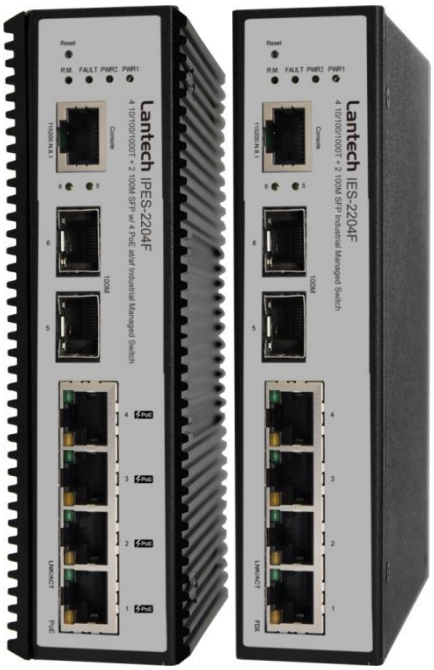
Lantech

IPES-2204F / IES-2204F



User Manual

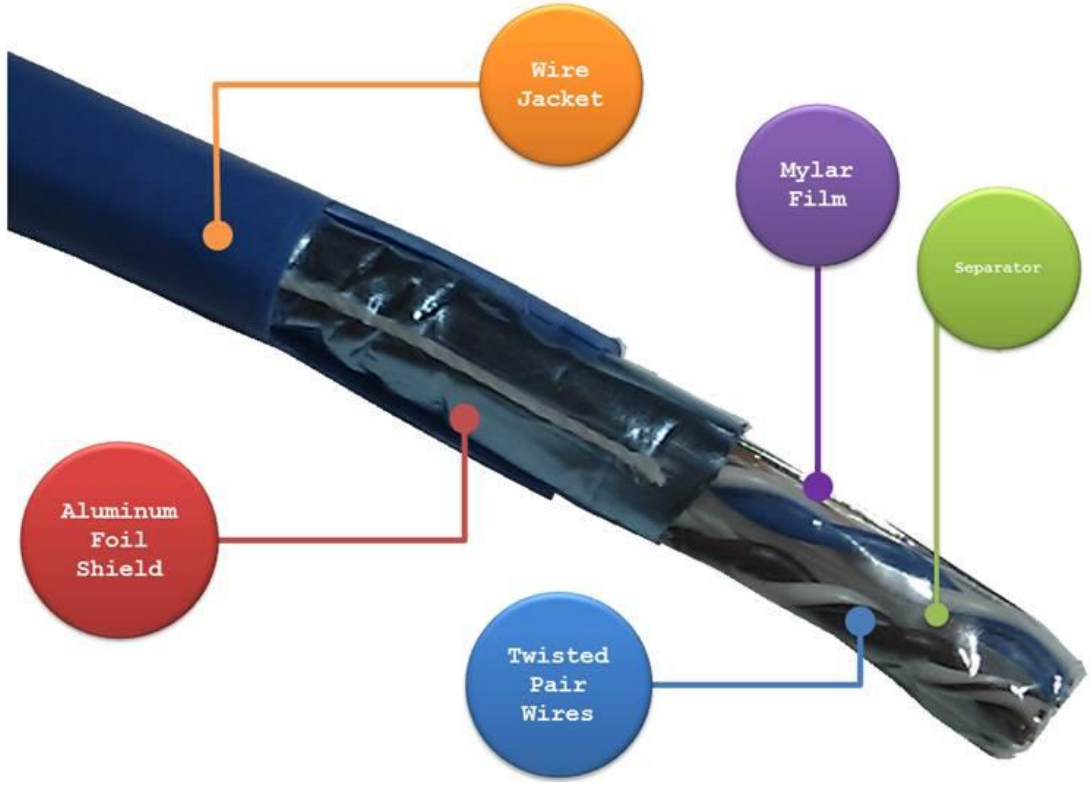
V2.2

Aug. 2017

Table of Content

Recommendation for Shielded network cables

STP cables have additional shielding material that is used to reduce external interference. The shield also reduces the emission at any point in the path of the cable. Our recommendation is to deploy an STP network cable in demanding electrical environments. Examples of demanding indoor environments are where the network cable is located in parallel with electrical mains supply cables or where large inductive loads such as motors or contactors are in close vicinity to the camera or its cable. It is also mandatory to use an STP cable where the power device (like IP camera) is used outdoors or where the network cable is routed outdoors.



FCC Warning

This Equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. It may cause harmful interference to radio communications if the equipment is not installed and used in accordance with the instructions. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CE Mark Warning

This is a Class-A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Chapter 1 Introduction

The Lantech IPES-2204Fand IES-2204F are Smart Redundant Ring Ethernet switches with 4 10/100TX + 2 100M SFP ports Industrial Switch. The IPES-2204F built in 4-port PoE injectors, feeding up to 30W per port.

IPES-2204F-48V	4 10/100TX PoE at/af + 2 100M SFP, 45~56VDC, -20~60°C
IPES-2204F-48V-E	4 10/100TX PoE at/af + 2 100M SFP, 45~56VDC, -40~75°C
IPES-2204F-12V	4 10/100TX PoE at/af + 2 100M SFP, 9.5~56VDC, -20~60°C
IPES-2204F-12V-E	4 10/100TX PoE at/af + 2 100M SFP, 9.5~56VDC, -40~75°C
IES-2204F	4 10/100TX + 2 100M SFP, 9.5~60VDC, -40~75°C

Management	SNMP v1 v2c, v3/ Web/Telnet
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
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.
Pro-Ring2s	Supports Pro-Ring2s. 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

IP Security	Supports 10 IP addresses that have permission to access the switch management and to prevent unauthorized intruder.
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. Topology Change 2. Power Trap
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 configuration file for system quick installation

ifAlias	Each port allows importing 128bits of alphabetic string of word on SNMP interface

1.1 Package Contents

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

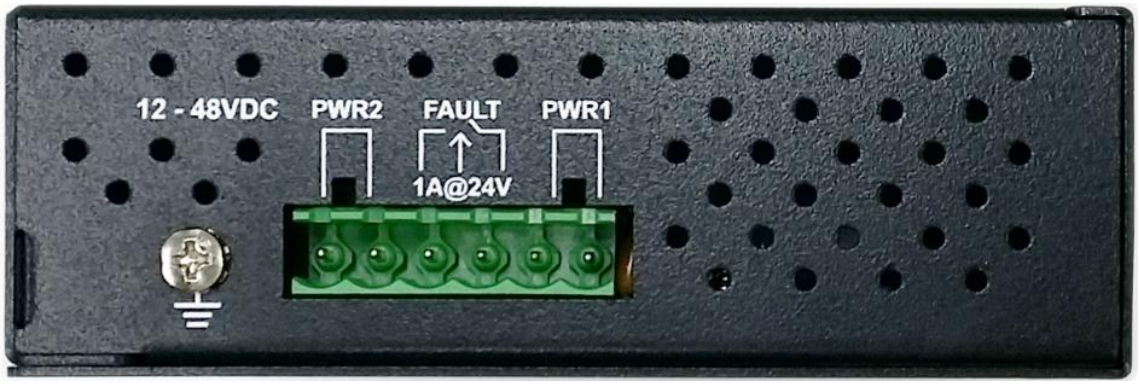
- Managed Industrial Switch x 1
- User manual x 1
- Pluggable Terminal Block x 1
- RJ-45 to DB9-Female cable x 1

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

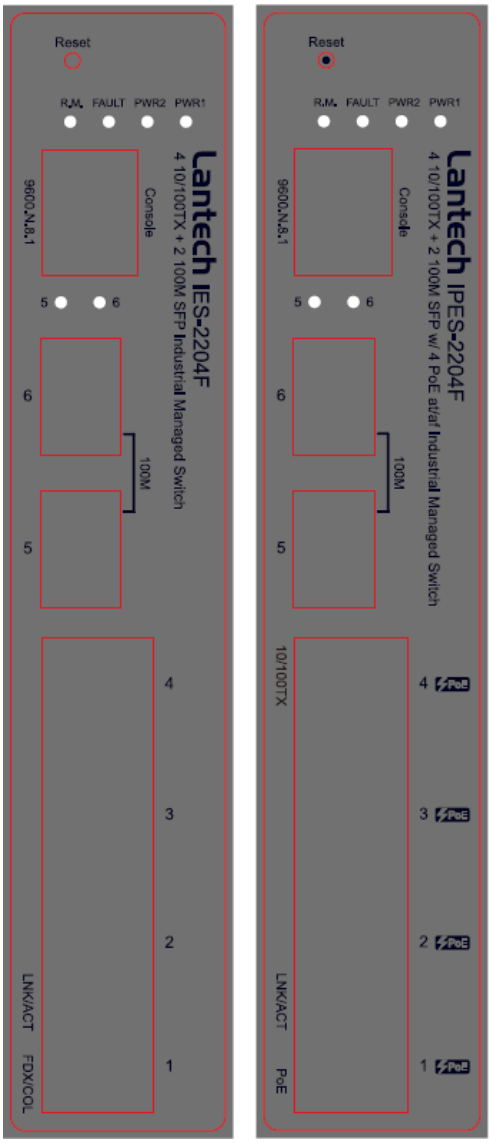
2.1 Bottom View

The bottom panel of the Industrial Managed Industrial Switch has one terminal block connector of two DC power inputs and one fault alarm.



Bottom Panel of the industrial switch

2.2 LED Indicators



Front Panel of IES-2204F and IPES-2204F

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 Pro-Ring2s group

		Off	The industrial switch is not a ring master in Pro-Ring2s 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
P5, P6 (SFP)	Green	On	A network device is detected.
		Blinking	The port is transmitting or receiving packets from the TX device.
		Off	No device attached
P1 ~ P4	Green	On	A network device is detected.
		Blinking	The port is transmitting or receiving packets from the TX device.
		Off	No device attached
	Amber (IES-2204F)	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.
	Amber (IPES-2204F)	On	The port is operating in PoE mode.
		Off	The port is not operating in PoE mode.

Chapter 3 Hardware Installation

In this paragraph, we will describe how to install the Pro-Ring2s Managed Industrial Switch and the installation points attended to it.

3.1 Installation Steps

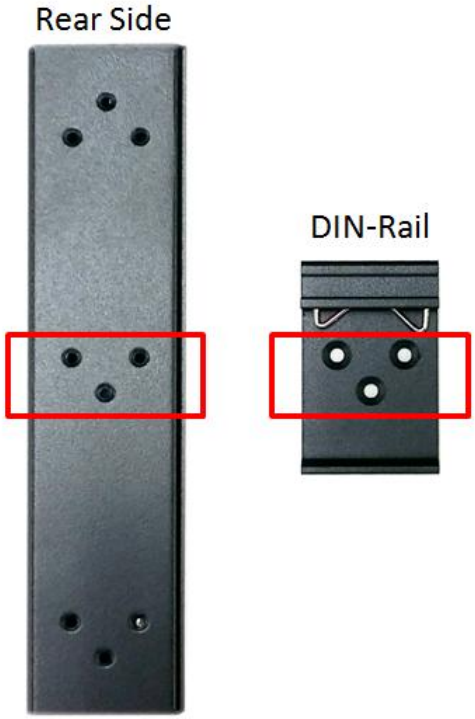
1. Unpack the Industrial switch
2. Check if the DIN-Rail is screwed on the Industrial switch or not. If the DIN-Rail is not screwed on the Industrial switch, please refer to **DIN-Rail Mounting** section for DIN-Rail installation. If users want to wall mount the Industrial switch, please refer to **Wall 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. Insert 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.

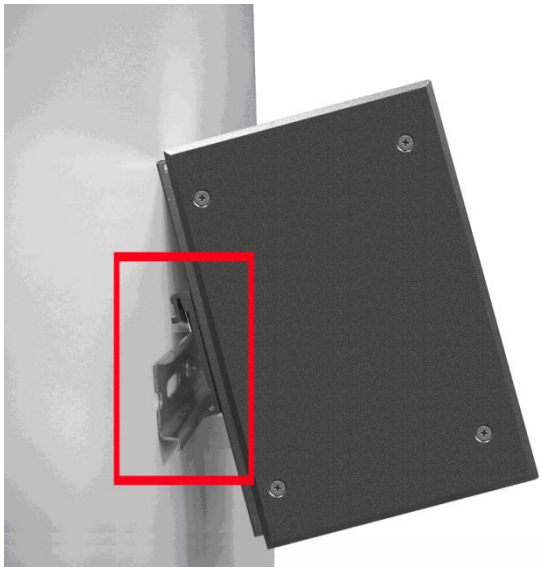
7. When all connections are set and LED lights all show in normal, the installation is complete.

3.2 DIN-Rail Mounting

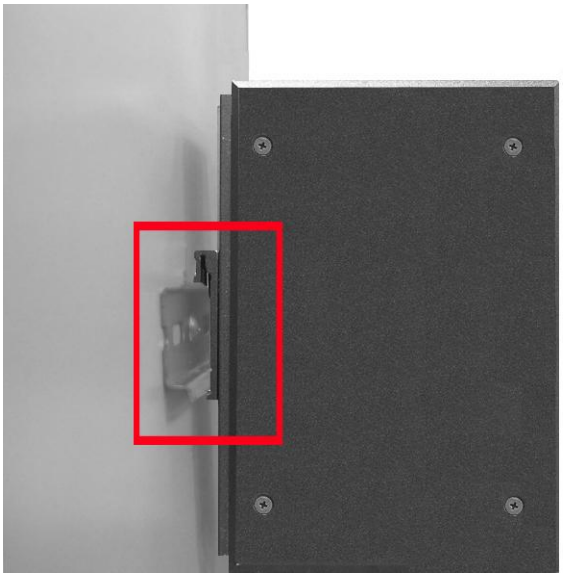
The DIN-Rail is screwed on the industrial switch when out of factory. If the DIN-Rail is not screwed on the industrial switch, please see the following pictures to screw the DIN-Rail on the switch. Follow the steps below to hang the industrial switch.



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



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

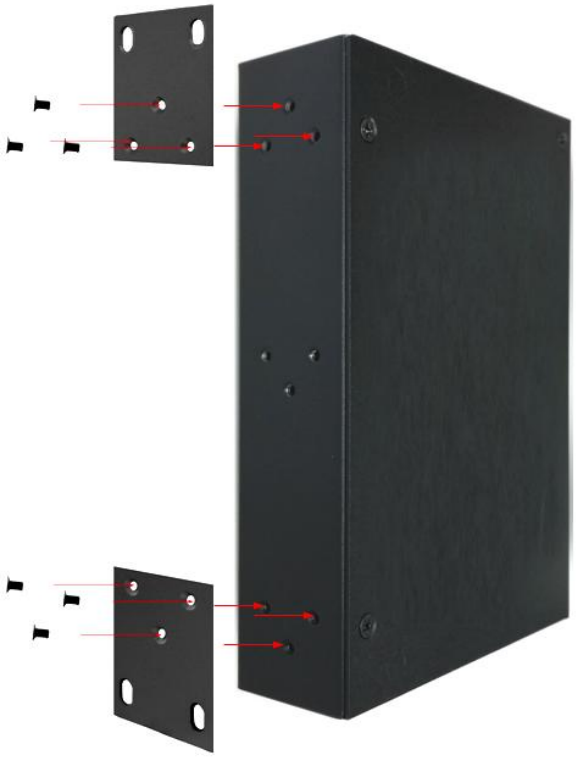


3. Check if the DIN-Rail is tightened on the track or not.
4. To remove the industrial switch from the track, reverse above steps.

3.3 Wall Mount Plate Mounting

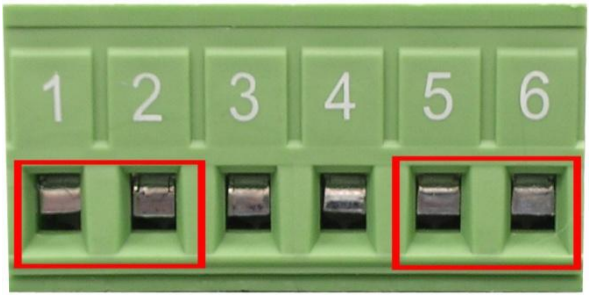
Follow the steps below to mount the industrial switch with wall mount plate.

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.

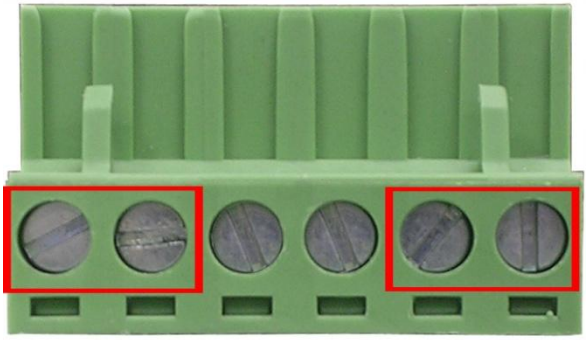


3.4 Wiring the Power Inputs

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.



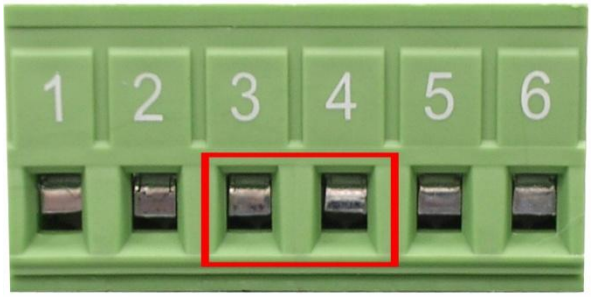
2. Tighten the wire-clamp screws for preventing the wires from loosing.

IPES-2204F-48V	45~56VDC
IPES-2204F-48V-E	45~56VDC
IPES-2204F-12V	9.5~56VDC
IPES-2204F-12V-E	9.5~56VDC
IES-2204F	9.5~60VDC

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

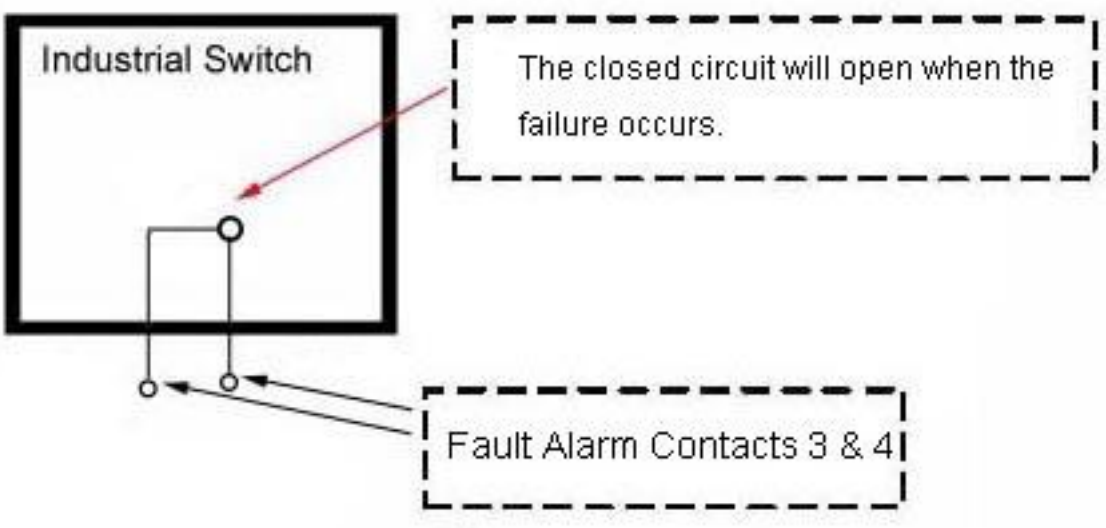
3.5 Wiring the Fault Alarm Contact

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.



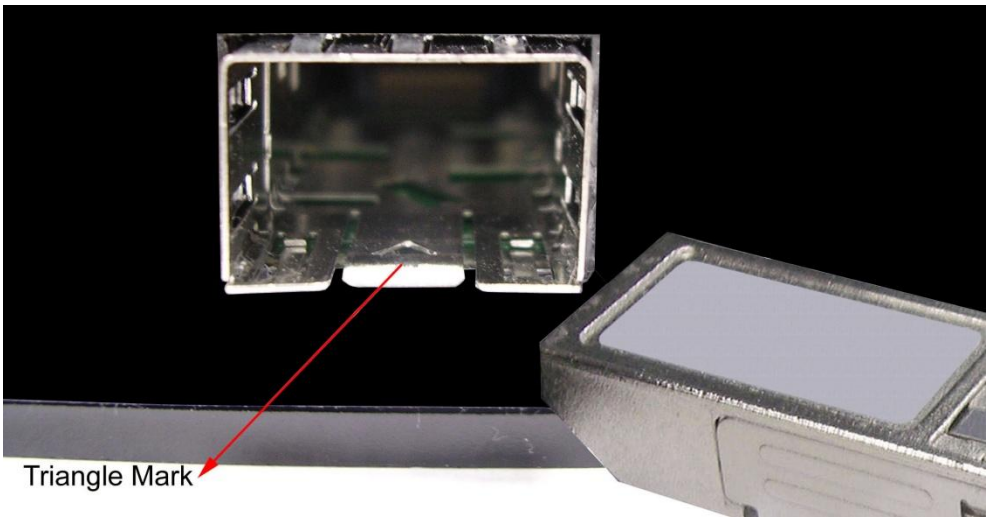
3.6 Cabling

- 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:**

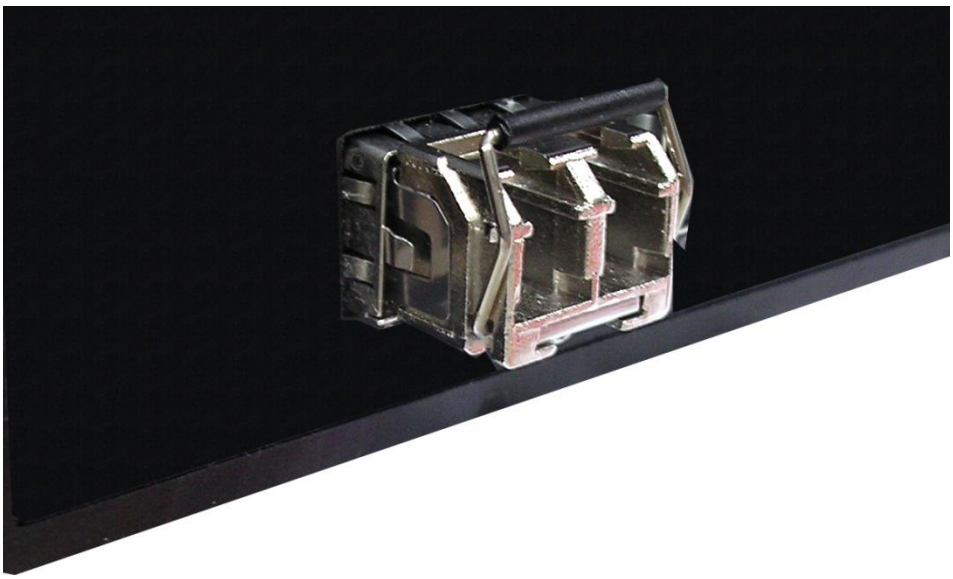
The Industrial switch has the auto-detected Giga port—Gigabit Copper/SFP combo ports. The Gigabit Copper (10/100/1000T) ports should use Category 5e or above UTP/STP cable for the connection up to 1000Mbps. The small form-factor pluggable (SFP) is a compact optical transceiver used in optical communications 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.

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.

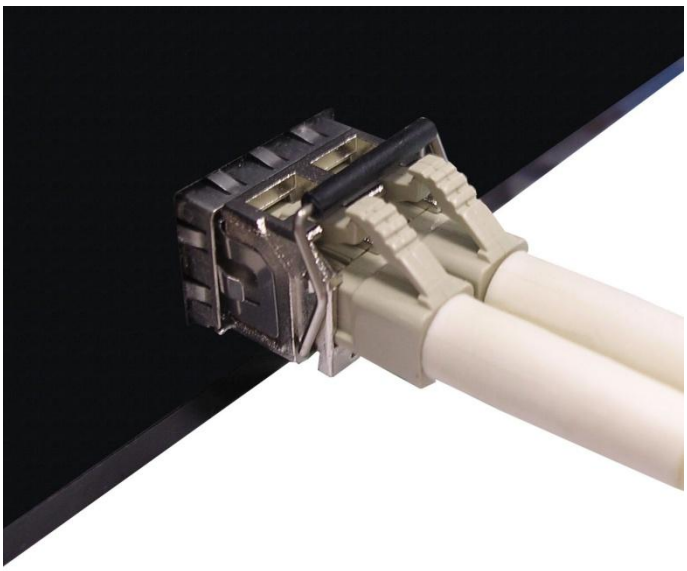


Transceiver to the SFP module



Transceiver Inserted

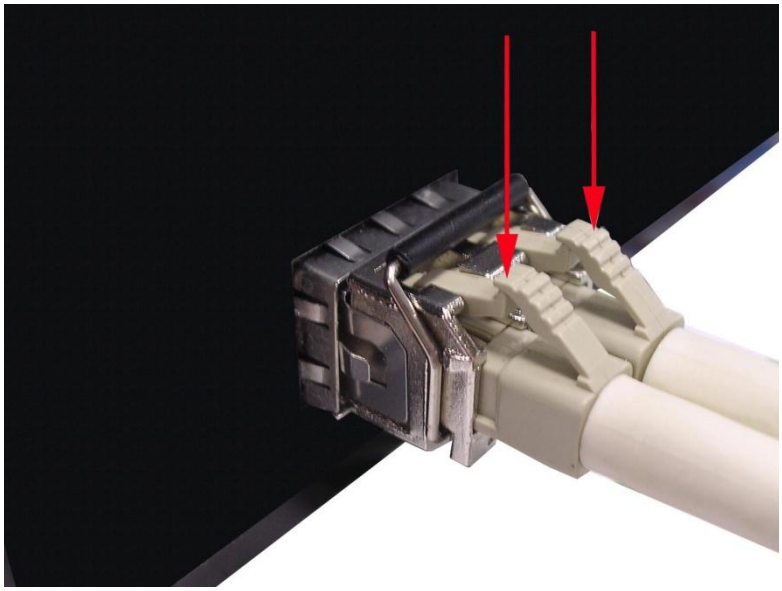
Second, insert the fiber cable of LC connector into the transceiver.



LC connector to the transceiver

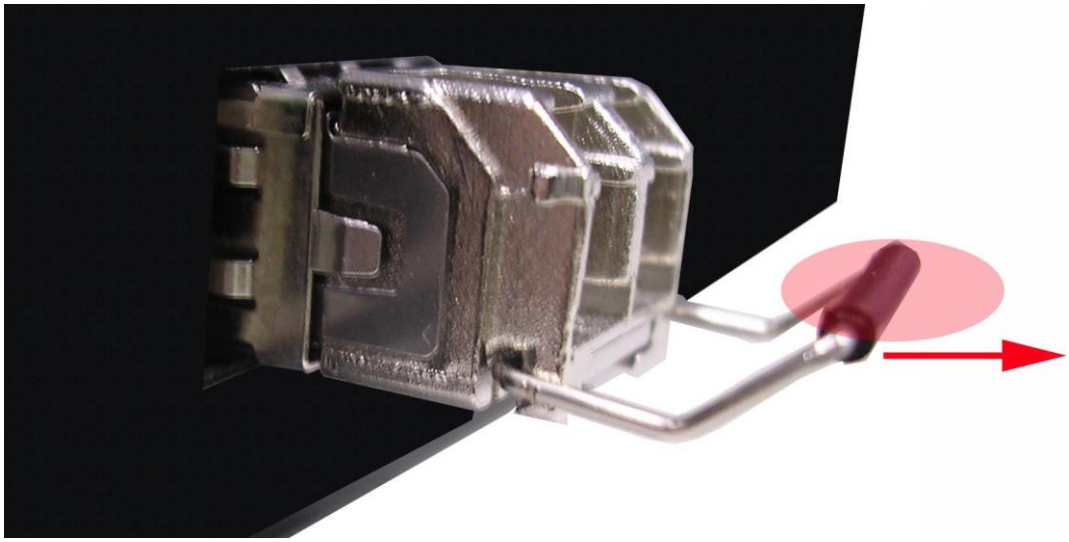
To remove the LC connector from the transceiver, please follow the steps shown below:

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.

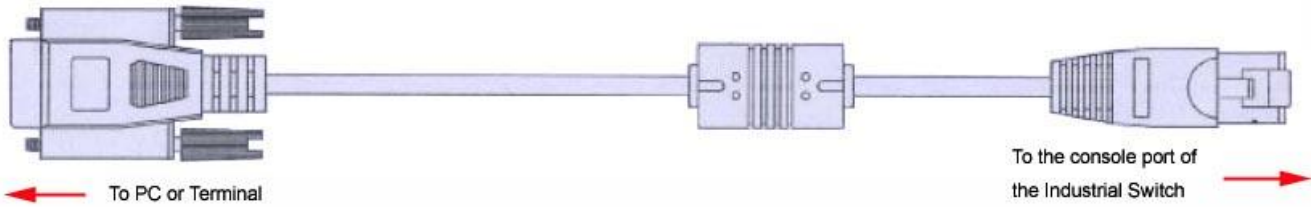


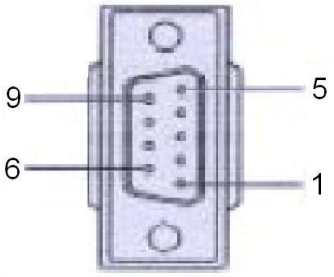
Pull out from the transceiver

Chapter 4 Console Management

4.1 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

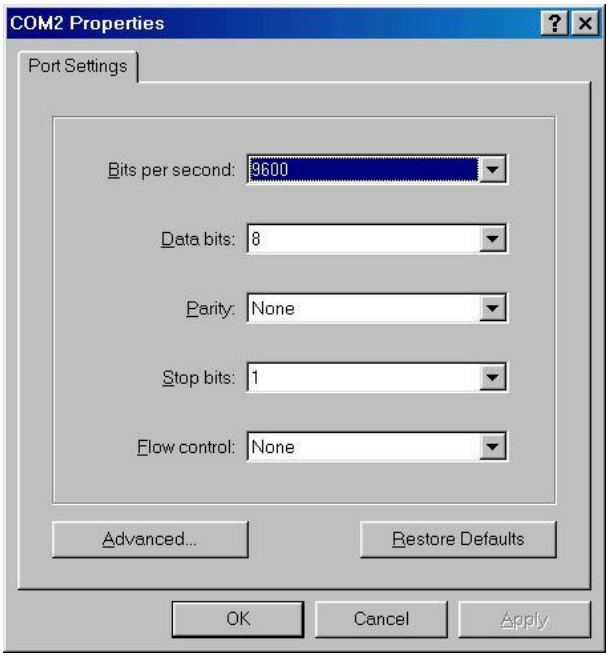
4.2 Pin Assignment

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

4.3 Login in the Console Interface

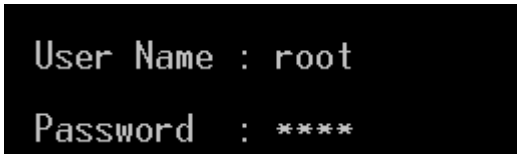
When the connection between Switch and PC is ready, turn on the PC and run a terminal emulation program or **Hyper Terminal** and configure its **communication parameters** to match the following default characteristics of the console port:

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



The settings of communication parameters

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



Console login interface

4.4 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

Chapter 5 Web-Based Management

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

5.1 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.

5.2 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: **192.168.16.1**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.168.16.254**
- User Name: **root**
- Password: **root**

5.3 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

5.4 System

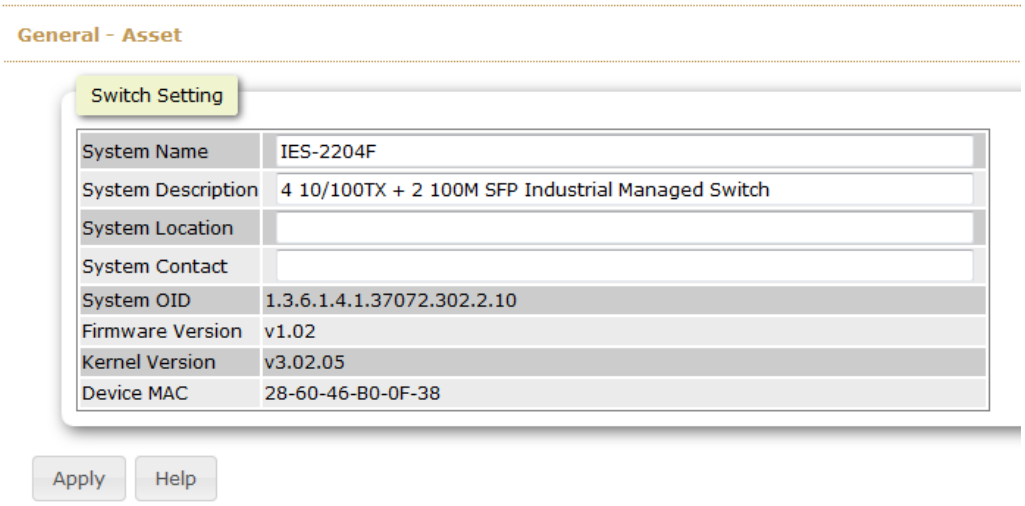
6.4.1 General – Switch Information

User can find 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.
- **System OID:** SNMP OID of switch
- **Firmware Version:** Displays the switch's firmware version
- **Kernel Version:** Displays the kernel software version
- **Device MAC :** Displays the unique hardware address assigned by manufacturer

6.4.2 General – Asset

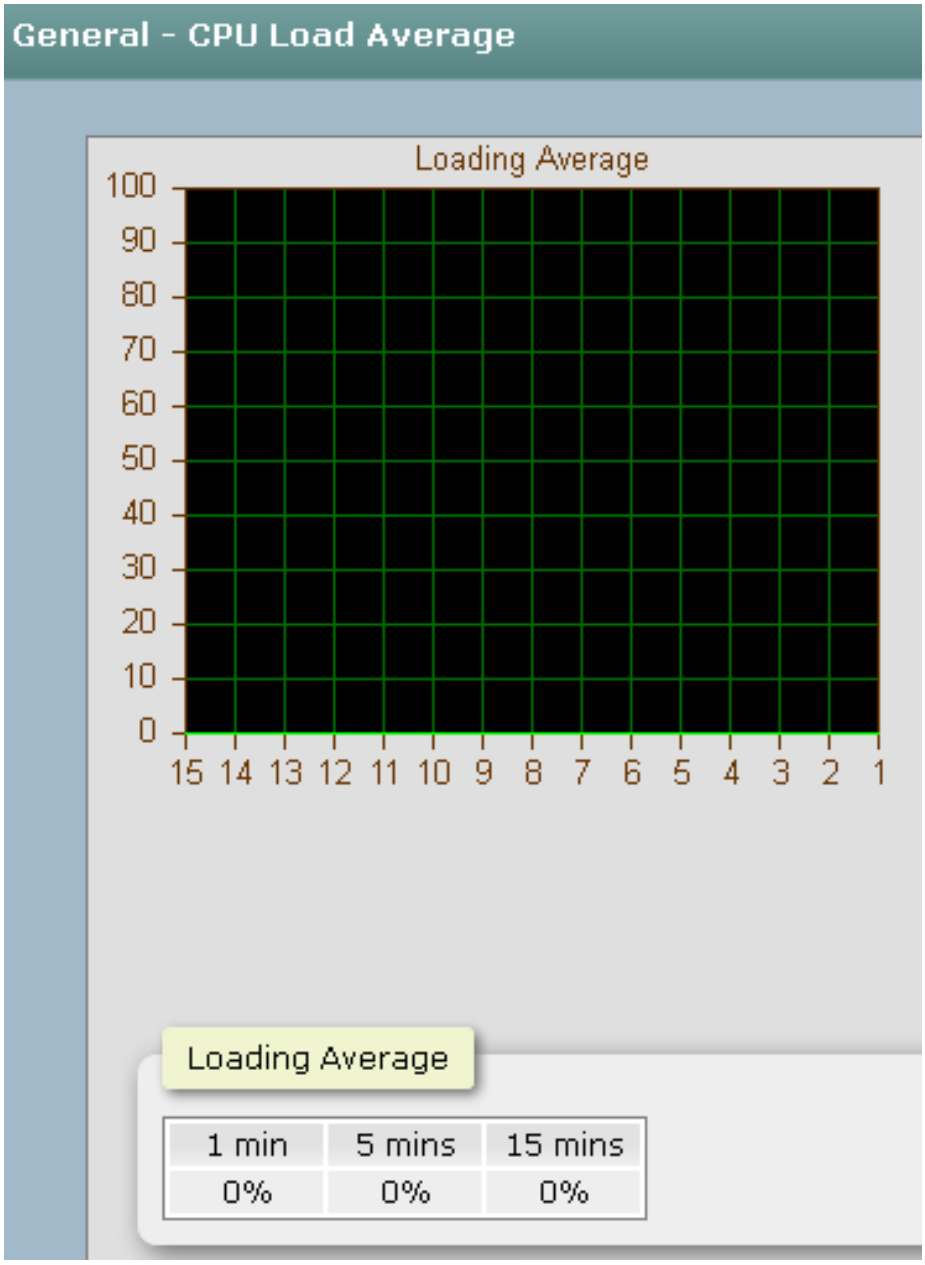
You can modify these information about System name 、System Description、System Location and System Contact in here.



Switch settings interface

6.4.2 General – CPU Load Average

Sometimes the user was worry about that ‘ Could my switch process too many network packets ? So the network throughput was keeping decreasing “. In this option, you can monitor the CPU of switch to see if the switch was in full loading status or not.



5.5 Time - SNTP

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.
- **UTC Timezone:** Universal Time, Coordinated. Set the switch location time zone. The following table lists the different location time zone for your reference.

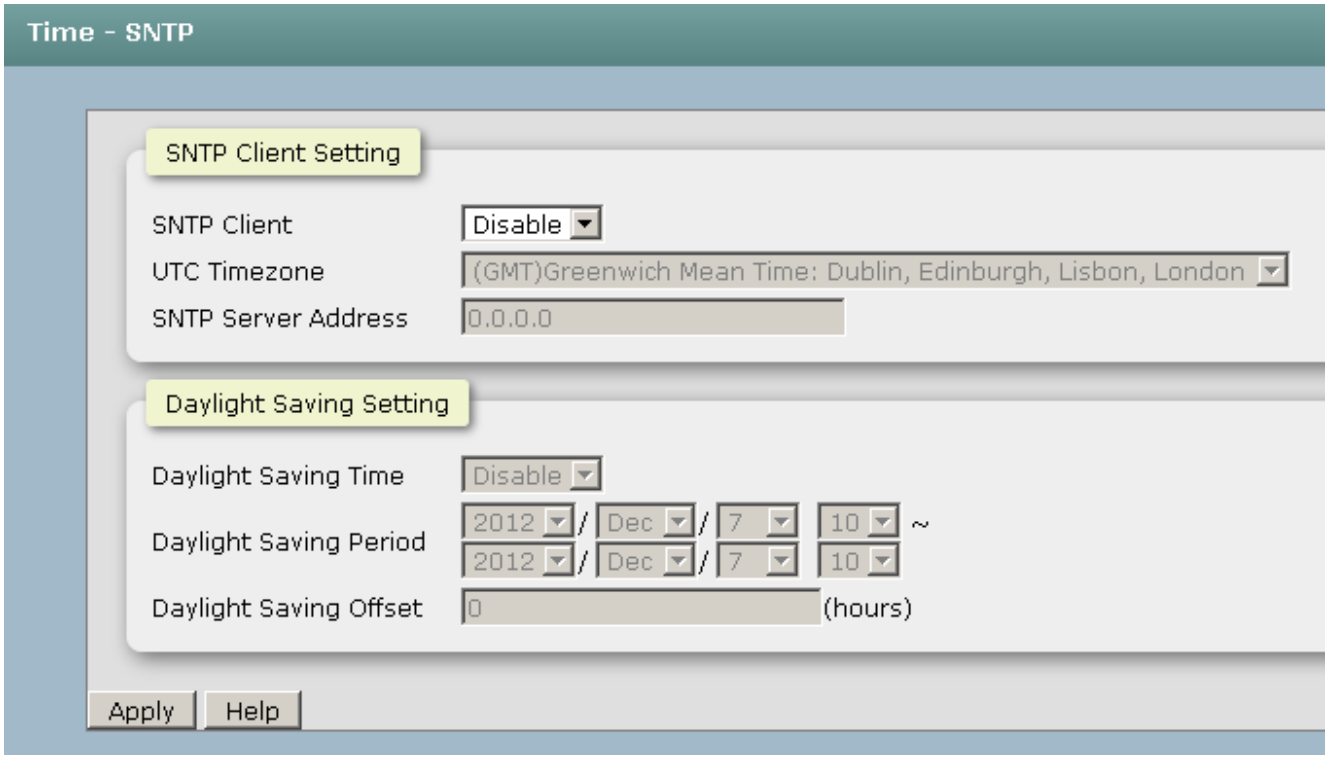
Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT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

PDT - Pacific Daylight		
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	+10 hours	10 pm

Guam Standard, USSR Zone 9		
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

- **SNTP Sever Address:** Set the SNTP server IP address. You can assign a local network time server IP address or an internet time server IP address.
- **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.
- **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 :** 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.

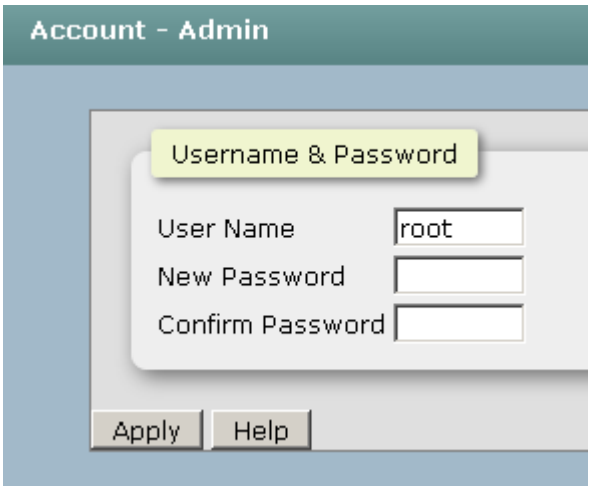


SNTP Configuration interface

5.6 Account - Admin

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’)
- **New Password:** Type in the new password (The default is ‘root’)
- **Confirm password:** Re-type the new password
- And then, click Apply



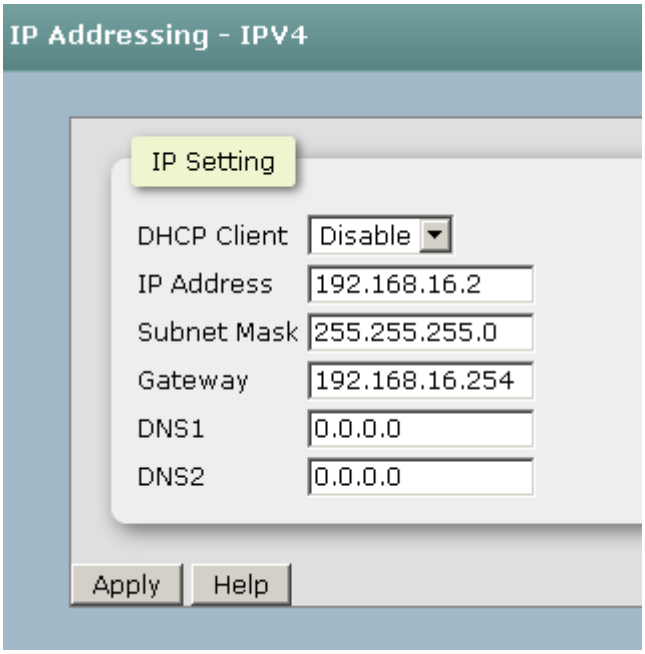
Account Authentication interface

5.7 IP Addressing – IPV4

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 

.

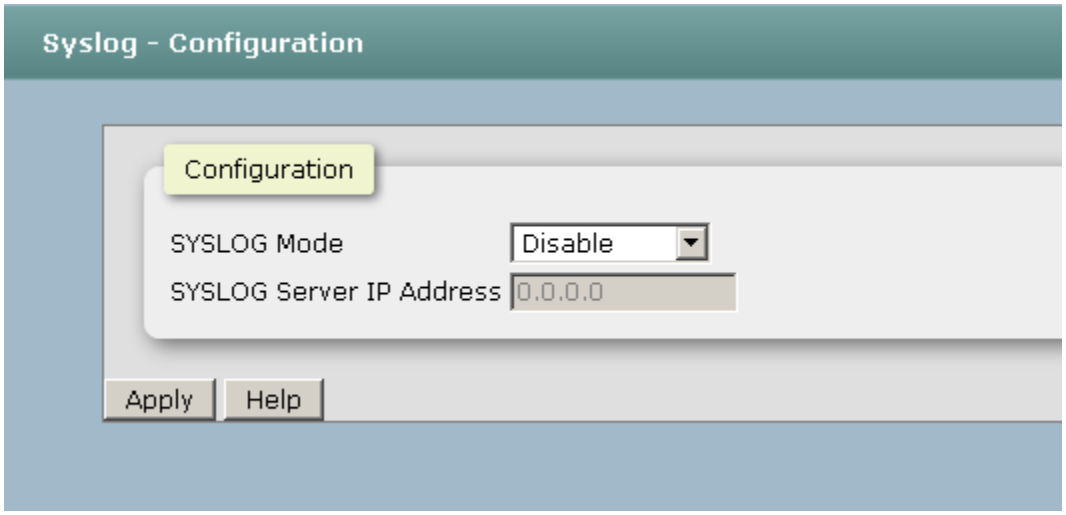


IP Addressing interface

5.8 Syslog

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

Syslog Configuration



Syslog Configuration interface

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

5.9 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.

SNMP - Agent

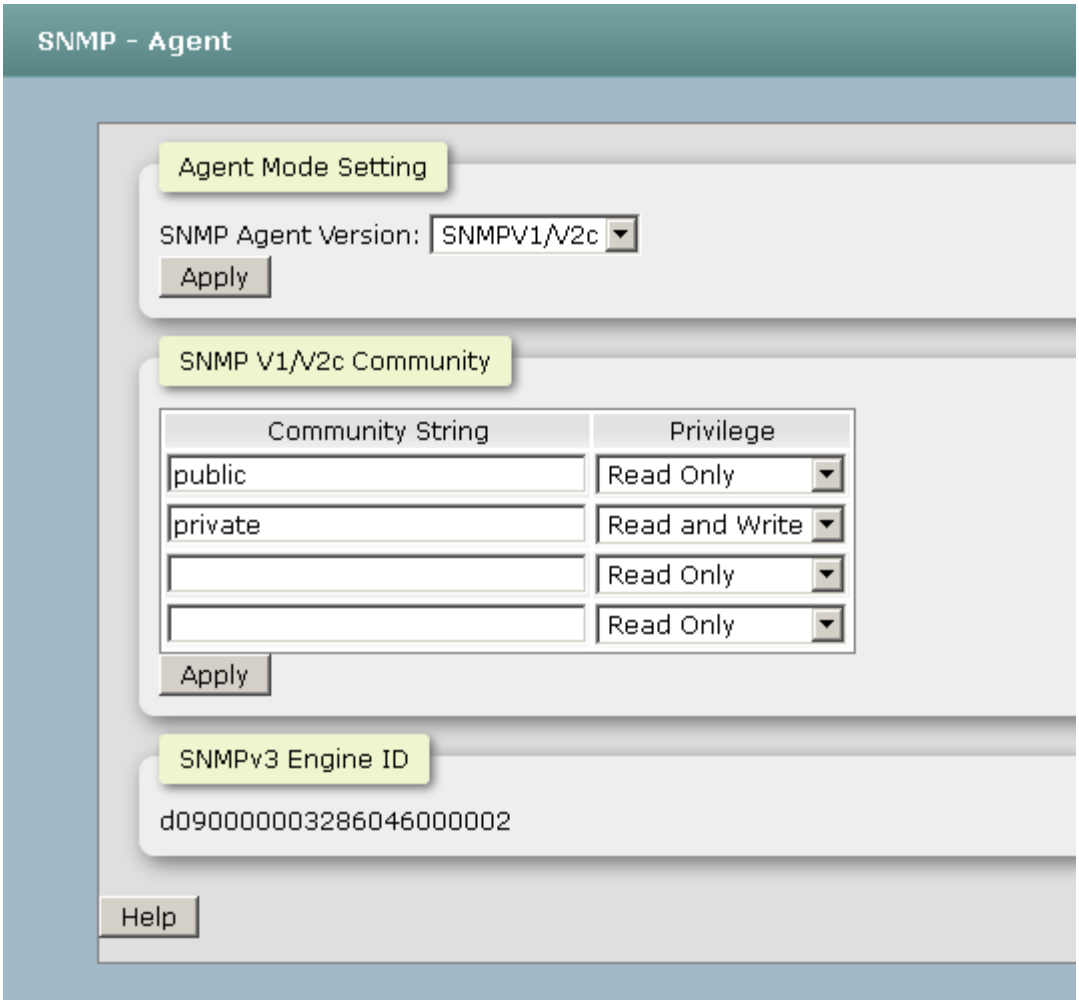
- **Agent Mode:** Select the SNMP version(V1/V2c or V3) that you want to use it. And then click Change to switch to the selected SNMP version mode.

- **SNMP V1V2c Community**

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

- **Community String:** Fill the name string.
- **Privilege:** Read only. Enables requests accompanied by this community string to display MIB-object information.

  Read/write. Enables requests accompanied by this community string to display MIB-object information and to set MIB objects.
- Click. Apply

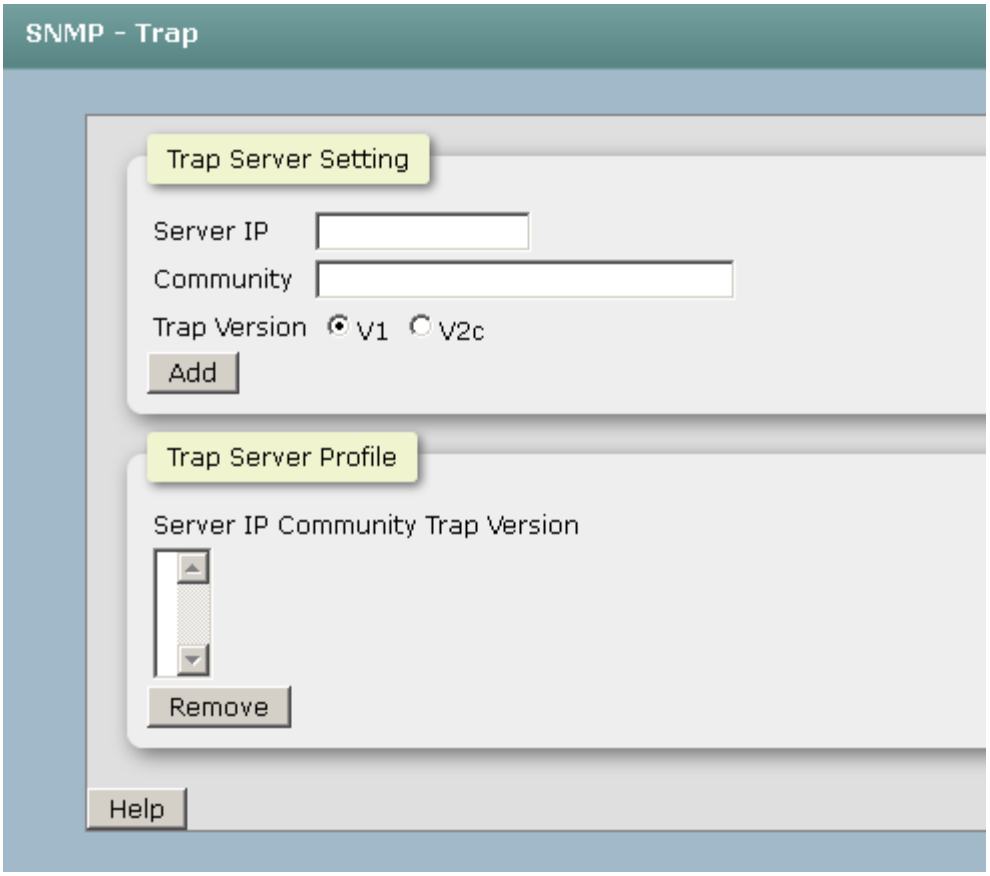


SNMP Agent Configuration interface

6.20.1 SNMP 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.

- **Server IP :** 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.

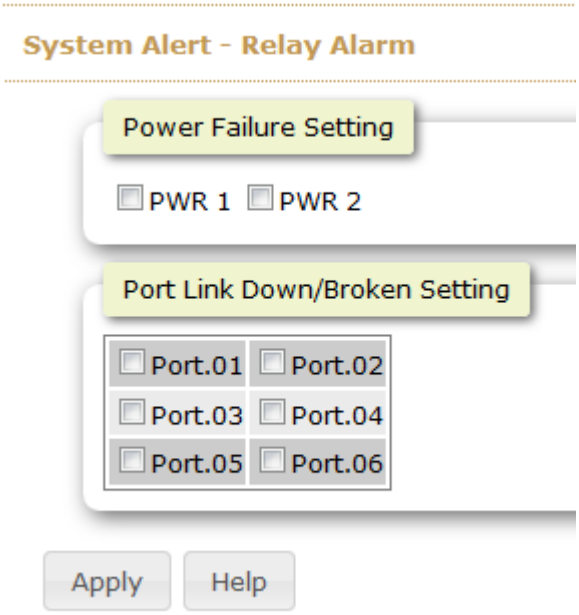


Trap Managers interface

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



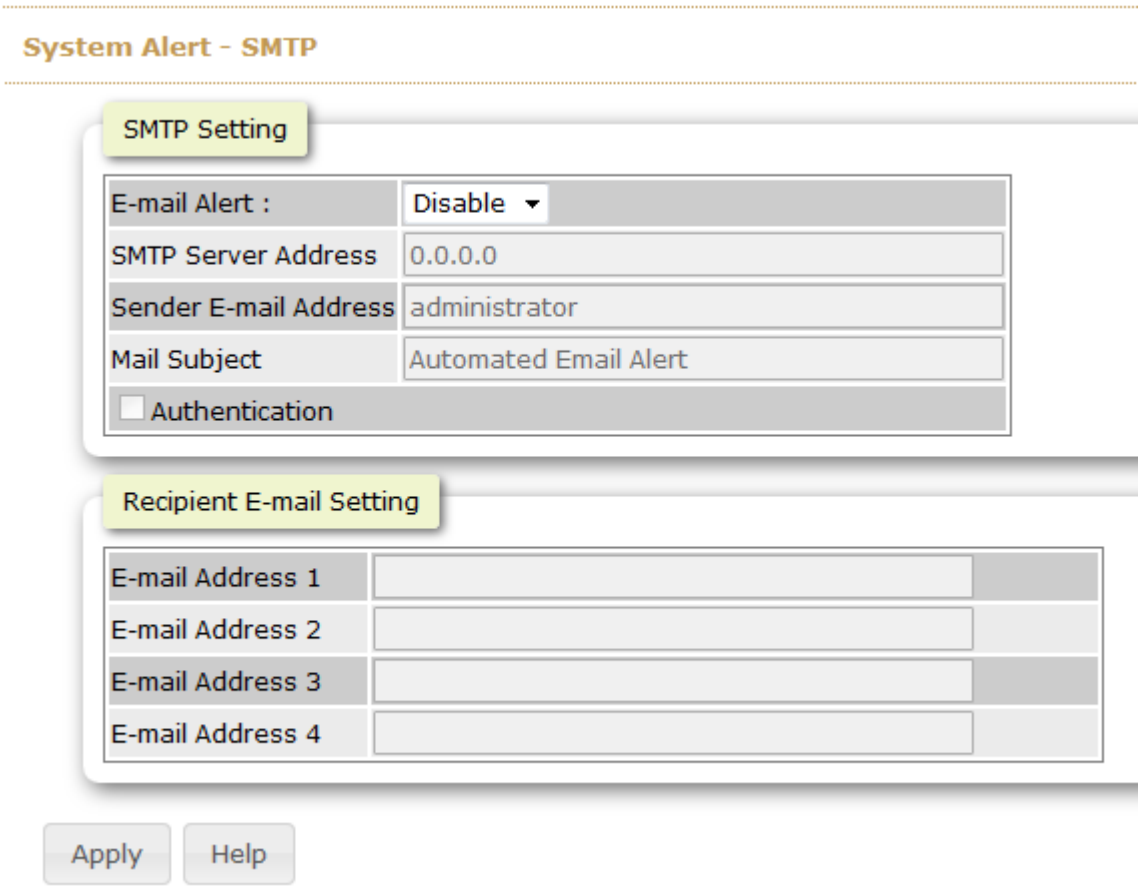
Fault Relay Alarm interface

6.8.1 System Alert - SMTP

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, 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 Email Address:** 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.
- **Mail Subject:** Input the subject of Email.
- **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.

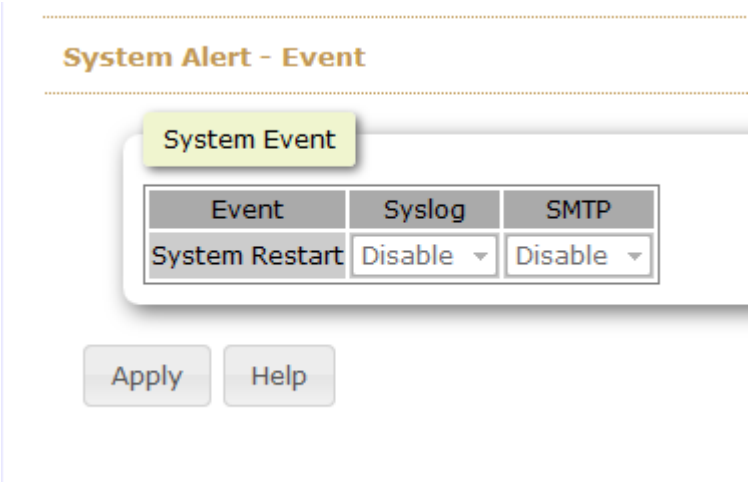


6.8.2 System Alert - Event

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 3 event types—Device Cold 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.
  - **System Restart:** When the device executes cold start action, the system will issue the event log/email alert to the system log/SMTP server respectively.

.

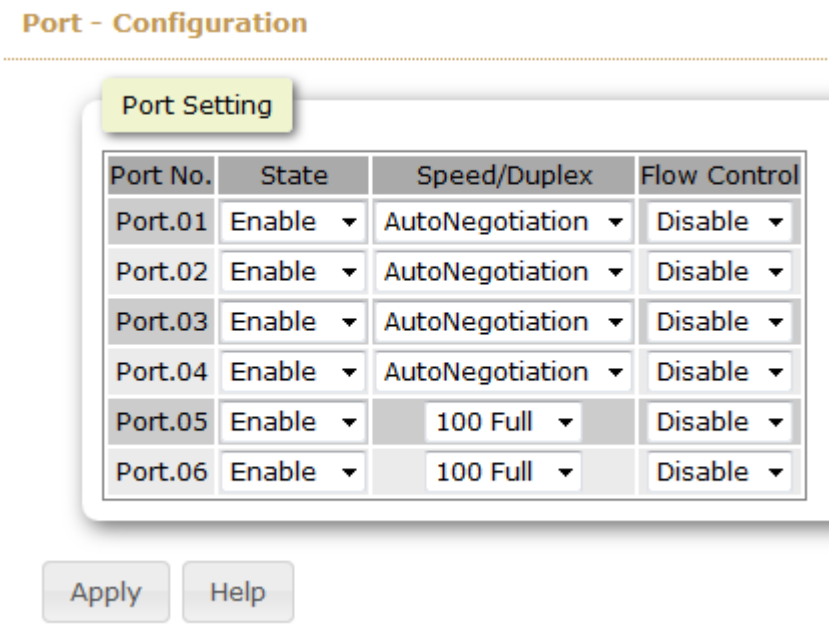


Event Configuration interface

5.11 Port - Configuration

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 No.:** The port number which you want 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..
- **Speed/Diplex:** It can be set as auto or set speed and negotiated way manually.
- **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.
- **Alies:** Add description of each port to let the manager know the connected device of each port, it will be showed by NMS utility.
- Click Apply to have the configuration take effect.



Port Control interface

5.12 Port Status

It will show you the status of port configuration setting .

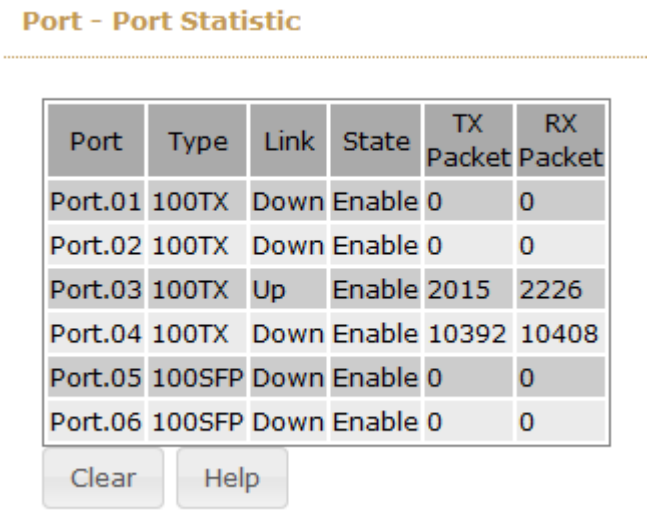
Port - Status

Port No.	Type	Link	State	Speed/Duplex	Flow Control
Port.01	100TX	Down	Enable	N/A	N/A
Port.02	100TX	Down	Enable	N/A	N/A
Port.03	100TX	UP	Enable	100 Full	Disable
Port.04	100TX	Down	Enable	N/A	N/A
Port.05	100SFP	Down	Enable	N/A	N/A
Port.06	100SFP	Down	Enable	N/A	N/A

5.13 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 Packet:** The counts of transmitting good packets via this port.
- **Rx Packet:** The counts of receiving good packets via this port.
- Click Clear button to clean all counts.



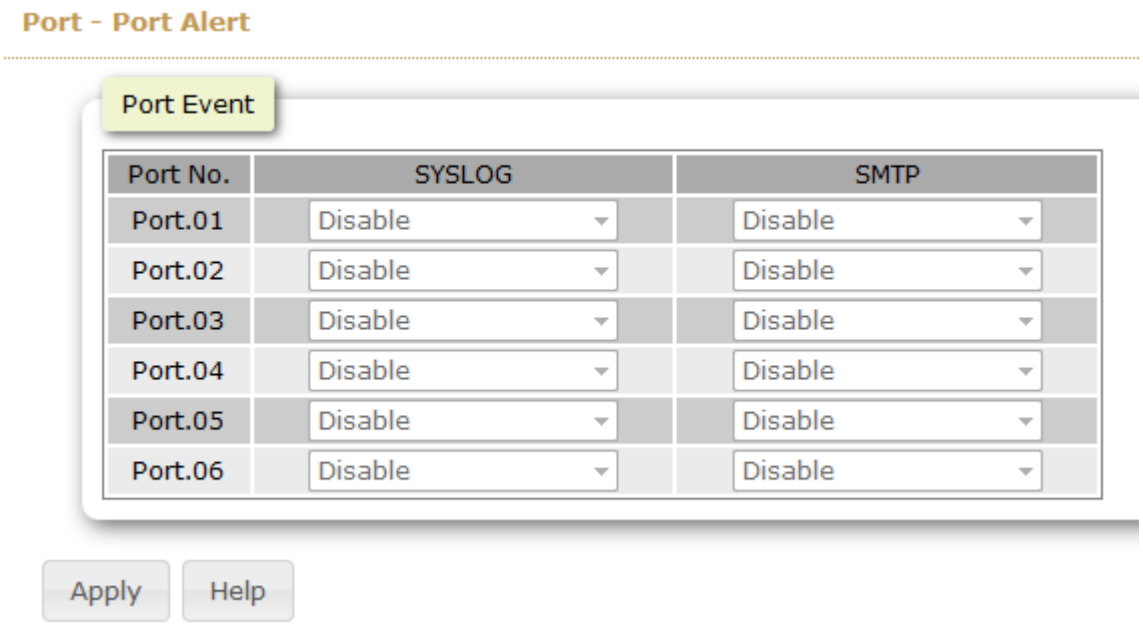
Port Statistics interfac

5.14 Port – Port Alert

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 3 event types—Device Cold 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.
  - **Authentication Failure:** When the SNMP authentication fails, the system will issue the event log/email alert to the system log/SMTP server respectively.
  - **MAC Violation:** When the MAC address has violated, 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.

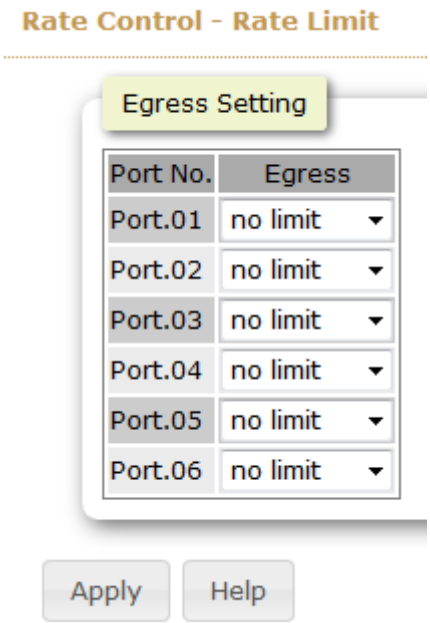


5.15 Rate Control –Rate Limit

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

All the ports support port 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

- And then, click Apply to apply the settings

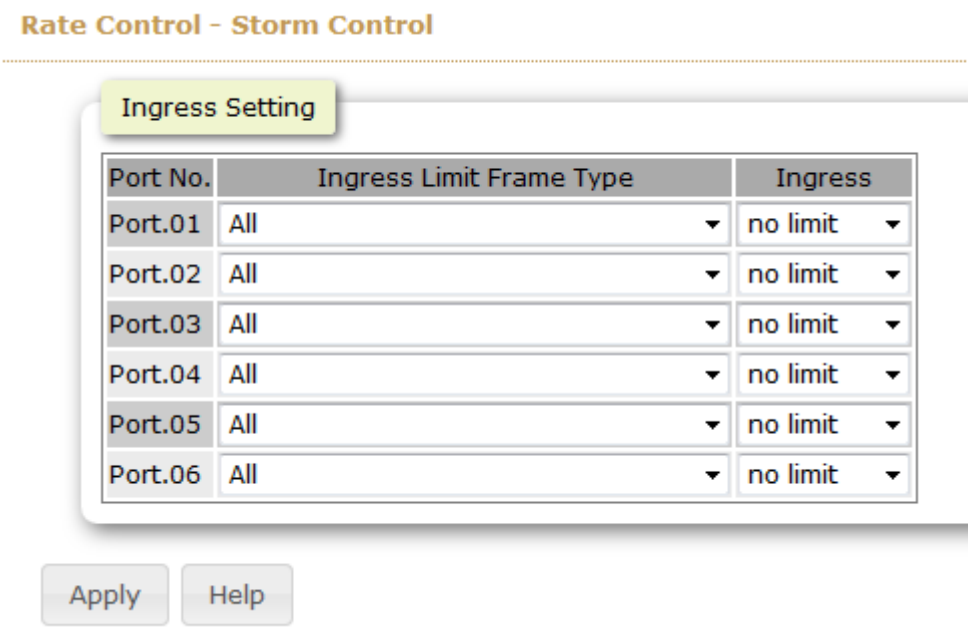


- **Storm Control:** select the frame type that wants to filter. There are four frame types for selecting:

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

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

■ And then, click Apply to apply the settings



5.16 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.

6.18.1 RSTP Setting

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.

- **RSTP mode:** The user must enable the RSTP function first before configuring the related parameters.
- **Priority :** 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 :** 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 :** 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 :** 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.

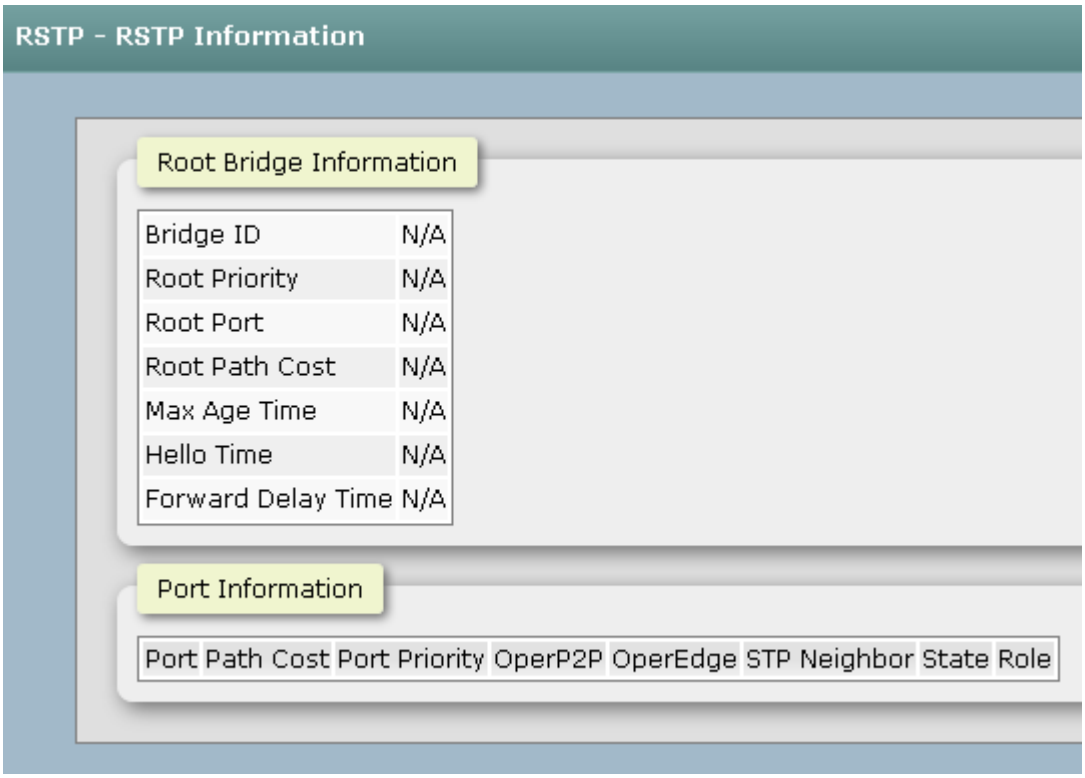
- **Enable:** Select the port which you want to be enabled with RSTP.
- **Path Cost:** The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200,000,000.
- **Priority:** Decide which port should be blocked by setting its priority as the lowest. Enter a number between 0 and 240. The value of priority must be the multiple of 16.
- **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.

- **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.
- Click Apply.

6.18.2 RSTP Information

This web page provides the port and switch information about RSTP.

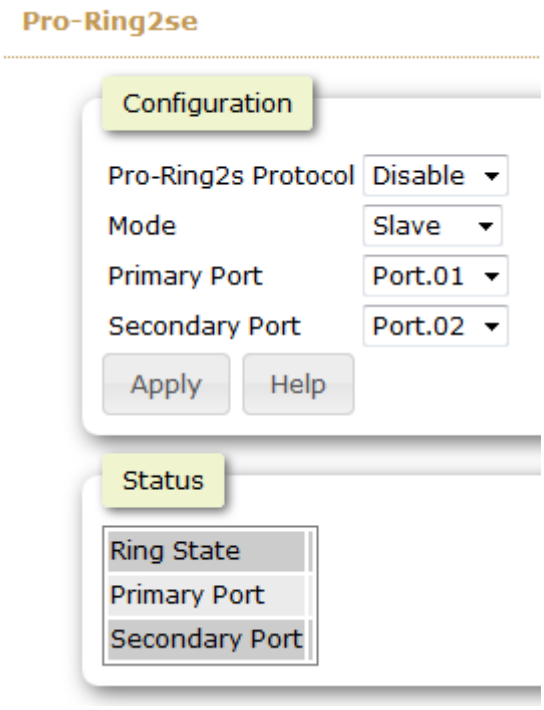


RSTP System Configuration interface

5.17 Pro-Ring II SE

Pro-Ring IIs is a new Ring mechanism for Lantech Industrial Switches in which it protects the network by flexible topology than ever. Pro-Ring IIs works as a Single Ring and Multiple Ring to recover the broken ring in less than 20 ms for up to 50 switch nodes..

- **Root Switch:** To enable the Pro-RingIISE function, first you must set your switch as Enable or Backup, “Enable” means this switch will play the role of root switch, “Backup” means this switch will take over the role of root switch when the original root switch fail.
- **Port setting:** set the port which you want to build the Ring topology. usually set as G1 and G2. With some advance redundancy solution like Couple ring and Dual homing, if you are confused about which port was needed to enable, just select all the port which was responsible for uplink.
- And then, click Apply to have the configuration take effect.



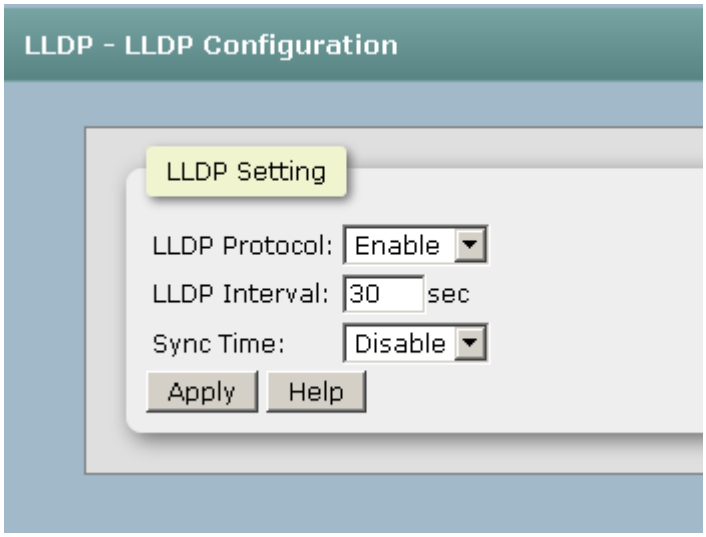
RSTP Port Configuration interface

5.18 LLDP

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.

6.21.1 LLDP Configuration

- **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
- **Sync Time**: How long will the switch Sync the LLDP information..
- Click Apply.



LLDP Interface

6.22.1 LLDP Neighbors

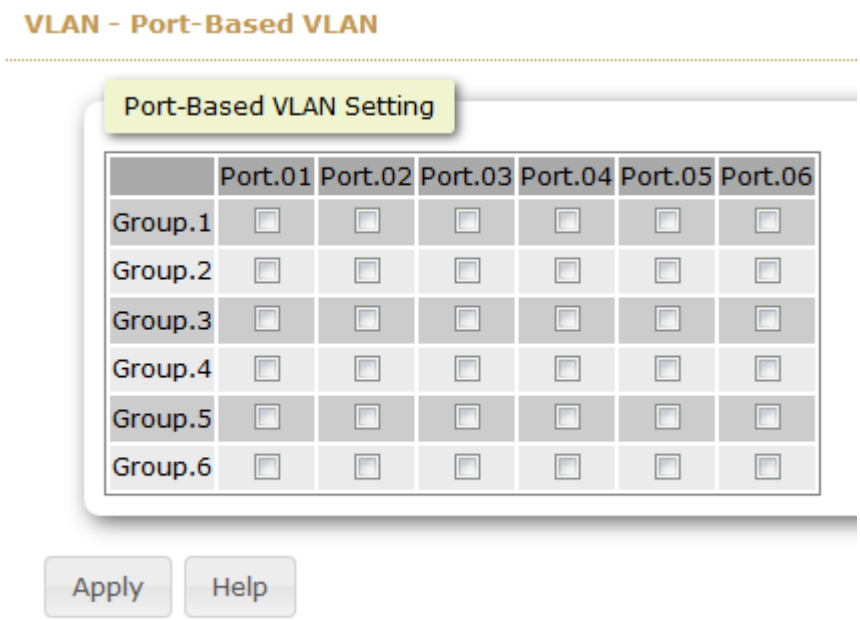
It will show you the information about Port Neighbor via LLDP protocol.

6.23 VLAN

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**".

6.24.1. VLAN Configuration



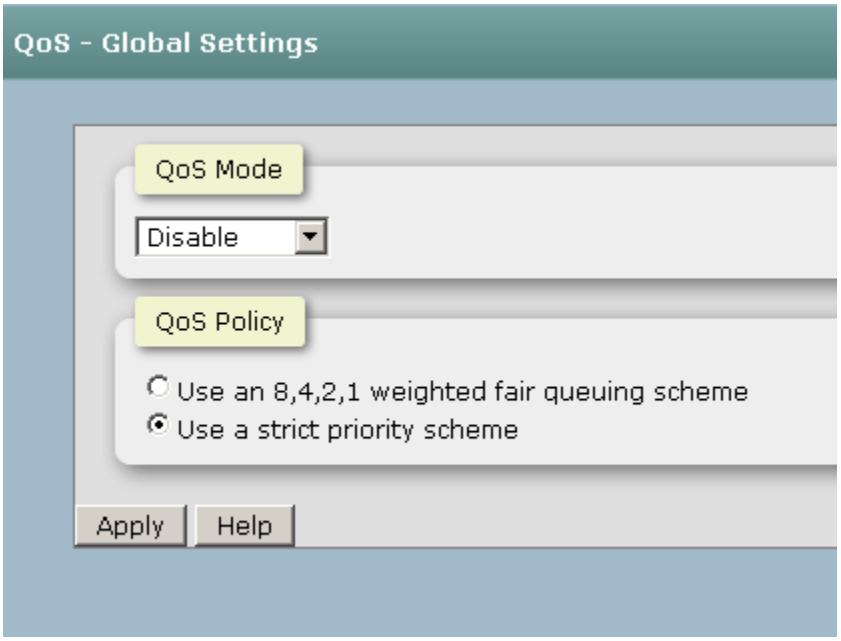
6.24 QoS

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.

6.25.1 Global Settings

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.

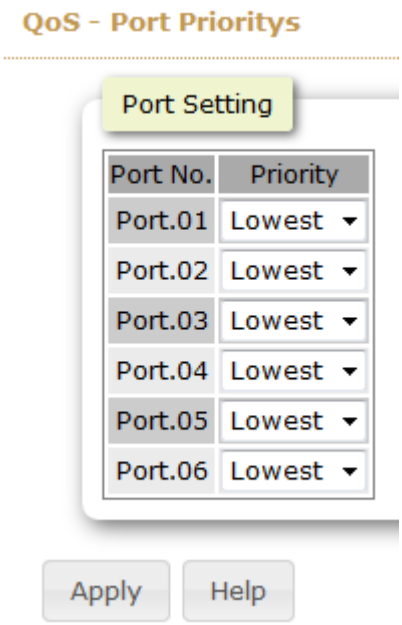
- **Qos Policy:** Select the QoS policy rule.
  - **Using the 8,4,2,1 weight fair queue scheme:** The switch will follow 8:4:2:1 rate to process priority queue from High to lowest queue. For example, while the system processing, 1 frame of the lowest queue, 2 frames of the low queue, 4 frames of the 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 Apply to have the configuration take effect.



6.25.2 Port 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.

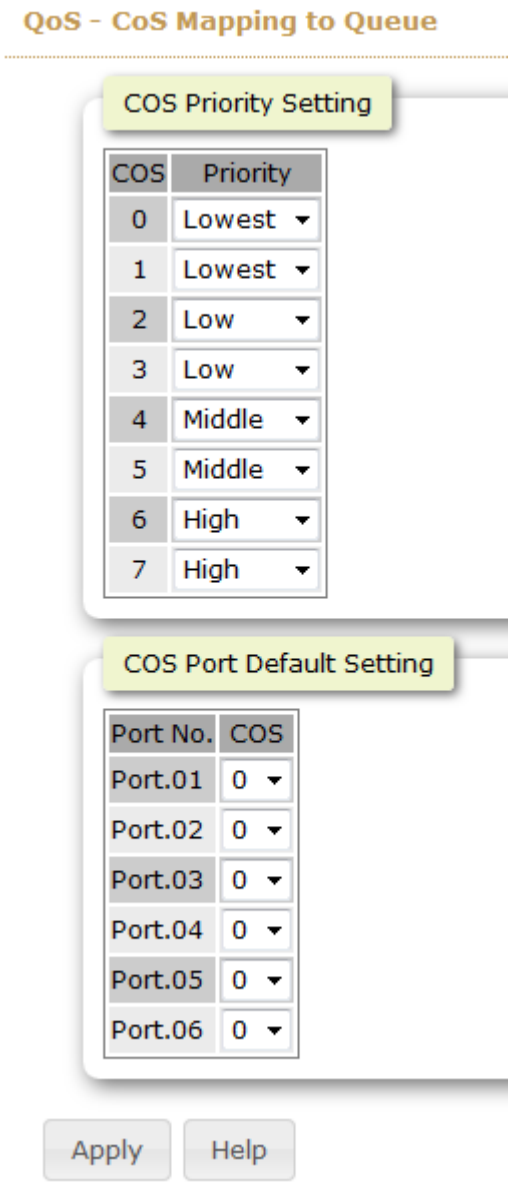
- **Port x:** Each port has 4 priority levels—High, Middle, Low, and Lowest—to be chosen.
- Click Apply to have the configuration take effect.



6.25.3 COS Mapping to Queue

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.

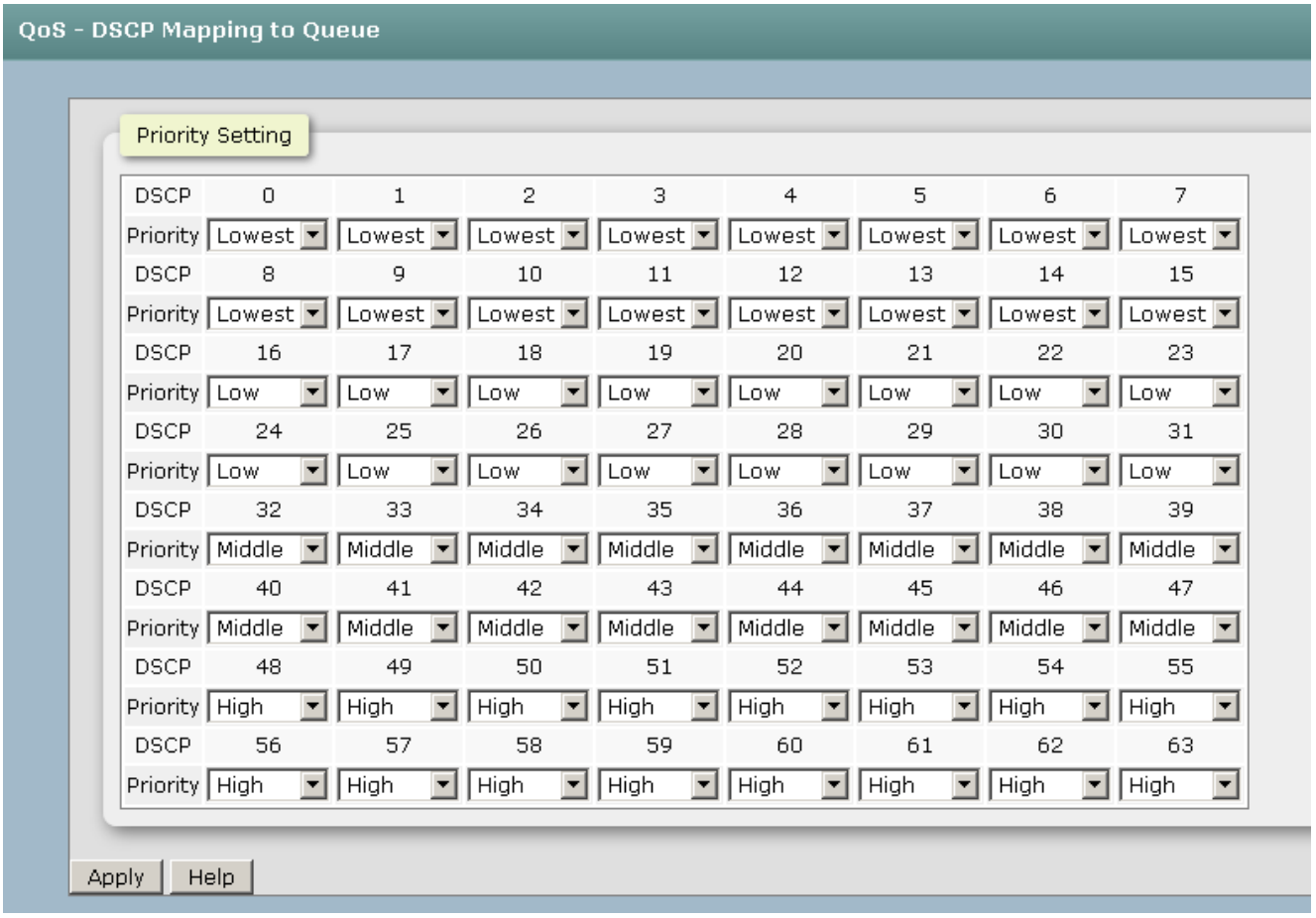
- **COS priority:** Set up the COS priority level 0~7—High, Middle, Low, Lowest.
- Click Apply.



6.25.4 DSCP mapping to queue

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

- **DSCP priority:** The system provides 0~63 DSCP 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 DSCP level value in the IP packet that has received. For example, the user sets the DSCP level 25 as high, the system will check the DSCP value of the received IP packet. If the DSCP 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.



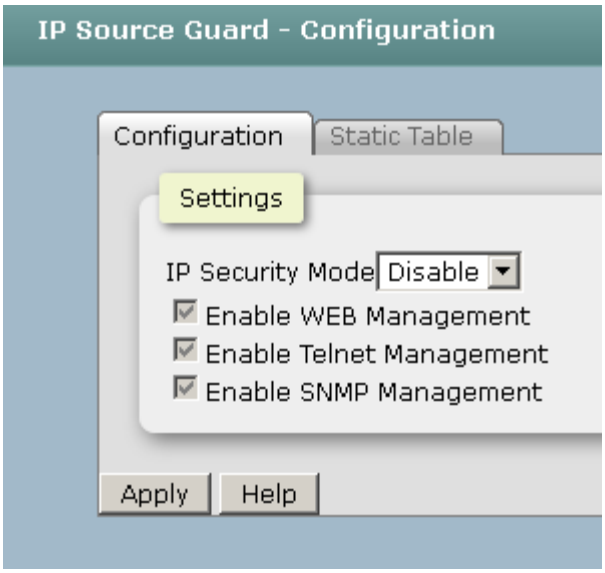
6.26.Security

You can block the un-authorized client in this function.

6.26.1 IP Source Guard - Configuration

IP Source Guard 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.

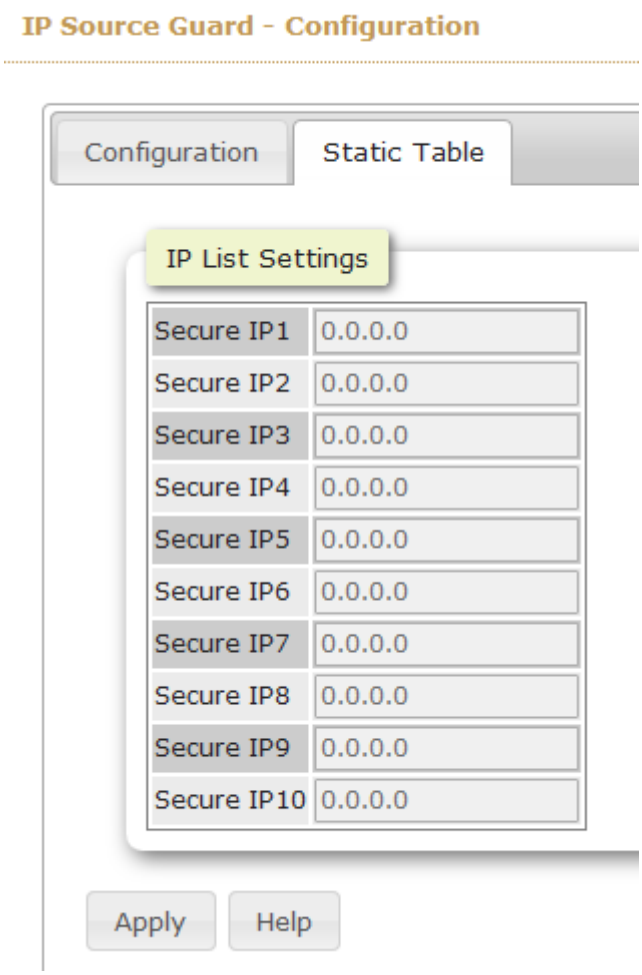
- **IP Security Mode:** Having set this selection item in the **Enable** mode, the **Enable HTTP Server**, **Enable Telnet Server** checkboxes and the ten security IP column fields will then be available. If not, those items will appear in grey.
- **Enable HTTP Server:** Having ticked this checkbox, 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.
- **Enable SNMP Management:** 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 SNMP service.



6.26.2 IP Source Guard – Static Table

- **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.

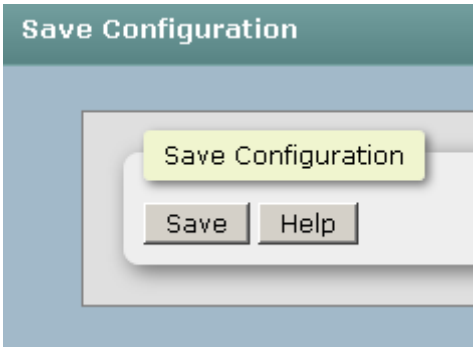
[NOTE]	Remember to execute the “Save Configuration” action, otherwise the new configuration will lose when the switch powers off.



6.27.Maintenance

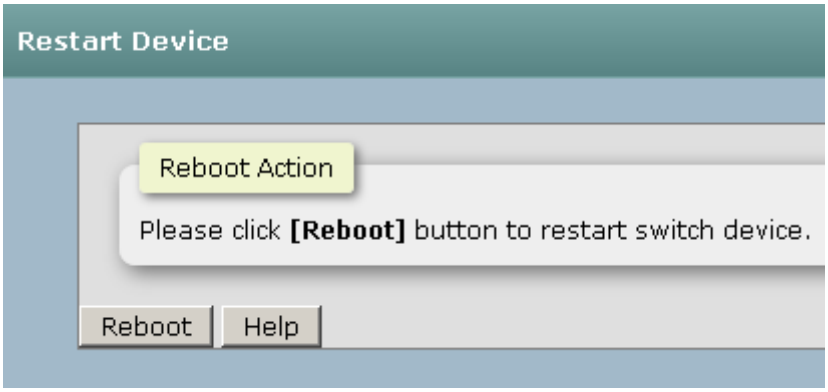
6.27.1 Save Configuration

Save the current setting of switch ..



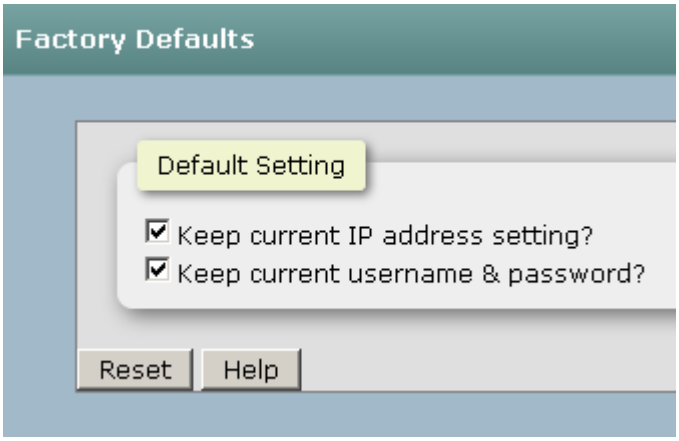
6.27.2 Restart Device

Make the switch warm start.



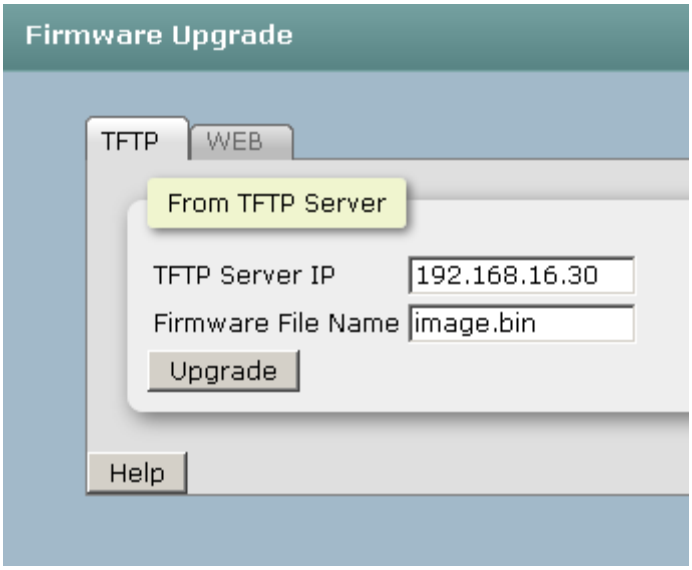
6.27.3 Factory Defaults

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

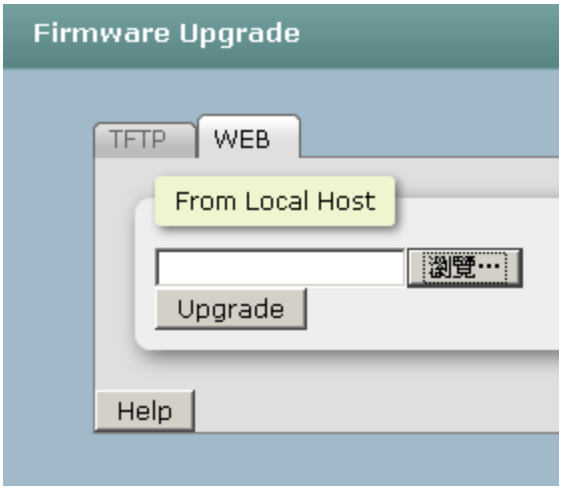


6.27.4 Firmware Upgrade

- **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 Upgrade



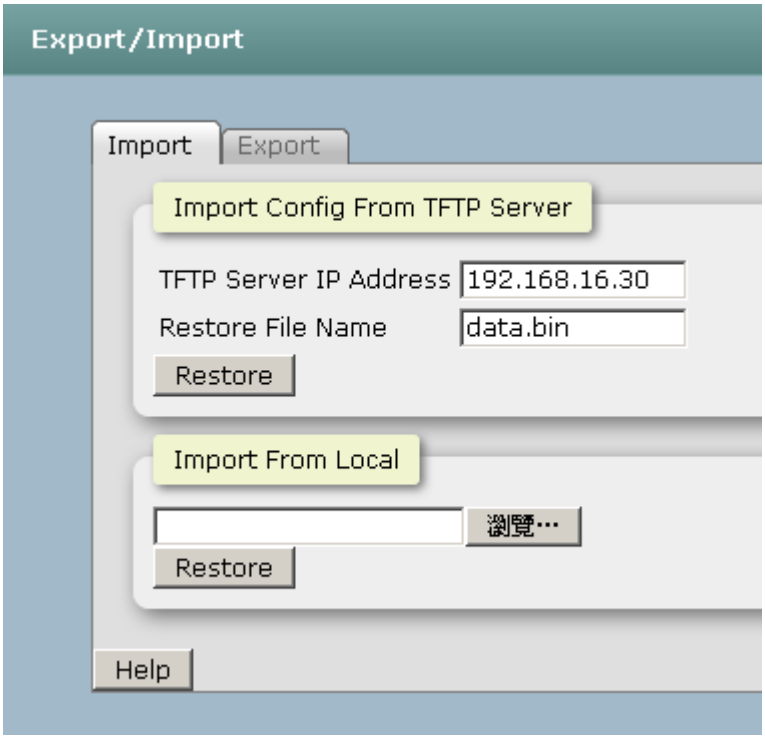
You can also browser the firmware on your hard drive by web update.



6.27.5 Export/Import

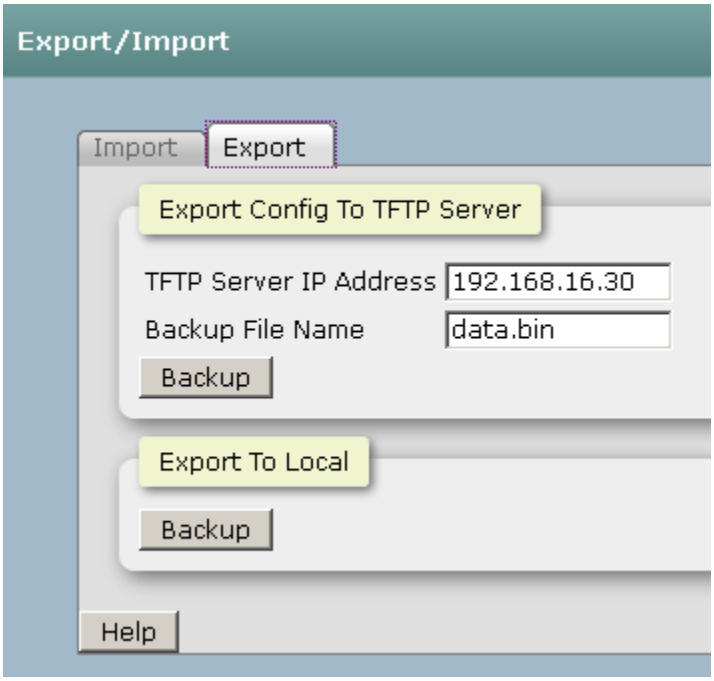
You can restore a previous backup configuration from the TFTP server to recover the settings. Before doing that, you must locate the image file on the TFTP server first and the switch will download back the flash image.

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



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.

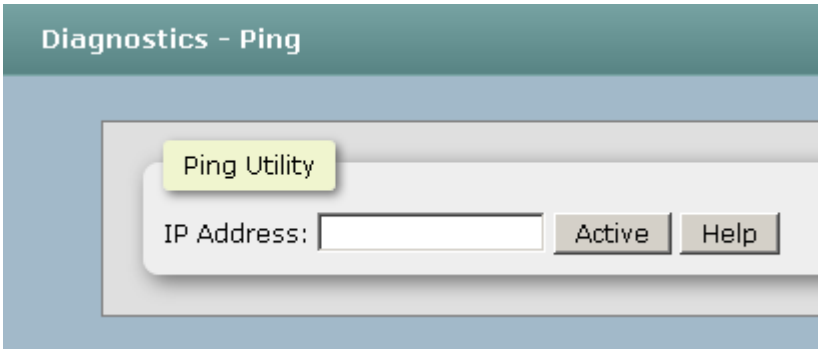
- **TFTP Server IP Address:** Type in the TFTP server IP.
- **Backup File Name:** Type in the file name.
- Click Backup..



6.27.6 Diagnostics

6.27.6.1 Ping

You can ping other network device in this function.

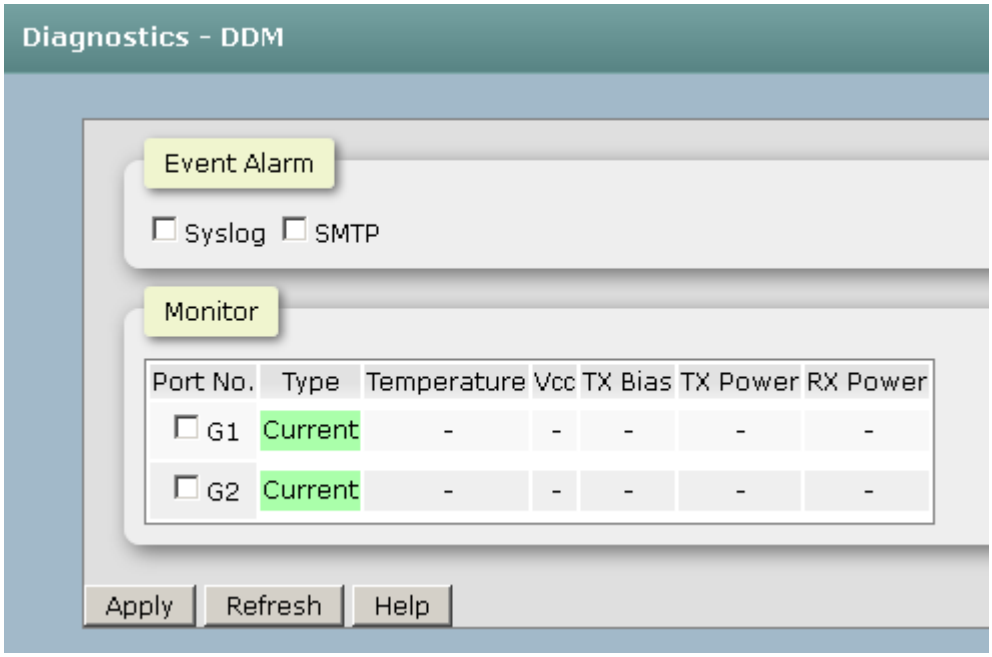


6.27.6.2 DDM

Port No.: Specify the SFP port and show the SFP module information.

- **Temperature:** Display the internal temperature of the SFP default threshold and present value.
- **Vcc:** Display the supply voltage of the SFP default threshold and present value.
- **Tx Bias:** Display the Bias current of the SFP default threshold and present value.

- **TX PWR:** Display the transmission power of the SFP default threshold and present value.
- **RX PWR:** Display the received power of the SFP default threshold and present value.
- **Syslog/SMTP:** The port will send an e-mail or log on local to administrator when detecting the exceptional value.



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 100 Ω 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-

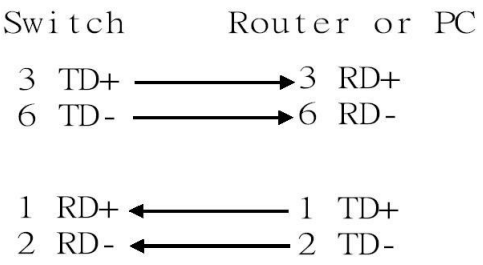
[NOTE] "+" and "-" signs represent the polarity of the wires that make up each wire pair.

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

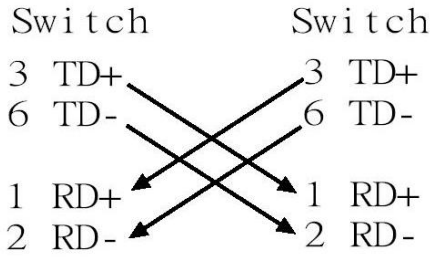
Pin Number	MDI-X Signal Name	MDI Signal Name
1	Receive Data plus (RD+)	Transmit Data plus (TD+)
2	Receive Data minus (RD-)	Transmit Data minus (TD-)
3	Transmit Data plus (TD+)	Receive Data plus (RD+)
6	Transmit Data minus (TD-)	Receive Data minus (RD-)

■ 10/100Base-TX Cable Schematic

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



Straight-through cable schematic

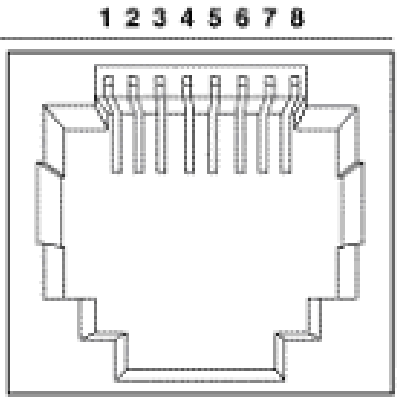


Cross over cable schematic

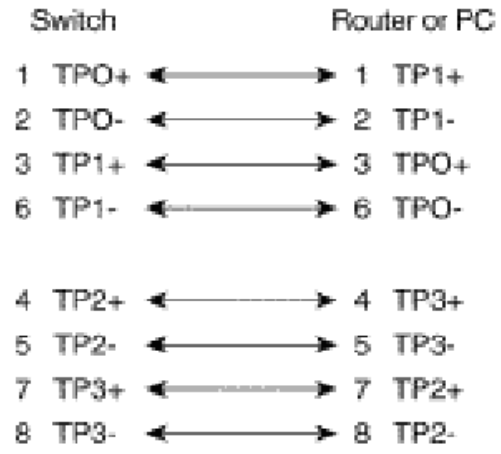
■ 10/100/1000Base-TX Pin outs

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

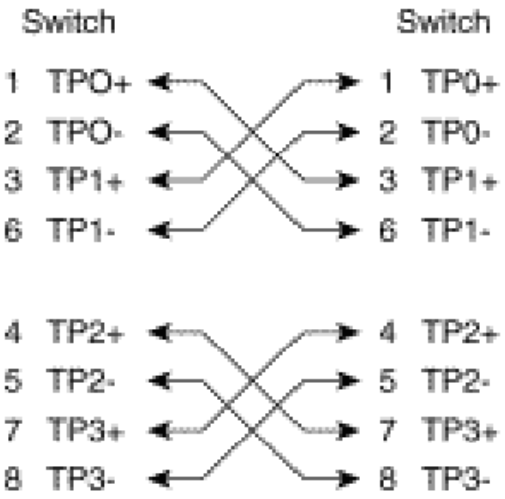
Pin	Label
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



■ 10/100/1000Base-TX Cable Schematic



Straight through cables schematic



Cross over cables schematic

RJ-45 Pin Assignment 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.