comnet
Communication Networks

INSTALLATION AND OPERATION MANUAL

CNGE8FX4TX4MS

ENVIRONMENTALLY HARDENED MANAGED
ETHERNET SWITCH WITH (4) 10/100/1000TX
+ (4) 100/1000FX SFP PORTS

V1.10 – July 2010

The ComNet™ CNGE8FX4TX4MS Managed Ethernet Switch provides transmission of (4) 100/1000 BASE-TX and (4) 10/100/1000FX combo ports. Unlike most Ethernet switches, these environmentally hardened units are designed for deployment in difficult operating environments, and are available for use with either conventional CAT-5e copper or optical transmission media. Ports 1 – 4 support the 10/100/1000 Mbps Ethernet IEEE 802.3 protocol, and auto-negotiating and auto-MDI/MDIX features are provided for simplicity and ease of installation. Ports 5 – 8 are 10/100/1000 configurable for copper or 100/1000 fiber media for use with multimode or single mode optical fiber without need for configuration, selected by optional SFP modules. These network managed layer 2 switches are optically 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 CNGE8FX4TX4MS incorporates LED indicators for monitoring the operating status of the managed switch and network.

Content

Overview

Introduction

To create reliability in your network, the ComNet CNGE8FX4TX4MS 4 10/100/1000T + 4 SFP Managed Switch comes equipped with a proprietary redundant network protocol—X-Ring provides users with an easy way to establish a redundant Ethernet network with ultra high-speed recovery time less than 20ms. Also, the long MTBF (Mean Time Between Failures) ensures that the switch will continue to operate until a Gigabit network infrastructure has been established, without requiring any extra upgrade costs.

Aside from 4 x 10/100/1000Base-T fast Ethernet ports, the CNGE8FX4TX4MS comes equipped with 4 SFP (mini-GBIC) ports. Traditional RJ45 ports can be used for uplinking wide-band paths in short distance (< 100 m), while the SFP slots can be used for the application of wideband uploading and long distance transmissions to fit the field request flexibility. Also, the long MTBF (Mean Time Between Failures) ensures that the CNGE8FX4TX4MS will continue to operate until a Gigabit network infrastructure has been established, without requiring any extra upgrade costs.

SFP Advantages

The SFP fiber slots provide a lot of flexibility when planning and implementing a network. The slot can accept any SFP-type fiber module and these modules are designed for transmitting over distances of either 550m (multi-mode), 10km, 30km, 50km, 70km or 110km (single-mode)—and the slot supports SFP modules for WDM single-fiber transmissions. This means that you can easily change the transmission mode and distance of the switch by simply pulling out the SFP module and plugging in a different module. The SFP modules are hot-swappable and plug-and-play.

SFP with DMI (Digital Monitoring Interface) function

The ComNet™ SFP supports a digital monitoring interface (DMI) function that allows real-time access to device operating parameters, and includes optional digital features such as soft control and monitoring of SFP I/O signals. In addition, you can set up the action of alarms and warnings by ports to manage your devices.

High-Speed Transmission

The CNGE8FX4TX4MS includes a switch controller that can automatically sense transmission speeds (10/100/1000 Mbps). The RJ45 interface can also be auto-detected, so MDI or MDI-X is automatically selected and a crossover cable is not required. All Ethernet ports have memory buffers that support the store-and-forward mechanism. This assures that data is properly transmitted.

Dual Power Input

The redundant power input design of the CNGE8FX4TX4MS is with power reserve protection to prevent the switch from being damaged by using the wrong power source. When one of power input has failed, the P-Fail LED will turn on and send an alarm through a relay output to notify the user.

Flexible Mounting

The CNGE8FX4TX4MS is a compact size and can be mounted on a DIN-rail or panel. It can be used in any location where space is scarce.

Advanced Protection

The power line of the CNGE8FX4TX4MS supports up to 3,000 V_{DC} EFT protection, which protects the switch from unregulated voltage and provides greater reliability. This high voltage protection feature protects all the ports and makes the CNGE8FX4TX4MS suitable for us in harsh industrial environments

Wide Operating Temperature

The ambient operating temperature of the CNGE8FX4TX4MS is between -40℃ ~ 75℃.

Easy Troubleshooting

LED indicators make troubleshooting quick and easy. Each 10/100/1000 Base-TX port has 2 LEDs that display the link status and transmission speed. The three power indicators: PWR1, PWR2 and P-Fail assist in diagnosing any problems quickly.

ComNet CNGE8FX4TX4MS Features

- Provides four 10/100/1000Base-T Mbps Ethernet ports
- Provides four SFP (mini-GBIC) port (supports 100/1000 Mbps Dual Mode)
- SFPs support DMI function
- Supports full/half duplex flow control
- Supports auto-negotiation
- Supports MDI/MDI-X auto-crossover
- Supports Packet Buffer up to 1Mb
- Supports MAC Address up to 8Kb
- Supports surge (EFT) protection 3,000 V_{DC}
- Supports 6,000 V_{DC} Ethernet ESD protection
- Power Supply
  - Wide-range Redundant Power Design
  - Reverse Power Polarity Protection
  - Current Overload Protection
- Case/Installation
  - IP-30 Protection
  - DIN Rail and Wall Mount Design
- Spanning Tree
  - Support IEEE802.1d Spanning Tree
  - Support IEEE802.1w Rapid Spanning Tree
- VLAN
  - Port Based VLAN
  - Support 802.1 Q Tag VLAN
  - GVRP
- X-Ring
  - X-Ring, Dual Homing and Couple Ring Topology
  - Provide redundant backup feature with a recovery time below 20ms
- Port Trunk with LACP
- QoS (Quality of Service)
  - Support IEEE 802.1p Class of Service
  - Per port provides 4 priority queues
  - Port Base, Tag Base and Type of Service Priority

- Bandwidth Control
  - Ingress Packet Filter and Egress Rate Limit
  - Broadcast/Multicast Packet Filter Control
- Port Mirror: Monitor traffic in switched networks.
  - TX Packet only
  - RX Packet only
  - Both of TX and RX Packet
- System Event Log
  - System Log Server/Client
  - SMTP e-mail Alert
  - Relay Alarm Output System Events
- Security
  - Port Security: MAC address entries/filter
  - IP Security: IP address security management to prevent unauthorized intruder
  - Login Security: IEEE802.1X/RADIUS
- SNMP Trap
  - Device cold start
  - Power status
  - Authentication failure
  - X-Ring topology changed
  - Port Link up/Link down
- IGMP with Query mode for Multi Media Application
- TFTP Firmware Update and System Configure Restore and Backup
- Ambient operating temperature range -40°C ~ 75°C

CNGE8FX4TX4MS Technical Specifications

Communication

Compatibility	IEEE 802.3, 802.3u, 802.3ab IEEE 802.3x, 802.3z, 802.3ad IEEE 802.1d, 802.1p, 802.1Q, 802.1x IEEE 802.1ab
LAN	10/100/1000Base-T, 1000Base-X
Transmission Speed	Up to 1000 Mbps

Interface

Connectors	4 x RJ45 (4-port 10/100/1000TX) 4 x 100/1000 SFP sockets 6-pin removable screw terminal (Power & Relay)
LED Indicators	Unit: Power1, Power2, P-Fail, R-Master Ethernet port: Link/Active, 1000M SFP: Link/Active

Network Management

Configuration	Web browser, Telnet, Serial Console, Windows Utility, TFTP, SNMP v1/v2c/v3, Port Speed/Duplex Configuration
VLAN	IEEE 802.1Q, GVRP, Port-based, VLAN
Redundancy	X-Ring (Recovery time < 20ms), Dual Homing, Couple Ring, 802.1w/d RSTP/STP
Security	IP Access security, post security, DHCP Server, Port and IP Binding, 802.1X Port Access Control
Traffic Control	IGMP Snooping/Query for multicast group management Port Trunking, Static/802.3ad LACP Rate limit and storm control IEEE 802.1p QoS Cos/TOS/DSCP priority queuing IEEE 802.3x flow control

Diagnostics	Port Mirroring, Real-time traffic statistic, MAC Address Table, SNTP, Syslog, E-Mail Alert, SNMP, Trap, RMON

Power

Power Consumption	13 Watts
Power Input	2 x Unregulated +12 ~ 48 V_{DC}
Fault Output	1 Relay Output

Mechanism

Dimensions (WxHxD)	59.6 x 152 x 105 mm
Enclosure	IP-30, Metal shell with solid mounting kits
Mounting	DIN-Rail, Wall Mount

Protection

ESD (Ethernet)	6,000 V_{DC}
Surge (EFT for power)	3,000 V_{DC}
Reverse Power Protection	Yes
Current Overload Protection	Yes

Environment

Operating Temperature Range	-40°C ~ 75°C
Operating Humidity Range	5% ~ 95% (non-condensing)
Storage Temperature	-40°C ~ 85°C
Storage Humidity	5% ~ 95% (non-condensing)

Certification

Safety	UL508, cUL
EMC	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)
	CE EN61000-4-11 (Voltage DIP)
	CE EN61000-3-2 (Harmonics Current)
	CE EN61000-3-3 (Voltage Fluctuation & Flickers)
Free Fall	IEC60068-2-32
Shock	IEC60068-2-27
Vibration	IEC60068-2-6

Packing List

- 1 x 4 10/100/1000T + 4 SFP Managed Switch
- 1 x RS232 Cable
- 1 x User Manual
- 2 x Wall Mounting Bracket and Screws

Safety Precaution

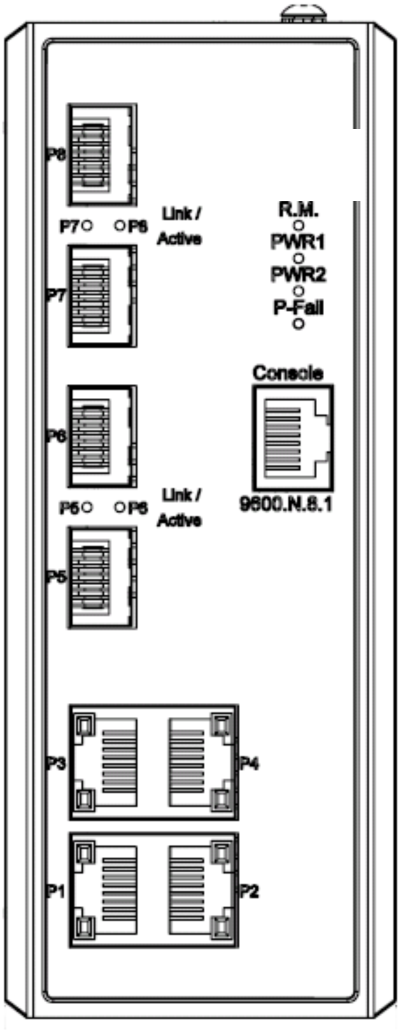
Attention: *IF DC voltage is supplied by an external circuit, please use a protection device on the power supply input.*

Hardware Description

In this section, we will introduce the CNGE8FX4TX4MS's hardware spec, port, cabling information, and wiring installation.

Front Panel

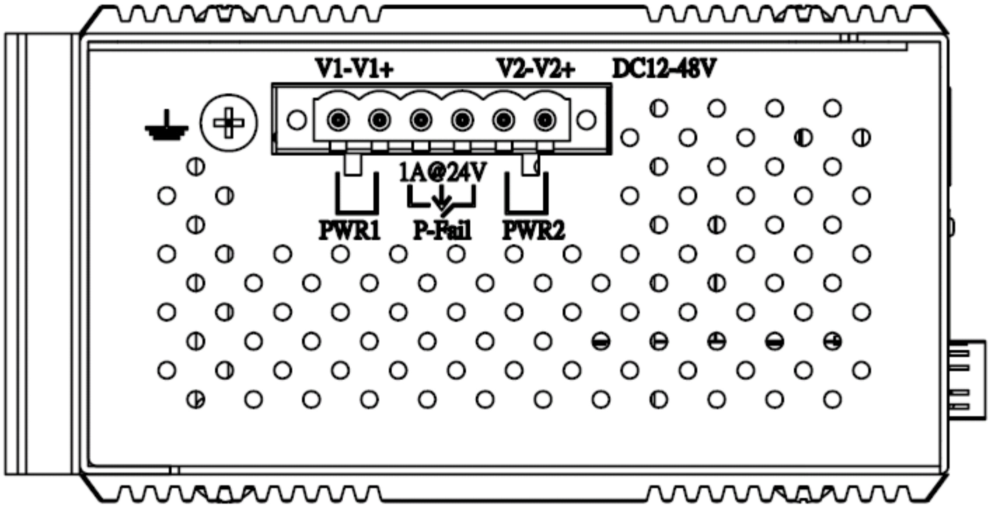
The Front Panel of the CNGE8FX4TX4MS is shown as follows:



Front Panel of the CNGE8FX4TX4MS Managed Switch

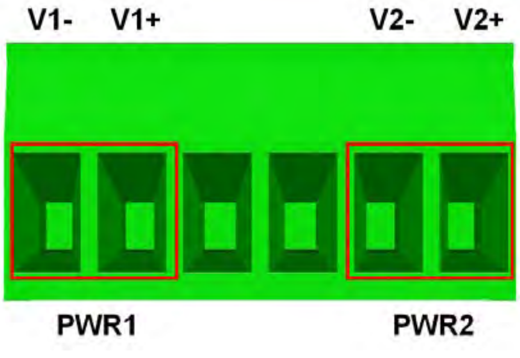
Top View

The top panel of the CNGE8FX4TX4MS is equipped with one terminal block connector for two DC power inputs.



Top panel of the 4 10/100/1000T + 4 SFP Switch

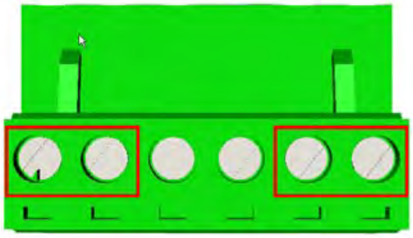
Wiring the Power Inputs



Primary
Voltage Input

Secondary (Redundant)
Power Input

Insert the positive and negative wires into the V+ and V- contacts on the terminal block connector.



Tighten the wire-clamp screws to prevent the wires from loosening.

Note *The wire gauge for the terminal block should be in the range between 12~ 20 AWG.*

LED Indicators

There are LEDs that display the power status and network status and are located on the front panel of the CNGE8FX4TX4MS switch. Each has its own specific meaning as noted below.

LED	Color	Description	
R-Master	Green	On	The switch is the master of the X-ring group
		Off	The switch is not the master of the X-ring group
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	Red	On	Power input 1 or 2 is inactive or port link down (depends on Fault Relay Alarm configuration)
		Off	Power input 1 and 2 are both functional, or no power inputs
Link/Active (P5 ~ P8)	Green	On	SFP port is linking
		Blinking	Transmitting or receiving data
		Off	Not connected to network
P1 ~ P4 (Upper LED)	Green	On	Connected to network
		Blinking	Data is being transmitted or received
		Off	Not connected to network
P1 ~ P4 (Lower LED)	Green	On	Connected to network at speed of 1000Mbps
		Off	Connected to network at speed of 10/100Mbps

LED indicators of the CNGE8FX4TX4MS Switch

Ports

RJ45 ports (Auto MDI/MDIX): The RJ45 ports are auto-sensing for 10Base-T, 100Base-TX or 1000Base-T device connections. Auto MDI/MDIX means that you can connect to another switch or workstation without changing straight through or crossover cabling. See figures below for straight-through and crossover cable schematic.

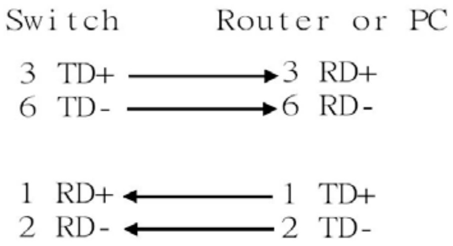
- **RJ45 Pin Assignments**

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

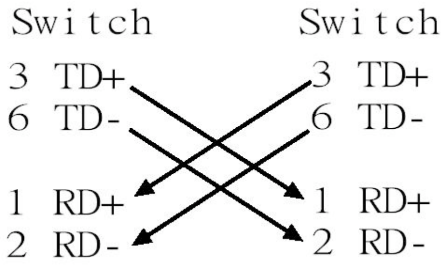
Note *"+" and "-" signs represent the polarity of the wires that make up each wire pair.*

All ports on this managed switch support automatic MDI/MDI-X operation. You can use straight-through cables (See Figure below) for all network connections to PCs or servers, or to other switches or hubs. In a straight-through cable, pins 1, 2, 3, and 6, at one end of the cable, are connected straight through to pins 1, 2, 3 and 6 at the other end of the cable. The 10BASE-T/100BASE-TX/1000BASE-T MDI and MDI-X port pin outs are as presented below.

Pin 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-)



Straight Through Cable Schematic



Cross Over Cable Schematic

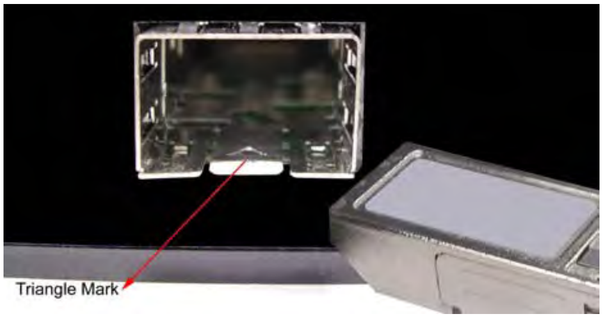
Cabling

Use the four twisted-pair, Category 5e or above cabling for all RJ45 port connections. The length of cable between the switch and the link partner (switch, hub, workstation, etc.) must be less than 100 meters (328 ft.) long.

The small form-factor pluggable (SFP) devices that are the compact optical transceivers used for optical communication for both telecommunication and data communication applications.

To connect the transceiver and LC cable, please follow the steps shown:

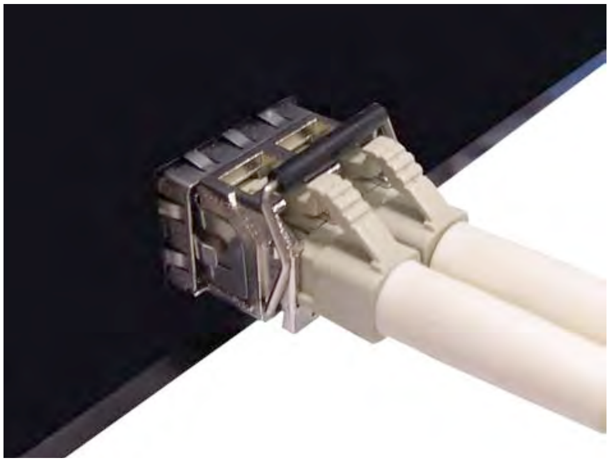
1. Insert the SFP device into the SFP receptacle. Notice that the triangle mark is the bottom of the module.



SFP Receptacle

SFP Inserted

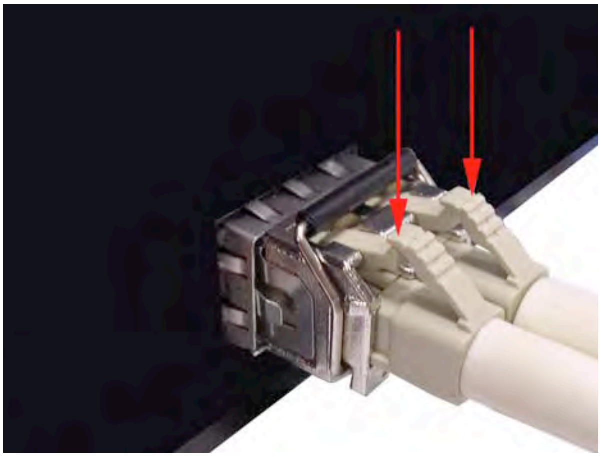
2. Insert the fiber cable of LC connector into the SFP.



LC connector to the SFP

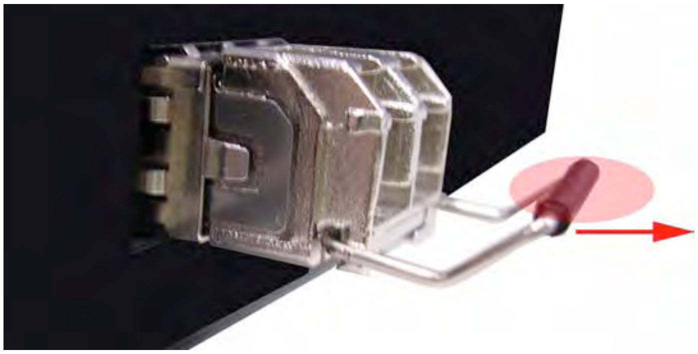
To remove the LC connector from the SFP, please follow the steps shown below:

1. Press the upper side of the LC connector from the SFP and pull it out to release.



Remove LC connector

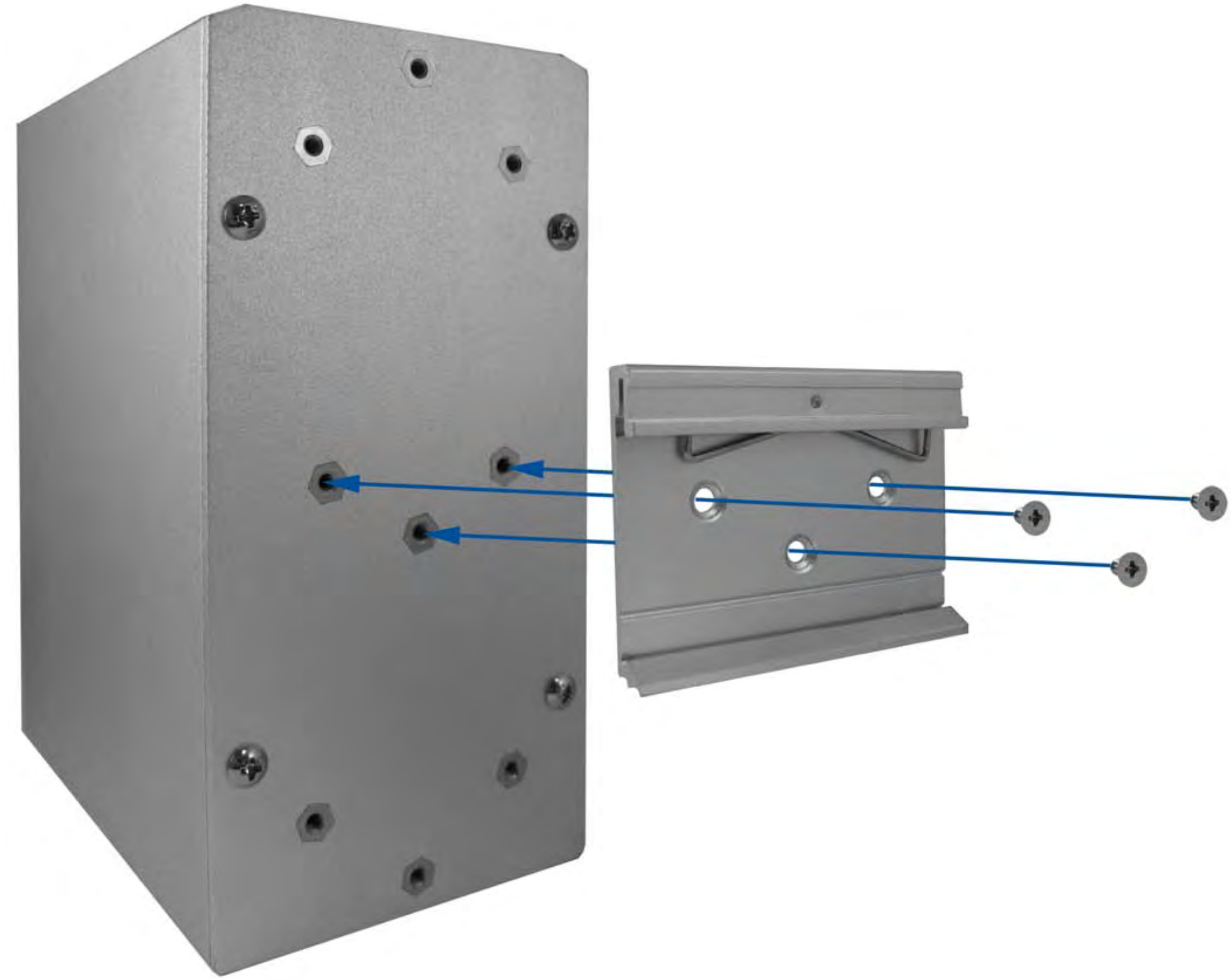
2. Push down the metal loop and pull the SFP out by the plastic part.



Pull out from the SFP receptacle

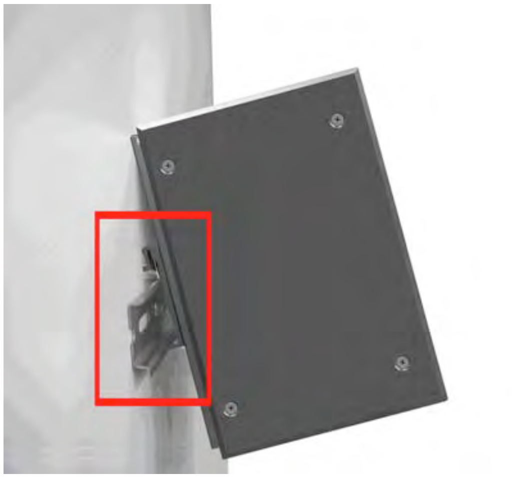
DIN-Rail Mounting Installation

The DIN-Rail mount is attached to the CNGE8FX4TX4MS at the factory. If the DIN-Rail is not attached to the switch, please see the following to attach the DIN-Rail to the switch.

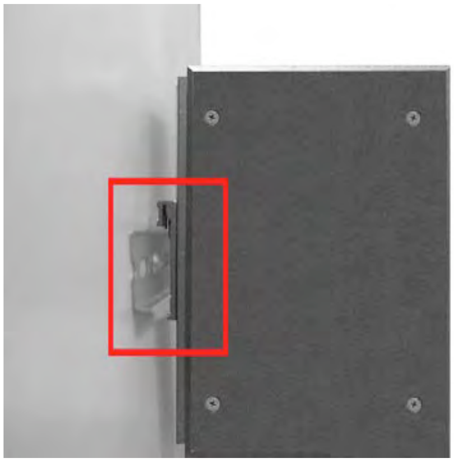


1. Insert the screws to attach the DIN-Rail to the switch.
2. To remove the DIN-Rail, reverse step 1.

1. Insert the top of DIN-Rail into the track.



2. Lightly push the button of DIN-Rail mount into the track.

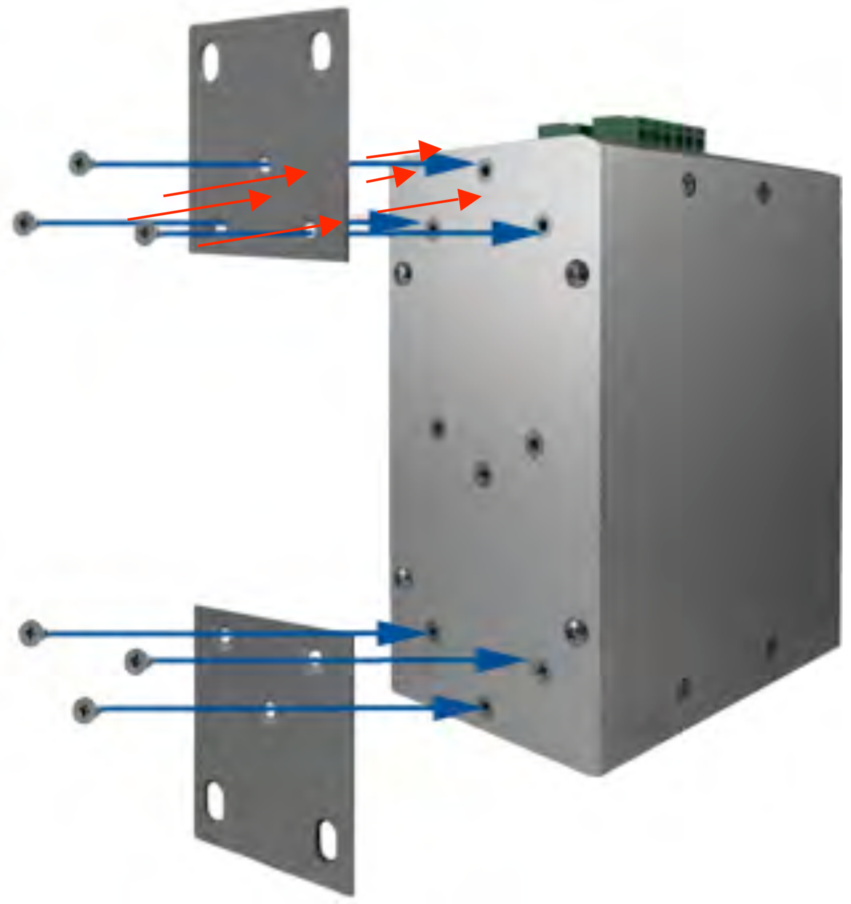


3. Check the switch is held securely on the track.
4. To remove the switch from the track, reverse the above steps.

Wall Mount Plate Mounting

Follow the steps as below to mount the switch with the wall mount plate.

1. Remove the DIN-Rail from the switch; loosen the screws to remove the DIN-Rail mount.
2. Place the wall mount plate on the rear panel of the switch.
3. Use the screws to screw the wall mount plate on the switch.
4. Use the hook holes at the corners of the wall mount plate to hang the switch on the wall.
5. To remove the wall mount plate, reverse steps above.



Use screws to screw the wall mount plate on the rear side

Hardware Installation

This section describes how to install the CNGE8FX4TX4MS Switch and the installation steps.

Installation Steps

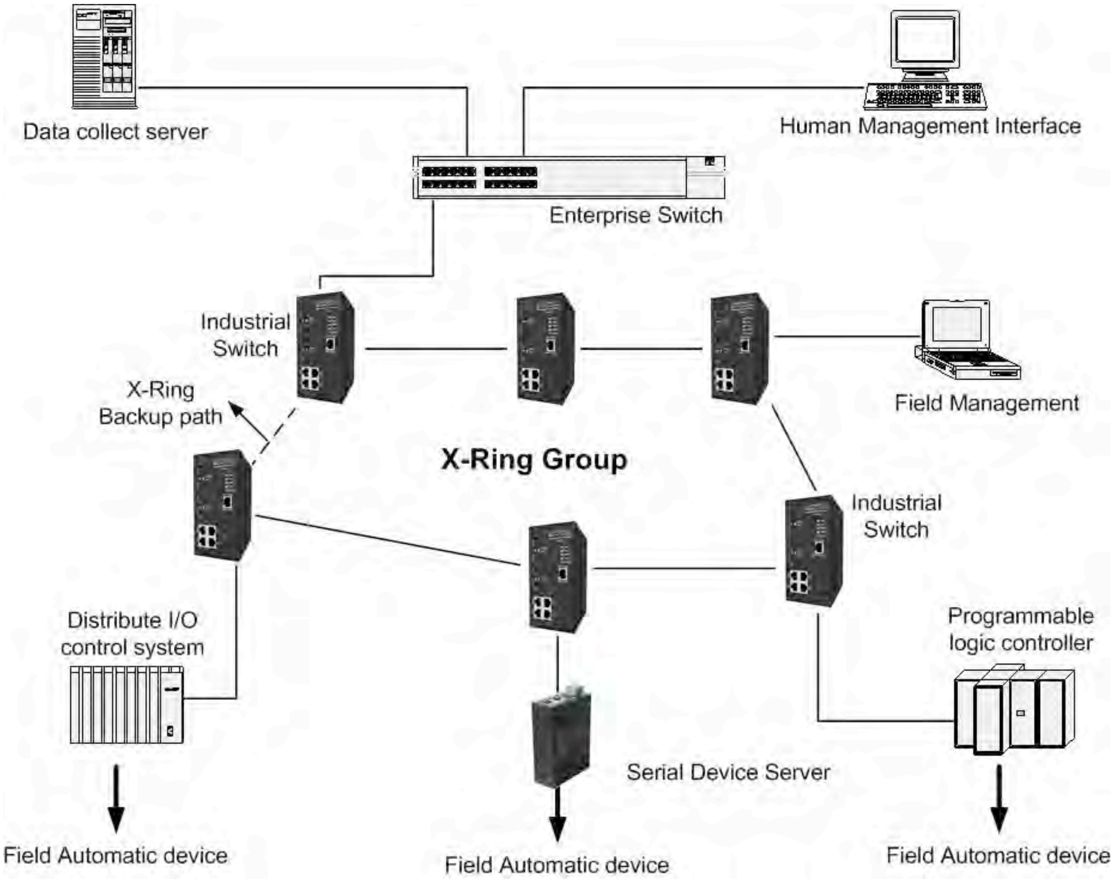
1. Unpack the switch from carton.
2. Check the DIN-Rail is screwed on the Switch. If the DIN-Rail mount is not attached to the switch, please refer to **DIN-Rail Mounting section** for DIN-Rail mounting installation. If you want to wall mount the switch, then please refer to **Wall Mount Plate Mounting section** for wall mount plate installation.
3. To hang the switch on the DIN-Rail track or wall, please refer to the **Mounting Installation section**.
4. Power on the switch. To wire power for the switch, please refer to the **Wiring the Power Inputs section**. The power LED on the switch will illuminate. Please refer to the **LED Indicators section** for the meaning of the LED lights.
5. Prepare the twisted-pair, straight-through Category 5e (or above) cable for the Ethernet connection and SFP transceiver for the fiber connection.
6. Insert one side of Category 5e (or above) cables into the switch Ethernet port (RJ45 port) and the other side of Category 5e (or above) cables to the network device's Ethernet port (RJ45 port), ex: switch, PC or Server. The UTP port (RJ45) LED on the switch will illuminate when the cable is connected to the network device. Please refer to the **LED Indicators section** for LED light meaning.

Note *Be sure the connected network devices support MDI/MDI-X. If it does not support, then use the crossover category 5e (or above) cable.*

7. For the SFP (mini-GBIC) port, please refer to the Cabling segment.
8. When all connections are set and LED lights illuminate normal, the installation is complete.

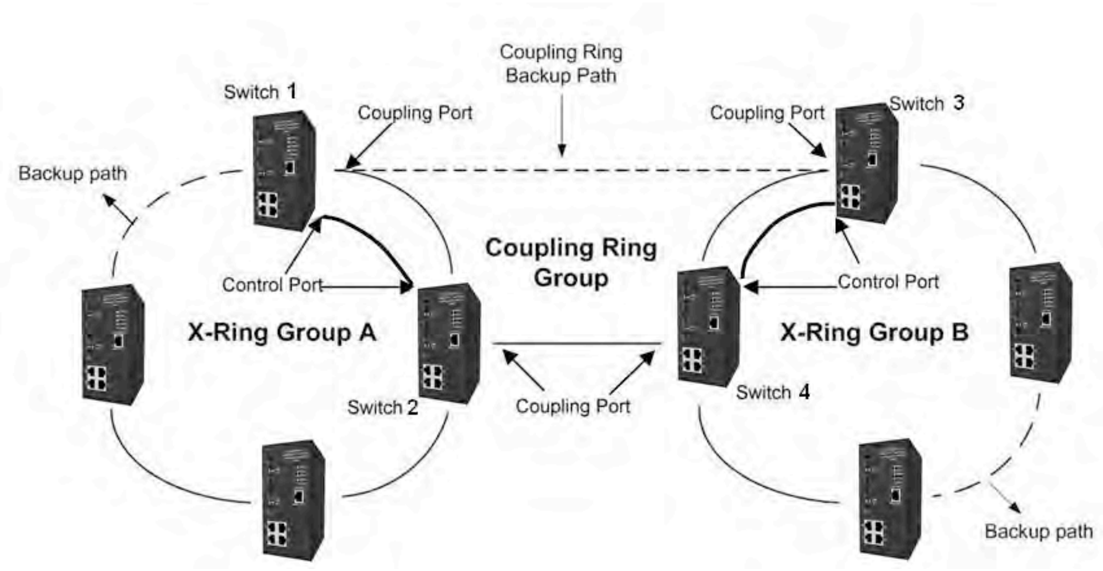
X-Ring Application

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



Coupling Ring Application

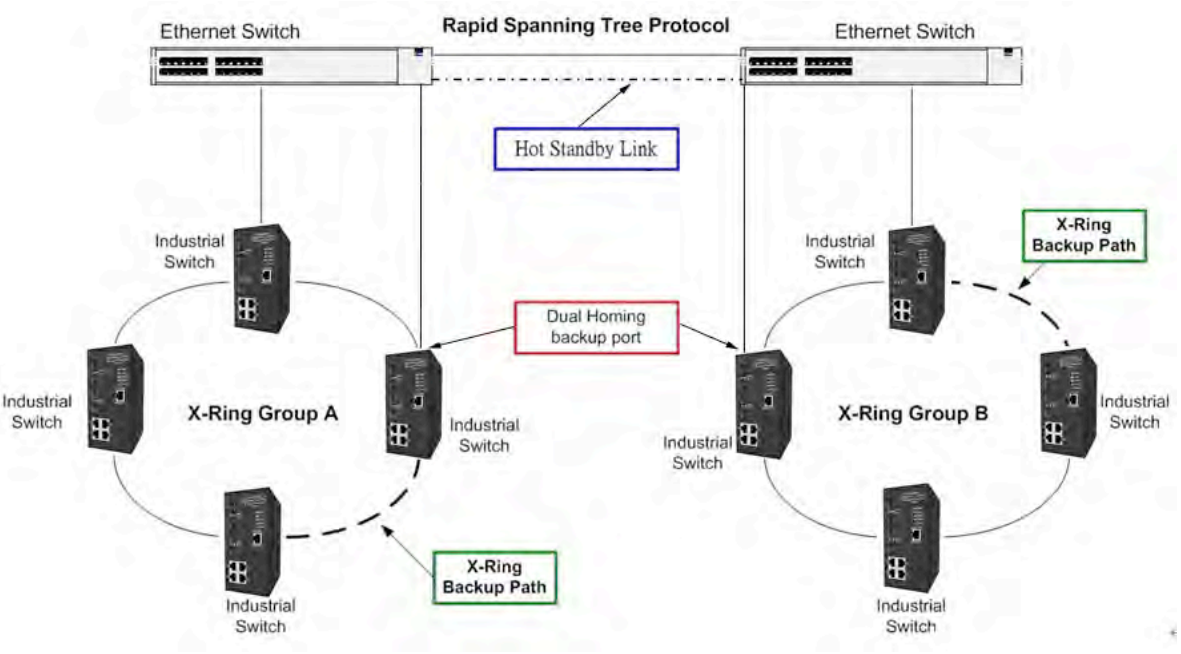
In the network, it may be necessary to have more than one X-Ring group. By using the coupling function it is possible to connect each X-Ring for a redundant backup. This will ensure the transmission between two ring groups will not fail. The following figure is an example of the coupling ring feature.



Dual Homing Application

The Dual Homing function is designed to prevent a connection loss between the X-Ring group and an upper level/core switch. By assigning two ports on the switches as Dual Homing ports, they will become the designated backup ports in the X-Ring group. The Dual Homing function only works when the X-Ring function is made active. Each X-Ring group can only have one Dual Homing port.

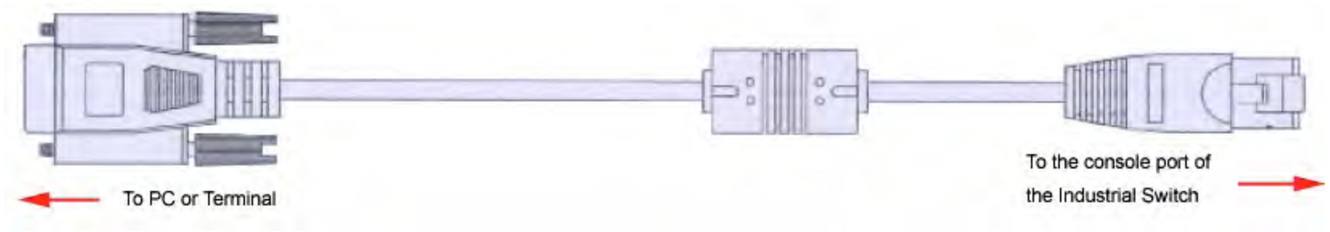
Note *In Dual Homing application architecture, the upper level switches must enable Rapid Spanning Tree protocol.*

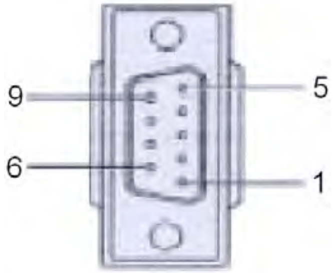


Console Management

Connecting to the Console Port

The cable supplied with the switch has an RS232 connector on one end and the other end is an RJ45 connector. Attach the end of the RS232 connector to a PC or terminal and the other end of RJ45 connector to the console port of switch. The connected terminal or PC must support the terminal emulation program.





DB 9-pin Female

Pin Assignment

DB9 Connector	RJ45 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

Login through the Console Interface

When the switch and PC are connected, turn on the PC and run a terminal emulation program or **Hyper Terminal** and configure the **communication parameters** to match the following default characteristics of the console port:

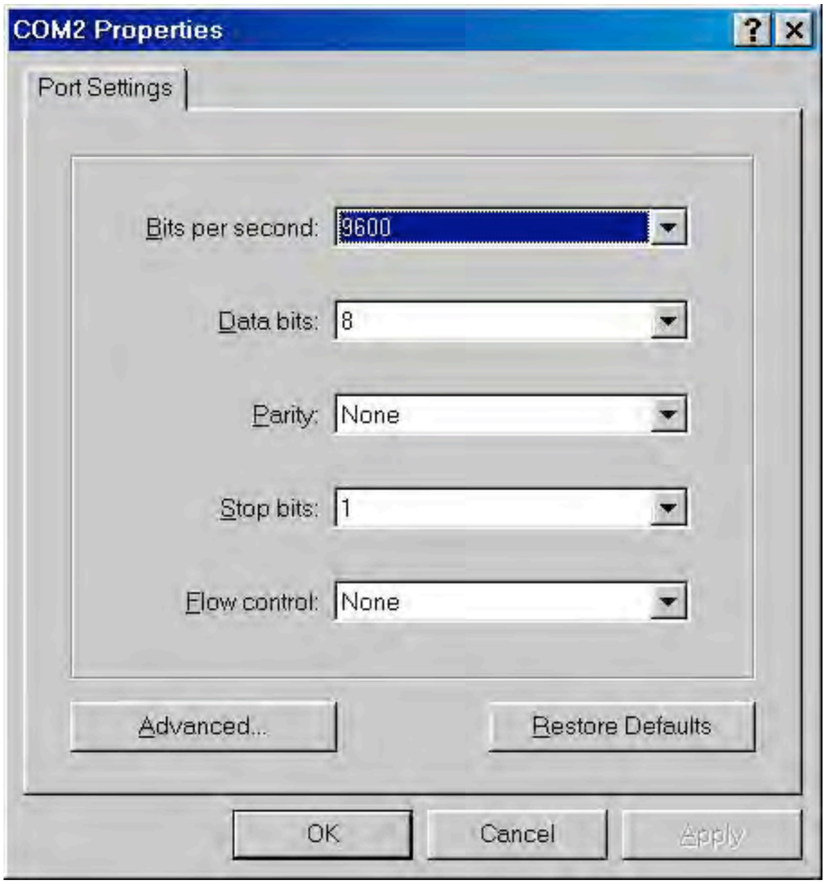
Baud Rate: 9600 bps

Data Bits: 8

Parity: none

Stop Bit: 1

Flow control: None



COM2 Properties

Bits per second: 9600

Data bits: 8

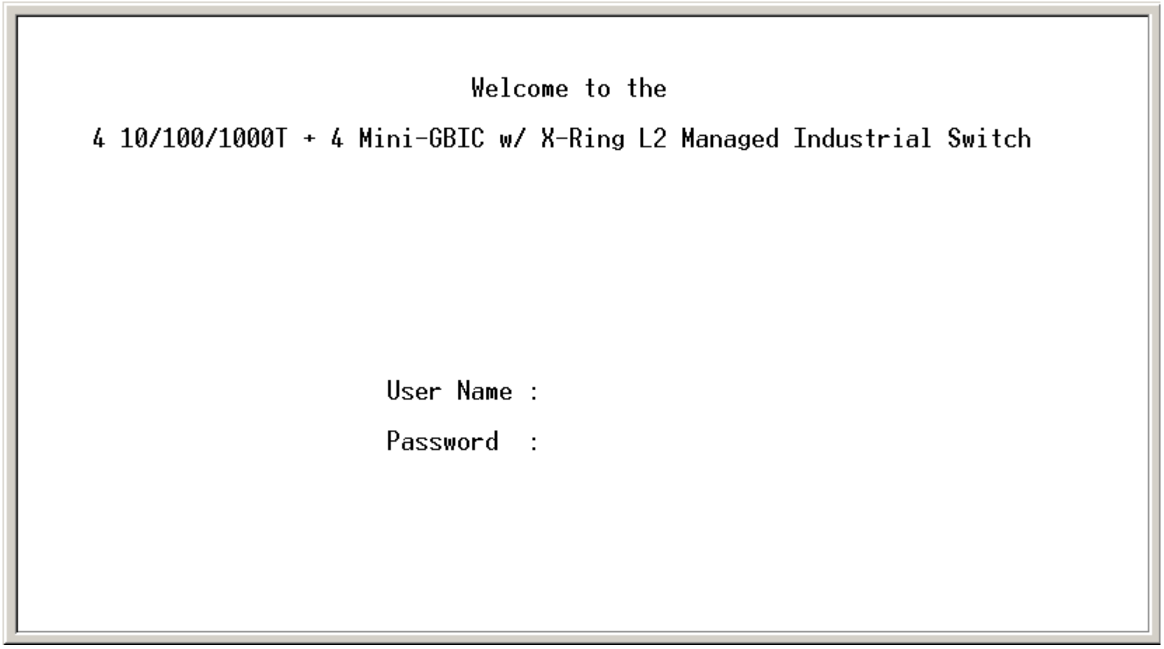
Parity: None

Stop bits: 1

Flow control: None

The settings of communication parameters

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

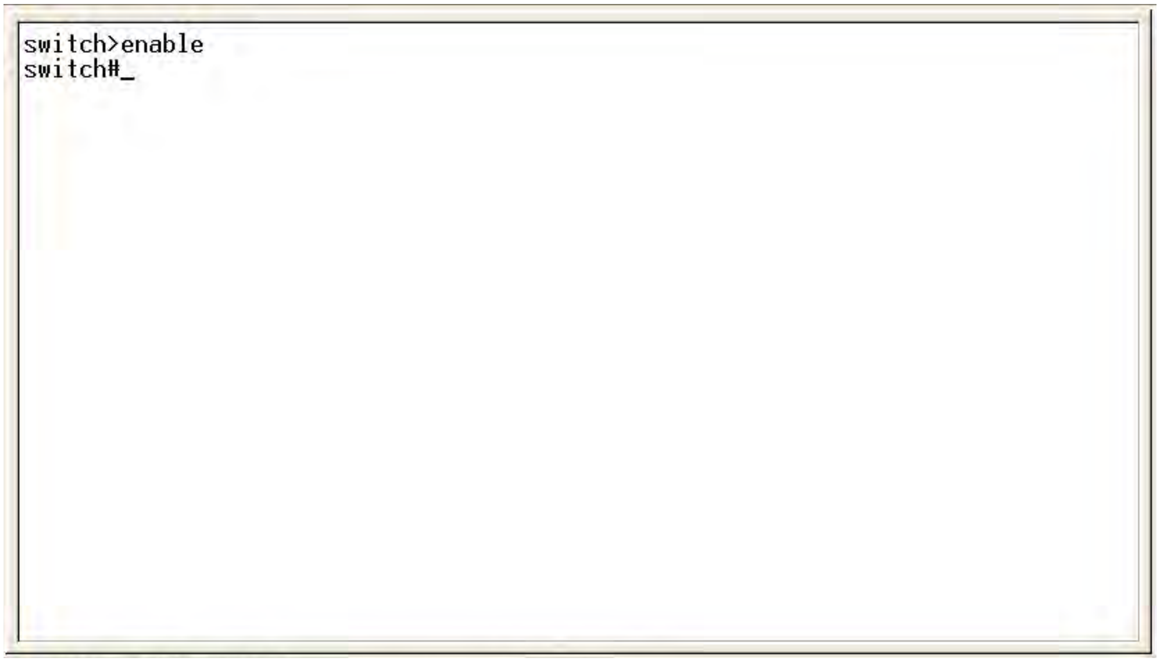


```
                         Welcome to the
  4 10/100/1000T + 4 Mini-GBIC w/ X-Ring L2 Managed Industrial Switch




                    User Name :
                    Password  :
```

Console login interface

CLI Management

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



```
switch>enable
switch#_
```

CLI command interface

Commands Level

The following table lists the CLI commands and description.

Modes	Access Method	Prompt	Exit Method	About This Mode1
User EXEC	Begin a session with your switch.	switch>	Enter logout or quit.	The user commands available at the user level are a subset of those available at the privileged level. Use this mode to • Perform basic tests. •Displays system information.
Privileged EXEC	Enter the enable command while in user EXEC mode.	switch#	Enter disable to exit.	The privileged command is advance mode Privileged this mode to •Displays advance function status • Save configures
Global Configuration	Enter the configure command while in privileged EXEC mode.	switch (config)#	To exit to privileged EXEC mode, enter exit or end	Use this mode to configure parameters that apply to your switch as a whole.
VLAN database	Enter the vlan database command while in privileged EXEC mode.	switch (vlan)#	To exit to user EXEC mode, enter exit.	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the interface of fast Ethernet command (with a specific interface) while in global configuration mode	switch (config-if) #	To exit to global configuration mode, enter exit. To exist to privileged EXEC mode, or end.	Use this mode to configure parameters for the switch and Ethernet ports.

System Commands Set

Command	Level	Description	Example
show config	E	Show switch configuration	switch>**show config**
show terminal	P	Show console information	switch#**show terminal**
write memory	P	Save user configuration into permanent memory (flash rom)	switch#**write memory**
system name [System Name]	G	Configure system name	switch(config)#**system name xxx**
system location [System Location]	G	Set switch system location string	switch(config)#**system location xxx**
system description [System Description]	G	Set switch system description string	switch(config)#**system description xxx**
system contact [System Contact]	G	Set switch system contact window string	switch(config)#**system contact xxx**
show system-info	E	Show system information	switch>**show system-info**
ip address [Ip-address] [Subnet-mask] [Gateway]	G	Configure the IP address of switch	switch(config)#**ip address 192.168.10.1 255.255.255.0 192.168.10.254**
ip dhcp	G	Enable DHCP client function of switch	switch(config)#**ip dhcp**
show ip	P	Show IP information of switch	switch#**show ip**
no ip dhcp	G	Disable DHCP client function of switch	switch(config)#**no ip dhcp**
reload	G	Halt and perform a cold restart	switch(config)#**reload**
default	G	Restore to default	switch(config)#**default**
admin username [Username]	G	Changes a login username. (maximum 10 words)	switch(config)#**admin username xxxxxx**
admin password [Password]	G	Specifies a password (maximum 10 words)	switch(config)#**admin password xxxxxx**

show admin	**P**	Show administrator information	switch#**show admin**
dhcpserver enable	**G**	Enable DHCP Server	switch(config)#**dhcpserver enable**
Dhcpserver disable	**G**	Disable DHCP Server	switch(config)#**no dhcpserver**
dhcpserver lowip **[Low IP]**	**G**	Configure low IP address for IP pool	switch(config)#**dhcpserver lowip 192.168.1.100**
dhcpserver highip **[High IP]**	**G**	Configure high IP address for IP pool	switch(config)#**dhcpserver highip 192.168.1.200**
dhcpserver subnetmask **[Subnet mask]**	**G**	Configure subnet mask for DHCP clients	switch(config)#**dhcpserver subnetmask 255.255.255.0**
dhcpserver gateway **[Gateway]**	**G**	Configure gateway for DHCP clients	switch(config)#**dhcpserver gateway 192.168.1.254**
dhcpserver dnsip **[DNS IP]**	**G**	Configure DNS IP for DHCP clients	switch(config)#**dhcpserver dnsip 192.168.1.1**
dhcpserver leasetime **[Hours]**	**G**	Configure lease time (in hour)	switch(config)#**dhcpserver leasetime 1**
dhcpserver ipbinding **[IP address]**	**I**	Set static IP for DHCP clients by port	switch(config)#**interface fastEthernet 2** switch(config-if)#**dhcpserver ipbinding 192.168.1.1**
show dhcpserver configuration	**P**	Show configuration of DHCP server	switch#**show dhcpserver configuration**
show dhcpserver clients	**P**	Show client entries of DHCP server	switch#**show dhcpserver clients**
show dhcpserver ip-binding	**P**	Show IP-Binding information of DHCP server	switch#**show dhcpserver ip-binding**
no dhcpserver	**G**	Disable DHCP server function	switch(config)#**no dhcpserver**
security enable	**G**	Enable IP security function	switch(config)#**security enable**
security http	**G**	Enable IP security of HTTP server	switch(config)#**security http**
security telnet	**G**	Enable IP security of telnet server	switch(config)#**security telnet**

security ip [Index(1..10)] [IP Address]	**G**	Set the IP security list	switch(config)#**security ip 1 192.168.1.55**
show security	**P**	Show the information of IP security	switch#**show security**
no security	**G**	Disable IP security function	switch(config)#**no security**
no security http	**G**	Disable IP security of HTTP server	switch(config)#**no security http**
no security telnet	**G**	Disable IP security of telnet server	switch(config)#**no security telnet**

Port Commands Set

Command	**Level**	**Description**	**Example**
interface fastEthernet **[Portid]**	**G**	Choose the port for modification.	switch(config)#**interface fastEthernet 2**
duplex **[full | half]**	**I**	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#**interface fastEthernet 2** switch(config-if)#**duplex full**
speed **[10|100|1000|auto]**	**I**	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can’t be set to 1000 if the port isn’t a giga port.	switch(config)#**interface fastEthernet 2** switch(config-if)#**speed 100**
no flowcontrol	**I**	Disable flow control of interface	switch(config-if)#**no flowcontrol**
security enable	**I**	Enable security of interface	switch(config)#**interface fastEthernet 2** switch(config-if)#**security enable**

no security	I	Disable security of interface	switch(config)#**interface fastEthernet 2** switch(config-if)#**no security**
bandwidth type all	I	Set interface ingress limit frame type to ‘accept all frame’	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type all**
bandwidth type broadcast-multicast-flooded-unicast	I	Set interface ingress limit frame type to ‘accept broadcast, multicast, and flooded unicast frame’	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type broadcast-multicast-flooded-unicast**
bandwidth type broadcast-multicast	I	Set interface ingress limit frame type to ‘accept broadcast and multicast frame’	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type broadcast-multicast**
bandwidth type broadcast-only	I	Set interface ingress limit frame type to ‘only accept broadcast frame’	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type broadcast-only**
bandwidth in **[Value]**	I	Set interface input bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth in 100**
bandwidth out **[Value]**		Set interface output bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth out 100**
show bandwidth	I	Show interfaces	switch(config)#**interface fastEthernet**

		bandwidth control	**2** switch(config-if)#**show bandwidth**
state **[Enable | Disable]**	**I**	Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disable form of this command to disable the port.	switch(config)#**interface fastEthernet 2** switch(config-if)#**state Disable**
show interface configuration	**I**	show interface configuration status	switch(config)#**interface fastEthernet 2** switch(config-if)#**show interface configuration**
show interface status	**I**	show interface actual status	switch(config)#**interface fastEthernet 2** switch(config-if)#**show interface status**
show interface accounting	**I**	show interface statistic counter	switch(config)#**interface fastEthernet 2** switch(config-if)#**show interface accounting**
no accounting	**I**	Clear interface accounting information	switch(config)#**interface fastEthernet 2** switch(config-if)#**no accounting**

Trunk Commands Set

Command	Level	Description	Example
aggregator priority **[1~65535]**	**G**	Set port group system priority	switch(config)#**aggregator priority 22**
aggregator activityport **[Group ID]** **[Port Numbers]**	**G**	Set activity port	switch(config)#**aggregator activityport 2**
aggregator group **[GroupID] [Port-list]**	**G**	Assign a trunk group with LACP active.	switch(config)#**aggregator group 1 1-4 lacp workp 2**

lacp **workp** **[Workport]**		[GroupID] :1~4 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount of member ports.	or switch(config)#**aggregator group 2 1,4,3 lacp workp 3**
aggregator group **[GroupID] [Port-list]** **nolacp**	**G**	Assign a static trunk group. [GroupID] :1~4 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	switch(config)#**aggregator group 1 2-4 nolacp** or switch(config)#**aggregator group 1 3,1,2 nolacp**
show aggregator	**P**	Show the information of trunk group	switch#**show aggregator 1** or switch#**show aggregator 2** or switch#**show aggregator 3**
no aggregator lacp **[GroupID]**	**G**	Disable the LACP function of trunk group	switch(config)#**no aggreator lacp 1**
no aggregator group **[GroupID]**	**G**	Remove a trunk group	switch(config)#**no aggreator group 2**

DMI Commands Set

Command	Level	Description	Example
show dmi	I	Show DMI port status (Port 5 to port 8 supports DMI fuction)	switch(config)#**interface fastEthernet 5** switch(config-if)#**show dmi**

VLAN Commands Set

Command	Level	Description	Example
vlan database	P	Enter VLAN configure mode	switch#**vlan database**
Vlanmode [portbase| 802.1q | gvrp]	V	To set switch VLAN mode.	switch(vlan)#**vlanmode portbase** or switch(vlan)#**vlanmode 802.1q** or switch(vlan)#**vlanmode gvrp**
no vlan	V	No VLAN	Switch(vlan)#**no vlan**
Ported based VLAN configuration			
vlan port-based grpname [Group Name] grpid [GroupID] port [PortNumbers]	V	Add new port based VALN	switch(vlan)#**vlan port-based grpname test grpid 2 port 2-4** or switch(vlan)#**vlan port-based grpname test grpid 2 port 2,3,4**
show vlan [GroupID] or show vlan	V	Show VLAN information	switch(vlan)#**show vlan 23**
no vlan group [GroupID]	V	Delete port base group ID	switch(vlan)#**no vlan group 2**
IEEE 802.1Q VLAN			
vlan 8021q name [GroupName] vid [VID]	V	Change the name of VLAN group, if the group didn't exist, this command can't be applied.	switch(vlan)#**vlan 8021q name test vid 22**
vlan 8021q port [PortNumber] access-link untag [UntaggedVID]	V	Assign a access link for VLAN by port, if the port	switch(vlan)#**vlan 8021q port 3 access-link untag 33**

		belong to a trunk group, this command can’t be applied.	
vlan 8021q port [PortNumber] **trunk-link tag** [TaggedVID List]	V	Assign a trunk link for VLAN by port, if the port belong to a trunk group, this command can’t be applied.	switch(vlan)#**vlan 8021q port 3 trunk-link tag 2,3,6,99** or switch(vlan)#**vlan 8021q port 3 trunk-link tag 3-20**
vlan 8021q port [PortNumber] **hybrid-link untag** [UntaggedVID] **tag** [TaggedVID List]	V	Assign a hybrid link for VLAN by port, if the port belong to a trunk group, this command can’t be applied.	switch(vlan)#**vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8** or switch(vlan)#**vlan 8021q port 3 hybrid-link untag 5 tag 6-8**
vlan 8021q trunk [PortNumber] **access-link untag** [UntaggedVID]	V	Assign a access link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 access-link untag 33**
vlan 8021q trunk [PortNumber] **trunk-link tag** [TaggedVID List]	V	Assign a trunk link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 trunk-link tag 2,3,6,99** or switch(vlan)#**vlan 8021q trunk 3 trunk-link tag 3-20**
vlan 8021q trunk [PortNumber] **hybrid-link untag** [UntaggedVID] **tag** [TaggedVID List]	V	Assign a hybrid link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 hybrid-link untag 4 tag 3,6,8** or switch(vlan)#**vlan 8021q trunk 3 hybrid-link untag 5 tag 6-8**
show vlan [GroupID] or **show vlan**	V	Show VLAN information	switch(vlan)#**show vlan 23**
no vlan group [GroupID]	V	Delete port base group ID	switch(vlan)#**no vlan group 2**

Spanning Tree Commands Set

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

		each of the listening and learning states last before the port begins forwarding.	
stp-path-cost **[1~200000000]**	**I**	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-path-cost 20**
stp-path-priority **[Port Priority]**	**I**	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-path-priority 128**
stp-admin-p2p **[Auto|True|False]**	**I**	Admin P2P of STP priority on this interface.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-admin-p2p Auto**
stp-admin-edge **[True|False]**	**I**	Admin Edge of STP priority on this interface.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-admin-edge True**

stp-admin-non-stp [True|False]	I	Admin NonSTP of STP priority on this interface.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-admin-non-stp False**
show spanning-tree	E	Displays a summary of the spanning-tree states.	switch>**show spanning-tree**
no spanning-tree	G	Disable spanning-tree.	switch(config)#**no spanning-tree**

QOS Commands Set

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

IGMP Commands Set

Command	Level	Description	Example
igmp enable	G	Enable IGMP snooping function	switch(config)#**igmp enable**
igmp query auto	G	Set IGMP query to auto mode	switch(config)#**igmp query auto**
igmp query force	G	Set IGMP query to force mode	switch(config)#**igmp query force**
Show igmp configuration	P	Displays the details of an IGMP configuration.	switch#**show igmp configuration**
Show igmp multi	P	Displays the details of an IGMP snooping entries.	switch#**show igmp multi**
no igmp	G	Disable IGMP snooping function	switch(config)#**no igmp**
no igmp query	G	Disable IGMP query	switch#**no igmp query**

Mac / Filter Table Commands Set

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

[MAC]		interface (static)	switch(config-if)#**no mac-address-table static hwaddr 000012345678**
no mac-address-table filter hwaddr [MAC]	G	Remove an entry of MAC address table (filter)	switch(config)#**no mac-address-table filter hwaddr 000012348678**
no mac-address-table	G	Remove dynamic entry of MAC address table	switch(config)#**no mac-address-table**

SNMP Commands Set

Command	Level	Description	Example
snmp system-name [System Name]	G	Set SNMP agent system name	switch(config)#**snmp system-name l2switch**
snmp system-location [System Location]	G	Set SNMP agent system location	switch(config)#**snmp system-location lab**
snmp system-contact [System Contact]	G	Set SNMP agent system contact	switch(config)#**snmp system-contact where**
snmp agent-mode [v1v2c|v3|v1v2cv3]	G	Select the agent mode of SNMP	switch(config)#**snmp agent-mode v1v2cv3**
snmp community-strings [Community] right [RO/RW]	G	Add SNMP community string.	switch(config)#**snmp community-strings public right rw**
snmp-server host [IP address] community [Community-string] trap-version [v1|v2c]	G	Configure SNMP server host information and community string	switch(config)#**snmp-server host 192.168.1.50 community public trap-version v1** **(remove)** Switch(config)# **no snmp-server host 192.168.1.50**
snmpv3 context-name [Context Name]	G	Configure the context name	switch(config)#**snmpv3 context-name Test**

snmpv3 user [User Name] group [Group Name] password [Authentication Password] [Privacy Password]	G	Configure the userprofile for SNMPV3 agent. Privacy password could be empty.	switch(config)#**snmpv3 user test01 group G1 password AuthPW PrivPW**
snmpv3 access context-name [Context Name] group [Group Name] security-level [NoAuthNoPriv|AuthNoPriv|AuthPriv] match-rule [Exact|Prifix] views [Read View Name] [Write View Name] [Notify View Name]	G	Configure the access table of SNMPV3 agent	switch(config)#**snmpv3 access context-name Test group G1 security-level AuthPriv match-rule Exact views V1 V1 V1**
snmpv3 mibview view [View Name] type [Excluded|Included] sub-oid [OID]	G	Configure the mibview table of SNMPV3 agent	switch(config)#**snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1**
show snmp	P	Show SNMP configuration	switch#**show snmp**
no snmp community-strings [Community]	G	Remove the specified community.	switch(config)#**no snmp community-strings public**
no snmp-server host [Host-address]	G	Remove the SNMP server host.	switch(config)#**no snmp-server 192.168.1.50**
no snmpv3 user	G	Remove specified user	switch(config)#**no snmpv3 user Test**

<table>
<tr><td>[User Name]</td><td></td><td>of SNMPv3 agent.</td><td></td></tr>
<tr><td>no snmpv3 access context-name [Context Name] group [Group Name] security-level [NoAuthNoPriv|AuthNoPriv|AuthPriv] match-rule [Exact|Prifix] views [Read View Name] [Write View Name] [Notify View Name]</td><td>G</td><td>Remove specified access table of SNMPv3 agent.</td><td>switch(config)#**no snmpv3 access context-name Test group G1 security-level AuthPriv match-rule Exact views V1 V1 V1**</td></tr>
<tr><td>no snmpv3 mibview view [View Name] type [Excluded|Included] sub-oid [OID]</td><td>G</td><td>Remove specified mibview table of SNMPV3 agent.</td><td>switch(config)#**no snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1**</td></tr>
</table>

Port Mirroring Commands Set

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

802.1x Commands Set

Command	Level	Description	Example
8021x enable	**G**	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# **8021x enable**
8021x system radiusip **[IP address]**	**G**	Use the 802.1x system radius IP global configuration command to change the radius server IP.	switch(config)# **8021x system radiusip 192.168.1.1**
8021x system serverport **[port ID]**	**G**	Use the 802.1x system server port global configuration command to change the radius server port	switch(config)# **8021x system serverport 1815**
8021x system	**G**	Use the 802.1x system	switch(config)# **8021x system**

accountport [port ID]		account port global configuration command to change the accounting port	**accountport 1816**
8021x system sharekey [ID]	G	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)# **8021x system sharekey 123456**
8021x system nasid [words]	G	Use the 802.1x system nasid global configuration command to change the NAS ID	switch(config)# **8021x system nasid test1**
8021x misc quietperiod [sec.]	G	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch(config)# **8021x misc quietperiod 10**
8021x misc txperiod [sec.]	G	Use the 802.1x misc TX period global configuration command to set the TX period.	switch(config)# **8021x misc txperiod 5**
8021x misc supportimeout [sec.]	G	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	switch(config)# **8021x misc supportimeout 20**
8021x misc servertimeout [sec.]	G	Use the 802.1x misc server timeout global configuration command to set the server timeout.	switch(config)#**8021x misc servertimeout 20**

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

TFTP Commands Set

Command	Level	Description	Defaults Example
backup flash:backup_cfg	G	Save configuration to TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#**backup flash:backup_cfg**
restore flash:restore_cfg	G	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.	switch(config)#**restore flash:restore_cfg**
upgrade flash:upgrade_fw	G	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#**upgrade flash:upgrade_fw**

SystemLog, SMTP and Event Commands Set

Command	Level	Description	Example
systemlog ip [IP address]	**G**	Set System log server IP address.	switch(config)# **systemlog ip 192.168.1.100**
systemlog mode [client|server|both]	**G**	Specified the log mode	switch(config)# **systemlog mode both**
show systemlog	**E**	Displays system log.	Switch>**show systemlog**
show systemlog	**P**	Show system log client & server information	switch#**show systemlog**
no systemlog	**G**	Disable systemlog functon	switch(config)#**no systemlog**
smtp enable	**G**	Enable SMTP function	switch(config)#**smtp enable**
smtp serverip [IP address]	**G**	Configure SMTP server IP	switch(config)#**smtp serverip 192.168.1.5**
smtp authentication	**G**	Enable SMTP authentication	switch(config)#**smtp authentication**
smtp account [account]	**G**	Configure authentication account	switch(config)#**smtp account User**
smtp password [password]	**G**	Configure authentication password	switch(config)#**smtp password**
smtp rcptemail [Index] [Email address]	**G**	Configure Rcpt e-mail Address	switch(config)#**smtp rcptemail 1 Alert@test.com**
show smtp	**P**	Show the information of SMTP	switch#**show smtp**
no smtp	**G**	Disable SMTP function	switch(config)#**no smtp**
event device-cold-start [Systemlog|SMTP|Both]	**G**	Set cold start event type	switch(config)#**event device-cold-start both**
event authentication-failure [Systemlog|SMTP|Both]	**G**	Set Authentication failure event type	switch(config)#**event authentication-failure both**
event ring-topology-change [Systemlog|SMTP|Both]	**G**	Set X-ring topology changed event type	switch(config)#**event ring-topology-change both**

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

SNTP Commands Set

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

X-ring Commands Set

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

Web-Based Management

About Web-based Management

On CPU board of the switch there is an embedded HTML web site residing in the flash memory. This Graphic User Interface (GUI) offers advanced management features and allows users to manage the switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The Web-Based Management supports Internet Explorer 6.0 or later version. It is applied for Java Applets to reducing the network bandwidth requirement while enhancing access speed and presenting an easy viewing screen.

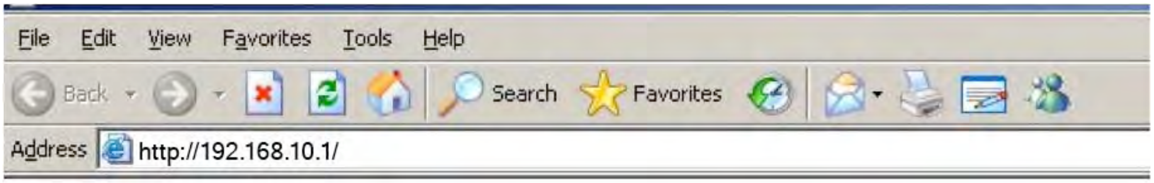
Preparing for Web Management

Before using the web-based management interface, install the switch on the network and make sure that any one of the PCs on the network can connect with the switch through the web browser. The switch's default IP address, subnet mask, username and password is shown below:

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

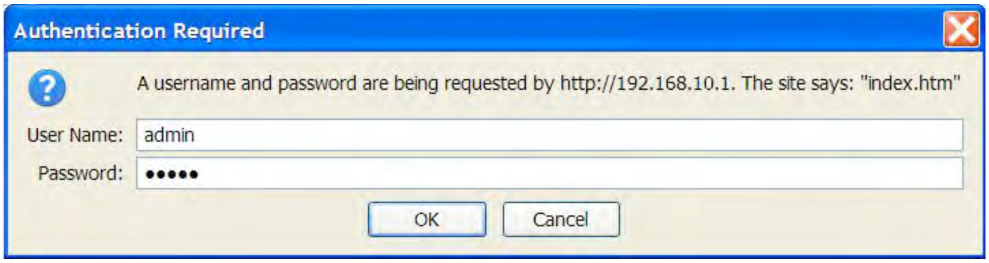
System Login

1. Launch Internet Explorer on the PC
2. Enter ‘http:// and the default IP address in the browser address bar. Press **Enter** or **Return**.



Address http://192.168.10.1/

3. The login screen will appear.
4. Enter the user name and password. The default user name and password are the same: **admin**
5. Press **Enter** or **OK**, and then the home screen of the Web-based management appears as shown below:



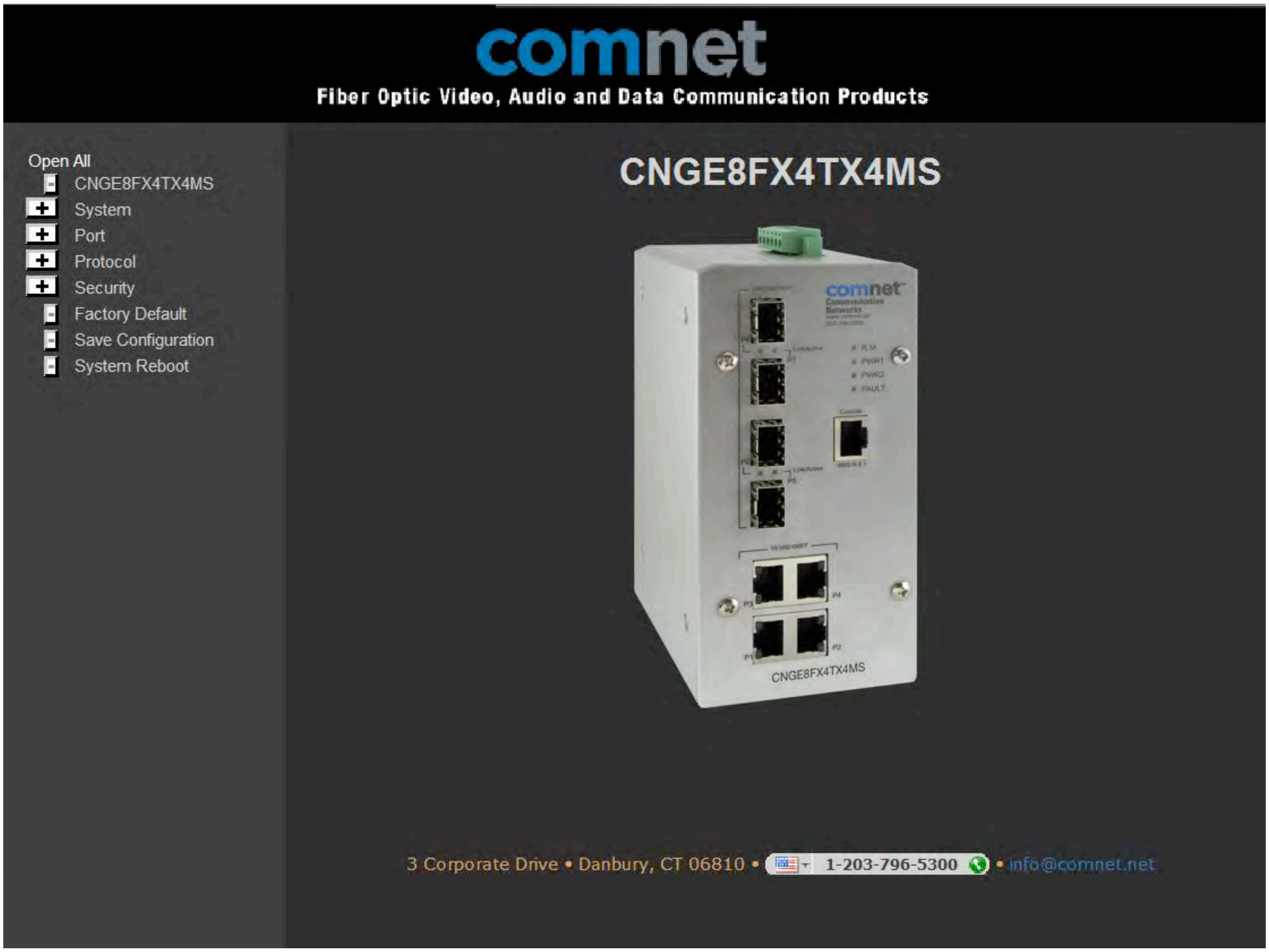
A username and password are being requested by http://192.168.10.1. The site says: "index.htm"

User Name: admin

Password: •••••

Login screen

Main interface



comnet

Fiber Optic Video, Audio and Data Communication Products

Open All

- CNGE8FX4TX4MS
- System
- Port
- Protocol
- Security
- Factory Default
- Save Configuration
- System Reboot

CNGE8FX4TX4MS

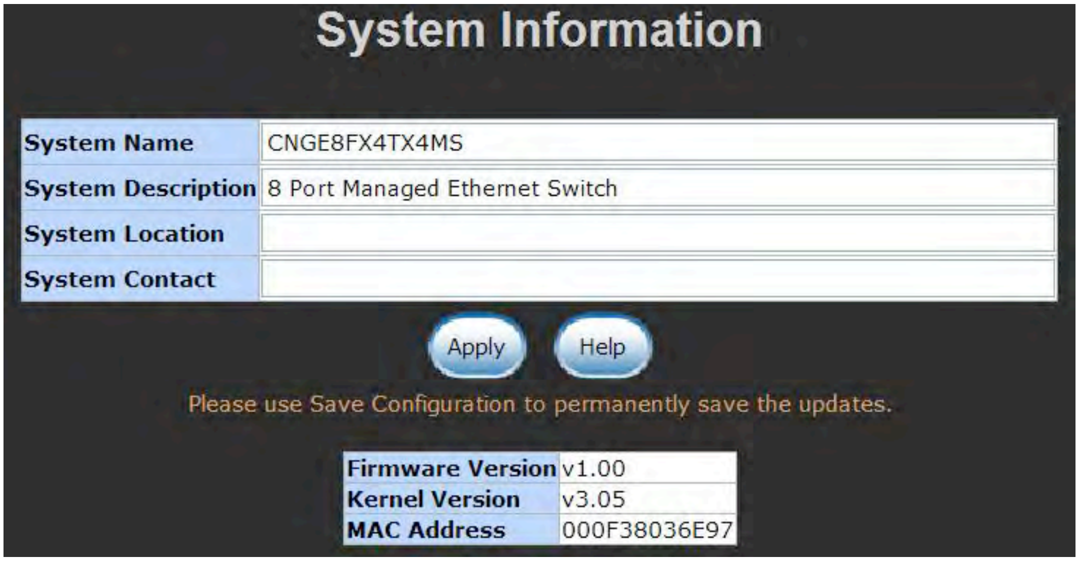
3 Corporate Drive • Danbury, CT 06810 • 1-203-796-5300 • info@comnet.net

Main interface

System Information

Assigning the system name, location and viewing the system information

- **System Name:** Assign the name of switch. The maximum length is 64 bytes
- **System Description:** Displays the description of switch. This is Read only and cannot be modified
- **System Location:** Assign the switch physical location. The maximum length is 64 bytes
- **System Contact:** Enter the name of contact person or organization
- **Firmware Version:** Displays the switch's firmware version
- **Kernel Version:** Displays the kernel software version
- **MAC Address:** Displays the unique hardware address assigned by manufacturer (default)



System Information

System Name	CNGE8FX4TX4MS
System Description	8 Port Managed Ethernet Switch
System Location	
System Contact	

Please use Save Configuration to permanently save the updates.

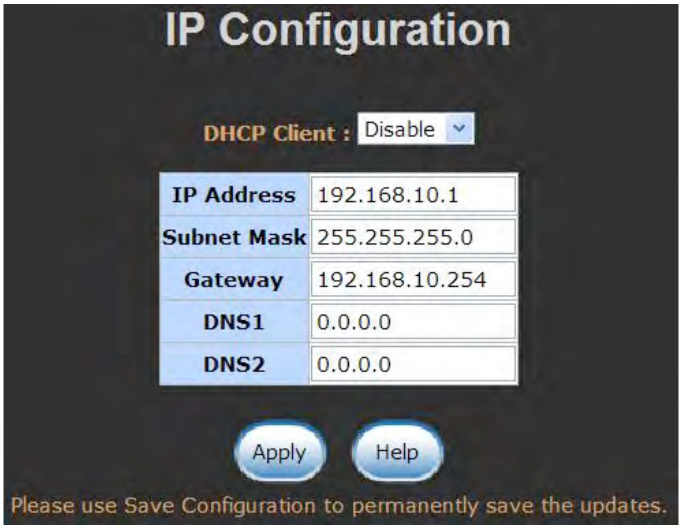
Firmware Version	v1.00
Kernel Version	v3.05
MAC Address	000F38036E97

System information interface

IP Configuration

To configure the IP Settings and DHCP client function

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



IP Configuration

DHCP Client : Disable

IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Gateway	192.168.10.254
DNS1	0.0.0.0
DNS2	0.0.0.0

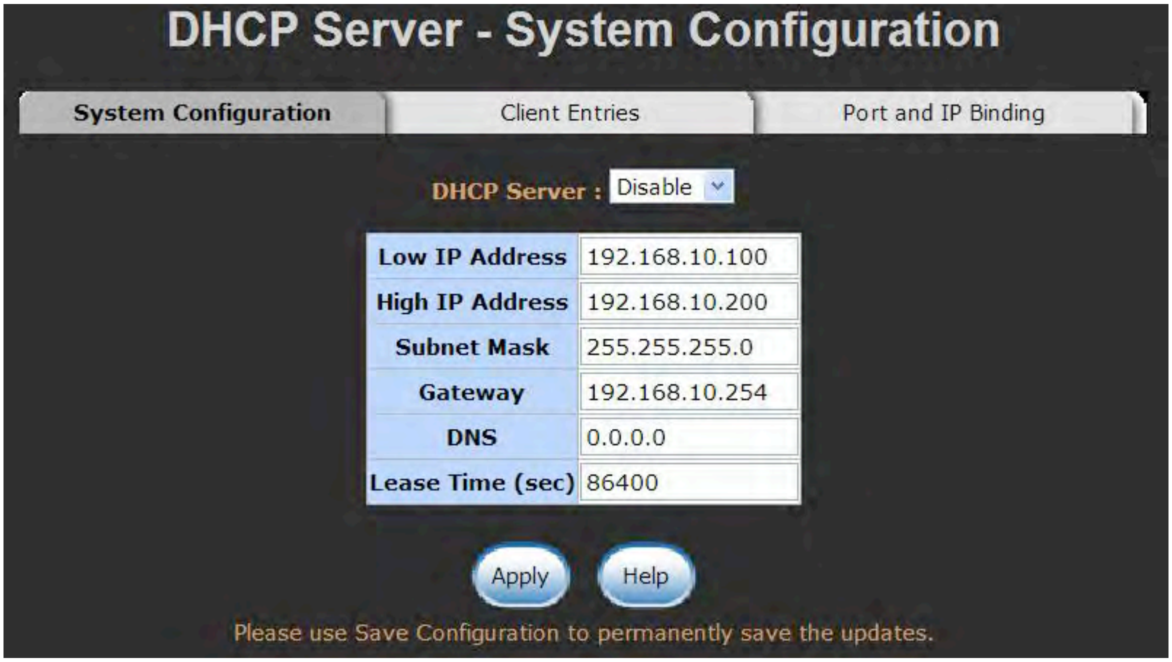
Please use Save Configuration to permanently save the updates.

IP configuration interface

DHCP Server – System configuration

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

- **DHCP Server:** Enable – the switch will become the DHCP server on your local network.
- **Low IP Address:** Low IP address is the beginning of the dynamic IP assignment range. For example: dynamic IP assignment range is from 192.168.10.100 ~ 192.168.10.200. In contrast, 192.168.10.100 is the Low IP address.
- **High IP Address:** High IP address is the end of the dynamic IP assignment range. For example: dynamic IP assignment range is from 192.168.10.100 ~ 192.168.10.200. In comparison, 192.168.10.200 is the High IP address.
- **Subnet Mask:** the dynamic IP assignment range subnet mask.
- **Gateway:** the gateway in your network.
- **DNS:** Domain Name Server IP Address in your network.
- **Lease Time (sec):** It is the time period that system will reset the dynamic IP assignment to ensure the dynamic IP will not been occupied for a long period of time or the server does not know that the dynamic IP is idle.
- And then, select Apply



DHCP Server - System Configuration

DHCP Server : Disable

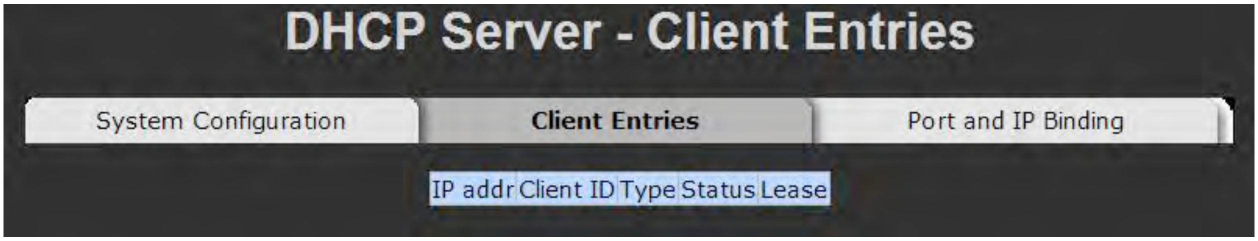
Low IP Address	192.168.10.100
High IP Address	192.168.10.200
Subnet Mask	255.255.255.0
Gateway	192.168.10.254
DNS	0.0.0.0
Lease Time (sec)	86400

Please use Save Configuration to permanently save the updates.

DHCP Server Configuration interface

DHCP Client – System Configuration

When the DHCP server function is active, the system will collect the DHCP client information and display it here.



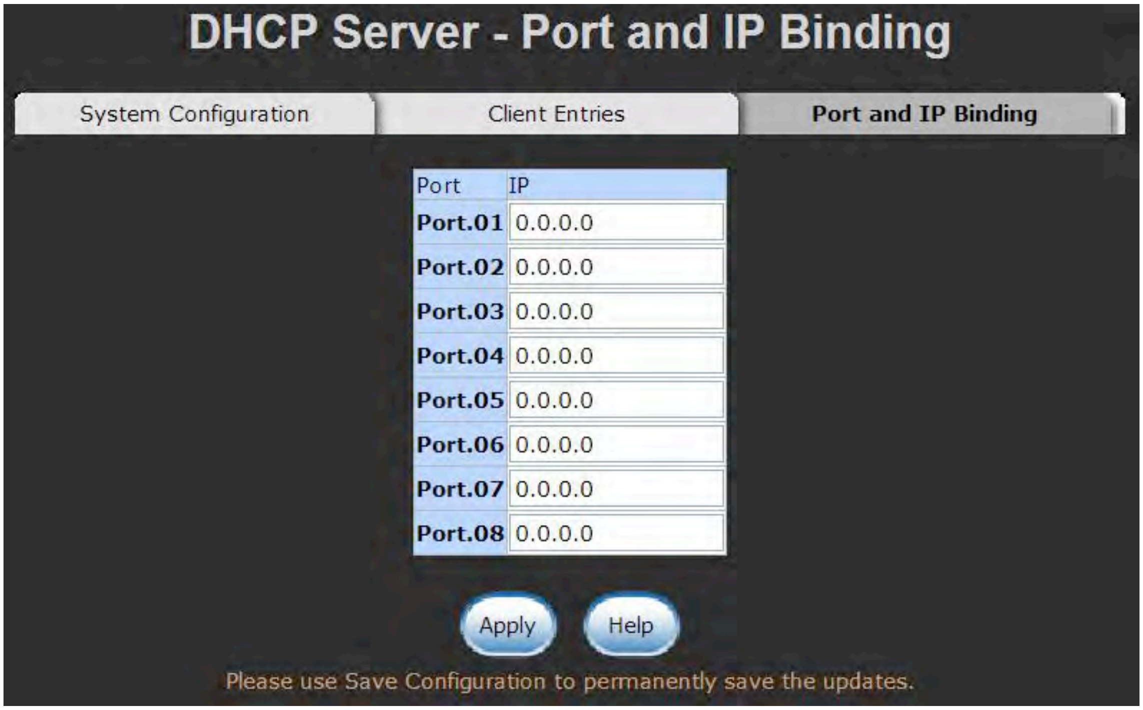
DHCP Server - Client Entries

IP addr	Client ID	Type	Status	Lease

DHCP Client Entries interface

DHCP Server - Port and IP Bindings

You can assign the specific IP address that is the IP address in dynamic IP address assignment range to the specific port. When the device is connected to the port and requests dynamic IP address assignment, the system will assign the IP address that has been assigned previously to the connected device.



DHCP Server - Port and IP Binding

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

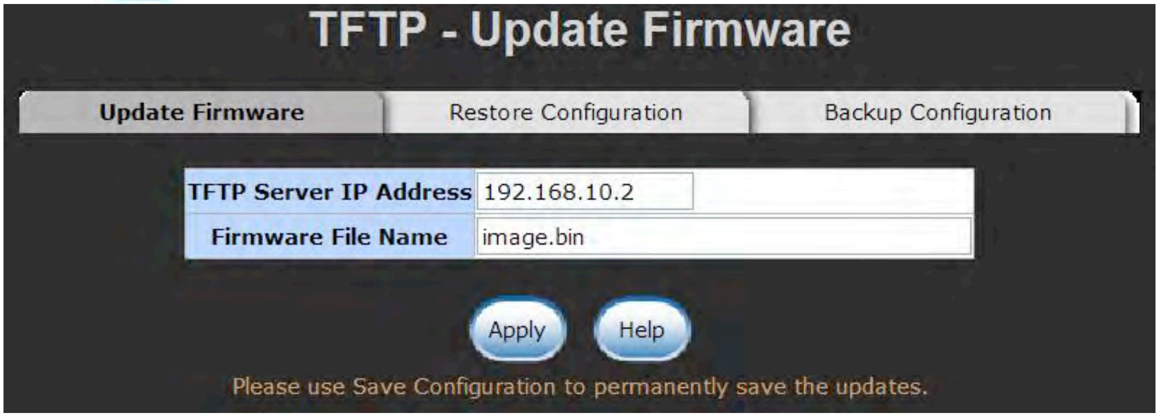
Please use Save Configuration to permanently save the updates.

Port and IP Bindings interface

TFTP – Firmware Update

It provides the functions to allow a user to update the switch’s firmware. Before updating, make sure you have your TFTP server ready and the firmware image is on the TFTP server.

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



TFTP - Update Firmware

TFTP Server IP Address	192.168.10.2
Firmware File Name	image.bin

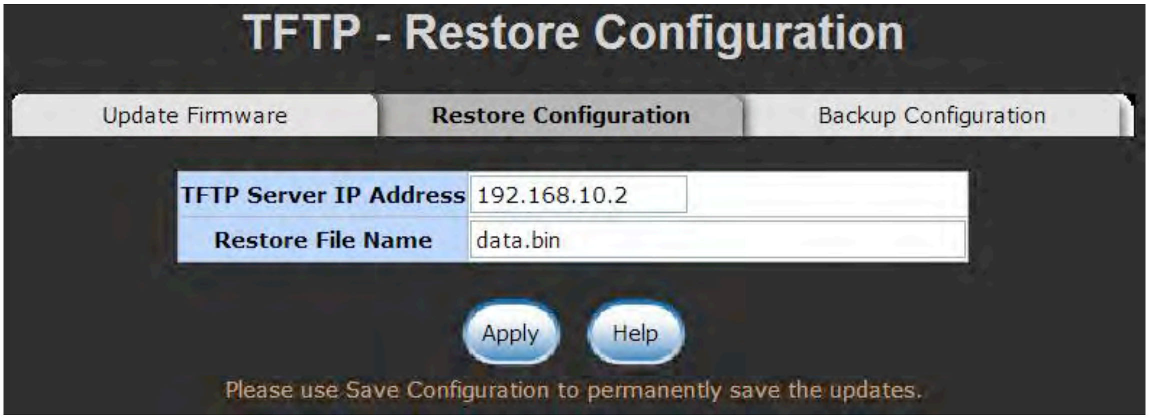
Please use Save Configuration to permanently save the updates.

Update Firmware interface

TFTP – Restore Configuration

You can restore EEPROM value from TFTP server, but you must put the file on the TFTP server first, the switch will download back the flash image.

1. **TFTP Server IP Address:** Enter the TFTP server IP address.
2. **Restore File Name:** fill in the correct restore file name.
3. Select Apply.



TFTP - Restore Configuration

TFTP Server IP Address	192.168.10.2
Restore File Name	data.bin

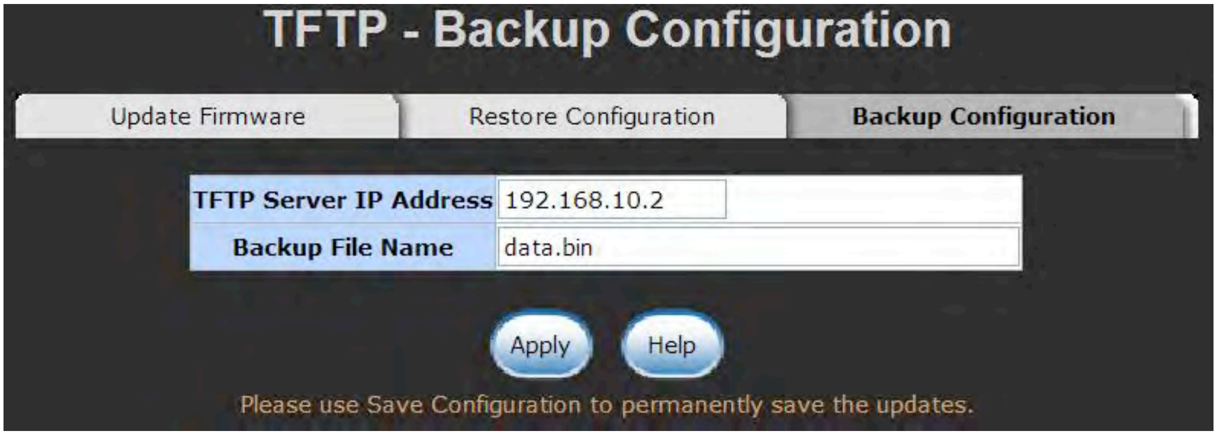
Please use Save Configuration to permanently save the updates.

Restore Configuration interface

TFTP - Backup Configuration

You can save current EEPROM value from the switch to the TFTP server. You can then go to the TFTP restore configuration page to restore the EEPROM value.

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



TFTP Server IP Address	192.168.10.2
Backup File Name	data.bin

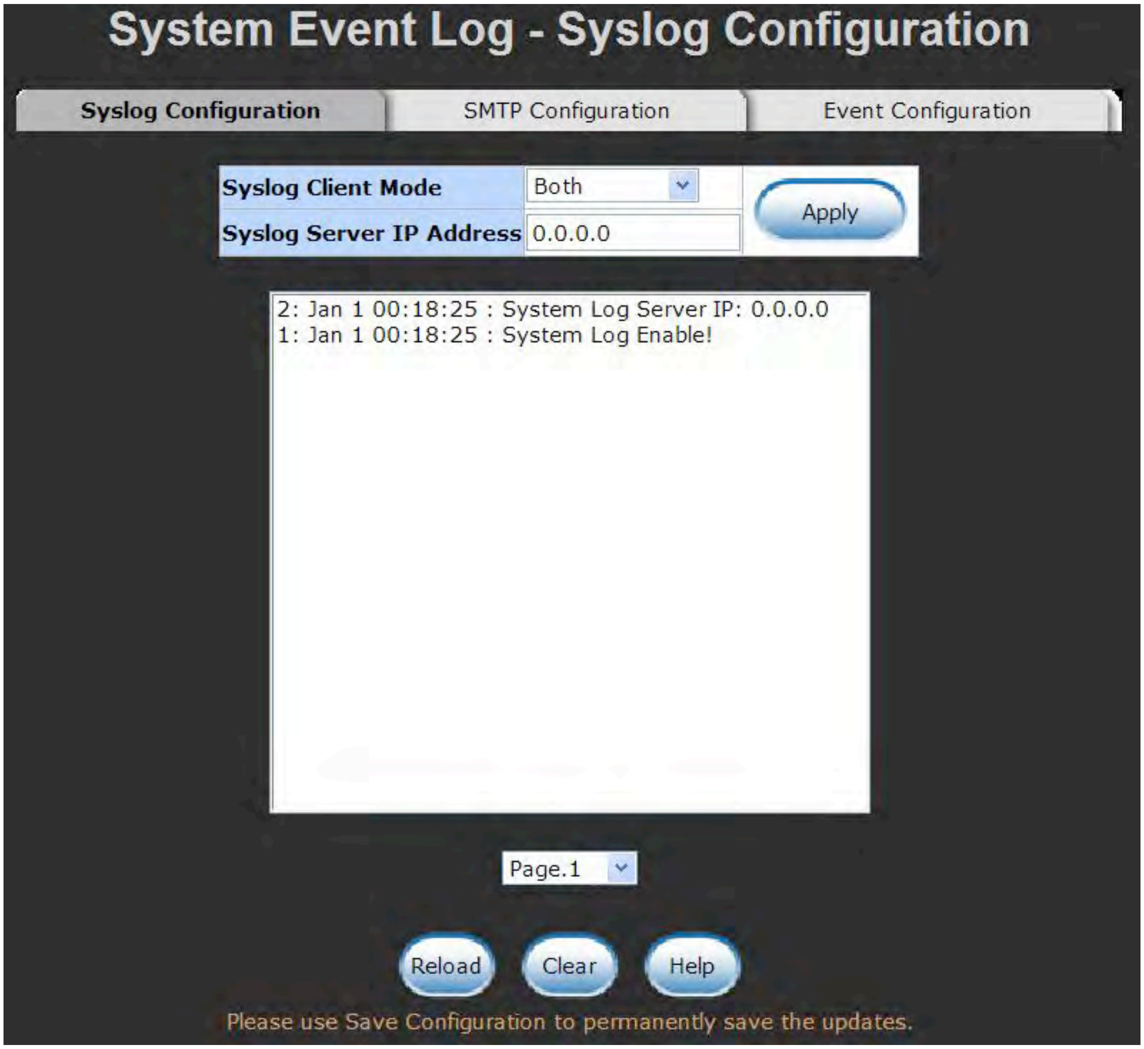
Please use Save Configuration to permanently save the updates.

Backup Configuration interface

System Event Log – Syslog Configuration

Configuring the system event mode that can be collected and the system log server IP address.

1. **Syslog Client Mode:** select the system log mode – client only, server only, or both client and server.
2. **System Log Server IP Address:** assigns the system log server IP address.
3. Select Reload to refresh the events log.
4. Select Clear to clear all current events log.
5. After configuring, select Apply.



Syslog Client Mode: Both

Syslog Server IP Address: 0.0.0.0

```
2: Jan 1 00:18:25 : System Log Server IP: 0.0.0.0
1: Jan 1 00:18:25 : System Log Enable!
```

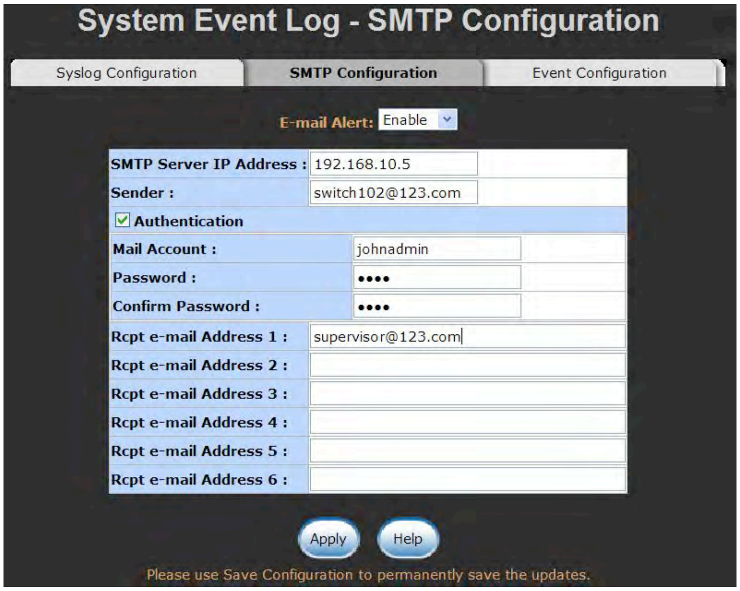
Please use Save Configuration to permanently save the updates.

Syslog Configuration interface

System Event Log - SMTP Configuration

You can set up the mail server IP address, Email address accounts, account passwords, and forwarded Email accounts for receiving the event alert.

1. **Email Alert:** enable or disable the Email alert function.
2. **SMTP Server IP:** set up the mail server IP address (when **Email Alert** is enabled, this function will then be available).
3. **Sender:** Enter in a complete Email address, e.g. switch102@123.com, to identify where the event log comes from.
4. **Authentication:** Select the check box to enable and configure the Email account and password needed for authentication (when **Email Alert** enabled, this function will then be available).
5. **Mail Account:** set up the Email account, e.g. johnadmin@123.com, to receive the alert. It must be an existing Email account on the mail server, which had been set up in **SMTP Server IP Address** column.
6. **Password:** The Email account's required password.
7. **Confirm Password:** reconfirm the password.
8. **Recipient Email Addresses 1 ~ 6:** you can assign up to 6 Email accounts also to receive the alert.
9. Select Apply.



System Event Log - SMTP Configuration

E-mail Alert: Enable

SMTP Server IP Address :	192.168.10.5
Sender :	switch102@123.com
☑ Authentication	
Mail Account :	johnadmin
Password :	••••
Confirm Password :	••••
Rcpt e-mail Address 1 :	supervisor@123.com
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 :	

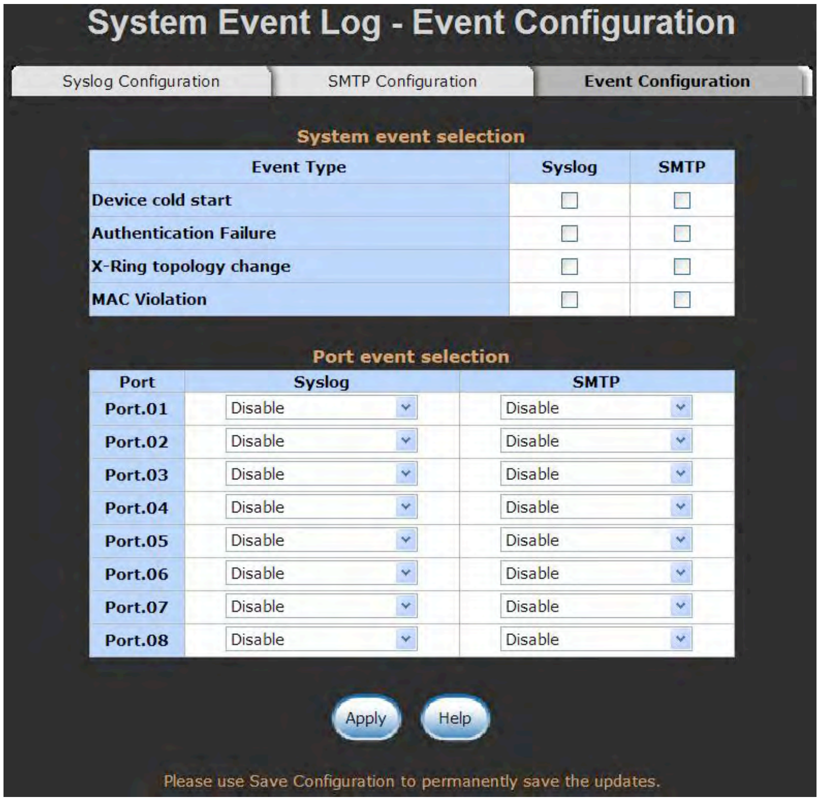
Please use Save Configuration to permanently save the updates.

SMTP Configuration interface

System Event Log - Event Configuration

You can select the system log events and SMTP events. When selected events occur, the system will send out the event log information. Also, event per port log and SMTP events can be selected. After configure, select Apply .

- **System event selection:** Four selections – 1) Device cold start, 2) Device warm start, 3) SNMP Authentication Failure, and 4) Topology change. Mark the checkbox to select the events to be monitored. When selected events occur, the system will log the event(s).
    - **Device cold start:** when the device executes cold start action, the system will note a log event.
    - **Authentication Failure:** when the SMTP authentication fails, the system will note a log event.
    - **X-ring topology change:** when the X-ring topology has changed, the system will note a log event.



System Event Log - Event Configuration

System event selection

Event Type	Syslog	SMTP
Device cold start	□	□
Authentication Failure	□	□
X-Ring topology change	□	□
MAC Violation	□	□

Port event selection

Port	Syslog	SMTP
Port.01	Disable	Disable
Port.02	Disable	Disable
Port.03	Disable	Disable
Port.04	Disable	Disable
Port.05	Disable	Disable
Port.06	Disable	Disable
Port.07	Disable	Disable
Port.08	Disable	Disable

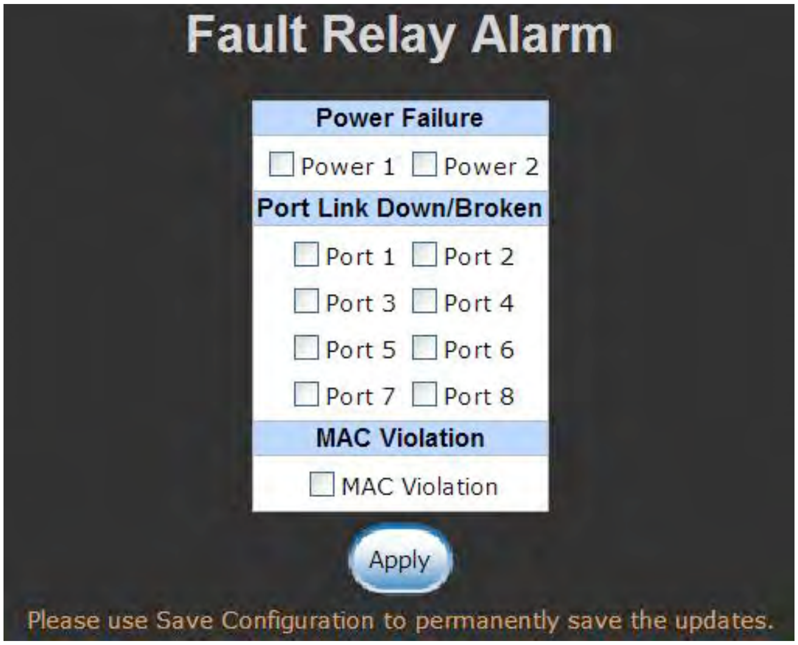
Please use Save Configuration to permanently save the updates.

Event Configuration interface

- **Port event selection:** select the per port events and per port SMTP events. It has three selections – 1) Link UP, 2) Link Down, and 3) Link UP & Link Down. Disable means no event is selected.
  - **Link UP:** the system will issue a log message when port connection is up only.
  - **Link Down:** the system will issue a log message when port connection is down only.
  - **Link UP & Link Down:** the system will issue a log message when port connection is up and down.

Fault Relay Alarm

- **Power Failure:** Select the check box to enable the function of lighting up **FAULT** LED on the panel in the event of a power failure.
- **Port Link Down/Broken:** Mark the check box to enable the function of lighting up **FAULT** LED on the panel when Ports' state reflect link down or link broken.



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
MAC Violation	
□ MAC Violation	

Please use Save Configuration to permanently save the updates.

Fault Relay Alarm interface

SNTP Configuration

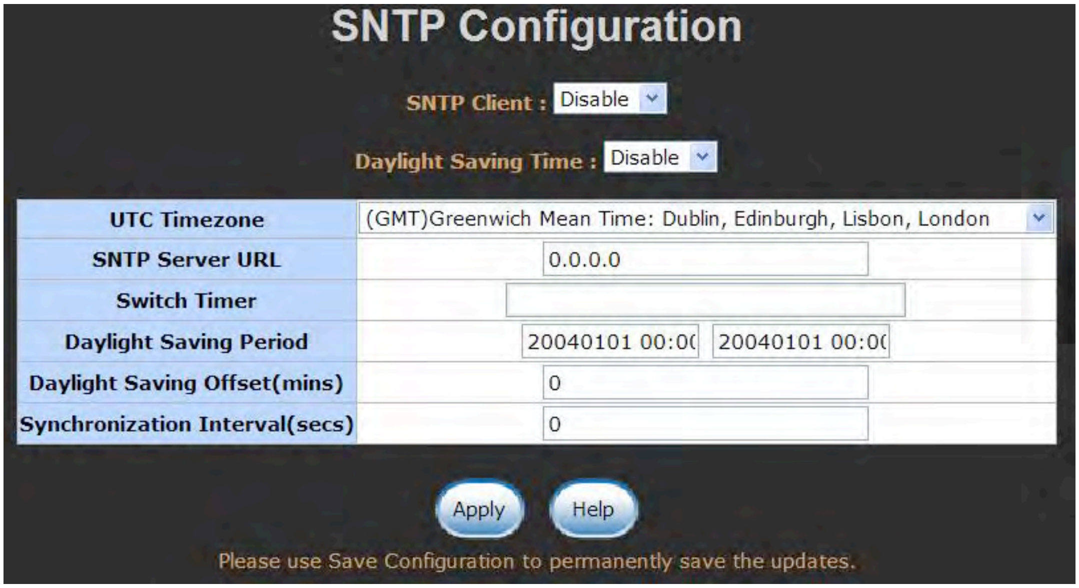
You can configure the SNTP (Simple Network Time Protocol) settings. The SNTP allows you to synchronize the switch's clocks through the internet website.

1. **SNTP Client:** enable or disable SNTP function to get the time from the SNTP server.
2. **Daylight Saving Time:** enable or disable daylight savings time function. When daylight saving time is enabling, you need to configure the daylight saving time period.
3. **UTC Timezone:** set the switch location time zone.

The table on the following page lists the different location time zone for your reference.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter 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

4. **SNTP Server URL:** set the SNTP server IP address.
5. **Daylight Saving Period:** set up the Daylight Saving beginning date and Daylight Savings ending date. Both will be different in every year.
6. **Daylight Savings Offset (mins):** set the offset time.
7. **Switch Timer:** Displays the current switch time.
8. Select Apply.



SNTP Configuration

SNTP Client : Disable

Daylight Saving Time : Disable

UTC Timezone	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
SNTP Server URL	0.0.0.0
Switch Timer	
Daylight Saving Period	20040101 00:0(20040101 00:0(
Daylight Saving Offset(mins)	0
Synchronization Interval(secs)	0

Please use Save Configuration to permanently save the updates.

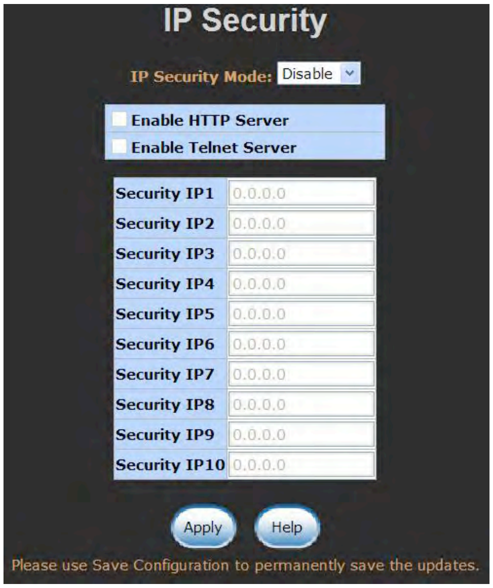
SNTP Configuration interface

IP Security

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

- **IP Security Mode:** when this option is in the **Enable** mode, the **Enable HTTP Server** and **Enable Telnet Server** check boxes will then be available.
- **Enable HTTP Server:** when this check box is checked, the IP addresses among Security IP1 ~ IP10 will be allowed access via HTTP service.
- **Enable Telnet Server:** when checked, the IP addresses among Security IP1 ~ IP10 will be allowed to access via telnet service.
- **Security IP 1 ~ 10:** Assign up to 10 specific IP address. Only these 10 IP address can access and manage the switch through the Web browser
- And then, select Apply button to apply the configuration

Note *Remember to execute the 'Save Configuration' action, otherwise the new configuration will be lost when switch is powered off*



IP Security

IP Security Mode: Disable

□ Enable HTTP Server
□ Enable Telnet Server

Security IP1	0.0.0.0
Security IP2	0.0.0.0
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

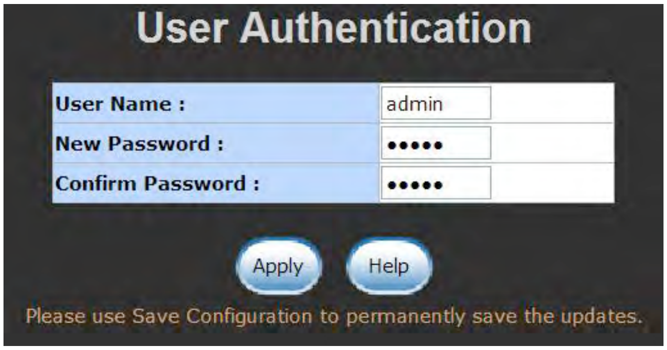
Please use Save Configuration to permanently save the updates.

IP Security interface

User Authentication

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

1. **User name:** Enter the new user name (The default is **admin**)
2. **Password:** Enter the new password (The default is **admin**)
3. **Confirm password:** Re-type the new password
4. And then, select Apply



User Authentication

User Name :	admin
New Password :	•••••
Confirm Password :	•••••

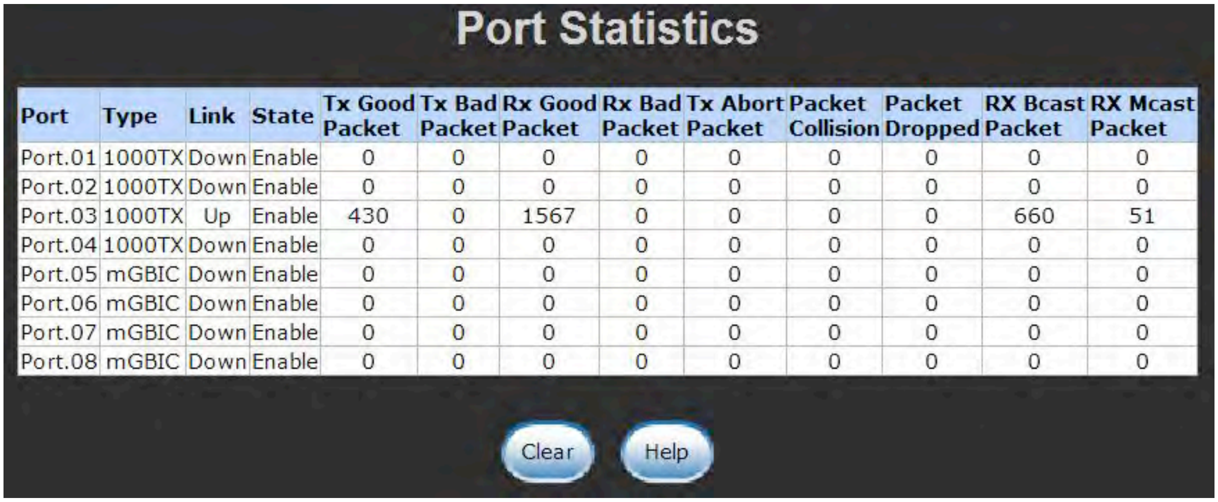
Please use Save Configuration to permanently save the updates.

User Authentication interface

Port Statistics

The following information provides current port information statistics.

- **Port:** The port number.
- **Type:** Displays the current connection speed of the port.
- **Link:** The linkstatus — port is ‘**Up**’ or ‘**Down**’.
- **State:** Set by Port Control. When the state is disabled, the port will not transmit or receive any packet.
- **Tx (Transmit) Good Packet:** The counts of transmitting good packets via this port.
- **Tx (Transmit) Bad Packet:** The counts of transmitting bad packets (including undersize [less than 64 octets], oversize, CRC Align errors, fragments and jabbers packets) via this port.
- **Rx (Receive) Good Packet:** The counts of receiving good packets via this port.
- **Rx (Receive) Bad Packet:** The counts of receiving good packets (including undersize [less than 64 octets], oversize, CRC error, fragments and jabbers) via this port.
- **Tx (Transmit) Abort Packet:** The aborted packets lost while transmitting.
- **Packet Collision:** The counts of packets lost through collision.
- **Packet Dropped:** The counts of packets lost when dropped.
- **Rx (Receive) Bcast (Broadcast) Packet:** The counts of broadcast packets.
- **Rx (Receive) Mcast (Multicast) Packet:** The counts of multicast packets.
- Select Clear button to clear all counts.



Port Statistics

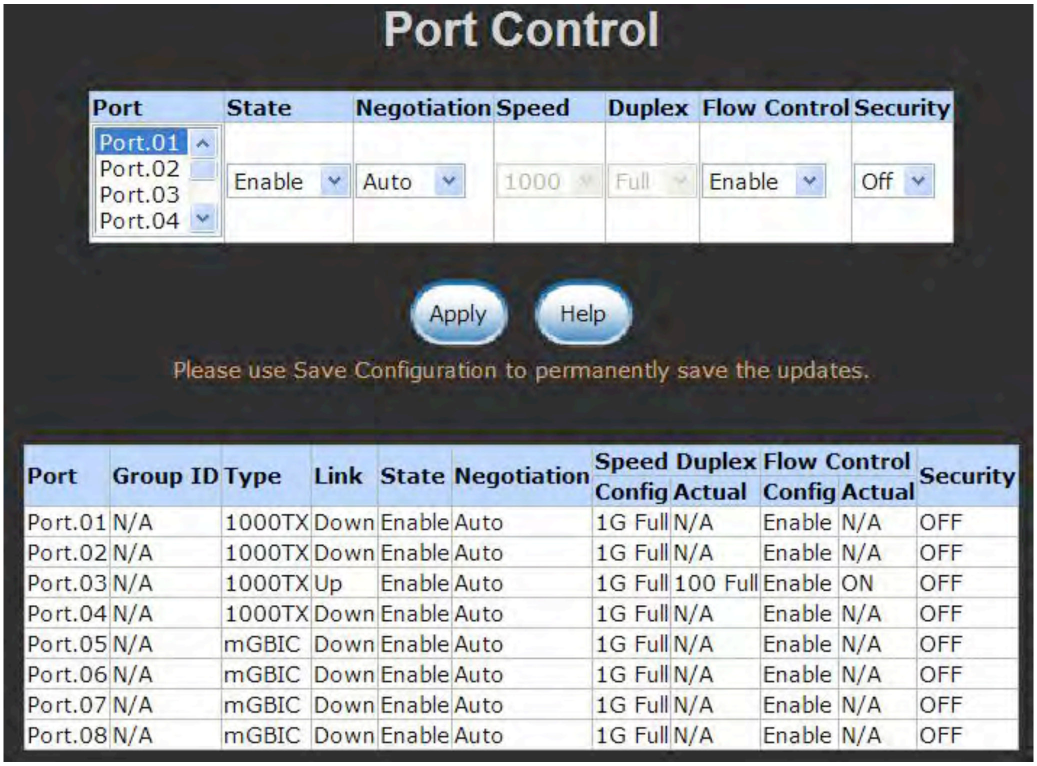
Port	Type	Link	State	Tx Good Packet	Tx Bad Packet	Rx Good Packet	Rx Bad Packet	Tx Abort Packet	Packet Collision	Packet Dropped	RX Bcast Packet	RX Mcast Packet
Port.01	1000TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.02	1000TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.03	1000TX	Up	Enable	430	0	1567	0	0	0	0	660	51
Port.04	1000TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.05	mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0
Port.06	mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0
Port.07	mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0
Port.08	mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0

Port Statistics interface

Port Control

In Port Control, you can view the status of every port status that depends on the user setting and the negotiation result.

1. **Port:** select the port that you want to configure.
2. **State:** Current port status. The port can be set to disable or enable mode. If the port setting is disabled then it will not receive or transmit any packet.
3. **Negotiation:** set auto negotiation status of the port.
4. **Speed:** set the link speed of the port.
5. **Duplex:** set full-duplex or half-duplex mode of the port.
6. **Flow Control:** The flow control function is **Symmetric** or **Asymmetric** in Full Duplex mode. The default value is **Symmetric**.
7. **Security:** When its state is **On**, it means this port accepts only one MAC address.
8. Select Apply.



Port Control

Port	State	Negotiation	Speed	Duplex	Flow Control	Security
Port.01 Port.02 Port.03 Port.04	Enable	Auto	1000	Full	Enable	Off

Please use Save Configuration to permanently save the updates.

Port	Group ID	Type	Link	State	Negotiation	Speed	Duplex	Flow Control		Security
						Config	Actual	Config	Actual	
Port.01	N/A	1000TX	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.02	N/A	1000TX	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.03	N/A	1000TX	Up	Enable	Auto	1G Full	100 Full	Enable	ON	OFF
Port.04	N/A	1000TX	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.05	N/A	mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.06	N/A	mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.07	N/A	mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.08	N/A	mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF

Port Control interface

Port Trunk

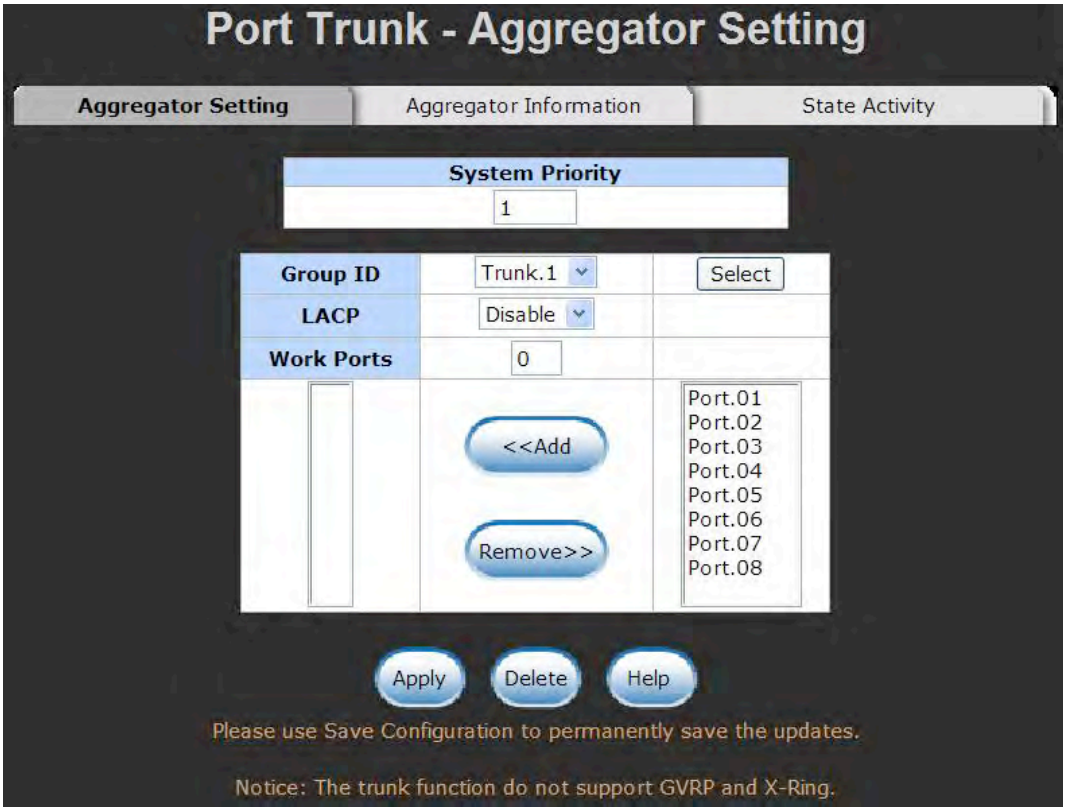
The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs. It can also move the link to that Link Aggregation Group and enable its transmission and receive functions to occur in an orderly manner. Link aggregation lets you group up to four consecutive ports into two dedicated connections. This feature can expand bandwidth to a device on the network. **LACP operation requires full-duplex mode,** more detailed information refers to IEEE 802.3ad.

Aggregator setting

1. **System Priority:** a value used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.
2. **Group ID:** There are three trunk groups to provide configure. Choose the **Group ID** and select Select.
3. **LACP:** If enabled, the group is LACP static trunk group. If disabled, the group is the local static trunk group. All ports support LACP dynamic trunk group. If connected to the device that also supports LACP, the LACP dynamic trunk group will be created automatically.
4. **Work ports:** allows a maximum of four ports to be aggregated at the same time. With LACP static trunk group, the exceed ports are on standby and can be aggregated if the working ports fail. If it is part of the local static trunk group, the number of ports must be the same as the group member ports.
5. Select the ports to join the trunk group. Allow max four ports can be aggregated at the same time. Select <<Add button to add the port. To remove unwanted ports, select the port and select Remove>> button.
6. If LACP enabled, you can configure LACP Active/Passive status in each of the ports on State Activity page.

7. Select Apply.

8. Use Delete button to delete the Trunk Group. Select the Group ID and select Delete.



Port Trunk - Aggregator Setting

System Priority
1

Group ID	Trunk.1	Select
LACP	Disable	
Work Ports	0	
		Port.01 Port.02 Port.03 Port.04 Port.05 Port.06 Port.07 Port.08

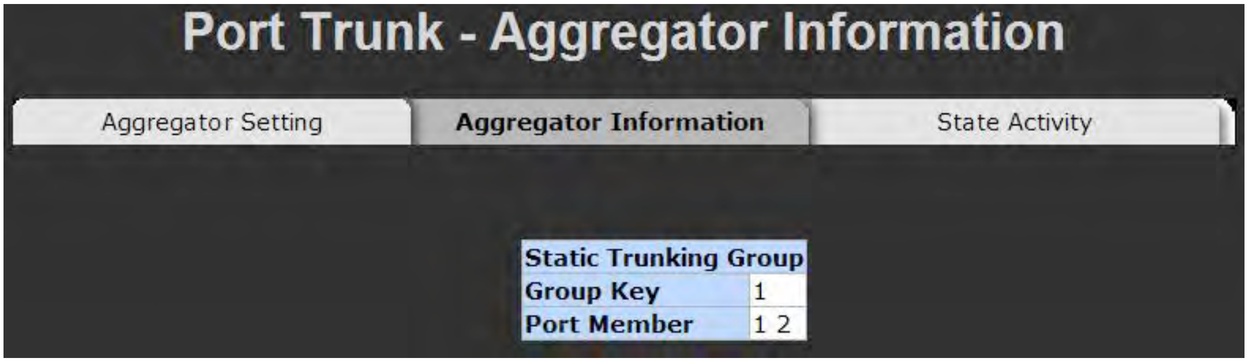
Please use Save Configuration to permanently save the updates.

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

Port Trunk—Aggregator Setting interface

Aggregator Information

When you set the aggregator setting with LACP disabled, the local static trunk group information will be displayedhere.



Port Trunk - Aggregator Information

Static Trunking Group	
Group Key	1
Port Member	1 2

Port Trunk – Aggregator Information interface

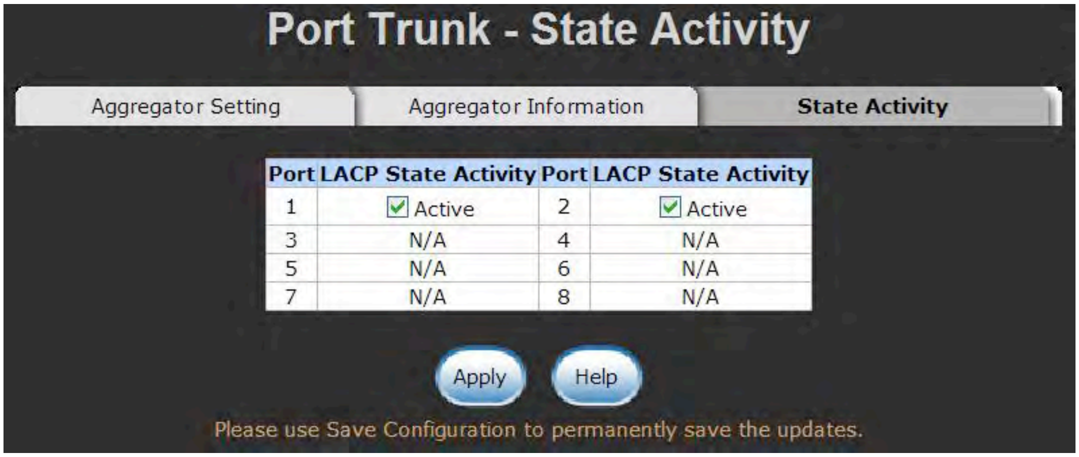
State Activity

When you setup the LACP aggregator, you can configure port state activity. You can select or deselect the port. When you mark the port and select Apply button the port state activity will change to **Active**. Opposite is **Passive**.

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

Note

1. *A link having either two active LACP ports or one active port can perform dynamic LACP trunk.*
2. *A link has two passive LACP ports will not perform dynamic LACP trunk because both ports are waiting for an LACP protocol packet from the opposite device.*
3. *If you are the active LACP's aggregator, after you have selected trunk port, the active status will be created automatically.*



Port	LACP State Activity	Port	LACP State Activity
1	☑ Active	2	☑ Active
3	N/A	4	N/A
5	N/A	6	N/A
7	N/A	8	N/A

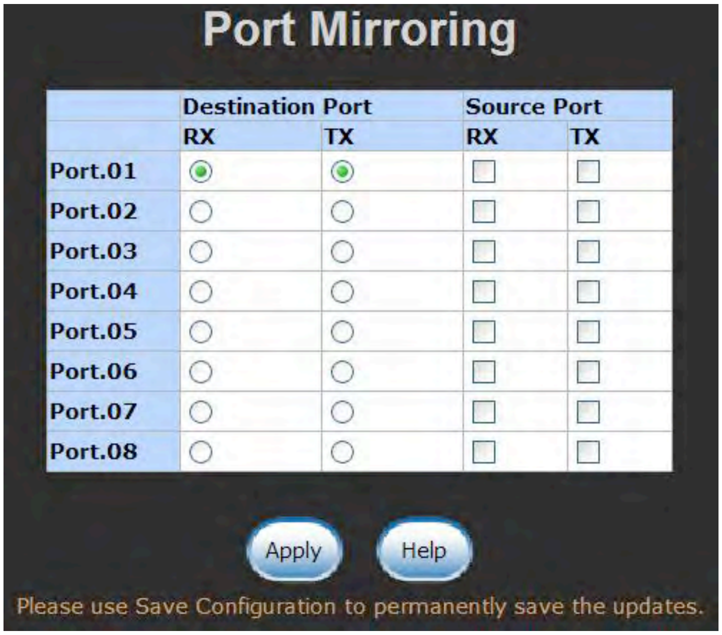
Please use Save Configuration to permanently save the updates.

Port Trunk – State Activity interface

Port Mirroring

The Port mirroring is a method for monitoring traffic in switched networks. Traffic through the ports can be monitored by one specific port. That means traffic that goes in or out monitored (source) ports will be duplicated into a mirror (destination) port.

- **Destination Port:** There is only one port can be selected to be the destination (mirror) port for monitoring both RX and TX traffic that comes from the source port. Or, use one of two ports for monitoring RX traffic only and the other port for TX traffic only. The user can connect the mirror port to LAN analyzer or Netxray.
- **Source Port:** The ports that the user wants to monitor. All monitored port traffic will be copied to a mirror (destination) port. The user can select multiple source ports by checking the **RX** or **TX** check boxes of the ports to be monitored.
- And then, select Apply button.



Port Mirroring

	Destination Port		Source Port	
	RX	TX	RX	TX
Port.01	●	●	□	□
Port.02	○	○	□	□
Port.03	○	○	□	□
Port.04	○	○	□	□
Port.05	○	○	□	□
Port.06	○	○	□	□
Port.07	○	○	□	□
Port.08	○	○	□	□

Please use Save Configuration to permanently save the updates.

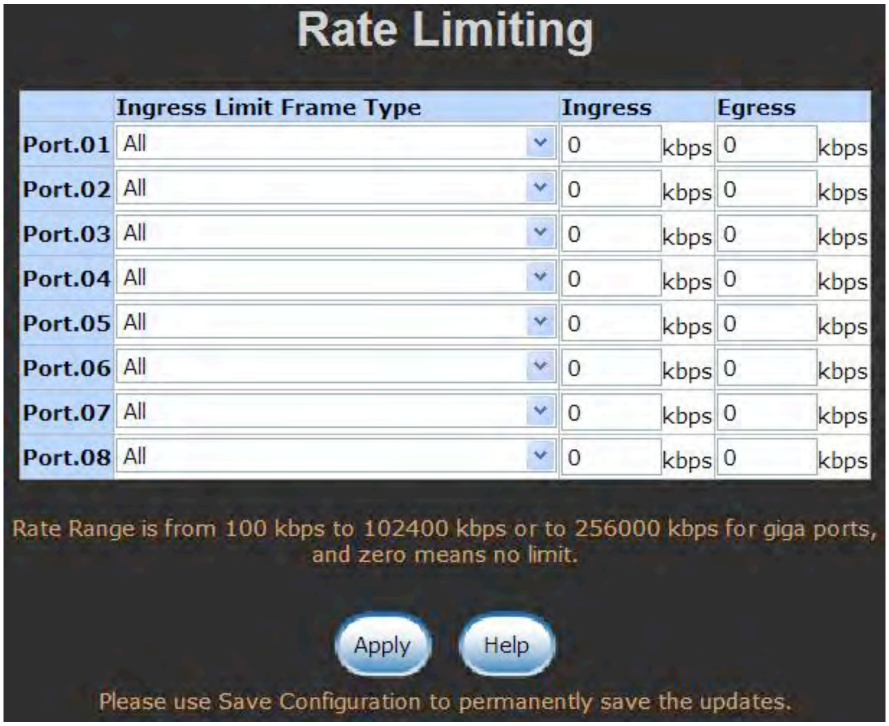
Port Trunk – Port Mirroring interface

Rate Limiting

You can set up every port's bandwidth rate and frame limitation type.

- **Ingress Limit Frame type:** select the frame type that wants to filter. The frame types have four options for selecting: 1) **All,** 2) **Broadcast/Multicast/Flooded Unicast,** 3) **Broadcast/Multicast** and 4) **Broadcast only.**

Broadcast/Multicast/Flooded Unicast, Broadcast/Multicast and **Bbroadcast only** types are only for ingress frames. The egress rate only supports **All** type.



Rate Limiting

	Ingress Limit Frame Type	Ingress	Egress
Port.01	All	0 kbps	0 kbps
Port.02	All	0 kbps	0 kbps
Port.03	All	0 kbps	0 kbps
Port.04	All	0 kbps	0 kbps
Port.05	All	0 kbps	0 kbps
Port.06	All	0 kbps	0 kbps
Port.07	All	0 kbps	0 kbps
Port.08	All	0 kbps	0 kbps

Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.

Please use Save Configuration to permanently save the updates.

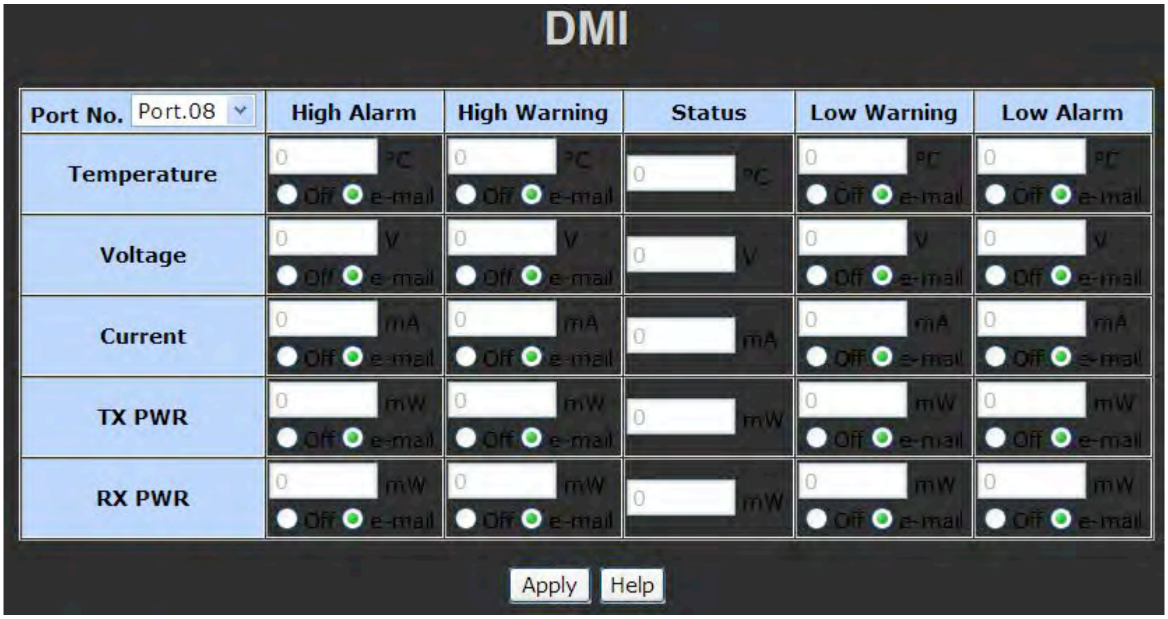
Rate Limiting interface

- All the ports support port ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set its effective egress rate at 1Mbps, ingress rate at 500Kbps. The switch performs the ingress rate by packet counter to meet the specified rate.
  - **Ingress:** Enter the port effective ingress rate(The default value is '0')
  - **Egress:** Enter the port effective egress rate(The default value is '0')
- And then, select Apply to apply the settings

DMI (Digital Monitoring Interface)

You can see the transceiver's status by ports and set up an action when detecting the exceptional value. The action includes the following options.

- **Off:** The port will be shut down when detecting the exceptional value**.**
- **e-mail:** The port will send an e-mail to the administrator when detecting the exceptional value.



DMI

Port No. Port.08	High Alarm	High Warning	Status	Low Warning	Low Alarm
Temperature	0 °C ○ Off ● e-mail	0 °C ○ Off ● e-mail	0 °C	0 °C ○ Off ● e-mail	0 °C ○ Off ● e-mail
Voltage	0 V ○ Off ● e-mail	0 V ○ Off ● e-mail	0 V	0 V ○ Off ● e-mail	0 V ○ Off ● e-mail
Current	0 mA ○ Off ● e-mail	0 mA ○ Off ● e-mail	0 mA	0 mA ○ Off ● e-mail	0 mA ○ Off ● e-mail
TX PWR	0 mW ○ Off ● e-mail	0 mW ○ Off ● e-mail	0 mW	0 mW ○ Off ● e-mail	0 mW ○ Off ● e-mail
RX PWR	0 mW ○ Off ● e-mail	0 mW ○ Off ● e-mail	0 mW	0 mW ○ Off ● e-mail	0 mW ○ Off ● e-mail

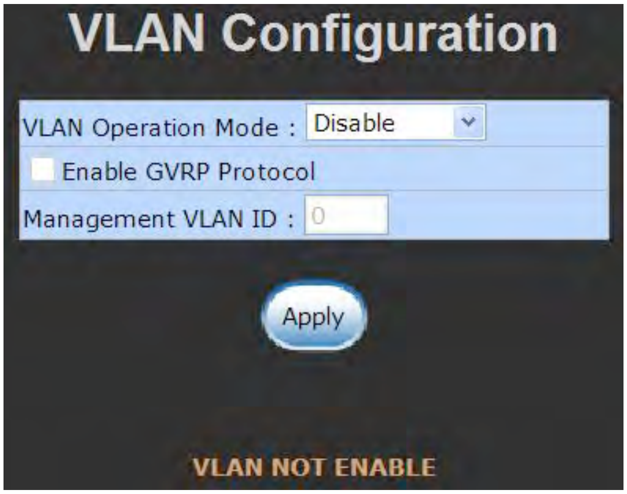
DMI interface

- Ports 5 to 8 support the DMI function. The DMI table (above) shows five parameters and four warning and alarm indicators. All of these warning and alarm indications are defined and supported by SFP transceivers with the DMI function.
- And then, select Apply to apply the settings

VLAN configuration

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

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



VLAN Configuration

VLAN Operation Mode : Disable

□ Enable GVRP Protocol

Management VLAN ID : 0

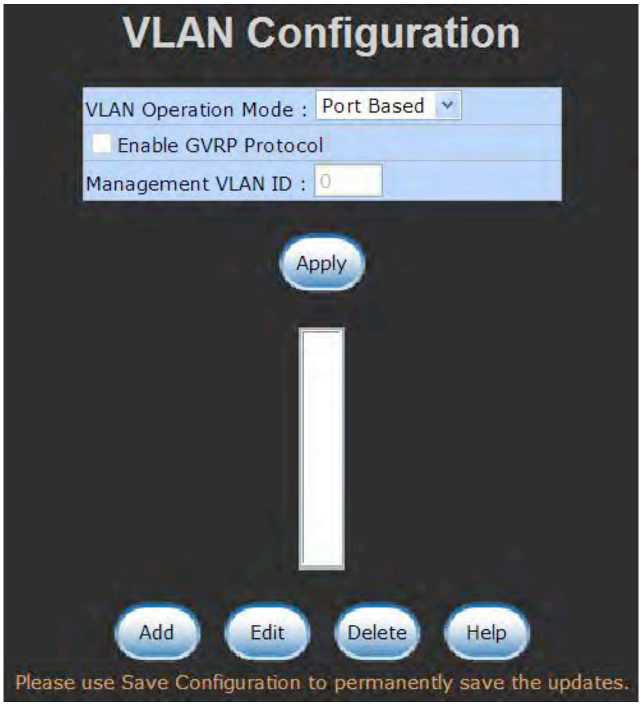
VLAN NOT ENABLE

VLAN Configuration interface

VLAN configuration - Port-based VLAN

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

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



VLAN Configuration

VLAN Operation Mode : Port Based

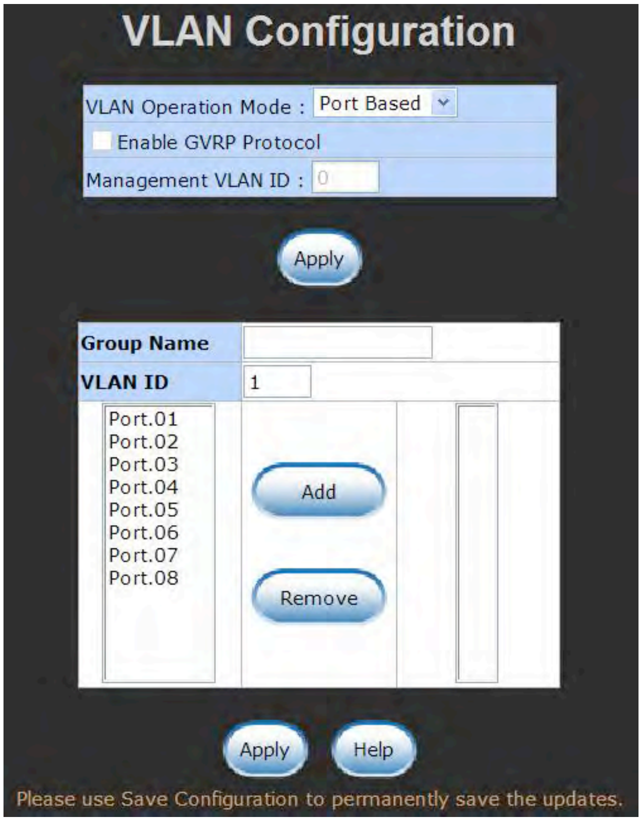
□ Enable GVRP Protocol

Management VLAN ID : 0

Please use Save Configuration to permanently save the updates.

VLAN – Port Based interface

- Select Add to imitate a new VLAN group (The maximum number of VLAN groups available is 64).
- Enter the VLAN name, group ID and the group of members in the VLAN.
- Select Apply



VLAN Configuration

VLAN Operation Mode : Port Based

□ Enable GVRP Protocol

Management VLAN ID : 0

Group Name

VLAN ID 1

Port.01
Port.02
Port.03
Port.04
Port.05
Port.06
Port.07
Port.08

Please use Save Configuration to permanently save the updates.

VLAN—Port Based Add interface

- You will see the VLAN displays.
- Use Delete button to delete an unwanted VLAN.
- Use Edit button to modify an existing VLAN group.

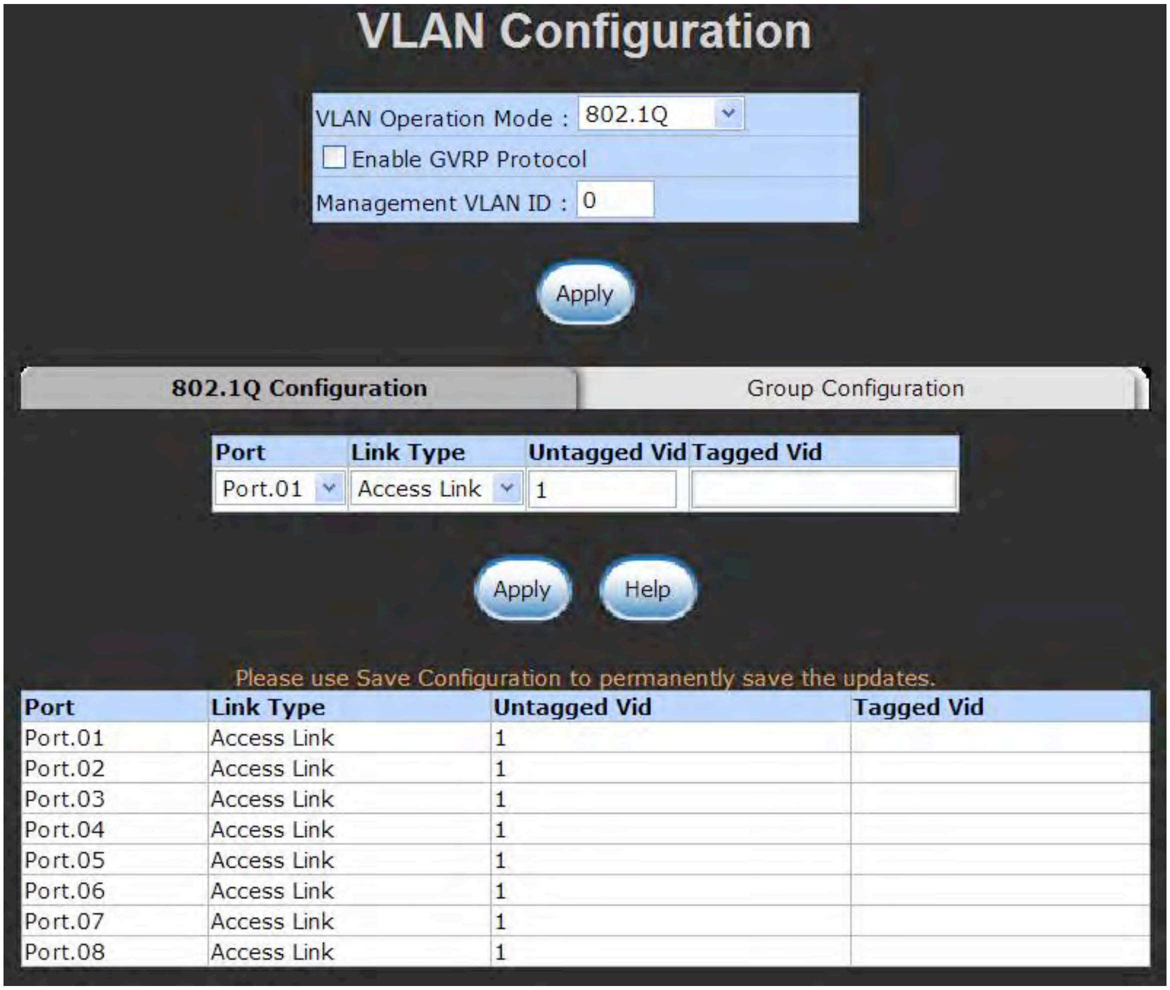
Note *Remember to execute the 'Save Configuration' action, otherwise the new configuration will be lost when switch is powered off.*

802.1Q VLAN

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

You can create tag-based VLAN, and enable or disable the GVRP protocol. There are 256 VLAN groups to provide a configuration for. Enable 802.1Q VLAN, and all ports on the switch belong to a default VLAN, VID is 1. The default VLAN cannot be deleted.

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



VLAN Configuration

VLAN Operation Mode : 802.1Q

□ Enable GVRP Protocol

Management VLAN ID : 0

Port	Link Type	Untagged Vid	Tagged Vid
Port.01	Access Link	1	

Please use Save Configuration to permanently save the updates.

Port	Link Type	Untagged Vid	Tagged Vid
Port.01	Access Link	1	
Port.02	Access Link	1	
Port.03	Access Link	1	
Port.04	Access Link	1	
Port.05	Access Link	1	
Port.06	Access Link	1	
Port.07	Access Link	1	
Port.08	Access Link	1	

802.1q VLAN interface

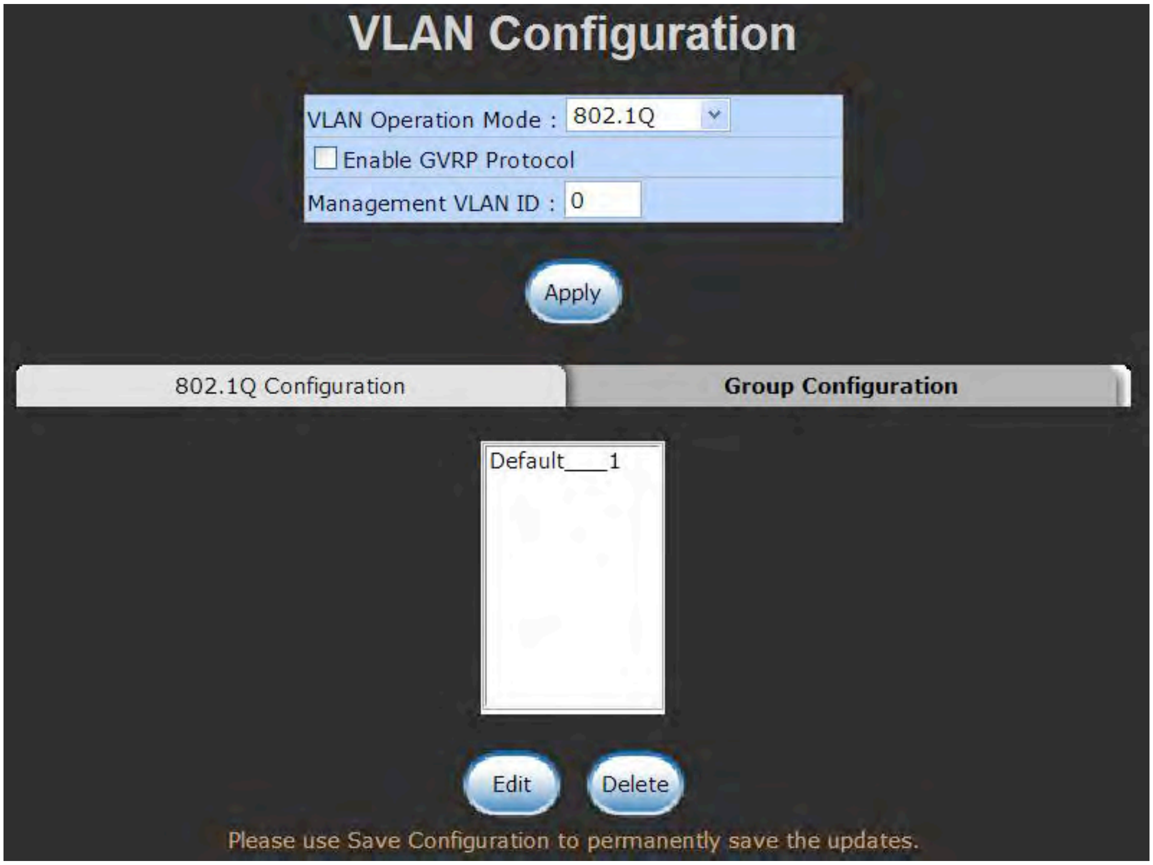
802.1Q Configuration

1. **Enable GVRP Protocol:** Select the check box to enable GVRP protocol.
2. Select the port that needs to be configured.
3. **Link Type**: there are three types of link:
    - **Access Link: a** single switch only, allows user to select group ports by setting the same VID.
    - **Trunk Link:** extended application of **Access Link**, allow user to group ports by setting the same VID on 2 or more switches.
    - **Hybrid Link:** Both **Access Link** and **Trunk Link** are available.
4. **Untagged VID:** assign the untagged frame VID.
5. **Tagged VID:** assign the tagged frame VID.
6. Select Apply
7. You can see each port setting in the below table on the screen.

Group Configuration

Edit the existing VLAN Group.

1. Select the VLAN group in the table list.
2. Select Apply



VLAN Configuration

VLAN Operation Mode : 802.1Q

□ Enable GVRP Protocol

Management VLAN ID : 0

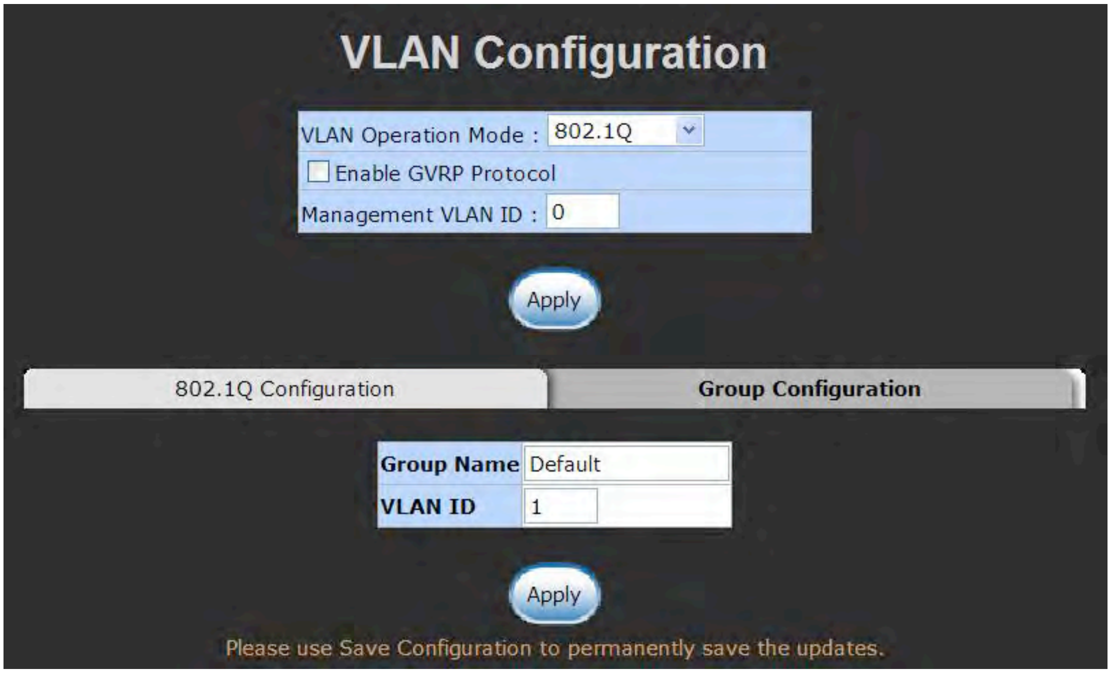
Default___1

Please use Save Configuration to permanently save the updates.

Group Configuration interface

3. You can change the VLAN group name and VLAN ID.

4. Select Apply .



VLAN Configuration

VLAN Operation Mode : 802.1Q

□ Enable GVRP Protocol

Management VLAN ID : 0

Group Name	Default
VLAN ID	1

Please use Save Configuration to permanently save the updates.

Group Configuration interface

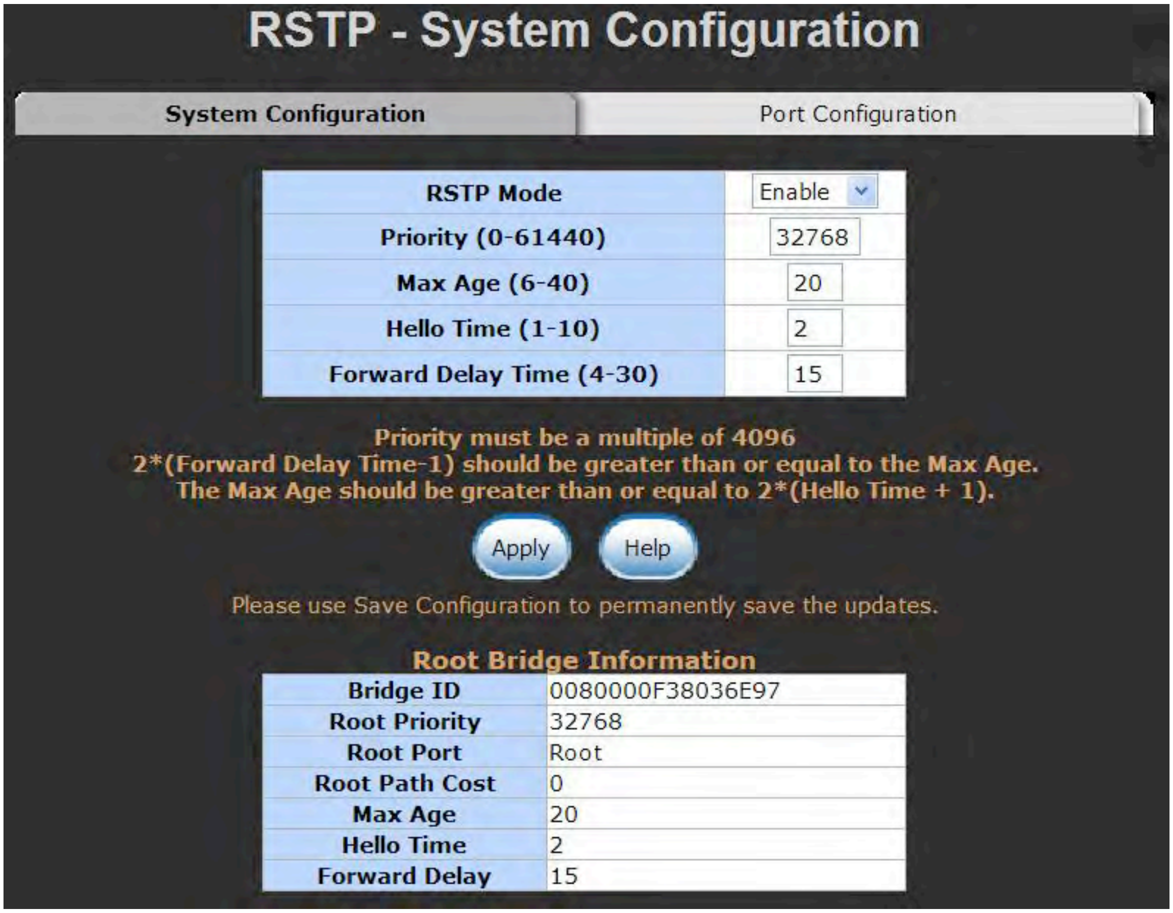
Rapid Spanning Tree

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

RSTP - System Configuration

- User can view spanning tree information about the Root Bridge
- User can modify RSTP state. After modification, select Apply button
  - **RSTP mode:** user must enable or disable RSTP function before configuring the related parameters
  - **Priority (0-61440):** a value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, the user must reboot the switch. The value must be multiple of 4096 according to the protocol standard rule
  - **Max Age (6-40):** the number of seconds a bridge waits without receiving a Spanning-Tree Protocol configuration message before attempting a reconfiguration. Enter a value between 6 through 40
  - **Hello Time (1-10):** the time that the switch controls sends out the BPDU packet to check RSTP current status. Enter a value between 1 through 10
  - **Forward Delay Time (4-30):** the number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30

Note *Follow the rule to configure the MAX Age, Hello Time, and Forward Delay Time.*
2 x (Forward Delay Time value -1) >= Max Age value >= 2 x (Hello Time value +1)



RSTP 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*(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*(Hello Time + 1).

Please use Save Configuration to permanently save the updates.

Root Bridge Information

Bridge ID	0080000F38036E97
Root Priority	32768
Root Port	Root
Root Path Cost	0
Max Age	20
Hello Time	2
Forward Delay	15

RSTP System Configuration interface

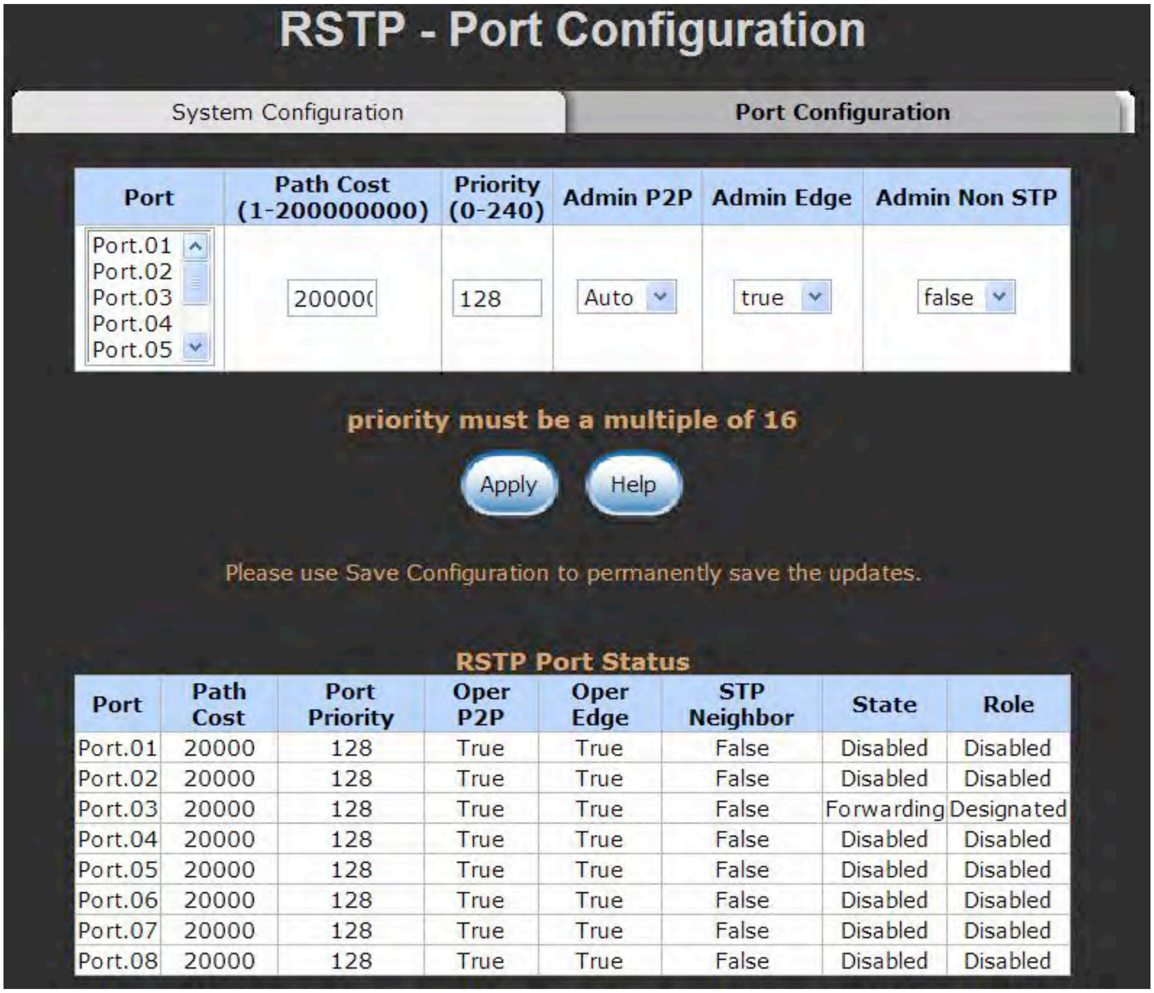
RSTP - Port Configuration

You can configure path cost and priority of every port.

1. Select the port in Port column.
1. **Path Cost:** The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000.
2. **Priority:** Decide which port should be blocked by priority in LAN. Enter a number 0 through 240. The value of priority must be the multiple of 16.
3. **P2P:** Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P

status of the link to be manipulated administratively. True is P2P enabling. False is P2P disabling.

4. **Edge:** The port directly connected to the end stations cannot create a bridging loop in the network. To configure the port as an edge port, set the port to **True** status.
5. **Non STP:** The port includes the STP mathematic calculation. **True** is not including STP mathematic calculation. **False** is including the STP mathematic calculation.
6. Select Apply.



RSTP - Port Configuration

Port	Path Cost (1-200000000)	Priority (0-240)	Admin P2P	Admin Edge	Admin Non STP
Port.01 Port.02 Port.03 Port.04 Port.05	20000(	128	Auto	true	false

priority must be a multiple of 16

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	20000	128	True	True	False	Disabled	Disabled
Port.02	20000	128	True	True	False	Disabled	Disabled
Port.03	20000	128	True	True	False	Forwarding	Designated
Port.04	20000	128	True	True	False	Disabled	Disabled
Port.05	20000	128	True	True	False	Disabled	Disabled
Port.06	20000	128	True	True	False	Disabled	Disabled
Port.07	20000	128	True	True	False	Disabled	Disabled
Port.08	20000	128	True	True	False	Disabled	Disabled

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

System Configuration

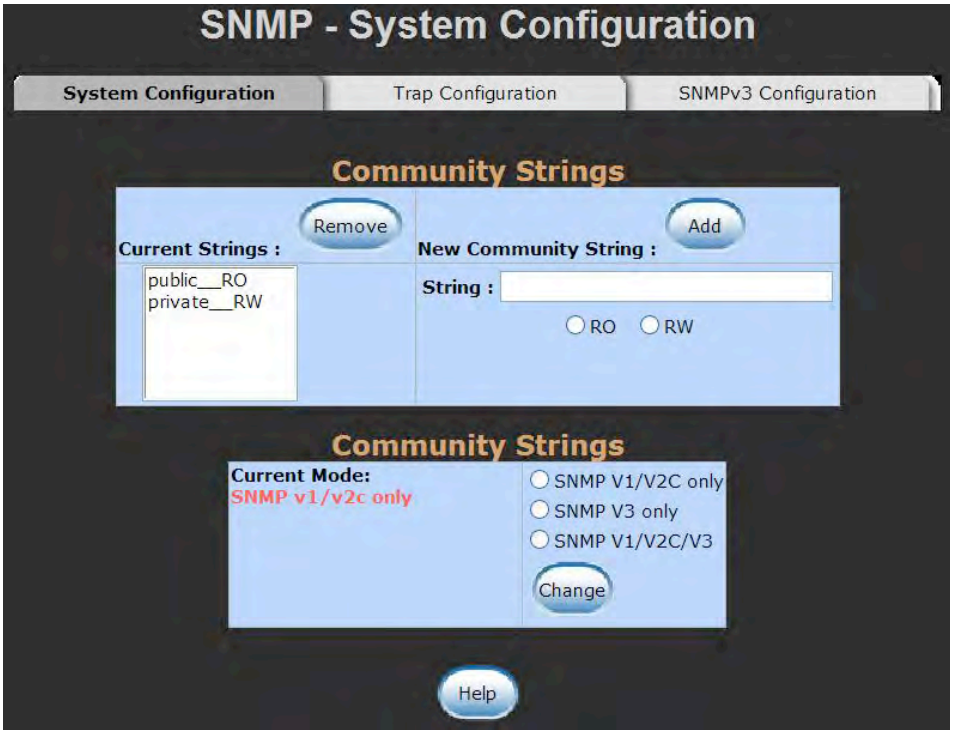
- **Community Strings**

You can define a new community string set and remove unwanted community string.

1. **String:** Enter the name of the string.
2. **RO:** Read Only. Enables requests accompanied by this string to display MIB-object information.
3. **RW:** Read/Write. Enables requests accompanied by this string to display MIB-object information and to set MIB objects.

1. Select Add.
2. To remove the community string, select the community string that you have defined and select Remove. You cannot edit the name of the default community string set.

- **Agent Mode:** Select the SNMP version that you want to use it. And then select Change to switch to the selected SNMP version mode.



Community Strings

Current Strings :
public__RO
private__RW

New Community String :
String :
○ RO ○ RW

Community Strings

Current Mode:
SNMP v1/v2c only

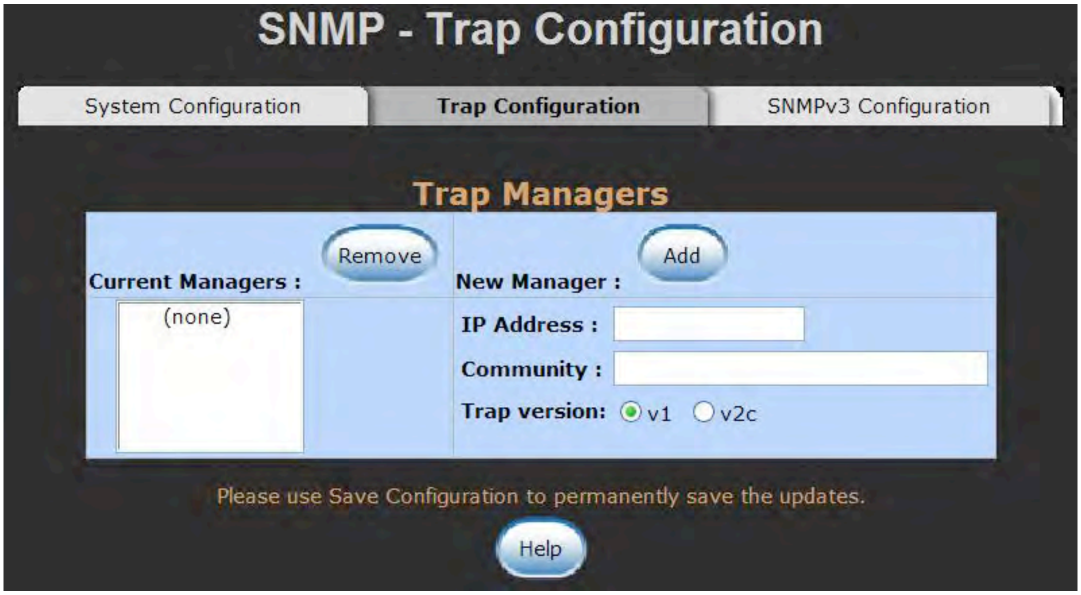
○ SNMP V1/V2C only
○ SNMP V3 only
○ SNMP V1/V2C/V3

SNMP System Configuration interface

Trap Configuration

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

1. **IP Address:** Enter the IP address of the trap manager.
2. **Community:** Enter the community string.
3. **Trap Version:** Select the SNMP trap version type – v1 or v2c.
4. Select Add.
5. To remove the community string, select the community string that you have defined and select Remove. You cannot edit the name of the default community string set.



SNMP - Trap Configuration

Trap Managers

Current Managers : (none)

New Manager :

IP Address :

Community :

Trap version: ● v1 ○ v2c

Please use Save Configuration to permanently save the updates.

Trap Managers interface

SNMPV3 Configuration

Configure the SNMP V3 function.

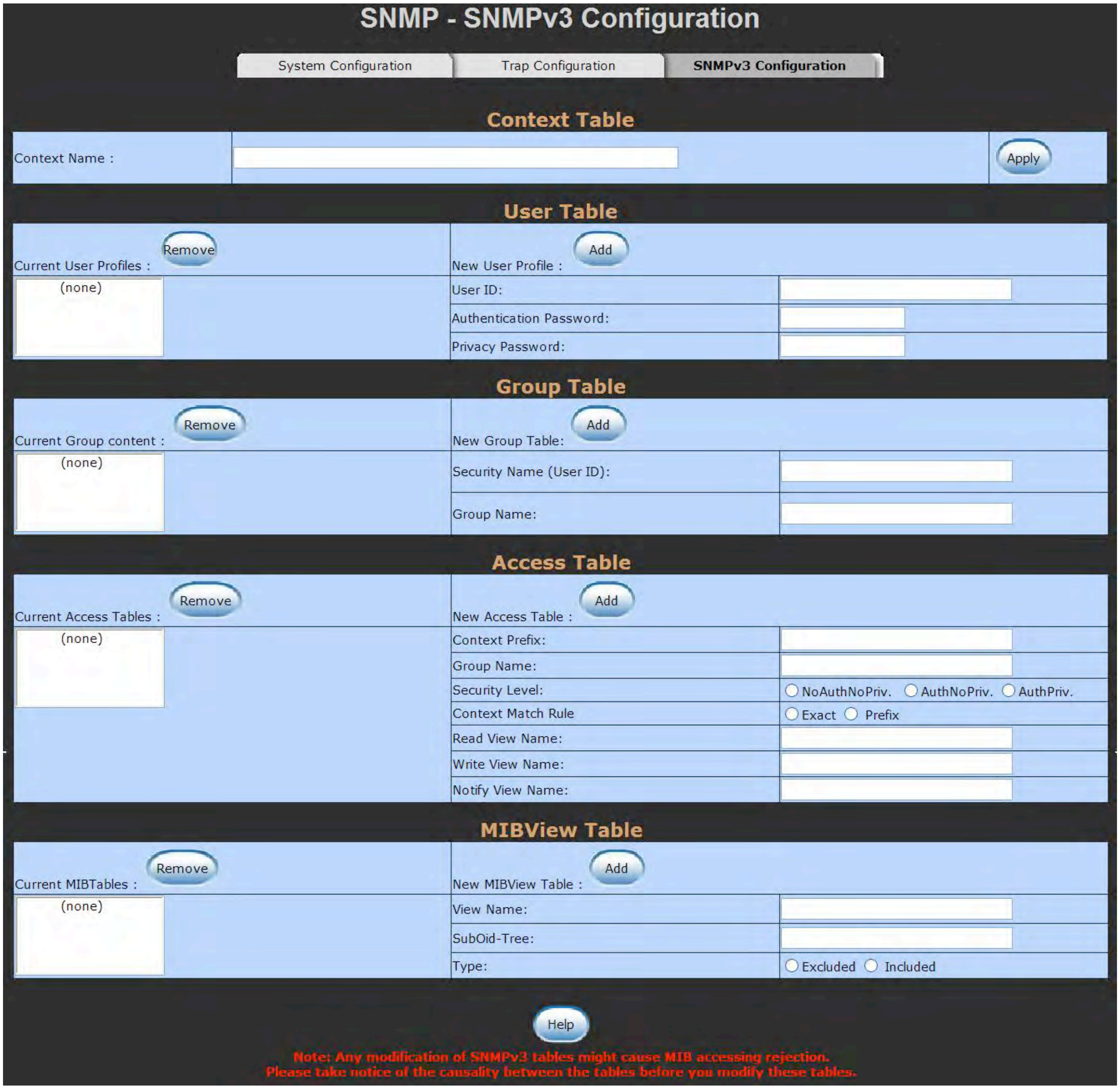
Context Table

Configure SNMP v3 context table. Assign the context name of context table. Select Add to add context name. Select Remove to remove unwanted context name.

User Profile

Configure SNMP v3 user table..

- **User ID:** set up the user name.
- **Authentication Password:** set up the authentication password.
- **Privacy Password:** set up the private password.
- Select Add to add context name.
- Select Remove to remove unwanted context name.



Note: Any modification of SNMPv3 tables might cause MIB accessing rejection.
Please take notice of the causality between the tables before you modify these tables.

SNMP V3 configuration interface

Group Table

Configure SNMP v3 group table.

- **Security Name (User ID):** Assign the user name that you have set up in user table.
- **Group Name:** Set up the group name.
- Select Add to add context name.
- Select Remove to remove unwanted context name.

Access Table

Configure SNMP v3 access table.

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

MIBview Table

Configure MIB view table.

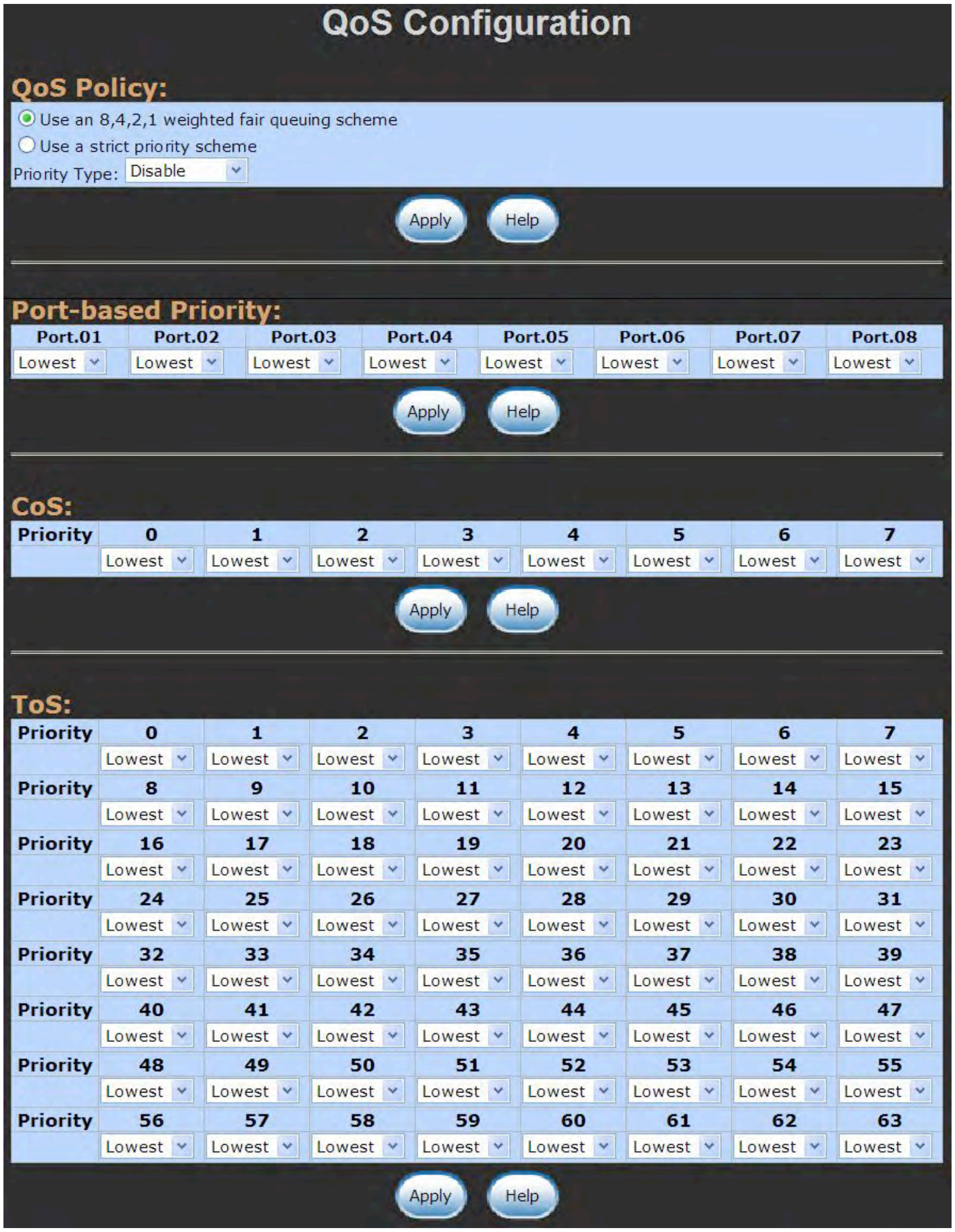
- **ViewName:** Set up the name.
- **Sub-Oid Tree:** Fill the Sub OID.
- **Type:** Select the type – exclude or included.
- Select Add to add context name.
- Select Remove to remove unwanted context name.

QoS Configuration

You can configure QoS policy and priority setting, per port priority setting, COS and TOS setting.

QoS Policy and Priority Type

- **QoS Policy:** select the QoS policy rule.
  - **Use an 8,4,2,1 weighted fair queuing scheme:** The switch will follow 8:4:2:1 rate to process priority queue from highest to lowest queue. For example, when the system processes, 1 frame of the lowest queue, 2 frames of the low queue, 4 frames of the middle queue, and 8 frames of the high queue will be processed at the same time in accordance with the 8,4,2,1 policy rule.
  - **Use the strict priority scheme:** The higher queue will always be processed first, except when the higher queue is empty.
- **Priority Type:** there are five priority type selections available. Disable means no priority type is selected.
- **Port-base:** the port priority will follow the **Port-base** that you have assigned – high, middle, low, or lowest.
  - **COS only:** the port priority will only follow the **COS priority** that you have assigned.
  - **TOS only:** the port priority will only follow the **TOS priority** that you have assigned.
  - **COS first:** the port priority will follow the COS priority first, and then other priority rule.
  - **TOS first:** the port priority will follow the TOS priority first, and the other priority rule.
- Select Apply.



QoS Configuration

QoS Policy:

● Use an 8,4,2,1 weighted fair queuing scheme

○ Use a strict priority scheme

Priority Type: Disable

Port-based Priority:

Port.01	Port.02	Port.03	Port.04	Port.05	Port.06	Port.07	Port.08
Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest

CoS:

Priority	0	1	2	3	4	5	6	7
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest

ToS:

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

QoS Configuration interface

Port Base Priority

Configure the per port priority level.

- **Port:** each port has 4 priority levels – high, middle, low, and lowest.
- Select Apply.

COS Configuration

Set up the COS priority level.

- **COS priority:** Set up the COS priority level 0~7 –high, middle, low, lowest.
- Select Apply.

TOS Configuration

Set up the TOS priority.

- **TOS priority:** the system provides 0~63 TOS priority level. Each level has four types of priority – high, middle, low, and lowest. The default value is ‘lowest’ priority for each level. When the IP packet is received, the system will check the TOS level value in the IP packet that has been received. For example, user set the TOS level 25 is high. The port 1 is following the TOS priority policy only. When the port 1 packet received, the system will check the TOS value of the received IP packet. If the TOS value of received IP packet is 25(priority = high), and then the packet priority will have highest priority.
- Select Apply.

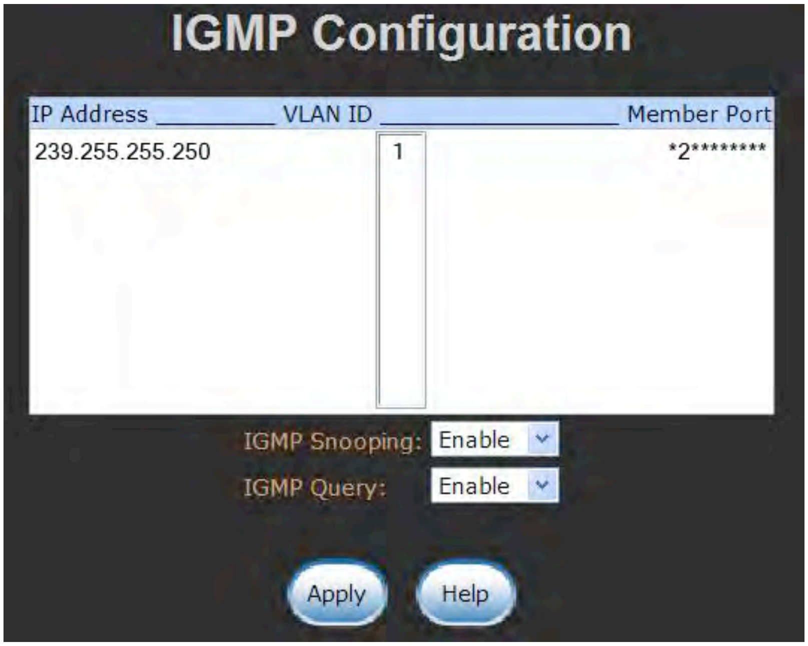
IGMP Configuration

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

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

The switch support IP multicast, you can enable IGMP protocol on web management's switch setting advanced page, then displays the IGMP snooping information. IP multicast addresses range are from 224.0.0.0 through 239.255.255.255.

- **IGMP Protocol:** Enable or disable the IGMP protocol.
- **IGMP Query:** Select the IGMP query function as **Enable** or **Auto** to set the switch as a querier for IGMP version 2 multicast network.
- Select Apply.



IGMP Configuration

IP Address	VLAN ID	Member Port
239.255.255.250	1	*2********

IGMP Snooping: Enable

IGMP Query: Enable

IGMP Configuration interface

X-Ring

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

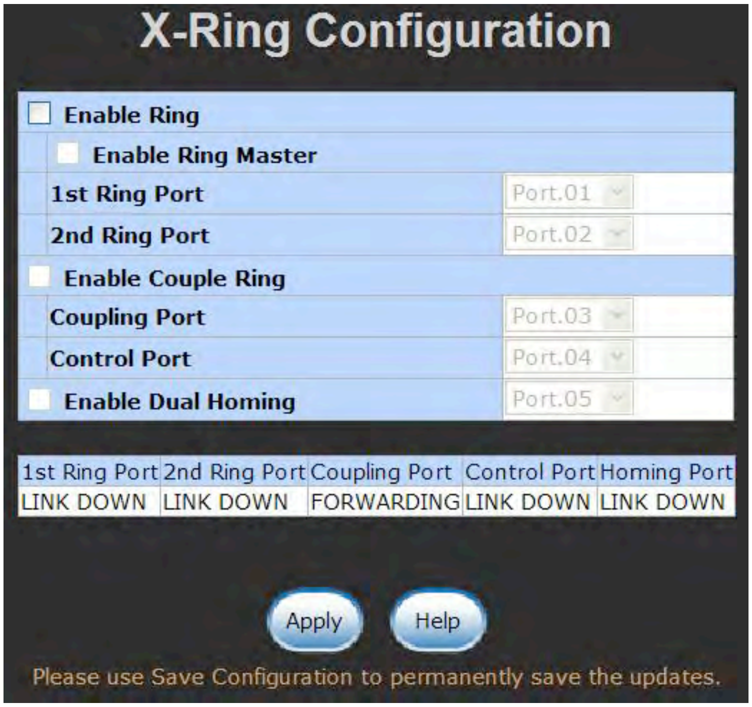
In the X-Ring topology, every switch should enable the X-Ring function and assign two member ports in the ring. Only one switch in the X-Ring group would be set as a master switch that would be blocked, called the backup port, and another port is called the working port. Other switches in the X-Ring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

The switch supports the functions and acts as an interface for setting the switch as the ring master or slave mode. The ring master can negotiate and place commands to other switches in the X-Ring group. If there are 2 or more switches in master mode, then software will select the switch with lowest MAC address number as the ring master. The X-Ring master ring mode will be enabled by the X-Ring configuration interface. Also, user can identify the switch as the ring master from the R.M. LED panel of the LED panel on the switch.

The system also supports the coupling ring that can connect 2 or more X-Ring groups for the redundant backup function and the dual homing function that prevents a connection loss between the X-Ring group and the upper level/core switch.

- **Enable X-Ring:** To enable the X-Ring function, select the check box that enables the X-Ring function.
- **Enable Ring Master:** Select the check box to enable this machine to be identified as a ring master.
- **1st & 2nd Ring Ports:** Pull down the selection menu to assign two ports as the member ports. **1st Ring Port** is the working port and **2nd Ring Port** is the backup port. When **1st Ring Port** fails, the system will automatically select the **2nd Ring Port** to be the working port.

- **Enable Coupling Ring:** To enable the coupling ring function, select the check box that enables the coupling ring function.
- **Coupling port:** Assign the member port.
- **Control port:** Set the switch as the master switch in the coupling ring.
- **Enable Dual Homing:** Set up one of port on the switch to be the Dual Homing port. In an X-Ring group, the maximum number of Dual Homing ports is one. Dual Homing only work when the X-Ring function is enabled.
- And then, select Apply to apply the configuration.



X-Ring Configuration

□ Enable Ring	
□ Enable Ring Master	
1st Ring Port	Port.01
2nd Ring Port	Port.02
□ Enable Couple Ring	
Coupling Port	Port.03
Control Port	Port.04
□ Enable Dual Homing	Port.05

1st Ring Port	2nd Ring Port	Coupling Port	Control Port	Homing Port
LINK DOWN	LINK DOWN	FORWARDING	LINK DOWN	LINK DOWN

Please use Save Configuration to permanently save the updates.

X-ring Interface

Note

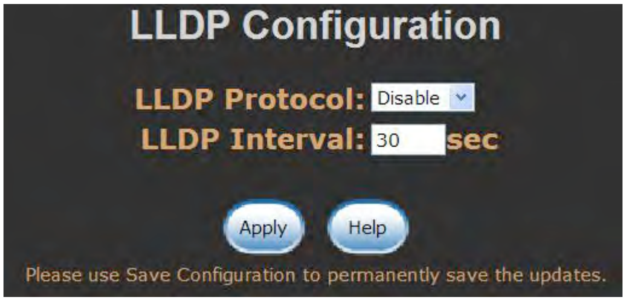
1. When the X-Ring function is enabled, the user must disable the RSTP first. X-Ring and RSTP function cannot be active at the same time.

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

LLDP Configuration

Link Layer Discovery Protocol (LLDP) is defined in the IEEE 802.1AB, it is an emerging standard which provides a solution for the configuration issues caused by expanding LANs. LLDP specifically defines a standard method for Ethernet network devices such as switches, routers and wireless LAN access points to advertise information about themselves to other nodes on the network and store the information they discover. 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.

- **LLDP Protocol**: Pull down the selection menu to disable or enable LLDP function.
- **LLDP Interval**: Set the interval of advertising the switch's information to other nodes.
- Click Apply.



LLDP Configuration

LLDP Protocol: Disable

LLDP Interval: 30 sec

Please use Save Configuration to permanently save the updates.

LLDP Interface

Security

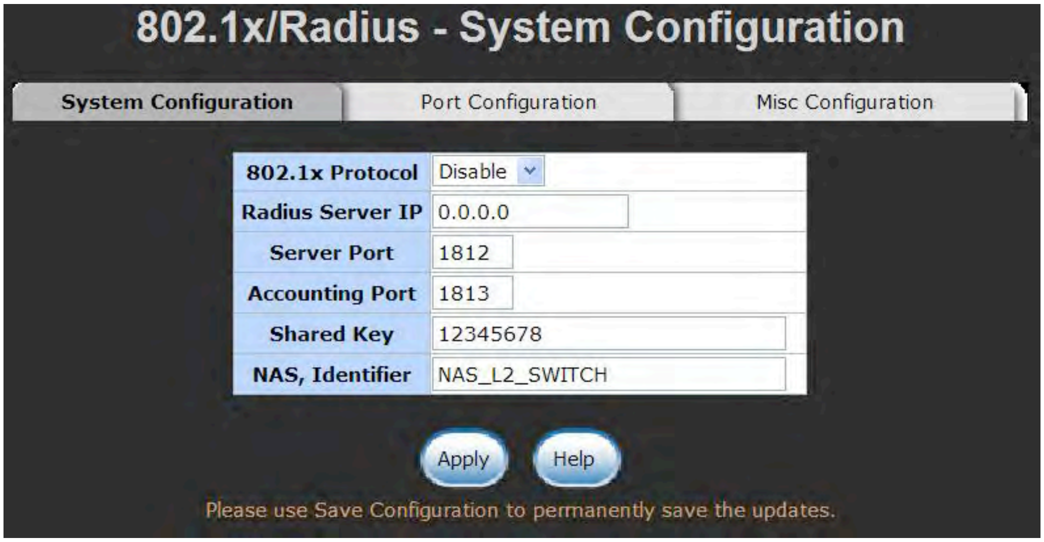
802.1X/Radius Configuration

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.

1. **IEEE 802.1x Protocol:** enable or disable 802.1x protocol.
2. **Radius Server IP:** set the Radius Server IP address.
3. **Server Port:** set the UDP destination port for authentication requests to the specified Radius Server.
4. **Accounting Port:** set the UDP destination port for accounting requests to the specified Radius Server.
5. **Shared Key:** set an encryption key for use during authentication sessions with the specified radius server. This key must match the encryption key used on the Radius Server.
6. **NAS, Identifier:** set the identifier for the radius client.
7. Select Apply.



802.1x/Radius - System Configuration

802.1x Protocol	Disable
Radius Server IP	0.0.0.0
Server Port	1812
Accounting Port	1813
Shared Key	12345678
NAS, Identifier	NAS_L2_SWITCH

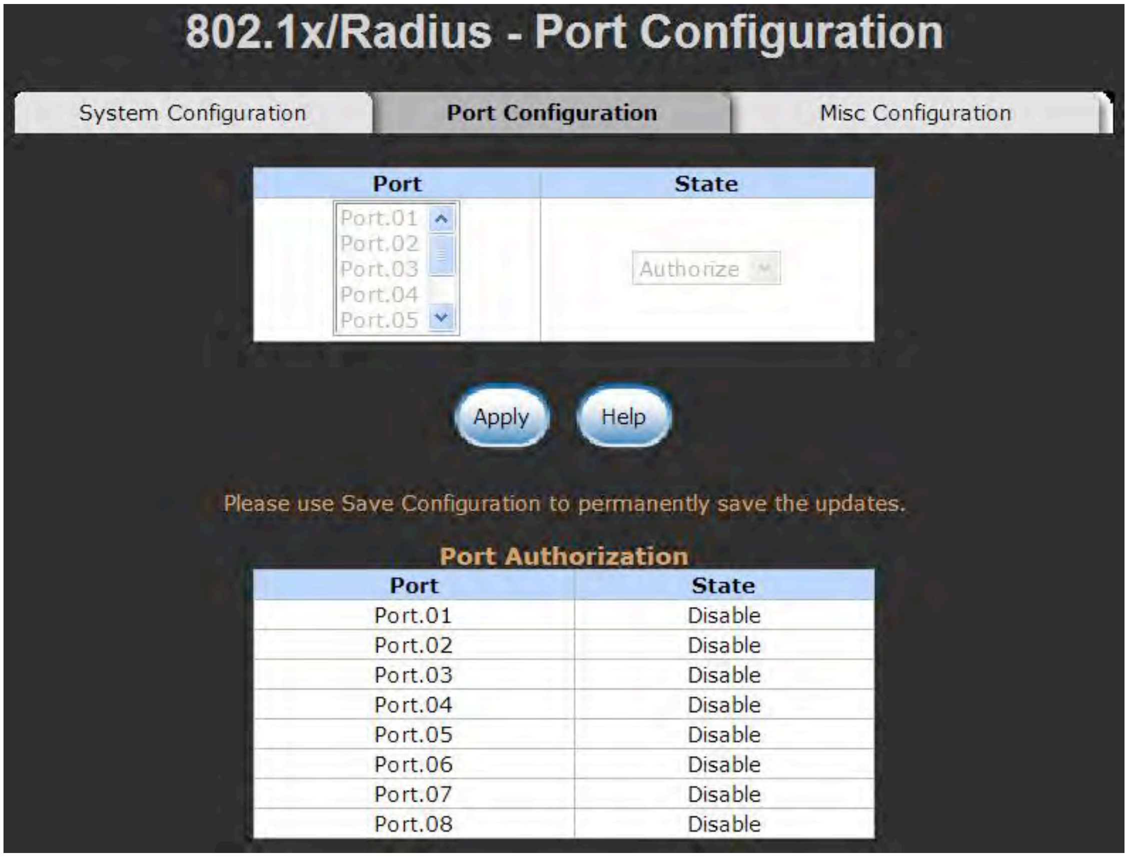
Please use Save Configuration to permanently save the updates.

802.1x System Configuration interface

802.1x Per Port Configuration

You can configure a 802.1x authentication state for each port. This state provides Disable, Accept, Reject and Authorize. Use **Space** key to change the state value.

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



802.1x/Radius - Port Configuration

Port	State
Port.01 Port.02 Port.03 Port.04 Port.05	Authorize

Please use Save Configuration to permanently save the updates.

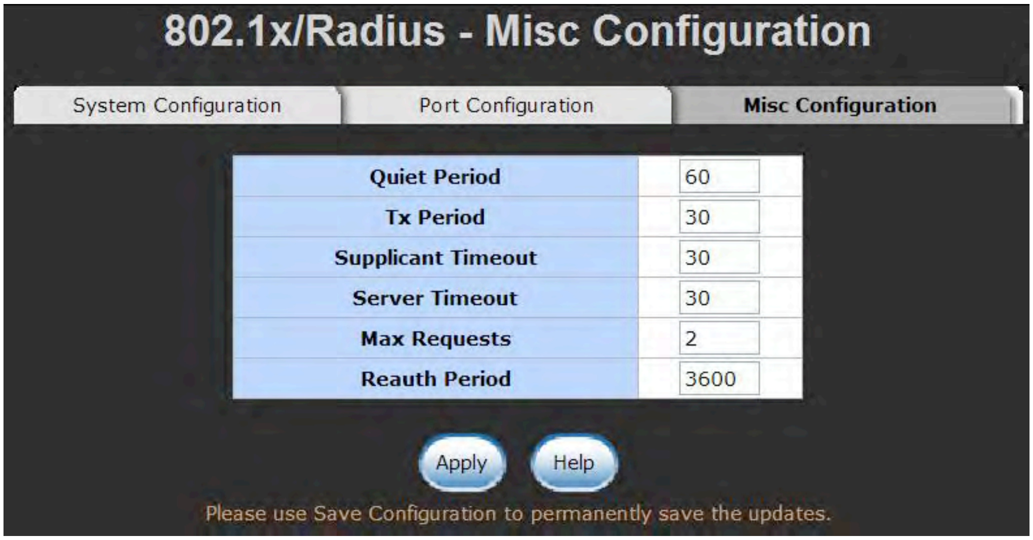
Port Authorization

Port	State
Port.01	Disable
Port.02	Disable
Port.03	Disable
Port.04	Disable
Port.05	Disable
Port.06	Disable
Port.07	Disable
Port.08	Disable

802.1x Per Port Setting interface

Miscellaneous Configuration

1. **Quiet Period:** set the period during which the port doesn't try to acquire a supplicant.
2. **TX Period:** set the period the port wait for retransmit next EAPOL PDU during an authentication session.
3. **Supplicant Timeout:** set the period of time the switch waits for a supplicant response to an EAP request.
4. **Server Timeout:** set the period of time the switch waits for a server response to an authentication request.
5. **Maximum Requests:** set the number of authentication attempts that must time-out before authentication fails and the authentication session ends.
6. **Reauthentication period:** set the period of time after which clients connected must be re-authenticated.
7. Click Apply.



802.1x/Radius - Misc Configuration

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

Please use Save Configuration to permanently save the updates.

802.1x Misc Configuration interface

MAC Address Table

Use the MAC address table to ensure the port security.

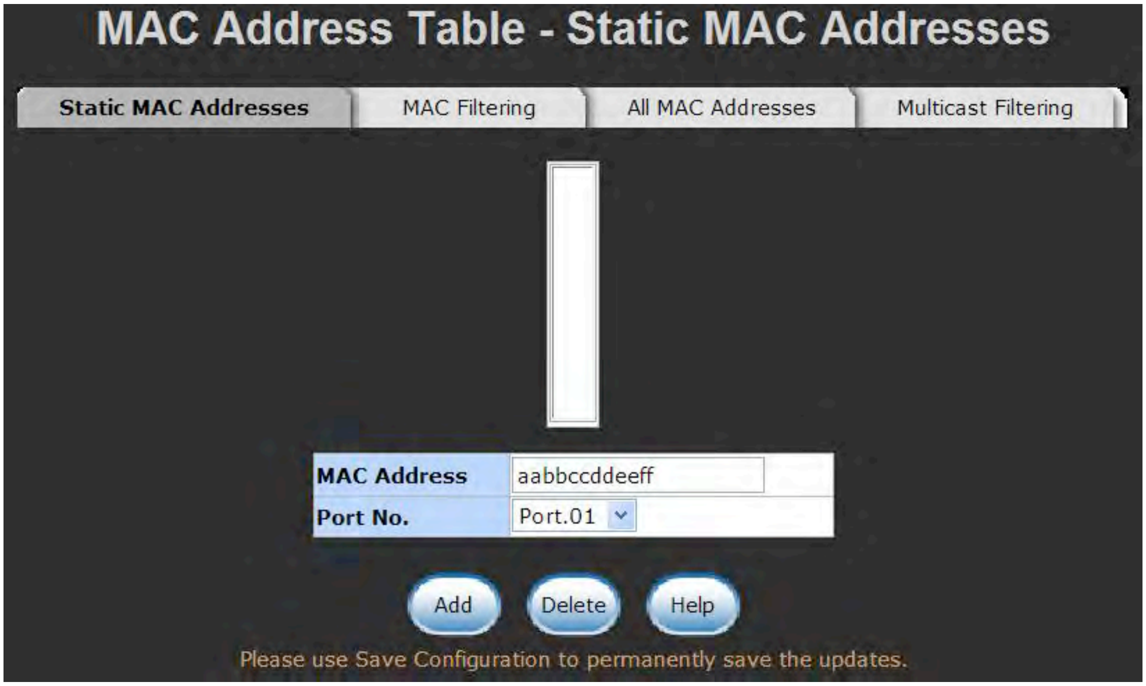
Static MAC Address

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

- **Add the Static MAC Address**

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

1. **MAC Address:** Enter the MAC address of the port that should permanently forward traffic, regardless of the device’s network activity.
2. **Port No.:** pull down the selection menu to select the port number.
3. Select Add.
4. If you want to delete the MAC address from filtering table, select the MAC address and select Delete.



MAC Address Table - Static MAC Addresses

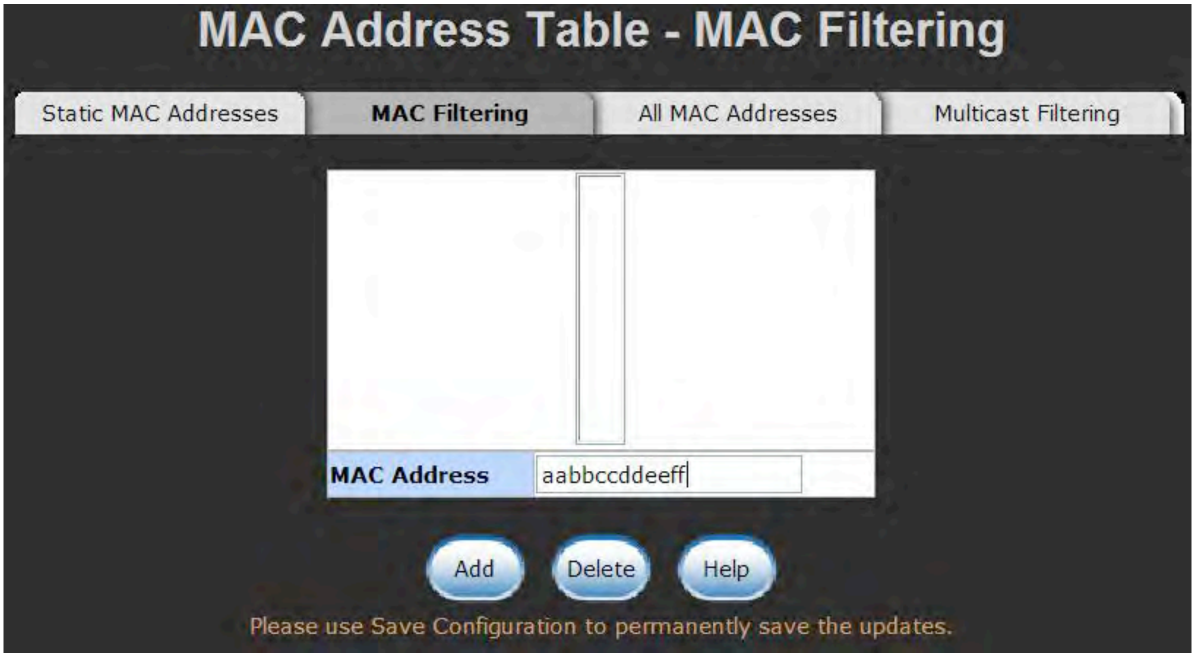
MAC Address	aabbccddeeff
Port No.	Port.01

Please use Save Configuration to permanently save the updates.

Static MAC Addresses interface

MAC Filtering

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



MAC Address: aabbccddeeff

Please use Save Configuration to permanently save the updates.

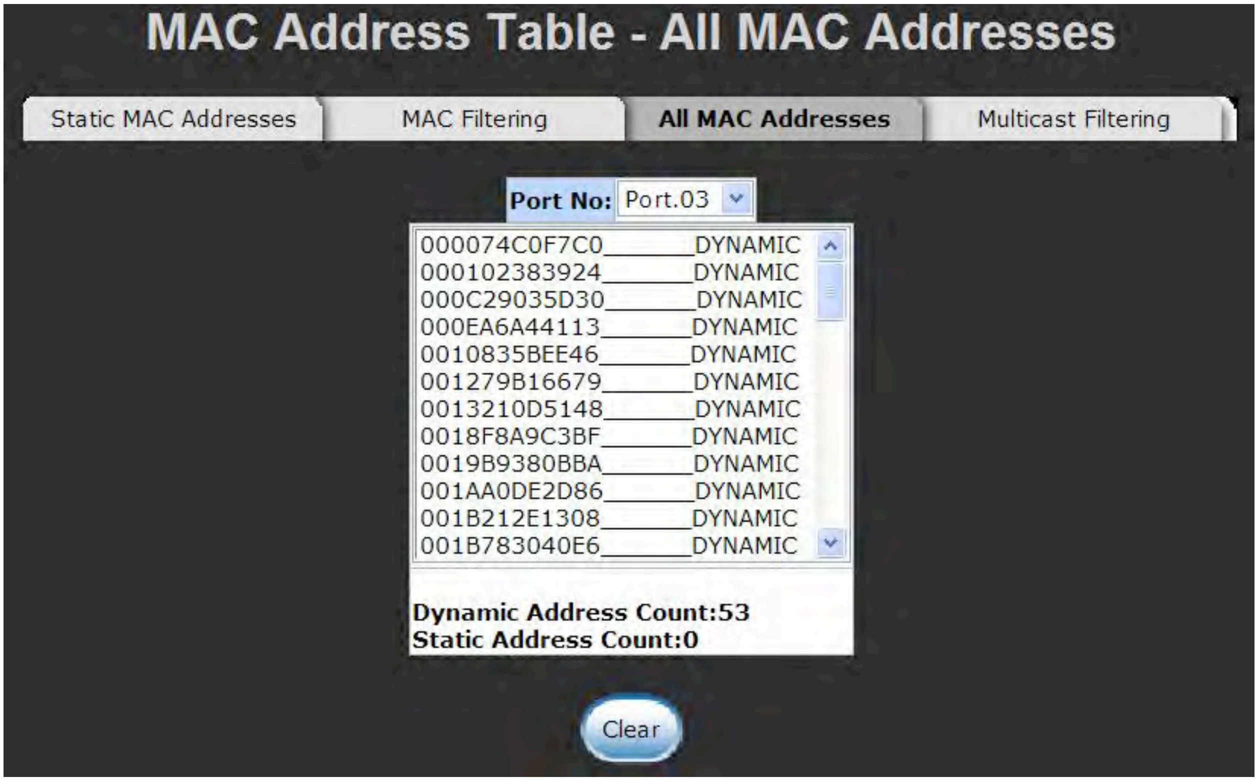
MAC Filtering interface

1. **MAC Address:** Enter the MAC address that you want to filter.
2. Select Add.
3. If you want to delete the MAC address from filtering table, select the MAC address and select Delete.

All MAC Addresses

You can view the port that connects a device's MAC address and related devices' MAC addresses.

1. Select the port.
2. The selected port of the static MAC addresses information will be displayed here.
3. Select Clear to clear the current port's static MAC address information on screen.



MAC Address Table - All MAC Addresses

Port No: Port.03

```
000074C0F7C0_______DYNAMIC
000102383924_______DYNAMIC
000C29035D30_______DYNAMIC
000EA6A44113_______DYNAMIC
0010835BEE46_______DYNAMIC
001279B16679_______DYNAMIC
0013210D5148_______DYNAMIC
0018F8A9C3BF_______DYNAMIC
0019B9380BBA_______DYNAMIC
001AA0DE2D86_______DYNAMIC
001B212E1308_______DYNAMIC
001B783040E6_______DYNAMIC
```

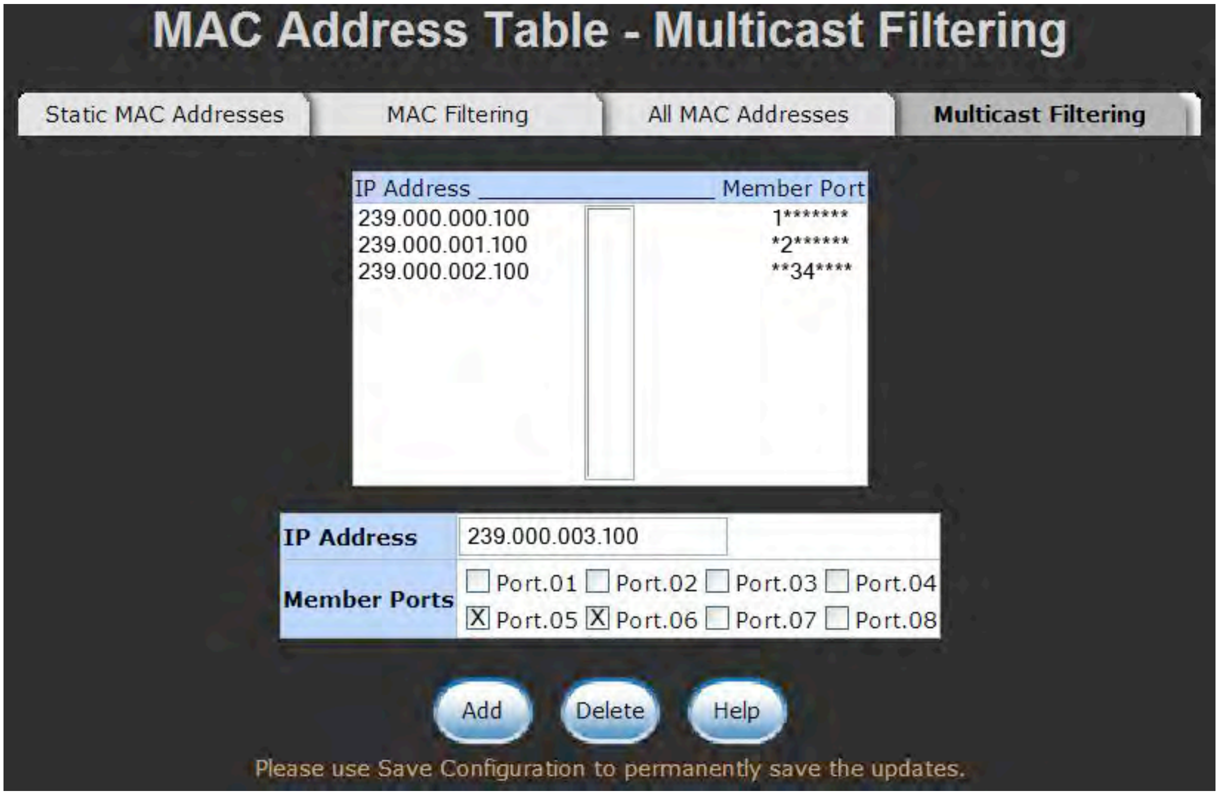
Dynamic Address Count:53
Static Address Count:0

All MAC Address interface

Multicast Filtering

Multicasts are similar to broadcasts, they are sent to all end stations on a LAN or VLAN. Multicast filtering is the function, which end stations can receive the multicast traffic if the connected ports had 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.

- **IP Address**: Assign a multicast group IP address in the range of 224.0.0.0 ~ 239.255.255.255.
- **Member Ports**: Tick the check box beside the port number to include them as the member ports in the specific multicast group IP address.
- Click Add to append a new filter of multicast to the field, or select the filter in the field and click Delete to remove it.



MAC Address Table - Multicast Filtering

IP Address	Member Port
239.000.000.100	1*******
239.000.001.100	*2******
239.000.002.100	**34****

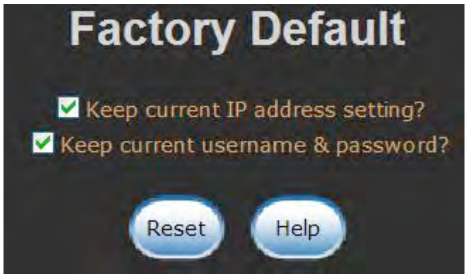
IP Address	239.000.003.100
Member Ports	□ Port.01 □ Port.02 □ Port.03 □ Port.04 ☒ Port.05 ☒ Port.06 □ Port.07 □ Port.08

Please use Save Configuration to permanently save the updates.

Multicast Filtering interface

Factory Default

To reset switch to the default configuration, select Reset to reset all switch configurations to the default value.



Factory Default

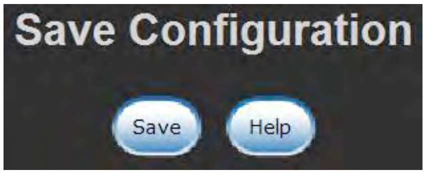
☑ Keep current IP address setting?

☑ Keep current username & password?

Factory Default interface

Save Configuration

Save all configuration changes that you have made in the system. To ensure that all configuration changes will be saved, select Save to save all the changes to the flash memory.

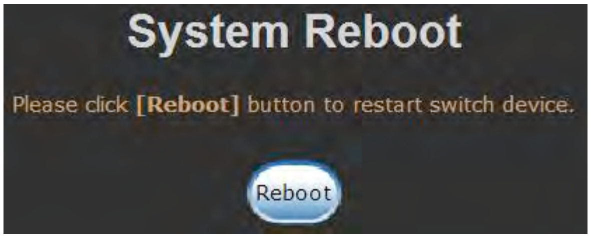


Save Configuration

Save Configuration interface

System Reboot

Reboot the switch in software reset. Select Reboot to reboot the system.



System Reboot

Please click **[Reboot]** button to restart switch device.

System Reboot interface

Help

- Verify that you are using the right power cord/adapter (DC 12 ~ 48V), please do not use the power adapter with a DC output greater than 48V, or it will damage this switch.
- Select the proper UTP cable to construct your network. Please check that you are using the correct cable. Use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ45 connections: 100Ω Category 3, 4, or 5 cable for 10Mbps connections, 100Ω Category 5 cable for 100Mbps, or 100Ω Category 5e/above cable for 1000Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).

LED Diagnostic Indicators

- **Diagnosing LED Indicators:** the Switch can be easily monitored through LED panel indicators, that describe common problems you may encounter and where you can find possible solutions to assist in identifying challenges.
- If the power indicator does not illuminate on when the power is applied, you may have a problem with the power cord. Check for loose power connections, power losses or surges at the power outlet. If you still cannot resolve the problem, contact ComNet for assistance.
- If the ComNet switch LED indicators are normal while the cables are correctly connected, but the packets still are not being transmitted, check your system's Ethernet devices' configuration or status.

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 address of ComNet Global Service Center: customercare@ComNet.net

Communication Networks

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

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

The COMNET logo is a registered trademark of Communication Networks Corporation. Additional Company and product names may be trademarks or registered trademarks of the individual companies and are respectfully acknowledged and do not imply endorsement.