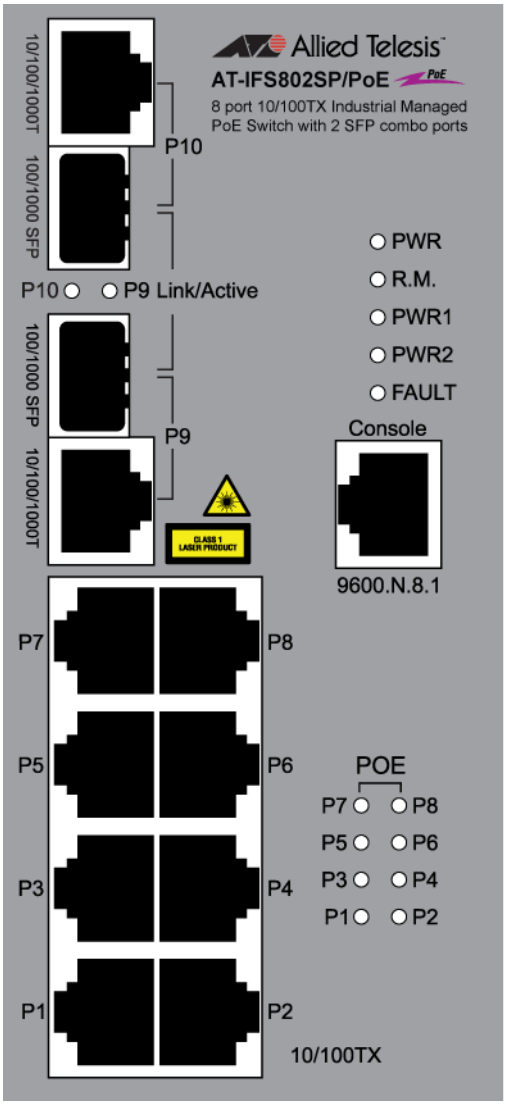
AT-IFS802SP/POE

8x10/100TX POE Layer 2 Managed Industrial Switch



AT-IFS802SP/POE Installation and User's Guide

613-001691 Rev.A

Copyright © 2012 Allied Telesis, Inc.

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc.

Allied Telesis and the Allied Telesis logo are trademarks of Allied Telesis, Incorporated. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.

Electrical Safety and Emissions Standards

This product meets the following standards.

U.S. Federal Communications Commission

Radiated Energy

Note: This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Note: Modifications or changes not expressly approved of by the manufacturer or the FCC, can void your right to operate this equipment.

Industry Canada

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

RFI Emissions	FCC Class A, CE EN61000-4-2, CE EN61000-4-3, CE EN-61000-4-4, CE EN61000-4-5, CE EN61000-4-6, CE EN61000-4-8, CE EN61000-4-11, CE EN61000-4-12, CE EN61000-6-2, CE EN61000-6-4

Warning: In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Electrical Safety	UL, cUL, CE/EN60950-1
Stability Testing	IEC60068-2-32 (Free fall), IEC60068-2-27 (Shock), IEC60068-2-6 (Vibration)

Preface

This manual is the installation and management guide for the AT-IFS802SP/POE 8x10/100TX POE Layer 2 Managed Industrial Switch. The instructions in this guide explain how to install the switch, start a management session, and use the CLI and web management interfaces.

Allied Telesis Contact Information

If you need assistance with this product, you may contact Allied Telesis technical support by going to the Support & Services section of the Allied Telesis web site at **www.alliedtelesis.com/support**. You can find links for the following services on this page:

- 24/7 Online Support - Enter our interactive support center to search for answers to your questions in our knowledge database, check support tickets, learn about RMAs, and contact Allied Telesis technical experts.
- USA and EMEA phone support - Select the phone number that best fits your location and customer type.
- Hardware warranty information - Learn about Allied Telesis warranties and register your product online.
- Replacement Services - Submit a Return Merchandise Authorization (RMA) request via our interactive support center.
- Documentation - View the most recent installation guides, user guides, software release notes, white papers and data sheets for your product.
- Software Updates - Download the latest software releases for your product.

For sales or corporate contact information, go to **www.alliedtelesis.com/purchase** and select your region.

Content

Chapter 1 Introduction 6
1.1 Hardware Features 6
1.2 Software Features 8
1.3 Package Contents 9
Chapter 2 Hardware Description 10
2.1 Physical Dimension 10
2.2 Front Panel 10
2.3 Bottom View 11
2.4 LED Indicators 12
Chapter 3 Hardware Installation 13
3.1 Installation Steps 13
3.2 DIN-Rail Mounting 14
3.3 Wall Mount Plate Mounting 15
3.4 Wiring the Power Inputs 16
3.5 Wiring the Fault Alarm Contact 17
3.6 Cabling 18
Chapter 4 Network Application 20
4.1 X-Ring Application 20
4.2 Coupling Ring Application 21
4.3 Dual Homing Application 22
Chapter 5 Console Management 23
5.1 Connecting to the Console Port 23
5.2 Pin Assignment 23
5.3 Login in the Console Interface 24
5.4 CLI Management 24
5.5 Commands Level 25
Chapter 6 Web-Based Management 26
6.1 About Web-based Management 26
6.2 Preparing for Web Management 26
6.3 System Login 26
6.4 System Information 27
6.5 IP Configuration 28
6.6 DHCP Server 29
6.6.1 System configuration 29
6.6.2 Client Entries 30
6.6.3 Port and IP Bindings 30
6.7 TFTP 31
6.7.1 Update Firmware 31
6.7.2 Restore Configuration 31
6.7.3 Backup Configuration 32
6.8 System Event Log 32
6.8.1 Syslog Configuration 32
6.8.2 System Event Log—SMTP Configuration 33
6.8.3 System Event Log - Event Configuration 34

6.9 Fault Relay Alarm 36
6.10 SNTP Configuration 36
6.11 IP Security 39
6.12 User Authentication 40
6.13 Port Statistics 40
6.14 Port Control 41
6.15 Port Trunk 42
6.15.1 Aggregator setting 42
6.15.2 Aggregator Information 44
6.15.3 State Activity 47
6.16 Port Mirroring 48
6.17 Rate Limiting 49
6.18 VLAN configuration 50
6.18.1 Port-based VLAN 50
6.18.2 802.1Q VLAN 52
802.1Q Configuration 53
6.19 Rapid Spanning Tree 55
6.19.1 RSTP System Configuration 55
6.19.2 Port Configuration 56
6.20 SNMP Configuration 57
6.20.1 System Configuration 57
6.20.2 Trap Configuration 58
6.20.3 SNMPV3 Configuration 59
6.21 QoS Configuration 60
6.21.1 QoS Policy and Priority Type 60
6.21.2 Port-based Priority 61
6.21.3 COS Configuration 62
6.21.4 TOS Configuration 62
6.22 IGMP Configuration 62
6.23 X-Ring 63
6.24 LLDP Configuration 65
6.25 Security—802.1X/Radius Configuration 65
6.25.1 System Configuration 65
6.25.2 Port Configuration 66
6.25.3 Misc Configuration 67
6.26 MAC Address Table 67
6.26.1 Static MAC Address 67
6.26.2 MAC Filtering 68
6.26.3 All MAC Addresses 69
6.26.4 MAC Address Table—Multicast Filtering 69
6.27 Power over Ethernet 71
6.28 Factory Default 73
6.29 Save Configuration 73
6.30 System Reboot 73
Troubles shooting 74
Appendix A—RJ-45 Pin Assignment 75
RJ-45 Pin Assignments 75
RJ-45 Pin Assignments of POE 78
Appendix B—Command Sets 79

System Commands Set....79
Port Commands Set....81
Trunk Commands Set....83
VLAN Commands Set....84
Spanning Tree Commands Set....86
QOS Commands Set....88
IGMP Commands Set....89
Multicast Filtering Commands Set....90
LLDP Commands Set....90
Mac / Filter Table Commands Set....90
SNMP Commands Set....91
Port Mirroring Commands Set....93
802.1x Commands Set....94
TFTP Commands Set....96
SystemLog, SMTP and Event Commands Set....97
Fault Relay Alarm Commands Set....98
SNTP Commands Set....99
X-ring Commands Set....100
PoE Commands Set....101

Chapter 1 Introduction

The 8 10/100TX + 2 10/100/1000T/Mini-GBIC Combo with 8 PoE Injectors Managed Industrial Switch is a cost-effective solution and meets the high reliability requirements demanded by industrial applications. Using fiber port can extend the connection distance that increases the network elasticity and performance. Besides, the industrial switch provides the PoE function for kinds of Powered Devices to receive power as well as data over the RJ-45 cable.

1.1 Hardware Features

Standard	IEEE 802.3 10Base-T Ethernet IEEE 802.3u 100Base-TX/ FX IEEE802.3ab 1000Base-T IEEE802.3z Gigabit fiber IEEE802.3x Flow Control and Back Pressure IEEE802.3ad Port trunk with LACP IEEE802.3af Power over Ethernet IEEE802.1d Spanning Tree/ IEEE802.1w Rapid Spanning Tree IEEE802.1p Class of Service IEEE802.1Q VLAN Tag IEEE 802.1x User Authentication (Radius) IEEE802.1ab LLDP
Switch Architecture	Back-plane (Switching Fabric): 5.6Gbps Packet throughput ability(Full-Duplex): 8.3Mpps @64bytes
Transfer Rate	14,880pps for Ethernet port 148,800pps for Fast Ethernet port 1,488,000pps for Gigabit Fiber Ethernet port
Packet Buffer	1Mbits
MAC Address	8K MAC address table
Flash ROM	4Mbytes
DRAM	32Mbytes
Connector	10/100TX: 8 x RJ-45 10/100/1000T/ SFP Combo: 2 x RJ-45 + 2 x 100/1000 SFP sockets RS-232 connector: RJ-45 type

Network Cable	10Base-T: 2-pair UTP/STP Cat. 3, 4, 5/ 5E cable EIA/TIA-568 100-ohm (100m) 100Base-TX: 2-pair UTP/STP Cat. 5/ 5E cable EIA/TIA-568 100-ohm (100m) 1000Base-TX: 2-pair UTP/STP Cat. 5/ 5E cable EIA/TIA-568 100-ohm (100m)
Optical Fiber	Distance: Multi mode: 0 to 5 km, 1300 nm (50/125 µm, 800 MHz*km) 0 to 4 km, 1300 nm (62.5/125 µm, 500 MHz*km) Single mode: 0 to 40 km, 1310 nm (9/125 µm, 3.5 PS/(nm*km)) 0 to 80 km, 1550 nm (9/125 µm, 19 PS/(nm*km)) Min. TX Output: Multi mode: -20 dBm Single mode: 0 to 40 km, -5 dBm; 0 to 80 km, -5 dBm Max. TX Output: Multi mode: -14 dBm Single mode: 0 to 40 km, 0 dBm; 0 to 80 km, 0 dBm Sensitivity: -36 to -32 dBm (Single mode); -34 to -30 dBm (Multi mode)
PoE pin assignment	RJ-45 port # 1~# 8 support IEEE 802.3af End-point, Alternative A mode. Per port provides 15.4W ability. Positive (VCC+): RJ-45 pin 1,2. Negative (VCC-): RJ-45 pin 3,6.
Protocol	CSMA/CD
LED	Per unit: Power (Green), Power 1 (Green), Power 2 (Green), Fault (Red), Master (Green), FWD (Green) 8 port 10/100: Link/Activity (Green), Full duplex/Collision (Amber) SFP port: LNK/ACT(Green), 1000T: LNK/ACT(Green), 1000M(Green)
Power Supply	External Power Supply: DC 48V, Redundant power DC 48V and connective removable terminal block for master and slave power
Power	116Watts (Full load)
Operating Humidity	5% to 95% (Non-condensing)
Operating Temperature	PIFE-802GBTMA: -10°C ~ 60°C PIFE-802GBTMAE: -40°C ~ 75°C
Storage Temperature	-40°C ~ 85°C
Case Dimension	IP-30, 72mm (W) x 105mm (D) x 152mm (H)
Installation	DIN rail and wall mount ear

EMI	FCC Class A, CE EN61000-4-2, CE EN61000-4-3, CE EN-61000-4-4, CE EN61000-4-5, CE EN61000-4-6, CE EN61000-4-8, CE EN61000-4-11, CE EN61000-4-12, CE EN61000-6-2, CE EN61000-6-4
Safety	UL, cUL, CE/EN60950-1
Stability Testing	IEC60068-2-32 (Free fall), IEC60068-2-27 (Shock), IEC60068-2-6 (Vibration)

1.2 Software Features

Management	SNMP v1 v2c, v3/ Web/Telnet/CLI
SNMP MIB	RFC 1215 Trap, RFC1213 MIBII, RFC 1157 SNMP MIB, RFC 1493 Bridge MIB, RFC 2674 VLAN MIB, RFC 1643 , RFC 1757, RSTP MIB, Private MIB, LLDP MIB
VLAN	Port Based VLAN IEEE 802.1Q Tag VLAN (256 entries)/ VLAN ID (Up to 4K, VLAN ID can be assigned from 1 to 4094.) GVRP (256 Groups)
Port Trunk with LACP	LACP Port Trunk: 4 Trunk groups/Maximum 4 trunk members
LLDP	Supports LLDP allowing switch to advertise its identification and capability on the LAN
Spanning tree	IEEE802.1d spanning tree IEEE802.1w rapid spanning tree.
X-Ring	Supports X-ring, Dual Homing and Couple Ring Topology Provides redundant backup feature and the recovery time below 20ms
Quality of Service	The quality of service determined by port, Tag and IPv4 Type of service, IPv4 Different Service
Class of Service	Supports IEEE802.1p class of service, per port provides 4 priority queues
Port Security	Supports 100 entries of MAC address for static MAC and another 100 for MAC filter
Port Mirror	Supports 3 mirroring types: "RX, TX and Both packet".
IGMP	Supports IGMP snooping v1,v2, 256 multicast groups and IGMP query
IP Security	Supports 10 IP addresses that have permission to access the switch management and to prevent unauthorized intruder.

Login Security	Supports IEEE802.1X Authentication/RADIUS
Bandwidth Control	Support ingress packet filter and egress packet limit The egress rate control supports all of packet type and the limit rates are 100K~102400Kbps(10/100), 100K~256000Kbps(1000) Ingress filter packet type combination rules are Broadcast/Multicast/Unknown Unicast packet, Broadcast/Multicast packet, Broadcast packet only and all of packet. The packet filter rate can be set from 100K~102400Kbps(10/100), 100K~256000Kbps(1000)
Flow Control	Supports Flow Control for Full-duplex and Back Pressure for Half-duplex
System Log	Supports System log record and remote system log server
SMTP	Supports SMTP Server and 6 e-mail accounts for receiving event alert
Relay Alarm	Provides one relay output for port breakdown, power fail Alarm Relay current carry ability: 1A @ DC24V
SNMP Trap	1. Cold start 2. Link up/down 3. X-Ring topology changed 4. Authorization fail 5. PD disconnect trap-PoE port event
DHCP	Provides DHCP Client/ DHCP Server/ Port and IP Binding
DNS	Provides DNS client feature and supports Primary and Secondary DNS server
SNTP	Supports SNTP to synchronize system clock in Internet
Firmware Update	Supports TFTP firmware update, TFTP backup and restore.
Configuration Upload/Download	Supports binary format file for configuration backup and restore
ifAlias	Each port allows importing 128bits of alphabetic string of word on SNMP and CLI interface

1.3 Package Contents

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

- 8 10/100TX + 2 10/100/1000T/Mini-GBIC Combo with 8 PoE Injectors Managed Industrial Switch x 1
- Pluggable Terminal Block x 1
- Mounting plate x 2
- RJ-45 to DB9-Female cable x 1

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.

Chapter 2 Hardware Description

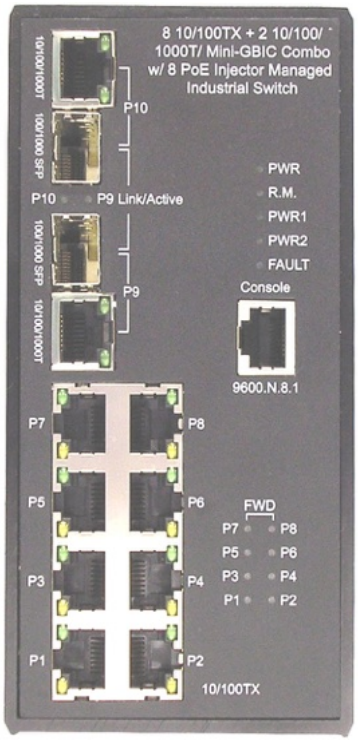
In this paragraph, it will describe the Industrial switch's hardware spec, port, cabling information, and wiring installation.

2.1 Physical Dimension

8 10/100TX w/ X-Ring Managed Industrial Switch dimension (W x D x H) is **72mm x 105mm x 152mm**

2.2 Front Panel

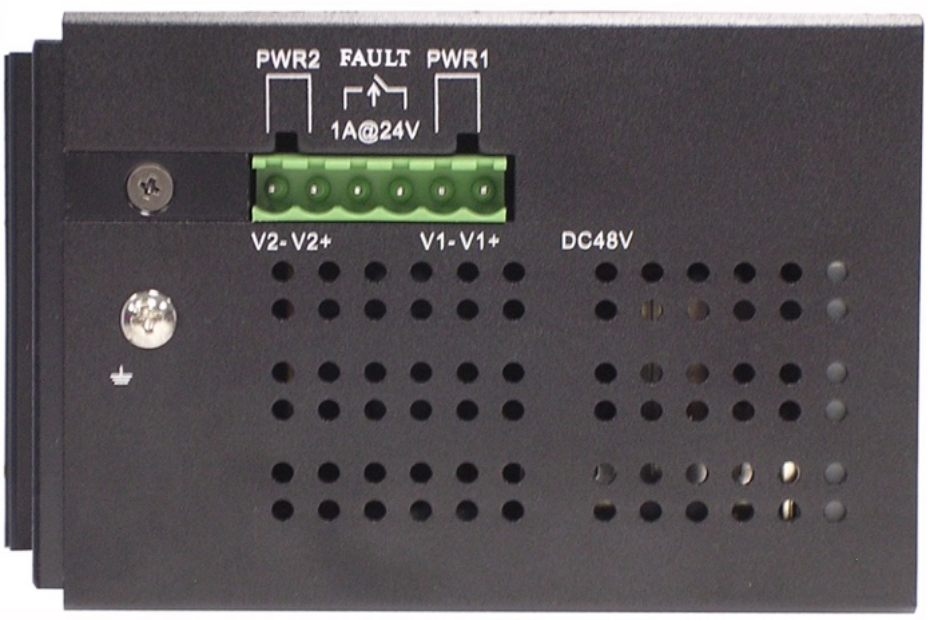
The Front Panel of the 8 10/100TX w/ X-Ring Managed Industrial Switch is shown as below:



Front Panel of the industrial switch

2.3 Bottom View

The bottom panel of the 8 10/100TX w/ X-Ring Managed Industrial Switch has one terminal block connector of two DC power inputs and one fault alarm.



Bottom Panel of the industrial switch

2.4 LED Indicators

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

LED	Color	Status	Meaning
PWR	Green	On	The switch unit is power on
		Off	No power
R.M.	Green	On	The industrial switch is the master of X-Ring group
		Off	The industrial switch is not a ring master in X-Ring group
PWR1	Green	On	Power 1 is active
		Off	Power 1 is inactive
PWR2	Green	On	Power 2 is active
		Off	Power 2 is inactive
FAULT	Red	On	Power or port failure
		Off	No failure
P9, P10 (RJ-45)	Green (Upper LED)	On	A network device is detected.
		Blinking	The port is transmitting or receiving packets from the TX device.
		Off	No device attached
	Green (Lower LED)	On	1000M
		Off	10/100M
Link/Active (P9, P10 SFP)	Green	On	The SFP port is linking
		Blinks	The port is transmitting or receiving packets from the TX device.
		Off	No device attached
P1 ~ P8	Green	On	A network device is detected.
		Blinking	The port is transmitting or receiving packets from the TX device.
		Off	No device attached
	Amber	On	The port is operating in full-duplex mode.
		Blinking	Collision of Packets occurs.
		Off	The port is in half-duplex mode or no device is attached.
FWD (P1 ~ P8)	Green	Green	A powered device is connected utilizing Power over Ethernet on the port
		Off	No device is connected or power forwarding fails

Chapter 3 Hardware Installation

In this paragraph, we will describe how to install the 8 10/100TX w/ X-Ring Managed Industrial Switch and the installation points attended to it.

3.1 Installation Steps

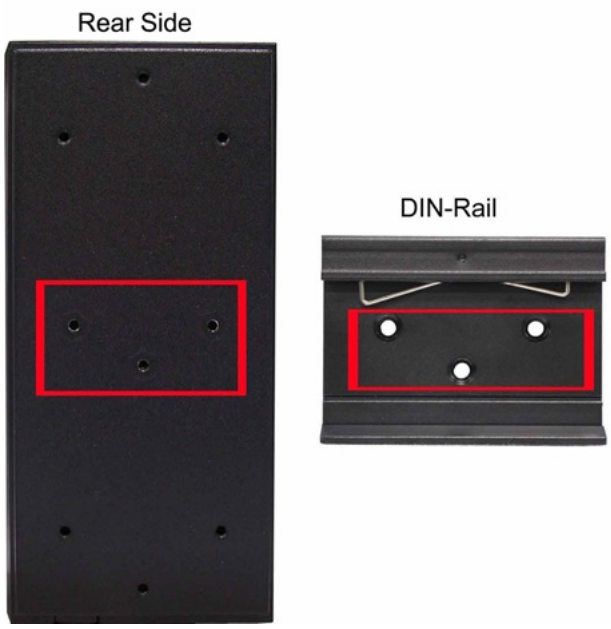
1. Unpack the Industrial switch
2. Check if the DIN-Rail is screwed on the Industrial switch or not. If the **DIN-Rail** is not screwed on the Industrial switch, please refer to DIN-Rail Mounting section for DIN-Rail installation. If users want to wall mount the Industrial switch, please refer to **Wall Mount Plate Mounting** section for wall mount plate installation.
3. To hang the Industrial switch on the DIN-Rail track or wall.
4. Power on the Industrial switch. Please refer to the Wiring the Power Inputs section for knowing the information about how to wire the power. The power LED on the Industrial switch will light up. Please refer to the LED Indicators section for indication of LED lights.
5. Prepare the twisted-pair, straight through Category 5 cable for Ethernet connection.
6. sert one side of RJ-45 cable (category 5) into the Industrial switch Ethernet port (RJ-45 port) and another side of RJ-45 cable (category 5) to the network device's Ethernet port (RJ-45 port), ex: Switch PC or Server. The UTP port (RJ-45) LED on the Industrial switch will light up when the cable is connected with the network device. Please refer to the **LED Indicators** section for LED light indication.

[note]	Make sure that the connected network devices support MDI/MDI-X. If it does not support, use the crossover category-5 cable.

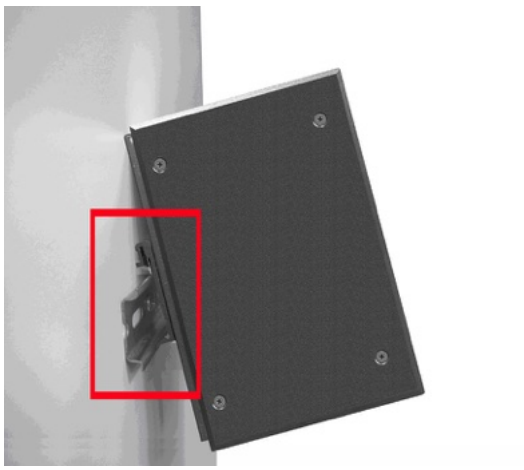
7. When all connections are set and LED lights all show in normal, the installation is complete.

3.2 DIN-Rail Mounting

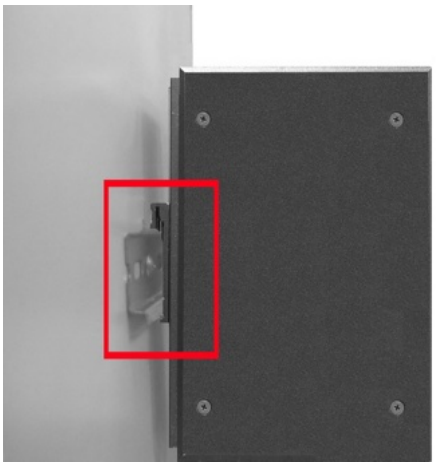
The DIN-Rail is screwed on the industrial switch when out of factory. If the DIN-Rail is not screwed on the industrial switch, please see the following pictures to screw the DIN-Rail on the switch. Follow the steps below to hang the industrial switch.



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



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

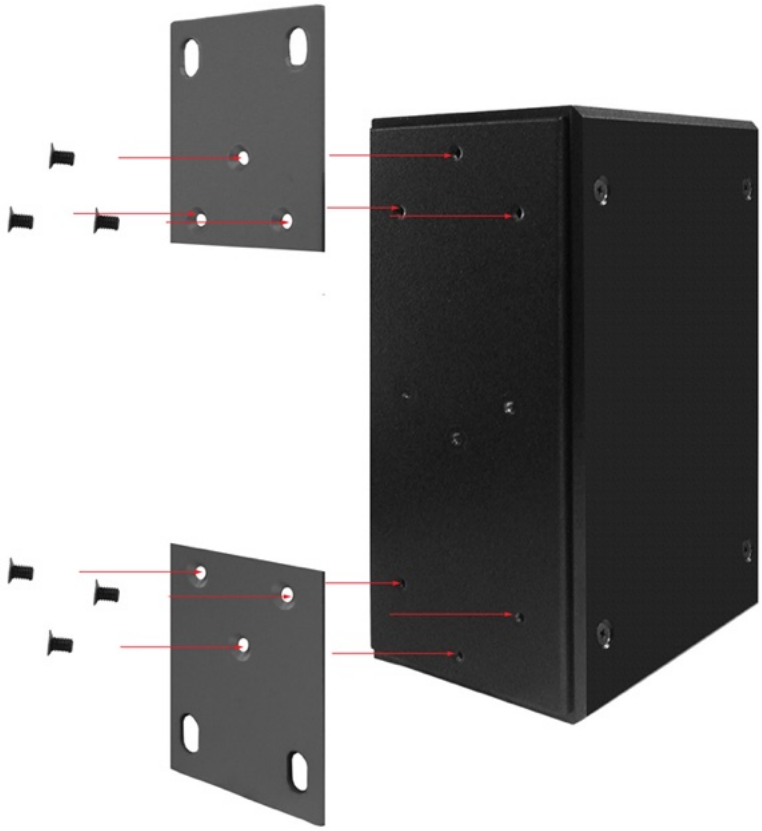


3. Check if the DIN-Rail is tightened on the track or not.
4. To remove the industrial switch from the track, reverse above steps.

3.3 Wall Mount Plate Mounting

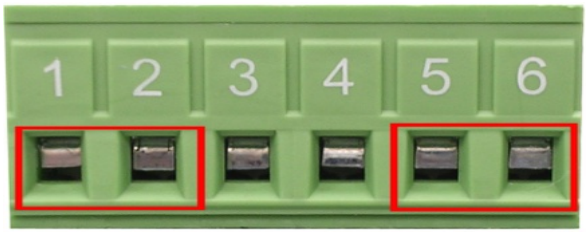
Follow the steps below to mount the industrial switch with wall mount plate.

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

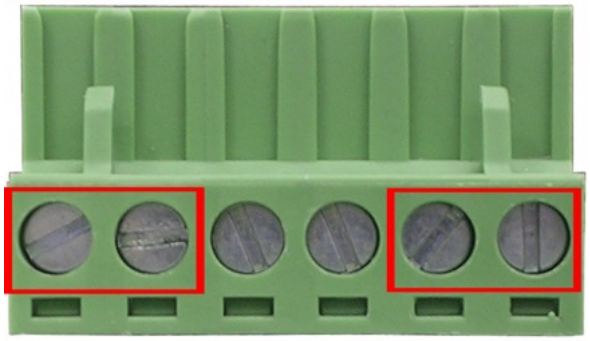


3.4 Wiring the Power Inputs

Please follow the steps below to insert the power wire.



1. Insert AC or DC power wires into the contacts 1 and 2 for power 1, or 5 and 6 for power.

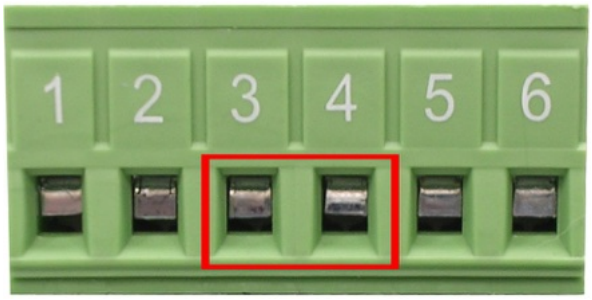


2. Tighten the wire-clamp screws for preventing the wires from loosing.

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

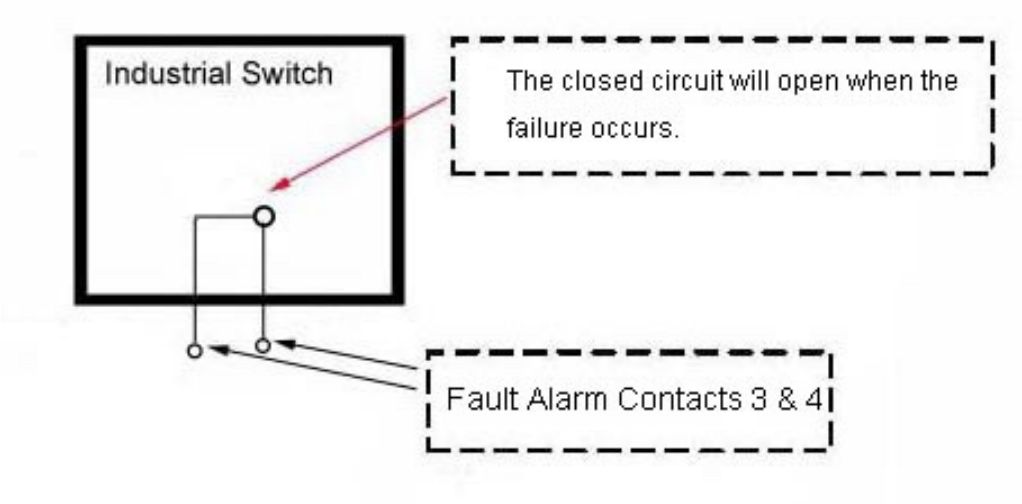
3.5 Wiring the Fault Alarm Contact

The fault alarm contacts are in the middle of the terminal block connector as the picture shows below. Inserting the wires, the switch will detect the fault status of the power failure, or port link failure (available for managed model) and then forms an open circuit. The following illustration shows an application example for wiring the fault alarm contacts



Insert the wires into the fault alarm contacts

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



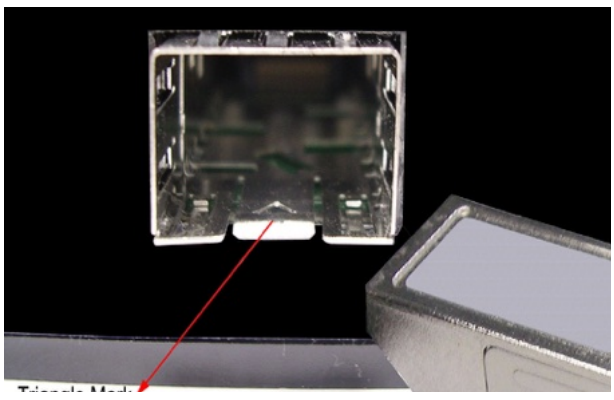
3.6 Cabling

- Use four twisted-pair, Category 5e or above cabling for RJ-45 port connection. The cable between the switch and the link partner (switch, hub, workstation, etc.) must be less than 100 meters (328 ft.) long.
- Fiber segment using **single-mode** connector type must use 9/125 µm single-mode fiber cable. User can connect two devices in the distance up to **30km**.
- Fiber segment using **multi-mode** connector type must use 50 or 62.5/125 µm multi-mode fiber cable. User can connect two devices up to **2km** distances.
- **Gigabit Copper/SFP (mini-GBIC) combo port:**

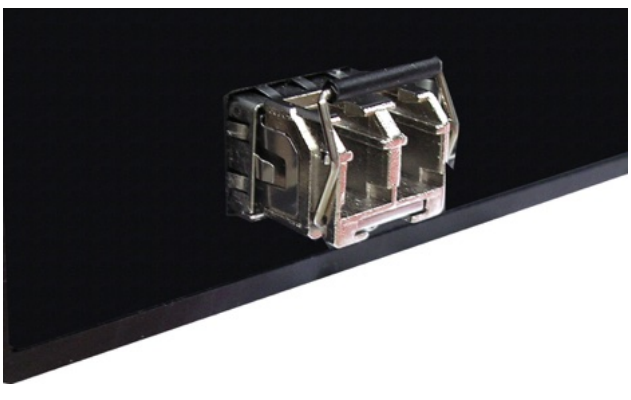
The Industrial switch has the auto-detected Giga port—Gigabit Copper/SFP combo ports. The Gigabit Copper (10/100/1000T) ports should use Category 5e or above UTP/STP cable for the connection up to 1000Mbps. The small form-factor pluggable (SFP) is a compact optical transceiver used in optical communications for both telecommunication and data communications. The SFP slots supporting dual mode can switch the connection speed between 100 and 1000Mbps. They are used for connecting to the network segment with single or multi-mode fiber. You can choose the appropriate SFP transceiver to plug into the slots. Then use proper multi-mode or single-mode fiber according to the transceiver. With fiber optic, it transmits at speed up to 1000 Mbps and you can prevent noise interference from the system.

[note]	The SFP/Copper Combo port can't both work at the same time. The SFP port has the higher priority than copper port; if you insert the 1000M SFP transceiver (which has connected to the remote device via fiber cable) into the SFP port, the connection of the accompanying copper port will link down. If you insert the 100M SFP transceiver into the SFP port even without a fiber connection to the remote, the connection of the accompanying copper port will link down immediately.

To connect the transceiver and LC cable, please follow the steps shown below:
First, insert the transceiver into the SFP module. Notice that the triangle mark is the bottom of the module.

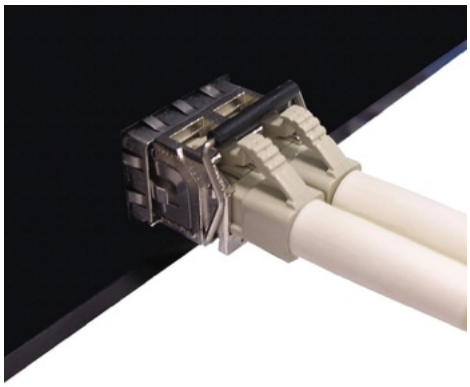


Transceiver to the SFP module



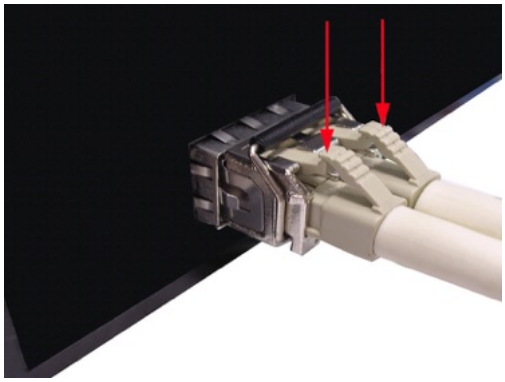
Transceiver Inserted

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



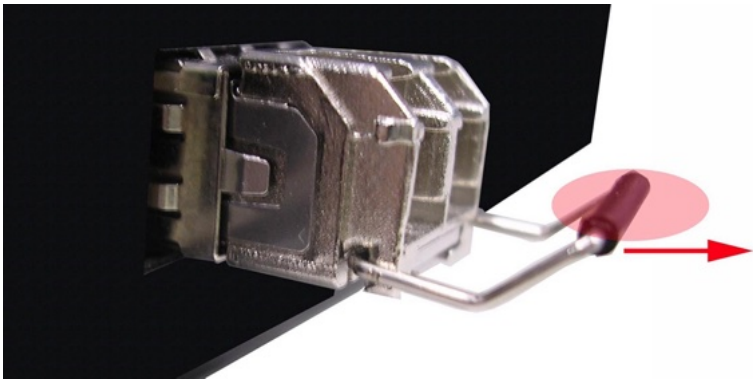
LC connector to the transceiver

To remove the LC connector from the transceiver, please follow the steps shown below:
First, press the upper side of the LC connector to release from the transceiver and pull it out.



Remove LC connector

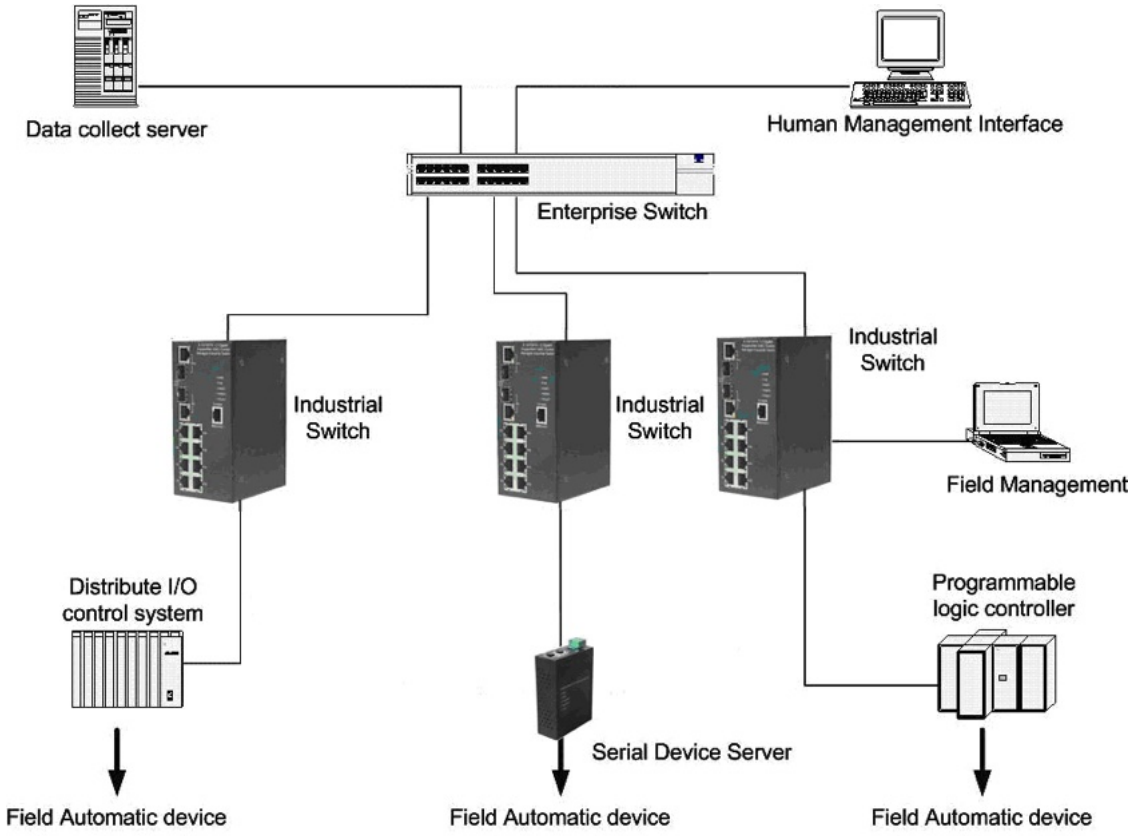
Second, push down the metal loop and pull the transceiver out by the plastic handle.



Pull out from the transceiver

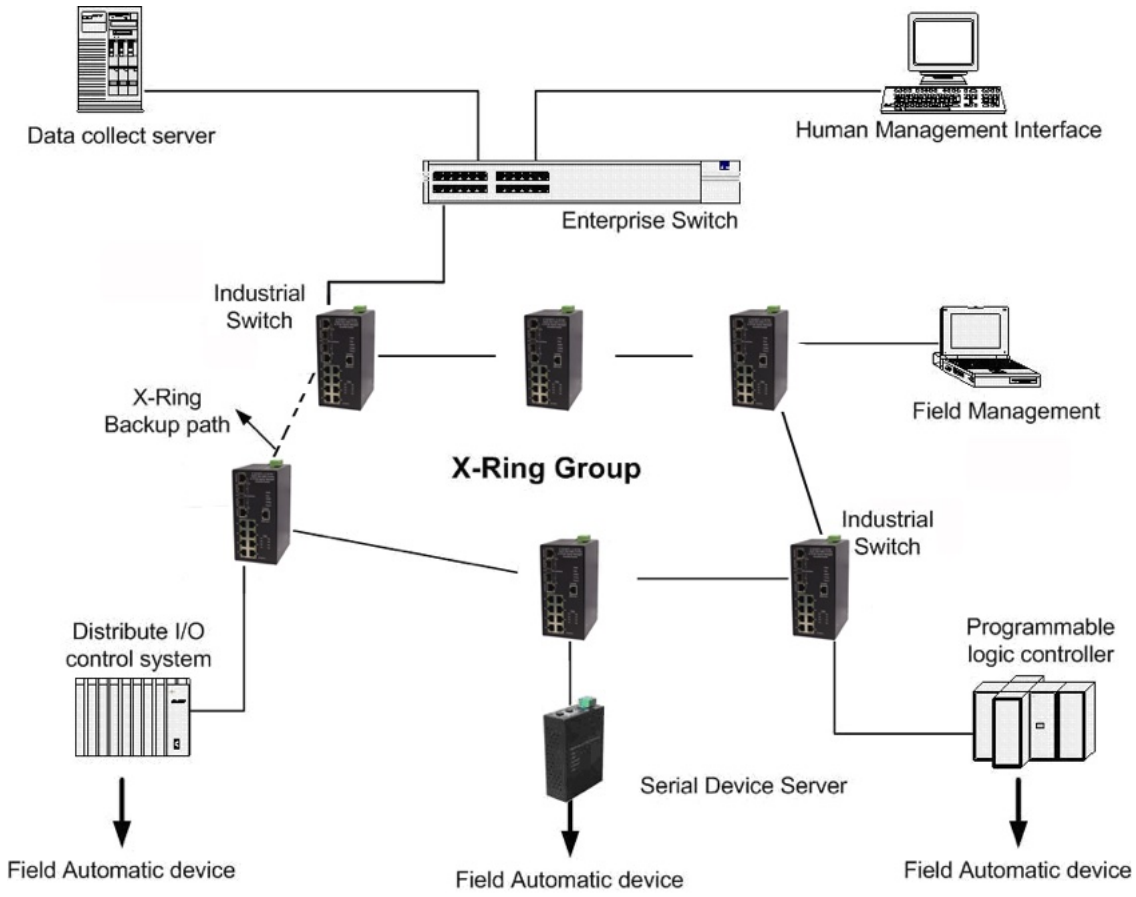
Chapter 4 Network Application

This chapter provides some sample applications to help user to have more actual idea of industrial switch function application. A sample application of the industrial switch is shown as below:



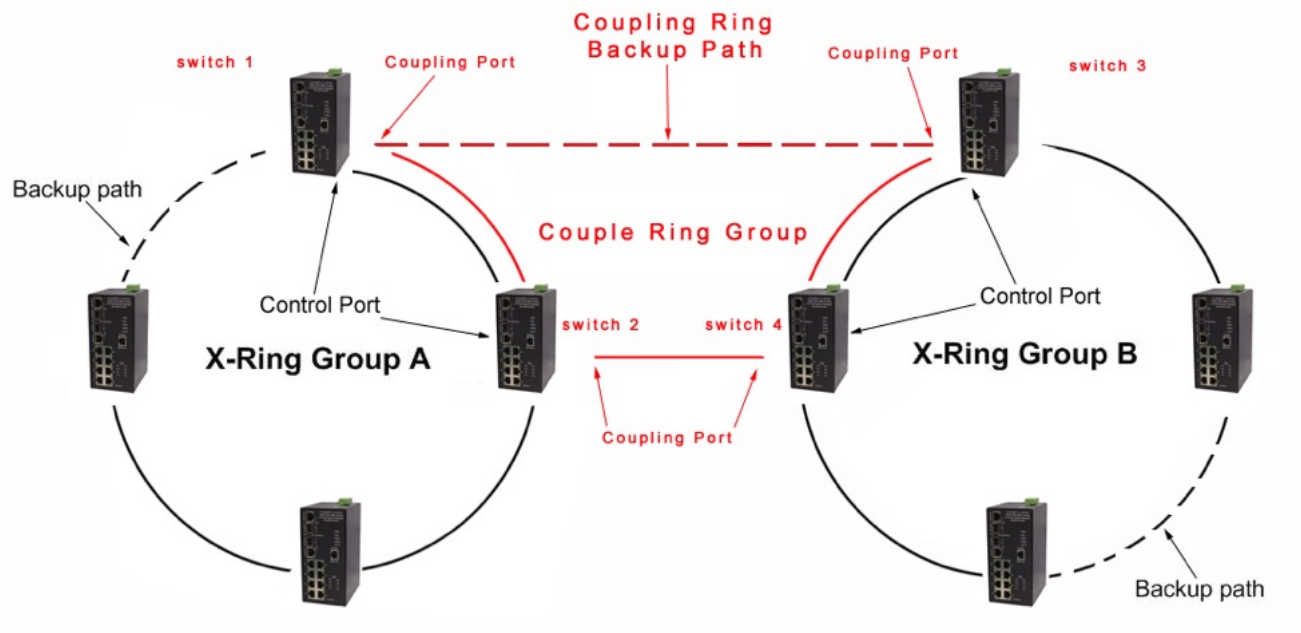
4.1 X-Ring Application

The industrial switch supports the X-Ring protocol that can help the network system to recovery from network connection failure within 20ms or less, and make the network system more reliable. The X-Ring algorithm is similar to spanning tree protocol (STP) algorithm but its recovery time is faster than STP. The following figure is a sample X-Ring application.



4.2 Coupling Ring Application

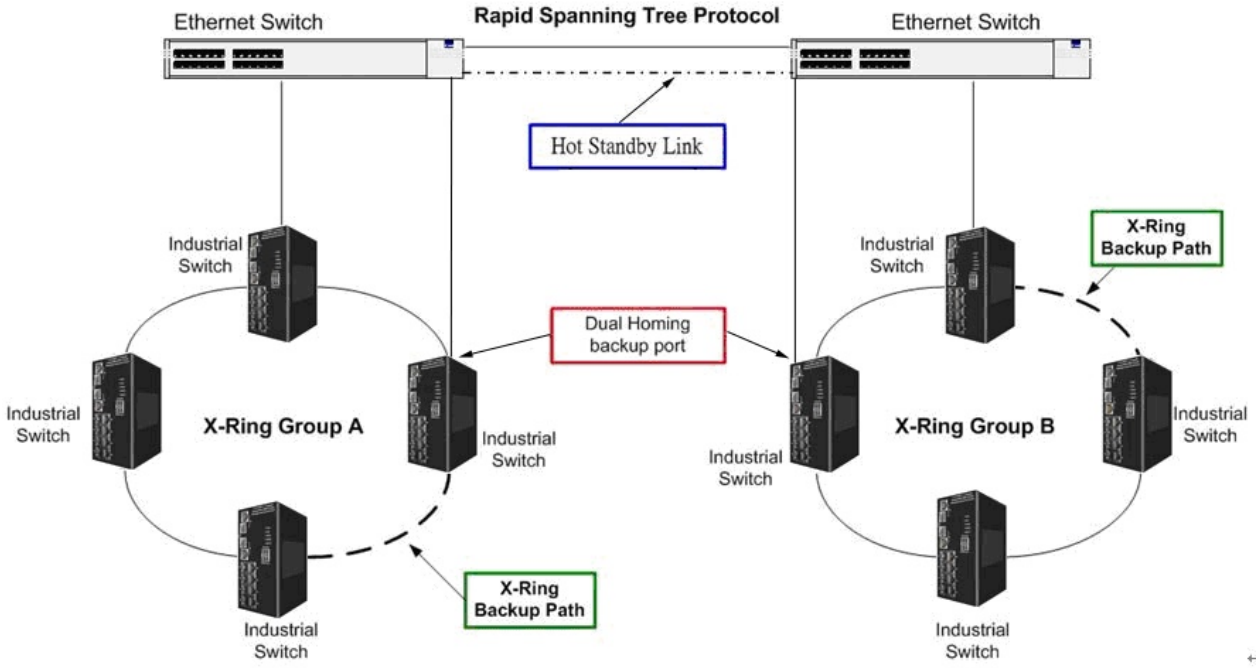
In the network, it may have more than one X-Ring group. By using the coupling ring function, it can connect each X-Ring for the redundant backup. It can ensure the transmissions between two ring groups not to fail. The following figure is a sample of coupling ring application.



4.3 Dual Homing Application

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

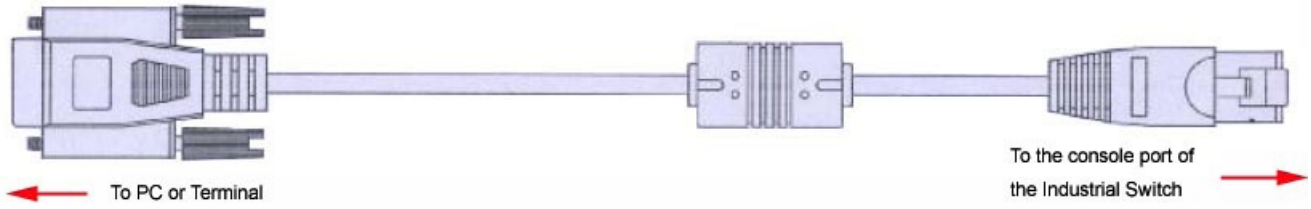
[note]	In Dual Homing application architecture, the upper level switches need to enable the Rapid Spanning Tree protocol.

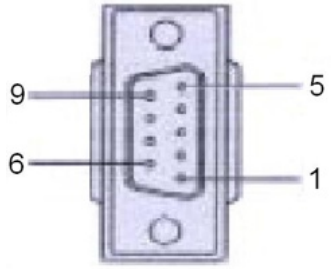


Chapter 5 Console Management

5.1 Connecting to the Console Port

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





DB 9-pin Female

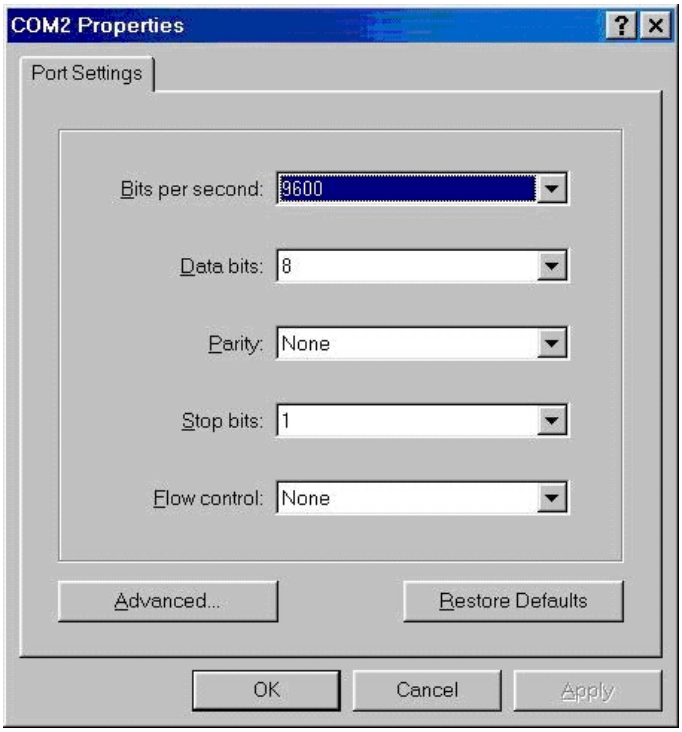
5.2 Pin Assignment

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

5.3 Login in the Console Interface

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

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



Having finished the parameter settings, click 'OK'. When the blank screen shows up, press Enter key to have the login prompt appears. Key in 'manager' (default value) for Username and "friend" for Password (use Enter key to switch), then press Enter and the Main Menu of console management appears. Please see below figure for login screen.

5.4 CLI Management

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

The following table lists the CLI commands and description.

5.5 Commands Level

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

Chapter 6 Web-Based Management

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

6.1 About Web-based Management

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

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

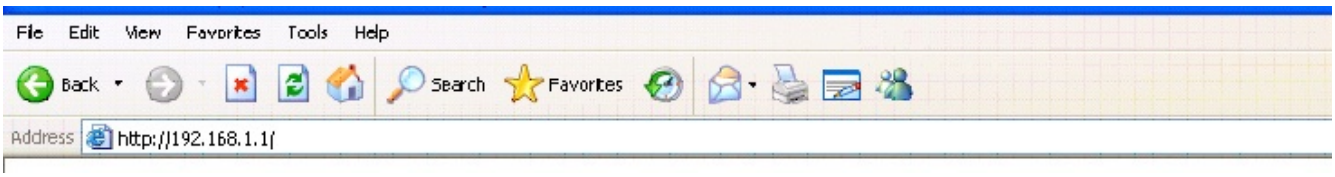
6.2 Preparing for Web Management

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

- IP Address: 192.168.1.1
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.254
- Default User Name: "manager"
- Default Password: "friend"

6.3 System Login

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



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



Login screen

6.4 System Information

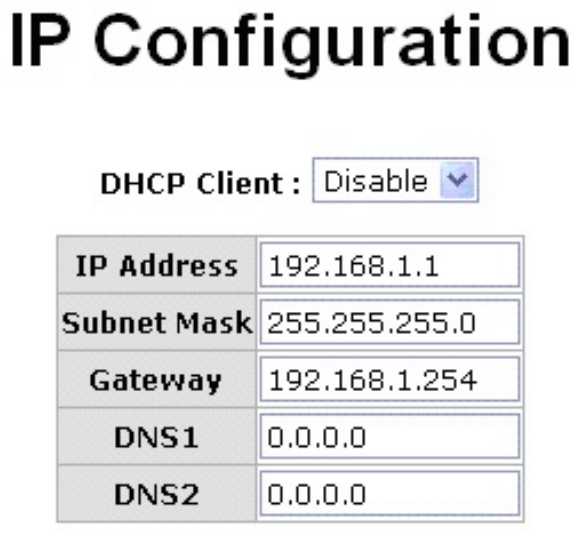
User can assign the system name, description, location and contact personnel to identify the switch. The version table below is a read-only field to show the basic information of the switch.

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

6.5 IP Configuration

The switch is a network device which needs to be assigned an IP address for being identified on the network. Users have to decide a means of assigning IP address to the switch.

- **DHCP Client**: Enable or disable the DHCP client function. When DHCP client function is enabled, the switch will be assigned an IP address from the network DHCP server. The default IP address will be replaced by the assigned IP address on DHCP server. After the user clicks Apply, a popup dialog shows up to inform the user that when the DHCP client is enabled, the current IP will lose and user should find the new IP on the DHCP server.
- **IP Address**: Assign the IP address that the network is using. If DHCP client function is enabled, this switch is configured as a DHCP client. The network DHCP server will assign the IP address to the switch and display it in this column. 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 DHCP client function is disabled, the user has to assign the subnet mask in this column field.
- **Gateway**: Assign the network gateway for the switch. If DHCP client function is disabled, the user has to assign the gateway in this column field. The default gateway is 192.168.16.254.
- **DNS1**: Assign the primary DNS IP address.
- **DNS2**: Assign the secondary DNS IP address.
- And then, click Apply



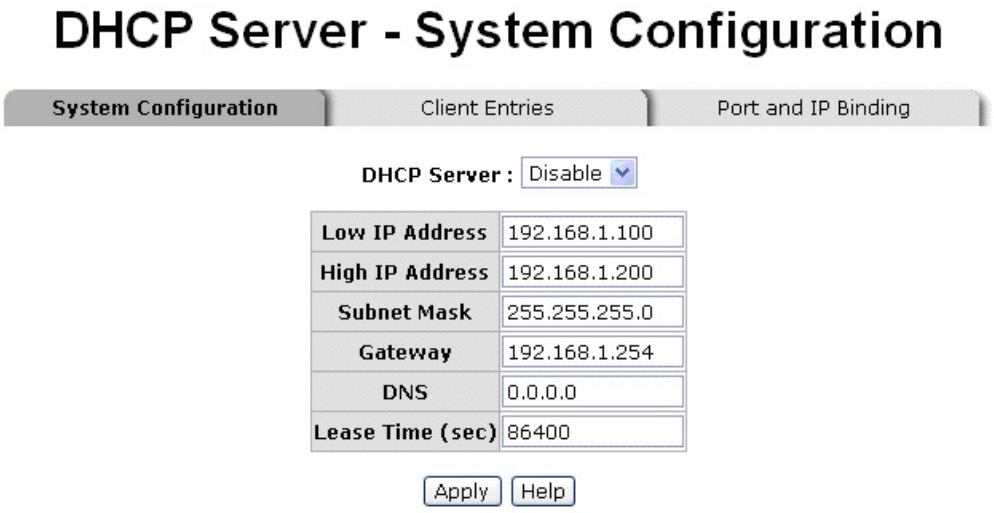
IP configuration interface

6.6 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 requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.
The system provides the DHCP server function. Having enabled the DHCP server function, the switch system will be configured as a DHCP server.

6.6.1 System configuration

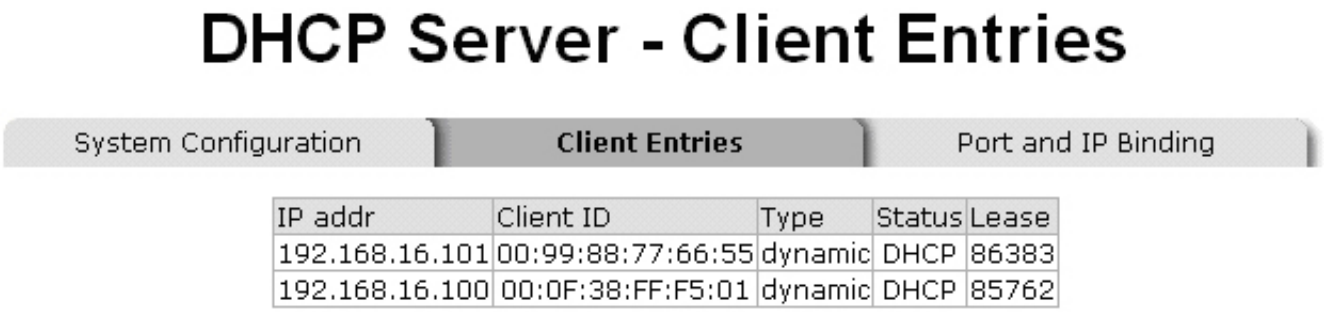
- **DHCP Server**: Enable or Disable the DHCP Server function. Enable—the switch will be the DHCP server on your local network.
- **Low IP Address**: Type in an IP address. Low IP address is the beginning of the dynamic IP range. For example, dynamic IP is in the range between 192.168.1.100 ~ 192.168.1.200. In contrast, 192.168.1.100 is the Low IP address.
- **High IP Address**: Type in an IP address. High IP address is the end of the dynamic IP range. For example, dynamic IP is in the range between 192.168.1.100 ~ 192.168.1.200. In contrast, 192.168.1.200 is the High IP address.
- **Subnet Mask**: Type in the subnet mask of the IP configuration.
- **Gateway**: Type in the IP address of the gateway in your network.
- **DNS**: Type in the Domain Name Server IP Address in your network.
- **Lease Time (sec)**: It is the time period that system will reset the dynamic IP assignment to ensure the dynamic IP will not been occupied for a long time or the server doesn't know that the dynamic IP is idle.
- And then, click Apply



DHCP Server Configuration interface

6.6.2 Client Entries

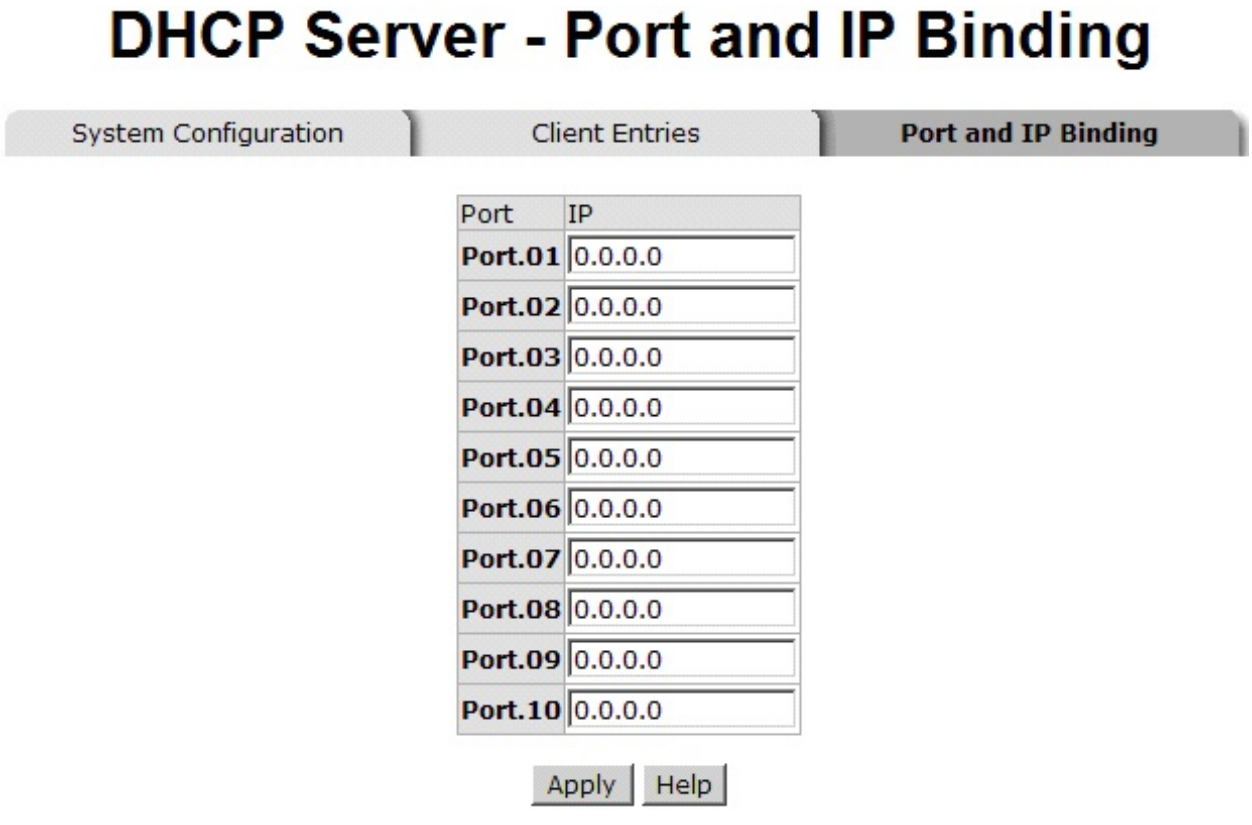
When the DHCP server function is enabled, the system will collect the DHCP client information including the assigned IP address, the MAC address of the client device, the IP assigning type, status and lease time.



DHCP Client Entries interface

6.6.3 Port and IP Bindings

Assign the dynamic IP address bound with the port to the connected client. The user is allowed to fill each port column 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.



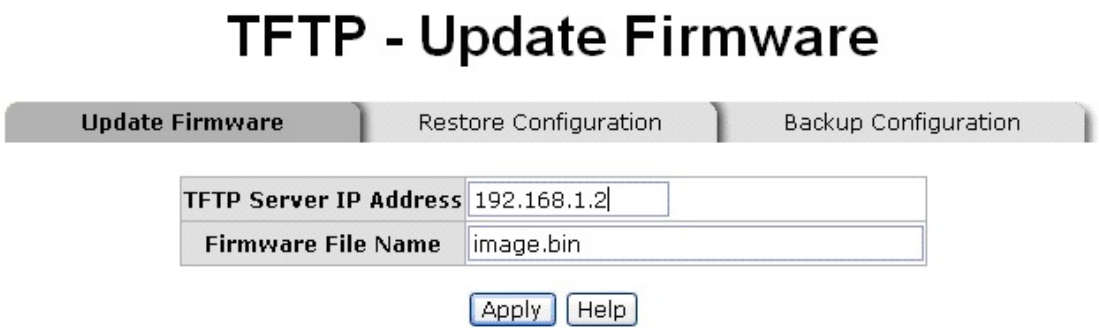
Port and IP Bindings interface

6.7 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.

6.7.1 Update Firmware

- **TFTP Server IP Address**: Type in your TFTP server IP.
- **Firmware File Name**: Type in the name of the firmware image file to be updated.
- Click Apply



Update Firmware interface

6.7.2 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 and the switch will download back the flash image.

- **TFTP Server IP Address**: Type in the TFTP server IP.
- **Restore File Name**: Type in the correct file name for restoring.
- Click Apply

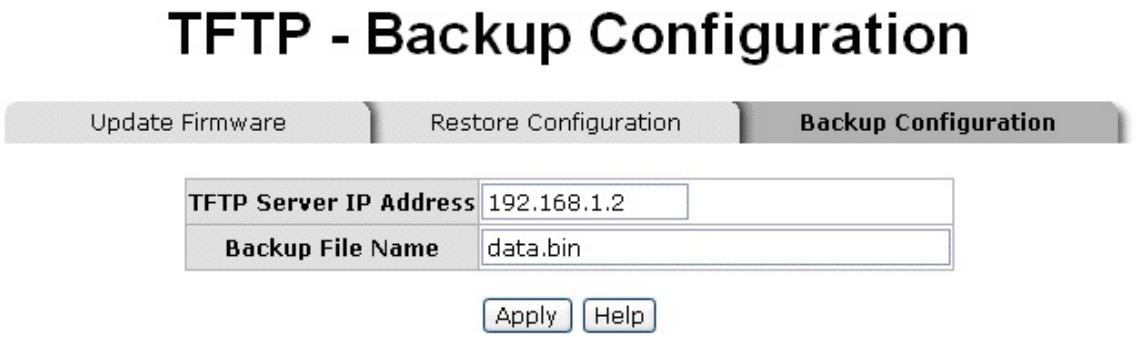


Restore Configuration interface

6.7.3 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 to avoid wasting time on configuring the settings by backing up the configuration.

- **TFTP Server IP Address**: Type in the TFTP server IP.
- **Backup File Name**: Type in the file name.
- Click Apply



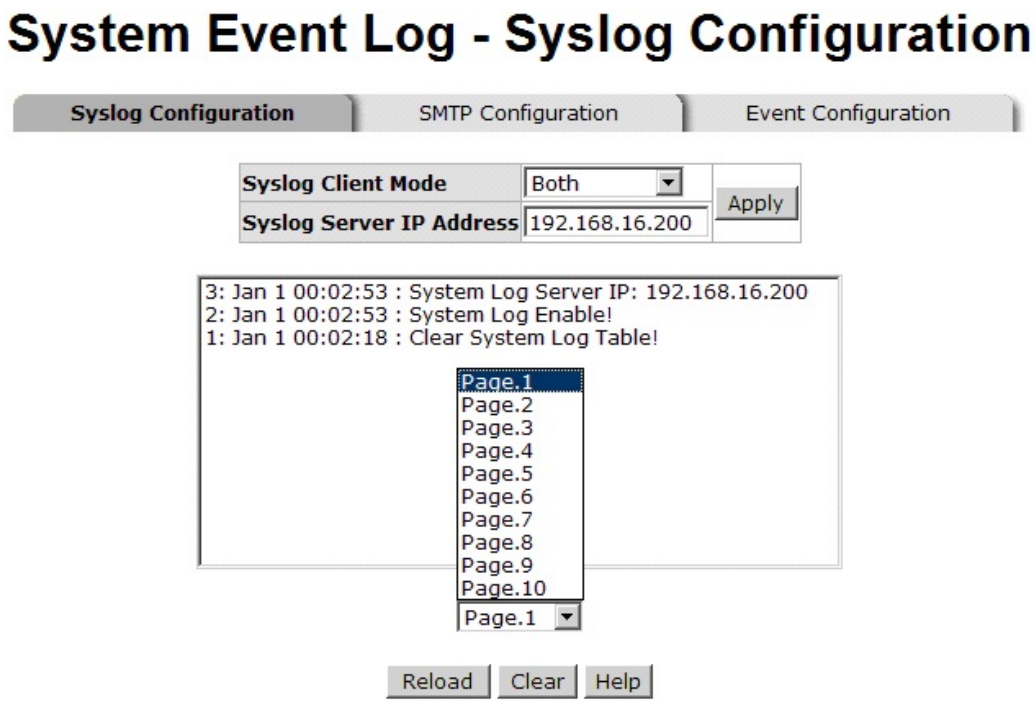
Backup Configuration interface

6.8 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. There are five types of event—Device Cold Start, Device Warm Start, Authentication Failure, X-Ring Topology Change, and Port Event—available to be issued as the event log.

6.8.1 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.
- **System Log Server IP Address**: When the 'Syslog Mode' item is set as Server Only/Both, the user has 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 all the current event logs.
- Make sure the selected mode is correct, and click Apply to have the setting take effect.

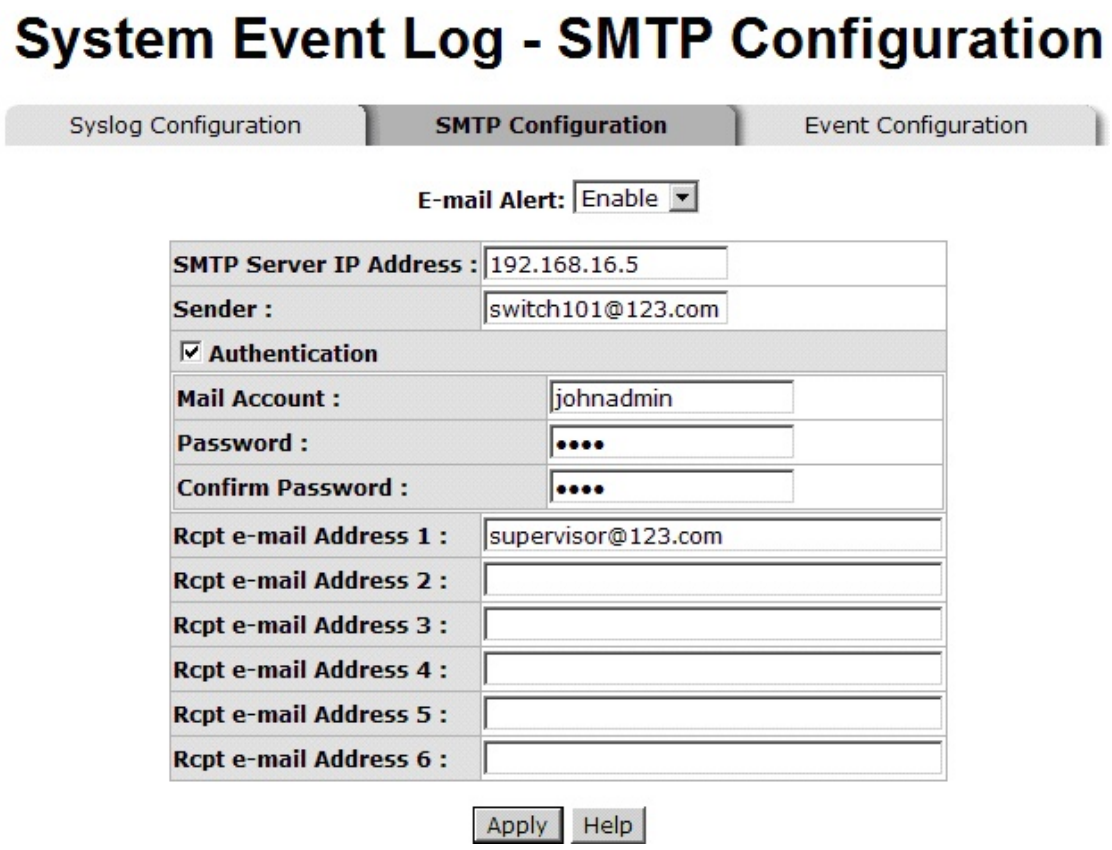


Syslog Configuration interface

6.8.2 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, mail subject, sender, mail account, password, and the recipient email addresses which the e-mail alert will send to. There are also five types of event—Device Cold Start, Device Warm Start, Authentication Failure, X-Ring Topology Change, and Port Event—available to be issued as the e-mail alert. Besides, this function provides the authentication mechanism including an authentication step through which the client effectively logs in to the SMTP server during the process of sending e-mail alert.

- **Email Alert**: With this function being 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**: Assign the mail server IP address (when Email Alert is enabled, this function 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**: Having ticked this checkbox, the mail account, password and confirm password column fields will then show up. Configure the email account and password for authentication 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 for the email account.
- Confirm Password: Reconfirm the password.
- **Rcpt e-mail Address 1 ~ 6:** You can also fill each of the column fields with up to 6 e-mail accounts to receive the email alert.
- Click Apply to have the configuration take effect.



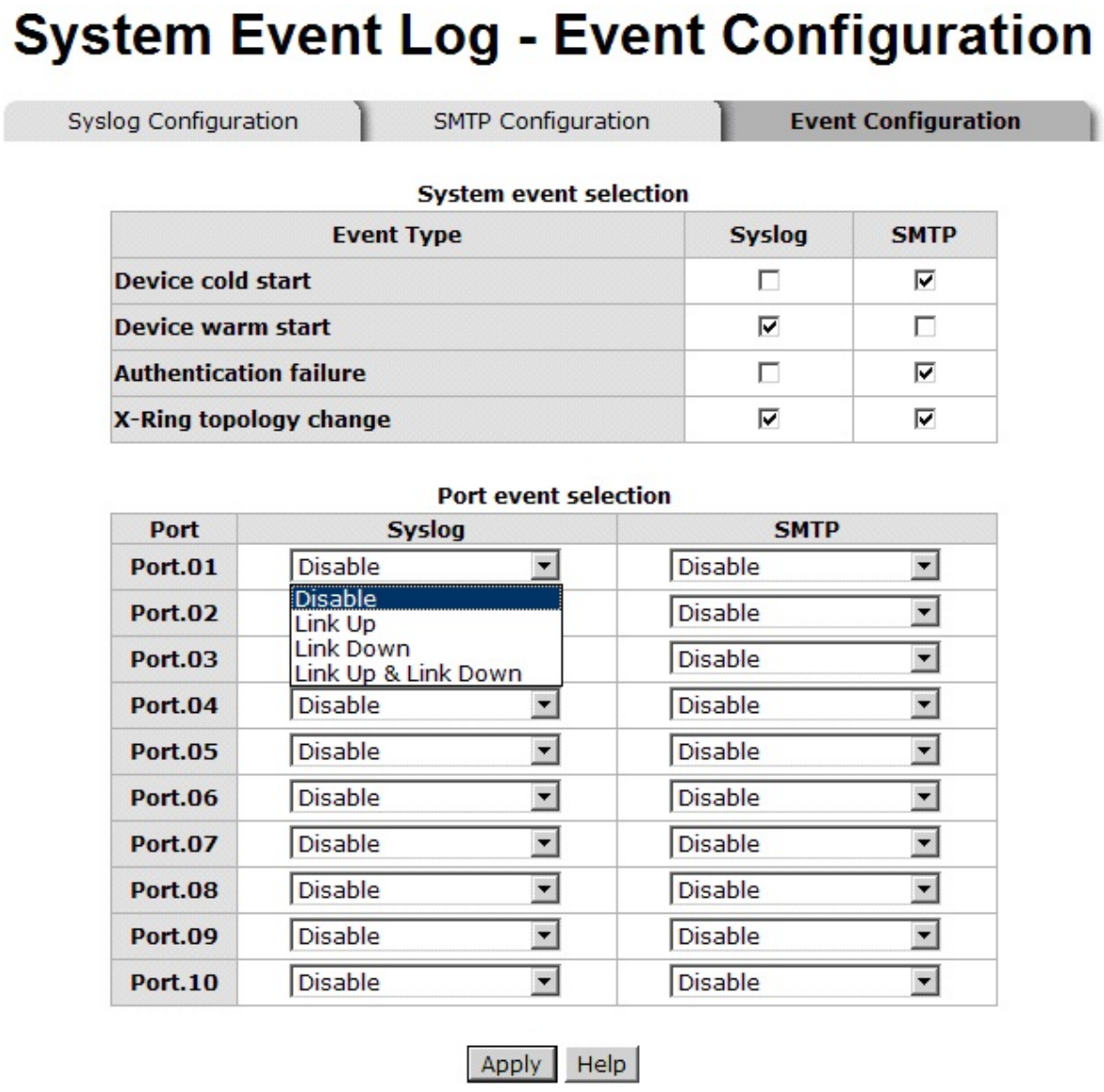
SMTP Configuration interface

6.8.3 System Event Log - Event Configuration

Having ticked the **Syslog/SMTP** checkboxes, the event log/email alert will be sent to the system log server and the SMTP server respectively. Also, Port event log/alert (link up, link down, and both) can be sent to the system log server/SMTP server respectively by setting the trigger condition.

- **System event selection**: There are 4 event types—Device Cold Start, Device Warm Start, Authentication Failure, and X-ring Topology Change. The checkboxes are not available for ticking unless the **Syslog Client Mode** on the Syslog Configuration tab and the **E-mail Alert** on the SMTP Configuration tab are enabled first.
  - > **Device cold start**: *When the device executes cold start action, the system will issue the event log/email alert to the system log/SMTP server respectively.*
  - > **Device warm star**t: *When the device executes warm start, the system will issue the event log/email alert to the system log/SMTP server respectively.*
  - > **Authentication Failure**: *When the SNMP authentication fails, the system will issue the event log/email alert to the system log/SMTP server respectively.*
  - > **X-ring topology change**: *When the X-ring topology has changed, the system will issue the event log/email alert to the system log/SMTP server respectively.*

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

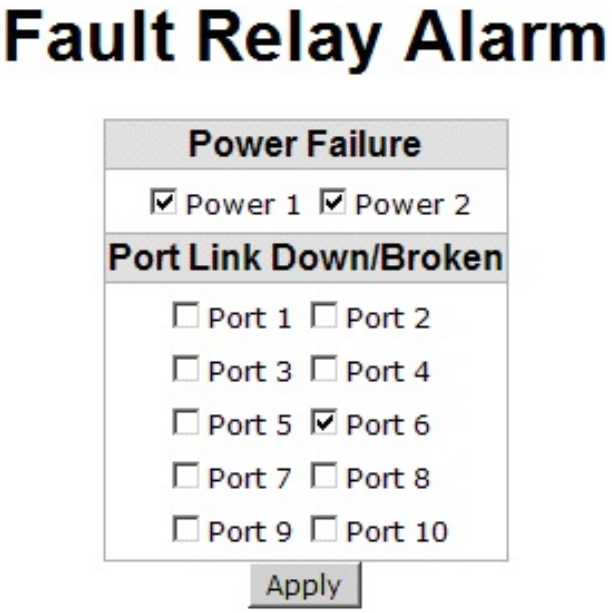


Event Configuration interface

6.9 Fault Relay Alarm

The Fault Relay Alarm function provides the Power Failure and Port Link Down/Broken detection. With both power input 1 and power input 2 installed and the check boxes of power 1/power 2 ticked, the FAULT LED indicator will then be possible to light up when any one of the power failures occurs. As for the Port Link Down/Broken detection, the FAULT LED indicator will light up when the port failure occurs; certainly the check box beside the port must be ticked first. Please refer to the segment of '**Wiring the Fault Alarm** Contact' for the failure detection.

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



Fault Relay Alarm interface

6.10 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 to some time reference. Because time usually just advances, the time on different node stations will 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 SNTP function to get the time from the SNTP server.
- **Daylight Saving Time**: This is used as a control switch to enable/disable daylight saving period and daylight saving offset. Users can configure Daylight Saving Period and Daylight Saving Offset in a certain period time and offset time while there is no need to enable daylight saving function. Afterwards, users can just set this item as enable without assign Daylight Saving Period and Daylight Saving Offset again.
- **UTC Timezone**: Universal Time, Coordinated. Set the switch location time zone. The following table lists the different location time zone for your reference

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

- **SNTP Sever URL**: Set 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 column field of SNTP Server URL, the current coordinated time is displayed here.
- **Daylight Saving Period**: Set up the Daylight Saving beginning date/time and Daylight Saving ending date/time. 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 02:04' in the two column 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.
- Click Apply to have the configuration take effect.



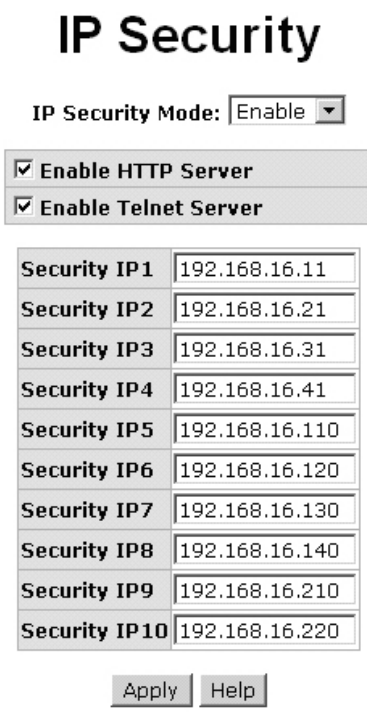
SNTP Configuration interface

6.11 IP Security

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

- **IP Security Mode**: Having set this selection item in the Enable mode, the Enable HTTP Server, Enable Telnet Server checkboxes and the ten security IP column fields will then be available. If not, those items will appear in grey.
- **Enable HTTP Server**: Having ticked this checkbox, the devices whose IP addresses match any one of the ten IP addresses in the Security IP1 ~ IP10 table will be given the permission to access this switch via HTTP service.
- **Enable Telnet Server**: Having ticked this checkbox, the devices whose IP addresses match any one of the ten IP addresses in the Security IP1 ~ IP10 table will be given the permission to access this switch via telnet service.
- **Security IP 1 ~ 10**:The system allows the user to assign up to 10 specific IP addresses for access security. Only these 10 IP addresses can access and manage the switch through the HTTP/Telnet service once IP Security Mode is enabled.
- 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

6.12 User Authentication

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

- **User name**: Type in the new user name (The default is 'root')
- **Password**: Type in the new password (The default is 'root')
- **Confirm password**: Re-type the new password
- And then, click Apply

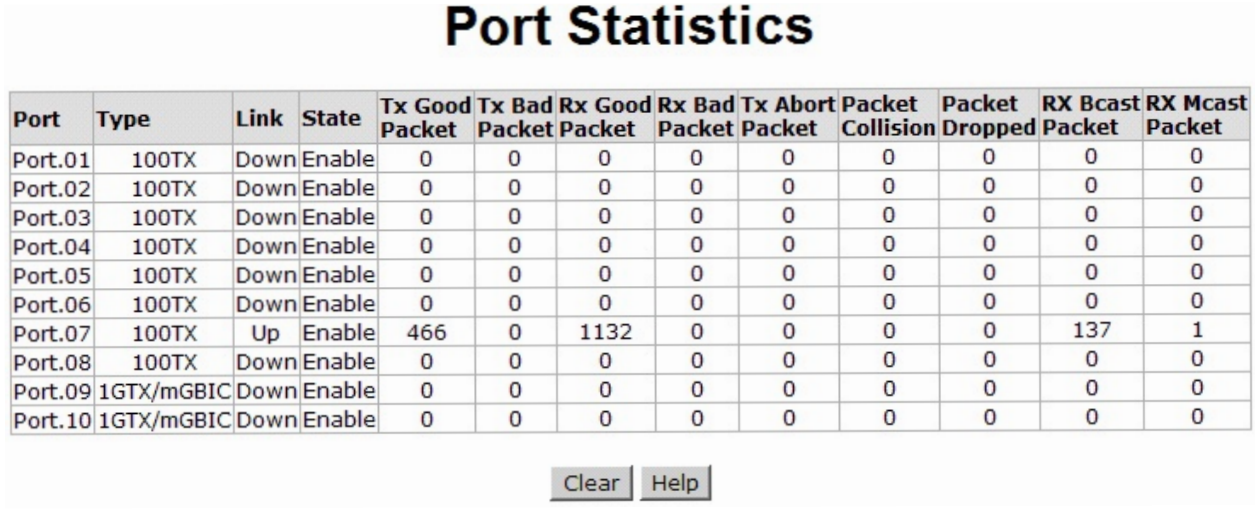


User Authentication interface

6.13 Port Statistics

The following chart provides the current statistic information which displays the real-time packet transfer status 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**: The port number.
- **Type**: Displays the current speed of connection to the port.
- **Link**: The status of linking—'Up' or 'Down'.
- **State**: It's set by Port Control. When the state is disabled, the port will not transmit or receive any packet.
- **Tx Good Packet**: The counts of transmitting good packets via this port.
- **Tx Bad Packet**: The counts of transmitting bad packets (including undersize [less than 64 octets], oversize, CRC Align errors, fragments and jabbers packets) via this port.
- **Rx Good Packet**: The counts of receiving good packets via this port.
- **Rx Bad Packet**: The counts of receiving good packets (including undersize [less than 64 octets], oversize, CRC error, fragments and jabbers) via this port.
- **Tx Abort Packet**: The aborted packet while transmitting.
- **Packet Collision**: The counts of collision packet.
- **Packet Dropped**: The counts of dropped packet.
- **Rx Bcast Packet**: The counts of broadcast packet.
- **Rx Mcast Packet**: The counts of multicast packet.
- Click Apply 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	Down	Enable	0	0	0	0	0	0	0	0	0
Port.02	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.03	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.04	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.05	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.06	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.07	100TX	Up	Enable	466	0	1132	0	0	0	0	137	1
Port.08	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.09	1GTX/mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0
Port.10	1GTX/mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0

Clear Help

Port Statistics interface

6.14 Port Control

In Port control you can configure the settings of each port to control the connection parameters, and the status of each port is listed beneath.

- **Port**: Use the scroll bar and click on the port number to choose the port to be configured.
- **State**: Current port state. The port can be set to disable or enable mode. If the port state is set as 'Disable', it will not receive or transmit any packet.
- **Negotiation**: Auto and Force. Being set as Auto, the speed and duplex mode are negotiated automatically. When you set it as Force, you have to set the speed and duplex mode manually.
- **Speed**: It is available for selecting when the Negotiation column is set as Force. When the Negotiation column is set as Auto, this column is read-only.
- **Duplex**: It is available for selecting when the Negotiation column is set as Force. When the Negotiation column is set as Auto, this column is read-only.
- **Flow Control**: Whether or not the receiving node sends feedback to the sending node is determined by this item. When enabled, once the device exceeds the input data rate of another device, the receiving device will send a PAUSE frame which halts the transmission of the sender for a specified period of time. When disabled, the receiving device will drop the packet if too much 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. See the segment of **MAC Address Table—Static MAC Addresses**.
- Click Apply to have the configuration take effect.



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

Port Control interface

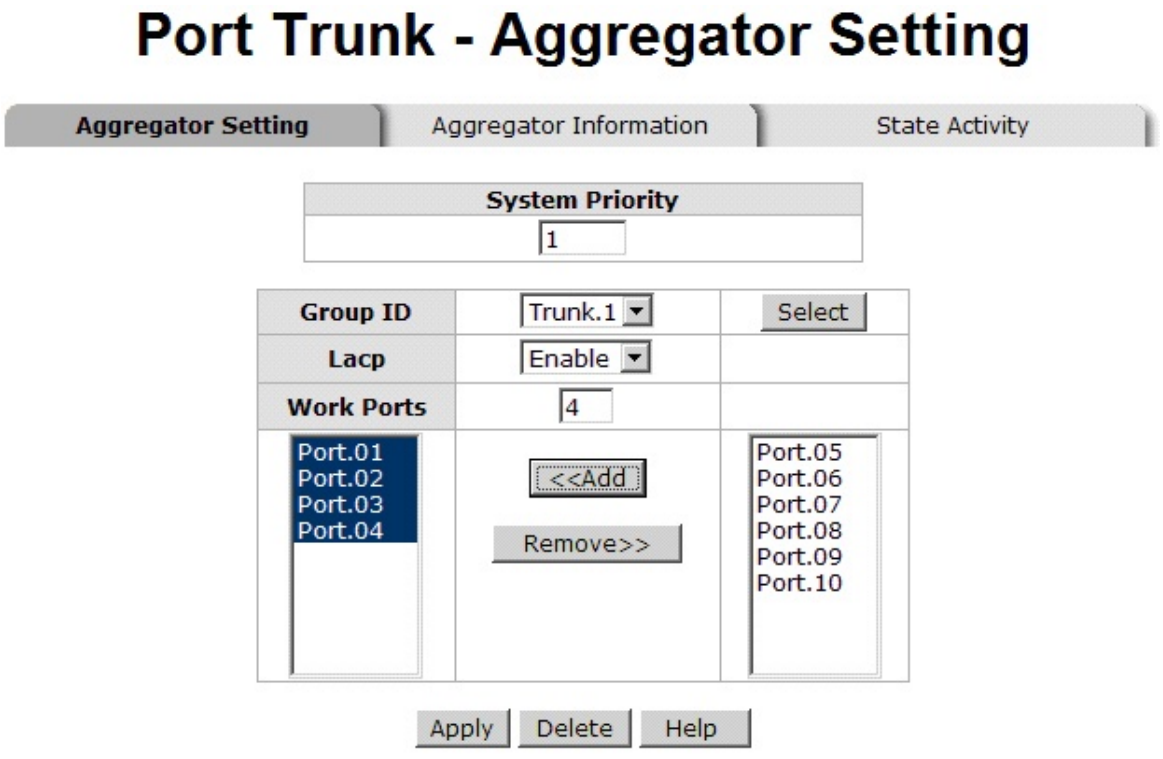
6.15 Port Trunk

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.

6.15.1 Aggregator setting

- **System Priority**: A value which is used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP peer of the trunk group.
- **Group ID**: There are 13 trunk groups to be selected. Assign the "**Group ID**" to the trunk group.
- **LACP**: When enabled, the trunk group is using LACP. A port 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 column field allows the user to type in the total number of active port up to four. **With LACP static trunk group**, e.g. you assign four ports to be the members of a trunk group whose work ports column field is set as two; the exceed ports are standby/ redundant ports and can be aggregated if working ports fail. If it is a **static trunk group** (non-LACP), the number of work ports must equal the total number of group member ports.
- Select the ports to join the trunk group. The system allows a maximum of four ports to be aggregated in a trunk group. Click Add and the ports focused in the right side will be shifted to the left side. To remove unwanted ports, select the ports and click Remove.
- When LACP enabled, you can configure LACP Active/Passive status for each port on the **State Activity** tab.
- Click Apply .
- Use Delete to delete Trunk Group. Select the Group ID and click Delete .

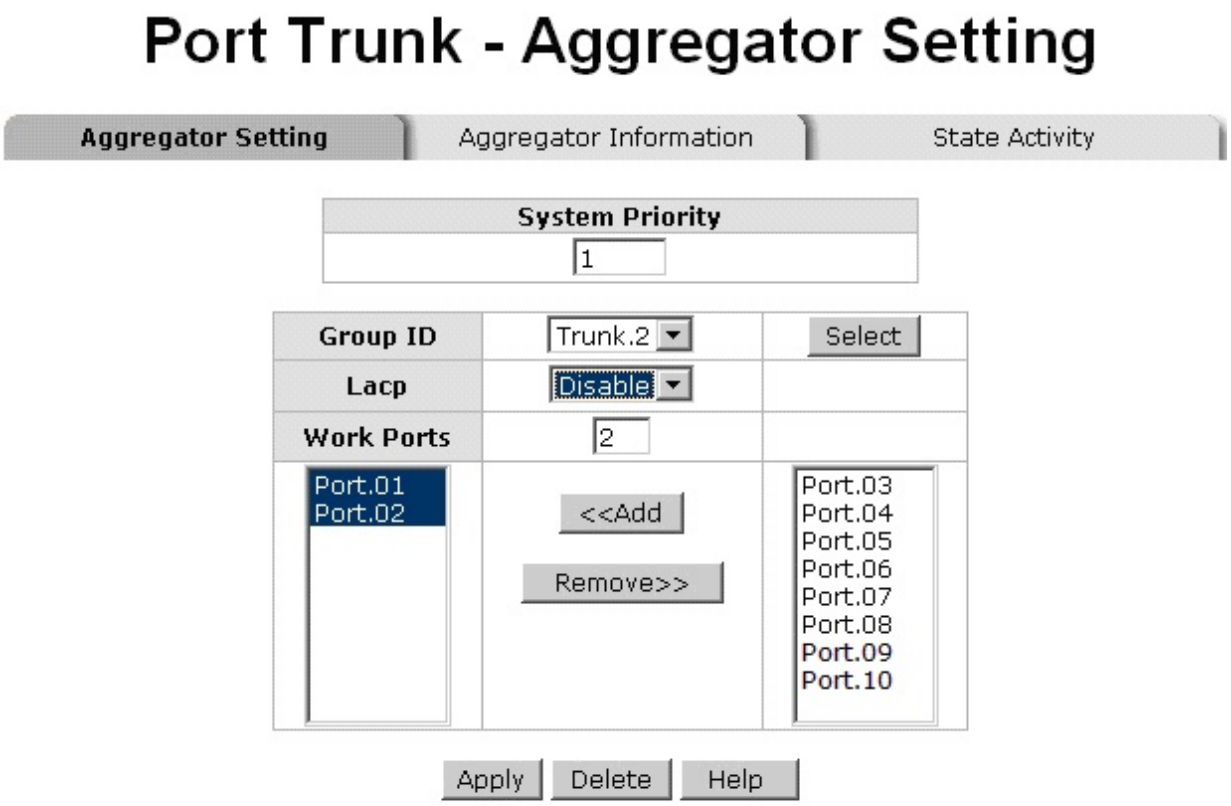


Port Trunk—Aggregator Setting interface (four ports are added to the left field with LACP enabled)

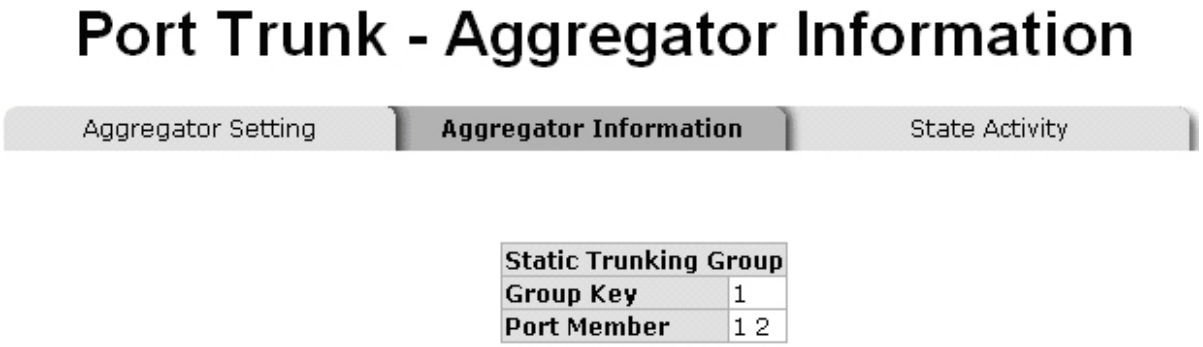
6.15.2 Aggregator Information

- **LACP disabled**

Having set up the aggregator setting with LACP disabled, you will see the local static trunk group information on the tab of **Aggregator Information**.



Assigning 2 ports to a trunk group with LACP disabled



Static Trunking Group information

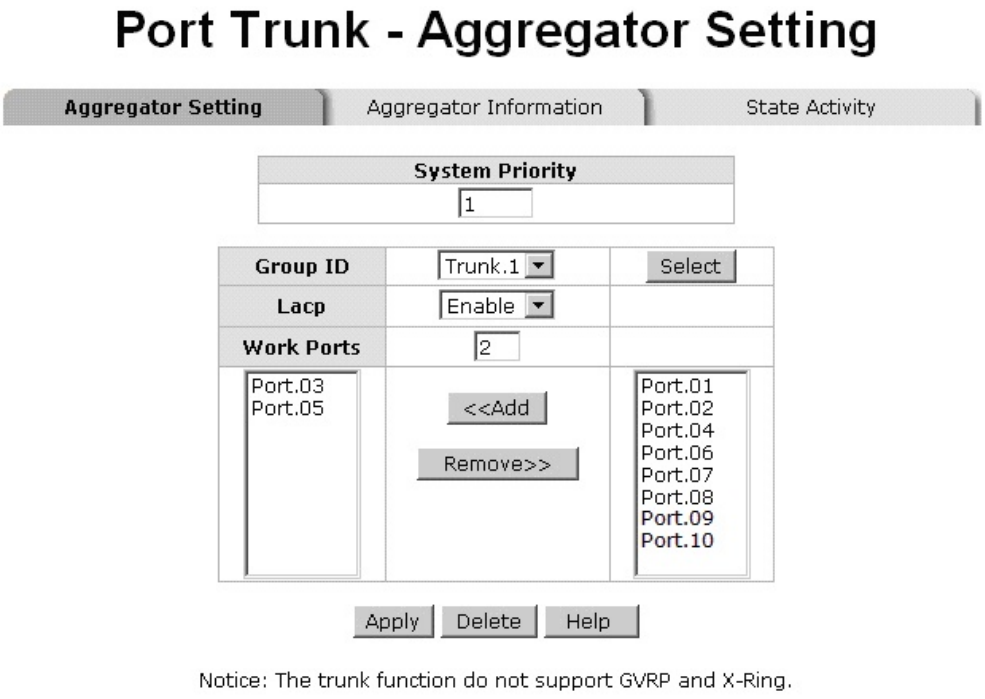
- **Group Key**: This is a read-only column field that displays the trunk group ID.
- **Port Member**: This is a read-only column field that displays the members of this static trunk group.

- **LACP enabled**

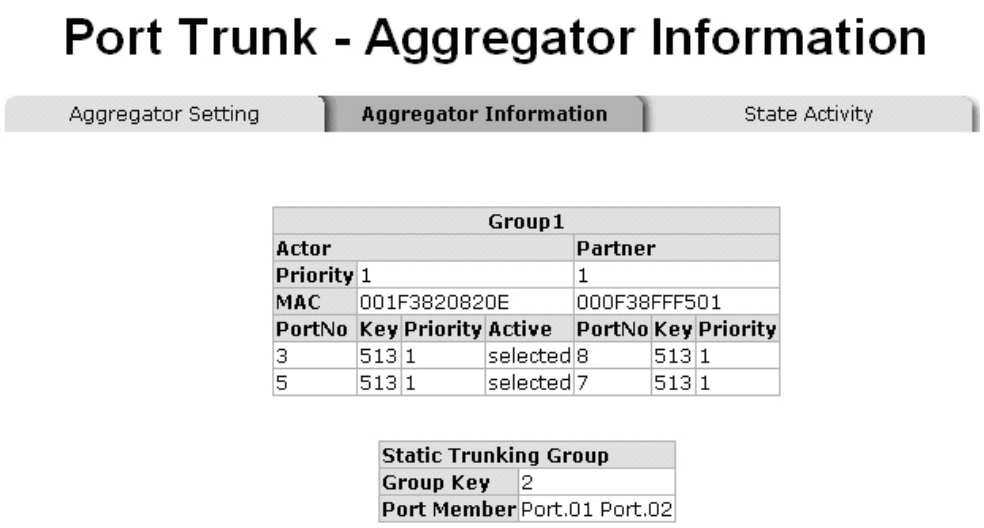
Having set up the aggregator setting with LACP enabled, you will see the trunking group information between two switches on the tab of **Aggregator Information**.

Switch 1 configuration

1. Set **System Priority** of the trunk group. The default is 1.
2. Select a **trunk group ID** by pull down the drop-down menu bar.
3. Enable LACP.
4. Include the member ports by clicking the **Add** button after selecting the port number and the column field of **Work Ports** changes automatically.



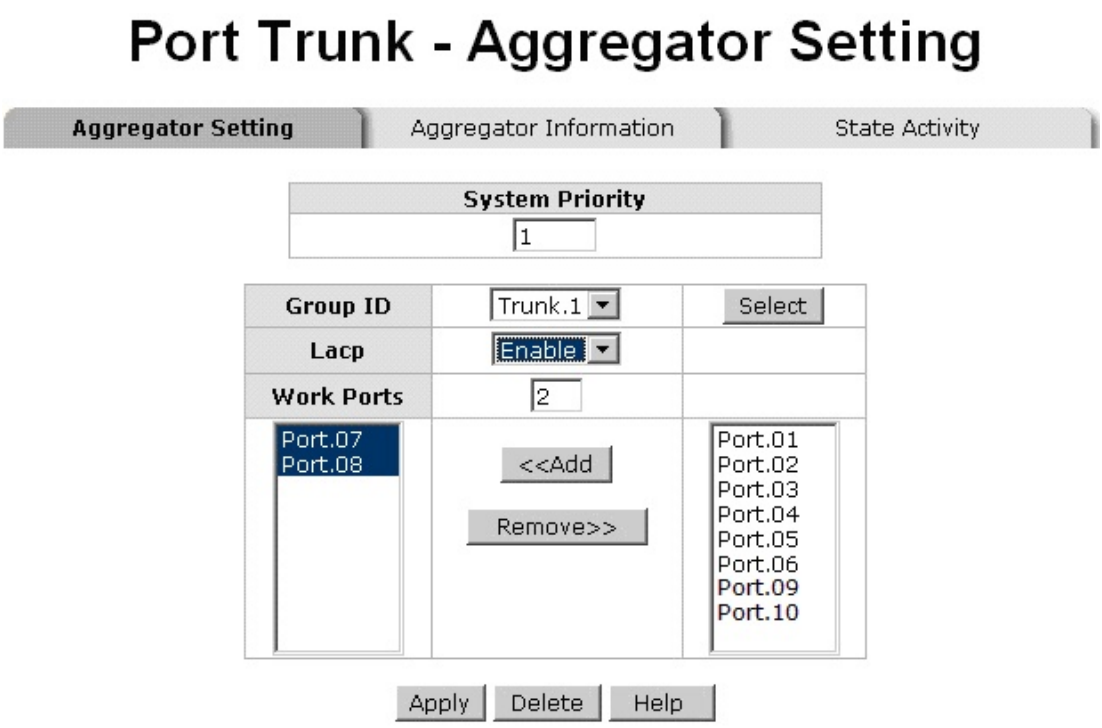
Switch 1 configuration interface



Aggregation Information of Switch 1

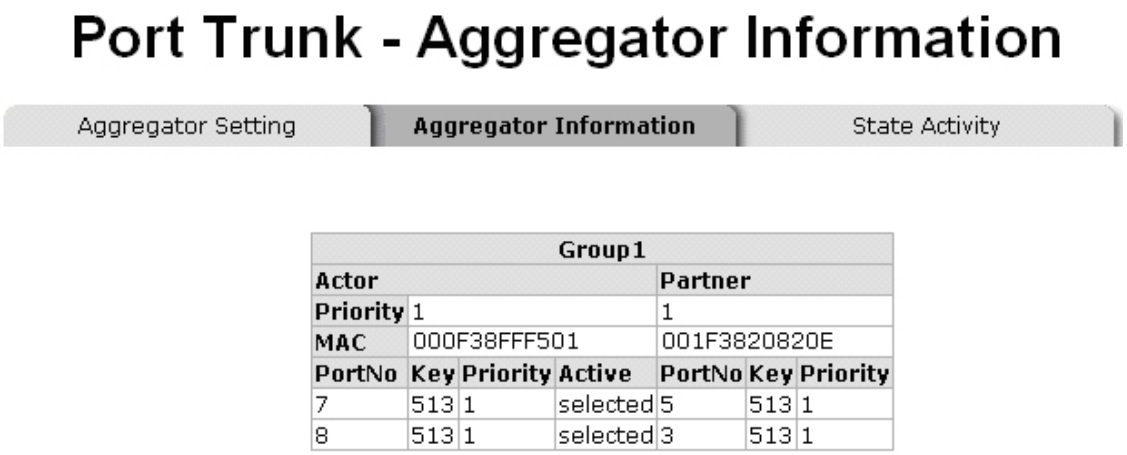
5. Click on the tab of **Aggregator Information** to check the trunked group information as the illustration shown above after the two switches configured.

Switch 2 configuration



Switch 2 configuration interface

1. Set **System Priority** of the trunk group. The default is 1.
2. Select a **trunk group ID** by pull down the drop-down menu bar.
3. Enable LACP.
4. Include the member ports by clicking the **Add** button after selecting the port number and the column field of **Work Ports** changes automatically.



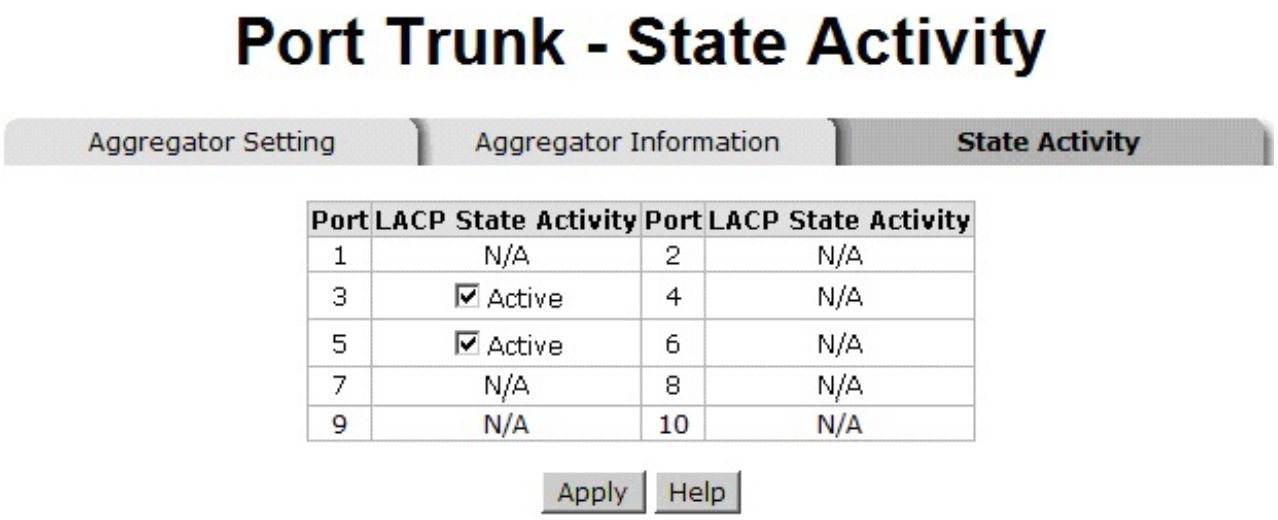
5. Click on the tab of **Aggregator Information** to check the trunked group information as the illustration shown above after the two switches configured.

6.15.3 State Activity

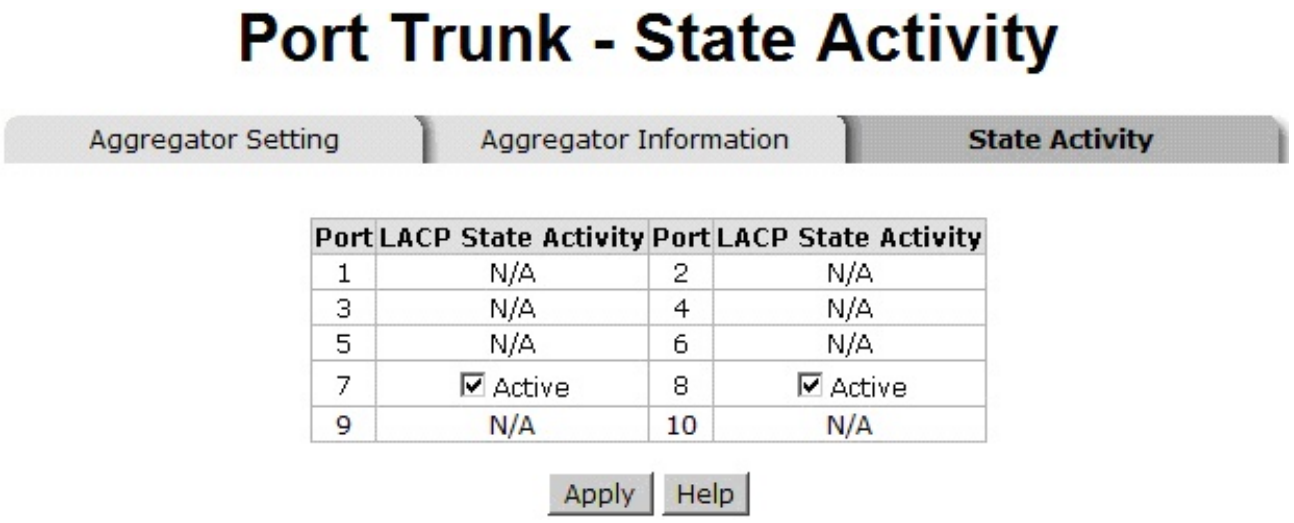
Having set up the LACP aggregator on the tab of Aggregator Setting, you can configure the state activity for the members of the LACP trunk group. You can tick or cancel the checkbox beside the state label. When you remove the tick mark of the port and click Apply , the port state activity will change to **Passive**.

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

[note]	**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

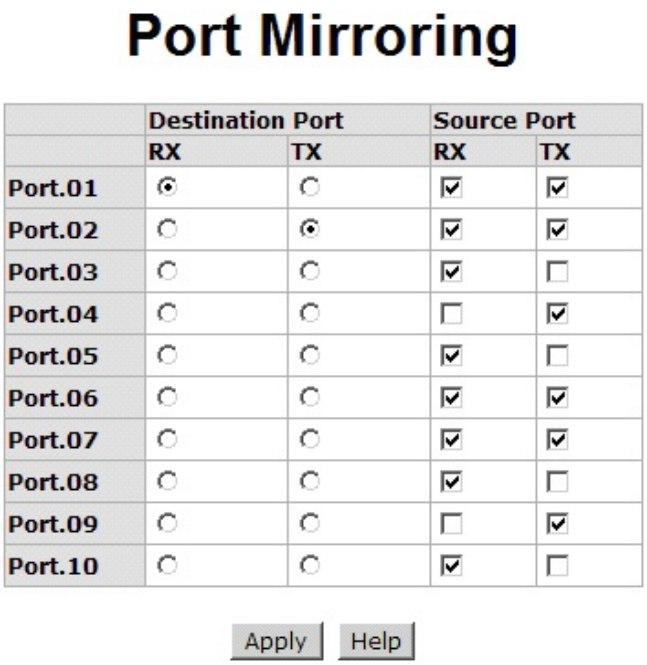


State Activity of Switch 2

6.16 Port Mirroring

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

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



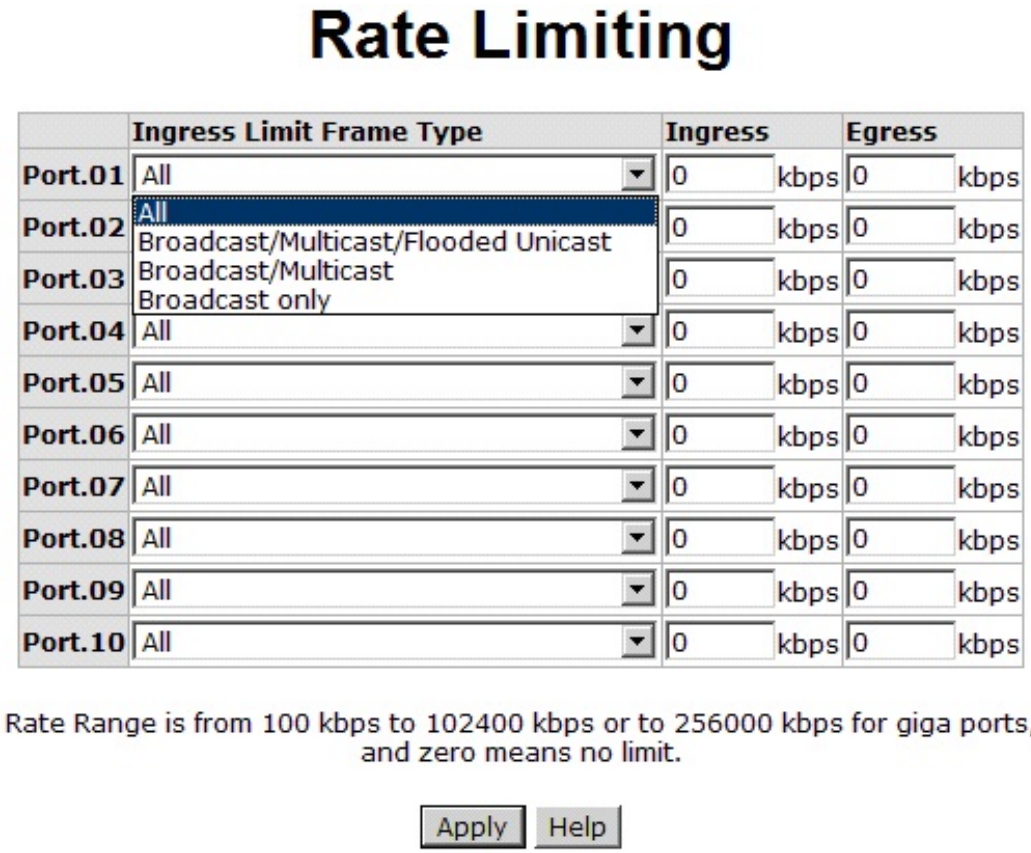
Port Trunk – Port Mirroring interface

6.17 Rate Limiting

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

- **Ingress Limit Frame type**: select the frame type that wants to filter. There are four frame types for selecting:
  > **All**
  > **Broadcast/Multicast/Flooded Unicast**
  > **Broadcast/Multicast**
  > **Broadcast only**

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



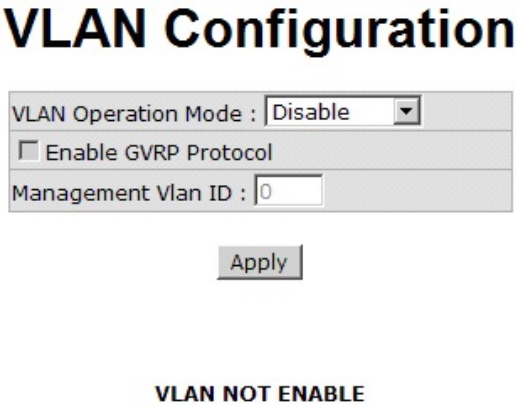
Rate Limiting interface

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

6.18 VLAN configuration

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

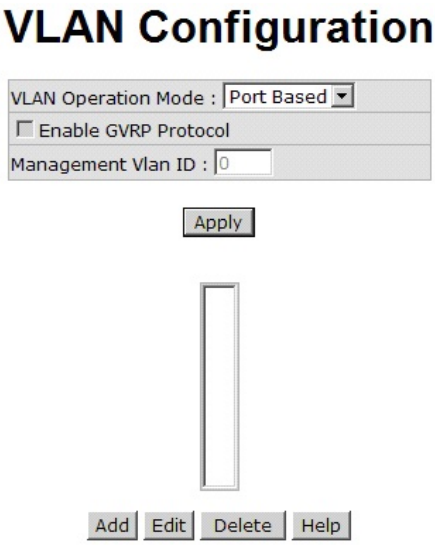
This switch supports **Port-based** and **802.1Q** (tagged-based) VLAN. The default configuration of VLAN operation mode is "**Disable**".



VLAN Configuration interface

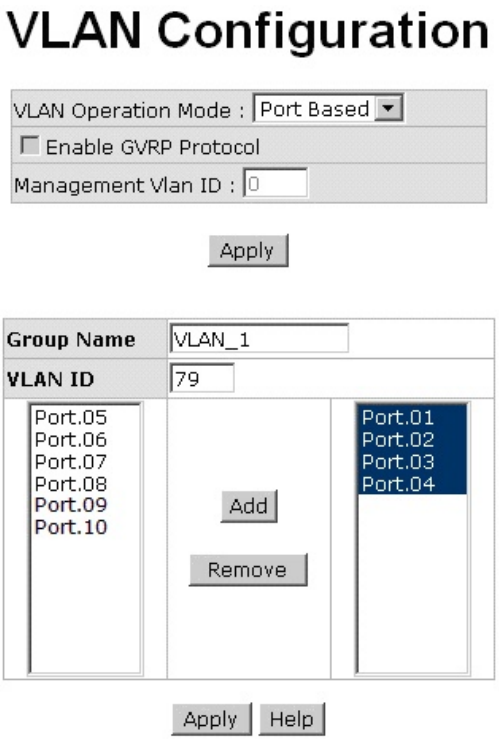
6.18.1 Port-based VLAN

A port-based VLAN basically 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. If the port-based VLAN enabled, the VLAN-tagging is ignored. The port-based VLAN function 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.



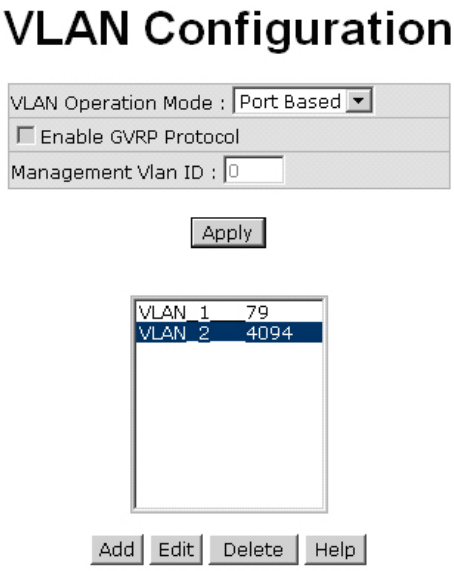
VLAN – Port Based interface

- Pull down the selection item and focus on **Port Based** then press Apply to set the VLAN Operation Mode in **Port Based** mode.
- Click Add to add a new VLAN group (The maximum VLAN groups are up to 64).



VLAN—Port Based Add interface

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



VLAN—Port Based Edit/Delete interface

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

[note]	Remember to execute the "Save Configuration" action, otherwise the new configuration will lose when switch power off.

6.18.2 802.1Q VLAN

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

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

Each member port of 802.1Q is on either an Access Link (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 one 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.

802.1Q Configuration

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

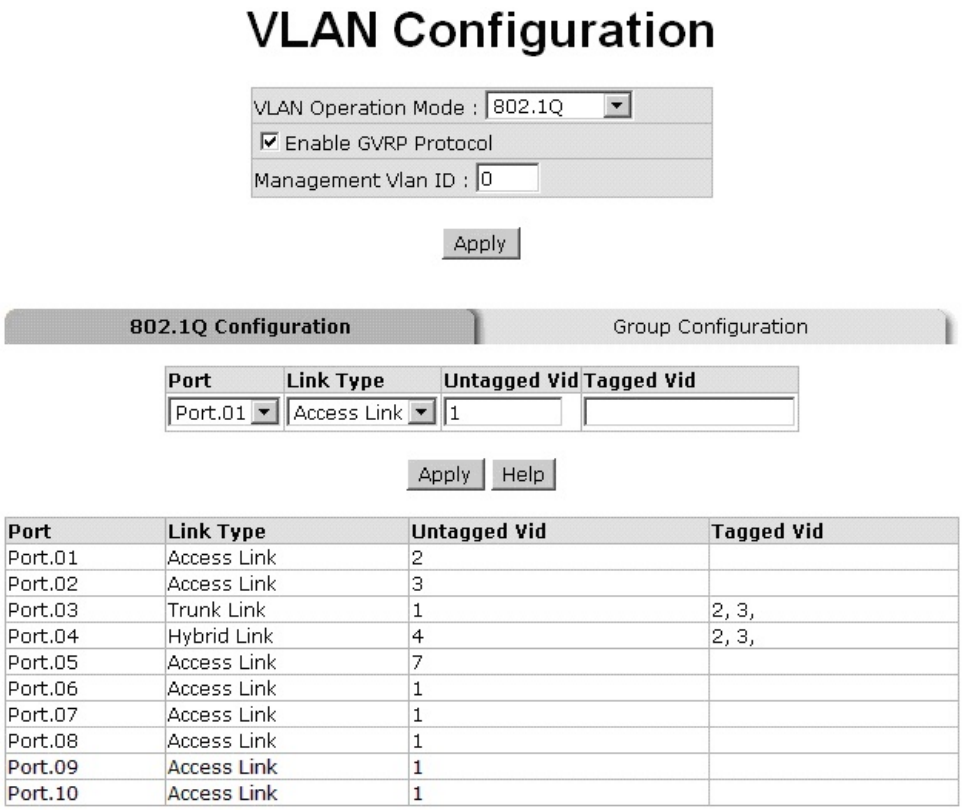
  > Trunk Link: A segment which provides the link path for one or more VLAN-aware devices (switches). A Trunk Port, connected to the trunk link, has an understanding of tagged frame, which is used for the communication among VLANs across switches. Which frames of the specified VIDs will be forwarded depends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

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

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

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

- **Untagged VID**: This column field is available when Link Type is set as Access Link and Hybrid Link. Assign a number in the range between 1 an 4094.
- **Tagged VID**: This column field is available when Link Type is set as Trunk Link and Hybrid Link. Assign a number in the range between 1 an 4094.
- Click Apply to have the configuration take effect.
- You can see the link type, untagged VID, and tagged VID information of each port in the table below on the screen.



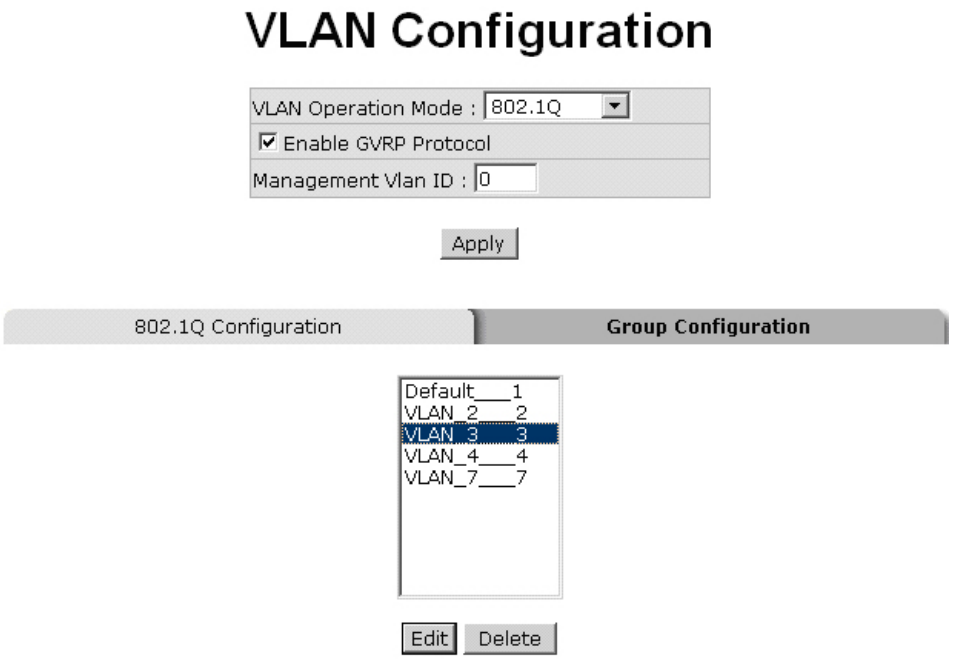
802.1Q VLAN interface

Group Configuration

Edit the existing VLAN Group.

> Select the VLAN group in the table list.

> Click Edit .



Group Configuration interface

> Click Apply .

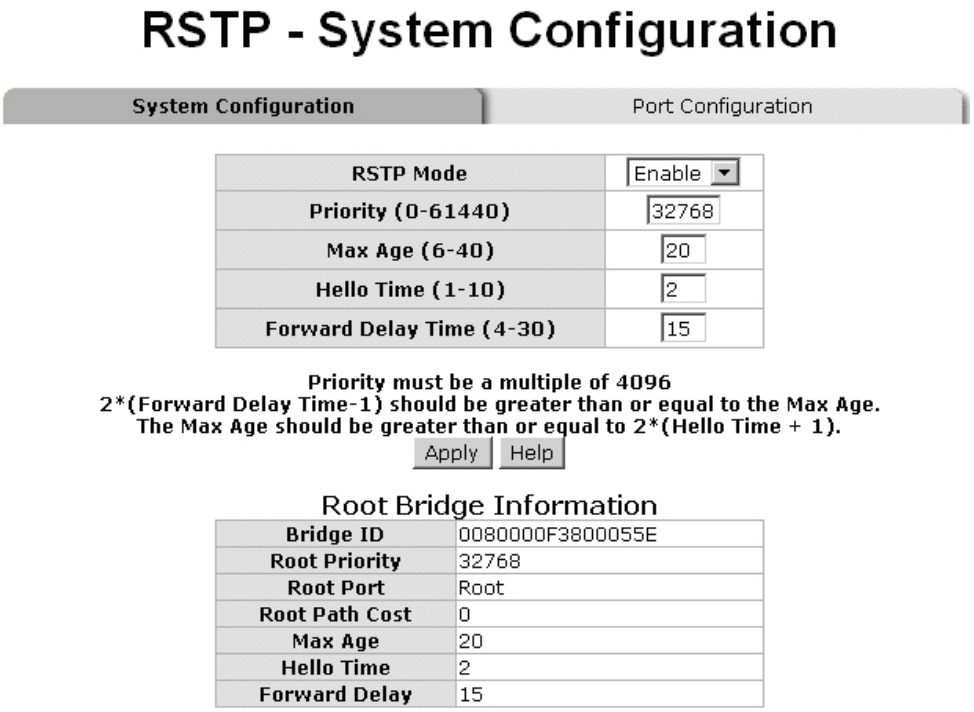
6.19 Rapid Spanning Tree

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

6.19.1 RSTP System Configuration

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

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

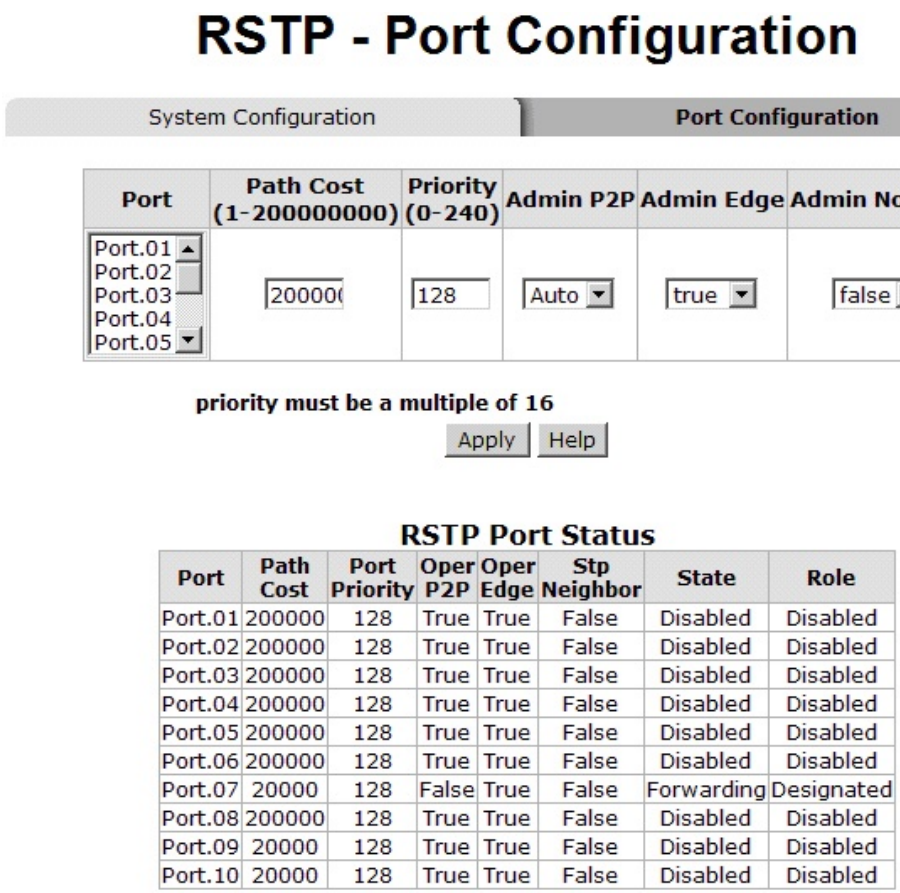


RSTP System Configuration interface

6.19.2 Port Configuration

This web page provides the port configuration interface for RSTP. You can assign higher or lower priority to each port. Rapid spanning tree 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.

- Select the port in the port column field.
- **Path Cost**: The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200,000,000.
- **Priority**: Decide which port should be blocked by setting its priority as the lowest. Enter a number between 0 and 240. The value of priority must be the 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 status 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 end stations won't create bridging loop in the network. To configure the port as an edge port, set the port to "True" status.
- **Admin Non Stp**: The port includes the STP mathematic calculation. True is not including STP mathematic calculation. False is including the STP mathematic calculation.
- Click Apply .



RSTP Port Configuration interface

6.20 SNMP Configuration

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

6.20.1 System Configuration

- Community Strings

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

> **String**: Fill the name string.

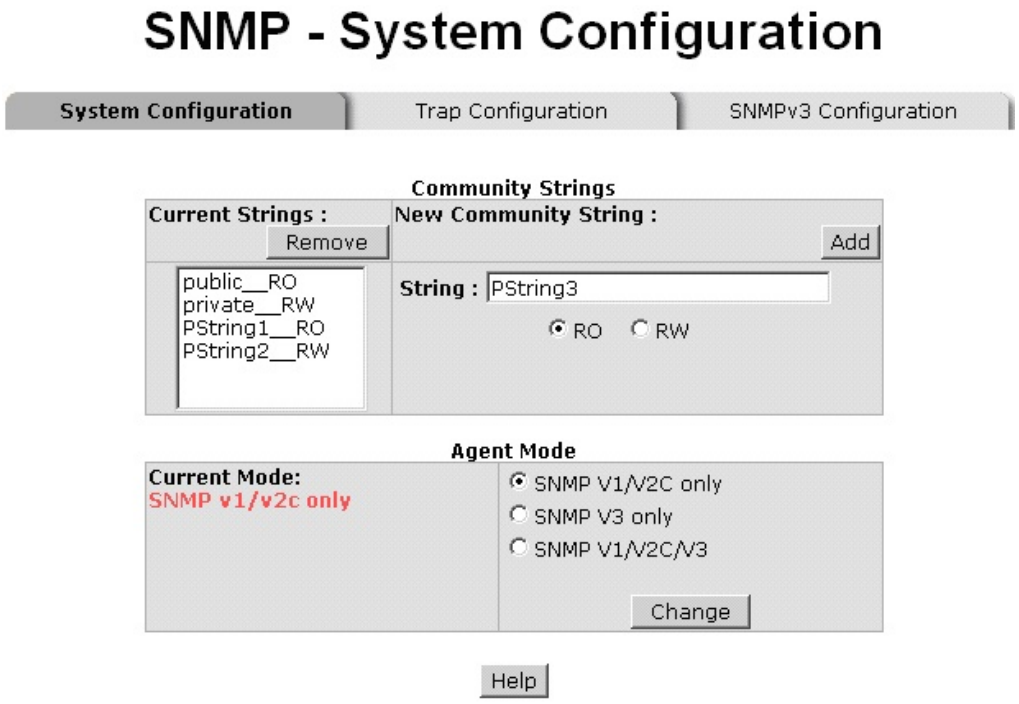
> **RO**: Read only. Enables requests accompanied by this community string to display MIB-object information.

> **RW**: Read/write. Enables requests accompanied by this community string to display MIB-object information and to set MIB objects.

Click Add.

> To remove the community string, select the community string that you defined before 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**: Select the SNMP version that you want to use it. And then click Change to switch to the selected SNMP version mode.

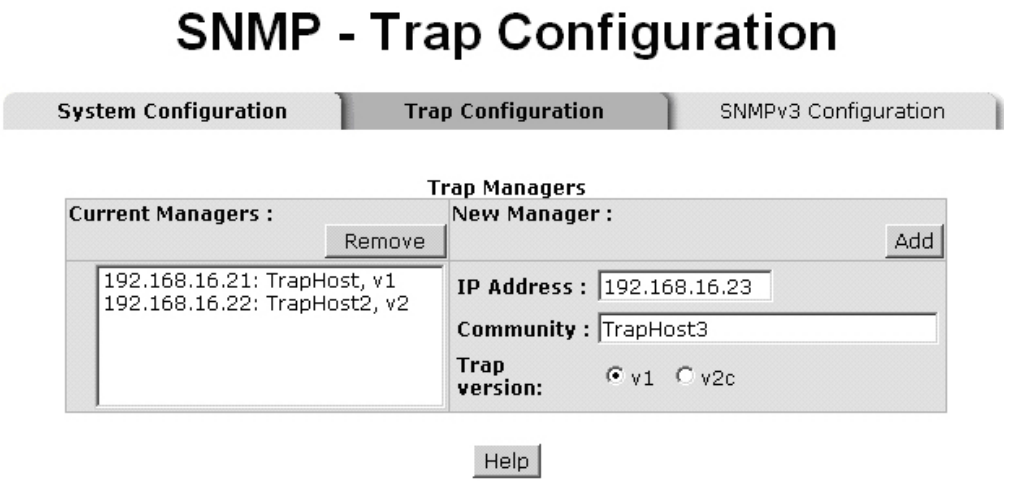


SNMP System Configuration interface

6.20.2 Trap Configuration

A trap manager is a management station that receives the trap messages generated by the switch. If no trap manager is defined, no traps will be issued. 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 type—v1 or v2c.
- Click Add .
- To remove the community string, select the community string listed in the current managers field and click Remove .



Trap Managers interface

6.20.3 SNMPV3 Configuration

Configure the SNMP V3 function.

Context Table

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

User Table

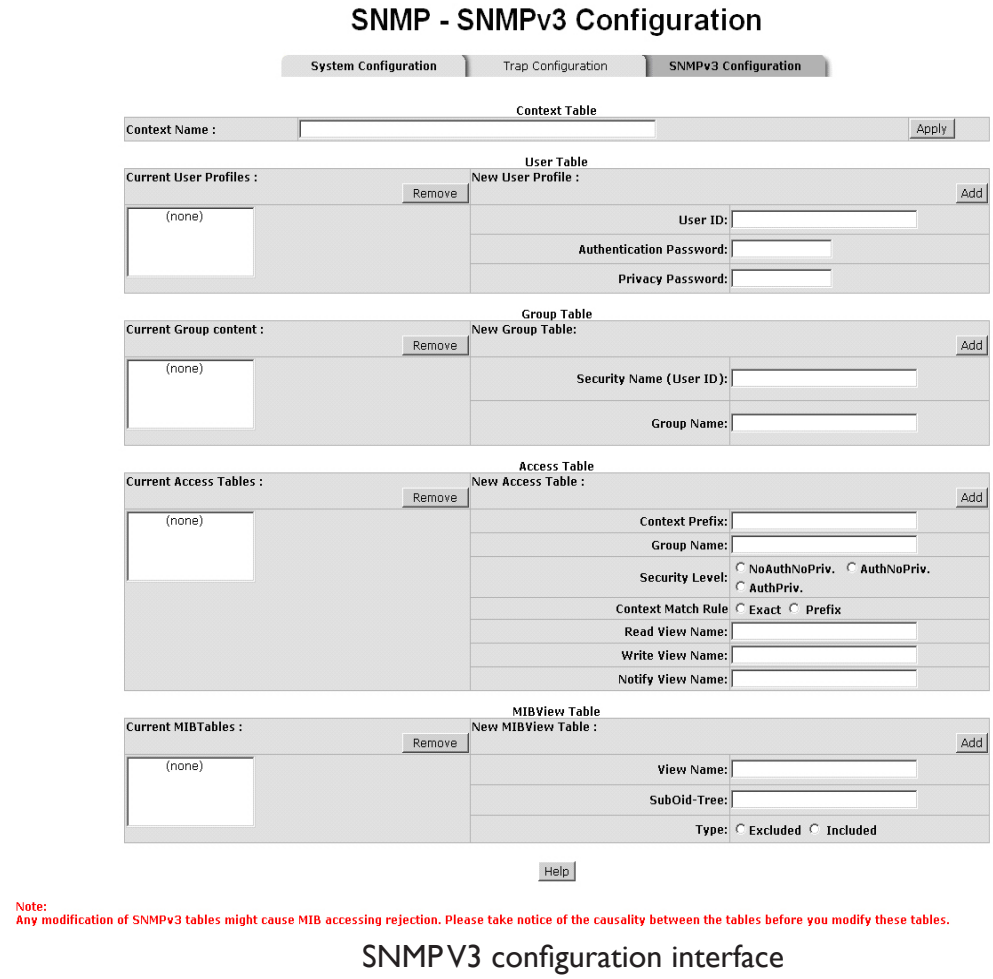
Configure SNMP v3 user table..

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

Group Table

Configure SNMP v3 group table.

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



SNMP V3 configuration interface

Access Table

Configure SNMP v3 access table.

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

MIBview Table

Configure MIB view table.

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

6.21 QoS Configuration

Quality of Service (QoS) is the ability to provide different priority to different applications, users or data flows, or to guarantee a certain level of performance to a data flow. QoS guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications such as voice over IP or Video Teleconferencing, since these often require fixed bit rate and are delay sensitive, and in networks where the capacity is a limited resource, for example in cellular data communication. In the absence of network congestion, QoS mechanisms are not required.

6.21.1 QoS Policy and Priority Type

Here you can choose to use an 8-4-2-1 queuing scheme or a strict priority scheme, or select the priority type to configure QoS policy.

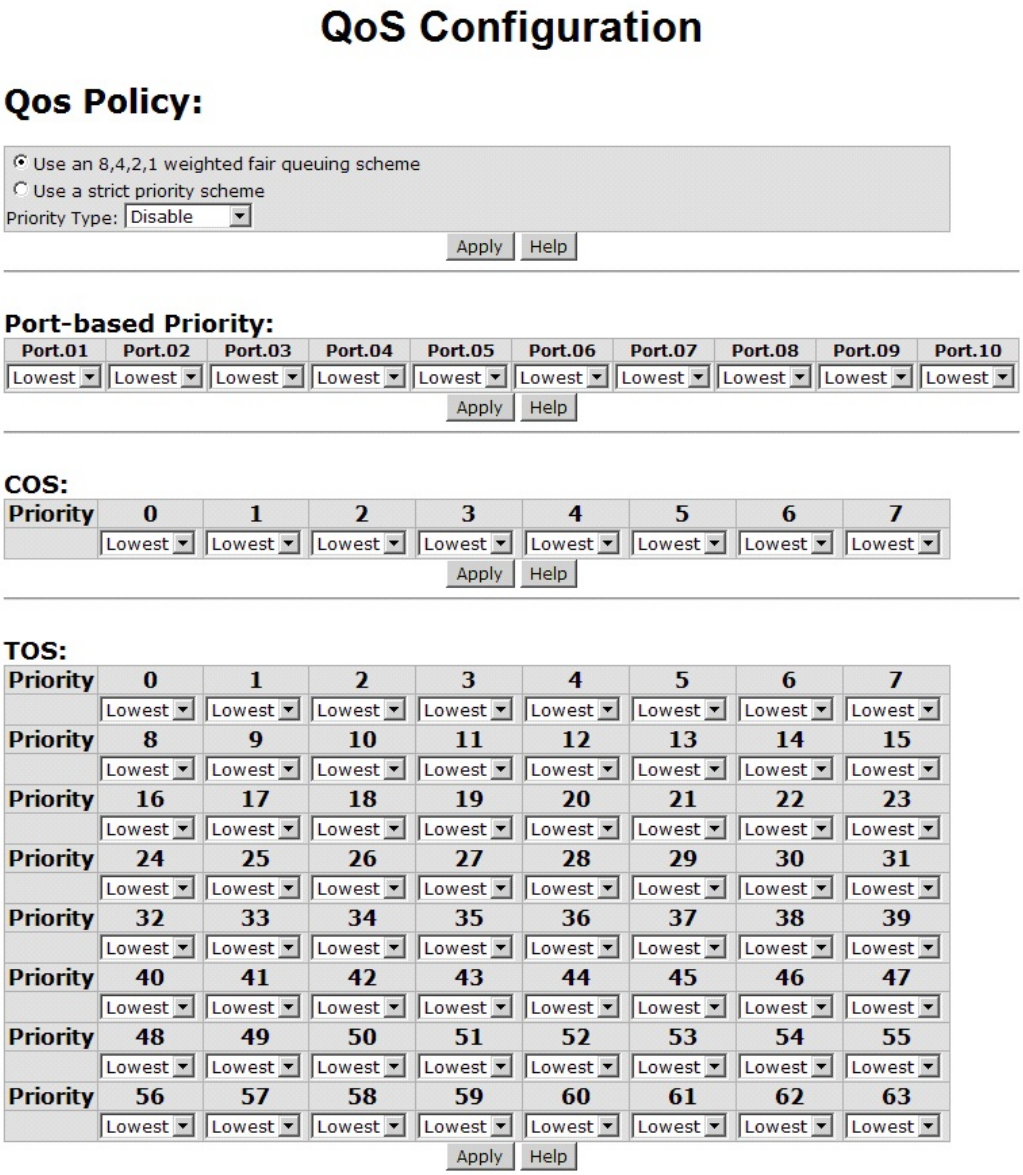
- **QoS Policy**: Select the QoS policy rule.
  - > **Using the 8,4,2,1 weight fair queue scheme**: The switch will follow 8:4:2:1 rate to process priority queue from High to lowest queue. For example, while the system processing, 1 frame of the lowest queue, 2 frames of the low queue, 4 frames of the middle queue, and 8 frames of the high queue will be processed at the same time in accordance with the 8,4,2,1 policy rule.

> **Use a strict priority scheme**: Always the higher queue will be processed first, except the higher queue is empty.

> **Priority Type**: There are 5 priority type selections available—**Port-based, TOS only, COS only, TOS first**, and **COS first**. Disable means no priority type is selected.

Click to have the configuration take effect.

- Click Apply to have the configuration take effect.



QoS Configuration interface

6.21.2 Port-based Priority

Configure the priority level for each port. With the drop-down selection item of **Priority Type** above being selected as Port-based, this control item will then be available to set the queuing policy for each port.

- **Port x**: Each port has 4 priority levels—High, Middle, Low, and Lowest—to be chosen.
- Click Apply to have the configuration take effect.

6.21.3 COS Configuration

Set up the COS priority level. With the drop-down selection item of **Priority Type** above being selected as COS only/COS first, this control item will then be available to set the queuing policy for each port.

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

6.21.4 TOS Configuration

Set up the TOS priority. With the drop-down selection item of **Priority Type** above being selected as TOS only/TOS first, this control item will then be available to set the queuing policy for each port.

- **TOS priority**: The system provides 0~63 TOS priority level. Each level has 4 types of priority—High, Middle, Low, and Lowest. The default value is 'Lowest' priority for each level. When the IP packet is received, the system will check the TOS level value in the IP packet that has received. For example, the user sets the TOS level 25 as high, the system will check the TOS value of the received IP packet. If the TOS value of received IP packet is 25 (priority = high), and then the packet priority will have highest priority.
- Click Apply to have the configuration take effect..

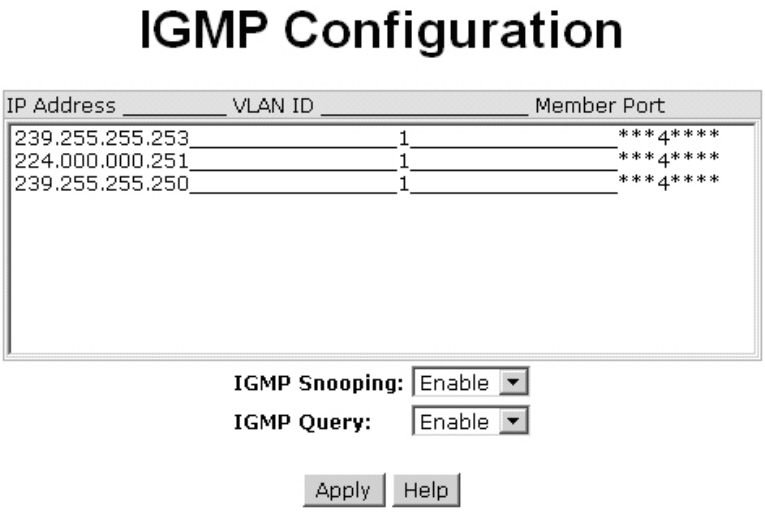
6.22 IGMP Configuration

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

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

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

- **IGMP Protocol**: enable or disable the IGMP protocol.
- **IGMP Query**: enable or disable the IGMP query function. The IGMP query information will be displayed in IGMP status section.
- Click Apply .



IGMP Configuration interface

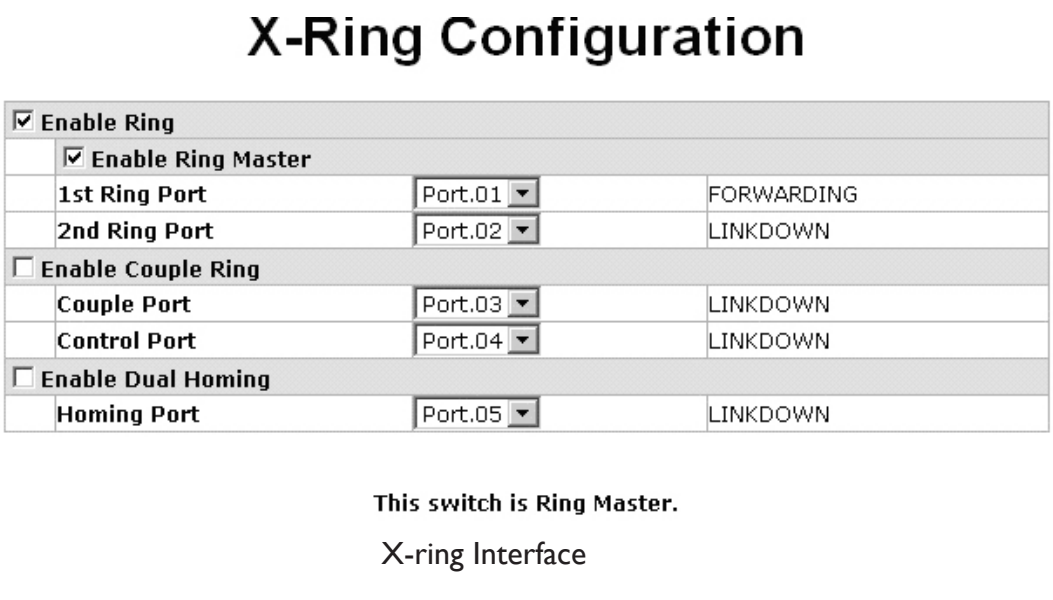
6.23 X-Ring

X-Ring provides a faster redundant recovery than Spanning Tree topology. The action is similar to STP or RSTP, but the algorithms between them are not the same. In the X-Ring topology, every switch should be enabled with X-Ring function and two ports should be assigned as the member ports in the ring. Only one switch in the X-Ring group would be set as the master switch that one of its two member ports would be blocked, called backup port, and another port is called working port. Other switches in the X-Ring group are called working switches and their two member ports are called working ports. When the failure of network connection occurs, the backup port of the master switch (Ring Master) will automatically become a working port to recover from the failure.

The switch supports the function and interface for setting the switch as the ring master or not. The ring master can negotiate and place command to other switches in the X-Ring group. If there are 2 or more switches in master mode, the software will select the switch with lowest MAC address number as the ring master. The X-Ring master ring mode can be enabled by setting the X-Ring configuration interface. Also, the user can identify whether the switch is the ring master by checking the R.M. LED indicator on the panel of the switch.

The system also supports the **Couple Ring** that can connect 2 or more X-Ring group for the redundant backup function; **Dual Homing** function that can prevent connection lose between X-Ring group and upper level/core switch.

- **Enable Ring**: To enable the X-Ring function, tick the checkbox beside the **Enable Ring** string label. If this checkbox is not ticked, all the ring functions are unavailable.
  > **Enable Ring Master**: Tick the checkbox to enable this switch to be the ring master.
  > **1st & 2nd Ring Ports**: Pull down the selection menu to assign the ports as the member ports. **1st Ring Port** is the working port and **2nd Ring Port** is the backup port. When **1st Ring Port** fails, the system will automatically upgrade the **2nd Ring Port** to be the working port.
- **Enable Couple Ring**: To enable the couple ring function, tick the checkbox beside the Enable Couple Ring string label.
  > Couple Port: Assign the member port which is connected to the other ring group.
  > Control Port: When the Enable Couple Ring checkbox is ticked, you have to assign the control port to form a couple-ring group between the two X-rings.
- **Enable Dual Ring**: When this check box is ticked, the '**Enable Ring Master**' check box will then also be enabled by the system, which means this equipment is assigned as the Ring Master. The Dual Ring differs from the Couple Ring in that it only needs a unit to form a redundant linking system of two rings.
- And then, click Apply to have the configuration take effect.



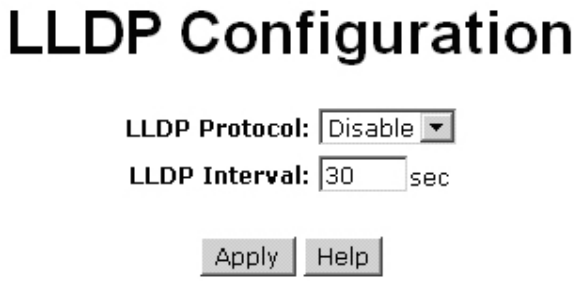
X-ring Interface

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

6.24 LLDP Configuration

Link Layer Discovery Protocol (LLDP) is defined in the IEEE 802.1AB, it is an emerging standard which provides a solution for the configuration issues caused by expanding LANs. LLDP specifically defines a standard method for Ethernet network devices such as switches, routers and wireless LAN access points to advertise information about themselves to other nodes on the network and store the information they discover. LLDP runs on all 802 media. The protocol runs over the data-link layer only, allowing two systems running different network layer protocols to learn about each other.

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



LLDP Interface

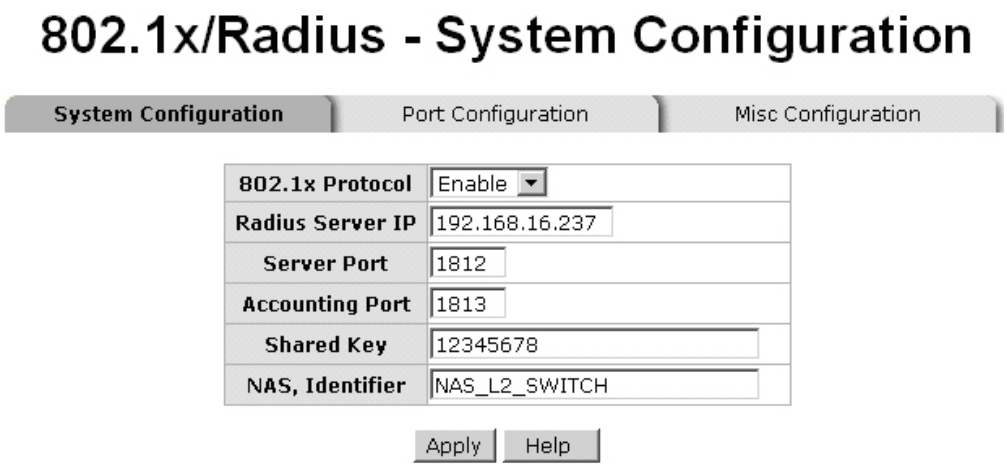
6.25 Security—802.1X/Radius Configuration

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

6.25.1 System Configuration

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

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

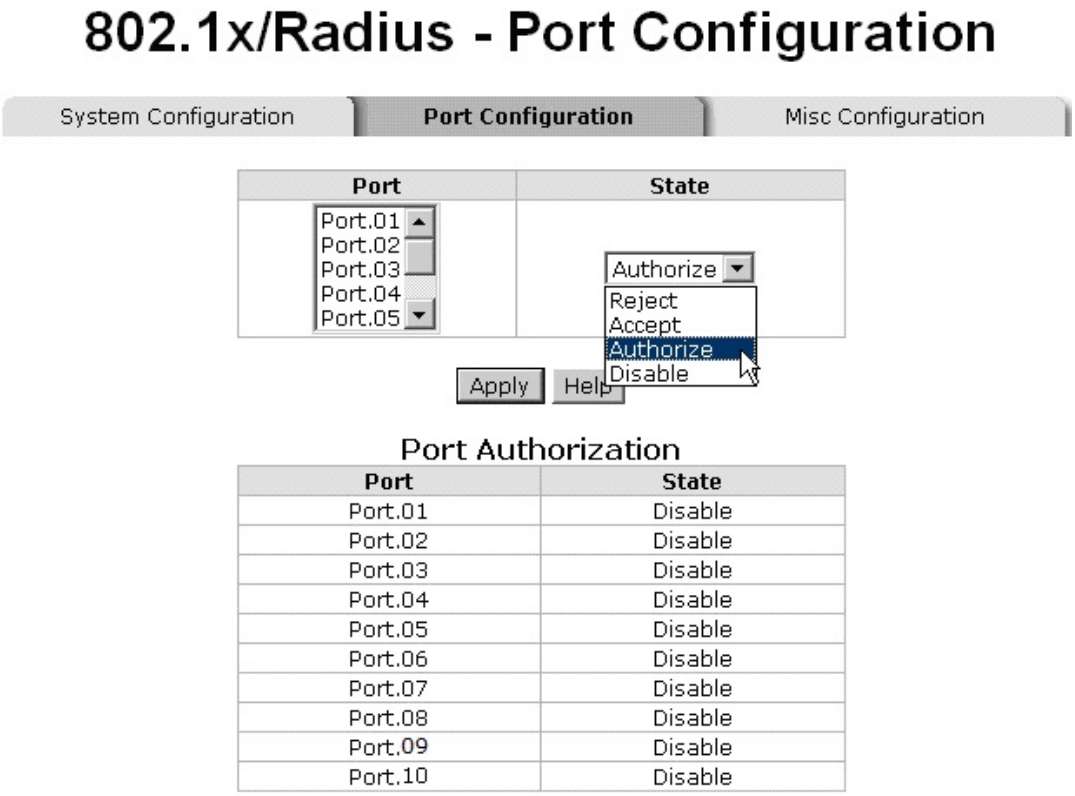


802.1x System Configuration interface

6.25.2 Port Configuration

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

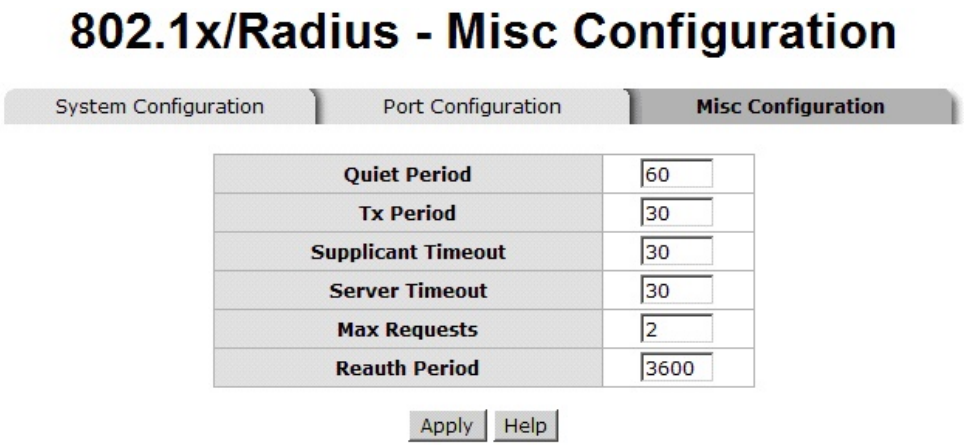
- **Reject**: The specified port is required to be held in the unauthorized state.
- **Accept**: The specified port is required to be held in the authorized state.
- **Authorize**: The specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange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



802.1x Per Port Setting interface

6.25.3 Misc Configuration

- **Quiet Period:** Set the period which the port doesn't try to acquire a supplicant.
- **TX Period**: Set the period port waits for retransmit 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 which clients connected must be re-authenticated.
- Click Apply .



802.1x Misc Configuration interface

6.26 MAC Address Table

Use the MAC address table to ensure the port security.

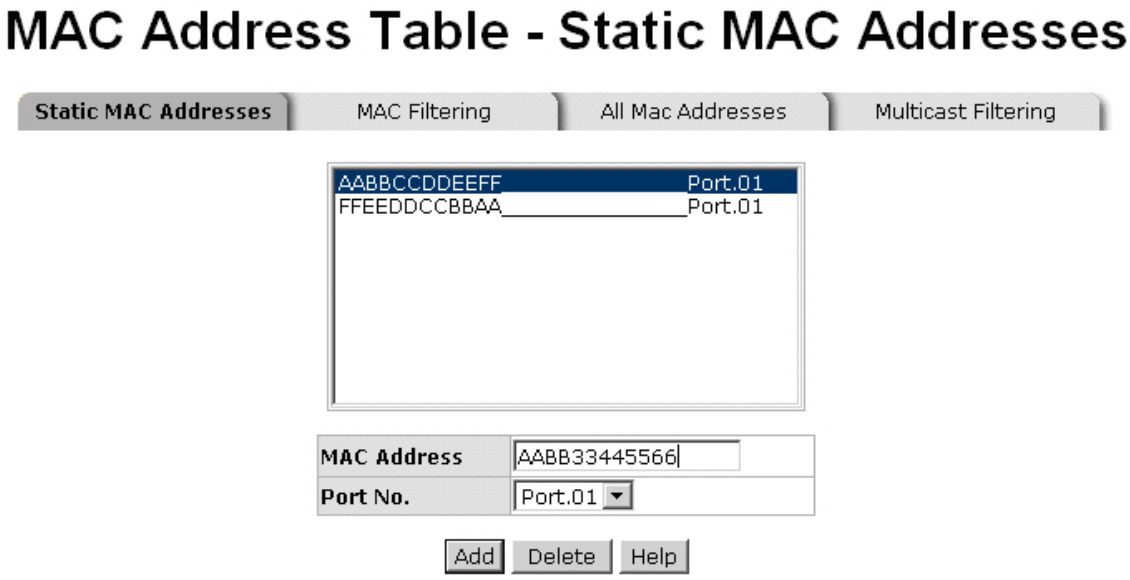
6.26.1 Static MAC Address

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 / delete a static MAC address.

Add the Static MAC Address

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

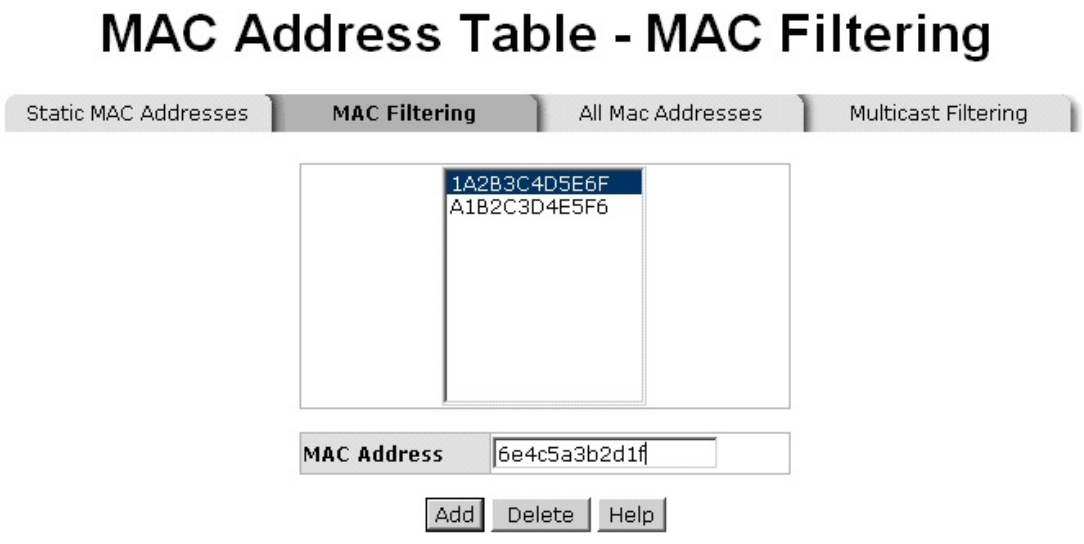
- **MAC Address**: Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.
- **Port No.**: Pull down the selection menu to select the port number.
- Click Apply .
- If you want to delete the MAC address from filtering table, select the MAC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



Static MAC Addresses interface

6.26.2 MAC Filtering

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



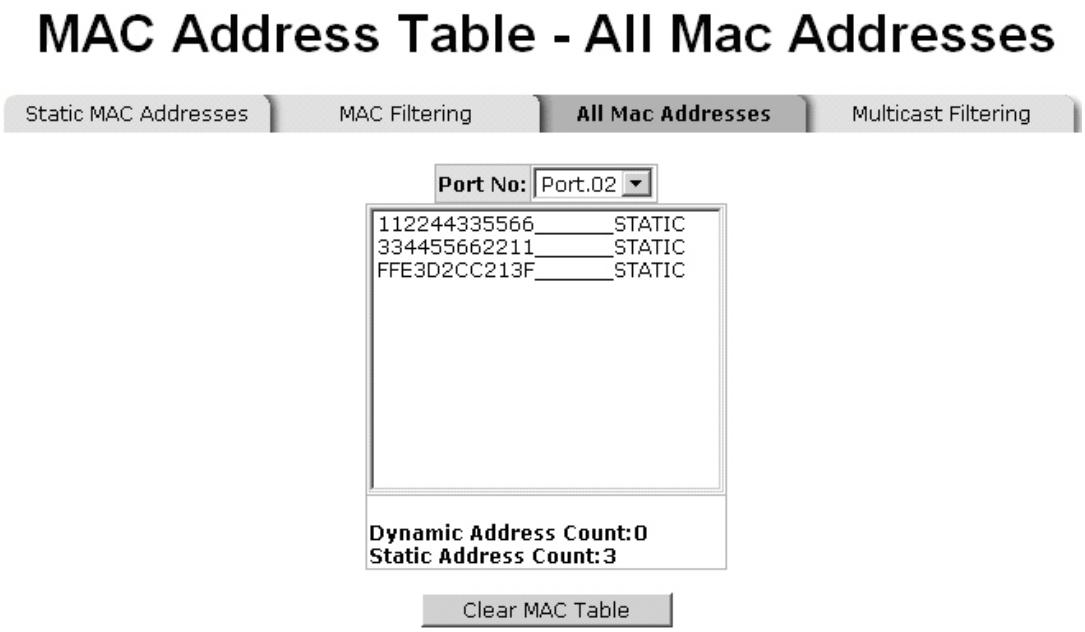
MAC Filtering interface

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

6.26.3 All MAC Addresses

You can view all of the MAC addresses learned by the selected port.

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

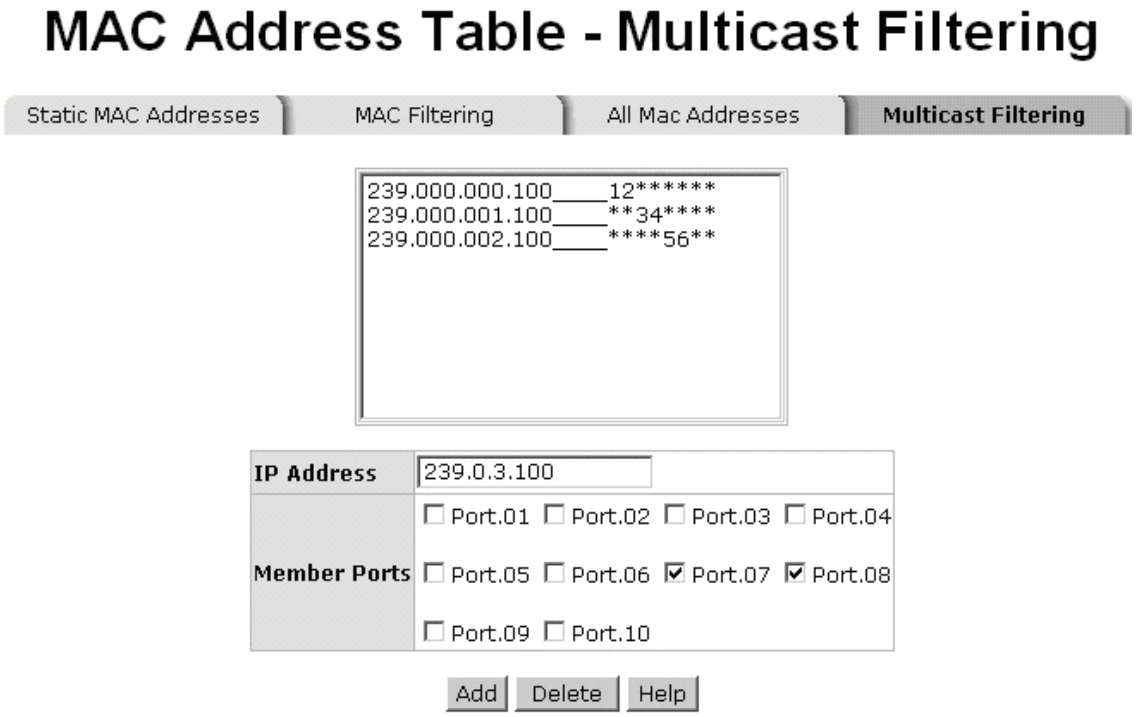


All MAC Address interface

6.26.4 MAC Address Table—Multicast Filtering

Multicasts are similar to broadcasts, they are sent to all end stations on a LAN or VLAN. Multicast filtering is the function, which end stations can receive the multicast traffic if the connected ports had been included in the specific multicast groups. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to the registered end stations.

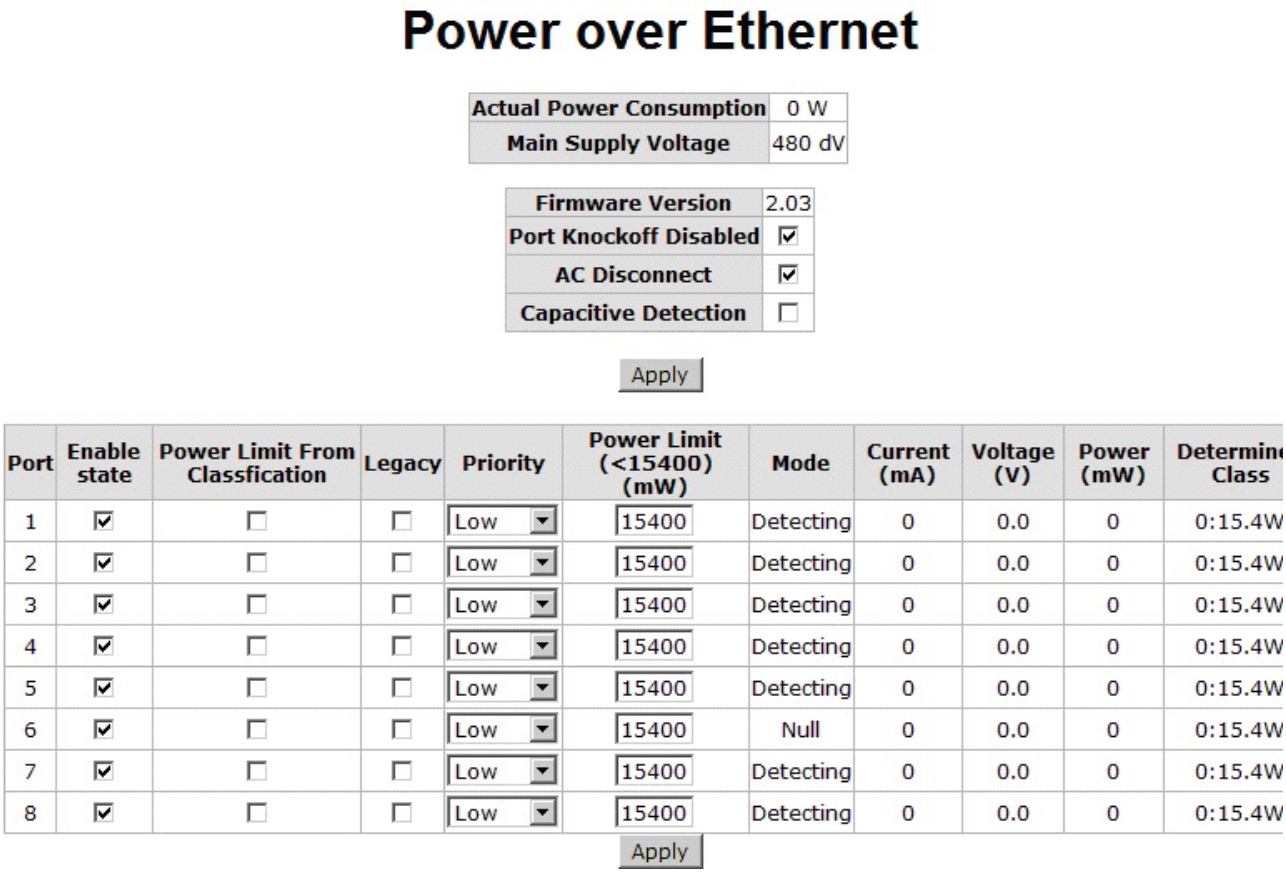
- **IP Address**: Assign a multicast group IP address in the range of 224.0.0.0 ~ 239.255.255.255.
- **Member Ports**:Tick the check box beside the port number to include them as the member ports in the specific multicast group IP address.
- Click Add to append a new filter of multicast to the field,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



Multicast Filtering interface

6.27 Power over Ethernet

This segment shows the Power over Ethernet function.



PoE Status

- **Actual Power Consumption**: This column shows the real-time total power consumption.
- **Main Supply Voltage**: This column shows the output voltage of the system for PoE ports.
- **Firmware Version**: This column shows the PoE chip's firmware version.
- **Port Knockoff Disabled**: Power Management state where one or more PDs have been powered down so that a higher priority PD may be powered up and yet not exceed the maximum total power available for PDs.
- **AC Disconnect**: Tick this checkbox to monitor the AC impedance on the port terminals and removes power when the impedance rises above a certain value, for a certain period (for details, see the IEEE 802.3af specification).
- **Capacitive Detection**: If the port and capacitive detection are enabled, the capacitances state reads in the voltage result from the constant current. This is then subtracted from the pre-capacitance voltage to get a charge rate. If this charge rate is within the window of the PD signatures, the device is considered to be discovered.
- And then, click Apply to carry into effect.
- **Port**: The index of PoE ports.
- **Enable State**: Check it to enable the PoE function to the port.

- **Power Limit From**: Check it to decide the power limit method.
  Classification: *When this check box is ticked, the system will limit the power supply to the powered device in accordance with the related class.*
- **Legacy**: Check it to support the legacy power devices.
- **Priority**: Pull down the selection menu item to choose the priority of power supplying.
- **Port Limit (<15400) mW**: User can key in the power limit value which is under 15.4 Watts.
- **Mode**: Displays the operating mode of the port.
- **Current (mA)**: Displays the operating current of the port.
- **Voltage (V)**: Displays the operating voltage of the port.
- **Power (mW)**: Displays the power consumption of the port.
- **Determined Class**: Displays the PD's class.
- And then, click Apply to carry into effect.

6.28 Factory Default

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



Factory Default interface

6.29 Save Configuration

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



Save Configuration interface

6.30 System Reboot

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



System Reboot interface

Troubles shooting

- Verify that is using the right power cord/adapter (DC 24-48V), please don't use the power adapter with DC output higher than 48V, or it may damage this device.
- Select the proper UTP/STP cable to construct the user network. Use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ-45 connections that depend on the connector type the switch equipped: 100Ω Category 3, 4 or 5 cable for 10Mbps connections, 100Ω Category 5 cable for 100Mbps connections, or 100Ω Category 5e/above cable for 1000Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).
- **Diagnosing LED Indicators**: To assist in identifying problems, the switch can be easily monitored through panel indicators, which describe common problems the user may encounter and where the user can find possible solutions.
- If the power indicator does not light on when the power cord is plugged in, you may have a problem with power cord. Then check for loose power connections, power losses or surges at power outlet. If you still cannot resolve the problem, contact the local dealer for assistance.
- If the LED indicators are normal and the connected cables are correct but the packets still cannot be transmitted. Please check the user system's Ethernet devices' configuration or status.

Appendix A—RJ-45 Pin Assignment

RJ-45 Pin Assignments

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

- **10 /100BASE-TX Pin outs**

  With10/100BASE-TX cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 for receiving data.

- **RJ-45 Pin Assignments**

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

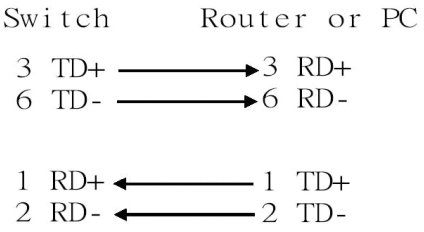
[note]	"+" and "-" signs represent the polarity of the wires that make up each wire pair.

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

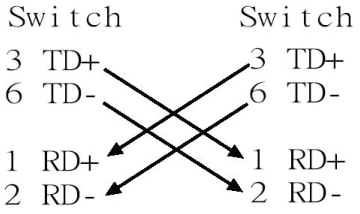
Pin Number	MDI-X Signal Name	MDI Signal Name
1	Receive Data plus (RD+)	Transmit Data plus (TD+)
2	Receive Data minus (RD-)	Transmit Data minus (TD-)
3	Transmit Data plus (TD+)	Receive Data plus (RD+)
6	Transmit Data minus (TD-)	Receive Data minus (RD-)

- **10/100Base-TX Cable Schematic**

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



Straight-through cable schematic

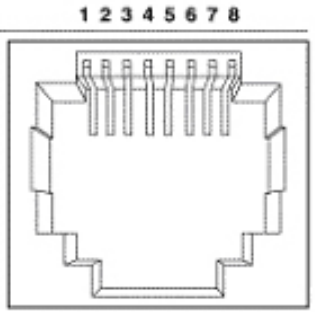


Cross over cable schematic

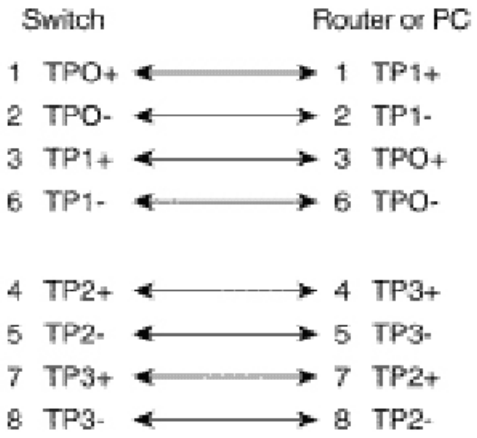
- **10/100/1000Base-TX Pin outs**

The following figure shows the 10/100/1000 Ethernet RJ-45 pin outs.

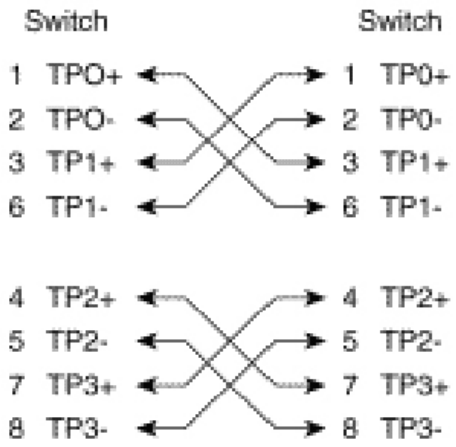
Pin	Label
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



- **10/100/1000Base-TX Cable Schematic**



Straight through cables schematic



Cross over cables schematic

RJ-45 Pin Assignments of POE

With 100BASE-TX/10BASE-T cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 for receiving data; pins 4, 5, 7 and 8 are used for power supplying.

- Pin out of Cisco non-802.3af standard PD

Pin	Signal
1	RX+
2	RX-
3	TX+
4	VCC -
5	VCC -
6	TX-
7	VCC +
8	VCC +

- Pin out of PoE Midspan Hub/Switch

Pin	Signal / Name
1	RX+
2	RX-
3	TX+
4	VCC+
5	VCC+
6	TX-
7	VCC-
8	VCC-

- Pin out of PoE Endspan Hub/Switch

Pin	Signal / Name
1	TX+/VCC+
2	TX-/VCC+
3	TX+/VCC-
4	
5	
6	TX-/VCC-
7	
8	

[note]	'+' and '-' signs represent the polarity of the wires that make up each wire pair. Before you power PD, please check the RJ-45 connector pin assignment follow IEEE802.3af standard; otherwise you may need to change one of the RJ-45 connector pin assignment attached with the UTP cable.

Appendix B—Command Sets

Commands Set List	
User EXEC	E
Privileged EXEC	P
Global configuration	G
VLAN database	V
Interface configuration	I

System Commands Set

Allied Telesis 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 192.168.1.1 255.255.255.0 192.168.1.254
ip dhcp	G	Enable DHCP client function of switch	switch(config)#ip dhcp
show ip	P	Show IP information of switch	switch#show ip
no ip dhcp	G	Disable DHCP client function of switch	switch(config)#no ip dhcp
reload	G	Halt and perform a cold restart	switch(config)#reload
default	G	Restore to default	switch(config)#default
admin username [Username]	G	Changes a login username. (maximum 10 words)	switch(config)#admin username xxxxxx

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

Port Commands Set

Allied Telesis Commands	Level	Description	Example
interface fastEthernet [Portid]	G	Choose the port for modification.	switch(config)#interface fastEthernet 2
duplex [full | half]	I	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#interface fastEthernet 2 switch(config-if)#duplex full
Speed [10|100|1000|auto]	I	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can't be set to 1000 if the port isn't a giga port..	switch(config)#interface fastEthernet 2 switch(config-if)#speed 100
no flowcontrol	I	Disable flow control of interface	switch(config-if)#no flowcontrol
security enable	I	Enable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#security enable
no security	I	Disable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#no security
bandwidth type all	I	Set interface ingress limit frame type to "accept all frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type all
bandwidth type broadcast-multicast-flooded-unicast	I	Set interface ingress limit frame type to "accept broadcast, multicast, and flooded unicast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast-flooded-unicast
bandwidth type broadcast-multicast	I	Set interface ingress limit frame type to "accept broadcast and multicast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast
bandwidth type broadcast-only	I	Set interface ingress limit frame type to "only accept broadcast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-only
bandwidth in [Value]	I	Set interface input bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth in 100

bandwidth out [Value]		Set interface output bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports and zero means no limit.	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth out 100
show bandwidth	I	Show interfaces bandwidth control	switch(config)#interface fastEthernet 2 switch(config-if)#show bandwidth
State [Enable | Disable]	I	Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disable form of this command to disable the port.	switch(config)#interface fastEthernet 2 switch(config-if)#state Disable
show interface configuration	I	show interface configuration status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface configuration
show interface status	I	show interface actual status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface status
show interface accounting	I	show interface statistic counter	switch(config)#interface fastEthernet 2 switch(config-if)#show interface accounting
no accounting	I	Clear interface accounting information	switch(config)#interface fastEthernet 2 switch(config-if)#no accounting

Trunk Commands Set

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

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

vlan 8021q trunk [PortNumber] access-link untag [UntaggedVID]	V	Assign a access link for VLAN by trunk group	switch(vlan)#vlan 8021q trunk 3 access-link untag 33
vlan 8021q trunk [PortNumber] trunk-link tag [TaggedVID List]	V	Assign a trunk link for VLAN by trunk group	switch(vlan)#vlan 8021q trunk 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q trunk 3 trunk-link tag 3-20
vlan 8021q trunk [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]	V	Assign a hybrid link for VLAN by trunk group	switch(vlan)#vlan 8021q trunk 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)#vlan 8021q trunk 3 hybrid-link untag 5 tag 6-8
show vlan [GroupID] or show vlan	V	Show VLAN information	switch(vlan)#show vlan 23
no vlan group [GroupID]	V	Delete port base group ID	switch(vlan)#no vlan group 2

Spanning Tree Commands Set

Allied Telesis 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 32768
spanning-tree max-age [seconds]	G	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	switch(config)#spanning-tree max-age 15
spanning-tree hello-time [seconds]	G	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#spanning-tree hello-time 3
spanning-tree forward-time [seconds]	G	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	switch(config)#spanning-tree forward-time 20
stp-path-cost [1~200000000]	I	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state.	switch(config)#interface fastEthernet 2 switch(config-if)#stp-path-cost 20

stp-path-priority [Port Priority]	I	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch.	switch(config)#interface fastEthernet 2 switch(config-if)#stp-path-priority 128
stp-admin-p2p [Auto|True|False]	I	Admin P2P of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)#stp-admin-p2p Auto
stp-admin-edge [True|False]	I	Admin Edge of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)#stp-admin-edge True
stp-admin-non-stp [True|False]	I	Admin NonSTP of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)#stp-admin-non-stp False
show spanning-tree	E	Displays a summary of the spanning-tree states.	switch>show spanning-tree
no spanning-tree	G	Disable spanning-tree.	switch(config)#no spanning-tree

QOS Commands Set

Allied Telesis 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

Allied Telesis Commands	Level	Description	Example
igmp enable	G	Enable IGMP snooping function	switch(config)#igmp enable
lgmp-query auto	G	Set IGMP query to auto mode	switch(config)#lgmp-query auto
lgmp-query force	G	Set IGMP query to force mode	switch(config)#lgmp-query force
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 flooding
show igmp configuration	P	Displays the details of an IGMP configuration.	switch#show igmp configuration
no igmp	G	Disable IGMP snooping function	switch(config)#no igmp
no igmp-query	G	Disable IGMP query	switch#no igmp-query

Multicast Filtering Commands Set

Allied Telesis Commands	Level	Description	Example
multicast-filtering [IP-Addr]	I	Configure multicast filtering entry of interface	Switch(config)#interface fastEthernet 2 switch(config-if)#multicast-filtering 228.1.1.1
no multicast-filtering [IP-Addr]	I	Remove multicast filtering entry of interface	Switch(config)#interface fastEthernet 2 switch(config-if)#no multicast-filtering 228.1.1.1

LLDP Commands Set

Allied Telesis Commands	Level	Description	Example
lldp enable	G	Enable LLDP function	switch(config)#lldp enable
lldp interval [Time sec]	G	Configure LLDP interval	switch(config)#lldp interval 20

Mac / Filter Table Commands Set

Allied Telesis 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 filter hwaddr [MAC]	G	Remove an entry of MAC address table (filter)	switch(config)#no mac-address-table filter hwaddr 000012348678
no mac-address-table	G	Remove dynamic entry of MAC address table	switch(config)#no mac-address-table

SNMP Commands Set

Allied Telesis Commands	Level	Description	Example
snmp system-name [System Name]	G	Set SNMP agent system name	switch(config)#snmp system-name l2switch
snmp system-location [System Location]	G	Set SNMP agent system location	switch(config)#snmp system-location lab
snmp system-contact [System Contact]	G	Set SNMP agent system contact	switch(config)#snmp system-contact where
snmp agent-mode [v1v2c|v3|v1v2cv3]	G	Select the agent mode of SNMP	switch(config)#snmp agent-mode v1v2cv3
snmp community-strings [Community] right [RO/RW]	G	Add SNMP community string.	switch(config)#snmp community-strings public right rw
snmp-server host [IP address] community [Community-string] trap-version [v1|v2c]	G	Configure SNMP server host information and community string	switch(config)#snmp-server host 192.168.1.50 community public trap-version v1 (remove) Switch(config)# no snmp-server host 192.168.1.50
snmpv3 context-name [Context Name]	G	Configure the context name	switch(config)#snmpv3 context-name Test
snmpv3 user [User Name] group [Group Name] password [Authentication Password] [Privacy Password]	G	Configure the userprofile for SNMPV3 agent. Privacy password could be empty.	switch(config)#snmpv3 user test01 group G1 password AuthPW PrivPW
snmpv3 access context-name [Context Name] group [Group Name] security-level [NoAuthNoPriv|AuthNoPriv|AuthPriv] match-rule [Exact|Prifix] views [Read View Name] [Write View Name] [Notify View Name]	G	Configure the access table of SNMPV3 agent	switch(config)#snmpv3 access context-name Test group G1 security-level AuthPriv match-rule Exact views V1 V1 V1

snmpv3 mibview view [View Name] type [Excluded|Included] sub-oid [OID]	G	Configure the mibview table of SNMPV3 agent	switch(config)#snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1
show snmp	P	Show SNMP configuration	switch#show snmp
no snmp community-strings [Community]	G	Remove the specified community.	switch(config)#no snmp community-strings public
no snmp-server host [Host-address]	G	Remove the SNMP server host.	switch(config)#no snmp-server host 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 AuthPriv 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

Allied Telesis Commands	Level	Description	Example
monitor [RX|TX|Both]	I	Configure source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#monitor RX
monitor rx [Port ID]	G	Set RX destination port of monitor function	switch(config)#monitor rx 2
monitor tx [Port ID]	G	Set TX destination port of monitor function	switch(config)#monitor tx 3
show monitor	P	Show port monitor information	switch#show monitor
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

Allied Telesis 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 1812
accountport [port ID]	G	Use the 802.1x system account port global configuration command to change the accounting port	switch(config)# 8021x system accountport 1813
8021x system sharedkey [ID]	G	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)# 8021x system sharedkey 123456
8021x system nasid [words]	G	Use the 802.1x system nasid global configuration command to change the NAS ID	switch(config)# 8021x system nasid test1
8021x misc quietperiod [sec.]	G	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch(config)# 8021x misc quietperiod 10
8021x misc txperiod [sec.]	G	Use the 802.1x misc TX period global configuration command to set the TX period.	switch(config)# 8021x misc txperiod 5
8021x misc supptimeout [sec.]	G	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	switch(config)# 8021x misc supptimeout 20
8021x misc servertimeout [sec.]	G	Use the 802.1x misc server timeout global configuration command to set the server timeout.	switch(config)#8021x misc servertimeout 20

8021x misc maxrequest [number]	G	Use the 802.1x misc max request global configuration command to set the MAX requests.	switch(config)# 8021x misc maxrequest 3
8021x misc reauthperiod [sec.]	G	Use the 802.1x misc reauth period global configuration command to set the reauth period.	switch(config)# 8021x misc reauthperiod 3000
8021x portstate [disable | reject | accept | authorize]	I	Use the 802.1x port state interface configuration command to set the state of the selected port.	switch(config)#interface fastethernet 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

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

SystemLog, SMTP and Event Commands Set

Allied Telesis 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 sender [sendername]	G	Configure sender of mail	switch(config)#smtp snder aaa@bbb.com
smtp authentication	G	Enable SMTP authentication	switch(config)#smtp authentication
smtp account [account]	G	Configure authentication account	switch(config)#smtp account John
smtp password [password]	G	Configure authentication password	switch(config)#smtp password 1234
smtp rcptemail [Index] [Email address]	G	Configure Rcpt e-mail Address	switch(config)#smtp rcptemail 1 Alert@test.com
show smtp	P	Show the information of SMTP	switch#show smtp
no smtp	G	Disable SMTP function	switch(config)#no smtp
event device-cold-start [Systemlog|SMTP|Both]	G	Set cold start event type	switch(config)#event device-cold-start both
event authentication-failure [Systemlog|SMTP|Both]	G	Set Authentication failure event type	switch(config)#event authentication-failure both
event ring-topology-change [Systemlog|SMTP|Both]	G	Set X-ring topology changed event type	switch(config)#event ring-topology-change both
event systemlog [Link-UP|Link-Down|Both]	I	Set port event for system log	switch(config)#interface fastethernet 3 switch(config-if)#event systemlog both
event smtp [Link-UP|Link-Down|Both]	I	Set port event for SMTP	switch(config)#interface fastethernet 3 switch(config-if)#event smtp both
show event	P	Show event selection	switch#show event

no event device-cold-start	G	Disable cold start event type	switch(config)#no event device-cold-start
no event authentication-failure	G	Disable Authentication failure event typ	switch(config)#no event authentication-failure
no event ring-topology-change	G	Disable X-ring topology changed event type	switch(config)#no event 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

Fault Relay Alarm Commands Set

Allied Telesis Commands	Level	Description	Example
faultrelay power	G	Configure Relay Alarm for Power Failure	switch(config)#faultrelay power 1
faultrelay [enable|disable]	I	Configure Relay Alarm for Port Link Down/Broken	switch(config)#interface fastethernet 3 switch(config-if)#faultrelay enable
no faultrelay	G	Disable Fault Relay Alarm Function	switch(config)#no faultrelay

SNTP Commands Set

Allied Telesis Commands	Level	Description	Example
sntp enable	G	Enable SNTP function	switch(config)#sntp enable
sntp daylight	G	Enable daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight
sntp daylight-period [Start time] [End time]	G	Set period of daylight saving time, if SNTP function is inactive, this command can't be applied. Parameter format: [yyyymmdd-hh:mm]	switch(config)# sntp daylight-period 20060101-01:01 20060202-01:01
sntp daylight-offset [Minute]	G	Set offset of daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight-offset 3
sntp ip [IP]	G	Set SNTP server IP, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp ip 192.169.1.1
sntp timezone [Timezone]	G	Set timezone index, use "show sntp timzezone" command to get more information of index number	switch(config)#sntp timezone 22
show sntp	P	Show SNTP information	switch#show sntp
sntp sync-interval [Secs]	G	Set synchronization interval	switch(config)#sntp sync-interval 64
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

Allied Telesis 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

PoE Commands Set

Allied Telesis Commands	Level	Description	Example
poe	P	Enter POE configure mode	switch#poe
system knockoff-disabled [Enable|Disable]	P	Set PoE system Port Knockoff Disabled	switch(poe)# system knockoff-disabled disable
system ac-disconnect [Enable|Disable]	P	Set PoE system AC Disconnect	switch(poe)# system ac-disconnect disable
system capacitive-detect [Enable|Disable]	P	Set PoE system Capacitive Detection	switch(poe)# system capacitive-detect enable
port [PortNumbers] state [Enable|Disable]	P	Set PoE port State	switch(poe)# port 1 state disable
port [PortNumbers] plfc [Enable|Disable]	P	Set PoE port Power Limit from Classification	switch(poe)# port 1 plfc enable
port [PortNumbers] legacy [Enable|Disable]	P	Set PoE port Legacy	switch(poe)# port 1 legacy enable
port [PortNumbers] priority [Low|High|Critical]	P	Set PoE port Priority	switch(poe)# port 1 priority high
port [PortNumbers] powerlimit [Value]	P	Set PoE port Power Limit Value	switch(poe)# port 1 powerlimit 15300
show poe	P	Show setting of PoE function	switch#show poe