PLANET
Networking & Communication

User’s Manual

IGS-8044MT

4-Port 10/100/1000T + 4G TP/SFP Combo Managed Industrial Switch (-40~75 Degree C)

Trademarks

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

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 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 the 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 whose own expense.

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.

WEEE Warning

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

4-Port 10/100/1000Mbps + 4G TP/SFP Combo Managed Industrial Switch

FOR MODELS: IGS-8044MT

REVISION: 1.0 (JANUARY. 2012)

Part No.: EM-IGS-8044MT_v1.0 (2081-AH0550-000)

TABLE OF CONTENTS

1. Introduction

The PLANET Layer 2 Managed Industrial Switch series - IGS-8044MT and IGS-8044MTT are multiple 10/100Mbps ports Ethernet Switched with Gigabit TP/SFP fiber optical combo connective ability and robust layer 2 features; the description of these models as below:

IGS-8044MT	:	4-Port 10/100Base-TX + 4-Port Gigabit TP/SFP Combo Managed Industrial Ethernet Switch (-40 ~ 75 Degree C)

Terms of "**Managed Industrial Switch**" means the Switches mentioned titled in the cover page of this User's manual, i.e.IGS-8044MT.

1.1 Package Contents

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

- The IGS-8044MT Managed Industrial Switch x 1
- User manual 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.

1.2 Product Description

Enhanced Reliability for Industrial Networks

The PLANET IGS-8044MT is a fully Gigabit Managed Industrial switch. It is equipped with **4 10/100/1000Mbps** Ethernet ports and **4 100/1000Mbps** TP/SFP combo interfaces. The 4-Port 100/1000Mbps combo Fiber interface delivers highly data transmit speed and compatible with Gigabit fiber device and Fast Ethernet fiber device.

IGS-8044MT supports multiple redundant ring technology; The IGS-8044MT delivered in a rugged high-strength case. It is an industrially (substation) hardened and fully managed Ethernet Switch specifically designed to operate reliably in electrically harsh and climatically demanding environments. The IGS-8044MT is the most reliable choice for highly-managed and Fiber Ethernet application.

- Redundant Ethernet Network
- Manageable
- Power Redundant
- Fully Gigabit throughput capability
- Dual Speed Fiber interfaces support
- -40 to 75 Degree C wide temperature
- 12V to 48V DC wide range power supported
- IP-30 metal case

Redundant Ring, Fast Recovery to a Redundant Ethernet Network

The IGS-8044MT features strong and rapid self-recovery capability to prevent interruptions, and outside intrusions. It incorporates advanced **Redundant Ring** technology, Rapid Spanning Protocol (IEEE 802.1w RSTP), and redundant power supply system into customer's industrial automation network to enhance system reliability, and uptime in the harsh factory environments. It also protects customer's industrial network connectivity with switching recovery capability that is used for implementing fault tolerant ring, and mesh network architectures. If the Industrial network was interrupted accidentally, the fault recovery times could be **less than 20ms** to quickly bring the network back to normal operation.

Tough, Environmentally Hardened Design

With **IP-30** aluminum industrial case protection, the IGS-8044MT provides a high level of immunity against electromagnetic interference, and heavy electrical surges which are usually found on plant floors or in curb side traffic control cabinets. The IGS-8044MT also provides a wide range of power supply options suitable for multiple industries and for worldwide operation. The feature of operating temperature range from **-40 to 75 Degree C** allows the Managed Industrial Switch to be placed in almost any difficult environment.

Robust Layer 2 Features and Advanced Security

The IGS-8044MT supports robust advanced features including IEEE 802.1Q VLAN, GVRP, Port link aggregation, QoS, broadcast storm control, MAC address filtering, IGMP snooping enhanced security and bandwidth utilization to fit a variety of applications. Via aggregation of supporting port, the IGS-8044MT allows the operation of high-speed trunk combining multiple ports. Maximum up to 4 ports of the IGS-8044MT can be assigned for 4 trunk groups and support fail-over as well. Additionally, its standard-compliant implementation ensures interoperability with equipments from other vendors.

1.3 Product Features

- **Physical Port**
  - 4-Port 10/100/1000Base-T RJ-45
  - 4-Port Gigabit TP/SFP combo interface, SFP(Mini-GBIC) supports 100/1000Mbps Dual Mode
  - 1 RJ-45 Console interface for Switch basic management and setup

- **Industrial Conformance**
  - 12 to 48V DC, redundant power with polarity reverse protect function
  - -40 to 75 Degree C operation temperature
  - IP-30 metal case
  - Relay alarm for port breakdown, power failure
  - Supports Ethernet ESD protection
  - FCC Class A, CE compatibility
  - Free fall, Shock and Vibration Stability
  - EMS EN6100-4-2 (ESD), EN6100-4-3(RS), EN6100-4-4 (EFT), EN6100-4-5 (Surge), EN6100-4-6(CS), EN6100-4-8, EN6100-4-11

- **Rapid Ring**
  - Redundant Ring, Dual Homing, Coupling Ring Topology
  - Provides redundant backup feature and the recovery time less than 20ms

- **Layer 2 Features**
  - Complies with the IEEE 802.3, IEEE 802.3u, IEEE 802.3ab 10/100/1000Base-T and 100Base-FX, IEEE 802.3z 1000Base-SX / LX Ethernet standards
  - Supports Auto-negotiation and half duplex/full duplex modes for all 10/100Base-TX and 1000Base-T ports
  - Auto-MDI/MDI-X detection on each RJ-45 port
  - Prevents packet loss with back pressure (Half-Duplex) and IEEE 802.3x PAUSE frame flow control (Full-Duplex)
  - Supports VLANs
    - IEEE 802.1Q Tagged based VLAN
    - Port-Based VLAN
    - GVRP
    - Up to 255 VLANs groups, out of 4K VLAN IDs
  - Supports Spanning Tree Protocol
    - RSTP, IEEE 802.1w Rapids Spanning Tree Protocol
  - Supports Link Aggregation
    - Up to 4 Trunk groups

   - Up to 4 ports per trunk group with 1600Mbps bandwidth (Full Duplex mode)
   - IEEE 802.3ad LACP (Link Aggregation Control Protocol)
   - Static Port Trunk supported

- **Quality of Service**
  - 4 priority queues on all switch ports
  - Traffic classification by:
    - Port-Based priority
    - IEEE 802.1p Class of Service
    - TOS / DSCP priority
  - Supports strict priority and Weighted Round Robin (WRR) policies
  - Ingress/Egress Bandwidth control on each port

- **Multicast**
  - IGMP Snooping v2 and v3 for filtering multicast traffic
  - IGMP Query mode for Multicast Media application

- **Security**
  - IEEE 802.1x Port-Based Authentication
  - MAC address Filtering
  - IP address security management to prevent unauthorized intruder
  - Port Monitoring to monitor the incoming or outgoing traffic on a particular port

- **Management**
  - WEB-based, Telnet, Console Command Line management
  - Access through SNMP v1, v2c and v3 set and get requests
  - SNMP Trap / SMTP email for alarm notification of events
  - System Log Server / Client
  - Configuration backup / restore
  - TFTP firmware upgrade
  - Support LLDP (Link Layer Discovery protocol) to allow switch to advise its identification and capability on the LAN

1.4 Product Specification

Product	**IGS-8044MT** 4-Port 10/100/1000Mbps + 4-Port Gigabit TP/SFP Combo Managed Industrial Switch
Hardware Specification	
Copper Ports	4 10/100/1000Base-T RJ-45 Auto-MDI/MDI-X ports
SFP/mini-GBIC Slots	4 100/1000Base-X SFP interfaces, shared with from Port-5 to Port-8
Switch Architecture	Store-and-Forward
Switch Fabric	16Gbps / non-blocking
Switch Throughput	11.9Mpps@64bytes
Address Table	8K entries
Share Data Buffer	1Mbit
Maximum Frame Size	1522 Bytes packet
Flow Control	Back pressure for Half-Duplex IEEE 802.3x Pause Frame for Full-Duplex
LED	Per unit: Power (Green), Power 1 (Green), Power 2 (Green), Fault (Orange) 4 port 10/100/1000T: Link/Activity (Green), 10/100TX Full duplex/Collision (Orange) SFP port: LNK/ACT(Green), 1000T: LNK/ACT(Green), 1000M(Green)
Console Interface	One RJ-45 to RS-232 male connector for switch management
Reset Button	< 5 seconds: System reboot > 10 seconds: Factory Default
Dimension (W x D x H)	74.3 x 109.2 x 153
Weight	1.15Kg
Power Input	12V to 48V DC input
Layer 2 function	
Management Interface	Console, Telnet, Web Browser, SNMP v1, v2c and v3
Port Configuration	Port disable/enable. Auto-negotiation 10/100/1000Mbps full and half duplex mode selection. Flow Control disable / enable. Bandwidth control on each port.
Port Status	Display each port's speed duplex mode, link status, Flow control status. Auto negotiation status
VLAN	Port-Based VLAN, up to 8 VLAN groups IEEE 802.1q Tagged Based VLAN , 4K VLAN ID, up to 256 VLAN groups
Spanning Tree	IEEE 802.1w Rapid Spanning Tree
Link Aggregation	IEEE 802.3ad LACP / Static Trunk Supports 4 groups of 4-Port trunk support
QoS	Traffic classification based on :

	• Port Number, • 802.1Q Tag, • 802.1p priority, • IP DSCP/TOS field in IP Packet
IGMP Snooping	V2 and v3 1024 multicast groups and IGMP query
Bandwidth Control	Per port bandwidth control Ingress: 500Kb~80Mbps Egress: 64Kb~80Mbps
Port Mirror	RX/TX/Both
Security	Support 100 entries of MAC address for static MAC and another 100 for MAC filter Support 10 IP addresses that have permission to access the switch management and to prevent unauthorized intruder
SNMP MIBs	RFC-1213 MIB-II RFC-2863 Interface MIB RFC-1493 Bridge MIB RFC-2674 Extended Bridge MIB (Q-Bridge) Private MIB
Standards Conformance	
Regulation Compliance	FCC Part 15 Class A, CE, EN60950
Safety	EN60950-1
Standards Compliance	IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX/100ase-FX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000T IEEE 802.3x Flow Control and Back pressure IEEE 802.1d Spanning tree protocol IEEE 802.1w Rapid spanning tree protocol IEEE 802.1p Class of service IEEE 802.1Q VLAN Tagging IEEE 802.1x Port Authentication Network Control

2. Installation

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

2.1 Hardware Description

2.1.1 Physical Dimension

- **IGS-8044MT** Managed Industrial Switch dimension (W x D x H) : **74.3mm x 109.2mm x 153.6mm**

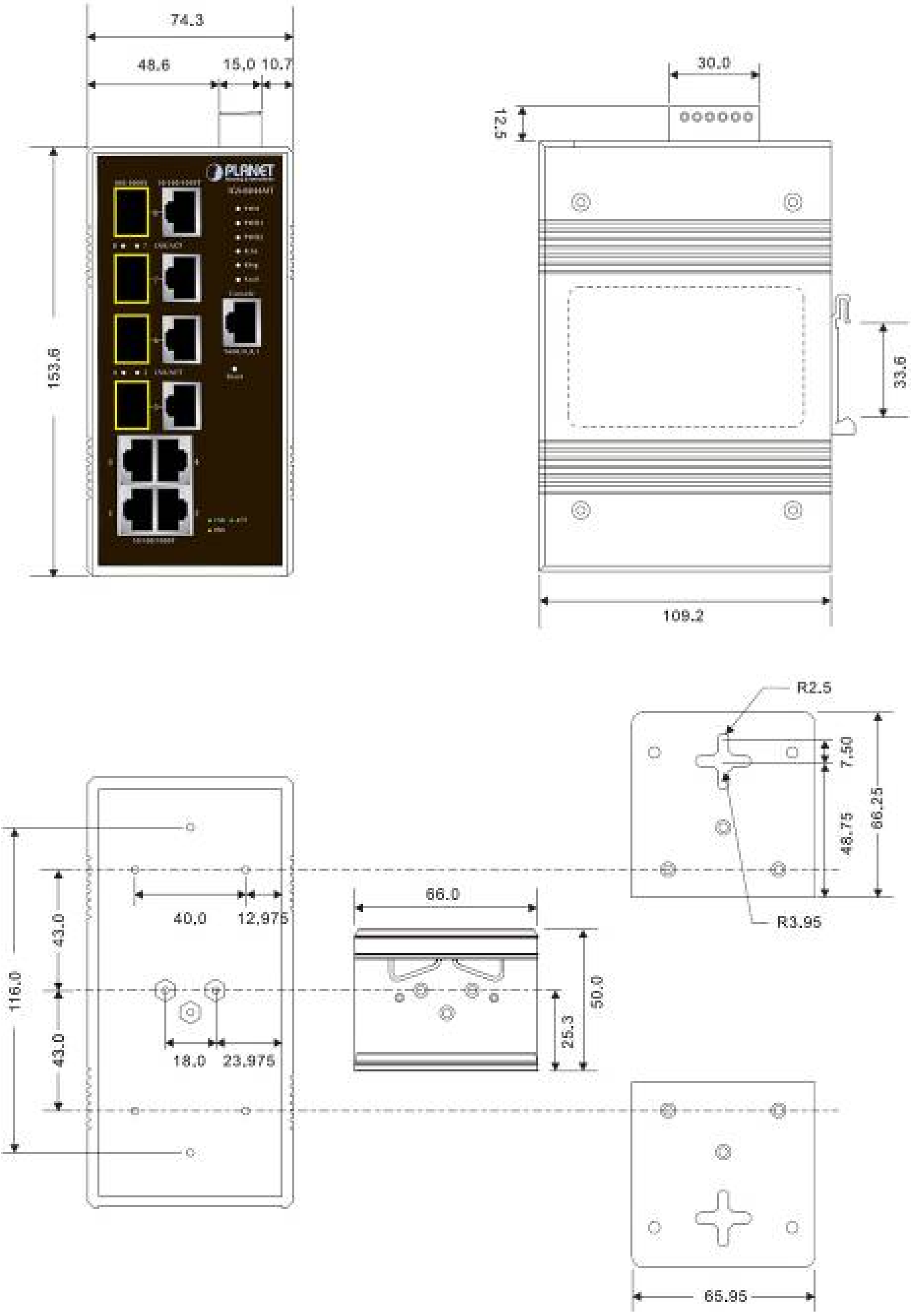


Figure 2-1 IGS-8044MT panel layout

2.1.2 Front / Rear Panel

The Front Panel and Rear Panel of the IGS-8044MT Managed Industrial Switch are shown as below:

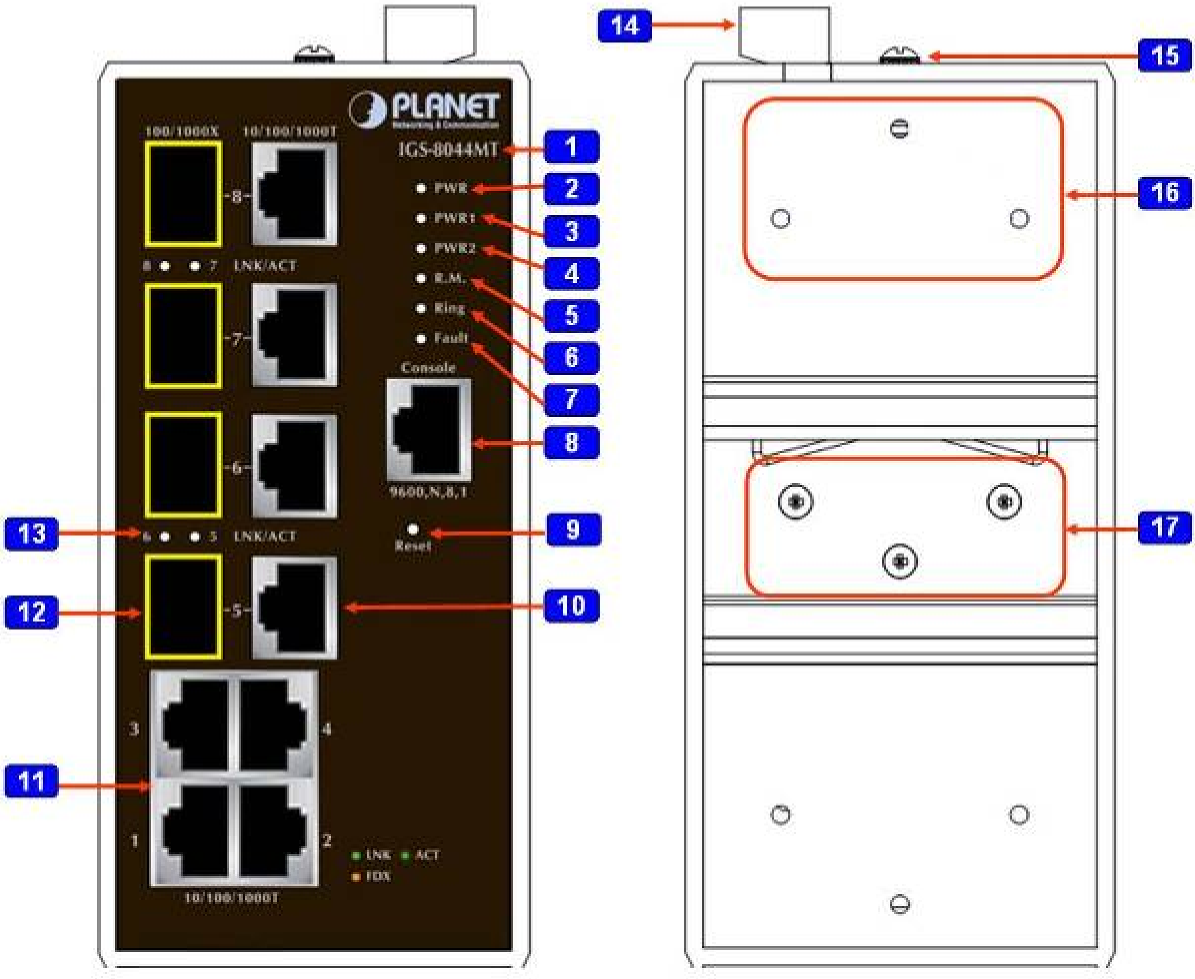


Figure 2-2 Front and Rear Panel of IGS-8044MT

1. Model Name	**10. 4 x 10/100/1000Base-T port shared with SFP Slot**
2. System Power: LED	**11. 4 x 10/100/1000Base-T ports**
3. LED for power 1 input	**12. 4 x 100/1000Base-X SFP Slot**
4. LED for power 2 input	**13. TP/SFP port LED**
5. Ring Master LED	**14. Terminal Block for power input and Fault Alarm**
6. Ring Status LED	**15. Grounding screw**
7. Fault Alarm LED	**16. Screw holes for Wall Mounting kit**
8. RJ-45 type RS-232 Console	**17. DIN-Rail Kit**
9. RESET Button	

2.1.3 Bottom View

The bottom panel of the IGS-8044MT Managed Industrial Switch has one terminal block connector of two DC power inputs and one fault alarm.

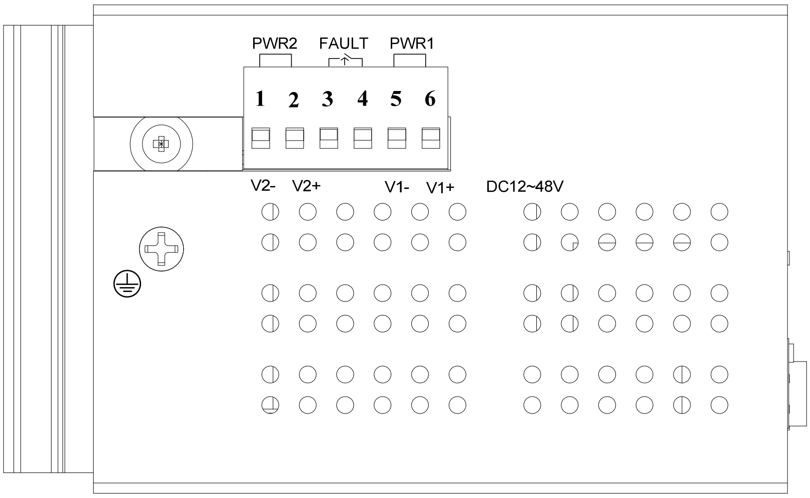


Figure 2-3 Bottom Panel of IGS-8044MT

2.1.4 LED Indicators

The diagnostic LEDs that provide real-time information of system and optional status are located on the front panel of the IGS-8044MT. The following table provides the description of the LED status and their meanings for the Managed Industrial Switch.

■ System

LED	Color	Status	Meaning
PWR	**Green**	On	The switch unit is power on.
		Off	No power.
PWR1	**Green**	On	Power 1 is active.
		Off	Power 1 is inactive.
PWR2	**Green**	On	Power 2 is active.
		Off	Power 2 is inactive.
R.M.	**Green**	On	The industrial switch is the master of Ring group.
		Off	The industrial switch is not a ring master in Ring group.
Ring	**Green**	On	Ring works normally.
		Blinking	Ring failed.
Fault	**Orange**	On	Power or port failure
		Off	No failure

■ Port-1 to Port-8 10/100/1000Base-T

LED	Color	Status	Meaning
Port-1 ~ Port-8	**Green**	On	A network device is detected.
		Blinking	The port is transmitting or receiving packets from the TX device.
		Off	No device attached
	Orange	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.

■ Port-5 to Port-8 100/1000Base-SX/LX SFP combo interface

LED	Color	Status	Meaning
Link/Active	**Green**	On	The SFP port is linking
		Blinking	The port is transmitting or receiving packets from the TX device.
		Off	No device attached

2.2 Install the Switch

This section describes how to install your Managed Industrial Switch and make connections to the Managed Industrial Switch. Please read the following topics and perform the procedures in the order being presented. To install your switch on a desktop or shelf, simply complete the following steps.

In this paragraph, we will describe how to install IGS-8044MT Managed Industrial Switch and the installation points attended to it.

2.2.1 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 5e/6 cable for Ethernet connection.**
6. **Insert one side of RJ-45 cable (category 5e/6) 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-5e/6 cable.

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

2.2.2 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.

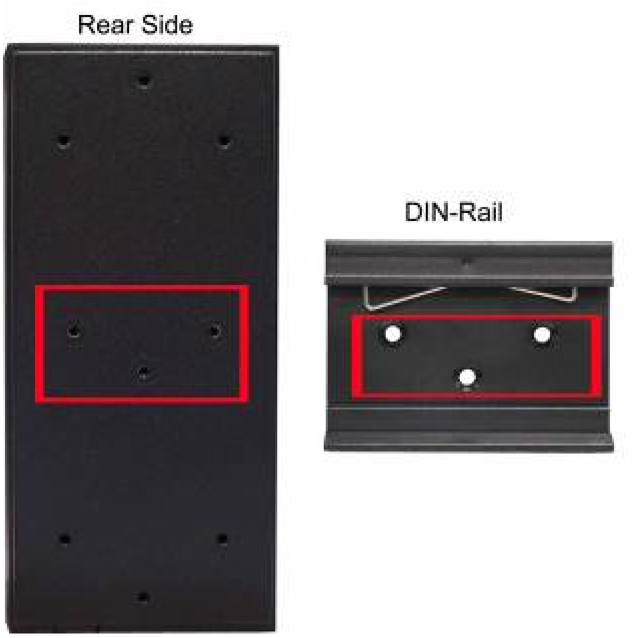


Figure 2-4 Rear Panel – DIN-Rail Kit

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

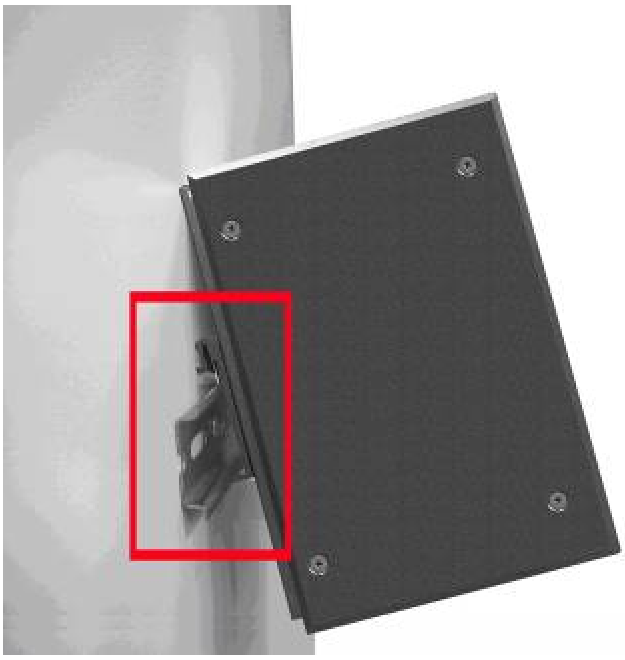


Figure 2-5 DIN-Rail Mounting

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

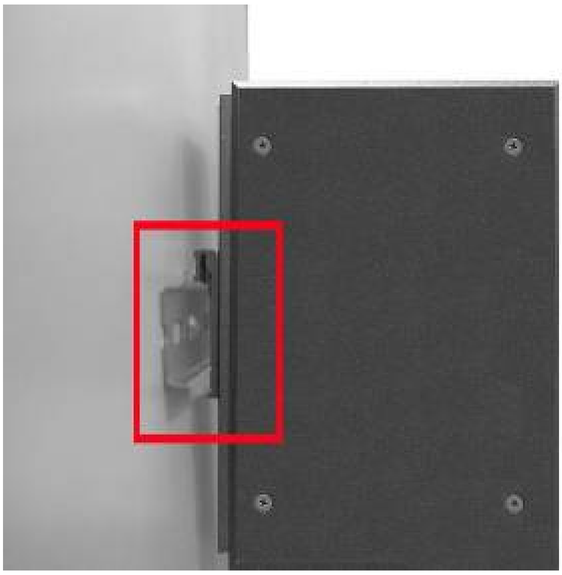


Figure 2-6 DIN-Rail mounting

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.**

2.2.3 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.

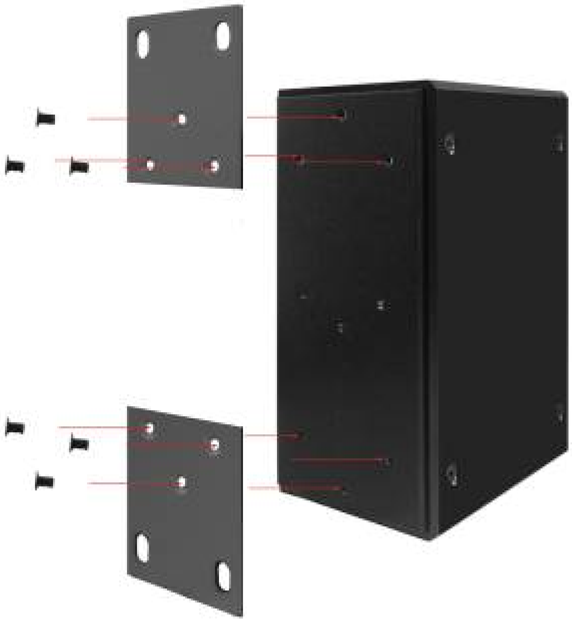


Figure 2-7 Wall mounting

2.2.4 Wiring the Power Inputs

The 6-contact terminal block connector on the top panel of IGS-8044MT is used for two DC redundant power input. Please follow the steps below to insert the power wire.

1. Insert positive / negative DC power wires into the contacts 1 and 2 for POWER 2, or 5 and 6 for POWER 1.

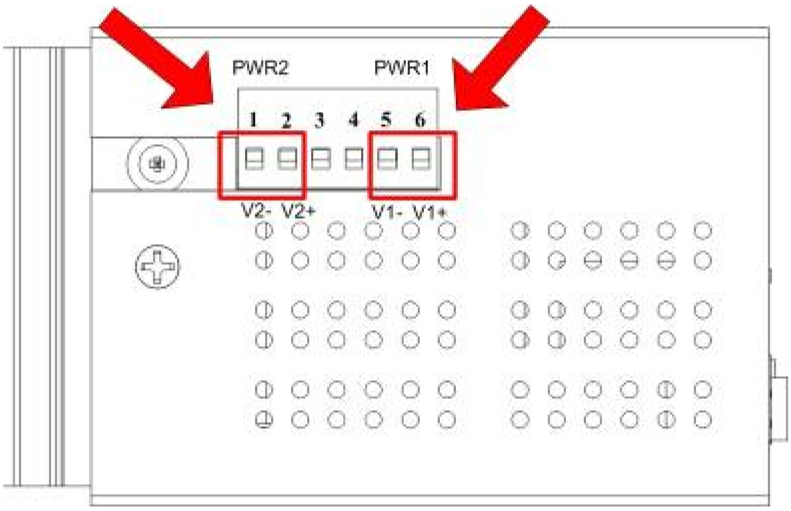


Figure 2-8 Wiring the redundant power inputs

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

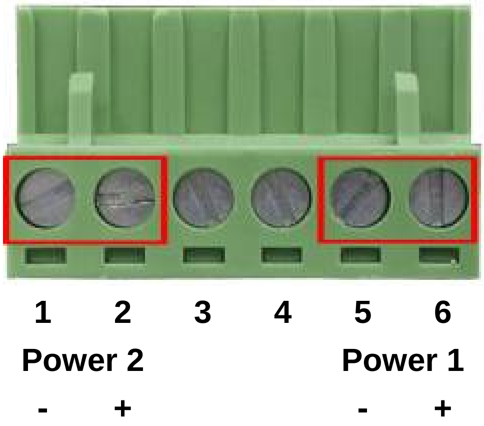


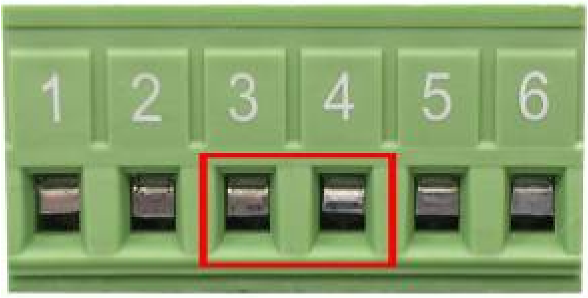
Figure 2-9 6-Pin Terminal Block power wiring input

Note

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

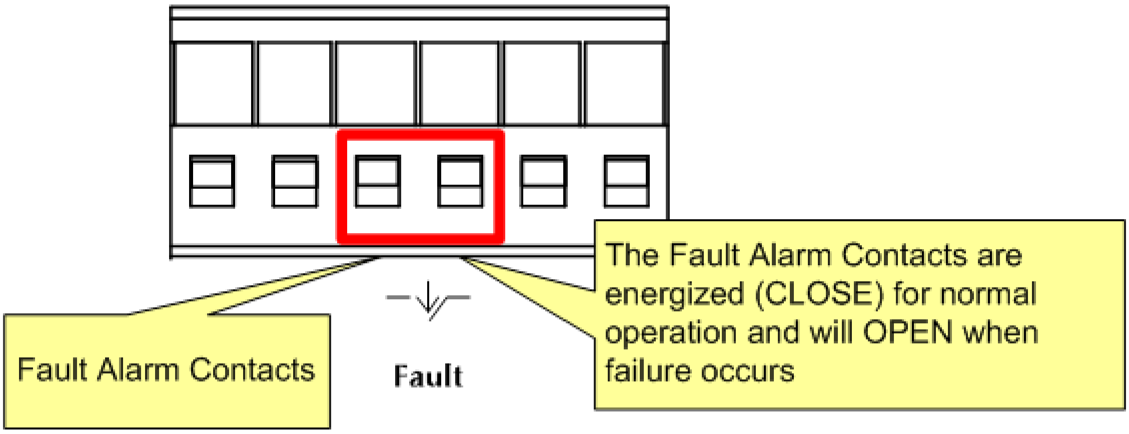
2.2.5 Wiring the Fault Alarm Contact

The fault alarm contacts are in the middle of the terminal block connector as the picture shows below. Inserting the wires, the Industrial 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

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


Fault Alarm Contacts
Fault
The Fault Alarm Contacts are energized (CLOSE) for normal operation and will OPEN when failure occurs

2.2.6 Installing the SFP transceiver

The sections describe how to insert an SFP transceiver into an SFP slot.

The SFP transceivers are hot-pluggable and hot-swappable. You can plug-in and out the transceiver to/from any SFP port without having to power down the Industrial Switch. As the Figure 2-10 appears.

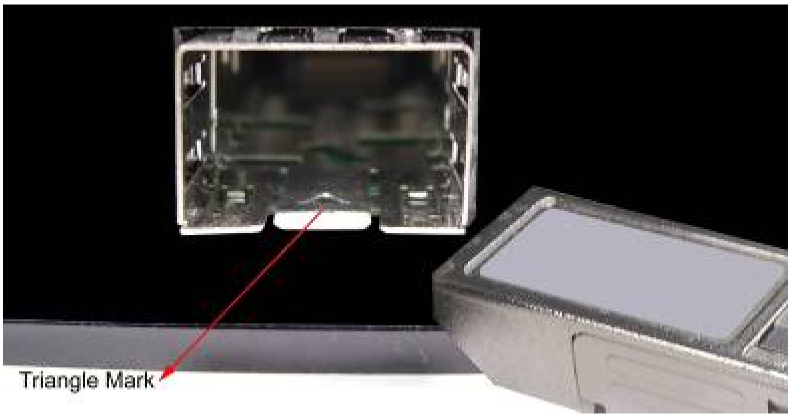


Figure 2-10 Plug-in the SFP transceiver

- **Approved PLANET SFP Transceivers**

PLANET Industrial Switch supports both Single mode and Multi-mode SFP transceiver. The following list of approved PLANET SFP transceivers is correct at the time of publication:

- MGB series SFP module

Gigabit Ethernet SFP Module List		
Model	**Interface**	**Fiber Connector type and distance**
MGB-GT	1000Base-T Module	RJ-45, 100m
MGB-SX	1000Base-SX Module	LC, Multi-Mode, 550m
MGB-SX2	1000Base-SX Module	LC, Multi-Mode, 2km
MGB-LX	1000Base-LX Module	LC, Single Mode, 10km
MGB-L30	1000Base-LX Module	LC, Single Mode, 30km
MGB-L50	1000Base-LX Module	LC, Single Mode, 50km
MGB-L70	1000Base-LX Module	LC, Single Mode, 70km
MGB-L120	1000Base-LX Module	LC, Single Mode, 120km
MGB-LA10	1000Base-LX Module	LC WDM (TX:1310nm), SM, 10km
MGB-LB10	1000Base-LX Module	LC WDM (TX:1550nm), SM, 10km
MGB-LA20	1000Base-LX Module	LC WDM (TX:1310nm), SM, 20km
MGB-LB20	1000Base-LX Module	LC WDM (TX:1550nm), SM, 20km
MGB-LA40	1000Base-LX Module	LC WDM (TX:1310nm), SM, 40km

MGB-LB40	1000Base-LX Module	LC WDM (TX:1550nm), SM, 40km
MGB-LA20S	1000Base-LX Module	SC WDM, SM, 20km (TX:1310nm, RX:1490nm)
MGB-LB20S	1000Base-LX Module	SC WDM, SM, 20km (TX:1490nm, RX:1310nm)
MGB-LA60S	1000Base-LX Module	SC WDM, SM, 60km (TX:1310nm, RX:1490nm)
MGB-LB60S	1000Base-LX Module	SC WDM, SM, 60km (TX:1490nm, RX:1310nm)
MGB-TSX	1000Base-SX Module	LC, Multi-Mode, 550m (-40~75℃)
MGB-TLX	1000Base-LX Module	LC, Single Mode, 10km (-40~75℃)
MGB-TL30	1000Base-LX Module	LC, Single Mode, 30km (-40~75℃)
MGB-TL70	1000Base-LX Module	LC, Single Mode, 70km (-40~75℃)

- MFB series module

Fast Ethernet SFP Module List

Model	Interface	Fiber connector type and distance
MFB-FX	100Base-FX Module	LC, Multi-Mode (1310nm) -2km
MFB-F20	100Base-FX Module	LC, Single Mode (1310nm) – 20km
MFB-F40	100Base-FX Module	LC, Single Mode (1310nm) – 40km
MFB-F60	100Base-FX Module	LC, Single Mode (1310nm) – 60km
MFB-FA20	100Base-BX Module	LC WDM, Single Mode (TX:1310nm, RX:1550nm) -20km
MFB-FB20	100Base-BX Module	LC WDM, Single Mode (TX:1550nm, RX:1310nm) -20km
MFB-TFX	100Base-FX Module	LC, Multi-Mode (1310nm) -2km (-40~75℃)
MFB-TF20	100Base-FX Module	LC, Single Mode (1310nm) – 20km (-40~75℃)

Note

1. It recommends using PLANET SFPs on the Managed Industrial Switch. If you insert a SFP transceiver that is not supported, the Managed Industrial Switch will not recognize it.
2. Please be noticed that choose high temperature supported SFP module if you want IGS-8044MT operate on **-40 to 75** Degree C environment.
3. As SFP install example, we choose MGB SFP module to describe how to install, however, 1000Base-FX series SFP module installation is the same with 1000Base-SX/LX module.

CAUTION

Fiber attenuator is required for the installation in some circumstances. Please base on the physical cable distance and link budget to deploy a proper attenuator, otherwise it may damage the mini GBIC transceiver.

Before connect the other switches, workstation or Media Converter.

1. Make sure both side of the SFP transceiver are with the same media type, for example: 1000Base-SX to 1000Base-SX, 1000Bas-LX to 1000Base-LX.
2. Check the fiber-optic cable type match the SFP transceiver model.
   - To connect to 1000Base-SX SFP transceiver, use the Multi-mode fiber cable- with one side must be male duplex LC connector type.
   - To connect to 1000Base-LX SFP transceiver, use the Single-mode fiber cable-with one side must be male duplex LC connector type.

Connect the fiber cable

1. Attach the duplex LC connector on the network cable into the SFP transceiver.
2. Connect the other end of the cable to a device – switches with SFP installed, fiber NIC on a workstation or a Media Converter.
3. Check the LNK/ACT LED of the SFP slot on the front of the Managed Industrial Switch. Ensure that the SFP transceiver is operating correctly.
4. Check the Link mode of the SFP port if the link failed. Co works with some fiber-NICs or Media Converters, set the Link mode to "1000 Force" is needed.

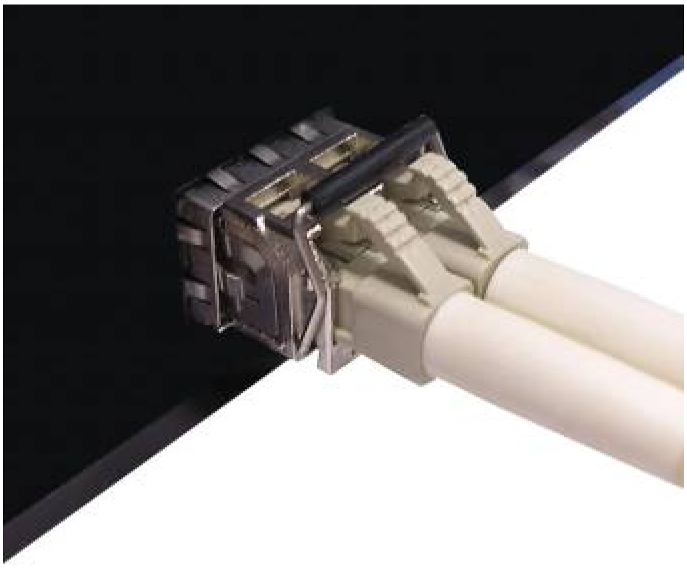


Figure 2-11 LC connector connects to the transceiver

Remove the transceiver module

1. Make sure there is no network activity by consult or check with the network administrator. Or through the management interface of the switch/converter (if available) to disable the port in advance.
2. Remove the Fiber Optic Cable gently.

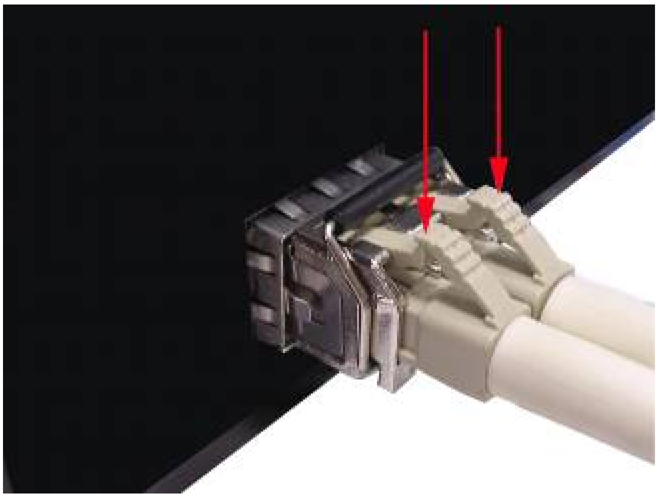


Figure 2-12 Pull out the SFP transceiver

3. Turn the handle of the MGB module to horizontal.
4. Pull out the module gently through the handle.

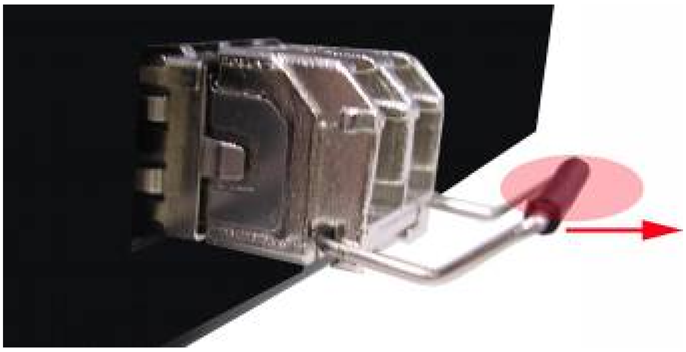


Figure 2-13 Pull out from the transceiver

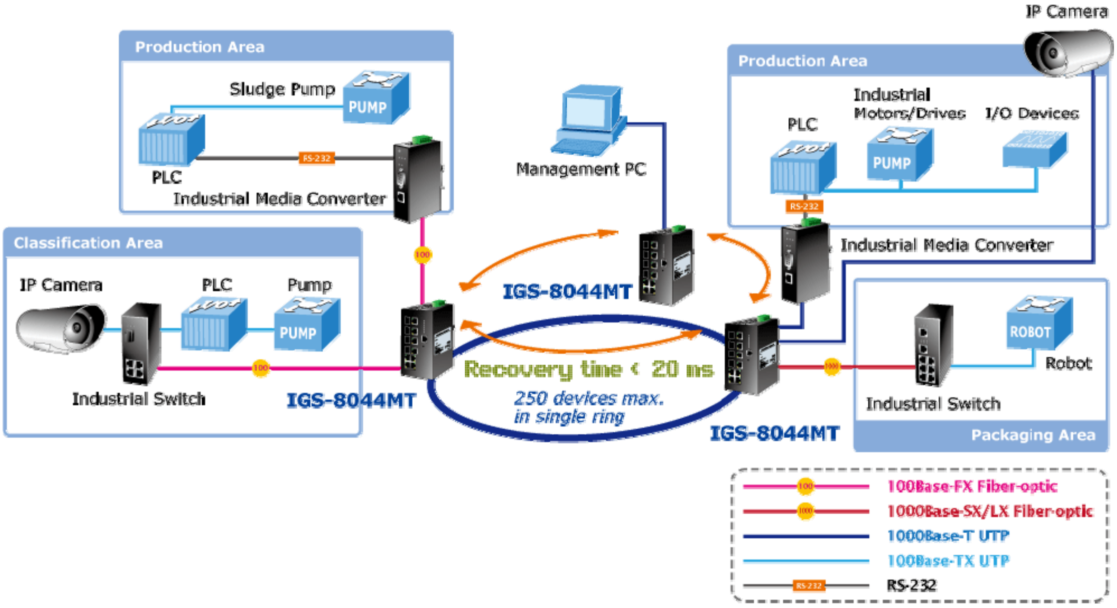
CAUTION

Never pull out the module without pull the handle or the push bolts on the module. Direct pull out the module with violent could damage the module and SFP module slot of the Managed Industrial Switch.

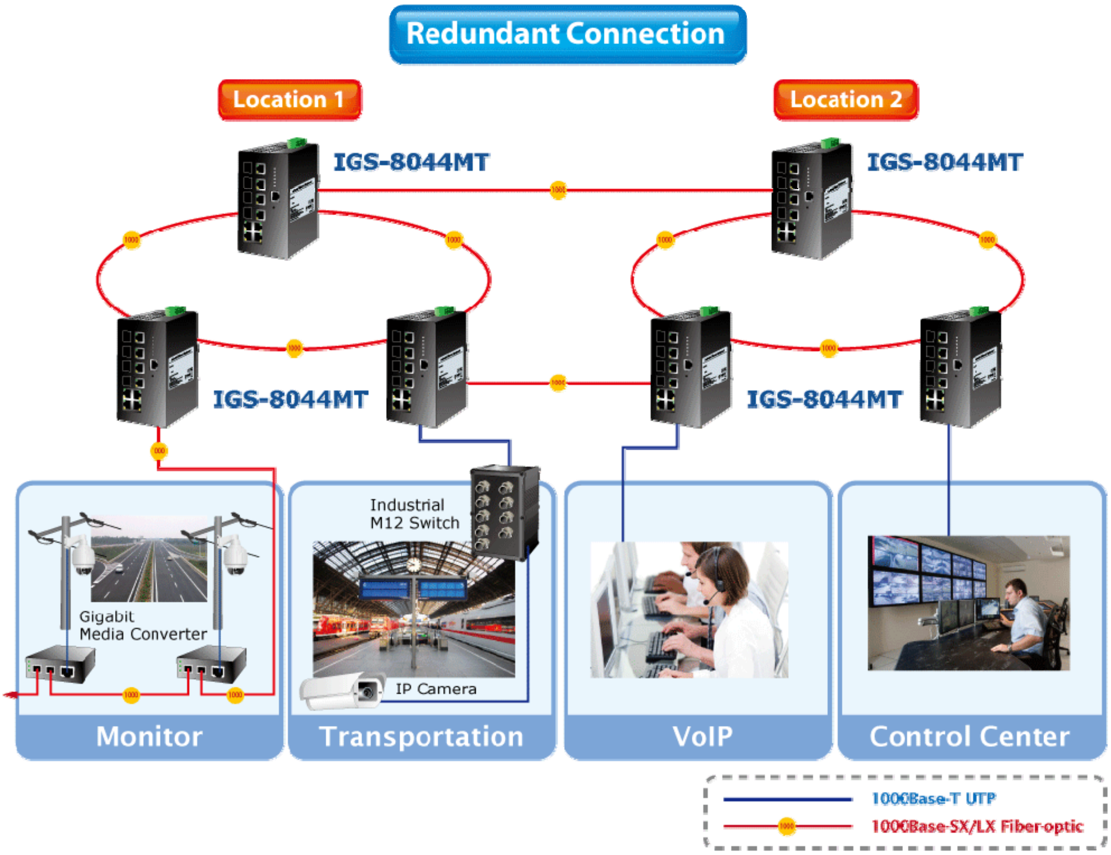
3. Network Application

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 as below:

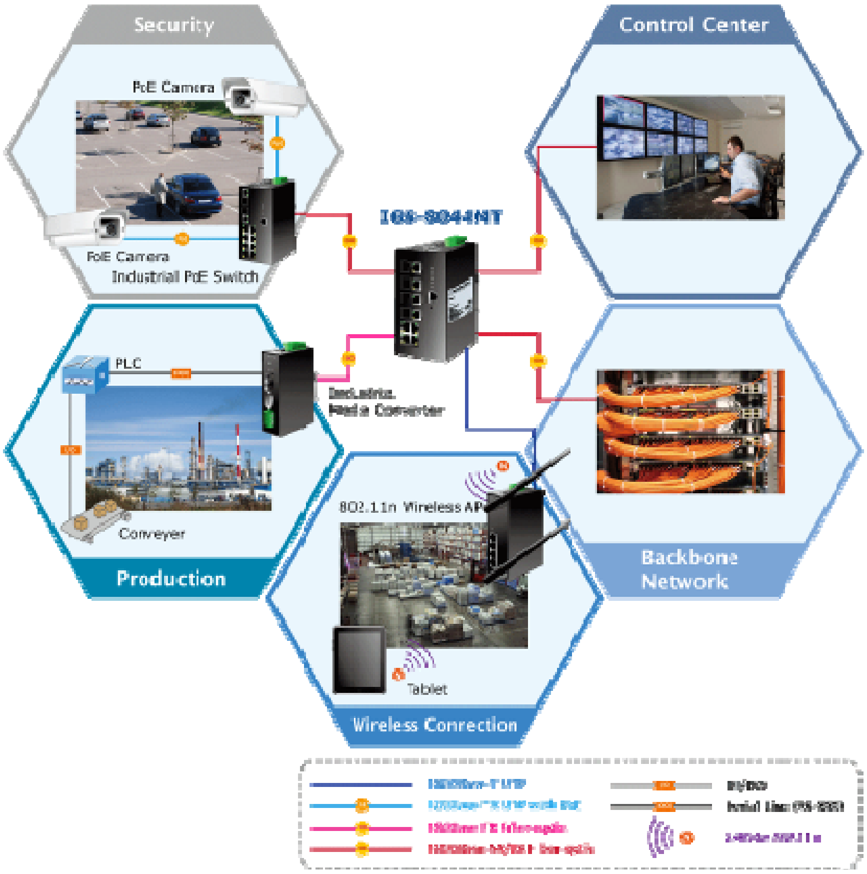
- **Factory redundant ring application**



- **Coupling Ring – Connection redundant with different area application**

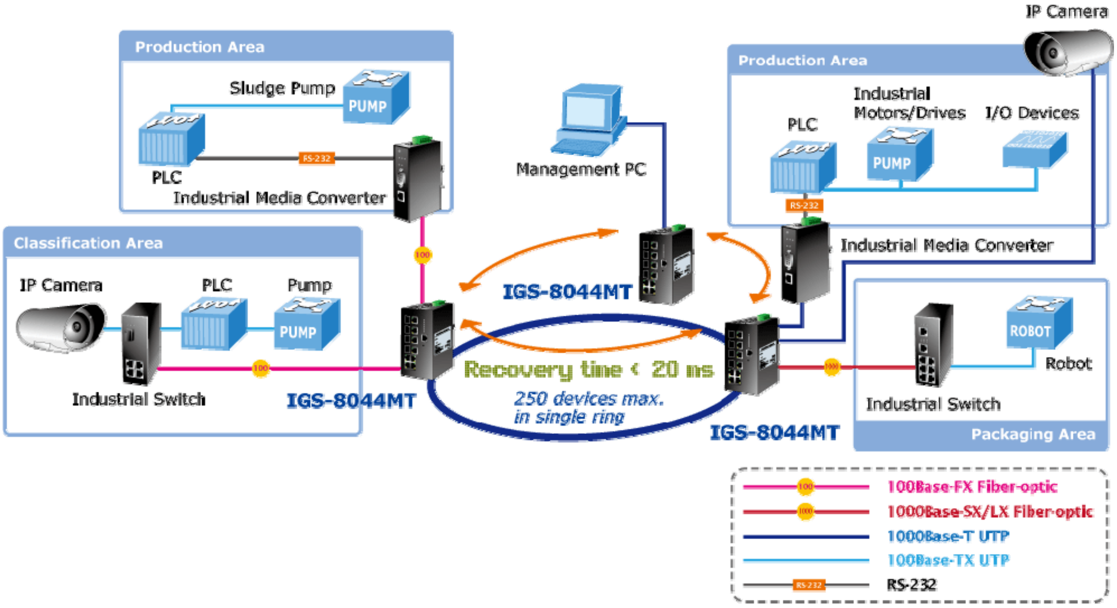


- **To be a Core Switch on the networking application**



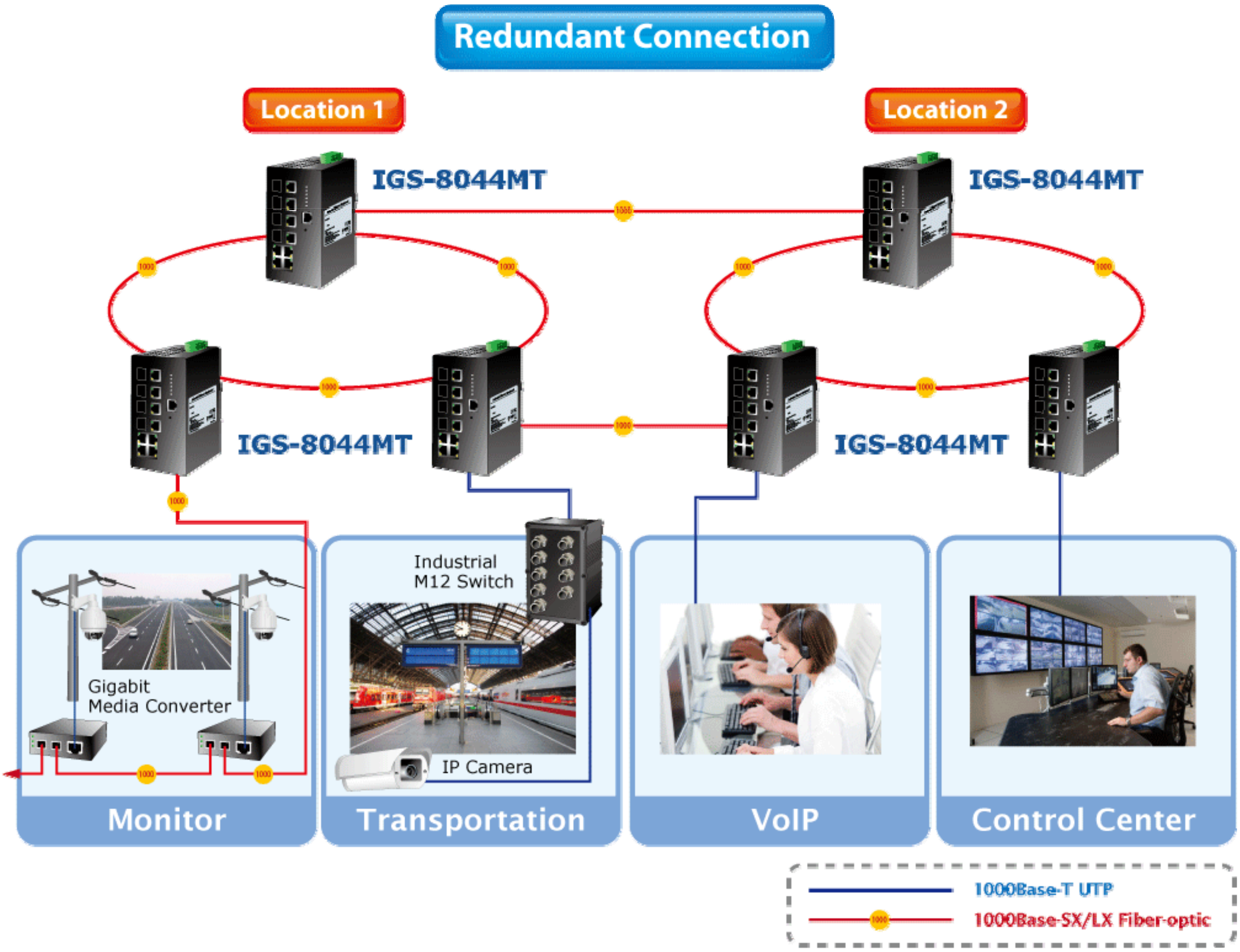
3.1 Ring Application

The IGS-8044MT supports the 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 Ring algorithm is similar to spanning tree protocol (STP) algorithm but its recovery time is faster than STP.



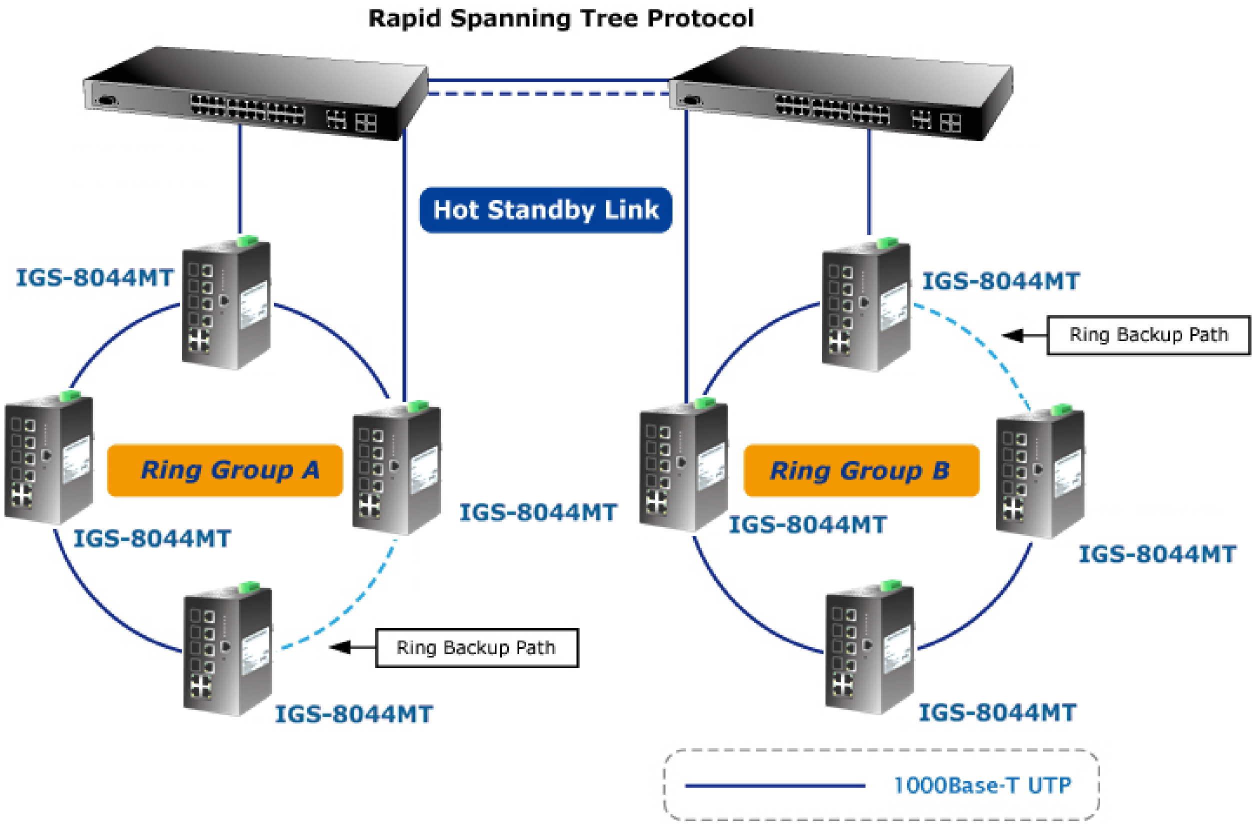
3.2 Coupling Ring Application

In the network, it may have more than one Ring group. By using the coupling ring function, it can connect each 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.



3.3 Dual Homing Application

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

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.

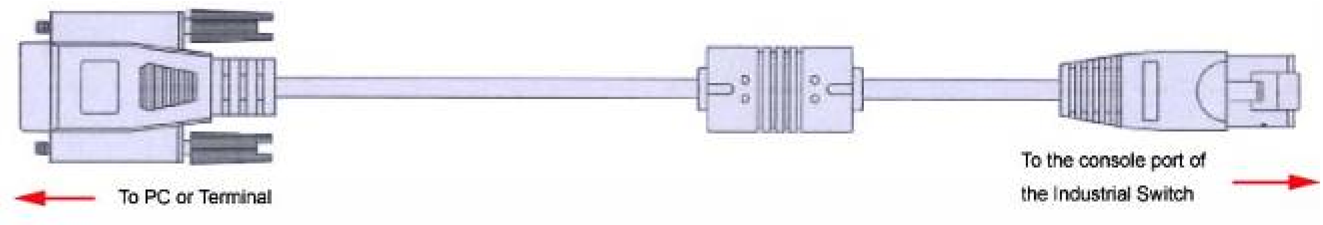
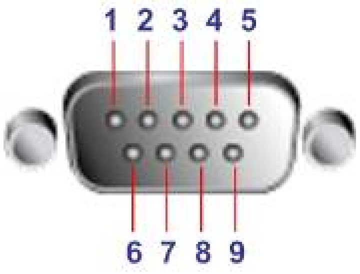


Figure 4-1 RJ-45 to DB9 Console cable

4.2 Pin Assignment

- **DB9 Pin Define for RJ-45 Connector**

	DB9-PIN	RJ-45 Connector
	1	1 Orange/White
	2	2 Orange
	3	3 Green/White
	4	4 Blue
	5	5 Blue/White
	6	6 Green
	7	7 Brown/White
	8	8 Brown
	9	

4.3 Login in the Console Interface

To configure the system, connect a serial cable to a **COM port** on a PC or notebook computer and to RJ-45 type serial (console) port of the Managed Industrial Switch. The console port of the Managed Industrial Switch is DCE already, so that you can connect the console port directly through PC without the need of Null Modem.

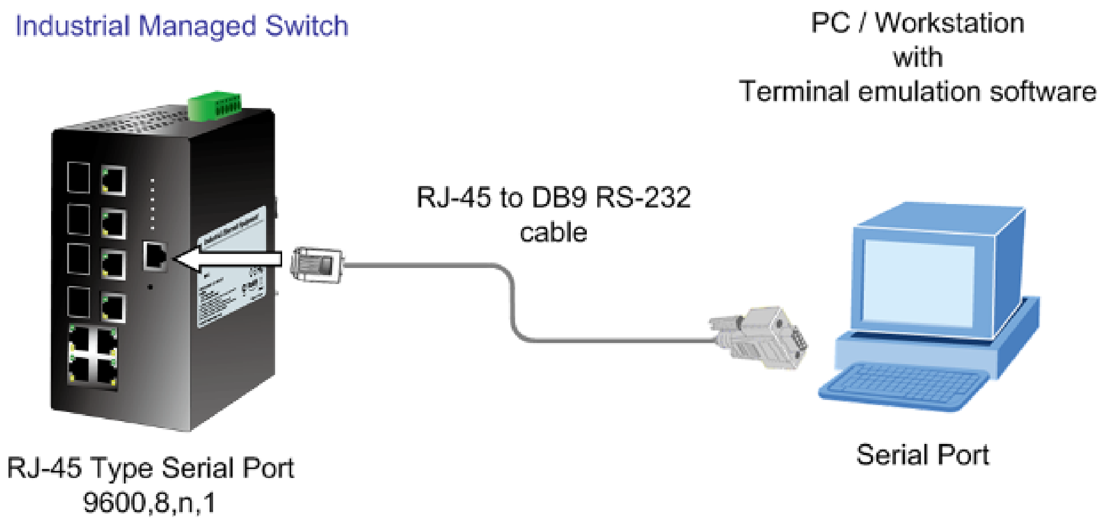

Industrial Managed Switch
PC / Workstation with Terminal emulation software
RJ-45 to DB9 RS-232 cable
RJ-45 Type Serial Port 9600,8,n,1
Serial Port

Figure 4-2 Console management connection

A terminal program is required to make the software connection to the ISW Managed Industrial Switch. Windows' **Hyper Terminal** program may be a good choice. The Hyper Terminal can be accessed from the **Start** menu.

1. Click **START**, then **Programs**, **Accessories** and then **Hyper Terminal**.

2. When the following screen appears, make sure that the COM port should be configured as:

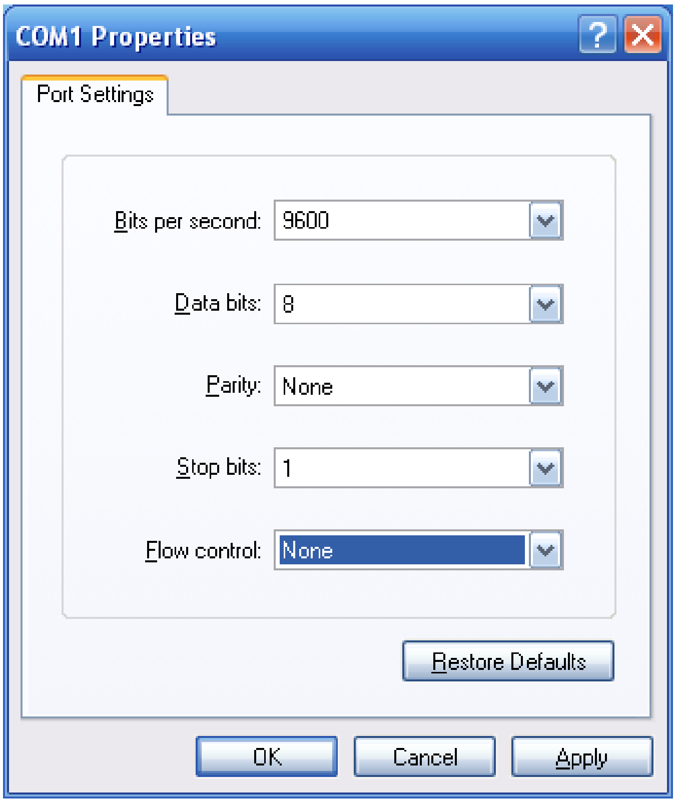
Baud Rate: 9600 bps

Data Bits: 8

Parity: none

Stop Bit: 1

Flow control: None



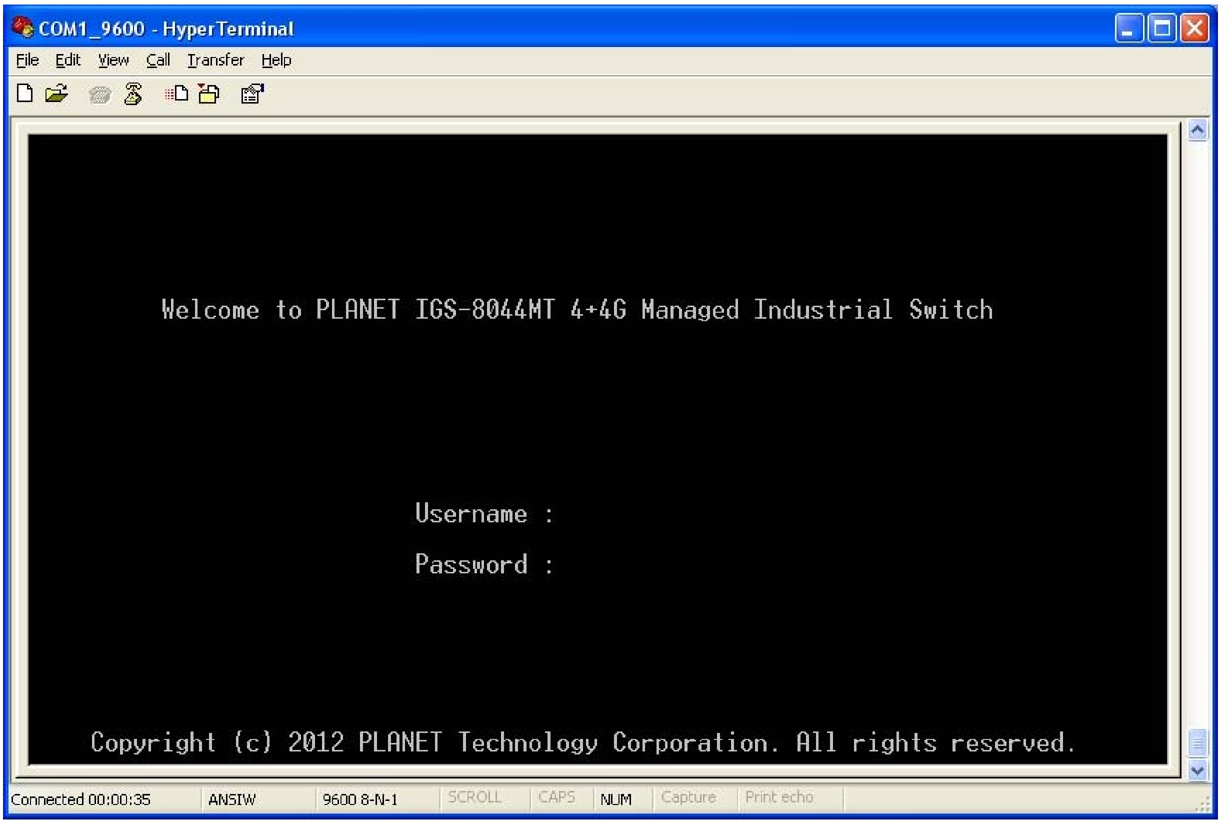
Bits per second: 9600
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None

Figure 4-3 The settings of communication parameters

Once the terminal has connected to the device, power on the ISW Managed Industrial Switch, the terminal will display that it is running testing procedures.

Then, the following message asks the login password. The factory default password as following and the login screen in below figure appears.

User name: **admin**
Password: **admin**



```
Welcome to PLANET IGS-8044MT 4+4G Managed Industrial Switch

                  Username :
                  Password :

Copyright (c) 2012 PLANET Technology Corporation. All rights reserved.
```

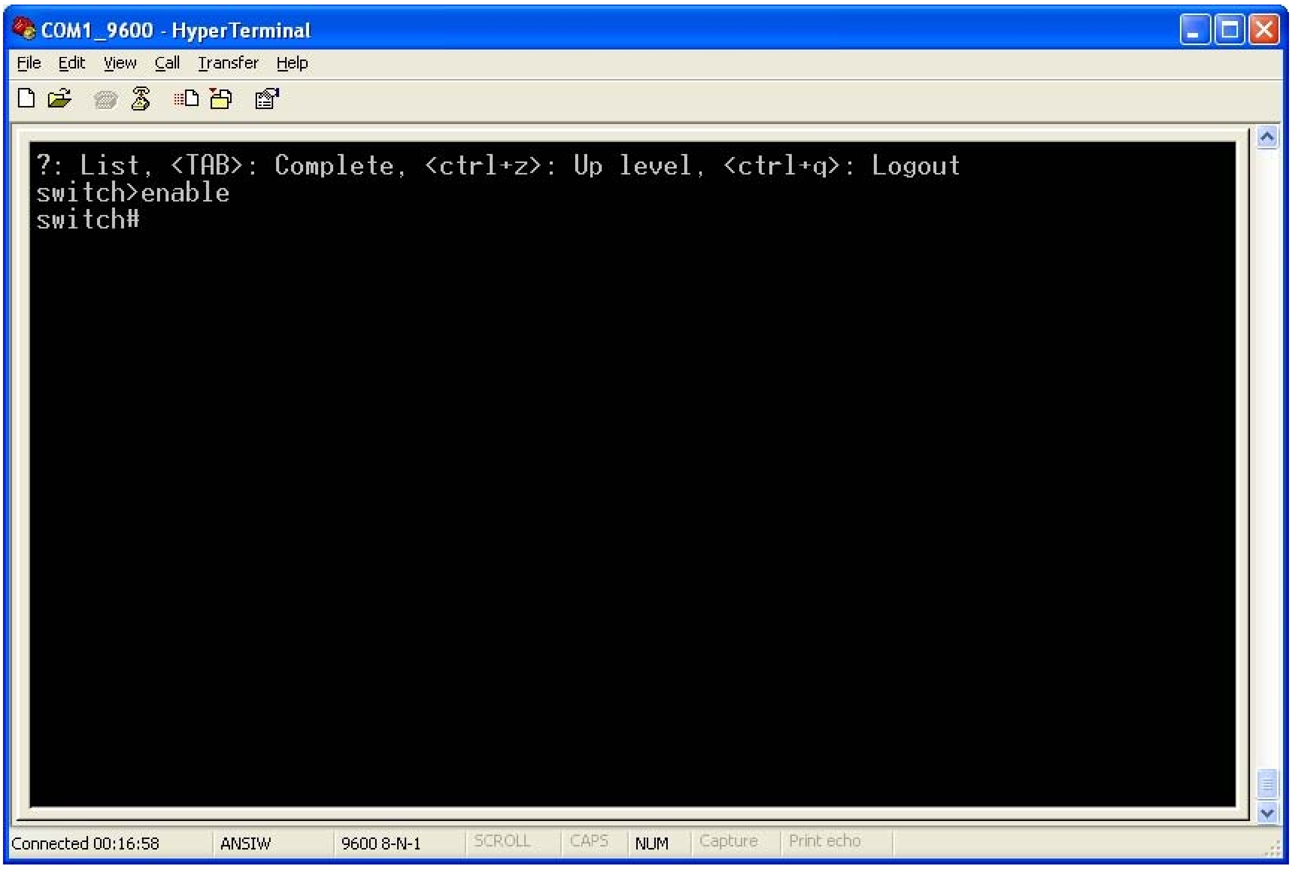
Figure 4-4 Console login interface

Note

1. For security reason, please change and memorize the new password after this first setup.
2. Only accept command in lowercase letter under console 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.



```
?: List, <TAB>: Complete, <ctrl+z>: Up level, <ctrl+q>: Logout
switch>enable
switch#
```

Figure 4-5 CLI command interface

The following table lists the CLI commands and description.

4.5 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.	Use this mode to configure parameters for the switch and Ethernet ports.

5. Web-Based Management

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

5.1 About Web-based Management

The Managed Industrial Switch offers management features that allow users to manage the Managed Industrial Switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

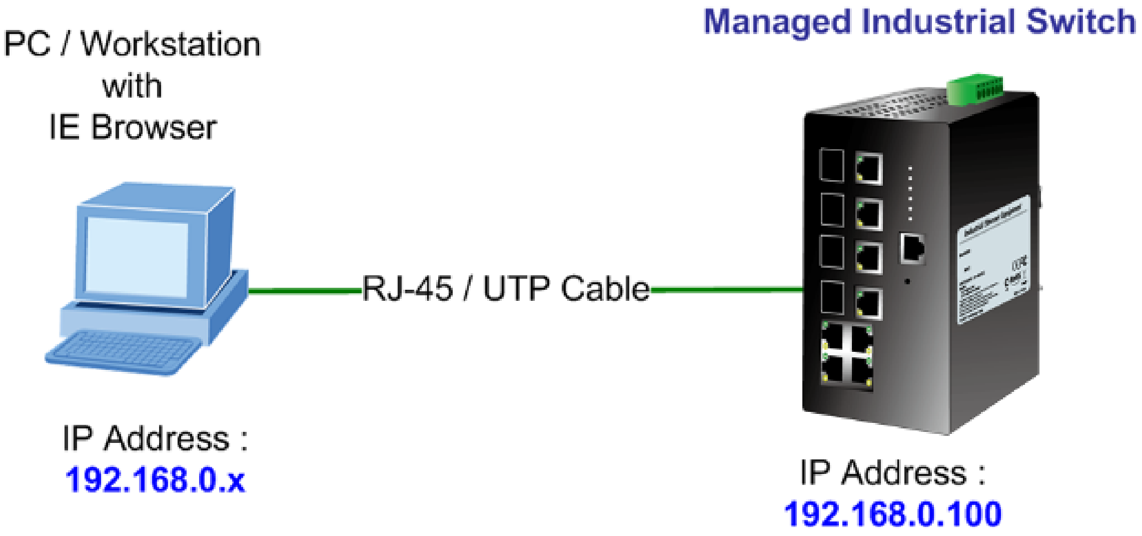
The Web-Based Management supports Internet Explorer 6.0 or above. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

Note: By default, IE6.0 or later version does not allow Java Applets to open sockets. The user has to explicitly modify the browser setting to enable Java Applets to use network ports.

The Managed Industrial Switch can be configured through an Ethernet connection, make sure the manager PC must be set on same the IP subnet address with the Managed Industrial Switch.

For example, the default IP address of the Managed Industrial Switch is ***192.168.0.100***, then the manager PC should be set at **192.168.0.x** (where x is a number between 1 and 254, except 100), and the default subnet mask is 255.255.255.0.

If you have changed the default IP address of the Managed Industrial Switch to 192.168.1.1 with subnet mask 255.255.255.0 via console, then the manager PC should be set at 192.168.1.x (where x is a number between 2 and 254) to do the relative configuration on manager PC.



5.2 Requirements

- Workstations of subscribers running Windows 98/ME, NT4.0, 2000/2003/XP, MAC OS9 or later, Linux, UNIX or other platform compatible with TCP/IP protocols.
- Workstation installed with Ethernet NIC (Network Card)
- **Ethernet Port connect**
  - ➢ Network cables - Use standard network (UTP) cables with RJ45 connectors.
  - ➢ Above PC installed with WEB Browser and JAVA runtime environment Plug-in

Note

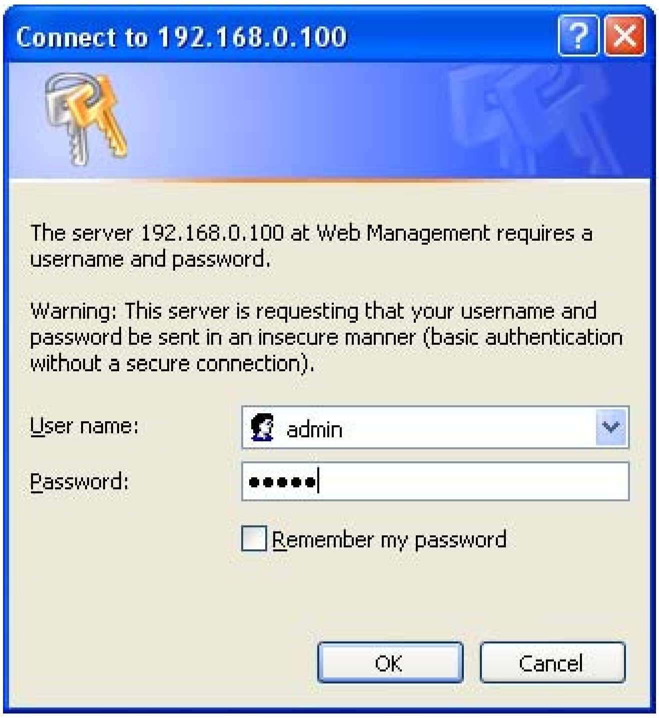
It is recommended to use Internet Explore 6.0 or above to access IGS-8044MT Managed Industrial Switch.

5.3 Logging on the switch

1. Use Internet Explorer 6.0 or above Web browser. Enter the factory-default IP address to access the Web interface. The factory-default IP Address as following:

http://192.168.0.100

2. When the following login screen appears, please enter the default username **"admin"** with password "**admin**" (or the username/password you have changed via console) to login the main screen of Managed Industrial Switch. The login screen in Figure 5-1 appears.



Connect to 192.168.0.100

The server 192.168.0.100 at Web Management requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name: admin

Password: •••••

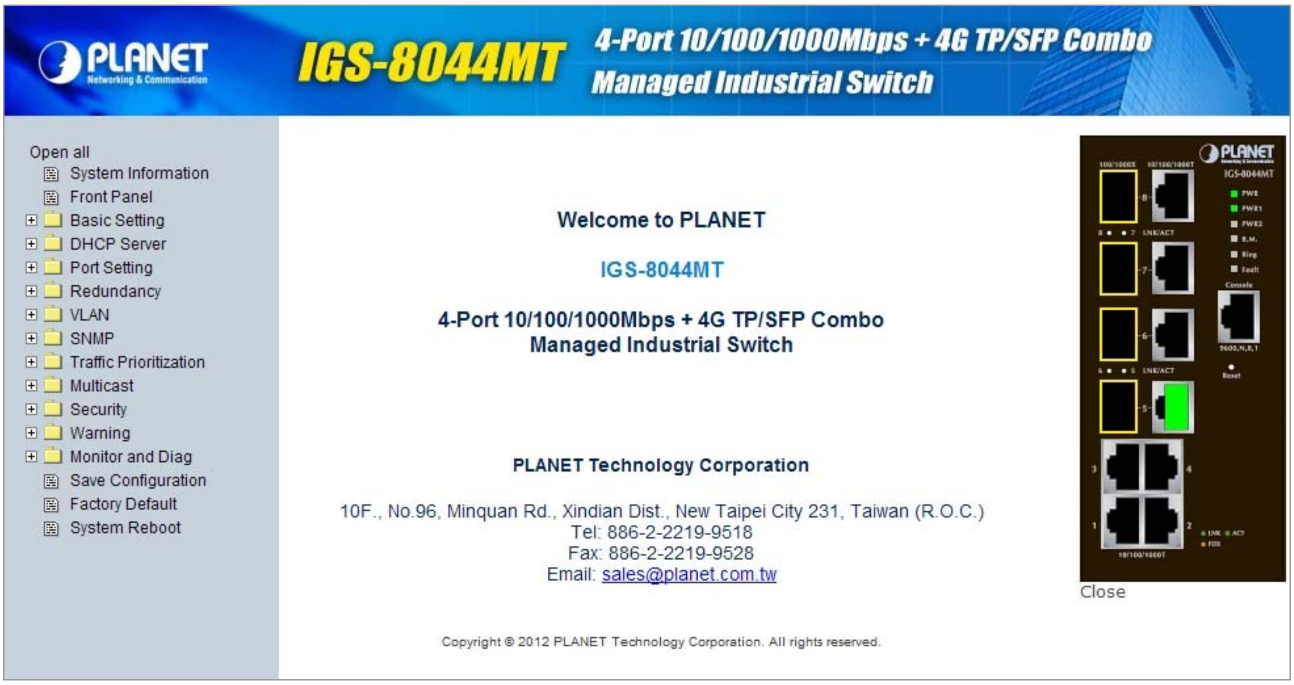
□ Remember my password

Figure 5-1 Login screen

Default User name: **admin**

Default Password: **admin**

3. After entering the username and password, the main screen appears as Figure 5-2.



Welcome to PLANET

IGS-8044MT

4-Port 10/100/1000Mbps + 4G TP/SFP Combo
Managed Industrial Switch

PLANET Technology Corporation

10F., No.96, Minquan Rd., Xindian Dist., New Taipei City 231, Taiwan (R.O.C.)
Tel: 886-2-2219-9518
Fax: 886-2-2219-9528
Email: sales@planet.com.tw

Copyright © 2012 PLANET Technology Corporation. All rights reserved.

Figure 5-2 Default main page

4. The Switch Menu on the left of the Web page let you access all the commands and statistics the Switch provides.

Now, you can use the Web management interface to continue the switch management or manage the Managed Industrial Switch by Web interface. The Switch Menu on the left of the web page let you access all the commands and statistics the Managed Industrial Switch provides.

Note

1. It is recommended to use Internet Explore 6.0 or above to access Managed Industrial Switch.
2. The changed IP address take effect immediately after click on the **Save** button, you need to use the new IP address to access the Web interface.
3. For security reason, please change and memorize the new password after this first setup.
4. Only accept command in lowercase letter under web interface.

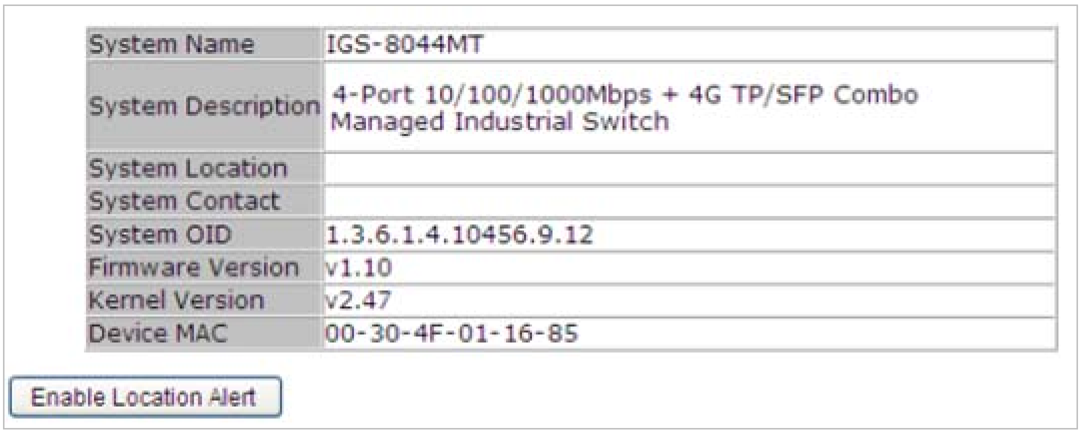
5.4 System

Use the System menu items to display and configure basic administrative details of the Managed Industrial Switch. Under System the following topics are provided to configure and view the system information: This section has the following items:

- **System Information** Provides basic system description, including contact information
- **Front Panel** To display switch front panel on the screen and indicates system LED and ports displaying.
- **Switch Setting** Allows user to input system location and system contact.
- **Admin Password** Allows user to change user name and password.
- **IP Setting** Allows user to set the IP address for management access or configures the switch to be DHCP client and get IP address from DHCP server.
- **SNTP (Time)** Allows user to set the switch correct system time from Internet via SNTP server.
- **LLDP** Allows user to enable LLDP function and advertises its information to other nodes on the network, and store the information it discovers.
- **Auto Provision** Allows user can make sure user configuration data and firmware image file is the newest version automatically from Server.
- **Backup & Restore** Allows user backup or restore IGS-8044MT configuration via TFTP server.
- **Upgrade Firmware** Allows user to upgrade firmware of IGS-8044MT from TFTP server to system.
- **Save Configuration** Allows user to save system configuration in flash memory of IGS-8044MT. If user doesn't save configuration, the current system configuration will be lost after reboot or after power recycle.
- **Factory Default** Reset the configuration of the Managed Industrial Switch
- **System Reboot** Restarts the switch

5.4.1 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. Please see Figure 5-3 as following.



System Name	IGS-8044MT
System Description	4-Port 10/100/1000Mbps + 4G TP/SFP Combo Managed Industrial Switch
System Location	
System Contact	
System OID	1.3.6.1.4.10456.9.12
Firmware Version	v1.10
Kernel Version	v2.47
Device MAC	00-30-4F-01-16-85

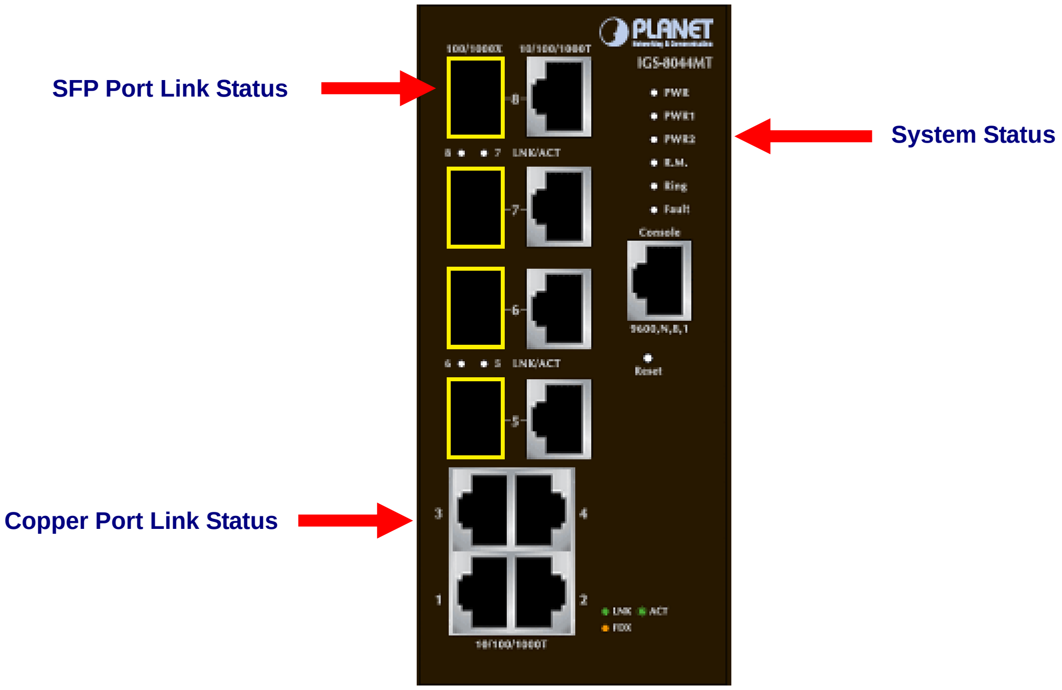
Figure 5-3 Switch settings interface

The page includes the following fields:

Object	Description
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	Displays the system SNMP object identifier.
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 (default)
Enable Location Alert Button	For user identify the device location. System LED is going to flash and indicates which device is using now.

5.4.2 Front Panel

As default value, the front panel will be activated on the WEB UI. On the front panel, it will be showed a green icon on the port which the port has been established connection. User can close or enable front panel from WEB UI in any time.



Front Panel of IGS-8044MT

Panel Display

The web agent displays an image of the Managed Industrial Switch's ports. The Mode can be set to display different information for the ports, including Link up or Link down. Clicking on the image of a port opens the **Port Statistics** page. The port states are illustrated as follows:

State	Down	Link
RJ-45 Ports	■	🟩
SFP Ports	■	🟩

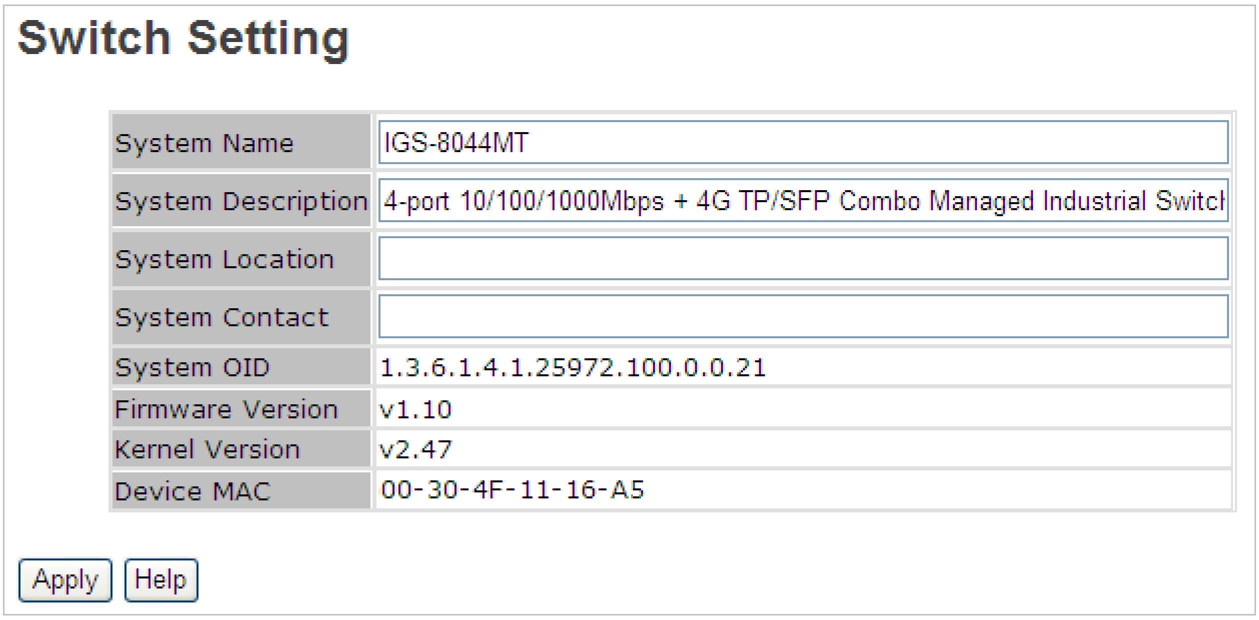
Main Menu

Using the onboard web agent, you can define system parameters, manage and control the Managed Industrial Switch, and all its ports, or monitor network conditions. Via the Web-Management, the administrator can setup the Managed Industrial Switch by select the functions those listed in the Main Function.

5.4.3 Basic Setting

5.4.3.1 Switch Setting

The Switch Setting allows user to custom System Name, System Description, System Location and System Contact information. As the other information is for software definition, user can't change it. Please see Figure 5-4 as following.



Switch Setting

System Name	IGS-8044MT
System Description	4-port 10/100/1000Mbps + 4G TP/SFP Combo Managed Industrial Switcl
System Location	
System Contact	
System OID	1.3.6.1.4.1.25972.100.0.0.21
Firmware Version	v1.10
Kernel Version	v2.47
Device MAC	00-30-4F-11-16-A5

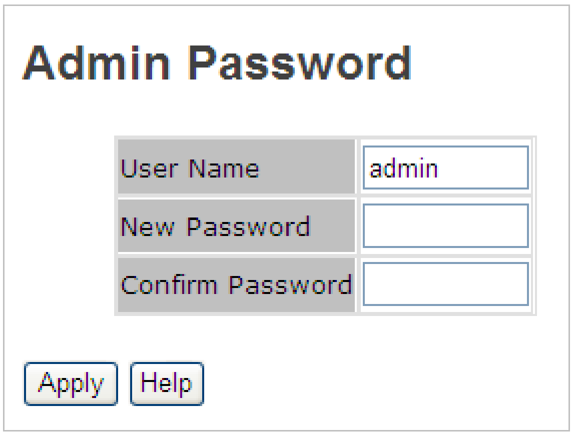
Figure 5-4 Switch Setting configuration interface

The page includes the following fields:

Object	Description
System Name	Assign the name of switch. The maximum length is 64 bytes
System Description	Display the description of 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	Display the switch's firmware version
Kernel Version	Display the kernel software version
MAC Address	Display the unique hardware address assigned by manufacturer (default)
Help	Show help file.

5.4.3.2 Admin Password

Change web management login username and password for the management security issue. Please see Figure 5-5 as following.



Admin Password

User Name	admin
New Password	
Confirm Password	

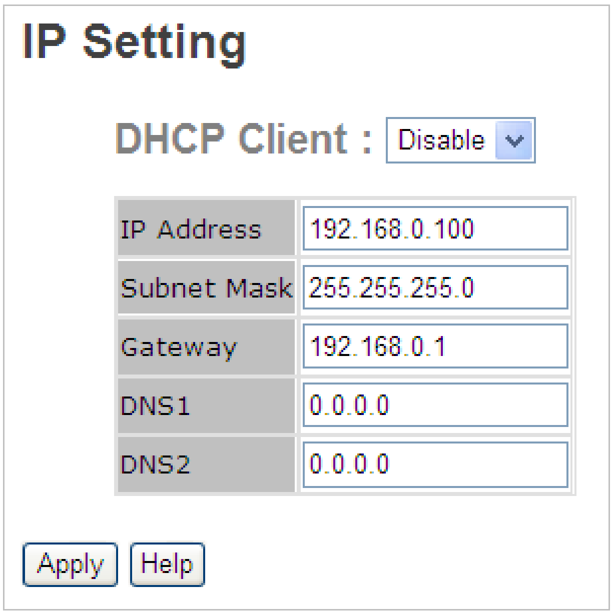
Figure 5-5 Admin Password configuration interface

The page includes the following fields:

Object	Description
User name	Key in the new username(The default is "**admin**")
New Password	Key in the new password(The default is "**admin**")
Confirm password	Re-type the new password.
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

5.4.3.3 IP Setting

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. Please see Figure 5-6 as following.



IP Setting

DHCP Client : Disable

IP Address	192.168.0.100
Subnet Mask	255.255.255.0
Gateway	192.168.0.1
DNS1	0.0.0.0
DNS2	0.0.0.0

Figure 5-6 IP Setting interface

The page includes the following fields:

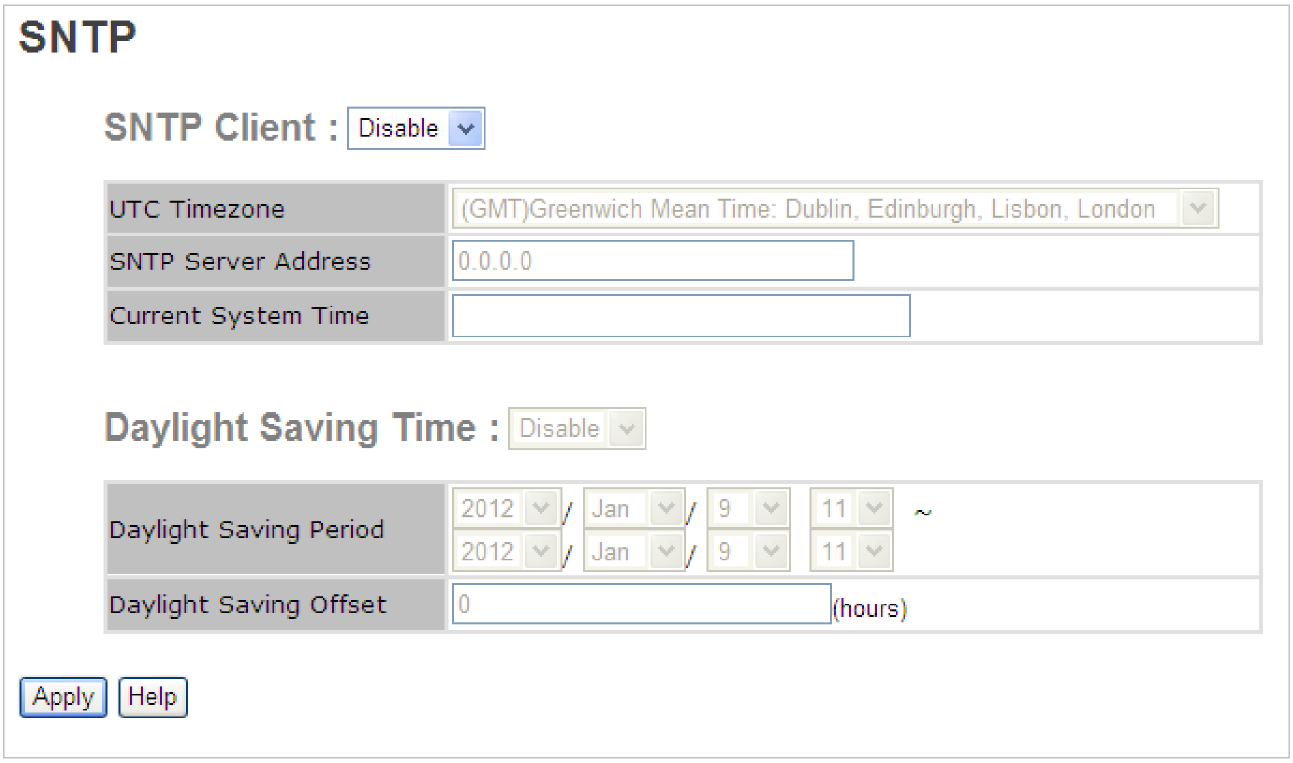
Object	Description
DHCP Client:	Enable or disable the DHCP client function. When DHCP client function is enabled, the switch will be assigned an IP address from the network DHCP server. The default IP address will be replaced by the assigned IP address on DHCP server. After the user clicks Apply, a popup 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 **192.168.0.100** 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 **192.168.0.1**.
DNS1:	Assign the primary DNS IP address.

DNS2:	Assign the secondary DNS IP address.
Apply	Click "**Apply**" to set the configurations
Help	Show help file.

5.4.3.4 SNTP (Time)

The SNTP (Simple Network Time Protocol) settings allow you to synchronize switch clocks in the Internet.

Please see Figure 5-7 as following.



SNTP

SNTP Client : Disable

UTC Timezone	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
SNTP Server Address	0.0.0.0
Current System Time	

Daylight Saving Time : Disable

Daylight Saving Period	2012 / Jan / 9 11 ~ 2012 / Jan / 9 11
Daylight Saving Offset	0 (hours)

Figure 5-7 SNTP configuration interface

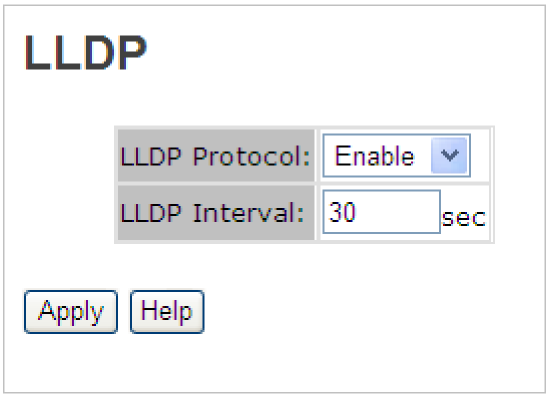
The page includes the following fields:

Object	Description
SNTP Client	Enable or disable SNTP function to get the time from the SNTP server.
UTC Time zone	Set the switch location time zone. The following table lists the different location time zone for your reference.
SNTP Sever IP Address	Set the SNTP server IP address.
Current System Time	Display the switch current time.
Daylight Saving Period	Set up the Daylight Saving beginning time and Daylight Saving ending time. Both will be different each year.

Daylight Saving Offset	Set up the offset time.
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

5.4.3.5 LLDP

LLDP (Link Layer Discovery Protocol) function allows the switch to advertise its information to other nodes on the network and store the information it discovers. Please see Figure 5-8 as following.



LLDP

LLDP Protocol: Enable

LLDP Interval: 30 sec

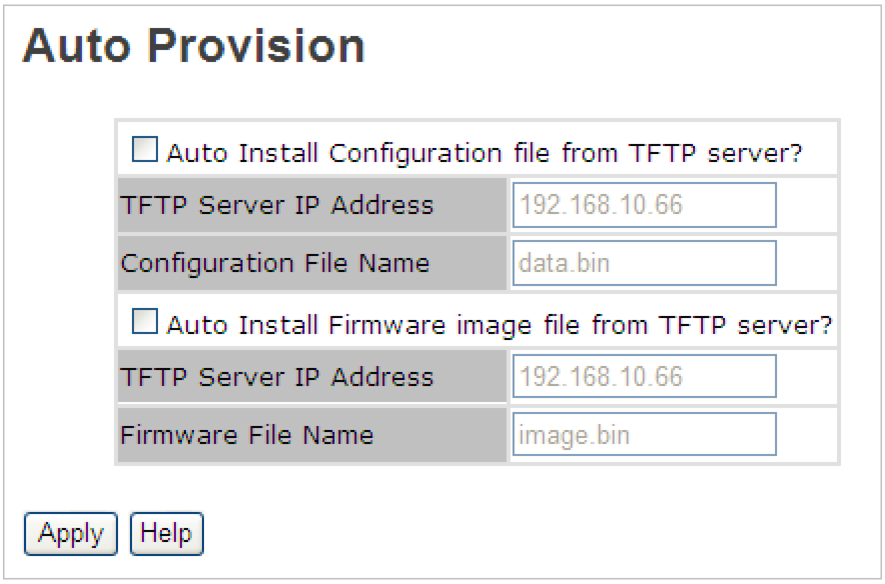
Figure 5-8 LLDP configuration interface

The page includes the following fields:

Object	Description
LLDP Protocol	"**Enable**" or "**Disable**" LLDP function.
LLDP Interval	The interval of resend LLDP (by default at 30 seconds)
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.4.3.6 Auto Provision

Auto Provision allows you to update the switch firmware automatically. You can put firmware or configuration file on TFTP server. When you reboot the switch, it will upgrade automatically. Before updating, make sure you have your TFTP server ready and the firmware image and configuration file is on the TFTP server. Please see Figure 5-9 as following.



Auto Provision

□ Auto Install Configuration file from TFTP server?	
TFTP Server IP Address	192.168.10.66
Configuration File Name	data.bin
□ Auto Install Firmware image file from TFTP server?	
TFTP Server IP Address	192.168.10.66
Firmware File Name	image.bin

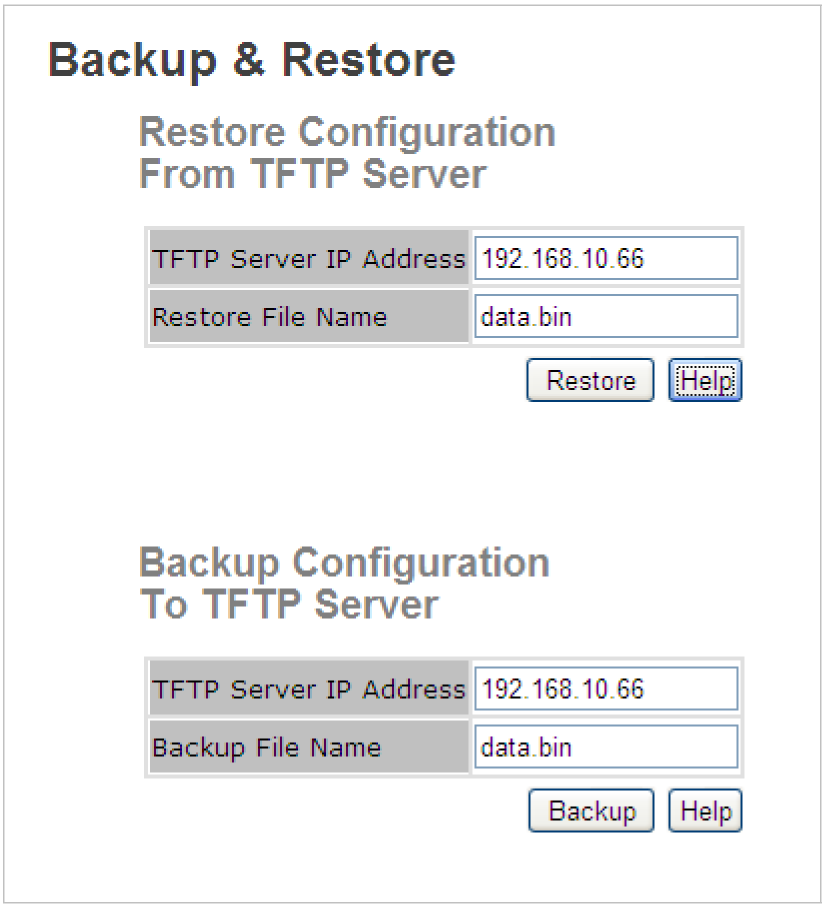
Figure 5-9 Auto Provision configuration interface

The page includes the following fields:

Object	Description
TFTP Server IP Address	Allows user to input TFTP Server IP address.
Configuration File Name	Allows user to input configuration file which backup it before.
Firmware File Name	Allows user to input firmware file name.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.4.3.7 Backup & Restore

You can back up the IGS-8044MT 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. Also, 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 Managed Industrial Switch will download back the flash image. Please see Figure 5-10 as following.



Backup & Restore

Restore Configuration From TFTP Server

TFTP Server IP Address	192.168.10.66
Restore File Name	data.bin

Backup Configuration To TFTP Server

TFTP Server IP Address	192.168.10.66
Backup File Name	data.bin

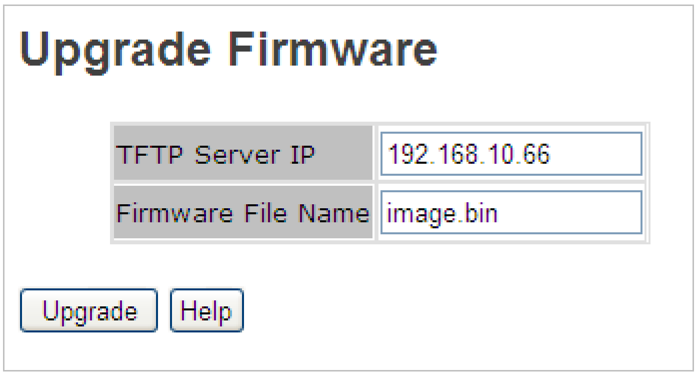
Figure 5-10 Backup & Restore configuration interface

The page includes the following fields:

Object	Description
TFTP Server IP Address	Allows user to input TFTP Server IP address.
Restore File Name	Allows user to input file name to restore switch configuration.
Backup File Name	Allows user to input file name to backup switch configuration.
Restore	Click “**Restore**” to activate the configurations.
Backup	Click “**Backup**” to activate the configurations.
Help	Show help file.

5.4.3.8 Upgrade Firmware

Upgrade Firmware allows you to update the switch firmware. Before updating, make sure you have your TFTP server ready and the firmware image is on the TFTP server. Please see Figure 5-11 as following.



Upgrade Firmware

TFTP Server IP: 192.168.10.66

Firmware File Name: image.bin

Figure 5-11 Upgrade Firmware configuration interface

The page includes the following fields:

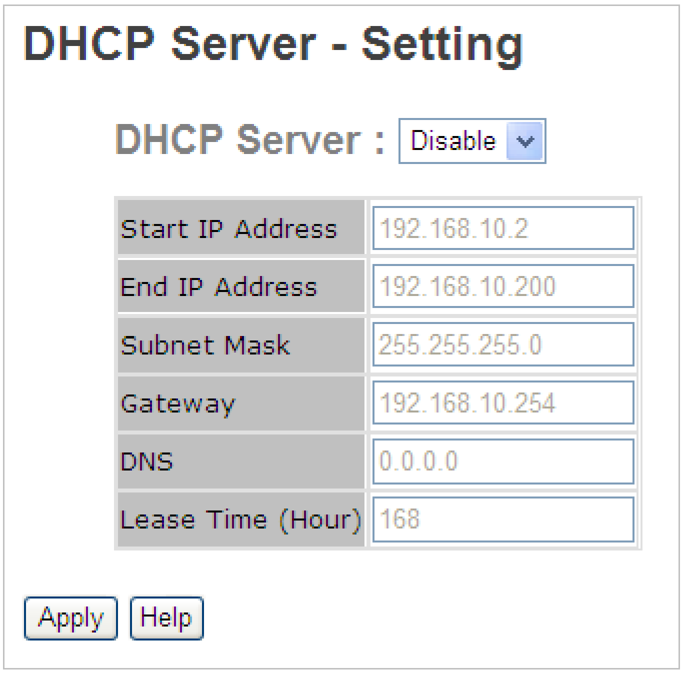
Object	Description
TFTP Server IP	Allows user to input TFTP server IP address.
Firmware File Name	Allows user to input firmware file name.
Upgrade	Click "**Upgrade**" to activate the configurations.
Help	Show help file.

5.4.4 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.

5.4.4.1 DHCP Server - Setting

The system provides the DHCP server function. Having enabled the DHCP server function, the switch system will be configured as a DHCP server. Please see Figure 5-12 as following.



DHCP Server - Setting

DHCP Server : Disable

Start IP Address	192.168.10.2
End IP Address	192.168.10.200
Subnet Mask	255.255.255.0
Gateway	192.168.10.254
DNS	0.0.0.0
Lease Time (Hour)	168

Figure 5-12 DHCP Server Configuration interface

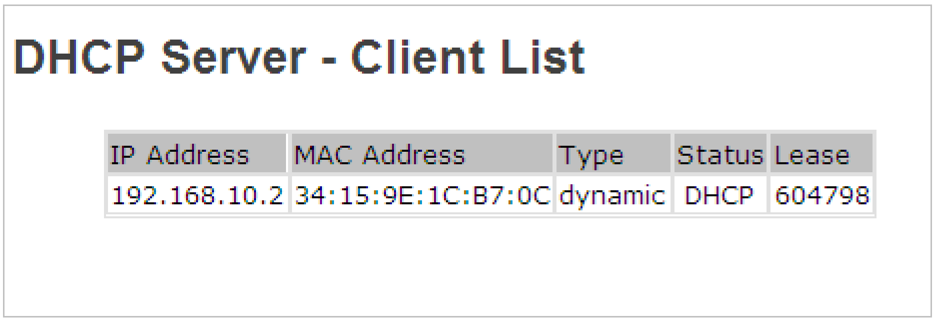
The page includes the following fields:

Object	Description
DHCP Server:	Enable or Disable the DHCP Server function. Enable—the switch will be the DHCP server on your local network.
Start IP Address:	Type in an IP address. Start IP address is the beginning of the dynamic IP range. For example, dynamic IP is in the range between 192.168.0.101 ~ 192.168.0.200. In contrast, **192.168.0.101** is the Start IP address.
End IP Address:	Type in an IP address. End IP address is the end of the dynamic IP range. For example, dynamic IP is in the range between 192.168.0.101 ~ 192.168.0.200. In contrast, **192.168.0.200** is the End 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.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.4.4.2 Client List

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. Please see Figure 5-13 as following.



DHCP Server - Client List

IP Address	MAC Address	Type	Status	Lease
192.168.10.2	34:15:9E:1C:B7:0C	dynamic	DHCP	604798

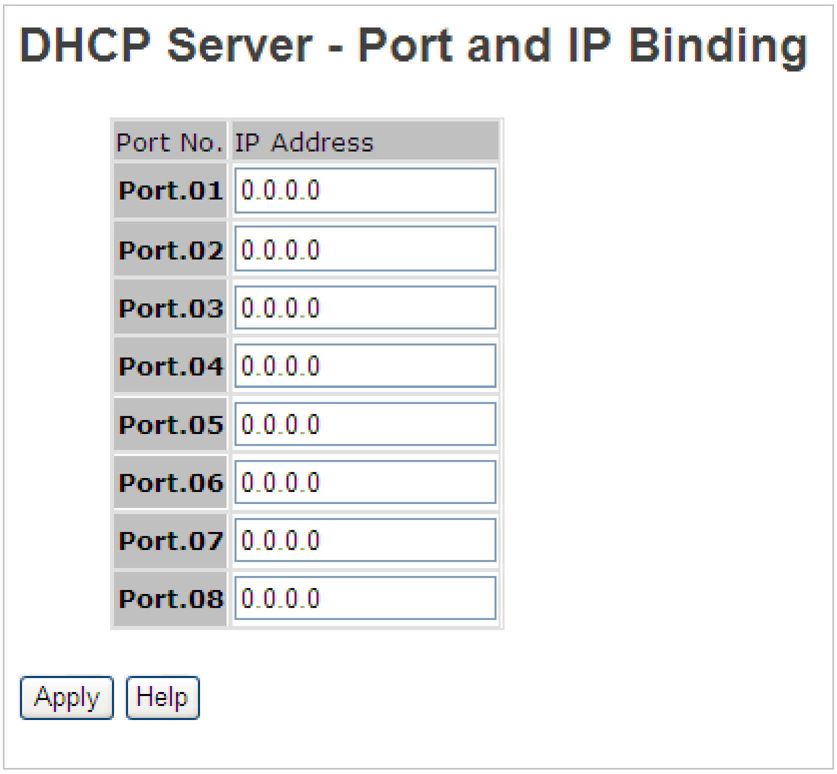
Figure 5-13 Client List Configuration interface

The page includes the following fields:

Object	Description
IP Address	Specifies the Client's IP Address.
MAC Address	Specifies the Client's Hardware Address.
Type	Specifies the Type of Binding: Dynamic / Manual.
Status	Shows the device current status.
Lease	Specifies the Lease time left in seconds.

5.4.4.3 DHCP Server – Port and IP Binding

You can assign the specific IP address which is in the assigned dynamic IP range to the specific port. When the device is connecting to the port and asks for dynamic IP assigning, the system will assign the IP address that has been assigned before in the connected device. Please see Figure 5-14 as following.



DHCP Server - Port and IP Binding

Port No.	IP Address
Port.01	0.0.0.0
Port.02	0.0.0.0
Port.03	0.0.0.0
Port.04	0.0.0.0
Port.05	0.0.0.0
Port.06	0.0.0.0
Port.07	0.0.0.0
Port.08	0.0.0.0

Figure 5-14 Port and IP Binding Configuration interface

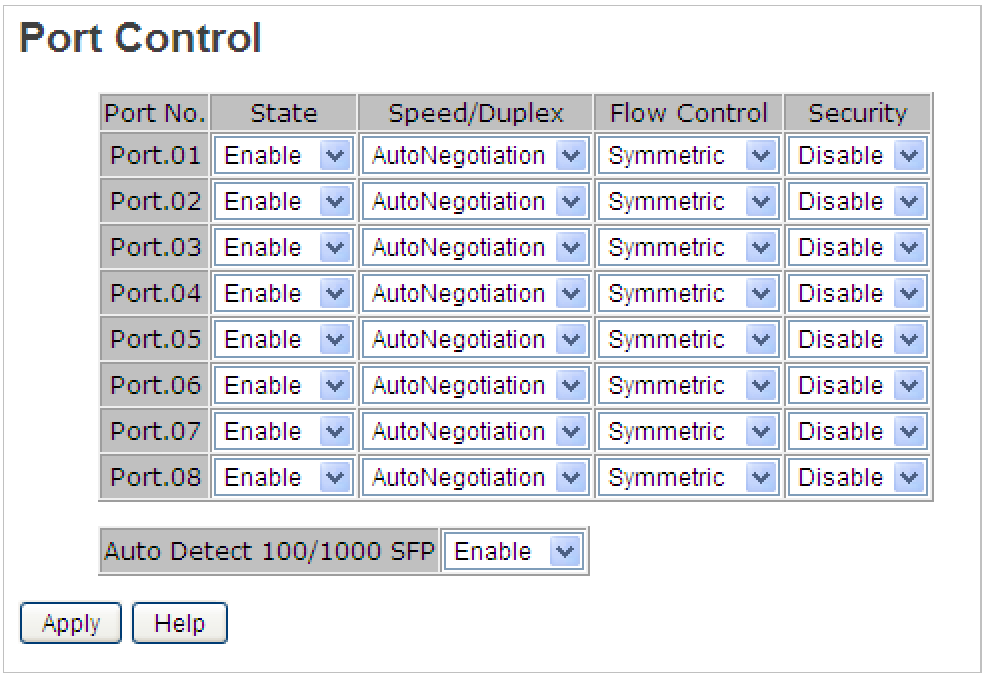
The page includes the following fields:

Object	Description
IP Address	Specifies the Client's IP Address.
Port.01~Port.08	Totally eight ports for specifying IP address.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.4.5 Port Setting

5.4.5.1 Port Control

Port Control function allows user to sett the state, speed/duplex, flow control, and security to the port. Please see Figure 5-15 as following.



Port Control

Port No.	State	Speed/Duplex	Flow Control	Security
Port.01	Enable	AutoNegotiation	Symmetric	Disable
Port.02	Enable	AutoNegotiation	Symmetric	Disable
Port.03	Enable	AutoNegotiation	Symmetric	Disable
Port.04	Enable	AutoNegotiation	Symmetric	Disable
Port.05	Enable	AutoNegotiation	Symmetric	Disable
Port.06	Enable	AutoNegotiation	Symmetric	Disable
Port.07	Enable	AutoNegotiation	Symmetric	Disable
Port.08	Enable	AutoNegotiation	Symmetric	Disable

Auto Detect 100/1000 SFP: Enable

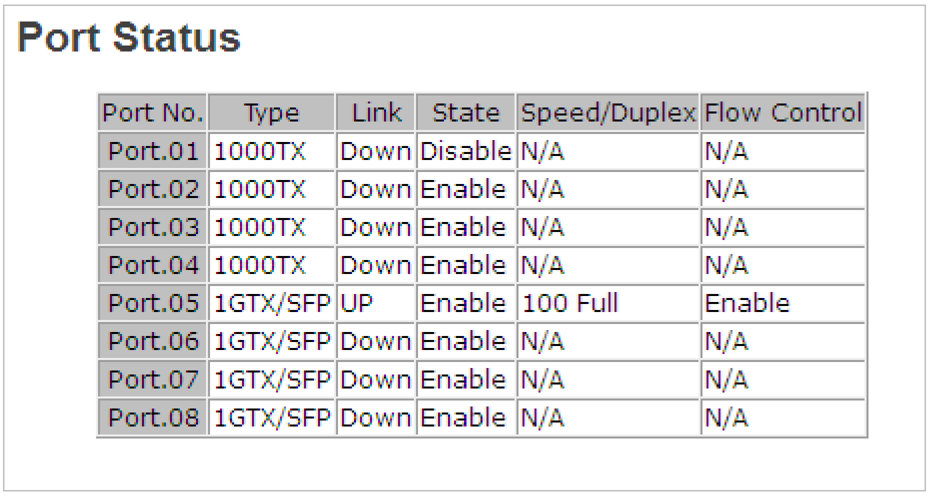
Figure 5-15 Port and IP Binding Configuration interface

The page includes the following fields:

Object	Description
Port No.	Port number for setting.
State	Enable or Disable port transmission.
Speed/ Duplex	Allows user to set Auto-negotiation, 100 full, 100 half, 10 full, 10 half mode.
Flow Control	Allows user to set symmetric or asymmetric mode to avoid packet loss when congestion occurred.
Security	Allows user to set port security function. When enable the function, the port will STOP learning MAC address dynamically.
Auto Detect 100/1000 SFP	Detects SFP Module to 100/1000Mbs automatically.
Apply	Click "**Apply**" to set the configurations.
Help	Shows HELP file.

5.4.5.2 Port Status

Port Status information provides the current port status information. Please see Figure 5-16 as following.



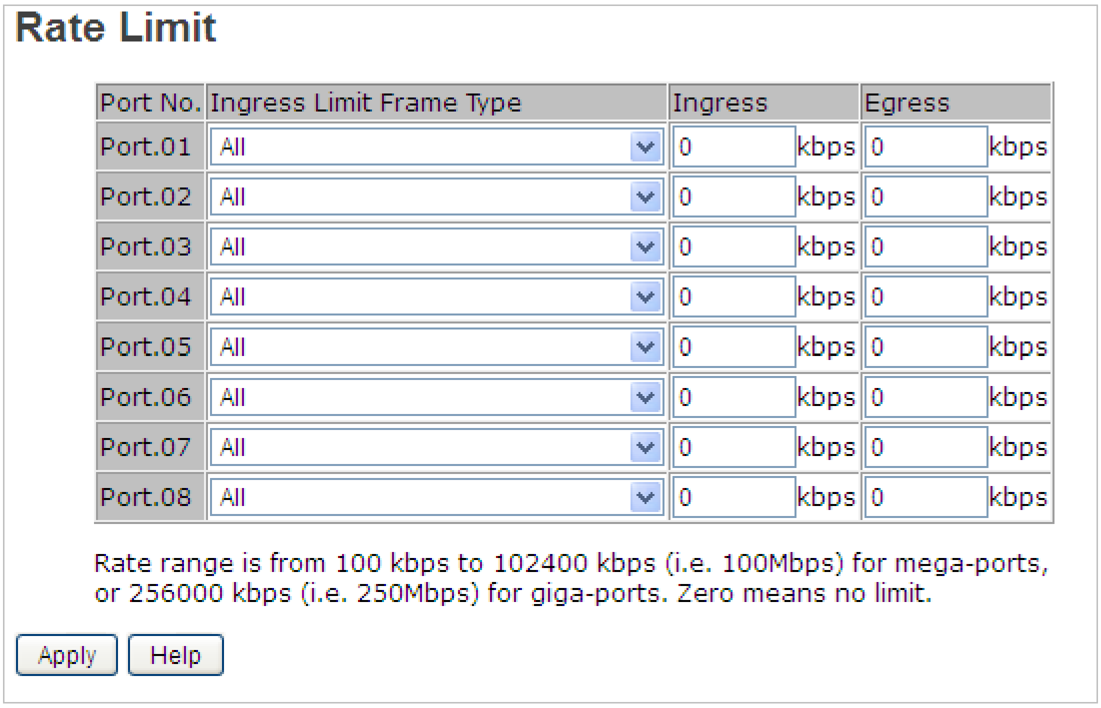
Port Status

Port No.	Type	Link	State	Speed/Duplex	Flow Control
Port.01	1000TX	Down	Disable	N/A	N/A
Port.02	1000TX	Down	Enable	N/A	N/A
Port.03	1000TX	Down	Enable	N/A	N/A
Port.04	1000TX	Down	Enable	N/A	N/A
Port.05	1GTX/SFP	UP	Enable	100 Full	Enable
Port.06	1GTX/SFP	Down	Enable	N/A	N/A
Port.07	1GTX/SFP	Down	Enable	N/A	N/A
Port.08	1GTX/SFP	Down	Enable	N/A	N/A

Figure 5-16 Port Status

5.4.5.3 Rate Limit

Rate Limit function allows user to set traffic limitation of all ports, including broadcast, multicast and flooded unicast. You can also set "Ingress" or "Egress" to limit traffic received or transmitted bandwidth. Please see Figure 5-17 as following.



Rate Limit

Port No.	Ingress Limit Frame Type	Ingress	Egress
Port.01	All	0 kbps	0 kbps
Port.02	All	0 kbps	0 kbps
Port.03	All	0 kbps	0 kbps
Port.04	All	0 kbps	0 kbps
Port.05	All	0 kbps	0 kbps
Port.06	All	0 kbps	0 kbps
Port.07	All	0 kbps	0 kbps
Port.08	All	0 kbps	0 kbps

Rate range is from 100 kbps to 102400 kbps (i.e. 100Mbps) for mega-ports, or 256000 kbps (i.e. 250Mbps) for giga-ports. Zero means no limit.

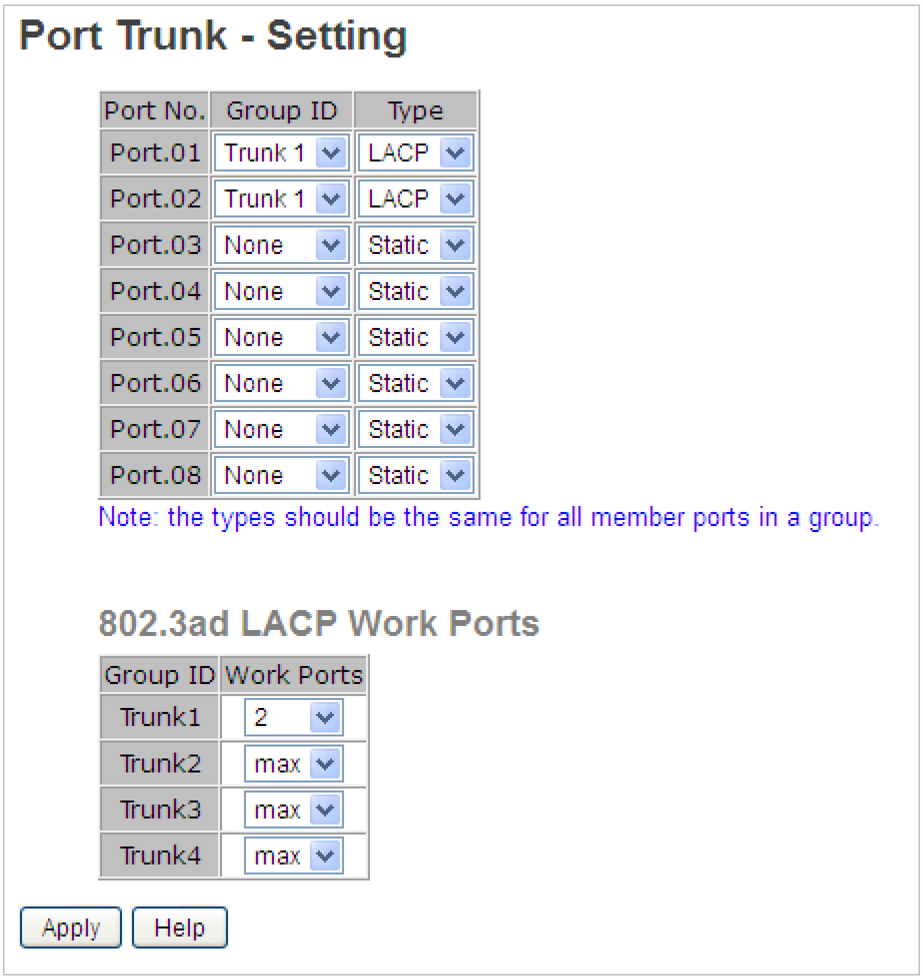
Figure 5-17 Rate Limit Configuration interface

The page includes the following fields:

Object	Description
Ingress Limit Frame Type	Allows user to set "all", "Broadcast only","Broadcast/Multicast" or"Broadcast/Multicast/Flooded Unicast" mode. These 4 types are only for ingress packet. The egress rate only support all types packet.
Ingress	The switch port received traffic.
Egress	The switch port transmitted traffic.
Apply	Click "**Apply**" to set the configurations.
Help	Shows HELP file.

5.4.5.4 Port Trunk

Port Trunk Setting allows user to select static trunk or 802.3ad LACP to combine several physical links with a logical link to increase the bandwidth. Please see Figure 5-18 as following.



Port Trunk - Setting

Port No.	Group ID	Type
Port.01	Trunk 1	LACP
Port.02	Trunk 1	LACP
Port.03	None	Static
Port.04	None	Static
Port.05	None	Static
Port.06	None	Static
Port.07	None	Static
Port.08	None	Static

Note: the types should be the same for all member ports in a group.

802.3ad LACP Work Ports

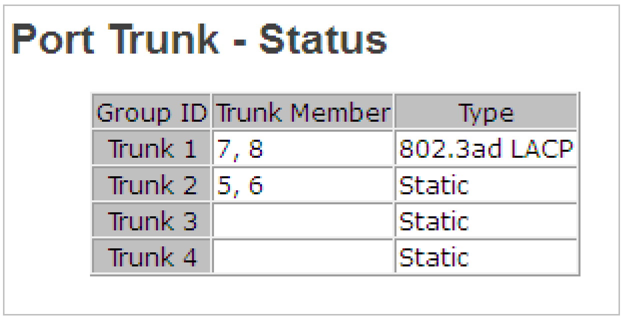
Group ID	Work Ports
Trunk1	2
Trunk2	max
Trunk3	max
Trunk4	max

Figure 5-18 Port Trunk Configuration interface

The page includes the following fields:

Object	Description
Port No.	Port number for setting.
Group ID	Select port to join a trunk group.
Type	Support static trunk and 802.3ad LACP
Works Port	Allows user to set how many port will be used with LACP port trunk. It offers 4 LACP trunk ports maximum.
Apply	Click "**Apply**" to set the configurations.
Help	Shows HELP file.

Port Trunk Status shows port trunk configuration status. User could check trunk member and type from this screen. Please see Figure 5-19 as following.



Port Trunk - Status

Group ID	Trunk Member	Type
Trunk 1	7, 8	802.3ad LACP
Trunk 2	5, 6	Static
Trunk 3		Static
Trunk 4		Static

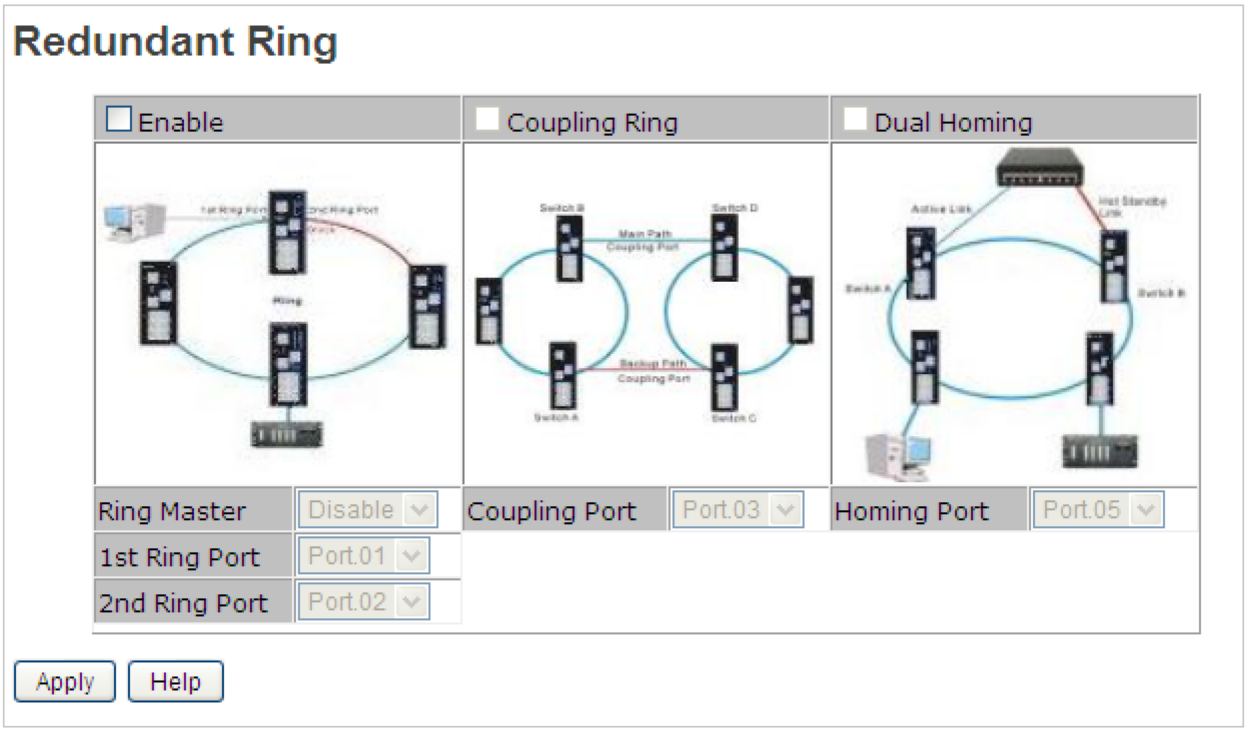
Figure 5-19 Port Trunk Status Configuration interface

5.4.6 Redundancy

5.4.6.1 Redundant Ring

Redundant 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 Ring topology, every switch should be enabled with Ring function and two ports should be assigned as the member ports in the Redundant Ring. Only one switch in the 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 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, A.K.A. R.M.**) will automatically become a working port to recover from the failure.

The IGS-8044MT supports the 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.
As Redundant Ring function as following, IGS-8044MT offers 3 types ring for user setting; they are Single Ring, Coupling Ring and Dual Homing. Please see Figure 5-20 as following



Redundant Ring

□ Enable

□ Coupling Ring

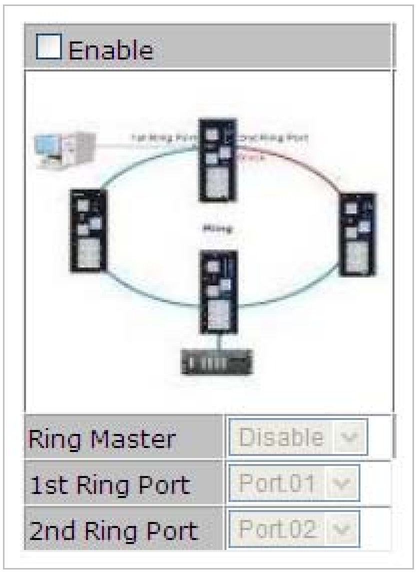
□ Dual Homing

Ring Master	Disable
1st Ring Port	Port.01
2nd Ring Port	Port.02
Coupling Port	Port.03
Homing Port	Port.05

Figure 5-20 Redundant Ring Configuration interface

Please be noted, the redundant ring doesn’t compatible with the X-Ring of ISW-1022M series model and ISW-1033MT model. If the network topology must mix to use the X-Ring model with IGS-8044MT, please disable all of redundant ring function and enable **Legacy Ring only**. However, Legacy Ring doesn’t support coupling ring and dual homing, and also can’t work with Redundant Ring together.

Firstly, let's see single Ring. Please see Figure 5-21 as following.



☐ Enable

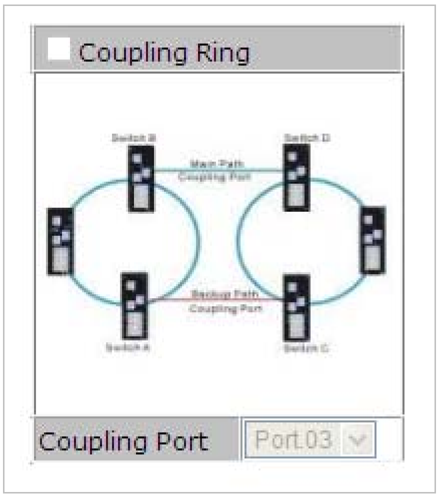
Ring Master	Disable
1st Ring Port	Port.01
2nd Ring Port	Port.02

Figure 5-21 Redundant Ring Configuration interface

The page includes the following fields:

Object	**Description**
Enable	Allows user to enable ring function.
Ring Master	Allows user to set this switch to be ring master. There should be one and only one Ring Master in a ring. However if there are two or more switches which set Ring Master to enable, the switch with the lowest MAC address will be the actual Ring Master and others will be Backup Masters.
1st Ring Port	Allows user to choose port to be 1st ring port.
2nd Ring Port	Allows user to choose port to be 2nd ring port.

In the network, it may have more than one Ring group. By using the coupling ring function, it can connect each Ring for the redundant backup. It can ensure the transmissions between two ring groups not to fail. Please see Figure 5-22 as following.



□ Coupling Ring

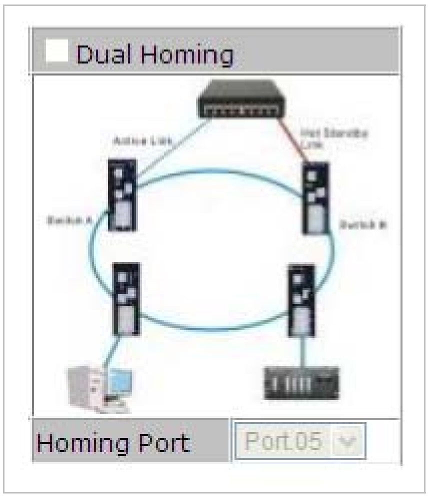
Coupling Port: Port 03

Figure 5-22 Coupling Ring Configuration interface

The page includes the following fields:

Object	Description
Coupling Ring	Allows user to enable Coupling Ring.
Coupling Port	Allows user to choose a port to be coupling port.

Dual Homing function is to prevent the connection lose from between Ring group and upper level/core switch. Assign a port to be the Dual Homing port that is backup port in the Ring group. The Dual Homing function only works when the Ring function is active. Each Ring group only has one Dual Homing port. Please see Figure 5-23 as following.



□ Dual Homing

Homing Port: Port 05

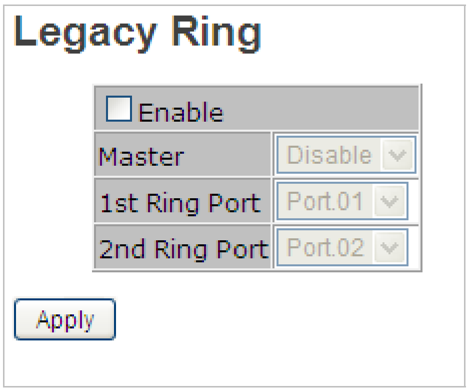
Figure 5-23 Dual Homing Configuration interface

The page includes the following fields:

Object	Description
Dual Homing	Allows user to enable Dual Homing.
Homing Port	Allows user to choose a port to be homing port.

5.4.6.2 Legacy Ring

Legacy Ring provides compatible with X-Ring of ISW-1022M / ISW-1022MT / ISW-1022MPT / ISW-1033MT. Please be noted, legacy ring works as single redundant ring, and do not co-work with coupling rig or dual homing. Please see Figure 5-24 as following.



Legacy Ring

□ Enable	
Master	Disable
1st Ring Port	Port.01
2nd Ring Port	Port.02

Figure 5-24 Legacy Ring Configuration interface

The page includes the following fields:

Object	Description
Enable	Allows user to enable Legacy Ring.
Master	Allows user enabling this switch to be a ring master.
1st Ring Port	Allows user to choose a port to be 1st ring port.
2nd Ring Port	Allows user to choose a port to be 2nd ring port.
Apply	Allows user to set configuration.

5.4.6.3 RSTP

Theory

The Spanning Tree protocol can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down. The spanning tree algorithms supported by this switch include these versions:

- **RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)**

The **Spanning Tree Protocols (STP)** allows for the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol allows for the duplicate links to be used in the event of a failure of the primary link. Once the Spanning Tree Protocol is configured and enabled, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically without operator intervention.

This automatic network reconfiguration provides maximum uptime to network users. However, the concepts of the Spanning Tree Algorithm and protocol are a complicated and complex subject and must be fully researched and understood. It is possible to cause serious degradation of the performance of the network if the Spanning Tree is incorrectly configured. Please read the following before making any changes from the default values.

The Switch STP performs the following functions:

- Creates a single spanning tree from any combination of switching or bridging elements.
- Creates multiple spanning trees – from any combination of ports contained within a single switch, in user specified groups.
- Automatically reconfigures the spanning tree to compensate for the failure, addition, or removal of any element in the tree.
- Reconfigures the spanning tree without operator intervention.

Bridge Protocol Data Units

For STP to arrive at a stable network topology, the following information is used:

- The unique switch identifier
- The path cost to the root associated with each switch port
- The port identifier

STP communicates between switches on the network using Bridge Protocol Data Units (BPDUs). Each BPDU contains the following information:

- The unique identifier of the switch that the transmitting switch currently believes is the root switch
- The path cost to the root from the transmitting port
- The port identifier of the transmitting port

The switch sends BPDUs to communicate and construct the spanning-tree topology. All switches connected to the LAN on which the packet is transmitted will receive the BPDU. BPDUs are not directly forwarded by the switch, but the receiving switch uses the information in the frame to calculate a BPDU, and, if the topology changes, initiates a BPDU transmission.

The communication between switches via BPDUs results in the following:

- One switch is elected as the root switch
- The shortest distance to the root switch is calculated for each switch
- A designated switch is selected. This is the switch closest to the root switch through which packets will be forwarded to the root.
- A port for each switch is selected. This is the port providing the best path from the switch to the root switch.
- Ports included in the STP are selected.

Creating a Stable STP Topology

It is to make the root port a fastest link. If all switches have STP enabled with default settings, the switch with the lowest MAC address in the network will become the root switch. By increasing the priority (lowering the priority number) of the best switch, STP can be forced to select the best switch as the root switch.

When STP is enabled using the default parameters, the path between source and destination stations in a switched network might not be ideal. For instance, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change.

STP Port States

The BPDUs take some time to pass through a network. This propagation delay can result in topology changes where a port that transitioned directly from a Blocking state to a Forwarding state could create temporary data loops. Ports must wait for new network topology information to propagate throughout the network before starting to forward packets. They must also wait for the packet lifetime to expire for BPDU packets that were forwarded based on the old topology. The forward delay timer is used to allow the network topology to stabilize after a topology change. In addition, STP specifies a series of states a port must transition through to further ensure that a stable network topology is created after a topology change.

Each port on a switch using STP exists is in one of the following five states:

- **Blocking** – the port is blocked from forwarding or receiving packets
- **Listening** – the port is waiting to receive BPDU packets that may tell the port to go back to the blocking state
- . **Learning** – the port is adding addresses to its forwarding database, but not yet forwarding packets
- **Forwarding** – the port is forwarding packets
- **Disabled** – the port only responds to network management messages and must return to the blocking state first

A port transitions from one state to another as follows:

- From initialization (switch boot) to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled
- From disabled to blocking

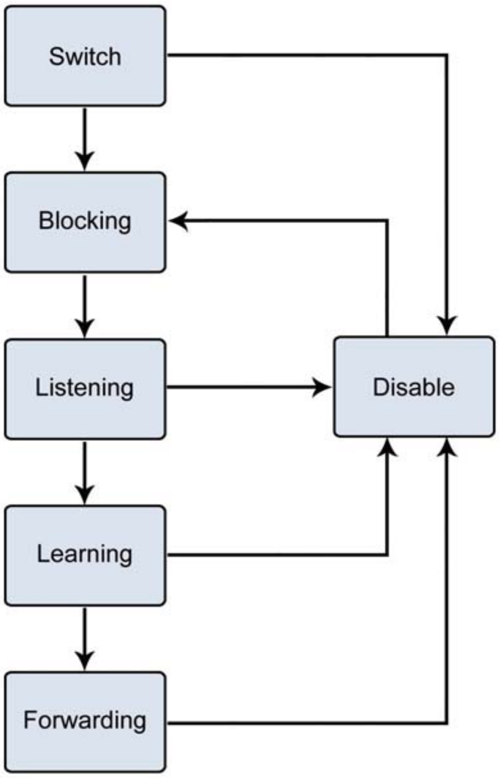


Figure 5-38 STP Port State Transitions

You can modify each port state by using management software. When you enable STP, every port on every switch in the network goes through the blocking state and then transitions through the states of listening and learning at power up. If properly configured, each port stabilizes to the forwarding or blocking state. No packets (except BPDUs) are forwarded from, or received by, STP enabled ports until the forwarding state is enabled for that port.

STP Parameters

STP Operation Levels

The Switch allows for two levels of operation: the switch level and the port level. The switch level forms a spanning tree consisting of links between one or more switches. The port level constructs a spanning tree consisting of groups of one or more ports. The STP operates in much the same way for both levels.

Note

On the switch level, STP calculates the Bridge Identifier for each switch and then sets the Root Bridge and the Designated Bridges.

On the port level, STP sets the Root Port and the Designated Ports.

The following are the user-configurable STP parameters for the switch level:

Parameter	Description	Default Value
Bridge Identifier(Not user configurable except by setting priority below)	A combination of the User-set priority and the switch's MAC address. The Bridge Identifier consists of two parts: a 16-bit priority and a 48-bit Ethernet MAC address 32768 + MAC	**32768** + **MAC**
Priority	A relative priority for each switch – lower numbers give a higher priority and a greater chance of a given switch being elected as the root bridge	**32768**
Hello Time	The length of time between broadcasts of the hello message by the switch	**2** seconds
Maximum Age Timer	Measures the age of a received BPDU for a port and ensures that the BPDU is discarded when its age exceeds the value of the maximum age timer.	**20** seconds
Forward Delay Timer	The amount time spent by a port in the learning and listening states waiting for a BPDU that may return the port to the blocking state.	**15** seconds

The following are the user-configurable STP parameters for the port or port group level:

Variable	Description	Default Value
Port Priority	A relative priority for each port –lower numbers give a higher priority and a greater chance of a given port being elected as the root port	**128**
Port Cost	A value used by STP to evaluate paths – STP calculates path costs and selects the path with the minimum cost as the active path	200,000-100Mbps Fast Ethernet ports 20,000-1000Mbps Gigabit Ethernet ports 0 - Auto

Default Spanning-Tree Configuration

Feature	Default Value
Enable state	STP disabled for all ports
Port priority	128
Port cost	0
Bridge Priority	32,768

User-Changeable STA Parameters

The Switch's factory default setting should cover the majority of installations. However, it is advisable to keep the default settings as set at the factory; unless, it is absolutely necessary. The user changeable parameters in the Switch are as follows:

Priority – A Priority for the switch can be set from 0 to 65535. 0 is equal to the highest Priority.

Hello Time – The Hello Time can be from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other Switches that it is indeed the Root Bridge. If you set a Hello Time for your Switch, and it is not the Root Bridge, the set Hello Time will be used if and when your Switch becomes the Root Bridge.

Note

The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.

Max. Age – The Max Age can be from 6 to 40 seconds. At the end of the Max Age, if a BPDU has still not been received from the Root Bridge, your Switch will start sending its own BPDU to all other Switches for permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge.

Forward Delay Timer – The Forward Delay can be from 4 to 30 seconds. This is the time any port on the Switch spends in the listening state while moving from the blocking state to the forwarding state.

Note

Observe the following formulas when setting the above parameters:

Max. Age _ 2 x (Forward Delay - 1 second)

Max. Age _ 2 x (Hello Time + 1 second)

Port Priority – A Port Priority can be from 0 to 240. The lower the number, the greater the probability the port will be chosen as the Root Port.

Port Cost – A Port Cost can be set from 0 to 200000000. The lower the number, the greater the probability the port will be chosen to forward packets.

Illustration of STP

A simple illustration of three switches connected in a loop is depicted in the below diagram. In this example, you can anticipate some major network problems if the STP assistance is not applied.

If switch A broadcasts a packet to switch B, switch B will broadcast it to switch C, and switch C will broadcast it to back to switch A and so on. The broadcast packet will be passed indefinitely in a loop, potentially causing a network failure. In this example, STP breaks the loop by blocking the connection between switch B and C. The decision to block a particular connection is based on the STP calculation of the most current Bridge and Port settings.

Now, if switch A broadcasts a packet to switch C, then switch C will drop the packet at port 2 and the broadcast will end there. Setting-up STP using values other than the defaults, can be complex. Therefore, you are advised to keep the default factory settings and STP will automatically assign root bridges/ports and block loop connections. Influencing STP to choose a particular switch as the root bridge using the Priority setting, or influencing STP to choose a particular port to block using the Port Priority and Port Cost settings is, however, relatively straight forward.

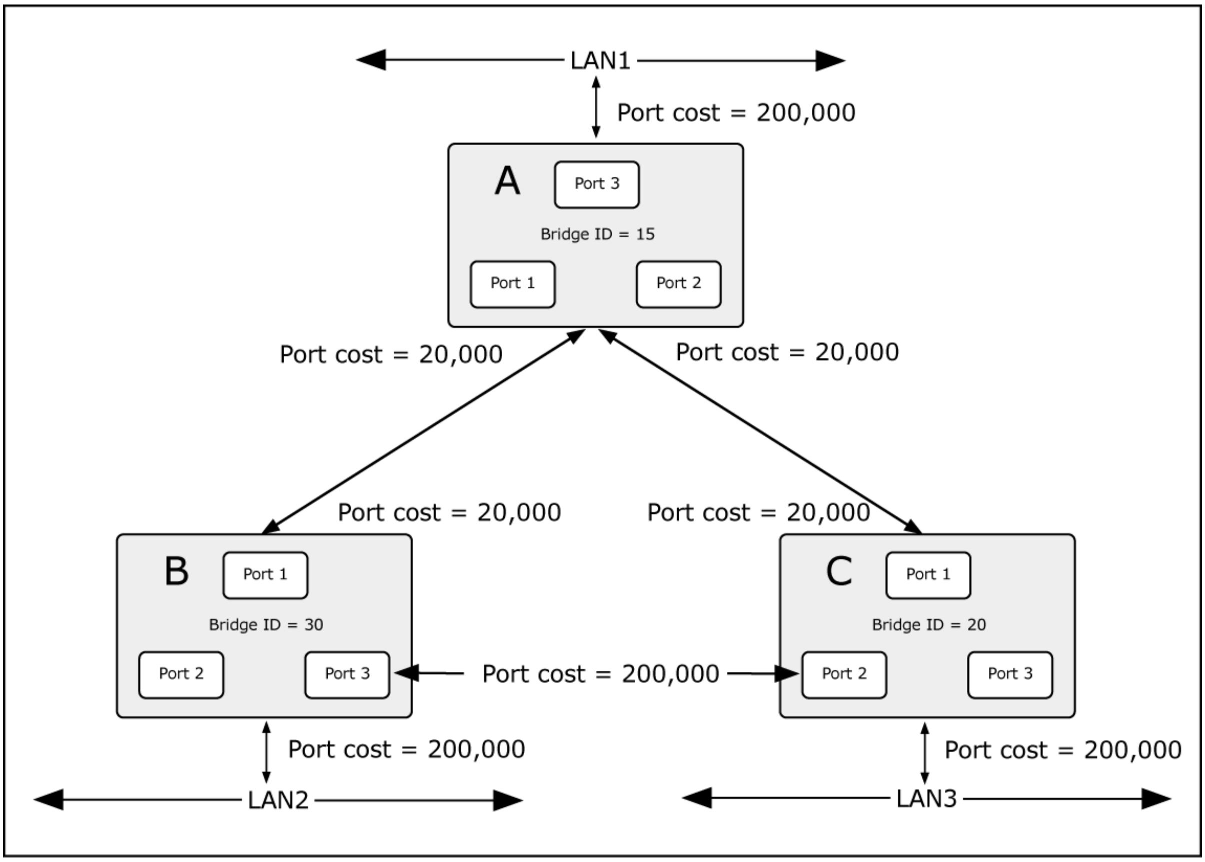


Figure 5-40 Before Applying the STA Rules

In this example, only the default STP values are used.

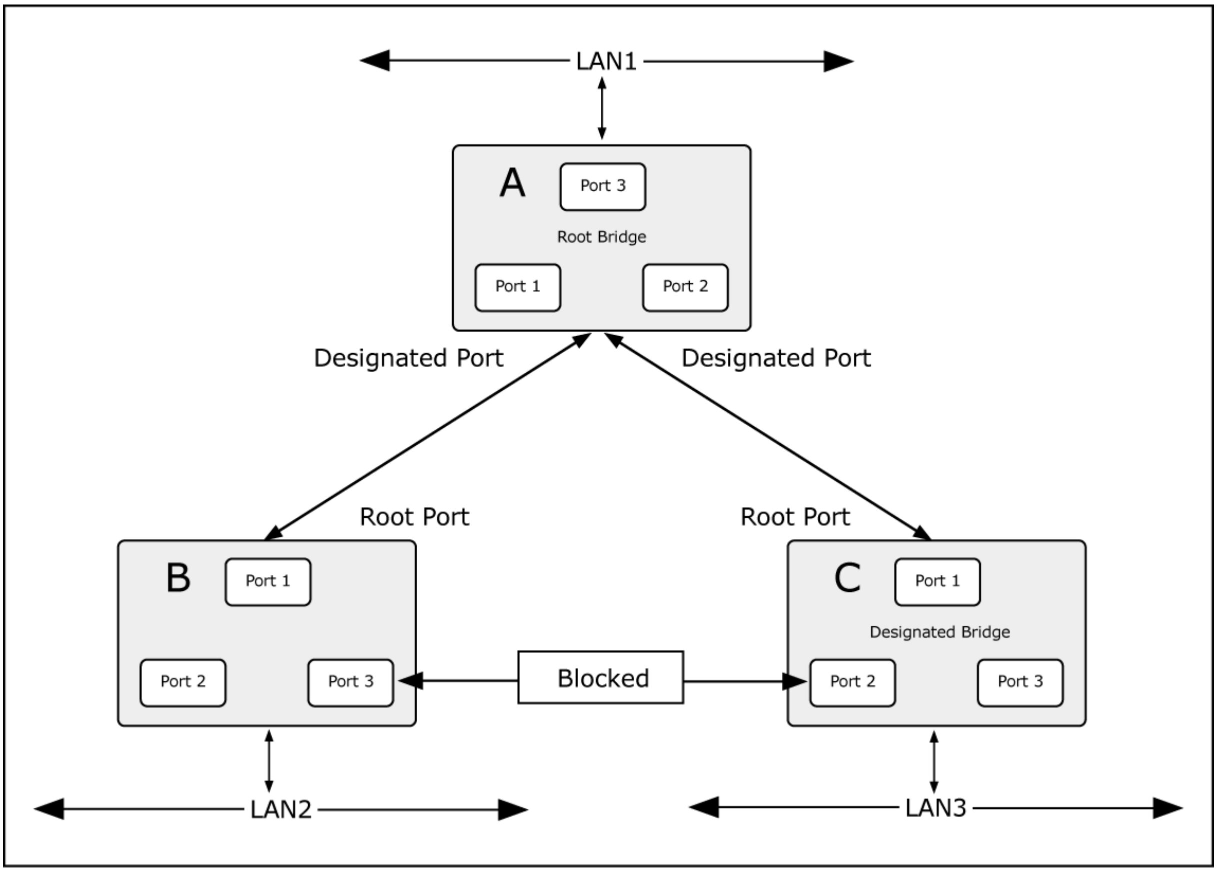
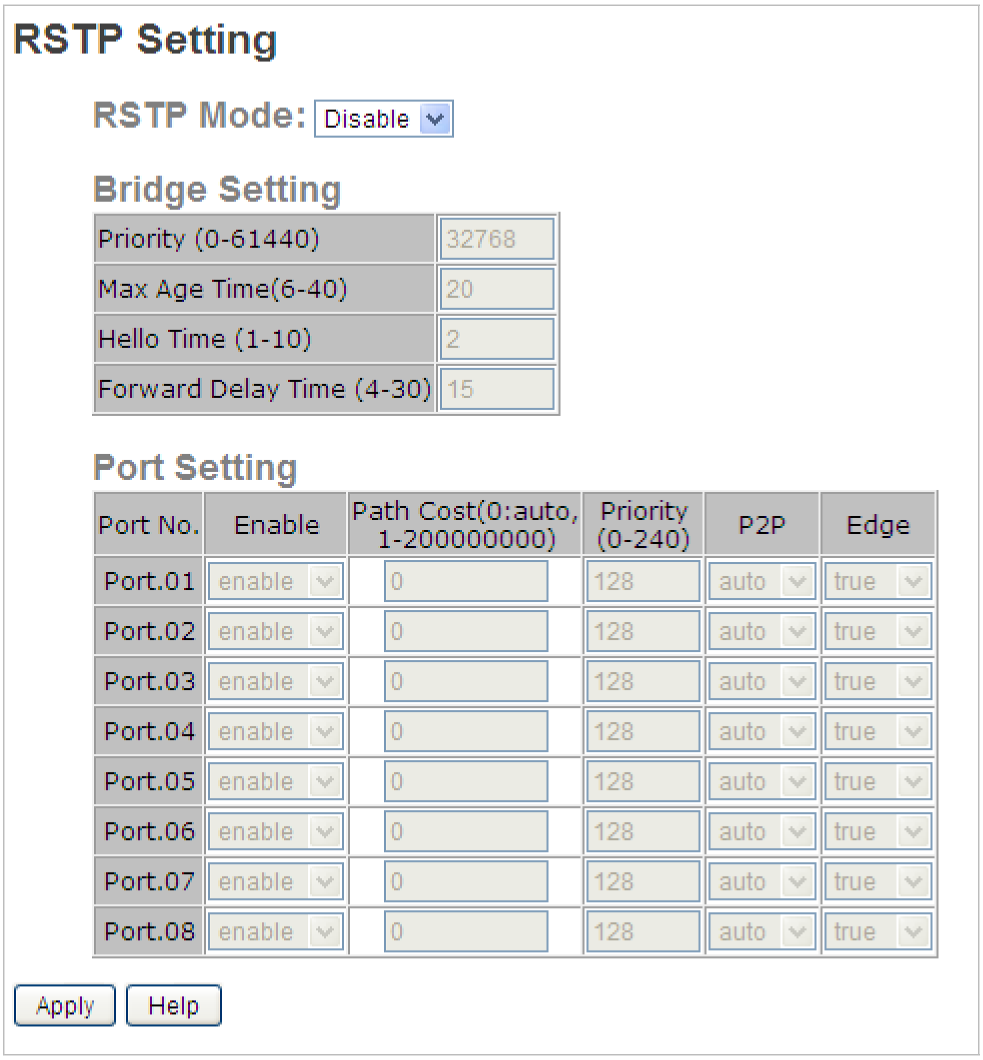


Figure 5-41 After Applying the STA Rules

The switch with the lowest Bridge ID (switch C) was elected the root bridge, and the ports were selected to give a high port cost between switches B and C. The two (optional) Gigabit ports (default port cost = 4) on switch A are connected to one (optional) Gigabit port on both switch B and C. The redundant link between switch B and C is deliberately chosen as a 100 Mbps Fast Ethernet link (default port cost = 200,000). Gigabit ports could be used, but the port cost should be increased from the default to ensure that the link between switch B and switch C is the blocked link.

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. Please see Figure 5-25 as following.



RSTP Setting

RSTP Mode: Disable

Bridge Setting

Priority (0-61440)	32768
Max Age Time(6-40)	20
Hello Time (1-10)	2
Forward Delay Time (4-30)	15

Port Setting

Port No.	Enable	Path Cost(0:auto, 1-200000000)	Priority (0-240)	P2P	Edge
Port.01	enable	0	128	auto	true
Port.02	enable	0	128	auto	true
Port.03	enable	0	128	auto	true
Port.04	enable	0	128	auto	true
Port.05	enable	0	128	auto	true
Port.06	enable	0	128	auto	true
Port.07	enable	0	128	auto	true
Port.08	enable	0	128	auto	true

Figure 5-25 Legacy Ring Configuration interface

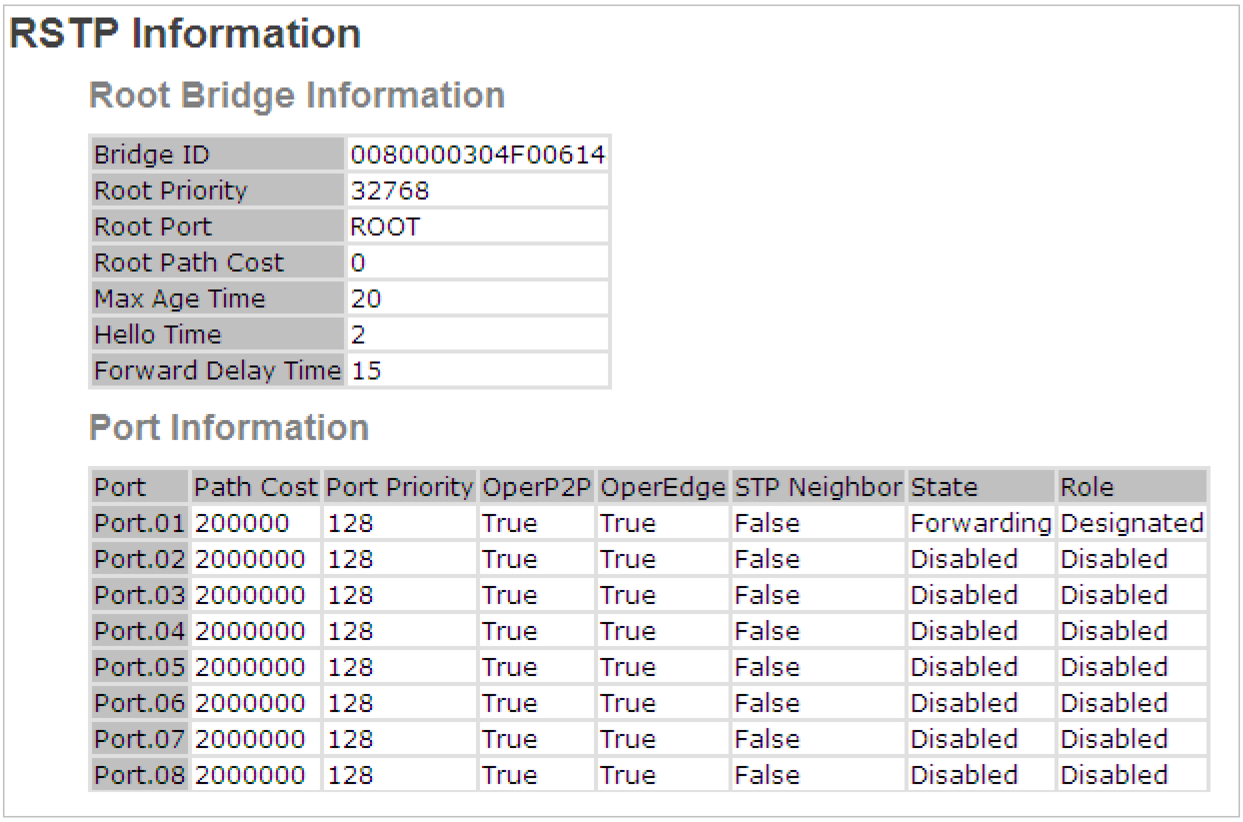
The page includes the following fields:

Object	Description
RSTP Mode	Allows user to enable or disable RSTP function.
Port No.	Port number for setting.
Enable	Allows user to enable or disable RSTP bridge port setting.
Path Cost (0:auto, 1-200000000)	Allows user to set path cost.
Priority (0-240)	**Priority:** a value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. The valid value is 0 ~ 61440 in steps of 4096 and the default value is 32768.. Note that if bridge priority is changed, the RSTP ***MUST*** be restarted.
P2P	Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. It is served by a point-to-point LAN

	segment), or it 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 P2P enabling. False means P2P disabling.
Edge	The port directly connected to end stations, and it cannot create bridging loop in the network. To configure the port as an edge port, set the port to "**True**".
Apply	Click "Apply" button to set configuration.
Help	Click "Help" button to show help file.

5.4.6.4 RSTP Information

Show RSTP algorithm result at this table. Please see Figure 5-26 as following.



RSTP Information

Root Bridge Information

Bridge ID	0080000304F00614
Root Priority	32768
Root Port	ROOT
Root Path Cost	0
Max Age Time	20
Hello Time	2
Forward Delay Time	15

Port Information

Port	Path Cost	Port Priority	OperP2P	OperEdge	STP Neighbor	State	Role
Port.01	200000	128	True	True	False	Forwarding	Designated
Port.02	2000000	128	True	True	False	Disabled	Disabled
Port.03	2000000	128	True	True	False	Disabled	Disabled
Port.04	2000000	128	True	True	False	Disabled	Disabled
Port.05	2000000	128	True	True	False	Disabled	Disabled
Port.06	2000000	128	True	True	False	Disabled	Disabled
Port.07	2000000	128	True	True	False	Disabled	Disabled
Port.08	2000000	128	True	True	False	Disabled	Disabled

Figure 5-26 Legacy Ring Configuration interface

5.4.7 VLAN

VLAN Overview

A **Virtual LAN (VLAN)** is a logical network grouping that limits the broadcast domain. It allows you to isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plug into the same switch physically.

The Managed Industrial Switch supports **IEEE 802.1Q (tagged-based)** and **Port-Base VLAN** setting in web management page. In the default configuration, VLAN support is **"Disable"**.

■ Port-based VLAN

Port-based VLAN limit traffic that flows into and out of switch ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a switch, or an entire department.

On port-based VLAN.NIC do not need to be able to identify 802.1Q tags in packet headers. NIC send and receive normal Ethernet packets. If the packet's destination lies on the same segment, communications take place using normal Ethernet protocols. Even though this is always the case, when the destination for a packet lies on another switch port, VLAN considerations come into play to decide if the packet is dropped by the Switch or delivered.

■ IEEE 802.1Q VLANs

IEEE 802.1Q (tagged) VLAN are implemented on the Switch. 802.1Q VLAN require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

VLAN allow a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast and unicast packets from unknown sources.

VLAN can also provide a level of security to your network. IEEE 802.1Q VLAN will only deliver packets between stations that are members of the VLAN. Any port can be configured as either **tagging** or **untagging**:

- The untagging feature of IEEE 802.1Q VLAN allows VLAN to work with legacy switches that don't recognize VLAN tags in packet headers.
- The tagging feature allows VLAN to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

Some relevant terms:

Tagging - The act of putting 802.1Q VLAN information into the header of a packet.

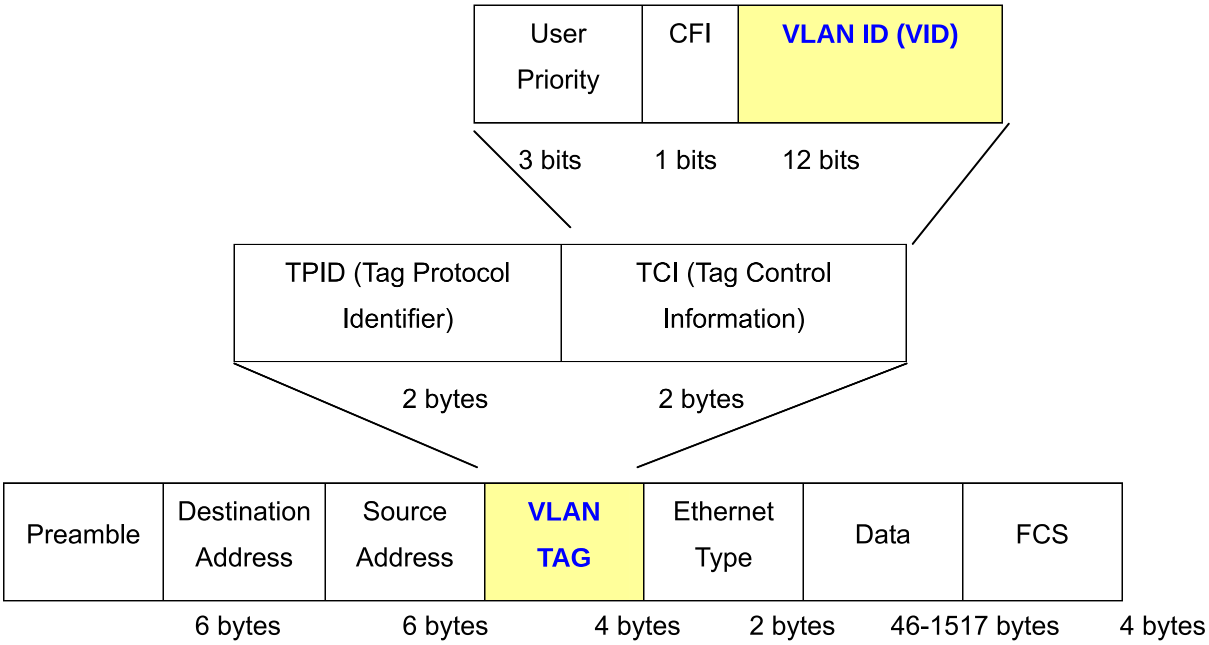
Untagging - The act of stripping 802.1Q VLAN information out of the packet header.

■ 802.1Q VLAN Tags

The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of 0x8100 in the Ether Type field. When a packet's Ether Type field is equal to **0x8100**, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI - used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and 12 bits of **VLAN ID (VID)**. The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLAN can be identified.

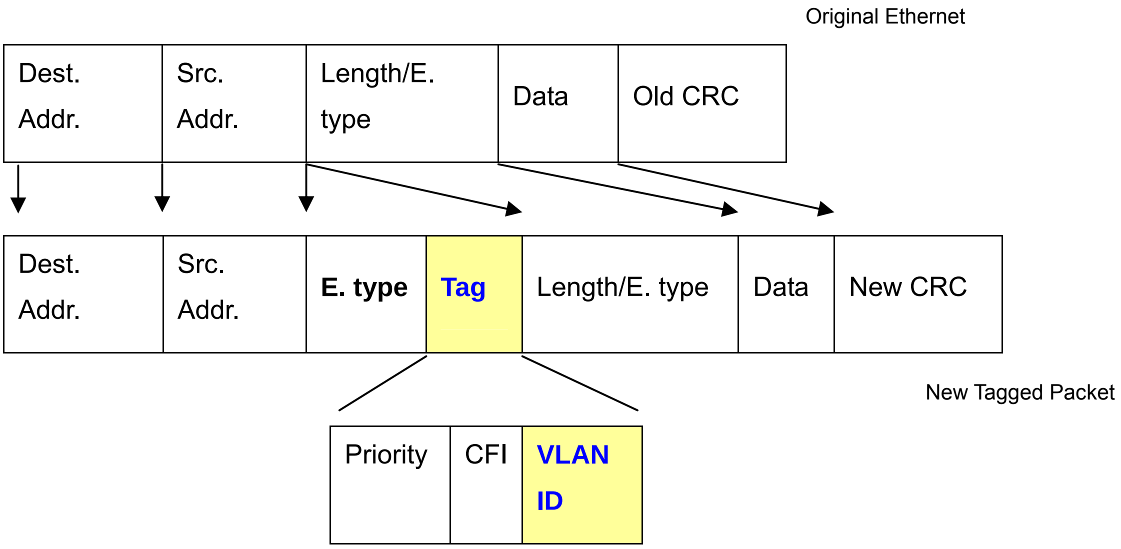
The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

802.1Q Tag



The Ether Type and VLAN ID are inserted after the MAC source address, but before the original Ether Type/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

Adding an IEEE802.1Q Tag



■ Port VLAN ID

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLAN to span network devices (and indeed, the entire network – if all network devices are 802.1Q compliant).

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the switch. If no VLAN are defined on the switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, in so far as VLAN are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet forwarding decisions, the VID is.

Tag-aware switches must keep a table to relate PVID within the switch to VID on the network. The switch will compare the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VID are different the switch will drop the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A switch port can have only one PVID, but can have as many VID as the switch has memory in its VLAN table to store them.

Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted – should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

■ Default VLANs

The Switch initially configures one VLAN, VID = 1, called **"default."** The factory default setting assigns all ports on the Switch to the **"default"**. As new VLAN are configured in Port-based mode, their respective member ports are removed from the "default."

Note

Base on the Switch chipset specification, the Managed Industrial Switch supports **SVL(Shared VLAN Learning)** , all VLAN groups share the same Layer 2 learned MAC address table.

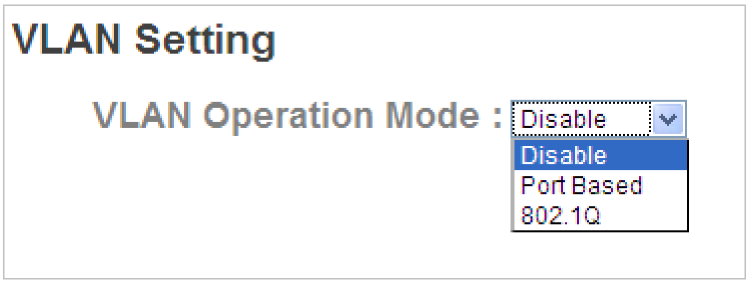
Note

1 No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLAN without a network device performing a routing function between the VLAN.

2 The Switch supports Port-based VLAN and IEEE 802.1Q VLAN. The port untagging function can be used to remove the 802.1 tag from packet headers to maintain compatibility with devices that are tag-unaware.

5.4.7.1 VLAN Setting

This section is describing how to configure VLAN. IGS-8044MT provides Port Based VLAN and IEEE 802.1Q VLAN, and as default setting VLAN operation mode is disabled, user has to choose one of VLAN to enable it. Please see Figure 5-27 as following.



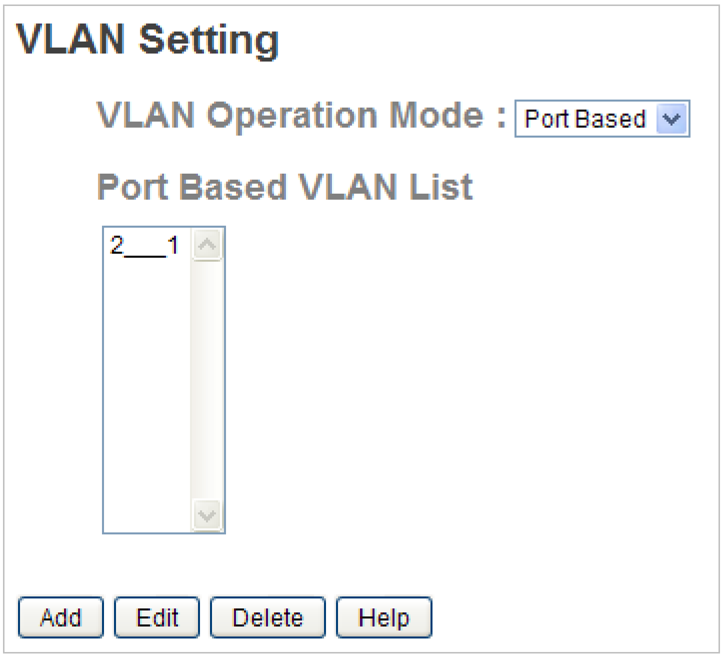
VLAN Setting

VLAN Operation Mode : Disable

Figure 5-27 Legacy Ring Configuration interface

Port Based VLAN

Traffic is forwarded to the member ports of the same VLAN group. Please see Figure 5-28 as following.



VLAN Setting

VLAN Operation Mode : Port Based

Port Based VLAN List

2___1

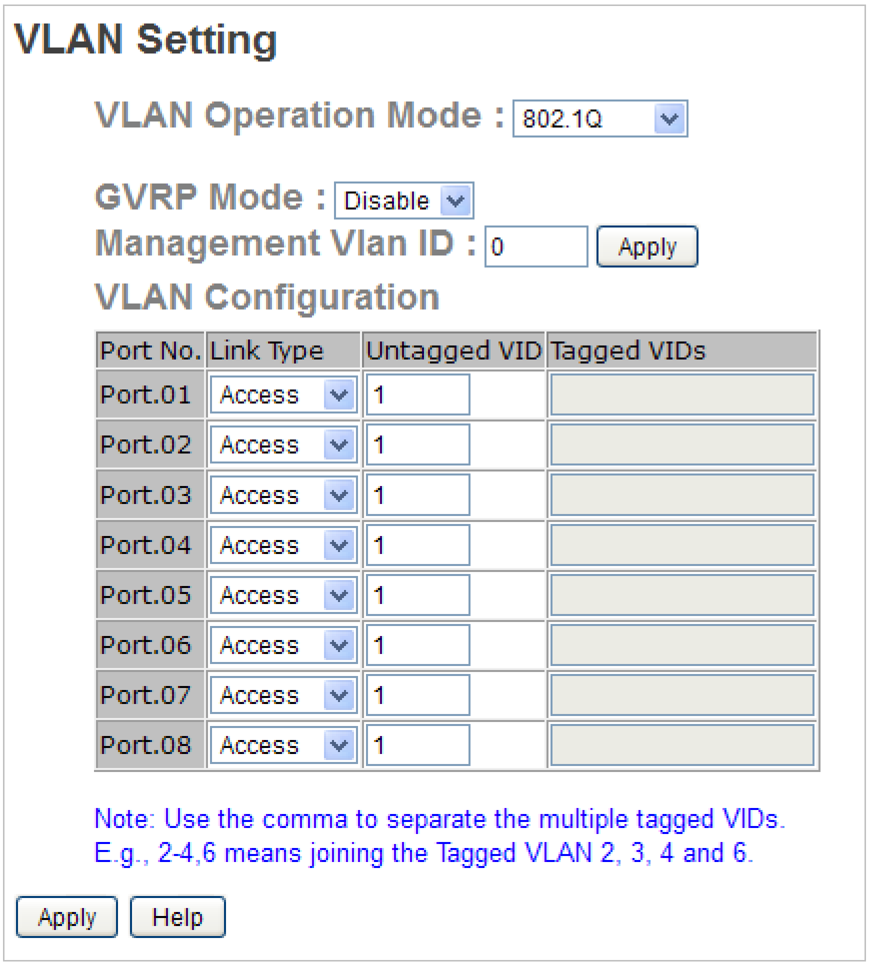
Figure 5-28 Port Based VLAN Configuration interface

The page includes the following fields:

Object	Description
VLAN Operation Mode	Allows user to choose VLAN operation mode. It offers Port Based mode and IEEE 802.1Q mode.
Port Based VLAN List	Display the created VLAN group.
Add	Click "Add" button to create new VLAN.
Edit	Choose a VLAN group on the Port Based VLAN List, and Click "Edit" button to edit the VLAN group.
Delete	Choose a VLAN group on the Port Based VLAN List, and Click "Delete" button to delete the VLAN group.
Help	Click "Help" button to show help file.

802.1Q VLAN

IEEE 802.1Q defines the operation of Virtual LAN (VLAN) Bridges that permit the definition, operation and administration of Virtual LAN topologies within a Bridged LAN infrastructure. The GARP (Generic Attribute Registration Protocol) VLAN Registration Protocol (GVRP) defines a GARP application that provides the 802.1Q-compliantVLAN pruning and dynamic VLAN creation on 802.1Q trunk ports. Please refer to IEEE 802.1Q. Please see Figure 5-29 as following.



VLAN Setting

VLAN Operation Mode : 802.1Q

GVRP Mode : Disable

Management Vlan ID : 0 Apply

VLAN Configuration

Port No.	Link Type	Untagged VID	Tagged VIDs
Port.01	Access	1	
Port.02	Access	1	
Port.03	Access	1	
Port.04	Access	1	
Port.05	Access	1	
Port.06	Access	1	
Port.07	Access	1	
Port.08	Access	1	

Note: Use the comma to separate the multiple tagged VIDs.
E.g., 2-4,6 means joining the Tagged VLAN 2, 3, 4 and 6.

Apply Help

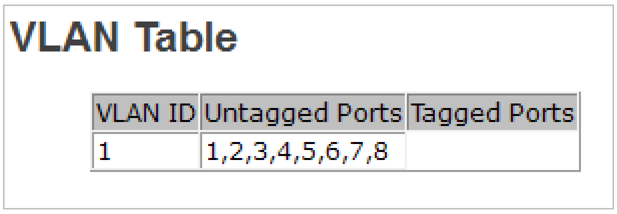
Figure 5-29 Port Based VLAN Configuration interface

The page includes the following fields:

Object	**Description**
VLAN Operation Mode	Allows user to choose VLAN operation mode. It offers Port Based mode and IEEE 802.1Q mode.
GVRP Mode	Allows user to enable or disable GVRP mode.
Management VLAN ID	Management VLAN can provide network administrator a secure VLAN to management Switch. Only the devices in the management VLAN can access the switch.
Link Type	There are 3 types of link type: ■ **Access Link:** single switch only, allows you to group ports by setting the same VID. ■ **Trunk Link:** extended application of **Access Link**, allows you to group ports by setting the same VID with 2 or more switches. ■ **Hybrid Link:** Both **Access Link** and **Trunk Link** are available.
Untagged VID	Set the port default VLAN ID for untagged devices that connect to the port. The range is 1 to 4094.
Tagged VID	Set the tagged VIDs to carry different VLAN frames to other switch.

Apply	Click "**Apply**" to activate the configurations.
Help	Click "Help" button to show help file.

The VLAN Table shows VLAN group current state. Please see Figure 5-30 as following.



VLAN Table

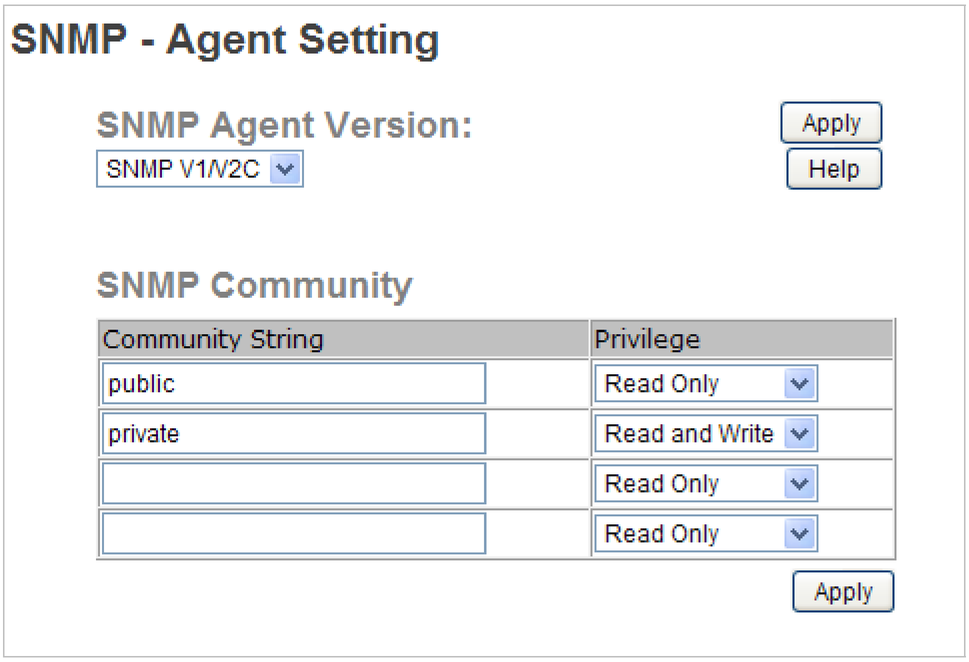
VLAN ID	Untagged Ports	Tagged Ports
1	1,2,3,4,5,6,7,8	

Figure 5-30 Port Based VLAN Configuration interface

5.4.8 SNMP

5.4.8.1 SNMP – Agent Setting

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. Please see Figure 5-31 as following.



SNMP - Agent Setting

SNMP Agent Version:

SNMP V1/V2C

SNMP Community

Community String	Privilege
public	Read Only
private	Read and Write
	Read Only
	Read Only

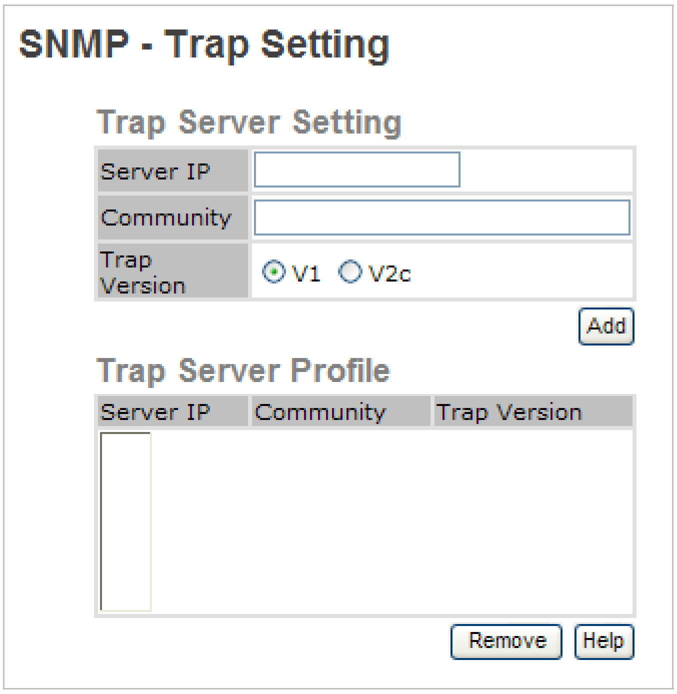
Figure 5-31 SNMP - Agent Configuration interface

The page includes the following fields:

Object	Description
SNMP Agent Version	Allows user to choose SNMP v1, v2c or v3.
SNMP V1/V2c Community	SNMP Community should be set for SNMP V1/V2c. Four sets of "Community String/Privilege" are supported. Each Community String is maximum 32 characters. Keep empty to remove this Community string.
Community String	Allows user to define SNMP community string.
Privilege	Allows user to choose what privilege will be applied.
Apply	Click "**Apply**" to activate the configurations.
Help	Click "Help" button to show help file.

5.4.8.2 SNMP – Trap Setting

A trap manager is a management station that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps will issue. Create a trap manager by entering the IP address of the station and a community string. To define management stations as trap manager and enter SNMP community strings and selects the SNMP version. Please see Figure 5-32 as following.



SNMP - Trap Setting

Trap Server Setting

Server IP	
Community	
Trap Version	● V1 ○ V2c

Trap Server Profile

Server IP	Community	Trap Version

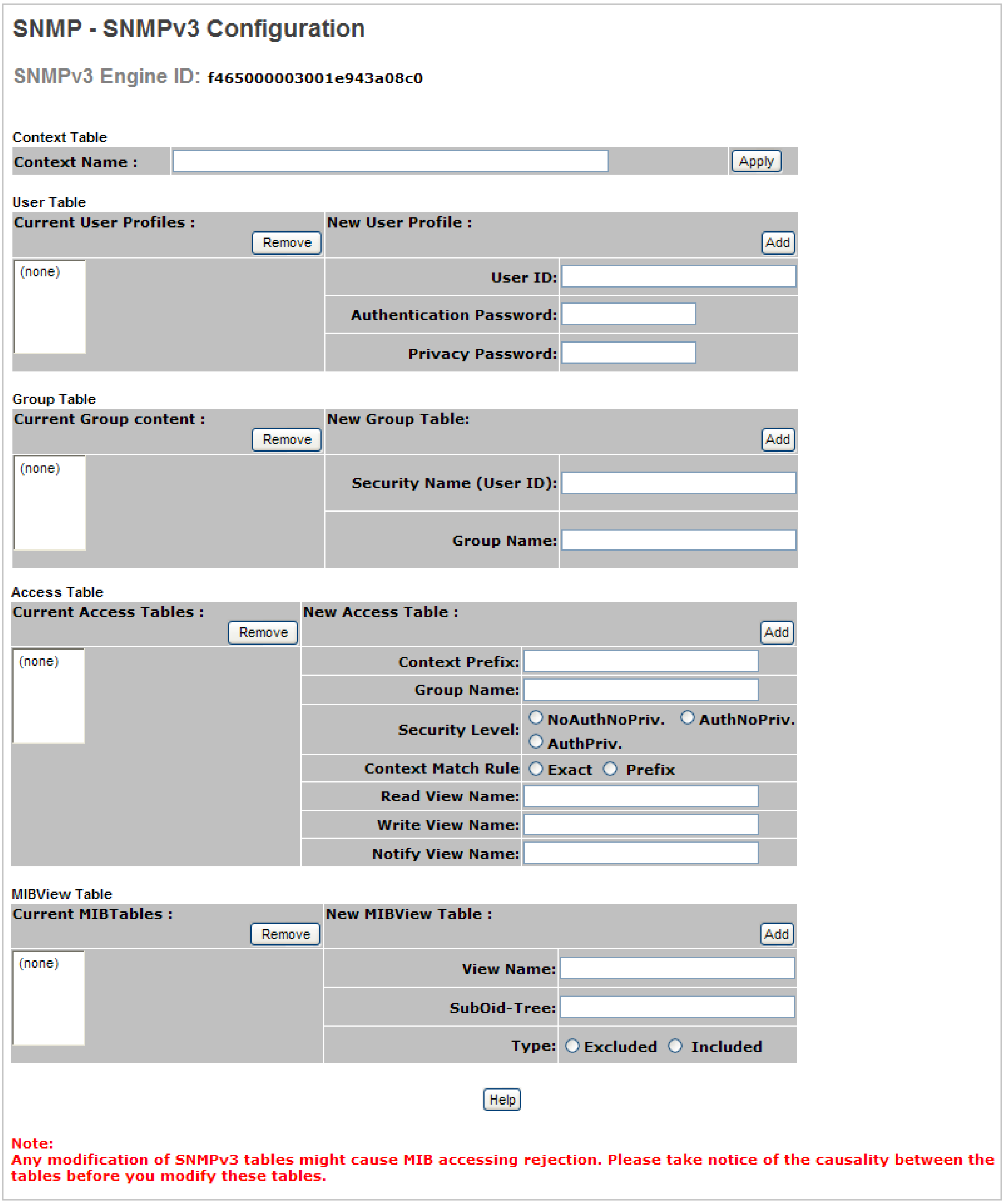
Figure 5-32 SNMP – Trap Configuration interface

The page includes the following fields:

Object	Description
Server IP	The server IP address to receive Trap
Community	Community for authentication
Trap Version	Trap Version supports V1 and V2c.
Trap Server profile	Add trap server profile.
Add	Remove trap server profile.
Remove	Show help file.
Help	Click "Help" button to show help file.

5.4.8.3 SNMP v3 Setting

SNMP V3 requires an authentication level of MD5 or DES to encrypt data to enhance data security. Please see Figure 5-33 as following.



SNMP - SNMPv3 Configuration

SNMPv3 Engine ID: f465000003001e943a08c0

Context Table

Context Name :

User Table

Current User Profiles : (none)

New User Profile :

User ID:

Authentication Password:

Privacy Password:

Group Table

Current Group content : (none)

New Group Table:

Security Name (User ID):

Group Name:

Access Table

Current Access Tables : (none)

New Access Table :

Context Prefix:

Group Name:

Security Level: ○ NoAuthNoPriv. ○ AuthNoPriv. ○ AuthPriv.

Context Match Rule ○ Exact ○ Prefix

Read View Name:

Write View Name:

Notify View Name:

MIBView Table

Current MIBTables : (none)

New MIBView Table :

View Name:

SubOid-Tree:

Type: ○ Excluded ○ Included

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

Figure 5-33 SNMPv3 Configuration interface

The page includes the following fields:

Object	Description
Context Name	Allows user to input context name.
Current User Profile	Display user profile list.
Current Group Content	Display group content list.
Current Access Tables	Display current access table list.
Current MIB Table	Display current MIB table list.
User ID	Allows user to input user ID.
Authentication Password	Allows user to input authentication password.
Privacy Password	Allows user to input privacy password.
Security Name (User ID)	Allows user to input security name (user ID)
Group Name	Allows user to input group name.
Context Prefix	Allows user to input context prefix.
Security Level	Allows user to choose security level. There are 3 level: ■ NoAuthNoPriv: it means no need authentication password and privacy password. ■ AuthNoPrivacy: it means to need authentication password and no need privacy password. ■ AuthPrivacy: it means to need authentication password and privacy password both.
Context Match Rule	Allows user to choose context match rule. There are 2 options are **Exact** and **Prefix**.
Read View Name	Allows user to input read view name.
Write View Name	Allows user to input write view name.
Notify View Name	Allows user to input notify view name.
View Name	Allows user to input view name.
SubOid-Tree	Allows user to input SNMP object ID.
Type	Allows user to choose excluded type or included type.
Add	Remove trap server profile.
Remove	Show help file.

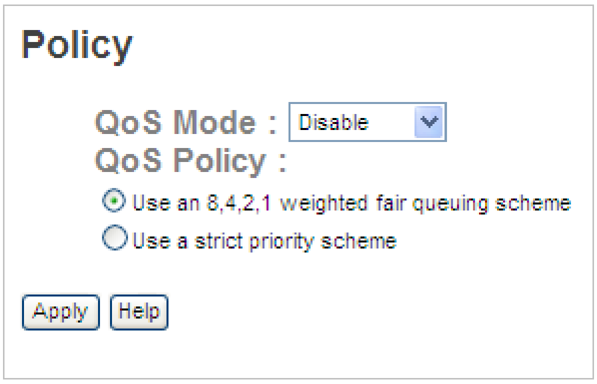
Apply	Click "**Apply**" to activate the configurations.
Help	Click "Help" button to show help file.

5.4.9 Traffic Prioritization

Traffic Prioritization includes 3 modes: port base, 802.1p/COS, and TOS/DSCP. By traffic prioritization function, you can classify the traffic into four classes for differential network application. SW-M series support 4 priority queues.

5.4.9.1 Policy

This section is allows user to set policy of QoS. Please see Figure 5-34 as following.



Policy

QoS Mode : Disable

QoS Policy :

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

○ Use a strict priority scheme

Figure 5-34 QoS Policy Configuration interface

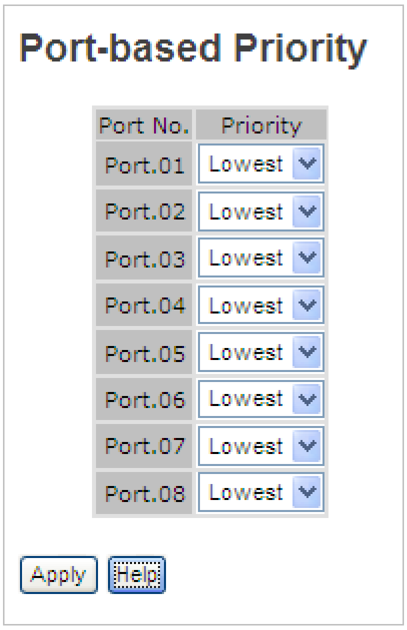
The page includes the following fields:

Object	Description
QoS Mode	The QoS mode allows user to choose different QoS mode, there are offers 5 types as following. ■ **Port-base:** the output priority is determined by ingress port. ■ **COS only: the output priority is determined by COS only.** ■ **TOS only: the output priority is determined by TOS only.** ■ **COS first: the output priority is determined by COS and TOS, but COS first.** ■ **TOS first: the output priority is determined by COS and TOS, but TOS first.**
QoS Policy	Allows user to choose 2 types policy as following. ■ **Use an 8, 4, 2, 1 weight fair queue scheme** Select the preference given to packets in the switch's higher-priority queue. These options represent the number of higher priority packets sent before one lower priority packet is sent. For example, 8 Highest : 4 Second High : 2 Second Low : 1 Lowest means that the switch sends 8 highest priority packets before sending 4 second high priority packet, before sending 2 second low priority packet, before sending 1 lowest priority packet.

	■ **Use a strict priority scheme** The high priority packets sent before low priority packets.
Apply	Click "**Apply**" to activate the configurations.
Help	Click "Help" button to show help file.

5.4.9.2 Port-Based priority

Configure the priority level for each port. With the drop-down selection item of Priority Type, this control item will then be available to set the queuing policy for each port. Please see Figure 5-35 as following.



Port-based Priority

Port No.	Priority
Port.01	Lowest
Port.02	Lowest
Port.03	Lowest
Port.04	Lowest
Port.05	Lowest
Port.06	Lowest
Port.07	Lowest
Port.08	Lowest

Figure 5-35 Port-Based Priority Configuration interface

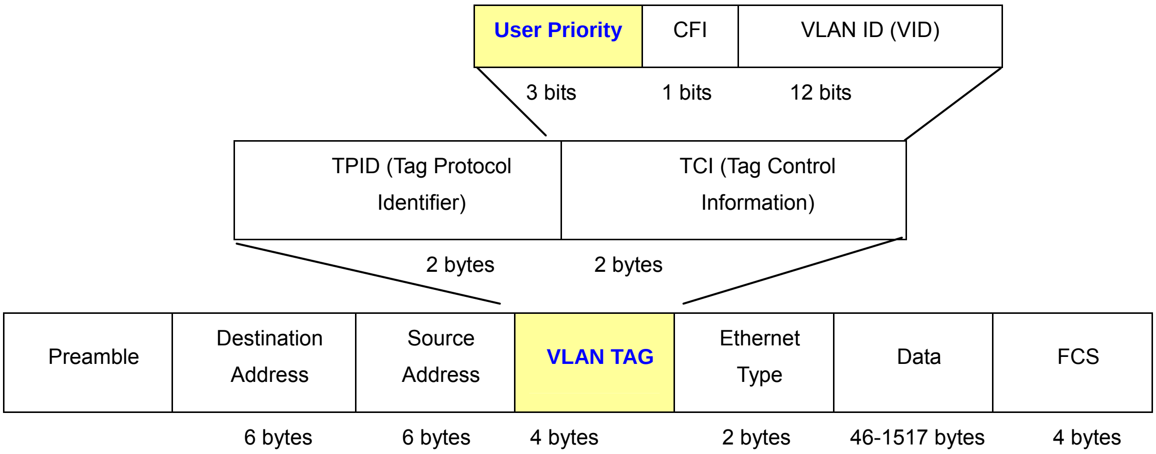
The page includes the following fields:

Object	Description
Port No.	The port number for setting.
Priority	Allows user to set priority type. There are totally 4 types for chosen, **High**, **Middle**, **Low**, **and Lowest**.
Apply	Click "**Apply**" to activate the configurations.
Help	Click "Help" button to show help file.

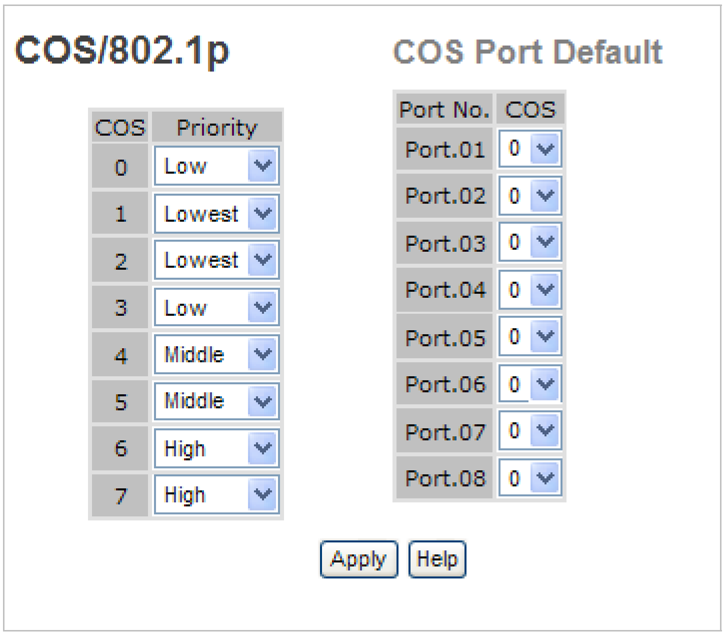
5.4.9.3 COS / 802.1p

QoS settings allow customization of packet priority in order to facilitate delivery of data traffic that might be affected by latency problems. When CoS / 802.1p Tag Priority is applied, the Switch recognizes 802.1Q VLAN tag packets and extracts the VLAN tagged packets with User Priority value.

802.1Q Tag and 802.1p priority



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 . Please see Figure 5-36 as following.



COS/802.1p

COS	Priority
0	Low
1	Lowest
2	Lowest
3	Low
4	Middle
5	Middle
6	High
7	High

COS Port Default

Port No.	COS
Port.01	0
Port.02	0
Port.03	0
Port.04	0
Port.05	0
Port.06	0
Port.07	0
Port.08	0

Figure 5-36 COS/802.1p Configuration interface

The page includes the following fields:

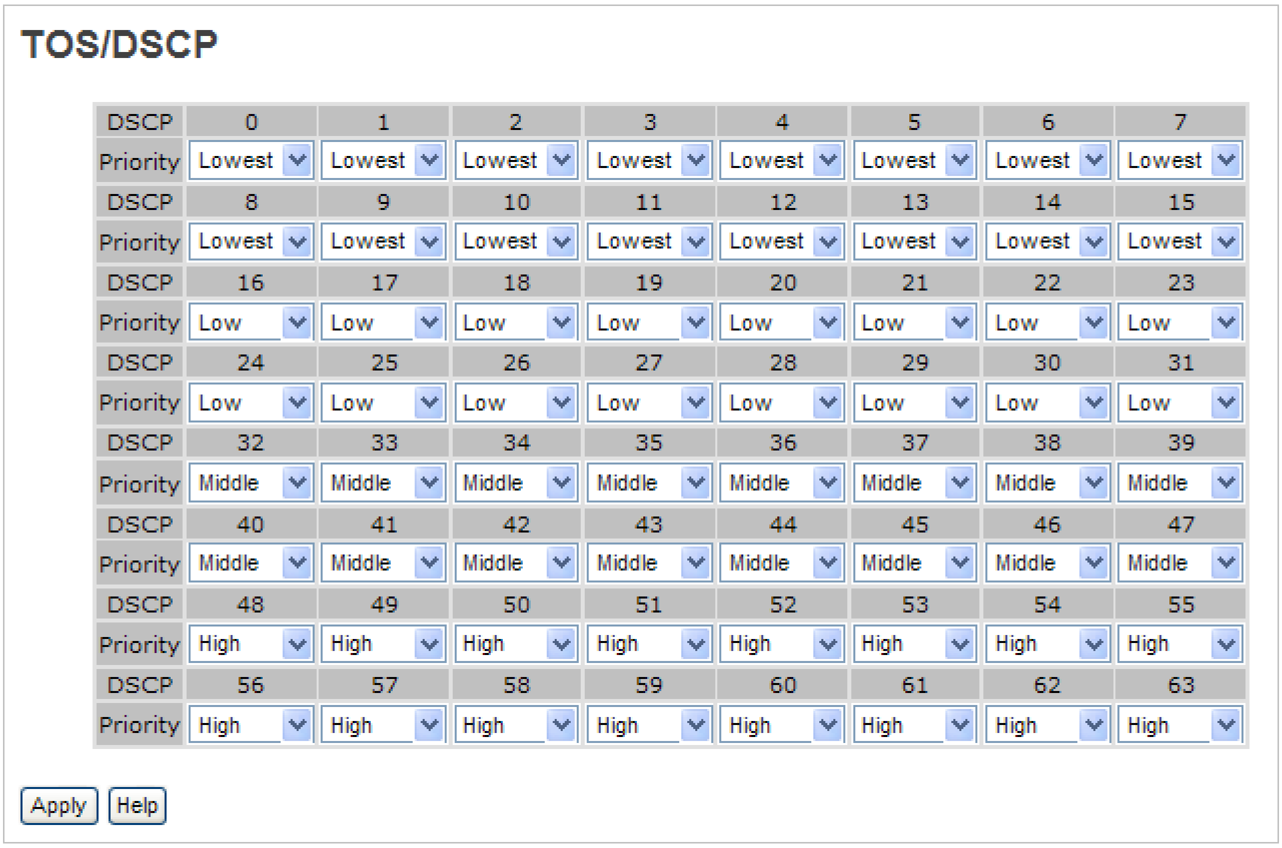
Object	Description
Port No.	The port number for setting.
Priority	Allows user to define COS priority level. There are totally 4 types for chosen, **High**, **Middle**, **Low**, **and Lowest**. For example, user can define 0 is lowest and 7 is high, or opposite.
COS	Allows user to set class priority level. (0-7) **COS Port Default** When an ingress packet has not VLAN tag, a default priority value is considered and determined by ingress port.
Apply	Click "**Apply**" to activate the configurations.
Help	Click "Help" button to show help file.

5.4.9.4 TOS / DSCP

The **TOS/DSCP** page provides fields for defining output queue to specific DSCP fields. When TCP/IP's TOS/DSCP mode is applied, the Managed Switch recognizes TCP/IP Differentiated Service Code Point (DSCP) priority information from the DS-field defined in RFC2474.

Set up IP TOS / DSCP mapping to 802.1p priority when receiving IPv4 packets, the Managed Switch allow to by port configuring the QoS Status. This TOS/DSCP Port Configuration page is to configure the IP TOS/DSCP mapping on the port and display the current port status.

Enable TOS/DSCP for traffic classification and then the DSCP to priority mapping column is configurable. Please see Figure 5-37 as following.



TOS/DSCP

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

Figure 5-37 TOS / DSCP Configuration interface

The page includes the following fields:

Object	**Description**
DSCP	The values of the IP DSCP header field within the incoming packet. 0~63.
Priority	Allows user to define COS priority level. There are totally 4 types for chosen, **High**, **Middle**, **Low**, **and Lowest**.
Apply	Click “**Apply**” to activate the configurations.
Help	Click “Help” button to show help file.

5.4.10 Multicast

Internet Group Management Protocol (IGMP) is used by IP hosts to register their dynamic multicast group membership. IGMP has 3 versions, IGMP v1, v2 and v3. Please refer to RFC 1112, 2236 and 3376. IGMP Snooping improves the performance of networks that carry multicast traffic. It provides the ability to prune multicast traffic so that it travels only to those end destinations that require that traffic and reduces the amount of traffic on the Ethernet LAN.

5.4.10.1 IGMP Snooping

- **Theory**

The **Internet Group Management Protocol (IGMP)** lets host and routers share information about multicast groups memberships. IGMP snooping is a switch feature that monitors the exchange of IGMP messages and copies them to the CPU for feature processing. The overall purpose of IGMP Snooping is to limit the forwarding of multicast frames to only ports that are a member of the multicast group.

About the Internet Group Management Protocol (IGMP) Snooping

Computers and network devices that want to receive multicast transmissions need to inform nearby routers that they will become members of a multicast group. The **Internet Group Management Protocol (IGMP)** is used to communicate this information. IGMP is also used to periodically check the multicast group for members that are no longer active. In the case where there is more than one multicast router on a sub network, one router is elected as the 'queried'. This router then keeps track of the membership of the multicast groups that have active members. The information received from IGMP is then used to determine if multicast packets should be forwarded to a given sub network or not. The router can check, using IGMP, to see if there is at least one member of a multicast group on a given subnet work. If there are no members on a sub network, packets will not be forwarded to that sub network.

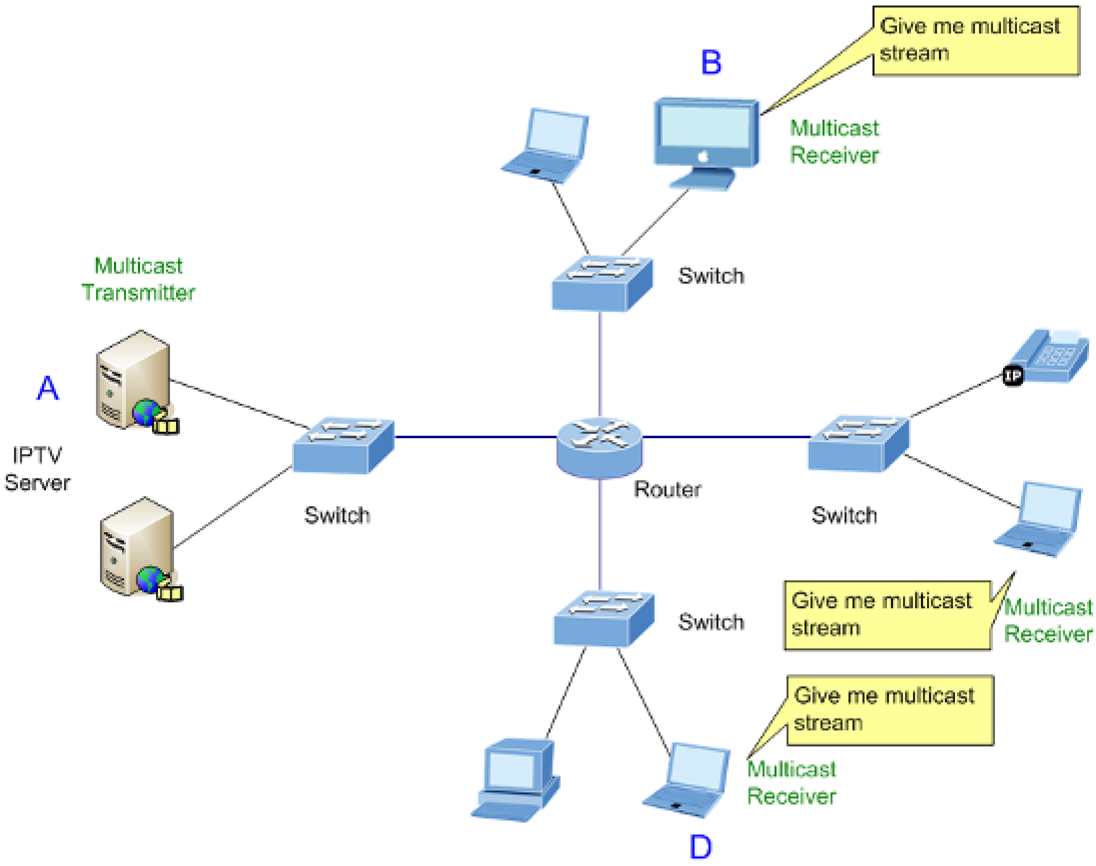
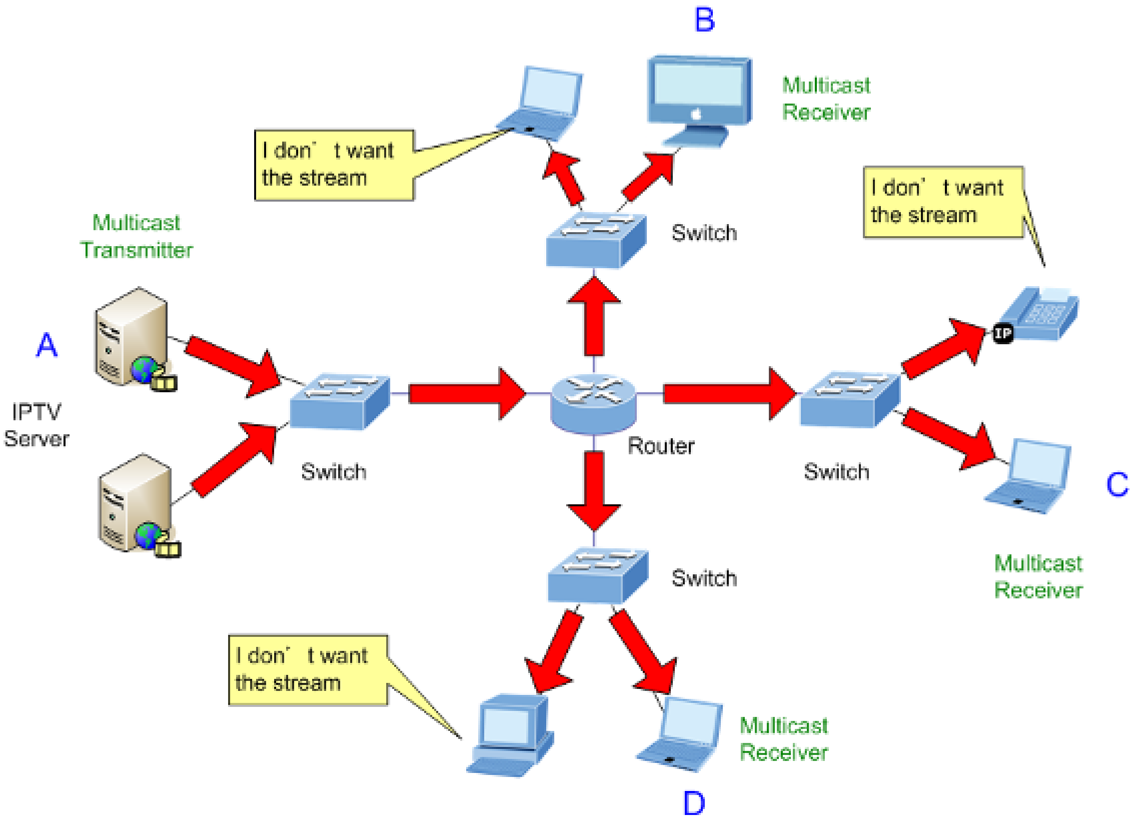
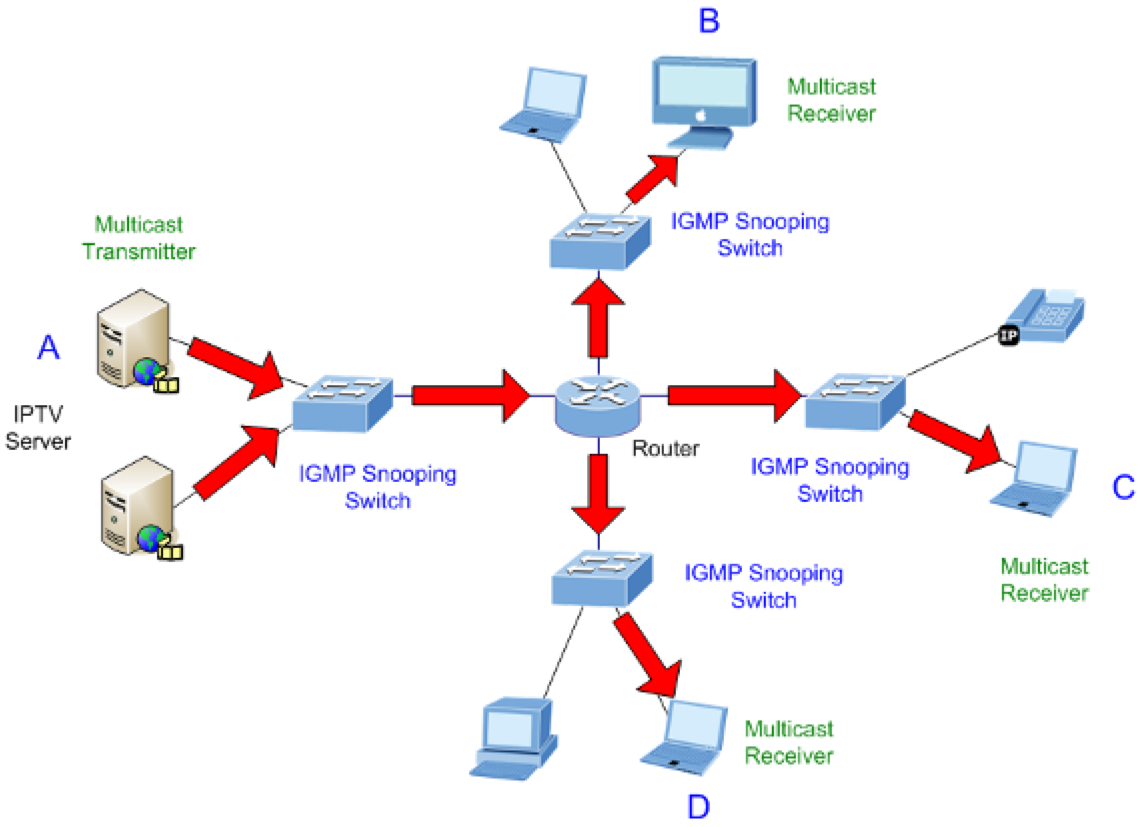


Figure 4-8-1: Multicast Service





IGMP Versions 1 and 2

Multicast groups allow members to join or leave at any time. IGMP provides the method for members and multicast routers to communicate when joining or leaving a multicast group.

IGMP version 1 is defined in RFC 1112. It has a fixed packet size and no optional data.

The format of an IGMP packet is shown below:

IGMP Message Format

Octets

0 8 16 31

Type	Response Time	Checksum
Group Address (all zeros if this is a query).		

The IGMP Type codes are shown below:

Type	Meaning
0x11	Membership Query (if Group Address is 0.0.0.0).
0x11	Specific Group Membership Query (if Group Address is Present).
0x16	**Membership Report (version 2).**

0x17	**Leave a Group (version 2).**
0x12	**Membership Report (version 1).**

IGMP packets enable multicast routers to keep track of the membership of multicast groups, on their respective sub networks. The following outlines what is communicated between a multicast router and a multicast group member using IGMP.
A host sends an IGMP **"report"** to join a group.

A host will never send a report when it wants to leave a group (for version 1).

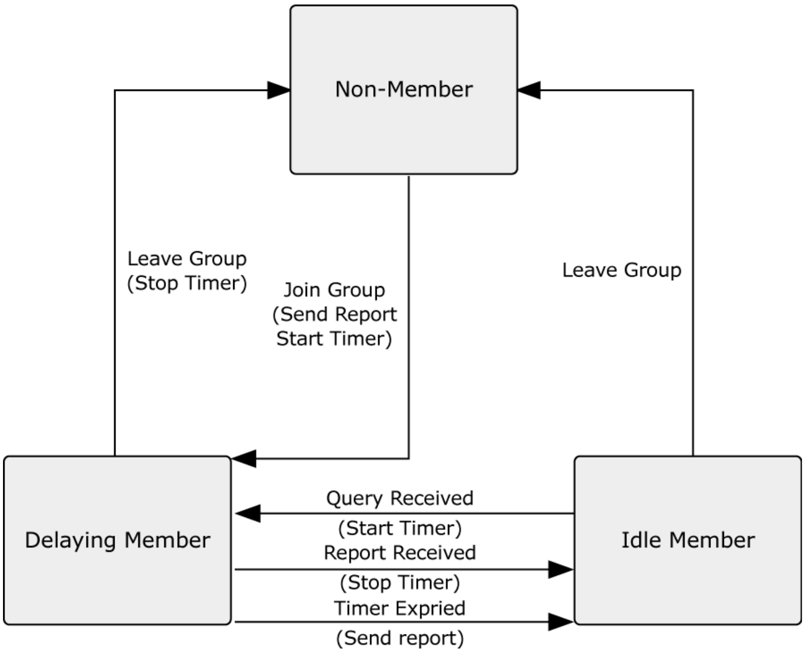
A host will send a **"leave"** report when it wants to leave a group (for version 2).

Multicast routers send IGMP queries (to the all-hosts group address: 224.0.0.1) periodically to see whether any group members exist on their sub networks. If there is no response from a particular group, the router assumes that there are no group members on the network.

The Time-to-Live (TTL) field of query messages is set to 1 so that the queries will not be forwarded to other sub networks.

IGMP version 2 introduces some enhancements such as a method to elect a multicast queried for each LAN, an explicit leave message, and query messages that are specific to a given group.

The states a computer will go through to join or to leave a multicast group are shown below:



IGMPv3 adds support for "source filtering", that is, the ability for a system to report interest in receiving packets *only* from specific source addresses, or from *all but* specific source addresses, sent to a

particular multicast address. That information may be used by multicast routing protocols to avoid delivering multicast packets from specific sources to networks where there are no interested receivers.

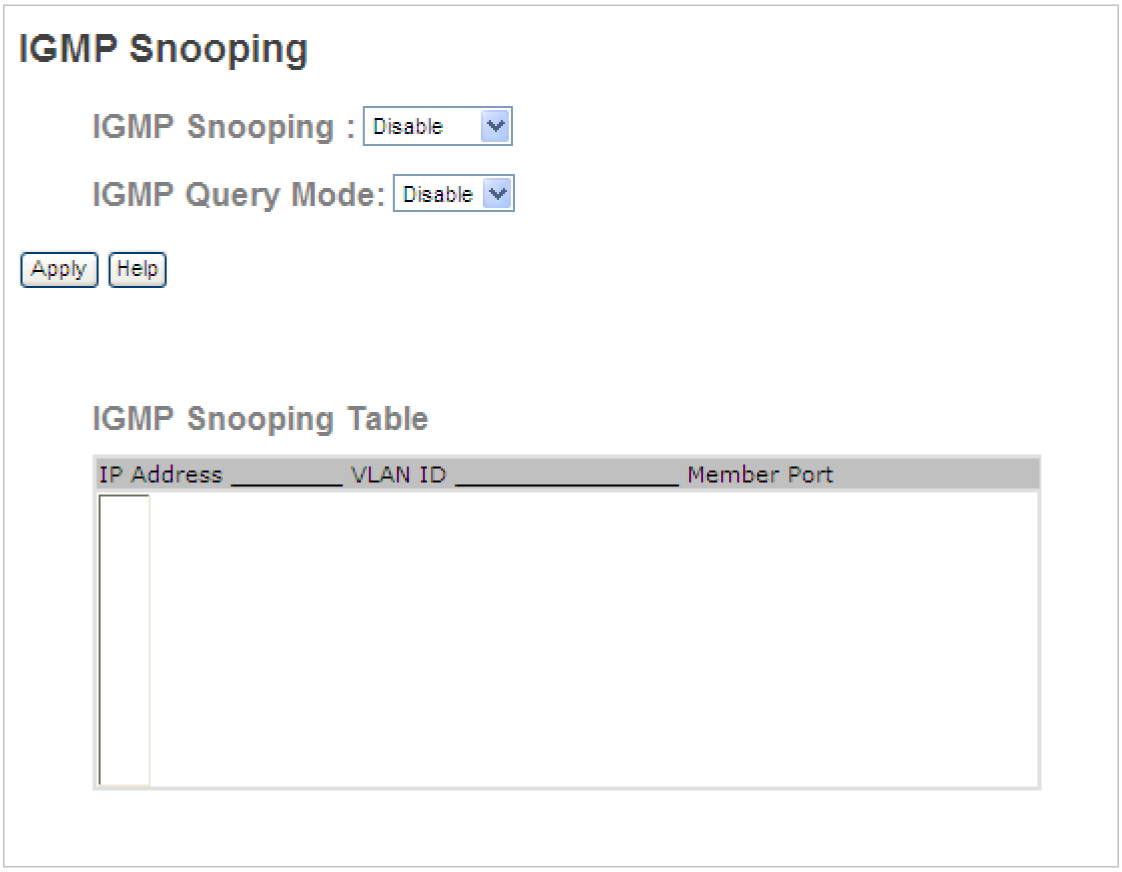
- **IGMP Querier**

A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "**querier**" and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

Note

Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

The IGS-8044MT supports IP multicast, you can enable IGMP protocol on WEB UI IGMP Snooping setting page, then the IGMP snooping information displays. IP multicast addresses range are from **224.0.0.0** through **239.255.255.255**. Please see Figure 5-38 as following.



IGMP Snooping

IGMP Snooping : Disable

IGMP Query Mode: Disable

IGMP Snooping Table

IP Address	VLAN ID	Member Port

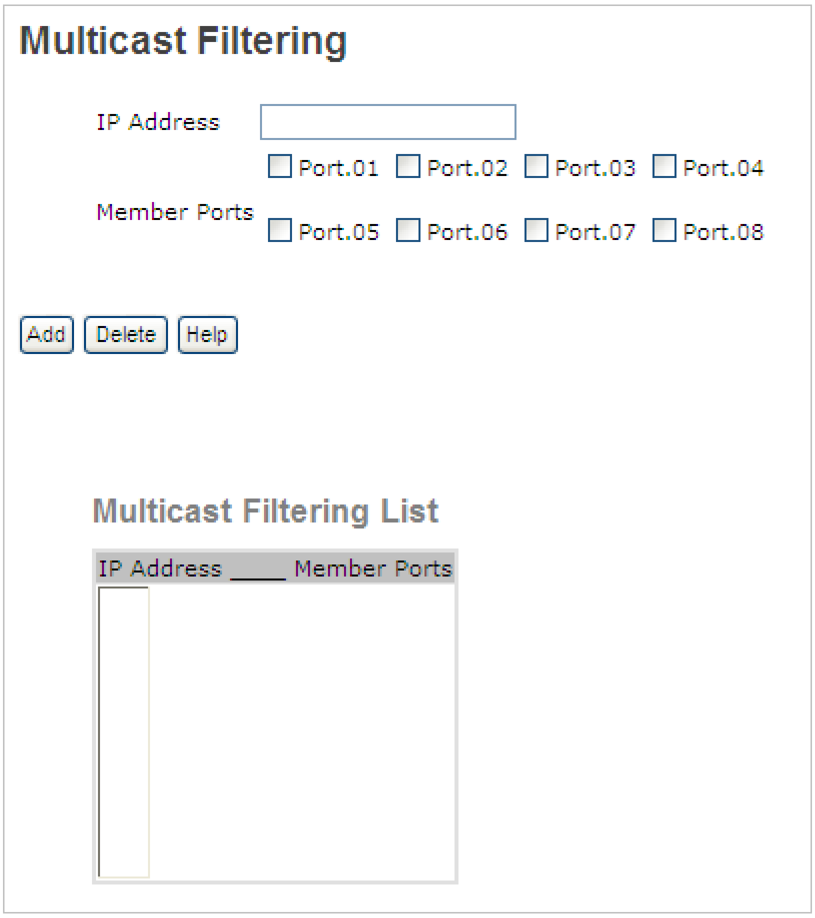
Figure 5-38 IGMP Snooping Configuration interface

The page includes the following fields:

Object	Description
IGMP Snooping	Allows user to enable or disable IGMPv1, v2 or v3.
IGMP Query Mode	Allows user to enable or disable IGMP query. There is should exist one and only one IGMP querier in an IGMP application. The "Auto" mode means that the querier is the one with lower IP address.
IGMP Snooping Table	Display current IP multicast list.
Apply	Click "**Apply**" to activate the configurations.
Help	Click "Help" button to show help file.

5.4.10.2 Multicast Filtering

Multicast filtering is the system by which end stations only receive multicast traffic if they register to join specific multicast groups. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered end stations. Please see Figure 5-39 as following.



Multicast Filtering

IP Address

Member Ports
□ Port.01 □ Port.02 □ Port.03 □ Port.04
□ Port.05 □ Port.06 □ Port.07 □ Port.08

Multicast Filtering List

IP Address ____ Member Ports

Figure 5-39 Multicast Filtering Configuration interface

The page includes the following fields:

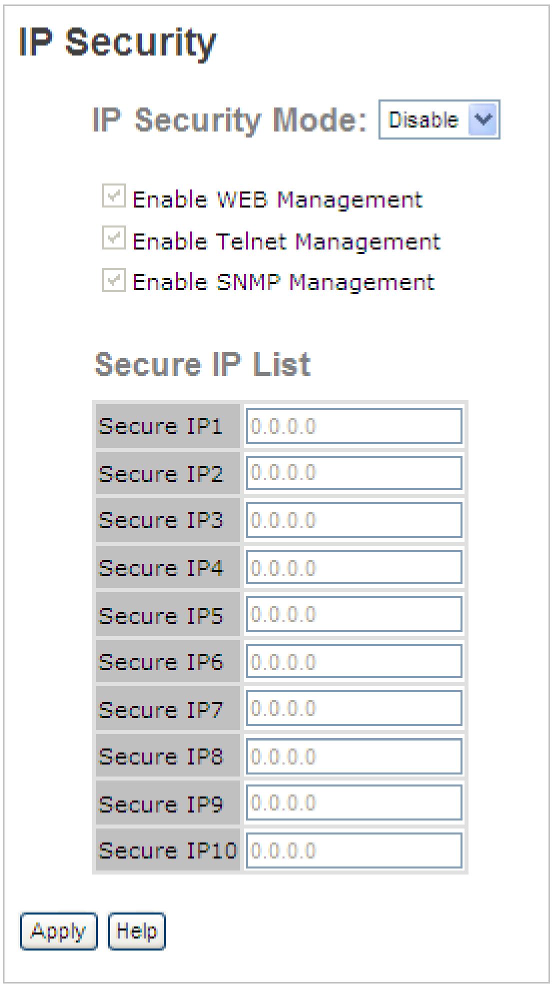
Object	Description
IP Address	Assign a multicast group IP address in the range of 224.0.0.0 ~ 239.255.255.255
Member Port	Tick the check box beside the port number to include them as the member ports in the specific multicast group IP address.
Multicast Filtering List	Show current IP multicast list
Add	Allows user to add multicast group to the list which will be filtered.
Delete	Delete an entry from table
Help	Click "Help" button to show help file.

5.4.11 Security

Five useful functions can enhance security of switch: IP Security, Port Security, MAC Blacklist, and MAC address Aging and 802.1x protocol.

5.4.11.1 IP Security

Only IP in the Secure IP List can manage the switch through your defined management mode. (WEB, Telnet, SNMP). Please see Figure 5-40 as following.



IP Security

IP Security Mode: Disable

☑ Enable WEB Management
☑ Enable Telnet Management
☑ Enable SNMP Management

Secure IP List

Secure IP1	0.0.0.0
Secure IP2	0.0.0.0
Secure IP3	0.0.0.0
Secure IP4	0.0.0.0
Secure IP5	0.0.0.0
Secure IP6	0.0.0.0
Secure IP7	0.0.0.0
Secure IP8	0.0.0.0
Secure IP9	0.0.0.0
Secure IP10	0.0.0.0

Figure 5-40 IP Security Configuration interface

The page includes the following fields:

Object	Description
IP security MODE	Enable/Disable the IP security function.
Enable WEB Management	Mark the blank to enable WEB Management.
Enable Telnet Management	Mark the blank to enable Telnet Management.

Enable SNMP Management	Mark the blank to enable MPSN Management.
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

5.4.11.2 Port Security

Port security is to add static MAC addresses to hardware forwarding database. If port security is enabled at Port Control page, only the frames with MAC addresses in this list will be forwarded, otherwise will be discarded. Please see Figure 5-41 as following.

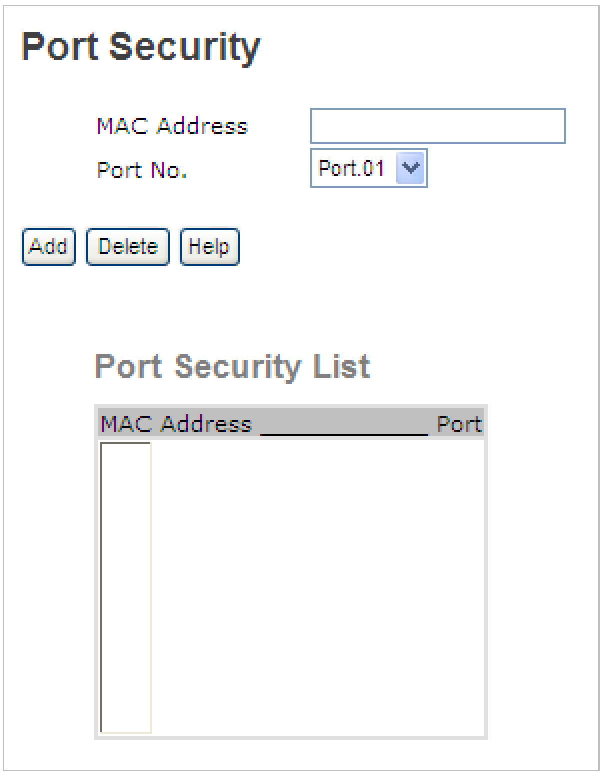


Figure 5-41 Port Security Configuration interface

The page includes the following fields:

Object	Description
MAC Address	Input MAC Address to a specific port.
Port No.	Select port of switch.
Add	Add an entry of MAC and port information.
Delete	Delete the entry.
Help	Show help file.

5.4.11.3 MAC Blacklist

MAC Blacklist can eliminate the traffic forwarding to specific MAC addresses in list. Any frames forwarding to MAC addresses in this list will be discarded. Thus the target device will never receive any frame. Please see Figure 5-42 as following.

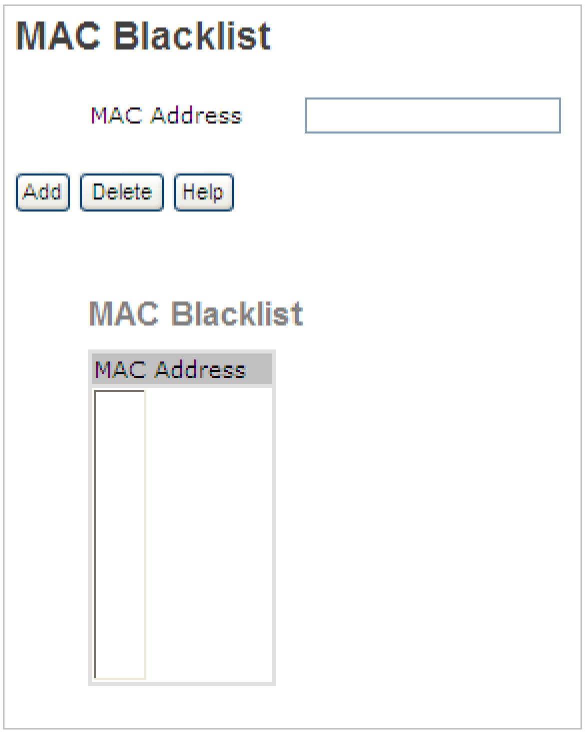


Figure 5-42 MAC Blacklist Configuration interface

The page includes the following fields:

Object	Description
MAC Address	Input MAC Address to add to MAC Blacklist.
Port NO.	Select port of switch.
Add	Add an entry to Blacklist table.
Delete	Delete the entry.
Help	Show help file.

5.4.11.4 802.1x

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).

Understanding IEEE 802.1X Port-Based Authentication

The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.

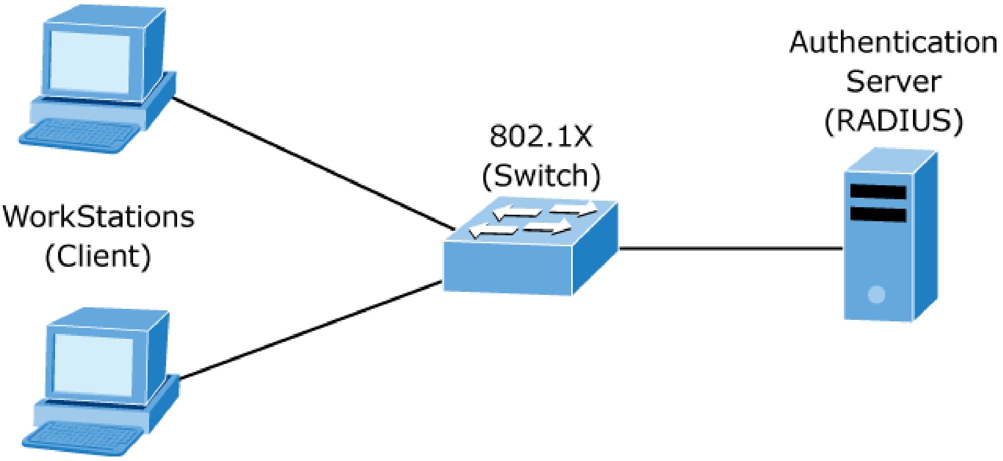
Until the client is authenticated, 802.1X access control allows only **Extensible Authentication Protocol over LAN (EAPOL)** traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

This section includes this conceptual information:

- Device Roles
- Authentication Initiation and Message Exchange
- Ports in Authorized and Unauthorized States

■ **Device Roles**

With 802.1X port-based authentication, the devices in the network have specific roles as shown below.



Client—the device (workstation) that requests access to the LAN and switch services and responds to requests from the switch. The workstation must be running 802.1X-compliant client software such as that offered in the Microsoft Windows XP operating system. (The client is the supplicant in the IEEE 802.1X specification.)

- ***Authentication server***—performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. In this release, the Remote Authentication Dial-In User Service (RADIUS) security system with **Extensible Authentication Protocol (EAP)** extensions is the only supported authentication server; it is available in Cisco Secure Access Control Server version 3.0. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

- ***Switch* (802.1X device)**—controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client. The switch includes the RADIUS client, which is responsible for encapsulating and decapsulating the Extensible Authentication Protocol (EAP) frames and interacting with the authentication server. When the switch receives EAPOL frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame is re-encapsulated in the RADIUS format. The EAP frames are not modified or examined during encapsulation, and the authentication server must support EAP within the native frame format. When the switch receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

■ Authentication Initiation and Message Exchange

The switch or the client can initiate authentication. If you enable authentication on a port by using the **dot1x port-control auto** interface configuration command, the switch must initiate authentication when it determines that the port link state transitions from down to up. It then sends an EAP-request/identity frame to the client to request its identity (typically, the switch sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the client responds with an EAP-response/identity frame.

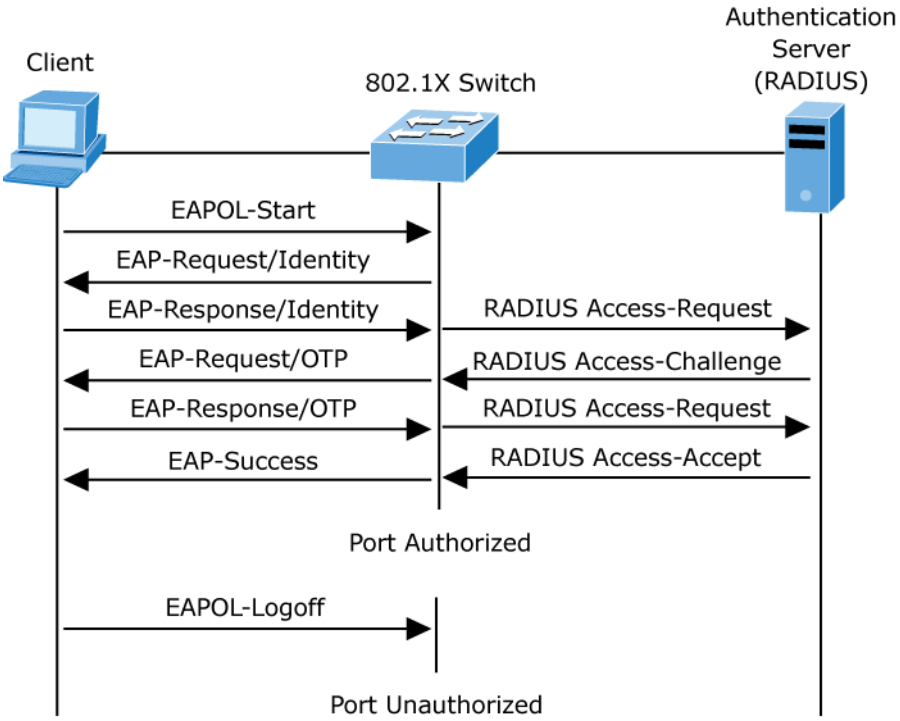
However, if during bootup, the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client's identity.

Note

If 802.1X is not enabled or supported on the network access device, any EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client transmits frames as if the port is in the authorized state. A port in the authorized state effectively means that the client has been successfully authenticated.

When the client supplies its identity, the switch begins its role as the intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized.

The specific exchange of EAP frames depends on the authentication method being used. Following image shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.



■ **Ports in Authorized and Unauthorized States**

The switch port state determines whether or not the client is granted access to the network. The port starts in the unauthorized state. While in this state, the port disallows all ingress and egress traffic except for 802.1X protocol packets. When a client is successfully authenticated, the port transitions to the authorized state, allowing all traffic for the client to flow normally.

If a client that does not support 802.1X is connected to an unauthorized 802.1X port, the switch requests the client's identity. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an 802.1X-enabled client connects to a port that is not running the 802.1X protocol, the client initiates the authentication process by sending the EAPOL-start frame. When no response is received, the client sends the request for a fixed number of times. Because no response is received, the client begins sending frames as if the port is in the authorized state

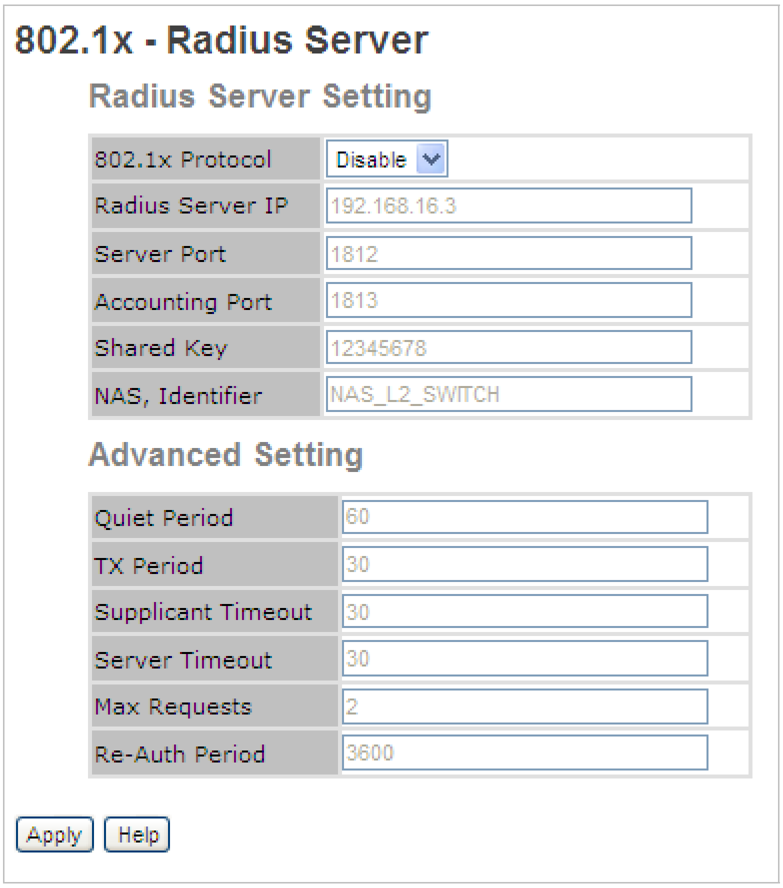
If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

When a client logs off, it sends an EAPOL-logoff message, causing the switch port to transition to the unauthorized state.

If the link state of a port transitions from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

802.1x Radius Server

802.1x makes the use of the physical access characteristics of IEEE802 LAN infrastructures in order to provide a authenticated and authorized devices attached to a LAN port. Please refer to IEEE 802.1X - Port Based Network Access Control. Please see Figure 5-43 as following.



802.1x - Radius Server

Radius Server Setting

802.1x Protocol	Disable
Radius Server IP	192.168.16.3
Server Port	1812
Accounting Port	1813
Shared Key	12345678
NAS, Identifier	NAS_L2_SWITCH

Advanced Setting

Quiet Period	60
TX Period	30
Supplicant Timeout	30
Server Timeout	30
Max Requests	2
Re-Auth Period	3600

Figure 5-42 802.1x - Radius Server Configuration interface

The page includes the following fields:

Radius Server Setting:

Object	Description
Radius Server IP	The IP address of the authentication server.
Server port	Set the UDP port number used by the authentication server to authenticate.
Account port	Set the UDP destination port for accounting requests to the specified Radius Server.

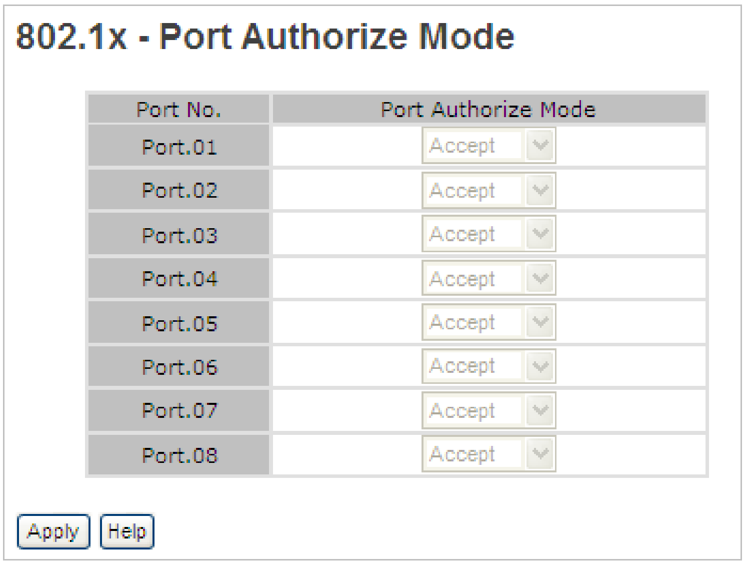
Shared Key	A key shared between this switch and authentication server.
NAS, Identifier	A string used to identify this switch.

Advanced Setting:

Object	Description
Quiet Period	Set the time interval between authentication failure and the start of a new authentication attempt.
Tx Period	Set the time that the switch can wait for response to an EAP request/identity frame from the client before resending the request.
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 Radius server response to an authentication request.
Max Requests	Set the maximum number of times to retry sending packets to the supplicant.
Re-Auth Period	Set the period of time after which clients connected must be re-authenticated.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.4.11.5 802.1x – Port Authorize Mode

This section allows user to set the 802.1x authorized mode of each port. Please see Figure 5-44 as following.



802.1x - Port Authorize Mode

Port No.	Port Authorize Mode
Port.01	Accept
Port.02	Accept
Port.03	Accept
Port.04	Accept
Port.05	Accept
Port.06	Accept
Port.07	Accept
Port.08	Accept

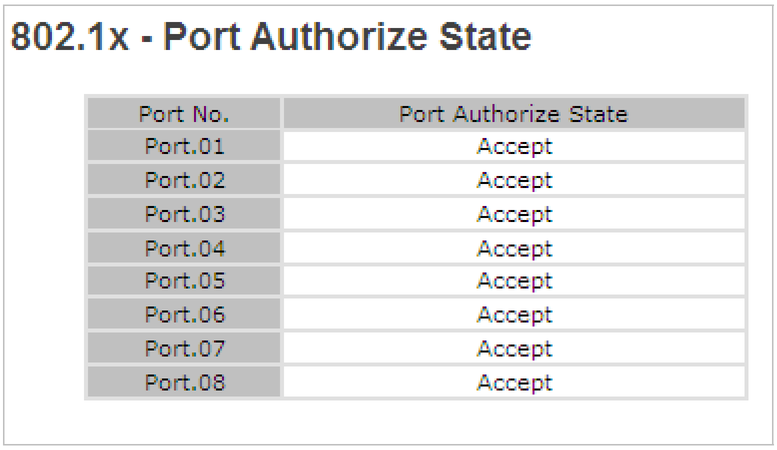
Figure 5-44 802.1x – Port Authorize Mode Configuration interface

The page includes the following fields:

Object	Description
Port Authorized Mode	■ **Reject:** force this port to be unauthorized. ■ **Accept:** force this port to be authorized. ■ **Authorize:** the state of this port was determined by the outcome of the 802.1x authentication. ■ **Disable:** this port will not participate in 802.1x.
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.4.11.6 802.1x – Port Authorize State

This section allows user to set the 802.1x authorized mode of each port. Please see Figure 5-45 as following.



802.1x - Port Authorize State

Port No.	Port Authorize State
Port.01	Accept
Port.02	Accept
Port.03	Accept
Port.04	Accept
Port.05	Accept
Port.06	Accept
Port.07	Accept
Port.08	Accept

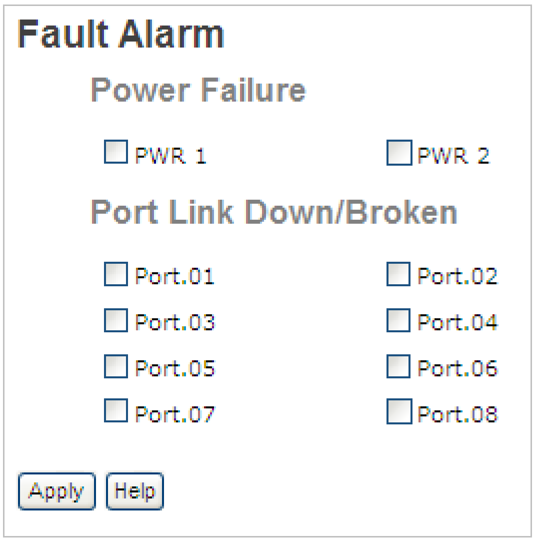
Figure 5-45 802.1x – Port Authorize State Table

5.4.12 Warning

Warning function is very important for managing switch. You can manage switch by SYSLOG, E-MAIL, and Fault Relay. It helps you to monitor the switch status on remote site. When events occurred, the warning message will send to your appointed server, E-MAIL, or relay fault to switch panel.

5.4.12.1 Fault Alarm

When any selected fault event is happened, the Fault LED in switch panel will light up and the electric relay will signal at the same time. Please see Figure 5-46 as following.



Fault Alarm

Power Failure

□ PWR 1 □ PWR 2

Port Link Down/Broken

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

Figure 5-46 Fault Alarm Configuration interface

The page includes the following fields:

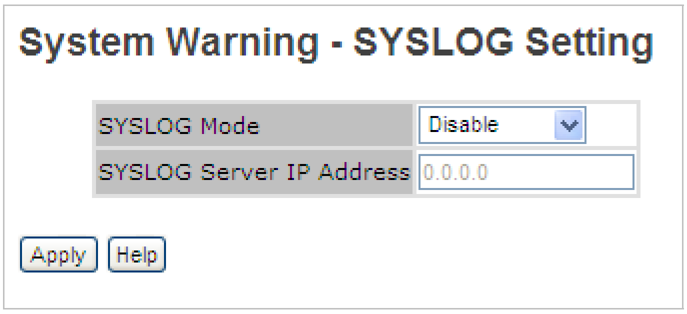
Object	Description
Power Failure	Mark the blank of PWR 1 or PWR 2 to monitor.
Port Link Down/Broken	Mark the blank of port 1 to port 8 to monitor.
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

5.4.12.2 System Warning

System alarm support two warning mode: 1. SYSLOG. 2. E-MAIL. You can monitor switch through selected system events.

System Warning – SYSLOG Setting

The SYSLOG is a protocol to transmit event notification messages across networks. Please refer to RFC 3164 - The BSD SYSLOG Protocol. Please see Figure 5-47 as following.



System Warning - SYSLOG Setting

SYSLOG Mode	Disable
SYSLOG Server IP Address	0.0.0.0

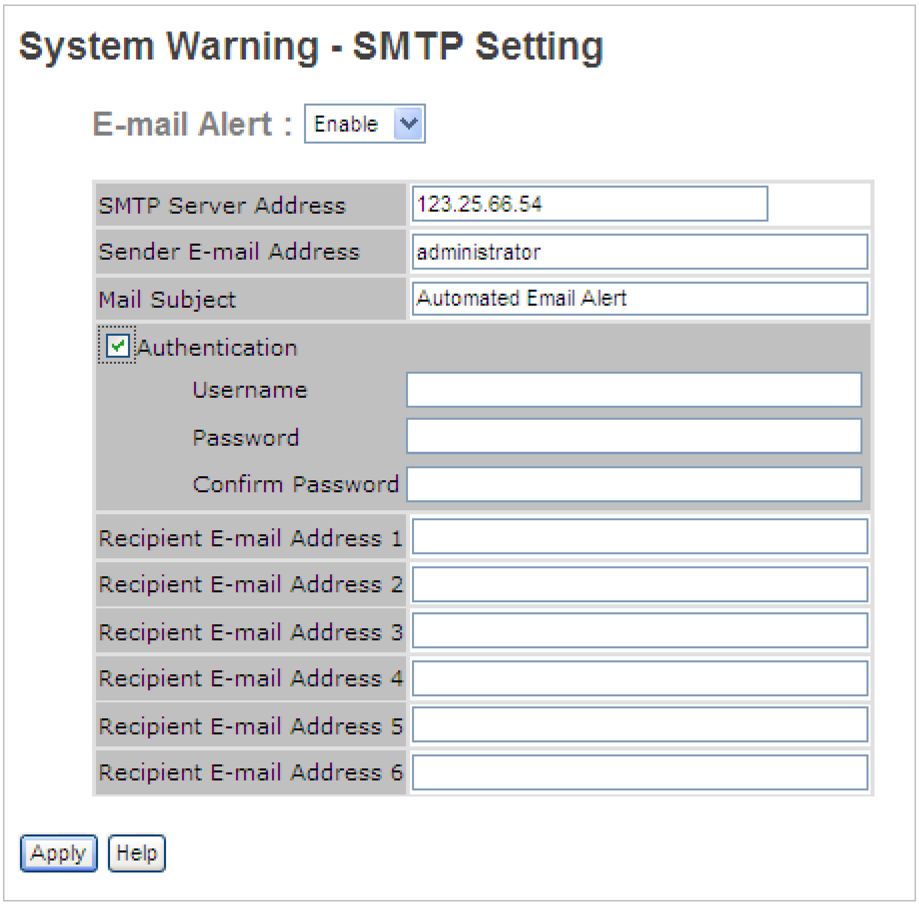
Figure 5-47 System Warning - Syslog Setting Configuration interface

The page includes the following fields:

Object	Description
SYSLOG Mode	■ **Disable:** disable SYSLOG. ■ **Client Only:** log to local system. ■ **Server Only:** log to a remote SYSLOG server. ■ **Both:** log to both of local and remote server.
SYSLOG Server IP Address	The remote SYSLOG Server IP address.
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

System Warning – SMTP Setting

The SMTP is Short for Simple Mail Transfer Protocol. It is a protocol for e-mail transmission across the Internet. Please refer to RFC 821 - Simple Mail Transfer Protocol. Please see Figure 5-48 as following.



System Warning - SMTP Setting

E-mail Alert : Enable

SMTP Server Address	123.25.66.54
Sender E-mail Address	administrator
Mail Subject	Automated Email Alert
☑ Authentication	
Username	
Password	
Confirm Password	
Recipient E-mail Address 1	
Recipient E-mail Address 2	
Recipient E-mail Address 3	
Recipient E-mail Address 4	
Recipient E-mail Address 5	
Recipient E-mail Address 6	

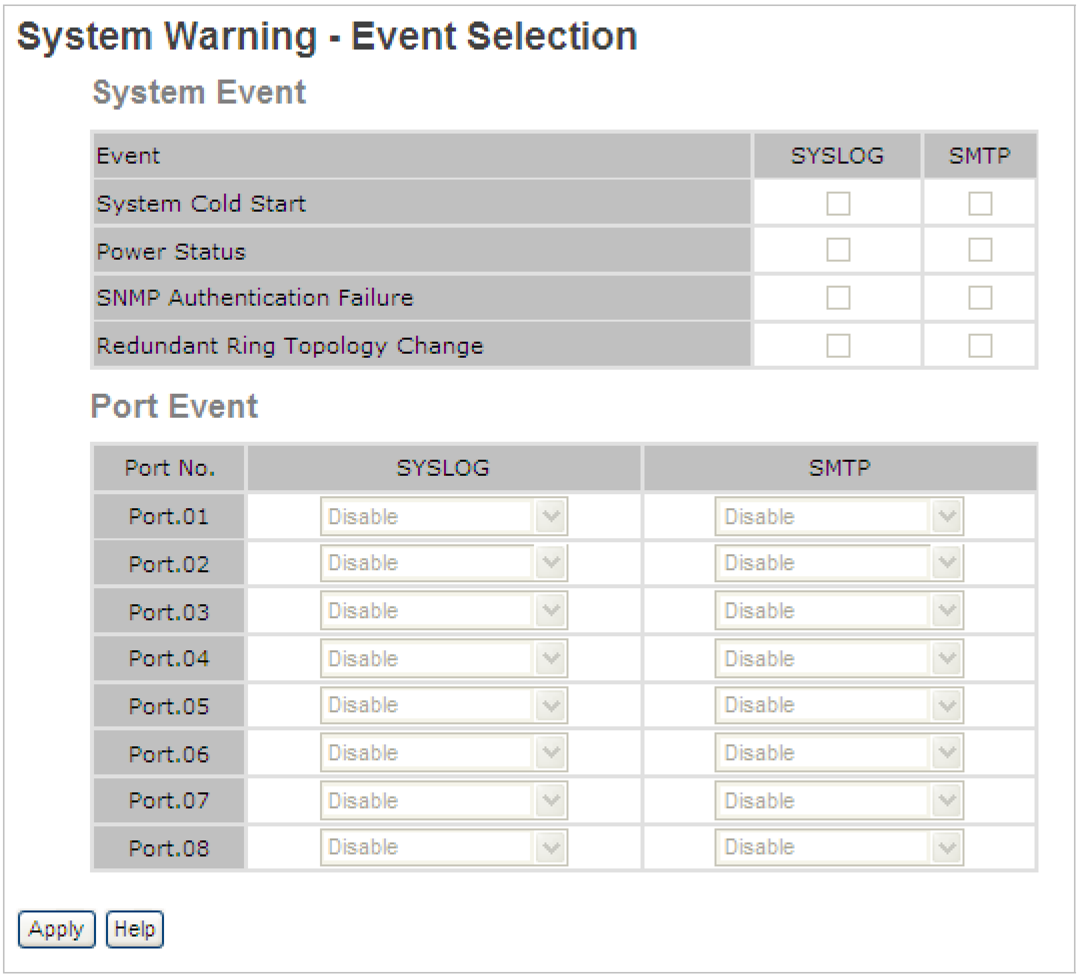
Figure 5-48 System Warning - SMTP Setting Configuration interface

The page includes the following fields:

Object	Description
E-mail Alarm	Enable/Disable transmission system warning events by e-mail.
Sender E-mail Address	The SMTP server IP address
Mail Subject	The Subject of the mail
Authentication	As default, the authentication is disabled. User should enable this function and input relating account information when user wants alarm mail relay to different domain with sender e-mail address. ■ **Username:** the authentication username. ■ **Password:** the authentication password. ■ **Confirm Password:** re-enter password.
Recipient E-mail Address	The recipient's E-mail address. It supports 6 recipients for a mail.
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

System Warning – Event Selection

SYSLOG and SMTP are the two warning methods that supported by the system. Check the corresponding box to enable system event warning method you wish to choose. Please note that the checkbox can not be checked when SYSLOG or SMTP is disabled. Please see Figure 5-49 as following.



System Warning - Event Selection

System Event

Event	SYSLOG	SMTP
System Cold Start	□	□
Power Status	□	□
SNMP Authentication Failure	□	□
Redundant Ring Topology Change	□	□

Port Event

Port No.	SYSLOG	SMTP
Port.01	Disable	Disable
Port.02	Disable	Disable
Port.03	Disable	Disable
Port.04	Disable	Disable
Port.05	Disable	Disable
Port.06	Disable	Disable
Port.07	Disable	Disable
Port.08	Disable	Disable

Figure 5-49 System Warning – Event Selection Configuration interface

The page includes the following fields:

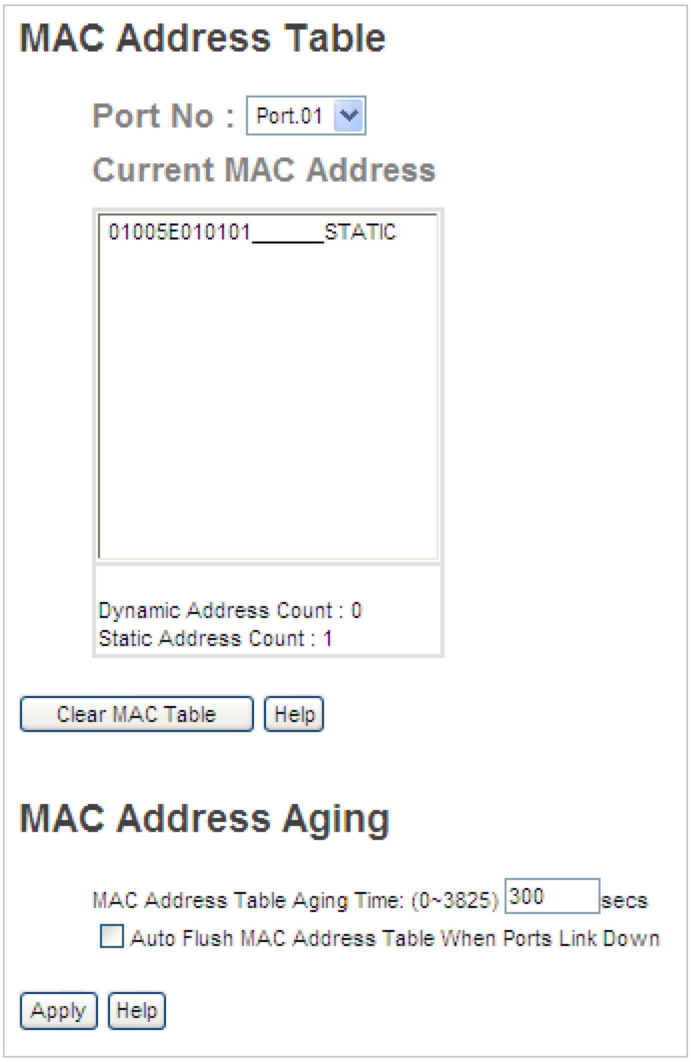
Object	Description
System Cold Start	Alert when system restart
Power Status	Alert when a power up or down
SNMP Authentication Failure	Alert when SNMP authentication failure.
S-Ring Topology Change	Alert when S-Ring topology changes.
Port Event	■ **Disable** ■ **Link Up** ■ **Link Down**

■ **Link Up & Link Down**	
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

5.4.13 Monitor and Diagnosis (Diag)

5.4.13.1 MAC Address Table

The MAC Address Table, that is Filtering Database, supports queries by the Forwarding Process, as to whether a frame received by a given port with a given destination MAC address is to be forwarded through a given potential transmission port. Please see Figure 5-50 as following



MAC Address Table

Port No : Port.01

Current MAC Address

01005E010101______STATIC

Dynamic Address Count : 0
Static Address Count : 1

MAC Address Aging

MAC Address Table Aging Time: (0~3825) 300 secs

□ Auto Flush MAC Address Table When Ports Link Down

Figure 5-50 MAC Address Table Configuration interface

The page includes the following fields:

Object	Description
Port No.	Show all MAC addresses mapping to a selected port in table.
Clear MAC Table	Clear all MAC addresses in table
Help	Show help file.

MAC Address Aging

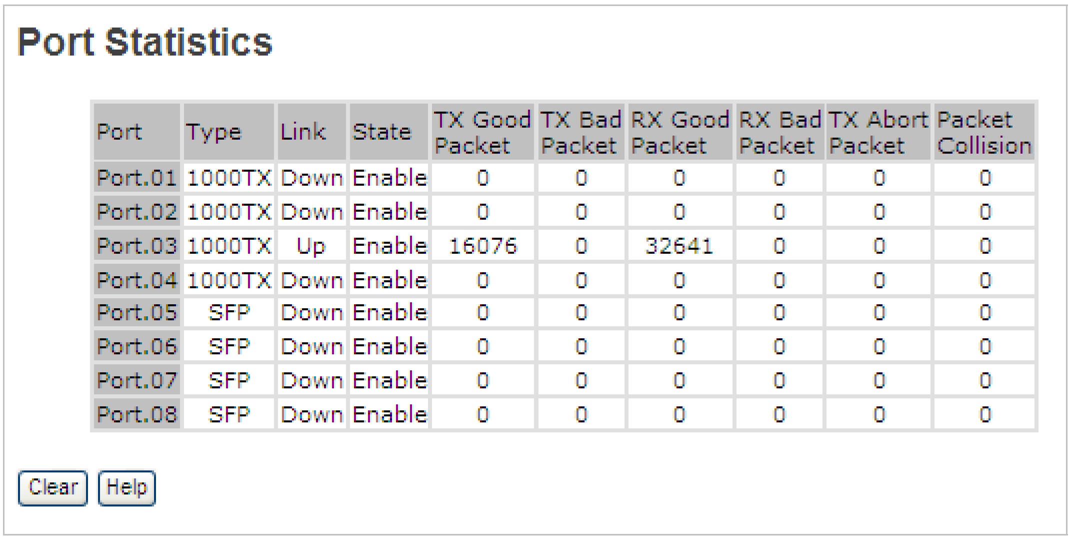
You can set MAC Address aging timer, as time expired, the unused MAC will be cleared from MAC table. SW-M series also support Auto Flush MAC Address Table When ports Link Down. Please see Figure 5-50 as following

The page includes the following fields:

Object	Description
MAC Address Table Aging Time: (0to3825)	Set the timer.
Auto Flush MAC Address Table When ports Link Down.	Mark the blank to enable the function,
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

5.4.13.2 Port Statistics

Port statistics show several statistics counters for all ports. Please see Figure 5-51 as following



Port Statistics

Port	Type	Link	State	TX Good Packet	TX Bad Packet	RX Good Packet	RX Bad Packet	TX Abort Packet	Packet Collision
Port.01	1000TX	Down	Enable	0	0	0	0	0	0
Port.02	1000TX	Down	Enable	0	0	0	0	0	0
Port.03	1000TX	Up	Enable	16076	0	32641	0	0	0
Port.04	1000TX	Down	Enable	0	0	0	0	0	0
Port.05	SFP	Down	Enable	0	0	0	0	0	0
Port.06	SFP	Down	Enable	0	0	0	0	0	0
Port.07	SFP	Down	Enable	0	0	0	0	0	0
Port.08	SFP	Down	Enable	0	0	0	0	0	0

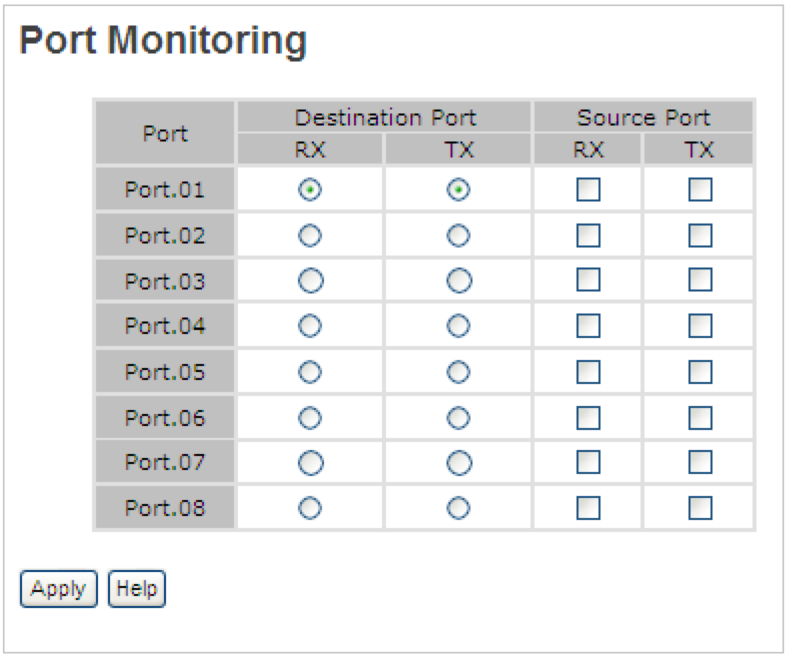
Figure 5-51 MAC Address Table Configuration interface

The page includes the following fields:

Object	Description
Type	Show port speed and media type.
Link	Show port link status.
State	Show ports enable or disable.
TX GOOD Packet	The number of good packets sent by this port.
TX Bad Packet	The number of bad packets sent by this port.
RX GOOD Packet	The number of good packets received by this port.
RX Bad Packet	The number of bad packets received by this port.
TX Abort Packet	The number of packets aborted by this port.
Packet Collision	The number of times a collision detected by this port.
Clear	Clear all counters.
Help	Show help file.

5.4.13.3 Port Monitor

Port monitoring does support TX (egress) only, RX (ingress) only and TX/RX monitoring. TX monitoring sends any data that egress out checked TX source ports to a selected TX destination port as well. RX monitoring sends any data that ingress in checked RX source ports out to a selected RX destination port as well as sending the frame where it normally would have gone.   Note that keep all source ports unchecked in order to disable port monitoring. Please see Figure 5-52 as following



Port Monitoring

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

Figure 5-52 Port Monitor Configuration interface

The page includes the following fields:

Object	Description
Destination Port	The port will receive a copied frame from source port for monitoring purpose.
Source Port	The port will be monitored. Mark the blank of TX or RX to be monitored.
TX	The frames come into switch port.
RX	The frames receive by switch port.
Apply	Click "**Apply**" to set the configurations.
Clear	Clear all marked blank.(disable the function)
Help	Show help file.

5.4.13.4 System Event Log

If system log client is enabled, the system event logs will show in this table. Please see Figure 5-53 as following

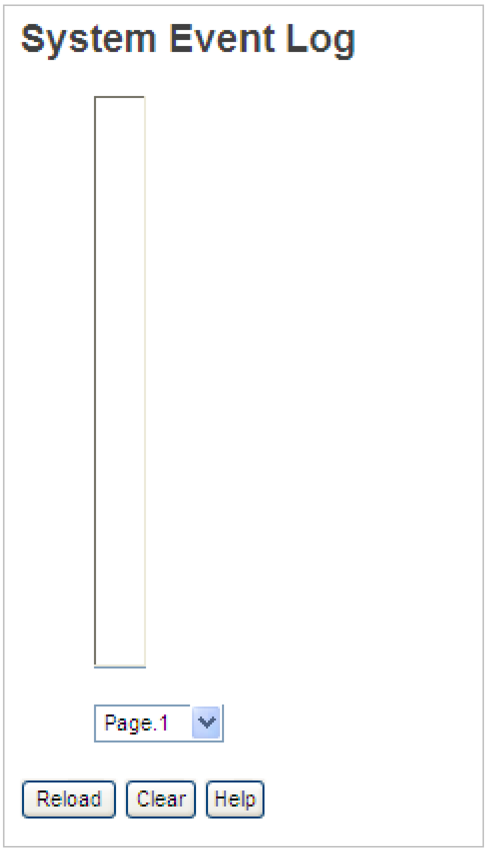


Figure 5-53 Port Monitor Configuration interface

The page includes the following fields:

Object	Description
Page	Select LOG page.
Reload	To get the newest event logs and refresh this page.
Clear	Clear log.
Help	Show help file.

5.4.14 Save Configuration

If any configuration changed, "**Save Configuration**" should be clicked to save current configuration data to the permanent flash memory. Otherwise, the current configuration will be lost when power off or system reset. Please see Figure 5-54 as following

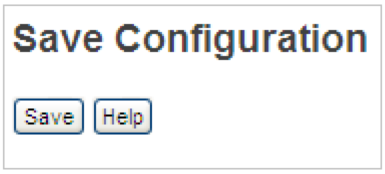

Save Configuration

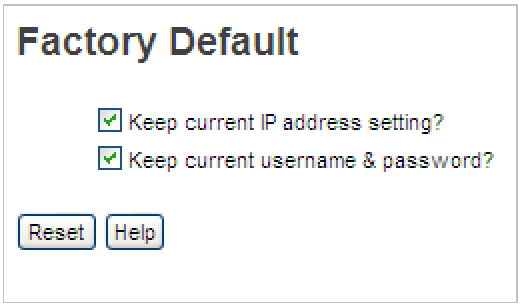
Figure 5-54 Save Configuration Configuration interface

The page includes the following fields:

Object	Description
Save	Allows user to save system configuration to flash.
Help	Show help file.

5.4.15 Factory Default

Reset switch to default configuration. Click **Reset** button to reset all configurations to the default value. You can select "**Keep current IP address setting**" and "**Keep current username & password**" to prevent IP and username and password form default. Please see Figure 5-55 as following.

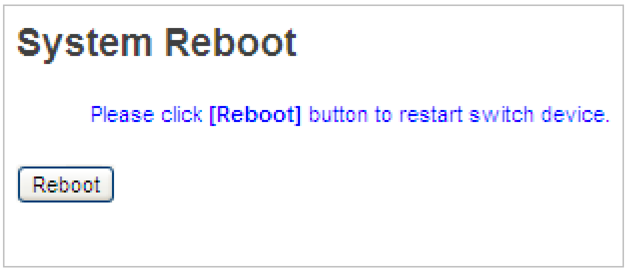

Factory Default

☑ Keep current IP address setting?
☑ Keep current username & password?

Figure 5-55 Save Configuration interface

5.4.16 System Reboot

This section allows user to press **Reboot** button to reboot system. Please see Figure 5-56 as following.



System Reboot

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

Figure 5-56 Save Configuration interface

6. Command Sets

Commands Level

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

Commands Set List

Mode	Symbol of Command Level
User EXEC	E
Privileged EXEC	P
Global configuration	G
VLAN database	V
Interface configuration	I

6.1 System Commands Set

Commands	Level	Description	Example
show config	**E**	Show switch configuration	switch>show config
show terminal	**P**	Show console information	switch#show terminal
menu	**E**	Enter MENU mode	switch>menu
write memory	**P**	Save your 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 lowip **[Low IP]**	**G**	Configure low IP address for IP pool	switch(config)# dhcpserver lowip 192.168.1.1
dhcpserver highip **[High IP]**	**G**	Configure high IP address for IP pool	switch(config)# dhcpserver highip 192.168.1.50
dhcpserver subnetmask **[Subnet mask]**	**G**	Configure subnet mask for DHCP clients	switch(config)#dhcpserver subnetmask 255.255.255.0
dhcpserver gateway **[Gateway]**	**G**	Configure gateway for DHCP clients	switch(config)#dhcpserver gateway 192.168.1.254
dhcpserver dnsip **[DNS IP]**	**G**	Configure DNS IP for DHCP clients	switch(config)# dhcpserver dnsip 192.168.1.1
dhcpserver leasetime **[Hours]**	**G**	Configure lease time (in hour)	switch(config)#dhcpserver leasetime 1
dhcpserver ipbinding **[IP address]**	**I**	Set static IP for DHCP clients by port	switch(config)#interface fastEthernet 2 switch(config-if)#dhcpserver ipbinding 192.168.1.1
show dhcpserver configuration	**P**	Show configuration of DHCP server	switch#show dhcpserver configuration
show dhcpserver clients	**P**	Show client entries of DHCP server	switch#show dhcpserver clinets
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	**G**	Set the IP security list	switch(config)#security ip 1 192.168.1.55

[Index(1..10)] [IP Address]			
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

6.2 Port Commands Set

Commands	Level	Description	Example
interface fastEthernet [Portid]	G	Choose the port for modification.	switch(config)#interface fastEthernet 2
duplex [full | half]	I	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#interface fastEthernet 2 switch(config-if)#duplex full
speed [10|100|1000|auto]	I	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can't be set to 1000 if the port isn't a giga port..	switch(config)#interface fastEthernet 2 switch(config-if)#speed 100
flowcontrol mode [Symmetric|Asymmetric]	I	Use the flowcontrol configuration command on Ethernet ports to control traffic rates during congestion.	switch(config)#interface fastEthernet 2 switch(config-if)#flowcontrol mode Asymmetric
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	switch(config)#interface fastEthernet 2 switch(config-if)#state Disable

		command to specify the state mode of operation for Ethernet ports. Use the disable form of this command to disable the port.	
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

6.3 Trunk Commands Set

Commands	Level	Description	Example
aggregator priority **[1to65535]**	G	Set port group system priority	switch(config)#aggregator priority 22
aggregator activityport **[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] :1to3 [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] :1to3 [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)#aggreator group 1 3,1,2 nolacp
show aggregator	P	Show the information of trunk group	switch#show aggregator
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

6.4 VLAN Commands Set

Commands	Level	Description	Example
vlan database	**P**	Enter VLAN configure mode	switch#vlan database
vlan **[8021q | gvrp]**	**V**	To set switch VLAN mode.	switch(vlan)# vlanmode 8021q or switch(vlan)# vlanmode gvrp
no vlan **[VID]**	**V**	Disable vlan group(by VID)	switch(vlan)#no vlan 2
no gvrp	**V**	Disable GVRP	switch(vlan)#no gvrp
IEEE 802.1Q VLAN			
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.	switch(vlan)# vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q port 3 hybrid-link untag 5 tag 6-8
vlan 8021q aggreator **[TrunkID]** **access-link untag** **[UntaggedVID]**	**V**	Assign a access link for VLAN by trunk group	switch(vlan)#vlan 8021q aggreator 3 access-link untag 33
vlan 8021q aggreator **[TrunkID]** **trunk-link tag** **[TaggedVID List]**	**V**	Assign a trunk link for VLAN by trunk group	switch(vlan)#vlan 8021q aggreator 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q aggreator 3 trunk-link tag 3-20
vlan 8021q aggreator **[PortNumber]** **hybrid-link untag**	**V**	Assign a hybrid link for VLAN by trunk group	switch(vlan)# vlan 8021q aggreator 3 hybrid-link untag 4 tag 3,6,8 or

[UntaggedVID] **tag** [TaggedVID List]			switch(vlan)# vlan 8021q aggreator 3 hybrid-link untag 5 tag 6-8
show vlan [VID] or **show vlan**	V	Show VLAN information	switch(vlan)#show vlan 23

6.5 Spanning Tree Commands Set

Commands	Level	Description	Example
spanning-tree enable	G	Enable spanning tree	switch(config)#spanning-tree enable
spanning-tree priority [0to61440]	G	Configure spanning tree priority parameter	switch(config)#spanning-tree priority 32767
spanning-tree max-age [seconds]	G	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	switch(config)# spanning-tree max-age 15
spanning-tree hello-time [seconds]	G	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#spanning-tree hello-time 3
spanning-tree forward-time [seconds]	G	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified	switch(config)# spanning-tree forward-time 20

		spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	
stp-path-cost **[1to200000000]**	**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 127
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**	Display a summary of the spanning-tree states.	switch>show spanning-tree
no spanning-tree	**G**	Disable spanning-tree.	switch(config)#no spanning-tree

6.6 QOS Commands Set

Commands	Level	Description	Example
qos policy [weighted-fair|strict]	G	Select QOS policy scheduling	switch(config)#qos policy weighted-fair
qos prioritytype [port-based|cos-only|tos-only|cos-first|tos-first]	G	Setting of QOS priority type	switch(config)#qos prioritytype
qos priority portbased [Port] [lowest|low|middle|high]	G	Configure Port-based Priority	switch(config)#qos priority portbased 1 low
qos priority cos [Priority][lowest|low|middle|high]	G	Configure COS Priority	switch(config)#qos priority cos 22 middle
qos priority tos [Priority][lowest|low|middle|high]	G	Configure TOS Priority	switch(config)#qos priority tos 3 high
show qos	P	Display the information of QoS configuration	switch>show qos
no qos	G	Disable QoS function	switch(config)#no qos

6.7 IGMP Commands Set

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

6.8 MAC / Filter Table Commands Set

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

6.9 SNMP Commands Set

Commands	Level	Description	Example
snmp agent-mode **[v1v2c | v3]**	G	Select the agent mode of SNMP	switch(config)#snmp agent-mode v1v2c
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 192.168.10.50 community public trap-version v1 (remove) Switch(config)# no snmp-server host 192.168.10.50
snmp community-strings **[Community-string]** **right** **[RO|RW]**	G	Configure the community string right	switch(config)#snmp community-strings public right RO or switch(config)#snmp community-strings

			public right RW
snmp snmpv3-user [User Name] **password** [Authentication Password] [Privacy Password]	**G**	Configure the userprofile for SNMPV3 agent. Privacy password could be empty.	switch(config)#snmp snmpv3-user test01 password AuthPW PrivPW
show snmp	**P**	Show SNMP configuration	switch#show snmp
show snmp-server	**P**	Show specified trap server information	switch#show snmp-server
no snmp community-strings [Community]	**G**	Remove the specified community.	switch(config)#no snmp community-strings public
no snmp snmpv3-user [User Name] **password** [Authentication Password] [Privacy Password]	**G**	Remove specified user of SNMPv3 agent. Privacy password could be empty.	switch(config)# no snmp snmpv3-user test01 password AuthPW PrivPW
no snmp-server host [Host-address]	**G**	Remove the SNMP server host.	switch(config)#no snmp-server 192.168.10.50

6.10 Port Mirroring Commands Set

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

6.11 802.1x Commands Set

Commands	Level	Description	Example
8021x enable	**G**	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# 8021x enable
8021x system radiousip **[IP address]**	**G**	Use the 802.1x system radious IP global configuration command to change the radious server IP.	switch(config)# 8021x system radiousip 192.168.1.1
8021x system serverport **[port ID]**	**G**	Use the 802.1x system server port global configuration command to change the radious server port	switch(config)# 8021x system serverport 1815
8021x system accountport **[port ID]**	**G**	Use the 802.1x system account port global configuration command to change the accounting port	switch(config)# 8021x system accountport 1816
8021x system sharekey **[ID]**	**G**	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)# 8021x system sharekey 123456
8021x system nasid **[words]**	**G**	Use the 802.1x system nasid global configuration command to change the NAS ID	switch(config)# 8021x system nasid test1
8021x misc quietperiod **[sec.]**	**G**	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch(config)# 8021x misc quietperiod 10
8021x misc txperiod **[sec.]**	**G**	Use the 802.1x misc TX period global configuration command to set the TX period.	switch(config)# 8021x misc txperiod 5
8021x misc supportimeout	**G**	Use the 802.1x misc supp	switch(config)# 8021x misc supportimeout

[sec.]		timeout global configuration command to set the supplicant timeout.	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**	Display 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

6.12 TFTP Commands Set

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

6.13 SystemLog, SMTP and Event Commands Set

Commands	Level	Description	Example
systemlog ip **[IP address]**	G	Set System log server IP address.	switch(config)# systemlog ip 192.168.1.100
systemlog mode **[client|server|both]**	G	Specified the log mode	switch(config)# systemlog mode both
show systemlog	E	Display system log.	Switch>show systemlog
show systemlog	P	Show system log client & server information	switch#show systemlog
no systemlog	G	Disable systemlog functon	switch(config)#no systemlog
smtp enable	G	Enable SMTP function	switch(config)#smtp enable
smtp serverip **[IP address]**	G	Configure SMTP server IP	switch(config)#smtp serverip 192.168.1.5
smtp authentication	G	Enable SMTP authentication	switch(config)#smtp authentication
smtp account **[account]**	G	Configure authentication account	switch(config)#smtp account User
smtp password **[password]**	G	Configure authentication password	switch(config)#smtp password
smtp rcptemail	G	Configure Rcpt e-mail	switch(config)#smtp rcptemail 1

[Index] [Email address]		Address	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 s 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 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

6.14 SNTP Commands Set

Commands	Level	Description	Example
sntp enable	**G**	Enable SNTP function	switch(config)#sntp enable
sntp daylight	**G**	Enable daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight

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

6.15 Ring Commands Set

Commands	Level	Description	Example
Ring enable	**G**	Enable 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 Ring	switch#show Ring
no Ring	**G**	Disable 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

7. SWITCH OPERATION

7.1 Address Table

The Switch is implemented with an address table. This address table composed of many entries. Each entry is used to store the address information of some node in network, including MAC address, port no, etc. This in-formation comes from the learning process of Ethernet Switch.

7.2 Learning

When one packet comes in from any port, the Switch will record the source address, port no. And the other related information in address table. This information will be used to decide either forwarding or filtering for future packets.

7.3 Forwarding & Filtering

When one packet comes from some port of the Ethernet Switching, it will also check the destination address besides the source address learning. The Ethernet Switching will lookup the address-table for the destination address. If not found, this packet will be forwarded to all the other ports except the port, which this packet comes in. And these ports will transmit this packet to the network it connected. If found, and the destination address is located at different port from this packet comes in, the Ethernet Switching will forward this packet to the port where this destination address is located according to the information from address table. But, if the destination address is located at the same port with this packet comes in, then this packet will be filtered. Thereby increasing the network throughput and availability

7.4 Store-and-Forward

Store-and-Forward is one type of packet-forwarding techniques. A Store-and-Forward Ethernet Switching stores the incoming frame in an internal buffer, do the complete error checking before transmission. Therefore, no error packets occurrence, it is the best choice when a network needs efficiency and stability.

The Ethernet Switch scans the destination address from the packet-header, searches the routing table pro-vided for the incoming port and forwards the packet, only if required. The fast forwarding makes the switch attractive for connecting servers directly to the network, thereby increasing throughput and availability. How-ever, the switch is most commonly used to segment existence hubs, which nearly always improves overall performance. An Ethernet Switching can be easily configured in any Ethernet network environment to signifi-cantly boost bandwidth using conventional cabling and adapters.

Due to the learning function of the Ethernet switching, the source address and corresponding port number of each incoming and outgoing packet are stored in a routing table. This information is subsequently used to filter packets whose destination address is on the same segment as the source address. This confines network traffic to its respective domain and reduce the overall load on the network.

The Switch performs "Store and forward" therefore, no error packets occur. More reliably, it reduces the re-transmission rate. No packet loss will occur.

7.5 Auto-Negotiation

The STP ports on the Switch have built-in "Auto-negotiation". This technology automatically sets the best possible bandwidth when a connection is established with another network device (usually at Power On or Reset). This is done by detect the modes and speeds at the second of both device is connected and capable of, both 10Base-T and 100Base-TX devices can connect with the port in either Half- or Full-Duplex mode.

If attached device is:	100Base-TX port will set to:
10Mbps, no auto-negotiation	10Mbps.
10Mbps, with auto-negotiation	10/20Mbps (10Base-T/Full-Duplex)
100Mbps, no auto-negotiation	100Mbps
100Mbps, with auto-negotiation	100/200Mbps (100Base-TX/Full-Duplex)

Appendix A—RJ-45 Pin Assignment

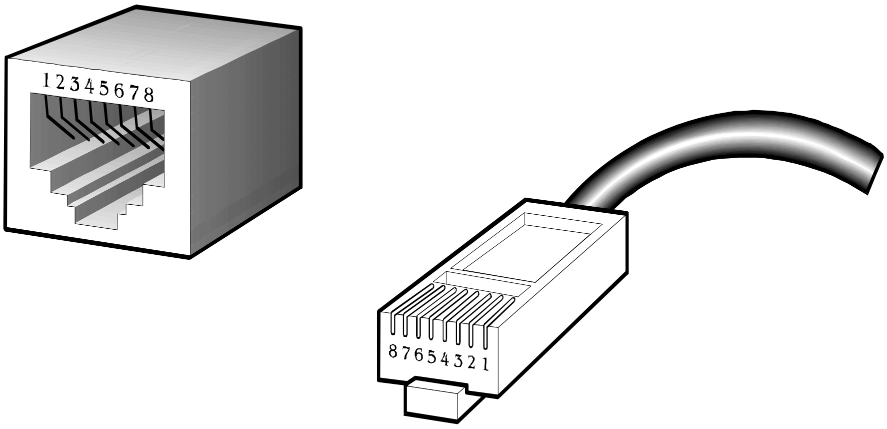
A.1 Switch's RJ-45 Pin Assignments

1000Mbps, 1000Base T

Contact	MDI	MDI-X
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

The standard cable, RJ-45 pin assignment



The standard RJ-45 receptacle/connector

There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight cable and crossover cable connection:

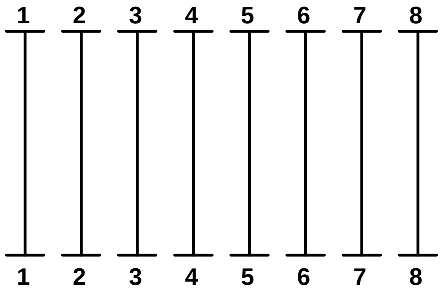
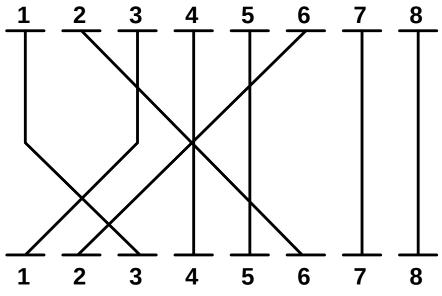
Straight Cable		**SIDE 1**	**SIDE2**
	SIDE 1	1 = White / Orange	1 = White / Orange
		2 = Orange	2 = Orange
		3 = White / Green	3 = White / Green
		4 = Blue	4 = Blue
		5 = White / Blue	5 = White / Blue
		6 = Green	6 = Green
		7 = White / Brown	7 = White / Brown
	SIDE 2	8 = Brown	8 = Brown
Crossover Cable		**SIDE 1**	**SIDE2**
	SIDE 1	1 = White / Orange	1 = White / Green
		2 = Orange	2 = Green
		3 = White / Green	3 = White / Orange
		4 = Blue	4 = Blue
		5 = White / Blue	5 = White / Blue
		6 = Green	6 = Orange
		7 = White / Brown	7 = White / Brown
	SIDE 2	8 = Brown	8 = Brown

Figure A-1: Straight-Through and Crossover Cable

Please make sure your connected cables are with same pin assignment and color as above picture before deploying the cables into your network.

Appendix B Troubles shooting

- Verify that is using the right power source (DC 12-48V), please don't use the DC power source 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 cable for 10Mbps connections, 100Ω Category 5 cable for 100Mbps connections, or 100Ω Category 5e/6 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

EC Declaration of Conformity

For the following equipment:

*Type of Product: 4-Port 10/100/1000Mbps + 4G TP/SFP Combo Managed Industrial Switch
*Model Number: IGS-8044MT

* Produced by:
Manufacturer‘s Name : **Planet Technology Corp.**
Manufacturer‘s Address: 10F., No.96, Minquan Rd., Xindian Dist.,
New Taipei City 231, Taiwan (R.O.C.).

is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility Directive on (2004/108/EC).
For the evaluation regarding the EMC, the following standards were applied:

EN 55022	(2006)
EN 61000-3-2	(2006)
EN 61000-3-3	(1995 + A1:2001 + A:2005)
EN 55024	(1998 + A1: 2001 + A2:2003)
IEC 61000-4-2	(Edition 1.2: 2001-04)
IEC 61000-4-3	(Edition 3.0: 2006)
IEC 61000-4-4	(2004)
IEC 61000-4-5	(Edition 2.0: 2005)
IEC 61000-4-6	(Edition 2.2: 2006)
IEC 61000-4-8	(Edition 1.1: 2001-03)
IEC 61000-4-11	(Second Edition: 2004-03)

Responsible for marking this declaration if the:

☒ **Manufacturer** □ **Authorized representative established within the EU**

Authorized representative established within the EU (if applicable):

Company Name: **Planet Technology Corp.**

Company Address: **10F., No.96, Minquan Rd., Xindian Dist., New Taipei City 231, Taiwan (R.O.C.)**

Person responsible for making this declaration

Name, Surname **Kent Kang**

Position / Title : **Product Manager**

Kent Kang

Taiwan — *Place*

29, Feb., 2012 — *Date*

Legal Signature