PLANET
Networking & Communication

User's Manual

8-Port VDSL2 + 2-Port Gigabit TP/SFP Managed Switch

► VC-820M

www.PLANET.com.tw

Trademarks

Disclaimer

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

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

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

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

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the Instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at 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 consume power from the power source. In view of saving the energy and reducing the unnecessary power consumption, it is strongly suggested to remove the power connection from 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 8-Port VDSL2 + 2 Gigabit TP/SFP Managed Switch User's manual

MODEL: VC-820M

REVISION: 2.0 (SEP. 2015)

TABLE OF CONTENTS

1. Introduction

Thank you for purchasing PLANET 8-port VDSL2 + 2-Port Gigabit TP/SFP Managed Switch, VC-820M. "Managed Switch" mentioned in this Guide refers to the VC-820M.

1.1 Package Contents

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

- **The Managed Switch x 1**
- **Quick Installation Guide x 1**
- **RS232 to RJ45 Cable x 1**
- **Rubber Feet x 4**
- **Two Rack-mounting Brackets with Attachment Screws x 1 set**
- **Power Cord x 1**
- **SFP Dust Cap x 2**

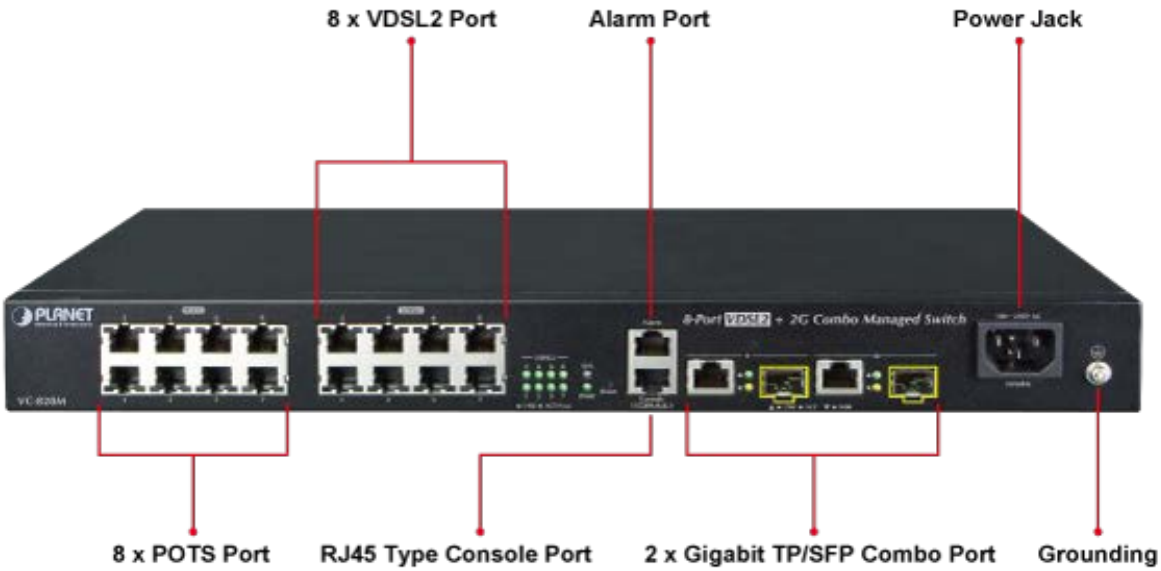
If any of these are missing or damaged, please contact your dealer immediately; if possible, retain the carton including the original packing material, and use them again to repack the product in case there is a need to return it to us for repair.

1.2 Product Description

High Performance VDSL2 Data Rate over Existing Phone Lines

PLANET VC-820M is an **8-Port VDSL2 Managed CO** (Central Office) **Switch** with **2 Gigabit TP/SFP combo** interfaces. The VDSL2 CO Switch is perfectly designed for the networking applications of communities, network service providers, SIs, IP surveillance providers, etc. It is based on two core networking technologies, Ethernet and VDSL2 (Very-high-data-rate Digital Subscriber Line 2). Worked with PLANET VC-23x series of VDSL2 CPE (Customer Premises Equipment), the VC-820M offers the absolutely fastest data transmission speeds over the existing copper telephone lines providing an ideal solution to the last-mile connectivity.

Each VDSL2 interface of the VC-820M provides two copper phone ports, one for VDSL2 connection and the other one for POTS (Plain Old Telephone Service) connection. To share the existing phone line with POTS, the VC-820M has a built-in POTS splitter that helps the voice over telephone and network data to transmit over the same wire without being interrupted.



Delivering Highly-demanding Connectivity for ISPs/Triple Play Devices

As the demand for home broadband connections increases, the VDSL2 technology is the next media to support the integration of home services and provides a significant transmission speed faster than that of the current cable modem and ADSL technology. The VC-820M applies the EoVDSL (Ethernet over VDSL) to providing up to 100Mbps download capability and makes the following multi-media services more efficient on the local network:

- IPTV/HDTV
- VoD (Video on Demand)
- Voice over IP
- Video Conferencing/Video Phone
- On-line Gaming
- Internet Radio/On-line Music
- Long-distance Education

The VC-820M offers an excellent bandwidth to meet the requirements of the triple play devices for home entertainment and communications.

QoS Features to Ensure Best Performance

The VDSL2 Switch contains robust QoS features such as port-based, 802.1p priority and IP ToS/DSCP to ensure the best performance of its VoIP and video stream transmission, thus empowering the enterprises to take full advantage of the limited network resources.

Selectable VDSL2 Data Rate for Service Differentiation

Through the management interface, the administrator can control the data transmission speed of each VDSL2 interface. Telecoms and ISPs can immediately and remotely upgrade/downgrade bandwidth service upon different demands.

Efficient Management

To further expand the current network, PLANET VC-820M provides **console** and **Telnet** command line interfaces, and advanced **Web** and **SNMP** management interfaces. With its built-in Web-based management interface, the VDSL2 switch offers an easy-to-use, platform-independent management and configuration facility. The VDSL2 switch supports standard Simple Network Management Protocol (SNMP) and can be monitored via any standard-based management software. For text-based management, the VDSL2 switch can also be accessed via Telnet and the console port. Moreover, the VDSL2 switch offers secure, remote management by supporting Secure Socket Layer (**SSL**) connection, which encrypts the packet content at each session. The features above provide an efficient way to manage the devices from the internet environment with no need to add extra secure system either by means of hardware or software.

Robust Layer 2 Features

For efficient management, via Web interface, the VC-820M can be programmed for basic switch management functions, such as port speed configuration, port **link aggregation**, IEEE **802.1Q** VLAN and Q-in-Q VLAN, port mirroring, **Rapid Spanning Tree**, and ACL security. Additionally, the firmware includes advanced features such as **IGMP snooping**, QoS (Quality of Service), broadcast storm and **bandwidth control** to enhance bandwidth utilization.

Advanced Security

The VDSL2 switch offers comprehensive Layer 2, Layer 3 and Layer 4 Access Control List (**ACL**) to filter out unwanted traffic. Its protection mechanisms comprise **RADIUS** and port-based **802.1X** user and device authentication. Moreover, the VDSL2 switch provides MAC filter, static MAC, IP/MAC binding and **Port Security** for enforcing security policies to the edge. The administrators can now construct highly-secured corporate networks with considerably less time and effort than before.

1.3 How to Use This Manual

This User Manual is structured as follows:

Section 2, **INSTALLATION**

The section explains the functions of the Switch 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, CONSOLE MANAGEMENT

The section describes how to use the Console management interface.

Section 6, COMMAND LINE INTERFACE

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

Section 7, SWITCH OPERATION

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

Section 8, TROUBLESHOOTING

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

Appendix A

The section contains the cabling information of the Managed Switch.

1.4 Product Features

VDSL Interface

- 8 x **RJ11** connectors for **VDSL2** connection
- 8 x **RJ11** connectors for **POTS** connection
- Built-in **POTS splitter** for each VDSL port
- Auto-speed function for VDSL2 link (by distance and cable quality)

Ethernet Interface

- 2 Gigabit TP and SFP shared combo interfaces
- Auto-MDI/MDI-X detection on Gigabit RJ45 port

VDSL2 Features

- Cost-effective VDSL2 link and central management solution
- ITU-T G.993.2 VDSL2 standard
- **DMT** (Discrete Multi-Tone) line coding VDSL
- Up to **100/100Mbps** symmetric data rate
- Copper wiring distance up to 1km
- Selectable target data rate and target SNR margin
- Built-in surge protection against surge damage from high energy spike
- Voice and data communication can be shared on the existing telephone wire simultaneously
- Supports downstream/upstream rate control on each port

➢ **Layer 2 Features**

- High performance of Store-and-Forward architecture and runt/CRC filtering eliminate erroneous packets to optimize the network bandwidth
- Broadcast/multicast/unicast storm control
- Supports **VLAN**
  - IEEE 802.1Q tag-based VLAN
  - Port-based VLAN
  - Q-in-Q tunneling (VLAN stacking)
  - GVRP for dynamic VLAN management
  - Private VLAN edge (PVE/protected port)
- Link Aggregation
  - IEEE 802.3ad LACP (Link Aggregation Control Protocol)
  - Cisco ether-channel (static trunk)
- Spanning Tree Protocol
  - STP, IEEE 802.1D
  - MSTP, IEEE 802.1s
- Port mirroring to monitor the incoming or outgoing traffic on a particular port

➢ **Quality of Service**

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

- **Multicast**
  - Supports IGMP snooping v1 and v2
  - IGMP querier mode support

- **Security**
  - IEEE 802.1X port-based network access control protocol
  - RADIUS users access authentication
  - L2/L3/L4 Access Control List (ACL)
  - MAC filtering and source IP-MAC/port-binding
  - Port security for source MAC address entries filtering

- **Management**
  - Switch Management Interface
    - Telnet command line interface
    - Web switch management
    - SNMP v1, v2c, v3 switch management
    - SSL switch management
  - DHCP client for IP address assignment
  - Link Layer Discovery Protocol (LLDP) for easy network management
  - DHCP option82 and DHCP relay
  - Built-in Trivial File Transfer Protocol (TFTP) client
  - Firmware upgrade via TFTP or HTTP
  - Configuration upload/download via TFTP or HTTP
  - Four RMON groups 1, 2, 3, 9 (history, statistics, alarms and events)
  - SNMP trap for interface Link Up and Link Down notification
  - Reset button for system management
  - RJ45 console interface for switch basic management and setup

1.5 Product Specifications

Product	**VC-820M**
Hardware Specifications	
Hardware Version	2.0
VDSL Interface	8 VDSL2 RJ11 interfaces
	8 POTS RJ11 interfaces
Copper Ports	2 10/100/1000BASE-T RJ45 auto-MDI/MDI-X ports
SFP/mini-GBIC Slots	2 1000BASE-X SFP interfaces, shared with Port-9 and Port-10
Console	1 RS232-to-RJ45 serial port (115200, 8, N, 1)
Transient Voltage Suppressor	IEC 61000-4-2 (ESD): ±15kV (air), ±8kV (contact) IEC 61000-4-4 (EFT): 40A (5/50ns) IEC 61000-4-5 (Lightning): 24A (8/20μs)
Switch Architecture	Store-and-Forward
Switch Fabric	5.6Gbps / non-blocking
Switch Throughput	4.16Mpps @64 bytes
Address Table	8K entries
Shared Data Buffer	256K bytes
Maximum Frame Size	9K bytes
Flow Control	Back pressure for half-duplex IEEE 802.3x pause frame for full-duplex
LED	VDSL2, PWR, SYS, LNK/ACT, 1000
Reset Button	< 5 sec: System reboot > 10 sec: Factory default
Dimensions (W x D x H)	404 x 174 x 44.5 mm, 1U height
Weight	2.4 kg
Power Requirements	100~240V AC, 50-60 Hz
Power Consumption/ Dissipation	36 watts (max.)/112.8 BTU/hr
VDSL2	
VDSL2 Standard	Complies with ITU-T G.993.1 and G.993.2. Supports provisioning the VDSL optional band (25K to 138K Hz) usage
Band Plan	Selectable band plan for each VDSL line on a per port basis Band Plan A: - Profile 998, Annex A of G.993.1; optimized for symmetric services Band Plan B: - Profile 997, Annex B of G.993.1; optimized for asymmetric services
Profile	Selectable spectrum profile of 8a/b/c/d, 12a/b, 17a, and 30a for frequency bands (Annex A, B and C) defined in G.993.2
Encoding	VDSL-DMT
VDSL2 Features	Selectable rate limit control Selectable target SNR (Signal to Noise Ratio) mode POTS voices passthrough
Layer 2 Function	
Management Interface	Console, Telnet, Web browser, SSL, SNMP v1, v2c, v3

Gigabit Port Configuration	Port disable/enable Auto-negotiation 10/100/1000Mbps full and half duplex mode selection Flow control disable/enable
Gigabit Port Status	Display each port's speed duplex mode, link status and flow control status Auto-negotiation status, trunk status
Port Mirroring	TX/RX/both 1 to 1 monitor
Bandwidth Control	Ingress/Egress rate limit control Gigabit Port: • Allow to configure per 128Kbps VDSL2 Port: • Allow to configure per 5Mbps
VLAN	IEEE 802.1Q tag-based VLAN, up to 256 VLANs groups, out of 4094 VLAN IDs Port-based VLAN GVRP, up to 128 dynamic VLAN groups Q-in-Q tunneling Private VLAN Edge (PVE/Protected port) with two protected port groups
Link Aggregation	Static port trunk IEEE 802.3ad LACP (Link Aggregation Control Protocol) Supports 13 groups with 8 ports per trunk
QoS	4 priority queue Traffic classification based on - Port priority - 802.1p priority - DSCP/TOS field in IP Packet VoIP QoS by application protocol no.
IGMP Snooping	IGMP (v1, v2) Snooping, up to 256 multicast groups
Access Control List	IP-based Layer 3/Layer 4 ACL Up to 220 ACL rule entries
Security	Port Security (Disable per port of MAC address learning) Static MAC, MAC filter, IP/MAC binding
SNMP MIBs	RFC 1213 MIB-II RFC 2863 Interface MIB RFC 2665 EtherLike MIB RFC 1493 Bridge MIB RFC 2819 RMON MIB (Group 1, 2, 3,9)
Standards Conformance	
Regulatory Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3z 1000BASE- SX/LX IEEE 802.3ab 1000BASE-T IEEE 802.3x Flow control and back pressure IEEE 802.3ad Port trunk with LACP IEEE 802.1D Spanning Tree Protocol IEEE 802.1w Rapid Spanning Tree Protocol IEEE 802.1p Class of Service IEEE 802.1Q VLAN Tagging IEEE 802.1x Port Authentication Network Control

	ITU-T G.993.1 (VDSL) G.997.1 G.993.2 VDSL2 RFC 768 UDP RFC 793 TFTP RFC 791 IP RFC 792 ICMP RFC 2068 HTTP RFC 1112 IGMP v1 RFC 2236 IGMP v2
Cables	• VDSL2: twisted-pair telephone wires (AWG24 or better) up to 1km • 10/100BASE-TX: 2-pair UTP Cat.5, up to 100m (328ft) • 1000BASE-T: 4-pair UTP Cat.5E, up to 100m • 1000BASE-SX: 50/125μm and 62.5/125μm fiber-optic cable, up to 550m • 1000BASE-LX: 9/125μm fiber optic cable, up to 10km 50/125μm and 62.5/125μm fiber-optic cable, up to 550m
Environment	
Operating	Temperature: -10 ~ 50 degrees C Relative Humidity: 10~ 90% (non-condensing)
Storage	Temperature: -20 ~ 70 degrees C Relative Humidity: 10~ 90% (non-condensing)

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 2-1-1 to 2-1-2 shows the front panel of the Managed Switches.

VC-820M Front Panel

Figure 2-1-2: VC-820M Switch front panel

■ **VDSL2 and POTS interface**

There are 8 POTS ports with RJ11 phone connectors on the front panel of the VC-820M. Each port is a built-in POTS splitter that helps the voice of telephone and data of network applications to transmit at the same wire without interruption.

The VDSL2 supports auto detection transmission rate that operates in a different band allocation and results in a different upstream and downstream bandwidth. Owing to a different telephone line quality, cross talk or extension distance may affect actual achievable speed; you can configure individual port in built-in management interface for optimized connectivity.

■ **Gigabit TP Interface**

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

■ **100/1000BASE-X SFP Slots**

Each of the SFP (Small Form-factor Pluggable) slots supports dual-speed, 1000BASE-SX/LX or 100BASE-FX

- For 1000BASE-SX/LX SFP transceiver module: From 550 meters (multi-mode fiber) to 10/30/50/70/120 kilometers (single-mode fiber).
- For 100BASE-FX SFP transceiver module: From 2 kilometers (multi-mode fiber) to 20/40/60 kilometers (single-mode fiber).

■ **Console Port**

The console port is an RJ45 port connector. It is an interface for connecting a terminal directly. Through the console port, it provides rich diagnostic information including IP address setting, factory reset, port management, link status and

system setting.

Users can use the attached **DB9 to RJ45 console cable** in the package and connect to the console port on the device. After the connection, users can run any terminal emulation program (**Hyper Terminal**, **ProComm Plus**, **Telix**, **Winterm** and so on) to enter the startup screen of the device.

1. The payload rate is about 9% less than the line rate due to framing overhead.
2. AWG 26 (0.4mm) cable can also be used but the distance is 20% to 40% shorter than the above table.
3. Each terminated bridge tap can reduce the VDSL link distance by 90m.The quality of the cable, the size of the cable bundles, and the cross talk within the bundle can also affect the overall reach.

■ Alarm Interface

The alarm port is an RJ45 port connector. It is an interface for connecting a sensor directly. Please refer chapter 4.2.9 to enable alarm function

■ Reset Button

On the left of the front panel, the reset button is designed to reboot the Managed Switch without turning 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.
> 5 sec: Factory Default	Reset the Managed Switch to Factory Default configuration. The Managed Switch will then reboot and load the default settings as shown below: ◦ Default username: **admin** ◦ Default password: **admin** ◦ Default IP address: **192.168.0.100** ◦ Subnet mask: **255.255.255.0** ◦ Default gateway: **192.168.0.254**

■ AC Power Receptacle

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

Plug the female end of the power cord firmly into the receptacle on the rear panel of the Managed Switch and plug the other end of the power cord into an electrical outlet, and the power will be ready.

Power Notice: The device is a power-required device, which means it will not work till it is powered. If your networks should be 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.

Power Notice: In some areas, installing a surge suppression device may also help to protect your Managed Switch from being damaged by unregulated surge or current to the Managed Switch.

2.1.2 LED Indications

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

VC-820M LED indication

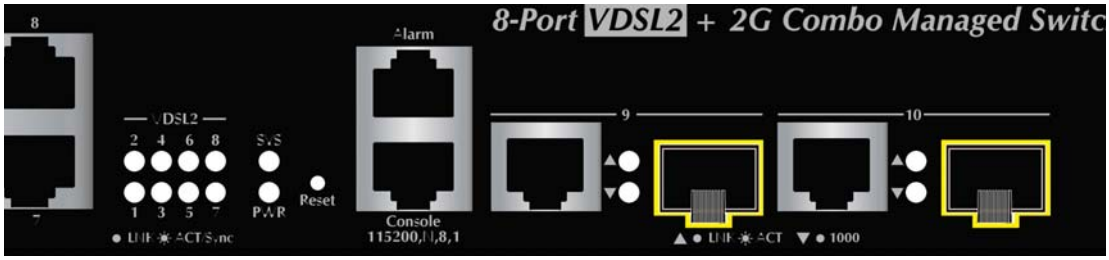


Figure 2-1-5: VC-820M System and Port LED panel

■ **System/Alert**

LED	Color	Function
PWR	**Green**	**Lights** to indicate that the Switch has power.
SYS	**Green**	**Lights** to indicate the system is working. **Off** to indicate the system is booting.
	Red	**Lights** to indicate that the FAN is down or the pin of RJ45 Alarm port is triggered.

■ **VDSL2 interfaces(Port-1 to Port-8)**

LED	Color	Function	
VDSL2	**Green**	**Lights**:	To indicate the link through that port is successfully established.
		Blinks:	To indicate that the switch is actively sending/receiving data or VDSL sync over that port.
		Off:	To indicate the port is link down.

■ **TP/SFP combo interfaces(Port-9 to Port-10)**

LED	Color	Function	
LNK/ACT	**Green**	**Lights**:	To indicate the link through that port is successfully established.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.
1000	**Orange**	**Lights**:	To indicate that the port is operating at **1000Mbps**.
		Off:	If LNK/ACT LED is lit, it indicates that the port is operating at **10/100Mbps**.
			If LNK/ACT LED is off, it indicates that the port is link down.

2.2 Installing the Switch

This section describes how to install the Managed Switch and make connections to it. Please read the following topics and perform the procedures in the order being presented.

2.2.1 Desktop Installation

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

Step 1: Attach the rubber feet to the recessed areas on the bottom of the Managed Switch.

Step 2: Place the Managed Switch on the desktop or the shelf near an AC power source.

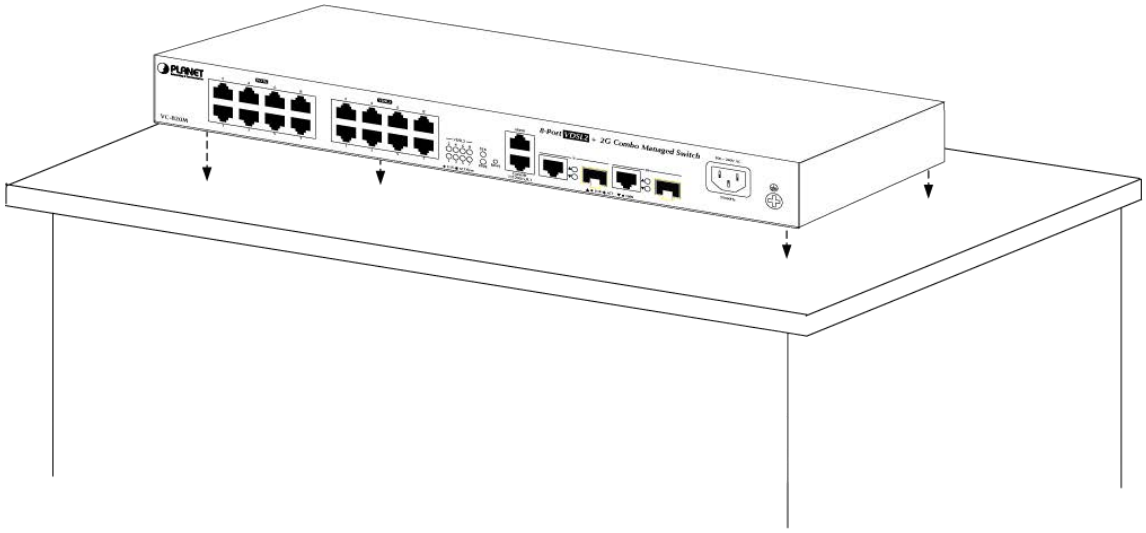


Figure 2-2-1: Place the Managed Switch on the desktop

Step 3: Keep enough ventilation space between the Managed Switch and the surrounding objects.

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

Step 4: Connect the Managed Switch to network devices.

- **A.** Connect one end of a standard network cable to the 10/100/1000 RJ45 ports on the front of the Managed Switch
- **B.** Connect the other end of the cable to the network devices such as printer servers, workstations or routers, etc.

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

Step 5: Supply power to the Managed Switch.

- **A.** Connect one end of the power cable to the Managed Switch.
- **B.** 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 follow the instructions described below.

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

Step 2: Attach the rack-mount bracket to each side of the Managed Switch with supplied screws attached to the package. Figure 2-2-2 and Figure 2-2-3 show how to attach brackets to one side of the Managed Switch.

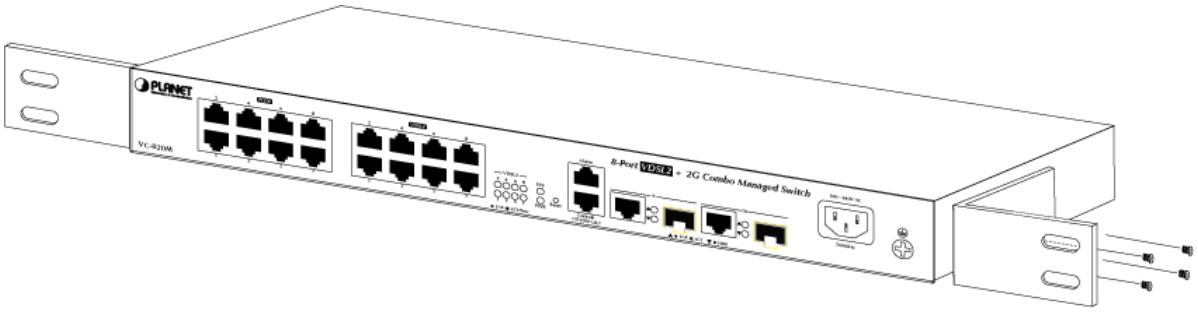


Figure 2-2-2: Attach brackets to VC-820M

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

Step 3: Secure the brackets tightly.

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

Step 5: After the brackets are attached to the Managed Switch, use suitable screws to securely attach the brackets to the rack, as shown in Figure 2-2-3 and Figure 2-2-4.

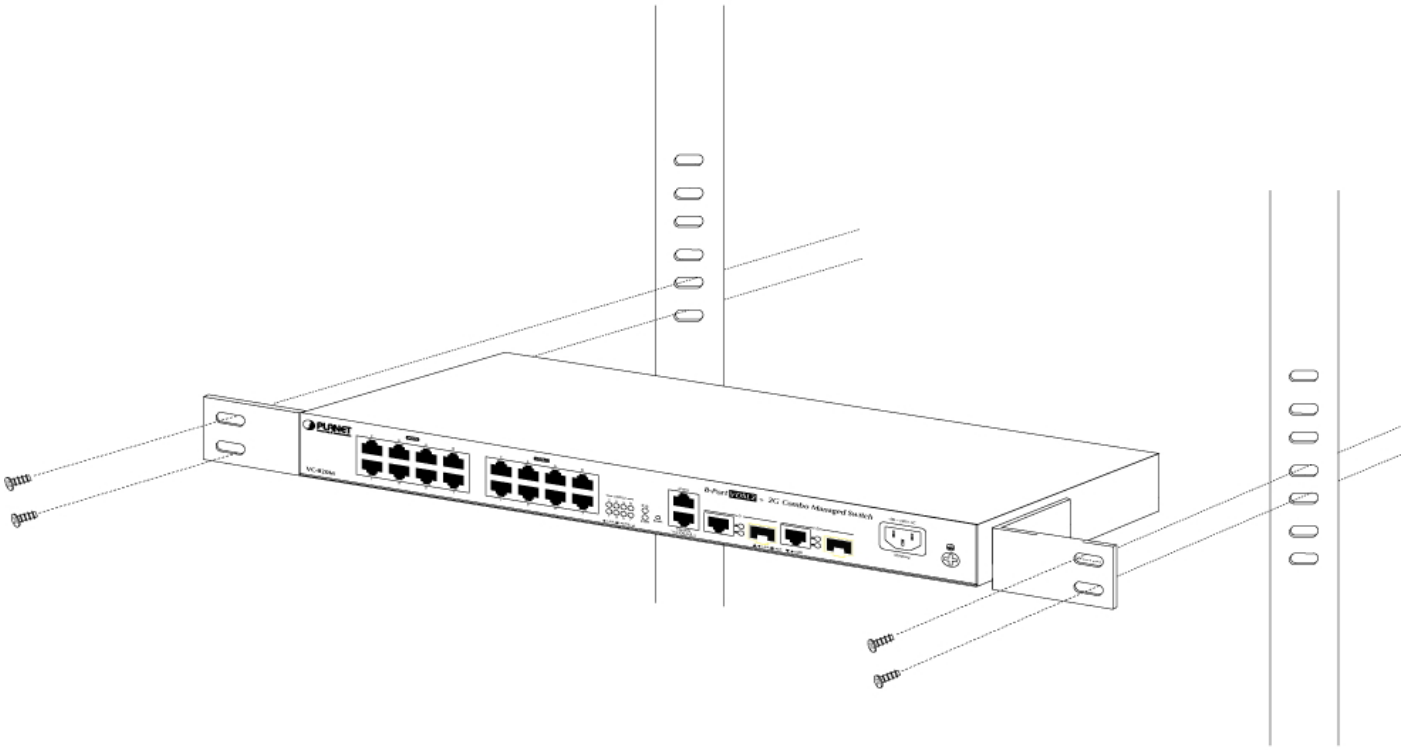


Figure 2-2-4: Mounting the VC-820M in a Rack

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

2.2.3 Installing 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 2-1-7 shows.

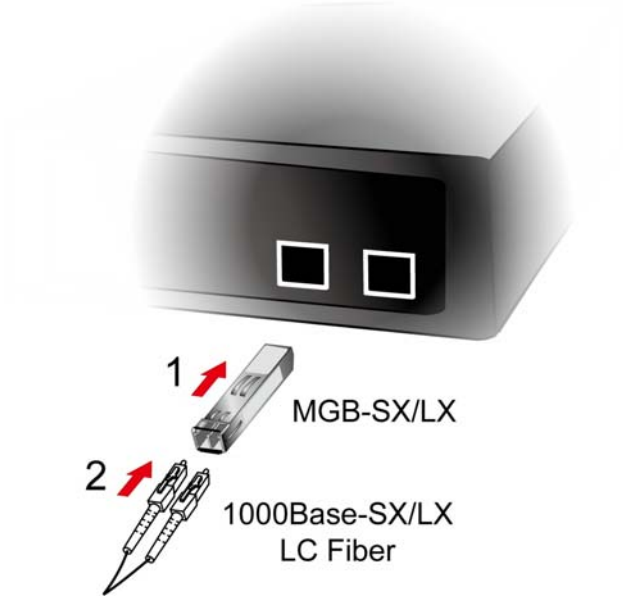


Figure 2-1-7 Plug in the SFP transceiver

■ Approved PLANET SFP Transceivers

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

Gigabit SFP Transceiver Modules

- **MGB-GT** SFP-Port 1000BASE-T Module
- **MGB-SX** SFP-Port 1000BASE-SX mini-GBIC module
- **MGB-LX** SFP-Port 1000BASE-LX mini-GBIC module
- **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) - 10km
- **MGB-LA20** SFP-Port 1000BASE-LX (WDM,TX:1310nm) - 20km
- **MGB-LB20** SFP-Port 1000BASE-LX (WDM,TX:1550nm) - 20km
- **MGB-LA40** SFP-Port 1000BASE-LX (WDM,TX:1310nm) - 40km
- **MGB-LB40** SFP-Port 1000BASE-LX (WDM,TX:1550nm) - 40km

Note

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

In the installation steps below, this Manual uses Gigabit SFP transceiver as an example. However, the steps for Fast Ethernet SFP transceiver are similar.

1. Before we connect Managed Switch to the other network device, we have to make sure both sides of the SFP transceivers are the same media type, for example, 1000BASE-SX to 1000BASE-SX and 1000BASE-LX to 1000BASE-LX.

2. Check whether the fiber-optic cable type matches with the SFP transceiver requirement.
   - To connect to 1000BASE-SX SFP transceiver, please use the multi-mode fiber cable with one side being the male duplex LC connector type.
   - To connect to 1000BASE-LX SFP transceiver, please use the single-mode fiber cable with one side being the male duplex LC connector type.

■ Connecting the Fiber Cable

1. Insert the duplex LC connector into the SFP transceiver.
2. Connect the other end of the cable to a device with SFP transceiver installed.
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 fails. To function with some fiber-NICs or media converters, user has to set the port Link mode to **"1000 Force"**.

■ Removing the Transceiver Module

1. Make sure there is no network activity anymore.
2. Remove the fiber-optic cable gently.
3. Lift up the lever of the MGB module and turn it to a horizontal position.
4. Pull out the module gently through the lever.

Figure 2-1-8 How to Pull Out the SFP Transceiver

Note	Never pull out the module without lifting up the lever of the module and turning it into a horizontal position. Directly pulling out the module could damage the module and the SFP module slot of the Managed Switch.

2.3 Wiring for VDSL2 Ports

The VDSL2 port of VC-820M uses eight RJ11 connectors which can be just directly connected to the remote CPEs (VC-231, VC-234, VDR-300NU or other compatible CPE) through structured or unstructured wiring, such as existing telephone lines. The link between the VDS2L CO Switch port and each CPE can reach speeds of up to 100/100 Mbps under 1000 feet (300 meters) with profile 30a or 18/1 Mbps over distances of up to 5000 feet (1500 meters). You can hot swap the VDSL2 CPEs without powering down the Managed Switch or disrupting the other switch ports.

Each VC-820M VDSL2 Managed Switch series has a built-in **Pain Old Telephone service (POTS)** splitter to transmit both VDSL2 traffic and telephone services, such as voice or fax, through the same phone wire. The splitter routes VDSL2 data (high-frequency) and voice (low-frequency) traffic from the telephone line and **Private Branch exchange (PBX)** switch or **Public Switched Telephone Network (PSTN)**.

The connection diagrams are as follows:

■ **VC-820M VDSL2 Connection**

The VDSL2 port of VC-820M uses eight RJ11 connectors which can be just directly connected to the remote CPEs through existing telephone lines.

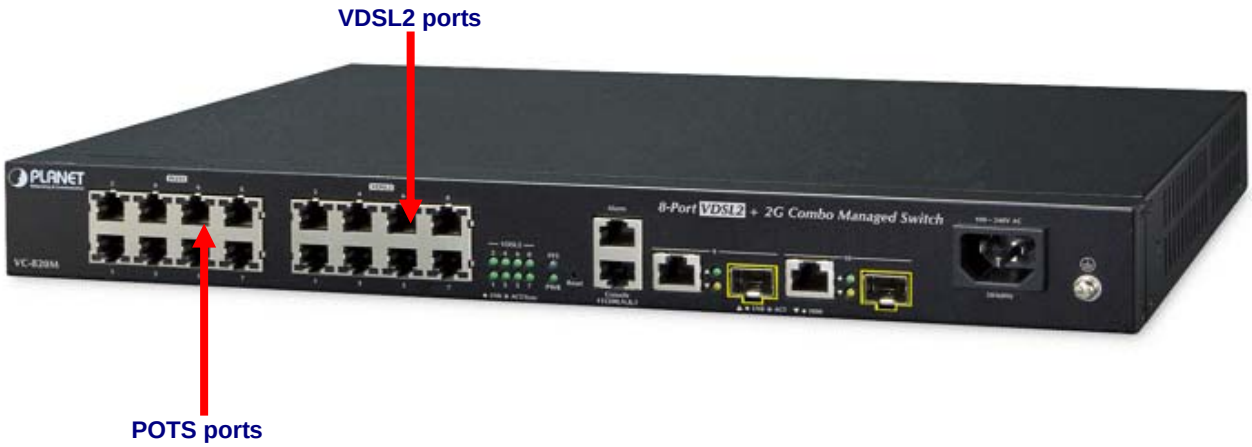


Figure 2-3-4: VC-820M VDSL2 Connection

If the port is connected but the relevant LED is dark, check the following items:

1. The VDSL2 Switch and the connected device's power are on or not.
2. The connecting cable is good and with the correct type.
3. The cable is firmly seated in its connectors in the Managed Switch and in the associated device.
4. The connecting device, including any network adapter, is well installed and functioning.
5. Confirm the CPE (VC-231/VC-234/VDR-300NU) is set to CPE mode. Check the DIP switch at the rear panel.
6. Confirm the CPE (VC-231/VC-234/VDR-300NU) device is implemented within the scope of operative without interference.

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 (workstation or personal computer) and the system. It also contains information about port connection options.

This chapter covers the following topics:

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

3.1 Requirements

- **Workstations** running Windows 98/ME, NT4.0, 2000/XP/7/8/10, MAC OS9 or later, Linux, UNIX or other platforms are compatible with **TCP/IP** protocols.
- **Workstations** are installed with **Ethernet NIC** (Network Interface Card).
- Ethernet Port connection
  - Network cables - Use standard network (UTP) cables with RJ45 connectors.
- The above workstations are installed with **Web browser** and **JAVA runtime environment** plug-in.
- **Serial Port** connection
  - The above workstations come with COM Port (DB-9 / RS-232) or USB-to-RS-232 converter.

It is recommended to use Internet Explore 6.0 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:

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

The administration console and Web browser interface 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
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)
Console	• No IP address or subnet needed • Text-based • Telnet functionality and HyperTerminal built into Windows 95/98/NT/2000/ME/XP/7/8/10 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

Table 3-1: Comparison of Management Methods

3.3 Web Management

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

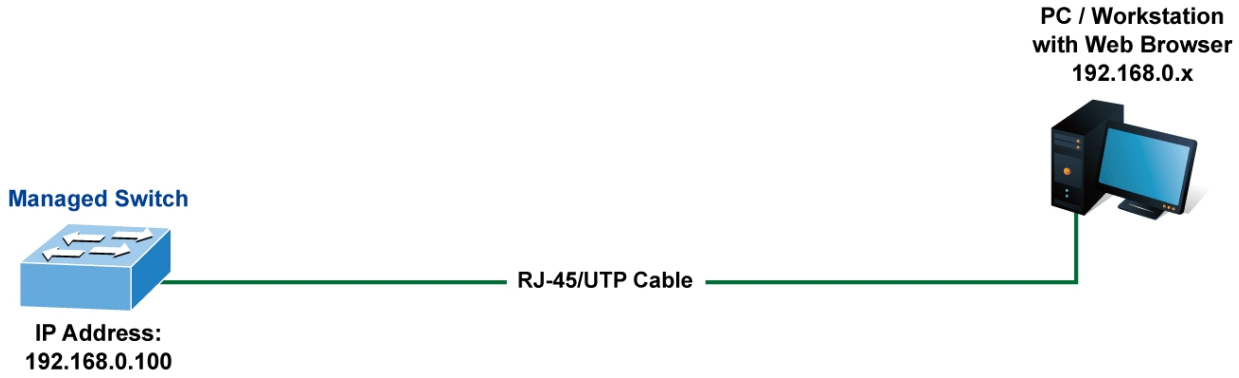


Figure 3-3-1 Web management

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 6.0** or later, **Safari** or **Mozilla Firefox 2.0** or later.

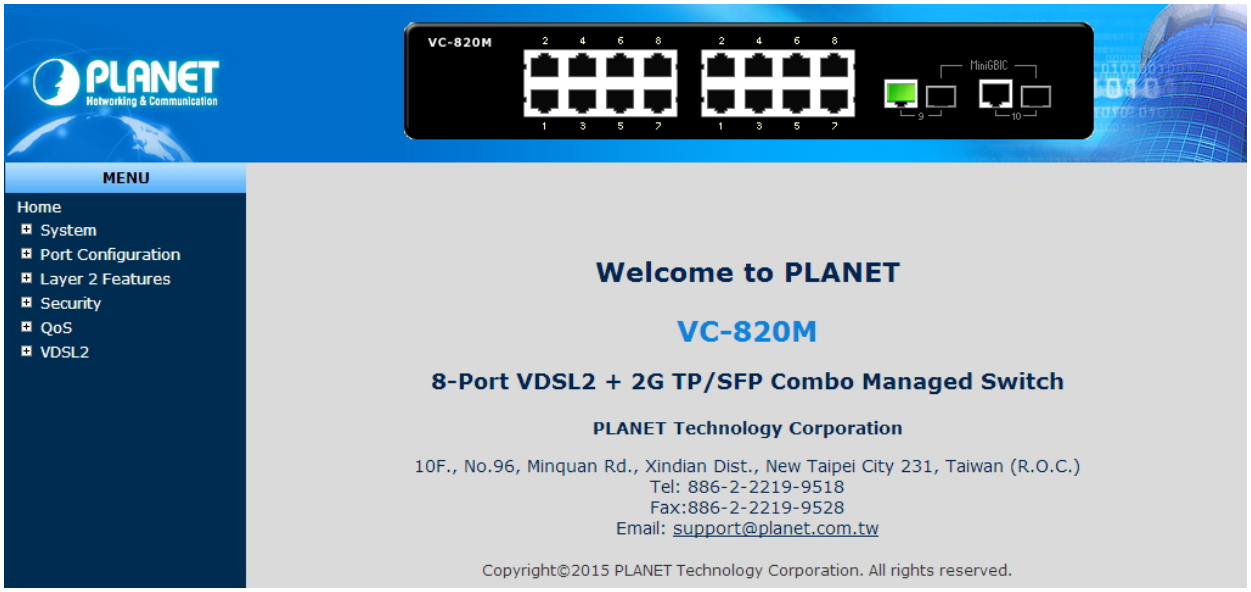


Figure 3-3-2 Web Main Screen of Managed Switch

3.4 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 Whatsup 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.

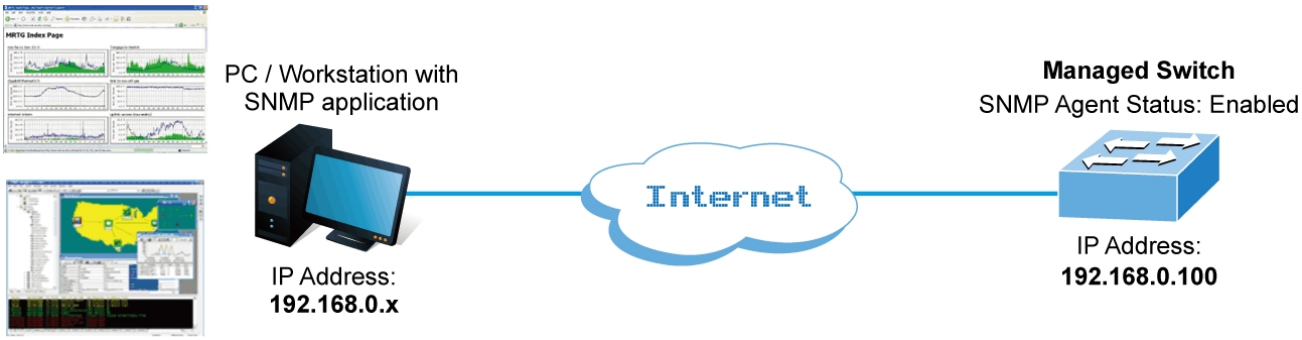


Figure 3-4-1 SNMP management

3.5 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 Console Management**.

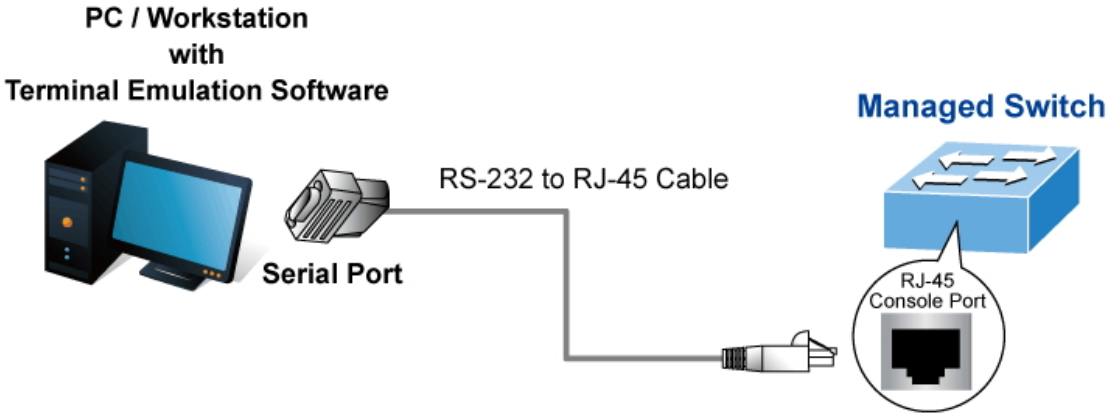


Figure 3-5-1 Console Management

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 **DB9 RS-232 straight-through cable** is required to connect the switch to the PC. After making this connection, configure the terminal-emulation program to use the following parameters:

The default parameters are:

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

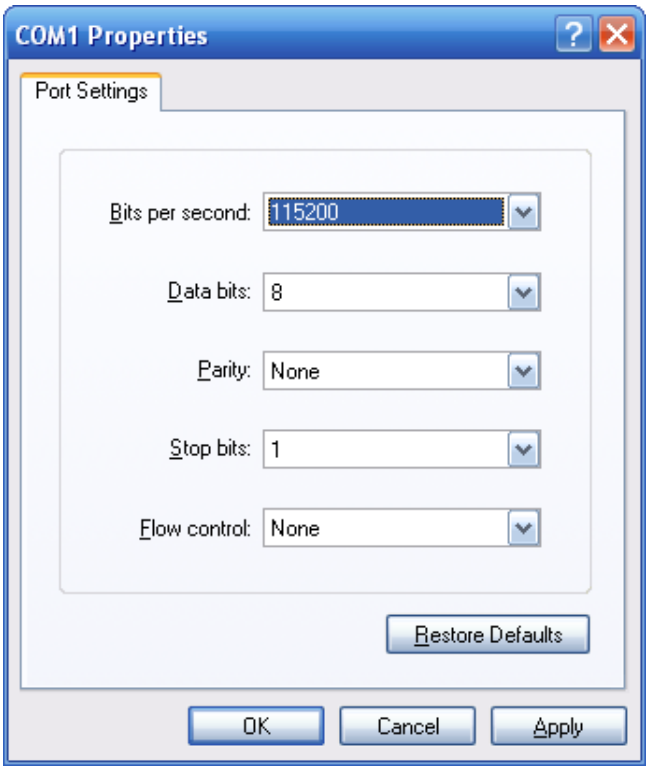


Figure 3-5-2 Terminal Parameter Settings

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.

3.6 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 as the RS232 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.

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 using one method (console port, for example) are immediately displayed 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-based Management

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

4.1 About Web-based Management

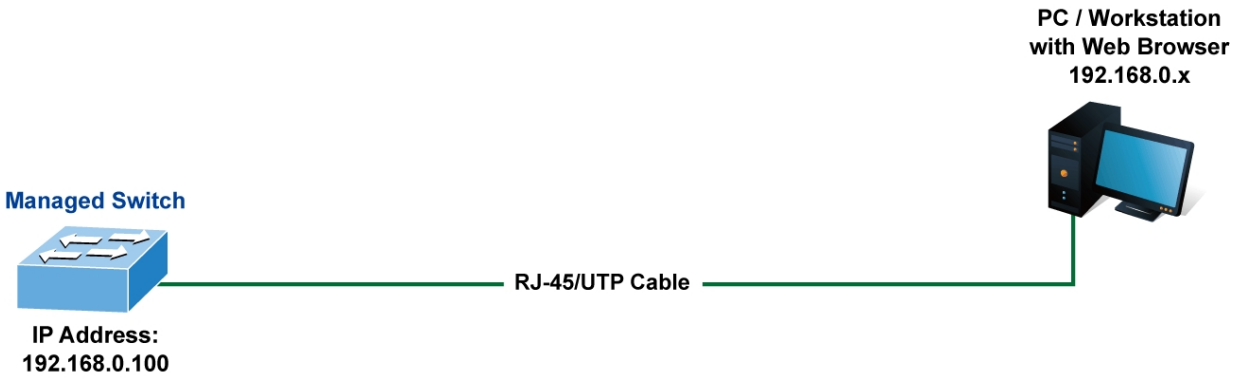
The Managed Switch offers management features that allow users to manage the Managed Switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer. The Web-based Management supports Internet Explorer 6.0. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

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

The Managed Switch can be configured through an Ethernet connection, making 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.



4.1.1 Requirements

- Workstations running Windows 98/ME, NT4.0, 2000/2003/XP/7/8/10, MAC OS9 or later, Linux, UNIX or other platforms are compatible with TCP/IP protocols.
- Workstations are installed with Ethernet NIC (Network Card).
- **Ethernet Port connection**
  - Network cables – Use standard network (UTP) cables with RJ45 connectors.
  - The above workstations are installed with Web browser and JAVA runtime environment plug-in.

It is recommended to use Internet Explore 6.0 or above to access VC-820M

4.1.2 Logging on to the switch

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

   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 4-1-1 appears.

Figure 4-1-1: Login Screen

Default User name: **admin**

Default Password: **admin**

1. After entering the username and password, the main screen appears as Figure 4-1-2.

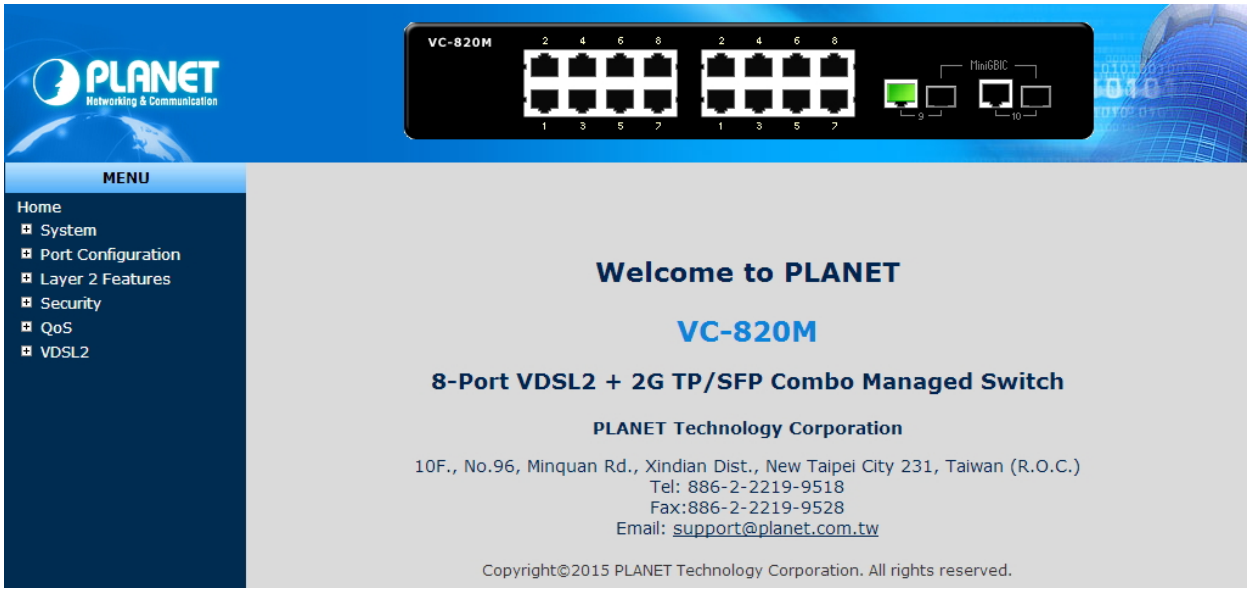


Figure 4-1-2: Web Main Page

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

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

Note

1. It is recommended to use Internet Explore 6.0 or above to access Managed Switch.
2. The changed IP address takes effect immediately after clicking on the **Apply** 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.

4.1.3 Main Web Page

The 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.

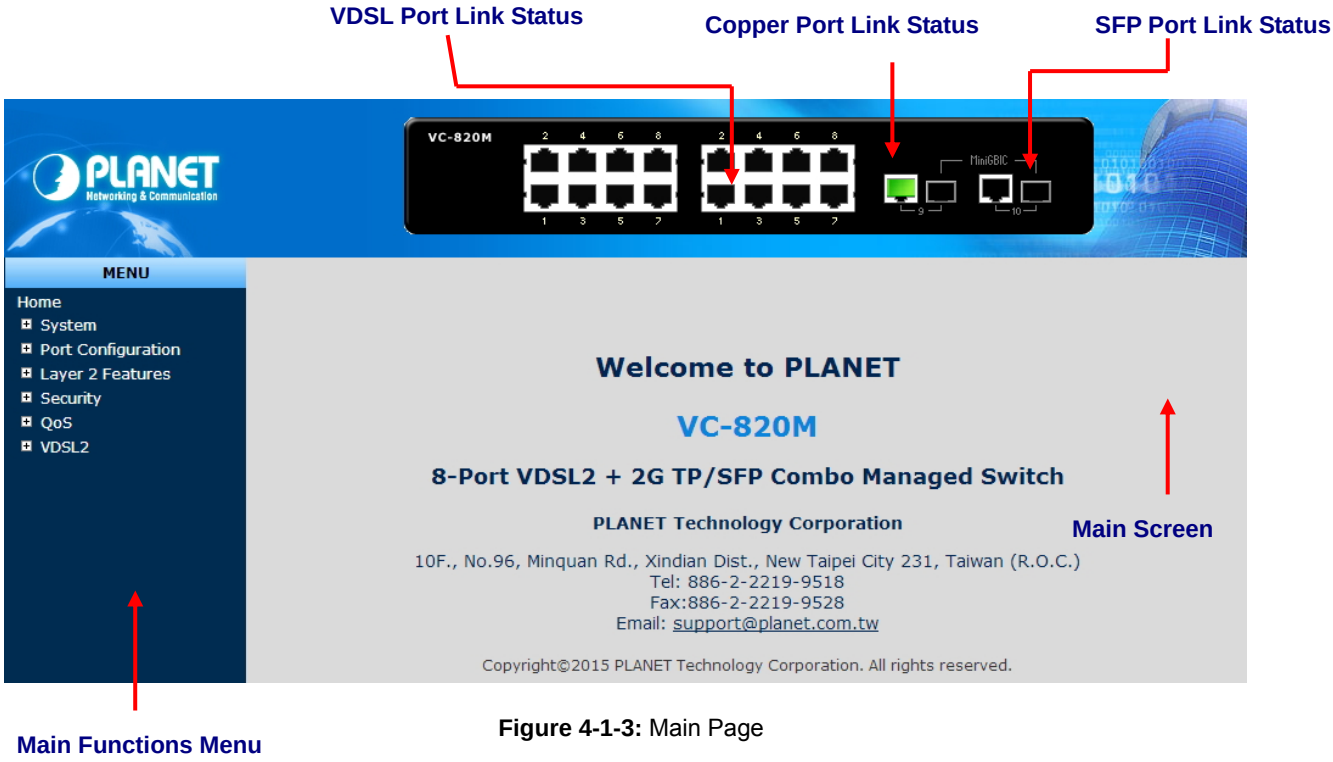


Figure 4-1-3: Main Page

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
RJ45 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 set up the Managed Switch by selecting the functions those listed in the Main Function. The screen in Figure 4-1-4 appears.

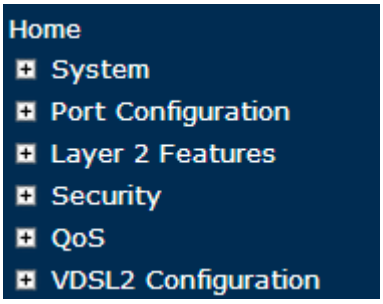


Figure 4-1-4: VC-820M Managed Switch Main Functions Menu

4.2 System

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

System Information	Provides basic system description, including contact information.
IP Configuration	Sets the IP address for management access.
Console Information	Displays the required console settings on the Managed Switch.
SNMP Configuration	Configures SNMP agent and SNMP Trap.
Syslog Setting	Configures login of messages and assign IP address of remote Syslog servers.
System Log	Displays the system log information
SMTP Setting	Configures SMTP function
SNTP Setting	Configures SNTP function
Alarm Configuration	Configures RJ45 alarm port function
Smart Fan	Configures smart fan control function
Firmware Upgrade	Upgrades the firmware via TFTP server or Web browser file transfer.
Configuration Backup	Saves/views the Managed Switch configuration to remote host. Uploads the switch configuration from remote host.
Factory Default	Resets the configuration of the Managed Switch.
System Reboot	Restarts the Managed Switch.

4.2.1 System Information

In the System information, the setting has two parts – **Basic** and **Misc Config**. We will describe the configure detail as follows:

4.2.1.1 Basic

The Basic System Info page provides information for the current device information. The Basic System Info page helps a switch administrator to identify the model name, firmware/hardware version and MAC address.

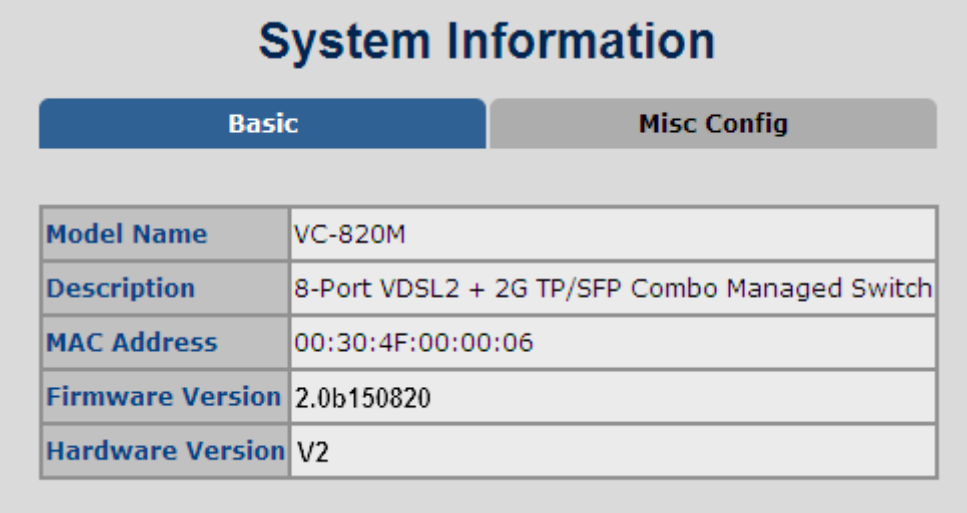


Figure 4-2-1-1: Basic System Information Screenshot

The page includes the following fields:

Object	Description
Model Name:	Displays the system name of the Managed Switch.
Description:	Describes the Managed Switch.
MAC Address:	Displays the unique hardware address assigned by manufacturer (default).
Firmware Version:	Displays the Managed Switch's firmware version.
Hardware Version:	Displays the Managed Switch's hardware version.
Firmware Building Date:	Displays the date information of the firmware.

4.2.1.2 Misc Config

Choose **Misc Config** from System Information of Managed Switch.

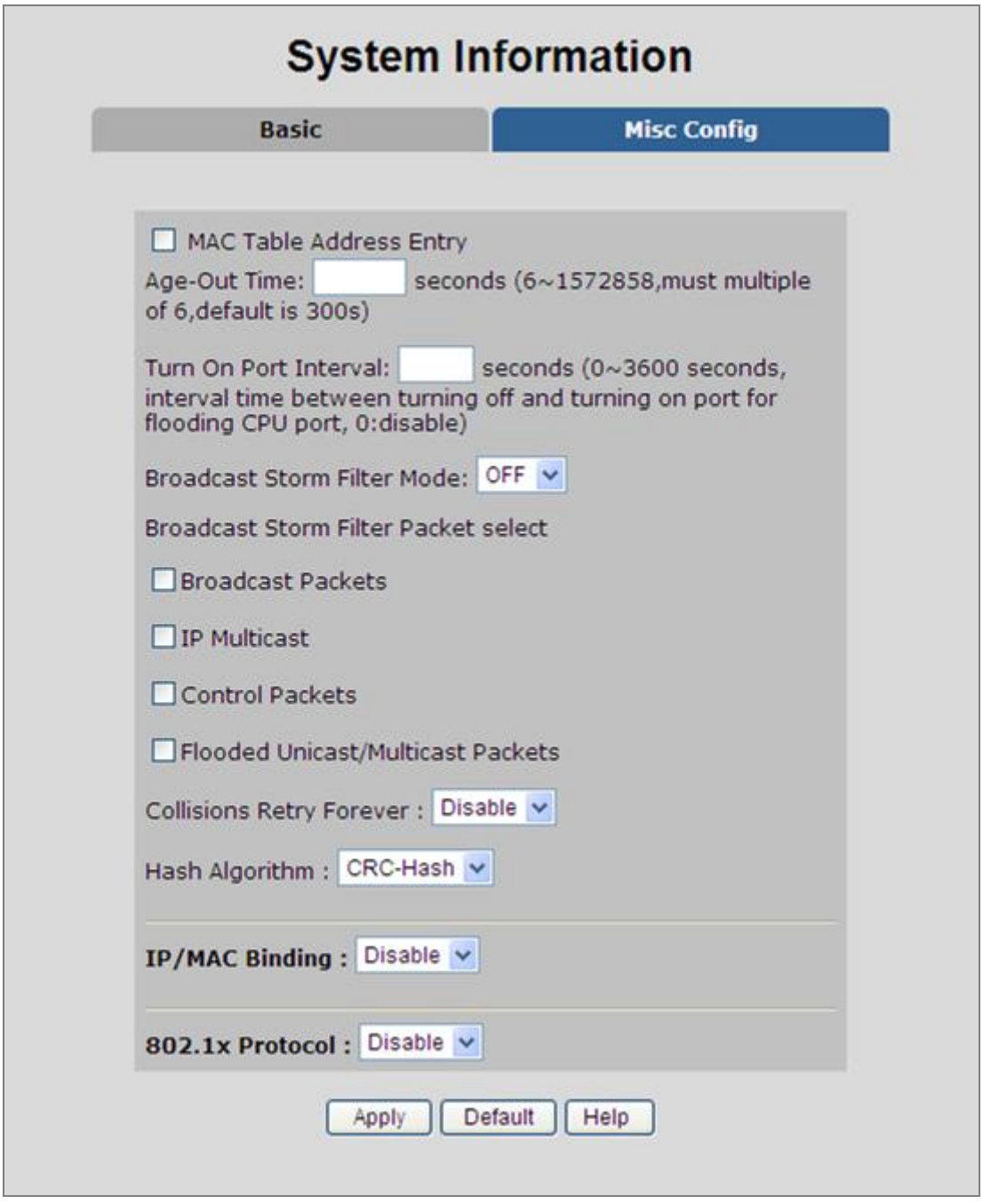


Figure 4-2-1-2: Switch Misc Config Screenshot

The page includes the following fields:

Object	Description
MAC Address Age-out Time	Type the number of seconds that an inactive MAC address remains in the switch's address table. The value is a multiple of 6. Default is **300** seconds.
Broadcast Storm Filter	To configure broadcast storm control, enable it and set the upper threshold for

Mode	individual ports. The threshold is the percentage of the port's total bandwidth used by broadcast traffic. When broadcast traffic for a port rises above the threshold you set, broadcast storm control becomes active. The valid threshold values are **1/2**, **1/4**, **1/8**, **1/16** and **OFF**. Default is "**OFF**".
Broadcast Storm Filter Packets Selection	To select broadcast storm Filter Packets type. If no packets type by selected, mean can not filter any packets .The Broadcast Storm Filter Mode will show OFF. The selectable items are shown below: • **Broadcast Packets** • **IP Multicast** • **Control Packets** • **Flooded Unicast/Multicast Packets**
Collision Retry Forever	Provide Collision Retry Forever function "**Disable**" or **16**, **32**, **48** collision numbers on Managed Switch. If this function is disabled, when a packet meet a collision, the Managed Switch will retry 6 times before discarding the packets. Otherwise, the Managed Switch will retry until the packet is successfully sent. Default value is **16**.
Hash Algorithm	Provide MAC address table Hashing setting on Managed Switch; available options are **CRC-Hash** and **DirectMap**. Default mode is **CRC-Hash**.
IP/MAC Binding	**Enable**/**Disable** IP MAC Binding function.
802.1x Protocol	**Enable**/**Disable** 802.1x protocols.
Apply Button	Press the button to complete the configuration.

4.2.2 IP Configuration

The Managed Switch is a network device which needs to be assigned an IP address for being identified on the network. Users have to decide a means of assigning IP address to the Managed Switch.

IP Address Overview

What is an IP address?

Each device (such as a computer) which participates in an IP network needs a unique "address" on the network. It's similar to having a US mail address so other people have a know way to send you messages. An IP address is a four byte number, which is usually written in "dot notation" - each of the bytes' decimal value is written as a number, and the numbers are separated by "dots" (aka periods). An example: 199.25.123.1

How do I get one for this box?

The IP addresses on most modern corporate nets are assigned by an employee called a "Network Administrator", or "Sys. Admin". This person assigns IP addresses and is responsible for making sure that IP addresses are not duplicated - If this happens one or both machines with a duplicate address will stop working. Another possibility is getting your address assigned to you automatically over the net via DHCP protocol. Enable DHCP function, and reset the machine. If your network is set up for this service, you will get an IP address assigned over the network. If you don't get an address in about 30 seconds, you probably don't have DHCP.

■ IP Configuration

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

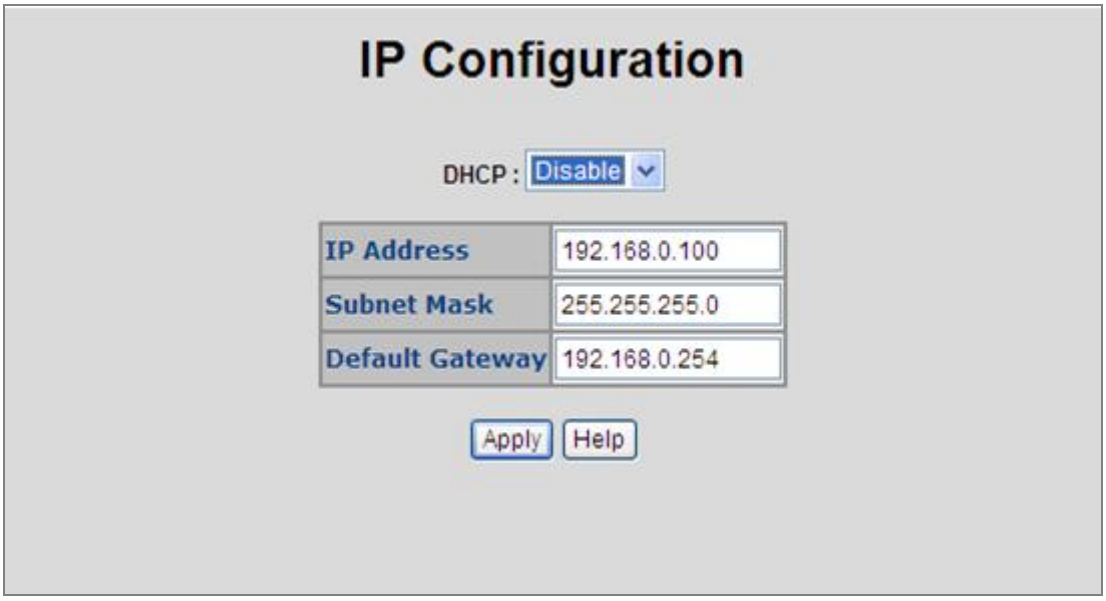


Figure 4-2-2-1: IP Configuration Interface

The page includes the following fields:

Object	Description
DHCP	Enable or disable the **DHCP client** function. When DHCP function is enabled, the Managed Switch will be assigned an IP address from the network DHCP server. The default IP address will be replaced by the assigned IP address on DHCP server. After the user clicks Apply, a popup dialog shows up to inform the user that when the DHCP client is enabled, the current IP will lose and user should find the new IP on the DHCP server.
IP Address	Assign the IP address that the network is using. If DHCP client function is enabled, this switch is configured as a **DHCP client**. The network DHCP server will assign the IP address to the switch and display it in this column. The default IP is **192.168.0.100** or the user has to assign an IP address manually when DHCP Client is disabled.
Subnet Mask	Assign the subnet mask to the IP address. If DHCP client function is disabled, the user has to assign the subnet mask in this column field.
Gateway	Assign the network gateway for the switch. If DHCP client function is disabled, the user has to assign the gateway in this column field. The default gateway is **192.168.0.254**.

4.2.3 Console Information

Console is a standard UART interface to communicate with Serial Port. You can use Windows HyperTerminal program to link the Managed Switch. The page displays the required console settings on the Managed Switch.

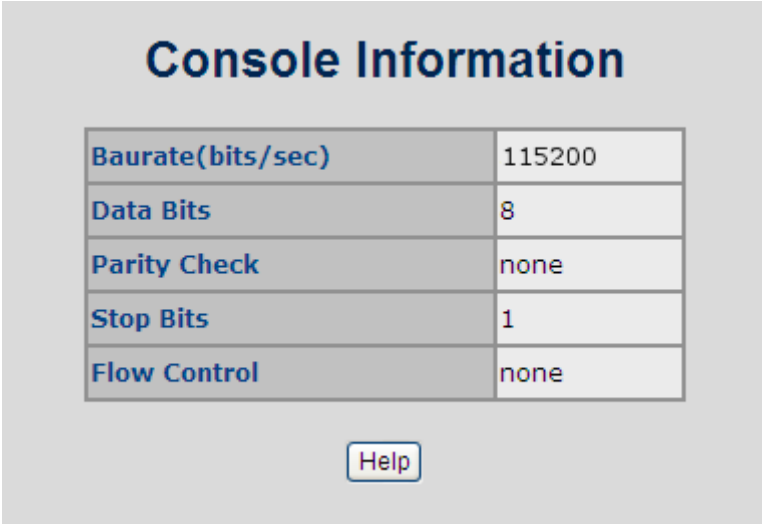


Figure 4-2-3-1: Console Information Interface

4.2.4 SNMP Configuration

4.2.4.1 SNMP Overview

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

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

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

SNMP Operations

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

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

SNMP community

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

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

4.2.4.2 System Options

Use this page to define management stations. You can also define a name, location, and contact person for the Managed Switch.

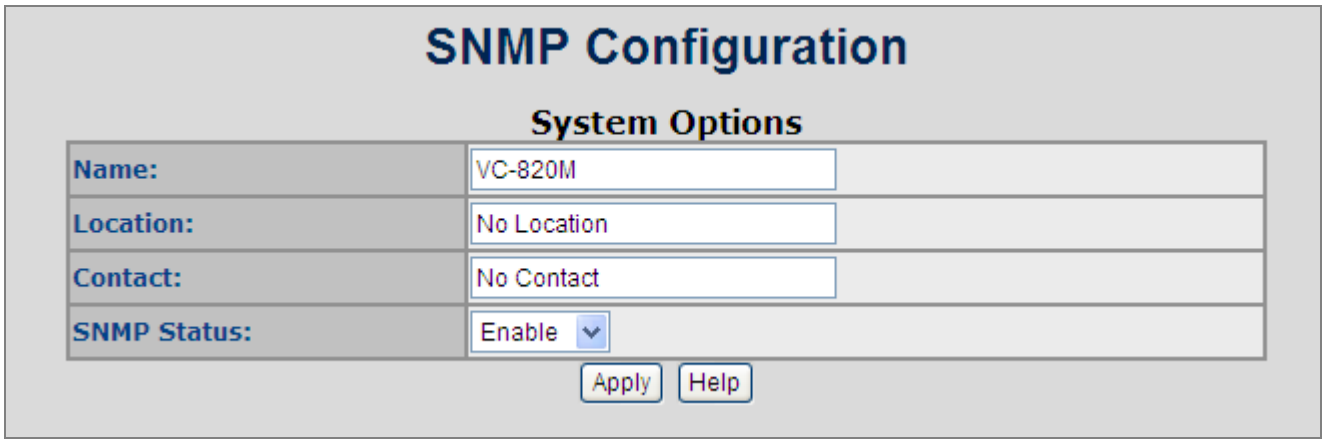


Figure 4-2-4-1: SNMP Configuration Interface

The page includes the following fields:

Object	Description
System Name	An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.
System Location	The physical location of this node (e.g., telephone closet, 3rd floor).

System Contact	The textual identification of the contact person for this managed node, together with information on how to contact this person.
SNMP Status	Indicates the SNMP mode operation. Possible modes are: • **Enabled**: Enable SNMP mode operation. • **Disabled**: Disable SNMP mode operation.

4.2.4.3 Community Strings

Community strings serve as passwords and can be entered as one of the following:

Figure 4-2-4-2: Community Strings Interface

The page includes the following fields:

Object	Description
Community Strings:	Here you can define the new community string set and remove the unwanted community string. ■ **String:** Fill out the name string. ■ **RO:** Read only. Enables requests accompanied by this community string to display MIB-object information. ■ **RW:** Read/write. Enables requests accompanied by this community string to display MIB-object information and to set MIB objects.
Add **button**	Press the button to add the management SNMP community strings on the Managed Switch.
Remove **button**	Press the button to remove the management SNMP community strings that you defined before on the Managed Switch.

4.2.4.4 Trap Managers

A trap manager is a management station that receives the trap messages generated by the switch. If no trap manager is defined, no traps will be issued. To define a management station as a trap manager, assign an IP address, enter the SNMP community strings, and select the SNMP trap version.

Figure 4-2-4-3: Trap Managers Interface

The page includes the following fields:

Object	Description
IP Address:	Enter the IP address of the trap manager.
Community:	Enter the community string for the trap station.

4.2.4.5 SNMPv3 Groups

Configure SNMPv3 groups table on this page. The entry index keys are Security Model and Security Name.

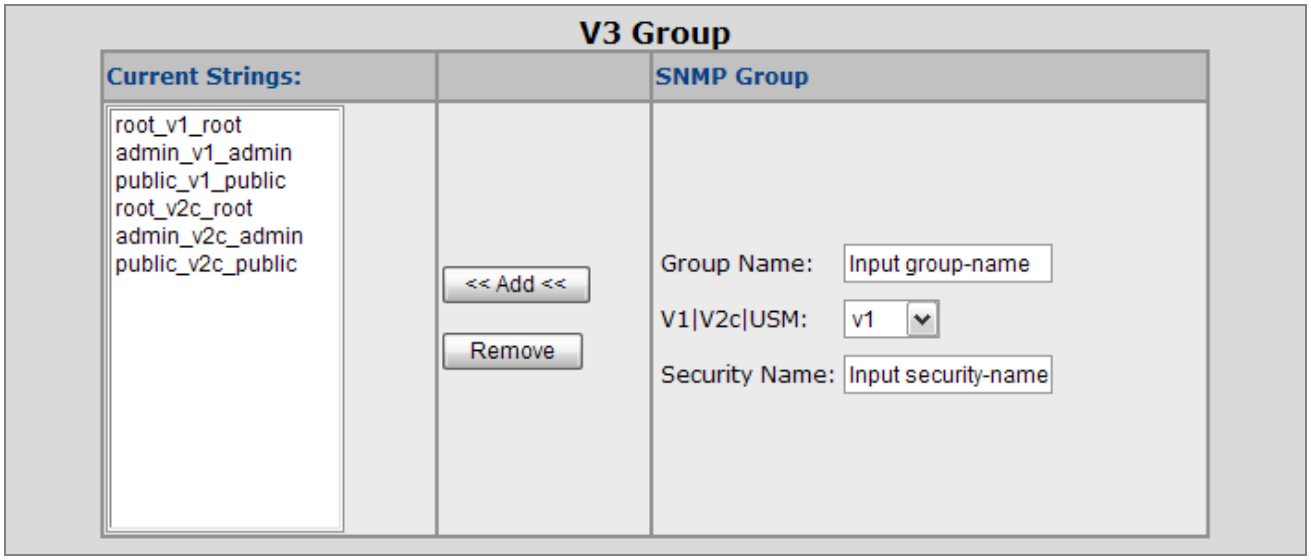


Figure 4-2-4-4: SNMP Configuration Interface

The page includes the following fields:

Object	Description
Group Name:	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 15.
V1 | V2c | USM	Indicates the security model that this entry should belong to. Possible security models are: • **v1**: Reserved for SNMPv1. • **v2c**: Reserved for SNMPv2c. • **usm**: User-based Security Model (USM).
Security Name:	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 15.
Remove	Check to delete the entry. It will be deleted during the next save.

4.2.4.6 SNMPv3 View

Configure SNMPv3 views table on this page. The entry index keys are View Name and OID Subtree.

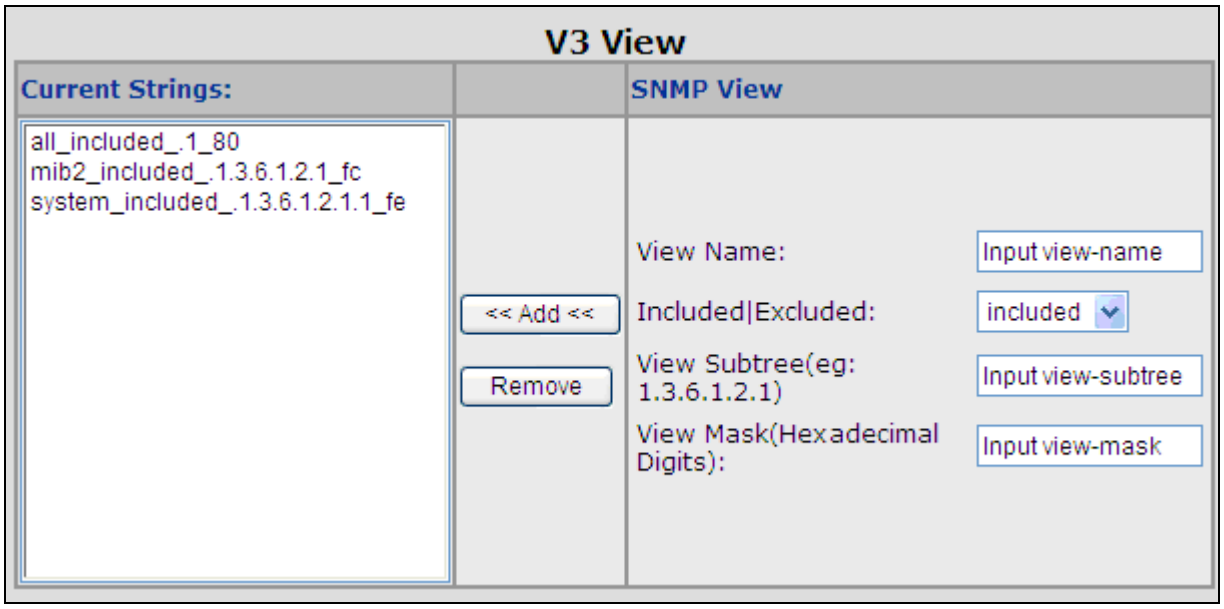


Figure 4-2-4-5: SNMP Configuration Interface

The page includes the following fields:

Object	Description
View Name:	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 15.
Included | Excluded:	Indicates the view type that this entry should belong to. Possible view type are: • **included**: An optional flag to indicate that this view subtree should be

	included. • **excluded**: An optional flag to indicate that this view subtree should be excluded.
View Subtree	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*)
View Mask (Hexadecimal Digits):	View mask is defined in order to reduce the amount of configuration information required when fine-grained access control is required (e.g., access control at the object instance level)

4.2.4.7 SNMPv3 Access

Configure SNMPv3 accesses table on this page. The entry index keys are Group Name, Security Model and Security Level.

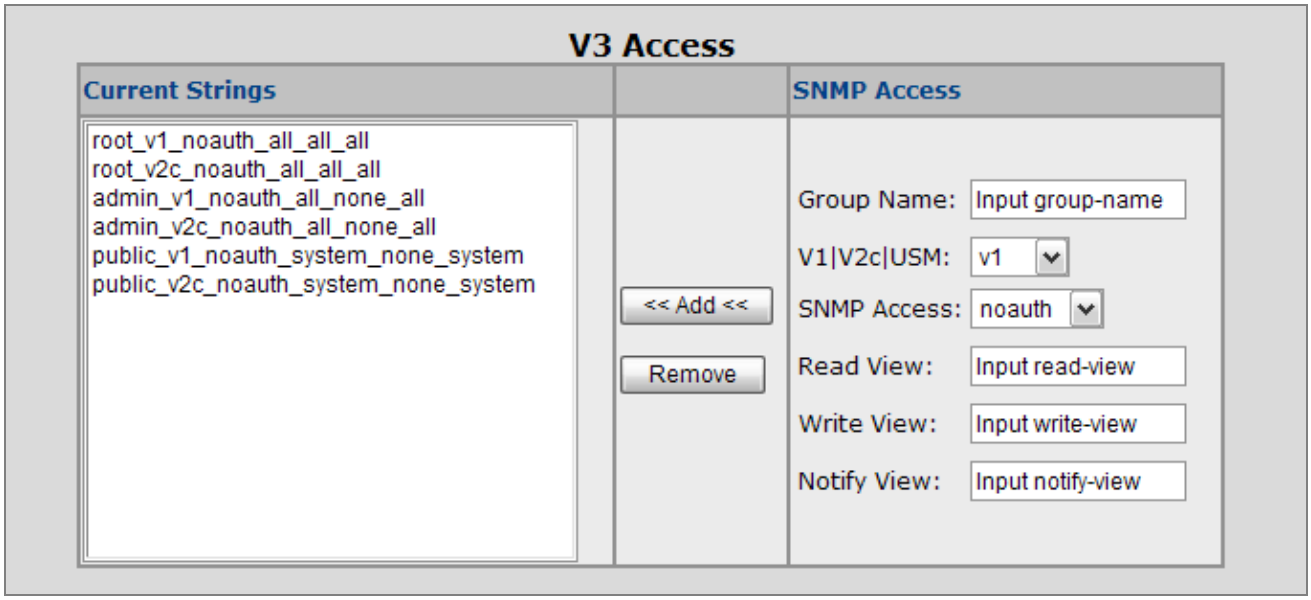


Figure 4-2-4-6: SNMP Configuration Interface

The page includes the following fields:

Object	Description
Group Name:	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 15.
V1 | V2c | USM:	Indicates the security model that this entry should belong to. Possible security models are: • **v1**: Reserved for SNMPv1. • **v2c**: Reserved for SNMPv2c. • **usm**: User-based Security Model (USM)
SNMP Access:	Indicates the security model that this entry should belong to. Possible security models are: • **NoAuth**: None authentication and none privacy. • **Auth**: Authentication and none privacy.

	• **Authpriv:** Authentication and privacy.
Read View:	The name of the MIB views defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 16.
Write View:	The name of the MIB views defining the MIB objects for which this request may potentially SET new values. The allowed string length is 1 to 16.
Notify View:	Set up the notify view.
Add **button**	Press the button to add the management SNMP community strings on the Managed Switch.
Remove **button**	Check to delete the selected entry. It will be deleted during the next save.

4.2.4.8 SNMP V3 usm-user

Configure SNMPv3 users table on this page. The entry index keys are Engine ID and User Name.

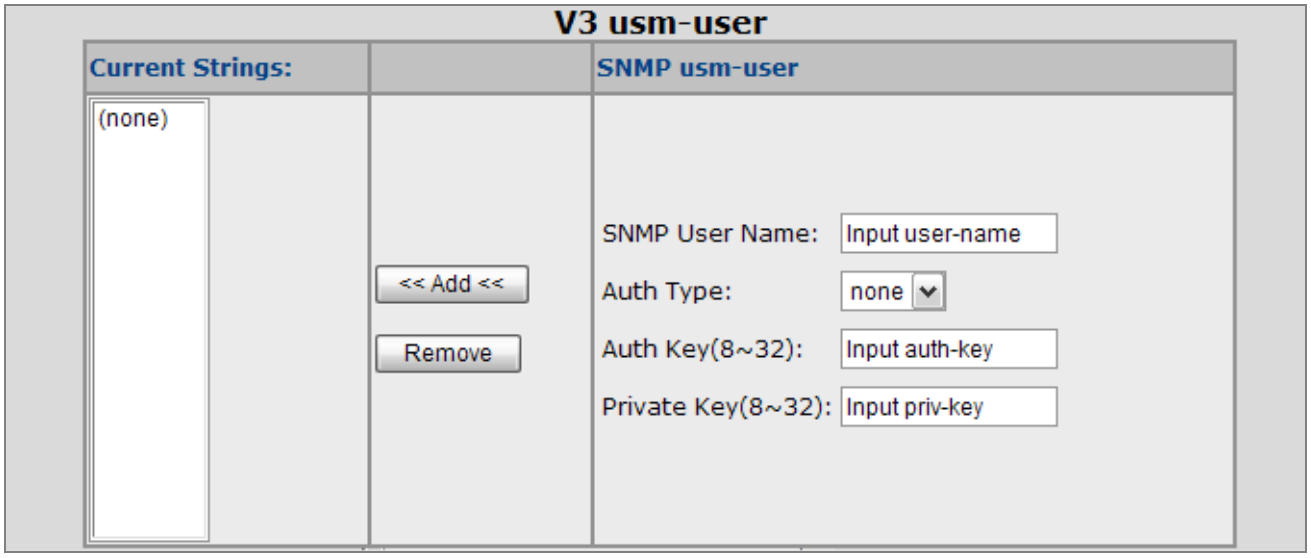


Figure 4-2-4-7: SNMP Configuration Interface

The page includes the following fields:

Object	Description
SNMP User Name:	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 15.
Auth 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 exists. That means must first ensure that the value is set correctly.
Auth Key(8~32):	A string identifying the authentication pass phrase. For MD5 authentication protocol, the allowed string length is 8 to 32.
Private Key(8~32):	A string identifying the privacy pass phrase. The allowed string length is 8 to 32.
Add **button**	Press the button to add the management SNMP community strings on the Managed Switch.
Remove **button**	Check to delete the selected entry. It will be deleted during the next save.

4.2.5 Syslog Setting

The Syslog Setting page allows you to configure the logging of messages that are sent to remote syslog servers or other management stations. You can also limit the event messages sent to only those messages below a specified level.

Figure 4-2-5-1: Syslog Setting Web Interface

The page includes the following fields:

Object	Description
Syslog Server IP	IP address of syslog server.
Log level	• **None**: No send syslog message to syslog server, and Max Age parameters of the root bridge, regardless of how it is configured. • **Major**: only send major syslog to syslog server, e.g., link up/down, system warm/cold start • **All**: send all syslog messages to syslog server.

4.2.6 System Log

The System Log page allows you to enable/disable syslog feature.

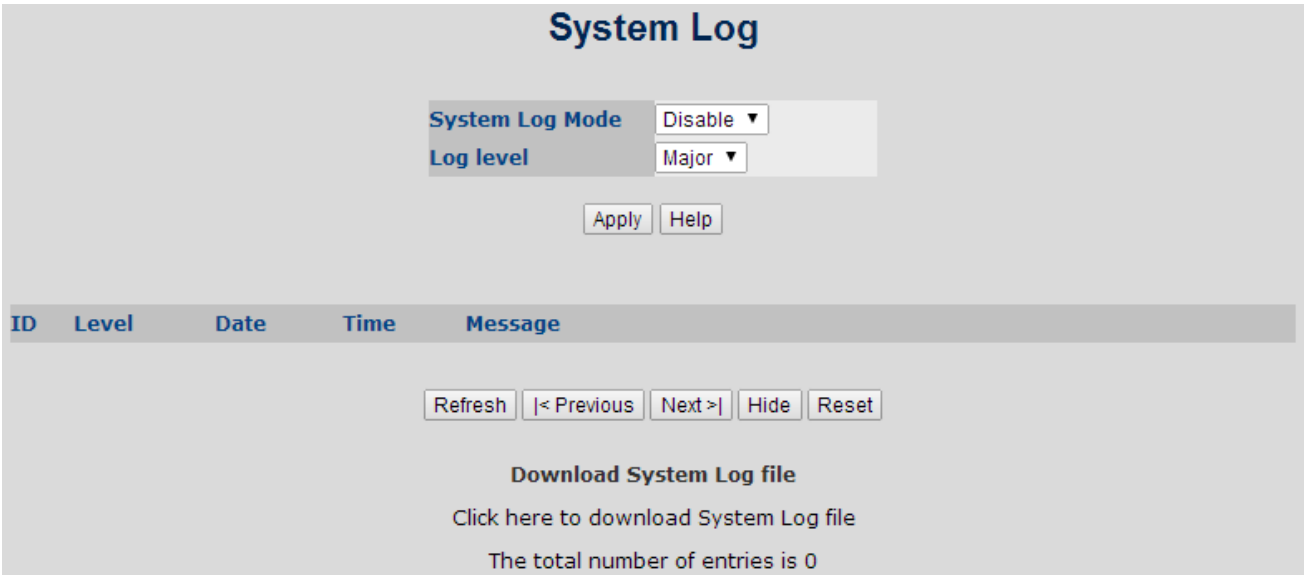


Figure 4-2-6-1: System Log Web Interface

The page includes the following fields:

Object	Description
System Log Mode	Enable/disable System Log service
Log level	• **Major**: only send major syslog to syslog server, e.g., link up/down, system warm/cold start • **All**: send all syslog messages to syslog server.

4.2.7 SMTP Setting

The SMTP alarm allows user to set e-mail account and receiver account; system will send error message via e-mail if there is an event happened.

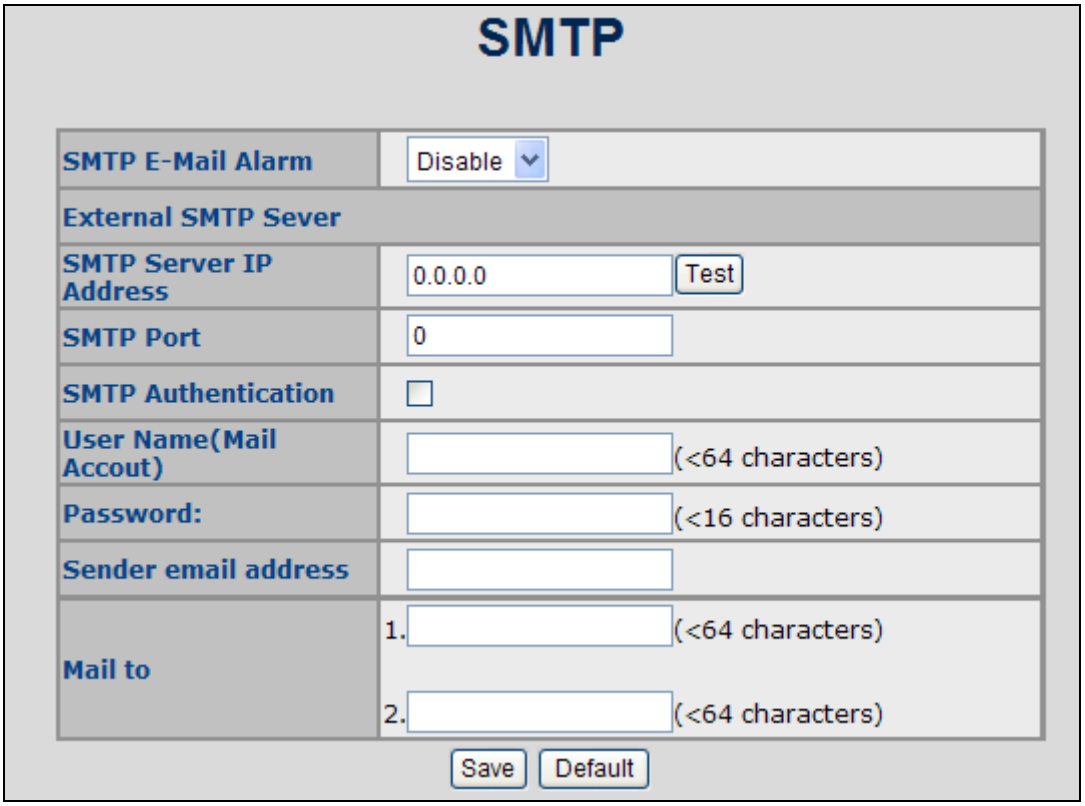


Figure 4-2-7-1: System Log Screenshot

The page includes the following fields:

Object	Description
SMTP E-Mail Alarm	Allows user to enable or disable SMTP alarm function.
SMTP Server IP Address	For inputting SMTP server IP address
SMTP Port	For inputting SMTP port number, the default value is 25.
SMTP Authentication	Allows user to enable SMTP authentication. Because SMTP server denies relaying mail to a different domain, user has to set a valid account for relaying

	mail. If the mail just sends to the same domain, it may not need SMTP authentication. Please consult with your network administrator first.
User (Mail Account)	For inputting mail account name, not mail address.
Password	For inputting mail account password.
Sender Email Address	For inputting the e-mail address from administrator.
Mail to	Allows user to input mail address where alarm will be notified.

4.2.8 SNTP Setting

The Simple Network Time Protocol (SNTP) allows user to configure the Managed Switch to send time synchronization requests to specific time servers (i.e., client mode) via IP address.

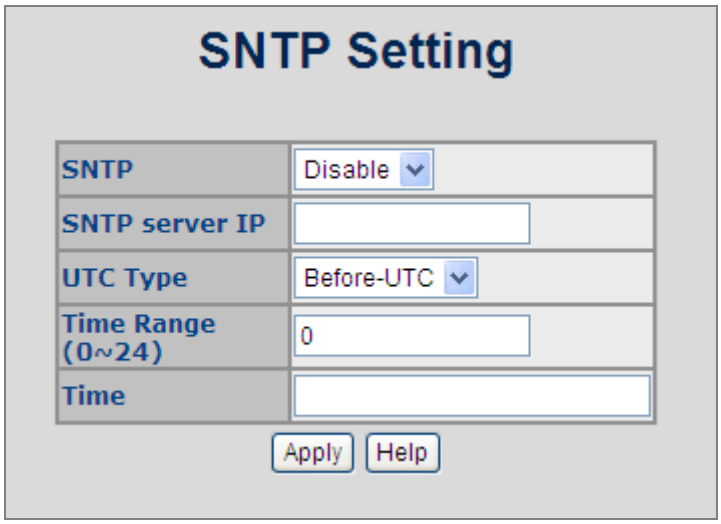


Figure 4-2-8-1: SNTP Setting Web Interface

The page includes the following fields:

Object	Description
SNTP	Enable or Disable SNTP Feature.
SNTP server IP	Allows to assign an SNTP sever IP address here.
UTC Type	Allows user to select time zone. For example, if your location is in Taipei (UTC+08), you have to choose After-UTC. If your location is in San Francisco (UTC-08), you have to choose Before-UCT.
Time Range (0~24)	Allows user input time range. For example, if time zone is UTC+08, input 8; if time zone is UTC-05, input 5.
Time	Shows current time after being connected to NTP server.

4.2.9 Alarm Configuration

This page allows the user to configure Alarm Configuration.

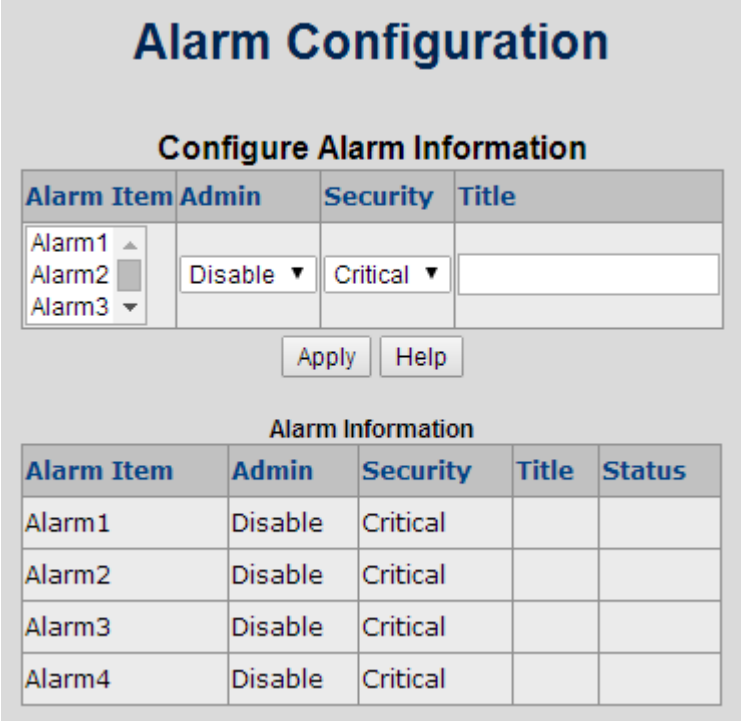
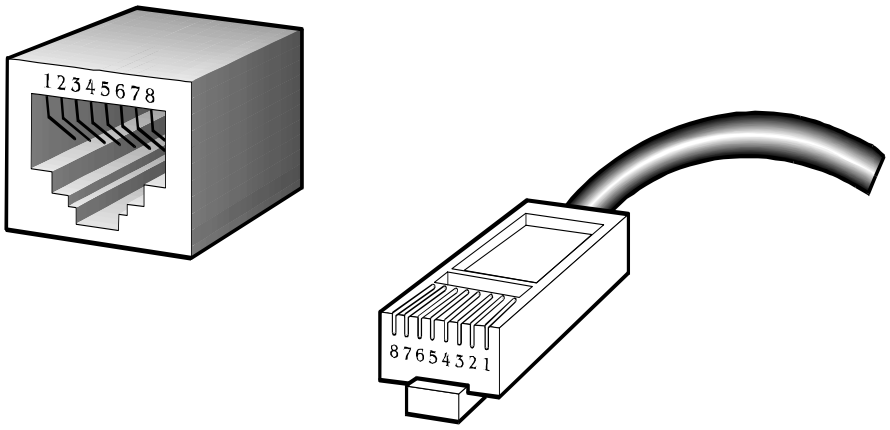


Figure 4-2-9-1: Alarm Configuration

Object	Description
Alarm Item	Select the alarm group.
Admin	Enable/disable the alarm group.
Security	Allow user to define security priority for the alarm output; the feature is for note only.
Title	Allow user to define description for the alarm output; the feature is for note only.
Status	Display the alarm group status

Alarm groups status and Alarm RJ45 pin definitions:

RJ45 Pin	Group	Short Circuit (Over 10 seconds)	Open Circuit
1, 2	**Alarm1**	**SYS LED: Red** **Alarm1 status: Happen**	**SYS LED: Green** **Alarm1 status: Clear**
3, 4	**Alarm2**	**SYS LED: Red** **Alarm2 status: Happen**	**SYS LED: Green** **Alarm2 status: Clear**
5, 6	**Alarm3**	**SYS LED: Red** **Alarm3 status: Happen**	**SYS LED: Green** **Alarm3 status: Clear**
7, 8	**Alarm4**	**SYS LED: Red** **Alarm4 status: Happen**	**SYS LED: Green** **Alarm4 status: Clear**



4.2.10 Smart Fan

This page allows the user to configure Smart Fan Configuration.

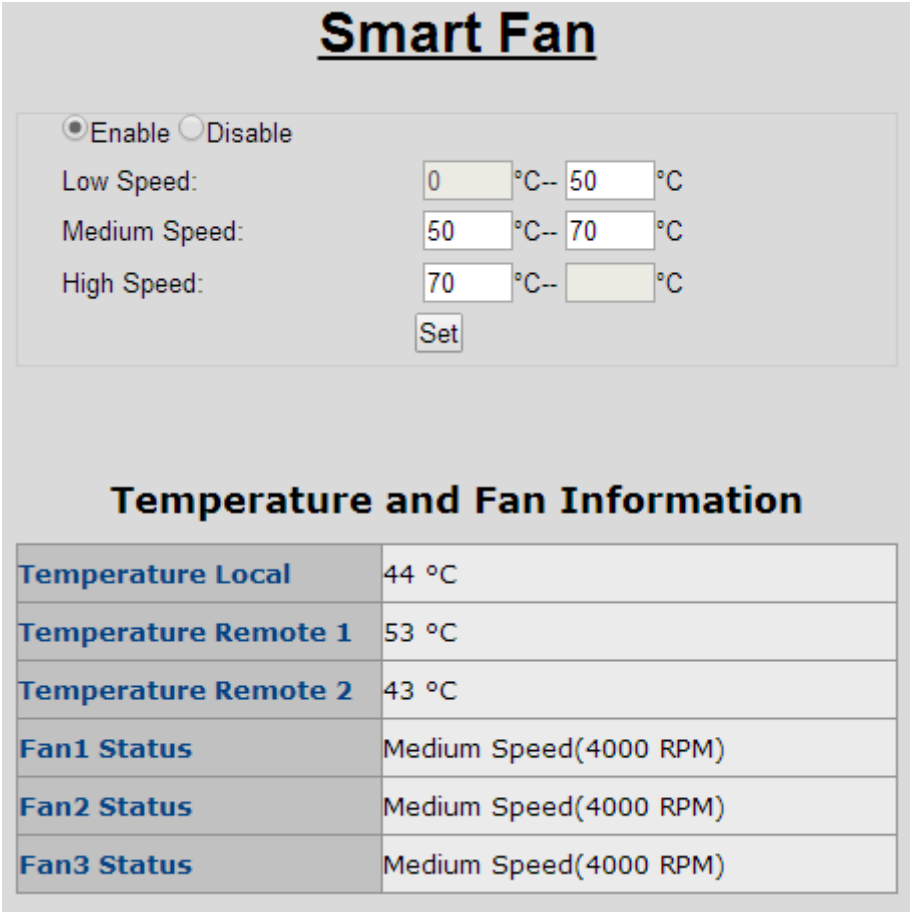


Figure 4-2-10-1: Smart Fan Configuration

The page includes the following fields:

Object	Description
Enable	Enable the Smart Fan feature.
Disable	Disable the Smart Fan feature.
Low Speed	Allows user to define temperature zone with low speed fan.
Medium Speed	Allows user to define temperature zone with medium speed fan.

High Speed	Allows user to define temperature zone with high speed fan.

If the temperature zone is modified without default value, it could damage the switch especially in the harsh environment.

4.2.11 Firmware Upgrade

It provides the functions allowing the user to update the switch firmware via 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.

4.2.11.1 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 4-2-11-1 appears.

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

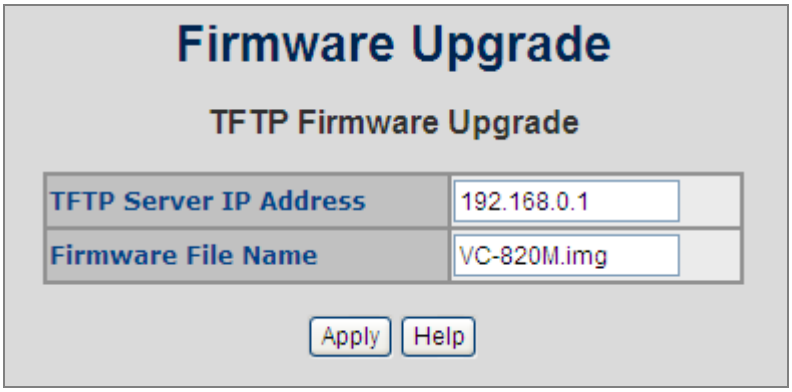


Figure 4-2-11-1: Firmware Upgrade Interface

The page includes the following fields:

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

4.2.11.2 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 4-2-11-2 appears.

Figure 4-2-11-2: HTTP Firmware Upgrade Interface

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

1. Click System -> Web Firmware Upgrade.
2. The Firmware Upgrade screen is displayed as in Figure 4-2-11-3.
3. Click the "Browse" button of the main page and the system would pop up the file selection menu to choose firmware.

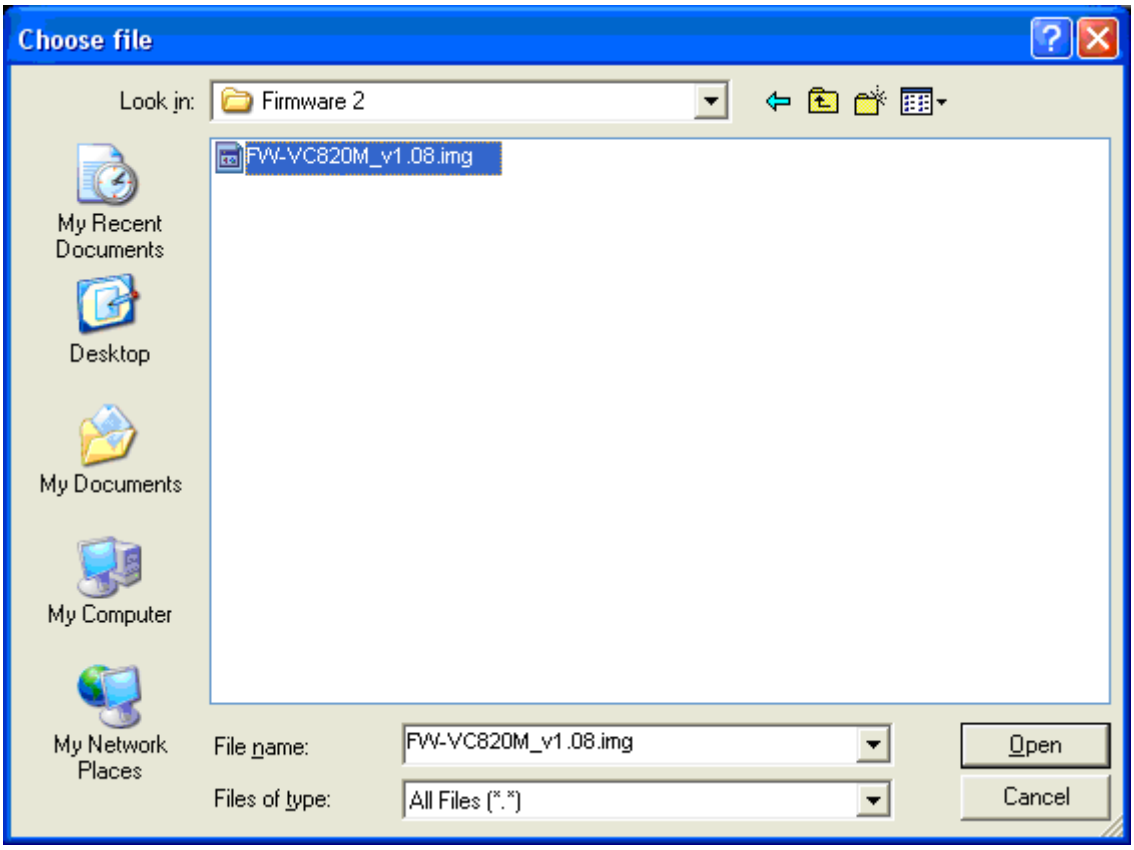


Figure 4-2-11-3: HTTP Firmware Upgrade Selection Window

4. Select on the firmware and then click "**Submit**", and the Software Upload Progress would show the upload status.

Firmware upgrade needs several minutes. Please wait a while, and then manually refresh the webpage.

4.2.12 Configuration Backup

4.2.12.1 TFTP Restore Configuration

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

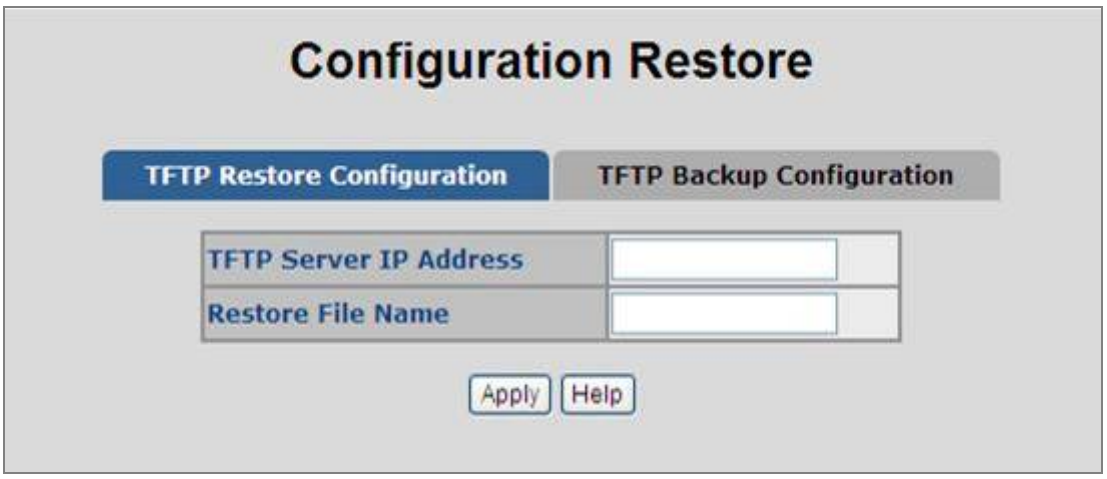


Figure 4-2-12-1: TFTP Configuration Restore Interface

The page includes the following fields:

Object	Description
TFTP Server IP Address:	Type in the TFTP server IP.
Restore File Name:	Type in the correct file name for restoring.

4.2.12.2 HTTP Config File Restore

You can also restore the previous backup configuration from the current workstation utilizing internet browser, such as Microsoft Internet Explore or Mozilla Firefox, to recover the settings. Before doing that, you must locate the image file on the local management station first and the Managed Switch will download back the flash image

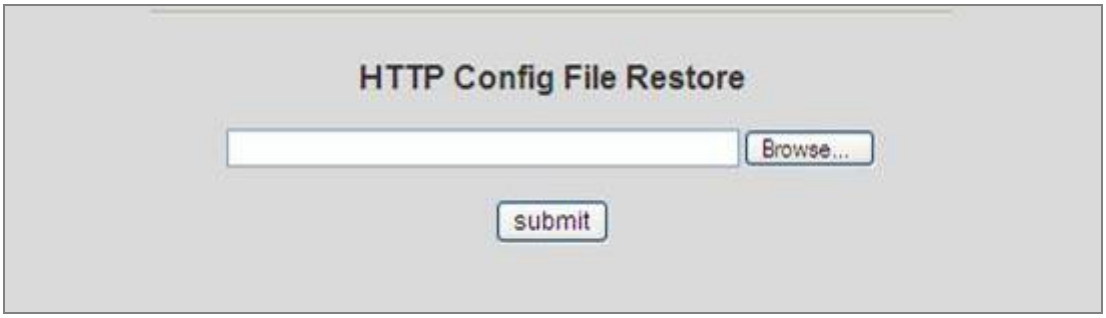


Figure 4-2-12-2: HTTP Configuration Restore Interface

4.2.12.3 TFTP Backup Configuration

You can back up the current configuration from flash ROM to the TFTP server for the purpose of recovering the configuration later. It helps you to avoid wasting time on configuring the settings by backing up the configuration.

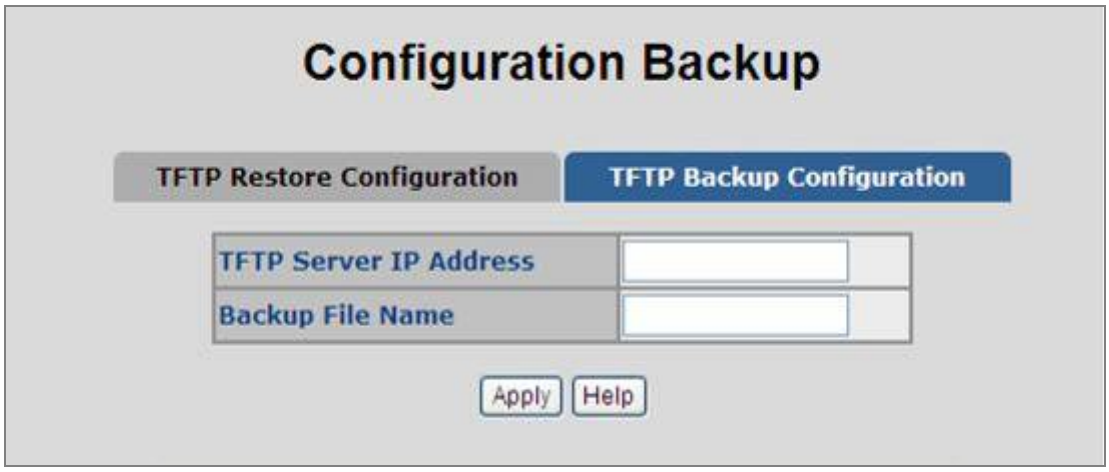


Figure 4-2-12-3: TFTP Configuration Backup Interface

The page includes the following fields:

Object	Description
TFTP Server IP Address:	Type in the TFTP server IP.
Backup File Name:	Type in the file name that will be back up on the TFTP server.

4.2.12.4 HTTP Config File Backup

This function allows backing up the current configuration of the Managed Switch to the local management station. The screens in Figure 4-2-12-4 and Figure 4-2-12-5 appear.

Figure 4-2-12-4: HTTP Configuration File Backup Interface

Move the cursor to "Click here to download configuration file" and click. The backup configuration file will be packaged as a "config.tar" file as default.

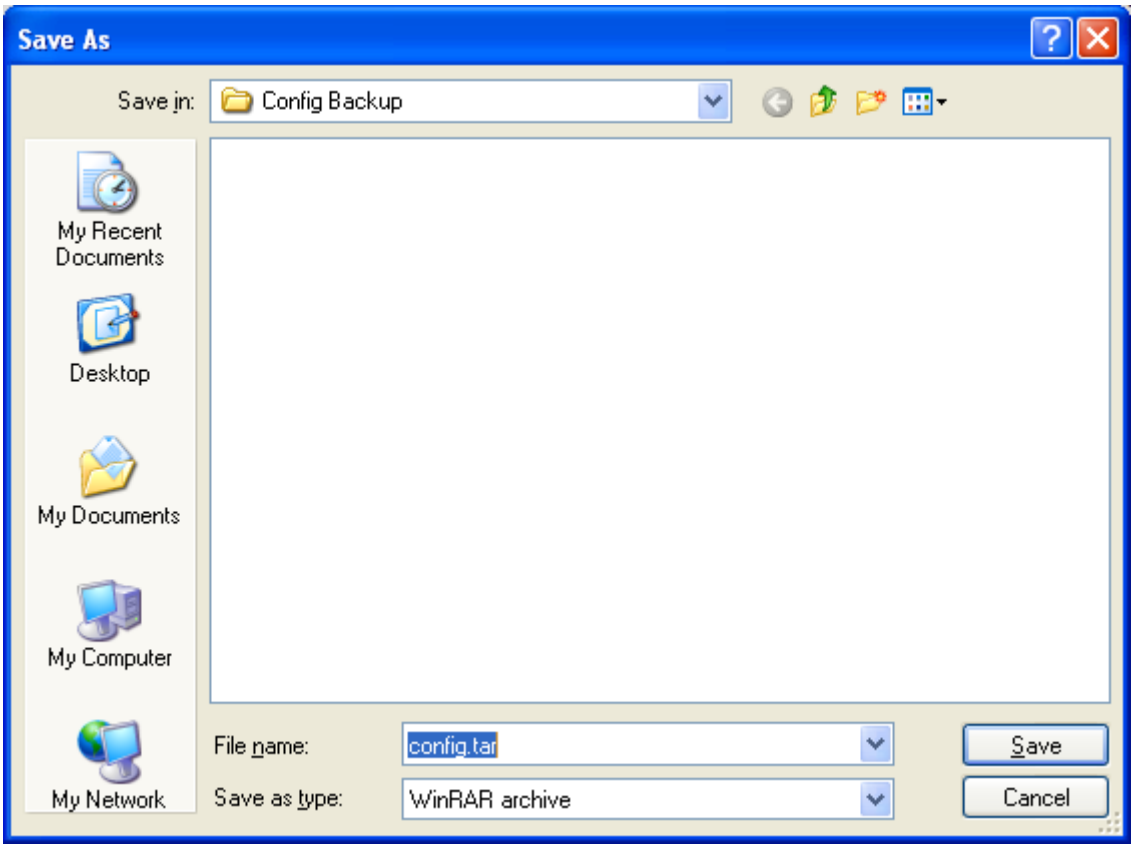


Figure 4-2-12-5: HTTP Configuration Backup Window

4.2.13 Factory Default

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

Figure 4-2-13-1: Factory Default Interface

4.2.14 System Reboot

Reboot the switch in software reset. Click Reboot to reboot the system.

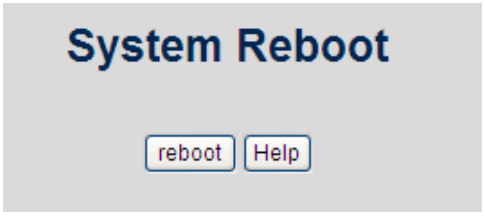


Figure 4-2-14-1: System Reboot Interface

4.3 Port Configuration

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

- **Port Control** Configures port connection settings
- **Rate Control** Configures port rate settings
- **Port Status** Displays the current port link status and speed, etc.
- **Port Statistics** Lists Ethernet and RMON port statistics
- **Port Sniffer** Sets the source and target ports for mirroring
- **Protected Port** Configures protected ports and groups

4.3.1 Port Control

In Port control, you can configure the settings of each port to control the connection parameters, and the status of each port is listed below.

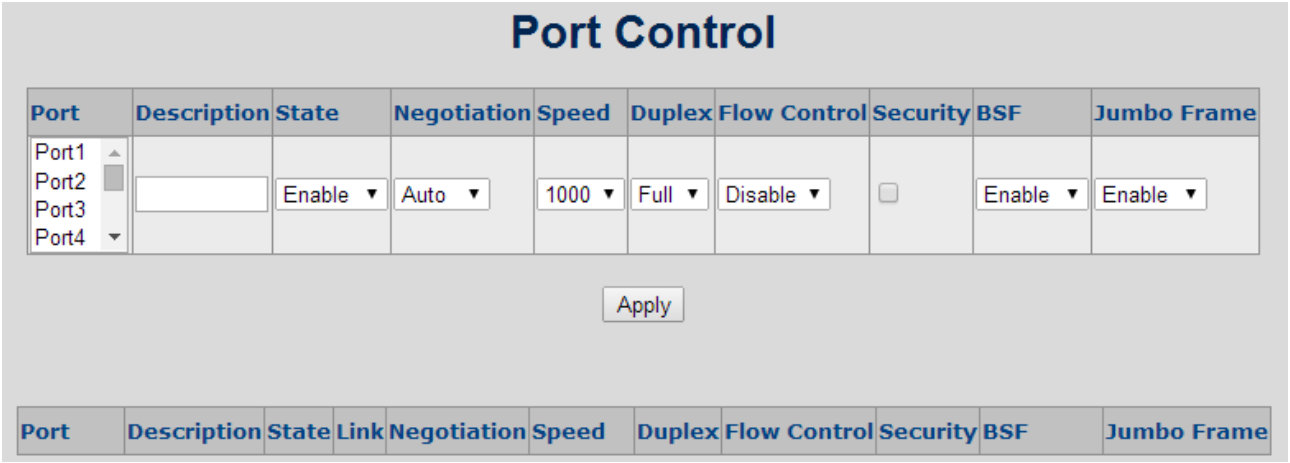


Figure 4-3-1: Port Control Interface

The page includes the following fields:

Object	Description
Port:	Use the scroll bar and click on the port number to choose the port to be configured.
State:	Current port state. The port can be set to disable or enable mode. If the port state is set as 'Disable', it will not receive or transmit any packet.
Negotiation:	The item is only for **Gigabit ports** of the Managed Switch. **Auto** and **Force**. Being set as Auto, the speed and duplex mode are negotiated automatically. When you set it as Force, you have to set the speed and duplex mode manually.
Speed:	The item is only for **Gigabit ports** of the Managed Switch. It is available for selecting when the Negotiation column is set as Force. When the Negotiation column is set as Auto, this column is read-only.

Duplex:	The item is only for **Gigabit ports** of the Managed Switch. It is available for selecting when the Negotiation column is set as Force. When the Negotiation column is set as Auto, this column is read-only.
Flow Control:	Whether or not the receiving node sends feedback to the sending node is determined by this item. When enabled, once the device exceeds the input data rate of another device, the receiving device will send a PAUSE frame which halts the transmission of the sender for a specified period of time. When disabled, the receiving device will drop the packet if too much to process.
Security:	A port in security mode will be "**locked**" without permission of address learning. Only the incoming packets with SMAC already existing in the address table can be forwarded normally. User can disable the port from learning any new MAC addresses, then use the static MAC addresses screen to define a list of MAC addresses that can use the secure port. Enter the settings and then click the Apply button to change on this page.
BSF:	User can disable/enable port **broadcast storm filtering** option by port. The filter mode and filter packet type can be selected in Switch Setting > **Misc Config** page.
Jumbo Frame:	User can disable/enable port jumbo frame option by port. When port jumbo frame is enabled, the port forward jumbo frame packet.

The Managed Switch supports up to **9Kbytes** jumbo frame forwarding.

4.3.2 Rate Control

The rate control allows user to do rate limit speed to the specific port.

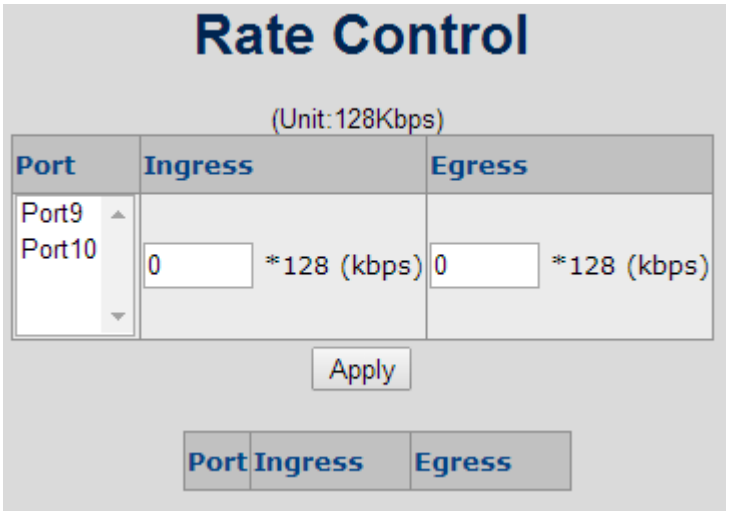


Figure 4-3-2: Rate Control Interface

The page includes the following fields:

Object	Description
Rate Control: **(Unit: 128KBbps)**	Port-9 ~ Port-10 support by-port ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set its effective egress rate at 1Mbps and ingress rate at 500Kbps. Device will perform flow control or backpressure to confine the ingress rate to meet the specified rate.
Port	Allows user to choose which port will be limited rate speed.
Ingress	Type the port effective ingress rate. The valid range is **0 ~ 8000**. The unit is **128K**. 0: disable rate control. 1 ~ 8000: valid rate value
Egress	Type the port effective egress rate. The valid range is **0 ~ 8000**. The unit is **128K**. 0: disable rate control. 1 ~8000: valid rate value.

4.3.3 Port Status

This page displays the current port configurations and operating status -- it is a summary table of ports' configurations. Via the summary table, you can know status of each port clearly at a glance, like Port Link Up/Link Down Status, Negotiation, Link Speed, Rate Control, Duplex Mode and Flow Control.

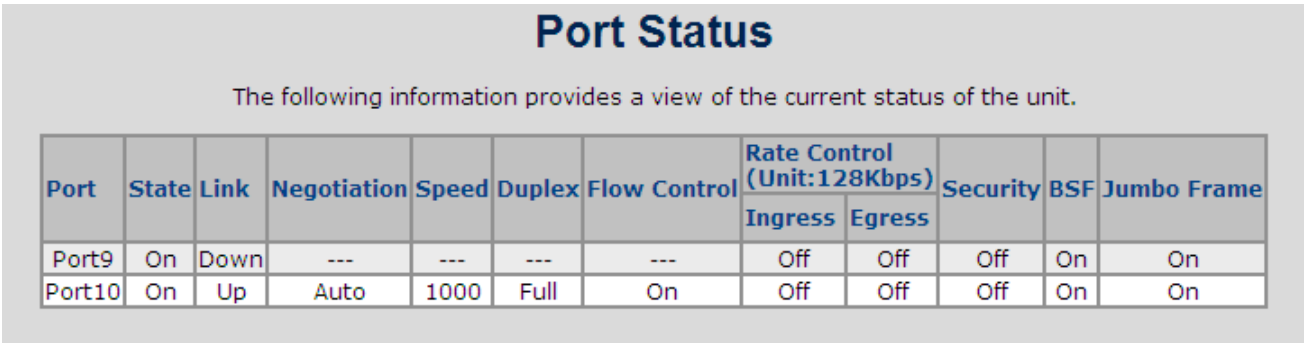


Figure 4-3-3: Port Status Interface

4.3.4 Port Statistics

The following chart provides the current statistic information which displays the real-time packet transfer status for each port. The user might use the information to plan and implement the network, or check and find the problem when the collision or heavy traffic occurs.

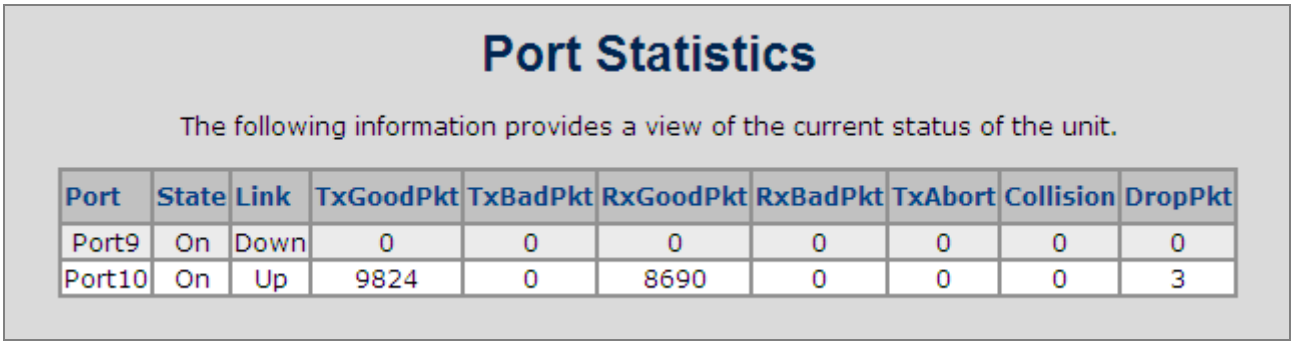


Figure 4-3-4: Port Statistics Interface

The page includes the following fields:

Object	Description
Port:	The port number.
State:	It's set by Port Control. When the state is disabled, the port will not transmit or receive any packet.
Link:	The status of linking—'**Up**' or '**Down**'.
Tx Good Packet:	The counts of transmitting good packets via this port.
Tx Bad Packet:	The counts of transmitting bad packets (including undersize [less than 64 octets], oversize, CRC Align errors, fragments and jabbers packets) via this port.
Rx Good Packet:	The counts of receiving good packets via this port.
Rx Bad Packet:	The counts of receiving good packets (including undersize [less than 64 octets], oversize, CRC error, fragments and jabbers) via this port.
Tx Abort Packet:	The aborted packet while transmitting.
Packet Collision:	The counts of collision packet.
Packet Dropped:	The counts of dropped packet.

4.3.5 Port Sniffer

The Port Sniffer (mirroring) is a method for monitoring traffic in switched networks. Traffic through a port can be monitored by one specific port. That is, traffic goes in or out a monitored port will be duplicated into sniffer port.

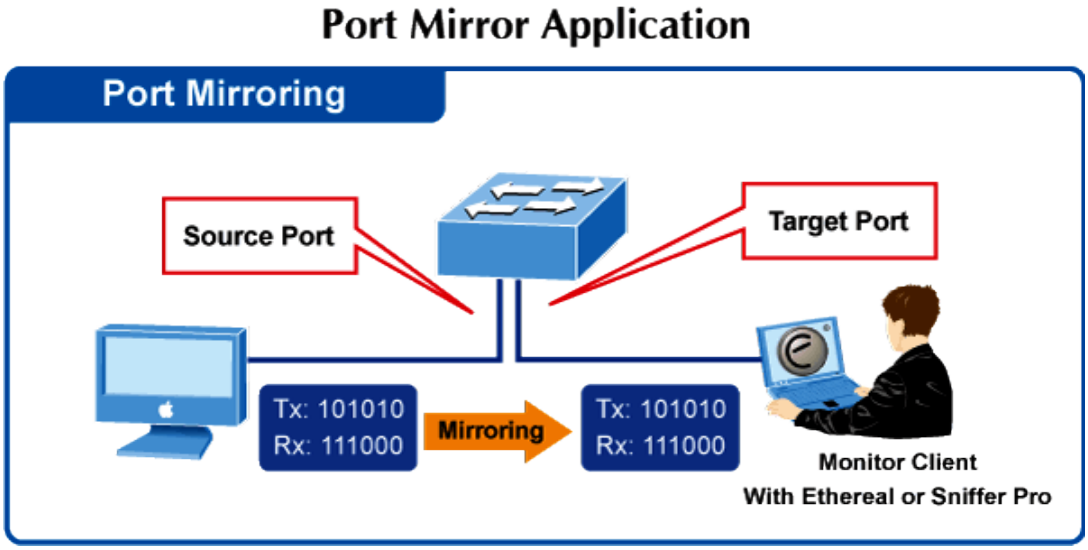


Figure 4-3-5: Port Mirror Application

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

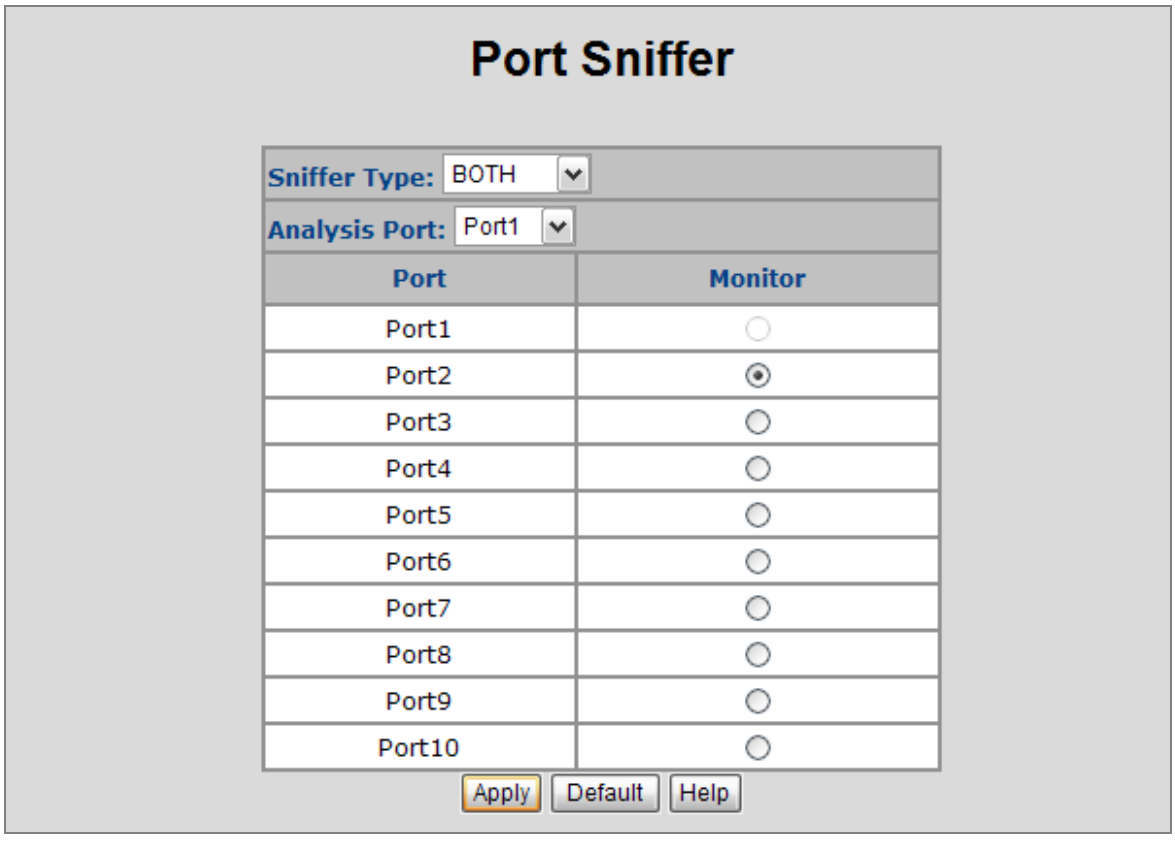


Figure 4-3-6: Port Sniffer Interface

The page includes the following fields:

Object	Description
Sniffer Type:	Select a sniffer mode: • **DISABLE** • **RX** • **TT** • **BOTH**
Analysis (Monitoring) Port:	It means Analysis port can be used to see the traffic on another port you want to monitor. You can connect Analysis port to LAN analyzer or netxray.
Monitored Port:	The port you want to monitor. The monitor port traffic will be copied to Analysis port. You can select one monitor port in the switch. User can choose which port that they want to monitor in only one sniffer type.

1 When the Mirror Mode is set to **RX** or **TX** and the **Analysis Port** is selected, the packets to and from the **Analysis Port** will not be transmitted. The Analysis Port will accept only copied packets from the **Monitored Port**.

2 If you want to disable the function, you must select monitor port to none.

4.3.6 Protected Port

There are two protected port groups; ports in different groups can't communicate. In the same group, protected ports can't communicate with each other, but can communicate with unprotected ports. Unprotected ports can communicate with any ports, including protected ports.

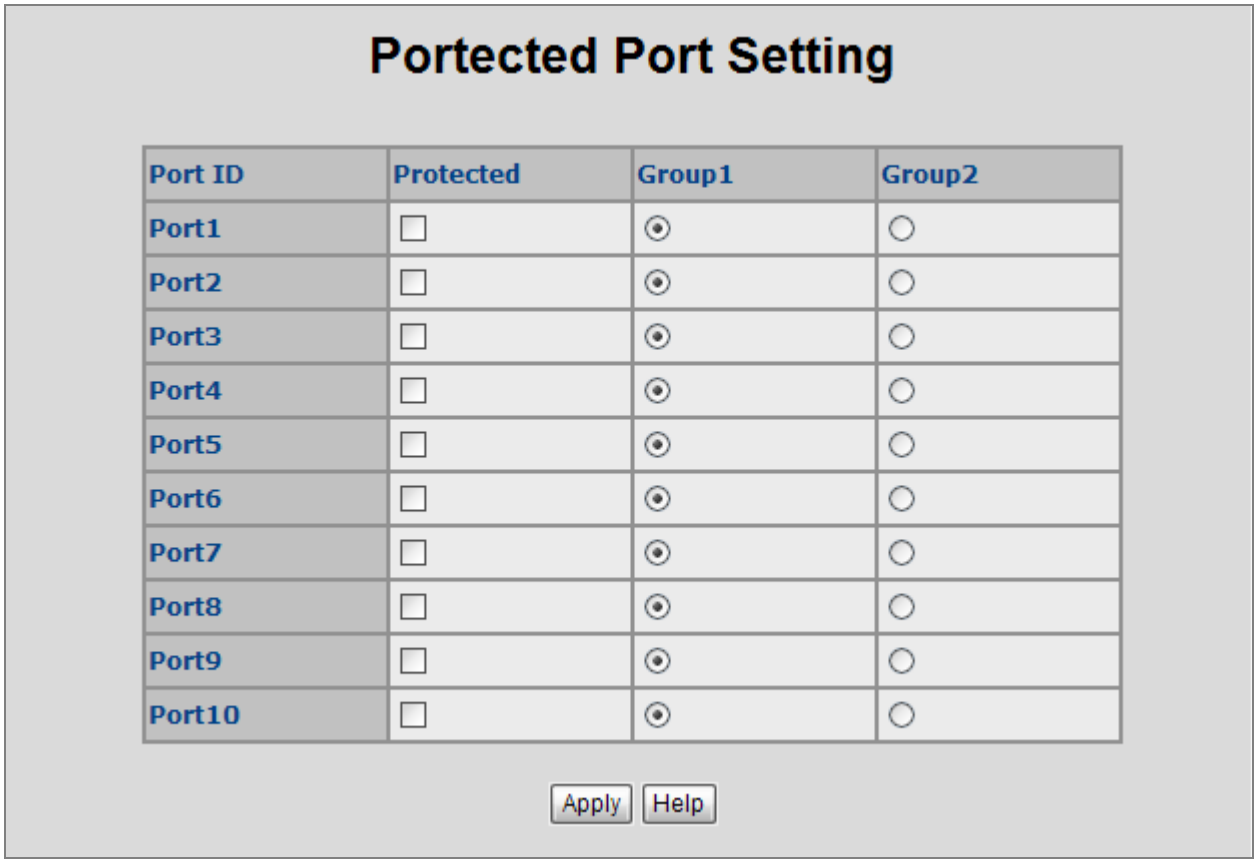


Figure 4-3-7: Protected Port Setting Web Interface

The page includes the following fields:

Object	Description
Port ID	Identify the Managed Switch interface.
Protected	Enable the Protected function on the selected port. If the check box is not shown as ☑ , then this port a unprotected port and it can communicate with any ports - including protected ports
Group 1	Set the protected port to be Group 1 member.
Group 2	Set the protected port to be Group 2 member.

Note

Usually, set the **Uplink port** or the Port is connected to Core switch or router to be the **Un-protected port**.

4.4 VLAN Configuration

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.

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.

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

■ Port-based VLAN

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

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

■ IEEE 802.1Q VLANs

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

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

Some relevant terms:

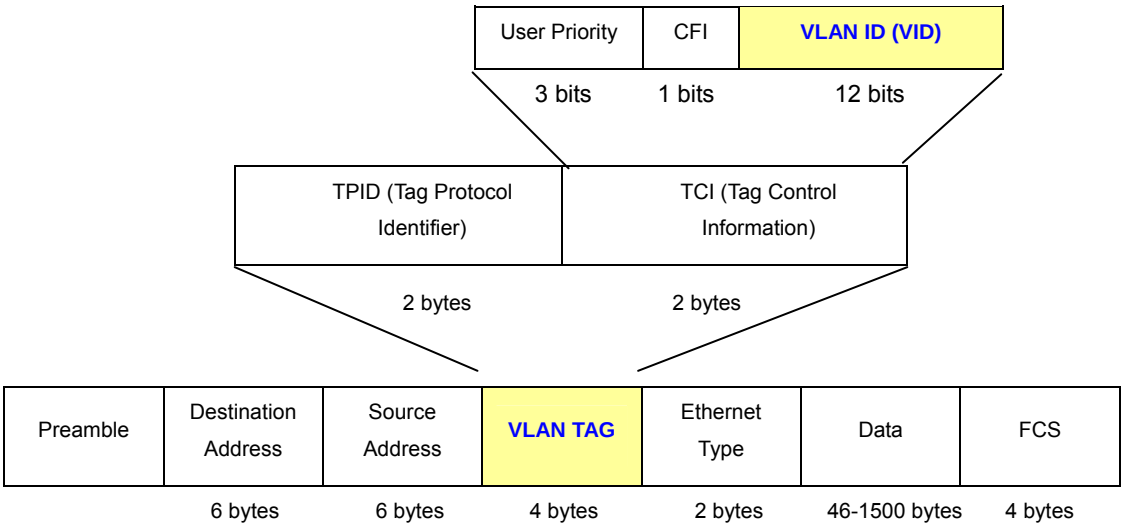
- **Tagging** - The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** - The act of stripping 802.1Q VLAN information out of the packet header.

■ 802.1Q VLAN Tags

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

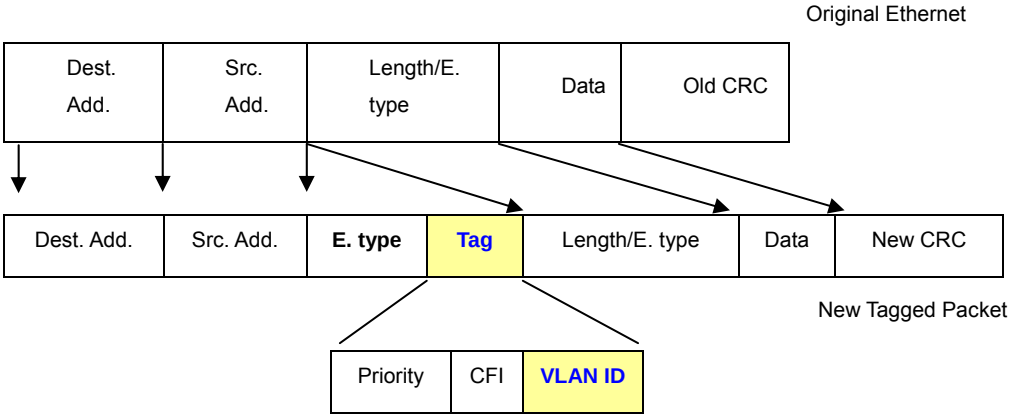
The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

802.1Q Tag



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

Adding an IEEE802.1Q Tag



■ Port VLAN ID

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

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

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

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

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

■ Default VLANs

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

■ VLAN and Link Aggregation Groups

In order to use VLAN segmentation in conjunction with port link aggregation groups, you can first set the port link aggregation group(s), and then you may configure VLAN settings. If you wish to change the port link aggregation grouping

with VLAN already in place, you will not need to reconfigure the VLAN settings after changing the port link aggregation group settings. VLAN settings will automatically change in conjunction with the change of the port link aggregation group settings.

4.4.2 Static VLAN Configuration

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

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

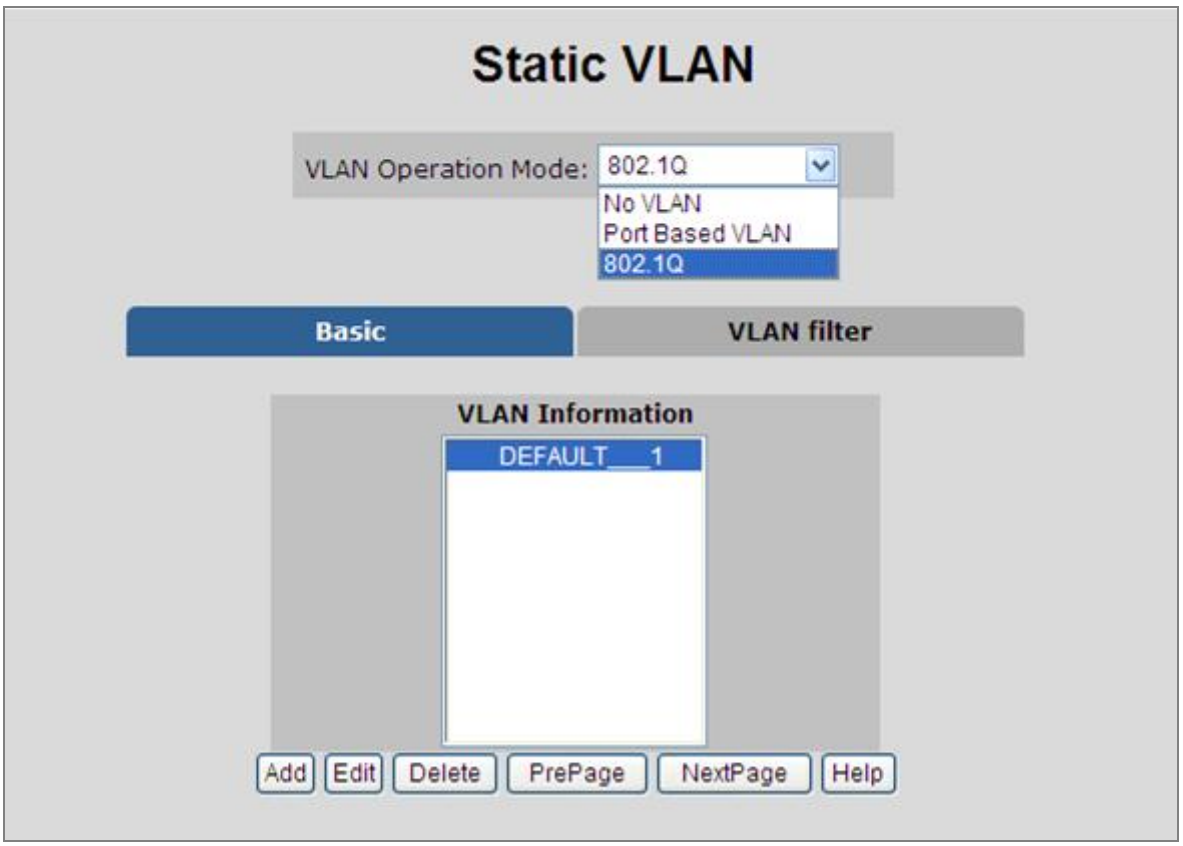


Figure 4-4-2-1: Static VLAN interface

Note

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

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

4.4.3 Port-based VLAN

Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN is enabled, the VLAN-tagging is ignored.

In order for an end station to send packets to different VLANs, it itself has to be either capable of tagging packets it sends with VLAN tags or attached to a VLAN-aware bridge that is capable of classifying and tagging the packet with a different VLAN ID based on not only default PVID but also other information about the packet, such as the protocol.

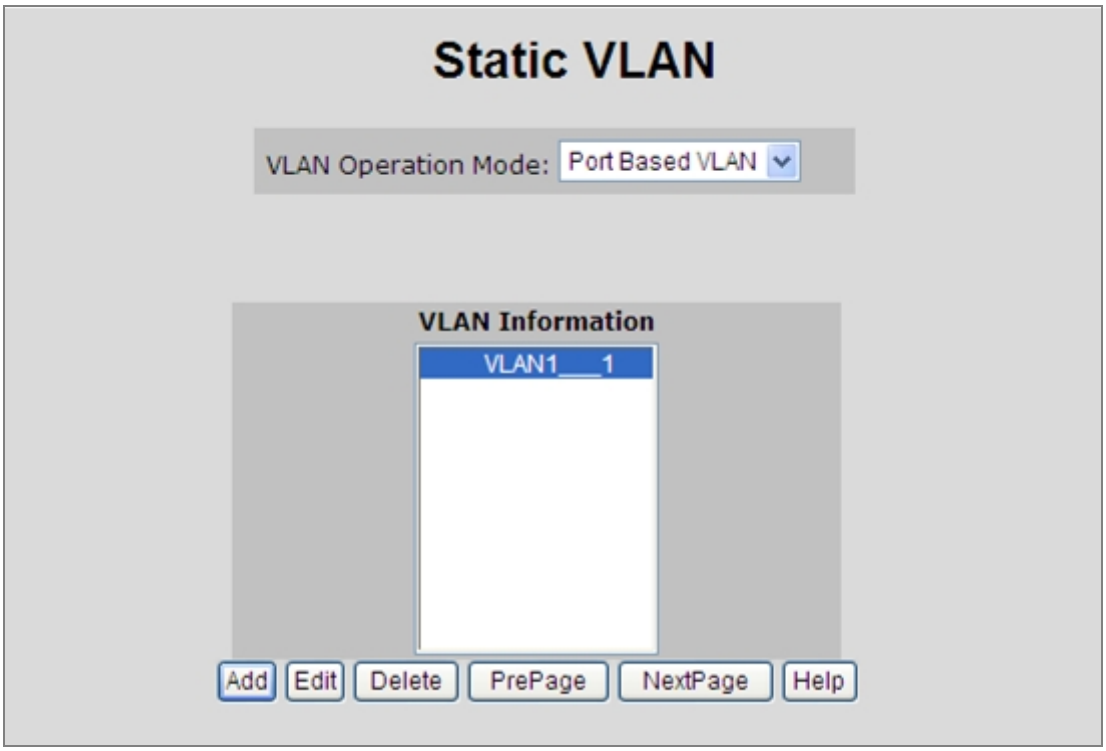


Figure 4-4-3-1: Port-based VLAN Interface

■ **Create a VLAN and Add Member Ports to it**

1. Click the hyperlink **"VLAN"\"Static VLAN"** to enter the VLAN configuration interface.
2. Select "**Port based VLAN**" in the VLAN Operation Mode to enable the port-based VLAN function.
3. Click "**Add** "to create a new VLAN group. Then the following **Figure 4-4-3** appears.
4. Type a name and Group ID for the new VLAN; the available range is **2-4094**.
5. From the Available ports box, select ports to add to the Managed Switch and click "**Add"**.
6. Click **Apply**.
7. You will see the VLAN Group displays.
8. If the port-based VLAN groups list over one page, please click "**Next Page**" to view other VLAN groups on another page.
9. Use the "**Delete**" button to delete the unwanted port-based VLAN groups
10. Use the "**Edit**" button to modify the existing port-based VLAN groups.

By adding ports to the VLAN, you have created one port-based VLAN group completely.

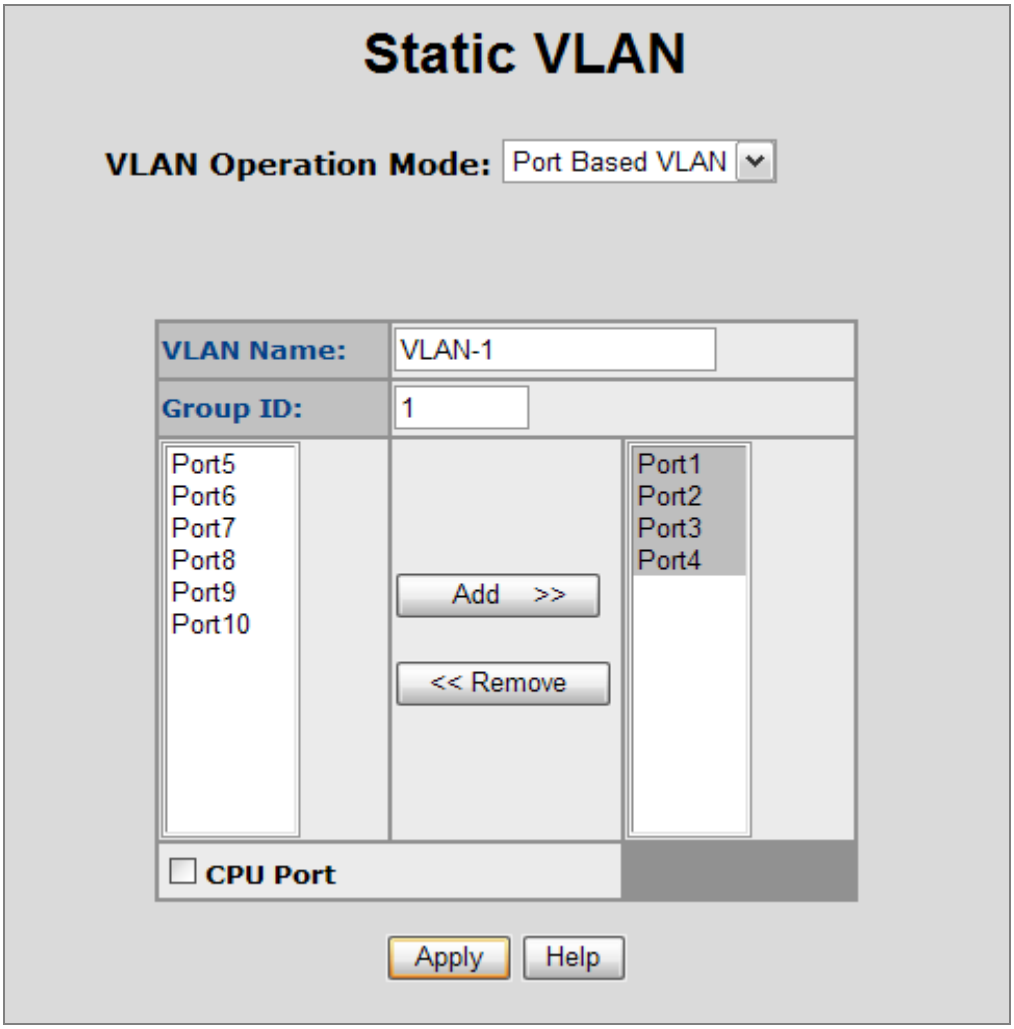


Figure 4-4-3-2: Static VLAN Interface

The page includes the following fields:

Object	Description	
VLAN Name	Use this optional field to specify a name for the VLAN. It can be up to 16 alphanumeric characters long, including blanks.	
Group ID	You can configure the ID number of the VLAN by this item. This field is used to add VLANs one at a time. The VLAN group ID and **available range is 2-4094**.	
Port	Indicate port 1 to port 10.	
Member	**Add**	Defines the interface as a Port-Based member of a VLAN.
	Remove	Forbidden ports are not included in the VLAN.

All unselected ports are treated as belonging to another single VLAN. If the port-based VLAN is enabled, the VLAN-tagging is ignored.

4.4.4 802.1Q VLAN

Tagged-based VLAN is an IEEE 802.1Q specification standard. Therefore, it is possible to create a VLAN across devices from different switch vendors. IEEE 802.1Q VLAN uses a technique to insert a "tag" into the Ethernet frames. Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.

You can create and delete tag-based VLAN. There are 256 VLAN groups to configure. Enable 802.1Q VLAN and all the ports on the switch belong to default VLAN; VID is 1. The default VLAN can't be deleted.

Understanding 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

4.4.4.1 VLAN Group Configuration

■ **VLAN Group Configuration**

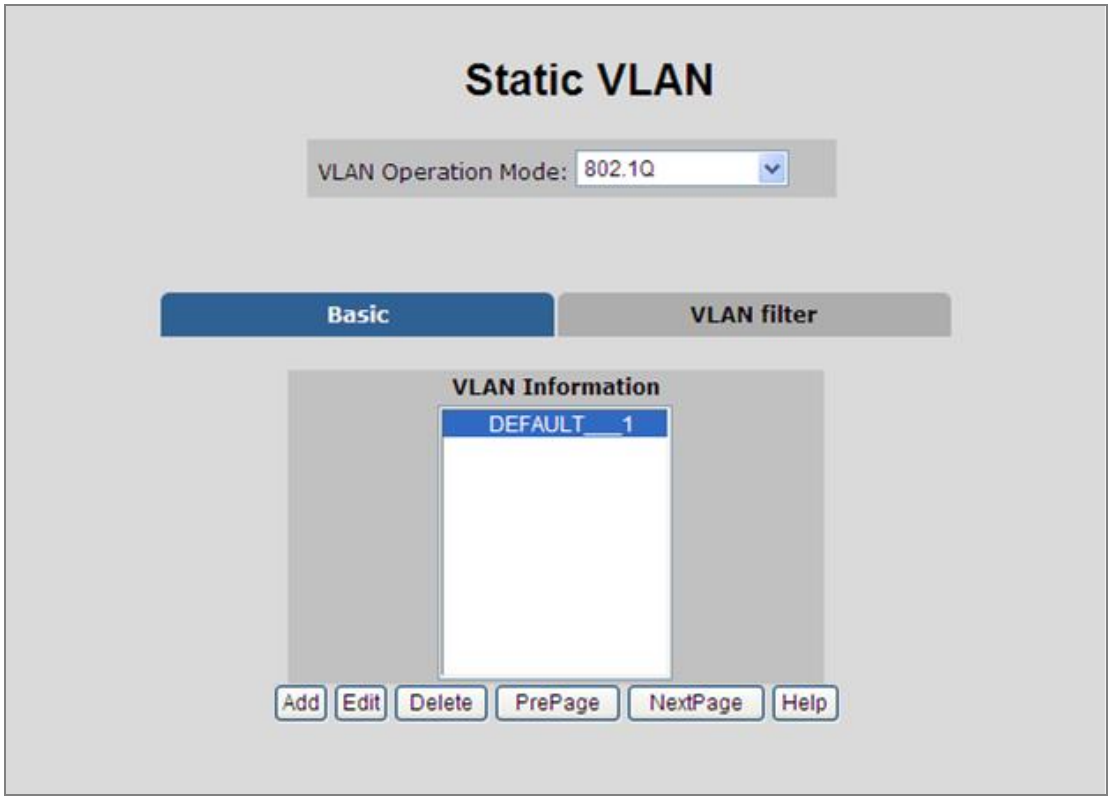


Figure 4-4-4-1: VLAN Group Configuration interface

1. Click the hyperlink "**VLAN**"\"**Static VLAN**" to enter the VLAN configuration interface.
2. Select **"802.1Q"** in the **VLAN Operation Mode** to enable the 802.1Q VLAN function.
3. Click **Add** to create a new VLAN group or Edit to the existing VLAN groups. Then the VLAN Group column appears.
4. Input a VLAN group ID and available range is 2-4094.

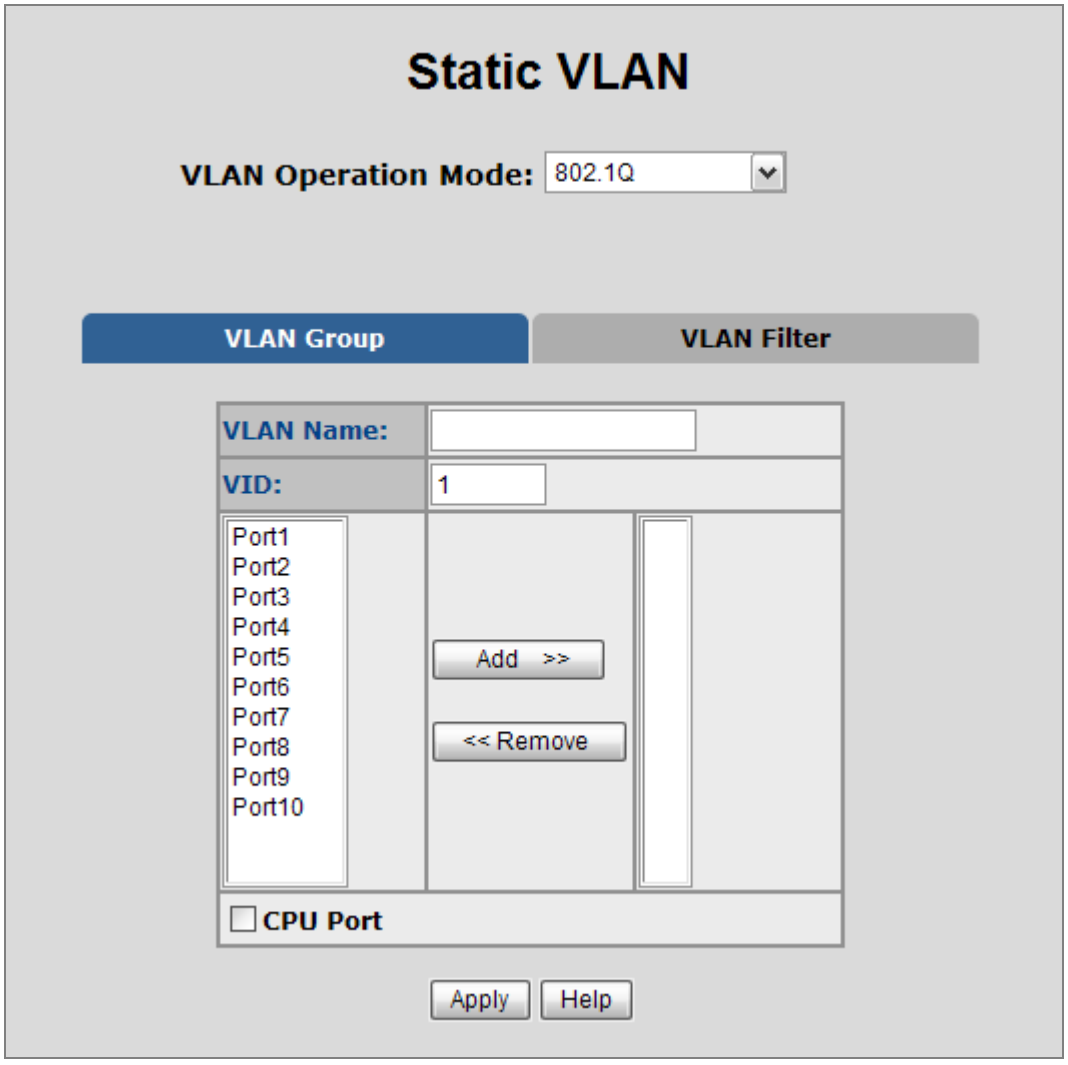


Figure 4-4-4-2: VLAN Group Configuration Interface

5. Select specific port as member port and the screen in Figure 4-4-4-3 appears.
6. After setup is completed, please press the "**Apply**" button to take effect.
7. Please press "**Back**" to return to VLAN configuration screen to add another VLAN group as the screen in Figure 4-33 appears.
8. If there are many groups that are over the limit of one page, you can click **Next** to view other VLAN groups.
9. Use the **Delete** button to delete the unwanted VLAN.
10. Use the **Edit** button to modify the existing VLAN group.

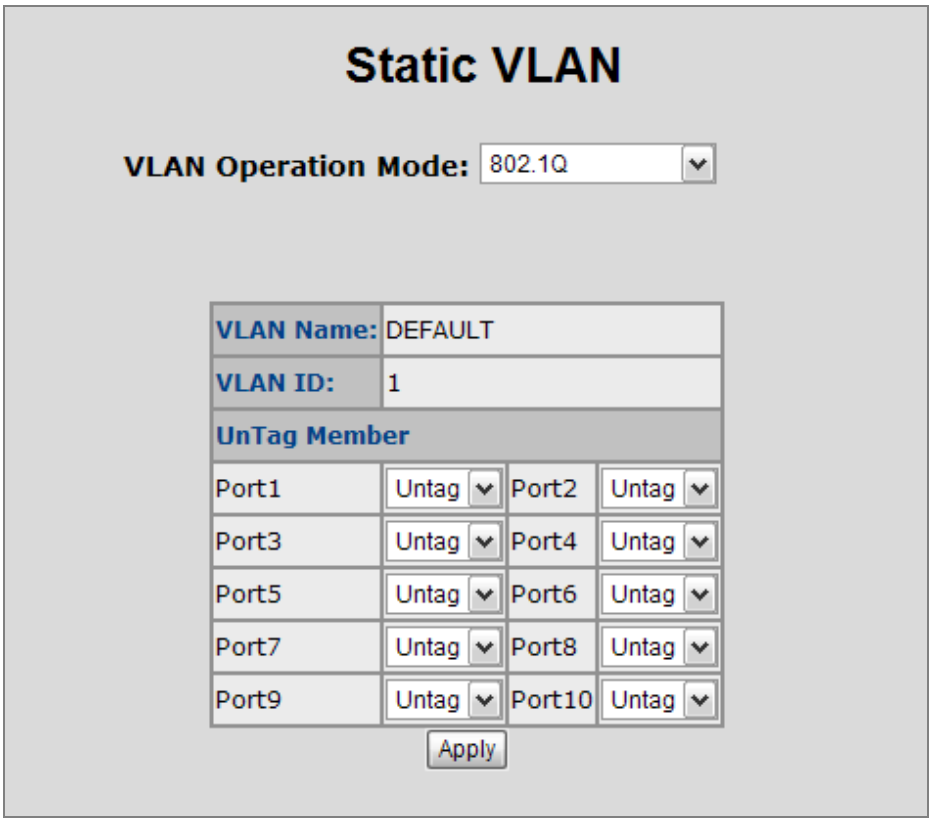


Figure 4-4-4-3: 802.1Q VLAN Setting Web Page Screen

The page includes the following fields:

Object	Description	
VLAN Name	Use this optional field to specify a name for the VLAN. It can be up to 16 alphanumeric characters long, including blanks.	
VLAN ID	You can configure the ID number of the VLAN by this item. This field is used to add VLANs one at a time. The VLAN group ID and **available range is 2-4094**.	
Port	Indicate port 1 to port 10.	
Untag Member	**Untag**	Packets forwarded by the interface are untagged.
	Tag	Defines the interface as a tagged member of a VLAN. All packets forwarded by the interface are tagged. The packets contain VLAN information.

Enable 802.1Q VLAN and all the ports on the switch belong to default VLAN; VID is 1. The default VLAN can't be deleted.

4.4.4.2 VLAN Filter

■ **802.1Q VLAN Port Configuration**

This page is used for configuring the 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.

This section provides 802.1Q Ingress Filter of each port from the Switch.

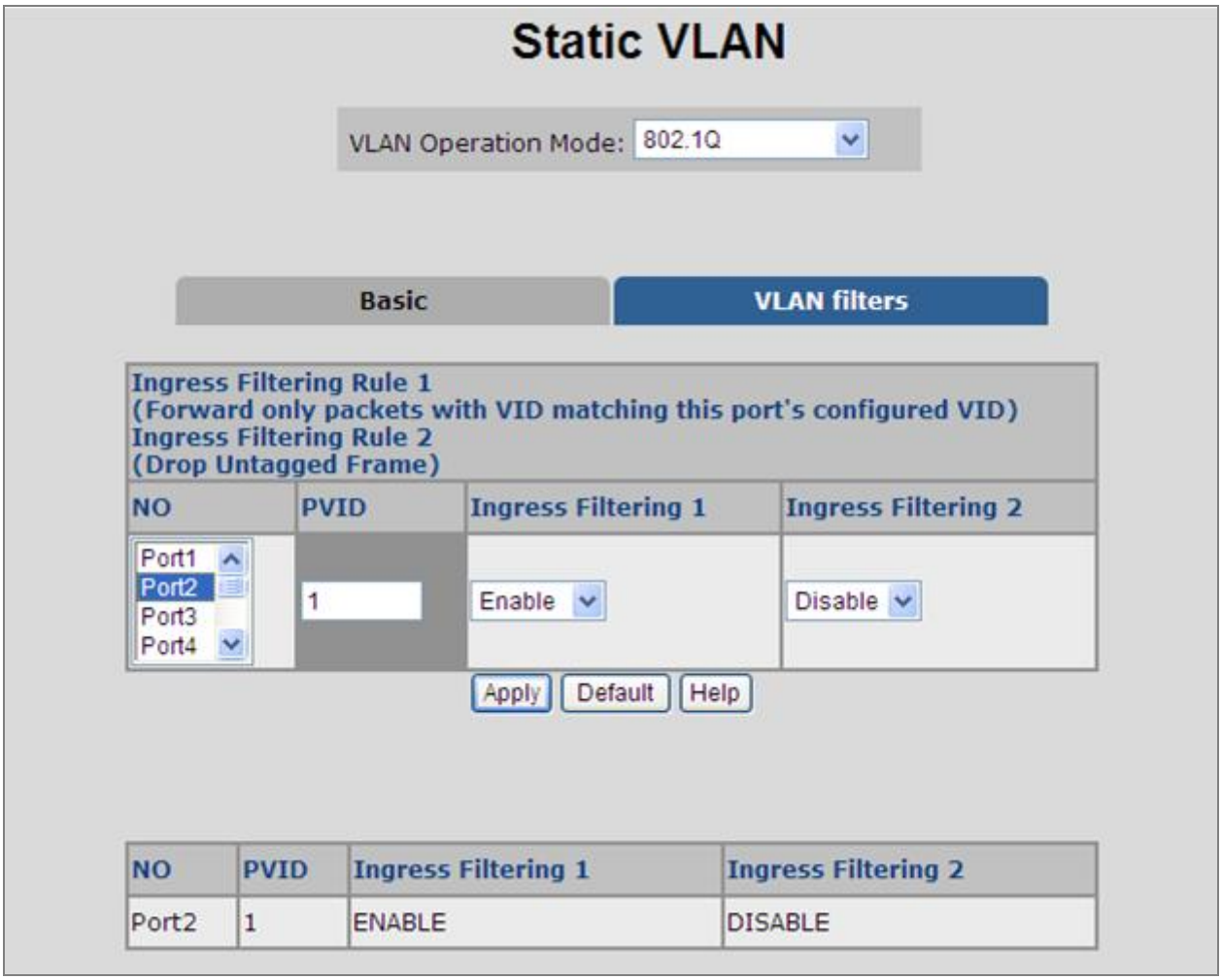


Figure 4-4-4-4: 802.1Q Ingress Filter Interface

The page includes the following fields:

Object	Description
NO	Indicate port 1 to port 10.
PVID	Set the port VLAN ID that will be assigned to untagged traffic on a given port. This feature is useful for accommodating devices that you want to participate in the VLAN but that don't support tagging. Each port allows user to set one VLAN ID; the range is 1~255. Default VLAN ID

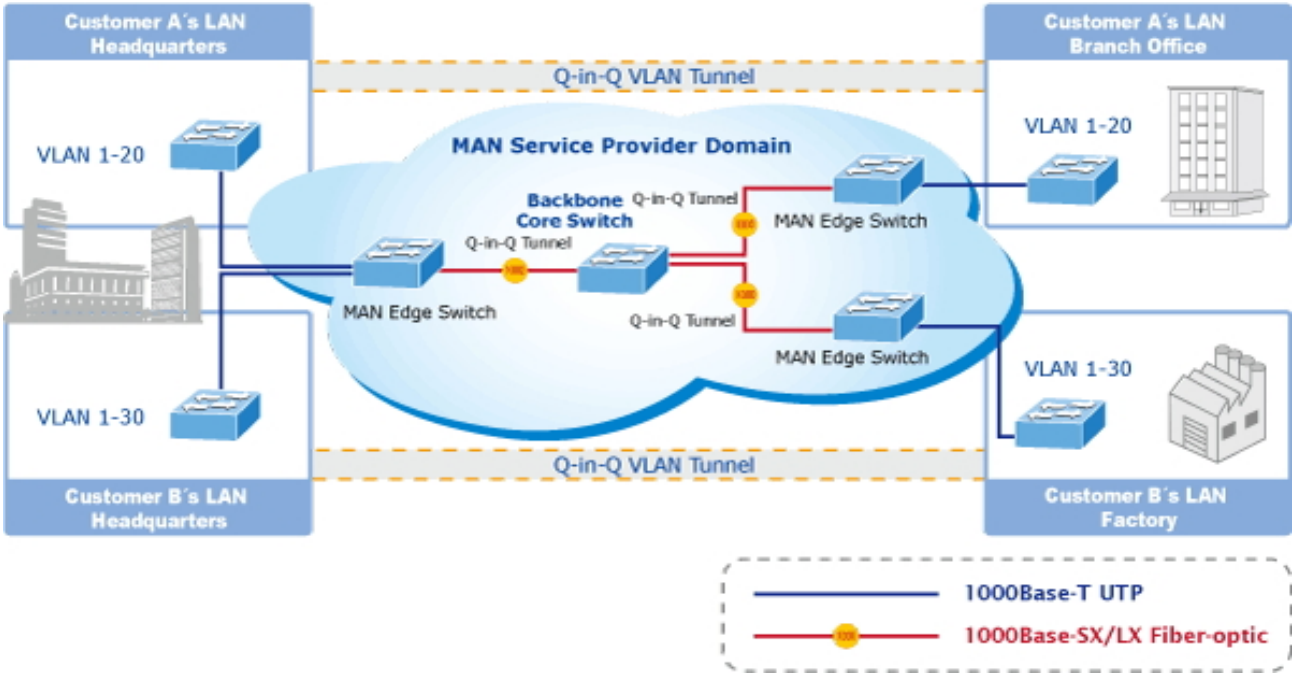
	is 1. The VLAN ID must be the same as the VLAN ID that the port belongs to VLAN group, or the untagged traffic will be dropped.
Ingress Filtering 1	Ingress filtering lets frames belonging to a specific VLAN to be forwarded if the port belongs to that VLAN. **Enable:** Forward only packets with VID matching this port's configured VID. **Disable:** Disable Ingress filter function.
Ingress Filtering 2	Drop untagged frame. **Disable:** All Packets are acceptable. **Enable:** Only packet with match VLAN ID can be permitted to go through the port.
Apply button	Press the button to save configurations.

4.4.5 Q-in-Q VLAN

■ IEEE 802.1Q Tunneling (Q-in-Q)

IEEE 802.1Q Tunneling (Q-in-Q) is designed for service providers carrying traffic for multiple customers across their networks. Q-in-Q tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting **Service Provider VLAN (SPVLAN)** tags into the customer's frames when they enter the service provider's network, and then strip the tags when the frames leave the network.

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096.



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

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

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

4.4.5.1 Q-in-Q Port Setting

The Q-in-Q VLAN**Q-in-Q Port Setting** screen in Figure 4-4-5-1 appears.

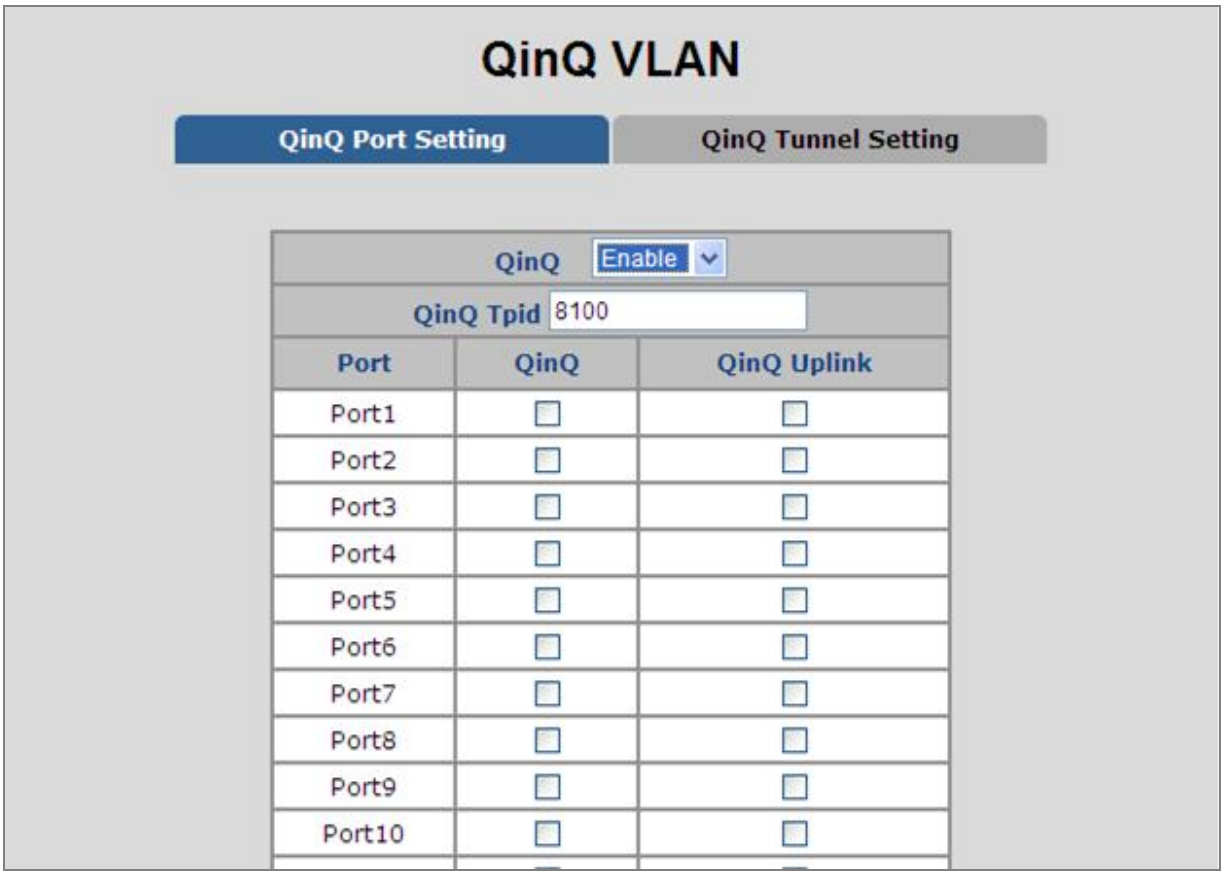


Figure 4-4-5-1: Q-in-Q Port Setting Interface

The page includes the following fields:

Object	Description
Q-in-Q	**Enable:** Sets the Managed Switch to **Q-in-Q** mode, and allows the Q-in-Q tunnel port to be configured. **Disable:** The Managed Switch operates in its normal VLAN mode. The default is for the Managed Switch to function in **Disable** mode.
Q-in-Q TPID	The **Tag Protocol Identifier (TPID)** specifies the ethertype of incoming packets on a tunnel access port. • **802.1Q Tag: 8100** • **vMAN Tag: 88A8** Default: 802.1Q Tag.
Port Q-in-Q	Check: Sets the Port to **Q-in-Q** mode. Or the port operates in its normal VLAN mode. Default: Un-check.

Q-in-Q Uplink	**Check:**	Configures IEEE 802.1Q tunneling (Q-in-Q) for an uplink port to another device within the service provider network.
	Cancel:	Configures IEEE 802.1Q tunneling (Q-in-Q) for a client access port to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.

4.4.5.2 Q-in-Q Tunnel Setting

Business customers of service providers often have specific requirements for VLAN IDs and the number of VLANs to be supported. The VLAN ranges required by different customers in the same service-provider network might overlap, and traffic of customers through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations and could easily exceed the VLAN limit (4096) of the IEEE 802.1Q specification.

Using the Q-in-Q feature, service providers can use a single VLAN to support customers who have multiple VLANs. Customer VLAN IDs are preserved, and traffic from different customers is segregated within the service-provider network, even when they appear to be in the same VLAN. Using Q-in-Q expands VLAN space by using a VLAN-in-VLAN hierarchy and retagging the tagged packets. A port configured to support Q-in-Q is called a Q-in-Q user-port. A port configured to support Q-in-Q Uplink is called a Q-in-Q uplink-port.

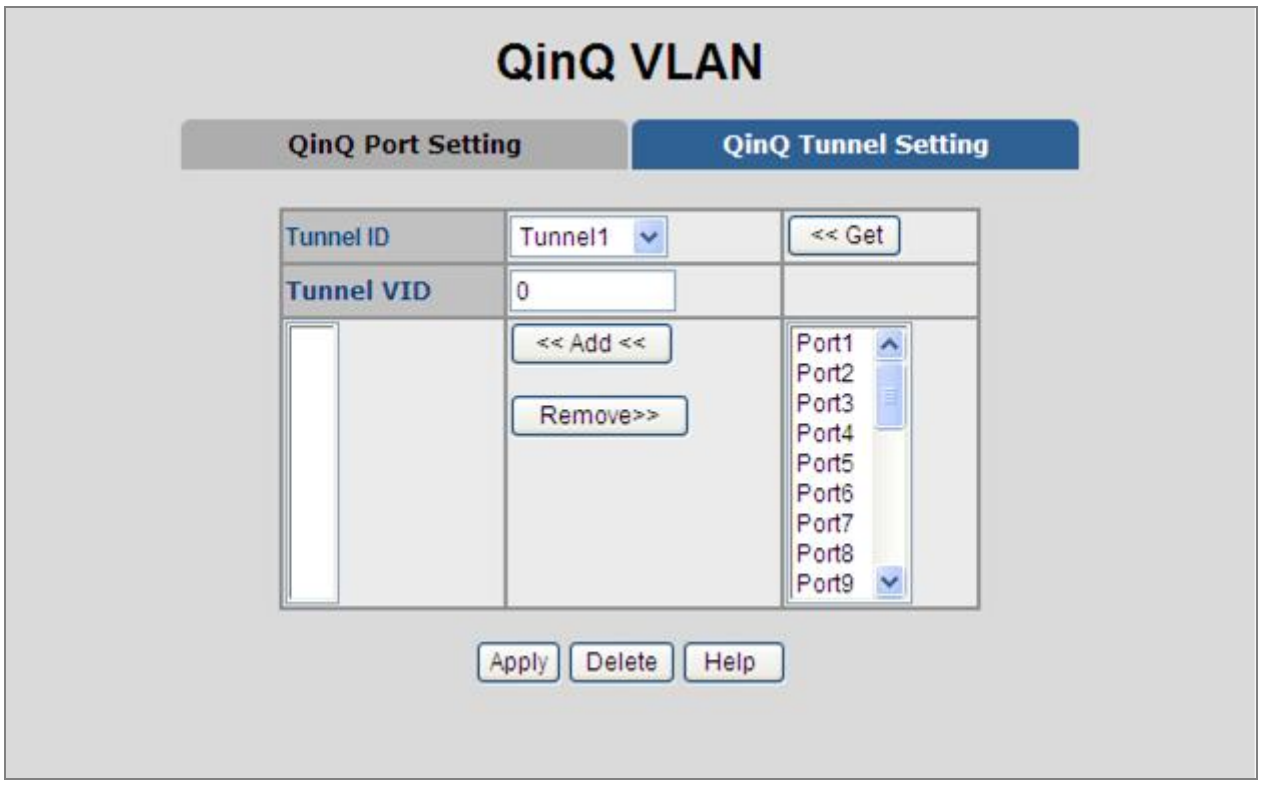


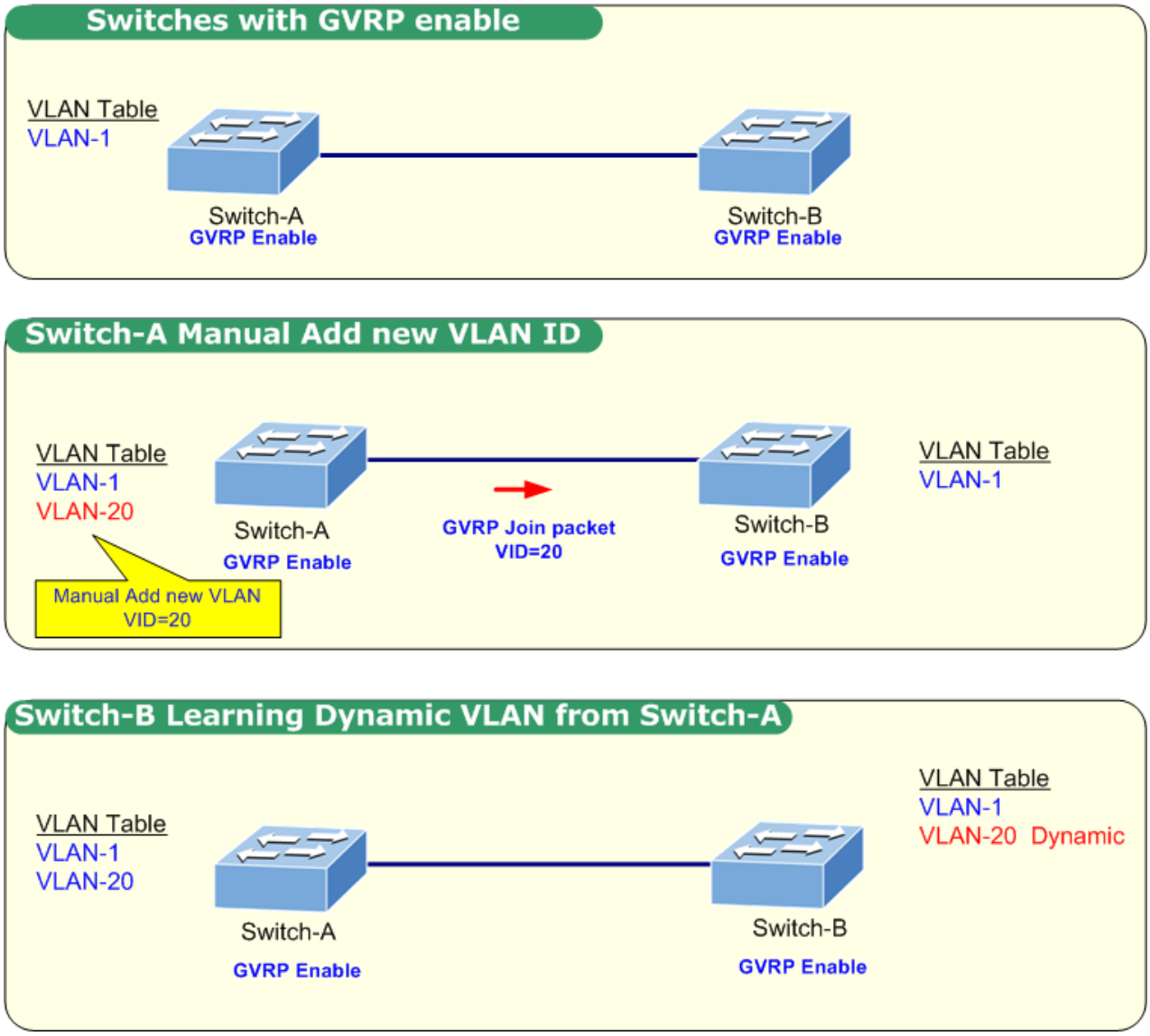
Figure 4-4-5-2: Q-in-Q Tunnel Setting interface

■ **To configure Q-in-Q Port**

1. To enable global Q-in-Q function, select **Q-in-Q** and enable "**Enable**".
2. Fill out Q-in-Q Tpid.
3. To enable port Q-in-Q function, select Q-in-Q checkbox for special port.
4. To enable port Q-in-Q Uplink function, select Q-in-Q Uplink checkbox for special port.

4.4.6 GVRP VLAN

GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration information with other devices.



4.4.6.1 GVRP Setting

To configure GVRP

To enable global GVRP function, select GVRP and "Enable".

To enable port GVRP function, select GVRP checkbox for special port.

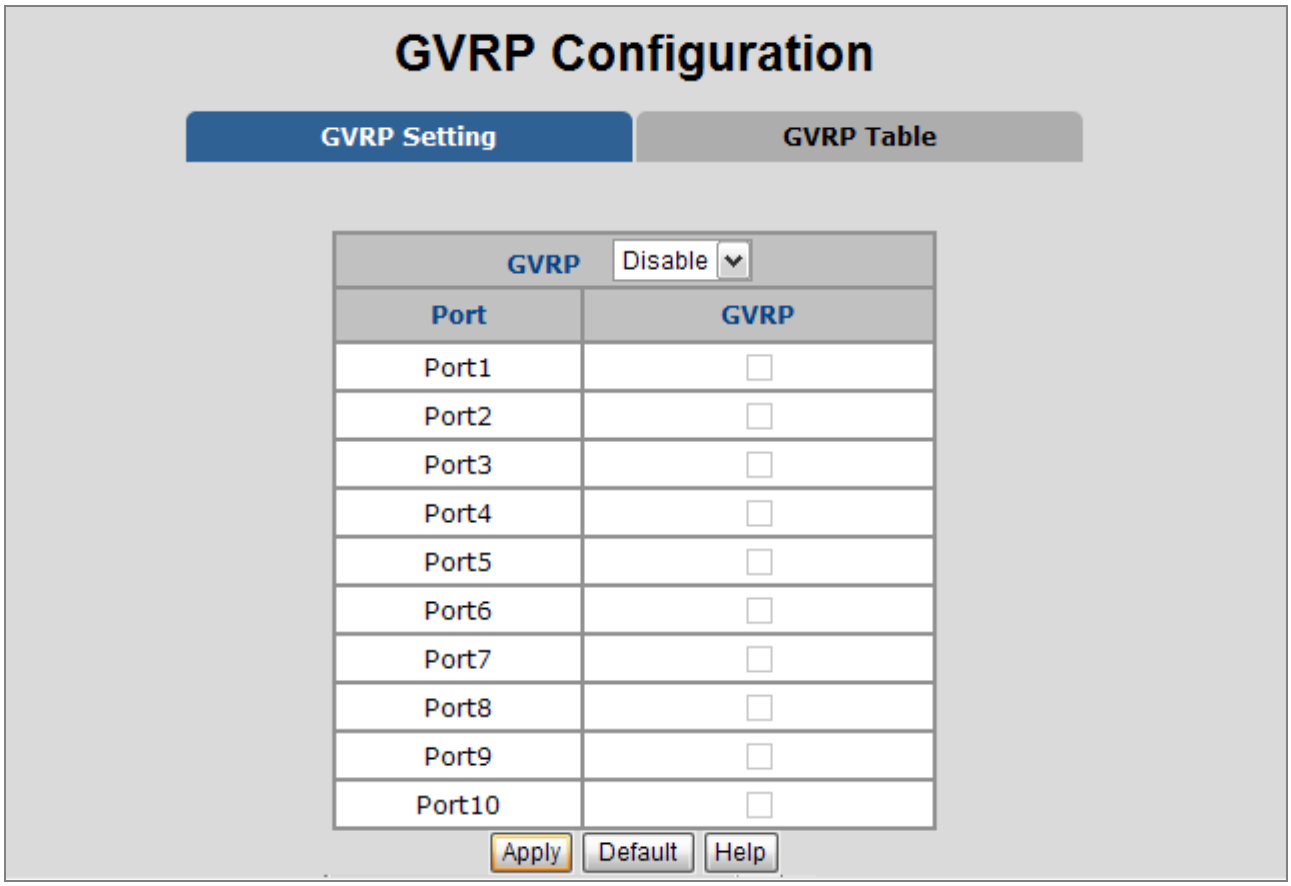


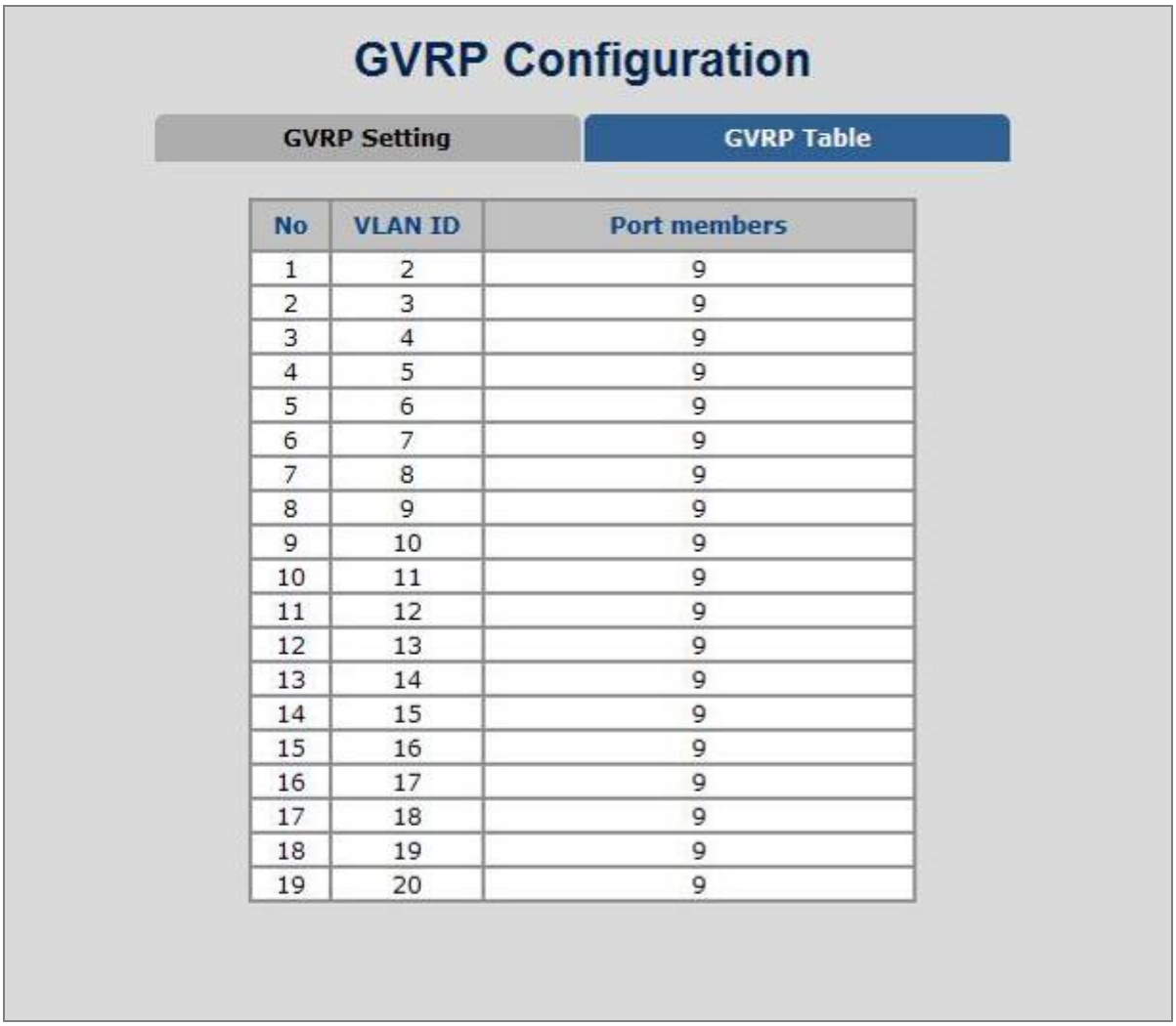
Figure 4-4-6-1: GVRP Configuration Web Interface

The page includes the following fields:

Object	Description
GVRP	Enable global GVRP function
Port	Indicate port 1 to port 10.
Port GVRP	Enable selected port GVRP function

4.4.6.2 GVRP Table

The GVRP Table can be used to display dynamic VLANs from being learned via GVRP.



No	VLAN ID	Port members
1	2	9
2	3	9
3	4	9
4	5	9
5	6	9
6	7	9
7	8	9
8	9	9
9	10	9
10	11	9
11	12	9
12	13	9
13	14	9
14	15	9
15	16	9
16	17	9
17	18	9
18	19	9
19	20	9

Figure 4-4-6-2: GVRP Table Web Interface

The page includes the following fields:

Object	Description
VLAN ID	Display the learned VLANs via GVRP protocol on GVRP enabled ports. The Managed Switch allows displaying up to 128 dynamic VLAN entries.
Port Members	Identify the GVRP enabled port that dynamic VLAN is learned from.

4.5 Trunking

Port Trunking (also called "Link Aggregation") is the combination of several ports or network cables to expand the connection speed beyond the limits of any one single port or network cable. The Managed Switch supports two types of port trunk technology:

- **Static Trunk**
- **LACP**

The **Link Aggregation Control Protocol (LACP)** provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. 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**. For more information, refer to IEEE 802.3ad.

4.5.1 Aggregator Setting

This section provides Port Trunk-Aggregator Setting of each port from the Managed Switch.

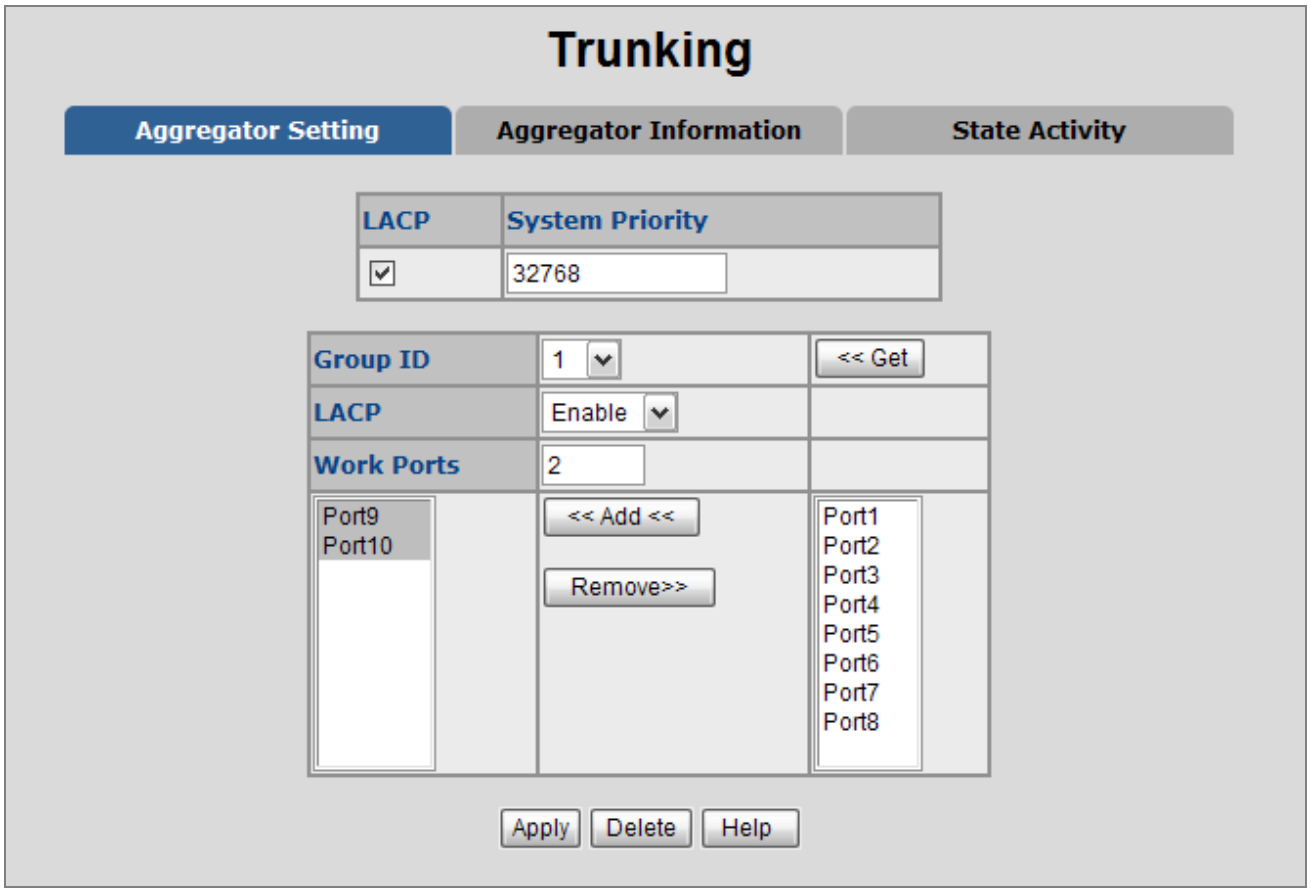


Figure 4-5-1-1: Port Trunk—Aggregator Setting Interface (two ports are added to the left field with LACP enabled)

The page includes the following fields:

Object	Description
System Priority:	A value which is used to identify the active LACP. The Managed Switch with the lowest value has the highest priority and is selected as the active LACP peer of the trunk group.
Group ID:	There are 13 trunk groups to be selected. Assign the "**Group ID**" to the trunk group.
LACP:	■ **Enabled** -- The trunk group uses **LACP**. A port which joins an LACP trunk group has to make an agreement with its member ports first. ■ **Disabled** -- The trunk group is a **static trunk group**. The advantage of having the LACP disabled is that a port joins the trunk group without any handshaking with its member ports, but member ports won't know that they should be aggregated together to form a logic trunk group.
Work Ports:	This column field allows the user to type in the total number of active port up to four. With **LACP static trunk group**, e.g., you assign four ports to be the members of a trunk group whose work ports column field is set as two; the exceeded ports are standby/redundant ports and can be aggregated if working ports fail. If it is a **static trunk group** (non-LACP), the number of work ports must equal the total number of group member ports.

Please note that a trunk group, including member ports split between two switches, **has to enable the LACP function of the two switches.**

4.5.2 Aggregator Information

When you set up the LACP aggregator, you will see the related information here.

■ LACP disabled

Having set up the aggregator setting with LACP disabled, you will see the local static trunk group information on the tab of **Aggregator Information**.

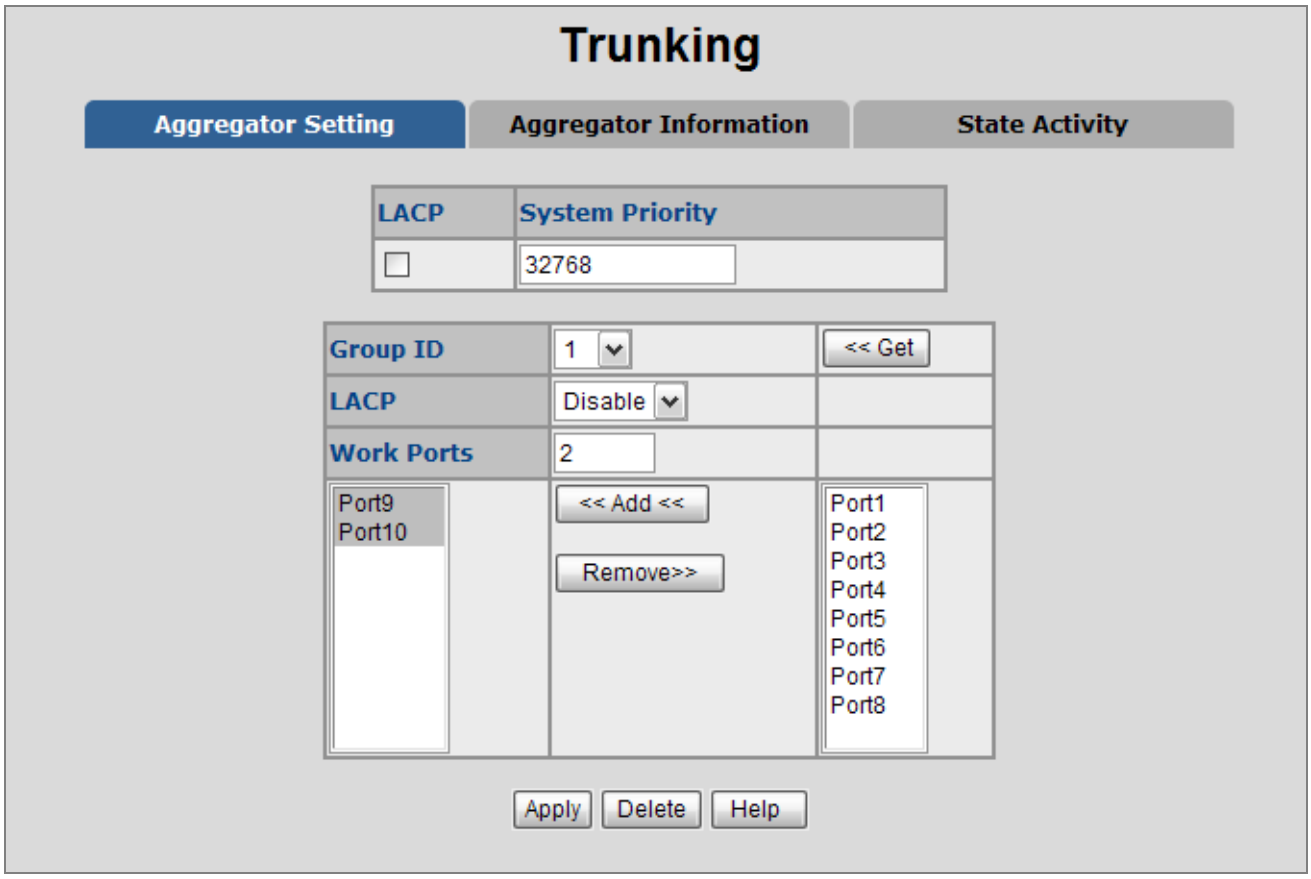


Figure 4-5-2-1: Assigning 2 ports to a Trunk Group with LACP Disabled

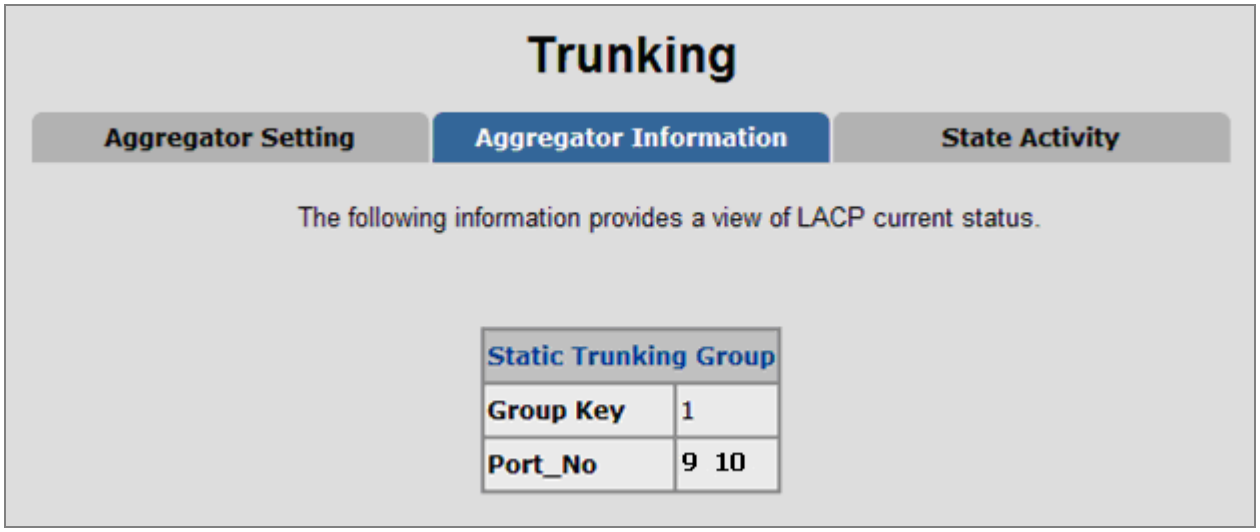


Figure 4-5-2-2: Static Trunking Group Information

The page includes the following fields:

Object	Description
Group Key:	This is a read-only column field that displays the trunk group ID.
Port Member:	This is a read-only column field that displays the members of this static trunk group.

■ LACP enabled

Having set up the aggregator setting with LACP enabled, you will see the trunking group information between two switches on the tab of **Aggregator Information**.

■ Switch 1 configuration

1. Set **System Priority** of the trunk group. The default is **32768**.
2. Select a **trunk group ID** by pulling down the drop-down menu bar.
3. Enable **LACP.**
4. Include the member ports by clicking the **Add** button after selecting the port number and the column field of **Work Ports** changes automatically.

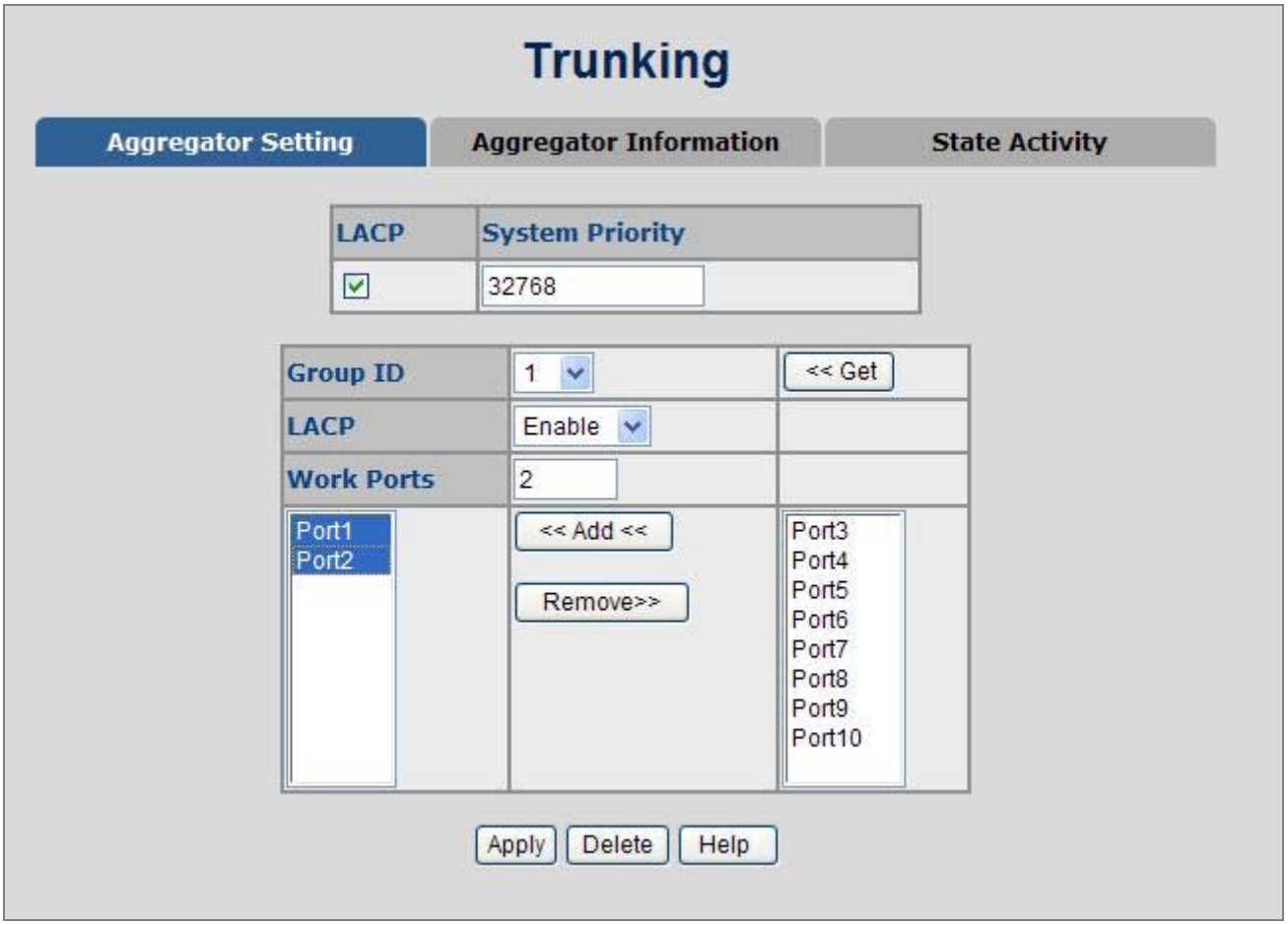


Figure 4-5-2-3: Aggregation Information of **Switch 1**

5. Click on the tab of **Aggregator Information** to check the trunk group information as the illustration is shown above after the two switches configured.

■ Switch 2 configuration

6. Set **System Priority** of the trunk group. For example: 1.
7. Select a **trunk group ID** by pulling down the drop-down menu bar.
8. Enable LACP.
9. Include the member ports by clicking the **Add** button after selecting the port number and the column field of **Work Ports** changes automatically.

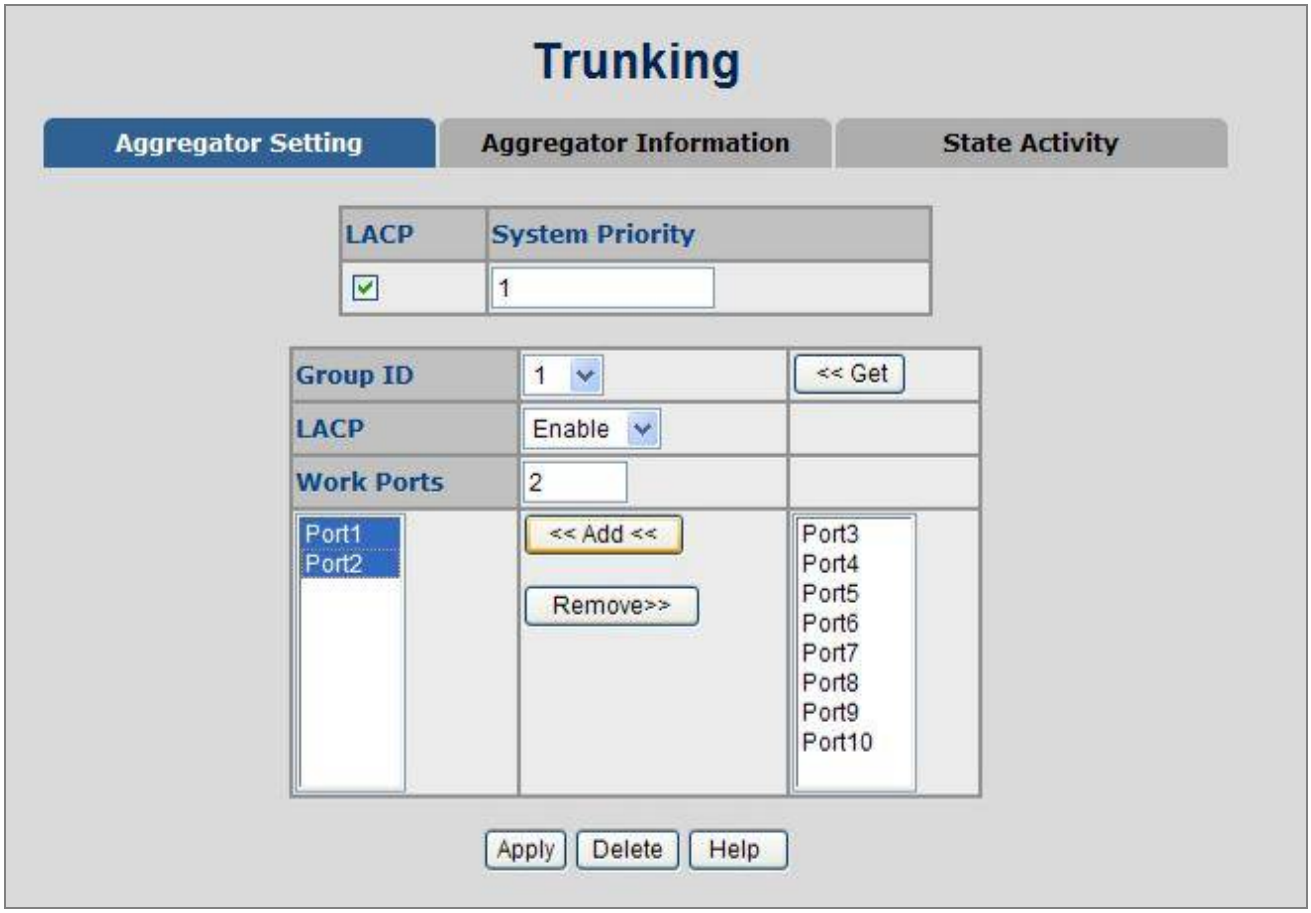


Figure 4-5-2-4: Switch 2 configuration interface

10. Click on the tab of **Aggregator Information** to check the trunk group information as the illustration is shown above after the two switches configured.

Figure 4-5-2-5: Switch 1 Aggregator Information

4.5.3 State Activity

Having set up the LACP aggregator on the tab of Aggregator Setting, you can configure the state activity for the members of the LACP trunk group. You can tick or cancel the checkbox beside the state label. When you remove the tick mark of the port and click Apply, the port state activity will change to **Passive**.

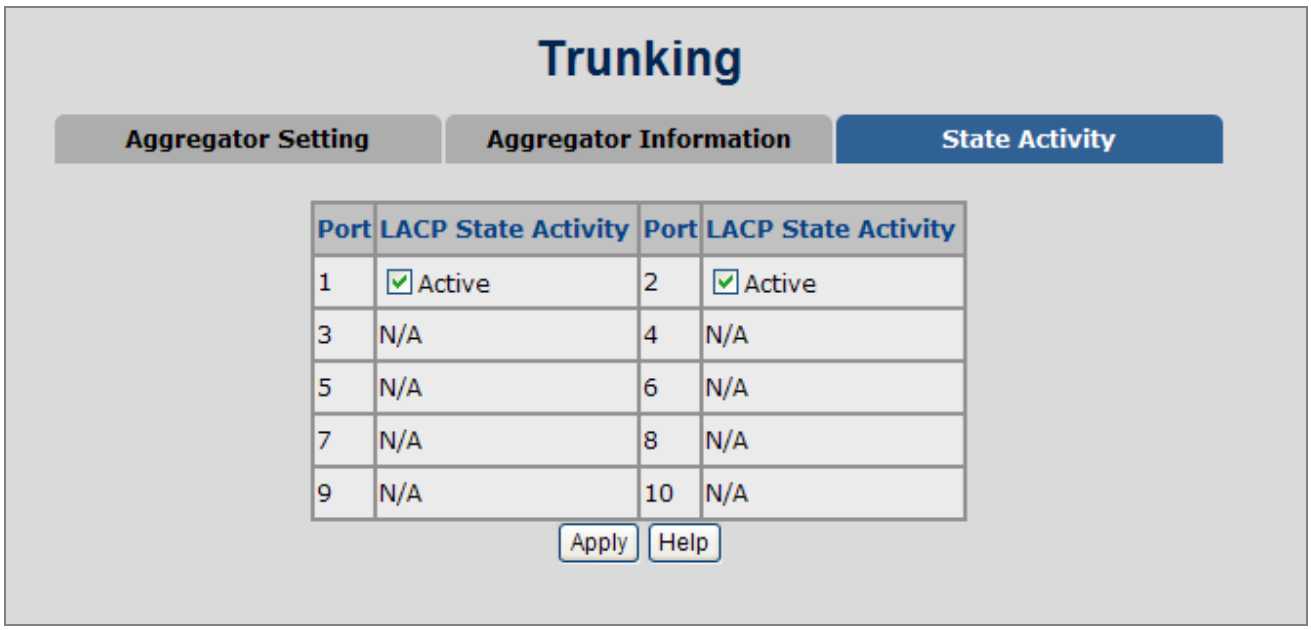


Figure 4-5-3-1: State Activity of **Switch 1**

The page includes the following fields:

Object	Description
Active:	The port automatically sends LACP protocol packets.
Passive:	The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.

Note

A link having two passive LACP nodes will not perform dynamic LACP trunk because both ports are waiting for an LACP protocol packet from the opposite device.

4.6 Forwarding and Filtering

The frames of Ethernet Packets 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 frames with the corresponding SMAC address have been seen after a configurable age time.

4.6.1 Dynamic MAC Table

Entries in the MAC Table are shown on this page. The Dynamic MAC Table contains up to **8192** entries, and is sorted first by VLAN ID, then by MAC address. You can view all of the dynamic MAC addresses learned by the listed port.

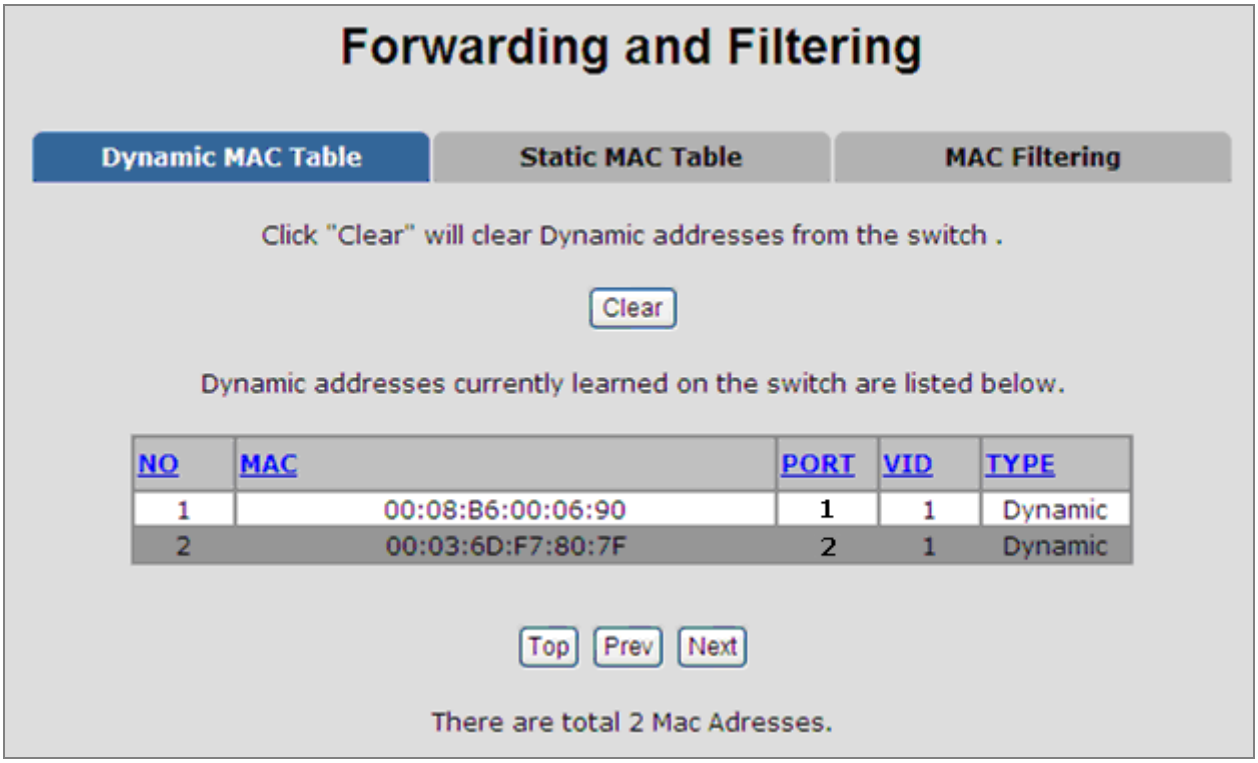


Figure 4-6-1: Dynamic MAC Address interface

MAC Table Columns

Object	Description
• **NO**	The MAC address index entry.
• **MAC**	The MAC address of the entry.
• **PORT**	The ports that are members of the entry.
• **VID**	The VLAN ID of the entry.
• **Type**	Indicates whether the entry is a static or dynamic entry.

Click "**Clear**" to clear the dynamic MAC addresses information of the current port shown on the screen.

4.6.2 Static MAC Table

You can add a static MAC address that remains in the switch's address table regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. Via this interface, you can add / delete a static MAC address.

■ Add the Static MAC Address

You can add static MAC address in the switch MAC table here.

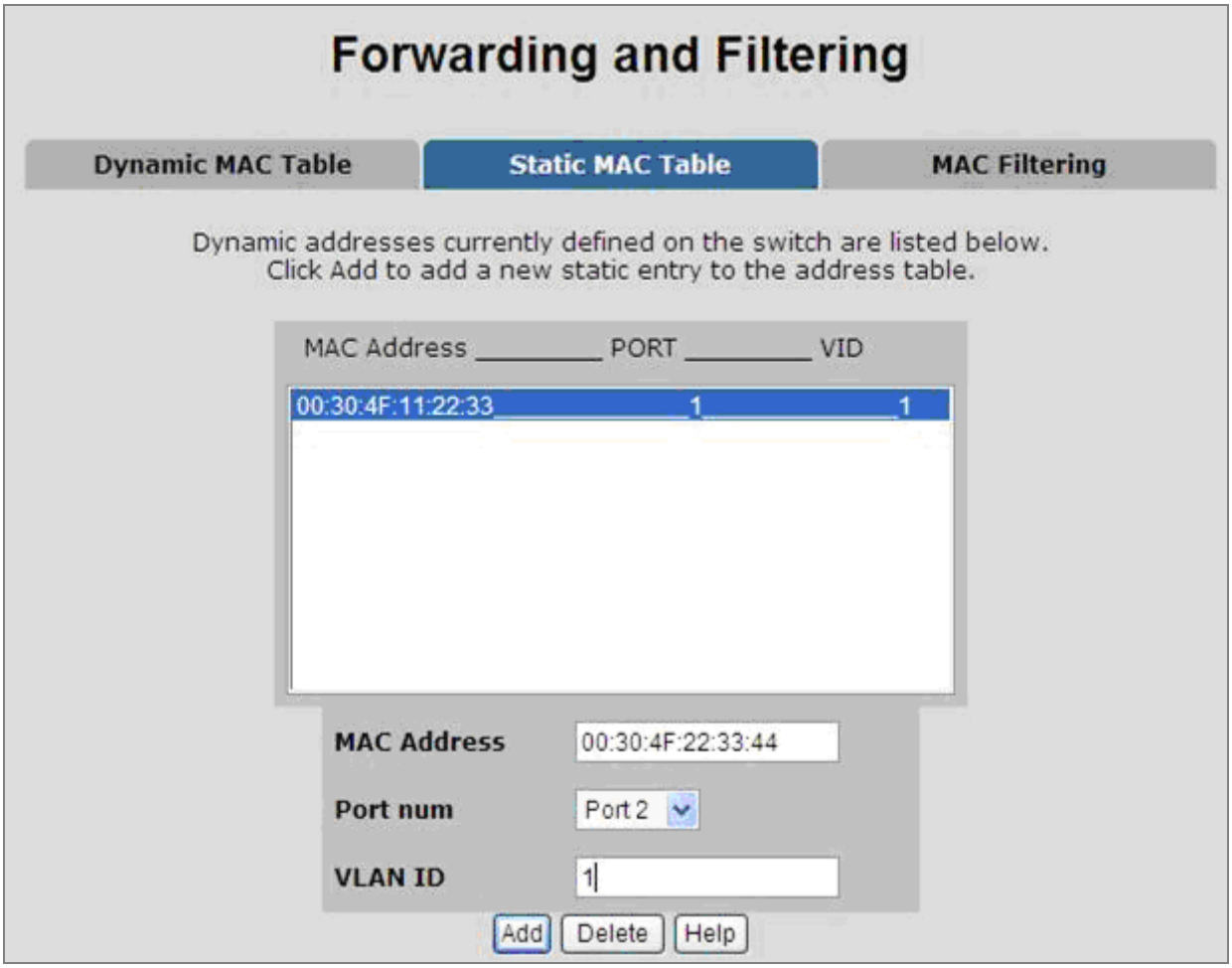


Figure 4-6-2: Static MAC Addresses interface

The page includes the following fields:

Object	Description
MAC Address:	Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.
Port Number:	Pull down the selection menu to select the port number.
VLAN ID:	The VLAN ID for the entry.

4.6.3 MAC Filtering

By filtering MAC address, the switch can easily filter the pre-configured MAC address and reduce the un-safety. You can add and delete filtering MAC address.

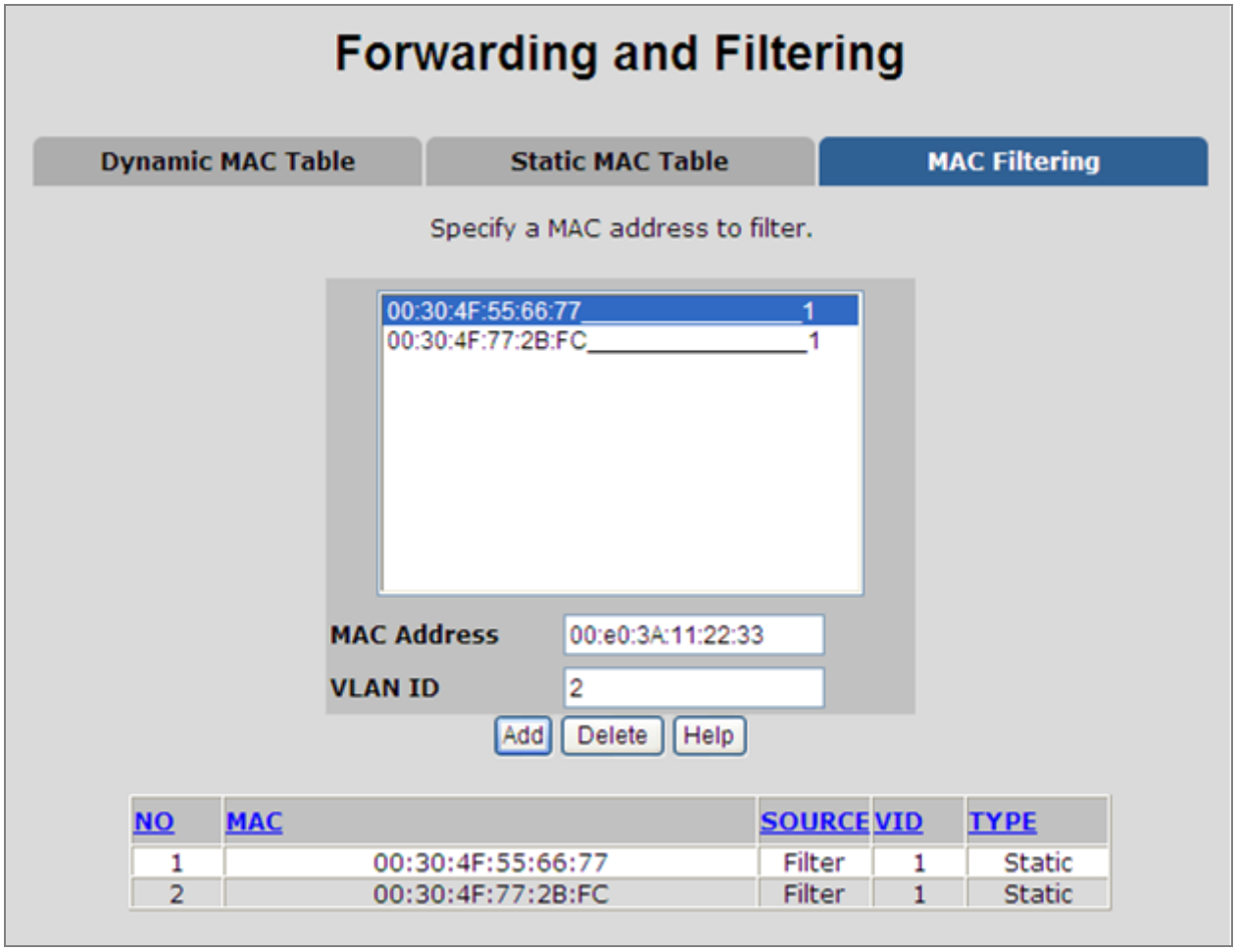


Figure 4-6-3: MAC Filtering interface

The page includes the following fields:

Object	Description
MAC Address:	Enter the MAC address that you want to filter.
VLAN ID:	The VLAN ID for the entry.

4.7 IGMP Snooping

4.7.1 Theory

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

About the Internet Group Management Protocol (IGMP) Snooping

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

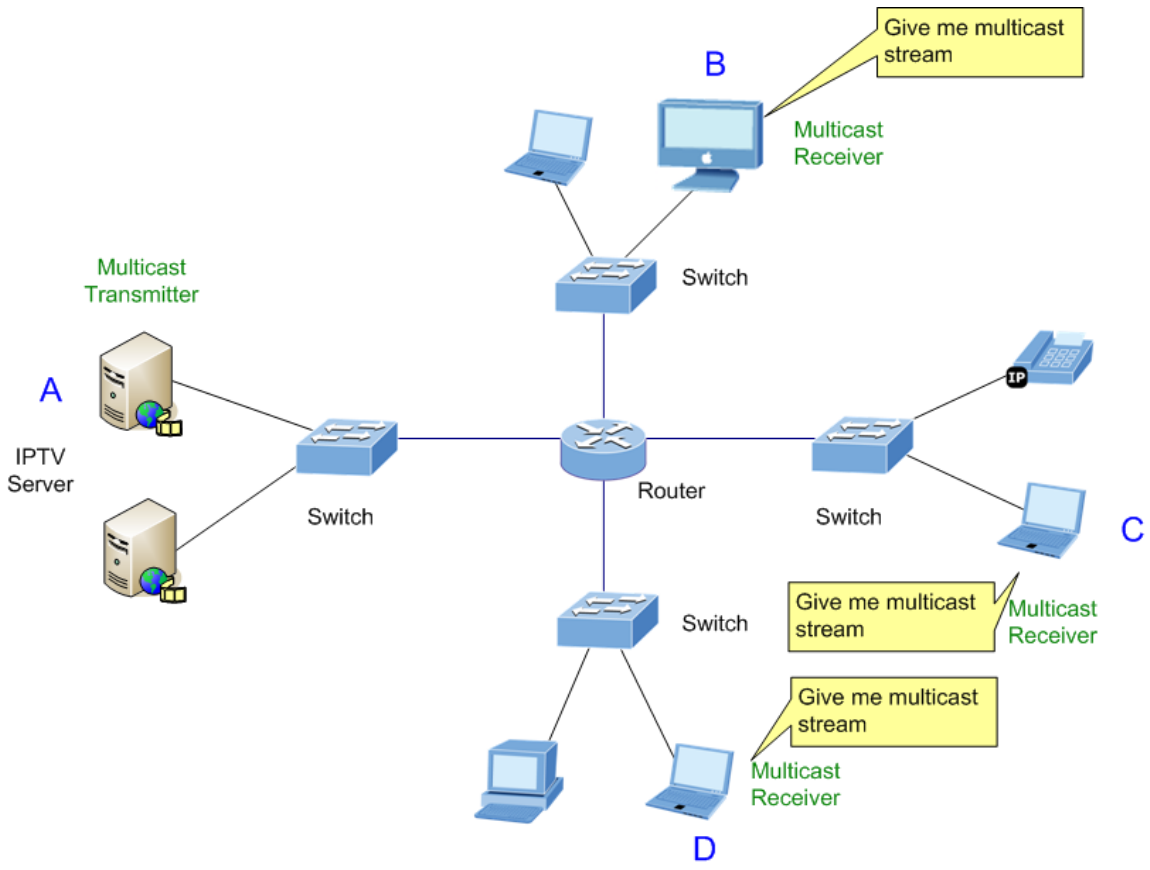


Figure 4-7-1-1: Multicast Service

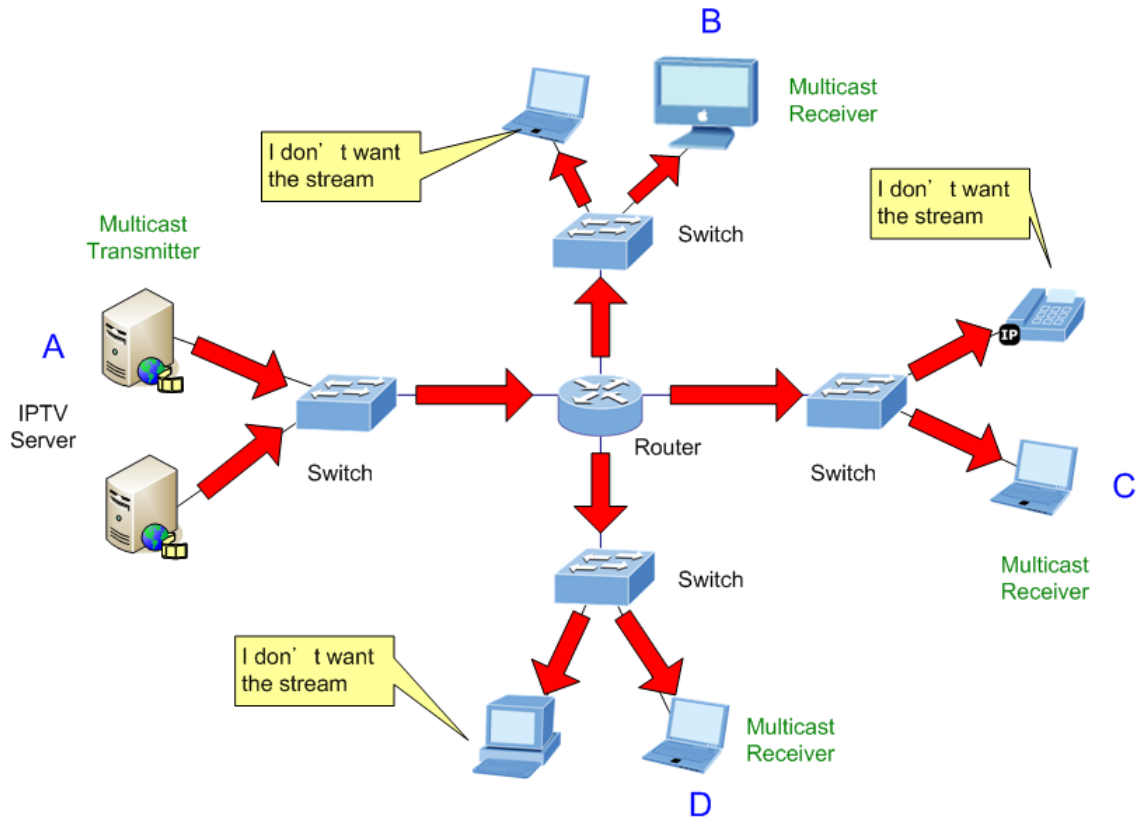


Figure 4-7-1-2: Multicast Flooding

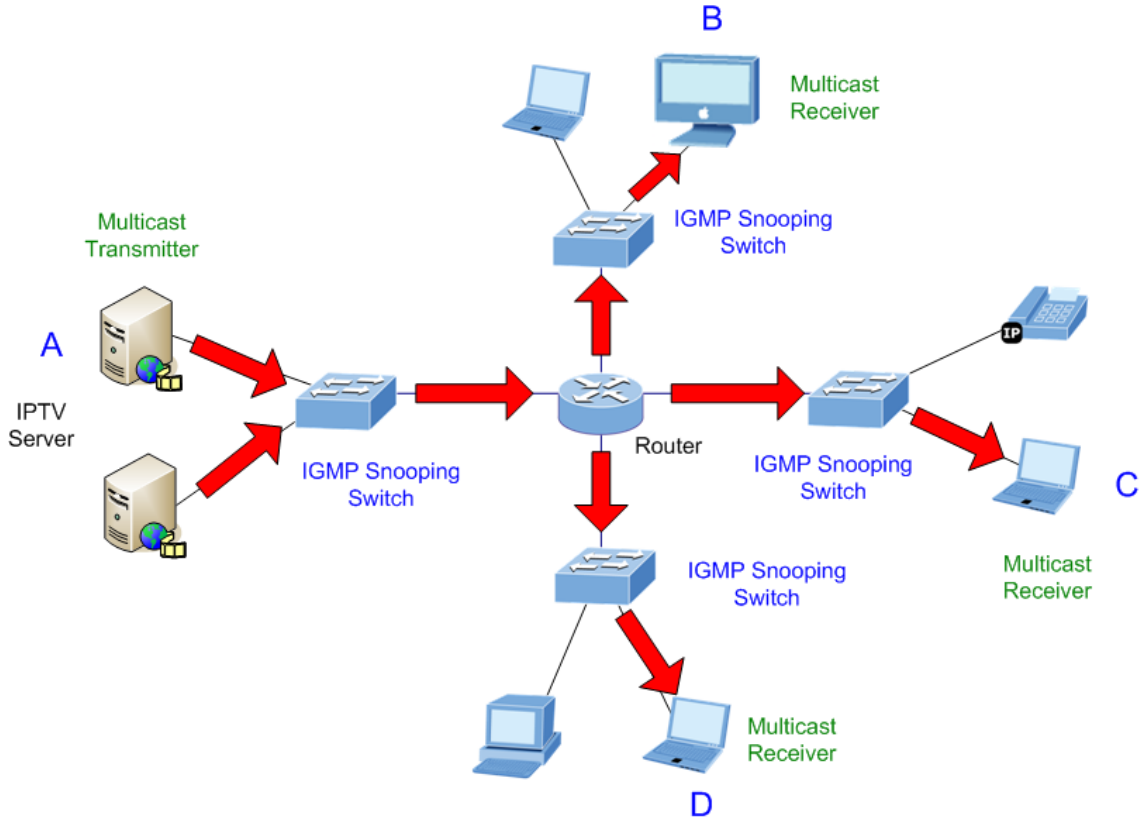


Figure 4-7-1-3: IGMP Snooping Multicast Stream Control

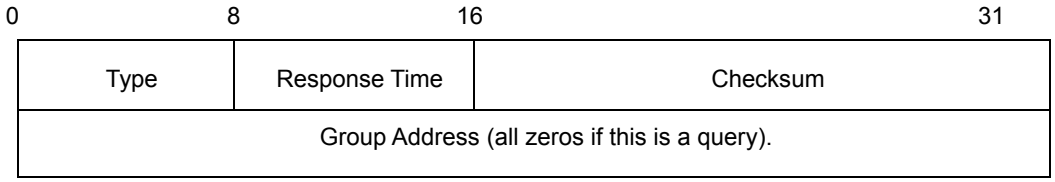
IGMP Versions 1 and 2

Multicast groups allow members to join or leave at any time. IGMP provides the method for members and multicast routers to communicate when joining or leaving a multicast group. IGMP version 1 is defined in RFC 1112. It has a fixed packet size and no optional data.

The format of an IGMP packet is shown below:

IGMP Message Format

Octets



The IGMP Type codes are shown below:

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

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

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

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

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

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

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

IGMP version 2 introduces some enhancements such as a method to elect a multicast queried for each LAN, an explicit

leave message, and query messages that are specific to a given group.

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

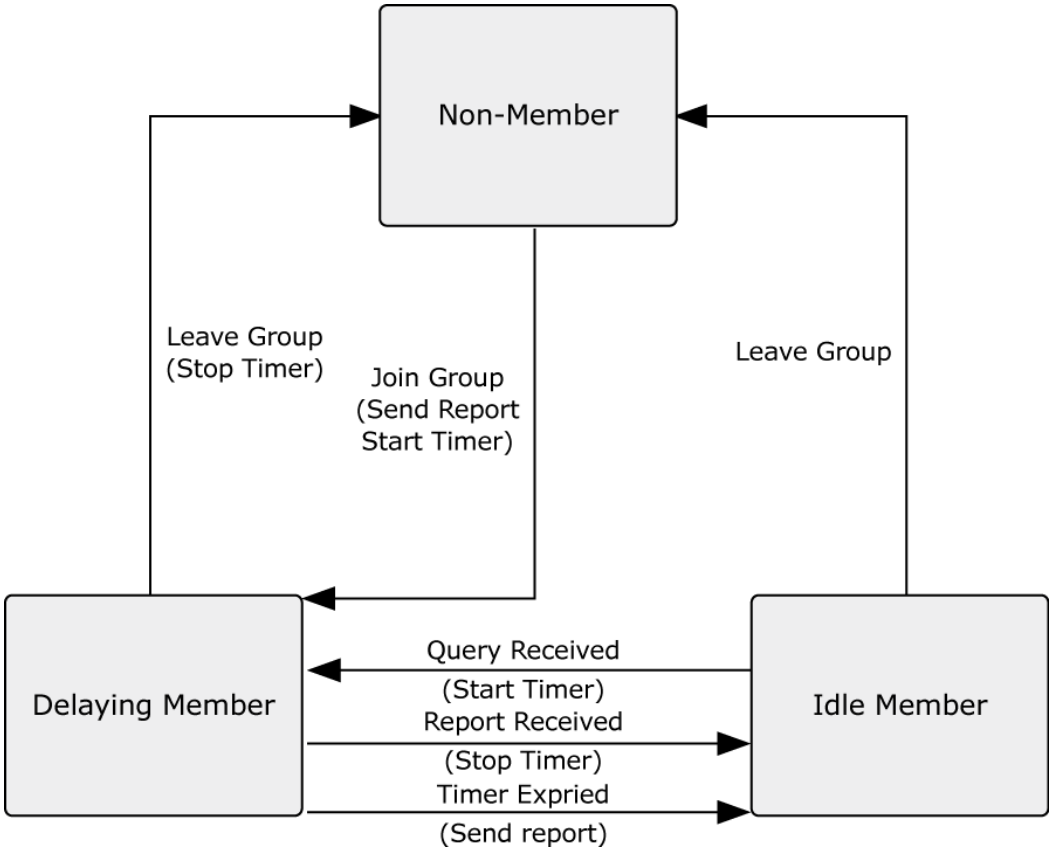


Figure 4-7-1-4: IGMP State Transitions

- **IGMP Querier**

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

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

4.7.2 IGMP Configuration

The Switch supports IP multicast and you can enable IGMP protocol on web management's switch setting advanced page. Then the IGMP snooping information will display. IP multicast addresses range from **224.0.0.0** through **239.255.255.255**.

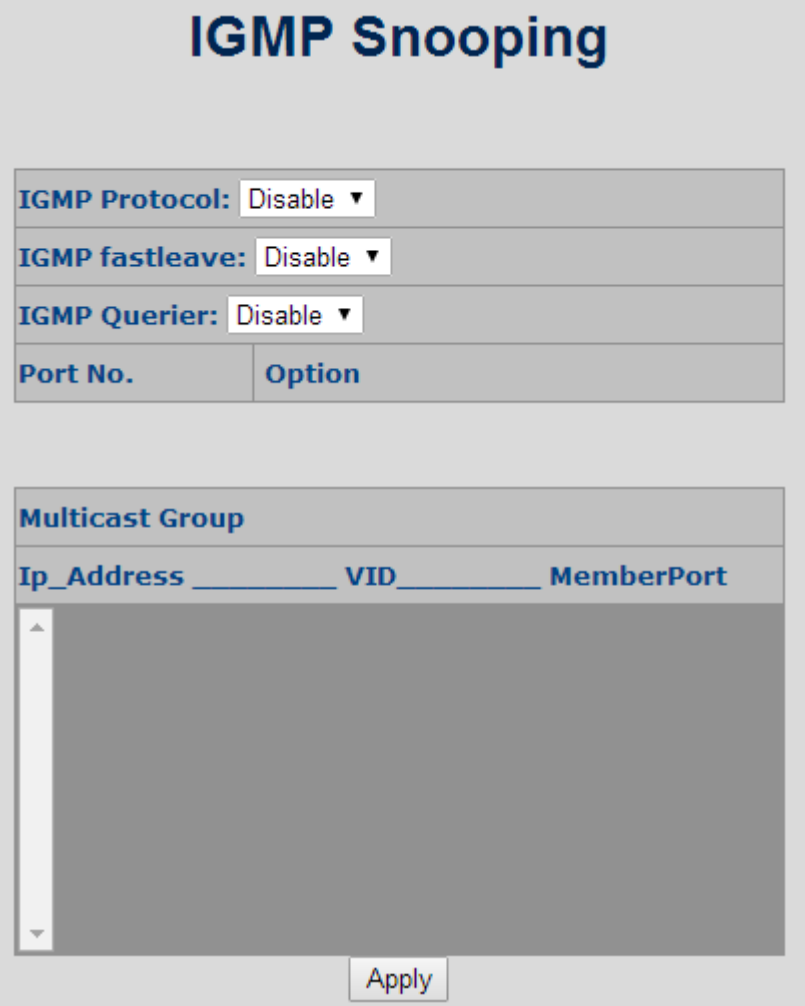


Figure 4-7-2-1: IGMP Configuration Interface Screenshot

The page includes the following fields:

Object	Description
IGMP Protocol:	Enable or disable the IGMP protocol.
IGMP Fast leave:	Enable or disable Fast Leave on the port.
IGMP Querier:	Enable or disable the IGMP query function. The IGMP query information will be displayed in IGMP status section.

Fast Leave:

The Managed Switch can be configured to immediately delete a member port of a multicast service if a leave packet is received at that port and the fast leave function is enabled for the parent VLAN. This allows the Managed Switch to remove a port from the multicast forwarding table without first having to send an IGMP group-specific query to that interface.

4.8 Spanning Tree Protocol

4.8.1 Theory

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

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

STP - The Spanning Tree Protocol (STP) is a standardized method (**IEEE 802.1D**) for avoiding loops in switching networks. Enable STP to ensure that only one path at a time is active between any two nodes on the network.

MSTP - The Multiple Spanning Tree Protocol (MSTP) is a standardized method (**IEEE 802.1S**) for providing 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 , or RSTP. 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)**.

The **IEEE 802.1D Spanning Tree** Protocol and **IEEE 802.1s Multiple Spanning Tree** Protocol allow for the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol allows for the duplicate links to be used in the event of a failure of the primary link. Once the Spanning Tree Protocol is configured and enabled, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically without operator intervention.

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

The Switch STP performs the following functions:

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

Bridge Protocol Data Units

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

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

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

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

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

The communication between switches via BPDUs results in the following:

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

Creating a Stable STP Topology

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

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

STP Port States

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

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

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

A port transitions from one state to another as follows:

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

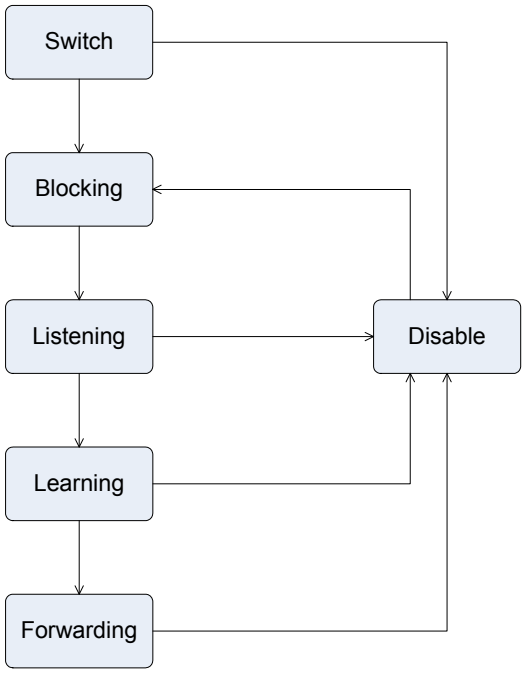


Figure 4-8-1: STP Port State Transitions

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

4.8.2 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.

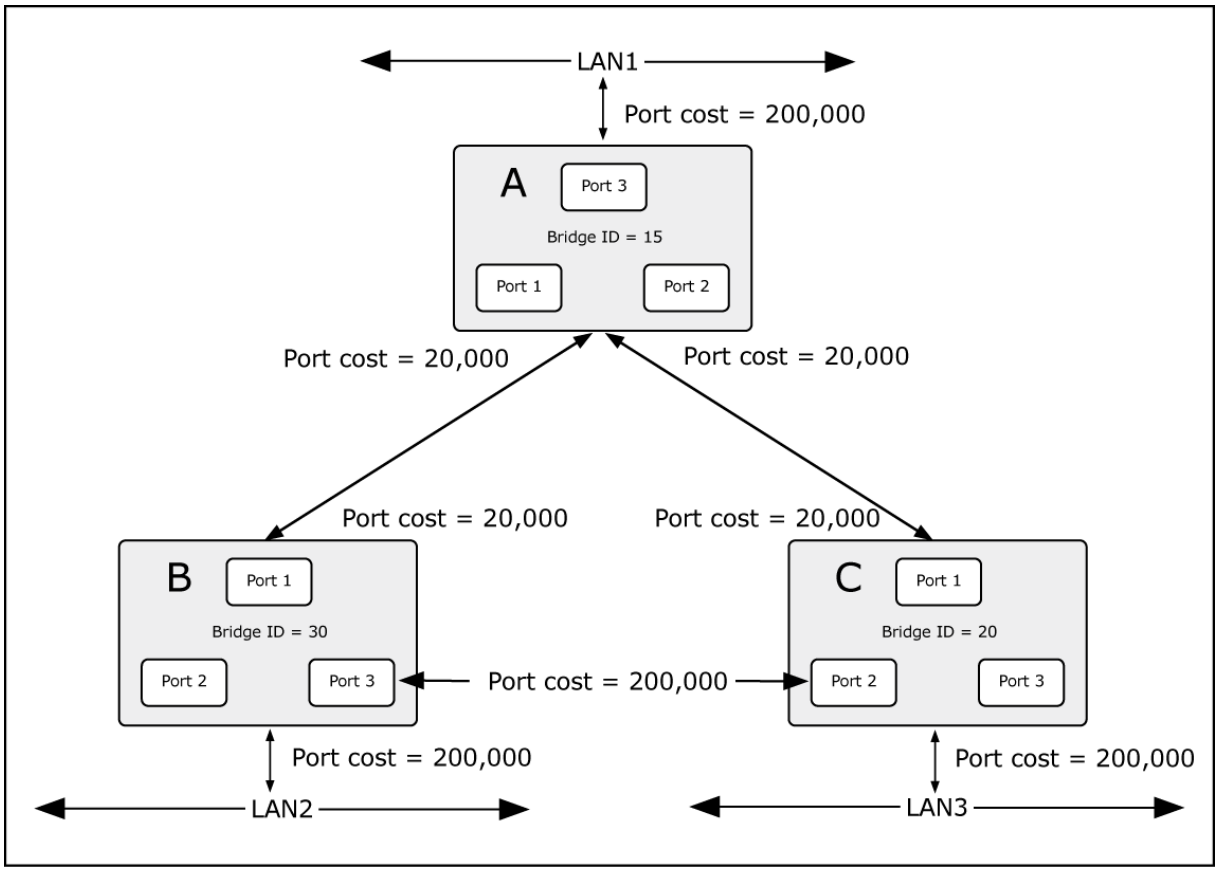


Figure 4-8-2: Before Applying the STA Rules

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.

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

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

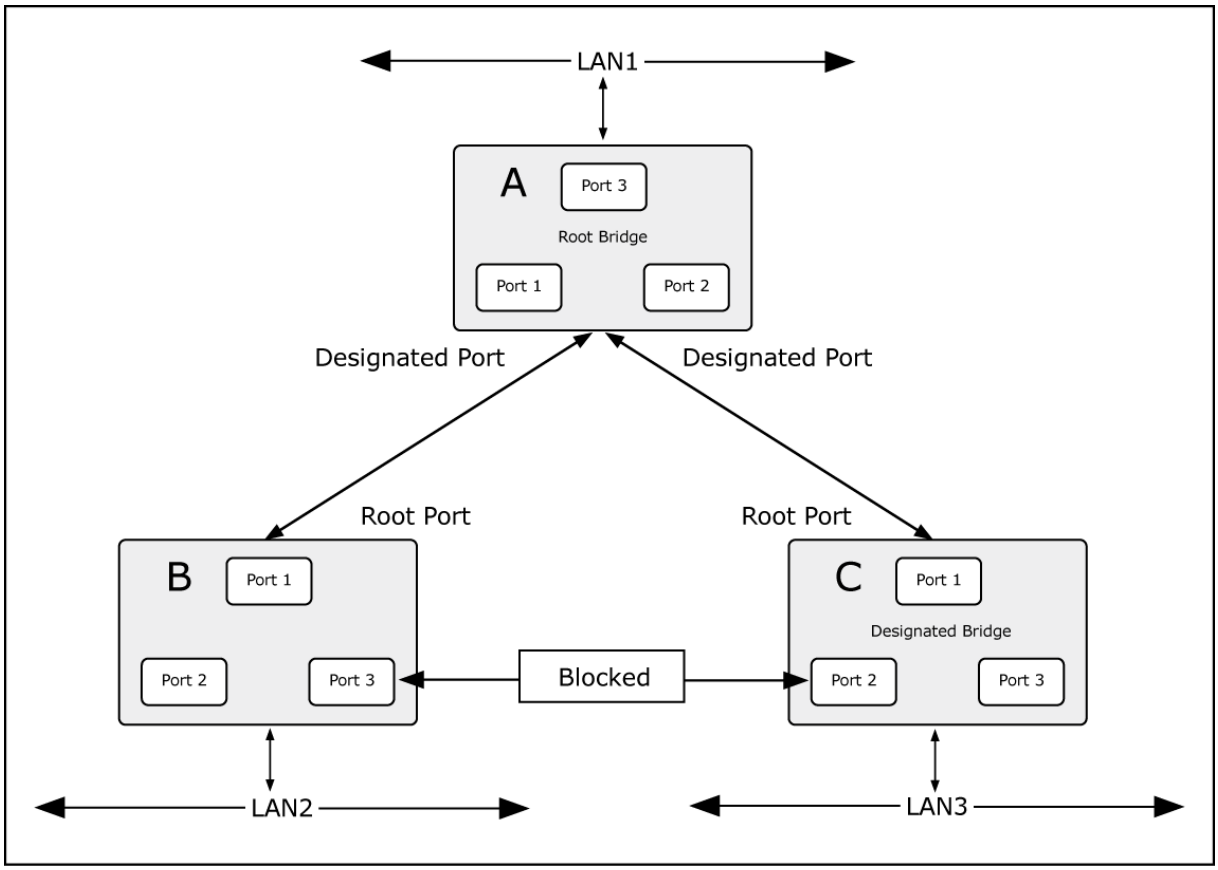


Figure 4-8-3: After Applying the STA Rules

4.8.3 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.

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

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

Note

Observe the following formulas when setting the above parameters:

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

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

4.8.4 STP System Configuration

This section provides STP-System Configuration from the Managed Switch as the screen in Figure 4-7-4 appears.

- The user can view spanning tree information of Root Bridge.
- The user can modify STP state. After modification, click Apply.

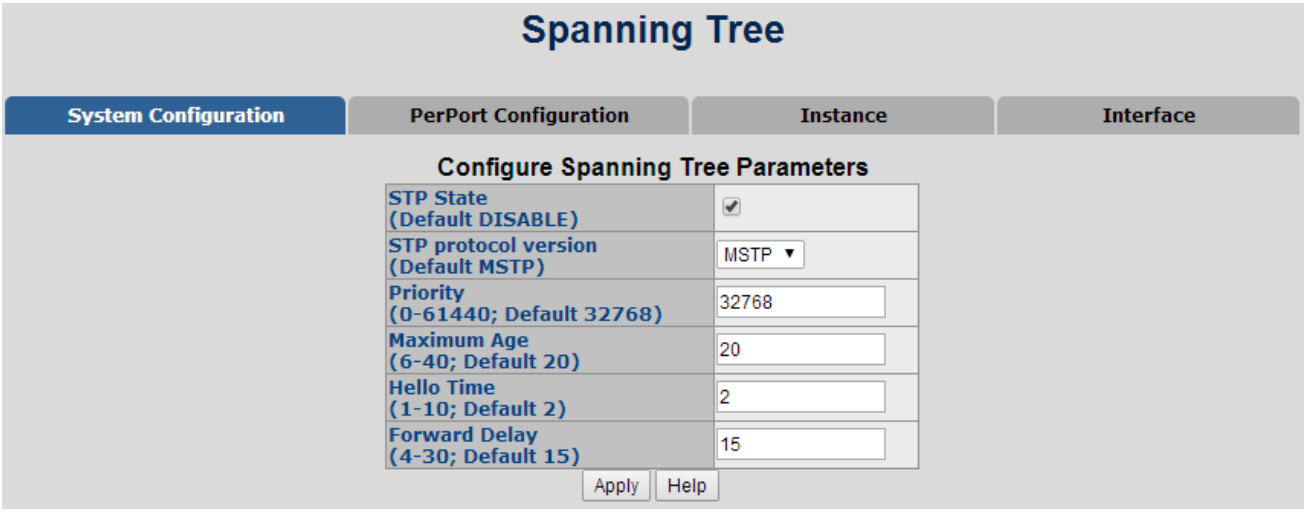


Figure 4-8-4: STP System Configuration Interface

The page includes the following fields:

Object	Description
STP State:	The user must enable the STP function first before configuring the related parameters.
Protocol Version	A value used to specify the spanning tree protocol, the original spanning tree protocol (**STP, 802.1d**) or the multiple spanning tree protocol (**MSTP, 802.1s**).
Priority (0-61440):	The switch with the lowest value has the highest priority and is selected as the root. If the value is changed, the user must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule.
Max Age (6-40):	The number of seconds a switch waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 and 40.
Hello Time (1-10):	The time that controls the switch to send out the BPDU packet to check STP current status. Enter a value between 1 and 10.

Forward Delay Time (4-30):	The number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 and 30.

Note

Follow the rule shown below to configure the Max Age, Hello Time, and Forward Delay Time.

2 x (Forward Delay Time value –1) > = Max Age value >= 2 x (Hello Time value +1).

Note

Each switch in a spanning-tree adopts the Hello Time, Forward Delay time, and Max Age parameters of the root bridge, regardless of how it is configured.

■ Root Bridge Information

This page provides a status overview for all STP bridge instances.

The displayed table contains a row for each STP bridge instance, where the column displays the following information:

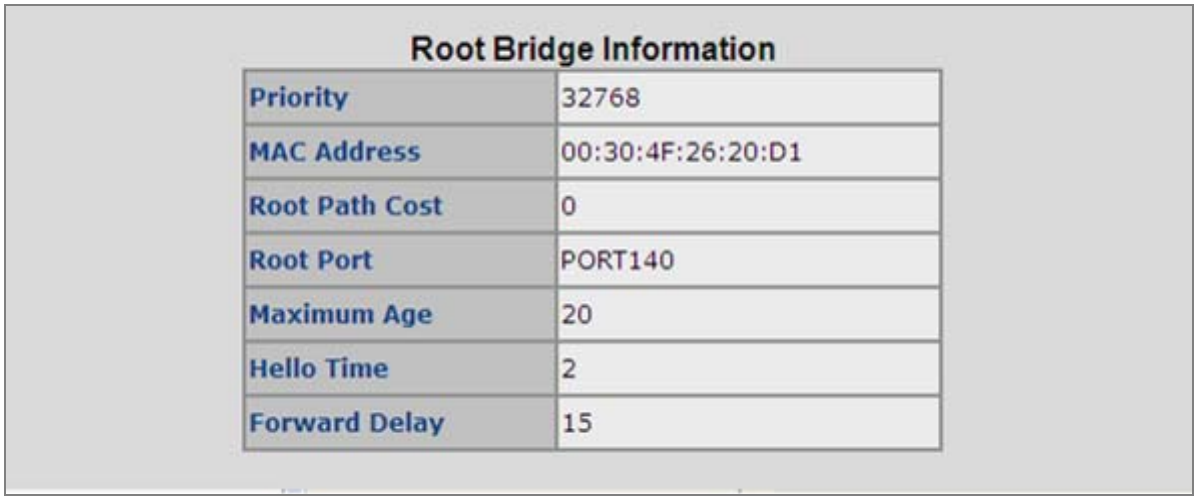


Figure 4-8-5: STP Bridge Status Screenshot

The page includes the following fields:

Object	Description
Priority	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
MAC Address	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
Root Path Cost	For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
Root Port	The switch port currently assigned the *root* port role.
Maximum Age	Path Cost to the Designated Root for the Root Bridge.
Hello Time	Minimum time between transmissions of Configuration BPDUs.
Forward Delay	Derived value of the Root Port Bridge Forward Delay parameter.

4.8.5 Port Configuration

This web page provides the port configuration interface for STP. You can assign higher or lower priority to each port. Spanning tree protocol will have the port with the higher priority in forwarding state and block other ports to make certain that there is no loop in the LAN.

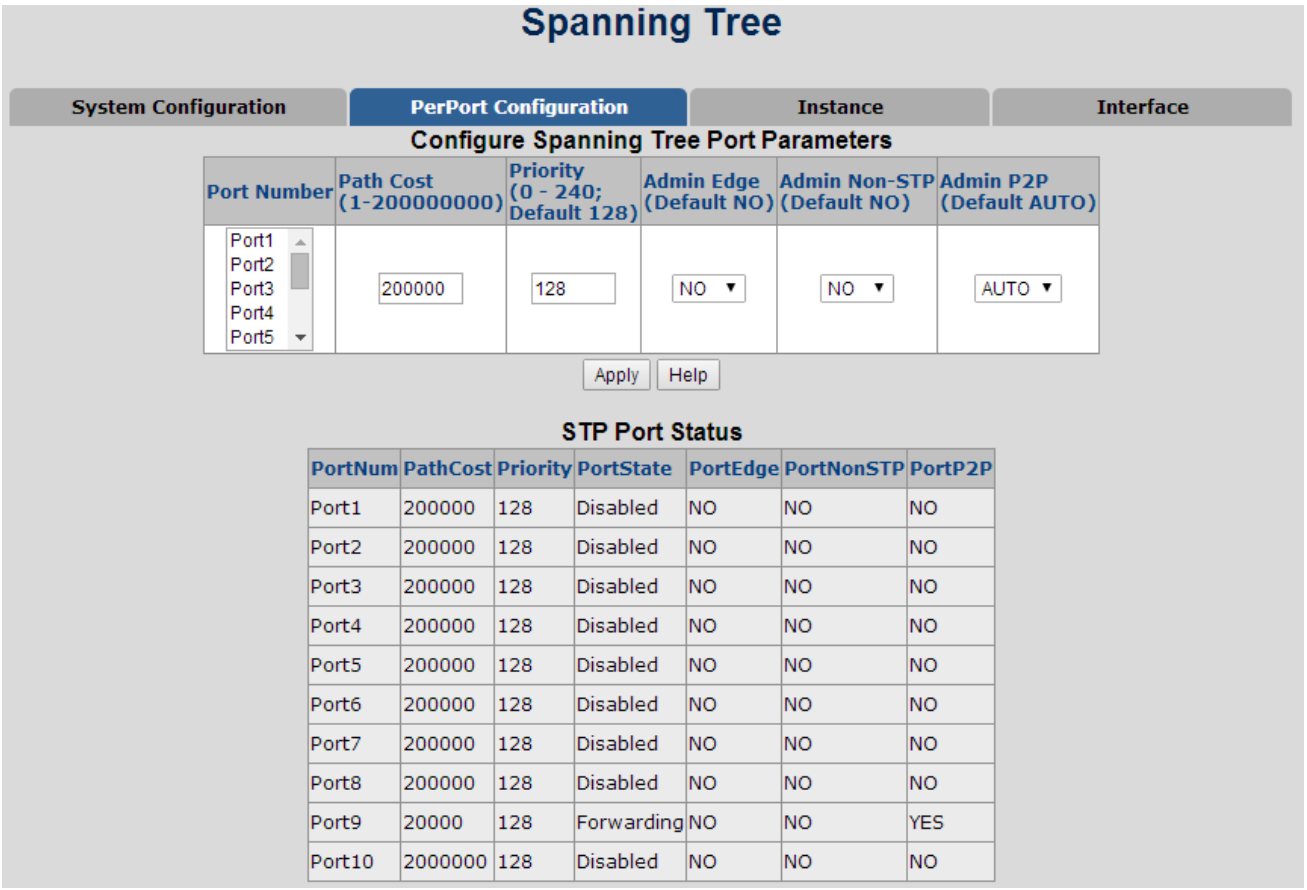


Figure 4-8-6: STP Port Configuration interface

The page includes the following fields:

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

Admin P2P:	The rapid state transitions possible within STP are dependent upon whether the port concerned can only be connected to exactly another bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. • **YES** means the port is regarded as a point-to-point link. • **NO** means the port is regarded as a shared link. • **AUTO** means the link type is determined by the auto-negotiation between the two peers.
Admin Edge:	The port directly connected to end stations won't create bridging loop in the network. To configure the port as an edge port, set the port to "**YES**" status.
Admin Non STP:	The port includes the STP mathematic calculation. • **YES** is not including STP mathematic calculation. • **NO** is including the STP mathematic calculation.

Path cost "**0**" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below.

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

Table 4-8-1: Recommended STP Path Cost Range

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

Table 4-8-2: Recommended STP Path Costs

4.8.6 Instance

This page allows the user to configure MST Instance Configuration.

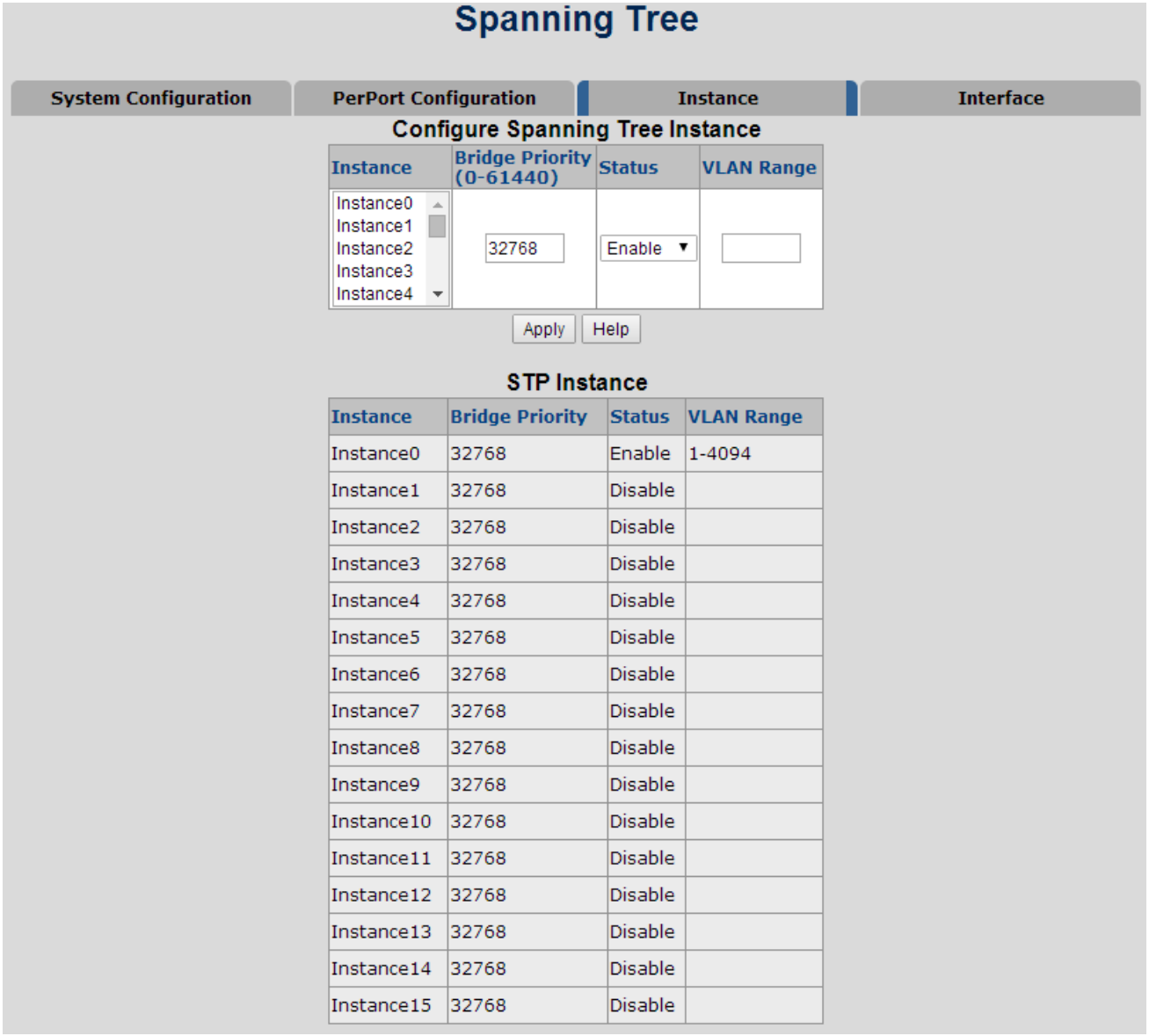


Figure 4-8-6: STP Port Configuration Interface

The page includes the following fields:

Object	Description
Instance:	Allow to assign MSTI ID. The range for the MSTI ID is 1-15.
Bridge Priority (0-61440):	Controls the bridge priority. Lower numerical values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.
Status:	Allow to enable or disable MSTI ID

VLAN Range:	Allow to assign VLANs list to special MSTI ID. The range for the VLAN list is 1-4094.

4.8.7 Interface

This page allows the user to configure MSTP Port Priority and Path Cost Configuration.

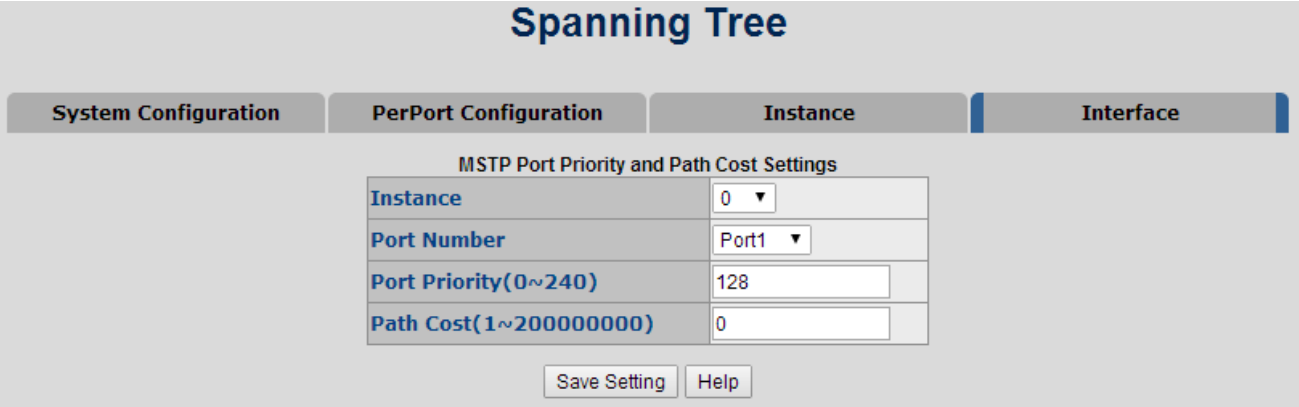


Figure 4-8-7: STP Port Configuration interface

The page includes the following fields:

Object	Description
Instance:	Select MSTI ID. The range for the MSTI ID is 1-15.
Port Number:	Select MSTI ID. The range for the Port Number is Port 1-Port 10.
Port Priority(0~240):	Controls the port priority. This can be used to control priority of ports having identical port cost. Valid values are in the range 0 to 240.
Path Cost(1~200000000):	Controls the path cost incurred by the port. The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.

4.9 DHCP Relay & Option 82

The Relay Agent Information option (**Option82**) is inserted by the **DHCP relay** agent when forwarding client-originated DHCP packets to a DHCP server (RFC 3046). Servers recognizing the Relay Agent Information option may use the information to implement IP address or other parameter assignment policies.

The DHCP Relay can forward the DHCP broadcast packets to a DHCP server in a different subnet (RFC 1542). So DHCP server can provide IP addresses to clients spanning multiple subnets instead of deploying a DHCP server on every subnet.

Configuring DHCP Relay & Option82

To configure DHCP Option82

1. Enable global option82 function: select DHCP Option82 enable "Enable".
2. Enable port option82 function: select Option82 checkbox for special port.
3. Select DHCP Router Port.
4. Click Apply.

To configure DHCP Relay

5. Enable global Relay function: select DHCP Relay enable "Enable".
6. Enable port Relay function: Type the IP addresses of the DHCP "Relay IP".
7. DHCP Server offers an IP address to client from its list of scopes, which subnet is same as the Relay IP.
8. Select DHCP Router Port.
9. Click Apply.

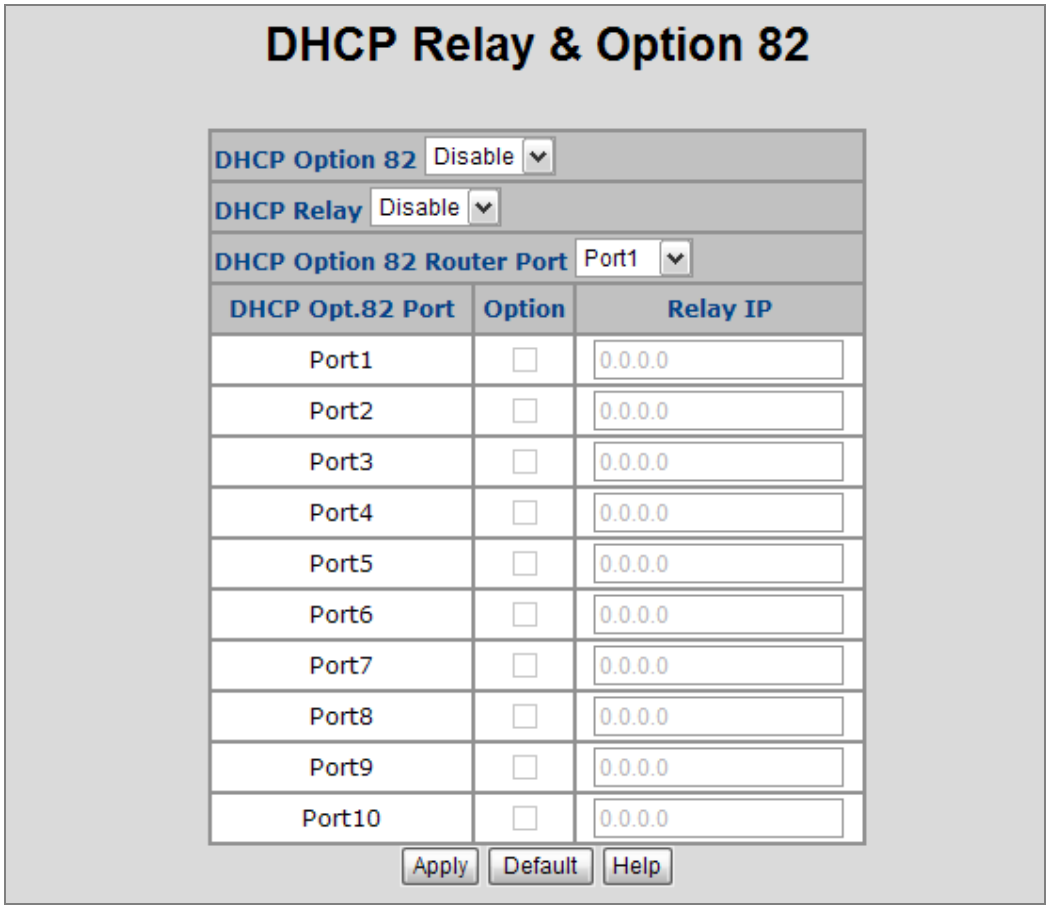


Figure 4-9-1: DHCP Relay & Option 82

The page includes the following fields:

Object	Description
DHCP Option 82	Enable global option82 function
DHCP Relay	Enable global Relay function
DHCP Option 82 Router Port	Select the Router Port that is used to connect to the DHCP server in the domain
DCHP Opt.82 Port	Identify Port-1 to Port-10 to configure DHCP option 82
Option	Enable port option82 function on selected port.
Relay IP	Type the IP addresses of the DHCP "Relay IP".

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.

4.10.1 LLDP Configuration

Use this page to change LLDP parameters.

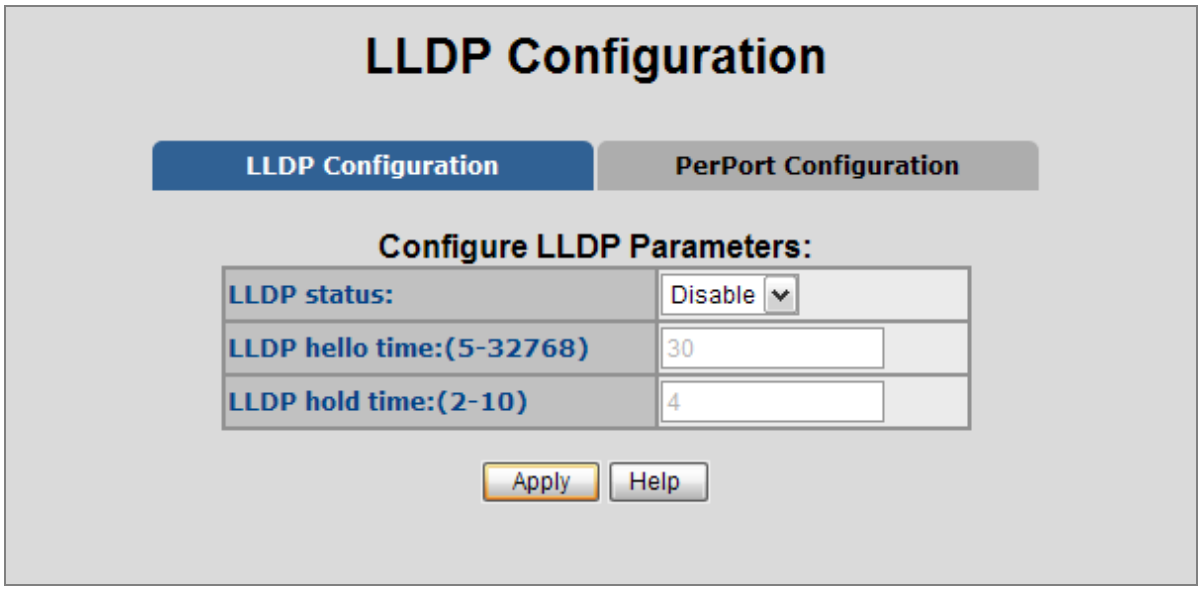


Figure 4-10-1: LLDP Configuration

The page includes the following fields:

Object	Description
LLDP Status	Enable/Disable LLDP.
LLDP Hello Time	You can change LLDP hello time value. The time interval between the transmission LLDP info packets. Value range is from 5 to 32768. Default value is 30.
LLDP Hold Time	You can change LLDP hold time value. (The hold time * the hello time) is the TTL time in the LLDP info packets. Value range is from 2 to 10. Default value is 4.

4.10.2 PerPort Configuration

This page allows the user to inspect and configure the current LLDP port settings.

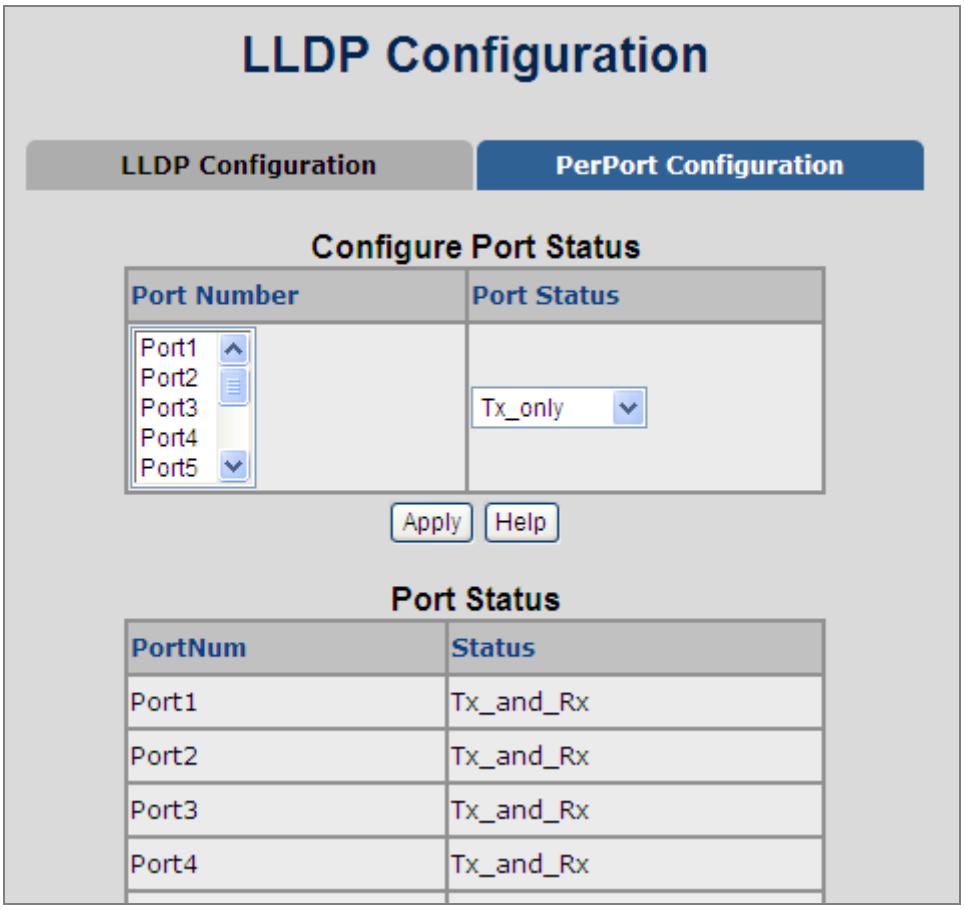


Figure 4-10-2: LLDP per Port Configuration

The page includes the following fields:

Object	Description
LLDP Status	Enable/Disable LLDP.
LLDP Hello Time	You can change LLDP hello time value. The time interval between the transmission LLDP info packets. Value range is from 5 to 32768. Default value is 30.
LLDP Hold Time	You can change LLDP hold time value. (The hold time * the hello time) is the TTL time in the LLDP info packets. Value range is from 2 to 10. Default value is 4.
Port Status	You can change LLDP port status to Tx_only/Rx_only/Tx_and_Rx/Disable. Tx_only: LLDP transmit the packet of the port only. Rx_only: LLDP receive the packet of the port only. Tx_and_Rx: LLDP transmit and receive the packets of the port. Disable: LLDP do not transmit and receive the packets of the port.

4.11 Access Control List

The **Access Control List (ACL)** is a concept in computer security used to enforce privilege separation. It is a means of determining the appropriate access rights to a given object depending on certain aspects of the process that is making the request, principally the process's user identifier. **Access Control List (ACL)** is a mechanism that implements access control for a system resource by listing the identities of the system entities that are permitted or denied to access the resource. The screen in following screen appears.

Packets can be forwarded or dropped by ACL rules include IPv4 or non-IPv4. The Managed Switch can be used to block packets by maintaining a table of packet fragments indexed by source and destination IP address, protocol, and so on.

※Packet Type/Binding can be selected to ACL for IPv4 or non-IPv4.

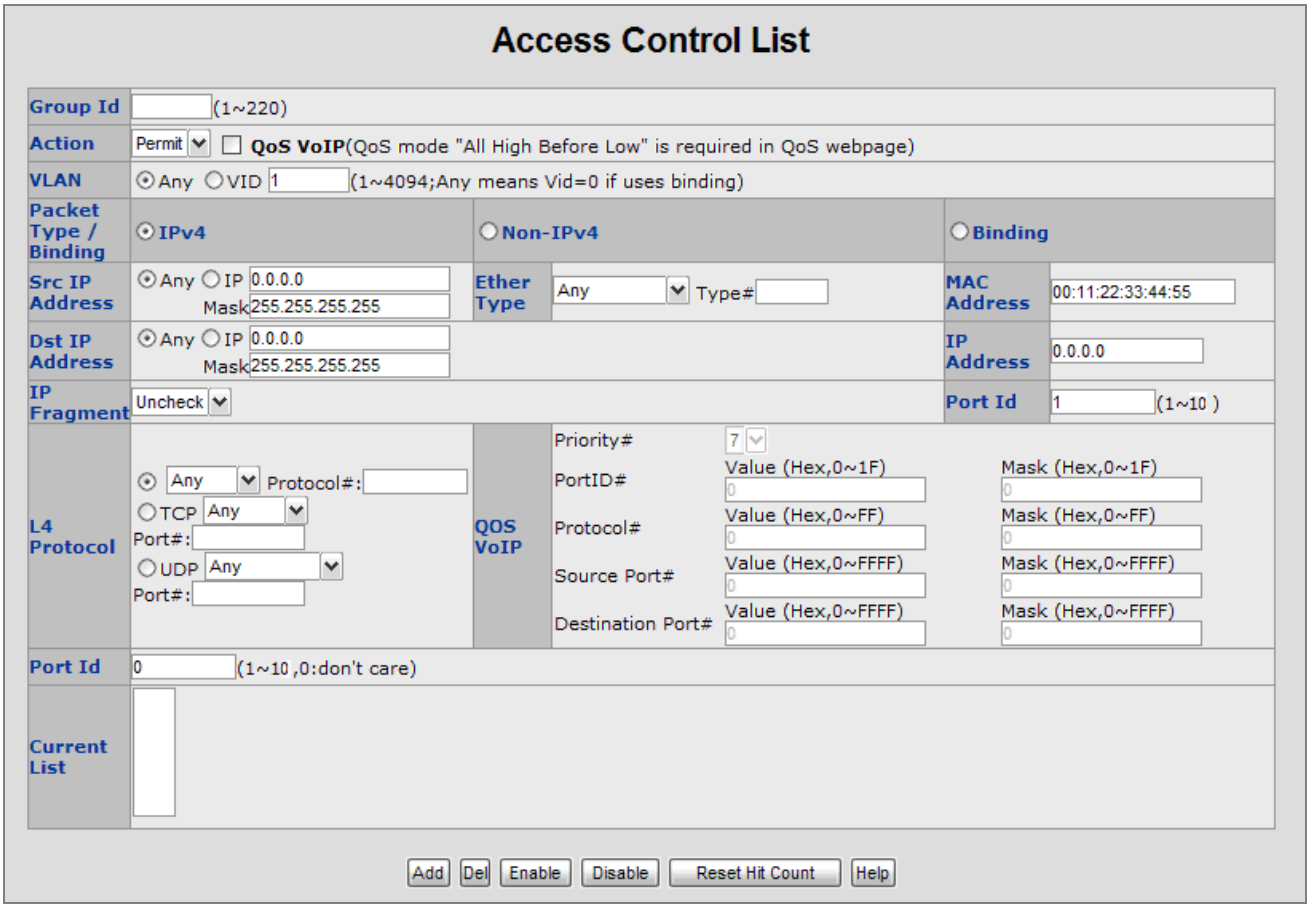


Figure 4-11-1: Access Control List (ACL) Web Page Screen

The page includes the following fields:

- **IPv4 ACL**

Object	Description	Default Vaule
Group ID	1 ~ 220 (max. 220 ACL group).	
Action	Permit/Deny. ■ **Permit**: Permit packet cross switch. ■ **Deny**: Drop packet.	Permit
VLAN	Any/VID. ■ **Any**: Any VLAN ID. ■ **VID**: 1~4094. A certain VLAN ID.	Any
Packet Type	IPv4/Non-IPv4/Binding ■ IPv4: Set IPv4 packet field. ■ Non-IPv4: Set non-IPv4 packet field. ■ Binding: Set binding entry.	IPv4
Src IP Address	Set this field if Packet Type is IPv4, or else ignore. Any/IP and Mask ■ Any: Any IP address. ■ IP: A certain IP address. Mask: ***.***.***.*** * is represent a digit from 0~9, *** is range from 0 to 255 **Note: This is not subnet mask.**	Any
Dst IP Address	Set this field if Packet Type is IPv4, or else ignore. Any/IP and Mask ■ Any: Any IP address. ■ IP: A certain IP address. Mask: ***.***.***.*** * is represent a digit from 0~9, *** is range from 0 to 255	Any
IP Fragment	Set this field if Packet Type is IPv4, or else ignore. Uncheck/Check ■ Uncheck: Not check IP fragment field. ■ Check: Check IP fragment field.	Uncheck
L4 Protocol	Set this field if Packet Type is IPv4, or else ignore. Any/ICMP(1)/IGMP(2)/TCP(6)/UDP(17)	Any
Protocol	Set this field if Packet Type is IPv4, or else ignore. 0~255. If protocol not find in L4 Protocol field, you can direct assigned number.	

TCP	Set this field if Packet Type is IPv4, or else ignore. Any/FTP(21)/HTTP(80)	Any
Port	Set this field if Packet Type is IPv4, or else ignore. 0~65535 If TCP port not find in TCP field, you can direct assign number.	
UDP	Set this field if Packet Type is IPv4, or else ignore. Any/DHCP(67)/TFTP(69)/NetBios(137)	Any
Port	Set this field if Packet Type is IPv4, or else ignore. 0~65535 If UDP port not find in UDP field, you can direct assigned number.	
Port ID	Source port ID, from 1~10, 0 means don't care.	0
Current List	You create ACL and Binding groups.	

- **Non-IPv4 ACL**

In ※Packet Type/Binding box should select ※Non-IPv4

Object	Description	Default Vaule
Group ID	1 ~ 220 (max. 220ACL group)	
Action	Permit/Deny. ■ **Permit**: Permit packet cross switch. ■ **Deny**: Drop packet.	Permit
VLAN	Any/VID. ■ **Any**: Any VLAN ID. ■ **VID**: 1~4094. A certain VLAN ID.	Any
Packet Type	IPv4/Non-IPv4/Binding ■ IPv4: Set IPv4 packet field. ■ Non-IPv4: Set non-IPv4 packet field. ■ Binding: Set binding entry.	IPv4
Ether Type	Set this field if Packet Type is Non-IPv4, or else ignore. Any/ARP(0x0806)/IPX(0x8137)	Any
Type	Set this field if Packet Type is Non-IPv4, or else ignore. 0~0xFFFF If ether type not found in the Ether Type field, you can direct assigned number.	
Current List	You create ACL and Binding groups.	

- **Binding**

Let device that has specific IP address and MAC address use network. We can set specific IP address, MAC address, VLAN ID and port ID to bind, and device can cross switch if all conditions match.

Use binding function; we should enable it first in the following page.

In ※Packet Type/Binding box should select ※Binding.

Object	Description	Default Vaule
Group ID	1 ~ 220 (max. 220 ACL group)	
Action	Permit/Deny. ■ Permit: Permit packet cross switch. ■ Deny: Drop packet.	Permit
VLAN	Any/VID. ■ Any: Any VLAN ID. ■ VID: 1~4094. A certain VLAN ID.	Any
Packet Type	IPv4/Non-IPv4 / Binding ■ IPv4: Set IPv4 packet field. ■ Non-IPv4: Set non-IPv4 packet field. ■ Binding: Set binding entry.	IPv4
MAC Address	**:**:**:**:**:** * is represent a digit from 0~9 and A~F, *** is range from 0 to FF.	00:11:22:33:44:55
IP Address	***.***.***.*** * is represent a digit from 0~9, *** is range from 0 to 255.	0.0.0.0
Port ID	Source port ID, from 1~10.	1
Current List	You create ACL and Binding groups.	

4.12 Security Manager

This web page provides user configuration for switch management access level.

Figure 4-12-1: User Configuration Interface Screenshot

The page includes the following fields:

Object	Description
Username:	Display Username of the Managed Switch.
Access Level:	Display the access level of the Managed Switch.
Edit:	Provide edit current specific user setting.
Add New User:	Provide add new user setting of the Managed Switch

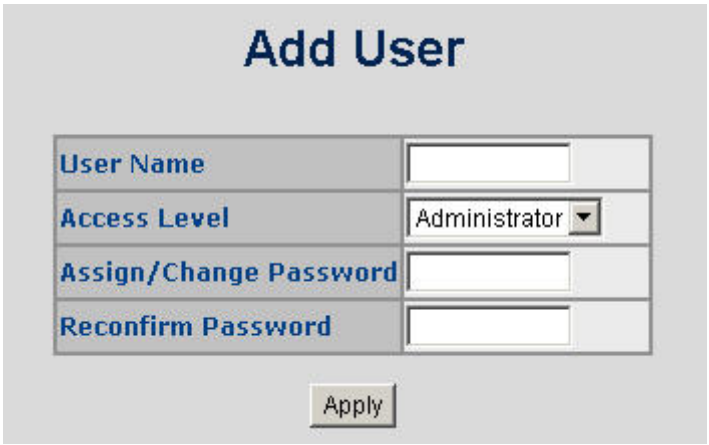


Figure 4-12-2: Add New User Configuration Interface Screenshot

The page includes the following fields:

Object	Description
User Name:	Assign Username for the Managed Switch.
Access Level:	Assign the access level of the Managed Switch; the available options are **"Administrator", "Operator"** and **"Viewer"**. Default is **"Administrator"**.
Assign/Change Password:	Assign password for the Managed Switch.
Reconfirm Password:	Input password again to confirm setting.
Apply:	Press this button to take affect.

4.13 MAC Limit

MAC limit allows users to set a maximum number of MAC addresses to be stored in the MAC address table. The MAC addresses chosen to be stored in MAC address table is the result of first-come-first-save policy. Once a MAC address is stored in the MAC address table, it stays in until it is aged out. When an "opening" is available, the switch stored the first new MAC address it sees in that opening. All packets from MAC addresses not in the MAC address table should be blocked.

4.13.1 MAC Limit Configuration

The Layer 2 MAC Limit function can be per-port configured for security management purposes. When the port is in MAC Limit mode, the port will be "locked" without permission of address learning. Only the incoming packets with Source MAC already existing in the address table can be forwarded normally. User can disable the port from learning any new MAC addresses.

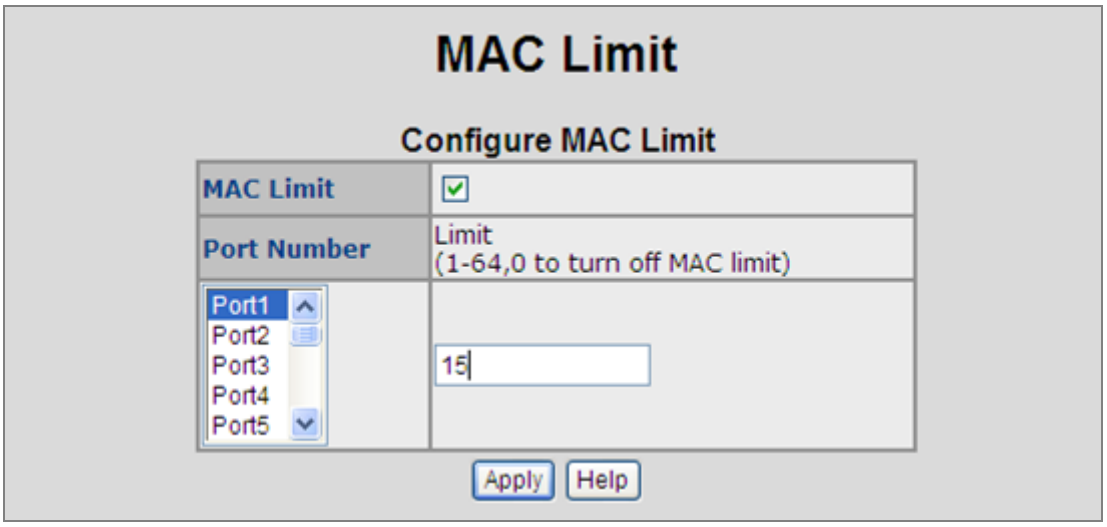


Figure 4-13-1: MAC Limit **-** Configure MAC Limit

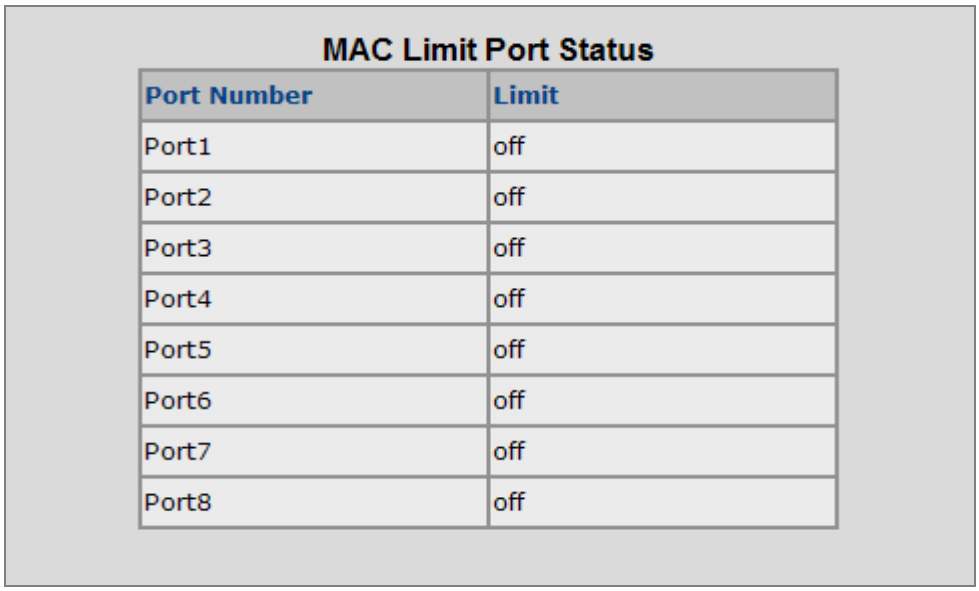
The page includes the following fields:

Object	Description
MAC Limit	**Enable** or **disable** MAC limit function for the Managed Switch.
Port Number	Indicate port 1 to port 8.
Limit	The maximum number of per-port MAC addresses to be learned (1-64, 0 to disable this port's MAC limit function).

MAC Limit is only functioned on Fast Ethernet port, Port-1 to Port-8 of VC-820M.

4.13.2 MAC Limit Port Status

This table displays the current MAC Limit status of each port.



MAC Limit Port Status

Port Number	Limit
Port1	off
Port2	off
Port3	off
Port4	off
Port5	off
Port6	off
Port7	off
Port8	off

Figure 4-13-2: MAC Limit – MAC Limit Port Status

The page includes the following fields:

Object	Description
Port Number	Indicate port 1 to port 8.
Limit	Display the current MAC Limit configuration and status of each port.

4.14 802.1x Configuration

802.1x is an IEEE authentication specification which prevents the client from accessing a wireless access point or wired switch until it provides authority, like the user name and password that are verified by an authentication server (such as RADIUS server).

4.14.1 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.

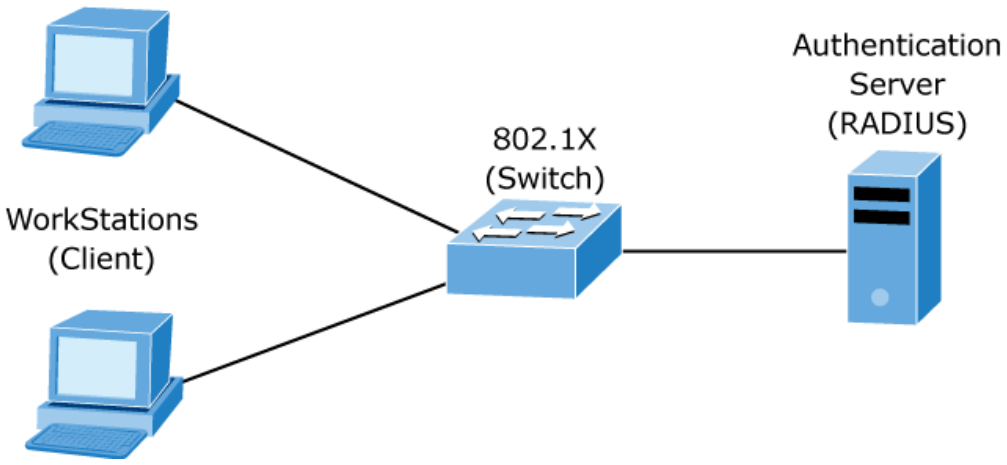


Figure 4-14-1: 802.1x Device Role

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

- ***Authentication server***—performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. In this release, the Remote Authentication Dial-In User Service (RADIUS) security system with **Extensible Authentication**

Protocol (EAP) extensions is the only supported authentication server; it is available in Cisco Secure Access Control Server version 3.0. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

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

■ **Authentication Initiation and Message Exchange**

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

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

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

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

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

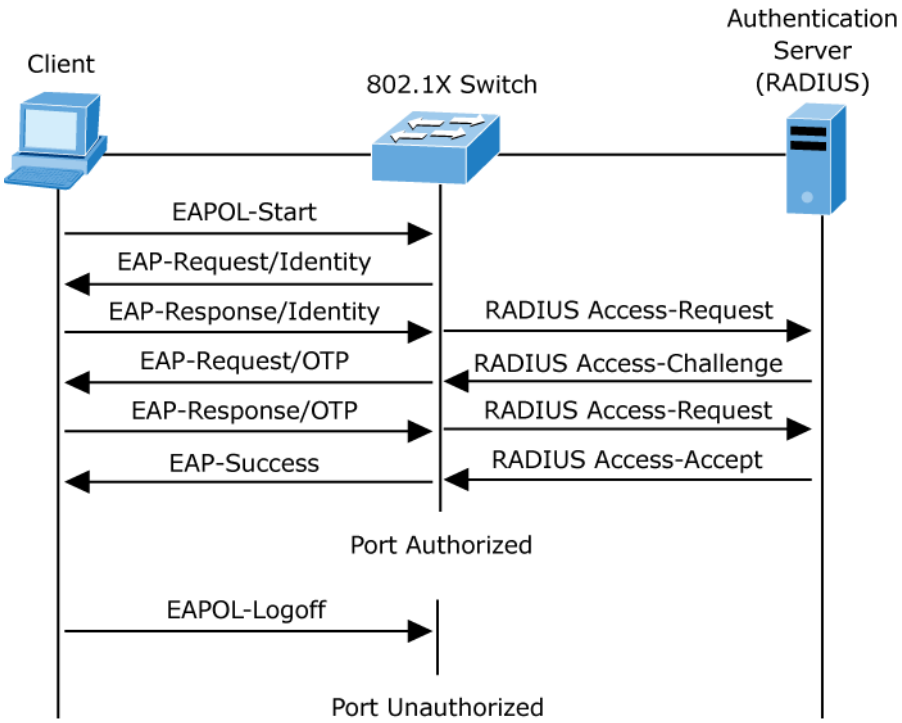


Figure 4-14-2: EAP message exchange

■ **Ports in Authorized and Unauthorized States**

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

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

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

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

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

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

4.14.2 System Configuration

802.1x makes use of the physical access characteristics of IEEE802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails.

To enable 802.1x, from **System** \ **System Information** \ **Misc Config** then you still to fill in the authentication server information：

Figure 4-14-3: System information\Misc Configuration\802.1x Protocol

After enabling the IEEE 802.1x function, you can configure the parameters of this function.

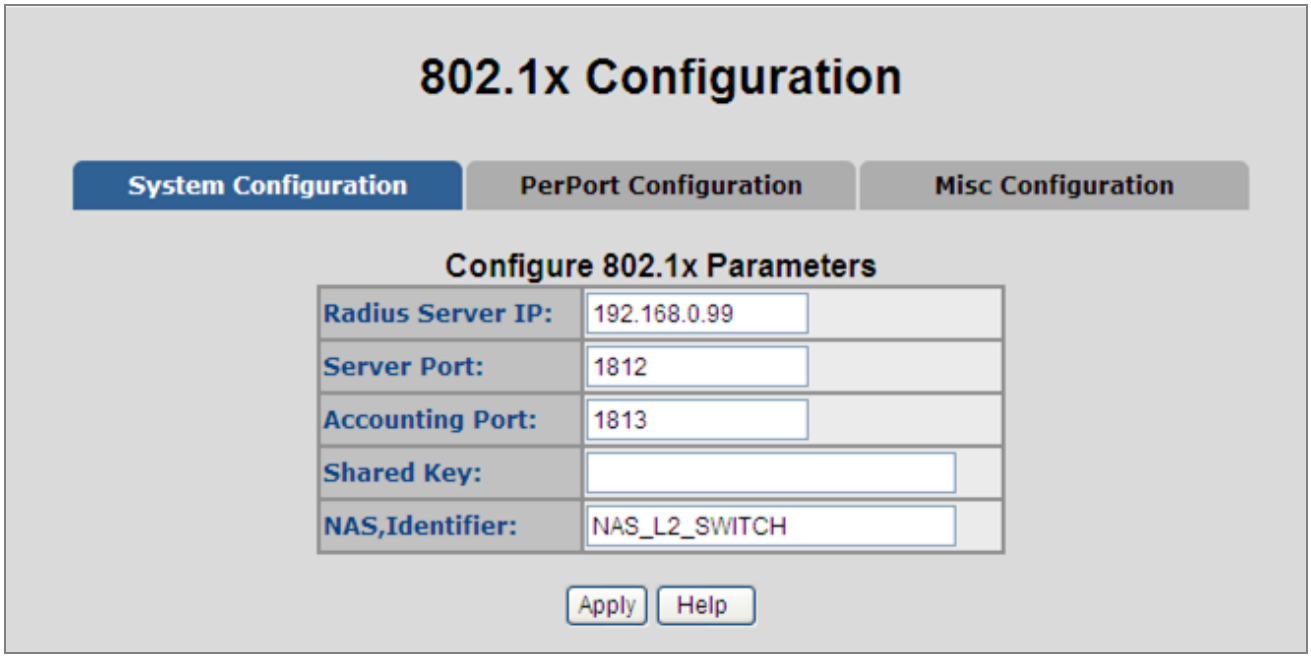


Figure 4-14-4: 802.1x System Configuration Interface

The page includes the following fields:

Object	Description
IEEE 802.1x Protocol:	Enable or disable 802.1x protocol.
RADIUS Server IP:	Assign the RADIUS Server IP address.
Server Port:	Set the UDP destination port for authentication requests to the specified RADIUS Server.
Accounting Port:	Set the UDP destination port for accounting requests to the specified RADIUS Server.
Shared Key:	Set an encryption key for using during authentication sessions with the specified RADIUS server. This key must match the encryption key used on the RADIUS Server.
NAS, Identifier:	Set the identifier for the RADIUS client.

4.14.3 802.1x Port Configuration

On this page, you can select the specific port and configure the authorization state. The state provides **No Authorization**, **Force Authorized**, **Force unauthorized**, and **Authorize**.

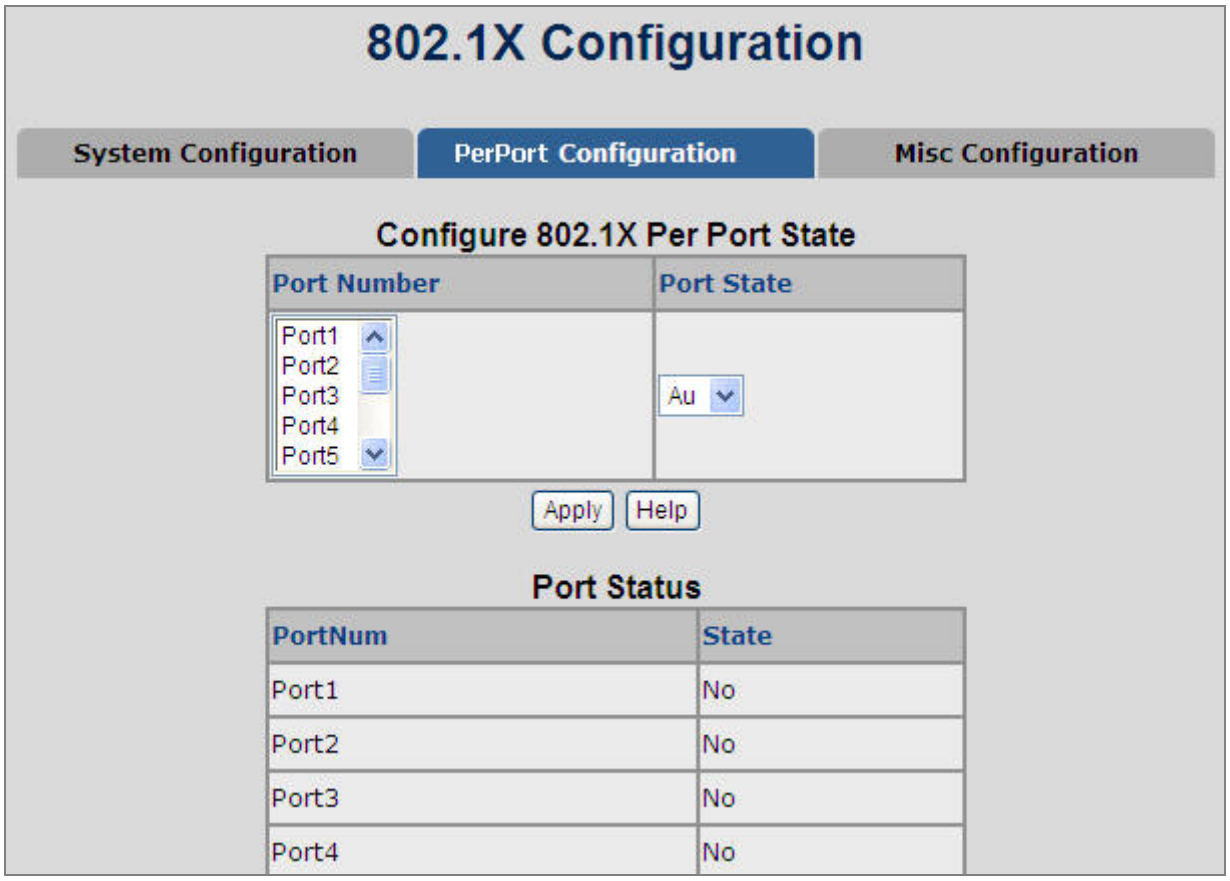


Figure 4-14-5: 802.1x Per Port Setting interface

The page includes the following fields:

Object	Description
Fu (Force Unauthorized)	The specified port is required to be held in the unauthorized state.
Fa (Force Authorized)	The specified port is required to be held in the authorized state.
Au (Authorize)	The specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the authentication server.
No	The specified port works without complying with 802.1x protocol.

4.14.4 Misc Configuration

On this page, you can change the default configuration for the 802.1x standard:

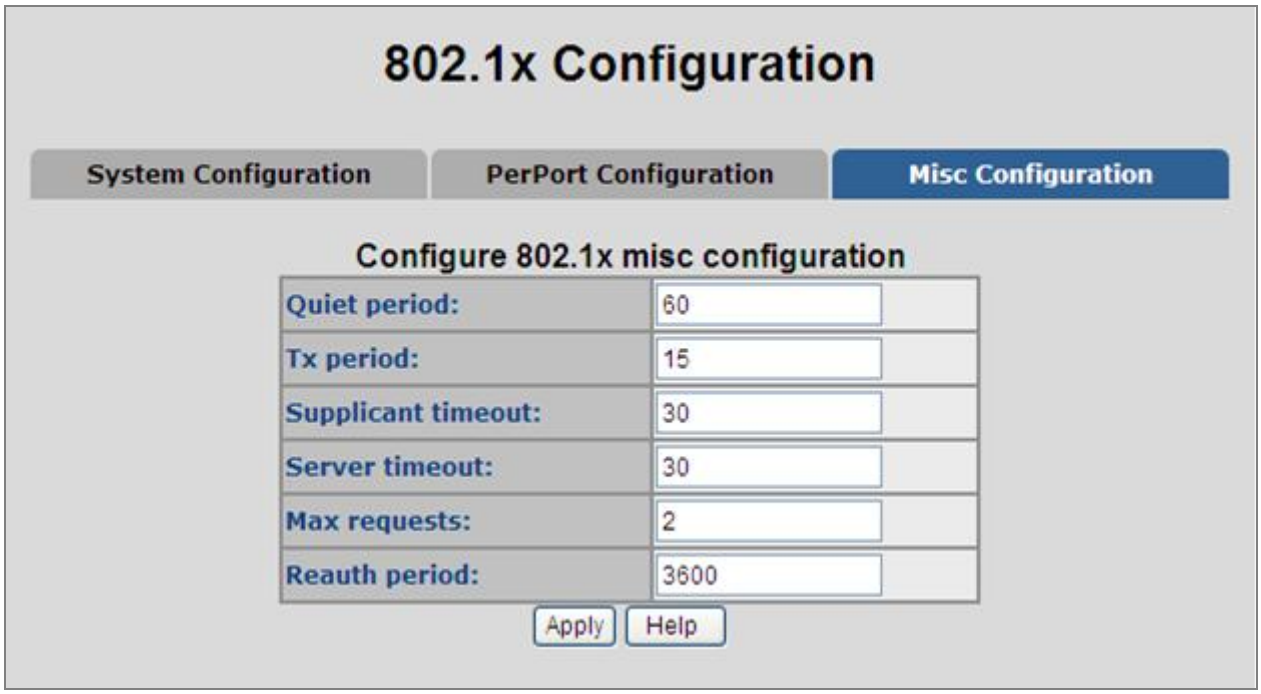


Figure 4-14-6: 802.1x Misc Configuration interface

The page includes the following fields:

Object	Description
Quiet Period:	Used to define periods of time during which it will not attempt to acquire a supplicant. Default time is **60** seconds.
TX Period:	Set the period the port waits for retransmit next EAPOL PDU during an authentication session. Default value is **30** seconds.
Supplicant Timeout:	Set the period of time the switch waits for a supplicant response to an EAP request. Default value is **30** seconds.
Server Timeout:	Set the period of time the switch waits for a server response to an authentication request. Default value is **30** seconds.
Max Requests:	Set the number of authentication that must time-out before authentication fails and the authentication session ends. Default value is **2** times.
Reauth Period:	Set the period of time which clients connected must be re-authenticated. Default value is **3600** seconds.

4.15 QoS Configuration

4.15.1 Understanding 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.

The **QoS** page of the Switch contains three types of QoS mode - the **CoS** mode, **ToS** mode or **Port-based** mode can be selected. Both the three mode rely on predefined fields within the packet to determine the output queue.

- **CoS / 802.1p Tag Priority** Mode –The output queue assignment is determined by the IEEE 802.1p VLAN priority tag.
- **ToS / DSCP** Mode - The output queue assignment is determined by the ToS or DSCP field in the IP packets.
- **Port-Based Priority** Mode – Any packet received from the specify high priority port will treated as a high priority packet.

4.15.2 QoS Configuration

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

802.1Q Tag and 802.1p priority

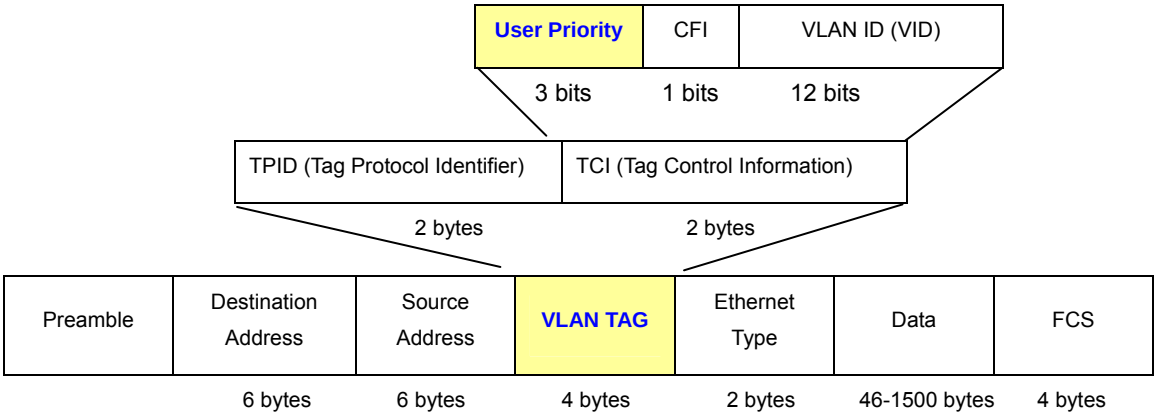


Figure 4-15-1: 802.1p Tag Priority

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.

4.15.2.1 Priority Queue Service settings

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 Switch supports Static Port Ingress priority and four queues.

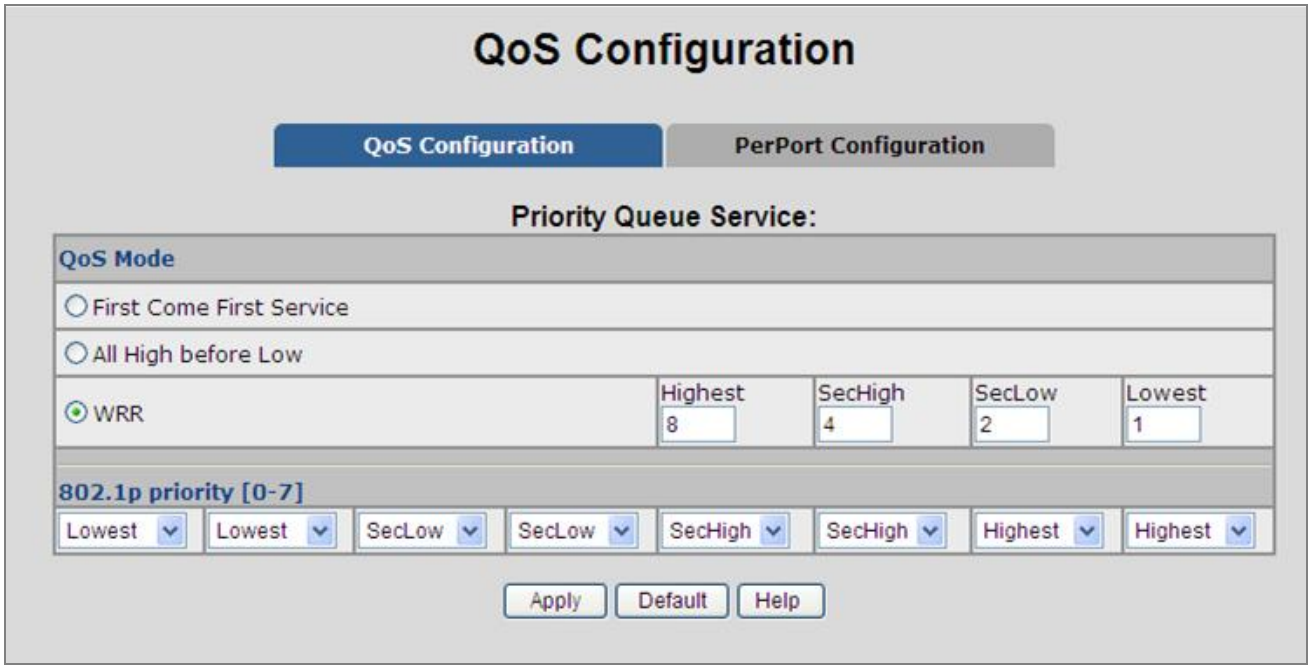


Figure 4-15-2: QoS Configuration – 802.1Priority

The table includes the following fields:

Object	Description
First Come First Served	The sequence of packets sent is depending on arrival order.
All High before Low	The high priority packets sent before low priority packets.
Weighted Round Robin	Select the preference given to packets in the switch's higher-priority queue. These options represent the number of higher priority packets sent before one lower priority packet is sent. For example, 8 Highest : 4 SecHigh : 2 SecLow : 1 Lowest means that the switch sends 8 highest priority packets before sending 4 second high priority packet, before sending 2 second low priority packet, before sending 1 lowest priority packet.
802.1p priority [0-7]	Set up the CoS priority level 0~7—**High**, **Middle**, **Low**, **Lowest**.

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 low class. The user may configure the mapping between CoS and Traffic classifiers.

4.15.2.2 QoS PerPort Configuration

Configure the priority level for each port. With the drop-down selection item of Priority Type above being selected as Port-based, this control item will then be available to set the queuing policy for each port.

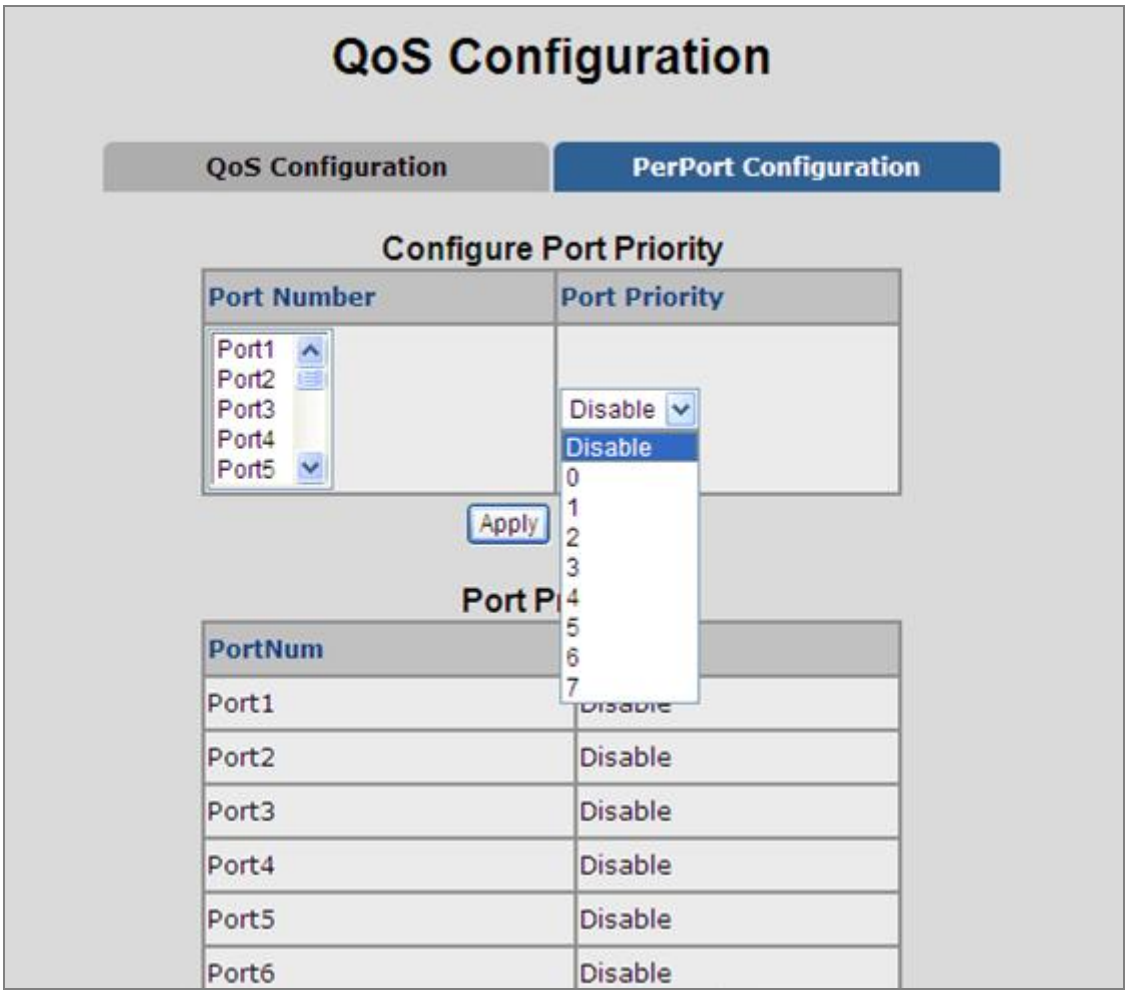


Figure 4-15-3: QoS Configuration – Port-Based Priority

The table includes the following fields:

Object	Description
Port Number:	Indicate port 1 to port 10.
Port Priority:	Each port has 8 priority levels—0~7 or Disable to be chosen. 7 is the highest priority.

4.15.3 ToS/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.

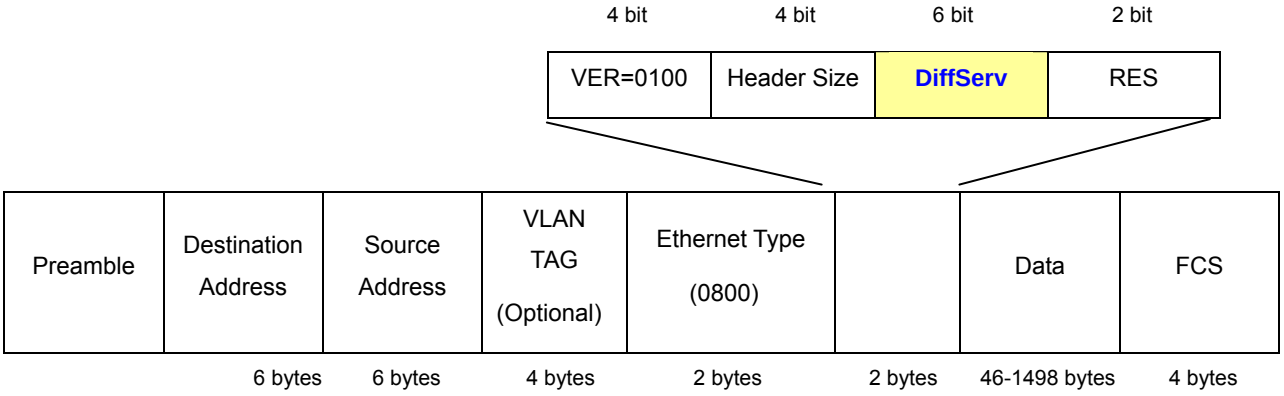


Figure 4-15-4: IPv4 Frame Format

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.

4.15.3.1 ToS/DSCP Configuration

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

Enable ToS/DSCP for traffic classification and then the DSCP to priority mapping column is configurable.

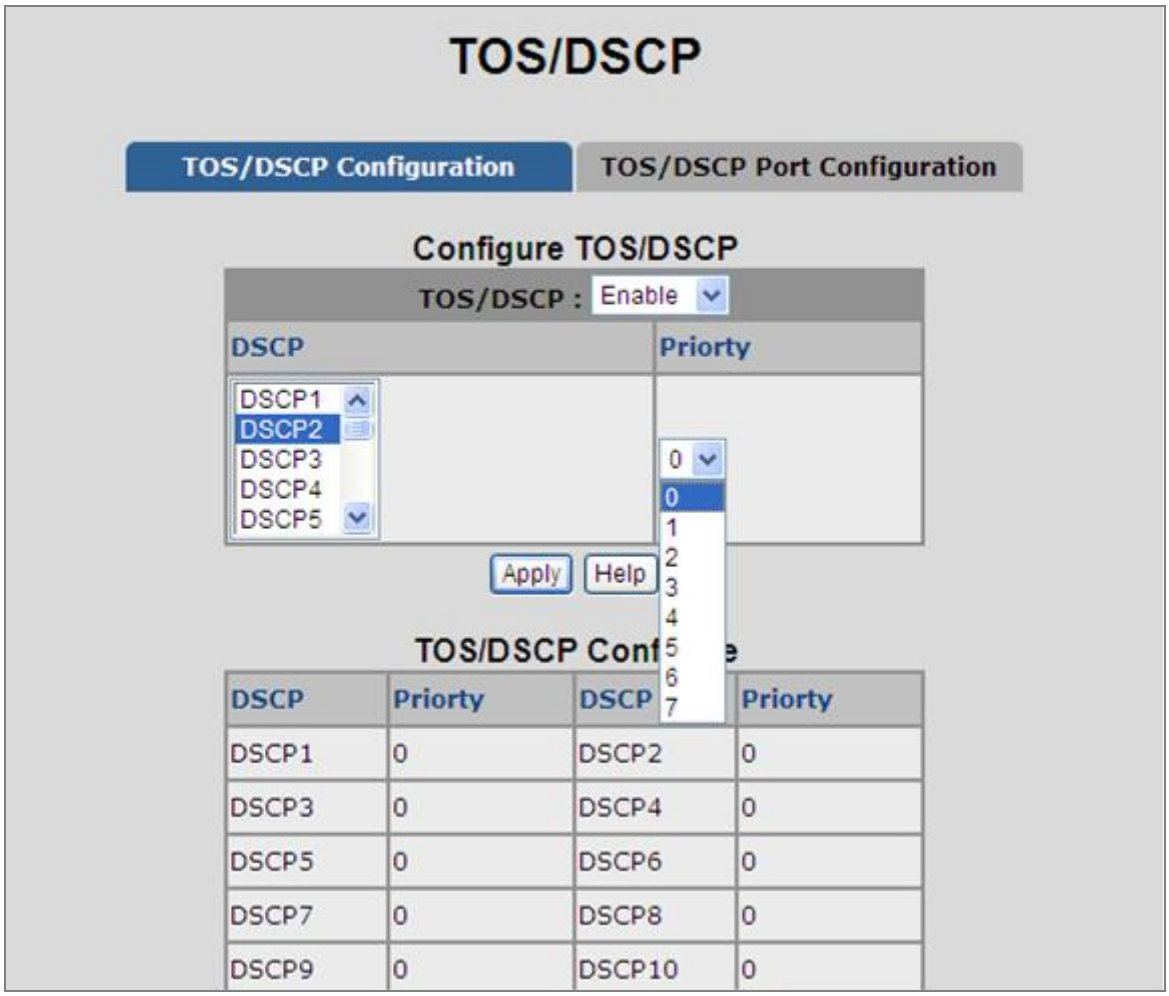


Figure 4-15-5: QoS Configuration – ToS Priority

The page includes the following fields:

Object	Description
ToS/DSCP	**Enable**/**Disable** internal traffic class (0~7) to map the corresponding IP DSCP value.
DSCP	The values of the IP DSCP header field within the incoming packet. 0~63.
Priority	Specify which 802.1p priority to map the corresponding IP DSCP. The value is 0~7.

4.15.3.2 ToS/DSCP Port Configuration

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

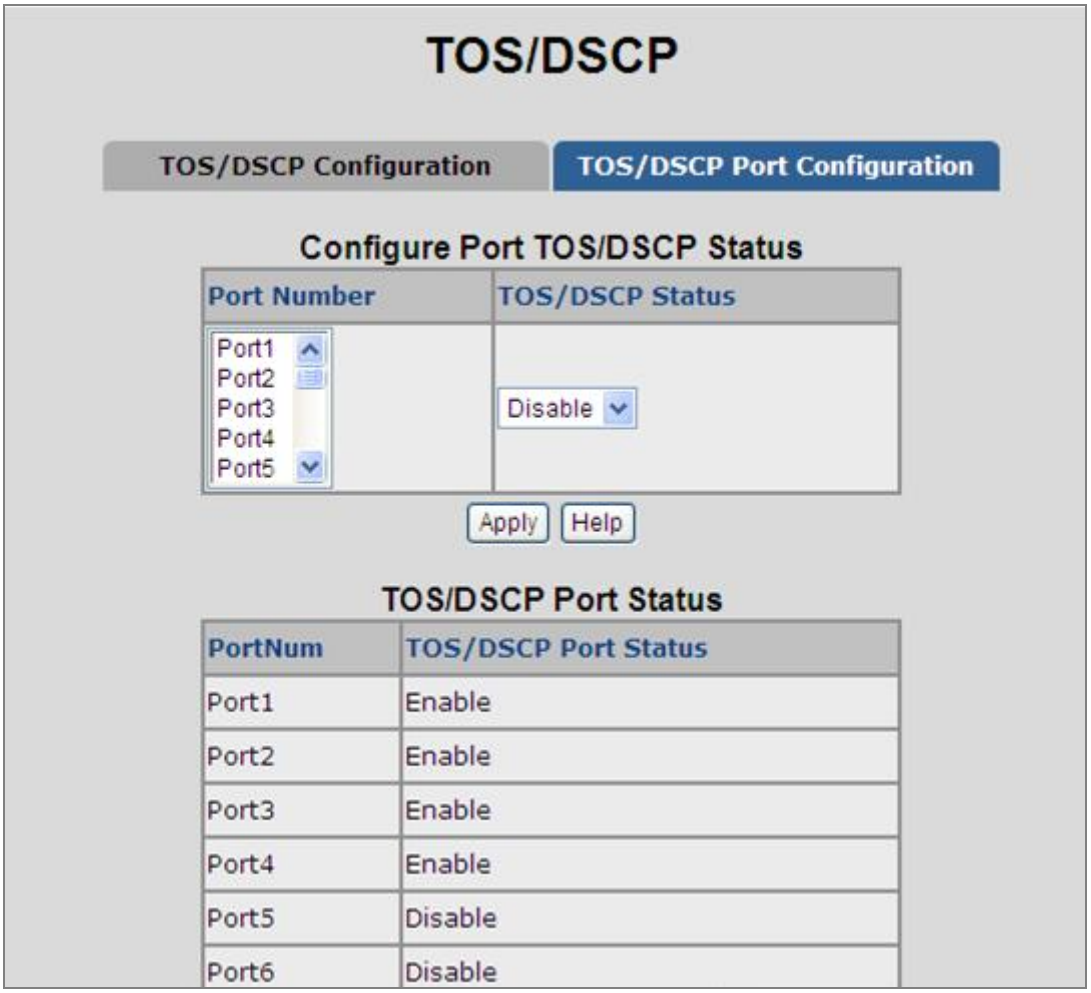


Figure 4-15-6: QoS Configuration – ToS/DSCP Port Status

The table includes the following fields:

Object	Description
Port Number	Indicate port 1 to port 10.
ToS/DSCP Status	Enable/Disable ToS/DSCP map to 802.1p priority on specify port.

4.16 VDSL Configuration

VDSL2 (Very High-Bit-Rate Digital Subscriber Line 2), G.993.2 is the newest and most advanced standard of xDSL broadband wire line communications. Designed to support the wide deployment of Triple Play services such as voice, data, high definition television (HDTV) and interactive gaming, VDSL2 enable operators and carrier to gradually, flexibly, and cost efficiently upgrade exiting xDSL-infrastructure.

VDSL2 was developed and standardized in record time to address the shortcomings of existing access technologies. It servers as the ideal xDSL technology for eliminating last-mile bottlenecks and enable global mass deployment of advance Triple Play services. Unlike its predecessor, which allowed choosing either **DMT (Discrete Multitone)** or QAM (Quadrature Amplitude Modulation) technology, VDSL2 only uses the DMT line code.

DMT is a method of separating a DSL signal so that the usable frequency range is separated into multiple small frequency bands, or tone. It uses up to 4096 tones which are spaced 4 kHz or 8 kHz apart. Each tone can be used for either downstream or upstream.

The PLANET VDSL2 Managed Switch can provide very high performance access to remote CPE, both downstream and upstream up to 100Mbps. The VDSL2 Managed Switch complies with ITU-T G993.2 standard, and supports CO operating mode. The CO by WEB UI and users can connect to multiple CPE for Point-to-Multi-Point Application, data transmission between multiple networks over existing copper telephone lines.

4.16.1 Profile Configuration

This option allows you to set up the VDSL configuration profile. From the **VDSL Configuration** menu, please click on VDSL Configuration Profile. The following page is displayed.

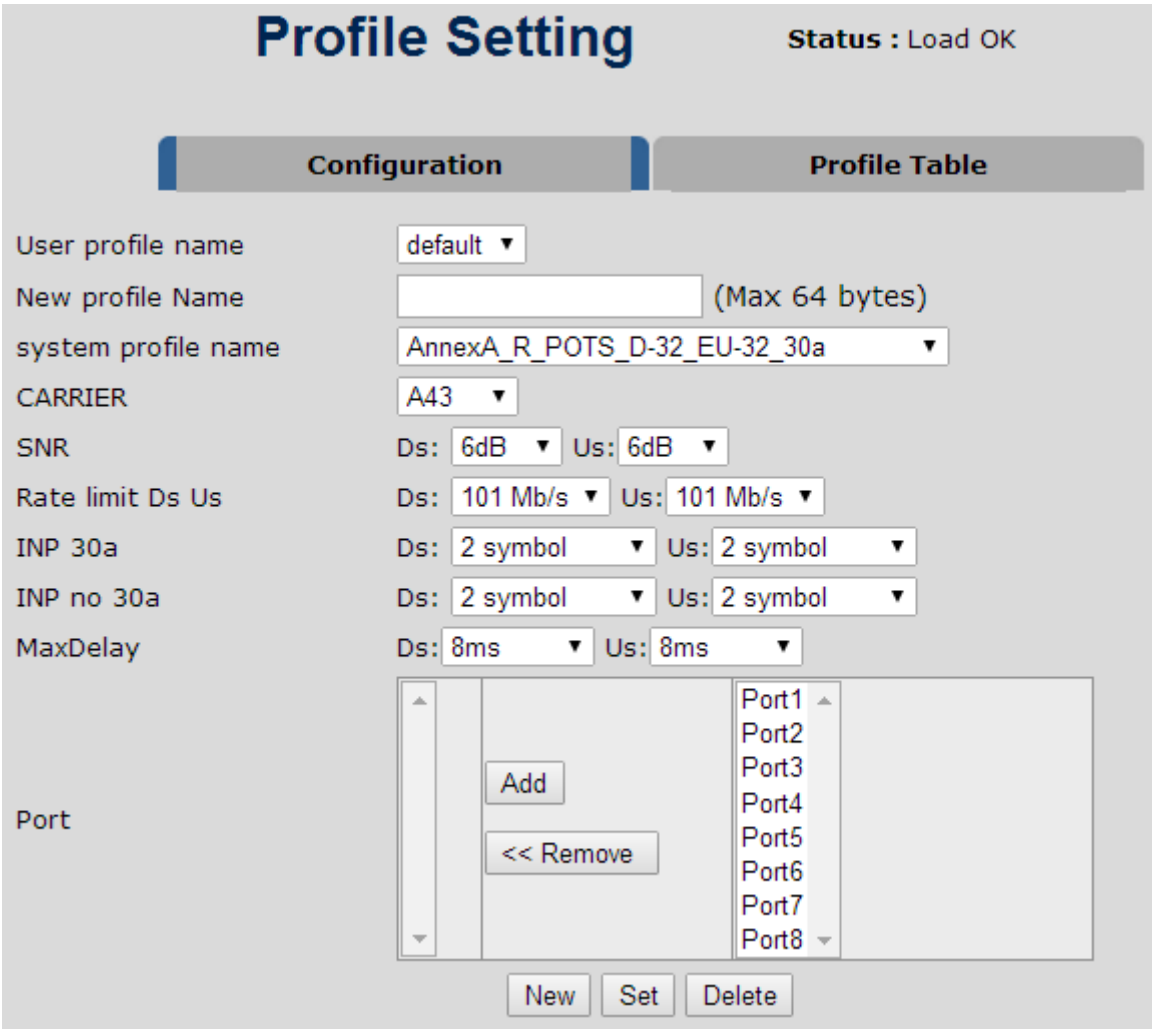


Figure 4-16-1: VDSL2 Profile Configuration Interface

The page includes the following fields:

Object	Description
User Profile Name	This field shows the index name of the profile. Click on the drop-down list and select the index profile name to be created or configured.
New Profile Name	Type in profile name when you're creating a new profile. The allowed characters include: 0-9, A-Z, a-z, "_" and "-". Maximum 64 bytes.
System Profile Name	The VDSL2 Managed Switch provides most common VDSL2 profiles for user; it supports the 30a, 17a, 12a, 12b, 8a, 8b, 8c and 8d. You can select the proper profile for your real environment. Different profiles provide different connection status of data rate and distance; please refer to Appendix A for more information. Click on the drop-down list and select the VDSL band plan to be used. The VDSL2 Managed Switch supports below profiles. 1. AnnexA_R_POTS_D-64_EU-64_30a 2. AnnexA_R_POTS_D-32_EU-32_17a 3. AnnexA_R_POTS_D-32_EU-32_12b 4. AnnexA_R_POTS_D-32_EU-32_12a 5. AnnexA_R_POTS_D-32_EU-32_8a

	6. AnnexA_R_POTS_D-32_EU-32_8b 7. AnnexA_R_POTS_D-32_EU-32_8c 8. AnnexA_R_POTS_D-32_EU-32_8d 9. AnnexA_R_POTS_D-64_EU-64_30a_NUS0 10. AnnexA_R_POTS_D-64_EU-64_17ª 11. AnnexB_B7-1_997-M1c-A-7 12. AnnexB_B7-2_997-M1x-M-8 13. AnnexB_B7-3_997_M1x-M 14. AnnexB_B7-4_997_M2x-M-8 15. AnnexB_B7-5_997_M2x-A 16. AnnexB_B7-6_997_M2x-M 17. AnnexB_B7-9_997E17-M2x-A 18. AnnexB_B7-10_997E30-M2x-NUS0 19. AnnexB_B8-1_998-M1x-A 20. AnnexB_B8-2_998-M1x-B 21. AnnexB_B8-4_998-M2x-A 22. AnnexB_B8-5_998-M2x-M 23. AnnexB_B8-6_998-M2x-B 24. AnnexB_B8-8_998E17-M2x-NUS0 25. AnnexB_B8-9_998E17-M2x-NUS0-M 26. AnnexB_B8-10_998ADE17-M2x-NUS0-M 27. AnnexB_B8-11_998ADE17-M2x-A 28. AnnexB_B8-12_998ADE17-M2x-B 29. AnnexB_B8-13_998E30-M2x-NUS0 30. AnnexB_B8-14_998E30-M2x-NUS0-M 31. AnnexB_B8-15_998ADE30-M2x-NUS0-M 32. AnnexB_B8-16_998ADE30-M2x-NUS0-A 33. AnnexC_POTS_25-138_b 34. AnnexC_POTS_25-276_b 35. AnnexC_TCM-ISDN
CARRIER	Configure G.handshake tone of VDSL ports. Click on the drop-down list and select the VDSL carrier plan to be used. The VDSL2 Managed Switch supports below profiles. 1. Auto 2. A43 3. B43 4. V43
SNR	The line quality is determined by using the **SNR (Signal to Noise Ratio)** and applies to VDSL line connections only. SNR is the ratio of the amplitude of the actual signal to the amplitude of noise signals at a given point in time. The higher the SNR is, the better the line quality. Please manually adapt SNR margin according to line quality and distance to get better performance or replace the line with new one. Click on the drop-down list and select the SNR to be used. Configures SNR margin of Downstream or Upstream. SNR margin value: **6 dB** to **24 dB** Default value: **6 dB**

Rate Limit DS US	■ **DS**: Configure the transmit rate of Maximum Downstream. The value of downstream traffic limitation in Mbps, from the VDSL2 CO Managed Switch to the CPE. Per port in step of 1 Mbps and 5Mbps. Default : **101Mbp/s** (bit per second) The range between 1Mbps to 101Mbps ■ **US**: Configure the transmit rate of Maximum Upstream. The value of upstream traffic limitation in Mbps, from the VDSL2 CPE to the CO Managed Switch. Per port in step of 1 Mbps and 5Mbps. Default : **101Mbp/s** (bit per second) The range between 1Mbps to 101Mbps
INP 30a	Configure INP with specifying Upstream or Downstream to set minimum protection values of port provision. Click on the drop-down list and select the **INP (Impulse Noise Protection)** to be used. The range between 1 (or 0.5 for no 30a case) to 16 symbol or **No Protection** Default value: **2 symbol**
MaxDelay	The VDSL line type can be configured by selecting **maximum Interleave delay** of Downstream or Upstream direction. Basically, there are three types ■ **No limit** ■ **Fast mode** ■ **Interleave** The interleave process is use to correct data error before modulation digital signal into analog signal. Interleave prevents error by enhanced correction but may slow down transmit rate because packets are gathered. **Interleaved mode** provides impulse noises protection for any impulse noise with a duration less than 250 us. By configuring interleave maximum-delay, it can prevent transmission delay caused of waiting data gathered. To skip Interleave process, select "No delay" to operate with Fast mode. **Fast mode** guarantees a minimum end to end latency less than 1 ms. Click on the drop-down list and select the MaxDelay to be used. Configures interleave-delay with specifying Downstream or Upstream. The unit is msec. The range between **0ms** to **63ms** Default value: **8ms**
Port	In the VDSL2 Managed Switch, all VDSL ports are contained on one profile. To change the member ports to other profile, the "**User Profile Name**" has to be selected first. **Add**: Applies Profile to specified ports. **Remove**: Disables profile in specified ports.

Note

1. The default profile of VDSL port is "**30a**"
2. If the SNR margin is configured too big, the transmit rate will slow down, whereas communications is stable.
3. If the "MaxDelay" is configured to "**No Delay**" (Fast mode), error correction will not be down well, whereas transmit rate of data becomes faster.

Note

Option Band:

AnnexA: use 6 to 32 tone in annex A environment in the direction of upstream.

AnnexB: use 32 to 64 tone in annex B environment in the direction of upstream.

4.16.2 VDSL Port Status

Network manager can check the VDSL Line status in this VDSL Port Status web page; it includes Line status, Upstream / Downstream Date Rate, SNR and VDSL2 firmware version.

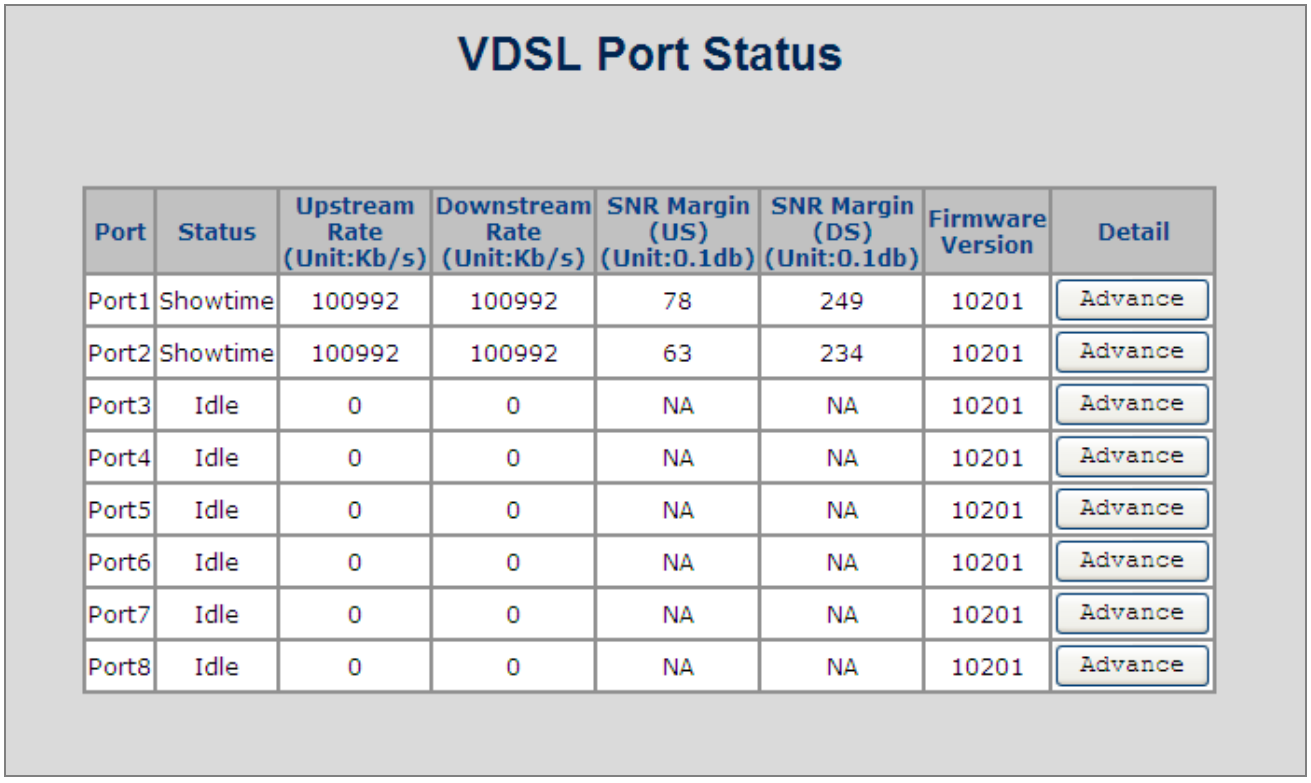


Figure 4-16-2: VDSL2 Port Status Interface

By click the **Advance** button and the windows popup shows detailed VDSL upstream/downstream information on specified port.

Up Stream		Down Stream	
Delay	5 ms	Delay	5 ms
INP	20 0.1 symbols	INP	20 0.1 symbols
CRC 15M	0	CRC 15M	0
CRC 1Day	0	CRC 1Day	0
CRC Total	0	CRC Total	0
Error Correction 15M	0	Error Correction 15M	0
Error Correction 1Day	1195	Error Correction 1Day	0
Error Correction Total	9808	Error Correction Total	456
xdsl2ChStatusPrevDataRate	0 Kbps	xdsl2ChStatusPrevDataRate	0 Kbps
xdsl2LineStatusAttainableRate	105448 Kbps	xdsl2LineStatusAttainableRate	168634 Kbps
xdsl2LineStatusElectricalLength	11 0.1 dB	xdsl2LineStatusElectricalLength	11 0.1 dB
xdsl2LineBandStatusSnrMargin	NA (US0) 0.1dB	xdsl2LineBandStatusSnrMargin	-- (--) 0.1dB
xdsl2LineBandStatusSnrMargin	79 (US1) 0.1dB	xdsl2LineBandStatusSnrMargin	248 (DS1) 0.1dB
xdsl2LineBandStatusSnrMargin	79 (US2) 0.1dB	xdsl2LineBandStatusSnrMargin	248 (DS2) 0.1dB
xdsl2LineBandStatusSnrMargin	77 (US3) 0.1dB	xdsl2LineBandStatusSnrMargin	249 (DS3) 0.1dB
xdsl2LineBandStatusSnrMargin	NA (US4) 0.1dB	xdsl2LineBandStatusSnrMargin	NA (DS4) 0.1dB
xdsl2PMLCurr15MTimeElapsed	733 secs	xdsl2PMLCurr15MTimeElapsed	29 secs
xdsl2PMLCurr15MFecs	0	xdsl2PMLCurr15MFecs	0
xdsl2PMLCurr15MEs	0	xdsl2PMLCurr15MEs	0
xdsl2PMLCurr15MSes	0	xdsl2PMLCurr15MSes	0
xdsl2PMLCurr15MLoss	0	xdsl2PMLCurr15MLoss	0
xdsl2PMLCurr15MUas	0	xdsl2PMLCurr15MUas	0
xdsl2PMLCurr1DayTimeElapsed	60133 secs	xdsl2PMLCurr1DayTimeElapsed	60329 secs
xdsl2PMLCurr1DayFecs	7	xdsl2PMLCurr1DayFecs	0
xdsl2PMLCurr1DayEs	0	xdsl2PMLCurr1DayEs	0
xdsl2PMLCurr1DaySes	0	xdsl2PMLCurr1DaySes	0
xdsl2PMLCurr1DayLoss	0	xdsl2PMLCurr1DayLoss	0
xdsl2PMLCurr1DayUas	0	xdsl2PMLCurr1DayUas	0
xdsl2PMLCurrTotalFecs	0	xdsl2PMLCurrTotalFecs	0
xdsl2PMLCurrTotalEs	0	xdsl2PMLCurrTotalEs	0

The page includes the following fields:

Object	Description
Delay	Display the current **Interleave delay** of the selected VDSL line of Downstream or Upstream direction
INP	Shows the configured INP in VDSL line.
CRC 15M	Shows the numbers of CRC errors in previous 15 minutes.

	It can be use to check times of error at present time from beginning of the 15 minutes and time of error of previous 15 minutes.
CRC 1Day	Shows the numbers of CRC errors in previous day. It can be use to check times of error at present time from starting Today, times of error of yesterday.
CRC Total	Shows the collected data of all errors from booting.
Error Correction 15M	Shows the numbers of error correction in previous 15 minutes.
Error Correction 1Day	Shows the numbers of error correction in previous day.
Error Correction Total	Shows the collected data of all error correction from booting.
xdsl2ChStatusPrevDataRate	The previous net data rate that the bearer channel was operating at just before the latest rate change event. This could be a full or short initialization, fast retrain, DRA or power management transitions, excluding transitions between L0 state and L1 or L2 states. The data rate is coded in bit/s.
xdsl2LineStatusAttainableRateUs	Maximum Attainable Data Rate Upstream. The maximum upstream net data rate currently attainable by the VTU-R transmitter and the VTU-C receiver, coded in bit/s.
xdsl2LineStatusElectricalLength	This parameter contains the estimated electrical length expressed in dB at 1 MHz, kl0. This is the final electrical length that would have been sent from the VTU-O to VTU-R if the electrical length was not forced by the CO-MIB. The value ranges from 0 to 128 dB in steps of 0.1 dB.
xdsl2LineBandStatusSnrMargin	SNR Margin is the maximum increase in dB of the noise power received at the VTU (VTU-R for a band in the downstream direction and VTU-C for a band in the upstream direction), such that the BER requirements are met for all bearer channels received at the VTU. Values range from -640 to 630 in units of 0.1 dB (Physical values are -64 to 63 dB). A special value of 0x7FFFFFFF (2147483647) indicates the SNR Margin is out of range to be represented. A special value of 0x7FFFFFFE (2147483646) indicates the SNR Margin measurement is currently unavailable
xdsl2PMLCurr15MTimeElapsed	Total elapsed seconds in this interval
xdsl2PMLCurr15MFecs	Count of seconds during this interval that there was at least one FEC correction event for one or more bearer channels in this line. This parameter is inhibited during UAS or SES
xdsl2PMLCurr15MEs	Count of seconds during this interval that there was: VTU-C: CRC-8 >= 1 for one or more bearer channels OR LOS >= 1 OR SEF >=1 OR LPR >= 1 VTU-R: FEBE >= 1 for one or more bearer channels OR

	LOS-FE >=1 OR RDI >=1 OR LPR-FE >=1 . This parameter is inhibited during UAS
xdsl2PMLCurr15MSes	Count of seconds during this interval that there was: VTU-C: (CRC-8 anomalies in one or more of the received bearer channels) >= 18 OR LOS >= 1 OR SEF >= 1 OR LPR >= 1 VTU-R: (FEBE anomalies in one or more of the received bearer channels) >= 18 OR LOS-FE >= 1 OR RDI >= 1 OR LPR-FE >= 1 This parameter is inhibited during UAS.
xdsl2PMLCurr15MLoss	Count of seconds during this interval that there was LOS (or LOS-FE for VTU-R
xdsl2PMLCurr15MUas	Count of seconds in Unavailability State during this interval. Unavailability begins at the onset of 10 contiguous severely-errored seconds, and ends at the onset of 10 contiguous seconds with no severely-errored seconds
xdsl2PMLCurr1DayTimeElapsed	Total elapsed seconds in this interval
xdsl2PMLCurr1DayFecs	Count of seconds during this interval that there was at least one FEC correction event for one or more bearer channels in this line. This parameter is inhibited during UAS or SES
xdsl2PMLCurr1DayEs	Count of seconds during this interval that there was: VTU-C: CRC-8 >= 1 for one or more bearer channels OR LOS >= 1 OR SEF >= 1 OR LPR >= 1 VTU-R: FEBE >= 1 for one or more bearer channels OR LOS-FE >= 1 OR RDI >= 1 OR LPR-FE >= 1. This parameter is inhibited during UAS.
xdsl2PMLCurr1DaySes	Count of seconds during this interval that there was: VTU-C: (CRC-8 anomalies in one or more of the received bearer channels) >= 18 OR LOS >= 1 OR SEF >= 1 OR LPR >= 1 VTU-R: (FEBE anomalies in one or more of the received bearer channels) >= 18 OR LOS-FE >= 1 OR RDI >= 1 OR LPR-FE >= 1 . This parameter is inhibited during UAS
xdsl2PMLCurr1DayLoss	Count of seconds during this interval that there was LOS (or LOS-FE for VTU-R
xdsl2PMLCurr1DayUas	Count of seconds in Unavailability State during this interval. Unavailability begins at the onset of 10 contiguous severely-errored seconds, and ends at the onset of 10 contiguous seconds with no severely-errored seconds

5. CONSOLE MANAGEMENT

The PLANET VDSL2 Managed Switch series is equipped with an RS-232 DB9 connector as default. And both of the two models support Telnet management.

5.1 Logging in to the Console Interface

To configure the system via console mode, connect a serial cable to a COM port on a PC or notebook computer and to RJ45 type serial (console) port of the Managed Switch. The console port of the Managed Switch is DCE already, so that you can connect the console port directly through PC without the need of Null Modem.

Please refer to **chapter 3.5- Administration Console** to get more information about how to connect to the console interface of VC-820M with HyperTerminal on Microsoft Windows platform.

Once the terminal has connected to the device, power on the VC-820M, the terminal will display that it is running testing procedures.

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

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

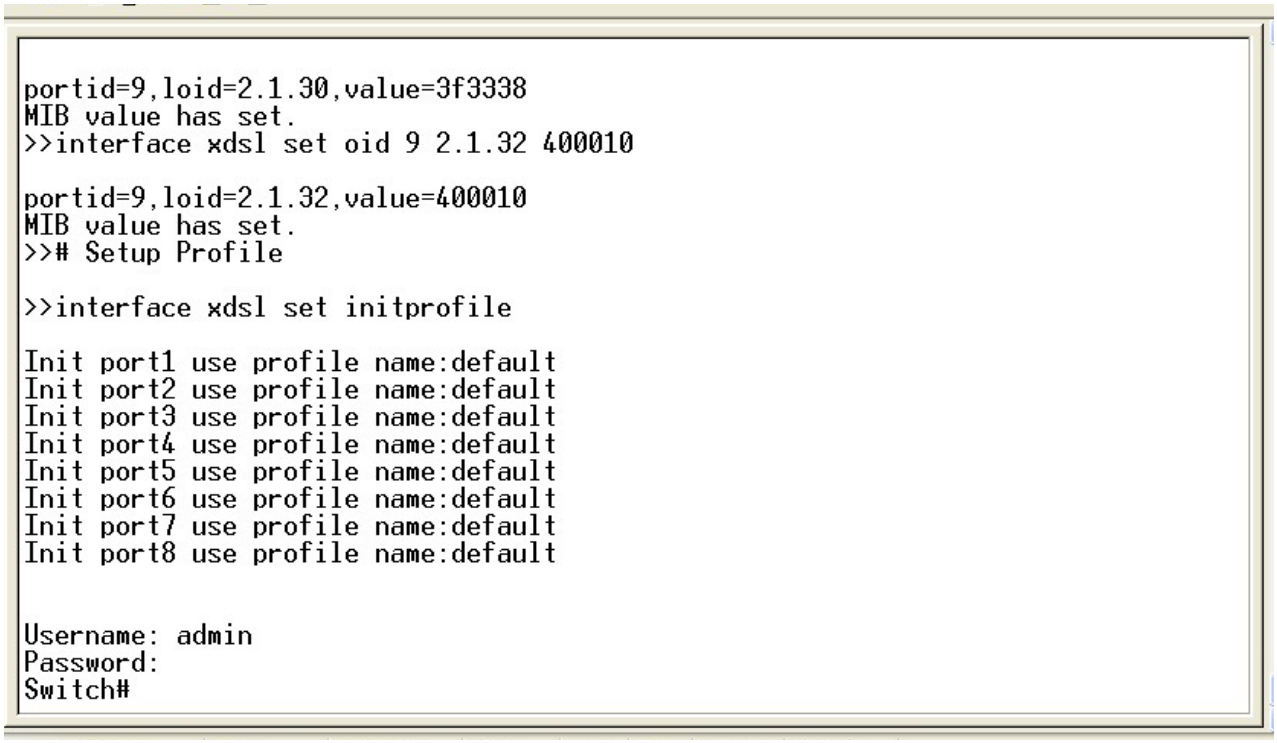


Figure 5-1-1: VDSL2 Managed Switch Console Login Screen

Note

1. For security reason, please change and memorize the new username and password after this first setup.
   Username Max: **6**, Min: **1** character

Password Max: **6**, Min: **1** character

2. Only accept command in lowercase letter under console interface.

5.2 Configuring IP address

The VC-820M Managed Switch is shipped with default IP address shown below:

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 follows:

- **Show the current IP address**

1. On "**Switch#** " prompt, enter "**configure**".
2. On "**Switch(config)#** " prompt, enter "**show ip**".
3. The screen displays the current IP address, Subnet Mask and Gateway as shown in Figure 5-2-1.

```
   QinQ.............OK
   Forwarding......OK
   IP Mcst.........OK
   IGMP............OK
   STP/RSTP/MSTP...OK
   MIB.............OK
   802.1X..........OK
   Port............OK
   ACL.............OK
   SNMP............OK
   Port interval...OK
   TOS/DSCP........OK
   MAC.............OK
   Completed!!


Username: admin
Password:
Switch# configure
Switch(config)# show ip
IP address: 192.168.0.100
Subnet mask: 255.255.255.0
Gateway: 192.168.0.254
Switch(config)# _
```

Figure 5-2-1: IP Information Screen

■ **Configure IP address**

1. On "**Switch(config)#** " prompt, enter the following command and press **<Enter>** as shown in Figure 5-2-2.

```
Switch(config)# ip address 192.168.1.100 255.255.255.0
Switch(config)# ip default-gateway 192.168.1.254
```

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

IP: 192.168.1.100
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.254

```
   Port.............OK
   ACL..............OK
   SNMP.............OK
   Port interval...OK
   TOS/DSCP........OK
   MAC..............OK
   Completed!!


Username: admin
assword:
Switch# configure
Switch(config)# show ip
IP address: 192.168.0.100
Subnet mask: 255.255.255.0
Gateway: 192.168.0.254
Switch(config)# ip address 192.168.1.100 255.255.255.0
Switch(config)# ip default-gateway 192.168.1.254
Switch(config)# show ip
IP address: 192.168.1.100
Subnet mask: 255.255.255.0
Gateway: 192.168.1.254
Switch(config)# copy running-config startup-config
Switch(config)# _
```

Figure 5-2-2: Set IP Address Screen

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

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

If you are not familiar with console command or the related parameter, enter "**help**" 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.

5.3 Commands Level

The following table lists the CLI commands and description.

Modes	Access Method	Prompt	Exit Method	About This Mode1
User EXEC	Begin a session with your switch.	**switch>**	Enter logout or quit.	The user commands available at the user level are a subset of those available at the privileged level. Use this mode to: • Perform basic tests. • Display system information.
Privileged EXEC	Enter the enable command while in User EXEC mode.	**switch#**	Enter disable to exit.	The privileged command is the advanced mode. Use this mode to • Display advanced function status • Save configuration
Global Configuration	Enter the configure command while in privileged EXEC mode.	**switch (config)#**	To exit to privileged EXEC mode, enter exit or end	Use this mode to configure those parameters that are going to be applied to your switch.

6. COMMAND LINE INTERFACE

6.1 Operation Notice

To enter the "configuration" mode, you need to be in the privileged mode, and then type in the command **configure**:

```
Switch# configure
Switch (config) #
```

6.1.1. Command Line Editing

Keys Function

<Ctrl>-B	; ← Moves the cursor back one character.
<Ctrl>-D	Deletes the character at the cursor.
<Ctrl>-E	Jumps to the end of the current command line.
<Ctrl>-F	; → Moves the cursor forward one character.
<Ctrl>-K	Deletes from the cursor to the end of the command line.
<Ctrl>-N	; ↓ Enters the next command line in the command history.
<Ctrl>-P	; ↑ Enters the previous command line in the command history.
<Ctrl>-U	Deletes from the cursor to the beginning of the command line.
<Ctrl>	-W Deletes the last word typed.
<Esc> B	Moves the cursor backward one word.
<Esc> D	Deletes from the cursor to the end of the word.
<Esc> F	Moves the cursor forward one word.
<Backspace>	Delete the character before the cursor.
<Del>	Delete the character at the cursor.

The following generic function keys provide functions in all of the menus:

6.1.2. Command Help

You may enter **?** in any command mode, and the CLI will return possible commands at that point, along with some description of

6.2 System Commands

show running-config

Description:

Display the running configuration of the switch.

copy running-config startup-config

Description:

Back up the switch configurations.

erase startup-config

Description:

Reset to default factory settings at next boot time.

clear arp

Description:

<*ip-addr*> specifies the IP address to be cleared. If no IP address is entered, the entire ARP cache is cleared.

show arp

Description:

Show the IP ARP translation table.

ping

Description:

Send ICMP ECHO_REQUEST to network hosts.

Parameters:

<1..999> specifies the number of repetitions. If not entered, it will continue to ping until you press <Ctrl>-C to stop.

syslog-server

Description:

Set the syslog server information.

Syntax

syslog-server <IP address > [<*0-2*>]

Parameters:

<*0-2* > specifies logging type. "0" is default value.

0: none

1: major

2: All

[no] sntp

Description:

Enable / disable SNTP.

Syntax

[no] sntp

sntp

Description:

Start SNTP service.

Syntax

sntp <IP address > [<*Time Zone Offset*>][<*Time Range*>]

Parameters:

<*Time Zone Offset*> specifies time zone offset is before / after UTC.

before-utc: Before-UTC

after-utc: After-UTC

<0-24 > Time range <Unit: hour>

6.3 Switch Static Configuration

6.3.1 Port Configuration and Show Status

port state

Turn the port state on or off.

Syntax:

port state <on | off> [<*port-list*>]

Parameters:

<*port-list*> specifies the ports to be turn on or off. If not entered, all ports are turn on or off.

port nego

Description:

Set port negotiation.

Syntax

port nego <force | auto | nway-force> [<*port-list*>]

Parameters:

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

port speed

Description:

Set port speed (in mbps) and duplex.

Syntax:

port speed <**10** | **100** | **1000**> <**full** | **half**> [<*port-list*>]

Parameters:

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

port flow

Description:

Enable or disable port flow control.

Syntax:

port flow <**enable** | **disable**> [<*port-list*>]

Parameters:

The <**enable** | **disable**> enables or disables flow control.

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

port rate

Description:

Set port effective ingress or egress rate.

Syntax:

port rate <**ingress** | **egress**> <0..8000> [<*port-list*>]

Parameters:

<0..8000> specifies the ingress or egress rate.<0..8000>

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

port priority

Description:

Set port priority.

Syntax:

port priority <**disable | 0..7**> [<*port-list*>]

Parameters:

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

port jumboframe

Description:

Set port jumbo frame. When port jumbo frame is enable, the port forward jumbo frame packet

Syntax:

port jumboframe <**enable** | **disable**> [<*port-list*>]

Parameters:

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

show port status

Description:

Show port status, including port State, Link, Trunking, VLAN, Negotiation, Speed, Duplex, Flow control, Rate control ,Priority, Security, BSF control.

```
Switch(config)# show port status
--------------------------------------------------------------------------
Port    1    Information
--------------------------------------------------------------------------
State: on
Link: down
Trunking: none
VLAN: DEFAULT
Priority: disable
Security: off
--------------------------------------------------------------------------
```

```
Port     2     Information
-------------------------------------------------------------------------
State: on
Link: down
Trunking: none
VLAN: DEFAULT
Priority: disable
Security: off
-------------------------------------------------------------------------
Port     3     Information
-------------------------------------------------------------------------
State: on
Link: down
--More--
```

show port statistics

Description:

Show port statistics, including TxGoodPkt, TxBadPkt, RxGoodPkt, RxBadPkt, TxAbort, Collision, and DropPkt.

Parameters:

<*port-id*> specifies the port to be shown.

```
Switch(config)# show port statistics
-------------------------------------------------------------------------
Port     1     Information
-------------------------------------------------------------------------
TxGoodPkt: 0
TxBadPkt: 0
RxGoodPkt: 0
RxBadPkt: 0
TxAbort: 0
Collision: 0
DropPkt: 0
-------------------------------------------------------------------------
Port     2     Information
-------------------------------------------------------------------------
TxGoodPkt: 0
TxBadPkt: 0
RxGoodPkt: 0
RxBadPkt: 0
TxAbort: 0
Collision: 0
DropPkt: 0
-------------------------------------------------------------------------
Port     3     Information
-------------------------------------------------------------------------
--More--
```

show port protection

Description:

Show protected port information.

```
Switch(config)# show port protection
--------+-----------+-------
   Port   | Protected | Group
--------+-----------+-------
        1  |      off      |  1
        2  |      off      |  1
        3  |      off      |  1
        4  |      off      |  1
        5  |      off      |  1
        6  |      off      |  1
        7  |      off      |  1
        8  |      off      |  1
        9  |      off      |  1
       10  |      off      |  1
     Trk1  |      off      |  1
```

6.4 Trunk Configuration

Trunk allows the switch to combine ports so that they function like a single high-speed link. It can be used to increase the bandwidth to some devices to provide a high-speed link. For example, trunk is useful when making connections between switches or connecting servers to the switch. Trunk can also provide a redundant link for fault tolerance. If one link in the trunk failed, the switch can balance the traffic among the remaining links.

1. The 10/100 Mbps port cannot be trunked with Gigabit port (Port 9 and Port 10).
2. All ports in the same trunk group will be treated as a single port. If a trunk group exists, the ports belonging to that trunk will be replaced by "TRUNK #" in the VLAN configuration screen. The following example configures Port 1~ Port 2 as "TRUNK 1."

6.4.1 Trunking Commands

show trunks

Description:

Show trunking information.

```
Switch(config)# show trunk
 Group ID | LACP |       Ports       | LACP Active
----------+------+-------------------+-------------
       1  | Yes  |          1, 2 |          1, 2
```

trunk add

Description:

Add a new trunk group.

Syntax:

trunk add <*trunk-id*> <*lacp* | *no-lacp*> <*port-list*> <*active-port-list*>

Parameters:

<*trunk-id*> specifies the trunk group to be added.

<lacp | no-lacp> to specify the added trunk group to be LACP enabled

<*port-list*> specifies the ports to be set.

<*active-port-list*> specifies the ports to be set to LACP active.

no trunk

Description:

Delete an existing trunk group.

Syntax:

no trunk <*trunk-id*>

Parameters:

<*trunk-id*> specifies the trunk group to be deleted

6.4.2 LACP Command

[no] lacp

Description:

Enable/disable LACP.

lacp system-priority

Description:

Set LACP system priority.

Syntax:

lacp system-priority <***1..65535***>

Parameters:

<1..65535> specifies the LACP system priority.

no lacp system-priority

Description:

Set LACP system priority to the default value 32768.

show lacp status

Description:

Show LACP enable/disable status and system priority.

```
Switch(config)# show lacp status
LACP is enabled.
LACP system priority: 32768
```

show lacp

Description:

Show LACP information.

show lacp agg

Description:

Show LACP aggregator information.

Syntax:

show lacp agg <*trunk-id*>

Parameters:

<*trunk-id*> specifies the trunk group to be shown.

show lacp port

Description:

Show LACP information by port.

Syntax:

show lacp port <*port-id*>

Parameters:

<*port-id*> specifies the port to be shown.

If VLAN group exist, all of the members of static trunk group must be in same VLAN group.

6.5 VLAN Configuration

6.5.1 Virtual LANs

A Virtual LAN (VLAN) is a logical network group that limits the broadcast domain. It allows you to isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. Basically, creating a VLAN within a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically. A station can belong to more than one VLAN group. VLAN prevents users from accessing network resources of another on the same LAN, thus the users can not see the hard disks and printers of another user in the same building. VLAN can also increase the network performance by reducing the broadcast traffic and enhance the security of the network by isolating groups.

The Managed Switch supports two types of VLANs:

- **Port-based**
- **IEEE 802.1Q (tag) –based**

Only one of the two VLAN types can be enabled at one time.

Port-based VLANs are VLANs where the packet forwarding decision is made based on the destination MAC address and its associated port. You must define the outgoing ports allowed for each port when you use port-based VLANs. In port-based VLANs, the packets received from one port can only be sent to the ports which are configured to the same VLAN. As shown in the following figure, the switch administrator configured port 1~2 as VLAN 1 and port 3~4 as VLAN 2. The packets received from port 1 can only be forwarded to port 2. The packets received from port 2 can only be forwarded to port 1. That means the computer A can send packets to computer B, and vice versa. The same situation also occurred in VLAN 2. The computer C and D can communicate with each other. However, the computers in VLAN 1 can not see the computers in VLAN 2 since they belonged to different VLANs.

IEEE 802.1Q (tag) -based VLANs enable the Ethernet functionality to propagate tagged packets across the bridges and provides a uniform way for creating VLAN within a network then span across the network. For egress packet, you can choose to tag it or not with the associated VLAN ID of this port. For ingress packet, you can forward this packet to a specific port as long as it is also in the same VLAN group.

The 802.1Q VLAN works by using a tag added to the Ethernet packets. The tag contains a VLAN Identifier (VID) which belongs to a specific VLAN group. And ports can belong to more than one VLAN.

The difference between a port-based VLAN and a tag-based VLAN is that the tag-based VLAN truly divided the network into several logically connected LANs. Packets rambling around the switches can be forwarded more intelligently. In the figure shown below, by identifying the tag, broadcast packets coming from computer A in VLAN1 at sw1 can be forwarded directly to VLAN1.

However, the switch could not be so smart in the port-based VLAN mechanism. Broadcast packets will also be forwarded to port 4 of sw2. It means the port-based VLAN can not operate a logical VLAN group among switches.

The VC-820M series support both Port-based VLAN and Tag-based (802.1Q) VLAN modes. The default configuration is

tag-based (802.1Q) VLAN. In the 802.1Q VLAN, initially, all ports on the switch belong to default VLAN, VID is 1.

You cannot delete the default VLAN group in 802.1Q VLAN mode.

6.5.2 VLAN Mode: Port-based

Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging is ignored.

show vlan mode

Description:

Display the current VLAN mode.

vlan mode

Description:

Change VLAN mode.

Syntax:

vlan mode (disabled|port-based|dot1q)

Parameters:

(disabled | port-based | dot1q) specifies the VLAN mode.

Every time when the VLAN mode is changed, user has to restart the switch for valid value.

6.5.3 Advanced 802.1Q VLAN Configuration

Ingress filters configuration

When a packet is received on a port, you can govern the switch to drop it or not if it is an untagged packet. Furthermore, if the received packet is tagged but not belonging to the same VLAN group of the receiving port, you can also control the switch to forward or drop the packet. The example below configures the switch to drop the packets not belonging to the same VLAN group and forward the packets not containing VLAN tags.

VLAN Commands:

show vlan mode

Description:

Display the current VLAN mode.

vlan mode

Description:

Change VLAN mode.

Syntax:

vlan mode (disabled|port-based|dot1q)

Parameters:

(disabled | port-based | dot1q) specifies the VLAN mode.

Every time when the VLAN mode is changed, user has to restart the switch for valid value.

vlan add

Description:

Add or edit VLAN entry.

Syntax:

vlan add <1-4094> NAME (cpu-port|no-cpu-port) LIST [LIST]

Parameters:

<1-4094> specifies the VLAN ID or Group ID (if port based VLAN mode)

NAME specifies the VLAN group name.

(cpu-port|no-cpu-port) specifies the CPU port belong this VLAN group.

LIST specifies the ports to be set to VLAN members.

[LIST] specifies the ports to be set to tagged members. If not entered, all members set to untagged.

```
e.g.. switch(config)# vlan add 1 vlan1 cpu-port 1-4
```

This VLAN entry has four members (from port1 to port4) and all members are untagged.

no vlan

Description:

Delete VLAN entry.

Syntax:

no vlan <1-4094>

Parameters:

<1-4094> specifies the VLAN ID or group ID (if port based VLAN).

e.g. no vlan 1

show vlan

Description:

Show VLAN entry information.

Syntax:

show vlan [<1-4094>]

Parameters:

<1-4094> specifies the VLAN ID, null means all valid entries.

e.g.

```
Switch(config)# show vlan 1
  VLAN                        : 1
  Type                        : Static
  Creation Time (sec.): 43
  CPU Port                    : Yes

   Port   |   Member
-----------+--------------
   Port1 | Untagged
   Port2 | Untagged
   Port3 | Untagged
   Port4 | Untagged
   Port5 | Untagged
   Port6 | Untagged
   Port7 | Untagged
   Port8 | Untagged
   Port9 | Untagged
  Port10 | Untagged
     Trk1 | Untagged
```

show vlan static

Description:

Show static VLAN entry information.

show vlan pvid

Description:

Show port default VLAN ID.

Syntax:

show vlan pvid [LIST]

Parameters:

[LIST] specifies the ports to be showed. If not entered, all port's PVID will be showed.

e.g.

```
Switch(config)# show vlan pvid
   Port    | PVID
-----------+-------
   Port1 | 1
   Port2 | 1
   Port3 | 1
   Port4 | 1
   Port5 | 1
   Port6 | 1
   Port7 | 1
   Port8 | 1
   Port9 | 1
  Port10 | 1
    Trk1 | 1
```

vlan filter

Description:

Set ingress filter rules.

Syntax:

vlan filter <enable | disable> <enable | disable> LIST

Parameters:

<**enable** | **disable**> specifies the non-members packet will be forwarded or not. If set enable, forward only packets with VID matching this port's configured VID.

<**enable** | **disable**> specifies the untagged frame will be dropped or not. If set enable, drop untagged frame.

show vlan filter

Description:

Show VLAN filter setting.

Syntax:

show vlan filter [LIST]

Parameters:

[LIST] specifies the ports to be showed. If not entered, all ports' filter rules will be showed.

```
Switch(config)# show vlan filter
   Port    | Rule 1    | Rule 2
  Filter   (nonmbr)    (untag)
-----------+-----------+---------
   Port1 | Drop       | Forward
   Port2 | Drop       | Forward
   Port3 | Drop       | Forward
   Port4 | Drop       | Forward
   Port5 | Drop       | Forward
   Port6 | Drop       | Forward
   Port7 | Drop       | Forward
   Port8 | Drop       | Forward
   Port9 | Drop       | Forward
  Port10 | Drop       | Forward
    Trk1 | Drop       | Forward
```

6.6 Misc Configuration

[no] mac-age-time

Description:

Disable MAC address age-out or set MAC address age-out time.

Syntax:

no mac-age-time Enable or disable MAC address age-out.

mac-age-time <6..1572858>

Parameters:

<6..1572858> specifies the MAC address age-out time. The MAC age-out time must be divisible by 6. Type the number of seconds that an inactive MAC address remains in the switch's address table.

show mac-age-time

Description:

Show MAC address age-out time

broadcast

Description:

Set broadcast storm filter mode to off, 1/2, 1/4, 1/8, 1/16

Syntax:

broadcast mode <**off | 1/2 | 1/4 | 1/8 | 1/16**>

broadcast select

Description:

Select the Broadcast storm filter packet type:

- ***Unicast/Multicast***: Flood unicast/multicast filter
- ***Control Packets***: Control packets filter
- ***IP multicast***: IP multicast packets filter
- ***Broadcast Packets***: Broadcast Packets filter

Syntax:

broadcast select <unicast/multicast | control packet | ip-multicast | broadcast>

Collision-Retry

Description:

Collision-Retry setting

Syntax:

Collision-Retry <off | 16 | 32 | 48>

Parameters:

<16 | 32 | 48> – In Half-Duplex, collision-retry maximum is 16 (or 32, 48) times and packet will be dropped if collisions still happen

off – In Half-Duplex, if happen collision will retry forever (Default).

6.7 Administration Configuration

6.7.1 Changing Username and Password

hostname

Description:

Set switch name.

Syntax:

hostname <*name-str*>

Parameters:

<*name-str*> specifies the switch name. If you would like to have spaces within the name, use quotes ("") around the name.

no hostname

Reset the switch name to factory default setting.

[no] password

Description:

Set or remove username and password for manager or operator.

Syntax:

[no] **password** <manager | operator | all>

Parameters:

The manager username and password are also used by the web UI.

6.7.2 IP Configuration

User can configure the IP setting and fill in the new value.

ip address

Description:

Set IP address and subnet mask.

Syntax:

ip address <*ip-addr*> <*ip-mask*>

ip default-gateway

Description:

Set the default gateway IP address.

Syntax:

ip default-gateway <*ip-addr*>

show ip

Description:

Show IP address, subnet mask, and the default gateway.

show info

Description:

Show basic information, including system info, MAC address and versions.

```
Switch(config)# show info
Model name: VC-820M
Description: 8-Port 10/100Mbps + 2G TP/SFP    Combo Managed Switch
MAC address: 00:30:4F:44:55:66
Firmware version: 1.08
CLI version: 1.07
802.1x: disabled
GVRP: disabled
LLDP: disabled
IGMP: enabled
LACP: enabled
```

dhcp

Description:

Set switch as dhcp client, it can get IP from dhcp server.

If you set this command, the switch will reboot.

show dhcp

Description:

show dhcp enable/disable.

6.7.3 Reboot switch

boot

Description:

Reboot (warm-start) the switch.

6.7.4 Reset to Default

erase startup-config

Description:

Reset configurations to default factory settings at next boot time.

6.7.5 TFTP Update Firmware

copy tftp firmware

Description:

Download firmware from TFTP server.

Syntax:

copy tftp firmware <*ip-addr*> <*remote-file*>

Parameters:

<*ip-addr*> specifies the IP address of the TFTP server.

<*remote-file*> specifies the file to be downloaded from the TFTP server.

6.7.6 Restore Configure File

copy tftp <running-config | flash>

Description:

Retrieve configuration from the TFTP server. If the remote file is the text file of CLI commands, use the keyword running-config.

If the remote file is the configuration flash image of the switch instead, use the keyword flash.

Syntax:

copy tftp <**running-config** | **flash**> <*ip-addr*> <*remote-file*>

Parameters:

<*ip-addr*> specifies the IP address of the TFTP server.

<*remote-file*> specifies the file to be downloaded from the TFTP server.

6.7.7 Backup Configure File

copy <running-config | flash> tftp

Description:

Send configuration to the TFTP server. If you want to save the configuration in a text file of CLI commands, use the keywordrunning-config. If you want to save the configuration flash image instead, use the keyword flash.

Syntax:

copy <**running-config** | **flash**> **tftp** <*ip-addr*> <*remote-file*>

Parameters:

<*ip-addr*> specifies the IP address of the TFTP server.

6.8 MAC limit

MAC limit allows users to set a maximum number of MAC addresses to be stored in the MAC address table. The MAC addresses chosen to be stored in MAC address table is the result of first-come-first-save policy. Once a MAC address is stored in the MAC address table, it stays in until it is aged out. When an "opening" is available, the switch stored the first new MAC address it sees in that opening. All packets from MAC addresses not in the MAC address table should be blocked.

User can configure the MAC limit setting and fill in the new value.

mac-limit

Description:

Enable MAC limit.

no mac-limit

Description:

Disable MAC limit.

mac-limit

Description:

Set port MAC limit value, 0 to turn off MAC limit of port.

Syntax:

Mac-limit <port-list> <1-64>

show mac-limit

Description:

Show MAC limit information, including MAC limit enable/disable, per-port MAC limit setting.

6.9 Port Mirroring Configuration

Port monitoring is a feature to redirect the traffic occurred on every port to a designated monitoring port on the switch. With this feature, the network administrator can monitor and analyze the traffic on the entire LAN segment. In the Managed Switch, you can specify one port to be the monitored ports and any single port to be the monitoring port. You also can specify the direction of the traffic that you want to monitor. After properly configured, packets with the specified direction from the monitored ports are forwarded to the monitoring port.

The default Port Monitoring setting is disabled.

mirror-port

Description:

Set port monitoring information. (RX only|TX only|both RX and TX)

Syntax:

mirror-port <**rx** | **tx** | **both**> <*port-id*> <*port-list*>

Parameters:

rx specifies monitoring rx only.

tx specifies monitoring tx only.

both specifies monitoring both rx and tx.

<*port-id*> specifies the analysis port ID. This port receives traffic from all monitored ports.

<*port-list*> specifies the monitored port list.

show mirror-port

Description:

Show port monitoring information

6.10 Quality of Service

There are four transmission queues with different priorities in the Managed Switch: **Highest**, SecHigh, **SecLow** and **Lowest**. The Managed Switch will take packets from the four queues according to its QoS mode setting. If the QoS mode was set to "Disable", the Managed Switch will not perform QoS on its switched network. If the QoS mode was set to "High Empty Then Low", the Managed Switch will never exhaust packets from a queue until the queues with higher priorities are empty. If the QoS mode was set to "**weight ratio**", the Managed Switch will exhaust packets from the queues according to the ratio. The default value of QoS mode is "**weight 8:4:2:1**." That means the switch will first exhaust 8 packets from the queue with highest priority, and then exhaust 4 packets from the queue with second high priority, and so on.

When the switch received a packet, the switch has to decide which queue to put the received packet into. In the Managed Switch, it will put received packets into queues according to the settings of "802.1p Priority" and "Static Port Ingress Priority." When the received packet is an 802.1p tagged packet, the switch will put the packet into a queue according to the 802.1p Priority setting.

Otherwise, the switch will put the packet into a queue according the setting of Static Port Ingress Priority.

- **802.1p Priority**: the 802.1p packet has a priority tag in its packet header. The range of the priority is 7~0. The Managed Switch can specify the mapping between 802.1p priority and the four transmission queues. In the default setting, the packets with 802.1p priority 0~1 are put into the queue with lowest priority, the packets with 802.1p priority 2~3 are put into queue with second low priority, and so on.

- **Static Port Ingress Priority**: each port is assigned with one priority 7~0. The priority of the packet received from one port is set to the same priority of the receiving port. When the priority of the received packet was determined, the packet is treated as an 802.1p packet with that priority and will be put into a queue according to the 802.1p Priority setting.

6.10.1 QoS Configuration

QoS mode:

- **First Come First Service**: The sequence of packets sent is depending on arrive orders.
- **All High before Low**: The high priority packets sent before low priority packets.
- **WRR**: Weighted Round Robin. Select the preference given to packets in the switch's high-priority queue. These options represent the number of higher priority packets sent before one lower priority packet is sent. For example, 8 Highest：4 second-high means that the switch sends 8 highest-priority packets before sending 4 second-high priority packets.
- **Qos level**: 0~7 priority level can map to highest, second-high, second-low, lowest queue.

Commands:

qos priority

Description:

Set 802.1p priority.

Syntax:

qos priority <first-come-first-service | all-high-before-low |weighted-round-robin>

Parameters:

[<*highest* >][<sec-*highweight*>][<sec *low -weight*>] [<*lowest-weight*>]

e.g. qos priority weighted-round-robin 8,4,2,1

qos level

Description:

Set priority levels to highest, second-high, second-low and lowest.

Syntax:

qos level < highest | second-high | second-low | lowest > <*level-list*>

Parameters:

<*level-list*> specifies the priority levels to be high or low.

Level must be between 0 and 7.

e.g. qos level highest 7

e.g. qos level lowest 0

show qos

Description:

Show QoS configurations, including802.1p priority, priority level.

e.g.

```
Switch(config)# show qos
QoS configurations:
QoS mode: weighted round robin
Highest weight: 8
Second High weight: 4
Second Low weight: 2
Lowest weight: 1
802.1p priority[0-7]:
Lowest    Lowest    SecLow    SecLow    SecHigh    SecHigh    Highest    Highest
```

6.10.2 Per Port Priority

port priority

Description:

Set port priority.

Syntax:

port priority <disable | [0-7]> [<*port-list*>]

Parameters:

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

e.g. port priority disable 1-5

6.11 MAC Address Configuration

clear mac-address-table

Description:

Clear all dynamic MAC address table entries.

mac-address-table static

Description:

Set static unicast or multicast MAC address. If multicast MAC address (address beginning with 01:00:5E) is supplied, the last parameter must be *port-list*. Otherwise, it must be *port-id*.

Syntax:

mac-address-table static <*mac-addr*> <*vlan-id*> <*port-id* | *port-list*>

no mac-address-table static mac-addr

Description:

Delete static unicast or multicast MAC address table entries.

Syntax:

no mac-address-table static *mac-addr* <*vlan-id*>

show mac-address-table

Description:

Display MAC address table entries.

```
Switch(config)# show mac-address-table
      MAC Address       | VLAN |    Type      | Source
-------------------------------+--------+--------------+------------------------------
 00:08:B6:00:06:90     |       1 |    Dynamic |9
 00:40:63:00:65:30     |       1 |    Dynamic | Trk1
 00:03:63:F7:80:7F     |       1 |    Dynamic | 9
```

show mac-address table static

Description:

Display static MAC address table entries.

show mac-address-table multicast

Description:

Display multicast related MAC address table.

smac-address-table static

Description:

Set static unicast or multicast MAC address in secondary MAC address table. If multicast MAC address (address beginning with 01:00:5E) is supplied, the last parameter must be *port-list*. Otherwise, it must be *port-id*.

Syntax:

smac-address-table static <*mac-addr*> <*vlan-id*> <*port-id* | *port-list*>

show smac-address-table

Description:

Display secondary MAC address table entries.

show smac-address-table multicast

Description:

Display multicast related secondary MAC address table.

[no] filter

Description:

Set MAC address filter. The packets will be filtered if both of the destination MAC address and the VLAN tag matches the filter entry. If the packet does not have a VLAN tag, then it matches an entry with VLAN ID 1.

Syntax:

[no] filter <*mac-addr*> <*vlan-id*>

show filter

Description:

Display filter MAC address table.

6.12 STP/MSTP Commands

[no] spanning-tree

Description:

Enable or disable spanning-tree.

spanning-tree forward-delay

Description:

Set spanning tree forward delay of CIST, in seconds.

Syntax:

spanning-tree forward-delay <*4-30*>

Parameters:

<*4-30*> specifies the forward delay, in seconds. Default value is 15.

The parameters must enforce the following relationships:

2*(hello-time + 1) <= maximum-age <= 2*(forward-delay - 1)

spanning-tree hello-time

Description:

Set spanning tree hello time of CIST, in seconds.

Syntax:

spanning-tree hello-time <*1-10*>

Parameters:

<*1-10*> specifies the hello time, in seconds. Default value is 2.

The parameters must enforce the following relationships:

2*(hello-time + 1) <= maximum-age <= 2*(forward-delay - 1)

spanning-tree maximum-age

Description:

Set spanning tree maximum age of CIST, in seconds.

Syntax:

spanning-tree maximum-age <*6-40*>

Parameters:

<*6-40*> specifies the maximum age, in seconds. Default value is 20.

The parameters must enforce the following relationships:

2*(hello-time + 1) <= maximum-age <= 2*(forward-delay - 1)

spanning-tree priority

Description:

Set spanning tree bridge priority of CIST and all MSTIs.

Syntax:

spanning-tree priority <*0-61440*>

Parameters:

<*0-61440*> specifies the bridge priority. The value must be in steps of 4096. Default value is 32768.

show spanning-tree

Description:

Show spanning-tree information.

show spanning-tree port

Description:

Show spanning tree per port information.

Syntax:

show spanning-tree port [<*port-list*>]

Parameters:

<*port-list*> specifies the port to be shown. Null means all ports.

spanning-tree protocol-version

Description:

Change spanning tree protocol version of CIST.

Syntax:

spanning-tree protocol-version <stp | mstp>

Parameters:

stp specifies the original spanning tree protocol **(STP,802.1d)**.

mstp specifies the multiple spanning tree protocol **(MSTP,802.1s)**

spanning-tree max-hops

Description:

Set spanning tree bridge maximum hops of CIST and all MSTIs.

Syntax:

spanning-tree max-hops <1-40>

Parameters:

<*1-40*> specifies the bridge maximum hops. Default value is **20**.

spanning-tree name

Description:

Set spanning tree bridge name of CIST.

Syntax:

spanning-tree name [<name-string>]

Parameters:

<*name-string*> specifies the bridge name. Default name is null.

spanning-tree revision

Description:

Set spanning tree bridge revision of CIST.

Syntax:

spanning-tree revision <0-65535>

Parameters:

<0-65535> specifies the bridge revision. Default value is 0.

spanning-tree port path-cost

Description:

Set spanning tree port path cost of CIST.

Syntax:

spanning-tree port path-cost <*1-200000000*> [<*port-list*>]

Parameters:

<***1-200000000***> specifies port path cost.

<*port-list*> specifies the ports to be set. Null means all ports.

spanning-tree port priority

Description:

Set spanning tree port priority of CIST.

Syntax:

spanning-tree port priority <*0-240*> [<*port-list*>]

Parameters:

<***0-240***> specifies the port priority. The value must be in steps of 16.

<*port-list*> specifies the ports to be set. Null means all ports.

[no] spanning-tree port mcheck

Description:

Force the port of CIST to transmit MST BPDUs. No format means not force the port of CIST to transmit MST BPDUs.

Syntax:

[no] spanning-tree port mcheck [<*port-list*>]

Parameters:

<*port-list*> specifies the ports to be set. Null means all ports.

[no] spanning-tree port edge-port

Description:

Set the port of CIST to be edge connection. No format means set the port of CIST to be non-edge connection.

Syntax:

[no] spanning-tree port edge-port [<*port-list*>]

Parameters:

<*port-list*> specifies the ports to be set. Null means all ports.

[no] spanning-tree port non-stp

Description:

Disable or enable spanning tree protocol on the CIST port.

Syntax:

[no] spanning-tree port non-stp [<*port-list*>]

Parameters:

<*port-list*> specifies the ports to be set. Null means all ports.

spanning-tree port point-to-point-mac

Description:

Set the port of CIST to be point to point connection.

Syntax:

spanning-tree port point-to-point-mac <auto | true | false> [<*port-list*>]

Parameters:

auto specifies point to point link auto connection.

true specifies point to point link true.

false specifies point to point link false.

<port-list> specifies the ports to be set. Null means all ports.

spanning-tree mst

Description:

Set spanning tree bridge priority of MSTI.

Syntax:

spanning-tree mst <0-15> priority <0-61440>

Parameters:

<*0-15*> specifies the MSTI instance ID.

<*0-61440*> specifies the MSTI bridge priority. The value must be in steps of 4096. Default value is 32768.

spanning-tree mst <0-15> vlan [<vlan-list>]

Description:

Set MSTI to map VLAN list.

Syntax:

spanning-tree mst <0-15> vlan [<vlan-list>]

Parameters:

<**0-15**> specifies the MSTI instance ID.

<vlan-list> specifies the mapped VLAN list. Null means all VLANs.

spanning-tree mst <0-15> port path-cost <1-200000000> [<port-list>]

Description:

Set spanning tree port path cost of MSTI.

Syntax:

spanning-tree mst <0-15> port path-cost <1-200000000> [<port-list>]

Parameters:

<1-200000000> specifies port path cost.

<port-list> specifies the ports to be set. Null means all ports.

spanning-tree mst <0-15> port priority <0-240> [<port-list>]

Description:

Set spanning tree port priority of MSTI.

Syntax:

spanning-tree mst <0-15> port priority <0-240> [<port-list>]

Parameters:

<**0-240**> specifies the port priority. The value must be in steps of 16.

<port-list> specifies the ports to be set. Null means all ports.

no spanning-tree mst

Description:

Delete the specific MSTI.

Syntax:

no spanning-tree mst <0-15>

Parameters:

<0-15> specifies the MSTI instance ID.

show spanning-tree

Description:

Show spanning-tree information of CIST.

show spanning-tree port

Description:

Show spanning tree port information of CIST.

Syntax:

show spanning-tree port [<*port-list*>]

Parameters:

<*port-list*> specifies the port to be shown. Null means all ports.

show spanning-tree mst configuration

Description:

Show MST instance map.

Syntax:

show spanning-tree mst configuration

show spanning-tree mst <0-15>

Description:

Show MST instance information.

Syntax:

show spanning-tree mst <0-15>

Parameters:

<0-15> specifies the MSTI instance ID.

show spanning-tree mst <0-15> port <1-10>

Description:

Show specific port information of MST instance.

Syntax:

show spanning-tree mst <0-15> port <1-10>

Parameters:

<0-15> specifies the MSTI instance ID.

<1-10> specifies port number.

show vlan spanning-tree

Description:

Show per VLAN per port spanning tree status.

Syntax:

show vlan spanning-tree

6.13 SNMP

Any Network Management running the simple Network Management Protocol (SNMP) can be management the switch.

6.13.1 System Options

[no] snmp

Description:

Enable or disable SNMP.

show snmp status

Description:

Show the enable or disable status of SNMP.

snmp system-name

Description:

Set agent system name string.

Syntax:

snmp system-name <*name-str*>

Parameters:

<*name-str*> specifies the system name string.

e.g. snmp system-name SWITCH

snmp system-location

Description:

Set agent location string.

Syntax:

snmp system-location <*location-str*>

Parameters:

<location-str> specifies the location string.

e.g. snmp system-location office

snmp system-contact

Description:

Set agent system contact string.

Syntax:

snmp system-contact <*contact-str*>

Parameters:

<*contact-str*> specifies the contact string.

e.g. snmp system-contact abc@sina.com

show snmp system

Description:

Show SNMP system information.

6.13.2 Community Strings

snmp community

Description:

Set SNMP community string.

Syntax:

snmp community <read-sysinfo-only | read-all-only | read-write-all><community-str>

Parameters:

<*community-str*> specifies the community string.

e.g. snmp community read-all-only public

no snmp community

Description:

Delete SNMP community string.

Syntax:

no snmp community <*community-str*>

Parameters:

<*community-str*> specifies the community string.

e.g. no snmp community public

show snmp community

Description:

Show SNMP community strings.

6.13.3 Trap Managers

snmp trap

Description:

Set SNMP trap receiver IP address, community string, and port number.

Syntax:

snmp trap <*ip-addr*> [<*community-str*>] [<1..65535>]

Parameters:

<*ip-addr*> specifies the IP address.

<*community-str*> specifies the community string.

<1..65535> specifies the trap receiver port number. Default value is 162 if not specified.

e.g. snmp trap 192.168.200.1 public

no snmp trap

Description:

Remove trap receiver IP address and port number.

Syntax:

no snmp trap <*ip-addr*> [<1..65535>]

Parameters:

<*ip-addr*> specifies the IP address.

<1..65535> specifies the trap receiver port number.

e.g. no snmp trap 192.168.200.1

show snmp trap

Description:

Show all trap receivers.

6.14 IGMP

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite.

[no] igmp

Description:

Enable/disable IGMP snooping.

Syntax:

[**no**] **igmp**

[no] igmp fastleave

Description:

Enable/disable IGMP snooping fast leave. If enable, switch will fast delete member who send leave report,

else wait one sec.

Syntax:

[**no**] **igmp fastleave**

[no] igmp querier

Description:

Enable/disable IGMP snooping querier.

Syntax:

[**no**] **igmp querier**

[no] igmp CrossVLAN

Description:

Enable/disable IGMP snooping CrossVLAN

Syntax:

[**no**] **igmp CrossVLAN**

show igmp

Description:

Show IGMP snooping information.

Syntax:

show igmp <**status** | **router** | **groups** | **table**>

Parameters:

status specifies IGMP snooping status and statistics information.

router specifies IGMP snooping router's IP address.

groups specifies IGMP snooping multicast group list.

table specifies IGMP snooping IP multicast table entries.

igmp clear_statistics

Description:

Clear IGMP snooping statistics counters.

6.15 802.1x Protocol

[no] dot1x

Description:

Enable or disable 802.1x.

Syntax:

[**no**] **dot1x**

radius-server host

Description:

Set radius server IP, port number, and accounting port number.

Syntax:

radius-server host <*ip-addr*> <1024..65535> <1024..65535>

Parameters:

<*ip-addr*> specifies server's IP address.

The first <1024..65535> specifies the server port number.

The second <1024..65535> specifies the accounting port number.

radius-server key

Description:

Set 802.1x shared key.

Syntax:

radius-server key <*key-str*>

Parameters:

<*key-str*> specifies shared key string.

radius-server nas

Description:

Set 802.1x NAS identifier.

Syntax:

radius-server nas <*id-str*>

Parameters:

<*id-str*> specifies NAS identifier string.

show radius-server

Description:

Show radius server information, including radius server IP, port number, accounting port number, shared key, NAS identifier,

dot1x timeout quiet-period

Description:

Set 802.1x quiet period. (default: 60 seconds)

Syntax:

dot1x timeout quiet-period <10-65535>

Parameters:

<10-65535> specifies the quiet period, in seconds.

dot1x timeout tx-period

Description:

Set 802.1x Tx period. (default: 15 seconds).

Syntax:

dot1x timeout tx-period <10-65535>

Parameters:

<10-65535> specifies the Tx period, in seconds.

dot1x timeout supplicant

Description:

Set 802.1x supplicant timeout (default: 30 seconds)

Syntax:

dot1x timeout supplicant <10-300>

Parameters:

<10-300> specifies the supplicant timeout, in seconds.

dot1x timeout radius-server

Description:

Set radius server timeout (default: 30 seconds).

Syntax:

dot1x timeout radius-server <10-300>

Parameters:

<10-300> specifies the radius server timeout, in seconds.

dot1x max-req

Description:

Set 802.1x maximum request retries (default: 2 times).

Syntax:

dot1x max-req <1-10>

Parameters:

<1-10> specifies the maximum request retries.

dot1x timeout re-authperiod

Description:

Set 802.1x re-auth period (default: 3600 seconds).

Syntax:

dot1x timeout re-authperiod <30-65535>

Parameters:

<30-65535> specifies the re-auth period, in seconds.

show dot1x

Description:

Show 802.1x information, quiet period, Tx period, supplicant timeout, server timeout, maximum requests, and re-auth period.

dot1x port

Description:

Set 802.1x per port information.

Syntax:

dot1x port <**fu** | **fa** | **au** | **no**> <*port-list*>

Parameters:

fu specifies forced unauthorized.

fa specifies forced authorized.

au specifies authorization.

no specifies disable authorization.

<*port-list*> specifies the ports to be set.

show dot1x port

Description:

Show 802.1x per port information.

Syntax:

show dot1x port <*port-list*>

Parameters:

<*port-list*> specifies the ports to be set.

6.16 Access Control List

Packets forwarded or dropped by ACL rules include IPv4 or non-IPv4. The Managed Switch can be used to block packets by maintaining a table of packet fragments indexed by source and destination IP address, protocol, and so on

6.16.1 IPv4 ACL commands

no acl

Description:

Delete ACL group.

Syntax:

no acl <1-220>

Parameters:

<1-220> specifies the group ID.

e.g. no acl 1

no acl count

Description:

Reset the ACL group count.

Syntax:

no acl count <Group ID>

Parameters:

Group ID: <1-220> specifies the group ID.

show acl

Description:

Show ACL group information.

Syntax:

show acl [<1-220>]

Parameters:

<1-220> specifies the group ID, null means all valid groups.

e.g.

```
Switch(config)# show acl 1
Group Id : 1
-------------------------------
Action : Permit
Rules:
Vlan ID : Any
IP Fragement : Uncheck
Src IP Address : Any
Dst IP Address : Any
L4 Protocol : Any
```

```
Port ID : Any
Hit Octet Count : 165074
Hit Packet count : 472
```

acl (add|edit) <1-220> (permit|deny) <0-4094> ipv4 <0-255>

Description:

Add ACL group for IPv4.

Syntax:

acl add <1-220> (permit|deny) <0-4094> ipv4 <0-255> A.B.C.D A.B.C.D A.B.C.D A.B.C.D (check|unCheck) <0-65535> <0-10>

Parameters:

<1-220> specifies the group ID.

(permit|deny) specifies the action. permit: permit packet cross switch; deny: drop packet.

<0-4094> specifies the VLAN ID. 0 means don't care.

<0-255> specifies the IP protocol. 0 means don't care.

A.B.C.D specifies the Source IP address. 0.0.0.0 means don't care.

A.B.C.D specifies the Mask. 0.0.0.0 means don't care, 255.255.255.255 means compare all.

A.B.C.D specifies the Destination IP Address. 0.0.0.0 means don't care.

A.B.C.D specifies the Mask. 0.0.0.0 means don't care, 255.255.255.255 means compare all.

(check|unCheck) specifies the IP Fragment. check: Check IP fragment field; unCheck: Not check IP fragment field.

<0-65535> specifies the Destination port number if TCP or UDP. 0 means don't care.

<0-10> specifies the Port ID. 0 means don't care.

e.g.

```
Switch(config)# acl add 1 deny 1 ipv4 0 192.168.1.1 255.255.255.255 0.0.0.0 0.0.0.0 unCheck 0 0
```

This ACL rule will drop all packet from IP is 192.168.1.1 with VLAN ID=1 and IPv4.

acl add <1-220> (qosvoip) <0-4094>

Description:

Add ACL group for IPv4.

Syntax:

acl add <1-220> (qosvoip) <0-4094> <0-7> <0-1F> <0-1F> <0-FF> <0-FF> <0-FFFF> <0-FFFF> <0-FFFF> <0-FFFF>

Parameters:

<1-220> specifies the group ID.

(qosvoip) specifies the action, do qos voip packet adjustment.

<0-4094> specifies the VLAN ID. 0 means don't care.

<0-1F> specifies the port ID value.

<0-1F> specifies the port ID mask.

<0-FF> specifies the protocol value.

<0-FF> specifies the protocol mask.

<0-FFFF> specifies the source port value.

<0-FFFF> specifies the source port mask.

<0-FFFF> specifies the destination port value.

<0-FFFF> specifies the destination mask.

e.g. acl add 1 qosvoip 1 7 1 1 0 0 0 0 0 0

6.16.2 Non-IPv4 ACL Commands

no acl <1-220> and **show acl** <1-220> commands are same as IPv4 ACL commands.

acl add <1-220> (permit|deny) <0-4094> nonipv4 <0-65535>

Description:

Add ACL group for non-IPv4.

Syntax:

acl add <1-220> (permit|deny) <0-4094> nonipv4 <0-65535>

Parameters:

<1-220> specifies the group ID.

(permit|deny) specifies the action. permit: permit packet cross switch; deny: drop packet.

<0-4094> specifies the VLAN ID. 0 means don't care.

<0-65535> specifies the Ether Type. 0 means don't care.

e.g. acl add 1 deny 0 nonipv4 2054. This ACL rule will drop all packets for ether type is 0x0806 and non-IPv4.

6.17 Binding

Let device that has specific IP address and MAC address use network. We can set specific IP address, MAC address, VLAN ID and port ID to bind, and device can cross switch if all conditions match.

6.17.1 SIP/SMAC binding commands

bind

Description:

Enable binding function.

no bind

Description:

Disable binding function.

Syntax:

no bind <1-220>

Parameters:

<1-220> specifies the group ID.

e.g. no bind 1

no bind

Description:

Delete Binding group.

Syntax:

no bind <1-220>

Parameters:

<1-220> specifies the group ID.

e.g. no bind 1

show bind

Description:

Show Binding group information.

Syntax:

show bind [<1-220>]

Parameters:

<1-220> specifies the group ID, null means all valid groups.

e.g. show bind 1

bind add

Description:

Add Binding group.

Syntax:

bind add <1-220> A:B:C:D:E:F <0-4094> A.B.C.D <1-10>

Parameters:

<1-220> specifies the group ID.

A.B.C.D specifies the MAC address.

<0-4094> specifies the VLAN ID. 0 means don't care.

A.B.C.D specifies the Source IP address. 0.0.0.0 means don't care.

A.B.C.D specifies the IP Address.

<1-10> specifies the Port ID.

e.g.

```
Switch(config)# bind add 1 00:11:22:33:44:55 0 192.168.1.1 1
```

This Binding rule will permit all packet cross switch from device's IP is 192.168.1.1 and MAC is 00:11:22:33:44:55 and this device connects to switch port ID=1.

6.18 DHCP Configuration

[no] dhcp-option82

Description:

Enable/disable dhcp-option82 function.

Syntax:

[no] dhcp-option82

dhcp-option82

Description:

Enable or disable dhcp-option82 port.

Syntax:

dhcp-option82 <**enable** | **disable**> [<*port-list*>]

Parameters:

The <**enable** | **disable**> enables or disables dhcp-option82 port.

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

[no] dhcp-relay

Description:

Enable/disable dhcp-relay function.

Syntax:

[no] dhcp-relay

dhcp-relay

Description:

Enable or disable dhcp-option82 port.

Syntax:

dhcp-option82 <**enable** | **disable**> [<*port-list*>] [<*IP address*>]

Parameters:

The <**enable** | **disable**> enables or disables dhcp-relay port.

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

<IP address> specifies the DHCP server IP address.

dhcp-router

Description:

Assign a port to connect a DHCP server in a domain.

Syntax:

dhcp-router [<*port-list*>]

Parameters:

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

6.19 VDSL2 Commands

interface	**Commands for VDSL interfaces**
profiles	**Commands for VDSL profiles**

6.19.1 VDSL2 Interface Commands

Interface xdsl

Description:

Commands for xdsl interfaces

Syntax:

Interface xdsl [show | set]

interface xdsl show oid

Description:

Show VDSL Logic MIB entry

Syntax:

interface xdsl show oid <portid> <oid>

Parameters:

<1-8> or <1-24> port ID

interface xdsl show roid

Description:

Show VDSL Real MIB entry

Syntax:

interface xdsl show roid <portid> <oid>

Parameters:

<1-8> or <1-24> port ID

interface xdsl show status

Description:

Show line status

Syntax:

interface xdsl show status <port ID>

Parameters:

<1-8> or <1-24> port ID

Switch(config)# **interface xdsl show status 1**

Status (Basic) of Line 1: Showtime

	Value	Description
Actual Data Rate	100992	(US) Kb/s
Actual Data Rate	100992	(DS) Kb/s
SNR Margin	79	(US) 0.1dB
SNR Margin	251	(DS) 0.1dB
Firmware Version	10201	

Status (Advance) of Line 1:

	Upstream	Downstream	
Actual delay	5	5	ms
Actual INP	20	20	0.1 symbols
15M CV	0	0	
1Day CV	0	0	
Total CV	0	0	
15M FEC	0	0	
1Day FEC	728	0	
Total FEC	728	0	
Previous Data Rate	0	100992	Kbps
Attainable Rate	106023	169169	Kbps
Electrical Length	11	11	0.1dB
SNR Margin	NA	--	(US0,--) 0.1 dB
SNR Margin	80	251	(US1,DS1) 0.1 dB
SNR Margin	80	250	(US2,DS2) 0.1 dB
SNR Margin	78	251	(US3,DS3) 0.1 dB
SNR Margin	NA	NA	(US4,DS4) 0.1 dB
15M Elapsed time	488	488	secs
15M FECS	0	0	
15M ES	0	0	
15M SES	0	0	
15M LOSS	0	0	
15M UAS	0	0	
1Day Elapsed time	69788	69788	secs
1Day FECS	7	5	
1Day ES	0	5	
1Day SES	0	0	
1Day LOSS	0	0	
1Day UAS	0	0	
Total FECS	0	0	
Total ES	0	0	
Total SES	0	0	
Total LOSS	0	0	
Total UAS	0	0	

Switch(config)#

interface xdsl show pm_line_curr

Description:

Show current counters of xdsl lines

Syntax:

interface xdsl show pm_line_curr <portid>

Parameters:

<1-8> or <1-24> port ID

interface xdsl show pm_ch_curr

Description:

Show current counters of xdsl channels

Synta x:

interface xdsl show pm_ch_curr <portid>

Parameters:

<1-8> or <1-24> port ID

interface xdsl show invent

Description:

Show inventory of xdsl lines

Syntax:

interface xdsl show invent <portid>

Parameters:

<1-8> or <1-24> port ID

interface xdsl show threshold

Description:

Show threshold of xdsl lines

Syntax:

interface xdsl show threshold <portid>

Parameters:

<1-8> or <1-24> port ID

interface xdsl show table

Description:

Show mib tables of xdsl line

Syntax:

interface xdsl show table line <portid>

Parameters:

<1-8> or <1-24> port ID

6.19.2 VDSL2 Profile Commands

profile xdsl-line

Description:

Commands for xdsl-line

Syntax:

profile xdsl-line new <profile_name>

profile xdsl-line del <profile_name>

profile xdsl-line show

profile xdsl-line save

profile xdsl-line init

profile xdsl-line

profile xdsl-line new

Description:

Create a new xdsl profile

Syntax:

profile xdsl-line new <profile_name>

profile xdsl-line del

Description:

Delete xdsl profile

Syntax:

profile xdsl-line del <profile_name>

profile xdsl-line show

Description:

Show all profile names or show detail information of a specified profile

Syntax:

profile xdsl-line show <profile> <profile_name>

profile xdsl-line show <profile>

profile xdsl-line show <sprofile>

profile xdsl-line show profile

Description:

Show exist profile name

Syntax:

profile xdsl-line show

```
Switch(config)# profiles xdsl-line show profile

Exist VDSL Config Profile
==========================
VDSL Config Profile Name: default
VDSL Config Profile Name: user1
VDSL Config Profile Name: user2
VDSL Config Profile Name: user3
VDSL Config Profile Name: user4
VDSL Config Profile Name: user5
VDSL Config Profile Name: user6
VDSL Config Profile Name: user7
VDSL Config Profile Name: user8
VDSL Config Profile Name: user9
VDSL Config Profile Name: user10
VDSL Config Profile Name: user11
VDSL Config Profile Name: user12
VDSL Config Profile Name: user13
VDSL Config Profile Name: user14
VDSL Config Profile Name: user15
VDSL Config Profile Name: user16
VDSL Config Profile Name: user17
VDSL Config Profile Name: user18
VDSL Config Profile Name: user19
VDSL Config Profile Name: user20
```

profile xdsl-line show sprofile

Description:

Show system support profile ID

Syntax:

profile xdsl-line show sprofile

```
Switch(config)# profiles xdsl-line show sprofile


Supported profile:
AnnexA_R_POTS_D-32_EU-32_30a
AnnexA_R_POTS_D-32_EU-32_17a
AnnexA_R_POTS_D-32_EU-32_12b
```

AnnexA_R_POTS_D-32_EU-32_12a
AnnexA_R_POTS_D-32_EU-32_8a
AnnexA_R_POTS_D-32_EU-32_8b
AnnexA_R_POTS_D-32_EU-32_8c
AnnexA_R_POTS_D-32_EU-32_8d
AnnexA_R_POTS_D-64_EU-64_30a_NUS0
AnnexA_R_POTS_D-64_EU-64_17a
AnnexB_B7-1_997-M1c-A-7
AnnexB_B7-2_997-M1x-M-8
AnnexB_B7-3_997-M1x-M
AnnexB_B7-4_997-M2x-M-8
AnnexB_B7-5_997-M2x-A
AnnexB_B7-6_997-M2x-M
AnnexB_B7-9_997E17-M2x-A
AnnexB_B7-10_997E30-M2x-NUS0
AnnexB_B8-1_998-M1x-A
AnnexB_B8-2_998-M1x-B
AnnexB_B8-4_998-M2x-A
AnnexB_B8-5_998-M2x-M
AnnexB_B8-6_998-M2x-B
AnnexB_B8-8_998E17-M2x-NUS0
AnnexB_B8-9_998E17-M2x-NUS0-M
AnnexB_B8-10_998ADE17-M2x-NUS0-M
AnnexB_B8-11_998ADE17-M2x-A
AnnexB_B8-12_998ADE17-M2x-B
AnnexB_B8-13_998E30-M2x-NUS0
AnnexB_B8-14_998E30-M2x-NUS0-M
AnnexB_B8-15_998ADE30-M2x-NUS0-M
AnnexB_B8-16_998ADE30-M2x-NUS0-A
AnnexC_POTS_25-138_b
AnnexC_POTS_25-276_b
AnnexC_TCM-ISDN

profile xdsl-line save

Description:

Save all profile configurations

Syntax:

profile xdsl-line save

profile xdsl-line init

Description:

Initialize profile from savefile

Syntax:

profile xdsl-line init

profile xdsl-line set

Description:

Set commands for xdsl profile

profile xdsl-line set dsl-bandplan

Description:

To enable a predefined set of PSD-mask, PSD-Level and sub carrier mask dependent on profile and bandplan selection for a VDSL config profile

Syntax:

profile xdsl-line set dsl-bandplan <profile_name> <value>

profile xdsl-line set fix-rate

Description:

Specify the profile to use fixed rate in bit/s

Syntax:

profile xdsl-line set fix-rate <profile_name> <value>

profile xdsl-line set margin-target-snr-ds

Description:

Signal Noise Ratio margin target downstream settings

Syntax:

profile xdsl-line set margin-target-snr-ds <profile_name> <value-dec>

Parameters:

<0-310>

profile xdsl-line set margin-target-snr-us

Description:

Signal Noise Ratio margin target upstream settings

Syntax:

profile xdsl-line set margin-target-snr-us <profile_name> <value-dec>

Parameters:

<0-310>

profile xdsl-line set margin-max-snr-ds

Description:

Signal Noise Ratio margin max downstream settings

Syntax:

profile xdsl-line set margin-max-snr-ds <profile_name> <value-dec>

Parameters:

<0-310>

profile xdsl-line set margin-max-snr-us

Description:

Signal Noise Ratio margin max upstream settings

Syntax:

profile xdsl-line set margin-max-snr-us <profile_name> <value-dec>

Parameters:

<0-310>

profile xdsl-line set margin-min-snr-ds

Description:

Signal Noise Ratio margin min downstream settings

Syntax:

profile xdsl-line set margin-min-snr-ds <profile_name> <value-dec>

Parameters:

<0-310>

profile xdsl-line set margin-min-snr-us

Description:

Signal Noise Ratio margin min upstream settings

Syntax:

profile xdsl-line set margin-min-snr-us <profile_name> <value-dec>

Parameters:

<0-310>

profile xdsl-line set rate-limit-max-ds-ch1

Description:

CH1 Maximum Data Rate on Downstream direction settings

Syntax:

profile xdsl-line set rate-limit-max-ds-ch1 <profile_name> <value-dec>

Parameters:

<0-200000> kbps

profile xdsl-line set rate-limit-max-us-ch1

Description:

CH1 Maximum Data Rate on Upstream direction settings

Syntax:

profile xdsl-line set rate-limit-max-us-ch1 <profile_name> <value-dec>

Parameters:

<0-200000> kbps

profile xdsl-line set rate-limit-max-ds-ch2

Description:

CH2 Maximum Data Rate on Downstream direction settings

Syntax:

profile xdsl-line set rate-limit-max-ds-ch2 <profile_name> <value-dec>

Parameters:

<0-200000> kbps

profile xdsl-line set rate-limit-max-us-ch2

Description:

CH2 Maximum Data Rate on Upstream direction settings

Syntax:

profile xdsl-line set rate-limit-max-us-ch2 <profile_name> <value-dec>

Parameters:

<0-200000> kbps

profile xdsl-line set rate-limit-min-ds-ch1

Description:

CH1 Minimum Data Rate on Downstream direction settings

Syntax:

profile xdsl-line set rate-limit-min-ds-ch1 <profile_name> <value-dec>

Parameters:

<0-200000> kbps

profile xdsl-line set rate-limit-min-us-ch1

Description:

CH1 Minimum Data Rate on Upstream direction settings

Syntax:

profile xdsl-line set rate-limit-min-us-ch1 <profile_name> <value-dec>

Parameters:

<0-200000> kbps

profile xdsl-line set rate-limit-min-ds-ch2

Description:

CH2 Minimum Data Rate on Downstream direction settings

Syntax:

profile xdsl-line set rate-limit-min-ds-ch2 <profile_name> <value-dec>

Parameters:

<0-200000> kbps

profile xdsl-line set rate-limit-min-us-ch2

Description:

CH2 Minimum Data Rate on Upstream direction settings

Syntax:

profile xdsl-line set rate-limit-min-us-ch2 <profile_name> <value-dec>

Parameters:

<0-200000> kbps

profile xdsl-line set max-delay-ds-ch1

Description:

CH1 Maximum Interleave Delay on Downstream direction settings

Syntax:

profile xdsl-line set max-delay-ds-ch1<profile_name> <value-dec>

Parameters:

<0-63> ms

profile xdsl-line set max-delay-us-ch1

Description:

CH1 Maximum Interleave Delay on Upstream direction settings

Syntax:

profile xdsl-line set max-delay-us-ch1 <profile_name> <value-dec>

Parameters:

<0-63> ms

profile xdsl-line set inp-min-prot-ds-ch1

Description:

CH1 Downstrem minimum impulse noise protection in 4.3125kHz(symbol) settings

Syntax:

profile xdsl-line set inp-min-prot-ds-ch1 <profile_name> <value-dec>

Parameters:

<1-18>

profile xdsl-line set inp-min-prot-us-ch1

Description:

CH1 Upstrem minimum impulse noise protection in 4.3125kHz(symbol) settings

Syntax:

profile xdsl-line set inp-min-prot-us-ch1 <profile_name> <value-dec>

Parameters:

<1-18>

profile xdsl-line set inp-min-prot8-ds-ch1

Description:

CH1 Downstrem minimum impulse noise protection in 8.625kHz settings

Syntax:

profile xdsl-line set inp-min-prot8-ds-ch1 <profile_name> <value-dec>

Parameters:

<1-17>

profile xdsl-line set inp-min-prot8-us-ch1

Description:

CH1 Upstrem minimum impulse noise protection in 8.625kHz settings

Syntax:

profile xdsl-line set inp-min-prot8-us-ch1 <profile_name> <value-dec>

Parameters:

<1-17>

profile xdsl-line set max-delay-ds-ch2

Description:

CH2 Maximum Interleave Delay on Downstream direction settings

Syntax:

profile xdsl-line set max-delay-ds-ch2 <profile_name> <value-dec>

Parameters:

<0-63> ms

profile xdsl-line set max-delay-us-ch2

Description:

CH2 Maximum Interleave Delay on Upstream direction settings

Syntax:

profile xdsl-line set max-delay-us-ch2 <profile_name> <value-dec>

Parameters:

<0-63> ms

profile xdsl-line set inp-min-prot-ds-ch2

Description:

CH2 Downstrem minimum impulse noise protection in 4.3125kHz(symbol) settings

Syntax:

profile xdsl-line set inp-min-prot-ds-ch2 <profile_name> <value-dec>

Parameters:

<1-18>

profile xdsl-line set inp-min-prot-us-ch2

Description:

CH2 Upstrem minimum impulse noise protection in 4.3125kHz(symbol) settings

Syntax:

profile xdsl-line set inp-min-prot-us-ch2 <profile_name> <value-dec>

Parameters:

<1-18>

profile xdsl-line set inp-min-prot8-ds-ch2

Description:

CH2 Downstrem minimum impulse noise protection in 8.625kHz settings

Syntax:

profile xdsl-line set inp-min-prot8-ds-ch2 <profile_name> <value-dec>

Parameters:

<1-17>

profile xdsl-line set inp-min-prot8-us-ch2

Description:

CH2 Upstrem minimum impulse noise protection in 8.625kHz settings

Syntax:

profile xdsl-line set inp-min-prot8-us-ch2 <profile_name> <value-dec>

Parameters:

<1-17>

7. SWITCH OPERATION

7.1 Address Table

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

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

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

7.5 Auto-Negotiation

The STP ports on the Switch have built-in "Auto-negotiation". This technology automatically sets the best possible

bandwidth when a connection is established with another network device (usually at Power On or Reset). This is done by detect the modes and speeds at the second of both device is connected and capable of, both 10BASE-T and 100BASE-TX devices can connect with the port in either Half- or Full-Duplex mode.

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

8. TROUBLESHOOTING

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 dedicated 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.

■ **IP address and password have been changed or forgotten**.

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** on the front panel for about **10 seconds.** After the device is rebooted, you can login the management Web interface within the same subnet of 192.168.0.xx.

APPENDIX A—RJ45 Pin Assignment

A.1 Switch's RJ45 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-

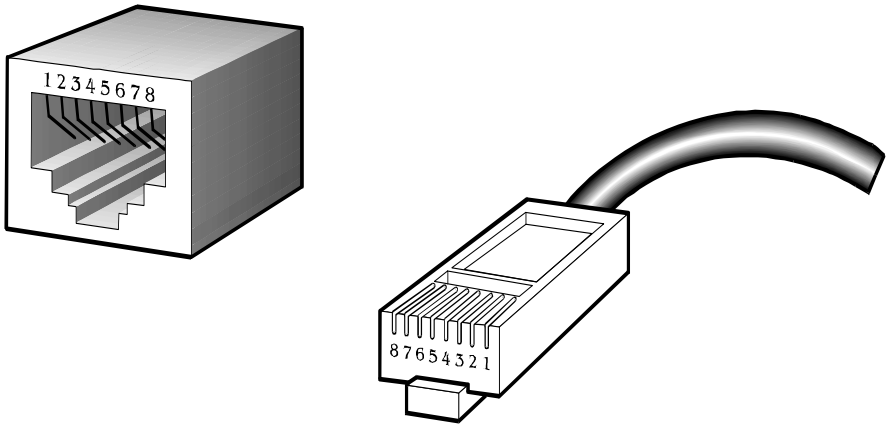
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

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

When connecting your 10/100Mbps Ethernet Switch to another switch, a bridge or a hub, a straight-through or crossover cable is necessary. Each port of the Switch supports auto-MDI/MDI-X detection. That means you can directly connect the Switch to any Ethernet devices without making a crossover cable. The following table and diagram show the standard RJ45 receptacle/connector and their pin assignments:

RJ45 Connector pin assignment		
Contact	MDI Media Dependent Interface	MDI-X Media Dependent Interface-Cross
1	Tx + (transmit)	Rx + (receive)
2	Tx - (transmit)	Rx - (receive)
3	Rx + (receive)	Tx + (transmit)
4, 5	Not used	
6	Rx - (receive)	Tx - (transmit)
7, 8	Not used	

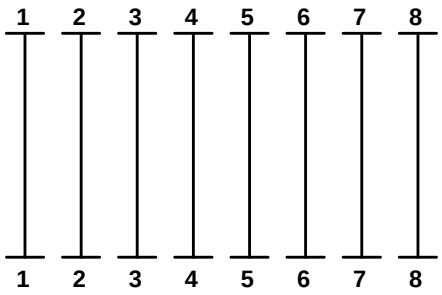
The standard cable, RJ45 pin assignment



The standard RJ45 receptacle/connector

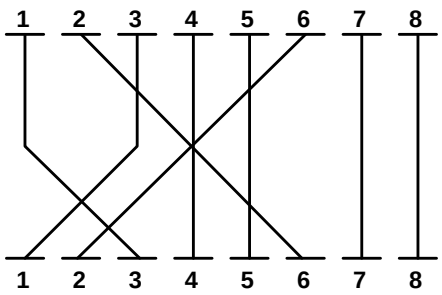
There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight-through cable and crossover cable connection:

Straight-through Cable



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

Crossover Cable



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

Figure A-1: Straight-through and Crossover Cable

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