4-port 10/100/1000TX + 4-port Mini GBIC L2 Managed Industrial Ethernet Switch with Ring Redundancy



User Manual

www.antaira.com

Content

Overview 1

Introduction 1

Features 4

Packing List 6

Safety Precaution 6

Hardware Description 7

Front Panel 7

Top View 8

Wiring the Power Inputs 8

LED Indicators 9

Ports 10

Cabling 11

Mounting Installation 15

DIN-Rail Mounting 15

Wall Mount Plate Mounting 16

Hardware Installation 17

Hardware Installation 18

Installation Steps 18
Xtreme Ring Application 19
Coupling Ring Application 20
Dual Homing Application 21
Console Management 23
Connecting to the Console Port 23
Pin Assignment 23
Login in the Console Interface 24
CLI Management 25
Commands Level 26
Commands Set List 27
System Commands Set 27
Port Commands Set 30
Trunk Commands Set 32
VLAN Commands Set 33
Spanning Tree Commands Set 35
QOS Commands Set 38
IGMP Commands Set 39
Mac / Filter Table Commands Set 39
SNMP Commands Set 40

Port Mirroring Commands Set 42
802.1x Commands Set 43
TFTP Commands Set 45
SystemLog, SMTP and Event Commands Set 46
SNTP Commands Set 48
Xtreme Ring Commands Set 49
Web-Based Management 50
About Web-based Management 50
Preparing for Web Management 50
System Login 51
Main interface 52
System Information 53
IP Configuration 53
DHCP Server – System configuration 54
DHCP Client – System Configuration 55
DHCP Server - Port and IP Bindings 56
TFTP - Update Firmware 56
TFTP – Restore Configuration 57
TFTP - Backup Configuration 57
System Event Log – Syslog Configuration 58

System Event Log - SMTP Configuration 59
System Event Log - Event Configuration 61
Fault Relay Alarm..... 63
SNTP Configuration 63
IP Security..... 66
User Authentication..... 67
Port Statistics 68
Port Control 69
Port Trunk 70
Aggregator setting..... 70
Aggregator Information..... 71
State Activity 72
Port Mirroring 73
Rate Limiting 73
VLAN configuration 74
VLAN configuration - Port-based VLAN..... 75
802.1Q VLAN..... 78
Rapid Spanning Tree 81
RSTP - System Configuration 81
RSTP - Port Configuration..... 82

SNMP Configuration 83
System Configuration 84
Trap Configuration 85
SNMPV3 Configuration 86
QoS Configuration 89
QoS Policy and Priority Type 89
Port Base Priority 90
COS Configuration 91
TOS Configuration 91
IGMP Configuration 91
Xtreme Ring 93
Security 95
802.1X/Radius Configuration 95
MAC Address Table 98
Factory Default 101
Save Configuration 101
System Reboot 101
Troubles shooting 102
Technical Specification 103

Overview

Introduction

To create reliability in your network, the 4 10/100/1000T + 4 SFP Managed Industrial Switch comes equipped with a proprietary redundant network protocol—Xtreme Ring provides users with an easy way to establish a redundant Ethernet network with ultra high-speed recovery time less than 20 ms. Also, the long MTBF (Mean Time Between Failures) ensures that the industrial 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-TX fast Ethernet ports, the 4 10/100/1000T + 4 SFP Managed Industrial Switch comes equipped with 4 SFP (mini-GBIC) ports. Traditional RJ-45 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 4 10/100/1000T + 4 SFP Managed Industrial Switch will continue to operate until a Gigabit network infrastructure has been established, without requiring any extra upgrade costs.

The SFP Advantage

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 500m (multi-mode), 10km, 30km, 50km, 70km or 110km (single-mode) – and the slot support 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.

High-Speed Transmissions

The 4 10/100/1000T + 4 SFP Managed Industrial Switch includes a switch controller that can automatically sense transmission speeds (10/100/1000 Mbps). The RJ-45 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 4 10/100/1000T + 4 SFP Managed Industrial Switch is with power reserve protection to prevent the switch device broken by wrong power wiring. When one of power input is fail, P-Fail LED will turn on and send an alarm through a relay output for notifying user.

Flexible Mounting

4 10/100/1000T + 4 SFP Managed Industrial Switch is compact and can be mounted on a DIN-rail or panel, so it is suitable for any space-constrained environment.

Advanced Protection

The power line of 4 10/100/1000T + 4 SFP Managed Industrial Switch supports up to 3,000 V_{DC} EFT protection, which secure equipment against unregulated voltage and make systems safer and more reliable. Meanwhile, 4,000 V_{DC} ESD protections for Ethernet ports make 4 10/100/1000T + 4 SFP Managed Industrial Switch more suitable for harsh environments.

Wide Operating Temperature

The operating temperature of the 4 10/100/1000T + 4 SFP Managed Industrial Switch is between -10 ~ 60 ℃. With such a wide range, you can use the 4 10/100/1000T + 4 SFP Managed Industrial Switch in some of the harshest industrial environments that exist.

Easy Troubleshooting

LED indicators make troubleshooting quick and easy. Each 10/100/1000 Base-TX port has 2 LEDs that display the link status, transmission speed and collision status. Also the three power indicators P1, P2 and Fault help you diagnose immediately.

Features

- Provides 4 x 10/100/1000Base-T Mbps Ethernet ports
- Provides 4 x SFP (mini-GBIC) port (support 100/1000 Dual Mode)
- Supports full/half duplex flow control
- Supports auto-negotiation
- Supports MDI/MDI-X auto-crossover
- Supports Packet Buffer up to 1Mbits
- Supports MAC Address up to 8Kbytes
- Supports surge (EFT) protection 3,000 V_{DC} for power line
- Supports 4,000 V_{DC} Ethernet ESD protection
- Power Supply
  - Wide-range Redundant Power Design
  - Power Polarity Reverse Protect
  - Overload Current 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
  - Double Tag VLAN (Q in Q)*
  - Private VLAN**
- Xtreme Ring
  - Xtreme Ring, Dual Homing, Couple Ring and Dual Ring Topology
  - Provide redundant backup feature and the recovery time below 20ms
- Port Trunk with LACP
- Support 802.1ab LLDP**
- 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
  - Xtreme 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
- Supports operating temperatures from -40 ~ 75 ℃ (wide operating temperature model) or -10 ~ 60 ℃ (standard model)

Packing List

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

Safety Precaution

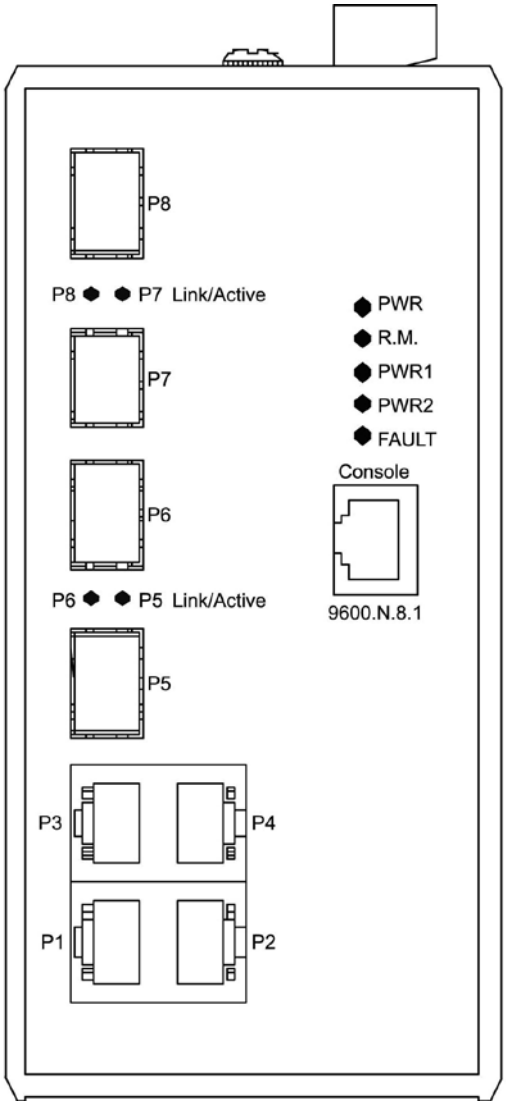
Attention *IF DC voltage is supplied by an external circuit, please use a protection device on the power supply input.*

Hardware Description

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

Front Panel

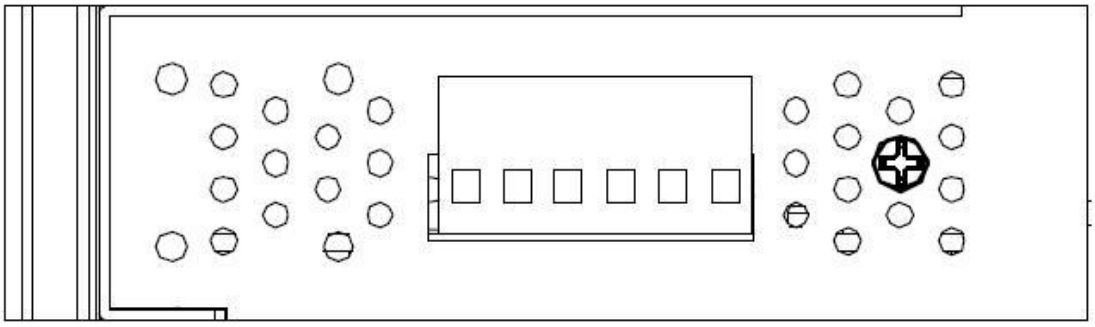
The Front Panel of 4 10/100/1000T + 4 SFP Managed Industrial Switch is shown as below.



Front Panel of 4 10/100/1000T + 4 SFP Managed Industrial Switch

Top View

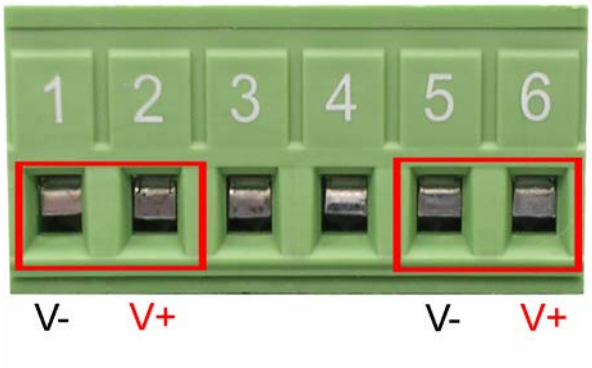
The top panel of 4 10/100/1000T + 4 SFP Managed Industrial Switch is equipped one terminal block connector of two DC power inputs.



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

Wiring the Power Inputs

Please follow the steps below to insert the power wire.



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



Tighten the wire-clamp screws for preventing the wires from loosing.

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

If only using one power source, jumper Pin 1 to Pin 5 and Pin 2 to Pin 6 to eliminate power fault alarm.

LED Indicators

There are few LEDs display the power status and network status located on the front panel of 4 10/100/1000T + 4 SFP Industrial Switch, each of them has its own specific meaning as tabled below.

LED	Color	Description	
PWR	Green	On	System power on
		Off	No power inputs
R.M.	Green	On	The industrial switch is the master of the Xtreme Ring group
		Off	The industrial switch is not the master of the Xtreme 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
Fault	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
		Flashing	Data is transmitting or receiving
		Off	Not connected to network
P1 ~ P4 (Upper LED)	Green	On	Connected to network
		Flashing	Networking is active at speed of 100Mbps
		Off	Not connected to network
P1 ~ P4 (Lower LED)	Green	On	Connected to network at speed of 1000Mbps
		Off	Not connected to network

LED indicators of 4 10/100/1000T + 4 SFP Managed Industrial Switch

Ports

RJ-45 ports (Auto MDI/MDIX): The RJ-45 ports are auto-sensing for 10Base-T, 100Base-TX or 1000Base-T devices connections. Auto MDI/MDIX means that you can connect to another switch or workstation without changing straight through or crossover cabling. See figures as below for straight through and crossover cable schematic.

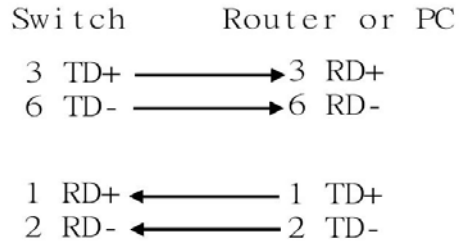
- **RJ-45 Pin Assignments**

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

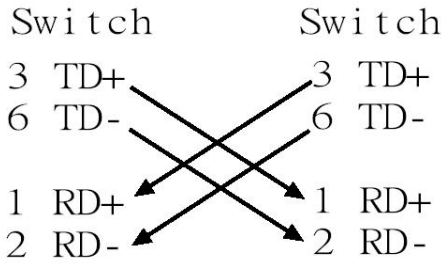
Note *"+" and "-" signs represent the polarity of the wires that make up each wire pair.*

All ports on this industrial 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 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 tabled 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

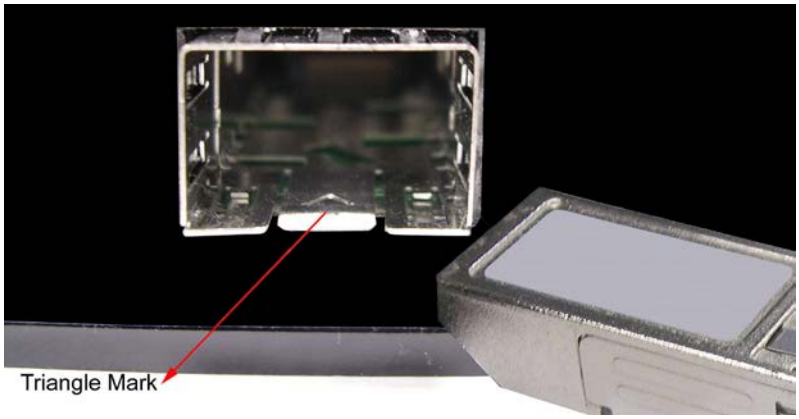
Cabling

Use the four twisted-pair, Category 5e or above cabling for RJ-45 port connection. The cable between the switch and the link partner (switch, hub, workstation, etc.) must be less than 100 meters (328 ft.) long.

As for the small form-factor pluggable (SFP), which is a compact optical transceiver used in optical communications for both telecommunication and data communication applications.

To connect the transceiver and LC cable, please take the steps shown as follows:

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

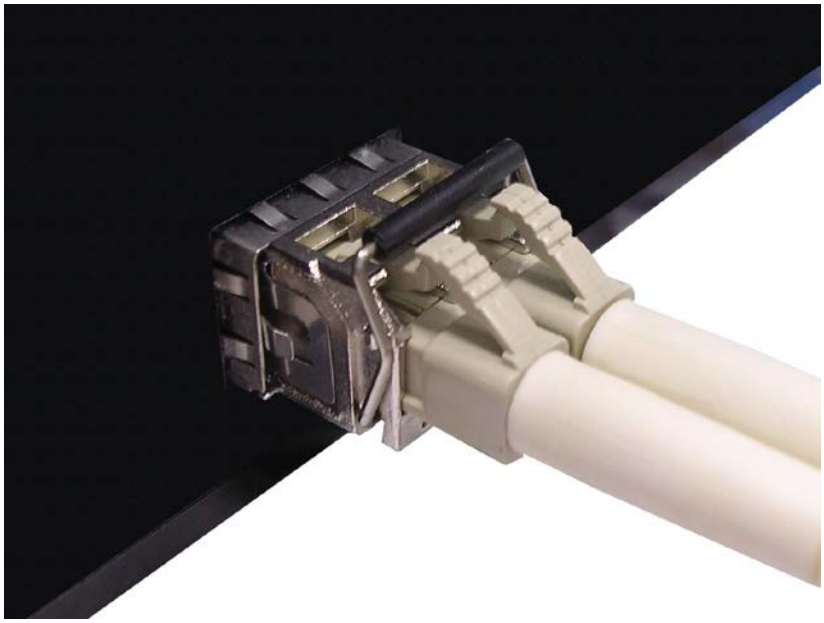


Transceiver to the SFP module



Transceiver Inserted

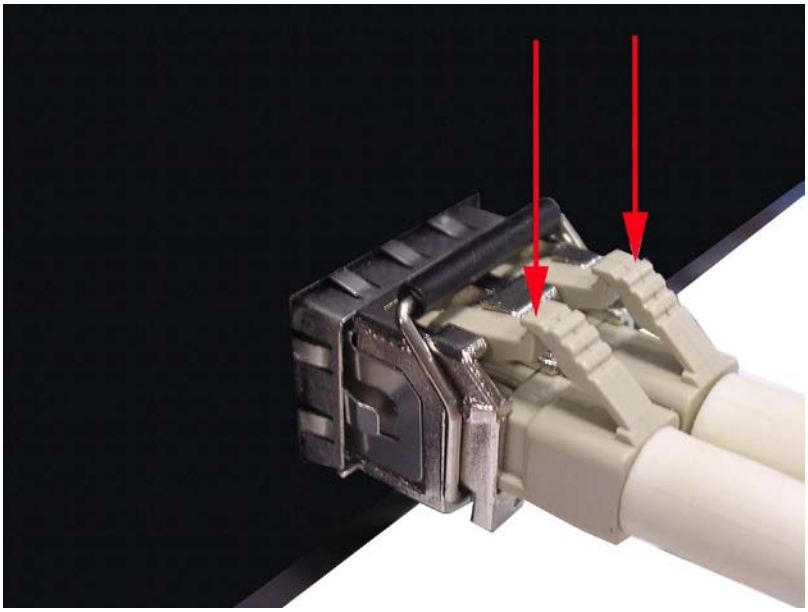
Second, insert the fiber cable of LC connector into the transceiver.



LC connector to the transceiver

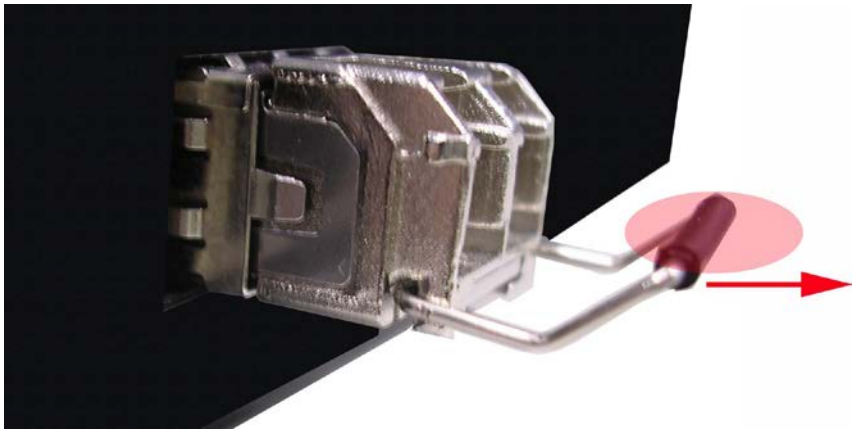
To remove the LC connector from the transceiver, please follow the steps shown below:

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



Remove LC connector

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

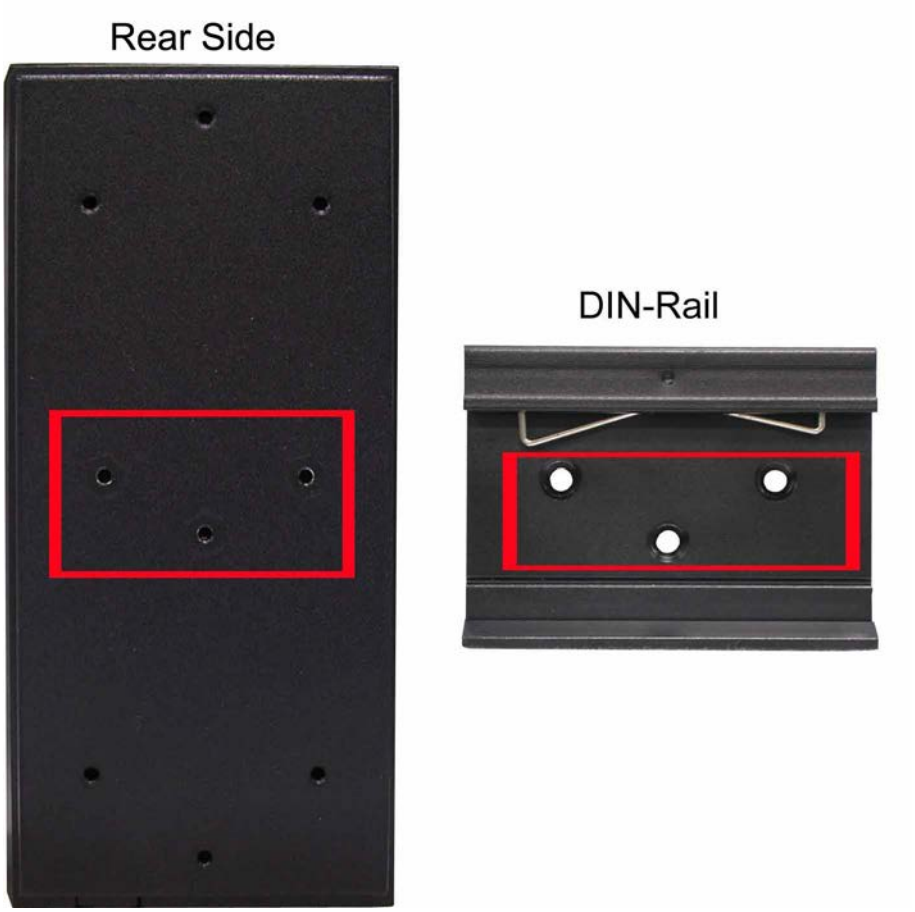


Pull out from the SFP module

Mounting Installation

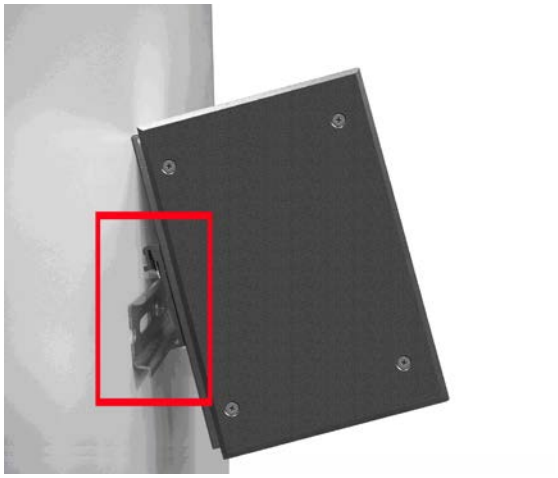
DIN-Rail Mounting

The DIN-Rail is screwed on the industrial switch when out of factory. If the DIN-Rail is not screwed on the industrial switch, please see the following figure to screw the DIN-Rail on the switch. Follow the below steps to hang the industrial switch.

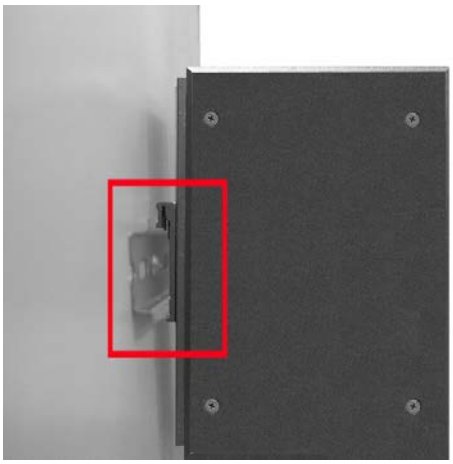


Step 1: Use the screws to screw on the DIN-Rail on the industrial switch.
Step 2: To remove the DIN-Rail, reverse step 1.

1. First, insert the top of DIN-Rail into the track.



2. Then, lightly push the button of DIN-Rail into the track.



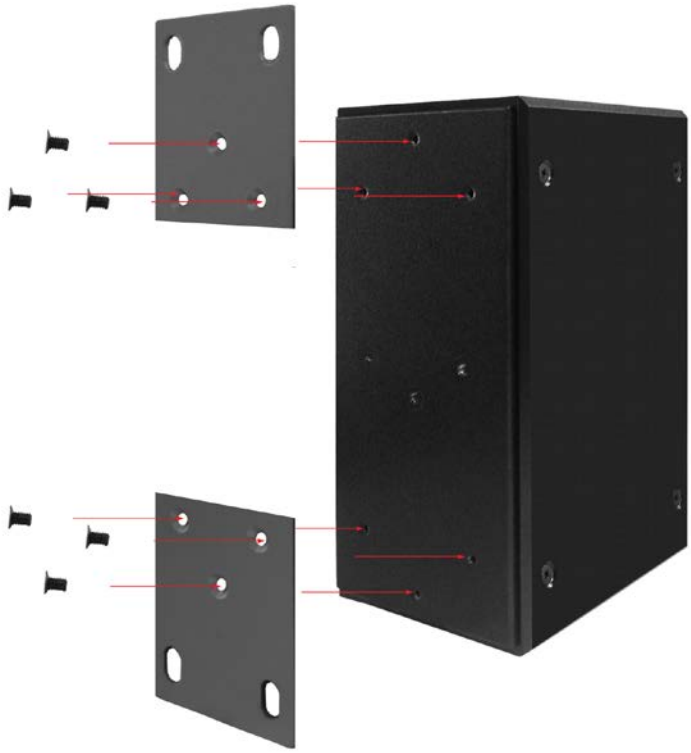
3. Check the DIN-Rail is tightly on the track.
4. To remove the industrial switch from the track, reverse the steps above.

Wall Mount Plate Mounting

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

1. Remove the DIN-Rail from the industrial switch; loose the screws to remove the DIN-Rail.
2. Place the wall mount plate on the rear panel of the industrial switch.
3. Use the screws to screw the wall mount plate on the industrial switch.

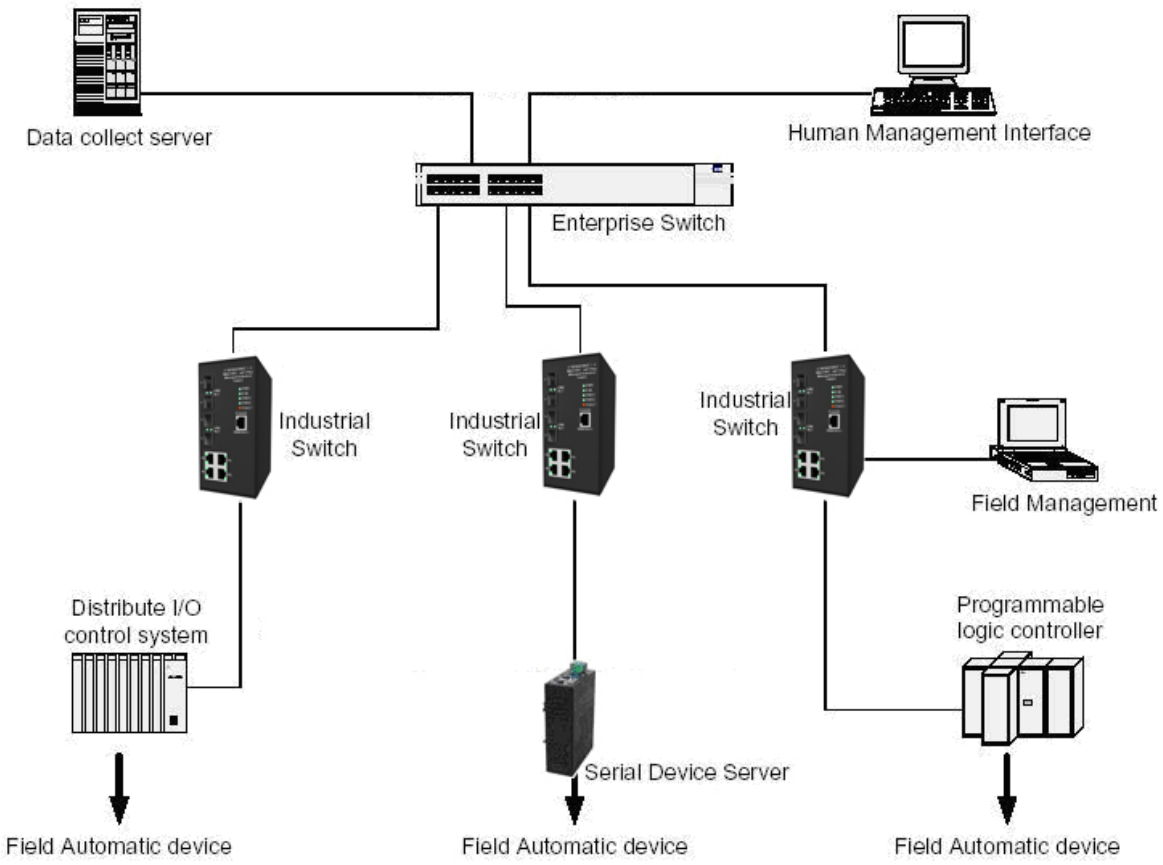
4. Use the hook holes at the corners of the wall mount plate to hang the industrial switch on the wall.
5. To remove the wall mount plate, reverse steps above.



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

Hardware Installation

In this paragraph, we will describe how to install the 4 10/100/1000T + 4 SFP Industrial Switch and the installation points for the attention.



Installation Steps

1. Unpacked the Industrial switch packing.
2. Check the DIN-Rail is screwed on the Industrial switch. If the DIN-Rail is not screwed on the Industrial switch. Please refer to **DIN-Rail Mounting** section for DIN-Rail installation. If you want to wall mount the Industrial switch, then please refer to **Wall Mount Plate Mounting** section for wall mount plate installation.
3. To hang the Industrial switch on the DIN-Rail track or wall, please refer to the **Mounting Installation** section.

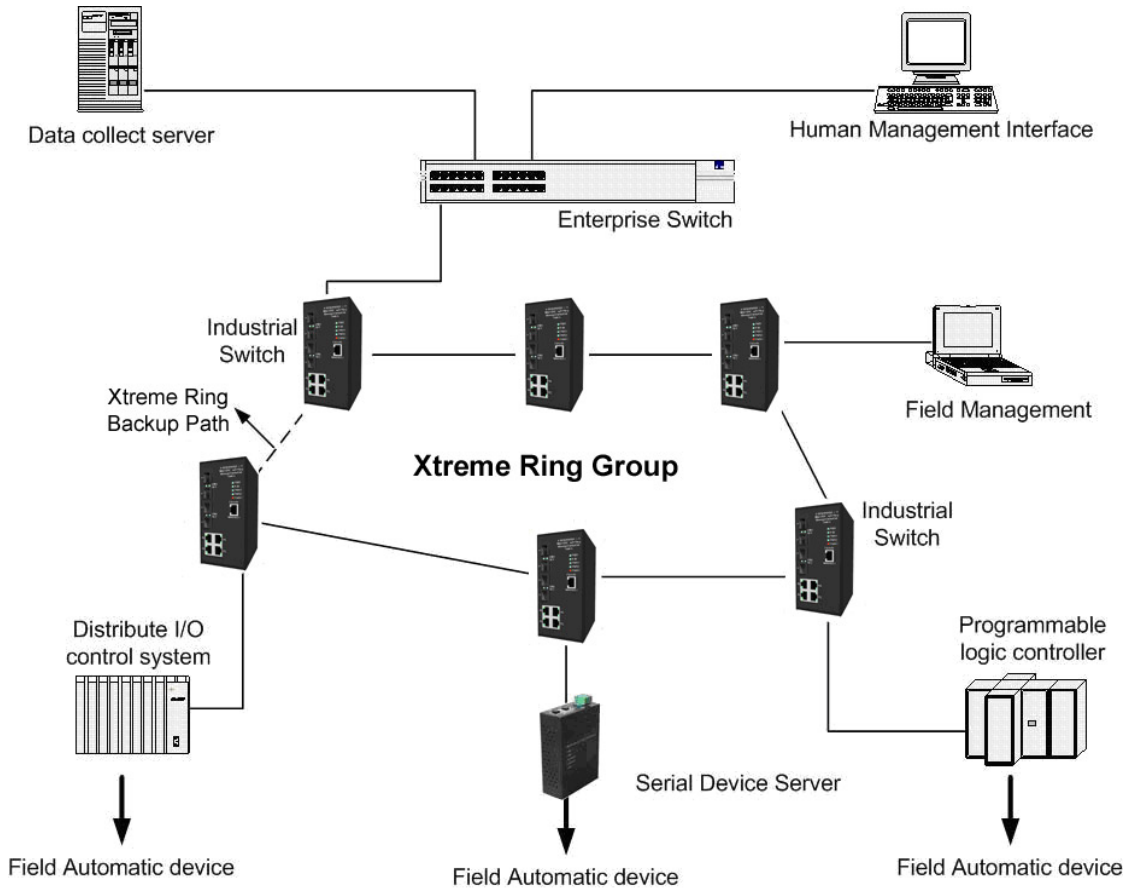
4. Power on the Industrial switch. How to wire the power; please refer to the **Wiring the Power Inputs** section. The power LED on the Industrial switch will light up. Please refer to the **LED Indicators** section for meaning of LED lights.
5. Prepare the twisted-pair, straight through Category 5e/above cable for Ethernet connection and SFP transceiver with LC cable for fiber connection.
6. Insert one side of Category 5e or above cables into the Industrial switch Ethernet port (RJ-45 port) and another side of category 5e or above cables to the network devices' Ethernet port (RJ-45 port), ex: switch, PC or Server. The UTP port (RJ-45) LED on the Industrial switch will light up when the cable connected with 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/above cable.*

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

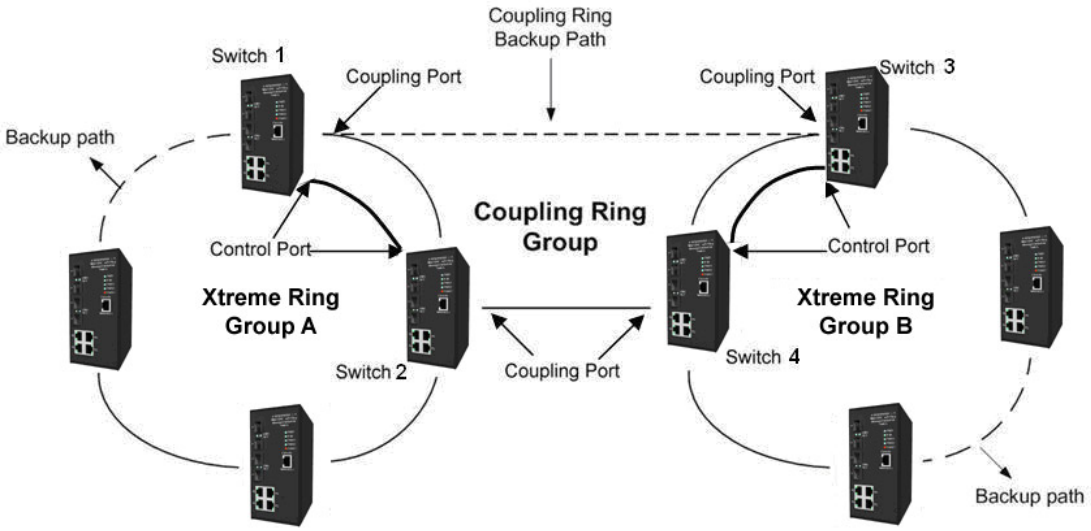
Xtreme Ring Application

The industrial switch supports the Xtreme Ring protocol that can help the network system recover from network connection failure within 20ms or less, and make the network system more reliable. The Xtreme 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 Xtreme Ring application.



Coupling Ring Application

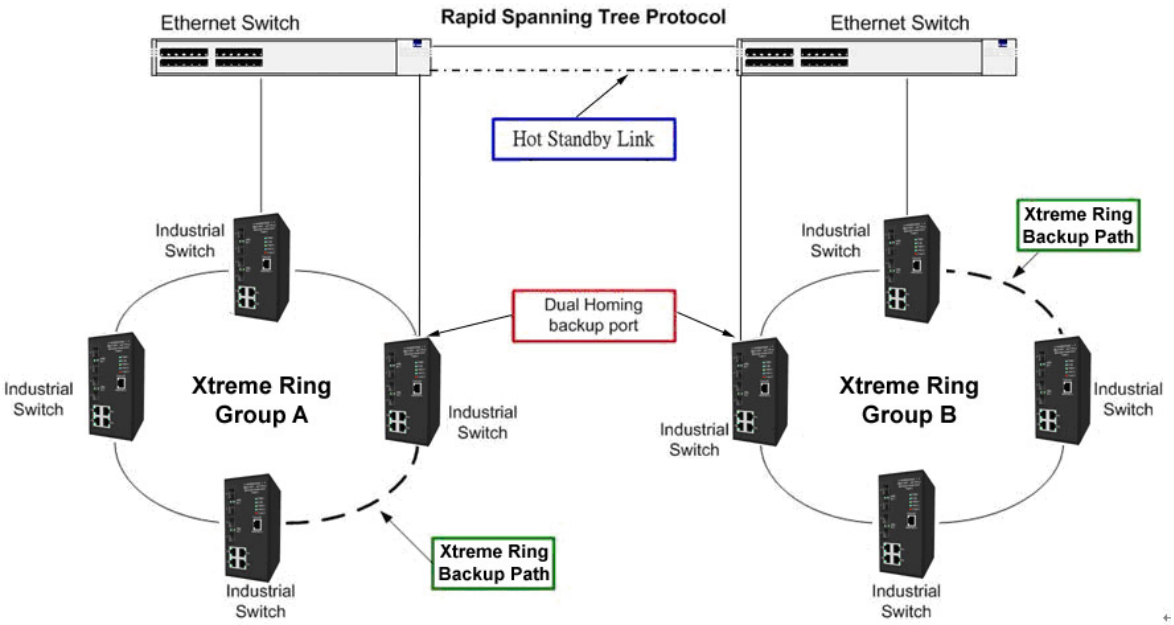
In the network, it may have more than one Xtreme Ring group. Using the coupling ring function can connect each Xtreme Ring for the redundant backup. It can ensure the transmissions between two ring groups not to fail. The following figure is a sample of coupling ring application.



Dual Homing Application

Dual Homing function is to prevent the connection loss from between Xtreme Ring group and upper level/core switch. Assign two ports to be the Dual Homing port that is backup port in the Xtreme Ring group. The Dual Homing function only works when the Xtreme Ring function is active. Each Xtreme Ring group only has one Dual Homing port.

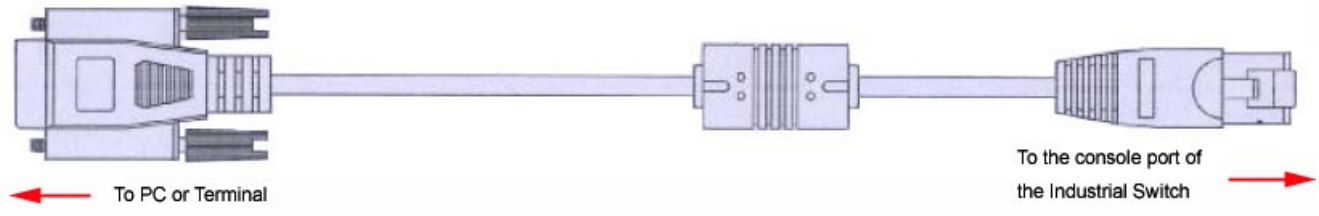
Note *In dual Homing application architecture, the upper level switches need to enable the Rapid Spanning Tree protocol.*

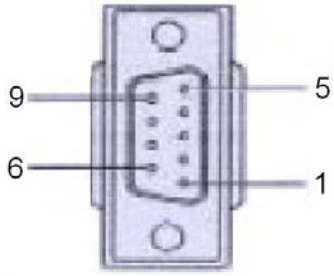

Ethernet Switch
Rapid Spanning Tree Protocol
Ethernet Switch
Hot Standby Link
Industrial Switch
Xtreme Ring Backup Path
Dual Homing backup port
Industrial Switch
Xtreme Ring Group A
Industrial Switch
Industrial Switch
Xtreme Ring Group B
Industrial Switch
Industrial Switch
Xtreme Ring Backup Path
Industrial Switch
Industrial Switch

Console Management

Connecting to the Console Port

The supplied cable which one end is RS-232 connector and the other end is RJ-45 connector. Attach the end of RS-232 connector to PC or terminal and the other end of RJ-45 connector to the console port of switch. The connected terminal or PC must support the terminal emulation program.





DB 9-pin Female

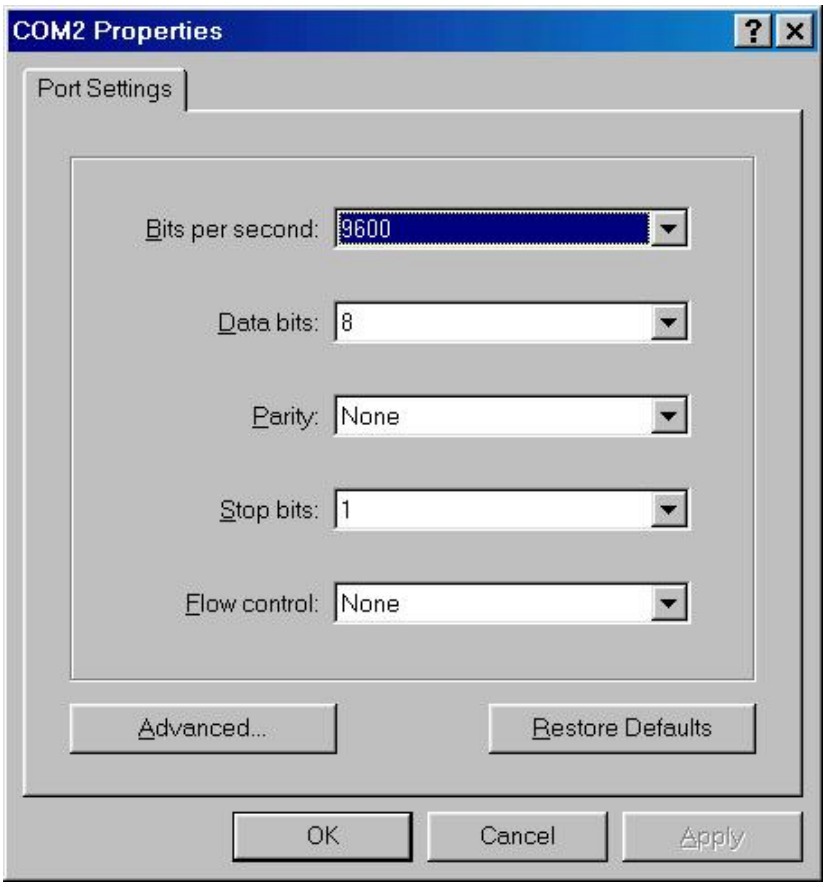
Pin Assignment

DB9 Connector	RJ-45 Connector
NC	1 Orange/White
2	2 Orange
3	3 Green/White
NC	4 Blue
5	5 Blue/White
NC	6 Green
NC	7 Brown/White
NC	8 Brown

Login in the Console Interface

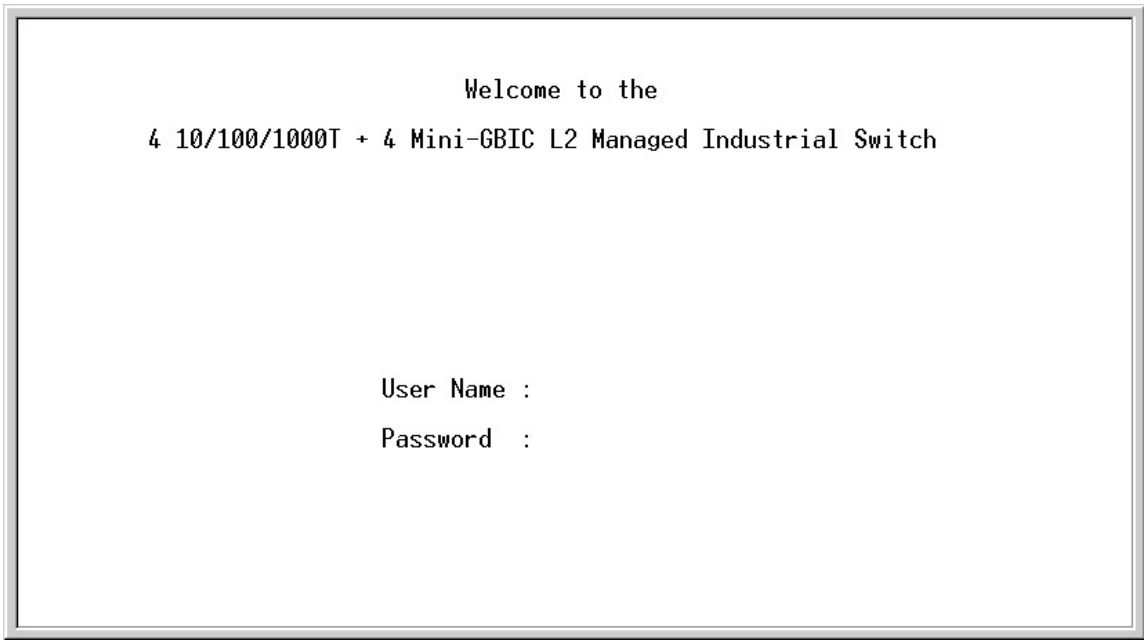
When the connection between Switch and PC is ready, turn on the PC and run a terminal emulation program or **Hyper Terminal** and configure its **communication parameters** to match the following default characteristics of the console port:

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



The settings of communication parameters

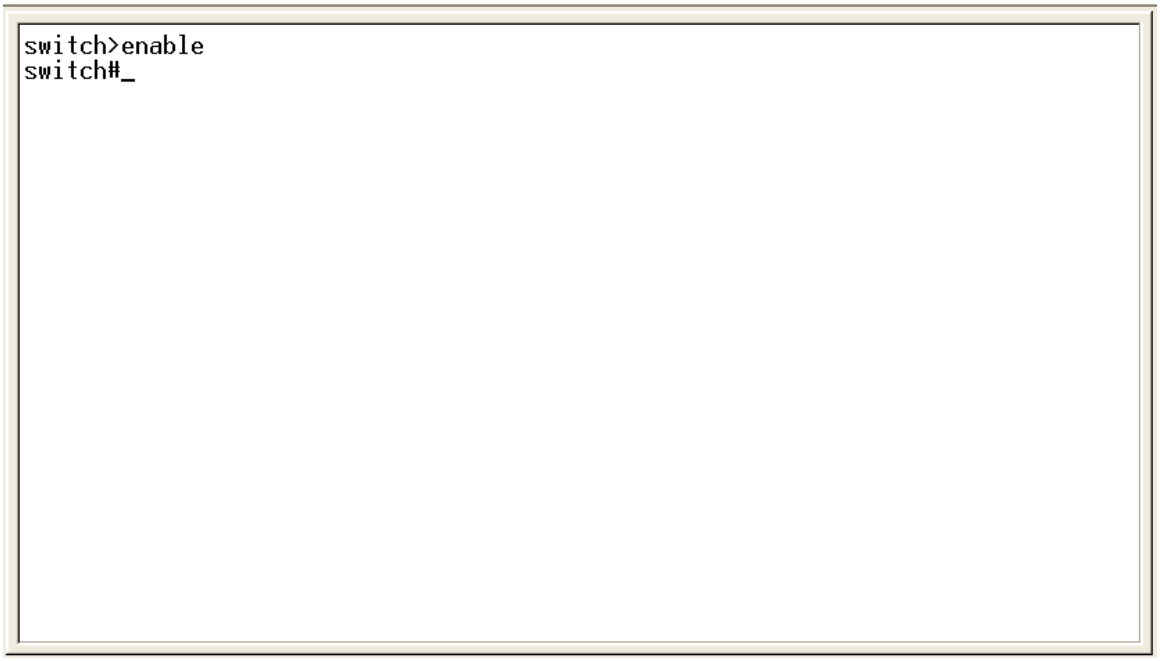
After finishing the parameter settings, click '**OK**'. When the blank screen shows up, press Enter key to bring out the login prompt. Key in the '**root**' (default value) for the both User name and Password (use **Enter** key to switch), then press Enter key and the Main Menu of console management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



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.



CLI command interface

The following table lists the CLI commands and description.

Commands Level

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	switch (vlan)#	To exit to user EXEC mode, enter exit.	Use this mode to configure VLAN-specific parameters.

	privileged EXEC mode.			
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.

Commands Set List

System Commands Set

Commands	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 192.168.16.1 255.255.255.0 192.168.16.254**
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)#**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	switch(config)#**no security telnet**

		telnet server	

Port Commands Set

Commands	Level	Description	Example
interface fastEthernet **[Portid]**	**G**	Choose the port for modification.	switch(config)#**interface fastEthernet 2**
duplex **[full | half]**	**I**	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#**interface fastEthernet 2** switch(config-if)#**duplex full**
speed **[10|100|1000|auto]**	**I**	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can't be set to 1000 if the port isn't a giga port..	switch(config)#**interface fastEthernet 2** switch(config-if)#**speed 100**
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 bandwidth control	switch(config)#**interface fastEthernet 2** switch(config-if)#**show bandwidth**

state **[Enable | Disable]**	**I**	Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disable form of this command to disable the port.	switch(config)#**interface fastEthernet 2** (config-if)#**state Disable**
show interface configuration	**I**	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** (config-if)#**show interface status**
show interface accounting	**I**	show interface statistic counter	switch(config)#**interface fastEthernet 2** (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

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

workp [Workport]		[Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount of member ports.	switch(config)#**aggregator group 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**

VLAN Commands Set

Commands	Level	Description	Example

vlan database	**P**	Enter VLAN configure mode	switch#**vlan database**
Vlanmode [portbase| 802.1q | gvrp]	**V**	To set switch VLAN mode.	switch(vlan)#**vlanmode portbase** or switch(vlan)#**vlanmode 802.1q** or switch(vlan)#**vlanmode gvrp**
no vlan	**V**	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 belong to a trunk group, this command can't be applied.	switch(vlan)#**vlan 8021q port 3 access-link untag 33**
vlan 8021q port [PortNumber] **trunk-link tag**	**V**	Assign a trunk link for VLAN by port, if the	switch(vlan)#**vlan 8021q port 3 trunk-link tag 2,3,6,99**

[TaggedVID List]		port belong to a trunk group, this command can't be applied.	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

Commands	Level	Description	Example
spanning-tree enable	**G**	Enable spanning tree	switch(config)#**spanning-tree enable**
spanning-tree priority [0~61440]	**G**	Configure spanning tree priority parameter	switch(config)#**spanning-tree priority 32767**
spanning-tree max-age	**G**	Use the spanning-tree	switch(config)#**spanning-tree**

[seconds]		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.	**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	switch(config)#**spanning-tree forward-time 20**

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

Commands	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

Commands	Level	Description	Example
igmp enable	**G**	Enable IGMP snooping function	switch(config)#**igmp enable**
Igmp-query auto	**G**	Set IGMP query to auto mode	switch(config)#**Igmp-query auto**
Igmp-query force	**G**	Set IGMP query to force mode	switch(config)#**Igmp-query force**
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

Commands	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	**P**	Show filter MAC	switch#**show mac-address-table**

filter		address table.	**filter**
no mac-address-table static hwaddr [MAC]	**I**	Remove an entry of MAC address table of interface (static)	switch(config)#**interface fastEthernet 2** switch(config-if)#**no mac-address-table static hwaddr 000012345678**
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

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

			192.168.1.50
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 [User Name]	**G**	Remove specified user of SNMPv3 agent.	switch(config)#**no snmpv3 user Test**
no snmpv3 access context-name [Context Name] **group** [Group Name] **security-level** [NoAuthNoPriv|AuthNoPriv|AuthPriv] **match-rule** [Exact|Prifix] **views** [Read View Name] [Write View Name] [Notify View Name]	**G**	Remove specified access table of SNMPv3 agent.	switch(config)#**no snmpv3 access context-name Test group G1 security-level AuthPr iv match-rule Exact views V1 V1 V1**
no snmpv3 mibview view [View Name] **type** [Excluded|Included] **sub-oid** [OID]	**G**	Remove specified mibview table of SNMPV3 agent.	switch(config)#**no snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1**

Port Mirroring Commands Set

Commands	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

Commands	Level	Description	Example
8021x enable	**G**	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# **8021x enable**
8021x system 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 accountport [port ID]	**G**	Use the 802.1x system account port global configuration	switch(config)# **8021x system accountport 1816**

		command to change the accounting port	
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

Commands	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	switch(config)#**restore flash:restore_cfg**

		server and the file name of image.	
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 lash:upgrade_fw**

SystemLog, SMTP and Event Commands Set

Commands	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 X-ring-topology-change [Systemlog|SMTP|Both]	**G**	Set Xtreme Ring topology changed event type	switch(config)#**event X-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 Xtreme 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

Commands	Level	Description	Example
sntp enable	**G**	Enable SNTP function	switch(config)#**sntp enable**
sntp daylight	**G**	Enable daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#**sntp daylight**
sntp daylight-period **[Start time] [End time]**	**G**	Set period of daylight saving time, if SNTP function is inactive, this command can't be applied. Parameter format: [yyyymmdd-hh:mm]	switch(config)# **sntp daylight-period 20060101-01:01 20060202-01-01**
sntp daylight-offset **[Minute]**	**G**	Set offset of daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#**sntp daylight-offset 3**
sntp ip **[IP]**	**G**	Set SNTP server IP, if SNTP function is inactive, this command can't be applied.	switch(config)#**sntp ip 192.169.1.1**
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**

Xtreme Ring Commands Set

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

Web-Based Management

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

About Web-based Management

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

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

Preparing for Web Management

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

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

System Login

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



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



Login screen

Main interface

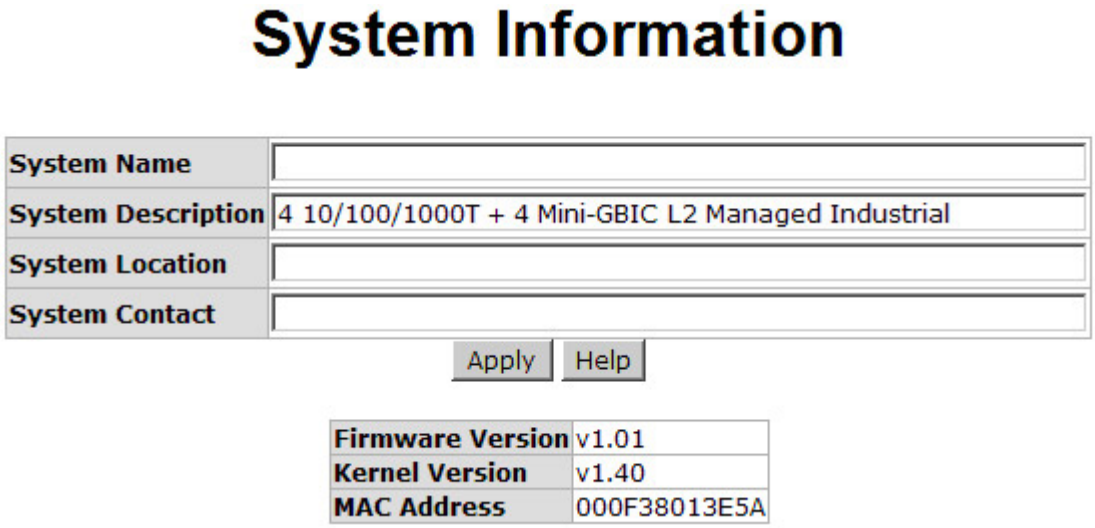


Main interface

System Information

Assigning the system name, location and view the system information

- **System Name:** Assign the name of switch. The maximum length is 64 bytes
- **System Description:** Displays the description of switch. Read only 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)



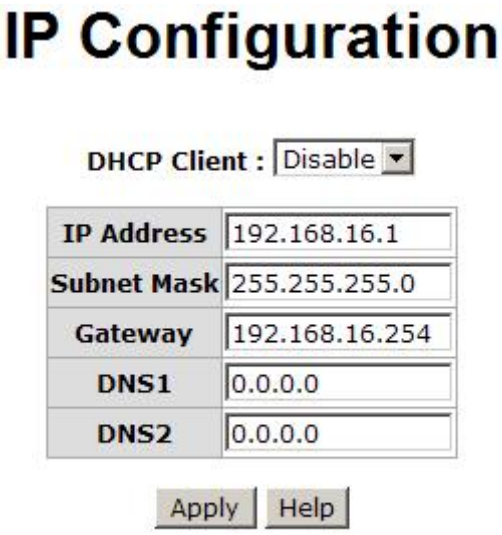
System information interface

IP Configuration

User can configure the IP Settings and DHCP client function

- **DHCP Client:** To enable or disable the DHCP client function. When DHCP client function is enabling, the industrial switch will be assigned the IP address from the network DHCP server. The default IP address will be replace by the DHCP server assigned IP address. After user click 'Apply' button, a popup dialog show up. It is to inform the user that when the DHCP client is enabling, the current IP will lose and user should find the new IP on the DHCP server.

- **IP Address:** Assign the IP address that the network is using. If DHCP client function is enabling, and then user don't need to assign the IP address. And, the network DHCP server will assign the IP address for the industrial switch and displays in this column. The default IP is 192.168.16.1.
- **Subnet Mask:** Assign the subnet mask of the IP address. If DHCP client function is enabling, and then user do not need to assign the subnet mask.
- **Gateway:** Assign the network gateway for the industrial switch. The default gateway is 192.168.16.254.
- **DNS1:** Assign the primary DNS IP address.
- **DNS2:** Assign the secondary DNS IP address.
- And then, click Apply



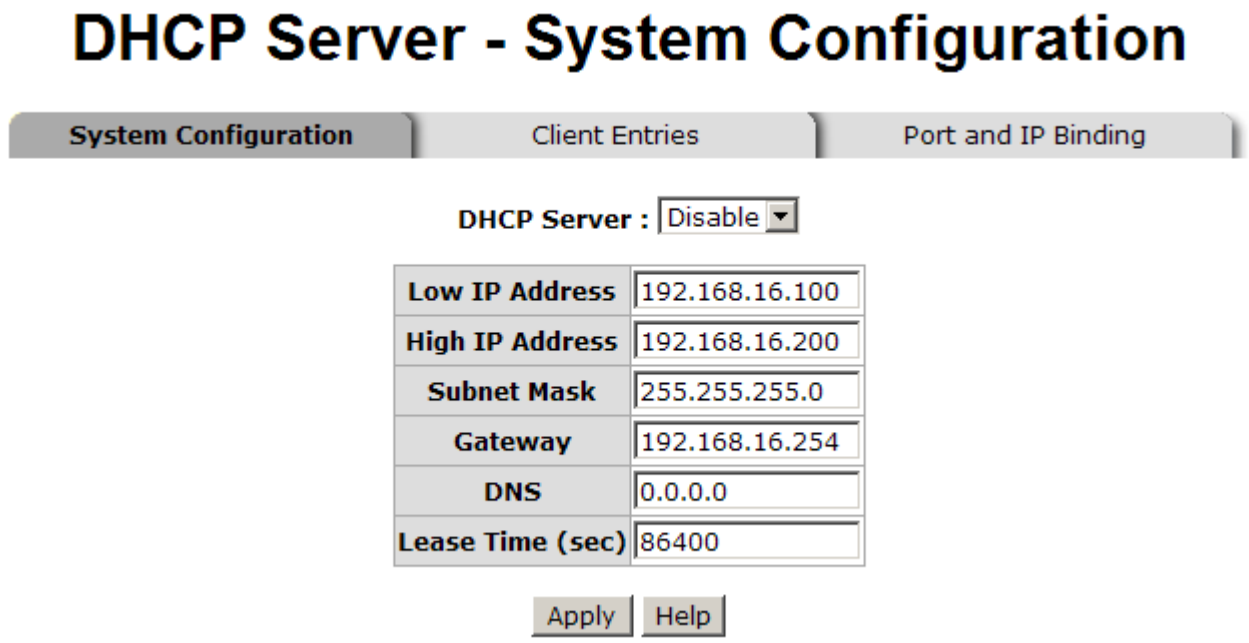
IP configuration interface

DHCP Server – System configuration

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

- **DHCP Server:** Enable or Disable the DHCP Server function. Enable – the switch will be the DHCP server on your local network.
- **Low IP Address:** the dynamic IP assign range. Low IP address is the beginning of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.168.1.100 ~ 192.168.1.200. In contrast, 192.168.1.100 is the Low IP address.

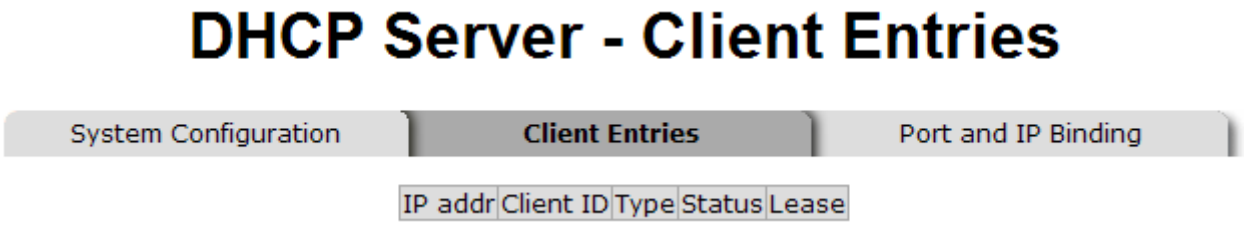
- **High IP Address:** the dynamic IP assign range. High IP address is the end of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.168.1.100 ~ 192.168.1.200. In comparison, 192.168.1.200 is the High IP address.
- **Subnet Mask:** the dynamic IP assign range subnet mask.
- **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 time or the server doesn't know that the dynamic IP is idle.
- And then, click Apply



DHCP Server Configuration interface

DHCP Client – System Configuration

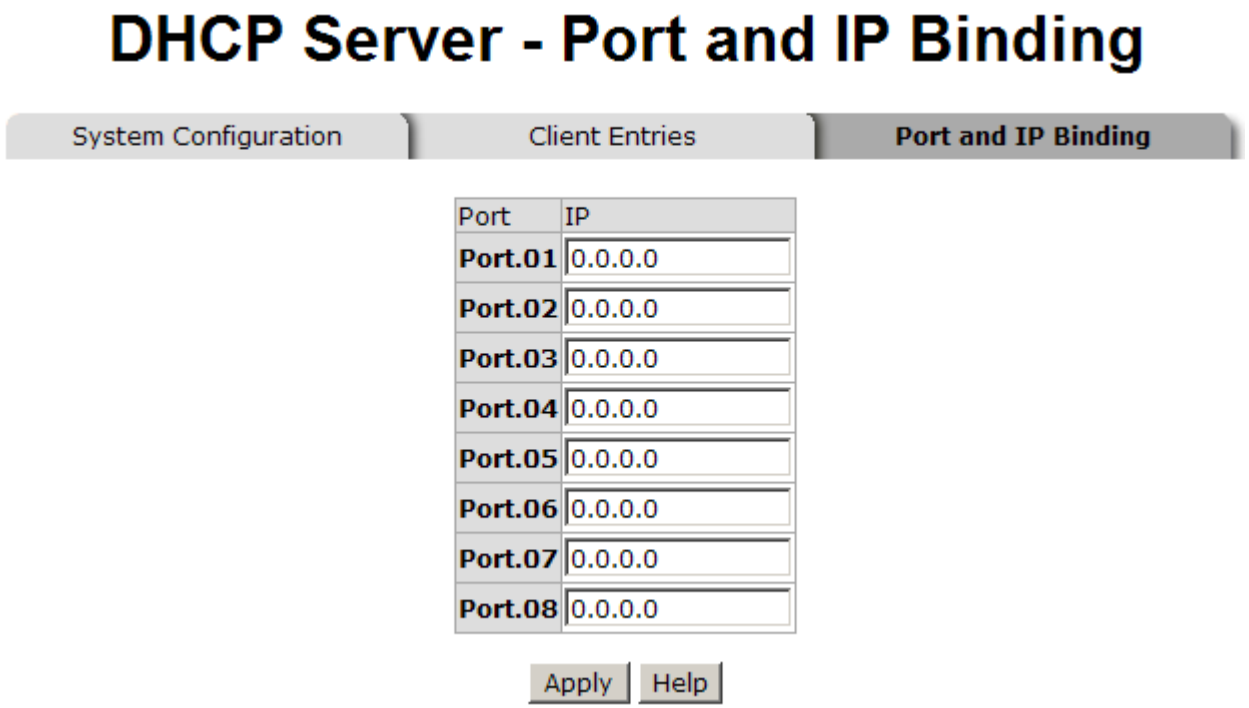
When the DHCP server function is active, the system will collect the DHCP client information and displays it here.



DHCP Client Entries interface

DHCP Server - Port and IP Bindings

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

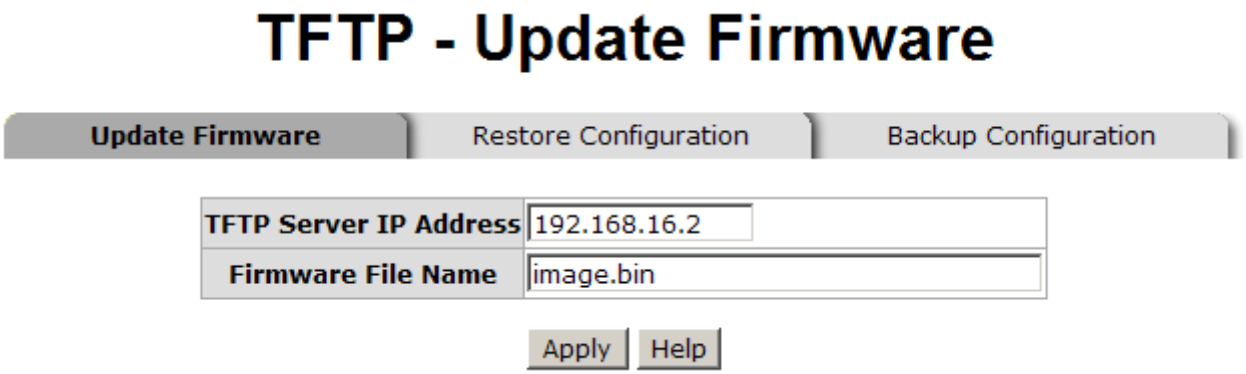


Port and IP Bindings interface

TFTP - Update Firmware

It provides the functions to allow a user to update the switch 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 image.
3. Click Apply.

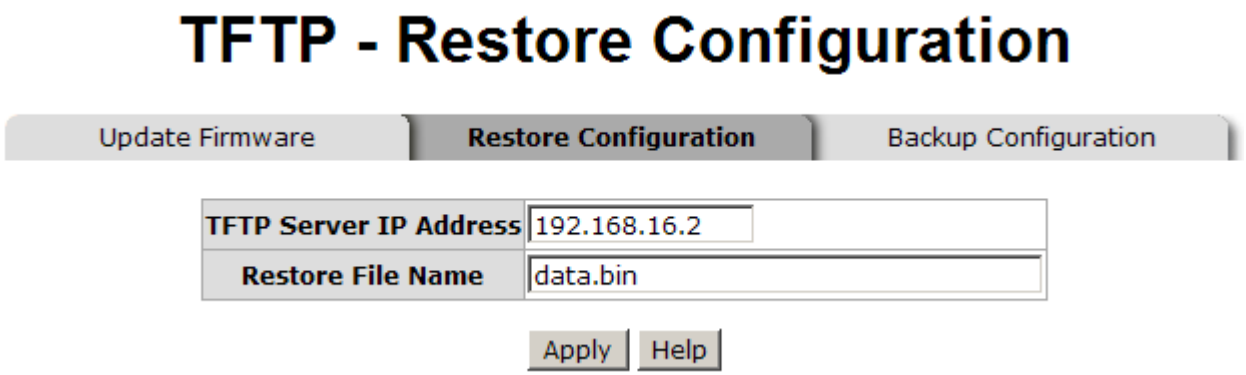


Update Firmware interface

TFTP – Restore Configuration

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

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



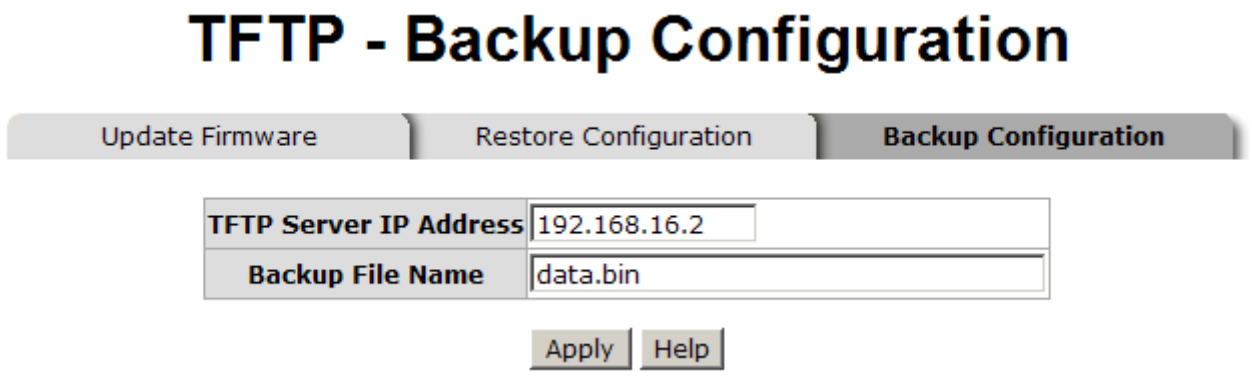
Restore Configuration interface

TFTP - Backup Configuration

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

1. **TFTP Server IP Address:** fill in the TFTP server IP
2. **Backup File Name:** fill the file name

3. Click Apply.

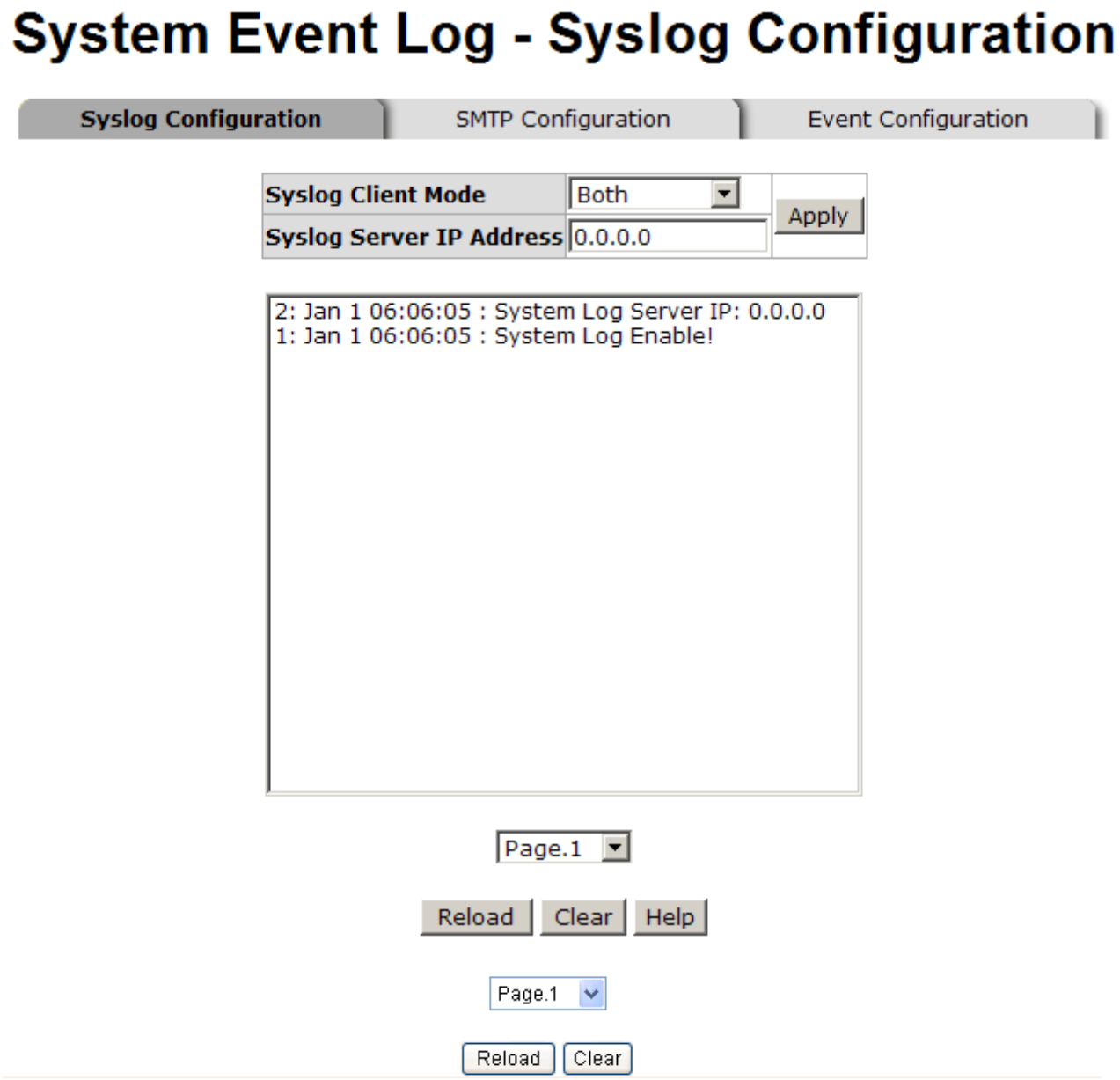


Backup Configuration interface

System Event Log – Syslog Configuration

Configuring the system event mode that want to be collected and system log server IP.

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



Syslog Configuration interface

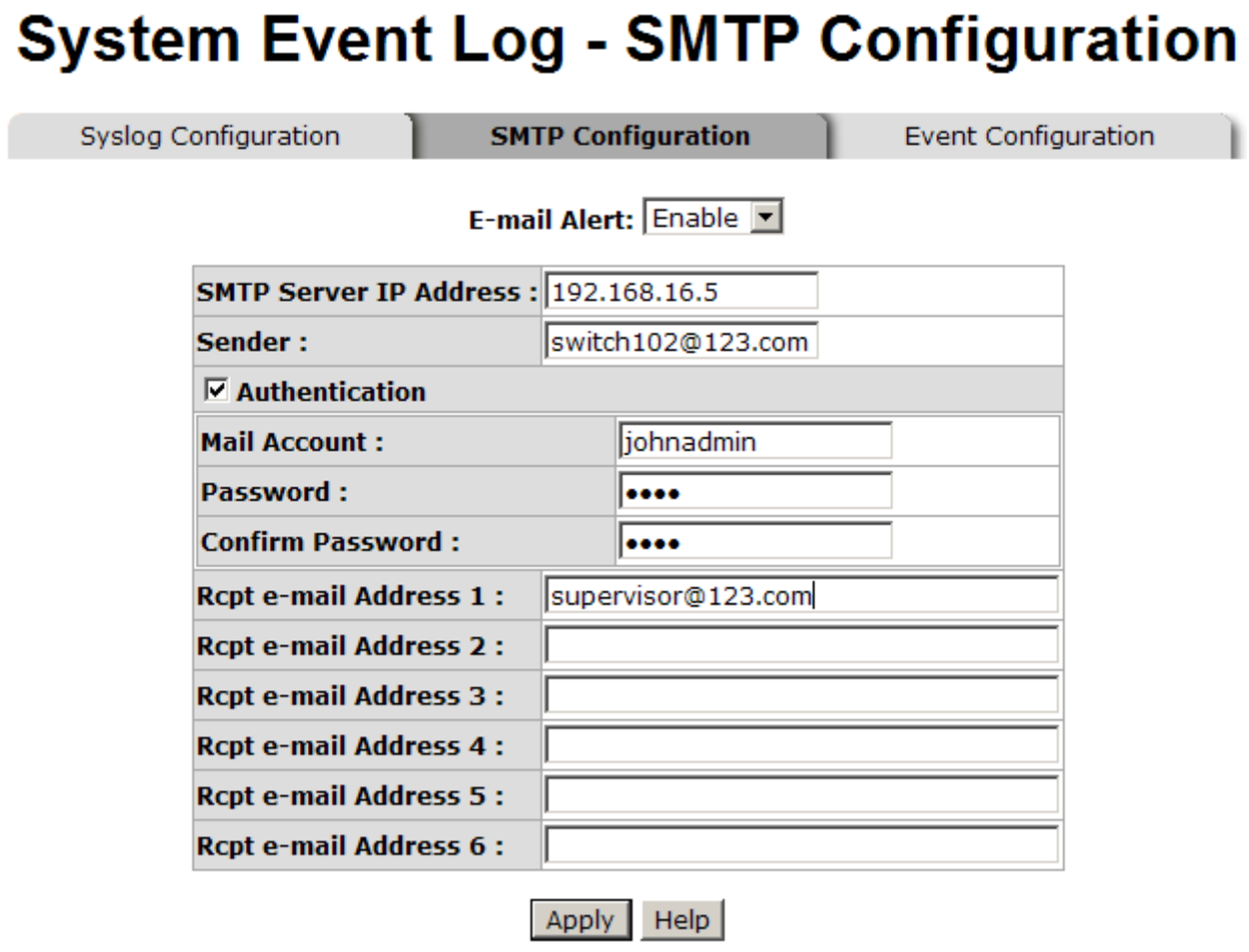
System Event Log - SMTP Configuration

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

1. **Email Alert:** enable or disable the email alert function.
2. **SMTP Server IP:** set up the mail server IP address (when **Email Alert** enabled, this function will then be available).
3. **Sender:** key in a complete email address, e.g. switch102@123.com, to identify

where the event log comes from.

4. **Authentication:** mark the check box to enable and configure the email account and password for authentication (when **Email Alert** enabled, this function will then be available).
5. **Mail Account:** set up the email account, e.g. johnadmin, to receive the alert. It must be an existing email account on the mail server, which you had set up in **SMTP Server IP Address** column.
6. **Password:** The email account password.
7. **Confirm Password:** reconfirm the password.
8. **Rcpt e-mail Address 1 ~ 6:** you can assign up to 6 e-mail accounts also to receive the alert.
9. Click Apply.

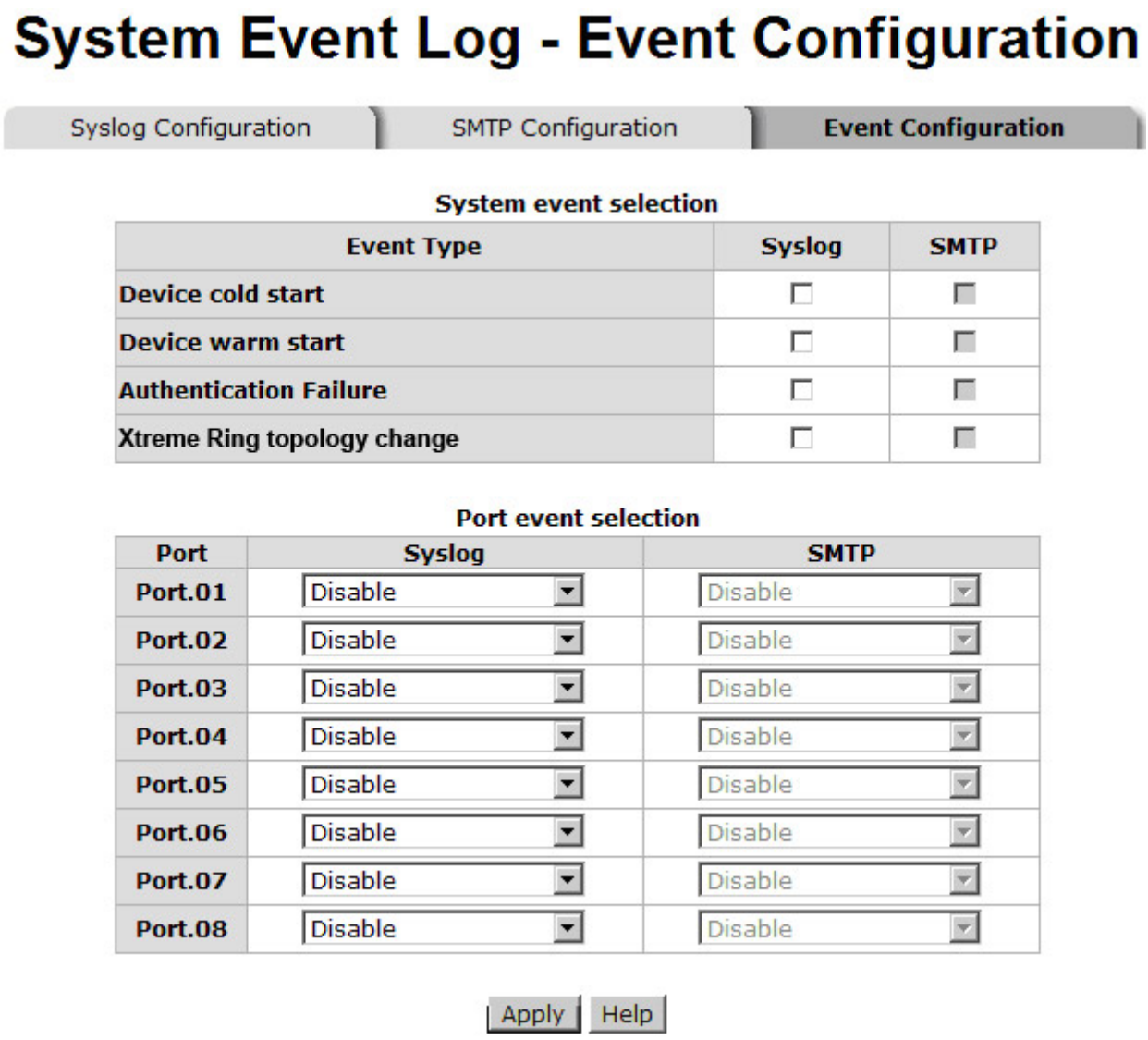


SMTP Configuration interface

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 log information. Also, per port log and SMTP events can be selected. After configure, Click Apply.

- **System event selection:** 4 selections – Device cold start, Device warm start, SNMP Authentication Failure, and Xtreme Ring topology change. Mark the checkbox to select the event. When selected events occur, the system will issue the logs.
  - **Device cold start:** when the device executes cold start action, the system will issue a log event.
  - **Device warm start:** when the device executes warm start, the system will issue a log event.
  - **Authentication Failure:** when the SMTP authentication fails, the system will issue a log event.
  - **Xtreme Ring topology change:** when the Xtreme Ring topology has changed, the system will issue a log event.

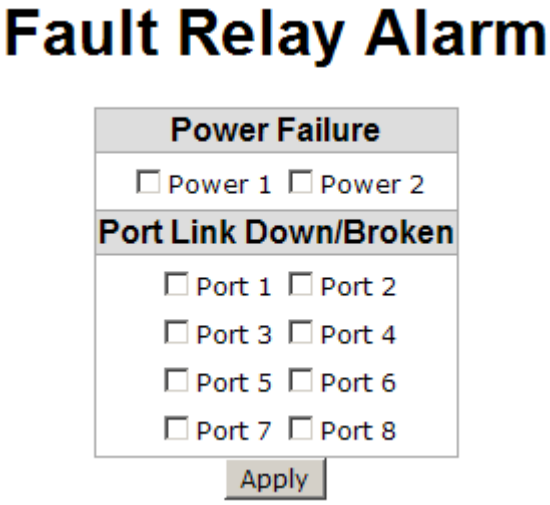


Event Configuration interface

- **Port event selection:** select the per port events and per port SMTP events. It has 3 selections – Link UP, Link Down, and 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:** Mark the check box to enable the function of lighting up **FAULT** LED on the panel when power fails.
- **Port Link Down/Broken:** Mark the check box to enable the function of lighting up **FAULT** LED on the panel when Ports' states are link down or broken.



Fault Relay Alarm interface

SNTP Configuration

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

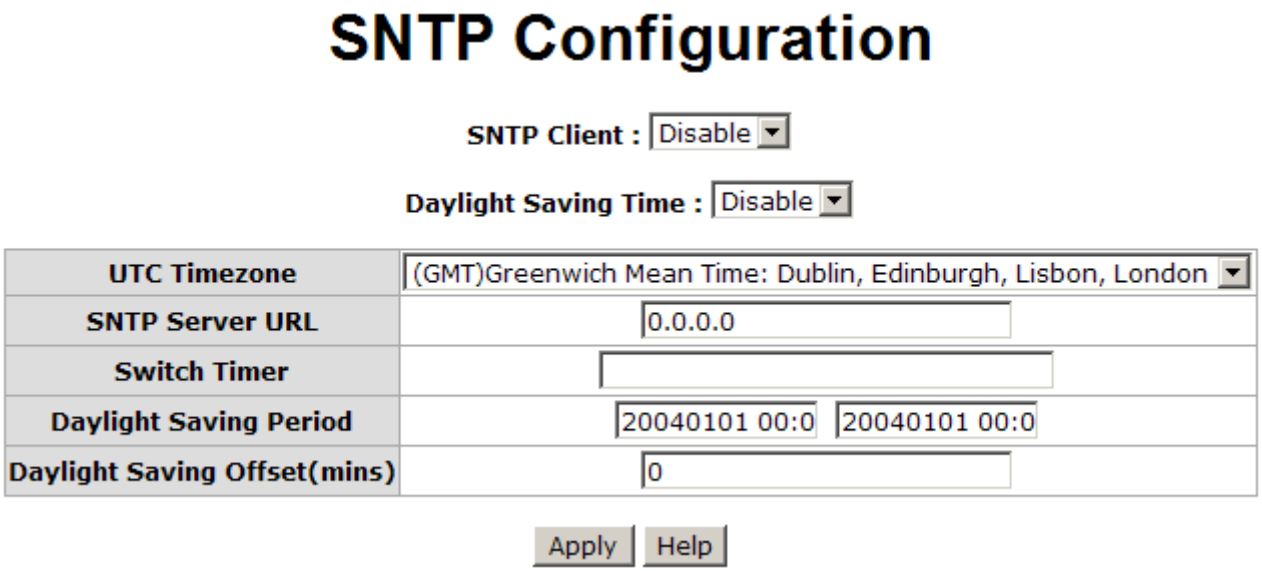
1. **SNTP Client:** enable or disable SNTP function to get the time from the SNTP server.
2. **Daylight Saving Time:** enable or disable daylight saving time function. When daylight saving time is enabling, you need to configure the daylight saving time period..
3. **UTC Timezone:** set the switch location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

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am

Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter 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 Sever URL:** set the SNTP server IP address.
5. **Daylight Saving Period:** set up the Daylight Saving beginning time and Daylight Saving ending time. Both will be different in every year.
6. **Daylight Saving Offset (mins):** set up the offset time.
7. **Switch Timer:** Displays the switch current time.
8. Click Apply.



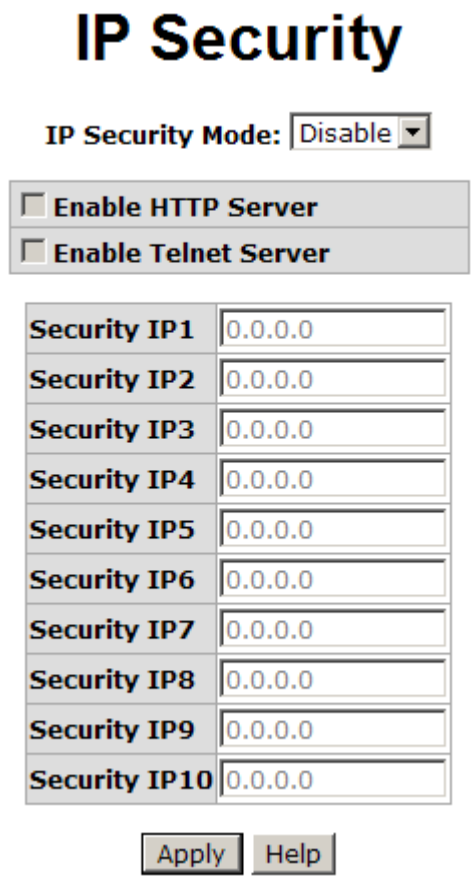
SNTP Configuration interface

IP Security

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 **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 to 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, click Apply button to apply the configuration

Note *Remember to execute the 'Save Configuration' action, otherwise the new configuration will lose when switch power off*



IP Security interface

User Authentication

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

1. **User name:** Key in the new user name (The default is 'root')
2. **Password:** Key in the new password (The default is 'root')
3. **Confirm password:** Re-type the new password
4. And then, click Apply



User Authentication interface

Port Statistics

The following information provides the current port statistic information.

- **Port:** The port number.
- **Type:** Displays the current speed of connection to the port.
- **Link:** The status of linking—'**Up**' or '**Down**'.
- **State:** It's set by Port Control. When the state is disabled, the port will not transmit or receive any packet.
- **Tx Good Packet:** The counts of transmitting good packets via this port.
- **Tx Bad Packet:** The counts of transmitting bad packets (including undersize [less than 64 octets], oversize, CRC Align errors, fragments and jabbers packets) via this port.
- **Rx Good Packet:** The counts of receiving good packets via this port.
- **Rx Bad Packet:** The counts of receiving good packets (including undersize [less than 64 octets], oversize, CRC error, fragments and jabbers) via this port.
- **Tx Abort Packet:** The aborted packet while transmitting.
- **Packet Collision:** The counts of collision packet.
- **Packet Dropped:** The counts of dropped packet.
- **Rx Bcast Packet:** The counts of broadcast packet.
- **Rx Mcast Packet:** The counts of multicast packet.
- Click Clear button to clean 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	Up	Enable	106	0	284	0	0	0	0	75	2
Port.02	1000TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.03	1000TX	Down	Enable	0	0	0	0	0	0	0	0	0
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

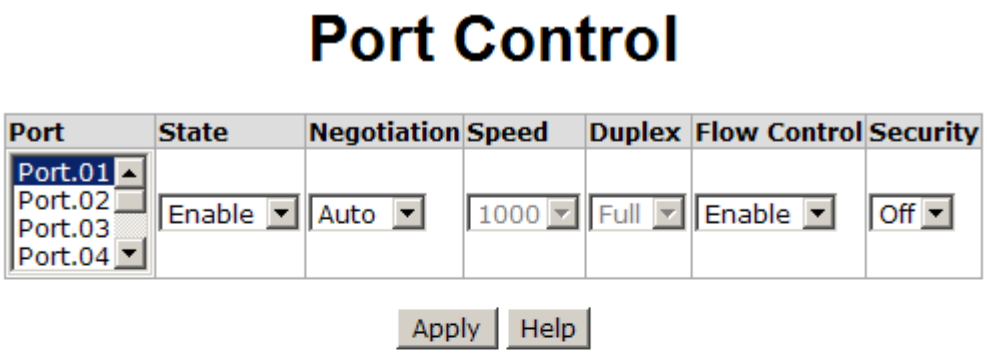
Clear Help

Port Statistics interface

Port Control

In Port control, you can view every port status that depended on 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 disable then will not receive or transmit any packet.
3. **Negotiation:** set auto negotiation status of port.
4. **Speed:** set the port link speed.
5. **Duplex:** set full-duplex or half-duplex mode of the port.
6. **Flow Control:** set flow control function is **Symmetric** or **Asymmetric** in Full Duplex mode. The default value is **Symmetric**.
7. **Security:** When its state is '**On**', means this port accepts only one MAC address.
8. Click Apply.



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

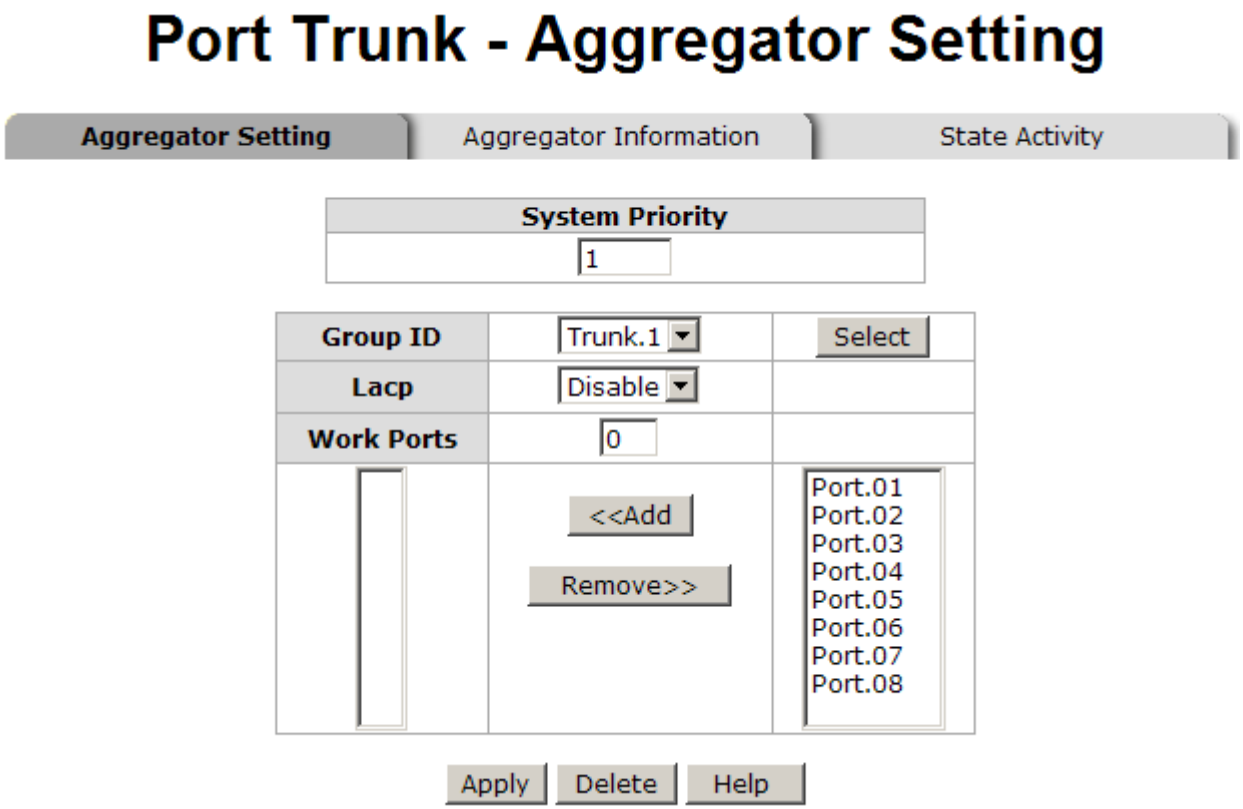
Port Trunk

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, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. Link aggregation lets you group up to 4 consecutive ports into two dedicated connections. This feature can expand bandwidth to a device on the network. **LACP operation requires full-duplex mode,** more detail 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 click Select.
3. **LACP:** If enable, the group is LACP static trunk group. If disable, the group is local static trunk group. All ports support LACP dynamic trunk group. If connecting to the device that also supports LACP, the LACP dynamic trunk group will be created automatically.
4. **Work ports:** allow max four ports can be aggregated at the same time. With LACP static trunk group, the exceed ports are standby and can be aggregated if work ports fail. If it is 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. Click Add button to add the port. To remove unwanted ports, select the port and click Remove button.
6. If LACP enable, you can configure LACP Active/Passive status in each ports on State Activity page.
7. Click Apply.

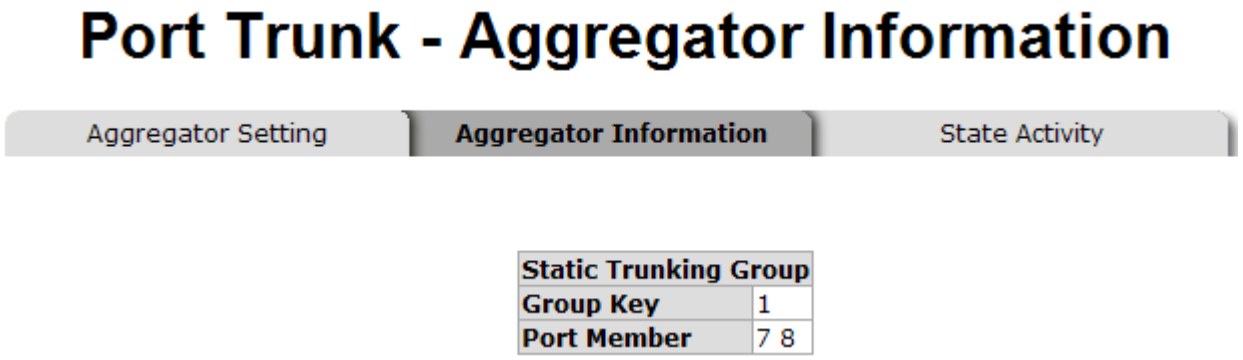
8. Use Delete button to delete Trunk Group. Select the Group ID and click Delete button.



Port Trunk—Aggregator Setting interface

Aggregator Information

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



Port Trunk – Aggregator Information interface

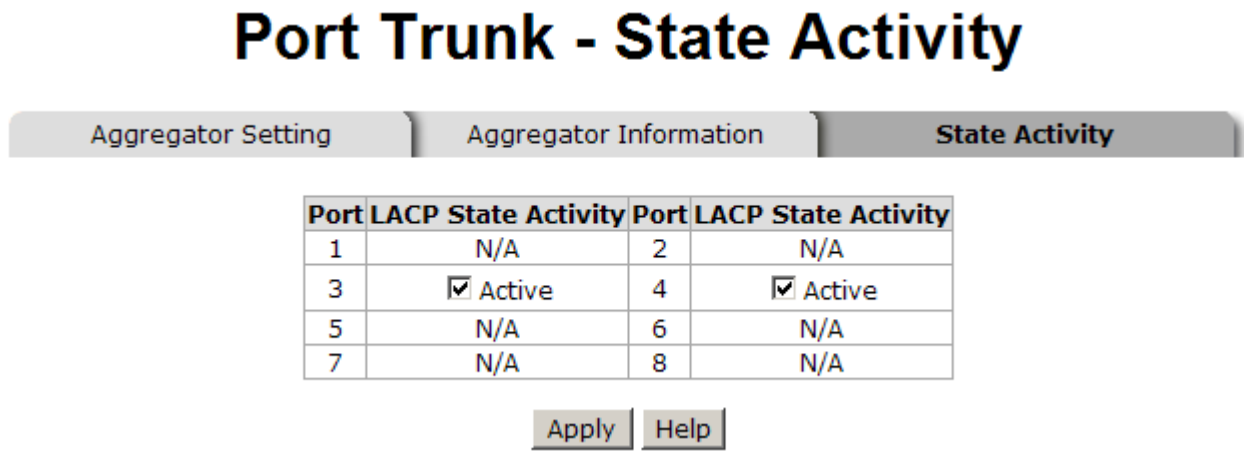
State Activity

When you had setup the LACP aggregator, you can configure port state activity. You can mark or un-mark the port. When you mark the port and click 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 active LACP's actor, after you have selected trunk port, the active status will be created automatically.*

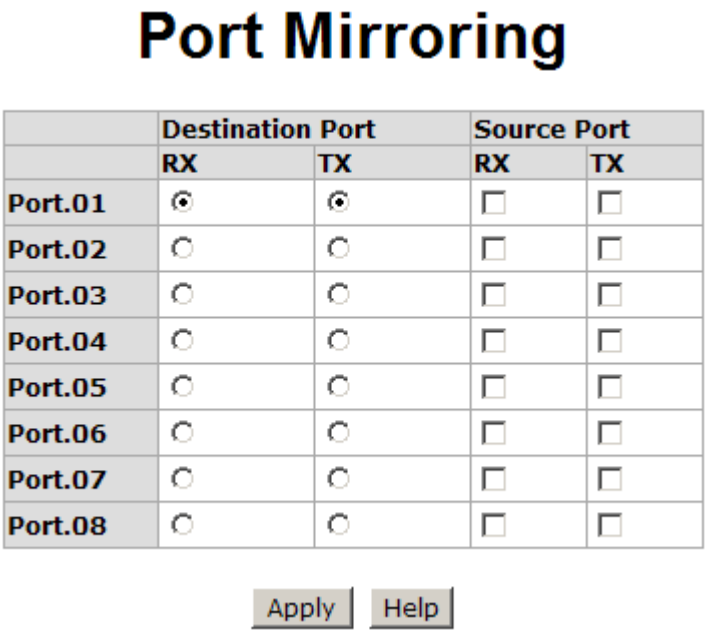


Port Trunk – State Activity interface

Port Mirroring

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

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



Port Trunk – Port Mirroring interface

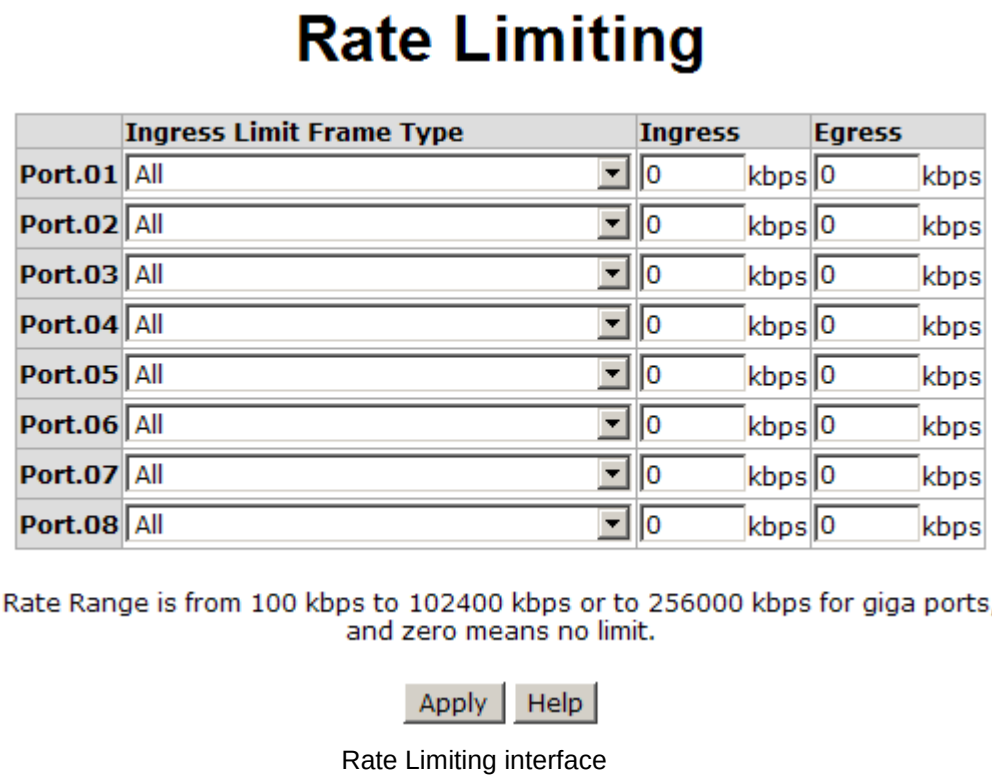
Rate Limiting

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 4 options for selecting: **All, Broadcast/Multicast/Flooded Unicast, Broadcast/Multicast** and **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 interface

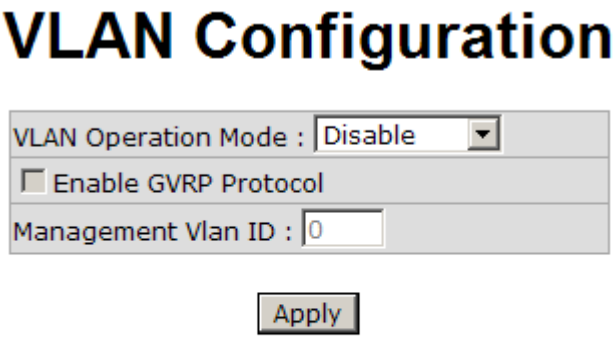
- All the ports support port ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set it's effective egress rate is 1Mbps, ingress rate is 500Kbps. The switch performs the ingress rate by packet counter to meet the specified rate
  - **Ingress:** Enter the port effective ingress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

VLAN configuration

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which would allow you to isolate network traffic, so only the members of the VLAN will

receive traffic from the same members of VLAN. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically.

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

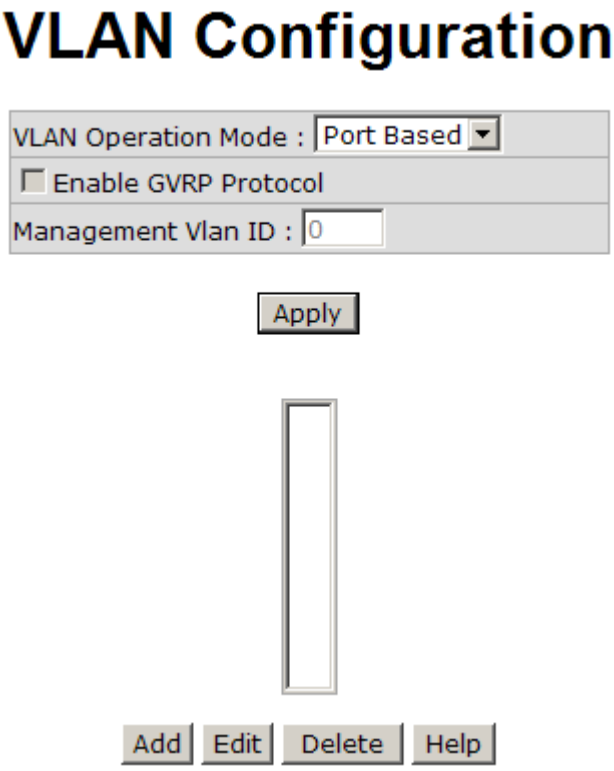


VLAN Configuration interface

VLAN configuration - Port-based VLAN

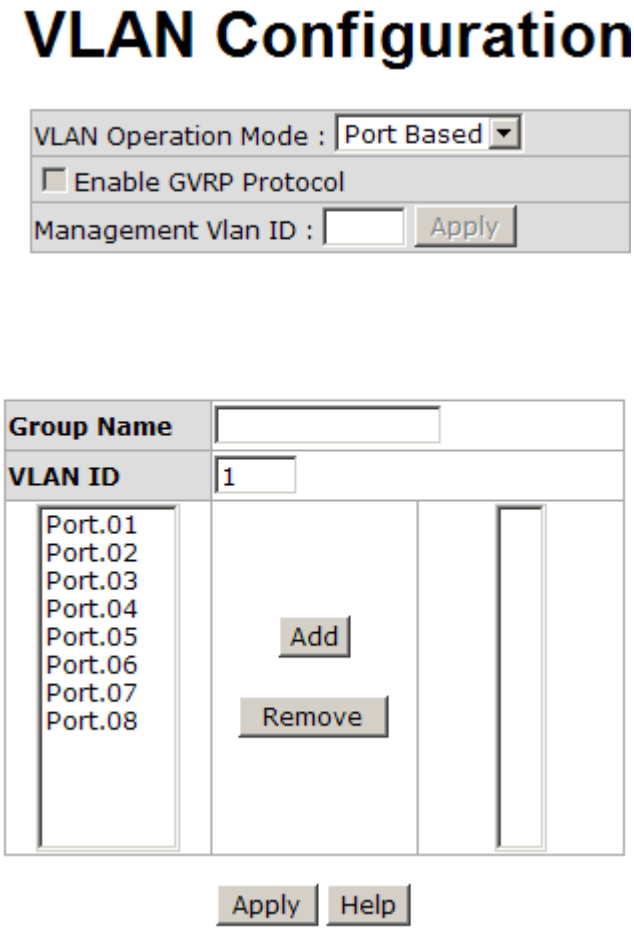
Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging is ignored.

In order for an end station to send packets to different VLAN groups, it itself 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 – Port Based interface

- Click Add to add a new VLAN group(The maximum VLAN group is up to 64 VLAN groups)
- Entering the VLAN name, group ID and grouping the members of VLAN group
- And then, click Apply



VLAN—Port Based Add interface

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

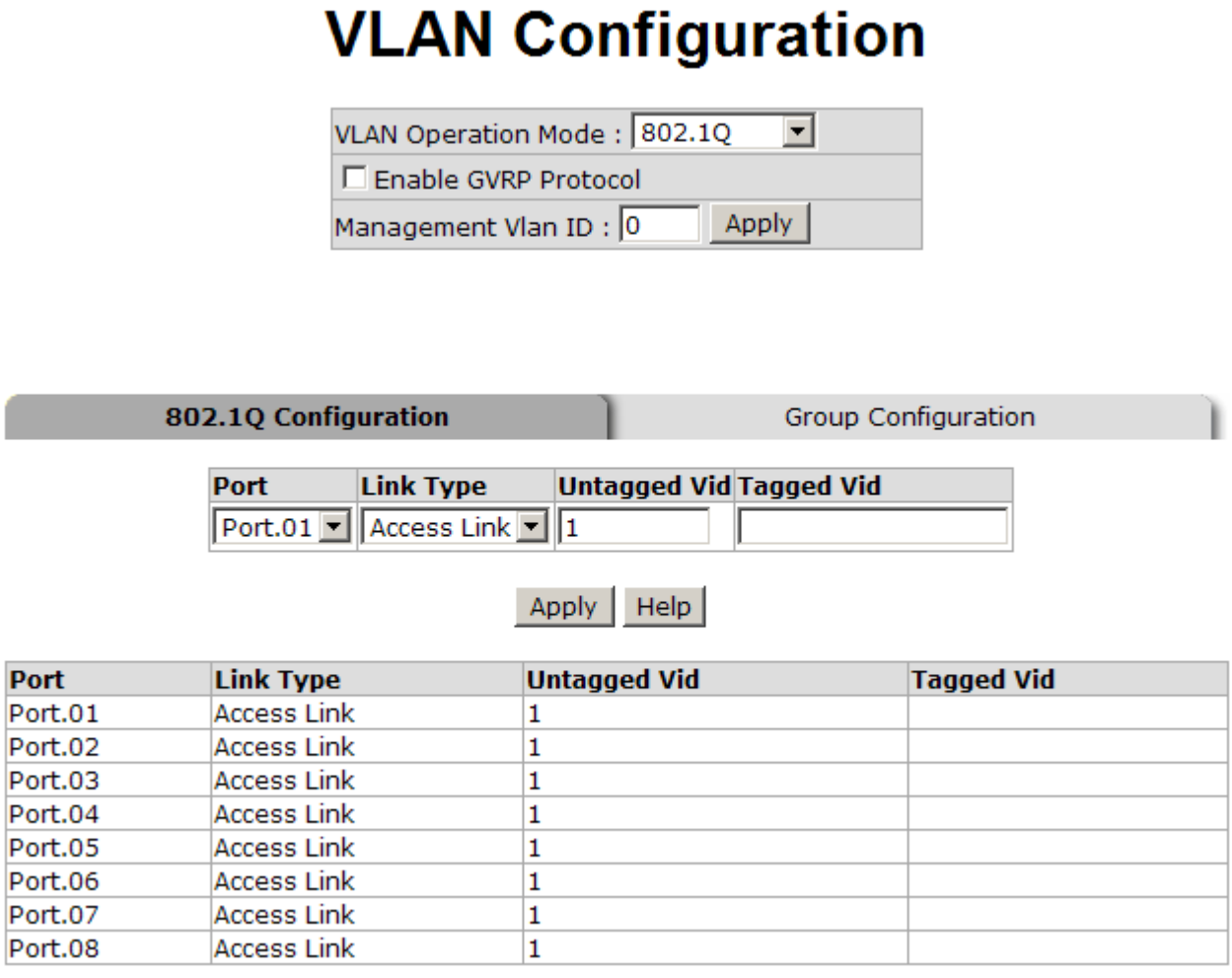
Note *Remember to execute the 'Save Configuration' action, otherwise the new configuration will lose when switch power off.*

802.1Q VLAN

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

You can create Tag-based VLAN, and enable or disable GVRP protocol. There are 256 VLAN groups to provide configure. Enable 802.1Q VLAN, the all ports on the switch belong to default VLAN, VID is 1. The default VLAN can’t be deleting.

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



802.1q VLAN interface

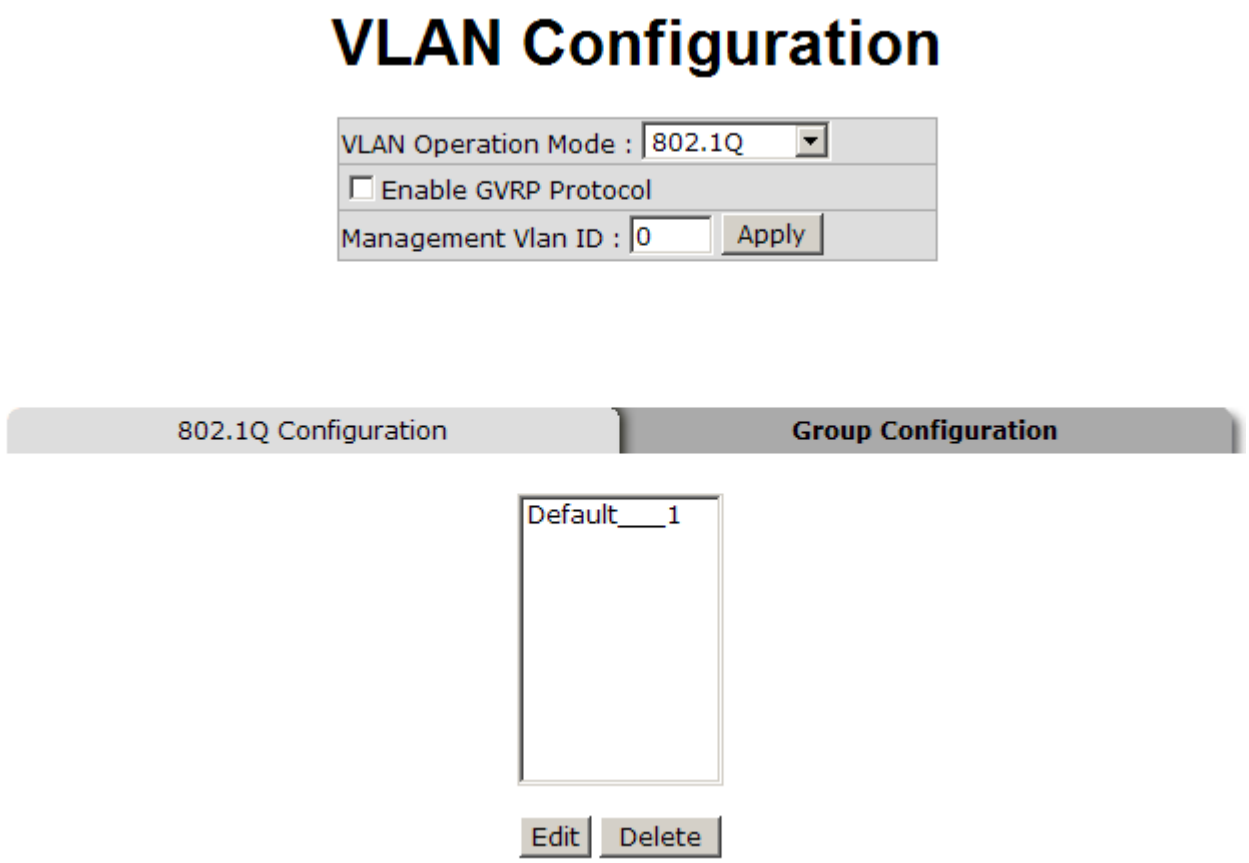
802.1Q Configuration

1. **Enable GVRP Protocol:** check the check box to enable GVRP protocol.
2. Select the port that wants to configure.
3. **Link Type**: there are 3 types of link type.
   - **Access Link:** single switch only, allow user to group ports by setting the same VID.
   - **Trunk Link:** extended application of **Access Link**, allow user to group ports by setting the same VID with 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. Click Apply
7. You can see each port setting in the below table on the screen.

Group Configuration

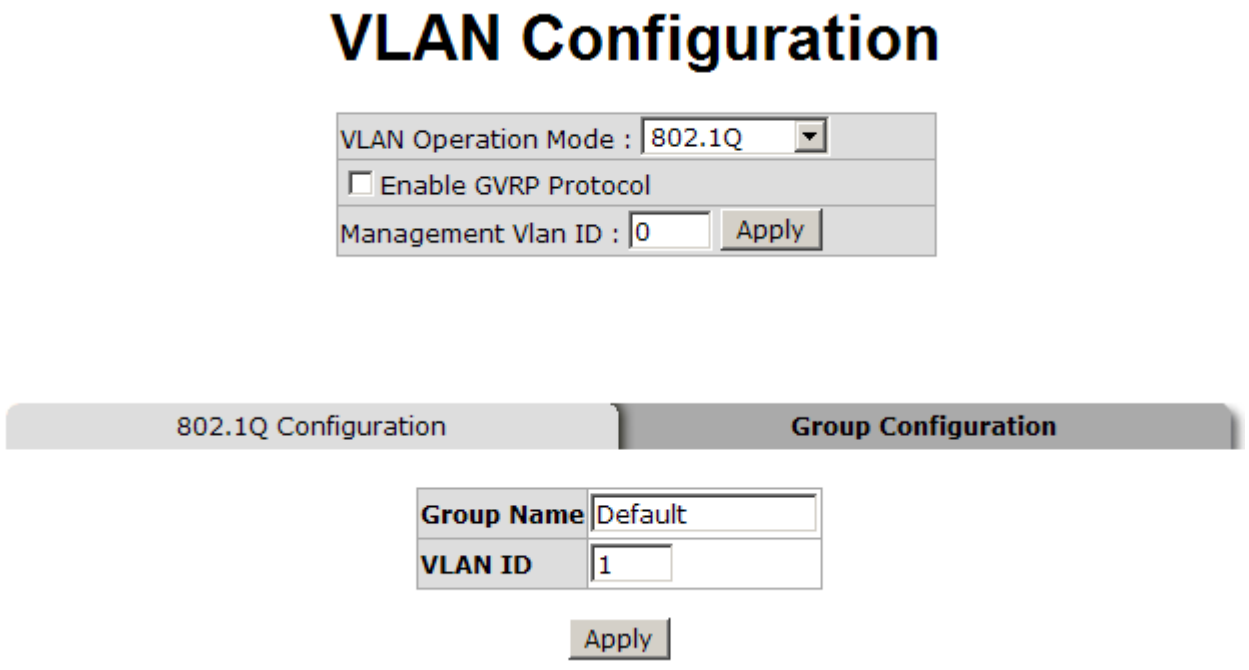
Edit the existing VLAN Group.

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



Group Configuration interface

3. You can Change the VLAN group name and VLAN ID.
4. Click Apply.



Group Configuration interface

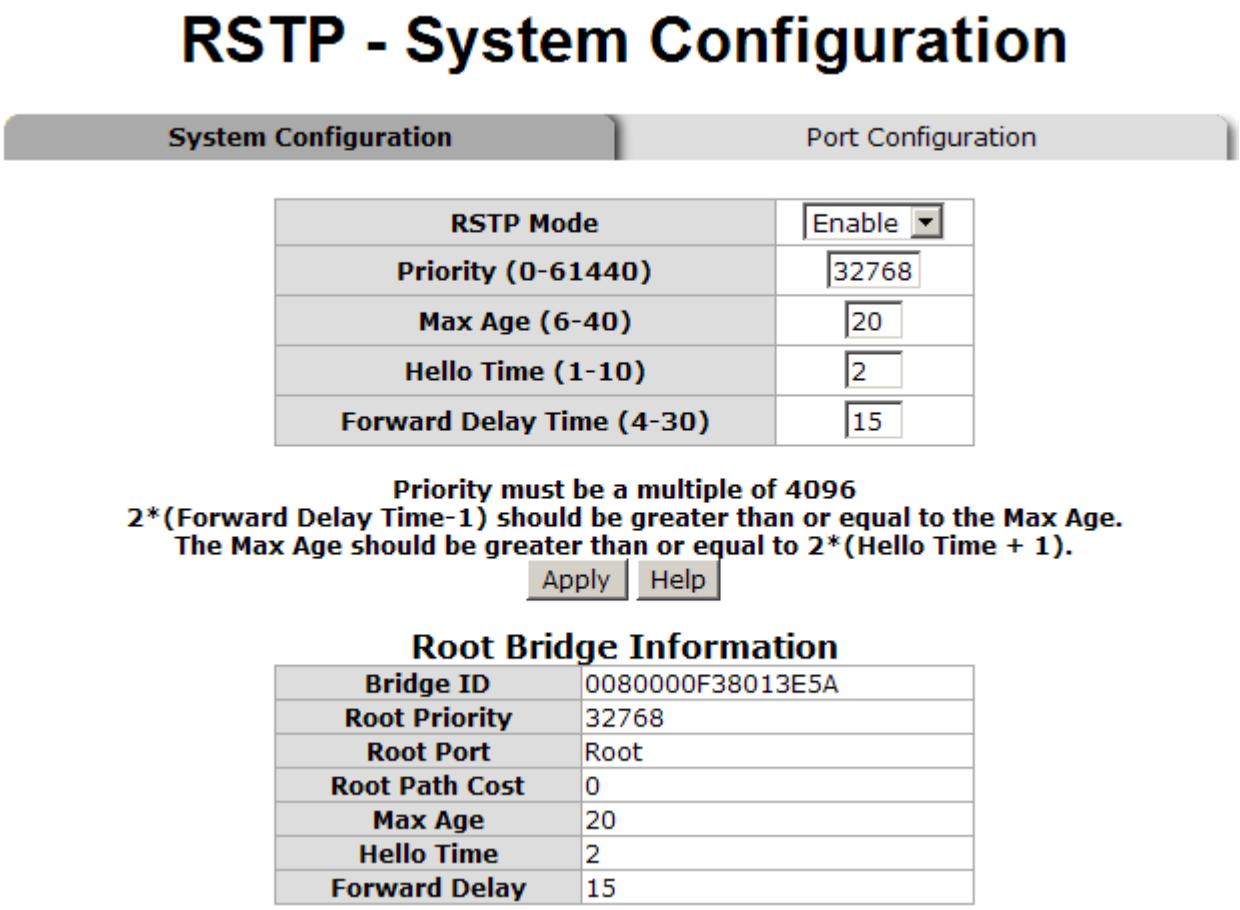
Rapid Spanning Tree

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

RSTP - System Configuration

- User can view spanning tree information about the Root Bridge
- User can modify RSTP state. After modification, click Apply button
  - **RSTP mode:** user must enable or disable RSTP function before configure 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, 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 Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40
  - **Hello Time (1-10):** the time that controls switch 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 System Configuration interface

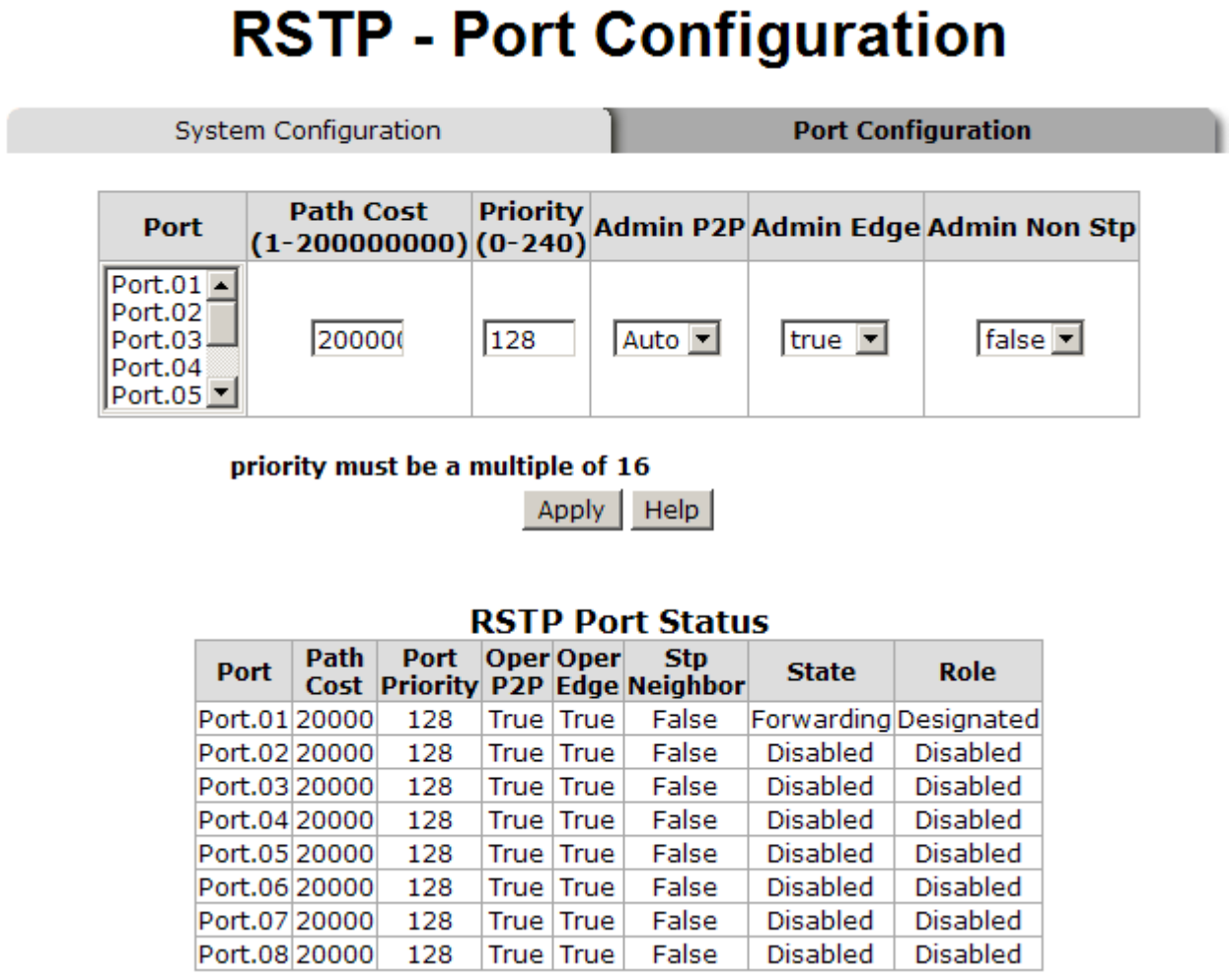
RSTP - Port Configuration

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 end stations cannot create 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. Click Apply.



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

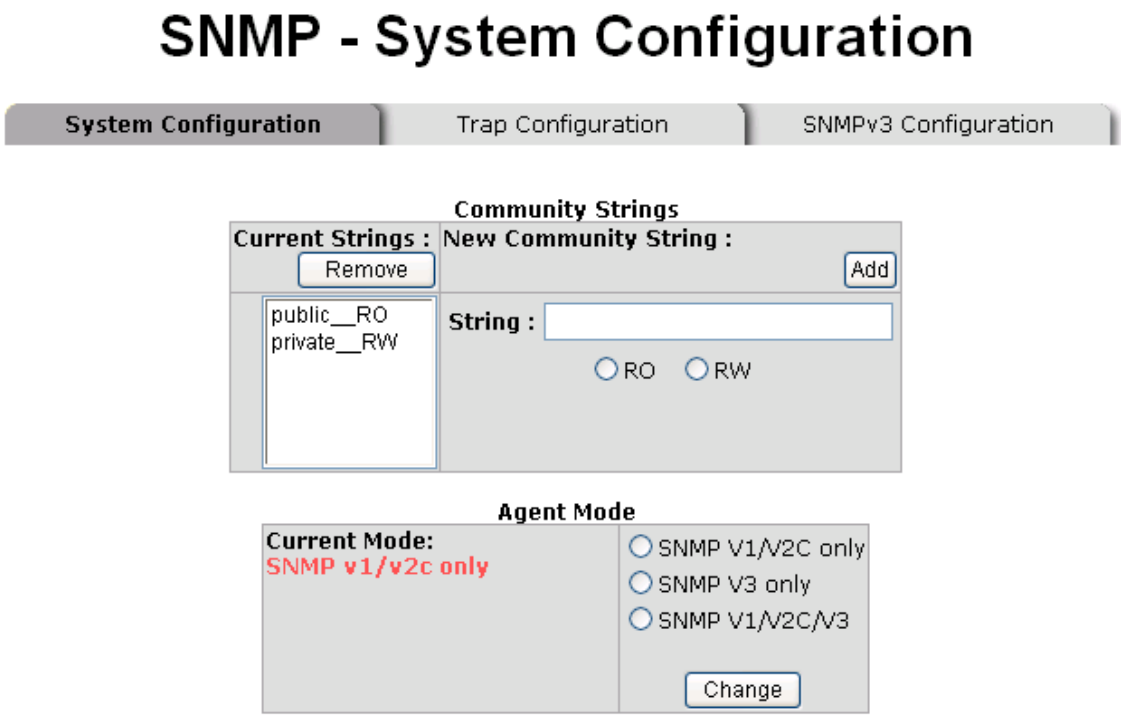
- **Community Strings**

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

1. **String:** fill the name of 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. Click Add.
2. To remove the community string, select the community string that you have defined and click 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 click Change to switch to the selected SNMP version mode.

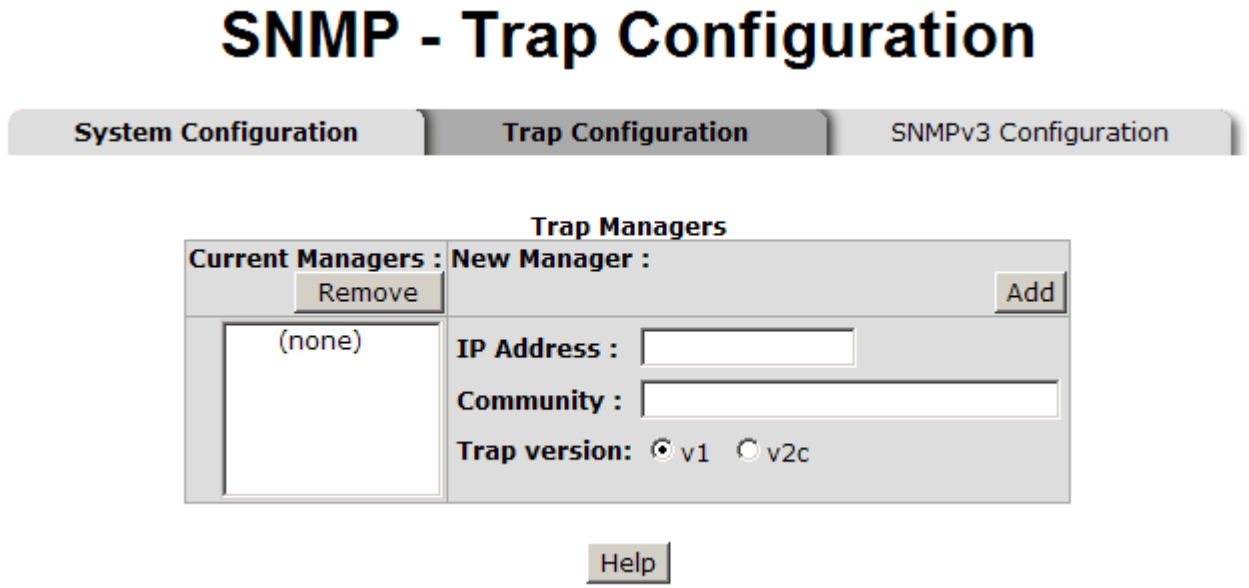


SNMP System Configuration interface

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 issue. Create a trap manager by entering the IP address of the station and a community string. To define management stations as trap manager and enter SNMP community strings and selects the SNMP version.

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



Trap Managers interface

SNMPV3 Configuration

Configure the SNMP V3 function.

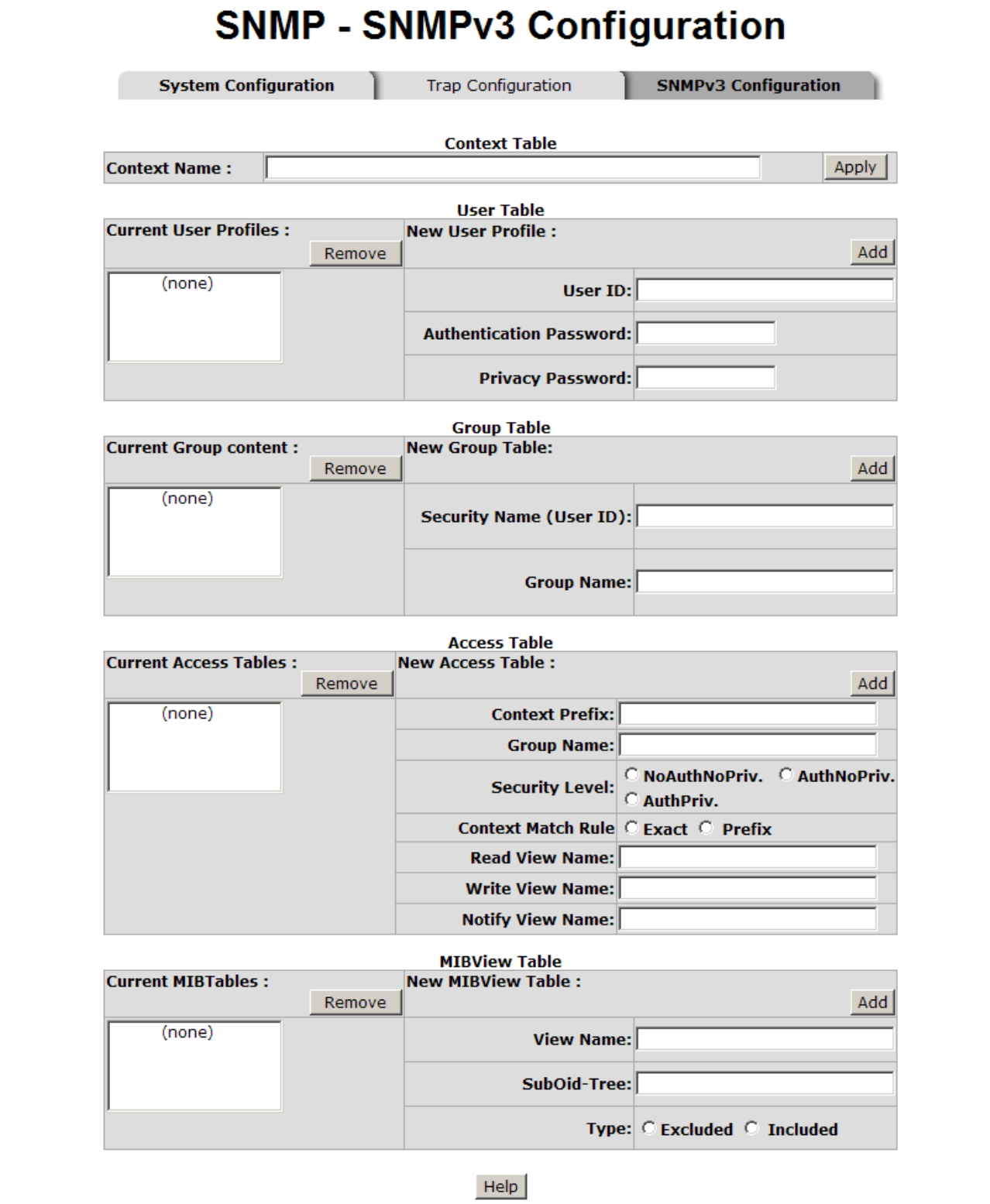
Context Table

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



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.
- Click Add to add context name.
- Click 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.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

MIBview Table

Configure MIB view table.

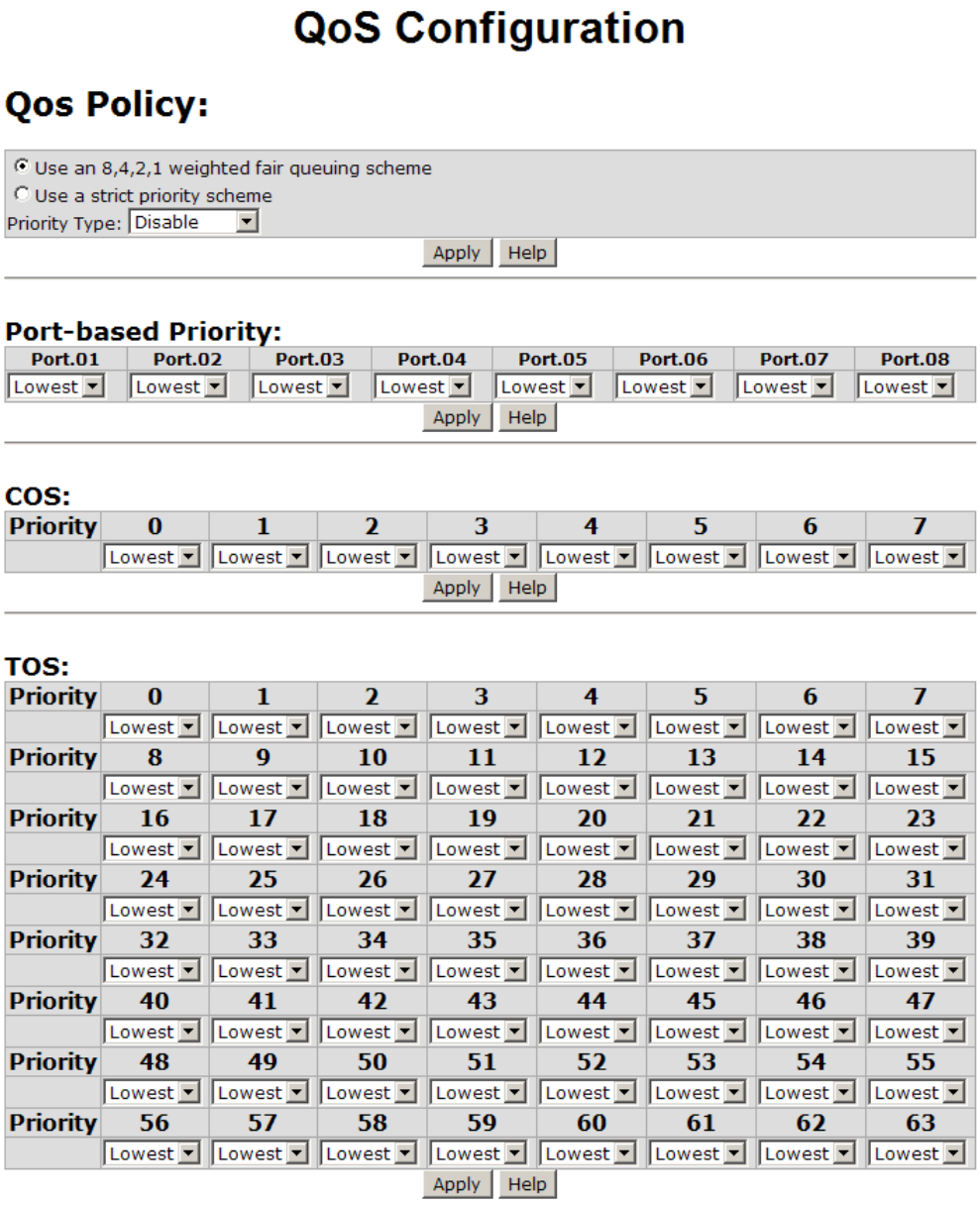
- **ViewName:** Set up the name.
- **Sub-Oid Tree:** Fill the Sub OID.
- **Type:** Select the type – exclude or included.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

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 High 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:** Always higher queue will be processed first, except higher queue is empty.
- **Priority Type:** there are 5 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.
- Click Apply.



QoS Configuration interface

Port Base Priority

Configure per port priority level.

- **Port:** each port has 4 priority levels – High, Middle, Low, and Lowest.
- Click Apply.

COS Configuration

Set up the COS priority level.

- **COS priority:** Set up the COS priority level 0~7 –High, Middle, Low, Lowest.
- Click Apply.

TOS Configuration

Set up the TOS priority.

- **TOS priority:** the system provides 0~63 TOS priority level. Each level has 4 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 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.
- Click Apply.

IGMP Configuration

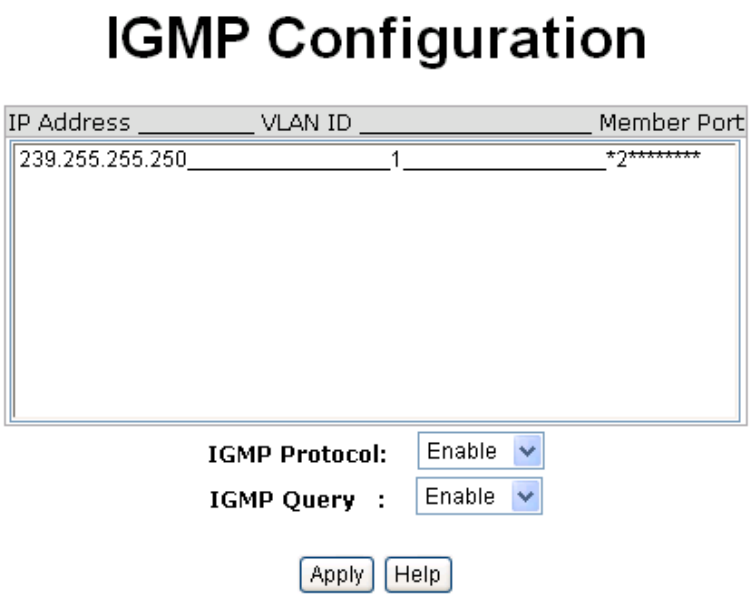
The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through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

Message	Description

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

The switch 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.
- Click Apply.



IGMP Configuration interface

Xtreme Ring

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

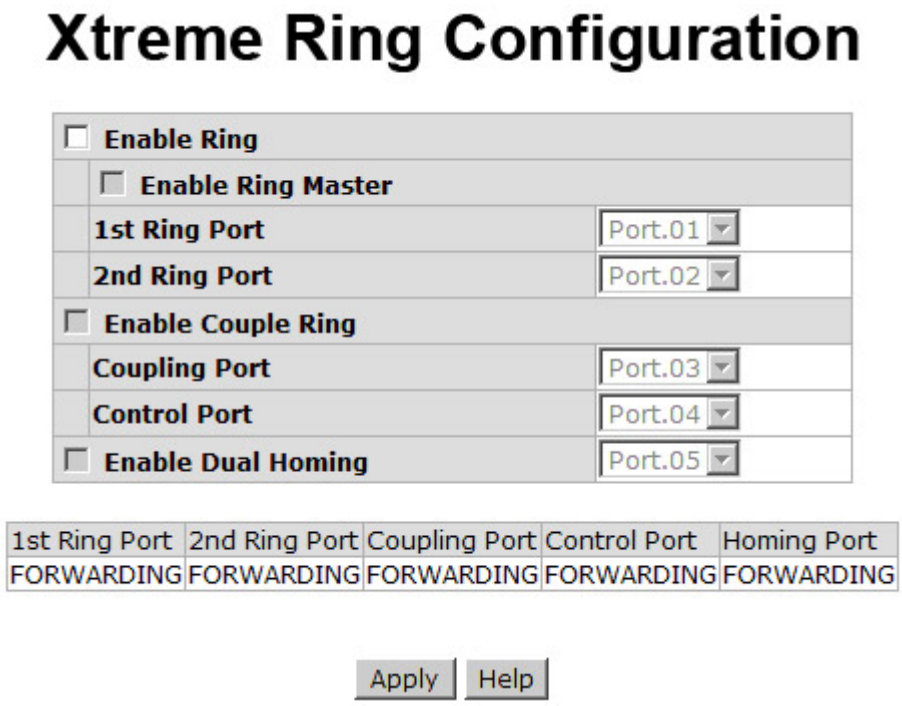
In the Xtreme Ring topology, every switch should enable Xtreme Ring function and assign two member ports in the ring. Only one switch in the Xtreme Ring group would be set as a master switch that would be blocked, called backup port, and another port is called working port. Other switches in the Xtreme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

The switch supports the function and interface for setting the switch as the ring master or slave mode. The ring master can negotiate and place command to other switches in the Xtreme 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 Xtreme Ring master ring mode will be enabled by the Xtreme 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 Xtreme Ring group for the redundant backup function and dual homing function that prevent connection lose between Xtreme Ring group and upper level/core switch.

- **Enable Xtreme Ring:** To enable the Xtreme Ring function. Marking the check box to enable the Xtreme Ring function.
- **Enable Ring Master:** Mark the check box for enabling this machine to be 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 upgrade the **2nd Ring Port** to be the working port.

- **Enable Coupling Ring:** To enable the coupling ring function. Marking the check box to enable 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 Xtreme Ring group, maximum Dual Homing port is one. Dual Homing only work when the Xtreme Ring function enable.
- And then, click Apply to apply the configuration.



Xtreme Ring Interface

Note

1. *When Xtreme Ring function is enabled, user must disable the RSTP first. Xtreme Ring and RSTP function cannot exist at the same time.*
2. *Remember to execute the 'Save Configuration' action, otherwise the new configuration will lose when switch powers off.*

Security

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

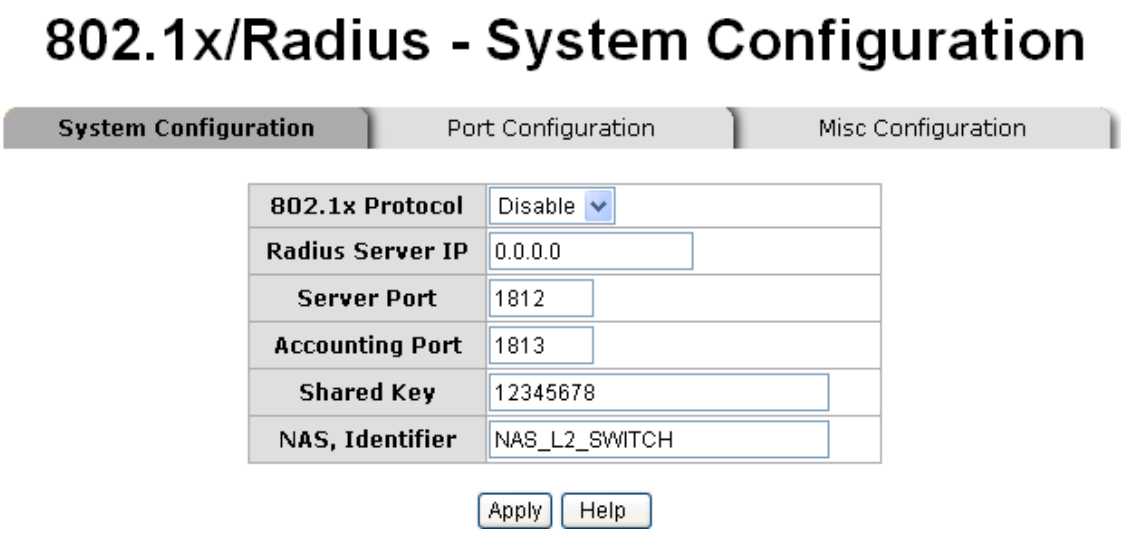
802.1X/Radius Configuration

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 using 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. Click Apply.

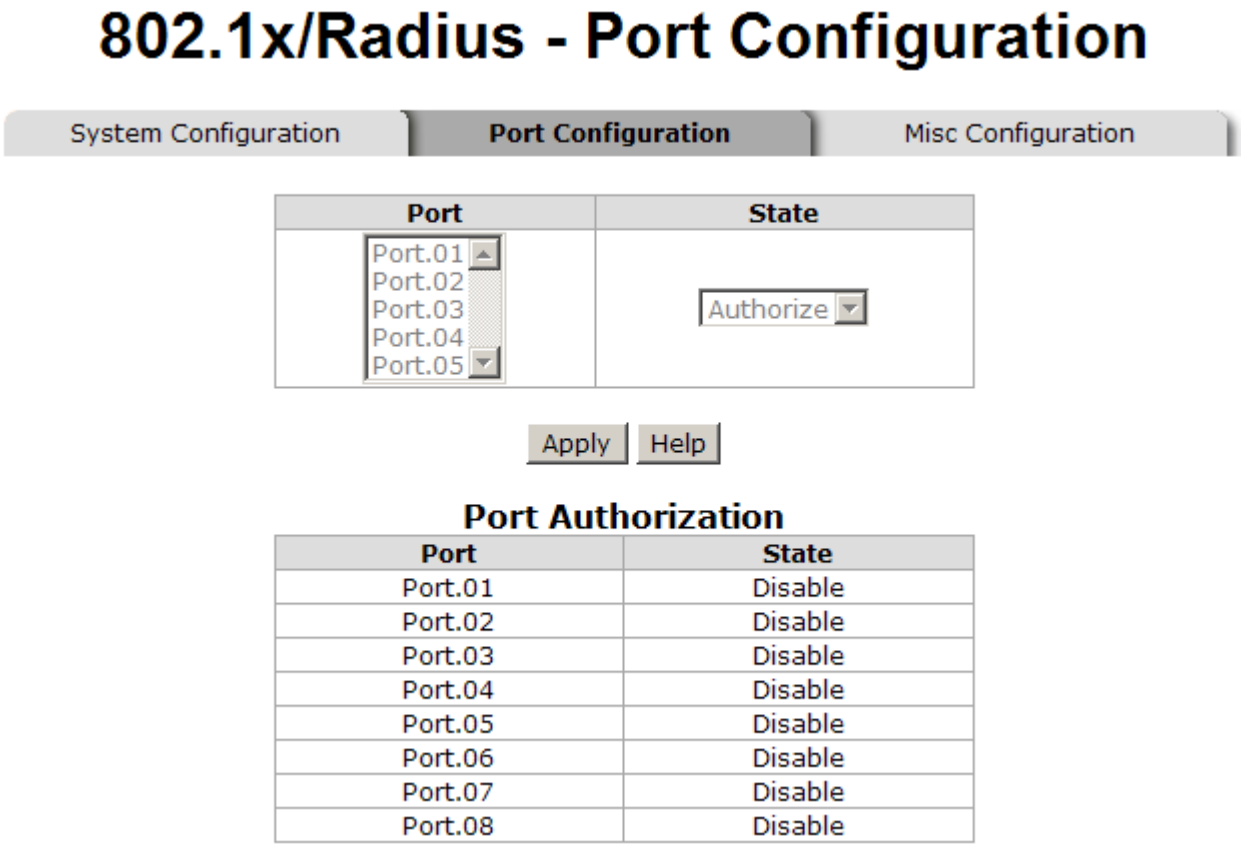


802.1x System Configuration interface

802.1x Per Port Configuration

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

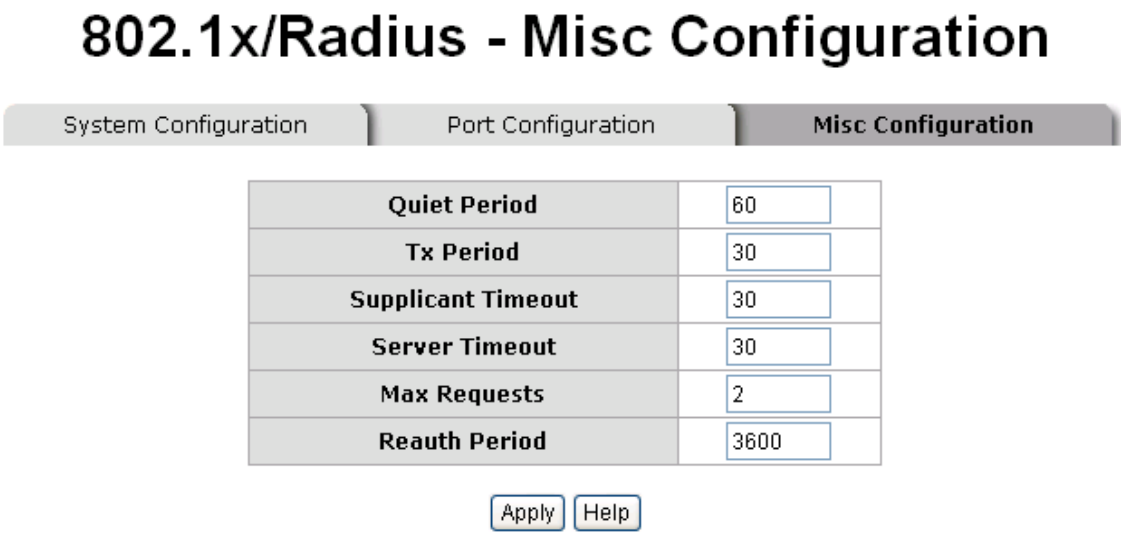
- **Reject:** the specified port is required to be held in the unauthorized state.
- **Accept:** the specified port is required to be held in the Authorized state.
- **Authorized:** the specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange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



802.1x Per Port Setting interface

Misc 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. **Max Requests:** set the number of authentication that must time-out before authentication fails and the authentication session ends.
6. **Reauth period:** set the period of time after which clients connected must be re-authenticated.
7. Click Apply.



802.1x Misc Configuration interface

MAC Address Table

Use the MAC address table to ensure the port security.

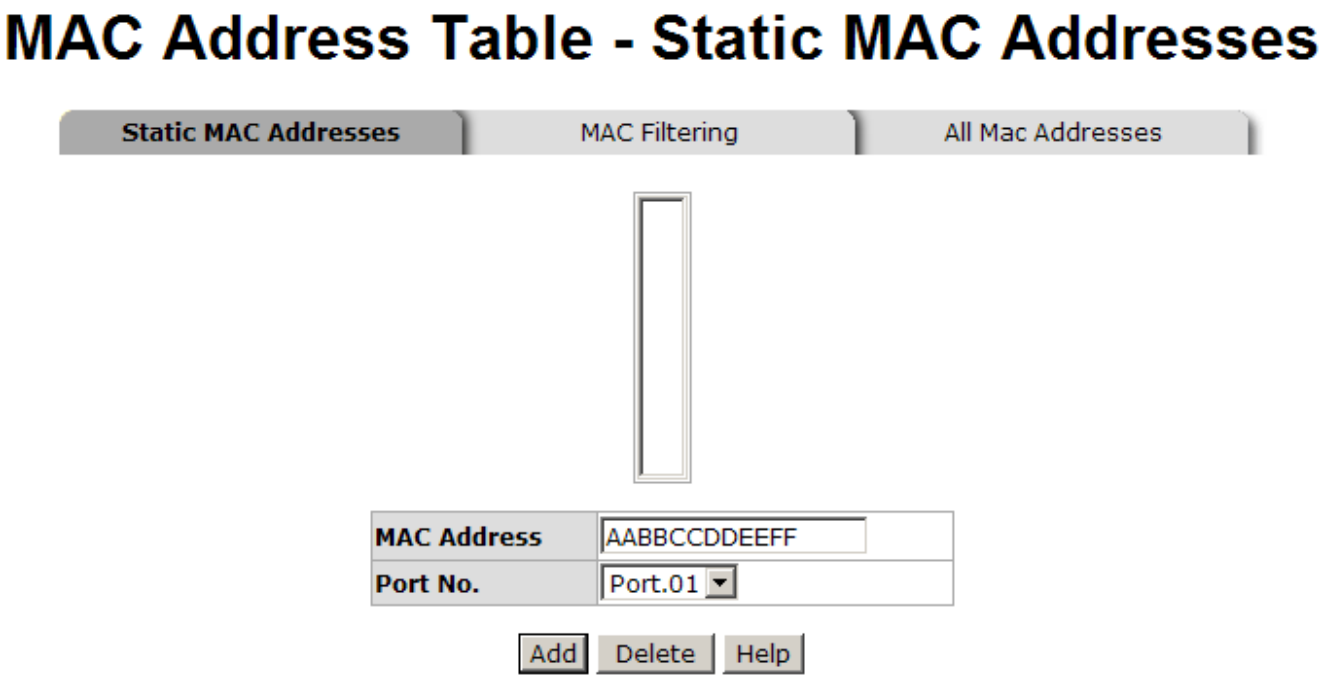
Static MAC Address

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 switch MAC table.

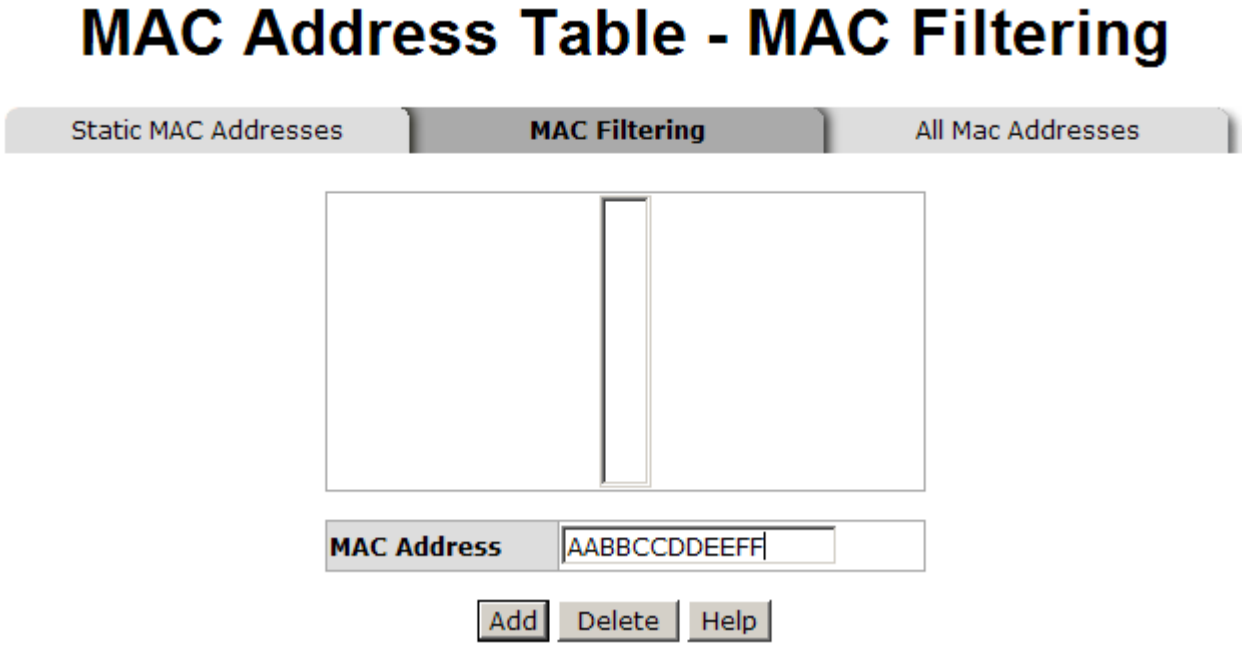
1. **MAC Address:** Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.
2. **Port No.:** pull down the selection menu to select the port number.
3. Click Add.
4. If you want to delete the MAC address from filtering table, select the MAC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



Static MAC Addresses interface

MAC Filtering

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



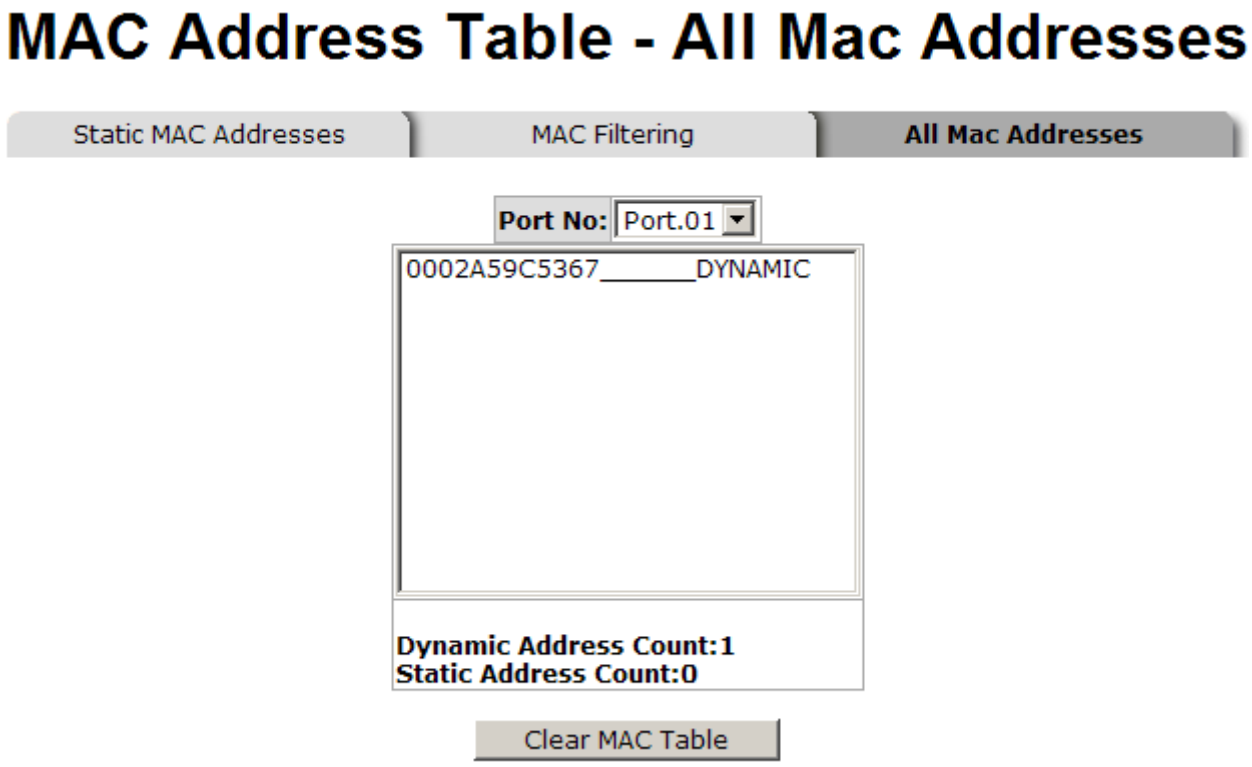
MAC Filtering interface

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

All MAC Addresses

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

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



All MAC Address interface

Factory Default

Reset switch to default configuration. Click Reset to reset all configurations to the default value.



Factory Default interface

Save Configuration

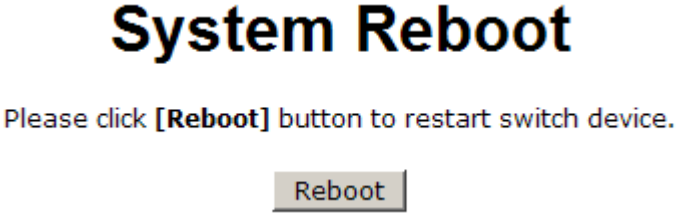
Save all configurations that you have made in the system. To ensure the all configuration will be saved. Click Save to save the all configuration to the flash memory.



Save Configuration interface

System Reboot

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



System Reboot interface

Troubles shooting

- Verify that you are using the right power cord/adapter (DC 12 ~ 48V), please don't use the power adapter with DC output higher than 48V, or it will burn this switch down.
- Select the proper UTP cable to construct your network. Please check that you are using the right cable. Use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ-45 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).
- **Diagnosing LED Indicators:** the Switch can be easily monitored through panel indicators, which describes common problems you may encounter and where you can find possible solutions, to assist in identifying problems.
- IF the power indicator does not light on when the power cord is plugged in, you may have a problem with power cord. Then check for loose power connections, power losses or surges at power outlet. IF you still cannot resolve the problem, contact your local dealer for assistance.
- If the Industrial Switch LED indicators are normal while the connected cables are correct, but the packets still cannot transmit. Please check your system's Ethernet devices' configuration or status.

Technical Specification

The technical specifications of 4 10/100/1000T + 4 SFP Industrial Switch are listed as follows.

Communications

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

Interface

Connectors	4 x RJ-45 (4-port 10/100/1000TX) 4 x 100/1000 SFP sockets 6-pin removable screw terminal (power & relay)
LED Indicators	Unit: System Power, Power1, Power2, Fault, 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	Xtreme Ring (Recovery time < 20ms at 30pcs full loading ring structure), 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	17.3 Watts
Power Input	2 x Unregulated +12 ~ 48 V_{DC}
Fault Output	1 Relay Output

Mechanism

Dimensions (WxDxH)	72 x 105 x 152 mm
Enclosure	IP-30, Metal shell with solid mounting kits
Mounting	DIN35 rail, Wall

Protection

ESD (Ethernet)	4,000 V_{DC}
Surge (EFT for power)	3,000 V_{DC}
Power Reverse	Yes
Overload current protection	Yes

Environment

Operating Temperature	-10 ~ 60 ℃
Operating Humidity	5% ~ 95% (non-condensing)
Storage Temperature	-40 ~ 85 ℃

Certifications

Safety	UL, cUL, CE EN60950-1
EMC	FCC Class A, 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 CE EN61000-4-11 CE EN61000-4-12 CE EN61000-6-2 CE EN61000-6-4
Free Fall	IEC60068-2-32
Shock	IEC60068-2-27
Vibration	IEC60068-2-6