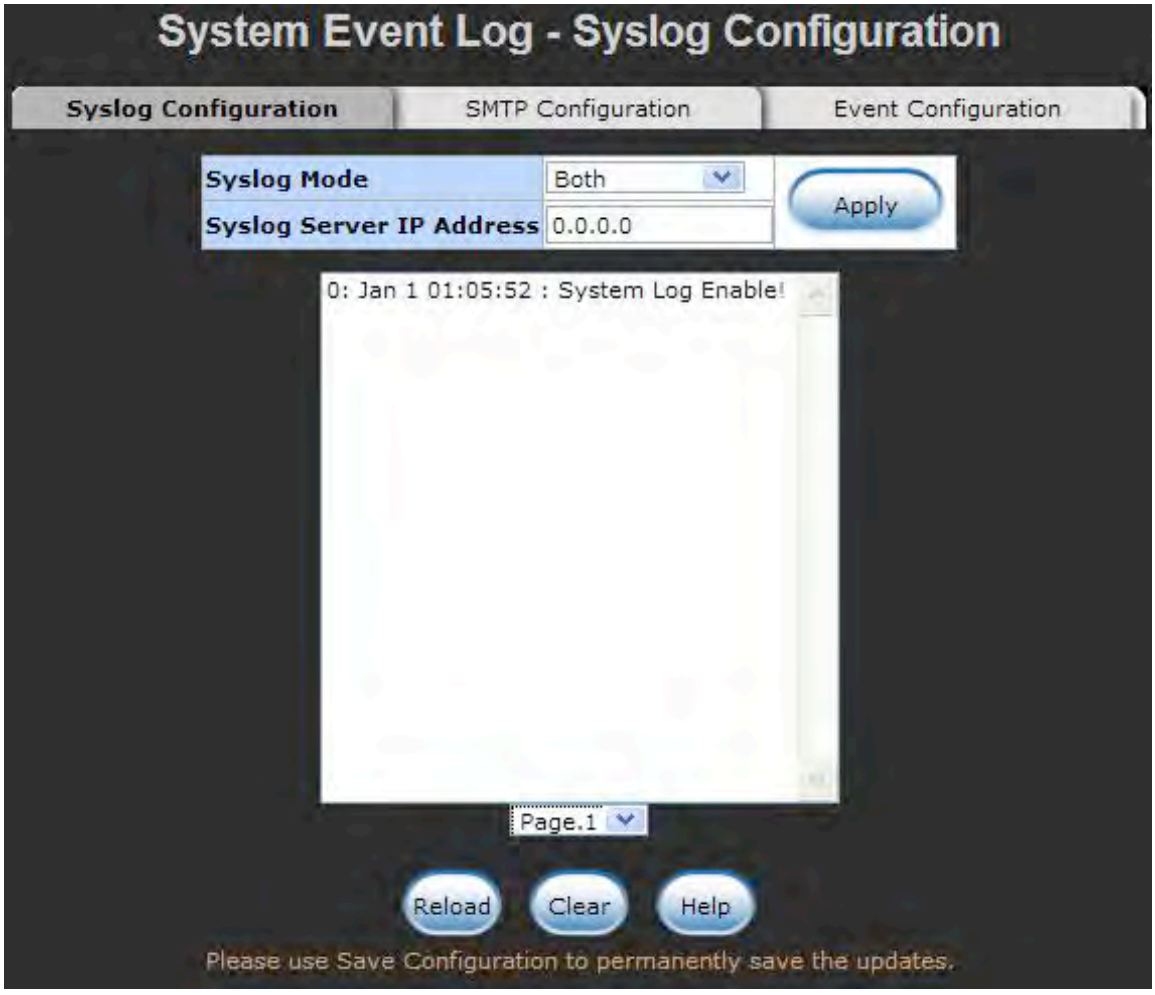
Backup Configuration interface

6.9 System Event Log – Syslog Configuration

Configure the system event mode to collect system log.

1. **Syslog Client Mode:** Select the system log mode—**Client Only**, **Server Only**, or **Both**.

2. **System Log Server IP Address:** Assign the system log server IP.
3. When Syslog Client Mode is set as **Client Only**, the system event log will only be reserved in the switch's RAM until next reboot. When Syslog Client Mode is set as **Server Only**, the system log will only be sent to the syslog server and you have to type the IP address of the Syslog Server in the "Syslog Server IP Address" column. If the Syslog Client Mode is set as **Both**, the system log will be reserved in the switch's RAM and sent to server.
4. Select Reload to refresh the events log.
5. Select Clear to clear all current events log.
5. After configuring, Select Apply.



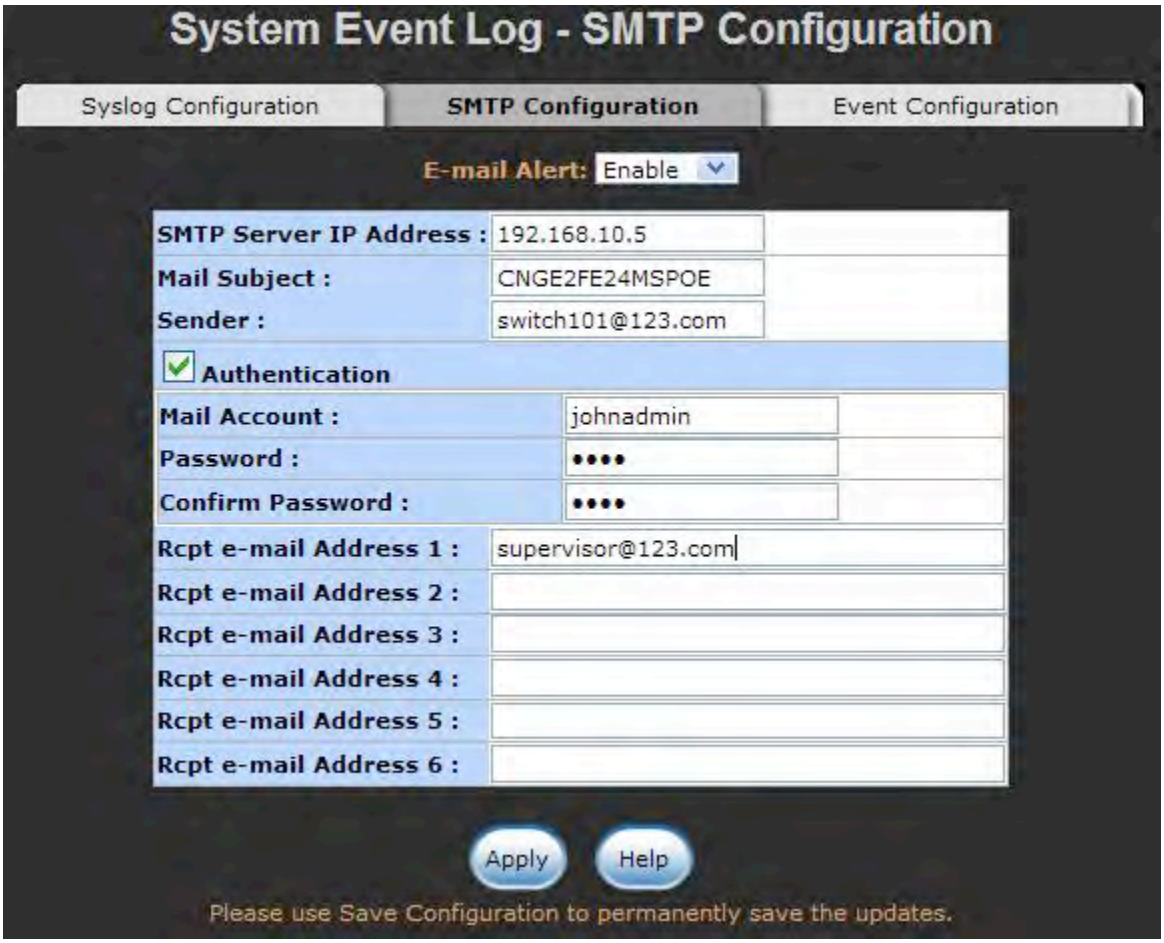
Syslog Configuration interface

6.10 System Event Log - SMTP Configuration

You can set up the mail server IP, mail account, password, and forwarded email account for receiving the event alert.

1. **Email Alert:** Enable or disable the email alert function.
2. **SMTP Server IP:** Set up the mail server IP address (when **Email Alert** is enabled, this function will become available).
3. **Sender:** Type in an alias of the switch in complete email address format, e.g. switch101@123.com, to identify where the event log comes from.
4. **Authentication:** Select the checkbox to enable this function, configuring the email account and password for authentication (when **Email Alert** is enabled, this function will become available).
5. **Mail Account:** Set up the email account, e.g. johnadmin, to receive the alert. It must be an existing email account on the mail server, which you had set up in **SMTP Server IP Address** column.
6. **Password:** Type in the password to the email account.
7. **Confirm Password:** Reconfirm the password.
8. **Rcpt e-mail Address 1 ~ 6:** You can also assign up to 6 e-mail accounts to receive the alert.
9. Select 

.



SMTP Configuration interface

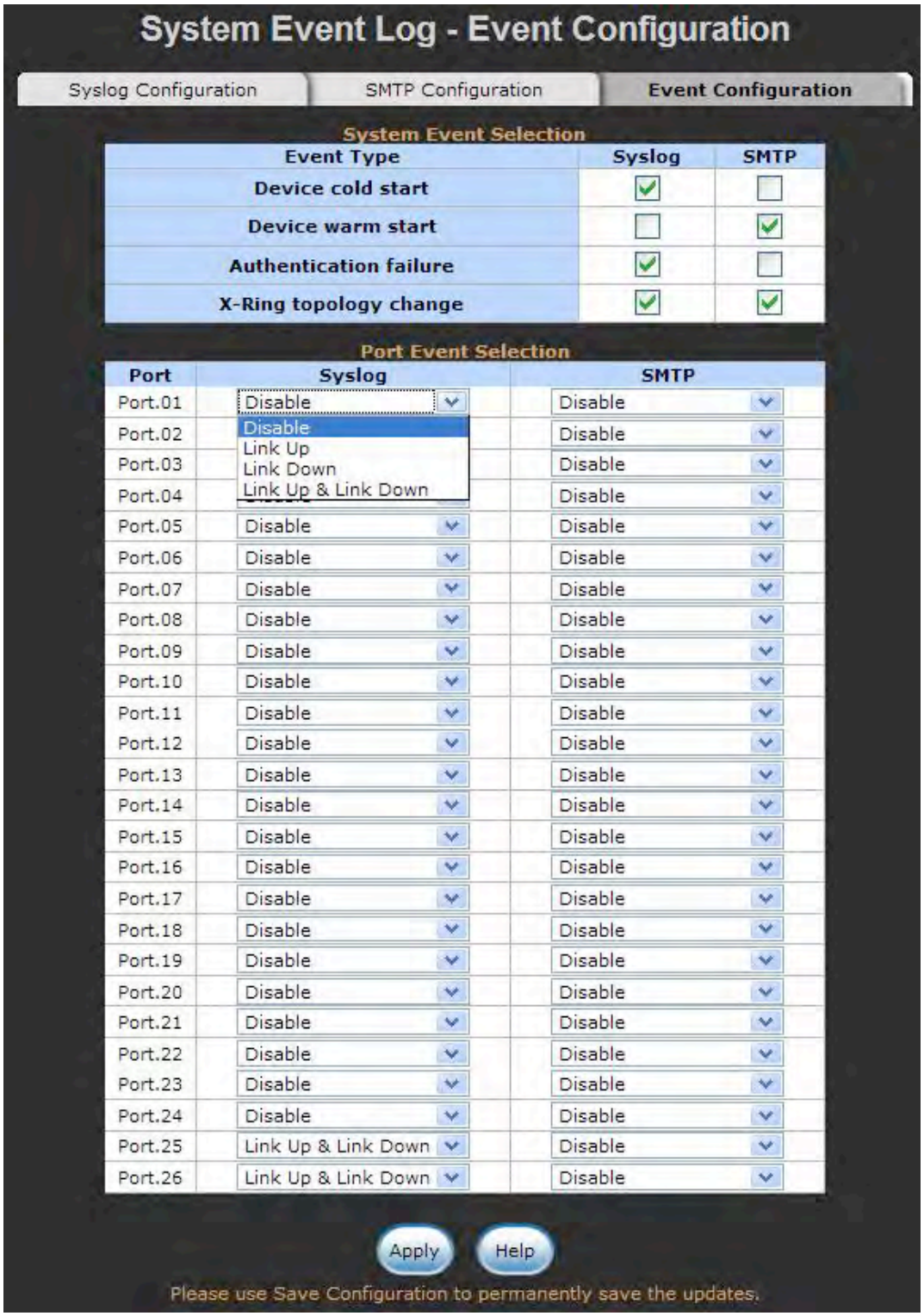
6.11 System Event Log - Event Configuration

The user must enable the Syslog or SMTP first to configure the condition setting in this page. When the **Syslog**/**SMTP** checkbox is marked, the event log will be sent to system log server/SMTP server. Also, per port log (link up, link down, and both) events can be sent to the system log server/SMTP server with the respective checkbox selected. After configuring, select  to have the setting taken effect.

- **System event selection:** There are 4 event types—device cold start, device warm start, authentication failure, and X-ring topology change. Before you can select the checkbox of each event type, the Syslog Client Mode column on the Syslog Configuration tab/E-mail Alert column on the SMTP Configuration tab must be enabled first.

- **Device cold start:** When the device disconnects the power supply and re-connects to it, the system will issue a log event.
- **Device warm start:** When the device reboots, the system will issue a log event.
- **Authentication Failure:** When the authentication fails, the system will issue a log event.
- **X-ring topology change:** When the X-ring topology has changed, the system will issue a log event.

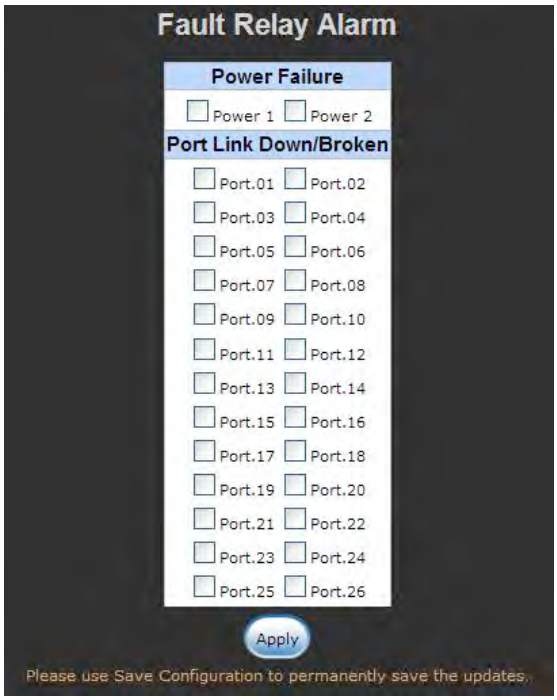
- **Port event selection:** Also, before the drop-down menu items are available, the Syslog Client Mode column on the Syslog Configuration tab and the E-mail Alert column on the SMTP Configuration tab must be enabled first. Those drop-down menu items have 3 selections—Link Up, Link Down, and Link Up & Link Down. Disable means no event will be sent to the system log server/SMTP server.
  - **Link Up:** The system will issue a log message when port connection is up only.
  - **Link Down:** The system will issue a log message when port connection is down only.
  - **Link Up & Link Down:** The system will issue a log message when port connection is up and down.



Event Configuration interface

6.12 Fault Relay Alarm

- **Power Failure:** Select the checkbox to enable the function of lighting up the **FAULT** LED on the panel when power fails.
- **Port Link Down/Broken:** Select the checkbox to enable the function of lighting up the **FAULT** LED on the panel when Ports' states are link down or broken.



Fault Relay Alarm interface

6.13 SNTP Configuration

You can configure the SNTP (Simple Network Time Protocol) settings. The SNTP allows you to synchronize switch clocks in the Internet.

1. **SNTP Client:** Enable/disable SNTP function to get the time from the SNTP server.
2. **Daylight Saving Time:** Enable/disable daylight saving time function. When daylight saving time is enabled, you need to configure the daylight saving time period.
3. **UTC Timezone:** Set the switch location time zone. The following table lists the different

location time zone for your reference.

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
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	+1 hour	1 pm

SWT - Swedish Winter		
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 Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

4. **SNTP Sever URL:** Set the SNTP server IP address.
5. **Switch Timer:** Displays the current time of the switch.
6. **Daylight Saving Period:** Set up the Daylight Saving beginning time and Daylight Saving ending time. Both will be different in every year.

7. **Daylight Saving Offset (mins):** For non-US and European countries, specify the time offset for Daylight Savings.
8. Select Apply.

SNTP Configuration interface

6.14 IP Security

IP security function allows the user to assign 10 specific IP addresses that have permission to access the switch through the web browser for the securing switch management.

- **IP Security Mode:** When this option is in the **Enable** mode, the **Enable HTTP Server** and **Enable Telnet Server** checkboxes will then be available.
- **Enable HTTP Server:** When this checkbox is selected, the IP addresses among Security IP1 ~ IP10 will be allowed to access this switch via HTTP service. *When IP Security is Enablde and this checkbox is not selected, no user will be allowed to login via HTTP.*
- **Enable Telnet Server:** When this checkbox is selected, the IP addresses among Security IP1 ~ IP10 will be allowed to access this switch via telnet service. *When IP Security is Enabled and this checkbox is not selected, no user will be allowed to login via Telnet.*

- **Security IP 1 ~ 10:** The system allows the user to assign up to 10 specific IP addresses for access security. Only these 10 IP addresses can access and manage the switch through the HTTP/Telnet service.
- And then, select Apply to have the configuration taken effect.

[NOTE] Remember to execute the “Save Configuration” action, otherwise the new configuration will lose when the switch powers off.

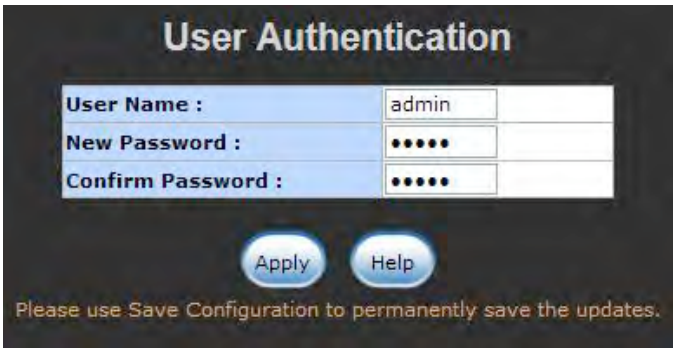
IP Security interface

6.15 User Authentication

Change web management login user name and password for the management security issue.

- **User name:** Type in the new user name (The default is ‘admin’)
- **Password:** Type in the new password (The default is ‘admin’)
- **Confirm password:** Re-type the new password

- And then, select 



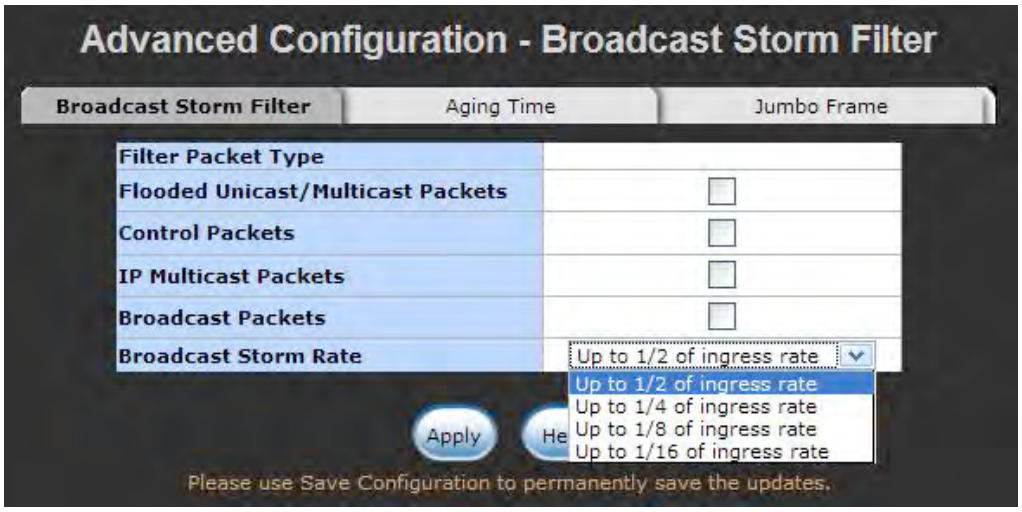
User Authentication interface

6.16 Advanced Configuration—Broadcast Storm Filter

This page enables the user to select the filter packet type. All the packet types filtering conditions could be selected at the same time.

- **Flooded Unicast/Multicast Packets:** When this check box is selected, the switch will filter the packet type of Flooded Unicast/Multicast.
- **Control Packets:** Select this check box to enable the switch to filter the control packet type.
- **IP Multicast Packets:** Select this check box to enable the switch to filter the IP Multicast packet type.
- **Broadcast Packets:** Select this check box to enable the switch to filter the broadcast packet type.
- **Broadcast Storm Rate:** User can set the filtering rate range from 1/2 of ingress to 1/16 of ingress.
- And then, select 

to have the configuration take effect.

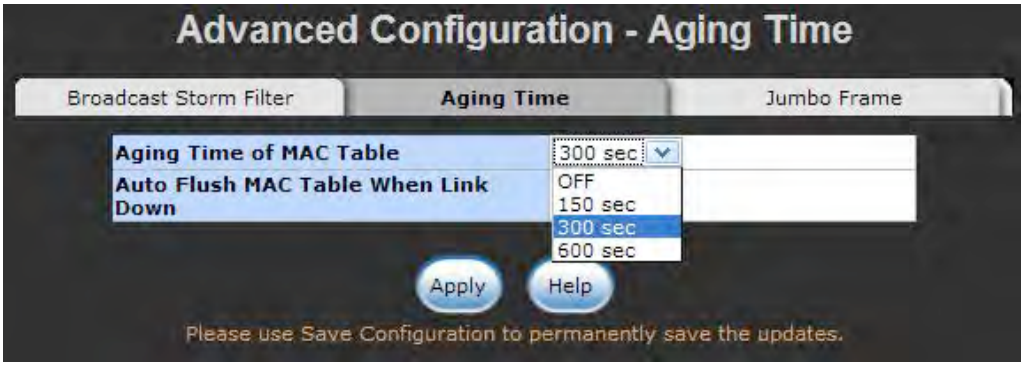


Broadcast Storm Filter interface

6.17 Advanced Configuration—Aging Time

This tab is used to assign the aging time of MAC table.

- **Aging Time of MAC Table:** Select the aging time as OFF, 150 sec, 300 sec, or 600 sec. When MAC table is not used within the aging time, the MAC address table will then be cleared.
- **Auto Flush MAC Table When Link Down:** When this item is enabled, the switch will flush its MAC address table when link down.
- And then, select  to have the configuration take effect.



Aging Time interface

6.18 Advanced Configuration—Jumbo Frame

This tab is used to enable the jumbo frame function.

- **Enable Jumbo Frame:** When this check box is selected, the Gigabit port of the switch extends the frame to 9022bytes.
- And then, select 

to have the configuration take effect.

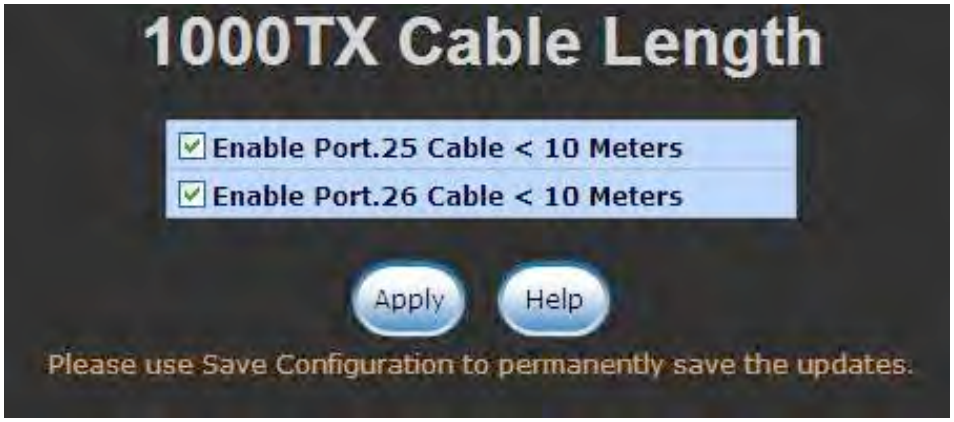
Jumbo Frame interface

6.19 1000TX Cable Length

This tab is used to allow port 25 and port 26 to support Cat5e or Cat6 cable length longer than 10 meters.

- **To support long cable:** Uncheck the check box for the port(s) you would like to effect.
- And then, click 

to have the configuration taken effect.



Jumbo Frame interface

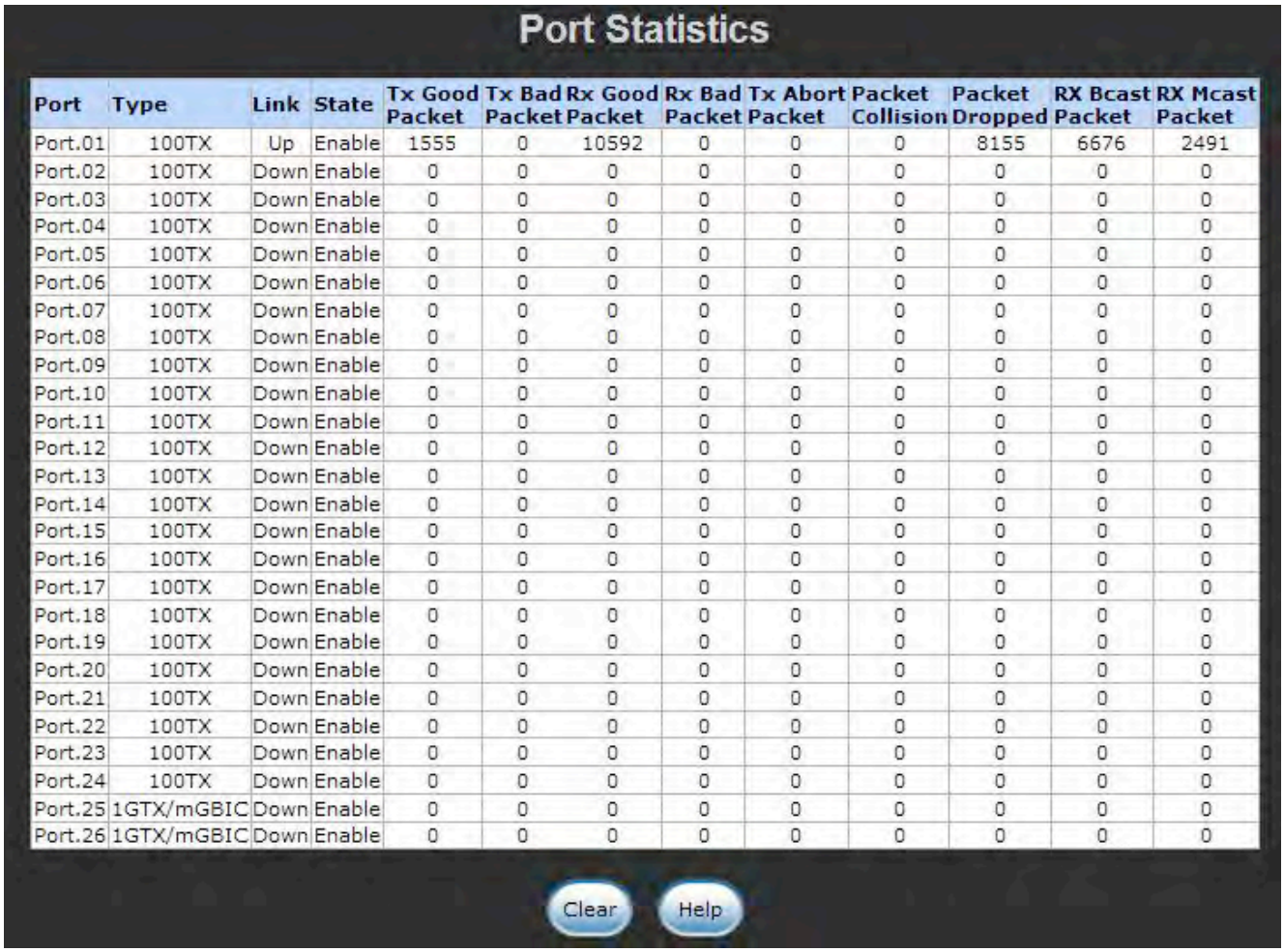
7 Port

7.1 Port Statistics

The following information provides the current port statistic information.

- **Port:** Displays the port number.
- **Type:** Displays the current speed of connection to the port.
- **Link:** The status of linking—'**Up**' or '**Down**'.
- **State:** The user can set the state of the port as 'Enable' or 'Disable' via Port Control. When the state is disabled, the port will not transmit or receive any packet.
- **Tx Good Packet:** The counts of transmitting good packets via this port.
- **Tx Bad Packet:** The counts of transmitting bad packets (including undersize [less than 64 bytes], oversize, CRC Align errors, fragments and jabbers packets) via this port.
- **Rx Good Packet:** The counts of receiving good packets via this port.
- **Rx Bad Packet:** The counts of receiving bad packets (including undersize [less than 64 bytes], oversize, CRC error, fragments and jabbers) via this port.
- **Tx Abort Packet:** The aborted packet while transmitting.
- **Packet Collision:** The counts of collision packet.
- **Packet Dropped:** The counts of dropped packet.
- **Rx Bcast Packet:** The counts of broadcast packet.
- **Rx Mcast Packet:** The counts of multicast packet.
- Select 

to clean all counts.



Port Statistics interface

7.2 Port Counters

This chart displays the transmitted and received traffic of a single port.

- **Select Port:** Pull down the menu bar to select a particular port, and then the counters for the port will be displayed.
- **RxBcastPkt:** The number of good broadcast packets received.
- **RxOctel:** The number of octets of data received (including those in bad packet, excluding framing bits but including FCS octets, excluding RxPausePkt).
- **RxMcastPkt:** The number of good multicast packets received except broadcast packets).

- **RxFCSErr:** The number of packets received that had a bad FCS or RX ER asserted with the proper and integral octets.
- **RxOverSizePkt:** The number of packets received that were longer than Max_Pkt_Len (=1522 bytes) and were otherwise well formed.
- **RxAlignErr:** The number of packets received that had a bad FCS or RX_ER asserted with the proper and non-integral octets.
- **RxJabber:** The number of packets received that were longer than Max_Pkt_Len (=1522 bytes) and had a bad FCS or RX_ER asserted.
- **RxFragment:** The number of packets received that were less than 64 octets long and had a bad FCS or RX_ER asserted.
- **RxUndersizePkt:** The number of packets received that were less than 64 octets long and were otherwise well formed.
- **RxPkt64:** The number of packets received that were 64 octets in length including bad packets but excluding RxPausePkt.
- **RxPkt65to127:** The number of packets received that were between 65 and 127 octets in length (including error packets).
- **RxPkt128to255:** The number of packets received that were between 128 and 255 octets in length (including error packets).
- **RxPkt256to511:** The number of packets received that were between 256 and 511 octets in length (including error packets).
- **RxPkt512to1023:** The number of packets received that were between 511 and 1023 octets in length (including error packets).
- **RxPkt1024to1522:** The number of packets received that were between 1024 and the Max_Pkt_Len (=1522 bytes) octets in length (including error packets).
- **TxUcastPkt:** The number of unicast packets transmitted.
- **TxBcastPkt:** The number of broadcast packets transmitted.
- **TxOctel:** The number of octets transmitted (only for good packets excluding TxPausePkt).
- **TxSingleCollisn:** The number of successfully transmitted packets where transmission is inhibited by exactly one collision.
- **TxMultiCollisn:** The number of successfully transmitted packets where transmission is

inhibited by more than one collision.

- **TxCollisn:** The number of collisions on this Ethernet segment.
- **TxDefferTrans:** The number of packets where the first transmission attempt is delayed because the medium is busy.
- **DropFwdLkup:** The number of unicast packets dropped after a forwarding table lookup.
- **DropIn:** The number of packets dropped because the input FIFO overrun and the FC violation.
- **TxMcst:** The number of multicast packets transmitted.
- **TxPause:** The number of Pause Packets transmitted.
- **RxPause:** The number of Pause Packets received.
- **TxUnderrun:** The number of packets dropped because the output FIFO underrun.
- Select Clear to reset the figures.

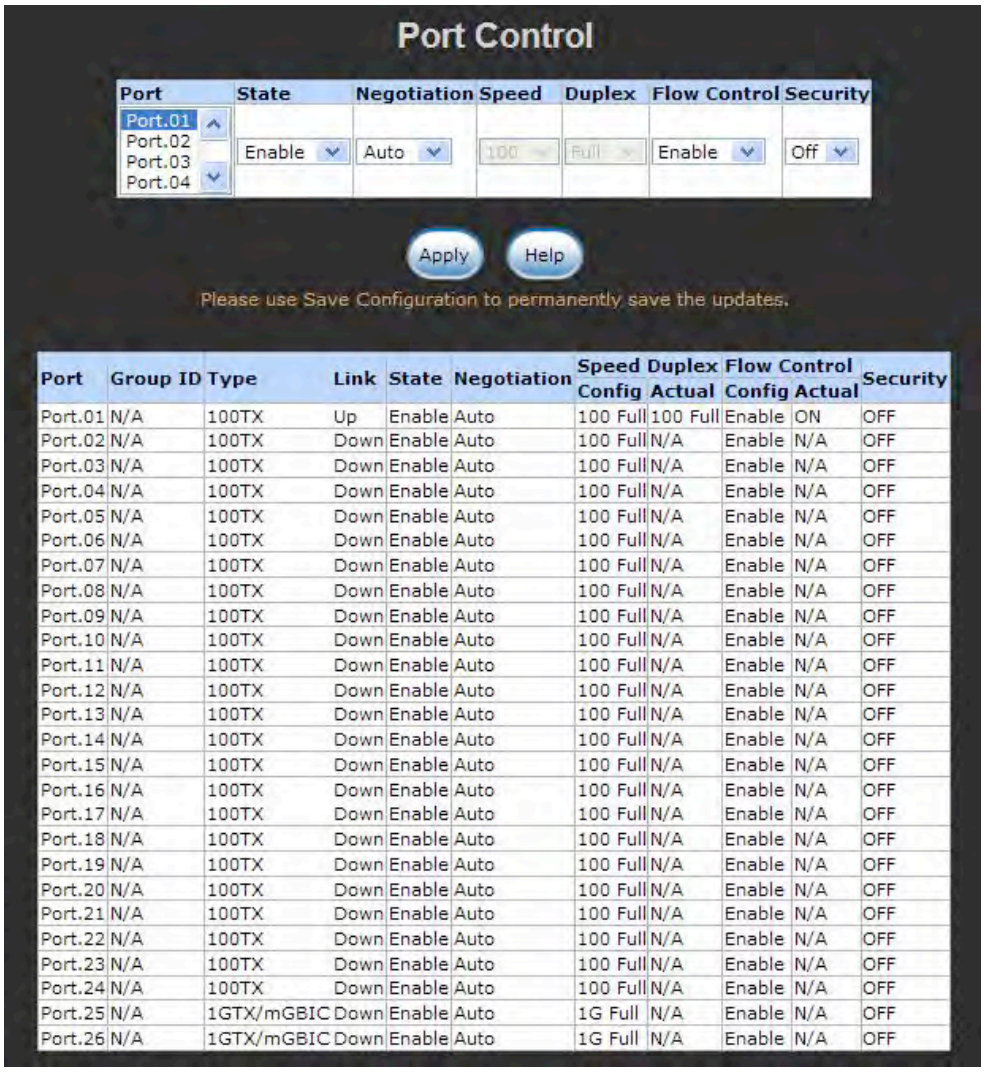
7.3 Port Control

In Port control, you can view and set the operation mode of each port.

1. **Port:** Select the port that you want to configure.

2. **State:** Current port status. The port can be set to disable or enable mode. *If the port state is set as 'Disable', it will not receive or transmit any packet.*
3. **Negotiation:** Auto and Force. Being set as Auto, the speed and duplex mode are negotiated automatically. When you set it as Force, you have to assign the speed and duplex mode manually.
4. **Speed:** Is available for selection when the Negotiation column is set as Force. When the Negotiation column is set as Auto, this column is read-only.
5. **Duplex:** Is available for selection when the Negotiation column is set as Force. When the Negotiation column is set as Auto, this column is read-only.
6. **Flow Control:** Set flow control function as Enable or Disable. When enabled, once the device has exceeded the input data rate of another device, the receiving device will send a PAUSE frame which halts the transmission of the sender for a specified period of time. When disabled, the receiving device will drop the packet if it is too much to process.
7. **Security:** Once the Security selection is set as '**On**', any access from the device that connects to this port will be blocked unless the MAC address of the device is included in the static MAC address table. See the segment of **MAC Address Table - Static MAC Addresses**.
8. Select 

to make the configuration taken effect.



Port	Group ID	Type	Link	State	Negotiation	Speed Duplex Config	Speed Duplex Actual	Flow Control Config	Flow Control Actual	Security
Port.01	N/A	100TX	Up	Enable	Auto	100 Full	100 Full	Enable	ON	OFF
Port.02	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.03	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.04	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.05	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.06	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.07	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.08	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.09	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.10	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.11	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.12	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.13	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.14	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.15	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.16	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.17	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.18	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.19	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.20	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.21	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.22	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.23	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.24	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.25	N/A	1GTX/mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.26	N/A	1GTX/mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF

Port Control interface

7.4 Port Trunk

Port trunking is combining several ports or network cables to expand the connection speed beyond the limits of any one single port or network cable. Link Aggregation Control Protocol (LACP), a protocol running on layer 2, provides a standardized means, in accordance with IEEE 802.3ad, to bundle several physical ports together to form a single logical channel. All the ports within the logical channel or logical aggregator work at the same connection speed and LACP operation requires full-duplex mode.

7.4.1 Aggregator setting

- **System Priority:** A value that is used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP peer of the trunk group.
- **Group ID:** There are 13 trunk groups to be selected. Assign the "**Group ID**" to the trunk group.
- **LACP:** When enabled, the trunk group is using LACP. A port that joins an LACP trunk group has to make an agreement with its member ports first. Please notice that a trunk group, including member ports split between two switches, has to enable the LACP function of the two switches. When disabled, the trunk group is a static trunk group. The advantage of having the LACP disabled is that a port joins the trunk group without any handshaking with its member ports; but member ports won't know that they should be aggregated together to form a logic trunk group.
- **Work ports:** This column field allows the user to type in the total number of active port up to four. With **LACP static trunk group**, e.g. you assign four ports to be the members of a trunk group whose work ports column field is set as two; the exceed ports are standby/redundant ports and can be aggregated if working ports fail. If it is a **static trunk group** (non-LACP), the number of work ports must equal the total number of group member ports.
- Select the ports to join the trunk group. The system allows a maximum of four ports to be aggregated in a trunk group. Select 

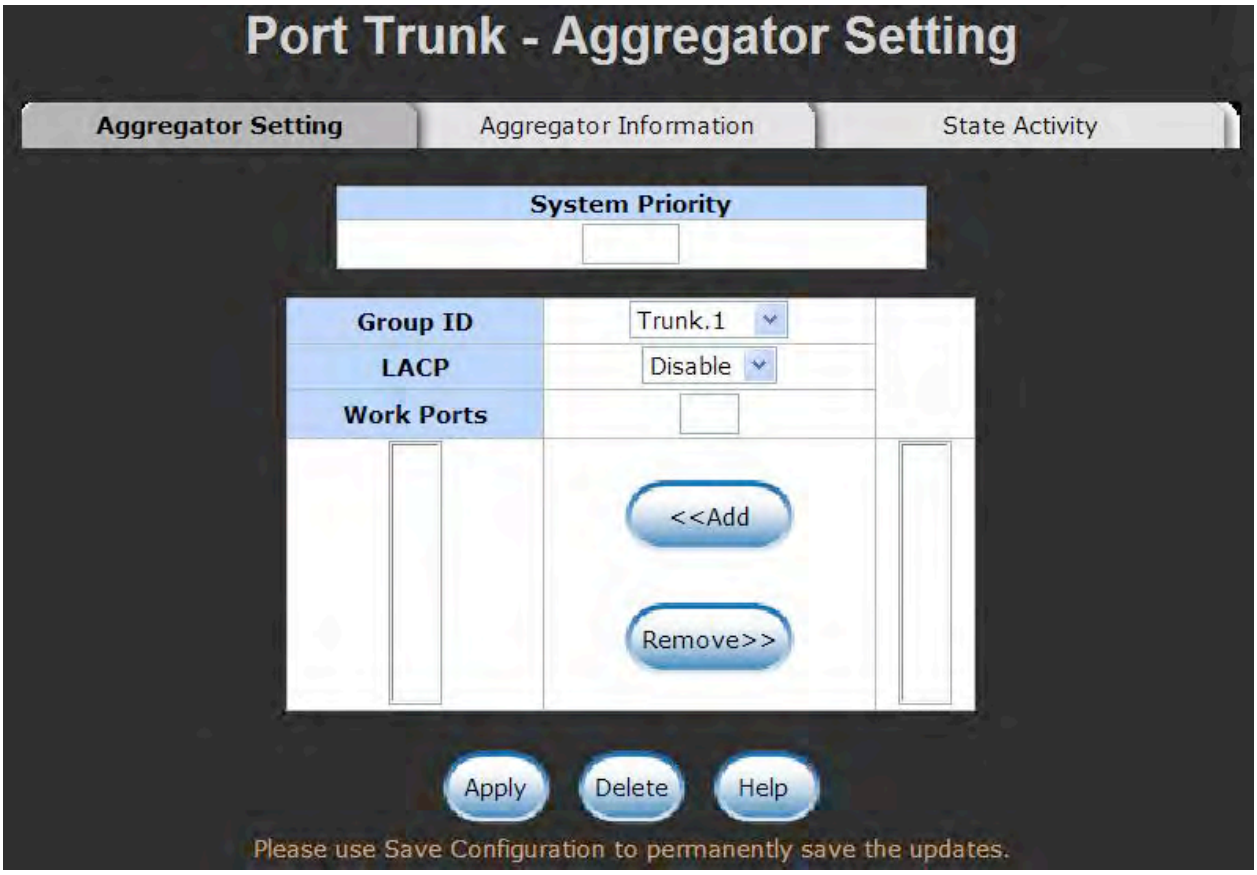
and the ports focused in the right side will be shifted to the left side. To remove unwanted ports, select the ports and select 

.
- When LACP enabled, you can configure LACP Active/Passive status for each port on the **State Activity** tab.
- Select 

.
- Use 

to delete the Trunk Group. Select the Group ID and select 

.

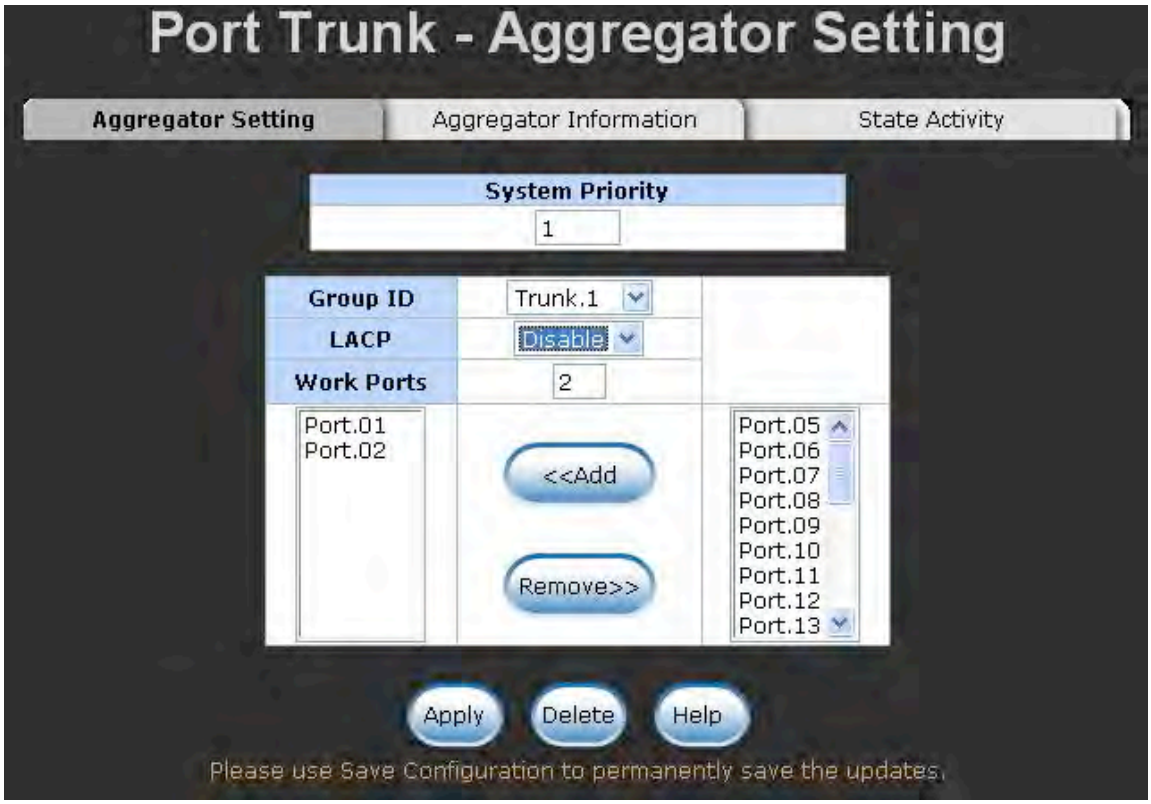


Port Trunk—Aggregator Setting interface (four ports are added to the left field with LACP enabled)

7.4.2 Aggregator Information

When you have setup the aggregator setting with LACP disabled, you will see the local static trunk group information in here.

1. **Group Key:** Displays the trunk group ID.
2. **Port Member:** Displays the members of this static trunk group.



Port Trunk—Aggregator Setting interface (two ports are added to the left field with LACP disable)

Port Trunk – Aggregator Information interface

7.4.3 State Activity

Having set up the LACP aggregator on the tab of Aggregator Setting, you can configure the state activity for the members of the LACP trunk group. You can select or cancel the checkbox beside the state display. When you remove the select mark to the port and select 

, the port state activity will change to **Passive**.

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

[NOTE]
1. **A link** having either two active LACP nodes or one active node can perform dynamic LACP trunk.
2. **A link** having two passive LACP nodes will not perform dynamic LACP trunk because both ports are waiting for an LACP protocol packet from the opposite device.

Port Trunk – State Activity interface

7.5 Port Mirroring

The Port mirroring is a method for monitoring traffic in switched networks. Traffic through

ports can be monitored by one specific port, which means traffic going in or out of the **Monitored** (source) port will be duplicated into the **Analysis** (destination) port.

Port Trunk – Port Mirroring interface

- **Mode:** Choose the type of monitored packets. **RX** means only the received packets of the monitored port will be copied and sent to the analysis port. **TX** means only the transmitted packets of the monitored port will be copied and sent to the analysis port. **Both RX/TX** means both received & transmitted packets of the monitored port will be copied and sent to the analysis port.
- **Analysis Port:** Only one port can be selected to be the analysis (destination) port for monitoring both RX and TX traffic which come from the source port. Users can connect the analysis port to LAN analyzer or Netxray.
- **Monitored Port:** Choose a port number to be monitored. Only one port can be monitored during the monitoring process.
- And then, select 

.

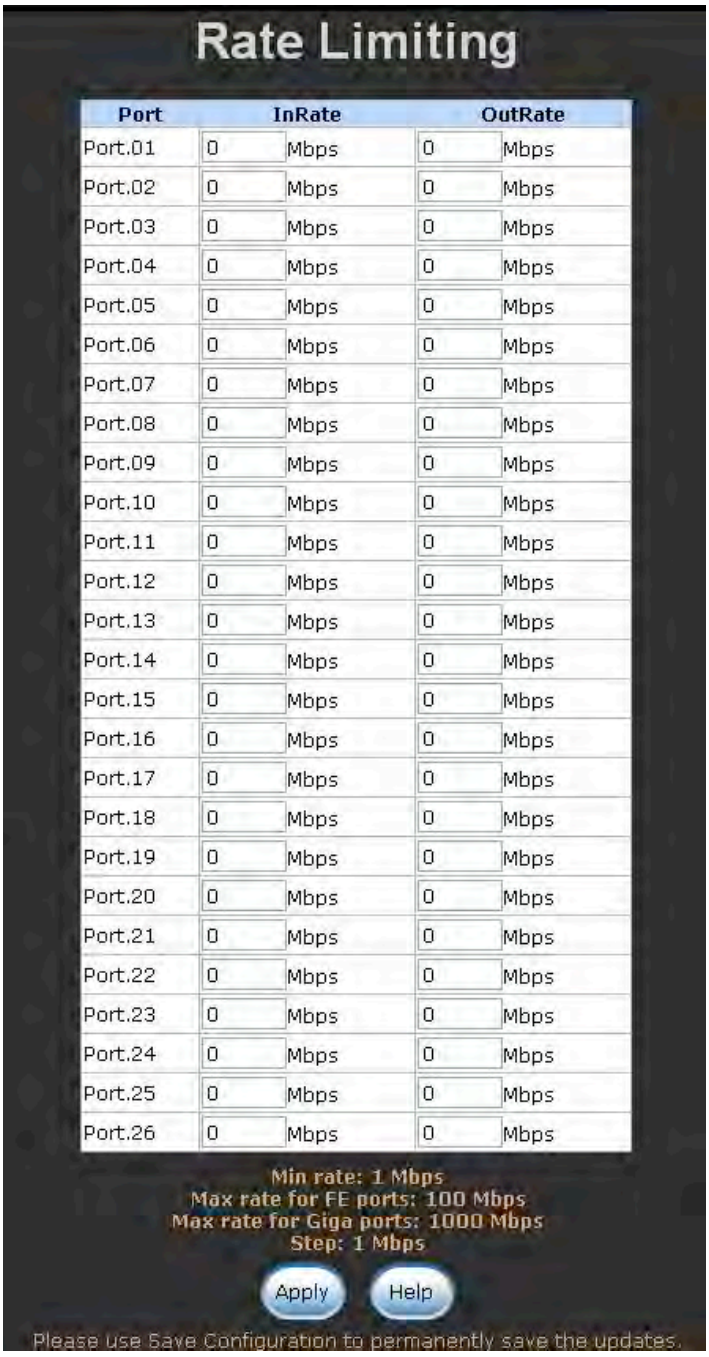
7.6 Rate Limiting

All the ports support packet ingress and egress rate control. For example, assume the wire speed of port 1 is 100Mbps; users can set its effective egress rate as 2Mbps, ingress rate as 1Mbps. The switch performs the ingress rate by packet counter to meet the specified rate.

- **Inrate:** Enter the port effective ingress rate (The default value is “0”).

- **OutRate:** Enter the port effective egress rate (The default value is “0”).

The rate range for port 1 to 24 is from 1 to 100 Mbps and the rate range for port 25, 26 is from 1 to 1000 Mbps. The zero means disabled.



Rate Limiting interface

7.7 VLAN configuration

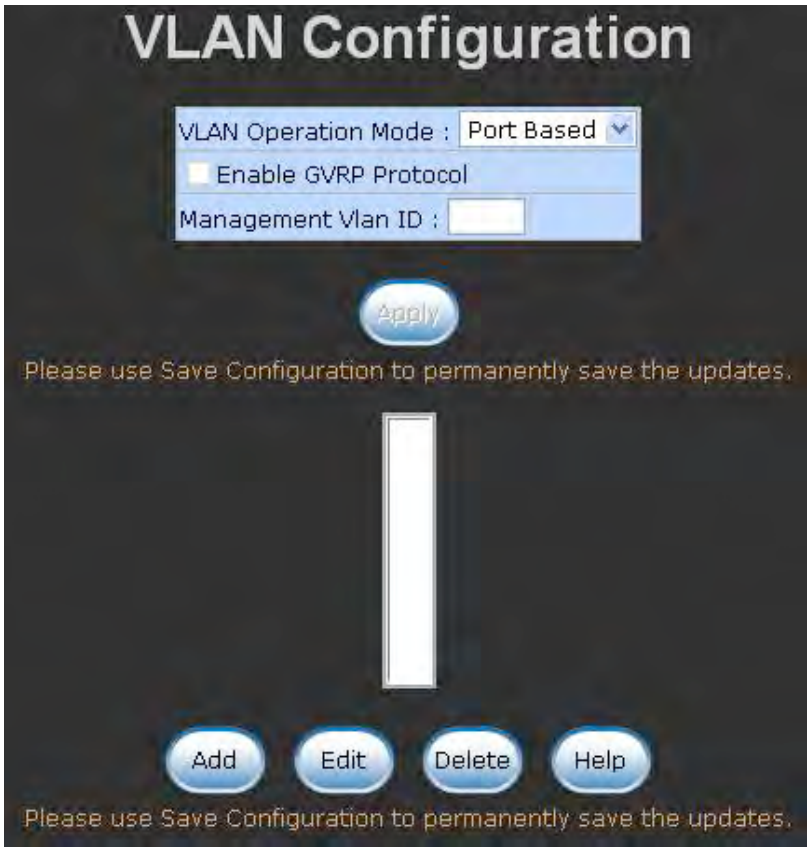
A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which would allow you to isolate network traffic, so only the members of the same VLAN will receive traffic from the ones of the same VLAN. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically.

The switch supports **Port-based** and **802.1Q** (tagged-based) VLAN. The default configuration of VLAN operation mode is **802.1Q**.

7.7.1 VLAN configuration - Port-based VLAN

Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN is enabled, the VLAN-tagging is ignored.

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

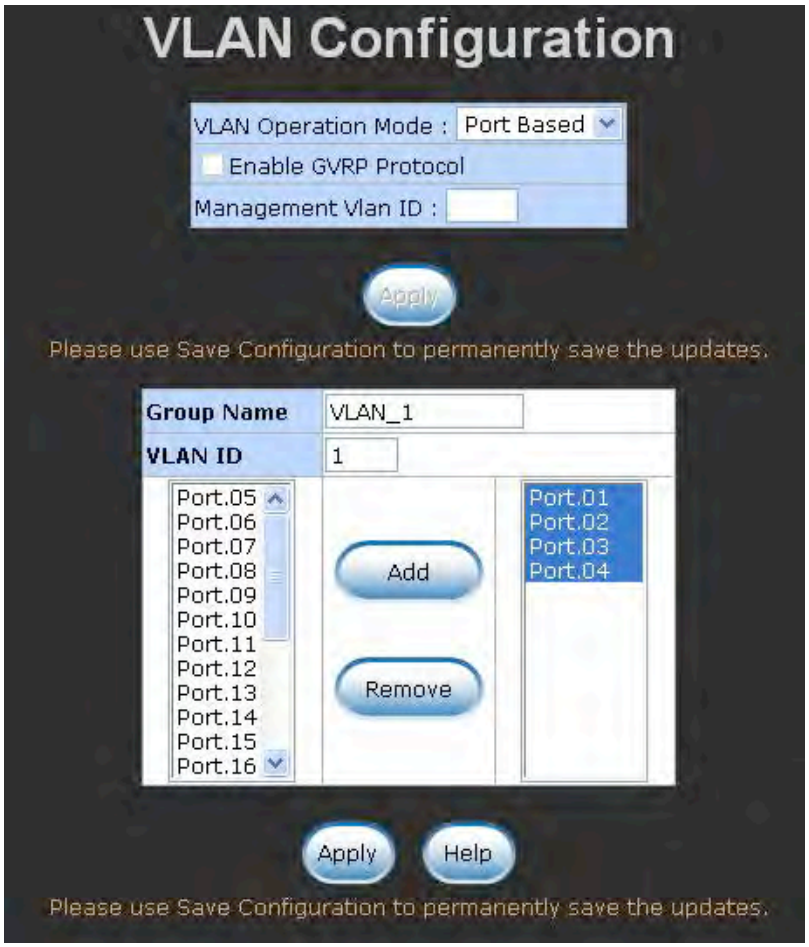


VLAN – Port Based interface

- Pull down the selection item and focus on **Port Based** then select 

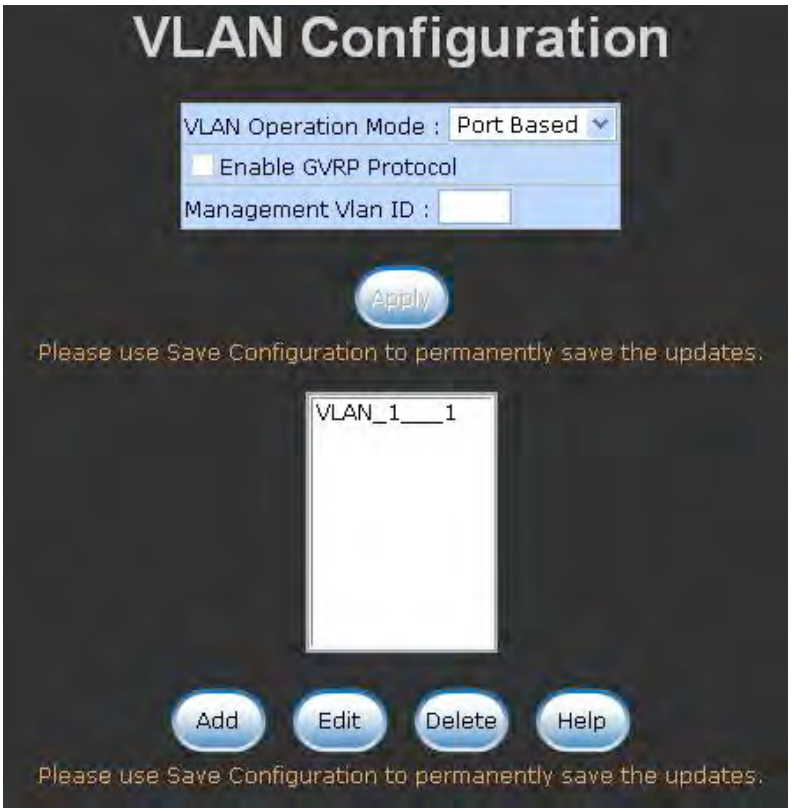
to set the VLAN Operation Mode in **Port Based** mode.
- Select 

to add a new VLAN group.



VLAN—Port Based Add interface

- Enter the group name and VLAN ID. Add the port number having selected into the right field to group these members to be a VLAN group or remove any of them listed in the right field from the VLAN.
- And then, select  to have the settings taken effect.
- You will see the VLAN displays.



VLAN—Port Based Edit/Delete interface

- Use  to delete the VLAN.
- Use  to modify group name, VLAN ID, or add/remove the members of the existing VLAN group.

[NOTE] Remember to execute the “Save Configuration” action, otherwise the new configuration will be lost when the switch powers off.

7.7.2 802.1Q VLAN

Virtual Local Area Network (VLAN) can be implemented on the switch to logically create different broadcast domains.

When the 802.1Q VLAN function is enabled, all ports on the switch belong to default VLAN of VID 1, which means they logically are regarded as members of the same broadcast domain. The valid VLAN ID is in the range of number between 1 and 4094. The amount of VLAN groups is up to 256 including default VLAN that cannot be deleted.

Each member port of 802.1Q is on either an Access Link (no VLAN-tagged) or a Trunk Link (VLAN-tagged). All frames on an Access Link carry no VLAN identification. Conversely, all frames on a Trunk Link are VLAN-tagged. Besides, there is the third mode—Hybrid. A Hybrid Link can carry both VLAN-tagged frames and untagged frames. A single port is supposed to belong to one VLAN group, except if it is on a Trunk/Hybrid Link.

The technique of 802.1Q tagging inserts a 4-byte tag, including VLAN ID of the destination port—PVID, in the frame. With the combination of Access/Trunk/Hybrid Links, the communication across switches also can make the packet be sent through tagged and untagged ports.

7.7.2.1 802.1Q Configuration

- Pull down the selection item and focus on **802.1Q** then select 

to set the VLAN Operation Mode in **802.1Q** mode.
- **Enable GVRP Protocol:** GVRP (GARP VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration information with other devices. For example, having enabled GVRP on two switches, they are able to automatically exchange the information of their VLAN database. Therefore, the user does not need to manually configure whether the link is trunk or hybrid, the packets belonging to the same VLAN can communicate across switches. Select this checkbox to enable GVRP protocol. This checkbox is available while the VLAN Operation Mode is in **802.1Q** mode.
- **Management VLAN ID:** Only when the VLAN members, whose Untagged VID (PVID) equals to the value in this column, will have the permission to access the switch. The default value is '0' that means this limit is not enabled (all members in different VLANs can access this switch).
- Select the port you want to configure.
- **Link Type**: There are 3 types of link type.
  - **Access Link:** A segment that provides the link path for one or more stations to the VLAN-aware device. An Access Port (untagged port), connected to the access link, has an untagged VID (also called PVID). After an untagged frame gets into the access port, the switch will insert a four-byte tag in the frame. The contents of the last 12-bit of the tag is untagged VID. When this frame is sent out through any of the access ports of the same PVID, the switch will remove the tag from the frame to recover it to what it was. Those ports of the same untagged VID are regarded as the same VLAN group members.

Note: Because the access port does not have an understanding of tagged frame, the column field of Tagged VID is not available.

- **Trunk Link:** A segment which provides the link path for one or more VLAN-aware devices (switches). A Trunk Port, connected to the trunk link, has an understanding of tagged frame, which is used for the communication among VLANs across multiple switches. Which frames of the specified VIDs will be forwarded depends on the values filled in the Tagged VID column field. Please insert a comma between two VIDs.

Note:

1. *A trunk port does not insert tag into an untagged frame, and therefore the untagged VID column field is not available.*
2. *It is not necessary to type '1' in the tagged VID. The trunk port will forward the frames of VLAN 1.*
3. *The trunk port has to be connected to a trunk/hybrid port of the other switch. Both the tagged VID of the two ports have to be the same.*

- **Hybrid Link:** A segment which consists of Access and Trunk links. The hybrid port has both the features of access and trunk ports. A hybrid port has a PVID belonging to a particular VLAN, and it also forwards the specified tagged-frames for the purpose of VLAN communication across switches.

Note:

1. *It's not necessary to type '1' in the tagged VID. The hybrid port will forward the frames of VLAN 1.*
2. *The trunk port has to be connected to a trunk/hybrid port of the other switch. Both the tagged VID of the two ports have to be the same.*

- **Untagged VID:** This column field is available when Link Type is set as Access Link and Hybrid Link. Assign a number in the range between 1 an 4094.
- **Tagged VID:** This column field is available when Link Type is set as Trunk Link and Hybrid Link. Assign a number in the range between 1 an 4094.
- Select 

to have the configuration take effect.
- You can see the link type, untagged VID, and tagged VID information of each port in the table below on the screen.

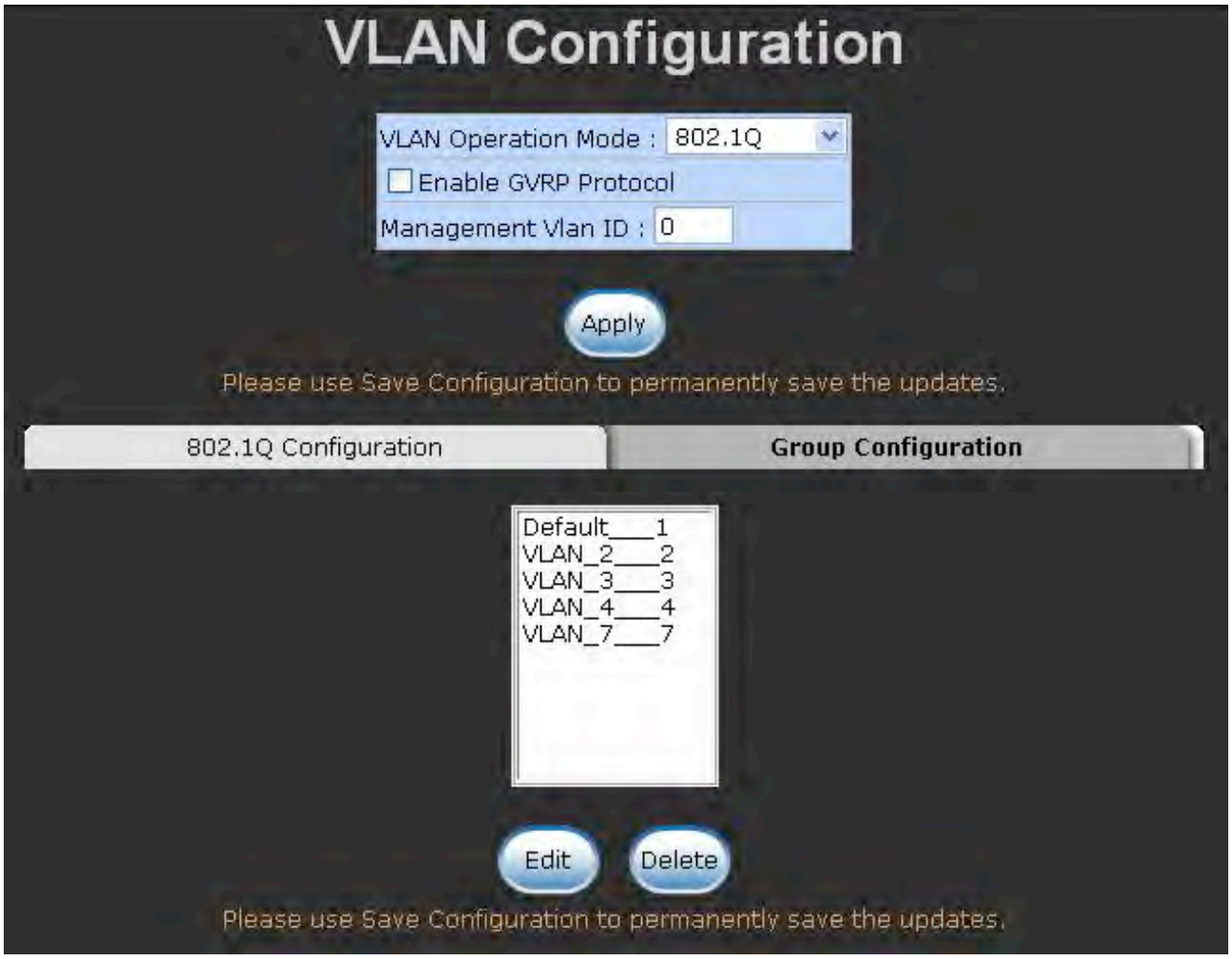
802.1Q VLAN interface

7.7.2.2 Group Configuration

Edit the existing VLAN Group.

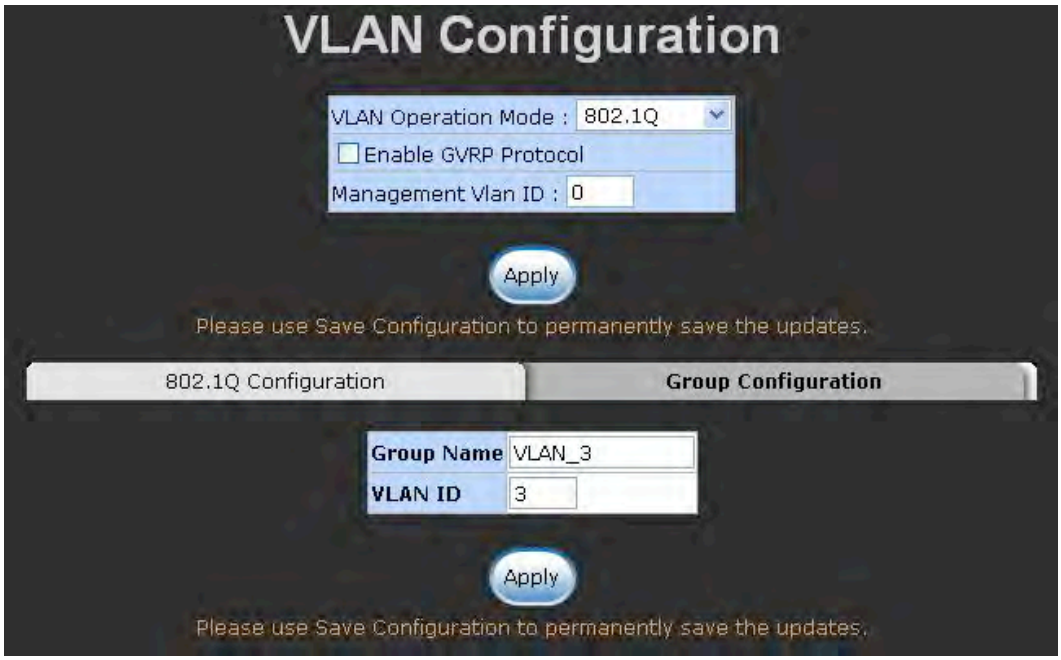
- Select the VLAN group in the table list.
- Select 

.



Group Configuration interface

- You can modify the VLAN group name and VLAN ID.



Group Configuration interface

- Select Apply.

7.8 Rapid Spanning Tree

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol and provides for faster spanning tree convergence after a topology change. The system also supports STP and the system will auto-detect the connected device that is running STP or RSTP protocol.

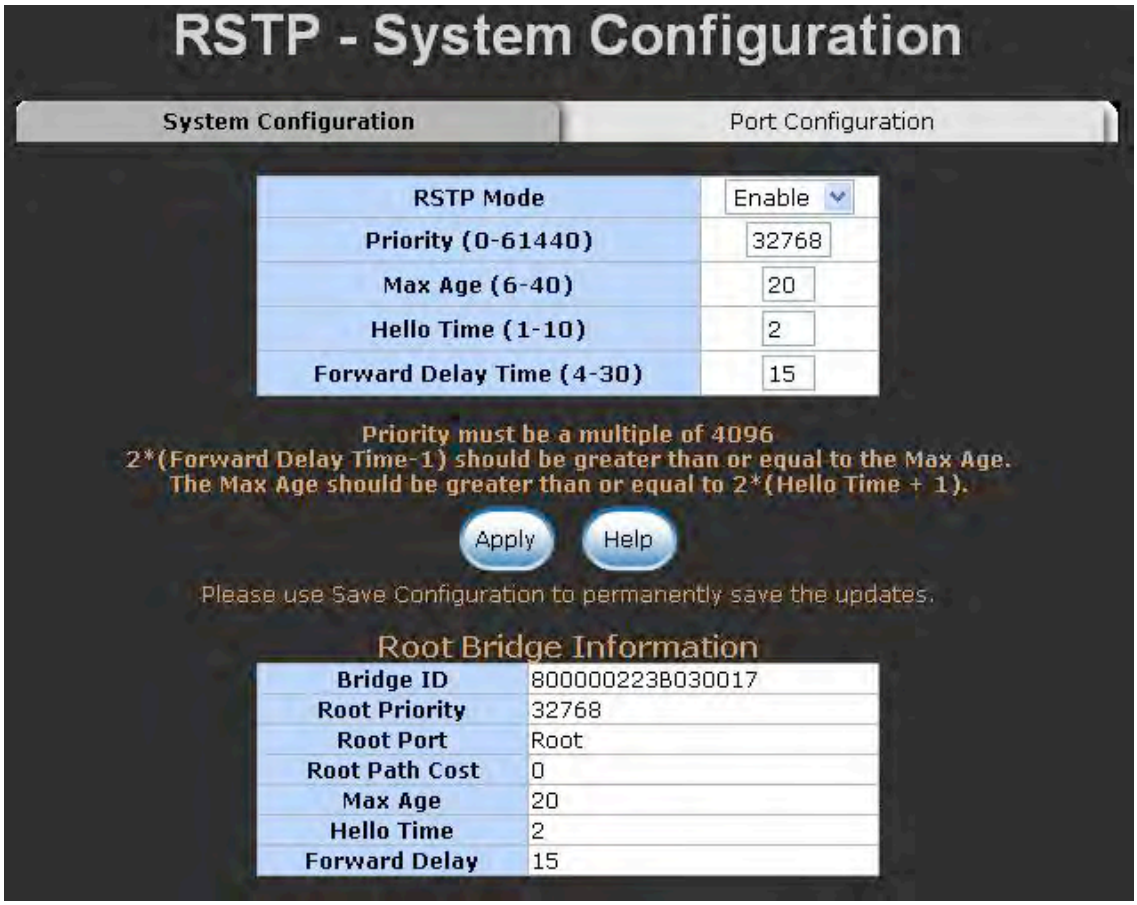
7.8.1 RSTP - System Configuration

- The user can view spanning tree information of Root Bridge.
- The user can modify RSTP state. After modification, select Apply.
  - **RSTP mode:** The user must enable the RSTP function first before configuring the related parameters.
  - **Priority (0-61440):** The switch with the lowest value has the highest priority and is

selected as the root. If the value is changed, the user must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule.

- **Max Age (6-40):** The number of seconds a switch waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40.
- **Hello Time (1-10):** The time that controls the switch to send out the BPDU packet 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 Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30.

[NOTE]	Follow the rule as below 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)**



RSTP System Configuration interface

7.8.2 RSTP—Port Configuration

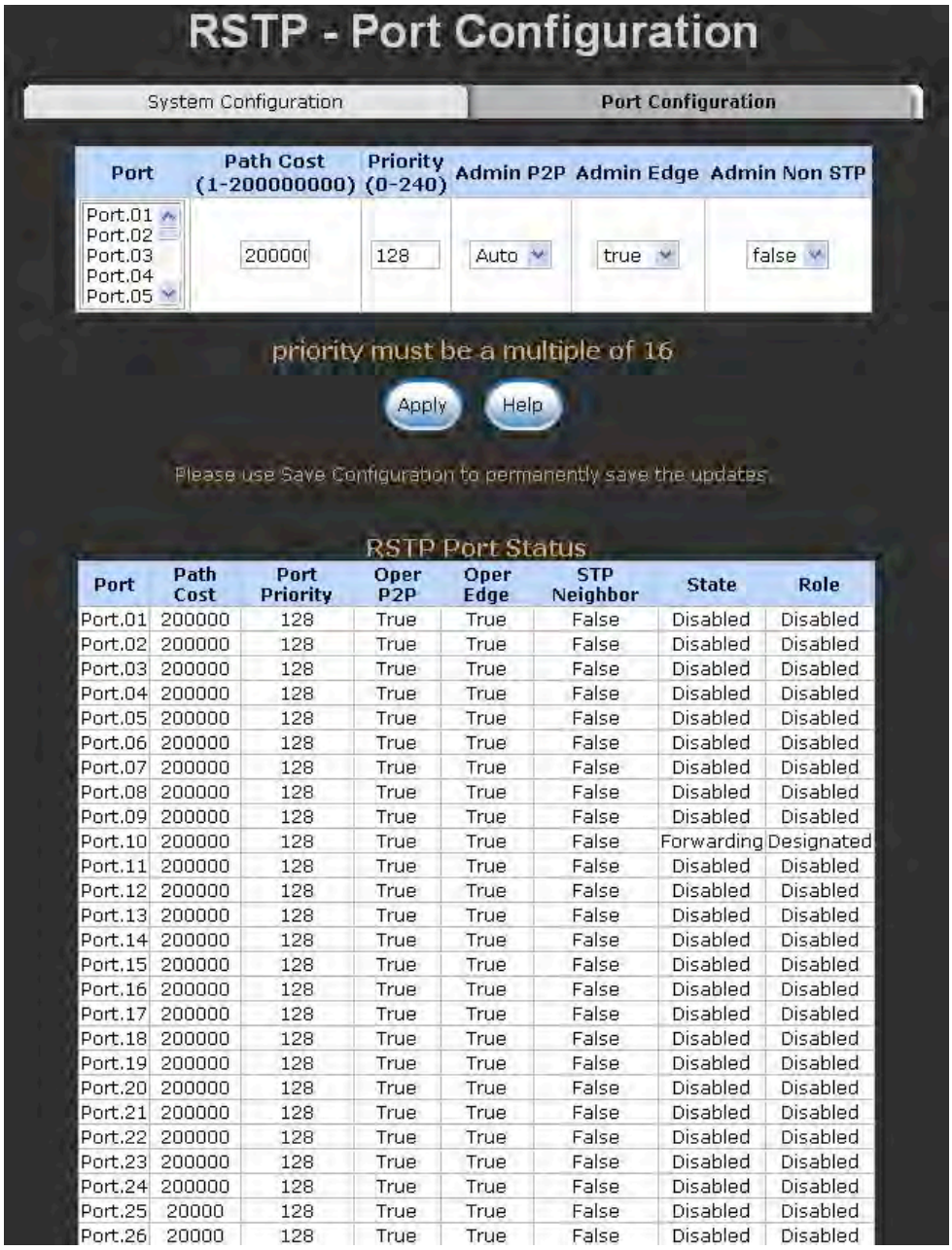
You can configure path cost and priority of every port.

- Select the port in the port column field.
- **Path Cost:** The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200,000,000.
- **Priority:** Decide which port should be blocked by priority in LAN. Enter a number 0 through 240 (the port of the highest value will be blocked). The value of priority must be the multiple of 16.
- **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 is P2P

enabling. False is P2P disabling.

- **Admin Edge:** The port directly connected to end stations won't create bridging loop in the network. To configure the port as an edge port, set the port to "**True**" status.
- **Admin Non Stp:** The port includes the STP mathematic calculation. **True** is not including STP mathematic calculation. **False** is including the STP mathematic calculation.
- Select 

.



RSTP Port Configuration interface

7.9 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 systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

7.9.1 System Configuration

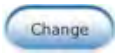
- **Community Strings**

Here you can define the new community string set and remove the unwanted community string.

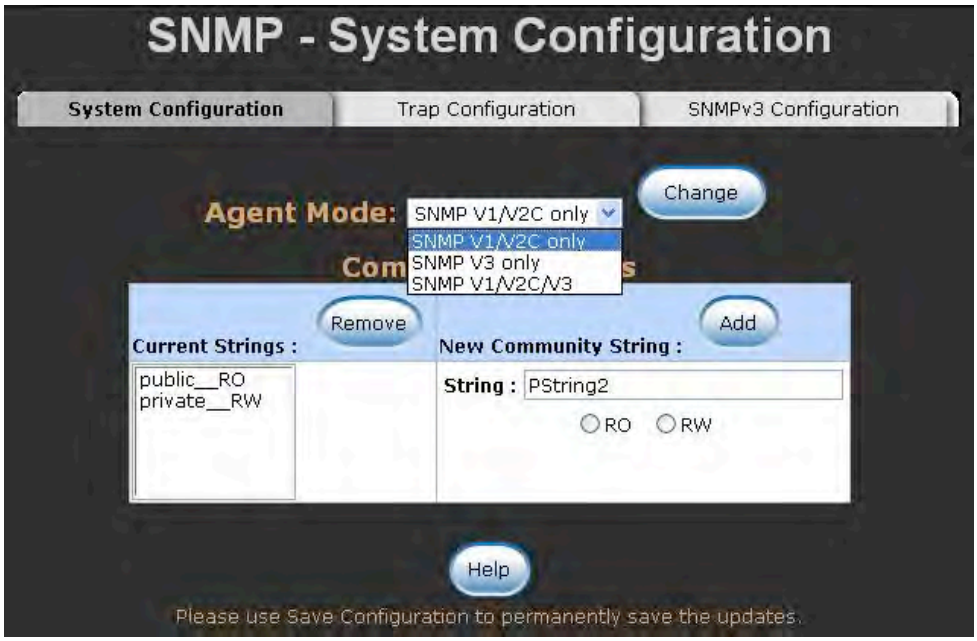
- **String:** Fill the name string.
- **RO:** Read only. Enables requests accompanied by this community string to display MIB-object information.
- **RW:** Read write. Enables requests accompanied by this community string to display MIB-object information and to set MIB objects.
- Select 

.
- To remove the community string, select the community string that you have defined and select 

. You cannot edit the name of the default community string set.

- **Agent Mode:** Select the SNMP version that you want to use and then select 

to switch to the selected SNMP version mode. The default value is 'SNMP v1/v2c only'

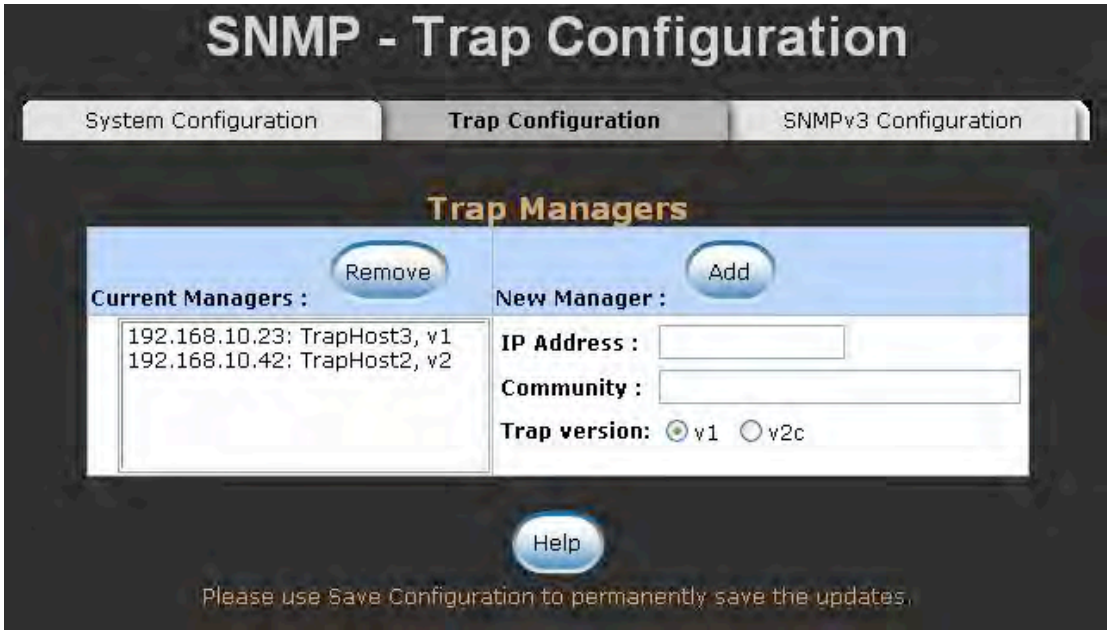


SNMP System Configuration interface

7.9.2 Trap Configuration

A trap manager is a management station that receives the trap messages generated by the switch. If no trap manager is defined, no traps will be issued. Create a trap manager by entering the IP address of the station and a community string. To define a management station as a trap manager, assign an IP address, enter the SNMP community strings, and select the SNMP trap version.

- **IP Address:** Enter the IP address of the trap manager.
- **Community:** Enter the community string.
- **Trap Version:** Select the SNMP trap version type—v1 or v2c.
- Select Add.
- To remove the community string, select the community string listed in the current managers field and select Remove.



Trap Managers interface

7.9.3 SNMPV3 Configuration

Configure the SNMP V3 function.

7.9.3.1.1 Context Table

Configure SNMP v3 context table. Assign the context name of context table. Select 

to add context name. Select 

to remove the unwanted context name.

7.9.3.1.2 User Profile

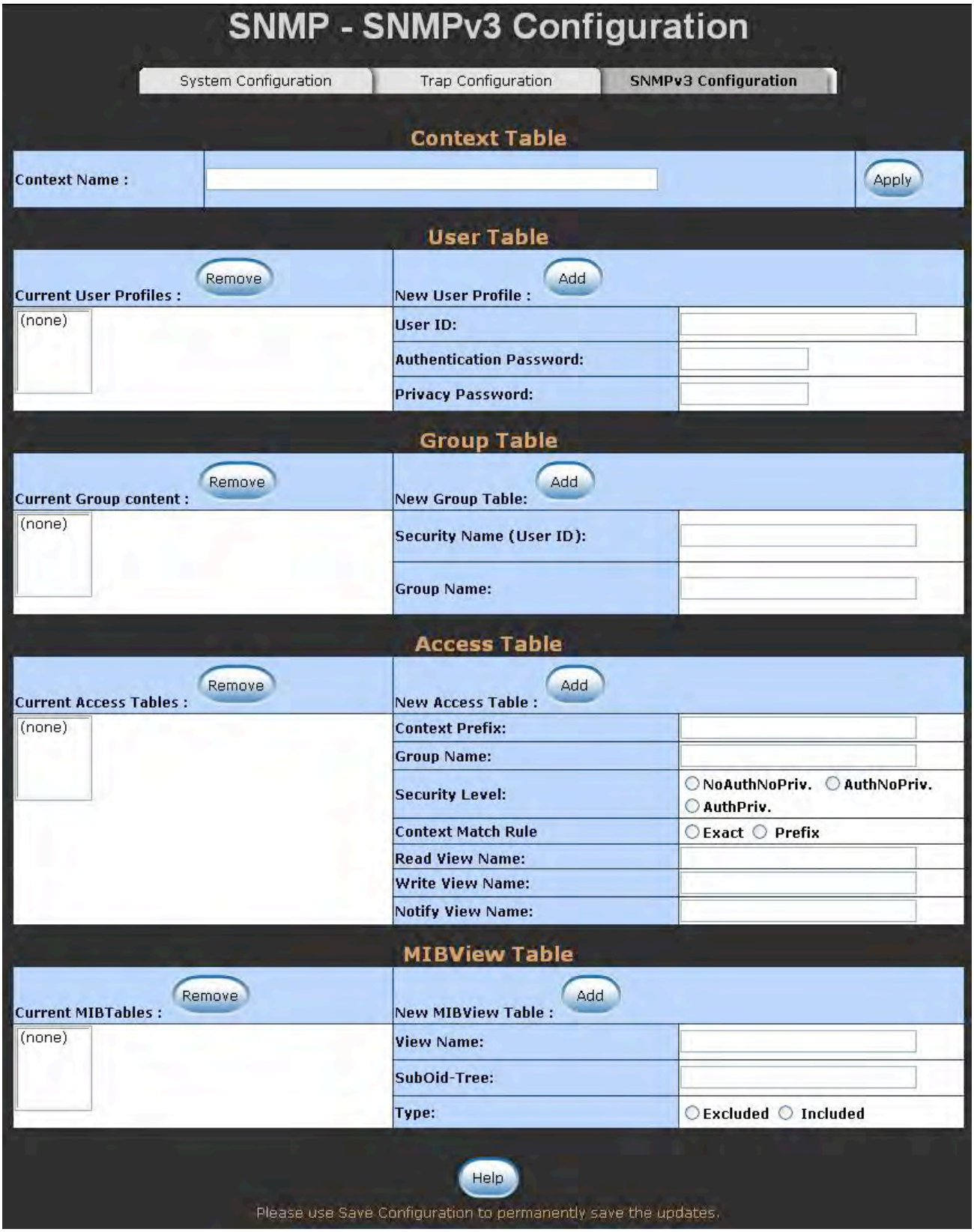
Configure SNMP v3 user table..

- **User ID:** Set up the user name.
- **Authentication Password:** Set up the authentication password.
- **Privacy Password:** Set up the private password.

- Select 

to add the user profile
- Select 

to remove the unwanted user profile.



SNMP V3 configuration interface

7.9.3.1.3 Group Table

Configure SNMP v3 group table.

- **Security Name (User ID):** Assign the user name that you have set up in group table.
- **Group Name:** Set up the group name.
- Select 

to add the group table.
- Select 

to remove the unwanted group table.

7.9.3.1.4 Access Table

Configure SNMP v3 access table.

- **Context Prefix:** Set up the context name.
- **Group Name:** Set up the group.
- **Security Level:** Set up the access level.
- **Context Match Rule:** Select the context match rule.
- **Read View Name:** Set up the read view.
- **Write View Name:** Set up the write view.
- **Notify View Name:** Set up the notify view.
- Select 

to add the access table.
- Select 

to remove the unwanted access table.

7.9.3.1.5 MIBview Table

Configure MIB view table.

- **ViewName:** Set up the name.
- **Sub-Oid Tree:** Fill the Sub OID.
- **Type:** Select the type—excluded or included.

- Select  to add the MIBview table.
- Select  to remove the unwanted MIBview table.

7.10 QoS Configuration

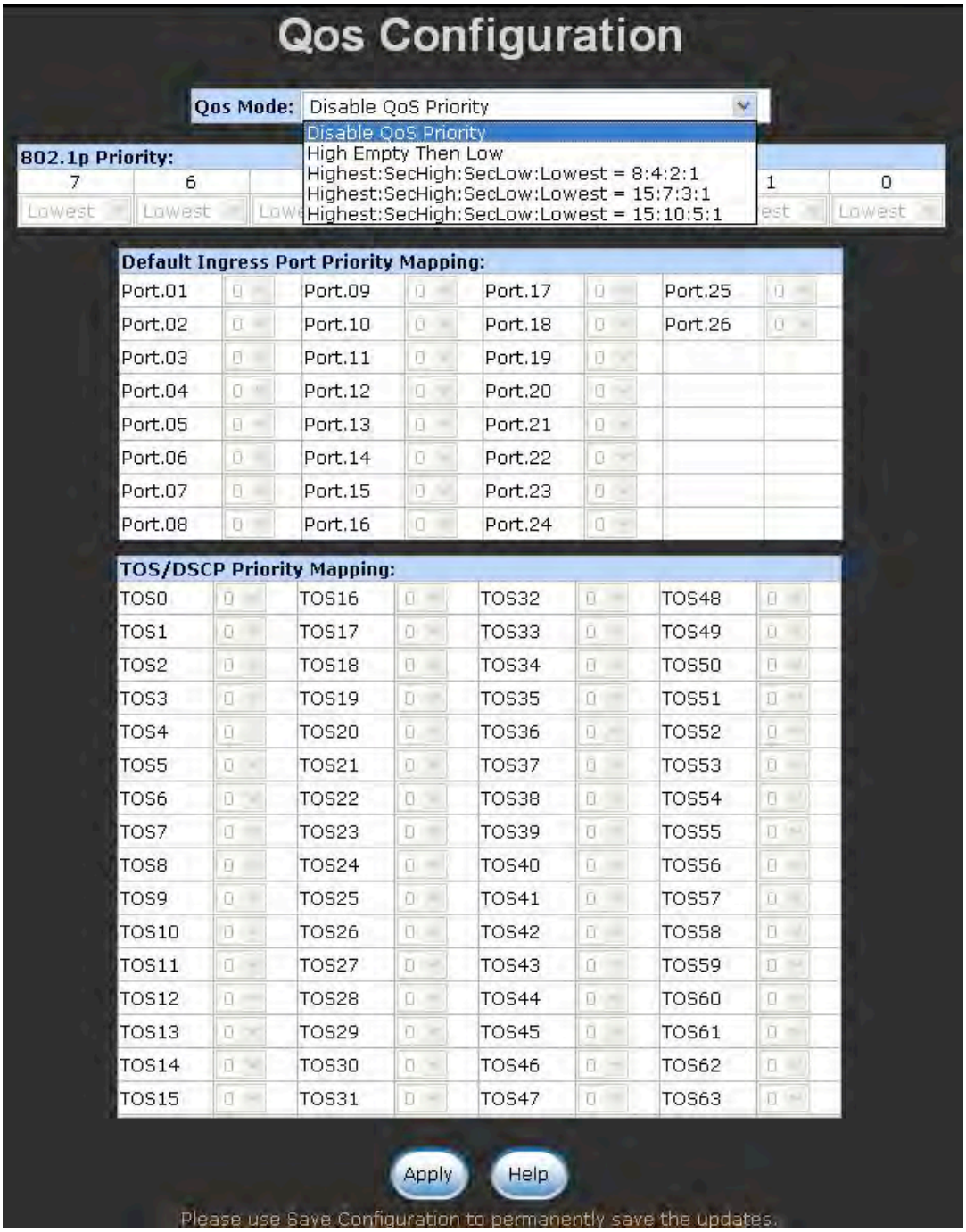
You can configure QoS mode, 802.1p priority [7-0] setting, Static Port Ingress Priority setting and TOS setting.

7.10.1 QoS Policy and Priority Type

- **Qos Mode:** Select the QoS policy rule.
  - **Disable QoS Priority:** The default status of Qos Priority is disabled.
  - **High Empty Then Low:** When all the high priority packets are empty in queue, low priority packets will be processed then.
  - **Highest:SecHigh:SecLow:Lowest:8:4:2:1:** The switch will follow 8:4:2:1 rate to process priority queue from Highest to lowest queue. For example: the system will process 80 % highest queue traffic, 40 % SecHigh queue traffic, 20 % SecLow queue traffic, and 10 % Lowest queue traffic at the same time. And the traffic in the Lowest Priority queue are not transmitted until all Highest, SecHigh, and SecLow traffic are serviced.
  - **Highest:SecHigh:SecLow:Lowest:15:7:3:1:** The process order is in compliance with the transfer rate of 15:7:3:1.
  - **Highest:SecHigh:SecLow:Lowest:15:10:5:1:** The process order is in compliance with the transfer rate of 15:10:5:1.

- **802.1p priority [7-0]:** Configure per priority level. Each priority has 4 priority levels—Highest, SecHigh, SecLow, and Lowest.
- **Default Ingress Port Priority Mapping:** The port ingress level is from 0 to 7.
- **TOS/DSCP Priority Mapping:** The system provides 0 ~ 63 TOS priority level. Each level has 8 priorities—0 ~ 7. The default value is "0" priority for each level. When the IP packet is received, the system will check the TOS level value in the IP packet that has received. For example, user set the TOS level 25 as 0. The port 1 is following the TOS

priority policy only. When the port 1 packet received, the system will check the TOS value of the received IP packet. If the TOS value of received IP packet is 25 (priority = 0), and then the packet priority will have highest priority.



QoS Configuration interface

7.11 IGMP Configuration

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

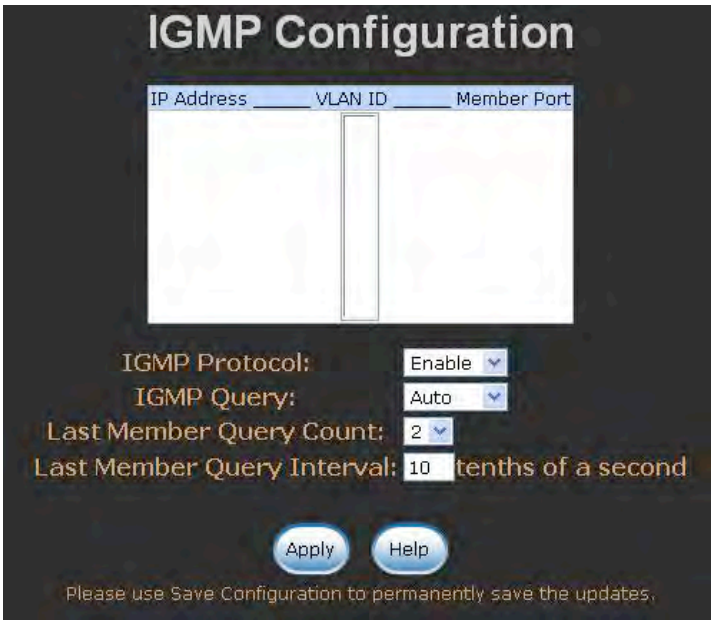
Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit being a member of a specific multicast group.

The switch supports IP multicast. You can enable IGMP protocol via setting the IGMP Configuration page to see the IGMP snooping information. IP multicast addresses are in the range of 224.0.0.0 through 239.255.255.255.

- **IGMP Protocol:** Enable or disable the IGMP protocol.
- **IGMP Query:** Select the IGMP query function as Enable or Auto to set the switch as a querier for IGMP version 2 multicast networks.
- **Last Member Query Count:** To define the count of send Last Member Query Count Group-Specific Queries. When a Querier receives a Leave Group message for a group

that has Group members on the reception interface.

- **Last Member Query Interval:** To define the interval time of send Last Member Query Count Group-Specific Queries. When a Querier receives a Leave Group message for a group that has Group members on the reception interface.
- Select Apply.



IGMP Configuration interface

7.12 LLDP Configuration

LLDP (Link Layer Discovery Protocol) function allows the switch to advertise its information to other nodes on the network and store the information it discovers.

- **LLDP Protocol:** Disable or enable LLDP function.
- **LLDP Interval:** Set the interval of learning the information time in second.
- Select Apply.

LLDP Configuration interface

7.13 X-Ring

X-Ring provides a faster redundant recovery than Spanning Tree topology. The action is similar to STP or RSTP, but the algorithms between them are not the same.

In the X-Ring topology, every switch should be enabled with X-Ring function and two ports should be assigned as the member ports in the ring. Only one switch in the X-Ring group would be set as the master switch and one of its two member ports would be blocked, called backup port, and another port is called working port. Other switches in the X-Ring group are called working switches and their two member ports are called working ports. When the failure of a network connection occurs, the backup port of the master switch (Ring Master) will automatically become a working port to recover from the failure.

The switch supports the function and interface for setting the switch as the ring master or not. The ring master can negotiate and place commands to other switches in the X-Ring group. If there are 2 or more switches in master mode, the software will select the switch with lowest MAC address number as the ring master. The X-Ring master ring mode can be enabled by setting the X-Ring configuration interface.

The system also supports the **Couple Ring** that can connect 2 or more X-Ring groups for the redundant backup function; **Dual Homing** function that can prevent connection loss between X-Ring groups and upper level/core switches. Apart from the advantages, **Central Ring** can handle up to 4 rings in the system and has the ability to recover from failure within 20 milliseconds.

- **Enable Ring:** To enable the X-Ring function, select the checkbox beside the **Enable Ring** string label. If this checkbox is not selected, all the ring functions will be unavailable.
  - **Enable Ring Master:** Select the checkbox to enable this switch to be the ring master.
  - **1st & 2nd Ring Ports:** Pull down the selection menu to assign the ports as the member ports. **1st Ring Port** is the working port and **2nd Ring Port** is the backup port. When **1st Ring Port** fails, the system will automatically upgrade the **2nd Ring Port** to be the working port.
- **Enable Couple Ring:** To enable the coupe ring function, select the checkbox beside the **Enable Couple Ring** string label.
  - **Couple Port:** Assign the member port that is connected to the other ring group.
  - **Control Port:** When the **Enable Couple Ring** checkbox is selected, you have to assign the control port to form a couple-ring group between the two X-rings.
- **Enable Dual Homing:** Set up one of the ports on the switch to be the Dual Homing port. For a switch, there is only one Dual Homing port. Dual Homing function only works when the X-Ring function enabled.
  - **Homing Port:** Assign a port which is used to be the dual homing port.
- **Enable Central Ring x:** Select the checkbox beside the string label of Enable Central Ring x to assign two ports as the blocking & forwarding ports of the ring.
  - **1st Ring Port:** Assign a port that is used to be the forwarding port to the ring.
  - **2nd Ring Port:** Assign a port that is used to be the blocking port to the ring.
- And then, select 

to have the configuration taken effect.

X-ring Interface

[NOTE]

1. When the X-Ring function enabled, the user must disable the RSTP. The X-Ring function and RSTP function cannot exist on a switch at the same time.
2. Remember to execute the “Save Configuration” action, otherwise the new configuration will be lost when the switch powers off.

7.14 Security

In this section, you can configure the 802.1x and MAC address table and ACL.

7.14.1 802.1X/Radius Configuration

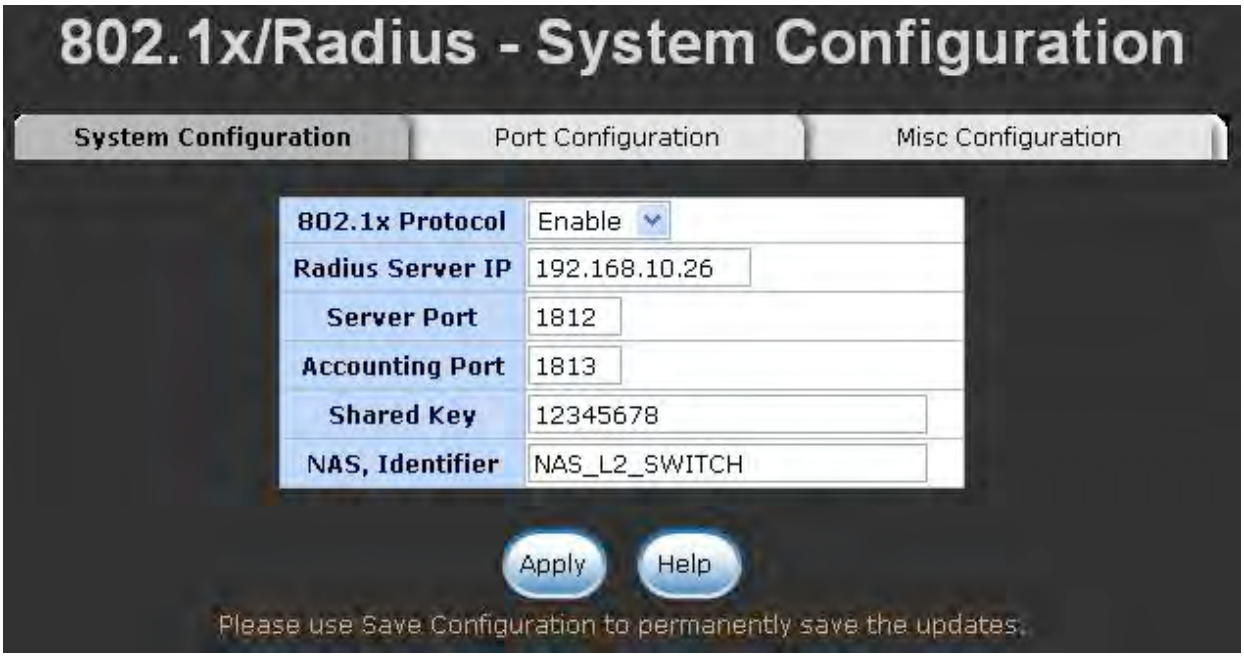
802.1x is an IEEE authentication specification which prevents the client from connecting to a wireless access point or wired switch until it provides authority, like the user name and password that are verified by an authentication server (such as RADIUS server).

7.14.1.1 System Configuration

After enabling the IEEE 802.1X function, you can configure the parameters of this function.

- **IEEE 802.1x Protocol:** Enable or disable 802.1x protocol.
- **Radius Server IP:** Assign 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 for using 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.
- Select 

.



802.1x System Configuration interface

7.14.1.2802.1x Per Port Configuration

You can configure the 802.1x authentication state for each port. The state provides Disable, Accept, Reject, and Authorize.

- **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:** When disabled, the specified port works without complying with 802.1x protocol.
- Select 

.

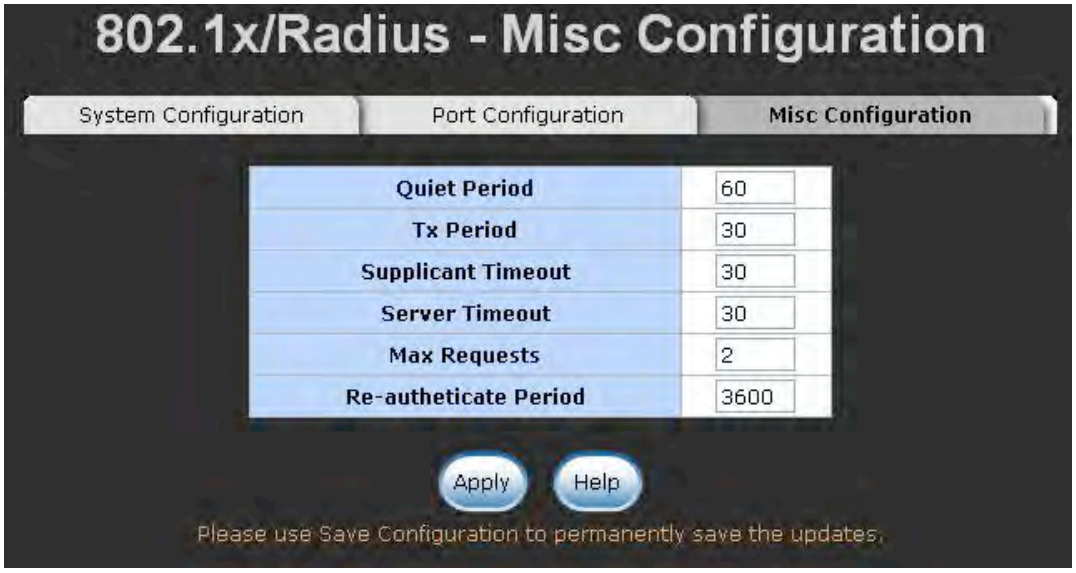
802.1x Per Port Setting interface

7.14.1.3 Misc Configuration

- **Quiet Period:** Used to define periods of time during which it will not attempt to acquire a supplicant (default time is 60 seconds)
- **TX Period:** Used to determine when an EAPOL PDU is to be transmitted (default value is 30 seconds).
- **Supplicant Timeout:** Used to determine timeout conditions in the exchanges between

the supplicant and authentication server (default value is 30 seconds).

- **Server Timeout:** Used to determine timeout conditions in the exchanges between the authenticator and authentication server (Default value is 30 seconds).
- **Max Requests:** Used to determine the number of reauthentication attempts that are permitted before the specific port becomes unauthorized (default value is 2 times).
- **Reauth Period:** Used to determine a nonzero number of seconds between periodic reauthentication of the supplications (the default value is 3,600 seconds).
- Select Apply.



802.1x Misc Configuration interface

7.14.2 MAC Address Table

Use the MAC address table to ensure the port security.

7.14.2.1 Static MAC Address

You can add a static MAC address; it remains in the switch's address table, regardless of

whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. You can add / modify / delete a static MAC address.

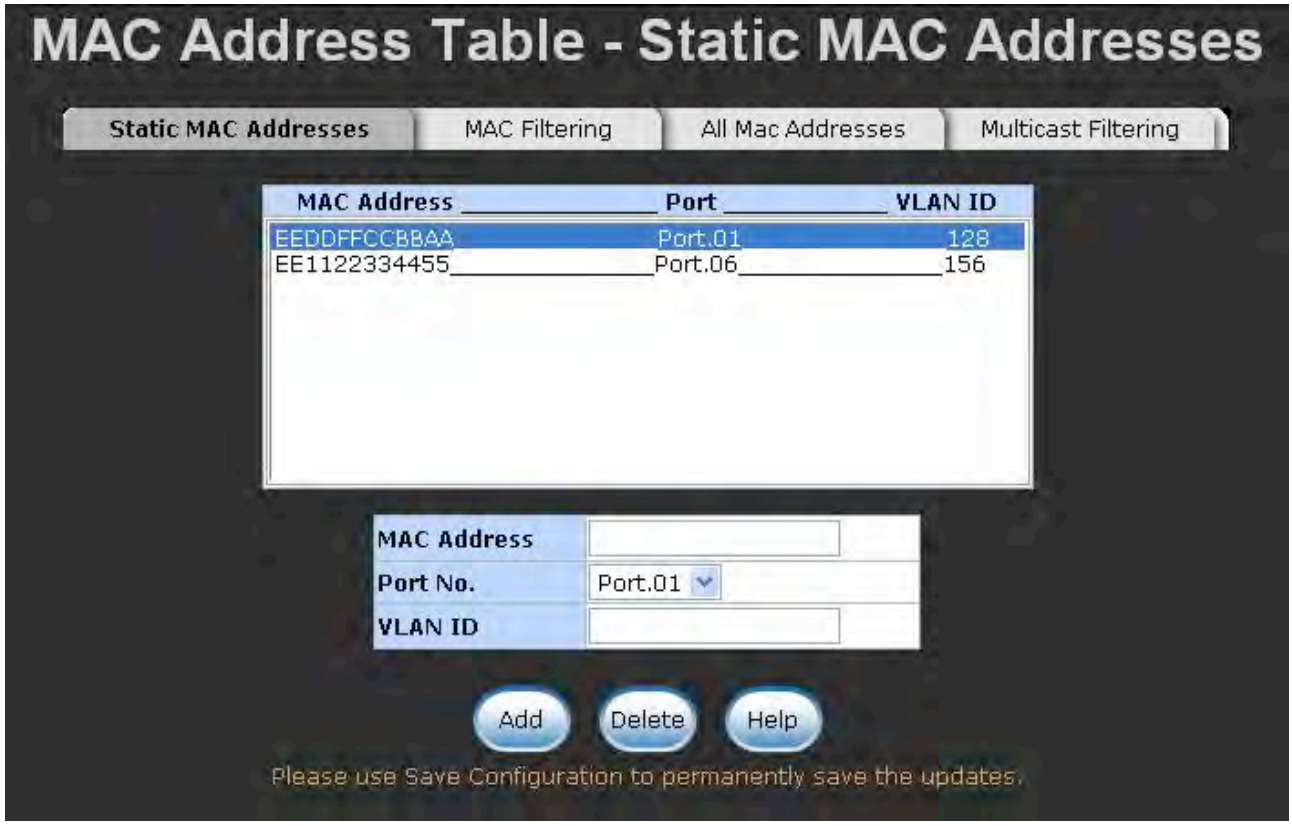
7.14.2.2 Add the Static MAC Address

You can add static MAC address in the switch MAC table in here.

- **MAC Address:** Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.
- **Port No.:** Pull down the selection menu to select the port number.
- Select 

.
- If you want to delete the MAC address from filtering table, select the MAC address and select 

.



Static MAC Addresses interface

7.14.2.3 MAC Filtering

By filtering the MAC address, the switch can easily filter the pre-configured MAC address and reduce the un-safety. You can add and delete filtering MAC address.

MAC Filtering interface

- **MAC Address:** Enter the MAC address that you want to filter.
- Select 

.
- If you want to delete the MAC address from the filtering table, select the MAC address and select 

.

7.14.2.4 All MAC Addresses

You can view the port that connected device's MAC address and the related devices' MAC address.

- Select the port.
- The selected port of static & dynamic MAC address information will be displayed in here.
- Select  to clear the current port static MAC address information on screen.

All MAC Address interface

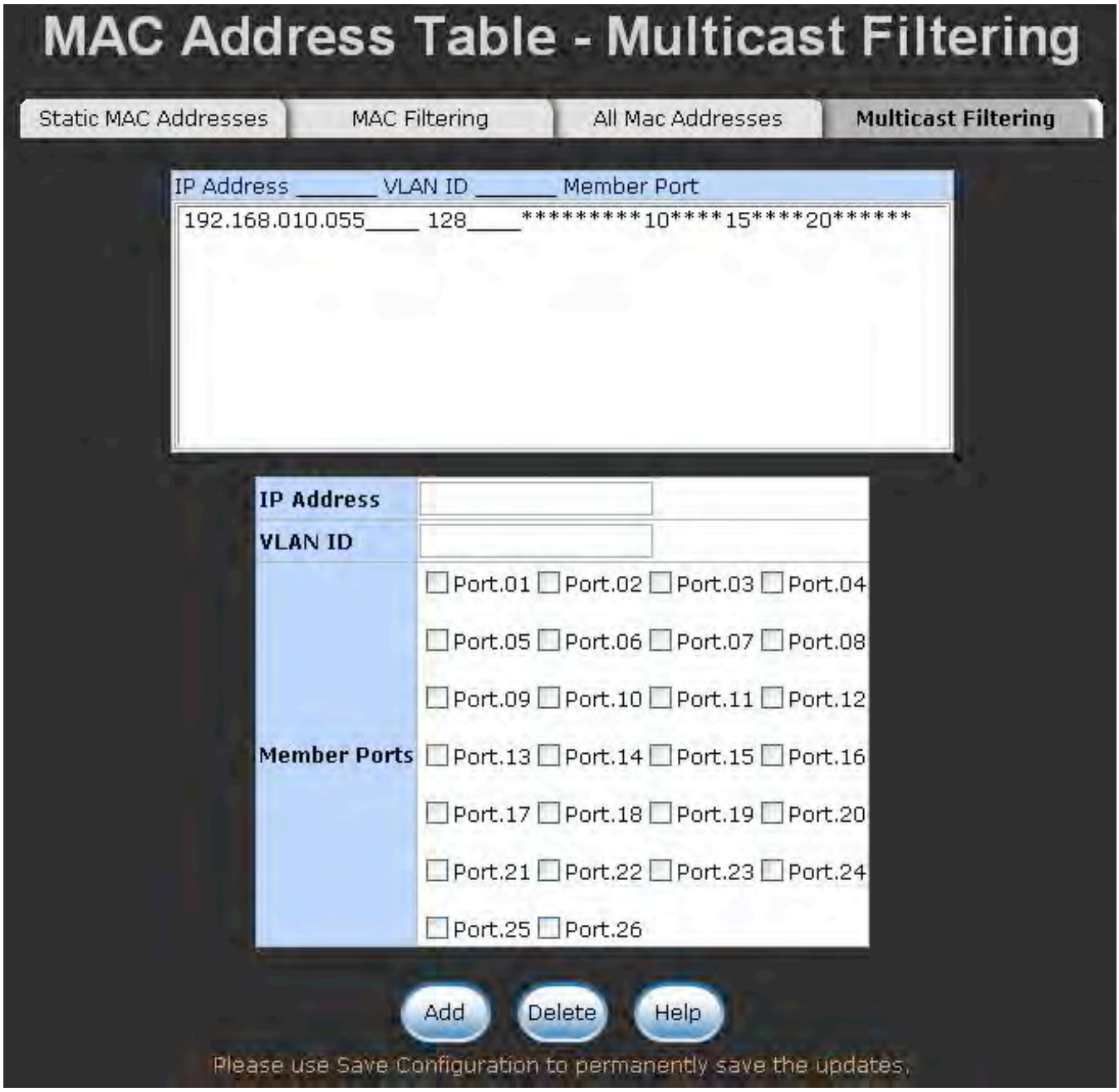
7.14.2.5 MAC Address Table—Multicast Filtering

Multicasts are similar to broadcasts, they are sent to all end stations on a LAN or VLAN. Multicast filtering is the system by which end stations only receive multicast traffic if they register to join specific multicast groups. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered end stations.

- IP Address: Assign a multicast group IP address in the range of 224.0.0.0 ~ 239.255.255.255.
- Member Ports: Select the check box beside the port number to include them as the

member ports in the specific multicast group IP address.

- Select Clear to clear the current port static MAC address information on screen.



Multicast Filtering interface

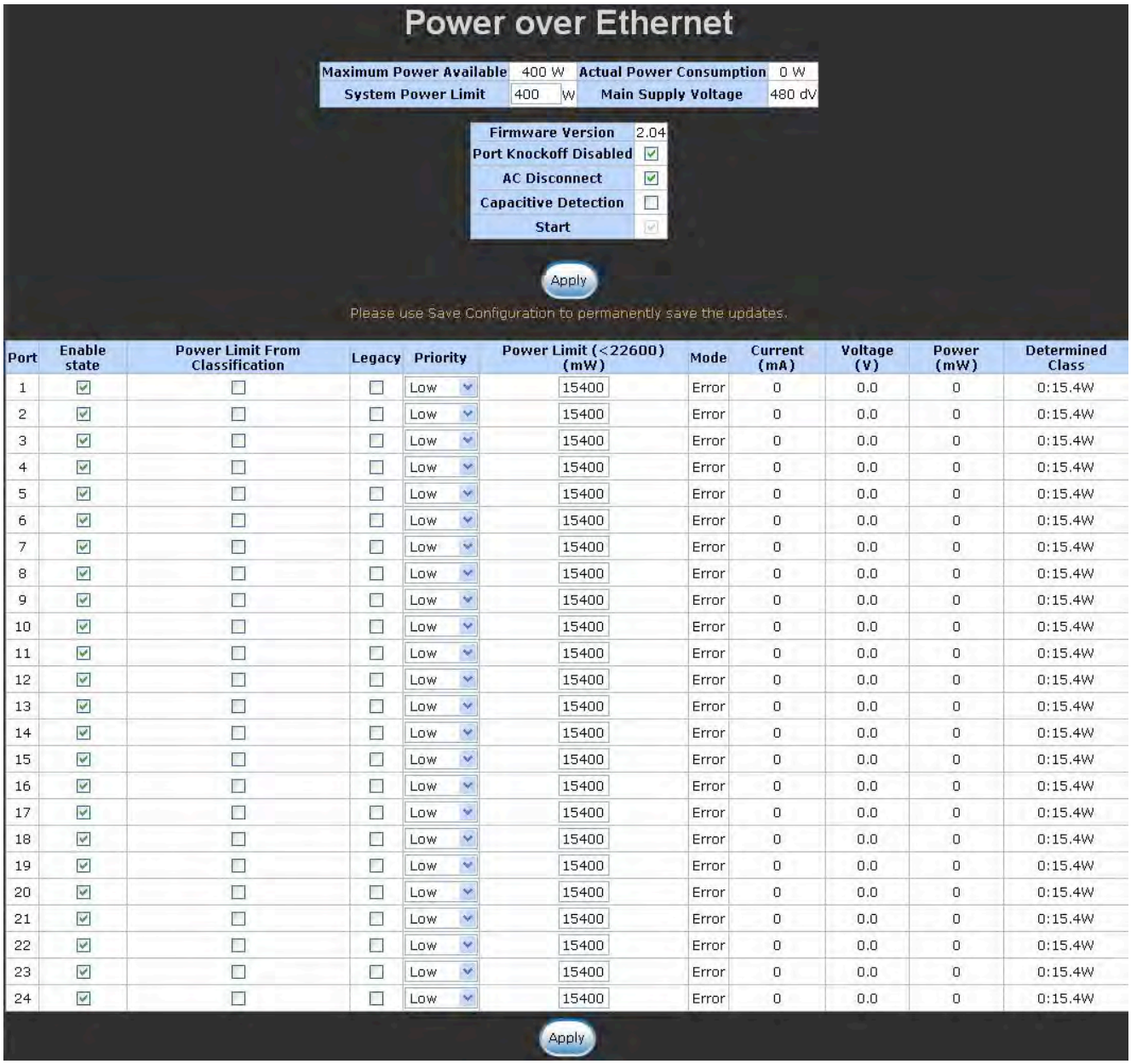
7.15 Access Control List

- **Group Id:** Type in the Group ID from 1 to 255.
- **Action:** Permit and Deny.
- **VLAN:** Select any or a particular VID.
- **Packet type:** Select packet type—IPv4 or Non-IPv4
- **Src IP Address:** Select any or assign an IP address with Subnet Mask for source IP address.
- **Dst IP Address:** Select any or assign an IP address with Subnet Mask for destination IP address.
- **Ether Type:** Pull down the select menu for Any, ARP or IPX.
- **IP Fragment:** Set this item as to whether the fragment is checked or not.
- **L4 Protocol:** Assign the L4 protocol from among ICMP(1), IGMP(2), TCP or UDP.
- **Current List:** Displays the current list information.

Access Control List interface

7.16 Power over Ethernet

This segment shows the Power over Ethernet function.



PoE Status

- **Maximum Power Available:** Displays the maximum power supply in Watt.
- **Actual Power Consumption:** This column shows the real-time total power consumption.
- **System Power Limit:** User can modify the value to this column field to limit the total output power for the system.
- **Main Supply Voltage:** This column shows the output voltage of the system for PoE ports.

- **Firmware Version:** This column shows the PoE chip's firmware version.
- **Port Knockoff Disabled:** Power Management state where one or more PDs have been powered down so that a higher priority PD may be powered up and yet not exceed the maximum total power available for PDs.
- **AC Disconnect:** Select this checkbox to monitor the AC impedance on the port terminals and removes power when the impedance rises above a certain value, for a certain period (for details, see the IEEE 802.3af specification).
- **Capacitive Detection:** If the port and capacitive detection are enabled, the capacitances state reads in the voltage result from the constant current. This is then subtracted from the pre-capacitance voltage to get a charge rate. If this charge rate is within the window of the PD signatures, the device is considered to be discovered.
- **Start:** Showing with a select symbol, the system initializes and resets successfully.
- And then, select 

to carry into effect.
- **Port:** The index of PoE ports.
- **Enable State:** Check it to enable the PoE function to the port.
- **Power Limit From:** Check it to decide the power limit method.
  - **Classification**: When this check box is selected, the system will limit the power supply to the powered device in accordance with the related class.
- **Legacy:** Check it to support the legacy power devices.
- **Priority:** Pull down the selection menu item to choose the priority of power supplying.
- **Port Limit (<22600) mW:** User can key in the power limit value that is under 22.6 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 PD's class.
- And then, select 

to carry into effect.

7.17 Factory Default

Reset switch to default configuration. Select 

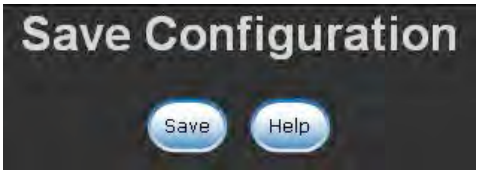
to reset all configurations to the default value.

Factory Default interface

7.18 Save Configuration

Save all configurations that you have made in the system. To ensure the all configuration will be saved. Select 

to save the all configuration to the flash memory.



Save Configuration interface

7.19 System Reboot

Reboot the switch in software reset. Select 

to restart the system.

System Reboot interface

8 Troubleshooting

8.1 Incorrect connections

The switch port can automatically detect straight or crossover cable when you link switch with other Ethernet device. For the RJ45 connector, the user should use correct UTP/STP cable. The link will fail if the RJ45 connector is not correctly pinned in the right position. For the fiber connection, please notice that fiber cable mode and fiber transceiver should match.

8.1.1.1 Faulty or loose cables

Look for loose or obviously faulty connections. If they appear to be correct, make sure the connections are snug. If that does not correct the problem, try a different cable.

8.1.1.2 Non-standard cables

Non-standard and miss-wired cables may cause numerous network collisions and other network problems, and can seriously impair network performance. A category 5e/6-cable tester is a recommended tool for network installation.

RJ45 ports: Use unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cable for RJ45 connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet). Gigabit ports should use Cat-5e or cat-6 cable for 1000Mbps connections. The length does not exceed 100 meters and the ITE is to be connected only to PoE networks without routing to the outside plant.

8.1.1.3 Improper Network Topologies

It is important to make sure that you have a valid network topology. Common topology faults include excessive cable length and too many repeaters (hubs) between end nodes. In

addition, you should make sure that your network topology contains no data path loops. Between any two end nodes, there should be only one active cabling path at any time. Data path loops will cause broadcast storms that will severely impact your network performance.

8.2 Diagnosing LED Indicators

To assist in identifying problems, the switch can be easily monitored through panel indicators, which describe common problems the user may encounter and where the user can find possible solutions.

IF the power indicator does not light on when the power cord is plugged in, you may have a problem with power outlet, or power cord. However, if the switch powers off after running for a while, check for loose power connections or power losses or surges at the power outlet. If you still cannot resolve the problem, contact ComNet for assistance.

9 Appendix A—RJ45 Pin Assignment

- **RJ45 ports**

The UTP/STP ports will automatically detect Fast Ethernet (10Base-T/100Base-TX connections), or Gigabit Ethernet (10Base-T/100Base-TX/1000Base-T connections). Auto MDI/MDIX means that the switch can connect to another switch or workstation without changing straight through or crossover cabling. See the figures below for straight through and crossover cable schematic.

9.1.1 10 /100BASE-TX Pin outs

With 10/100BASE-TX cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 for receiving data.

- **RJ45 Pin Assignments**

Pin Number	Assignment
1	Tx+
2	Tx-
3	Rx+
6	Rx-

[NOTE] "+" and "-" signs represent the polarity of the wires that make up each wire pair.

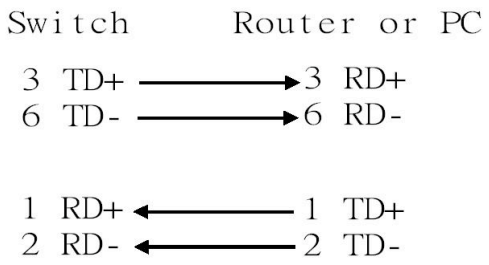
The table below shows the 10/100BASE-TX MDI and MDI-X port pin outs.

Pin Number	MDI-X Signal Name	MDI Signal Name
1	Receive Data plus (RD+)	Transmit Data plus (TD+)

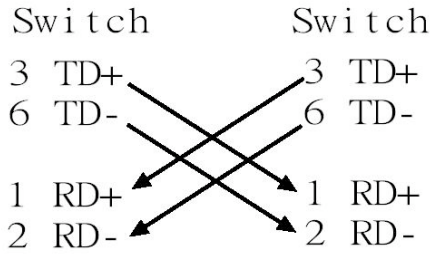
2	Receive Data minus (RD-)	Transmit Data minus (TD-)
3	Transmit Data plus (TD+)	Receive Data plus (RD+)
6	Transmit Data minus (TD-)	Receive Data minus (RD-)

9.1.2 10/100Base-TX Cable Schematic

The following two figures show the 10/100Base-TX cable schematic.



Straight-through cable schematic

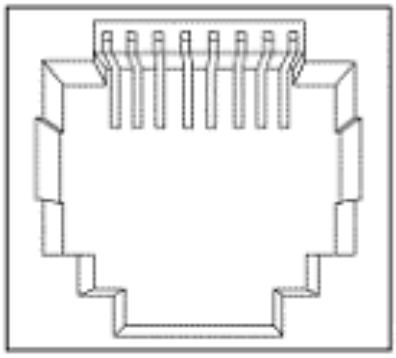


Cross over cable schematic

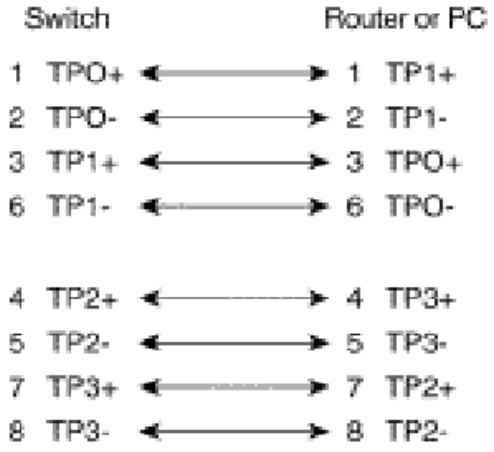
9.1.3 10/100/1000Base-TX Pin outs

The following figure shows the 10/100/1000 Ethernet RJ45 pin outs.

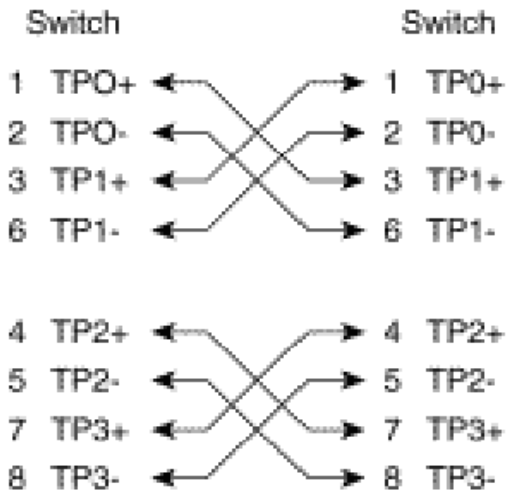
Pin	Label
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



9.1.4 10/100/1000Base-TX Cable Schematic



Straight through cables schematic



Cross over cables schematic

10 Appendix B—Command Sets

10.1.1 Commands Set List

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

10.1.2 System Commands Set

Comnet Commands	Level	Description	Example
show config	**E**	Show switch configuration	switch>show config
show terminal	**P**	Show console information	switch#show terminal
write memory	**G**	Save user configuration into permanent memory (flash rom)	switch#write memory
system name [System Name]	**G**	Configure system name	switch(config)#system name xxx
system location [System Location]	**G**	Set switch system location string	switch(config)#system location xxx
system description [System Description]	**G**	Set switch system description string	switch(config)#system description xxx
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 192.168.10.1 255.255.255.0 192.168.10.254
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
faultrelay power [number] [enable|disable]	**G**	Configure Relay Alarm for Power Failure	switch(config)# faultrelay power 1 enable
faultrelay enable [enable|disable]	**I**	Configure Relay Alarm for Port Link Down/Broken	switch(config)# interface fastEthernet 3 switch(config-if)# faultrelay enable
show faultrelay	**P**	Show Fault Relay Alarm setting	switch#show faultrelay
default	**G**	Restore to default	Switch(config)#default
admin username [Username]	**G**	Changes a login username. (maximum 10 words)	switch(config)#admin username xxxxxx
admin password [Password]	**G**	Specifies a password (maximum 10 words)	switch(config)#admin password xxxxxx
show admin	**P**	Show administrator information	switch#show admin
dhcpserver enable	**G**	Enable DHCP Server	switch(config)#dhcpserver enable
dhcpserver lowip [Low IP]	**G**	Configure low IP address for IP pool	switch(config)# dhcpserver lowip 192.168.10.1
dhcpserver highip [High IP]	**G**	Configure high IP address for IP pool	switch(config)# dhcpserver highip 192.168.10.50
dhcpserver subnetmask [Subnet mask]	**G**	Configure subnet mask for DHCP clients	switch(config)#dhcpserver subnetmask 255.255.255.0
dhcpserver gateway [Gateway]	**G**	Configure gateway for DHCP clients	switch(config)#dhcpserver gateway 192.168.1.254
dhcpserver dnsip [DNS IP]	**G**	Configure DNS IP for DHCP clients	switch(config)# dhcpserver dnsip 192.168.10.1
dhcpserver leasetime [Hours]	**G**	Configure lease time (in hour)	switch(config)#dhcpserver leasetime 1
dhcpserver ipbinding [IP address]	**I**	Set static IP for DHCP clients by port	switch(config)#interface fastEthernet 2 switch(config-if)#dhcpserver ipbinding 192.168.10.1

show dhcpserver configuration	**P**	Show configuration of DHCP server	switch#show dhcpserver configuration
show dhcpserver clients	**P**	Show client entries of DHCP server	switch#show dhcpserver clinets
show dhcpserver ip-binding	**P**	Show IP-Binding information of DHCP server	switch#show dhcpserver ip-binding
no dhcpserver	**G**	Disable DHCP server function	switch(config)#no dhcpserver
security enable	**G**	Enable IP security function	switch(config)#security enable
security http	**G**	Enable IP security of HTTP server	switch(config)#security http
security telnet	**G**	Enable 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 1 192.168.10.55
show security	**P**	Show the information of IP security	switch#show security
no security	**G**	Disable IP security function	switch(config)#no security
no security http	**G**	Disable IP security of HTTP server	switch(config)#no security http
no security telnet	**G**	Disable IP security of telnet server	switch(config)#no security telnet
bsf rate	**G**	Configure Broadcast Storm Filter selection	switch(config)#bsf rate 1/2
bsf flooded-unicast-multicast	**G**	Enable Flooded Unicast/Multicast Packets BSF	switch(config)#bsf flooded-unicast-multicast
bsf control	**G**	Enable Control Packets BSF	switch(config)#bsf control
bsf ip-multicast	**G**	Enable IP Multicast Packets BSF	switch(config)#bsf ip-multicast
bsf broadcast	**G**	Packets BSF	switch(config)#bsf broadcast
no bsf flooded-unicast-multicast	**G**	Disable Flooded Unicast/Multicast Packets BSF	switch(config)#no bsf flooded-unicast-multicast

no bsf control	**G**	Disable Control Packets BSF	switch(config)#no bsf control
no bsf ip-multicast	**G**	Disable IP Multicast Packets BSF	switch(config)#no bsf ip-multicast
no bsf broadcast	**G**	Disable Broadcast Packets BSF	switch(config)#no bsf broadcast
jumbo-frame	**G**	Enable jumbo frame	switch(config)# jumbo-frame
no jumbo-frame	**G**	Disable jumbo frame	switch(config)#no jumbo-frame
show jumbo-frame	**G**	Show jumbo frame enable/disable	switch#show jumbo-frame

10.1.3 Port Commands Set

Comnet Commands	Level	Description	Example
interface fastEthernet [Portid]	**G**	Choose the port for modification.	switch(config)#interface fastEthernet 2
duplex [full | half]	**I**	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	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 of operation for Fast Ethernet., the speed can't be set to 1000 if the port isn't a giga port.	switch(config)#interface fastEthernet 2 switch(config-if)#speed 100
flowcontrol [Enable|Disable]	**I**	Use the flow control configuration command on Ethernet ports to control traffic rates during congestion.	switch(config)#interface fastEthernet 2 switch(config-if)#flowcontrol enable
no flowcontrol	**I**	Disable flow control of interface	switch(config-if)#no flowcontrol
security enable	**I**	Enable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#security enable

no security	**I**	Disable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#no security
ratelimit in **[Value]**	**I**	Set interface input rate limiting	switch(config)#interface fastEthernet 2 switch(config-if)# ratelimit in 100
ratelimit out **[Value]**		Set interface output rate limiting	switch(config)#interface fastEthernet 2 switch(config-if)# ratelimit out 100
show ratelimit	**I**	Show interfaces rate limiting	switch(config)#interface fastEthernet 2 switch(config-if)#show ratelimit
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 switch(config-if)#state Disable
show interface configuration	**I**	show interface configuration status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface configuration
show interface status	**I**	show interface actual status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface status
show interface accounting1	**I**	show interface statistic counter1	switch(config)#interface fastEthernet 2 switch(config-if)#show interface accounting1
show interface accounting2	**I**	show interface statistic counter2	switch(config)#interface fastEthernet 2 switch(config-if)#show interface accounting2
no accounting	**I**	Clear interface accounting information	switch(config)#interface fastEthernet 2 switch(config-if)#no accounting
alias **[name]**	**I**	Configure alias name of port	switch(config)#interface fastEthernet 2 switch(config-if)#alias PORT002

10.1.4 Trunk Commands Set

Comnet Commands	Level	Description	Example
aggregator priority [1~65535]	G	Set port group system priority	switch(config)#aggregator priority 22
aggregator activityport [Group ID][Port Numbers]	G	Set activity port	switch(config)#aggregator activityport 2 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 separate by a comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount 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 list separate by a comma(ex.2, 3, 6)	switch(config)#aggregator group 1 2-4 nolacp or switch(config)#aggreator group 1 3,1,2 nolacp
show aggregator [Group-number]	P	Show the information of trunk group	switch#show aggregator 1

no aggregator lacp [GroupID]	**G**	Disable the LACP function of trunk group	switch(config)#no aggreator lacp 1
no aggregator group [GroupID]	**G**	Remove a trunk group	switch(config)#no aggreator group 2

10.1.5 VLAN Commands Set

Comnet Commands	Level	Description	Example
vlan database	**P**	Enter VLAN configure mode	switch#vlan database
vlanmode [portbase| 802.1q | gvrp]	**V**	To set switch VLAN mode.	switch(vlan)# vlanmode portbase or switch(vlan)# vlanmode 802.1q or switch(vlan)# vlanmode gvrp
no vlan	**V**	Disable VLAN	Switch(vlan)#no vlan
Ported based VLAN configuration			
vlan port-based grpname [Group Name] **grpid** [GroupID] **port** [PortNumbers]	**V**	Add new port based VALN	switch(vlan)# vlan port-based grpname test grpid 2 port 2-4
show vlan [GroupID] **or** **show vlan**	**V**	Show VLAN information	switch(vlan)#show vlan 23
no vlan group [GroupID]	**V**	Delete port base group ID	switch(vlan)#no vlan group 2
IEEE 802.1Q VLAN			
vlan 8021q name **[GroupName]** **vid** [VID]	**V**	Change the name of VLAN group, if the group didn't exist, this command can't be applied.	switch(vlan)#vlan 8021q test vid 22

vlan 8021q port [PortNumber] **access-link untag** [UntaggedVID]	V	Assign a access link for VLAN by port, if the port belong 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 VLAN by port, if the port belong 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 VLAN by port, if the port belong 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 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** [UntaggedVID] **tag** [TaggedVID List]	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 trunk 3 hybrid-link untag 5 tag 6-8
show vlan [GroupID] **or show vlan**	V	Show VLAN information	switch(vlan)#show vlan 23
vlan 8021q mnt-vid [VID]	V	Configure management VID (0 is disabled)	switch(vlan)# vlan 8021q mnt-vid 1

10.1.6 Spanning Tree Commands Set

Comnet Commands	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 recomputed 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 time determines how long each of the listening and learning states last before the port begins forwarding.	switch(config)# spanning-tree forward-time 20

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 on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-p2p Auto
stp-admin-edge [True|False]	I	Admin Edge of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-edge True
stp-admin-non-stp [True|False]	I	Admin NonSTP of STP priority on this interface.	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

10.1.7 QOS Commands Set

Comnet Commands	Level	Description	Example
qos priority-tos [TosNum][Priority]	G	Configure TOS Priority	switch(config)#qos priority-tos 9 7
qos mode [SP|WRR|WRR1|WRR2]	G	Configure QOS mode	switch(config)#qos mode sp

qos 8021p-priority [Index][Lowest|SecLow|SecHigh|Highest]	**G**	Configure 8021p Priority	switch(config)#qos 8021p-Priority 1 lowest
qos priority-portbased [Priority]	**I**	Configure COS Priority	switch(config)#interface fastEthernet 2 switch(config-if)#qos priority-portbased 1

10.1.8 IGMP Commands Set

Comnet Commands	Level	Description	Example
igmp enable	**G**	Enable 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
igmp query-interval [1~250 sec.]	**G**	Configure query interval	switch(config)# igmp query-interval 10
igmp query-response-interval [1~250 tenths of a sec.]	**G**	Configure query response interval	switch(config)# igmp query-response-interval 60
igmp last-query-count [1~2]	**G**	Configure last member query count	switch(config)# igmp last-query-count 1
igmp last-query-interval [1~250 tenths of a sec.]	**G**	Configure last member query interval	switch(config)# igmp last-query-interval 60
igmp unregister flooding [flooding blocking]	**G**	Configure IGMP unregister stream	switch(config)# igmp unregister flooding
show igmp configuration	**P**	Show IGMP configuration	switch#show igmp configuration
show igmp table	**P**	Show IGMP snooping table	switch#show igmp table
no igmp	**G**	Disable IGMP snooping function	switch(config)#no igmp
no igmp query	**G**	Disable IGMP query	switch#no igmp query

10.1.9 Mac / Filter Table Commands Set

Comnet Commands	Level	Description	Example
mac-address-table static hwaddr [HW-Addr][VID]	I	Configure MAC address table of interface (static).	switch(config)#interface fastEthernet 2 switch(config-if)#mac-address-table static hwaddr 000012345678 1
mac-address-table filter hwaddr [HW-Addr][VID]	G	Configure MAC address table(filter)	switch(config)#mac-address-table filter hwaddr 000012348678 1
show mac-address-table	I	Show all MAC address table	switch(config)#interface fastEthernet 2 switch(config-if)#show mac-address-table
show mac-address-table static	P	Show static MAC address table	switch#show mac-address-table static
show mac-address-table filter	P	Show filter MAC address table.	switch#show mac-address-table filter
no mac-address-table static hwaddr [HW-Addr][VID]	I	Remove an entry of MAC address table of interface (static)	switch(config)#interface fastEthernet 2 switch(config-if)#no mac-address-table static hwaddr 000012345678 1
no mac-address-table filter hwaddr [HW-Addr][VID]	G	Remove an entry of MAC address table (filter)	switch(config)#no mac-address-table filter hwaddr 000012348678 1
no mac-address-table	G	Remove dynamic entry of MAC address table	switch(config)#no mac-address-table
auto-age [150|300|600]	G	Configure auto age time of MAC table	switch(config)#auto-age 150
no auto-age	G	Disable auto age time of MAC table	switch(config)#no auto-age
show auto-age	P	Display auto age time of MAC table	switch# show auto-age
auto-flush	G	Enable auto flush MAC Table when link down	switch(config)#auto-flush
no auto-flush	G	Disable auto flush MAC Table when link down	switch(config)#no auto-flush
show auto-flush	P	Disable auto flush function of MAC table	switch# show auto-flush
multicast-filtering	I	Configure multicast filtering	switch(config)#interface fastEthernet 2

[IP-Addr][VID]		entry of interface	switch(config-if)# multicast-filtering 239.0.0.1 1
no multicast-filtering [IP-Addr][VID]	I	Remove multicast filtering entry of interface	switch(config)#interface fastEthernet 2 switch(config-if)#no multicast-filtering 239.0.0.1 1
no multicast-filtering [IP-Addr][VID]	G	Remove multicast filtering entry	switch(config)#no multicast-filtering 239.0.0.1 1
show multicast-filtering	I	Show multicast filtering table	switch#show multicast-filtering

10.1.10 SNMP Commands Set

Comnet Commands	Level	Description	Example
snmp system-name [System Name]	G	Set SNMP agent system name	switch(config)#snmp system-name l2switch
snmp system-location [System Location]	G	Set SNMP agent system location	switch(config)#snmp system-location lab
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	Add 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 information and community string	switch(config)#snmp-server host 192.168.1.50 community public trap-version v1 (remove) Switch(config)# no snmp-server host 192.168.10.50
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 userprofile for SNMPV3 agent. Privacy password could be empty.	switch(config)#snmpv3 user test01 group G1 password AuthPW PrivPW
snmpv3 access context-name [Context Name] **group** [Group Name] **security-level** [NoAuthNoPriv|AuthNoPriv|AuthPriv] **match-rule** [Exact|Prifix] **views** [Read View Name] [Write View Name] [Notify View Name]	**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 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**	Show 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 host 192.168.10.50
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** [Group Name] **security-level** [NoAuthNoPriv|AuthNoPriv|AuthPriv] **match-rule** [Exact|Prifix] **views** [Read View Name] [Write View Name] [Notify View Name]	**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
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

10.1.11 Port Mirroring Commands Set

Comnet Commands	Level	Description	Example
monitor destination [Port ID]	**G**	Set destination port	switch(config)#monitor destination 1
monitor source [Port ID]	**G**	Set source port	switch(config)#monitor source 2
monitor mode [RX|TX|Both|Disabled]	**G**	Configure mode of monitor function	switch(config)#monitor mode rx
show monitor	**P**	Show port monitor information	switch#show monitor

10.1.12 802.1x Commands Set

Comnet Commands	Level	Description	Example
8021x enable	G	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# 8021x enable
8021x system radiousip [IP address]	G	Use the 802.1x system radious IP global configuration command to change the radious server IP.	switch(config)# 8021x system radiusip 192.168.10.1
8021x system serverport [port ID]	G	Use the 802.1x system server port global configuration command to change the radious server port	switch(config)# 8021x system serverport 1815
8021x system accountport [port ID]	G	Use the 802.1x system account port global configuration command to change the accounting port	switch(config)# 8021x system accountport 1816
8021x system sharekey [ID]	G	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)# 8021x system sharedkey 123456
8021x system nasid [words]	G	Use the 802.1x system nasid global configuration command to change the NAS ID	switch(config)# 8021x system nasid test1
8021x misc quietperiod [sec.]	G	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch(config)# 8021x misc quietperiod 10
8021x misc txperiod [sec.]	G	Use the 802.1x misc TX period global configuration command to set the TX period.	switch(config)# 8021x misc txperiod 5

8021x misc supportimeout [sec.]	**G**	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	switch(config)# 8021x misc supptimeout 20
8021x misc servertimeout [sec.]	**G**	Use the 802.1x misc server timeout global configuration command to set the server timeout.	switch(config)#8021x misc servertimeout 20
8021x misc maxrequest [number]	**G**	Use the 802.1x misc max request global configuration command to set the MAX requests.	switch(config)# 8021x misc maxrequest 3
8021x misc reauthperiod [sec.]	**G**	Use the 802.1x misc reauth period global configuration command to set the reauth period.	switch(config)# 8021x misc reauthperiod 3000
8021x portstate [disable | reject | accept | authorize]	**I**	Use the 802.1x port state interface configuration command to set the state of the selected port.	switch(config)#interface fastethernet 2 switch(config-if)#8021x portstate accept
show 8021x	**E**	Display a summary of the 802.1x properties and also the port sates.	switch>show 8021x
no 8021x	**G**	Disable 802.1x function	switch(config)#no 8021x

10.1.13 TFTP Commands Set

Comnet Commands	Level	Description	Example
backup flash:backup_cfg	**G**	Save configuration to TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#backup flash:backup_cfg
restore flash:restore_cfg	**G**	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.	switch(config)#restore flash:restore_cfg

upgrade flash:upgrade_fw	**G**	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#upgrade flash:upgrade_fw

10.1.14 SystemLog, SMTP and Event Commands Set

Comnet Commands	Level	Description	Example
systemlog ip [IP address]	**G**	Set System log server IP address.	switch(config)# systemlog ip 192.168.10.100
systemlog mode [client|server|both]	**G**	Specified the log mode	switch(config)# systemlog mode both
show systemlog	**E**	Display system log.	Switch>show systemlog
show systemlog	**P**	Show system log client & server information	switch#show systemlog
no systemlog	**G**	Disable systemlog functon	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 192.168.10.5
smtp subject [subject]	**G**	Configure subject of mail	switch(config)#smtp subject test
smtp sender [sender]	**G**	Configure sender of mail	switch(config)#smtp sender tester
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 Rcpt e-mail Address	switch(config)#smtp rcptemail 1 Alert@test.com
show smtp	**P**	Show the information of SMTP	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 device-warm-start [Systemlog|SMTP|Both]	**G**	Set warm start event type	switch(config)#event device-warm-start both
event authentication-failure [Systemlog|SMTP|Both]	**G**	Set Authentication failure event type	switch(config)#event authentication-failure both
event ring-topology-change [Systemlog|SMTP|Both]	**G**	Set X-ring topology changed event type	switch(config)#event ring-topology-change both
event systemlog [Link-UP|Link-Down|Both]	**I**	Set port event for system log	switch(config)#interface fastethernet 2 switch(config-if)#event systemlog both
event smtp [Link-UP|Link-Down|Both]	**I**	Set port event for SMTP	switch(config)#interface fastethernet 2 switch(config-if)#event smtp both
show event	**P**	Show event selection	switch#show event
no event device-cold-start	**G**	Disable cold start event type	switch(config)#no event device-cold-start both
no event device-warm-start	**G**	Disable warm start event type	switch(config)#no event device-warm-start both
no event authentication-failure	**G**	Disable Authentication failure event typ	switch(config)#no event authentication-failure both
no event ring-topology-change	**G**	Disable super ring topology changed event type	switch(config)#no event ring-topology-change both
no event systemlog	**I**	Disable port event for system log	switch(config)#interface fastethernet 2 switch(config-if)#no event systemlog
no event smpt	**I**	Disable port event for SMTP	switch(config)#interface fastethernet 2 switch(config-if)#no event smtp
show systemlog	**P**	Show system log client & server information	switch#show systemlog

10.1.15 SNTP Commands Set

Comnet Commands	Level	Description	Example
sntp enable	G	Enable SNTP function	switch(config)#sntp enable
sntp daylight	G	Enable daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight
sntp daylight-period [Start time] [End time]	G	Set period of daylight saving time, if SNTP function is inactive, this command can't be applied. Parameter format: [yyyymmdd-hh:mm]	switch(config)# sntp daylight-period 20060101-01:01 20060202-01-01
sntp daylight-offset [Minute]	G	Set offset of daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight-offset 3
sntp ip [IP]	G	Set SNTP server IP, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp ip 192.168.1.1
sntp timezone [Timezone]	G	Set timezone index, use "show sntp timzezone" command to get more information of index number	switch(config)#sntp timezone 22
show sntp	P	Show SNTP information	switch#show sntp
show sntp timezone	P	Show 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 saving time	switch(config)#no sntp daylight

10.1.16 X-Ring Commands Set

Comnet Commands	Level	Description	Example
ring enable	G	Enable X-ring	switch(config)#ring enable
ring master	G	Enable ring master	switch(config)#ring master
ring ringport [1st Ring Port] [2nd Ring Port]	G	Configure 1st/2nd Ring Port	switch(config)#ring ringport 7 8
ring couplering	G	Enable couple ring	switch(config)#ring couplering
ring couplering couplingport [Coupling Port]	G	Configure Coupling Port	switch(config)#ring couplering couplingport 1
ring couplering controlport [Control Port]	G	Configure Control Port	switch(config)#ring couplering controlport 2
ring dualhoming	G	Enable dual homing	switch(config)#ring dualhoming
ring dualhoming homingport [Dual Homing Port]	G	Configure Dual Homing Port	switch(config)#ring dualhoming homingport 3
show ring	P	Show the information of X-Ring	switch#show ring
no ring	G	Disable X-ring	switch(config)#no ring
no ring master	G	Disable ring master	switch(config)# no ring master
no ring couplering	G	Disable couple ring	switch(config)# no ring couplering
no ring dualhoming	G	Disable dual homing	switch(config)# no ring dualhoming
ring centralring [ring ID (1~4)] [1st Ring Port] [2nd Ring Port]	G	Enable and configure central ring port	switch(config)#ring centralring 1 7 8
no ring centralring [ring ID (1~4)]	G	Disable central ring	switch(config)# no ring centralring 1

10.1.17 LLDP Command Set

Comnet Commands	Level	Description	Example
lldp enable	G	Enable LLDP function	switch(config)#lldp enable
lldp interval [TIME sec]	G	Configure LLDP interval	switch(config)#lldp interval 10
no lldp	G	Disable LLDP function	switch(config)#no lldp
show lldp	P	Show LLDP function	switch#show lldp

10.1.18 Access Control List Command Set

Comnet Commands	Level	Description	Example
acl gid [Group ID]	G	Configure ACL group id	switch(config)#acl gid 1
acl action [Permit|Deny]	G	Configure ACL action	switch(config)#acl action permit
acl vid [Any|VLAN ID]	G	Configure ACL VLAN ID	switch(config)#acl vid any
acl pktype [IPv4|Non-IPv4]	G	Configure ACL packet type	switch(config)#acl pktype ipv4
acl ethtype [Any|ARP|IPX|Type value]	G	Configure ACL ether type	switch(config)#acl ethtype arp
acl sip any	G	Any Src IP	switch(config)#acl sip any
acl sip ip [IP address][Mask]	G	Specify Src IP and Mask	switch(config)#acl sip ip 192.168.10.1 255.255.255.0
acl dip any	G	Any Des IP	switch(config)#acl dip any
acl dip ip [IP address][Mask]	G	Specify Des IP and Mask	switch(config)#acl dip ip 192.168.10.1 255.255.255.0
acl frg [Check|Uncheck]	G	Configure ACL IP fragment	switch(config)#acl frg check
acl l4 other [Any|ICMP|IGMP|Protocol value]	G	Configure ACL L4 protocol other type	switch(config)#acl l4 other any

acl l4 tcp [Any|FTP|HTTP|Port Number]	**G**	Configure ACL L4 protocol TCP	switch(config)#acl l4 tcp ftp
acl l4 udp [Any|TFTP|Port Number]	**G**	Configure ACL L4 protocol UDP	switch(config)#acl l4 udp tftp
acl add	**G**	Add new group structure	switch(config)#acl add
acl show	**G**	Show content of current configured ACL group.	switch(config)#acl show
acl test	**G**	Debug command for ACL.	switch(config)#acl test 0
no acl	**G**	Delete ACL group.	switch(config)#no acl 1
show acl	**P**	Show ACL list.	switch#show acl

10.1.19 Power over Ethernet Set

Comnet Commands	Level	Description	Example
poe	**P**	Enter POE configure mode	switch#poe
system power-limit [Value] **Parameter only** [0~400]		Set PoE system System Power Limit	switch(poe)# system power-limit 350
system knockoff-disabled [Enable|Disable]		Set PoE system Port Knockoff Disabled	switch(poe)# system knockoff-disabled disable
system ac-dissconnect [Enable|Disable]		Set PoE system AC Dissconnect	switch(poe)# system ac-dissconnect disable
system capacitive-detect [Enable|Disable]		Set PoE system Capacitive Detection	switch(poe)# system capacitive-detect enable
port 1 state disable **port** [PortNumbers] **stace** [Enable|Disable]		Set PoE port State	switch(poe)# port 1 state disable
port 1 plfc enable **port** [PortNumbers] **plfc** [Enable|Disable]		Set PoE port Power Limit from Classification	switch(poe)# port 1 plfc enable
port 1 legacy enable **port** [PortNumbers] **legacy** [Enable|Disable]		Set PoE port Legacy	switch(poe)# port 1 legacy enable

port 1 priority high **port** [PortNumbers] **priority** [Low|High|Critical]		Set PoE port Priority	switch(poe)# port 1 priority high
port 1 powerlimit 15300 **port** [PortNumbers] **powerlimit** [Value] **Parameter only** [0~15400]		Set PoE port Power Limit Value	switch(poe)# port 1 powerlimit 15300
show poe	**P**	Show setting of PoE function	switch#show poe

ComNet Customer Service

Customer Care is ComNet Technology's global service center, where our professional staff are ready to answer your questions at any time. Email address of ComNet Global Service Center: customercare@ComNet.net

Communication Networks

World Headquarters
3 Corporate Drive
Danbury, CT 06810 USA
T 203 796-5300
F 203 796-5303
888 678-9427 Tech Support
info@ComNet.net

ComNet Europe Ltd
8 Turnberry Park Road
Gildersome, Morley
Leeds, LS27 7LE, UK
T +44 (0)113 307 6400
F +44 (0)113 253 7462
info-europe@ComNet.net