antaira

8-port 10/100TX + 2-port 100FX IP-67

Managed Industrial Ethernet Switch

User Manual

antaira

www.antaira.com

Content

Overview

Introduction

To create the reliability in your network, the IP-67 Managed Industrial Switch comes equipped with a proprietary redundant network protocol—X-Ring II, which provides users with an easy way to establish a redundant Ethernet network with ultra high-speed recovery time less than 10ms. 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.

Apart from eight fast Ethernet ports, the 8 10/100TX + 2 100FX IP-67 Managed Industrial Switch also comes equipped with 2 waterproof fiber ports for both single and multi mode fiber optic cabling. The fiber slots can be used for the application of wideband uploading and long distance transmission to fit the field request flexibility.

Heavy Duty

Designed with circular M12 connectors for Fast Ethernet interface, the Managed Industrial Switch provides the rugged construction which complies with IP67 standards. Therefore, the equipment is especially intended for the damp, dusty, and vibrant environments.

Dual Power Inputs

The redundant power input design for the IP-67 Managed Industrial Switch gives a backup power solution. With both the power inputs supplied, and if either one fails the other one will be activated to keep the system operating continually. When one of the power inputs fails, the P-Fail LED indicator lights up and send an alarm through the relay output for notification purposes.

Flexible Mounting

The IP-67 Managed Industrial Switch is compact and can be mounted on the wall, so it is suitable for any space-constrained environment.

Wide Operating Temperature

The operating temperature of the IP-67 Managed Industrial Switch is between -40 and 75^{o}C. With such a wide range, you can use the IP-67 Managed Industrial Switch in some of the harshest industrial environments that exist.

Easy Troubleshooting

LED indicators make troubleshooting quick and easy. Each 10/100Base-TX port has an LED indicator displaying the link status. Also the indicators PWR1, PWR2 and P-Fail help you diagnose the system immediately.

Features – 8 10/100TX + 2 100FX

- 2Gbps back-plane (switching fabric)
- 2 x 100Base-FX waterproof LC-type single/multi mode fiber ports
- X-Ring II path redundant supported
- IPv6 supported
- Wide-range redundant power
- TFTP firmware update and system configuration restoration/backup
- Supports N-Key for configuration restoration/backup (optional)

Features – 8 10/100TX

- 1.6Gbps back-plane (switching fabric)
- X-Ring II path redundant supported
- IPv6 supported
- Wide-range redundant power
- TFTP firmware update and system configuration restoration/backup
- Supports N-Key for configuration restoration/backup (optional)

Technical Specifications – 8 10/100TX + 2 100FX

The technical specifications of 8 10/100TX + 2 100FX IP-67 Managed Industrial Switch are listed as follows.

Communications

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

Interface

Ethernet	8 x M12, 4-pole D-coded, female (10/100TX) 2 x 100 LC type socket with waterproof (100FX)
Console	1 x M12, 8-pole A-coded, female (RS-232)
Power Receptacle	1 x M12, 5-pole A-coded, male
Relay Alarm	1 x M12, 3-pole A-coded, female (1A @ 24 V_{DC})
LED Indicators	System: Power1, Power2, P-Fail, R-Master 10/100BaseTX port: Link/Active 100BaseFX port: Link/Active

Management

Configuration	Web browser, serial console, SNMP v1/v2c/v3, Telnet, TFTP, N-Key (optional), IPv6, SNTP
SNMP MIB	RFC 1215 Trap, RFC1213 MIBII, RFC 1157 SNMP MIB, RFC 1493 Bridge MIB, RFC 2674 VLAN MIB, RFC1643 , RFC 1757, RSTP MIB, LLDP MIB, Private MIB
VLAN	Port-based VLAN, IEEE 802.1Q tagged and double-tagged VLAN, GVRP
Redundancy	802.1w/d RSTP/STP X-Ring II (Recovery time < 10ms)
Security	SSL, SSH, DHCP Server with Port-IP binding, IP access security, user authentication, multi-user login , 802.1X port access control

Traffic Control	Port trunking with LACP, rate limit and storm control, IGMP Snooping/Query for multicast group, multicast filtering, IEEE 802.3x flow control, IEEE 802.1p QoS
Diagnostics	Port mirroring, real-time traffic statistics, MAC address table, system event log, E-mail alert, SNMP trap, RMON, LLDP/LLDP-MED

Power

Power Consumption	8.1 watts max. @ 48 V_{DC}
Power Input	2 x unregulated +12 ~ 48 V_{DC}

Mechanism

Dimensions (WxHxD)	193 x 176 x 62.5 mm
Enclosure	IP-67 protection, aluminum shell
Installation	Wall-mount

Environment

Operating Temperature	-40 ~ 75^{o}C
Operating Humidity	5% ~ 95% (non-condensing)
Storage Temperature	-40 ~ 85^{o}C
Storage Humidity	5% ~ 95% (non-condensing)
MTBF	320420 hrs

Certifications

Safety	UL 508; (suitable for use in Class I, Division 2, Groups A, B, C, and D locations)
Railway	EN50155 compliant
EMC	CE, FCC Class A CE EN61000-6-2 CE EN61000-6-4 CE EN61000-4-2 (ESD) CE EN61000-4-3 (RS)

	CE EN61000-4-4 (EFT)
	CE EN61000-4-5 (Surge)
	CE EN61000-4-6 (CS)
	CE EN61000-4-8 (Magnetic Field)
Free Fall	IEC60068-2-32
Shock	IEC61373
Vibration	IEC61373

Technical Specifications – 8 10/100TX

The technical specifications of 8 10/100TX IP-67 Managed Industrial Switch are listed as follows.

Communications

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

Interface

Ethernet	8 x M12, 4-pole D-coded, female (10/100TX)
Console	1 x M12, 8-pole A-coded, female (RS-232)
Power Receptacle	1 x M12, 5-pole A-coded, male
Relay Alarm	1 x M12, 3-pole A-coded, female (1A @ 24 V_{DC})
LED Indicators	System: Power1, Power2, P-Fail, R-Master 10/100BaseTX port: Link/Active

Management

Configuration	Web browser, serial console, SNMP v1/v2c/v3, Telnet, TFTP, N-Key (optional), IPv6, SNTP
SNMP MIB	RFC 1215 Trap, RFC1213 MIBII, RFC 1157 SNMP MIB, RFC 1493 Bridge MIB, RFC 2674 VLAN MIB, RFC1643 , RFC 1757, RSTP MIB, LLDP MIB, Private MIB
VLAN	Port-based VLAN, IEEE 802.1Q tagged and double-tagged VLAN, GVRP
Redundancy	802.1w/d RSTP/STP X-Ring II (Recovery time < 10ms)
Security	SSL, SSH, DHCP Server with Port-IP binding, IP access security, user authentication, multi-user login , 802.1X port access control
Traffic Control	Port trunking with LACP, rate limit and storm control,

	IGMP Snooping/Query for multicast group, multicast filtering, IEEE 802.3x flow control, IEEE 802.1p QoS
Diagnostics	Port mirroring, real-time traffic statistics, MAC address table, system event log, E-mail alert, SNMP trap, RMON, LLDP/LLDP-MED

Power

Power Consumption	4.8 watts max. @ 48 V_{DC}
Power Input	2 x unregulated +12 ~ 48 V_{DC}

Mechanism

Dimensions (WxHxD)	193 x 176 x 62.5 mm
Enclosure	IP-67 protection, aluminum shell
Installation	Wall-mount

Environment

Operating Temperature	-40 ~ 75^{o}C
Operating Humidity	5% ~ 95% (non-condensing)
Storage Temperature	-40 ~ 85^{o}C
Storage Humidity	5% ~ 95% (non-condensing)
MTBF	388201 hrs

Certifications

Safety	UL 508; (suitable for use in Class I, Division 2, Groups A, B, C, and D locations)
Railway	EN50155 compliant
EMC	CE, FCC Class A CE EN61000-6-2 CE EN61000-6-4 CE EN61000-4-2 (ESD) CE EN61000-4-3 (RS) CE EN61000-4-4 (EFT)

	CE EN61000-4-5 (Surge)
	CE EN61000-4-6 (CS)
	CE EN61000-4-8 (Magnetic Field)
Free Fall	IEC60068-2-32
Shock	IEC61373
Vibration	IEC61373

Packing List

- 1 x IP-67 Managed Industrial Switch
- 1 x M12 to D-sub 9 female console cable
- 1 x User Manual (CD-ROM)

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

Safety Precaution

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

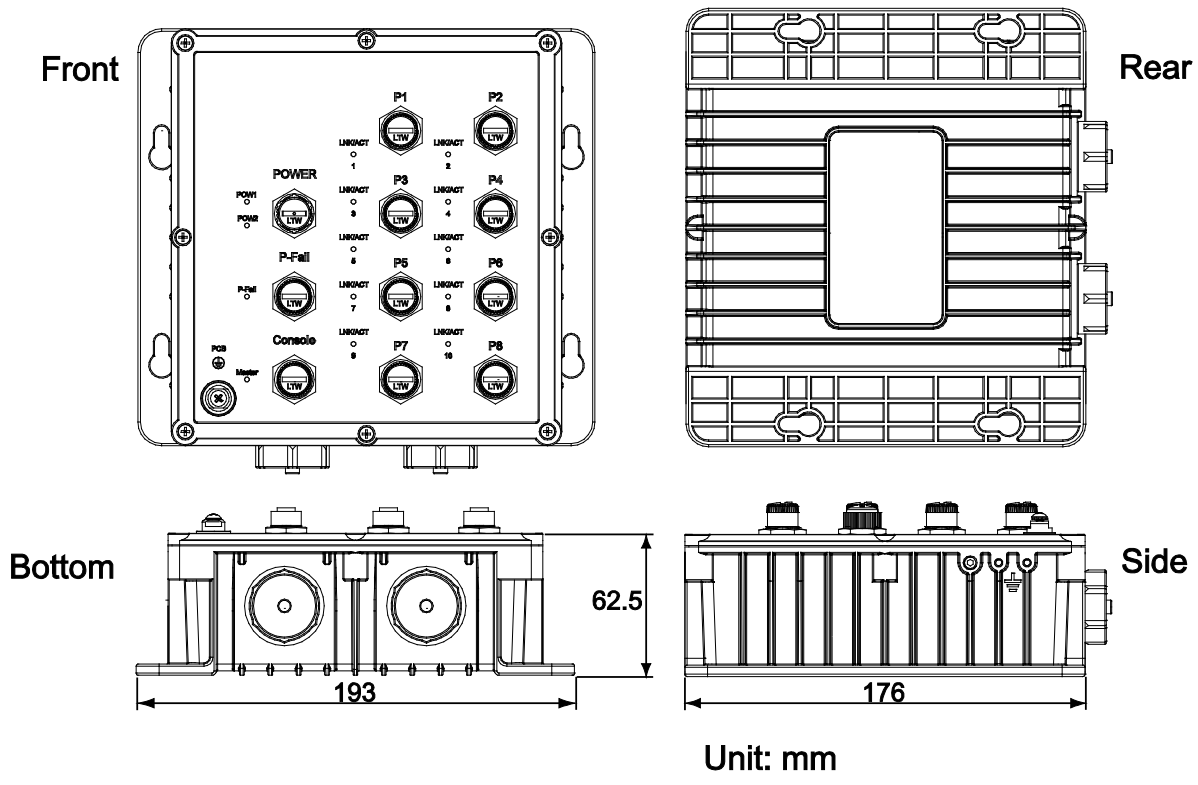
Hardware Description

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

Physical Dimensions

8 10/100TX + 2 100FX

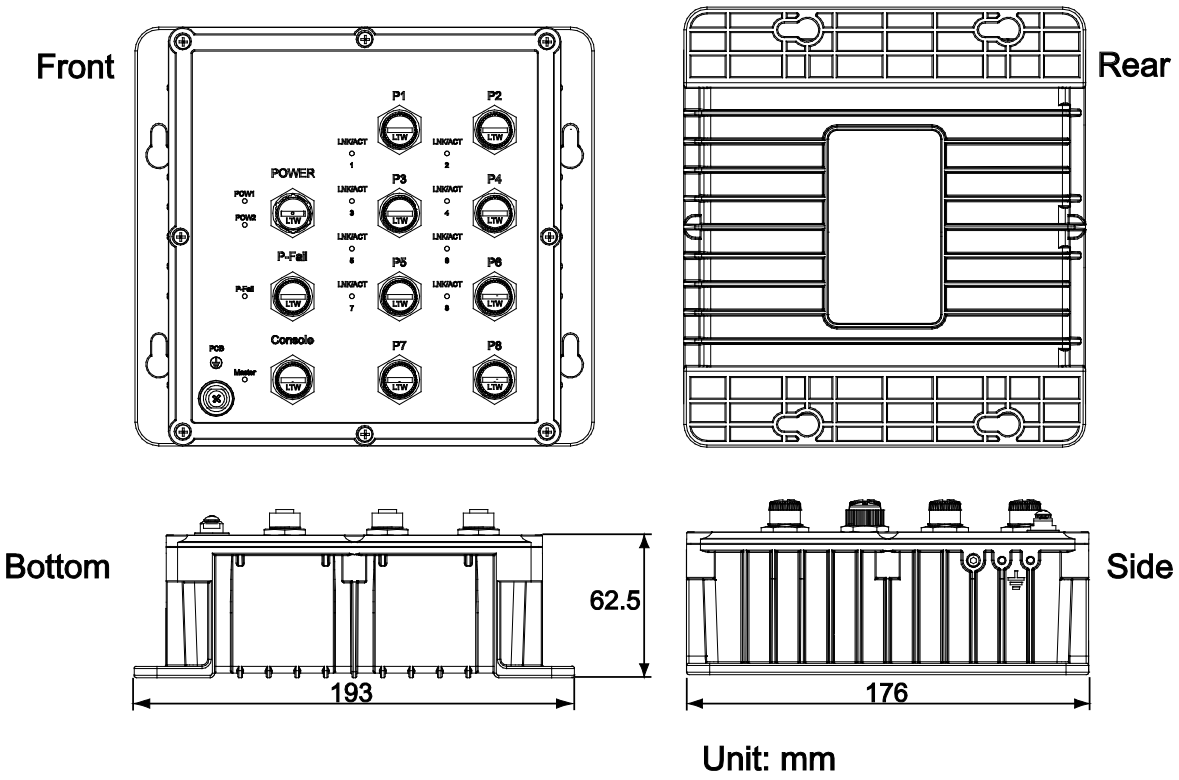
The figure below illustrates the dimensions 193mm x 176mm x 62.5mm (W x H x D) for the 8 10/100TX + 2 100FX IP-67 Managed Industrial Switch.



Mechanical Dimensions

8 10/100TX

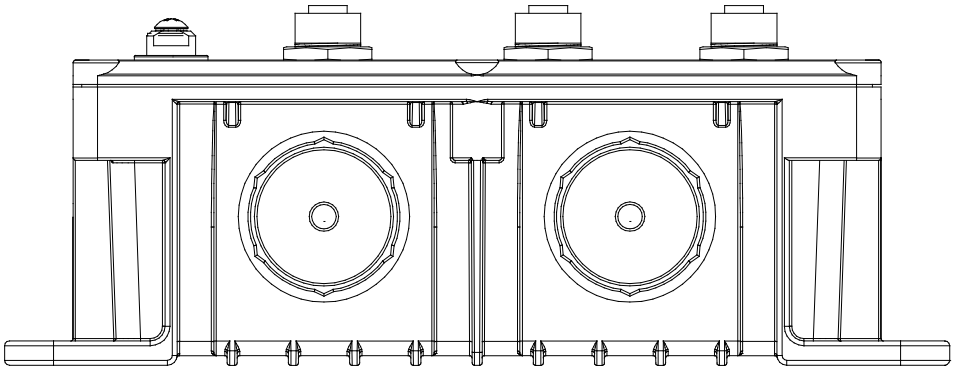
The figure below illustrates the dimensions 193mm x 176mm x 62.5mm (W x H x D) for the 8 10/100TX IP-67 Managed Industrial Switch.



Mechanical Dimensions

Bottom View

The 8 10/100TX + 2 100FX IP-67 Managed Industrial Switch, as the figure shown below, is equipped with two LC type fiber connectors located on the bottom.



The bottom side of the 8 10/100TX + 2 100FX IP-67 Managed Industrial Switch

LED Indicators

8 10/100TX + 2 100FX

LED indicators located on the front panel display the power status and network status of the **8 10/100TX + 2 100FX** IP67 Managed Industrial Switch. Please refer to the following table for further details.

LED	Color	Description	
PWR1	Green	On	Power input 1 is active
		Off	Power input 1 is inactive
PWR2	Green	On	Power input 2 is active
		Off	Power input 2 is inactive
P-Fail (depends on the **Fault Relay Alarm** configuration)	Red	On	Power or Ethernet port failure occurs
		Off	No failure occurs
R-Master	Green	On	The industrial switch is the master of the X-ring group
		Off	Non-master device
P9, P10	Green	On	LC fiber port is linking
		Blinks	Data is transmitting or receiving
		Off	Not connected to network
P1 ~ P8	Green	On	Connected to network
		Blinks	Data is transmitting or receiving
		Off	Not connected to network

Definition of LED indicators

8 10/100TX

LED indicators located on the front panel display the power status and network status of the **8 10/100TX** IP67 Managed Industrial Switch. Please refer to the following table for further details.

LED	Color	Description	
PWR1	Green	On	Power input 1 is active
		Off	Power input 1 is inactive
PWR2	Green	On	Power input 2 is active
		Off	Power input 2 is inactive
P-Fail (depends on the **Fault Relay Alarm** configuration)	Red	On	Power or Ethernet port failure occurs
		Off	No failure occurs
R-Master	Green	On	The industrial switch is the master of the X-ring group
		Off	Non-master device
P1 ~ P8	Green	On	Connected to network
		Blinking	Data is transmitting or receiving
		Off	Not connected to network

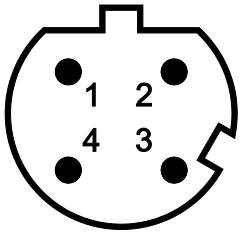
Definition of LED indicators

Installation

Fast Ethernet Ports

The M-12 D-coded Fast Ethernet ports are auto-sensing for 10Base-T or 100Base-TX devices connections. Auto MDI/MDIX means that you can connect to another switch or workstation without changing straight through or crossover cabling.

- **M12 D-coded Connector Pin Assignments**

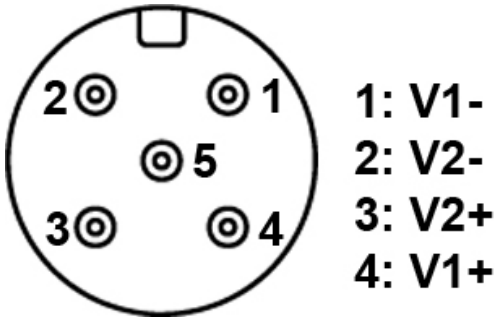


Pin Number	Assignments
1	Tx+
2	RX+
3	TX-
4	Rx-

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

Wiring the Power Inputs

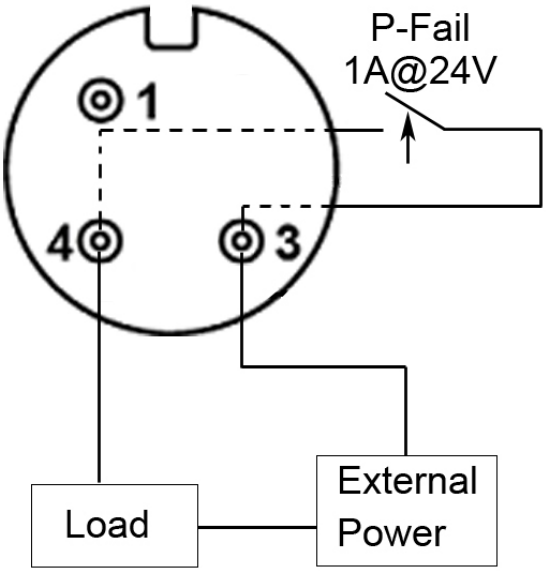
Connect the positive and negative wires to **PWR1 (V1+, V1-)** and **PWR2 (V2+, V2-)** as the power pin assignments shown below.



Power1 & Power2 Contacts of the M12 Connector

Wiring the P-Fail Alarm Contacts

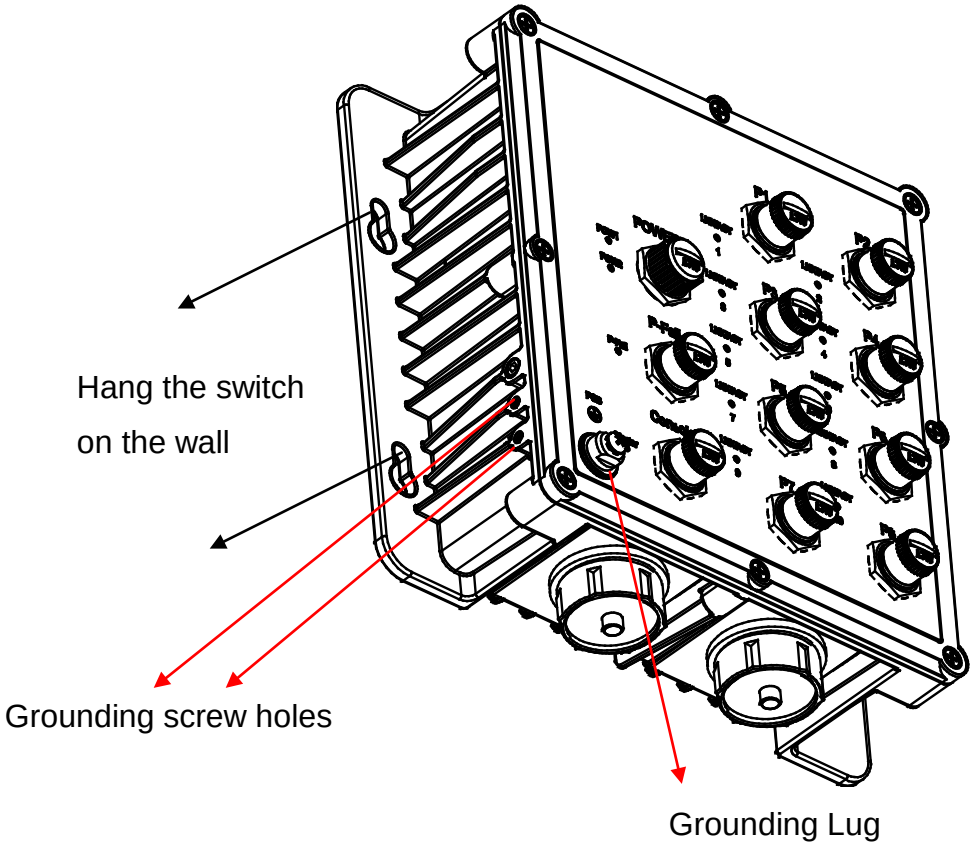
The “P-Fail” alarm relay is provided to signal critical error conditions that may occur on the switch. The contacts are energized upon powering up of the switch and remain energized until a critical error occurs including power failure, Ethernet port disconnection and MAC violation. Take the wiring illustration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



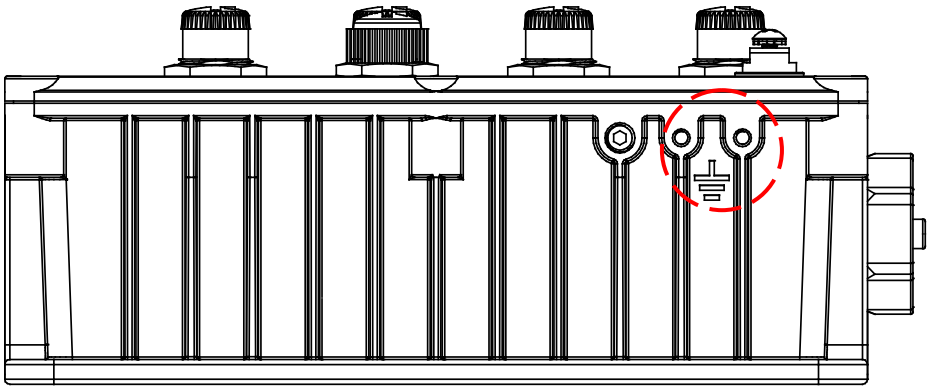
P-Fail Alarm Wiring

Wall Mounting

Besides desktop installation, the industrial switch is specially designed to hang on the wall for space-constrained environments. The drawing below illustrates the wall-mounting installation to hang the switch on the wall via the four mounting holes on the sides.



Grounding the Ethernet Switch



As the figure illustrated above, you can use an M3 screw to secure a grounding wire to the side screw holes near the ground mark or to the grounding lug at the corner of the front panel.

Note ***To earth the switch to ground with the grounding lug, please prepare an M8 wrench to hold the grounding contact from rotating when you are trying to tighten or release the fixing screw above the contact.***

Installation Steps

1. Unpack the Industrial switch
2. To hang the Industrial switch on the wall, please refer to the **Wall Mounting** section.
3. Use an M8 wrench to hold the grounding contact and remove the fixing screw above the contact.
4. Align the grounding lug with the contact; and still use the M8 wrench to hold the contact from rotating while you are tightening the fixing screw.
5. To power on the Industrial switch, please refer to the **Wiring the Power Inputs** section for further information on how to wire the power. And then the power LED on the Industrial switch will light up. Please refer to the **LED Indicators** section for indication of LED lights.
6. Prepare the M12 D-Code Fast Ethernet Port mating cable for Ethernet connection.
7. The Fast Ethernet port LED on the Industrial switch will light up when the cable is connected with the network device. Please refer to the **LED Indicators** section for LED light indication.
8. When all connections are set and LED lights all show in normal, the installation is complete.

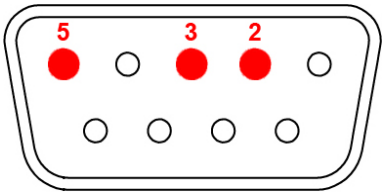
Note ***This equipment is intended for use in a Pollution Degree 2 industrial environment.***

Configuration

RS-232 Console

One end of the supplied console cable is D-sub 9 female connector and the other end is M12, 8-pole A-coded male connector. Attach the D-sub end to a PC or terminal and the of M12 end to the console port of the switch. The connected terminal or PC must support the terminal emulation program.

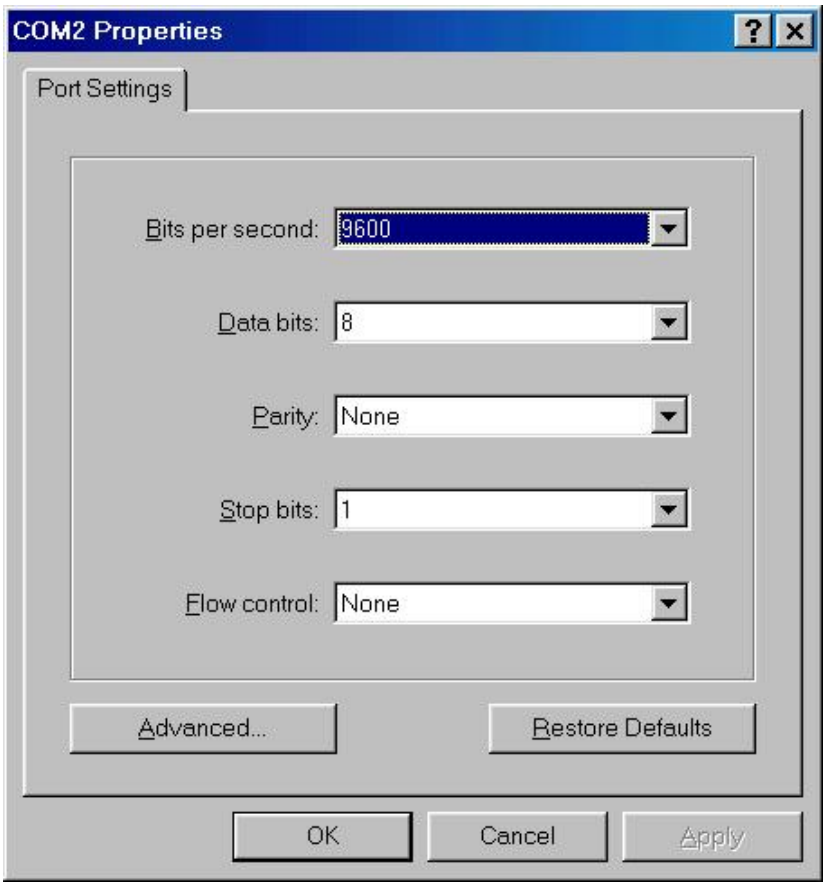
Pin Assignments

DB9 Connector Pin Assignments	D-sub 9 Connector (To PC)	M12 Connector (To Switch)	M12 Connector Pin Assignments
	Pin 2 TX	Pin 2 TX	
	Pin 3 RX	Pin 3 RX	
	Pin 5 GND	Pin 5 GND	

Login in the Console Interface

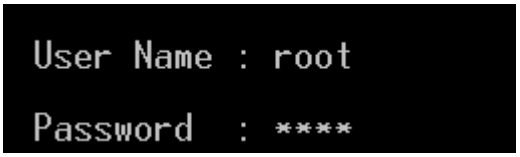
After the connection between Switch and PC is ready, turn on the PC and run a terminal emulation program like **Hyper Terminal** and configure its **communication parameters** to match the following default characteristics of the console port:

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



The settings of communication parameters

Having finished the parameter settings, click '**OK**'. When the blank screen shows up, press **Enter** to have the login prompt appear. Key in '**root**' (default value) for both User Name and Password (press **Enter** to switch between); and then press **Enter** to have the Main Menu of console management show up. Please see the figure below.



Console login interface

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

CLI command interface

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

SSH

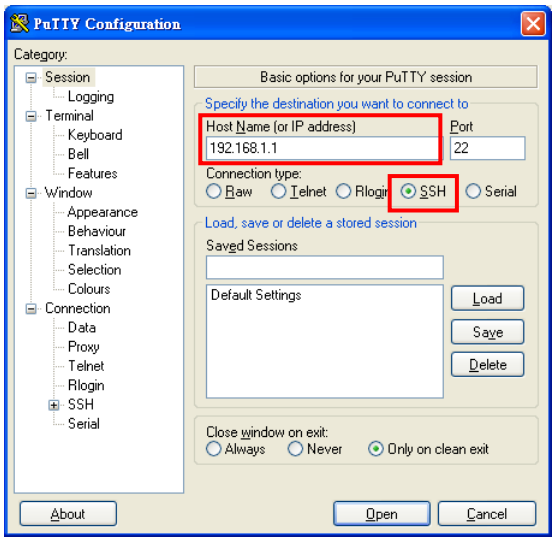
The Ethernet switch also supports SSH (Secure Shell) which allows the user to log in from a remote computer over the network.

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

Configuring PuTTY

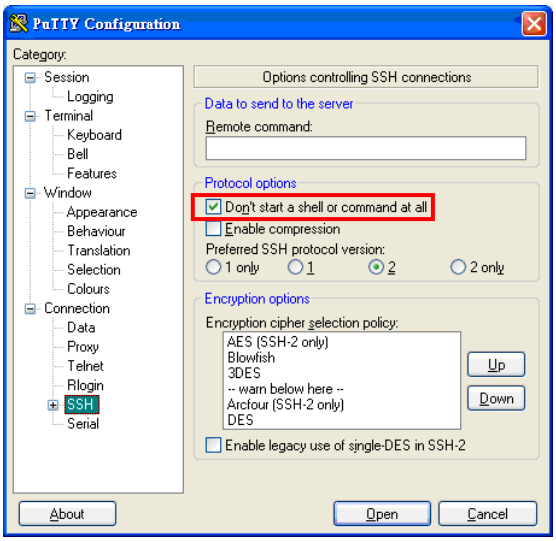
Launch **PuTTy**, and you will see a dialog box which allows you to control everything PuTTY can do. You don't usually need to change most of the configuration options. To start the simplest kind of session, please follow the steps below.

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



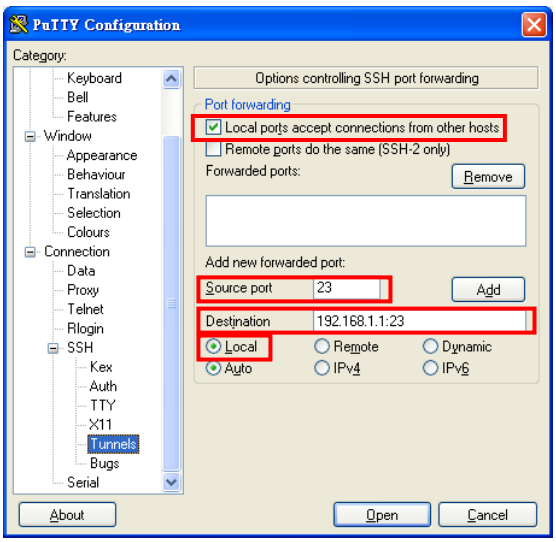
Basic Options for PuTTY

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



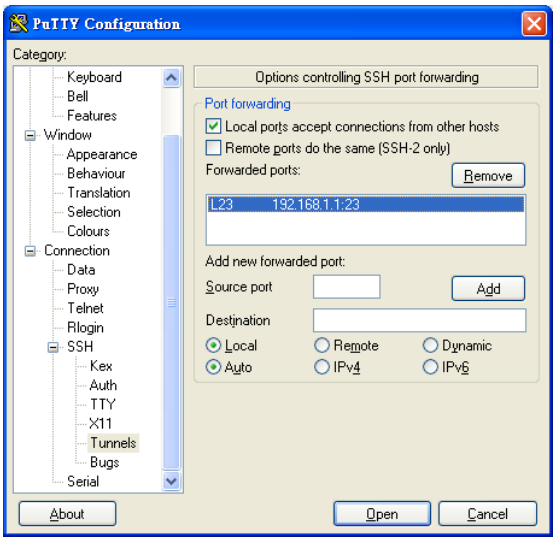
Options Controlling SSH Connections

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



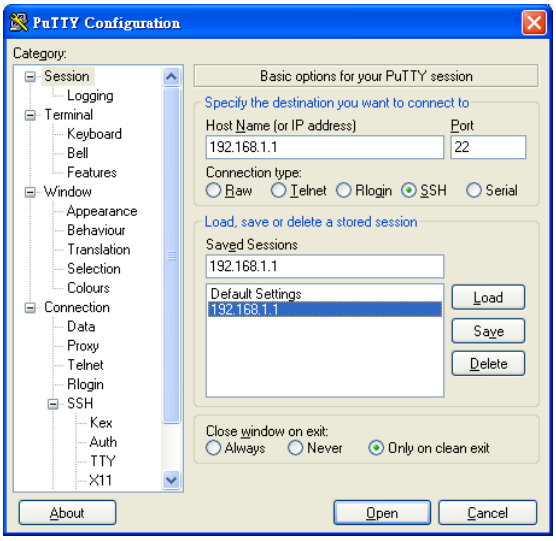
Options Controlling SSH Port Forwarding

8. After filling in, click the Add button. And you will see an entry added to the list box.



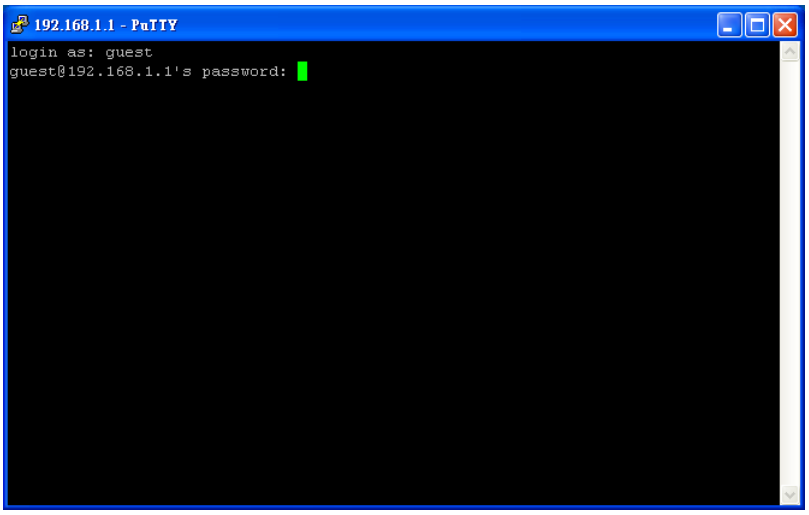
Entry of Port Forwarding Added

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



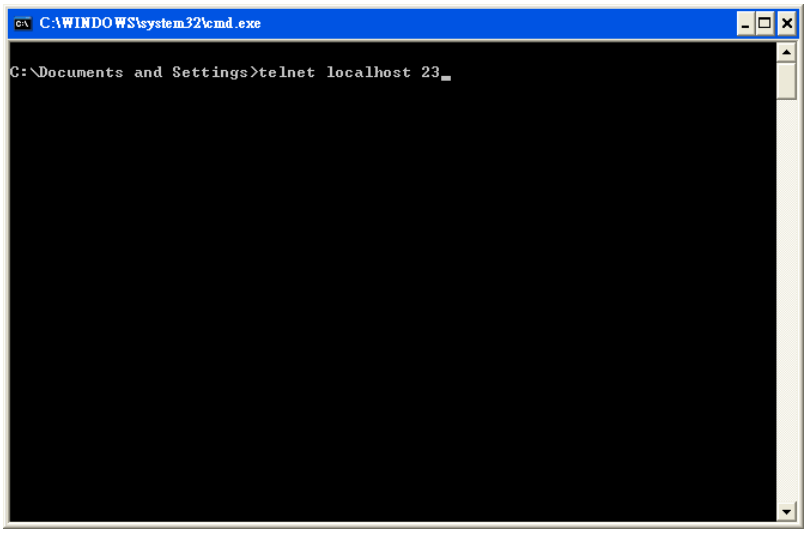
Saving Sessions

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



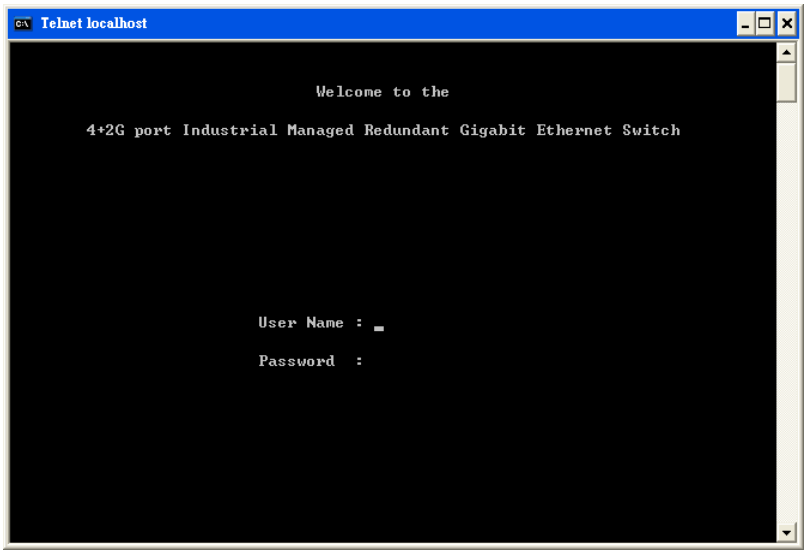
Logging-in interface

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



Command Prompt interface

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



Console via SSH

Web-Based Management

This industrial switch provides a convenient configuring way via web browser. You can follow the steps below to access the equipment.

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

Connect the industrial switch to the Ethernet then your host PC could be configured via Ethernet. Or you can directly connect it to your host PC with a straight-through or cross over Ethernet cable.

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

1. Launch the Internet Explorer on the PC.
2. Type the IP address of the switch in the URL field, and then Press "**Enter**".

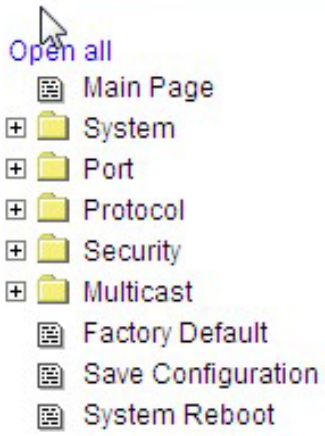
3. With the login dialog box showing up, type the user name and password in the respective fields. The default user name and password are the same as '**root**'.
4. Press **Enter** or click the **OK** button, and then the home screen of the Web-based management appears. You can change user name/password in the ***User Authentication*** section.

Login dialog box

SSL

The Ethernet switch also provides an option for you to connect with your browser via HTTP over SSL, called HTTPS. The SSL (Secure Socket Layer) protocol allows users to make a secured session between the browser (client) and the Ethernet switch (server). You can then type the prefix "***https://***" followed by the IP address of the Ethernet switch in the URL of the browser. Beside the URL a padlock icon shows up indicating that client is successfully connecting to server via HTTPS.

In the main page, you can find the tree menu structure of the Ethernet switch in the left side. Click the “+” symbol to unroll the hiding hyperlink, and click any one of the hyperlinks to open its function page.

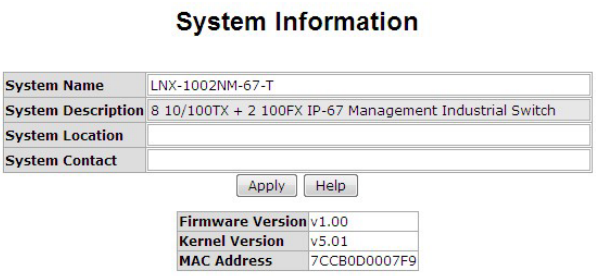


System Information

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

- **System Name:** Assign the name of the switch. The maximum length is 64 bytes.
- **System Description:** A read-only field displaying the description of the switch.
- **System Location:** Assign the switch physical location. The maximum length is 64 bytes.
- **System Contact:** Enter the name of contact person or department.
- **Firmware Version:** Displays the switch's firmware version.
- **Kernel Version:** Displays the kernel software version.
- **MAC Address:** Displays the unique hardware address assigned by manufacturer (default).
- Click Apply to have the configuration take effect.

[NOTE] Don't set "0" for the first segment of the subnet mask and default gateway (000.xxx.xxx.xxx).
Refresh the web screen if the web could not be displayed while you change the setting.



System Information interface

IP Configuration

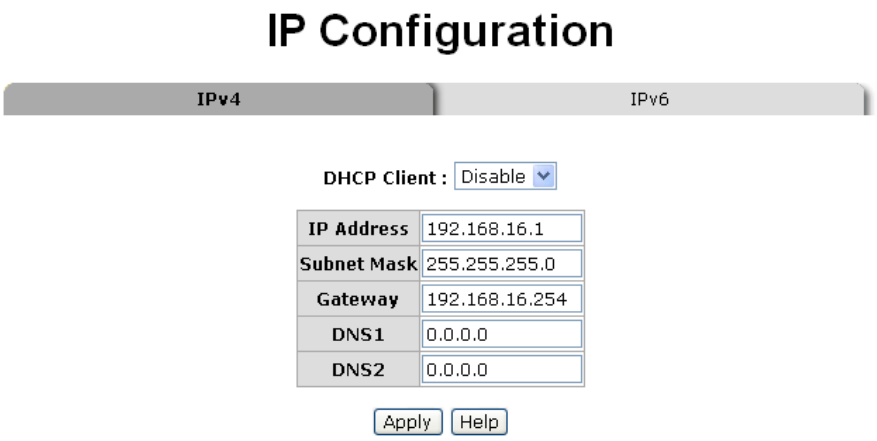
Due to the foreseeable address exhaustion of IPv4, the IP configuration of the Ethernet switch is designed to provide an interface for users to configure the switch running both IPv4 and IPv6 architecture.

IPv4

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

- **DHCP Client**: Enable or disable the DHCP client function. When the **DHCP Client** function is enabled, the industrial switch will be assigned an IP address from the network DHCP server. The default IP address will be replaced by the assigned IP address on DHCP server. After users click Apply, a popup dialog shows up. It is to inform the user that when the DHCP client is enabled, the current IP will lose and the user should find the new IP on the DHCP server
- **IP Address:** Assign the IP address for the industrial switch. With the **DHCP Client** function enabled, the switch is configured as a DHCP client and users doesn't need to assign the IP address that is assigned by the DHCP server. The default IP is 192.168.16.1 or the user has to assign an IP address manually when DHCP Client is disabled.
- **Subnet Mask:** Assign the subnet mask to the IP address. If the **DHCP Client** function is disabled, the user has to assign the subnet mask manually.
- **Gateway:** Assign the network gateway for the switch. If the **DHCP Client** function is disabled, the user has to assign the gateway manually. The default gateway is 192.168.16.254.
- **DNS1:** The abbreviation of Domain Name Server—an Internet service that translates domain names into IP addresses. The domain name is in alphabetic order, which is easy to be remembered. The Internet is based on IP address. Therefore, every time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.net.com might translate to 192.168.16.1.

- **DNS2:** The backup for DNS1. When DNS1 cannot function, DNS2 will then replace DNS1.
- When finished, click Apply to have the configuration take effect.



IP configuration—IPv4

IPv6

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

Global Unicast Address: A display-only field. When this Ethernet switch is connected to a network segment where one or more routers connected, the Ethernet switch will be assigned an address known as Global Unicast Address by the router(s). Being assigned the Global Unicast Address, the Ethernet switch can then have access to different network segments.

Link-Local Address: A display-only field. Link-Local Address is for use during auto-configuration and when no any router presents. Being assigned the Link-Local Address, the Ethernet switch can have access to all hosts on the same local segment to where it belongs.

IP configuration—IPv6

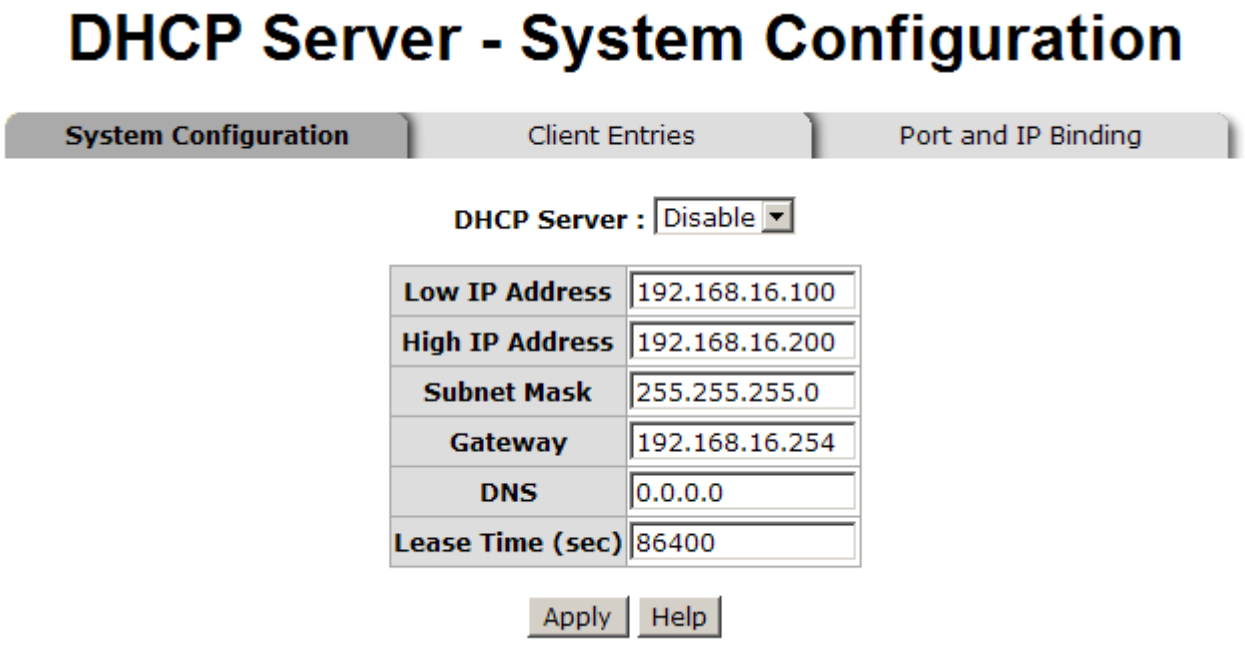
DHCP Server

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

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

System Configuration

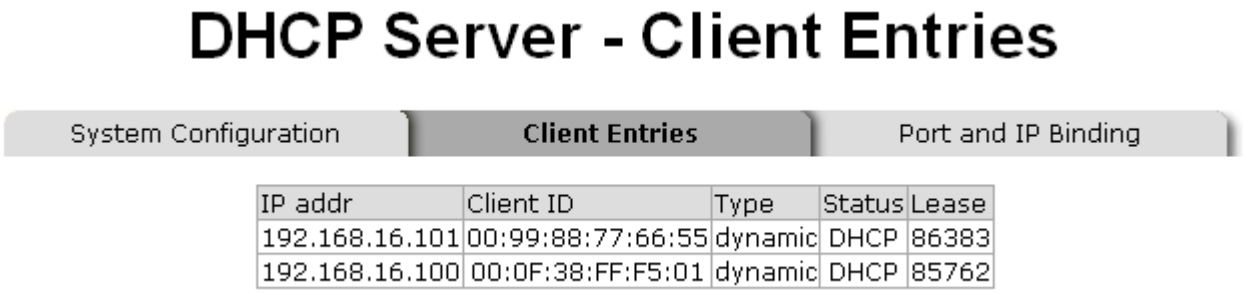
- **DHCP Server:** This pull-down menu allows you to configure the switch to be the DHCP server on your local network.
- **Low IP Address:** Type in an IP address as the beginning of a range of the dynamic IP address. As the figure shown below, for example, 192.168.16.100 is the relatively low IP address of the range.
- **High IP Address:** Type in an IP address as the beginning of a range of the dynamic IP address. As the figure shown below, for example, 192.168.16.200 is the relatively high IP address of the range.
- **Subnet Mask:** Type in the subnet mask of the IP configuration.
- **Gateway:** Type in the IP address of the gateway in your network.
- **DNS:** Type in the IP address of Domain Name Server in your network.
- **Lease Time (sec):** The length of time the dynamic IP addresses assigned to clients.
- Click Apply to have the configuration take effect.



DHCP Server—System Configuration interface

Client Entries

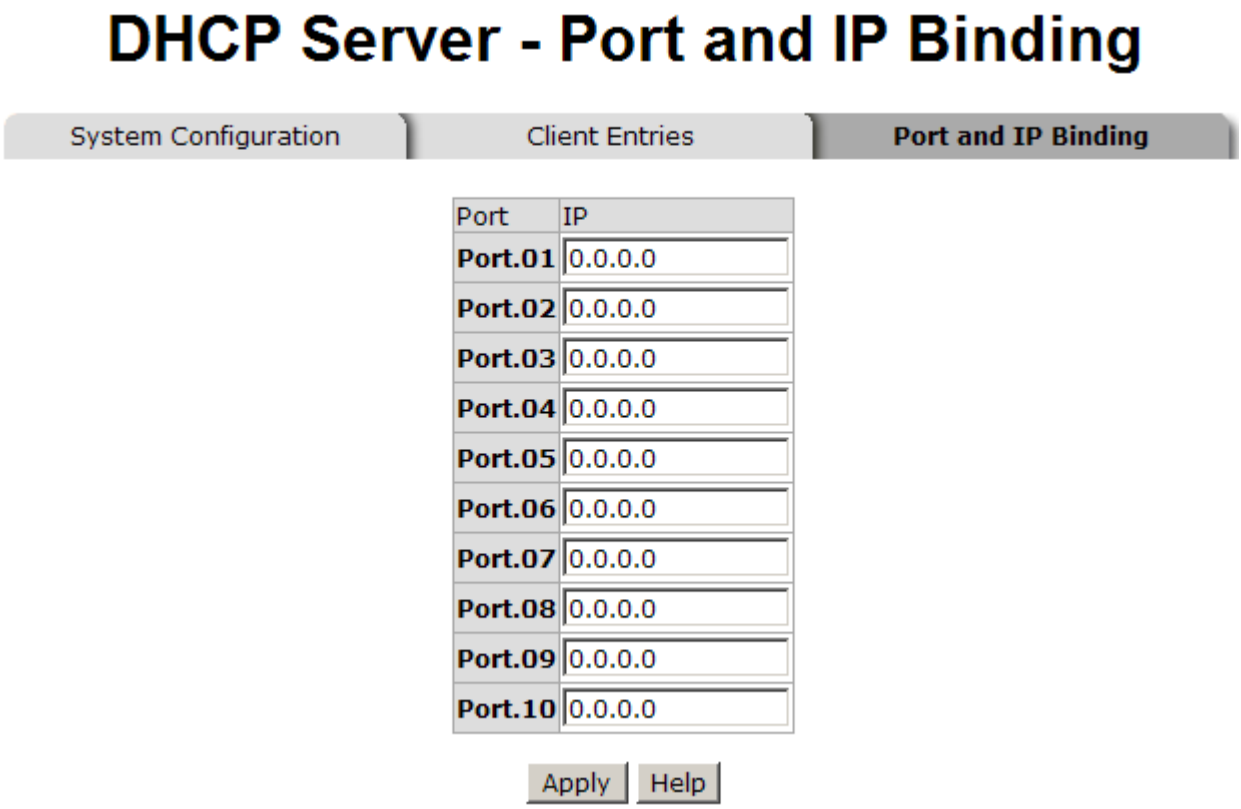
When the **DHCP Server** function is enabled, the system will collect the DHCP client information including the assigned IP address, the MAC address of the client device, the IP assigning type, states and lease time.



DHCP Client Entries interface

Port and IP Bindings

As the figure shown below, the switch will assign the IP address to the connected client according to the Port-IP binding table. The user is allowed to fill each port with one particular IP address. When the device is connecting to the port and asks for IP assigning, the system will assign the IP address bound with the port to the device.



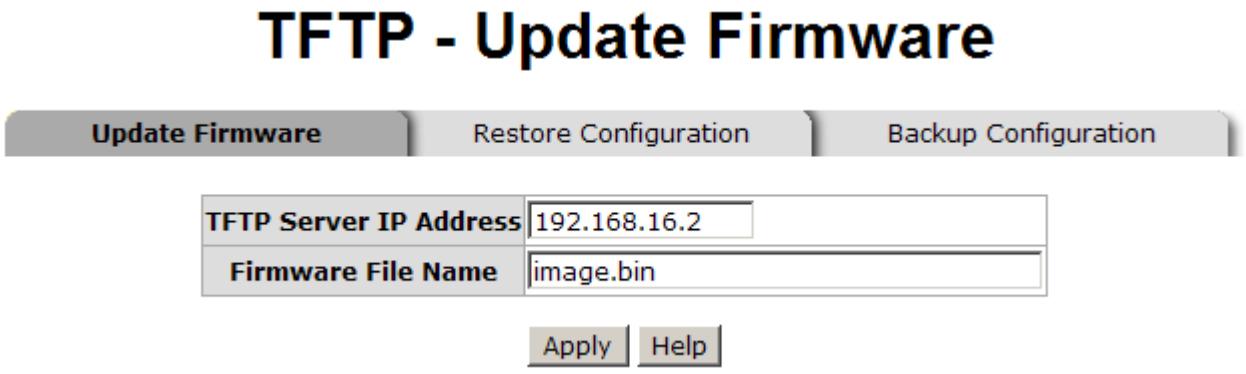
Port and IP Bindings interface

TFTP

It provides the functions allowing the user to update the switch firmware via the Trivial File Transfer Protocol (TFTP) server. Before updating, make sure the TFTP server is ready and the firmware image is located on the TFTP server.

Update Firmware

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

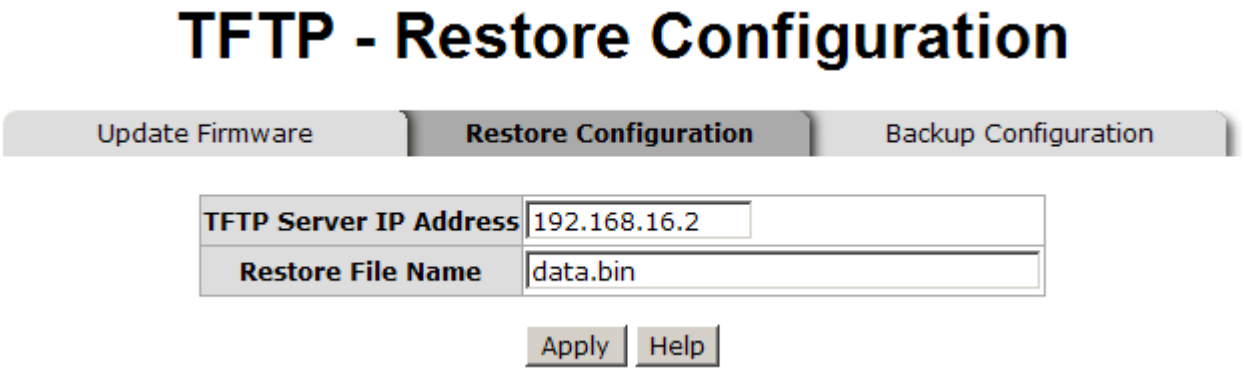


Update Firmware interface

Restore Configuration

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

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

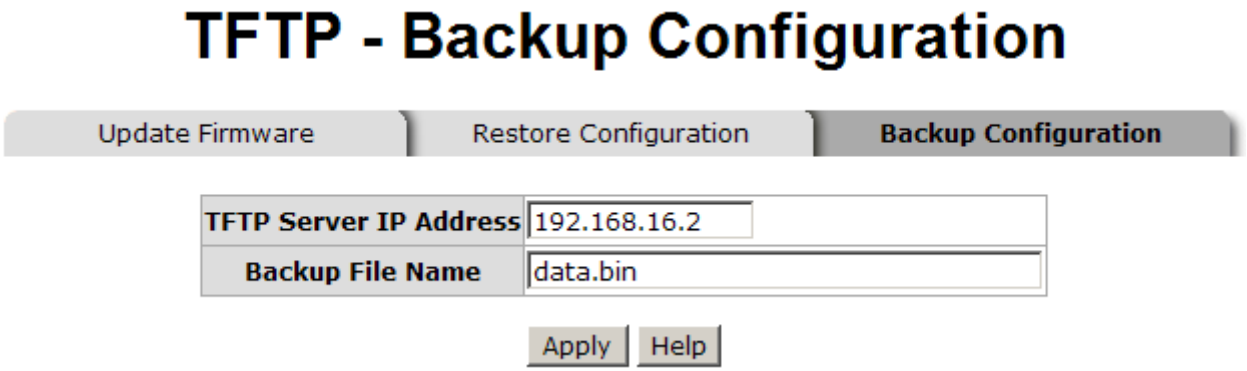


Restore Configuration interface

Backup Configuration

You can back up the current configuration from flash ROM to the TFTP server for the purpose of recovering the configuration later. It helps you avoid wasting time on configuring the settings by backing up the entire configuration.

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



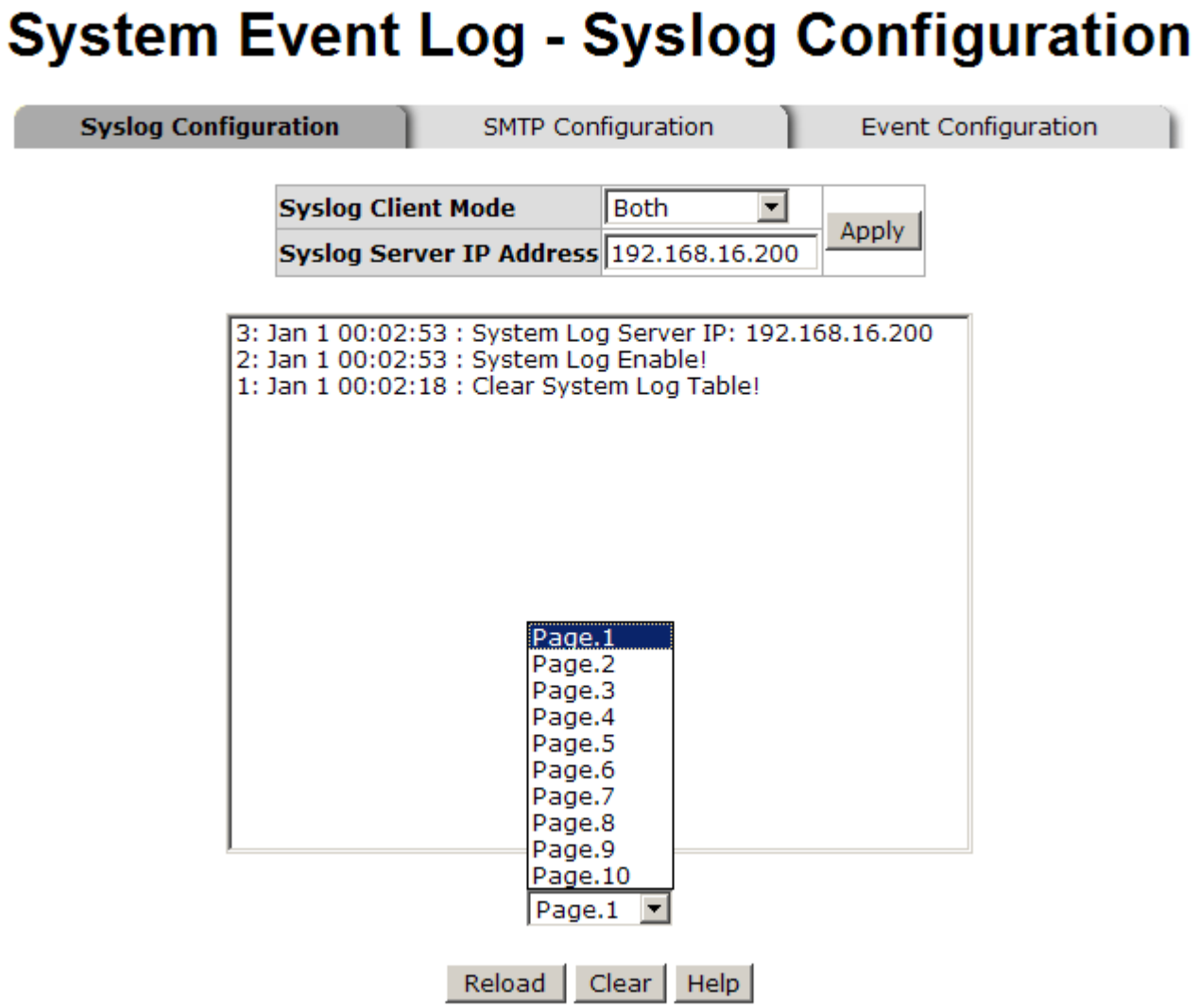
Backup Configuration interface

System Event Log

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

System Event Log—Syslog Configuration

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

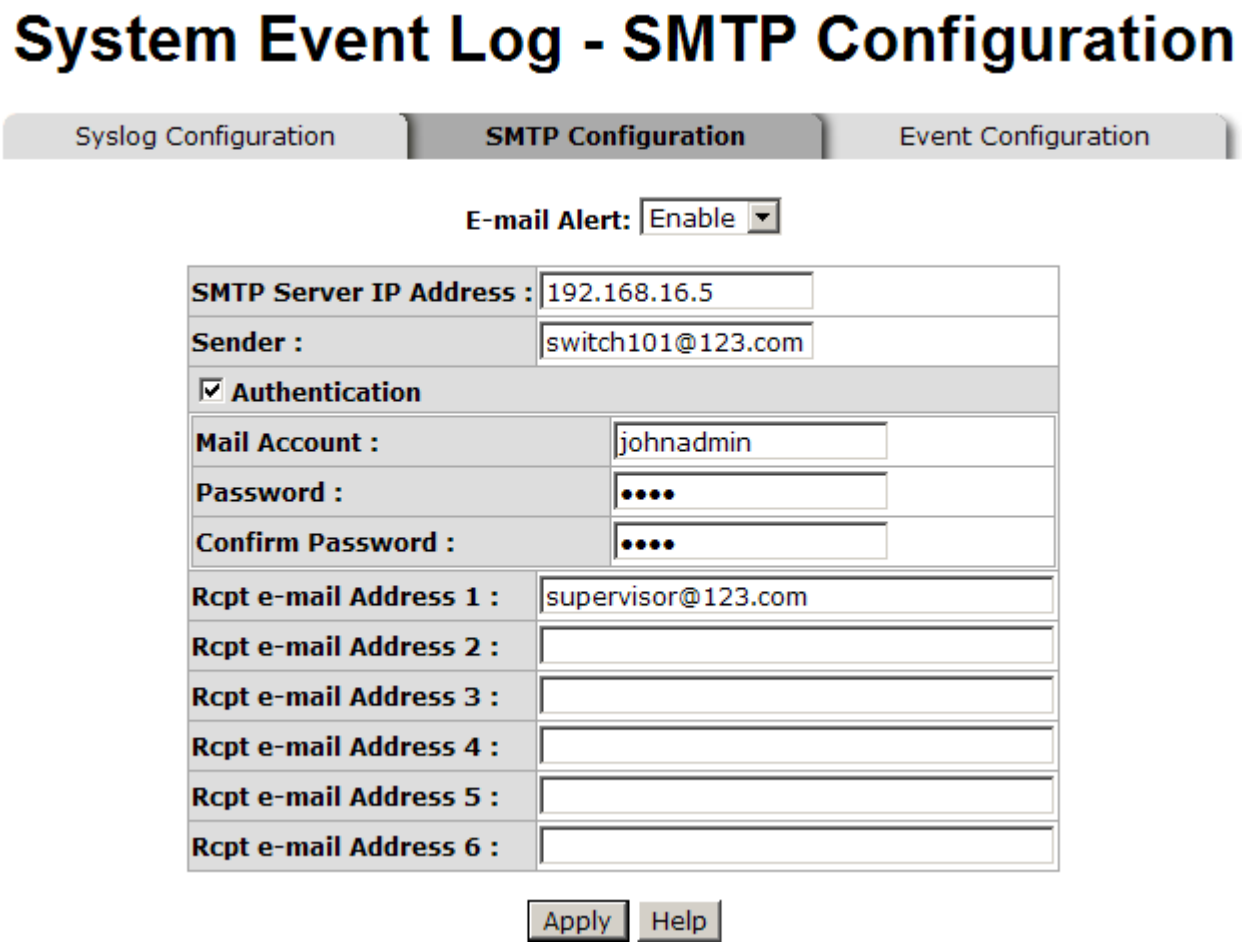


Syslog Configuration interface

System Event Log—SMTP Configuration

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

- **Email Alert:** With this function enabled, the user is allowed to configure the detail settings for sending the e-mail alert to the SMTP server when the events occur.
- **SMTP Server IP Address:** Assign the mail server IP address (when **Email Alert** is enabled, this field will then be available).
- **Sender:** Type in an alias of the switch in complete email address format, e.g. switch101@123.com, to identify where the e-mail alert comes from.
- **Authentication:** Tick the checkbox to have the mail account, password and confirm password fields show up. Configure the email account and password for authentication procedures when this switch logs in to the SMTP server.
- **Mail Account:** Set up the email account, e.g. johnadmin, to receive the email alert. It must be an existing email account on the mail server.
- **Password:** Type in the password to the email account.
- **Confirm Password:** Reconfirm the password.
- **Rcpt e-mail Address 1 ~ 6:** You can also specify up to 6 e-mail accounts to receive the email alert.
- Click Apply to have the configuration take effect.



SMTP Configuration interface

System Event Log—Event Configuration

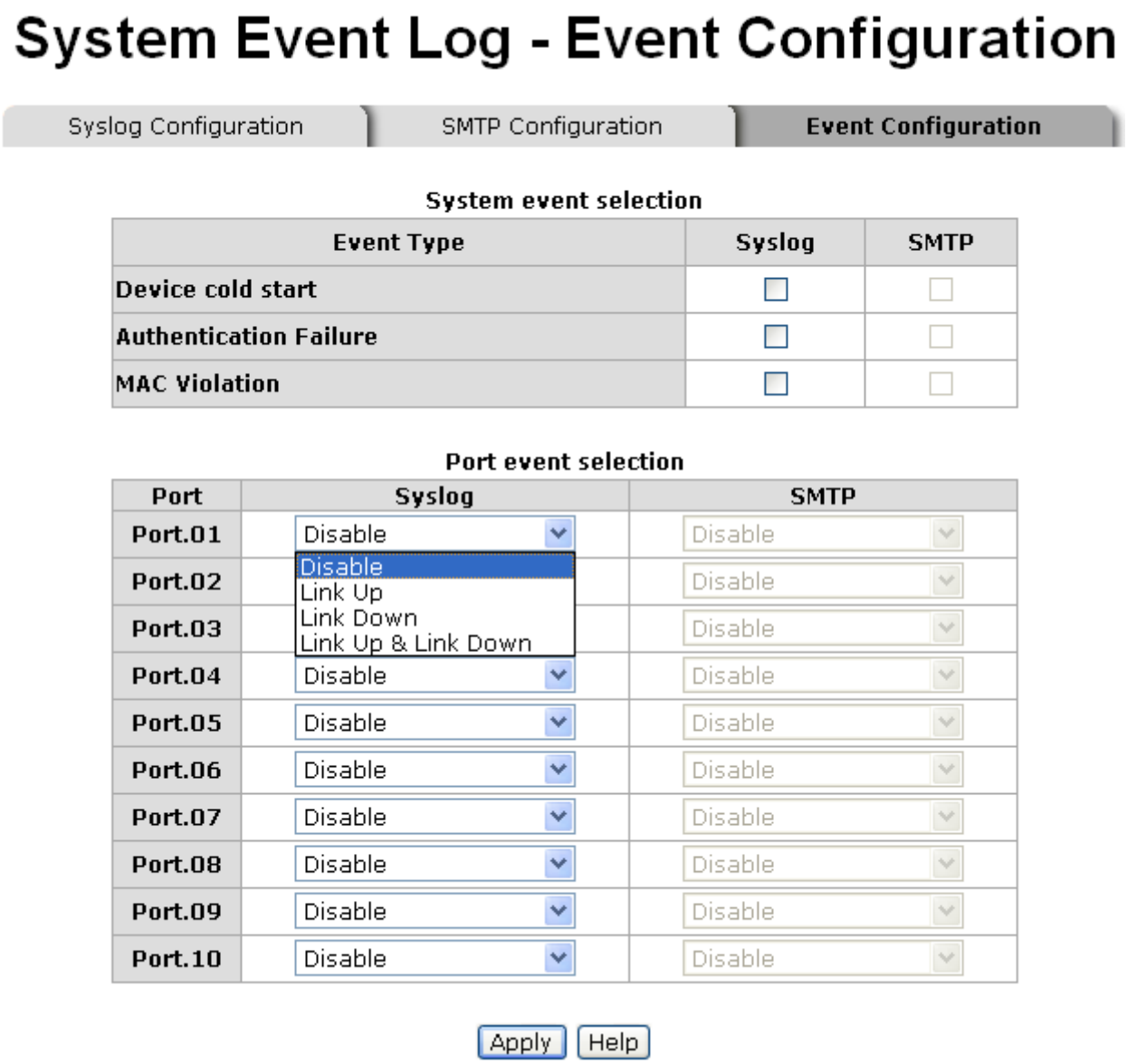
The checkboxes and pull-down menus are not available unless the **Syslog Client Mode** on the Syslog Configuration tab and the **E-mail Alert** on the SMTP Configuration tab are enabled first.

This tab mainly controls whether an event notification is to be sent to the **Syslog**/**SMTP** server. The part of **System Event Selection** controls the event notification including Device Cold Start, Authentication Failure, and MAC Violation. With the **Syslog**/**SMTP** checkbox ticked, the event log/email alert will be sent to the system log server/SMTP server respectively. As for the part of **Port Event Selection**, port events (link up, link down, and both) can be sent to the system log server/SMTP server by setting the trigger condition for each port respectively.

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

- **Port event selection:** Each drop-down menu has four options—**Disable**, **Link UP**, **Link Down**, and **Link UP & Link Down**. Disable means no event will be sent to the system log/SMTP server.
  - **Link UP:** The system will issue a log message only when the link-up event of the port occurs.
  - **Link Down:** The system will issue a log message only when the link-down event of port occurs.

- **Link UP & Link Down:** The system will issue a log message at the time when port connection is link-up and link-down.

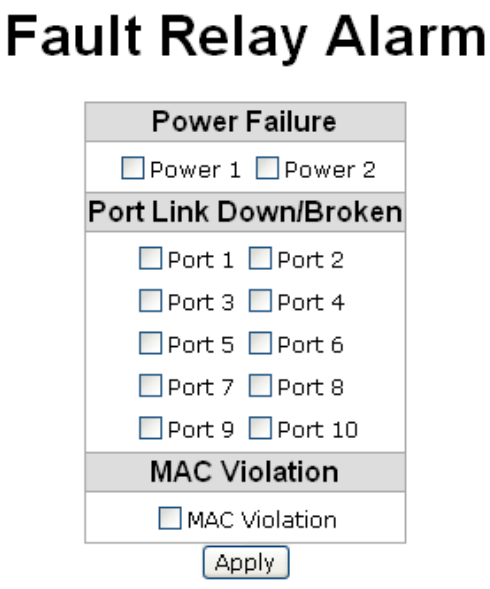


Event Configuration interface

Fault Relay Alarm

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

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



Fault Relay Alarm interface

SNTP Configuration

SNTP (Simple Network Time Protocol) is a simplified version of NTP which is an Internet protocol used to synchronize the clocks of computers with some time reference. Because time usually just advances, the time on different node stations might be different. With the communicating programs running on those devices, it would cause time to jump forward and back, a non-desirable effect. Therefore, the switch provides comprehensive mechanisms to access national time and frequency dissemination services, organize the time-synchronization subnet and the local clock in each participating subnet peer.
Daylight Saving Time (DST) is the convention of advancing clocks so that afternoons have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.

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

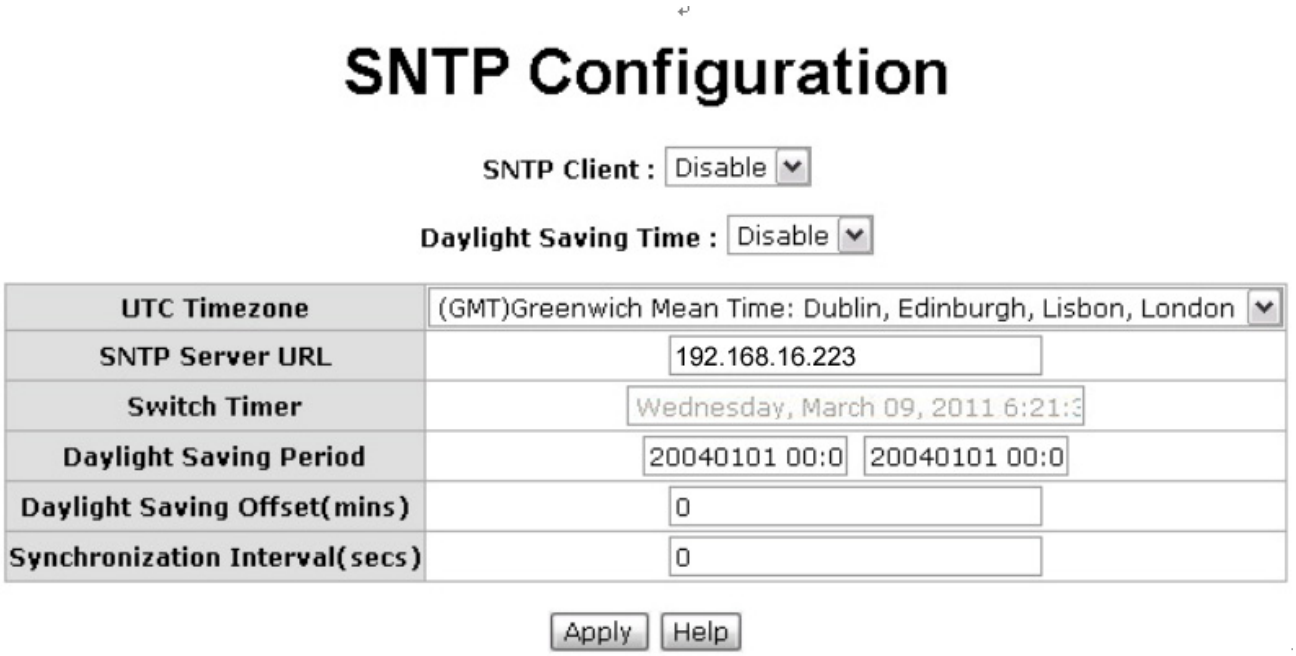
Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11 am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard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

MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm

EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

- **SNTP Sever URL:** Specify the SNTP server IP address. You can assign a local network time server IP address or an internet time server IP address.
- **Switch Timer:** When the switch has successfully connected to the SNTP server whose IP address was assigned in the field of **SNTP Server URL**, the current coordinated time is displayed here.
- **Daylight Saving Period:** Set up the start and end date/time of the daylight saving period. Please key in the value in the format of 'YYYYMMDD' and 'HH:MM' (leave a space between 'YYYYMMDD' and 'HH:MM').
  - **YYYYMMDD:** an eight-digit year/month/day specification.
  - **HH:MM:** a five-digit (including a colon mark) hour/minute specification.

  For example, key in '20070701 02:00' and '20071104 02:00' in the two fields respectively to represent that DST begins at 2:00 a.m. on March 11, 2007 and ends at 2:00 a.m. on November 4, 2007.
- **Daylight Saving Offset (mins):** For non-US and European countries, specify the amount of time for day light savings. Please key in the valid figure in the range of minute between 0 and 720, which means you can set the offset up to 12 hours.
- **Synchronization Interval (secs):** The Synchronization Interval is used for sending synchronizing packets periodically. Users can assign the time ranging from 64 to 1024 seconds. The "0" value displaying by default means that you disable the auto-synchronized feature in the SNTP client mode. You can enable the feature by filling the interval range from 64~1024 seconds.
- Click Apply to have the configuration take effect.



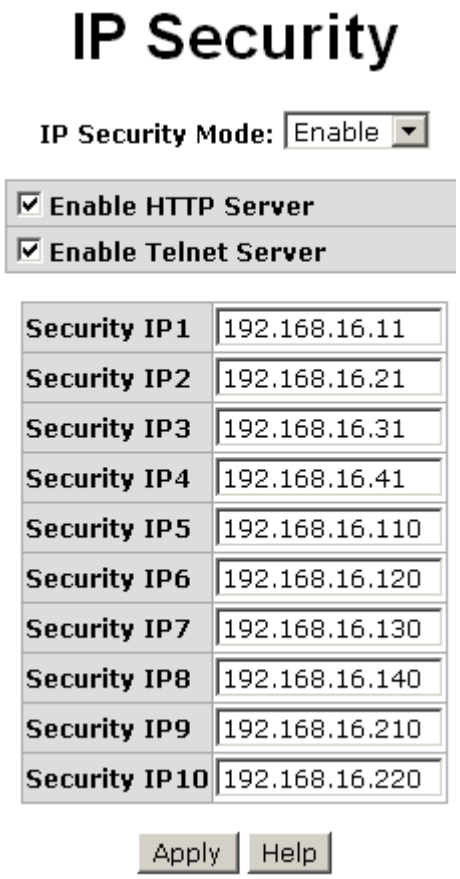
SNTP Configuration interface

IP Security

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

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

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



IP Security interface

User Authentication

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

Admin User

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

Guest User

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

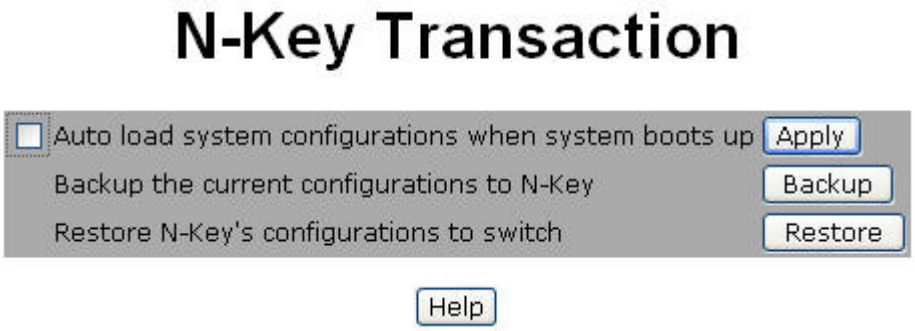
User Authentication interface

N-Key Transaction

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

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

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



N-Key Transaction interface

Port Statistics

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

- **Port:** Port number indexed.
- **Type:** Displays the network media type of the port.
- **Link:** The states of linking—'**Up**' or '**Down**'.
- **State:** Displays port states set by the Port Control interface. When the state is disabled, the port will not transmit or receive any packet.
- **Tx Good Packet:** The counts of transmitting good packets via this port.
- **Tx Bad Packet:** The counts of transmitting bad packets (including undersize [less than 64 bytes], oversize, CRC Align errors, fragments and jabbers packets) via this port.
- **Rx Good Packet:** The counts of receiving good packets via this port.
- **Rx Bad Packet:** The counts of receiving good packets (including undersize [less than 64 bytes], oversize, CRC error, fragments and jabbers) via this port.
- **Tx Abort Packet:** The counts of aborted packets while transmitting.
- **Packet Collision:** The counts of packet collision.
- **Packet Dropped:** The counts of dropped packets.
- **Rx Bcast Packet:** The counts of broadcast packets.
- **Rx Mcast Packet:** The counts of multicast packets.
- Click the 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	100TX	Up	Enable	1481	0	1513	0	0	0	0	66	0
Port.02	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.03	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.04	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.05	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.06	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.07	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.08	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.09	100FX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.10	100FX	Down	Enable	0	0	0	0	0	0	0	0	0

Clear Help

Port Statistics interface

Port Control

In Port Control you can configure the parameters of the connection for each port.

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

Port Control

Port	State	Negotiation	Speed	Duplex	Flow Control	Security
Port.01 Port.02 Port.05 Port.06	Enable	Auto	100	Full	Enable	Off

Apply Help

Port	Group ID	Type	Link	State	Negotiation	Speed Duplex		Flow Control		Security
						Config	Actual	Config	Actual	
Port.01	N/A	100TX	Up	Enable	Auto	100 Full	100 Full	Enable	ON	OFF
Port.02	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.03	Trunk.1	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.04	Trunk.1	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.05	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.06	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.07	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.08	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.09	N/A	100FX	Down	Enable	Force	100 Full	N/A	Enable	N/A	OFF
Port.10	N/A	100FX	Down	Enable	Force	100 Full	N/A	Enable	N/A	OFF

Port Control interface

Port Trunk

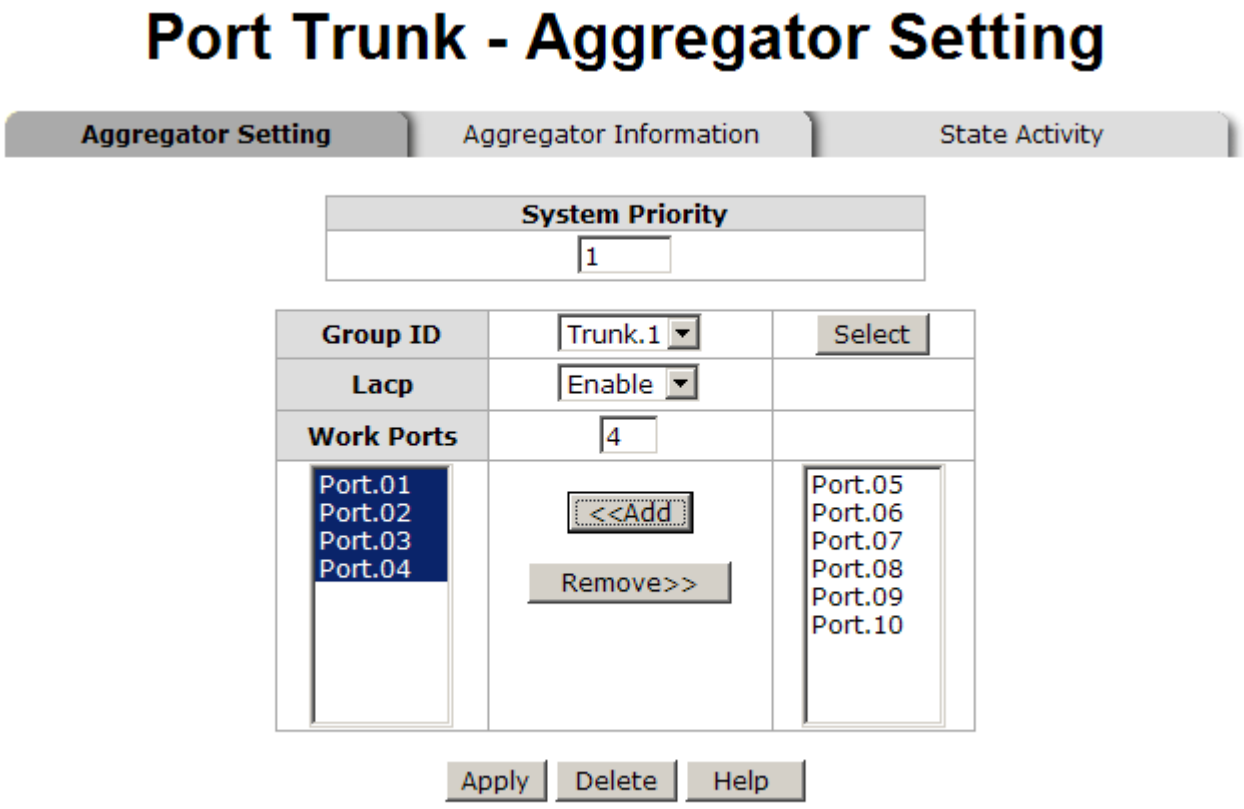
Port trunking is the combination of several ports or network cables to expand the connection speed beyond the limits of any one single port or network cable. Link Aggregation Control Protocol (LACP), which is a protocol running on layer 2, provides a standardized means in accordance with IEEE 802.3ad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

Aggregator Setting

Please read the instructions below to make an LACP or non-LACP trunk group.

- **System Priority:** A value which is used to identify the controlling switch of an LACP link system. The switch with the lower value has the higher system priority and is selected as the controlling end, which controls port priorities, of the LACP link system.
- **Group ID:** There are four trunk groups to be selected. Assign the group ID to the particular trunk group.
- **LACP:** Click the pull-down menu to enable/disable LACP for the trunk group. With LACP enabled, a port which joins an **LACP trunk group** has to make an agreement with its member ports first. Please notice that a trunk group, including member ports split between two switches, has to enable the LACP function of the two switches. When disabled, the trunk group is a **static trunk group**. The advantage of having the LACP disabled is that a port joins the trunk group without any handshaking with its member ports; but member ports won't know that they should be aggregated together to form a logic trunk group.
- **Work Ports:** This field allows the user to type in the total number of active ports up to four. With a **LACP trunk group** employed, for example you assign four ports to be the members of a trunk group whose *Work Ports* field is set as two the excessive ports will be standby/redundant ports and can be aggregated instead of working ports that fail. As for the **static trunk group** (non-LACP), the number of work ports must equal the total number of the group member ports.

- The system allows a maximum of four ports to be aggregated in a trunk group. Having configured the parameters above, highlight the ports in the right list box to join the trunk group. Click the Add button and the ports highlighted in the right list box will be shifted to the left list box. To remove unwanted ports, select the ports in the left list box and click the Remove button.
- When LACP enabled, you can configure LACP Active/Passive states for each member port on the **State Activity** tab.
- When finished, click Apply to take the configuration take effect.
- To remove a trunk group, select the Group ID by clicking the pull-down menu labeled as 'Group ID' and click then click the Delete button.

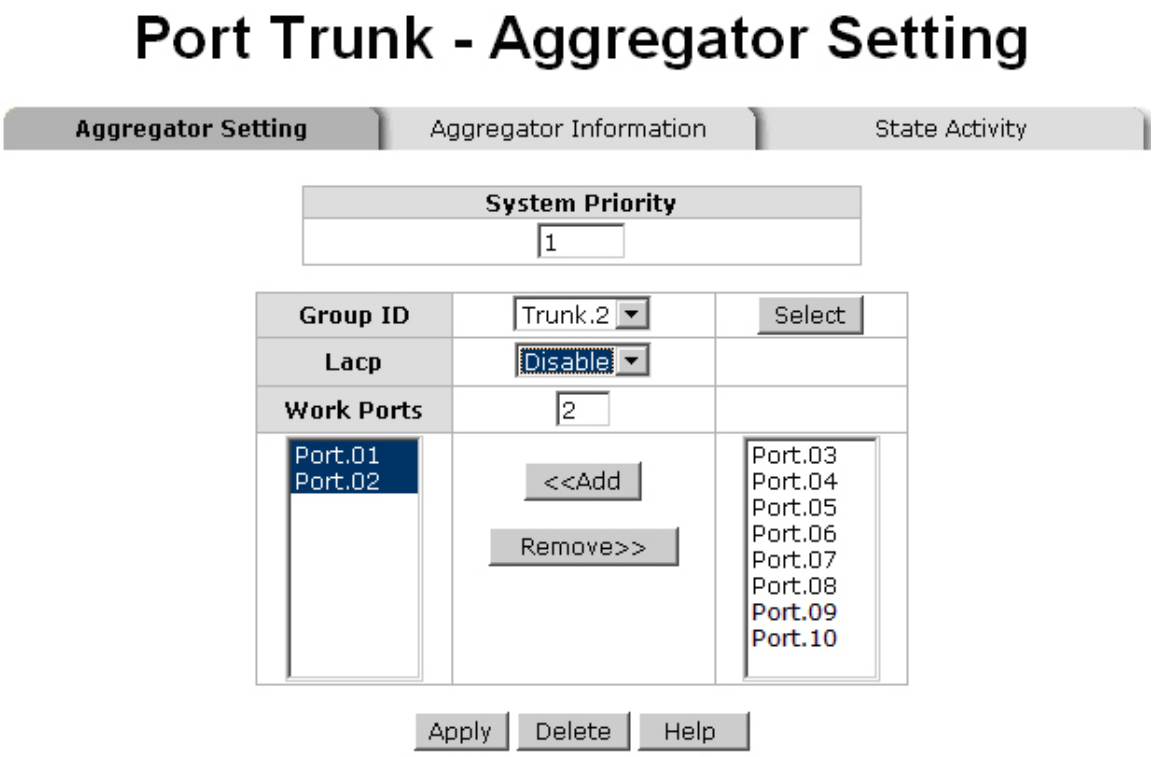


Port Trunk—Aggregator Setting interface (four ports are added to the left field with LACP enabled)

Aggregator Information

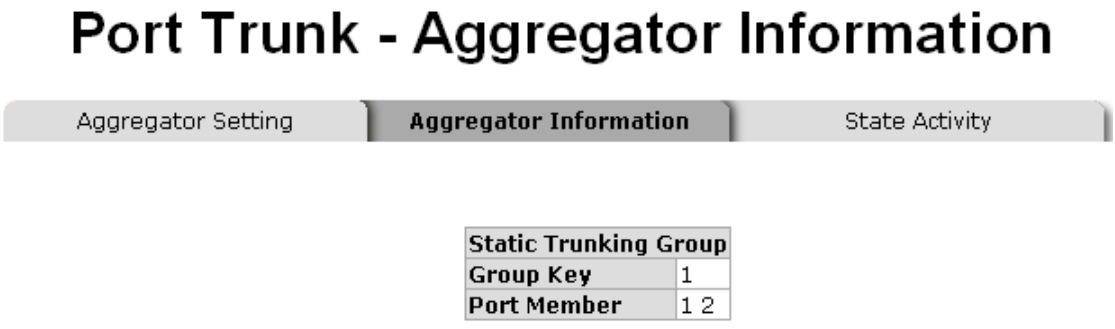
- **LACP Disabled**

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



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

Assigning 2 ports to a trunk group with LACP disabled



Static Trunking Group Information tab

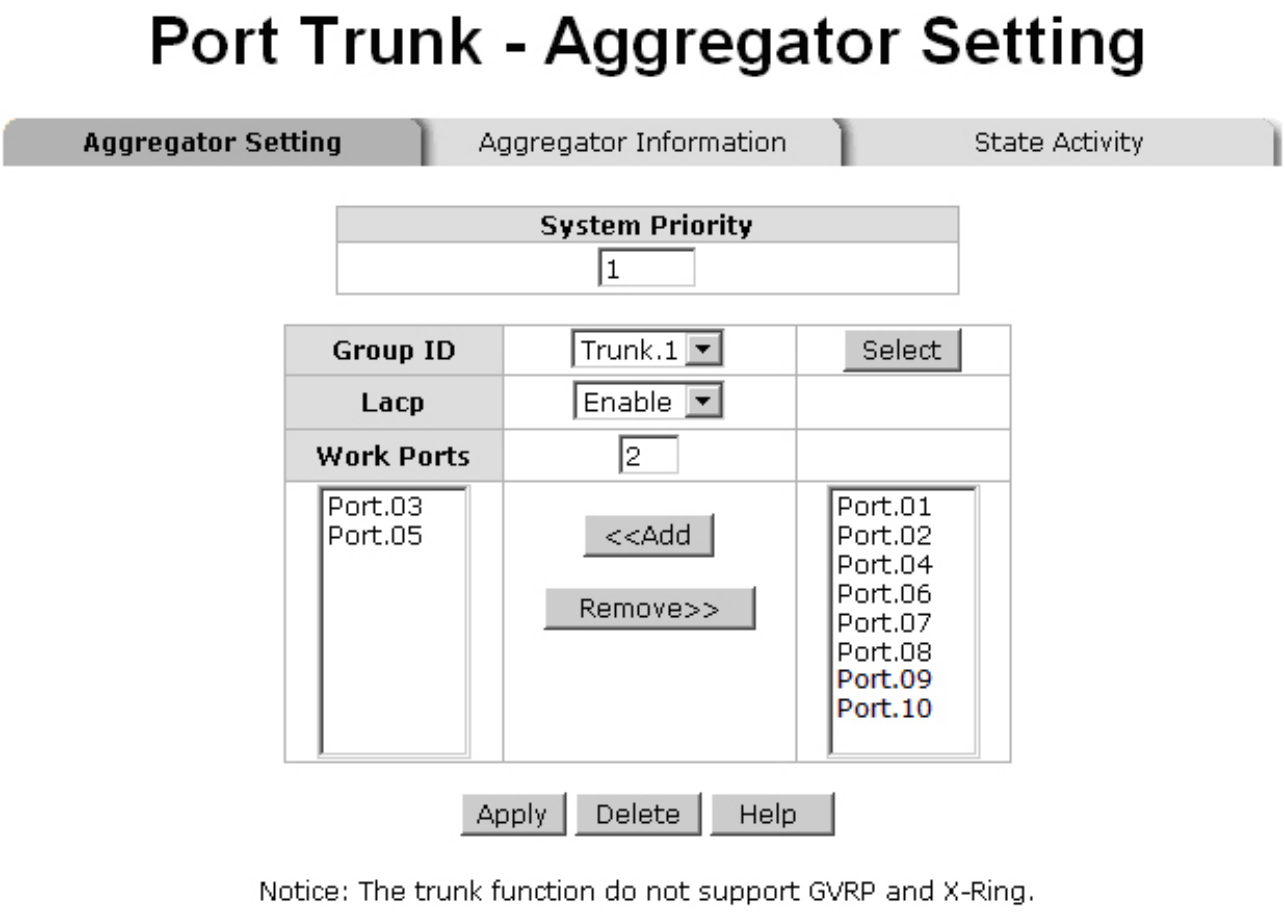
- **Group Key:** This is a read-only field that displays the trunk group ID.
- **Port Member:** This is a read-only field that displays the members of the static trunk group.

- **LACP Enabled**

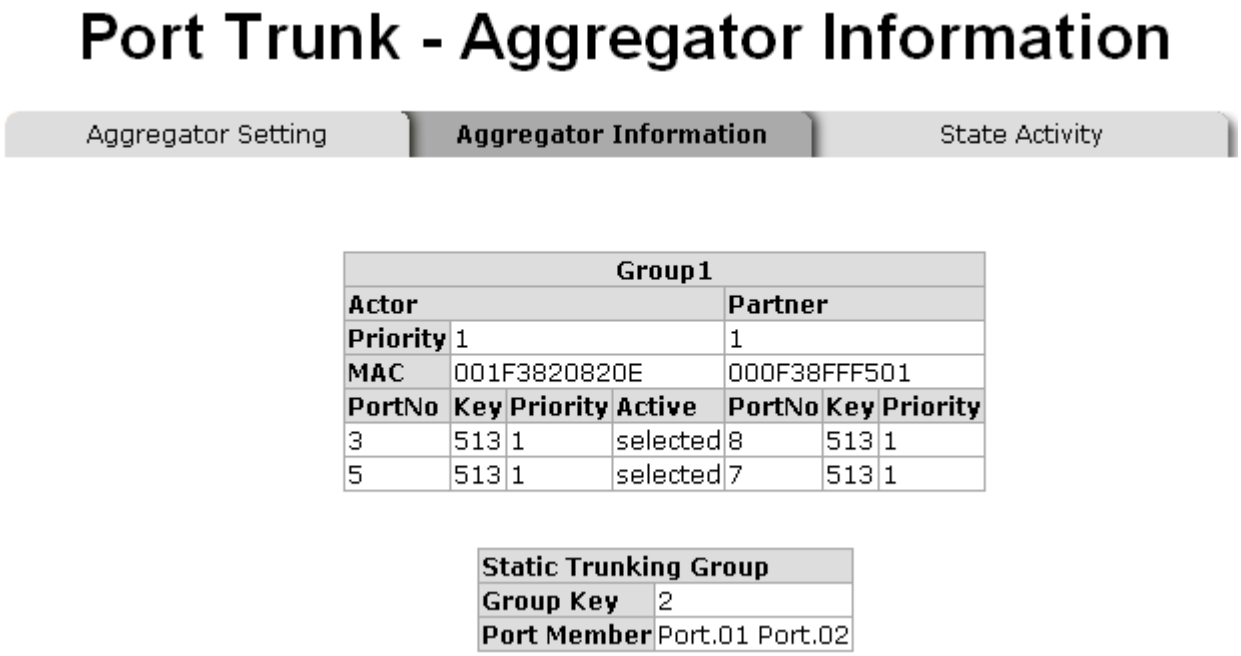
Having configured the aggregator setting with LACP enabled, you can check the trunking group information between two switches on the **Aggregator Information** tab.

■ **Configuration for Switch 1**

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



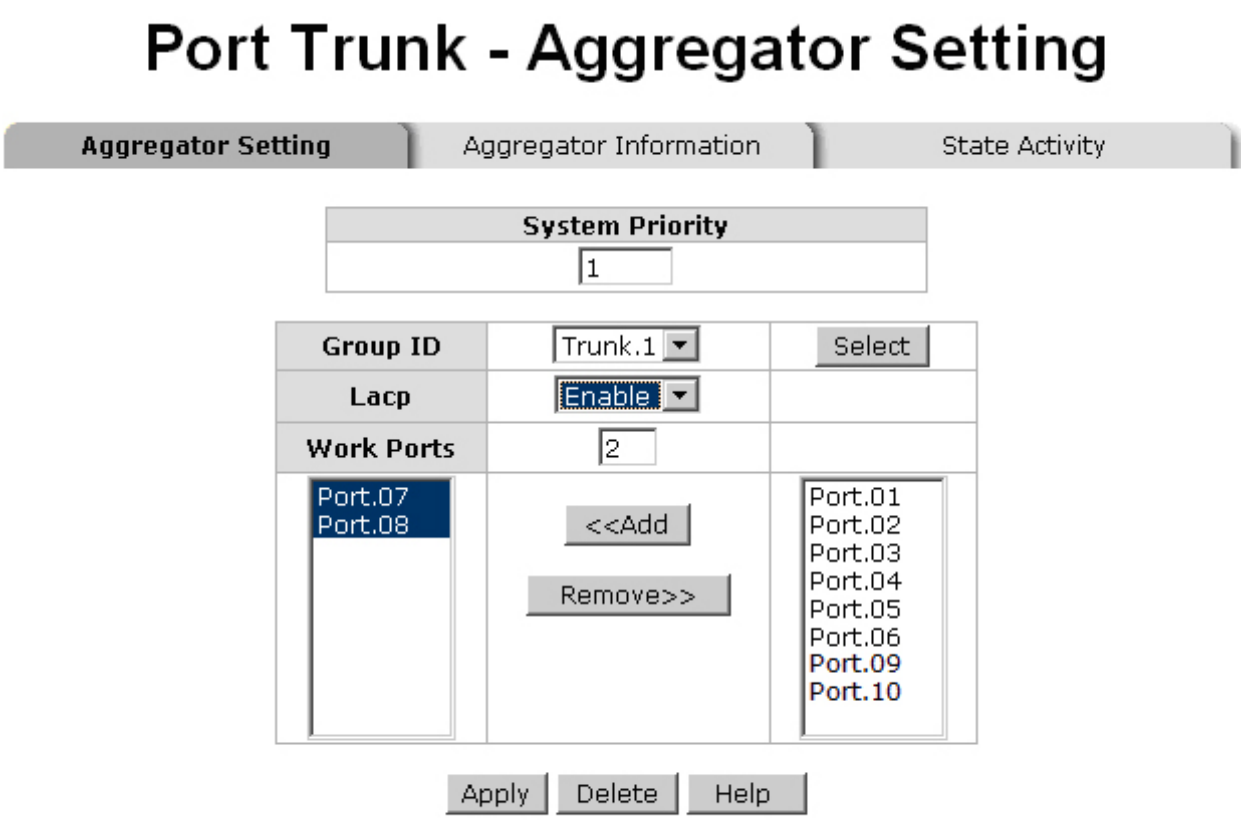
Switch 1 configuration interface



Aggregation Information of Switch 1

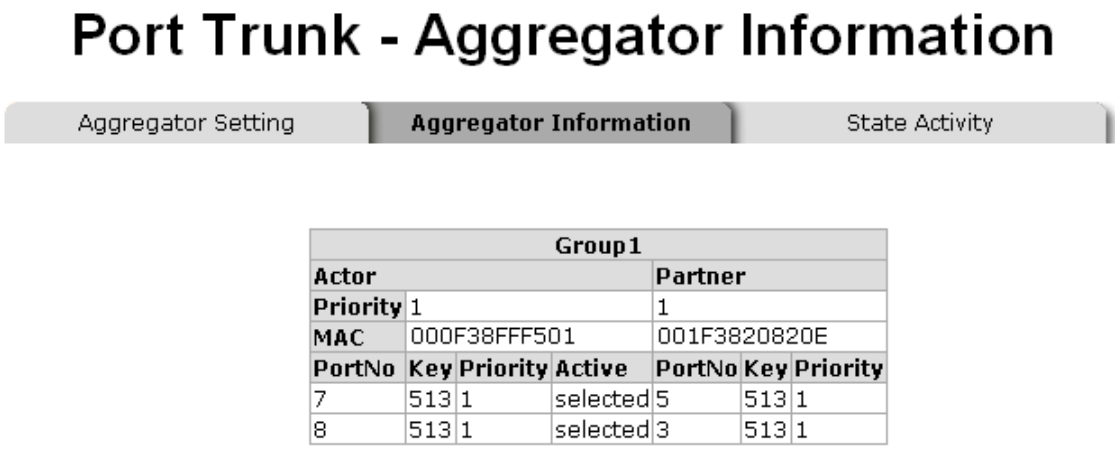
5. Click on the **Aggregator Information** tab to check the trunked group information as the illustration shown above after the two switches configured.

■ **Configuration for Switch 2**



Switch 2 configuration interface

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



Aggregation Information of Switch 2

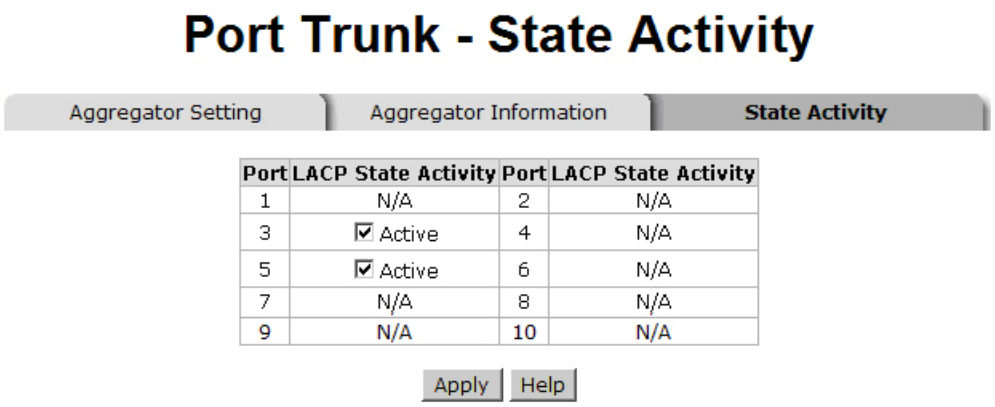
5. Click on the **Aggregator Information** tab to check the trunked group information as the illustration shown above after the two switches configured.

State Activity

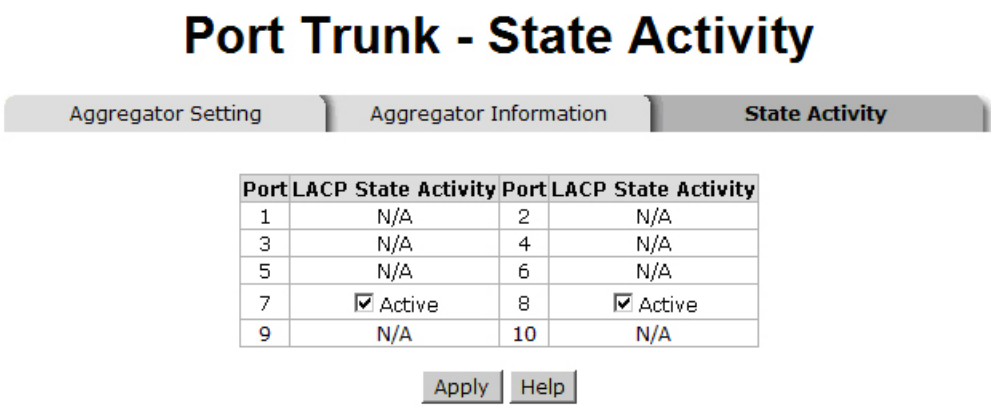
Having configured the LACP aggregator on the **Aggregator Setting** tab, you may want to change the state activity for the members of the LACP trunk group. You can tick/un-tick the checkbox beside the state label. If you remove the tick mark of the corresponding port and click the Apply button, the port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

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

[NOTE]	**A link** having two passive LACP nodes will not perform dynamic LACP trunk because both ports are waiting for an LACP protocol packet from the opposite device.



State Activity of Switch 1

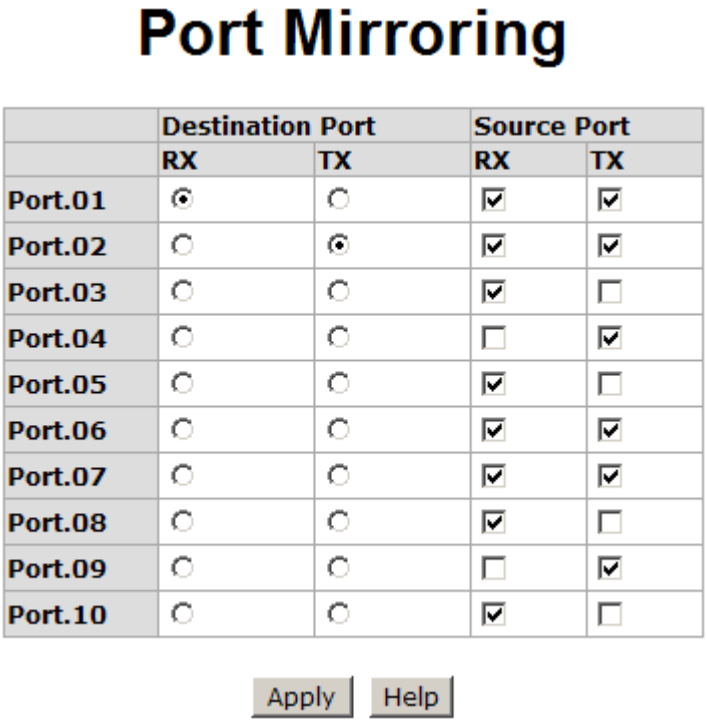


State Activity of Switch 2

Port Mirroring

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

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



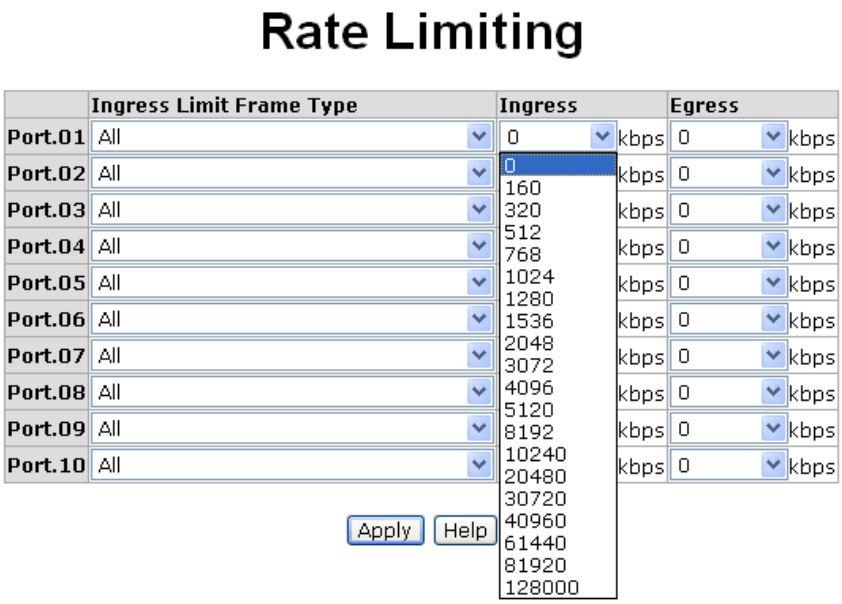
Port Mirroring interface

Rate Limiting

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

- **Ingress Limit Frame Type:** Select the limit type for ingress frames. Four options are available as follows:
  - **All**
  - **Broadcast/Multicast/Flooded Unicast**
  - **Broadcast/Multicast**
  - **Broadcast only**

  The egress rate will limit all types of frame.



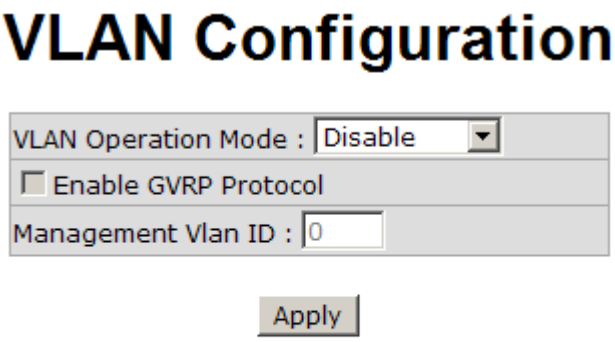
Rate Limiting interface

- Click the Ingress/Egress pull-down menus to select the bandwidth limit.
- When finished, click Apply to have the configuration take effect.

VLAN Configuration

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

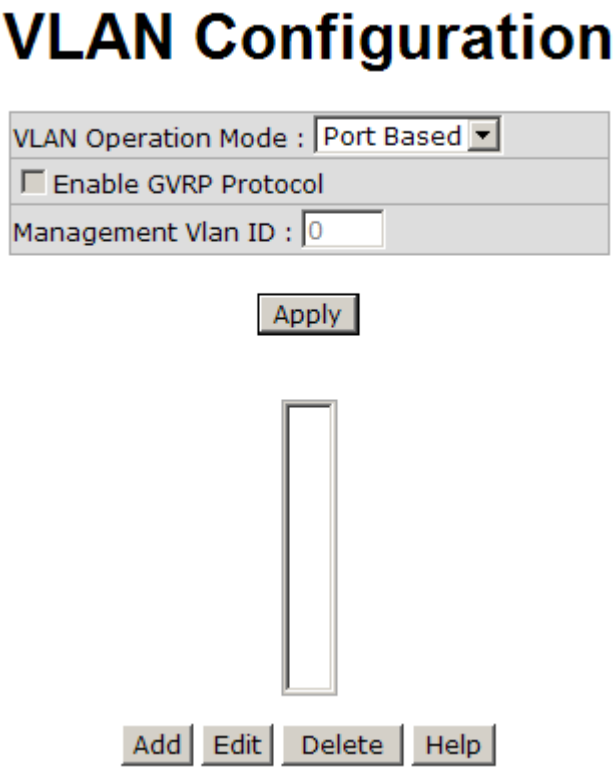
This switch supports **Port-based** and **802.1Q** (tagged-based) VLAN. Please read the following instructions to configure the appropriate type of VLAN for your need.



VLAN Configuration interface

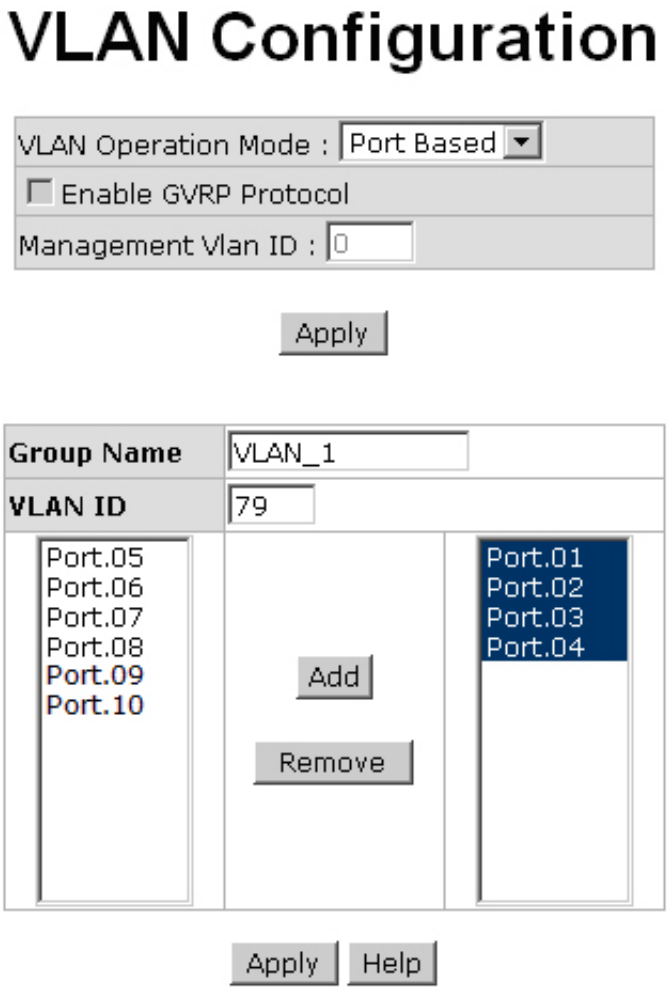
- **Port-based VLAN**

A port-based VLAN normally consists of its members—ports, which means the VLAN is created by grouping the selected ports. This method provides the convenience for users to configure a simple VLAN easily without complicated steps. Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN that is, technically, a single broadcast domain. If the port-based VLAN is enabled, the VLAN-tagging will be ignored. Port-based VLAN allows the user to create separate VLANs to limit the unnecessary packet flooding; however, for the purpose of sharing resource, a single port called a common port can belongs to different VLANs, which all the member devices (ports) in different VLANs have the permission to access the common port while they still cannot communicate with each other in different VLANs.



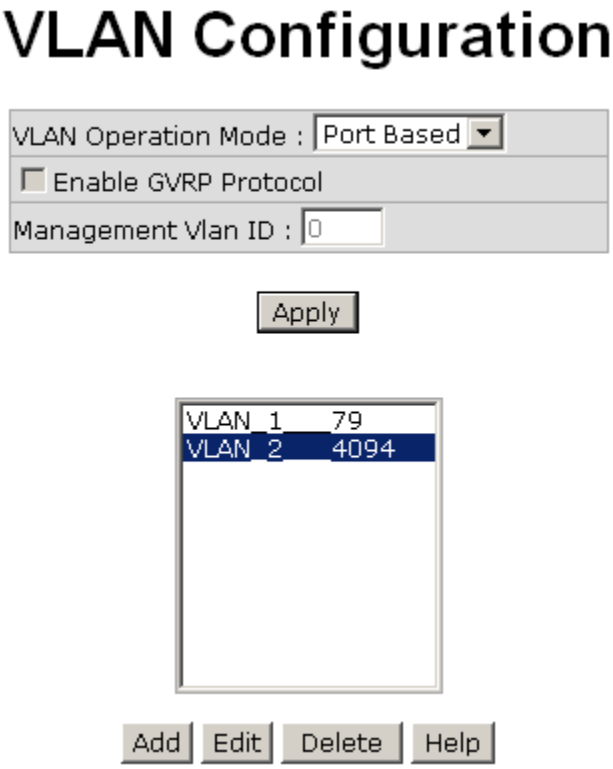
VLAN – Port Based interface

- Click the pull-down menu to select **Port Based** and then click the Apply button to set the VLAN operation mode on **Port Based**.
- With the VLAN operation mode selected, click Add to create a new VLAN group.



Add a Port Based VLAN

- Enter the group name and VLAN ID. Select the port number available in the left list box, and click the Add button to move the highlighted ports to the right list box. Or you can select any of the ports listed in the right field and click Remove to remove port(s) from the VLAN.
- When finished, click Apply to have the VLAN configuration take effect.
- And then you will see the VLAN list shows up.



Edit/Delete Port Based VLAN

- With the VLAN list box showing up, select VLAN(s) and click the Delete button to get rid of the VLAN(s).
- Highlight a VLAN and click the Edit button to change group name, VLAN ID, or to add/remove the members of the existing VLAN group.

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

- **802.1Q VLAN**

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

GVRP (GARP VLAN Registration Protocol) is a protocol that facilitates control of VLANs within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration information with other devices. For example, with GVRP enabled, the switches are able to automatically exchange the information of their VLAN database. Therefore, the user needn't manually configure the link type. The packets belonging to the same VLAN can communicate across switches.

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

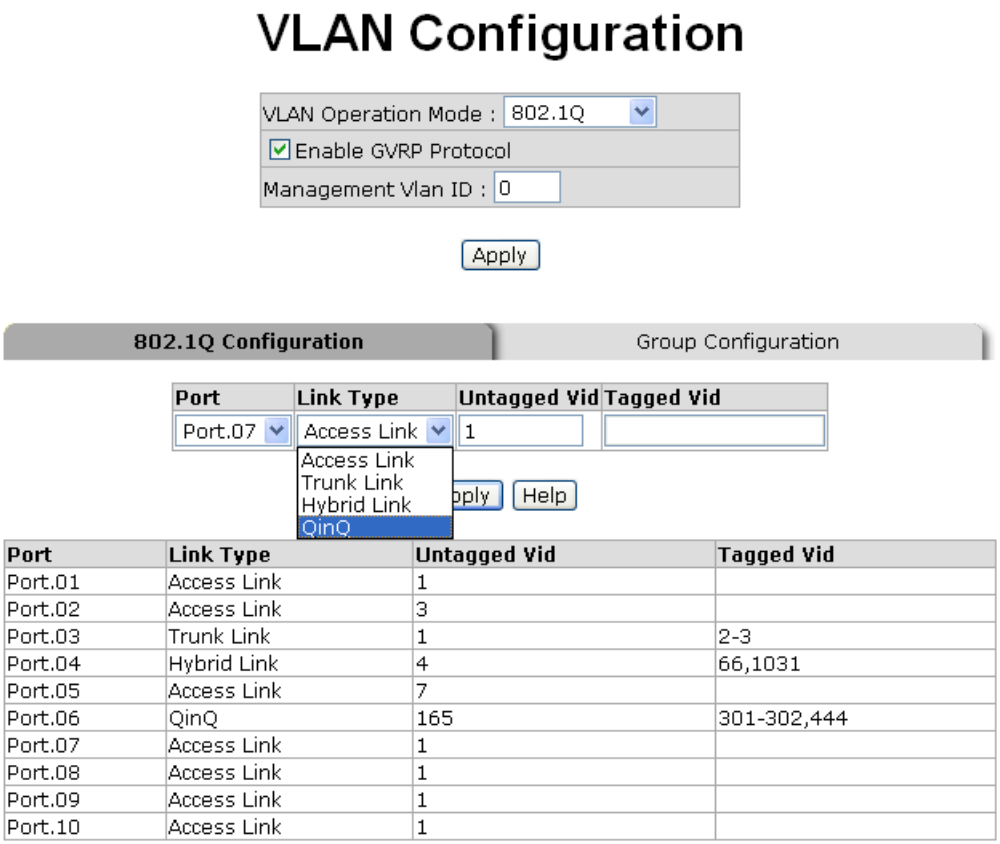
The technique of 802.1Q tagging inserts a 4-byte tag, including VLAN ID of the destination port—PVID, in the frame. With the combination of Access/Trunk/Hybrid Links, the communication across switches also can make the packet sent through tagged and untagged ports.

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

802.1Q Configuration

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

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



802.1Q VLAN interface

- On the 802.1Q Configuration tab, click the *Port* pull-down menu to select a port you

want to configure within the VLAN.

- **Link Type**: Three options are available. Click the pull-down menu to select the link type.
  - **Access Link:** A segment which provides the link path for one or more stations to the VLAN-aware device like switches. An Access Port (untagged port) connecting to the access link has an untagged VID (also called PVID). After an untagged frame gets into the access port, the switch inserts a four-byte tag in the frame. The contents of the last 12-bit of the tag is the untagged VID. When this frame is sent out through any of the access ports of the same PVID, the switch will remove the tag from the frame to recover it to what it was. Those ports of the same untagged VID are regarded as the same VLAN group members.

[NOTE] *Because the access port doesn't have an understanding of tagged frame, the field of Tagged VID is not available.*

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

[NOTE]

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

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

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

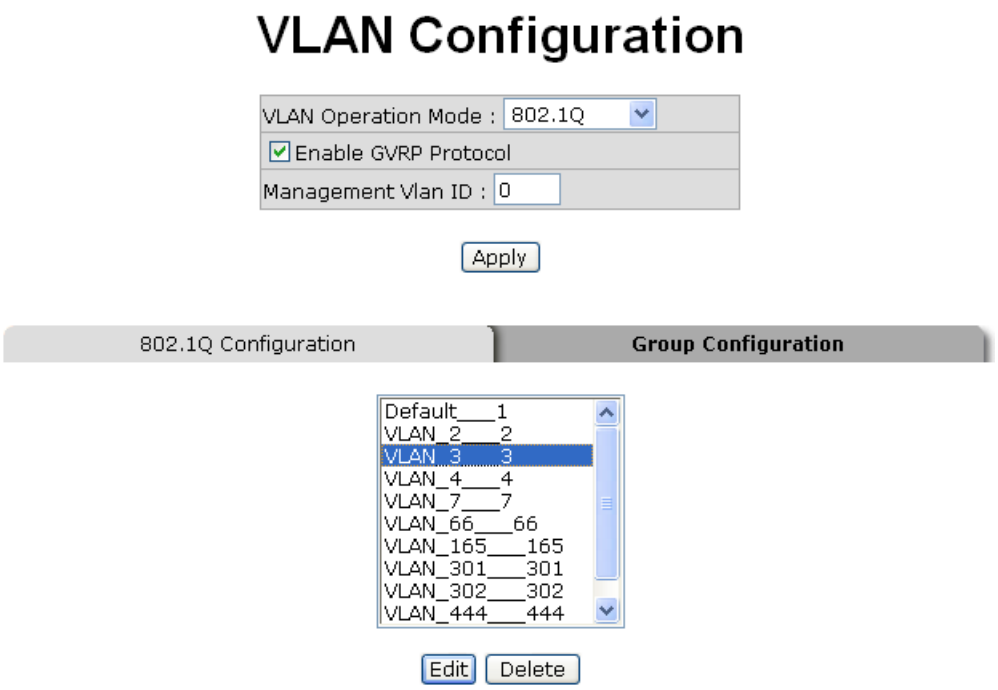
- **QinQ:** With the given port set its link type on QinQ, where frames received will be added a tag as an outer 802.1Q VLAN header that needs to be specified by users in the *Untagged Vid* field next to this pull-down menu. The value(s) specified in the *Tagged Vid* field show the inner 802.1Q VLAN header(s) that constitute frames with those VLAN headers will be encapsulated.

- **Untagged Vid:** This field is available when the *Link Type* pull-down menu is set on *Access Link*, *Hybrid Link* and *QinQ*. Assign a number in the range between 1 and 4094.
- **Tagged Vid:** This field is available when the *Link Type* pull-down menu is set on *Trunk Link* and *Hybrid Link* and *QinQ*. Assign a number in the range between 1 and 4094.
- Click the Apply button on the tab to have the port configuration take effect.
- And then you can see the link type, untagged VID, and tagged VID information of each port shown in the table on the screen.

Group Configuration

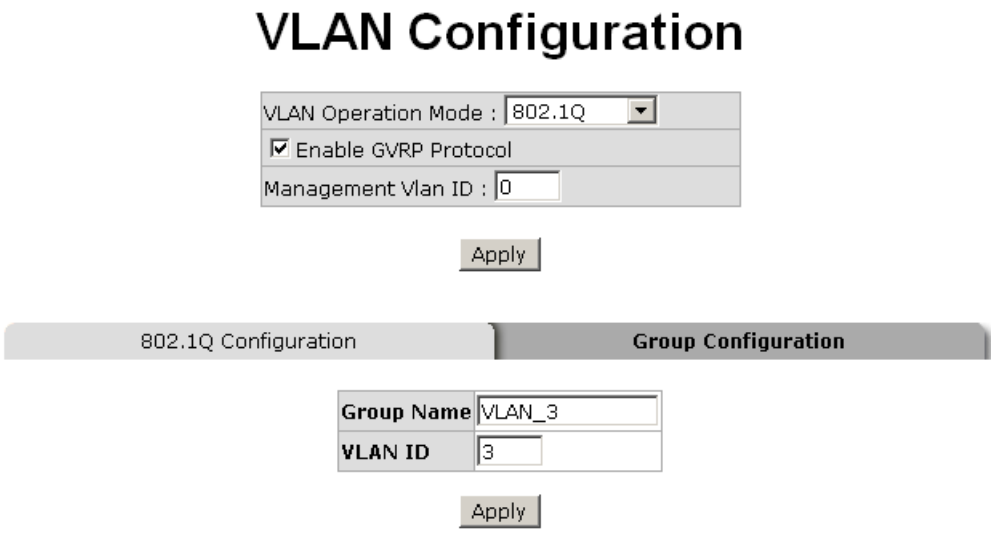
Edit the existing VLAN Groups.

- Click the Group Configuration tab.
- Select a VLAN group in the list box and click the Edit button.



Group Configuration interface

- After clicking the Edit button, you can change group name and VLAN ID of the selected VLAN group.



Group Configuration interface

- When finished, click Apply to have the modification take effect.

Rapid Spanning Tree

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

RSTP System Configuration

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

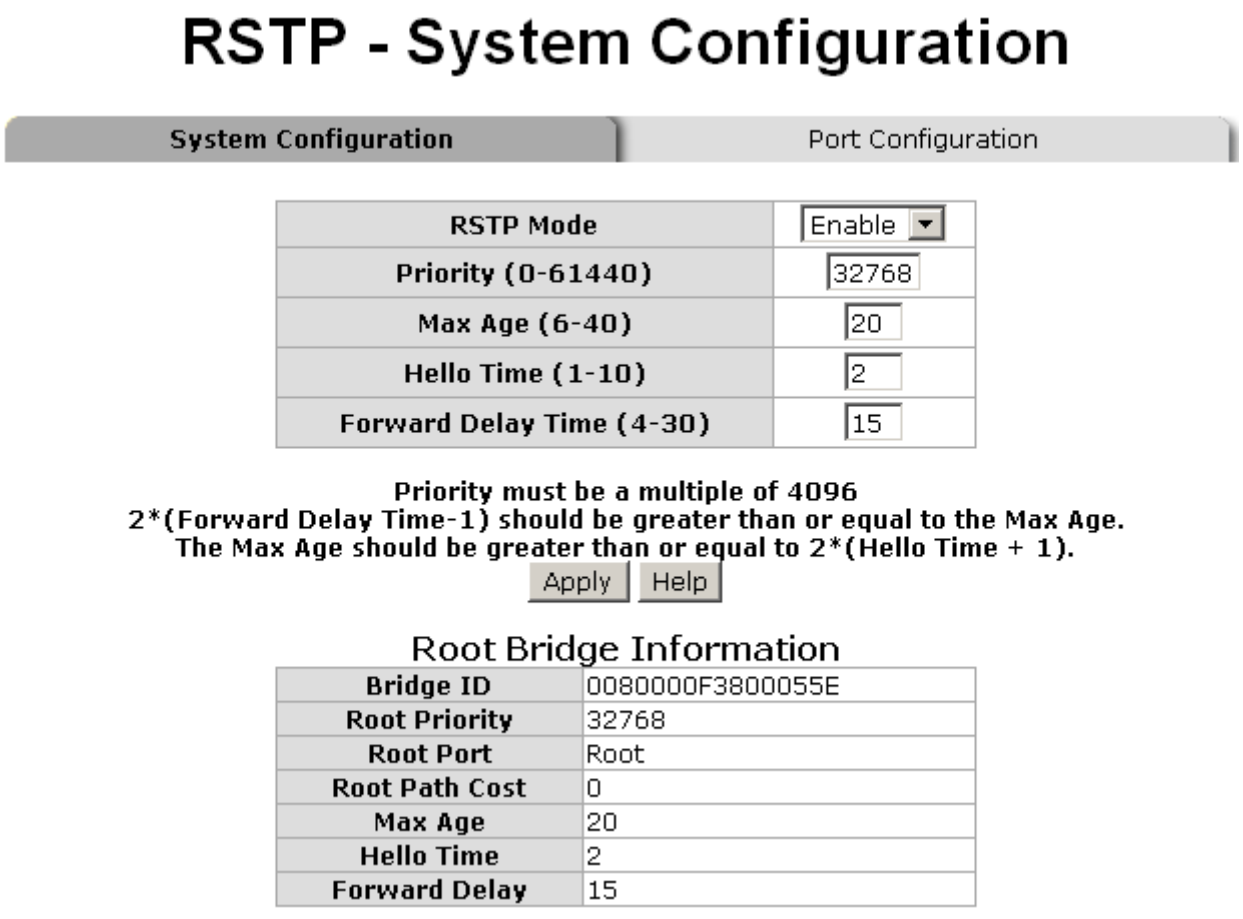
- **RSTP mode:** Click the pull-down menu to enable the RSTP function.
- **Priority (0-61440):** The switch with the lowest numerical value has the highest priority and will be selected as the root device. If the value is changed, users must reboot the switch. Note the value specified in this field must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

[NOTE]	Follow the rule below to configure *Max Age*, *Hello Time*, and *Forward Delay Time* parameters. **2 x (Forward Delay Time value –1) > = Max Age value >= 2 x (Hello Time value +1)**

Root Bridge Information

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

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



RSTP System Configuration interface

Port Configuration

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

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

RSTP - Port Configuration

System Configuration | **Port Configuration**

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

priority must be a multiple of 16

Apply Help

RSTP Port Status

Port	Path Cost	Port Priority	Oper P2P	Oper Edge	Stp Neighbor	State	Role
Port.01	200000	128	True	True	False	Disabled	Disabled
Port.02	200000	128	True	True	False	Disabled	Disabled
Port.03	200000	128	True	True	False	Disabled	Disabled
Port.04	200000	128	True	True	False	Disabled	Disabled
Port.05	200000	128	True	True	False	Disabled	Disabled
Port.06	200000	128	True	True	False	Disabled	Disabled
Port.07	20000	128	False	True	False	Forwarding	Designated
Port.08	200000	128	True	True	False	Disabled	Disabled
Port.09	20000	128	True	True	False	Disabled	Disabled
Port.10	20000	128	True	True	False	Disabled	Disabled

RSTP Port Configuration interface

SNMP Configuration

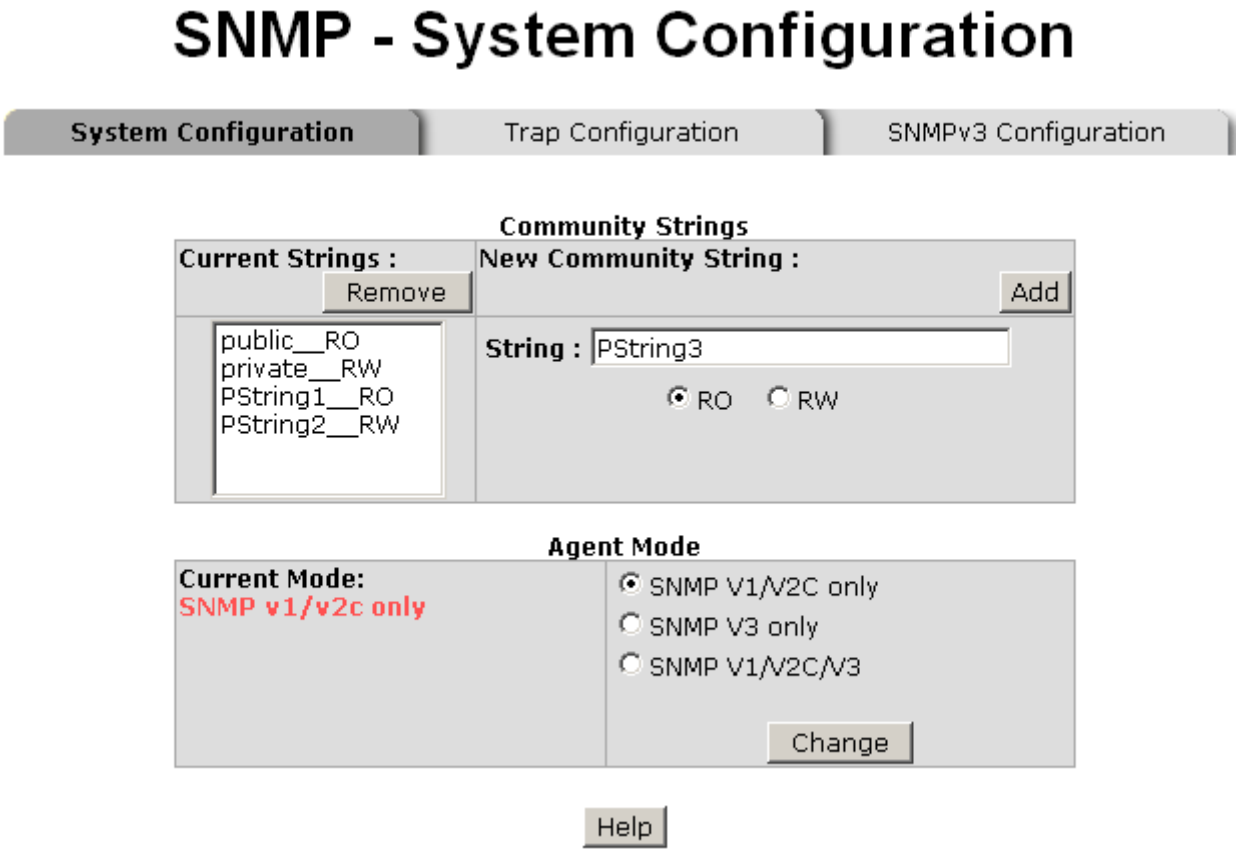
Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management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

System Configuration

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

- **String:** Enter the community string in the field as a password for authentication.
- **RO:** Read only. With this radio button selected, the community string is given the read-only permission for the MIB objects.
- **RW:** Read/write. With this radio button selected, the community string is given the read/write permission for the MIB objects.
- Click Add to finish adding a new community string.
- To remove a specific community string, select the community string shows in the list box and click Remove. The strings of Public_RO and Private_RW are default strings. You can remove them but after resetting the switch to default, the two strings show up again.

- **Agent Mode:** Click one of the radio buttons to select the SNMP version that the community string will use. And then click Change to ensure the selected SNMP version mode is changed.

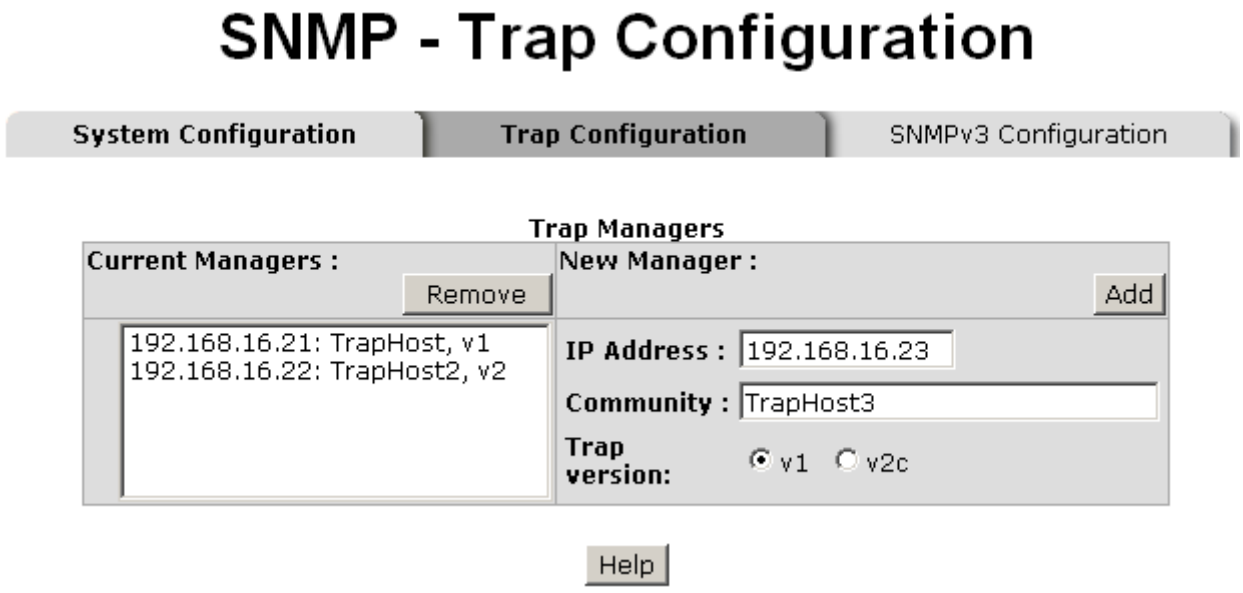


SNMP System Configuration interface

Trap Configuration

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

- **IP Address:** Enter the IP address of the trap manager.
- **Community:** Enter the community string for the trap station.
- **Trap Version:** Select the SNMP trap version—v1 or v2c.
- When finished, click Add.
- To remove a specific manager station, select the entries listed in the Current Managers field and click Remove.



Trap Managers interface

SNMPV3 Configuration

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

►Context Table

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

►User Table

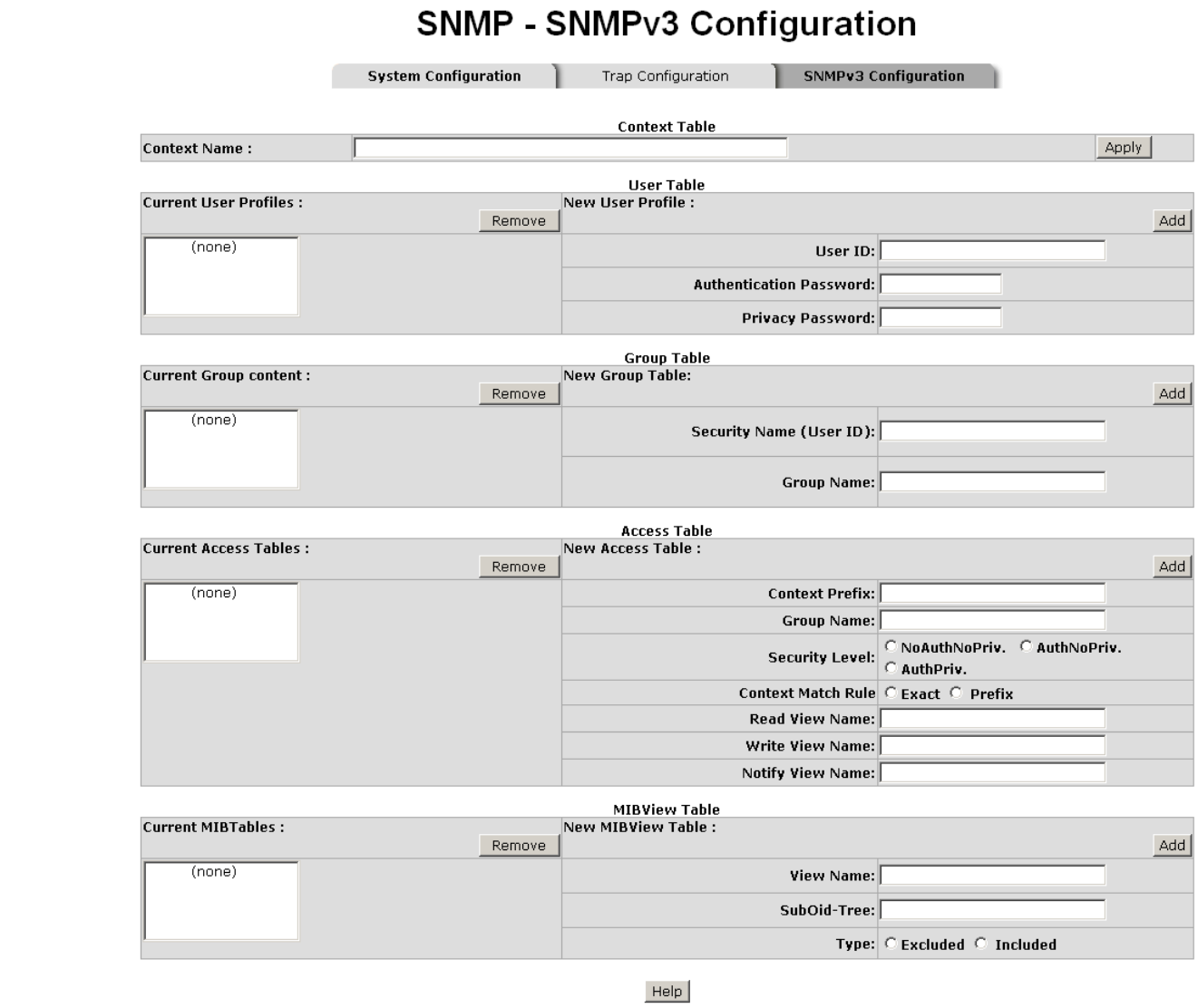
Configure the SNMPv3 user table.

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

►Group Table

Configure the SNMPv3 group table.

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



SNMPv3 configuration interface

►Access Table

Configure the SNMPv3 access table.

- **Context Prefix:** In this filed type in the prefix letters of the context name that is assigned in the context table.
- **Group Name:** Type in the group name that is assigned in the group table.
- **Security Level:** Select a radio button to determine which security level is assigned to the group. The options include:

  NoAuthNoPriv: Communications are made without authentication or encryption.

  AuthNoPriv: Communications are made with authentication but without encryption.

AuthPriv: Communications are made with authentication and encryption.

- **Context Match Rule:** Select the radio button to determine the context matching rule. You can configure it as a complete matching or prefix matching condition.
- **Read View Name:** Assign permission of reading to a user ID typed that exists in the User Table.
- **Write View Name:** Assign permission of writing to a user ID typed that exists in the User Table.
- **Notify View Name:** Assign permission of notifying to a user ID typed that exists in the User Table.
- Click Add to create a new access entry.
- Select an entry in the Current Access Tables listbox and click Remove to delete the unwanted access entry.

►MIBview Table

Configure the SNMPv3 MIB view table.

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

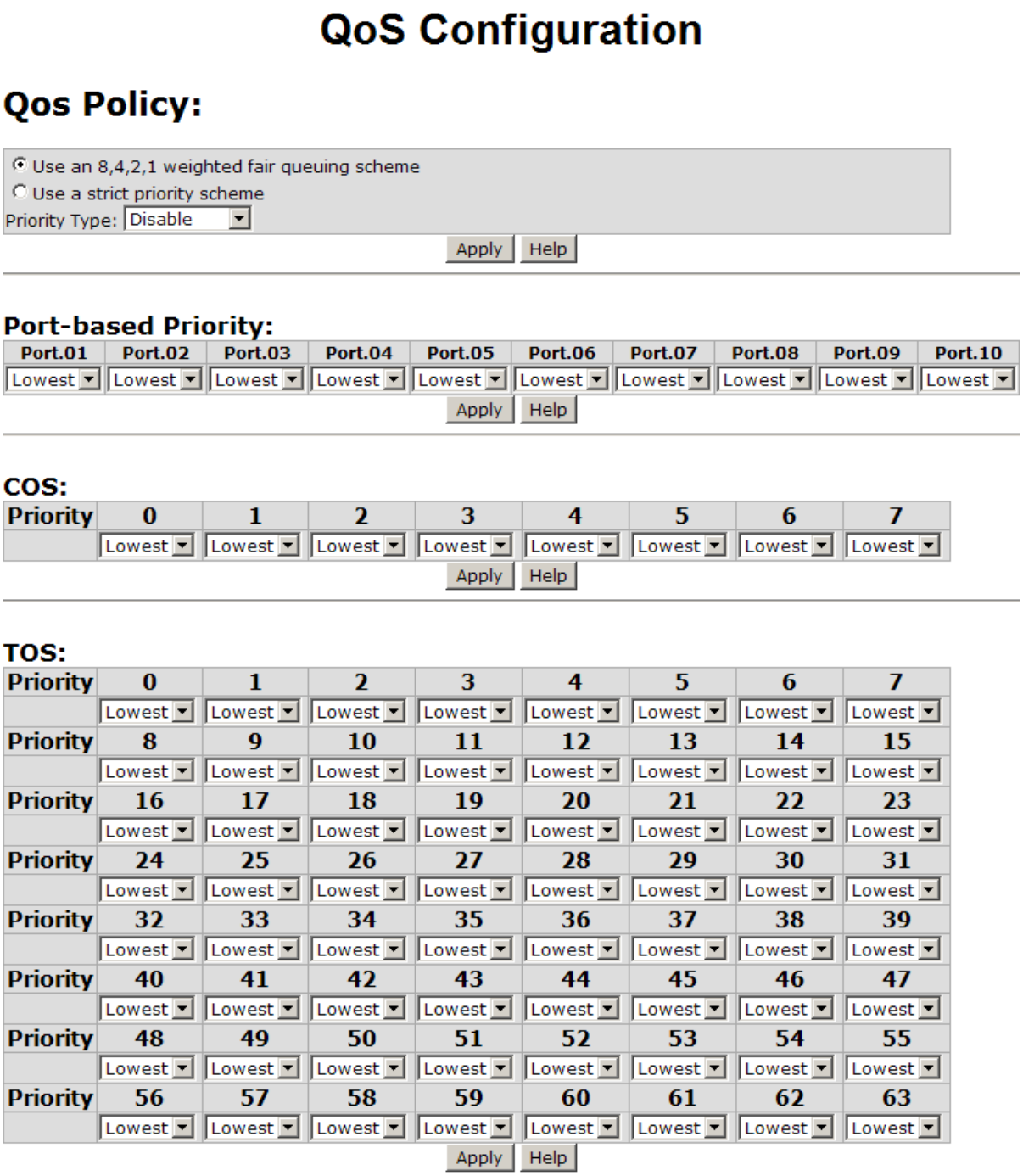
QoS Configuration

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

►QoS Policy

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

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



QoS Configuration interface

►Port-based Priority

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

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

►COS Configuration

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

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

►TOS Configuration

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

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

X-Ring2

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

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

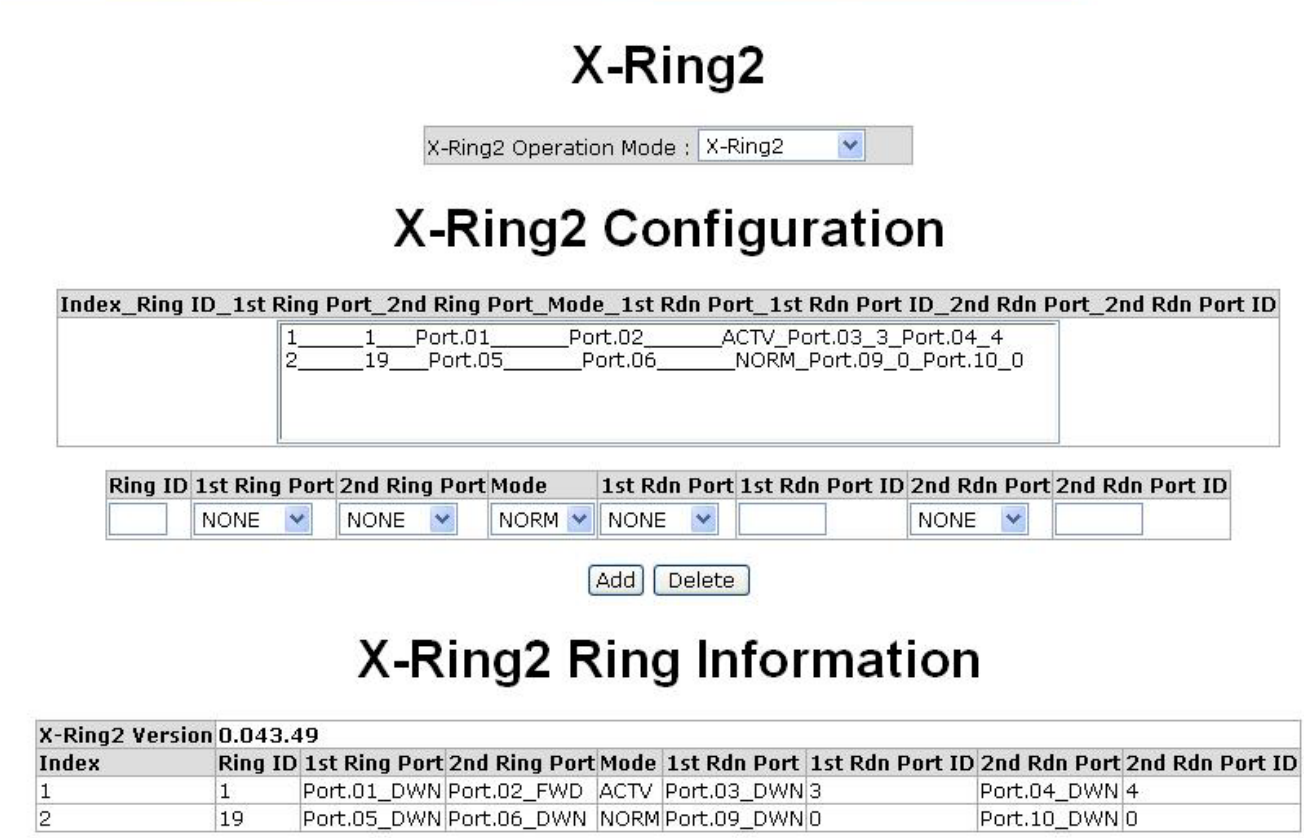
Other switches in the X-Ring group are naturally the working (forwarding) switches and both their two member ports are working (forwarding) ports. If the failure of network connection occurs, the backup ports of master switches (ring master devices) will automatically become working (forwarding) ports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

- **X-Ring2 Operation Mode:** Click the pull-down menu to configure the operation mode for X-Ring2 or disable the X-Ring2 function.

►X-Ring2 Mode

- **Ring ID:** Specify a number ranging from 0 to 99 for identifying a given ring group.
- **1st Ring Port:** One of the two member ports of this switch connecting to the ring group. Click the pull-down menu to select a port as the first ring port.
- **2nd Ring Port:** The other member port of this switch connecting to the ring group. Click the pull-down menu to select a port as the second ring port.
- **Mode:** Click the pull-down menu to select ACTV, PASV and NORM mode for connection of redundant ports.
- **1st Rdn Port:** Click the pull-down menu to select a port as the first redundant port.
- **1st Rdn Port ID:** Specify a number ranging from 0 to 99 for identifying the first redundant port.

- **2nd Rdn Port:** Click the pull-down menu to select a port as the second redundant port.
- **2nd Rdn Port ID:** Specify a number ranging from 0 to 99 for identifying the second redundant port.
- When finished, click the Apply button to have the configuration take effect.

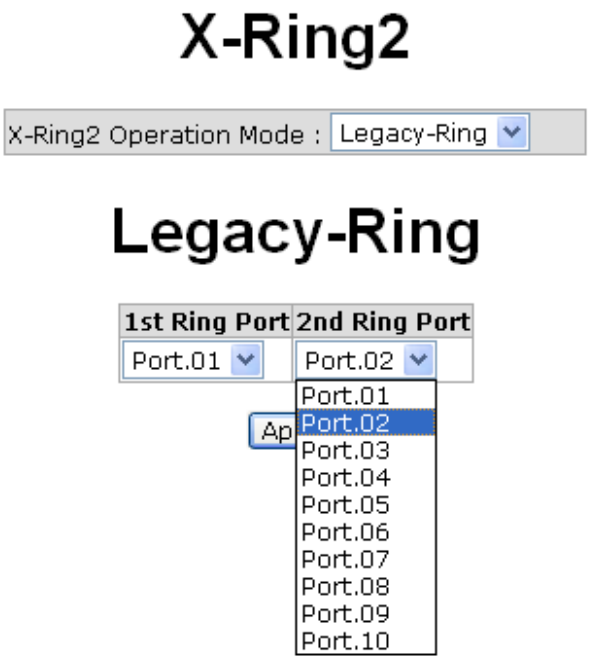


X-Ring2 Interface

►Legacy_Ring Mode

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

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



Legacy-Ring Interface

[NOTE]

1. When the X-Ring function is enabled, the user must disable the RSTP function. The X-Ring and RSTP functions cannot work simultaneously on a switch.
2. Remember to execute the “Save Configuration” action, otherwise the new configuration will lose when the switch powers off.

LLDP Configuration

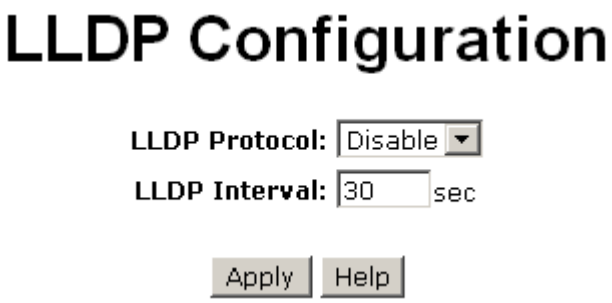
Link Layer Discovery Protocol (LLDP), a one way protocol, specified in the IEEE 802.1AB standard allows stations attached to the same IEEE 802 LAN to advertise their information to neighbors and store the information received from adjacent stations.

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

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

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

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



LLDP Interface

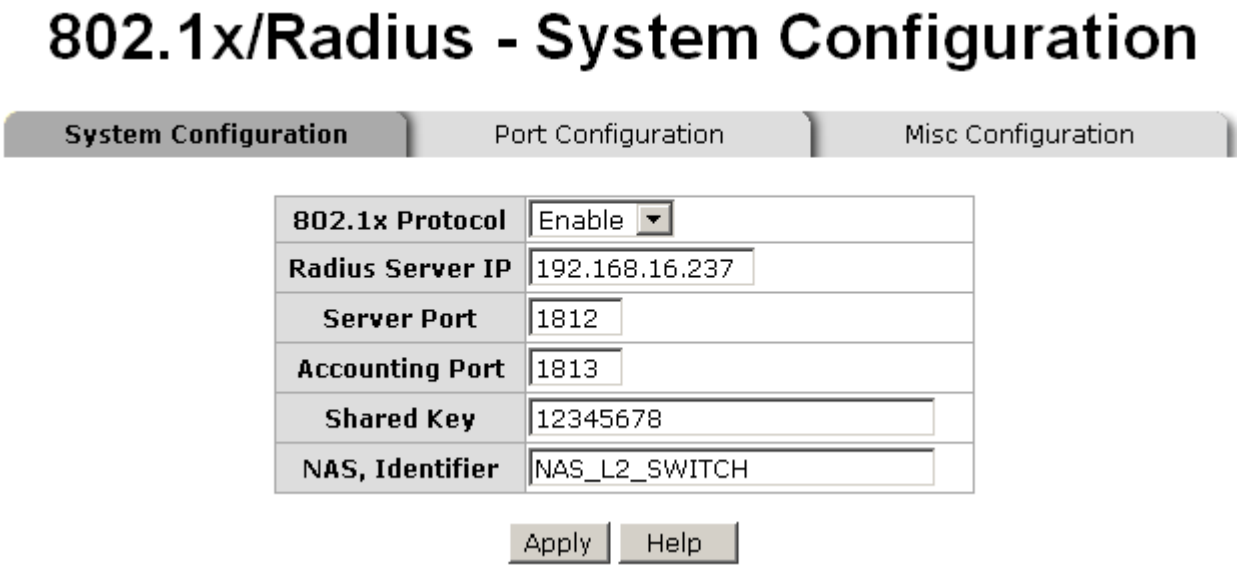
802.1X/Radius

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

System Configuration

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

- **IEEE 802.1x Protocol:** Click the pull-down menu to enable or disable the 802.1x protocol on the switch.
- **Radius Server IP:** Assign the RADIUS Server IP address.
- **Server Port:** Set the UDP destination port for authentication requests to the specified RADIUS Server.
- **Accounting Port:** Set the UDP destination port for accounting requests to the specified RADIUS Server.
- **Shared Key:** Set an encryption key for using during authentication sessions with the specified RADIUS server. This key must match the encryption key used on the RADIUS Server.
- **NAS, Identifier:** Set the identifier for the RADIUS client.
- Click the Apply button to have the configuration take effect.

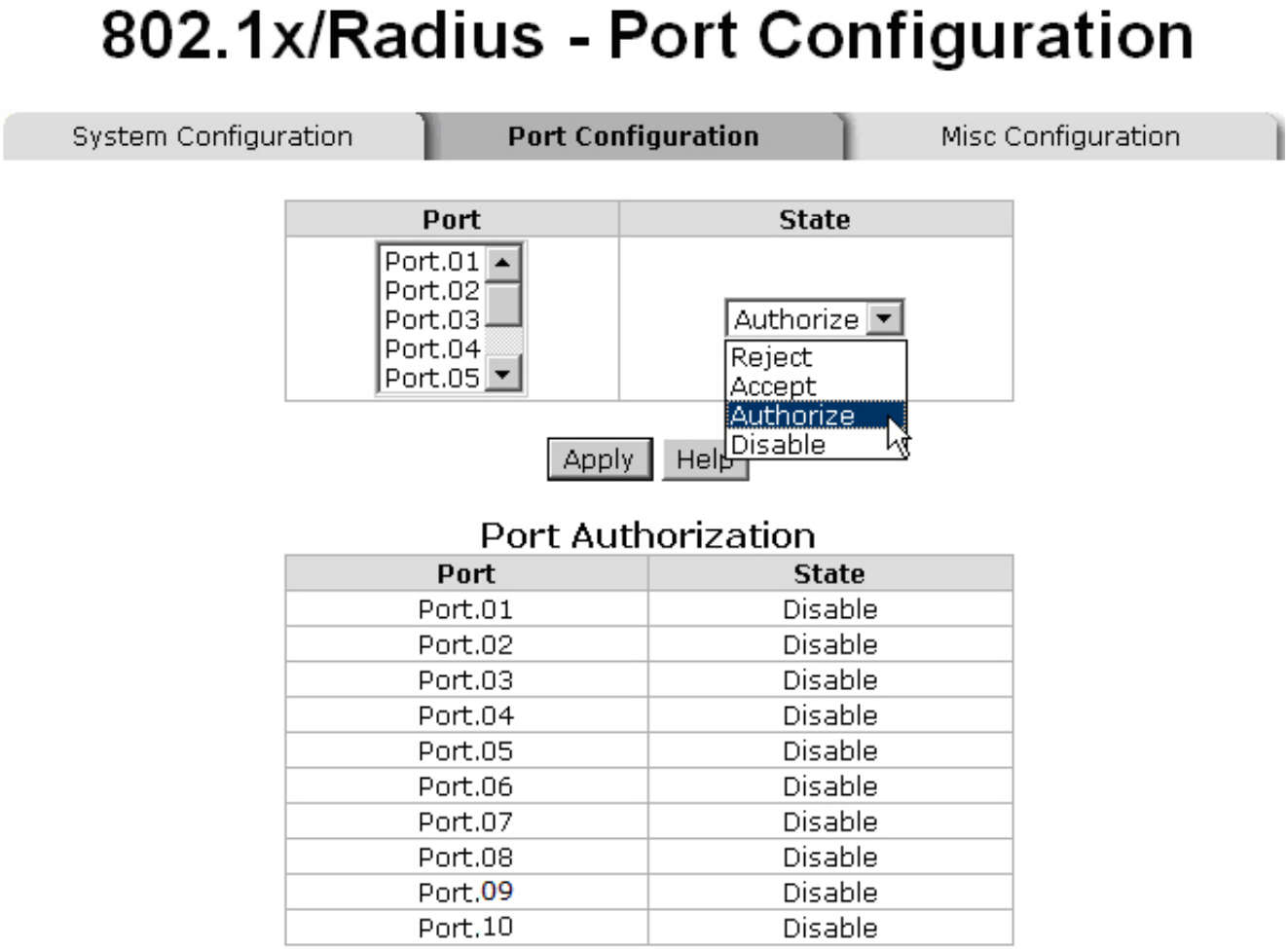


802.1x System Configuration interface

Port Configuration

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

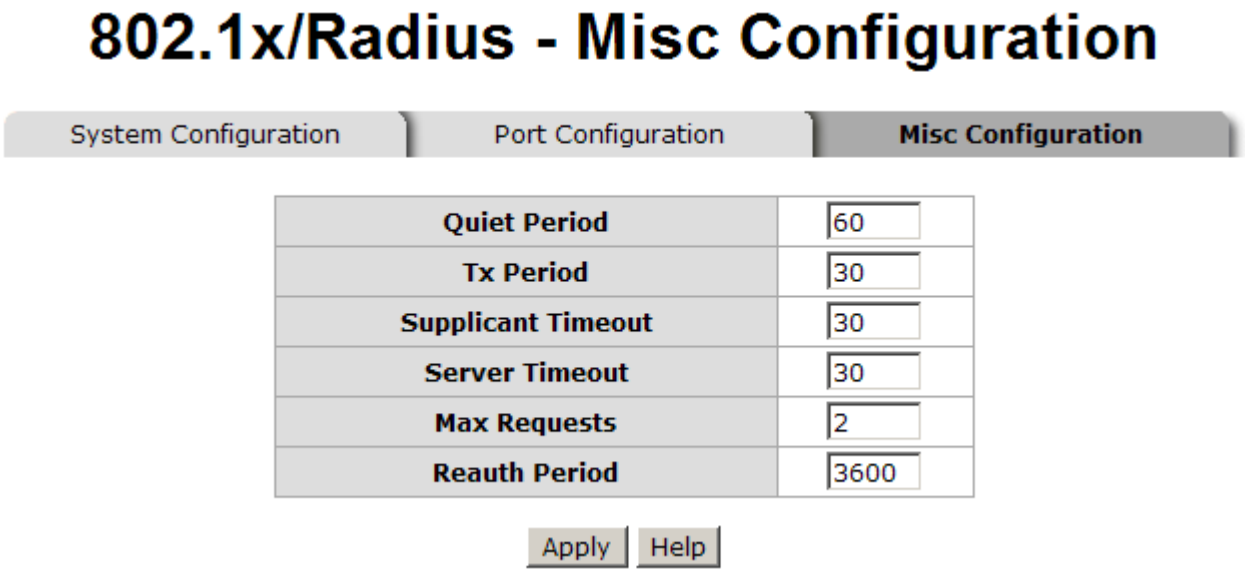
- **Reject:** The specified port is required to be held in the unauthorized state.
- **Accept:** The specified port is required to be held in the authorized state.
- **Authorize:** The specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the supplicant and the authentication server.
- **Disable:** When disabled, the specified port works without complying with 802.1x protocol.
- Click Apply to have the configuration take effect.



802.1x Per Port Setting interface

Misc Configuration

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



802.1x Misc Configuration interface

MAC Address Table

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

Static MAC Address

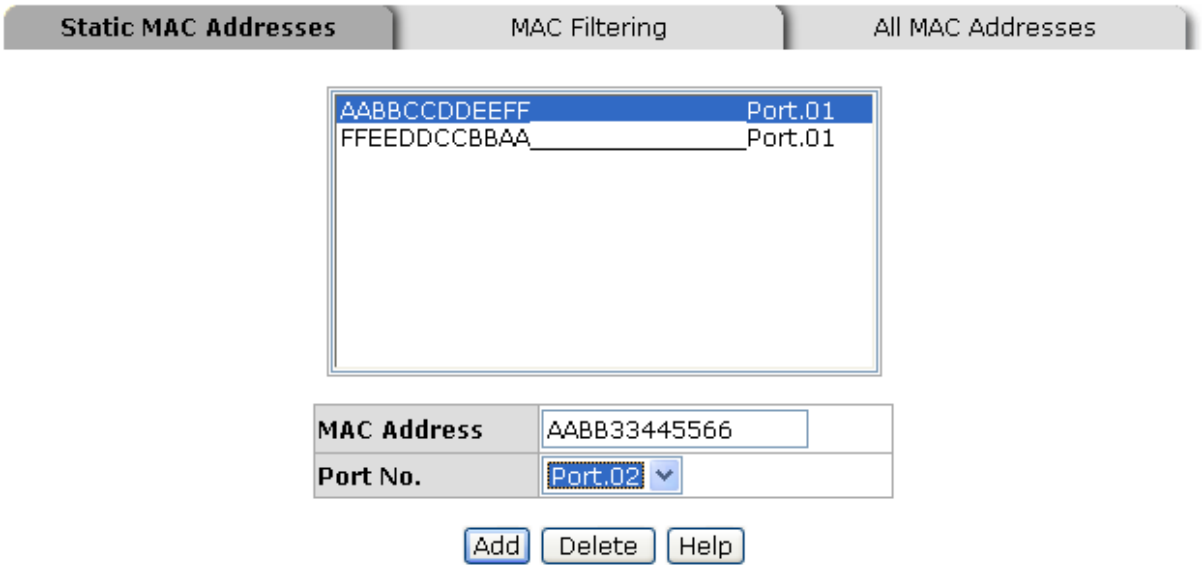
Configure the static MAC address tab to make a list in which traffic from devices with the MAC address included will pass the port. You can add a static MAC address that remains in the switch's address table regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. Via this interface, you can add, modify and delete entries of static MAC address.

Add the Static MAC Address

You can add static MAC addresses up to 256 entries in the switch MAC table here.

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

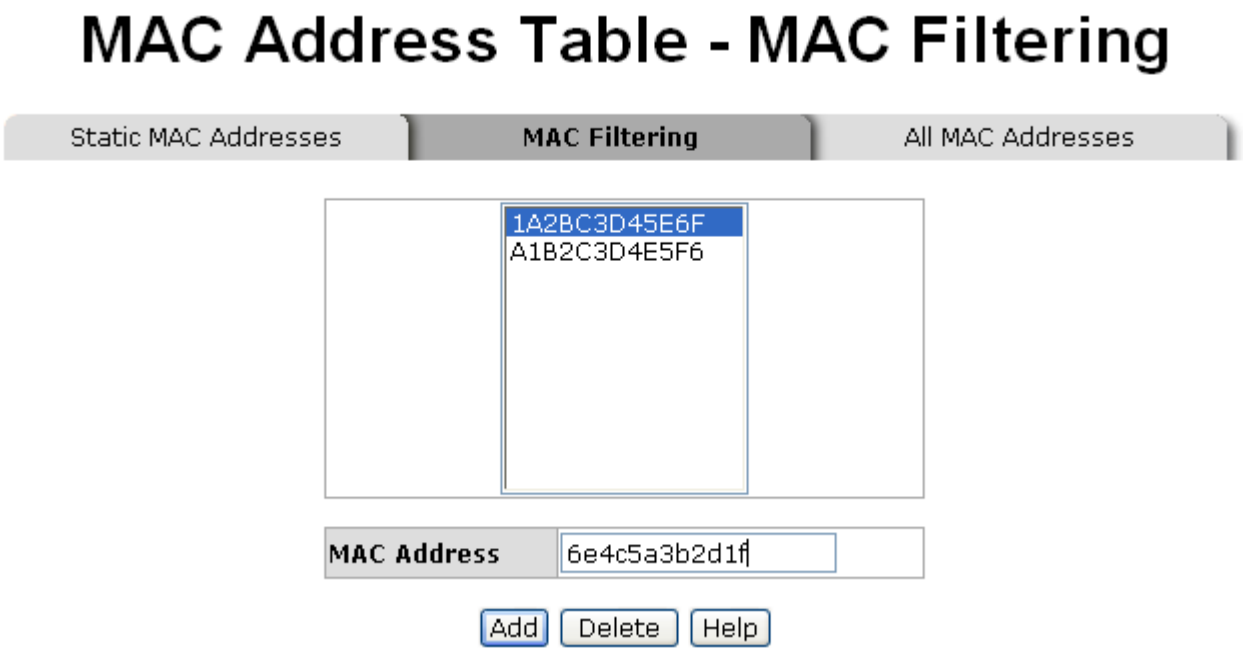
MAC Address Table - Static MAC Addresses



Static MAC Addresses interface

MAC Filtering

Traffic from devices with the MAC address listed in this table will be block by the switch.



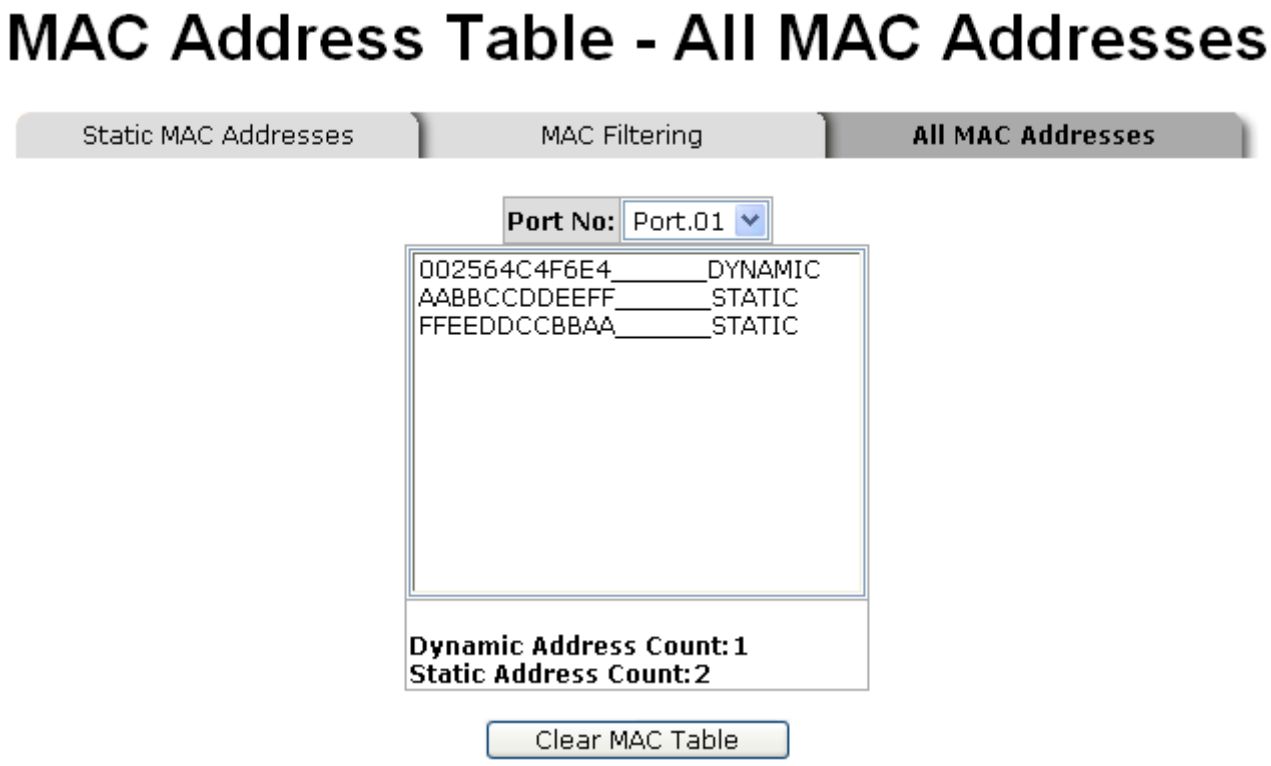
MAC Filtering interface

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

All MAC Addresses

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

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



All MAC Address interface

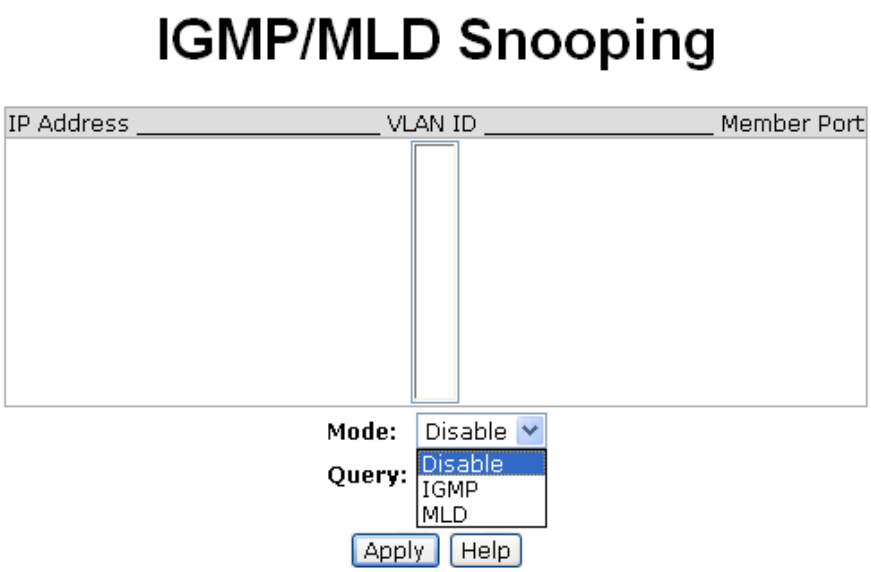
IGMP/MLD Snooping

IGMP is the protocol used by IPv4 systems to report their IP multicast group memberships to neighboring multicast routers. IGMPv3 adds support for "source filtering", that is, the ability for a system to report interest in receiving packets only from specific source addresses, or from all but specific source addresses, sent to a particular multicast address.

IGMP is used on IPv4 networks. To handle multicast management on IPv6 networks, Multicast Listener Discovery (MLD) is used in a similar way by IPv6 systems.

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

- **Mode:** Click the pull-down menu to specify the snooping mode, IGMP or MLD.
- **Query:** Click the pull-down menu to select the IGMP query functions including enable, disable and auto.
- Click Apply to have the configuration take effect.

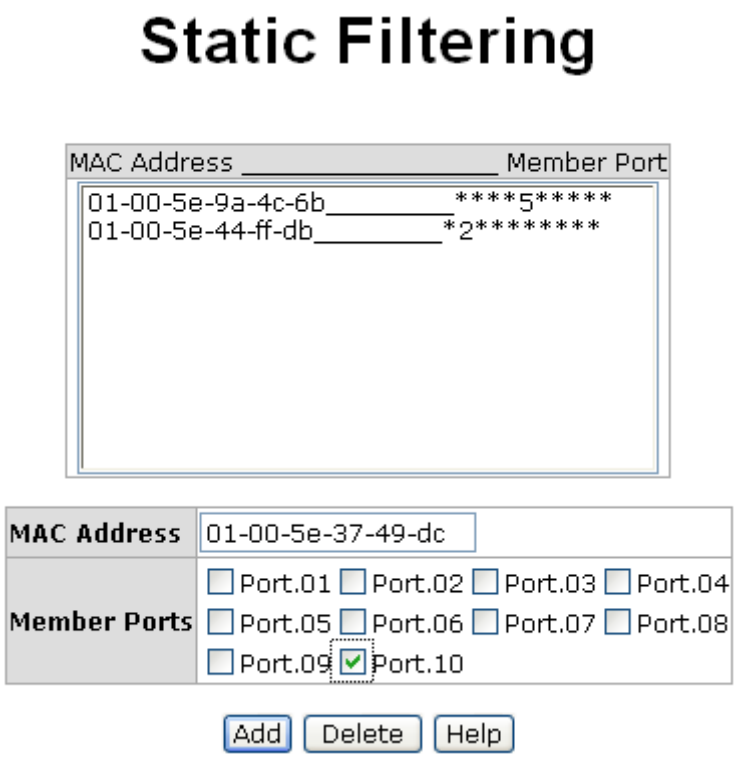


IGMP/MLD Snooping interface

Static Filtering

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

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



Static Filtering interface

Factory Default

Click the Reset button to reset the switch back to factory defaults. Before resetting, you can tick the checkboxes to keep the current IP address and user name/password.

Factory Default interface

Save Configuration

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

Save Configuration interface

System Reboot

Reboot the switch under software control. Click the Reboot button to restart the system.

System Reboot interface

Troubleshooting

- Verify that you are using the right power cord/adapter. Don't use the power adapter with DC output higher than the rated voltage of the switch. Or it will burn this switch down.
- Select the proper network cable to construct your network. Please check that you are using the right cable.
- **Diagnosing LED Indicators:** The Ethernet switch can be easily monitored through LED indicators on the front panel, 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 up 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.

Appendix A—Command Sets

Command Level

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

Modes	Access Method	Prompt	Exit Method	About This Model
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 commands are the advanced mode. Use this mode to • Display advance function states • Save configurations
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 to be applied to your switch.
VLAN database	Enter the vlan database command while in privileged	switch (vlan)#	To return to User EXEC mode, enter **exit**.	Use this mode to configure VLAN-specific parameters.

	EXEC mode.			
Interface configuration	Enter the interface command with a specific interface while in global configuration mode	switch (config-if)#	To return to the previous mode, enter **exit** or **end**.	Use this mode to configure parameters for the switch and Ethernet ports.

System Commands Set

Commands	Level	Description	Example
show config	**E**	Show switch configuration	switch>**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 lowip **[Low IP]**	**G**	Configure low IP address for IP pool	switch(config)#**dhcpserver lowip 192.168.1.100**
dhcpserver highip **[High IP]**	**G**	Configure high IP address for IP pool	switch(config)#**dhcpserver highip 192.168.1.200**
dhcpserver subnetmask **[Subnet mask]**	**G**	Configure subnet mask for DHCP clients	switch(config)#**dhcpserver subnetmask 255.255.255.0**
dhcpserver gateway [Gateway]	**G**	Configure gateway for DHCP clients	switch(config)#**dhcpserver gateway 192.168.1.254**
dhcpserver dnsip **[DNS IP]**	**G**	Configure DNS IP for DHCP clients	switch(config)#**dhcpserver dnsip 192.168.1.1**
dhcpserver leasetime **[Hours]**	**G**	Configure lease time (in hour)	switch(config)#**dhcpserver leasetime 1**
dhcpserver ipbinding **[IP address]**	**I**	Set static IP for DHCP clients by port	switch(config)#**interface fastEthernet 2** switch(config-if)#**dhcpserver ipbinding 192.168.1.1**
show dhcpserver	**P**	Show configuration of	switch#**show dhcpserver**

configuration		DHCP server	**configuration**
show dhcpserver clients	**P**	Show client entries of DHCP server	switch#**show dhcpserver clients**
show dhcpserver ip-binding	**P**	Show IP-Binding information of DHCP server	switch#**show dhcpserver ip-binding**
no dhcpserver	**G**	Disable DHCP server function	switch(config)#**no dhcpserver**
security enable	**G**	Enable IP security function	switch(config)#**security enable**
security http	**G**	Enable IP security of HTTP server	switch(config)#**security http**
security telnet	**G**	Enable IP security of telnet server	switch(config)#**security telnet**
security ip [Index(1..10)] [IP Address]	**G**	Set the IP security list	switch(config)#**security ip 1 192.168.1.55**
show security	**P**	Show the information of IP security	switch#**show security**
no security	**G**	Disable IP security function	switch(config)#**no security**
no security http	**G**	Disable IP security of HTTP server	switch(config)#**no security http**
no security telnet	**G**	Disable IP security of telnet server	switch(config)#**no security telnet**

Port Commands Set

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	switch(config)#**interface fastEthernet 2**

		command to specify the duplex mode of operation for Fast Ethernet.	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	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type**

		multicast frame'	**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** **workp** **[Workport]**	**G**	Assign a trunk group with LACP active. [GroupID] :1~4 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount	switch(config)#**aggregator group 1 1-4 lacp workp 2** or switch(config)#**aggregator group 2 1,4,3 lacp workp 3**

		of member ports.	
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 [TaggedVID List]**	**V**	Assign a trunk link for VLAN by port; if the port belongs to a trunk group, this command can't be applied.	switch(vlan)#**vlan 8021q port 3 trunk-link tag 2,3,6,99** or switch(vlan)#**vlan 8021q port 3 trunk-link tag 3-20**
vlan 8021q port [PortNumber] **hybrid-link untag [UntaggedVID]** **tag [TaggedVID List]**	**V**	Assign a hybrid link for VLAN by port; if the port belongs to a trunk group, this command can't be applied.	switch(vlan)#**vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8** or switch(vlan)#**vlan 8021q port 3 hybrid-link untag 5 tag 6-8**
vlan 8021q trunk [PortNumber]	**V**	Assign a access link	switch(vlan)#**vlan 8021q trunk 3**

access-link untag [UntaggedVID]		for VLAN by trunk group	**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 [seconds]	**G**	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge	switch(config)#**spanning-tree max-age 15**

		protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	
spanning-tree hello-time [seconds]	**G**	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#**spanning-tree hello-time 3**
spanning-tree forward-time [seconds]	**G**	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	switch(config)#**spanning-tree forward-time 20**
stp-path-cost [1~200000000]	**I**	Use the spanning-tree cost interface configuration command to set the	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-path-cost 20**

		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.	
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	switch>**show spanning-tree**

		states.	
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 enable	**G**	Set IGMP query to force mode	switch(config)#**igmp query enable**
igmp unregister flooding	**G**	Set unregister stream flooding	switch(config)#**igmp unregister flooding**

igmp unregister blocking	**G**	Set unregister stream blocking	switch(config)#**igmp unregister blocking**
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 filter	**P**	Show filter MAC address table.	switch#**show mac-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	**G**	Remove an entry of	switch(config)#**no**

filter hwaddr **[MAC]**		MAC address table (filter)	**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]**	**G**	Configure the userprofile for SNMPV3 agent. Privacy password	switch(config)#**snmpv3 user test01 group G1 password AuthPW PrivPW**

password [Authentication Password] [Privacy Password]		could be empty.	
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 command to change the accounting port	switch(config)# **8021x system accountport 1816**
8021x system sharekey [ID]	**G**	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)# **8021x system 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	switch(config)# **8021x misc reauthperiod 3000**

		configuration command to set the reauth period.	
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 server and the file name of image.	switch(config)#**restore flash:restore_cfg**
upgrade flash:upgrade_fw	**G**	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#**upgrade flash:upgrade_fw**

SystemLog, SMTP and Event Commands Set

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	G	Set X-ring topology	switch(config)#**event**

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

SNTP Commands Set

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	switch(config)#**sntp daylight**

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

X-ring Commands Set

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