PLANET
Networking & Communication

User's Manual

Industrial 24-Port 10/100/1000T + 4 1000X SFP Layer 3 Managed Switch

► IGS-6330-24T4S

www.PLANET.com.tw

Trademarks

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

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

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

FCC Warning

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

Energy Saving Note of the Device

This power required device does not support Standby mode operation. For energy saving, please remove the power cable to disconnect the device from the power circuit. In view of saving the energy and reducing the unnecessary power consumption, it is strongly suggested to remove the power connection for the device if this device is not intended to be active.

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

User's Manual of PLANET Industrial 24-Port 10/100/1000T + 4 1000X SFP Layer 3 Managed Switch

FOR MODEL: IGS-6330-24T4S

REVISION: 1.0 (February, 2015)

Part No: EM-IGS-6330-24T4S_v1.0

TABLE OF CONTENTS

1. INTRODUCTION

PLANET IGS-6330-24T4S Industrial 24-Port 10/100/1000T + 4-Port 1000X SFP Layer 3 Managed Switch (-40~75 degrees C) come with the multi-port Gigabit Ethernet Switch and SFP fiber optic connectibility, and robust layer 2 features.

The term "**Industrial Managed Switch**" is used as an alternative name in this user's manual.

1.1 Packet Contents

Open the box of the Industrial Managed Switch and carefully unpack it. The box should contain the following items:

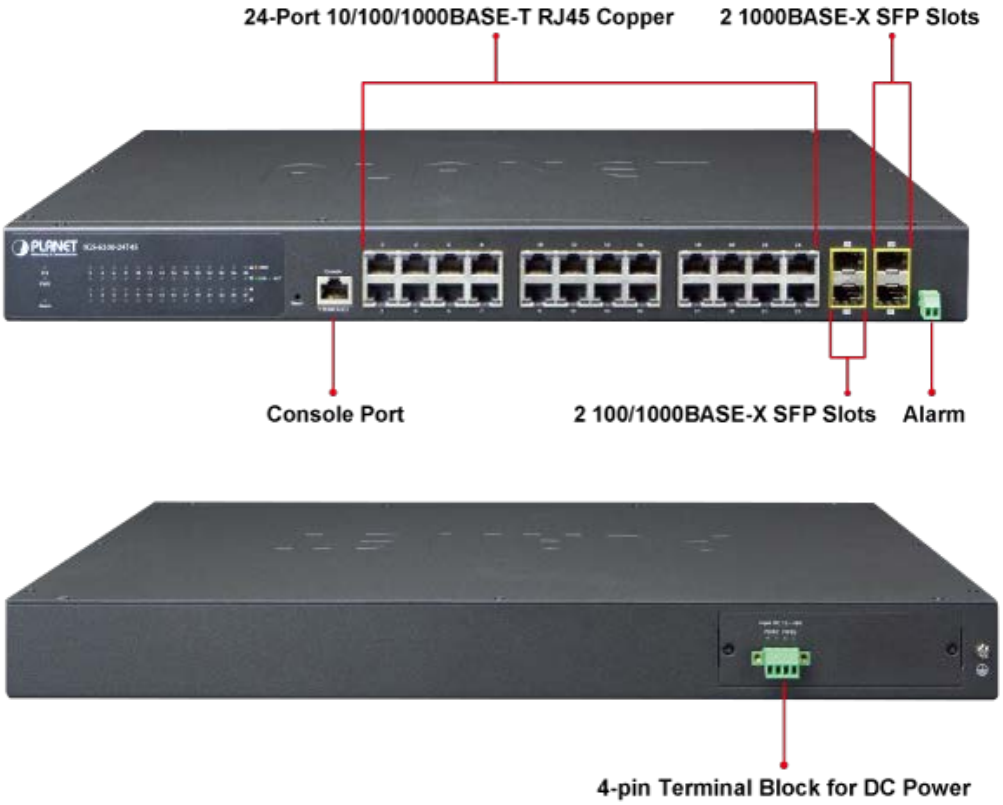
☑ **Industrial Managed Switch**	x 1
☑ **Quick Installation Guide**	x 1
☑ **RJ45 to RS232 Cable**	x 1
☑ **Two Rack-mounting Brackets with Attachment Screws**	x 1
☑ **RJ45 Dust Cap**	x 25
☑ **SFP Dust Cap**	x 4

If any of these are missing or damaged, please contact your dealer immediately; if possible, retain the carton including the original packing material, and use them again to repack the product in case there is a need to return it to us for repair.

1.2 Product Description

Powerful Layer 3 Routing Switch for Industrial Environment

PLANET IGS-6330-24T4S is an **Industrial-grade Layer 3 Rack-mount Managed Ethernet Switch** specially designed to build a full Gigabit backbone to transmit reliable but high-speed data in heavy industrial demanding environments and forward data to remote network through fiber optic. It provides **24-Port 10/100/1000BASE-T copper** and **4 extra 1000BASE-X SFP fiber optic** interfaces delivered in an IP30 rugged strong case with redundant power system, and supports various Layer 3 functions, such as **static Layer 3 routing**, **RIP v1/v2**, **OSPF v2** and **VRRP** for router redundancy.



Layer 3 Wire-speed Routing Performance and VLAN Routing for Secure and Flexible Management

With hardware-based Layer 3 routing capability, the IGS-6330-24T4S provides functionality to facilitate the deployment of applications across networks. It offers VLAN routing feature which allows to cross over different VLANs and different IP addresses for the purpose of having a highly-secured, flexible management and simpler networking application.

Dual Redundant Power to Ensure Continuous Operation

The IGS-6330-24T4S supports DC redundant power supplies to ensure reliable and continuous operation in Industrial Network. The redundant power systems of the IGS-6330-24T4S are provided to enhance the reliability with 12~48V DC power supply unit and specifically designed to fulfill the demands of high-tech facilities in handling the highest power integrity.

Environmentally Hardened Design for Mission-critical Network

With IP30 industrial metal case, the IGS-6330-24T4S provides a high level of immunity against electromagnetic interference and heavy electrical surges which are usually found on plant floors or in curbside traffic control cabinets. It also possesses an integrated power supply source with a wide range of voltages (**12 to 48V DC**) for worldwide high availability applications

requiring dual or backup power inputs. Being able to operate under the temperature range from **-40 to 75 degrees C** as well as with the fan-less cooling system, the IGS-6330-24T4S can be placed in almost any difficult environment.

Fast Recovery to a Redundant Ethernet Network

The IGS-6330-24T4S features strong and self-recovery capability to prevent interruptions and outside intrusions. It incorporates **Rapid Spanning Protocol (RSTP)** and **Multiple Spanning Tree (MSTP)** protocols that will shut down specific Ethernet interfaces when system detects a loop. The **port Link Aggregation** allows the operation of a high-speed trunk combining multiple ports and supports connection fail-over as well. It greatly protects customer's industrial automation network with switching recovery capability that is used for implementing fault tolerant ring architectures.

Efficient Traffic Control

The IGS-6330-24T4S is loaded with robust QoS features and powerful traffic management to enhance services to business-class data, voice, and video solutions. The functionality includes broadcast / multicast storm control, per port bandwidth control and QoS priority. It guarantees the best performance at VoIP and video stream transmission, and empowers the enterprises to take full advantage of the limited network resources.

Powerful Security

The Industrial Managed Giagbit Switch offers comprehensive **Access Control List (ACL)** for enforcing security to the edge. Its protection mechanisms also comprise **802.1x port-based** user and device authentication. **Port Security** allows to limit the number of users on a given port. The network administrators can now construct highly-secured corporate networks with considerably less time and effort than before.

User-friendly Secure Management

For efficient management, the IGS-6330-24T4S is equipped with console, web and SNMP management interfaces. With the built-in web-based management interface, the IGS-6330-24T4S offers an easy-to-use, platform independent management and configuration facility. The IGS-6330-24T4S supports SNMP and it can be managed via any management software based on standard of SNMP v1 and v2 protocol. For text-based management, the switch can be accessed via Telnet and the console port.

Moreover, the IGS-6330-24T4S offers remote secure management by supporting **SSH**, **SSL** and **SNMPv3** connection which can encrypt the packet content at each session.

Flexible and Extendable Solution

The 4 mini-GBIC slots built in the IGS-6330-24T4S are compatible with the **1000BASE-SX/LX and WDM SFP** (Small Form-factor Pluggable) fiber transceivers, meaning the administrator now can flexibly choose the suitable SFP transceiver according to the transmission distance required to extend the network efficiently. It is well suited for applications in the industrial data centers and distributions.

1.3 How to Use This Manual

This User's Manual is structured as follows:

Section 2, **INSTALLATION**

The section explains the functions of the **Industrial Managed Switch** and how to physically install the **Industrial Managed Switch**.

Section 3, **SWITCH MANAGEMENT**

The section contains the information about the software function of the **Industrial Managed Switch**.

Section 4, **WEB CONFIGURATION**

The section explains how to manage the **Industrial Managed Switch** by Web interface.

Section 5, **COMMAND LINE INTERFACE**

The chapter explains how to do the CLI operation of the **Industrial Managed Switch**.

Section 6, **COMMAND LINE MODE**

The chapter explains how to manage the **Industrial Managed Switch** by CLI.

Section 7, **TROUBLESHOOTING**

The chapter explains how to do troubleshooting of the **Industrial Managed Switch**.

Appendix A

The section contains cable information of the **Industrial Managed Switch**.

1.4 Product Features

- **Physical Port**
  - **24-Port 10/100/1000BASE-T** RJ45 copper
  - **4 1000BASE-X mini-GBIC/SFP** slots; Port 25 and 26 support 100/1000 dual mode SFP type
  - One RJ45 console interface for basic management and setup

- **Industrial Case / Installation**
  - IP30 metal case protection
  - Rack mount and fanless design
  - Redundant power design
    - 12 to 48V DC, redundant power with polarity reverse protect function
  - Supports EFT protection 2000 VDC for power line
  - Supports 6000 VDC Ethernet ESD protection
  - -40 to 75 degrees C operating temperature

- **IP Routing Features**
  - Static Layer 3 routing
  - Dynamic IP Routing protocol supports RIP v1/v2, OSPF v2
  - Routing interface provides per-VLAN routing mode
  - VRRP protocol for redundant routing deployment
  - Supports route redistribution

- **Layer 2 Features**
  - High performance of Store-and-Forward architecture and runt/CRC filtering eliminates erroneous packets to optimize the network bandwidth
  - Storm Control support
    - Broadcast / Unknown Multicast / Unknown Unicast
  - Supports VLAN
    - IEEE 802.1Q tagged VLAN
    - Provider Bridging (VLAN Q-in-Q) support (IEEE 802.1ad)
    - Private VLAN
    - Protocol-based VLAN
    - Voice VLAN
  - Supports Spanning Tree Protocol
    - STP, IEEE 802.1D Spanning Tree Protocol
    - RSTP, IEEE 802.1w Rapid Spanning Tree Protocol
    - MSTP, IEEE 802.1s Multiple Spanning Tree Protocol, spanning tree by VLAN
  - Supports Link Aggregation
    - Cisco ether-channel (Static Trunk)
    - Maximum 2 trunk groups, up to 4 ports per trunk group
  - Port mirroring of the incoming or outgoing traffic on a particular port

- **Quality of Service**
  - Ingress Shaper and Egress Rate Limit per port bandwidth control
  - 8 priority queues on all switch ports
  - Traffic classification
    - IEEE 802.1p CoS
  - Strict priority and Weighted Round Robin (WRR) CoS policies
  - Supports QoS and In/Out bandwidth control on each port
  - Traffic-policing policies on the switch port

- **Multicast**
  - Supports IGMP Snooping v1, v2 and v3
  - Querier mode support
  - IGMP Snooping port filtering
  - MVR (Multicast VLAN Registration)

- **Security**
  - Authentication
    - IEEE 802.1x port-based network access authentication
    - Built-in RADIUS client to co-operate with the RADIUS servers
    - RADIUS users access authentication
  - Access Control List
    - IP-based Access Control List (ACL)
    - MAC-based Access Control List

- **Management**
  - Switch Management Interfaces
    - Console / Telnet Command Line Interface
    - Web switch management
    - SNMP v1, v2c, and v3 switch management
    - SSH / SSL secure access
  - IP address / SNTP / DNS management
  - System Maintenance
    - Firmware upload/download via FTP
    - Reset button for system reboot
    - Dual Images
  - User Privilege levels control
  - SNTP (Simple Network Time Protocol)
  - Syslog remote alarm
  - SNMP trap for interface Link Up and Link Down notification
  - System Log
  - DHCP Server

1.5 Product Specifications

Model Name	**IGS-6330-24T4S**
Hardware Specifications	
Copper Ports	24 10/100/1000BASE-T RJ45 auto-MDI/MDI-X ports
SFP/mini-GBIC Slots	4 1000BASE-SX/LX/BX SFP interfaces Compatible with 100BASE-FX SFP for port 25 and 26
Console	1 x RJ45 serial port (115200, 8, N, 1)
Switch Architecture	Store-and-Forward
Switch Fabric	56Gbps / non-blocking
Throughput (packet per second)	41.6Mpps
Address Table	8K entries, automatic source address learning and ageing
Shared Data Buffer	8Mbits
Flow Control	IEEE 802.3x pause frame for full-duplex Back pressure for half-duplex
Jumbo Frame	9Kbytes
Reset Button	< 5 sec: System reboot
ESD Protection	6KV DC
EFT Protection	2KV DC
Enclosure	IP30 metal case
Installation	Rack mount kit
Connector	Removable 4-pin terminal block for power input Pin 1/2 for Power 1; Pin 3/4 for Power 2
Alarm	Removable 2-pin terminal block for fault alarm
LED Indicator	System: SYS (Green) PWR (Green) Alarm (Red) Per Port: 1000 (Orange) LNK/ACT (Green)
Dimensions (W x D x H)	440 x 253 x 44 mm
Weight	3.1kg
Power Requirements	12 to 48V DC
Power Consumption	11.6 watts / 40BTU (System on) 20.8 watts / 71BTU (Full loading)
Layer 2 Functions	
Basic Management Interfaces	Web browser, remote Telnet, SNMPv1, v2c, local console
Secure Management Interface	SSH, SSL, SNMP v3
Port Configuration	Port disable/enable Auto-negotiation 10/100/1000Mbps full and half duplex mode selection Flow control disable / enable

Port Status	Display each port's speed duplex mode, link status, flow control status, auto negotiation status, trunk status.	
Port Mirroring	TX / RX 1 to 1 monitor	
VLAN	802.1Q tagged-based VLAN, up to 255 VLAN groups Q-in-Q tunneling Private VLAN Edge (PVE) Protocol-based VLAN MVR (Multicast VLAN Registration) Up to 255 VLAN groups, out of 4094 VLAN IDs	
Link Aggregation	Static trunk Supports 2 groups of 4-port trunk support Up to 8Gbps bandwidth(duplex mode)	
QoS	Traffic classification based, strict priority and WRR 8-level priority for switching - 802.1p priority - 802.1Q VLAN tag	
IGMP Snooping	IGMP (v1/v2/v3) snooping, up to 255 multicast Groups IGMP querier mode support	
Access Control List	IP-based ACL / MAC-based ACL Up to 20 entries	
Bandwidth Control	Per port bandwidth control Ingress: 1Kbps~1000Mbps	
Storm Control	Broadcast, Unicast and Multicast storm control Supports storm control by per port and by VLAN interface Rate range: 1~1000000 Kbps	
SNMP MIBs	RFC-1213 MIB-II IF-MIB RFC 1493 Bridge MIB RFC 1643 Ethernet MIB RFC 2863 Interface MIB RFC 2665 Ether-Like MIB	RFC 2737 Entity MIB RFC 2618 RADIUS Client MIB RFC 2933 IGMP-STD-MIB RFC 3411 SNMP-Frameworks-MIB IEEE 802.1X PAE MAU-MIB
Layer 3 Functions		
IP Routing Protocol	RIP v1/v2, OSPF v2, VRRP	
Routing Table	512	
Routing Interface	Per VLAN	
Standards Conformance		
Regulation Compliance	FCC Part 15 Class A, CE	
Stability Testing	IEC 60068-2-32 (free fall) IEC 60068-2-27 (shock) IEC 60068-2-6 (vibration)	

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 802.1D Spanning Tree Protocol IEEE 802.1w Rapid Spanning Tree Protocol IEEE 802.1s Multiple Spanning Tree Protocol IEEE 802.1p Class of service	IEEE 802.1Q VLAN tagging IEEE 802.1x Port Authentication Network Control RFC 768 UDP RFC 791 IP RFC 792 ICMP RFC 2068 HTTP RFC 1112 IGMP version 1 RFC 2236 IGMP version 2 RFC 3376 IGMP version 3 RFC 2131/2132 DHCP (Server) RFC 2328 OSPF v2 RFC 1058 RIP v1 RFC 2453 RIP v2 RFC 3768 VRRP v2
Environment		
Operating	Temperature: -40 ~ 75 degrees C Relative Humidity: 5 ~ 95% (non-condensing)	
Storage	Temperature: -40 ~ 85 degrees C Relative Humidity: 5 ~ 95% (non-condensing)	

2. INSTALLATION

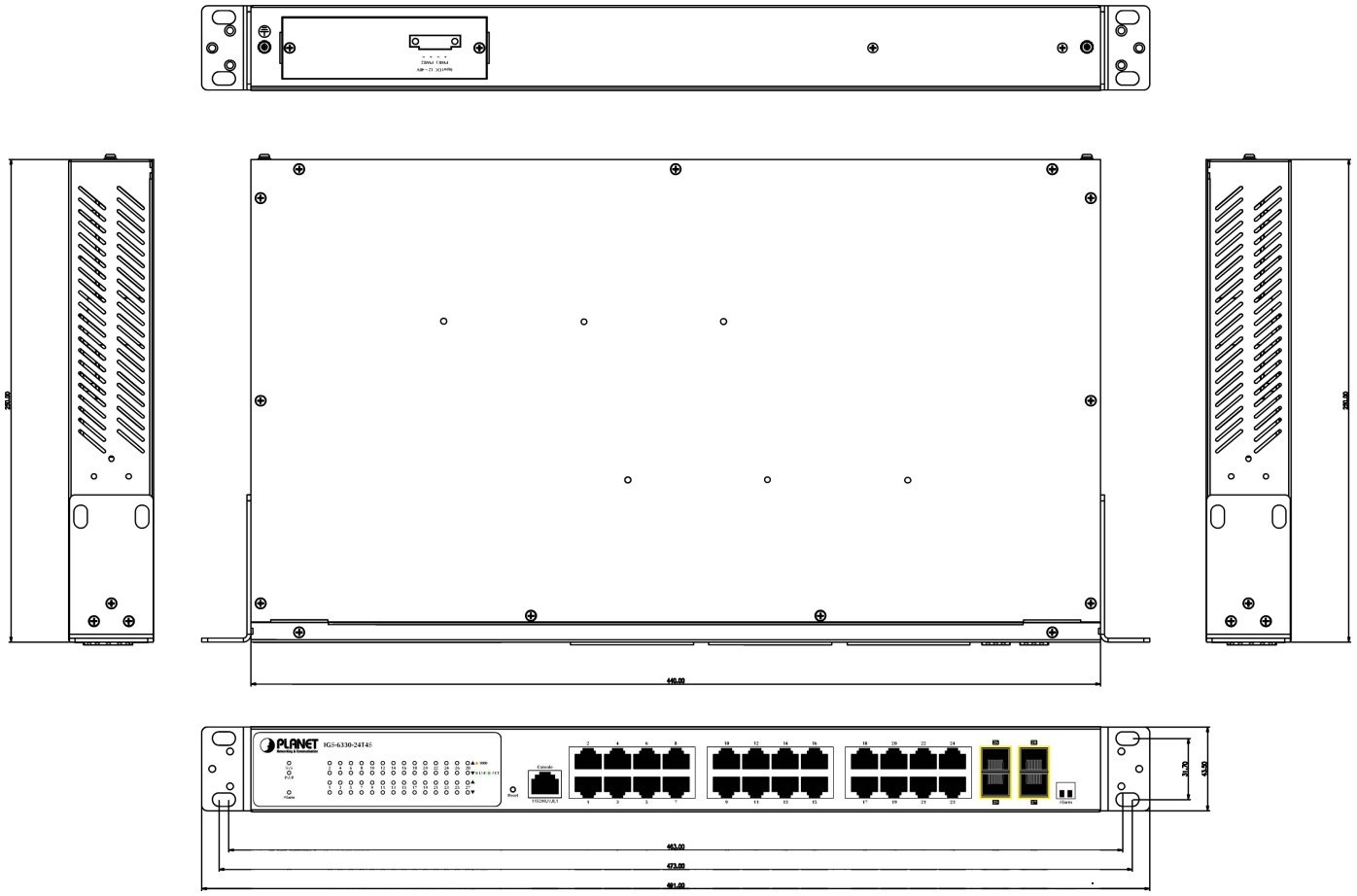
2.1 Hardware Description

The Industrial Managed Switch provides three different running speeds – 10Mbps, 100Mbps and 1000Mbps in the same Switch and automatically distinguishes the speed of incoming connection.

This section describes the hardware features of Industrial Managed Switch. For easier management and control of the Industrial Managed Switch, familiarize yourself with its display indicators and ports. Front panel illustrations in this chapter display the unit LED indicators. Before connecting any network device to the Industrial Managed Switch, read this chapter carefully.

2.1.1 Physical Dimensions

- **IGS-6330-24T4S**
  - Dimensions (W x D x H) : 440 x 44 x 253 mm



2.1.2 Front Panel

Figure 2-1 shows the front panel of **Industrial Managed Switch**.

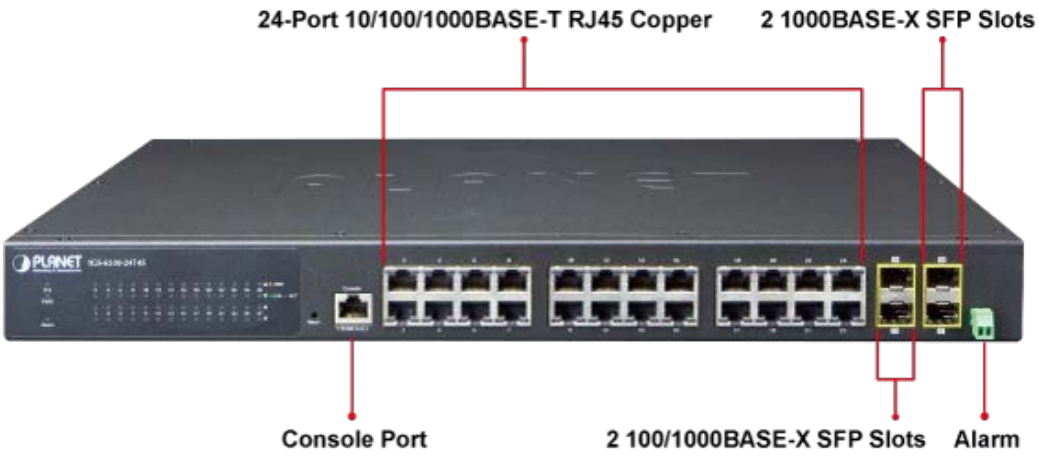


Figure 2-1: IGS-6330-24T4S Switch Front Panel

■ **Gigabit TP interface**

10/100/1000BASE-T copper, RJ45 twisted pair: Up to 100 meters.

■ **SFP slot**

100/1000BASE-X mini-GBIC slot, SFP (Small-form Factor Pluggable) transceiver module: From 550 meters to 2km (multi-mode fiber), up to above 10/20/30/40/50/70/120 kilometers (single-mode fiber).

■ **Console Port**

The console port is an RJ45 port connector. It is an interface for connecting a terminal directly. Through the console port, it provides rich diagnostic information including IP address setting, factory reset, port management, link status and system setting. Users can use the attached DB9 to RJ45 console cable in the package and connect to the console port on the device. After the connection, users can run any terminal emulation program (Hyper Terminal, ProComm Plus, Telix, Winterm and so on) to enter the startup screen of the device.

■ **Reset Button**

On the upper left side of the front panel, the reset button is designed for rebooting the Industrial Industrial Managed Switch without turning off and on the power. The following is the summary table of reset button functions:

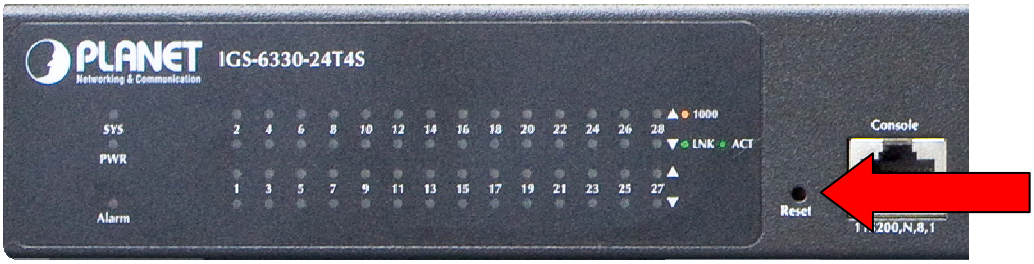


Figure 2-2: Reset button of **Industrial Managed Switch**

Reset Button Pressed and Released	Function
< 5 sec: System Reboot	Reboot the Industrial Managed Switch.

2.1.3 LED Indications

LED Definition:

■ **System**

LED	Color	Function	
SYS	**Green**	**Light**	System is working normal
		Blink	System is booting, or database is saving or remote download is in-progress
PWR	**Green**	**Light**	Switch has power
		Blink	Indicates the power failure
		Off	Switch does not have power supply
ALM	**Red**	**Light**	Indicates the switch power or port failure

■ **Per Port**

LED	Color	Function	
1000	**Orange**	**Light**	Indicates the port is running at **1000Mbps** speed and successfully established.
LNK/ACT	**Green**	**Light**	Indicates that the switch is actively sending or receiving data over that port.
		Blink	Indicates that the switch is actively sending or receiving data over port.

2.1.4 Switch Rear Panel

The rear Panel of the **Industrial Managed Switch** indicates a DC inlet power socket and consists one terminal block connector within 4 contacts. It accepts input power from 12 to 48V DC.

1. Insert positive / negative DC power wires into contacts 1 and 2 for DC Power 1, or 3 and 4 for DC Power 2.

Figure 2-3: IGS-6330-24T4S Rear Panel

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

Figure 2-4 6-Pin Terminal Block Power Wiring Input

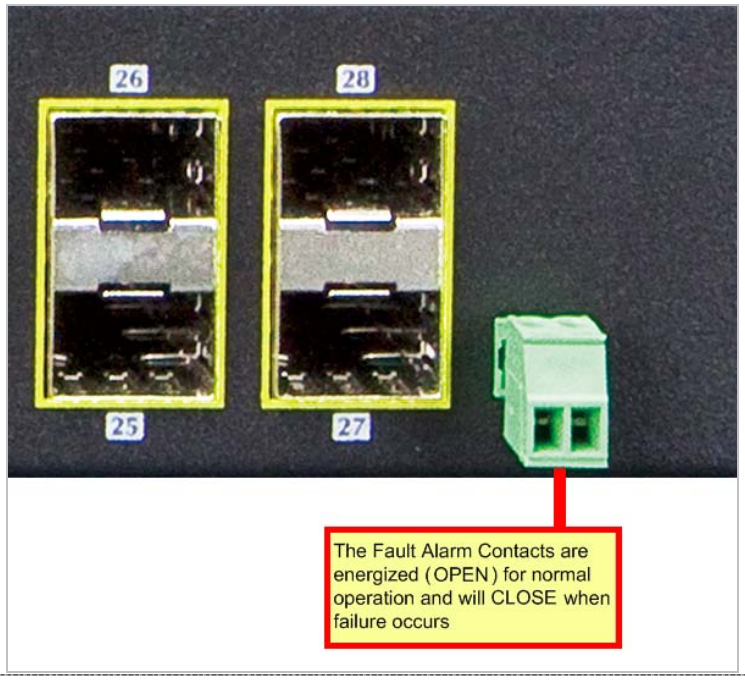
Note

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

2. When performing any of the procedures like inserting the wires or tighten the wire-clamp screws, make sure the power is OFF to prevent from getting an electric shock.

2.1.5 Wiring the Fault Alarm Contact

The fault alarm contacts of the terminal block connector are shown in the picture below. Inserting the wires, the **Industrial Managed Switch** will detect the fault status of the power failure, or port link failure (available for managed model). The following illustration shows an application example for wiring the fault alarm contacts



Insert the wires into the fault alarm contacts

Note

1. The wire gauge for the terminal block should be in the range of 12 ~ 24 AWG.
2. When performing any of the procedures like inserting the wires or tighten the wire-clamp screws, make sure the power is OFF to prevent from getting an electric shock.

2.2 Installingh the Industrial Managed Switch

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

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

2.2.1 Desktop Installation

To install the Industrial Managed Switch on desktop or shelf, please follow these steps:

Step 1: Place the Industrial Managed Switch on the desktop or the shelf near a DC power source, as shown in Figure 2-5.

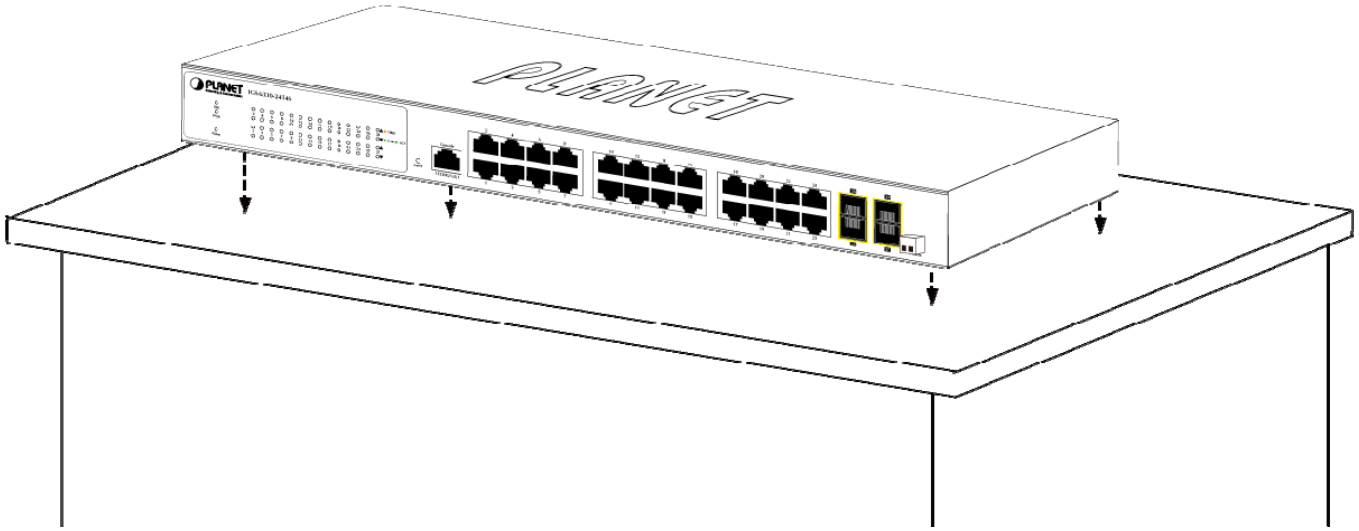


Figure 2-5: Place the Industrial Managed Switch on the Desktop

Step 2: Keep enough ventilation space between the Industrial Managed Switch and the surrounding objects.

Note

When choosing a location, please keep in mind the environmental restrictions discussed in Chapter 1, Section 4, and specifications.

Step 3: Connect the Industrial Managed Switch to network devices.

Connect one end of a standard network cable to the 10/100/1000 RJ45 ports on the front of the Industrial Managed Switch, and connect the other end of the cable to the network devices such as printer server, workstation or router.

Note

Connection to the Indurstial Managed Switch requires UTP Category 5e network cabling with RJ45 tips. For more information, please see the Cabling Specification in Appendix A.

Step 4: Supply power to the Indurstial Managed Switch.

Connect one end of the DC power source to the Managed Switch. When the Indurstial Managed Switch receives power, the Power LED should remain solid Green.

2.2.2 Rack Mounting

To install the Industrial Managed Switch in a 19-inch standard rack, please follow the instructions described below.

Step 1: Place the Indurstial Managed Switch on a hard flat surface, with the front panel positioned towards the front side.

Step 2: Attach the rack-mount bracket to each side of the Industrial Managed Switch with supplied screws attached to the

package.

Figure 2-6 shows how to attach brackets to one side of the Industrial Managed Switch.

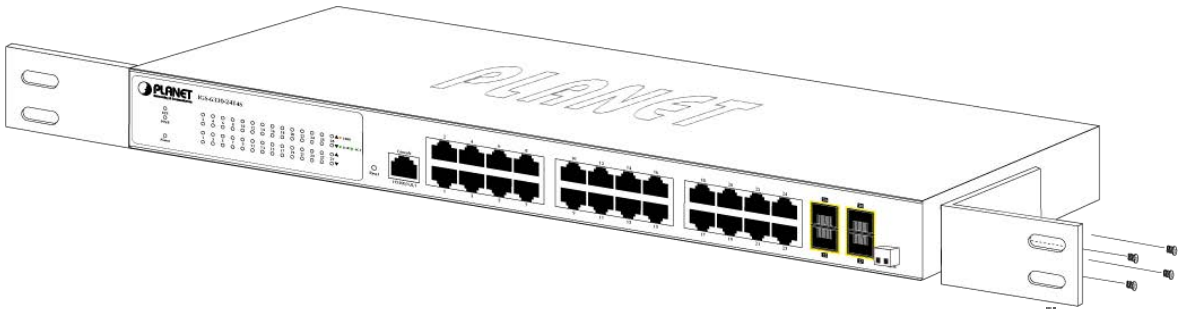


Figure 2-6: Attaching Brackets to the Industrial Managed Switch.

You must use the screws supplied with the mounting brackets. Damage caused to the parts by using incorrect screws would invalidate the warranty.

Step 3: Secure the brackets tightly.

Step 4: Follow the same steps to attach the second bracket to the opposite side.

Step 5: After the brackets are attached to the Industrial Managed Switch, use suitable screws to securely attach the brackets to the rack, as shown in Figure 2-7.

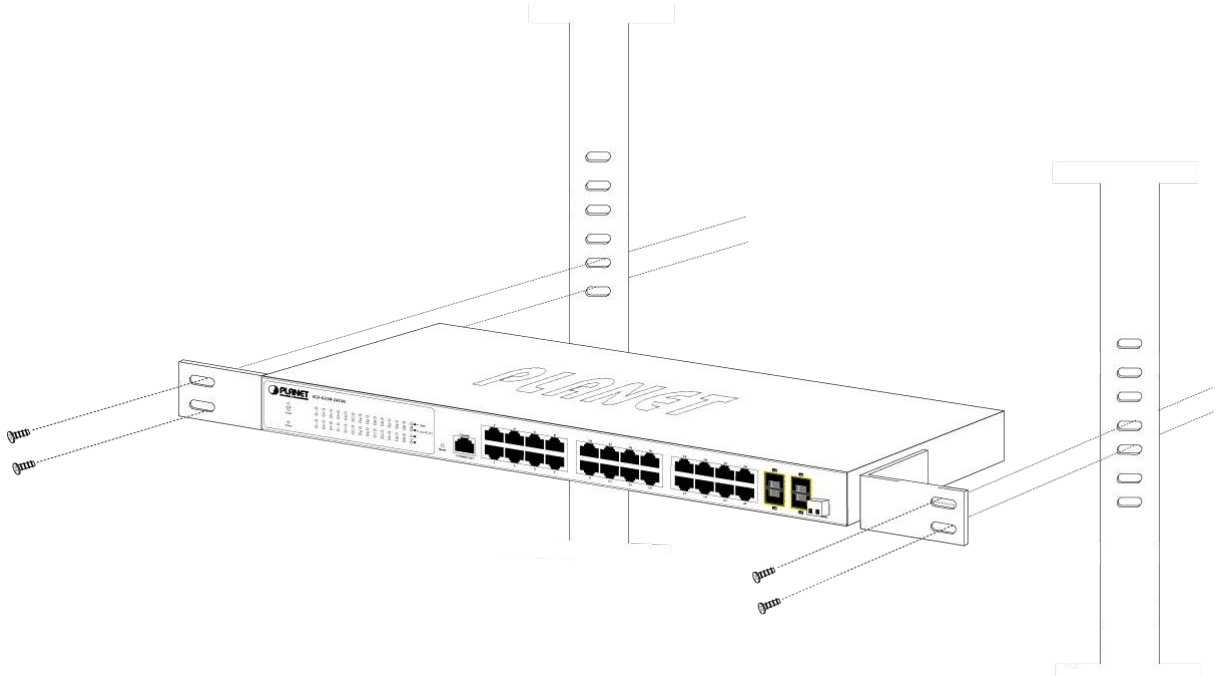


Figure 2-7: Mounting Industrial Managed Switch in a Rack

Step 6: Proceed with Steps 4 and 5 of session 2.2.1 Desktop Installation to connect the network cabling and supply power to the Industrial Managed Switch.

2.3 Cabling

- **10/100/1000BASE-T**

All 10/100/1000BASE-T ports come with auto-negotiation capability. They automatically support 1000BASE-T, 100BASE-TX and 10BASE-T networks. Users only need to plug a working network device into one of the 10/100/1000BASE-T ports, and then turn on the **Industrial Managed Switch**. The port will automatically run at 10Mbps, 20Mbps, 100Mbps or 200Mbps and 1000Mbps or 2000Mbps after negotiating with the connected device.

- **100BASE-FX / 1000BASE-SX/LX**

The **Industrial Managed Switch** has four SFP interfaces that support 100/1000Mbps dual speed mode (optional multi-mode / single-mode 100BASE-FX / 1000BASE-SX/LX SFP module).

- **Cabling**

Each 10/100/1000BASE-T port uses an RJ45 socket -- similar to phone jacks -- for unshielded twisted-pair cable (UTP). The IEEE 802.3 / 802.3u 802.3ab Fast / Gigabit Ethernet standard requires Category 5 UTP for 100Mbps 100BASE-TX. 10BASE-T networks can use Cat. 3, 4, 5 or 1000BASE-T uses Cat. 5/5e/6 UTP (see table below). Maximum distance is 100 meters (328 feet). The 100BASE-FX / 1000BASE-SX/LX SFP slot uses an LC connector with optional SFP module. Please see table below and know more about the cable specifications.

Port Type	Cable Type	Connector
10BASE-T	Cat. 3, 4, 5, 2-pair	RJ45
100BASE-TX	Cat. 5 UTP, 2-pair	RJ45
1000BASE-T	Cat. 5/5e/6 UTP, 2-pair	RJ45
100BASE-FX	50 / 125μm or 62.5 / 125μm multi-mode 9 / 125μm single-mode	LC (multi / single mode)
1000BASE-SX/LX	50 / 125μm or 62.5 / 125μm multi-mode 9 / 125μm single-mode	LC (multi / single mode)

Any Ethernet devices like hubs and PCs can connect to the **Industrial Managed Switch** by using straight-through wires. The two 10/100/1000Mbps ports are auto-MDI/MDI-X and can be used on straight-through or crossover cable.

2.3.1 Installing the SFP Transceiver

The sections describe how to insert an SFP transceiver into an SFP slot. The SFP transceivers are hot-pluggable and hot-swappable. You can plug in and out the transceiver to/from any SFP port without having to power down the **Industrial Managed Switch** as the Figure 2-8 appears.

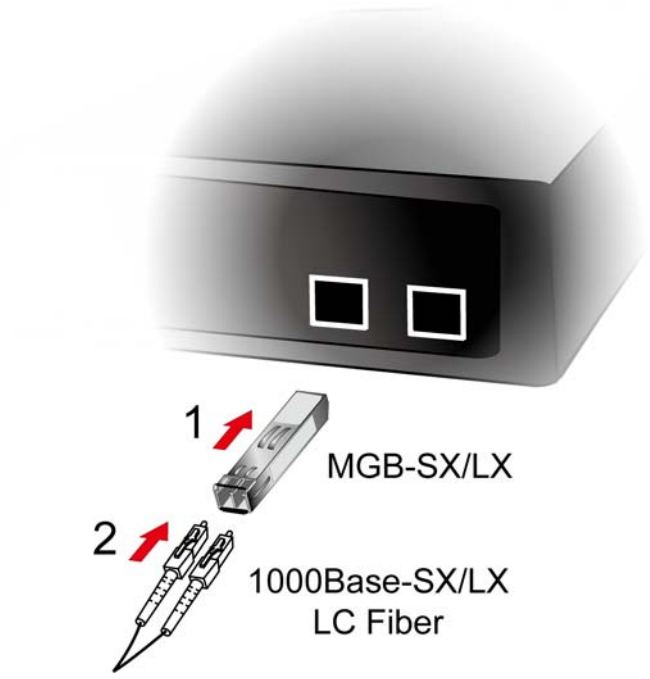


Figure 2-8: Plugging in the SFP Transceiver

■ Approved PLANET SFP Transceivers

PLANET **Industrial Managed Switch** supports 100/1000 dual mode with both single mode and multi-mode SFP transceivers. The following list of approved PLANET SFP transceivers is correct at the time of publication:

Fast Ethernet Transceiver (100BASE-X SFP)

Model	Speed (Mbps)	Connector Interface	Fiber Mode	Distance	Wavelength (nm)	Operating Temp.
MFB-FX	100	LC	Multi Mode	2km	1310nm	0 ~ 60 degrees C
MFB-F20	100	LC	Single Mode	20km	1310nm	0 ~ 60 degrees C
MFB-F40	100	LC	Single Mode	40km	1310nm	0 ~ 60 degrees C
MFB-F60	100	LC	Single Mode	60km	1310nm	0 ~ 60 degrees C
MFB-F120	100	LC	Single Mode	120km	1550nm	0 ~ 60 degrees C
MFB-TFX	100	LC	Multi Mode	2km	1310nm	-40 ~ 75 degrees C
MFB-TF20	100	LC	Single Mode	20km	1550nm	-40 ~ 75 degrees C

Fast Ethernet Transceiver (100BASE-BX, Single Fiber Bi-Directional SFP)

Model	Speed (Mbps)	Connector Interface	Fiber Mode	Distance	Wavelength (TX/RX)	Operating Temp.
MFB-FA20	100	WDM(LC)	Single Mode	20km	1310nm / 1550nm	0 ~ 60 degrees C
MFB-FB20	100	WDM(LC)	Single Mode	20km	1550nm / 1310nm	0 ~ 60 degrees C
MFB-TFA20	100	WDM(LC)	Single Mode	20km	1310nm / 1550nm	-40 ~ 75 degrees C
MFB-TFB20	100	WDM(LC)	Single Mode	20km	1550nm / 1310nm	-40 ~ 75 degrees C
MFB-TFA40	100	WDM(LC)	Single Mode	40km	1310nm / 1550nm	-40 ~ 75 degrees C
MFB-TFB40	100	WDM(LC)	Single Mode	40km	1550nm / 1310nm	-40 ~ 75 degrees C

Gigabit Ethernet Transceiver (1000BASE-X SFP)

Model	Speed (Mbps)	Connector Interface	Fiber Mode	Distance	Wavelength (nm)	Operating Temp.
MGB-GT	1000	Copper	--	100m	--	0 ~ 60 degrees C
MGB-SX	1000	LC	Multi Mode	550m	850nm	0 ~ 60 degrees C
MGB-SX2	1000	LC	Multi Mode	2km	1310nm	0 ~ 60 degrees C
MGB-LX	1000	LC	Single Mode	10km	1310nm	0 ~ 60 degrees C
MGB-L30	1000	LC	Single Mode	30km	1310nm	0 ~ 60 degrees C
MGB-L50	1000	LC	Single Mode	50km	1550nm	0 ~ 60 degrees C
MGB-L70	1000	LC	Single Mode	70km	1550nm	0 ~ 60 degrees C
MGB-L120	1000	LC	Single Mode	120km	1550nm	0 ~ 60 degrees C
MGB-TSX	1000	LC	Multi Mode	550m	850nm	-40 ~ 75 degrees C
MGB-TLX	1000	LC	Single Mode	10km	1310nm	-40 ~ 75 degrees C
MGB-TL30	1000	LC	Single Mode	30km	1310nm	-40 ~ 75 degrees C
MGB-TL70	1000	LC	Single Mode	70km	1550nm	-40 ~ 75 degrees C

Gigabit Ethernet Transceiver (1000BASE-BX, Single Fiber Bi-Directional SFP)

Model	Speed (Mbps)	Connector Interface	Fiber Mode	Distance	Wavelength (TX/RX)	Operating Temp.
MGB-LA10	1000	WDM(LC)	Single Mode	10km	1310nm / 1550nm	0 ~ 60 degrees C
MGB-LB10	1000	WDM(LC)	Single Mode	10km	1550nm / 1310nm	0 ~ 60 degrees C
MGB-LA20	1000	WDM(LC)	Single Mode	20km	1310nm / 1550nm	0 ~ 60 degrees C
MGB-LB20	1000	WDM(LC)	Single Mode	20km	1550nm / 1310nm	0 ~ 60 degrees C
MGB-LA40	1000	WDM(LC)	Single Mode	40km	1310nm / 1550nm	0 ~ 60 degrees C
MGB-LB40	1000	WDM(LC)	Single Mode	40km	1550nm / 1310nm	0 ~ 60 degrees C
MGB-LA60	1000	WDM(LC)	Single Mode	60km	1310nm / 1550nm	0 ~ 60 degrees C
MGB-LB60	1000	WDM(LC)	Single Mode	60km	1550nm / 1310nm	0 ~ 60 degrees C
MGB-TLA10	1000	WDM(LC)	Single Mode	10km	1310nm / 1550nm	-40 ~ 75 degrees C
MGB-TLB10	1000	WDM(LC)	Single Mode	10km	1550nm / 1310nm	-40 ~ 75 degrees C
MGB-TLA20	1000	WDM(LC)	Single Mode	20km	1310nm / 1550nm	-40 ~ 75 degrees C
MGB-TLB20	1000	WDM(LC)	Single Mode	20km	1550nm / 1310nm	-40 ~ 75 degrees C
MGB-TLA40	1000	WDM(LC)	Single Mode	40km	1310nm / 1550nm	-40 ~ 75 degrees C
MGB-TLB40	1000	WDM(LC)	Single Mode	40km	1550nm / 1310nm	-40 ~ 75 degrees C
MGB-TLA60	1000	WDM(LC)	Single Mode	60km	1310nm / 1550nm	-40 ~ 75 degrees C
MGB-TLB60	1000	WDM(LC)	Single Mode	60km	1550nm / 1310nm	-40 ~ 75 degrees C

It is recommended to use PLANET SFPs on the **Industrial Managed Switch**. If you insert an SFP transceiver that is not supported, the **Industrial Managed Switch** might not recognize it.

Please choose the SFP transceiver which can be operated in the temperature range of -40~75 degrees C.

1000BASE-SX/LX:

Before connecting the other switches, workstation or media converter,

1. Make sure both sides of the SFP transceiver are with the same media type, for example: 1000BASE-SX to 1000BASE-SX, 1000BASE-LX to 1000BASE-LX.
2. Check whether the fiber-optic cable type matches the SFP transceiver model.
   - To connect to 1000BASE-SX SFP transceiver, use the multi-mode fiber cable -- with one side being the male duplex LC connector type.
   - To connect to 1000BASE-LX SFP transceiver, use the single-mode fiber cable -- with one side being the male duplex LC connector type.

Connect the fiber cable

1. Attach the duplex LC connector on the network cable to the SFP transceiver.
2. Connect the other end of the cable to a device – switches with SFP installed, fiber NIC on a workstation or a media converter.
3. Check the LNK/ACT LED of the SFP slot on the front of the **Industrial Managed Switch**. Ensure that the SFP transceiver is operating correctly.

100BASE-FX:

Before connecting the other switches, workstation or media converter,

1. Make sure both sides of the SFP transceiver are with the same media type or WDM pair, for example: 100BASE-FX to 100BASE-FX, 100BASE-BX20-U to 100BASE-BX20-D.
2. Check whether the fiber-optic cable type matches the SFP transceiver model.
   - To connect to MFB-FX SFP transceiver, use the multi-mode fiber cable -- with one side being the male duplex LC connector type.
   - To connect to MFB-F20/F40/F60/FA20/FB20 SFP transceiver, use the single-mode fiber cable -- with one side being the male duplex LC connector type.

Connect the fiber cable

1. Attach the duplex LC connector on the network cable to the SFP transceiver.
2. Connect the other end of the cable to a device – switches with SFP installed, fiber NIC on a workstation or a media converter.
3. Check the LNK/ACT LED of the SFP slot of the switch / converter. Ensure that the SFP transceiver is operating correctly.
4. Check the Link mode of the SFP port if the link fails. It can function with some fiber-NICs or media converters, and set the Link mode to "**100 Force**" when needed.

2.3.2 Removing the SFP Transceiver

1. Make sure there is no network activity by consulting or checking with the network administrator. Or through the management interface of the switch/converter (if available) to disable the port in advance.
2. Remove the fiber optic cable gently.
3. Turn the lever of the MGB / MFB module to a horizontal position.
4. Pull out the module gently through the lever.

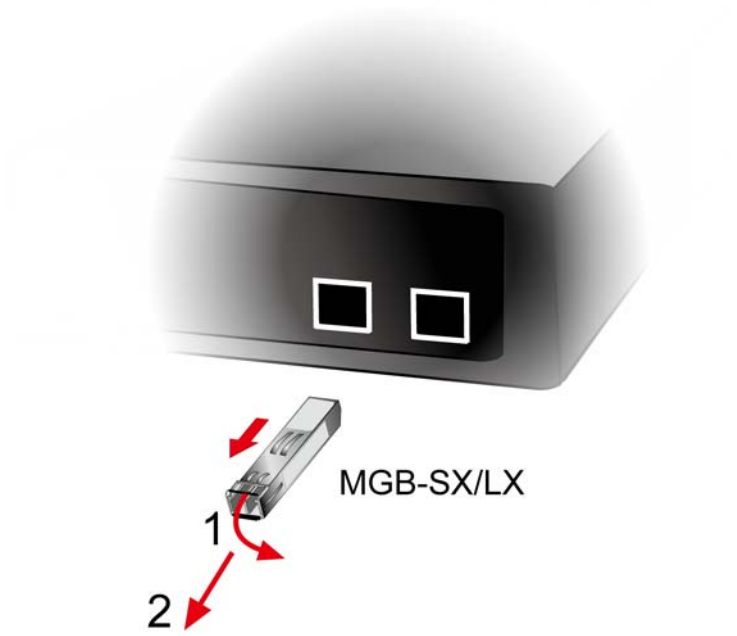


Figure 2-9: Pulling out the SFP Transceiver Module

Note

Never pull out the module without pulling the lever or the push bolts on the module. Directly pulling out the module with force could damage the module and SFP module slot of the device.

3. SWITCH MANAGEMENT

This chapter explains the methods that you can use to configure management access to the **Industrial Managed Switch**. It describes the types of management applications and the communication and management protocols that deliver data between your management device (workstation or personal computer) and the system. It also contains information about port connection options.

This chapter covers the following topics:

- Requirements
- Management Access Overview
- Remote Telnet Access
- Web Management Access
- SNMP Access
- Standards, Protocols, and Related Reading

3.1 Requirements

- Workstation running Windows XP/2003, Vista, Windows 7, MAC OS X, Linux, Fedora, Ubuntu or other platform is compatible with **TCP/IP** protocols.
- **Workstation** is installed with **Ethernet NIC** (Network Interface Card)
- **Serial Port** (Terminal)
  - The above PC comes with COM Port (DB9 / RS232) or USB-to-RS232 converter
- Ethernet Port
  - Network cables -- Use standard network (UTP) cables with RJ45 connectors.
- The above workstation is installed with **Web browser** and **JAVA runtime environment** Plug-in

It is recommended to use Internet Explore 8.0 or above to access **Industrial Managed Switch**.

3.2 Management Access Overview

The **Industrial Managed Switch** gives you the flexibility to access and manage it using any or all of the following methods:

- Remote Telnet Interface
- **Web browser** Interface
- An external **SNMP-based network management application**

The remote Telnet and Web browser interfaces are embedded in the **Industrial Managed Switch** software and are available for immediate use. Each of these management methods has their own advantages. Table 3-1 compares the three management methods.

Method	Advantages	Disadvantages
Console	• No IP address or subnet needed • Text-based • Telnet functionality and HyperTerminal built into Windows 95/98/NT/2000/ME/XP operating systems • Secure	• Must be near the switch or use dial-up connection • Not convenient for remote users • Modem connection may prove to be unreliable or slow
Remote Telnet	• Text-based • Telnet functionality built into Windows XP/2003, Vista, Windows 7 operating systems • Can be accessed from any location	• Security can be compromised (hackers need only know the IP address)
Web Browser	• Ideal for configuring the switch remotely • Compatible with all popular browsers • Can be accessed from any location • Most visually appealing	• Security can be compromised (hackers need only know the IP address and subnet mask) • May encounter lag times on poor connections
SNMP Agent	• Communicates with switch functions at the MIB level • Based on open standards	• Requires SNMP manager software • Least visually appealing of all three methods • Some settings require calculations • Security can be compromised (hackers need only know the community name)

Table 3-1: Comparison of Management Methods

3.3 Administration Console

The administration console is an internal, character-oriented, and command line user interface for performing system administration such as displaying statistics or changing option settings. Using this method, you can view the administration console from a terminal, personal computer, Apple Macintosh, or workstation connected to the Managed Switch's console (serial) port.

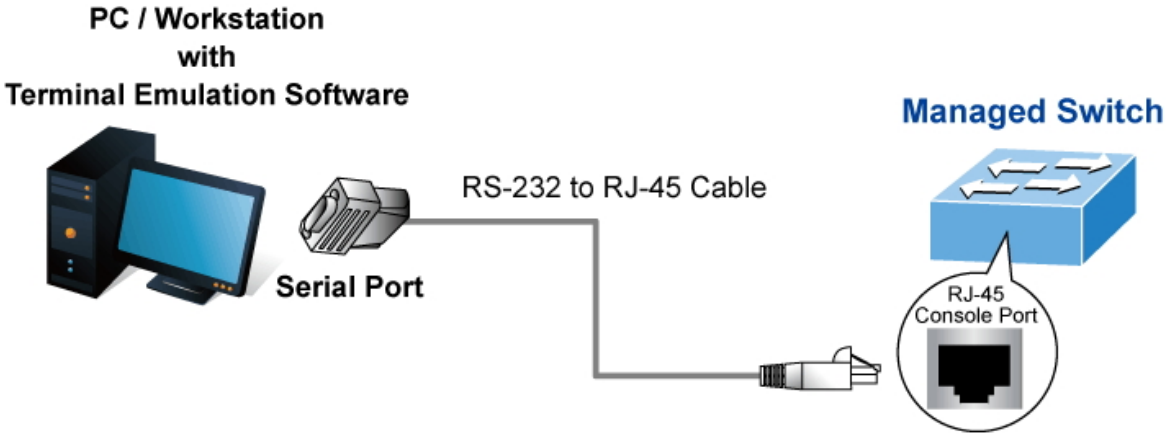


Figure 3-1-1: Console Management

Direct Access

Direct access to the administration console is achieved by directly connecting a terminal or a PC equipped with a terminal-emulation program (such as **HyperTerminal**) to the Managed Switch console (serial) port. When using this management method, a **straight DB9 RS232 cable** is required to connect the switch to the PC. After making this connection, configure the terminal-emulation program to use the following parameters:

The default parameters are:

- **115200 bps**
- **8 data bits**
- **No parity**
- **1 stop bit**

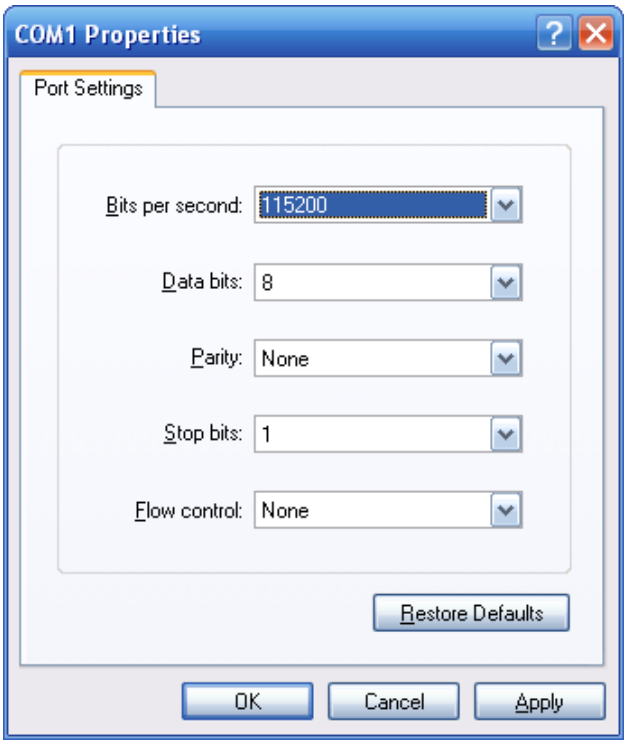


Figure 3-1-2: Terminal Parameter Settings

You can change these settings, if desired, after you log on. This management method is often preferred because you can remain connected and monitor the system during system reboots. Also, certain error messages are sent to the serial port, regardless of the interface through which the associated action was initiated. A Macintosh or PC attachment can use any terminal-emulation program for connecting to the terminal serial port. A workstation attachment under UNIX can use an emulator such as TIP.

3.4 Web Management

The Managed Switch offers management features that allow users to manage the Managed Switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer. After you set up your IP address for the switch, you can access the Managed Switch's Web interface applications directly in your Web browser by entering the IP address of the Managed Switch.

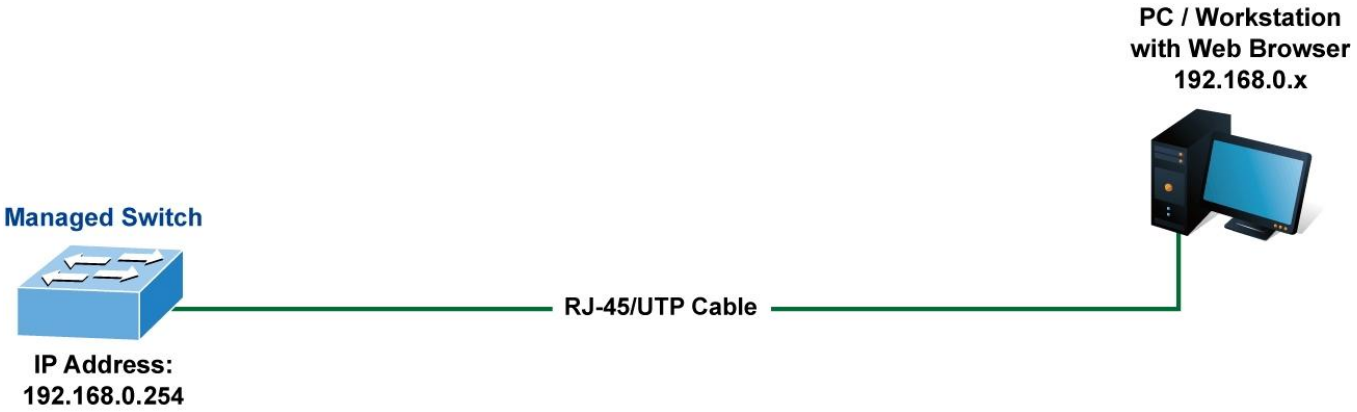


Figure 3-1-3: Web Management

You can then use your Web browser to list and manage the Managed Switch configuration parameters from one central location, just as if you were directly connected to the Managed Switch's console port. Web Management requires either **Microsoft Internet Explorer 7.0** or later, **Safari** or **Mozilla Firefox 1.5** or later.

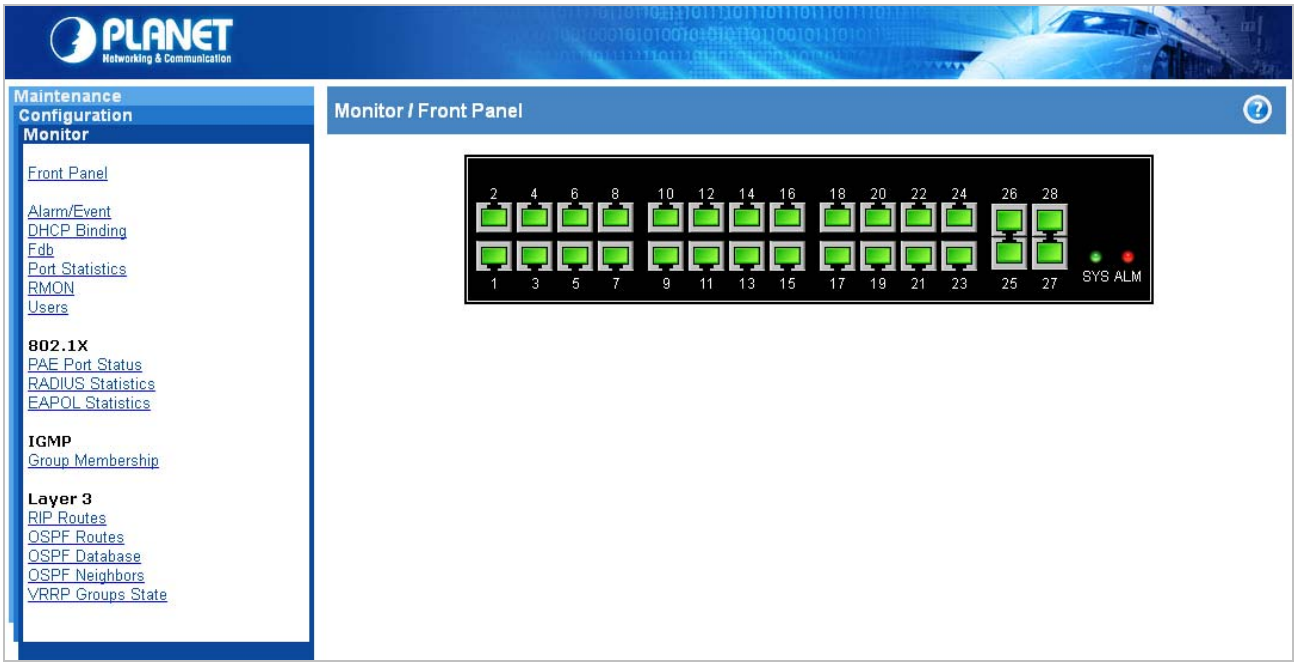


Figure 3-1-4: Web Main Screen of Managed Switch

3.5 SNMP-based Network Management

You can use an external SNMP-based application to configure and manage the Managed Switch, such as SNMP Network Manager, HP Openview Network Node Management (NNM) or What's Up Gold. This management method requires the SNMP agent on the switch and the SNMP Network Management Station to use the **same community string**. This management method, in fact, uses two community strings: the **get community** string and the **set community** string. If the SNMP Network Management Station only knows the set community string, it can read and write to the MIBs. However, if it only knows the get community string, it can only read MIBs. The default getting and setting community strings for the Managed Switch is public.

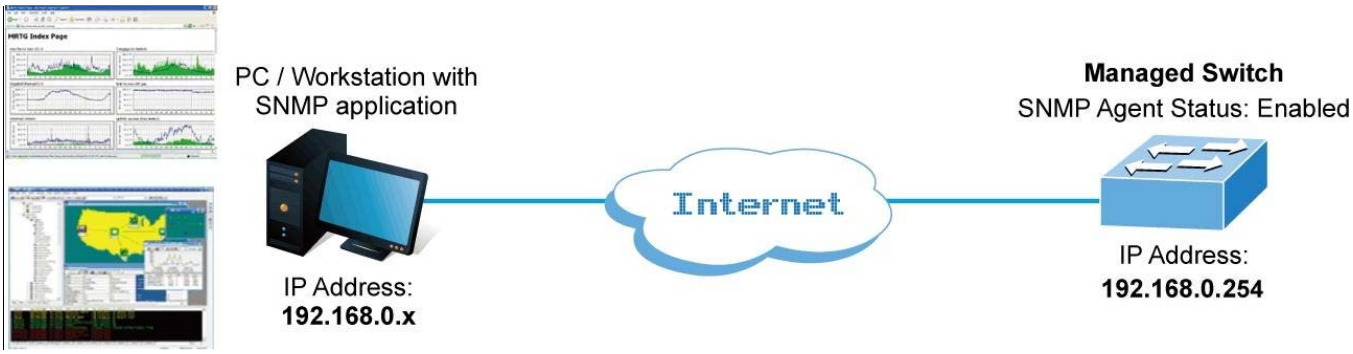


Figure 3-1-5: SNMP Management

4. WEB CONFIGURATION

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

About Web-based Management

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

The Web-based Management supports Internet Explorer 7.0. It is based on Java Applets with an aim to reducing network bandwidth consumption, enhancing access speed and presenting an easy viewing screen.

By default, IE7.0 or later version does not allow Java Applets to open sockets. The user has to explicitly modify the browser setting to enable Java Applets to use network ports.

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

For example, the default IP address of the **Industrial Managed Switch** is ***192.168.0.254***, then the manager PC should be set at **192.168.0.x** (where x is a number between 1 and 253, except 254), and the default subnet mask is 255.255.255.0.

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

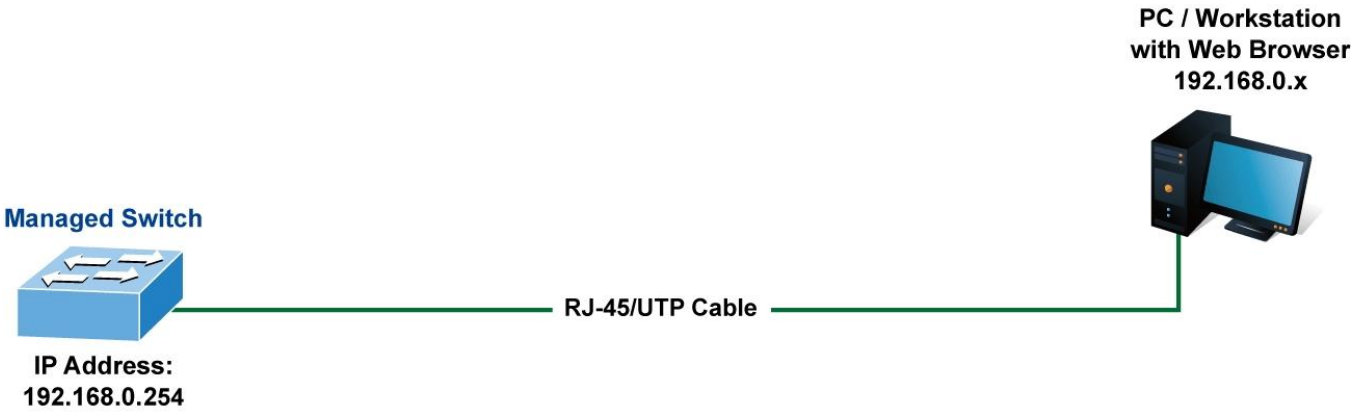


Figure 4-1-1: Web Management

■ **Logging on the Industrial Managed Switch**

1. Use Internet Explorer 7.0 or above Web browser. Enter the factory-default IP address to access the Web interface. The factory-default IP address is as follows:

http://192.168.0.254

2. When the following login screen appears, please enter the default username **"admin"** with password "**admin**" (or the username/password you have changed via console) to login the main screen of **Industrial Managed Switch**. The login screen in Figure 4-1-2 appears.

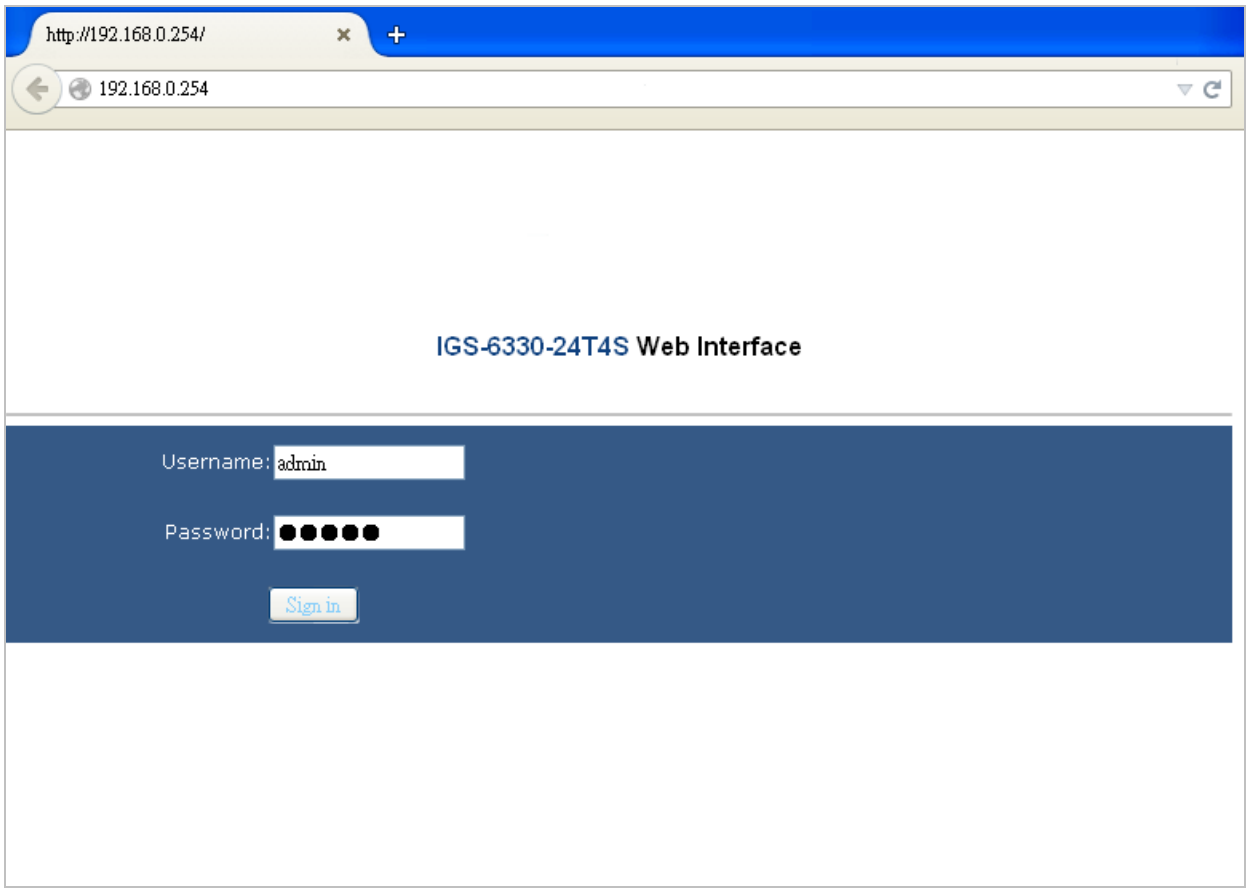


Figure 4-1-2: Login Screen

Default User Name: **admin**

Default Password: **admin**

After entering the username and password, the main screen appears as Figure 4-1-3.

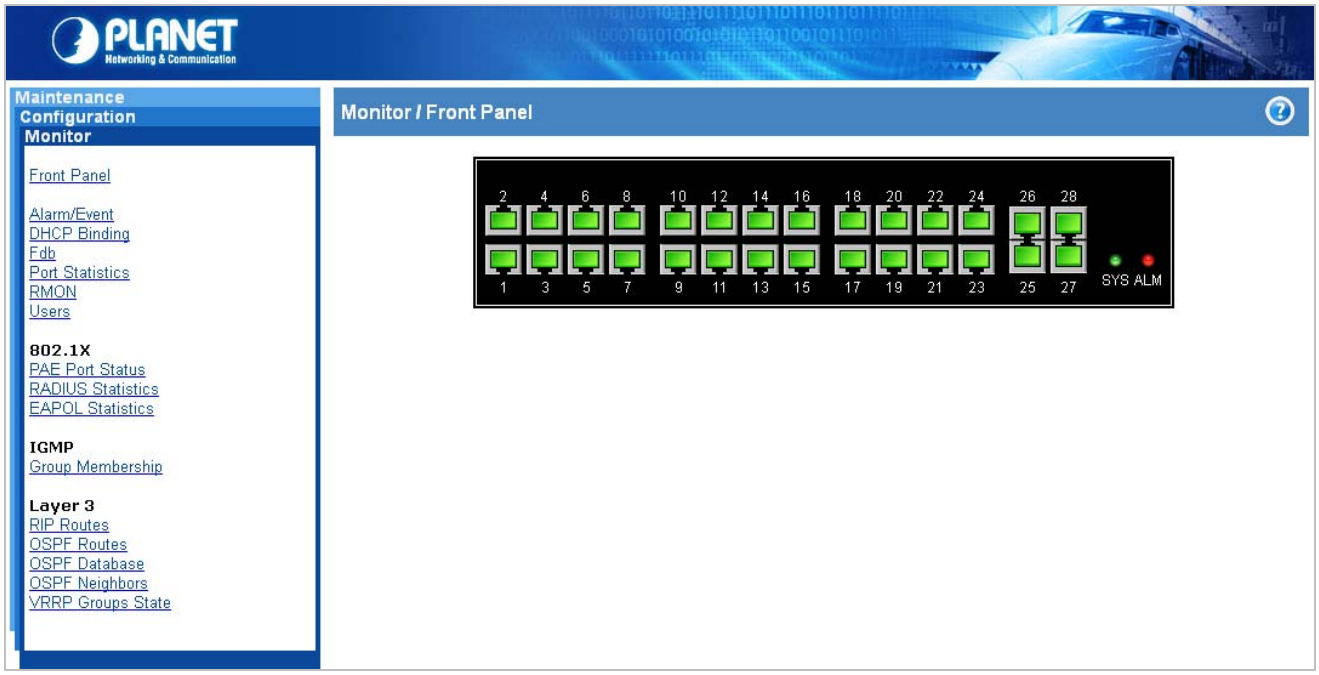


Figure 4-1-3: Default Main Page

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

Note

1. It is recommended to use Internet Explore 7.0 or above to access **Industrial Managed Switch**.
2. The changed IP address takes effect immediately after clicking on the **Save** button. From now on, you need to use the new IP address to access the Internet.

Note

3. For security reason, please change and memorize the new password after this first setup.
4. Only accept command in lowercase letter.

4.1 Main Web Page

The **Industrial Managed Switch** provides a Web-based browser interface for configuring and managing it. This interface allows you to access the **Industrial Managed Switch** using the Web browser of your choice. This chapter describes how to use the **Industrial Managed Switch**'s Web browser interface to configure and manage it.

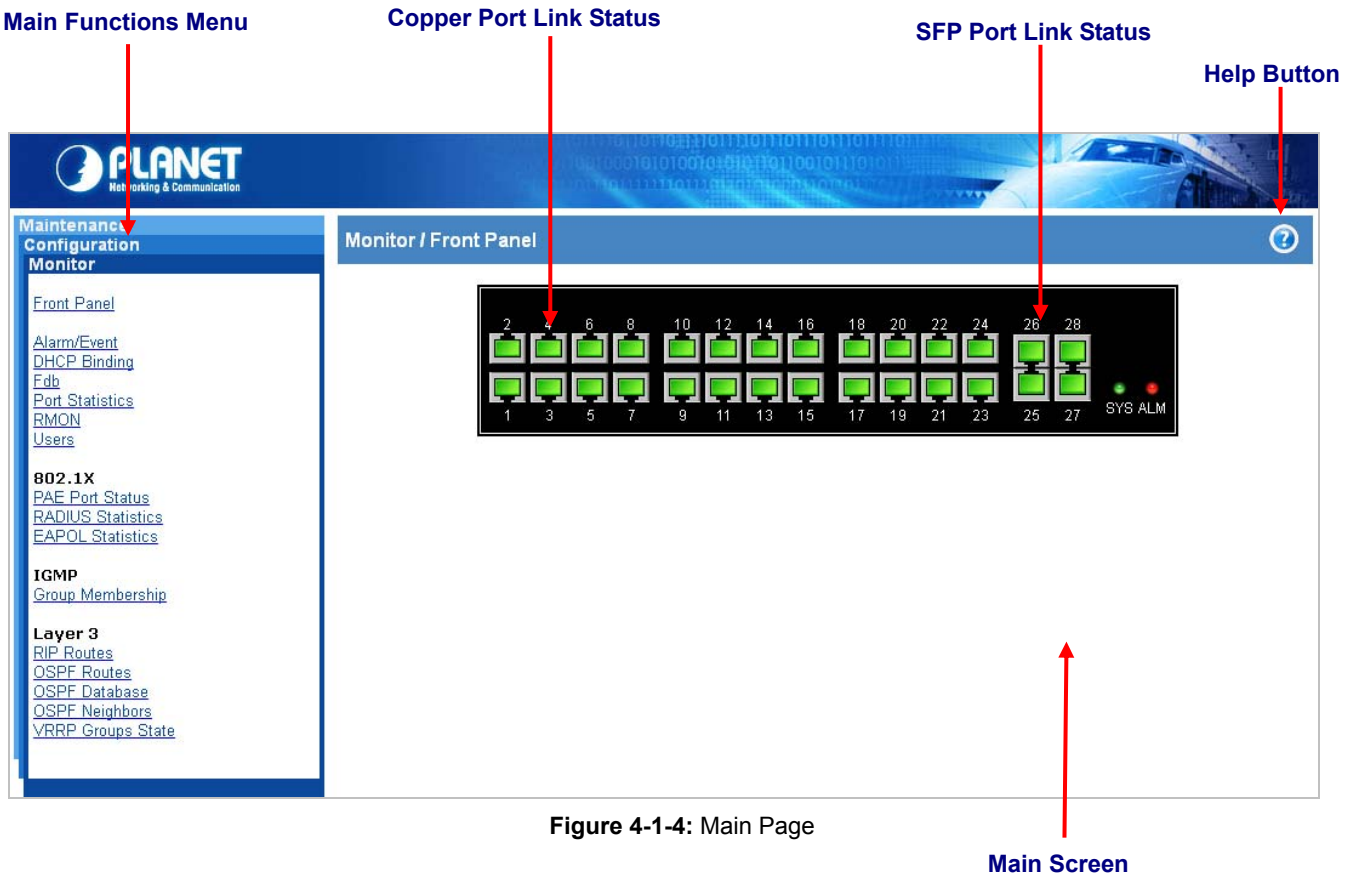


Figure 4-1-4: Main Page

Panel Display

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

State	Down	Link
RJ45 Ports		
SFP Ports		

Main Menu

Using the onboard web agent, you can define system parameters, manage and control the **Industrial Managed Switch**, and all its ports, or monitor network conditions. Via the Web-Management, the administrator can set up the **Industrial Managed Switch** by selecting the functions those listed in the Main Function. The screen in Figure 4-1-5 appears.

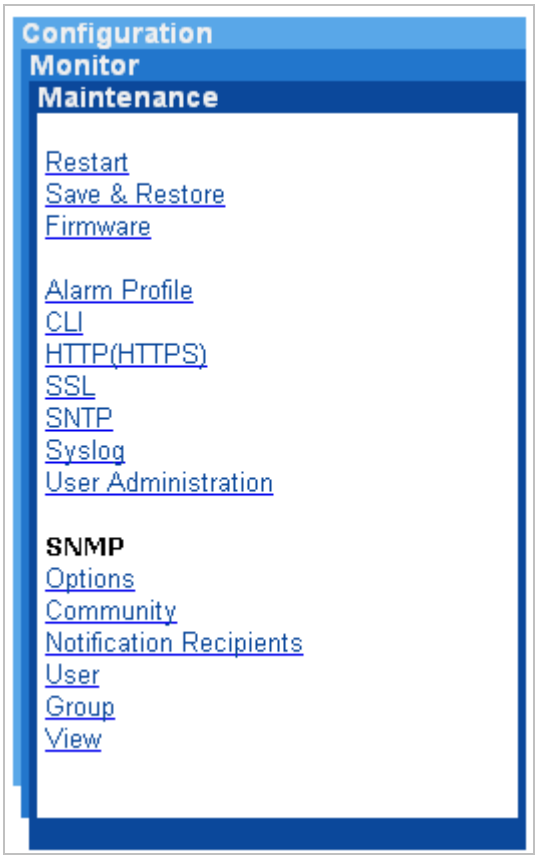


Figure 4-1-5: Industrial Managed Switch Main Functions Menu

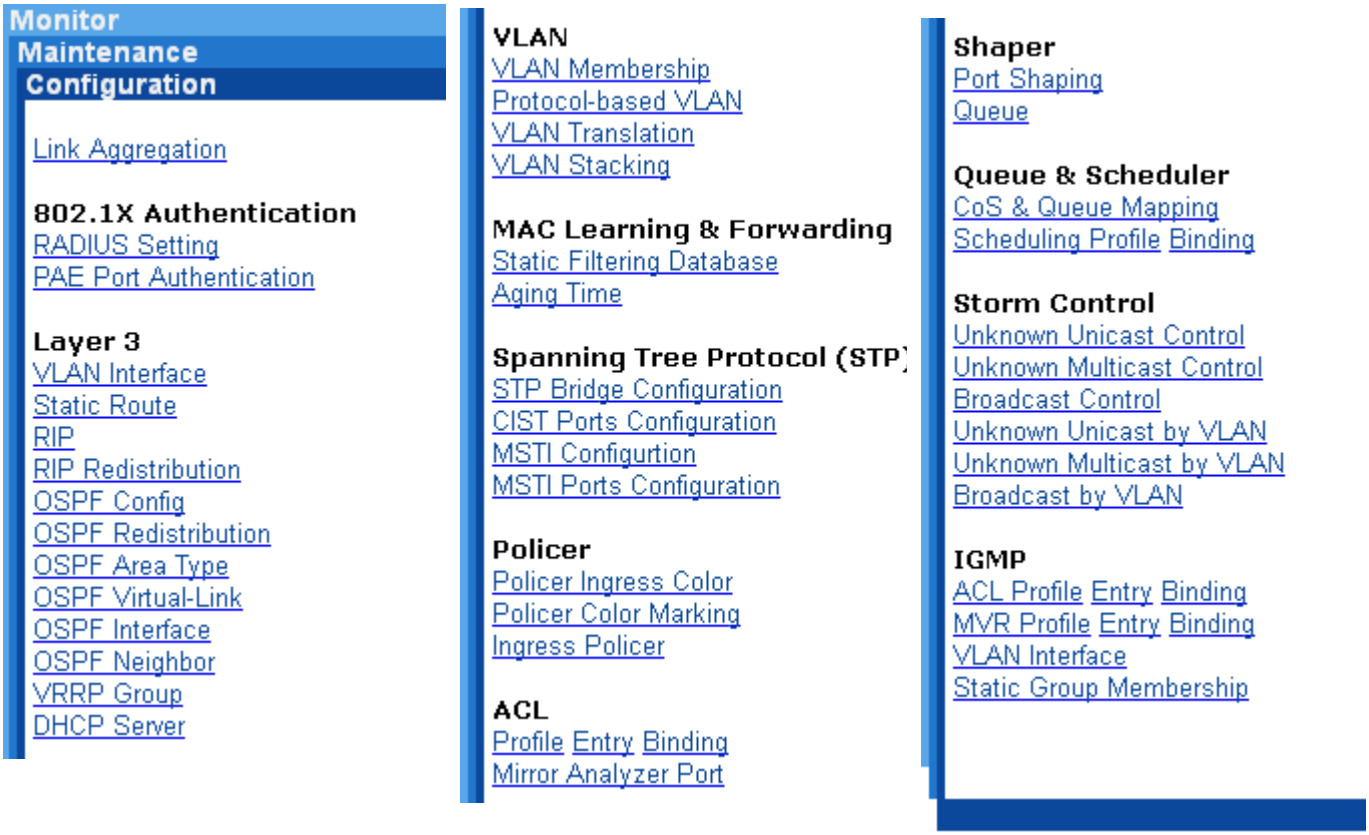
Buttons

 : Help Button: For more information about any screen, click on the Help button on the screen. Help information is displayed in the same window.

 : Click to save changes

4.2 Configuration Menu Tree

Use the configuration menu items to configure basic administrative details of the **Industrial Managed Switch**.



4.3 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.

Aggregated Links can be assigned manually (**Port Trunk**).

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.

The device supports the following Aggregation links :

- **Static LAGs** (**Port Trunk**) – Force aggregared selected ports to be a trunk group.

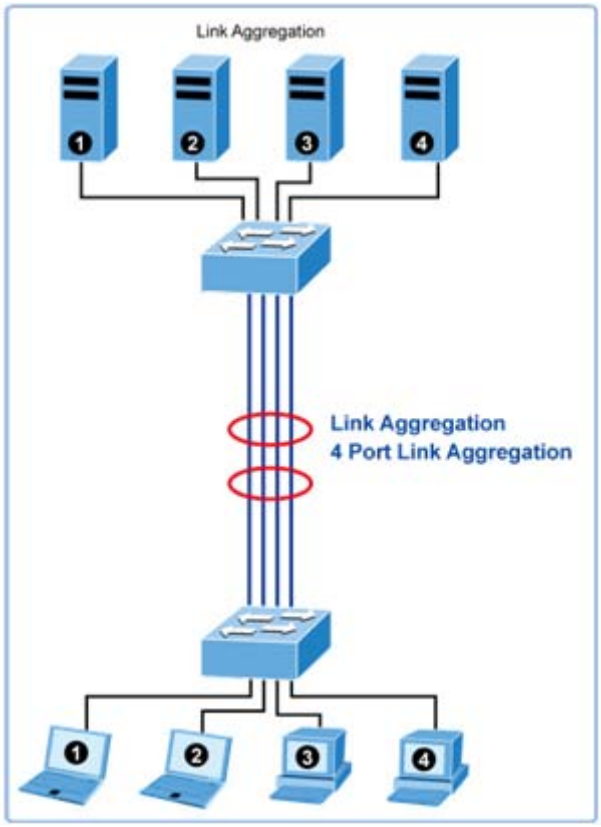


Figure 4-3-1: Link Aggregation

Port link aggregations can be used to increase the bandwidth of a network connection or to ensure fault recovery. Link aggregation lets you group up to 4 consecutive ports into a single dedicated connection between any two the Switch or other Layer 2 switches. However, before making any physical connections between devices, use the Link aggregation Configuration menu to specify the link aggregation on the devices at both ends. When using a port link aggregation, note that:

- The ports used in a link aggregation must all be of the same media type (RJ45, fiber).
- 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.
- Enable the link aggregation prior to connecting any cable between the switches to avoid creating a data loop.
- Disconnect all link aggregation port cables or disable the link aggregation ports before removing a port link aggregation to avoid creating a data loop.

It allows a maximum of 4 ports to be aggregated at the same time. The Industrial Managed Switch supports Gigabit Ethernet ports (up to 2 groups). If the group is defined as a local static link aggregationing group, then the number of ports must be the same as the group member ports. The screen in Figure 4-3-2 appears.

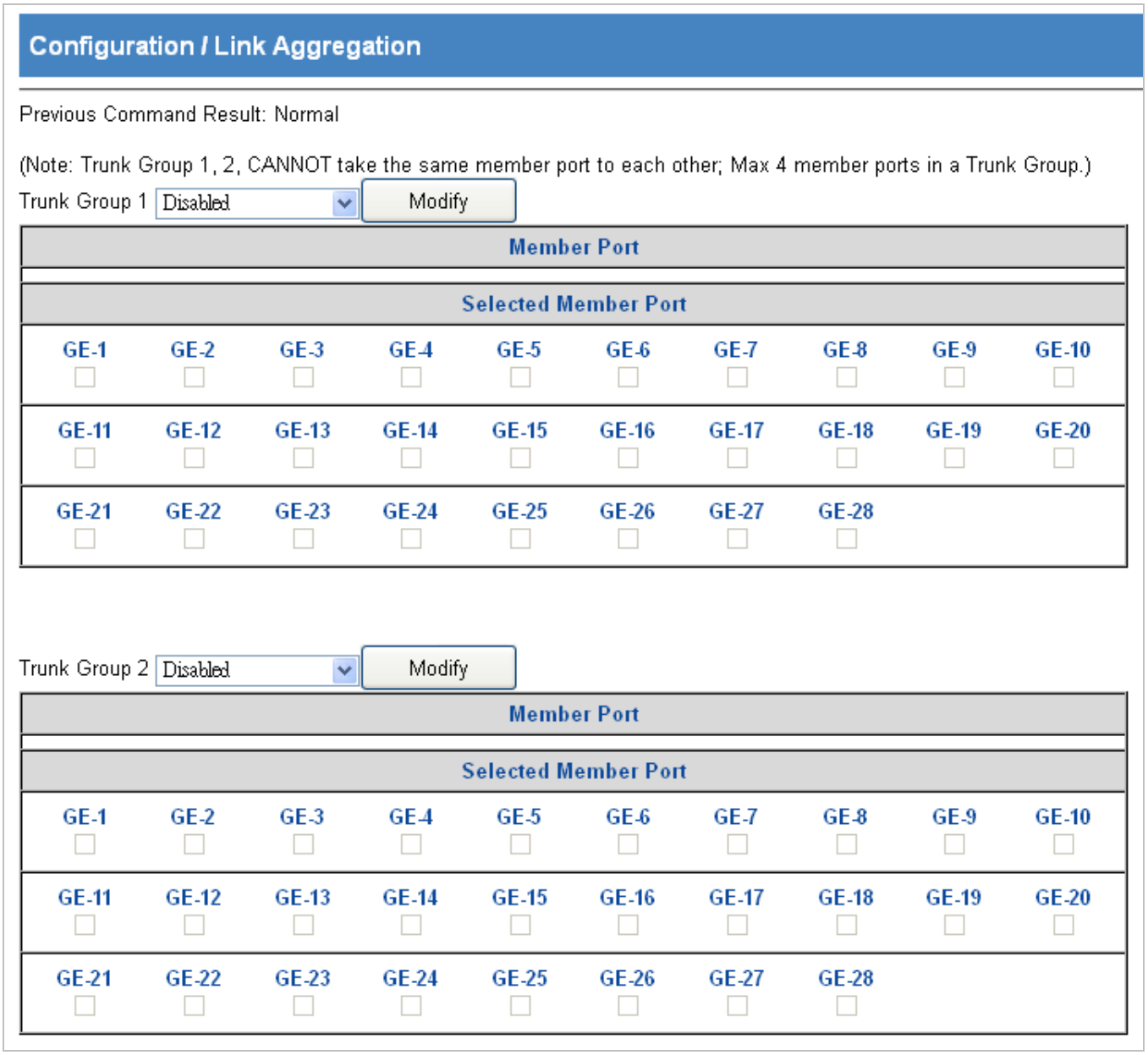


Figure 4-3-2: Configuration / Link Aggregation Page Screenshot

Object	Description
• **Operation**	**Modify:** Select port with check box from GE-1 ~ GE-28. Click the **Modify** button.

The page includes the following fields:

Object	Description
• **Trunk Group**	Trunk Group number. Note: Trunk Group 1 & 2 CANNOT take the member port that is already assigned to another Trunk Group; Max 4 member ports in a Trunk Group.

	Otherwise, the modification would fail.
• **Member Port**	Display current member port of Trunk Group.
• **Mode**	To enable/disable Link Aggregation for Trunk Group.
• **GE-1~GE-28**	To select member ports for Trunk Group. If Link Aggregation mode is disabled, then the member port would be cleared, meaning no member port is assigned to Trunk Group.

4.4 802.1X Authentication

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 PDU**s (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 completed, 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.

4.4.1 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.

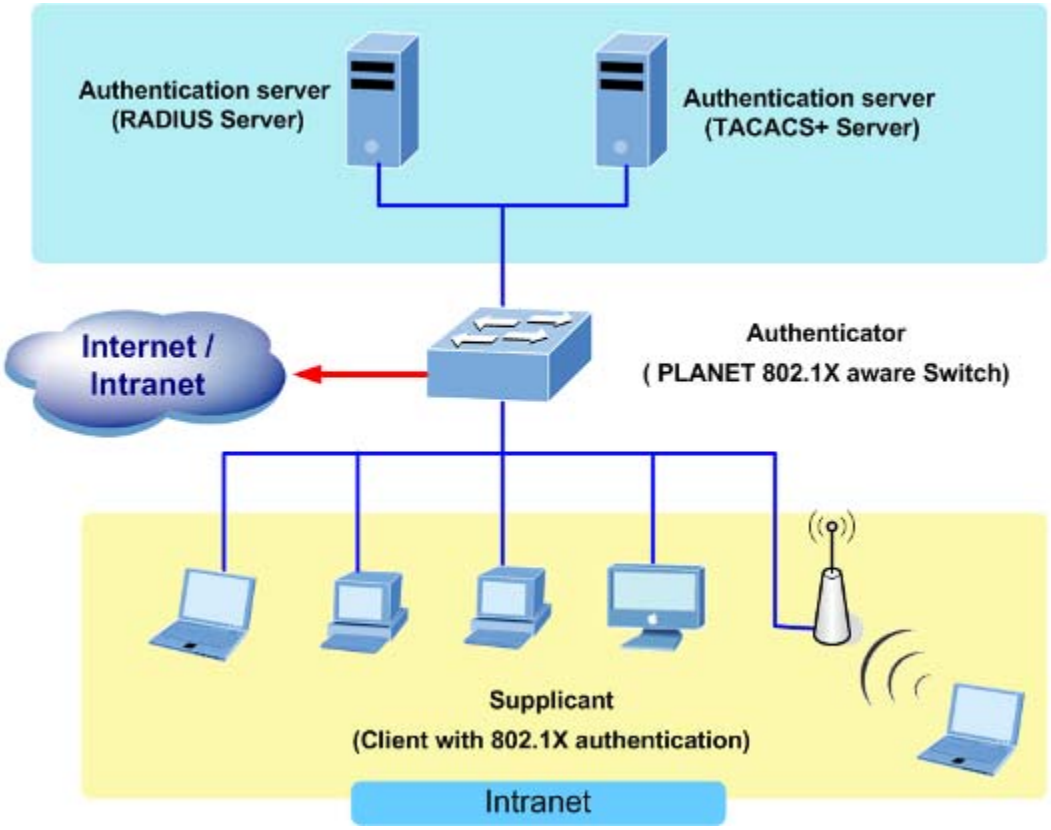


Figure 4-4-1

- ***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 4-4-2 shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.

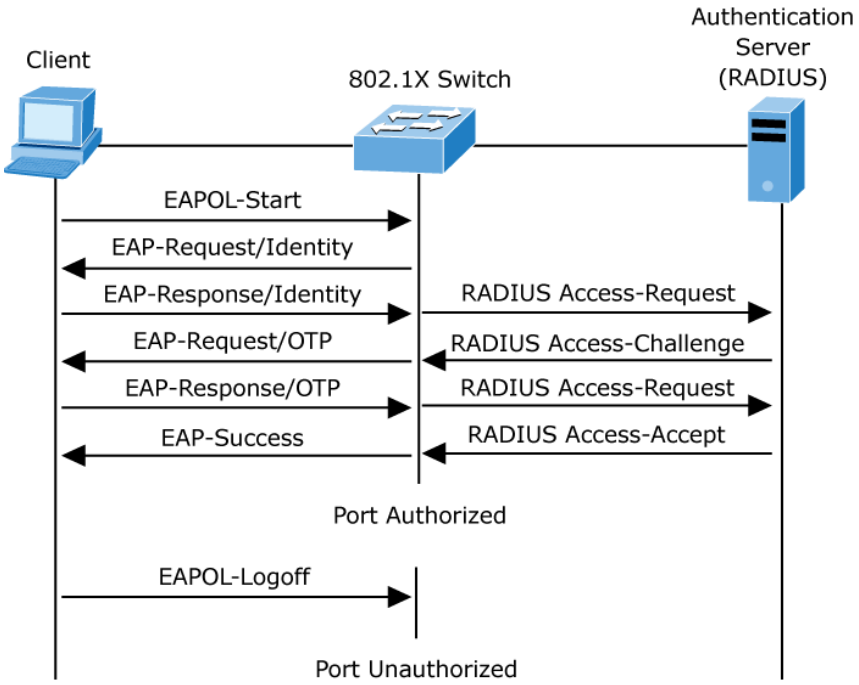


Figure 4-4-2: EAP Message Exchange

■ **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.

4.4.2 RADIUS Setting

This page allows you to configure the RADIUS Servers. The RADIUS Configuration screen in Figure 4-4-3 appears.

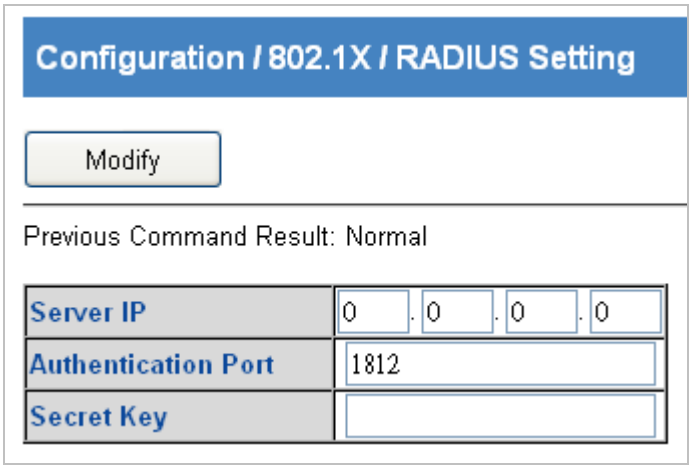


Figure 4-4-3: Confiugration / 802.1X / RADIUS Setting Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Modify Server IP, Authentication Port and Secret Key fields. Click the **Modify** button to apply change.

The page includes the following fields:

Object	Description
• **Server IP**	The IP address of RADIUS server. Allow IPv4 address. 0.0.0.0 means disable RADIUS. Default is 0.0.0.0.
• **Authentication Port**	The UDP port of RADIUS server for authentication. Range 1~65535. Default is 1812.
• **Secret Key**	The key to be used between RADIUS server and Authenticator. Range 0~16 chars. Default is empty string.

4.4.3 PAE Port Authentication

This page allows you to configure the IEEE 802.1X authentication 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. The Configuration / 802.1X / PEA Port Authentication Configuration screen in Figure 4-4-4 appears.

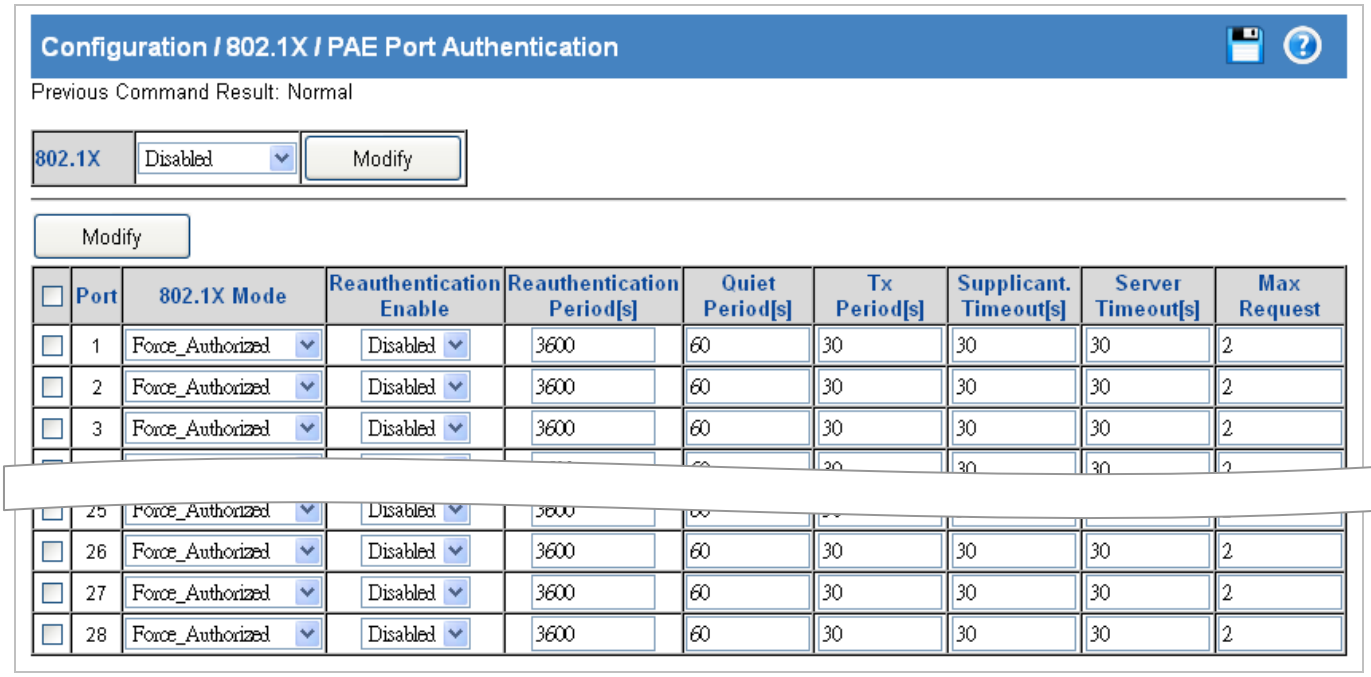


Figure 4-4-4: Confiugration / 802.1X / PAE Port Configuration Page Screenshot

Object	Description
• **Operation**	**Modify System Auth. Control:** Select System Auth. Control. Click "Modify" button to apply change. **Modify PAE Port Authentication:** Update below fields. Check up the port(s) to be changed. Click the **Modify** button to modify PAE Port Authentication options.

The page includes the following fields:

Object	Description
• **802.1X**	Enable/Disable system 802.1X authentication function. Default value is Disabled.
• **Port**	PAE port: 1 ~ MAX Number of Port.
• **802.1X Mode**	The authentication type of PAE port. Allow Force_Unauthorized/Force_Authorized/Auto. **force-authorized**—disables 802.1X and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. This is the default setting. **force-unauthorized**—causes the port to remain in the unauthorized state,

	ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface. **auto**—enables 802.1X authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the switch by using the client's MAC address. Default is Force_Authorized.
• **Reauthentication Enable**	Enable/Disable re-authenticate of PAE port. Default is Disable.
• **Reauthentication Period**	The period of re-authenticant of PAE port. Range 1~3600 sec. Default is 3600 sec.
• **Quiet Period[s]**	The quiet period of PAE port. Range 1~255 sec. Default is 60 sec.
• **Tx Period[s]**	The timeout of authenticator waiting for EAP-Response/ Identity from supplication of PAE port. Range 1~255 sec. Default is 30 sec.
• **Supplicant. Timeout[s]**	The timeout of authenticator wait for EAP-Response (exclude EAP-Request/Identify) after sending EAP-Request. Range 1~255 sec. Default is 30 sec.
• **Server Timeout[s]**	The timeout time of Authenticator wait Access-Challenge/ Access-Accept/ Access-Reject after sending Access-Request. Range 1~255 sec. Default is 30 sec.
• **Max Request**	The max times of backend Authenticator send EAP-Request to supplicant before restarting the authentication process. Range 1~10. Default is 2.

4.5 Layer 3

4.5.1 VLAN Interface

The VLAN Interface includes the IP Configuration and IP Interface. The configured column is used to view or change the IP configuration. The maximum number of interfaces supported is 5. The screen in Figure 4-5-1 appears.

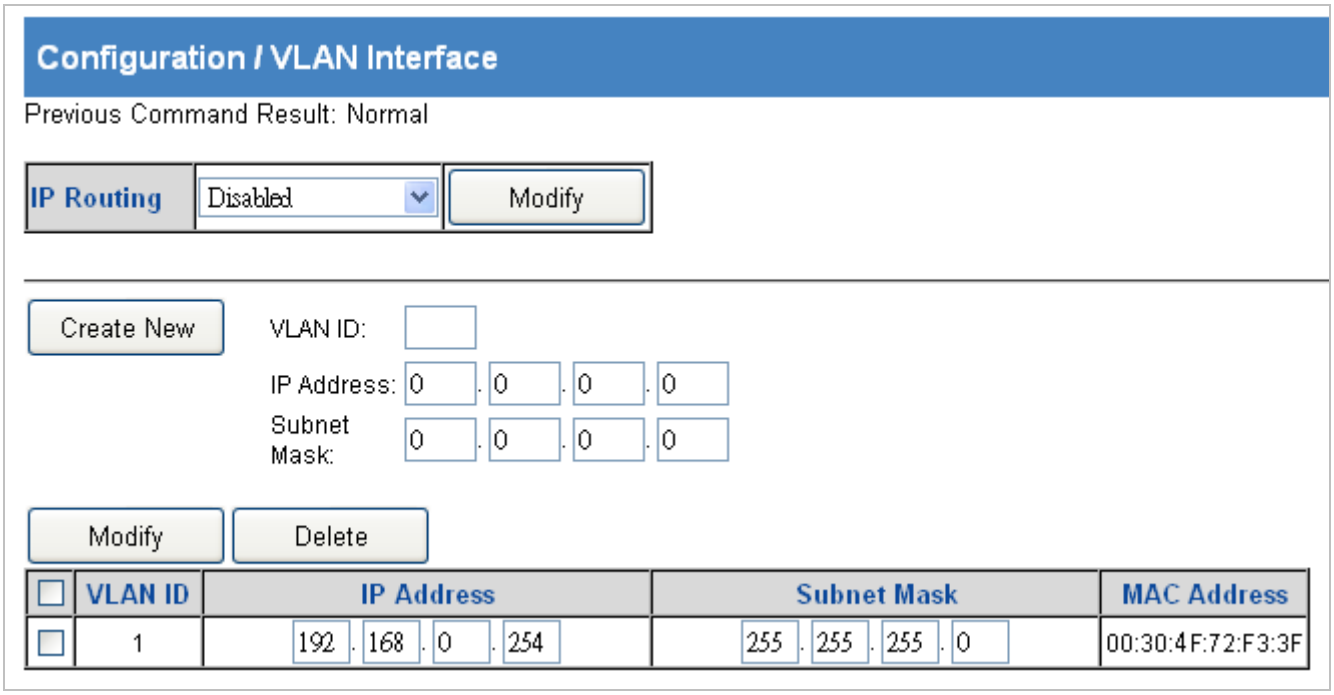


Figure 4-5-1: Configuration / VLAN Interface Configuration Page Screenshot

Object	Description
• **Operation**	**Modify the IP Routing:** Select IP Routing field. Click the **Modify** button to apply change. **Create New:** Fill out VID, IP Address and Netmask. Click the **Create New** button to create Interface VLAN. **Delete:** Multi-select a row data in Interface VLAN table. Click the **Delete** button to delete Interface VLAN.

The page includes the following fields:

Object	Description

• **IP Routing**	Layer 3 IP routing/forward. Allow Disabled/Enabled. Default value is Disabled.
• **VID**	The identity for the RIP Interface. Range 1~4094. 1st RIP interface VLAN always exist for VLAN 1. (Only support set can't be deleted)
• **IP Address**	IP address for the vlan interface. Range 0~255. Default value is 0.
• **Netmask**	Network subnet mask for the VLAN interface. Range 0~255. Default value is 0.
• **MAC Address**	MAC address for the VLAN interface. Read only.

4.5.2 Static Route

The Static Route includes the destination, subnet mask and gateway. The configured column is used to view or change the static routing table. The screen in Figure 4-5-2 appears.

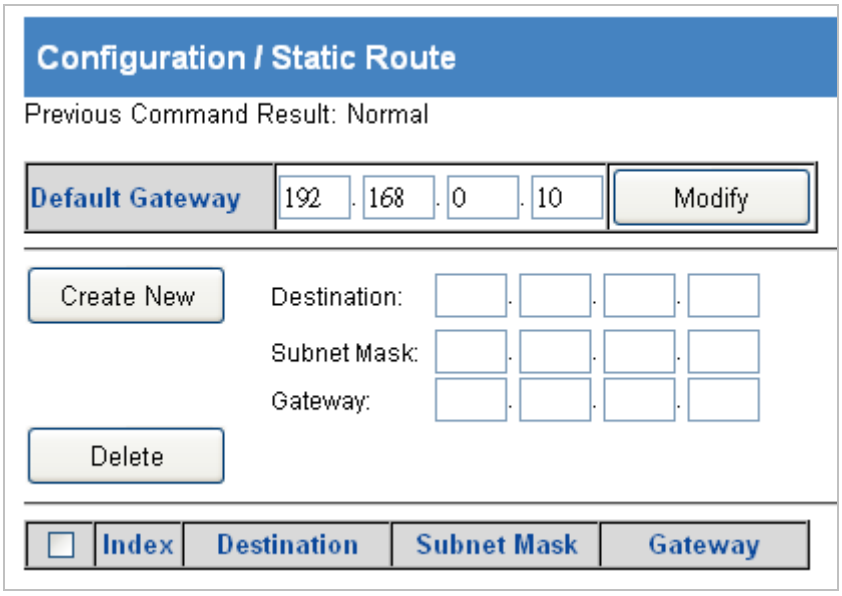


Figure 4-5-2: Confiugration / VLAN Interface Configuration Page Screenshot

Object	Description

• **Operation**	**Modify default gateway:** Click the **Modify** button to apply new gateway. **Create new static route:** Fill Destination, Netmask and Gateway. Click the **Create New** button to create one static route. **Delete static route:** Select static route entry(s). Click the **Delete** button to delete selection.

The page includes the following fields:

Object	Description
• **Default Gateway**	Input default gateway IP address for management and Layer3 VLAN interface routing.
• **Destination**	Destination network address of static route.
• **Netmask**	Network subnet mask for the route.
• **Gateway**	Next hop IP address for the destination network.
• **Index**	The index of the static route.

4.5.3 RIP

RIP is first introduced in ARPANET, this is a protocol dedicated to small, simple networks. RIP is a distance vector routing protocol based on the Bellman-Ford algorithm. Network devices running vector routing protocol send two kind of information to the neighboring devices regularly:

• Number of hops to reach the destination network, or metrics to use or number of networks to pass.

• What is the next hop, or the director (vector) to use to reach the destination network.

The distance vector Layer 3 switch send all their route selecting tables to the neighbor layer3 switches at regular interval. A layer3 switch will build their own route selecting information table based on the information received from the neighbor layer3 switches. Then, it will send this information to its own neighbor layer3 switches. As a result, the route selection table is built on second hand information, route beyond 15 hops will be deemed as unreachable.

RIP protocol is an optional routing protocol based on UDP. Hosts using RIP send and receive packets on UDP port 520. All layer3 switches running RIP send their route table to all neighbor layer3 switches every 30 seconds for update. If no information from the partner is received in 180 seconds, then the device is deemed to have failed and the network connected to that device is considered to be unreachable. However, the route of that layer3 switch will be kept in the route table for another 120 seconds

before deletion.

As layer3 switches running RIP built route table with second hand information, infinite count may occur. For a network running RIP routing protocol, when an RIP route becomes unreachable, the neighboring RIP layer3 switch will not send route update packets at once, instead, it waits until the update interval timeout (every 30 seconds) and sends the update packets containing that route. If before it receives the updated packet, its neighbors send packets containing the information about the failed neighbor, "infinite count" will be resulted. In other words, the route of unreachable layer3 switch will be selected with the metrics increasing progressively. This greatly affects the route selection and route aggregation time.

To prevent "infinite count", RIP provides mechanism such as "split horizon" and "triggered update" to solve route loop. "Split horizon" is done by avoiding sending to a gateway routes leaned from that gateway. There are two split horizon methods: "simple split horizon" and "poison reverse split horizon". Simple split horizon deletes from the route to be sent to the neighbor gateways the routes learnt from the neighbor gateways; poison reverse split horizon not only deletes the abovementioned routes, but set the costs of those routes to infinite. "Triggering update" mechanism defines whenever route metric changed by the gateway, the gateway advertise the update packets immediately, regardless of the 30 second update timer status.

There two versions of RIP, version 1 and version 2. RFC1058 introduces RIP-I protocol, RFC2453 introduces RIP-II, which is compatible with RFC1723 and RFC1388. RIP-I updates packets by packets broadcast, subnet mask and authentication is not supported. Some fields in the RIP-I packets are not used and are required to be all 0's; for this reason, such all 0's fields should be checked when using RIP-I, the RIP-I packets should be discarded if such fields are non-zero. RIP-II is a more improved version than RIP-I. RIP-II sends route update packets by multicast packets (multicast address is 224.0.0.9). Subnet mask field and RIP authentication filed (simple plaintext password and MD5 password authentication are supported), and support variable length subnet mask. RIP-II used some of the zero field of RIP-I and require no zero field verification. switch send RIP-II packets in multicast by default, both RIP-I and RIP-II packets will be accepted.

Each layer3 switch running RIP has a route database, which contains all route entries for reachable destination, and route table is built based on this database. When a RIP layer3 switch sent route update packets to its neighbor devices, the complete route table is included in the packets. Therefore, in a large network, routing data to be transferred and processed for each layer3 switch is quite large, causing degraded network performance.

Besides the above mentioned, RIP protocol allows route information discovered by the other routing protocols to be introduced to the route table.

The operation of RIP protocol is shown below:

1. Enable RIP. The switch sends request packets to the neighbor layer3 switches by broadcasting; on receiving the request, the neighbor devices reply with the packets containing their local routing information.
2. The Layer3 switch modifies its local route table on receiving the reply packets and sends triggered update packets to the neighbor devices to advertise route update information. On receiving the triggered update packet, the neighbor lay3 switches send triggered update packets to their neighbor lay3 switches. After a sequence of triggered update packet broadcast, all layer3 switches get and maintain the latest route information.

In addition, RIP layer3 switches will advertise its local route table to their neighbor devices every 30 seconds. On receiving the packets, neighbor devices maintain their local route table, select the best route and advertise the updated information to their own neighbor devices, so that the updated routes are globally valid. Moreover, RIP uses a timeout mechanism for outdated route, that is, if a switch does not receive regular update packets from a neighbor within a certain interval (invalid timer interval), it considers the route from that neighbor invalid, after holding the route fro a certain interval (holddown timer interval), it will delete that route. The screen in Figure 4-5-3 appears.

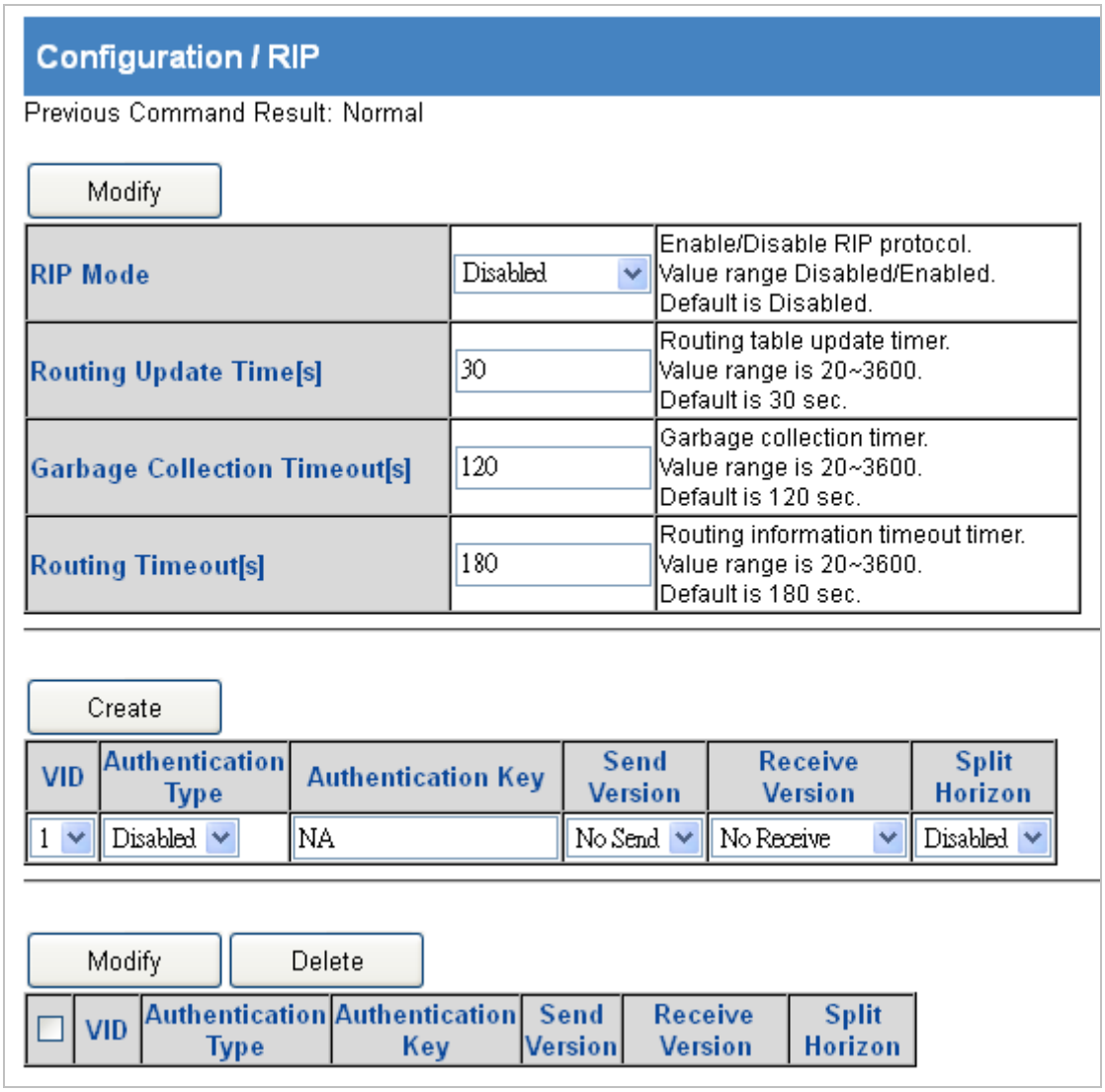


Figure 4-5-3: Configuration / RIP Configuration Page Screenshot

Object	Description
• **Operation**	**Modify RIP settings:** Select RIP Mode, Routing Update Time, Garbage Collection Timeout and Routing Timeout. Click the **Modify** button to apply changes. **Create RIP interface VLAN settings:** Create VID, RIP Mode, Auth Type, Auth Key, Send Version, Recv Version and

	Split Horizon. Click the **Modify** button to apply changes. **Modify RIP interface VLAN settings:** Modify RIP Mode, Auth Type, Auth Key, Send Version, Recv Version and Split Horizon. Click the **Modify** button to apply changes.

The Page includes the following fields:

Object	Description
• **RIP Mode**	RIP protocol mode. Allow Disabled/Enabled. Default value is Disabled.
• **Routing Update Time**	Routing table update timer. Range is 20~3600. Default value is 30 sec.
• **Garbage Collection Timeout**	Garbage collection timer. Range is 20~3600. Default value is 120 sec.
• **Routing Timeout**	Routing information timeout timer. Range is 20~3600. Default value is 180 sec.
• **VID**	The identity for the RIP interface VLAN. Range 1~4094. 1st RIP interface VLAN always exists for VLAN 1. (Only support set can't be deleted)
• **RIP Mode**	RIP Mode is used to enable RIP on an VLAN interface. Range Disabled/Enabled. Default value is Disabled.
• **Authentication Type**	Auth Type is the type of Authentication used on this interface. Range Disabled/Enabled. Default value is Disabled.
• **Authentication Key**	The Authentication Key. The max is 16 chars. The default value is empty string which is all nulls.
• **Send Version**	Version of RIP packet sent from this interface. Range NoSend/RIP 1/RIP 2/ Both The default value is RIP1.

• **Receive Version**	Version of RIP packet which will be received by this interface. Range NoRecv/RIP 1/RIP 2/ RIP 1 or RIP 2. Default value is RIP 1 or RIP 2.
• **Split Horizon**	SplitHorizon is used to control split horizon routing update behavior. Range Disabled/ Simple /Poison. Default value is Simple.

4.5.4 RIP Redistribution

Introduce the routes learnt from other routing protocols into RIP. The screen in Figure 4-5-4 appears.

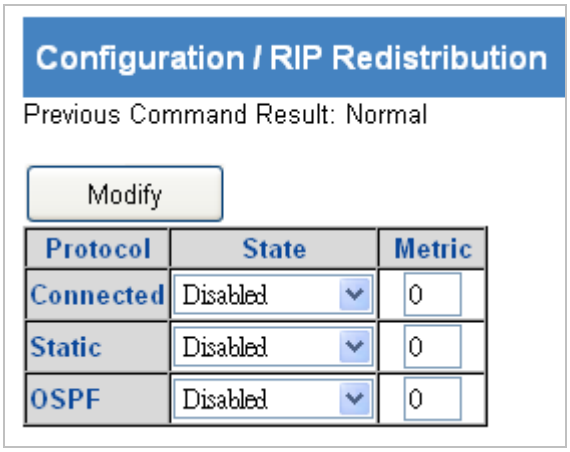


Figure 4-5-4: Configuration / RIP Redistribution Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Modify State, and Metric. Click the **Modify** button to apply changes.

The Page includes the following fields:

Object	Description
• **State**	Disabled / Enabled Protocol.
• **Metric**	Range is 0~ 16. Default value is 0.

4.5.5 OSPF Config

OSPF is abbreviation for Open Shortest Path First. It is an interior dynamic routing protocol for autonomous system based on

link-state. The protocol creates a link-state database by exchanging link-states among layer3 switches, and then uses the Shortest Path First algorithm to generate a route table basing on that database.

Autonomous system (AS) is a self-managed interconnected network. In large networks, such as the Internet, a giant interconnected network is broken down to autonomous systems. Big enterprise networks connecting to the Internet are independent AS, since the other hosts on the Internet are not managed by those AS and they don't share interior routing information with the layer3 switches on the Internet.
Each link-state Layer3 switch can provide information about the topology with its neighboring Layer3 switches.

- The network segment (link) connecting to the layer3 switch
- State of the connecting link

Link-state information is flooded throughout the network so that all Layer3 switches can get firsthand information. Link-state Layer3 switches will not broadcast all information contained in their route tables; instead, they only send changed link-state information. Link-state Layer3 switches establish neighborhood by sending "HELLO" to their neighbors, then link-state advertisements (LSA) will be sent among neighboring Layer3 switches. Neighboring Layer3 switch copy the LSA to their routing table and transfer the information to the rest part of the network. This process is referred to as "flooding". In this way, firsthand information is sent throughout the network to provide accurate map for creating and updating routes in the network. Link-state routing protocols use cost instead of hops to decide the route. Cost is assigned automatically or manually. According to the algorithm in link-state protocol, cost can be used to calculate the hop number for packets to pass, link bandwidth, and current load of the link. The administrator can even add weight for better assessment of the link-state.

1) When a link-state layer3 switch enters a link-state interconnected network, it sends a HELLO packet to get to know its neighbors and establish neighborhood.
2) The neighbors respond with information about the links they are connecting and the related costs.
3) The originate layer3 switch uses this information to build its own routing table
4) Then, as part of the regular update, layer3 switch send link-state advertisement (LSA) packets to its neighboring layer3 switches. The LSA include links and related costs of that layer3 switch.
5) Each neighboring layer3 switch copies the LSA packet and passes it to the next neighbor (i.e. flooding).
6) Since routing database is not recalculated before layer3 switch forwards LSA flooding, the converging time is greatly reduced.

One major advantage of link-state routing protocols is the fact that infinite counting is impossible, this is because of the way link-state routing protocols build up their routing table. The second advantage is that converging in a link-state interconnected network is very fast, once the routing topology changes, updates will be flooded throughout the network very soon. Those advantages release some layer3 switch resources, as the process ability and bandwidth used by bad route information are minor.

The features of OSPF protocol include the following: OSPF supports networks of various scales, several hundreds of layer3 switches can be supported in an OSPF network. Routing topology changes can be quickly found and updating LSAs can be

sent immediately, so that routes converge quickly. Link-state information is used in shortest path algorithm for route calculation, eliminating loop route. OSPF divides the autonomous system into areas, reducing database size, bandwidth occupation and calculation load. (According to the position of layer3 switches in the autonomous system, they can be grouped as internal area switches, area border switches, AS border switches and backbone switches). OSPF supports load balance and multiple routes to the same destination of equal costs. OSPF supports 4 level routing mechanisms (process routing according to the order of intra-area path, inter-area path, type 1 external path and type 2 external path). OSPF supports IP subnet and redistribution of routes from the other routing protocols, and interface-based packet verification. OSPF supports sending packets in multicast.

Each OSPF layer3 switch maintains a database describing the topology of the whole autonomous system. Each layer3 switch gathers the local status information, such as available interface, reachable neighbors, and sends link-state advertisement (sending out link-state information) to exchange link-state information with other OSPF layer3 switches to form a link-state database describing the whole autonomous system. Each layer3 switch builds a shortest path tree rooted by itself according to the link-state database, this tree provides the routes to all nodes in an autonomous system. If two or more layer3 switches exist (i.e. multi-access network), "designated layer3 switch" and "backup designated layer3 switch" will be selected. Designated layer3 switch is responsible for spreading link-state of the network. This concept helps reducing the traffic among the Layer3 switches in multi-access network.

OSPF protocol requires the autonomous system to be divided into areas. That is to divide the autonomous system into 0 area (backbone area) and non-0 areas. Routing information between areas are further abstracted and summarized to reduce the bandwidth required in the network. OSPF uses four different kinds of routes; they are intra-area route, inter-area route, type 1 external route and type 2 external route, in the order of highest priority to lowest. The route inside an area and between areas describes the internal network structure of an autonomous system, while external routes describe how to select the routing information to destination outside the autonomous system. The first type of exterior route corresponds to the information introduced by OSPF from the other interior routing protocols, the costs of those routes are comparable with the costs of OSPF routes; the second type of exterior route corresponds to the information introduced by OSPF from the other exterior routing protocols, but the costs of those routes are far greater than that of OSPF routes, so OSPF route cost is ignored when calculating route costs.

OSPF areas are centered with the Backbone area, identified as Area 0, all the other areas must be connected to Area 0 logically, and Area 0 must be continuous. For this reason, the concept of virtual link is introduced to the backbone area, so that physically separated areas still have logical connectivity to the backbone area. The configurations of all the layer3 switches in the same area must be the same.
In conclusion, LSA can only be transferred between neighboring Layer3 switches, OSPF protocol includes 5 types of LSA: router LSA, network LSA, network summary LSA to the other areas, ASBR summary LSA and AS external LSA. They can also be called type1 LSA, type2 LSA, type3 LSA, type4 LSA, and type5 LSA. Router LSA is generated by each layer3 switch inside an OSPF area, and is sent to all the other neighboring layer3 switches in the same area; network LSA is generated by the designated layer3 switch in the OSPF area of multi-access network, and is sent to all other neighboring layer3 switches in this area. (In order to reduce traffic on layer3 switches in the multi-access network, "designated layer3 switch" and "backup designated layer3 switch" should be selected in the multi-access network, and the network link-state is broadcasted by the designated layer3 switch); network summary LSA is generated by border switches in an OSPF area , and is transferred among

area border layer3 switches; AS external LSA is generated by layer3 switches on external border of AS, and is transferred throughout the AS.

As to autonomous systems mainly advertises exterior link-state, OSPF allow some areas to be configured as STUB areas to reduce the size of the topology database. Type4 LSA (ASBR summary LSA) and type5 LSA (AS external LSA) are not allowed to flood into/through STUB areas. STUB areas must use the default routes, the layer3 switches on STUB area edge advertise the default routes to STUB areas by type 3 summary LSA, those default routes only floods inside STUB area and will not get out of STUB area. Each STUB area has a corresponding default route, the route from a STUB area to AS exterior destination must rely on the default route of that area.

The following simply outlines the route calculation process of OSPF protocol:

1） Each OSPF-enabled layer3 switch maintains a database (LS database) describing the link-state of the topology structure of the whole autonomous system. Each layer3 switch generates a link-state advertisement according to its surrounding network topology structure (router LSA), and sends the LSA to other layer3 switches through link-state update (LSU) packets. Thus each layer3 switches receives LSAs from other layer3 switches, and all LSAs are combined to the link-state database.

2） Since a LSA is the description of the network topology structure around a layer3 switch, the LS database is the description of the network topology structure of the whole network. The layer3 switches can easily create a weighted vector map according to the LS database. Obviously, all layer3 switches in the same autonomous system will have the same network topology map.

3） Each layer3 switch uses the shortest path first (SPF) algorithm to calculate a tree of shortest path rooted by itself. The tree provides the route to all the nodes in the autonomous system, leaf nodes consist of the exterior route information. The exterior route can be marked by the layer3 switch broadcast it, so that additional information about the autonomous system can be recorded. As a result, the route table of each layer3 switch is different.

OSPF protocol is developed by the IETF, the OSPF v2 widely used now is fulfilled according to the content described in RFC2328. The screen in Figure 4-5-5 appears.

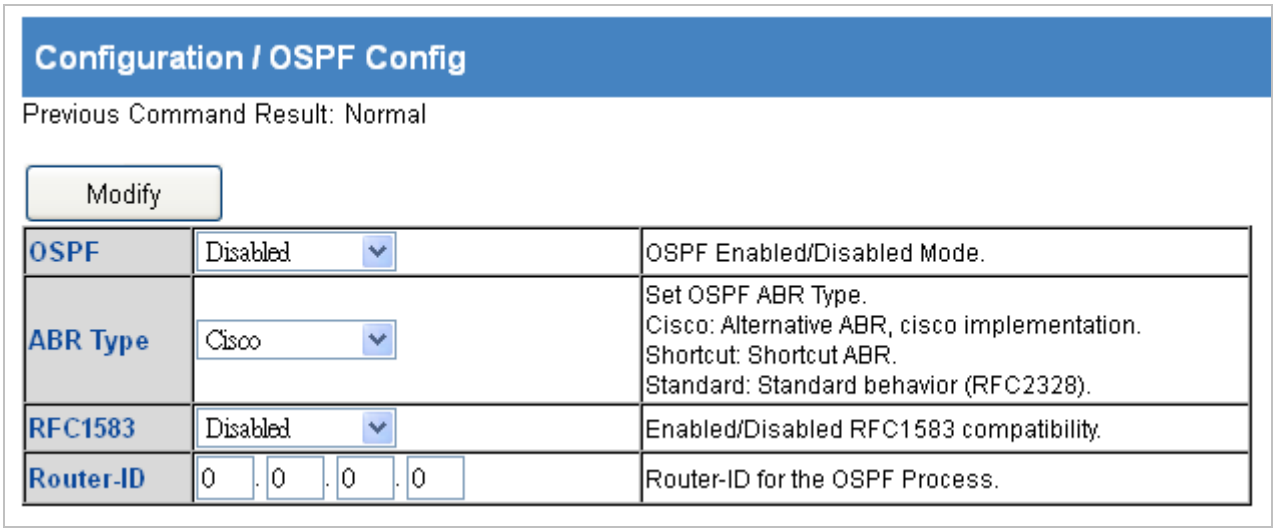


Figure 4-5-5: Configuration / OSPF Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Modify OSPF, ABR Type, RFC 1583, and Router-ID. Click the **Modify** button to apply changes.

The page includes the following fields:

Object	Description
• **OSPF**	Value range Disabled/Enabled, default is Disabled.
• **ABR Type**	Set OSPF ABR Type. Cisco: Alternative ABR, cisco implementation. Shortcut: Shortcut ABR. Standard: Standard behavior (RFC2328).
• **RFC 1583**	Enabled/Disabled RFC1583 compatibility. Value range Disabled/Enabled, default is Disabled.
• **Route-ID**	Router-ID for the OSPF Process.

4.5.6 OSPF Redistribution

To redistribute of process ID routing to this process. The no form of command deletes the redistribution of process ID routing to this process. When input the optional parameters of metric, metric type and routermap, then restores default configuration. Learn and introduce other routing protocol into OSPF area. The screen in Figure 4-5-6 appears.

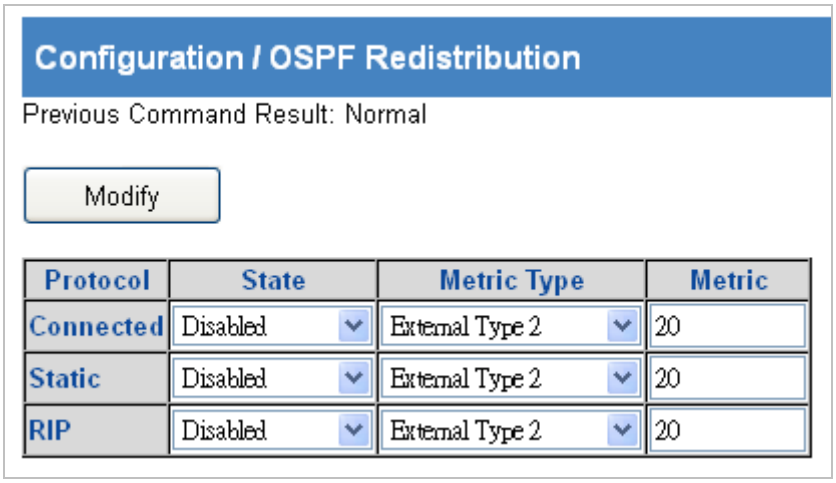


Figure 4-5-6: Confiugration / OSPF Redistribution Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Modify State, Metric Type, and Metric of Protocols.. Click the **Modify** button to apply changes.

The Page includes the following fields:

Object	Description
• **Protocol**	OSPF Redistribute System supports Connect, Static, RIP Three entry Protocol.
• **State**	Disabled / Enabled Protocol.
• **Metric Type**	Select External Type1, External Type2, Default: External Type2.
• **Metric**	Range is 0~ 16777214. Default value is 20.

4.5.7 OSPF Area Type

Set the area to stub or Not-So-Stubby-Area (NSSA) area. The screen in Figure 4-5-7 appears.

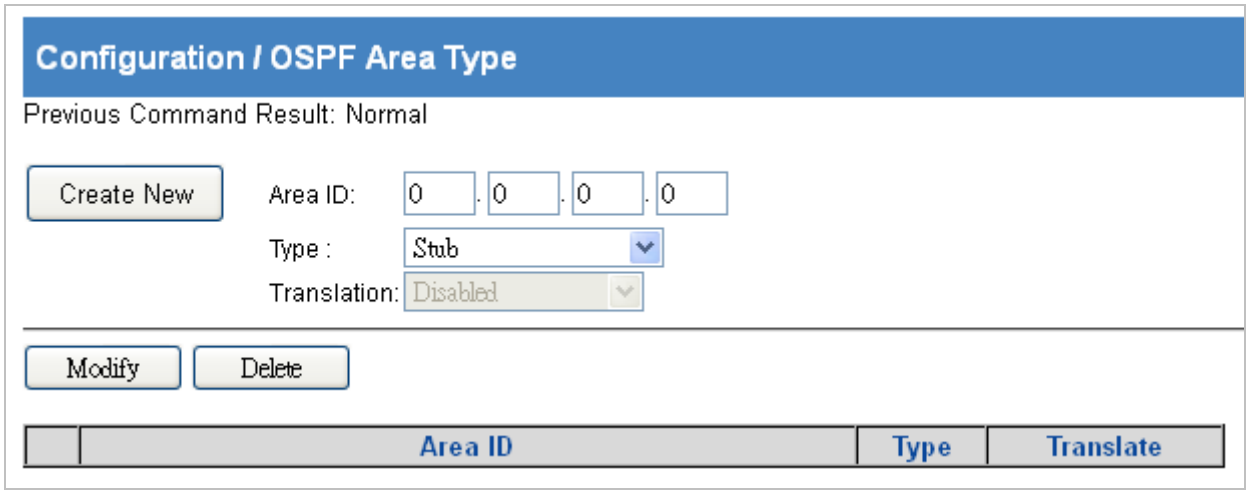


Figure 4-5-7: Confiugration / OSPF Area Type Configuration Page Screenshot

Object	Description
• **Operation**	**Create:** Fill the fields of Area ID, Type, and Translate. Clink "Create New" to create a new Area ID. **Modify:** Modify State, Metric Type, and Metric of Protocols.. Click "Modify" button to apply changes. **Delete:**

	To select checkbox. Click "Delete" button to Delete OSPF STUB/NSSA.

The Page includes the following fields:

Object	Description
• **Area ID**	IP Address Format Range 0.0.0.1~ 255.255.255.255.
• **Type**	1. STUB (No support Translate Function) 2. STUB NO SUMMARY (No support Translate Function) 3. NSSA 4. NSSA NO SUMMARY
• **Translation**	Range: Disabled / Enabled. Default: Disabled.

4.5.8 OSPF Virtual-Link

In the OSPF all non-backbone areas will be connected to a backbone area. If the connection to the backbone area is lost, virtual link will repair this connection. You can configure virtual link between any two backbone area routers connected with the public non-backbone area. The protocol treat routers connected by virtual links as a point-to-point network.

The screen in Figure 4-5-8 appears.

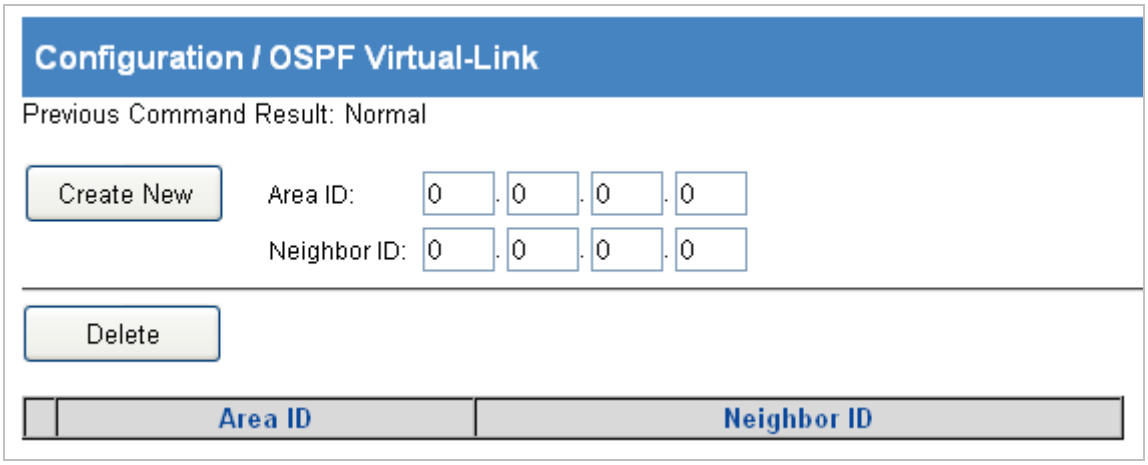


Figure 4-5-8: Confiugration / OSPF Virtual-Link Configuration Page Screenshot

Object	Description
• **Operation**	**Create:** Fill out the fields of Area ID, and Neighbor ID. Click the **Create New** button to create OSPF Virtual-Link.

	Delete: To select checkbox. Click the **Delete** button to delete OSPF Virtual-Link .

The page includes the following fields:

Object	Description
• **Area ID**	IP Address Format Range 0.0.0.1~ 255.255.255.255.
• **Neighbor ID**	IP Address Format Range 0.0.0.0~ 255.255.255.255.

4.5.9 OSPF Interface

The OSPF Interface includes the area ID, network type, priority, cost, hello-interval, dead-interval, retransmit-interval, transmit-delay, MTU-ignore, authentication mode / key & message digest key-ID. The configured column is used to change the OSPF interface configuration. The screen in Figure 4-5-9 appears.

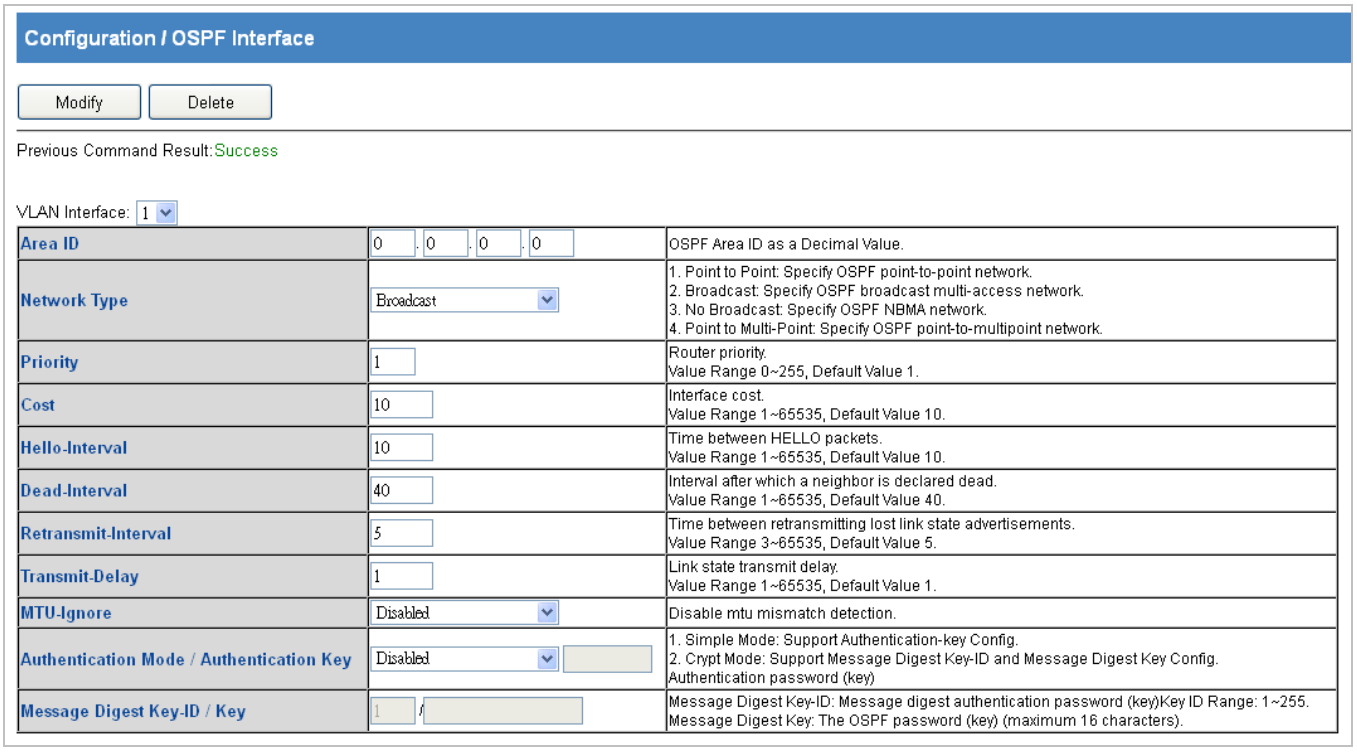


Figure 4-5-9: Configuration / OSPF Interface Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** To modify setting data Click the **Modify** button to modify OSPF Interface Config data.

	Delete: Click the **Delete** button to delete OSPF Interface Config data.

The Page includes the following fields:

Object	Description
• **Area ID**	OSPF Area ID as a Decimal Value.
• **Network Type**	1. Point to Point: Specify OSPF point-to-point network. 2. Broadcast: Specify OSPF broadcast multi-access network. 3. No Broadcast: Specify OSPF NBMA network. 4. Point to Multi-Point: Specify OSPF point-to-multipoint network.
• **Priority**	Router priority. Value Range 0~255, Default Value 1.
• **Cost**	Interface cost. Value Range 1~65535, Default Value 10.
• **Hello-Interval**	Time between HELLO packets. Value Range 1~65535, Default Value 10.
• **Dead-Interval**	Interval after which a neighbor is declared dead. Value Range 1~65535, Default Value 40.
• **Retransmit-Interval**	Time between retransmitting lost link state advertisements. Value Range 3~65535, Default Value 5.
• **Transmit-Delay**	Link state transmit delay. Value Range 1~65535, Default Value 1.
• **MTU-Ignore**	Disable mtu mismatch detection.
• **Authentication Mode / Authentication key**	1. Simple Mode: Support Authentication-key Config. 2. Crypt Mode: Support Message Digest Key-ID and Message Digest Key Config. Authentication password (key)
• **Message Digest Key-ID / Key**	Message Digest Key-ID: Message digest authentication password (key)Key ID Range: 1~255. Message Digest Key: The OSPF password (key) (maximum 16 characters).

4.5.10 OSPF Neighbor

Use this page on NBMA network to configure neighbor manually. Every known non-broadcasting neighbor router should be configured with a neighbor entry. The configured neighbor address should be the main address of the interface. The poll-interval should be much larger than the hello-interval. The screen in Figure 4-5-10 appears.

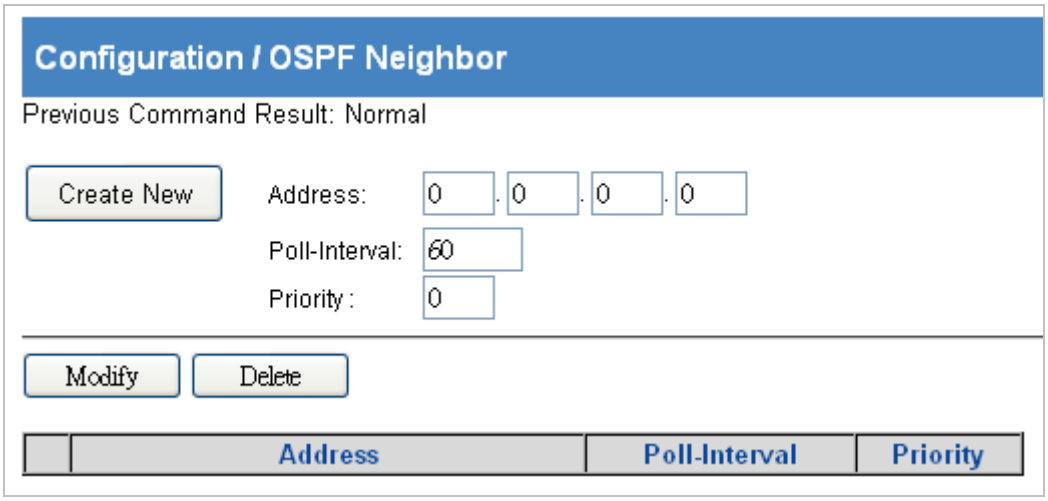


Figure 4-5-10: Confiugration / OSPF Neighbor Configuration Page Screenshot

Object	Description
• **Operation**	**Create:** To fill out Address, Poll-Interval and Priority Click the **Create New** button to create OSPF Neighbor Config. **Modify:** To modify setting data Select checkbox Click the **Modify** button to modify OSPF Neighbor Config data. **Delete:** Select checkbox Click the **Delete** button to delete OSPF Neighbor Config data.

The Page includes the following fields:

Object	Description
• **Address**	IP Address Format Range 0.0.0.1~ 255.255.255.255.
• **Poll-Interval**	Value Range 1~65535 second, Default Value 60.
• **Priority**	Value Range 1~255, Default Value 0.

4.5.11 VRRP Group

VRRP (Virtual Router Redundancy Protocol) is a fault tolerant protocol designed to enhance connection reliability between routers (or L3 Ethernet switches) and external devices. It is developed by the IETF for local area networks (LAN) with

multicast/broadcast capability (Ethernet is a Configuration Example) and has wide applications.

All hosts in one LAN generally have a default route configured to specified default gateway, any packet destined to an address outside the native segment will be sent to the default gateway via this default route. These hosts in the LAN can communicate with the external networks. However, if the communication link connecting the router serving as default game and external networks fails, all hosts using that gateway as the default next hop route will be unable to communicate with the external networks.

VRRP emerged to resolve such problem. VRRP runs on multiple routers in a LAN, simulating a "virtual" router (also referred to as a "Standby cluster") with the multiple routes. There is an active router (the "Master") and one or more backup routers (the "Backup") in the Standby cluster. The workload of the virtual router is actually undertaken by the active router, while the Backup routers serve as backups for the active router.

The virtual router has its own "virtual" IP address (can be identical with the IP address of some router in the Standby cluster), and routers in the Standby cluster also have their own IP address. Since VRRP runs on routes or Ethernet Switches only, the Standby cluster is transparent to the hosts with the segment. To them, there exists only the IP address of the Virtual Router instead of the actual IP addresses of the Master and Backup(s). And the default gateway setting of all the hosts uses the IP address of the Virtual Router. Therefore, hosts within the LAN communicate with the other networks via this Virtual Router. But basically, they are communicating with the other networks via the Master. In the case when the Master of the Standby cluster fails, a backup will take over its task and become the Master to serve all the hosts in the LAN, so that uninterrupted communication between LAN hosts and external networks can be achieved.

To sum it up, in a VRRP Standby cluster, there is always a router/Ethernet serving as the active router (Master), while the rest of the Standby cluster servers act as the backup router(s) (Backup, can be multiple) and monitor the activity of Master all the time. Should the Master fail, a new Master will be elected by all the Backups to take over the work and continue serving the hosts within the segment. Since the election and take-over duration is brief and smooth, hosts within the segment can use the Virtual Router as normal and uninterrupted communication can be achieved. The screen in Figure 4-5-11 appears.

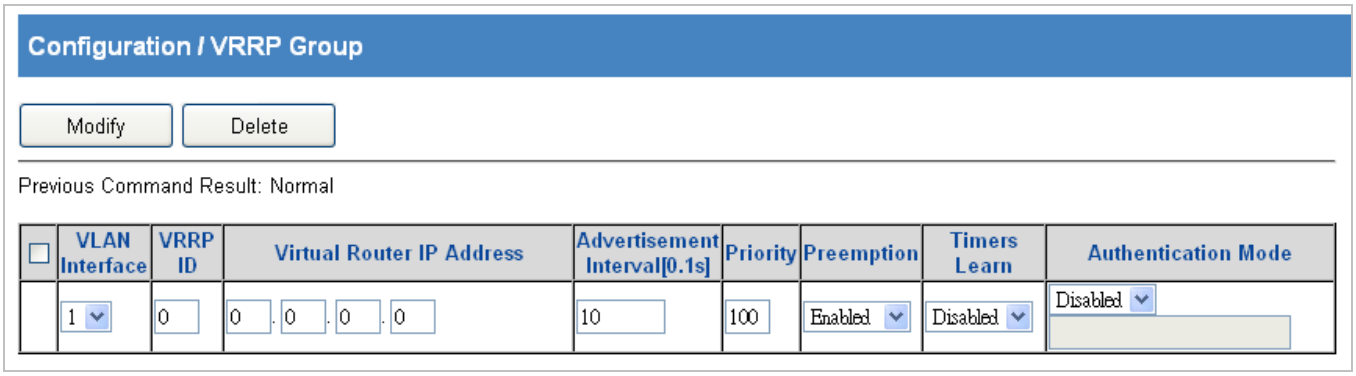


Figure 4-5-11: Configuration / VRRP Group Configuration Page Screenshot

Object	Description
• **Operation**	**Modify (Create):** Fill out the first row data. Click the **Modify** button to modify (create) VRRP Group Config data. **Modify:** Update setting data. Select a row item selected. Click the **Modify** button to modify VRRP Group Config data. **Delete:** Select a row item selected. Click the **Delete** button to delete VRRP Group Config data.

The Page includes the following fields:

Object	Description
• **VLAN Interface**	The identity for the VLAN Interface. Range 1~4094.
• **VRRP ID**	VRRP group index identity.
• **Virtual Router IP Address**	Virtual router IP should be in the same subnet with VLAN interface. Different VRRP group should not have the same virtual router IP.
• **Advertisement Interval [0.1sec]**	Value Range 1~2550, Default Value 10. Value 10 stands for 1 second. (0.1s * 10 = 1s)
• **Priority**	Value Range 1~254, Default Value 100.
• **Preemption**	Range: Disabled / Enabled Default: Enabled.
• **Timers Learn**	Range: Disabled / Enabled Default: Disabled.
• **Authentication Mode**	Range: Disabled / Enabled Default: Disabled. Enabled Support VRRP Group Auth Data.

4.5.12 DHCP Server

DHCP [RFC2131] is the acronym for Dynamic Host Configuration Protocol. It is a protocol that assigns IP address dynamically from the address pool as well as other network configuration parameters such as default gateway, DNS server, and default route and host image file position within the network. DHCP is the enhanced version of BOOTP. It is a mainstream technology that can not only provide boot information for diskless workstations, but can also release the administrators from manual recording of

IP allocation and reduce user effort and cost on configuration. Another benefit of DHCP is it can partially ease the pressure on IP demands, when the user of an IP leaves the network that IP can be assigned to another user.

DHCP is a client-server protocol, the DHCP client requests the network address and configuration parameters from the DHCP server; the server provides the network address and configuration parameters for the clients; if DHCP server and clients are located in different subnets, DHCP relay is required for DHCP packets to be transferred between the DHCP client and DHCP server.

Explanation:

1. DHCP client broadcasts DHCPDISCOVER packets in the local subnet.
2. On receiving the DHCPDISCOVER packet, DHCP server sends a DHCPOFFER packet along with IP address and other network parameters to the DHCP client.
3. DHCP client broadcast DHCPREQUEST packet with the information for the DHCP server it selected after selecting from the DHCPOFFER packets.
4. The DHCP server selected by the client sends a DHCPACK packet and the client gets an IP address and other network configuration parameters.

The screens in Figure 4-5-12 are Figure 4-5-13 appear.

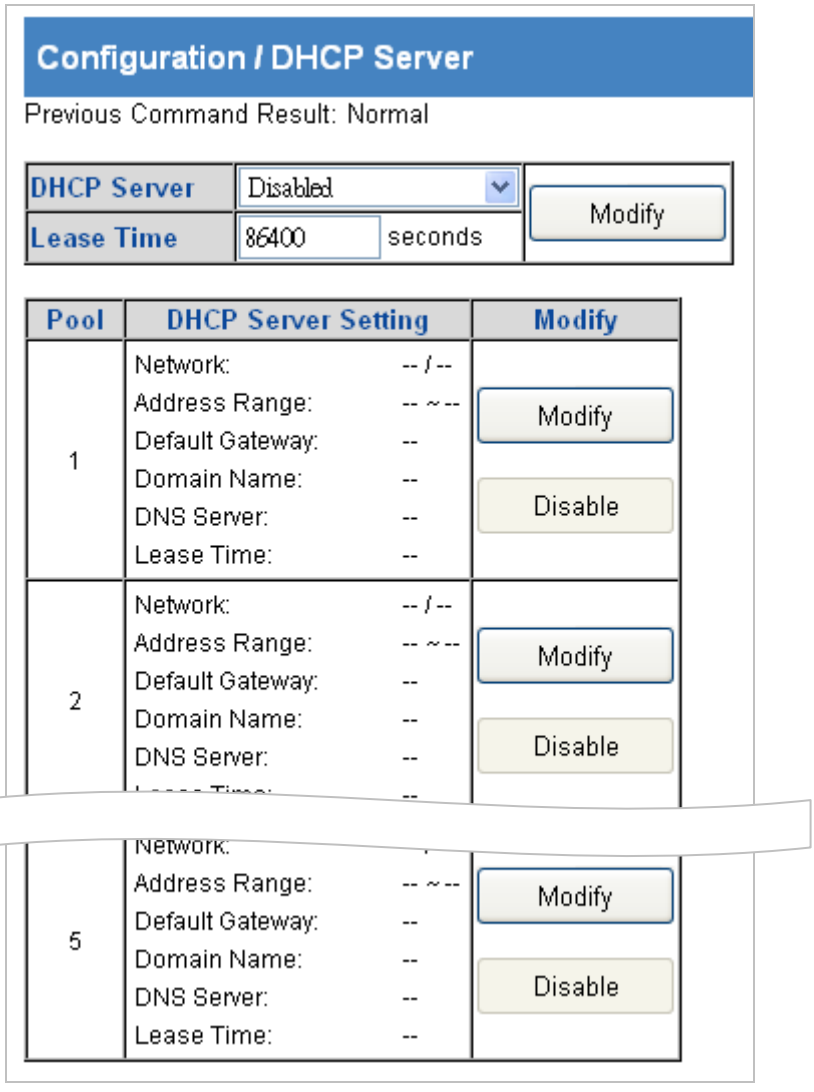


Figure 4-5-12: Confiugration / DHCP Server Configuration Page Screenshot

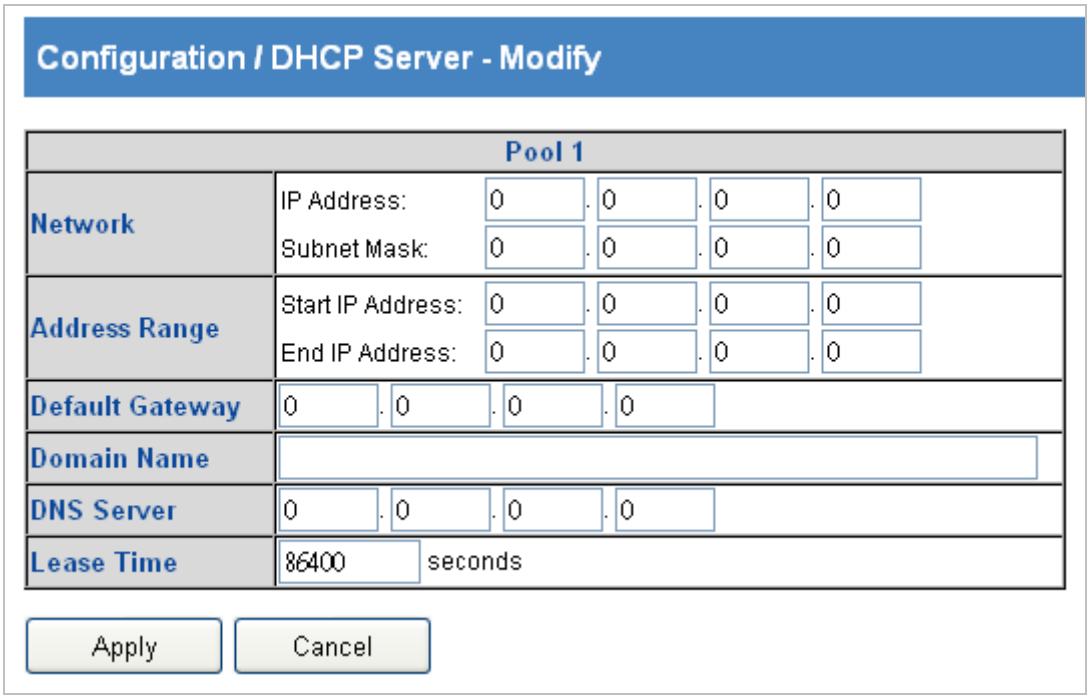


Figure 4-5-13: Confiugration / DHCP Server Configuration Page Screenshot

Object	Description
• **Operation**	**Modify the IP Routing:** Select IP Routing field. Click the **Modify** button to apply change. **Create New:** Fill VID, IP Address and Netmask. Click the **Create New** button to create Interface VLAN. **Delete:** Multi-select a row data in Interface VLAN table. Click the **Delete** button to delete Interface VLAN.

The page includes the following fields:

Object	Description
• **IP Routing**	Layer 3 IP routing/forward. Allow Disabled/Enabled. Default value is Disabled.

• **VID**	The identity for the RIP Interface. Range 1~4094. 1st RIP interface VLAN always exist for VLAN 1. (Only support set can't be deleted)
• **IP Address**	IP address for the vlan interface. Range 0~255. Default value is 0.
• **Netmask**	Network subnet mask for the VLAN interface. Range 0~255. Default value is 0.
• **MAC Address**	MAC address for the VLAN interface. Read only.

4.6 Port Configuration

Use the Port Menu to display or configure the Industrial Managed Switch's ports.

4.6.1 VLAN Port Configuration

The VLAN Port Configuration includes the PVID, default priority, accepted frame tyre, port security and L2 entry number. The configured column is used to view or change the L2 function. The VLAN Port Configuration screen in Figure 4-6-1 appears.

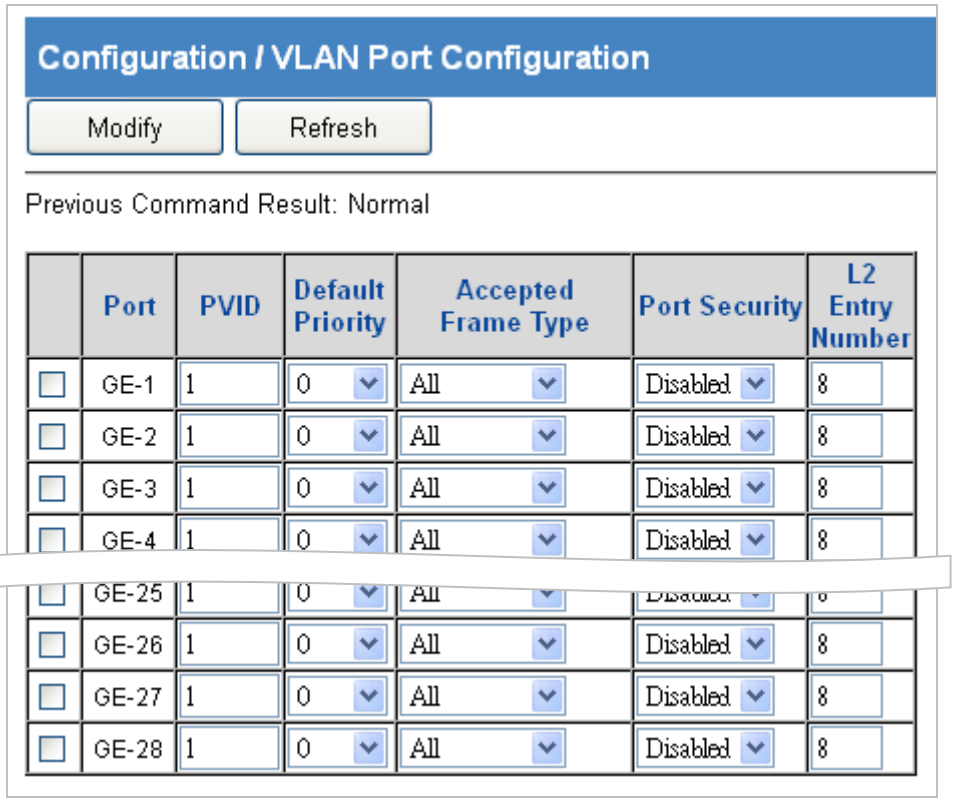


Figure 4-6-1: Configuration / VLAN Port Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Enter or select row by checking up check box. Modify the configuration Press the **Modify** button to apply modification. **Refresh:** Click the **Refresh** button to get current data.

The Page includes the following fields:

Object	Description
• **Port**	Bridge port number
• **PVID**	Value: 1~4094. Default value is 1.
• **Default Priority**	Default Priority value: 0~7. Default is 0.
• **Accepted Frame Type**	Type: All/ OnlyVlanTagged/ Only Untagged. Default is All.
• **Port Security**	Range: Enabled/ Disabled. Default is Disabled.
• **L2 Entry Number**	Range: 0~32. Default is 8.

4.6.2 Giga Port

This page displays current port configurations. Ports can also be configured here. The screen in Figure 4-6-2 appears.

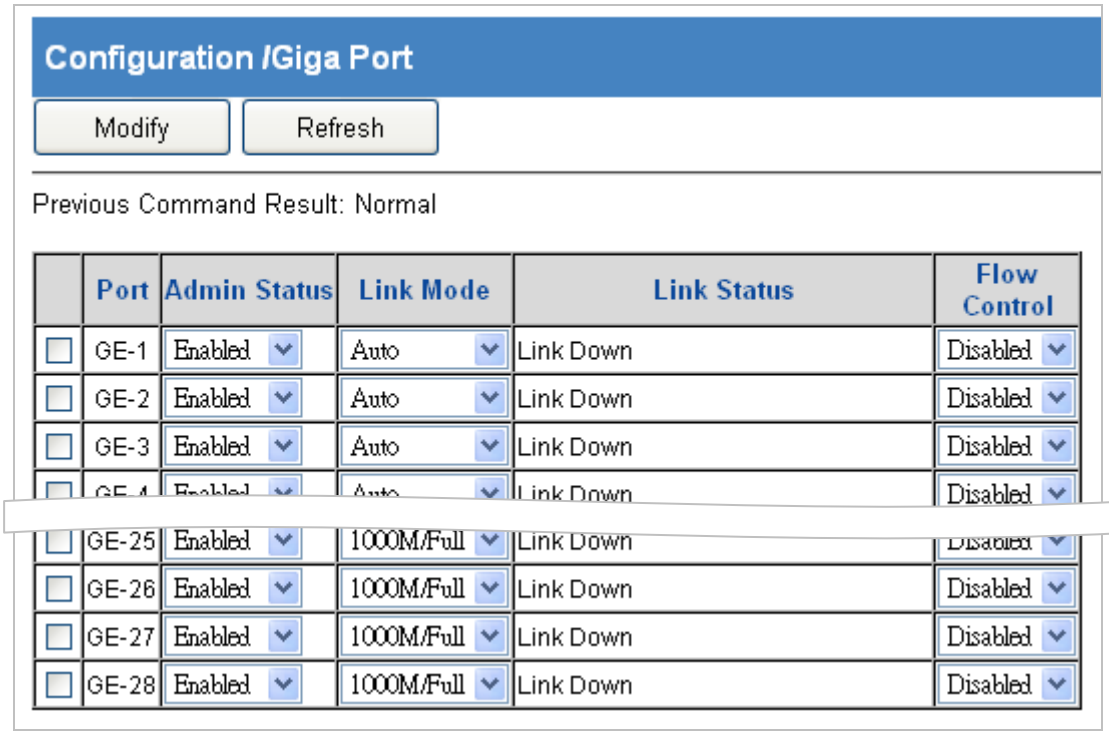


Figure 4-6-2: Confiugration / Giga Port Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Select a row item to selected Set or select the following fields. Click the **Modify** button to modify.

The Page includes the following fields:

Object	Description
• **Port**	GE-1~ 28 Number of Port.
• **Admin Status**	Enabled/Disabled port status, default=Enabled.
• **Link Mode**	Configuration for Link Mode: Auto (default is Auto) 10Mbps Half/Full Duplex 100Mbps Half/Full Duplex 1000Mbps Full Duplex
• **Link Status**	Display Link type and speed Possible Type: Copper/ SFP Possible Status: 10Mbps Half-Duplex or Full-Duplex 100Mbps Half-Duplex or Full-Duplex 1000Mbps Full-Duplex

• **Flow Control**	When **Auto** speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner.

4.6.3 Port Isolation

The port isolation for the switch can be monitored and modified here. Port isolation can be added or deleted here. Port members of each port isolation can be added or removed here. The screen in Figure 4-6-3 appears.

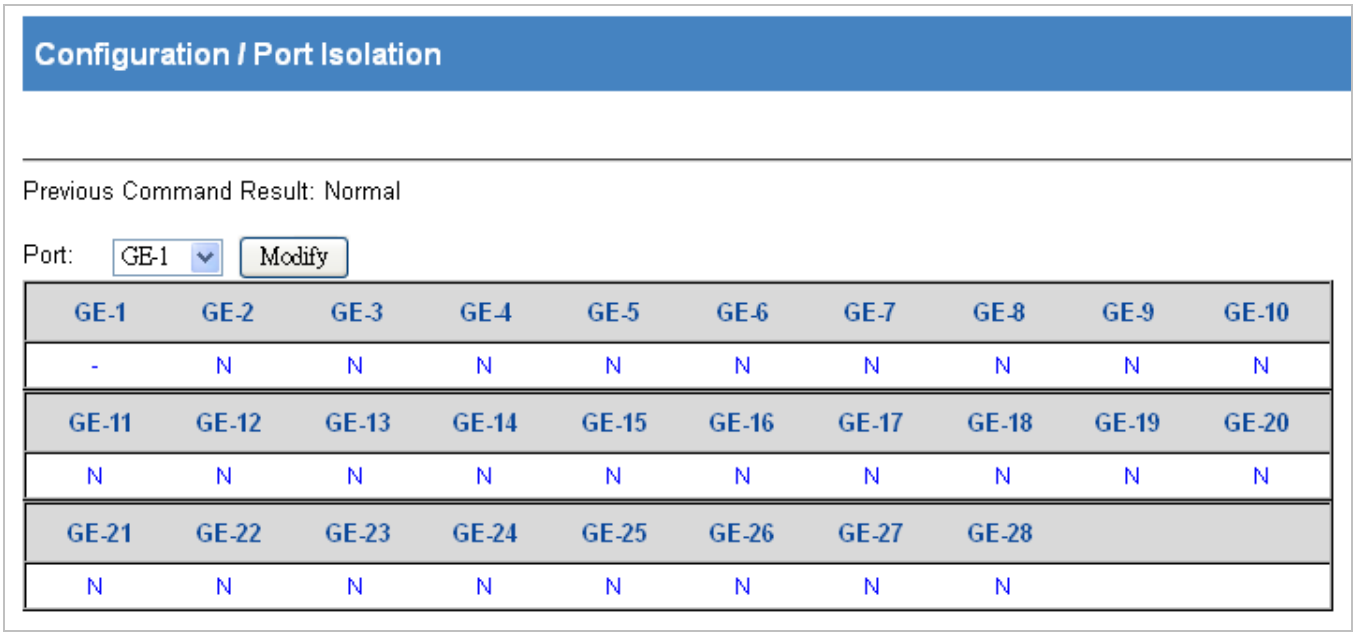


Figure 4-6-3: Configuration / Port Isolation Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Click the **Modify** button to open the modification page. **Port Isolation - Modify:** Click the **Disable All**, or **Enable All** or click on (Y/N/-) to change isolation setting by port. Click the **Apply** button to apply change or press "Cancel" to cancel and go back to main page of Isolation.

The page includes the following fields:

Object	Description
• **Source Port**	GE-1 ~ 28 Number of Port.

• **Isolation Port**	Option: Y/ N/ -. Y: Isolation is true N: Isolation is false -: Not permit setting (Isolation port is the same as source port)
• **Disable All**	Disable Isolation to all ports
• **Enable All**	Enable Isolation to all ports
• **Apply**	Apply setting data.
• **Cancel**	Cancel setting data.

4.6.4 Jumbo Frame

This page provides to select the **maximum frame size** allowed for the switch port. The Jumbo Frame screen in Figure 4-6-4 appears.

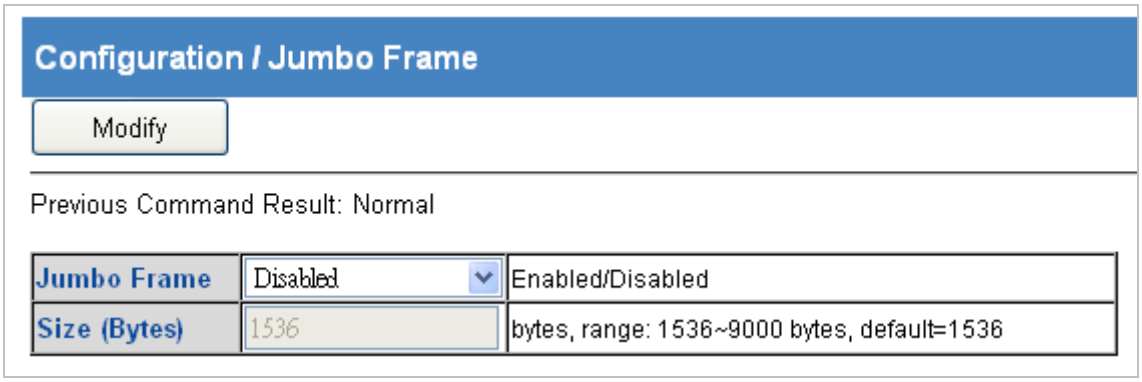


Figure 4-6-4: Configuration / Jumbo Frame Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Modify the configuration. Click the **Modify** button to apply change.

The Page includes the following fields:

Object	Description
• **Jumbo Frame**	Option: Enabled/ Disabled, Default is Disabled.
• **Size**	Range: 1536~9000 bytes, Default is 1536 bytes.

4.6.5 Port Mirroring

Configure port Mirroring on this page. This function provides 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.

- To debug network problems, selected traffic can be copied, or mirrored to a mirror port where a frame analyzer can be attached to analyze the frame flow.
- The Industrial Managed Switch can unobtrusively mirror traffic from any port to a monitor port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.

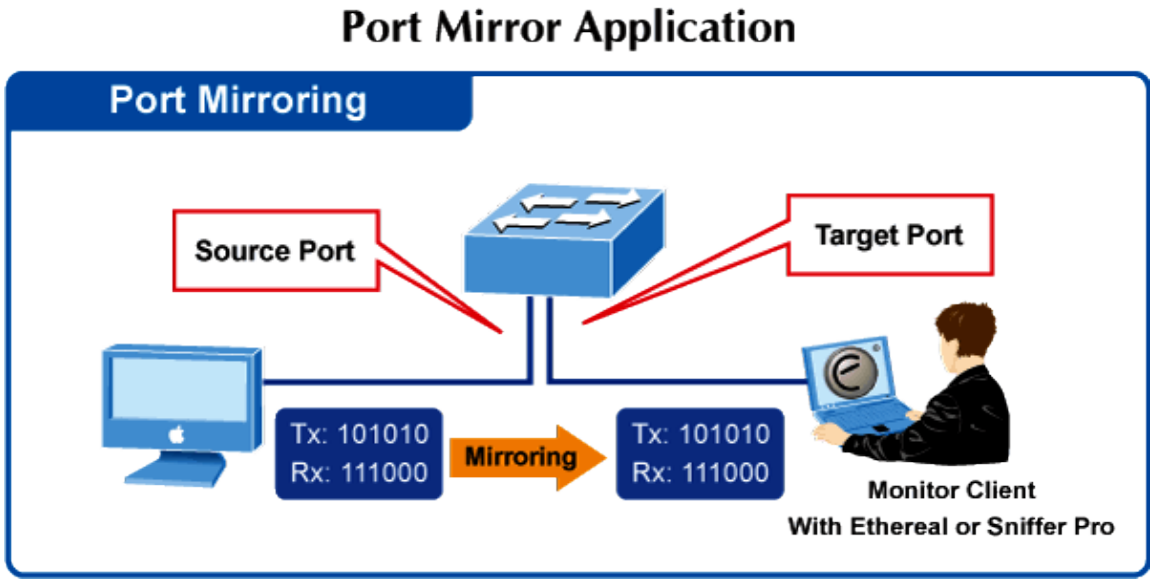


Figure 4-6-5: Port Mirror Application

The traffic to be copied to the mirror port is selected as follows:

- All frames received on a given port (also known as ingress or source mirroring).
- All frames transmitted on a given port (also known as egress or destination mirroring).

Mirror Port Configuration

The Port Mirror screen in Figure 4-6-6 appears.

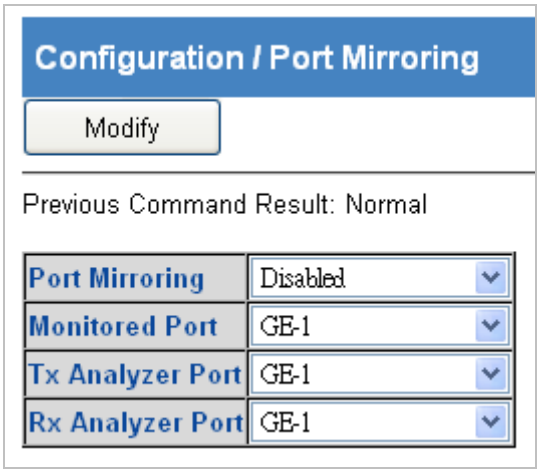


Figure 4-6-6: Confiugration / Port Mirror Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Modify the configuration Click the **Modify** button to apply change

The Page includes the following fields:

Object	Description
• **Port Mirror**	Enable/Disable Port Mirror function, default is Disabled.
• **Monitored Port**	Value range is GE-1 ~ 28, default is GE-1. Port to be monitored.
• **Tx Analyzer Port**	Value range is GE-1 ~ 28, default is GE-1. It monitors 'out' packet of monitored port.
• **Rx Analyzer Port**	Value range is GE-1 ~ 28, default is GE-1. It monitors 'in' packet of monitored port.

4.7 VLAN

4.7.1 VLAN Membership

■ **Adding Static Members to VLANs**

Use the VLAN membership to configure port members for the selected VLAN index. The VLAN membership configuration for the selected switch can be monitored and modified here. Up to 255 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 screen in Figure 4-7-1 appears.

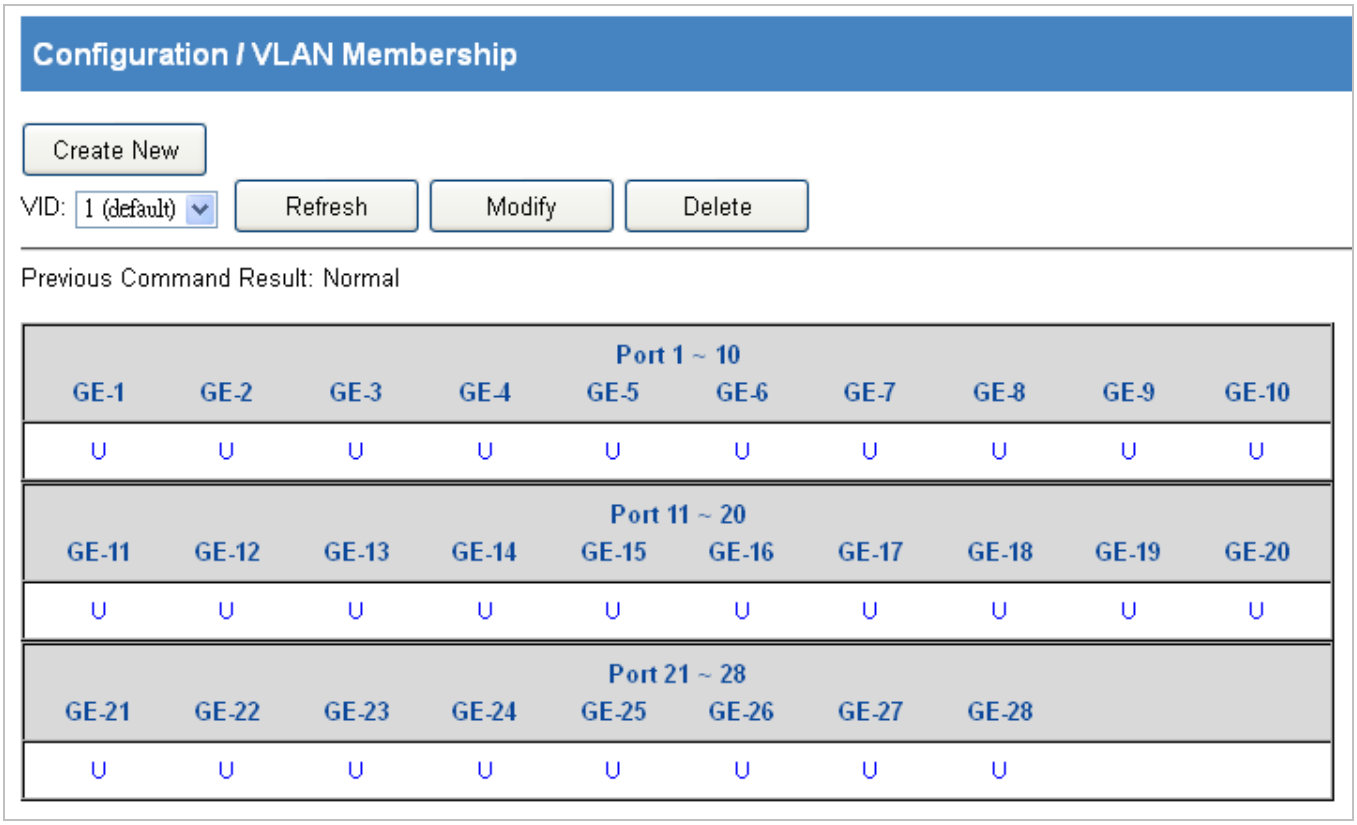


Figure 4-7-1: Configuration / VLAN Membership Configuration Page Screenshot

Object	Description
• **Operation**	**Create New:** Click the **Create New** button to open "Create New" page. Set VID and Name. Click fields to change status. Click the **Apply** button to create, or click the **Cancel** button to cancel. **Modify:** Click the **Modify** button to open "Modify" page. Modify Name. Click the **Apply** button to modify, or click the **Cancel** button to cancel. **Delete:** Choice VLANs checkbox to select. Click **Delete** to delete all selected VLANs. **Refresh:** Click the **Refresh** button to get current data.

The page includes the following fields:

Object	Description
• VID	Value: 1~4094. Default value is 1.
• Name	Range:0~32 characters
• Tagged	Range: T/ U/ －. T: Tagged U: Untagged －: None (not join this VLAN)
• Set All Ports to None	Set all ports to None (no port join this VLAN) －
• Set All Ports to Tagged	Set all ports join the VLAN as Tagged. T
• Set All Ports to Untagged	Set all ports join the VLAN as Untagged U

4.7.2 Protocol-based VLAN

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this Managed Switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type being used by the inbound packets.

This page allows you to configure protocol-based VLAN Group Setting. The protocol-based VLAN screens in Figure 4-6-2 appear.

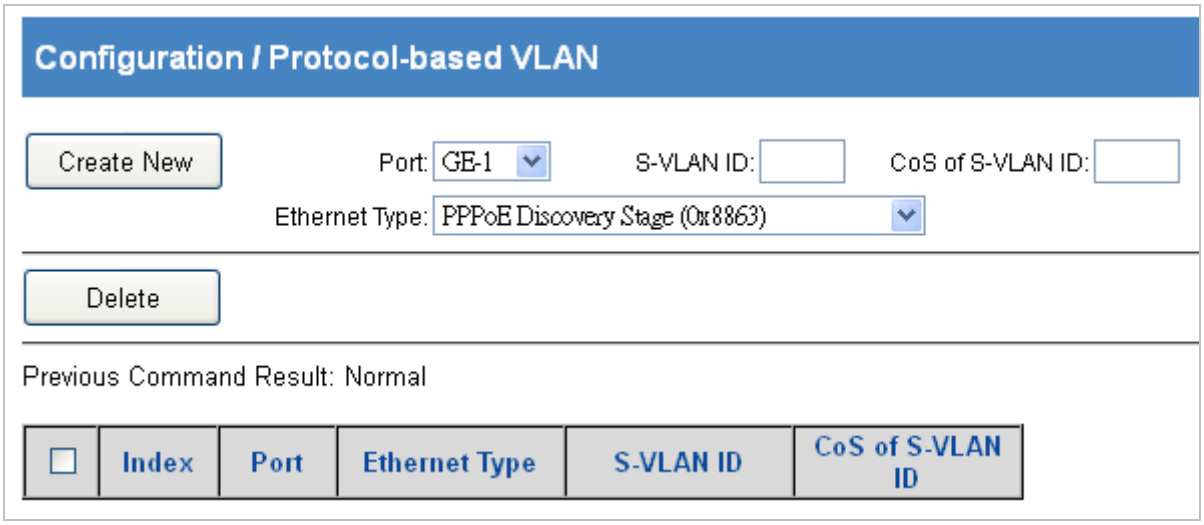


Figure 4-7-2: Configuration / Protocol-based VLAN Configuration Page Screenshot

Object	Description
• **Operation**	**Create New:** Click the **Create New** button to create New page. Set Port and Ether Type, input SVLAN and S-Prio. Click the **Create New** button. (Max entry: 10.) **Delete:** Select Index with check box. Click the **Delete** button to delete data.

The Page includes the following fields:

Object	Description
• **Index**	Index 1~10.
• **Port**	Protocol-base VLAN config port number, Port range:1 ~ 28 of Port.
• **Ether Type**	Select Ether Type: 1. PPPoE Discovery Stage (0x8863). 2. PPPoE Session Stage (0x8864). 3. Internet Protocol (0x0800). 4. Address Resolution Protocol (ARP) (0x0806). 5. Others (input ether type), Range 0000~FFFF.
• **S-VLAN ID**	Service VLAN ID, Range 1 ~ 4094
• **CoS of S-VLAN ID**	CoS of SVLAN: 0~7, 8:reserve

4.7.3 VLAN Translation

VLAN translation, as one can tell from the name, which translates the original VLAN ID to new VLAN ID according to the user requirements so to exchange data across different VLANs. VLAN translation is classified to ingress translation and egress translation, this switch only supports switchover of ingress for VLAN ID. Application and configuration of VLAN translation will be explained in detail in this section. The screen in Figure 4-7-3 appears.

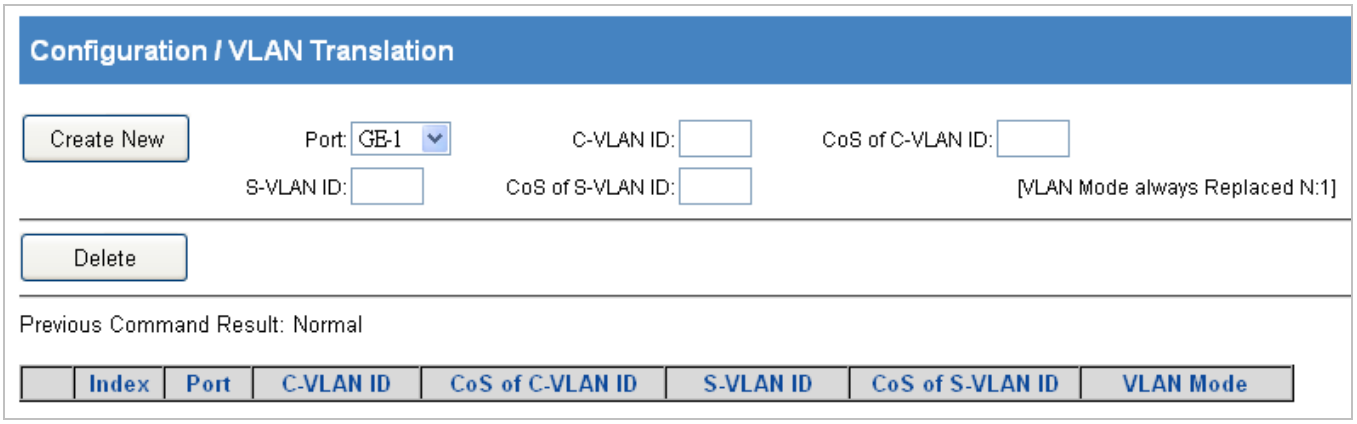


Figure 4-7-3: Configuration / VLAN Translation Configuration Page Screenshot

Object	Description
• **Operation**	**Create:** Select Port, fill CVLAN, C-Prio, SVLAN and S-Prio. Click the **Create New** button to create new entry. Click the **Delete** button to delete selected entry(s).

The page includes the following fields:

Object	Description
• **Index**	Index 1~10, max entry number: 10.
• **Port**	VLAN translation port number: GE-1 ~ MAX Number of Port.
• **C-VLAN ID**	Customer VLAN ID: Range: 1 ~ 4094
• **CoS of C-VLAN ID**	CoS of CVLAN: Range: 0~7, 8: reserve
• **S-VLAN ID**	Service VLAN ID: Range: 1 ~ 4094
• **CoS of S-VLAN ID**	CoS of SVLAN: Range: 0~7, 8: reserve
• **VLAN Mode**	Currently only supports: Replaced N to 1.

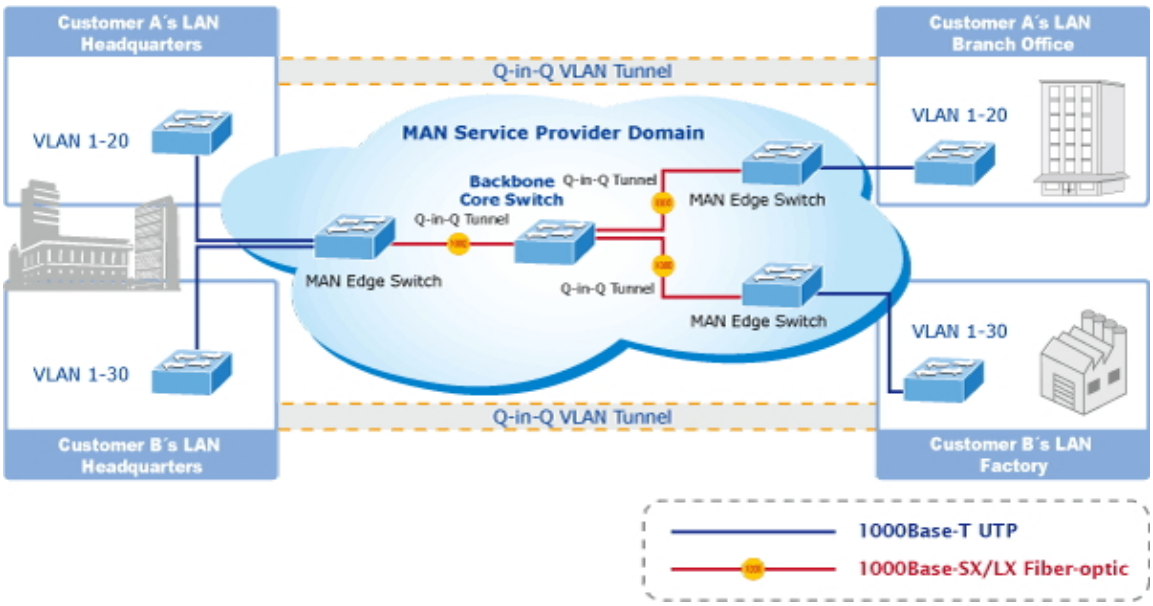
4.7.4 VLAN Stacking

■ IEEE 802.1Q Tunneling (Q-in-Q)

IEEE 802.1Q Tunneling (QinQ) is designed for service providers carrying traffic for multiple customers across their networks.

QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting **Service Provider VLAN (SPVLAN)** tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4094.



The Industrial Managed Switch supports multiple VLAN tags and can therefore be used in MAN applications as a provider bridge, aggregating traffic from numerous independent customer LANs into the **MAN (Metro Access Network)** space. One of the purposes of the provider bridge is to recognize and use VLAN tags so that the VLANs in the MAN space can be used independent of the customers' VLANs. This is accomplished by adding a VLAN tag with a MAN-related VID for frames entering the MAN. When leaving the MAN, the tag is stripped and the original VLAN tag with the customer-related VID is again available.

This provides a tunneling mechanism to connect remote costumer VLANs through a common MAN space without interfering with the VLAN tags. All tags use EtherType **0x8100** or **0x88A8**, where 0x8100 is used for customer tags and 0x88A8 are used for service provider tags.

In cases where a given service VLAN only has two member ports on the switch, the learning can be disabled for the particular VLAN and can therefore rely on flooding as the forwarding mechanism between the two ports. This way, the MAC table requirements is reduced.

The screen in Figure 4-7-4 appears.

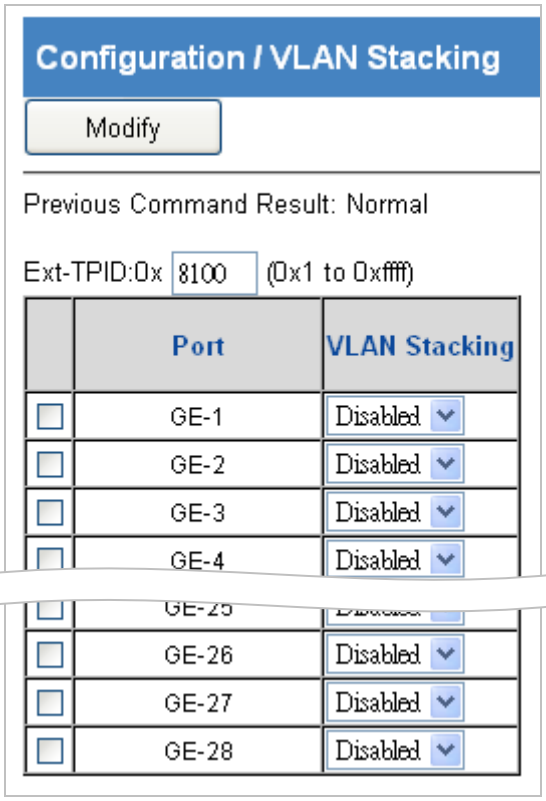


Figure 4-7-4: Confiugration / VLAN Stacking Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Select Port check box : Select Select mode Disabled/ Enabled and click the **Modify** button to apply change.

The page includes the following fields:

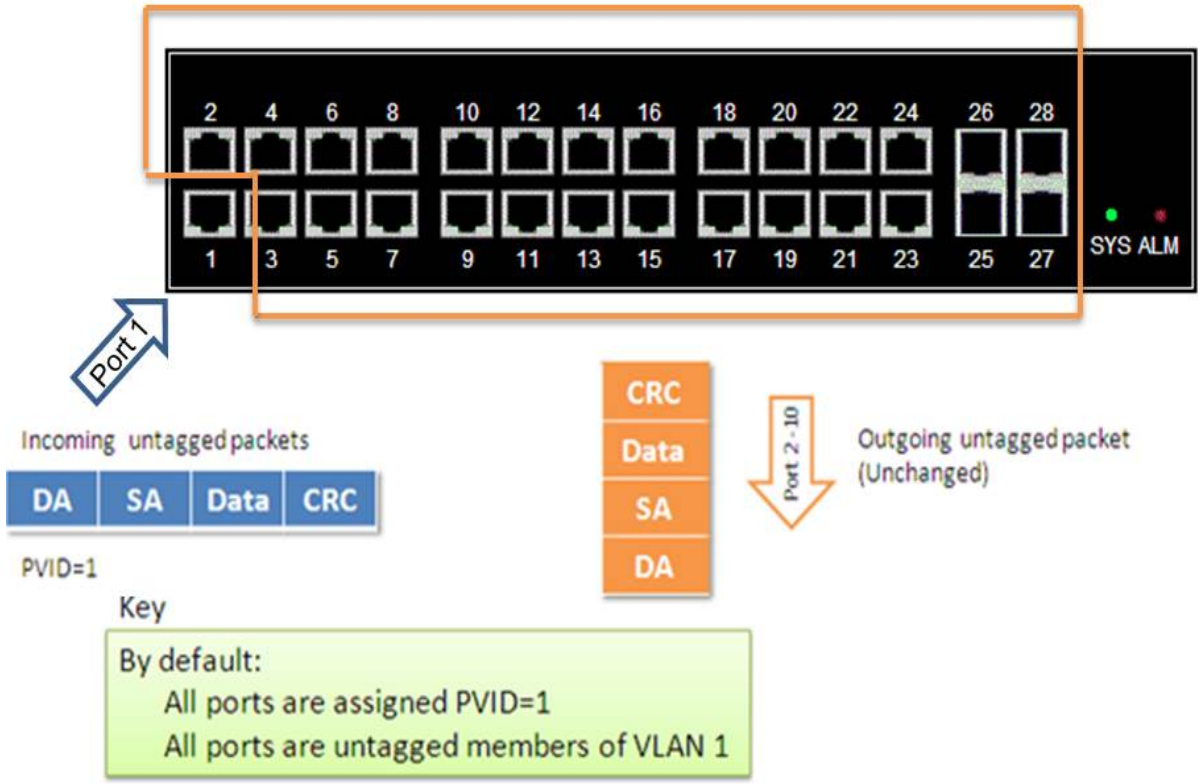
Object	Description
• **Ext-TPID (Hex)**	The range is from 1~FFFF (0x1 to 0xffff) Default is 0x8100
• **VLAN Stacking Port**	Port: GE-1 ~ 28 of Port.
• **VLAN Stacking**	Enable/Disable VLAN Stacking (QinQ) mode. Default value is disable.

4.7.5 VLAN Example

This part describes how to configure Virtual LANs (VLANs) in Industrial Managed Switch. The Industrial Managed Switch supports up to 4094 VLANs. Ports are grouped into broadcast domains by assigning them to the same VLAN. Frames received in on VLAN can only be forwarded within that VLAN, and multicast frames and unknown unicast frames are flooded only to ports in the same VLAN.

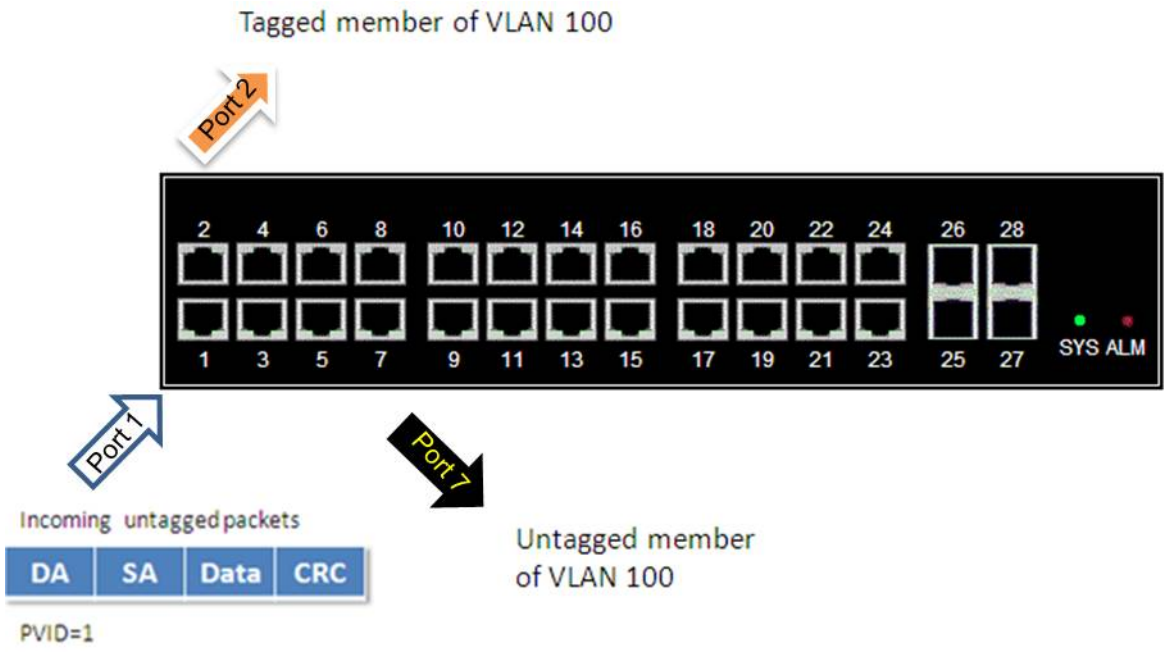
4.7.5.1 Default VLAN Settings

Each port in the Industrial Managed Switch has a configurable default VLAN number, known as its PVID. This places all ports on the same VLAN initially, although each port PVID is configurable to any VLAN number between 1 and 4094.
The default configuration settings for Industrial Managed Switch have all ports set as untagged members of VLAN 1 with all ports configured as PVID=1. In default configuration example shown in the following figure, all incoming packets are assigned to VLAN 1 by the default port VLAN identifier (PVID=1).



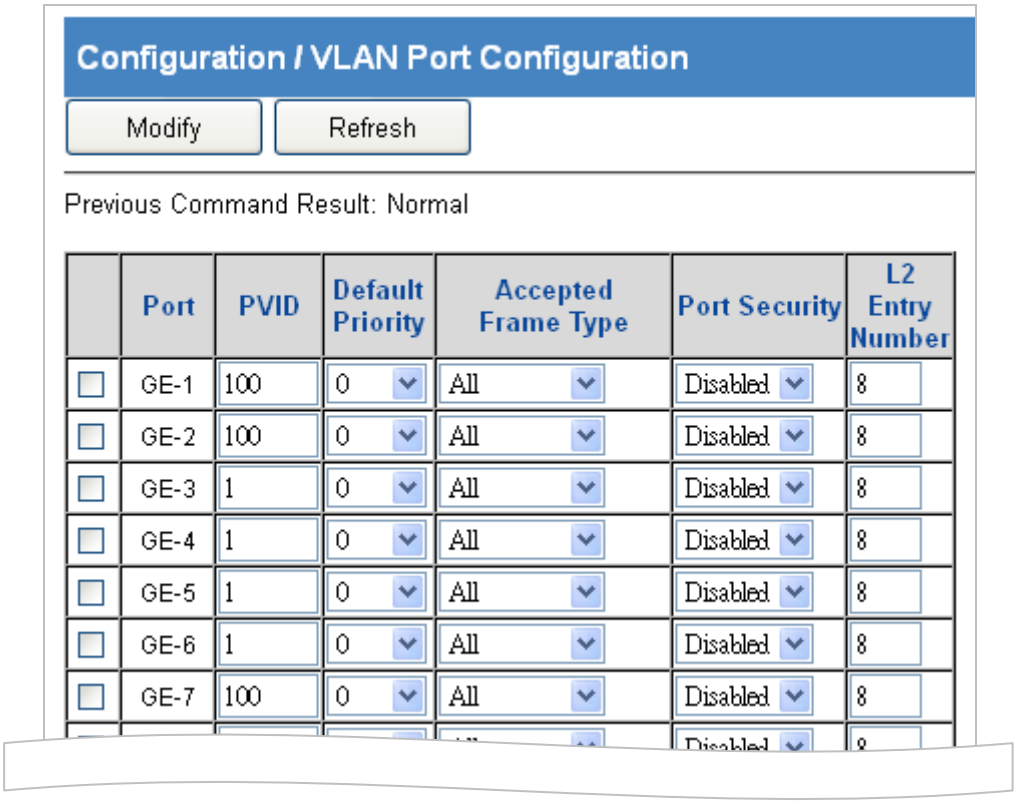
4.7.5.2 Port-based VLANs

When the Industrial Managed Switch receives an untagged VLAN packet, it will add a VLAN tag to the frame according to the PVID setting on a port. As shown in the following figure, the untagged packet is marked (tagged) as it leaves the Industrial Managed Switch through Port 2, which is configured as a tagged member of VLAN100. The untagged packet remains unchanged as it leaves the Industrial Managed Switch through Port 7, which is configured as an untagged member of VLAN100.



Configuration:

Step 1. Go to Configuration-> VLAN Port Configuration and configure PVID 100 on Port 1, Port 2 and Port 7.



Step 2. Select Configuration-> VLAN Membership. Create a VLAN with VLAN ID 100. Enter a VLAN name in the Name field.

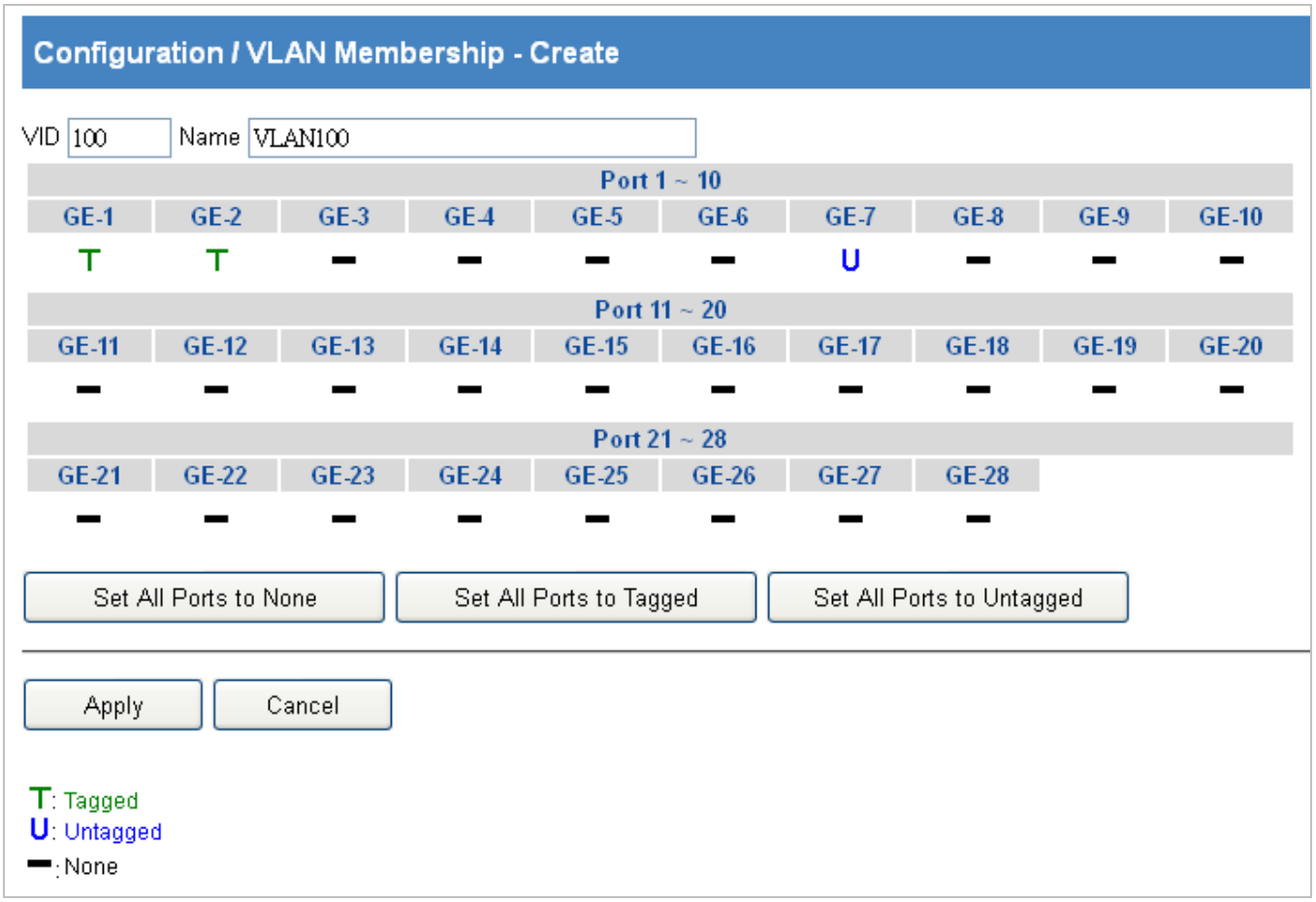
Step 3. Assign VLAN tag setting to or remove it from a port by toggling the check box under an individual port number. The tag settings determine if packets that are transmitted from the port tagged or untagged with the VLAN ID. The possible tag settings are:

T Specifies that the egress packet is tagged for the port.

U Specifies that the egress packet is untagged for the port.

— Specifies that the port is not part of the VLAN.

Here we set tagged VLAN100 on Port 1 and Port 2, untagged VLAN100 on Port7.



Step 4. Transmit untagged unicast packets from Port 1 to Port 2 and Port 7. The Industrial Managed Switch should tag it with VID 100. The packet has access to Port2 and Port 7. The outgoing packet is stripped of its tag to leave Port 7 as an untagged packet. For Port 2, the outgoing packet leaves as a tagged packet with VID 100.

Step 5. Transmit untagged unicast packets from Port 2 to Port 1 and Port 7. The Industrial Managed Switch should tag it with VID 100. The packet has access to Port1 and Port 7. The outgoing packet is stripped of its tag to leave Port 7 as an untagged packet. For Port 1, the outgoing packet leaves as a tagged packet with VID 100.

Step 6. Transmit untagged unicast packets from Port 7 to Port 1 and Port 2. The Industrial Managed Switch should tag it with VID 100. The packet has access to Port1 and Port 2. For Port 1 and Port 2, the outgoing packet leaves as a tagged packet with VID 100.

Step 7. Repeat step 4 using broadcast and multicast packets.

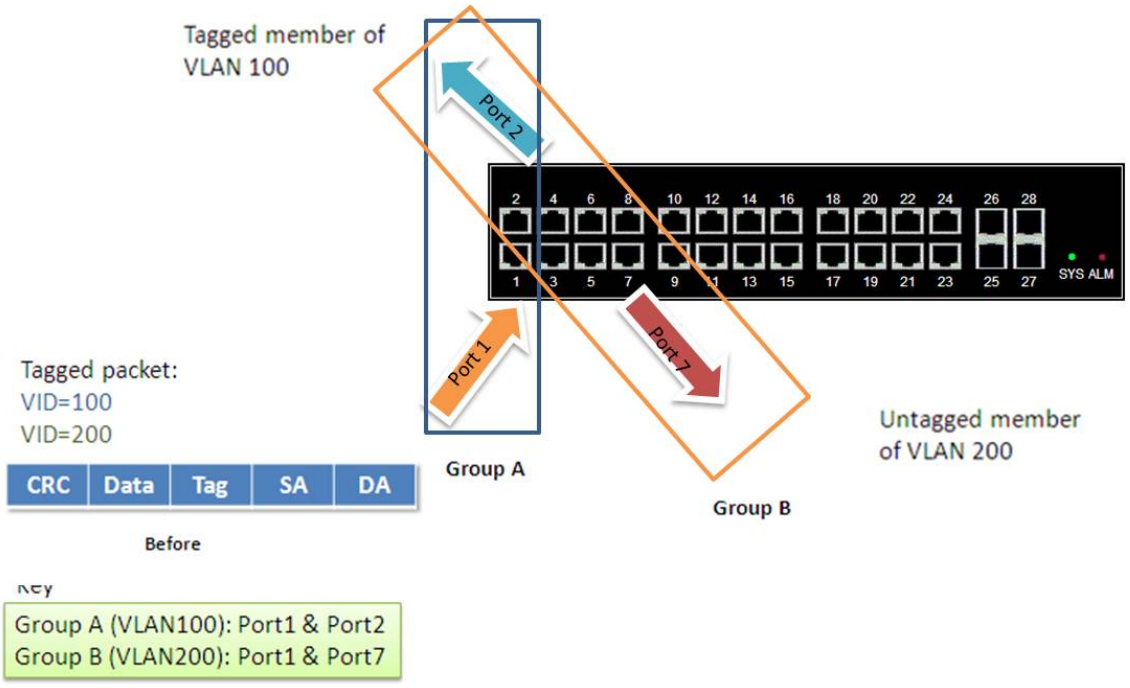
CLI Command:

```
enable
configure
interface gigabit 1
default vlan 100
vlan 100 tag
exit
interface gigabit 2
default vlan 100
vlan 100 tag
exit
interface gigabit 7
default vlan 100
vlan 100 untag
exit
```

4.7.5.3 IEEE802.1Q Tagging

Industrial Managed Switch is able to construct layer-2 broadcast domain by identifying VLAN ID specified by IEEE 802.1Q. It forwards a frame between bridge ports assigned to the same VLAN ID and can set multiple VLANs on each bridge port.

In the following figure, the tagged incoming packets are assigned directly to VLAN 100 and VLAN 200 because of the tag assignment in the packet. Port 2 is configured as a tagged member of VLAN 100, and Port 7 is configured as an untagged member of VLAN 200. Hosts in the same VLAN communicate with each other as if they in a LAN. However, hosts in different VLANs cannot communicate with each other directly.

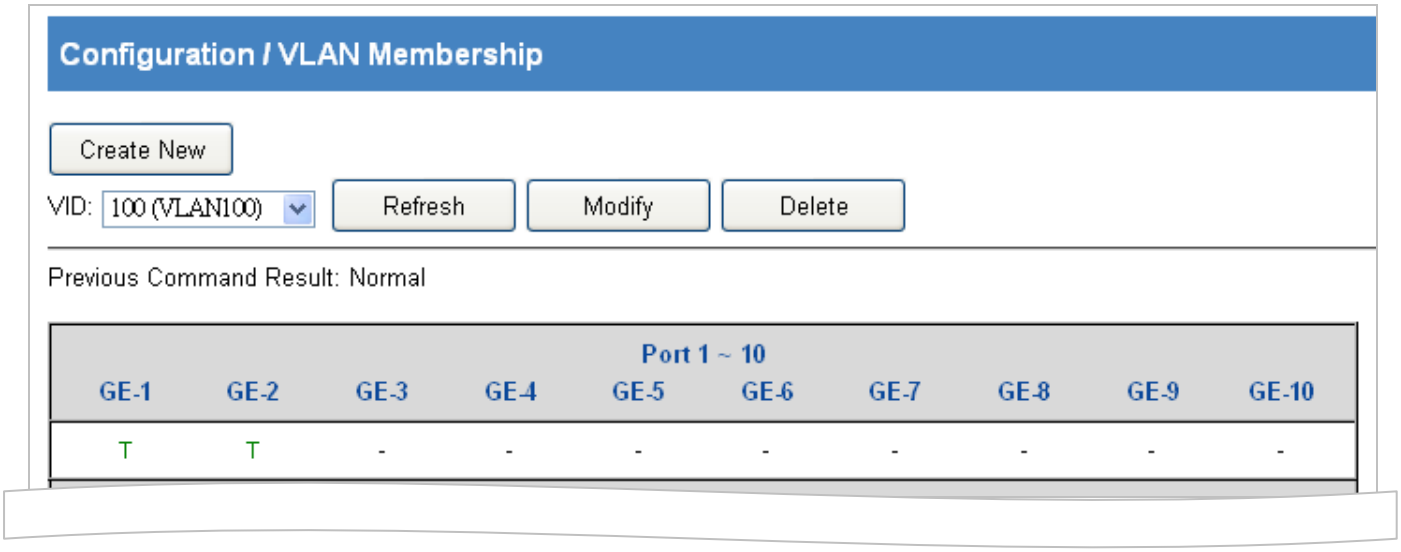


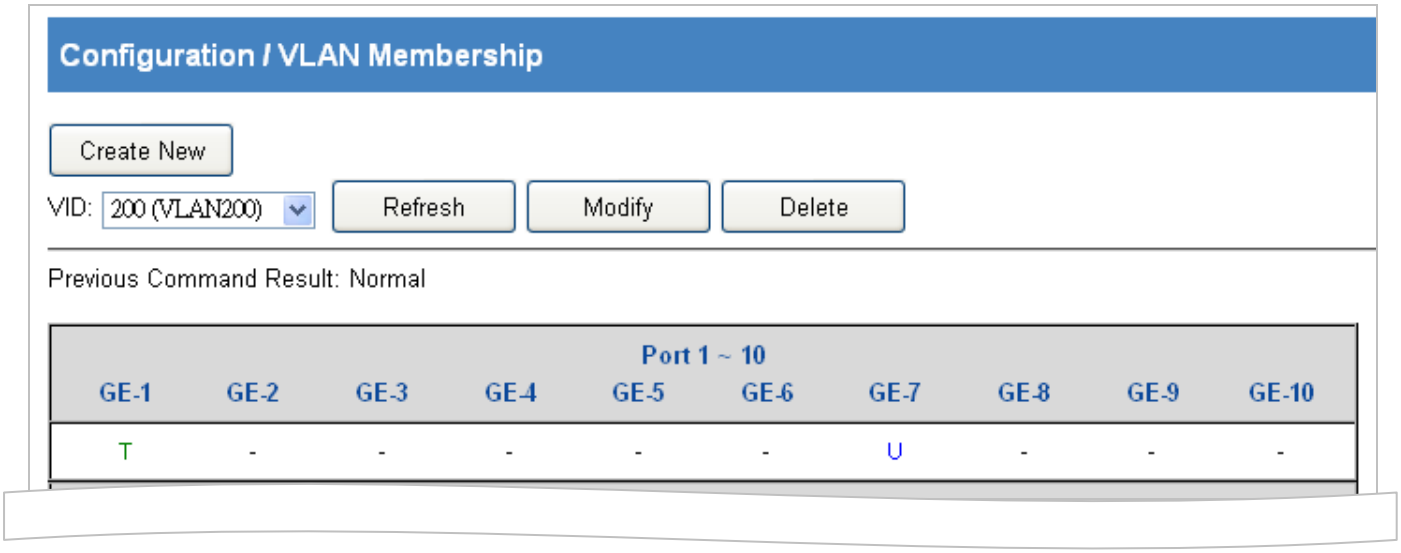
In this case:

1. The hosts from Group A can communicate with each other.
2. The hosts from Group B can communicate with each other.
3. The hosts of Group A and Group B can't communicate with each other.
4. Both the Group A and Group B can go to Internet through Industrial Managed Switch

Configuration:

Step 1. In the Configuration/ Static VLAN page specify the VLAN membership as follows:





Step 2. Transmit unicast packets with VLAN tag 100 from Port 1 to Port 2 and Port 7. The Industrial Managed Switch should tag it with VID 100. The packet only has access to Port2. For Port 2, the outgoing packet leaves as a tagged packet with VID 100.

Step 3. Transmit unicast packets with VLAN tag 200 from Port 1 to Port 2 and Port 7. The Industrial Managed Switch should tag it with VID 200. The packet only has access to Port7. The outgoing packet on Port 7 is stripped of its tag as an untagged packet.

Step 4. Transmit unicast packets with VLAN tag 100 from Port 2 to Port 1 and Port 7. The Industrial Managed Switch should tag it with VID 100. The packet only has access to Port1. For Port 1, the outgoing packet leaves as a tagged packet with VID 100.

Step 5. Transmit unicast packets with VLAN tag 200 from Port 7 to Port 1 and Port 2. The Industrial Managed Switch should tag it with VID 200. The packet only has access to Port1. The outgoing packet on Port 1 will leave as a tagged packet with VID 200.

Step 6. Repeat the above steps using broadcast and multicast packets.

CLI Command:

```
enable
configure
vlan 100 v100
vlan 200 v200
interface gigabit 1
vlan 100 tag
vlan 200 tag
exit
interface gigabit 2
vlan 100 tag
exit
interface gigabit 7
vlan 200 untag
```

4.8 MAC Learning & Forwarding

Switching of frames is based upon the DMAC address contained in the frame. The Industrial Managed 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.

4.8.1 Static Filtering Database

The static entries in the MAC table are shown in this table. The static MAC table can contain 512 entries. The MAC table is sorted first by VLAN ID and then by MAC address. The screen in Figure 4-8-1 appears.

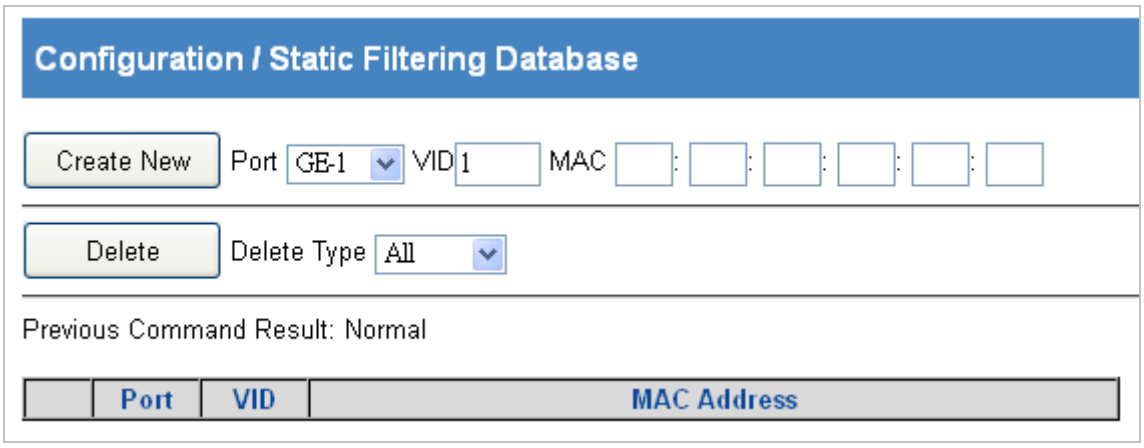


Figure 4-8-1: Configuration / Static Filtering Database Configuration Page Screenshot

Object	Description
• **Operation**	**Create New:** Setting Port, VID and MAC Address Click the **Create New** button to create a new data **Delete:** Select a delete type "All/Port/VID/Selected" If delete type is "Port", then select a port from list. If delete type is "VID", then input a VID. If delete type is "Selected", then select row(s) to be deleted. Click the **Delete** button to delete.

The page includes the following fields:

Object	Description
• **Port**	Giga Port: GE-1~ 28 of Port
• **VID**	Range: 1~4094. Default value is 1.
• **MAC Address**	Format XX:XX:XX:XX:XX:XX

4.8.2 Aging Time

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

The screen in Figure 4-8-2 appears.

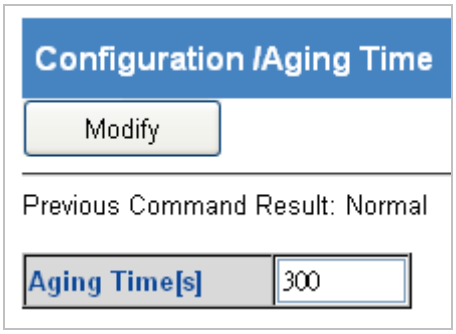


Figure 4-8-2: Configuration / Aging Time Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Modify the configuration Click the Modify button to apply the change

The page includes the following fields:

Object	Description
• **Aging Time(Sec)**	Range: 10~1000000, Default is 300 seconds.

4.9 Spanning Tree Protocol (STP)

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

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

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 is in one of the following five states:

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

A port transitions from one state to another as follows:

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

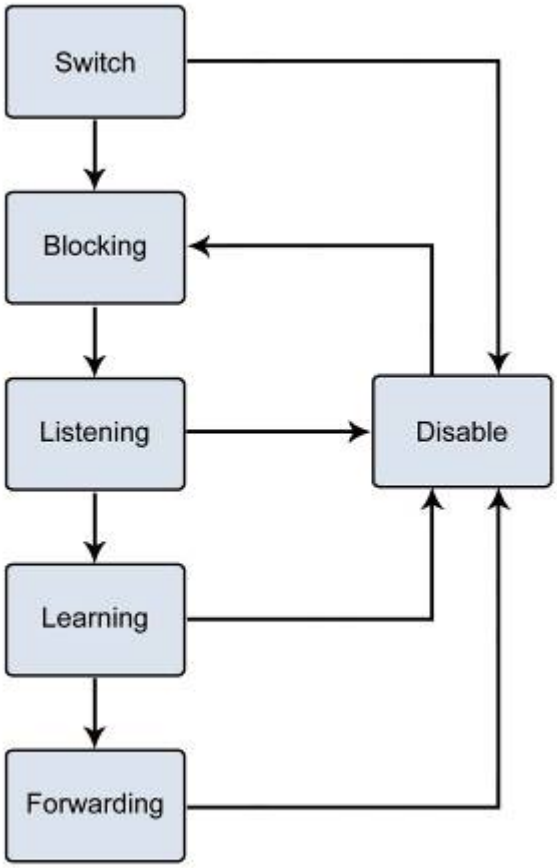


Figure 4-9-1: STP Port State Transitions

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

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

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

Default Spanning Tree Configuration

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

User-Changeable STA Parameters

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

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

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

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

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

Forward Delay Timer – The Forward Delay can be from 4 to 30 seconds. This is the time any port on the

Switch spends in the listening state while moving from the blocking state to the forwarding state.

Observe the following formulas when setting the above parameters:

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

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

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

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

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.

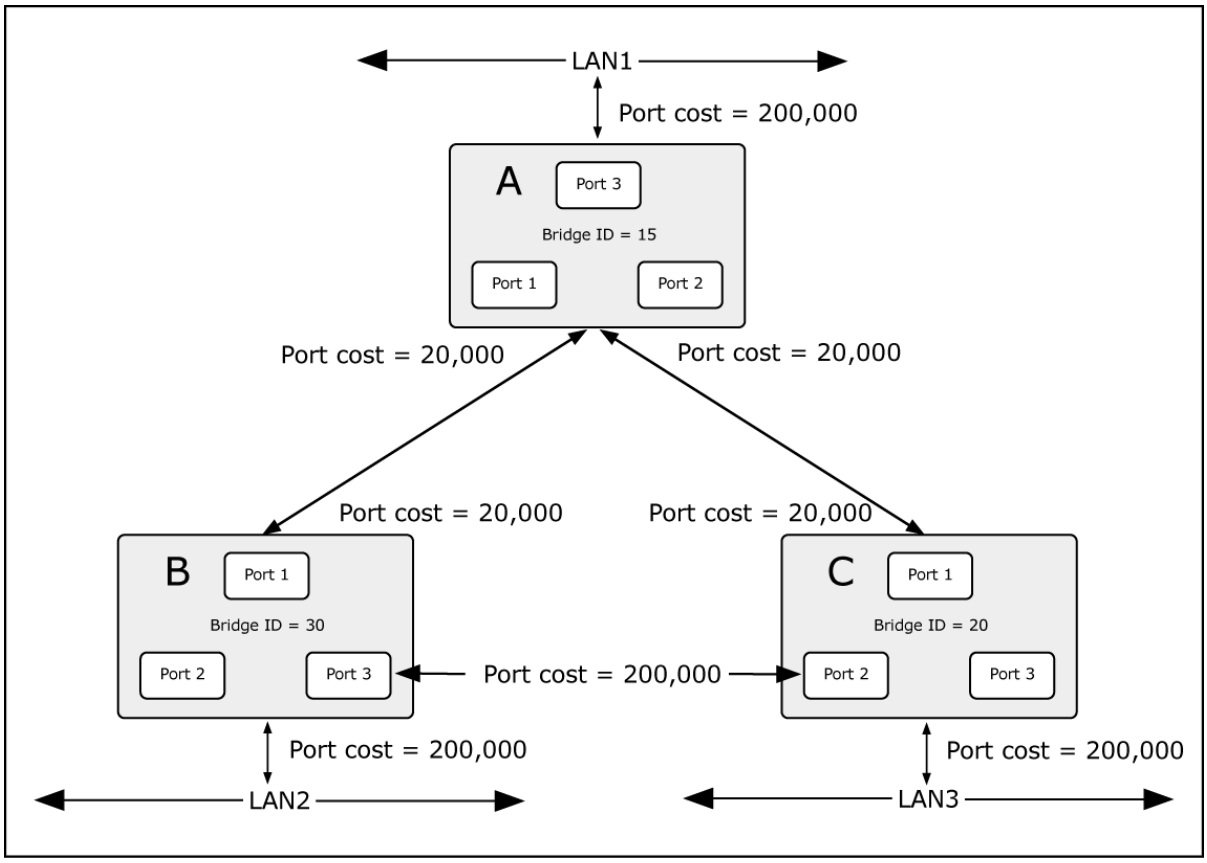


Figure 4-9-2: Before Applying the STA Rules

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

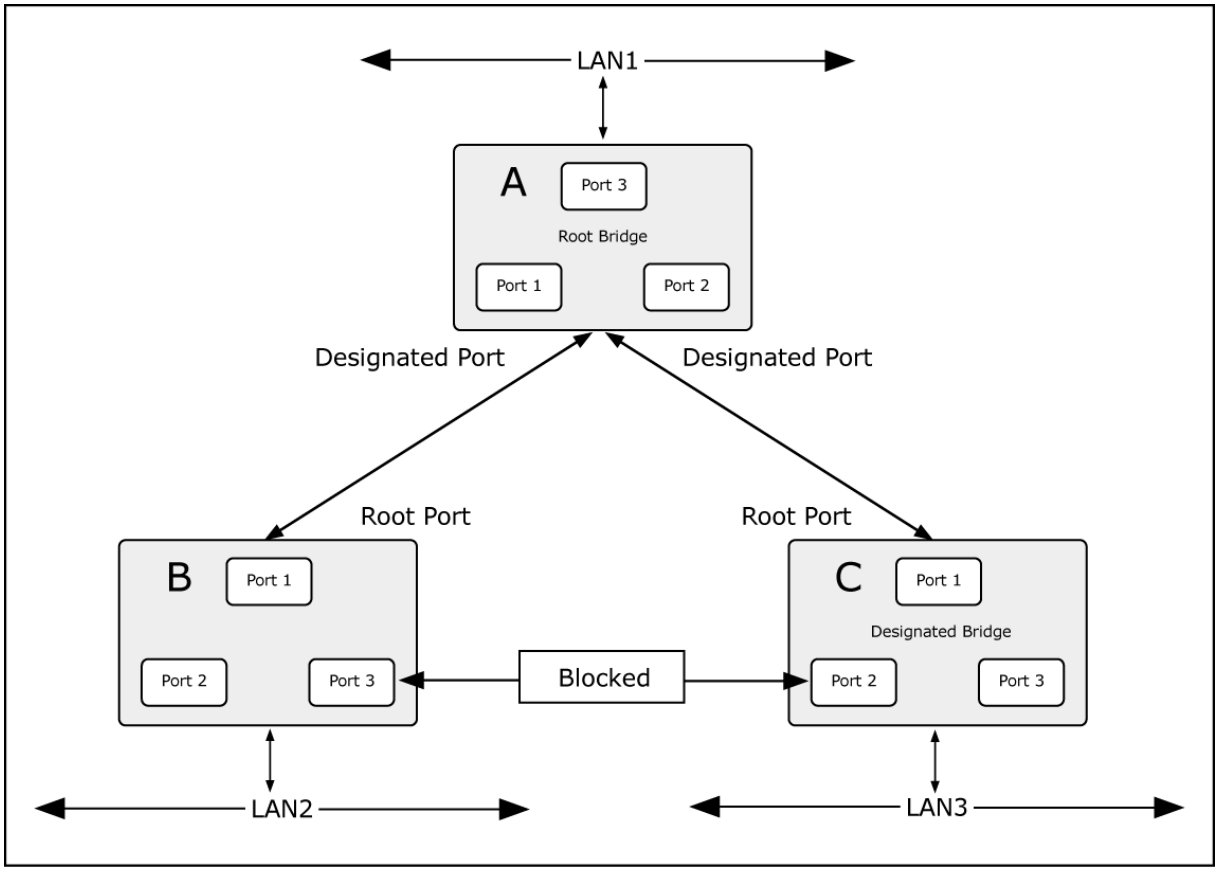


Figure 4-9-3: After Applying the STA Rules

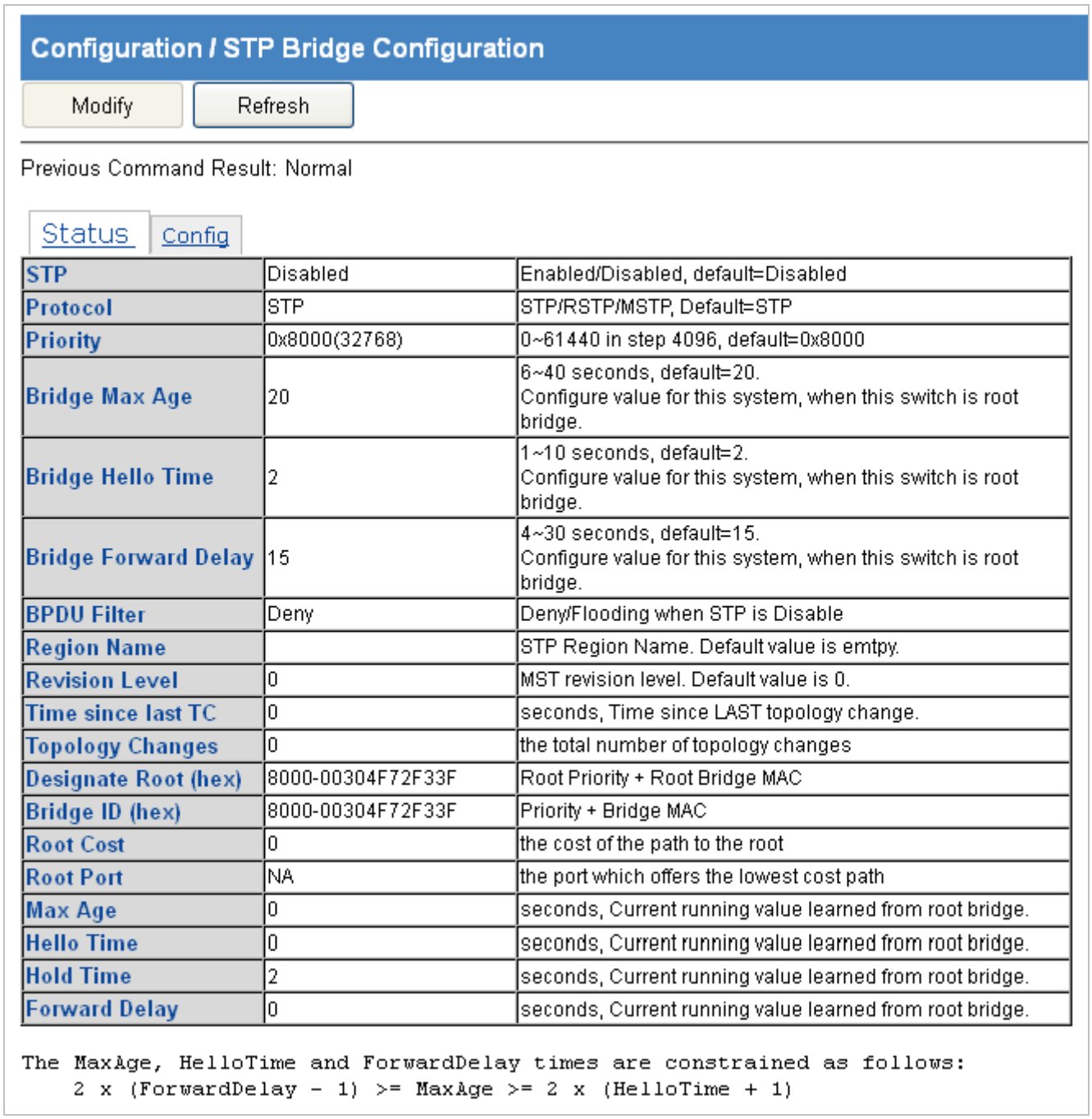
The switch with the lowest Bridge ID (switch C) was elected the root bridge, and the ports were selected to give a high port cost between switches B and C. The two (optional) Gigabit ports (default port cost = 20,000) on switch A are connected to one (optional) Gigabit port on both switch B and C. The redundant link between switch B and C is deliberately chosen as a 100 Mbps Fast Ethernet link (default port cost = 200,000). Gigabit ports could be used, but the port cost should be increased from the default to ensure that the link between switch B and switch C is the blocked link.

4.9.2 STP Bridge Configuration

This page allows you to configure STP system settings. The settings are used by all STP Bridge instances in the Switch or Switch Stack. The Industrial Managed Switch support the following Spanning Tree protocols:

- **Compatibility -- Spanning Tree Protocol (STP):** Provides a single path between end stations, avoiding and eliminating loops.
- **Normalcy -- Rapid Spanning Tree Protocol (RSTP):** Detects and uses network topologies that provide faster spanning tree convergence, without creating forwarding loops.
- **Extension – Multiple Spanning Tree Protocol (MSTP):** Defines an extension to RSTP to further develop the usefulness of virtual LANs (VLANs). This "Per-VLAN" Multiple Spanning Tree Protocol configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each Spanning Tree.

The screens in Figure 4-9-4 and Figure 4-9-5 appear.



Configuration / STP Bridge Configuration

Modify | Refresh

Previous Command Result: Normal

Status | Config

STP	Disabled	Enabled/Disabled, default=Disabled
Protocol	STP	STP/RSTP/MSTP, Default=STP
Priority	0x8000(32768)	0~61440 in step 4096, default=0x8000
Bridge Max Age	20	6~40 seconds, default=20. Configure value for this system, when this switch is root bridge.
Bridge Hello Time	2	1~10 seconds, default=2. Configure value for this system, when this switch is root bridge.
Bridge Forward Delay	15	4~30 seconds, default=15. Configure value for this system, when this switch is root bridge.
BPDU Filter	Deny	Deny/Flooding when STP is Disable
Region Name		STP Region Name. Default value is emtpy.
Revision Level	0	MST revision level. Default value is 0.
Time since last TC	0	seconds, Time since LAST topology change.
Topology Changes	0	the total number of topology changes
Designate Root (hex)	8000-00304F72F33F	Root Priority + Root Bridge MAC
Bridge ID (hex)	8000-00304F72F33F	Priority + Bridge MAC
Root Cost	0	the cost of the path to the root
Root Port	NA	the port which offers the lowest cost path
Max Age	0	seconds, Current running value learned from root bridge.
Hello Time	0	seconds, Current running value learned from root bridge.
Hold Time	2	seconds, Current running value learned from root bridge.
Forward Delay	0	seconds, Current running value learned from root bridge.

The MaxAge, HelloTime and ForwardDelay times are constrained as follows:
2 x (ForwardDelay - 1) >= MaxAge >= 2 x (HelloTime + 1)

Figure 4-9-4: Configuration / STP Bridge Configuration Page Screenshot

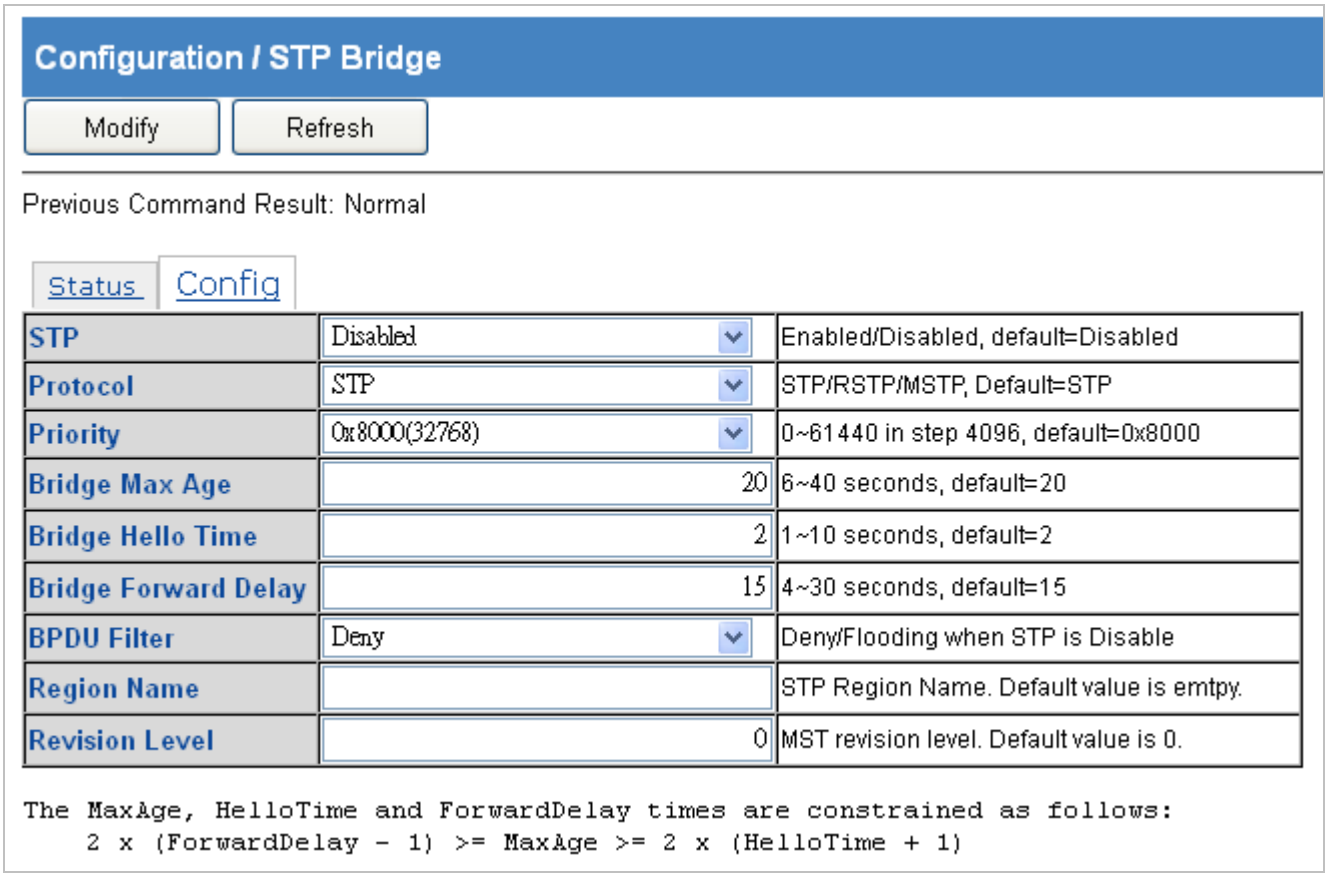


Figure 4-9-5: Configuration / STP Bridge Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Select "**Config**" page. Modify the configuration. Clicks the **Modify** button to apply change. **Refresh:** Click the **Refresh** button to get current data.

The page includes the following fields:

Object	Description
• **STP**	Specify whether or not the system is to implement the Spanning Tree Protocol. Range: Enabled/Disabled, default=Disabled.
• **Protocol**	RSTP (IEEE 802.1W), STP (IEEE 802.1D) Option: STP/RSTP, Default=STP.
• **Priority**	Sets the spanning tree protocol priority. The lower the priority number, the more significant the bridge becomes in protocol terms. Where two bridges have the same priority, their MAC address is compared and the smaller MAC address is treated as the most significant. Range: 0~61440 in step 4096, Default is default=0x8000(32768).
• **Bridge MaxAge**	Sets the maximum age of received spanning tree protocol information before it is discarded. This is used when the bridge is or is attempting to become the root bridge. Range: 6~40 seconds, Default=20 seconds.
• **Bridge Hello Time**	Sets the time after which the spanning tree process sends notification of topology changes to the root bridge. This is used when the bridge is or is attempting to become the root bridge. Range: 1~10 seconds, Default=2 seconds.
• **Bridge Forward Delay**	Sets the time that the bridge spends in listening or learning states when the bridge is or is attempting to become the root bridge. Range: 4~30 seconds, Default=15 seconds. The maxage, hellotime and forwarddelay times are constrained as follows: 2 x (forwarddelay - 1) >= maxage maxage >= 2 x (hellotime + 1) For example, the default settings are: 2 x (15 - 1) >= 20 20 >= 2 x (2 + 1)
• **BPDU Filter**	Deny/Flooding when STP is Disable.

4.9.3 CIST Ports Configuraiton

This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well.

The screens in Figure 4-9-6 and Figure 4-9-7 appear.

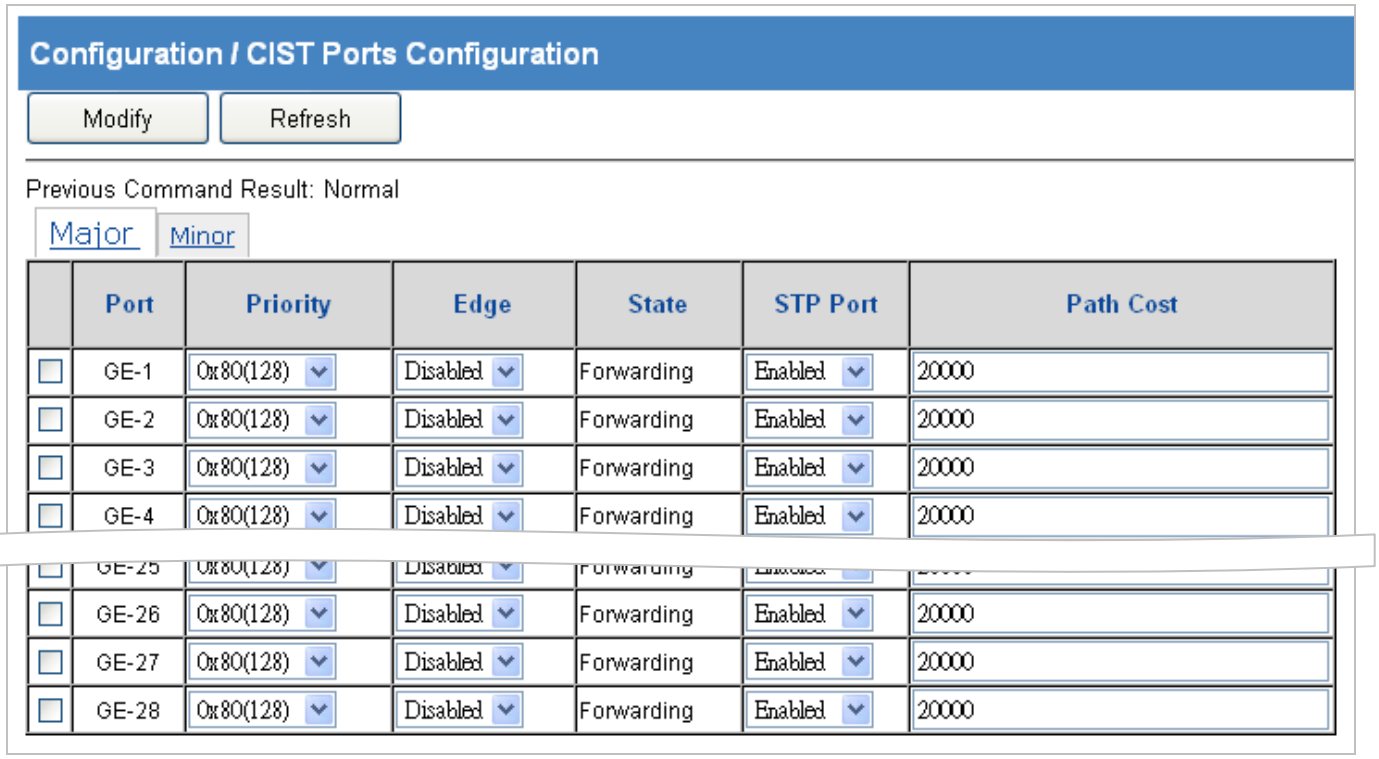


Figure 4-9-6: Configuration / CIST Port Configuration Page Screenshot

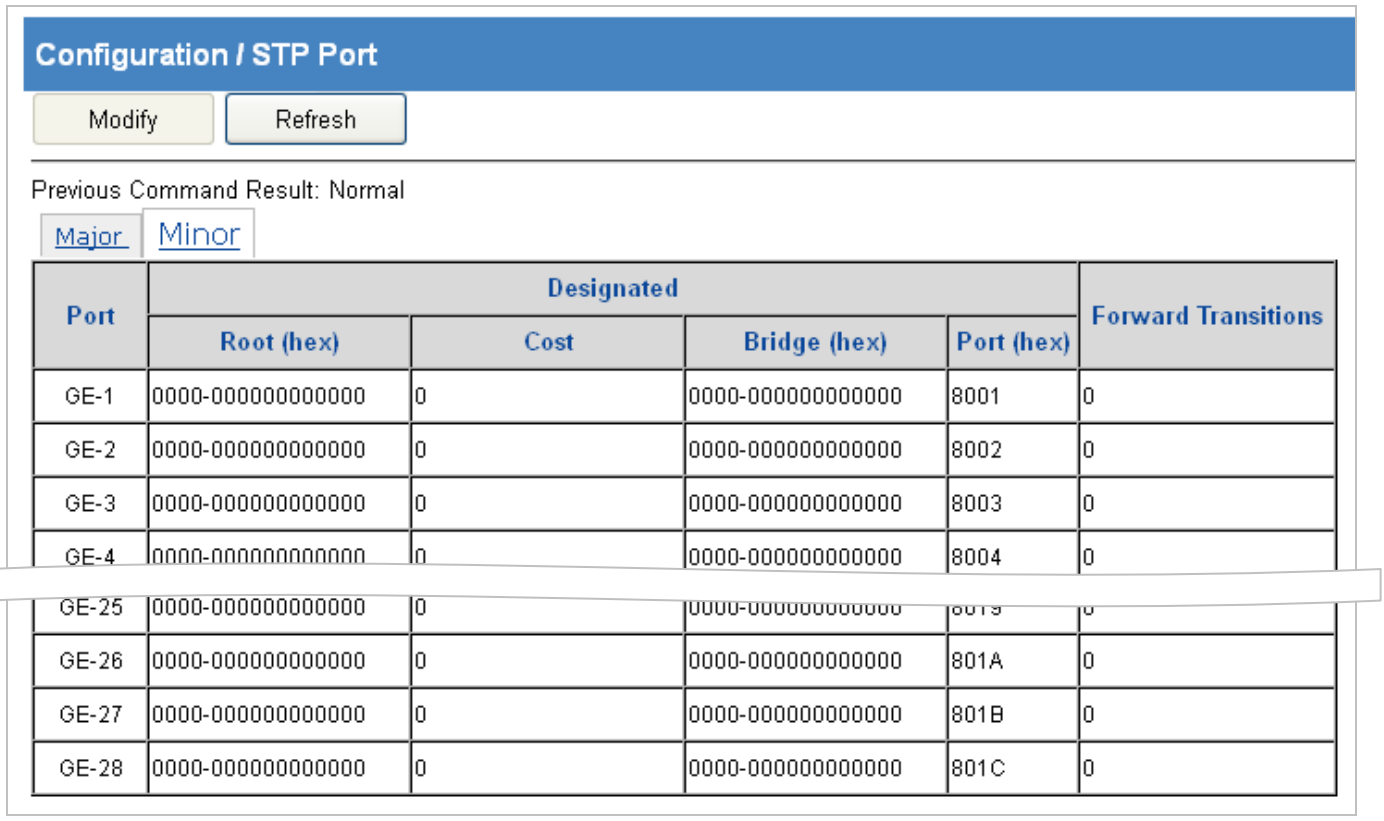


Figure 4-9-7: Configuration / STP Port Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Select "Major" page Select row(s) to be changed by checking up checkbox Modify the configuration Click the **Modify** button to apply change. **Refresh:** Click the **Refresh** button to get current data.

The page includes the following fields:

Object	Description
• **Port**	Range: GE-1 ~ 28 of Port
• **Priority**	Range: 0~240 in step 16, Default is default=0x80(128). Default is default=0x80(128).
• **Edge**	Range: Enabled/Disabled, default=Disabled.
• **State** •	■ **Range**: Disabled/ Blocking/ Listening/ Learning/ Forwarding/ Broken ■ **Disabled** : For ports which are disabled (see dot1dStpPortEnable), this object will have a value of disabled. ■ **Blocking**: The port will go into a blocking state at the time of selection process, when a switch receives a BPDU on a port that indicates a better path to the root switch, and if a port is not a root port or a designated port. ■ **Listening**: After blocking state, a root port or a designated port will move to a listening state. All other ports will remain in a blocked state. During the listening state the port discards frames received from the attached network segment and it also discards frames switched from another port for forwarding. At this state, the port receives BPDUs from the network segment and directs them to the switch system module for processing. After a forward time delay (The default forward delay time is 15 seconds.), the switch port moves from the listening state to the learning state. ■ **Learning**: A port changes to learning state after listening state. During the learning state, the port is listening for and processing BPDUs. In the listening state, the port begins to process user frames and start updating the MAC address table. But the user frames are not forwarded to the destination. After a forward time delay (The default forward delay time is 15 seconds), the switch port moves from the learning state to the forwarding state.

•	■ **Forwarding**: A port in the forwarding state forwards frames across the attached network segment. In a forwarding state, the port will process BPDUs, update its MAC Address table with frames that it receives, and forward user traffic through the port. Forwarding State is the normal state. Data and configuration messages are passed through the port, when it is in forwarding state. ■ **Broken**: If the bridge has detected a port that is malfunctioning it will place that port into the broken state.
• **STP Port**	Range: Enabled/ Disabled, Default is Enabled.
• **Path Cost**	Range: 1 ~ 200000000, Default is 20000.
• **Designated Root**	The parameter is the unique Bridge Identifier of the Bridge recorded as the Root in the Configuration BPDUs transmitted by the Designated Bridge for the segment to which the port is attached. Format : Root bridge priority + Root Bridge MAC address
• **Designated Cost**	The parameter is the path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received BPDUs.
• **Designated Bridge**	The parameter is the Bridge Identifier of the bridge which this port considers to be the Designated Bridge for this port's segment. Format: Designated bridge priority + Designated Bridge MAC address. [0x8000-001122334455]
• **Designated Port**	The parameter (dot1dStpPortDesignatedPort) is the Port Identifier of the port of the Designated Bridge for this port's segment. Format: Designated port priority + Designated Port ID. [0x8001]
• **Forward Transitions**	Forward Transitions count.
• **MAC Address**	MAC address for the VLAN interface. Read only.

4.9.4 MSTI Configuration

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well. The screen in Figure 4-9-8 appears.

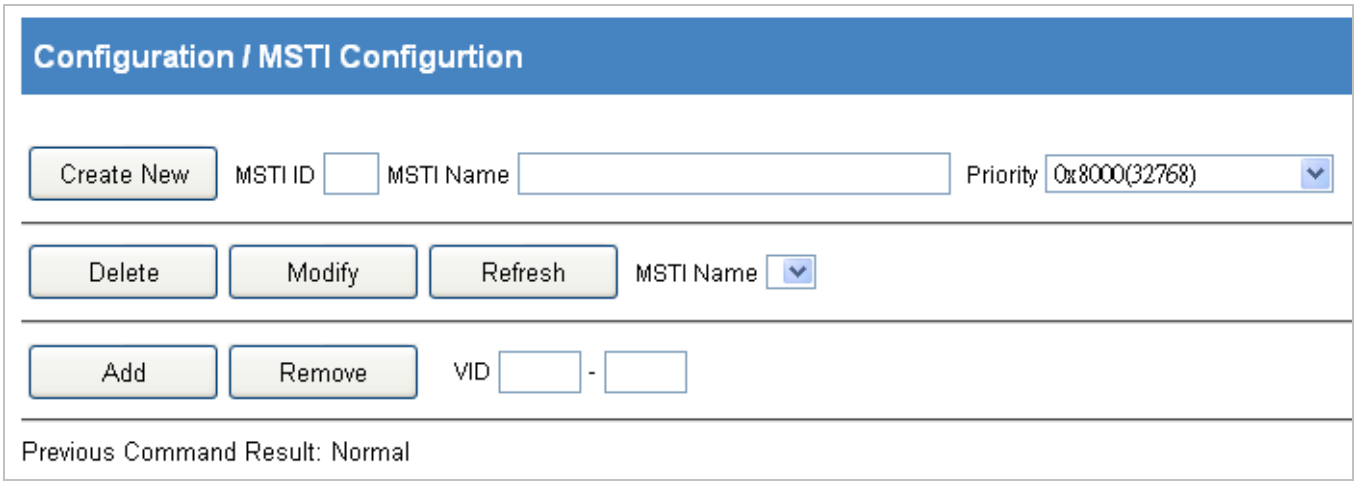


Figure 4-9-8: Configuration / MSTI Configuration Page Screenshot

Object	Description
• **Operation**	**Create New:** Fill out "MSTI Name" and select "Priority" fields. (Default MSTI Name will be set when name is not input.) Click the **Create New** button to create new data. Max MSTI number is 10. **Delete:** Select "MSTI Name". Click the **Delete** button to the Instance. **Modify:** Select "MSTI Name" from list. Modify "MSTI Name", "VID" or select "Priority". Click the **Modify** button. **Add or Remove VID:** Fill start VID and end VID. Click the **Add** or **Remove** button to edit VID range. Or input the VID range with the format in the VID cell.

The page includes the following fields:

Object	Description
• **ID**	MSTI ID, value range is 1~10.
• **MSTI Name**	MSTI Name, 1~30 characters. Can not be empty, if empty, system will give default name.
• **VID Start**	VLAN ID, Range 1-4094.
• **VID End**	VLAN ID, Range 1-4094.
• **VID**	VLAN ID, Format: 2-5,7,100-4094. Accept number, space, dash and comma.
• **Priority**	MSTI's priority. The lower the priority number, the more significant the bridge becomes in protocol terms. Where two bridges have the same priority, their MAC address is compared and the smaller MAC address is treated as the most significant. Range: 0~61440 in step 4096, Default is default=0x8000(32768).
• **Designated Root**	The parameter is the unique Bridge Identifier of the Bridge recorded as the Root in the Configuration BPDUs transmitted by the Designated Bridge for the segment to which the port is attached. Format: MSTI's Root bridge priority + Root Bridge MAC address
• **Bridge ID**	The parameter is the Bridge Identifier of the bridge which this port considers to be the Designated Bridge for this port's segment. Format: MSTI's priority + Bridge MAC address. [0x8000-001122334455]
• **Root Cost**	The parameter is the path cost of the MSTI's Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received BPDUs.
• **Root Port**	The parameter is the MSTI's Port Identifier of the port of the Designated Bridge for this port's segment. [0x8001]

4.9.5 MSTI Port Configuration

This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well. A MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured and applicable for the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.
The screen in Figure 4-9-9 appears.

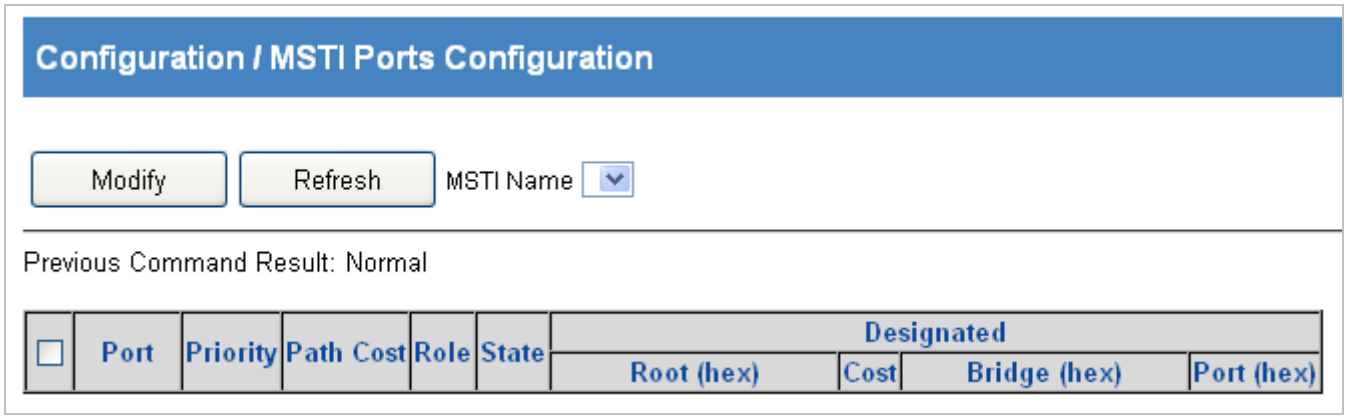


Figure 4-9-9: Configuration / VLAN Interface Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Select a row item to selected Set or select the following fields. Click the **Modify** button.

The page includes the following fields:

Object	Description
• **Port**	Range: GE-1 ~ 28 of Port
• **Priority**	Range: 0~240 in step 16, Default is default=0x80(128).
• **Path Cost**	Range: 1 ~ 200000000, Default is 20000.
• **Role**	Range: Disabled/ Root/ Designated/ Alternate/ Backup/ Master/ Unknown.
• **State**	■ **Range**: Disabled/ Blocking/ Listening/ Learning/ Forwarding/ Broken ■ **Disabled**: For ports which are disabled (see dot1dStpPortEnable), this object will have a value of disabled. ■ **Blocking**: The port will go into a blocking state at the time of selection process, when a switch receives a BPDU on a port that indicates a better path to the root switch, and if a port is not a root port or a designated port. ■ **Listening**: After blocking state, a root port or a designated port will move to a listening state. All other ports will remain in a blocked state. During the listening state the port discards frames received from the attached network segment and it also discards frames switched from another port for forwarding. At this state, the port receives BPDUs from the network segment and directs them to the switch system module for processing. After a forward time delay (The default forward delay time is 15 seconds.), the switch port moves from the listening state to the learning state.

•	■ **Learning**: A port changes to learning state after listening state. During the learning state, the port is listening for and processing BPDUs. In the listening state, the port begins to process user frames and start updating the MAC address table. But the user frames are not forwarded to the destination. After a forward time delay (The default forward delay time is 15 seconds), the switch port moves from the learning state to the forwarding state. ■ **Forwarding**: A port in the forwarding state forwards frames across the attached network segment. In a forwarding state, the port will process BPDUs, update its MAC Address table with frames that it receives, and forward user traffic through the port. Forwarding State is the normal state. Data and configuration messages are passed through the port, when it is in forwarding state. ■ **Broken**: If the bridge has detected a port that is malfunctioning it will place that port into the broken state.
• **Designated Root**	The parameter is the unique Bridge Identifier of the Bridge recorded as the Root in the Configuration BPDUs transmitted by the Designated Bridge for the segment to which the port is attached. Format : Root bridge priority + Root Bridge MAC address
• **Designated Cost**	The parameter is the path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received BPDUs.
• **Designated Bridge**	The parameter is the Bridge Identifier of the bridge which this port considers to be the Designated Bridge for this port's segment. Format: Designated bridge priority + Designated Bridge MAC address. [0x8000-001122334455]
• **Designated Port**	The parameter (dot1dStpPortDesignatedPort) is the Port Identifier of the port of the Designated Bridge for this port's segment. Format: Designated port priority + Designated Port ID. [0x8001]

4.10 Policer

The Two Rate Three Color Marker (trTCM) takes the following four traffic parameters:

- Committed Information Rate (CIR)
- Peak Information Rate (PIR)
- Committed Burst Size (CBS)
- Peak Burst Size (PBS)

It marks packets as either Green, Yellow, or Red Random Early Detection; Quality of Service (QoS) queue management protocol., based on these values. The number of bytes available for CBS packet bursts grows at the CIR, and the number of bytes available for PBS packet bursts grows at the PIR.

It operates in one of the following modes:

- **Color-Aware Mode:** Here, packets may have been previously colored. This color, as well as how the flow fits within the CBS and PBS, affects how the trTCM will mark the packet. In Color-Aware mode, packets that have been precolored Green and arrive within the CBS remain Green. The number of bytes available for both CBS and PBS packet bursts decreases by the size of the Green packet. Packets that have been precolored Green or Yellow and arrive between the CBS and PBS are marked Yellow, and the number of bytes available for PBS packet bursts decreases by the size of the Yellow packet. Packets that have been precolored Red remain Red. Packets exceeding the EBS are marked Red, regardless of precoloring.

- **Color-Blind Mode:** In Color-Blind mode, all packets are treated as if they were uncolored. In Color-Blind mode, packets that arrive within the CBS are marked Green, and the number of bytes available for both CBS and PBS packet bursts decreases by the size of the Green packet. Packets between the CBS and the PBS are marked Yellow, and the number of bytes available for PBS packet bursts decreases by the size of the Yellow packet. Packets exceeding the PBS are marked Red.

4.10.1 Policer Ingress Color

The policer ingress color includes the color aware mode and color. The screen in Figure 4-10-1 appears.

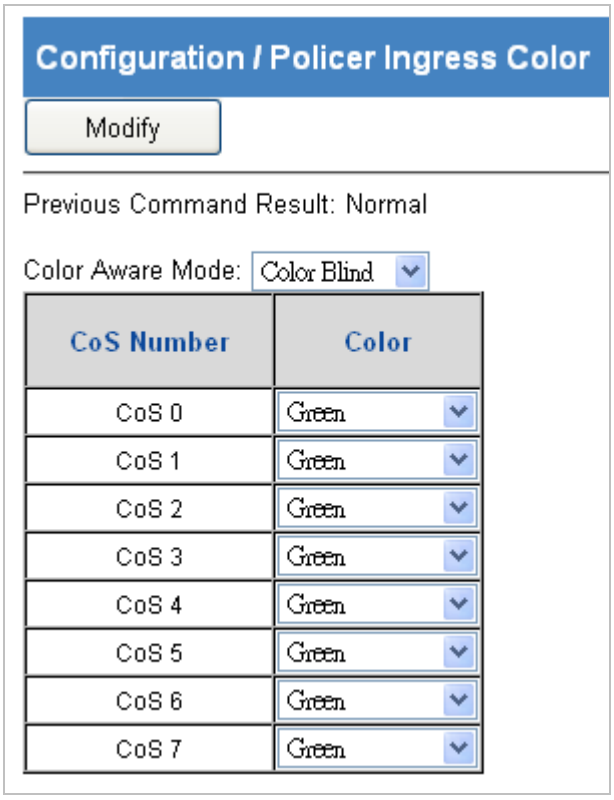


Figure 4-10-1: Configuration / Policer Ingress Color Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Select "Color Blind" or "Color Aware" Modify the configuration Click the **Modify** button to apply change

The Page includes the following fields:

Object	Description
• **Color Aware Mode**	Color Blind/ Color Aware. Default is Color Blind.
• **CoS 0**	Green/Yellow/Red, default is green

4.10.2 Policer Color Marking

This page allows you to configure the policer color marking to CoS and DSCP. The screen in Figure 4-10-2 appears.

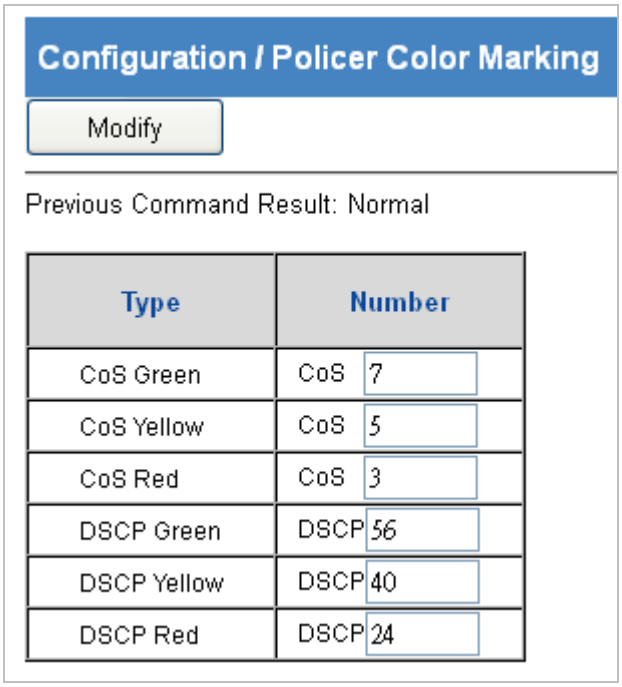


Figure 4-10-2: Configuration / Policer Color Marking Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Modify the configuration Click the **Modify** button to apply change

The page includes the following fields:

Object	Description
• **Color Aware Mode**	Color Blind/ Color Aware. Default is Color Blind.
• **CoS Green**	Range: 0~7, Default is 7
• **CoS Yellow**	Range: 0~7, Default is 5
• **CoS Red**	Range: 0~7, Default is 3
• **DSCP Green**	Range: 0~63, Default is 56
• **DSCP Yellow**	Range: 0~63, Default is 40
• **DSCP Red**	Range: 0~63, Default is 24

4.10.3 Ingress Policer

This page allows you to configure the Policer settings. The screen in Figure 4-10-3 appears.

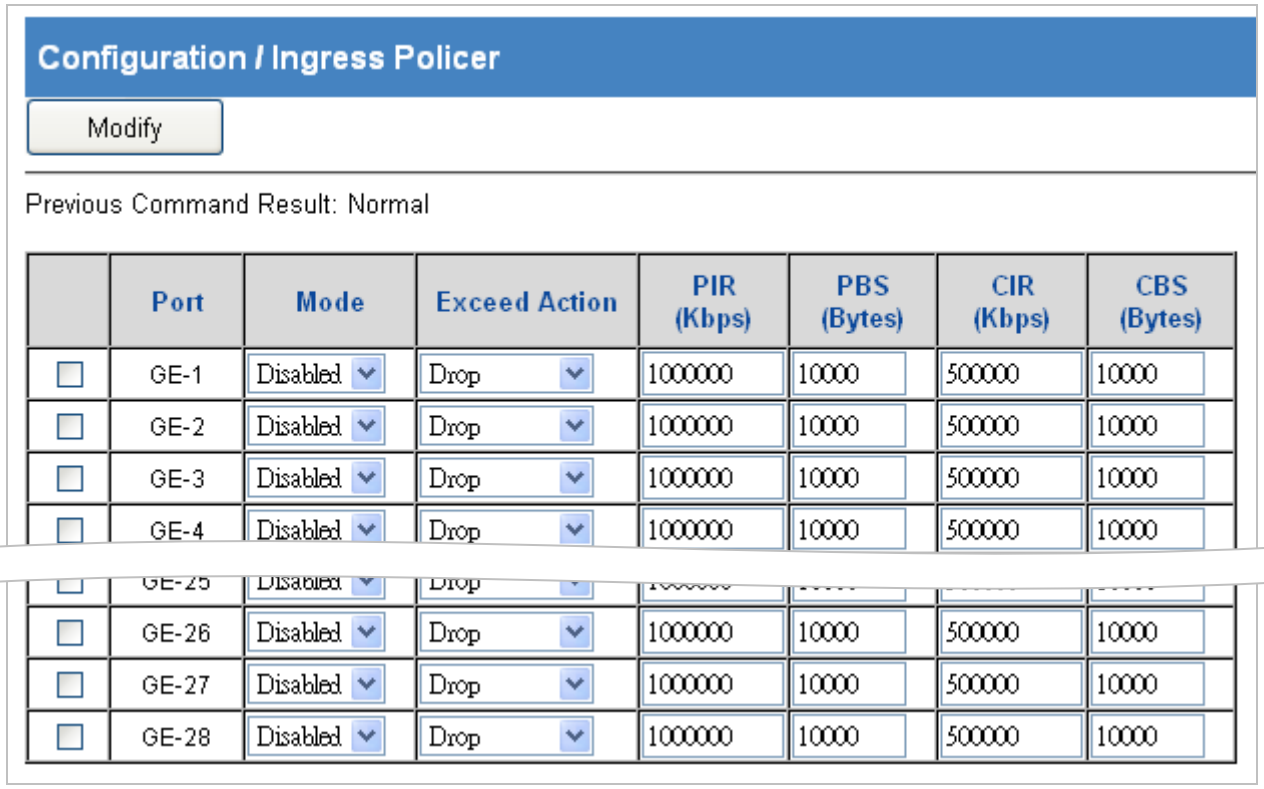


Figure 4-10-3: Configuration / VLAN Interface Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Modify the configuration Click the **Modify** button to apply change

The page includes the following fields:

Object	Description
• **Port**	Bridge port number. GE-1 ~ 28 of Port.
• **Mode**	Ingress Policer Mode Enabled/Disabled, default is Disabled.
• **Exceed Action**	Value range is Drop/CoS Mark/DSCP Mark, default is Drop.
• **PIR (Kbps)**	Value range is 1~1000000 Kbps, default is 1000000 Kbps.
• **PBS (Bytes)**	Value range is 1~65535 Bytes, default is 10000 Bytes.
• **CIR (Kbps)**	Value range is 1~1000000 Kbps, default is 500000 Kbps.
• **CBS (Bytes)**	Value range is 1~65535 Kbps, default is 10000 Kbps.

4.11 ACL

ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.
Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

4.11.1 Profile

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is **20** on each switch. The screen in Figure 4-11-1 appears.

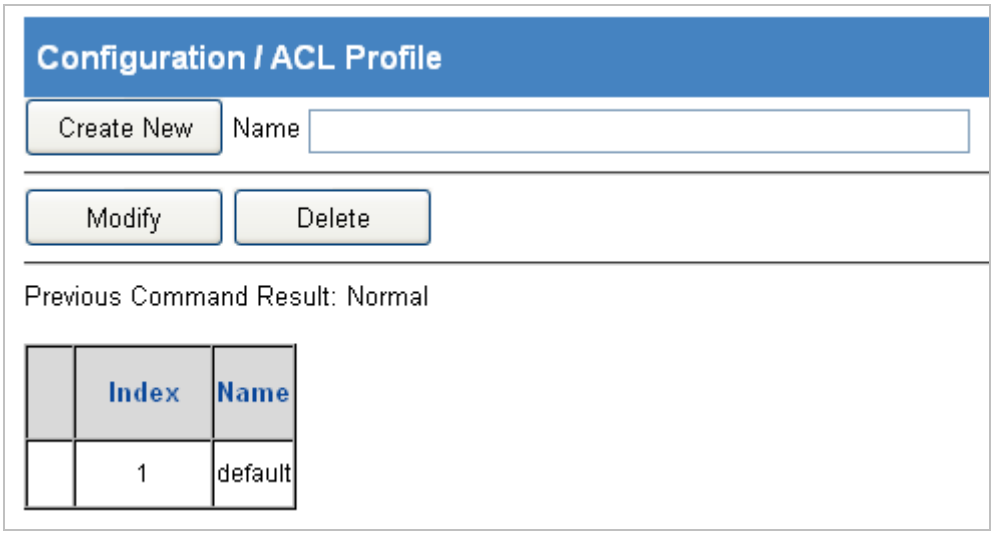


Figure 4-11-1: Configuration / VLAN Interface Configuration Page Screenshot

Object	Description
• **Operation**	**Create New:** Fill ACL Profile Name, the max length is 31. Click the **Create New** button to Create New ACL profile. **Modify:** Select checkbox of profile to be changed. Modify the "Name" of profile Click the **Modify** button to apply change **Delete:** Select one row for delete Click the **Delete** button to delete data

The page includes the following fields:

Object	Description
• **Index**	ACL Profile Index, range is 1 ~ 20 of profile, Profile 1 is a default profile, can not be modified
• **Name**	ACL Profile Name, the max length 31 characters.

4.11.2 Entry

This page shows the ACL status by different ACL users. The screens in Figure 4-11-2 and Figure 4-11-3 appear.

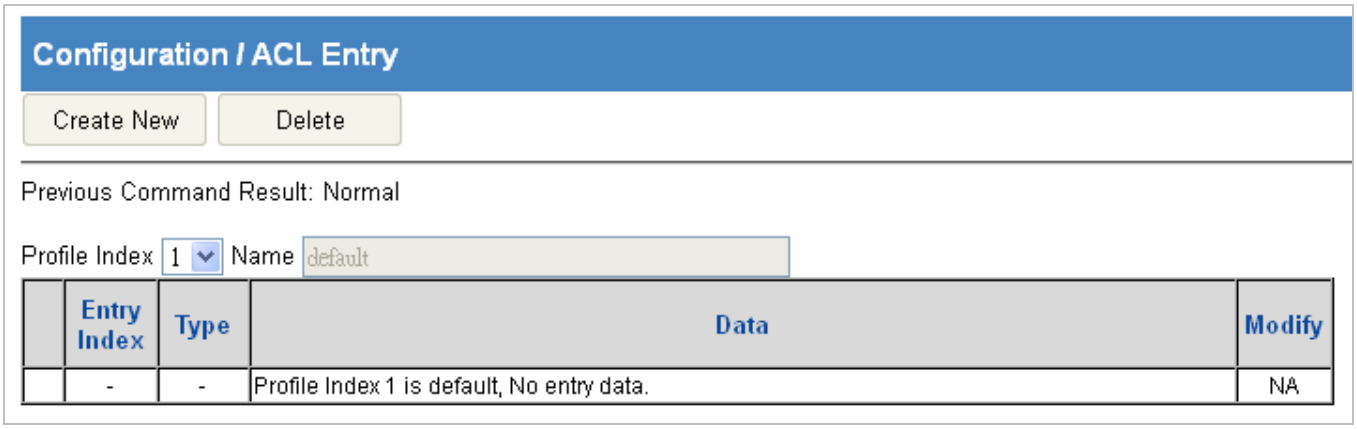


Figure 4-11-2: Configuration / ACL Entry Configuration Page Screenshot

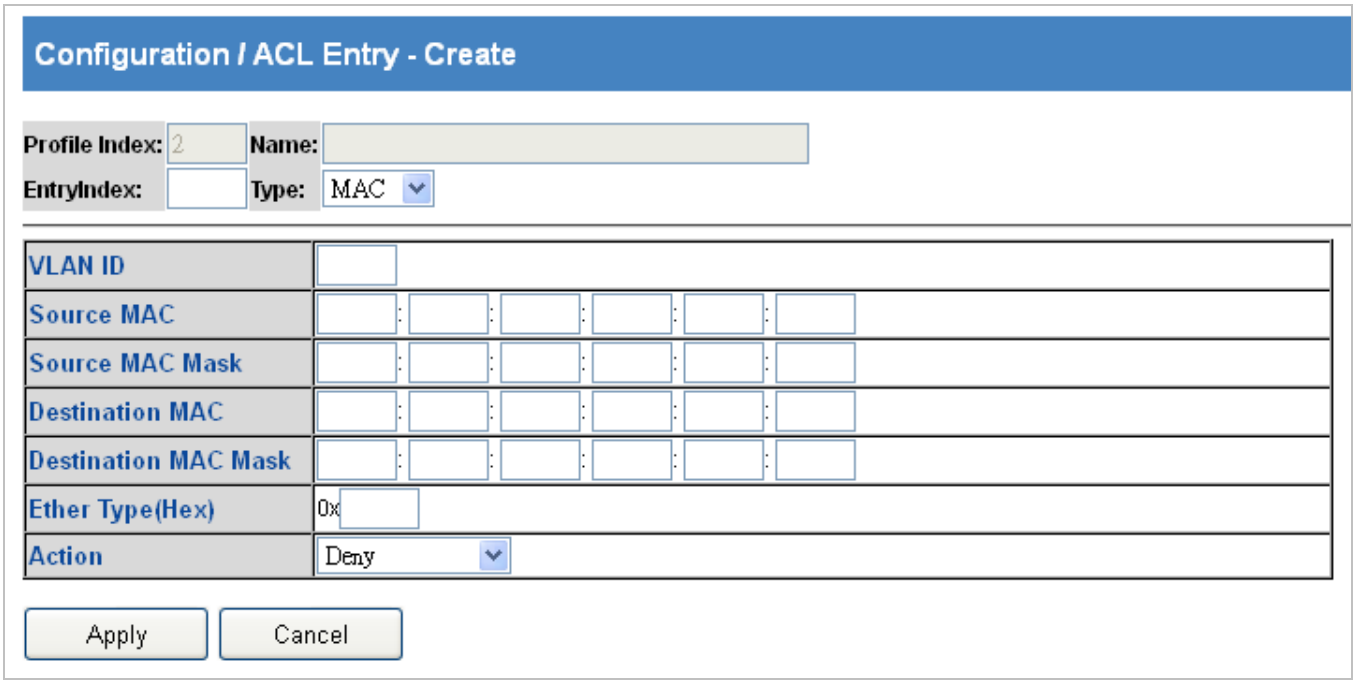


Figure 4-11-3: Configuration / ACL Entry - Create Configuration Page Screenshot

Object	Description
• **Operation**	**Create New:** Click "Create New" button to open page of Create New entry. Fill ACL Entry Index field and select Type. Fill fields and then click "Apply" to create or click "Cancel" to cancel. **Modify:** Modify field data. Click the **Modify** button to open modification page. Fill Entry Index field and select Type. Fill fields and then click "Apply" to modify or click "Cancel" to cancel. **Delete:** Select one row. Click the **Delete** button to delete data.

The page includes the following fields:

Object	Description
• **Profile Index**	Range: 1~20
• **Entry Index**	Range: 1~32
• **Type**	MAC/IPV4/L4PORT/TOS
• **VLAN ID**	ACL Profile VLAN ID, value range is 1~4094.
• **Source MAC**	ACL Profile Source MAC format XX:XX:XX:XX:XX:XX, each field value range 0~FF
• **Source MAC Mask**	ACL Profile Source MAC Mask format XX:XX:XX:XX:XX:XX, each field value range 0~FF
• **Destination MAC**	ACL Profile Destination MAC format XX:XX:XX:XX:XX:XX, each field value range 0~FF
• **Destination MAC Mask**	ACL Profile Destination MAC Mask format XX:XX:XX:XX:XX:XX, each field value range 0~FF
• **Ether Type (Hex)**	Value range 0,05DD~FFFF,format XXXX
• **Action**	Value range Deny/Permit/Queue Mapping/CoS Marking/Copy Frame.
• **Source IP**	Format XXX:XXX:XXX:XXX, each field value range 0~255.
• **Source IP Mask**	Format XXX:XXX:XXX:XXX, each field value range 0~255.
• **Destination IP**	Format XXX:XXX:XXX:XXX, each field value range 0~255.
• **Destination IP Mask**	Format XXX:XXX:XXX:XXX, each field value range 0~255.
• **Protocol**	Value range 0~255.
• **Action**	Value range Deny/Permit/Queue Mapping/CoS Marking/Copy Frame.
• **Protocol**	Value range TCP/UDP.

• **Source IP**	Format XXX:XXX:XXX:XXX, each field value range 0~255.
• **Source IP Mask**	Format XXX:XXX:XXX:XXX, each field value range 0~255.
• **Port**	Source IP Port, value range 0~65535.
• **Destination IP**	Format XXX:XXX:XXX:XXX, each field value range 0~255.
• **Destination IP Mask**	Format XXX:XXX:XXX:XXX, each field value range 0~255.
• **Port**	Source IP Port, value range 0~65535.
• **Action**	Value range Deny/Permit/Queue Mapping/CoS Marking/Copy Frame.
• **Source IP**	Format XXX.XXX.XXX.XXX, each field value range 0~255.
• **Source IP Mask**	Format XXX.XXX.XXX.XXX, each field value range 0~255.
• **Destination IP**	Format XXX.XXX.XXX.XXX, each field value range 0~255.
• **Destination IP Mask**	Format XXX.XXX.XXX.XXX, each field value range 0~255.
• **ToS Type**	Value range Precedence/ToS/DSCP/Any,0~7 in Precedence,0~15 in ToS,0~63 in DSCP.
• **Action**	Value range Deny/Permit/Queue Mapping/CoS Marking/Copy Frame.

4.11.3 Binding

Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE. The screen in Figure 4-11-4 appears.

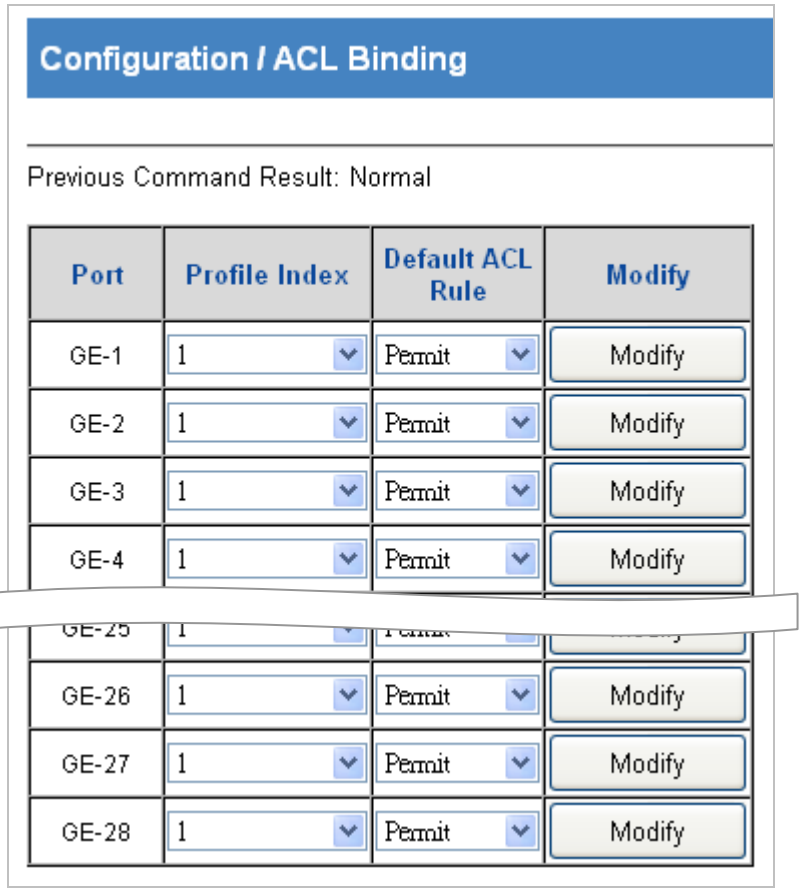


Figure 4-11-4: Configuration / ACL Binding Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Modify the configuration. Click the **Modify** button to apply change.

The page includes the following fields:

Object	Description
• **Port**	Giga Port, GE-1 ~ 28 of Port.
• **Profile Index**	ACL Profile Index, range is 1 ~ 20 of profile, default is 1.
• **Default ACL Rule**	ACL Default Rule, could be Permit/Deny, default is Permit.

4.11.4 Mirror Analyze Port

The VLAN Interface includes the IP Configuration and IP Interface. The configured column is used to view or change the IP configuration. The maximum number of interfaces supported is 5. The screen in Figure 4-11-5 appears.

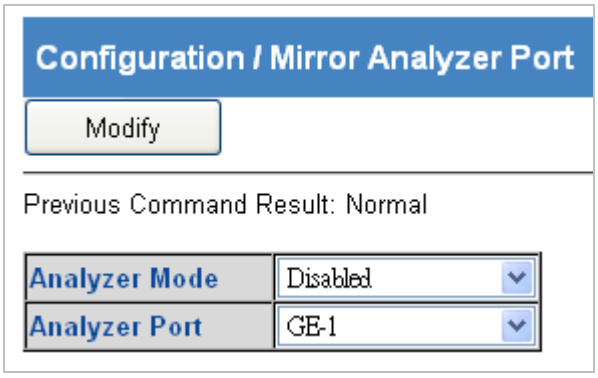


Figure 4-11-5: Configuration / Mirror Analyze Port Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Modify the configuration. Click the **Modify** button to apply change.

The page includes the following fields:

Object	Description
• **Analyzer Mode**	Enabled/Disabled, default is Disabled.
• **Analyzer Port**	Giga Port GE-1 ~ 28 of Port, default is GE-1.

4.12 Shaper

4.12.1 Port Shaping

The Port Shapers for a specific port are configured on this page. The screen in Figure 4-12-1 appears.

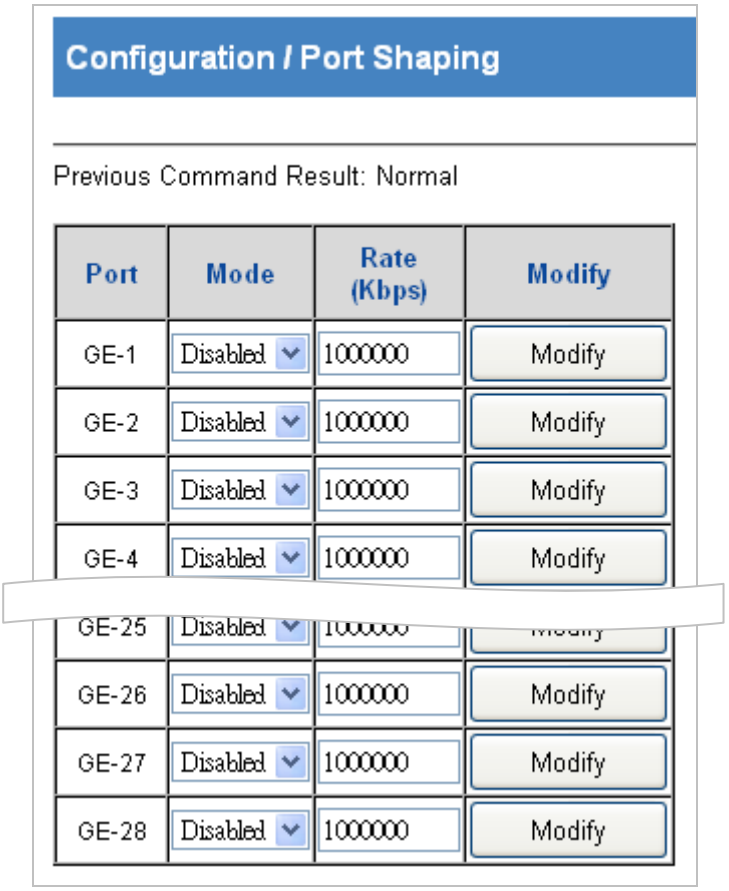


Figure 4-12-1: Configuration / Port Shaping Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Modify the configuration. Click the **Modify** button to apply change.

The page includes the following fields:

Object	Description
• **Port**	Bridge port, range is 1 ~ 28 of Port.
• **Mode**	Enabled/Disabled, default is Disabled.
• **Rate (Kbps)**	Rate range is 1~1000000 Kbps, default is 1000000 Kbps.

4.12.2 Queue

This page allows you to configure the per-queue rate for all switch ports. The screen in Figure 4-12-2 appears.

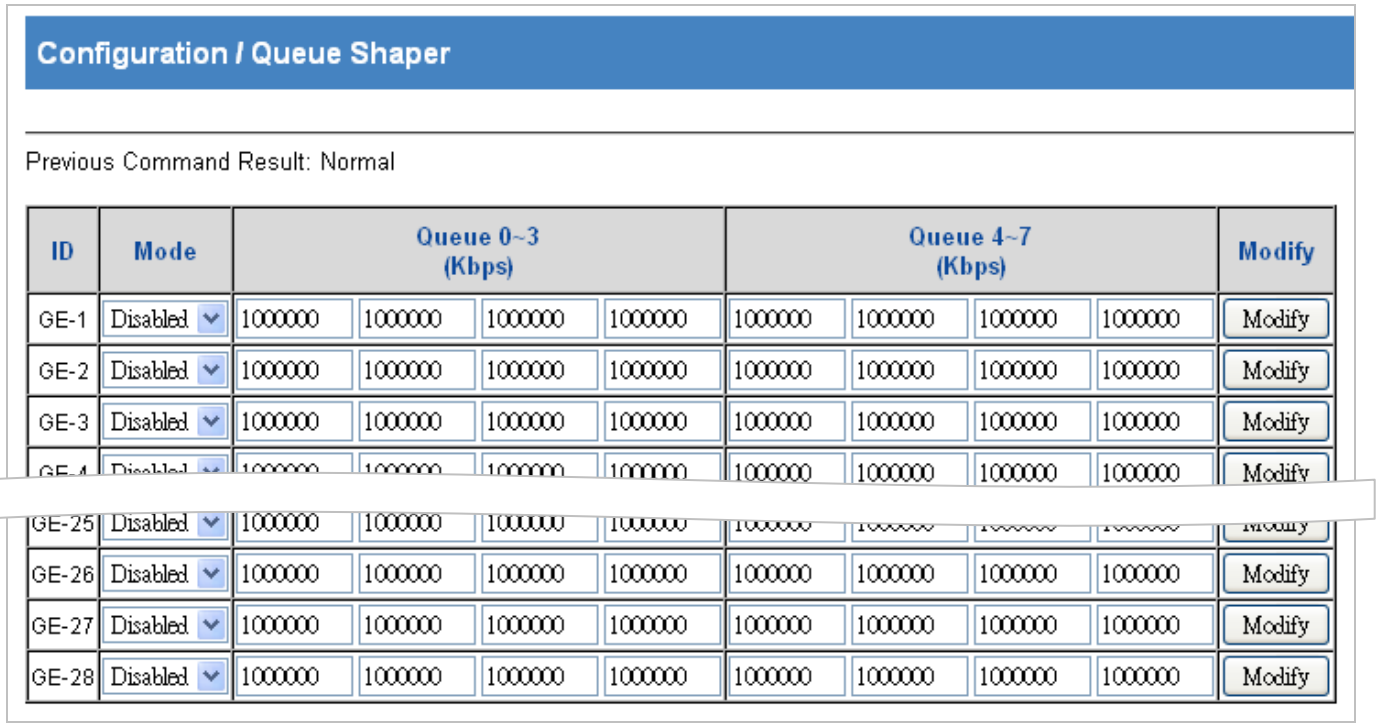


Figure 4-12-2: Configuration / Queue Sharper Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Modify the configuration. Click the **Modify** button to apply change.

The page includes the following fields:

Object	Description
• **ID**	Bridge port, range is 1 ~ 28 of Port.
• **Mode**	Option: Enabled/Disabled, default is Disabled.
• **Queue 0~3 (Rate)**	Queue 0~3, rate range is 1~1000000 Kbps, default is 1000000 Kbps.
• **Queue 4~7 (Rate)**	Queue 4~7, rate range is 1~1000000 Kbps, default is 1000000 Kbps.

4.13 Queue & Scheduler

4.13.1 CoS & Queue Mapping

This page allows you to map CoS value to a QoS Class. The screen in Figure 4-13-1 appears.

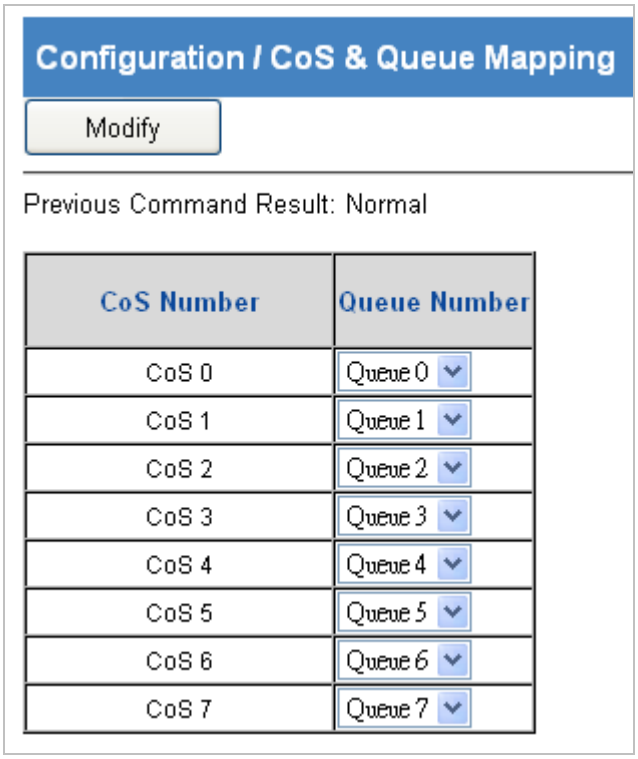


Figure 4-13-1: Configuration / CoS & Queue Mapping Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Modify the configuration. Click the **Modify** button to apply change.

The page includes the following fields:

Object	Description
• **CoS 0**	Queue 0~7, default is Queue 0.
• **CoS 1**	Queue 0~7, default is Queue 1.
• **CoS 2**	Queue 0~7, default is Queue 2.
• **CoS 3**	Queue 0~7, default is Queue 3.
• **CoS 4**	Queue 0~7, default is Queue 4.
• **CoS 5**	Queue 0~7, default is Queue 5.
• **CoS 6**	Queue 0~7, default is Queue 6.
• **CoS 7**	Queue 0~7, default is Queue 7.

4.13.2 Scheduling Profile

This page allows you to set schedule profile. The screen in Figure 4-13-2 appears.

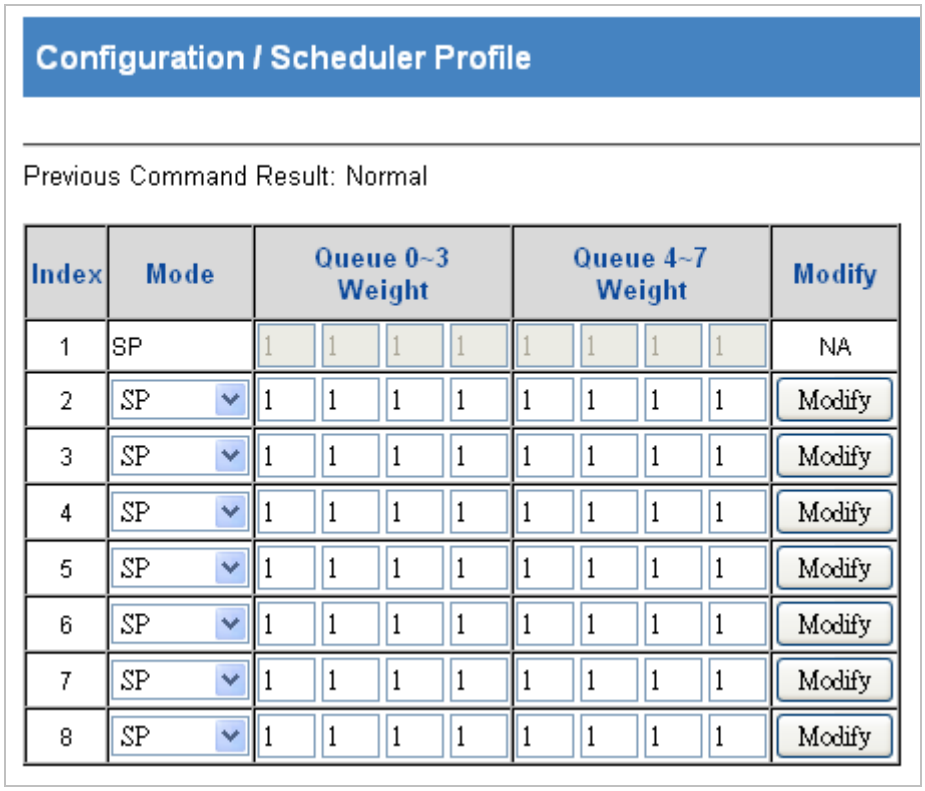


Figure 4-13-2: Configuration / Scheduler Profile Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Modify the configuration. Click "the **Modify** button to apply change.

The page includes the following fields:

Object	Description
• **Index**	Value range is 1~8.
• **Mode**	Option: SP/SPWRR/WRR, default is SP.
• **Queue 0~3 weight**	Queue 0~3 Weight, range is 1~255, default is 1.
• **Queue 4~7 weight**	Queue 4~7 Weight, range is 1~255, default is 1.

4.13.3 Binding

This page allows you to bind the Policy content to the appropriate schedule index. The screen in Figure 4-13-3 appears.

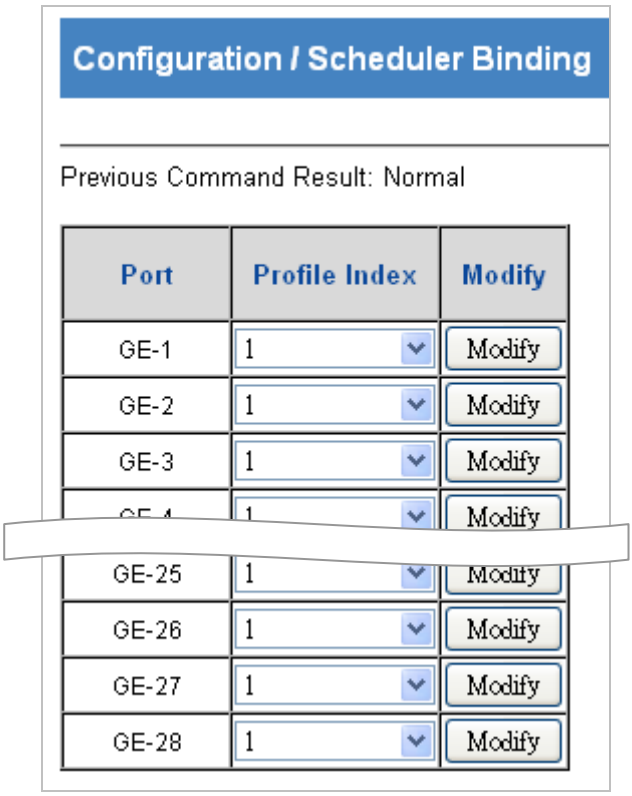


Figure 4-13-3: Configuration / Schedule Binding Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Modify the configuration. Click the **Modify** button to apply change.

The page includes the following fields:

Object	Description
• **Port**	Giga Port GE-1 ~ 28 of Port.
• **Profile Index**	Range is 1~8, default is 1.

4.14 Storm Control

4.14.1 Unknown Unicast Control

The configuration indicates the permitted packet rate for unknown unicast traffic across the switch. The screen in Figure 4-14-1 appears.

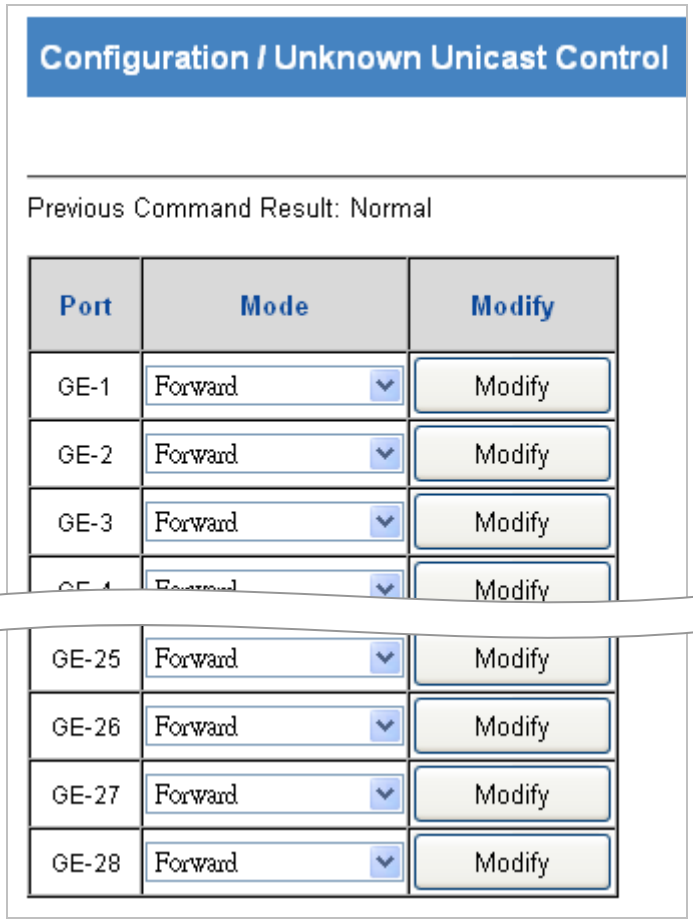


Figure 4-14-1: Configuration / Unknow Unicast Control Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Modify the configuration. Click the **Modify** button to apply change.

The page includes the following fields:

Object	Description
• **Port**	Giga Port GE-1 ~ 28 of Port.
• **Mode**	Forward -> Forward unknown unicast packet (default) Block -> Block unknown unicast packet Rate limit -> Control rate. Rate range is 1~1000000 Kbps, default is 1000000 Kbps.

4.14.2 Unknown Multicast Control

The configuration indicates the permitted packet rate for unknown multicast traffic across the switch. The screen in Figure 4-14-2 appears.

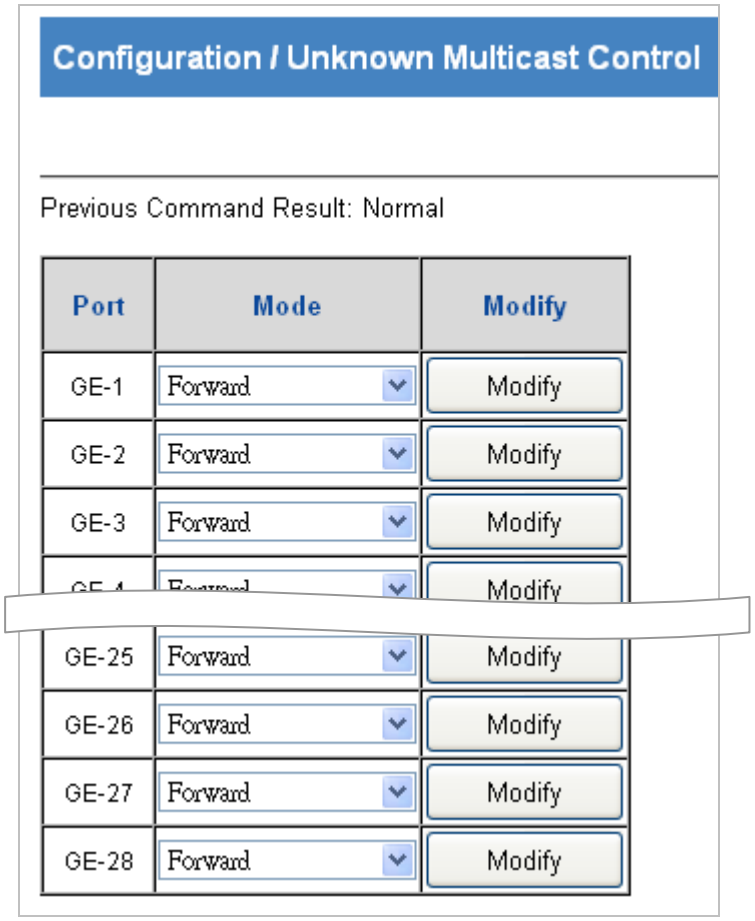


Figure 4-14-2: Configuration / Unknown Multicast Control Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Modify the configuration. Click the **Modify** button to apply change.

The page includes the following fields:

Object	Description
• **Port**	Giga Port GE-1 ~ 28 of Port.
• **Mode**	Forward -> Forward unknown multicast packet (default) Block -> Block unknown multicast packet Rate limit -> Control rate. Rate range is 1~1000000 Kbps, default is 1000000 Kbps.

4.14.3 Broadcast Control

The configuration indicates the permitted packet rate for broadcast traffic across the switch. The screen in Figure 4-14-3 appears.

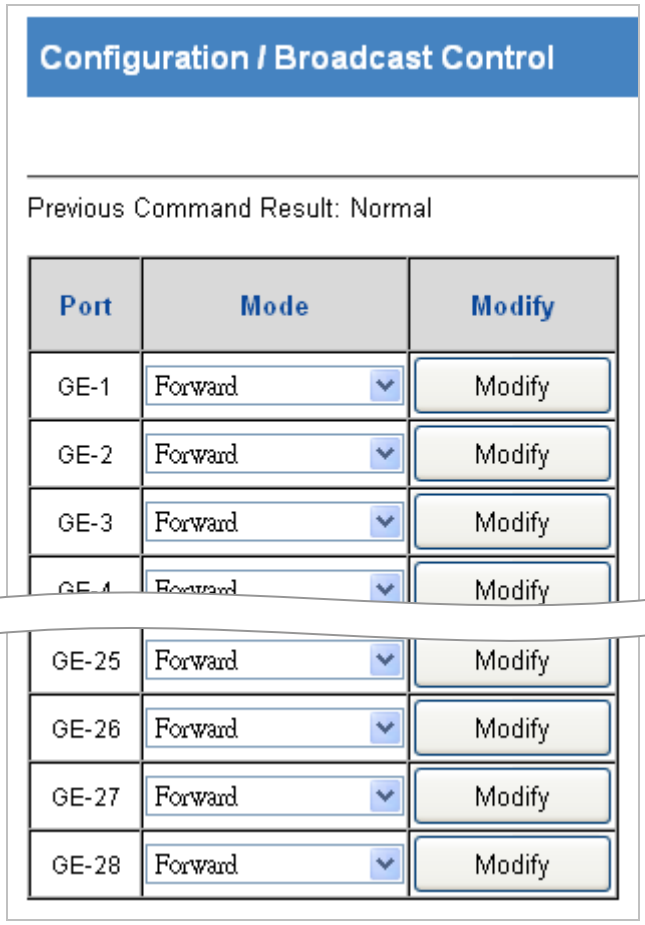


Figure 4-14-2: Configuration / Broadcast Control Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Modify the configuration. Click the **Modify** button to apply change.

The page includes the following fields:

Object	Description
• **Port**	Giga Port GE-1 ~ 28 of Port.
• **Mode**	Forward -> Forward broadcast packet (default) Block -> Block broadcast packet Rate limit -> Control rate. Rate range is 1~1000000 Kbps, default is 1000000 Kbps.

4.14.4 Unknown Unicast by VLAN

This page shows the special VLAN forward or black unknown unicast traffic. The screen in Figure 4-14-4 appears.

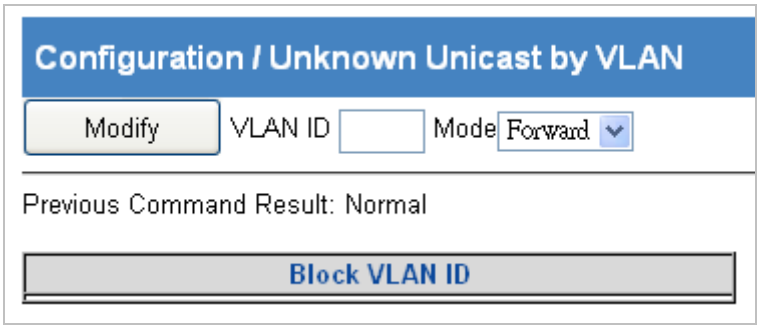


Figure 4-14-4: Configuration / Unknown Unicast by VLAN Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Fill VLAN ID Change Mode Click the **Modify** button to apply change

The page includes the following fields:

Object	Description
• **VLAN ID**	Value range is 1~4094.
• **Mode**	Forward -> Forward unicast packet (default). Block -> Block unicast packet.
• **Block VLAN ID**	All blocked VLAN ID

4.14.5 Unknown Multicast by VLAN

This page shows the special VLAN forward or black unknown multicast traffic. The screen in Figure 4-14-5 appears.

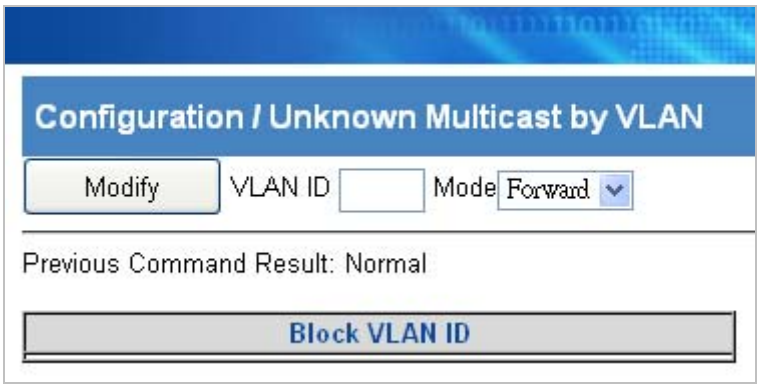


Figure 4-14-5: Configuration / Unknown Multicast by VLAN Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Fill VLAN ID Change Mode Click the **Modify** button to apply change

The page includes the following fields:

Object	Description
• **VLAN ID**	Value range is 1~4094.
• **Mode**	Forward -> Forward multicast packet (default). Block -> Block multicast packet.
• **Block VLAN ID**	All blocked VLAN ID

4.14.6 Broadcast by VLAN

This page shows the special VLAN forward or black broadcast traffic. The screen in Figure 4-14-6 appears.

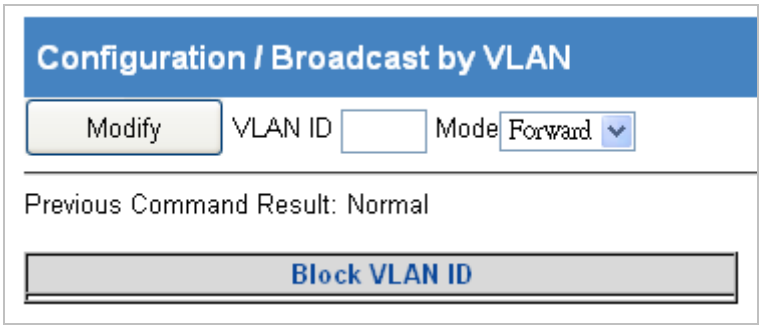


Figure 4-14-6: Configuration / Unknown Multicast by VLAN Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Fill VLAN ID Change Mode Click the **Modify** button to apply change

The page includes the following fields:

Object	Description
• **VLAN ID**	Value range is 1~4094.
• **Mode**	Forward -> Forward broadcast packet (default). Block -> Block broadcast packet.
• **Block VLAN ID**	All blocked VLAN ID

4.15 IGMP

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

About the Internet Group Management Protocol (IGMP) Snooping

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

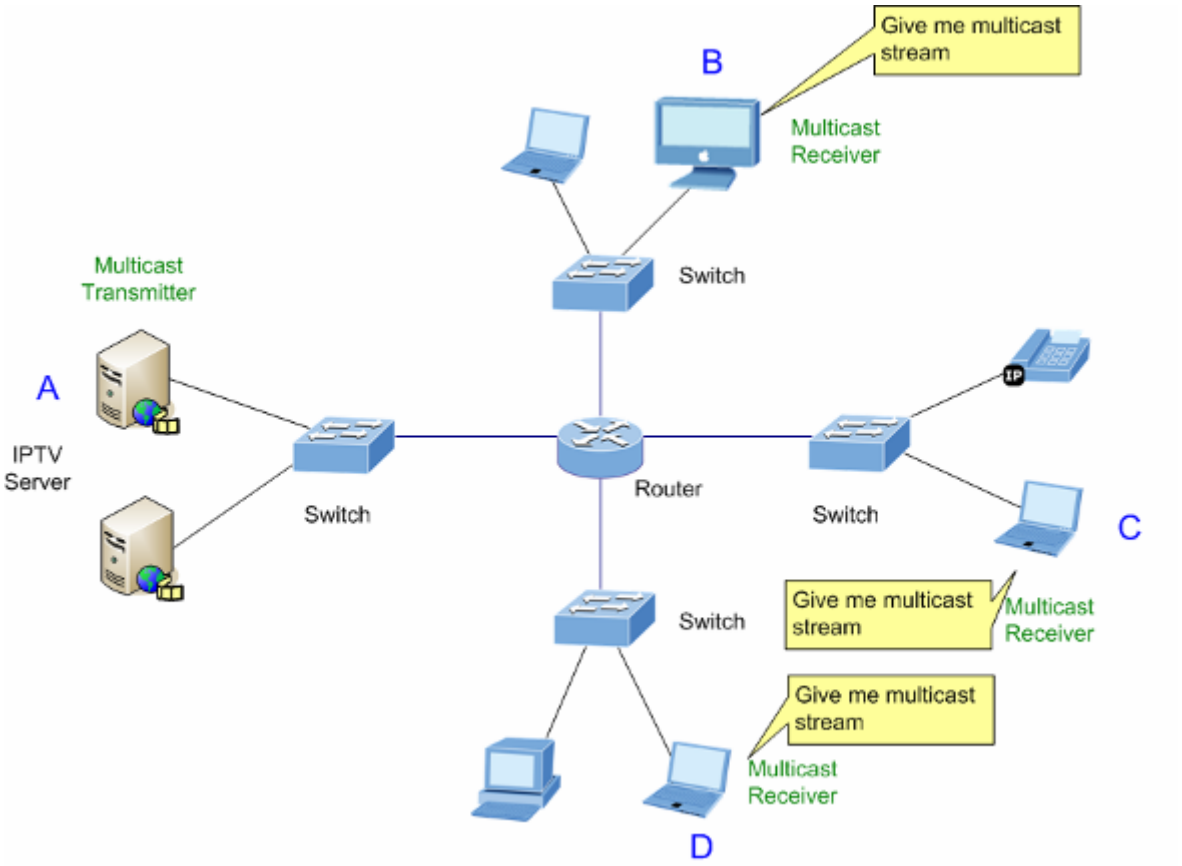


Figure 4-15-1: Multicast Service

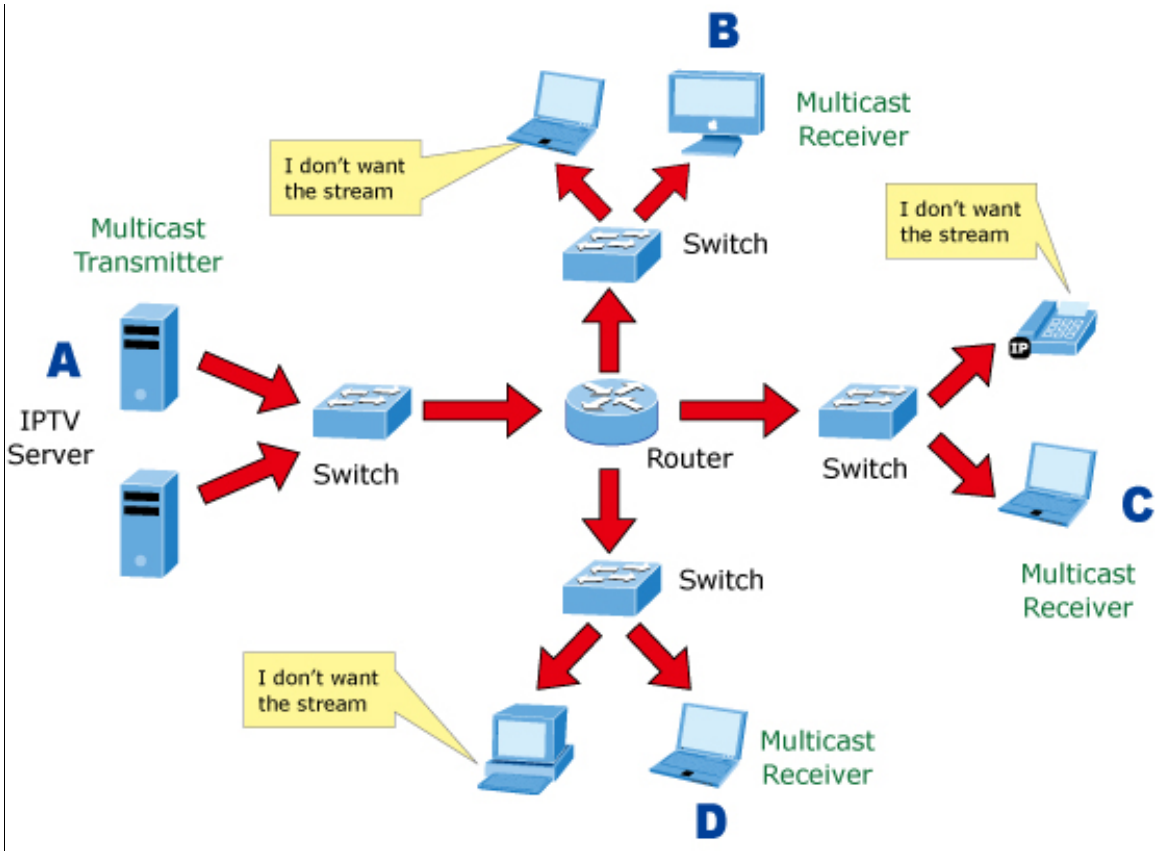


Figure 4-15-2: Multicast Flooding

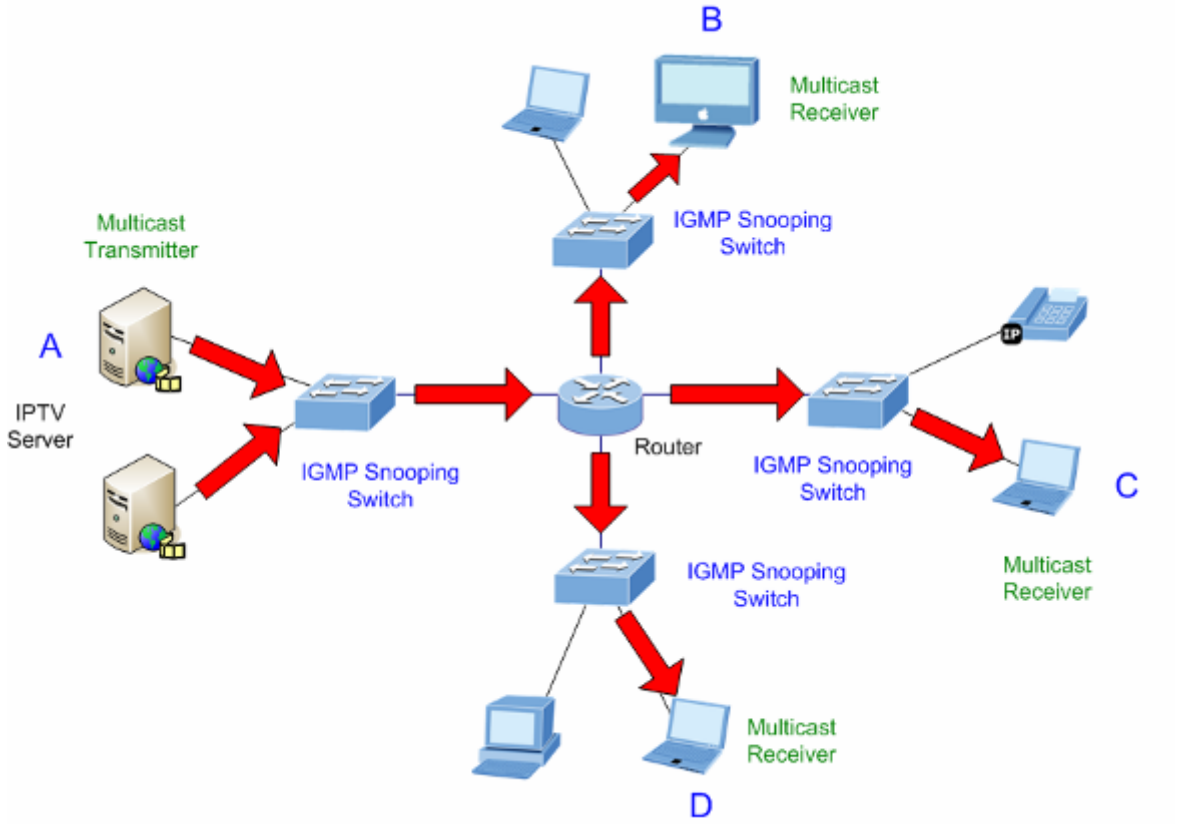
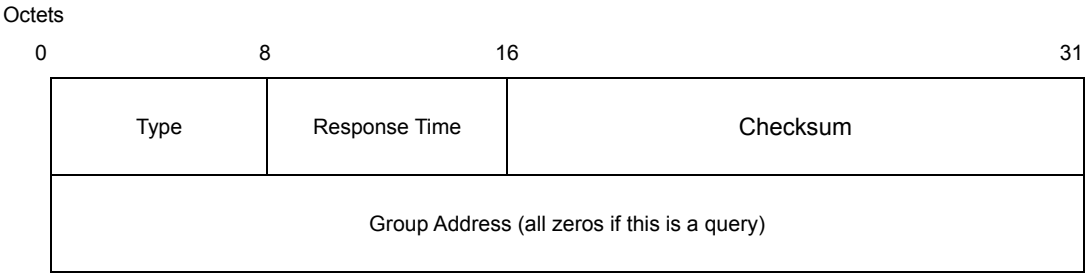


Figure 4-15-3: IGMP Snooping Multicast Stream Control

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



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:

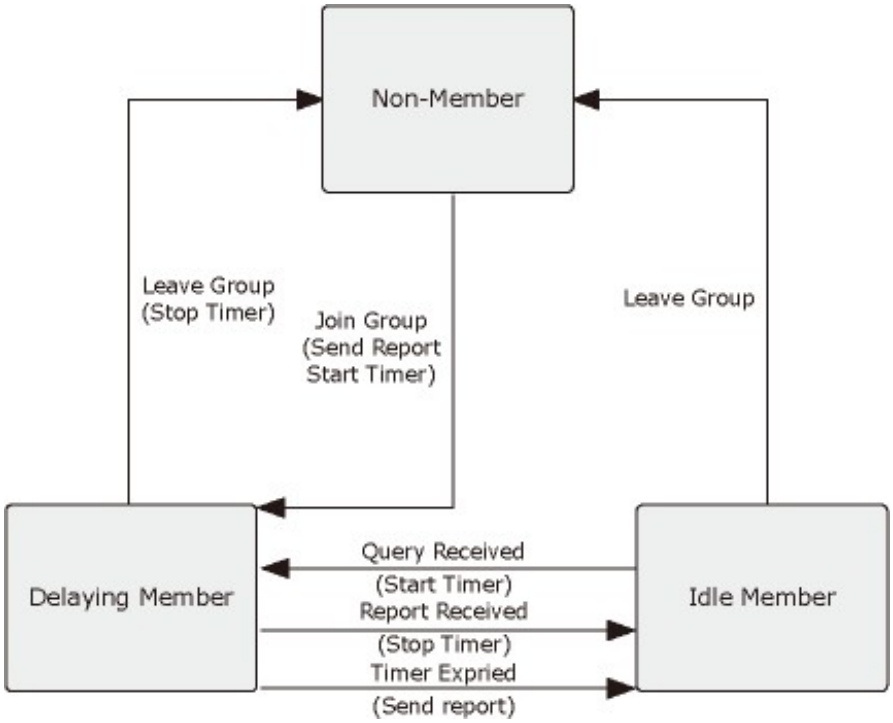


Figure 4-15-4: IGMP State Transitions

- **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.

Note

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

4.15.1 ACL Profile

This page provides IGMP ACL Profile related configurations. The IGMP ACL profile is used to deploy the access control on IP multicast streams. The screen in Figure 4-15-5 appears.

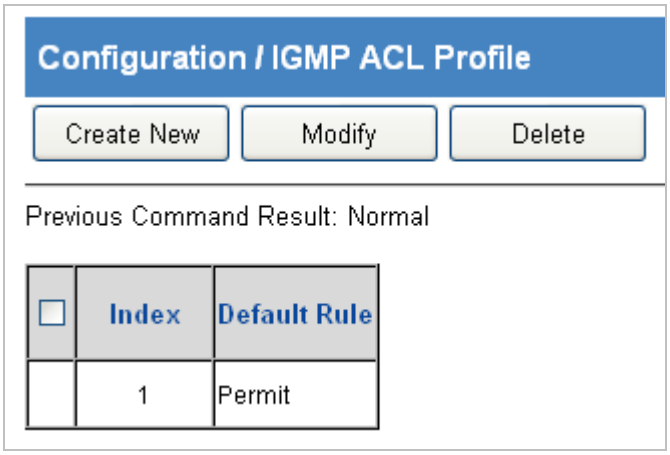


Figure 4-15-5: Confiugration / IGMP ACL Profile Configuration Page Screenshot

Object	Description
• **Operation**	**Create New:** Click the **Create New** button to create a default profile. Click the **Modify** button to modify existing profile. **Modify (allow multiple selection):** Check up Profile Index and select Default Rule for profile. Click the **Modify** button to modify IGMP ACL Profile. **Delete:** Click the **Delete** button to delete profile. (also allow multiple delete) If profile is in use, delete action will be failed.

The page includes the following fields:

Object	Description
• **Profile Index**	IGMP ACL Profile Index: 1~15, but profile 1 is default existing and read-only.
• **Default Rule**	IGMP ACL Default rule: Permit/Deny. Default is permit.

4.15.2 Entry

This page provides address range settings used in IGMP ACL Entry. The address entry is used to specify the address range that will be associated with IGMP ACL Entry. The screen in Figure 4-15-6 appears.

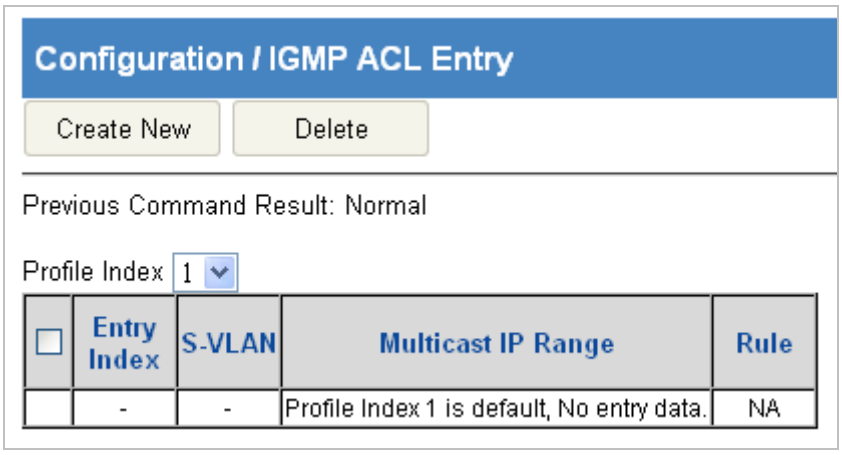


Figure 4-15-6: Configuration / IGMP ACL Entry Configuration Page Screenshot

Object	Description
• **Operation**	**Create:** Click the **Create New** button to open new page for create. Fill Entry Index, SVLAN, Start IP, End IP and select Permission Rule. Click the **Apply** button to create IGMP ACL entry or click "Cancel" to cancel create. **Delete:** Check up target entry, click Delete button to delete them. (also allow multiple delete) **Refresh:** Select Profile index. Click the **Refresh** button to refresh current IGMP ACL profile entry(s).

The page includes the following fields:

Object	Description
• **Profile Index**	IGMP ACL profile index. Index range is 2~15.
• **Entry Index**	IGMP ACL entry index. Range is 1~32.
• **SVLAN**	IGMP ACL VLAN: VLAN to be Permitted/Denied, 0 is any VLAN.
• **Start IP ~ End IP**	IGMP ACL Start IP address. Range: 224.0.1.0 - 239.255.255.255 Start IP address <= End IP address
• **Permission Rule**	IGMP ACL entry parameter. Default is Permit.

4.15.3 Binding

This page allows you to bind the IGMP ACL entry to the special port. The screen in Figure 4-15-7 appears.

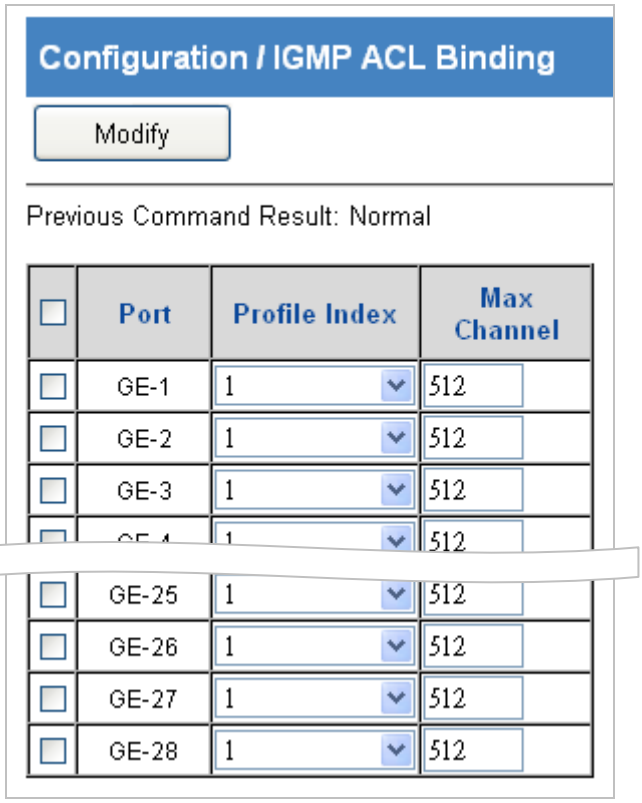


Figure 4-15-7: Confiugration / IGMP ACL Binding Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Check up the rows to be modified, select ACL Profile and set Max channel. Click the **Modify** button to change IGMP ACL Binding.

The page includes the following fields:

Object	Description
• **Port**	GE Port: 1 ~ 28 of Port.
• **Profile Index**	IGMP ACL profile index: 1~15. Default is 1.
• **Max channel**	Port Max channel. Range is 1~512. Default is 512.

4.15.4 MVR Profile

This page provides IGMP MVR Profile related configurations. The IGMP MVR profile is used to deploy the access control on IP multicast streams. The screen in Figure 4-15-8 appears.;

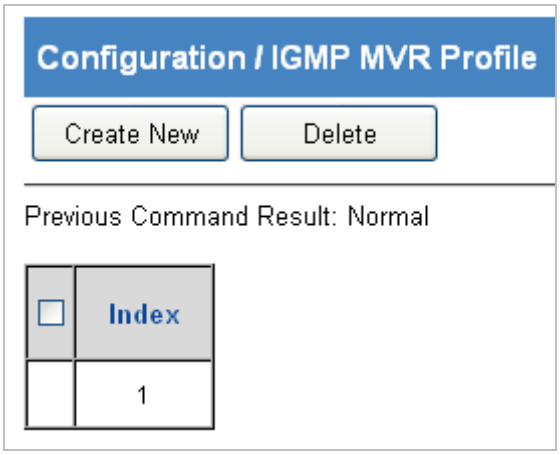


Figure 4-15-8: Configuration / IGMP MVR Profile Configuration Page Screenshot

Object	Description
• **Operation**	**Create:** Click the **Create New** button to create a new profile. **Modify:** Check up Profile Index. Click the Profile Index hyper link to open page for profile entry modification. [or click "Delete" to delete Profile, allow multiple delete. If profile is in use, delete action will be failed.]

The page includes the following fields:

Object	Description
• **Profile Index**	Profile 1 is default existing and read-only, IGMP MVR Profile 2~15 allow to create.

4.15.5 Entry

This page provides address range settings used in IGMP MVR Entry. The address entry is used to specify the address range that will be associated with IGMP MVR Entry. The screen in Figure 4-15-9 appears.

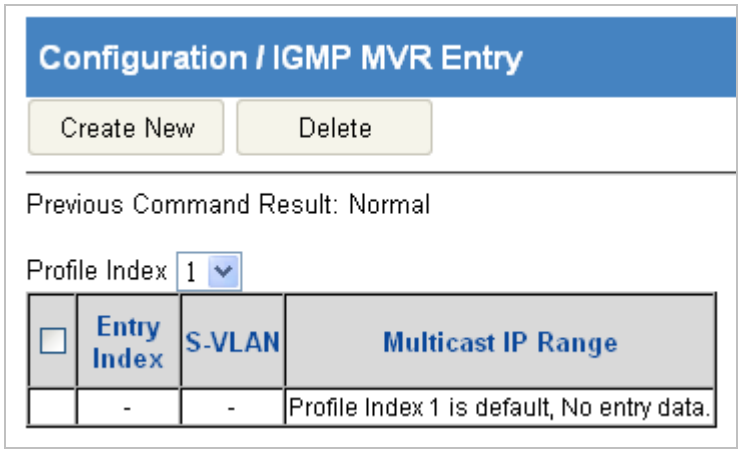


Figure 4-15-9: Configuration / IGMP MVR Entry Configuration Page Screenshot

Object	Description
• **Operation**	**Create New:** Click the **Create New** button to open new page for create. Fill Entry Index, SVLAN, Start IP, End IP. Click the **Apply** button to create IGMP MVR entry or click "Cancel" to cancel create. **Delete:** Check target entry, and click the **Delete** button to delete them. (also allow multiple delete) **Refresh:** Change the Profile Index to refresh the data.

The page includes the following fields:

Object	Description
• **Profile Index**	IGMP MVR profile index. Index range is 2~15.
• **Entry Index**	IGMP MVR entry index. Range is 1~32.
• **SVLAN**	IGMP MVR VLAN: VLAN to be Permitted/Denied, 0 is any VLAN..
• **Start IP ~ End IP**	IGMP MVR Start IP address. Range: 224.0.1.0 - 239.255.255.255 Start IP address <= End IP address

4.15.6 Binding

This page allows you to bind the IGMP MVR entry to the special port. The screen in Figure 4-15-10 appears.

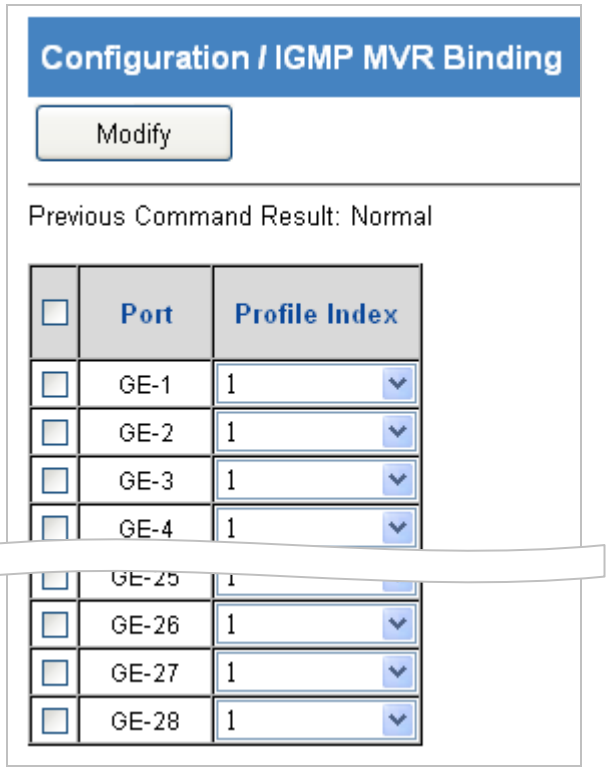


Figure 4-15-10: Configuration / IGMP MVR Binding Configuration Page Screenshot

Object	Description
• **Operation**	**Modify:** Check up the rows to be modified, select MVR Profile. Click the **Modify** button to change IGMP MVR Binding.

The page includes the following fields:

Object	Description
• **Port**	GE Port: 1 ~ MAX Number of Port
• **Profile Index**	IGMP MVR profile index. Value range is 1~15. Default is 1.

4.15.7 VLAN Interface

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. The screens in Figure 4-15-11 and Figure 4-15-12 appear.

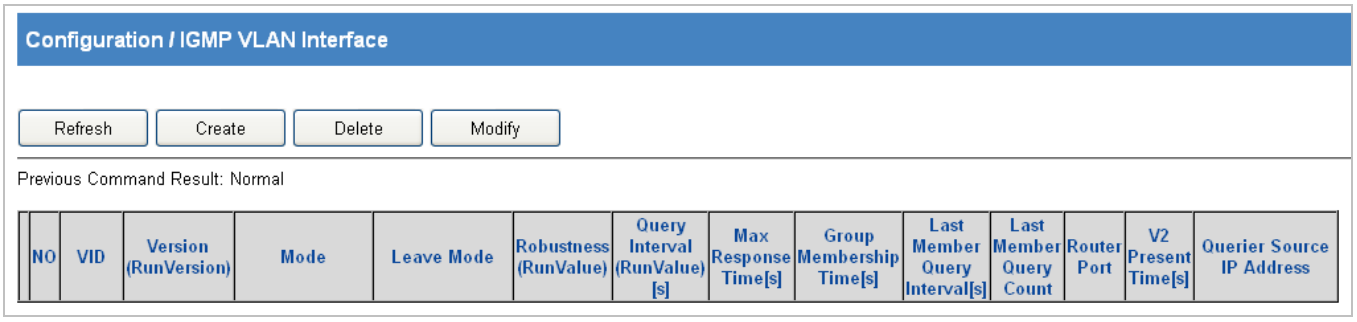


Figure 4-15-11: Configuration / IGMP VLAN Interface Configuration Page Screenshot

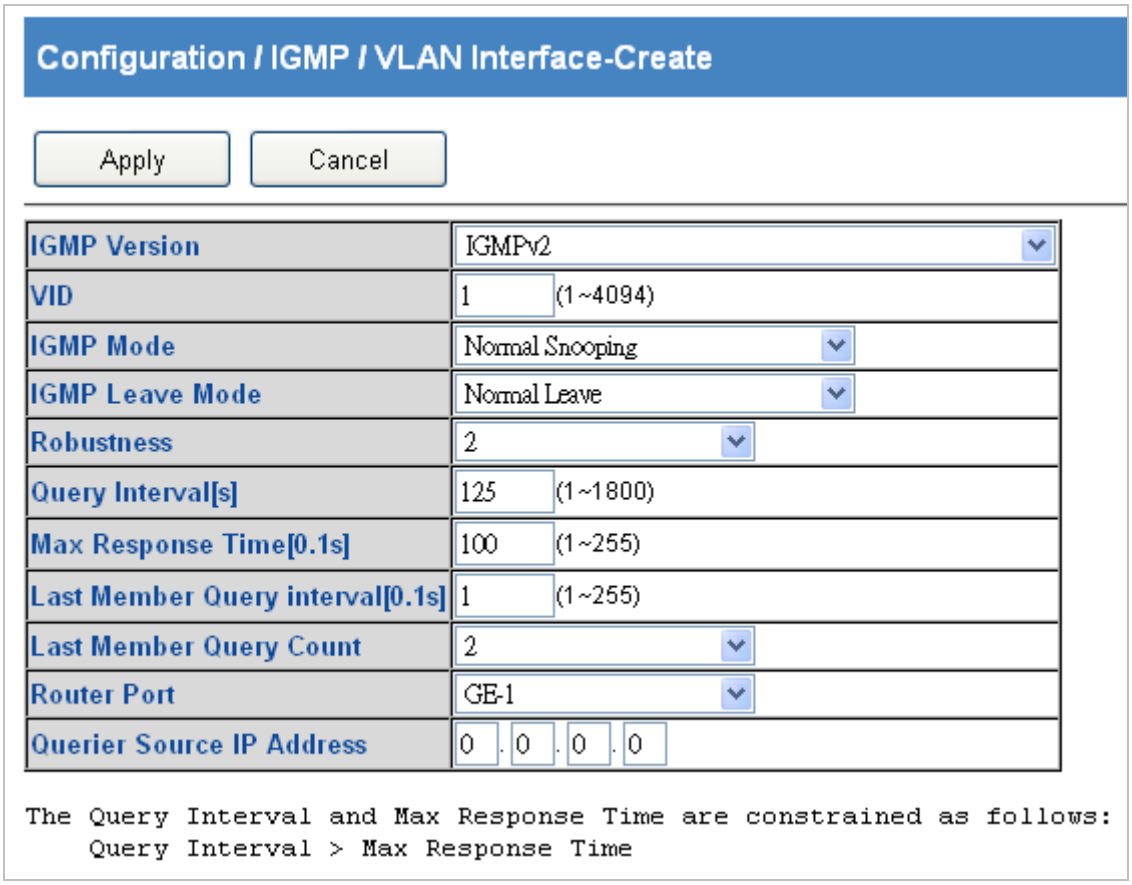


Figure 4-15-12: Configuration / IGMP VLAN Interface Configuration Page Screenshot

Object	Description
• **Operation** •	**Refresh:** Refresh to get current data. **Create:** Into Create web page. Setting data Click "Apply" to setting data or click "Cancel" to cancel setting data. **Delete:** Delete current selected row data. **Modify:** Into Modify web page. Setting data Click "Apply" to setting data or click "Cancel" to cancel setting data.

The page includes the following fields:

Object	Description
• **NO**	Entry Index, max 64.
• **VID**	VLAN ID (1~4094)
• **Version**	IGMP Version: IGMPv2 or IGMPv3.
• **Run Version**	Current running IGMP version.
• **Mode**	IGMP Access Mode: Normal Snooping (default) or Proxy.
• **Leave Mode**	IGMP Leave Mode: Normal Leave (default) or Fast Leave.
• **Robustness**	IGMP VLAN robustness variable. (1~3)
• **Robustness Run Value**	Display QRV value or configured value: To support QRV and QQIC in IGMPv3 mode. Industrial Ethernet Switch support 2 parameters to represent the running Robustness Variable and running Query Interval. These 2 parameters is support for each IGMP VLAN interface. When IGMPv3 proxy mode, these 2 value will apply the value which get from IGMPv3 Query packet. In other mode, the value is applied the configured value.
• **Query Interval (sec)**	IGMP VLAN query interval.(unit: sec) Default: 125 seconds Limitation: Query Interval>Max Response Time

• **Query Interval Run Value (sec)**	Display QQIC value or configured value: To support QRV and QQIC in IGMPv3 mode. Industrial Ethernet Switch support 2 parameters to represent the running Robustness Variable and running Query Interval. These 2 parameters is support for each IGMP VLAN interface. When IGMPv3 proxy mode, these 2 value will apply the value which get from IGMPv3 Query packet. In other mode, the value is applied the configured value
• **Max Response Time**	IGMP VLAN max response time. Default: 10.0 seconds. (Display in second, configure it with 0.1 second) The Query Interval and Max Response Time are constrained as follows: Query Interval > Max Response Time
• **Group Membership Time**	IGMP Group Membership Time (Unit: sec) Read-only
• **Last Member Query Interval**	IGMP VLAN last member query interval. (Display in second, configure it with 0.1 second) Default: 0.1 second
• **Last Member Query Count**	IGMP VLAN last member query count, range 1~3. Default: 2
• **Router Port**	IGMP VLAN interface: Bridge port:GE-1 ~ 28. Default value is 1
• **V2 Present Time(sec)**	Read-only, it can be tuned by (last RunQueryInterval *10*robustness + maxRespTime)
• **Querier Source IP Address**	Querier Source IP Address. Default: 0.0.0.0

4.15.8 Static Group Membership

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages as described in above sections. For certain applications that require tighter control, you may need to statically configure a multicast service on the Managed Switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group. The screen in Figure 4-15-13 appears.

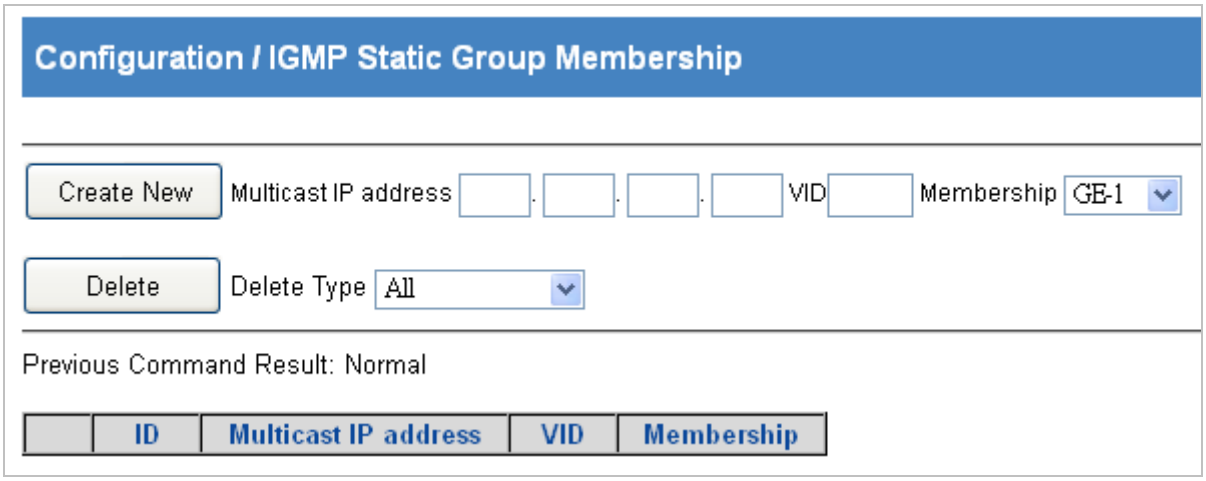


Figure 4-15-13: Configuration / IGMP Static Group Membership Configuration Page Screenshot

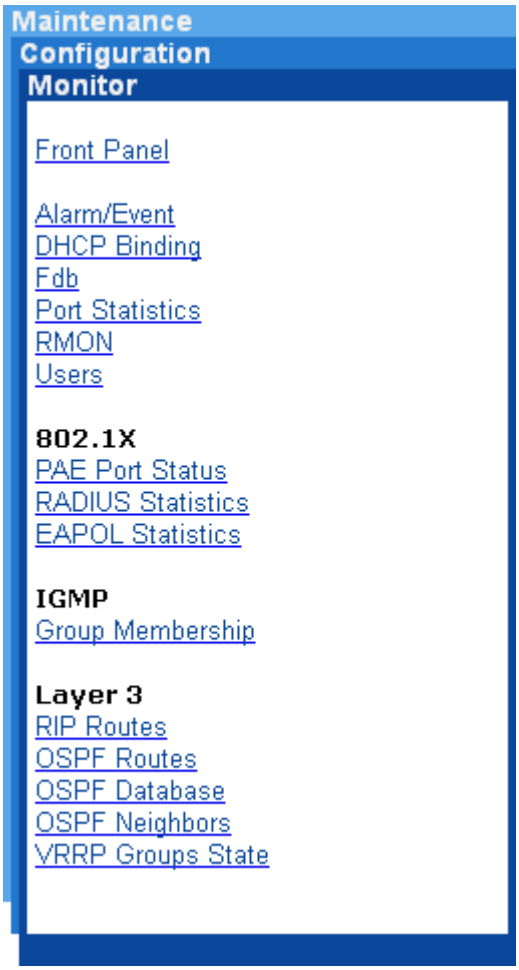
Object	Description
• **Operation**	**Create New:** Fill IP Address, VID and select Membership. Click "Create New" button to create new data. **Delete:** Select Delete Type "All/ Membership/ VID/ Selected" If delete type is "Port", then select a port If delete type is "VID", then fill a VID If delete type is "Selected", then select one row Click "Delete" button to delete data.

The page includes the following fields:

Object	Description
• **ID**	Entry Index, value range is 1~128.
• **IP Address**	Group Membership IP Address, range is 224.0.0.0~239.255.255.255
• **VID**	VLAN ID, range is 1 ~ 4094.
• **ID**	Entry Index, value range is 1~128.

4.16 Monitor Menu Tree

Use the monitor menu items to monitor basic administrative details of the Industrial Managed Switch.



4.16.1 Front Panel

This page will display the status of system's panel. The screen in Figure 4-16-1 appears.

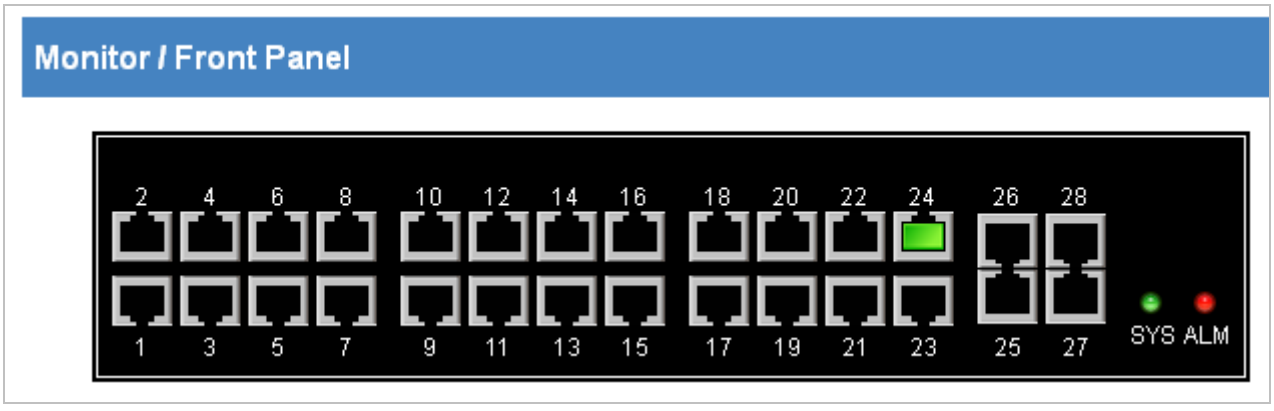


Figure 4-16-1: Monitor / Front Panel Monitor Page Screenshot

Object	Description
• **RJ45 Port**	Link Down:  , Link Up: 
• **SFP Port**	Link Down:  , Link Up: 
• **ALM LED**	Normal:  , Fauliar: 

4.16.2 Alarm/Event

The Industrial Managed Switch system log information is provided here. The screens in Figure 4-16-2, Figure 4-16-3 and Figure 4-16-4 appear.

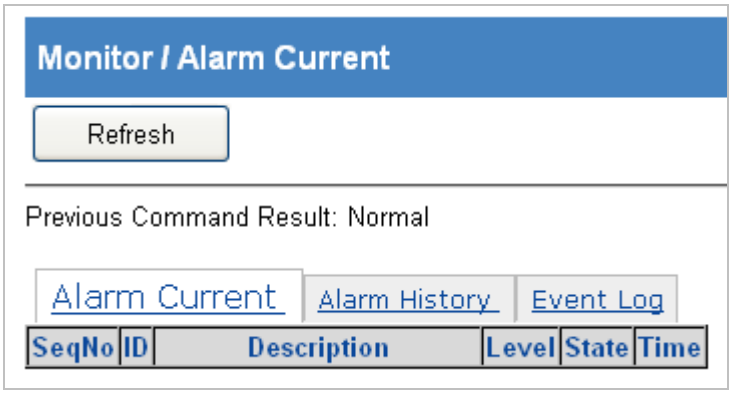


Figure 4-16-2: Monitor / Alarm Current Page Screenshot

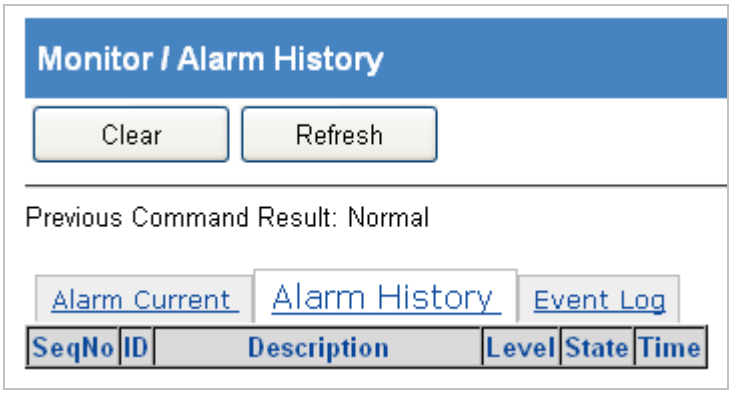


Figure 4-16-3: Monitor / Alarm History Page Screenshot

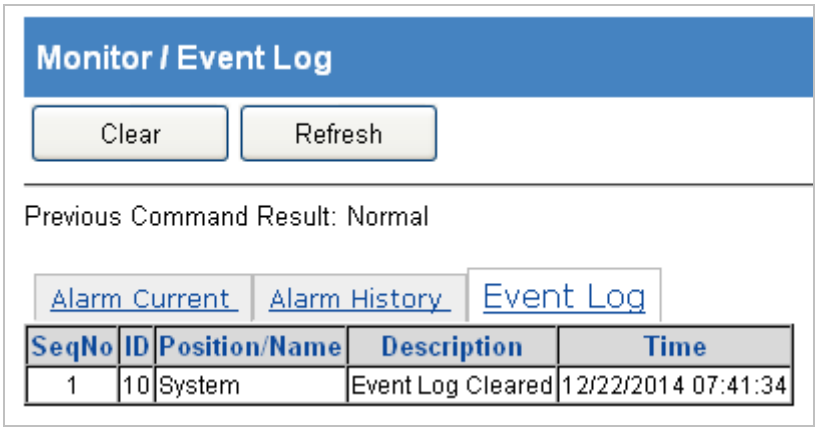


Figure 4-16-4: Monitor / Event Log Page Screenshot

Object	Description
• **Operation**	**Refresh:** Click "Refresh" button to refresh data. **Clear:** Click "Clear" to clear data.

The Page includes the following fields:

Object	Description
• **SeqNo**	Alarm/Event Sequential Number.
• **ID**	Alarm/Event Type ID.
• **Description**	Alarm/Event Type Description.
• **Position/Name**	Event Position/Name.
• **Level**	No matter alarm is major/minor, Alarm LED color always be red.
• **State**	Alarm State. Value is Set/Cleared.
• **Time**	Time.

4.16.3 DHCP Binding

This section diplays a DHCP client list, which includes IP address, hardware address, start time, end time and interface. The screen in Figure 4-16-5 appears.

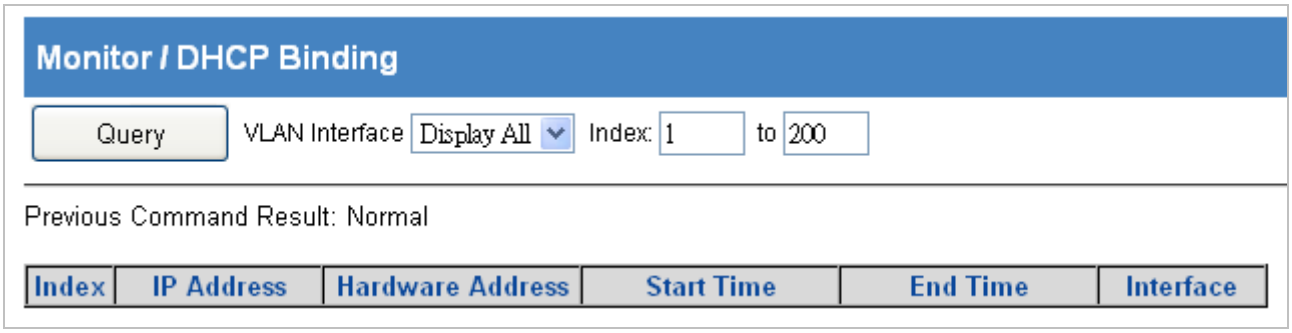


Figure 4-16-5: Monitor / VLAN Interface Monitor Page Screenshot

Object	Description
• **Operation**	**Query:** Click "Query" button to display DHCP Binding Table.

The page includes the following fields:

Object	Description
• **Index**	DHCP client index
• **IP Address**	Display the currest IP address of DHCP client
• **Hardware Address**	Display the currest MAC address of DHCP client
• **Start Time**	Start to use IP address
• **End Time**	Stop to use IP address
• **Interface**	Display the current VLAN interface

4.16.4 Fdb

MAC address table is shown on this page. The MAC address table is sorted first by VLAN ID and then by MAC address. The screen in Figure 4-16-6 appears.

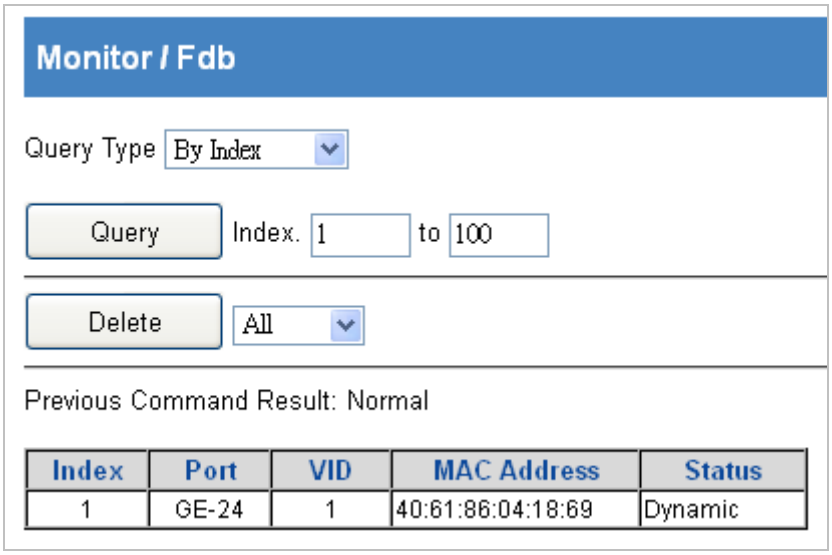


Figure 4-16-6: Monitor / Fdb Page Screenshot

Object	Description
• **Operation**	**Query:** Select a Query Type Fill query condition Modify query record range Click "Query" button to query **Delete:** Select delete type (All/ By VID/By Port) Fill delete condition Click "Delete" to delete data.

The page includes the following fields:

Object	Description
• **Port**	GE-1 ~ 28 of Port or Trunk Group.
• **VID**	VLAN ID: 1~4094
• **MAC Address**	Format xx:xx:xx:xx:xx:xx
• **Status**	Data type: Dynamic/ Static

4.16.5 Port Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display. The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit. The screen in Figure 4-16-7 appears.

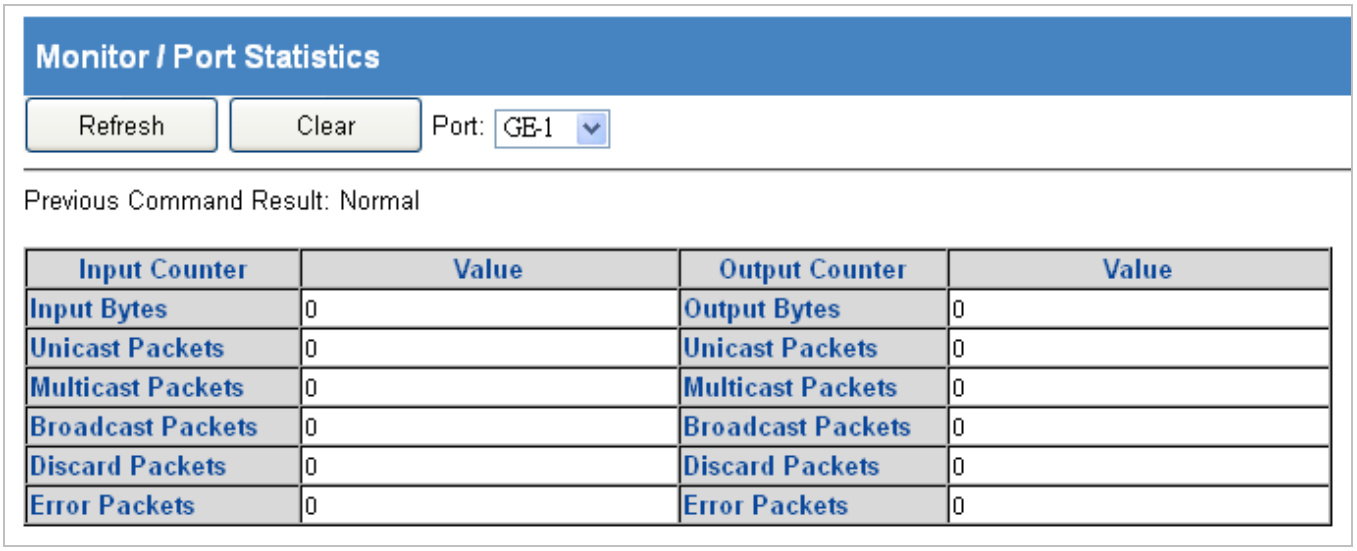


Figure 4-16-7: Monitor / Port Statistics Page Screenshot

Object	Description
• **Operation**	**Refresh:** Fill query condition (Port) Refresh current data. **Clear:** Select clear port. Click "Clear" to clear setting port data.

The page includes the following fields:

Object	Description
• **Port**	Range: GE-1 ~ 28 of Port.
• **Input Bytes**	The total number of octets received on the interface, including framing characters.
• **Input Unicast Pkts**	The number of packets, delivered by this sub-layer to a higher (sub-) layer, which were not addressed to a multicast or broadcast address at this sub-layer.
• **Input Multicast Pkts**	The number of packets, delivered by this sub-layer to a higher (sub-) layer, which were addressed to a multicast address at this sub-layer. For a MAC layer protocol, this includes both Group and Functional address.

• **Input Broadcast Pkts**	The number of packets, delivered by this sub-layer to a higher (sub-) layer, which were addressed to a broadcast address at this sub-layer.
• **Input Discard Pkts**	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
• **Input Error Pkts**	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
• **Output Bytes**	The total number of octets transmitted out of the interface, including framing characters.
• **Output Unicast Pkts**	The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
• **Output Multicast Pkts**	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional address.
• **Output Broadcast Pkts**	The total number of packets that higher-level protocol requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
• **Output Discard Pkts**	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
• **Output Error Pkts**	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.

4.16.5 RMON

This [page provides detailed RMON statistics for a specific switch port. The screen in Figure 4-16-8 appears.

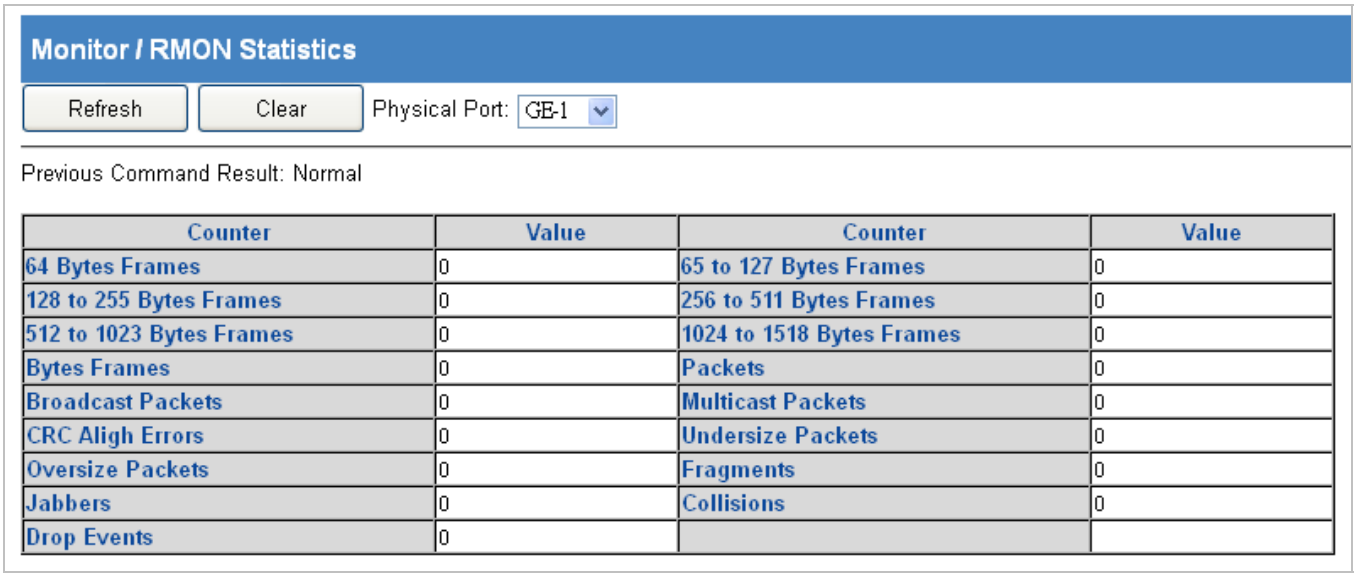


Figure 4-16-8: Monitor / RMON Statistics Page Screenshot

Object	Description
• **Operation**	**Refresh:** Click "Refresh" button to refresh current data. **Clear:** Select clear port. Click "Clear" to clear setting physical port data.

The page includes the following fields:

Object	Description
• **64 Bytes Frames**	Total number of packets (including bad packets) received that were 64 octets in length.
• **65 to 127 Bytes Frames**	Total number of packets (including bad packets) received that were between 65 and 127 octets in length.
• **128 to 255 Bytes Frames**	Total number of packets (including bad packets) received that were between 128 and 255 octets in length.
• **256 to 511 Bytes Frames**	Total number of packets (including bad packets) received that were between 256 and 511 octets in length.
• **512 to 1023 Bytes Frames**	Total number of packets (including bad packets) received that were between 512 and 1023 octets in length.

• **1024 to 1518 Bytes Frames**	Total number of packets (including bad packets) received that were between 1024 and 1518 octets in length.
• **Bytes Frames**	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
• **Packets**	The total number of packets (including bad packets, broadcast packets, and multicast packets)received
• **Broadcast Packets**	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets
• **Multicast Packets**	The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
• **CRC Align Errors**	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
• **Undersize Pkts**	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
• **Oversize Pkts**	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
• **Fragments**	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
• **Jabbers**	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
• **Collisions**	The best estimate of the total number of collisions on this Ethernet segment.
• **Drop Events**	The total number of events in which packets were dropped by the probe due to lack of resources. Note that this number is not necessarily the number of packets dropped; it is just the number of times this condition has been detected.

4.16.6 User

This page provides an overview of the current users. The screen in Figure 4-16-9 appears.

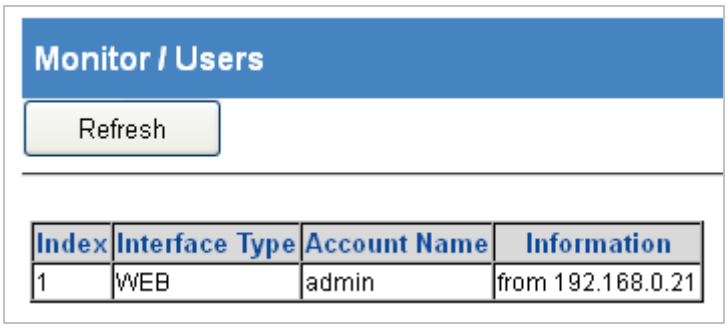


Figure 4-16-9: Monitor / User Page Screenshot

Object	Description
• **Operation**	**Refresh:** Click "Refresh" button to refresh current data.

The page includes the following fields:

Object	Description
• **Index**	Show the index of login user list.
• **Interface Type**	Show the mode of access. Possible values Console, CLI, Web.
• **Account Name**	Show the account name of the user.
• **Information**	Show more information about the user, including IP address of the management host.

4.16.7 802.1X

4.16.7.1 PAE Port Status

This page provides an overview of the current PAE port states for the switch. The screen in Figure 4-16-10 appears.

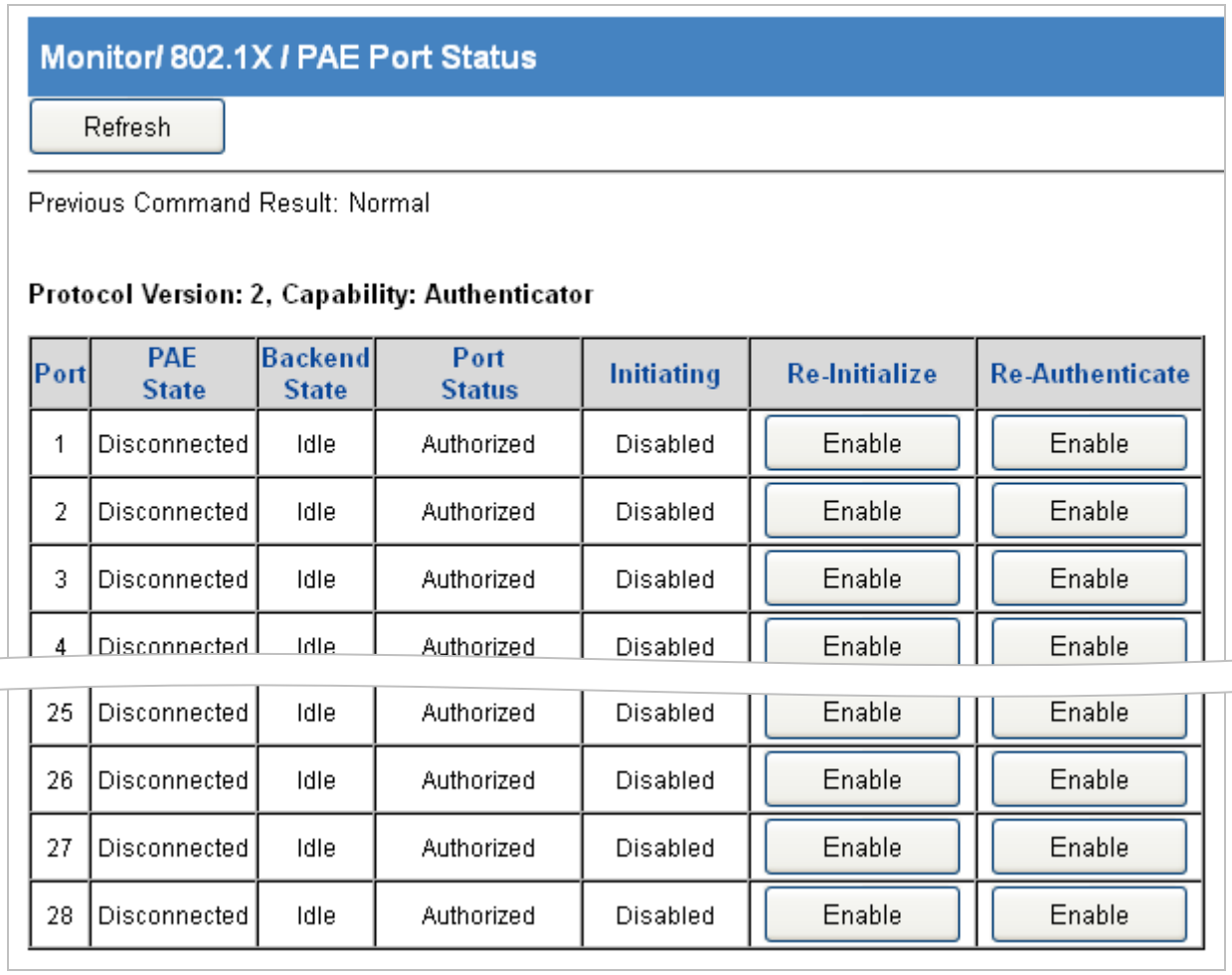


Figure 4-16-10: Monitor / 802.1X / PEA Port Status Page Screenshot

Object	Description
• **Operation**	**Refresh:** Click "Refresh" button to refresh current data.

The page includes the following fields:

Object	Description
• **Port**	The index of PAE Port: Value Range 1 ~ 28 of Port.

• **PAE State**	The authenticator status of PAE port: Possible state: ■ Initialize ■ Disconnected ■ Authenticating ■ Authenticated ■ Aborting ■ Held ■ Force Auth ■ Force Unauth
• **Backend State**	The number of RADIUS Access-Accept received from RADIUS server. Range: 0~65535.
• **Rejects**	The backend authenticator status of PAE port. Possible state: ■ Initialize ■ Idle ■ Request ■ Response ■ Success ■ Fail ■ Timeout ■ Ignore
• **Port Status**	The authentication status of PAE port. Possible state: Authorized/Unauthorized
• **Initiating**	Enable for force PAE port re-initialize.
• **Re-Initialize**	Set Enable to force PAE port re-initialize.
• **Re-Authenticate**	Set Enable to force PAE port re-authenticate.

4.16.7.2 RADIUS Statistics

This page provides detailed statistics for a particular RADIUS server. The screen in Figure 4-16-11 appears.

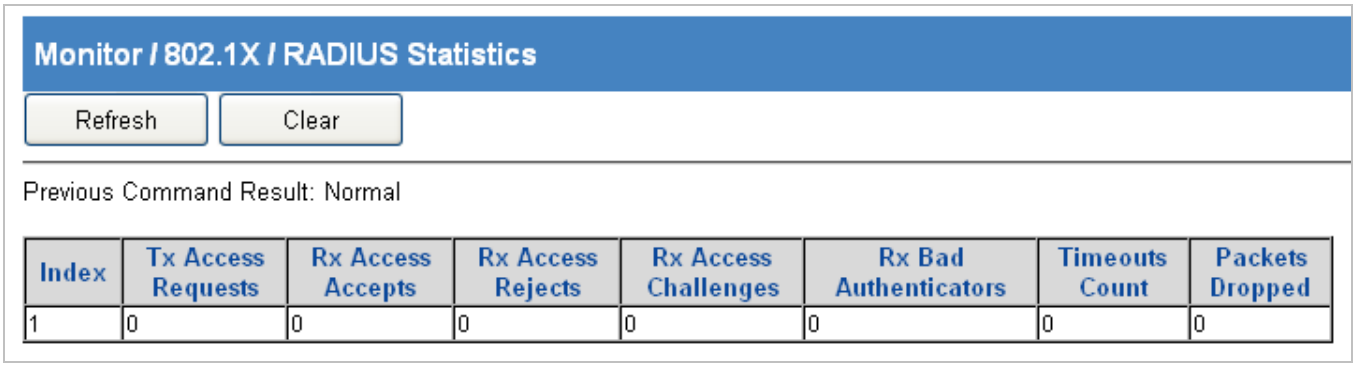


Figure 4-16-11: Monitor / 802.1X / RADIUS Statistics Page Screenshot

Object	Description
• **Operation**	**Refresh:** Click "Refresh" button to refresh current data. **Clear:** Click "Clear" button to reset the counters.

The page includes the following fields:

Object	Description
• **Index**	The index of RADIUS Server: Current only support 1 RADIUS server
• **Requests**	The number of RADIUS Access-Request sent to RADIUS server Range 0~65535.
• **Accepts**	The number of RADIUS Access-Accept received from RADIUS server: Range 0~65535.
• **Rejects**	The number of RADIUS Access-Reject received from RADIUS server: Range 0~65535.
• **Challenges**	The number of RADIUS Access-Challenge received from RADIUS server: Range 0~65535.
• **Bad Authenticators**	The number of invalid RADIUS response packet received from RADIUS server: Range 0~65535.
• **Timeout**	The number of server Timeout happens on Backend Authentication state machine: Range 0~65535
• **Packets Dropped**	The number of packet from RADIUS server to be silent drop by Authenticator Range 0~65535

4.16.7.3 EAPOL Statistics

This page provides detailed EAPOL statistics for all ports. The screen in Figure 4-16-12 appears.

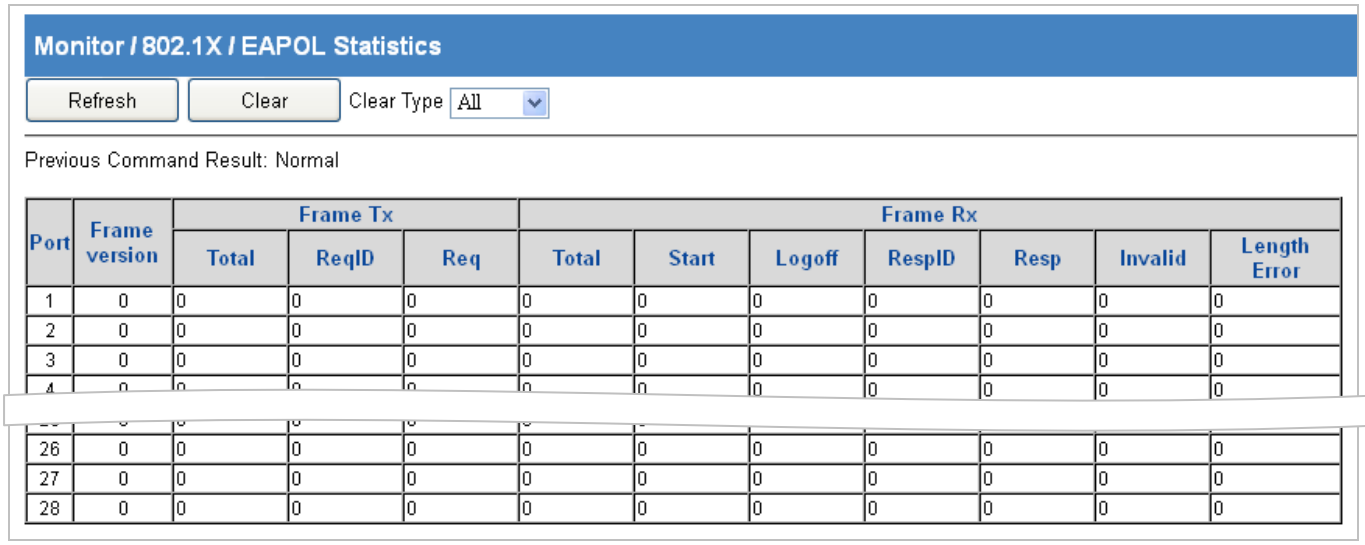


Figure 4-16-12: Monitor / VLAN Interface Monitor Page Screenshot

Object	Description
• **Operation**	**Clear:** Select "Clear Type". If clear type is "Port", then select port number to be cleared. Click "Clear" button.

The page includes the following fields:

Object	Description
• **Port**	The index of PAE port: Value range 1 ~ 28 of port.
• **Protocol Version**	The protocol version number carried in the most recently received EAPOL frame. Range 0~65535.
• **Frame Tx**	The number of EAPOL frames of any type that has been transmitted. Range 0~65535.
• **Req Id Frame Tx**	The number of EAP Req/Id frames that have been transmitted. Range 0~65535.
• **Req Frame Tx**	The number of EAP Request frames (other than Req/Id frames) that have been transmitted. Range 0~65535.
• **Frame Rx**	The number of valid EAPOL frames of any type that has been received. Range 0~65535.

• **Start Frame Rx**	The number of EAPOL Start frames that have been received. Range 0~65535.
• **Logoff Frame Rx**	The number of EAPOL Logoff frames that have been received. Range 0~65535.
• **Resp Id Frame Rx**	The number of EAP Resp/Id frames that have been received. Range 0~65535.
• **Resp Frame Rx**	The number of valid EAP Response frames(other than Resp/Id frames) that have been received. Range 0~65535.
• **Invalid Frame Rx**	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized. Range 0~65535.
• **Length Error Frame Rx**	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid. Range 0~65535.

4.16.8 IGMP Group Membership

Entries in the IGMP Group Information Table are shown on this Page. The screen in Figure 4-16-13 appears.

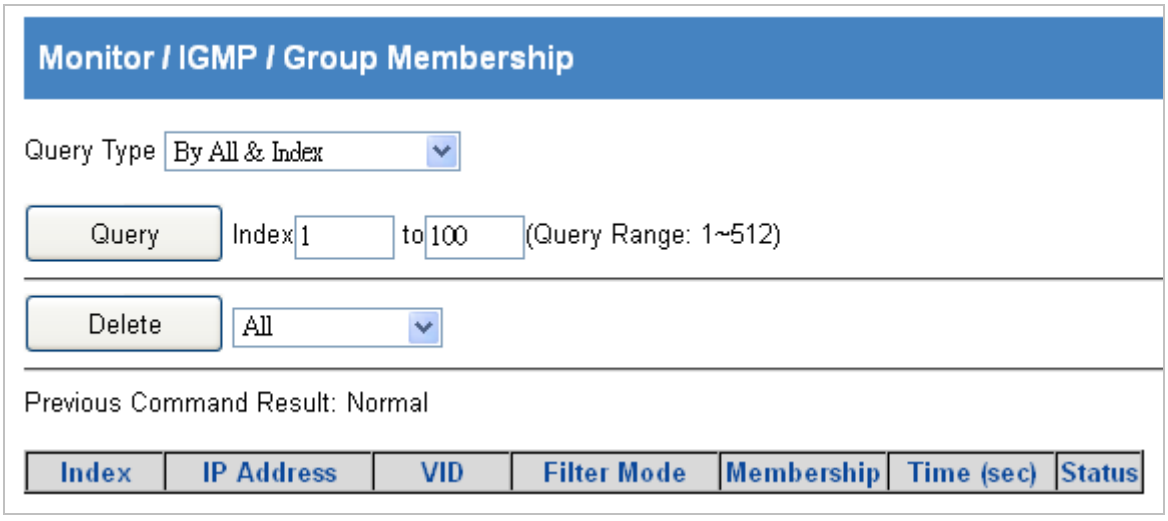


Figure 4-16-13: Monitor / IGMP / Group Membership Page Screenshot

Object	Description
• **Operation**	**Query:** Select Query Type Fill query condition Modify query record range (Index range) Click "Query" button to query data. **Delete:** Select Delete Type Fill VLAN ID when delete type is "By VID" Select one membership when delete type is "By Membership" Click "Delete" button to delete data.

The page includes the following fields:

Object	Description
• **Index**	Index, value range 1~512
• **IP Address**	Group IP Address.
• **VID**	VLAN ID, range 1~4094
• **Filter Mode**	Multicast FDB entry Filter Mode.
• **Membership**	Bridge Port ID, range GE-1 ~ MAX Number of Port.
• **Time (sec)**	Remain Time, unit is second
• **Status**	Group Membership status, Dynamic or Static.

4.16.9 Layer 3

4.16.9.1 RIP Routes

This page provides an overview of the current RIP route table. The screen in Figure 4-16-14 appears.

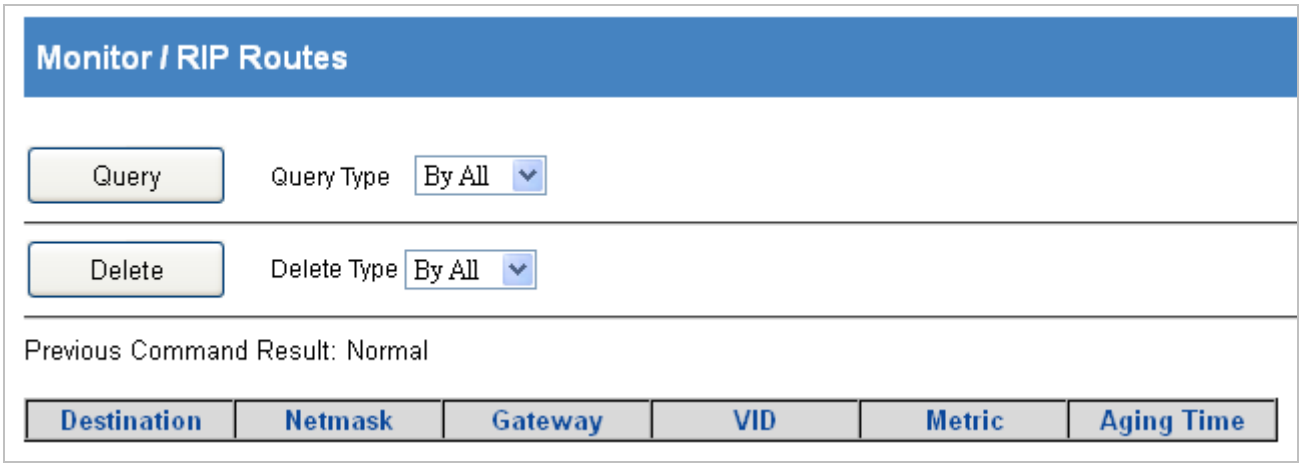


Figure 4-16-14: Monitor / RIP Routes Page Screenshot

Object	Description
• **Operation**	**To query RIP Route Table:** Select Query Type to query by All or by VID. Fill VID when query type is "by VID". **To delete RIP Route entry:** Select RIP route entry(s). Click "Delete" button to delete RIP Route entry.

The page includes the following fields:

Object	Description
• **Destination**	The destination network address for the RIP route.
• **Netmask**	The network subnet mask for the RIP route.
• **Gateway**	The next hop gateway address of the RIP route.
• **VID**	The VLAN ID which is the Route of the RIP packet comes from. Range is 1 ~ 4094.
• **Metric**	The metric of the route. Range 1~16.
• **Aging Time**	The timeout value of Routing information timeout timer or Garbage collection timer. Range 0~3600 seconds.

4.16.9.2 OSPF Routes

This page provides an overview of the current OSPF route table. The screen in Figure 4-16-15 appears.

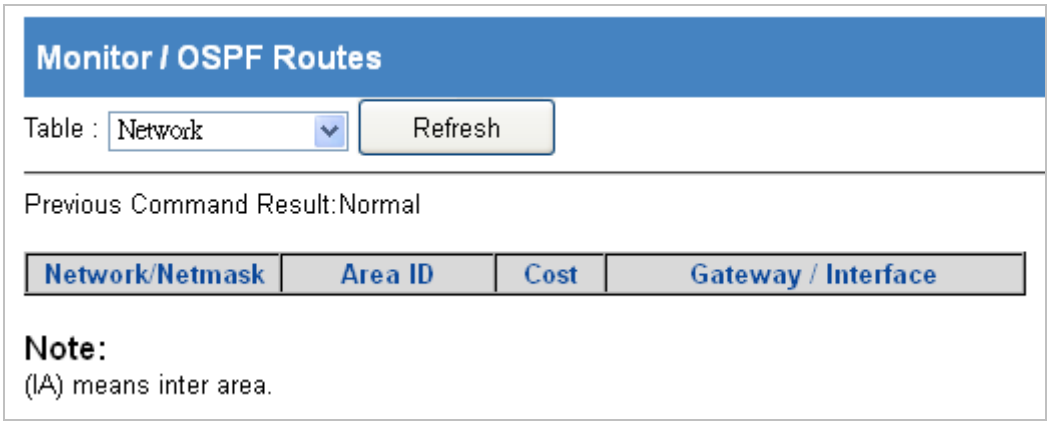


Figure 4-16-15: Monitor / OSPF Routes Page Screenshot

Object	Description
• **Operation**	**To query RIP Route Table:** Select Table type. Click "Refresh" button to get OSPF Routes data.

The page includes the following fields:

Object	Description
• **Router**	Router Address Area ID Cost Flag Gateway/Interface
• **Network**	Network/Netmask Area ID Cost Gateway/Interface
• **External**	Network/Netmask Area ID Cost/Ext Cost Gateway/Interface

4.16.9.3 OSPF Database

This page provides an overview of the current OSPF database informaiton. The screen in Figure 4-16-16 appears.

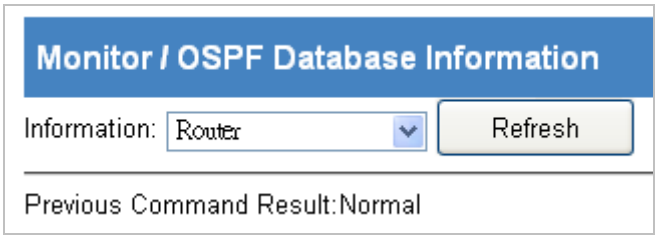


Figure 4-16-16: Monitor / OSPF Database Information Page Screenshot

Object	Description
• **Operation**	**To display OSPF Database data:** Select Information type. Click "Refresh" button to get OSPF database information data.

The page includes the following fields:

Object	Description
• **Information**	Router/Network/Summary/ASBRS Summary/ External/ NSSA External
• **Router**	Index: max 16 Link Connected Link ID Link Data Number of TOS Metrics TOS 0 Metrics
• **Network**	Network mask Attached Router
• **Summary**	Network mask TOS Metric
• **ASBR Summary**	Network mask TOS Metric
• **External**	Network mask TOS Metric Forward Address External Route Tag
• **NSSA External**	Network mask TOS Metric Forward Address External Route Tag
• **Information**	Router/Network/Summary/ASBRS Summary/ External/ NSSA External

4.16.9.4 OSPF Neighbors

This page provides an overview of the current OSPF neighbors. The screen in Figure 4-16-17 appears.

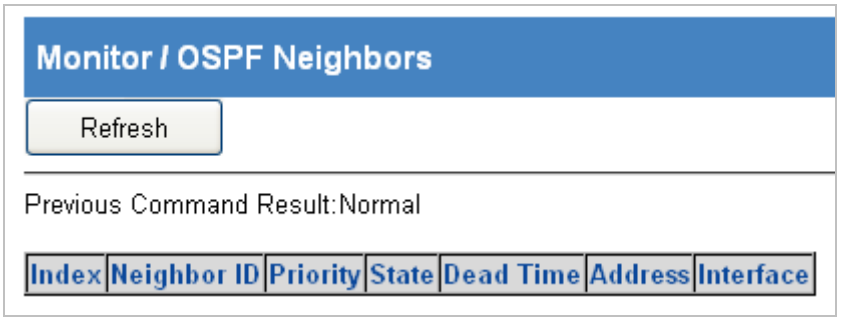


Figure 4-16-17: Monitor / OSPF neighbors Page Screenshot

Object	Description
• **Operation**	**To display OSPF Neighbor data:** Click "Refresh" button to get OSPF neighbor information data.

The page includes the following fields:

Object	Description
• **Index**	OSPF Neighbor Index.
• **Neighbor ID**	OSPF Neighbor ID.
• **Priority**	OSPF Neighbor Priority.
• **State**	Display format NSM/ISM OSPF Neighbor NSM: DOWN/ Attempt/ Init/ To Way/ Exatart/ Loading/ Full OSPF Neighbor ISM: DOWN/ LoopBack/ Waiting/ Point to Point/ Drother/ Back Up/ DR
• **Dead Time**	OSPF Neighbor Dead Timer.
• **Address**	OSPF Neighbor Source.
• **Interface**	OSPF Neighbor interface VLAN.

4.16.9.5 VRRP Groups State

This page provides an overview of the current VRRP group state. The screen in Figure 4-16-18 appears.

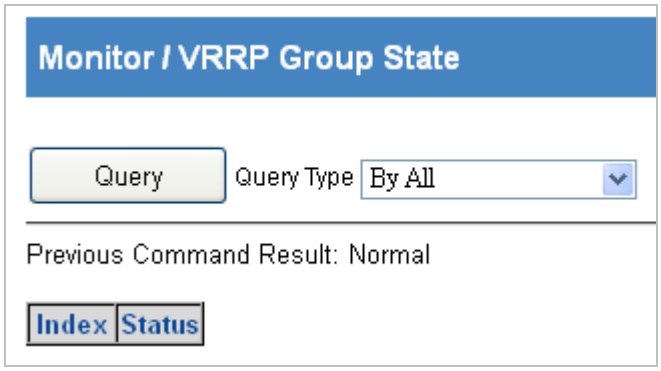


Figure 4-16-18: Monitor / VRRP group state Page Screenshot

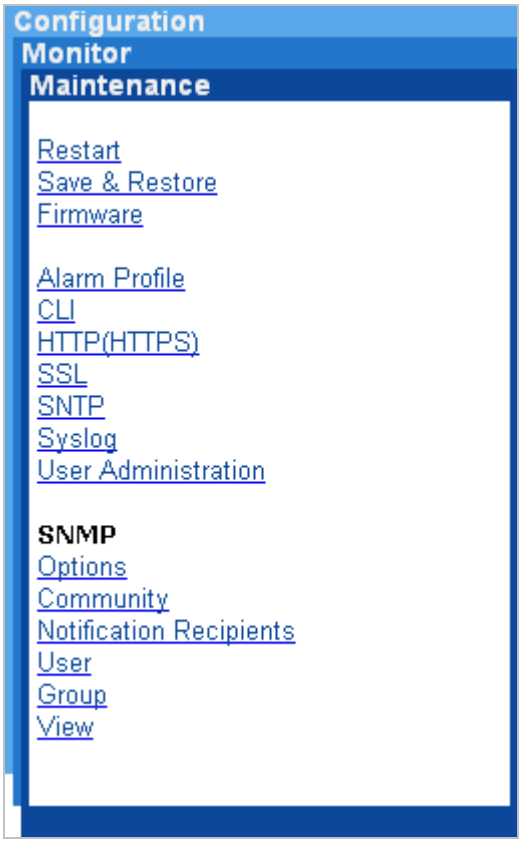
Object	Description
• **Operation**	**Query by All:** Select Query type "By All" Click "Query" button to query VRRP Group state. **Query by VLAN Interface ID:** Select Query type "By VLAN Interface ID" Select VLAN Interface. Click "Query" button to Query VRRP Group state data. **Query by VRRP Group ID:** Select Query type "By VRRP Group ID" Select VRRP Group ID range. Click "Query" button to Query VRRP Group state data.

The page includes the following fields:

Object	Description
• **Index**	The index of VRRP.
• **Status**	Display VRRP Group number on which VLAN interface and current VRRP State

4.17 Maintenance Menu Tree

Use the maintenance menu items to maintenance basic administrative details of the Industrial Managed Switch.



4.17.1 Restart

The Restart Page enables the device to be rebooted from a remote location. The screen in Figure 4-17-1 appears.

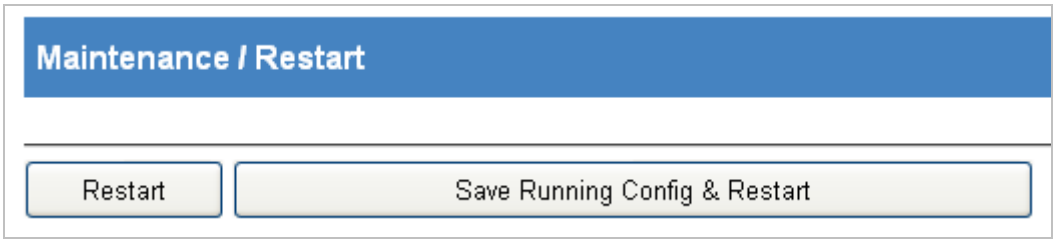


Figure 4-17-1: Maintenance / Restart Page Screenshot

Object	Description
• Operation	**Restart:** Click "Restart" button will restart the system **Save Running Config & Restart:** Click " Save Running Config & Restart" button will redirect page to "Save & Restore"

4.17.2 Save & Restore

The Restart Page enables the device to be rebooted from a remote location. The screen in Figure 4-17-2 appears.

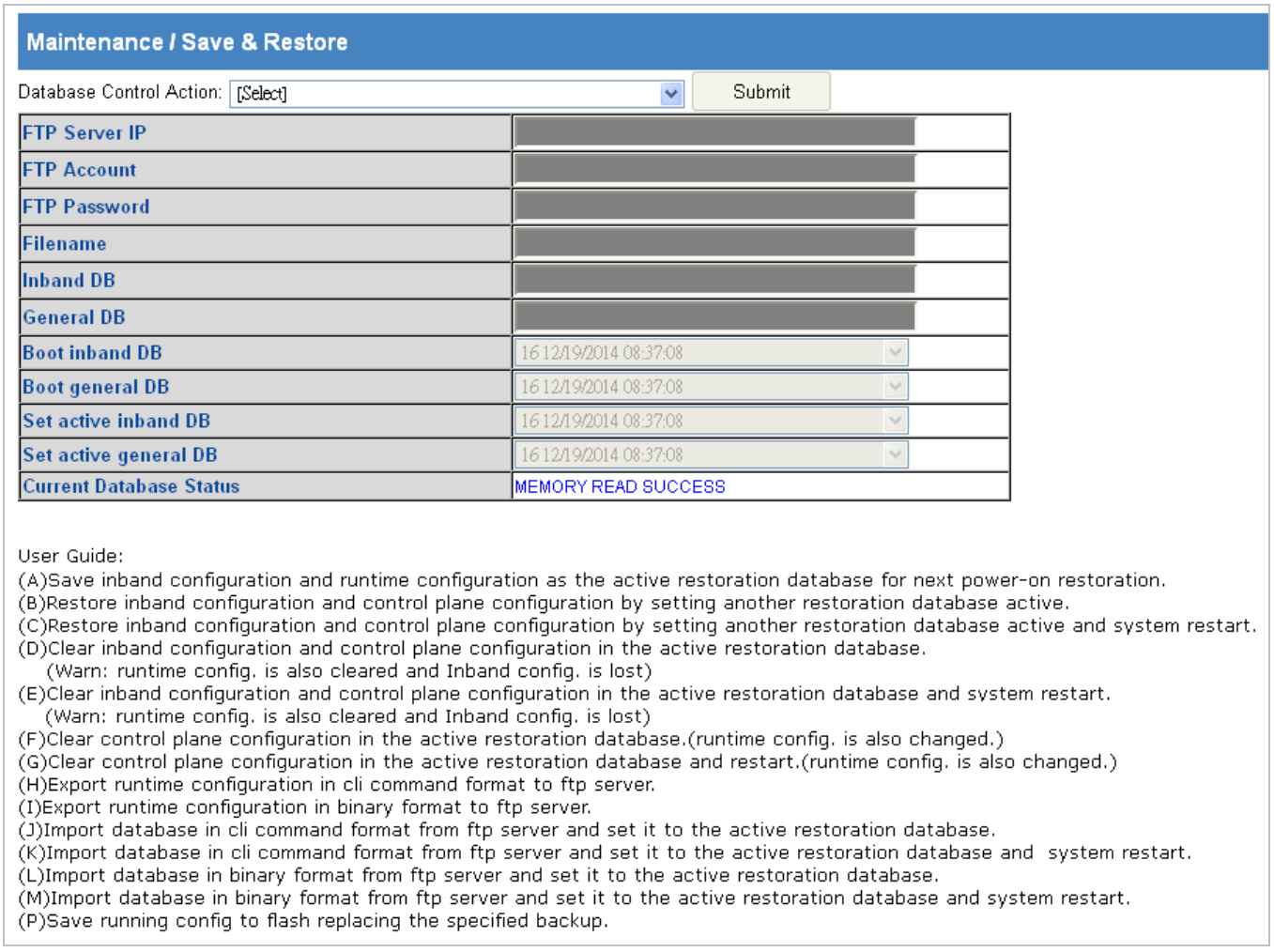


Figure 4-17-2: Maintenance / Save & Restore Page Screenshot

Object	Description
• Operation	**Submit:** Select Control Action. Fill necessary data for action. Click "Submit" button to start the instruction.

The page includes the following fields:

Object	Description
• **Database Control action**	Select Database control. **(A)**Save Inband configuration and runtime configuration as the active restoration database for next power-on restoration. **(B)**Restore Inband configuration and control plane configuration by setting another restoration database active. **(C)**Restore Inband configuration and control plane configuration by setting another restoration database active and system restart. **(D)**Clear Inband configuration and control plane configuration in the active restoration database.(Warn: runtime configuration is also cleared and Inband configuration is lost) **(E)**Clear Inband configuration and control plane configuration in the active restoration database and system restart.(Warn: runtime configuration is also cleared and Inband configuration. is lost) **(F)**Clear control plane configuration in the active restoration database. (runtime configuration. is also changed.) **(G)**Clear control plane configuration in the active restoration database and restart. (runtime configuration is also changed.) **(H)**Export runtime configuration in CLI command format to ftp server. **(I)**Export runtime configuration in binary format to ftp server. **(J)**Import database in CLI command format from ftp server and set it to the active restoration database. **(K)**Import database in CLI command format from ftp server and set it to the active restoration database and system restart. **(L)**Import database in binary format from ftp server and set it to the active restoration database. **(M)**Import database in binary format from ftp server and set it to the active restoration database and system restart. **(P)**Save running configure to flash replacing the specified backup.
• **FTP Server IP**	Input FTP Server IP Address
• **FTP Account**	Input FTP Name
• **FTP Password**	Input FTP Password
• **Filename**	Input File Name
• **Inband DB**	Inband Backup Name (1 ~ 31 characters)
• **General DB**	General Backup Name (1 ~ 31 characters)
• **Boot inband DB**	Show runningcfg backup
• **Boot general DB**	Show runningcfg backup
• **Set active inband DB**	Show runningcfg backup
• **Set active general DB**	Show runningcfg backup

4.17.3 Firmware

The Firmware Upgrade Page provides the functions to allow a user to update the Industrial Managed Switch firmware from the FTP server in the network. Before updating, make sure you have your FTP server ready and the firmware image is on the FTP server. The screen in Figure 4-17-3 appears.

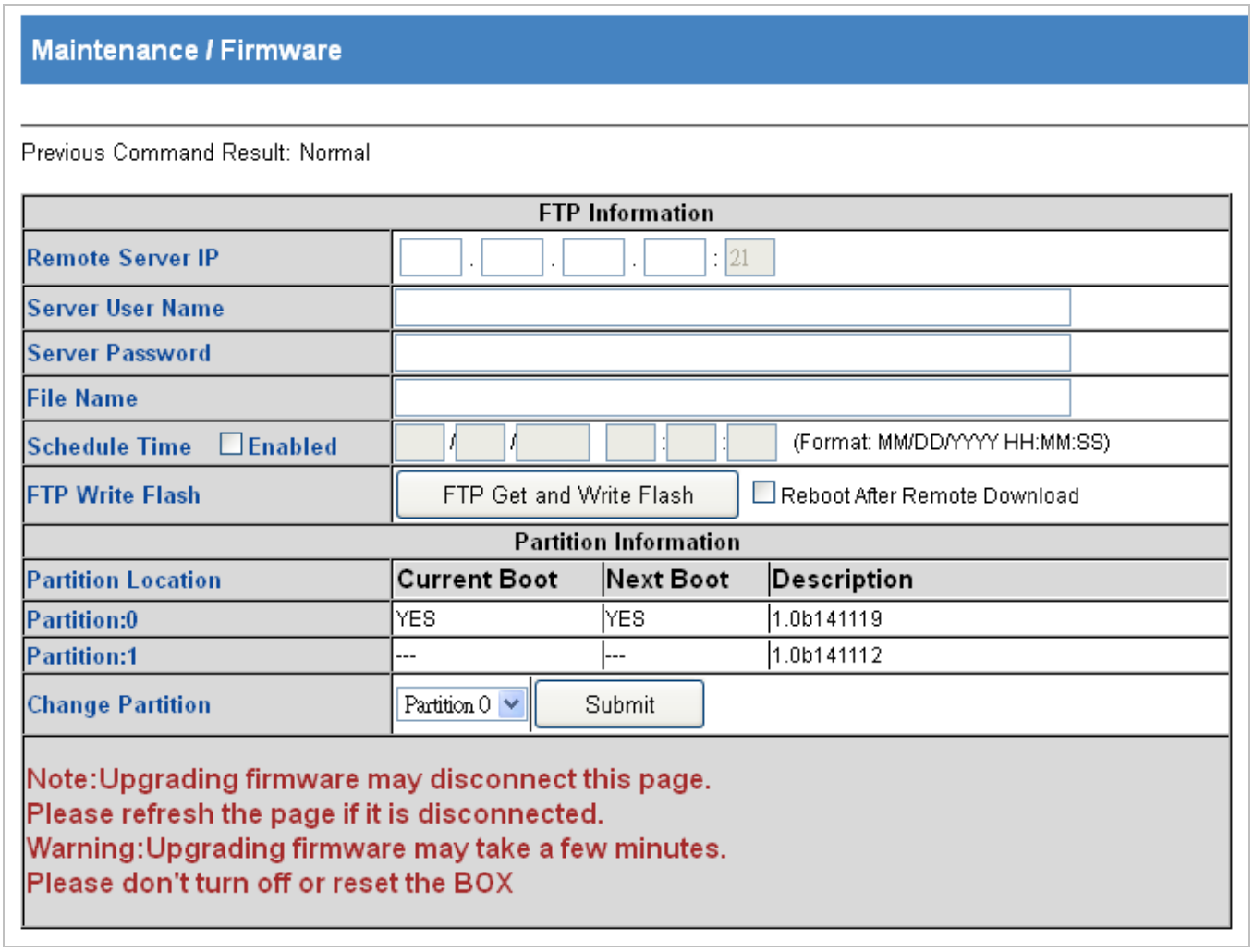


Figure 4-17-3: Maintenance / Firmware Page Screenshot

Object	Description
• **Operation**	**FTP Get and Write Flash:** Select Schedule time checkbox to setting schedule Fill schedule time Click "FTP Get and Write Flash" button will load firmware from remote server IP, If the "Reboot After Remote Download" was selected it will restart system when the firmware was changed. **Submit:** Click "Submit" button will change the partition. The system will use this partition number when the system is restart.

The page includes the following fields:

Object	Description
• **Remote Server IP**	Type in the IP address of the FTP server where the firmware is stored.
• **Server User Name**	Type in a user name accepted by the FTP server.
• **Server Password**	Type in a password accepted by the FTP server.
• **File Name**	Type in the name of the firmware file (string length 1 ~ 64).
• **Schedule Time**	Select Enable checkbox and type in the schedule time to update of the firmware file. The time format: MM/DD/YYYY HH:MM:SS
• **FTP Get and Write Flash**	After you have entered the FTP server, user name, password and firmware file name, click on this button to start the firmware update process.
• **Reboot After Remote Download**	Select the checkbox if you want the system reboot automatically once the firmware update is finished.

4.17.4 Alarm Profile

The Fault Relay Alarm function provides the Power Failure and Port Link Down/Broken detection. With both power input 1 and power input 2 installed and the check boxes of power alarm ticked, the FAULT LED indicator will then be possible to light up when any one of the power failures occurs. As for the Port Link Down/Broken detection, the FAULT LED indicator will light up when the port failure occurs; certainly the check box beside the port must be ticked first. Please refer to the segment of 'Wiring the Fault Alarm Contact' for the failure detection. The screen in Figure 4-17-4 appears.

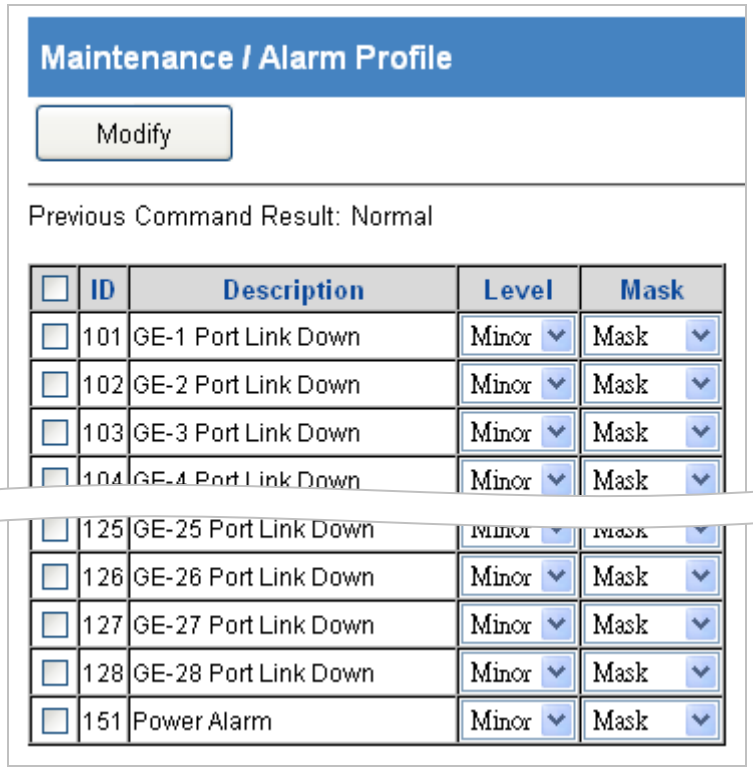


Figure 4-17-4: Maintenance / Alarm Profile Page Screenshot

Object	Description
• **Operation**	**Modify:** Select Row data checkbox. Modify Level and Mask. Note: When any alarm exists, the Alarm LED will be lit, and Alarm Output Relay will also be enabled. Click "Modify" button to modify data.

The page includes the following fields:

Object	Description
• **ID**	Alarm Type ID.
• **Description**	Alarm Type Description.
• **Level**	No matter alarm is major/minor, Alarm LED color always be red.
• **Mask**	If alarm is masked, then alarm item will not be captured in alarm history/current; SNMP trap either. If specific alarm item is masked, then it will not trigger the Alarm LED on or off.

4.17.5 CLI

Specify the console port connettion parameters as required. The screen in Figure 4-17-5 appears.

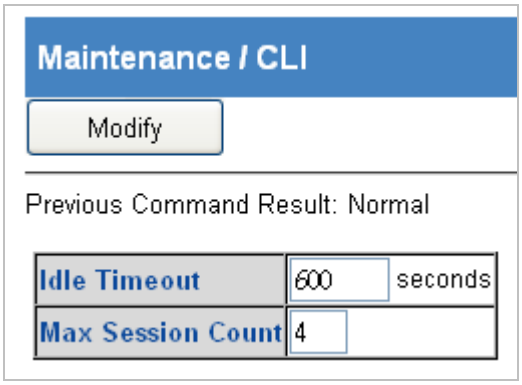


Figure 4-17-5: Maintenance / CLI Page Screenshot

Object	Description
• **Operation**	**Modify:** Modify the configuration. Click "Modify" button to apply change.

The page includes the following fields:

Object	Description
• **Idle Timeout**	Specify the timeout seconds for the operational interface. The session will be closed once the idle time exceeds this timeout value. Value range is 60 ~ 65535. 0 means disable timeout.
• **Max session count**	Specify the maximum allowed sessions for the CLI (command line interface): 1 ~ 10.

4.17.6 HTTP(HTTPS)

You can configure the switch to enable the Secure Hypertext Transfer Protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's web interface. The screen in Figure 4-17-6 appears.

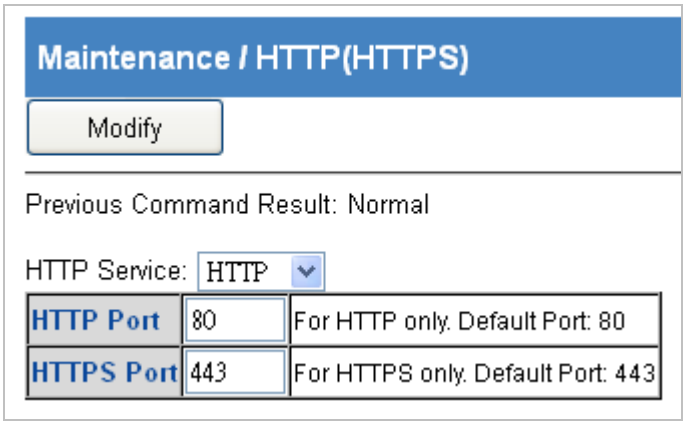


Figure 4-17-6: Maintenance / HTTP(HTTPS) Page Screenshot

Object	Description
• **Operation**	**Modify:** Select HTTP or HTTPS. Change the port number if necessary. Click "Modify" button to apply the change.

The page includes the following fields:

Object	Description
• **HTTPS Service**	HTTPS / HTTP. Default is HTTP (HTTPS disabled).
• **HTTPS Port**	HTTPS service port. Range: 1~65535, Default Port: 443.
• **HTTP Port**	HTTP service port. Range: 1~65535, Default Port: 80.

4.17.7 SSL

A host public/private key pair is used to provide secure communications between an SSH client and the switch. After generating this key pair, you must provide the host public key to SSH clients and import the client's public key to the switch as described in the proceeding section (Command Usage). The screen in Figure 4-17-7 appears.

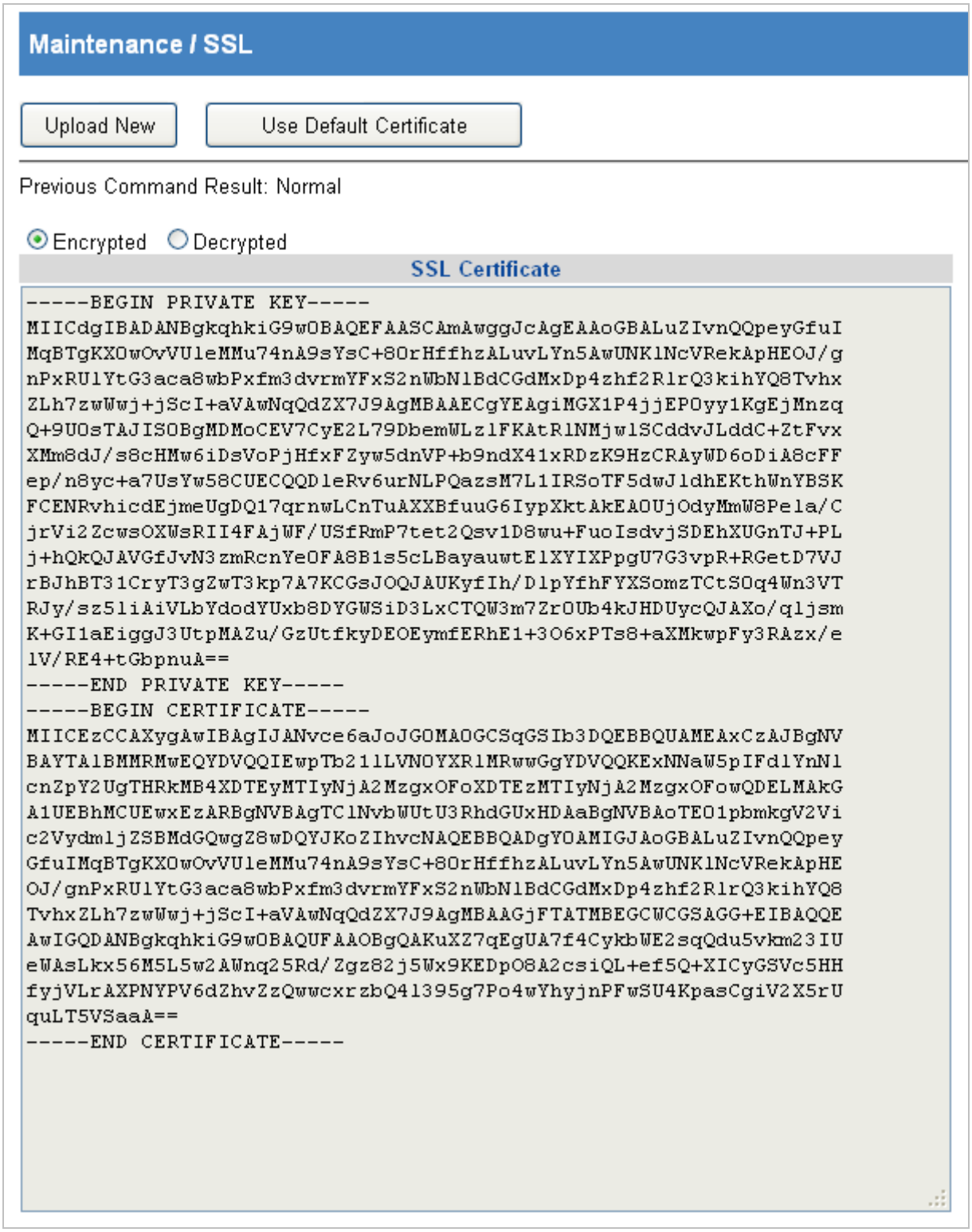


Figure 4-17-7: Maintenance /SSL Page Screenshot

Object	Description
• Operation	**Use Default Certificate:** Click "Use Default Certificate" button. System will delete uploaded certificate, if it's exist. After delete success, it will show default SSL certificate. **Upload New:** Click "Upload New" button. Copy and Paste both Private Key (privatekey) and Self-Signed SSL Certificate (cert) in the input area. The certificate must be in PEM format as the following, otherwise upload would be failed: **-----BEGIN RSA PRIVATE KEY-----** **....** **-----END RSA PRIVATE KEY-----** **-----BEGIN CERTIFICATE-----** **....** **-----END CERTIFICATE-----**

4.17.8 SNTP

Configure SNTP on this page. SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. You can specify SNTP Servers. The screen in Figure 4-17-8 appears.

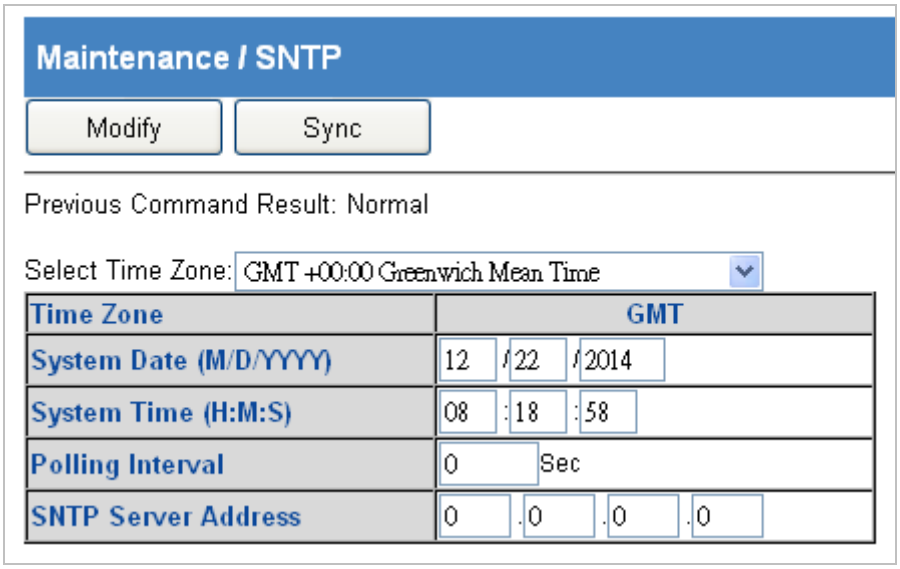


Figure 4-17-8: Maintenance / SNTP Page Screenshot

Object	Description
• **Operation**	**Modify:** Modify the configuration. Click "Modify" button to modify data. **Sync:** Click "Sync" button to manual synchronize system time from SNTP server.

The page includes the following fields:

Object	Description
• **Select Time zone**	Sets the local time zone with Time Zone list. Sixty-six of the world's time zones are presented (including those using standard time and summer/daylight savings time).
• **System Date**	Sets system date (mm/dd/yyyy).
• **System Time**	Sets system time (hh:mm:ss).
• **Polling Interval**	Sets polling interval (seconds) that SNTP client will sync with designated SNTP server.
• **SNTP Server address**	Sets SNTP server IP address for your system.

4.17.9 Syslog

Configure remote syslog on this page. The screen in Figure 4-17-9 appears.

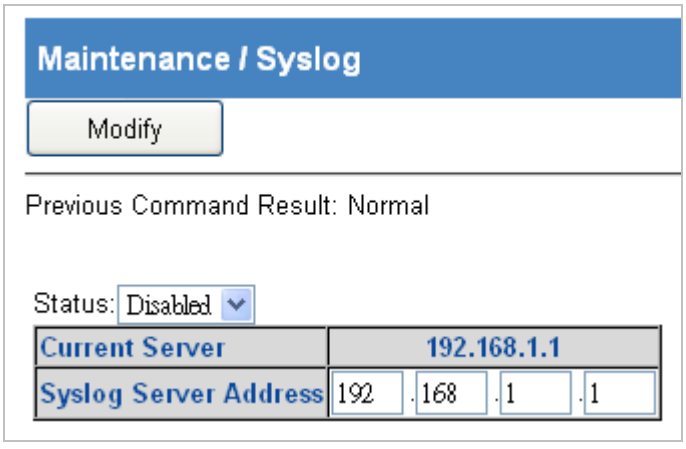


Figure 4-17-9: Maintenance / Syslog Page Screenshot

Object	Description
• **Operation**	**Modify:** Select Enabled/Disabled option and click Modify button to enable Syslog function. Modify the configuration. Click "Modify" button to modify data.

The page includes the following fields:

Object	Description
• **Status**	Value is Enabled/Disabled, default is Disables. It will control the system log work or not.
• **Current Server**	Current Syslog server IP address.
• **Syslog Server Address**	New Syslog server IP address. The server must be a remote host.

4.17.10 User Administration

This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser. The screen in Figure 4-17-10 appears.

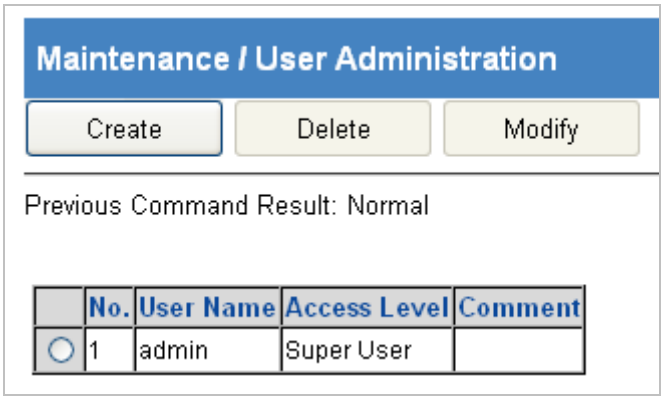


Figure 4-17-10: Maintenance / User Administration Page Screenshot

Object	Description
• **Operation**	**Create:** Click "Create" button to create page. Fill user name, access level, password, confirm password and comment fields. Click "Apply" to create setting data or click "Cancel" to cancel it. **Delete:** Select one row data for delete. Click "Delete" to delete selected data. **Modify:** Click "Modify" button to modify page. Select "Change Password" checkbox if you want to change password. Fill user name, access level, New Password, Retry Password and comment fields. Click "Apply" to apply change or click "Cancel" to cancel it.

The page includes the following fields:

Object	Description
• **User Name**	Shows the user name (up to 32 characters).
• **Access Level**	Show the access level of the user: Super User - The user can access to all functions. Engineer - The user can access to all functions except user account management. Guest - The user can access to basic display functions.
• **Password**	Enter a login password of 1-31 characters.
• **Comment**	Description of the user account (up to 31 characters).

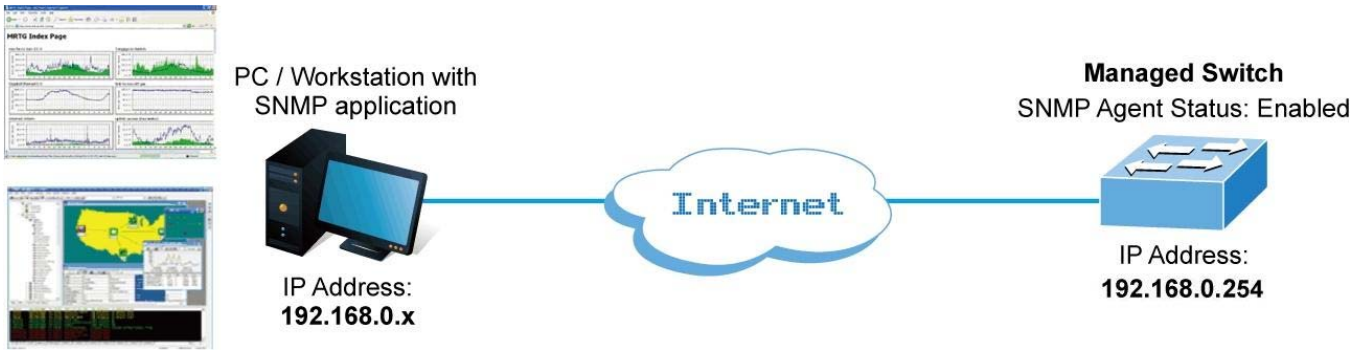
4.17.11 SNMP

4.17.11.1 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

4.17.11.2 Option

Restart SNMP function. The screen in Figure 4-17-11 appears.

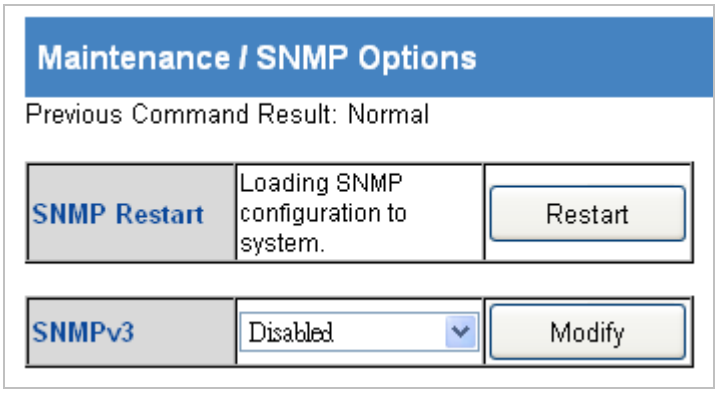


Figure 4-17-11: Maintenance / SNMP Options Page Screenshot

Object	Description
• **Operation**	**Restart:** After any SNMP setting changed, only configuration is changed, but not apply to the system yet. All SNMP changed configuration could work after restart SNMP. It will not reboot system, but may take several seconds to load SNMP setting. **Modify SNMP Version:** This button is used to set whether snmp v3 is enable or not. If snmpV3 switch is set to disable, the system would use snmp v2c only. If snmpV3 switch is set to enable, the system would use snmp v3 setting. Changing this will restart SNMP automatically. The snmp v3 parameters would be valid only if snmp v3 is enabled.

4.17.11.3 Community

Configure SNMPv3 communities table on this page. The entry index key is Community. The screen in Figure 4-17-12 appears.

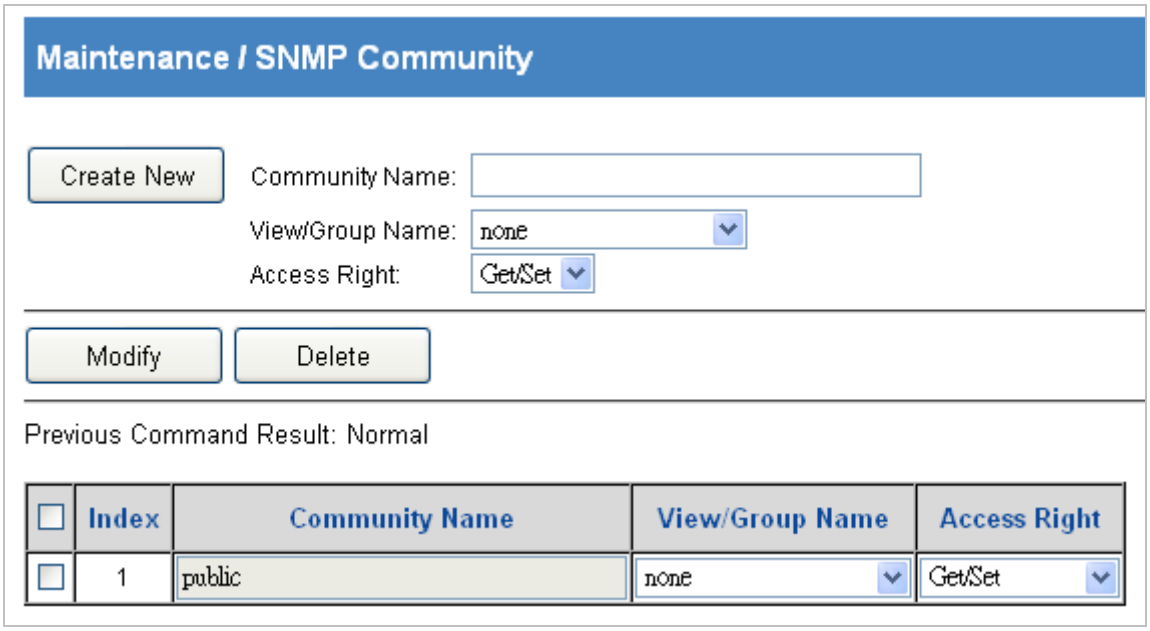


Figure 4-17-12: Maintenance / SNMP Community Page Screenshot

Object	Description
• **Operation**	**Create:** Fill the Community name. Click "Create New" button to create new Community. **Modify community entry:** Select entry by check up the check box Modify field data: Click "Modify" button to apply the change **Delete community entry:** Select entry by check box, then click "Delete". Note: This page supports multi-selection, click one or more row items to delete. User also could click "select all" to delete all target items.

The page includes the following fields:

Object	Description
• **Community Name**	SNMP Community name, for SNMP v1/v2c. Only if community name match, the SNMP request would be received. Community Name max size is 31 characters.

• **View/Group Name**	View and Group are used for SNMP v3 only. A community is allowed to bind one of the view or group name. If it does not take any group or view, it will be a v1/v2c community. If it takes a view or a group name, the community will be treated as a v3 community. The v2c and v3 communities could exit in the community table concurrently. It will display "unknown(name) when view/group name doesn't exist in view/group table.
• **Access Mode**	Choice access right. Allow Get operation only, or allow both Get and Set.
• **Community Name**	SNMP Community name, for SNMP v1/v2c. Only if community name match, the SNMP request would be received. Community Name max size is 31 characters.

4.17.11.4 Notification Recipients

Configure SNMP Trap on this page. The screen in Figure 4-17-13 appears.

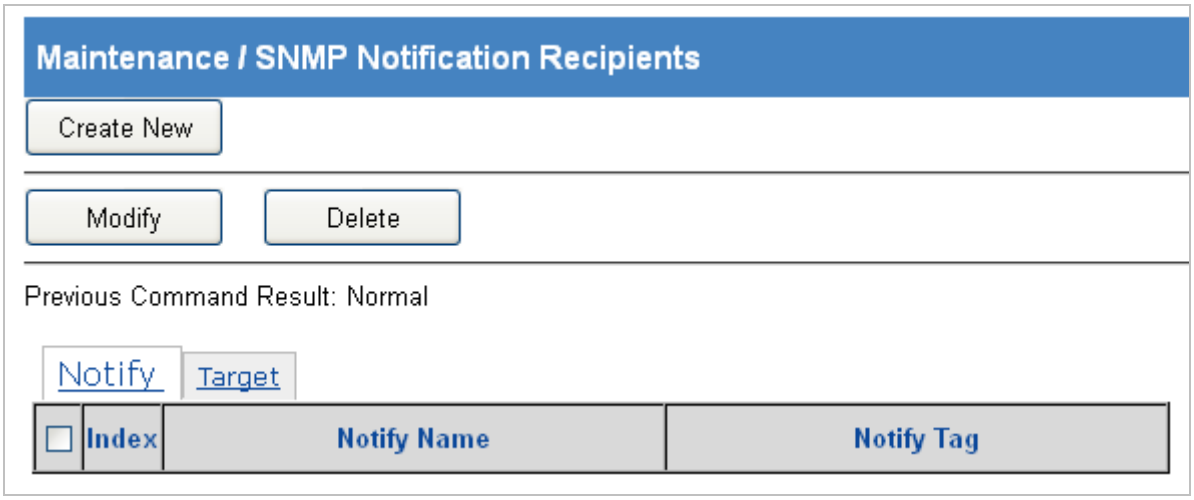


Figure 4-17-13: Maintenance / SNMP Notification Recipients Page Screenshot

Object	Description
• **Operation**	**Create:** Click "Create New" button to create new notify tag. Fill the notify name and notify tag. Click "Apply" to create, "Cancel" to abort. **Modify:** Select entry by check box Modify field data Click "Modify" button to apply change.

•	**Delete:** Select entry by check box Click "Delete" button to delete Notify Tag item.

The page includes the following fields:

Object	Description
• **Index**	SNMP notify tag index, The system supports up to 32 notify tags.
• **Notify Name**	Name of Notify entry. Notify Name max size is 31 characters.
• **Notify Tag**	Notify Tag string. If tag of Target entry matches any tag from tags of Notify Table, then SNMP trap function would work. Notify Tag max size is 31 characters.

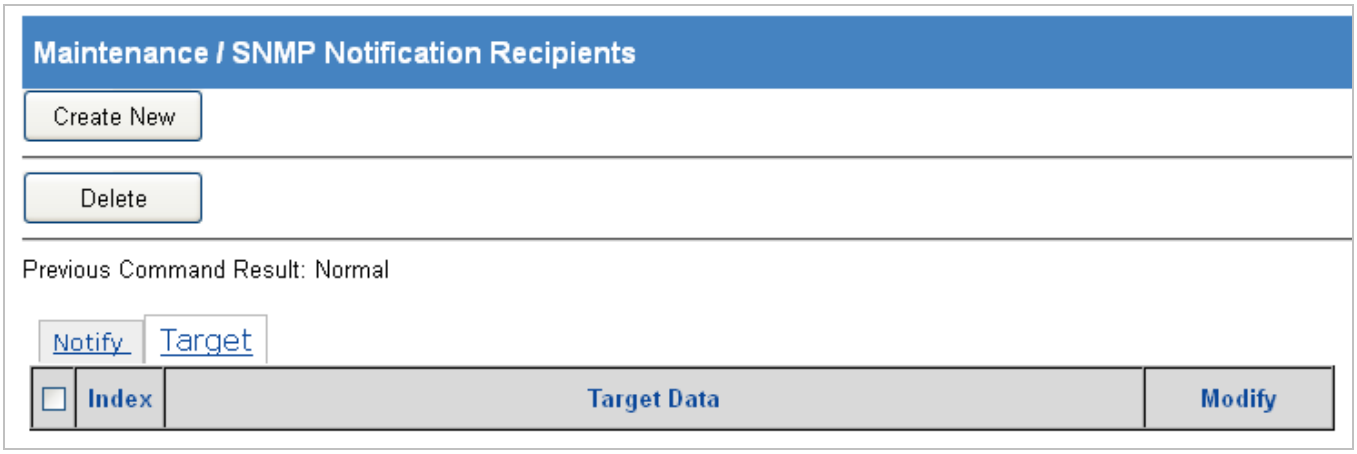


Figure 4-17-14: Maintenance / SNMP Notification Recipients Page Screenshot

Object	Description
• **Operation**	**Create:** Click "Create New" button to create new target data Fill the target IP address, name, port number, and trap version. Give a new tag name or select a existing notify tag name as target name Click "Apply" to create, "Cancel" to abort. **Modify:** Click row item "modify" button to modify existence target data.
•	**Delete:** Select entry by check box, then click "Delete". Note: This page supports multi-selection, click one or more row items to delete. User also could click "select all" to delete all target items.

The page includes the following fields:

Object	Description
• **Index**	SNMP target index, The system supports up to 32 target entries.
• **Target Address**	Target IP address, the host IP address of trap receiver. Value range 0.0.0.0 ~ 255.255.255.255
• **Address Port**	Target Address port number. TCP Port number of Trap receiver. Range: 0 ~ 65535, Default is 162
• **Target Name**	Name of target. Target Name max size is 31 characters.
• **Target Tag**	Add a target tag, or pick up existing notify tag from Notify Table.
• **Trap Version**	Select SNMP trap version. Supports v1/v2c

4.17.11.5 User

Configure SNMPv3 users table on this page. The entry index keys are Engine ID and User Name. The screen in Figure 4-17-15 appears.

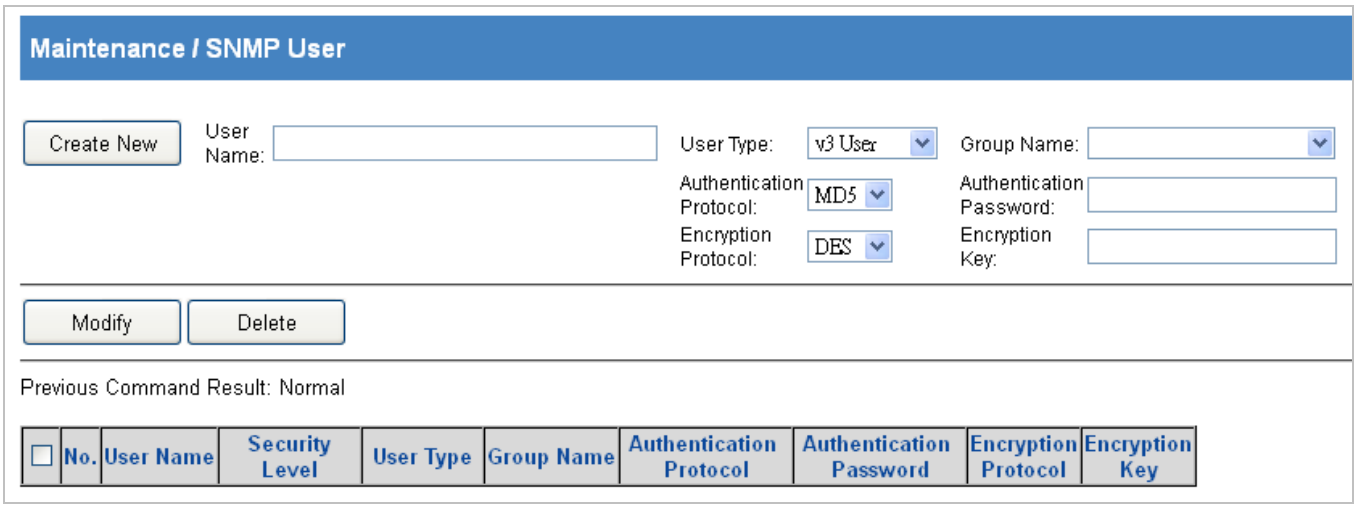


Figure 4-17-15: Maintenance / User Page Screenshot

Object	Description
• **Operation**	**Create new:** Fill "User Name" and select "User Type", "Auth Protocol" and "Priv Protocol". Click "Create New" button to create new user. **Delete:** Select a row data in user account table (also support multi-select). Click "Delete" button to delete user account.

The page includes the following fields:

Object	Description
• **User Name**	User name, length 1~31. Accept any characters except space, quote mark and "?".
• **User Type**	SNMPv3 user type. Options: 1. Read Only 2. Read Write 3. v3 User If "User type" is "v3 User", the "Group Name" should be provided. No matter which User Type is selected, the authentication and Privacy options are allowed.
• **Group Name**	Access Group name, length 1~15. Accept any characters except space, quote mark and "?". If user type is "Read Only" or "Read Write", then this field is not needed.
• **Auth Protocol**	User authentication protocol. Works only if SNMPv3 is enabled. Options: 1. None 2. MD5 3. SHA If "Auth Protocol" is "None", "Priv Protocol" always is "None". If "Auth Protocol" is MD5 or SHA, "Auth Password" should be input.
• **Auth Password**	Authentication password, length 8~15. Works only if SNMPv3 is enabled. Accept any characters except space, quote mark and "?". If Authentication Protocol is "None", then Privacy options are not needed.
• **Priv Protocol**	User Privacy protocol. Works only if SNMPv3 is enabled. If "Priv Protocol" is not "None", "Priv Password" should be input. Options: 1. None 2. DES
• **Priv Password**	Privacy password, length 8~15. Works only if SNMPv3 is enabled. Accept any characters except space, quote mark and "?". If "Priv Protocol" is "None" the field not needed.

4.17.11.6 Group

Configure SNMPv3 groups table on this page. The screen in Figure 4-17-16 appears.

Figure 4-17-16: Maintenance / SNMP Group Page Screenshot

Object	Description
• **Operation**	**Create new:** Fill "Group Name" and select "Sec. Model", "Sec. Level". Click "Create New" button to create new group. Note: max group entry: 32 **Delete :** Select a row data in VACM group table (also support multi-select). Click "Delete" button to delete user account.

The page includes the following fields:

Object	Description
• **Group Name**	Group name, length 1~15. Accept any characters except space, quote mark and "?".
• **Security Model**	SNMP security model. Options: - v1 supports read/write view. - v2c supports read/write view. - v3usm supports read/write view & security level.

• **Security Level**	User security level. If "Security Model" is "v1" or "v2c", the field is not used, it will be show as "--". States as below: - NoAuth, NoPriv (No authentication and no Privacy) - Auth, NoPriv (Authentication and no Privacy) - Auth, Priv (Authentication and Privacy)
• **Read View**	Access View for Read (snmp-get) Select from the view list. If list is empty, create access view with page "SNMP View" first. It will display "unknown(xxxx) when the name of xxxx doesn't exist in view name.
• **Write View**	Access View for Write (snmp-set) Select from the view list. If list is empty, create access view with page "SNMP View" first. It will display "unknown(xxxx) when the name of xxxx doesn't exist in view name.

4.17.11.7 View

Configure SNMPv3 views table on this page. The screen in Figure 4-17-17 appears.

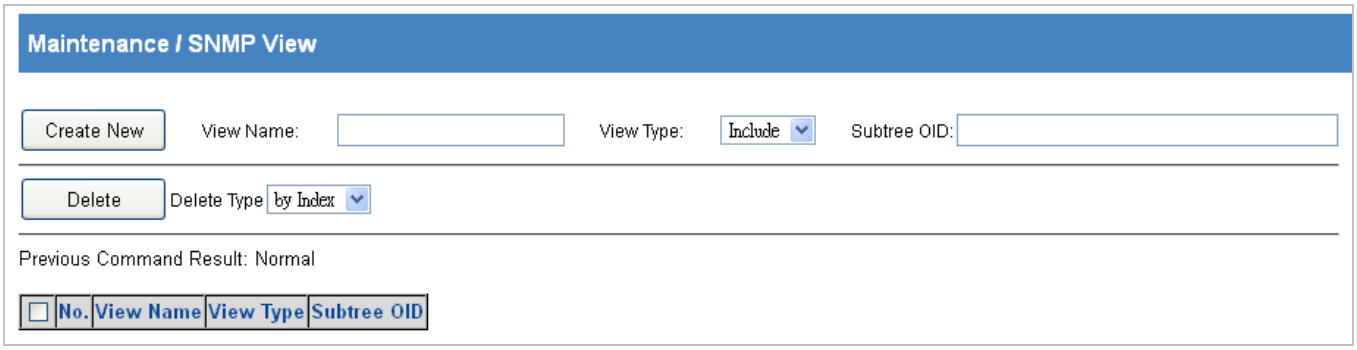


Figure 4-17-17: Maintenance / SNMP View Page Screenshot

Object	Description
• **Operation**	**Create new:** Fill "View Name", "Sub Tree" and select "View Type". Click "Create New" button to create new view. Note: max group entry: 32 **Delete:** Select a row data in VACM view table (also support multi-select). Click "Delete" button to delete user account. VACM View can be delete by Name or by Index. Note that if delete by name, all entries with the same name would be deleted together.

The page includes the following fields:

Object	Description
• **View Name**	View name, length 1~15. Accept any characters except space, quote mark and "?".
• **View Type**	Accessible/Not accessible of object (SNMP OID). Select down list box: 1. Include, allow access the subtree/oid; 2. Exclude, doesn't allow access the subtree/oid. Note: the oid is a prefix, no need to match it exactly. For example: 1.3.6.1.2.1 (include), it means 1.3.6.1.2.1.* are accessible. For example: 1.3.6.1.2.1 (exclude), it means 1.3.6.1.2.1.* are NOT accessible. An example of wildcard(*): 1.3.6.1.*.1 (include), it means that 1.3.6.1.4.1.* are accessible and 1.3.6.1.2.1.* are accessible.
• **Sub Tree**	SNMP OID or Object Name of MIB Input format is OID, char length 1~31. Accept MIB object name "iswitch", or wildcard (*). iswitch represents 1.3.6.1.4.1.5833.2012 For example: 1.3.6.1.2.1 1.3.6.1.4.1.5833.2012 iswitch.1 iswitch.2.6.1.1.*.4 (iswitch.2.6.1.1 is EthernetPort Entry, it means this view include/exclude the 4th port of the table.)

5. COMMAND LINE INTERFACE

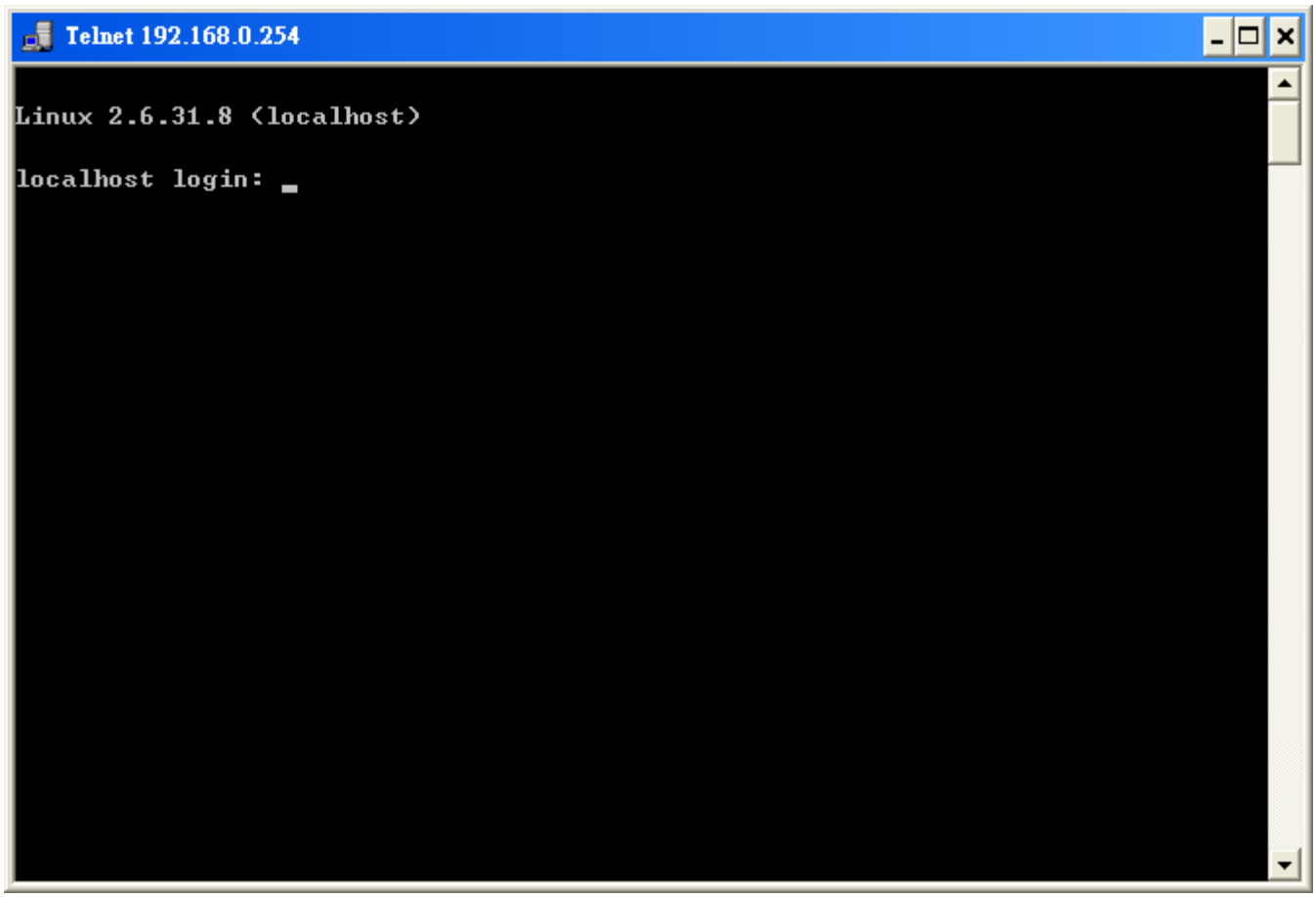
5.1 Accessing the CLI

When accessing the management interface for the **Industrial Managed Switch** via a Telnet connection, the **Industrial Managed Switch** can be managed by entering command keywords and parameters at the prompt. Using the **Industrial Managed Switch**'s command-line interface (CLI) is very similar to entering commands on a UNIX system.

This chapter describes how to use the Command Line Interface (CLI).

5.2 Telnet Login

The **Industrial Managed Switch** supports telnet for remote management. The **Industrial Managed Switch** asks for user name and password for remote login when using telnet, please use **"admin"** for username & password.



5.3 Requirements

- **Workstations** running Windows XP/Vista/7/8/, Windows 2003/2008, MAC OS X or later, Linux, UNIX, or other platforms are compatible with TCP/IP protocols.
- Workstations are installed with Ethernet NIC (Network Interface Card)
- **Serial Port** Connection (Terminal)
  - The above Workstations come with **COM Port** (DB9) or **USB-to-RS232** converter.
  - The above Workstations have been installed with **terminal emulator**, such as Hyper Terminal included in Windows XP/2003.
  - **Serial cable** -- one end is attached to the RS232 serial port, while the other end to the console port of the Managed Switch.
- **Ethernet Port** Connection
  - Network cables -- Use standard network (UTP) cables with RJ45 connectors.

The above PC is installed with Web Browser and JAVA runtime environment plug-in.

5.3 Terminal Setup

To configure the system, connect a serial cable to a **COM port** on a PC or notebook computer and to RJ45 type of serial (console) port of the Managed Switch.

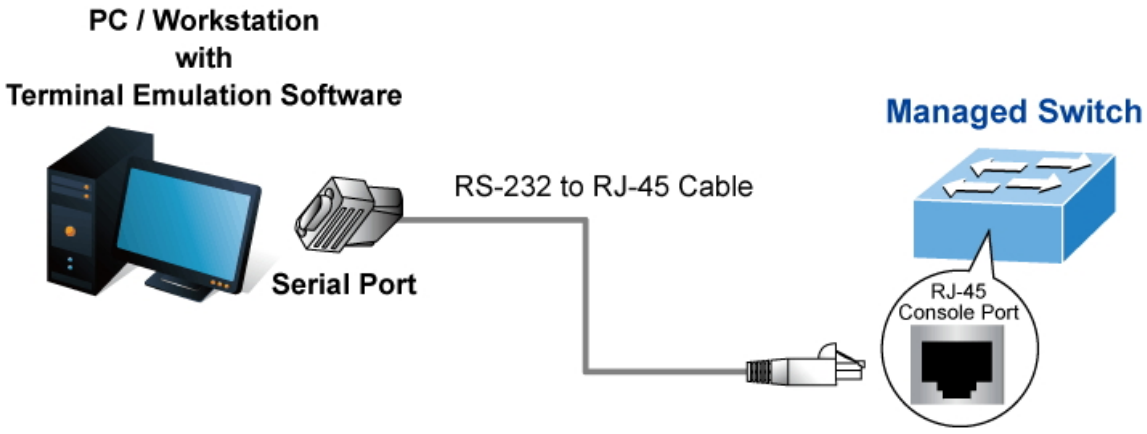


Figure 5-1 Managed Switch Console Connectivity

The console port of the Managed Switch is a RJ45 type, RS232 serial port connector. It is an interface for connecting a terminal directly. Through the console port, it provides rich diagnostic information including IP Address setting, factory reset, port management, link status and system setting. Users can use the attached RS232 cable in the package and connect to the console port on the device. After the connection, users can run any terminal emulation program (Hyper Terminal, ProComm Plus, Telix, Winterm and so on) to enter the startup screen of the device.

IGS-6330-24T4S Front Panel

Figure 5-2: Front Panels of IGS-6330-24T4S

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

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

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

- **Baud : 115200**
- **Data bits : 8**
- **Parity : None**
- **Stop bits : 1**
- **Flow control : None**

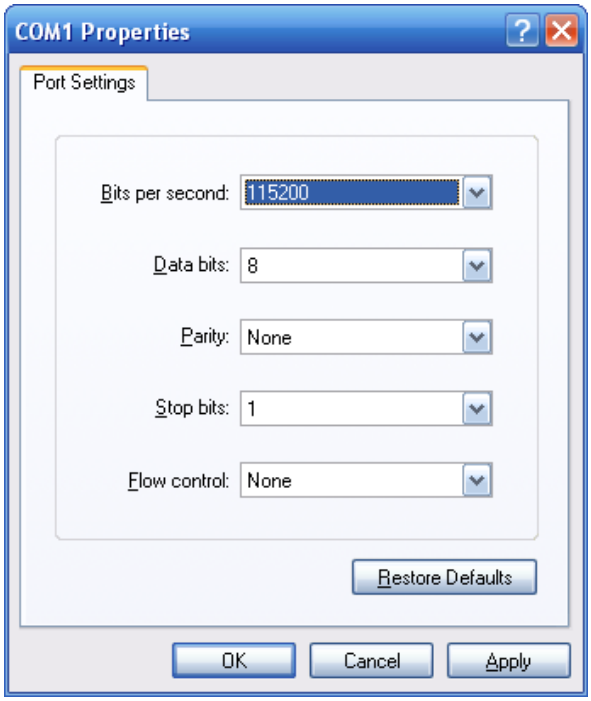


Figure 5-3 Hyper Terminal COM Port Configuration

You can change these settings, if desired, after you log on. This management method is often preferred because you can remain connected and monitor the system during system reboots. Also, certain error messages are sent to the serial port, regardless of the interface through which the associated action was initiated. A Macintosh or PC attachment can use any

terminal-emulation program for connecting to the terminal serial port. A workstation attachment under UNIX can use an emulator such as TIP.

5.4 Logon to the Console

Once the terminal is connected to the device, power on the Managed Switch, and the terminal will display "running testing procedures". Then, the following message asks to log-in user name and password. The factory default user name and password are shown as follows and the login screen in Figure 5-4 appears.

Username: **admin**
Password: **admin**

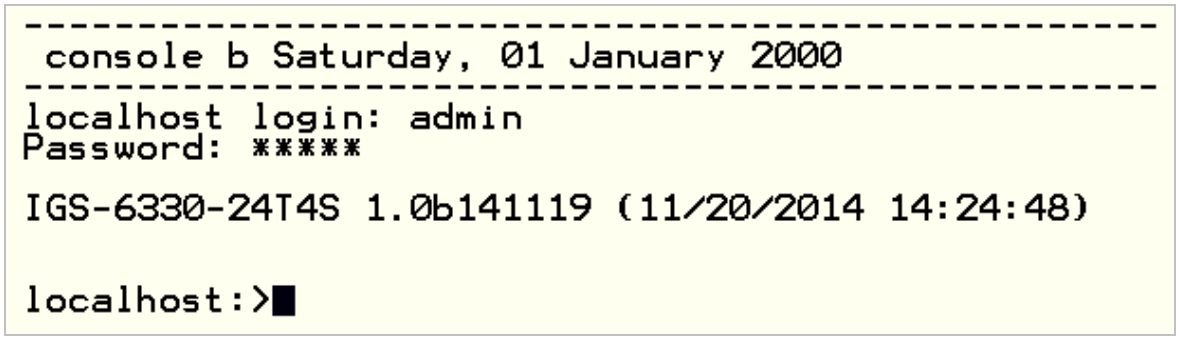


Figure 5-4: Managed Switch Console Login Screen

The user can now enter commands to manage the Managed Switch. For a detailed description of the commands, please refer to the following chapters.

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

5.5 Configuration IP Address

The Managed Switch is shipped with default IP address shown below.

IP Address: **192.168.0.254**
Subnet Mask: **255.255.255.0**

To check the current IP address or modify a new IP address for the Switch, please use the procedures as follows:

■ **Show the current IP Address**

1. At the **"#"** prompt, enter **"show interface vlan 1".**

2. The screen displays the current IP address as shown in Figure 5-5.

```
localhost:(conf)#show interface vlan 1
VLAN interface information of VLAN 1
=============================================================
Interface Setting
        IP Address                              : 192.168.0.254
        Netmask                                 : 255.255.255.0
        Mac                                     : a8:f7:e0:72:f3:3f
-------------------------------------------------------------
localhost:(conf)#
```

Figure 5-5: IP Information Screen

- **Configuring IP Address**

3. At the "#" prompt, enter the following command and press **<Enter>** as shown in Figure 5-6.

```
localhost:>configure
localhost:(conf)#interface vlan 1
localhost:(vlan-intf-conf:1)#ip-address 192.168.1.100 netmask 255.255.255.0
```

The previous command would apply the following settings for the Managed Switch.

IP Address: **192.168.1.100**
Subnet Mask: **255.255.255.0**

```
localhost:>configure
localhost:(conf)#interface vlan 1
localhost:(vlan-intf-conf:1)#ip-address 192.168.1.100 netmask 255.255.255.0
localhost:(vlan-intf-conf:1)#
```

Figure 5-6: Configuring IP Address Screen

4. Repeat step 1 to check if the IP address is changed.

- **Store current switch configuration**

5. At the "**#**" prompt, enter the following command and press **<Enter>.**

```
# runningcfg save
```

```
localhost:>configure
localhost:(conf)#runningcfg save
Writing FLASH ...
Save success.
localhost:(conf)#
```

Figure 5-7: Saving Current Configuration Command Screen

If the IP is successfully configured, the Managed Switch will apply the new IP address setting immediately. You can access the Web interface of the Managed Switch through the new IP address.

Note

If you are not familiar with the console command or the related parameter, enter "**?**" anytime in console to get the help description.

5.6 Command Line Mode

The CLI groups all the commands in appropriate modes according to the nature of the command. A sample of the CLI command modes are described below. Each of the command modes supports specific software commands.

Mode-based Command Hierarchy

The **Command Line Interface (CLI)** groups all the commands in appropriate modes by the nature of the commands. Examples of the CLI command modes are described below. Each of the command modes supports specific switch's commands.

The CLI Command Modes table captures the command modes, the prompts visible in that mode and the exit method from that mode.

Mode	Access Level	Prompt
Init Mode	Guest	**>**
Enable Mode	Guest	**%**
Config Mode	Guest	**(conf)#**
Alarm Profile Config Mode	Adminastor	**(alarm-profile-conf)#**
Gigabit Interface Config Mode	Adminastor	**(gigabit-intf-conf)#**
ACL Profile Config Mode	Adminastor	**(acl-profile-conf)#**
scheduler Profile Config Mode	Adminastor	**(sch-profile-conf)#**
Vlan Interface Config Mode	Adminastor	**(vlan-intf-conf)#**
IGMP MVR Profile Config Mode	Adminastor	**(igmp-mvr-profile-conf)#**
IGMP ACL Profile Config Mode	Adminastor	**(igmp-acl-profile-conf)#**
Ring Group Config Mode	Adminastor	**(ring-group-conf)#**
Trunk Group Config Mode	Adminastor	**(trunk-group-conf)#**
Router Rip Config Mode	Adminastor	**(router-rip-conf)#**
Router Ospf Config Mode	Adminastor	**(router-ospf-conf)#**

Table 5-1 CLI Command Modes

5.7 Terminal Key Function

Following is the list of all the terminal keys and their function.

ENTER	Run a CLI config script
CTRL-M	
TAB	Tab completion.
CTRL-I	If tab is pressed after a non-whitespace character, complete the word before the Tab. If tab is pressed after a whitespace character, complete the next word.
?	Display available commands If ? is pressed after a non-whitespace character, show possible choices for this word. If ? is pressed after a whitespace character, show possible choices for the next word.
<Up Arrow>	Up history
CTRL-P	
<Down Arrow>	Down history
CTRL-N	
Home	Move the cursor to the beginning of the input line
CTRL-A	
End	Move the cursor to the end of the input line
CTRL-E	
<Left Arrow>	Move the cursor backward
CTRL-B	
<Right Arrow>	Move the cursor forward
CTRL-F	
BACKSPACE	Erase the character before the cursor
CTRL-H	

6. COMMAND LINE MODE

6.1 Initialize Mode Commands

bye

Description:

Quit CLI.

Syntax:

bye

!

Description:

Execute the specific number of command in history

Syntax:

! <number>

Parameters:

<number>: **Valid values**: 1 ~ 32

Type: Mandatory

configure

Description:

Enter configuration mode.

Syntax:

configure

enable

Description:

Enter enable mode.

Syntax:

enable

exit

Description:

Exit current mode.

Syntax:

exit

list alarm table detail

Description:

List valid alarm ID

Syntax:

list alarm table detail

list command-tree

Description:

List tree of all available CLI commands

Syntax:

list command-tree

list event table

Description:

List valid event ID

Syntax:

list event table

list execution-modes

Description:

List all available execution modes

Syntax:

list execution-modes

list timezone

Description:

List time zones

Syntax:

list timezone

show env

Description:

Show CLI environment variables

Syntax:

show env

show history

Description:

Show command history (Note: commands issued in one execution mode only appear in history of that execution mode)

Syntax:

show history

show time

Description:

Show current time

Syntax:

show time

show uptime

Description:

Show uptime

Syntax:

Show uptime

show version

Description:

Show version

Syntax:

show version

6.2 Enable Mode Commands

configure

Description:

Enter configuration mode.

Syntax:

configure

disable

Description:

Enter init mode

Syntax:

disable

kick

Description:

Kick off a logged-in user

Syntax:

kick <index> {console | cli | web}

Parameters:

<index>:	**Valid values**: 1 ~ 10
	Type: Mandatory

ping

Description:

send ICMP ECHO_REQUEST to network hosts

Syntax:

ping <ip>

ping <ip> count <count>

ping <ip> count <count> size <size>

ping <ip> size <size>

Parameters:

<ip>	**Valid values**: -
	Type: Mandatory
<count>	Packet count
	Valid values: 1 ~ 4294967295
	Default value: 0
	Type: Mandatory
<size>	The number of data bytes to be sent
	Valid values: 1 ~ 65500
	Default value: 0
	Type: Mandatory

show account

Description:

Show account list.

Syntax:

show account

show aging

Description:

Show aging time for MAC learning table (system-wide).

Syntax:

show aging

show bootloader

Description:

Show boot loader information.

Syntax:

show bootloader

show clisettings

Description:

Show CLI settings.

Syntax:

show clisettings

show cos-queue-mapping

Description:

Show CoS queue mapping configuration.

Syntax:

show cos-queue-mapping

show cpu

Description:

Show CPU information

Syntax:

show cpu

show dot1x

Description:

Show dot1x information

Syntax:

show dot1x

show dot1x eapol-stats {<portNo>|all}

Description:

Show dot1x EAPOL stats.

Syntax:

show dot1x eapol-stats {<portNo>|all}

Parameters:

<portNo>	Gigabit port. **Valid values**: 1 ~ 28 **Type**: Mandatory

show dot1x pae-info-status {<portNo>|all}

Description:

Show dot1x PAE status.

Syntax:

show dot1x pae-info-status {<portNo>|all}

Parameters:

<portNo>	Gigabit port. **Valid values**: 1 ~ 28 **Type**: Mandatory

show dot1x radius-stats

Description:

Show dot1x radius stats.

Syntax:

show dot1x radius-stats

show env

Description:

Show CLI environment variables

Syntax:

show env

show ext-tpid

Description:

Show TPID for the VLAN Tag

Syntax:

show ext-tpid

show fdb

Description:

Show MAC learning table per gigabit port.

Syntax:

show fdb interface gigabit <portNo>

Parameters:

<portNo>	**Valid values**: 1 ~ 28
	Type: Mandatory

show fdb interface trunk-group <number>

Description:

Show forwarding table per trunk group.

Syntax:

show fdb interface trunk-group <number>

Parameters:

<Group number>	**Valid values**: 1 ~ 2
	Type: Mandatory

show fdb vlan <vlanid>

Description:

Show MAC learning table per VLAN index.

Syntax:

Show fdb vlan <vlanid>

Parameters:

<vlanid>	**Valid values**: 1~4094
	Type: Mandatory

show fdb interface trunk-group <number>

Description:

Show forwarding table per trunk group.

Syntax:

show fdb interface trunk-group <number>

Parameters:

<number>	Trunk group.
	Valid values: 1 ~ 2
	Type: Mandatory

show fdbstatic

Description:

Show static MAC forwarding table.

Syntax:

Show fdbstatic

show fdbstatic interface gigabit <portNo>

Description:

Show static MAC forwarding table per gigabit port.

Syntax:

Show fdbstatic interface gigabit <protNo>

Parameters:

<portNo>	**Valid values**: 1 ~ 28
	Type: Mandatory

show fdbstatic vlan <vlanid>

Description:

Show static MAC forwarding table per VLAN index.

Syntax:

show fdbstatic vlan <vlanid>

Parameters:

<vlanid>	**Valid values:** 1~4094
	Type: Mandatory

show firmware status

Description:

Show firmware update status.

Syntax:

show firmware status

show firmware partition

Description:

Show firmware partition information.

Syntax:

show firmware partition

show history

Description:

Show command history (Note: commands issued in one execution mode only appear in history of that execution mode)

Syntax:

show history

show http

Description:

Show HTTP configuration.

Syntax:

show http

show igmp-acl-profile {<number>|all}

Description:

Show IGMP ACL profile

Syntax:

Show profile igmp-acl-profile {<number>|all}

Parameters:

<number>	IGMP ACL profile number.
	Valid values: 1 ~ 15
	Type: Mandatory

show igmp-mvr-profile {<number>|all}

Description:

Show IGMP MVR profile

Syntax:

Show profile igmp-mvr-profile {<number>|all}

Parameters:

<number>	IGMP MVR profile number.
	Valid values: 1 ~ 15
	Type: Mandatory

show interface gigabit all

Description:

Show interface information of all ports

Syntax:

show interface gigabit all

show interface gigabit <portNo>

Description:

Show interface information per gigabit port.

Syntax:

show interface gigabit <portNo>

Parameters:

<portNo>	**Valid values**: 1 ~ 28
	Type: Mandatory

show interface gigabit <portNo> acl

Description:

Show ACL profile per gigabit port.

Syntax:

show interface gigabit <portNo> acl

Parameters:

<portNo>	**Valid values**: 1 ~ 28
	Type: Mandatory

show interface gigabit <portNo> counter

Description:

Show Ethernet counter per gigabit port.

Syntax:

show interface gigabit <portNo> counter

Parameters:

<portNo>	**Valid values**: 1 ~ 28
	Type: Mandatory
counter	Show Gigabit Ethernet counter.

show interface gigabit <portNo> igmp

Description:

Show IGMP information per port.

Syntax:

show interface gigabit <portNo> igmp

Parameters:

<portNo>	Gigabit port.
	Valid values: 1 ~ 28
	Type: Mandatory

show interface gigabit <portNo> msti

Description:

Show MSTI info for specific gigabit.

Syntax:

show interface gigabit <portNo> msti

show interface gigabit <portNo> port-isolation

Description:

Show isolation information per gigabit port.

Syntax:

show interface gigabit <portNo> port-isolation

Parameters:

<portNo>	**Valid values**: 1 ~ 28
	Type: Mandatory

show interface gigabit <portNo> qos

Description:

Show QoS per gigabit port.

Syntax:

show interface gigabit <portNo> qos

Parameters:

<portNo>	**Valid values**: 1 ~ 28
	Type: Mandatory

show interface gigabit <portNo> rmon-counter

Description:

Show Ethernet counter per gigabit port.

Syntax:

show interface gigabit <portNo> rmon-counter

Parameters:

<portNo>	**Valid values**: 1~28.
	Type: Mandatory

show interface gigabit <portNo> storm-control

Description:

Show storm control information per gigabit port.

Syntax:

show interface gigabit <portNo> storm-control

Parameters:

<portNo>	**Valid values**: 1~28
	Type: Mandatory

show interface gigabit <portNo> stp

Description:

Show STP information per gigabit port.

Syntax:

show interface gigabit <portNo> stp

Parameters:

<portNo>	**Valid values**: 1 ~ 28
	Type: Mandatory
stp	Show STP port information.

show interface gigabit <portNo> vlan

Description:

Show VLAN information of a port

Syntax:

show interface gigabit <portNo> vlan

Parameters:

<portNo>	**Valid values**: 1 ~ 28
	Type: Mandatory
vlan	Show VLAN information.

show interface trunk-group

Description:

show trunk group information.

Syntax:

show interface trunk-group

show interface vlan

Description:

Show VLAN interface information of all VLANs.

Syntax:

show interface vlan

show interface vlan igmp

Description:

Show IGMP information.

Syntax:

show interface vlan igmp

show interface vlan <vlanid>

Description:

Show VLAN interface information of specify VLAN.

Syntax:

show interface vlan <vlanid>

Parameters:

<vlanid>	VLAN ID.
	Valid values: 1 ~ 4094
	Type: Mandatory

show interface vlan <vlanid> igmp

Description:

Show IGMP information per vlan

Syntax:

show interface vlan <vlanid> igmp

Parameters:

<vlanid>	VLAN ID.
	Valid values: 1 ~ 4094
	Type: Mandatory

show jumboframe

Description:

Show jumbo frame settings.

Syntax:

show jumboframe

show login-users

Description:

Show logged-in users.

Syntax:

show login-users

show multicast-fdb

Description:

Show IGMP VLAN multicast forwarding table.

Syntax:

show multicast-fdb

show multicast-fdb vlan <vlanid>

show multicast-fdb interface gigabit <portNo>

Parameters:

<vlanid>	**Valid values**: 1~4094.
	Type: Optional
<portNo>	**Valid values**: 1~28.
	Type: Optional

show multicast-fdb srclist

Description:

Show multicast source list table.

Syntax:

show multicast-fdb srclist

show multicast-fdb static

Description:

Show IGMP VLAN static multicast forwarding table.

Syntax:

show multicast-fdb static

show multicast-fdb static vlan <vlanid>

show multicast-fdb static interface gigabit <portNo>

Parameters:

<vlanid>	**Valid values**: 1~4094.
	Type: Optional
<portNo>	**Valid values**: 1~28.
	Type: Optional

show policer

Description:

Show ingress policer table.

Syntax:

show policer

show port-isolation

Description:

Show all port isolation information.

Syntax:

show port-isolation

show port-mirror

Description:

Show port mirror information.

Syntax:

show port-mirror

show port-shaper

Description:

Show port shaper information.

Syntax:

show port-shaper

show profile acl {<number>|all}

Description:

Show ACL profile detail information.

Syntax:

show profile acl {<number>|all}.

Parameters:

<number>	**Valid values**: 1 ~ 20
	Type: Mandatory
all	Show all ACL profile.

show protocol-vlan

Description:

Show protocol based VLAN information for all entries.

Syntax:

show protocol-vlan

show queue-scheduler profile

Description:

Show scheduler profile table.

Syntax:

show queue-scheduler profile

show queue-shaper

Description:

Show queue shaper information.

Syntax:

show queue-shaper

show runningcfg

Description:

Show running configuration.

Syntax:

show runningcfg

show runningcfg default

Description:

Show default running configuration.

Syntax:

show runningcfg default

show runningcfg backup

Description:

Show running configuration backup.

Syntax:

show runningcfg backup

show sntp

Description:

Show SNTP information.

Syntax:

show sntp

show ssl decrypted

Description:

Show ssl certificate with decrypted format.

Syntax:

show ssl decrypted

show ssl encrypted

Description:

Show ssl certificate with encrypted format.

Syntax:

show ssl encrypted

show stp

Description:

System Wide Spanning Tree Setting/Status.

Syntax:

show stp

show syslog

Description:

Show syslog configuration.

Syntax:

show syslog

show system information

Description:

Show system information.

Syntax:

show system information

show system inventory

Description:

Show system inventory.

Syntax:

show system inventory

show time

Description:

Show current time.

Syntax:

Show time

show topology-ring

Description:

Show neighbor device information, the MAC address and connected port numbers.

Syntax:

show topology-ring

show uptime

Description:

Show uptime

Syntax:

show uptime

show version

Description:

Show version information.

Syntax:

show version

show vlan

Description:

Show bridge port memberset/status.

Syntax:

show vlan

show vlan <vlanid>

Description:

Show bridge port member set/status per VLAN index (1~4094).

Syntax:

show vlan <vlanid>

Parameters:

<vlanid>	**Valid values**: 1~4094
	Type: Mandatory.

show vlan {unknown-uc|unknown-mc|broadcast}

Description:

Show storm control information by VLAN.

Syntax:

show vlan unknown-uc

show vlan unknown-mc

show vlan broadcast

Parameters:

unknown-uc	Show unknown unicast storm control information by VLAN.
	Type: Mandatory
unknown-mc	Show unknown multicast storm control information by VLAN.
	Type: Mandatory

broadcast	Show broadcast storm control information by VLAN. **Type**: Mandatory

show vlan-trans

Description:

Show VLAN translation table for all

Syntax:

show vlan-trans

show route static

Description:

Show routing static table.

Syntax:

show route static

show http

Description:

show http and https information.

Syntax:

show http

6.3 Configure Mode Commands

interface gigabit <portNo>

Description:

Gigabit Ethernet interface. (enter gigabit interface mode)

Syntax:

interface gigabit <portNo>

Parameters:

<portNo> **Valid values**: 1 ~ 28

Type: Mandatory

interface vlan <vlanid>

Description:

Vlan Ethernet interface (enter mode of interface vlan)

Syntax:

interface vlan <vlanid>

Parameters:

<vlanid> **Valid values**: 1 ~ 4094

Type: Mandatory

profile acl

Description:

Enter Acl Profile Config Mode

Syntax:

profile acl

profile sch

Description:

Enter Scheduling Profile Config Mode

Syntax:

profile sch

sntp polling-interval <interval>

Description:

Set SNTP Polling interval.

Syntax:

sntp polling-interval <interval>

Parameters:

<interval>	**Valid values**: 60 ~ 65535 seconds, 0: disable polling
	Type: Mandatory

sntp server address <ip>

Description:

Set SNTP server address.

Syntax:

sntp server address <ip>

Parameters:

<ip>	**Type**: Mandatory

sntp sync

Description:

Manual SNTP synchronization.

Syntax:

sntp sync

time set timezone

Description:

Set time zone.

Syntax:

time set timezone <timezone>

time set timezone default

Parameters:

<timezone>	**Valid values**: please see 'list timezone'
	Type: Mandatory

default	Set time zone to default (GMT/UTC).
	Type: Mandatory

time set {date|time}

Description:

Set date/time.

Syntax:

time set date <month> <day> <year>

time set time <hour> <minute>

time set time <hour> <minute> <second>

Parameters:

<month>	**Valid values**: 1 ~ 12
	Type: Mandatory
<day>	**Valid values**: 1 ~ 31
	Type: Mandatory
<year>	**Valid values**: 0 ~ 36
	Type: Mandatory
<hour>	**Valid values**: 0 ~ 23
	Type: Mandatory
<minute>	**Valid values**: 0 ~ 59
	Type: Mandatory
<second>	**Valid values**: 0 ~ 59
	Type: Optional

account add <username>

Description:

Add an account.

Syntax:

account add <username>

account add <username> password <password>

account add <username> password <password> comment <comment>

account add <username> password <password> level <account_level>

account add <username> password <password> level <account_level> comment <comment>

Parameters:

<username>	**Valid values**: 1 ~ 31 characters
	Type: Mandatory
<password>	**Valid values**: 0 ~ 31 characters
	Type: Mandatory
<account_level>	**Valid values**:
	superuser
	engineer
	guest
	Type: Mandatory
<comment>	**Valid values**: 0 ~ 31 characters
	Type: Mandatory

account delete <username>

Description:

Delete an account.

Syntax:

account delete <username>

Parameters:

<username>	**Valid values**: 1 ~ 31 characters
	Type: Mandatory

account modify <username>

Description:

Modify an account

Syntax:

account modify <username>

account modify <username> comment <comment>

account modify <username> level <account_level>

account modify <username> level <account_level> comment <comment>

account modify <username> password <password>

account modify <username> password <password> comment <comment>

account modify <username> password <password> level <account_level>

account modify <username> password <password> level <account_level> comment <comment>

Parameters:

<username>	**Valid values**: 1 ~ 31 characters
	Type: Mandatory
<password>	**Valid values**: 0 ~ 31 characters
	Type: Mandatory
<account_level>	**Valid values**:
	dsuperuser
	engineer
	guest
	Type: Mandatory
<comment>	**Valid values**: 0 ~ 31 characters
	Type: Mandatory

kick <index> { cli|console|web}

Description:

Kick off a logged-in user.

Syntax:

kick <index> cli

kick <index> console

kick <index> web

Parameters:

<index>	**Valid values**: 1 ~ 10
	Type: Mandatory

syslog server <ip>

Description:

Configure syslog server IP address.

Syntax:

syslog server <ip>

Parameters:

<ip>	Syslog server IP address.
	Type: Mandatory

syslog {enable|disable}

Description:

Disable or enable syslog service.

Syntax:

syslog enable

syslog disable

clisettings <timeout>

Description:

Configure CLI settings.

Syntax:

clisettings <timeout>

clisettings <timeout> <flag>

clisettings <timeout> <flag> <maxSessions>

Parameters:

<timeout>	**Valid values**: 60 ~ 65535 seconds, 0: no timeout
	Type: Mandatory
<flag>	**Valid values**: bitmap
	showAlarm(0)
	showEvent(1)
	showReadWriteStatus(2)
	Type: Optional
<maxSessions>	**Valid values**: 1 ~ 10 sessions
	Type: Mandatory

runningcfg clear

Description:

Clear configuration.

Syntax:

runningcfg clear all

runningcfg clear all noreboot

runningcfg clear general

runningcfg clear general noreboot

Parameters:

all	Clear all configuration.
	Type: Mandatory
general	Clear general configuration.
	Type: Mandatory
noreboot	Clear configuration without Reboot.
	Must reboot system manually for the changes to take effect!
	Type: Optional

runningcfg get <ip> <username> <password> {binary|cli} <string>

Description:

Get exported configuration files from a FTP server.

Syntax:

runningcfg get <ip> <username> <password> binary <string>

runningcfg get <ip> <username> <password> cli <string>

Parameters:

<ip>	**Type**: Mandatory
<username>	**Valid values**: 1 ~ 32 characters
	Type: Mandatory
<password>	**Valid values**: 1 ~ 32 characters
	Type: Mandatory
binary	Get two binary images.
	Type: Mandatory
cli	Get two CLI scripts.
	Type: Mandatory
<string>	Remote filename prefix.
	Valid values: 1 ~ 64 characters
	Type: Mandatory

runningcfg import download

Description:

Import configuration from files retrieved via 'runningcfg get'.

Syntax:

runningcfg import download binary

runningcfg import download binary noreboot

runningcfg import download cli

runningcfg import download cli noreboot

Parameters:

binary	Import configuration from binary images retrieved via 'runningcfg get'.
	Type: Mandatory
cli	Import configuration from the CLI scripts retrieved via 'runningcfg get'.
	Type: Mandatory
Noreboot	Import configuration without Reboot.
	Must reboot system manually for the changes to take effect!
	Type: Optional

runningcfg put <ip> <username> <password> {binary|cli} <string>

Description:

Put exported configuration files to a FTP server.

Syntax:

runningcfg put <ip> <username> <password> binary <string>

runningcfg put <ip> <username> <password> cli <string>

Parameters:

<ip>	**Type**: Mandatory
<username>	**Valid values**: 1 ~ 32 characters
	Type: Mandatory
<password>	**Valid values**: 1 ~ 32 characters
	Type: Mandatory
binary	Put two binary images.
	Type: Mandatory
cli	Put CLI scripts.
	Type: Mandatory
<string>	Remote filename prefix.
	Valid values: 1 ~ 64 characters
	Type: Mandatory

runningcfg replace-save <inbandBackupIndex>

Description:

Save running config to FLASH replacing existing the specified backup.

Syntax:

runningcfg replace-save <inbandBackupIndex>

runningcfg replace-save <inbandBackupIndex> <inbandBackupName>

runningcfg replace-save <inbandBackupIndex> <inbandBackupName> <generalBackupIndex>

runningcfg replace-save <inbandBackupIndex> <inbandBackupName> <generalBackupIndex> <generalBackupName>

Parameters:

<inbandBackupIndex>	**Valid values**: 1 ~ 16
	Type: Mandatory
<inbandBackupName>	**Valid values**: 1 ~ 31 characters
	Type: Optional
<generalBackupIndex>	**Valid values**: 1 ~ 16
	Type: Optional
<generalBackupName>	**Valid values**: 1 ~ 31 characters
	Type: Optional

runningcfg restore index <inbandBackupIndex>

Description:

Restore configuration.

Syntax:

runningcfg restore index <inbandBackupIndex>

runningcfg restore index <inbandBackupIndex> <generalBackupIndex>

runningcfg restore index <inbandBackupIndex> <generalBackupIndex> noreboot

Parameters:

<inbandBackupIndex>	**Valid values**: 1 ~ 16
	Type: Mandatory
<generalBackupIndex>	**Valid values**: 1 ~ 16
	Type: Optional (if omitted, use the same index as <inbandBackupIndex>)
noreboot	Restore database without reboot.
	Must reboot system manually for the changes to take effect!
	Type: Optional

runningcfg restore name <inbandBackupName>

Description:

Restore configuration.

Syntax:

runningcfg restore name <inbandBackupName>

runningcfg restore name <inbandBackupName> <generalBackupName>

runningcfg restore name <inbandBackupName> <generalBackupName> noreboot

Parameters:

<inbandBackupName>	**Valid values**: 1 ~ 31 characters
	Type: Mandatory
<generalBackupName>	**Valid values**: 1 ~ 31 characters
	Type: Optional (if omitted, use the same name as <inbandBackupName>)
noreboot	Restore database without reboot.
	Must reboot system manually for the changes to take effect!
	Type: Optional

runningcfg save

Description:

Save running config to FLASH.

Syntax:

runningcfg save

runningcfg save <inbandBackupName>

runningcfg save <inbandBackupName> <generalBackupName>

Parameters:

<inbandBackupName>	**Valid values**: 1 ~ 31 characters
	Type: Optional
<generalBackupName>	**Valid values**: 1 ~ 31 characters
	Type: Optional (if omitted, use the same name as <inbandBackupName>)

firmware partition <partition>

Description:

Set boot partition.

Syntax:

firmware partition <partition>

Parameters:

<partition>	**Valid values**: 0 ~ 1
	Type: Mandatory

firmware write

Description:

Perform Remote Download.

Schedule a remote download (scheduled upgrade).

Cancel a scheduled upgrade.

Syntax:

firmware write <ip> <username> <password> <string> {bootloader| image}

firmware write <ip> <username> <password> <string> {bootloader| image} {noreboot|<time>}

firmware write <ip> <username> <password> <string> {bootloader| image} noreboot <time>

firmware write cancel

Parameters:

<ip>	**Type**: Mandatory
<username>	**Valid values**: 1 ~ 32 characters
	Type: Mandatory
<password>	**Valid values**: 0 ~ 32 characters
	Type: Mandatory
<string>	Image path and filename.
	Valid values: 1 ~ 64 characters
	Type: Mandatory
image	Perform remote download for the software image.
	Type: Mandatory
bootloader	Perform remote download for the boot loader.
	Type: Mandatory
noreboot	Perform Remote Download without Reboot.
	Must reboot system manually for the changes to take effect!
	Type: Optional
<noreboot>	Time for scheduled upgrade.
	(MM/DD/YYYY HH:MM:SS)
	Type: Optional
cancel	Cancel scheduled upgrade.
	Type: Mandatory

system restart

Description:

Restart system.

Syntax:

system restart

system restart <time>

Parameters:

<time>	Time for scheduled restart.
	(MM/DD/YYYY HH:MM:SS)
	Type: Optional

system restart cancel

Description:

Cancel a previously-scheduled system restart.

Syntax:

system restart cancel

route add <network> netmask <netmask> gateway <gateway>

Description:

Add a route

Syntax:

route add <network> netmask <netmask> gateway <gateway>

Parameters:

<network>	Destination network address.
	Type: Mandatory
<netmask>	**Type**: Mandatory
<gateway>	**Type**: Mandatory

route delete <network> netmask <netmask>

Description:

Delete a route.

Syntax:

route delete <network> netmask <netmask>

Parameters:

<network>	Destination network address.
	Type: Mandatory
<netmask>	**Type**: Mandatory

default-gateway <default_gateway>

Description:

Configure default gateway IP address.

Syntax:

default-gateway <default_gateway>

Parameters:

<default_gateway>	**Type**: Mandatory

ip-address <ip>

Description:

Configure IP address / netmask / gateway.

Syntax:

ip-address <ip>

ip-address <ip> netmask <netmask>

ip-address <ip> netmask <netmask> <default_gateway>

Parameters:

<ip>	**Type**: Mandatory
<netmask>	**Type**: Optional
<default_gateway>	**Type**: Optional

default all

Description:

Set all configurations to default.

Syntax:

default all

default all except account

Parameters:

except account	Set all configurations to default except user account.
	Type: Mandatory

list timezone

Description:

List timezones.

Syntax:

list timezone

system-info contact <string>

Description:

Modify system contact.

Syntax:

system-info contact <string>

Parameters:

<string>	**Valid values**: 0 ~ 255 characters (ASCII code: 0x20 - 0x7E)
	Type: Mandatory

system-info location <string>

Description:

Modify system location.

Syntax:

system-info location <string>

Parameters:

<string>	**Valid values**: 0 ~ 255 characters (ASCII code: 0x20 - 0x7E)
	Type: Mandatory

system-info name <string>

Description:

Modify system name.

Syntax:

system-info name <string>

Parameters:

<string>	**Valid values**: 1 ~ 255 characters (ASCII code: 0x21 - 0x7E)
	Type: Mandatory

http port {<portNo>|default}

Description:

Set HTTP server port.

Syntax:

http port <portNo>

http port default

Parameters:

<portNo>	**Valid values**: 1 ~ 65535
	Type: Mandatory
default	Set http server port to default (80)
	Type: Mandatory

temperature shift down <time>

Description:

Set downshift time.

Syntax:

temperature shift down <time>

Parameters:

<timer> **Valid values**: 1 ~ 255 seconds

Type: Mandatory

temperature shift up <time>

Description:

Set upshift time.

Syntax:

temperature shift up <time>

Parameters:

<timer> **Valid values**: 1 ~ 255 seconds

Type: Mandatory

temperature threshold down <threshold>

Description:

Set downshift temperature threshold.

Syntax:

temperature threshold down <threshold>

Parameters:

<threshold> **Valid values**: -55 ~ 85 degrees Centigrade

Type: Mandatory

temperature threshold up <threshold>

Description:

Set upshift temperature threshold.

Syntax:

temperature threshold up <threshold>

Parameters:

<threshold> **Valid values**: -55 ~ 85 degrees Centigrade

Type: Mandatory

vlan <vlanid>

Description:

Configure VLAN.

Syntax:

vlan <vlanid>

Parameters:

<vlanid> Create an empty VLAN index.

Valid values: 1 ~ 4094

Type: Mandatory

vlan <vlanid> <name>

Description:

Configure VLAN's name.

Syntax:

vlan <vlanid> <name>

Parameters:

<vlanid> Create an empty VLAN index.

Valid values: 1 ~ 4094

Type: Mandatory

vlan disable <vlanid>

Description:

Delete VLAN memberset/setting.

Syntax:

vlan disable <vlanid>

Parameters:

<vlanid> **Valid values**: 1 ~ 4094

Type: Mandatory

aging <time>

Description:

Configure aging time for a bridge port.

Syntax:

aging <time>

Parameters:

<time> **Valid values**: 10 ~ 1000000 (seconds)

Type: Mandatory

fdb-delete all

Description:

Delete all dynamic entries from forwarding table.

Syntax:

fdb-delete all

Parameters:

all Delete all dynamic FDB entries.

Type: Mandatory

fdb-delete interface gigabit <portNo>

Description:

Delete Forwarding table entries per gigabit port.

Syntax:

fdb-delete interface gigabit <portNo>

Parameters:

<portNo> **Valid values**: 1~ 28

Type: Mandatory

fdb-delete vlan <vlanid>

Description:

Delete forwarding table entries per VLAN index.

Syntax:

fdb-delete vlan <vlanid>

Parameters:

<vlanid> **Valid values**: 1~4094

Type: Mandatory

fdbstatic <number> interface gigabit <portNo> <vlanid><mac>

Description:

Create static MAC forwarding table entry.

Syntax:

fdbstatic <number> interface gigabit<portNo><vlanid><mac>

Parameters:

<number> Entry position.

Valid values: 1~512

Type: Mandatory

<portNo> **Valid values**: 1~28

Type: Mandatory

<vlanid> **Valid values**: 1~4094

Type: Mandatory

<mac> **Valid values**: xx:xx:xx:xx:xx:xx

Type: Mandatory

fdbstatic delete <number>

Description:

Delete static MAC forwarding table entry.

Syntax:

fdbstatic delete <number>

Parameters:

<number> **Valid values**: 1~512

Type: Mandatory

fdbstatic delete all

Description:

Delete all entries of static MAC forwarding table.

Syntax:

fdbstatic delete all

fdbstatic delete interface gigabit <portNo>

Description:

Delete static MAC forwarding table entry per gigabit port.

Syntax:

fdbstatic delete interface gigabit <portNo>

Parameters:

<portNo> **Valid values**: 1~28

Type: Mandatory

fdbstatic delete vlan <vlanid>

Description:

Delete static MAC forwarding table entry per VLAN index.

Syntax:

fdbstatic delete vlan <vlanid>

Parameters:

<vlanid> **Valid values**: 1~4094

Type: Mandatory

stp {disable|enable}

Description:

Configure spanning tree protocol settings.

Syntax:

stp {disable|enable}

Parameters:

disable	Disable STP.

stp bpdu {deny|flooding}

Description:

Set BPDU packet filter (deny/flooding).

Syntax:

stp bpdu {deny|flooding}

Parameters:

deny	Deny BPDU packet.
flooding	Flood BPDU packet.

stp forward-delay <number>

Description:

Set STP forward delay time.

Syntax:

stp forward-delay <number>

Parameters:

<number>	**Valid values**: 4 ~ 30 (seconds) **Type**: Mandatory

stp hello-time <number>

Description:

Set STP hello time.

Syntax:

stp hello-time <number>

Parameters:

<number> **Valid values**: 1 ~ 10 (seconds)

Type: Mandatory

stp max-age <number>

Description:

Set STP max age value.

Syntax:

stp max-age <number>

Parameters:

<number> **Valid values**: 6 ~ 40 (seconds)

Type: Mandatory

stp priority <number>

Description:

Set STP priority.

Syntax:

stp priority <number>

Parameters:

<number> **Valid values**: 0 ~ 61440 step 4096

Type: Mandatory

stp version {stp|rstp}

Description:

Set STP version.

Syntax:

stp version {stp|rstp}

Parameters:

stp	Spanning tree protocol.
rstp	Rapid spanning tree protocol.

jumboframe {enable|disable}

Description:

Set jumbo frame settings.

Syntax:

jumboframe {enable|disable}

Parameters:

enable	Enable jumbo frame.
disable	Disable jumbo frame.

jumboframe mtu <value>

Description:

MTU size.

Syntax:

jumboframe mtu <value>

Parameters:

<value>	Range. **Valid values**: 1536~9000 (bytes) **Type**: Mandatory

cos-queue-mapping cos <cos-number> queue <queue-number>

Description:

Set CoS and queue mapping.

Syntax:

cos-queue-mapping cos <cos-number> queue <queue-number>

Parameters:

<cos-number>	**Valid values**: 0~7
	Type: Mandatory
<queue-number>	**Valid values**: 0~7
	Type: Mandatory

policer cos-mark green <green-number> yellow <yellow-number> red <red-number>

Description:

Set ingress policer CoS remark mapping table.

Syntax:

policer cos-mark green <green-number> yellow <yellow-number> red <red-number>

Parameters:

<green-number>	Color green and CoS number mapping.
	Valid values: 0~7 **Type**: Mandatory
<yellow-number>	Color yellow and CoS number mapping.
	Valid values: 0~7 **Type**: Mandatory
<red-number>	Color red and CoS number mapping.
	Valid values: 0~7 **Type**: Mandatory

policer dscp-mark green <green-number> yellow <yellow-number> red <red-number>

Description:

Set ingress policer DSCP remark mapping table.

Syntax:

policer dscp-mark green <green-number> yellow <yellow-number> red <red-number>

Parameters:

<green-number>	Color green and DSCP number mapping.
	Valid values: 0~63 **Type**: Mandatory
<yellow-number>	Color yellow and DSCP number mapping.
	Valid values: 0~63 **Type**: Mandatory
<red-number>	Color red and DSCP number mapping.
	Valid values: 0~63 **Type**: Mandatory

policer ingress-color {aware|blind}

Description:

Enable/Disable ingress-color function.

Syntax:

policer ingress-color {aware|blind}

Parameters:

aware	Enable ingress color function.
blind	Disable ingress color function.

policer ingress-color cos <number> {red|yellow|green}

Description:

Set ingress-color mapping table.

Syntax:

policer ingress-color cos <number> {green|yellow|red}

Parameters:

<number>	**Valid values**: 0~7
	Type: Mandatory
green|yellow|red	Green or yellow or red.
	Type: Mandatory

mirror analyzer-port {enable|disable}

Description:

Enable/Disable analyzer port configuration.

Syntax:

mirror analyzer-port {enable|disable}

Parameters:

enable	Enable port mirror.
disable	Disable port mirror.

mirror analyzer-port <portNo>

Description:

Set analyzer port.

Syntax:

mirror analyzer-port <portNo>

Parameters:

<portNo>	**Valid values**: 1~28
	Type: Mandatory

vlan <vlanid> unknown-uc {blcok|forward}

Description:

Block/ Forward unknown unicast packet per VLAN.

Syntax:

vlan <vlanid> unknown-uc block

vlan <vlanid> unknown-uc forward

Parameters:

<vlanid>	**Valid values**: 1~4094
	Type: Mandatory

vlan <vlanid> unknown-mc {block|forward}

Description:

Block/Forward unknown multicast packet per VLAN.

Syntax:

vlan <vlanid> unknown-mc block

vlan <vlanid> unknown-mc forward

Parameters:

<vlanid> **Valid values**: 1~4094

Type: Mandatory

vlan <vlanid> broadcast {block|forward}

Description:

Block/Forward broadcast packet per VLAN.

Syntax:

vlan <vlanid> broadcast block

vlan <vlanid> broadcast forward

Parameters:

<vlanid> **Valid values**: 1~4094

Type: Mandatory

port-mirror monitor-port <portNo>

Description:

Set the gigabit port to be monitored.

Syntax:

port-mirror monitor-port <portNo>

Parameters:

<portNo> **Valid values**: 1~28

Type: Mandatory

port-mirror {enable|disable}

Description:

Enable/Disable port mirror.

Syntax:

port-mirror enable

port-mirror disable

port-mirror {tx-analyzer-port|rx-analyzer-port} <portNo>

Description:

Set Tx analyzer port (monitor 'out' packet of monitored port)/Rx analyzer port (monitor 'in' packet of monitored port).

Syntax:

port-mirror tx-analyzer-port <portNo>

port-mirror rx-analyzer-port <portNo>

Parameters:

<portNo> **Valid values**: 1~28

Type: Mandatory

counter interface-counter clear <portNo>

Description:

Clear interface counter per gigabit port.

Syntax:

counter interface-counter clear <portNo>

Parameters:

<portNo> **Valid values**: 1~28.

Type: Mandatory

counter rmon-counter clear <portNo>

Description:

Clear Ethernet counter per gigabit port.

Syntax:

counter rmon-counter clear <portNo>

Parameters:

<portNo> **Valid values**: 1~28.

Type: Mandatory

multicast-fdb delete all

Description:

Delete multicast forwarding table.

Syntax:

multicast-fdb delete all

multicast-fdb delete vlan <vlanid>

multicast-fdb delete interface gigabit <portNo>

Parameters:

<vlanid>	**Valid values**: 1~4094.
	Type: Mandatory
<portNo>	**Valid values**: 1~28.
	Type: Mandatory

multicast-fdb static delete

Description:

Delete static multicast forwarding table.

Syntax:

multicast-fdb static delete <number>

multicast-fdb static delete all

multicast-fdb static delete vlan <vlanid>

multicast-fdb static delete interface gigabit <portNo>

Parameters:

<number>	Static multicast forwarding table entry index.
	Valid values: 1~128
	Type: Mandatory
<vlanid>	**Valid values**: 1~4094.
	Type: Mandatory
<portNo>	**Valid values**: 1~28.
	Type: Mandatory

multicast-fdb static <number> interface gigabit <portNo> <vlan> <ipaddr>

Description:

Create static IGMP VLAN forwarding table entry.

Syntax:

multicast-fdb static <number> interface gigabit <portNo> <vlan> <ipaddr>

Parameters:

<number>	Static multicast forwarding table entry index.
	Valid values: 1~128
	Type: Mandatory
<portNo>	**Valid values**: 1~28.
	Type: Mandatory
<vlanid>	**Valid values**: 1~4094.
	Type: Mandatory
<ipaddr>	IGMP VLAN group IP address.
	Valid values: 224.0.0.0~239.255.255.255
	Type: Mandatory

ext-tpid <number>

Description:

Set tpid.

Syntax:

ext-tpid <number>

Parameters:

<number>	tpid
	Valid values: 0x0000~0xffff
	Type: Mandatory

profile igmp-mvr

Description:

Entry IGMP MVR interface.

Syntax:

profile igmp-mvr

profile igmp-acl

Description:

Entry IGMP ACL interface.

Syntax:

profile igmp-acl

dot1x {enable|disable}

Description:

Enable / disable dot1x.

Syntax:

dot1x {enable|disable}

dot1x radius set <ip> <auth_port> <secret>

Description:

Set dot1x parameters.

Syntax:

dot1x radius set <ip> <auth_port> <secret>

Parameters:

<ip>	IP address.
	Format : 0.0.0.0 ~ 255.255.255.255
	Type: Mandatory
<auth_port>	Authentication port.
	Valid values: 1 ~ 65535
	Default values: 1812
	Type: Mandatory
<secret>	Authentication key.
	Length: 1 ~ 16
	Type: Mandatory

dot1x clear eapol-stats {<portNo>|all}

Description:

Clear dot1x EAPOL stats.

Syntax:

dot1x clear eapol-stats {<portNo>|all}

Parameters:

<portNo>	Gigabit port.
	Valid values: 1 ~ 28
	Type: Mandatory

dot1x clear dot1x-radius-stats

Description:

Clear dot1x radius-stats

Syntax:

dot1x clear dot1x-radius-stats

https {enable|disable}

Description:

Enable/Disable https.

Syntax:

https {enable|disable}

https port {<portNo>|default}

Description:

Set https port by specific port or default port.

Syntax:

https port {<portNo>|default}

Parameters:

<portNo>	https port number. **Valid values:** 1 ~ 65535 **Type**: Mandatory
default	https default port number is 443. **Type**: Mandatory

interface trunk-group <number>

Description:

Enter trunk group configure mode.

Syntax:

interface trunk-group <number>

Parameters:

<number>	Trunk group index. **Valid values:** 1 ~ 2 **Type**: Mandatory

fdb-delete interface trunk-group <number>

Description:

Delete forwarding table per trunk group.

Syntax:

fdb-delete interface trunk-group <number>

Parameters:

<number>	Trunk group index. **Valid values:** 1 ~ 2 **Type**: Mandatory

ssl default-certificate

Description:

Use system default SSL certificate

Syntax:

ssl default-certificate

ssl upload

Description:

Upload new SSL certificate

Syntax:

ssl upload

6.4 Interface Gigabit Mode Commands

accfrm

Description:

Set acceptable frame type.

Syntax:

Accfrm{all|tag|untag}

Parameters:

all	Accept all frames.
tag	Accept tagged frame only.
untag	Accept un-tagged frame only.

max-mac-limit {enable|disable}

Description:

Enable/Disable max-MAC limitation of learning MAC address.

Syntax:

max-mac-limit {enable|disable}

Parameters:

disable	Disable max-mac limitation.
enable	Enable max-mac limitation.

max-mac <value>

Description:

Set max-MAC limitation number.

Syntax:

max-mac <value>

Parameters:

<value> **Valid values**: 0~32

Type: Mandatory

priority <priority>

Description:

Set user priority for the gigabit port.

Syntax:

priority <priority>

Parameters:

<priority> **Valid values**: 0 ~ 7

Type: Mandatory

vlan <vlanid>

Description:

Join VLAN with default setting (tagged).

Syntax:

vlan <vlanid>

Parameters:

<vlanid> **Valid values**: 1~4094

Type: Mandatory

vlan <vlanid> disable

Description:

Leave joined VLAN.

Syntax:

vlan <vlanid> disable

Parameters:

<vlanid>	**Valid values**: 1~4094
	Type: Mandatory
disable	Leave joined VLAN

vlan <vlanid> tag

Description:

Join tagged VLAN.

Syntax:

vlan <vlanid> tag

Parameters:

<vlanid>	**Valid values**: 1~4094
	Type: Mandatory
tag	Join Tagged VLAN

stpport {disable|enable}

Description:

Configure STP port.

Syntax:

stpport {disable|enable}

Parameters:

disable	Disable STP port.
enable	Enable STP port.

stpport cost <number>

Description:

Set STP port path cost.

Syntax:

stpport cost <number>

Parameters:

<number>	**Valid values**: 1 ~ 200000000
	Type: Mandatory

stpport edge-port {enable|disable}

Description:

Set STP port edge-type.

Syntax:

stpport edge-port {enable|disable}

Parameters:

enable	Set as edge-type.
disable	Set as none edge-type.

stpport priority <number>

Description:

Set STP port priority.

Syntax:

stpport priority <number>

Parameters:

<number>	**Valid values**: 0~240 step 16
	Type: Mandatory

flow-control {enable|disble}

Description:

Enable/Disable flow-control.

Syntax:

flow-control {enable|disble}

Parameters:

enable	Enable flow-control.
disable	Disable flow-control.

speed

Description:

Configure copper port Ethernet speed.

Syntax:

speed {auto|full-l000mbps|full-100mbps|full-10mbps|half-100mbps|half-10mbps}

Parameters:

auto	Auto negotiation.
full-l000mbps	Set 1000Mbps full duplexing.
full-100mbps	Set 100Mbps full duplexing.
full-10mbps	Set 10Mbps full duplexing.
half-100mbps	Set 100Mbps half duplexing.
half-10mbps	Set 10Mbps half duplexing.

sfp-speed

Description:

Configure fiber port Ethernet speed.

Syntax:

speed {auto|full-l000mbps|full-100mbps}

Parameters:

auto	Auto negotiation.
full-l000mbps	Set 1000Mbps full duplexing.
full-100mbps	Set 100Mbps full duplexing.

port {enable/disable}

Description:

Set interface gigabit port enable or disable.

Syntax:

port {enable/disable}

Parameters:

disable	Turn off gigabit port.
enable	Turn on gigabit port.

default vlan

Description:

Set default VLAN to gigabit port.

Syntax:

default vlan <vlanid>

Parameters:

<vlanid>	**Valid values**: 1 ~ 4094
	Type: Mandatory

policer pir <pir-rate> pbs <pbs-size> cir <cir-rate> cbs <cbs-size> {drop|cos|dscp}

Description:

Set ingress policer parameters.

Syntax:

policer pir <pir-rate> pbs <pbs-size> cir <cir-rate> cbs <cbs-size> {drop|cos|dscp}

Parameters:

<pir-rate>	Ingress total max rate setting.
	Valid values: 1~1000000 **Type**: Mandatory
<pbs-size>	Ingress queue size setting.
	Valid values: 1~65535 **Type**: Mandatory

<cir-rate>	Ingress max rate for first stage setting.
	Valid values: 1~1000000 **Type**: Mandatory
<cbs-size>	Ingress max rate for second stage setting.
	Valid values: 1~65535 **Type**: Mandatory
{drop|cos|dscp}	Policer type **Type**: Mandatory

policer disable

Description:

Disable policer function.

Syntax:

policer disable

acl-profile-bind <number>

Description:

Port ACL profile binding.

Syntax:

acl-profile-bind <number>

Parameters:

<number>	**Valid values**: 1~20
	Type: Mandatory

def-acl {permit|deny}

Description:

Set port default ACL rule.

Syntax:

def-acl permit

def-acl deny

queue-scheduler bind <number>

Description:

Scheduler profile binding.

Syntax:

queue-scheduler bind <number>

Parameters:

<number>	Scheduler profile index. **Valid values**: 1~8 **Type**: Mandatory

port-shaper {enable|disable}

Description:

Enable/Disable port shaper.

Syntax:

port-shaper {enable|disable}

port-shaper <rate>

Description:

Set port shaper rate.

Syntax:

port-shaper <rate>

Parameters:

<rate>	**Valid values**: 1~1000000 **Type**: Mandatory

queue-shaper {enable|disable}

Description:

Enable/Disable queue shaper.

Syntax:

queue-shaper {enable|disable}

queue-shaper queue <number> <rate>

Description:

Set queue shaper parameters.

Syntax:

queue-shaper queue <number> <rate>

Parameters:

<number>	**Valid values**: 0~7
	Type: Mandatory
<rate>	**Valid values**: 1~1000000
	Type: Mandatory

port-isolation <portNo>

Description:

Enable/Diabled port-isolation action.

Syntax:

port-isolation <portNo>

port-isolation <portNo> disable

Parameters:

<portNo>	**Valid values**: 1~28
	Type: Mandatory

unknown-uc rate <rate>

Description:

Set storm rate for unknown unicast packet.

Syntax:

unknown-uc rate <rate>

Parameters:

<rate>	**Valid values**: 1~1000000 (Kbps)
	Type: Mandatory

unknown-uc {block|forward}

Description:

Block/ Forward unknown unicast packet.

Syntax:

unknown-uc block

unknown-uc forward

unknown-mc rate <rate>

Description:

Set storm rate for unknown multicast packet.

Syntax:

unknown-mc rate <rate>

Parameters:

<rate>	**Valid values**: 1~1000000 (Kbps)
	Type: Mandatory

unknown-mc {block|forward}

Description:

Block/Forward unknown multicast packet.

Syntax:

unknown-mc block

unknown-mc forward

broadcast rate <rate>

Description:

Set storm rate for broadcast packet.

Syntax:

broadcast rate <rate>

Parameters:

<rate> **Valid values**: 1~1000000 (Kbps)

Type: Mandatory

broadcast {block|forward}

Description:

Block/Forward broadcast packet.

Syntax:

broadcast block

broadcast forward

vlan-stack {enable|disable}

Description:

Enable/disable vlan stack.

Syntax:

vlan-stack {enable|disable}

protocol-vlan <number> create <ether-type> <svlan> <s-prio>

Description:

Create protocol VLAN.

Syntax:

protocol-vlan <number> create <ether-type> <svlan> <s-prio>

Parameters:

<number> Protocol VLAN index.

Valid values: 1 ~ 20

Type: Mandatory

<ether-type>	Ether type. **Valid values**: 0 ~ FFFF,(hex) **Type**: Mandatory
<svlan>	Service VLAN (SVALN). **Valid values**: 1 ~ 4094 **Type**: Mandatory
<s-prio>	CoS of SVLAN. **Valid values**: 0 ~ 8 **Type**: Mandatory

protocol-vlan <number> delete

Description:

Delete protocol VLAN.

Syntax:

protocol-vlan <number> delete

Parameters:

<number>	Protocol VLAN index. **Valid values**: 1 ~ 20 **Type**: Mandatory

vlan-trans <number> create <cvlan> <c-prio> <svlan> <s-prio> many-to-replaced

Description:

Create VLAN translation.

Syntax:

vlan-trans <number> create <cvlan> <c-prio> <svlan> <s-prio> many-to-one-replaced

Parameters:

<number>	VLAN translation index. **Valid values**: 1 ~ 20 **Type**: Mandatory
<cvlan>	Customer VLAN (CVLAN). **Valid values**: 1 ~ 4094 **Type**: Mandatory

<c-prio>	CoS of VLAN. **Valid values**: 0 ~ 8 **Type**: Mandatory
<svlan>	Service VLAN (SVLAN). **Valid values**: 1 ~ 4094 **Type**: Mandatory
<s-prio>	CoS of SVLAN. **Valid values**: 0 ~ 8 **Type**: Mandatory

vlan-trans <number> delete

Description:

Delete VLAN translation.

Syntax:

vlan-trans <number> delete

Parameters:

<number>	VLAN translation index. **Valid values**: 1 ~ 20 **Type**: Mandatory

igmp mvrprofile <index>

Description:

Binding IGMP MVR profile to specified port.

Syntax:

igmp mvrprofile <index>

Parameters:

<index>	IGMP MVR index. **Valid values**: 1 ~ 15 **Type**: Mandatory

igmp aclprofile <index>

Description:

Binding IGMP ACL profile to specified port.

Syntax:

igmp aclprofile <index>

Parameters:

<index>	IGMP ACL index.
	Valid values: 1 ~ 15
	Type: Mandatory

igmp max-channel <number>

Description:

Set max channel to specified port.

Syntax:

igmp max-channel <number>

Parameters:

<number>	Max channel number.
	Valid values: 1 ~ 512
	Type: Mandatory

dot1x {force-reinitialize| force-reauthenticate}

Description:

Enable for force PAE port re-initialize / re-authenticate.

Syntax:

dot1x {force-reinitialize| force-reauthenticate}

dot1x auth-port-control {auto| force-authorized| force-unauthorized}

Description:

Set dot1x authentication type of PAE port.

Syntax:

dot1x auth-port-control {auto| force-authorized| force-unauthorized}

dot1x auth-quiet-period <period>

Description:

Set quiet period of PAE port

Syntax:

dot1x auth-quiet-period <period>

Parameters:

<period>	The quiet period of PAE port
	Valid values: 1 ~ 255 seconds.
	Default values: 60 seconds
	Type: Mandatory

dot1x auth-tx-period <period>

Description:

Set timeout of authenticator waiting for EAP-Response / Identity from supplication of PAE port

Syntax:

dot1x auth-tx-period <period>

Parameters:

<period>	The quiet period of PAE port
	Valid values: 1 ~ 255 seconds.
	Default values: 30 seconds
	Type: Mandatory

dot1x max-req <number>

Description:

Set max times of backend Authenticator send EAP-Request to supplicant before restarting the authentication process.

Syntax:

dot1x max-req <number>

Parameters:

<number> Max request number.

Valid values: 1 ~ 10.

Default values: 2

Type: Mandatory

dot1x auth-supp-timeout <timeout>

Description:

Set timeout of authenticator wait for EAP-Response(exclude EAP-Request / Identify) after sending EAP-Request.

Syntax:

dot1x auth-supp-timeout <timeout>

Parameters:

<timeout> Authenticator timeout.

Valid values: 1 ~ 255 seconds.

Default values: 30 seconds

Type: Mandatory

dot1x auth-server-timeout <timeout>

Description:

Set timeout of Authenticator wait Access-Challenge / Access-Accept / Access-Reject after sending Access-Request

Syntax:

dot1x auth-server-timeout <timeout>

Parameters:

<timeout> Authenticator timeout.

Valid values: 1 ~ 255 seconds.

Default values: 30 seconds

Type: Mandatory

dot1x reauth {enable|disable}

Description:

Enable/Disable re-authentication of APE port

Syntax:

dot1x reauth {enable|disable}

dot1x reauth-period <period>

Description:

period of re-authentication of PAE port

Syntax:

dot1x reauth-period <period>

Parameters:

<period>	Period of re-authentication.
	Valid values: 1 ~ 3600 seconds.
	Default values: 3600 seconds
	Type: Mandatory

6.5 ACL-profile Configure Mode Commands

acl-profile <number> {create|delete}

Description:

Create/Delete ACL profile.

Syntax:

acl-profile <number> {create|delete}

Parameters:

<number>	**Valid values**: 2~20
	Type: Mandatory
create|delete	**Type**: Mandatory

acl-profile <prof-number> {create|delete} entry <entry-number>

Description:

Create/Delete ACL profile entry.

Syntax:

acl-profile <prof-number> create entry <entry-number>

acl-profile <prof-number> delete entry <entry-number>

Parameters:

<prof-number>	**Valid values**: 2~20
	Type: Mandatory
<entry-number>	**Valid values**: 1~32
	Type: Mandatory

acl-profile <prof-number> set name <name>

Description:

Set ACL profile name.

Syntax:

acl-profile <prof-number> set name <name>

Parameters:

<prof-number>	**Valid values**: 2~20
	Type: Mandatory
<name>	**Valid Length**: 0~31
	Type: Mandatory

acl-profile <prof-number> set entry <entry-number> mac-type set vlan <vlanid>

Description:

Set VLAN index for ACL MAC type entry.

Syntax:

acl-profile <prof-number> set entry <entry-number> mac-type set vlan <vlanid>

Parameters:

<prof-number>	**Valid values**: 2~20
	Type: Mandatory
<entry-number>	**Valid values**: 1~32
	Type: Mandatory
<vlanid>	**Valid values**: 1~4094
	Type: Mandatory

acl-profile <prof-number> set entry <enrty-number> mac-type set vlan any

Description:

Set VLAN index for ACL MAC type entry.

Syntax:

acl-profile <prof-number> set entry <enrty-number> mac-type set vlan any

Parameters:

<prof-number>	**Valid values**: 2~20
	Type: Mandatory
<entry-number>	**Valid values**: 1~32
	Type: Mandatory

acl-profile <prof-number> set entry <entry-number> mac-type set {srcmac|dstmac} <mac> <mask>

Description:

Set MAC for ACL MAC type entry.

Syntax:

acl-profile <prof-number> set entry <entry-number> mac-type set {srcmac|dstmac} <mac> <mask>

Parameters:

<prof-number>	**Valid values**: 2~20
	Type: Mandatory
<entry-number>	**Valid values**: 1~32
	Type: Mandatory
srcmac|dstmac	Source / Destination MAC Address
	Type: Mandatory
<mac>	**Valid values**: 00:00:00:00:00:00 ~ FF:FF:FF:FF:FF:FF
	Type: Mandatory
<mask>	**Valid values**: 00:00:00:00:00:00 ~ FF:FF:FF:FF:FF:FF
	Type: Mandatory

acl-profile <prof-number> set entry <entry-number> mac-type set ethertype <ethertype>

Description:

Set ether type for ACL MAC type entry.

Syntax:

acl-profile <prof-number> set entry <entry-number> mac-type set ethertype <ethertype>

Parameters:

<prof-number>	**Valid values**: 2~20
	Type: Mandatory
<entry-number>	**Valid values**: 1~32
	Type: Mandatory
<ethertype>	**Valid values**: 0x0001~0xFFFF
	Type: Mandatory

acl-profile <prof-number> set entry <entry-number> mac-type set ethertype any

Description:

Set ether type for ACL MAC type entry.

Syntax:

acl-profile <prof-number> set entry <entry-number> mac-type set ethertype any

Parameters:

<prof-number>	**Valid values**: 2~20
	Type: Mandatory
<entry-number>	**Valid values**: 1~32
	Type: Mandatory

acl-profile <prof-number> set entry <entry-number> ipv4-type set {srcip|dstip} <ipaddr> <mask>

Description:

Set IP for ACL IPv4 type entry.

Syntax:

acl-profile <prof-number> set entry <entry-number> ipv4-type set {srcip|dstip} <ipaddr> <mask>

Parameters:

<prof-number>	**Valid values**: 2~20
	Type: Mandatory
<entry-number>	**Valid values**: 1~32
	Type: Mandatory
srcip|dstip	Source / Destination IP Address
	Type: Mandatory
<ipaddr>	**Valid values**: 0.0.0.0 ~ 255.255.255.255
	Type: Mandatory
<mask>	**Valid values**: 0.0.0.0 ~ 255.255.255.255
	Type: Mandatory

acl-profile <prof-number> set entry <entry-number> ipv4-type set ip-protocol <protocol-id>

Description:

Set protocol for ACL IPv4 type entry.

Syntax:

acl-profile <prof-number> set entry <entry-number> ipv4-type set ip-protocol <protocol-id>

Parameters:

<prof-number>	**Valid values**: 2~20
	Type: Mandatory
<entry-number>	**Valid values**: 1~32
	Type: Mandatory
<protocol-id>	**Valid values**: 1~255
	Type: Mandatory

acl-profile <prof-number> set entry <entry-number> ipv4-type set ip-protocol any

Description:

Set protocol for ACL IPv4 type entry.

Syntax:

acl-profile <prof-number> set entry <entry-number> ipv4-type set ip-protocol any

Parameters:

<prof-number>	**Valid values**: 2~20
	Type: Mandatory

<entry-number>	**Valid values**: 1~32
	Type: Mandatory

acl-profile <prof-number> set entry <entry-number> l4port-type set protocol {tcp|udp}

Description:

Set protocol for ACL L4Port type entry.

Syntax:

acl-profile <prof-number> set entry <entry-number> l4port-type set protocol {tcp|udp}

Parameters:

<prof-number>	**Valid values**: 2~20
	Type: Mandatory
<entry-number>	**Valid values**: 1~32
	Type: Mandatory
tcp|udp	TCP or UDP packet.
	Type: Mandatory

acl-profile <prof-number> set entry <entry-number> l4port-type set {srcip|dstip} <ipaddr> <mask>

Description:

Set IP for ACL L4Port type entry.

Syntax:

acl-profile <prof-number> set entry <entry-number> l4port-type set {srcip|dstip} <ipaddr> <mask>

Parameters:

<prof-number>	**Valid values**: 2~20
	Type: Mandatory
<entry-number>	**Valid values**: 1~32
	Type: Mandatory
srcip|dstip	Source / Destination IP Address
	Type: Mandatory
<ipaddr>	**Valid values**: 0.0.0.0 ~ 255.255.255.255
	Type: Mandatory
<mask>	**Valid values**: 0.0.0.0 ~ 255.255.255.255
	Type: Mandatory

acl-profile <prof-number> set entry <entry-number> l4port-type set {srcport|dstport} <number>

Description:

Set port for ACL L4Port type entry.

Syntax:

acl-profile <prof-number> set entry <entry-number> l4port-type set {srcport|dstport} <number>

Parameters:

<prof-number>	**Valid values**: 2~20
	Type: Mandatory
<entry-number>	**Valid values**: 1~32
	Type: Mandatory
srcport|dstport	Source / Destination port
	Type: Mandatory
<number>	**Valid values**: 1~65535
	Type: Mandatory

acl-profile <prof-number> set entry <entry-number> l4port-type set {srcport|dstport} any

Description:

Set port for ACL L4Port type entry.

Syntax:

acl-profile <prof-number> set entry <entry-number> l4port-type set {srcport|dstport} any

Parameters:

<prof-number>	**Valid values**: 2~20
	Type: Mandatory
<entry-number>	**Valid values**: 1~32
	Type: Mandatory
srcport|dstport	Source / Destination port.
	Type: Mandatory

acl-profile <prof-number> set entry <entry-number> tos-type set {srcip|dstip} <ipaddr> <mask>

Description:

Set IP for ACL ToS type entry.

Syntax:

acl-profile <prof-number> set entry <entry-number> tos-type set {srcip|dstip} <ipaddr> <mask>

Parameters:

<prof-number>	**Valid values**: 2~20
	Type: Mandatory
<entry-number>	**Valid values**: 1~32
	Type: Mandatory
srcip|dstip	Source / Destination IP Address
	Type: Mandatory
<ipaddr>	**Valid values**: 0.0.0.0 ~ 255.255.255.255
	Type: Mandatory
<mask>	**Valid values**: 0.0.0.0 ~ 255.255.255.255
	Type: Mandatory

acl-profile <prof-number> set entry <entry -number> tos-type set type {precedence|tos|dscp } <number>

Description:

Set type for ACL ToS type entry.

Syntax:

acl-profile <prof-number> set entry <entry -number> tos-type set type {precedence|tos|dscp } <number>

Parameters:

<prof-number>	**Valid values**: 2~20 **Type**: Mandatory
<entry-number>	**Valid values**: 1~32 **Type**: Mandatory
precedence|tos|dscp	Precedence or ToS or DSCP Type.
	Type: Mandatory
<number>	Precedence type.
	Valid values: 0~7
	Tos type.
	Valid values: 0~15
	DSCP type.
	Valid values: 0~63
	Type: Mandatory

acl-profile <prof-number> set entry <entry-number> tos-type set type any

Description:

Set type for ACL ToS type entry.

Syntax:

acl-profile <prof-number> set entry <entry-number> tos-type set type any

Parameters:

<prof-number>	**Valid values**: 2~20
	Type: Mandatory
<entry-number>	**Valid values**: 1~32
	Type: Mandatory

acl-profile <prof-number> set entry <entry-number> action forwarding {deny|permit}

Description:

Set ACL entry action is forwarding.

Syntax:

acl-profile <prof-number> set entry <entry-number> action forwarding {deny|permit}

Parameters:

<prof-number>	**Valid values**: 2~20
	Type: Mandatory
<entry-number>	**Valid values**: 1~32
	Type: Mandatory
deny|permit	Deny or Permit forwarding.
	Type: Mandatory

acl-profile <prof-number> set entry <entry-number> action queue <number>

Description:

Set ACL entry action to specific queue number.

Syntax:

acl-profile <prof-number> set entry <entry-number> action queue <number>

Parameters:

<prof-number>	**Valid values**: 2~20
	Type: Mandatory

<entry-number>	**Valid values**: 1~32
	Type: Mandatory
<number>	**Valid values**: 0~7
	Type: Mandatory

acl-profile <prof-number> set entry <entry-number> action cos <number>

Description:

Set ACL entry action is mark CoS number.

Syntax:

acl-profile <prof-number> set entry <entry-number> action cos <number>

Parameters:

<prof-number>	**Valid values**: 2~20
	Type: Mandatory
<entry-number>	**Valid values**: 1~32
	Type: Mandatory
<number>	**Valid values**: 0~7
	Type: Mandatory

acl-profile <prof-number> set entry <entry-number> action copyframe

Description:

Set ACL entry action is copy frame.

Syntax:

acl-profile <prof-number> set entry <entry-number> action copyframe

Parameters:

<prof-number>	**Valid values**: 2~20
	Type: Mandatory
<enrty-number>	**Valid values**: 1~32
	Type: Mandatory

6.6 Schedule-profile Configure Mode Commands

scheduler-profile <number> method {spq|spq-wrr|wrr}

Description:

Set scheduler profile method.

Syntax:

scheduler-profile <number> method {spq|spq-wrr|wrr}

Parameters:

<number>	Scheduler profile index.
	Valid values: 1~8
	Type: Mandatory
sp|sp-wrr|wrr	sp: strict priority
	sp-wrr: strict priority + weighted round robin
	wrr: weighted round robin
	Type: Mandatory

scheduler-profile <prof-number> queue <queue-number> weight <number>

Description:

Set scheduler profile queue weight.

Syntax:

scheduler-profile <prof-number> queue <queue-number> weight <number>

Parameters:

<prof-number>	**Valid values**: 2~8
	Type: Mandatory
<queue-number>	**Valid values**: 0~7
	Type: Mandatory
<number>	**Valid values**: 1~255
	Type: Mandatory

6.7 Interface VLAN Mode Commands

igmp vlan {create|delete}

Description:

Create / Delete IGMP.

Syntax:

igmp vlan create

igmp vlan delete

igmp router-port <portNo>

Description:

Set IGMP VLAN source port.

Syntax:

igmp router-port <portNo>

Parameters:

<portNo>	**Valid values**: 1~28.
	Type: Mandatory

igmp access-mode {snooping|proxy}

Description:

Set IGMP VLAN access mode.

Syntax:

igmp access-mode snooping

igmp access-mode proxy

igmp leave-mode {normal|fast}

Description:

Set IGMP VLAN leave mode.

Syntax:

igmp leave-mode normal

igmp leave-mode fast

igmp version {v1|v2}

Description:

Set IGMP VLAN version.

Syntax:

igmp version v1

igmp version v2

igmp robustness <number>

Description:

Set IGMP VLAN robustness.

Syntax:

igmp robustness <number>

Parameters:

<number> **Valid values**: 1~3.

Type: Mandatory

igmp query-interval <number>

Description:

Set IGMP VLAN query interval.

Syntax:

igmp query-interval <number>

Parameters:

<number> **Valid values**: 1~1800 (unit: sec).

Type: Mandatory

igmp max-response-time <number>

Description:

Set IGMP VLAN max response time.

Syntax:

igmp max-response-time <number>

Parameters:

<number> **Valid values**: 1~255 (unit: 100ms).

Type: Mandatory

igmp last-member-query-count <number>

Description:

Set IGMP VLAN last member query count.

Syntax:

igmp last-member-query-count <number>

Parameters:

<number> **Valid values**: 1~3.

Type: Mandatory

igmp last-member-query-interval <number>

Description:

Set IGMP VLAN last member query interval.

Syntax:

igmp last-member-query-interval <number>

Parameters:

<number> **Valid values**: 1~255 (unit: 100ms).

Type: Mandatory

igmp vlan interface address <ipaddr>

Description:

Set IP address of IGMP VLAN interface.

Syntax:

igmp vlan interface address <ipaddr>

Parameters:

<ipaddr> **Valid values**: 0.0.0.0~223.255.255.255.

Type: Mandatory

ip-address <ip>

Description:

Set layer3 IP address for specified VLAN.

Syntax:

ip-address <ip>

Parameters:

<ip> IP address.

Valid values: 0.0.0.0~255.255.255.255

Type: Mandatory

ip-address <ip> netmask <netmask>

Description:

Set layer3 IP address and netmask for specified VLAN.

Syntax:

ip-address <ip> netmask <netmask>

Parameters:

<ip> IP address.

Valid values: 0.0.0.0~255.255.255.255

Type: Mandatory

<netmask> IP address.

Valid values: 0.0.0.0~255.255.255.255

Type: Mandatory

igmp version {v2|v3| v3compatible}

Description:

Set IGMP version.

Syntax:

igmp version {v2|v3| v3compatible}

6.8 IGMP MVR Mode Commands

igmp-mvr <number,2..15> {create|delete}

Description:

Create / delete IGMP MVR profile.

Syntax:

igmp-mvr <number,2..15> {create|delete}

Parameters:

<number> IGMP MVR profile index.

Valid values: 2~15

Type: Mandatory

igmp-mvr <p-number> entry <e-number> <startIP> <endIP> <vid>

Description:

Create IGMP MVR entry.

Syntax:

igmp-mvr <p-number> entry <e-number> <startIP> <endIP> <vid>

Parameters:

<p-number>	IGMP MVR profile index. **Valid values**: 2~15 **Type**: Mandatory
<e-number>	IGMP MVR entry index. **Valid values**: 1~32 **Type**: Mandatory
<startIP> **<endIP>**	IP address. **Valid values**: 0.0.0.0~255.255.255.255 **Type**: Mandatory
<vid>	VLAN ID. **Valid values**: 1~4094 **Type**: Mandatory

igmp-mvr <p-number> entry <e-number> delete

Description:

Delete IGMP MVR entry.

Syntax:

igmp-mvr <p-number> entry <e-number> delete

Parameters:

<p-number>	IGMP MVR profile index. **Valid values**: 2~15 **Type**: Mandatory
<e-number>	IGMP MVR entry index. **Valid values**: 1~32 **Type**: Mandatory

6.9 IGMP ACL Mode Commands

igmp-acl <number> {create|delete}

Description:

Create / delete IGMP ACL profile.

Syntax:

igmp-acl <number> {create|delete}

Parameters:

<number>	IGMP ACL profile index.
	Valid values: 2~15
	Type: Mandatory

igmp-acl <number> {default-deny| default-permit}

Description:

Set IGMP ACL default rule.

Syntax:

igmp-acl <number> {default-deny| default-permit}

Parameters:

<number>	IGMP ACL profile index.
	Valid values: 2~15
	Type: Mandatory

igmp-acl <p-number> entry <e-number> <startIP> <endIP> {<vid>|all} {permit|deny}

Description:

Create IGMP ACL entry.

Syntax:

igmp-acl <p-number> entry <e-number> <startIP> <endIP> {<vid>|all} {permit|deny}

Parameters:

<p-number>	IGMP ACL profile index.
	Valid values: 2~15
	Type: Mandatory
<e-number>	IGMP MVR entry index.
	Valid values: 1~32
	Type: Mandatory
<startIP>	IP address.
<endIP>	**Valid values**: 0.0.0.0~255.255.255.255
	Type: Mandatory
<vid>	VLAN ID.
	Valid values: 1~4094
	Type: Mandatory

igmp-acl <p-number> entry <e-number> delete

Description:

Delete IGMP ACL entry

Syntax:

igmp-acl <p-number> entry <e-number> delete

Parameters:

<p-number>	IGMP ACL profile index. **Valid values**: 2~15 **Type**: Mandatory
<e-number>	IGMP MVR entry index. **Valid values**: 1~32 **Type**: Mandatory

6.10 Trunk Group Mode Commands

trunk enable static

Description:

Enable link aggregation group and its mode is static.

Syntax:

trunk enable static

trunk disable

Description:

Disable link aggregation group and all member port will be remove on specific port.

Syntax:

trunk disable

port-trunk add <portNo>

Description:

Add member port to specific trunk group, the max member ports is 4.

Syntax:

port-trunk add <portNo>

Parameters:

<portNo>	Port number.
	Valid values: 1~28
	Type: Mandatory

port-trunk remove {<portNo>|all}

Description:

Remove member port from specific trunk group.

Syntax:

port-trunk remove <portNo>

Parameters:

<portNo>	Port number.
	Valid values: 1~28
	Type: Mandatory
all	All member port.
	Type: Mandatory

6.11 Alarm Related Mode Commands

show profile alarm

Description:

Show alarm profile list

Syntax:

show profile alarm

show alarm current

Description:

Show current alarm list

Syntax:

show alarm current

show event

Description:

Show event list

Syntax:

show event

show alarm history

Description:

Show alarm history

Syntax:

show alarm history

event clear

Description:

Clear event.

Syntax:

event clear

alarm history clear

Description:

Clear alarm history.

Syntax:

alarm history clear.

profile alarm

Description:

Enter Alarm Profile Configuration Mode.

Syntax:

profile alarm

alarm <alarmid> {mask|unmask|major|minor}

Description:

Configure an alarm profile entry

(default setting for each alarm is unmask and minor)

Syntax:

alarm <alarmid> mask

alarm <alarmid> unmask

alarm <alarmid> major

alarm <alarmid> minor

Parameters:

<alarmid>	Alarm ID
	Valid values: Refer to. Alarm Table
	Type: Mandatory
mask	Mask this alarm
	Type: Mandatory
unmask	Unmask this alarm
	Type: Mandatory
major	Set alarm level to major
	Type: Mandatory
minor	Set alarm level to minor
	Type: Mandatory

6.12 Layer 3 Enable Mode Commands

show system layer3

Description:

Show system layer3.

Syntax:

show system layer3

show route rip

Description:

Show RIP information.

Syntax:

show rip

show route ospf

Description:

Show route OSPF information.

Syntax:

show route ospf

show ospf database

Description:

Show OSPF database information.

Syntax:

show ospf database

show ospf databse asbr-summary

Description:

Show OSPF database information detail for ASBR summary link states.

Syntax:

show ospf databse asbr-summary

show ospf databse external

Description:

Show OSPF database information detail for external link states

Syntax:

show ospf databse external

show ospf databse network

Description:

Show OSPF database information detail for network link states

Syntax:

show ospf databse network

show ospf databse nssa-external

Description:

Show OSPF database information detail for NSSA external link state

Syntax:

show ospf databse nssa-external

show ospf databse router

Description:

Show OSPF database information detail for router link states.

Syntax:

show ospf databse router

show ospf databse summary

Description:

Show OSPF database information detail for network summary link states.

Syntax:

show ospf databse summary

show ospf neighbor

Description:

Show OSPF neighbor

Syntax:

show ospf neighbor

show ospf

Description:

Show OSPF configure parameters.

Syntax:

Show ospf

show vrrp

Description:

Show VRRP group status.

Syntax:

Show vrrp

show route

Description:

Show routing table. (include RIP, OSPF, static)

Syntax:

Show route

show dhcp binding

Description:

Show DHCP binding table.

Syntax:

show dhcp binding

show dhcp binding <vlan-id>

Parameters:

<vlan-id> Interface VLAN

Valid values: 1~4094.

Type: Optional

show dhcp pool

Description:

Show DHCP pool configuration

Syntax:

show dhcp pool

show dhcp pool <pool-id>

Parameters:

<pool-id> DHCP pool index.

Valid values: 1~5.

Type: Optional

6.13 Layer 3 Configure Mode Commands

dhcp {enable|disable}

Description:

Enable / disable DHCP server.

Syntax:

dhcp enable

dhcp disable

dhcp lease <1-31536000>

Description:

Set DHCP pool default lease time, when DHCP pool be created, take this value as default lease time.

Syntax:

dhcp lease <1-31536000>

Parameters:

<1-31536000>	Lease time
	Valid values: 1~31536000.
	Type: Mandatory

dhcp pool <pool-id> address-range <start-ip> <end-ip>

Description:

Set DHCP pool address range. Start IP must smaller than End IP

Syntax:

dhcp pool <pool-id> address-range <start-ip> <end-ip>

Parameters:

<pool-id>	DHCP Pool index
	Valid values: 1 ~ 5
	Type: Mandatory
<start-ip>	Start IP address
	Valid values: 0.0.0.0 ~ 255.255.255.255
	Type: Mandatory
<end-ip>	End IP address
	Valid values: 0.0.0.0 ~ 255.255.255.255
	Type: Mandatory

dhcp pool <pool-id> default-router <router-ip>

Description:

Set DHCP pool default router

Syntax:

dhcp pool <pool-id> default-router <router-ip>

Parameters:

<pool-id>	DHCP Pool index
	Valid values: 1 ~ 5
	Type: Mandatory

<router-ip>	Router IP address
	Valid values: 0.0.0.0 ~ 255.255.255.255
	Type: Mandatory

dhcp pool <pool-id> disable

Description:

To disable/remove DHCP pool.

Syntax:

dhcp pool <pool-id> disable

Parameters:

<pool-id>	DHCP Pool index
	Valid values: 1 ~ 5
	Type: Mandatory

dhcp pool <pool-id> dns-server <DNS>

Description:

Set DHCP pool domain name server address

Syntax:

dhcp pool <pool-id> dns-server<DNS>

Parameters:

<pool-id>	DHCP Pool index
	Valid values: 1 ~ 5
	Type: Mandatory
<DNS>	DNS IP address
	Valid values: 0.0.0.0 ~ 255.255.255.255
	Type: Mandatory

dhcp pool <pool-id> domain-name <name>

Description:

Set DHCP pool domain name

Syntax:

dhcp pool <pool-id> domain-name <name>

Parameters:

<pool-id>	DHCP Pool index
	Valid values: 1 ~ 5
	Type: Mandatory
<name>	Router IP address
	Valid length: 0 ~ 64 characters
	Type: Mandatory

dhcp pool <pool-id> lease <1-31536000>

Description:

Set DHCP pool lease time

Syntax:

dhcp pool <pool-id> lease <1-31536000>

Parameters:

<pool-id>	DHCP Pool index
	Valid values: 1 ~ 5
	Type: Mandatory
<1-31536000>	Lease time
	Valid values: 1~31536000.
	Type: Mandatory

dhcp pool <pool-id> network <subnet> <netmask>

Description:

Set DHCP pool network. If pool not exist, call create, else call set

Syntax:

dhcp pool <pool-id> network <subnet> <netmask>

Parameters:

<pool-id>	DHCP Pool index
	Valid values: 1 ~ 5
	Type: Mandatory
<subnet>	Subnet address
	Valid values: 0.0.0.0 ~ 255.255.255.255
	Type: Mandatory

<netmask> netmask address

Valid values: 0.0.0.0 ~ 255.255.255.255

Type: Mandatory

ip-routing {enable|disable}

Description:

Enable/disable IP routing.

Syntax:

ip-routing {enable|disable}

route rip delete {<vlanid>|all}

Description:

Delete RIP route.

Syntax:

route rip delete {<vlanid>|all}

Parameters:

<vlanid> VLAN ID.

Valid values: 1 ~ 4094

Type: Mandatory

6.14 Layer 3 Interface VLAN Mode Commands

layer3 {enable|disable}

Description:

Enable/disable layer3.

Syntax:

layer3 {enable|disable}

ip rip auth {enable|diable}

Description:

Enable/disable RIP for specified VLAN.

Syntax:

ip rip auth {enable|diable}

ip rip auth string <string>

Description:

Set RIP Authentication Key.

Syntax:

ip rip auth string <string>

Parameters:

<string>	Authentication Key.
	Valid values: 0~16
	Type: Mandatory

ip rip {send|receive} version {v1|v2|both}

Description:

Set RIP send/receive version.

Syntax:

ip rip {send|receive} version {v1|v2|both}

ip rip {send|receive} disable

Description:

Disable RIP send/receive function.

Syntax:

ip rip {send|receive} disable

ip rip split-horizon {simple| poisoned-reverse| disable}

Description:

Set RIP split horizon type.

Syntax:

ip rip split-horizon {simple| poisoned-reverse| disable}

ip rip {enable| disable}

Description:

Enable/disable RIP for specified VLAN.

Syntax:

ip rip {enable| disable}

ip ospf authentication {message-digest|null|disable}

Description:

Set OSPF authentication mode

Syntax:

ip ospf authentication {message-digest|null|disable}

ip ospf authentication

Parameters:

message-digest	Use message-digest authentication
null	Use no authentication
disable	Disable authentication
	Type: Optional

ip ospf authentication-key <string>

Description:

Set authentication key.

Syntax:

ip ospf authentication-key <string>

Parameters:

<string>	Authentication key.
	Valid length: 0~8
	Type: Mandatory

ip ospf cost <number>

Description:

Set interface cost

Syntax:

ip ospf cost <number>

Parameters:

<number>	Cost
	Valid values: 1~65535
	Type: Mandatory

ip ospf dead-interval <number>

Description:

Set interval after which a neighbor is declared dead.

Syntax:

ip ospf dead-interval <number>

Parameters:

<number>	Interval, unit: seconds
	Valid values: 1~65535
	Type: Mandatory

ip ospf hello-interval <number>

Description:

Set time between HELLO packets.

Syntax:

ip ospf hello-interval <number>

Parameters:

<number>	Interval, unit:
	Valid values: 1~65535
	Type: Mandatory

ip ospf message-digest-key <numebr> <string>

Description:

Set message digest authentication password (key)

Syntax:

ip ospf message-digest-key <number> <string>

Parameters:

<number>	Key ID
	Valid values: 1~255
	Type: Mandatory
<string>	Key
	Valid length: 0~16
	Type: Mandatory

ip ospf mtu-ignore disable

Description:

Enable/Disable OSPF mtu mismatch detection

Syntax:

ip ospf mtu-ignore

ip ospf mtu-ignore disable

Parameters:

disable	**Enable** mtu mismatch detection.
	Type: Mandatory

ip ospf network {broadcast|non-broadcast|point-to-multipoint|point-to-point}

Description:

Set OSPF network type.

Syntax:

ip ospf network {broadcast|non-broadcast)

ip ospf network {point-to-multipoint|point-to-point}

Parameters:

broadcast	Specify OSPF broadcast multi-access network
non-broadcast	Specify OSPF NBMA network
point-to-multipoint	Specify OSPF point-to-multipoint network
point-to-point	Specify OSPF point-to-point network
	Type: Mandatory

ip ospf priority <number>

Description:

Set router priority

Syntax:

ip ospf priority <number>

Parameters:

<number>	Priority
	Valid values: 0~255
	Type: Mandatory

ip ospf retransmit-interval <interval>

Description:

Set time between retransmitting lost link state advertisements

Syntax:

ip ospf retransmit-interval <interval>

Parameters:

<interval>	Interval, unit: seconds
	Valid values: 3~65535
	Type: Mandatory

ip ospf transmit-delay <number>

Description:

Set link state transmit delay

Syntax:

ip ospf transmit-delay <number>

Parameters:

<number>	Delay time, unit: seconds.
	Valid values: 1~65535
	Type: Mandatory

ip ospf enable area {<number>|<ip>}

Description:

Configure OSPF area parameters

Syntax:

ip ospf enable area {<number>|<ip>}

Parameters:

<ip>	OSPF area ID in IP address format
<number>	OSPF area ID as a decimal value
	Type: Mandatory

ip ospf {enable|disable}

Description:

Enable/Disable OSPF on the interface

Syntax:

ip ospf {enable|disable}

vrrp <number> advertise-interval <interval>

Description:

Set the advertisement timer.

Syntax:

vrrp <number> advertise-interval <interval>

Parameters:

<number>	VRRP group number
	Valid values: 1~255
	Type: Mandatory
<interval>	Advertisement interval, unit: 0.1 seconds
	Valid values: 1~2550
	Type: Mandatory

vrrp <number> authentication disable

Description:

Enable/Disable plain-text authentication

Syntax:

vrrp <number> authentication

vrrp <number> authentication disable

Parameters:

<number>	VRRP group number
	Valid values: 1~255
	Type: Mandatory
disable	Disable authentication
	Type: Optional

vrrp <number> authentication-key <string>

Description:

Set key for plain-text authentication

Syntax:

vrrp <number> authentication-key <string>

Parameters:

<number>	VRRP group number
	Valid values: 1~255
	Type: Mandatory

<string>	Key
	Valid length: 0~8
	Type: Mandatory

vrrp <number> ip <ip>

Description:

Set IP of virtual router redundancy protocol (VRRP)

Syntax:

vrrp <number> ip <ip>

Parameters:

<number>	VRRP group number
	Valid values: 1~255
	Type: Mandatory
<ip>	IP address
	Valid values:
	Type: Mandatory

vrrp <number> learn-master-adv-int disable

Description:

Enable/Disable advertisement interval from current master

Syntax:

vrrp <number> learn-master-adv-int

vrrp <number> learn-master-adv-int disable

Parameters:

<number>	VRRP group number
	Valid values: 1~255
	Type: Mandatory
disable	Ignore advertisement interval from current master
	Type: Optional

vrrp <number> preempt dsiable

Description:

Enable/Disable preemption of lower priority Master

Syntax:

vrrp <number> preempt

vrrp <number> preempt disable

Parameters:

<number>	VRRP group number
	Valid values: 1~255
	Type: Mandatory
disable	Disable preemption of lower priority Master
	Type: Optional

vrrp <number> priority <priority>

Description:

Set priority of this VRRP group

Syntax:

vrrp <number> priority <priority>

Parameters:

<number>	VRRP group number
	Valid values: 1~255
	Type: Mandatory
<priority>	Priority level
	Valid values: 1~254
	Type: Mandatory

vrrp <number> disable

Description:

Delete VRRP group

Syntax:

vrrp <number> disable

Parameters:

<number>	VRRP group number
	Valid values: 1~255
	Type: Mandatory

6.15 Router RIP Configure Mode Commands

rip {enable|disable}

Description:

Enable/Disable RIP

Syntax:

rip {enable|disable}

update-time <time>

Description:

Set RIP update-time

Syntax:

update-time <time>

Parameters:

<time>	Update time, unit :second
	Valid values: 20~3600
	Type: Mandatory

gc-timeout <time>

Description:

Set RIP garbage collection timeout.

Syntax:

gc-timeout <time>

Parameters:

<time>	Garbage collection timeout, unit : second
	Valid values: 20~3600
	Type: Mandatory

redistribute {connected|ospf|static} disable

Description:

Create/Delete another routing protocol configuration.

Syntax:

redistribute {connected|ospf|static}

redistribute {connected|ospf|static} disable

Parameters:

connected	Connected routes (directly attached subnet or host).
ospf	Open Shortest Path Protocol (OSPF).
static	Statically configured routes.
	Type: Mandatory
disable	Delete connected|OSPF|statically routes.
	Type: Optional

redistribute {connected|ospf|static} metric <number>

Description:

Redistribute information from another routing protocol with metric.

Syntax:

redistribute {connected|ospf|static} metric <number>

Parameters:

<number>	Metric for redistributed routes
	Valid values: 0~16
	Type: Mandatory

6.16 Router OSPF Configure Mode Commands

ospf {enable|disable}

Description:

Enable/Disable OSPF

Syntax:

ospf {enable|disable}

abr-type {cisco|shortcut|standard}

Description:

Set OSPF ABR type

Syntax:

abr-type {cisco|shortcut|standard}

Parameters:

cisco	Alternative ABR, cisco implementation.
shortcut	Shortcut ABR.
standard	Standard behavior (RFC2328).
	Type: Mandatory

rfc1583compatibility disable

Description:

Enable/Disable for RFC1583 compatibility.

Syntax:

rfc1583compatibility

rfc1583compatibility disable

Parameters:

disable	Disable RFC1583 compatibility.
	Type: Optional

router-id <ip>

Description:

Set OSPF router ID in IP address format.

Syntax:

router-id <ip>

Parameters:

<ip>	IP address.
	Type: Mandatory

area {<ip>|<number>} {nssa|stub|normal}

Description:

Set OSPF area parameters.

Syntax:

area {<ip>|<number>} {nssa|stub|normal}

Parameters:

<ip>	IP address, OSPF area ID in IP address format
<number>	Number, OSPF area ID as a decimal value
	Type: Mandatory
nssa	Configure OSPF area as NSSA
stub	Configure OSPF area as STUB
normal	Configure OSPF area as normal, delete the entry.
	Type: Mandatory

area {<ip>|<number>} {nssa|stub} no-summary

Description:

Set OSPF area parameters

Syntax:

area {<ip>|<number>} {nssa|stub} no-summary

Parameters:

<ip>	IP address, OSPF area ID in IP address format
<number>	Number, OSPF area ID as a decimal value
	Type: Mandatory
nssa	Configure OSPF area as NSSA
stub	Configure OSPF area as STUB
normal	Configure OSPF area as normal, delete the entry.
	Type: Mandatory

area {<ip>|<number>} nssa translate disable

Description:

Configure OSPF NSSA area parameters

Syntax:

area {<ip>|<number>} nssa

area {<ip>|<number>} nssa translate

area {<ip>|<number>} nssa translate disable

Parameters:

<ip>	IP address, OSPF area ID in IP address format
<number>	Number, OSPF area ID as a decimal value
	Type: Mandatory
translate	Configure NSSA-ABR to translate
	Type: Optional
disable	Never translate LSA
	Type: Optional

area {<ip>|<number>} nssa no-summary translate disable

Description:

Configure OSPF NSSA area parameters

Syntax:

area {<ip>|<number>} nssa no-summary

area {<ip>|<number>} nssa no-summary translate

area {<ip>|<number>} nssa no-summary translate disable

Parameters:

<ip>	IP address, OSPF area ID in IP address format
<number>	Number, OSPF area ID as a decimal value
	Type: Mandatory
no-summary	Do not inject summary-LSA into NSSA
	Type: Mandatory
translate	Configure NSSA-ABR to translate
	Type: Optional
disable	Never translate LSA
	Type: Optional

area {<ip>|<number>} virtual-link <virtual-ip> disable

Description:

Configure a virtual link

Syntax:

area {<ip>|<number>} virtual-link <virtual-ip>

area {<ip>|<number>} virtual-link <virtual-ip> disable

Parameters:

<ip>	IP address, OSPF area ID in IP address format
<number>	Number, OSPF area ID as a decimal value
	Type: Mandatory
<virtual-ip>	IP address
	Type: Mandatory
disable	Delete the virtual link configuration.
	Type: Optional

redistribute {connected|static|rip} disable

Description:

Redistribute information from another routing protocol.

Syntax:

redistribute {connected|static|rip}

redistribute {connected|static|rip} disable

Parameters:

connected	Connected routes (directly attached subnet or host)
static	Statically configured routes
rip	Routing Information Protocol (RIP)
	Type: Mandatory
disable	Delete the routing protocol configuration.
	Type: Optional

redistribute {connected|static|rip} metric <number>

Description:

Redistribute information from another routing protocol.

Syntax:

redistribute {connected|static|rip} metric <number>

Parameters:

connected	Connected routes (directly attached subnet or host)
static	Statically configured routes
rip	Routing Information Protocol (RIP)
	Type: Mandatory
<number>	OSPF default metric
	Valid values: 0~16777214
	Type: Mandatory

redistribute {connected|static|rip} metric <num> metric-type <num1>

Description:

Redistribute information from another routing protocol.

Syntax:

Redistribute {connected|static|rip} metric <num> metric-type <num1>

Parameters:

connected	Connected routes (directly attached subnet or host)
static	Statically configured routes
rip	Routing Information Protocol (RIP)
	Type: Mandatory

< num >	OSPF default metric
	Valid values: 0~16777214
	Type: Mandatory
<num1>	OSPF exterior metric type for redistributed routes
	Valid values: 1~2
	Type: Mandatory

redistribute {connected|static|rip} metric-type <1|2>

Description:

Redistribute information from another routing protocol.

Syntax:

redistribute {connected|static|rip} metric-type <number>

Parameters:

connected	Connected routes (directly attached subnet or host)
static	Statically configured routes
rip	Routing Information Protocol (RIP)
	Type: Mandatory
<number>	OSPF exterior metric type for redistributed routes
	Valid values: 1~2
	Type: Mandatory

redistribute {connected|static|rip} metric-type <num> metric <num1>

Description:

Redistribute information from another routing protocol.

Syntax:

redistribute {connected|static|rip} metric-type <num> metric <num1>

Parameters:

connected	Connected routes (directly attached subnet or host)
static	Statically configured routes
rip	Routing Information Protocol (RIP)
	Type: Mandatory

<num>	OSPF exterior metric type for redistributed routes **Valid values**: 1~2 **Type**: Mandatory
<num1>	OSPF default metric **Valid values**: 0~16777214 **Type**: Mandatory

neighbor <ip> disable

Description:

Enable/Disable OSPF neighbor.

Syntax:

neighbor <ip>

Parameters:

<ip>	OSPF nieghbor address **Type**: Mandatory
disable	Delete OSPF nieghbor **Type**: Optional

neighbor <ip> poll-interval <interval> priority <priority>

Description:

Set OSPF neighbor parameters.

Syntax:

neighbor <ip> poll-interval <interval> priority <priority>

neighbor <ip> priority <priority> poll-interval <interval>

Parameters:

<ip>	OSPF nieghbor address **Type**: Mandatory
<interval>	Polling interval. **Valid values**: 1~65535 **Type**: Mandatory
<priority>	Priority. **Valid values**: 0~255 **Type**: Mandatory

7. SWITCH OPERATION

7.1 Address Table

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

7.2 Learning

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

7.3 Forwarding & Filtering

When one packet comes from some port of the **Industrial Managed Switch**, it will also check the destination address besides the source address learning. The **Industrial Managed Switch** 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 **Industrial Managed Switch** will forward this packet to the port where this destination address is located according to the information from address table. But, if the destination address is located at the same port with this packet comes in, then this packet will be filtered. Thereby increasing the network throughput and availability.

7.4 Store-and-Forward

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

Due to the learning function of the **Industrial Managed Switch**, 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 **Industrial Managed Switch** performs **"Store and Fforward"** therefore, no error packets occur. More reliably, it reduces the re-transmission rate. No packet loss will occur.

7.5 Auto-Negotiation

The STP ports on the Switch have built-in **"Auto-negotiation"**. This technology automatically sets the best possible bandwidth when a connection is established with another network device (usually at Power On or Reset). This is done by detect the modes and speeds at the second of both device is connected and capable of, both 10Base-T and 100Base-TX devices can connect with the port in either Half- or Full-Duplex mode. 1000Base-T can be only connected in Full-duplex mode.

8. TROUBLESHOOTING

This chapter contains information to help you solve issues. If the Industrial Managed Switch is not functioning properly, make sure the Industrial Managed Switch was set up according to instructions in this manual.

■ **The Link LED is not lit**

Solution:
Check the cable connection and remove duplex mode of the Industrial Managed Switch

■ **Some stations cannot talk to other stations located on the other port**

Solution:
Please check the VLAN settings, trunk settings, or port enabled / disabled status.

■ **Performance is bad**

Solution:
Check the full duplex status of the Industrial Managed Switch. If the Industrial Managed Switch is set to full duplex and the partner is set to half duplex, then the performance will be poor. Please also check the in/out rate of the port.

■ **Why the Switch doesn't connect to the network**

Solution:

1. Check the LNK/ACT LED on the switch
2. Try another port on the Switch
3. Make sure the cable is installed properly
4. Make sure the cable is the right type
5. Turn off the power. After a while, turn on power again

■ **1000Base-T port link LED is lit, but the traffic is irregular**

Solution:
Check that the attached device is not set to dedicate full duplex. Some devices use a physical or software switch to change duplex modes. Auto-negotiation may not recognize this type of full-duplex setting.

■ **Switch does not power up**

Solution:

1. AC power cord not inserted or faulty
2. Check that the AC power cord is inserted correctly
3. Replace the power cord If the cord is inserted correctly, check that the AC power source is working by connecting a different device in place of the switch.
4. If that device works, refer to the next step.
5. If that device does not work, check the AC power

APPENDIX A: Networking Connection

A.1 Switch's Data RJ45 Pin Assignments - 1000Mbps, 1000Base-T

PIN NO	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-

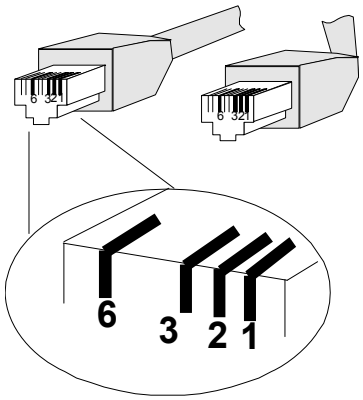
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

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

When connecting your Switch to another Fast Ethernet 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 RJ45 receptacle/ connector and their pin assignments:

RJ45 Connector pin assignment		
PIN NO	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, RJ45 pin assignment



The standard RJ45 receptacle/connector

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

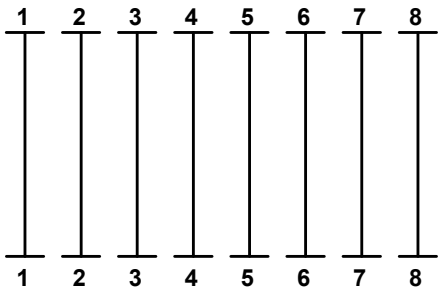
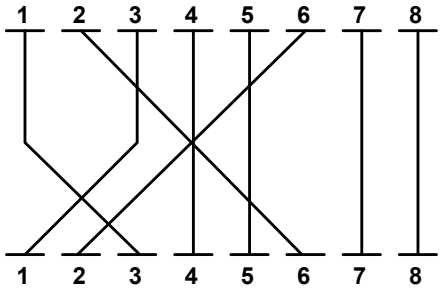
Straight Cable		SIDE 1	SIDE 2
	SIDE 1 SIDE 2	1 = White / Orange 2 = Orange 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown	1 = White / Orange 2 = Orange 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown
Crossover Cable		**SIDE 1**	**SIDE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

Figure A-1: Straight-through and Crossover Cable

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