



## INSTALLATION AND OPERATION MANUAL

# CNGE2FE16MS

## MANAGED ETHERNET SWITCH WITH (16) 10/100TX + (2) CONFIGURABLE 10/100/1000TX / 100/1000FX PORTS

v2.01 Jan 2012

The ComNet™ CNGE2FE16MS Managed Ethernet Switch provides robust transmission of (16) 10/100 BASE-TX and (2) 10/100/1000TX or 100/1000FX combo ports, of gigabit Ethernet data. Unlike most Ethernet switches, these environmentally hardened units are designed for direct deployment in difficult out-of-plant or roadside operating environments, and are available for use with either conventional CAT-5e copper or optical transmission media. Diverse media selection allows for easy implementation of point-to-point, linear add-drop, drop-and-repeat, star, or true self-healing ring and mesh network system architectures. The 16 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. 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 (100/1000 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 CNGE2FE16MS incorporates LED indicators for monitoring the operating status of the managed switch and network. These units are DIN-rail or wall mountable.

## Contents

<b>FCC Warning</b>	<b>3</b>
<b>CE Mark Warning</b>	<b>3</b>
<b>Overview</b>	<b>4</b>
Introduction	4
Features	5
Technical Specifications	6
Packing List	8
Safety Precaution	8
<b>Hardware Description</b>	<b>9</b>
Physical Dimensions	9
LED Indicators	10
<b>Installation</b>	<b>11</b>
RJ-45 Cabling	11
SFP Cabling	15
Grounding the CNGE2FE16MS	17
Wiring the Power Inputs	18
Wiring the P-Fail Alarm Contacts	19
DIN-Rail Mounting	20
Wall Mounting	22
Installation Steps	23
<b>Configuration</b>	<b>24</b>
RS-232 Console	24
Login in the Console Interface	25
<b>SSH</b>	<b>27</b>
Configuring PuTTY	27
Web-Based Management	32
X-Ring2	88
<b>Troubleshooting</b>	<b>105</b>
<b>Appendix A—Command Sets</b>	<b>106</b>
Command Level	106

## 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 the 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.

# Overview

## Introduction

To create the reliability in your network, the CNGE2FE16MS comes equipped with a proprietary redundant network protocol, X-Ring II, which provides users with an easy way to establish a redundant Ethernet network with ultra high-speed recovery time of less than 10ms. Also, the extended MTBF (Mean Time Between Failures) ensures that the CNGE2FE16MS will continue to operate until a Gigabit network infrastructure has been established without requiring any extra upgrade costs.

The CNGE2FE16MS also comes equipped with 2 Gbps (gigabit) Ethernet combo ports; each combo port consists of a copper and a SFP sockets. The combo ports can be used for the application of wideband uploading and especially long distance transmission by connecting the SFP socket to fit the field request flexibility.

## Heavy Duty

Designed with metal housing, the CNGE2FE16MS provides the rugged construction that complies with IP30 standards.

## Dual Power Inputs

The redundant power input design for the CNGE2FE16MS provides a backup power solution. With both the power inputs supplied, if a failure occurs the other supply will be activated to keep the system continually operating. When one of the power inputs fails, the P-Fail LED indicator illuminates and sends an alarm through the relay output as notification.

## Flexible Mounting

The CNGE2FE16MS can be mounted on the wall or on a standard DIN rail, so it is suitable for any space-constrained environment.

## Wide Operating Temperature

The operating temperature range of the CNGE2FE16MS is between -40 and +75°C. With such a wide range, you can deploy the CNGE2FE16MS in some of the harshest industrial environments.

## Easy Troubleshooting

LED indicators make solving any challenges easy. Users can identify the status of the switch by observing the LED indicators with the definition table.

## N-Key Quick Installation

An optional accessory is offered for the CNGE2FE16MS for quick installation especially when you are planning to do routine tasks. Users can simply plug the accessory known as N-Key into the console port for system configuration backup/restoration.

## Features

- » 7.2Gbps back-plane (switching fabric)
- » 2 x 1000Base-T/1000Base-FX Combo ports
- » Wide-range redundant power
- » Power polarity reversal protection
- » X-Ring II path redundant supported
- » TFTP firmware update and system configuration restoration/backup
- » N-Key for configuration restoration/backup (optional)

## Technical Specifications

### Communications

Standard	IEEE 802.3, 802.3u, 802.3x, 802.3ad IEEE 802.1d, 802.1p, 802.1Q, 802.1w, 802.1x
LAN	10/100/1000BaseT, 1000BaseFX
Transmission Speed	Up to 1000 Mbps

### Interface

Ethernet	16 x RJ-45 (10/100TX) 2 x RJ-45/SFP (mini-GBIC) combo ports (1000T/1000FX)
Console	1 x RJ-45 (RS-232)
Power & Relay Alarm Receptacle	1 x 6-plug terminal block
LED Indicators	System: Power1, Power2, P-Fail, R-Master 10/100BaseTX port: Link/Active, Full duplex/Collision 1000T: Link/Active, Speed SFP: Link/Activity

### Management

Configuration	Web browser, serial console, SNMP v1/v2c/v3, Telnet, TFTP, N-Key (optional), IPv6, SNTP
SNMP MIB	RFC 1215 Trap, RFC1213 MIBII, RFC 1157 SNMP MIB, RFC 1493 Bridge MIB, RFC 2674 VLAN MIB, RFC1643 , RFC 1757, RSTP MIB, LLDP MIB, Private MIB
VLAN	IEEE 802.1Q tagged, double-tagged VLAN, GVRP
Redundancy	802.1w/d RSTP/STP X-Ring II (Recovery time < 10ms)
Security	SSL, SSH, DHCP Server with Port-IP binding, IP access security, user authentication, multi-user login, 802.1X port access control
Traffic Control	Port trunking with LACP, rate limit and storm control, IGMP Snooping/Query for multicast group, multicast filtering, IEEE 802.3x flow control, IEEE 802.1p QoS
Diagnostics	Port mirroring, real-time traffic statistics, MAC address table, system event log, E-mail alert, SNMP trap, RMON, LLDP/LLDP-MED, DMI for SFP

## Power

Power Consumption 10.75 watts max.

Power Input 12 ~ 48 VDC

## Mechanical

Dimensions (WxHxD) 72 x 152 x 106.2 mm

Enclosure IP30 protection, aluminum shell

Installation Wall/DIN-rail mounting

## Environment

Operating Temperature -40° ~ 75°C (-40° ~ 167°F)

Operating Humidity 5% ~ 95% (non-condensing)

Storage Temperature -40° ~ 85°C (-40° ~ 185°F)

Storage Humidity 5% ~ 95% (non-condensing)

MTBF 218490 hrs

## Certifications

Safety UL, cUL, CE/EN60950-1; (suitable for use in Class I, Division 2, Groups A, B, C, and D locations)

EMC  
CE, FCC Class A  
CE EN61000-6-2  
CE EN61000-6-4  
CE EN61000-4-2 (ESD)  
CE EN61000-4-3 (RS)  
CE EN61000-4-4 (EFT)  
CE EN61000-4-5 (Surge)  
CE EN61000-4-6 (CS)  
CE EN61000-4-8 (Magnetic Field)

Free Fall IEC60068-2-32

Shock IEC61373

Vibration IEC61373

## Packing List

- » 1 x CNGE2FE16MS
- » 1 x RJ-45 to D-sub 9 female console cable
- » 1 x User Manual (CD-ROM)
- » 1 x Wall-mount kit

Compare the contents of the CNGE2FE16MS with the standard checklist above. If any item is damaged or missing, please contact the local dealer for service.

## Safety Precaution

**Attention**     *If DC voltage is supplied by an external circuit, please use a protection device on the power supply input.*



## Hardware Description

This section is intended to introduce the industrial switch's hardware specification, port, cabling and wiring information.

### Physical Dimensions

Figure 1 illustrates the dimensions 72 × 152 × 106.2mm (W × H × D) for the CNGE2FE16MS.

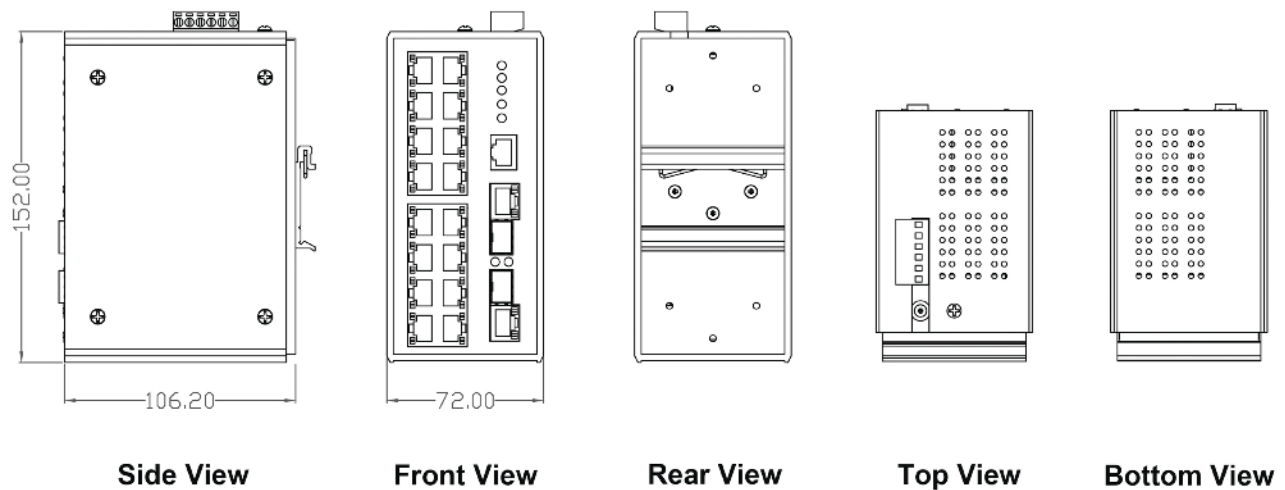


Figure 1 - Mechanical Dimensions

## LED Indicators

LED indicators located on the front panel display the power status and network status of the CNGE2FE16MS. Please Table 1 for further details.

LED	Color	Description	
PWR	Green	On	System power on
		Off	No power inputs
R.M.	Green	On	The switch is the master device of the X-ring group
		Off	Non-master device
PWR1	Green	On	Power input 1 is active
		Off	Power input 1 is inactive
PWR2	Green	On	Power input 2 is active
		Off	Power input 2 is inactive
P-Fail (depends on the Fault Relay Alarm configuration)	Red	On	Power or Ethernet port linking failure occurs
		Off	No failure occurs
P1 ~ P16	Green	On	Connected to network
		Blinking	Data is transmitting or receiving
		Off	Not connected to network
	Amber	On	Full duplex
		Blinking	Collision of packets occurs
		Off	Half duplex or not connected to network
P17, P18 (10/100/1000T)	Green (Upper LED)	On	Connected to network
		Blinking	Data is transmitting or receiving
		Off	Not connected to network
	Green (Lower LED)	On	Operating at speed of 1000M
		Off	Disconnected or operating at speed of 10/100M
P17, P18 (100/1000 SFP)	Green	On	Connected to network
		Blinking	Data is transmitting or receiving
		Off	Not connected to network

Table 1 - Definition of LED indicators

## Installation

### RJ-45 Cabling

Use four twisted-pair, Category 5e or above cabling for the RJ-45 port connection.

The cable between the switch and the link partner (switch, hub, workstation, etc.) must be less than 100 meters (328 feet) long.

The RJ-45 copper ports will auto-sense for 10Base-T, 100Base-TX, or 1000Base-T connections. Auto MDI/MDIX means that the switch can connect to another switch or workstation without changing straight through or crossover cabling.

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-)

Table 2 – 10/100Base-TX Pinouts

**Note** “+” and “-” signs represent the polarity of the wires that make up each wire pair.

## 10/100Base-TX Cable Schema

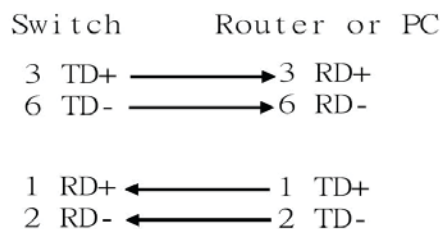


Figure 2 - Straight Through Cable Schematic

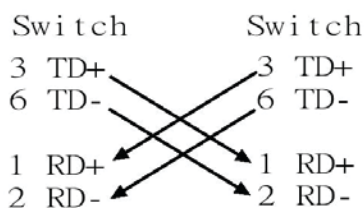


Figure 3 - Cross Over Cable Schematic

## 10/100/1000Base-T Pinouts

Pin	Signal name	Description
1	BI_DA+	Bi-directional pair A+
2	BI_DA-	Bi-directional pair A-
3	BI_DB+	Bi-directional pair B+
4	BI_DC+	Bi-directional pair C+
5	BI_DC-	Bi-directional pair C-
6	BI_DB-	Bi-directional pair B-
7	BI_DD+	Bi-directional pair D+
8	BI_DD-	Bi-directional pair D-

Table 3 - Gigabit Ethernet RJ-45 pinouts

10/100/1000Base-T Cable Schema

The following two figures illustrate the 10/100/1000Base-T cable schema.

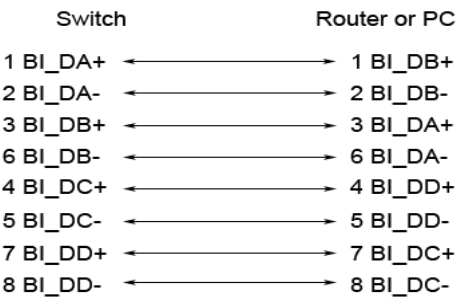


Figure 4 - Straight Through Cable Schema

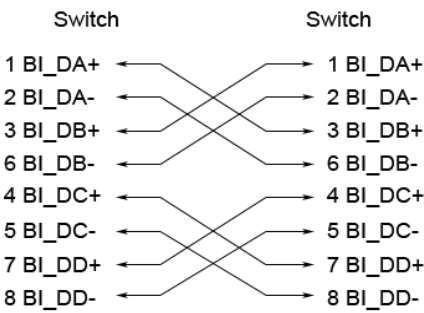


Figure 5 - Crossover Cable Schema

## Gigabit Copper/SFP Combo Port

The CNGE2FE16MS is equipped with Gigabit Copper/SFP combo ports. The Gigabit Copper (10/100/1000T) ports should use Category 5e or above UTP/STP cable for the connection speed up to 1000Mbps. SFP slots supporting dual mode to toggle the connection speed between 100 and 1000Mbps are used for connecting to the network segment with single or multi-mode fiber optics. You can choose the appropriate SFP transceiver to plug into the SFP socket with proper multi-mode or single-mode fiber cable according to that transceiver.

**Note** *The particular SFP/Copper Combo port is deemed to be a single port that either the SFP or Copper port operates; the SFP and Copper ports cannot both operate at the same time.*

*The SFP port has the higher priority than the corresponding copper port; if you insert the **1000M** SFP transceiver (which has connected a fiber cable between that transceiver and the remote node) into the SFP port, the connection of the corresponding copper port will link down.*

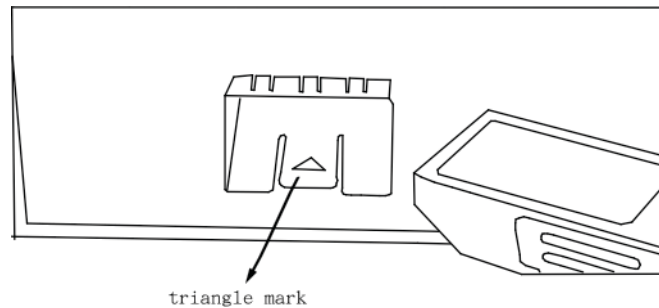
*If you insert the **100M** SFP transceiver into the SFP port even without a fiber cable between that transceiver and the remote node, the connection of the corresponding copper port will link down immediately.*

## SFP Cabling

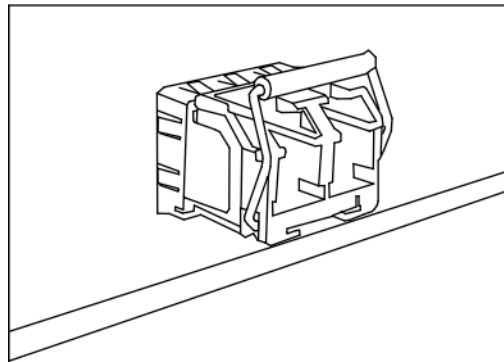
### SFP Connection

To connect the transceiver and the LC cable, please follow the steps shown in Figures 6 – 8.

- » First, insert the transceiver into the SFP slot. Notice that the triangle mark indicates the bottom of the slot.

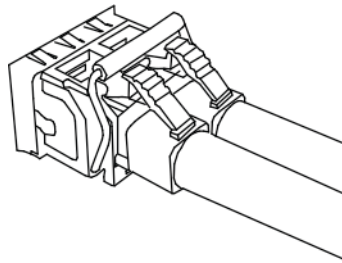


*Figure 6 - Insert transceiver into the SFP slot*



*Figure 7 -Transceiver Inserted*

- » Second, insert LC connector of the fiber cable into the transceiver.



*Figure 8 - LC connector to the transceiver*

## SFP Disconnection

To remove the LC connector from the transceiver, follow the steps shown in Figures 9 and 10.

- » First, press down the latches and pull the LC connector out of the transceiver.

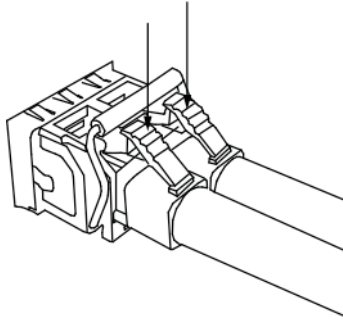


Figure 9 - Press down the latches to remove the LC connector

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

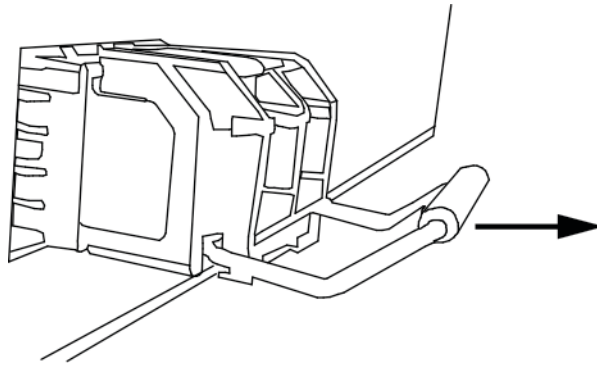


Figure 10 - Pull the transceiver out of the slot



## Grounding the CNGE2FE16MS

Follow the instructions below to attach the CNGE2FE16MS to ground.

**Attention** When installing the CNGE2FE16MS, the ground connection must always be made first and disconnected last.

- » On the top of the CNGE2FE16MS, locate and remove the dome screw that has a ground symbol beside it.
- » Attach the ground wire to the screw hole with the dome screw.

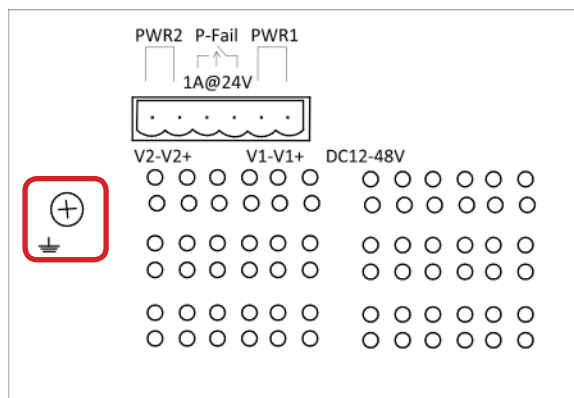


Figure 11 – Top plate of CNGE2FE16MS

## Wiring the Power Inputs

Please follow these steps to connect power lines from the terminal block to the compliant external DC power source.

- » Before wiring, make sure the power source is disconnected.
- » Using a wire-stripping tool, remove a short piece of insulation from the output wires of the DC power source.
- » Identify the positive and negative polarity feed positions for the terminal block connection. See the symbols printed on the panel indicating the polarities and DC input power range in voltage.

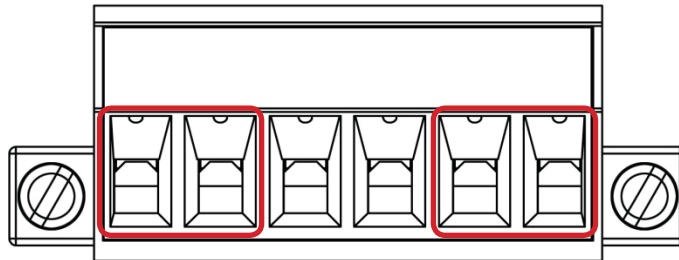


Figure 12 - Plugs for Power 1 & Power 2

- » Insert the exposed wires into the terminal block plugs. Only wires with insulation should extend from the terminal block plugs. Note that the polarities between the wires and the terminal block plugs must be positive-to-positive and negative-to-negative.
- » Use a slotted screwdriver to tighten the captive screws.

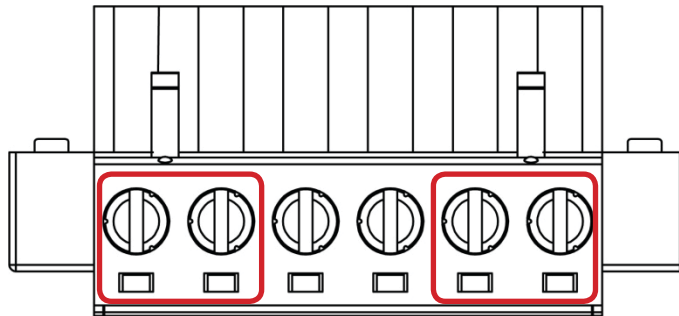


Figure 13 Captive Screws for Fixing Wires

**Attention:** Use Copper Conductors Only, 60/75°C, tightening to 5 lb-in

**The wire gauge for the terminal block should be in the range between 12~ 24 AWG.**

## Wiring the P-Fail Alarm Contacts

The “P-Fail” alarm relay is provided to signal critical error conditions that may occur on the switch. The contacts are energized upon powering up of the switch and remain energized until a critical error occurs including power failure, Ethernet port disconnection and MAC violation. Take the wiring illustration below as an example that illustrates the proper relay connection forming a normally closed circuit, and the connection is to be broken when an error occurs.

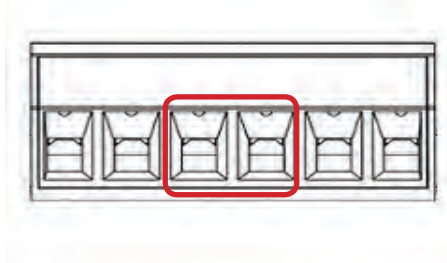


Figure 14 - Terminal Block Plugs for Fault Alarm Contacts

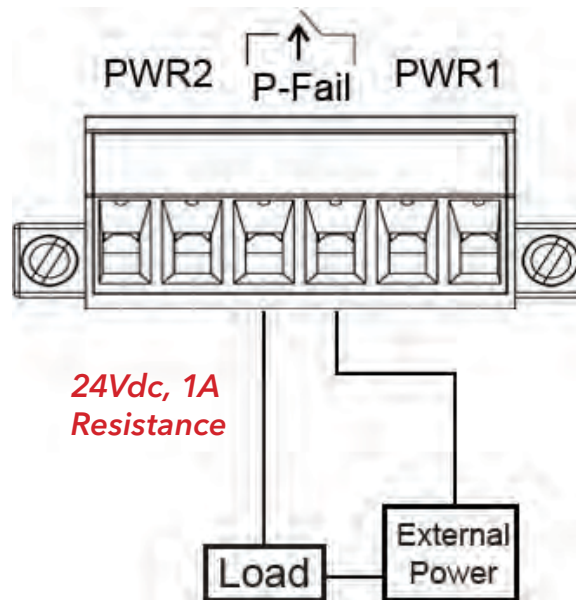


Figure 15 - Fault Alarm Wiring Example

## DIN-Rail Mounting

### Assembling the DIN-Rail Clip

The DIN-rail clip is screwed on the CNGE2FE16MS when out of factory. If not, please refer to the following steps to secure the DIN-rail clip on the switch.

- » Use the included screws to secure the DIN-rail clip on the CNGE2FE16MS.
- » To remove the DIN-rail clip, remove the screws from the clip to separate it from the unit.

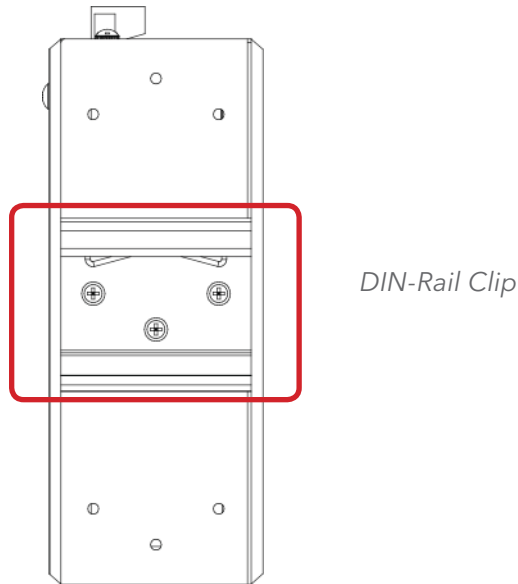
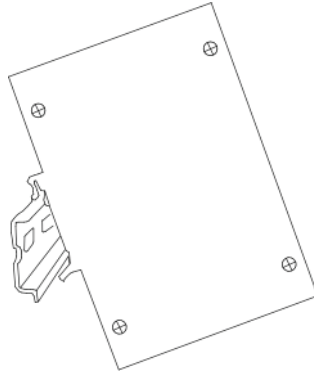


Figure 16 - Rear Side of the Switch

## Hanging the Industrial Switch

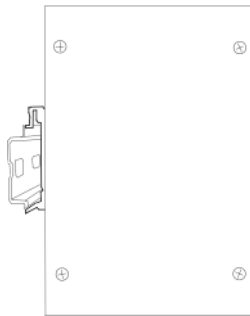
Follow the steps below to hang the CNGE2FE16MS on the DIN rail.

- » First, position the rear side of the switch directly in front of the DIN rail. Make sure the top of the clip hooks over the top of the DIN rail.



*Figure 17 - Positioning DIN-rail clip on the DIN rail*

- » Push the unit downward.



*Figure 18 - Successful installation onto DIN rail*

- » Check the DIN-Rail clip is tightly affixed on the DIN rail.
- » To remove the CNGE2FE16MS from the track, reverse the steps above.

## Wall Mounting

To hang the Ethernet switch on the wall, please follow the steps below.

- » Remove the DIN-rail clip.
- » Prepare the two wall-mount plates and six screws (included).
- » Align the screw holes between the wall-mount plates and the unit as the figure illustrated.
- » Secure the plates to the unit with the accompanying screws.

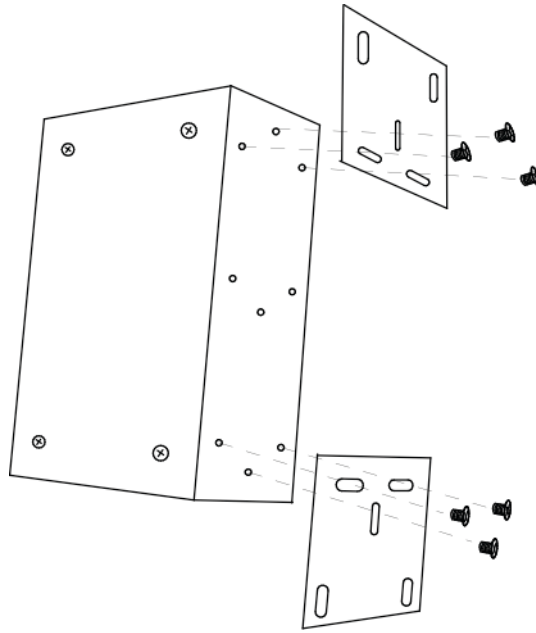


Figure 19 – Alignment of CNGE2FE16MS and Wall Mounting Hardware

## Installation Steps

- » Unpack the CNGE2FE16MS.
- » To hang the CNGE2FE16MS on the wall, please refer to the Wall Mounting section.
- » Ground the CNGE2FE16MS.
- » To power on the CNGE2FE16MS, please refer to the Wiring the Power Inputs section for further information on how to wire the power. And then the power LED on the CNGE2FE16MS will light up. Please refer to the LED Indicators section for indication of LED lights.
- » Prepare the appropriate cables for the Ethernet connection.
- » The Ethernet port LED on the CNGE2FE16MS will light up when the cable is connected with the network device. Please refer to the LED Indicators section for LED light indication.
- » When all connections are set and LED lights all show in normal, the installation is complete.

**Note** *This equipment is intended for use in a Pollution Degree 2 industrial environment.*

# Configuration

The CNGE2FE16MS can be configured via RS-232 Console, SSH (Secure Shell) or a web browser.

## RS-232 Console

Attach the supplied cable, which one end is D-sub 9 and the other end is RJ-45, to connect the CNGE2FE16MS and your host PC or terminal. The connected PC or terminal must support the terminal emulation program.

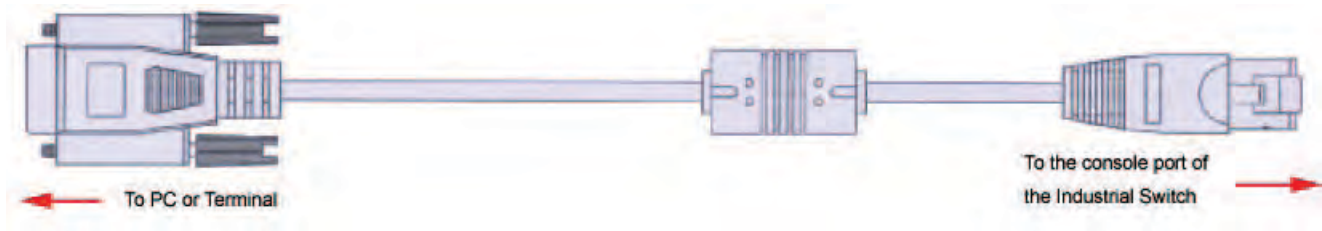


Figure 20 - Connection Cable

## Pin Assignments

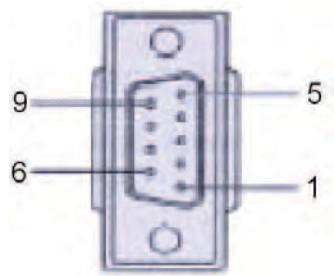


Figure 21 - DB 9-pin Female

D-sub 9 Connector	RJ-45 Connector
NC	1 Orange/White
2	2 Orange
3	3 Green/White
NC	4 Blue
5	5 Blue/White
NC	6 Green
NC	7 Brown/White
NC	8 Brown

Table 4 - Pin Assignments



## Login in the Console Interface

After the connection between Switch and PC is ready, turn on the PC and run a terminal emulation program like 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**

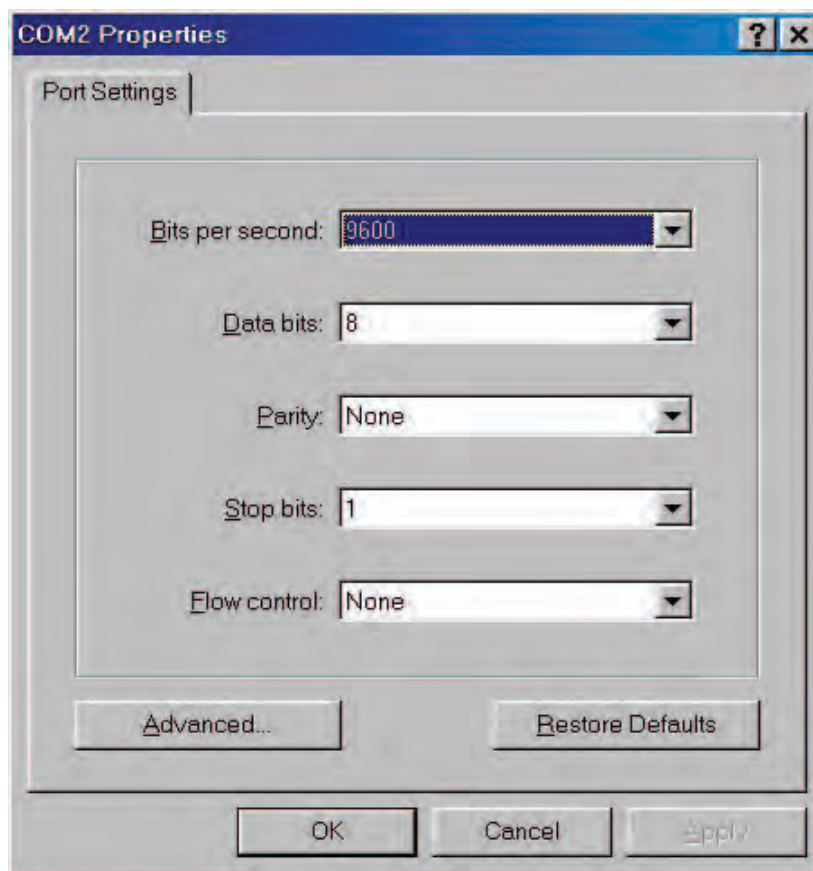
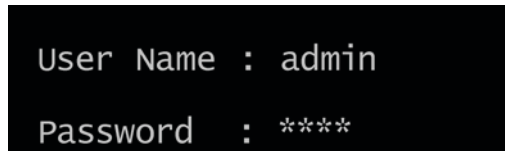


Figure 22 – Communication Parameters

- » Having selected the parameter settings, click **OK**.

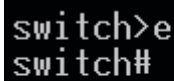
- » When the blank screen shows up, press Enter to have the login prompt appear. Key in **admin** (default value) for both User Name and Password (press **Enter** to switch between); and then press **Enter** to reach the Main Menu of console management.

A screenshot of a console login interface. It shows two lines of text: "User Name : admin" and "Password : \*\*\*\*". The text is white on a black background.

```
User Name : admin
Password  : ****
```

*Figure 23 - Console login interface*

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

A screenshot of a CLI command interface. It shows two lines of text: "switch>e" and "switch#". The text is white on a black background.

```
switch>e
switch#
```

*Figure 24 - CLI command interface*

For further details about the CLI commands, please refer to Appendix A Command Sets.

## SSH

The Ethernet switch also supports SSH (Secure Shell) which allows the user to log in from a remote computer over the network.

The next section is intended to guide users on how to use an SSH client–PuTTY to make a connection to the Ethernet switch.

### Configuring PuTTY

Launch **PuTTY**, and you will see a dialog box that allows you to control everything PuTTY can do. You do not usually need to change most of the configuration options. To start the simplest kind of session, please follow the steps below.

- » In the **Host Name (or IP address)** field, enter the Internet host name or IP address of the server you want to connect to.
- » Now select a login session protocol to use, from the **Connection type** radio buttons. For a login session, you should always select SSH.

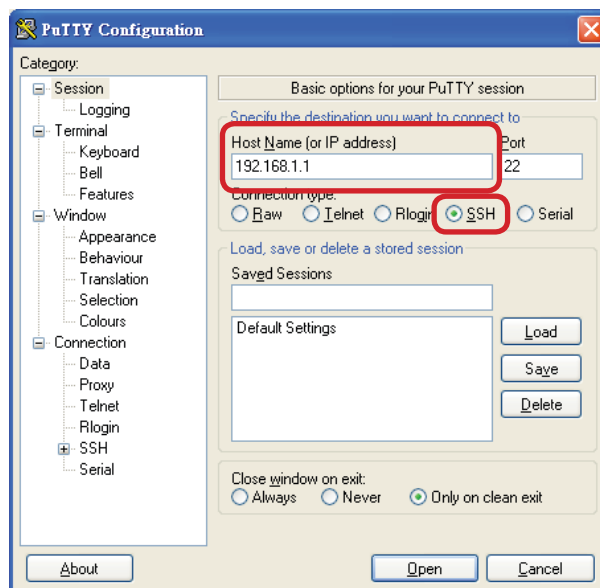


Figure 25 - Basic Options for PuTTY

- » Select the **Connection**→**SSH** node of the tree-menu to configure options for controlling SSH connections.
- » Tick the check box labeled **Don't start a shell or command at all**.

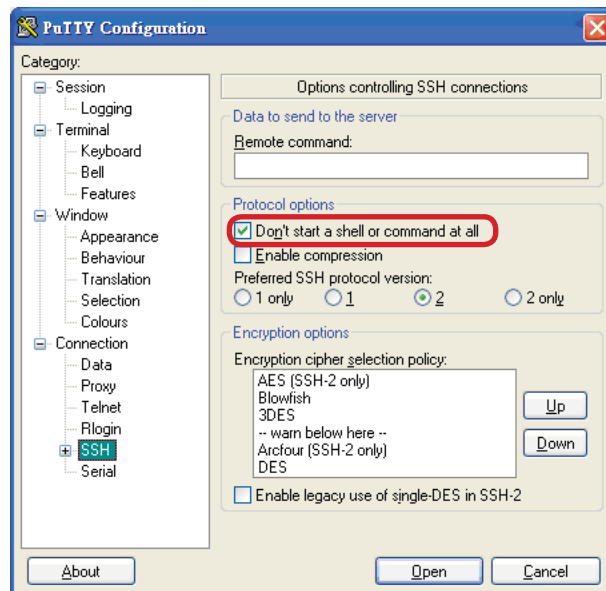


Figure 26 - Options Controlling SSH Connections

- » Select the **Connection**→**SSH**→**Tunnel** node of the tree-menu to configure options for controlling SSH port forwarding.
- » Tick the check box labeled **Local ports accept connection from other hosts** that allows you to set up local-to-remote port forwards (including dynamic port forwards) in such a way that machines other than your client PC can connect to the forwarded port.
- » Add a new forwarded port to connect to the SSH server and set the type to **Local**.

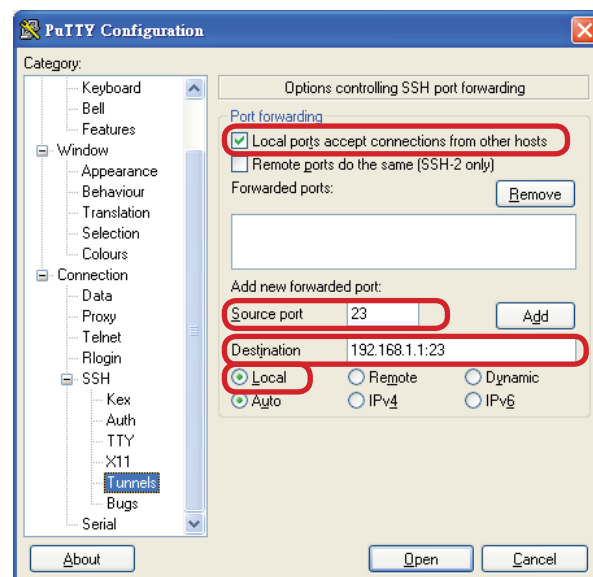


Figure 27 - Options Controlling SSH Port Forwarding

- » After filling in, select the **Add** button. And you will see an entry added to the list box.

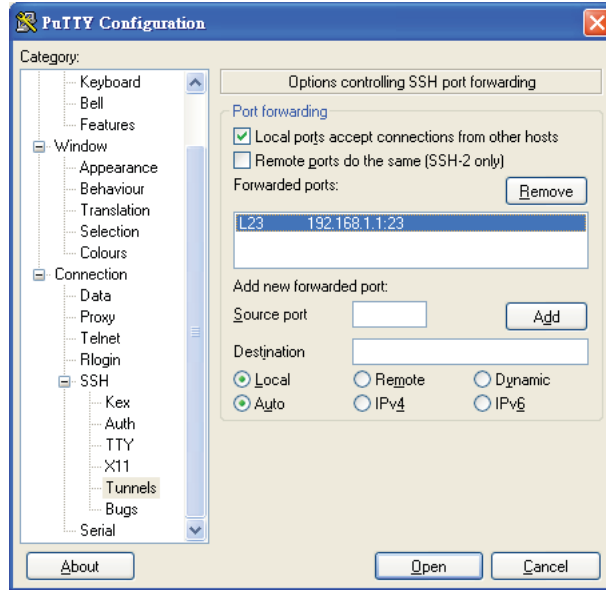


Figure 28 - Entry of Port Forwarding Added

- » You can also save your preferred PuTTY options for a quick connection the next time it is needed. Just go back to the Session node, and select the **Save** button with a session name filled in. When you see the saved session in the list box, the session is saved.

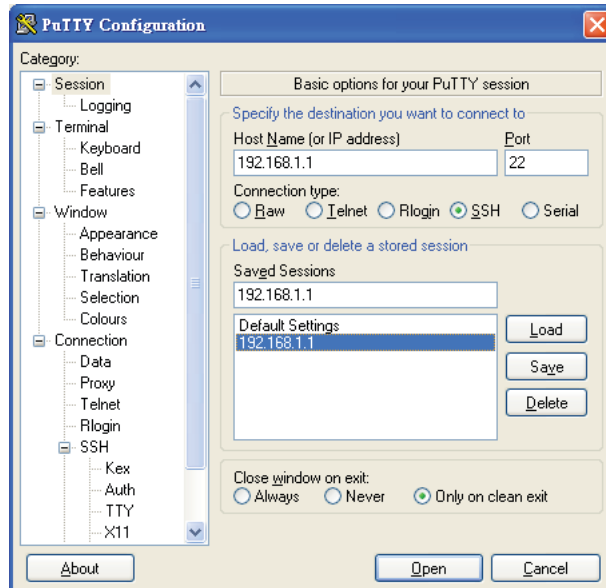


Figure 29 - Saving Sessions

- » To connect to the SSH server, select the session name and select the **Open** button. And then you will see a window shows up with prompt message **login as:** Type **guest** for both user name and password.

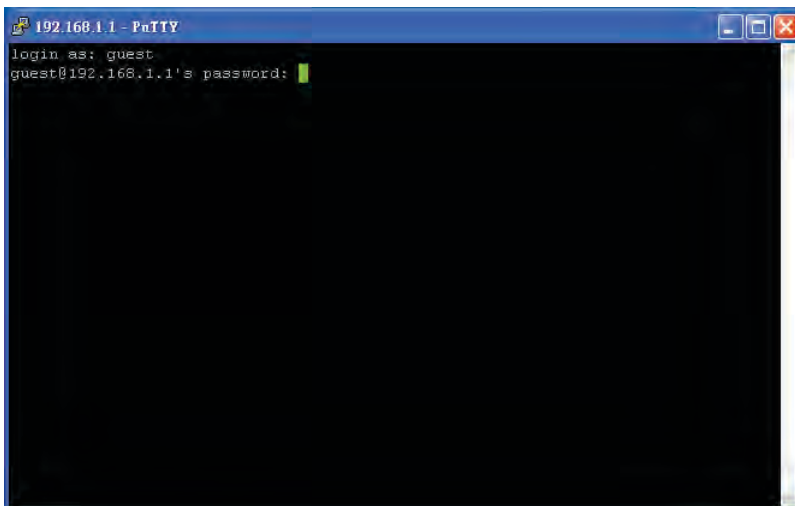


Figure 30 - Logging-in interface

- » Run the **cmd** command to start the command prompt interface. Type **telnet localhost 23** and press **Enter**.

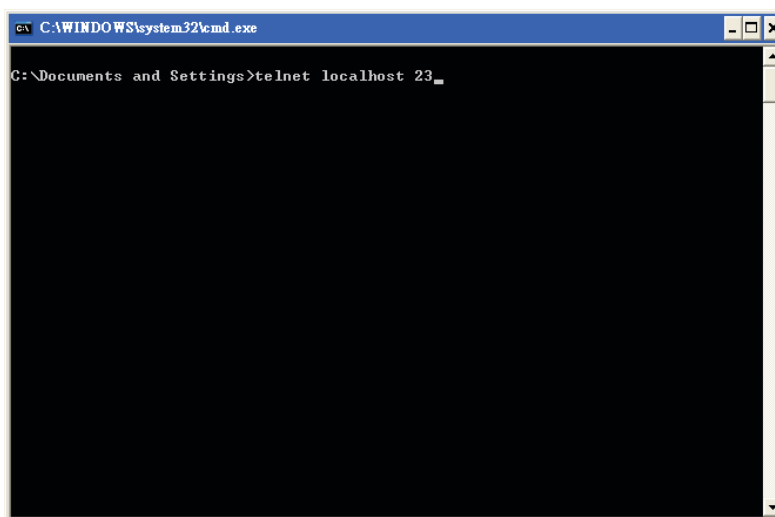
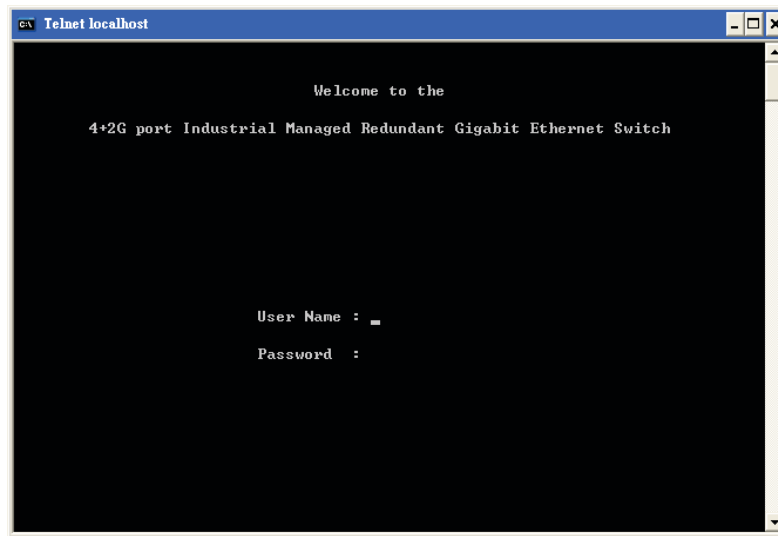


Figure 31 - Command Prompt interface

» When finished, a telnet session is successfully made using the SSH protocol.



*Figure 32 – Console via SSH*

## Web-Based Management

This CNGE2FE16MS provides a convenient configuration method via web browser. You can follow the steps below to access the equipment.

**Note** *Your host PC should be in the same VLAN setting with the CNGE2FE16MS, or the management will not be configured.*

Connect the CNGE2FE16MS to the Ethernet network and your host PC can configure the switch over the network. Or you can directly connect it to your host PC with a straight-through or crossover Ethernet cable.

Before using web management, install the CNGE2FE16MS on the network and make sure that any one of the PCs on the network can connect with the CNGE2FE16MS through the web browser. The CNGE2FE16MS default values for IP, subnet mask, username and password are 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**

**Note** *Do not set "0" for the first segment of the subnet mask and default gateway (000.xxx.xxx.xxx).  
Refresh the web screen if the web could not be displayed while you change the setting.*

- » Launch Internet Explorer on the PC.
- » Type the IP address of the switch in the Address Bar, and then Press **Enter**.

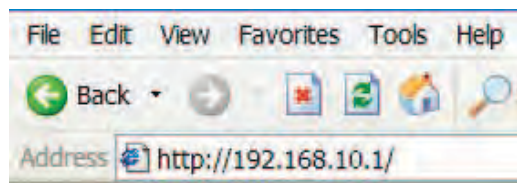


Figure 33 - Web Address Bar of Browser



- » When the login dialog box appears, type the user name and password in the respective fields. The default user name and password are the same: **admin**
- » Press **Enter** or select the **OK** button, and then the home screen of the web-based management will appear. You can change user name/password in the **User Authentication** section.

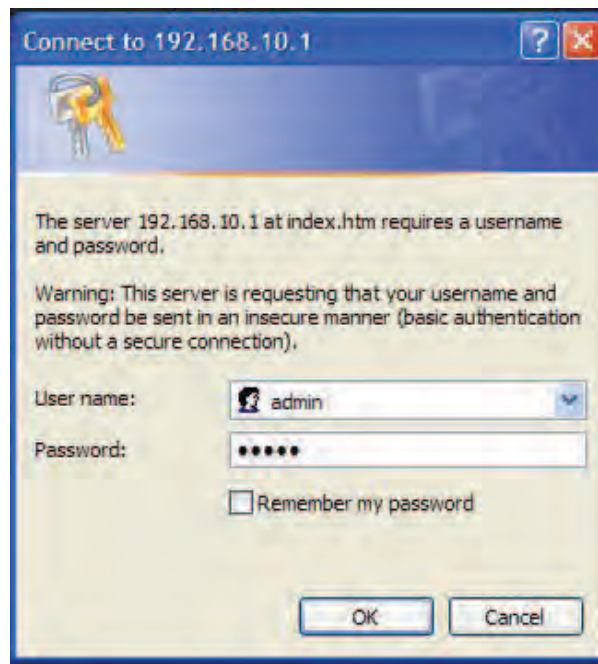


Figure 34 - Login dialog box

## SSL

The CNGE2FE16MS also provides an option for you to connect with your browser via HTTP over SSL, called HTTPS. The SSL (Secure Socket Layer) protocol allows users to make a secured session between the browser (client) and the Ethernet switch (server).

You can type the prefix **https://** followed by the IP address of the Ethernet switch in the address bar of the browser. A closed padlock icon will appear next to the address bar, indicating that the client is successfully connecting to the server via HTTPS.

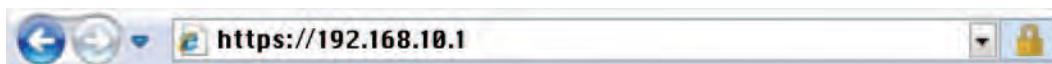


Figure 35 - Secure Connection

On the left side of the main page, you can find the tree menu structure of the Ethernet switch. Select the "+" symbol to expand a category, and select any one of the hyperlinks to open its function page.

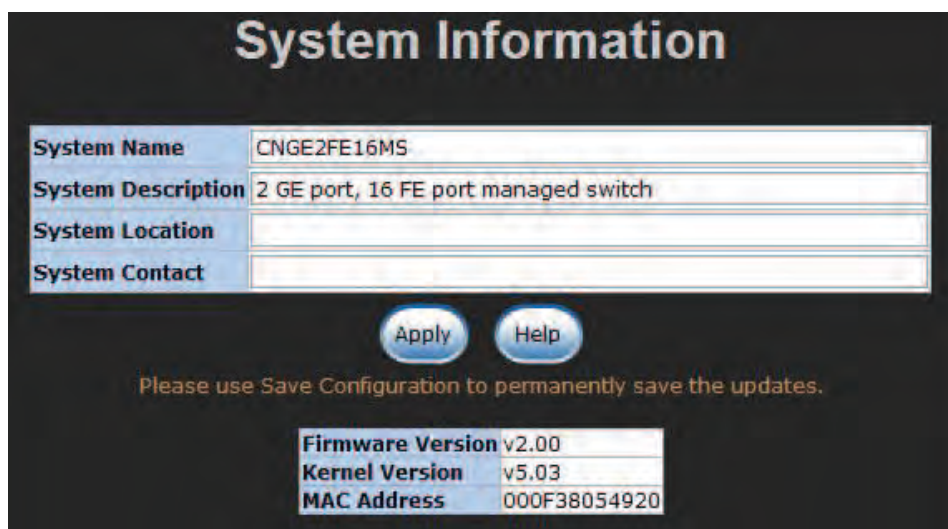


Figure 36 – Web Based Management Home Screen

## System Information

Here you can view the system information and assign the system name and location to make this switch more easily identified on your network.

- » **System Name:** Assign the name of the switch. The maximum length is 64 bytes.
- » **System Description:** A read-only field displaying the description of the switch.
- » **System Location:** Assign the switch physical location. The maximum length is 64 bytes.
- » **System Contact:** Enter the name of contact person or department.
- » **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).
- » Select **Apply** to have the any configuration changes take effect.



The screenshot displays the 'System Information' web interface. It features a dark background with a title bar at the top. Below the title, there are four input fields for configuration: 'System Name' (containing 'CNGE2FE16MS'), 'System Description' (containing '2 GE port, 16 FE port managed switch'), 'System Location' (empty), and 'System Contact' (empty). Below these fields are two blue buttons labeled 'Apply' and 'Help'. A message in orange text states: 'Please use Save Configuration to permanently save the updates.' At the bottom, a table displays read-only information: Firmware Version v2.00, Kernel Version v5.03, and MAC Address 000F38054920.

System Name	CNGE2FE16MS
System Description	2 GE port, 16 FE port managed switch
System Location	
System Contact	

Apply Help

Please use Save Configuration to permanently save the updates.

Firmware Version	v2.00
Kernel Version	v5.03
MAC Address	000F38054920

Figure 37- System Information interface

## IP Configuration

Due to the foreseeable address exhaustion of IPv4, the IP configuration of the Ethernet switch is designed to provide an interface for users to configure the switch running both IPv4 and IPv6 architecture.

### IPv4

The IPv4 tab allows users to configure the switch to receive an IP address from DHCP server or manually fill in **IP Address, Subnet Mask, Gateway** and IP addresses of the primary and the secondary **DNS servers**.

- » **DHCP Client:** Enable or disable the DHCP client function. When the DHCP Client function is enabled, the CNGE2FE16MS will be assigned an IP address from the network DHCP server. The default IP address will be replaced by the assigned IP address on DHCP server. After users select **Apply**, a popup dialog informs the user that when the DHCP client is enabled, the current IP will be lost and the user should find the new IP on the DHCP server
- » **IP Address:** Assign the IP address for the CNGE2FE16MS. With the DHCP Client function enabled, the switch is configured as a DHCP client and users don't need to assign the IP address that is assigned by the DHCP server. The default IP is 192.168.10.1 or the user has to assign an IP address manually when DHCP Client is disabled.
- » **Subnet Mask:** Assign the subnet mask to the IP address. If the DHCP Client function is disabled, the user has to assign the subnet mask manually.
- » **Gateway:** Assign the network gateway for the switch. If the DHCP Client function is disabled, the user has to assign the gateway manually. The default gateway is 192.168.10.254.
- » **DNS1:** The Domain Name Server (DNS) translates domain names into IP addresses. The domain name is in alphabetic order, which is easy to remember. The Internet is based on IP addresses. Therefore, every time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.net.com might translate to 192.168.10.1.
- » **DNS2:** The backup for DNS1. When DNS1 cannot function, DNS2 will then replace DNS1.
- » When finished, select **Apply** to have the configuration take effect.

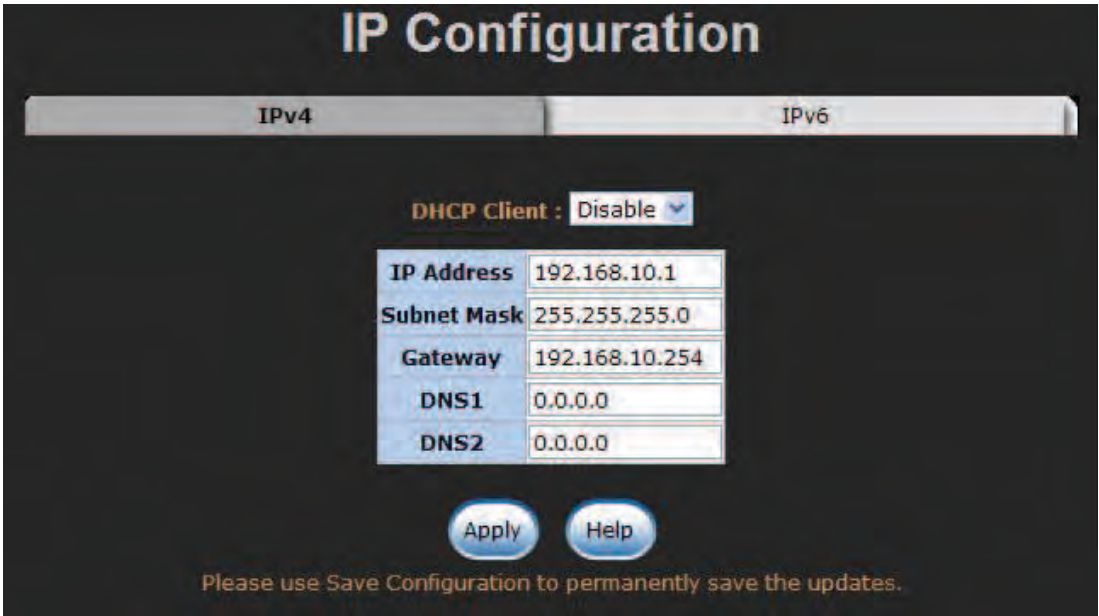


Figure 38 - IP configuration–IPv4

## IPv6

The IPv6 tab mainly features two fields displaying the Ethernet switch's **Global Unicast Address** and **Link-Local Address**.

- » **Global Unicast Address:** A read-only field. When the CNGE2FE16MS switch is connected to a network segment with one or more routers connected, the switch will be assigned an address known as Global Unicast Address by the router(s). Being assigned the Global Unicast Address, the CNGE2FE16MS can then have access to different network segments.
- » **Link-Local Address:** A read-only field. Link-Local Address is for use during auto-configuration and when no any router presents. Being assigned the Link-Local Address, the Ethernet switch can have access to all hosts on the same local segment to where it belongs.

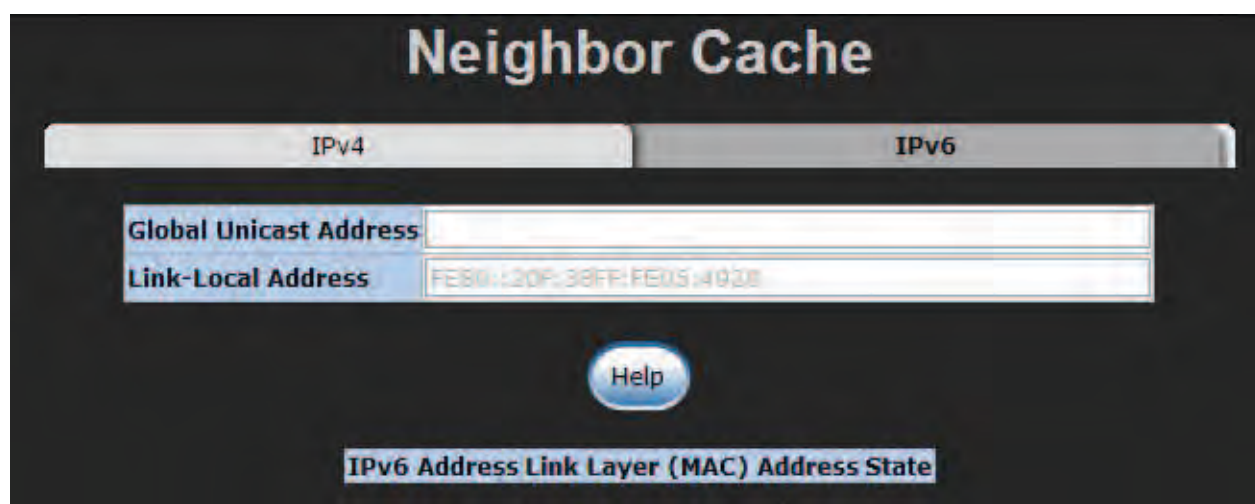


Figure 39 - IP configuration—IPv6



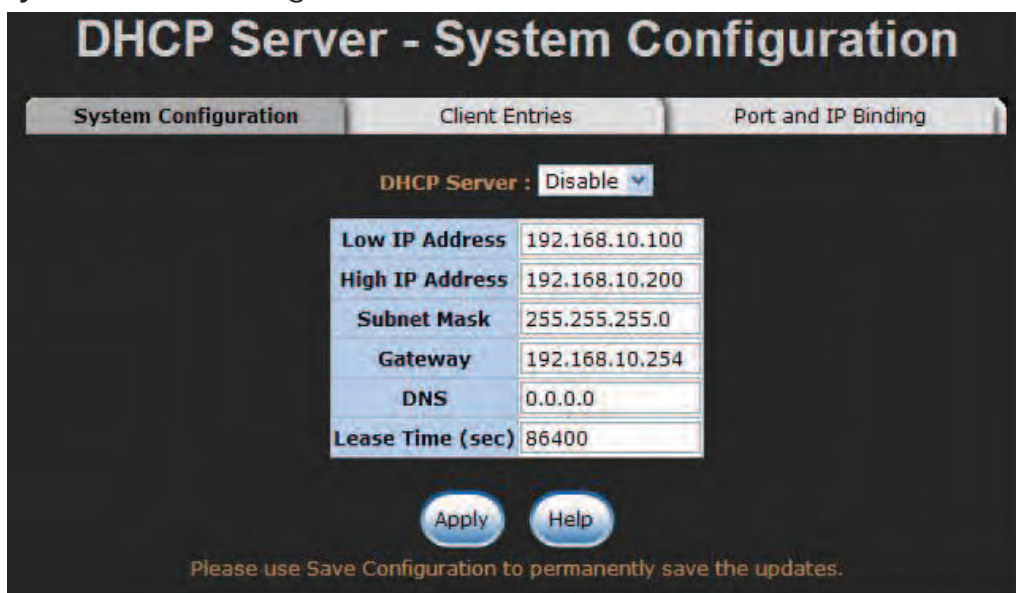
## DHCP Server

Dynamic Host Configuration Protocol (DHCP) is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device 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 requires an administrator to manage the task. This means that a new computer can be easily added to a network without the hassle of manually assigning it a unique IP address.

The system provides the DHCP server function. With the DHCP server function enabled, the switch can be configured as a DHCP server.

## System Configuration

- » **DHCP Server:** This pull-down menu allows you to configure the switch to be the DHCP server on your local network.
- » **Low IP Address:** Type in an IP address as the beginning of a range of the dynamic IP address. In Figure 40, for example, 192.168.10.100 is the relatively low IP address of the range.
- » **High IP Address:** Type in an IP address as the beginning of a range of the dynamic IP address. In Figure 40, for example, 192.168.10.200 is the relatively high IP address of the range.
- » **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 IP address of Domain Name Server in your network.
- » **Lease Time (sec):** The length of time the dynamic IP addresses assigned to clients.
- » Select **Apply** to have the configuration take effect.



DHCP Server - System Configuration	
System Configuration   Client Entries   Port and IP Binding	
DHCP Server : Disable ▼	
Low IP Address	192.168.10.100
High IP Address	192.168.10.200
Subnet Mask	255.255.255.0
Gateway	192.168.10.254
DNS	0.0.0.0
Lease Time (sec)	86400
<div>Apply   Help</div>	
Please use Save Configuration to permanently save the updates.	

Figure 40 - DHCP Server–System Configuration interface

## Client Entries

When the **DHCP Server** function is enabled, the system will collect the DHCP client information including the assigned IP address, the MAC address of the client device, the IP assigning type, states and lease time.

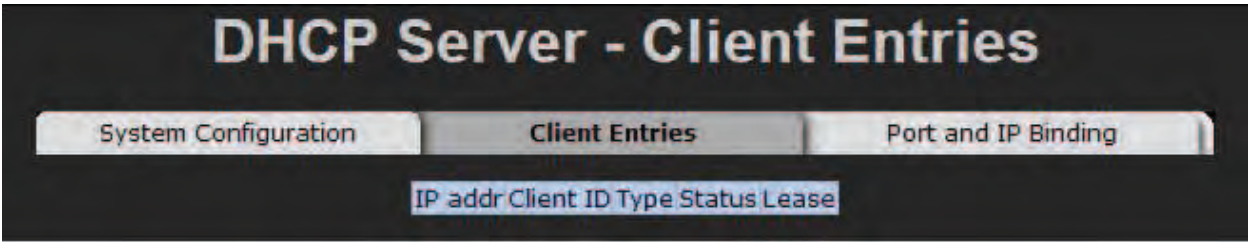
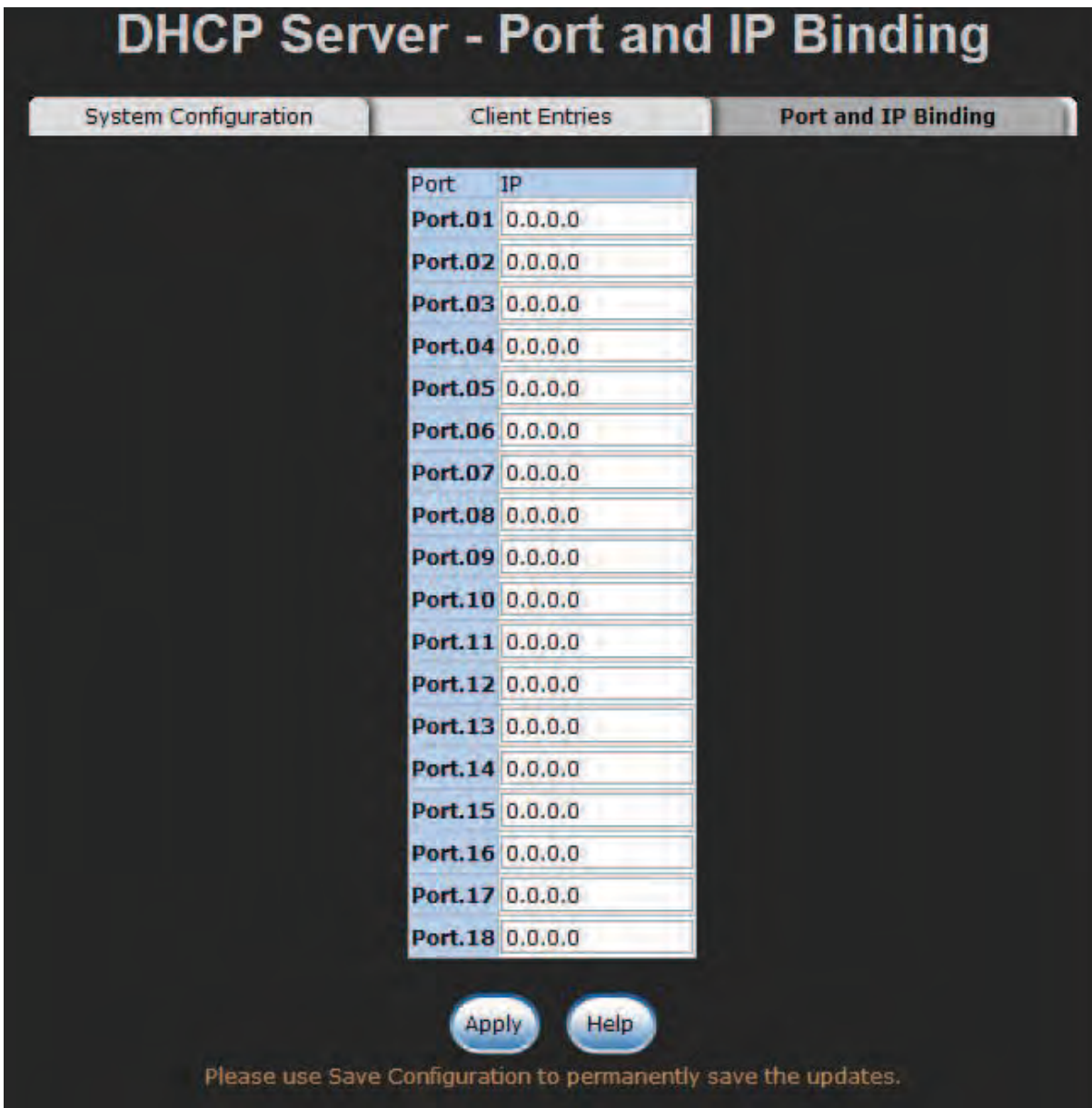


Figure 41 - DHCP Client Entries interface



## Port and IP Bindings

As shown in Figure 42, the switch will assign the IP address to the connected client according to the Port-IP binding table. The user is allowed to fill each port with one particular IP address. When the device connects to the port and asks for an IP assignment, the system will assign the IP address bound with the port to the device.



Port	IP
Port.01	0.0.0.0
Port.02	0.0.0.0
Port.03	0.0.0.0
Port.04	0.0.0.0
Port.05	0.0.0.0
Port.06	0.0.0.0
Port.07	0.0.0.0
Port.08	0.0.0.0
Port.09	0.0.0.0
Port.10	0.0.0.0
Port.11	0.0.0.0
Port.12	0.0.0.0
Port.13	0.0.0.0
Port.14	0.0.0.0
Port.15	0.0.0.0
Port.16	0.0.0.0
Port.17	0.0.0.0
Port.18	0.0.0.0

Apply Help

Please use Save Configuration to permanently save the updates.

Figure 42 - Port and IP Bindings interface

## TFTP

The Trivial File Transfer Protocol (TFTP) server allows the 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.

### Update Firmware

- » **TFTP Server IP Address:** Type in the IP address of the TFTP server.
- » **Firmware File Name:** Type in the name of the firmware image file to be updated.
- » When finished, select **Apply** to start updating.

Figure 43 - Update Firmware interface

## Restore Configuration

You can restore a previous backup configuration from the TFTP server to recover the settings. Before doing that, you must locate the image file on the TFTP server first for the switch to download back the flash image.

- » **TFTP Server IP Address:** Type in the IP address of the TFTP server.
- » **Restore File Name:** Type in the correct file name for restoring.
- » When finished, select **Apply** to start configuration restoration.

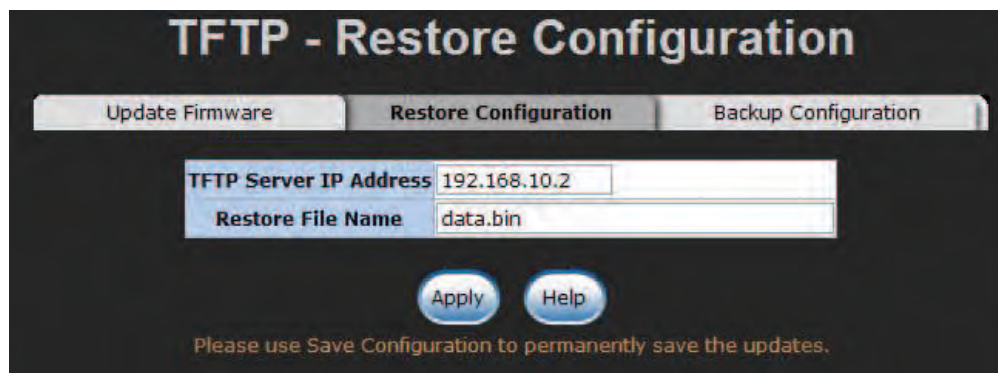
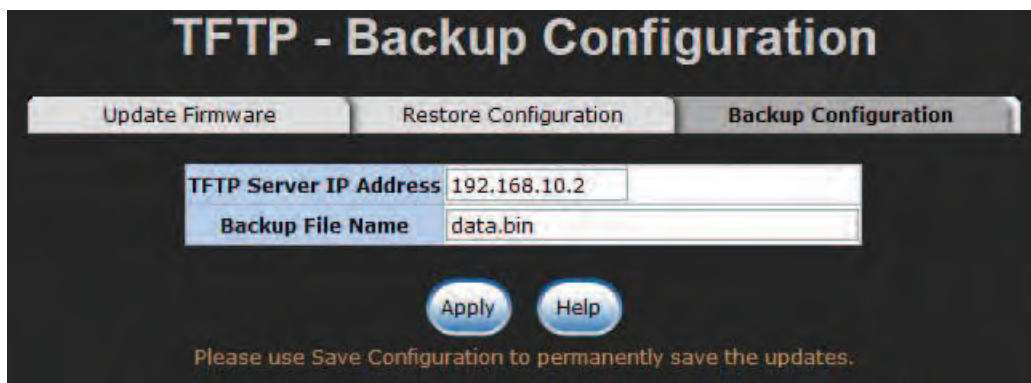


Figure 44 - Restore Configuration interface

## Backup Configuration

You can back up the current configuration from flash ROM to the TFTP server for the purpose of recovering the configuration at another time. It helps avoid wasted time spent configuring the settings by backing up the entire configuration.

- » **TFTP Server IP Address:** Type in the IP address of the TFTP server.
- » **Backup File Name:** Type in the file name.
- » When finished, select **Apply** to start backing up.



**TFTP - Backup Configuration**

Update Firmware   Restore Configuration   **Backup Configuration**

TFTP Server IP Address: 192.168.10.2

Backup File Name: data.bin

Apply   Help

Please use Save Configuration to permanently save the updates.

Figure 45 – Backup Configuration interface

## System Event Log

This feature allows the user to decide whether to send the system event log, and to select the mode which the system event log will be sent to: client only, server only, or both client and server. What kind of event log will be issued to the client/server depends on the selection on the **Event Configuration** tab.

### System Event Log–Syslog Configuration

- » **Syslog Client Mode:** Select the system log mode—**Client Only**, **Server Only**, or **Both**.  
**Client Only** means the system event log will only be sent to this interface of the switch, but on the other hand **Server Only** means the system log will only be sent to the remote system log server with its IP assigned. If the mode is set in **Both**, the system event log will be sent to the remote server and this interface.
- » **Syslog Server IP Address:** When the **Syslog Mode** item is set as Server Only/Both, the user is required to assign the system log server IP address to which the log will be sent.
- » Select **Reload** to refresh the event log displaying area.
- » Select **Clear** to clear the displaying area.
- » Make sure the selected mode and IP address, if needed, is correct and select **Apply** to have the setting take effect.

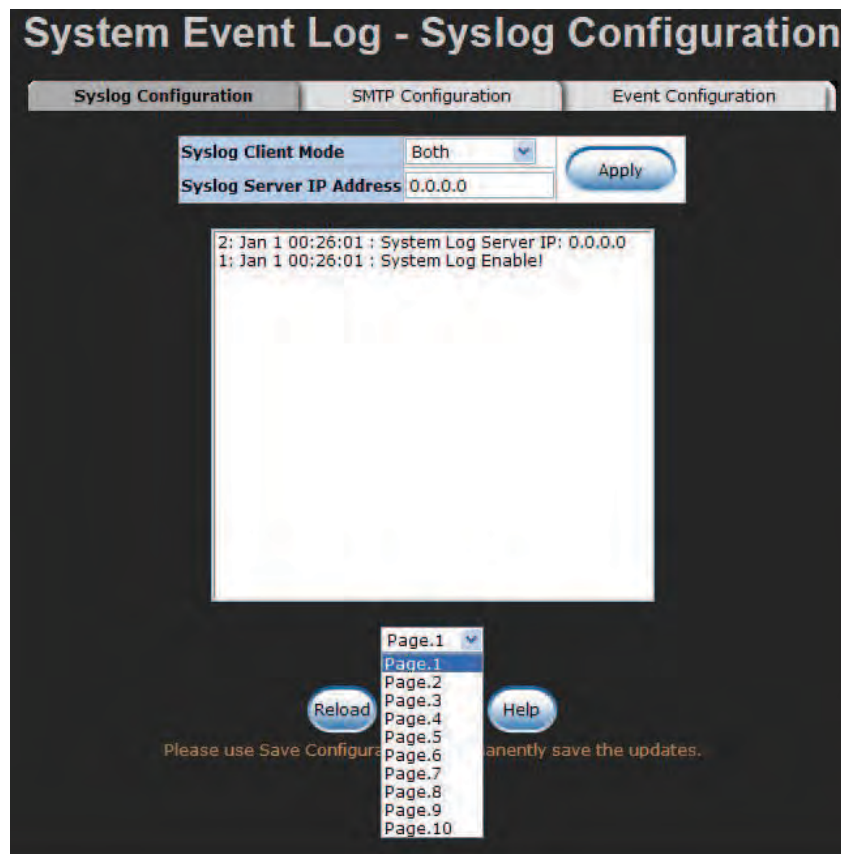
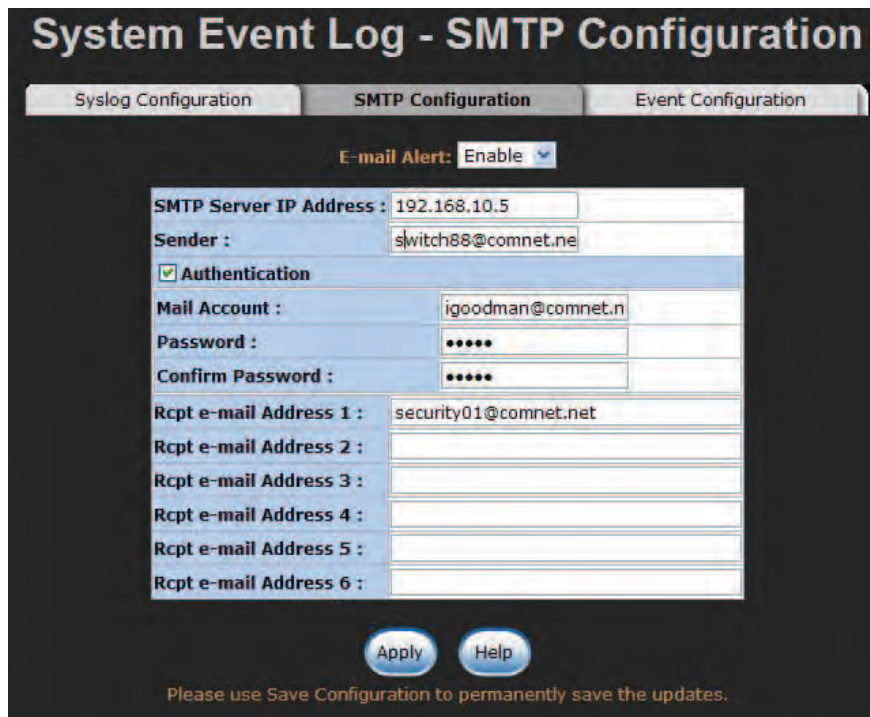


Figure 46 – Syslog Configuration interface

## System Event Log–SMTP Configuration

Simple Mail Transfer Protocol (SMTP) is the standard for email transmissions across the network. You can configure the SMTP server IP address, sender mail account, password, and the recipient email account to which the e-mail alert will send. This page provides the authentication mechanism including the authentication steps through which the client effectively logs in to the SMTP server during the process of sending email alert.

- » **Email Alert:** With this function enabled, the user is allowed to configure the detail settings for sending the e-mail alert to the SMTP server when the events occur.
- » **SMTP Server IP Address:** Assign the mail server IP address (when **Email Alert** is enabled, this field will then be available).
- » **Sender:** Type in an alias of the switch in **complete** email address format, e.g. switch88@comnet.net, to identify where the e-mail alert comes from.
- » **Authentication:** Select the checkbox to have the mail account, password and confirm password fields show up. Configure the email account and password for authentication procedures when this switch logs in to the SMTP server.
- » **Mail Account:** Specify the email, e.g. igoodman@comnet.net, to receive the email alert. It must be an existing email account on the mail server.
- » **Password:** Type in the password for the email account entered for **Mail Account**.
- » **Confirm Password:** Enter the password again.
- » **Rcpt e-mail Address 1 ~ 6:** You can specify up to 6 e-mail accounts to receive the email alert.
- » Select **Apply** to have the configuration take effect.



**System Event Log - SMTP Configuration**

Syslog Configuration    **SMTP Configuration**    Event Configuration

E-mail Alert: Enable

SMTP Server IP Address : 192.168.10.5

Sender : switch88@comnet.net

☒ Authentication

Mail Account : igoodman@comnet.net

Password : .....

Confirm Password : .....

Rcpt e-mail Address 1 : security01@comnet.net

Rcpt e-mail Address 2 :

Rcpt e-mail Address 3 :

Rcpt e-mail Address 4 :

Rcpt e-mail Address 5 :

Rcpt e-mail Address 6 :

Apply    Help

Please use Save Configuration to permanently save the updates.

Figure 47 - SMTP Configuration interface



## System Event Log–Event Configuration

The checkboxes and pull-down menus are not available unless the **Syslog Client Mode** on the Syslog Configuration tab and the **E-mail Alert** on the SMTP Configuration tab are enabled first.

This tab mainly controls whether an event notification is to be sent to the **Syslog/SMTP** server. The section labeled **System Event Selection** controls the event notification including Device Cold Start, Authentication Failure, and MAC Violation. With the **Syslog/SMTP** checkbox selected, the event log/email alert will be sent to the system log server/SMTP server respectively. The section labeled **Port Event Selection** sets the trigger conditions for each port, triggering port events (link up, link down, and both) to be sent to the system log server/SMTP server.

### System event selection

There are three event types–Device Cold Start, Authentication Failure, and MAC Violation.

- » **Device Cold Start:** Check the Syslog/SMTP checkboxes respectively to have the system issue the event log/email alert to the system log/SMTP server when the device executes the cold start action.
- » **Authentication Failure:** When the SNMP authentication fails, the system will issue the event log/email alert to the system log/SMTP server respectively.
- » **MAC Address Violation:** If a device whose MAC address is not in the MAC address table attempts to access the port, the system will issue the event log/email alert to the system log/SMTP server respectively. (Note that the **Security** property of the **Port Control** function also has to be set at **On**. See the **Port Control** section for further details.)

### Port event selection

Each drop-down menu has four options–**Disable**, **Link UP**, **Link Down**, and **Link UP & Link Down**.

- » **Disable** means no event will be sent to the system log/SMTP server.
- » **Link UP:** The system will issue a log message only when the link-up event of the port occurs.
- » **Link Down:** The system will issue a log message only when the link-down event of port occurs.
- » **Link UP & Link Down:** The system will issue a log message at the time when port connection is link-up and link-down.

## System Event Log - Event Configuration

Syslog Configuration
SMTP Configuration
Event Configuration

### System event selection

Event Type	Syslog	SMTP
Device cold start	<input type="checkbox"/>	<input type="checkbox"/>
Authentication Failure	<input type="checkbox"/>	<input type="checkbox"/>
MAC Violation	<input type="checkbox"/>	<input type="checkbox"/>

### Port event selection

Port	Syslog	SMTP
Port.01	Disable <span style="float: right;">▼</span>	Disable <span style="float: right;">▶</span>
Port.02	Disable <span style="float: right;">▼</span>	Disable <span style="float: right;">▶</span>
Port.03	Link Up Link Down Link Up & Link Down <span style="float: right;">▼</span>	Disable <span style="float: right;">▶</span>
Port.04	Disable <span style="float: right;">▼</span>	Disable <span style="float: right;">▶</span>
Port.05	Disable <span style="float: right;">▼</span>	Disable <span style="float: right;">▶</span>
Port.06	Disable <span style="float: right;">▼</span>	Disable <span style="float: right;">▶</span>
Port.07	Disable <span style="float: right;">▼</span>	Disable <span style="float: right;">▶</span>
Port.08	Disable <span style="float: right;">▼</span>	Disable <span style="float: right;">▶</span>
Port.09	Disable <span style="float: right;">▼</span>	Disable <span style="float: right;">▶</span>
Port.10	Disable <span style="float: right;">▼</span>	Disable <span style="float: right;">▶</span>
Port.11	Disable <span style="float: right;">▼</span>	Disable <span style="float: right;">▶</span>
Port.12	Disable <span style="float: right;">▼</span>	Disable <span style="float: right;">▶</span>
Port.13	Disable <span style="float: right;">▼</span>	Disable <span style="float: right;">▶</span>
Port.14	Disable <span style="float: right;">▼</span>	Disable <span style="float: right;">▶</span>
Port.15	Disable <span style="float: right;">▼</span>	Disable <span style="float: right;">▶</span>
Port.16	Disable <span style="float: right;">▼</span>	Disable <span style="float: right;">▶</span>

Figure 48 - Event Configuration interface



## Fault Relay Alarm

The Fault Relay Alarm function provides **Power Failure**, **Port Link Down/Broken** and **MAC Violation** detection. Select the checkbox to enable the relay alarming function. Please refer to the segment of '**Wiring the Fault Alarm Contacts**' for the external warning device installation.

- » **Power Failure:** With the checkbox selected the relay device inside the CNGE2FE16MS changes its state and the **FAULT** LED indicator is on if a power failure occurs.
- » **Port Link Down/Broken:** With the checkbox selected the relay device inside the CNGE2FE16MS changes its state and the **FAULT** LED indicator is on if the corresponding ports' states become link down or broken.
- » **MAC Violation:** With the checkbox selected the relay device inside the CNGE2FE16MS changes its state and the **FAULT** LED indicator is on if a MAC address violation event occurs.

**Fault Relay Alarm**

**Power Failure**

☐ Power 1 ☐ Power 2

**Port Link Down/Broken**

☐ Port 1 ☐ Port 2  
☐ Port 3 ☐ Port 4  
☐ Port 5 ☐ Port 6  
☐ Port 7 ☐ Port 8  
☐ Port 9 ☐ Port 10  
☐ Port 11 ☐ Port 12  
☐ Port 13 ☐ Port 14  
☐ Port 15 ☐ Port 16  
☐ Port 17 ☐ Port 18

**MAC Violation**

☐ MAC Violation

Apply Help

Please use Save Configuration to permanently save the updates.

Figure 49 - Fault Relay Alarm interface

## SNTP Configuration

SNTP (Simple Network Time Protocol) is a simplified version of NTP, that is an Internet protocol used to synchronize the clocks of computers with a selected time reference. Because time usually just advances, the time on different node stations might be different. With the communicating programs running on those devices, it would cause time to jump forward and back, an undesirable effect. Therefore, the CNGE2FE16MS provides comprehensive mechanisms to access national time and frequency dissemination services, organize the time-synchronization subnet and the local clock in each participating subnet peer.

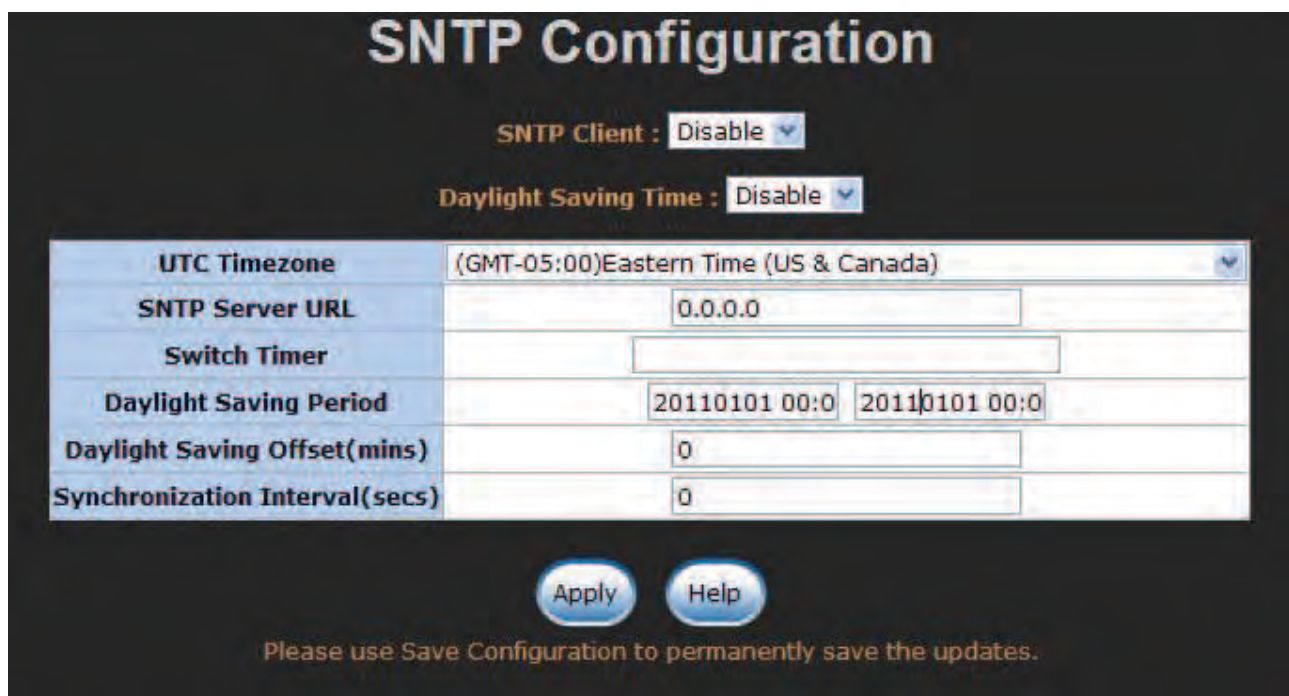
Daylight Saving Time (DST) is the convention of advancing clocks so that afternoons have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.

- » **SNTP Client:** Enable/disable the SNTP function to get the time from the SNTP server.
- » **Daylight Saving Time:** This function is used to enable/disable Daylight Saving Period and Daylight Saving Offset fields.
- » **UTC Timezone:** Set the location time zone for the switch. Table 5 lists different location time zones for your reference.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11 am
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 SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian 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

Table 5 - UTC Time Zones

- » **SNTP Server URL:** Specify the SNTP server IP address. You can assign a local network time-server IP address or an internet time-server IP address.
- » **Switch Timer:** When the switch has successfully connected to the SNTP server whose IP address was assigned in the field of SNTP Server URL, the current coordinated time is displayed here.
- » **Daylight Saving Period:** Set up the start and end date/time of the daylight saving period. Please key in the value in the format of 'YYYYMMDD' and 'HH:MM' (leave a space between 'YYYYMMDD' and 'HH:MM').
  - › **YYYYMMDD:** an eight-digit year/month/day specification.
  - › **HH:MM:** a five-digit (including a colon mark) hour/minute specification.
  - › For example, key in '20070701 02:00' and '20071104 02:00' in the two fields respectively to represent that DST begins at 2:00 a.m. on March 11, 2007 and ends at 2:00 a.m. on November 4, 2007.
- » **Daylight Saving Offset (mins):** For non-US and European countries, specify the amount of time for daylight savings. Please key in the valid figure in the range of minute between 0 and 720, which means you can set the offset up to 12 hours.
- » **Synchronization Interval (secs):** The Synchronization Interval is used for sending synchronizing packets periodically. Users can assign the time ranging from 64 to 1024 seconds. A **0** value displaying by default means that you disabled the auto-synchronized feature in the SNTP client mode. You can enable the feature by filling the interval range from 64~1024 seconds.
- » Select **Apply** to have the configuration take effect.



The screenshot shows the 'SNTP Configuration' window. At the top, 'SNTP Client' is set to 'Disable' and 'Daylight Saving Time' is also set to 'Disable'. Below these are several input fields: 'UTC Timezone' is set to '(GMT-05:00)Eastern Time (US & Canada)', 'SNTP Server URL' is '0.0.0.0', 'Switch Timer' is empty, 'Daylight Saving Period' has two fields with '20110101 00:0' and '20110101 00:0', 'Daylight Saving Offset(mins)' is '0', and 'Synchronization Interval(secs)' is '0'. At the bottom are 'Apply' and 'Help' buttons. A message at the very bottom says 'Please use Save Configuration to permanently save the updates.'

UTC Timezone	(GMT-05:00)Eastern Time (US & Canada)	
SNTP Server URL	0.0.0.0	
Switch Timer		
Daylight Saving Period	20110101 00:0	20110101 00:0
Daylight Saving Offset(mins)	0	
Synchronization Interval(secs)	0	

Apply Help

Please use Save Configuration to permanently save the updates.

Figure 50 - SNTP Configuration interface

## IP Security

The IP security function allows the user to assign up to 10 specific IP addresses that have permission to manage the switch through the http and telnet services for securing switch management. The purpose of giving permission to limited IP addresses is to allow only the authorized personnel/device to do the management task on the switch.

- » **IP Security Mode:** With this selection item set in the **Enable** mode, the **Enable HTTP Server**, **Enable Telnet Server** checkboxes and the ten security IP fields will then be available. If not, those items will appear in grey.
- » **Enable HTTP Server:** With this checkbox selected, Ethernet devices whose IP addresses match any one of the ten IP addresses in the Security IP table will be given permission to access this switch via the HTTP service.
- » **Enable Telnet Server:** With this checkbox selected, Ethernet devices whose IP addresses match any one of the ten IP addresses in the Security IP table will be given permission to access this switch via the telnet service.
- » **Security IP 1 ~ 10:** The system allows the user to assign up to 10 specific IP addresses for access security. Only when **IP Security Mode** is enabled can these 10 IP addresses access and manage the switch through the HTTP/Telnet services.
- » And then, select **Apply** to have the configuration take effect.

**Note** Remember to execute the **Save Configuration** action, otherwise the new configuration will be lost when the switch powers off.



IP Security	
IP Security Mode:	Enable
<input checked="" type="checkbox"/> Enable HTTP Server	
<input checked="" type="checkbox"/> Enable Telnet Server	
Security IP1	192.168.10.8
Security IP2	192.168.10.68
Security IP3	0.0.0.0
Security IP4	0.0.0.0
Security IP5	0.0.0.0
Security IP6	0.0.0.0
Security IP7	0.0.0.0
Security IP8	0.0.0.0
Security IP9	0.0.0.0
Security IP10	0.0.0.0
<input type="button" value="Apply"/> <input type="button" value="Help"/>	
Please use Save Configuration to permanently save the updates.	

Figure 51 - IP Security interface

## User Authentication

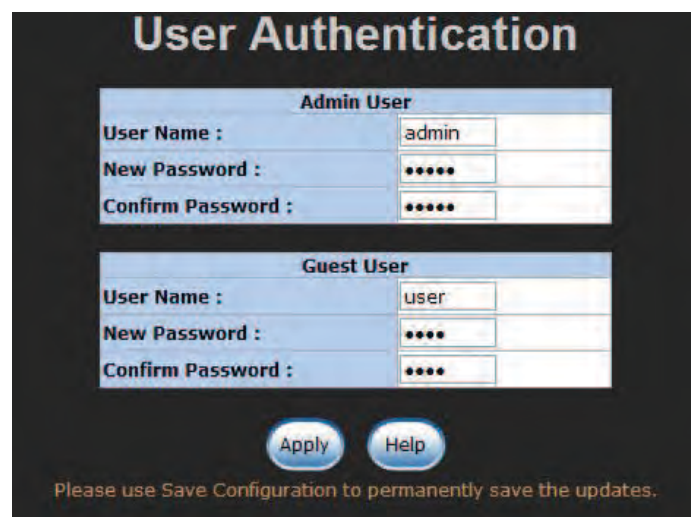
The User Authentication interface allows users to configure different login accounts for security reasons. The Admin User account is given administrative privileges. If you want others to access the Ethernet switch with a restricted account, configure the Guest User account for login authentication.

### Admin User

- » **User Name:** The admin user account is **admin** by default. Type in the User Name field with a new name as you wish.
- » **New Password:** The password to the admin user account is **admin** by default. Specify a new password as you wish.
- » **Confirm password:** Type in the new password again for confirmation.
- » When finished, select **Apply** to have the configuration take effect.

### Guest User

- » **User Name:** The guest user account is **user** by default. Type in the User Name field with a new name as you wish.
- » **New Password:** The password to the guest user account is **user** by default. Specify a new password as you wish.
- » **Confirm password:** Type in the new password again for confirmation.
- » When finished, select **Apply** to have the configuration take effect.



The screenshot displays the 'User Authentication' configuration page. It features two main sections: 'Admin User' and 'Guest User'. Each section contains three input fields: 'User Name', 'New Password', and 'Confirm Password'. The 'Admin User' section has 'admin' in the User Name field and masked passwords in the other two. The 'Guest User' section has 'user' in the User Name field and masked passwords in the other two. At the bottom, there are 'Apply' and 'Help' buttons, and a note stating 'Please use Save Configuration to permanently save the updates.'

Figure 52 – User Authentication interface

## N-Key Transaction

Users can back up or restore configuration from/to the switch via this interface.

- » **Auto mode:** Tick this check box and select **Apply** to enable the function that with the N-Key device connected to the RS-232 console port, the switch will automatically load the system configuration from N-Key when booting up.
- » **Backup:** Make sure N-Key is connected with the RS-232 console port and then select this button to back up the current configuration from the switch.
- » **Restore:** Make sure N-Key is connected and then select this button to load the system configuration from N-Key.

**Note:** After selecting the **Backup/Restore** button, for the purpose of confirmation, you will see a dialog box showing up to display the current N-Key information including model name, firmware version, kernel version, and the last backup time.

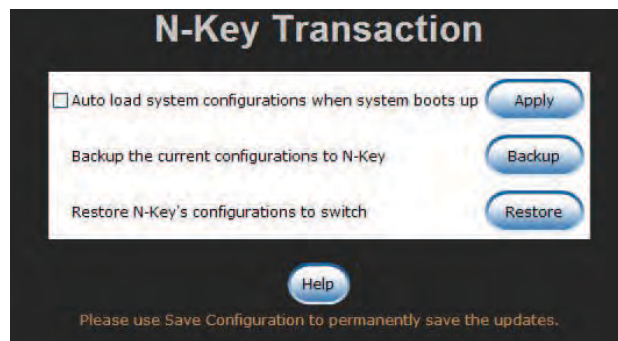


Figure 53 - N-Key Transaction interface



## Port Statistics

The Port Statistics chart provides the current statistics information that displays the real-time packet transfer states for each port. The user might use the information to plan and implement the network, or check and find the problem when a collision or heavy traffic occurs.

- » **Port:** Port number indexed.
- » **Type:** Displays the network media type of the port.
- » **Link:** The states of linking – **Up** or **Down**.
- » **State:** Displays port states set by the Port Control interface. 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 good packets (including undersize [less than 64 bytes], oversize, CRC error, fragments and jabbers) via this port.
- » **Tx Abort Packet:** The counts of aborted packets while transmitting.
- » **Packet Collision:** The counts of packet collision.
- » **Packet Dropped:** The counts of dropped packets.
- » **Rx Bcast Packet:** The counts of broadcast packets.
- » **Rx Mcast Packet:** The counts of multicast packets.
- » Select the **Clear** button to clear the Port Statistics chart of all counts.

Port Statistics												
Port	Type	Link	State	Tx Good Packet	Tx Bad Packet	Rx Good Packet	Rx Bad Packet	Tx Abort Packet	Packet Collision	Packet Dropped	RX Bcast Packet	RX Mcast Packet
Port.01	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.02	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.03	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.04	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.05	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.06	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.07	100TX	Up	Enable	1122	0	3122	0	0	0	0	1338	86
Port.08	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.09	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.10	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.11	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.12	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.13	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.14	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.15	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.16	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.17	1GTX/mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0
Port.18	1GTX/mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0

Figure 54 – Port Statistics interface



## Port Control

In Port Control (See Figure 55) you can configure the parameters of the connection for each port.

- » **Port:** Scroll up/down the scroll bar and select on the port number to choose a particular port to be configured.
- » **State:** Enable/disable the port. If the port state is set on **Disable**, the port will not be able to receive or transmit any packet.
- » **Negotiation:** Options include **Auto** and **Force**. With this parameter set on **Auto**, the speed and duplex fields display in grey, which means the ports are negotiated automatically. When you set it on **Force**, you have to set the speed and duplex mode manually by selecting the pull-down menus of the **Speed** and **Duplex** fields.
- » **Speed:** It is available for selecting when the **Negotiation** field is set on **Force**. When the **Negotiation** field is set on **Auto**, this field becomes a read-only field displaying in grey.
- » **Duplex:** It is available for selecting when the **Negotiation** field is set on **Force**. When the **Negotiation** field is set on **Auto**, this field becomes a read-only field displaying in grey.
- » **Flow Control:** Whether or not the receiving node sends feedback to the sending node is determined by this item. With this item enabled, if the input data rate of the receiving device exceeds, the receiving device will send a PAUSE frame that halts the transmission of the sender for a specified period of time. With this item disabled, the receiving device will drop the packets it is unable to process.
- » **Security:** When 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. Keep in mind that the Security item is set as **On** so that the MAC violation event log/email alert will then be issued. Further information please review the segments of **MAC Address Table–Static MAC Addresses** and **System Event Log–Event Configuration**.
- » Select **Apply** to have the configuration take effect.

## Port Control

Port	State	Negotiation	Speed	Duplex	Flow Control	Security
Port.01	Enable	Auto	100	Full	Enable	Off
Port.02						
Port.03						
Port.04						

Please use Save Configuration to permanently save the updates.

Port	Group ID	Type	Link	State	Negotiation	Speed Config	Duplex Actual	Flow Control Config	Flow Control Actual	Security
Port.01	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	ON
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	ON
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	ON
Port.06	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.07	N/A	100TX	Up	Enable	Auto	100 Full	100 Full	Enable	ON	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	1GTX/mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.18	N/A	1GTX/mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF

Figure 55 - Port Control interface

## Port Trunk

Port-trunking is the combination of several ports or network cables in order to expand the connection speed beyond the limits of any one single port or network cable. Link Aggregation Control Protocol (LACP), which is 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 so-called logical aggregator work at the same connection speed and LACP operation requires full-duplex mode.

## Aggregator Setting

Please read the instructions below and refer to Figure 66 to make an LACP or non-LACP trunk group.

- » **System Priority:** A value that is used to identify the controlling switch of an LACP link system. The switch with the lower value has the higher system priority and is selected as the controlling end, which controls port priorities, of the LACP link system.
- » **Group ID:** There are four trunk groups to be selected. Assign the group ID to the particular trunk group.
- » **LACP:** Select the pull-down menu to enable/disable LACP for the trunk group. With LACP enabled, 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 field allows the user to type in the total number of active ports up to four. With a **LACP trunk group** employed, for example you assign four ports to be the members of a trunk group whose Work Ports field is set as two the excessive ports will be standby/redundant ports and can be aggregated instead of working ports that fail. As for the **static trunk group** (non-LACP), the number of work ports must equal the total number of the group member ports.
- » The system allows a maximum of four ports to be aggregated in a trunk group. Having configured the parameters above, highlight the ports in the right list box to join the trunk group. Select the **Add** button and the ports highlighted in the right list box will be shifted to the left list box. To remove unwanted ports, select the ports in the left list box and select the **Remove** button.
- » When LACP enabled, you can configure LACP Active/Passive states for each member port on the **State Activity** tab.
- » When finished, select **Apply** to take the configuration take effect.
- » To remove a trunk group, select the Group ID by selecting the pull-down menu labeled as **Group ID** and select then select the **Delete** button.

## Port Trunk - Aggregator Setting

Aggregator SettingAggregator InformationState Activity

**System Priority**

<b>Group ID</b>	<input type="text" value="Trunk.1"/>	<input type="button" value="Select"/>	
<b>LACP</b>	<input type="text" value="Enable"/>		
<b>Work Ports</b>	<input type="text" value="4"/>		
<div style="border: 1px solid black; padding: 2px;">Port.01 Port.02 Port.03 Port.04</div>	<input type="button" value=" &lt;&lt;Add"/>  <input type="button" value="Remove&gt;&gt;"/>		<div style="border: 1px solid black; padding: 2px;">Port.05 Port.06 Port.07 Port.08 Port.09 Port.10 Port.11 Port.12 Port.13</div>

Please use Save Configuration to permanently save the updates.

Notice: The trunk function do not support GVRP and X-Ring.

Figure 56 - Port Trunk–Aggregator Setting interface (four ports are added to the left field with LACP enabled)

## Aggregator Information

### LACP Disabled

Having configured the aggregator setting with LACP disabled, you can check the static trunk group information on the **Aggregator Information** tab.

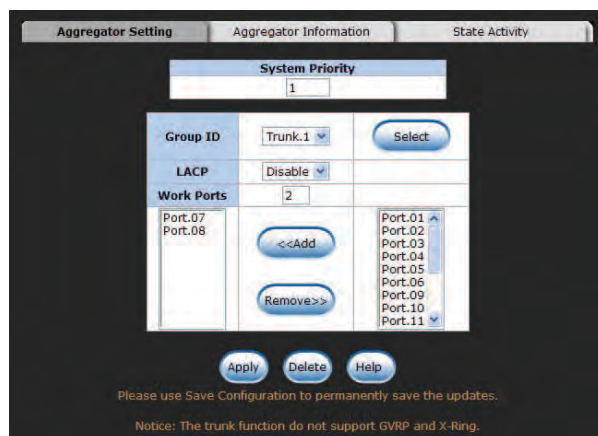


Figure 57 - Assigning 2 ports to a trunk group with LACP disabled



Figure 58 - Static Trunking Group Information tab

- » **Group Key:** This is a read-only field that displays the trunk group ID.
- » **Port Member:** This is a read-only field that displays the members of the static trunk group.



## LACP Enabled

Having configured the aggregator setting with LACP enabled, you can check the trunking group information between two switches on the Aggregator Information tab.

### Configuration for Switch 1

- » Set **System Priority** of the trunk group. The field displays **1** by default.
- » Select a trunk **Group ID** by selecting the pull-down menu.
- » **Enable** LACP.
- » Include the member ports by highlighting the ports in the right list box and then select the **Add** button. Note the number in the Work Ports field changes automatically depending on how many ports you have selected.

The screenshot shows the 'Port Trunk - Aggregator Setting' window with three tabs: 'Aggregator Setting' (selected), 'Aggregator Information', and 'State Activity'. The 'Aggregator Setting' tab contains the following fields and controls:

- System Priority:** A text box containing the value '1'.
- Group ID:** A dropdown menu showing 'Trunk.1' and a 'Select' button.
- LACP:** A dropdown menu showing 'Enable'.
- Work Ports:** A text box containing the value '2'.
- Port Selection:** Two list boxes. The left box contains 'Port.01' and 'Port.02'. The right box contains 'Port.03' through 'Port.11'. Between the boxes are '<<Add' and 'Remove>>' buttons.
- Buttons:** 'Apply', 'Delete', and 'Help' buttons at the bottom.

Below the buttons, there is a message: 'Please use Save Configuration to permanently save the updates.' and a notice: 'Notice: The trunk function do not support GVRP and X-Ring.'

Figure 59 – Switch 1 configuration interface

Group1							
Actor				Partner			
Priority	1			1			
MAC	000F38054920			00223B030732			
PortNo	Key	Priority	Active	PortNo	Key	Priority	
PORT1	513	1	selected	PORT7	513	1	
PORT2	513	1	selected	PORT8	513	1	

Figure 60 – Aggregation Information of Switch 1

- » Select the **Aggregator Information** tab to check the trunked group information as the illustration shown above after the two switches configured.

## Configuration for Switch 2

**Port Trunk - Aggregator Setting**

Aggregator Setting | Aggregator Information | State Activity

**System Priority**  
1

Group ID	LACP	Work Ports
Trunk.1	Enable	2

Port.07  
Port.08

<<Add

Remove>>

Port.01  
Port.02  
Port.03  
Port.04  
Port.05  
Port.06  
Port.09  
Port.10

Apply Delete Help

Please use Save Configuration to permanently save the updates.

Notice: The trunk function do not support GVRP and X-Ring.

Figure 61 - Switch 2 Configuration Interface

- » Set **System Priority** of the trunk group. The field displays **1** by default.
- » Select a trunk **Group ID** by selecting the pull-down menu.
- » **Enable** LACP.
- » Include the member ports by highlighting the ports in the right list box and then select the **Add** button. Note the number in the Work Ports field changes automatically depending on how many ports you have selected.



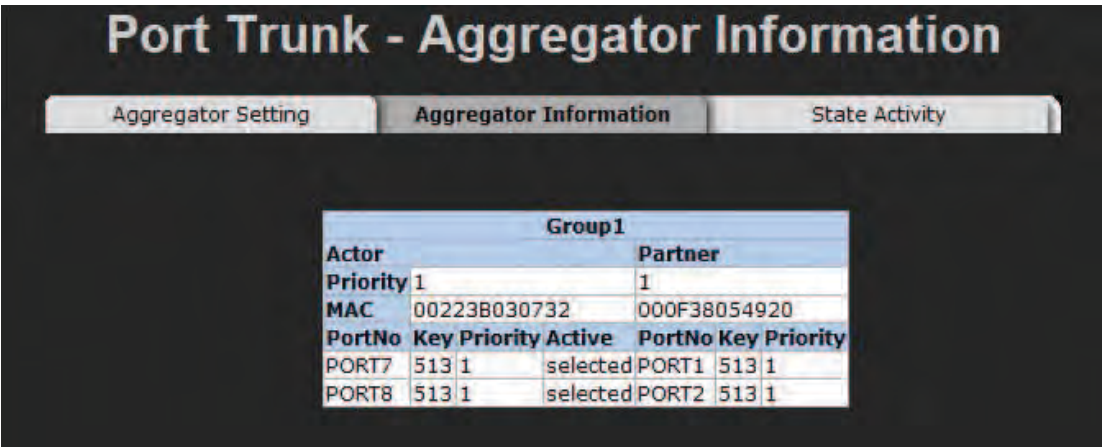


Figure 62 - Aggregation Information of Switch 2

- » Select the **Aggregator Information** tab to check the trunked group information as the illustration shown above after the two switches configured.

State Activity

Having configured the LACP aggregator on the **Aggregator Setting** tab, you may want to change the state activity for the members of the LACP trunk group. You can select/unselect the checkbox beside the state label. If you remove the select mark of the corresponding port and select the **Apply** button, the port state activity will change to Passive.

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

*Note 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.*

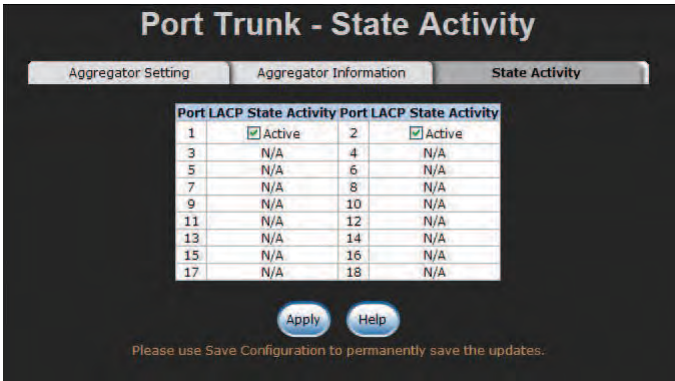


Figure 63 - State Activity of Switch 1

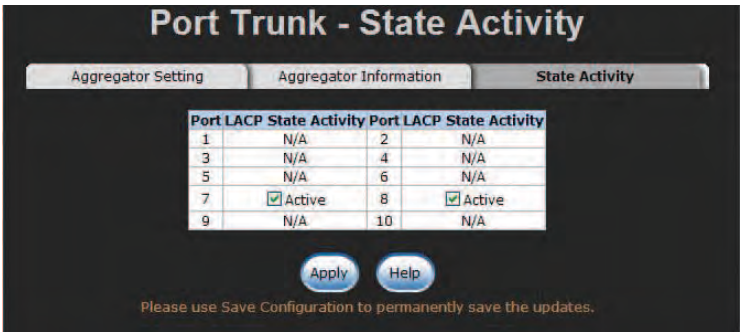


Figure 64 - State Activity of Switch 2

## Port Mirroring

Port Mirroring is a method for monitoring of network traffic on switched networks. Traffic through ports can be monitored by one specific port, which means traffic going in or out the monitored (source) ports will be duplicated into the mirroring (destination) port.

	Destination Port		Source Port	
	RX	TX	RX	TX
Port.01	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.02	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.03	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.04	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.05	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.06	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.07	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.08	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.09	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.10	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.11	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.12	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.13	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.14	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.15	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.16	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.17	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.18	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply Help

Please use Save Configuration to permanently save the updates.

Figure 65 - Port Mirroring interface

- » **Destination Port:** Select one port to be the destination (mirroring) port for monitoring both RX and TX traffic coming from the source port. Or, select two ports for monitoring RX traffic and TX traffic respectively. Users can forward the traffic captured by the mirroring port to the packet analyzer such as Netxray for further analyses.
- » **Source Port:** Select the checkbox to monitor the corresponding port. All monitored port traffic will be copied to the mirroring (destination) port. Users can select multiple source ports by selecting the **RX** or **TX** checkboxes.
- » When finished, select the **Apply** button.

## Rate Limiting

You can respectively configure the ingress limitation type and ingress/egress rate for each port.

### Ingress Limit Frame Type

Select the limit type for ingress frames. Four options are available as follows:

- » **All**
- » **Broadcast/Multicast/Flooded Unicast**
- » **Broadcast/Multicast**
- » **Broadcast only**

The egress rate will limit all types of frame.

	Ingress Limit Frame Type	Ingress	Egress
Port.01	All	0 kbps	0 kbps
Port.02	All	0 kbps	0 kbps
Port.03	All	160 kbps	0 kbps
Port.04	All	320 kbps	0 kbps
Port.05	All	512 kbps	0 kbps
Port.06	All	768 kbps	0 kbps
Port.07	All	1024 kbps	0 kbps
Port.08	All	1280 kbps	0 kbps
Port.09	All	1536 kbps	0 kbps
Port.10	All	2048 kbps	0 kbps
Port.11	All	3072 kbps	0 kbps
Port.12	All	4096 kbps	0 kbps
Port.13	All	5120 kbps	0 kbps
Port.14	All	8192 kbps	0 kbps
Port.15	All	10240 kbps	0 kbps
Port.16	All	20480 kbps	0 kbps
Port.17	All	30720 kbps	0 kbps
Port.18	All	40960 kbps	0 kbps

Apply Help

Please use Save Configuration to permanently save the updates.

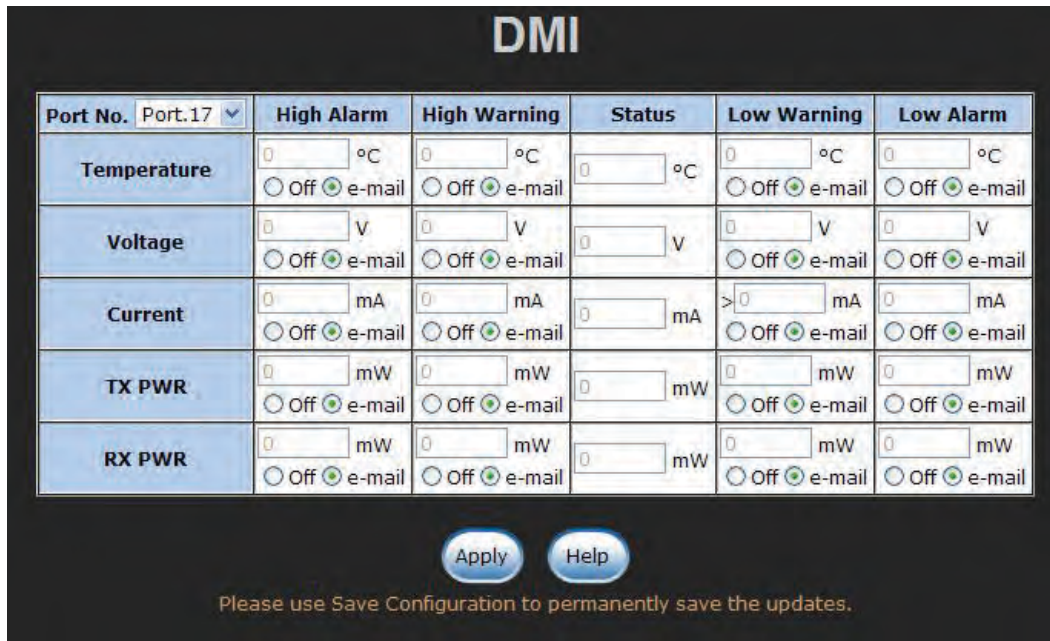
Figure 66 - Rate Limiting interface

- » Select the **Ingress** and **Egress** pull-down menus to select the bandwidth limit.
- » When finished, select **Apply** to have the configuration take effect.



## DMI

The DMI (Diagnostic Monitoring Interface) is developed for monitoring temperature, voltage, current, transmitting power and receiving power for SFP (Mini-GBIC) ports. If the real detected values, such as temperature, voltage, current etc., of the respective ports reach the threshold of the connected transceiver, the system will shut down the device or send e-mail to notify the related staff. The recipients can be specified via the SMTP configuration. Please refer to the System Event Log–SMTP Configuration section.



Port No.	High Alarm	High Warning	Status	Low Warning	Low Alarm
Port.17					
Temperature	<input type="text"/> °C <input type="radio"/> Off <input checked="" type="radio"/> e-mail	<input type="text"/> °C <input type="radio"/> Off <input checked="" type="radio"/> e-mail	<input type="text"/> °C	<input type="text"/> °C <input type="radio"/> Off <input checked="" type="radio"/> e-mail	<input type="text"/> °C <input type="radio"/> Off <input checked="" type="radio"/> e-mail
Voltage	<input type="text"/> V <input type="radio"/> Off <input checked="" type="radio"/> e-mail	<input type="text"/> V <input type="radio"/> Off <input checked="" type="radio"/> e-mail	<input type="text"/> V	<input type="text"/> V <input type="radio"/> Off <input checked="" type="radio"/> e-mail	<input type="text"/> V <input type="radio"/> Off <input checked="" type="radio"/> e-mail
Current	<input type="text"/> mA <input type="radio"/> Off <input checked="" type="radio"/> e-mail	<input type="text"/> mA <input type="radio"/> Off <input checked="" type="radio"/> e-mail	<input type="text"/> mA	> <input type="text"/> mA <input type="radio"/> Off <input checked="" type="radio"/> e-mail	<input type="text"/> mA <input type="radio"/> Off <input checked="" type="radio"/> e-mail
TX PWR	<input type="text"/> mW <input type="radio"/> Off <input checked="" type="radio"/> e-mail	<input type="text"/> mW <input type="radio"/> Off <input checked="" type="radio"/> e-mail	<input type="text"/> mW	<input type="text"/> mW <input type="radio"/> Off <input checked="" type="radio"/> e-mail	<input type="text"/> mW <input type="radio"/> Off <input checked="" type="radio"/> e-mail
RX PWR	<input type="text"/> mW <input type="radio"/> Off <input checked="" type="radio"/> e-mail	<input type="text"/> mW <input type="radio"/> Off <input checked="" type="radio"/> e-mail	<input type="text"/> mW	<input type="text"/> mW <input type="radio"/> Off <input checked="" type="radio"/> e-mail	<input type="text"/> mW <input type="radio"/> Off <input checked="" type="radio"/> e-mail

Apply Help

Please use Save Configuration to permanently save the updates.

Figure 67 - DMI interface

- » **Port No.:** Select the pull-down menu to select a particular SFP port to display its information and define reaction options.
- » **Temperature:** The fields showing values measured in degrees Celsius. Select the radio button labeled as **Off** to shut down the device or the other one labeled as **e-mail** to send e-mail for notifications when the port temperature reaches the threshold.
- » **Voltage:** The fields showing values measured in voltages. Select the radio button labeled as **Off** to shut down the device or the other one labeled as **e-mail** to send e-mail for notifications when the port voltage reaches the threshold.
- » **Current:** The fields showing values measured in milliamperes. Select the radio button labeled as **Off** to shut down the device or the other one labeled as **e-mail** to send e-mail for notifications when the port current reaches the threshold.
- » **TX PWR:** The fields showing values measured in milliwatts. Select the radio button labeled as **Off** to shut down the device or the other one labeled as **e-mail** to send e-mail for notifications when the port transmitting power reaches the threshold.
- » **RX PWR:** The fields showing values measured in milliwatts. Select the radio button labeled as **Off** to shut down the device or the other one labeled as **e-mail** to send e-mail for notifications when the port receiving power reaches the threshold.

## VLAN Configuration

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which allows you to isolate network traffic. Therefore only the members of the same VLAN will receive traffic from the ones among the same VLAN. Basically, creating a VLAN on 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.

This switch supports **802.1Q** (tagged-based) VLAN. Please read the following instructions to configure the appropriate type of VLAN for your need.

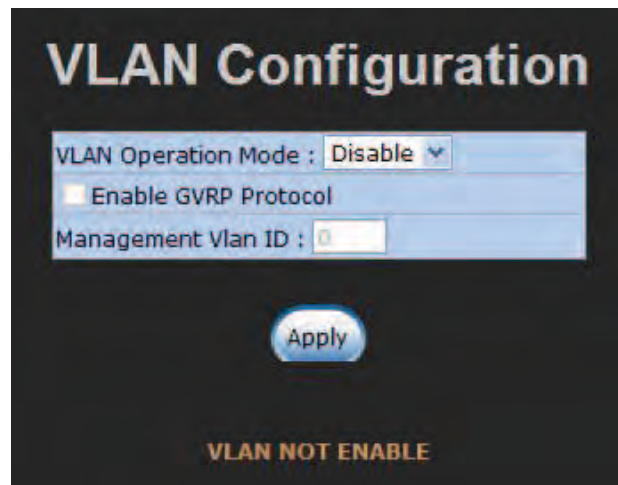


Figure 68 - VLAN Configuration interface

## 802.1Q VLAN

When the VLAN operation mode is set on 802.1Q, all ports on the switch belong to the 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 the default VLAN that cannot be deleted.

GVRP (GARP VLAN Registration Protocol) is a protocol that facilitates control of 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, with GVRP enabled, the switches are able to automatically exchange the information of their VLAN database. Therefore, the user needn't manually configure the link type. The packets belonging to the same VLAN can communicate across switches.

Each member port of 802.1Q is on either an Access Link (VLAN-tagged) or a Trunk Link (no 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 a

particular VLAN group, except 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 sent through tagged and untagged ports.

This switch supports IEEE 802.1Q-in-Q or IEEE 802.1ad standard developed to break through the limitation of 802.1Q for multi-VLAN environments where the amount of VLAN may exceeds 4096. Q-in-Q allows a given Ethernet frame with two VLAN headers inserted, known as doubled-tagged or stacked VLANs. And therefore, a double-tagged frame is sufficient to accommodate the amount of VLANs up to  $4096 \times 4096 = 16777216$ .

## 802.1Q Configuration

Please follow the instructions below to configure the 802.1Q VLAN.

- » Select the pull-down menu to select **802.1Q** and select Apply to configure the VLAN Operation Mode on 802.1Q.
- » **Enable GVRP Protocol:** Select this checkbox to enable GVRP protocol. This checkbox is available while the VLAN Operation Mode is set on **802.1Q**.
- » **Management VLAN ID:** Only the VLAN members, whose Untagged VID (PVID) equals to the value specified in this field, have permission to access the switch. The default value is **0** meaning this limit is not enabled (all members in different VLANs can access this switch).
- » After you have configured the three parameters, select the **Apply** button right beneath this area to finish creating an 802.1Q VLAN.

**VLAN Configuration**

VLAN Operation Mode : 802.1Q

☐ Enable GVRP Protocol

Management Vlan ID : 0

Apply

**802.1Q Configuration** | Group Configuration

Port	Link Type	Untagged Vid	Tagged Vid
Port.01	QinQ	1	
Port.02	Access Link	1	
Port.04	Access Link	1	
Port.06	Access Link	1	
Port.07	Access Link	1	
Port.08	Access Link	1	
Port.09	Access Link	1	
Port.10	Access Link	1	
Port.11	Access Link	1	
Port.12	Access Link	1	
Port.13	Access Link	1	
Port.14	Access Link	1	
Port.15	Access Link	1	
Port.16	Access Link	1	
Port.17	Access Link	1	
Port.18	Access Link	1	
Trunk.1	Access Link	1	

Please use Save Configuration to permanently save the updates.

Figure 69 – 802.1Q VLAN interface

- » On the 802.1Q Configuration tab, select the **Port** pull-down menu to select a port you want to configure within the VLAN.



- » **Link Type:** Three options are available. Select the **Link Type** pull-down menu to select the link type.
- » **Access Link:** A segment that provides the link path for one or more stations to the VLAN-aware device like switches. An Access Port (untagged port) connecting to the access link has an untagged VID (also called PVID). After an untagged frame gets into the access port, the switch inserts a four-byte tag in the frame. The contents of the last 12-bit of the tag is the 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 doesn't have an understanding of tagged frame, the field of Tagged VID is not available.*

- » **Trunk Link:** A segment that provides the link path for one or more VLAN-aware devices. A Trunk Port connecting to the trunk link has an understanding of tagged frame, which is used for communications across VLANs. Which frames of the specified VIDs will be forwarded depends on the values filled in the Tagged VID field. Insert a comma between two VIDs.

***Note:** A trunk port doesn't insert tags into an untagged frame, and therefore the untagged VID field is not available.*

***It's not necessary to type 1 in the tagged VID field. The trunk port will forward the frames of VLAN 1.***

***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 that consists of Access and Trunk links. The hybrid port has both the features of the access and trunk ports. A hybrid port has a PVID belonging to a particular VLAN, and also forwards the specified tagged-frames for the purpose of VLAN communications between switches.

***Note:** It's not necessary to type 1 in the tagged VID field. The hybrid port will forward the frames of VLAN 1.*

***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.***

- » **QinQ:** With the given port set its link type on QinQ, where frames received will be added a tag as an outer 802.1Q VLAN header that needs to be specified by users in the Untagged Vid field next to this pull-down menu. The value(s) specified in the Tagged Vid field show the inner 802.1Q VLAN header(s) that constitute frames with those VLAN headers will be encapsulated.
- » **Untagged Vid:** This field is available when the Link Type pull-down menu is set on Access Link, Hybrid Link and QinQ. Assign a number in the range between 1 and 4094.
- » **Tagged Vid:** This field is available when the Link Type pull-down menu is set on Trunk Link and Hybrid Link and QinQ. Assign a number in the range between 1 and 4094.
- » Select the **Apply** button on the tab to have the port configuration take effect.
- » And then you can see the link type, untagged VID, and tagged VID information of each port shown in the table on the screen.

## Group Configuration

Edit the existing VLAN Groups.

- » Select the **Group Configuration** tab.
- » Select a VLAN group in the list box and select the **Edit** button.

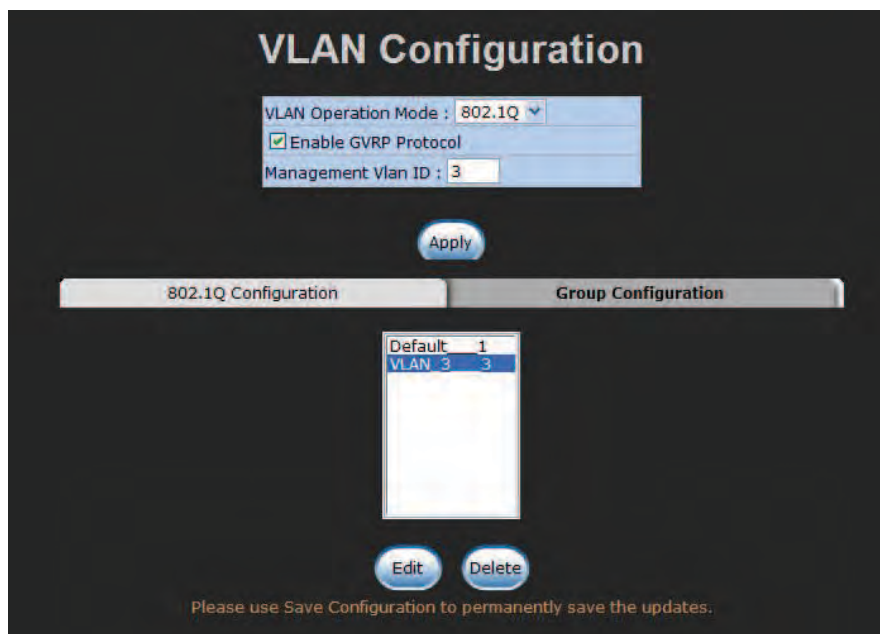


Figure 70 - Group Configuration interface

- » After selecting the **Edit** button, you can change **Group Name** and **VLAN ID** of the selected VLAN group.

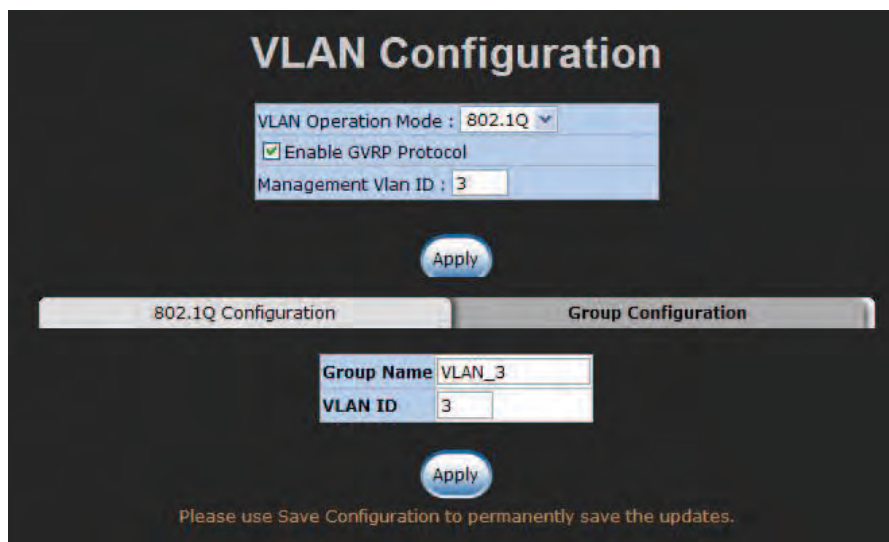


Figure 71 - Group Configuration interface

- » When finished, select **Apply** to have the modification take effect.

## Rapid Spanning Tree

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

### RSTP System Configuration

This tab allows users to configure parameters for RSTP and displays the spanning tree information of the root bridge. Refer to Figure 72.

- » **RSTP Mode:** Select the **RSTP Mode** pull-down menu to enable the RSTP function.
- » **Priority (0-61440):** The switch with the lowest numerical value has the highest priority and will be selected as the admin device. If the value is changed, users must reboot the switch. **Note** the value specified in the Priority field must be a multiple of 4096 according to the protocol rule.
- » **Max Age (6-40):** Enter the time in seconds between 6 and 40 for which the switch waits to attempt to save its configuration.
- » **Hello Time (1-10):** Enter the time in seconds between 1 and 10 that controls the switch to send out the BPDU packet to check current states of RSTP.
- » **Forward Delay Time (4-30):** Enter the time in seconds between 4 and 30 that a port spends changing from its learning and listening state to the forwarding state.
- » When finished, select the **Apply** button to have the configuration take effect.

**Note:** *Follow the rule below to configure Max Age, Hello Time, and Forward Delay Time parameters.*

*$2 \times (\text{Forward Delay Time value} - 1) > = \text{Max Age value} > = 2 \times (\text{Hello Time value} + 1)$*

## Root bridge Information

The column fields give the current bridge information for the switch.

- » **Bridge ID:** This field displays the bridge ID by showing the MAC address of this switch.
- » **Root Priority:** This field displays the numerical value indicating bridge priority of the switch. Generally, the switch with the lowest numerical value in the network is set as the root bridge.
- » **Root Port:** This field indicates which port is connecting to the root bridge. When the switch is set as the root bridge, the word **Root** shows here.
- » **Root Path Cost:** This field displays the path cost between the switch's Root Port and the designated port of the root bridge. Path cost is a value to each port typically based on rules described as part of 802.1d. For the root bridge this is zero. For all other bridges, it is the sum of the port path costs on the least cost path to the root bridge.
- » **Max Age:** Displays the configured aging time of the switch.
- » **Hello Time:** Displays the configured Hello Time.
- » **Forward Delay:** Displays the configured forward delay time.

**RSTP - System Configuration**

System Configuration | Port Configuration

RSTP Mode	Enable ▾
Priority (0-61440)	32768
Max Age (6-40)	20
Hello Time (1-10)	2
Forward Delay Time (4-30)	15

Priority must be a multiple of 4096  
 $2 * (\text{Forward Delay Time} - 1)$  should be greater than or equal to the Max Age.  
 The Max Age should be greater than or equal to  $2 * (\text{Hello Time} + 1)$ .

Apply Help

Please use Save Configuration to permanently save the updates.

**Root Bridge Information**

Bridge ID	8000000F38054920
Root Priority	32768
Root Port	Root
Root Path Cost	0
Max Age	20
Hello Time	2
Forward Delay	15

Figure 72 - RSTP System Configuration interface

## Port Configuration

This tab (Figure 73) offers the interface for RSTP port configuration where you can assign parameters to each port. The rapid spanning tree protocol will have the port with the higher priority in forwarding state and block other ports to make certain that there is no loop in the LAN.

Scroll the list box to select a port for configuration.

- » **Path Cost:** The path cost can be managed. Enter a number in the range of 1 to 200,000,000.
- » **Priority:** Port Priority. Give the value to decide which port is to be blocked by setting its priority. Enter a number between 0 and 240. **The entered value must be a multiple of 16.**
- » **Admin P2P:** The rapid state transitions possible within RSTP are dependent upon whether the port concerned can only be connected to exactly another 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 states of the link to be manipulated administratively. **True** means the port is regarded as a point-to-point link. **False** means the port is regarded as a shared link. **Auto** means the link type is determined by the auto-negotiation between the two peers.
- » **Admin Edge:** The port directly connected to an end station is known as an edge port that won't create bridging loop in the network. To configure the port as an edge port, set the port to **True** state.
- » **Admin Non STP:** Configure whether the port includes the STP mathematic calculation. **True** means not to include the STP mathematic calculation. **False** means the STP mathematic calculation is included.
- » When finished, select **Apply** to have the configuration take effect.



## RSTP - Port Configuration

System Configuration
Port Configuration

Port	Path Cost (1-20000000)	Priority (0-240)	Admin P2P	Admin Edge	Admin Non STP
Port.01					
Port.02					
Port.03	200000	128	Auto	true	false
Port.04					
Port.05					

priority must be a multiple of 16

Apply
Help

Please use Save Configuration to permanently save the updates.

### RSTP Port Status

Port	Path Cost	Port Priority	Oper P2P	Oper Edge	STP Neighbor	State	Role
Port.01	200000	128	True	True	False	Disabled	Disabled
Port.02	200000	128	True	True	False	Disabled	Disabled
Port.03	200000	128	True	True	False	Disabled	Disabled
Port.04	200000	128	True	True	False	Disabled	Disabled
Port.05	200000	128	True	True	False	Disabled	Disabled
Port.06	200000	128	True	True	False	Disabled	Disabled
Port.07	200000	128	True	True	False	Forwarding	Designated
Port.08	200000	128	True	True	False	Disabled	Disabled
Port.09	200000	128	True	True	False	Disabled	Disabled
Port.10	200000	128	True	True	False	Disabled	Disabled
Port.11	200000	128	True	True	False	Disabled	Disabled
Port.12	200000	128	True	True	False	Disabled	Disabled
Port.13	200000	128	True	True	False	Disabled	Disabled
Port.14	200000	128	True	True	False	Disabled	Disabled
Port.15	200000	128	True	True	False	Disabled	Disabled
Port.16	200000	128	True	True	False	Disabled	Disabled
Port.17	200000	128	True	True	False	Disabled	Disabled
Port.18	200000	128	True	True	False	Disabled	Disabled

Figure 73 – RSTP Port Configuration interface

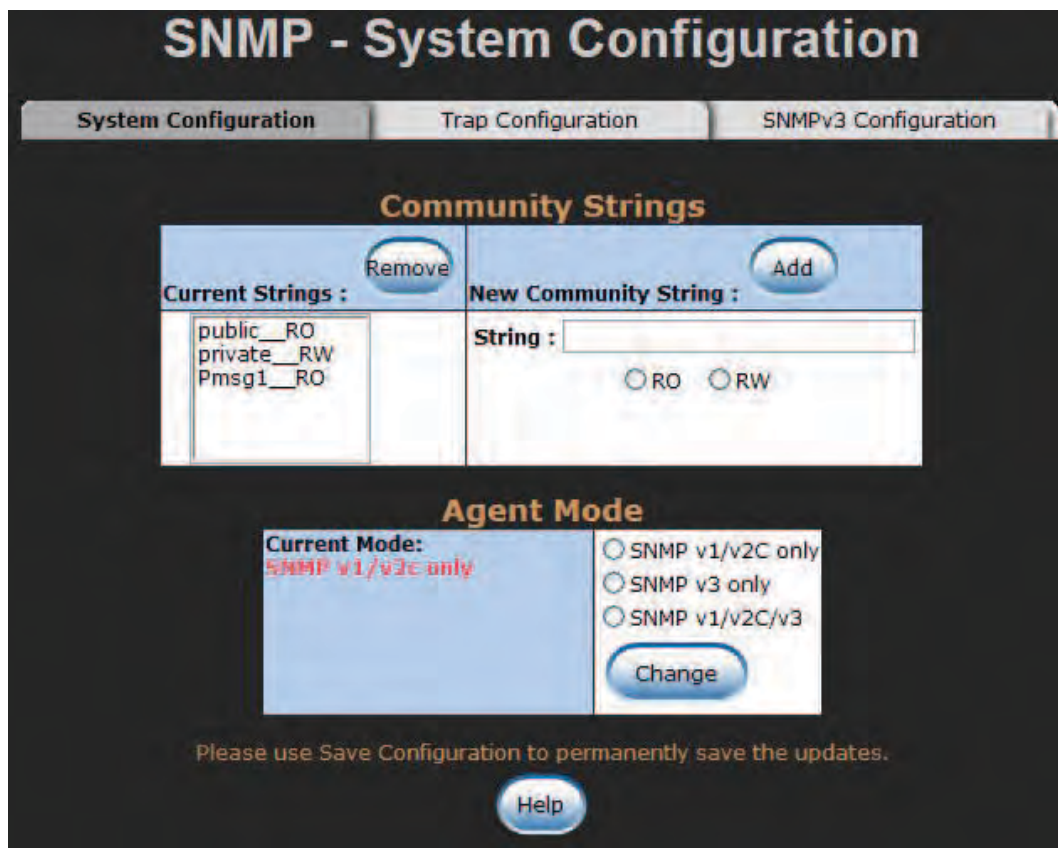
## SNMP Configuration

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 (NMS) learn of problems by receiving traps or change notices from network devices implementing SNMP.

## System Configuration

This tab allows users to define new community strings and remove the unwanted community strings for authentication purposes. With adding a new community string, you should also specify the type of access permission and the agent mode.

- » **String:** Enter the community string in the field as a password for authentication.
- » **RO:** Read only. With this radio button selected, the community string is given the read-only permission for the MIB objects.
- » **RW:** Read/write. With this radio button selected, the community string is given the read/write permission for the MIB objects.
- » Select **Add** to finish adding a new community string.
- » To remove a specific community string, select the community string shows in the list box and select **Remove**. The strings of Public\_RO and Private\_RW are default strings. You can remove them but after resetting the switch to default, the two strings show up again.
- » **Agent Mode:** Select one of the radio buttons to choose the SNMP version that the community string will use. And then select **Change** to ensure the selected SNMP version mode is changed.



The screenshot displays the 'SNMP - System Configuration' web interface. At the top, there are three tabs: 'System Configuration' (selected), 'Trap Configuration', and 'SNMPv3 Configuration'. Below the tabs, the 'Community Strings' section is visible. It features a 'Current Strings' list box containing 'public\_\_RO', 'private\_\_RW', and 'Pmsg1\_\_RO', with a 'Remove' button to its right. To the right of this is the 'New Community String' section, which includes a 'String' input field, radio buttons for 'RO' and 'RW', and an 'Add' button. Below these sections is the 'Agent Mode' section. It shows the 'Current Mode' as 'SNMP v1/v2C only' and provides three radio button options: 'SNMP v1/v2C only' (selected), 'SNMP v3 only', and 'SNMP v1/v2C/v3'. A 'Change' button is located below these options. At the bottom of the interface, a message states 'Please use Save Configuration to permanently save the updates.' and a 'Help' button is centered.

Figure 74 - SNMP System Configuration interface



## Trap Configuration

A trap manager is a management station that receives trap messages generated by the switch. If no trap manager is defined, no traps will be issued. 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 for the trap station.
- » **Trap Version:** Select the SNMP trap version—v1 or v2c.
- » When finished, select **Add**.
- » To remove a specific manager station, select the entries listed in the Current Managers field and select **Remove**.

The image shows a web-based configuration interface titled "SNMP - Trap Configuration". It has three tabs: "System Configuration", "Trap Configuration" (which is active), and "SNMPv3 Configuration". The main section is titled "Trap Managers" and is divided into two panels. The left panel, "Current Managers", has a "Remove" button and contains a table with one entry: "192.168.10.8; TrapHost1, v1". The right panel, "New Manager", has an "Add" button and contains fields for "IP Address", "Community", and "Trap version" (with radio buttons for "v1" and "v2c", where "v1" is selected). At the bottom, there is a message: "Please use Save Configuration to permanently save the updates." and a "Help" button.

Figure 75 - Trap Managers interface

## SNMPV3 Configuration

This tab allows users to configure the SNMPv3 settings for communications via SNMPv3.

### Context Table

Configure the SNMPv3 context table. Assign the context name in the field. Select **Apply** to add the context name added or changed.

### User Table

Configure the SNMPv3 user table.

- » **User ID:** Type the user name in the field.
- » **Authentication Password:** Assign the authentication password to the user ID.
- » **Privacy Password:** Assign the private password to the user ID.
- » Select the **Add** button to create a new user profile.
- » To remove a user profile, select an entry in the Current User Profiles list box and select the **Remove** button to remove the unwanted user profile.

### Group Table

Configure the SNMPv3 group table.

- » **Security Name (User ID):** Specify the user name that you have set up in the user table.
- » **Group Name:** Type the group name in the field.
- » Select the **Add** button to create a new group name
- » To remove a group name, select an entry in the Current Group Content list box and select the **Remove** button to remove the unwanted group.

## SNMP - SNMPv3 Configuration

System Configuration
Trap Configuration
SNMPv3 Configuration

### Context Table

Context Name :

Apply

### User Table

Current User Profiles : Remove

New User Profile : Add

(none)	<div>User ID: <input style="width: 80%;" type="text"/></div> <div>Authentication Password: <input style="width: 80%;" type="password"/></div> <div>Privacy Password: <input style="width: 80%;" type="password"/></div>
--------	---

### Group Table

Current Group content : Remove

New Group Table: Add

(none)	<div>Security Name (User ID): <input style="width: 80%;" type="text"/></div> <div>Group Name: <input style="width: 80%;" type="text"/></div>
--------	--

Figure 76 - SNMPv3 configuration interface

## Access Table

### Access Table

Current Access Tables : Remove

New Access Table : Add

(none)	<div>Context Prefix: <input style="width: 80%;" type="text"/></div> <div>Group Name: <input style="width: 80%;" type="text"/></div> <div>Security Level: <input type="radio"/> NoAuthNoPriv. <input type="radio"/> AuthNoPriv. <input type="radio"/> AuthPriv.</div> <div>Context Match Rule <input type="radio"/> Exact <input type="radio"/> Prefix</div> <div>Read View Name: <input style="width: 80%;" type="text"/></div> <div>Write View Name: <input style="width: 80%;" type="text"/></div> <div>Notify View Name: <input style="width: 80%;" type="text"/></div>
--------	--

### MIBView Table

Current MIBTables : Remove

New MIBView Table : Add

(none)	<div>View Name: <input style="width: 80%;" type="text"/></div> <div>SubOid-Tree: <input style="width: 80%;" type="text"/></div> <div>Type: <input type="radio"/> Excluded <input type="radio"/> Included</div>
--------	--

Any modification of SNMPv3 tables might cause MIB accessing rejection.  
 Please take notice of the causality between the tables before you modify these tables.  
 Please use Save Configuration to permanently save the updates.

Help

Figure 77 - Configure the SNMPv3 access table

- » **Context Prefix:** In this field type in the prefix letters of the context name that is assigned in the context table.
- » **Group Name:** Type in the group name that is assigned in the group table.
- » **Security Level:** Select a radio button to determine which security level is assigned to the group. The options include:
  - › **NoAuthNoPriv:** Communications are made without authentication or encryption.
  - › **AuthNoPriv:** Communications are made with authentication but without encryption.
  - › **AuthPriv:** Communications are made with authentication and encryption.
- » **Context Match Rule:** Select the radio button to determine the context-matching rule. You can configure it as a complete matching or prefix matching condition.
- » **Read View Name:** Assign permission of reading to a user ID type that exists in the User Table.
- » **Write View Name:** Assign permission of writing to a user ID type that exists in the User Table.
- » **Notify View Name:** Assign permission of notifying a user ID type that exists in the User Table.
- » Select **Add** to create a new access entry.
- » Select an entry in the Current Access Tables list box and select **Remove** to delete the unwanted access entry.

## MIBview Table

Configure the SNMPv3 MIB view table.

- » **ViewName:** Type in a new view name in the field.
- » **Sub-OID Tree:** Type in the Sub OID that allows the view to access the objects of the level.
- » **Type:** Select the radio button to determine the view type - exclude or included.
- » Select **Add** to create a new entry.
- » Select **Remove** to delete the unwanted entry.

## QoS Configuration

In general, traffic on networks is treated as the same priority and delivered equally. With QoS enabled, users can classify frames or packets into different priorities to ensure specific network traffic is delivered on a foundation of best-effort. The incoming frames or packets can be sent to different priority queues for different priority service according to the configured policies.

### QoS Policy

Select one of the two radio buttons to determine the QoS policy—an **8-4-2-1 weighted fair queuing scheme** or a **strict priority scheme**. The 8-4-2-1 weighed fair queuing scheme designed with four queues to which allocate traffic in the rate of 8:4:2:1. As for the strict priority scheme, traffic will be identified according to the priority determined.

### QoS Policy

Select the QoS policy rule.

- » **Use an 8,4,2,1 weighted fair queuing scheme:** The switch will follow the ratio of 8:4:2:1 to process priority queues including High, Middle, Low and Lowest. For example, while the system processing, 1 frame in the lowest queue, 2 frames in the low queue, 4 frames in the middle queue, and 8 frames in the high queue will be processed at the same time in accordance with the 8,4,2,1 policy rule.
- » **Use a strict priority scheme:** With this radio button selected, you have to select the pull-down menu labeled **Priority Type**.
- » **Priority Type:** Five options **Port-based**, **TOS only**, **COS only**, **TOS first**, and **COS first**. **Disable** means QoS function is not activated.
- » Select **Apply** to have the configuration take effect.

The screenshot shows the 'QoS Configuration' interface. It has three main sections:

- QoS Policy:** Contains two radio buttons: 'Use an 8,4,2,1 weighted fair queuing scheme' (selected) and 'Use a strict priority scheme'. Below them is a 'Priority Type' dropdown menu set to 'Disable'. There are 'Apply' and 'Help' buttons.
- Port-based Priority:** A table with 18 columns labeled Port.01 through Port.18. Each column has a dropdown menu, all of which are currently set to 'Lowest'. There are 'Apply' and 'Help' buttons below the table.
- CoS:** A table with 8 columns labeled Priority 0 through 7. Each column has a dropdown menu, all of which are currently set to 'Lowest'. There are 'Apply' and 'Help' buttons below the table.

Figure 78 - QoS Configuration interface

## Port-based Priority

Configure the priority level for each port. Any packet received from a single port is sent to the **Lowest** queue by default. This item allows users to change the priority level for each port respectively.

- » **Port x:** Four priority levels are available – **High**, **Middle**, **Low**, and **Lowest**.
- » Select the **Apply** button to have the configuration take effect.

## CoS Configuration

Configure this item to allocate the identified packet to different queues according to the packet's 3-bit 802.1p priority classification field that is embedded in the 4-byte 802.1q VLAN tag field. Before configuring this field, users have to select the **Use a strict priority scheme** radio button and set the Priority Type on **COS only** or **COS first**.

- » **Priority:** The 3-bit 802.1p priority values range from 0 to 7. Select the pull-down menu to specify the corresponding queue for the identified COS value (priority) to which the identified frame will be sent.
- » Select the **Apply** button to have the configuration take effect.



## ToS Configuration

Configure this item to allocate the identified packet to different queues according to the packet's 6-bit DSCP (Differentiated Service Code Point) value inside the 1-byte ToS (Type of Service) field. The 6-bit DSCP value defines up to 64 priority values. Therefore, you can assign one of the four queues to each priority respectively.

- » **Priority:** Select the pull-down menu to specify the corresponding queue for the identified TOS (DSCP) value to which the identified packet will be sent.
- » Select the **Apply** button to have the configuration take effect.

**ToS:**

<b>Priority</b>	<b>0</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>
	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾
<b>Priority</b>	<b>8</b>	<b>9</b>	<b>10</b>	<b>11</b>	<b>12</b>	<b>13</b>	<b>14</b>	<b>15</b>
	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾
<b>Priority</b>	<b>16</b>	<b>17</b>	<b>18</b>	<b>19</b>	<b>20</b>	<b>21</b>	<b>22</b>	<b>23</b>
	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾
<b>Priority</b>	<b>24</b>	<b>25</b>	<b>26</b>	<b>27</b>	<b>28</b>	<b>29</b>	<b>30</b>	<b>31</b>
	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾
<b>Priority</b>	<b>32</b>	<b>33</b>	<b>34</b>	<b>35</b>	<b>36</b>	<b>37</b>	<b>38</b>	<b>39</b>
	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾
<b>Priority</b>	<b>40</b>	<b>41</b>	<b>42</b>	<b>43</b>	<b>44</b>	<b>45</b>	<b>46</b>	<b>47</b>
	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾
<b>Priority</b>	<b>48</b>	<b>49</b>	<b>50</b>	<b>51</b>	<b>52</b>	<b>53</b>	<b>54</b>	<b>55</b>
	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾
<b>Priority</b>	<b>56</b>	<b>57</b>	<b>58</b>	<b>59</b>	<b>60</b>	<b>61</b>	<b>62</b>	<b>63</b>
	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾

Figure 79 - Configure Port-based Priority

## X-Ring2

X-Ring provides a faster redundant recovery than the Spanning Tree topology. The action is similar to STP or RSTP, but the algorithms between them are not the same. To configure an X-Ring group, enable the X-Ring function on each switch whose two ports connecting to the ring group in which should be assigned as the member ports.

The two switches forming the last segment of a multi-device X-Ring group will automatically be designated as master switches, between which the connection is called the backup path. Known as backup ports, the two ports of the backup path will be blocked. Also, the user can identify whether the switch is the ring master device by checking the LED indicator on the panel of the switch.

Other switches in the X-Ring group are naturally the working (forwarding) switches and both their two member ports are working (forwarding) ports. If the failure of network connection occurs, the backup ports of master switches (ring master devices) will automatically become working (forwarding) ports to recover from the failure.

### X-Ring2 Operation Mode

Select the X-Ring2 Operation Mode pull-down menu to configure the operation mode for **X-Ring2** or **Disable** the X-Ring2 function.

### X-Ring2 Configuration

- » **Ring ID:** Specify a number ranging from 0 to 99 for identifying a given ring group.
- » **1st Ring Port:** One of the two member ports of this switch connecting to the ring group. Use the pull-down menu to select a port as the first ring port.
- » **2nd Ring Port:** The other member port of this switch connecting to the ring group. Use the pull-down menu to select a port as the second ring port.
- » **1st Rdn Port:** Use the pull-down menu to select a port as the first redundant port.
- » **1st Rdn Port ID:** Specify a number ranging from 0 to 99 for identifying the first redundant port.
- » **2nd Rdn Port:** Use the pull-down menu to select a port as the second redundant port.
- » **2nd Rdn Port ID:** Specify a number ranging from 0 to 99 for identifying the second redundant port.
- » When finished, select the **Add** button to save the configuration for this Ring ID.



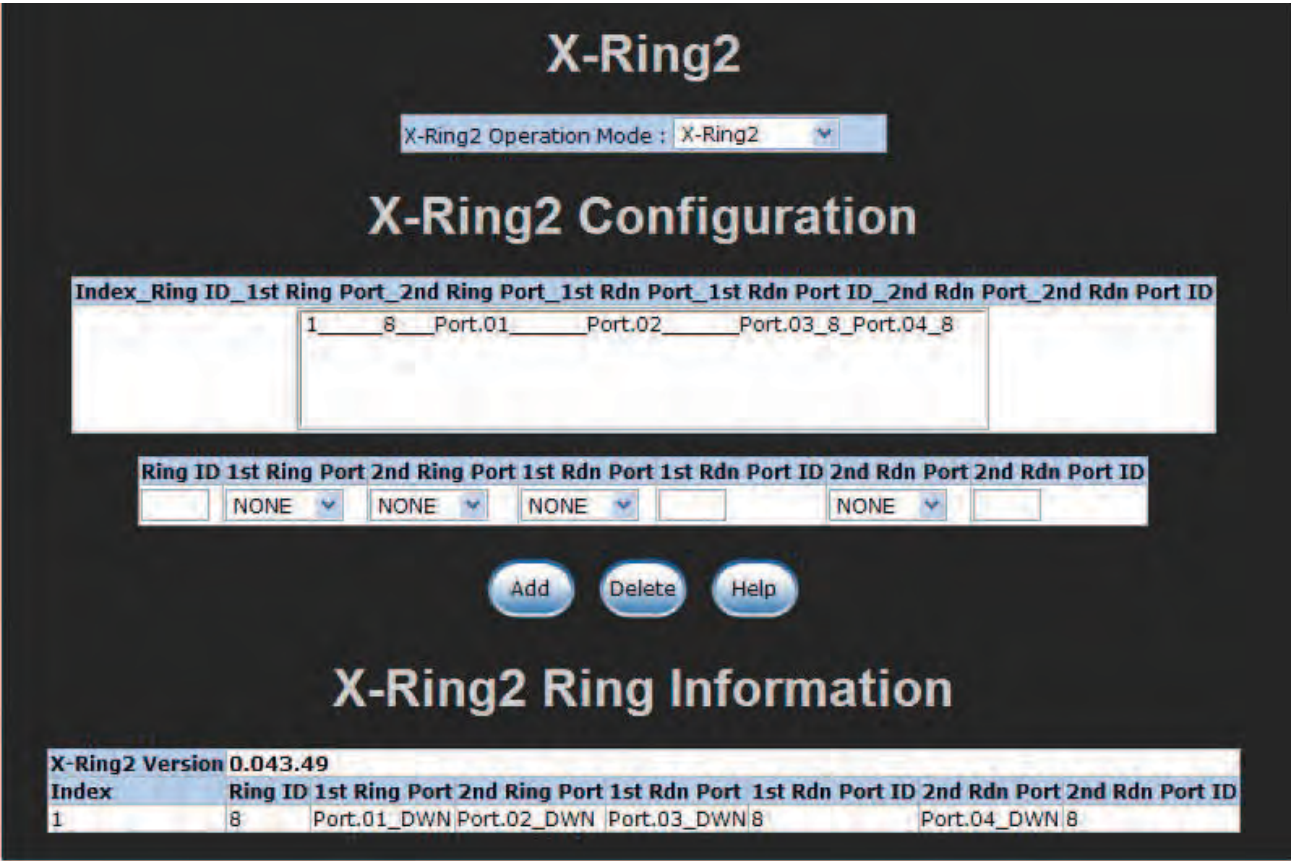


Figure 80 - X-Ring2 Interface

## X-Ring II Applications

X-Ring II is an enhanced X-Ring mechanism for ComNet industrial switches which eliminates the need to pre-define the Master Switch as it is in the X-Ring. It protects a network with the most secure topologies ever. X-Ring II works as a chain of rings to reduce the risk of master switch failure or link down. X-Ring II is backwards compatible with existing X-Ring topologies in legacy mode.

### Single X-Ring II

Recover Time: 10ms

Maximum switches: 256

Backup masters: 256

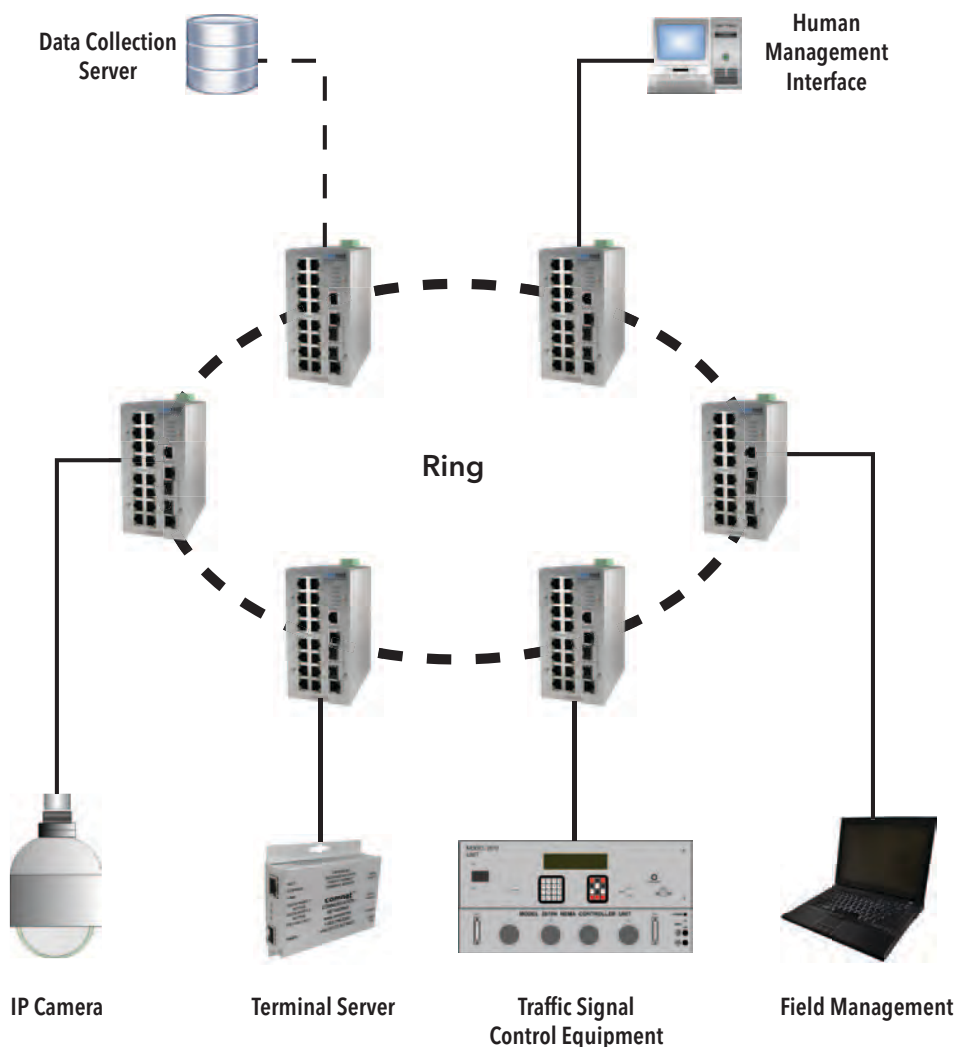


Figure 81 - Single X-Ring II Topology

## Coupled X-Ring II

Recover Time: 10ms

Maximum switches: 256

Backup masters: 256

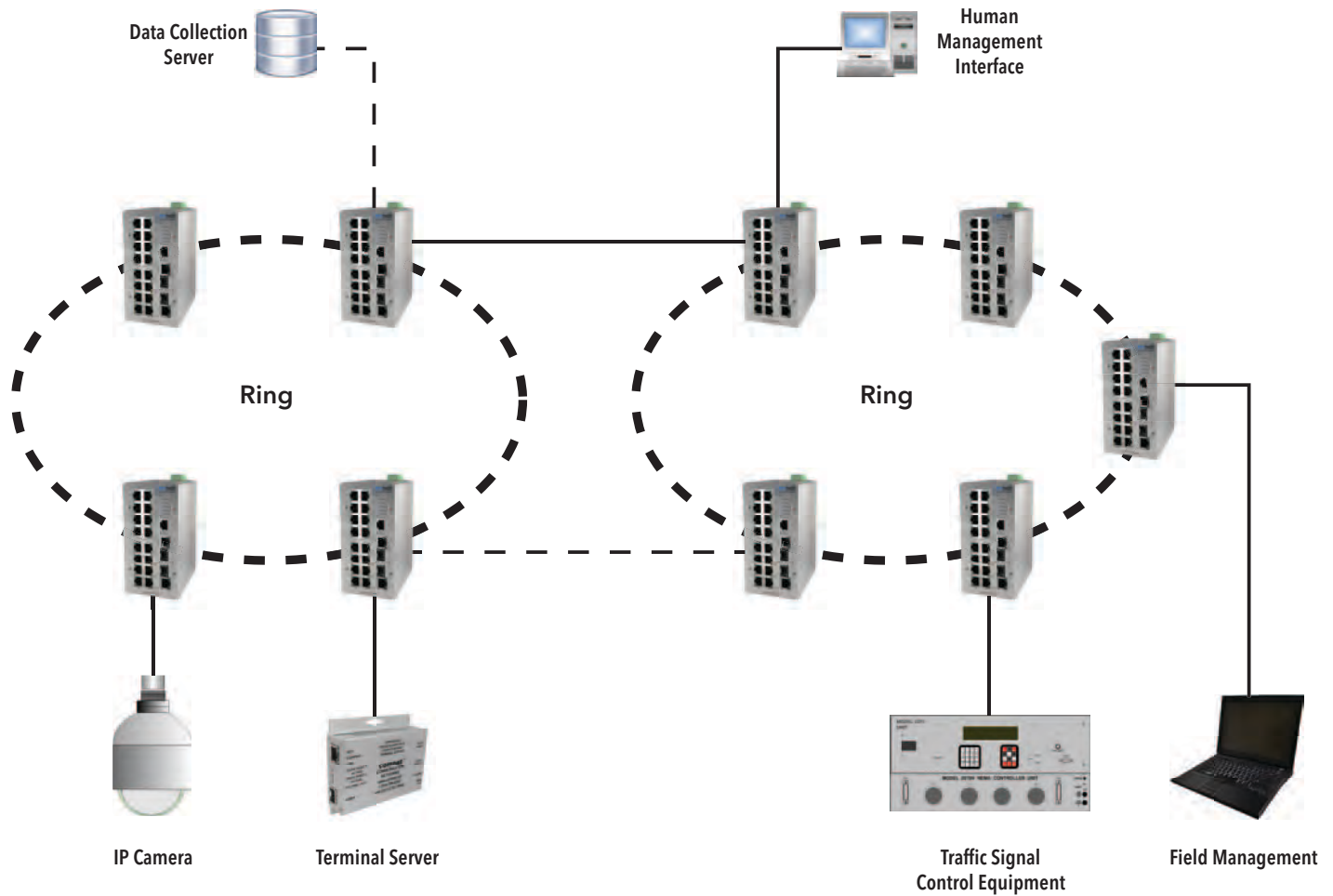


Figure 82 - Coupled X-Ring II Topology

## Multiple Coupled X-Ring II

Recover Time: 10ms

Maximum switches: 256

Backup masters: 256

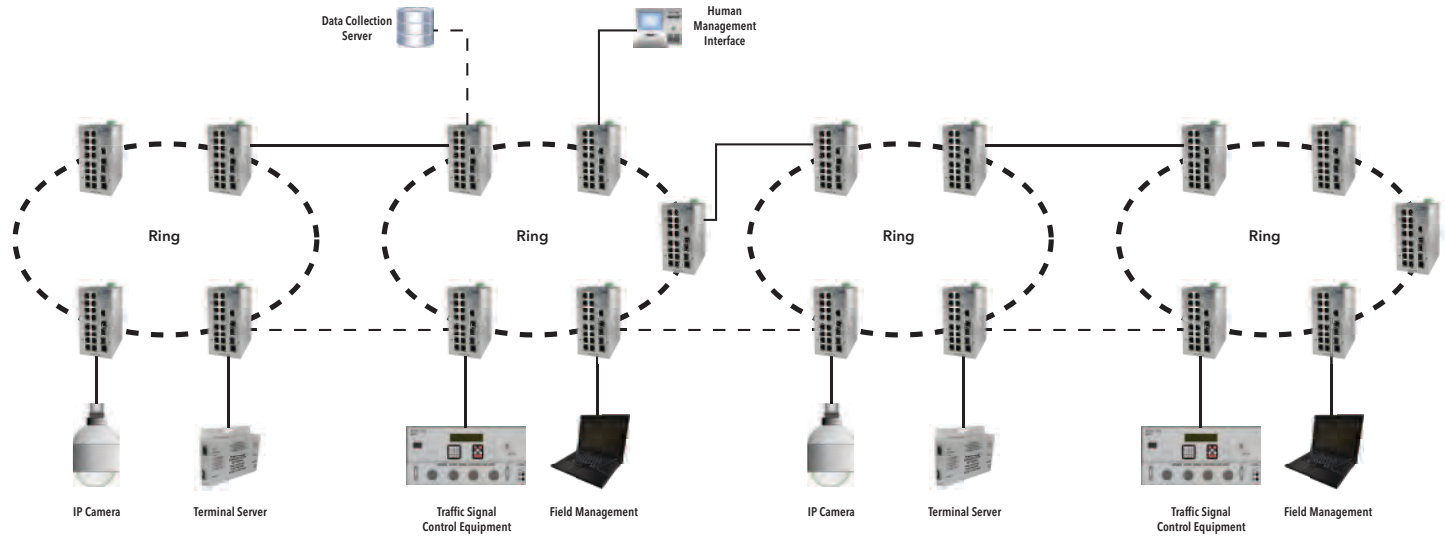


Figure 83 - Multiple Coupled X-Ring II Topology

## Dual Homing X-Ring II

RSTP ring: Recover Time: 10ms  
Maximum switches: 256  
Backup masters: 256

X-Ring II: Recover Time: 10ms  
Maximum switches: 50  
Backup masters: 50

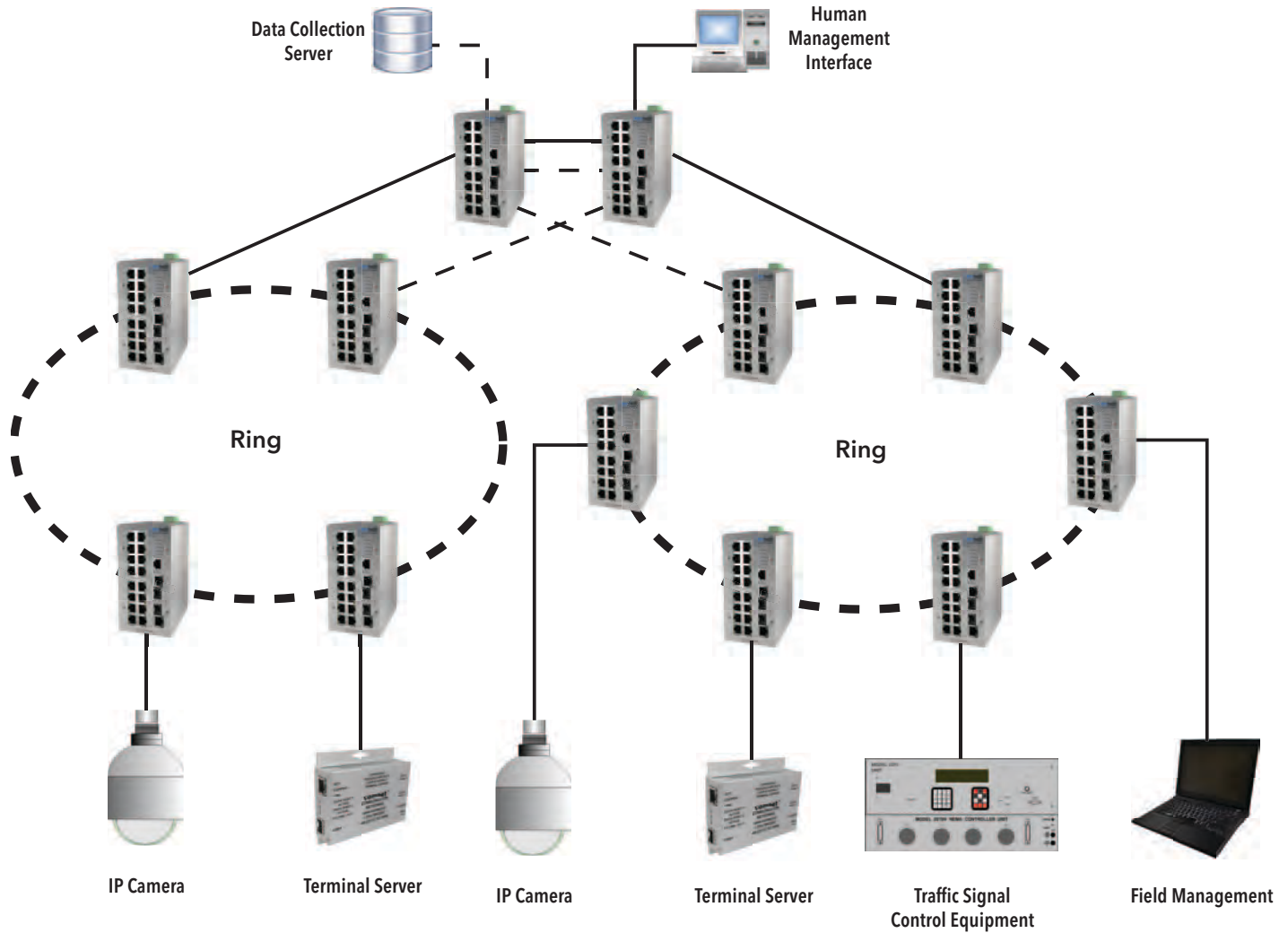


Figure 84 - Dual Homing X-Ring II Topology

## Dual Homing Three X-Ring II

Recover Time: 10ms

Maximum switches: 50

Backup masters: 50

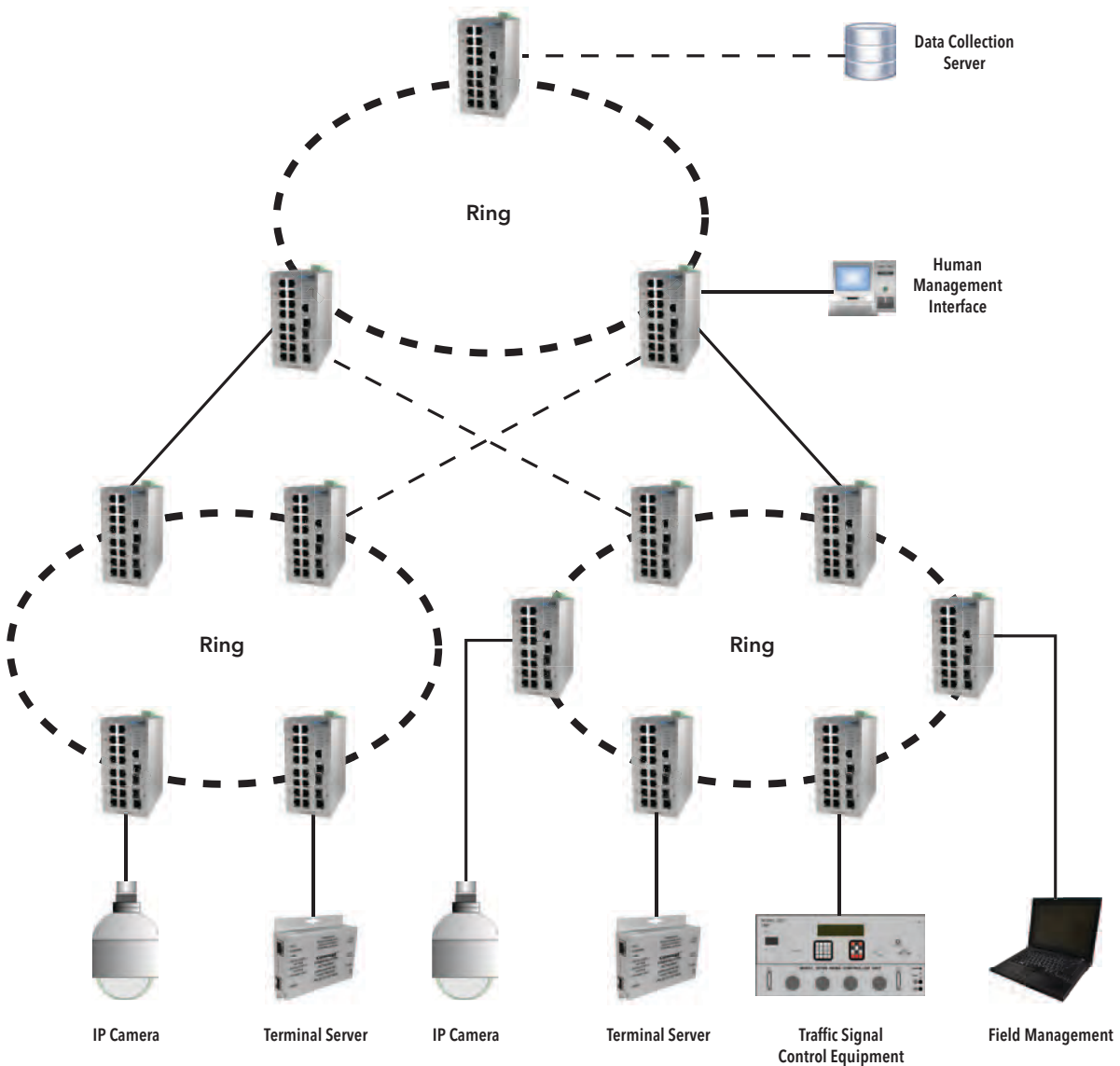


Figure 85 – Dual Homing Three X-Ring II Topology

## Legacy\_Ring Mode

Setting the X-Ring2 Operation Mode on **Legacy-Ring** mode means the switch is configured as a backward compatible device that could only be a non-master switch when joining a legacy X-Ring group.

- » **1st Ring Port:** Use the pull-down menu to select a port as the first ring port.
- » **2nd Ring Port:** Use the pull-down menu to select a port as the second ring port.
- » When finished, select the **Apply** button to have the configuration take effect.



Figure 86 - Legacy-Ring Interface

**Note:** When the X-Ring function is enabled, the user must disable the RSTP function. The X-Ring and RSTP functions cannot work simultaneously on a switch.

**Remember to execute the Save Configuration action, otherwise the new configuration will lose when the switch powers off.**

## LLDP Configuration

Link Layer Discovery Protocol (LLDP), a one-way protocol, specified in the IEEE 802.1ab standard allows stations attached to the same IEEE 802 LAN to advertise their information to neighbors and store the information received from adjacent stations.

Receivers on the same physical LAN will store the information distributed via LLDP in a standard Management Information Base (MIB) where the information can be accessed by a **Network Management System (NMS)** using a protocol like the **Simple Network Management Protocol (SNMP)**.

LLDP runs on all 802 media. The protocol runs over the data-link layer only, allowing two systems running different network layer protocols to learn about each other.

The switch also supports LLDP-MED (Media Endpoint Devices) that is the enhanced standard of the basic LLDP protocol that is specific to the requirements of Media Endpoint Devices in an IEEE 802 LAN environment. With LLDP-MED employed; the switch can deal with network configuration and policy, device location, Power over Ethernet management, and inventory management. Media Endpoint Devices include, but are not limited to, IP phones, IP voice/media gateways, IP media servers, and IP communications controllers.

- » **LLDP Protocol:** Use the pull-down menu to disable or enable the LLDP function.
- » **LLDP Interval:** Type the value, in seconds, as the interval for the switch to advertise its information to other nodes.
- » Select **Apply** to have the configuration take effect.



Figure 87 - LLDP Interface



## 802.1X/Radius

802.1x is an IEEE authentication specification that allows a client to connect to a wireless access point or wired switch but prevents the client from gaining access to the Internet until it provides authority, like a user name and password that are verified by a separate server.

### System Configuration

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

- » **IEEE 802.1x Protocol:** Use the pull-down menu to **Enable** or **Disable** the 802.1x protocol on the switch.
- » **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 the **Apply** button to have the configuration take effect.

802.1x/Radius - System Configuration	
System Configuration    Port Configuration    Misc Configuration	
802.1x Protocol	Enable ▾
Radius Server IP	192.168.10.100
Server Port	1812
Accounting Port	1813
Shared Key	12345678
NAS, Identifier	NAS_L2_SWITCH

Apply    Help

Please use Save Configuration to permanently save the updates.

Figure 88 - 802.1x System Configuration interface

## 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.
- » **Authorize**: 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 **Apply** to have the configuration take effect.

**802.1x/RADIUS - Port Configuration**

System Configuration | **Port Configuration** | Misc Configuration

Port	State
Port.01	Authorize
Port.02	Reject
Port.03	Accept
Port.04	Authorize
Port.05	Disable

Apply Help

Please use Save Configuration to permanently save the updates.

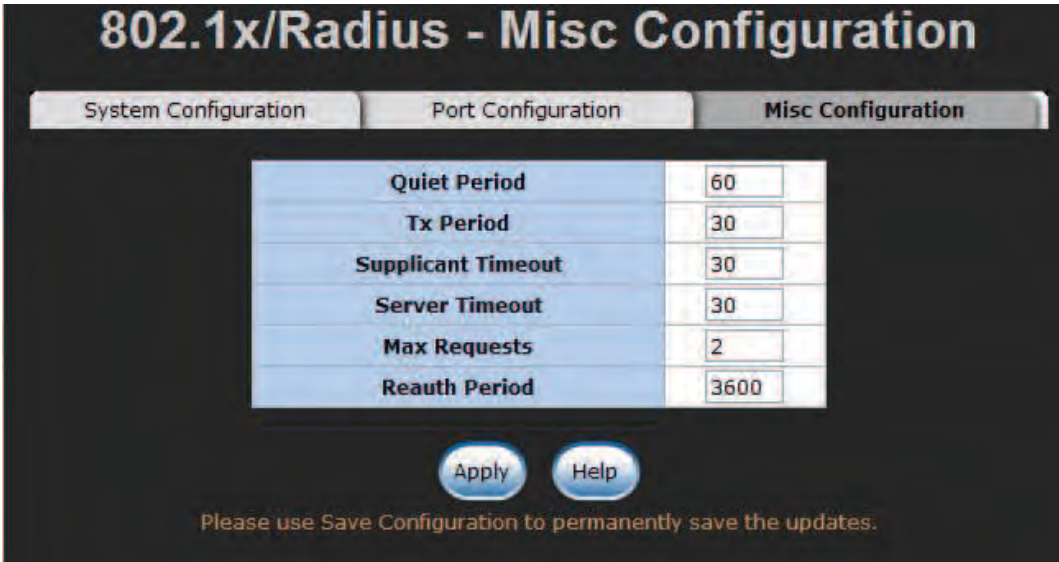
**Port Authorization**

Port	State
Port.01	Authorize
Port.02	Disable
Port.03	Disable
Port.04	Disable
Port.05	Disable
Port.06	Disable
Port.07	Disable
Port.08	Disable
Port.09	Disable
Port.10	Disable
Port.11	Disable
Port.12	Disable
Port.13	Disable
Port.14	Disable
Port.15	Disable
Port.16	Disable
Port.17	Disable
Port.18	Disable

Figure 89 – 802.1x Per Port Setting interface

## Misc Configuration

- » **Quiet Period:** Set the period that the port does not try to acquire a supplicant.
- » **TX Period:** Set the period the port waits for retransmitting the next EAPOL PDU during an authentication session.
- » **Supplicant Timeout:** Set the period of time the switch waits for a supplicant response to an EAP request.
- » **Server Timeout:** Set the period of time the switch waits for a server response to an authentication request.
- » **Max Requests:** Set the number of authentication that must time-out before authentication fails and the authentication session ends.
- » **Reauth Period:** Set the period of time the connected clients authenticated to be authenticated again.
- » Select **Apply** to have the configuration take effect.



The image shows a web-based configuration interface titled "802.1x/RADIUS - Misc Configuration". It features three tabs: "System Configuration", "Port Configuration", and "Misc Configuration", with the latter being the active tab. Below the tabs is a table with six rows, each containing a configuration parameter and its value in a text input field. The parameters and their values are: Quiet Period (60), Tx Period (30), Supplicant Timeout (30), Server Timeout (30), Max Requests (2), and Reauth Period (3600). Below the table are two buttons: "Apply" and "Help". At the bottom, a message states: "Please use Save Configuration to permanently save the updates."

Parameter	Value
Quiet Period	60
Tx Period	30
Supplicant Timeout	30
Server Timeout	30
Max Requests	2
Reauth Period	3600

Figure 90 – 802.1x Misc Configuration interface

## MAC Address Table

Here users can determine whether the incoming traffic passes through the particular ports or is blocked in accordance with the MAC-address filtering table.

### Static MAC Address

Configure the static MAC address tab to make a list in which traffic from devices with the MAC address included will pass the port. You can add a static MAC address that 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. Via this interface, you can add, modify and delete entries of static MAC address.

### Add the Static MAC Address

You can enter up to 256 static MAC addresses in the switch MAC Address Table here.

- » **MAC Address:** Enter entries of MAC address on the port that should permanently forward traffic, regardless of the device network activity.
- » **Port No.:** Use the pull-down menu to select the port number.
- » Select the **Add** button to finish adding the entry.
- » If you want to delete the entry from the table, select the MAC address entry listed in the list and select the **Delete** button.

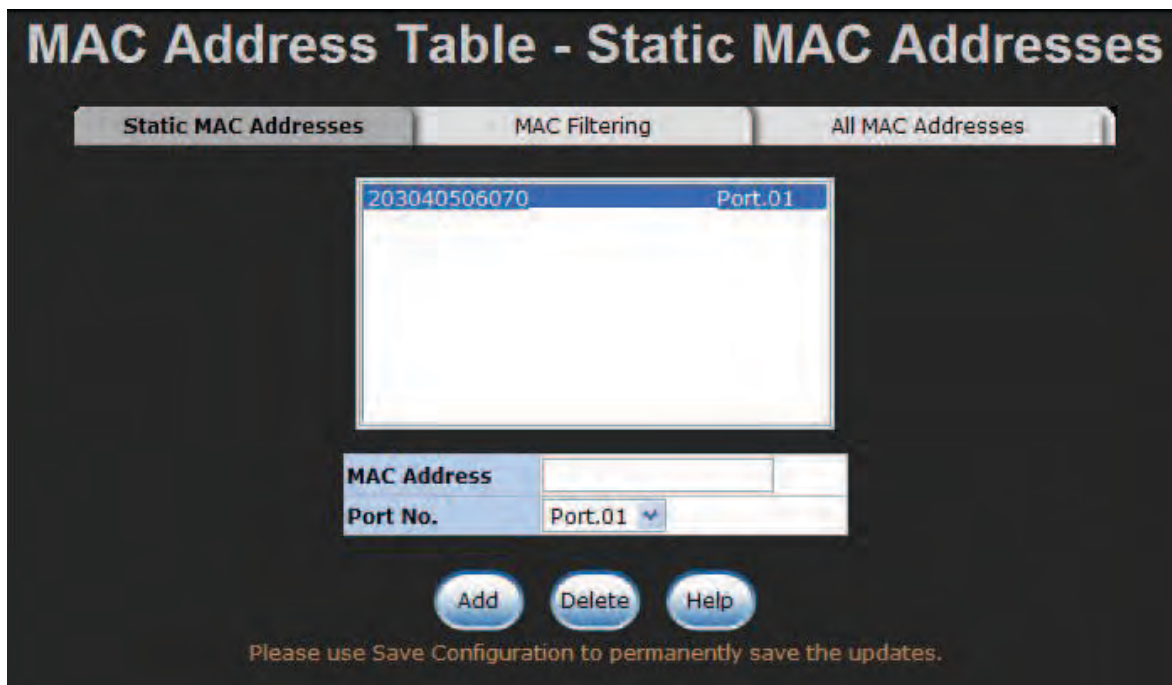


Figure 91 – Static MAC Addresses interface

## MAC Filtering

The switch will block traffic from devices with the MAC address listed in this table.

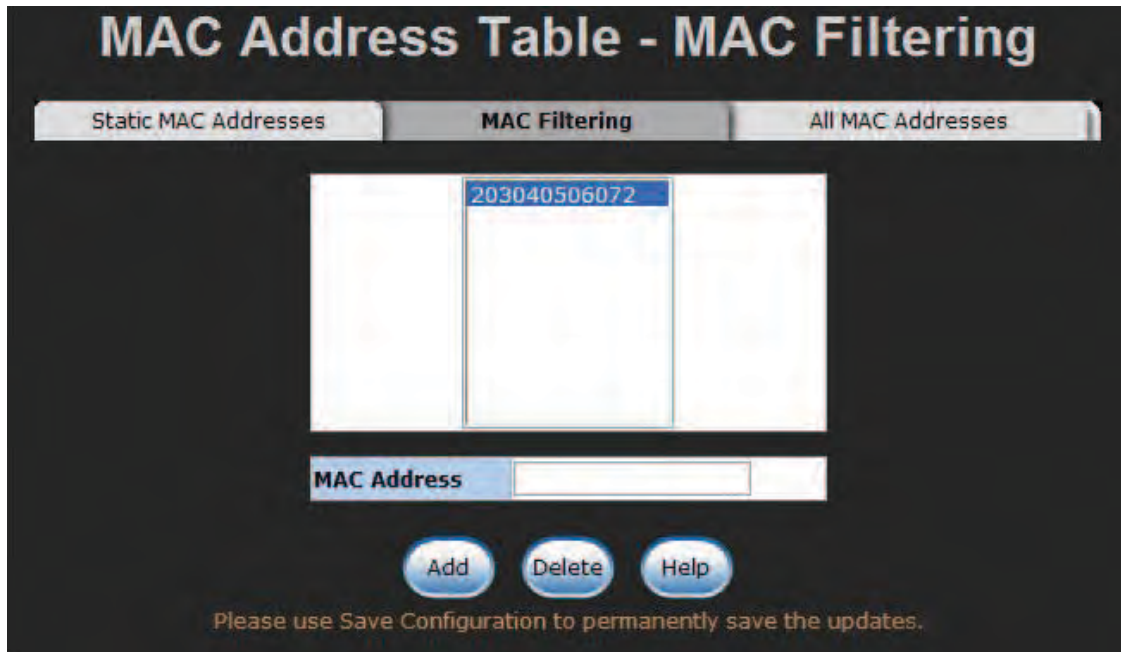


Figure 92 - MAC Filtering interface

- » **MAC Address:** Enter up to 256 MAC addresses.
- » Select the **Add** button.
- » If you want to delete the MAC address from the table, select the MAC address entry and select the **Delete** button.

## All MAC Addresses

This tab displays dynamic and static MAC addresses on each port.

- » **Port No:** Use the pull-down menu to select a particular port to show its MAC address information.
- » Select the **Clear MAC Table** button to clear the listed entries of the current MAC address information.



Figure 93 - All MAC Address interface



## IGMP/MLD Snooping

IGMP is the protocol used by IPv4 systems to report their IP multicast group memberships to neighboring multicast routers. To handle multicast management on IPv6 networks, Multicast Listener Discovery (MLD) is used in a similar way by IPv6 systems.

With the switch supporting IP multicast, you can enable IGMP/MLD protocol via this interface. Destination IP multicast addresses range from 224.0.0.0 to 239.255.255.255.

- » **Mode:** Use the pull-down menu to specify the snooping mode, IGMP or MLD.
- » **Query:** Use the pull-down menu to select the IGMP query functions including **Enable**, **Disable** and **Auto**.
- » Select **Apply** to have the configuration take effect.

IP Address	VLAN ID	Member Port
------------	---------	-------------

Mode: Disable

Query: Enable

Apply Help

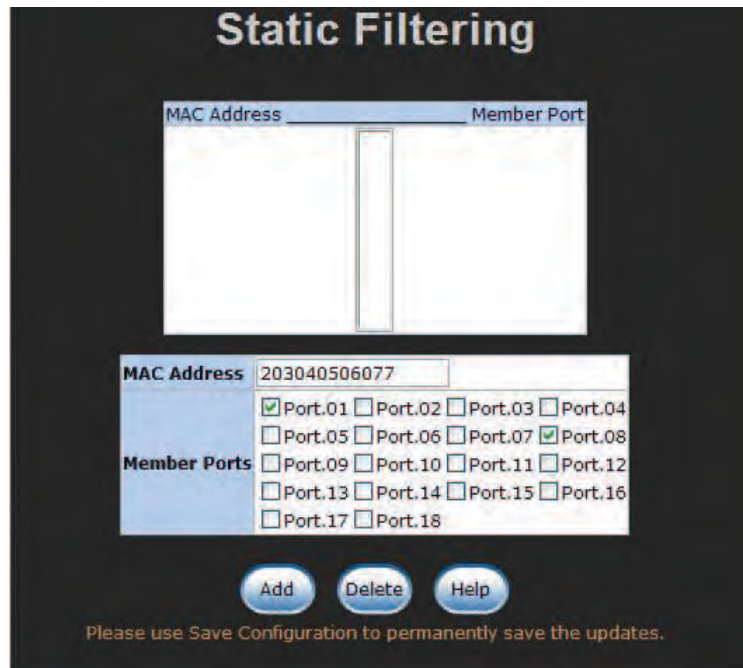
Figure 94 - IGMP/MLD Snooping interface



## Static Filtering

Multicasts are similar to broadcasts, they are sent to all end stations on a LAN or VLAN. Static filtering is the function for users to configure a list of multicast groups by specifying the multicast MAC address and member ports for each entry. A multicast MAC address is expressed in the format with a 24-bit prefix: **01-00-5E** (Hexadecimal). For example, you should give a multicast MAC address like 01-00-5E-xx-xx-xx for the multicast group from which end stations can receive multicast traffic via the connected ports that have been included in the specific multicast groups. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to the registered end stations.

- » **MAC Address:** Assign a multicast group MAC address in the format of 01-00-5E-xx-xx-xx.
- » **Member Ports:** Select the checkboxes beside the port number to include them as the member ports in the specific multicast group MAC address.
- » Select **Add** to append a static filter of multicast group, or select the filter listed in the field and select **Delete** to remove it.



The screenshot shows the 'Static Filtering' configuration window. At the top, there is a table with two columns: 'MAC Address' and 'Member Port'. Below this, there is a form for adding a new entry. The 'MAC Address' field contains '203040506077'. The 'Member Ports' section contains 18 checkboxes, with 'Port.01' and 'Port.08' checked. At the bottom, there are three buttons: 'Add', 'Delete', and 'Help'. A note at the bottom states: 'Please use Save Configuration to permanently save the updates.'

Figure 95 - Static Filtering interface

## Factory Default

- » Select the **Reset** button to reset the switch back to factory defaults. Before resetting, you can select the checkboxes to keep the current IP address and user name/password.

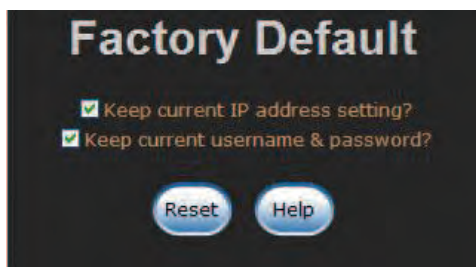


Figure 96 - Factory Default interface

## Save Configuration

- » Save all changes you have made in the system. To ensure the configurations you have made will be implemented the next time you power on the switch, remember to select the **Save** button to save all configurations into the flash memory.

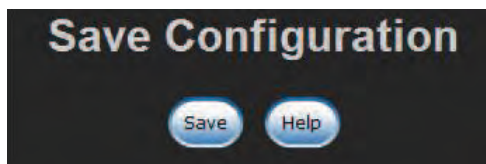


Figure 97 - Save Configuration interface

## System Reboot

- » Reboot the switch under software control. Select the **Reboot** button to restart the system.

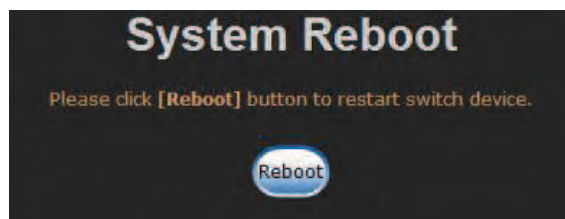


Figure 98 - System Reboot interface

## Troubleshooting

- » Verify that you are using the right power cord/adaptor. Do not use a power adapter with DC output higher than the rated voltage of the switch. This will result in severe damage.
- » Select the proper network cable to construct your network. Please confirm that you are using the correct cable.
- » Diagnosing LED Indicators: The Ethernet switch can be easily monitored through LED indicators on the front panel. These indicators describe common problems you may encounter and where you can find possible solutions to assist in identifying and solving problems.
- » If the power indicator does not light up when the power cord is plugged in, you may have a problem with your power cord. Check for loose power connections, power losses or surges at the power outlet. If you still cannot resolve the problem, contact your local dealer for assistance.
- » If the LED indicators are normal while the connected cables are correct but the packets still cannot transmit, please check your system's Ethernet devices' configuration or status.

## Appendix A—Command Sets

### Command Level

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

Modes	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with your switch.	switch>	Enter <b>logout</b> or <b>quit</b> .	The user commands available at the user level are a subset of those available at the privileged level. Use this mode to <ul style="list-style-type: none"> <li>• Perform basic tests.</li> <li>• Displays system information.</li> </ul>
Privileged EXEC	Enter the enable command while in user EXEC mode.	switch#	Enter <b>disable</b> to exit.	The privileged commands are the advanced mode. Use this mode to <ul style="list-style-type: none"> <li>• Display advance function states</li> <li>• Save configurations</li> </ul>
Global Configuration	Enter the configure command while in privileged EXEC mode.	switch (config)#	To exit to Privileged EXEC mode, enter <b>exit</b> or <b>end</b>	Use this mode to configure parameters to be applied to your switch.
VLAN database	Enter the vlan database command while in privileged EXEC mode.	switch (vlan)#	To return to User EXEC mode, enter <b>exit</b> .	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the interface command with a specific interface while in global configuration mode	switch (config-if)#	To return to the previous mode, enter <b>exit</b> or <b>end</b> .	Use this mode to configure parameters for the switch and Ethernet ports.

## System Commands Set

Commands	Level	Description	Example
show config	E	Show switch configuration	switch> <b>show config</b>
show terminal	P	Show console information	switch# <b>show terminal</b>
write memory	P	Save user configuration into permanent memory (flash rom)	switch# <b>write memory</b>
<b>system name</b> [System Name]	G	Configure system name	switch(config)# <b>system name xxx</b>
<b>system location</b> [System Location]	G	Set switch system location string	switch(config)# <b>system location xxx</b>
<b>system description</b> [System Description]	G	Set switch system description string	switch(config)# <b>system description xxx</b>
<b>system contact</b> [System Contact]	G	Set switch system contact window string	switch(config)# <b>system contact xxx</b>
show system-info	E	Show system information	switch> <b>show system-info</b>
<b>ip address</b> [Ip-address] [Subnet-mask] [Gateway]	G	Configure the IP address of switch	switch(config)# <b>ip address 192.168.1.1 255.255.255.0 192.168.1.254</b>
<b>ip dhcp</b>	G	Enable DHCP client function of switch	switch(config)# <b>ip dhcp</b>
show ip	P	Show IP information of switch	switch# <b>show ip</b>
<b>no ip dhcp</b>	G	Disable DHCP client function of switch	switch(config)# <b>no ip dhcp</b>
reload	G	Halt and perform a cold restart	switch(config)# <b>reload</b> Do you want reboot the device now? <b>yes</b>
default	G	Restore to default	switch(config)# <b>default</b> Keep current IP address setting? <b>yes</b> Keep current user ID/password? <b>yes</b> Default setting restored. Do you want to reboot the system now? <b>yes</b>
<b>admin username</b> [Username]	G	Configure the administrator's login username. (maximum 10 words)	switch(config)# <b>admin username xxxxxx</b>
<b>admin password</b> [Password]	G	Configure the password for the administrator account (maximum 10 words)	switch(config)# <b>admin password xxxxxx</b>
show admin	P	Show administrator information	switch# <b>show admin</b>
<b>guest username</b> [Username]	G	Configure the guest's login username	switch(config)# <b>guest username xxxxxx</b>

guest password [Password]	G	Configure the password for for the guest account	switch(config)# <b>guest password xxxxxx</b>
show guest	P	Show guest information	switch# <b>show guest</b>
dhcpserver enable	G	Enable DHCP Server	switch(config)# <b>dhcpserver enable</b>
dhcpserver lowip [Low IP]	G	Configure low IP address for IP pool	switch(config)# <b>dhcpserver lowip 192.168.1.100</b>
dhcpserver highip [High IP]	G	Configure high IP address for IP pool	switch(config)# <b>dhcpserver highip 192.168.1.200</b>
dhcpserver subnetmask [Subnet mask]	G	Configure subnet mask for DHCP clients	switch(config)# <b>dhcpserver subnetmask 255.255.255.0</b>
dhcpserver gateway [Gateway]	G	Configure gateway for DHCP clients	switch(config)# <b>dhcpserver gateway 192.168.1.254</b>
dhcpserver dnsip [DNS IP]	G	Configure DNS IP for DHCP clients	switch(config)# <b>dhcpserver dnsip 192.168.1.1</b>
dhcpserver leasetime [sec.]	G	Configure lease time in seconds	switch(config)# <b>dhcpserver leasetime 1</b>
dhcpserver ipbinding [IP address]	I	Set static IP for DHCP clients by port	switch(config)# <b>interface fastEthernet 2</b> switch(config-if)# <b>dhcpserver ipbinding 192.168.1.1</b>
show dhcpserver configuration	P	Show configuration of DHCP server	switch# <b>show dhcpserver configuration</b>
show dhcpserver clients	P	Show client entries of DHCP server	switch# <b>show dhcpserver clients</b>
show dhcpserver ip-binding	P	Show IP-Binding information of DHCP server	switch# <b>show dhcpserver ip-binding</b>
no dhcpserver	G	Disable DHCP server function	switch(config)# <b>no dhcpserver</b>
security enable	G	Enable IP security function	switch(config)# <b>security enable</b>
security http	G	Enable IP security of HTTP server	switch(config)# <b>security http</b>
security telnet	G	Enable IP security of telnet server	switch(config)# <b>security telnet</b>
security ip [Index(1..10)] [IP Address]	G	Set the IP security list	switch(config)# <b>security ip 1 192.168.1.55</b>
show security	P	Show the information of IP security	switch# <b>show security</b>
no security	G	Disable IP security function	switch(config)# <b>no security</b>
no security http	G	Disable IP security of HTTP server	switch(config)# <b>no security http</b>
no security telnet	G	Disable IP security of telnet server	switch(config)# <b>no security telnet</b>

## Port Commands Set

Commands	Level	Description	Example
<code>interface fastEthernet</code> [Portid]	G	Choose the port for modification.	<code>switch(config)#interface fastEthernet 2</code>
<code>state</code> [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.	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#state disable</code>
<code>duplex</code> [full   half]	I	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#duplex full</code>
<code>speed</code> [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.	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#speed 100</code>
<code>flowcontrol</code> [enable disable]	I	Configure flow control	<code>switch(config-if)# flowcontrol enable</code>
<code>security enable</code>	I	Enable security of interface	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#security enable</code>
<code>no security</code>	I	Disable security of interface	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#no security</code>
<code>bandwidth type all</code>	I	Set interface ingress limit frame type to "accept all frame"	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#bandwidth type all</code>
<code>bandwidth type broadcast-multicast-flooded-unicast</code>	I	Set interface ingress limit frame type to "accept broadcast, multicast, and flooded unicast frame"	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#bandwidth type broadcast-multicast-flooded-unicast</code>
<code>bandwidth type broadcast-multicast</code>	I	Set interface ingress limit frame type to "accept broadcast and multicast frame"	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#bandwidth type broadcast-multicast</code>
<code>bandwidth type broadcast-only</code>	I	Set interface ingress limit frame type to "only accept broadcast frame"	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#bandwidth type broadcast-only</code>



<code>bandwidth in</code> [0/160/320/512/768/1024/1280/1536/2048/3072/4096/5120/8192/10240/20480/30720/40960/61440/81920/128000]		Set interface input bandwidth. Zero means no limit.	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#bandwidth in 160</code>
<code>bandwidth out</code> [0/160/320/512/768/1024/1280/1536/2048/3072/4096/5120/8192/10240/20480/30720/40960/61440/81920/128000]		Set interface output bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports. Zero means no limit.	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#bandwidth out 160</code>
<code>show bandwidth</code>		Show interfaces bandwidth control	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#show bandwidth</code>
<code>alias [name]</code>		Set port alias name	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#alias 1111</code>
<code>show interface configuration</code>		show interface configuration status	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#show interface configuration</code>
<code>show interface status</code>		show interface actual status	<code>switch(config)#interface fastEthernet 2</code> <code>switch switch (config-if)#show interface status</code>
<code>show interface accounting</code>		show interface statistic counter	<code>switch(config)#interface fastEthernet 2</code> <code>switch switch (config-if)#show interface accounting</code>
<code>no accounting</code>		Clear interface accounting information	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#no accounting</code>

## Trunk Commands Set

Commands	Level	Description	Example
<code>aggregator priority</code> [1~65535]	G	Set port group system priority	<code>switch(config)#<b>aggregator priority 22</b></code>
<code>aggregator group</code> [GroupID] [Port-list] <code>lacp</code> <code>workp</code> [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 greater than the amount of member ports.	<code>switch(config)#<b>aggregator group 1 1-4 lacp workp 2</b></code> or <code>switch(config)#<b>aggregator group 2 1,4,3 lacp workp 3</b></code>
<code>aggregator activityport</code> [Group ID] [Port Numbers]	G	Set activity port	<code>switch(config)#<b>aggregator activityport 1 2</b></code>
<code>aggregator group</code> [GroupID] [Port-list] <code>nolacp</code>	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).	<code>switch(config)#<b>aggregator group 1 2-4 nolacp</b></code> or <code>switch(config)#<b>aggregator group 1 3,1,2 nolacp</b></code>
<code>show aggregator</code>	P	Show the information of trunk group	<code>switch#<b>show aggregator 1</b></code> or <code>switch#<b>show aggregator 2</b></code> or <code>switch#<b>show aggregator 3</b></code>
<code>no aggregator lacp</code> [GroupID]	G	Disable the LACP function of trunk group	<code>switch(config)#<b>no aggregator lacp 1</b></code>
<code>no aggregator group</code> [GroupID]	G	Remove a trunk group	<code>switch(config)#<b>no aggregator group 1</b></code>

## DMI Commands Set

Commands	Level	Description	Example
show dmi	I	Display DMI status for Mini-GBIC ports	switch(config)# <b>interface fastEthernet 7</b> switch(config-if)# <b>show dmi</b>
<b>dmi temperature</b> [HighAlarm HighWarning LowWarning LowAlarm] [E-mail ShutDown]	I	Set reactions for port temperature monitoring	switch(config)# <b>interface fastEthernet 7</b> switch(config-if)# <b>dmi temperature highalarm shutdown</b>
<b>dmi voltage</b> [HighAlarm HighWarning LowWarning LowAlarm] [E-mail ShutDown]	I	Set reactions for port voltage monitoring	switch(config)# <b>interface fastEthernet 7</b> switch(config-if)# <b>dmi voltage highwarning e-mail</b>
<b>dmi current</b> [HighAlarm HighWarning LowWarning LowAlarm] [E-mail ShutDown]	I	Set reactions for port current monitoring	switch(config)# <b>interface fastEthernet 7</b> switch(config-if)# <b>dmi current highalarm shutdown</b>
<b>dmi txpwr</b> [HighAlarm HighWarning LowWarning LowAlarm] [E-mail ShutDown]	I	Set reactions for port transmitting power monitoring	switch(config)# <b>interface fastEthernet 7</b> switch(config-if)# <b>dmi txpwr highwarning e-mail</b>
<b>dmi rxpwr</b> [HighAlarm HighWarning LowWarning LowAlarm] [E-mail ShutDown]	I	Set reactions for port receiving power monitoring	switch(config)# <b>interface fastEthernet 7</b> switch(config-if)# <b>dmi rxpwr highalarm shutdown</b>

## VLAN Commands Set

Commands	Level	Description	Example
vlan database	P	Enter VLAN configure mode	switch# <b>vlan database</b>
vlanmode [802.1q   gvrp]	V	To set switch VLAN mode.	switch(vlan)# <b>vlanmode 802.1q</b> or switch(vlan)# <b>vlanmode gvrp</b>
no vlan	V	No VLAN	Switch(vlan)# <b>no vlan</b>
IEEE 802.1Q VLAN			
<b>vlan 8021q mnt-vid</b> [VID]	V	Configure management VID (0 means disabled)	switch(vlan)# <b>vlan 8021q mnt-vid 22</b> Is Management VLAN ID equal to Management Port VLAN ID? <b>yes</b>
<b>vlan 8021q name</b> [GroupName] <b>vid</b> [VID]	V	Change the name of VLAN group. If the group doesn't exist, this command can't be applied.	switch(vlan)# <b>vlan 8021q name test vid 22</b>

<code>vlan 8021q port</code> [PortNumber] <code>access-link untag</code> [UntaggedVID]	V	Assign an access link for VLAN by port. If the port belongs to a trunk group, this command can't be applied.	<code>switch(vlan)#vlan 8021q port 3 access-link untag 22</code>
<code>vlan 8021q port</code> [PortNumber] <code>trunk-link tag</code> [TaggedVID List]	V	Assign a trunk link for VLAN by port. If the port belongs to a trunk group, this command can't be applied.	<code>switch(vlan)#vlan 8021q port 3 trunk-link tag 2,3,6,99</code> or <code>switch(vlan)#vlan 8021q port 3 trunk-link tag 3-20</code>
<code>vlan 8021q port</code> [PortNumber] <code>hybrid-link untag</code> [UntaggedVID] <code>tag</code> [TaggedVID List]	V	Assign a hybrid link for VLAN by port. If the port belongs to a trunk group, this command can't be applied.	<code>switch(vlan)#vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8</code> or <code>switch(vlan)#vlan 8021q port 3 hybrid-link untag 5 tag 6-8</code>
<code>vlan 8021q port</code> [PortNumber] <code>qinq untag</code> [UntaggedVID] <code>tag</code> [TaggedVID List]	V	Assign a qinq link for VLAN by port. If the port belongs to a trunk group, this command can't be applied.	<code>switch(vlan)#vlan 8021q port 3 qinq untag 4 tag 3,6,8</code> or <code>switch(vlan)#vlan 8021q port 3 qinq untag 5 tag 6-8</code>
<code>vlan 8021q trunk</code> [PortNumber] <code>access-link untag</code> [UntaggedVID]	V	Assign an access link for VLAN by trunk group	<code>switch(vlan)#vlan 8021q trunk 3 access-link untag 33</code>
<code>vlan 8021q trunk</code> [PortNumber] <code>trunk-link tag</code> [TaggedVID List]	V	Assign a trunk link for VLAN by trunk group	<code>switch(vlan)#vlan 8021q trunk 3 trunk-link tag 2,3,6,99</code> or <code>switch(vlan)#vlan 8021q trunk 3 trunk-link tag 3-20</code>
<code>vlan 8021q trunk</code> [PortNumber] <code>hybrid-link untag</code> [UntaggedVID] <code>tag</code> [TaggedVID List]	V	Assign a hybrid link for VLAN by trunk group	<code>switch(vlan)#vlan 8021q trunk 3 hybrid-link untag 4 tag 3,6,8</code> or <code>switch(vlan)#vlan 8021q trunk 3 hybrid-link untag 5 tag 6-8</code>
<code>vlan 8021q trunk</code> [PortNumber] <code>qinq untag</code> [UntaggedVID] <code>tag</code> [TaggedVID List]	V	Assign a q-in-q link for VLAN by trunk group	<code>switch(vlan)#vlan 8021q trunk 3 qinq untag 4 tag 3,6,8</code> or <code>switch(vlan)#vlan 8021q trunk 3 qinq untag 5 tag 6-8</code>
<code>show vlan [GroupID]</code> or <code>show vlan</code>	V	Show VLAN information	<code>switch(vlan)#show vlan 2</code>
<code>no vlan group</code> [GroupID]	V	Delete the port-base group ID	<code>switch(vlan)#no vlan group 2</code>

## Spanning Tree Commands Set

Commands	Level	Description	Example
spanning-tree enable	<b>G</b>	Enable spanning tree	switch(config)# <b>spanning-tree enable</b>
spanning-tree priority [0~61440]	G	Configure spanning tree priority parameters	switch(config)# <b>spanning-tree priority 4096</b>
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 admin switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the admin switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	switch(config)# <b>spanning-tree max-age 15</b>
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)# <b>spanning-tree hello-time 3</b>
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)# <b>spanning-tree forward-time 20</b>
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 looping, the spanning tree considers the path cost when selecting an interface to place into the forwarding state.	switch(config)# <b>interface fastEthernet 2</b> switch(config-if)# <b>stp-path-cost 20</b>

<code>stp-path-priority</code> [0-240]	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 admin switch.	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#stp-path-priority 16</code>
<code>stp-admin-p2p</code> [Auto True False]	I	Configure Admin P2P of STP priority on this interface.	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#stp-admin-p2p Auto</code>
<code>stp-admin-edge</code> [True False]	I	Configure Admin Edge of STP priority on this interface.	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#stp-admin-edge True</code>
<code>stp-admin-non-stp</code> [True False]	I	Configure Admin NonSTP of STP priority on this interface.	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#stp-admin-non-stp False</code>
<code>show spanning-tree</code>	E	Display a summary of the spanning-tree states.	<code>switch&gt;show spanning-tree</code>
<code>no spanning-tree</code>	G	Disable spanning-tree.	<code>switch(config)#no spanning-tree</code>

## QoS Commands Set

Commands	Level	Description	Example
<code>qos policy</code> [weighted-fair strict]	G	Select QOS policy scheduling	<code>switch(config)#qos policy weighted-fair</code>
<code>qos prioritytype</code> [port-based cos-only tos-only cos-first tos-first]	G	Setting of QOS priority type	<code>switch(config)#qos prioritytype port-base</code>
<code>qos priority portbased</code> [Port] [lowest low middle high]	G	Configure Port-based Priority	<code>switch(config)#qos priority portbased 1 low</code>
<code>qos priority cos</code> [Priority] [lowest low middle high]	G	Configure COS Priority	<code>switch(config)#qos priority cos 0 middle</code>
<code>qos priority tos</code> [Priority] [lowest low middle high]	G	Configure TOS Priority	<code>switch(config)#qos priority tos 3 high</code>
<code>show qos</code>	P	Display information of QoS configuration	<code>Switch#show qos</code>
<code>no qos</code>	G	Disable QoS function	<code>switch(config)#no qos</code>

## IGMP Commands Set

Commands	Level	Description	Example
igmp enable	G	Enable IGMP snooping function	switch(config)# <b>igmp enable</b>
igmp query auto	G	Set IGMP query to auto mode	switch(config)# <b>igmp query auto</b>
igmp query enable	G	Set IGMP query to force mode	switch(config)# <b>igmp query enable</b>
<b>igmp unregister</b> [flooding/blocking]	G	Configure IGMP unregister stream	switch(config)# <b>igmp unregister flooding</b>
show igmp configuration	P	Displays the details of an IGMP configuration.	switch# <b>show igmp configuration</b>
show igmp multi	P	Displays the details of an IGMP snooping entries.	switch# <b>show igmp multi</b>
no igmp	G	Disable IGMP snooping function	switch(config)# <b>no igmp</b>
no igmp query	G	Disable IGMP query	switch(config)# <b>no igmp query</b>

## MLD Commands Set

Commands	Level	Description	Example
mld enable	G	Enable MLD function	switch(config)# <b>mld enable</b>
mld query auto	G	Configure MLD query mode	switch(config)# <b>mld query auto</b>
mld query enable	G	Set MLD query to force mode	switch(config)# <b>mld query enable</b>
<b>mld unregister</b> [flooding/blocking]	G	Configure MLD unregister stream	switch(config)# <b>igmp unregister flooding</b>
show mld configuration	P	Show MLD configuration	switch# <b>show mld configuration</b>
show mld multi	P	Show MLD multicast table	switch# <b>show mld multi</b>
no mld	G	Disable MLD snooping function	switch(config)# <b>no mld</b>
no mld query	G	Disable MLD query function	switch# <b>no mld query</b>



## Multicast Static Filtering Table Commands Set

Commands	Level	Description	Example
<code>multicast-filtering</code> [IP-Addr]	I	Add entries for the multicast filtering.	<code>switch(config)#interface</code> <b><code>fastEthernet 2</code></b> <code>switch(config-if)# multicast-filtering</code> <b><code>01-00-5e-00-00-01</code></b> or <code>switch(config-if)# multicast-filtering</code> <b><code>33-33-00-00-00-01</code></b>
<b><code>no multicast-filtering</code></b> <b>[IP-Addr]</b>	I	Remove entries for the multicast filtering.	<code>switch(config)#interface</code> <b><code>fastEthernet 2</code></b> <code>switch(config-if)#no multicast-</code> <b><code>filtering 01-00-5e-00-00-01</code></b> or <code>switch(config-if)# no multicast-</code> <b><code>filtering 33-33-00-00-00-01</code></b>

## MAC / Filter Table Commands Set

Commands	Level	Description	Example
<code>mac-address-table static</code> <code>hwaddr</code> [MAC]	I	Configure the MAC address table (static).	<code>switch(config)#interface</code> <b><code>fastEthernet 2</code></b> <code>switch(config-if)#mac-address-table</code> <b><code>static hwaddr 000012345678</code></b>
<code>mac-address-table filter</code> <code>hwaddr</code> [MAC]	G	Configure the MAC address table (filter)	<code>switch(config)#mac-address-table</code> <b><code>filter hwaddr 000012348678</code></b>
<code>show mac-address-table</code>	P	Show the table with all MAC addresses	<code>switch#show mac-address-table</code>
<code>show mac-address-table static</code>	P	Show the table with static MAC addresses	<code>switch#show mac-address-table</code> <b><code>static</code></b>
<code>show mac-address-table filter</code>	P	Show entries of the filter MAC address table.	<code>switch#show mac-address-table</code> <b><code>filter</code></b>
<code>no mac-address-table static</code> <code>hwaddr</code> [MAC]	I	Remove an entry from the MAC address table (static)	<code>switch(config)#interface</code> <b><code>fastEthernet 2</code></b> <code>switch(config-if)#no mac-</code> <b><code>address-table static hwaddr</code></b> <b><code>000012345678</code></b>
<code>no mac-address-table filter</code> <code>hwaddr</code> [MAC]	G	Remove an entry from the MAC address table (filter)	<code>switch(config)#no mac-address-</code> <b><code>table filter hwaddr 000012348678</code></b>
<code>no mac-address-table</code>	G	Remove dynamic entries from the MAC address table	<code>switch(config)#no mac-address-</code> <b><code>table</code></b>

## SNMP Commands Set

Commands	Level	Description	Example
<code>snmp system-name</code> [System Name]	G	Set SNMP agent system name	<code>switch(config)#snmp system-name l2switch</code>
<code>snmp system-location</code> [System Location]	G	Set SNMP agent system location	<code>switch(config)#snmp system-location lab</code>
<code>snmp system-contact</code> [System Contact]	G	Set SNMP agent system contact	<code>switch(config)#snmp system-contact where</code>
<code>snmp agent-mode</code> [v1v2c v3 v1v2cv3]	G	Select the agent mode of SNMP	<code>switch(config)#snmp agent-mode v1v2cv3</code>
<code>snmp community-strings</code> [Community] right [RO/RW]	G	Add SNMP community string.	<code>switch(config)#snmp community-strings public right rw</code>
<code>snmp-server host</code> [IP address] <code>community</code> [Community-string] <code>trap-version</code> [v1 v2c]	G	Configure SNMP server host information and community string	<code>switch(config)#snmp-server host 192.168.1.50 community public trap-version v1</code>
<code>snmpv3 context-name</code> [Context Name ]	G	Configure the context name	<code>switch(config)#snmpv3 context-name Test</code>
<code>snmpv3 user</code> [User Name] <code>group</code> [Group Name] <code>password</code> [Authentication Password] [Privacy Password]	G	Configure the userprofile for SNMPV3 agent. Privacy password can be empty.	<code>switch(config)#snmpv3 user test01 group G1 password AuthPW PrivPW</code>
<code>snmpv3 access context-name</code> [Context Name ] <code>group</code> [Group Name ] <code>security-level</code> [NoAuthNoPriv AuthNoPriv AuthPriv] <code>match-rule</code> [Exact Prefix] <code>views</code> [Read View Name] [Write View Name] [Notify View Name]	G	Configure the access table of the SNMPV3 agent	<code>switch(config)#snmpv3 access context-name Test group G1 security-level AuthPriv match-rule Exact views V1 V1 V1</code>

<code>snmpv3 mibview view</code> [View Name] <code>type</code> [Excluded Included] <code>sub-oid</code> [OID]	G	Configure the mibview table of the SNMPV3 agent	<code>switch(config)#snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1</code>
<code>show snmp</code>	P	Show SNMP configuration	<code>switch#show snmp</code>
<code>no snmp community-strings</code> [Community]	G	Remove the specified community.	<code>switch(config)#no snmp community-strings public</code>
<code>no snmp-server host</code> [Host-address]	G	Remove the SNMP server host.	<code>switch(config)#no snmp-server host 192.168.1.50</code>
<code>no snmpv3 user</code> [User Name]	G	Remove the specified user of the SNMPv3 agent.	<code>switch(config)#no snmpv3 user test01</code>
<code>no snmpv3 access context-name</code> [Context Name ] <code>group</code> [Group Name ] <code>security-level</code> [NoAuthNoPriv AuthNoPriv AuthPriv] <code>match-rule</code> [Exact Prefix] <code>views</code> [Read View Name] [Write View Name] [Notify View Name]	G	Remove the specified access table of the SNMPv3 agent.	<code>switch(config)#no snmpv3 access context-name Test group G1 security-level AuthPriv match-rule Exact views V1 V1 V1</code>
<code>no snmpv3 mibview view</code> [View Name] <code>type</code> [Excluded Included] <code>sub-oid</code> [OID]	G	Remove the specified mibview table of SNMPV3 agent.	<code>switch(config)#no snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1</code>

## Port Mirroring Commands Set

Commands	Level	Description	Example
<code>monitor</code> <code>[RX TX Both]</code>	I	Configure the source port of monitor function	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#monitor RX</code>
<code>monitor rx</code> [Port ID]	G	Set RX destination port of monitor function	<code>switch(config)#monitor rx 3</code>
<code>monitor tx</code> [Port ID]	G	Set TX destination port of monitor function	<code>switch(config)#monitor tx 4</code>
<code>show monitor</code>	P	Show port monitor information	<code>switch#show monitor</code>
<code>show monitor</code>	I	Show port monitor information	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#show monitor</code>
<code>no monitor</code>	I	Disable source port of monitor function	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#no monitor</code>

## 802.1x Commands Set

Commands	Level	Description	Example
<code>8021x enable</code>	<b>G</b>	Use the 802.1x global configuration command to enable 802.1x protocols.	<code>switch(config)# 8021x enable</code>
<code>8021x system radiusip</code> [IP address]	G	Use the global configuration command to change the radius server IP.	<code>switch(config)# 8021x system radiusip 192.168.1.1</code>
<code>8021x system serverport</code> [port ID]	G	Use the global configuration command to change the radius server port	<code>switch(config)# 8021x system serverport 1815</code>
<code>8021x system accountport</code> [port ID]	G	Use the global configuration command to change the accounting port	<code>switch(config)# 8021x system accountport 1816</code>
<code>8021x system sharedkey</code> [ID]	G	Use the global configuration command to change the shared key value.	<code>switch(config)# 8021x system sharedkey 123456</code>
<code>8021x system nasid</code> [words]	G	Use the global configuration command to change the NAS ID	<code>switch(config)# 8021x system nasid test1</code>
<code>8021x misc quietperiod</code> [sec.]	G	Use the global configuration command to specify the quiet period of the switch in seconds	<code>switch(config)# 8021x misc quietperiod 10</code>

<b>8021x misc txperiod</b> [sec.]	G	Use the global configuration command to set the TX period in seconds.	switch(config)# <b>8021x misc txperiod 5</b>
<b>8021x misc supptimeout</b> [sec.]	G	Use the global configuration command to set the supplicant timeout in seconds.	switch(config)# <b>8021x misc supptimeout 20</b>
<b>8021x misc servertimeout</b> [sec.]	G	Use the global configuration command to set the server timeout in seconds.	switch(config)# <b>8021x misc servertimeout 20</b>
<b>8021x misc maxrequest</b> [number]	G	Use the global configuration command to set the maximum requests.	switch(config)# <b>8021x misc maxrequest 3</b>
<b>8021x misc reauthperiod</b> [sec.]	G	Use the global configuration command to set the reauthorized period in seconds.	switch(config)# <b>8021x misc reauthperiod 3000</b>
<b>8021x portstate</b> [disable   reject   accept   authorize]	I	Use the configuration command to set the state of the selected port.	switch(config)# <b>interface fastethernet 3</b> switch(config-if)# <b>8021x portstate accept</b>
<b>show 8021x</b>	E	Display a summary of the 802.1x properties and also the port sates.	switch> <b>show 8021x</b>
<b>no 8021x</b>	G	Disable 802.1x function	switch(config)# <b>no 8021x</b>

## TFTP Commands Set

Commands	Level	Description	Defaults Example
<b>backup flash:backup_cfg</b>	G	Save configuration to the TFTP server. IP address of the TFTP server and the file name of the image are required.	switch(config)# <b>backup flash:backup_cfg</b>
<b>restore flash:restore_cfg</b>	G	Get configuration from the TFTP server. IP address of the TFTP server and the file name of the image are required.	switch(config)# <b>restore flash:restore_cfg</b>
<b>upgrade flash:upgrade_fw</b>	G	Upgrade firmware via TFTP. IP address of the TFTP server and the file name of the image are required.	switch(config)# <b>upgrade flash:upgrade_fw</b>

## SystemLog, SMTP and Event Commands Set

Commands	Level	Description	Example
<code>systemlog mode</code> [client server both]	G	Specify the log mode	switch(config)# <b>systemlog mode both</b>
<code>systemlog ip</code> [IP address]	G	Set System log server IP address.	switch(config)# <b>systemlog ip 192.168.1.100</b>
<code>show systemlog</code>	E	Display system log.	Switch> <b>show systemlog</b>
<code>show systemlog</code>	P	Show system log client & server information	switch# <b>show systemlog</b>
<code>no systemlog</code>	G	Disable systemlog function	switch(config)# <b>no systemlog</b>
<code>smtp enable</code>	G	Enable SMTP function	switch(config)# <b>smtp enable</b>
<code>smtp serverip</code> [IP address]	G	Configure SMTP server IP	switch(config)# <b>smtp serverip 192.168.1.5</b>
<code>smtp sender</code>	G	Send the sender identification when an event occurs	switch(config)# <b>smtp sender test01</b>
<code>smtp authentication</code>	G	Enable SMTP authentication	switch(config)# <b>smtp authentication</b>
<code>smtp account</code> [account]	G	Configure authentication accounts	switch(config)# <b>smtp account John</b>
<code>smtp password</code> password: [password] confirm password: [password]	G	Configure authentication password	switch(config)# <b>smtp password</b> password: <b>1234</b> confirm password: <b>1234</b>
<code>smtp rcptemail</code> [Index] [Email address]	G	Configure Rcpt e-mail Address	switch(config)# <b>smtp rcptemail 1</b> <b><a href="mailto:Alert@test.com">Alert@test.com</a></b>
<code>show smtp</code>	P	Show the information of SMTP	switch# <b>show smtp</b>
<code>no smtp</code>	G	Disable SMTP function	switch(config)# <b>no smtp</b>
<code>event device-cold-start</code> [Systemlog SMTP Both]	G	Set cold start event type	switch(config)# <b>event device-cold-start both</b>
<code>event authentication-failure</code> [Systemlog SMTP Both]	G	Set the event type of Authentication failure	switch(config)# <b>event authentication-failure both</b>
<code>event mac-violation</code> [Systemlog SMTP Both]	G	Set the event type of MAC Violation	switch(config)# <b>event mac-violation both</b>
<code>event systemlog</code> [Link-UP Link-Down Both]	I	Set port event for system log	switch(config)# <b>interface fastethernet 3</b> switch(config-if)# <b>event systemlog both</b>
<code>event smtp</code> [Link-UP Link-Down Both]	I	Set port event for SMTP	switch(config)# <b>interface fastethernet 3</b> switch(config-if)# <b>event smtp both</b>
<code>show event</code>	P	Show event selection	switch# <b>show event</b>
<code>no event device-cold-start</code> [Systemlog SMTP Both]	G	Disable cold start event type	switch(config)# <b>no event device-cold-start both</b>

no event authentication-failure [Systemlog SMTP Both]	G	Disable the event type of Authentication failure	switch(config)#no event authentication-failure both
no event mac-violation [Systemlog SMTP Both]	G	Disable the event type of MAC Violation	switch(config)#no event mac-violation both
no event systemlog	I	Disable port event for system log	switch(config)#interface fastethernet 3 switch(config-if)#no event systemlog
no event smpt	I	Disable port event for SMTP	switch(config)#interface fastethernet 3 switch(config-if)#no event smtp



## SNTP Commands Set

Commands	Level	Description	Example
sntp enable	G	Enable SNTP function	switch(config)# <b>sntp enable</b>
sntp daylight	G	Enable daylight saving time. If the SNTP function is inactive, this command can't be applied.	switch(config)# <b>sntp daylight</b>
sntp daylight-period [Start time] [End time]	G	Set period of daylight saving time. If the SNTP function is inactive, this command can not be applied. Parameter format: [yyyymmdd-hh:mm]	switch(config)# <b>sntp daylight-period 20110101-01:01 20110202-01:01</b>
sntp daylight-offset [Minute]	G	Set offset of daylight saving time. If SNTP is inactive, this command can't be applied.	switch(config)# <b>sntp daylight-offset 3</b>
sntp ip [IP]	G	Set the SNTP server IP. If SNTP is inactive, this command can't be applied.	switch(config)# <b>sntp ip 192.168.1.1</b>
sntp timezone [Timezone]	G	Set time zone index. Use the "show sntp timezone" command to get more information of index number	switch(config)# <b>sntp timezone 22</b>
sntp sync-interval [Secs]	G	Set synchronization interval in seconds	switch(config)# <b>sntp sync-interval 1024</b>
show sntp	P	Show SNTP information	switch# <b>show sntp</b>
show sntp timezone	P	Show index number of the time zone list	switch# <b>show sntp timezone</b>
no sntp	G	Disable SNTP	switch(config)# <b>no sntp</b>
no sntp daylight	G	Disable daylight saving time	switch(config)# <b>no sntp daylight</b>

## X-ring2 Commands Set

Commands	Level	Description	Example
<b>ring2 mode</b> [X-Ring2 Legacy-Ring]	G	Set X-ring in X-ring2 mode	switch(config)# <b>ring2 mofde x-ring2</b>
<b>ring2 add</b> [Ring ID][1st Ring Port][2nd Ring Port][1st Rdn Port][1st Rdn Port ID][2nd Rdn Port][2nd Rdn Port ID]	G	Add an X-Ring2 entry	switch(config)# <b>ring2 add 1 5 6 7 2 8 2</b>
<b>ring2 ringport</b> [1st Ring Port][2nd Ring Port]	G	Add Legacy-Ring 1st/2nd Ring Port	switch(config)# <b>ring2 ringport 1 2</b>
<b>ring2 del</b> [Index]	G	Delete an X-Ring2 entry	switch(config)# <b>ring2 del 1</b>
<b>ring2 show</b>	G	Show X-Ring2 configuration	switch(config)# <b>ring2 show</b>
<b>no ring2</b>	G	Disable X-Ring2	switch(config)# <b>no ring2</b>
<b>show ring2</b>	P	Show X-Ring2 configuration	switch# <b>show ring2</b>

## Fault Relay Alarm Commands Set

Commands	Level	Description	Example
<b>faultrelay power</b> [number] [enable/disable]	G	Enable/Disable Power Relay Alarm function	switch(config)# <b>faultrelay power 1 enable</b>
<b>faultrelay</b> [enable/disable]	I	Enable/Disable Port Fault Relay Alarm function	switch(config)# <b>interface fastEthernet 1</b> switch(config-if)# <b>faultrelay enable</b>
<b>faultrelay macviolation</b> [enable/disable]	G	Configure Relay Alarm for MAC Violation Failure	switch(config)# <b>faultrelay macviolation enable</b>
<b>show faultrelay</b>	P	Show Fault Relay Alarm setting	switch# <b>show faultrelay</b>

## N-Key Commands Set

Commands	Level	Description	Example
<code>nkey auto</code> [on/off]	G	System configurations auto-loaded when system boots up	switch(config)# <b>nkey auto on</b>

## LLDP Commands Set

Commands	Level	Description	Example
<code>lldp enable</code>	G	Enable LLDP function	switch(config)# <b>lldp enable</b>
<code>lldp interval</code> [TIME sec]	G	Configure LLDP interval in seconds	switch(config)# <b>lldp interval 1800</b>
<code>show lldp</code>	P	Show LLDP information	switch# <b>show lldp</b>
<code>no lldp</code>	G	Disable LLDP	switch(config)# <b>no lldp</b>

## IPv6 Commands Set

Commands	Level	Description	Example
<code>show ipv6</code>	P	Show ipv6 and ND cache information	switch# <b>show ipv6</b>
<code>ping6</code> [ipv6 address]	G	Start ICMPv6 ping	switch(config)# <b>ping6 ff02::1</b>
<code>show ndclear</code>	G	Clear neighbor discovery cache	switch# <b>show ndclear</b>

## MECHANICAL INSTALLATION INSTRUCTIONS

### ComNet Customer Service

Customer Care is ComNet Technology's global service center, where our professional staff is ready to answer your questions at any time.

Email ComNet Global Service Center: [customercare@comnet.net](mailto:customercare@comnet.net)



3 CORPORATE DRIVE | DANBURY, CT 06810 | USA  
T: 203.796.5300 | F: 203.796.5303 | TECH SUPPORT: 1.888.678.9427 | [INFO@COMNET.NET](mailto:INFO@COMNET.NET)  
8 TURNBERRY PARK ROAD | GILDERSOME | MORLEY | LEEDS, UK LS27 7LE  
T: +44 (0)113 307 6400 | F: +44 (0)113 253 7462 | [INFO-EUROPE@COMNET.NET](mailto:INFO-EUROPE@COMNET.NET)