

User's Manual

IGS-801M

*8-Port 10/100/1000Mbps
Managed Industrial Switch*



Trademarks

Copyright © PLANET Technology Corp. 2009.

Contents subject to which revision without prior notice.

PLANET is a registered trademark of PLANET Technology Corp. All other trademarks belong to their respective owners.

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

8-Port 10/100/1000Mbps Managed Industrial Switch

FOR MODELS: IGS-801M

REVISION: 1.0 (AUGUST.2009)

Part No.: EM-IGS-801M_v1.0 (2081-AH0120-000)

TABLE OF CONTENTS

1. INTRODUCTION	6
1.1 PACKAGE CONTENTS	6
1.2 PRODUCT DESCRIPTION.....	6
1.3 PRODUCT FEATURES.....	7
1.4 PRODUCT SPECIFICATION	8
2. INSTALLATION.....	11
2.1 HARDWARE DESCRIPTION.....	11
2.1.1 Physical Dimension	11
2.1.2 Front / Rear Panel	12
2.1.3 Top View.....	12
2.1.4 Bottom View.....	13
2.1.5 LED Indicators	13
2.2 INSTALL THE SWITCH.....	15
2.2.1 Installation Steps	15
2.2.2 DIN-Rail mounting	15
2.2.3 Wall Mount Plate Mounting.....	18
2.2.4 Wiring the Power Inputs	18
2.2.5 Wiring the Fault Alarm Contact.....	19
3. SWITCH MANAGEMENT	20
3.1 OVERVIEW	20
3.2 MANAGEMENT METHODS	20
3.2.1 Web Management	20
3.2.2 Login the Switch	21
3.2.3 PLANET Smart Discovery Utility	22
4. WEB CONFIGURATION	24
4.1 MAIN MENU.....	24
4.2 SYSTEM	25
4.2.1 System Info.....	25
4.2.2 IP Configuration	26
4.2.3 User Authentication	27
4.2.4 SNMP	28
4.2.5 Firmware Upgrade.....	30
4.2.6 Configuration Upload.....	31
4.2.7 Factory Reset	33
4.2.8 System Reboot	33
4.2.9 Ping.....	34
4.2.10 Fault Relay Alarm	35
4.2.11 Green Networking.....	36

4.2.12 Logout.....	36
4.3 PORT MANAGEMENT.....	38
4.3.1 Port Configuration.....	38
4.3.2 Port Statistics.....	39
4.3.3 Port Mirroring.....	41
4.3.4 Cable Diagnostics.....	42
4.4 LINK AGGREGATION	44
4.4.1 Port Trunk.....	45
4.4.2 LACP	46
4.4.3 LACP Status	47
4.5 VLANs.....	50
4.5.1 VLAN Membership	54
4.5.2 Per Port Configuration	56
4.5.3 VLAN setting example:.....	60
4.6 RAPID SPANNING TREE	68
4.6.1 Theory.....	68
4.6.2 RSTP System Configuration.....	74
4.6.3 RSTP Port Configuration	75
4.6.4 RSTP Status.....	78
4.7 MULTICAST	81
4.7.1 IGMP Snooping Configuration.....	85
4.7.2 IGMP Snooping Status	86
4.7.3 Multicast Group Table	88
4.8 QUALITY OF SERVICE	89
4.8.1 Understand QOS	89
4.8.2 QoS Configuration	89
4.8.3 802.1p QoS Mode	90
4.8.4 DSCP QoS Mode	93
4.9 802.1X NETWORK ACCESS CONTROL.....	95
4.9.1 Understanding IEEE 802.1X Port-Based Authentication	96
4.9.2 RADIUS Server Configuration.....	99
4.9.3 802.1X Authentication Port Configuration	101
4.10 MAC ADDRESSES	104
4.10.1 Dynamic Address Table	104
4.10.2 Static MAC Address	105
5. SWITCH OPERATION	107
5.1 ADDRESS TABLE	107
5.2 LEARNING	107
5.3 FORWARDING & FILTERING	107
5.4 STORE-AND-FORWARD.....	107
5.5 AUTO-NEGOTIATION	108

APPENDIX A—RJ-45 PIN ASSIGNMENT	109
A.1 SWITCH'S RJ-45 PIN ASSIGNMENTS	109
A.2 10/100MBPS, 10/100BASE-TX.....	109
APPENDIX B TROUBLES SHOOTING	111
APPENDEX C : GLOSSARY	112

1. Introduction

1.1 Package Contents

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

- The IGS-801M Managed Industrial Switch x 1
- User manual x 1
- Pluggable Terminal Block x 1
- Mounting plate x 2

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

The PLANET **IGS-801M** is **8-Port 10/100/1000Mbps** Industrial Gigabit Ethernet Switch with non-blocking wire-speed performance and new slim type with IP-30 metal shape for easily deployment in Heavy Industrial demanding environments.

High Gigabit Performance / Wire-Speed Switching

With a **16Gbps** internal switching fabric, the IGS-801M Industrial Gigabit Ethernet Switch can handle extremely large amounts of data in a secure topology linking to a backbone or high capacity servers. The IGS-801M Industrial Gigabit Ethernet Switch has 8K MAC Address table and offers wire-speed packets transfer performance without risk of packet loss. The Gigabit ports with 9K jumbo packet support can handle large amounts of data transmission in a secure topology linking to a backbone or high-power servers. The high data throughput of the device makes it ideal for most Gigabit environments.

Tough, Environmentally Hardened Design

With IP-30 industrial case protection, the IGS-801M 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-801M also provides a wide range of power supply options suitable for multiple industries and for worldwide operation. The feature of operating temperature range from **-10 to 60 Degree C** allows the Managed Industrial Switch to be placed in almost any difficult environment.

Robust Layer 2 Features

The IGS-801M supports robust advanced features including IEEE 802.1Q VLAN, Port link aggregation, QoS, broadcast storm control, IGMP snooping enhanced security and bandwidth utilization to fit a variety of applications. Via aggregation of supporting port, the IGS-801M allows the operation of high-speed trunk combining multiple ports. Maximum up to 4 ports of the IGS-801M can be assigned for 8 trunk groups and support fail-over as well. Additionally, its standard-compliant implementation ensures interoperability with equipments from other vendors.

Remote and Centralize Management installation

For efficient management, with its built-in **Web-based management**, the IGS-801M offers an easy-to-use and friendly configuration facility. Affording the current network to grow and expand, the IGS-801M supports standard Simple Network Management Protocol (**SNMP**) and can be monitored via any standard-based management software. These features provide a cost-effective way to manage the devices from the Internet whenever you are at work or at home.

Fast Recovery to a Redundant Ethernet Network

The IGS-801M features strong and self-recovery capability to prevent interruptions and outside intrusions. It incorporates **Rapid Spanning Protocol (IEEE 802.1w RSTP)** and **redundant power supply system** into customers' 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.

1.3 Product Features

➤ **Physical Port**

- 8-Port 10/100/1000Base-T RJ-45 copper interface

➤ **Layer 2 Features**

- Supports Auto-negotiation and Half-Duplex / Full-Duplex modes for all 10Base-T/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)
- High performance Store and Forward architecture, broadcast storm control, runt/CRC filtering eliminates erroneous packets to optimize the network bandwidth
- Back-plane (Switching Fabric): 16Gbps
- 9K Jumbo packet size support
- 8K MAC Address Table
- VLANs:
 - IEEE 802.1Q Tag-Based VLAN
 - Up to 64 VLANs groups, out of 4096 VLAN IDs
 - Port-Based VLAN
- Link Aggregation
 - Up to 4 trunk groups
 - Up to 8 ports per trunk group with 16Gbps bandwidth
 - IEEE 802.3ad LACP (Link Aggregation Control Protocol)
 - Cisco ether-channel (Static Trunk)
- Spanning Tree Protocol:
 - IEEE 802.1d classic Spanning Tree Algorithm

- IEEE802.1w Rapid Spanning Tree Protocol

➤ **Quality of Service**

- 4 priority queues on all switch ports
- Traffic classification:
 - IEEE 802.1p CoS
 - IP TOS / DSCP
- Strict priority and Weighted Round Robin (WRR) CoS policies

➤ **Multicast**

- IGMP Snooping v1 and v2
- IGMP Query mode for Multicast Media application

➤ **Security**

- IEEE 802.1x Port-Based Authentication
- Port Mirroring to monitor the incoming or outgoing traffic on a particular port

➤ **Management**

- Remote WEB-based management
- Access through SNMP v1, v2c
- SNMP Trap for alarm notification of events
- Firmware upgrade through web interface
- Cable Diagnostics technology
- Supports PLANET Smart-DISCOVERY Utility for deploy management

➤ **Industrial Case / Installation**

- IP-30 Aluminum case protection
- DIN Rail and Wall Mount Design
- Redundant Power Design
- 12 to 48V DC, redundant power with polarity reverse protect function
- Supports EFT protection 6000 VDC for power line
- Supports 6000 VDC Ethernet ESD protection
- 10 to 60 Degree C operation temperature

1.4 Product Specification

Product	IGS-801M
Hardware Specification	
Copper Ports	8 10/ 100/1000Base-T RJ-45 Auto-MDI/MDI-X ports
Switch Processing Scheme	Store-and-Forward
Switch Fabric	16Gbps
Throughput (packet per second)	11.9Mpps
Address Table	8K entries
Share Data Buffer	176 kilobytes on-chip frame buffer

Flow Control	IEEE 802.3x Pause Frame for Full-Duplex Back pressure for Half-Duplex
Jumbo Frame	9Kbytes
LED	System: Power 1, Power 2, Fault Alarm Ports: 10/100 Link/Act 1000 Link/Act
Installation	DIN rail kit and wall mount ear
Power Supply	External Power Supply: DC 12~48V Redundant power DC 12~48V and connective removable terminal block for master and slave power
Power Consumption	8.2 Watts (Full load)
Operating Temperature	Standard: -10 Degree C ~ 60 Degree C
Operating Humidity	5% to 95% (Non-condensing)
Storage Temperature	-40 Degree C ~ 85 Degree C
Case Dimension	IP-30, 135mm x 87mm x 32mm (W x D x H)
Weight	473g
Layer 2 Function	
System Configuration	Web Browser, SNMPv1, v2c monitor, SNMP Trap
Port configuration	Port disable/enable. Auto-negotiation 10/100/1000Mbps full and half duplex mode selection. Flow Control disable / enable.
VLAN	802.1Q Tagged Based VLAN , up to 64 VLAN groups Port-Based VLAN, up to 8 VLAN groups
Port trunking	IEEE 802.3ad LACP / Static Trunk Support 4 groups of 8-Port trunk support
QoS	Traffic classification based, Strict priority and WRR 4-level priority for switching - 802.1p priority - DSCP/TOS field in IP Packet
IGMP Snooping	IGMP (v1/v2) Snooping, up to 256 multicast Groups IGMP Querier mode support
Storm Control	<ul style="list-style-type: none"> • Broadcast storm control • Multicast storm control • Flooded Unicast storm control
SNMP MIBs	RFC-1213 MIB-II IF-MIB RFC-1493 Bridge MIB RFC-2863 Interface MIB Q-Bridge MIB

	RMON Group 1 statistics
Standards Conformance	
Regulation Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX/100Base-FX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000T IEEE 802.3x Flow Control and Back pressure IEEE 802.3ad Port trunk with LACP 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
Stability testing	IEC60068-2-32(Free fall) IEC60068-2-27(Shock) IEC60068-2-6(Vibration)

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-801M Managed Industrial Switch dimension (W x D x H) : 135mm x 87mm x 32mm

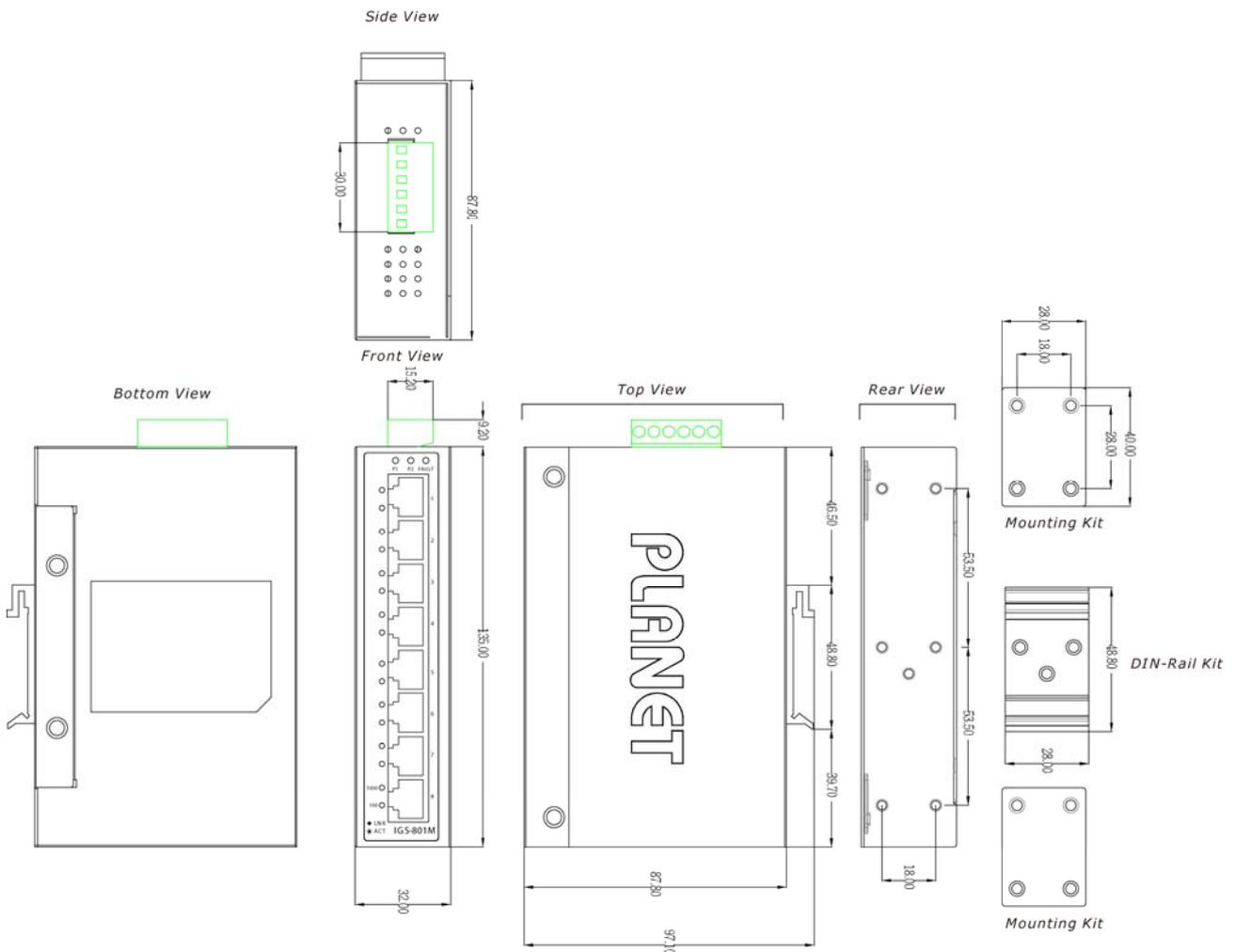


Figure 2-1 IGS-801M panel layout

2.1.2 Front / Rear Panel

The Front Panel and Rear Panel of the IGS-801M Managed Industrial Switch are shown as below:

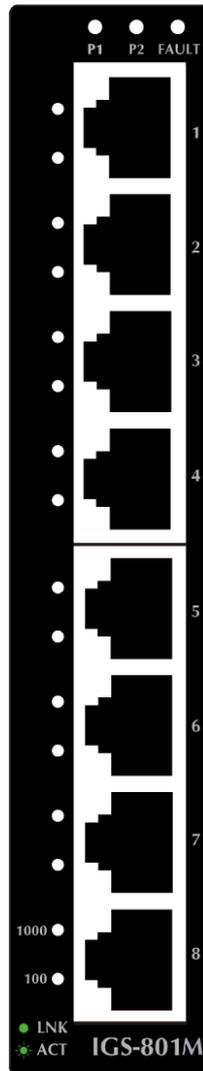


Figure 2-2 Front and Rear Panel of IGS-801M

2.1.3 Top View

The Top panel of the IGS-801M Managed Industrial Switch has one terminal block connector of two DC power inputs and one fault alarm.

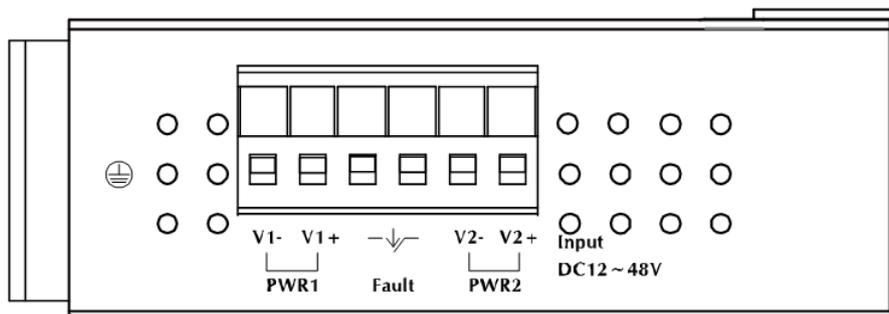


Figure 2-3 Top Panel of IGS-801M

2.1.4 Bottom View

At the bottom of the IGS-801M, the **RESET** button is designed for reboot the Managed Industrial Switch without turn off and on the power.

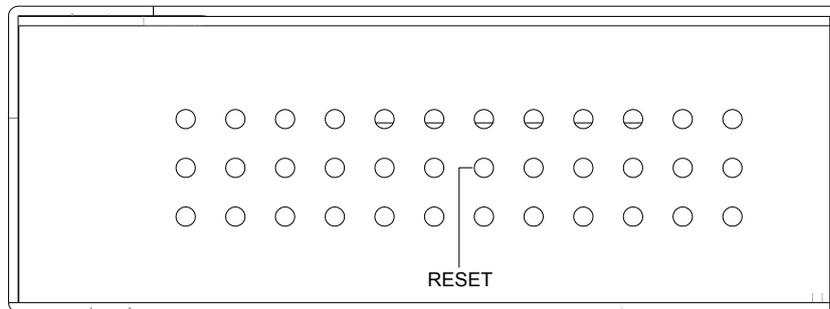


Figure 2-4 Bottom Panel of IGS-801M

The following is the summary table of Reset button functions:

Reset Button Pressed and Released	Function
About 1~3 second	Reboot the Managed Industrial Switch
Until the PWR LED lit off	Reset the Managed Industrial Switch to Factory Default configuration. The Managed Industrial Switch will then reboot and load the default settings as below: <ul style="list-style-type: none"> ◦ Default Password: admin ◦ Default IP address: 192.168.0.100 ◦ Subnet mask: 255.255.255.0 ◦ Default Gateway: 192.168.0.254

2.1.5 LED Indicators

The diagnostic LEDs that provide real-time information of system and optional status are located on the front panel of the IGS-801M. The following table provides the description of the LED status and their meanings for the Managed Industrial Switch.

■ System

LED	Color	Function	
P1	Green	Lit:	Power 1 is active
		Off:	Power 1 is inactive
P2	Green	Lit:	Power 2 is active
		Off:	Power 2 is inactive
FAULT	Green	Lit:	Indicate the either Power 1 or Power 2 has no power
		Off:	No failure

■ Port-1 to Port-8 10/100/1000Base-T

LED	Color	Function	
1000	Green	Lit:	Indicate the port is successfully connecting to the network at 1000Mbps
		Blinking:	Indicate that the port is actively sending or receiving data over that port.
		Off:	Indicate that no device attached or it is successfully connecting to the network at 10Mbps or 100Mbps.
100	Green	Lit:	Indicate the port is successfully connecting to the network at 100Mbps or 10Mbps.
		Blinking:	Indicate that the port is actively sending or receiving data over that port.
		Off:	Indicate that no device attached or it is successfully connecting to the network at 1000Mbps.

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 the 8 10/100TX w/ X-Ring 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 5 cable for Ethernet connection.**
6. **Insert one side of RJ-45 cable (category 5) into the Industrial switch Ethernet port** (RJ-45 port) and another side of RJ-45 cable (category 5) to the network device's Ethernet port (RJ-45 port), ex: Switch PC or Server. The UTP port (RJ-45) LED on the Industrial switch will light up when the cable is connected with the network device. Please refer to the **LED Indicators** section for LED light indication.



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

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

2.2.2 DIN-Rail mounting

The DIN-Rail is screwed on the Industrial Gigabit Ethernet Switch when out of factory. When need to replace the wall mount application with DIN-Rail application on Industrial Gigabit Ethernet, please refer to following figures to screw the DIN-Rail on the Industrial Gigabit Ethernet Switch. To hang the Industrial Gigabit Ethernet Switch, follow the below steps:

Step 1: screw the DIN-Rail on the Industrial Gigabit Ethernet Switch.



Step 2: Lightly press the button of DIN-Rail into the track.



Step 3: Check the DIN-Rail is tightly on the track.



Please refer to following procedures to remove the Industrial Gigabit Ethernet Switch from the track.

Step 4: Lightly press the button of DIN-Rail for remove it from the track.



2.2.3 Wall Mount Plate Mounting

To install the Industrial Gigabit Ethernet Switch on the wall, please follows the instructions described below.

Step 1: Remove the DIN-Rail from the Industrial Gigabit Ethernet Switch; loose the screws to remove the DIN-Rail.

Step 2: Place the wall mount plate on the rear panel of the Industrial Gigabit Ethernet Switch.



Step 3: Use the screws to screw the wall mount plate on the Industrial Gigabit Ethernet Switch.

Step 4: Use the hook holes at the corners of the wall mount plate to hang the Industrial Gigabit Ethernet Switch on the wall.

Step 5: To remove the wall mount plate, reverse steps above.

2.2.4 Wiring the Power Inputs

The 6-contact terminal block connector on the top panel of IGS-801M 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 1, or 5 and 6 for POWER 2.
- 2.

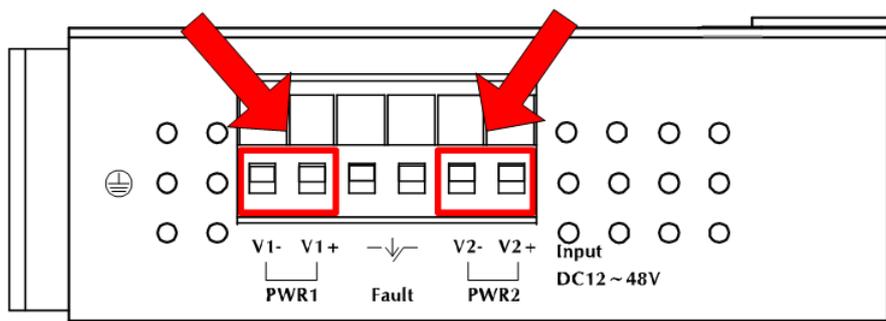


Figure 2-5 Wiring the redundant power inputs

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

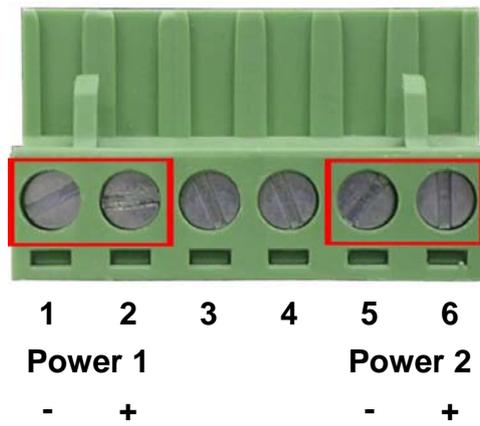


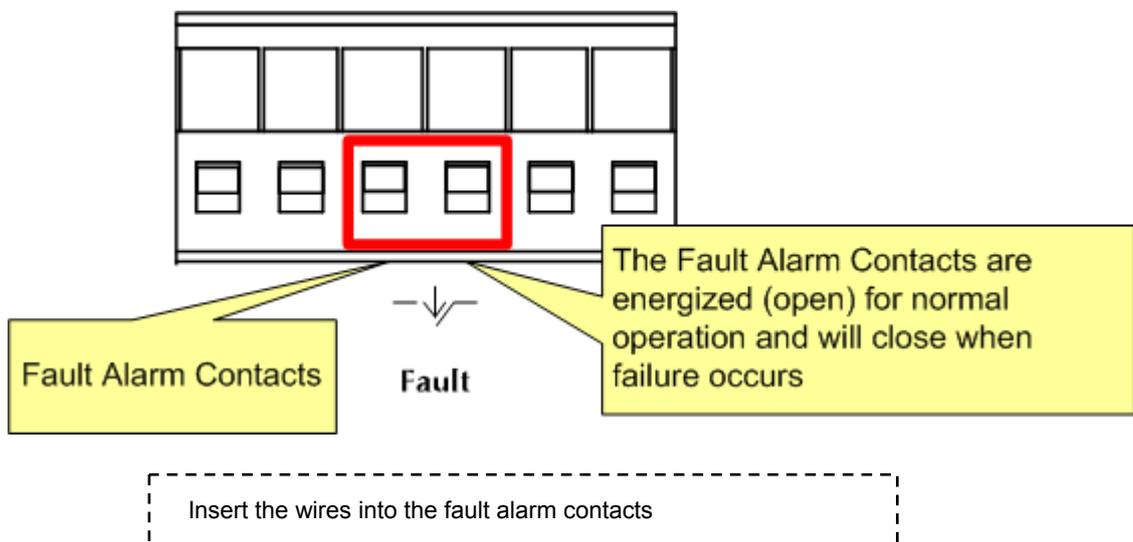
Figure 2-6 6-Pin Terminal Block power wiring input



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.



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

3. SWITCH MANAGEMENT

This chapter describes how to manage the Gigabit Ethernet Switch. Topics include:

- **Overview**
- **Management methods**
- **Logging on to the Gigabit Ethernet Switch**

3.1 Overview

This chapter gives an overview of switch management. The Gigabit Ethernet Switch provides a simply WEB browser interface. Using this interface, you can perform various switch configuration and management activities, including:

- **System**
- **Port Management**
- **VLANs**
- **Rapid Spanning Tree**
- **Multicast**
- **Traffic Control**
- **MAC Address**

Please refer to the following Chapter 4 for more details.

3.2 Management Methods

The way to manage the Gigabit Ethernet Switch:

- Web Management via a network or dial-up connection.

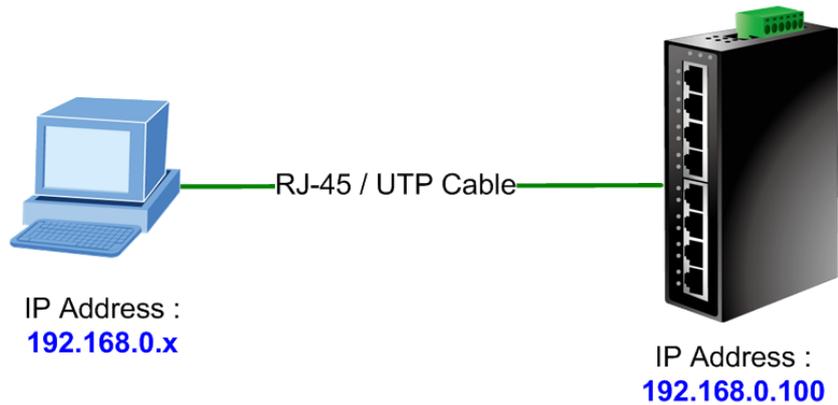
3.2.1 Web Management

The PLANET Gigabit Ethernet Switch provides a built-in browser interface. You can manage the Gigabit Ethernet Switch remotely by having a remote host with web browser, such as Microsoft Internet Explorer, Netscape Navigator or Mozilla Firefox.

Using this management method:

The Gigabit Ethernet Switch must have an Internet Protocol (IP) address accessible for the remote host.

IGS Managed Industrial Switch



3.2.2 Login the Switch

Before you start configure the Gigabit Ethernet Switch, please note the Gigabit Ethernet Switch is configured through an Ethernet connection, make sure the manager PC must be set on same the **IP subnet address**. For example, the default IP address of the Gigabit Ethernet Switch is **192.168.0.100**, then the manager PC should be set at 192.168.0.x (where x is a number between 2 and 254), and the default subnet mask is 255.255.255.0. Use Internet Explorer 5.0 or above Web browser. Enter IP address **http://192.168.0.100** (the factory-default IP address) to access the Web interface.

When the following login screen appears, please enter the default password "**admin**" and press Login to enter the main screen of Gigabit Ethernet Switch. The login screen in Figure 3-1 appears.

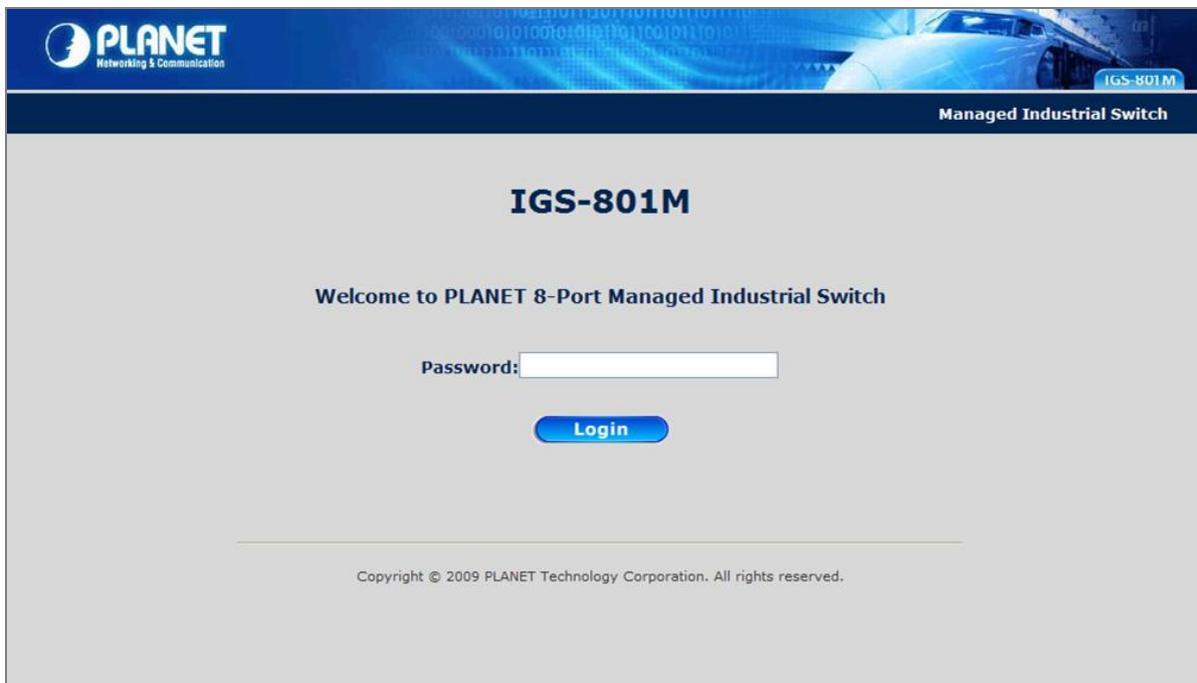


Figure 3-1 Web Login screen of Gigabit Ethernet Switch



Note

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

3.2.3 PLANET Smart Discovery Utility

For easily list the IGS-801M in your Ethernet environment, the Planet Smart Discovery Utility from user's manual CD-ROM is an ideal solution. The following install instructions guiding you for run the Planet Smart Discovery Utility.

1. Deposit the Planet Smart Discovery Utility in administrator PC.
2. Run this utility and the following screen appears.

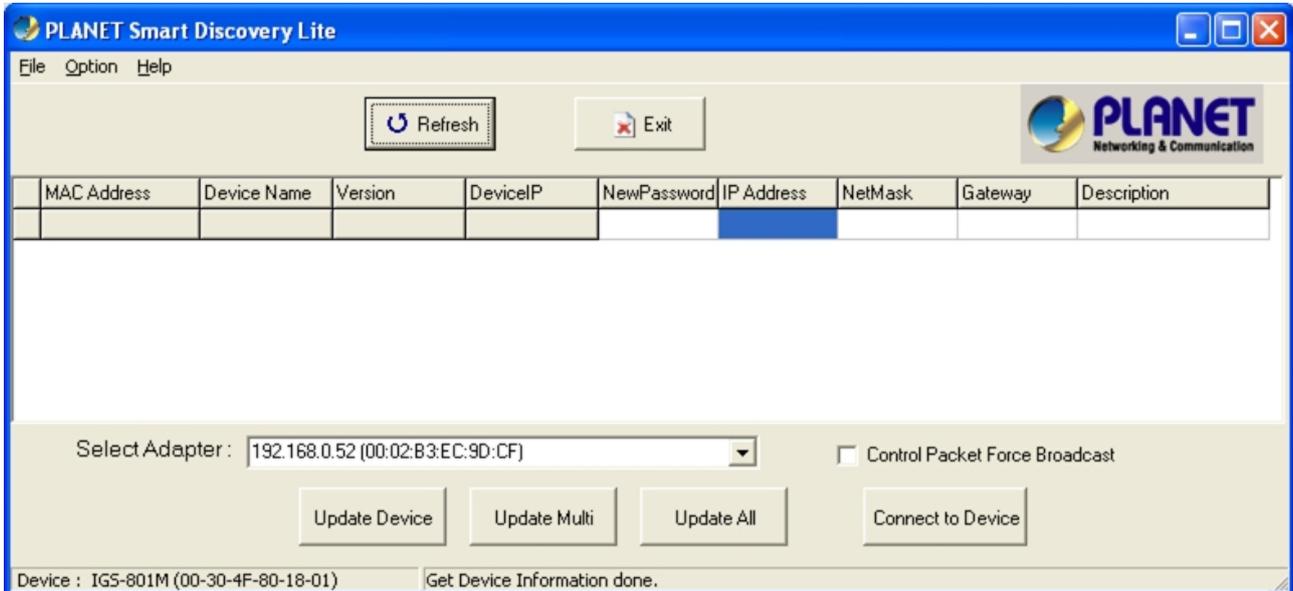


Figure 3-2 Planet Smart Discovery Utility Screen



If there are two LAN cards or above in the same administrator PC, choose different LAN card by use the “**Select Adapter**” tool.

3. Press “**Refresh**” button for list current connected devices in the discovery list, the screen is shown as follow.

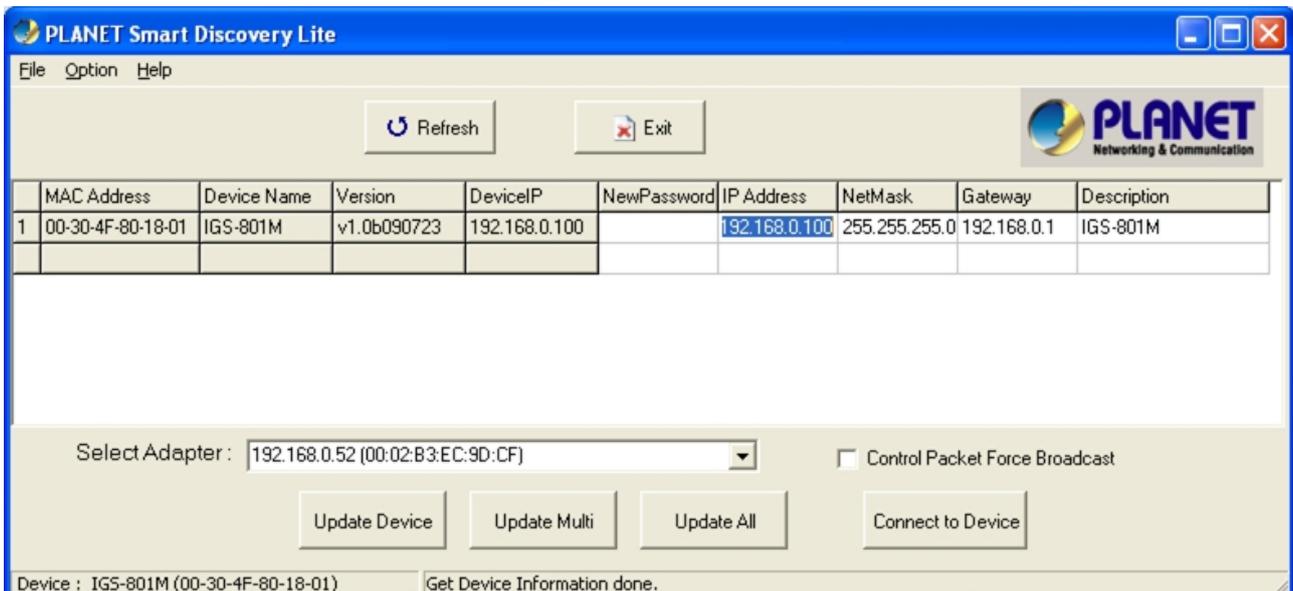


Figure 3-3 Planet Smart Discovery Utility Screen

1. This utility show all necessary information from the devices, such as MAC Address, Device Name, firmware version, Device IP Subnet address, also can assign new password, IP Subnet address and description for the devices.
2. After setup completed, press “**Update Device**”, “**Update Multi**” or “**Update All**” button to take affect. The meaning of the 3 buttons above are shown as below:
 - **Update Device:** use current setting on one single device.
 - **Update Multi:** use current setting on choose multi-devices.
 - **Update All:** use current setting on whole devices in the list.

The same functions mentioned above also can be finding in “**Option**” tools bar.

3. To click the “**Control Packet Force Broadcast**” function, it can allow assign new setting value to the Web Smart Switch under different IP subnet address.
4. Press “**Connect to Device**” button then the Web login screen appears in [Figure 3-1](#).
5. Press “**Exit**” button to shutdown the planet Smart Discovery Utility.

4. WEB CONFIGURATION

The Gigabit Ethernet Switch provide Web interface for Switch smart function configuration and make the Switch operate more effectively - They can be configured through the Web Browser. A network administrator can manage and monitor the Gigabit Ethernet Switch from the local LAN. This section indicates how to configure the Gigabit Ethernet Switch to enable its smart function.

4.1 Main Menu

After a successful login, the main screen appears, the main screen displays the Switch status. The screen in Figure 4-1-1 appears.



Figure 4-1-1 Web Main screen

As listed at the left of the main screen, the configurable smart functions are shown as below:

- **System** – Check the hardware, software version and System MAC address. Setting the IP address and SNMP management for the Gigabit Ethernet Switch. System Reboot / Factory Reset / Firmware Update / Configuration Upload / Ping
- **Port Management** - Setup per port Speed/Duplex mode, Flow Control, jumbo frame, Port Mirroring and Port Link Aggregation and Cable Diagnostic.
- **VLANs** – Configure VLAN Member / Port Configuration.

- **Spanning Tree** – Configure Rapid spanning tree topography for any arrangement of bridges.
- **Multicast** - Enables or disables IGMP Snooping on the device to filter the multicast stream.
- **Traffic Control**
 - **Quality of Service** – Mapping the packet level to classify the packets priority.
 - **802.1X Management** – Specify ports with network access control.
- **MAC Address Table** – Dynamic Address Table / Static MAC Address.

4.2 System

4.2.1 System Info

The System Info page provides information for the current device information. System Info page helps a switch administrator to identify the firmware / hardware version and IP subnet address / DHCP server IP address. The screen in Figure 4-2-1 appears.

System Information	
MAC Address	00-30-4f-80-18-01
S/W Version	v1.0b090730
H/W Version	1.0
Active IP Address	192.168.0.100
Active Subnet Mask	255.255.255.0
Active Gateway	192.168.0.1
DHCP Server	0.0.0.0
Lease Time Left	0 secs

Figure 4-2-1 System Information screen

The page includes the following fields:

Object	Description
MAC Address	Specifies the device MAC address.
S/W Version	The current software version running on the device.
H/W Version	The current hardware versions running on the device.
Active IP Address	The current IP Address of the device. The IP Address could be manual assigned or get via DHCP server.

Active Subnet Mask	The current IP Subnet Mask setting on the device.
Active Gateway	The current IP Gateway of the device.
DHCP Server	If the IP address is got and assigned via a DHCP server, the field shows the IP Address of the DHCP server.
Lease Time left	If the IP address of the device be assigned via a DHCP Server, a DHCP lease time would be apply to the device too. The lease time left shows the left time if the device didn't request the IP Address to the DHCP server, then the IP address will be released.

4.2.2 IP Configuration

The IP Configuration includes the IP Address, Subnet Mask, Gateway, management VLAN, System name, and Inactivity Timeout. Through the Web page or SNMP application, you can easily recognize the device by using the System Name. The Inactivity Timeout is to set the idle time-out for security issue, when there is no action in running the Web page and the time is up, you must re-login to Web interface before you browse the page. Fill up the IP Address, Subnet Mask and Gateway for the device. The screen in Figure 4-2-2 appears.

IP Configuration	
DHCP Enabled	Disable <input type="button" value="v"/>
IP Address	192.168.0.100
Subnet Mask	255.255.255.0
Gateway	192.168.0.1
Management VLAN	1
System Description	IGS-801M
Inactivity Timeout	300 (60~10000 secs 0: No limit)

Figure 4-2-2 IP Configuration screen

The page includes the following configurable data:

Object	Description
DHCP Enable	Choose what the switch should do following power-up: transmit a DHCP request, or manual setting (Disable). The factory default is Disable .
IP Address	The IP address of the interface. The factory default value is 192.168.0.100

Subnet Mask	The IP subnet mask for the interface. The factory default value is 255.255.255.0
Gateway	The default gateway for the IP interface. The factory default value is 192.168.0.1.
Management VLAN	Specifies the management VLAN ID of the switch. It may be configured to any value in the range of 1 - 4093. The management VLAN is used for management of the switch. The factory default management VLAN is " VLAN 1 ".
System Description	Defines the user-defined device name.
Inactivity Timeout	Specifies a time period for the user login. The web interface will be auto logout if there're no actions from the login user. The default value is 300 seconds; 0 means no inactivity time limit.

4.2.3 User Authentication

This page allows you to configure the system password required to access the web pages. After setup completed, please press "**Apply**" button to take effect. Please login web interface with new password, the screen in [Figure 4-2-3](#) appears.

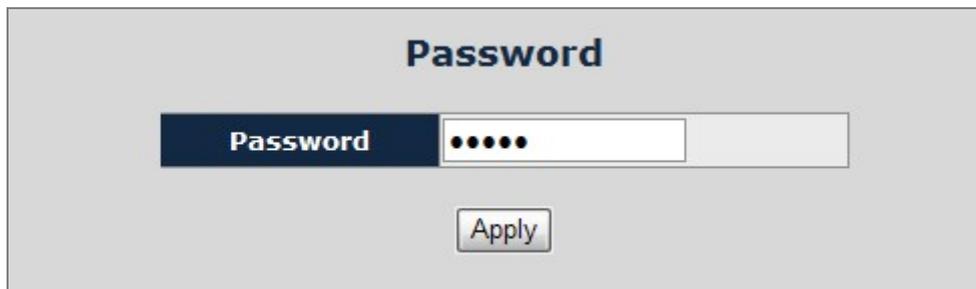


Figure 4-2-3 User Authentication page screenshot

The page includes the following fields:

Object	Description
Password	The system password. The allowed string length is 1 to 16 , and the allowed content is the ASCII characters from 32 to 126. It will not display as it is typed, only asterisks (*) will show. Passwords are alpha numeric characters in length, and are case sensitive.



After change the default password, if you forget the password. Please press the "**Reset**" button in the front panel of the Managed Switch over 10 seconds and then release, the current setting includes VLAN, will be lost and the Managed Switch will restore to the default mode.

4.2.4 SNMP

4.2.4.1 SNMP Overview

The **Simple Network Management Protocol (SNMP)** is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

An SNMP-managed network consists of three key components: Network management stations (NMSs), SNMP agents, Management information base (MIB) and network-management protocol :

- **Network management stations (NMSs)** : Sometimes called consoles, these devices execute management applications that monitor and control network elements. Physically, NMSs are usually engineering workstation-caliber computers with fast CPUs, megapixel color displays, substantial memory, and abundant disk space. At least one NMS must be present in each managed environment.
- **Agents** : Agents are software modules that reside in network elements. They collect and store management information such as the number of error packets received by a network element.
- **Management information base (MIB)** : A MIB is a collection of managed objects residing in a virtual information store. Collections of related managed objects are defined in specific MIB modules.
- **Network-management protocol** : A management protocol is used to convey management information between agents and NMSs. SNMP is the Internet community's de facto standard management protocol.

SNMP Operations

SNMP itself is a simple request/response protocol. NMSs can send multiple requests without receiving a response.

- **Get** -- Allows the NMS to retrieve an object instance from the agent.
- **Set** -- Allows the NMS to set values for object instances within an agent.
- **Trap** -- Used by the agent to asynchronously inform the NMS of some event. The SNMPv2 trap message is designed to replace the SNMPv1 trap message.

SNMP community

An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent. The community name is used to identify the group. A SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities. SNMP default communities are:

- **Write** = private
- **Read** = public

4.2.4.2 SNMP Configuration

Use this page to define management stations. You can also define SNMP Trap destination, SNMP Read/Write Community string and system name for the Managed Switch.

The image shows a web-based configuration interface titled "SNMP Configuration". It contains a table of configuration options with corresponding input fields:

Configuration Item	Value
SNMP enabled	<input checked="" type="checkbox"/>
SNMP Trap destination	0.0.0.0
SNMP Read Community	public
SNMP Write Community	
SNMP Trap Community	public
System Name	IGS-801M

Below the table is an "Apply" button.

Figure 4-2-4: SNMP configuration interface

The page includes the following configurable data:

Object	Description
SNMP Enable	Enable or Disable the SNMP function of the device. While set to enable, the manager could remotely get the interface status and received the traps information.
SNMP Trap Destination	SNMP Trap destination is a management station that receives the trap messages generated by the switch. If no trap manager is defined, no traps will be issued. To define a management station as a trap destination, assign an IP address and enter the SNMP community strings.
SNMP Read Community	Functions as a password and used to authenticate the access right of the device. The Read Community is restricted to read-only, for all MIBs except the community table, for which there is no access.
SNMP write Community	Functions as a password and used to authenticate the access right of the device. The Write Community accesses the device both read and write - configure to the device via SNMP.
SNMP Trap Community	Identifies the community string of the trap manager.
System Name	Defines the user-defined device name.

4.2.5 Firmware Upgrade

The **Firmware Upgrade** page contains fields for downloading system image files from the Local File browser to the device.

To open **Firmware Upgrade** screen perform the following:

1. Click **Tools** -> **Firmware Upgrade**.
2. The Firmware Upgrade screen is displayed as in Figure 4-51.
3. Click the **"Browse"** button of the main page, the system would pop up the file selection menu to choose firmware.
4. Select on the firmware then click **"Upload"**, the **Software Upload Progress** would show the file upload status.

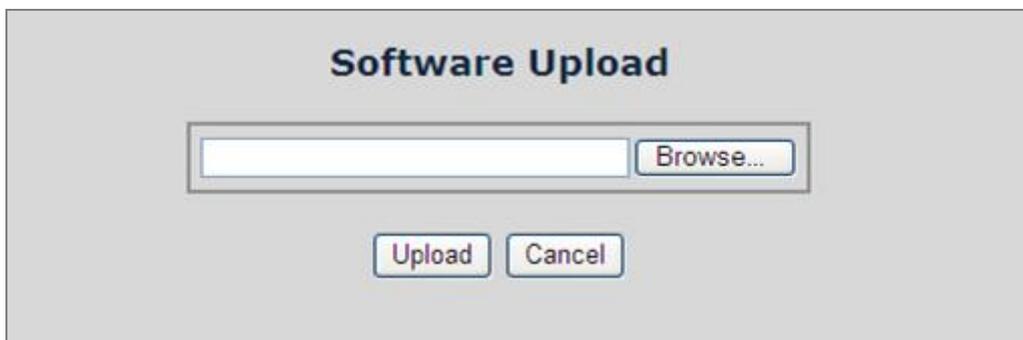


Figure 4-2-5 Firmware Upgrade screen

5. Once the software be loaded to the system successfully. The following screen appears. Click the **"Yes"** button to activate the new software immediately. The system will load the new software after reboot.



Figure 4-2-6 Software successfully loaded notice screen



1. Do not power off the switch until the update progress is complete.
2. Do not quit the Firmware Upgrade page without press the **"Yes"** button - after the image be loaded. Or the system won't apply the new firmware. User has to repeat the firmware upgrade processes again.

4.2.6 Configuration Upload

This function allows backup and reload the current configuration of Switch to the local management station. The screen in Figure 4-2-7 appears.

- **Configuration Upload:** Upload the existed configuration file to the Switch. The configuration file had been saved at the local machine already.
- **Configuration Download:** Download the current configuration file of the switch to the local machine.

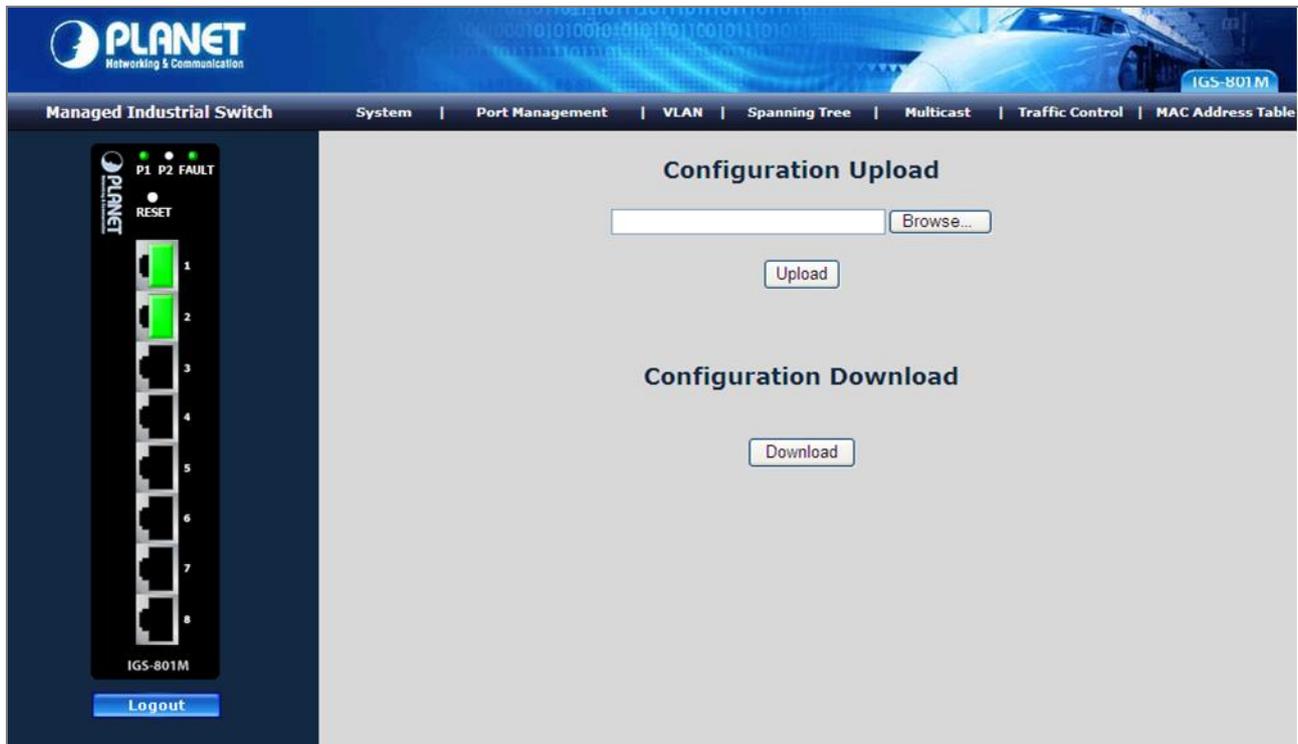


Figure 4-2-7 Configuration Upload/Download screen

■ Configuration Download

1. Press the “**Download**” button to save the current configuration in manager workstation. The following screens in Figure 4-2-8 and 4-2-9 appear



Figure 4-2-8 File Download screen

2. Chose the file save path in management workstation.

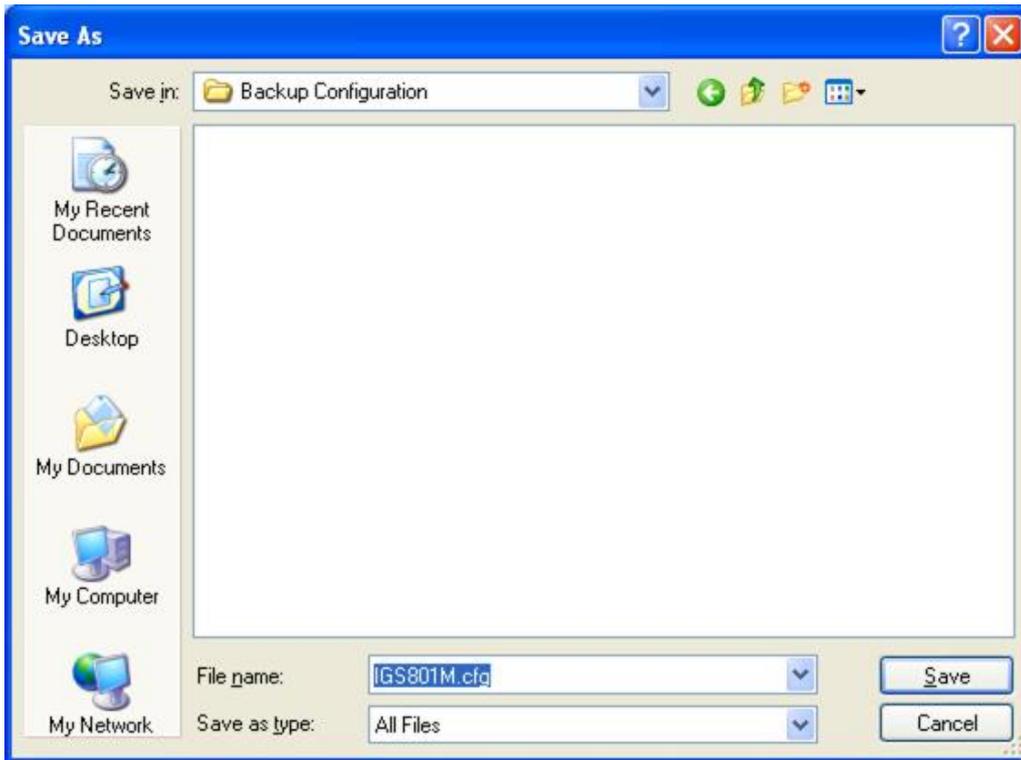


Figure 4-2-9 File save screen

■ Configuration Upload

1. Click the “Browse” button of the main page, the system would pop up the file selection menu to choose saved configuration.

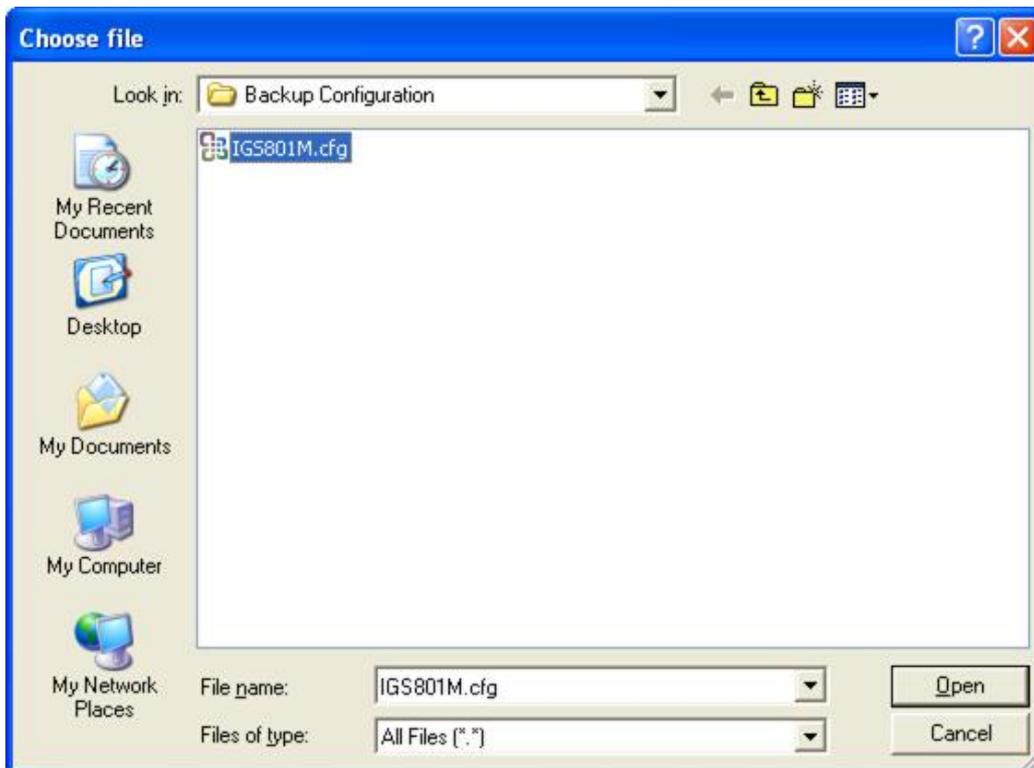


Figure 4-2-10 Windows file selection menu popup

2. Select on the configuration file then click **“Upload”**, the bottom of the browser shows the upload status.
3. After down, the main screen appears **“Transfer Completed”**.

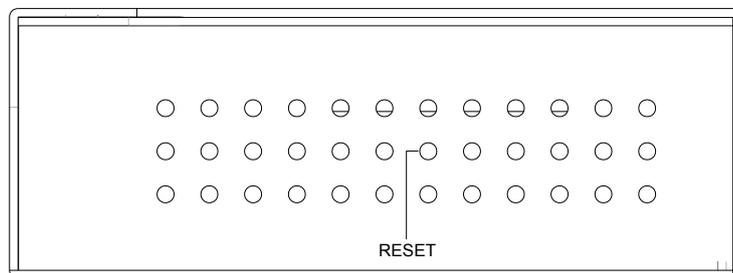
4.2.7 Factory Reset

The Factory Reset button can reset the Gigabit Ethernet Switch back to the factory default mode. Be aware that the entire configuration will be reset; expect the IP address of the Gigabit Ethernet Switch. Once the Factory Reset item be pressed, the screen in Figure 4-2-11 appears.



Figure 4-2-11 Factory Reset screen

To reset the IP address to the default IP Address **“192.168.0.100”**. Press the hardware reset button at the bottom panel about 5 seconds. After the device be rebooted. You can login the management WEB interface within the same subnet of 192.168.0.xx.



4.2.8 System Reboot

The Reboot page enables the device to be rebooted from a remote location. Once the Reboot button be pressed, user have to re-login the WEB interface about 20 seconds later, the screen in Figure 4-2-12 appears.

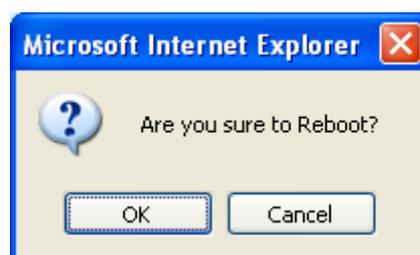


Figure 4-2-12 Reboot screen

4.2.9 Ping

Use this screen to tell the switch to send a Ping request to a specified IP address. You can use this to check whether the switch can communicate with a particular IP station. Once you click the Apply button, the switch will send n pings and the results will be displayed below the configurable data.

Ping Parameters

Target IP address	<input type="text"/>
Count	1 ▼
Time Out (in secs)	1 ▼

Apply

Ping Results	
Target IP address	0.0.0.0
Status	Test complete
Received replies	0
Request timeouts	0
Average Response Time (in ms)	0

Refresh

Figure 4-2-13 Ping function screen

The Ping Parameters includes the following fields:

Object	Description
Target IP Address	Enter the IP address of the station you want the switch to ping. The initial value is blank. The IP Address you enter is not retained across a power cycle.
Count	Number of echo requests to send.
Time Out (in secs)	Timeout in milliseconds to wait for each reply.

After field the parameter and press “**Apply**” to execute the Ping function. The Ping result shows at the next table. As the Figure 4-2-14 screen appears.

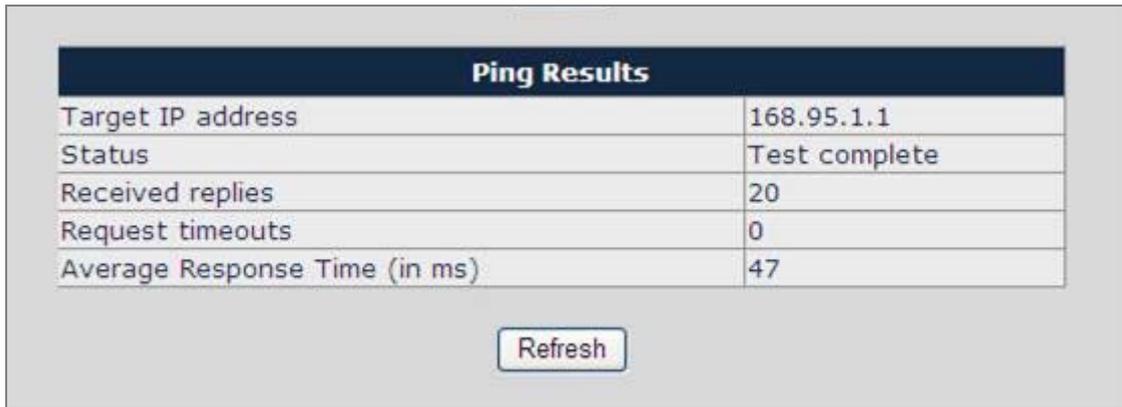


Figure 4-2-14 Ping Result screen



Be sure the target IP Address is within the same network subnet of the switch, or you had setup the correct gateway IP address.

4.2.10 Fault Relay Alarm

The Fault Relay Alarm function provides the Power Failure detection. With both power input 1 and power input 2 installed and the check boxes of power 1/power 2 ticked, the FAULT LED indicator will then be possible to light up when any one of the power failures occurs.



Figure 4-2-15 Fault Relay Alarm interface

The page includes the following fields:

Object	Description
Power Failure:	Tick the check box to enable the function of lighting up the FAULT LED on the panel when power fails.

4.2.11 Green Networking

This page is used to enable/disable green networking function. Enable Power Saving mode will reduce system power consumption when the link is not present.

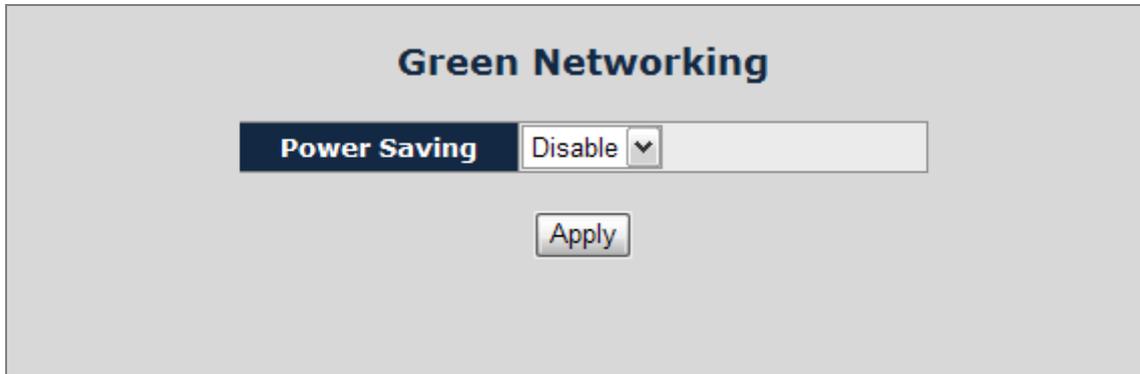


Figure 4-2-16 Green Ethernet screenshot

The page includes the following fields:

Object	Description
Power Saving	Enable mode will reduce chip power when the signal from the copper link partner is not present.

4.2.12 Logout

Press this function; the web interface will go back to login screen. The screen in Figure 4-67 and Figure 4-2-17 appears.



Figure 4-2-17 Logout screen

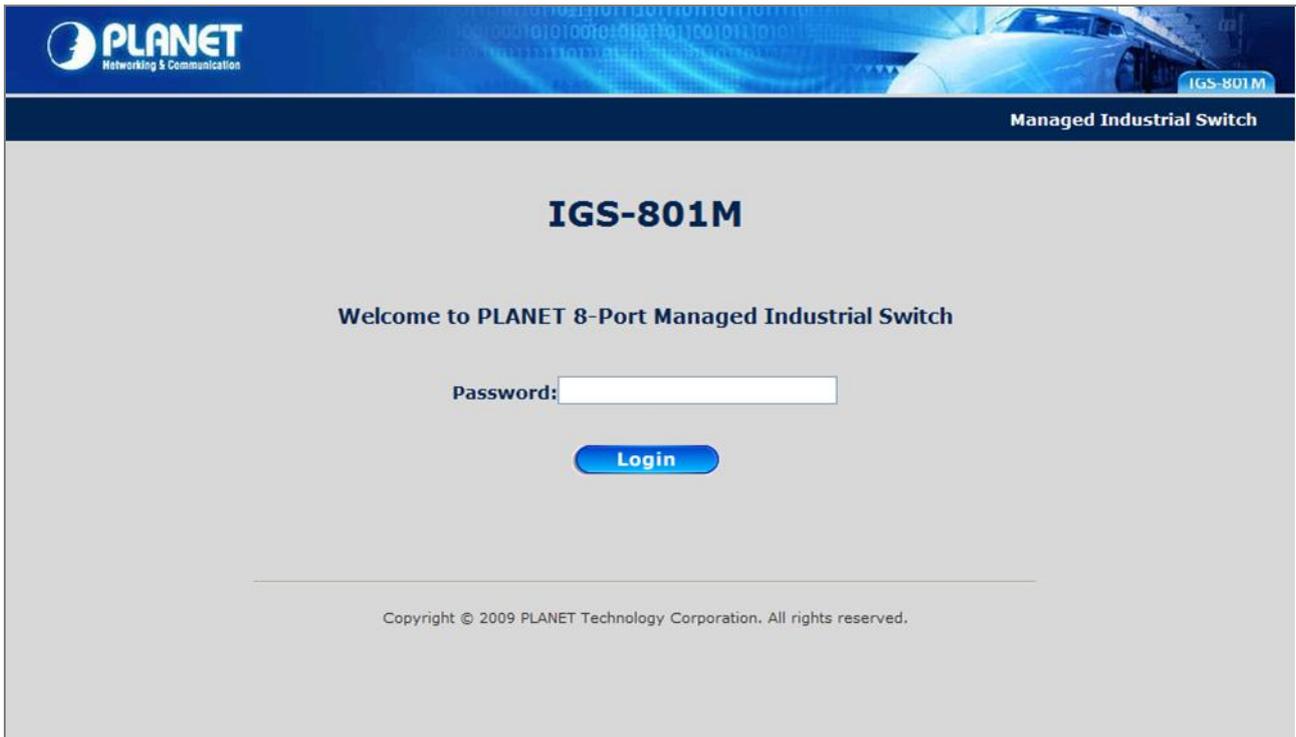


Figure 4-2-18 Login screen

4.3 Port Management

4.3.1 Port Configuration

This function allows displaying each port's status. The Link Status in the screen displays the current connection speed and duplex mode; else this function will show "Down" when the port is disconnected. Press the "Refresh" button to renew the screen. The screen in [Figure 4-3-1](#) appears.

Port Configuration

All Ports Jumbo Frames Setting	Disable ▾
Drop frames after excessive collisions	<input type="checkbox"/>

Note : Jumbo Frame mode is NOT supported when WRR enabled.

Port	Link	Mode	Flow Control	Port Description
1	Down	Auto Speed ▾	<input type="checkbox"/>	<input type="text"/>
2	100FDX	Auto Speed ▾	<input type="checkbox"/>	<input type="text"/>
3	Down	Auto Speed ▾	<input type="checkbox"/>	<input type="text"/>
4	Down	Auto Speed ▾	<input type="checkbox"/>	<input type="text"/>
5	Down	Auto Speed ▾	<input type="checkbox"/>	<input type="text"/>
6	Down	Auto Speed ▾	<input type="checkbox"/>	<input type="text"/>
7	Down	Auto Speed ▾	<input type="checkbox"/>	<input type="text"/>
8	Down	Auto Speed ▾	<input type="checkbox"/>	<input type="text"/>

Figure 4-3-1 Port Configuration screen

The page includes the following configurable data:

Object	Description
All Ports Jumbo Frames Setting	<p>The maximum Ethernet frame size the interface supports or is configured, including Ethernet header, CRC, and payload. Draw the menu bar to select the mode.</p> <ul style="list-style-type: none"> Disable - The default maximum frame size is 1518. 4096 Kbytes – Set the maximum frame size to 4096 Bytes. 9600 Kbytes - Set the maximum frame size to 9600 Bytes.

Drop frames after excessive collisions	Enable or Disable the device to drop frames once the excessive collisions be detected.
Port	Indicate port 1 to port 8.
Mode	<p>Allow configuring the port speed and operation mode. Draw the menu bar to select the mode.</p> <ul style="list-style-type: none"> • Auto Speed - Setup Auto negotiation. • 10 half - Force sets 10Mbps/Half-Duplex mode. • 10 Full - Force sets 10Mbps/Full-Duplex mode. • 100 half - Force sets 100Mbps/Half-Duplex mode. • 100 full - Force sets 100Mbps/Full-Duplex mode. • 1000 full - Force sets 1000Mbps/Full-Duplex mode. • Disable - Shutdown the port manually.
Flow Control	<p>Allow Enable or Disable flow control for selected port.</p> <ul style="list-style-type: none"> • Enable – 802.3x flow control is enabled on Full-Duplex mode or Backpressure is enabled on Half-Duplex mode. • Disable – No flow control or backpressure function on no matter Full-Duplex or Half-Duplex mode.
Port Description	Can key in the description for the port.



When set each port to run at 100M Full, 100M Half, 10M Full, and 10M Half-speed modes. The Auto-MDIX function will disable.

4.3.2 Port Statistics

The Port Statistic page displays the status of packet count from each port. The Port statistics screen in Figure 4-3-2 appears.

Port Statistics								
		<input type="button" value="Clear"/>		<input type="button" value="Refresh"/>				
Port	Receive Total				Transmit Total			
	Packets	Octets	Broad- and Multicast	Error Packets	Packets	Octets	Broad- and Multicast	Error Packets
1	0	0	0	0	0	0	0	0
2	7193	752933	5771	0	1171	561209	77	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	258	23239	49	1	3538	387337	3426	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0

Figure 4-3-2 Port Statistics Overview screen

The page includes the following fields:

Object	Description
Port	The Port number.
Receive Packets	Number of packets received on the port. Include the Unicast packets.
Receive Octets	Number of octets of data (including those in bad packets) received on the port. This object can be used as a reasonable estimate of Ethernet utilization.
Broad- and Multicast	Number of packets received on the port. Include the broadcast and multicast packets.
Error Packets	The numbers of error packets received from the port.
Transmit Packets	Number of packets transmitted on the port. Include the Unicast packets.
Transmit Octets	Number of octets of data (including those in bad packets) transmitted on the port. This object can be used as a reasonable estimate of Ethernet utilization.
Broad- and Multicast	Number of packets transmitted on the port. Include the broadcast and multicast packets.
Error Packets	The numbers of error packets transmit from the port.

4.3.3 Port Mirroring

This function provide to monitoring network traffic that forwards a copy of each incoming or outgoing packet from one port of a network Switch to another port where the packet can be studied. It enables the manager to keep close track of switch performance and alter it if necessary. The Port Mirroring screen in Figure 4-3-3 appears.

Port Mirroring

Destination Port

1 ▾

Source Port

1

2

3

4

5

6

7

8

Apply

Refresh

Destination Port:

Use this option to select the port for monitored traffic. This is the port that your network analyzer would be connected to.

Source Port:

Duplicate the data transmitted from the source port and forward it to the Destination port.

Figure 4-3-3 Mirror Setting screen

The page includes the following configurable data:

Object	Description
Destination Port	Use this option to select the port for monitored traffic. This is the port that your network analyzer would be connected to – such as NAI Sniffer Pro or Ethereal.
Source Port	Duplicate the data transmitted from the source port and forward it to the Destination port.

Configuring the port mirroring by assigning a source port from which to copy all packets and a destination port where those packets will be sent.

4.3.4 Cable Diagnostics

The Cable Diagnostics page contains fields for performing tests on copper cables. These functions have the ability to identify the cable length and operating conditions, and to isolate a variety of common faults that can occur on the Cat5 twisted-pair cabling. There might be two statuses as follow:

- If the link is established on the twisted-pair interface in 1000Base-T mode, the Cable Diagnostics can run without disruption of the link or of any data transfer.
- If the link is established in 100Base-TX or 10Base-T, the Cable Diagnostics cause the link to drop while the diagnostics are running.

After the diagnostics are finished, the link is reestablished. And the following functions are available.

- Coupling between cable pairs.
- Cable pair termination
- Cable Length

Anomalous coupling between cable pairs can be caused by shorted wires, improper termination, or high crosstalk resulting from an incorrect wire map. These conditions can all prevent the PLANET switch from establishing a link. The screen in Figure 4-3-4 appears.

Cable Diagnostics

Port	Port 2 ▾
Mode	Full ▾

Cable Status		
Pair	Length [m]	Status
A (Pin 1,2)	3	Abnormal termination
B (Pin 3,6)	2	Abnormal termination
C (Pin 4,5)	2	Short
D (Pin 7,8)	2	Short

Figure 4-3-4 Cable Diagnostics

The Cable Diagnostics includes the following fields:

Object	Description
<ul style="list-style-type: none"> • Port 	Specifies the port numbers for which to run the cable diagnostics.

<ul style="list-style-type: none"> • Mode 	<p>There're three cable test mode for selection:</p> <p>Full – test full pairs.</p> <p>Anomaly – test with only anomaly pairs.</p> <p>Anomaly w/o X-pair - test anomaly pairs but without X-pair.</p>
---	--

The Cable status includes the following items:

Object	Description
<ul style="list-style-type: none"> • Pair 	<p>The twist pair of the UTP cable. The pair groups as follow:</p> <p>A (Pin 1,2)</p> <p>B (Pin 3,6)</p> <p>C (Pin 4,5)</p> <p>D (Pin 7,8)</p>
<ul style="list-style-type: none"> • Length[m] 	<p>When properly terminated, Cable Diagnostics reports the approximate cable length in meters of each of the four cable pair A, B, C, and D.</p>
<ul style="list-style-type: none"> • Status 	<p>The cable test results. Possible values are:</p> <ul style="list-style-type: none"> • Proper - The cable passed the test. • Open - The cable is connected on only one side or there is no cable connected to the port • Short - A short has occurred in the cable. With 10/100BASE link, the status of Pair C and Pair D will be "Short". • Abnormal termination – An improper termination be detected. Proper termination of Cat5 cable requires a 100Ω differential impedance between the positive and negative cable terminals. IEEE Std 802.3 allows for a termination of as large as 115Ω or as small as 85Ω. If the termination falls out of this range, it is reported as falls an anomalous termination.



Be sure to running the Cable diagnostics with standard Cat 5e or Cat 6 UTP cable. With some of the UTP cables that not match the standard of Cat 5e, it might cause the 10/100Base link down after the cable diagnostics.

4.4 Link Aggregation

Port Aggregation optimizes port usage by linking a group of ports together to form a single **Link Aggregated Groups (LAGs)**. Port Aggregation multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy.

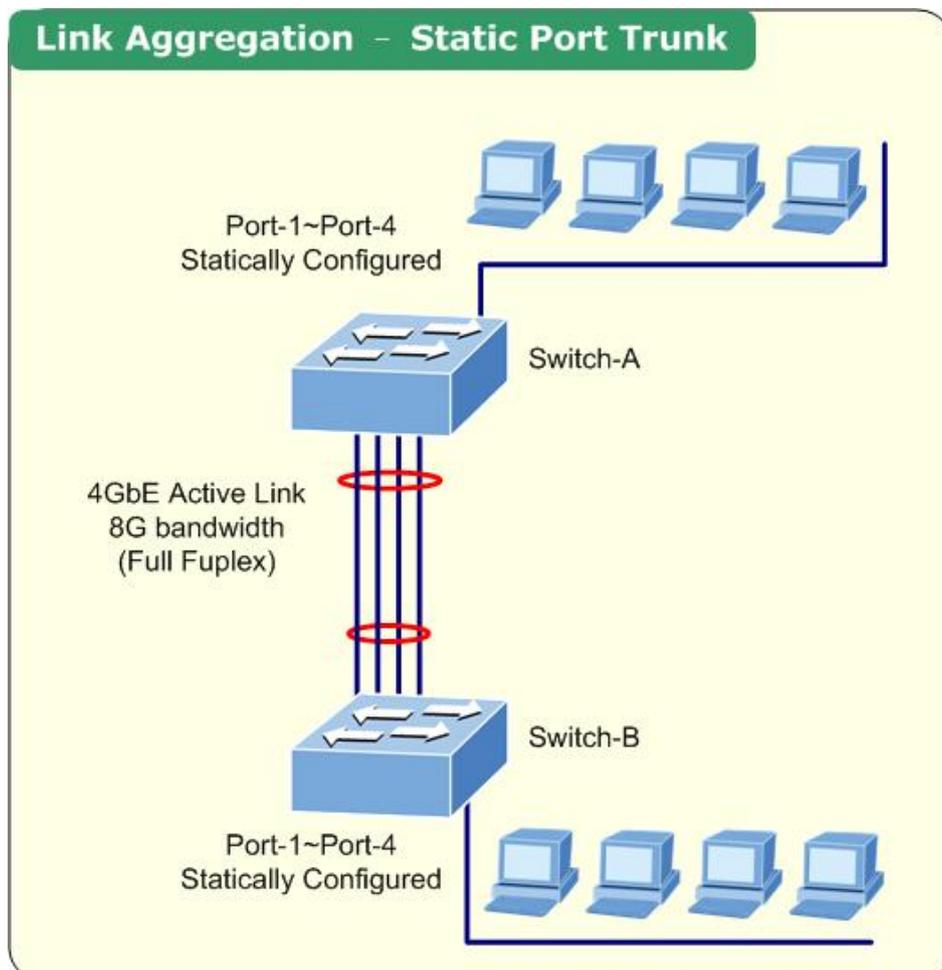
Each LAG is composed of ports of the same speed, set to full-duplex operations. Ports in a LAG, can be of different media types (UTP/Fiber, or different fiber types), provided they operate at the same speed.

The device supports the following Aggregation links :

- **Static LAGs (Port Trunk)** – Force aggregated selected ports to be a trunk group.
- **Link Aggregation Control Protocol (LACP)** LAGs - LACP LAG negotiate Aggregated Port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them.

Aggregated Links can be assigned manually (**Port Trunk**) or automatically by enabling Link Aggregation Control Protocol (**LACP**) on the relevant links.

Aggregated Links are treated by the system as a single logical port. Specifically, the Aggregated Link has similar port attributes to a non-aggregated port, including auto-negotiation, speed, Duplex setting, etc.



4.4.1 Port Trunk

This function provides to cascade two Switch devices with a double bandwidth.

- 4 Trunk Group per system, up to 8 ports per Trunk Group.

The Port Trunking configuration screen in Figure 4-4-1 appears.

Aggregation/Trunking Configuration

Group\Port	1	2	3	4	5	6	7	8
Normal	<input checked="" type="radio"/>							
Group 1	<input type="radio"/>							
Group 2	<input type="radio"/>							
Group 3	<input type="radio"/>							
Group 4	<input type="radio"/>							

(Maximum 8 Ports per Trunk Group)

Figure 4-4-1 Aggregation/Trunking Configuration screen

The page includes the following fields:

Object	Description
Port	Indicate port 1 to port 8.
Normal	While a port is checked as "Normal", the port is not joining to any Static Trunk Group.
Group	Specify the Joined Trunk Group. There're maximum 4 trunk groups per system and the maximum 8 ports in a trunk group. Note. A port can be assigned to only one Trunk Group.

4.4.2 LACP

Link Aggregation Control Protocol (LACP) - LACP LAG negotiate Aggregated Port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them.

The LACP Port Configuration page contains fields for assigning LACP properties to individual ports. The screen in Figure 4-4-2 appears.

Port	Protocol Enabled	Key Value
1	<input type="checkbox"/>	auto
2	<input type="checkbox"/>	auto
3	<input type="checkbox"/>	auto
4	<input type="checkbox"/>	auto
5	<input type="checkbox"/>	auto
6	<input type="checkbox"/>	auto
7	<input type="checkbox"/>	auto
8	<input type="checkbox"/>	auto

Figure 4-4-2 LACP Port Configuration

The page includes the following fields:

Object	Description
Port	Indicate port 1 to port 8.
Protocol Enable	To Enable or disable the LACP protocol on a selected port. Once the LACP protocol be enabled, the system will start transmit the LACP control packets and exchange with another LACP aware switch. If the linked switch didn't support LACP, then the aggregated link will not be established.
Key Value	The Key Value will be filed in the LACP control packets. Ports with same key value will be set to the same LACP Group. If two ports are set with different key value, they will become two different LACP groups. The key value will also be the identify ID to the linked LACP switch. The default setting is "Auto"



When using a port link aggregation, note that:

- The ports that can be assigned to the same link aggregation have certain other restrictions (see below).
- Ports can only be assigned to one link aggregation.
- The ports at both ends of a connection must be configured as link aggregation ports.
- None of the ports in a link aggregation can be configured as a mirror source port or a mirror target port.
- All of the ports in a link aggregation have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- The Spanning Tree Protocol will treat all the ports in a link aggregation as a whole.
- Disconnect all link aggregation port cables or disable the link aggregation ports before removing a port link aggregation to avoid creating a data loop.

4.4.3 LACP Status

The LACP Status page display the current LACP aggregation Groups and LACP Port status.

To open **LACP Status** screen perform the folling:

1. Click Status -> LACP Status.
2. The “LACP Aggregation Overview” and “LACP Port Status” screen is displayed as in Figure 4-4-3.

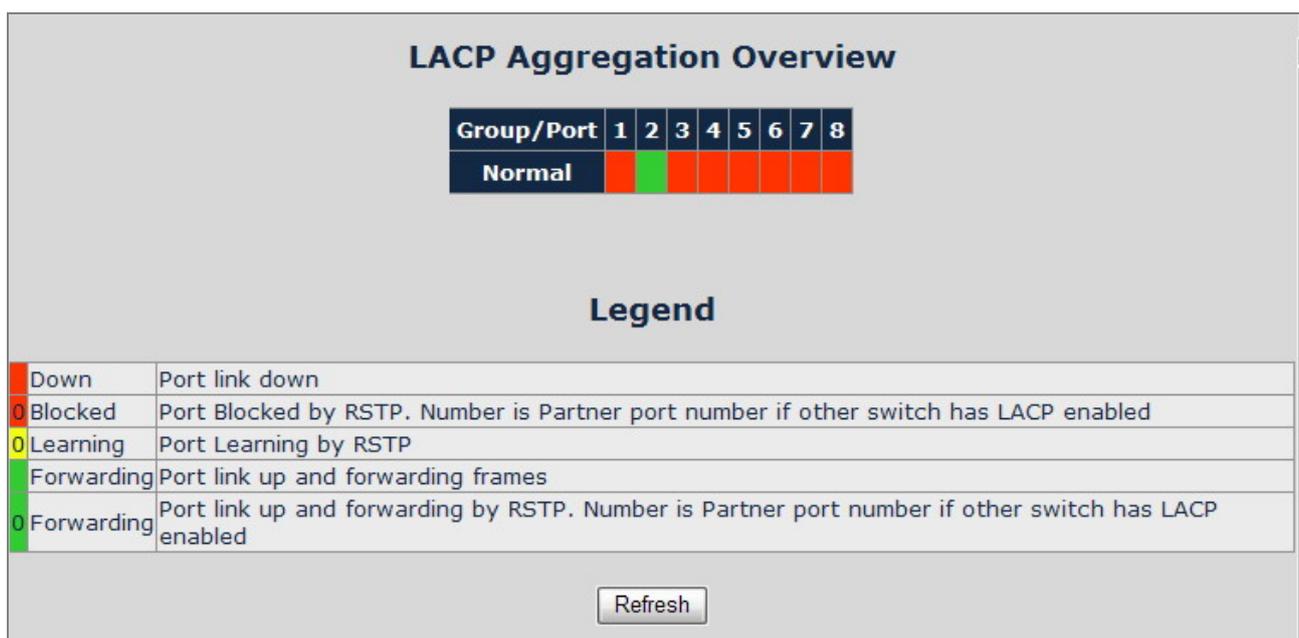


Figure 4-4-3 LACP Status

■ **LACP Aggregation Overview Table**

The LACP Aggregation Overview Table lists the active LACP ports and mapped Group. It also indicates the Partner Port number of the other LACP aware switches. The screen in Figure 4-4-4 appears.



Figure 4-4-4 LACP Aggregation Overview

The page includes the following fields:

Object	Description
Group / Port	Indicate port 1 to port 8.
Normal	While a port is checked as “Normal”, the port is not joining to any LACP Trunk Group.
Group #	The Linked LACP aggregation group. The Group ID is the first port ID of the LACP group member. Ex. Port 7 and Port 8 as a LACP group-> Group 7.

The Color and ID legend

	Down	Port link down.
0	Blocked	Port Blocked by RSTP. Number is Partner port number if other switch has LACP enabled.
0	Learning	Port Learning by RSTP.
	Forwarding	Port link up and forwarding frames.
0	Forwarding	Port link up and forwarding by RSTP. Number is Partner port number if other switch has LACP enabled.

■ **LACP Port Status Table**

The LACP Port Status Table lists the active LACP ports and the Partner Port number with the operational Port Key value. The screen in Figure 4-4-5 appears.

LACP Port Status			
Port	Protocol Active	Partner Port Number	Operational Port Key
1	no		
2	no		
3	no		
4	no		
5	yes	7	3
6	yes	8	3
7	no		
8	no		

Figure-4-4-5 LACP Port Status

The page includes the following fields:

Object	Description
Protocol Active	<p>Indicate the LCAP protocol is enable or not on the port.</p> <p>Yes- LACP is enabled and active on the port.</p> <p>No- LACP is not enabled, or LACP is enabled but not active on the port.</p> <p>It's usually depends on the partner switch is LACP enabled or not.</p>
Partner Port Number	<p>The port number/ID of the linked partner switch- if other switch has LACP enabled.</p> <p>Ex. Row of Port 7with Partner Port Number value=15.</p> <p>The Port 7 of the switch is connecting to the Port 15 of the partner switch directly – both of the two switches are with LACP enabled.</p>
Operational Port Key	<p>The current operational key value of the partner port. Within the same LACP group, the port key value should be the same with the other LACP active ports.</p>

4.5 VLANs

■ 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 Gigabit Ethernet Switch supports **IEEE 802.1Q (tagged-based)** and **Port-Base VLAN** setting in web management page. In the default configuration, VLAN support is “**802.1Q**”.

■ 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:

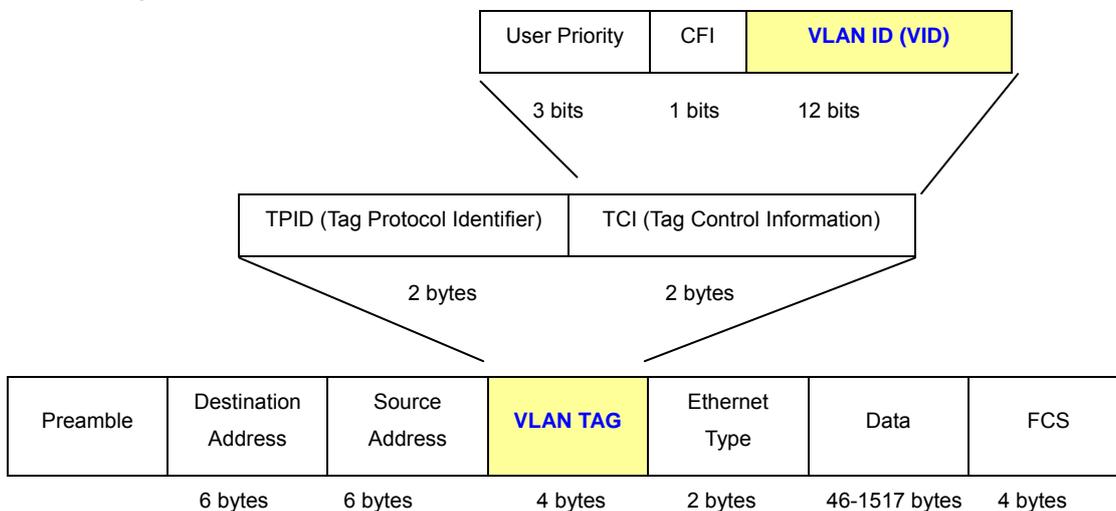
- **Tagging** - The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** - The act of stripping 802.1Q VLAN information out of the packet header.

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.

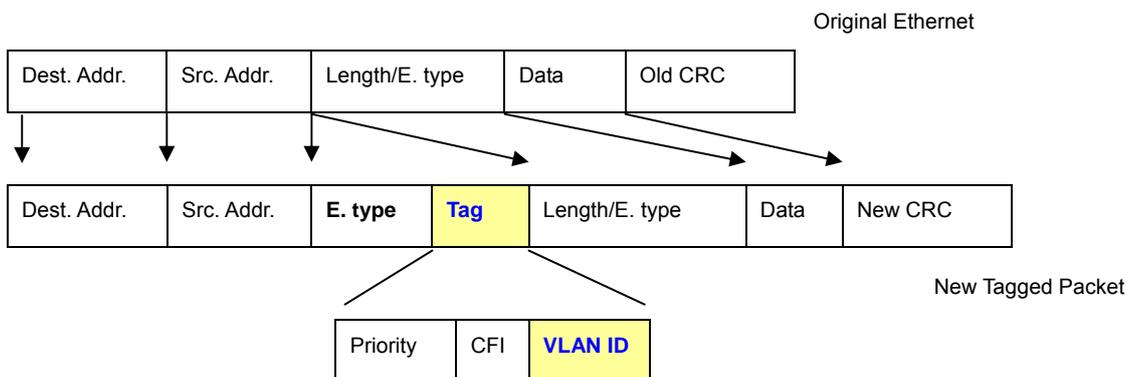
The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

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."



-
- 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.
-

■ Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs.

Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s),

either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.



VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.

■ VLAN Classification

When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

■ Port Overlapping

Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by enabled routing on this switch.

■ Untagged VLANs

Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets.

4.5.1 VLAN Membership

■ Adding Static Members to VLANs (VLAN Index)

Use the VLAN Static Table to configure port members for the selected VLAN index. The VLAN membership configuration for the switch can be monitored and modified here. Up to 64 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN. The VLAN Membership Configuration screen in [Figure 4-5-1](#) appears.

Figure 4-5-1 VLAN Membership screen

The page includes the following items:

Object	Description
VLAN ID	Specify the VLAN Identifier for the new VLAN. (You can only enter data in this field when you are creating a new VLAN.) The range of the VLAN ID is (1 to 4094) .
Add	To add a new VLAN Group with the specify VLAN ID. Once the Add button is pressed. The page will be redirect to have the VLAN member assign page.
Modify	To modify an existence VLAN Group- adds new member ports or remove ports from the selected VLAN Group.
Delete	Delete the selected VLAN Group.

4.5.1.1 Add a VLAN Group

The Gigabit Ethernet Switch supports up to 64 active VLAN groups and the range for the VLAN ID is **1-4094**.

1. To add a VLAN group, filled in the VLAN ID (from 1-4094) and please press “**Add**” button, the new VLAN Setup screen will pop out.
2. Checked the Member box to select the members for the VLAN group.
3. After setup completed, please press “**Apply**” to take affect.

As show in Figure 4-5-2 and Figure 4-5-3

Port Segmentation (VLAN) Configuration

Add a VLAN

VLAN ID

(VID: 1~4094)

Figure 4-5-2 Add a VLAN screen

VLAN Setup

VLAN ID: 2	
Port	Member
1	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>

Figure 4-5-3 VLAN Member Setup screen

4.5.1.2 Modify the VLAN Group Member

Once you want to modify the existence VLAN Group member or delete a existence VLAN Group. Refer to the following steps.

1. To modify the members of an existence VLAN Group, check the VLAN Group ID and press "**Modify**" button. The ID VLAN Setup screen will pop out.
2. To add/remove a port from specific VLAN group, just check/cancel the Member check Box and press "**Apply**" to take affect.
3. To delete an existence VLAN Group, check the VLAN Group ID and press "**Delete**" button.

As show in Figure 4-5-4 appears.

Port Segmentation (VLAN) Configuration

Add a VLAN

VLAN ID

Add
(VID: 1~4094)

VLAN Configuration List
(Maximum 64 VLAN Group)

1	2						
---	---	--	--	--	--	--	--

Modify Delete Refresh

Figure 4-5-4 VLAN Group – member modify and delete VLAN Group screen



Once the VLAN Group be deleted, the Ports with the PVID set to this VLAN Group have to re-configure the PVID. Or the PVID will be set to "**None**"

4.5.2 Per Port Configuration

The VLAN per Port Configuration page contains fields for managing ports that are part of a VLAN. The port default VLAN ID (**PVID**) is configured on the VLAN Port Configuration page. All untagged packets arriving to the device are tagged by the ports PVID.

Understand nomenclature of the Managed Industrial Switch

■ IEEE 802.1Q Tagged and Untagged

Every port on an 802.1Q compliant switch can be configured as **tagged** or **untagged**.

- Tagged:** Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into those ports. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet-forwarding decisions.
- Untagged:** Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the Switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

Frame Income / Frame Leave	Income Frame is tagged	Income Frame is untagged
Leave port is tagged	Frame remains tagged	Tag is inserted
Leave port is untagged	Tag is removed	Frame remain untagged

VLAN Per Port Configuration

The VLAN Port Configuration screen in [Figure 4-5-5](#) appears.

VLAN Per Port Configuration

VLAN Type 802.1Q VLAN

Port	Link Type	Ingress Filtering Enabled	Acceptable Frame Type	PVID
1	UnTag	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	1
2	UnTag	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	2
3	UnTag	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	1
4	UnTag	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	1
5	UnTag	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	1
6	UnTag	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	1
7	UnTag	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	1
8	UnTag	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	1

Figure 4-5-5 VLAN Port Configuration

The page includes the following fields:

Object	Description
VLAN Type	<p>There're two VLAN mode support – 802.1Q VLAN and Port-Bas VLAN</p> <ul style="list-style-type: none"> • 802.1Q – Packets income will be tagged with VID as the PVID setting. All ports on the switch belong to default VLAN (VID 1). • Port-Base - Packets can only be broadcast among other members of the same VLAN group. Note all unselected ports are treated as belonging to the default system VLAN. <p>If port-based VLAN are enabled, then VLAN-tagging feature is ignored.</p>
Port	Select the physical interface for which you want to display or configure data.
Link Type	<p>Allow 802.1Q Untagged or Tagged VLAN for selected port.</p> <p>When adding a VLAN to selected port, it tells the switch whether to keep or remove the tag from a frame on egress.</p> <ul style="list-style-type: none"> • Untag: outgoing frames without VLAN-Tagged. • Tagged: outgoing frames with VLAN-Tagged.

Ingress Filtering Enable	<p>Enabled - the frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame.</p> <p>Disabled - all frames are forwarded in accordance with the 802.1Q VLAN bridge specification. The factory default is disabled.</p>
Acceptable Frame Types	<p>Specifies the types of frames that may be received on this port. The options are 'All' and 'Tagged only'.</p> <ul style="list-style-type: none"> • All- untagged frames or priority tagged frames received on this port are accepted and assigned the value of the Port VLAN ID for this port. • Tagged only - untagged frames or priority tagged frames received on this port are discarded. <p>With either option, VLAN tagged frames are forwarded in accordance to the 802.1Q VLAN specification.</p>
PVID	<p>Allow assign PVID for selected port. The range for the PVID is 1-4094</p> <p>The PVID will be inserted into all untagged frames entering the ingress port. The PVID must as same as the VLAN ID that the port belong to VLAN group, or the untagged traffic will be dropped.</p>

4.5.3 VLAN setting example:

4.5.3.1 Two separate 802.1Q VLAN

The diagram shows how the switch handle Tagged and Untagged traffic flow for two VLANs. VLAN Group 2 and VLAN Group 3 are separated VLAN. Each VLAN isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. The screen in Figure 4-5-6 appears and Table 4-1 describes the port configuration of switch.

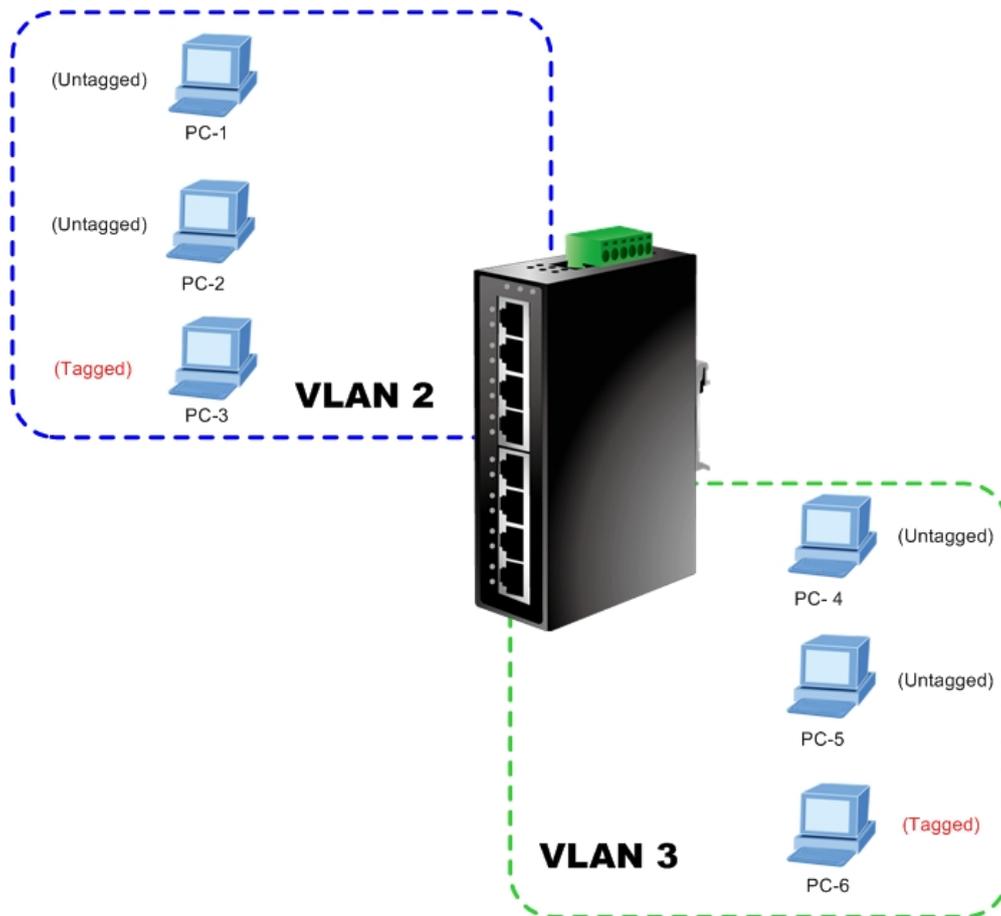


Figure 4-5-6 two separate VLAN diagram

VLAN Group	VID	Untagged Members	Tagged Members
VLAN Group 1	1	Port-7~Port-8	N/A
VLAN Group 2	2	Port-1,Port-2	Port-3
VLAN Group 3	3	Port-4,Port-5	Port-6

Table 4-1 VLAN and Port Configuration

The scenario described as follow:

■ Untagged packet entering VALN 2

1. While [PC-1] transmit an **untagged** packet enters **Port-1**, the switch will tag it with a **VLAN Tag=2**. [PC-2] and [PC-3] will received the packet through **Port-2** and **Port-3**.
2. [PC-4],[PC-5] and [PC-6] received no packet.

3. While the packet leaves **Port-2**, it will be stripped away its tag becoming an **untagged** packet.
4. While the packet leaves **Port-3**, it will keep as a **tagged** packet with **VLAN Tag=2**.

■ **Tagged packet entering VLAN 2**

5. While **[PC-3]** transmits a **tagged** packet with **VLAN Tag=2** enters **Port-3**, **[PC-1]** and **[PC-2]** will receive the packet through **Port-1** and **Port-2**.
6. While the packet leaves **Port-1** and **Port-2**, it will be stripped away its tag becoming an **untagged** packet.

■ **Untagged packet entering VLAN 3**

1. While **[PC-4]** transmits an **untagged** packet enters **Port-4**, the switch will tag it with a **VLAN Tag=3**. **[PC-5]** and **[PC-6]** will receive the packet through **Port-5** and **Port-6**.
2. While the packet leaves **Port-5**, it will be stripped away its tag becoming an **untagged** packet.
3. While the packet leaves **Port-6**, it will keep as a **tagged** packet with **VLAN Tag=3**.



At this example, VLAN Group 1 is just set as default VLAN, but only focus on VLAN 2 and VLAN 3 traffic flow

Setup steps

1. Create VLAN Group

Set VLAN Group 1 = default-VLAN with VID (VLAN ID)=1

Add two VLANs – VLAN 2 and VLAN 3

VLAN Group 2 with VID=2

VLAN Group 3 with VID=3

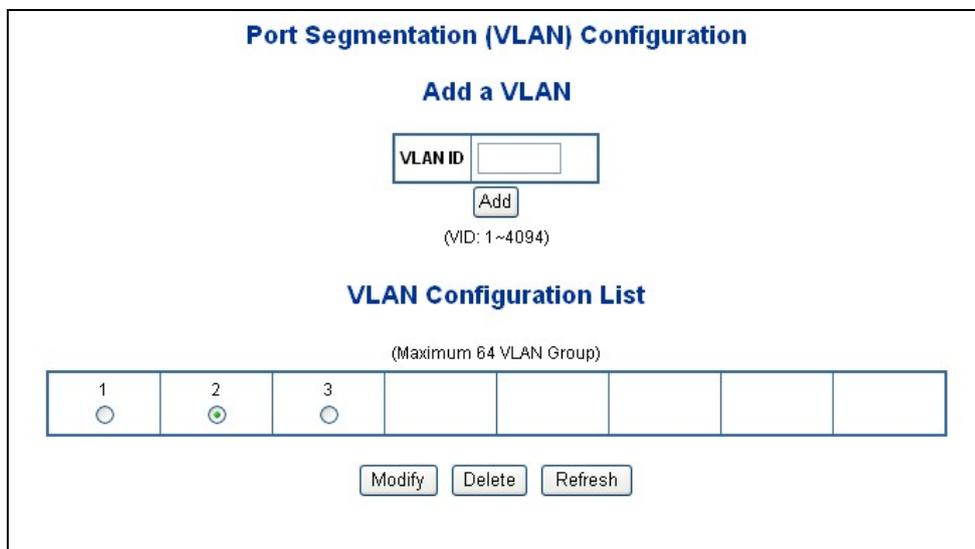


Figure 4-5-7 Add new VLAN Group screen

2. Assign VLAN Member :

VLAN 2 : Port-1,Port-2 and Port-3

VLAN 3 : Port-4, Port-5 and Port-6

VLAN 1 : All other ports – Port-7–Port-8

VLAN Setup

VLAN ID: 2	
Port	Member
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>

VLAN Setup

VLAN ID: 3	
Port	Member
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>
6	<input checked="" type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>

Figure 4-5-8 Assign VLAN members for VLAN 2 and VLAN 3

Remember to remove the Port 1 – Port 6 from VLAN 1 membership, since the Port 1 – Port 6 had been assigned to VLAN 2 and VLAN 3.

VLAN Setup

VLAN ID: 1	
Port	Member
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input checked="" type="checkbox"/>
8	<input checked="" type="checkbox"/>

Figure 4-5-9 Remove specify ports from VLAN 1 member



It's import to remove the VLAN members from VLAN 1 configuration. Or the ports would become overlap setting. (About the overlapped VLAN configuration, see next VLAN configure sample)

3. Assign PVID for each port:

Port-1,Port-2 and Port-3 : PVID=2

Port-4,Port-5 and Port-6 : PVID=3

Port-7~Port-8: PVID=1

4. Enable VLAN Tag for specific ports

Link Type: *Port-3* (VLAN-2) and *Port-6* (VLAN-3)

The Per Port VLAN configuration in Figure 4-5-10 appears.

VLAN Per Port Configuration

VLAN Type 802.1Q VLAN

Port	Link Type	Ingress Filtering Enabled	Acceptable Frame Type	Pvid
1	UnTag	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	2
2	UnTag	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	2
3	Tag	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	2
4	UnTag	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	3
5	UnTag	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	3
6	Tag	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	3
7	UnTag	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	1
8	UnTag	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	1

Apply
Cancel

Figure 4-5-10 Port 1-Port 6 VLAN Configuration

4.5.3.2 Two VLANs with overlap area

Follow the example of 4.5.3.1. There're two exist separate VLANs – VLAN 2 and VLAN 3, and the PCs of each VLANs are not able to access each other of different VLANs. But they all need to access with the same server. The screen in Figure 4-5-11 appear. This section will show you how to configure the port for the server – that could be accessed by both VLAN 2 and VLAN 3.

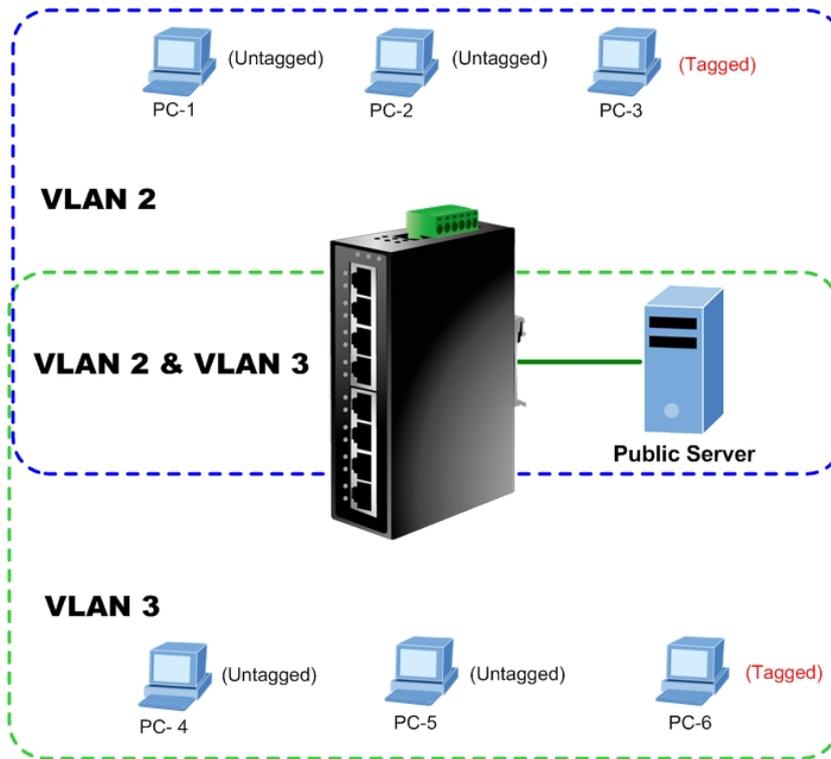


Figure 4-5-11 A Server connect to the VLAN overlap area

1. Specify **Port-7** on the device to connect to the server.
2. Assign **Port-7** to both **VLAN 2** and **VLAN 3** at the VLAN Member configuration page. The screen in Figure 4-5-12 appears.

VLAN Setup

VLAN ID: 2	
Port	Member
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input checked="" type="checkbox"/>
8	<input type="checkbox"/>

Apply Refresh

VLAN Setup

VLAN ID: 3	
Port	Member
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>
6	<input checked="" type="checkbox"/>
7	<input checked="" type="checkbox"/>
8	<input type="checkbox"/>

Apply Refresh

Figure 4-5-12 VLAN overlap port setting

- Define a **VLAN 1** as a "Public Area" that overlapping with both **VLAN 2 members** and **VLAN 3 members**.

VLAN Setup

VLAN ID: 1	
Port	Member
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>
4	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>
6	<input checked="" type="checkbox"/>
7	<input checked="" type="checkbox"/>
8	<input checked="" type="checkbox"/>

Figure 4-5-13 VLAN 1 – The public area member assign

- Setup **Port-7** with "PVID=1" at VLAN per Port Configuration page. The screen in Figure 4-5-14 appears.

VLAN Per Port Configuration

VLAN Type 802.1Q VLAN

Port	Link Type	Ingress Filtering Enabled	Acceptable Frame Type	Pvid
1	UnTag	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	2
2	UnTag	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	2
3	Tag	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	2
4	UnTag	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	3
5	UnTag	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	3
6	Tag	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	3
7	UnTag	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	1
8	UnTag	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	1

Figure 4-5-14 Setup Port-7 with PVID-1

That is, although the VLAN 2 members: Port-1 to Port-3 and VLAN 3 members: Port-4 to Port-6 also belong to VLAN 1. But with different PVID settings, packets from VLAN 2 or VLAN 3 is not able to access to the other VLAN.

4.5.3.3 VLAN Trunking between two 802.1Q aware switch

The most cases are used for “Uplink” to other switches. VLANs are separated at different switches, but they need to access with other switches within the same VLAN group. The screen in Figure-4-5-15 appears.

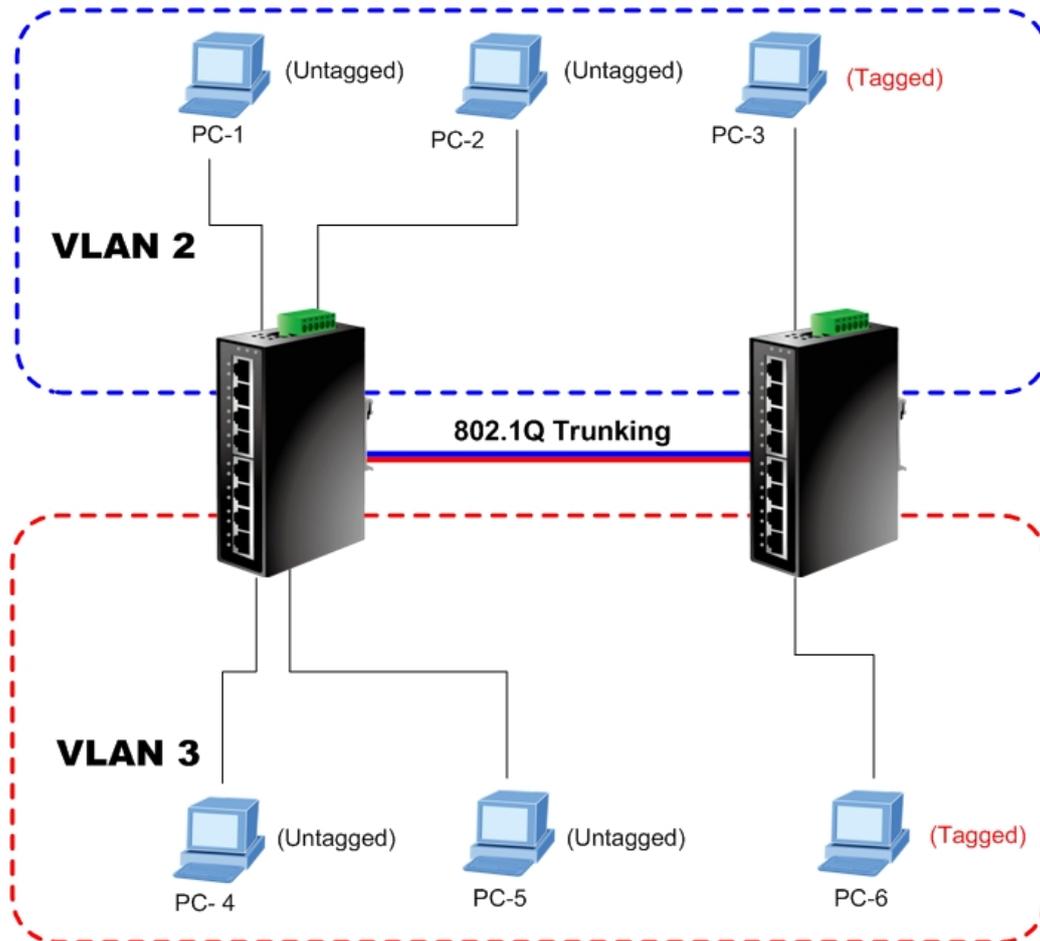


Figure 4-5-15 802.1Q Trunking with other VLAN aware device

About the VLAN ports connect to the hosts, please refer to 4.5.3.1 and 4.5.3.2 examples. The following steps will focus on the VLAN **Trunk port** configuration.

1. Specify **Port-8** to be the 802.1Q VLAN **Trunk port**, and the Trunking port must be a **Tagged** port while egress. The Port-8 configuration as the following screen in Figure 4-5-16.



Figure 4-5-16 The configuration of VLAN Trunk port

- Assign the VLAN Trunk Port to be the member of each VLAN – which wants to be aggregated. At this sample, add **Port-8** to be **VLAN 2** and **VLAN 3** member port.

VLAN Setup

VLAN ID: 2	
Port	Member
1	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input checked="" type="checkbox"/>

Apply Refresh

VLAN Setup

VLAN ID: 3	
Port	Member
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input checked="" type="checkbox"/>
5	<input checked="" type="checkbox"/>
6	<input checked="" type="checkbox"/>
7	<input type="checkbox"/>
8	<input checked="" type="checkbox"/>

Apply Refresh

Figure 4-5-17 Add VLAN Trunk port to each VLAN

- Repeat Step 1 and 2, setup the VLAN Trunk port at the partner switch.
- To add more VLANs to join the VLAN trunk, repeat Step 2 to assign the Trunk port to the VLANs.

4.6 Rapid Spanning Tree

4.6.1 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 Managed Industrial Switch include these versions:

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

Spanning Tree Protocol (STP) provides tree topography for any arrangement of bridges. STP also provides one path between end stations on a network, eliminating loops.

Rapid Spanning Tree Protocol (RSTP) - While Classic Spanning Tree guarantees preventing L2 forwarding loops in a general network topology, convergence can take up to 30-60 seconds. The convergence time is considered too long for many applications. When network topology allows, faster convergence may be possible. The **Rapid Spanning Tree Protocol (RSTP)** detects and uses of network topologies that provide faster convergence of the spanning tree, without creating forwarding loops.

The **IEEE 802.1D Spanning Tree** Protocol and **IEEE 802.1W Rapid Spanning Tree** Protocol allow 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 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

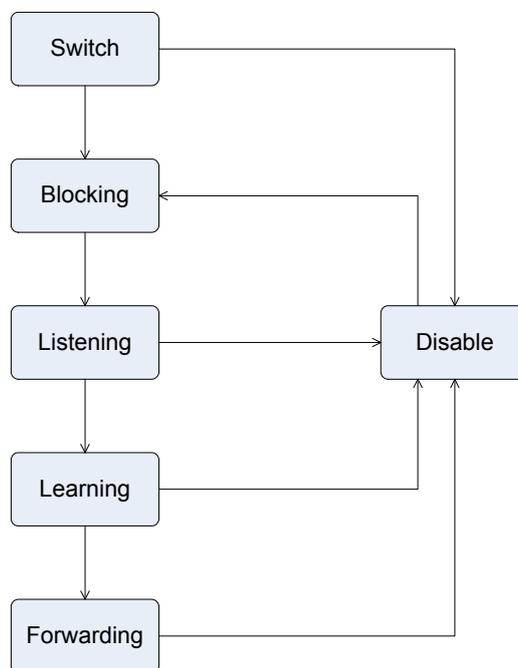


Figure 4-6-1 STP Port State Transitions

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.

2. 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



Note

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



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)

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

3. 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.

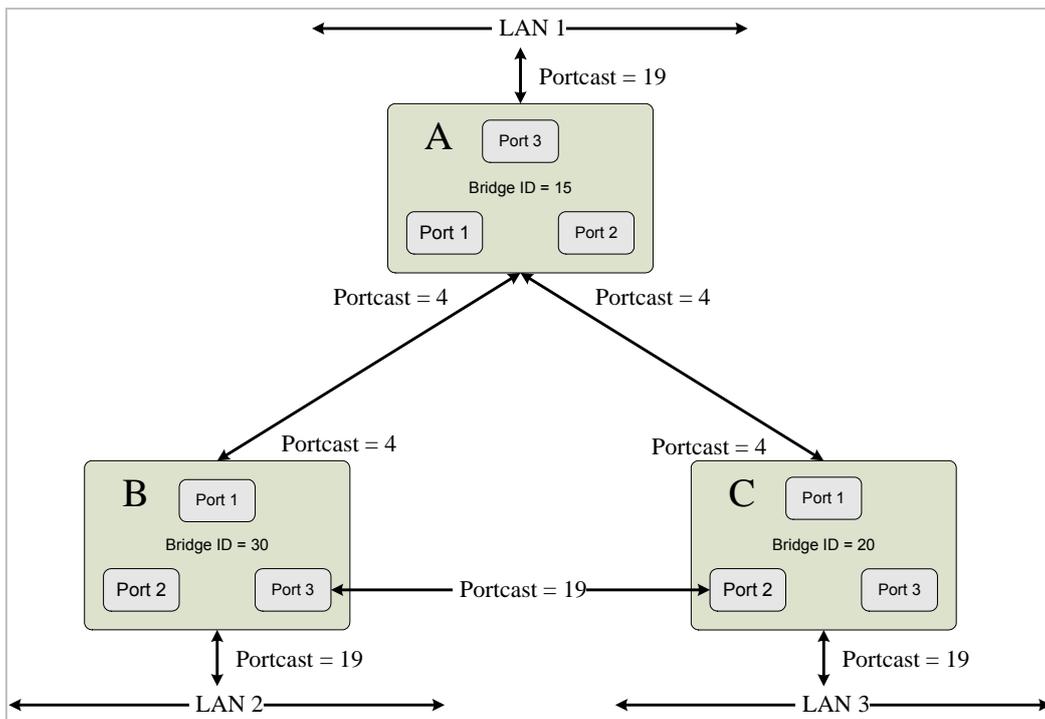


Figure 4-6-2 Before Applying the STA Rules

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

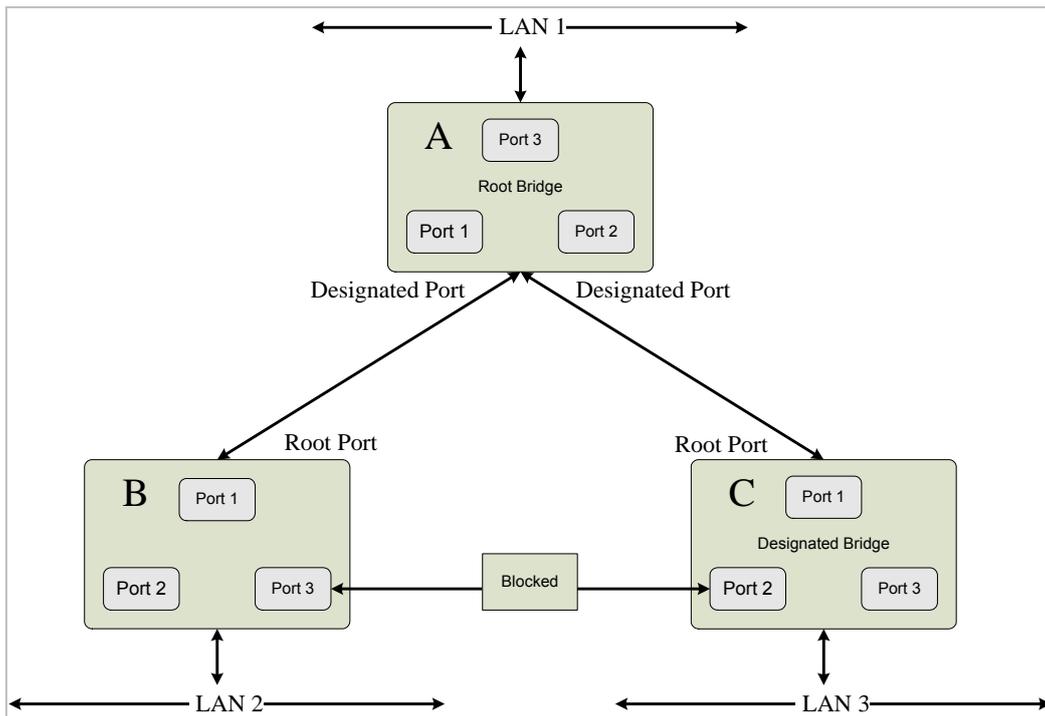


Figure 4-6-3 After Applying the STA Rules

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 = 19). 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.

4.6.2 RSTP System Configuration

This page allows you to configure RSTP system settings. The settings are used by all RSTP Bridge instances in the switch. The Managed Industrial Switch supports the following Spanning Tree protocols:

- **Compatible -- Spanning Tree Protocol (STP):** Provides a single path between end stations, avoiding and eliminating loops.
- **Normal -- Rapid Spanning Tree Protocol (RSTP) :** Detects and uses of network topologies that provide faster spanning tree convergence, without creating forwarding loops.



The Managed Industrial Switch implement the Rapid Spanning Protocol as the default spanning tree protocol. While select "**Compatibles**" mode, the system use the RSTP (802.1w) to compatible and co work with another STP (802.1d)'s BPDU control packets.

This page is to enable/disable the Spanning Tree protocol and is allow configuring the spanning tree parameters.. The Managed Industrial Switch supports IEEE 802.1d Spanning Tree (STP), IEEE 802.1w Rapid Spanning Tree (RSTP). The screen in Figure 4-6-4 appears.

RSTP System Configuration

RSTP Enabled	Enable <input type="button" value="v"/>
System Priority	32768 <input type="button" value="v"/>
Hello Time	2 (1~10)
Max Age	20 (6~40)
Forward Delay	15 (4~30)
Force version	Normal <input type="button" value="v"/>

Figure 4-6-4 RSTP System Configuration

The page includes the following fields:

Object	Description
• System Priority	Specifies the bridge priority value. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the Root Bridge. The bridge priority value is provided in increments of 4096 (4K increments). For example, 0, 4096, 8192, etc. The default value is 32768 .
• Hello Time	Specifies the device Hello Time. The Hello Time indicates the amount of time in seconds a root bridge waits between configuration messages.

	<p>Value Range: 1-10.</p> <p>The default is 2 seconds.</p>
<ul style="list-style-type: none"> • Max Age 	<p>Specifies the device Maximum Age Time. The Maximum Age Time indicates the amount of time in seconds a bridge waits before sending configuration messages.</p> <p>Value Range: 6-40.</p> <p>The default max age is 20 seconds.</p>
<ul style="list-style-type: none"> • Forward Delay 	<p>Specifies the device forward delay time. The Forward Delay Time indicates the amount of time in seconds a bridge remains in a listening and learning state before forwarding packets.</p> <p>Value Range : 4-30.</p> <p>The default is 15 seconds.</p>
<ul style="list-style-type: none"> • Force version 	<p>Specifies the Force Protocol Version parameter for the switch. The options are Normal and Compatible</p> <p>Normal – Rapid STP (802.1w): Detects and uses of network topologies that provide faster spanning tree convergence, without creating forwarding loops.</p> <p>Compatible – Classis STP (802.1d): Provides a single path between end stations, avoiding and eliminating loops.</p>



- **Max Age** -. The value lies between 6 and 40, with the value being less than or equal to " $(2 * \text{Bridge Forward Delay}) - 1$ " and greater than or equal to " $2 * (\text{Bridge Hello Time} + 1)$ ". The default value is 20.
- **Hello Time** - The value being less than or equal to " $(\text{Bridge Max Age} / 2) - 1$ ". The default hello time value is 2.
- **Forward Delay**- Bridge Forward Delay must be greater or equal to " $(\text{Bridge Max Age} / 2) + 1$ ". The time range is from 4 seconds to 30 seconds. The default value is 15.

4.6.3 RSTP Port Configuration

The RSTP Port Configuration page contains fields for assigning RSTP properties to individual ports. The screen in Figure 4-6-5 appears.

RSTP Port Configuration

Port	Edge	Path Cost	Port Priority
1	<input checked="" type="checkbox"/>	0	128
2	<input checked="" type="checkbox"/>	0	128
3	<input checked="" type="checkbox"/>	0	128
4	<input checked="" type="checkbox"/>	0	128
5	<input checked="" type="checkbox"/>	0	128
6	<input checked="" type="checkbox"/>	0	128
7	<input checked="" type="checkbox"/>	0	128
8	<input checked="" type="checkbox"/>	0	128

Figure 4-6-5 RSTP Port Configuration

The page includes the following fields:

Object	Description
Port	Indicate port 1 to port 24.
Edge	<p>Indicates whether the port is enabled as an edge port.</p> <p>Edge port cannot create loops, but it loses edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received it automatically loses edge port status.</p>
Path Cost	<p>The port contribution to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path being rerouted.</p> <p>Value Range : 1-20000000.</p> <p>Default Path Cost -- The default path cost of the port is automatically set by the port speed and the default path cost method. The default values for path costs are:</p> <ul style="list-style-type: none"> - Ethernet – 2000000. - Fast Ethernet - 200000. - Gigabit Ethernet - 20000.

Port Priority	<p>Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).</p> <p>Default: 128</p> <p>Range: 0-240, in steps of 16</p>
----------------------	--

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

Table 4-6-1 Recommended STP Path Cost Range

Port Type	Link Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex	100	2,000,000
	Full Duplex	95	1,999,999
	Trunk	90	1,000,000
Fast Ethernet	Half Duplex	19	200,000
	Full Duplex	18	100,000
	Trunk	15	50,000
Gigabit Ethernet	Full Duplex	4	10,000
	Trunk	3	5,000

Table 4-6-2 Recommended STP Path Costs

Port Type	Link Type	IEEE 802.1w-2001
Ethernet	Half Duplex	2,000,000
	Full Duplex	1,000,000
	Trunk	500,000
Fast Ethernet	Half Duplex	200,000
	Full Duplex	100,000
	Trunk	50,000
Gigabit Ethernet	Full Duplex	10,000
	Trunk	5,000

Table 4-6-3 Default STP Path Costs

4.6.4 RSTP Status

The RSTP Status page display the current **STP bridge**, **root bridge** and per port stp status.

To access **RSTP Status** screen and perform the following procedure:

1. Click **Spanning Tree** -> **RSTP Status**
2. The “**RSTP VLAN Bridge Overview**” and “**RSTP Port Status**” screen is displayed as in Figure 4-6-4..

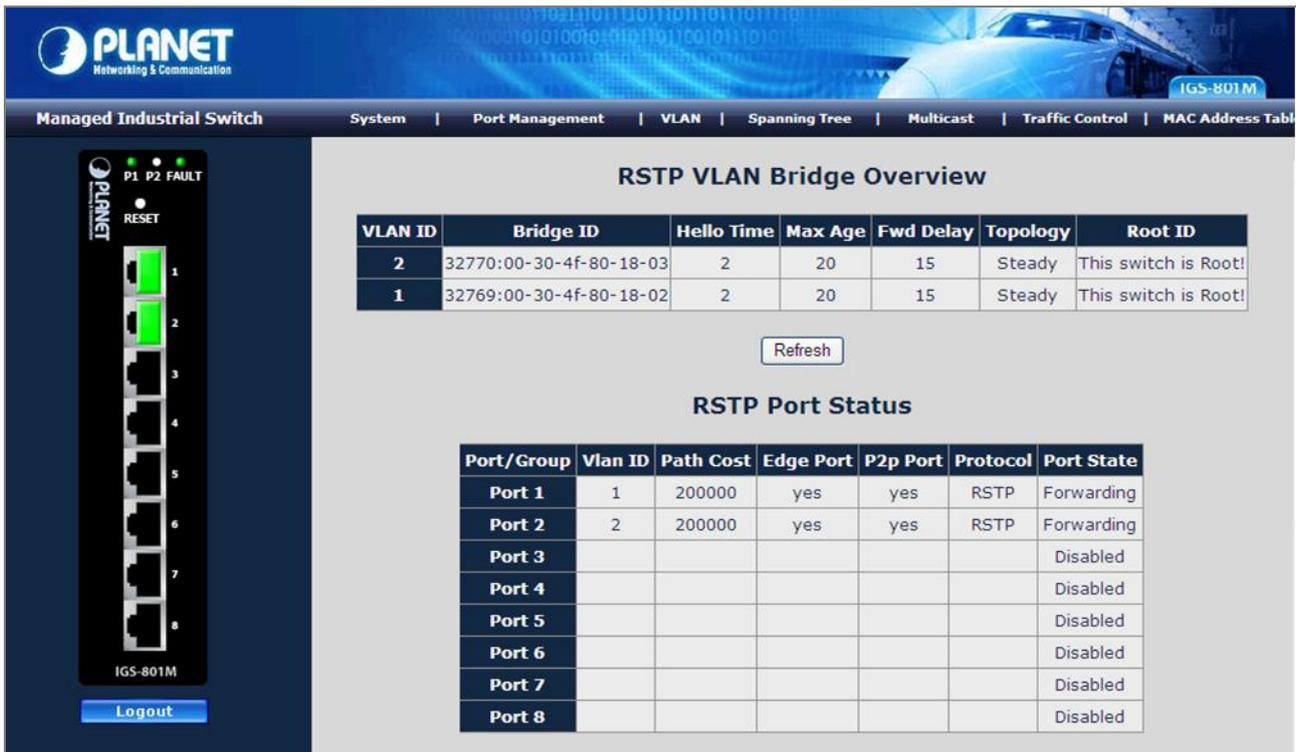


Figure 4-6-4 RSTP Status screen

■ RSTP VLAN Bridge Overview

The information of the RSTP Root shows in the Bridge overview table. The screen in Figure 4-6-7 appears.

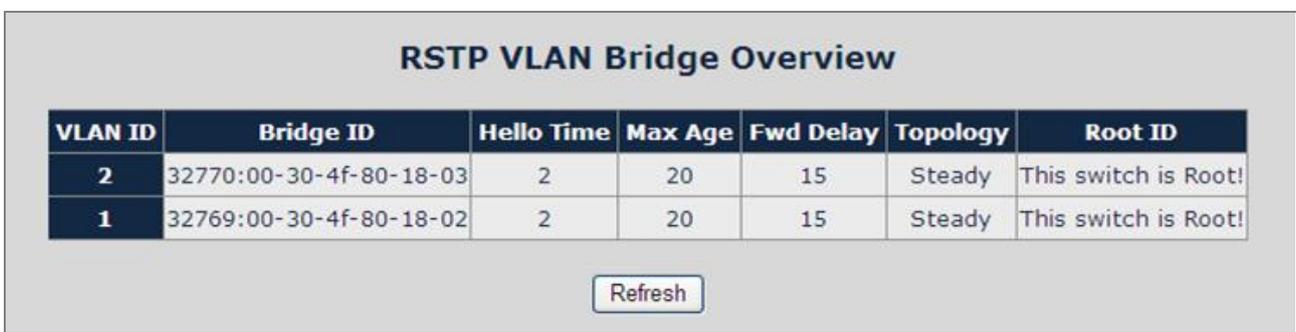


Figure 4-6-7 RSTP Status screen

The page includes the following fields:

Object	Description
VLAN Id	Identifies VLANs associated with the Rapid Spanning Tree.
Bridge IDd	Identifies the Bridge priority and MAC address.
Hello Time	Minimum time between transmissions of Configuration BPDUs.
Max Age	Path Cost to the Designated Root for the spanning tree.
Forward Delay	Derived value of the Root Port Bridge Forward Delay parameter.
Topology	Specifies the Tolology change status of the current operation. If no topology change happened, the table show " Steady ".
Root Id	Identifies the Root Bridge priority and MAC address.

■ RSTP Port Status

The information of the RSTP Per Port and Trunk group shows in the RSTP Port Status table. The screen in Figure 4-6-8 appears.

Port/Group	Vlan ID	Path Cost	Edge Port	P2p Port	Protocol	Port State
Port 1	1	200000	yes	yes	RSTP	Forwarding
Port 2	2	200000	yes	yes	RSTP	Forwarding
Port 3						Disabled
Port 4						Disabled
Port 5						Disabled
Port 6						Disabled
Port 7						Disabled
Port 8						Disabled

Figure 4-6-8 RSTP Status screen

The page includes the following fields:

Object	Description
Port/Group	Port or Link Aggregation group on which Rapid STP is enabled

VLAN Id	Port or Link Aggregation interfaces associated with VLANs associated with the Rapid Spanning Tree.
Path Cost	Cost of the port participating in the RSTP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
Edge Port	Indicates whether the port is enabled as an edge port. It takes the value "Yes" or "No".
P2p Port	The Point-to-Point operating state. This is the actual device port link type.
Protocol	Indicates the current spanning protocol on the ports.
Port State	<p>The current port STP state. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are:</p> <ul style="list-style-type: none"> • Disabled -- The port link is currently down. • Blocking -- The port is currently blocked and cannot be used to forward traffic or learn MAC addresses. Blocking is displayed when Classic STP is enabled. • Listening -- The port is currently in the listening mode. The port cannot forward traffic nor can it learn MAC addresses. • Learning -- The port is currently in the learning mode. The port cannot forward traffic however it can learn new MAC addresses. • Forwarding -- The port is currently in the forwarding mode. The port can forward traffic and learn new MAC addresses.



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.

4.7 Multicast

The **Internet Group Management Protocol (IGMP)** lets host and routers share information about multicast group 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.

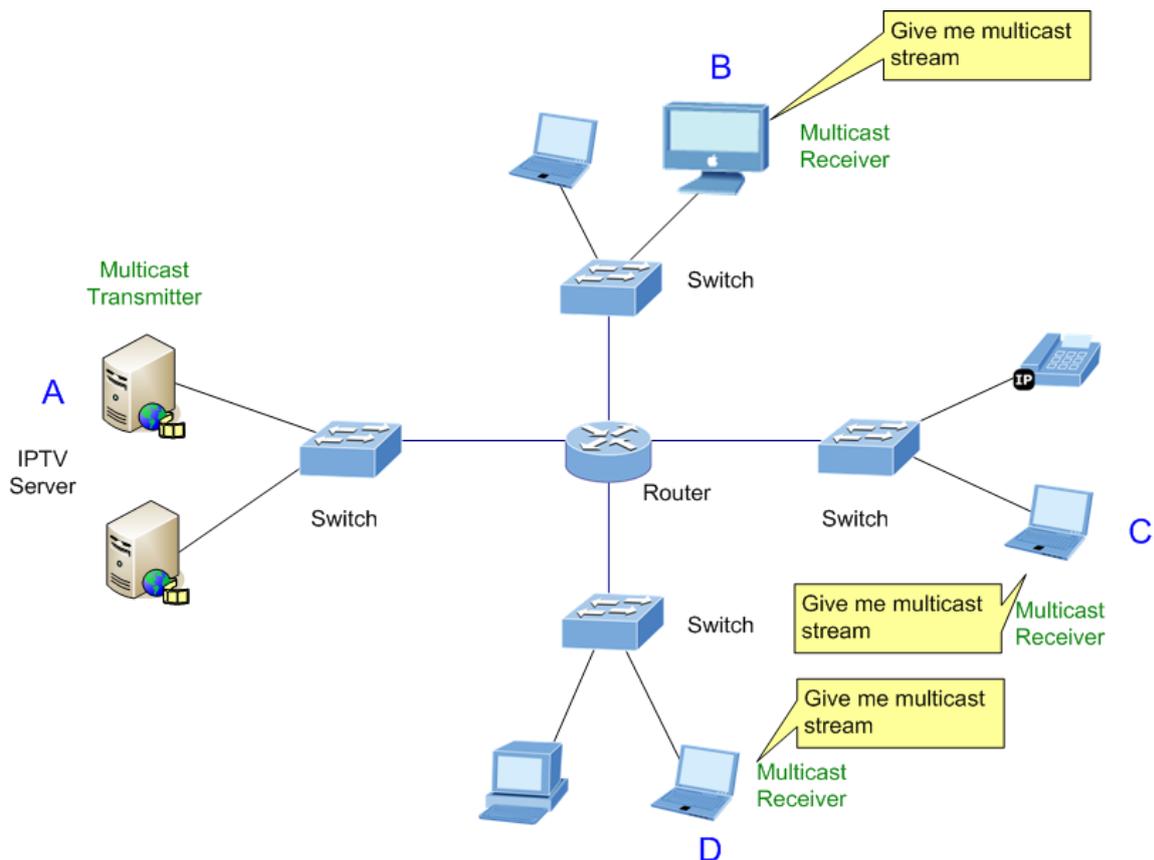


Figure 4-7-1 Multicast Service

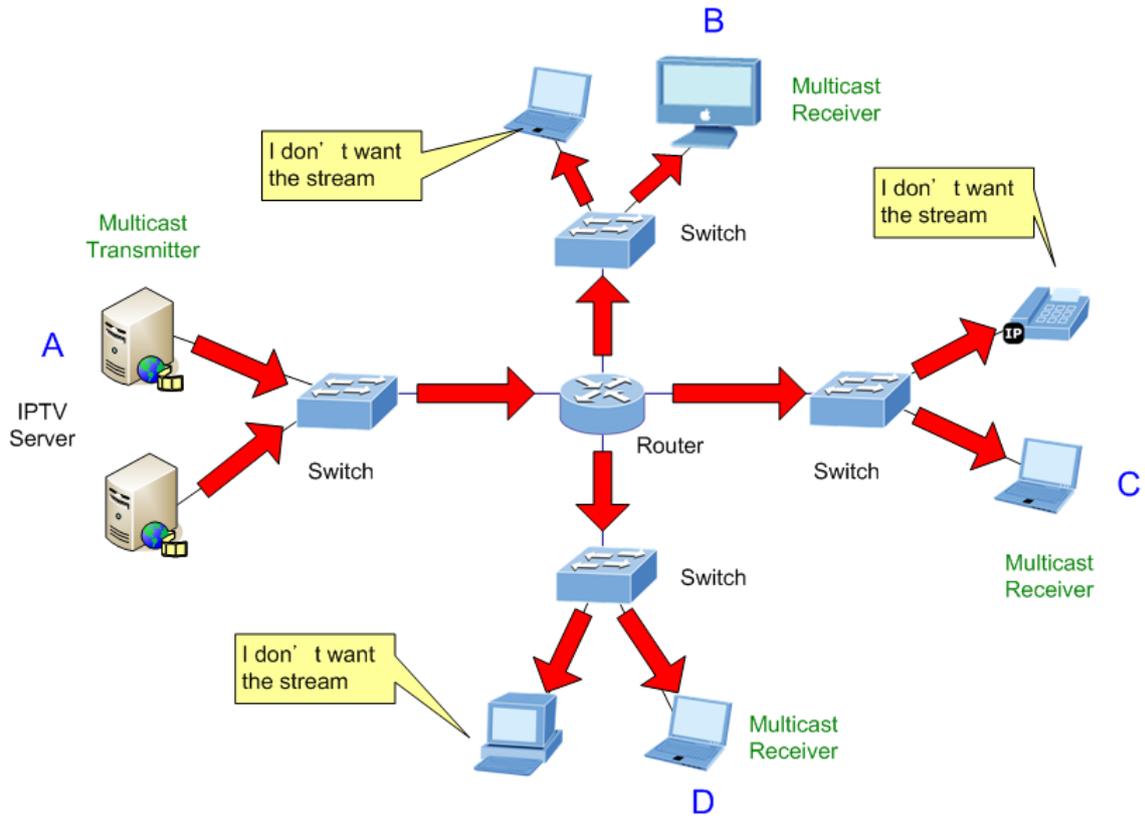


Figure 4-7-2 Multicast flooding

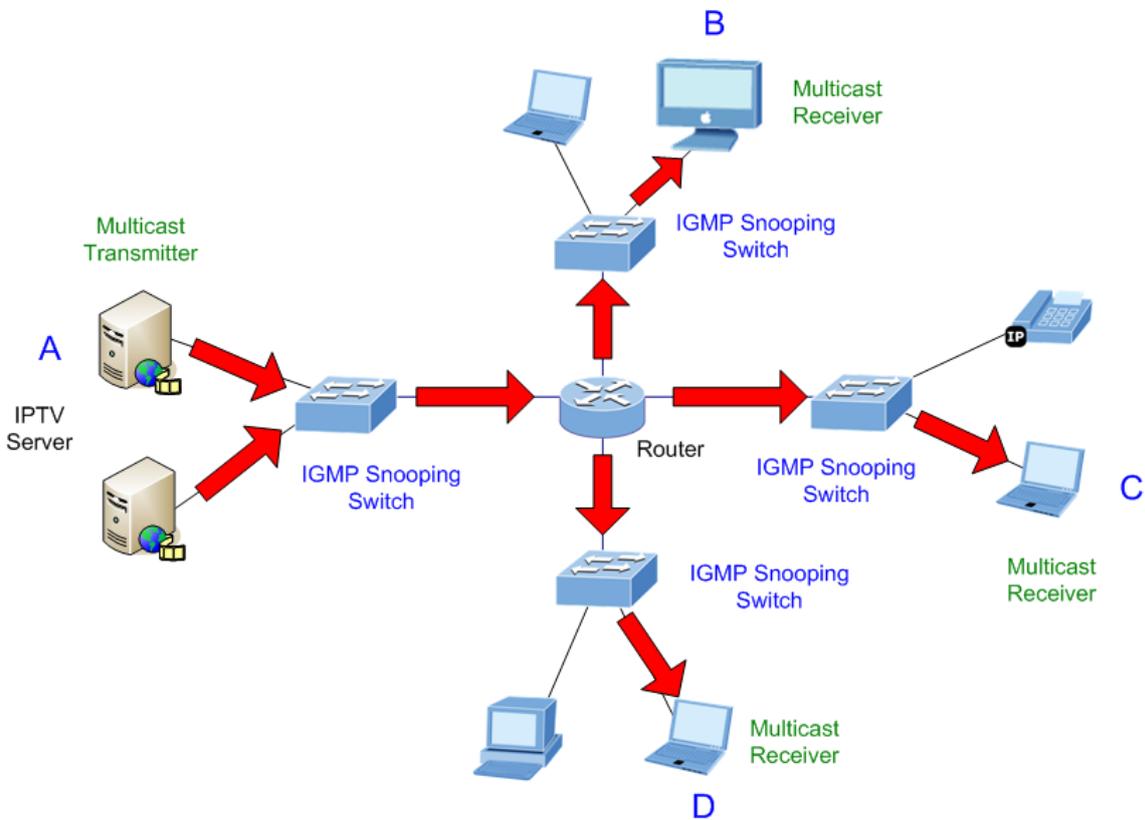


Figure 4-7-3 IGMP Snooping multicast stream control

IGMP Versions 1 and 2

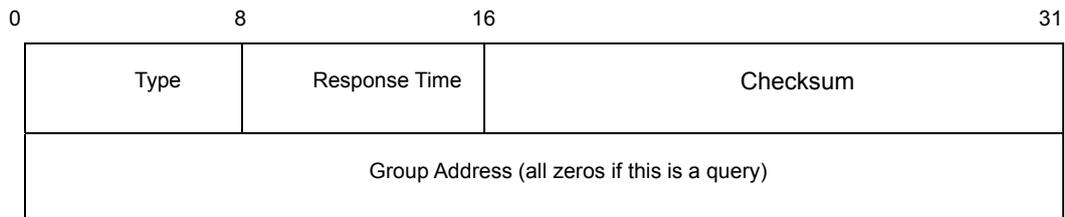
Multicast groups allow members to join or leave at any time. IGMP provides the method for members and multicast routers to communicate when joining or leaving a multicast group.

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



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:

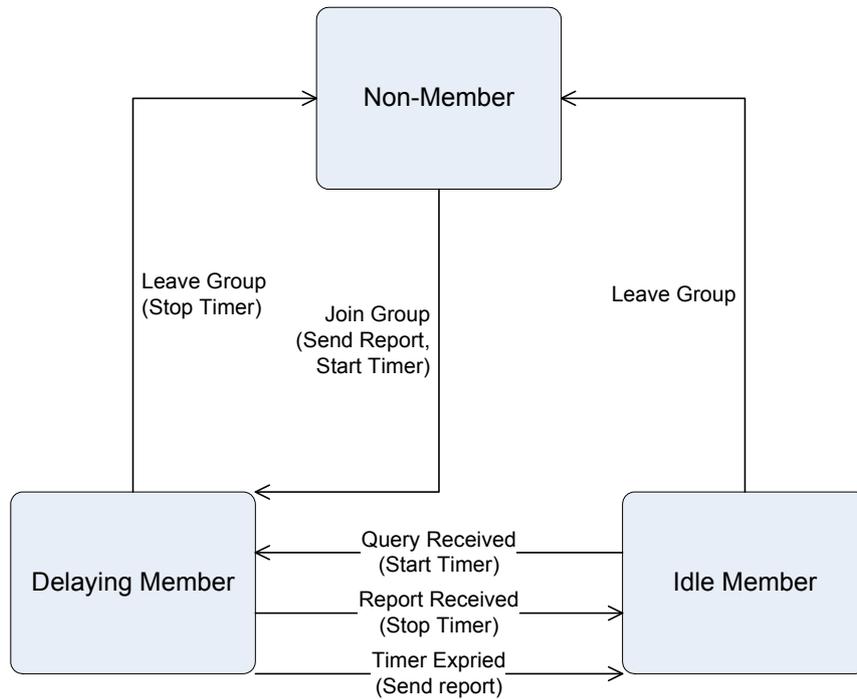


Figure 4-7-4 IGMP State Transitions

■ 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.



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

4.7.1 IGMP Snooping Configuration

The IGMP Configuration page let the administrator to configure the parameters for IGMP Snooping, which is used to build forwarding lists for multicast traffic. The screen in Figure 4-7-5 appears.

IGMP Snooping Configuration

IGMP Enabled	<input type="checkbox"/>
Router Ports	1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/>
Unregistered IPMC Flooding enabled	<input type="checkbox"/>

VLAN ID	IGMP Snooping Enabled	IGMP Querying Enabled
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 4-7-5 IGMP Snooping Configuration and Status

The page includes the following fields:

Object	Description
IGMP Enable	Enables or disables IGMP global function on the device. Disabled is the default value.
Router Ports	The Router Ports check box fields for attaching ports to a device that is attached to a neighboring Multicast router/switch. Once IGMP Snooping is enabled, Multicast packets are forwarded to the appropriate port .
Unregistered IPMC Flooding Enable	The function is to set "Enable" or "Disable" to allow the unregistered IP Multicast Group streams to flood to all ports of this switch. The unregistered IP Multicast means that the received Multicast Group address not listed in the Multicast Group Table of the switch. Enabled is the default value. The switch forwards all the multicast steams to all the host or linked switch.
VLAN ID	Identifies a VLAN and contains information about the Multicast group configuration. Add a new VLAN group and the Table will add the VLAN entry automatically.
IGMP Snooping	Enables or disables IGMP snooping on the VLAN. Ports be assign to the VLAN will

<p>Enabled</p>	<p>be applied to filter the Multicast stream. Enabled is the default value.</p>
<p>IGMP Querying Enabled</p>	<p>Enables or disables IGMP Query mode on the VLAN. The Query mode is 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. Enabled is the default value.</p>


 Note

Add a new VLAN group, the VLAN ID will be added to the table automatically with both "IGMP Snooping Enabled" and "IGMP Querying Enabled".

4.7.2 IGMP Snooping Status

The IGMP Snooping page displays the current IGMP Status and the statistics of received Query / report packets.

To open **IGMP Status** screen perform the following:

1. Click **Multicast** -> **IGMP Snooping Status**
2. The "IGMP Snooping Status" screen is displayed as in Figure 4-7-6.

IGMP Snooping Status

VLAN ID	Querier	Queries transmitted	Queries received	v1 Reports	v2 Reports	v3 Reports	v2 Leaves
1	Active	777	0	0	208	27	2
2	Active	777	0	0	5350	49	145

Figure 4-7-6 IGMP Snooping Status

The page includes the following fields:

Object	Description
VLAN ID	Identifies a VLAN and contains information about the Multicast group configuration.
Querier	<p>Display the current status of IGMP Querier on the device.</p> <p>Active – The IGMP Query function had been enabled on the device and played as a main Querier within a subnet domain. Within a network domain, there will be only one IGMP Querier. While two or more Querier exist, only one Querier operation by election.</p> <p>The Querier will transmit a IGMP Query packet about every 125 secs.</p> <p>Idle – The IGMP Querier function had be enabled but might be at the initiation status, or there're already other Querier exist.</p>
Queries transmitted	Statistics of IGMP Query packets transmitted from the VLAN. Only the "IGMP Querying Enabled" be checked, the counter is active.
Queries received	Statistics of IGMP Query packets received at the VLAN –from another switches or routers.
V1 Reports	<p>Statistics of IGMP V1 report packets received at the VLAN.</p> <p>(Packets with content type = 0x12 ; The Membership Report (version 1))</p>
V2 Reports	<p>Statistics of IGMP V2 report packets received at the VLAN.</p> <p>(Packets with content type = 0x16 ; The Membership Report (version 2))</p>
V3 Reports	Statistics of IGMP V3 report packets received at the VLAN.
V2 Leaves	<p>Statistics of IGMP V2 leave packets received at the VLAN.</p> <p>(Packets with content type = 0x17 ; Leave a Group (version 2))</p>

4.7.3 Multicast Group Table

The Multicast Group page displays the ports attached to the Multicast service group in the Ports tables. The Port a tables also reflects the manner in which the port joined the Multicast group. Ports can be added either to existing groups or to new Multicast service groups. The Bridge Multicast Group page permits new Multicast service groups to be created. The Bridge Multicast Group page also assigns ports to a specific Multicast service address group.

To open **Multicast Group Tables** screen perform the folling:

1. Click **Multicast** -> Multicast Group Table.
2. The Multicast Group Table screen is displayed as in Figure 4-7-7.

Index	Multicast Group	VID	Ports
1	01-00-5e-00-01-18	2	2
2	01-00-5e-00-00-fc	2	2
3	01-00-5e-7f-ff-fe	2	2
4	01-00-5e-50-44-53	2	2
5	01-00-5e-00-00-09	2	2
6	01-00-5e-7f-ff-fa	2	2

Page: 01 Refresh

Maximum display output : 256

Figure 4-7-7 The Multicast Group Table screen

The page includes the following fields:

Object	Description
Multicast Group entries Count	The total count of the current Multicast Group entries of the switch.
Multicast Group	Identifies the Multicast group MAC address/IP address
VID	Identifies a VLAN and contains information about the Multicast group address.
Ports	Identifies assigned ports to a specific Multicast service address group- By received Join or leave packets.

4.8 Quality of Service

4.8.1 Understand QoS

Quality of Service (QoS) is an advanced traffic prioritization feature that allows you to establish control over network traffic. QoS enables you to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical, and file-backup traffic.

QoS reduces bandwidth limitations, delay, loss, and jitter. It also provides increased reliability for delivery of your data and allows you to prioritize certain applications across your network. You can define exactly how you want the switch to treat selected applications and types of traffic.

You can use QoS on your system to:

- Classifying traffic based on packet attributes.
- Assigning priorities to traffic (for example, to set higher priorities to time-critical or business-critical applications).
- Applying security policy through traffic filtering.
- Provide predictable throughput for multimedia applications such as video conferencing or voice over IP by minimizing delay and jitter.
- Improve performance for specific types of traffic and preserve performance as the amount of traffic grows.
- Reduce the need to constantly add bandwidth to the network.
- Manage network congestion.

4.8.2 QoS Configuration

The **QoS Configuration** page contains fields for enabling or disabling QoS. In addition, the **802.1p** mode or **DSCP** mode can be selected. Both the two mode rely on predefined fields within the packet to determine the output queue. The QoS Configuration page in Figure 4-8-1 appears.

QoS Configuration

Queue Mode	<input checked="" type="radio"/> Strict <input type="radio"/> WRR Note : WRR is not supported in Jumbo Frame mode.
QoS Mode	QoS Disabled ▼ QoS Disabled 802.1p DSCP

Figure 4-8-1 QoS Configuration screen

The page includes the following fields:

Object	Description
Queue Mode	This indicates that traffic scheduling for the selected queue is based strictly or WRR (Weight Round Robin) on the queue priority.
QoS Mode	<p>Configure the QoS mode for the switch:</p> <ul style="list-style-type: none"> ■ QoS Disabled - Disables managing network traffic using Quality of Service. ■ 802.1p Mode –The output queue assignment is determined by the IEEE802.1p VLAN priority tag. ■ DSCP Mode - The output queue assignment is determined by the DSCP field.

4.8.3 802.1p QoS Mode

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

802.1Q Tag and 802.1p priority

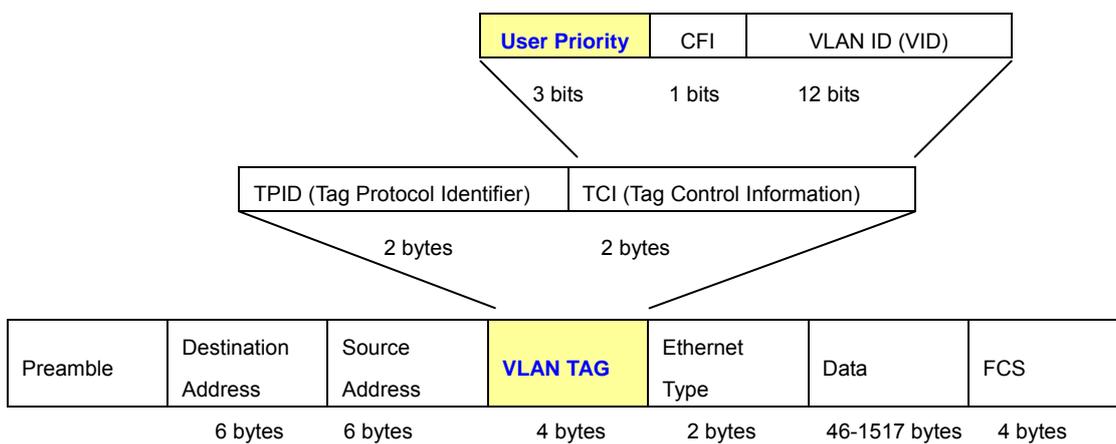


Figure 4-8-2 802.1p Tag Priority

The IEEE 802.1p Priority specification uses 4 priority levels to classify data packets. The screen in Figure 4-8-3 and Figure 4-8-4 appears.

QoS Configuration

Queue Mode	<input checked="" type="radio"/> Strict <input type="radio"/> WRR <small>Note : WRR is not supported in Jumbo Frame mode.</small>		
QoS Mode	802.1p ▼		
Prioritize Traffic	Custom ▼		

802.1p Configuration							
802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority
0	normal ▼	1	low ▼	2	low ▼	3	normal ▼
4	medium ▼	5	medium ▼	6	high ▼	7	high ▼

Figure 4-8-3 802.1p QoS Configuration screen

QoS Configuration

Queue Mode	<input checked="" type="radio"/> Strict <input type="radio"/> WRR <small>Note : WRR is not supported in Jumbo Frame mode.</small>		
QoS Mode	802.1p ▼		
Prioritize Traffic	Custom ▼ Custom All Low Priority All Normal Priority All Medium Priority All High Priority		

Figure 4-8-4 Prioritize Traffic screen

The page includes the following fields:

Object	Description
Prioritize Traffic	<p>The draw menu allows customization of 802.1p to Traffic classifiers. Total 5 selections for the Prioritize Traffic.</p> <ul style="list-style-type: none"> • Custom – Manual mapping the 802.1p priority to the 4-level queues. Setup at the next table. • All Low Priority - mapping all 802.1p tagged packets to Queue 0 • All Normal Priority - mapping all 802.1p tagged packets to Queue 1 • All Medium Priority - mapping all 802.1p tagged packets to Queue 2 • All High Priority - mapping all 802.1p tagged packets to Queue 3
802.1p Value	<p>Specifies the CoS priority tag values, where zero is the lowest and 7 is the highest.</p>
Priority	<p>The traffic forwarding queue to which the CoS priority is mapped. Four traffic priority queues are supported as follow :</p> <ul style="list-style-type: none"> • Low = Queue 0 • Normal = Queue 1 • Medium = Queue 2 • High = Queue 3

4.8.4 DSCP QoS Mode

DiffServ Code Point (DSCP) – is the traffic prioritization bits within an IP header that are encoded by certain applications and/or devices to indicate the level of service required by the packet across a network.

The **DSCP Configuration** page provides fields for defining output queue to specific DSCP fields.

Select the QoS mode to DSCP, the DSCP to queue mapping configuration page appears, as the Figure 4-8-5 shows.

Figure 4-8-5 DSCP QoS Configuration screen

The page includes the following fields:

Object	Description
Prioritize Traffic	<p>The draw menu allows customization of DSCP to Traffic classifiers. Total 5 selections for the Prioritize Traffic.</p> <ul style="list-style-type: none"> • Custom – Manual mapping the DSCP to the 4-level queues. Setup at the next table. • All Low Priority - mapping all IP DCSP header packets to Queue 0

	<ul style="list-style-type: none"> • All Normal Priority - mapping all IP DCSP header packets to Queue 1 • All Medium Priority - mapping all IP DCSP header packets to Queue 2 • All High Priority - mapping all IP DCSP header packets to Queue 3
DSCP Value (0..63)	The values of the IP DSCP header field within the incoming packet.
Priority	<p>The traffic forwarding queue to which the DSCP is mapped. Four traffic priority queues are supported.</p> <p>The queue to which packets with the specific DSCP value is assigned. The values are low,Normal,Medium and High.</p> <ul style="list-style-type: none"> • Low = Queue 0 • Normal = Queue 1 • Medium = Queue 2 • High = Queue 3

4.9 802.1X Network Access Control

Overview of 802.1X (Port-Based) Authentication

In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as **EAPOL (EAP Over LANs)** frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like **MD5-Challenge**, **PEAP**, and **TLS**. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

4.9.1 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.

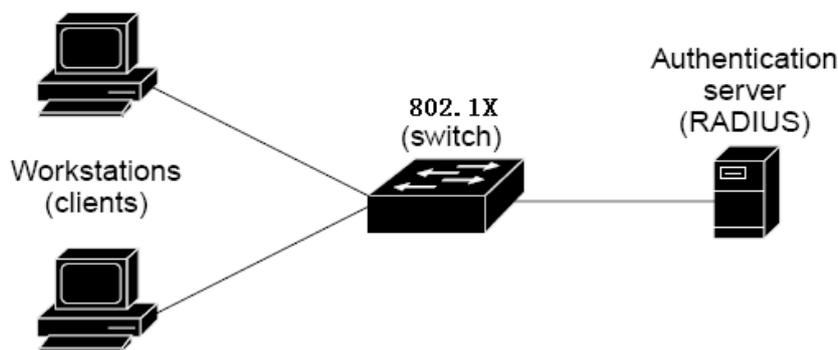


Figure 4-9-1

- **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



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. “[Figure 4-9-2](#)” shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.

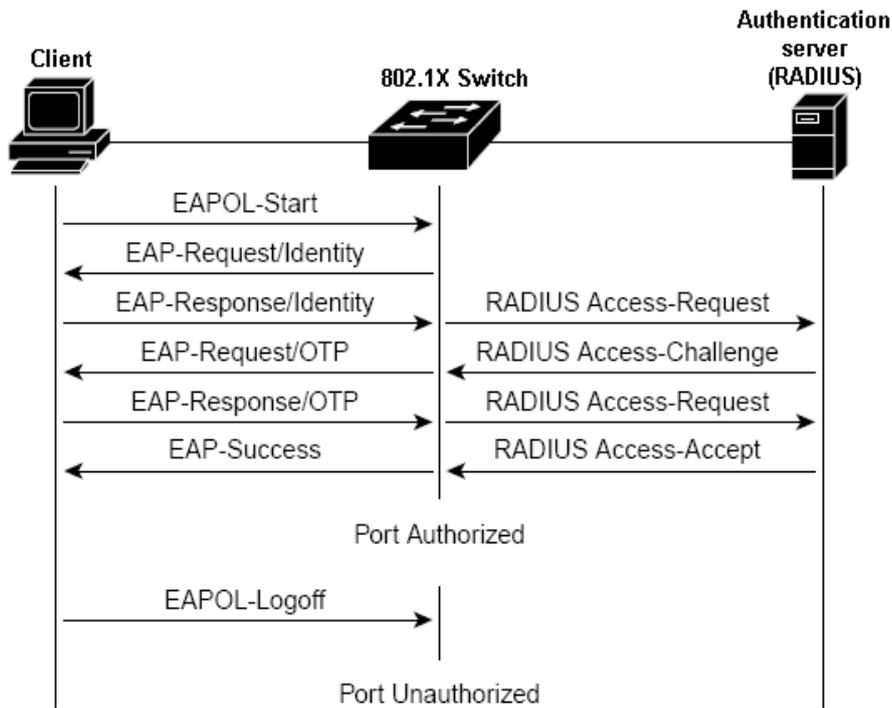


Figure 4-9-2 EAP message exchange

■ 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.

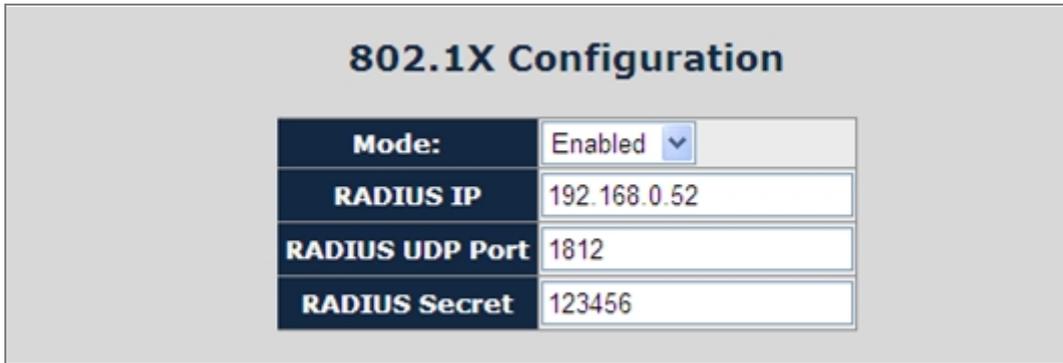
When a client logs off, it sends an EAPOL-logoff message, causing the switch port to transition to the unauthorized state.

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.

4.9.2 RADIUS Server Configuration

This page allows you to configure the **IEEE 802.1X** authentication system and port settings. The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. A central server, the RADIUS server, determines whether the user is allowed access to the network.

This page is to configure the RADIUS server connection features. The screen in Figure 4-9-3 appears.



802.1X Configuration	
Mode:	Enabled <input type="button" value="v"/>
RADIUS IP	192.168.0.52
RADIUS UDP Port	1812
RADIUS Secret	123456

Figure 4-9-3 RADIUS Server configuration table screen

The RADIUS Server configuration table includes the following fields:

Object	Description
• Mode	To Enable/Disable the port access control administrative mode. This selector lists the two options for administrative mode: enable and disable. The default value is disabled .
• RADIUS Server IP	The IP address of the RADIUS server being added.
• RADIUS UDP Port	The UDP port used by this server. The valid range is 0 - 65535. The default UDP Port No. is 1812
• RADIUS Secret	Indicates if the shared secret for this server has been configured.

Setup the RADIUS server and assign the client IP address to the Web-Smart switch. In this case, field in the default IP Address of the Web-Smart switch with 192.168.0.100. And also make sure the shared secret key is as same as the one you had set at the switch RADIUS server – 123456 at this case.

Add RADIUS Client

Client Information
Specify information regarding the client.

Client address (IP or DNS):
192.168.0.100 Verify...

Client-Vendor:
RADIUS Standard

Client must always send the signature attribute in the request

Shared secret: ****

Confirm shared secret: ****

< Back Finish Cancel

Figure 4-9-4 RADIUS Server configuration

4.9.3 802.1X Authentication Port Configuration

When 802.1X is enabled, you need to configure the parameters for the authentication process that runs between the client and the switch (i.e., authenticator), as well as the client identity lookup process that runs between the switch and authentication server. These parameters are described in this section. The 802.1X Port Configuration screen in [Figure 4-9-5](#) appears.

Port	Admin State	Port State			
1	Force Authorized	Link Down	Re-authenticate	Force Reinitialize	Statistics
2	Force Authorized	Authorized	Re-authenticate	Force Reinitialize	Statistics
3	Force Authorized	Link Down	Re-authenticate	Force Reinitialize	Statistics
4	Force Authorized	Link Down	Re-authenticate	Force Reinitialize	Statistics
5	Force Authorized	Authorized	Re-authenticate	Force Reinitialize	Statistics
6	Force Authorized	Link Down	Re-authenticate	Force Reinitialize	Statistics
7	Force Authorized	Link Down	Re-authenticate	Force Reinitialize	Statistics
8	Force Authorized	Link Down	Re-authenticate	Force Reinitialize	Statistics
			Re-authenticate All	Force Reinitialize All	

Figure 4-9-5 Per Port network access control configure table

Port	Admin State
1	Force Authorized
2	Auto
3	Force Authorized
	Force Unauthorized

Figure 4-9-6 802.1X Network access control mode selection

The Network Access Control port configuration table includes the following fields:

Object	Description
Port	Selects the port to be configured. When the selection is changed, a screen refresh will occur causing all fields to be updated for the newly selected port.

<p>Admin State</p>	<p>This selector lists the options for control mode. The control mode is only set if the link status of the port is link up. The options are:</p> <ul style="list-style-type: none"> • Auto: The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server. • Force authorized: The authenticator PAE unconditionally sets the controlled port to be authorized. • Force unauthorized: The authenticator port access entity (PAE) unconditionally sets the controlled port to unauthorized.
<p>Port State</p>	<p>This field indicates the configured control mode for the port.</p>
<p>Re-authenticate</p>	<p>This button begins the re-authentication sequence on the selected port. This button is only selectable if the control mode is 'auto'. If the button is not selectable, it will be grayed out. Once this button is pressed, the action is immediate. It is not required to press the Submit button for the action to occur.</p>
<p>Force Reinitialize</p>	<p>This button begins the re-initialization sequence on the selected port. This button is only selectable if the control mode is 'auto'. If the button is not selectable, it will be grayed out. Once this button is pressed, the action is immediate. It is not required to press the Submit button for the action to occur.</p>
<p>Statistics</p>	<p>This button redirect to the “802.1X Statistics” page on the selected port.</p>
<p>Re-authenticate All</p>	<p>This button begins the re-authentication sequence on the all ports.</p>
<p>Force Reinitialize All</p>	<p>This button begins the re-initialization sequence on all ports.</p>

At the bottom of this page, click “**Parameter**” button will redirect to the “**802.1X parameter**” configure page. The screen in Figure 4-9-7 appears.

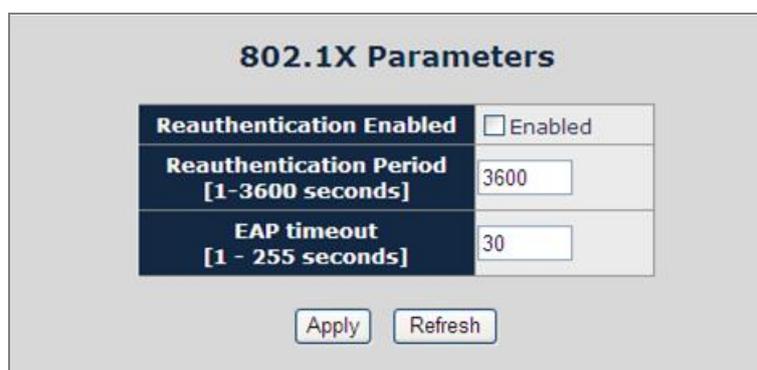


Figure 4-9-7 802.1X Parameter configuration screen

The 802.1X Parameters table includes the following fields:

Object	Description
Reauthentication Enabled	<p>This select field allows the user to enable or disable reauthentication of the supplicant for the specified port. If "Enabled" be checked, reauthentication will occur. Otherwise, reauthentication will not be allowed. Changing the selection will not change the configuration until the Apply button is pressed.</p> <p>The default value is not "Enabled"</p>
Reauthentication Period [1-3600 seconds]	<p>This input field allows the user to enter the reauthentication period for the selected port. The reauthentication period is the value, in seconds, of the timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The reauthentication period must be a value in the range of 1 and 65535. Changing the value will not change the configuration until the Apply button is pressed.</p> <p>The default value is 3600.</p>
EAP Timeout [1-255 seconds]	<p>This input field allows the user to enter the EAP timeout for the selected port. The EAP timeout is the value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The EAP timeout must be a value in the range of 1 and 255.</p> <p>The default value is 30.</p>

4.10 MAC Addresses

4.10.1 Dynamic Address Table

Use this page to set the Address Ageing Timeout for the MAC Address database, and to display information about entries in the MAC Address database. These entries are used by the transparent bridging function to determine how to forward a received frame. The screen in Figure 4-10-1 appears.

Aging Time Configuration

Aging Time
(Seconds)

 (0 ~ 65535)

MAC Address Table

MAC Address entries count : 124

Index	VID	Ports	Type	MAC Address
1	1	2	Dynamic	00-19-21-0c-85-08
2	1	2	Dynamic	00-0a-79-9f-42-03
3	1	2	Dynamic	00-0c-6e-5b-ba-c3
4	1	2	Dynamic	00-0d-61-32-23-ff
5	1	2	Dynamic	00-15-58-48-24-52
6	1	2	Dynamic	00-0c-6e-7b-ee-e0
7	1	2	Dynamic	00-14-85-03-f2-1d
8	1	2	Dynamic	00-0f-ea-f2-29-61
9	1	2	Dynamic	00-30-4f-1f-6a-43
10	1	2	Dynamic	00-0c-6e-60-8d-01

Page:

Maximum display output : 256

Figure 4-10-1 Dynamic Address Table

■ Ageing Timeout Configuration (seconds)

The MAC Address database contains static entries, which are never aged out, and dynamically learned entries, which are removed if they are not updated within a given time. You specify that time by entering a value for the Address Ageing Timeout. You may enter any number of seconds between 0 and 65535.

IEEE 802.1D recommends a default of **300** seconds, which is the factory default.

■ MAC Address Table

The MAC Address Table includes the following fields:

Object	Description
MAC Address entries count	Display the MAC address count numbers.
VID	The VLAN ID for which the table is queried.
Ports	Specifies the port numbers for which the table is queried.
Type	The MAC Address type for which the table is queried. There're two possible type- <ul style="list-style-type: none"> • Dynamic - Addresses are associated with ports by learning the ports from the frame source address. • Static - Static addresses are manually configured. Packets received with the destined MAC address match the port static MAC setting will be forward to the specify port.
MAC-Address	Specifies the MAC address for which the table is queried.

4.10.2 Static MAC Address

The Static MAC Address page contains a list of static MAC addresses. Static Address can be added and removed from the page. In addition, several MAC Addresses can be defined for a single port. The screen in Figure 4-10-2 appears.

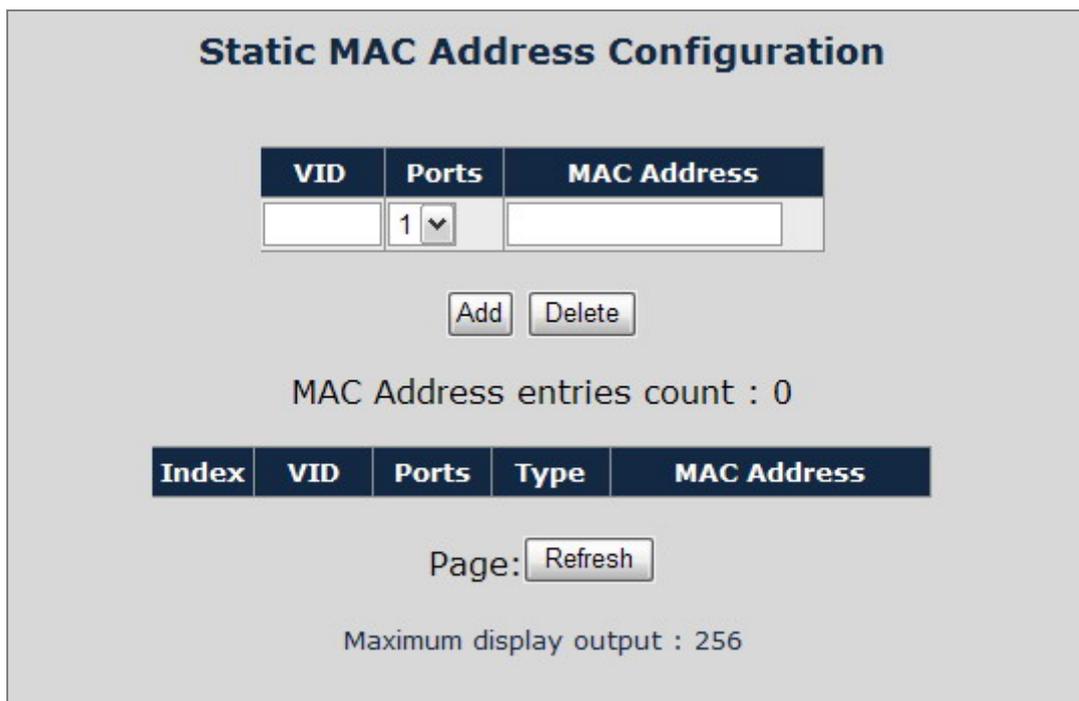


Figure-4-10-2 Static MAC Address Configuration

The configurable fields includes the following items:

Object	Description
VID	The VLAN ID attached to the MAC Address.
Ports	Specifies the port numbers for which the table is queried.
MAC-Address	Input the MAC address entry be manually bind to the specify port.

The MAC Address Table includes the following fields:

Object	Description
VID	The VLAN ID attached to the MAC Address.
Ports	Specifies the port numbers for which the table is queried.
Type	Static - Static addresses are manually configured. Packets received with the destined MAC address match the port static MAC setting will be forward to the specify port.
MAC-Address	The MAC address listed in the current static address list.

5. SWITCH OPERATION

5.1 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 information comes from the learning process of Ethernet Switch.

5.2 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.

5.3 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

5.4 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 provided 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. However, 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 significantly 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.

5.5 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-

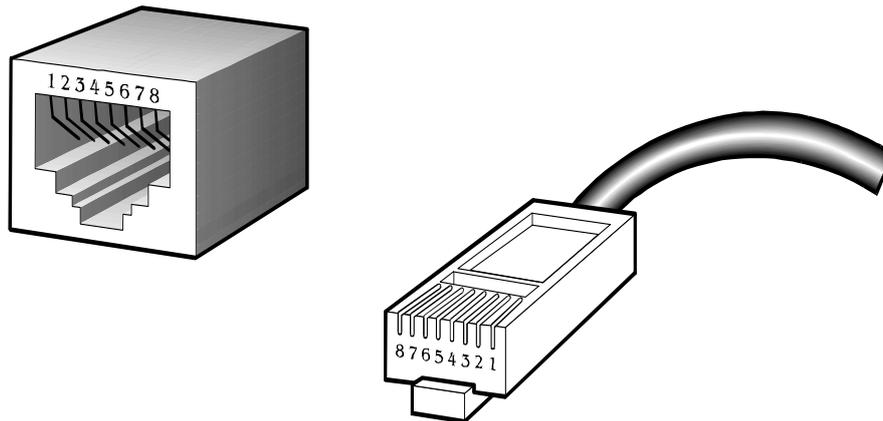
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

A.2 10/100Mbps, 10/100Base-TX

When connecting your 10/100Mbps Ethernet Switch to another switch, a bridge or a hub, a straight or crossover cable is necessary. Each port of the Switch supports auto-MDI/MDI-X detection. That means you can directly connect the Switch to any Ethernet devices without making a crossover cable. The following table and diagram show the standard RJ-45 receptacle/ connector and their pin assignments:

RJ-45 CONNECTOR PIN ASSIGNMENT		
CONTACT	MDI MEDIA DEPENDANT INTERFACE	MDI-X MEDIA DEPENDANT INTERFACE-CROSS
1	TX + (TRANSMIT)	RX + (RECEIVE)
2	TX - (TRANSMIT)	RX - (RECEIVE)
3	RX + (RECEIVE)	TX + (TRANSMIT)
4, 5	NOT USED	
6	RX - (RECEIVE)	TX - (TRANSMIT)
7, 8	NOT USED	

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:

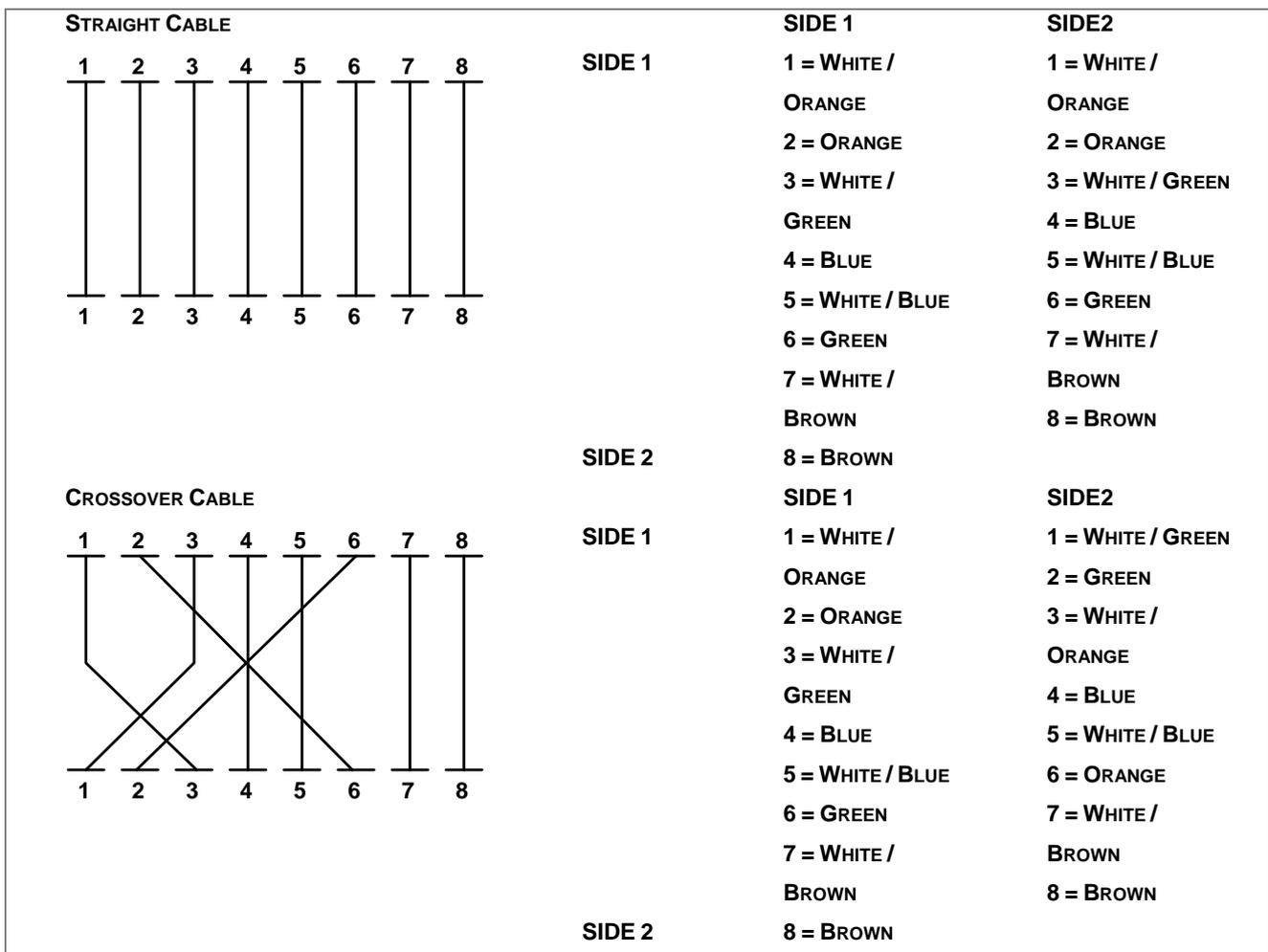


Figure A-1: Straight-Through and Crossover Cable

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

APPENDIX C : GLOSSARY

A

Aggregation

Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

(Also *Port Aggregation, Link Aggregation*).

ARP

ARP is an acronym for Address Resolution Protocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

Auto-Negotiation

Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

D

DHCP

DHCP is an acronym for Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

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.

DNS

DNS is an acronym for Domain Name System. It stores and associates many types of information with domain

names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name `www.example.com` might translate to `192.168.0.1`.

DSCP

DSCP is an acronym for **D**ifferentiated **S**ervices **C**ode **P**oint. It is a field in the header of IP packets for packet classification purposes.

E

Ethernet Type

Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

F

Fast Leave

IGMP snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously.

H

HTTP

HTTP is an acronym for **H**ypertext **T**ransfer **P**rotocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW).

HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

ICMP

ICMP is an acronym for **I**nternet **C**ontrol **M**essage **P**rotocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

IGMP is an acronym for **I**nternet **G**roup **M**anagement **P**rotocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier.

IP

IP is an acronym for **I**nternet **P**rotocol. It is a protocol used for communicating data across a internet network.

IP is a "best effort" system, which means that no packet of information sent over it is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC

IPMC is an acronym for **I**P **M**ulti**C**ast.

L

LACP

LACP is an IEEE 802.3ad standard protocol. The **L**ink **A**ggregation **C**ontrol **P**rotocol, allows bundling several physical ports together to form a single logical port.

M

MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

N

NetBIOS

NetBIOS is an acronym for **N**etwork **B**asic **I**nput/**O**utput **S**ystem. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).

The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS

NFS is an acronym for **N**etwork **F**ile **S**ystem. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.

NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

O

P

PING

`ping` is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

`ping` uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

Private VLAN

In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

Q

QoS

QoS is an acronym for **Q**uality **o**f **S**ervice. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

R

RARP

RARP is an acronym for **R**everse **A**ddress **R**esolution **P**rotocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

Router Port

A router port is a port on the Ethernet switch that leads switch towards the Layer 3 multicast device.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the **R**apid **S**panning **T**ree **P**rotocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

SNMP

SNMP is an acronym for **S**imple **N**etwork **M**anagement **P**rotocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

STP

Spanning **T**ree **P**rotocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsoleted by RSTP.

T

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP

TCP is an acronym for **T**ransmission **C**ontrol **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET

TELNET is an acronym for **TEL**etype **NET**work. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

ToS

ToS is an acronym for **T**ype **o**f **S**ervice. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

U

UDP

UDP is an acronym for **U**ser **D**atagram **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

User Priority

User Priority is a 3-bit field storing the priority level for the 802.1Q frame.

V

VLAN

Virtual LAN. A method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

EC Declaration of Conformity

For the following equipment:

*Type of Product : 8-Port 10/100/1000Mbps Industrial Ethernet Switch

*Model Number : IGS-801 / IGS-801T / IGS-801M

* Produced by:

Manufacturer's Name : **Planet Technology Corp.**

Manufacturer's Address : 11F, No. 96, Min Chuan Road, Hsin Tien,
Taipei, 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:

Emission	EN 55022	(Class A: 2006)
Harmonic	EN 61000-3-2	(2006)
Flicker	EN 61000-3-3	(1995 + A1: 2001 + A2: 2005)
Immunity	EN 55024	(1998 + A1: 2001 + A2: 2003)
ESD	IEC 61000-4-2	(2001)
RS	IEC 61000-4-3	(2008)
EFT/ Burst	IEC 61000-4-4	(2004)
Surge	IEC 61000-4-5	(2005)
CS	IEC 61000-4-6	(2008)
Magnetic Field	IEC 61000-4-8	(2001)
Voltage Disp	IEC 61000-4-11	(2004)

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: 11F, No.96, Min Chuan Road, Hsin Tien, Taipei, Taiwan, R.O.C

Person responsible for making this declaration

Name, Surname Kent Kang

Position / Title : Product Manager

Taiwan
Place

22nd, Apr., 2009
Date



Legal Signature

PLANET TECHNOLOGY CORPORATION

e-mail: sales@planet.com.tw http://www.planet.com.tw

11F, No. 96, Min Chuan Road, Hsin Tien, Taipei, Taiwan, R.O.C. Tel:886-2-2219-9518 Fax:886-2-2219-9528