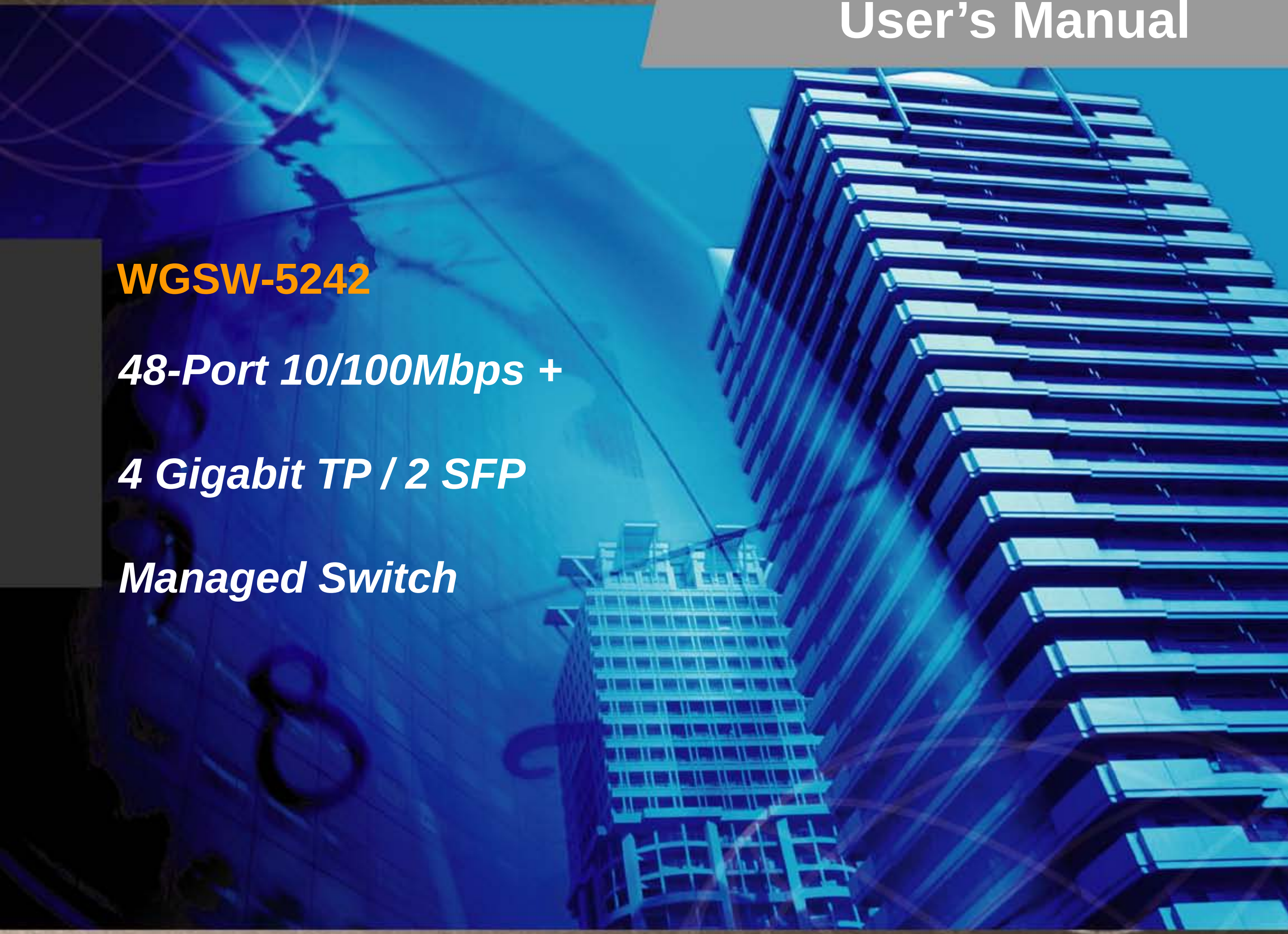
PLANET
Networking & Communication

User’s Manual



WGSW-5242

48-Port 10/100Mbps + 4 Gigabit TP / 2 SFP Managed Switch

PLANET
48-Port 10/100Mbps + 4 Gigabit / 2 SFP Managed Switch WGSW-5242

Trademarks

Disclaimer

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

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

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

FCC Warning

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

CE Mark Warning

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

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.

Without removing power cable, the device will still consuming power from the power source. In the view of Saving the Energy and reduce the unnecessary power consuming, 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

PLANET 48-Port 10/100Mbps + 4 Gigabit TP / 2 SFP Managed Switch User's Manual

FOR MODEL: WGSW-5242

REVISION: 1.0 (January.2011)

Part No: EM-WGSW-5242 (2081-A92490-000)

TABLE OF CONETNTS

1. INTRODUTION

The PLANET WGSW-5242 is 48-Port 10/100Mbps + 4 Gigabit TP / 2 SFP Managed Switch and robust layer 2+ features; the description of this model shown as below:

Terms of "**Managed Switch**" means the Switch mentioned titled in the cover page of this User's manual, i.e.WGSW-5242.

1.1 Packet Contents

Open the box of the Managed Switch and carefully unpack it. The box should contain the following items:
Check the contents of your package for following parts:

☑ **The Managed Switch**	x1
☑ **User's Manual CD**	x1
☑ **Quick Installation Guide**	x1
☑ **19" Rack Mount Accessory Kit**	x2
☑ **Power Cord**	x1
☑ **Rubber Feet**	X4
☑ **RS-232 DB9 Male Console Cable**	x1

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 against to repack the product in case there is a need to return it to us for repair.

1.2 Product Description

High-Density and Cost-effective Fast Ethernet Solution for SMB / Enterprise Network

The PLANET WGSW-5242 is a 48-Port 10/100Mbps plus 4 Gigabit TP / 2 SFP Managed Switch with advanced Web-based management support. It is ideal for small businesses, the network edge, or workgroups within large organizations where requires extra bandwidth, powerful QoS or security features. The WGSW-5242 is capable of providing non-blocking switch fabric and wire-speed throughput as high as 17.6Gbps to perform effective data traffic control for VoIP, video streaming and multicast applications in SMB and Enterprise, which greatly simplifies the tasks of upgrading the LAN for catering to increasing bandwidth demands.

Robust Layer 2 Features

The WGSW-5242 can be programmed for basic Switch management functions such as Port speed configuration, Port aggregation, VLAN, Spanning Tree protocol, QoS, bandwidth control and IGMP Snooping. The WGSW-5242 provides 802.1Q VLAN protocol, which enables you to quickly segregate network traffic by department or workgroup. The VLAN groups allowed on the WGSW-5242 will be maximally up to 256. For port aggregation, the WGSW-5242 has 4 Gigabit copper with 2 SFP fiber uplink interfaces for connecting to the core Switch that allows the operation of high-speed trunk combining multiple ports. It enables up to 6 groups of maximum 8-Port trunking, and supports fail-over as well.

Excellent Traffic Control

The WGSW-5242 is loaded with powerful traffic management and includes numerous QoS and bandwidth limiting features to ensure that traffic is prioritized properly to deliver the best possible user experience for real-time applications such as voice and video or bandwidth-intensive graphic/video file uploads or downloads. It also empowers the enterprises to take full advantages of the limited network resources and guarantees the best performance at VoIP and Video conferencing transmission.

Efficient Management

For efficient management, the WGSW-5242 Managed Ethernet Switch is equipped with console, telnet, SSH, SSL, Web and SNMP management interfaces. With its built-in Web-based management interface, the WGSW-5242 offers an easy-to-use, platform-independent management and configuration facility. The WGSW-5242 supports standard Simple Network Management Protocol (SNMP) and can be managed via any standard-based management software. For text-based management, the WGSW-5242 can be accessed via Telnet and the console port. Moreover, the WGSW-5242 offers secure remote management by supporting SSL and SSH connection which encrypts the packet content at each session.

Powerful Security

PLANET WGSW-5242 features comprehensive Access Control List (ACL) for enforcing security to the edge. Its protection mechanisms also comprise port-based 802.1x user and device authentication, which prompts end users to provide their username and password before they are permitted to pass data. The port-security is effective in limiting the numbers of clients pass through, so that network administrators can now construct highly secured corporate networks with time and effort considerably less than before. The WGSW-5242 enables you to monitor the type of traffic being transmitted on the network by many-to-one or one-to-one port mirroring function. In addition, the unicast & multicast storm control feature of the WGSW-5242 provides threshold for bandwidth used by unicast & multicast traffic.

Flexibility and Extension solution

The WGSW-5242 is well suited for applications within the enterprise data centers and distributions. The four mini-GBIC slots built in the WGSW-5242 are compatible with 100Base-FX, 1000Base-SX/LX and WDM SFP (Small Factor Pluggable) fiber-optic modules which offers great flexibility for network expansion. The distance can be extended from 550 meters (Multi-Mode fiber) up to above 10/20/30/40/50/70/120 kilometers (Single-Mode fiber or WDM fiber).

1.3 How to Use This Manual

This User Manual is structured as follows:

Section 2, **INSTALLATION**

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

Section 3, **SWITCH MANAGEMENT**

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

Section 4, **WEB CONFIGURATION**

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

Section 5, **COMMAND LINE INTERFACE**

The section describes how to use the Command Line interface (CLI).

Section 6, **CLI CONFIGURATION**

The section explains how to manage the Managed Switch by Command Line interface.

Section 7, **SWITCH OPERATION**

The chapter explains how to does the switch operation of the Managed Switch.

Section 8, **TROUBSHOOTING**

The chapter explains how to trouble shooting of the Managed Switch.

Appendix A

The section contains cable information of the Managed Switch.

1.4 Product Features

■ **Physical Port**

- □ 48-Port 10/100Base-TX Fast Ethernet RJ-45
- □ 4-Port 10/100/1000Base-T Gigabit Ethernet RJ-45
- □ 2 100/1000Base-X mini-GBIC/SFP slots, shared with Port-51 and Port-52
- □ RS-232 DB9 console interface for Switch basic management and setup

■ **Layer 2 Features**

- □ Complies with the IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z Gigabit Ethernet standards
- □ Supports Auto-Negotiation and Half-Duplex / Full-Duplex modes for all 10Base-T/100Base-TX and 1000Base-T ports
- □ Auto-MDI/MDI-X detection on each RJ-45 port
- □ Prevents packet loss Flow Control
  - IEEE 802.3x PAUSE Frame flow control for Full-Duplex mode
  - Back-Pressure Flow Control in Half-Duplex mode
- □ High performance Store and Forward architecture, broadcast storm control, runt/CRC filtering eliminate erroneous packets to optimize the network bandwidth
- □ 8K MAC address table, automatic source address learning and ageing
- □ 4Mbit embedded memory for packet buffers
- □ Supports VLAN
  - IEEE 802.1Q Tag-Based VLAN
  - GVRP for dynamic VLAN Management
  - Up to 256 VLANs groups, out of 4096 VLAN IDs
  - Private VLAN Edge (PVE) supported
  - Management VLAN
- □ Supports Link Aggregation
  - up to 6 trunk groups
  - up to 8 ports per trunk group with 1.6Gbps bandwidth (Full Duplex Mode / Fast Ethernet port)
  - up to 4 ports per trunk group with 8Gbps bandwidth (Full Duplex Mode / Gigabit Ethernet port)
  - IEEE 802.3ad LACP (Link Aggregation Control Protocol)
- □ Spanning Tree Protocol
  - STP, IEEE 802.1D (Classic Spanning Tree Protocol)
  - RSTP, IEEE 802.1w (Rapid Spanning Tree Protocol)
  - MSTP, IEEE 802.1s (Multiple Spanning Tree Protocol, spanning tree by VLAN)
- □ Port Mirroring to monitor the incoming or outgoing traffic on a particular port (many to one)

■ **Quality of Service**

- □ 4 priority queues on all Switch ports
- □ Traffic classification
  - IEEE 802.1p CoS
  - IP TOS / DSCP / IP Precedence
  - Port-Based QoS
- □ Supports QoS and In/Out bandwidth control on each port

- **Multicast**
  - □ Supports IGMP Snooping v1 and v2
  - □ IGMP Querier / IGMP Proxy / IGMP Immediately Leave support

- **Security**
  - □ IEEE 802.1x Port-Based Authentication
  - □ IP-Based Access Control List (ACL)
  - □ MAC-Based Access Control List
  - □ Port Security
  - □ Supports Auto DoS
  - □ Port Self-loop Detection

- **Management**
  - □ Switch Management Interface
    - Console / Telnet Command Line Interface
    - Web switch management
    - SNMP v1, v2c, and v3 switch management
    - SSH / SSL secure access
  - □ DHCP client for IP address assignment
  - □ Supports DHCP relay function
  - □ Built-in Trivial File Transfer Protocol (TFTP) client
  - □ Firmware upload / download via TFTP or HTTP protocol
  - □ Configuration upload / download via TFTP or HTTP protocol
  - □ SNTP (Simple Network Time Protocol)
  - □ Logging to syslog server
  - □ Four RMON groups 1, 2, 3, 9 (history, statistics, alarms, and events)
  - □ Supports Ping function
  - □ Cable Diagnostic technology provides the mechanism to detect and report potential cabling issues such as cable opens, cable shorts, and etc. on Copper Links
  - □ Link Layer Discovery Protocol (LLDP)
  - □ Management IP
  - □ Supports memory & flash log

1.5 Product Specification

Product	**WGSW-5242** 48-Port 10/100Mbps + 4 Gigabit TP / 2 SFP Managed Switch
Hardware Specification	
Copper Ports	48 10/100Base-TX + 4 10/ 100/1000Base-T RJ-45 Auto-MDI/MDI-X ports
SFP / mini-GBIC slots	2 100/1000Base-X SFP interfaces, shared with Port-51 and Port-52
Switch Architecture	Store-and-Forward
Switch Fabric	17.6Gbps / non-blocking
Switch throughput	13.09Mpps
Address Table	8K MAC address table with Auto learning function
Share data Buffer	4Mbits
Flow Control	Back pressure for Half-Duplex IEEE 802.3x Pause Frame for Full-Duplex
LED	Power, Link/Act per port
Reset Button	< 5 sec: System reboot > 10 sec: Factory Default
Dimension (W x D x H)	430 x 250x 44.5 mm, 1U height
Weight	2672g
Power Consumption	27.8 Watts / 110.70 BTU (Maximum)
Power Requirement	AC 100~240V, 50/60Hz ,2.2A (Maximum)
Layer Function	
Management Interface	Console, Telnet, SSH, Web Browser, SSL, SNMPv1, v2c and 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
VLAN	IEEE 802.1Q Tag-Based VLAN GVRP for VLAN Management Up to 256 VLANs groups, out of 4049 VLAN IDs Private VLAN Edge (PVE) supported
Bandwidth Control	Ingress Rate Limit Egress Traffic Shaper
Link Aggregation	IEEE 802.3ad LACP Supports 6 groups of 8-Port trunk
QoS	Traffic classification based on 802.1p priority, IP TOS / DSCP / IP Precedence
IGMP Snooping	IGMP (v1/v2) Snooping, IGMP Querier mode
Access Control List	IP-Based ACL / MAC-Based ACL Up to 128 entries

SNMP MIBs	RFC-1213 MIB-II RFC-2863 Interface MIB RFC-2665 EtherLike MIB RFC-1493 Bridge MIB RFC-2674 Extended Bridge MIB RFC-2819 RMON MIB (Group 1, 2, 3 and 9) RFC-2737 Entity MIB RFC-2618 RADIUS Client MIB
Standard Conformance	
Regulation Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX / 100Base-FX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000T IEEE 802.3x Flow Control and Back pressure IEEE 802.3ad Port trunk with LACP IEEE 802.1D Spanning tree protocol IEEE 802.1w Rapid spanning tree protocol IEEE 802.1s Multiple Spanning tree protocol IEEE 802.1p Class of service IEEE 802.1Q VLAN Tagging IEEE 802.1x Port Authentication Network Control IEEE 802.1ad LLDP

2. INSTALLATION

This section describes the hardware features and installation of the Managed Switch on the desktop or rack mount. For easier management and control of the 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 Managed Switch, please read this chapter completely.

2.1 Hardware Description

2.1.1 Switch Front Panel

The unit front panel provides a simple interface monitoring the switch. Figure 2-1 shows the front panel of the Managed Switches.

WGSW-5242 Front Panel

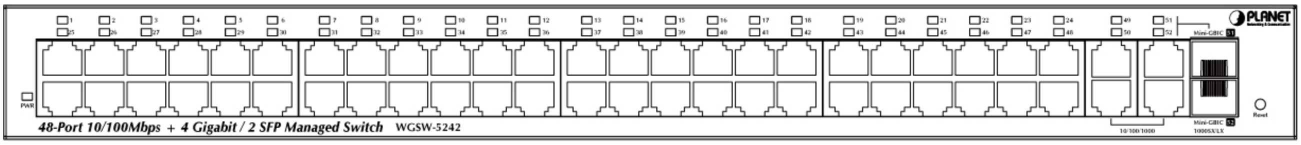


Figure 2-1 WGSW-5242 front panel.

- **Fast Ethernet TP interface** (Port-1 ~ Port-48)

  10/100ase-TX Copper, RJ-45 Twist-Pair: Up to 100 meters.

- **Gigabit TP interface** (Port-49 ~ Port-52)

  10/100/1000Base-T Copper, RJ-45 Twist-Pair: Up to 100 meters.

- **Gigabit SFP slots** (Shared with 10/100/1000Base-T Port-51 and Port-52)

  1000Base-SX/LX mini-GBIC slot, SFP (Small Factor Pluggable) transceiver module: From 550 meters (Multi-mode fiber), up to 10/30/50/70/120 kilometers (Single-mode fiber).

- **Reset button**

  At the left of front panel, the reset button is designed for reboot the Managed Switch without turn off and on the power. The following is the summary table of Reset button functions:

Reset Button Pressed and Released	Function
< 5 sec: System reboot	Reboot the Managed Switch
> 10 sec: Factory Default	Reset the Managed Switch to Factory Default configuration. The Managed Switch will then reboot and load the default settings as below: Default Password: **admin** Default IP Address: **192.168.0.100** Subnet Mask: **255.255.255.0** Default Gateway: **192.168.0.254**

2.1.2 LED Indications

The front panel LEDs indicates instant status of port links, data activity, system operation and system power, helps monitor and troubleshoot when needed.

WGSW-5242 LED Indication

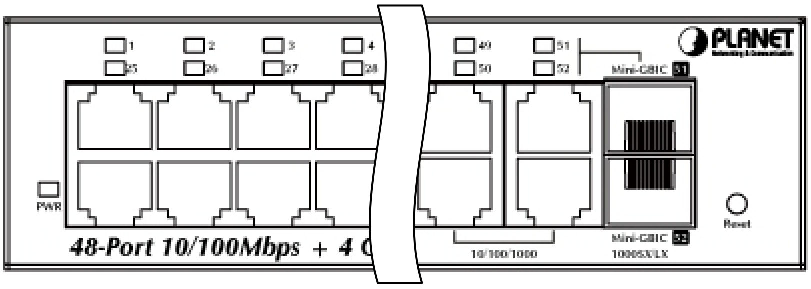


Figure 2-2 WGSW-5242 LED panel

LED Definition

- **System**

LED	Color	Function
PWR	**Green**	Lights to indicate that the Switch has power.

- **Per 10/100/Base-T RJ-45 port** (Port-1 ~ Port-48)

LED	Color	Function
LNK/ACT	**Orange**	**Lights** to indicate the link through that port is successfully established. **Blink**: indicate that the Switch is actively sending or receiving data over that port.

- **Per 10/100/1000Base-T RJ-45 port** (Port-49 ~ Port-52)

LED	Color	Function
LNK/ACT (Dual Color)	**Orange**	**Lights** to indicate the port is running in 1000Mbps speed. **Blink**: indicate that the Switch is actively sending or receiving data over that port.
	Green	**Lights**: indicate that the port is operating at 10Mbps or 100Mbps. **Blink**: indicate that the Switch is actively sending or receiving data over that port.

- **Per SFP interfaces** (Shared with 10/100/1000Base-T Port-51 and Port-52)

LED	Color	Function
LNK/ACT (Dual Color)	**Orange**	**Lights** to indicate the port is running in 1000Mbps speed. **Blink**: indicate that the Switch is actively sending or receiving data over that port.
	Green	**Lights**: indicate that the port is operating at 100Mbps. **Blink**: indicate that the Switch is actively sending or receiving data over that port.

2.1.3 Switch Rear Panel

The rear panel of the Managed Switch indicates an AC inlet power socket, which accept input power from 100 to 240V AC, 50-60Hz. Figure 2-3 shows the rear panel of these Managed Switch.

WGSW-5242 Rear Panel

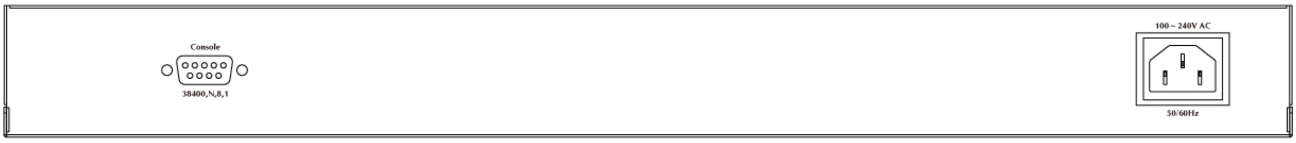


Figure 2-3 Rear panel of WGSW-5242

- **Console Port**

  The console port is a DB9, RS-232 male seria port connector. It is an interface for connecting a terminal directly. Through the console port, it provides rich diagnostic information includes IP Address setting, factory reset, port management, link status and system setting. Users can use the attached RS-232 cable in the package and connect to the console port on the device. After the connection, users an run any terminal emulation program (Hyper Terminal, ProComm Plus, Telix, Winterm and so on) to enter the statup screen of the device.

- **AC Power Receptacle**

  For compatibility with electric service in most areas of the world, the Managed Switch's power supply automatically adjusts to line power in the range 100-240VAC and 50/60 Hz.

  Plug the female end of the power cord firmly into the receptalbe on the rear panel of the Managed Switch. Plug the other end of the power cord into an electric service outlet then the power will be ready.

Power Notice:

The device is a power-required device, it means, it will not work till it is powered. If your networks should active all the time, please consider using UPS (Uninterrupted Power Supply) for your device. It will prevent you from network data loss or network downtime.

In some area, installing a surge suppression device may also help to protect your Managed Switch from being damaged by unregulated surge or current to the Switch or the power adapter.

2.2 Install the Switch

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

2.2.1 Desktop Installation

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

Step1: Attach the rubber feet to the recessed areas on the bottom of the Managed Switch.

Step2: Place the Managed Switch on the desktop or the shelf near an AC power source, as shown in Figure 2-4.

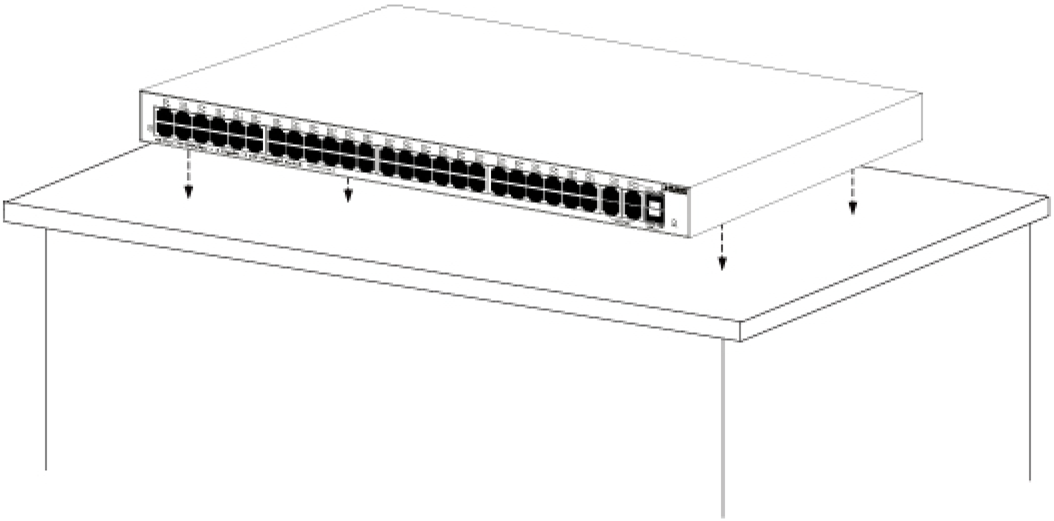


Figure 2-4 Place the Managed Switch on the desktop

Step3: Keep enough ventilation space between the 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 Specification.

Step4: Connect the Managed Switch to network devices.

Connect one end of a standard network cable to the 10/100/1000 RJ-45 ports on the front of the Managed Switch

Connect the other end of the cable to the network devices such as printer servers, workstations or routers…etc.

> Note
>
> Connection to the Managed Switch requires UTP Category 5 network cabling with RJ-45 tips. For more information, please see the Cabling Specification in Appendix A.

Step5: Supply power to the Managed Switch.

Connect one end of the power cable to the Managed Switch.

Connect the power plug of the power cable to a standard wall outlet.

When the Managed Switch receives power, the Power LED should remain solid Green.

2.2.2 Rack Mounting

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

Step1: Place the Managed Switch on a hard flat surface, with the front panel positioned towards the front side.

Step2: Attach the rack-mount bracket to each side of the Managed Switch with supplied screws attached to the package.

Figure 2-5 shows how to attach brackets to one side of the Managed Switch.

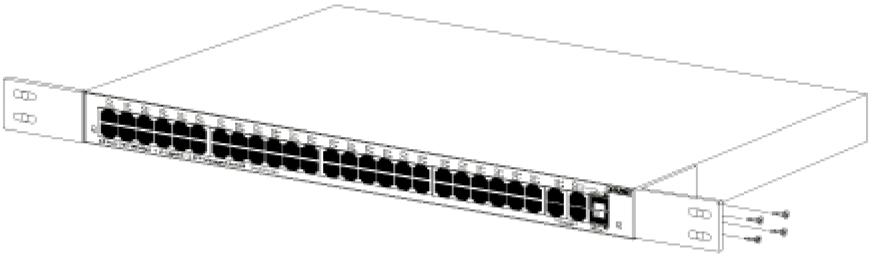


Figure 2-5 Attach brackets to the Managed Switch.

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

Step3: Secure the brackets tightly.

Step4: Follow the same steps to attach the second bracket to the opposite side.

Step5: After the brackets are attached to the Managed Switch, use suitable screws to securely attach the brackets to the rack, as shown in Figure 2-6.

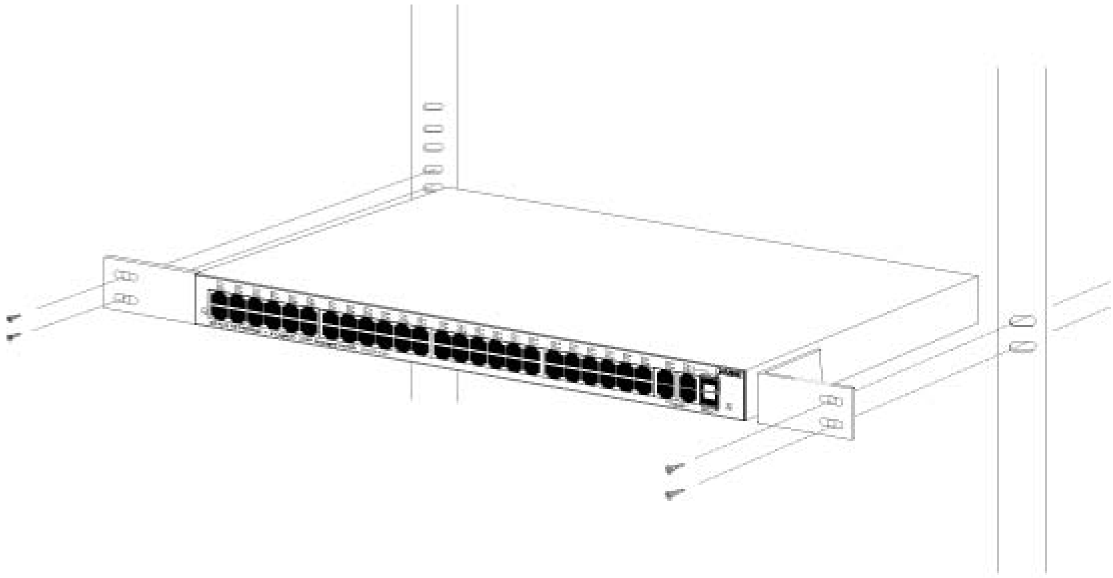


Figure 2-6 Mounting Managed Switch in a Rack

Step6: Proceeds with the steps 4 and steps 5 of session 2.2.1 Desktop Installation to connect the network cabling and supply power to the Managed Switch.

2.2.3 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 Managed Switch. As the Figure 2-7 appears.

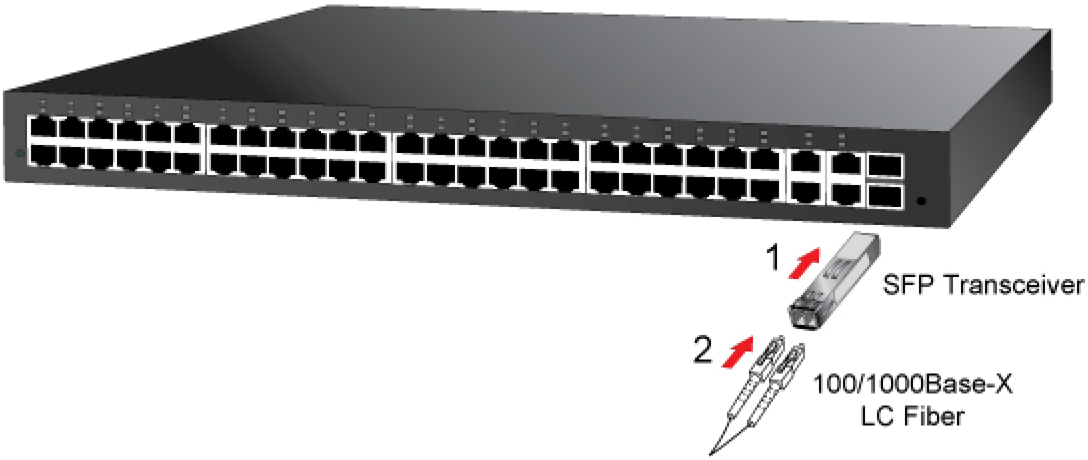


Figure 2-7 Plug-in the SFP transceiver

■ Approved PLANET SFP Transceivers

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

Module Name	Description
MGB-GT	SFP-Port 1000Base-T Module
MGB-SX	SFP-Port 1000Base-SX mini-GBIC module - 550m
MGB-LX	SFP-Port 1000Base-LX mini-GBIC module -10km
MGB-L30	SFP-Port 1000Base-LX mini-GBIC module - 30km
MGB-L50	SFP-Port 1000Base-LX mini-GBIC module - 50km
MGB-L70	SFP-Port 1000Base-LX mini-GBIC module - 70km
MGB-L120	SFP-Port 1000Base-LX mini-GBIC module - 120km
MGB-LA10	SFP-Port 1000Base-LX (WDM,TX:1310nm) mini-GBIC module - 10km
MGB-LB10	SFP-Port 1000Base-LX (WDM,TX:1550nm) mini-GBIC module - 10km
MGB-LA20	SFP-Port 1000Base-LX (WDM,TX:1310nm) mini-GBIC module - 20km
MGB-LB20	SFP-Port 1000Base-LX (WDM,TX:1550nm) mini-GBIC module - 20km
MGB-LA40	SFP-Port 1000Base-LX (WDM,TX:1310nm) mini-GBIC module - 40km
MGB-LB40	SFP-Port 1000Base-LX (WDM,TX:1550nm) mini-GBIC module - 40km
MFB-FX	SFP-Port 100Base-FX Transceiver (1310nm) - 2km
MFB-F20	SFP-Port 100Base-FX Transceiver (1310nm) - 20km
MFB-F40	SFP-Port 100Base-FX Transceiver (1310nm) - 40KM
MFB-F60	SFP-Port 100Base-FX Transceiver (1310nm) - 60KM
MFB-FA20	SFP-Port 100Base-BX Transceiver (WDM,TX:1310nm) - 20km
MFB-FB20	SFP-Port 100Base-BX Transceiver (WDM,TX:1550nm) - 20km

Note

It recommends using PLANET SFPs on the Managed Switch. If you insert a SFP transceiver that is not supported, the Managed Switch will not recognize it.

Before connect the other Managed Switches, workstation or Media Converter.

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

■ Connect the fiber cable

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

■ Remove the transceiver module

1. Make sure there is no network activity by consult or check with the network administrator. Or through the management interface of the switch/converter (if available) to disable the port in advance.
2. Remove the Fiber Optic Cable gently.
3. Turn the handle of the MGB/MFB module to horizontal.
4. Pull out the module gently through the handle.

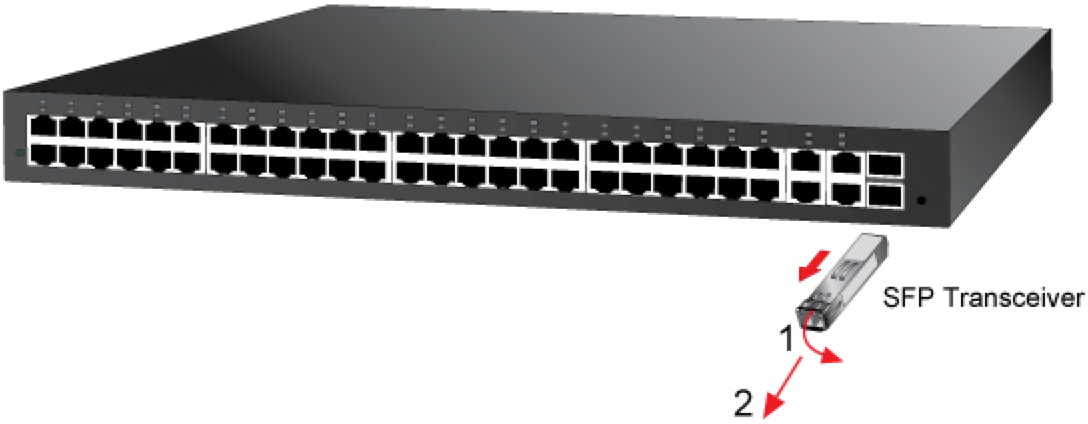


Figure 2-8 Pull out the SFP transceiver

Note

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

3. SWITCH MANAGEMENT

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

This chapter covers the following topics:

- Requirements
- Management Access Overview
- Administration Console Access
- Web Management Access
- SNMP Access
- Standards, Protocols, and Related Reading

3.1 Requirements

- **Workstations** of subscribers running Windows 2000/XP/2003/Vista/7/2008, MAC OS9 or later, Linux, UNIX or other platform compatible with **TCP/IP** protocols.
- **Workstation** installed with **Ethernet NIC** (Network Interface Card)
- **Serial Port** connect (Terminal)
  - Above PC with COM Port (DB-9 / RS-232) or USB-to-RS-232 converter
- Ethernet Port connect
  - Network cables - Use standard network (UTP) cables with RJ-45 connectors.
- Above Workstation installed with **WEB Browser** and **JAVA runtime environment** Plug-in

Note

It is recommended to use Internet Explore 7.0 or above to access Managed Switch.

3.2 Management Access Overview

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

- An administration **console**
- **Web browser** interface
- An external **SNMP-based network management application**

The administration console and Web browser interface support are embedded in the 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 switch or use dial-up connection • Not convenient for remote users • Modem connection may prove to be unreliable or slow
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 Management Methods Comparison

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 switch's console (serial) port. There are two ways to use this management method: via direct access or modem port access. The following sections describe these methods. For more information about using the console, refer to **Chapter 5 Command Line Interface Console Management**.

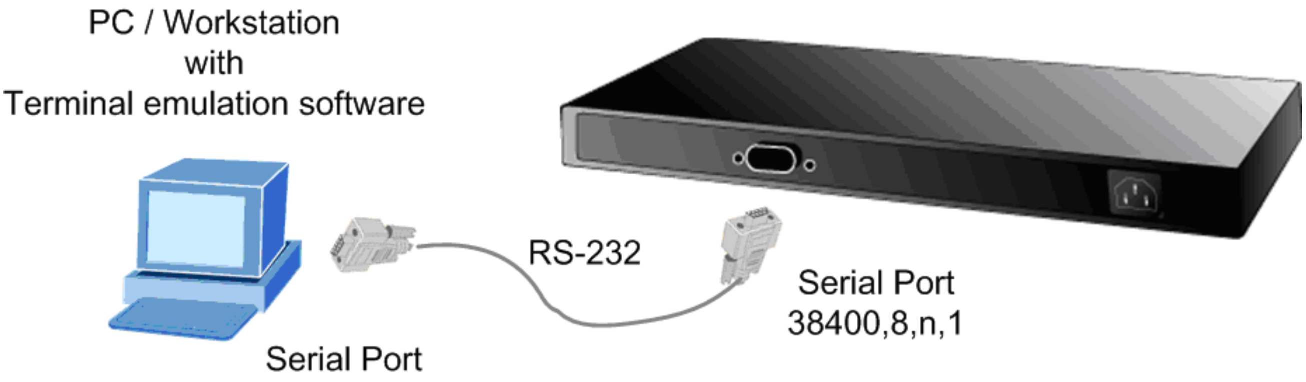


Figure 3-1 Console management

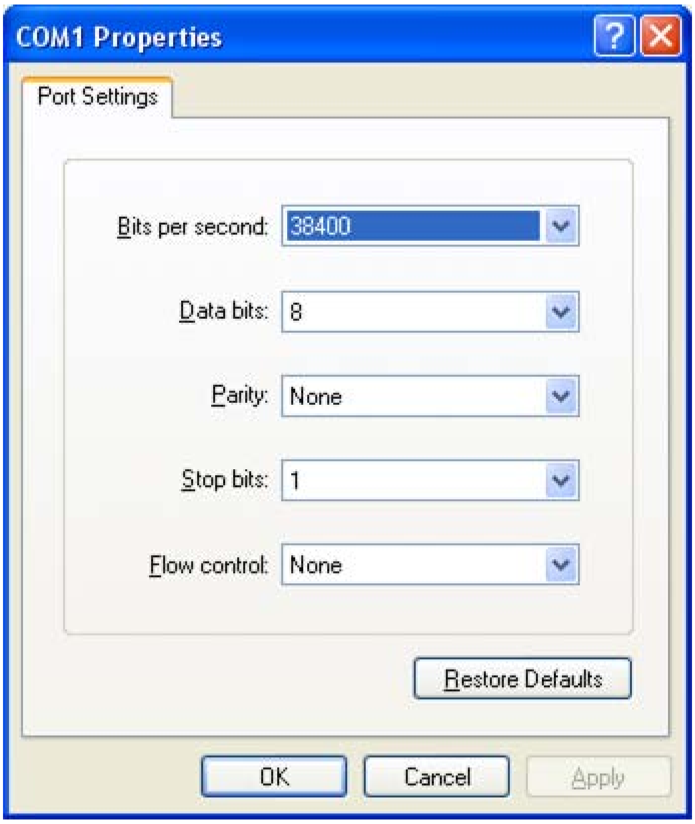
Direct Access

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 RS-232 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:

- **38400 bps**
- **8 data bits**
- **No parity**
- **1 stop bit**



Bits per second: 38400

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

Figure 3-2 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 Managed 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.

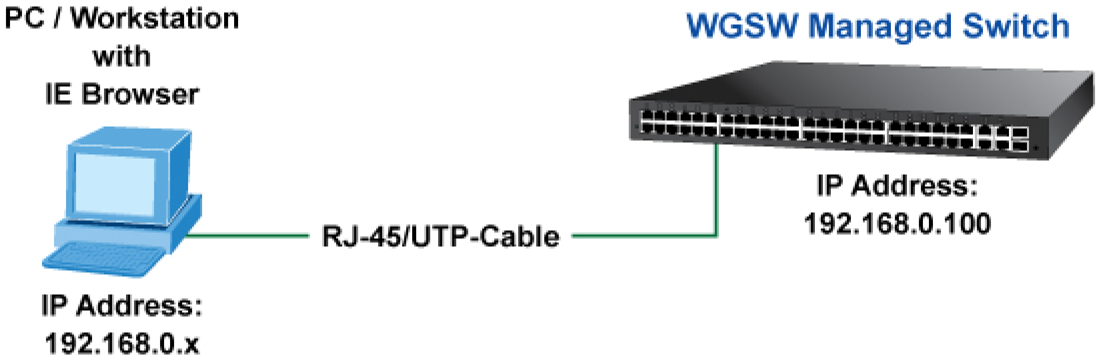
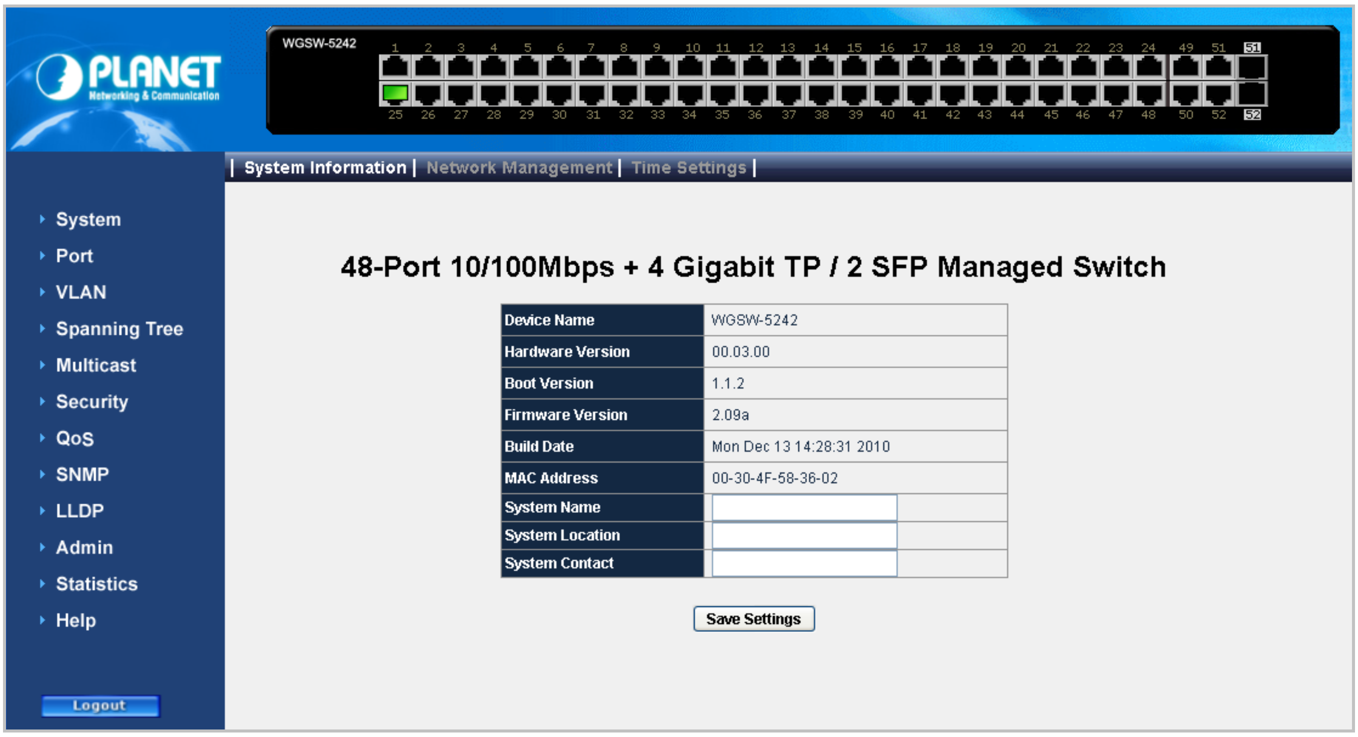


Figure 3-3 Web management

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 3.0** or later.



48-Port 10/100Mbps + 4 Gigabit TP / 2 SFP Managed Switch

Device Name	WGSW-5242
Hardware Version	00.03.00
Boot Version	1.1.2
Firmware Version	2.09a
Build Date	Mon Dec 13 14:28:31 2010
MAC Address	00-30-4F-58-36-02
System Name	
System Location	
System Contact	

Figure 3-4 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 SNMPc 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 Net-work 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 gets and sets community strings for the Managed Switch are public.

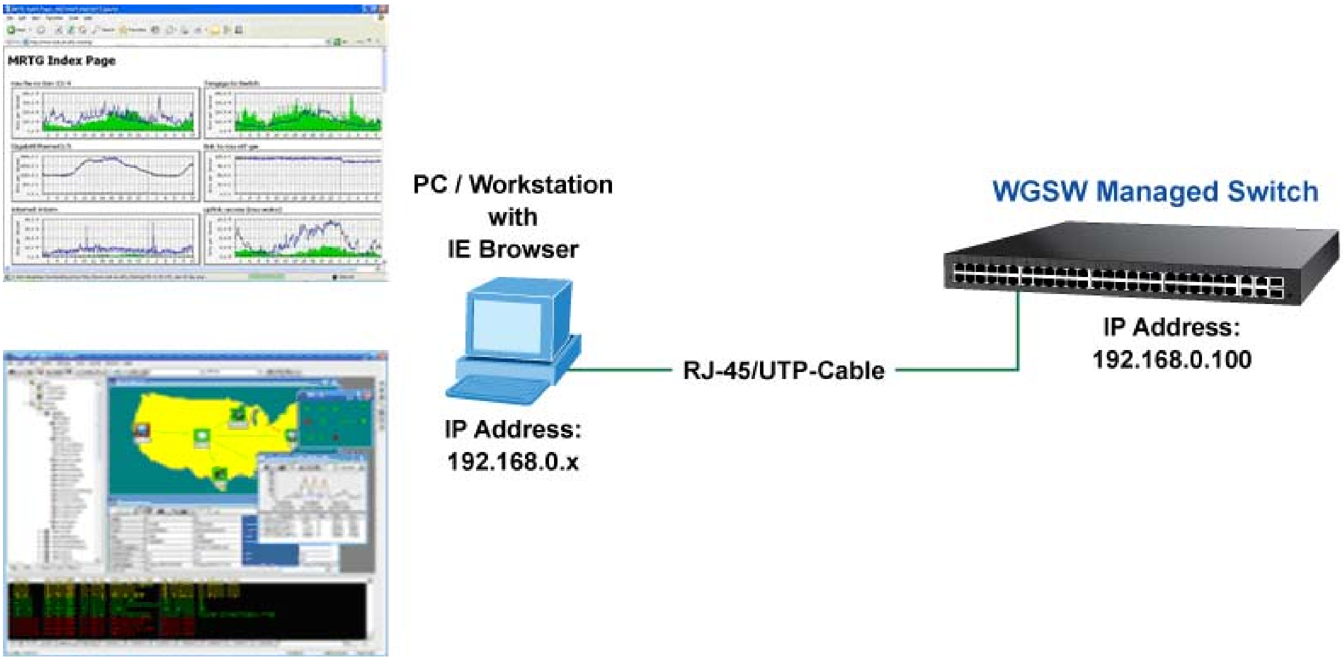


Figure 3-5 SNMP management

3.6 Protocols

The Managed Switch supports the following protocols:

- Virtual terminal protocols, such as Telnet
- Simple Network Management Protocol (SNMP)

3.6.1 Virtual Terminal Protocols

A virtual terminal protocol is a software program, such as **Telnet**, that allows you to establish a management session from a Macintosh, a PC, or a UNIX workstation. Because Telnet runs over TCP/IP, you must have at least one IP address configured on the Managed Switch before you can establish access to it with a virtual terminal protocol.

Terminal emulation differs from a virtual terminal protocol in that you must connect a terminal directly to the console (serial) port.

To access the Managed Switch through a Telnet session:

1. Be Sure of the Managed Switch is configured with an IP address and the Managed Switch is reachable from a PC.
2. Start the Telnet program on a PC and connect to the Managed Switch.

The management interface is exactly the same with RS-232 console management.

3.6.2 SNMP Protocol

Simple Network Management Protocol (SNMP) is the standard management protocol for multi-vendor IP networks. SNMP supports transaction-based queries that allow the protocol to format messages and to transmit information between reporting devices and data-collection programs. SNMP runs on top of the User Datagram Protocol (UDP), offering a connectionless-mode service.

3.6.3 Management Architecture

All of the management application modules use the same Messaging Application Programming Interface (MAPI). By unifying management methods with a single MAPI, configuration parameters set using one method (console port, for example) are immediately displayable by the other management methods (for example, SNMP agent of Web browser).

The management architecture of the switch adheres to the IEEE open standard. This compliance assures customers that the Managed Switch is compatible with, and will interoperate with other solutions that adhere to the same open standard.

4. WEB CONFIGURATION

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

About Web-based 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.

The Web-Based Management supports Internet Explorer 7.0. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present 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 Managed Switch can be configured through an Ethernet connection, make sure the manager PC must be set on same the IP subnet address with the Managed Switch.

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

If you have changed the default IP address of the Managed 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.

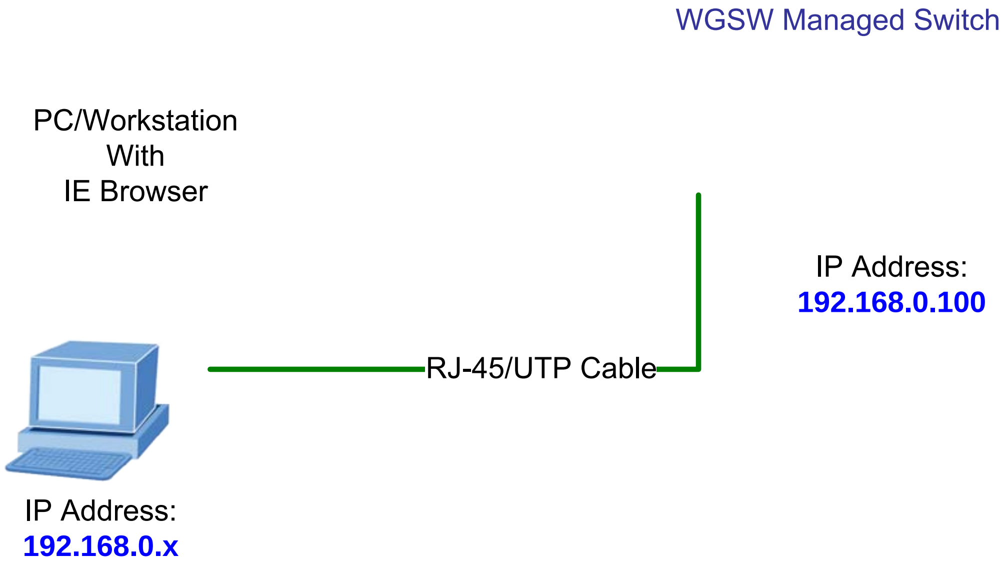


Figure 4-1-1 Web Management

- **Logging on the 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 as following:

http://192.168.0.100

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

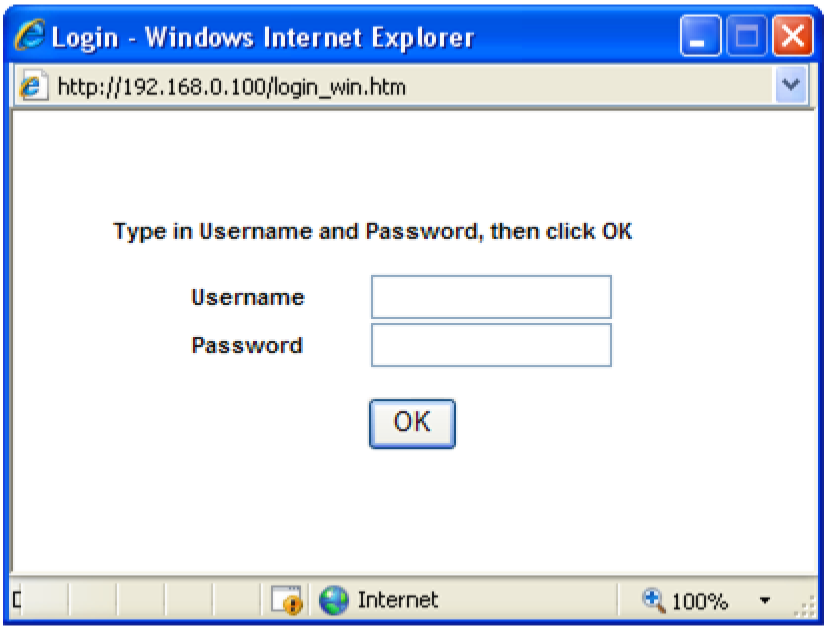
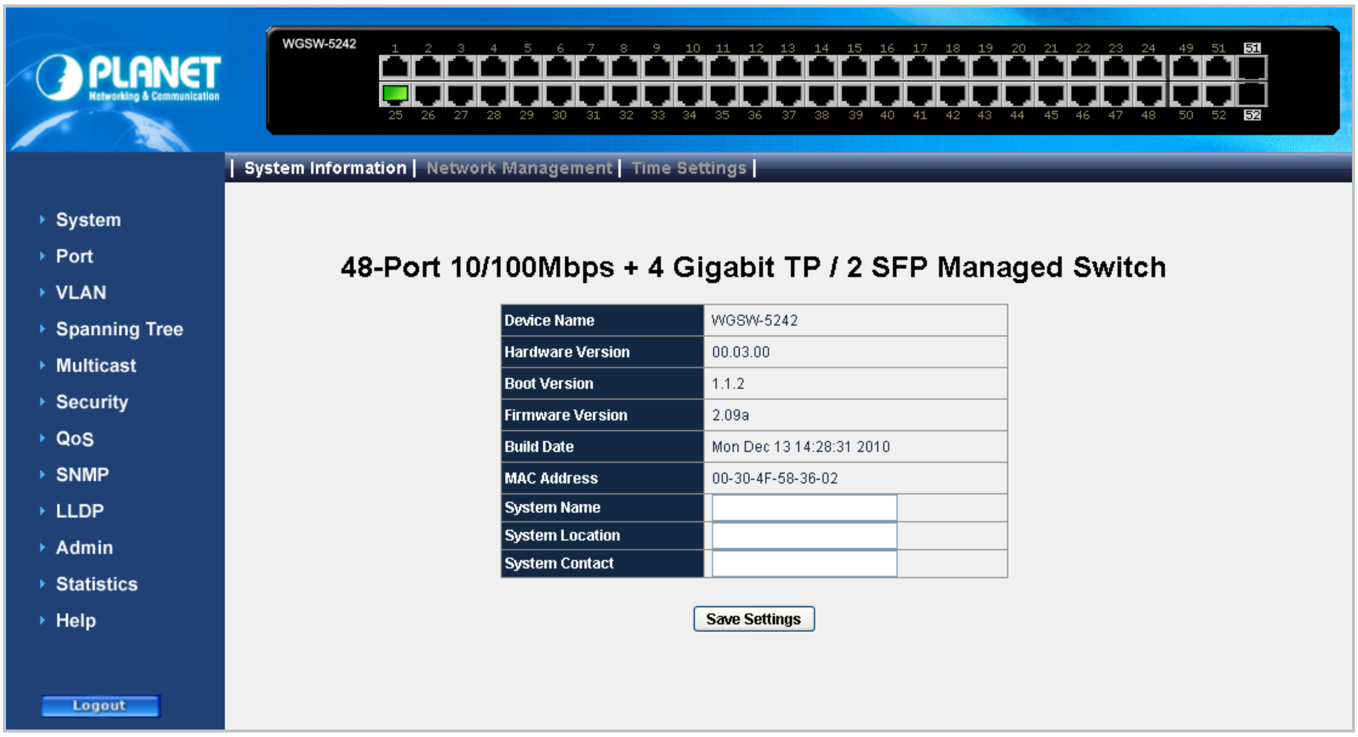

Login - Windows Internet Explorer
http://192.168.0.100/login_win.htm
Type in Username and Password, then click OK
Username
Password
OK
Internet
100%

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.



48-Port 10/100Mbps + 4 Gigabit TP / 2 SFP Managed Switch

Device Name	WGSW-5242
Hardware Version	00.03.00
Boot Version	1.1.2
Firmware Version	2.09a
Build Date	Mon Dec 13 14:28:31 2010
MAC Address	00-30-4F-58-36-02
System Name	
System Location	
System Contact	

Figure 4-1-3 Web main page

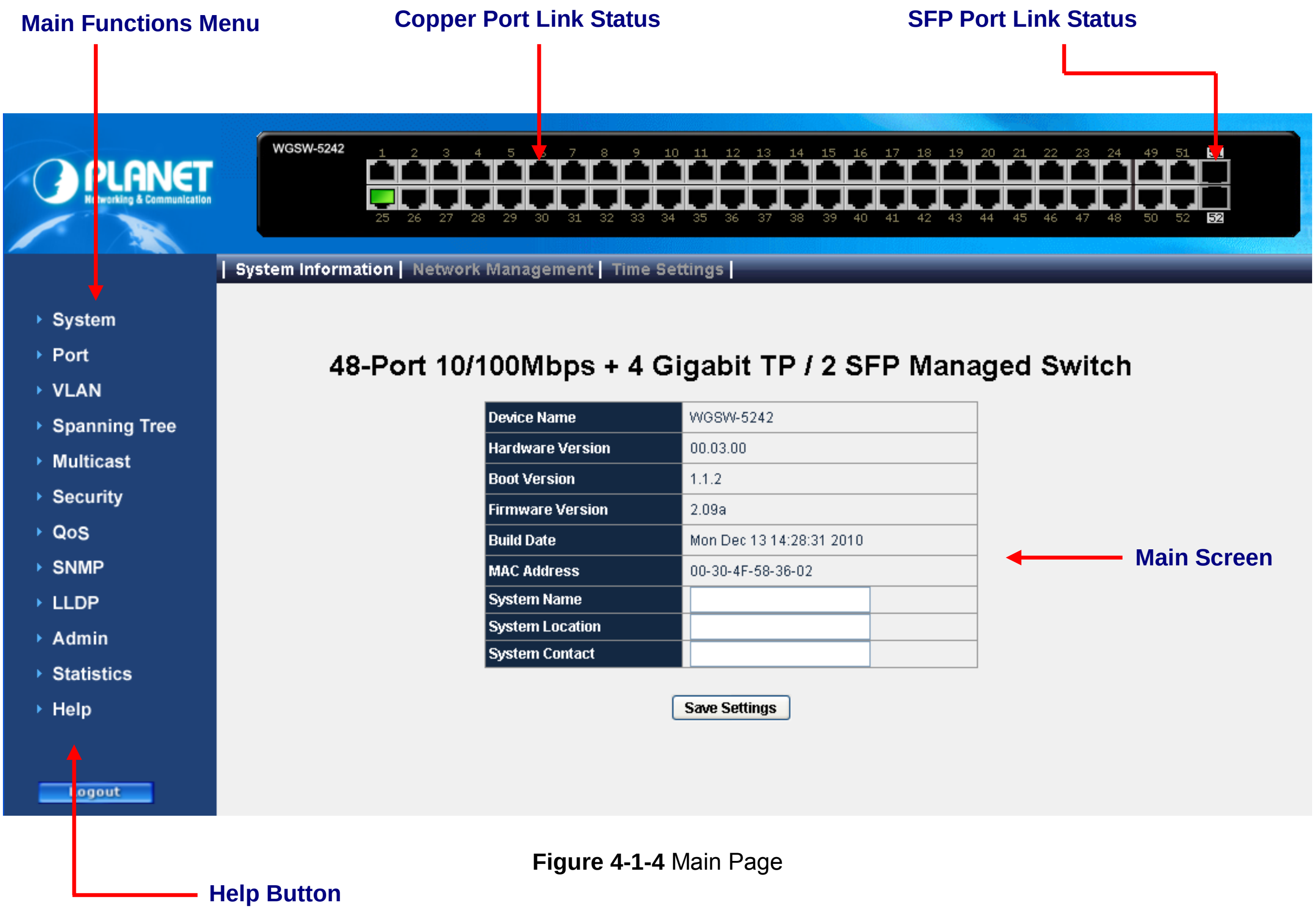
Now, you can use the Web management interface to continue the switch management or manage the Managed Switch by Web interface. The Switch Menu on the left of the web page let you access all the commands and statistics of the Managed Switch.

Note

1. It is recommended to use Internet Explore 7.0 or above to access Managed Switch.
2. The IP address changed take effect immediately after click on the **Save** button, you need to use the new IP address to access the Web interface.
3. For security reason, please change and memorize the new password after this first setup.
4. Only accept command in lowercase letter under web interface.

4.1 Main Web Page

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



48-Port 10/100Mbps + 4 Gigabit TP / 2 SFP Managed Switch

Device Name	WGSW-5242
Hardware Version	00.03.00
Boot Version	1.1.2
Firmware Version	2.09a
Build Date	Mon Dec 13 14:28:31 2010
MAC Address	00-30-4F-58-36-02
System Name	
System Location	
System Contact	

Save Settings

Figure 4-1-4 Main Page

Panel Display

The web agent displays an image of the 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	Disabled	Down	Link
RJ-45 Ports	🟥	⬛	🟩
SFP Ports	🟥	⬛	🟩

Main Menu

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

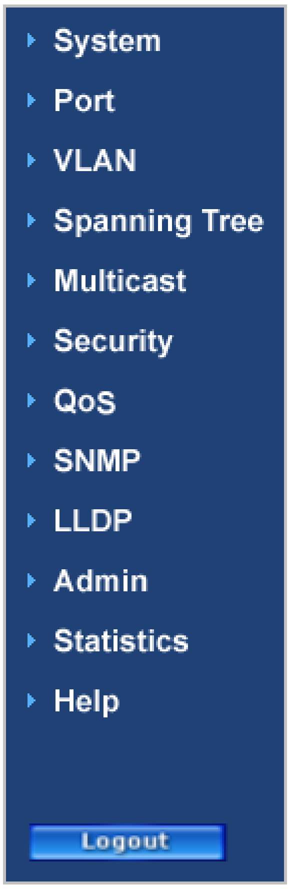


Figure 4-1-5 Managed Switch Main Funcrions Menu

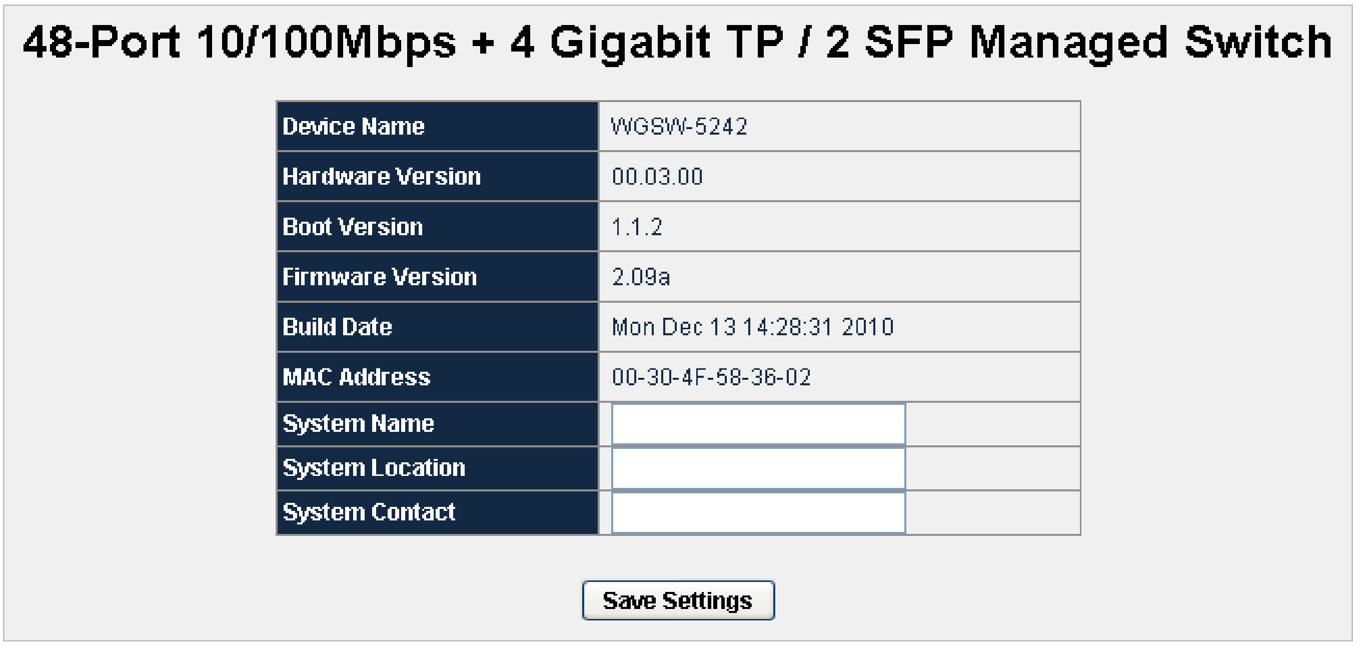
4.2 System

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

- **System Information**
- **Network Management**
- **Time Settings**

4.2.1 System Information

The **System Info** page provides information for the current device information. System Info page helps a switch administrator to identify the hardware MAC address, software version and system uptime.



48-Port 10/100Mbps + 4 Gigabit TP / 2 SFP Managed Switch

Device Name	WGSW-5242
Hardware Version	00.03.00
Boot Version	1.1.2
Firmware Version	2.09a
Build Date	Mon Dec 13 14:28:31 2010
MAC Address	00-30-4F-58-36-02
System Name	
System Location	
System Contact	

Figure 4-2-1 System Information Screenshot

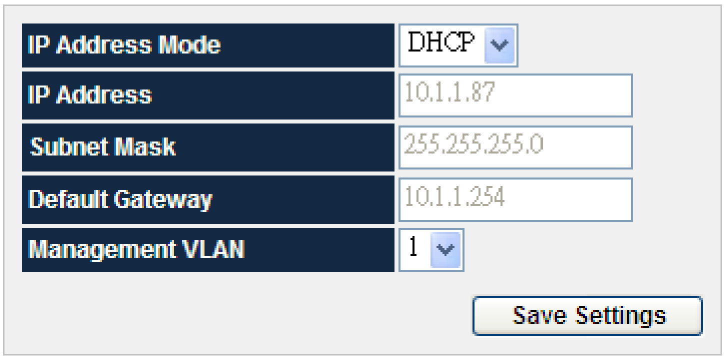
The page includes the following fields:

Object	Description
• **Device Name**	Displays the switch model name.
• **Hardware Version**	Displays the hardware version number.
• **Boot Version**	Displays the switch boot version.
• **Firmware Version**	Displays the switch firmware version.
• **Build Date**	Displays the firmware built date.
• **MAC Address**	Displays the MAC address of the switch.
• **System Name**	Displays the user-defined system name.
• **System Location**	Displays the user-defined system location.

• **System Contact**	Displays the user-defined system contact person.

4.2.2 Network Management

The **Network Managment** includes the IP Address, Subnet Mask and Gateway. The Configured column is used to view or change the IP configuration.Fill up the IP Address, Subnet Mask and Gateway for the device. The screen in Figure 4-2-2 appears.



IP Address Mode	DHCP
IP Address	10.1.1.87
Subnet Mask	255.255.255.0
Default Gateway	10.1.1.254
Management VLAN	1

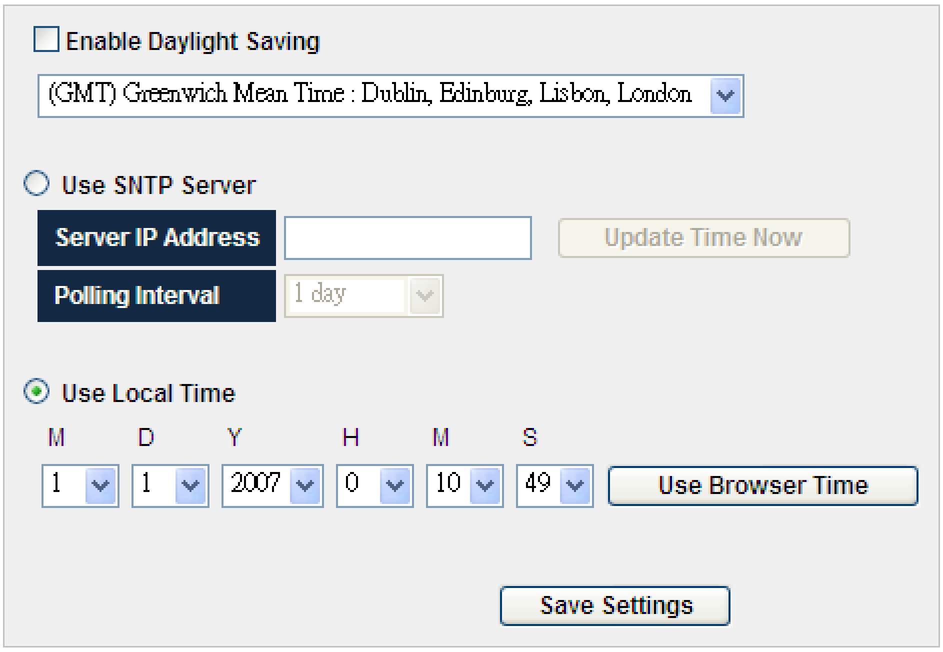
Figure 4-2-2 Network Management screenshot

The page includes the following fields:

Object	Description
• **IP Address Mode**	Retrieves the IP address using **DHCP** or **Static**. The possible field values are DHCP that retrieves the IP addresses using DHCP client; Static indicates IP address is statically assigned. If Static was selected, the IP Address, Subnet Mask and Default Gateway fields are available.
• **IP Address**	Defines the IP address of the system.
• **Subnet Mask**	Defines the subnet mask of the system.
• **Default Gateway**	Defines the default gateway IP address of the system.
• **Management VLAN**	Indicates the VLAN group that system belongs to.

4.2.3 Time Setting

In the System sub-function menu, you can see the **Time Setting**, by which you can configure the time settings for the Managed Switch. You can specify SNTP Servers and set GMT Timezone. The SNTP Configuration screen in Figure 4-2-3 appears.



☐ Enable Daylight Saving

(GMT) Greenwich Mean Time : Dublin, Edinburg, Lisbon, London

○ Use SNTP Server

Server IP Address

Polling Interval: 1 day

● Use Local Time

M	D	Y	H	M	S
1	1	2007	0	10	49

Figure 4-2-3 Time Settings Screenshot

The page includes the following fields:

Object	Description
• **Daylight Saving**	Indicates the Daylight Savings Time (DST) on the device based on the devices location. When daylight saving is enabled, one hour will be added to time zone offset value. (Only for SNTP)
• **Time Zone**	Specifies the difference between Greenwich Mean Time (GMT) and local time. For example, the Time Zone Offset for Paris is GMT +1, while the local time in New York is GMT -5. (Only for SNTP)
• **Use SNTP Server**	The device supports the Simple Network Time Protocol (SNTP). SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. The device operates only as an SNTP client, and cannot provide time services to other systems. The device can poll the following server types for the server time: **Server IP Address** - Sets the SNTP server's IP address. **Update Time Now** - Synchronizes current device time with the SNTP server right away. **Polling Interval** - Sets the interval at which SNTP client polls for time.
• **Use Local Time**	M**:** Month - Sets the month. D: Day - Sets the day. Y: Year - Sets the year.

H: Hours - Sets the hours.

M: Minutes - Sets the minutes.

S: Seconds - Sets the seconds.

Use Browser Time - The device system time is configured by your Desktop/Laptop's time setting.

Use Browser Time - Synchronizes current device time with the web browser right away.

4.3 Port Management

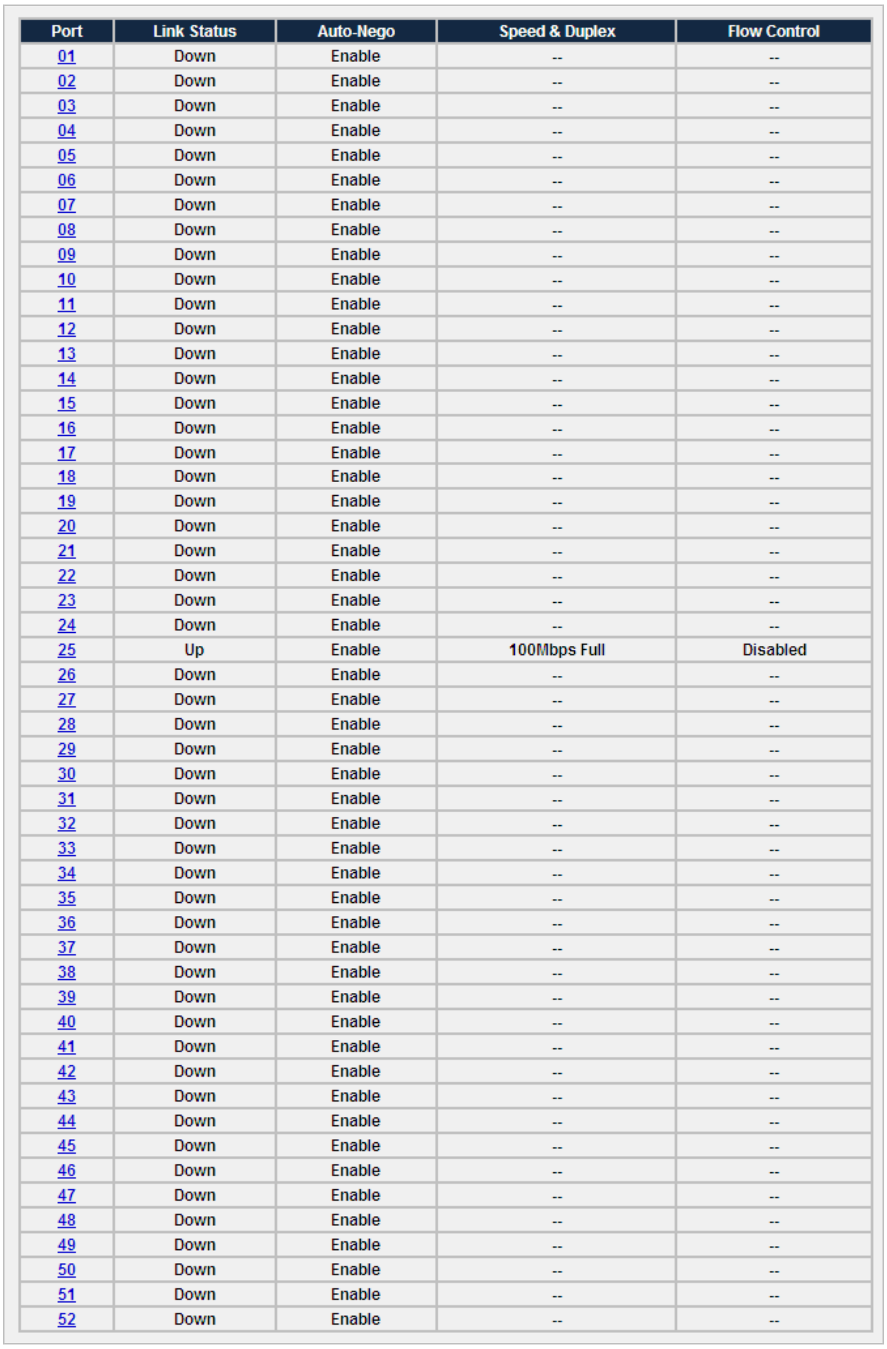
Use the Port Menu to display or configure the Managed Switch's ports. This section has the following items:

- **Port Configuration**
- **LACP Property**
- **LAG Group**

4.3.1 Port Configuration

This page displays current port configurations. Ports can also be configured here.

The port settings relate to the currently selected stack unit, as reflected by the page header.

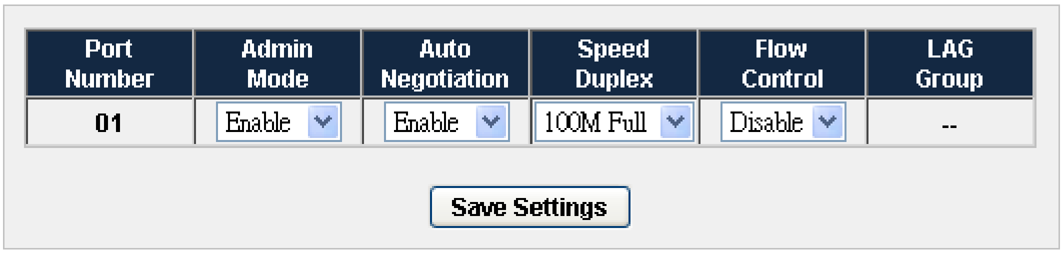


Port	Link Status	Auto-Nego	Speed & Duplex	Flow Control
01	Down	Enable	--	--
02	Down	Enable	--	--
03	Down	Enable	--	--
04	Down	Enable	--	--
05	Down	Enable	--	--
06	Down	Enable	--	--
07	Down	Enable	--	--
08	Down	Enable	--	--
09	Down	Enable	--	--
10	Down	Enable	--	--
11	Down	Enable	--	--
12	Down	Enable	--	--
13	Down	Enable	--	--
14	Down	Enable	--	--
15	Down	Enable	--	--
16	Down	Enable	--	--
17	Down	Enable	--	--
18	Down	Enable	--	--
19	Down	Enable	--	--
20	Down	Enable	--	--
21	Down	Enable	--	--
22	Down	Enable	--	--
23	Down	Enable	--	--
24	Down	Enable	--	--
25	Up	Enable	100Mbps Full	Disabled
26	Down	Enable	--	--
27	Down	Enable	--	--
28	Down	Enable	--	--
29	Down	Enable	--	--
30	Down	Enable	--	--
31	Down	Enable	--	--
32	Down	Enable	--	--
33	Down	Enable	--	--
34	Down	Enable	--	--
35	Down	Enable	--	--
36	Down	Enable	--	--
37	Down	Enable	--	--
38	Down	Enable	--	--
39	Down	Enable	--	--
40	Down	Enable	--	--
41	Down	Enable	--	--
42	Down	Enable	--	--
43	Down	Enable	--	--
44	Down	Enable	--	--
45	Down	Enable	--	--
46	Down	Enable	--	--
47	Down	Enable	--	--
48	Down	Enable	--	--
49	Down	Enable	--	--
50	Down	Enable	--	--
51	Down	Enable	--	--
52	Down	Enable	--	--

Figure 4-3-1 Port Configuration screenshot

The page includes the following fields:

Object	Description
• **Port**	Indicates the port numbers in the system. Click on the port index will enter port configuration page.
• **Link Status**	Displays the link status of the port.
• **Auto-Nego**	Displays the auto-negotiation mode of the port.
• **Speed & Duplex**	Displays the speed & duplex mode of the port.
• **Flow Control**	Displays the flow control status of the port.



Port Number	Admin Mode	Auto Negotiation	Speed Duplex	Flow Control	LAG Group
01	Enable	Enable	100M Full	Disable	--

Figure 4-3-2 Port Detail Configuration

The page includes the following fields:

Object	Description
• **Port Number**	Indicates the port numbers in the system.
• **Admin Mode**	Configure the administrative mode of the port. Sets to Disable will force the port to link down status.
• **Auto Negotiation**	Configure the port auto-negotiation capability. When auto-negotiation is enabled, the port negotiates with the link partner and works out speed and duplex operation. When auto-negotiation is disabled, port speed and duplex operation is programmable by the user.
• **Speed Duplex**	Indicates the speed and duplex mode if the port is linkup.
• **Flow Control**	Indicates the state of flow control if the port is linkup.
• **LAG Group**	Indicates the LAG group if the port is a LAG port.

4.3.2 LACP Property

Link Aggregation Control Protocol (LACP) is part of an IEEE specification (**802.3ad**) that allows several physical ports to be bundled together to form a single logical channel. Link Aggregation allows one or more links to be aggregated together to form a Link Aggregation Group, such that a MAC Client can treat the Link Aggregation Group as if it were a single link. Link aggregation can be used on 10Mbps, 100Mbps, or 1000Mbps ethernet full duplex ports. Example: A network administrator could combine a group of four 1000Mbps ports into a logical link that will function as a single 4000Mbps port (The actual throughput however will be less than the sum total of the links).

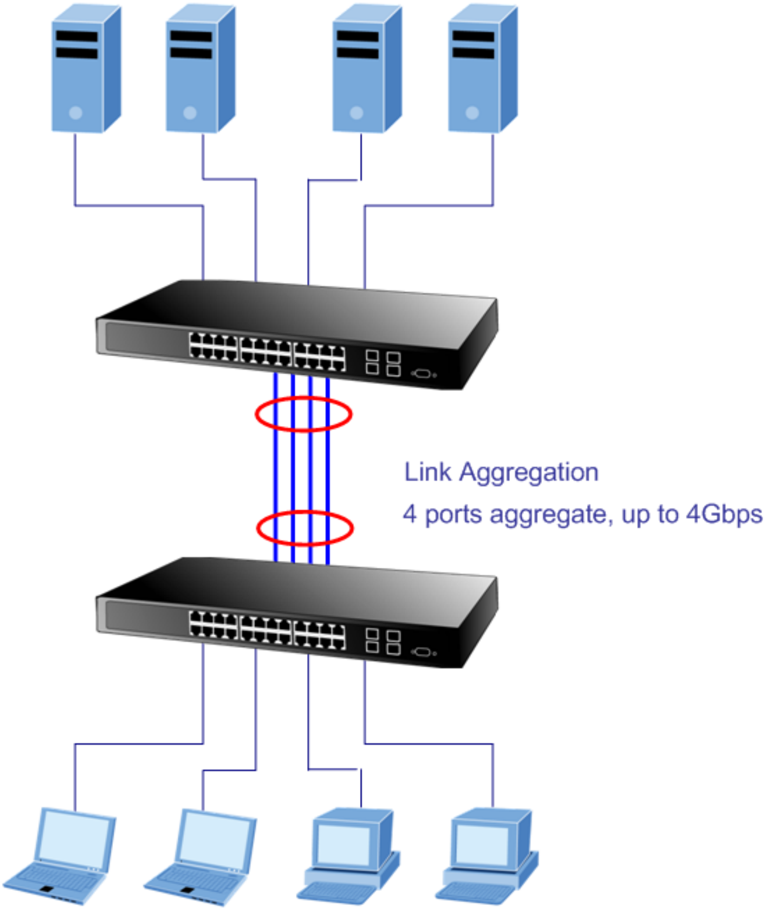


Figure 4-3-3 Link Aggregation

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems that require high speed redundant links. Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. LACP operation requires full-duplex mode, more detail information refer to the IEEE 802.3ad standard.

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 (RJ-45, 100 Mbps 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 8 ports to be aggregated at the same time. The Managed Switch support Gigabit Ethernet ports. If the group is defined as a LACP static link aggregationing group, then any extra ports selected are placed in a standby mode for redundancy if one of the other ports fails. 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 aggregation code ensures that frames belonging to the same frame flow (for example, a TCP connection) are always forwarded on the same link aggregation member port. Reording of frames within a flow is therefore not possible. The aggregation code is based on the following information:

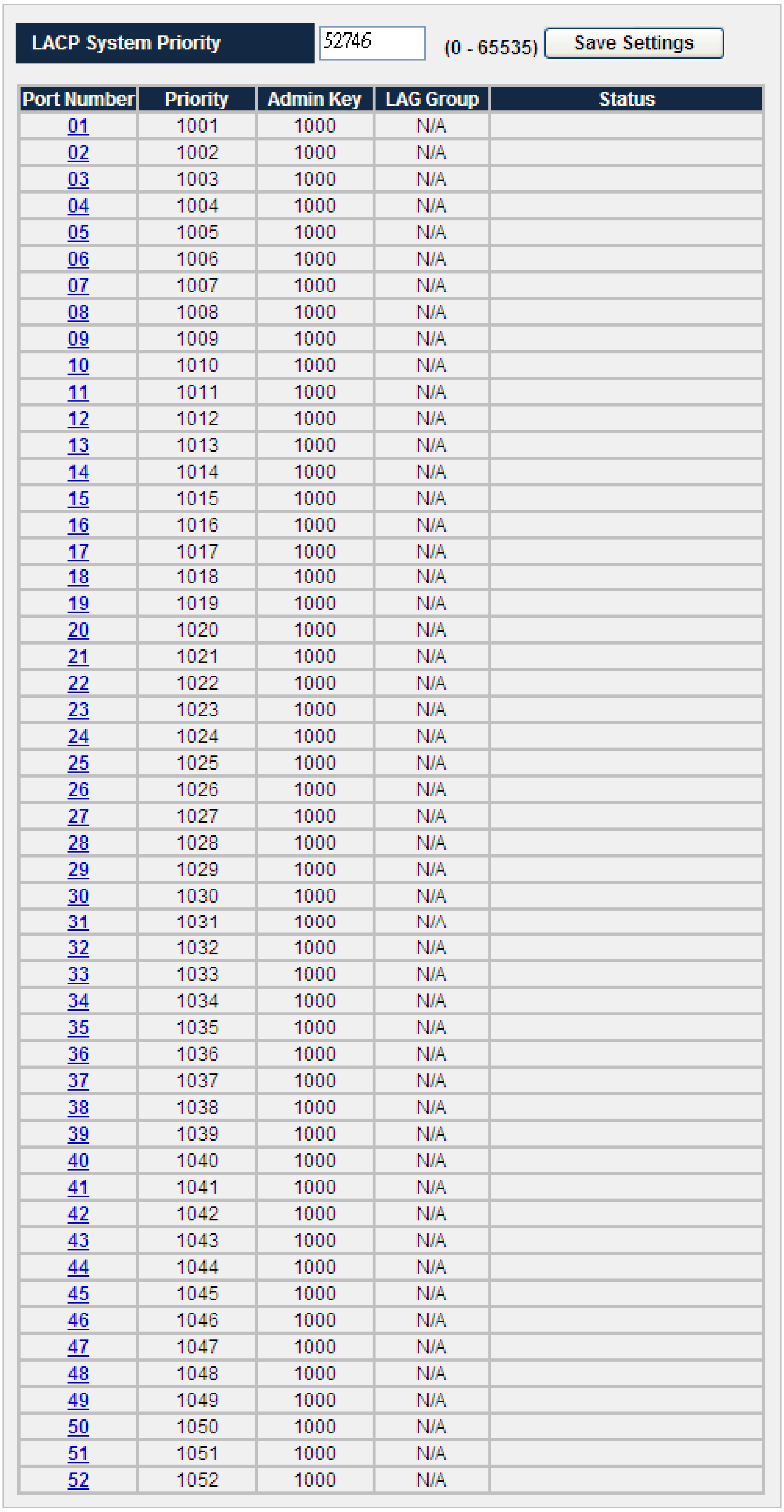
- **Source MAC**
- **Destination MAC**
- **Source and destination IPv4 address.**
- **Source and destination TCP/UDP ports for IPv4 packets**

Normally, all 5 contributions to the aggregation code should be enabled to obtain the best traffic distribution among the link aggregation member ports. Each link aggregation may consist of up to 8 member ports. Any quantity of link aggregation s may be configured for the device (only limited by the quantity of ports on the device.) To configure a proper traffic distribution, the ports within a link aggregation must use the same link speed.

■ Link Aggregation Port Configuration

Link Aggregation Control Protocol (LACP) - LACP LAG negotiate Aggregated Port links with other LACP ports located on a different device. LACP allows switches connected to each other to discover automatically whether any ports are member of the same LAG.

This page allows the user to inspect the current LACP port configurations, and possibly change them as well. The LACP port settings relate to the currently selected stack unit, as reflected by the page header. The LACP Port Configuration screen in Figure 4-3-4 appears.



LACP System Priority 52746 (0 - 65535)

Port Number	Priority	Admin Key	LAG Group	Status
01	1001	1000	N/A	
02	1002	1000	N/A	
03	1003	1000	N/A	
04	1004	1000	N/A	
05	1005	1000	N/A	
06	1006	1000	N/A	
07	1007	1000	N/A	
08	1008	1000	N/A	
09	1009	1000	N/A	
10	1010	1000	N/A	
11	1011	1000	N/A	
12	1012	1000	N/A	
13	1013	1000	N/A	
14	1014	1000	N/A	
15	1015	1000	N/A	
16	1016	1000	N/A	
17	1017	1000	N/A	
18	1018	1000	N/A	
19	1019	1000	N/A	
20	1020	1000	N/A	
21	1021	1000	N/A	
22	1022	1000	N/A	
23	1023	1000	N/A	
24	1024	1000	N/A	
25	1025	1000	N/A	
26	1026	1000	N/A	
27	1027	1000	N/A	
28	1028	1000	N/A	
29	1029	1000	N/A	
30	1030	1000	N/A	
31	1031	1000	N/A	
32	1032	1000	N/A	
33	1033	1000	N/A	
34	1034	1000	N/A	
35	1035	1000	N/A	
36	1036	1000	N/A	
37	1037	1000	N/A	
38	1038	1000	N/A	
39	1039	1000	N/A	
40	1040	1000	N/A	
41	1041	1000	N/A	
42	1042	1000	N/A	
43	1043	1000	N/A	
44	1044	1000	N/A	
45	1045	1000	N/A	
46	1046	1000	N/A	
47	1047	1000	N/A	
48	1048	1000	N/A	
49	1049	1000	N/A	
50	1050	1000	N/A	
51	1051	1000	N/A	
52	1052	1000	N/A	

Figure 4-3-4 LACP Property

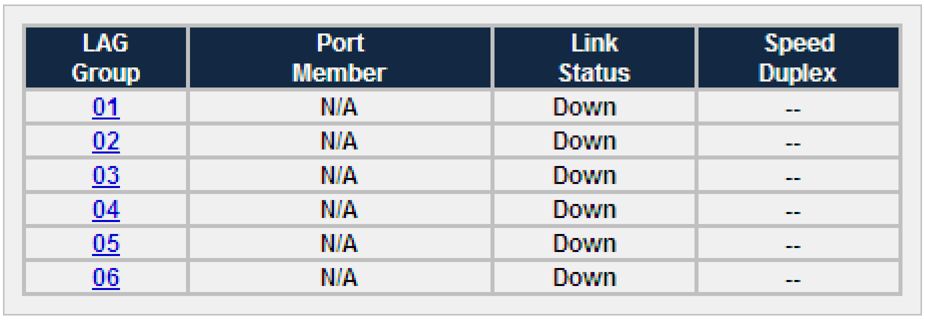
The page includes the following fields:

Object	Description
• **LACP System Priority**	Specifies the actor device's link aggregation priority relative to the devices at the other ends of the links on which link aggregation is enabled. A higher value indicates a lower priority.
• **Port Number**	Display the port number. Click on the index number will enter port LACP properties configuration screen.
• **Priority**	Indicates actor port priority. The port priority determines the active and standby links. When a group of ports is negotiating with a group of ports on another device to establish a trunk group, the port with the highest priority becomes the default active port. The other ports (with lower priorities) become standby ports in the trunk group.
• **Admin Key**	Indicates actor administration key for the port. The LACP administration key must be set to the same value for ports that belong to the same LAG.
• **LAG Group**	Indicates the LAG group ID if the port is the member of this LAG group.
• **Status**	Summarizes the current LACP status for this port.

All information listed here is for reference only. Please refer to IEEE 802.3ad for details.

4.3.3 LAG Group

Link Aggregated Groups optimize port usage by linking a group of ports together to form a single aggregated group. Link aggregated groups multiply the bandwidth between the devices, increase port flexibility, and provide link redundancy.



LAG Group	Port Member	Link Status	Speed Duplex
01	N/A	Down	--
02	N/A	Down	--
03	N/A	Down	--
04	N/A	Down	--
05	N/A	Down	--
06	N/A	Down	--

Figure 4-3-5 LAG Group Screenshot

The page includes the following fields:

Object	Description
• **LAG Group**	Displays the LAG groups.
• **Port Member**	Displays the ports that are members of this LAG.
• **Link Status**	Displays the link status.
• **Speed Duplex**	Display the connection speed and duplex.

4.4 VLAN

4.4.1 VLAN Overview

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLAN also logically segment the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

VLAN can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated.

Note

1. No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLAN without a network device performing a routing function between the VLAN.
2. The Managed Switch supports **IEEE 802.1Q VLAN**. The port untagging function can be used to remove the 802.1 tag from packet headers to maintain compatibility with devices that are tag-unaware.
3. The Managed Switch's default is to assign all ports to a single 802.1Q VLAN named DEFAULT_VLAN. As new VLAN is created, the member ports assigned to the new VLAN will be removed from the DEFAULT_ VLAN port member list. The DEFAULT_VLAN has a VID = 1.

This section has the following items:

- **IEEE 802.1Q VLAN** Enable IEEE 802.1Q Tag based VLAN group

4.4.2 IEEE 802.1Q VLAN

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. This Managed Switch provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This Managed Switch supports the following VLAN features:

- Up to **255 VLANs** based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and **GVRP** protocol
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

> Note
>
> The Managed Switch allows 4k user-manageable VLANs.

IEEE 802.1Q Standard

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

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

VLAN can also provide a level of security to your network. IEEE 802.1Q VLAN will only deliver packets between stations that are members of the VLAN. Any port can be configured as either tagging or untagging. The untagging feature of IEEE 802.1Q VLAN allows VLAN to work with legacy switches that don't recognize VLAN tags in packet headers. The tagging feature allows VLAN to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

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

Some relevant terms:

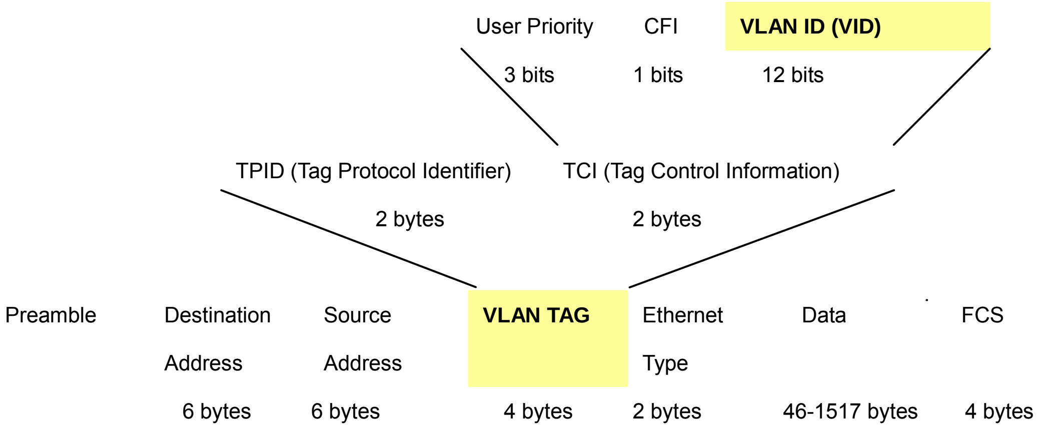
- **Tagging** - The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** - The act of stripping 802.1Q VLAN information out of the packet header.

802.1Q VLAN Tags

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

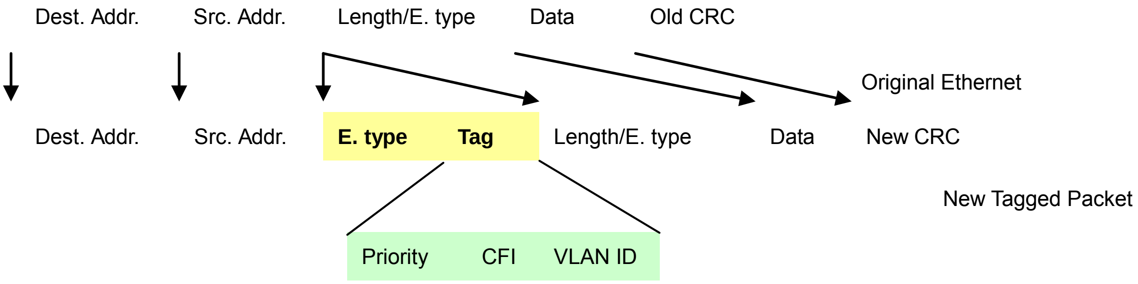
The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

802.1Q Tag



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

Adding an IEEE802.1Q Tag



Port VLAN ID

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

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

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

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

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

Default VLANs

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

Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

Note

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

■ VLAN Classification

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

■ Port Overlapping

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

■ Untagged VLANs

Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets. However, you should use IEEE 802.3 tagged VLANs with GVRP whenever possible to fully automate VLAN registration.

3. Automatic VLAN Registration

GVRP (GARP VLAN Registration Protocol) defines a system whereby the switch can automatically learn the VLANs to which each end station should be assigned. If an end station (or its network adapter) supports the IEEE 802.1Q VLAN protocol, it can be configured to broadcast a message to your network indicating the VLAN groups it wants to join. When this switch receives these messages, it will automatically place the receiving port in the specified VLANs, and then forward the message to all other ports. When the message arrives at another switch that supports GVRP, it will also place the receiving port in the specified VLANs, and pass the message on to all other ports. VLAN requirements are propagated in this way throughout the network. This allows GVRP-compliant devices to be automatically configured for VLAN groups based solely on endstation requests.

To implement GVRP in a network, first add the host devices to the required VLANs (using the operating system or other application software), so that these VLANs can be propagated onto the network. For both the edge switches attached directly to these hosts, and core switches in the network, enable GVRP on the links between these devices. You should also determine security boundaries in the network and disable GVRP on the boundary ports to prevent advertisements from being propagated, or forbid those ports from joining restricted VLANs.

Note

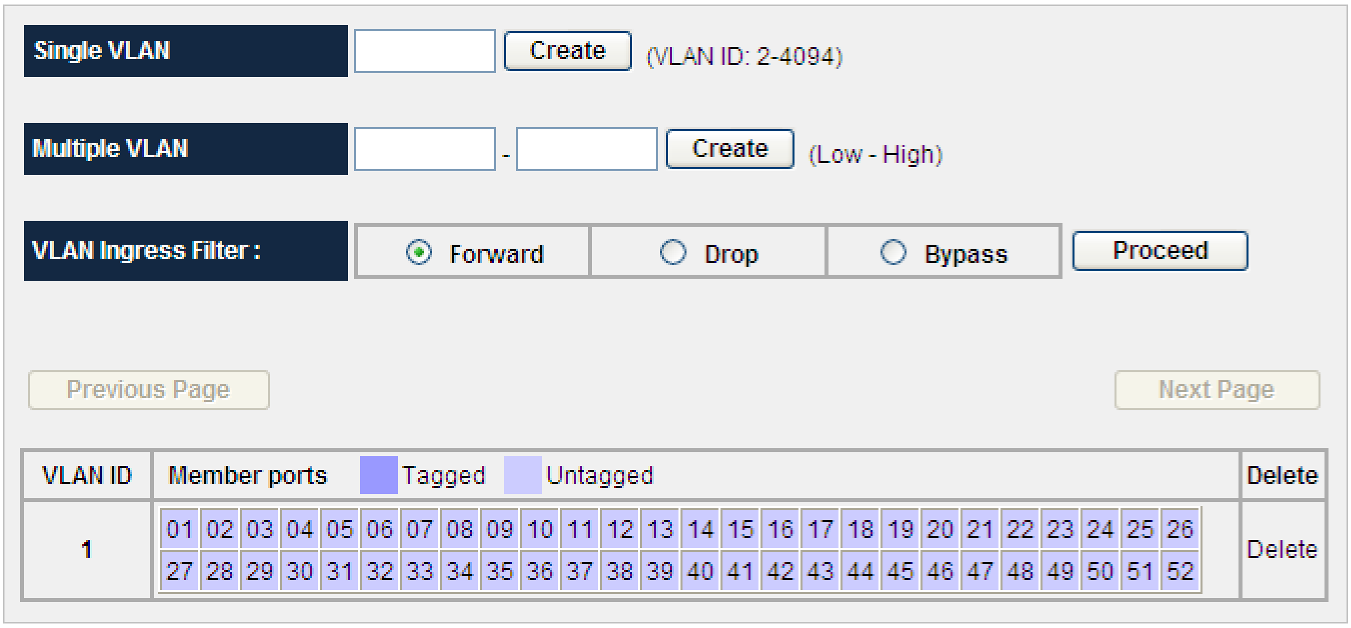
If you have host devices that do not support GVRP, you should configure static or untagged VLANs for the switch ports connected to these devices (as described in "Adding Static Members to VLANs (VLAN Index)"). But you can still enable GVRP on these edge switches, as well as on the core switches in the network.

This section is to control the VLAN of the switch, the VLAN function contains links to the following topics:

- **Create VLAN**
- **VLAN Settings**
- **VLAN Port**
- **GVRP**

4.4.3 Create VLAN

The Create VLAN screen provides information and global parameters for configuring and working with VLANs.



Single VLAN [ ] Create (VLAN ID: 2-4094)

Multiple VLAN [ ] - [ ] Create (Low - High)

VLAN Ingress Filter : ● Forward ○ Drop ○ Bypass Proceed

Previous Page Next Page

VLAN ID	Member ports ■ Tagged □ Untagged	Delete
1	01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52	Delete

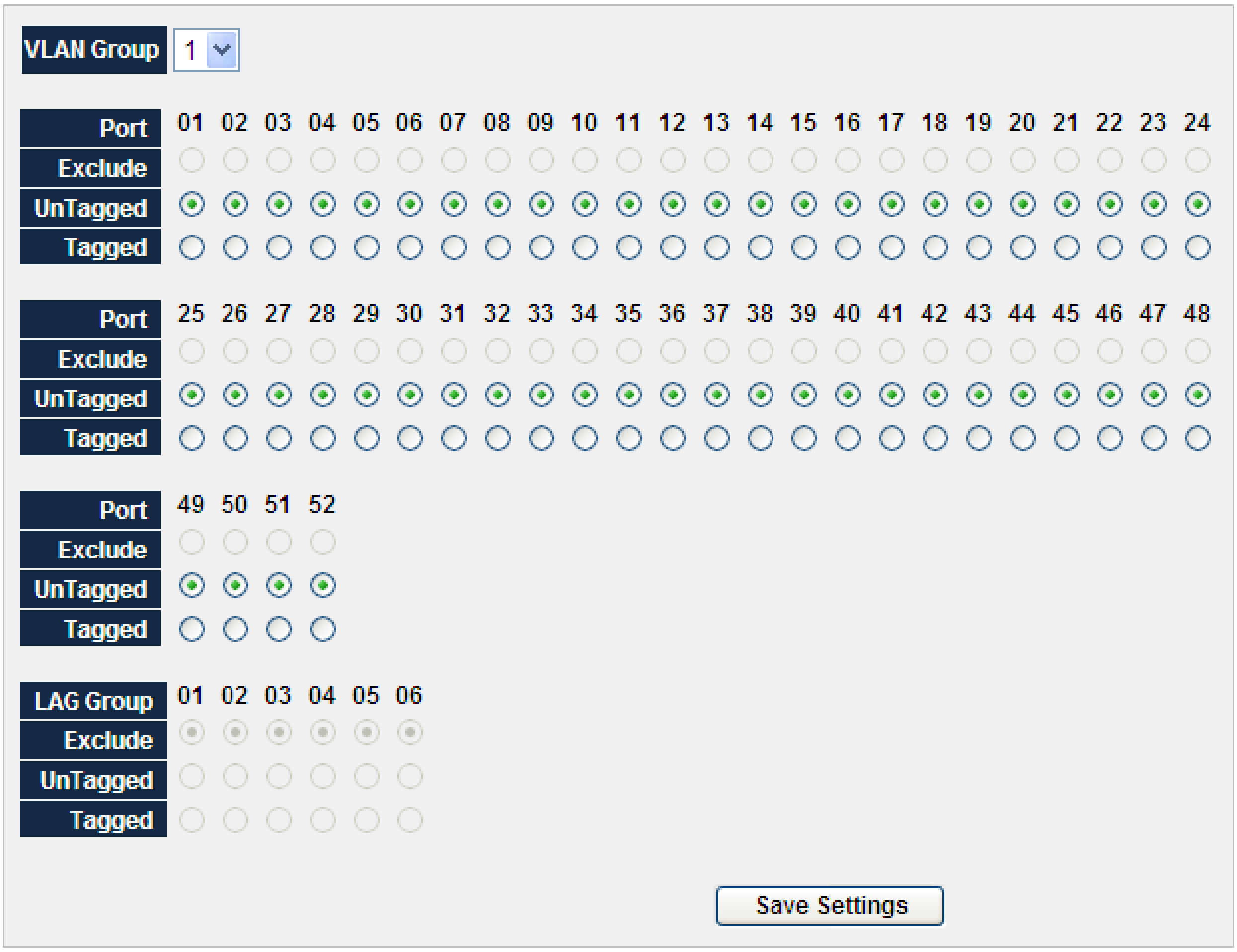
Figure 4-4-1 Create VLAN screenshot

The page includes the following fields:

Object	Description
• **Single VLAN**	Indicates the ID number of the VLAN being configured. Up to 256 VLANs can be created. This field is used to create one VLAN group at a time.
• **Multiple VLAN**	Specifies a range of VLANs being configured. It allows multiple VLAN groups being created at a time.
• **VLAN Ingress Filter**	Enable ingress filtering for a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded. By default, ingress filtering is forward.
• **VLAN Group Table**	Displays all VLAN groups with their member ports . There are two color symbols for each VLAN group member port, that is **Tagged** and **Untagged.** **Tagged -** Indicates that this port is a member of the VLAN. When the packet leaves the member port, the VLAN tag is kept. **Untagged** - Indicates that this port is a member of the VLAN. When the packet leaves the member port, the VLAN tag is removed.

4.4.4 VLAN Setting

The VLAN Setting screen contains fields for configuring ports to a VLAN. The port default VLAN ID (PVID) is configured on the Create VLAN screen. All untagged packets arriving to the device are tagged by the ports PVID. The VLAN Settings screen contains a Port Table for VLAN parameters for each port. Ports are assigned VLAN membership by selecting and configuring the presented configuration options, you can refer to Figure 4-4-2.



VLAN Group: 1

Port	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Exclude	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
UnTagged	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Tagged	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Port	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
Exclude	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
UnTagged	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Tagged	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Port	49	50	51	52
Exclude	○	○	○	○
UnTagged	●	●	●	●
Tagged	○	○	○	○

LAG Group	01	02	03	04	05	06
Exclude	●	●	●	●	●	●
UnTagged	○	○	○	○	○	○
Tagged	○	○	○	○	○	○

Figure 4-4-2 VLAN Setting Screenshot

Understand nomenclature of the Switch

■ IEEE 802.1Q Tagged and Untagged

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

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

device.

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

The page includes the following fields:

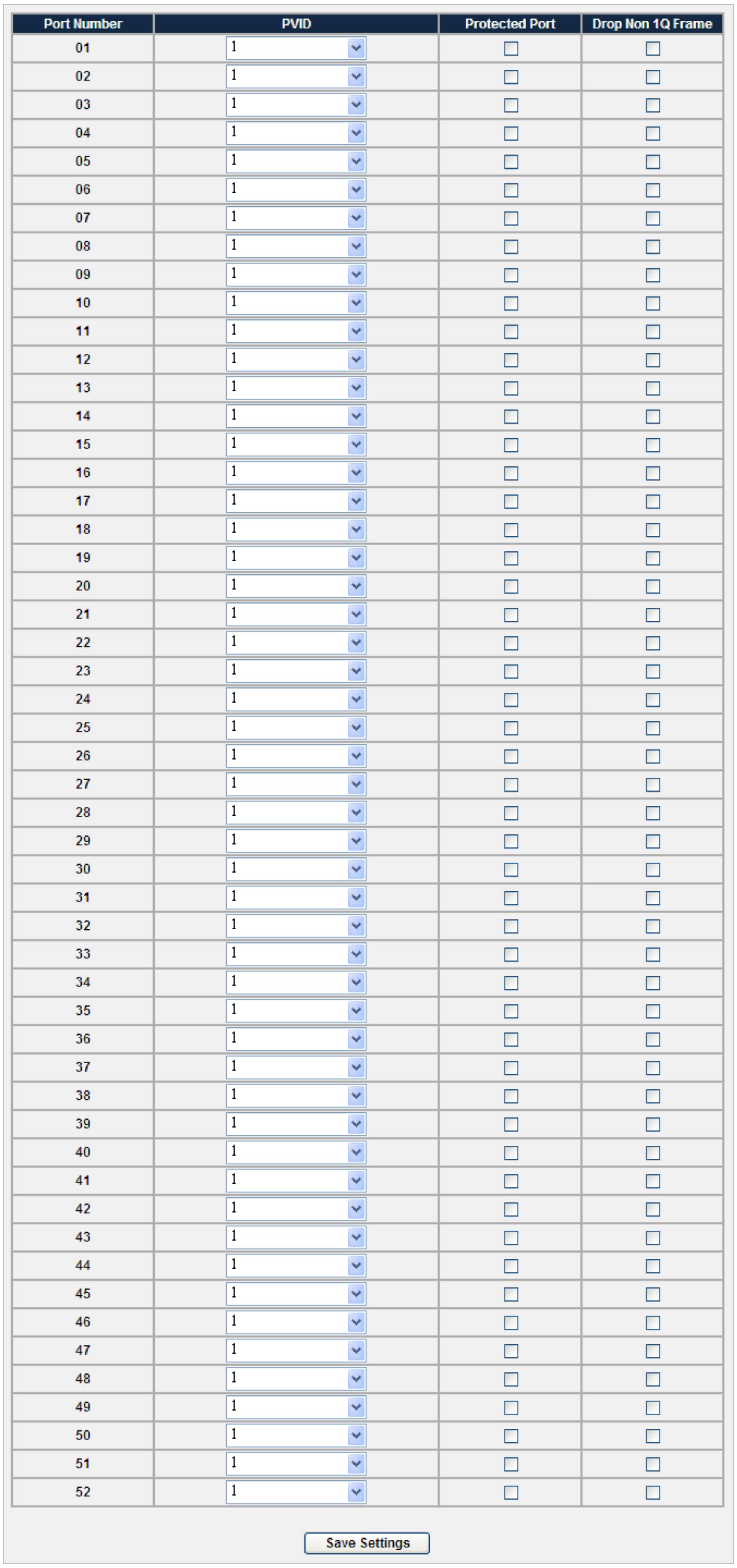
Object	Description
• **VLAN Group**	Indicates the VLAN for which the port membership is configured.
• **Excluded**	Excludes the Port/LAG from the VLAN.
• **Untagged**	Indicates that this Port/LAG is a member of the VLAN. When the packet leaves the member Port/LAG, the VLAN tag is removed.
• **Tagged**	Indicates that this Port/LAG is a member of the VLAN. When the packet leaves the member Port/LAG, the VLAN tag is kept.

Note

The port must be a member of the same VLAN as the Port VLAN ID**.**

4.4.5 VLAN Port

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



Port Number	PVID	Protected Port	Drop Non 1Q Frame
01	1	□	□
02	1	□	□
03	1	□	□
04	1	□	□
05	1	□	□
06	1	□	□
07	1	□	□
08	1	□	□
09	1	□	□
10	1	□	□
11	1	□	□
12	1	□	□
13	1	□	□
14	1	□	□
15	1	□	□
16	1	□	□
17	1	□	□
18	1	□	□
19	1	□	□
20	1	□	□
21	1	□	□
22	1	□	□
23	1	□	□
24	1	□	□
25	1	□	□
26	1	□	□
27	1	□	□
28	1	□	□
29	1	□	□
30	1	□	□
31	1	□	□
32	1	□	□
33	1	□	□
34	1	□	□
35	1	□	□
36	1	□	□
37	1	□	□
38	1	□	□
39	1	□	□
40	1	□	□
41	1	□	□
42	1	□	□
43	1	□	□
44	1	□	□
45	1	□	□
46	1	□	□
47	1	□	□
48	1	□	□
49	1	□	□
50	1	□	□
51	1	□	□
52	1	□	□

Figure 4-4-3 VLAN Port Screenshot

The page includes the following fields:

Object	Description
• **PVID**	The port default VLAN ID (PVID) is configured on the VLAN Port screen. All untagged packets arrive to the device are tagged by the ports PVID.
• **Protected Port**	When the ports specified as 'Protected Port', they can not forward traffic to each other. Only the ports that are not specified as 'Protected Port' can forward traffic to and from the protected ports respectively.
• **Drop Non 1Q Frame**	When enabled, any Non-1Q ingress frame will be dropped by this port.

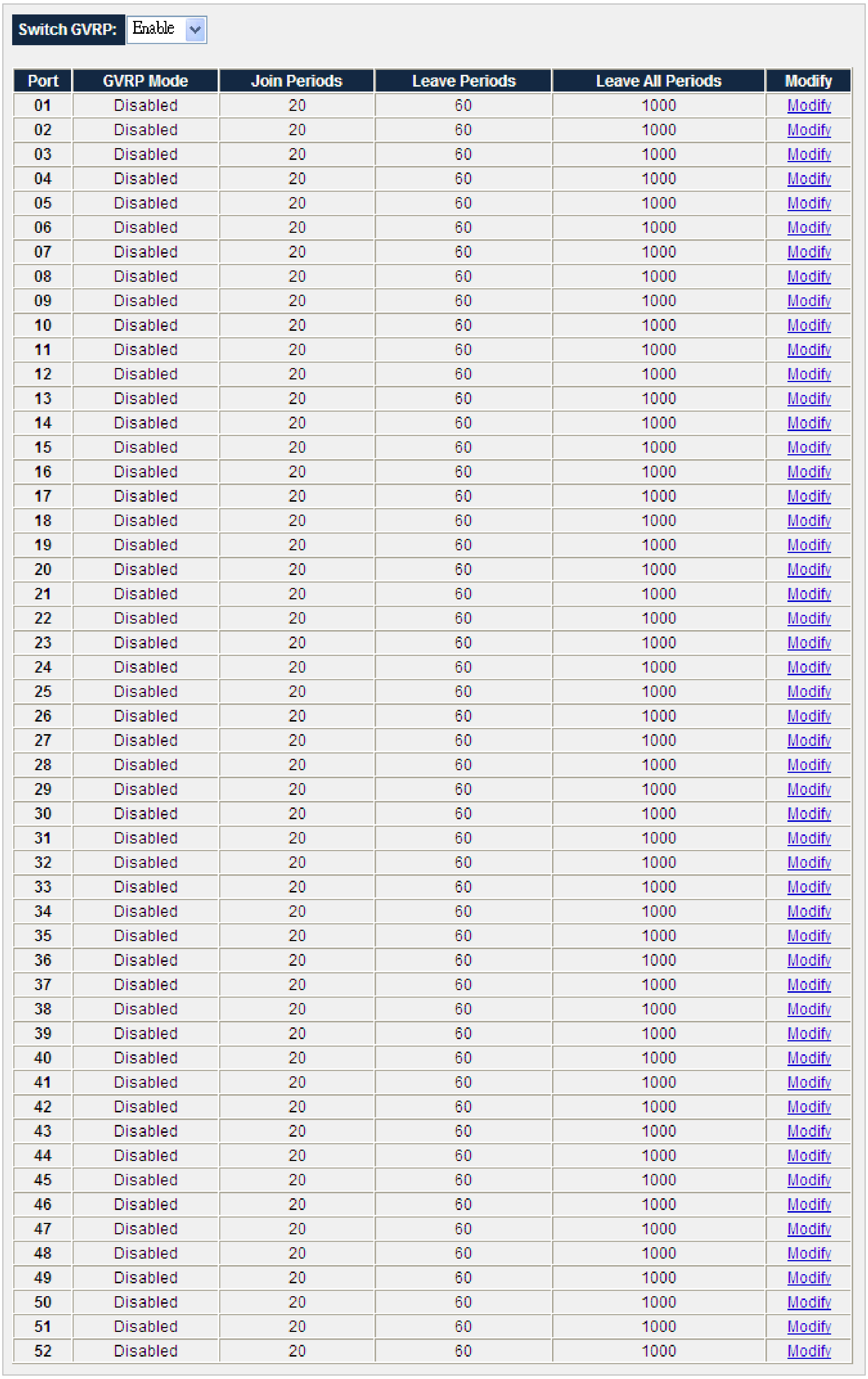
4.4.6 GVRP

When Switch GVRP is enabled, you can modify the GVRP settings of multiple ports.

But if it's disabled, GVRP will be disabled on all ports.

Click the Modify hyperlink to modify the GVRP settings of multiple ports when Switch GVRP is enabled.

On the port GVRP modification page, you can enable/disable GVRP on the port you specified.



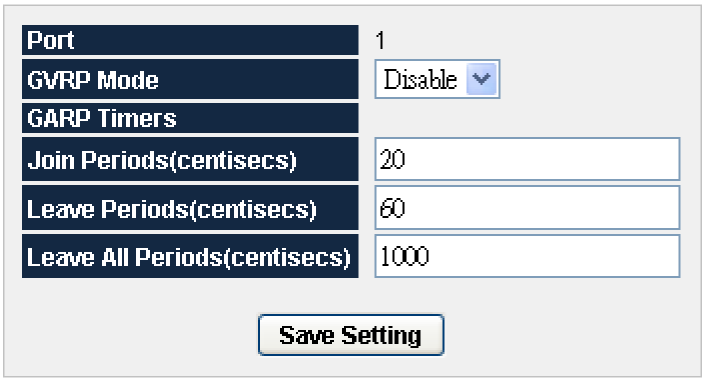
Switch GVRP: Enable

Port	GVRP Mode	Join Periods	Leave Periods	Leave All Periods	Modify
01	Disabled	20	60	1000	Modify
02	Disabled	20	60	1000	Modify
03	Disabled	20	60	1000	Modify
04	Disabled	20	60	1000	Modify
05	Disabled	20	60	1000	Modify
06	Disabled	20	60	1000	Modify
07	Disabled	20	60	1000	Modify
08	Disabled	20	60	1000	Modify
09	Disabled	20	60	1000	Modify
10	Disabled	20	60	1000	Modify
11	Disabled	20	60	1000	Modify
12	Disabled	20	60	1000	Modify
13	Disabled	20	60	1000	Modify
14	Disabled	20	60	1000	Modify
15	Disabled	20	60	1000	Modify
16	Disabled	20	60	1000	Modify
17	Disabled	20	60	1000	Modify
18	Disabled	20	60	1000	Modify
19	Disabled	20	60	1000	Modify
20	Disabled	20	60	1000	Modify
21	Disabled	20	60	1000	Modify
22	Disabled	20	60	1000	Modify
23	Disabled	20	60	1000	Modify
24	Disabled	20	60	1000	Modify
25	Disabled	20	60	1000	Modify
26	Disabled	20	60	1000	Modify
27	Disabled	20	60	1000	Modify
28	Disabled	20	60	1000	Modify
29	Disabled	20	60	1000	Modify
30	Disabled	20	60	1000	Modify
31	Disabled	20	60	1000	Modify
32	Disabled	20	60	1000	Modify
33	Disabled	20	60	1000	Modify
34	Disabled	20	60	1000	Modify
35	Disabled	20	60	1000	Modify
36	Disabled	20	60	1000	Modify
37	Disabled	20	60	1000	Modify
38	Disabled	20	60	1000	Modify
39	Disabled	20	60	1000	Modify
40	Disabled	20	60	1000	Modify
41	Disabled	20	60	1000	Modify
42	Disabled	20	60	1000	Modify
43	Disabled	20	60	1000	Modify
44	Disabled	20	60	1000	Modify
45	Disabled	20	60	1000	Modify
46	Disabled	20	60	1000	Modify
47	Disabled	20	60	1000	Modify
48	Disabled	20	60	1000	Modify
49	Disabled	20	60	1000	Modify
50	Disabled	20	60	1000	Modify
51	Disabled	20	60	1000	Modify
52	Disabled	20	60	1000	Modify

Figure 4-4-4 GVRP Screenshot

The page contains the following fields:

Object	Description
• **Enable GVRP**	Enables and disables GVRP on the device
• **Port**	Displays the interface on which GVRP is enabled. Possible field values are: **Port** - indicates the port number on which GVRP is enabled. **LAG** - indicates the LAG number on which GVRP is enabled.
• **GVRP Mode**	When the checkbox is checked, GVRP is enabled on the interface
• **Join Period**	The interval between transmitting requests/queries to participate in a VLAN group. Range: 20-1000 centiseconds. Default: **20** centiseconds
• **Leave Period**	The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group. Range: 60-3000 centiseconds Default: **60** centiseconds
• **Leave All Period**	The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group. Range: 500-18000 centiseconds; Default: **1000** centiseconds
• **Modify**	Modify detail GVRP on the device. Click on the Modify index will enter GVRP configuration page.



Port	1
GVRP Mode	Disable
GARP Timers	
Join Periods(centisecs)	20
Leave Periods(centisecs)	60
Leave All Periods(centisecs)	1000

Figure 4-4-5 GVRP Screenshot

The page contains the following fields:

Object	Description
• **Port**	This is the logical port number for this row.
• **GVRP Mode**	When the checkbox is checked, GVRP is enabled on the interface
• **Join Periods (centisecs)**	The interval between transmitting requests/queries to participate in a VLAN group. Range: 20-1000 centiseconds. Default: **20** centiseconds
• **Leave Periods (centisecs)**	The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group. Range: 60-3000 centiseconds Default: **60** centiseconds
• **Leave All Period (centisecs)**	The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group. Range: 500-18000 centiseconds; Default: **1000** centiseconds

4.5 Spanning Tree

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)**

Theory of Spanning Tree Protocol

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 por tidentifier

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

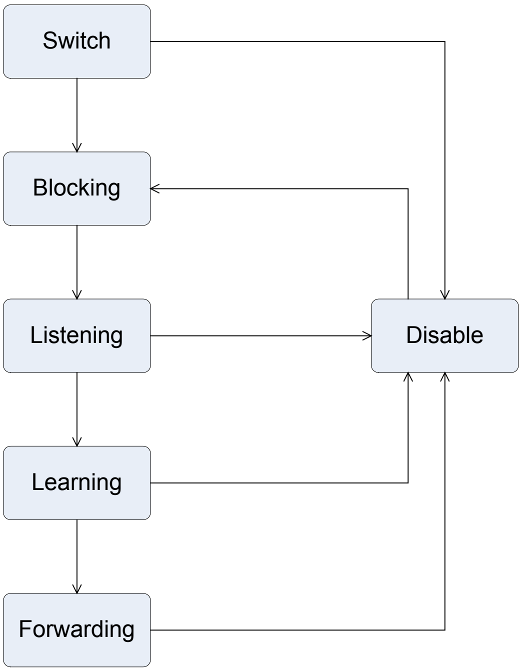


Figure 4-5-1 STP Port State Transitions Screenshot

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

STP Parameters

STP Operation Levels

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

Note

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

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

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

Parameter	Description	Default Value
Bridge Identifier(Not user configurable except by setting priority below)	A combination of the User-set priority and the switch's MAC address. The Bridge Identifier consists of two parts: a 16-bit priority and a 48-bit Ethernet MAC address 32768 + MAC	32768 + MAC

Priority	A relative priority for each switch – lower numbers give a higher priority and a greater chance of a given switch being elected as the root bridge	32768
Hello Time	The length of time between broadcasts of the hello message by the switch	2 seconds
Maximum Age Timer	Measures the age of a received BPDU for a port and ensures that the BPDU is discarded when its age exceeds the value of the maximum age timer.	20 seconds
Forward Delay Timer	The amount time spent by a port in the learning and listening states waiting for a BPDU that may return the port to the blocking state.	15 seconds

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

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

Default Spanning-Tree Configuration

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

User-Changeable STA Parameters

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

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

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

Note

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

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

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

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

Note

Observe the following formulas when setting the above parameters:

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

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

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

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

Illustration of STP

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

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

Now, if switch A broadcasts a packet to switch C, then switch C will drop the packet at port 2 and the broadcast will end there.

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

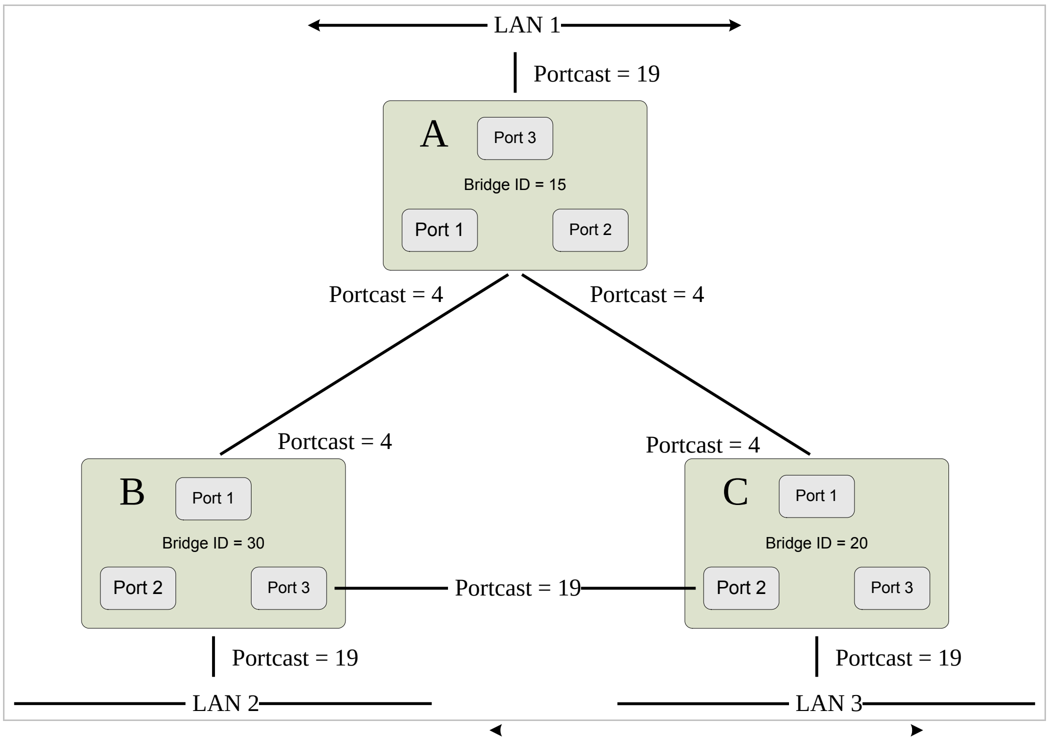


Figure 4-5-2 Before Applying the STA Rules

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

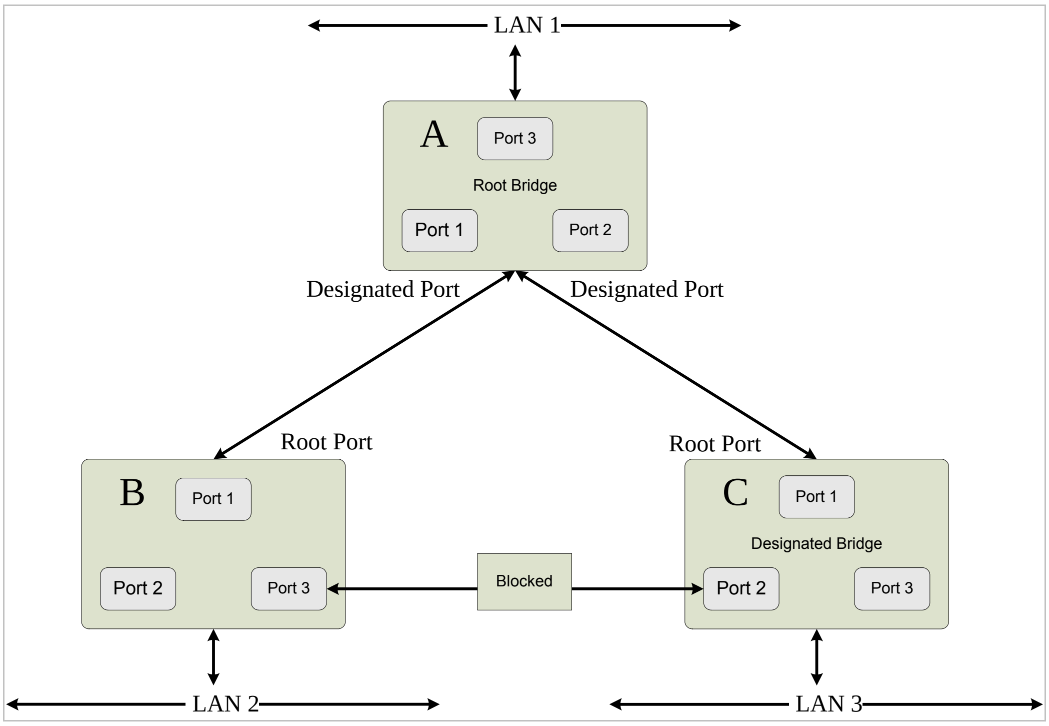


Figure 4-5-3 After Applying the STA Rules

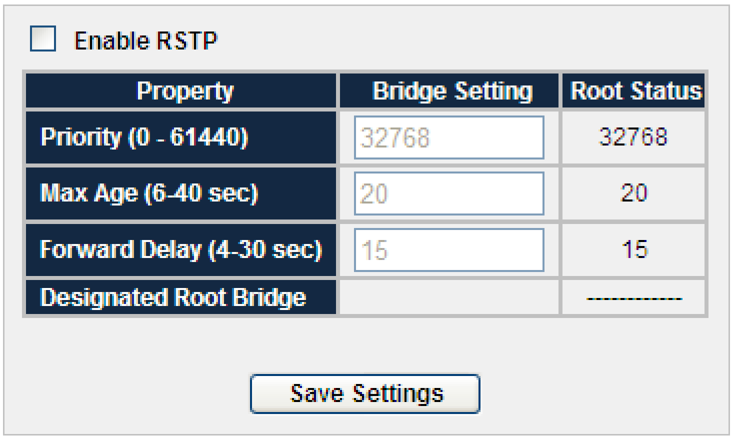
The switch with the lowest Bridge ID (switch C) was elected the root bridge, and the ports were selected to give a high port cost between switches B and C. The two (optional) Gigabit ports (default port cost = 4) on switch A are connected to one (optional) Gigabit port on both switch B and C. The redundant link between switch B and C is deliberately chosen as a 100 Mbps Fast Ethernet link (default port cost = 19). Gigabit ports could be used, but the port cost should be increased from the default to ensure that the link between switch B and switch C is the blocked link.

This section is to control the spanning tree of the switch, the spanning tree function contains links to the following topics:

- **RSTP**
- **RSTP Port**
- **MSTP**
- **MSTP Port**
- **MSTP Instance**
- **MSTP Interface**

4.5.1 RSTP (Rapid Spanning Tree Protocol)

The Rapid Spanning Tree Protocol (RSTP) provides rapid convergence of the spanning tree by assigning port roles and by determining the active topology. The RSTP builds upon the IEEE 802.1D STP protocol to select the switch with the highest switch priority as the root switch.



☐ Enable RSTP

Property	Bridge Setting	Root Status
Priority (0 - 61440)	32768	32768
Max Age (6-40 sec)	20	20
Forward Delay (4-30 sec)	15	15
Designated Root Bridge		------------

Figure 4-5-4 RSTP Screenshot

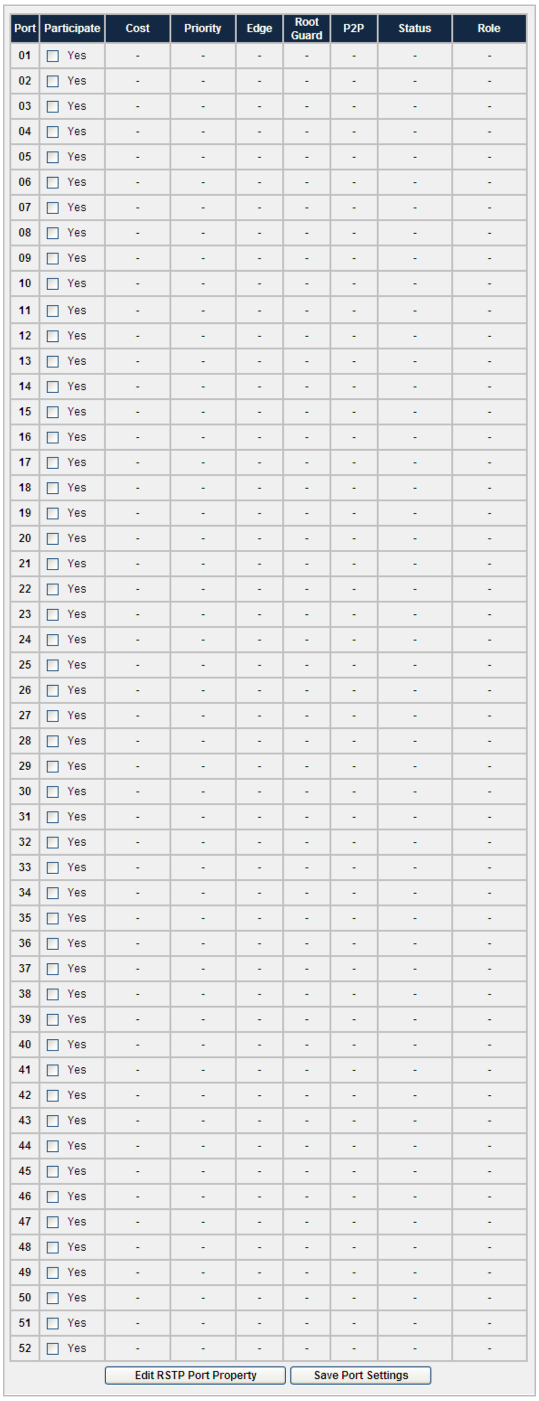
The page includes the following fields:

Object	Description
• **Enable RSTP**	Enables **RSTP** of the switch will allow you to control the RSTP parameters from the bridge point of view.
• **Priority**	Specifies the bridge priority value. When switches or bridges are running STP, each is assigned a priority. The default value is **32768**. The port priority value is provided in increments of **4096**. For example, 4096, 8192, 12288, etc. The range is 0 to 61440.
• **Max Age**	The max age timer controls the maximum length of time that passes before a bridge port saves its configuration BPDU information.
• **Forward Delay**	Forward delay is a time value, which controls how fast a port changes its state. The value determines how long the port stays in each of the listening and learning states which precede the forward state. This value is also used to age all

	dynamic entries in the forwarding databases when a topology change has been detected and is underway.
- **Designated Root Bridge**	The bridge identifier of the root of the spanning tree is determined by the RSTP protocol as executed by this node. The bridge identifier value is used as the root identifier parameter in all configuration bridge BPDUs originated by this node.

4.5.2 RSTP Port

RSTP port settings control and monitor per port spanning tree status.



Port	Participate	Cost	Priority	Edge	Root Guard	P2P	Status	Role
01	□ Yes	-	-	-	-	-	-	-
02	□ Yes	-	-	-	-	-	-	-
03	□ Yes	-	-	-	-	-	-	-
04	□ Yes	-	-	-	-	-	-	-
05	□ Yes	-	-	-	-	-	-	-
06	□ Yes	-	-	-	-	-	-	-
07	□ Yes	-	-	-	-	-	-	-
08	□ Yes	-	-	-	-	-	-	-
09	□ Yes	-	-	-	-	-	-	-
10	□ Yes	-	-	-	-	-	-	-
11	□ Yes	-	-	-	-	-	-	-
12	□ Yes	-	-	-	-	-	-	-
13	□ Yes	-	-	-	-	-	-	-
14	□ Yes	-	-	-	-	-	-	-
15	□ Yes	-	-	-	-	-	-	-
16	□ Yes	-	-	-	-	-	-	-
17	□ Yes	-	-	-	-	-	-	-
18	□ Yes	-	-	-	-	-	-	-
19	□ Yes	-	-	-	-	-	-	-
20	□ Yes	-	-	-	-	-	-	-
21	□ Yes	-	-	-	-	-	-	-
22	□ Yes	-	-	-	-	-	-	-
23	□ Yes	-	-	-	-	-	-	-
24	□ Yes	-	-	-	-	-	-	-
25	□ Yes	-	-	-	-	-	-	-
26	□ Yes	-	-	-	-	-	-	-
27	□ Yes	-	-	-	-	-	-	-
28	□ Yes	-	-	-	-	-	-	-
29	□ Yes	-	-	-	-	-	-	-
30	□ Yes	-	-	-	-	-	-	-
31	□ Yes	-	-	-	-	-	-	-
32	□ Yes	-	-	-	-	-	-	-
33	□ Yes	-	-	-	-	-	-	-
34	□ Yes	-	-	-	-	-	-	-
35	□ Yes	-	-	-	-	-	-	-
36	□ Yes	-	-	-	-	-	-	-
37	□ Yes	-	-	-	-	-	-	-
38	□ Yes	-	-	-	-	-	-	-
39	□ Yes	-	-	-	-	-	-	-
40	□ Yes	-	-	-	-	-	-	-
41	□ Yes	-	-	-	-	-	-	-
42	□ Yes	-	-	-	-	-	-	-
43	□ Yes	-	-	-	-	-	-	-
44	□ Yes	-	-	-	-	-	-	-
45	□ Yes	-	-	-	-	-	-	-
46	□ Yes	-	-	-	-	-	-	-
47	□ Yes	-	-	-	-	-	-	-
48	□ Yes	-	-	-	-	-	-	-
49	□ Yes	-	-	-	-	-	-	-
50	□ Yes	-	-	-	-	-	-	-
51	□ Yes	-	-	-	-	-	-	-
52	□ Yes	-	-	-	-	-	-	-

Figure 4-5-5 RSTP Port Screenshot

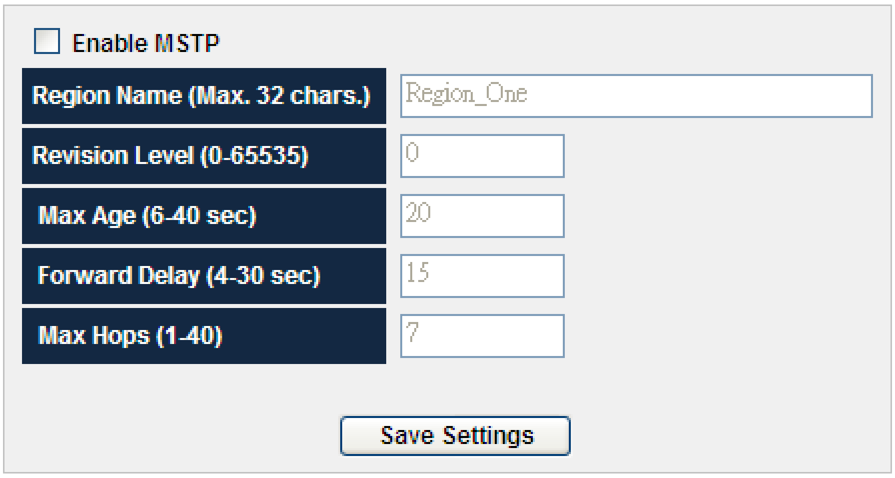
The page includes the following fields:

Object	Description
• **Port**	Indicates the port numbers of the system.
• **Participate**	Indicates if the port is runung RSTP protocol or not.
• **Cost**	Indicates the cost of this port, which means the contribution of this port to the path cost of paths towards the spanning tree root which include this port.
• **Priority**	Indicates the priority of this port. This is the value of the priority field contained in the first octect of the Port ID.
• **Edge**	Indicates if this port is the edge port. Once configured as an edge port, the port state immediately transitions from disable/block to forwarding state.
• **Root Guard**	Indicates if this port is the root guard port. Once configured as a root guard port, the port can prevent outside swit Displays the RSTP port status.ch with suprior BID from affecting former topology.
• **P2P**	Indicates if this port is a point-to-point link. If you connect a port to another port though a point-to-point link and the local port becomes a designated port, it negotiates a rapid transition with the other port to ensure a loop-free topology.
• **Status**	Displays the RSTP port status.
• **Role**	Displays the role of this RSTP port.
• **Edit RSTP Port Property**	Click on this button to allow you to configure RSTP port properties.

4.5.3 MSTP

The **Multiple Spanning Tree Protocol (MSTP)** algorithm and protocol provides simple and full connectivity for frames assigned to any given VLAN throughout a Bridged Local Area Network comprising arbitrarily interconnected Bridges, each operating MSTP, STP (Clause 8 of IEEE Std 802.1D, 1998 Edition), or RSTP (Clause 17 of IEEE Std 802.1D,1998 Edition).

MSTP allows frames assigned to different VLANs to follow separate paths, each based on an independent **Multiple Spanning Tree Instance (MSTI)**, within **Multiple Spanning Tree (MST)** Regions composed of LANs and or MST Bridges. These Regions and the other Bridges and LANs are connected into a single **Common Spanning Tree (CST)**.



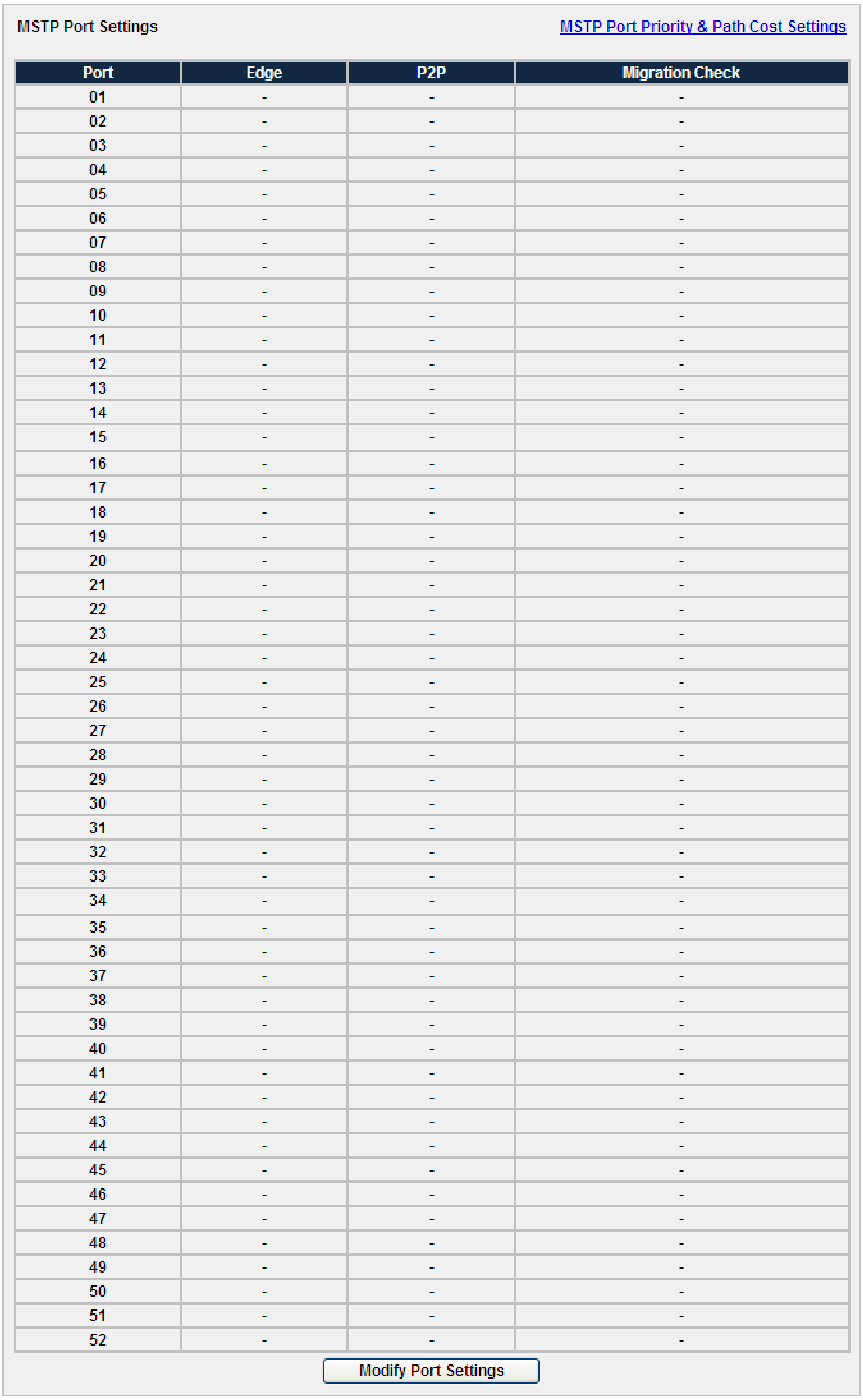
□ Enable MSTP	
Region Name (Max. 32 chars.)	Region_One
Revision Level (0-65535)	0
Max Age (6-40 sec)	20
Forward Delay (4-30 sec)	15
Max Hops (1-40)	7

Figure 4-5-6 MSTP Screenshot

The page includes the following fields:

Object	Description
• **Enable MSTP**	Enable or disable MSTP capability.
• **Region Name**	Specifies the configuration region name. The name string has a maximum length of 32 characters and is case sensitive.
• **Revision Level**	Specifies the configuration revision level. The range is 0 to 65535.
• **Max Age**	Configures the maximum age of the current bridge. This is the maximum age of spanning tree protocol information learned from the network on any port before it is discarded.
• **Forward Delay**	Forward delay is a time value which controls how fast a port changes its state. The value determines how long the port stays in each of the listening and learning states which precede the forward state. This value is also used to age all dynamic entries in the forwarding databases when a topology change has been detected and is underway. **Note: Max Age <= 2*(Forward Delay-1)**
• **Max Hops**	Specifies the number of hops in a region before the BPDU is discarded and the information held for a port is aged.

4.5.4 MSTP Port



MSTP Port Settings

MSTP Port Priority & Path Cost Settings

Port	Edge	P2P	Migration Check
01	-	-	-
02	-	-	-
03	-	-	-
04	-	-	-
05	-	-	-
06	-	-	-
07	-	-	-
08	-	-	-
09	-	-	-
10	-	-	-
11	-	-	-
12	-	-	-
13	-	-	-
14	-	-	-
15	-	-	-
16	-	-	-
17	-	-	-
18	-	-	-
19	-	-	-
20	-	-	-
21	-	-	-
22	-	-	-
23	-	-	-
24	-	-	-
25	-	-	-
26	-	-	-
27	-	-	-
28	-	-	-
29	-	-	-
30	-	-	-
31	-	-	-
32	-	-	-
33	-	-	-
34	-	-	-
35	-	-	-
36	-	-	-
37	-	-	-
38	-	-	-
39	-	-	-
40	-	-	-
41	-	-	-
42	-	-	-
43	-	-	-
44	-	-	-
45	-	-	-
46	-	-	-
47	-	-	-
48	-	-	-
49	-	-	-
50	-	-	-
51	-	-	-
52	-	-	-

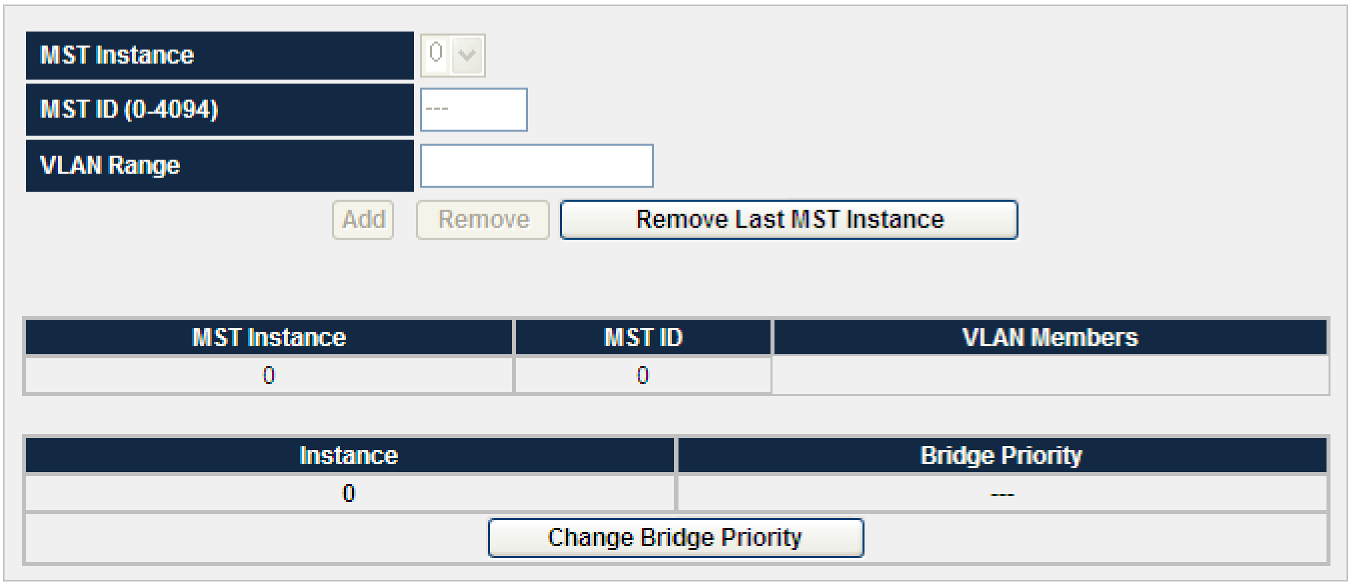
Figure 4-5-7 MSTP Port Screenshot

The page includes the following fields:

Object	Description
• **MSTP Port Settings**	The MSTP Port Settings configure MSTP port parameters.
• **Port**	Indicates the port numbers of the system.
• **Edge**	Indicates if this port is the edge port. Once configured as an edge port, the port state immediately transitions from disable/block to forwarding state.
• **P2P**	Indicates if this port is a point-to-point link. If you connect a port to another port though a point-to-point link and the local port becomes a designated port, it negotiates a rapid transition with the other port to ensure a loop-free topology.
• **Migration Check**	Re-checks the appropriate BPDU format to send on this port.
• **Path Cost**	Displays the cost of this port for the specified MST instance. "Cost" means the contribution of this port to the path cost of paths towards the spanning tree root which include this port.
• **Port Priority**	Displays the priority of this port for the specified MST instance.

4.5.5 MSTP Instance

MSTP operation maps VLANs into STP instances. Packets assigned to various VLANs are transmitted along different paths within **Multiple Spanning Tree Regions** (MST Regions). Regions are one or more Multiple Spanning Tree bridges by which frames can be transmitted. In configuring MST, the MST region to which the device belongs is defined. A configuration consists of the name, revision, and region to which the device belongs.



MST Instance	0
MST ID (0-4094)	---
VLAN Range	

MST Instance	MST ID	VLAN Members
0	0	

Instance	Bridge Priority
0	---

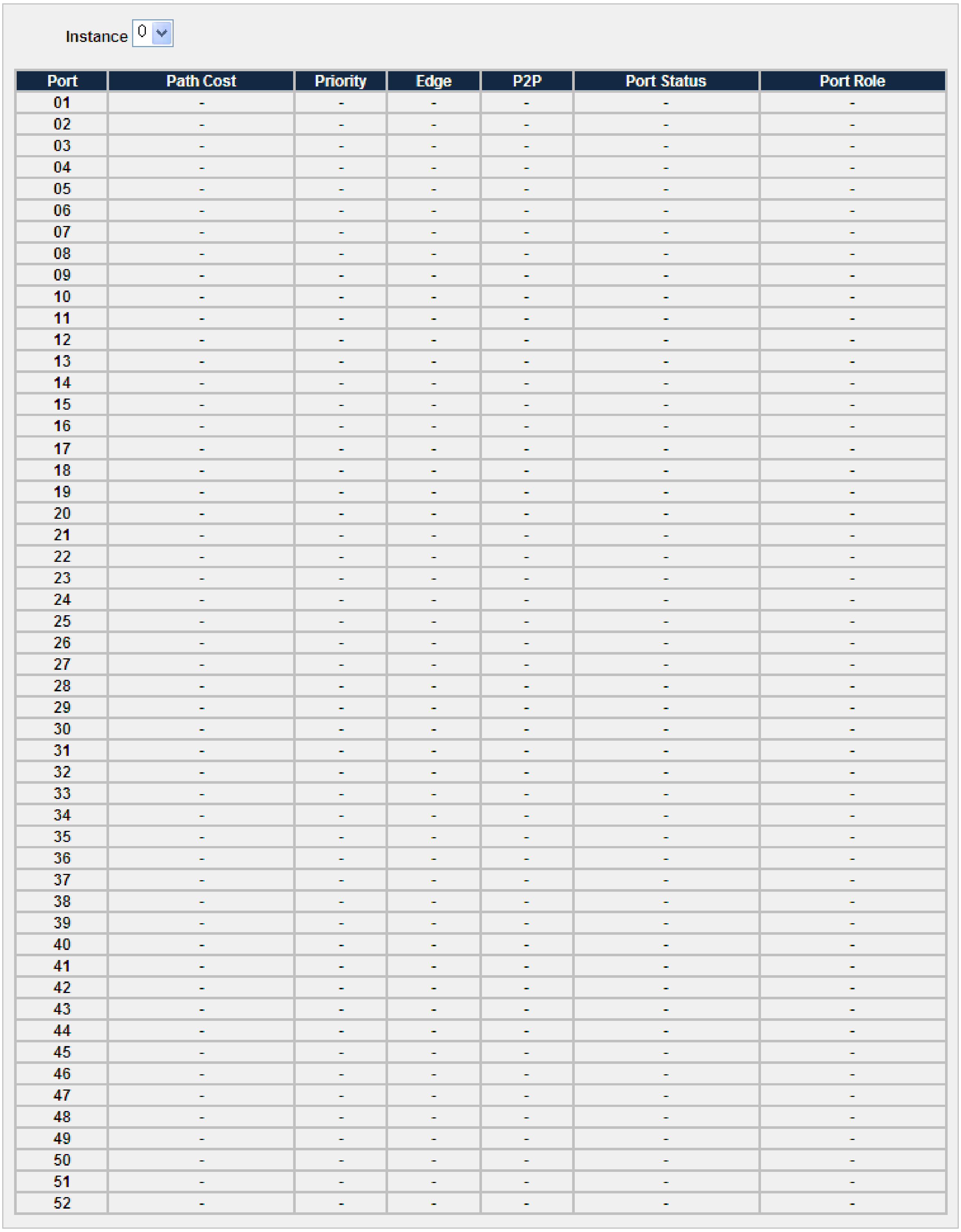
Figure 4-5-8 MSTP Instance Screenshot

The page includes the following fields:

Object	Description
• **MST Instance**	Specifies the instance to configure. This system can support up to **16** MSTP instances.
• **MST ID**	Specifies the instance identifier. the range is 0 to 4094.
• **VLAN Range**	Specifies vlan-range, the range is 1 to 4094. To specify a VLAN range, use a hyphen; for example, 1-63 means VLANs 1 through 63. To specify a VLAN series, use a comma; for example, 10,20,30 means VLANs 10, 20, and 30.
• **"Add"**	Creates a MST instance, map VLANs to a MST instance.
• **"Remove"**	Remove VLANs from the specified MST instance.
• **"Remove the last MST instance"**	Removes the last created MST instance.
• **Change Bridge Priority**	Specifies the selected spanning tree instance device priority. The field range is 0-61440

4.5.6 MSTP Interface

Network Administrators can assign MSTP Interface settings through the "MSTP Port" page.



Instance 0

Port	Path Cost	Priority	Edge	P2P	Port Status	Port Role
01	-	-	-	-	-	-
02	-	-	-	-	-	-
03	-	-	-	-	-	-
04	-	-	-	-	-	-
05	-	-	-	-	-	-
06	-	-	-	-	-	-
07	-	-	-	-	-	-
08	-	-	-	-	-	-
09	-	-	-	-	-	-
10	-	-	-	-	-	-
11	-	-	-	-	-	-
12	-	-	-	-	-	-
13	-	-	-	-	-	-
14	-	-	-	-	-	-
15	-	-	-	-	-	-
16	-	-	-	-	-	-
17	-	-	-	-	-	-
18	-	-	-	-	-	-
19	-	-	-	-	-	-
20	-	-	-	-	-	-
21	-	-	-	-	-	-
22	-	-	-	-	-	-
23	-	-	-	-	-	-
24	-	-	-	-	-	-
25	-	-	-	-	-	-
26	-	-	-	-	-	-
27	-	-	-	-	-	-
28	-	-	-	-	-	-
29	-	-	-	-	-	-
30	-	-	-	-	-	-
31	-	-	-	-	-	-
32	-	-	-	-	-	-
33	-	-	-	-	-	-
34	-	-	-	-	-	-
35	-	-	-	-	-	-
36	-	-	-	-	-	-
37	-	-	-	-	-	-
38	-	-	-	-	-	-
39	-	-	-	-	-	-
40	-	-	-	-	-	-
41	-	-	-	-	-	-
42	-	-	-	-	-	-
43	-	-	-	-	-	-
44	-	-	-	-	-	-
45	-	-	-	-	-	-
46	-	-	-	-	-	-
47	-	-	-	-	-	-
48	-	-	-	-	-	-
49	-	-	-	-	-	-
50	-	-	-	-	-	-
51	-	-	-	-	-	-
52	-	-	-	-	-	-

Figure 4-5-9 MSTP Interface Screenshot

The page includes the following fields:

Object	Description
• **Instance**	Specifies the MST instance.
• **Path Cost**	Displays the cost of this port for the specified MST instance. "Cost" means the contribution of this port to the path cost of paths towards the spanning tree root which include this port.
• **Priority**	Displays the priority of this port for the specified MST instance.
• **Edge**	Indicates if this port is the edge port. Once configured as an edge port, the port state immediately transitions from disable/block to forwarding state.
• **P2P**	Indicates if this port is a point-to-point link. If you connect a port to another port though a point-to-point link and the local port becomes a designated port, it negotiates a rapid transition with the other port to ensure a loop-free topology.
• **Port Status**	Displays the MSTP port status for the specified MST instance.
• **Port Role**	Displays the role of this port for the specified MST instance.

4.6 Multicast

This section is to control the multicast of the switch, the multicast function contains links to the following topics:

- **Static Multicast**
- **Static Multicast Table**
- **IGMP**

4.6.1 IGMP Snooping

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.

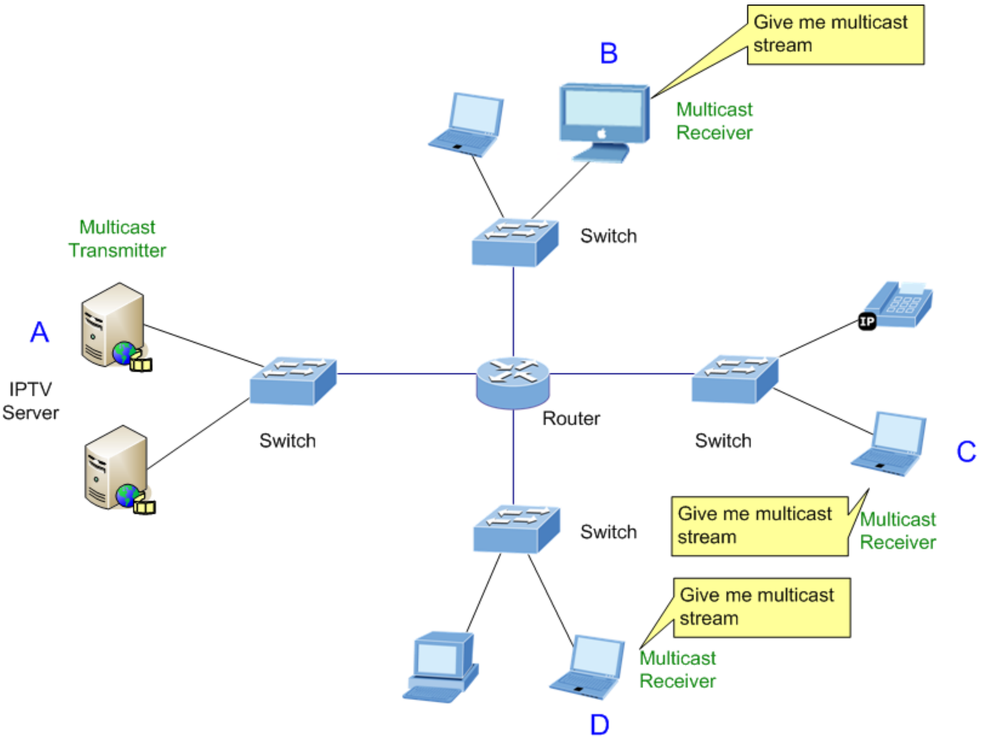


Figure 4-6-1 Multicast Service

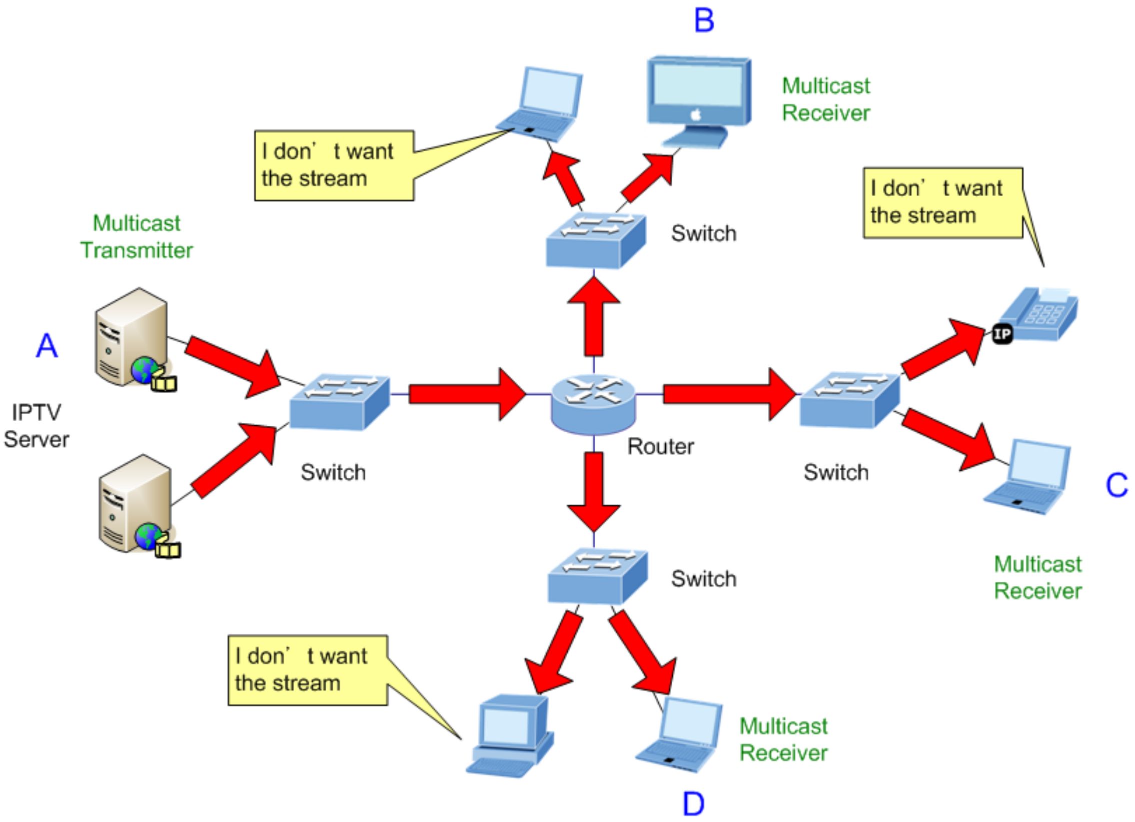


Figure 4-6-2 Multicast flooding

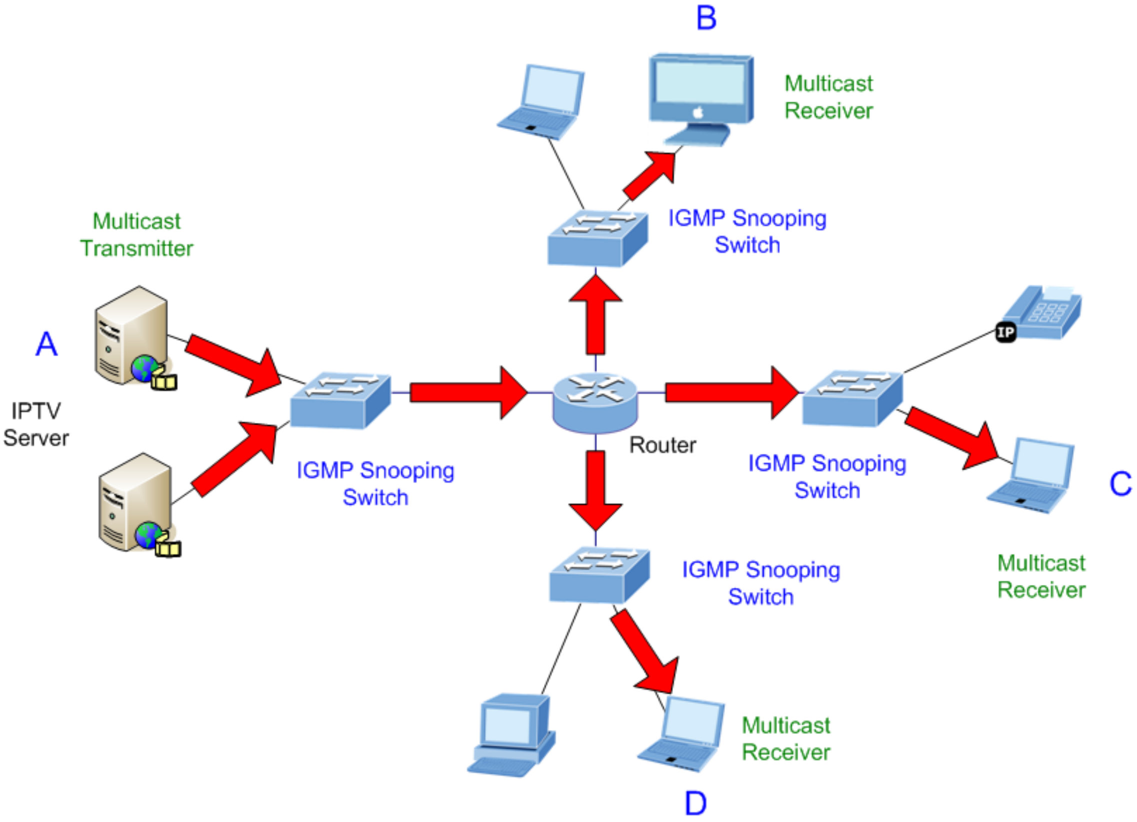


Figure 4-6-3 IGMP Snooping multicast stream control

IGMP Versions 1 and 2

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

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

The format of an IGMP packet is shown below:

IGMP Message Format

Octets

0	8	16	31
Type	Response Time	Checksum	
Group Address (all zeros if this is a query)			

The IGMP Type codes are shown below:

Type	Meaning
0x11	Membership Query (if Group Address is 0.0.0.0)
0x11	Specific Group Membership Query (if Group Address is Present)
0x16	**Membership Report (version 2)**
0x17	**Leave a Group (version 2)**
0x12	**Membership Report (version 1)**

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

A host sends an IGMP **"report"** to join a group

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

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

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

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

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

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

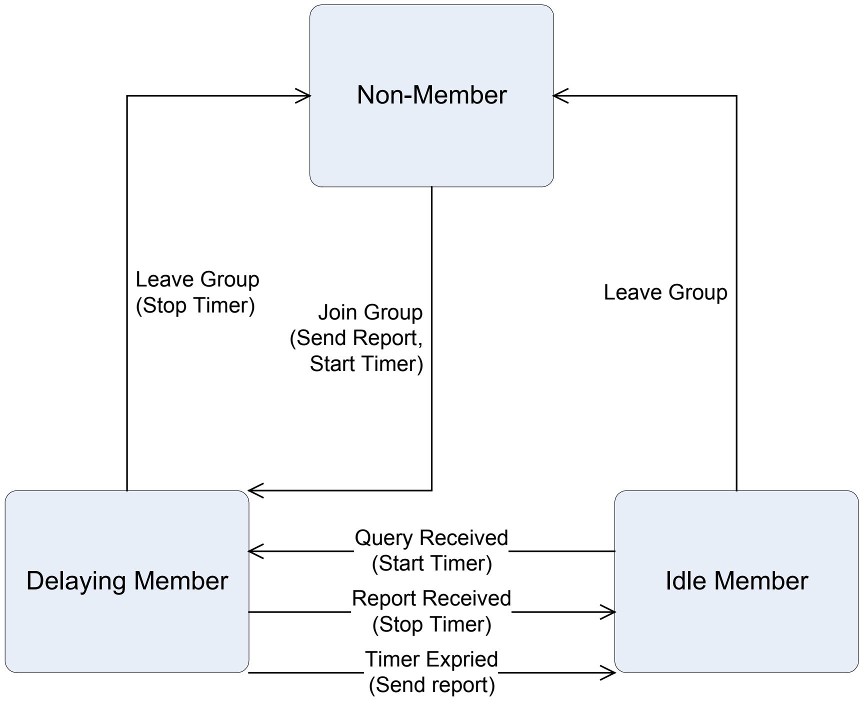


Figure 4-6-4 IGMP State Transitions

- **IGMP Querier –**

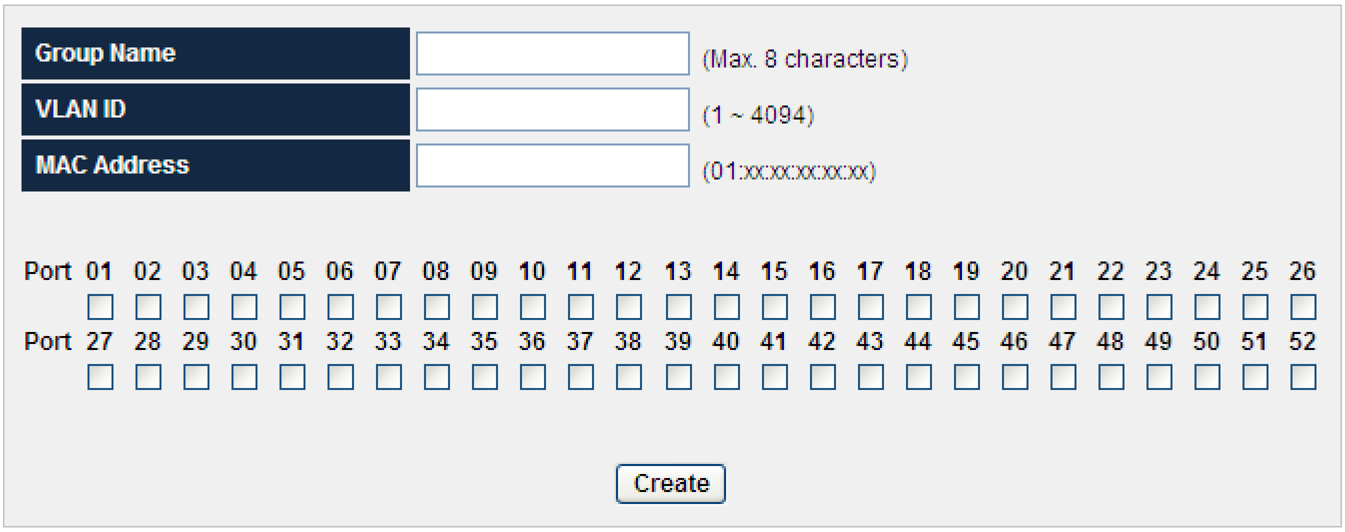
  A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "**querier**" and assumes the role of querying the LAN for group members. It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

4.6.2 Static Multicast

Static multicast groups provides a way to add and delete multicast addresses in the L2 address table.



Group Name		(Max. 8 characters)
VLAN ID		(1 ~ 4094)
MAC Address		(01:xx:xx:xx:xx:xx)

Port	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Port	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

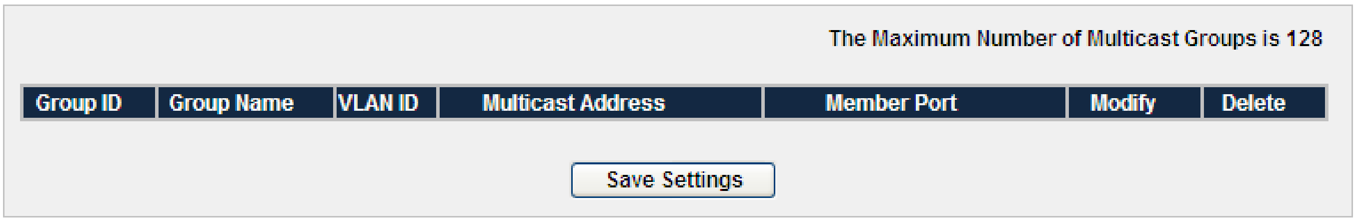
Figure 4-6-5 Static Multicast Screenshot

The page includes the following fields:

Object	Description
• **Group Name**	Inserts a symbolic name for easy maintenance for this multicast group.
• **VLAN ID**	Specifies a VLAN ID for this multicast group(1 - 4094).
• **MAC Address**	Specifies a L2 multicast address(Format: 01:XX:XX:XX:XX:XX).
• **Port**	Specifies the multicast port members.

4.6.3 Static Multicast Table

The IGMP Static Multicast Table allowed the network administrator to assigning a specificy Multicast Group to a port. The port is configured to send and receive all traffic for a particular mulcast group. Usually, the function is use to test the multicast protocols in the network or for the PC/Laptop manufactory to pre-install operation system via multicast. There is maximum 128 static Multicast Groups are able to assign.



The Maximum Number of Multicast Groups is 128

Group ID	Group Name	VLAN ID	Multicast Address	Member Port	Modify	Delete

Figure 4-6-6 Static Multicast Table Screenshot

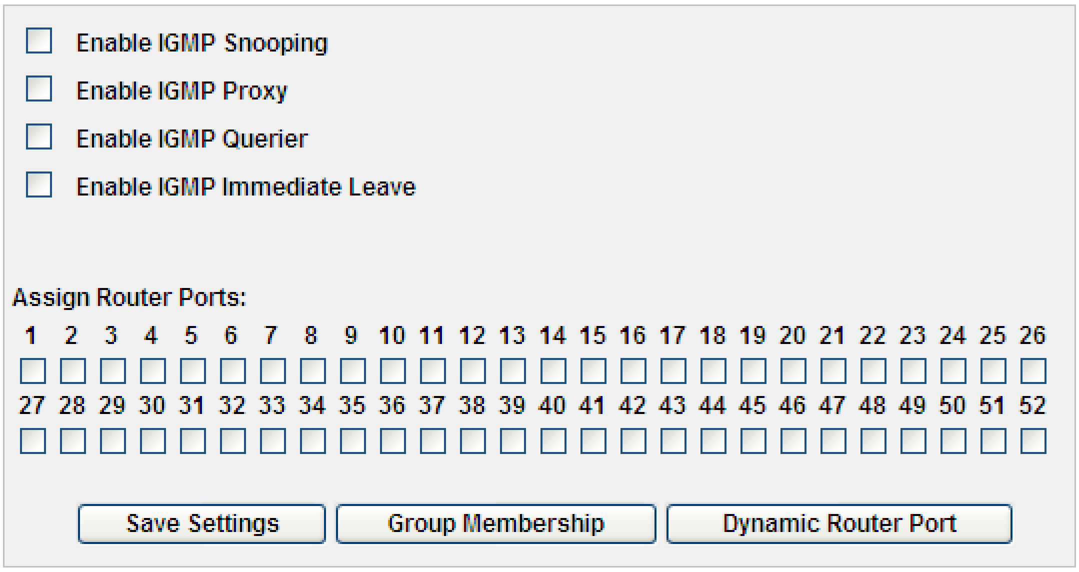
The page includes the following fields:

Object	Description
• **Group ID**	The index for this static multicast group.

• **Group Name**	The name for this static multicast group.
• **VLAN ID**	The VLAN ID for this static multicast group.
• **Multicast Address**	The multicast address for this static multicast group.
• **Member Port**	The port members for this static multicast group.
• **Modify**	Specifies the states of port member for this static multicast group.
• **Delete**	To destroy the existing multicast group.

4.6.4 IGMP

IGMP is a standard defined in RFC1112 for IGMPv1, and in RFC2236 for IGMPv2. IGMP specifies how a host can register a router in order to receive specific multicast traffic. Configure the switch to use IGMP snooping in subnets that receive IGMP queries from either IGMP or the IGMP snooping querier. IGMP snooping constrains multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward multicast traffic only to those ports that want to receive it.



□ Enable IGMP Snooping

□ Enable IGMP Proxy

□ Enable IGMP Querier

□ Enable IGMP Immediate Leave

Assign Router Ports:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Figure 4-6-7 IGMP Screenshot

The page includes the following fields:

Object	Description
• **Enable IGMP Snooping**	Enable or disable IGMP snooping.
• **Enable IGMP Proxy**	Enable or disable IGMP proxy.
• **Enable IGMP Querier**	Enable or disable IGMP querier.
• **Enable IGMP Immediate Leave**	Enable or disable IGMP immediate leave.
• **Assign Router Ports**	Specify ports to which IGMP routers were connected.
• **Dynamic Router Port**	Click on this button to display the port that receive the following traffic.

	1. IGMP Query 2. Packet with destination IP 224.0.0.2
• **Group Membership**	Click on this button to display the IGMP groups information.
• **VLAN ID**	Indicates the VLAN ID of the specified multicast group.
• **Group Address**	Indicates IPv4 multicast group address of the group being reported.
• **Member Port(s)**	Indicates the membership associated with the group.

4.7 Security

This section is to control the security access of the switch, includes the user access and management control.

The Security function contains links to the following topics:

- **ACL**
- **Port Security**
- **802.1X**
- **RADIUS**
- **TACACS+**
- **Strom Control**
- **Management IP List**
- **Auto DoS**
- **SSH**
- **HTTPS**
- **Telnet**

4.7.1 ACL

An ACL consists of a set of rules which are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit / Deny) is taken and the additional rules are not checked for a match. On this menu the interfaces to which an ACL applies must be specified, as well as whether it applies to inbound or outbound traffic. Rules for the ACL are specified/created using the ACL Rule Configuration menu.

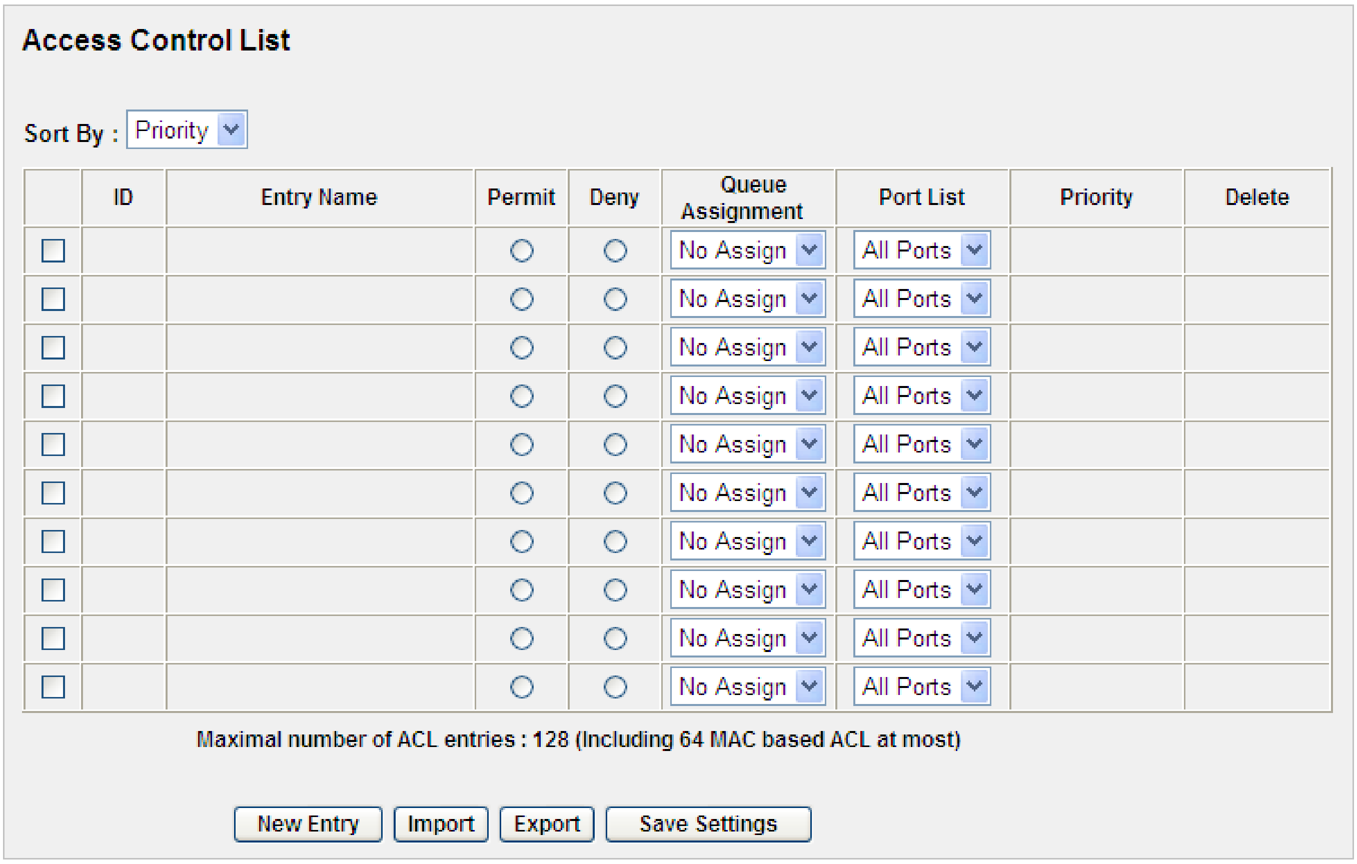
ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

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.

ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID.

There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.



Access Control List

Sort By : Priority

	ID	Entry Name	Permit	Deny	Queue Assignment	Port List	Priority	Delete
□			○	○	No Assign	All Ports		
□			○	○	No Assign	All Ports		
□			○	○	No Assign	All Ports		
□			○	○	No Assign	All Ports		
□			○	○	No Assign	All Ports		
□			○	○	No Assign	All Ports		
□			○	○	No Assign	All Ports		
□			○	○	No Assign	All Ports		
□			○	○	No Assign	All Ports		
□			○	○	No Assign	All Ports		

Maximal number of ACL entries : 128 (Including 64 MAC based ACL at most)

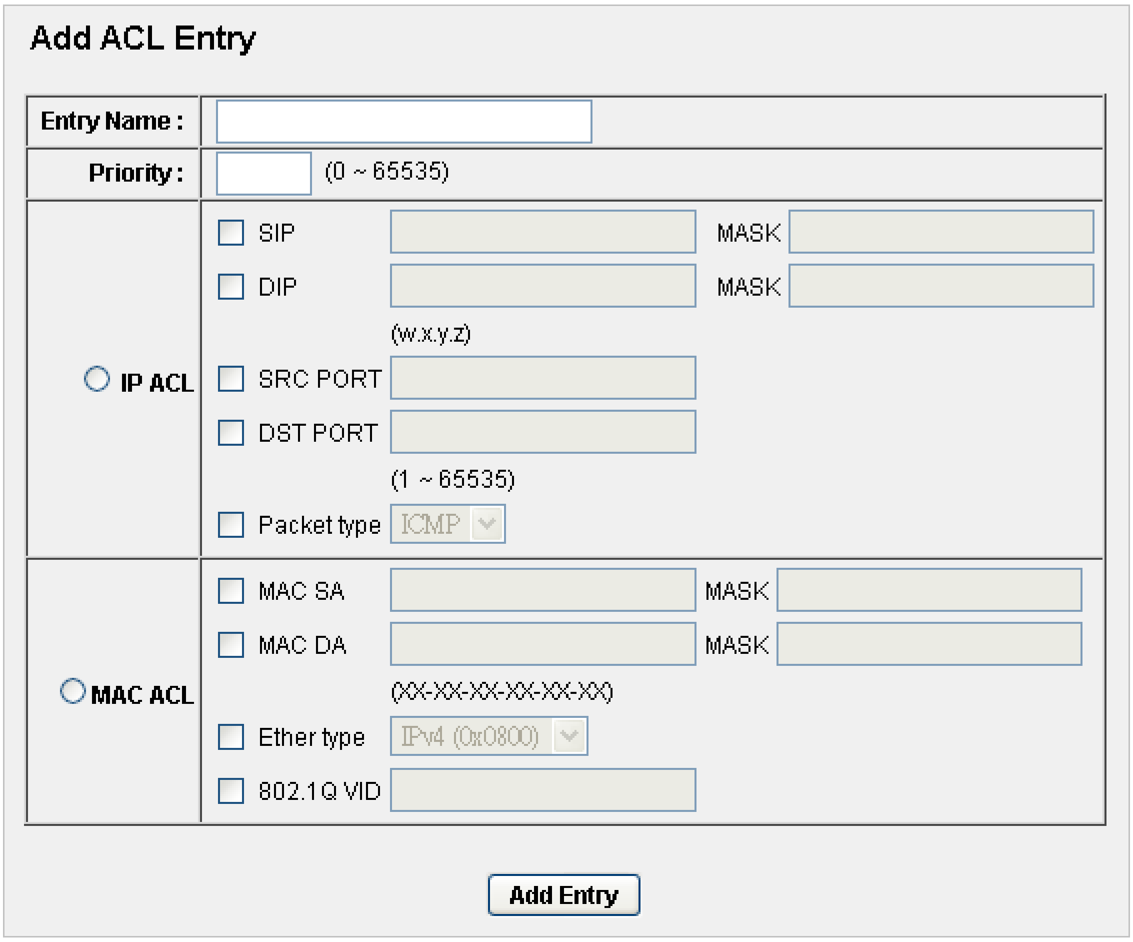
Figure 4-7-1 Access Control List main page Screenshot

The page includes the following fields:

Object	Description
• **Sort By**	Defines the type of sort. It includes **priority**, **deny** and **permit**.
• **Entry Name**	Indicates the name of ACL entry. The length of name have to be smaller than 20. And Different ACL entries can't have the same name.
• **Permit**	Frames matching the ACL entries may be forwarded and learned.
• **Deny**	Frames matching the ACL entries are dropped.
• **Queue Assignment**	Select a traffic class of **No Assign**, **1**, **2**, **3** or **4** to apply to the ACL.
• **Port List**	Indicates the ports ,ACL entry apply to. When add new entry default to all ports,so you can click "modify" linker to modify it.
• **Proiority**	Indicates the priority of ACL entry. The largest value have highest priority. The range is from 0 to 65535. And Different ACL entries can't have the same priority. **+** increase priority by 1. **-** decrease priority by 1.
• **Delete**	By which deletes the selected ACL.
• **New Entry**	Inserts a new ACL entry.
• **Import**	Selects an XML file to import.

• **Export**	Writes all ACL entries to an XML file.
• **Save Settings**	Modifies the changes of ACL entries which are shown on this page.

■ **Create new ACL entry**



Add ACL Entry

Entry Name :	
Priority :	(0 ~ 65535)
○ IP ACL	□ SIP MASK □ DIP MASK (w.x.y.z) □ SRC PORT □ DST PORT (1 ~ 65535) □ Packet type ICMP
○ MAC ACL	□ MAC SA MASK □ MAC DA MASK (XX-XX-XX-XX-XX-XX) □ Ether type IPv4 (0x0800) □ 802.1Q VID

Add Entry

Figure 4-7-2 Access Control List – add new ACL entry Screenshot

The Page contains the following fields:

Object	Description
• **Entry Name**	Defines a new user-defined IP based ACL
• **Priority**	Indicates the priority of ACL entry. The largest value have highest priority. The range is from 0 to 65535. And Different ACL entries can't have the same priority.
IP ACL	
• **SIP** (Source IP Address)	Matches the **source port IP address** to which packets are addressed to the ACE. And it's format is **w.x.y.z**.
• **MASK**	Defines the source IP address **mask**.
• **DIP**	Matches the **destination port IP address** to which packets are addressed to the ACE. And it's format is **w.x.y.z**.

(Destination IP Address)

- **MASK**

  Defines the destination IP address **mask**

- **SRC Port**

  Defines the **TCP/UDP source port** to which the ACE is matched. This field is active only if 800/6-TCP or 800/17-UDP is selected in the Select from List drop-down menu.

  The possible field range is **0 - 65535**

- **DST Port**

  Defines the **TCP/UDP destination port**. This field is active only if 800/6-TCP or 800/17-UDP is selected in the Select from List drop-down menu.

  The possible field range is **0 - 65535**

- **Packet Type**

  Where selects from a protocols list on which ACE can be based. The possible field values are:

  - **ICMP**, which indicates that the Internet Control Message Protocol (ICMP) is used to classify network flows.
  - **IGMP**, which indicates that the Internet Group Management Protocol (IGMP) is used to classify network flows.
  - **TCP**, which indicates that the Transmission Control Protocol is used to classify network flows.
  - **UDP**, which indicates that the User Datagram Protocol is used to classify network flows.
  - **IP**, which indicates that all IPv4 frames are used to classify network flows.
  - **GRE** , which indicates that the Generic Routing Encapsulation (GRE) protocol is used to classify network flows.

MAC ACL

- **MAC SA**

  Matches the **source MAC address** to which packets are addressed to the ACE. And it's format is XX-XX-XX-XX-XX-XX.

- **MASK**

  Defines the source MAC address mask.

- **MAC DA**

  Where matches the **destination MAC address** to which packets are addressed to the ACE. And it's format is XX-XX-XX-XX-XX-XX.

- **MASK**

  Defines the destination MAC address mask.

- **Ether Type**

  Means destination TCP/UDP port number.

  The range is from 1 to 65535.

- **802.1Q VLAN ID**

  When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.

- **Add Entry**

  Inserts this ACL entry.

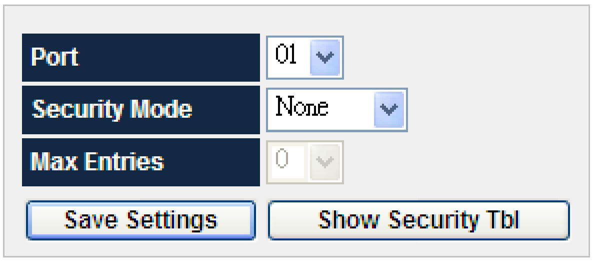
Note

1. If the rule/filter of ACL entry is empty, the check box of this entry will not be checked by default.
2. If the check box is not checked, the corresponding ACL entry will not be programmed to hardware.
3. Before input MAC, IP, port number, Packet type or Ether type, you have to check the corresponding check box of rule/filter.
4. The count of ACL entries which own PORT rule/filter have to be smaller than 8, otherwise it would cause NO RESOURCE when add ACL entry.

4.7.2 Port Security

Port security is a feature that allows you to configure a switch port with one or more device MAC addresses that are authorized to access the network through that port.

When port security is enabled on a port, the Managed Switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be authorized to access the network through that port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

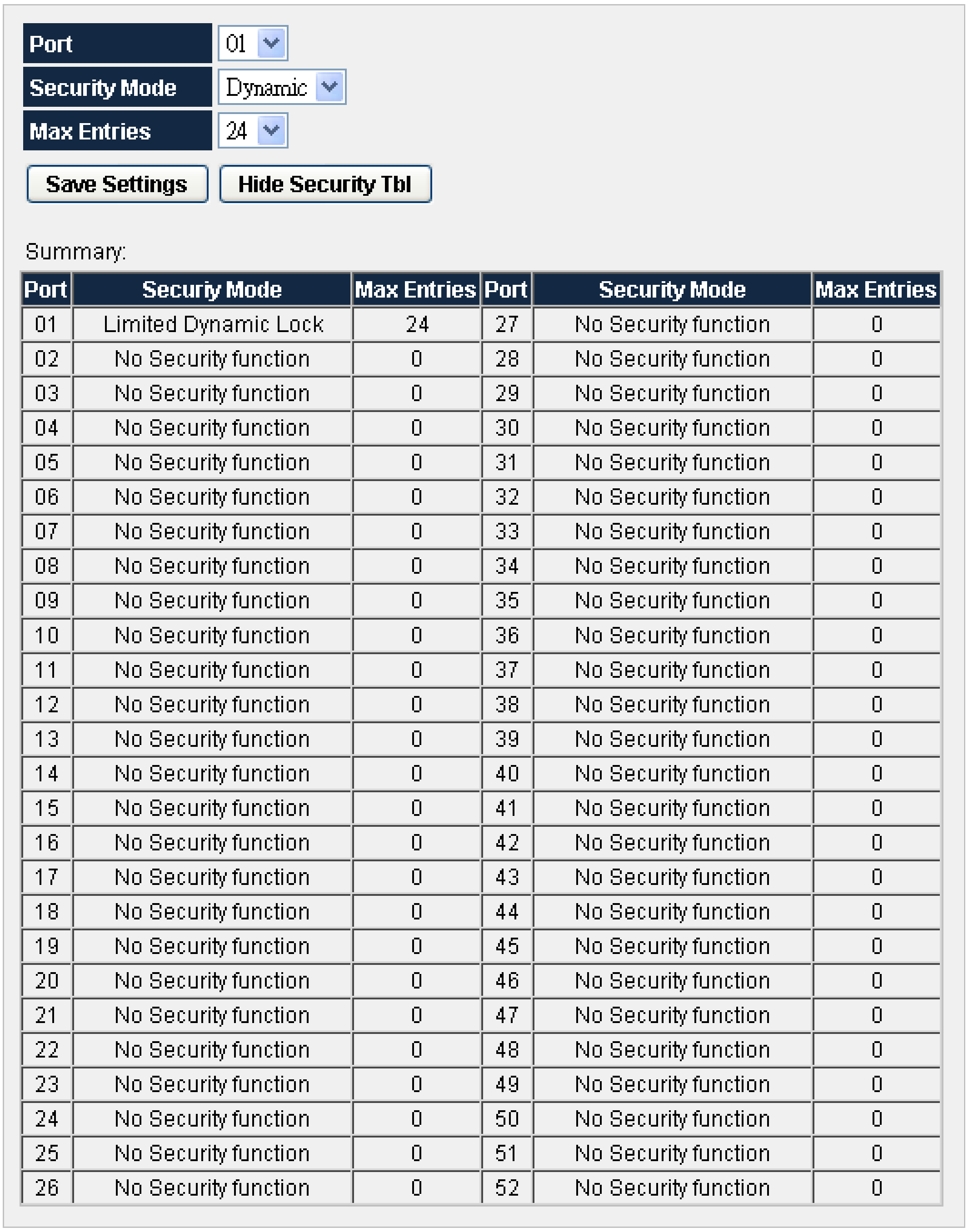


Port	01
Security Mode	None
Max Entries	0

Figure 4-7-3 Port Security main screen Screenshot

The page includes the following fields:

Object	Description
• **Port**	Selects a specific port to configure.
• **Security Mode**	Specifies the port security mode **None:** Disable port security on the port. **Dynamic:** Determines dynamic learning mode with accept function.
• **Max Entries**	It associates with Dynamic mode and indicates the maximum SA addresses can be learnt(**0~24**) on this port.



Port	01
Security Mode	Dynamic
Max Entries	24

Summary:

Port	Securiy Mode	Max Entries	Port	Security Mode	Max Entries
01	Limited Dynamic Lock	24	27	No Security function	0
02	No Security function	0	28	No Security function	0
03	No Security function	0	29	No Security function	0
04	No Security function	0	30	No Security function	0
05	No Security function	0	31	No Security function	0
06	No Security function	0	32	No Security function	0
07	No Security function	0	33	No Security function	0
08	No Security function	0	34	No Security function	0
09	No Security function	0	35	No Security function	0
10	No Security function	0	36	No Security function	0
11	No Security function	0	37	No Security function	0
12	No Security function	0	38	No Security function	0
13	No Security function	0	39	No Security function	0
14	No Security function	0	40	No Security function	0
15	No Security function	0	41	No Security function	0
16	No Security function	0	42	No Security function	0
17	No Security function	0	43	No Security function	0
18	No Security function	0	44	No Security function	0
19	No Security function	0	45	No Security function	0
20	No Security function	0	46	No Security function	0
21	No Security function	0	47	No Security function	0
22	No Security function	0	48	No Security function	0
23	No Security function	0	49	No Security function	0
24	No Security function	0	50	No Security function	0
25	No Security function	0	51	No Security function	0
26	No Security function	0	52	No Security function	0

Figure 4-7-4 Port Security – current security table Screenshot

4.7.3 802.1x

■ Overview of 802.1X Port-Based Authentication

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

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

4.7.3.1 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.

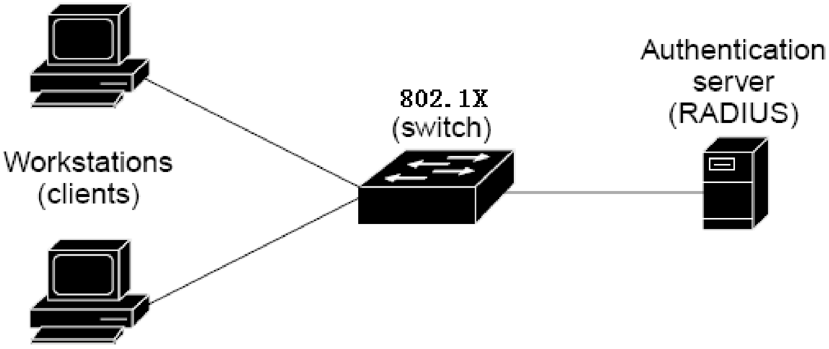


Figure 4-7-5 Device Roles

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

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

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

- **Authentication Initiation and Message Exchange**

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

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

Note

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

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

The specific exchange of EAP frames depends on the authentication method being used. "Figure 4-7-6" shows a message exchange initiated by the client using the **One-Time-Password (OTP)** authentication method with a RADIUS server.

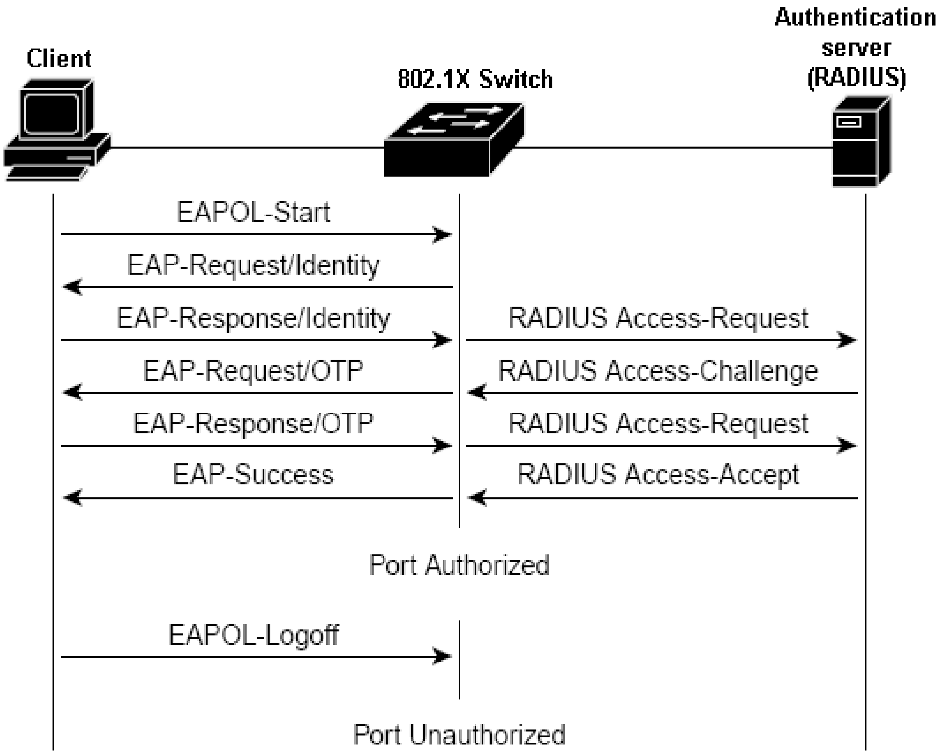


Figure 4-7-6 EAP message exchange

- **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

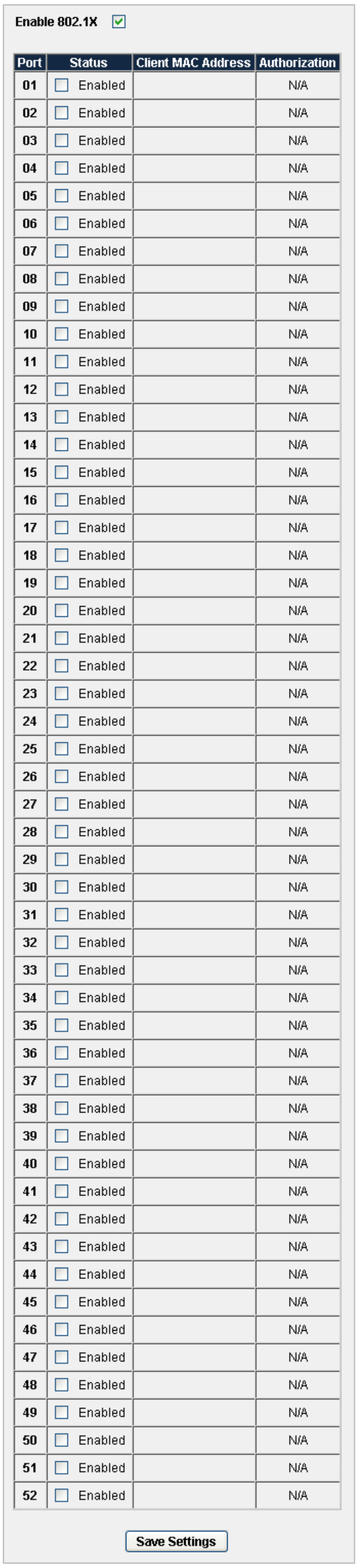
If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication 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.

4.7.3.2 802.1x Port Configuration

The Port Authentication function establishes security between ports.



Enable 802.1X ☑

Port	Status	Client MAC Address	Authorization
01	☐ Enabled		N/A
02	☐ Enabled		N/A
03	☐ Enabled		N/A
04	☐ Enabled		N/A
05	☐ Enabled		N/A
06	☐ Enabled		N/A
07	☐ Enabled		N/A
08	☐ Enabled		N/A
09	☐ Enabled		N/A
10	☐ Enabled		N/A
11	☐ Enabled		N/A
12	☐ Enabled		N/A
13	☐ Enabled		N/A
14	☐ Enabled		N/A
15	☐ Enabled		N/A
16	☐ Enabled		N/A
17	☐ Enabled		N/A
18	☐ Enabled		N/A
19	☐ Enabled		N/A
20	☐ Enabled		N/A
21	☐ Enabled		N/A
22	☐ Enabled		N/A
23	☐ Enabled		N/A
24	☐ Enabled		N/A
25	☐ Enabled		N/A
26	☐ Enabled		N/A
27	☐ Enabled		N/A
28	☐ Enabled		N/A
29	☐ Enabled		N/A
30	☐ Enabled		N/A
31	☐ Enabled		N/A
32	☐ Enabled		N/A
33	☐ Enabled		N/A
34	☐ Enabled		N/A
35	☐ Enabled		N/A
36	☐ Enabled		N/A
37	☐ Enabled		N/A
38	☐ Enabled		N/A
39	☐ Enabled		N/A
40	☐ Enabled		N/A
41	☐ Enabled		N/A
42	☐ Enabled		N/A
43	☐ Enabled		N/A
44	☐ Enabled		N/A
45	☐ Enabled		N/A
46	☐ Enabled		N/A
47	☐ Enabled		N/A
48	☐ Enabled		N/A
49	☐ Enabled		N/A
50	☐ Enabled		N/A
51	☐ Enabled		N/A
52	☐ Enabled		N/A

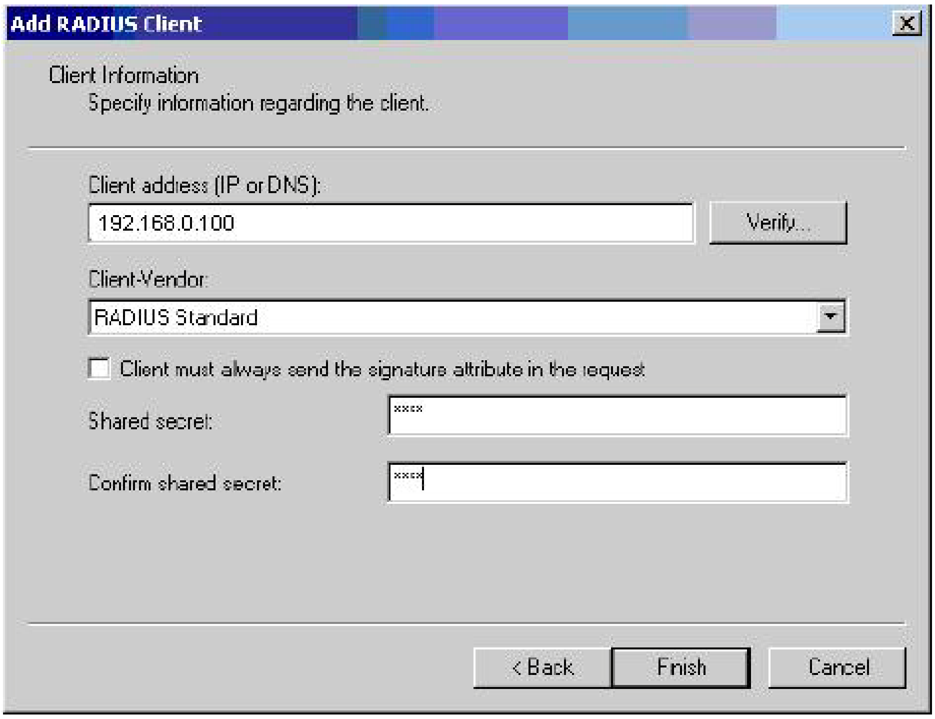
Figure 4-7-7 802.1X port configuration Screenshot

The page includes the following fields:

Object	Description
• **Enable 802.1X**	**Enables** or **disables** 802.1X function.
• **Status**	**Enables** or **disables** port authentication. • Enabled checked means these ports should be authorized by a RADIUS server to forward traffic. No traffic is forwarded if it is unauthorized. • Otherwise, no authentication process is required for those ports; all traffic could be forwarded normally.
• **Client MAC Address**	Displays the last client in the MAC address who send out the EAPOL control frame of the port.
• **Authorization**	Displays the authentication status of an enabled port. • **In Progress**: Indicates that the authentication is still in progress. Traffic is not forwarded before authentication is verified. • **N/A**: means no authentication required.

4.7.3.3 Windows Platform RADIUS Server Configuration

1. Setup the **RADIUS server** and assign the client IP address to the Managed switch. In this case, field in the default IP Address of the Managed Switch with **192.168.0.100**. And also make sure the shared secret key is as same as the one you had set at the switch RADIUS server – **12345678** at this case.



Add RADIUS Client

Client Information

Specify information regarding the client.

Client address (IP or DNS): 192.168.0.100

Client-Vendor: RADIUS Standard

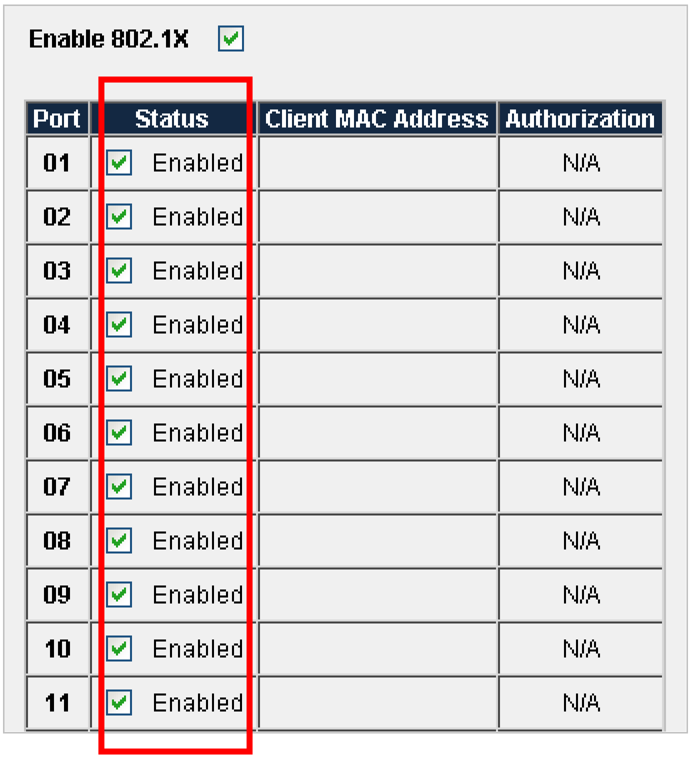
□ Client must always send the signature attribute in the request

Shared secret: ****

Confirm shared secret: ****

Figure 4-7-8 Windows Server RADIUS Server setting Screenshot

2. Configure ports attribute of 802.1X, the same as “802.1X Port Configuration”.



Enable 802.1X ☑

Port	Status	Client MAC Address	Authorization
01	☑ Enabled		N/A
02	☑ Enabled		N/A
03	☑ Enabled		N/A
04	☑ Enabled		N/A
05	☑ Enabled		N/A
06	☑ Enabled		N/A
07	☑ Enabled		N/A
08	☑ Enabled		N/A
09	☑ Enabled		N/A
10	☑ Enabled		N/A
11	☑ Enabled		N/A

Figure 4-7-9 802.1x Port Configuration Screenshot

3. Create user data. That step are different of “**Local Authenticate**”, the establishment of the user data needs to be created on the Radius Server PC. For example, the Radius Server founded on Win2000 Server, and then:

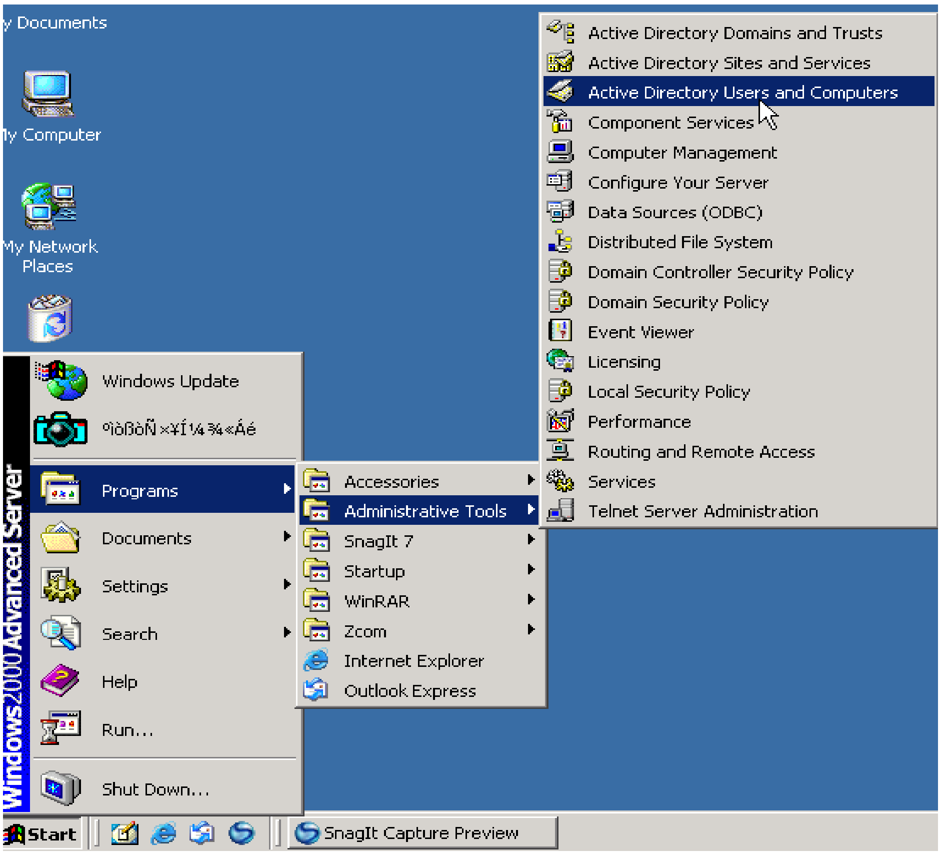
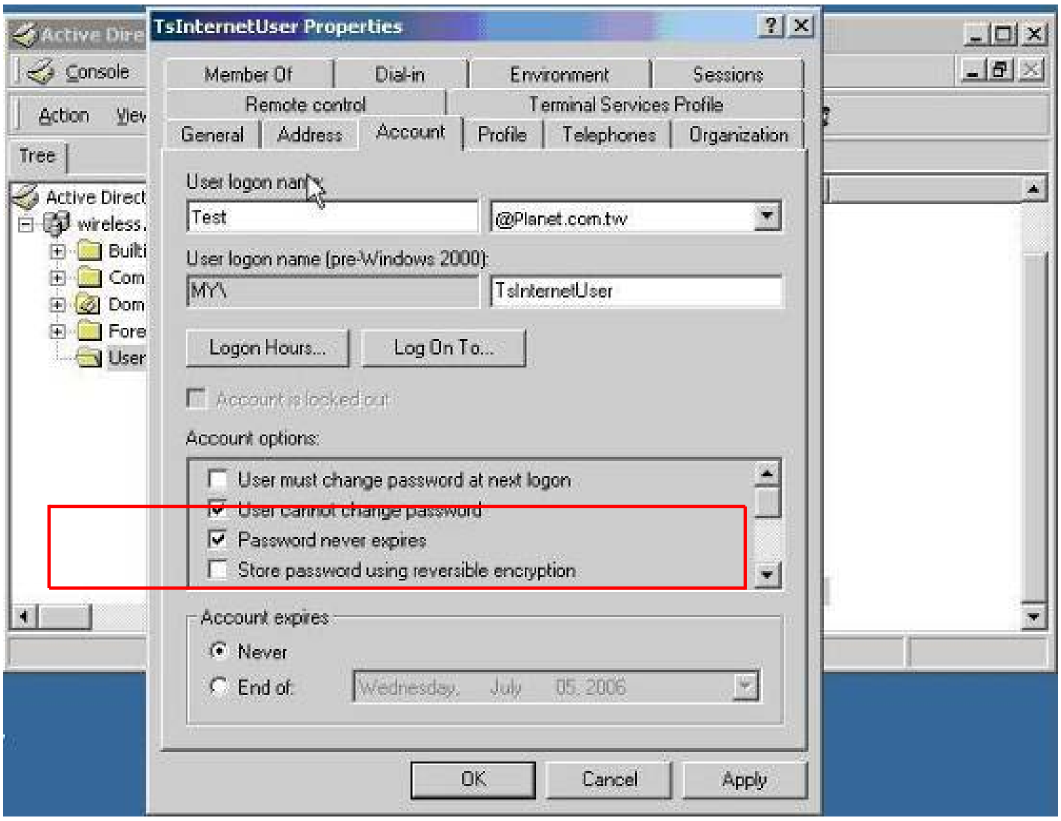


Figure 4-7-10 Windows Server RADIUS Server setting path

5. Enter " **Active Directory Users and Computers**", create legal user data, the next, right-click a user what you created to enter properties, and what to be noticed:



TsInternetUser Properties

User logon name: Test @Planet.com.tw

User logon name (pre-Windows 2000): MY\ TsInternetUser

□ Account is locked out

Account options:

□ User must change password at next logon

☑ User cannot change password

☑ Password never expires

□ Store password using reversible encryption

Account expires

● Never

○ End of: Wednesday, July 05, 2006

Figure 4-7-11 TsInternetUser Properties Screenshot

Note

> Set the Ports Authenticate Status to "**Disable**" if the port is connected to the RADIUS server or the port is a uplink port that is connected to another switch. Or once the 802.1X stat to work, the switch might not be able to access the RADIUS server.

4.7.3.4 802.1X Client Configuration

Windows XP is originally 802.1X support. As to other operating systems (windows 98SE, ME, 2000), an 802.1X client utility is needed. The following procedures show how to configure 802.1X Authentication in Windows XP.

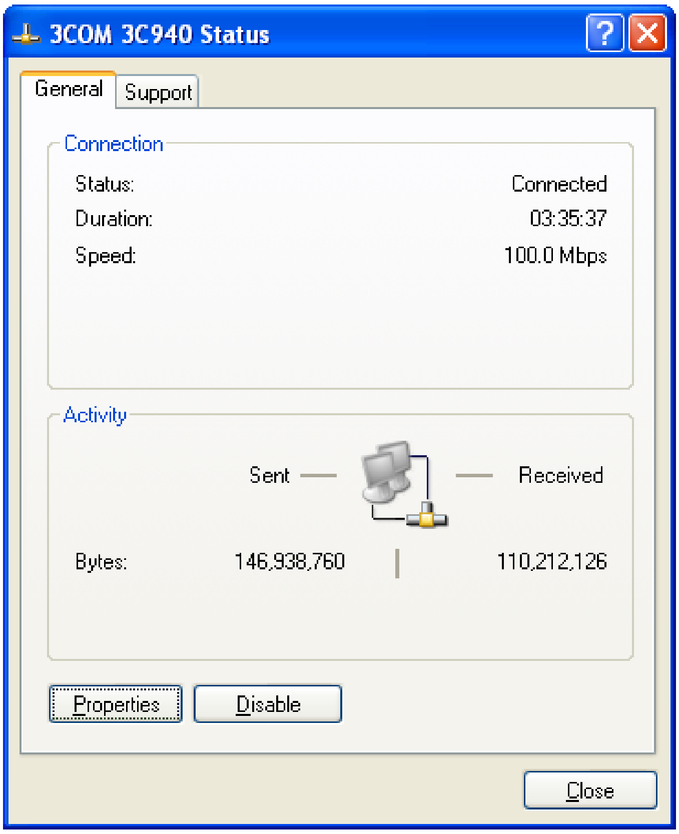
Please note that if you want to change the 802.1x authentication type of a wireless client, i.e. switch to EAP-TLS from EAP-MD5, you must remove the current existing wireless network from your preferred connection first, and add it in again.

- **Configure Sample: EAP-MD5 Authentication**

1. Go to **Start** > **Control Panel,** double-click on "**Network Connections**".

2. Right-click on the Local Network Connection.

3. Click "**Properties**" to open up the Properties setting window.



3COM 3C940 Status

Connection

Status: Connected
Duration: 03:35:37
Speed: 100.0 Mbps

Activity

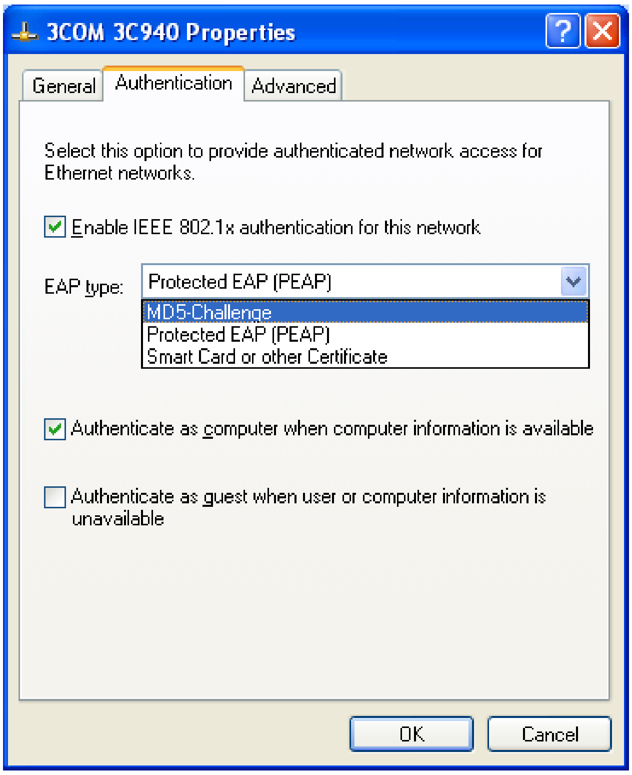
Bytes: 146,938,760 | 110,212,126

Figure 4-7-12 Client's NIC Screenshot

4. Select "**Authentication**" tab.

5. Select "**Enable network access control using IEEE 802.1X**" to enable 802.1x authentication.

6. Select "**MD-5 Challenge**" from the drop-down list box for EAP type.



3COM 3C940 Properties

Select this option to provide authenticated network access for Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: Protected EAP (PEAP)

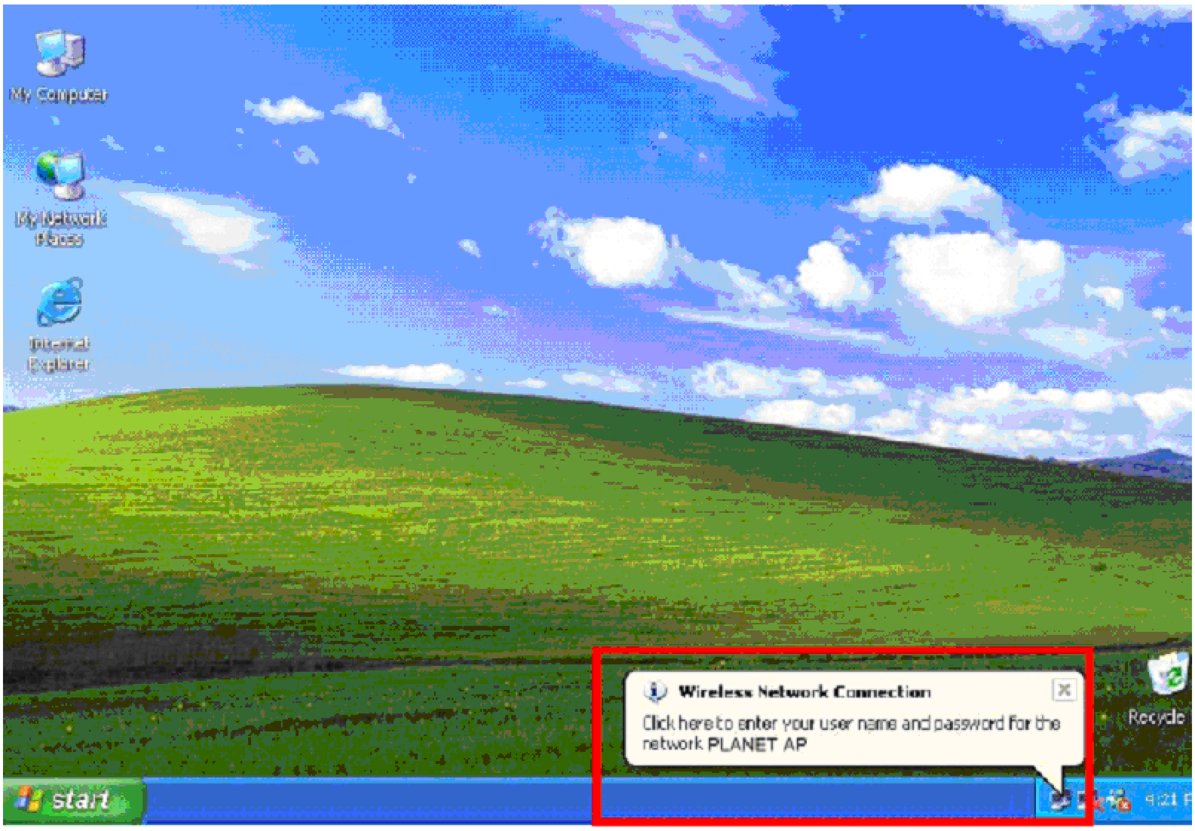
MD5-Challenge
Protected EAP (PEAP)
Smart Card or other Certificate

☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

Figure 4-7-13 802.1x client configuration Screenshot

7. Click "**OK**".
8. When client has associated with the Managed Switch, a user authentication notice appears in system tray. Click on the notice to continue.

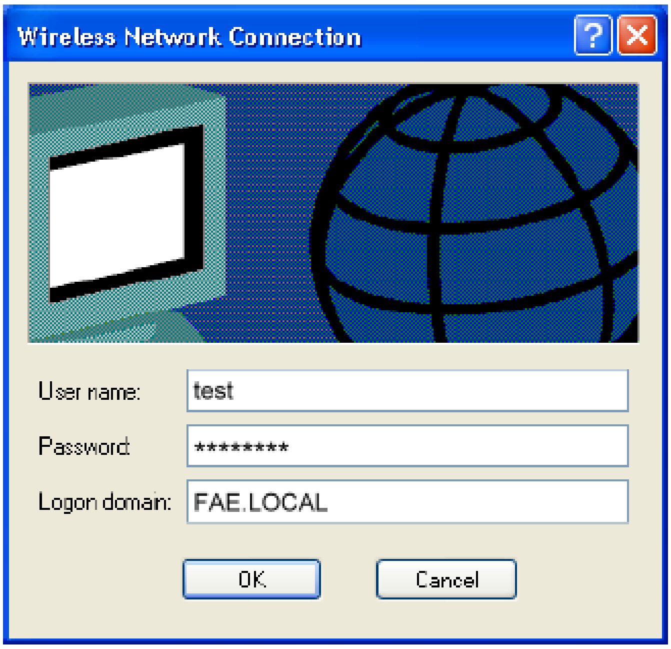


Wireless Network Connection

Click here to enter your user name and password for the network PLANET AP

Figure 4-7-14 802.1x client port-based authentication Screenshot

9. Enter the user name, password and the logon domain that your account belongs.
10. Click "**OK**" to complete the validation process.



Wireless Network Connection

User name: test

Password: ********

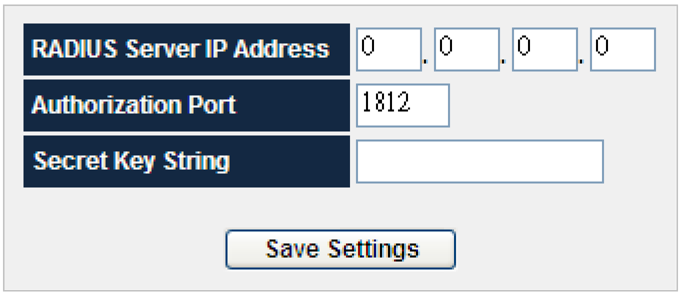
Logon domain: FAE.LOCAL

Figure 4-7-15 802.1x authentication dialogue window Screenshot

4.7.4 RADIUS

The RADIUS server is **Remote Authentication Dial-In User Service (RADIUS)** defined in RFC2865. It is primarily used by ISPs who authenticate a username and password before authorizing use of the network.

The RADIUS server configuration screen in Figure 4-7-16 appears.



RADIUS Server IP Address	0 . 0 . 0 . 0
Authorization Port	1812
Secret Key String	

Figure 4-7-16 RADIUS server configuration screenshot

The page includes the following fields:

Object	Description
• **RADIUS Server IP Address**	Specifies the IP address of the RADIUS server.
• **Authorization Port**	Specifies the UDP port number of the EAPOL control frame.
• **Secret Key String**	It is a string used by the RADIUS server as a password to identify EAPOL control frames.

4.7.5 TACACS+

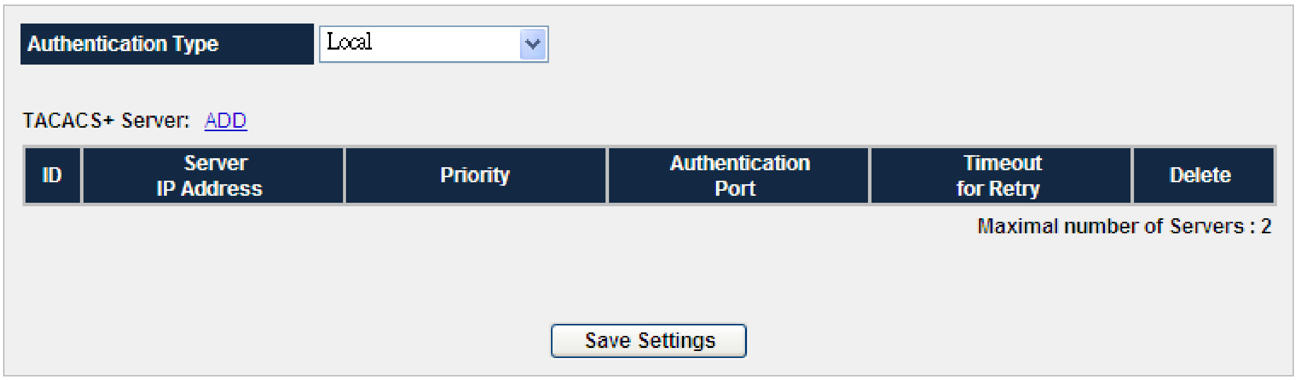
TACACS+ (Terminal Access Controller Access-Control System Plus) is a protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

TACACS+ is based on TACACS, but, in spite of its name, it is an entirely new protocol which is incompatible with any previous version of TACACS. TACACS+ and RADIUS have generally replaced the earlier protocols in more recently built or updated networks, although TACACS and XTACACS are still running on many older systems.

Whereas RADIUS combines authentication and authorization in a user profile, TACACS+ separates the two operations. Another difference is that TACACS+ uses the TCP while RADIUS uses the UDP. Most administrators recommend using TACACS+ because TCP is seen as a more reliable protocol.

The extensions to the TACACS+ protocol provide for more types of authentication requests and more types of response codes than were in the original specification.

The TACACS+ server configuration screen in Figure 4-7-17 appears.



Authentication Type	Local

TACACS+ Server: ADD

ID	Server IP Address	Priority	Authentication Port	Timeout for Retry	Delete

Maximal number of Servers : 2

Figure 4-7-17 TACACS+ server configuration Screenshot

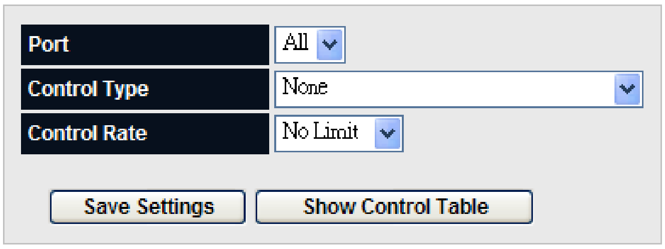
The page includes the following fields:

Object	Description
• **Authentication Type**	**Local** : Local authentication only. **TACACS+** : TACACS+ authentication only. **TACACS+ And Local** : Both enabled. TACACS+ authentication first, if failed, then Local authentication used.
• **Server IP Address**	TACACS+ Server IP address.
• **Priority**	The order in which the TACACS+ servers are used. 0 means highest priority.
• **Key String**	The encryption key for TACACS+. It must match the key used on the TACACS+ server.
• **Authentication Port**	Port number of TACACS+. The default is port **49**.
• **Timeout for Reply**	Time that passes before the connection between the device and the TACACS+ server time out. The field range is **1-120** seconds.

4.7.6 Storm Control

Forwarding broadcast traffic consumes switch resuources, which can negatively impact the forwarding of other traffic. This configuration page is used to protect regular traffic from an overabundance of broadcast or multicast traffic. The system measures the incoming Broadcast and Multicast frame rate separately on each port, and discard frames when the rate exceeds a user-defined rate.

The Storm Control page provides fields for enabling and configuring Storm Control. The screen in Figure 4-7-18 appears.



Port	All
Control Type	None
Control Rate	No Limit

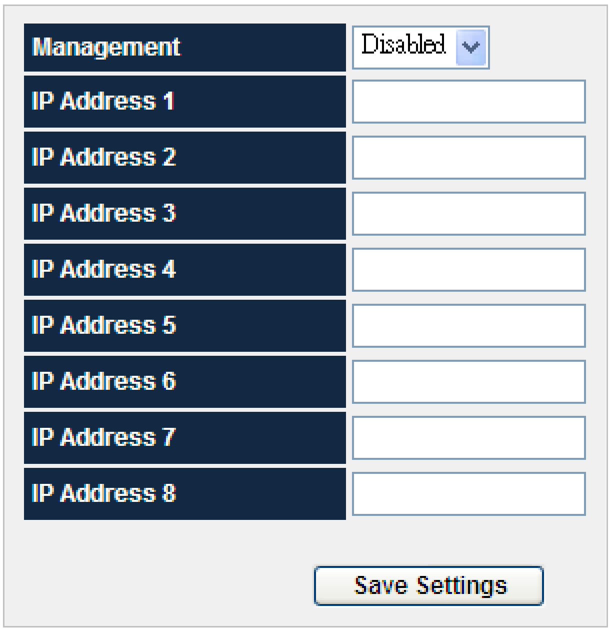
Figure 4-7-18 Storm Control screenshot

The page includes the following fields:

Object	Description
• **Port**	Configure a single port or all ports.
• **Control Type**	By which specifies the Broadcast mode currently enabled on the device. The possible field values are: • **None**: disable storm control function • **Broadcast**: counts only Broadcast traffic. • **Broadcast, Multicast:** counts Broadcast and Multicast traffic together. • **Broadcast**, **Unknown Unicast:** counts Broadcast and unknown unicast traffic. • **Broadcast, Multicast, Unknown Unicast:** counts Unicast, Multicast, and Broadcast traffic.
• **Control Rate**	Specifies a rate for storm control. Where the maximum rate (packets per second) at which unknown packets are forwarded. The available rate as below: • **No Limit** • **64kbps** • **256Kbps** • **1Mbps** • **10Mbps** • **64Mbps** • **100Mbps**

4.7.7 Management IP List

Management IP List specifies the IP addresses which can access the system.



Management	Disabled
IP Address 1	
IP Address 2	
IP Address 3	
IP Address 4	
IP Address 5	
IP Address 6	
IP Address 7	
IP Address 8	

Figure 4-7-19 Management IP List Screenshot

The page includes the following fields:

Object	Description
• **Management**	Enables or disables Management IP List.
• **IP Address (1~8)**	Indicates the IP addresses of the Management IP List.

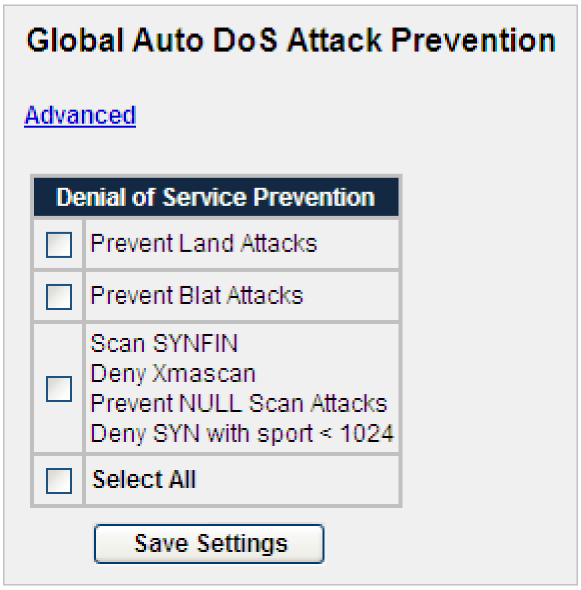
4.7.8 Auto DoS

Getting started with Global Auto DoS Attack Prevention.

Settings apply to all ports.

Denial of Sevice Prevention

Global Auto DoS Attack Prevention



Global Auto DoS Attack Prevention

Advanced

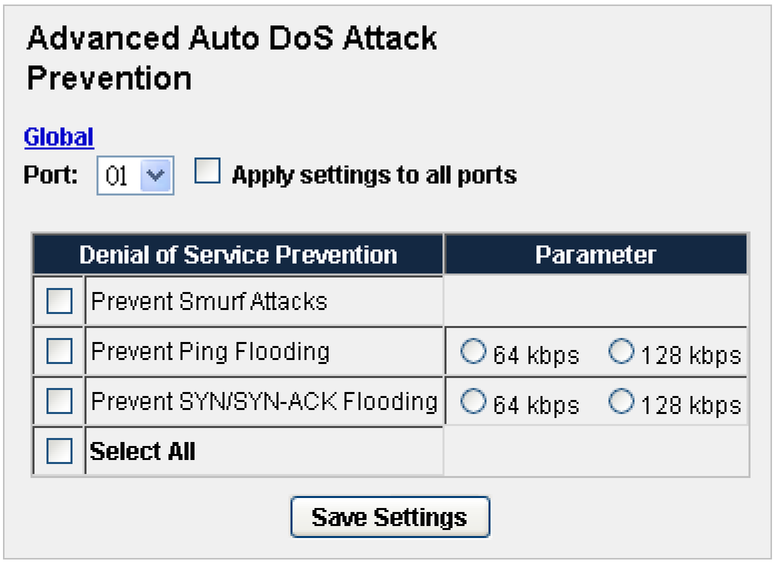
Denial of Service Prevention	
□	Prevent Land Attacks
□	Prevent Blat Attacks
□	Scan SYNFIN Deny Xmascan Prevent NULL Scan Attacks Deny SYN with sport < 1024
□	Select All

Figure 4-7-20 Global Auto DoS Attack Prevention screenshot

The page includes the following fields:

Object	Description
• **Prevent Land Attack**	Packets with Source IP = Destination IP.
• **Prevent Blat Attack**	Packets with Source port = Destination port.
• **SYNFIN**	SYN and FIN bits set in the packets.
• **Xmascan**	Sequence number is zero and the FIN, URG, and PSH bits are set.
• **NULL scan**	TCP sequence number is zero and all control bits are zeroes.
• **SYN with sport < 1024**	SYN packets with source port less than 1024.

Advanced Auto DoS Attack Prevention



Advanced Auto DoS Attack Prevention

Global

Port: 01 □ Apply settings to all ports

	Denial of Service Prevention	Parameter
□	Prevent Smurf Attacks	
□	Prevent Ping Flooding	○ 64 kbps ○ 128 kbps
□	Prevent SYN/SYN-ACK Flooding	○ 64 kbps ○ 128 kbps
□	**Select All**	

Figure 4-7-21 Advanced Auto DoS Attack Prevention screenshot

The page includes the following fields:

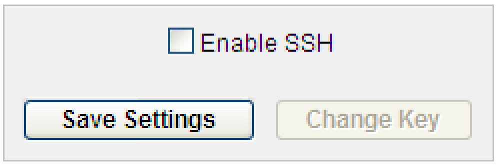
Object	Description
• **Prevent Smurf Attack**	Packets with ICMP from broadcast address
• **Prevent Ping Flooding**	Packets with ICMP
• **Prevent SYN/SYN-ACK Flooding**	Packets with SYN/SYN-ACK

4.7.9 SSH

SSH (secure shell) is a network protocol that allows data to be exchanged using a secure channel between two networked devices. SSH was designed as a replacement for TELNET and other insecure remote shells, which sent information, notably passwords, in plaintext, leaving them open for interception. The encryption used by SSH provides confidentiality and integrity of data over an insecure network, such as the Internet.

SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user, if necessary. SSH is typically used to log into a remote machine and execute commands.

An SSH server, by default, listens on the standard **TCP port 22**.



□ Enable SSH

Figure 4-7-22 SSH page screenshot

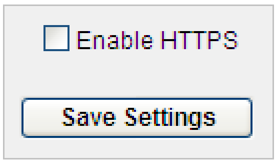
The page includes the following fields:

Object	Description
• **Enable SSH**	Whether or not to activate the SSH daemon inside the switch. Login will be denied if that deamon is inactive.
• **Save Settings**	Save current settings for SSH.
• **Change Key**	Change the public key used for encryption. But please note, that key cannot be changed if any clients are currently connected.

4.7.10 HTTPS

■ **Getting started with HTTPS setting**

Hypertext Transfer Protocol over Secure Socket Layer or HTTPS is a URI scheme used to indicate a secure HTTP connection. It is syntactically identical to the http:// scheme normally used for accessing resources using HTTP. Using an https: URL indicates that HTTP is to be used, but with a different default TCP port (443) and an additional encryption/authentication layer between the HTTP and TCP.



□ Enable HTTPS

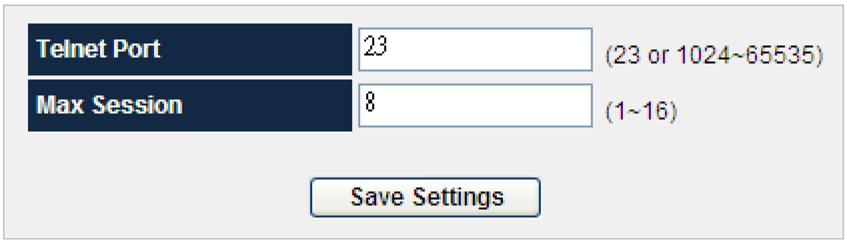
Figure 4-7-23 HTTPs configuration Screenshot

The page includes the following fields:

Object	Description
• **Enable HTTPs**	HTTPS enable Enable HTTPS for security access. HTTPS disable Disable HTTPS.

4.7.11 Telnet

Telnet is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communications facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP).



Telnet Port	23	(23 or 1024~65535)
Max Session	8	(1~16)

Figure 4-7-24 HTTPs configuration Screenshot

The page includes the following fields:

Object	Description
• **Telnet Port**	Port number of telent. The default is port **23**.
• **Max Session**	Max session of telnet. The default is **8** sesions.

4.8 Quality of Service

4.8.1 Understand QoS

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

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

You can use QoS on your system to:

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

■ QoS Terminology

- **Classifier**－classifies the traffic on the network. Traffic classifications are determined by protocol, application, source, destination, and so on. You can create and modify classifications. The Switch then groups classified traffic in order to schedule them with the appropriate service level.
- **DiffServ Code Point (DSCP)** － is the traffic prioritization bits within an IP header that are encoded by certain applications and/or devices to indicate the level of service required by the packet across a network.
- **Service Level**－defines the priority that will be given to a set of classified traffic. You can create and modify service levels.
- **Policy**－comprises a set of "rules" that are applied to a network so that a network meets the needs of the business. That is, traffic can be prioritized across a network according to its importance to that particular business type.
- **QoS Profile**－consists of multiple sets of rules (classifier plus service level combinations). The QoS profile is assigned to a port(s).
- **Rules**－comprises a service level and a classifier to define how theSwitch will treat certain types of traffic. Rules are associated with a QoS Profile (see above).

To implement QoS on your network, you need to carry out the following actions:

1. Define a service level to determine the priority that will be applied to traffic.

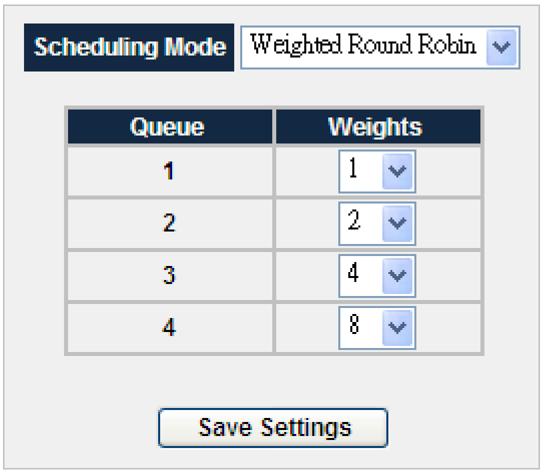
2. Apply a classifier to determine how the incoming traffic will be classified and thus treated by the Managed Switch.

3. Create a QoS profile which associates a service level and a classifier.

4. Apply a QoS profile to a port(s).

4.8.2 Queue Settings

The Queue Setting page contains fields for defining the QoS queue forwarding types. The screen in Figure 4-8-1 appears.



Scheduling Mode: Weighted Round Robin

Queue	Weights
1	1
2	2
3	4
4	8

Figure 4-8-1 Queue Settings screenshot

The page includes the following fields:

Object	Description
• **Scheduling Mode**	There are two available schedule mode: • **Strict Priority**: the packets in the higher queue will always be served first until the queue is empty. • **Weighted Round Robin**: the packets will be served according to the queue weight.
• **Queue**	Indicates priority queues. **Queue 1** is the **lowest** priority queue, and **Queue 4** is the **highest** priority queue.
• **Weight**	Indicates the weight (number of packets) to be served in the queue before moving to serve next queue. A high priority queue should have a higher weight than a low priority queue.

4.8.3 DSCP

TOS/DSCP priority is obtained through a 6-bit **Type-of-Service (TOS)** or **Differentiated Service Code Point (DSCP)** to 3-bit priority mapping.

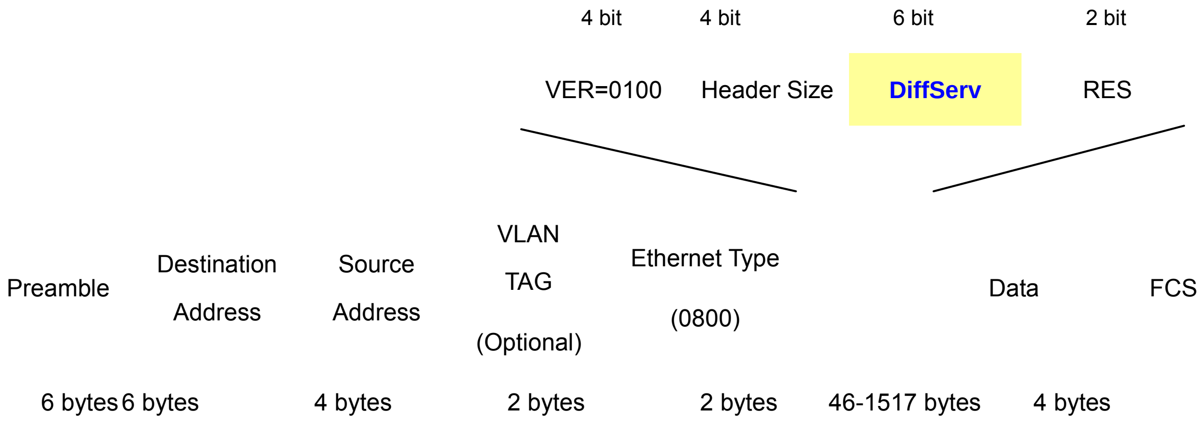
The **Type of Service (TOS)** octet in the IPv4 header is divided into three parts; Precedence (3 bits), TOS (4 bits), and MBZ (1 bit). The Precedence bits indicate the importance of a packet, whereas the TOS bits indicate how the network should make tradeoffs between throughput, delay, reliability, and cost (as defined in RFC 1394). The MBZ bit (for "must be zero") is currently unused and is either set to zero or just ignored.

0	1	2	3	4	5	6	7
Precedence			**TOS**				**MBZ**

IPv4 Packet Header Type of Service Octet

The four TOS bits provide 15 different priority values, however only five values have a defined meaning.

DiffServ Code Point (DSCP) — is the traffic prioritization bits within an IP header that are encoded by certain applications and/or devices to indicate the level of service required by the packet across a network. DSCP are defined in RFC2597 for classifying traffic into different service classes. The Managed Switch extracts the codepoint value of the DS field from IPv4 packets and identifies the priority of the incoming IP packets based on the configured priority.

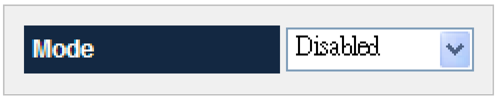


4 bit	4 bit	6 bit	2 bit
VER=0100	Header Size	**DiffServ**	RES

Preamble	Destination Address	Source Address	VLAN TAG (Optional)	Ethernet Type (0800)	Data	FCS
6 bytes	6 bytes	4 bytes	2 bytes	2 bytes	46-1517 bytes	4 bytes

Figure 4-8-2 IPv4 frame format

The DSCP is **six bits** wide, allowing coding for up to 64 different forwarding behaviors. The DSCP retains backward compatibility with the three precedence bits so that non-DSCP compliant, TOS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding.



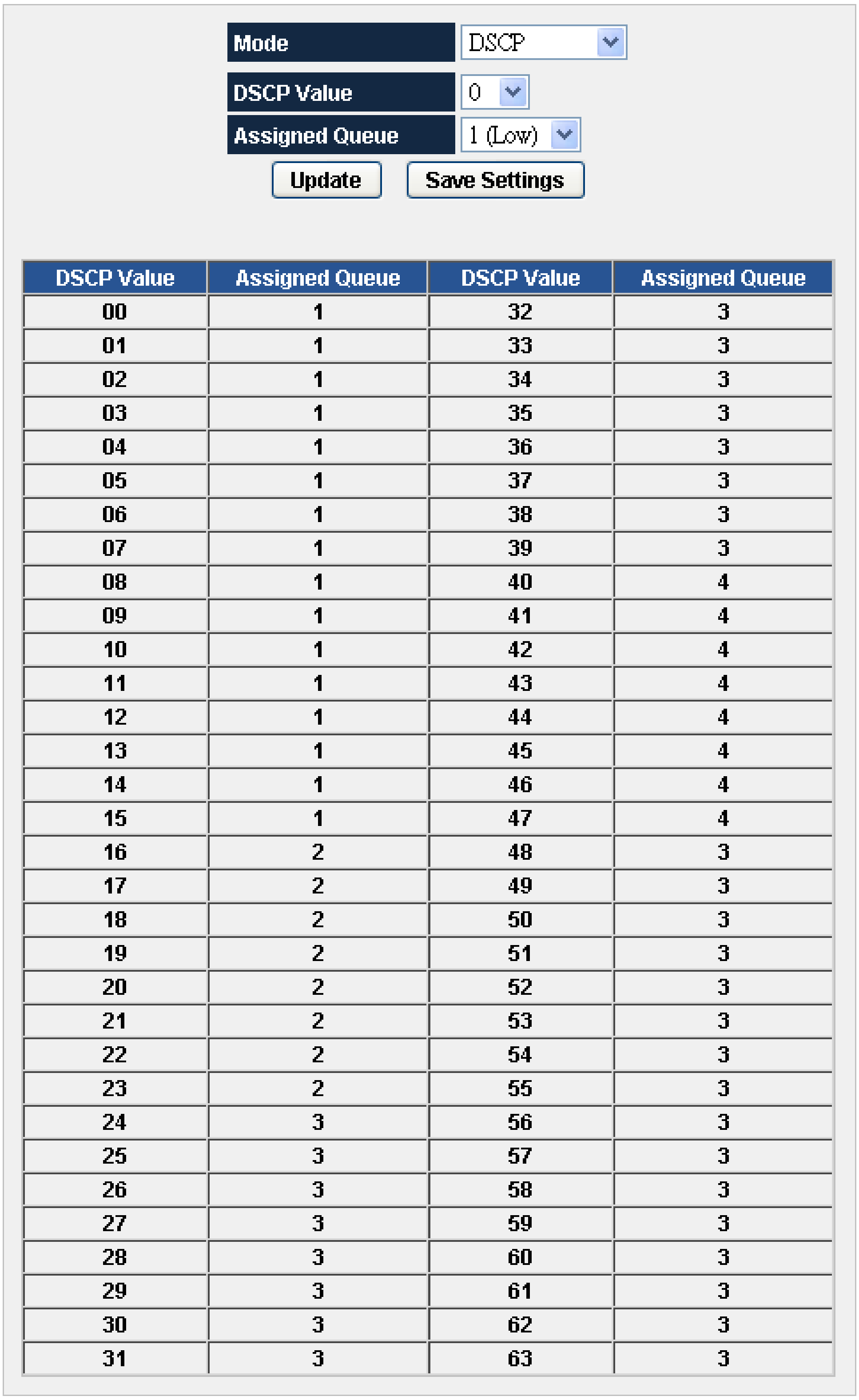
Mode: Disabled

Figure 4-8-3 DSCP configuration page screenshot

The page includes the following fields:

Object	Description
• **Mode**	Specifies the advanced QoS mode to be used. • **Disable** Disables advanced QoS mode on the device. • **DSCP** Specifies trust mode to DSCP on the device. • **IP Precedence** Specifies trust mode to IP Precedence on the device. • **Update** Changes the priority map. (Note, before you click "Save Settings", theses change will not be saved.

- **DSCP mode configuration**

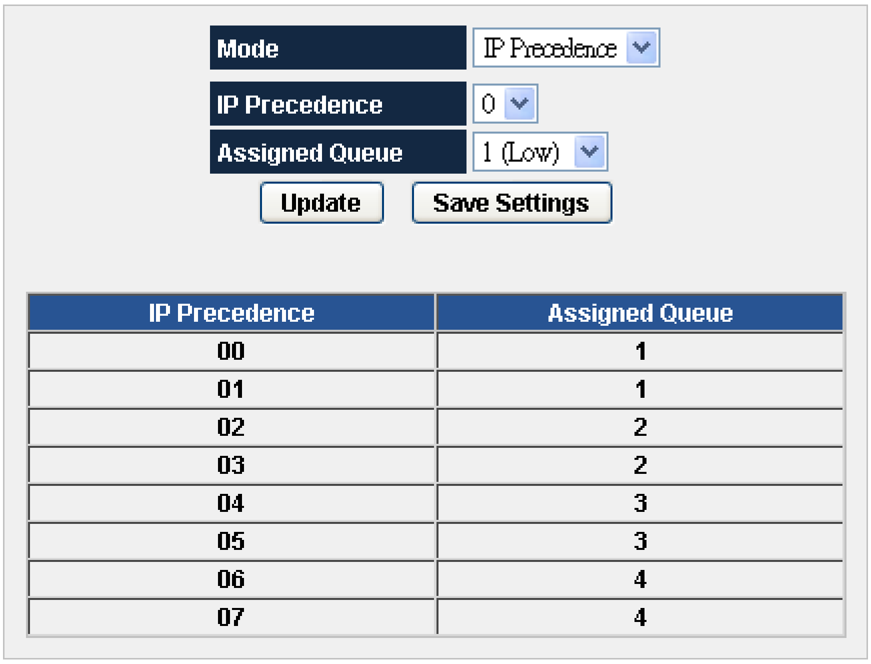


Mode	DSCP
DSCP Value	0
Assigned Queue	1 (Low)

DSCP Value	Assigned Queue	DSCP Value	Assigned Queue
00	1	32	3
01	1	33	3
02	1	34	3
03	1	35	3
04	1	36	3
05	1	37	3
06	1	38	3
07	1	39	3
08	1	40	4
09	1	41	4
10	1	42	4
11	1	43	4
12	1	44	4
13	1	45	4
14	1	46	4
15	1	47	4
16	2	48	3
17	2	49	3
18	2	50	3
19	2	51	3
20	2	52	3
21	2	53	3
22	2	54	3
23	2	55	3
24	3	56	3
25	3	57	3
26	3	58	3
27	3	59	3
28	3	60	3
29	3	61	3
30	3	62	3
31	3	63	3

Figure 4-8-4 DSCP mode configuration page screenshot

- **IP Precedence mode configuration**



Mode	IP Precedence
IP Precedence	0
Assigned Queue	1 (Low)

IP Precedence	Assigned Queue
00	1
01	1
02	2
03	2
04	3
05	3
06	4
07	4

Figure 4-8-5 IP Precedence mode configuration page screenshot

4.8.4 802.1P

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

- ***802.1Q Tag and 802.1p priority***

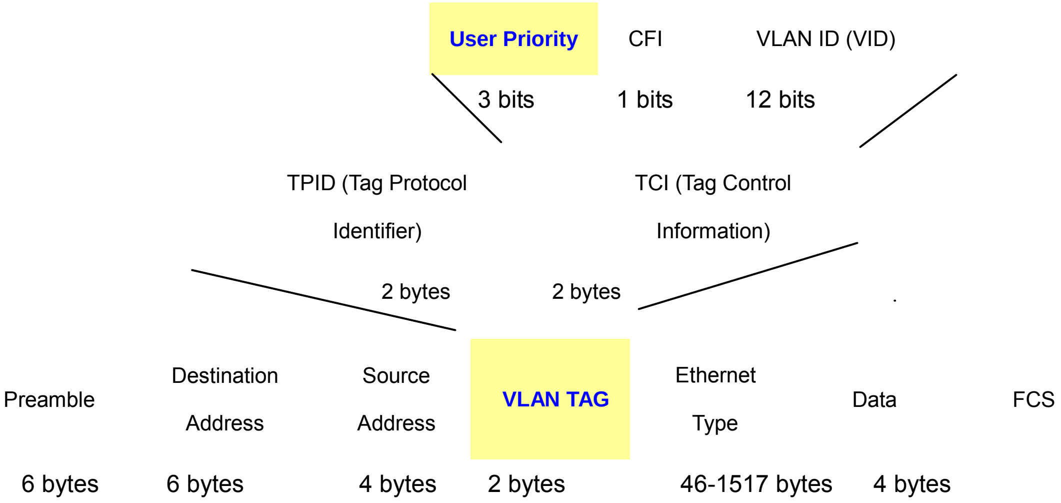


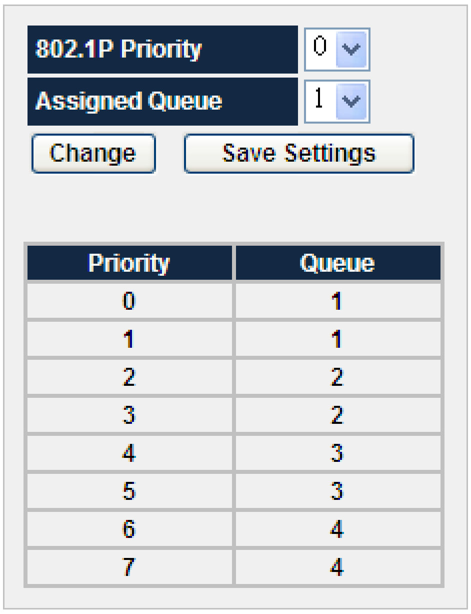
Figure 4-8-6: 802.1p Tag Priority

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

QoS settings allow customization of packet priority in order to facilitate delivery of data traffic that might be affected by latency problems. The IEEE 802.1p Priority specification uses 8 priority levels to classify data packets. In 802.1p compliant devices, a tag inserted into the packet header is used to identify the priority level of data packets.

The Managed Switch supports **Port-based QoS** (Port priority mapping) and **four queues**. The screen in Figure 4-8-7 appears.

802.1P sets the priority relationships between queues and 802.1p priority.



802.1P Priority: 0

Assigned Queue: 1

Priority	Queue
0	1
1	1
2	2
3	2
4	3
5	3
6	4
7	4

Figure 4-8-7 802.1P configuration screenshot

The page includes the following fields:

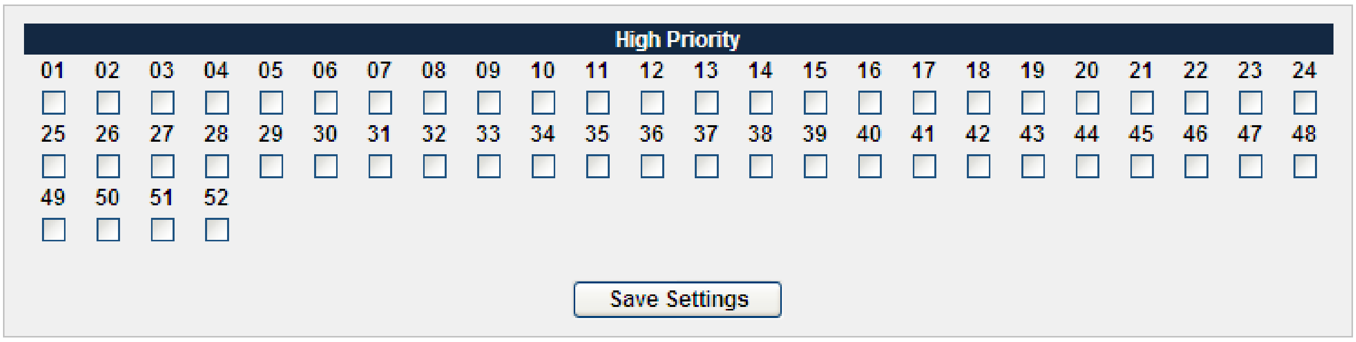
Object	Description
• **802.1P Priority**	This value is retrieved from the priority tag field, with values from **0** to **7**. 0 indicates the lowest priority, 7 indicates the highest priority.
• **Assigned Queue**	Indicates priority queue mapping for 802.1P. There are four priority queues, Queue 1 is the lowest priority queue, and Queue 4 is the highest priority queue.

Note

802.1p Priority: Priority classifiers of the Switch forward packet. COS range is from 0 to 7. Seven is the high class. Zero is the less class. The user may configure the mapping between COS and Traffic classifiers.

4.8.5 Port-Based QoS

When Port-Based priority is applied, any packets received from a high priority port will be treated as a high priority packet. Select the QoS mode to Port-Based Priority, the Port ID to queue mapping configuration page appears, as the Figure 4-8-8 shows.



High Priority

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
49	50	51	52																				
□	□	□	□																				

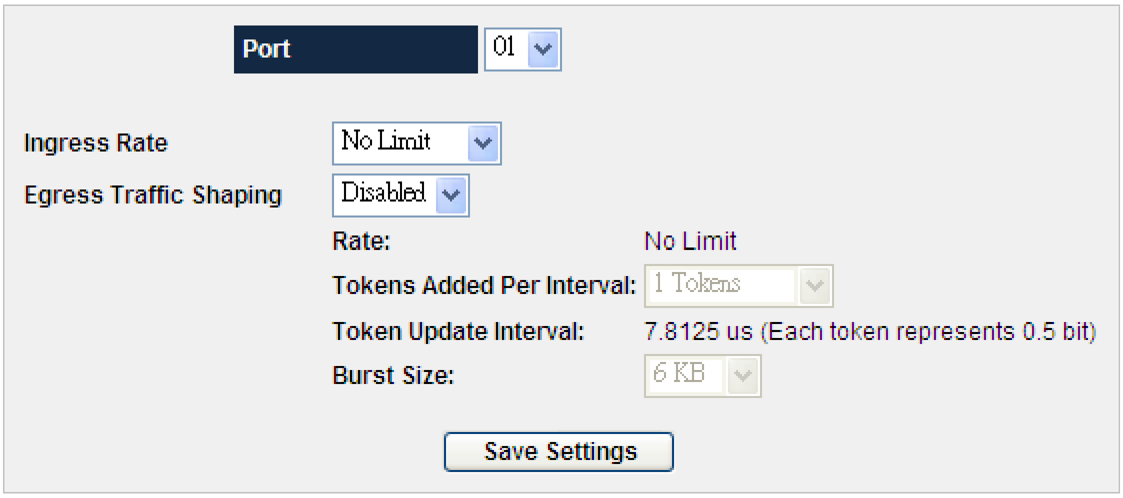
Figure 4-8-8 Port-Base QoS configuration screenshot

The page includes the following fields:

Object	Description
• **Port**	Specifies the high priority port members.
• **Save Settings**	Means program these changes to database.

4.8.6 Rate Control

Configure the switch port rate limit for Policers and Shapers on this page. The settings relate to the Managed Switch, as reflected by the page header. The screen Rate Control in Figure 4-8-9 appears.



Port: 01

Ingress Rate: No Limit

Egress Traffic Shaping: Disabled

Rate: No Limit

Tokens Added Per Interval: 1 Tokens

Token Update Interval: 7.8125 us (Each token represents 0.5 bit)

Burst Size: 6 KB

Figure 4-8-9 Rate Control configuration screenshot

The page includes the following fields:

Object	Description
- **Port**	Selects a port to configure.
- **Ingress Rate**	Selects a rate for incoming traffic. The selectable values are **64kbps / 128kbps / 256kbps ~ 100Mbps** for each Fast Ethernet port. The selectable values are **64kbps / 128kbps / 256kbps ~ 1Gbps** for each Gigabit port.
- **Egress Traffic Shaping**	Egress Traffic Shaping is an attempt to control network traffic in order to optimize or guarantee performance, low-latency, and/or bandwidth. - **Rate:** displays the rate for egress traffic. And it's value comes from tokens. - **Tokens Added Per Interval:** means tokens will be added to the token bucket in "token update interval" - **Token Update Interval:** is 7.8125 us. And each token represents 0.5 bit. - **Burst Size:** selects the size of burst.

4.9 SNMP

4.9.1 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.

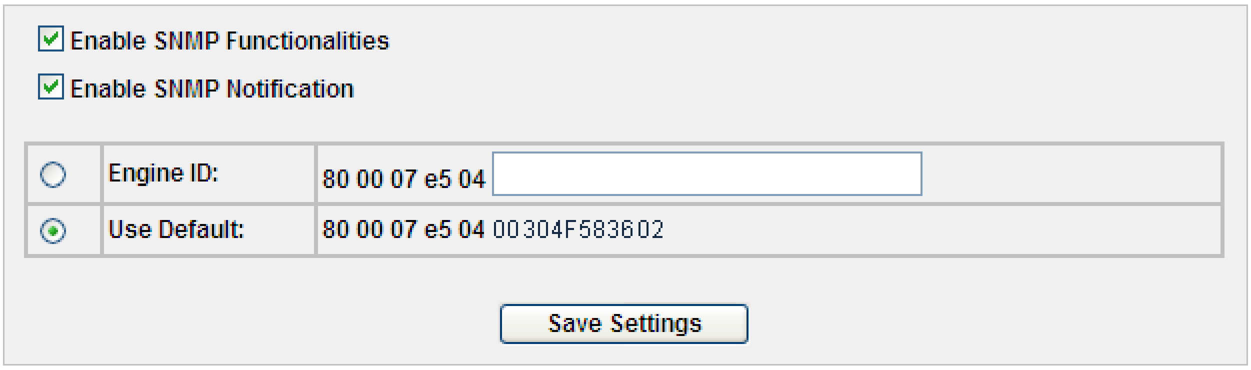
SNMP community

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

4.9.2 SNMP

Configure SNMP on this page. The SNMP System Configuration screen in Figure 4-9-1 appears.



☑ Enable SNMP Functionalities

☑ Enable SNMP Notification

○	Engine ID:	80 00 07 e5 04
●	Use Default:	80 00 07 e5 04 00304F583602

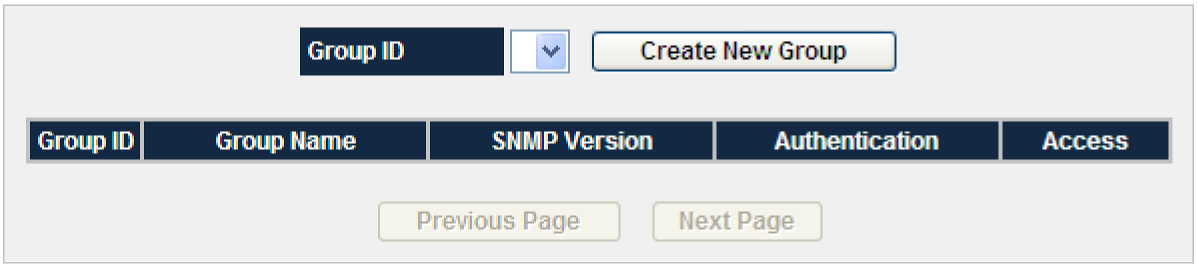
Figure 4-9-1 SNMP configuration screenshot

The page includes the following fields:

Object	Description
• **Enable SNMP Functionalities**	Enables or Disables SNMP function on this device.
• **Enable SNMP Notification**	Enables or Disables SNMP notification function on this device.
• **Engine ID**	Configures the Engine ID on this device. The field value is a hexadecimal string. Each byte in hexadecimal character strings consists of two hexadecimal digits. Each byte can be separated by a period or a colon. The Engine ID must be defined before SNMPv3 is enabled. For stand-alone devices, select a default Engine ID that is comprised of Enterprise number and the default MAC address.
• **Use Default**	Uses the device generated Engine ID. It's defined per standard as: First 4 octets — first bit = 1, the rest is IANA Enterprise number. To locate the IANA Enterprise number by referring to the Vendor website, or use the show SNMP

4.9.3 Group Profile

The Group Profile screen provides information for creating SNMP groups and assigning SNMP access control privileges to SNMP groups. Groups allow network managers to assign access rights to specific device features, or features aspects. The SNMP Groups Configuration screen in Figure 4-9-2 appears.



Group ID	Group Name	SNMP Version	Authentication	Access

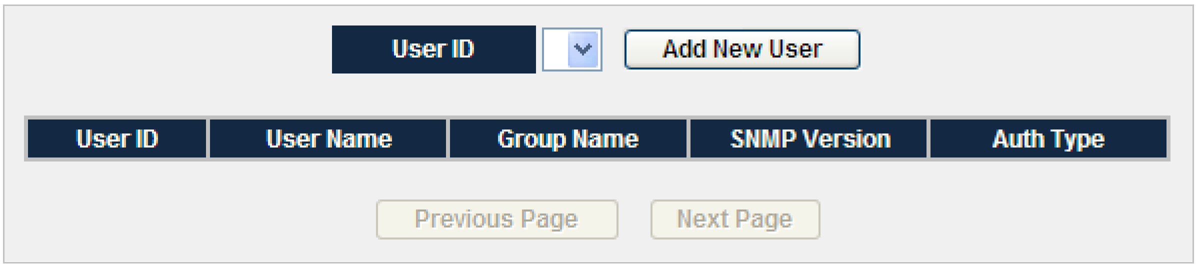
Figure 4-9-2 Group Profile Screenshot

The page includes the following fields:

Object	Description
• **Group ID**	Click on Group ID to edit or remove group.
• **Group Name**	Indicates the name of the group which access control rules are applied. The field range is up to 32 characters.
• **SNMP Version**	Indicates the SNMP version of the group. The Possible versions are: • **SNMP v1**: Set SNMP supported version 1. • **SNMP v2c**: Set SNMP supported version 2c. • **SNMP v3**: Set SNMP supported version 3.
• **Authentication**	Defines the security level attached to the group. Security levels apply to **SNMPv3 only**. The possible field values are: • **Disable (No Authentication)**, which indicates that neither the Authentication nor the Privacy security levels are assigned to the group. • **Enable (Authentication)**, which authenticates SNMP messages, and ensures the SNMP messages original is authenticated.
• **Access**	Defines the group access rights. The possible field values are: • **Read Enable**: The management access is restricted to read-only, and changes cannot be made to the assigned SNMP view. • **Write Enable**: The management access is read-write and changes can be made to the assigned SNMP view. • **Disable**: Sends traps for the assigned SNMP view.
• **Add New Group**	Add a new SNMP group.

4.9.4 User Profile

Configure SNMPv3 users table on this page. The entry index key are Engine ID and User Name. The SNMPv3 Users Configuration screen in Figure 4-9-3 appears.



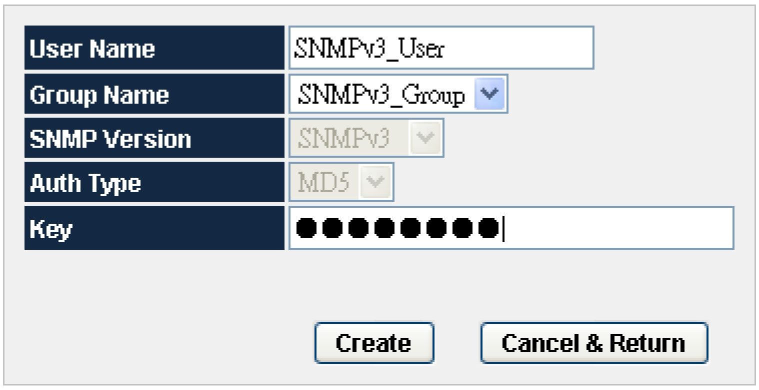
User ID	User Name	Group Name	SNMP Version	Auth Type

Figure 4-9-3 User Profile Screenshot

The page includes the following fields:

Object	Description
• **User ID**	Click on User ID to edit or remove user.
• **User Name**	Indicates the name of the user. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
• **Group Name**	Indicates which group the user belongs to. SNMP groups are defined in the SNMP **Group Profile** page.
• **SNMP Version**	Indicates the SNMP version of the user.
• **Auth Type**	Indicates the security model that this entry should belong to. Possible security models are: • **None**: None authentication protocol. • **MD5**: An optional flag to indicate that this user using MD5 authentication protocol. The value of security level cannot be modified if entry already exist. That means must first ensure that the value is set correctly.
• **Add New User**	Creates a SNMP user.

- **Add New User**



User Name	SNMPv3_User
Group Name	SNMPv3_Group
SNMP Version	SNMPv3
Auth Type	MD5
Key	●●●●●●●●●

Figure 4-9-4 Add new user screenshot

The page includes the following fields:

Object	Description
• **Delete**	Check to delete the entry. It will be deleted during the next save.
• **User Name**	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
• **Group Name**	Contains a list of user-defined SNMP groups. SNMP groups are defined in the SNMP **Group Profile** page.
• **SNMP Version**	Indicates the SNMP version of the user.

- **Authentication Type** Indicates the authentication protocol that this entry should belong to. Possible authentication protocol are:
  - **None**: None authentication protocol.
  - **MD5**: An optional flag to indicate that this user using MD5 authentication protocol.

  The value of security level cannot be modified if entry already exist. That means must first ensure that the value is set correctly.

- **Key** A string identifying the authentication pass phrase.

  For MD5 authentication protocol, the allowed string length is 8 to 32. The allowed content is the ASCII characters from 33 to 126.

- **Privacy Protocol** Indicates the privacy protocol that this entry should belong to. Possible privacy protocol are:
  - **None**: None privacy protocol.
  - **DES**: An optional flag to indicate that this user using DES authentication protocol.

- **Privacy Password** A string identifying the privacy pass phrase. The allowed string length is 8 to 32, and the allowed content is the ASCII characters from 33 to 126.

4.9.5 Community Profile

Configure SNMP communities table on this page. The entry index key is Community. The SNMP Communities Configuration screen in Figure 4-9-5 and Figure 4-9-6 appears.

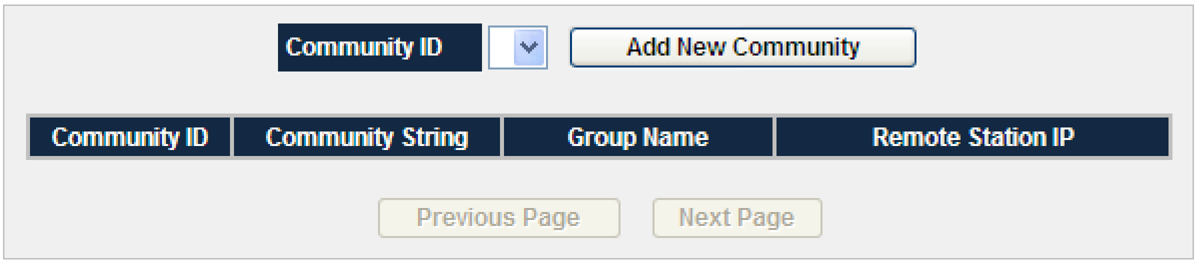
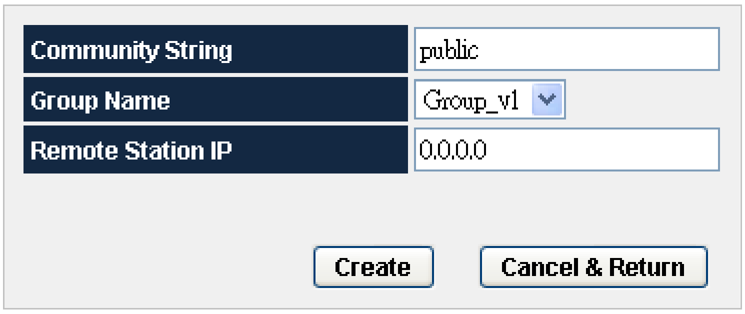


Figure 4-9-5 SNMP Community Profile Screenshot



Community String	public
Group Name	Group_v1
Remote Station IP	0.0.0.0

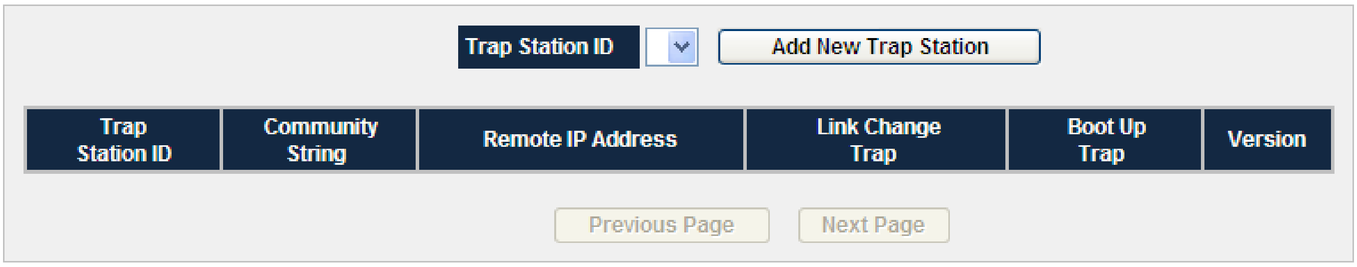
Figure 4-9-6 SNMP Community Profile Screenshot

The page includes the following fields:

Object	Description
• **Community ID**	Click on Community ID to edit or remove community.
• **Community String**	Indicates the community string. It just like to defines the password used to authenticate the management station to the device.
• **Group Name**	Indicates the group which the community belongs to. SNMP groups are defined in the SNMP **Group Profile** page.
• **Remote Station IP**	Indicates the management station IP address. There are two definition options: • **IP Address -** Define the management station IP address. • **0.0.0.0** - which includes **all** management station IP addresses.
• **Add New Community**	Creates a community.

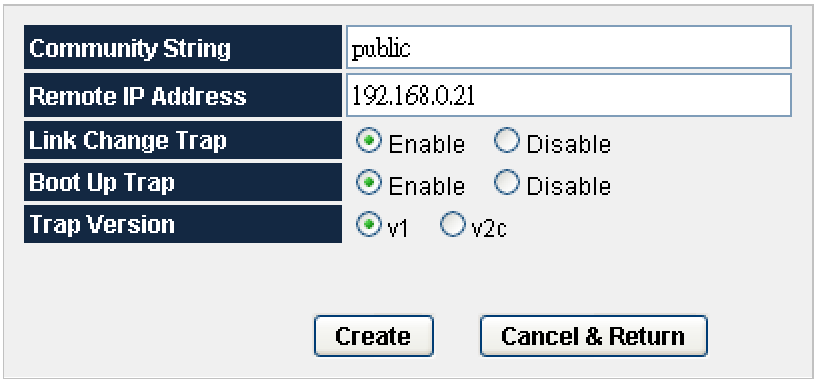
4.9.6 SNMP Trap Station

Configure SNMP trap on this page. The SNMP Trap Configuration screen in Figure 4-9-7 and Figure 4-9-8 appears.



Trap Station ID	Community String	Remote IP Address	Link Change Trap	Boot Up Trap	Version

Figure 4-9-7 SNMP Trap Station Screenshot



Community String	public
Remote IP Address	192.168.0.21
Link Change Trap	● Enable ○ Disable
Boot Up Trap	● Enable ○ Disable
Trap Version	● v1 ○ v2c

Figure 4-9-8 Add new SNMP Trap Station Screenshot

The page includes the following fields:

Object	Description
• **Trap Station ID**	Click on Trap Station ID to edit or remove trap station.
• **Community String**	Indicates the community string for this trap station.
• **Link Change Trap**	Indicates if link up and link down traps are sent.
• **Remote IP Address**	Indicates the IP address which traps are sent.
• **Boot Up Trap**	Indicates if WarmStart and ColdStart traps are sent.
• **Version**	Indicates the SNMP version of the trap station.
• **Add New Trap Station**	Creates a trap station.

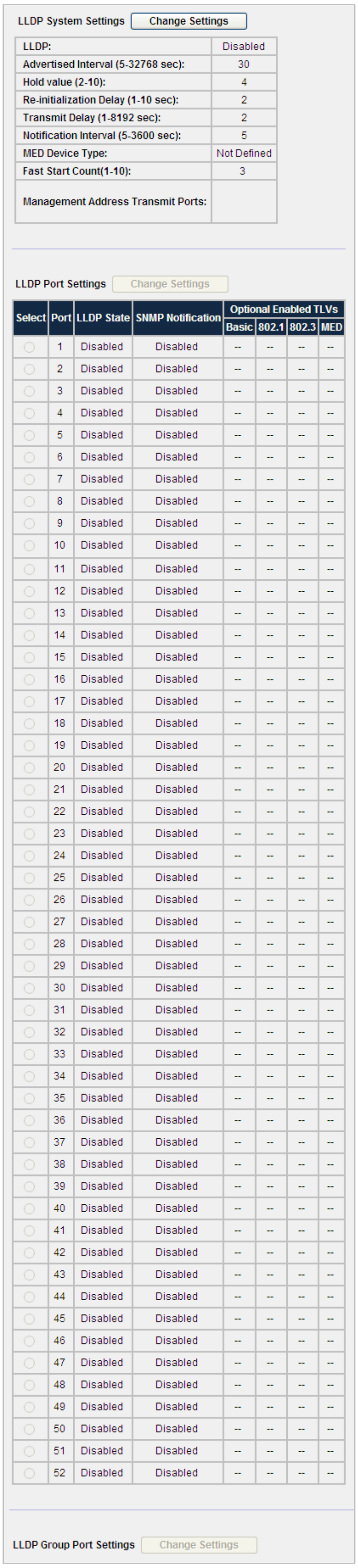
4.10 LLDP

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in **Type Length Value (TLV)** format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power, inventory, and device location details. LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

4.10.1 LLDP Settings

This page allows the user to inspect and configure the current LLDP port settings. The LLDP settings screen in Figure 4-10-1 appears.



LLDP System Settings

LLDP:	Disabled
Advertised Interval (5-32768 sec):	30
Hold value (2-10):	4
Re-initialization Delay (1-10 sec):	2
Transmit Delay (1-8192 sec):	2
Notification Interval (5-3600 sec):	5
MED Device Type:	Not Defined
Fast Start Count(1-10):	3
Management Address Transmit Ports:	

LLDP Port Settings

Select	Port	LLDP State	SNMP Notification	Optional Enabled TLVs			
				Basic	802.1	802.3	MED
○	1	Disabled	Disabled	--	--	--	--
○	2	Disabled	Disabled	--	--	--	--
○	3	Disabled	Disabled	--	--	--	--
○	4	Disabled	Disabled	--	--	--	--
○	5	Disabled	Disabled	--	--	--	--
○	6	Disabled	Disabled	--	--	--	--
○	7	Disabled	Disabled	--	--	--	--
○	8	Disabled	Disabled	--	--	--	--
○	9	Disabled	Disabled	--	--	--	--
○	10	Disabled	Disabled	--	--	--	--
○	11	Disabled	Disabled	--	--	--	--
○	12	Disabled	Disabled	--	--	--	--
○	13	Disabled	Disabled	--	--	--	--
○	14	Disabled	Disabled	--	--	--	--
○	15	Disabled	Disabled	--	--	--	--
○	16	Disabled	Disabled	--	--	--	--
○	17	Disabled	Disabled	--	--	--	--
○	18	Disabled	Disabled	--	--	--	--
○	19	Disabled	Disabled	--	--	--	--
○	20	Disabled	Disabled	--	--	--	--
○	21	Disabled	Disabled	--	--	--	--
○	22	Disabled	Disabled	--	--	--	--
○	23	Disabled	Disabled	--	--	--	--
○	24	Disabled	Disabled	--	--	--	--
○	25	Disabled	Disabled	--	--	--	--
○	26	Disabled	Disabled	--	--	--	--
○	27	Disabled	Disabled	--	--	--	--
○	28	Disabled	Disabled	--	--	--	--
○	29	Disabled	Disabled	--	--	--	--
○	30	Disabled	Disabled	--	--	--	--
○	31	Disabled	Disabled	--	--	--	--
○	32	Disabled	Disabled	--	--	--	--
○	33	Disabled	Disabled	--	--	--	--
○	34	Disabled	Disabled	--	--	--	--
○	35	Disabled	Disabled	--	--	--	--
○	36	Disabled	Disabled	--	--	--	--
○	37	Disabled	Disabled	--	--	--	--
○	38	Disabled	Disabled	--	--	--	--
○	39	Disabled	Disabled	--	--	--	--
○	40	Disabled	Disabled	--	--	--	--
○	41	Disabled	Disabled	--	--	--	--
○	42	Disabled	Disabled	--	--	--	--
○	43	Disabled	Disabled	--	--	--	--
○	44	Disabled	Disabled	--	--	--	--
○	45	Disabled	Disabled	--	--	--	--
○	46	Disabled	Disabled	--	--	--	--
○	47	Disabled	Disabled	--	--	--	--
○	48	Disabled	Disabled	--	--	--	--
○	49	Disabled	Disabled	--	--	--	--
○	50	Disabled	Disabled	--	--	--	--
○	51	Disabled	Disabled	--	--	--	--
○	52	Disabled	Disabled	--	--	--	--

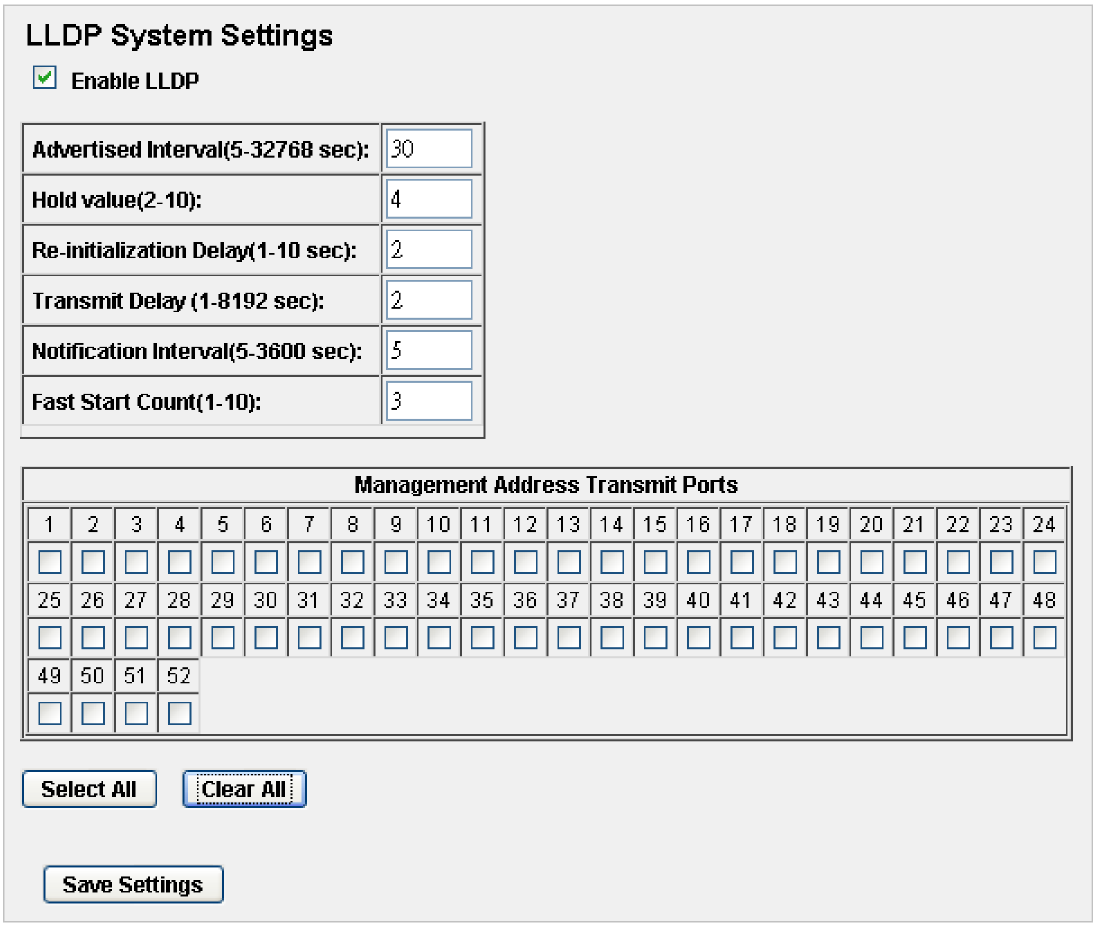
LLDP Group Port Settings

Figure 4-10-1 LLDP Settings screenshot

The page includes the following fields:

Object	Description
• **Advertised Interval**	The interval at which LLDP frames are transmitted on behalf of this LLDP agent.
• **Hold value**	A multiplier to Advertised interval. The result would be the TTL value for the information advertised.
• **Re-initialization delay**	The minimum delay period before from the time a ports becomes disabled until re-initialization.
• **Transmit Delay**	The delay between successive LLDP frame transmissions initiated by value/status changes in the local system
• **Notification Interval**	The interval at which notification are generated when remote MSAP information changes.
• **MED Device Type**	Display the information included in the MED TLV field of advertised messages.
• **Fast Start Type**	Indicates the number of fast start LLDP MED PDUs that are sent when a LLDP MED Peer is detected.
• **Management Address Transmit Ports**	Indicates the ports on which the management address will be transmitted.

■ **Enable LLDP function**



LLDP System Settings

☑ Enable LLDP

Advertised Interval(5-32768 sec):	30
Hold value(2-10):	4
Re-initialization Delay(1-10 sec):	2
Transmit Delay (1-8192 sec):	2
Notification Interval(5-3600 sec):	5
Fast Start Count(1-10):	3

Management Address Transmit Ports

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
49	50	51	52																				
□	□	□	□																				

Figure 4-10-2 LLDP System Settings screenshot

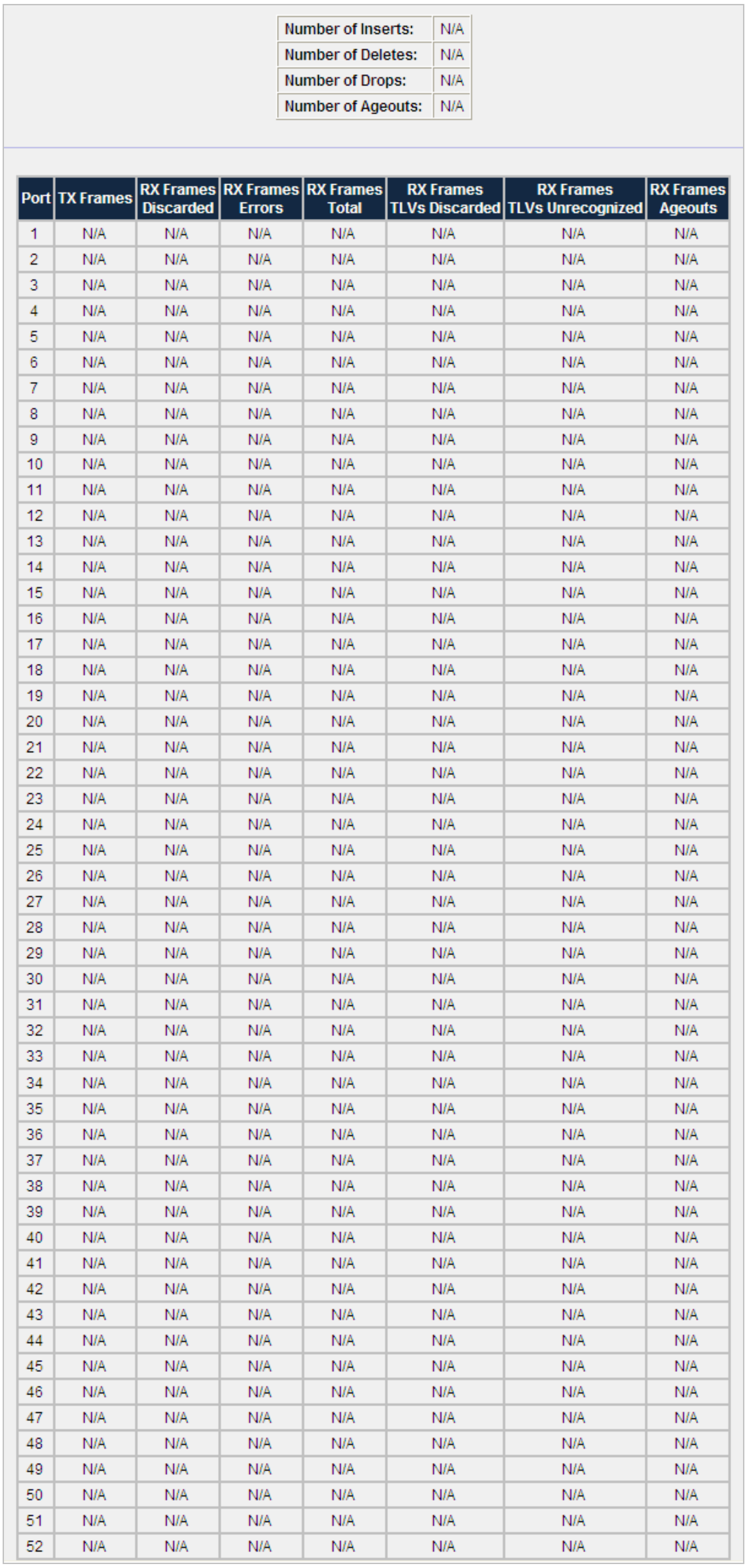
The page includes the following fields:

Object	Description
• **Enable LLDP**	Enables LLDP globally on the switch.
• **Advertised Interval (5-32768 sec)**	Configures the periodic transmit interval for LLDP advertisements. Range: 5-32768seconds; Default: **30** seconds This attribute must comply with the following rule: (Transmission Interval * Hold Time Multiplier) ≤65536, and Transmission Interval >= (4 * Delay Interval)
• **Hold Value (2-10)**	Configures the **time-to-live (TTL)** value sent in LLDP advertisements as shown in the formula below. Range: 2-10; Default: **4** The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner. TTL in seconds is based on the following rule: (Transmission Interval * Holdtime Multiplier) ≤ 65536. Therefore, the default TTL is 4*30 = 120 seconds.
• **Re-initialization Delay (1-10 sec)**	Configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down. Range: 1-10 seconds; Default: **2** seconds When LLDP is re-initialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.
• **Transmit Delay (1-8192 sec)**	Configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. Range: 1-8192 seconds; Default: **2** seconds The transmit delay is used to prevent a series of successive LLDP transmissions during a short period of rapid changes in local LLDP MIB objects, and to increase the probability that multiple, rather than single changes, are reported in each transmission. This attribute must comply with the rule: (4 * Delay Interval) ≤Transmission Interval
• **Notification Interval**	Configures the allowed interval for sending SNMP notifications about LLDP MIB changes.

(5-3600 sec)	Range: 5-3600 seconds; Default: **5** seconds This parameter only applies to SNMP applications which use data stored in the LLDP MIB for network monitoring or management. Information about changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.
• **Fast Start Count (1-10)**	Configures the amount of LLDP MED Fast Start LLDPDUs to transmit during the activation process of the LLDP-MED Fast Start mechanisim. Range: 1-10 packets; Default: **4** packets The MED Fast Start Count parameter is part of the timer which ensures that the LLDP-MED Fast Start mechanism is active for the port. LLDP-MED Fast Start is critical to the timely startup of LLDP, and therefore integral to the rapid availability of Emergency Call Service.
• **Management Address Transmit Ports**	Specifies the LLDP port members.

4.10.2 LLDP Statistics

This page provides an overview of all LLDP traffic. Two types of counters are shown. Global counters are counters that refer to the Managed Switch, while local counters refers to counters for the currently selected switch. The LLDP Statistics screen in Figure 4-10-3 appears.



Number of Inserts:	N/A
Number of Deletes:	N/A
Number of Drops:	N/A
Number of Ageouts:	N/A

Port	TX Frames	RX Frames Discarded	RX Frames Errors	RX Frames Total	RX Frames TLVs Discarded	RX Frames TLVs Unrecognized	RX Frames Ageouts
1	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2	N/A	N/A	N/A	N/A	N/A	N/A	N/A
3	N/A	N/A	N/A	N/A	N/A	N/A	N/A
4	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5	N/A	N/A	N/A	N/A	N/A	N/A	N/A
6	N/A	N/A	N/A	N/A	N/A	N/A	N/A
7	N/A	N/A	N/A	N/A	N/A	N/A	N/A
8	N/A	N/A	N/A	N/A	N/A	N/A	N/A
9	N/A	N/A	N/A	N/A	N/A	N/A	N/A
10	N/A	N/A	N/A	N/A	N/A	N/A	N/A
11	N/A	N/A	N/A	N/A	N/A	N/A	N/A
12	N/A	N/A	N/A	N/A	N/A	N/A	N/A
13	N/A	N/A	N/A	N/A	N/A	N/A	N/A
14	N/A	N/A	N/A	N/A	N/A	N/A	N/A
15	N/A	N/A	N/A	N/A	N/A	N/A	N/A
16	N/A	N/A	N/A	N/A	N/A	N/A	N/A
17	N/A	N/A	N/A	N/A	N/A	N/A	N/A
18	N/A	N/A	N/A	N/A	N/A	N/A	N/A
19	N/A	N/A	N/A	N/A	N/A	N/A	N/A
20	N/A	N/A	N/A	N/A	N/A	N/A	N/A
21	N/A	N/A	N/A	N/A	N/A	N/A	N/A
22	N/A	N/A	N/A	N/A	N/A	N/A	N/A
23	N/A	N/A	N/A	N/A	N/A	N/A	N/A
24	N/A	N/A	N/A	N/A	N/A	N/A	N/A
25	N/A	N/A	N/A	N/A	N/A	N/A	N/A
26	N/A	N/A	N/A	N/A	N/A	N/A	N/A
27	N/A	N/A	N/A	N/A	N/A	N/A	N/A
28	N/A	N/A	N/A	N/A	N/A	N/A	N/A
29	N/A	N/A	N/A	N/A	N/A	N/A	N/A
30	N/A	N/A	N/A	N/A	N/A	N/A	N/A
31	N/A	N/A	N/A	N/A	N/A	N/A	N/A
32	N/A	N/A	N/A	N/A	N/A	N/A	N/A
33	N/A	N/A	N/A	N/A	N/A	N/A	N/A
34	N/A	N/A	N/A	N/A	N/A	N/A	N/A
35	N/A	N/A	N/A	N/A	N/A	N/A	N/A
36	N/A	N/A	N/A	N/A	N/A	N/A	N/A
37	N/A	N/A	N/A	N/A	N/A	N/A	N/A
38	N/A	N/A	N/A	N/A	N/A	N/A	N/A
39	N/A	N/A	N/A	N/A	N/A	N/A	N/A
40	N/A	N/A	N/A	N/A	N/A	N/A	N/A
41	N/A	N/A	N/A	N/A	N/A	N/A	N/A
42	N/A	N/A	N/A	N/A	N/A	N/A	N/A
43	N/A	N/A	N/A	N/A	N/A	N/A	N/A
44	N/A	N/A	N/A	N/A	N/A	N/A	N/A
45	N/A	N/A	N/A	N/A	N/A	N/A	N/A
46	N/A	N/A	N/A	N/A	N/A	N/A	N/A
47	N/A	N/A	N/A	N/A	N/A	N/A	N/A
48	N/A	N/A	N/A	N/A	N/A	N/A	N/A
49	N/A	N/A	N/A	N/A	N/A	N/A	N/A
50	N/A	N/A	N/A	N/A	N/A	N/A	N/A
51	N/A	N/A	N/A	N/A	N/A	N/A	N/A
52	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Figure 4-10-3 LLDP Statistics Screenshot

- **Global Counters**

Object	Description
• **Number of Inserts:**	Shows the number of new entries added since switch reboot.
• **Number of Deletes:**	Shows the number of new entries deleted since switch reboot.
• **Number of Drops:**	Shows the number of LLDP frames dropped due to that the entry table was full.
• **Number of Ageouts:**	Shows the number of entries deleted due to Time-To-Live expiring.

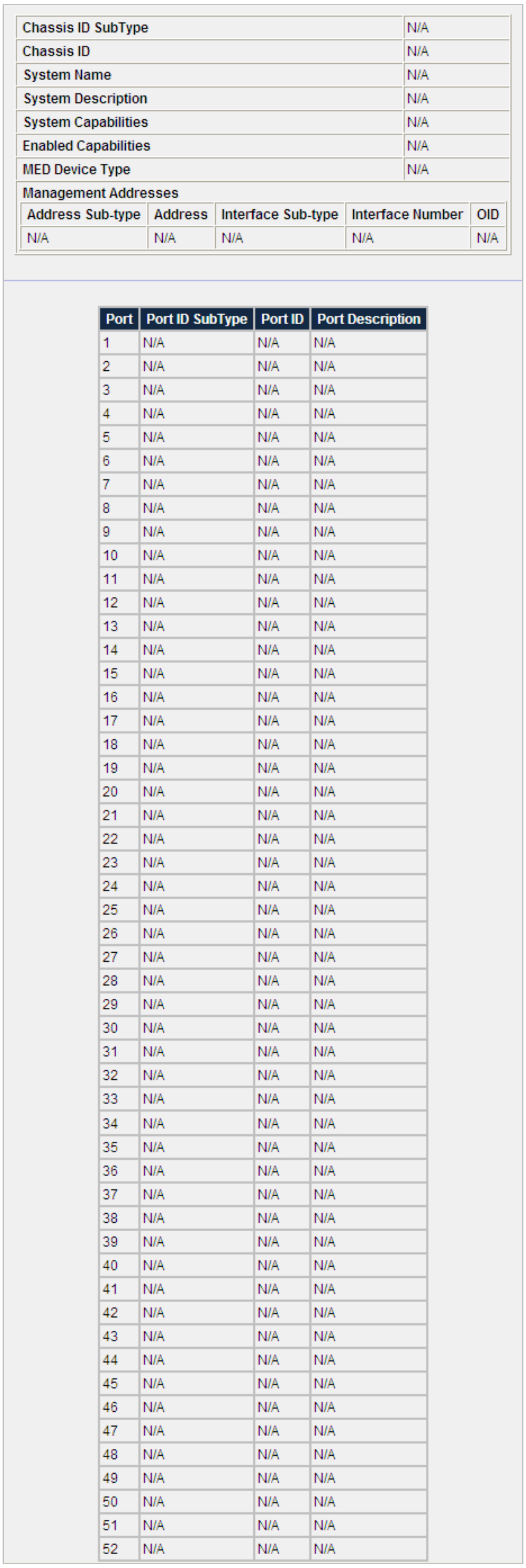
- **Local Counters**

The displayed table contains a row for each port. The columns hold the following information:

Object	Description
• **Port**	The port on which LLDP frames are received or transmitted.
• **Tx Frames**	The number of LLDP frames transmitted on the port.
• **RX Frames Discarded**	If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port links down, an LLDP shutdown frame is received, or when the entry ages out.
• **Rx Frame Errors**	The number of received LLDP frames containing some kind of error.
• **Rx Frames Total**	The number of LLDP frames received on the port.
• **Rx Frames TLVs Discarded**	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
• **Rx Frames TLVs Unrecognized**	The number of well-formed TLVs, but with an unknown type value.
• **Rx Frames Ageouts**	Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the **Age-Out** counter is incremented.

4.10.3 Local Information

Use the LLDP Local Information screen to display information about the Managed Switch, such as its **MAC address**, **chassis ID**, **system capabilities**, **system description**, **management IP address**, and **port information**.



Chassis ID SubType	N/A
Chassis ID	N/A
System Name	N/A
System Description	N/A
System Capabilities	N/A
Enabled Capabilities	N/A
MED Device Type	N/A

Management Addresses

Address Sub-type	Address	Interface Sub-type	Interface Number	OID
N/A	N/A	N/A	N/A	N/A

Port	Port ID SubType	Port ID	Port Description
1	N/A	N/A	N/A
2	N/A	N/A	N/A
3	N/A	N/A	N/A
4	N/A	N/A	N/A
5	N/A	N/A	N/A
6	N/A	N/A	N/A
7	N/A	N/A	N/A
8	N/A	N/A	N/A
9	N/A	N/A	N/A
10	N/A	N/A	N/A
11	N/A	N/A	N/A
12	N/A	N/A	N/A
13	N/A	N/A	N/A
14	N/A	N/A	N/A
15	N/A	N/A	N/A
16	N/A	N/A	N/A
17	N/A	N/A	N/A
18	N/A	N/A	N/A
19	N/A	N/A	N/A
20	N/A	N/A	N/A
21	N/A	N/A	N/A
22	N/A	N/A	N/A
23	N/A	N/A	N/A
24	N/A	N/A	N/A
25	N/A	N/A	N/A
26	N/A	N/A	N/A
27	N/A	N/A	N/A
28	N/A	N/A	N/A
29	N/A	N/A	N/A
30	N/A	N/A	N/A
31	N/A	N/A	N/A
32	N/A	N/A	N/A
33	N/A	N/A	N/A
34	N/A	N/A	N/A
35	N/A	N/A	N/A
36	N/A	N/A	N/A
37	N/A	N/A	N/A
38	N/A	N/A	N/A
39	N/A	N/A	N/A
40	N/A	N/A	N/A
41	N/A	N/A	N/A
42	N/A	N/A	N/A
43	N/A	N/A	N/A
44	N/A	N/A	N/A
45	N/A	N/A	N/A
46	N/A	N/A	N/A
47	N/A	N/A	N/A
48	N/A	N/A	N/A
49	N/A	N/A	N/A
50	N/A	N/A	N/A
51	N/A	N/A	N/A
52	N/A	N/A	N/A

Figure 4-10-4 Local Information Screenshot

The LLDP port settings relate to the currently selected stack unit, as reflected by the page header.

Object	Description
• **Chassis ID SubType**	Identifies the chassis containing the IEEE 802 LAN entity associated with the transmitting LLDP agent. There are several ways in which a chassis may be identified and a chassis ID subtype is used to indicate the type of component being referenced by the chassis ID field. The Managed Switch uses **MAC Address** as Chassis ID.
• **Chassis ID**	The **Chassis ID** is the identification of the Managed Switch's LLDP frames.
• **System Name**	Optional TLV: When checked the "system name" is included in LLDP information transmitted.
• **System Description**	Optional TLV: When checked the "system description" is included in LLDP information transmitted.
• **System Capabilities**	Optional TLV: When checked the "system capability" is included in LLDP information transmitted. The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.
• **Enable Capabilities**	The capabilities that define the primary function(s) of the system.
• **MED Device Type**	Display the information included in the MED TLV field of advertised messages.
• **Management Addresses**	Optional TLV: When checked the "management address" is included in LLDP information transmitted. The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement. The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address
• **Port ID SubType**	Identifies the chassis containing the IEEE 802 LAN entity associated with the transmitting LLDP agent's interfaces.
• **Port ID**	The **Port ID** is the identification of the Managed Switch's port.

ID Basis	Reference
Chassis component	EntPhysicalAlias when entPhysClass has a value of 'chassis(3)' (IETF RFC 2737)
Interface alias	IfAlias (IETF RFC 2863)
Port component	EntPhysicalAlias when entPhysicalClass has a value 'port(10)' or 'backplane(4)' (IETF RFC 2737)
MAC address	MAC address (IEEE Std 802-2001)

Network address	networkAddress
Interface name	ifName (IETF RFC 2863)
Locally assigned	locally assigned

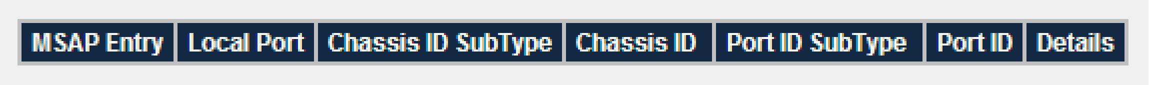
Table 4-10-1 Chassis ID Subtype

ID Basis	Reference
Other	—
Repeater	IETF RFC 2108
Bridge	IETF RFC 2674
WLAN Access Point	IEEE 802.11 MIB
Router	IETF RFC 1812
Telephone	IETF RFC 2011
DOCSIS cable device	IETF RFC 2669 and IETF RFC 2670
End Station Only	IETF RFC 2011

Table 4-10-2 System Capabilities

4.10.4 Remote Information

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The LLDP Neighbor screen in Figure 4-10-5 appears.



MSAP Entry	Local Port	Chassis ID SubType	Chassis ID	Port ID SubType	Port ID	Details

Figure 4-10-5 Remote Information page screenshot

The columns hold the following information:

Object	Description
• **Local Port**	The port on which the LLDP frame was received.
• **Chassis ID SubType**	Identifies the chassis containing the IEEE 802 LAN entity associated with the transmitting LLDP agent. There are several ways in which a chassis may be identified and a chassis ID subtype is used to indicate the type of component being referenced by the chassis ID field.
• **Chassis ID**	The **Chassis ID** is the identification of the neighbor's LLDP frames.
• **Port ID SubType**	Indicates the basis for the identifier that is listed in the Port ID field.
• **Port ID**	The **Remote Port ID** is the identification of the neighbor port.

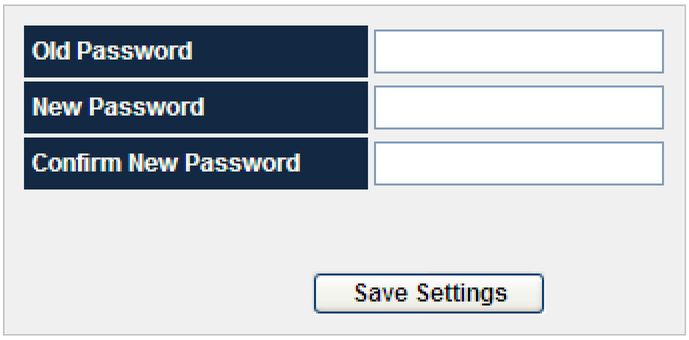
4.11 Admin

The Admin section provides information for devining system parameters including User account and file management, device software. Under Admin the folling topics are provided to devine and view the system informatin:

- **Admin Password**
- **L2 Table**
- **Static Address**
- **Port Mirroting**
- **Admin Timeout**
- **Firmware Upgrade**
- **Reboot**
- **Save Configurations**
- **Logs Settings**
- **Log Server**
- **Memory Logs**
- **Flash Logs**
- **Ping Function**
- **Cable Diagnostic**
- **DHCP Relay**
- **DHCP Option 82**
- **SelfLoop Detection**
- **BOOTP ConfigDownload**

4.11.1 Admin Password

The screen allows user to change the password of the administrator.



Old Password	
New Password	
Confirm New Password	

Figure 4-11-1 Admin Password Screenshot

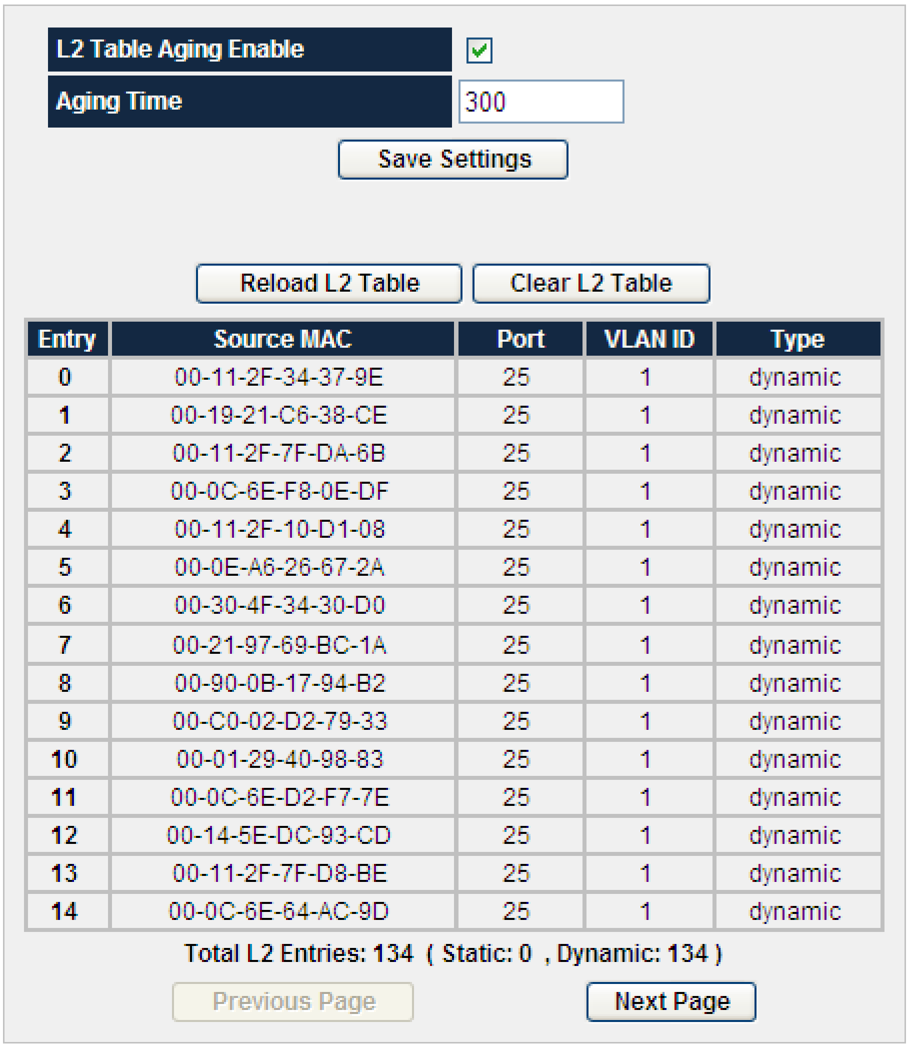
The page includes the following fields:

Object	Description
• **Old Password**	Enter original password.
• **New Password**	Enter a desired password to replace the original one.
• **Confirm New Password**	Enter new password again for confirmation.

4.11.2 L2 Table

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



L2 Table Aging Enable	☑
Aging Time	300

Entry	Source MAC	Port	VLAN ID	Type
0	00-11-2F-34-37-9E	25	1	dynamic
1	00-19-21-C6-38-CE	25	1	dynamic
2	00-11-2F-7F-DA-6B	25	1	dynamic
3	00-0C-6E-F8-0E-DF	25	1	dynamic
4	00-11-2F-10-D1-08	25	1	dynamic
5	00-0E-A6-26-67-2A	25	1	dynamic
6	00-30-4F-34-30-D0	25	1	dynamic
7	00-21-97-69-BC-1A	25	1	dynamic
8	00-90-0B-17-94-B2	25	1	dynamic
9	00-C0-02-D2-79-33	25	1	dynamic
10	00-01-29-40-98-83	25	1	dynamic
11	00-0C-6E-D2-F7-7E	25	1	dynamic
12	00-14-5E-DC-93-CD	25	1	dynamic
13	00-11-2F-7F-D8-BE	25	1	dynamic
14	00-0C-6E-64-AC-9D	25	1	dynamic

Total L2 Entries: 134 (Static: 0 , Dynamic: 134)

Figure 4-11-2 L2 Table Screenshot

The page includes the following fields:

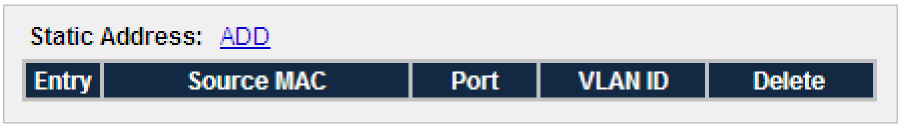
Object	Description
• **L2 Table Aging Enable**	Enable or Disable switch L2 Table aging capability.
• **Aging Time**	Specifies the amount of time the MAC address remains in the L2 table before it is timed out, if no traffic from the source is detected. Enter "0" means to disable aging too.
• **Reload L2 Table**	Retrieves current L2 address table.
• **Clear L2 Table**	Click on the button to clear the dynamic MAC address table.
• **Entry**	Indicates the sequence number for valid MAC address in the L2 address table.
• **Source MAC**	Indicates the valid MAC address in the L2 address table.
• **Port**	Indicates the port number.
• **VLAN ID**	Indicates the VLAN ID the valid MAC address belongs to.
• **Type**	Indicates the MAC address type, either static or dynamic.
• **L2 Entry Lookup**	To seach if MAC existed in L2 Table by entering desired MAC and its VLAN ID and then

	click on "Lookup" button.

4.11.3 Static Address

A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and cannot be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table (see Figure 4-11-3)

This Static Address page provides a way to **add**, **delete** MAC addresses in the L2 address table.



Static Address: ADD

Entry	Source MAC	Port	VLAN ID	Delete

Figure 4-11-3 Static Address Screenshot

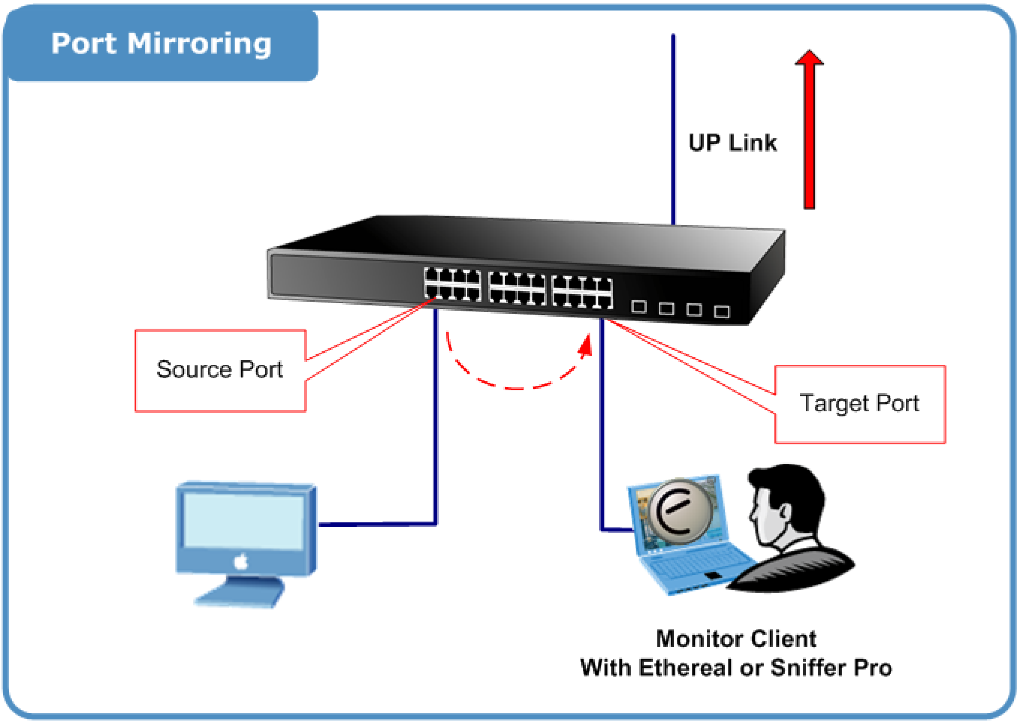
The page includes the following fields:

Object	Description
• **Add**	Clickes on this button to inserts a static MAC address into the L2 address table.
• **Static MAC Address**	Specifies the MAC address to add.
• **Port**	Specifies the port number.
• **VLAN ID**	Specifies the VLAN ID of the MAC address.
• **Delete**	Removes the specified MAC address.

4.11.4 Port Mirroring

Configure port Mirroring on this page. This function provide to monitoring network traffic that forwards a copy of each incoming or outgoing packet from one port of a network switch to another port where the packet can be studied. It enables the manager to keep close track of switch performance and alter it if necessary.

- 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 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.

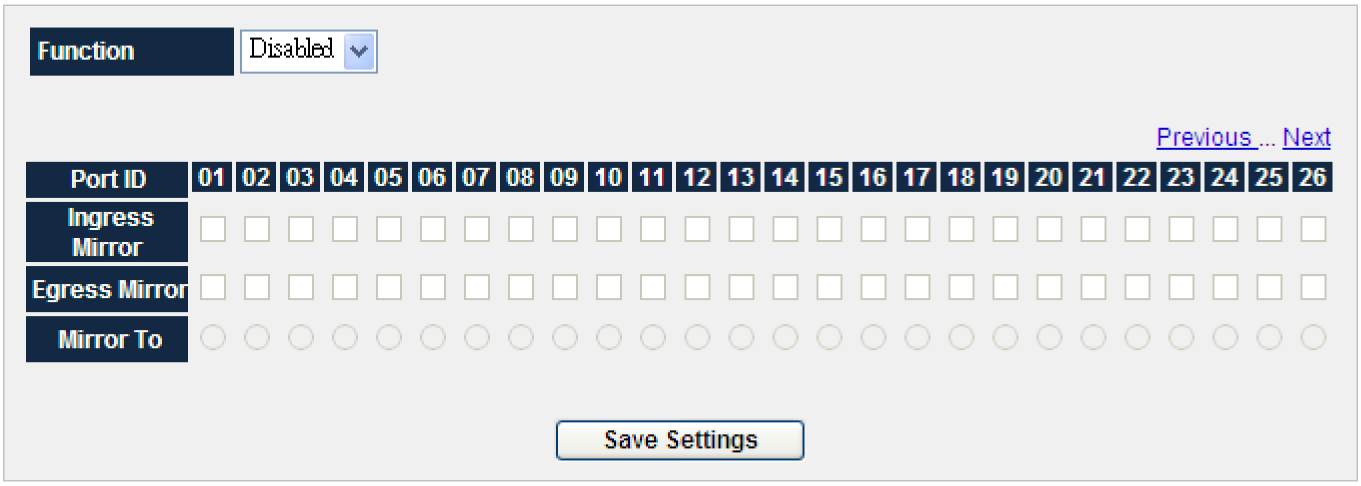


The traffic to be copied to the mirror port is selected as follows:

- 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

Port mirroring monitors ingress and/or egress traffic from specific ports to a single monitor-to port. The Port Mirror Configuration screen in Figure 4-11-4 appears.



Function	Disabled

Port ID	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Ingress Mirror	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Egress Mirror	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Mirror To	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Figure 4-11-4 Port Mirroring Screenshot

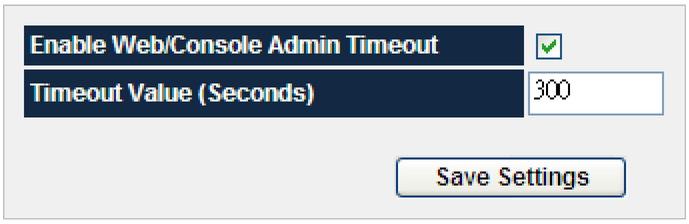
The page includes the following fields:

Object	Description
• **Function**	Enables or disables port mirroring.

• **Ingress Mirror**	Specifies an Ingress Mirror port to which ingress traffic will be mirrored.
• **Egress Mirror**	Specifies an Egress Mirror port to which egress traffic will be mirrored.
• **Mirror To**	Specifies the mirrored-to port.

4.11.5 Admin Timeout

Specifies the web/console administrative time out value.



Enable Web/Console Admin Timeout ☑

Timeout Value (Seconds) 300

Figure 4-11-5 Admin Timeout Screenshot

The page includes the following fields:

Object	Description
• **Enable Web/Console Admin Timeout**	Enable or Disable Admin Timeout function. The web/console connection session will not be terminated if function is disabled.
• **Timeout Value (Seconds)**	Specifies Admin Timeout value. The web/console session will be terminated if no action on current web/console session during this time out value.

4.11.6 Firmware Upgrade

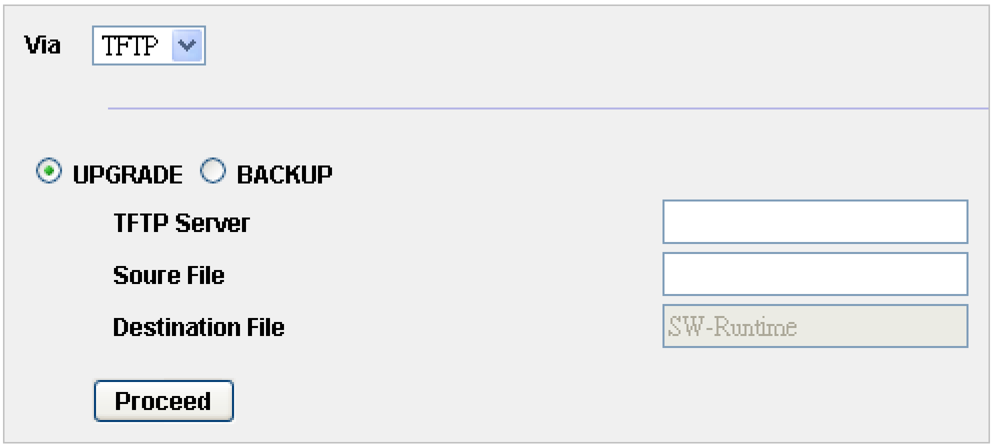
The page provides the ways to upgrade/backup switch firmware.

It provides the functions allowing the user to update the switch firmware via **HTTP** or the **Trivial File Transfer Protocol (TFTP)** server. Before updating, make sure the TFTP server is ready and the firmware image is located on the TFTP server.

■ TFTP Firmware Upgrade

The **Firmware Upgrade** page provides the functions to allow a user to update the Managed Switch firmware from the TFTP server in the network. Before updating, make sure you have your TFTP server ready and the firmware image is on the TFTP server. The screen in Figure 4-11-6 appears.

Use this menu to download a file from specified TFTP server to the Managed Switch.



Via: TFTP

● UPGRADE ○ BACKUP

TFTP Server

Soure File

Destination File: SW-Runtime

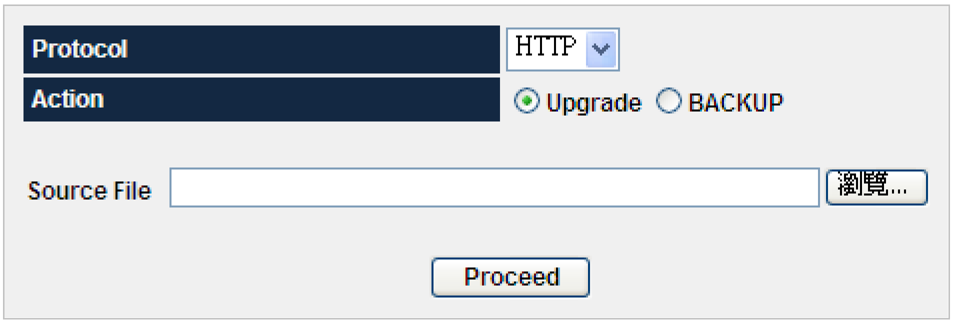
Figure 4-11-6 TFTP Firmware Upgrade Screenshot

The page includes the following fields:

Object	Description
TFTP Server	Type in your TFTP server IP.
Source File	Type in the name of the firmware image file to be updated.

■ HTTP Firmware Upgrade

The **HTTP Firmware Upgrade** page contains fields for downloading system image files from the Local File browser to the device. The Web Firmware Upgrade screen in Figure 4-11-7 appears.



Protocol: HTTP

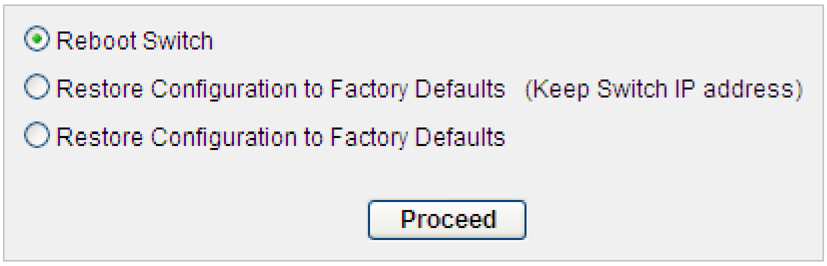
Action: ● Upgrade ○ BACKUP

Source File

Figure 4-11-7 HTTP Firmware Upgrade Screenshot

4.11.7 Reboot

The **Reboot** page enables the device to be rebooted from a remote location. Once the Reboot button is pressed, user have to re-login the WEB interface about 60 seconds later, the screen in Figure 4-11-9 and Figure 4-11-10 appears.

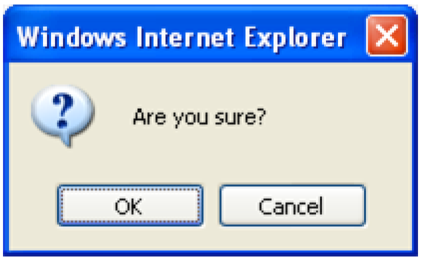


◉ Reboot Switch
○ Restore Configuration to Factory Defaults (Keep Switch IP address)
○ Restore Configuration to Factory Defaults

Figure 4-11-8 Reboot Screenshot

The page includes the following fields:

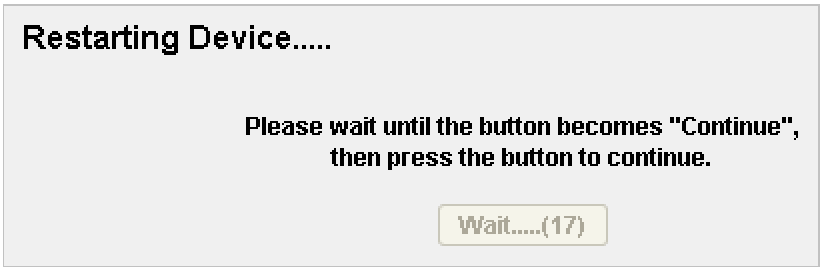
Object	Description
• **Reboot Switch**	Restart the switch with current configuration.
• **Restore Configuration to Factory Defaults (Keep IP address)**	This option will restore the switch configuration to factory defaults. All configuration will be removed except IP address.
• **Restore Configuration to Factory Defaults**	This option will restore the switch configuration to factory defaults. All configuration will be removed.



Windows Internet Explorer

Are you sure?

Figure 4-11-9 Reboot dialogue Screenshot



Restarting Device.....

Please wait until the button becomes "Continue",
then press the button to continue.

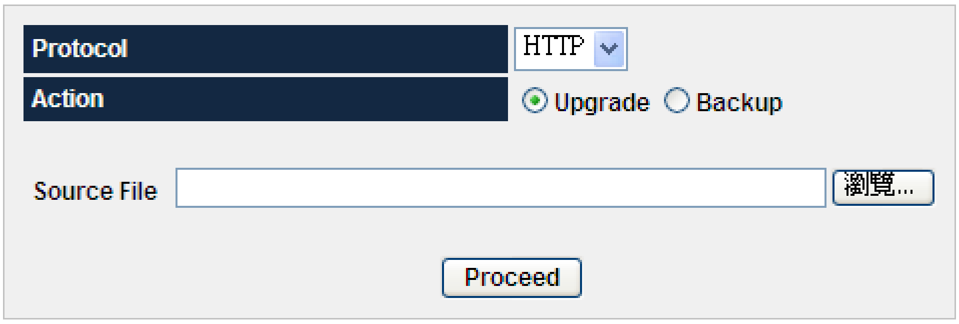
Figure 4-11-10 Reboot message Screenshot

Note

You can also check the **PWR LED** at the front panel to identify the System is load completely or not. If the PWR LED is blinking, then it is in the firmware load stage; if the PWR LED light on, you can use the WEB browser to login the Switch.

4.11.8 Save Configurations

The page provides the ways to upgrade/backup switch configuration via TFTP/HTTP protocol. The screen in Figure 4-11-11 appears.



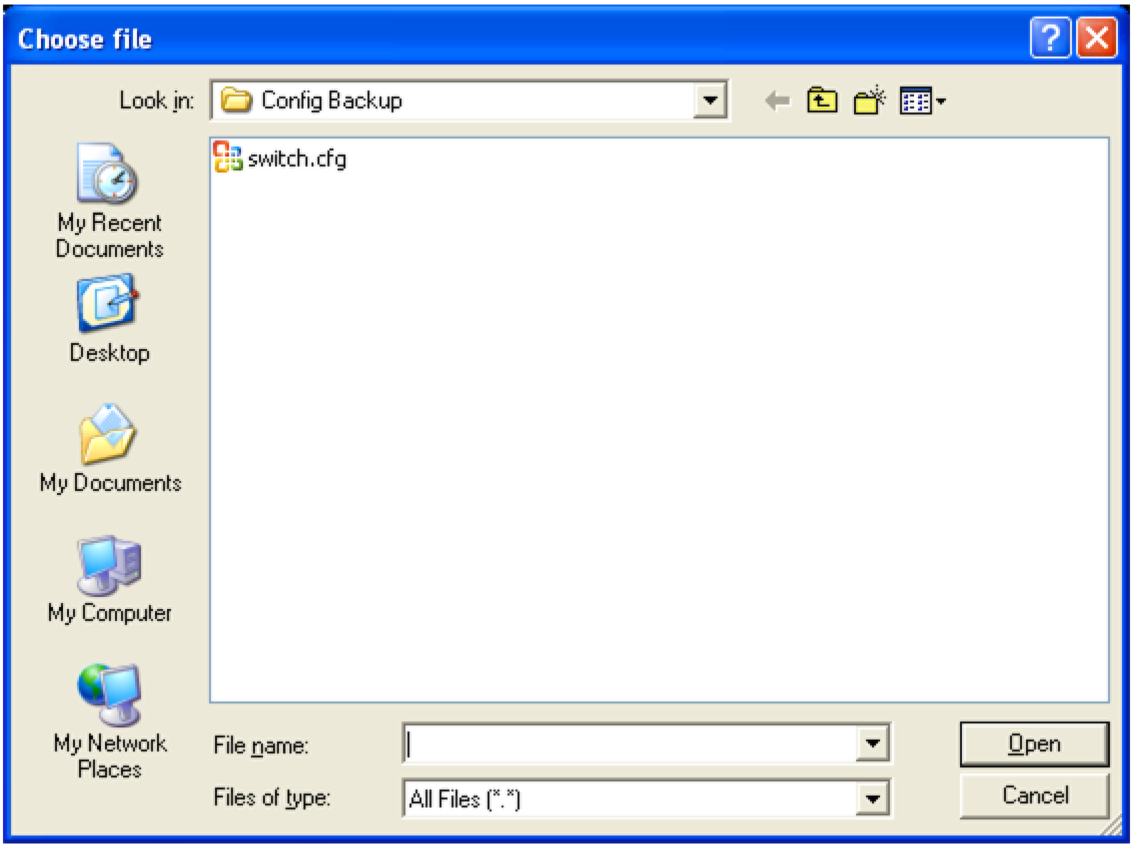
Protocol	HTTP
Action	● Upgrade ○ Backup

Source File

Figure 4-11-11 Save Configurations Screenshot

- **HTTP Configuration Upgrade**

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



Choose file

Look in: Config Backup

switch.cfg

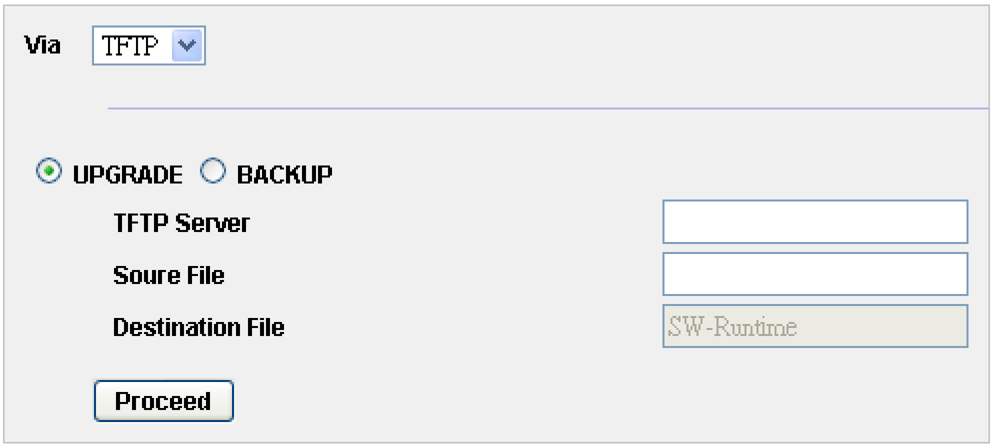
File name:

Files of type: All Files (*.*)

Figure 4-11-12 Windows file selection menu popup Screenshot

2. Select on the configuration file then click "**Proceed**", the bottom of the browser shows the upload status.

- **HTTP Configuration Backup**



Via TFTP

● UPGRADE ○ BACKUP

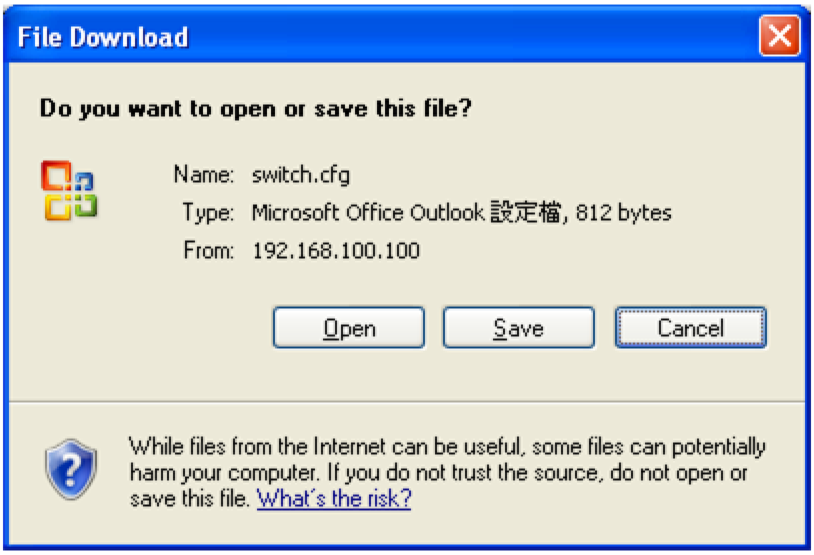
TFTP Server

Soure File

Destination File SW-Runtime

Figure 4-11-13 HTTP configuration backup screenshot

1. Select "Backup" and press the **"Proceed"** button to save the current configuration in manager workstation. The following screens in Figure 4-11-14 and 4-11-15 appear



Do you want to open or save this file?

Name: switch.cfg

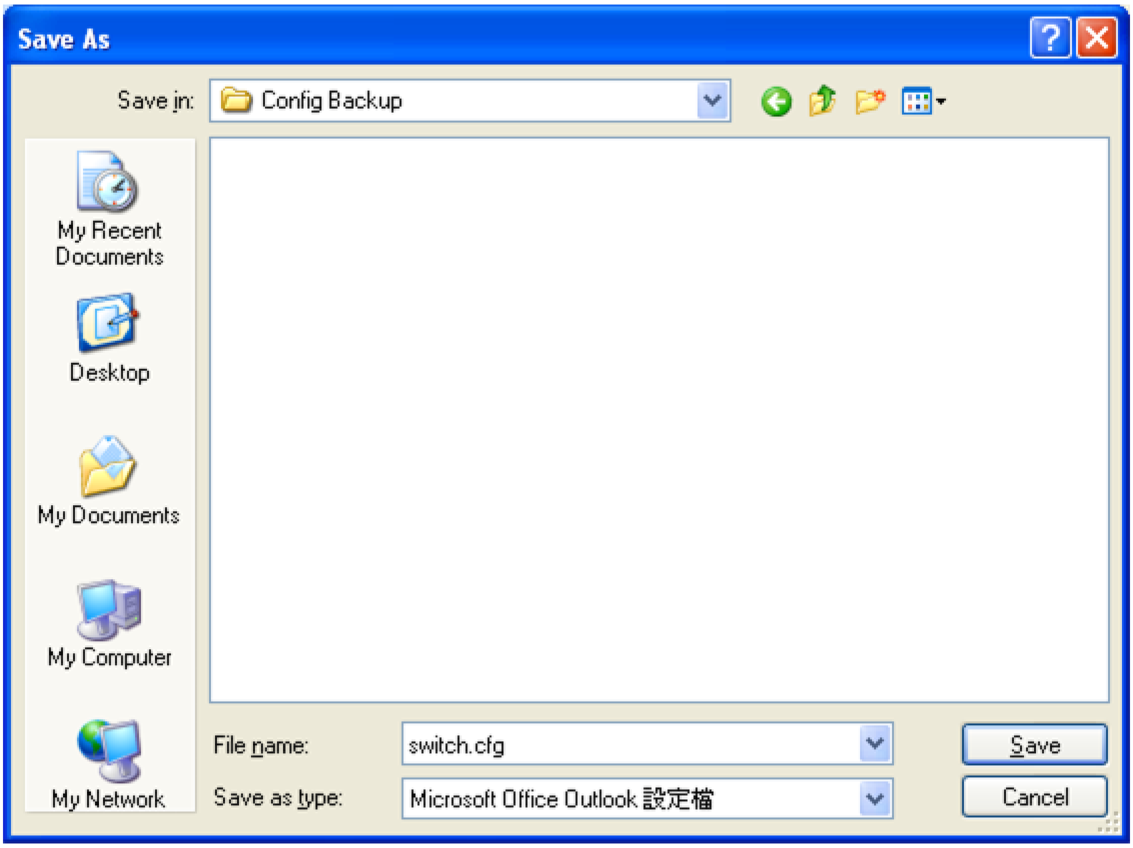
Type: Microsoft Office Outlook 設定檔, 812 bytes

From: 192.168.100.100

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

Figure 4-11-14 File Download screen Screenshot

2. Chose the file save path in management workstation.



Save in: Config Backup

File name: switch.cfg

Save as type: Microsoft Office Outlook 設定檔

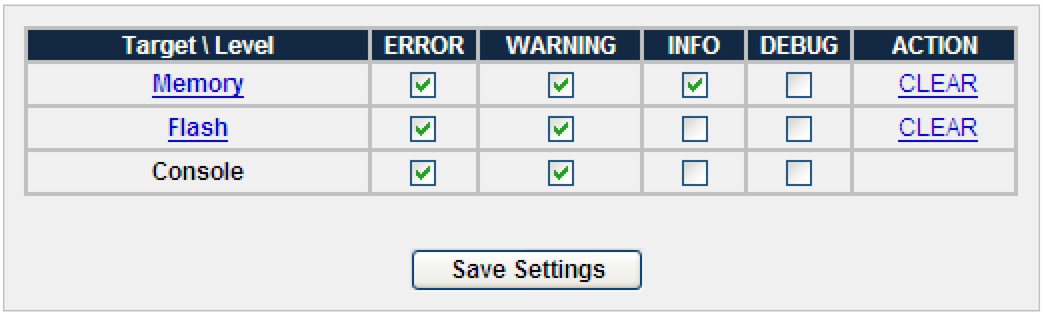
Figure 4-11-15 File save screen Screenshot

4.11.9 Logs Settings

This page allows you to log the messages happened in this system for later reference.

There are 4 types of logging targets are provided for the logs,

- **Memory Logs**: The logs will be cleared after system reboot.
- **Flash Logs**: The logs will be stored into flash.
- **Console**: Display log message through UART interface.
- **Syslogs**: Log the message to a remote host with BSD syslogd compliant daemon running.
    - Name - A short name for identifying this server.
    - IP Address - Syslog Server IP address.
    - Port - UDP port of the Syslogs Server.
    - Facility - The facility value to be used when logs are recorded in the remote server. See RFC 3164 for more details.



Target \ Level	ERROR	WARNING	INFO	DEBUG	ACTION
Memory	☑	☑	☑	□	CLEAR
Flash	☑	☑	□	□	CLEAR
Console	☑	☑	□	□	

Figure 4-11-16 Logs Settings Screenshot

The page includes the following fields:

Object	Description
• **Level**	Indicates the severity of the logs.
• **ACTION**	Click on hyperlink 'Clear Logs' will erase the logs.

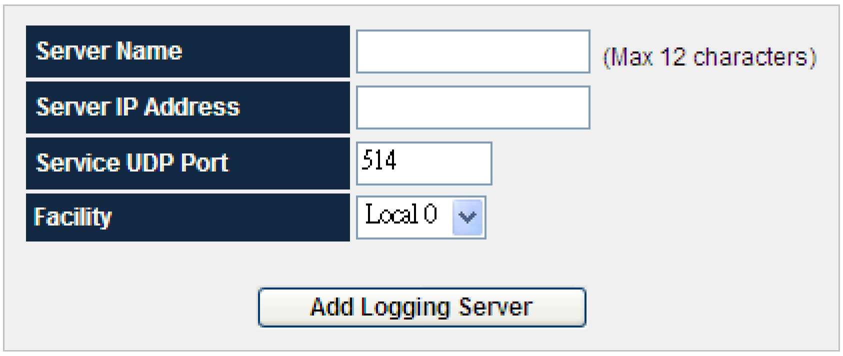
4.11.10 Log Server

The Global Log Parameters page contains fields for enabling logs globally, and fields for defining log parameters. The Severity log messages are listed from the highest severity to the lowest.

Event messages have a unique format, as per the SYSLOG RFC recommended message format for all error reporting. For example, Syslog+ local device reporting. Messages are assigned a severity code, and include a message mnemonic, which identifies the source application generating the message. Messages are filtered based on their urgency or relevancy. The severity of each message determines the set of event logging devices to which are sent for each event logging device. The following table contains the Log Severity Levels:

Severity Type	Severity Level	Description	Example
Emergency	0	The system is not functioning.	Memories overflow.
Alert	1	The system needs immediate attention.	Main system memory pool overflow.
Critical	2	The system is in a critical state.	Cannot bind to SNMP.
Error	3	A system error has occurred.	Failed to delete entry.
Warning	4	A system warning has occurred.	Port down.
Notice	5	The system is functioning properly, but system notice has occurred.	Bad route.
Informational	6	Provides device information.	Link up.
Debug	7	Provides detailed information about the log. If a Debug error occurs, contact Dell Online Technical Support	Method list created.

The Server Logs screen contains information for viewing and configuring the Remote Log Servers. New log servers can be defined, and the log severity sent to each server.



Server Name	(Max 12 characters)
Server IP Address	
Service UDP Port	514
Facility	Local 0

Figure 4-11-17 Log Server Screenshot

The page includes the following fields:

Object	Description
• **Server Name**	Specifies a short name for identifying this server.
• **Server IP Address**	Specifies IP address of the server inn dotted decimal notation.
• **Service UDP Port**	Specifies UDP port of the server. The possible range is 1 to 65535. The default value is **514**.
• **Facility**	Specifies the facility value to be used when logs are recorded in the remote server. See RFC 3164 for more details.

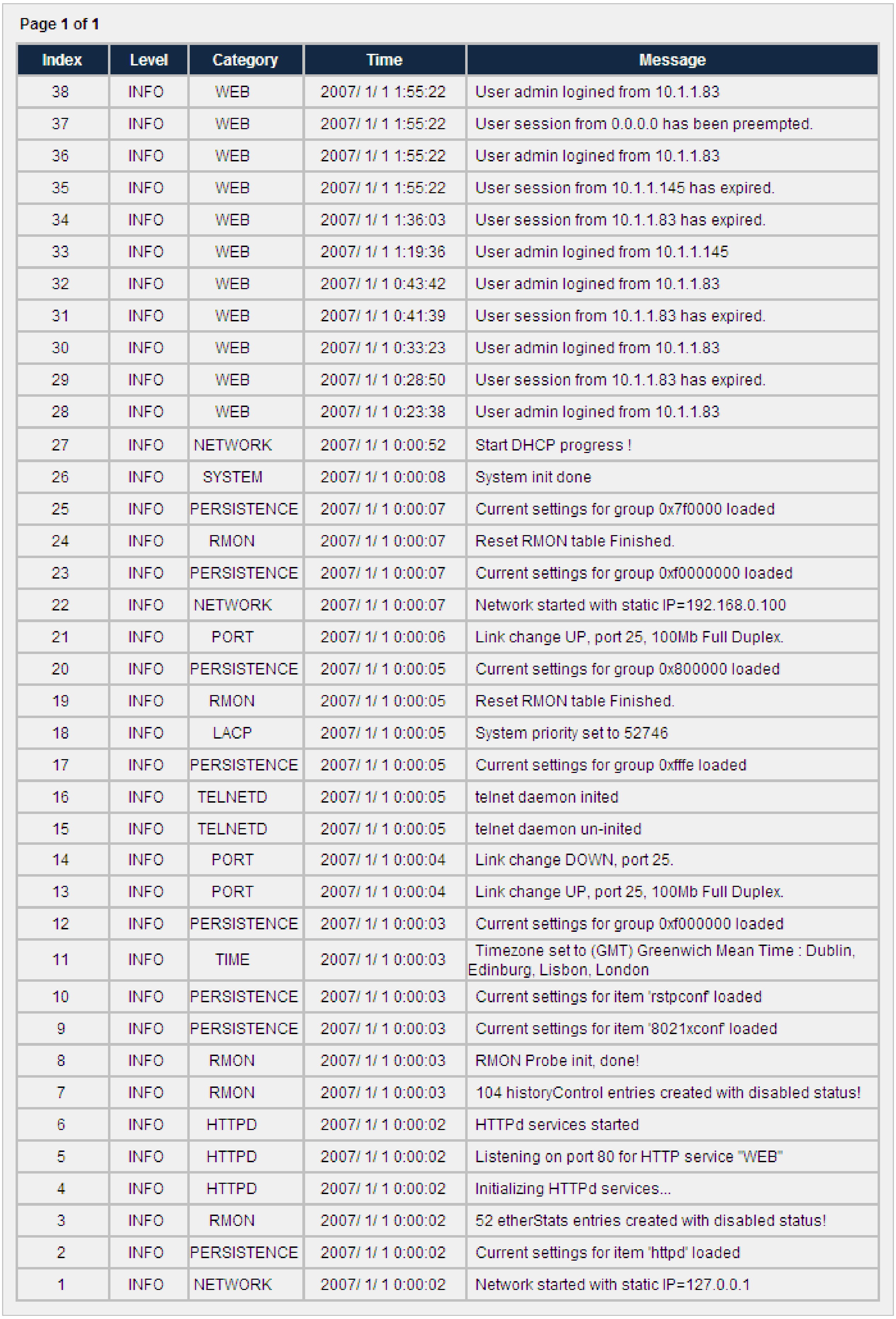
	Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility is overridden. All applications defined for a device utilize the same facility on a server. The possible field values are Local 0 - Local 7. The field default is Local **7**.

Note

When a severity level is selected, all severity level choices above the selection are selected automatically.

4.11.11 Memory Logs

The Memory Log screen contains all system logs in a chronological order that are saved in RAM (Cache), Log Index which shows the log number, Log Time at which the log was generated, Severity which shows the log severity, and the description that shows log message text.



Page **1** of **1**

Index	Level	Category	Time	Message
38	INFO	WEB	2007/ 1/ 1 1:55:22	User admin logined from 10.1.1.83
37	INFO	WEB	2007/ 1/ 1 1:55:22	User session from 0.0.0.0 has been preempted.
36	INFO	WEB	2007/ 1/ 1 1:55:22	User admin logined from 10.1.1.83
35	INFO	WEB	2007/ 1/ 1 1:55:22	User session from 10.1.1.145 has expired.
34	INFO	WEB	2007/ 1/ 1 1:36:03	User session from 10.1.1.83 has expired.
33	INFO	WEB	2007/ 1/ 1 1:19:36	User admin logined from 10.1.1.145
32	INFO	WEB	2007/ 1/ 1 0:43:42	User admin logined from 10.1.1.83
31	INFO	WEB	2007/ 1/ 1 0:41:39	User session from 10.1.1.83 has expired.
30	INFO	WEB	2007/ 1/ 1 0:33:23	User admin logined from 10.1.1.83
29	INFO	WEB	2007/ 1/ 1 0:28:50	User session from 10.1.1.83 has expired.
28	INFO	WEB	2007/ 1/ 1 0:23:38	User admin logined from 10.1.1.83
27	INFO	NETWORK	2007/ 1/ 1 0:00:52	Start DHCP progress !
26	INFO	SYSTEM	2007/ 1/ 1 0:00:08	System init done
25	INFO	PERSISTENCE	2007/ 1/ 1 0:00:07	Current settings for group 0x7f0000 loaded
24	INFO	RMON	2007/ 1/ 1 0:00:07	Reset RMON table Finished.
23	INFO	PERSISTENCE	2007/ 1/ 1 0:00:07	Current settings for group 0xf0000000 loaded
22	INFO	NETWORK	2007/ 1/ 1 0:00:07	Network started with static IP=192.168.0.100
21	INFO	PORT	2007/ 1/ 1 0:00:06	Link change UP, port 25, 100Mb Full Duplex.
20	INFO	PERSISTENCE	2007/ 1/ 1 0:00:05	Current settings for group 0x800000 loaded
19	INFO	RMON	2007/ 1/ 1 0:00:05	Reset RMON table Finished.
18	INFO	LACP	2007/ 1/ 1 0:00:05	System priority set to 52746
17	INFO	PERSISTENCE	2007/ 1/ 1 0:00:05	Current settings for group 0xfffe loaded
16	INFO	TELNETD	2007/ 1/ 1 0:00:05	telnet daemon inited
15	INFO	TELNETD	2007/ 1/ 1 0:00:05	telnet daemon un-inited
14	INFO	PORT	2007/ 1/ 1 0:00:04	Link change DOWN, port 25.
13	INFO	PORT	2007/ 1/ 1 0:00:04	Link change UP, port 25, 100Mb Full Duplex.
12	INFO	PERSISTENCE	2007/ 1/ 1 0:00:03	Current settings for group 0xf000000 loaded
11	INFO	TIME	2007/ 1/ 1 0:00:03	Timezone set to (GMT) Greenwich Mean Time : Dublin, Edinburg, Lisbon, London
10	INFO	PERSISTENCE	2007/ 1/ 1 0:00:03	Current settings for item 'rstpconf loaded
9	INFO	PERSISTENCE	2007/ 1/ 1 0:00:03	Current settings for item '8021xconf loaded
8	INFO	RMON	2007/ 1/ 1 0:00:03	RMON Probe init, done!
7	INFO	RMON	2007/ 1/ 1 0:00:03	104 historyControl entries created with disabled status!
6	INFO	HTTPD	2007/ 1/ 1 0:00:02	HTTPd services started
5	INFO	HTTPD	2007/ 1/ 1 0:00:02	Listening on port 80 for HTTP service "WEB"
4	INFO	HTTPD	2007/ 1/ 1 0:00:02	Initializing HTTPd services...
3	INFO	RMON	2007/ 1/ 1 0:00:02	52 etherStats entries created with disabled status!
2	INFO	PERSISTENCE	2007/ 1/ 1 0:00:02	Current settings for item 'httpd' loaded
1	INFO	NETWORK	2007/ 1/ 1 0:00:02	Network started with static IP=127.0.0.1

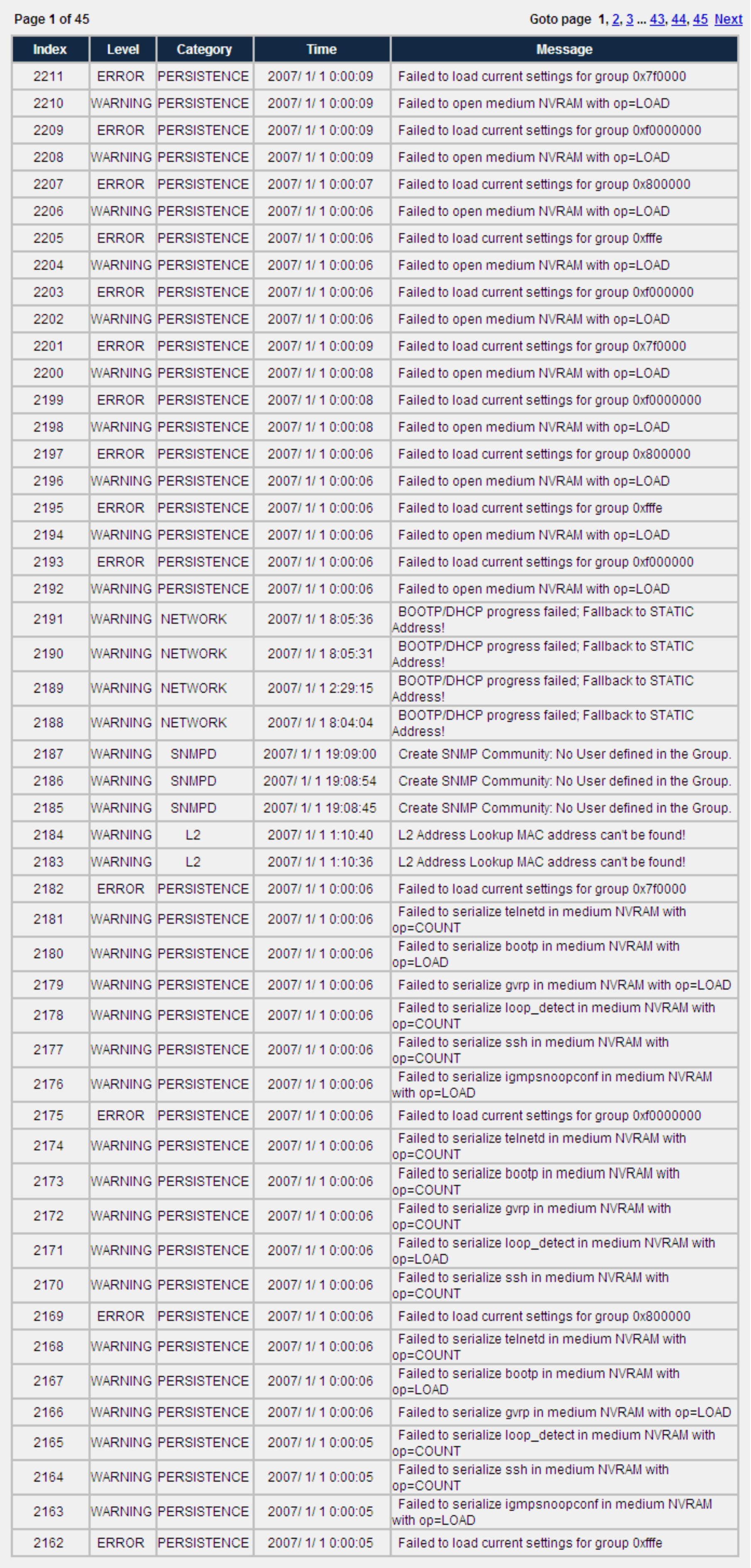
Figure 4-11-18 Memory Logs Screenshot

The page includes the following fields:

Object	Description
- **Index**	Indicates the global sequence number for the log.
- **Level**	ndicates the severity of the log.
- **Category**	Indicates the facility/category that the log belongs to.
- **Time**	Indicates the time when the log is recorded.
- **Message**	Shows the detailed description of the log.

4.11.12 Flash Logs

The Flash Log screen contains information about log entries saved to the Log File in FLASH, the time that the log generated, the log severity, and description of the log message. The Message Log is available after reboot.



Page **1** of 45

Goto page **1**, 2, 3 ... 43, 44, 45 Next

Index	Level	Category	Time	Message
2211	ERROR	PERSISTENCE	2007/ 1/ 1 0:00:09	Failed to load current settings for group 0x7f0000
2210	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:09	Failed to open medium NVRAM with op=LOAD
2209	ERROR	PERSISTENCE	2007/ 1/ 1 0:00:09	Failed to load current settings for group 0xf0000000
2208	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:09	Failed to open medium NVRAM with op=LOAD
2207	ERROR	PERSISTENCE	2007/ 1/ 1 0:00:07	Failed to load current settings for group 0x800000
2206	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to open medium NVRAM with op=LOAD
2205	ERROR	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to load current settings for group 0xfffe
2204	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to open medium NVRAM with op=LOAD
2203	ERROR	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to load current settings for group 0xf000000
2202	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to open medium NVRAM with op=LOAD
2201	ERROR	PERSISTENCE	2007/ 1/ 1 0:00:09	Failed to load current settings for group 0x7f0000
2200	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:08	Failed to open medium NVRAM with op=LOAD
2199	ERROR	PERSISTENCE	2007/ 1/ 1 0:00:08	Failed to load current settings for group 0xf0000000
2198	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:08	Failed to open medium NVRAM with op=LOAD
2197	ERROR	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to load current settings for group 0x800000
2196	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to open medium NVRAM with op=LOAD
2195	ERROR	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to load current settings for group 0xfffe
2194	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to open medium NVRAM with op=LOAD
2193	ERROR	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to load current settings for group 0xf000000
2192	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to open medium NVRAM with op=LOAD
2191	WARNING	NETWORK	2007/ 1/ 1 8:05:36	BOOTP/DHCP progress failed; Fallback to STATIC Address!
2190	WARNING	NETWORK	2007/ 1/ 1 8:05:31	BOOTP/DHCP progress failed; Fallback to STATIC Address!
2189	WARNING	NETWORK	2007/ 1/ 1 2:29:15	BOOTP/DHCP progress failed; Fallback to STATIC Address!
2188	WARNING	NETWORK	2007/ 1/ 1 8:04:04	BOOTP/DHCP progress failed; Fallback to STATIC Address!
2187	WARNING	SNMPD	2007/ 1/ 1 19:09:00	Create SNMP Community: No User defined in the Group.
2186	WARNING	SNMPD	2007/ 1/ 1 19:08:54	Create SNMP Community: No User defined in the Group.
2185	WARNING	SNMPD	2007/ 1/ 1 19:08:45	Create SNMP Community: No User defined in the Group.
2184	WARNING	L2	2007/ 1/ 1 1:10:40	L2 Address Lookup MAC address can't be found!
2183	WARNING	L2	2007/ 1/ 1 1:10:36	L2 Address Lookup MAC address can't be found!
2182	ERROR	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to load current settings for group 0x7f0000
2181	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to serialize telnetd in medium NVRAM with op=COUNT
2180	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to serialize bootp in medium NVRAM with op=LOAD
2179	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to serialize gvrp in medium NVRAM with op=LOAD
2178	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to serialize loop_detect in medium NVRAM with op=COUNT
2177	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to serialize ssh in medium NVRAM with op=COUNT
2176	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to serialize igmpsnoopconf in medium NVRAM with op=LOAD
2175	ERROR	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to load current settings for group 0xf0000000
2174	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to serialize telnetd in medium NVRAM with op=COUNT
2173	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to serialize bootp in medium NVRAM with op=COUNT
2172	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to serialize gvrp in medium NVRAM with op=COUNT
2171	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to serialize loop_detect in medium NVRAM with op=LOAD
2170	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to serialize ssh in medium NVRAM with op=COUNT
2169	ERROR	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to load current settings for group 0x800000
2168	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to serialize telnetd in medium NVRAM with op=COUNT
2167	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to serialize bootp in medium NVRAM with op=LOAD
2166	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:06	Failed to serialize gvrp in medium NVRAM with op=LOAD
2165	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:05	Failed to serialize loop_detect in medium NVRAM with op=COUNT
2164	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:05	Failed to serialize ssh in medium NVRAM with op=COUNT
2163	WARNING	PERSISTENCE	2007/ 1/ 1 0:00:05	Failed to serialize igmpsnoopconf in medium NVRAM with op=LOAD
2162	ERROR	PERSISTENCE	2007/ 1/ 1 0:00:05	Failed to load current settings for group 0xfffe

Figure 4-11-19 Flash Logs Screenshot

The page includes the following fields:

Object	Description
• **Index**	Indicates the global sequence number for the log.
• **Level**	Indicates the severity of the log.
• **Category**	Indicates the facility/category that the log belongs to.
• **Time**	Indicates the time when the log is recorded.
• **Message**	Shows the detailed description of the log.

4.11.13 Ping Function

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.

After you press , 4 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs. The ICMP Ping screen in Figure 4-11-20 appears.

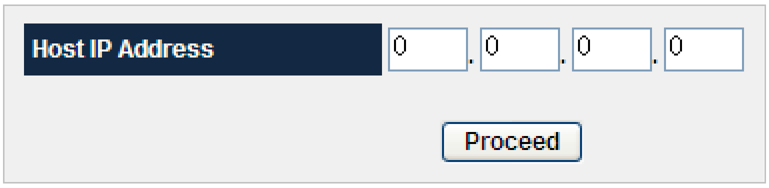


Figure 4-11-20 Ping Function Screenshot

The page includes the following fields:

Object	Description
• **Host IP Address**	The destination IP Address.

Note

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

4.11.14 Cable Diagnostic

The accuracy for detecting fault free cable length is within +/- 5 meters normally. However, under the following conditions, the fault free cable length detection accuracy can be beyond 5 meters limit. The frequency of this occurrence is very low.

1. The remote link partner has a termination incompatible with IEEE 802.3 specification (100 Ω).

2. A cable coupler is placed within 7 meters from the link partner.

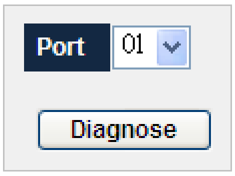
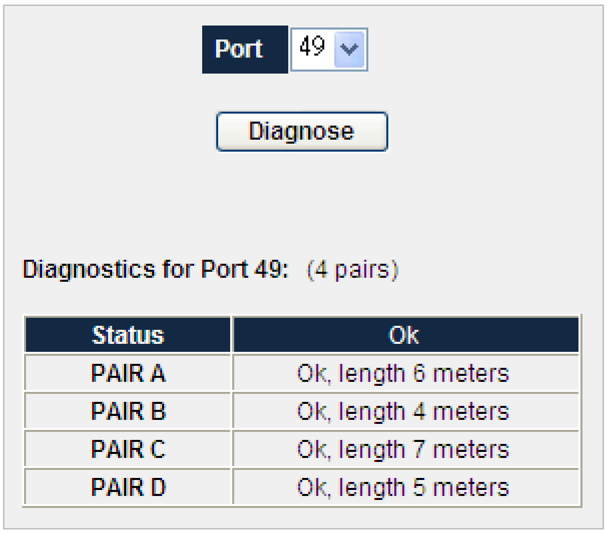


Figure 4-11-21 Cable Diagnostic Screenshot



Diagnostics for Port 49: (4 pairs)

Status	Ok
PAIR A	Ok, length 6 meters
PAIR B	Ok, length 4 meters
PAIR C	Ok, length 7 meters
PAIR D	Ok, length 5 meters

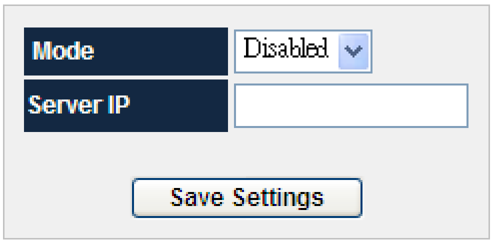
Figure 4-11-22 Cable Diagnostic Screenshot

The page contains the following fields:

Object	Description
• **Port**	This is the port to which the cable is connected.
• **Test Result**	• **OK** - indicates that the cable passed the test. • **Open** -means the cable is connected on only one side. • **Short** - indicates that a short has occurred in the cable. This is the approximate length of the cable. The Cable Length test can be performed only when the port is up.

4.11.15 DHCP Relay

A DHCP Relay agent is configured to listen for DHCP or BOOTP broadcast from DHCP clients and then relay those messages to DHCP servers on different subnets.



Mode	Disabled
Server IP	

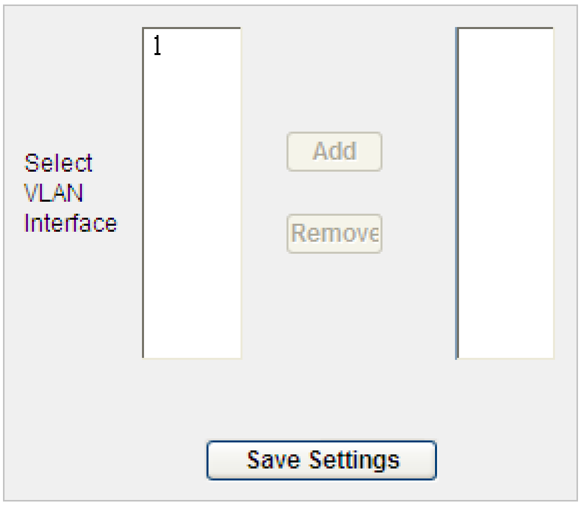
Figure 4-11-23 DHCP Relay Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Enables or Disables DHCP Relay function.
• **Server IP**	Enteres remote DHCP server IP address.

4.11.16 DHCP Option 82

The DHCP option 82 enables a Dynamic Host Configuration Protocol (DHCP) relay agent to include information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP server can use this information to implement IP address or other parameter-assignment policies.



Select VLAN Interface

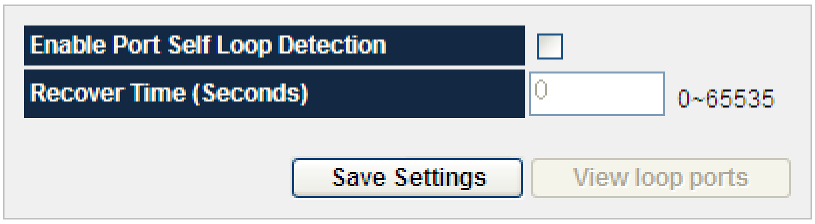
Figure 4-11-24 DHCP Option 82 Screenshot

The page includes the following fields:

Object	Description
• **Select VLAN Interface**	Selects desired VLAN groups to perform relay function.

4.11.17 Self Loop Detection

Self Loop Detection means when one port produces a self loop and Switch can detect this situation. When it happens, the port will be disabled. After a recover time's later switch will enable this port and try to detect this port again until there is no self loop on this port.



Enable Port Self Loop Detection □

Recover Time (Seconds) 0 0~65535

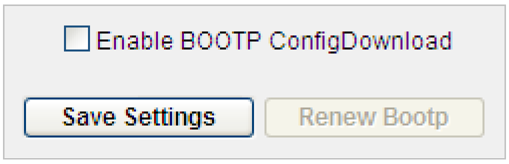
Figure 4-11-25 Self Loop Detection Screenshot

The page includes the following fields:

Object	Description
• **Enable Port Self Loop Detection**	Enable or Disable port self loop detection function on the Managed Switch.
• **Recover Time (Seconds)**	Specifies port recover time value, 0 indicate the port will not auto recover.

4.11.18 BOOTP Configure Download

BOOTP Configure Download is a feature of download switch configure file from the special TFTP server automaticly. Enable DHCP Client and DHCP Server assigned the Switch IP Address, at the same time the Switch can acquire the Option 66/67 message (bootp file name & TFTP server IP) from the DCHP Packet or BOOTP Packet. According to these message, Switch use tftp client download the special configure file from the special TFTP Server. When switch download succeed, these message will be saved. Next time Switch get the different file name or TFTP server IP, and try to download the new configure file again.



□ Enable BOOTP ConfigDownload

Figure 4-11-26 BOOTP Configure Download Screenshot

Note

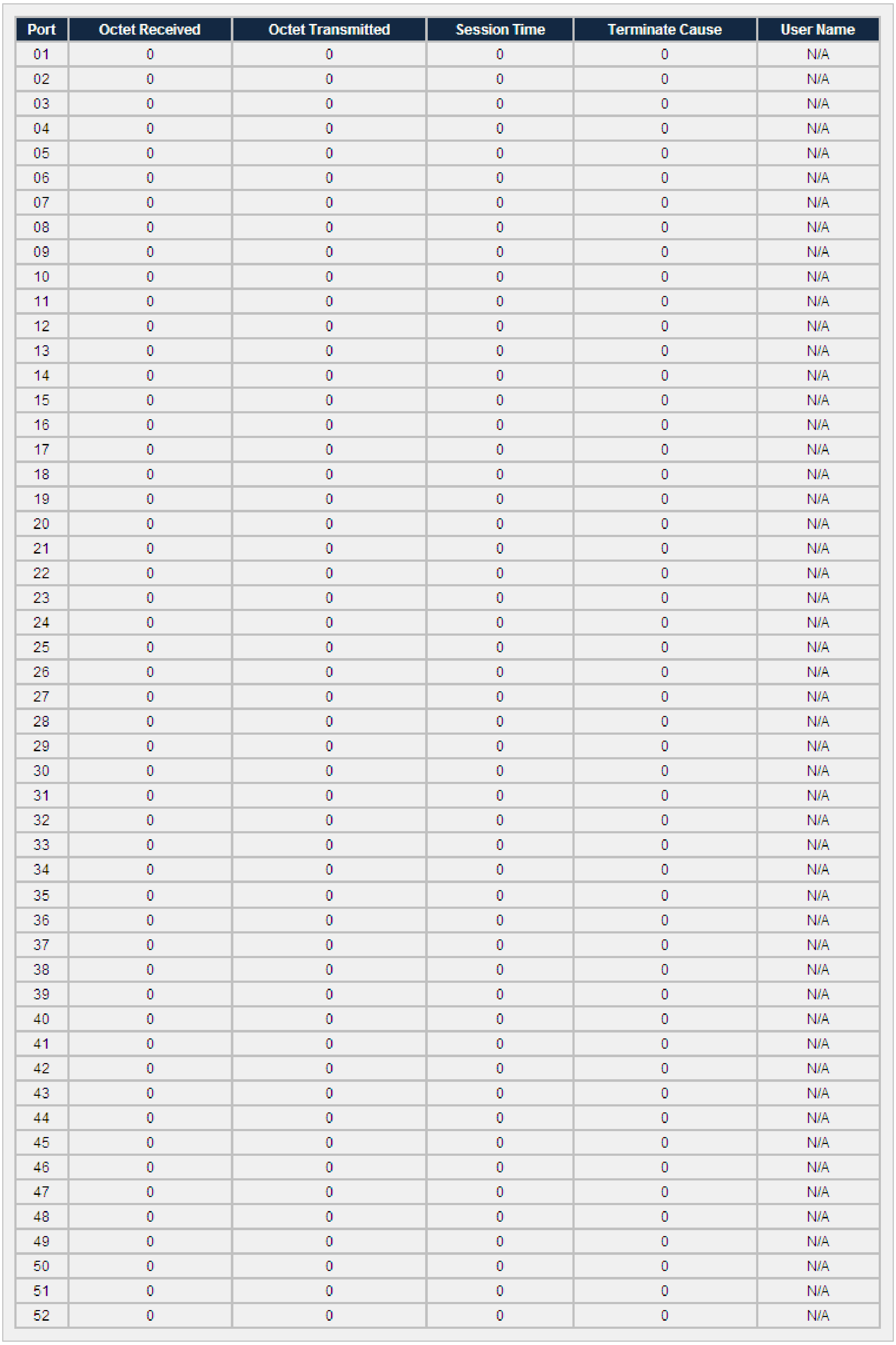
Enable DHCP Client and should have a DHCP Server or BOOTP Server support Option 66/67.

4.12 Statistics

This chapter shows Statistic of the Managed Switch.

4.12.1 802.1X Statistic

This page provides detailed IEEE 802.1X statistics of each port running port-based authentication. The 802.1X Statistics screen in Figure 4-12-1 appears.



Port	Octet Received	Octet Transmitted	Session Time	Terminate Cause	User Name
01	0	0	0	0	N/A
02	0	0	0	0	N/A
03	0	0	0	0	N/A
04	0	0	0	0	N/A
05	0	0	0	0	N/A
06	0	0	0	0	N/A
07	0	0	0	0	N/A
08	0	0	0	0	N/A
09	0	0	0	0	N/A
10	0	0	0	0	N/A
11	0	0	0	0	N/A
12	0	0	0	0	N/A
13	0	0	0	0	N/A
14	0	0	0	0	N/A
15	0	0	0	0	N/A
16	0	0	0	0	N/A
17	0	0	0	0	N/A
18	0	0	0	0	N/A
19	0	0	0	0	N/A
20	0	0	0	0	N/A
21	0	0	0	0	N/A
22	0	0	0	0	N/A
23	0	0	0	0	N/A
24	0	0	0	0	N/A
25	0	0	0	0	N/A
26	0	0	0	0	N/A
27	0	0	0	0	N/A
28	0	0	0	0	N/A
29	0	0	0	0	N/A
30	0	0	0	0	N/A
31	0	0	0	0	N/A
32	0	0	0	0	N/A
33	0	0	0	0	N/A
34	0	0	0	0	N/A
35	0	0	0	0	N/A
36	0	0	0	0	N/A
37	0	0	0	0	N/A
38	0	0	0	0	N/A
39	0	0	0	0	N/A
40	0	0	0	0	N/A
41	0	0	0	0	N/A
42	0	0	0	0	N/A
43	0	0	0	0	N/A
44	0	0	0	0	N/A
45	0	0	0	0	N/A
46	0	0	0	0	N/A
47	0	0	0	0	N/A
48	0	0	0	0	N/A
49	0	0	0	0	N/A
50	0	0	0	0	N/A
51	0	0	0	0	N/A
52	0	0	0	0	N/A

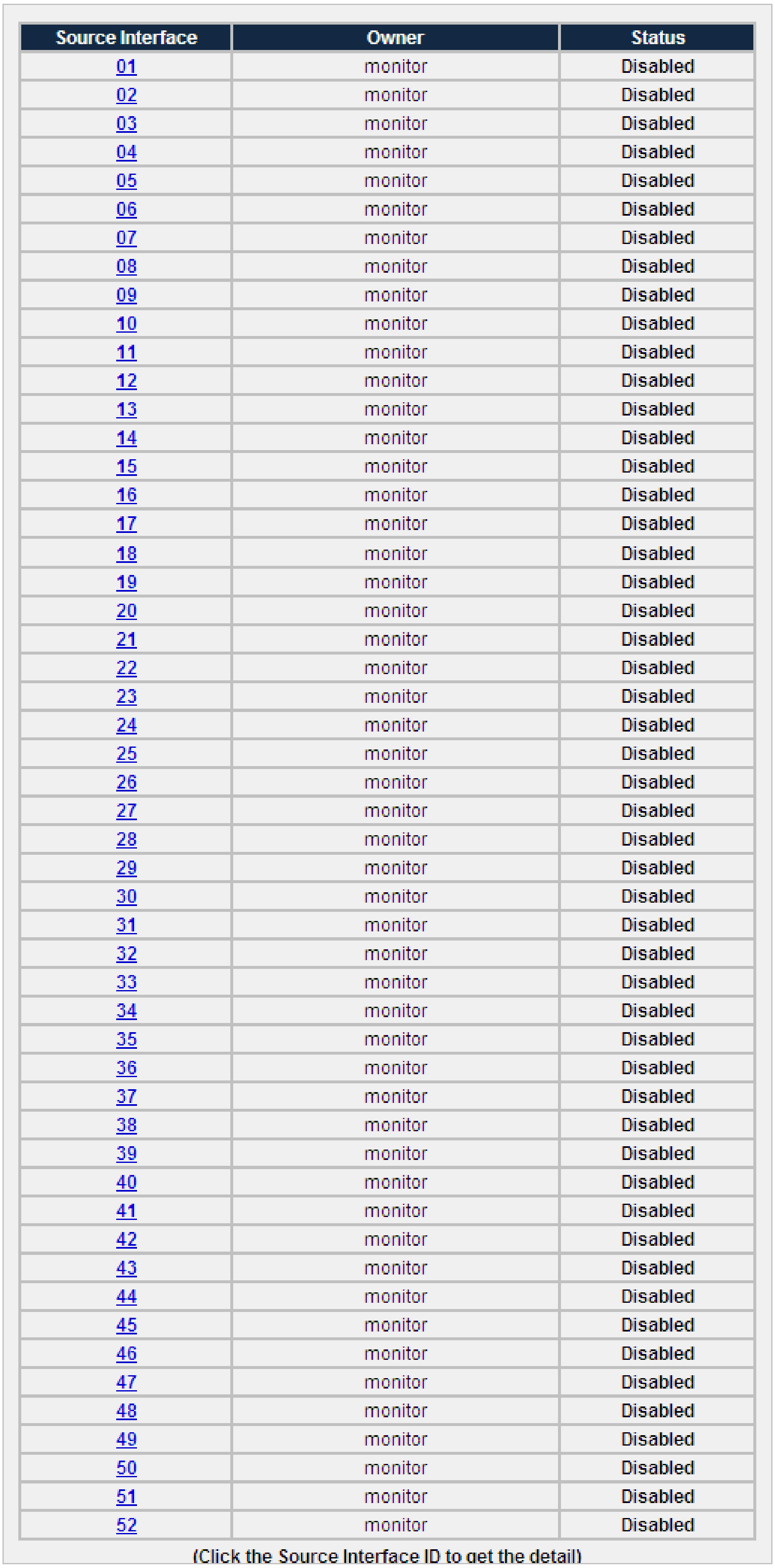
Figure 4-12-1 802.1X Statistic screenshot

The page includes the following fields:

Object	Description
• **Port**	Indicates the port number.
• **Octets Recieved**	The number of octets received on this port during the session.
• **Octets Transmitted**	The number of octets transmitted on this port during the session.
• **Session Time**	The duration of the session in seconds.
• **Termination Cause**	The reason for the session termination.T his parameter can take the following values, 1) Supplicant Logoff (1) 2) Port Failure (2) 3) Supplicant Restart (3) 4) Reauthentication Failure (4) 5) AuthControlledPortControl set to ForceUnauthorized (5) 6) Port re-initialization (6) 7) Port Administratively Disabled (7) 8) Not Terminated Yet (999)
• **User Name**	Represents the identity of the Supplicant PAE.

4.12.2 RMON Statistic

In this table overview, each entry which created for each port was listed by showing owner and status fileds. Use the port select link to select which port details to be displayed. The RMON Statistics screen in Figure 4-12-2 and Figure 4-12-3 appears.



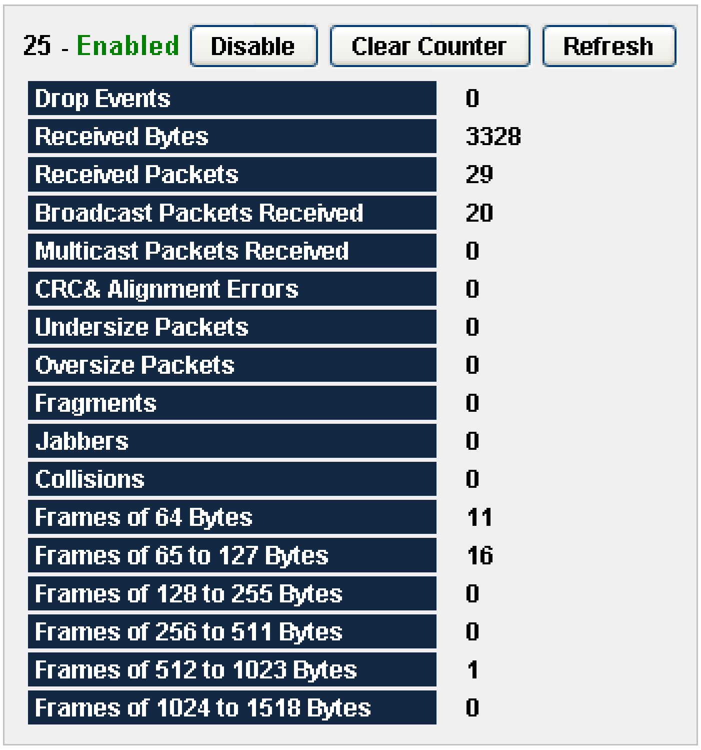
Source Interface	Owner	Status
01	monitor	Disabled
02	monitor	Disabled
03	monitor	Disabled
04	monitor	Disabled
05	monitor	Disabled
06	monitor	Disabled
07	monitor	Disabled
08	monitor	Disabled
09	monitor	Disabled
10	monitor	Disabled
11	monitor	Disabled
12	monitor	Disabled
13	monitor	Disabled
14	monitor	Disabled
15	monitor	Disabled
16	monitor	Disabled
17	monitor	Disabled
18	monitor	Disabled
19	monitor	Disabled
20	monitor	Disabled
21	monitor	Disabled
22	monitor	Disabled
23	monitor	Disabled
24	monitor	Disabled
25	monitor	Disabled
26	monitor	Disabled
27	monitor	Disabled
28	monitor	Disabled
29	monitor	Disabled
30	monitor	Disabled
31	monitor	Disabled
32	monitor	Disabled
33	monitor	Disabled
34	monitor	Disabled
35	monitor	Disabled
36	monitor	Disabled
37	monitor	Disabled
38	monitor	Disabled
39	monitor	Disabled
40	monitor	Disabled
41	monitor	Disabled
42	monitor	Disabled
43	monitor	Disabled
44	monitor	Disabled
45	monitor	Disabled
46	monitor	Disabled
47	monitor	Disabled
48	monitor	Disabled
49	monitor	Disabled
50	monitor	Disabled
51	monitor	Disabled
52	monitor	Disabled

(Click the Source Interface ID to get the detail)

Figure 4-12-2 RMON Statistic screenshot

The page includes the following fields:

Object	Description
• **Source Interface**	indicates the ethernet interface of this system.
• **Owner**	indicates the entry creator. ('Monitor' means created by device itself).
• **Status**	indicates the enable/disable status on this interface.



Drop Events	0
Received Bytes	3328
Received Packets	29
Broadcast Packets Received	20
Multicast Packets Received	0
CRC& Alignment Errors	0
Undersize Packets	0
Oversize Packets	0
Fragments	0
Jabbers	0
Collisions	0
Frames of 64 Bytes	11
Frames of 65 to 127 Bytes	16
Frames of 128 to 255 Bytes	0
Frames of 256 to 511 Bytes	0
Frames of 512 to 1023 Bytes	1
Frames of 1024 to 1518 Bytes	0

Figure 4-12-3 Port detail RMON Statistic screenshot

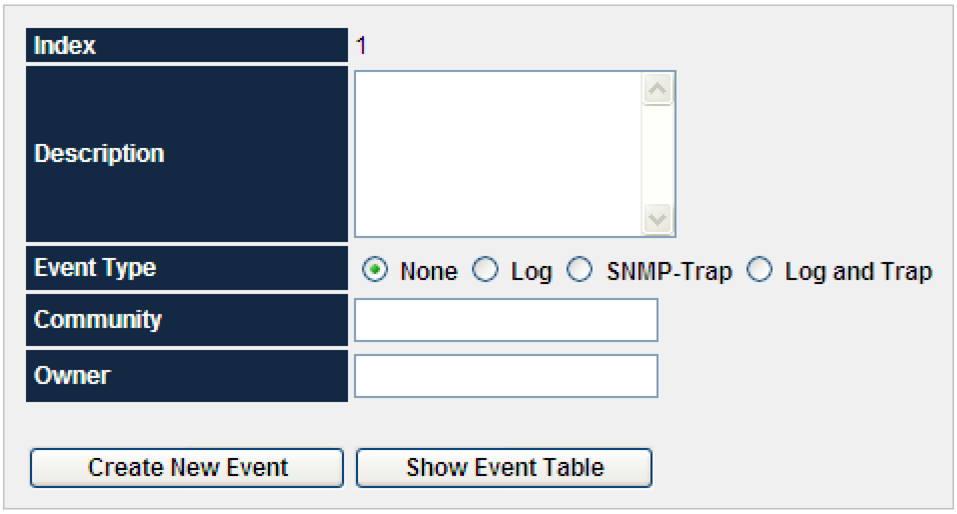
The port detail RMON statistic page includes the following fields:

Object	Description
• **Enable**	To enable/disable this interface statistics counters.
• **Clear Counter**	Clear all counters on this interface and restart by zero.
• **Refresh**	Retrieves all counters in this page.
• **Drop Events**	indicates the drop event counted value.
• **Received Bytes**	indicates the Octets(including error) counted value.
• **Received Packets**	indicates the packets(including error) counted value.
• **Broadcast Packets Received**	indicates the Broadcasts packets counted value.
• **Multicast Packets Received**	indicates the Multicast packets counted value.
• **CRC& Alignment Errors**	indicates the CRC & Alignment errors counted value.

• **Undersize Packets**	indicates the undersize packets counted value.
• **Oversize Packets**	indicates the oversize packets counted value.
• **Fragments**	indicates the fragments counted value.
• **Jabbers**	indicates the jabbers counted value.
• **Collisions**	indicates the collisions counted value.
• **Frames of 64 Bytes**	indicates the 64 bytes(and under) packets counted value.
• **Frames of 65 to 127 Bytes**	indicates the counted value which packets length are 65 to 127 bytes.
• **Frames of 128 to 255 Bytes**	indicates the counted value which packets length are 128 to 255 bytes.
• **Frames of 256 to 511 Bytes**	indicates the counted value which packets length are 256 to 511 bytes.
• **Frames of 512 to 1023 Bytes**	indicates the counted value which packets length are 512 to 1023 bytes.
• **Frames of 1024 to 1518 Bytes**	indicates the counted value which packets length are 1024 to 1518 bytes.

4.12.3 RMON Event

In this table overview, every valid entry will be listed in the same page to help user to get the overview image on each control entry setting.



Index	1
Description	
Event Type	● None ○ Log ○ SNMP-Trap ○ Log and Trap
Community	
Owner	

Figure 4-12-4 RMON Event screenshot

The page includes the following fields:

Object	Description
• **Index**	Indicate the event index value.
• **Description**	Indicates the description of the assoccicated entry.
• **Event Type**	Indicates the entry event type.[1:None, 2:Log, 3:STrap, 4:Log and Trap]

• **Community**	Indicates community for SNMP trap.
• **Last Time Sent**	Indicates the value of sysUpTime at the time this event entry last generated an event by "xxD: xxH: xxM: xxS" format.
• **Owner**	Indicates the entry creator.('Monitor' means created by device itself).
• **Delete**	Click this hyperlink to delete a specific event entry.

Note

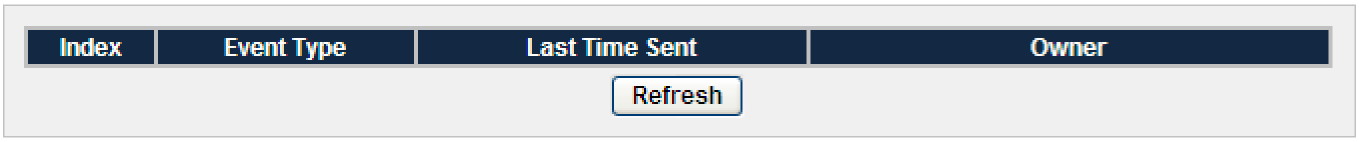
[RFC 2819]:

-- The Event group controls the generation and notification
-- of events from this device. Each entry in the eventTable
-- describes the parameters of the event that can be triggered.
-- Each event entry is fired by an associated condition located
-- elsewhere in the MIB. An event entry may also be associated
-- with a function elsewhere in the MIB that will be executed
-- when the event is generated. For example, a channel may
-- be turned on or off by the firing of an event.

4.12.4 RMON Event Log

In this table overview, every valid Event entry will be listed in the same page to help user to enter the other page to checking all the associated entries by the selected specific Event entry index.

The 'Event Index' field contains each entry's hyper link on directing to the index dependency log data page.



Index	Event Type	Last Time Sent	Owner

Figure 4-12-5 RMON Event Log screenshot

The page includes the following fields:

Object	Description
• **Index**	Indicates event entry index value.
• **Event Type**	Indicates the entry event type.[1:None, 2:Log, 3:Trap, 4:Log and Trap]
• **Last Time Sent**	Indicates the value of sysUpTime at the time this event entry last generated an event by "xxD: xxH: xxM: xxS" format.
• **Owner**	Indicates the entry creator.

Note

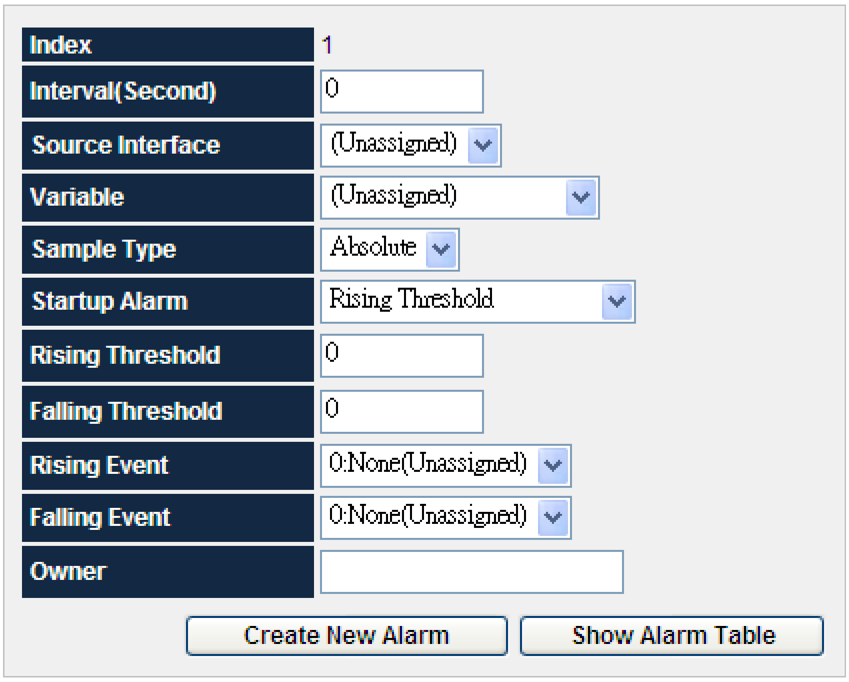
[RFC 2819]:

-- Each eventEntry may optionally specify that a log entry

-- be created on its behalf whenever the event occurs.

4.12.5 RMON Alarm

In this table overview, every valid entry will be listed in the same page to help user to get the overview image on each control entry setting.



Index	1
Interval(Second)	0
Source Interface	(Unassigned)
Variable	(Unassigned)
Sample Type	Absolute
Startup Alarm	Rising Threshold
Rising Threshold	0
Falling Threshold	0
Rising Event	0:None(Unassigned)
Falling Event	0:None(Unassigned)
Owner	

Figure 4-12-6 RMON Alarm screenshot

The page includes the following fields:

Object	Description
• **Index**	Indicates the alarm entry index value.
• **Interval(Second)**	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds.
• **Source Interface**	Indicates the port number.
• **Variable**	Indicates which etherStatistics counter per interface been assigned for alarm. The value might be (Unassigned) if the alarm entry is created but no variable been configurred and the value might be (ohter) if the value is assigned already but not in etherStatistics table with valid interface.
• **Sample Type**	Indicates the method of sampling the selected variable and calculating the value to be compared against the thresholds.
• **Startup Alarm**	Indicates the alarm that may be sent when this entry is first set to valid.

• **RisingThreshold**	Indicates a threshold for the sampled statistic.
• **FallingThreshold**	Indicates a threshold for the sampled statistic.
• **RisingEvent**	Indicates the index of the eventEntry that is used when a rising threshold is crossed. The eventEntry identified by a particular value of this index is the same as identified by the same value of the eventIndex object. If there is no corresponding entry in the eventTable, then no association exists. In particular, if this value is zero, no associated event will be generated, as zero is not a valid event index.
• **FallingEvent**	Indicates the index of the eventEntry that is used when a falling threshold is crossed. The eventEntry identified by a particular value of this index is the same as identified by the same value of the eventIndex object. If there is no corresponding entry in the eventTable, then no association exists. In particular, if this value is zero, no associated event will be generated, as zero is not a valid event index.
• **Owner**	Indicates the entry creator.

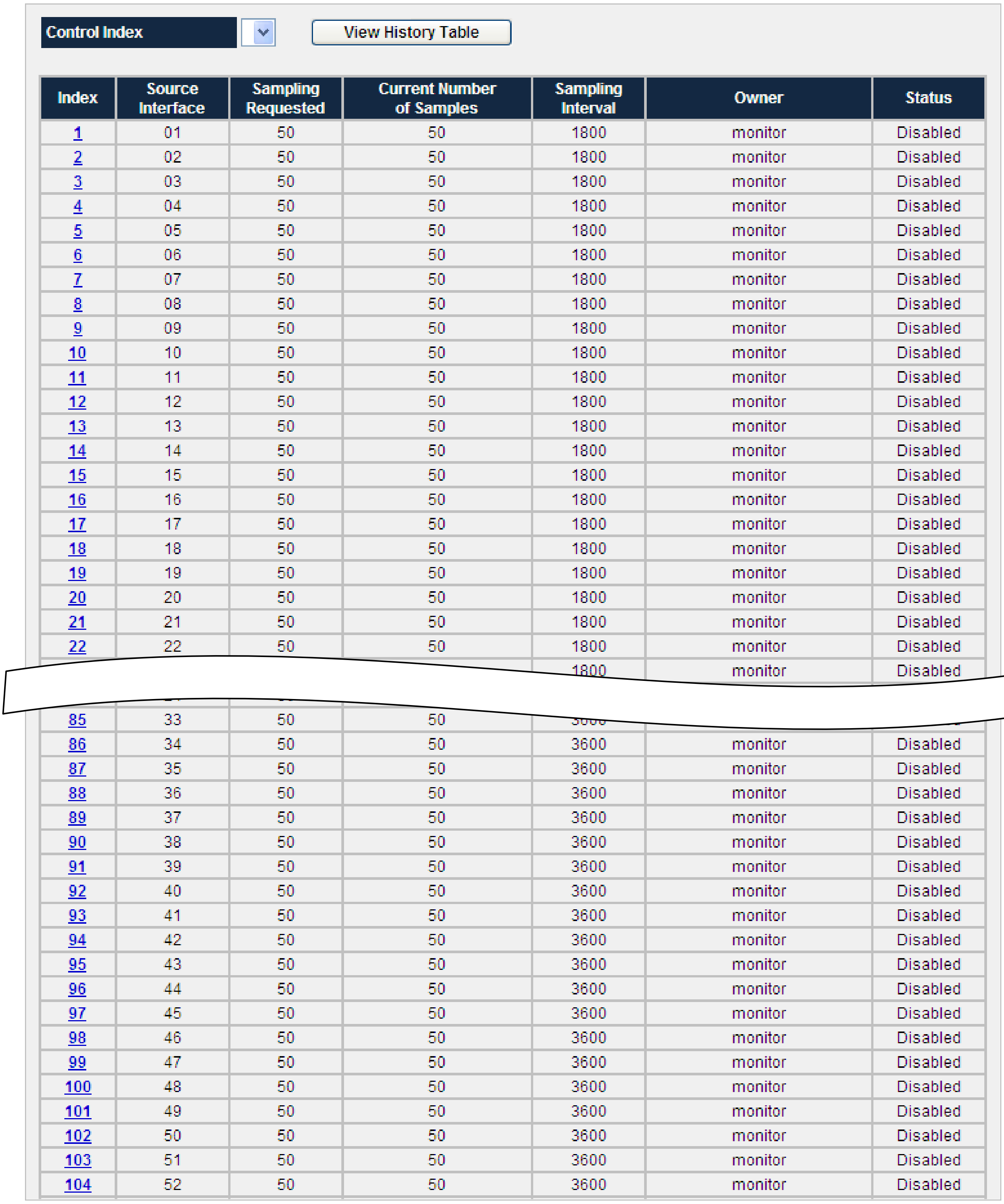
Note

[RFC 2819]:

-- The Alarm group periodically takes statistical samples from
-- variables in the probe and compares them to thresholds that have
-- been configured. The alarm table stores configuration
-- entries that each define a variable, polling period, and
-- threshold parameters. If a sample is found to cross the
-- threshold values, an event is generated.

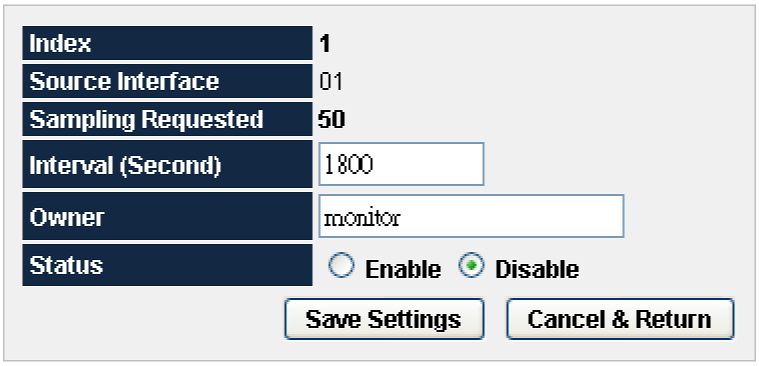
4.12.6 RMON History

In this table overview, every enabled History Control entry will be listed in the same page to help user to enter the page on checking all the sampled entries by the selected specific History Control entry index.



Index	Source Interface	Sampling Requested	Current Number of Samples	Sampling Interval	Owner	Status
1	01	50	50	1800	monitor	Disabled
2	02	50	50	1800	monitor	Disabled
3	03	50	50	1800	monitor	Disabled
4	04	50	50	1800	monitor	Disabled
5	05	50	50	1800	monitor	Disabled
6	06	50	50	1800	monitor	Disabled
7	07	50	50	1800	monitor	Disabled
8	08	50	50	1800	monitor	Disabled
9	09	50	50	1800	monitor	Disabled
10	10	50	50	1800	monitor	Disabled
11	11	50	50	1800	monitor	Disabled
12	12	50	50	1800	monitor	Disabled
13	13	50	50	1800	monitor	Disabled
14	14	50	50	1800	monitor	Disabled
15	15	50	50	1800	monitor	Disabled
16	16	50	50	1800	monitor	Disabled
17	17	50	50	1800	monitor	Disabled
18	18	50	50	1800	monitor	Disabled
19	19	50	50	1800	monitor	Disabled
20	20	50	50	1800	monitor	Disabled
21	21	50	50	1800	monitor	Disabled
22	22	50	50	1800	monitor	Disabled
				1800	monitor	Disabled
85	33	50	50			
86	34	50	50	3600	monitor	Disabled
87	35	50	50	3600	monitor	Disabled
88	36	50	50	3600	monitor	Disabled
89	37	50	50	3600	monitor	Disabled
90	38	50	50	3600	monitor	Disabled
91	39	50	50	3600	monitor	Disabled
92	40	50	50	3600	monitor	Disabled
93	41	50	50	3600	monitor	Disabled
94	42	50	50	3600	monitor	Disabled
95	43	50	50	3600	monitor	Disabled
96	44	50	50	3600	monitor	Disabled
97	45	50	50	3600	monitor	Disabled
98	46	50	50	3600	monitor	Disabled
99	47	50	50	3600	monitor	Disabled
100	48	50	50	3600	monitor	Disabled
101	49	50	50	3600	monitor	Disabled
102	50	50	50	3600	monitor	Disabled
103	51	50	50	3600	monitor	Disabled
104	52	50	50	3600	monitor	Disabled

Figure 4-12-7 RMON History screenshot



Index	1
Source Interface	01
Sampling Requested	50
Interval (Second)	1800
Owner	monitor
Status	○ Enable ● Disable

Figure 4-12-8 Port RMON History screenshot

The page includes the following fields:

Object	Description
• **Control Index**	Control entry index value.
• **Source Interface**	Indicates the ethernet interface of this system.
• **Sampling Requested**	Indicates the total numbers of sampling
• **Current Number of Samples**	Indicates how many smaple were created per this control entry.
• **Sampling Interval**	Indicates the time period on sampling etherHistory data.
• **Owner**	Indicates the entry creator.('Monitor' means created by device itself).
• **Status**	Indicates the Enabled/Disabled status.
• **History Table**	RMON History statistics consists of sampled data entries which created by RMON-lite probe. Every entry within a index key.
• **Sample**	Index indicates the index key in this control index class.
• **Drop Events**	indicates the packcet dropped counted value.
• **Octects**	indicates the Octets(including error) counted value.
• **Packets**	indicates the Received packets counted value.
• **Broadcast Packets**	indicates the Broadcasts packets counted value.
• **Multicast Packets**	indicates the Multicast packets counted value.
• **CRC & Alignment Errors**	indicates the CRC/Alignment error counted value.
• **UndersizePackets**	indicates the undersize packets counted value.
• **OversizePackets**	indicates the oversize counted value.
• **Fragments**	indicates the fragments counted value.
• **Jabbers**	indicates the jabbers counted value.

• **Collisions**	indicates the collision counted value.
• **Utilization**	indicates the counted utilication(%).

Note

[RFC 2819]:

-- The Ethernet History group records periodic statistical samples
-- from a network and stores them for later retrieval.
-- Once samples are taken, their data is stored in an entry
-- in a media-specific table. Each such entry defines one
-- sample, and is associated with the historyControlEntry that
-- caused the sample to be taken.

5. COMMAND LINE INTERFACE

5.1 Accessing the CLI

When accessing the management interface for the switch over a direct connection to the server's console port, or via a Telnet connection, the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

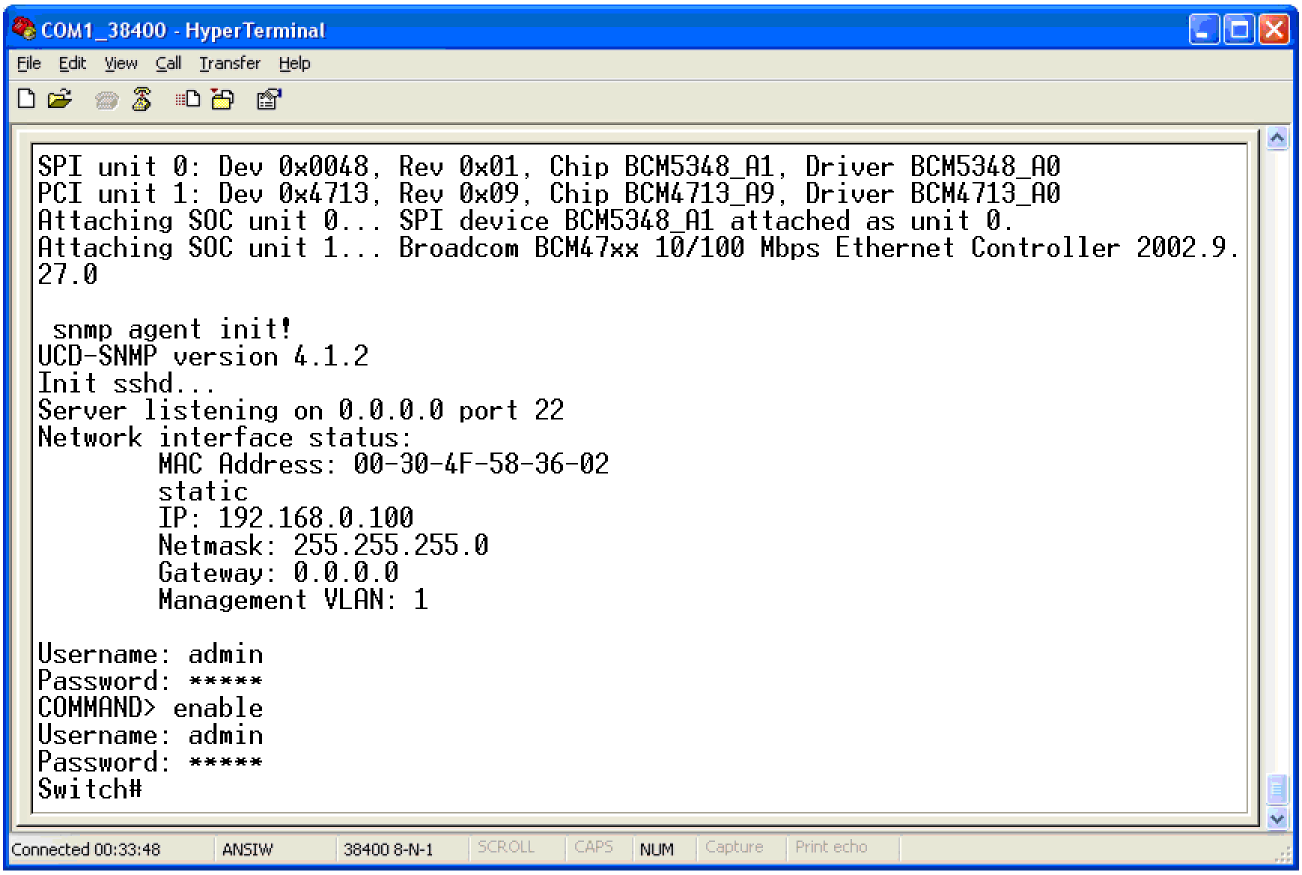
This chapter describes how to use the Command Line Interface (CLI).

Logon to the Console

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

Then, the following message asks the login password. The factory default password as following and the login screen in Figure 5-1 appears.

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



```
SPI unit 0: Dev 0x0048, Rev 0x01, Chip BCM5348_A1, Driver BCM5348_A0
PCI unit 1: Dev 0x4713, Rev 0x09, Chip BCM4713_A9, Driver BCM4713_A0
Attaching SOC unit 0... SPI device BCM5348_A1 attached as unit 0.
Attaching SOC unit 1... Broadcom BCM47xx 10/100 Mbps Ethernet Controller 2002.9.
27.0

 snmp agent init!
UCD-SNMP version 4.1.2
Init sshd...
Server listening on 0.0.0.0 port 22
Network interface status:
        MAC Address: 00-30-4F-58-36-02
        static
        IP: 192.168.0.100
        Netmask: 255.255.255.0
        Gateway: 0.0.0.0
        Management VLAN: 1

Username: admin
Password: *****
COMMAND> enable
Username: admin
Password: *****
Switch#
```

Figure 5-1 WGSW Managed Switch Console Login screen

To have access to the full suite of commands, the operator must enter the Privileged Mode. Enter "**enable**" to into the Privileged Mode and it requires password authentication. From Privileged Mode, the operator can issue any Exec command to enter the Global Configuration mode.

Command> **enable**
Username: **admin**
Password: **admin**

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.

Configure IP address

The WGSW Managed Switch is shipped with default IP address as following.

IP Address : **192.168.0.100**

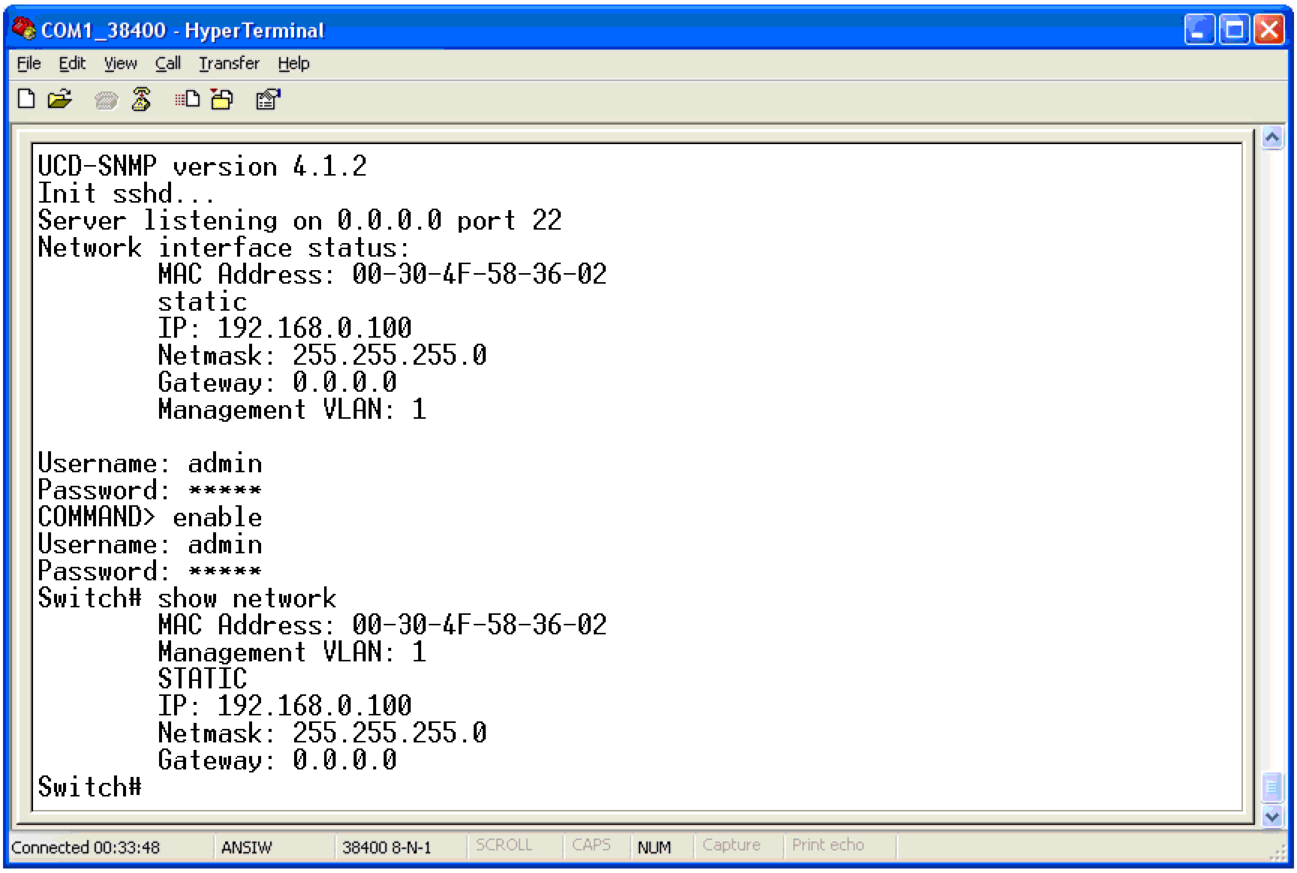
Subnet Mask : **255.255.255.0**

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

- **Show the current IP address**

1. On **"Switch# "** prompt, enter **"show network".**

2. The screen displays the current IP address, Subnet Mask and Gateway. As show in Figure 5-2.



```
UCD-SNMP version 4.1.2
Init sshd...
Server listening on 0.0.0.0 port 22
Network interface status:
        MAC Address: 00-30-4F-58-36-02
        static
        IP: 192.168.0.100
        Netmask: 255.255.255.0
        Gateway: 0.0.0.0
        Management VLAN: 1

Username: admin
Password: *****
COMMAND> enable
Username: admin
Password: *****
Switch# show network
        MAC Address: 00-30-4F-58-36-02
        Management VLAN: 1
        STATIC
        IP: 192.168.0.100
        Netmask: 255.255.255.0
        Gateway: 0.0.0.0
Switch#
```

Figure 5-2 Show IP information screen

- **Configure IP address**

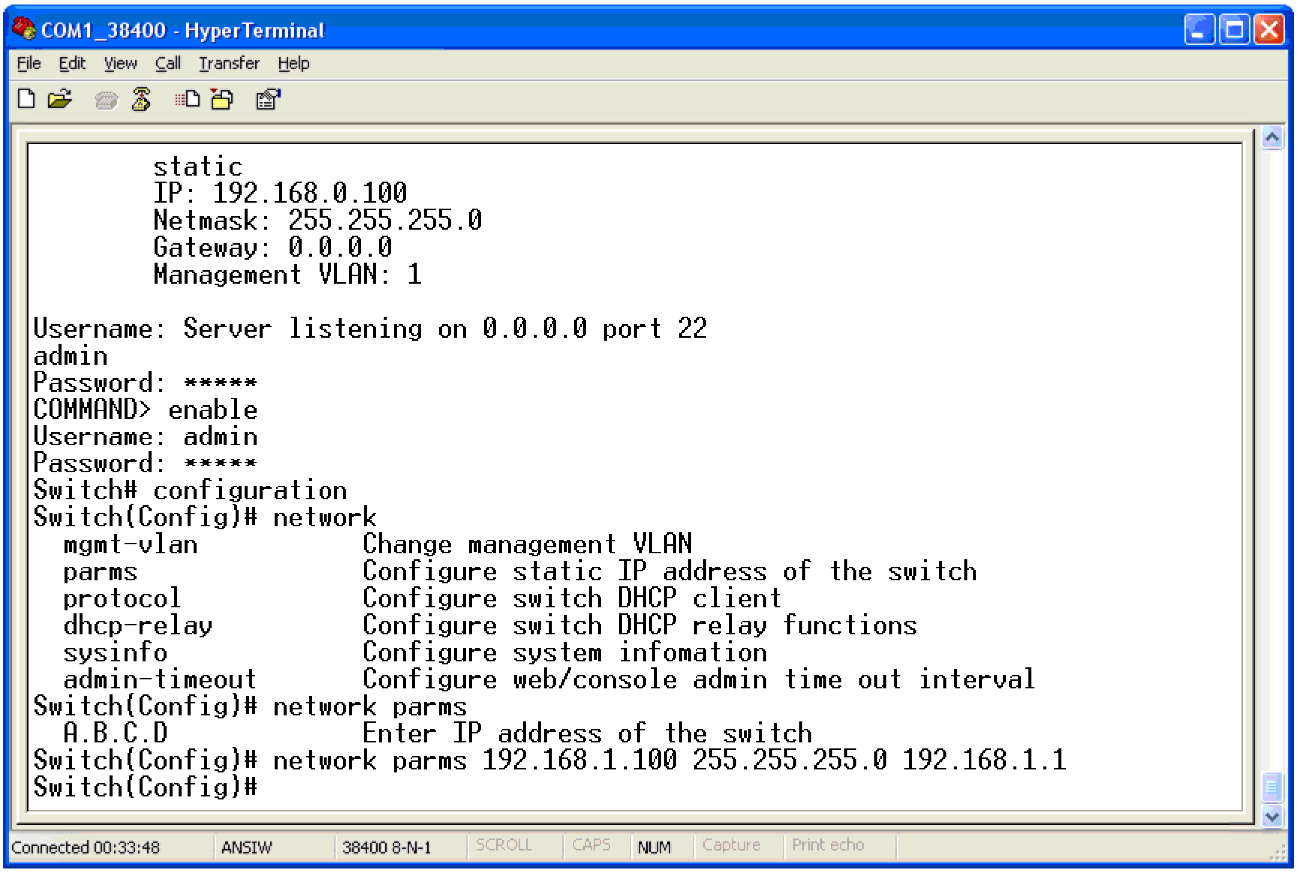
1. On "**Switch#** " prompt, type "**configuration**" to enter into global configuration mode.

2. On "**Switch(Config)#** " prompt, enter the following command and press **<Enter>.** As show in Figure 5-3.

```
Switch(Config)# network parms 192.168.1.100 255.255.255.0 192.168.1.1
```

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

IP: 192.168.1.100
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.1



```
        static
        IP: 192.168.0.100
        Netmask: 255.255.255.0
        Gateway: 0.0.0.0
        Management VLAN: 1

Username: Server listening on 0.0.0.0 port 22
admin
Password: *****
COMMAND> enable
Username: admin
Password: *****
Switch# configuration
Switch(Config)# network
  mgmt-vlan             Change management VLAN
  parms                 Configure static IP address of the switch
  protocol              Configure switch DHCP client
  dhcp-relay            Configure switch DHCP relay functions
  sysinfo               Configure system infomation
  admin-timeout         Configure web/console admin time out interval
Switch(Config)# network parms
  A.B.C.D               Enter IP address of the switch
Switch(Config)# network parms 192.168.1.100 255.255.255.0 192.168.1.1
Switch(Config)#
```

Figure 5-3 Set IP address screen

3. Repeat Step 1 to check if the IP address is changed.

4. On "**Switch#** " prompt, type "**Save**" to save the current configuration.

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

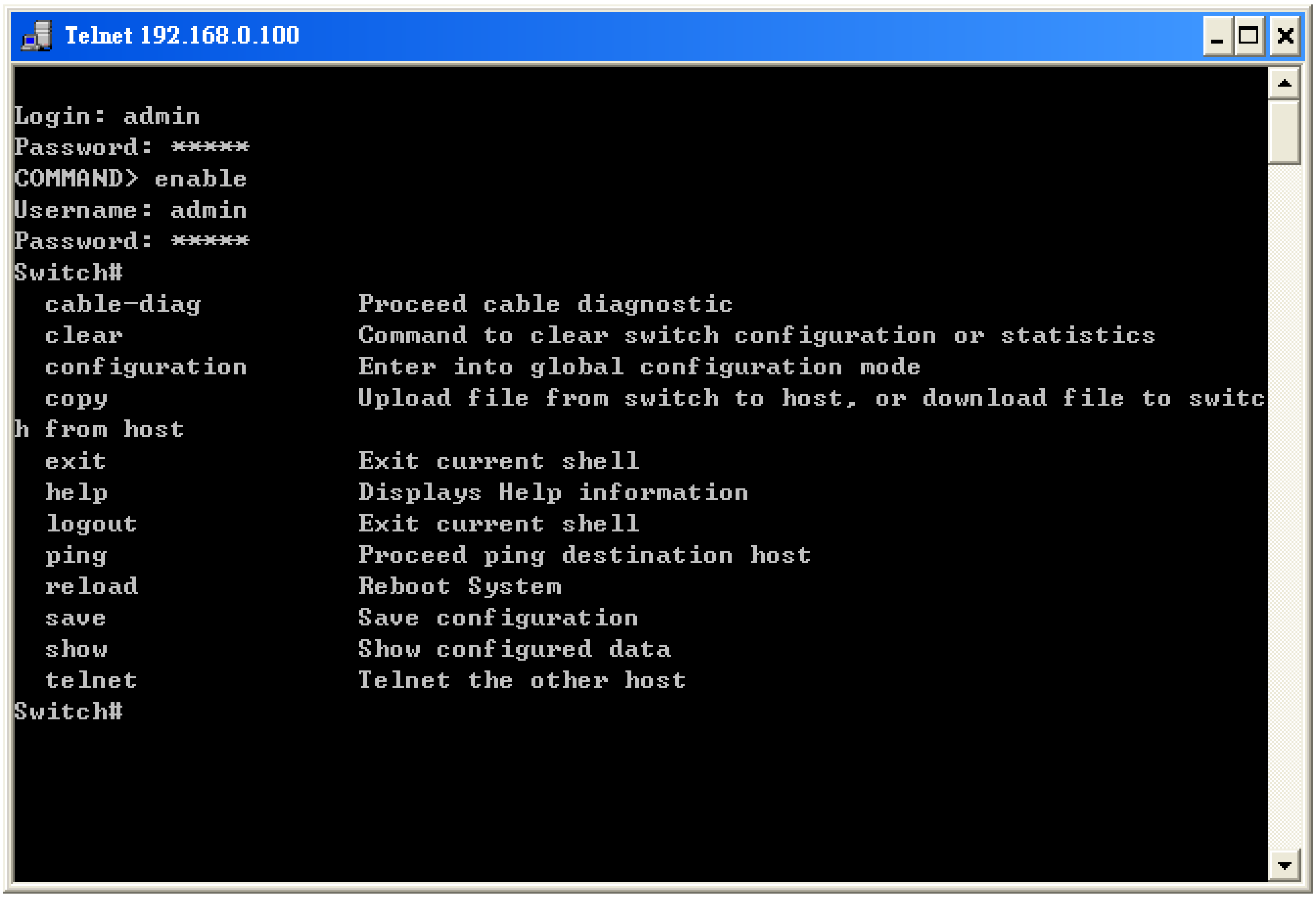
Note

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

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.

5.2 Telnet login

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



```
Login: admin
Password: *****
COMMAND> enable
Username: admin
Password: *****
Switch#
  cable-diag            Proceed cable diagnostic
  clear                 Command to clear switch configuration or statistics
  configuration         Enter into global configuration mode
  copy                  Upload file from switch to host, or download file to switc
h from host
  exit                  Exit current shell
  help                  Displays Help information
  logout                Exit current shell
  ping                  Proceed ping destination host
  reload                Reboot System
  save                  Save configuration
  show                  Show configured data
  telnet                Telnet the other host
Switch#
```

Figure 5-4 Telnet screen

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.

Command Mode	Access Method	Prompt	Exit or Access Previous Mode
User Mode	This is the first level of access. Perform basic tasks and list system information.	COMMAND>	Enter Logout command
Privileged Mode	From the User Mode, enter the enable command.	Switch#	To exit to the User Mode, enter exit or Logout.
Global Config Mode	From the Privileged Mode, enter the configuration command.	Switch (Config)#	To exit to the Privileged Mode, enter the exit command.
Interface Config Mode	From the Global Config mode, enter the interface <port#> command.	Switch (Interface <port#>)#	To exit to the Global Config mode, enter exit.

Table 6-1 CLI Command Modes

The CLI is divided into various modes. The commands in one mode are not available until the operator switches to that particular mode. The commands available to the operator at any point in time depend upon the mode. Entering a question mark (?) at the CLI prompt, and displayss a list of the available commands and descriptions of the commands.

The CLI provides the following modes:

User Mode

When the operator logs into the CLI, the User Mode is the initial mode. The User Mode contains a limited set of commands. The command prompt shown at this level is:

Command Prompt: COMMAND>

Privileged Mode

To have access to the full suite of commands, the operator must enter the Privileged Mode. The Privileged Mode requires password authentication. From Privileged Mode, the operator can issue any Exec command to enter the Global Configuration mode. The command prompt shown at this level is:

Command Prompt: Switch#

Global Config Mode

This mode permits the operator to make modifications to the running configuration. General setup commands are grouped in this mode. From the Global Configuration mode, the operator can enter the Interface Configuration mode. The command prompt at this level is:

Command Prompt: Switch(Config)#

From the Global Config mode, the operator may enter the following configuration modes:

Interface Config Mode

Many features are enabled for a particular interface. The Interface commands enable or modify the operation of an interface. In this mode, a physical port is set up for a specific logical connection operation. The command prompt at this level is:

Command Prompt: Switch(Interface <port#>)#

6.1 User Mode commands

6.1.1 Help Command

help

Description:

This command displays help information

Syntax:

help

Mode

User Mode

6.1.2 Logout Command

logout

Description:

This command is used to exit from the telnet

Syntax:

logout

Mode

User Mode

6.1.3 Ping Command

ping

Description:

This command sends echo messages.

Syntax:

ping <*A.B.C.D*>

Parameters:

<*A.B.C.D*>

Mode

User Mode

6.1.4 Show Command

show port

Description:

This command displays port status.

Syntax:

show port {<*port#*> | all}

Parameters:

{<*port#*> | all}

Mode

User Mode

show network

Description:

This command displays switch IP configuration.

Syntax:

show network

Mode

User Mode

show system

Description:

This command displays system information.

Syntax:

show system

Mode

User Mode

show port statistics

Description:

This command displays port statistics.

Syntax:

show port statistics {<*port#*> | all}

Parameters:

{<*port#*> | all}

Mode

User Mode

6.1.5 Enable Command

enable

Description:

Enter into the Privileged Mode

Syntax:

enable

Mode

User Mode

6.1.6 Save Command

save

Description:

This command is used to save configurations

6.2 Privileged Mode commands

6.2.1 Cable-diag Port Command

cable-diag port

Description:

This command is used to proceed cable diagnostic

Syntax:

cable-diag port *<port ID>*

Parameters:

<port-list> specifies the ports to be set. If not entered, all ports are set.

Mode

Privileged Mode

Example

```
Switch# cable-diag port 1
```

6.2.2 Clear Command

clear arl dynamic

Description:

This command is used to Clear dynamic arl table entries.

Syntax:

clear arl dynamic

Mode

Privileged Mode

clear arl static

Description:

This command is used to clear static arl table entries

Syntax:

clear arl static mac <mac-addr>

Parameters:

<mac-addr>

Mode

Privileged Mode

clear config

Description:

This command is used to restore switch factory default configuration.

Syntax:

clear config

Mode

Privileged Mode

clear counters

Description:

This command is used to clear RMON statistics for entire switch

Syntax:

clear counters

Mode

Privileged Mode

clear igmpsnooping

Description:

This command is used to restore igmpsnooping configuration to factory default

Syntax:

clear igmpsnooping

Mode

Privileged Mode

clear static-mcast

Description:

This command is used to clear static multicast groups

Syntax:

clear static-mcast

Mode

Privileged Mode

clear pass

Description:

This command is used to restore administrator’s password to factory default

Syntax:

clear pass

Mode

Privileged Mode

clear lacp

Description:

This command is used to restore LAG and LACP configuration to factory default

Syntax:

clear lacp

Mode

Privileged Mode

clear logs

Description:

This command is used to clear memory/flash logs

Syntax:

clear logs

Mode

Privileged Mode

clear vlan

Description:

This command is used to delete all VLAN groups

Syntax:

clear vlan

Mode

Privileged Mode

6.2.3 Configuration Command

configuration

Description:

Enter into Global Configuration mode

Syntax:

configuration

Mode

Privileged Mode

6.2.4 Copy Command

This command is used to upload file from switch to host, or download file to switch from host

copy nvram_config

Description:

This command is used to backup switch configuration

Syntax:

copy nvram_config tftp <*A.B.C.D*> file <*filename*>

Parameters:

<*A.B.C.D*> file <*filename*>

Mode

Privileged Mode

Example

```
Switch# copy nvram_config tftp 192.168.1.100 file switch_configuration
```

copy system_image

Description:

This command is used to backup switch runtime image

Syntax:

copy system_image tftp <*A.B.C.D*> <*filename*>

Parameters:

<*A.B.C.D*> <*filename*>

Mode

Privileged Mode

Example

```
Switch# copy system_image tftp 192.168.1.100 image_file
```

copy tftp

Description:

This command is used to download configuration or runtime image from host to switch.

Syntax:

copy tftp <*A.B.C.D*> file <*filename*> {nvram_config | system_image}

Parameters:

<*A.B.C.D*> file <*filename*> {nvram_config | system_image}

Mode

Privileged Mode

Example

```
Switch#copy tftp 192.168.1.100 file switch_configuration nvram_config
Switch#copy tftp 192.168.1.100 file runtime_code system_image
```

6.2.5 Exit Command

exit

Description:

This command is used to exit current shell

Syntax:

exit

Mode

Privileged Mode

6.2.6 Help Command

help

Description:

This command displayss help information

Syntax:

help

Mode

Privileged Mode

6.2.7 Logout Command

logout

Description:

This command is used to exit current shell

Syntax:

logout

Mode

Privileged Mode

6.2.8 Reload Command

reload

Description:

This command is used to reboot system

Syntax:

reload

Mode

Privileged Mode

6.2.9 Save Command

save

Description:

This command is used to save configuration

Syntax:

save

Mode

Privileged Mode

6.2.10 Show Command

This command is used to show configured data

show qos

Description:

This command displays class of service information

show qos cos

Description:

This command displays the cos mapping

Syntax:

show qos cos

Mode

Privileged Mode

show qos queue-settings

Description:

This command displays the queue-settings mapping

Syntax:

show qos queue-settings

Mode

Privileged Mode

show qos advanced

Description:

This command displays qos advanced mode information

show qos advanced mode

Description:

This command displays mode of qos

Syntax:

show qos advanced mode

Mode

Privileged Mode

show qos advanced dscp

Description:

This command displays qos dscp mapping

Syntax:

show qos advanced dscp

Mode

Privileged Mode

show qos advanced ip-precedence

Description:

This command displays qos ip precedence mapping

Syntax:

show qos advanced ip-precedence

Mode

Privileged Mode

show qos port-based

Description:

This command is used to displays class of service information

show qos port-based port

Description:

This command displays class of service information

Syntax:

show qos port-based port *<port-ID>*

Parameters:

<port-ID>

Mode

Privileged Mode

show qos port-based all

Description:

This command displays all switch interfaces' cos settings

Syntax:

show qos port-based all

Mode

Privileged Mode

show dot1x

Description:

This command displays dot1x information

show dot1x config

Description:

This command displays dot1x and port configuration

Syntax:

show dot1x config

Mode

Privileged Mode

show dot1x radius

Description:

This command displays radius configuration

Syntax:

show dot1x radius

Mode

Privileged Mode

show dot1x statistics

Description:

This command displays dot1x statistics

Syntax:

show dot1x statistics

Mode

Privileged Mode

show igmpsnooping

Description:

This command displays IGMP snooping information

show igmpsnooping dynamic_router_port

Description:

This command displays dynamic router ports information

Syntax:

show *igmp*snooping dynamic_router_port

Mode

Privileged Mode

show igmpsnooping groups

Description:

This command is used to displays *igmp* groups information

Syntax:

show igmpsnooping groups

Mode

Privileged Mode

show igmpsnooping info

Description:

This command displays IGMP Snooping configuration information

Syntax:

show igmpsnooping info

Mode

Privileged Mode

show lag

Description:

This command is used to displays link aggregation groups information

show lag lag-index

Description:

This command is used to specify an switch lag

Syntax:

show lag lag-index <lag-id>

Parameters:

<lag-id>

Mode

Privileged Mode

show lag all

Description:

This command is used to displays all switch lags

Syntax:

show lag all <lag-id>

Parameters:

<lag-id>

Mode

Privileged Mode

show lldp

Description:

This command is use to displays lldp statistics

show lldp statistic

Description:

This command is used to displays lldp statistic

Syntax:

show lldp statistic

Mode

Privileged Mode

show lldp local

Description:

This command is used to displays local information

Syntax:

show lldp local

Mode

Privileged Mode

show lldp msap

Description:

This command is used to displays msap information

Syntax:

show lldp msap

Mode

Privileged Mode

show lldp msap-entry

Description:

This command is used to displays msap details information

Syntax:

show lldp msap-entry *<1..26>*

Parameters:

<1..26>

Mode

Privileged Mode

show logging

Description:

This command is used to displays trap records

show logging memory-log

Description:

This command displays memory log

Syntax:

show logging memory-log

Mode

Privileged Mode

show logging flash-log

Description:

This command displays flash logs

Syntax:

show logging flash-log

Mode

Privileged Mode

show monitor

Description:

This command is used to displays port mirroring settings

Syntax:

show monitor

Mode

Privileged Mode

show network

Description:

This command is used to configuration for inband connectivity.

Syntax:

show network

Mode

Privileged Mode

show port

Description:

This command is used to displays port mode and settings, displays port status

show port port-index

Description:

This command is used to specify an switch interface.

Syntax:

show port port-index *<port-ID>*

Parameters:

<port-ID>

Mode

Privileged Mode

show port all

Description:

This command is used to displays all switch interface

Syntax:

show port all

Mode

Privileged Mode

show port-security

Description:

This command is used to displays port security settings

show port-security port

Description:

This command is used to specify an switch interface

Syntax:

show port-security port *<port-ID>*

Parameters:

<port-ID>

Mode

Privileged Mode

show port-security all

Description:

This command is used to displays all interfaces' status

Syntax:

show port-security all

Mode

Privileged Mode

show rate-limit

Description:

This command is used to displays ingress and egress rate limit information

show rate-limit port

Description:

This command is used to specify an switch interface

Syntax:

show rate-limit port *<port-ID>*

Parameters:

<port-ID>

Mode

Privileged Mode

Example

```
Switch#Show rate-limit port 1
Switch#Show rate-limit port g1
```

show rate-limit all

Description:

This command is used to displays all interfaces' status

Syntax:

show rate-limit all

Mode

Privileged Mode

show running-config

Description:

This command is used to displays switch running config

Syntax:

show running-config

Mode

Privileged Mode

show snmp

Description:

This command is used to displays all snmp config

show snmp groups

Description:

This command displays all snmp groups

Syntax:

show snmp groups

Mode

Privileged Mode

show snmp users

Description:

This command displays all snmp users

Syntax:

show snmp users

Mode

Privileged Mode

show snmp communities

Description:

This command displays all snmp communities

Syntax:

show snmp communities

Mode

Privileged Mode

show snmp info

Description:

This command displays all snmp information.

Syntax:

show snmp info

Mode

Privileged Mode

show sntp

Description:

This command is used to displays switch sntp information

Syntax:

show sntp

Mode

Privileged Mode

show spanning-tree

Description:

This command displayss Spanning Tree information

show spanning-tree interface

Description:

This command displays RSTP ports information

show spanning-tree interface port

Description:

This command specify an switch interface

Syntax:

show spanning-tree interface port*<port-ID>*

Parameters:

<port-ID>

Mode

Privileged Mode

show spanning-tree interface all

Description:

This command displays all switch interface

Syntax:

show spanning-tree interface all

Mode

Privileged Mode

show spanning-tree mst

Description:

This command displays MST information

show spanning-tree mst detailed

Description:

This command displays a MST instance information

Syntax:

show spanning-tree mst detailed *<0..4094>*

Parameters:

<0..4094>

Mode

Privileged Mode

show spanning-tree mst instance

Description:

This command displays ports information on a MST instance

Syntax:

show spanning-tree mst instance *<0..4094>*

Parameters:

<0..4094>

Mode

Privileged Mode

show spanning-tree mst summary

Description:

This command displays all MST instance information

Syntax:

show spanning-tree mst summary

Mode

Privileged Mode

show spanning-tree status

Description:

This command is used to displays spanning-tree status

Syntax:

show Spanning-tree status

Mode

Privileged Mode

show storm-control

Description:

This command is used to displays storm-control information

Syntax:

show storm-control

Mode

Privileged Mode

show sysinfo

Description:

This command is used to displays system information including system up time.

Syntax:

show sysinfo

Mode

Privileged Mode

show switch

Description:

This command is used to displays switch information

show switch admin-time

Description:

This command displays the age time of web and console.

Syntax:

show switch admin-time

Mode

Privileged Mode

show switch age-time

Description:

This command displays the age time of L2 table

Syntax:

show switch age-time

Mode

Privileged Mode

show switch mac-table

Description:

This command is used to displays address resolution protocol cache

show switch mac-table all

Description:

This command displays all element of the mac table.

Syntax:

show switch mac-table all

Mode

Privileged Mode

show switch mac-table vlan

Description:

This command displays all mac in a specify vlan.

Syntax:

show switch mac-table vlan <vlan-id>

Parameters:

<vlan-id>

Mode

Privileged Mode

show switch mac-table port

Description:

This command displays all mac in a specify port.

Syntax:

show switch mac-table port <port-id>

Parameters:

port <port-id>

Mode

Privileged Mode

show switch mcast-table

Description:

This command displays multicast address table

Syntax:

show switch mcast-table

Mode

Privileged Mode

show switch mac

Description:

This command displays vlan and port info by the specific mac address

Syntax:

show switch mac

Mode

Privileged Mode

show trapflags

Description:

This command is used to displays the value of trap flags that apply to the switch

Syntax:

show trapflags

Mode

Privileged Mode

show vlan

Description:

This command is used to displays vlan configuration

show vlan member

Description:

This command displays vlan configuration

Syntax:

show vlan member *<1..4094>*

Parameters:

<1..4094>

Mode

Privileged Mode

show vlan number

Description:

This command displays how many vlans has been created.

Syntax:

show vlan number

Mode

Privileged Mode

show rmon

Description:

This command displays rmon information.

show rmon event Index

Description:

This command displays rmon event table.

Syntax:

show rmon event index *<1..65535>*

Parameters:

<1..65535>

Mode

Privileged Mode

show rmon event

Syntax:

Show rmon event<CR>

Parameters:

<CR>

Mode

Privileged Mode

Show rmon event log event _index

Description:

This command displays rmon event log.

Syntax:

Show rmon event log event _index <1..65535>

Parameters:

<1..65535>

Mode

Privileged Mode

show rmon alarm index

Description:

This command displays rmon Alarm table.

Syntax:

show rmon alarm index <1..65535>

Parameters:

<1..65535>

Mode

Privileged Mode

show rmon alarm

Syntax:

show rmon alarm<CR>

Parameters:

<CR>

Mode

Privileged Mode

show rmon history index

Description:

This command displays enabled rmon history.

Syntax:

show rmon history index <1..65535>

Parameters:

<1..65535>

Mode

Privileged Mode

show rmon history

Description:

Syntax:

show rmon history <CR>

Parameters:

<CR>

Mode

Privileged Mode

show rmon statistics

Description:

This command displayss port summary statistics.

Syntax:

Show rmon statistics <port-index>

Parameters:

<port-index>

Mode

Privileged Mode

show tacplus

Description:

This command is used to displays TACACS+ information, includes authentication type and server parameters.

Syntax:

show tacplus

Mode

Privileged Mode

show arp

Description:

This command is used to displays table of static ARP.

Syntax:

show arp

Mode

Privileged Mode

show acl

Description:

This command is used to displays information about ACL entries

Syntax:

show acl

Mode

Privileged Mode

show dhcpsnooping config

Description:

This command is used to displays dhcp snooping global configuration

Syntax:

show dhcpsnooping config

Mode

Privileged Mode

show dhcpsnooping port

Description:

This command is used to displays dhcp snooping trust port.

Syntax:

show dhcpsnooping port

Mode

Privileged Mode

show dhcpsnooping vlan

Description:

This command is used to displays dhcp snooping vlan.

Syntax:

show dhcpsnooping vlan

Mode

Privileged Mode

show dhcpsnooping database

Description:

This command is used to displays dhcp snooping database entries.

show dhcpsnooping database all

Description:

This command is used to show all dhcpsnooping entries

Syntax:

show show dhcpsnooping database all

Mode

Privileged Mode

show dhcpsnooping database static

Description:

This command is used to show all dhcpsnooping static entries.

Syntax:

show dhcpsnooping database static

Mode

Privileged Mode

show dhcpsnooping database dynamic

Description:

This command is used to show all dhcpsnooping dynamic entries

Syntax:

show show dhcpsnooping database dynamic

Mode

Privileged Mode

show ipsrcgd config

Description:

This command is used to displays the configuration of IP Source Guard.

Syntax:

show ipsrcgd config

Mode

Privileged Mode

show ipsrcgd ports

Description:

This command is used to displays ports which enabled IP Source Guard

Syntax:

show ipsrcgd ports

Mode

Privileged Mode

show ipsrcgd database

Description:

This command is used to displays the database of IP Source Guard.

Syntax:

show ipsrcgd database

Mode

Privileged Mode

show https

Description:

This command is used to displays https information.

Syntax:

show https

Mode

Privileged Mode

show loop_detect

Description:

This command is used to displays selfloop detect information

Syntax:

show loop_detect

Mode

Privileged Mode

telnet

Description:

This command is used to telnet the other host.

Syntax:

telnet *<A.B.C.D>*

Parameters:

<A.B.C.D>

Mode

Privileged Mode

6.3 Global Config mode commands

6.3.1 Exit Command

exit

Description:

This command is used to exit current shell

Syntax:

exit

Mode

Global Config

6.3.2 VLAN Command

This command is used to configure vlan

vlan add

Description:

This command is used to create a new vlan or some vlans

vlan add number

Description:

This command enter a vlan ID

Syntax:

vlan add number <*vlan-ID*>

Parameters:

<*vlan-ID*>

Mode

Global Config

vlan add range

Description:

This command enter a range of vlan ID

Syntax:

vlan add range from < *vlan-ID* > to <*vlan-ID*>

Parameters:

< *vlan-ID* > to <*vlan-ID*>

Mode

Global Config

vlan delete

Description:

This command remove a existed vlan.

Syntax:

vlan delete *<vlan-ID>*

Parameters:

<vlan-ID>

Mode

Global Config

vlan ingress forward

Description:

The command is used to forward frame but don't learn SA into ARL table.

Syntax:

vlan ingress forward

Mode

Global Config

vlan ingress drop

Description:

This command is used to drop frames violation vid.

Syntax:

vlan ingress drop

Mode

Global Config

vlan ingress bypass

Description:

This command is used to forward frame and learn SA into ARL table.

Syntax:

vlan ingress bypass

Mode

Global Config

vlan port

Description:

This command is used to configure 802.1Q port parameters for vlans

vlan port all

Description:

This command is used to configure all ports

vlan port all port-configure

Description:

This command is used to configure ports in a specific vlan.

Syntax:

vlan port all port configure <*vlan-ID*>

Parameters:

<*vlan-ID*>

Mode

Global Config

vlan port all protected

Description:

This command is used to configure protected ports.

Syntax:

vlan port all protected {enable|disable}

Parameters:

{enable|disable}

Mode

Global Config

vlan port all pvid

Description:

This command is used to configure port pvid

Syntax:

vlan port all pvid <*vlan-ID*>

Parameters:

<*vlan-ID*>

Mode

Global Config

vlan port ports

Description:

This command is used to configure multiple ports

vlan port ports port-configure

Description:

This command is used to configure ports in a specific vlan

Syntax:

vlan port ports port-configure *<vlan-ID>*

Parameters:

<vlan-ID>

Mode

Global Config

vlan port ports protected

Description:

This command is used to configure protected ports.

Syntax:

vlan port ports protected {enable|disable}

Parameters:

{enable|disable}

Mode

Global Config

vlan port ports pvid

Description:

This command is used to configure port vid

Syntax:

vlan port ports pvid < *vlan-ID>*

Parameters:

< *vlan-ID>*

Mode

Global Config

vlan lag

This command is used to configure lag to a special vlan

vlan lag vlan < vlan-id> exclude

Description:

This command is used to remove lag from a vlan

Syntax:

vlan lag vlan < *vlan-ID*> exclude lags <*lag-ID*>

Parameters:

<*lag-ID*>

Mode

Global Config

vlan lag vlan <vlan-ID> untagged

Description:

This command is used to set to untagged lag.

Syntax:

vlan lag vlan <*vlan-ID*> untagged lags <*lag-ID*>

Parameters:

<*lag-ID*>

Mode

Global Config

vlan lag vlan <vlan-ID> tagged

Description:

This command is used to set to tagged lag.

Syntax:

vlan lag vlan <*vlan-ID*> tagged lags <*lag-ID*>

Parameters:

<*lag-ID*>

Mode

Global Config

6.3.3 Bridge Command

bridge

Description:

This command is used to configure switch aging time.

Syntax:

bridge aging-time <0-1048575>

Parameters:

<0-1048575>

Mode

Global Config

6.3.4 Link Aggregation Command

lacp-syspri system-priority

Description:

This command is used to configure lacp system priority

Syntax:

lacp-syspri system-priority <0-65535>

Parameters:

<0-65535>

Mode

Global Config

link-aggregation

Description:

This command is used to configure link aggregation

link-aggregation addport

Description:

This command is used to configure LAG groups.

Syntax:

Link-Aggregation addport lag <*LAG-ID*>

Parameters:

<*LAG-ID*>

Mode

Global Config

link aggregation delport

Description:

This command remove ports from LAG

Link aggregation delport all

Description:

This command remove all ports from a LAG

Syntax:

link-aggregation-delport all lag <*LAG-ID*>

Parameters:

<LAG-ID>

Mode

Global Config

link aggregation delport lag

Description:

This command remove specify LAG group.

Syntax:

link aggregation delport lag *<LAG-ID>*

Parameters:

<LAG-ID>

Mode

Global Config

6.3.5 LLDP Command

lldp enable

Description:

This command is used to enable lldp functions

Syntax:

lldp enable

Mode

Global Config

lldp disable

Description:

This command is used to disable lldp functions

Syntax:

lldp disable

Mode

Global Config

lldp adv-interval

Description:

This command is used to specify advertised interval in seconds.

Syntax:

lldp adv-interval <5-32768>

Parameters:

<5-32768>

Mode

Global Config

lldp fast-startcnt

Description:

This command is used to specify fast-start count.

Syntax:

lldp fast-startcnt *<1-10>*

Parameters:

<1-10>

Mode

Global Config

lldp hold

Description:

This command is used to specify hold value.

Syntax:

lldp hold *<2-10>*

Parameters:

<2-10>

Mode

Global Config

lldp notify-interval

Description:

This command is used to specify notification interval in seconds

Syntax:

lldp notify-interval <5-3600>

Parameters:

<5-3600>

Mode

Global Config

lldp reinit-delay

Description:

This command is used to specify re-initialization delay in seconds

Syntax:

lldp reinit-delay <1-10>

Parameters:

<1-10>

Mode

Global Config

lldp tx-delay

Description:

Transmit Delay in seconds

Syntax:

lldp tx-delay <1-8192>

Parameters:

<1-8192>

Mode

Global Config

lldp mgmt-addrtxport

Description:

A range of ports can be set.

Syntax:

lldp mgmt-addrtxport ports <port list>

Parameters:

<port list>

Mode

Global Config

Example

```
switch(config)# lldp mgmt-addrtxport ports 1
switch(config)# lldp mgmt-addrtxport ports 1-4
```

6.3.6 Log Command

log

Description:

This command is used to configure log server

log log-server

Description:

This command is used to configure log server

log log-server name <WORD> add

Description:

This command is used to specify log server name, enter a name, up to 12 characters, add a log server IP address

Syntax:

log log-server name <*WORD*> add ipaddr word

Parameters:

<*WORD*>

Mode

Global Config

log log-server name <word> delete

Description:

This command is used to delete a log server

Syntax:

log log-server name <*WORD*> delete

Parameters:

<*WORD*>

Mode

Global Config

log logging-target

Description:

This command is used to configure log notification level

log logging-target memory

Description:

This command is used to specify memory log notify-level

Syntax:

log logging-target memory {enable|disable}

Parameters:

{enable|disable}

Mode

Global Config

log logging-target flash

Description:

This command is used to specify flash log notify-level

Syntax:

log logging-target flash {enable|disable}

Parameters:

{enable|disable}

Mode

Privileged Mode

log logging-target console

Description:

This command is used to specify console log notify-level

Syntax:

log logging-target console {enable|disable}

Parameters:

{enable|disable}

Mode

Global Config

log logging-target server name <*WORD*>

Description:

This command is used to specify console log notify-level

Syntax:

log logging-target server name <*WORD*> {enable|disable}

Parameters:

{enable|disable}

Mode

Global Config

radius-server ip

Description:

This command is used to configure radius server

Syntax:

radius-server ip <*IP addr*>

Parameters:

<*IP addr*>

Mode

Global Config

static-address

This command is used to specify static address

static-address add

Description:

This command is used to add static mac address

Syntax:

static-address add <*mac addr*> vid <*vlan-ID*> port <*port-ID*>

Parameters:

<*mac addr*> vid <*vlan-ID*> port <*port-ID*>

Mode

Global Config

static-address delete

Description:

This command is used to delete static mac address

Syntax:

static-address delete <mac *addr*> vid <vlan-*ID*>

Parameters:

<mac *addr*> vid <vlan-*ID*>

Mode

Global Config

6.3.7 Mgmt Command

mgmt-accesslist ipaddr

Description:

This command specifies a management access IP for the DUT, up to 8 IP address can be set.

Syntax:

mgmt-accesslist ipaddr <*IP addr*>

Parameters:

<*IP addr*>

Mode

Global Config

mgmt-accesslist enable

Description:

This command enables management access list. Only the IP address specified in the management list is allowed to access DUT.

Syntax:

mgmt-accesslist enable

Mode

Global Config

mgmt-accesslist disable

Description:

This command disables management access list.

Syntax:

mgmt-accesslist disable

Mode

Global Config

6.3.8 Monitor Command

monitor enable

Description:

This command enables port mirroring.

Syntax:

monitor enable

Mode

Global Config

monitor disable

Description:

This command disables port mirroring.

Syntax:

monitor disable

Mode

Global Config

monitor des

Description:

Configure destination port.

monitor des <port-ID> probetype bidirection

Description:

This command configures port monitor probetype as bi-direction traffic.

Syntax:

monitor des <*port-ID*> probetype bidirection src <*port list*>

Parameters:

<*port list*>

Mode

Global Config

Example

```
Switch(config)# monitor des 1 probetype bidirection src 2-8
```

monitor des <port-ID> probetype ingress

Description:

This command configures port monitor probetype as ingress traffic.

Syntax:

monitor des <*port-ID*> probetype ingress src <*port list*>

Parameters:

<*port list*>

Mode

Global Config

Example

```
Switch(config)# monitor des 1 probetype ingress src 2-8
```

monitor des <port-ID> probetype egress

Description:

This command configures port monitor probetype as egress traffic.

Syntax:

monitor des <*port-ID*> probetype egress src <*port list*>

Parameters:

<*port list*>

Mode

Global Config

Example

```
Switch(config)# monitor des 1 probetype egress src 2-8
```

6.3.9 Dot1x Command

dot1x enable

Description:

This command enables global 802.1x function.

Syntax:

dot1x enable

Mode

Global Config

dot1x disable

Description:

This command disables global 802.1x function.

Syntax:

dot1x disable

Mode

Global Config

dot1x port-control

Description:

Configure port auto-authentication mode.

dot1x port-control enable port

Description:

This command set auto-authorized on a list of ports.

Syntax:

dot1x port-control enable port *<port list>*

Parameters:

<port list>

Mode

Global Config

dot1x port-control disable port

Description:

This command set force authorized on a list of ports.

Syntax:

dot1x port-control disable port *<port list>*

Parameters:

<port list>

Mode

Global Config

Example

```
Switch(config)# dot1x port-control disable port 1-4
```

6.3.10 Network Command

network mgmt-vlan

Description:

This command changes management vlan.

Syntax:

network mgmt-vlan *<vlan-ID>*

Parameters:

<vlan-ID>

Mode

Global Config

network parms

Description:

This command configures static IP address of the switch.

Syntax:

network parms *<IP addr> <subnet mask> <gateway>*

Parameters:

<IP addr> <subnet mask> <gateway>

Mode

Global Config

network protocol

Description:

This command configure switch dhcp client.

Syntax:

network protocol {dhcp|none}

Parameters:

{dhcp|none}

Mode

Global Config

network dhcp-relay

Description:

Configure switch dhcp relay functions.

network dhcp-relay mode

Description:

This command configures dhcp relay mode.

Syntax:

network dhcp-relay mode {enable|disable}

Parameters:

{enable|disable}

Mode

Global Config

network dhcp-relay server

Description:

This command configures dhcp-relay server ip-address.

Syntax:

network dhcp-relay server *<A.B.C.D>*

Parameters:

<A.B.C.D>

Mode

Global Config

network dhcp-relay vlan

Description:

Configure dhcp-relay option-82 vlan information.

network dhcp-relay vlan <vlan-ID> add

Description:

This command enters a vlan which will be enable DHCP-relay option82.

Syntax:

network dhcp-relay vlan <*vlan-ID*> add

Mode

Global Config

network dhcp-relay vlan <vlan-ID> remove

Description:

This command enters a vlan which will be disable dhcp-relay option82.

Syntax:

network dhcp-relay vlan <*vlan-ID*> remove

Mode

Global Config

network sysinfo

Description:

Configure switch system information.

network sysinfo sysname

Description:

This command configures system name.

Syntax:

network sysinfo sysname *<WORD>*

Parameters:

<WORD>

Mode

Global Config

network sysinfo syslocate

Description:

This command configures system location.

Syntax:

network sysinfo syslocate *<WORD>*

Parameters:

<WORD>

Mode

Global Config

network sysinfo syscontact

Description:

This command configures system contact information.

Syntax:

network sysinfo syscontact *<WORD>*

Parameters:

<WORD>

Mode

Global Config

network admin-timeout

Description:

This command configures web/console admin time out interval.

'0' means disable.

Syntax:

network admin-timeout *<0-65535>*

Parameters:

<0-65535>

Mode

Global Config

6.3.11 Port Command

port-all admin-mode

Description:

This command configures ports admin mode.

Syntax:

port-all admin-mode {enable | disable}

Parameters:

{enable | disable}

Mode

Global Config

port-all auto-negotiate

Description:

This command configures ports auto-negotiation mode.

Syntax:

port-all auto-negotiate {enable|disable}

Parameters:

{enable|disable}

Mode

Global Config

port-all flow-control

Description:

This command configures ports flow control.

Syntax:

port-all flow-control {enable|disable}

Parameters:

{enable|disable}

Mode

Global Config

port-all portsec-lockmode

Configure port security.

port-all portsec-lockmode none

Description:

This command disable port security.

Syntax:

port-all portsec-lockmode none

Mode

Global Config

port-all portsec-lockmode static

Description:

This command enable static lock mode.

Syntax:

port-all portsec-lockmode static

Mode

Global Config

port-all portsec-lockmode dynamic max-entries

Description:

This command enable limited dynamic lock mode.

Syntax:

port-all portsec-lockmode dynamic max-entries <0-24>

Parameters:

<0-24>

Mode

Global Config

port-all rate-limit

Description:

Configure rate limit value on all ports.

port-all rate-limit egress

Description:

This command specifies egress rate limit.

Syntax:

port-all Rate-Limit egress <*value*>

Parameters:

<*value*>

Mode

Global Config

port-all rate-limit ingress

Description:

This command specifies ingress rate limit.

Syntax:

port-all rate-limit ingress <*value*>

Parameters:

<*value*>

Mode

Global Config

port-all rmon-counter

Description:

This command configures rmon counter capability on ports.

Syntax:

port-all rmon-counter {enable|disable}

Parameters:

{enable|disable}

Mode

Global Config

port-all speed

Description:

This command configures ports speed.

Syntax:

port-all speed {10hd|10fd|100hd|100fd}

Parameters:

{10hd|10fd|100hd|100fd}

Mode

Global Config

port-all storm-control

Description:

Configure all ports' storm control settings.

port-all storm-control disable

Description:

This command disables storm control.

Syntax:

port-all Storm-Control disable

Mode

Global Config

port-all storm-control broadcast

Description:

This command configures storm control for broadcast only.

Syntax:

port-all storm-control broadcast <*value*>

Parameters:

<*value*>

Mode

Global Config

port-all storm-control broadcast-multicast

Description:

This command configures storm control for broadcast and multicast.

Syntax:

port-all Storm-Control broadcast-multicast <*value*>

Parameters:

<*value*>

Mode

Global Config

port-all storm-control broadcast-unknown

Description:

This command configures storm control for broadcast and unknown unicast.

Syntax:

port-all storm-control broadcast-unknown <*value*>

Parameters:

<*value*>

Mode

Global Config

port-all storm-control all-cast

Description:

This command configures storm control for broadcast, multicast and unknown unicast.

Syntax:

port-all Storm-Control all-cast <*value*>

Parameters:

<*value*>

Mode

Global Config

6.3.12 QoS Command

qos qos-advanced

Description:

Configure qos advanced mode.

qos qos-advanced DSCP

Description:

This command enables DSCP mode.

Syntax:

qos qos-advanced DSCP

Mode

Global Config

qos qos-advanced ip_precedence

Description:

This command enables IP Precedence mode.

Syntax:

qos qos-advanced ip_precedence

Mode

Global Config

qos qos-advanced none

Description:

This command disables qos advanced mode.

Syntax:

qos qos-advanced none

Mode

Global Config

qos cos priority

Description:

This command configures 802.1p priority queue mapping.

Syntax:

Qos cos priority <0-7> queue <1-4>

Parameters:

<0-7>

<1-4>

Mode

Global Config

qos dscp

Description:

This command specifies dscp value to queue mapping.

Syntax:

qos dscp <0-63> queue <1-4>

Parameters:

<0-63>

<1-4>

Mode

Global Config

qos port-based port <*WORD*>status

Description:

This command configures port-based priority mapping.

Syntax:

qos port-based port <*WORD*>status {enable | disable}

Parameters:

{enable | disable}

Mode

Global Config

qos scheduling

Configure qos scheduling mode.

qos scheduling strict

Description:

This command sets to strict priority.

Syntax:

qos scheduling strict

Mode

Global Config

qos scheduling wrr

Description:

This command sets to Weight Round-Robin.

Syntax:

qos scheduling wrr

Mode

Global Config

qos ip-precedence

Description:

This command configures IP precedence queue mapping.

Syntax:

qos ip-precedence <0-7> queue <1-4>

Parameters:

<0-7>

<1-4>

Mode

Global Config

qos wrr weight

Description:

This command configures queue weight for weight round robin.

Syntax:

qos wrr weight <1-15> queue <1-4>

Parameters:

<1-15>

<1-4>

Mode

Global Config

qos dscp-remark acl_entry_name

Description:

This command is used to change DSCP value if the outgoing packet is an IP packet. Select an ACL Entry Name as the criterion and then enter New DSCP Value as the action. Once the criterion is hit, the DSCP value will be changed.

Syntax:

qos dscp-remark acl_entry_name <name> new_dscp_value <0-63>

Parameters:

<name>

<0-63>

Mode

Global Config

6.3.13 Set Command

set igmp

Description:

Configure IGMP snooping.

set igmp enable

Description:

This command enables igmp snooping.

Syntax:

set igmp enable

Mode

Global Config

set igmp disable

Description:

This command disables IGMP snooping.

Syntax:

set igmp disable

Mode

Global Config

set igmp last-memberquery

Description:

This command specifies last member query interval.

Syntax:

set igmp last-memberquery <1-200>

Parameters:

<1-200>

Mode

Global Config

set igmp last-membercount

Description:

This command specifies last member count.

Syntax:

set igmp last-membercount <1-20>

Parameters:

<1-20>

Mode

Global Config

set igmp query-interval

Description:

This command specifies igmp query interval<secs>.

Syntax:

set igmp query-interval <10-600>

Parameters:

<10-600>

Mode

Global Config

set igmp query-resinterval

Description:

This command specifies igmp query response interval<secs>.

Syntax:

set igmp query-resinterval <0-200>

Parameters:

<0-200>

Mode

Global Config

set igmp robustness

Description:

This command specifies robustness variable.

Syntax:

set igmp robustness <1-20>

Parameters:

<1-20>

Mode

Global Config

set igmp router-port ports

Description:

This command specifies igmp router port.

Syntax:

set igmp router-port ports *<port list>*

Parameters:

<port list>

Mode

Global Config

Example

```
Switch(config)# set igmp router-port ports 1-10
```

set igmp-querier

Description:

This command configures igmp querier.

Syntax:

set igmp-querier {enable | disable}

Parameters:

{enable | disable}

Mode

Global Config

set igmp-proxy

Description:

This command configures igmp proxy.

Syntax:

set igmp-proxy {enable | disable}

Parameters:

{enable | disable}

Mode

Global Config

set static-mcast

Description:

Configure static multicast.

set static-mcast name <WORD> add vid

Description:

This command create a multicast group.

Syntax:

set static-mcast name <*WORD*> add vid <*vlan-ID*> mac <*mac-addr*>member port <*port list*>

Parameters:

<*vlan-ID*>

<*mac-addr*>

<*port list*>

Mode

Global Config

set static-mcast name <WORD>delete

Description:

This command delete a static multicast group.

Syntax:

set static-mcast name <*WORD*>delete

Mode

Global Config

6.3.14 SNMP Command

snmp notify

Description:

This command configures snmp notification.

Syntax:

snmp notify {enable|disable}

Parameters:

{enable|disable}

Mode

Global Config

snmp group add

Description:

This command create a snmp group.

Syntax:

snmp group add <*WORD*>version <1-2>

Parameters:

<*WORD*>

<1-2>

Mode

Global Config

snmp group delete

Description:

This command delete a snmp group.

Syntax:

snmp group delete <*WORD*>

Parameters:

<*WORD*>

Mode

Global Config

snmp user add

Description:

This command creates a snmp user.

Syntax:

snmp user add <*user name*> group <*group name*> version <*1-3*>

Parameters:

<*user name*>

<*group name*>

<*1-3*>

Mode

Global Config

snmp user delete

Description:

This command deletes a snmp user.

Syntax:

snmp user delete <*WORD*>

Parameters:

<*WORD*>

Mode

Global Config

snmp community add

Description:

This command creates a community.

Syntax:

snmp community add <*community name*> group <*group name*> mgmt-ip <*ip-addr*>

Parameters:

<community name>

<group name>

<ip-addr>

Mode

Global Config

snmp community delete

Description:

This command deletes a community.

Syntax:

snmp community delete *<community name>*

Parameters:

<community name>

Mode

Global Config

snmp trapstation add

Description:

Create a snmp trap station.

snmp trapstation add <ip-addr> community <community name> type bootup trap-version

Description:

Send trap when system reboot

Syntax:

snmp trapstation add <*ip-addr*> community <*community name*> type bootup trap-version {1|2}

Parameters:

{1|2}

Mode

Global Config

snmp trapstation add <ip-addr> community <community name> type linkchange trap-version

Description:

Send trap when port link change.

Syntax:

snmp trapstation add <i*p-addr*> community <*community name*> type linkchange trap-version {1|2}

Parameters:

{1|2}

Mode

Global Config

snmp trapstation add <ip-addr> community <community name> type both trap-version

Description:

Send trap when system reboot or port link change.

Syntax:

snmp trapstation add <*ip-addr*> community <*community name*> type both trap-version {1-2}

Parameters:

{1-2}

Mode

Global Config

snmp trapstation add <ip-addr> community <community name> type none trap-version

Description:

Send no trap.

Syntax:

snmp trapstation add <*ip-addr*> community <*community name*> type none trap-version {1-2}

Parameters:

{1-2}

Mode

Global Config

snmp trapstation delete

Description:

This command delete a trap station.

Syntax:

snmp trapstation delete *<WORD>*

Parameters:

<WORD>

Mode

Global Config

6.3.15 SNTP Command

sntp daylight

Description:

This command enables or disables the daylight saving configuration.

Syntax:

sntp daylight {enable|disable}

Parameters:

{enable|disable}

Mode

Global Config

sntp localtime

Description:

Configure the local time.

sntp localtime enable

Description:

This command enables local time.

Syntax:

sntp localtime enable

Mode

Global Config

sntp localtime localtime_date

Description:

This command sets local time.

Syntax:

sntp localtime localtime_date <*year*> <*month*> <*date*> <*hour*> <*minute*> <*second*>

Parameters:

<*year*>

<*month*>

<*date*>

<*hour*>

<*minute*>

<*second*>

Mode

Global Config

sntp server enable

Description:

This command enables sntp server.

Syntax:

sntp server enable

Mode

Global Config

sntp server ipaddr

Description:

This command sets sntp server IP address.

Syntax:

sntp server ipaddr <*IP-addr*>

Parameters:

<*IP-addr*>

Mode

Global Config

sntp server polling

Description:

This command sets sntp server polling time interval.

Syntax:

sntp serve polling *<0-9>*

Parameters:

<0-9>

Mode

Global Config

sntp timezone

Description:

This command sets sntp timezone.

Syntax:

sntp timezone <1-75>

Parameters:

<1-75>

Mode

Global Config

6.3.16 Spanning-tree Command

spanning-tree forceversion

Description:

This command configures Spanning Tree protocol version.

spanning-tree forceversion 8021s

Description:

This command selects spanning tree type as 802.1s(multiple Spanning Tree).

Syntax:

spanning-tree forceversion 802.1s

Mode

Global Config

spanning-tree forceversion 8021w

Description:

This command selects spanning tree type as 802.1w(rapid Spanning Tree).

Syntax:

spanning-tree forceversion 8021w

Mode

Global Config

spanning-tree forceversion none

Description:

This command selects none spanning tree type.

Syntax:

spanning-tree forceversion none

Mode

Global Config

spanning-tree configuration

Description:

This command configures MSTP region name and revision.

spanning-tree configuration name

Description:

This command configures MSTP region name (Max.32 chars).

Syntax:

spanning-tree configuration name <*WORD*>

Parameters:

<*WORD*>

Mode

Global Config

spanning-tree configuration revision

Description:

This command configures revision level.

Syntax:

spanning-trees configuration revision <0-65535>

Parameters:

<0-65535>

Mode

Global Config

spanning-tree forward-time

Description:

This configures the bridge forward delay parameter.

Syntax:

spanning-tree forward-time <4-30>

Parameters:

<4-30>

Mode

Global Config

spanning-tree max-age

Description:

This command configures the bridge max age parameter.

Syntax:

spanning-tree max-age <6-40>

Parameters:

<6-40>

Mode

Global Config

spanning-tree max-hops

Description:

This command configure the number of hops in a region.

Syntax:

spanning-tree max-hops <1-40>

Parameters:

<1-40>

Mode

Global Config

spanning-tree port all

Description:

This command specifies RSTP capability for all ports.

Syntax:

spanning-tree port all {enable |disable}

Parameters:

{enable |disable}

Mode

Global Config

spanning-tree port cost

Description:

This command configures RSTP port path cost.

Syntax:

spanning-tree port cost <0-200000000>

Parameters:

<0-200000000>

Mode

Global Config

spanning-tree port priority

Description:

This command configures RSTP port priority.

Syntax:

spanning-tree port priority <0-24>

Parameters:

<0-24>

Mode

Global Config

spanning-tree port edge

Description:

This command configures STP edge.

Syntax:

spanning-tree port edge {enable|disable} ports <port-list>

Parameters:

{enable|disable} ports <port-list>

Mode

Global Config

spanning-tree port force-p2plink

Description:

This command configures force point to point link mode on ports.

Syntax:

spanning-tree port force-p2plink {auto|enable|disable} ports <port-list>

Parameters:

{auto|enable|disable}

<port-list>

Mode

Global Config

spanning-tree port migration-check

Description:

This command Re-checks the appropriate BPDU format to send on ports.

Syntax:

spanning-tree port migration-check {enable|disable} ports <port-list>

Parameters:

{enable|disable}

<port-list>

Mode

Global Config

spanning-tree port root-guard

Description:

This command is used to configure stp root guard.

Syntax:

spanning-tree port root-guard {enable|disable} ports <port-list>

Parameters:

{enable|disable}

<port-list>

Mode

Global Config

spanning-tree priority

Description:

This command configures RSTP bridge priority value.

Syntax:

spanning-tree priority <0-61440>

Parameters:

<0-61440>

Mode

Global Config

spanning-tree mst

Description:

Configure a multiple spanning tree instance.

spanning-tree mst instance

Description:

This command creates or removes a MST instance

spanning-tree mst instance add vlan

Description:

This command creates a MST instance.

Syntax:

spanning-tree mst instance add vlan <*vlan list*> mstpid <*MST ID*>

Parameters:

<*vlan list*>

<*MST ID*>

Mode

Global Config

Example

```
Switch(Config)# Spanning-Tree mst instance add vlan 2-5 mstpid 2
Switch(Config)# Spanning-Tree mst instance add vlan 6 mstpid 3
```

spanning-tree mst instance delete

Description:

This command removes the last MST instance.

Syntax:

spanning-tree mst instance delete

Mode

Global Config

spanning-tree mst vlan

This command adds or deletes vlan frome a MSTP instance.

spanning-tree mst vlan <MST ID> <vlan list> add

Description:

This command creates a MST instance.

Syntax:

spanning-tree mst vlan <*MST ID*> <*vlan list*> add

Mode

Global Config

Example

```
Switch(Config)# Spanning-Tree mst vlan 3 3-5 add
```

spanning-tree mst vlan <MST ID> <vlan list> delete

Description:

This command deletes a vlan from a MST instance.

Syntax:

Spanning-Tree mst vlan <*MST ID*> < vlan *list*> delete

Mode

Global Config

spanning-tree mst bridgepri

Description:

This command configures bridge priority for a MST instance.

Syntax:

spanning-tree mst bridgepri <*MST ID*> <*priority*>

Parameters:

<*MST ID*>

<*priority*>

Mode

Global Config

spanning-tree mst cost

Description:

This command configures port path cost in a MST instance.

Syntax:

spanning-tree mst cost <*MST ID*> <*path cost*> ports <*port list*>

Parameters:

<*MST ID*>

<*path cost*>

<*port list*>

Mode

Global Config

spanning-tree mst priority

Description:

This command configures port priority in a MST instance.

Syntax:

spanning-tree mst priority <*MST ID*> <*priority*> ports <*port list*>

Parameters:

<*MST ID*>

<*priority*>

<*port list*>

Mode

Global Config

user password

Description:

This command changes user password.

Syntax:

user password

Mode

Global Config

Interface

Description:

This command enters into configure interface mode.

Syntax:

Interface *<port-ID>*

Parameters:

<port-ID>

Mode

Global Config

6.3.17 RMON Command

rmon

Description:

This command is used to configure RMON.

rmon event index

Description:

This command creates rmon event entry.

Syntax:

rmon event index < *1..65535* > desc <*WORD*> event <*1..4*> community <*WORD*>owner<*WORD*>

Parameters:

< *1..65535* >

<*WORD*>

<*1..4*>

Mode

Global Config

Example

```
Switch(Config)# rmon event index 1 desc 123 event 4 community 123 owner test
```

rmon alarm index

Description:

This command creates rmon alarm entry.

Syntax:

rmon alarm index < 1..65535 >interval<0..3600>interface<port number>counter<1..17>sample{absolute|delta}start{rasing|falling|all}rthreshold<0..65535>fthreshold<*0..65535*> reindex <*0..65535*> feindex<*0..65535*> owner< *WORD*>

Mode

Global Config

Example

```
Switch(Config)# RMON alarm index 1 interval 10 interface   counter 1 sample delta start all
rthreshold 100   fthreshold 10 reindex 1 feindex 0 owner test
```

rmon del event index

Description:

This command deletes rmon event entry.

Syntax:

rmon del event index< 1..65535 >

Parameters:

< 1..65535 >

Mode

Global Config

rmon del alarm index

Description:

This command deletes rmon alarm entry.

Syntax:

rmon del alarm index< 1..65535 >

Parameters:

< 1..65535 >

Mode

Global Config

6.3.18 Access List Command

access-list name <WORD> add priority

Description:

This command creates a new access-list.

Syntax:

access-list name <*WORD*> add priority <1-65535>

Parameters:

<1-65535>

Mode

Global Config

access-list name <WORD> action deny

Description:

This command denies an ACL entry.

Syntax:

access-list name <*WORD*> action deny

Mode

Global Config

access-list name <WORD> action permit

Description:

This command permits an ACL entry and queue 1-4 will assign priority queue when rule activated.

Syntax:

access-list name <*WORD*> action permit {<cr>|queue <1-4>}

Parameters:

{<cr>|queue <1-4>}

Mode

Global Config

access-list name <WORD> clear

Description:

This command clears ACL entry contents.

access-list name <WORD> clears SRC IP

Description:

This command clears the source IP/subnet mask filter.

Syntax:

access-list name <*WORD*> clear SRC IP

Mode

Global Config

access-list name <WORD> clears DST IP

Description:

This command clears the destination IP/subnet mask filter.

Syntax:

access-list name <*WORD*> clear DST IP

Mode

Global Config

access-list name <WORD> clear L4port SRC port

Description:

This command clears TCP/UDP source port filter.

Syntax:

access-list name <*WORD*> clear l4port SRC port

Mode

Global Config

access-list name <WORD> clear l4port DST port

Description:

This command clears TCP/UDP destination port filter.

Syntax:

access-list name <*WORD*> clear l4port DST port

Mode

Global Config

access-list name <WORD> clear packet-type

Description:

This command clears packet type filter.

Syntax:

access-list name <*WORD*> clear packet-type

Mode

Global Config

access-list name <WORD> clear mac SA

Description:

This command clears a source mac address.

Syntax:

Access-list name <*WORD*> clear mac SA

Mode

Global Config

access-list name <WORD> clear MAC DA

Description:

This command clears a destination mac address.

Syntax:

Access-list name <*WORD*> clear mac DA.

Mode

Global Config

access-list name <WORD> clear VID

Description:

This command clears the 802.1Q VLAN tag of packet.

Syntax:

Access-list name <*WORD*> clear VID

Mode

Global Config

access-list name <WORD> clear ether-type

Description:

This command clears ether type filter.

Syntax:

access-list name <*WORD*> clear ether-type

Mode

Global Config

access-list name <WORD> deletes

Description:

This command removes the ACL entry.

Syntax:

access-list name <*WORD*> deletes

Mode

Global Config

access-list name <WORD> {enable|disable}

Description:

This command enables/disables the ACL entry.

Syntax:

access-list name <*WORD*> {enable|disable}

Mode

Global Config

access-list name <WORD> set priority

Description:

This command specifies ACL entry priority.

Syntax:

access-list name <*WORD*> set priority <0-65535>

Parameters:

<0-65535>

Mode

Global Config

access-list name <WORD> set IP-mode SRC IP.

Description:

This command specifies a source IP address.

Syntax:

access-list name <*WORD*> set IP-mode SRC IP <IP-addr> <*mask-addr*>

Parameters:

<IP-addr>

<*mask-addr*>

Mode

Global Config

access-list name <WORD> set IP-mode DST IP

Description:

This command specifies a destination IP address.

Syntax:

access-list name <*WORD*> set IP-mode DSP IP <*IP-addr*> <*mask-addr*>

Parameters:

<IP-addr>

<*mask-addr*>

Mode

Global Config

access-list name <WORD> set L4port

Description:

This command specifies the TCP/UDP port range.

access-list name <WORD> set l4port SRC-port SRE-port

Description:

This command specifies the source TCP/UDP port range.

Syntax:

Access-list name <*WORD*> set L4 port SRE-port from <1-65535> to <1-65535>

Parameters:

<1-65535>

Mode

Global Config

access-list name <WORD> set l4port DST-port

Description:

This command specifies the destination TCP/UDP port range.

Syntax:

access-list name <*WORD*> set l4port DST-port from <1-65535> to <1-65535>

Parameters:

<1-65535>

Mode

Global Config

access-list name <WORD> set IP-mode packet-type

Description:

This command specifies the packet type.

Syntax:

access-list name <*WORD*> set IP-mode packet-type {ICMP|IGMP|IP|TCP|UDP|GRE}

Parameters:

{ICMP|IGMP|IP|TCP|UDP|GRE}

Mode

Global Config

access-list name <WORD> set mac-mode

Description:

Specify ACL entry priority.

access-list name <WORD> set mac-mode mac SA

Description:

This command specifies a source mac address.

Syntax:

access-list name <*WORD*> set mac-mode mac SA <mac-addr> <mask-addr>

Parameters:

<mac-addr>

<mask-addr>

Mode

Global Config

access-list name <WORD> set mac-mode mac DA

Description:

This command specifies a destination mac address.

Syntax:

access-list name <*WORD*> set mac-mode mac DA <*mac-addr*> <*mask-addr*>

Parameters:

<mac-addr>

<mask-addr>

Mode

Global Config

access-list name <WORD> set mac-mode ether-type

Description:

This command specifies the ether type of the packet.

Syntax:

access-list name <*WORD*> set mac-mode ether-type {ipv4|ARP|xns}

Parameters:

{ipv4|ARP|xns}

Mode

Global Config

access-list name <name> set portlist

Description:

This command is used to specify an acl entry to be work on a list of ports.

Syntax:

access-list name <name> set portlist <LINE | port_id>

Parameters:

<LINE | port_id>

Mode

Global Config

6.3.19 ARP Command

arp dynamic

Description:

This command enables and disables dynamic arp functions.

Syntax:

arp dynamic {enable|disable}

Parameters:

{enable|disable}

Mode

Global Config

arp dynamic aging-time

Description:

This command set arp dynamic aging-time between 0s and 999s."0"means disable.

Syntax:

arp dynamic aging-time <0~999>

Parameters:

<0~999>

Mode

Global Config

arp dynamic ports

Description:

This command set dynamic arp ports to trust and un-trust.

Syntax:

arp dynamic ports {trust|untrust} <port-list>

Parameters:

{trust|untrust}

<port-list>

Mode

Global Config

Example

```
Swtich<Config># arp dynamic ports trust 1-4
Swtich<Config># arp dynamic ports untrust 4
```

arp dynamic vlan

Description:

This command set add/remove dynamic arp on specified vlan.

Syntax:

arp dynamic vlan {add|remove} from < vlan -id> to < vlan -id>

Parameters:

{add|remove}

< vlan -id>

Mode

Global Config

Example

```
Swtich<Config># arp dynamic vlan add from 1 to 1
Swtich<Config># arp dynamic vlan remove from 1 to 1
```

arp static

Description:

This command set arp static address table for mac address with IP Address.

Syntax:

arp static {add|delete} vid <1~4094> ip <A.B.C.D> mac <mac-address>

Parameters:

{add|delete}

<1~4094>

<A.B.C.D>

<mac-address>

Mode

Global Config

6.3.20 Dos Command

dos land

Description:

This command enables and disables land-type attacks prevention.

Syntax:

dos land {enable|disable}

Parameters:

{enable|disable}

Mode

Global Config

dos blat

Description:

This command enables and disables blat-type attack prevention.

Syntax:

dos blat {enable|disable}

Parameters:

{enable|disable}

Mode

Global Config

dos syn-fin

Description:

This command enables and disables SYN-fin-type attack prevention.

Syntax:

dos syn-fin {enable|disable}

Parameters:

{enable|disable}

Mode

Global Config

dos ports smurf

Description:

This command enables and disables Smurf-TYPR attack prevention.

Syntax:

dos ports smurf {enable|disable}

Parameters:

{enable|disable}

Mode

Global Config

dos ports ping-flooding

Description:

This command enables and disables ping-flooding-type attack prevention.

Syntax:

dos ports ping-flooding {enable|disable}

Parameters:

{enable|disable}

Mode

Global Config

dos ports synack-flooding

Description:

This command enables and disables SYNACK -flooding -type attack prevention. Set rate is 64 kbps or 128kbps for port lists (1, 3-5, 7-9.11)

Syntax:

dos ports synack -flooding {enable|disable} rate {64|128} <port-list>

Parameters:

{enable|disable}

{64|128}

<port-list>

Mode

Global Config

Example

```
Switch<Config>#dos ports synack -flooding enablerate 64 1-4
Switch<Config>#dos ports synack -flooding enablerate 64 5
```

6.3.21 Tacplus Command

tacplus authen_type

Description:

This command is used to set authentication type. There are three types for selecting: local, tacplus, localandtacplus.

Syntax:

tacplus authen_type {local | tacplus | localandtacplus}

Parameters:

{local | tacplus | localandtacplus}

Mode

Global Config

tacplus add server

Description:

This command is used to add a new TACACS+ server and set server IP address, priority, key string, authentication port and timeout for reply.

Syntax:

tacplus add server <IP_addr> priority <0-65535> key <key string> port <auth port id> timeout <1-30>

Parameters:

<IP_addr>

<0-65535>

<key string>

<auth port id>

<1-30>

Mode

Global Config

tacplus del server

Description:

This command is used to delete a TACACS+ server.

Syntax:

tacplus del server <IP_addr>

Parameters:

<IP_addr>

Mode

Global Config

6.3.22 DHCP Snooping Command

dhcpsnooping enable

Description:

This command is used to enable dhcp snooping functions.

Syntax:

dhcpsnooping enable

Mode

Global Confi

dhcpsnooping disable

Description:

This command is used to disable dhcp snooping functions.

Syntax:

dhcpsnooping disable

Mode

Global Config

dhcpsnooping option82

Description:

This command is used to set option82 packets.

Syntax:

dhcpsnooping option82 {enable|disable}

Parameters:

{enable|disable}

Mode

Global Config

dhcpsnooping verifymac

Description:

This command is used to set verify mac address.

Syntax:

dhcpsnooping verifymac{enable|disable}

Parameters:

{enable|disable}

Mode

Global Config

dhcpsnooping ports

Description:

This command is used to set ports to trust or untrust.

dhcpsnooping ports trust

Description:

This command is used to set ports to trust

Syntax:

dhcpsnooping ports trust <port-list>

Parameters:

<port-list>

Mode

Global Config

dhcpsnooping ports untrust

Description:

This command is used to set ports to untrust

Syntax:

dhcpsnooping ports untrust <port-list>

Parameters:

<port-list>

Mode

Global Config

dhcpsnooping vlan

Description:

This command is used to configure dhcp vlan.

dhcpsnooping vlan add

Description:

This command is used to enable dhcp snooping in a specified vlan.

Syntax:

dhcpsnooping vlan add from <vlan-id> to <vlan-id>

Parameters:

<vlan-id>

Mode

Global Config

dhcpsnooping vlan remove

Description:

This command is used to disable dhcp snooping in a specified vlan.

Syntax:

dhcpsnooping vlan remove from <vlan-id> to <vlan-id>

Parameters:

<vlan-id>

Mode

Global Config

dhcpsnooping static

Description:

This command is used to configure dhcp static entry.

dhcpsnooping static add ip

Description:

This command is used to add a static dhcp entry.

Syntax:

dhcpsnooping static add ip <A.B.C.D> mac <mac-address> port <port-id> vid <vlan-id>

Parameters:

<A.B.C.D>

<mac-address>

<port-id>

<vlan-id>

Mode

Global Config

dhcpsnooping static delete ip

Description:

This command is used to delete a static dhcp entry.

Syntax:

dhcpsnooping static delete ip <A.B.C.D> mac <mac-address> port <port-id> vid <vlan-id>

Parameters:

<A.B.C.D>

<mac-address>

<port-id>

<vlan-id>

Mode

Global Config

dhcpsnooping dyamic

Description:

This command is used to configure dhcp dynamic entry.

dhcpsnooping dynamic add ip

Description:

This command is used to add a dynamic dhcp entry.

Syntax:

dhcpsnooping dynamic add ip <A.B.C.D> mac <mac-address> port <port-id> vid <vlan-id> lease-time <1..9999999>

Parameters:

<A.B.C.D>

<mac-address>

<port-id>

<vlan-id>

Mode

Mode Global Config

dhcpsnooping dynamic delete ip

Description:

This command is used to delete a dynamic dhcp entry.

Syntax:

dhcpsnooping dynamic delete ip <A.B.C.D> mac <mac-address> port <port-id> vid <vlan-id> lease-time <1...9999999>

Parameters:

<A.B.C.D>

<mac-address>

<port-id>

<vlan-id>

Mode

Global Config

6.3.23 Loop_detect Command

Loop_detect enable

Description:

This command is used to enable port self-loop detection.

Syntax:

loop_detect enable

Mode

Global Config

loop_detect disable

Description:

This command is used to disable port self-loop detection.

Syntax:

loop_detect disable

Mode

Global Config

loop_detect recovertime

Description:

This command is used to set the recover time.

Syntax:

loop_detect recovertime <0…65535>

Parameters:

<0…65535>

Mode

Global Config

loop detect trytorecover

Description:

This command is used to try to recover all the selfloop port immediately

Syntax:

loop_detect trytorecover

Mode

Global Config

6.3.24 GVRP Command

gvrp enable

Description:

This command is used to enable gvrp function globally.

Syntax:

gvrp enable

Mode

Global Config

gvrp disable

Description:

This command is used to disable gvrp function globally.

Syntax:

gvrp disable

Mode

Global Config

gvrp port_enable

Description:

This command is used to enable gvrp function on a specified port .

Syntax:

gvrp port_enable <port-id>

Parameters:

<port-id>

Mode

Global Config

gvrp port_disable

Description:

This command is used to disable gvrp function on a specified port .

Syntax:

gvrp port_disable <port-id>

Parameters:

<port-id>

Mode

Global Config

gvrp port_status

Description:

This command is used to displays the gvrp port information.

Syntax:

gvrp port_status <port-list>

Parameters:

<port-list>

Mode

Global Config

6.3.25 HTTPs Command

https

Description:

This command is used to set https enable or disable.

Syntax:

https { enable | disable }

Parameters:

{ enable | disable }

Mode

Global Config

6.3.26 BOOTP Command

bootp enable

Description:

This command is used to enable bootp function.

Syntax:

bootp enable

Mode

Global Config

bootp disable

Description:

This command is used to disable bootp function.

Syntax:

bootp disable

Mode

Global Config

bootp renew

Description:

This command is used to renew bootp.

Syntax:

bootp renew

Mode

Global Config

6.3.27 SSH Command

ssh enable

Description:

This command is used to enable ssh function.

Syntax:

ssh enable

Mode

Global Config

ssh disable

Description:

This command is used to disable ssh function.

Syntax:

ssh disable

Mode

Global Config

ssh changekey

Description:

This command is used to change key function.

Syntax:

ssh changekey

Mode

Global Config

6.3.28 IP Source Guard Command

ipsrcgd enable

Description:

This command is used to enable ip source guard function.

Syntax:

ipsrcgd enable

Mode

Global Config

ipsrcgd disable

Description:

This command is used to disable ip source guard function.

Syntax:

ipsrcgd disable

Mode

Global Config

ipsrcgd ports

Description:

This command is used to configure ports to enable or disable ip source guard.

Syntax:

ipsrcgd ports {enable|disable}

Parameters:

{enable|disable}

Mode

Global Config

ipsrcgd retry

Description:

This command is used to configure the retry mechanism of ip source guard database.

ipsrcgd retry now

Description:

This command is used to retry inactive entries now.

Syntax:

ipsrcgd retry now

Mode

Global Config

ipsrcgd retry interval

Description:

This command is used to retry inactive entries after a interval.

Syntax:

ipsrcgd retry interval <0-1440>

Parameters:

<0-1440>

Mode

Global Config

6.4 Interface Config mode commands

6.4.1 Exit Command

exit

Description:

Exit current shell

Syntax:

exit

Mode

Interface Config

6.4.2 dot1x Command

Set 802.1x port control.

Description:

Set auto-authorized or force authorized on ports

Syntax:

802.1x port-control {enable|disable}

Parameters:

{enable|disable}

Mode

Interface Config

6.4.3 LACP Command

lacp admin

Description:

Configure admin key of port

Syntax:

lacp admin <0 ..65535>

Parameters:

<0 ..65535>

Mode

Interface Config

Example

```
switch(interface g1)#lacp admin 36768
```

lacp priority

Description:

Configure lacp port priority

Syntax:

lacp priority <0..65535>

Parameters:

<0..65535>

Mode

Interface Config

addport

Description:

add one port to a LAG group

Syntax:

addport *<LAG-ID>*

Parameters:

<LAG-ID>

Mode

Interface Config

delport

Description:

Remove a port from a LAG group

Syntax:

delport *<LAG-ID>*

Parameters:

<LAG-ID>

Mode

Interface Config

6.4.4 LLDP Command

An lldp agent can transmit information about the capabilities and current status of the system associated with its MSAP identifier. The lldp agent can also receive information about the capabilities and current status of the system associated with a remote MSAP identifier. However, lldp agents are not provided any means of soliciting information from other lldp agents via this protocol.

lldp state

Description:

Only transfer the lldp status

Syntax:

lldp state {tx | rx | tx_rx | disable}

Parameters:

{tx | rx | tx_rx | disable}

Mode

Interface Config

lldp notifications

Description:

Enable/disable notification form the agent

Syntax:

lldp notification {enable|disable}

Parameters:

{enable|disable}

Mode

Interface Config

lldp tlvs-tx

Syntax:

lldp tlvs-tx {enable | disable} option basic {port-desc | sys-name | sys-desc | sys-capa }

Parameters:

{enable | disable}

{port-desc | sys-name | sys-desc | sys-capa }

Mode

Interface Config

802.1 set

Description:

Status of local-802.1 settings

Syntax:

lldp tlvs-tx {enable | disable} option **8021** {pvid | vlanname | protocol-id}

Parameters:

{enable | disable}

{pvid | vlanname | protocol-id}

Mode

Interface Config

Example

```
switch(interdface 1)#lldp tlvs enable option 8021 pvid 1
```

802.3 set

Syntax:

lldp tlvs-tx {enable | disable} option **8023** {mac-phy | power| link-aggregation| frame-size}

Parameters:

{enable | disable}

{mac-phy | power| link-aggregation| frame-size}

Mode

Interface Config

6.4.5 Port Command

admin-mode

Description:

Configure administrative mode on a port

Syntax:

Switch(Interface 1)# **admin-mode** {enable | disable}

Parameters:

Switch(Interface 1)

{enable | disable}

Mode

Interface Config

auto-negotiate

Description:

Configure auto-negotiate mode on a port

Syntax:

auto-negotiate {enable | disable}

Parameters:

{enable | disable}

Mode

Interface Config

speed

Description:

Set port speed to 10Mbps half duplex/ 10Mbps full/ 100Mbps half/ 100Mbps full/ 1000Mbps 100FX mode/1000base-x full .

Syntax:

speed {10hd | 10fd | 100hd | 100fd | 1000fd | 100fx | 1000base-x}

Parameters:

{10hd | 10fd | 100hd | 100fd | 1000fd | 100fx | 1000base-x}

Mode

Interface Config

flow-control

Description:

This command enable/disable flow-control on ports.

Syntax:

flow-control {enable | disable}

Parameters:

{enable | disable}

Mode

Interface Config

6.4.6 Port-security Command

port-security lock-mode dynamic max-entries 24

Description:

This command enable limited dynamic lock mode,and specify maximin learning entries for limited dynamic lock mode.the max-entries value :0~24

Syntax:

port-security lock-mode dynamic max-entries 24

Mode

Interface Config

port-security none

Description:

This command specifies port-based qos priority mapping.

Syntax:

qos port-based priority <0..7>

Mode

Interface Config

Qos port-based status

Description:

This command is used to set port-based status.

Syntax:

qos port-based status {enable|disable}

Parameters:

{enable|disable}

Mode

Interface Config

6.4.7 Rate-limit Command

rate-limit egress enable token bsize

Description:

This command limits egress rate, which the unit is Kbps.

Syntax:

rate-limit egress enable token bsize <Burst Size Value>

Parameters:

<Burst Size Value>

Mode

Interface Config

rate-limit egress disable

Description:

This command disable egress rate limit.

rate-limit ingress

Description:

This command limits ingress rate, which the unit is Kbps.

Syntax:

rate-limit ingress <*rate*>

Parameters:

<*rate*>

Mode

Interface Config

storm-control

Description:

Enable/disable storm control.

Syntax:

storm-control {enable | disable}

Parameters:

{enable | disable}

Mode

Interface Config

storm-control broadcast

Description:

This command storm control for broadcast only, and limited value :0,64,256,1024,10240,65536.102400,1024000,which the unit is Kbps and 0 means no limit.

Syntax:

storm-control broadcast <*rate*>

Parameters:

<*rate*>

Mode

Interface Config

storm-control broadcast-multicast

Description:

This command storm control limited value :0,64,256,1024,10240,65536.102400,1024000,which the unit is Kbps and 0 means no limit.

Syntax:

storm-control broadcast-multicast <*rate*>

Parameters:

<*rate*>

Mode

Interface Config

storm-control broadcast-unknown

Description:

This command storm control limited value :0,64,256,1024,10240,65536.102400,1024000,which the unit is Kbps and 0 means no limit.

Syntax:

storm-control broadcast-unknown <*rate*>

Parameters:

<*rate*>

Mode

Interface Config

Example

```
Switch(Interface 1)# storm-control broadcast-unknown 64
```

storm-control all-cast

Description:

This command storm control limited value :0,64,256,1024,10240,65536.102400,1024000,which the unit is Kbps and 0 means no limit.

Syntax:

storm-control all-cast <*rate*>

Parameters:

<*rate*>

Mode

Interface Config

rmon-counter

Description:

This command specifies rmon counter capability on a port

Syntax:

rmon-counter {enable | disable}

Parameters:

{enable | disable}

Mode

Interface Config

set igmp-router-port

Description:

This command specifies a igmp router port .

Syntax:

set igmp-router-port {enable | disable}

Parameters:

{enable | disable}

Mode

Interface Config

6.4.8 Spanning Tree Command

spanning-tree cost

Description:

This command configure RSTP port path cost, path cost value:0~200000000.

Syntax:

spanning-tree cost <*pathcost*>

Parameters:

<*pathcost*>

Mode

Interface Config

spanning-tree edge

Description:

This command configure edge property

Syntax:

spanning-tree edge {enable|disable}

Parameters:

{enable|disable}

Mode

Interface Config

Example

```
Switch(Interface 1)# spanning-tree edge enable
```

spanning-tree force-p2plink

Description:

This command configure force point to point link mode.

Syntax:

spanning-tree force-p2plink {auto|enable|disable}

Parameters:

{auto|enable|disable}

Mode

Interface Config

spanning-tree migration-check

Description:

This command re-checks the appropriate BPDU format to send on this port

Syntax:

spanning-tree migration-check {enable|disable}

Parameters:

{enable|disable}

Mode

Interface Config

spanning-tree mst cost

Description:

This command configure the path cost on a MST instance :1~200000000.

Syntax:

spanning-tree mst cost <MST ID> <*pathcost*>

Parameters:

<MST ID>

<*pathcost*>

Mode

Interface Config

spanning-tree mst priority

Description:

This command configure the port priority on a MST instance:0~4094.

Syntax:

spanning-tree mst priority <0 ~4094> <0~240>

Parameters:

<0 ~4094>

<0~240>

Mode

Interface Config

spanning-tree participation

Description:

This command configures RSTP capability on a port.

Syntax:

spanning-tree participation {enable|disable}

Parameters:

{enable|disable}

Mode

Interface Config

spanning-tree priority

Description:

This command configure RSTP port priority:0~240

Syntax:

spanning-tree priority <0..240>

Parameters:

<0..240>

Mode

Interface Config

6.4.9 VLAN Command

vlan participation exclude

Description:

This command is used to leave a vlan.

Syntax:

vlan participation exclude < *vlan id*>

Parameters:

< *vlan id*>

Mode

Interface Config

vlan participation

Description:

This command join a vlan with untagged/tagged mode.

Syntax:

vlan participation {untagged |tagged}< vlan id>

Parameters:

{untagged |tagged}

< vlan id>

Mode

Interface Config

vlan protected

Description:

This command configures port protected property.

Syntax:

vlan protected {enable|disable}

Parameters:

{enable|disable}

Mode

Interface Config

vlan dropnq

Description:

This command configure port drop none 802.1Q frame.

Syntax:

vlan dropnq {enable|disable}

Parameters:

{enable|disable}

Mode

Interface Config

vlan pvid

Description:

This command configure port PVID.

Syntax:

vlan pvid *<pvid>*

Parameters:

<pvid>

Mode

Interface Config

Example

```
Switch(Interface 1)# vlan pvid 1
```

Interface commands

Description:

This command is used to change to another interface

Syntax:

Interface commands *<port number>*

Parameters:

<port number>

Mode

Interface Config

Example

```
Switch(Interface 1)# interface g1
```

7. SWITCH OPERATION

7.1 Address Table

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

7.2 Learning

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

7.3 Forwarding & Filtering

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

7.4 Store-and-Forward

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

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

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

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

7.5 Auto-Negotiation

The STP ports on the Switch have built-in "Auto-negotiation". This technology automatically sets the best possible bandwidth when a connection is established with another network device (usually at Power On or Reset). This is done by detect the modes and speeds at the second of both device is connected and capable of, both 10Base-T and 100Base-TX devices can connect with the port in either Half- or Full-Duplex mode. 1000Base-T can be only connected in Full-duplex mode.

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

8. TROUBLE SHOOTING

This chapter contains information to help you solve problems. If the Ethernet Switch is not functioning properly, make sure the Ethernet 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 Ethernet 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 Ethernet Switch. If the Ethernet 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

- **100Base-TX 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.

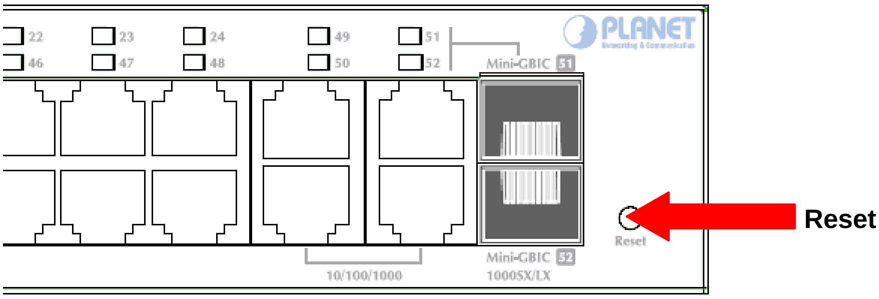
- **Switch does not power up**

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

- **While IP Address be changed or forgotten admin password** –

To reset the IP address to the default IP Address "192.168.0.100" or reset the password to default value. Press the hardware **reset button** at the front panel about **10 seconds.** After the device is rebooted, you can login the management WEB interface within the same subnet of 192.168.0.xx.



APPENDEX A

A.1 Switch's RJ-45 Pin Assignments

1000Mbps, 1000Base-T

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

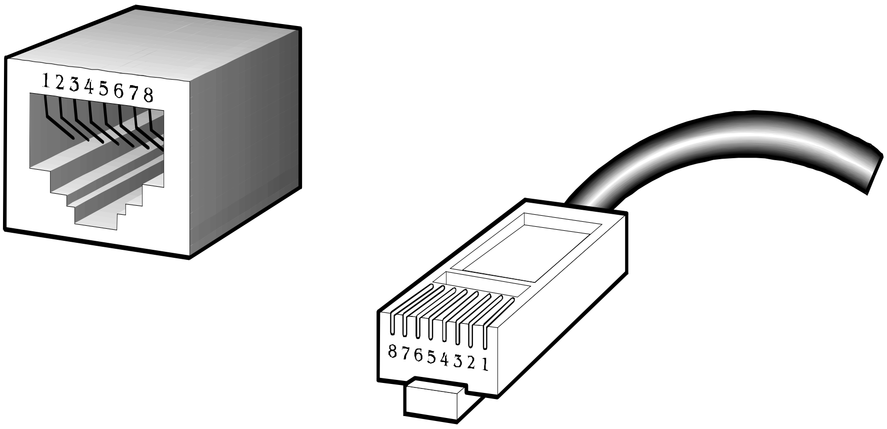
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

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

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

RJ-45 Connector pin assignment		
Contact	MDI Media Dependant Interface	MDI-X Media Dependant Interface-Cross
1	Tx + (transmit)	Rx + (receive)
2	Tx - (transmit)	Rx - (receive)
3	Rx + (receive)	Tx + (transmit)
4, 5	Not used	
6	Rx - (receive)	Tx - (transmit)
7, 8	Not used	

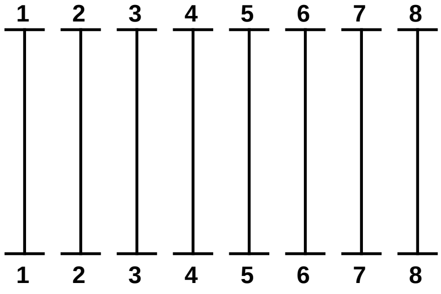
The standard cable, RJ-45 pin assignment



The standard RJ-45 receptacle/connector

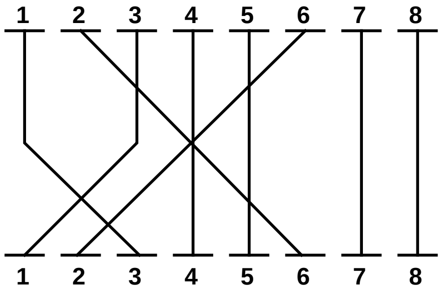
There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight cable and crossover cable connection:

Straight Cable



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

Straight Cable



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

Figure A-1: Straight-Through and Crossover Cable

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

A.3 Available Modules

The following list the available Modules for WGSW-5242

Module Name	Description
MGB-GT	SFP-Port 1000Base-T Module
MGB-SX	SFP-Port 1000Base-SX mini-GBIC module - 550m
MGB-LX	SFP-Port 1000Base-LX mini-GBIC module - 10km
MGB-L30	SFP-Port 1000Base-LX mini-GBIC module - 30km
MGB-L50	SFP-Port 1000Base-LX mini-GBIC module - 50km
MGB-L70	SFP-Port 1000Base-LX mini-GBIC module - 70km
MGB-L120	SFP-Port 1000Base-LX mini-GBIC module - 120km
MGB-LA10	SFP-Port 1000Base-LX (WDM,TX:1310nm) mini-GBIC module - 10km
MGB-LB10	SFP-Port 1000Base-LX (WDM,TX:1550nm) mini-GBIC module - 10km
MGB-LA20	SFP-Port 1000Base-LX (WDM,TX:1310nm) mini-GBIC module - 20km
MGB-LB20	SFP-Port 1000Base-LX (WDM,TX:1550nm) mini-GBIC module - 20km
MGB-LA40	SFP-Port 1000Base-LX (WDM,TX:1310nm) mini-GBIC module - 40km
MGB-LB40	SFP-Port 1000Base-LX (WDM,TX:1550nm) mini-GBIC module - 40km
MFB-FX	SFP-Port 100Base-FX Transceiver (1310nm) - 2km
MFB-F20	SFP-Port 100Base-FX Transceiver (1310nm) - 20km
MFB-F40	SFP-Port 100Base-FX Transceiver (1310nm) – 40km
MFB-F60	SFP-Port 100Base-FX Transceiver (1310nm) – 60km
MFB-FA20	SFP-Port 100Base-BX Transceiver (WDM,TX:1310nm) - 20km
MFB-FB20	SFP-Port 100Base-BX Transceiver (WDM,TX:1550nm) - 20km

PLANET
Networking & Communication

EC Declaration of Conformity

For the following equipment:

*Type of Product: 48-Port 10/100Mbps + 4 Gigabit TP / 2 SFP Managed Switch
*Model Number: WGSW-5242

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

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

EN55022	(CLASS A: 2006)
EN 61000-3-2	(2006, refer to Note* below)
EN 61000-3-3	(1995 / A1: 2001 / A2: 2005)
EN55024	(1998 / A1: 2001 / A2: 2003)
IEC 61000-4-2	(2001 ED.1.2)
IEC 61000-4-3	(2006 / A1:2007 ED.3.0)
IEC 61000-4-4	(2004 ED.2.0)
IEC 61000-4-5	(2005 ED.2.0)
IEC 61000-4-6	(2006 ED.2.2)
IEC 61000-4-8	(2001 ED.1.1)
IEC 61000-4-11	(2004 ED.2.0)

Note*:The power consumption of EUT is 24. 10W, which is less than 75W and no limits apply. Therefore it is deemed to comply with EN 61000-3-2 without any testing.

Responsible for marking this declaration if the:

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

Authorized representative established within the EU (if applicable):

Company Name: **Planet Technology Corp.**

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

Person responsible for making this declaration

Name, Surname **Kent Kang**

Position / Title : **Product Manager**

Taiwan	**9th May., 2011**	Kent Kang
Place	*Date*	*Legal Signature*