VigorSwitch P2260

User’s Guide

Version: 1.0

Date: 2008/12/08

Copyright Information

Copyright Declarations

Trademarks

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows, Windows 95, 98, Me, NT, 2000, XP and Explorer are trademarks of Microsoft Corp.
- Apple and Mac OS are registered trademarks of Apple Inc.
- Other products may be trademarks or registered trademarks of their respective manufacturers.

Caution and Electronic Emission Notices

Caution

Circuit devices are sensitive to static electricity, which can damage their delicate electronics. Dry weather conditions or walking across a carpeted floor may cause you to acquire a static electrical charge.

To protect your device, always:

- Touch the metal chassis of your computer to ground the static electrical charge before you pick up the circuit device.
- Pick up the device by holding it on the left and right edges only.

Warranty

We warrant to the original end user (purchaser) that the device will be free from any defects in workmanship or materials for a period of **one (1)** years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary tore-store the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

Be a Registered Owner

Web registration is preferred. You can register your Vigor device via http://www.draytek.com.

Firmware & Tools Updates

Due to the continuous evolution of DrayTek technology, all devices will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents.

http://www.draytek.com

European Community Declarations

Manufacturer: DrayTek Corp.
Address: No. 26, Fu Shing Road, HuKou County, HsinChu Industrial Park, Hsin-Chu, Taiwan 303
Product: VigorSwitch Series Device

The product conforms to the requirements of Electro-Magnetic Compatibility (EMC) Directive 2004/108/EC by complying with the requirements set forth in EN55022/Class A and EN55024/Class A.

The product conforms to the requirements of Low Voltage (LVD) Directive 2006/95/EC by complying with the requirements set forth in EN6095-1.

Regulatory Information

Federal Communication Commission Interference Statement

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 in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the use is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different form that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device may accept any interference received, including interference that may cause undesired operation.

Table of Contents

1

2

1 Preface

In this user's manual, it will not only tell you how to install and connect your network system but configure and monitor the VigorSwitch P2260 through the built-in CLI and web by RS-232 serial interface and Ethernet ports step-by-step. Many explanations in detail of hardware and software functions are shown as well as the examples of the operation for web-based interface and command-line interface (CLI).

1.1 Overview

VigorSwitch P2260, implemented 24 10/100Mbps TP + 2 Gigabit dual media ports with TP/SFP, is a standard switch that meets all IEEE 802.3/u/x/z Gigabit, Fast Ethernet and Ethernet specifications. The switch can be managed through RS-232 serial port via directly connection, or through Ethernet port using Telnet or Web-based management unit, associated with SNMP agent. With the SNMP agent, the network administrator can logon the switch to monitor, configure and control each port's activity in a friendly way. The overall network management is enhanced and the network efficiency is also improved to accommodate high bandwidth applications. In addition, the switch features comprehensive and useful function such as QoS (Quality of Service), Spanning Tree, VLAN, Port Trunking, Bandwidth Control, Port Security, SNMP/RMON and IGMP Snooping capability via the intelligent software. It is suitable for both metro-LAN and office application.

Model Description

Model	**Port 25, 26 Configurations**
24-Port PoE L2 Managed Fast Ethernet Switch with 2 SFP Dual Media	Two types of media --- TP and SFP Fiber

10/100/1000Mbps TP is a standard Ethernet port that meets all IEEE 802.3/u/x/z Gigabit, Fast Ethernet specifications. 1000Mbps SFP Fiber transceiver is a Gigabit Ethernet port that fully complies with all IEEE 802.3z and 1000Base-SX/LX standards.

1000Mbps Single Fiber WDM (BiDi) transceiver is designed with an optic Wavelength Division Multiplexing (WDM) technology that transports bi-directional full duplex signal over a single fiber simultaneously.

For upgrading firmware, please refer to the **Section 2-22** for more details. The switch will not stop operating while upgrading firmware and after that, the configuration keeps unchanged.

Below shows key features of this device:

QoS

Support Quality of Service by the IEEE 802.1P standard. There are two priority queue and packet transmission schedule using Weighted Round Robin (WRR). User-defined weight classification of packet priority can be based on either VLAN tag on packets or user-defined port priority.

Spanning Tree

Support IEEE 802.1D, IEEE 802.1w (RSTP: Rapid Spanning Tree Protocol) standards.

VLAN

Support Port-based VLAN and IEEE802.1Q Tag VLAN. Support 256 active VLANs and VLAN ID 1~4094.

Port Trunking

Support static port trunking and port trunking with IEEE 802.3ad LACP.

Bandwidth Control

Support ingress and egress per port bandwidth control.

Port Security

Support allowed, denied forwarding and port security with MAC address.

SNMP/RMON

SNMP agent and RMON MIB. In the device, SNMP agent is a client software which is operating over SNMP protocol used to receive the command from SNMP manager (server site) and echo the corresponded data, i.e. MIB object. Besides, SNMP agent will actively issue TRAP information when happened.

RMON is the abbreviation of Remote Network Monitoring and is a branch of the SNMP MIB.

The device supports MIB-2 (RFC 1213), Bridge MIB (RFC 1493), RMON MIB (RFC 1757)-statistics Group 1,2,3,9, Ethernet-like MIB (RFC 1643), Ethernet MIB (RFC 1643) and so on.

IGMP Snooping

Support IGMP version 2 (RFC 2236): The function IGMP snooping is used to establish the multicast groups to forward the multicast packet to the member ports, and, in nature, avoid wasting the bandwidth while IP multicast packets are running over the network.

1.2 Features

The VigorSwitch P2260 with 2 SFP Dual Media, a standalone off-the-shelf switch, provides the comprehensive features listed below for users to perform system network administration and efficiently and securely serve your network.

Hardware

- Supports 24-port 10/100M TP ports with Nway and auto MDIX function

- In 24-Port PoE L2 Managed Fast Ethernet Switch with 2 SFP Dual Media switch, it supports 2 Gigabit dual media ports(TP/SFP) and 2 slots for removable SFP module supporting 1000M SFP fiber module
- Supports on-line pluggable fiber transceiver modules
- Supports 256KB packet buffer and 128KB control memory
- Maximal packet length can be up to 1536 bytes
- Full-duplex flow control (IEEE802.3x) and half-duplex backpressure
- Extensive front-panel diagnostic LEDs; System: Power, CPURUN, ACT / FDX / SPD(LEDSET), 10/100Mbps TP Port1-24:LINK/ACT, FDX, SPD, 10/100/1000Mbps/Fiber port 25,26: LINK/ACT, FDX, SPD, 24 port IEEE802.3af PoE PSE,
- Endpoint with 48VDC power through RJ-45 pin 1, 2, 3, 6
- Powered Device (PD) auto detection and classification.
- PoE status and activity LED indicator.

Management

- Supports concisely the status of port and easily port configuration
- Supports per port traffic monitoring counters
- Supports a snapshot of the system Information when you login
- Supports port mirror function
- Supports the static trunk function
- Supports 802.1Q VLAN with 256 entries.
- Supports user management and limits three users to login
- Supports DHCP Broadcasting Suppression to avoid network suspended or crashed
- Supports to send the trap event while monitored events happened
- Supports default configuration which can be restored to overwrite the current configuration which is working on via web browser and CLI
- Supports on-line plug/unplug SFP modules
- Supports 5 kinds of QoS, are as follows, MAC Priority, 802.1p Priority, IP TOS Priority, and DiffServ DSCP Priority.
- Built-in web-based management and CLI management, providing a more convenient UI for the user
- Supports port mirror function with ingress/egress traffic
- Supports rapid spanning tree (802.1w RSTP)
- Supports 802.1X port security on a VLAN
- Supports user management and only first login administrator can configure the device. The rest of users can only view the switch
- SNMP access can be disabled and prevent from illegal SNMP access
- Supports Ingress, Non-unicast and Egress Bandwidth rating management
- The trap event and alarm message can be transferred via e-mail and mobile phone short message

- Supports diagnostics to let administrator knowing the hardware status
- Supports external loopback test to check if the link is ok
- TFTP for firmware upgrade, system log upload and config file import/export
- Supports remote boot the device through user interface and SNMP
- Supports network time synchronization and daylight saving
- Supports 120 event log records in the main memory and display on the local console

1.3 Packing List

Before you start installing the switch, verify that the package contains the following:

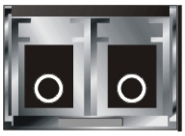
- VigorSwitch P2260
- AC Power Cord
- CD
- Console Cable
- Rubber feet
- Rack mount kit

Please notify your sales representative immediately if any of the aforementioned items is missing or damaged.

Optional Modules

In the switch, Port 25~26 includes two types of media --- TP and SFP Fiber (LC, BiDi LC…); this port supports 10/100/1000Mbps TP or 1000Mbps SFP Fiber with auto-detected function. 1000Mbps SFP Fiber transceiver is used for high-speed connection expansion; the following are optional SFP types compatible for the switch:

- 1000Mbps LC, MM, SFP Fiber transceiver
- 1000Mbps LC, SM 10km, SFP Fiber transceiver
- 1000Mbps LC, SM 30km, SFP Fiber transceiver
- 1000Mbps LC, SM 50km, SFP Fiber transceiver
- 1000Mbps BiDi LC, type 1, SM 20km, SFP Fiber WDM transceiver
- 1000Mbps BiDi LC, type 2, SM 20km, SFP Fiber WDM transceiver
- 1000Mbps LC, SM 10km, SFP Fiber transceiver with DDM



Front View of 1000Base-SX/LX LC, SFP Fiber Transceiver

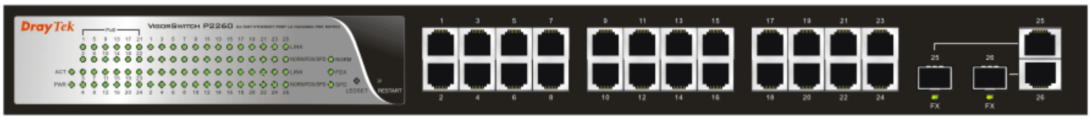
Front View of 1000Base-LX BiDi LC, SFP Fiber Transceiver

1.4 LED Indicators and Connectors

Before you use the Vigor device, please get acquainted with the LED indicators and connectors first.

There are 24 TP Fast Ethernet ports and 2 slots for optional removable modules on the front panel of the switch. LED display area, locating on the front panel, contains a ACT, Power LED and 26 ports working status of the switch.

LED Explanation

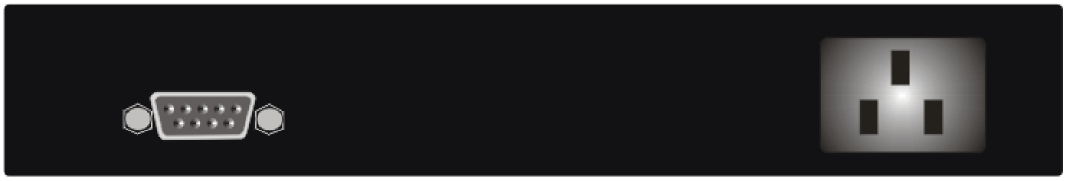


LED	Color	Explanation
ACT	Green	Blinks when CPU is active.
PWR	Green	Lit when +5V DC power is on and good
NORM	Green	Lit when LEDSET(NORM/FDX/SPD) set on normal mode
FDX	Green	Lit when LEDSET (NORM/FDX/SPD) set on full-duplex mode
SPD	Green	Lit when LEDSET (NORM/FDX/SPD) set on speed mode
LINK	Green	Lit when connection with remote device is good. Off when cable connection is not good.
NORM/FDX/ SPD	Amber (1 to 26, Ethernet TP Port)	➢ LEDSET set on NORM mode: Blinks when any traffic is present ➢ LEDSET set on FDX (full-duplex) mode: Lit when full-duplex mode is active Blinks when any collision is present ➢ LEDSET set on SPD (speed) mode: Lit when 100Mbps speed is active Off when 10Mbps speed is active
PoE	Green (1 to 24)	Lit when PoE Power is active
FX 25/26 (Gigabit Fiber Port)	Green	Lit when Fiber port is active; Off when TP port is active

Connector Explanation

Interface	Description
LEDSET	Used to change the LED display mode.
RESTART	Used to reset the management system.
FX (25, 26)	SFP Fiber Port
LAN P1 – P24	Fast Ethernet Port

User Interfaces on the Rear Panel



One RS-232 DB-9 interface is offered for configuration or management.

1.5 Hardware Installation

At the beginning, please do first:

- Wear a grounding device to avoid the damage from electrostatic discharge
- Be sure you have inserted the power cord to power source

1.5.1 Connecting the SFP Fiber Transceiver to the Chassis

The optional SFP modules are hot swappable, so you can plug or unplug it before or after powering on.

1. Verify that the SFP module is the right model and conforms to the chassis
2. Slide the module along the slot. Also be sure that the module is properly seated against the slot socket/connector
3. Install the media cable for network connection
4. Repeat the above steps, as needed, for each module to be installed into slot(s)
5. Have the power ON after the above procedures are done

TP Port and Cable Installation

In the switch, TP port supports MDI/MDI-X auto-crossover, so both types of cable, straight-through (Cable pin-outs for RJ-45 jack 1, 2, 3, 6 to 1, 2, 3, 6 in 10/100M TP; 1, 2, 3, 4, 5, 6, 7, 8 to 1, 2, 3, 4, 5, 6, 7, 8 in Gigabit TP) and crossed-over (Cable pin-outs for RJ-45 jack 1, 2, 3, 6 to 3, 6, 1, 2) can be used. It means you do not have to tell from them, just plug it.

1. Use Cat. 5 grade RJ-45 TP cable to connect to a TP port of the switch and the other end is connected to a network-aware device such as a workstation or a server.
2. Repeat the above steps, as needed, for each RJ-45 port to be connected to a Gigabit 10/100/1000 TP device.
3. Now, you can start having the switch in operation.

Power On

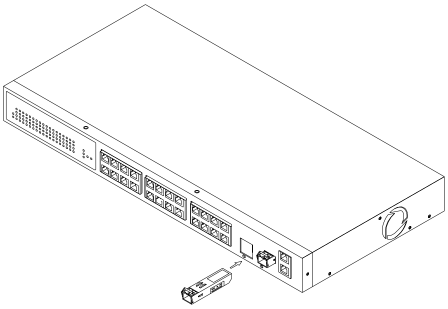
The switch supports 100-240 VAC, 50-60 Hz power supply. The power supply will automatically convert the local AC power source to DC power. It does not matter whether any connection plugged into the switch or not when power on, even modules as well. After the power is on, all LED indicators will light up immediately and then all off except the power LED still keeps on. This represents a reset of the system.

Firmware Loading

After resetting, the bootloader will load the firmware into the memory. It will take about 30 seconds, after that, the switch will flash all the LED once and automatically performs self-test and is in ready state.

1.5.2 Installing Optional SFP Fiber Transceivers to the switch

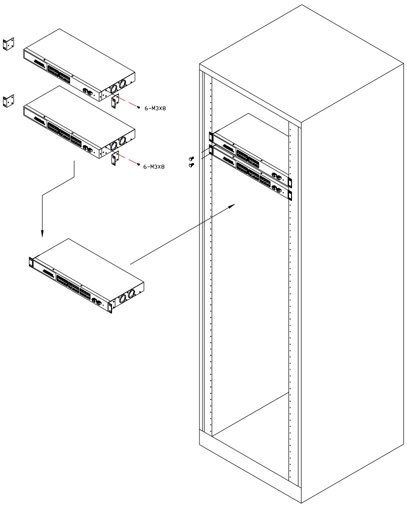
If you have no modules, please skip this section.



1.5.3 Installing Chassis to a 19-Inch Wiring Closet Rail

> **Caution:** Allow a proper spacing and proper air ventilation for the cooling fan at both sides of the chassis.

1. Wear a grounding device for electrostatic discharge.
2. Screw the mounting accessory to the front side of the switch (See Fig. 2-2).
3. Place the Chassis into the 19-inch wiring closet rail and locate it at the proper position. Then, fix the Chassis by screwing it.



1.5.4 Cabling Requirements

To help ensure a successful installation and keep the network performance good, please take a care on the cabling requirement. Cables with worse specification will render the LAN to work poorly.

Cabling Requirements for TP Ports

For Fast Ethernet TP network connection

- The grade of the cable must be Cat. 5 or Cat. 5e with a maximum length of 100 meters.

Gigabit Ethernet TP network connection

- The grade of the cable must be Cat. 5 or Cat. 5e with a maximum length of 100 meters. Cat. 5e is recommended.

Cabling Requirements for 1000SX/LX SFP Module

It is more complex and comprehensive contrast to TP cabling in the fiber media. Basically, there are two categories of fiber, multi mode (MM) and single mode (SM). The later is categorized into several classes by the distance it supports. They are SX, LX, LHX, XD, and ZX. From the viewpoint of connector type, there mainly are LC and BIDI LC.

- Gigabit Fiber with multi-mode LC SFP module
- Gigabit Fiber with single-mode LC SFP module
- Gigabit Fiber with BiDi LC 1310nm SFP module
- Gigabit Fiber with BiDi LC 1550nm SFP module

The following table lists the types of fiber that we support and those else not listed here are available upon request.

IEEE 802.3z Gigabit Ethernet 1000SX 850nm	Multi-mode Fiber Cable and Modal Bandwidth			
	Multi-mode 62.5/125µm		Multi-mode 50/125µm	
	Modal Bandwidth	Distance	Modal Bandwidth	Distance
	160MHz-Km	220m	400MHz-Km	500m
	200MHz-Km	275m	500MHz-Km	550m
1000Base-LX/LH X/XD/ZX	SFP.0LC.212.10/30/50/70/B0 Km			
	Single-mode Fiber 9/125µm			
	Single-mode transceiver 1310nm 10Km			
	Single-mode transceiver 1550nm 30, 50, 70, 110Km			
1000Base-LX Single Fiber WDM Module	SFP.0BL.621.2 02	Single-Mode *20Km	TX(Transmit) 1310nm	
			RX(Receive) 1550nm	
	SFP.0BL.621.2 01	Single-Mode *20Km	TX(Transmit) 1550nm	
			RX(Receive) 1310nm	

Switch Cascading in Topology

Takes the Delay Time into Account

Theoretically, the switch partitions the collision domain for each port in switch cascading that you may up-link the switches unlimitedly. In practice, the network extension (cascading levels & overall diameter) must follow the constraint of the IEEE 802.3/802.3u/802.3z and other 802.1 series protocol specifications, in which the limitations are the timing requirement from physical signals defined by 802.3 series specification of Media Access Control (MAC) and PHY, and timer from some OSI layer 2 protocols such as 802.1d, 802.1q, LACP and so on.

The fiber, TP cables and devices' bit-time delay (round trip) are as follows:

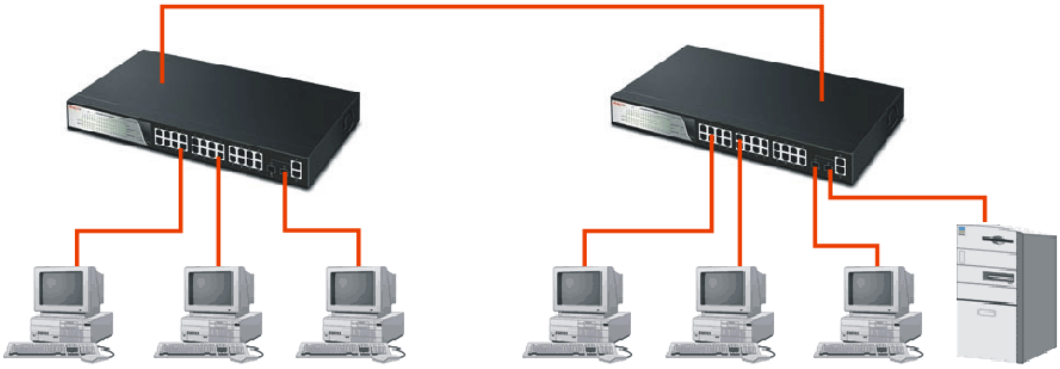
1000Base-X TP, Fiber		**100Base-TX TP**			
Round trip Delay: 4096		Round trip Delay: 512			
Cat. 5 TP Wire:	11.12/m	Cat. 5 TP Wire:	1.12/m	Fiber Cable:	1.0/m
Fiber Cable:	10.10/m	TP to fiber Converter: 56			
Bit Time unit: 1ns (1sec./1000 Mega bit)		Bit Time unit: 0.01µs (1sec./100 Mega bit)			

Sum up all elements' bit-time delay and the overall bit-time delay of wires/devices must be within Round Trip Delay (bit times) in a half-duplex network segment (collision domain). For full-duplex operation, this will not be applied. You may use the TP-Fiber module to extend the TP node distance over fiber optic and provide the long haul connection.

Typical Network Topology in Deployment

A hierarchical network with minimum levels of switch may reduce the timing delay between server and client station. Basically, with this approach, it will minimize the number of switches in any one path; will lower the possibility of network loop and will improve network efficiency. If more than two switches are connected in the same network, select one switch as Level 1 switch and connect all other switches to it at Level 2. Server/Host is recommended to connect to the Level 1 switch. This is general if no VLAN or other special requirements are applied.

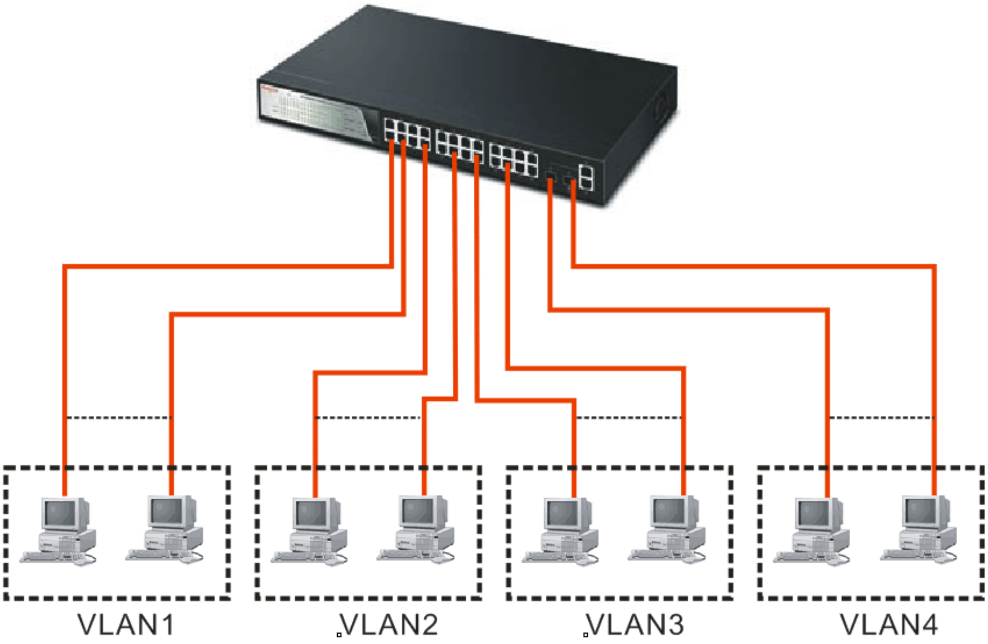
Case 1: All switch ports are in the same local area network.
Every port can access each other.



If VLAN is enabled and configured, each node in the network that can communicate each other directly is bounded in the same VLAN area.

Here VLAN area is defined by what VLAN you are using. The switch supports both port-based VLAN and tag-based VLAN. They are different in practical deployment, especially in physical location. The following diagram shows how it works and what the difference they are.

Case 2: Port-based VLAN -1

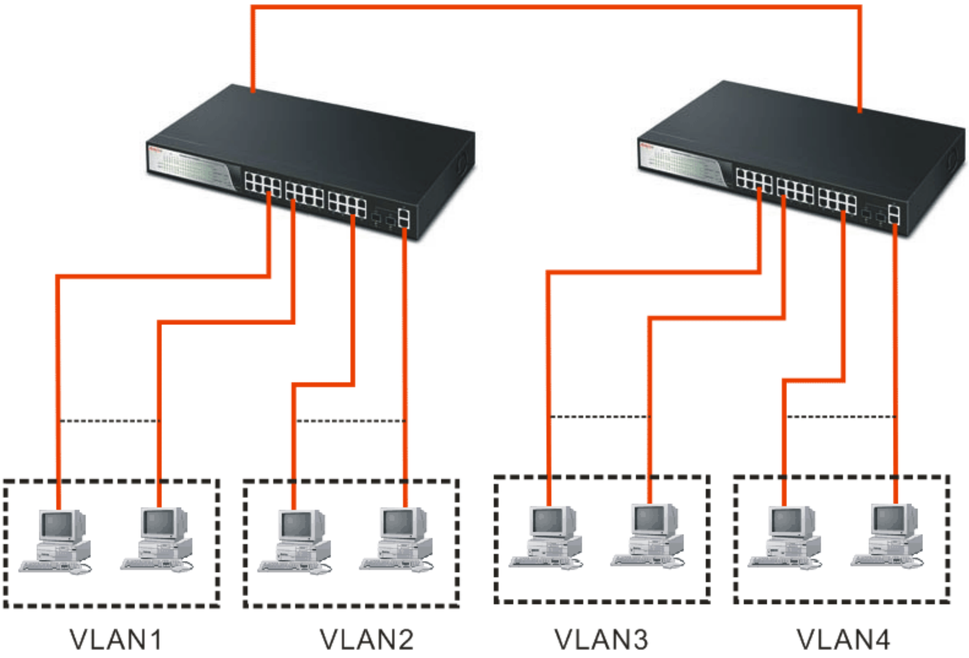


The same VLAN members could not be in different switches.

Every VLAN members could not access VLAN members each other.

The switch manager has to assign different names for each VLAN groups at one switch.

Case 3: Port-based VLAN - 2



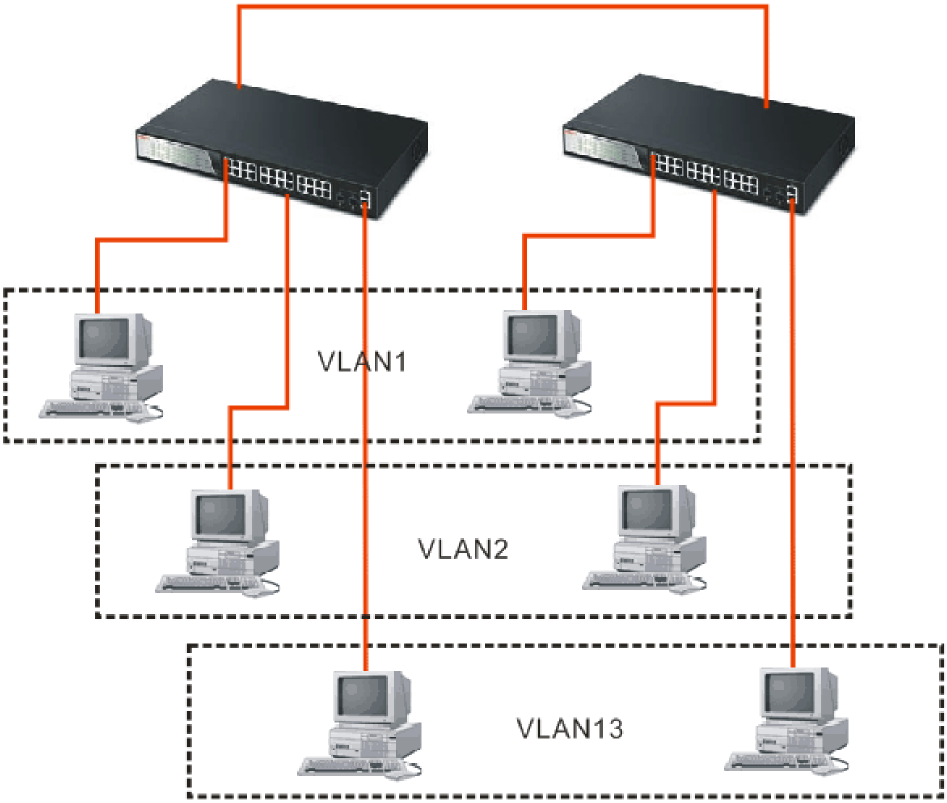
VLAN1 members could not access VLAN2, VLAN3 and VLAN4 members.

VLAN2 members could not access VLAN1 and VLAN3 members, but they could access VLAN4 members.

VLAN3 members could not access VLAN1, VLAN2 and VLAN4.

VLAN4 members could not access VLAN1 and VLAN3 members, but they could access VLAN2 members.

Case 4: The same VLAN members can be at different switches with the same VID



1.5.5 Configuring the Management Agent of Switch

We offer you three ways to startup the switch management function. They are RS-232 console, CLI, and Web. Users can use any one of them to monitor and configure the switch. You can touch them through the following procedures.

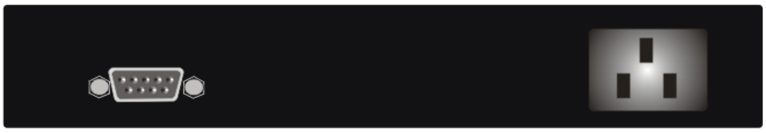
- Configuring the Management Agent of VigorSwitch P2260 through the Serial RS-232 Port
- Configuring the Management Agent of VigorSwitch P2260 through the Ethernet Port

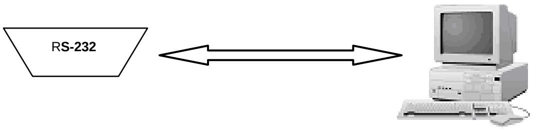
Note: Please first modify the IP address, Subnet mask, Default gateway and DNS through RS-232 console, and then do the next.

Configuring the Management Agent of VigorSwitch P2260 through the Serial RS-232 Port

To perform the configuration through RS-232 console port, the switch's serial port must be directly connected to a DCE device, for example, a PC, through RS-232 cable with DB-9 connector. Next, run a terminal emulator with the default setting of the switch's serial port. With this, you can communicate with the switch.

In the switch, RS-232 interface only supports baud rate 57.6k bps with 8 data bits, 1 stop bit, no parity check and no flow control.





RS-232 cable with female DB-9 connector at both ends

VigorSwitch P2260
Default IP Setting:
IP address = DHCP Enabled
Subnet Mask = DHCP Enabled
Default Gateway = DHCP Enabled

To configure the switch, please follow the procedures below:

1. Find the RS-232 DB-9 cable with female DB-9 connector bundled. Normally, it just uses pins 2, 3 and 7. See also Appendix B for more details on Null Modem Cable Specifications.
2. Attaches the DB-9 female cable connector to the male serial RS-232 DB-9 connector on the switch.
3. Attaches the other end of the serial RS-232 DB-9 cable to PC's serial port, running a terminal emulator supporting VT100/ANSI terminal with the switch's serial port default settings. For example, Windows98/2000/XP HyperTerminal utility.

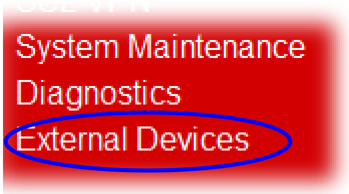
Note: The switch's serial port default settings are listed as follows:

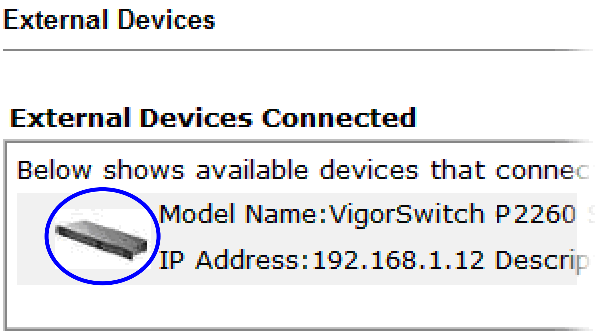
Baud rate	57600

Stop bits	1
Data bits	8
Parity	N
Flow control	none

4. When you complete the connection, then press **<Enter>** key. The login prompt will be shown on the screen. The default username and password are shown as below:
Username = admin *Password = admin*

Additionally, if a user connects VigorSwitch to VigorPro router, he also can access into VigorPro web configuration page to find out External Devices menu item. Then click the new added switch icon to open the web configuration of VigorSwitch.




External Devices

External Devices Connected

Below shows available devices that connec

Model Name:VigorSwitch P2260

IP Address:192.168.1.12 Descrip

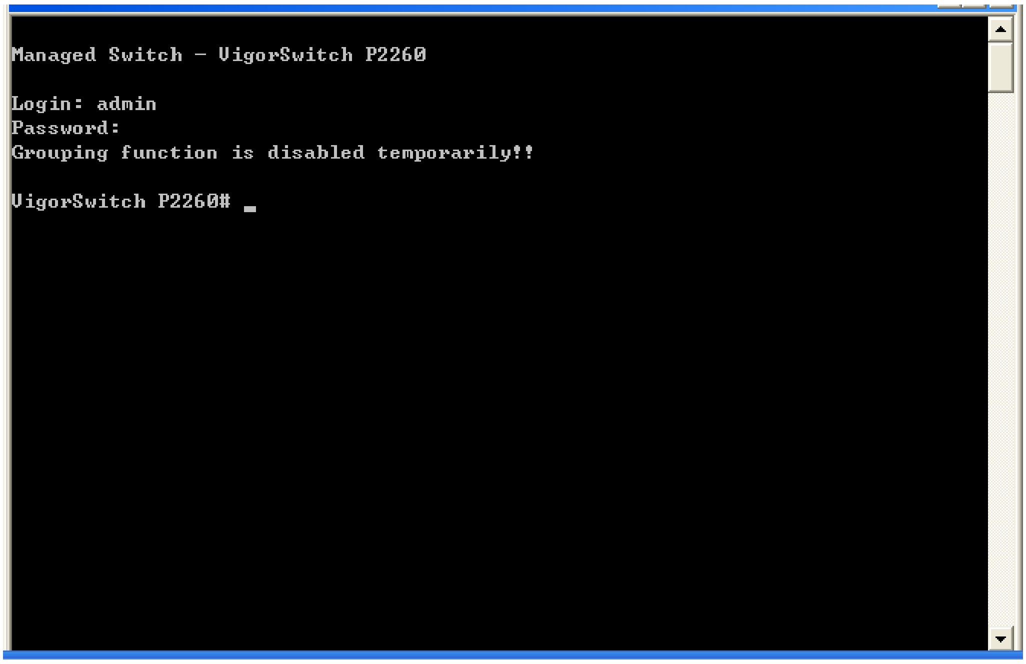
Set IP Address, Subnet Mask and Default Gateway IP Address

You can first either configure your PC IP address or change IP address of the switch, next to change the IP address of default gateway and subnet mask.

For example, your network address is 10.1.1.0, and subnet mask is 255.255.255.0. You can change the switch’s default IP address 192.168.1.1 to 10.1.1.1 and set the subnet mask to be 255.255.255.0. Then, choose your default gateway, may be it is 10.1.1.254.

Default Value	VigorSwitch P2260	Your Network Setting
IP Address	192.168.1.1	10.1.1.1
Subnet	255.255.255.0	255.255.255.0
Default Gateway	192.168.1.254	10.1.1.254

After completing these settings in the switch, it will reboot to have the configuration taken effect. After this step, you can operate the management through the network, no matter it is from a web browser or Network Management System (NMS).



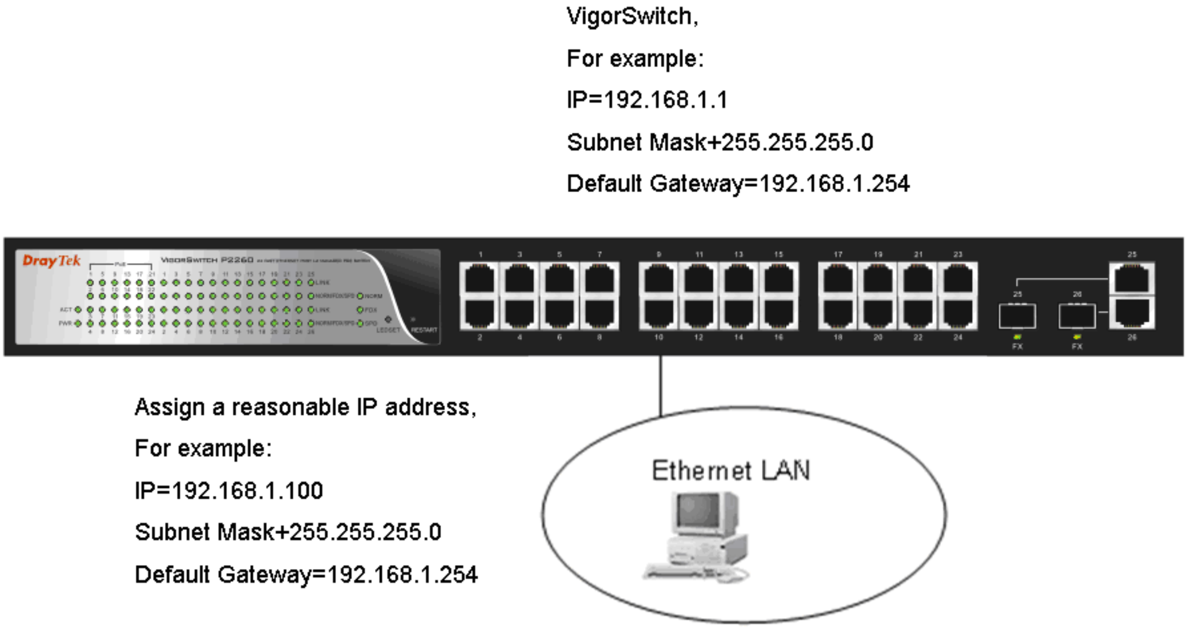
```
Managed Switch - VigorSwitch P2260

Login: admin
Password:
Grouping function is disabled temporarily!!

VigorSwitch P2260# _
```

Configuring the Management Agent of VigorSwitch P2260 through the Ethernet Port

There are three ways to configure and monitor the switch through the switch’s Ethernet port. They are CLI, Web browser and SNMP manager. The user interface for the last one is NMS dependent and does not cover here. We just introduce the first two types of management interface.


VigorSwitch,
For example:
IP=192.168.1.1
Subnet Mask+255.255.255.0
Default Gateway=192.168.1.254
DrayTek
VigorSwitch P2260
Assign a reasonable IP address,
For example:
IP=192.168.1.100
Subnet Mask+255.255.255.0
Default Gateway=192.168.1.254
Ethernet LAN

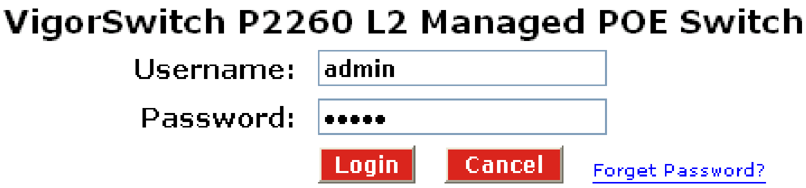
Managing VigorSwitch P2260 through Ethernet Port

Before you communicate with the switch, you have to finish the configuration of the IP address or to know the IP address of the switch. Then, follow the procedures listed below.

1. Set up a physical path between the configured the switch and a PC by a qualified UTP Cat. 5 cable with RJ-45 connector.

> **Note:** If PC directly connects to the switch, you have to setup the same subnet mask between them. But, subnet mask may be different for the PC in the remote site.

2. Run CLI or web browser and follow the menu. Please refer to Chapter 2.



VigorSwitch P2260 L2 Managed POE Switch

Username: admin

Password: ●●●●●

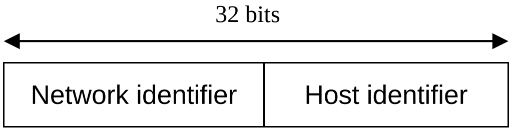
1.5.6 IP Address Assignment

For IP address configuration, there are three parameters needed to be filled in. They are IP address, Subnet Mask, Default Gateway and DNS.

IP address:

The address of the network device in the network is used for internetworking communication. Its address structure looks is shown below. It is "classful" because it is split into predefined address classes or categories.

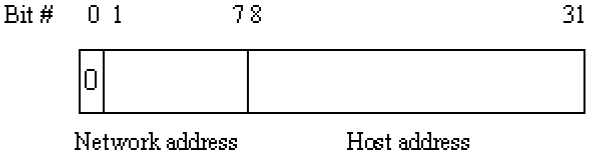
Each class has its own network range between the network identifier and host identifier in the 32 bits address. Each IP address comprises two parts: network identifier (address) and host identifier (address). The former indicates the network where the addressed host resides, and the latter indicates the individual host in the network which the address of host refers to. And the host identifier must be unique in the same LAN. Here the term of IP address we used is version 4, known as IPv4.



With the classful addressing, it divides IP address into three classes, class A, class B and class C. The rest of IP addresses are for multicast and broadcast. The bit length of the network prefix is the same as that of the subnet mask and is denoted as IP address/X, for example, 192.168.1.0/24. Each class has its address range described below.

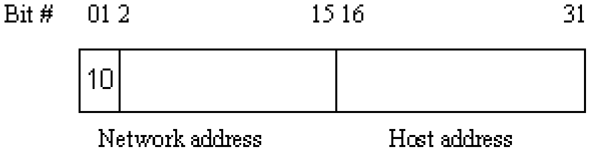
Class A:

Address is less than 126.255.255.255. There are a total of 126 networks can be defined because the address 0.0.0.0 is reserved for default route and 127.0.0.0/8 is reserved for loopback function.



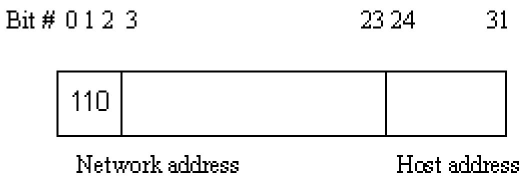
Class B:

IP address range between 128.0.0.0 and 191.255.255.255. Each class B network has a 16-bit network prefix followed 16-bit host address. There are 16,384 (2^14)/16 networks able to be defined with a maximum of 65534 (2^16 –2) hosts per network.



Class C:

IP address range between 192.0.0.0 and 223.255.255.255. Each class C network has a 24-bit network prefix followed 8-bit host address. There are 2,097,152 (2^21)/24 networks able to be defined with a maximum of 254 (2^8 –2) hosts per network.



Class D and E:

Class D is a class with first 4 MSB (Most significance bit) set to 1-1-1-0 and is used for IP Multicast. See also RFC 1112. Class E is a class with first 4 MSB set to 1-1-1-1 and is used for IP broadcast.

According to IANA (Internet Assigned Numbers Authority), there are three specific IP address blocks reserved and able to be used for extending internal network. We call it Private IP address and list below:

Class A	10.0.0.0 --- 10.255.255.255
Class B	172.16.0.0 --- 172.31.255.255
Class C	192.168.0.0 --- 192.168.255.255

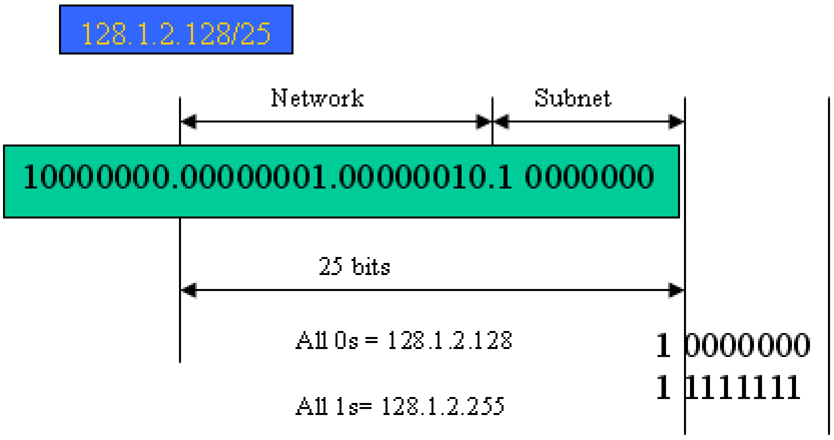
Please refer to RFC 1597 and RFC 1466 for more information.

Subnet mask:

It means the sub-division of a class-based network or a CIDR block. The subnet is used to determine how to split an IP address to the network prefix and the host address in bitwise basis. It is designed to utilize IP address more efficiently and ease to manage IP network.

For a class B network, 128.1.2.3, it may have a subnet mask 255.255.0.0 in default, in which the first two bytes is with all 1s. This means more than 60 thousands of nodes in flat IP address will be at the same network. It’s too large to manage practically. Now if we divide it into smaller network by extending network prefix from 16 bits to, say 24 bits, that’s using its third byte to subnet this class B network. Now it has a subnet mask 255.255.255.0, in which each bit of the first three bytes is 1. It’s now clear that the first two bytes is used to identify the class B network, the third byte is used to identify the subnet within this class B network and, of course, the last byte is the host number.

Not all IP address is available in the sub-netted network. Two special addresses are reserved. They are the addresses with all zero’s and all one’s host number. For example, an IP address 128.1.2.128, what IP address reserved will be looked like? All 0s mean the network itself, and all 1s mean IP broadcast.



In this diagram, you can see the subnet mask with 25-bit long, 255.255.255.128, contains 126 members in the sub-netted network. Another is that the length of network prefix equals the number of the bit with 1s in that subnet mask. With this, you can easily count the number of IP addresses matched. The following table shows the result.

Prefix Length	No. of IP matched	No. of Addressable IP
/32	1	-
/31	2	-
/30	4	2
/29	8	6
/28	16	14
/27	32	30
/26	64	62
/25	128	126
/24	256	254
/23	512	510
/22	1024	1022
/21	2048	2046
/20	4096	4094
/19	8192	8190
/18	16384	16382
/17	32768	32766
/16	65536	65534

According to the scheme above, a subnet mask 255.255.255.0 will partition a network with the class C. It means there will have a maximum of 254 effective nodes existed in this sub-netted network and is considered a physical network in an autonomous network. So it owns a network IP address which may looks like 168.1.2.0.

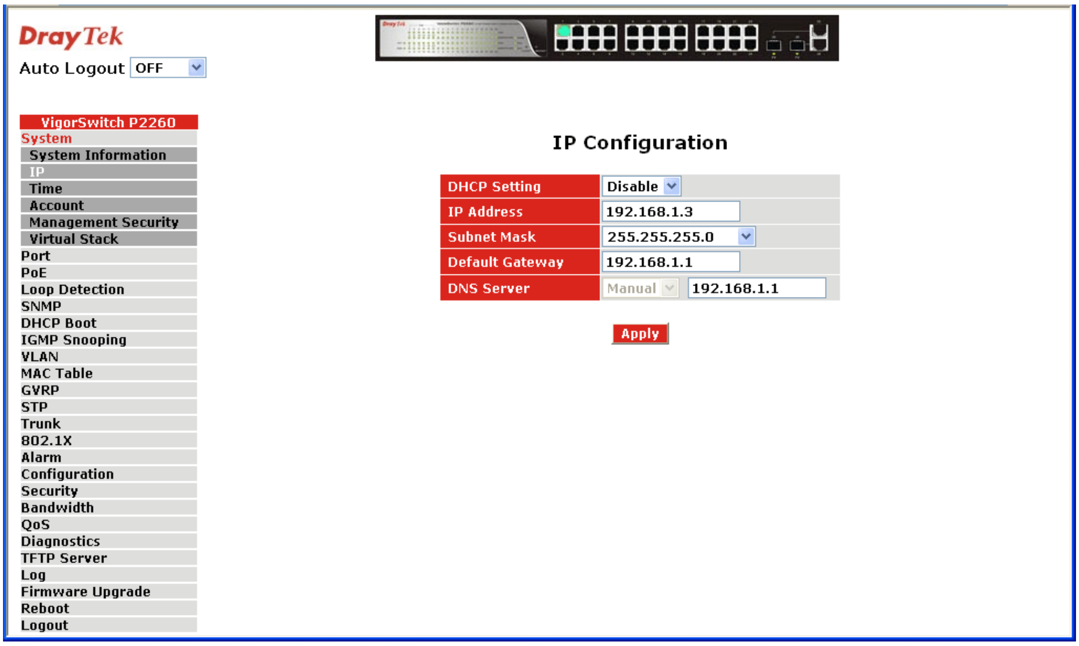
With the subnet mask, a bigger network can be cut into small pieces of network. If we want to have more than two independent networks in a worknet, a partition to the network must be performed. In this case, subnet mask must be applied.

For different network applications, the subnet mask may look like 255.255.255.240. This means it is a small network accommodating a maximum of 15 nodes in the network.

Default gateway:

For the routed packet, if the destination is not in the routing table, all the traffic is put into the device with the designated IP address, known as default router. Basically, it is a routing policy. The gateway setting is used for Trap Events Host only in the switch.

For assigning an IP address to the switch, you just have to check what the IP address of the network will be connected with the switch. Use the same network address and append your host address to it.



IP Configuration

DHCP Setting	Disable
IP Address	192.168.1.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	Manual 192.168.1.1

First, IP Address: as shown above, enter “192.168.1.1”, for instance. For sure, an IP address such as 192.168.1.x must be set on your PC.

Second, Subnet Mask: as shown above, enter “255.255.255.0”. Any subnet mask such as 255.255.255.x is allowable in this case.

DNS:

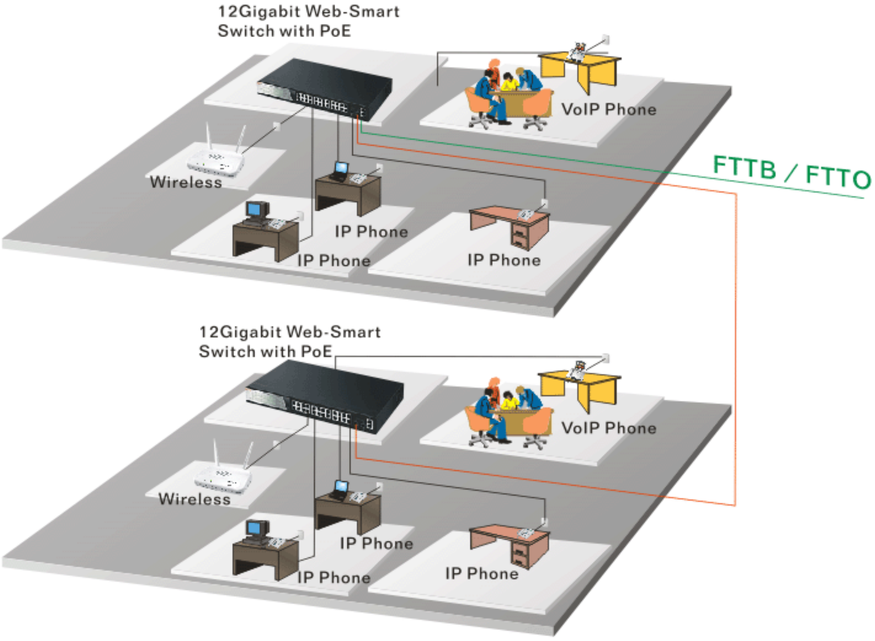
The Domain Name Server translates human readable machine name to IP address. Every machine on the Internet has a unique IP address. A server generally has a static IP address. To connect to a server, the client needs to know the IP of the server. However, user generally uses the name to connect to the server. Thus, the switch DNS client program (such as a browser) will ask the DNS to resolve the IP address of the named server.

1.6 Typical Applications

The 24-Port PoE L2 Managed Fast Ethernet Switch with 2 SFP Dual Media implements 24 Fast Ethernet TP ports with auto MDIX and 2 Gigabit dual media ports with SFP for removable module supported comprehensive fiber types of connection, including LC, BiDi LC for SFP. For more details on the specification of the switch, please refer to Appendix A.

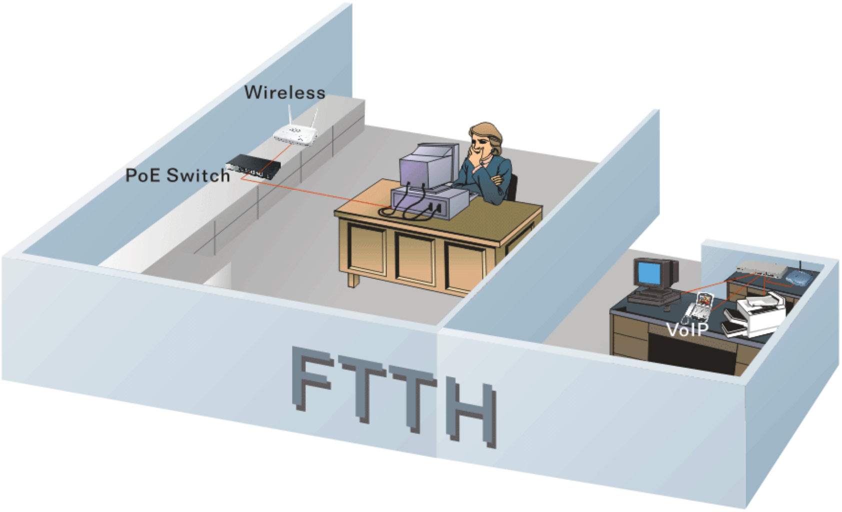
The switch is suitable for the following applications.

- FTTB/FTTO application is used in carrier or ISP

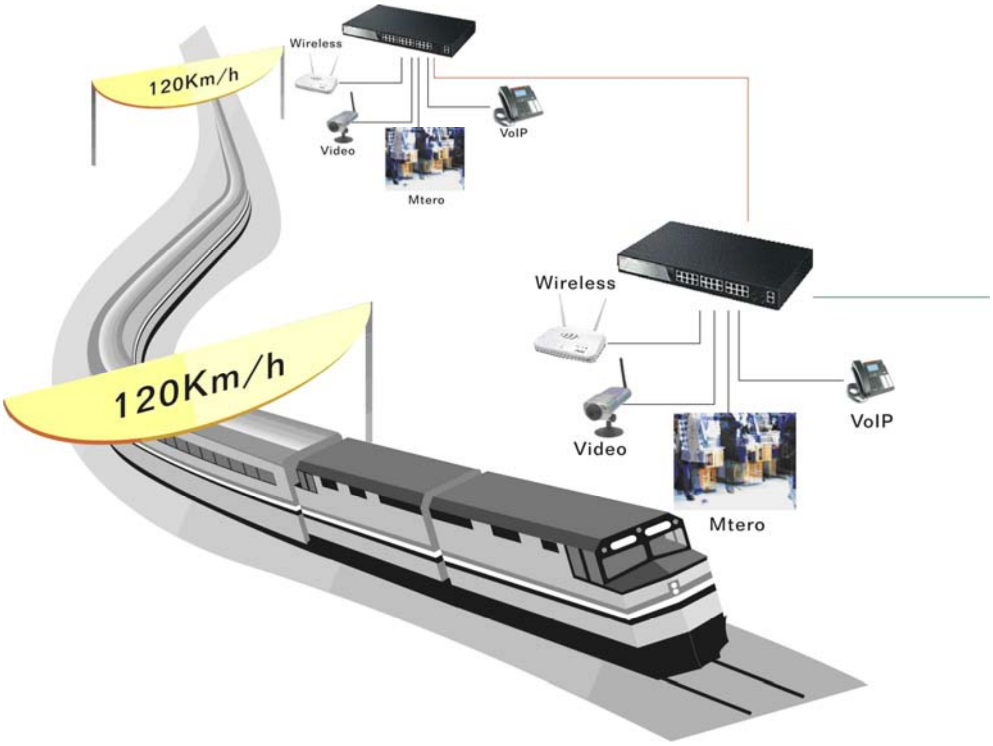


Network Connection of FTTB/FTTO – it is a system wide basic reference connection diagram. This diagram demonstrates how the switch connects with other network devices and hosts.

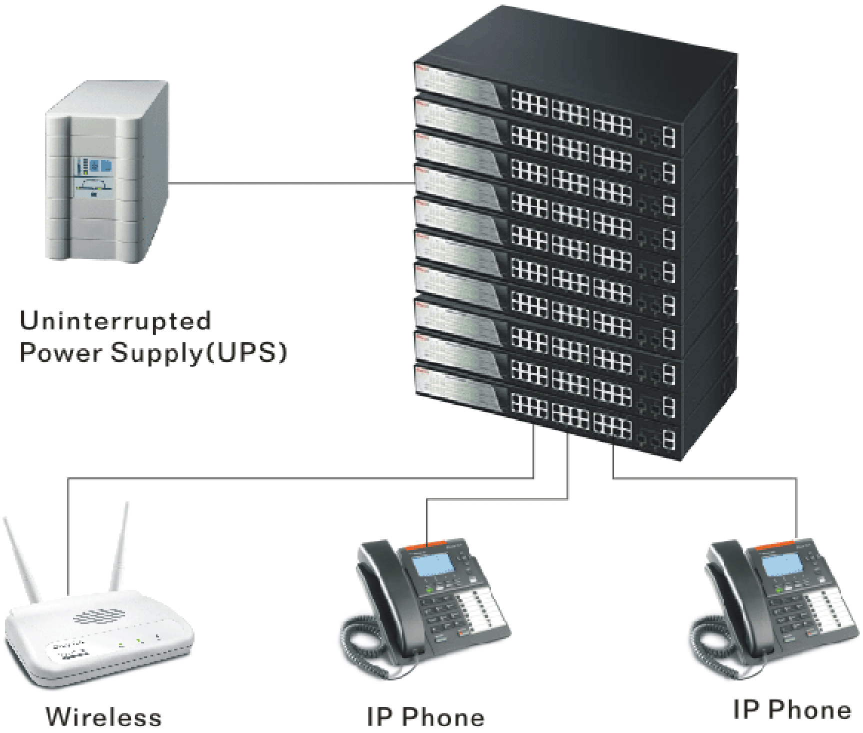
- FTTH application is used in carrier or ISP



- Daisy-Chain Fiber Network Connection



- Uninterrupted Power Supply for IP Phone Application



2 Operation of Web-based Management

This chapter instructs you how to configure and manage the switch through the web user interface it supports, to access and manage the 24-Port 10/100Mbps TP and 2-Port Gigabit TP/SFP Fiber management Ethernet switch. With this facility, you can easily access and monitor through any one port of the switch all the status of the switch, including MIBs status, each port activity, Spanning tree status, port aggregation status, multicast traffic, VLAN and priority status, even illegal access record and so on.

The default values of the managed switch are listed in the table below:

IP Address	DHCP Enabled
Subnet Mask	DHCP Enabled
Default Gateway	DHCP Enabled
Username	admin
Password	admin

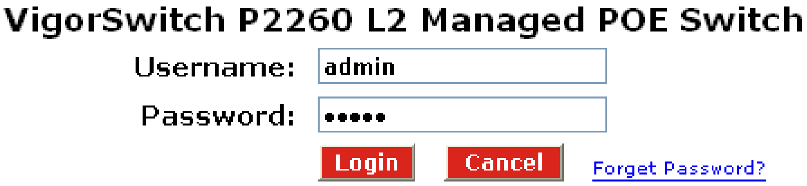
After the managed switch has been finished configuration in the CLI via the switch's serial interface, you can browse it. For example, type http://192.168.1.1 in the address row in a browser, it will show the following screen (see Figure below) and ask you inputting username and password in order to login and access authentication. The default username and password are both "admin". For the first time to use, please enter the default username and password, then click the **<Login>** button. The login process now is completed.

Just click the link of "Forget Password" in WebUI or input "Ctrl+Z" in CLI's login screen in case the user forgets the manager's password. Then, the system will display a serial No. for the user. Write down this serial No. and contact your vendor, the vendor will give you a temporary password. Use this new password as ID and Password, and it will allow the user to login the system with manager authority temporarily. Due to the limit of this new password, the user only can login the system one time, therefore, please modify your password immediately after you login in the system successfully.

In this login menu, you have to input the complete username and password respectively, the switch will not give you a shortcut to username automatically. This looks inconvenient, but safer.

In the switch, it supports a simple user management function allowing only one administrator to configure the system at the same time. If there are two or more users using administrator's identity, the switch will allow the only one who logins first to configure the system. The rest of users, even with administrator's identity, can only monitor the system. For those who have no administrator's identity, can only monitor the system. There are only a maximum of three users able to login simultaneously in the switch.

To optimize the display effect, we recommend you use Microsoft IE 6.0 above, Netscape V7.1 above or FireFox V1.00 above and have the resolution 1024x768. The switch supported neutral web browser interface.



VigorSwitch P2260 L2 Managed POE Switch

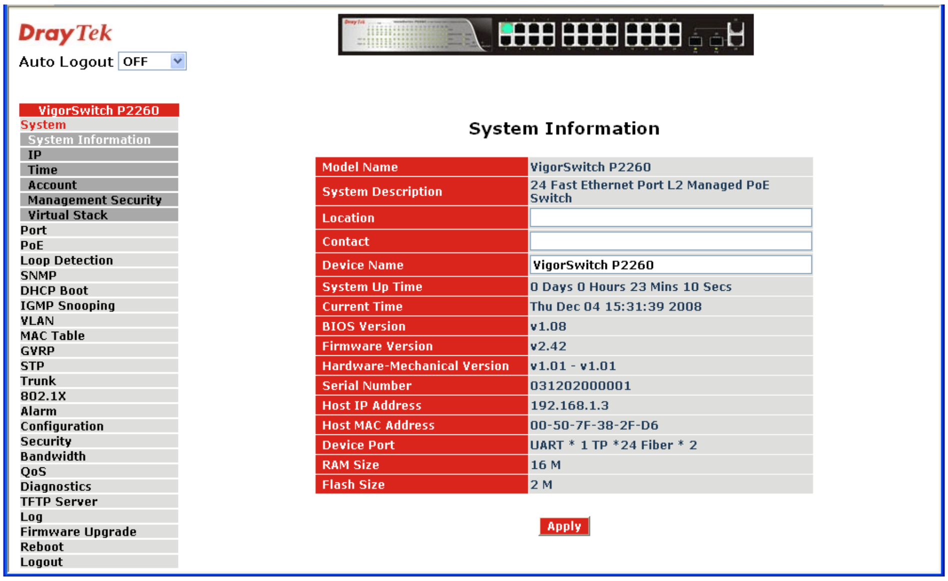
Username: admin

Password: •••••

2.1 Web Management Home Overview

After you login, the switch shows you the system information as shown below. This page is default and tells you the basic information of the system, including “Model Name”, “System Description”, “Location”, “Contact”, “Device Name”, “System Up Time”, “Current Time”, “BIOS Version”, “Firmware Version”, “Hardware-Mechanical Version”, “Serial Number”, “Host IP Address”, “Host MAC Address”, “Device Port”, “RAM Size” and “Flash Size”. With this information, you will know the software version used, MAC address, serial number, how many ports good and so on. This is helpful while malfunctioning.

In the following figure, left section is the whole function tree with web user interface and we will travel it through this chapter.



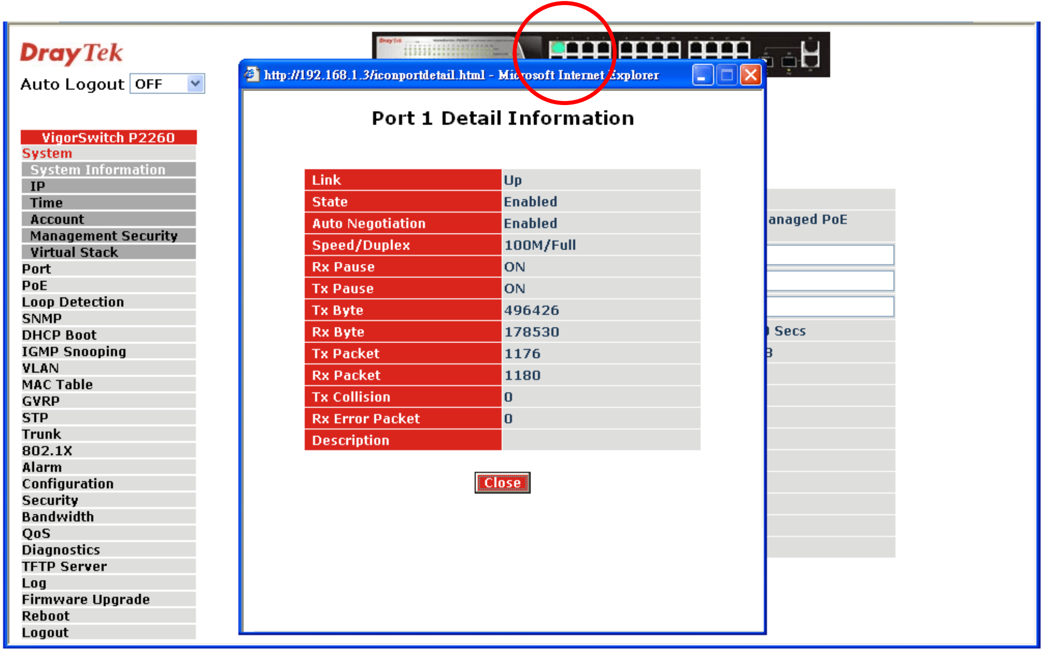
System Information

Model Name	VigorSwitch P2260
System Description	24 Fast Ethernet Port L2 Managed PoE Switch
Location	
Contact	
Device Name	VigorSwitch P2260
System Up Time	0 Days 0 Hours 23 Mins 10 Secs
Current Time	Thu Dec 04 15:31:39 2008
BIOS Version	v1.08
Firmware Version	v2.42
Hardware-Mechanical Version	v1.01 - v1.01
Serial Number	031202000001
Host IP Address	192.168.1.3
Host MAC Address	00-50-7F-38-2F-D6
Device Port	UART * 1 TP *24 Fiber * 2
RAM Size	16 M
Flash Size	2 M

2.1.1 The Information of Page Layout

On the top side, it shows the front panel of the switch. In the front panel, the linked ports will display green; as to the ports, which are link off, they will be dark. For the optional modules, the slot will show only a cover plate if no module exists and will show a module if a module is present. The image of module depends on the one you inserted. The same, if disconnected, the port will show just dark, if linked, green.

In this device, there are clicking functions on the panel provided for the information of the ports. These are very convenient functions for browsing the information of a single port. When clicking the port on the front panel, an information window for the port will be pop out.



Auto Logout OFF

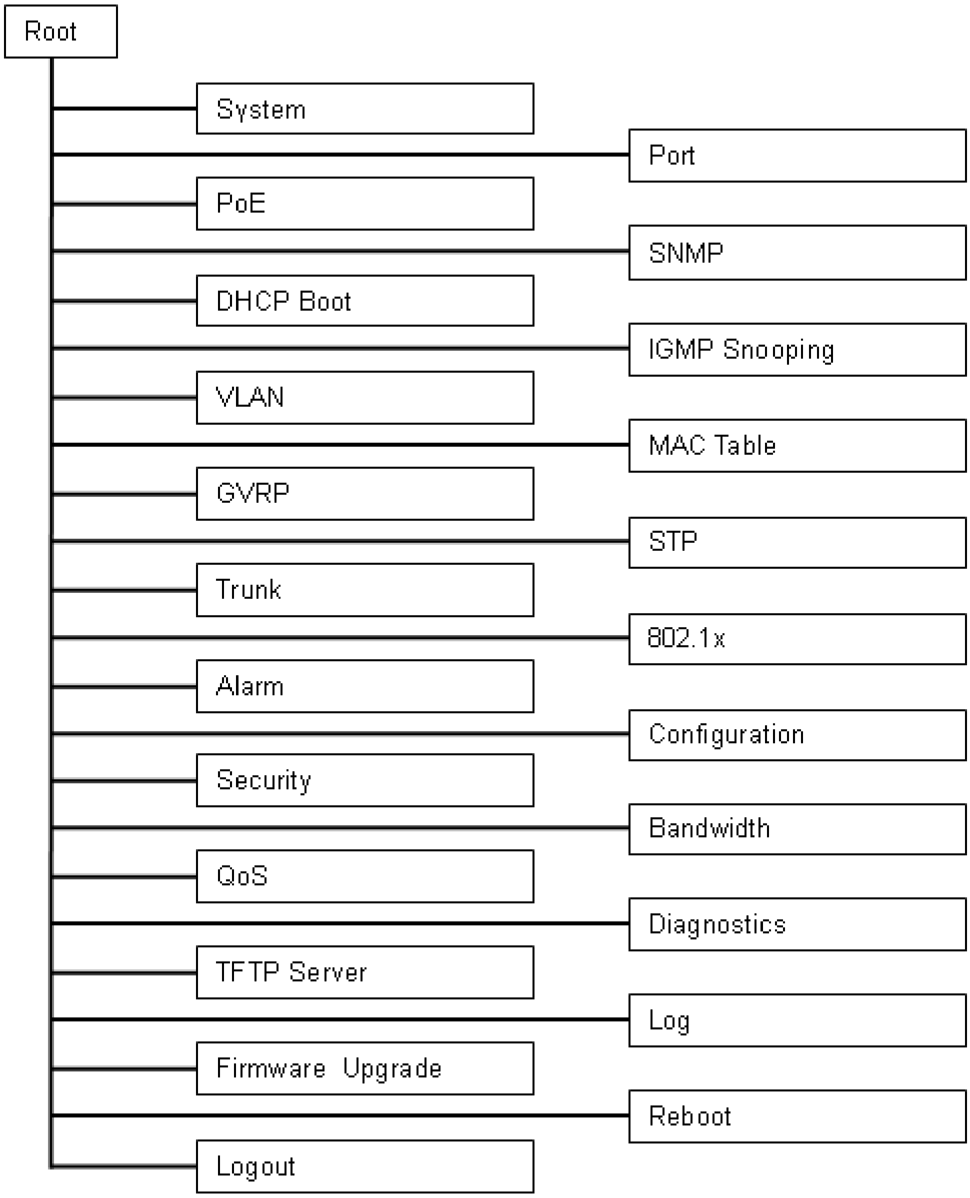
Port 1 Detail Information

Link	Up
State	Enabled
Auto Negotiation	Enabled
Speed/Duplex	100M/Full
Rx Pause	ON
Tx Pause	ON
Tx Byte	496426
Rx Byte	178530
Tx Packet	1176
Rx Packet	1180
Tx Collision	0
Rx Error Packet	0
Description	

It shows the basic information of the clicked port. With this, you’ll see the information about the port status, traffic status and bandwidth rating for egress and ingress respectively.

On the left-top corner, there is a pull-down list for Auto Logout. For the sake of security, we provide auto-logout function to protect you from illegal user as you are leaving. If you do not choose any selection in Auto Logout list, it means you turn on the Auto Logout function and the system will be logged out automatically when no action on the device 3 minutes later. If OFF is chosen, the screen will keep as it is. Default is ON

On the left side, the main menu tree for web is listed in the page. They are hierarchical menu. Open the function folder, a sub-menu will be shown. The functions of each folder are described in its corresponded section respectively. When clicking it, the function is performed. The following list is the full function tree for web user interface.



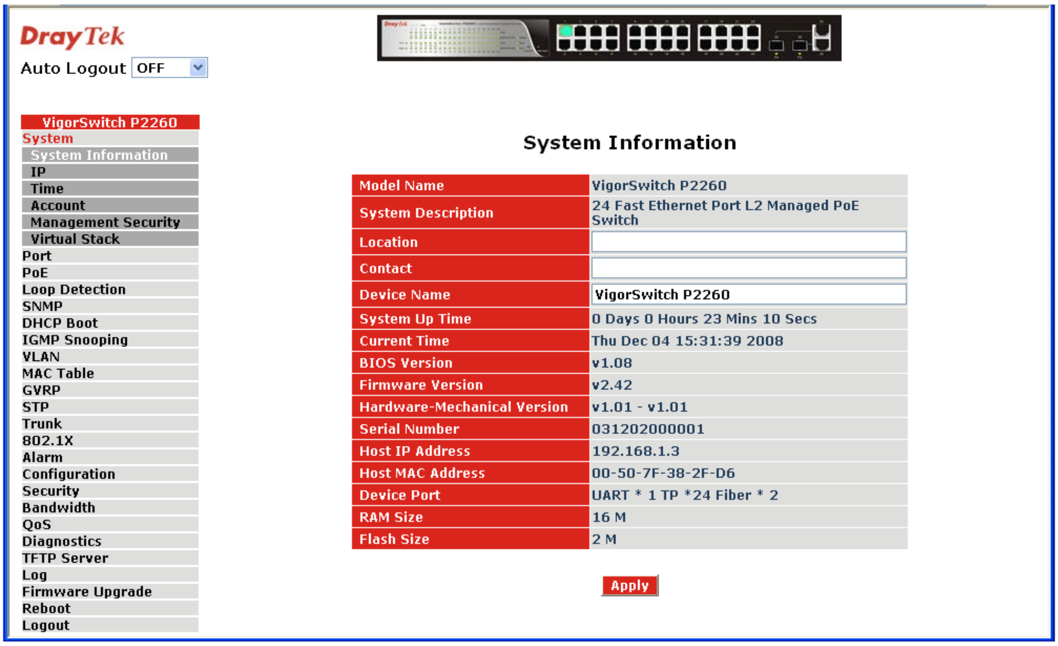
2.1.2 System Information

Function name:

System Information

Function description:

Show the basic system information.



System Information

Model Name	VigorSwitch P2260
System Description	24 Fast Ethernet Port L2 Managed PoE Switch
Location	
Contact	
Device Name	VigorSwitch P2260
System Up Time	0 Days 0 Hours 23 Mins 10 Secs
Current Time	Thu Dec 04 15:31:39 2008
BIOS Version	v1.08
Firmware Version	v2.42
Hardware-Mechanical Version	v1.01 - v1.01
Serial Number	031202000001
Host IP Address	192.168.1.3
Host MAC Address	00-50-7F-38-2F-D6
Device Port	UART * 1 TP *24 Fiber * 2
RAM Size	16 M
Flash Size	2 M

Parameter description:

Model name: The model name of this device.

System description: Type the device description to identity what the device is.

Location: Type the device location description for management.

Contact: For easily managing and maintaining device, you may write down the contact person and phone here for getting help soon. You can configure this parameter through the device's user interface or SNMP.

Device name: The name of the switch, User-defined. Default is VigorSwitch P2260.

System up time: The time accumulated since this switch is powered up. Its format is day, hour, minute, second.

Current time: Show the system time of the switch. Its format: day of week, month, day, hours: minutes: seconds, year. For instance, Wed, Apr. 23, 12:10:10, 2004.

BIOS version: The version of the BIOS in this switch.

Firmware version: The firmware version in this switch.

Hardware-Mechanical version: The version of Hardware and Mechanical. The figure before the hyphen is the version of electronic hardware; the one after the hyphen is the version of mechanical.

Serial number: The serial number is assigned by the manufacturer.

Host IP address: The IP address of the switch.

Host MAC address: It is the Ethernet MAC address of the management agent in this switch.

Device Port: Show all types and numbers of the port in the switch.

RAM size: The size of the DRAM in this switch.

Flash size: The size of the flash memory in this switch.

2.1.3 IP Configuration

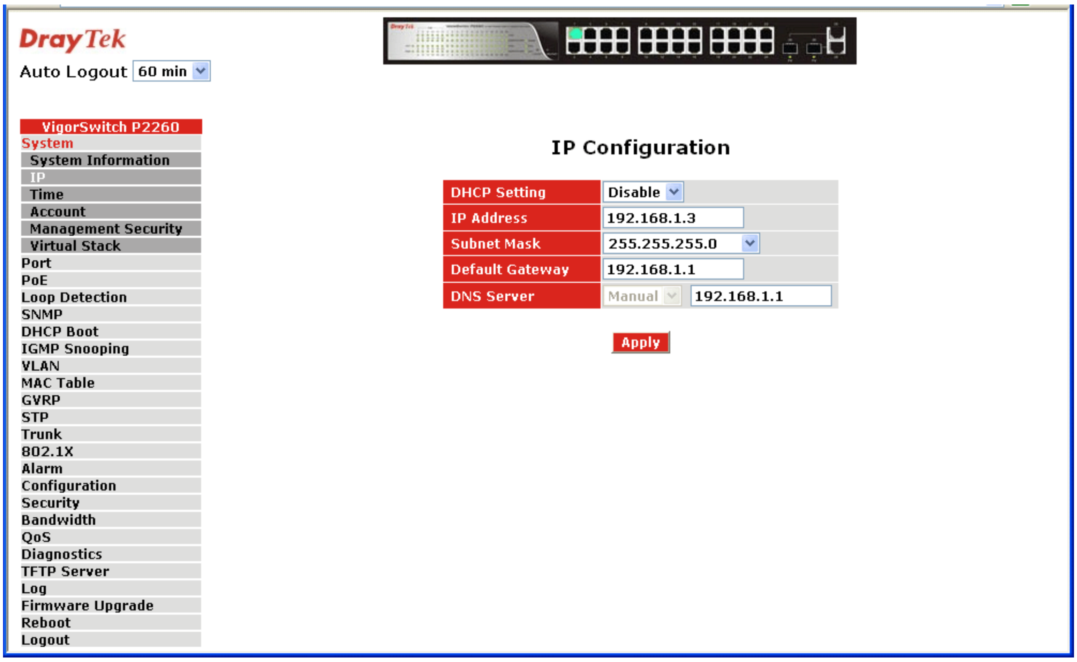
IP configuration is one of the most important configurations in the switch. Without the proper setting, network manager will not be able to manage or view the device. The switch supports both manual IP address setting and automatic IP address setting via DHCP server. When IP address is changed, you must reboot the switch to have the setting taken effect and use the new IP to browse for web management and CLI management.

Function name:

IP Configuration

Function description:

Set IP address, subnet mask, default gateway and DNS for the switch.



IP Configuration

DHCP Setting	Disable
IP Address	192.168.1.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	Manual 192.168.1.1

Parameter description:

DHCP Setting:

DHCP is the abbreviation of Dynamic Host Configuration Protocol. Here DHCP means a switch to turn ON or OFF the function.

The switch supports DHCP client used to get an IP address automatically if you set this function "Enable". When enabled, the switch will issue the request to the DHCP server resided in the network to get an IP address. If DHCP server is down or does not exist, the switch will issue the request and show IP address is under requesting, until the DHCP server is up. Before getting an IP address from DHCP server, the device will not continue booting procedures. If set this field "Disable", you'll have to input IP address manually. For more details about IP address and DHCP, please see the Section 2-1-5 "IP Address Assignment" in this manual.
Default: Disable

IP address:

Users can configure the IP settings and fill in new values if users set the DHCP function "Disable". Then, click

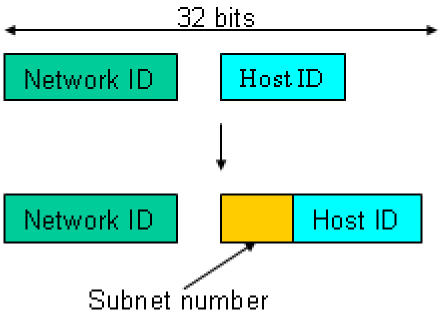
<**Apply**> button to update.

When DHCP is disabled, Default: 192.168.1.1

If DHCP is enabled, this field is filled by DHCP server and will not allow user manually set it any more.

Subnet mask:

Subnet mask is made for the purpose to get more network address because any IP device in a network must own its IP address, composed of Network address and Host address, otherwise can't communicate with other devices each other. But unfortunately, the network classes A, B, and C are all too large to fit for almost all networks, hence, subnet mask is introduced to solve this problem. Subnet mask uses some bits from host address and makes an IP address looked Network address, Subnet mask number and host address. It is shown in the following figure. This reduces the total IP number of a network able to support, by the amount of 2 power of the bit number of subnet number (2^(bit number of subnet number)).



Subnet mask is used to set the subnet mask value, which should be the same value as that of the other devices resided in the same network it attaches.

For more information, please also see the Section 2-1-5 "IP Address Assignment" in this manual.

Default: 255.255.255.0

Default gateway:

Set an IP address for a gateway to handle those packets that do not meet the routing rules predefined in the device. If a packet does not meet the criteria for other pre-defined path, it must be forwarded to a default router on a default path. This means any packet with undefined IP address in the routing table will be sent to this device unconditionally.

When DHCP is disabled, Default: 192.168.1.254

DNS Server

You can set the DNS server by manual or auto when the DHCP is enabled. Only manual setting is supported when DHCP is disabled. The DNS server IP will be obtained from DHCP server when you set the DNS server by auto.

2.1.4 Time Configuration

The switch provides manual and automatic ways to set the system time via NTP. Manual setting is simple and you just input “Year”, “Month”, “Day”, “Hour”, “Minute” and “Second” within the valid value range indicated in each item. If you input an invalid value, for example, 61 in minute, the switch will clamp the figure to 59.

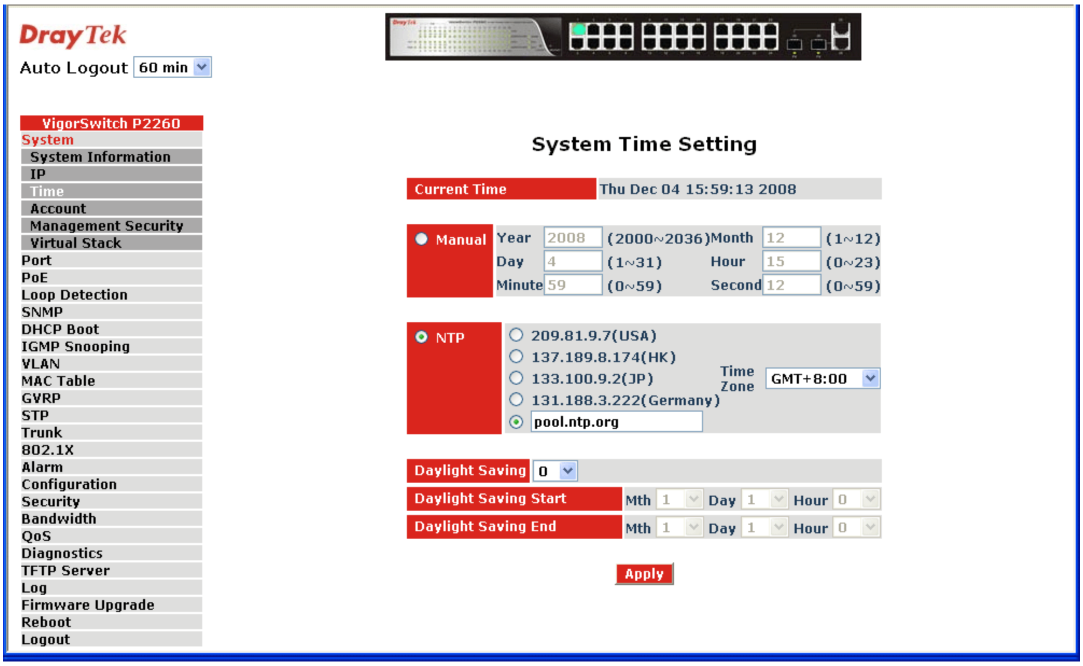
NTP is a well-known protocol used to synchronize the clock of the switch system time over a network. NTP, an internet draft standard formalized in RFC 1305, has been adopted on the system is version 3 protocol. The switch provides four built-in NTP server IP addresses resided in the Internet and a user-defined NTP server IP address. The time zone is Greenwich-centered which uses the expression form of GMT+/- xx hours.

Function name:

Time

Function description:

Set the system time by manual input or set it by syncing from Time servers. The function also supports daylight saving for different area’s time adjustment.



System Time Setting

Current Time: Thu Dec 04 15:59:13 2008

○ Manual: Year 2008 (2000~2036) Month 12 (1~12) Day 4 (1~31) Hour 15 (0~23) Minute 59 (0~59) Second 12 (0~59)

● NTP:
- ○ 209.81.9.7(USA)
- ○ 137.189.8.174(HK)
- ○ 133.100.9.2(JP)
- ○ 131.188.3.222(Germany)
- ● pool.ntp.org

Time Zone: GMT+8:00

Daylight Saving: 0

Daylight Saving Start: Mth 1 Day 1 Hour 0

Daylight Saving End: Mth 1 Day 1 Hour 0

Parameter description:

Current Time: Show the current time of the system.

Manual: This is the function to adjust the time manually. Filling the valid figures in the fields of Year, Month, Day, Hour, Minute and Second respectively and press <**Apply**> button, time is adjusted. The valid figures for the parameter Year, Month, Day, Hour, Minute and Second are >=2000, 1-12, 1-31, 0-23, 0-59 and 0-59 respectively. Input the wrong figure and press <**Apply**> button, the device will reject the time adjustment request. There is no time zone setting in Manual mode.

NTP: NTP is Network Time Protocol and is used to sync the network time based Greenwich Mean Time (GMT). If use the NTP mode and select a built-in NTP time server or manually specify an user-defined NTP server as well as

Time Zone, the switch will sync the time in a short after pressing **<Apply>** button. Though it synchronizes the time automatically, NTP does not update the time periodically without user’s processing.

Time Zone is an offset time off GMT. You have to select the time zone first and then perform time sync via NTP because the switch will combine this time zone offset and updated NTP time to come out the local time, otherwise, you will not able to get the correct time. The switch supports configurable time zone from –12 to +13 step 1 hour.

Default Time zone: +8 Hrs.

Daylight Saving: Daylight saving is adopted in some countries. If set, it will adjust the time lag or in advance in unit of hours, according to the starting date and the ending date. For example, if you set the day light saving to be 1 hour. When the time passes over the starting time, the system time will be increased one hour after one minute at the time since it passed over. And when the time passes over the ending time, the system time will be decreased one hour after one minute at the time since it passed over.

The switch supports valid configurable day light saving time is –5 ~ +5 step one hour. The zero for this parameter means it need not have to adjust current time, equivalent to in-act daylight saving. You don’t have to set the starting/ending date as well. If you set daylight saving to be non-zero, you have to set the starting/ending date as well; otherwise, the daylight saving function will not be activated.

Default for Daylight Saving: 0.

The following parameters are configurable for the function Daylight Saving and described in detail.

Day Light Saving Start:
This is used to set when to start performing the day light saving time.

Mth:	Range is 1 ~ 12.	Default: 1
Day:	Range is 1 ~ 31.	Default: 1
Hour:	Range is 0 ~ 23.	Default: 0

Day Light Saving End:
This is used to set when to stop performing the daylight saving time.

Mth:	Range is 1 ~ 12.	Default: 1
Day:	Range is 1 ~ 31.	Default: 1
Hour:	Range is 0 ~ 23.	Default: 0

2.1.5 Account Configuration

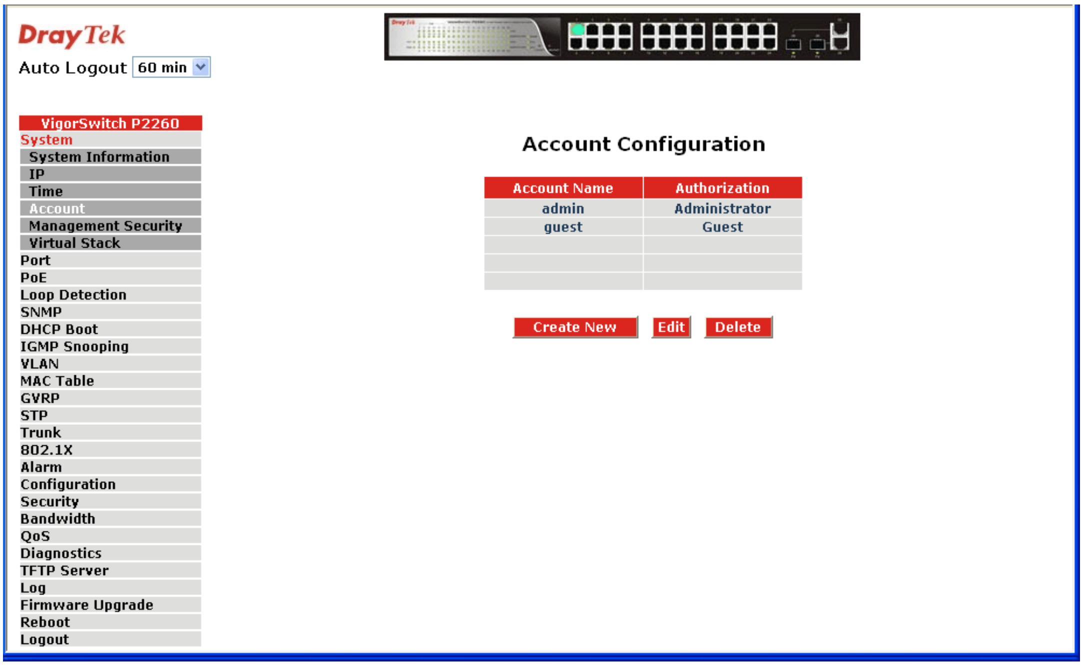
In this function, only administrator can create, modify or delete the username and password. Administrator can modify other guest identities’ password without confirming the password but it is necessary to modify the administrator-equivalent identity. Guest-equivalent identity can modify his password only. Please note that you must confirm administrator/guest identity in the field of Authorization in advance before configuring the username and password. Only one administrator is allowed to exist and unable to be deleted. In addition, up to 4 guest accounts can be created.

The default setting for user account is:

Username:	admin
Password:	admin

The default setting for guest user account is:

Username:	guest
Password:	guest



Account Configuration

Account Name	Authorization
admin	Administrator
guest	Guest

2.1.6 Management Policy

Through the management security configuration, the administrator can do the strict setup to control the switch and limit the user to access this switch.

The following rules are offered for the administrator to manage the switch:

Rule 1) : When no lists exists, then it will accept all connections.

Accept

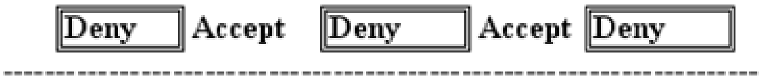
---

Rule 2): When only "accept lists" exist, then it will deny all connections, excluding the connection inside of the accepting range.

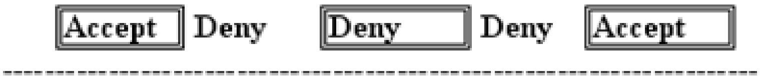
Accept Deny Accept Deny Accept

---

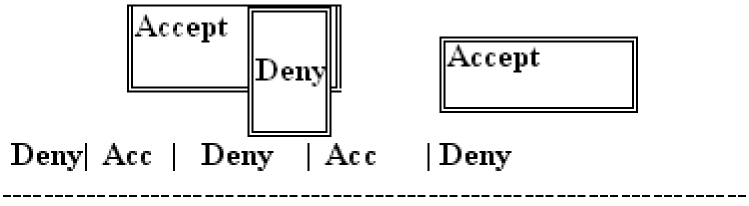
Rule 3): **When only "deny lists" exist, then it will accept all connections, excluding the connection inside of the denying range.**



Rule 4): **When both "accept and deny" lists exist, then it will deny all connections, excluding the connection inside of the accepting range.**



Rule 5): **When both "accept and deny" lists exist, then it will deny all connections, excluding the connection inside of the accepting range and NOT inside of the denying range at the same time.**

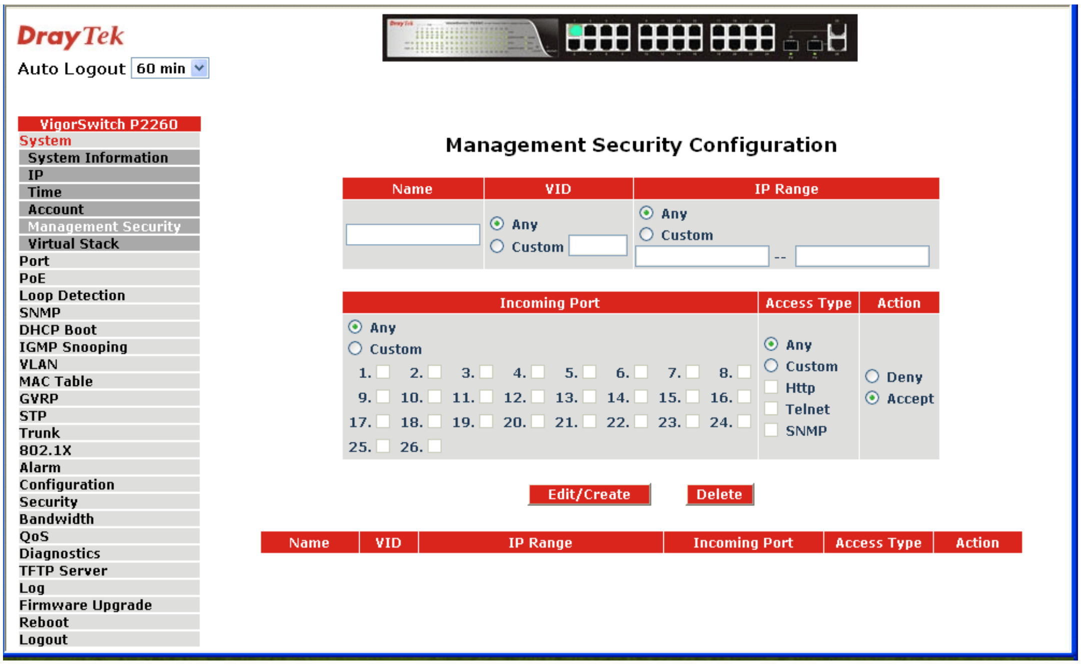


Function name:

Management Security Configuration

Function description:

The switch offers Management Security Configuration function. With this function, the manager can easily control the mode that the user connects to the switch. According to the mode, users can be classified into two types: Those who are able to connect to the switch (Accept) and those who are unable to connect to the switch (Deny). Some restrictions also can be placed on the mode that the user connect to the switch, for example, we can decide that which VLAN VID is able to be accepted or denied by the switch, the IP range of the user could be accepted or denied by the switch, the port that the user is allowed or not allowed to connect with the switch, or the way of controlling and connecting to the switch via Http, Telnet or SNMP.



Management Security Configuration

Name	VID	IP Range
	● Any ○ Custom	● Any ○ Custom --

Incoming Port	Access Type	Action
● Any ○ Custom 1. □ 2. □ 3. □ 4. □ 5. □ 6. □ 7. □ 8. □ 9. □ 10. □ 11. □ 12. □ 13. □ 14. □ 15. □ 16. □ 17. □ 18. □ 19. □ 20. □ 21. □ 22. □ 23. □ 24. □ 25. □ 26. □	● Any ○ Custom □ Http □ Telnet □ SNMP	○ Deny ● Accept

Name	VID	IP Range	Incoming Port	Access Type	Action

Parameter description:

Name: A name is composed of any letter (A-Z, a-z) and digit (0-9) with maximal 8 characters.

VID: The switch supports two kinds of options for managed valid VLAN VID, including “Any” and “Custom”. Default is “Any”. When you choose “Custom”, you can fill in VID number. The valid VID range is 1~4094.

IP Range: The switch supports two kinds of options for managed valid IP Range, including “Any” and “Custom”. Default is “Any”. In case that “Custom” had been chosen, you can assign effective IP range. The valid range is 0.0.0.0~255.255.255.255.

Incoming Port: The switch supports two kinds of options for managed valid Port Range, including “Any” and “Custom”. Default is “Any”. You can select the ports that you would like them to be worked and restricted in the management security configuration if “Custom” had been chosen.

Access Type: The switch supports two kinds of options for managed valid Access Type, including “Any” and “Custom”. Default is “Any”. “Http”, “Telnet” and “SNMP” are three ways for the access and managing the switch in case that” Custom” had been chosen.

Action: The switch supports two kinds of options for managed valid Action Type, including “Deny” and “Accept”. Default is “Deny”. When you choose “Deny” action, you will be restricted and refused to manage the switch due to the “Access Type” you choose. However, while you select “Accept” action, you will have the authority to manage the switch.

Edit/Create: A new entry of Management Security Configuration can be created after the parameters as mentioned above had been

	setup and then press **<Edit/Create>** button. Of course, the existed entry also can be modified by pressing this button.
Delete:	Remove the existed entry of Management Security Configuration from the management security table.

2.1.7 Virtual Stack

Function name:

Virtual Stack

Function description:

Virtual Stack Management (VSM) is the group management function. Through the proper configuration of this function, switches in the same LAN will be grouped automatically. And among these switch, one switch will be a master machine, and the others in this group will become the slave devices.

VSM offers a simple centralized management function. It is not necessary to remember the addresses of all devices, manager is capable of managing the network with knowing the address of the Master machine. Instead of SNMP or Telnet UI, VSM is only available in Web UI. While one switch becomes the Master, two rows of buttons for group device will appear on the top of its Web UI. By pressing these buttons, user will be allowed to connect the Web UI of the devices of the group in the same window without the login of these devices.

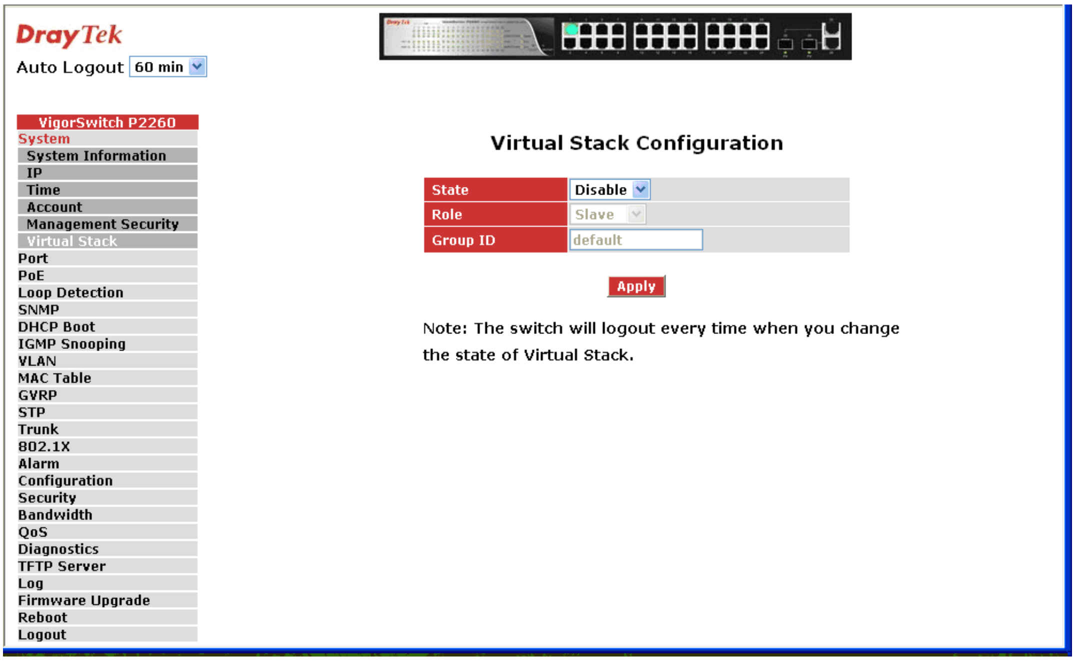
The most top-left button is only for Master device. The background color of the button you press will be changed to represent that the device is under your management.

> **Note:** It will remove the grouping temporarily in case that you login the switch via the console.

The device of the group will be shown as station address (the last number of IP Address) + device name on the button (e.g. 196_GEL2-SW8), otherwise it will show ” ---- “ if no corresponding device exists.

Once the devices join the group successfully, then they are merely able to be managed via Master device, and user will fail to manage them via telnet/console/web individually.

Up to 16 devices can be grouped for VSM, however, only one Master is allowed to exist in each group. For Master redundancy, user may configure more than two devices as the Master device. However, the Master device with the smaller MAC value will be the Master one. All of these 16 devices can become Master device and back up with each other.



Virtual Stack Configuration

State	Disable
Role	Slave
Group ID	default

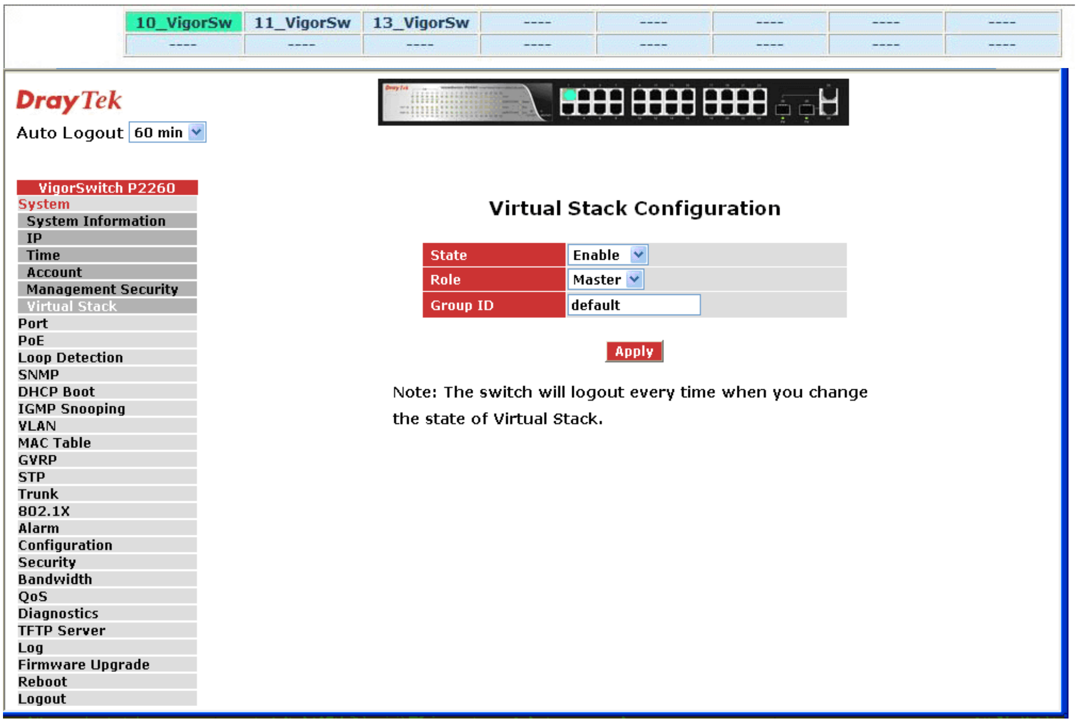
Note: The switch will logout every time when you change the state of Virtual Stack.

Parameter description:

State: It is used for the activation or de-activation of VSM. Default is Disable.

Role: The role that the switch would like to play in virtual stack. Two types of roles, including master and slave are offered for option. Default is Master.

Group ID: It is the group identifier (GID) which signs for VSM. Valid letters are A-Z, a-z, 0-9, “ - “ and “_”   characters. The maximal length is 15 characters



10_VigorSw	11_VigorSw	13_VigorSw	----	----	----	----	----
----	----	----	----	----	----	----	----

Virtual Stack Configuration

State	Enable
Role	Master
Group ID	default

Note: The switch will logout every time when you change the state of Virtual Stack.

2.2 Port Configuration

Four functions, including Port Status, Port Configuration, Simple Counter and Detail Counter are contained in this function folder for port monitor and management. Each of them will be described in detail orderly in the following sections.

2.2.1 Port Status

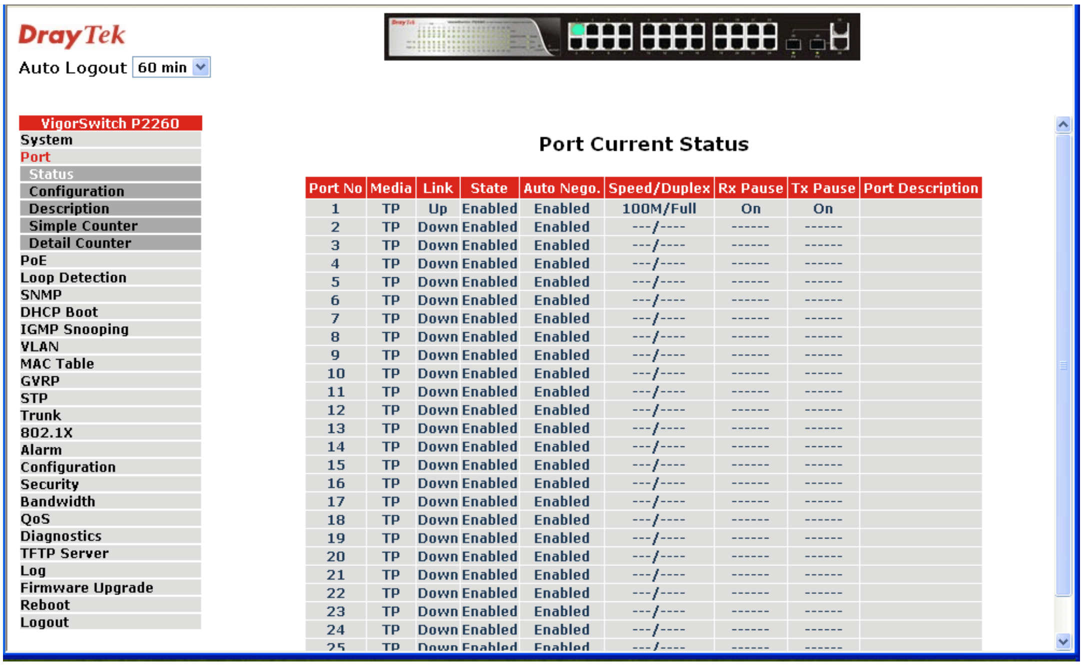
The function Port Status gathers the information of all ports' current status and reports it by the order of port number, media, link status, port state, Auto-Negotiation status, speed/duplex, Rx Pause and Tx Pause. An extra media type information for the module ports 25 and 26 is also offered.

Function name:

Port Status

Function Description:

Report the latest updated status of all ports in this switch. When any one of the ports in the switch changes its parameter displayed in the page, it will be automatically refreshed the port current status about every 5 seconds.



Port Current Status

Port No	Media	Link	State	Auto Nego.	Speed/Duplex	Rx Pause	Tx Pause	Port Description
1	TP	Up	Enabled	Enabled	100M/Full	On	On	
2	TP	Down	Enabled	Enabled	---/----	------	------	
3	TP	Down	Enabled	Enabled	---/----	------	------	
4	TP	Down	Enabled	Enabled	---/----	------	------	
5	TP	Down	Enabled	Enabled	---/----	------	------	
6	TP	Down	Enabled	Enabled	---/----	------	------	
7	TP	Down	Enabled	Enabled	---/----	------	------	
8	TP	Down	Enabled	Enabled	---/----	------	------	
9	TP	Down	Enabled	Enabled	---/----	------	------	
10	TP	Down	Enabled	Enabled	---/----	------	------	
11	TP	Down	Enabled	Enabled	---/----	------	------	
12	TP	Down	Enabled	Enabled	---/----	------	------	
13	TP	Down	Enabled	Enabled	---/----	------	------	
14	TP	Down	Enabled	Enabled	---/----	------	------	
15	TP	Down	Enabled	Enabled	---/----	------	------	
16	TP	Down	Enabled	Enabled	---/----	------	------	
17	TP	Down	Enabled	Enabled	---/----	------	------	
18	TP	Down	Enabled	Enabled	---/----	------	------	
19	TP	Down	Enabled	Enabled	---/----	------	------	
20	TP	Down	Enabled	Enabled	---/----	------	------	
21	TP	Down	Enabled	Enabled	---/----	------	------	
22	TP	Down	Enabled	Enabled	---/----	------	------	
23	TP	Down	Enabled	Enabled	---/----	------	------	
24	TP	Down	Enabled	Enabled	---/----	------	------	
25	TP	Down	Enabled	Enabled	---/----	------	------	

Parameter Description:

Port No: Display the port number. The number is 1 – 26. Both port 25 and 26 are optional modules.

Media: Show the media type adopted in all ports. The Port 25 and Port 26 are optional modules, which support either fiber or UTP media with either Gigabit Ethernet (1000Mbps) or 10/100Mbps Fast Ethernet port. They may have different media types and speed. Especially, fiber port has comprehensive types of connector, distance, fiber mode and so on. The switch describes the module ports with the following page.

Link: Show that if the link on the port is active or not. If the link is connected to a working-well device, the Link will show the link “Up”; otherwise, it will show “Down”. This is determined by the hardware on both devices of the connection. No default value.

State: Show that the communication function of the port is “Enabled” or “Disabled”. When it is enabled, traffic can be transmitted and received via this port. When it is disabled, no traffic can be transferred through this port. Port State is configured by user.

Default: Enabled.

Auto Nego.: Show the exchange mode of Ethernet MAC. There are two modes supported in the switch. They are auto-negotiation mode “Enabled” and forced mode “Disabled”. When in “Enabled” mode, this function will automatically negotiate by hardware itself and exchange each other the capability of speed and duplex mode with other site which is linked, and comes out the best communication way. When in “Disabled” mode, both parties must have the same setting of speed and duplex, otherwise, both of them will not be linked. In this case, the link result is “Down”.

Default: Enabled

Speed / Duplex Mode: Display the speed and duplex of all port. There are three speeds 10Mbps, 100Mbps and 1000Mbps supported for TP media, and the duplex supported is half duplex and full duplex. If the media is 1Gbps fiber, it is 1000Mbps supported only. The status of speed/duplex mode is determined by 1) the negotiation of both local port and link partner in “Auto Speed” mode or 2) user setting in “Force” mode. The local port has to be preset its capability.

In port 1 – 24, they are supported Fast Ethernet with TP media only, so the result will show 100M/Full or 100M/Half, 10M/Full and 10M/Half duplex.

In port 25 and port 26, if the media is 1000Mbps with TP media, it will show the combinations of 10/100M and Full/Half duplex, 1000Mbps and Full duplex only. If the media is 1000Mbps with fiber media, it will show only 1000M/Full duplex.

RX Pause: The way that the port adopts to process the PAUSE frame. If it shows “on”, the port will care the PAUSE frame; otherwise, the port will ignore the PAUSE frame.
Default: None

Tx Pause: It decides that whether the port transmits the PAUSE frame or not. If it shows “on”, the port will send PAUSE frame; otherwise, the port will not send the PAUSE frame.
Default: None

Port Description: General information for that port.

2.2.2 Port Configuration

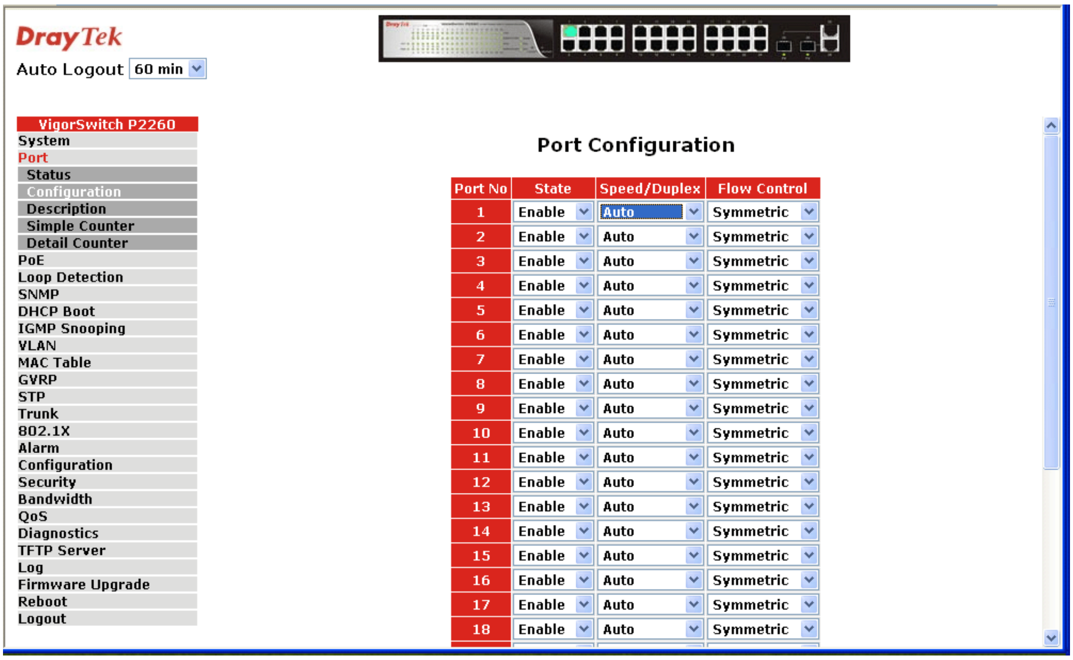
Port Configuration is applied to change the setting of each port. In this configuration function, you can set/reset the following functions. All of them are described in detail below.

Function name:

Port Configuration

Function description:

It is used to set each port’s operation mode. The switch supports 3 parameters for each port. They are state, mode and flow control.



Auto Logout 60 min

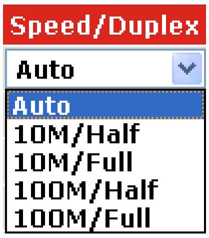
Port Configuration

Port No	State	Speed/Duplex	Flow Control
1	Enable	Auto	Symmetric
2	Enable	Auto	Symmetric
3	Enable	Auto	Symmetric
4	Enable	Auto	Symmetric
5	Enable	Auto	Symmetric
6	Enable	Auto	Symmetric
7	Enable	Auto	Symmetric
8	Enable	Auto	Symmetric
9	Enable	Auto	Symmetric
10	Enable	Auto	Symmetric
11	Enable	Auto	Symmetric
12	Enable	Auto	Symmetric
13	Enable	Auto	Symmetric
14	Enable	Auto	Symmetric
15	Enable	Auto	Symmetric
16	Enable	Auto	Symmetric
17	Enable	Auto	Symmetric
18	Enable	Auto	Symmetric

Parameter description:

State: Set the communication capability of the port is Enabled or Disabled. When enabled, traffic can be transmitted and received via this port. When disabled, the port is blocked and no traffic can be transferred through this port. Port State is configurable by the user. There are only two states “Enable” and “Disable” able to choose. If you set a port’s state “Disable”, then that port is prohibited to pass any traffic, even it looks Link up.
Default: Enable.

Speed/Duplex: Set the speed and duplex of the port. In speed, 10/100Mbps baud rate is available for Fast Ethernet, Gigabit module in port 25, 26. If the media is 1Gbps fiber, it is always 1000Mbps and the duplex is full only. If the media is TP, the Speed/Duplex is comprised of the combination of speed mode, 10/100/1000Mbps, and duplex mode, full duplex and half duplex. The following table summarized the function the media supports.



Media type	NWay	Speed	Duplex
100M TP	ON/OFF	10/100M	Full/Half
1000M TP	ON/OFF	10/100/1000M	Full for all, Half for 10/100
1000M Fiber	ON/OFF	1000M	Full

In Auto-negotiation mode, no default value. In Forced mode, default value depends on your setting.

Flow Control:

There are two modes to choose in flow control, including Symmetric and Asymmetric. If flow control is set Symmetric, both parties can send PAUSE frame to the transmitting device(s) if the receiving port is too busy to handle. When it is set Asymmetric, this will let the receiving port care the PAUSE frame from transmitting device(s), but it doesn’t send PAUSE frame. This is one-way flow control. Default: Symmetric.

2.2.3 Simple Counter

The function of Simple Counter collects any information and provides the counting about the traffic of the port, no matter the packet is good or bad.

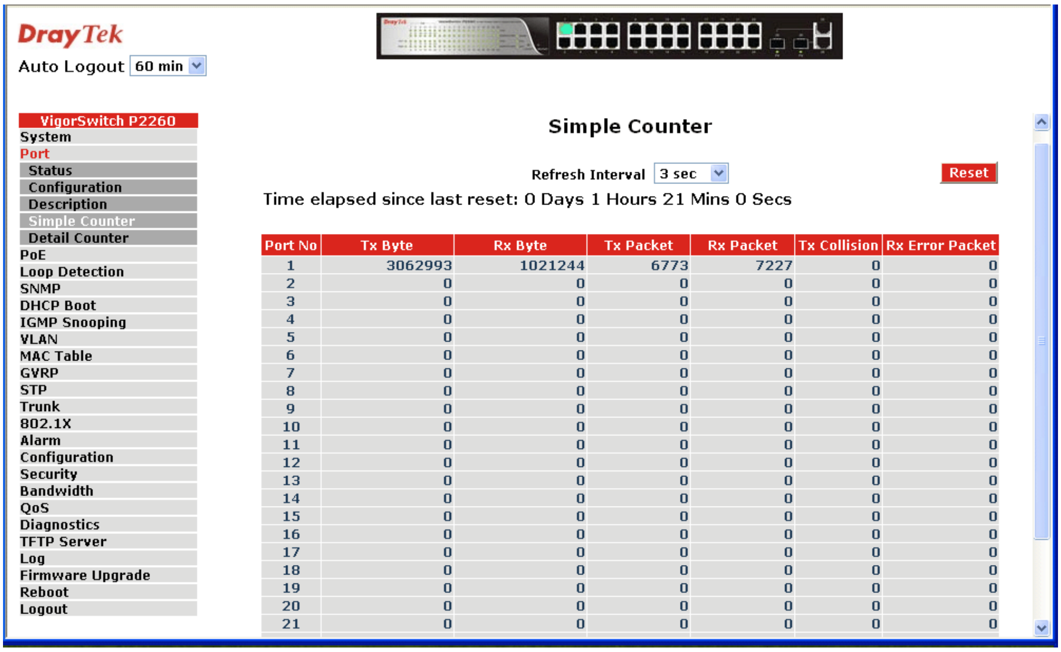
In the following figure, the window can show all ports’ counter information at the same time. Each data field has 20-digit long. If the counting is overflow, the counter will be reset and restart counting. The data is updated every time interval defined by the user. The valid range is 3 to 10 seconds. The Refresh Interval is used to set the update frequency. Default update time is 3 seconds.

Function name:

Simple Counter

Function description:

Display the summary counting of each port’s traffic, including Tx Byte, Rx Byte, Tx Packet, Rx Packet, Tx Collision and Rx Error Packet.



Simple Counter

Refresh Interval 3 sec

Time elapsed since last reset: 0 Days 1 Hours 21 Mins 0 Secs

Port No	Tx Byte	Rx Byte	Tx Packet	Rx Packet	Tx Collision	Rx Error Packet
1	3062993	1021244	6773	7227	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0
11	0	0	0	0	0	0
12	0	0	0	0	0	0
13	0	0	0	0	0	0
14	0	0	0	0	0	0
15	0	0	0	0	0	0
16	0	0	0	0	0	0
17	0	0	0	0	0	0
18	0	0	0	0	0	0
19	0	0	0	0	0	0
20	0	0	0	0	0	0
21	0	0	0	0	0	0

Parameters description:

Tx Byte: Total transmitted bytes.

Rx Byte: Total received bytes.

Tx Packet: The counting number of the packet transmitted.

Rx Packet: The counting number of the packet received.

Tx Collision: Number of collisions transmitting frames experienced.

Rx Error Packet: Number of bad packets received.

2.2.4 Detail Counter

The function of Detail Counter collects any information and provides the counting about the traffic of the port, no matter the packet is good or bad.

In the following figure, the window can show only one port counter information at the same time. To see another port’s counter, you have to pull down the list of Select, then you will see the figures displayed about the port you had chosen.

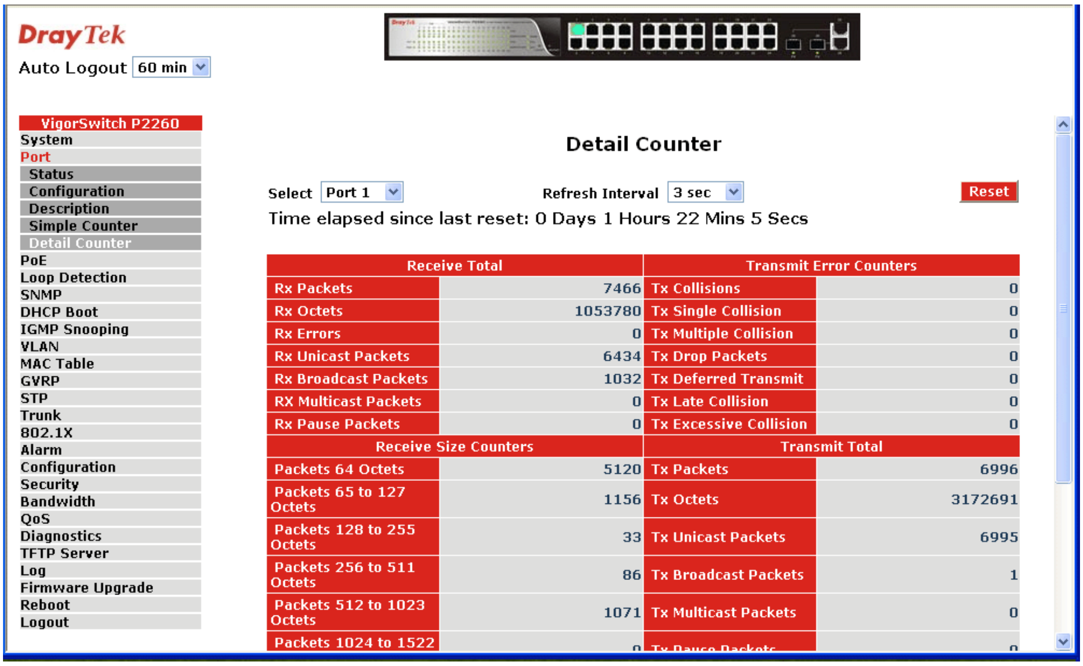
Each data field has 20-digit long. If the counting is overflow, the counter will be reset and restart counting. The data is updated every time interval defined by the user. The valid range is 3 to 10 seconds. The Refresh Interval is used to set the update frequency. Default update time is 3 seconds.

Function name:

Detail Counter

Function description:

Display the detailed counting number of each port’s traffic. In the Fig. 3-14, the window can show all counter information of each port at one time.



Detail Counter

Select Port 1 Refresh Interval 3 sec

Time elapsed since last reset: 0 Days 1 Hours 22 Mins 5 Secs

Receive Total		Transmit Error Counters	
Rx Packets	7466	Tx Collisions	0
Rx Octets	1053780	Tx Single Collision	0
Rx Errors	0	Tx Multiple Collision	0
Rx Unicast Packets	6434	Tx Drop Packets	0
Rx Broadcast Packets	1032	Tx Deferred Transmit	0
RX Multicast Packets	0	Tx Late Collision	0
Rx Pause Packets	0	Tx Excessive Collision	0
Receive Size Counters		**Transmit Total**	
Packets 64 Octets	5120	Tx Packets	6996
Packets 65 to 127 Octets	1156	Tx Octets	3172691
Packets 128 to 255 Octets	33	Tx Unicast Packets	6995
Packets 256 to 511 Octets	86	Tx Broadcast Packets	1
Packets 512 to 1023 Octets	1071	Tx Multicast Packets	0
Packets 1024 to 1522	0	Tx Pause Packets	0

Parameter description:

Rx Unicast Packets: The counting number of the packet received.

Rx Octets: Total received bytes.

Rx Errors: Number of bad packets received.

Rx Unicast Packets: Show the counting number of the received unicast packet.

Rx Broadcast Packets: Show the counting number of the received broadcast packet.

Rx Multicast Packets: Show the counting number of the received multicast packet.

Rx Pause Packets: Show the counting number of the received pause packet.

Tx Collisions: Number of collisions transmitting frames experienced.

Tx Single Collision: Number of frames transmitted that experienced exactly one collision.

Tx Multiple Collision: Number of frames transmitted that experienced more than one collision.

Tx Drop Packets: Number of frames dropped due to excessive collision, late collision, or frame aging.

Tx Deferred Transmit: Number of frames delayed to transmission due to the medium is busy.

Tx Late Collision: Number of times that a collision is detected later than 512 bit-times into the transmission of a frame.

Tx Excessive Collision: Number of frames that are not transmitted because the frame experienced 16 transmission attempts.

Packets 64 Octets: Number of 64-byte frames in good and bad packets received.

Packets 65-127 Octets: Number of 65 ~ 127-byte frames in good and bad packets received.

Packets 128-255 Octets: Number of 128 ~ 255-byte frames in good and bad packets received.

Packets 256-511 Octets: Number of 256 ~ 511-byte frames in good and bad packets received.

Packets 512-1023 Octets: Number of 512 ~ 1023-byte frames in good and bad packets received.

Packets 1024- 1522 Octets: Number of 1024-1522-byte frames in good and bad packets received.

Tx Packets: The counting number of the packet transmitted.

TX Octets: Total transmitted bytes.

Tx Unicast Packets: Show the counting number of the transmitted unicast packet.

Tx Broadcast Packets: Show the counting number of the transmitted broadcast packet.

Tx Multicast Packets: Show the counting number of the transmitted multicast packet.

Tx Pause Packets: Show the counting number of the transmitted pause packet.

Rx FCS Errors: Number of bad FSC packets received.

Rx Alignment Errors: Number of Alignment errors packets received.

Rx Fragments: Number of short frames (< 64 bytes) with invalid CRC.

Rx Jabbers: Number of long frames(according tomax_length register) with invalid CRC.

Rx Drop Packets: Frames dropped due to the lack of receiving buffer.

Rx Undersize Packets: Number of short frames (<64 Bytes) with valid CRC.

Rx Oversize Packets: Number of long frames(according to max_length register) with valid CRC.

2.3 POE Configuration

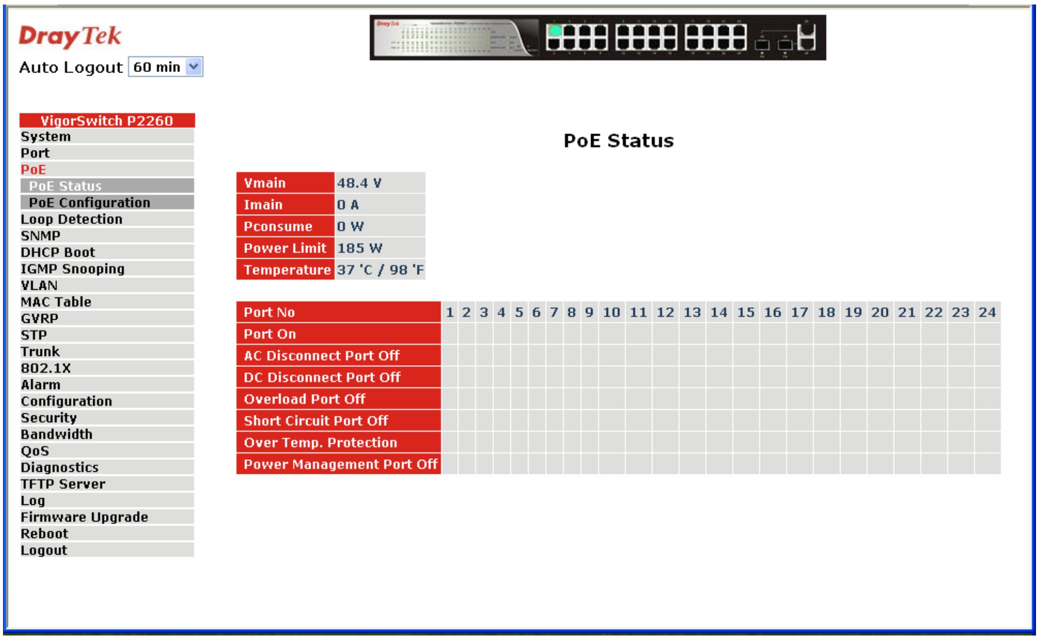
2.3.1 POE Status

Function name:

POE Status

Function description:

Display the information about the PoE status.



PoE Status

Vmain	48.4 V
Imain	0 A
Pconsume	0 W
Power Limit	185 W
Temperature	37 'C / 98 'F

Port No	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Port On																								
AC Disconnect Port Off																								
DC Disconnect Port Off																								
Overload Port Off																								
Short Circuit Port Off																								
Over Temp. Protection																								
Power Management Port Off																								

Parameter description:

Vmain: It displays what volt was supplied by the Switch.

Imain: The sum of the current that every port supplies.

Pconsume: The sum of the power that every port supplies.

Power Limit: The maximal power that the switch can supply (Read Only).

Temperature: The temperature of the chip on PoE.

Port No: Port number.

Port On: Show whether the port is supplying the power to the PD or not.

AC Disconnect Port Off: Port is turned off due to the AC Disconnect function.

DC Disconnect Port Off: Port is turned off due to the DC Disconnect function.

Overload Port Off: The switch will stop supplying the power to the port due to the power required by the PD that is linked to the port on the switch excesses the Class setting of the PD.

Short Circuit Port Off: The switch will stop supplying the power to the port if it detects that the PD linked to the port is short circuit.

Over Temp. Protection: The port of the switch will be disabled due to fast transient rise in temperature to 240^{o}C or slow rise in temperature to 200^{o}C.

Power Management Port Off: Due to total power required by all PDs linked to the switch excesses the power limit, so the switch stops supplying the power to this port after referring to the information of the priority.

2.3.2 POE Configuration

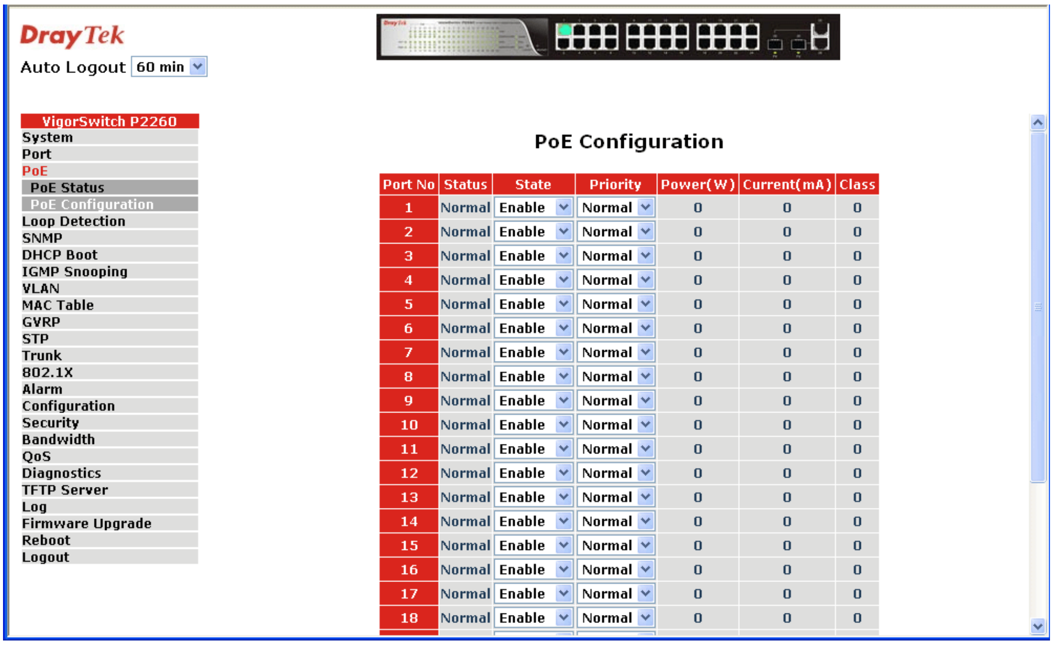
Function name:

POE Configuration

Function description:

In PoE Port Management function, user can configure the settings about PoE.

The switch complies with IEEE 802.3af protocol and be capable of detecting automatically that whether the device linked to the port on the switch is PD (Powered Device) or not. The switch also manage the power supplement based on the Class of the PD, and it will stop supplying the power once the power required by the PD excesses the Class, Short Circuit or over temperature occurs.



Auto Logout 60 min

PoE Configuration

Port No	Status	State	Priority	Power(W)	Current(mA)	Class
1	Normal	Enable	Normal	0	0	0
2	Normal	Enable	Normal	0	0	0
3	Normal	Enable	Normal	0	0	0
4	Normal	Enable	Normal	0	0	0
5	Normal	Enable	Normal	0	0	0
6	Normal	Enable	Normal	0	0	0
7	Normal	Enable	Normal	0	0	0
8	Normal	Enable	Normal	0	0	0
9	Normal	Enable	Normal	0	0	0
10	Normal	Enable	Normal	0	0	0
11	Normal	Enable	Normal	0	0	0
12	Normal	Enable	Normal	0	0	0
13	Normal	Enable	Normal	0	0	0
14	Normal	Enable	Normal	0	0	0
15	Normal	Enable	Normal	0	0	0
16	Normal	Enable	Normal	0	0	0
17	Normal	Enable	Normal	0	0	0
18	Normal	Enable	Normal	0	0	0

Parameter description:

Status: Include “Normal” or “Active” two kinds of status. The former means the port is ready to link and supply the power to the PD at any time. The latter means the port is in the condition of supplying the power.

State: “Enable” means the manager allows the power supplied to the PD is legal while the port linked to the PD; “Disable” means the port does not own PoE function.

Priority: Three options are offered for the user to choose, including Normal, Low and High. Default is Normal. The switch will stop supplying the power to the port based on the order of the priority Low→Normal→High in case total power required by all PDs linked to the switch excesses the power limit. As the ports have the same priority, then the switch will cease the power supplement from the port with the highest port id (12→1).

Power(W): The power is consumed by the port.

Current(mA): The current is supplied to the PD by the port.

Class: The Class of the PD linked to the port of the switch.

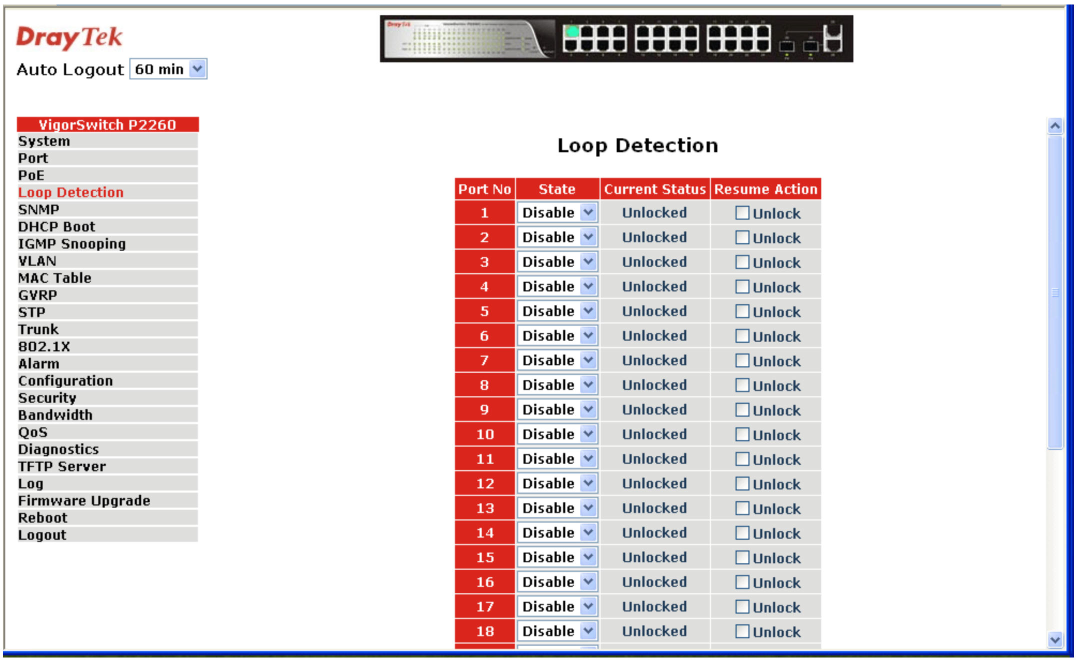
2.4 Loop Detection

Function name:

Loop Detection

Function description:

The switch will send out looping detection frame to detect the ports on the switch whether they have looping traffic happen. When the switch port receives the looping detection frame from itself, it means there is looping happen in the network. The looping ports will be locked to avoid the looping storm causing all traffic be blocked.



Auto Logout 60 min

Loop Detection

Port No	State	Current Status	Resume Action
1	Disable	Unlocked	□Unlock
2	Disable	Unlocked	□Unlock
3	Disable	Unlocked	□Unlock
4	Disable	Unlocked	□Unlock
5	Disable	Unlocked	□Unlock
6	Disable	Unlocked	□Unlock
7	Disable	Unlocked	□Unlock
8	Disable	Unlocked	□Unlock
9	Disable	Unlocked	□Unlock
10	Disable	Unlocked	□Unlock
11	Disable	Unlocked	□Unlock
12	Disable	Unlocked	□Unlock
13	Disable	Unlocked	□Unlock
14	Disable	Unlocked	□Unlock
15	Disable	Unlocked	□Unlock
16	Disable	Unlocked	□Unlock
17	Disable	Unlocked	□Unlock
18	Disable	Unlocked	□Unlock

Parameter description:

Port: User can set up the port (1~26) respectively to set loop detection.

State: Enable or Disable the port loop detection. When it is enabled, the port will send out loop detection frame and detect if any loop happens. When it is disabled, the port can detect only when the loop happens. Default: Disable.

Current Status: Show current status of this port. Unlocked means there is no loop happened for this port. Locked means there is loop happened in this port and that port is blocked.

Resume Action: You can use resume action to unlock the locked port when you make sure the looping issue has been resolved. You also can remove the locked port cable then reconnect the cable to resume the locked port.

Action: Start loop detection.

2.5 SNMP Configuration

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. SNMP agent is running on the switch to response the request issued by SNMP manager.

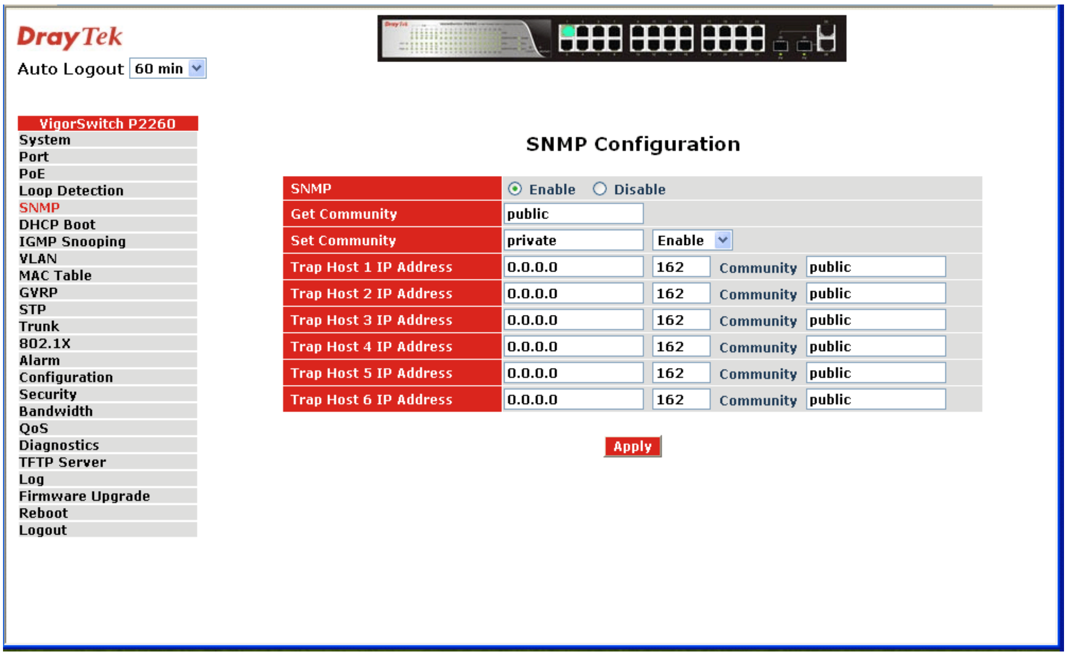
Basically, it is passive except issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP “Enable”, SNMP agent will be started up. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set “Disable”, SNMP agent will be de-activated, the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

Function name:

SNMP Configuration

Function description:

This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP. A SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So, both parties must have the same community name. Once completing the setting, click <**Apply**> button, the setting takes effect.



SNMP Configuration

SNMP	● Enable ○ Disable			
Get Community	public			
Set Community	private	Enable		
Trap Host 1 IP Address	0.0.0.0	162	Community	public
Trap Host 2 IP Address	0.0.0.0	162	Community	public
Trap Host 3 IP Address	0.0.0.0	162	Community	public
Trap Host 4 IP Address	0.0.0.0	162	Community	public
Trap Host 5 IP Address	0.0.0.0	162	Community	public
Trap Host 6 IP Address	0.0.0.0	162	Community	public

Parameters description:

SNMP:

The term SNMP here is used for the activation or de-activation of SNMP. Default is Enable.

Get/Set/Trap Community:

Community name is used as password for authenticating if the requesting network management unit belongs to the same community group. If they both don’t have the same community name, they don’t belong to the same group. Hence, the requesting network management unit can not access the device with different community name via SNMP protocol; If they both have the same community name, they can talk each other.

Community name is user-definable with a maximum length of 15 characters and is case sensitive. There is not allowed to put any blank in the community name string. Any printable character is allowable.

The community name for each function works independently. Each function has its own community name. Say, the community name for GET only works for GET function and can’t be applied to other function such as SET and Trap.

Default SNMP function: Enable

Default community name for GET: public

Default community name for SET: private

Default community name for Trap: public

Default Set function: Enable

Default trap host IP address: 0.0.0.0

Default port number:162

Trap:

In the switch, there are 6 trap hosts supported. Each of them has its own community name and IP address; is user-definable. To set up a trap host means to create a trap manager by assigning an IP address to host the trap message. In other words, the trap host is a network management unit with SNMP manager receiving the trap message from the managed switch with SNMP agent issuing the trap message. 6 trap hosts can prevent the important trap message from losing.

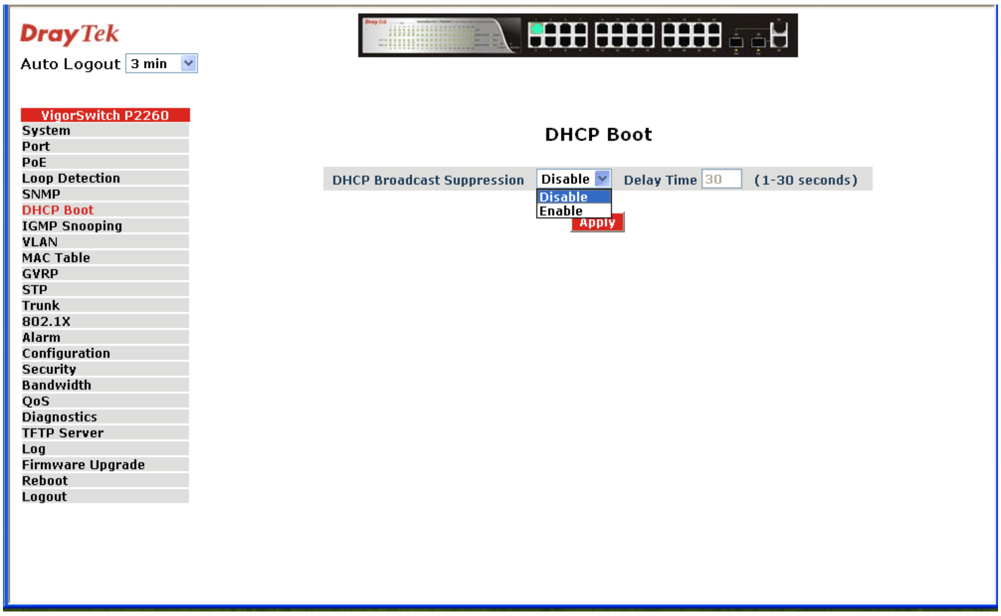
For each public trap, the switch supports the trap event Cold Start, Warm Start, Link Down, Link Up and Authentication Failure Trap. They can be enabled or disabled individually. When enabled, the corresponded trap will actively send a trap message to the trap host when a trap happens. If all public traps are disabled, no public trap message will be sent. As to the Enterprise (no. 6) trap is classified as private trap, which are listed in the Trap Alarm Configuration function folder.

Default for all public traps: Enable.

2.6 DHCP Boot

The DHCP Boot function is used to spread the request broadcast packet into a bigger time frame to prevent the traffic congestion due to broadcast packets from many network devices which may seek its NMS, boot server, DHCP server and many connections predefined when the whole building or block lose the power and then reboot and recover. At this moment, a bunch of switch or other network device on the LAN will try its best to find the server to get the services or try to set up the predefined links, they will issue many broadcast packets in the network.

The switch supports a random delay time for DHCP and boot delay for each device. This suppresses the broadcast storm while all devices are at booting stage in the same time. The maximum user-defined delay time is 30 sec. If DHCP Broadcasting Suppression function is enabled, the delay time is set randomly, ranging from 0 to 30 seconds, because the exactly delay time is computed by the switch itself. The default is “Disable”.



DHCP Boot

DHCP Broadcast Suppression: Disable

Delay Time: 30 (1-30 seconds)

2.7 IGMP Snooping

The function, IGMP Snooping, is used to establish the multicast groups to forward the multicast packet to the member ports, and, in nature, avoids wasting the bandwidth while IP multicast packets are running over the network. This is because a switch that does not support IGMP or IGMP Snooping can not tell the multicast packet from the broadcast packet, so it can only treat them all as the broadcast packet. Without IGMP Snooping, the multicast packet forwarding function is plain and nothing is different from broadcast packet.

A switch supported IGMP Snooping with the functions of query, report and leave, a type of packet exchanged between IP Multicast Router/Switch and IP Multicast Host, can update the information of the Multicast table when a member (port) joins or leaves an IP Multicast Destination Address. With this function, once a switch receives an IP multicast packet, it will forward the packet to the members who joined in a specified IP multicast group before.

The packets will be discarded by the IGMP Snooping if the user transmits multicast packets to the multicast group that had not been built up in advance.

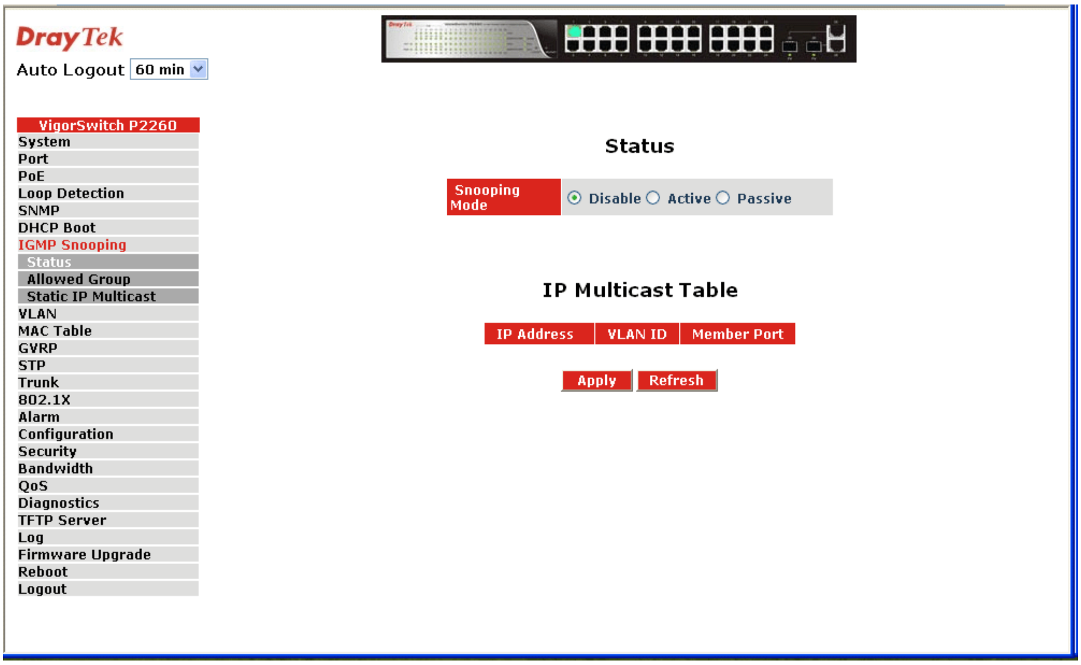
2.7.1 IGMP Snooping - Status

Function name:

IGMP Snooping Status

Function description:

IGMP is used to snoop the status of IP multicast groups and display its associated information in both tagged VLAN and non-tagged VLAN networks. Enabling IGMP with either passive or active mode, you can monitor the IGMP snooping information, which contains the multicast member list with the multicast groups, VID and member port.



Snooping Mode ● Disable ○ Active ○ Passive

Parameter description:

Snooping Mode: The switch supports three kinds of IGMP Snooping status, including “Passive”, “Active” and “Disable”.

Disable -
Set “Disable” mode to disable IGMP Snooping function.
Default: Disable

Active -
In Active mode, IGMP snooping switch will periodically issue the Membership Query message to all hosts attached to it and gather the Membership report message to update the database of the Multicast table. By the way, this also reduces the unnecessary multicast traffic.

Passive -
In Passive Snooping mode, the IGMP snooping will not periodically poll the hosts in the groups. The switch will send a Membership Query message to all hosts only when it has received a Membership Query message from a router.

IP Address: Show all multicast groups IP addresses that are registered on this device.

VLAN ID: Show VLAN ID for each multicast group.

Member Port: Show member ports that join each multicast group. Member port may be only or more than one.

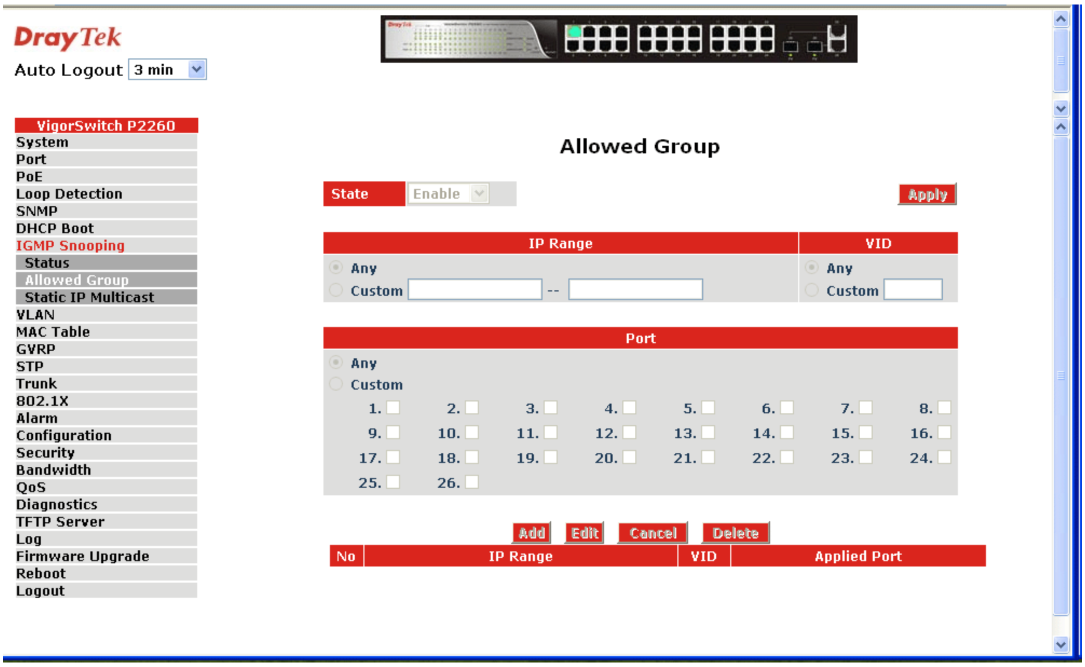
2.7.2 Allowed Group

Function name:

Allowed Group

Function description:

The Allowed Group function allows the IGMP Snooping to set up the IP multicast table based on user's specific conditions. IGMP report packets that meet the items you set up will be joined or formed the multicast group.



Auto Logout 3 min

State Enable

Parameter description:

IP Range: The switch supports two kinds of options for managed valid IP range, including "Any" and "Custom". Default is "Any". In case that "Custom" had been chosen, you can assigned effective IP range. The valid range is 224.0.0.0~239.255.255.255.

VID: The switch supports two kinds of options for managed valid VLAN VID, including "Any" and "Custom". Default is "Any". When you choose "Custom", you can fill in VID number. The valid VID range is 1~4094.

Port: The switch supports two kinds of options for managed valid port range, including "Any" and "Custom". Default is "Any". You can select the ports that you would like them to be worked and restricted in the allowed group configuration if "Custom" had been chosen.

Add: A new entry of allowed group configuration can be created after the parameters as mentioned above had been setup and then press <**Add**> button.

Edit: The existed entry also can be modified after pressing <**Edit**> button.

Delete: Remove the existed entry of allowed group configuration from the allowed group.

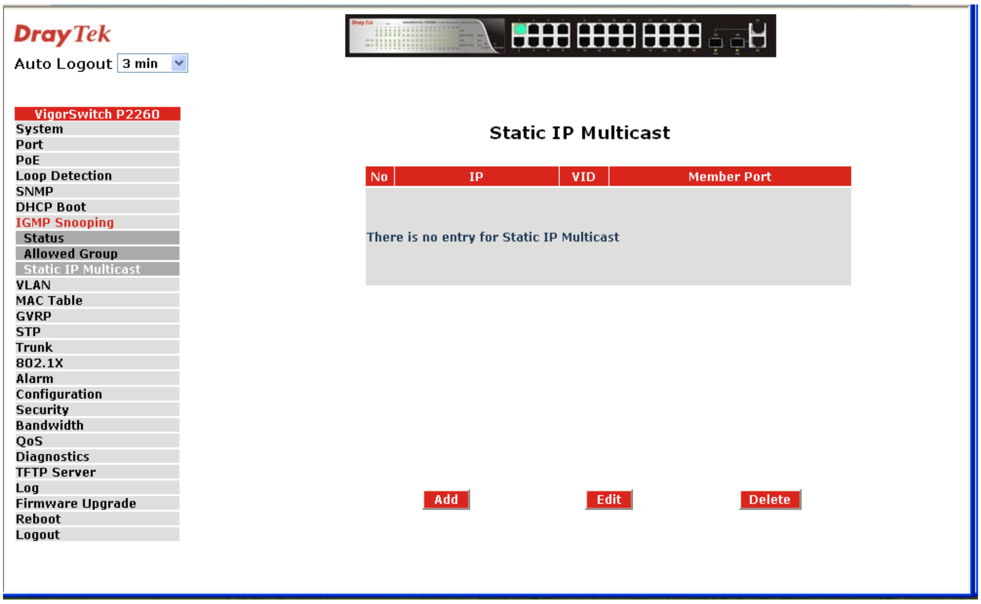
2.7.3 Static IP Multicast

Function name:

Static IP Multicast

Function description:

Set static IP Multicast Group entry for IGMP snooping that you need to configure static group membership entries on an interface. It includes IP address, VID and member port.



Static IP Multicast

No	IP	VID	Member Port

There is no entry for Static IP Multicast

Parameter description:

No.: The entry number.

IP: Set Multicast groups IP addresses that are registered on this device.

VID: Set VLAN ID for each multicast group.

Member Port: Set member ports that join each multicast group. Member port may be only or more than one.

Add: Create a new Static IP Multicast group entry.

Edit: Modify a Static IP Multicast group entry.

Delete: Remove a static IP Multicast group entry.

2.8 VLAN

The switch supports Tag-based VLAN (802.1q) and Port-based VLAN. Support 256 active VLANs and VLAN ID 1~4094. VLAN configuration is used to partition your LAN into small ones as your demand. Properly configuring it, you can gain not only improving security and increasing performance but greatly reducing VLAN management.

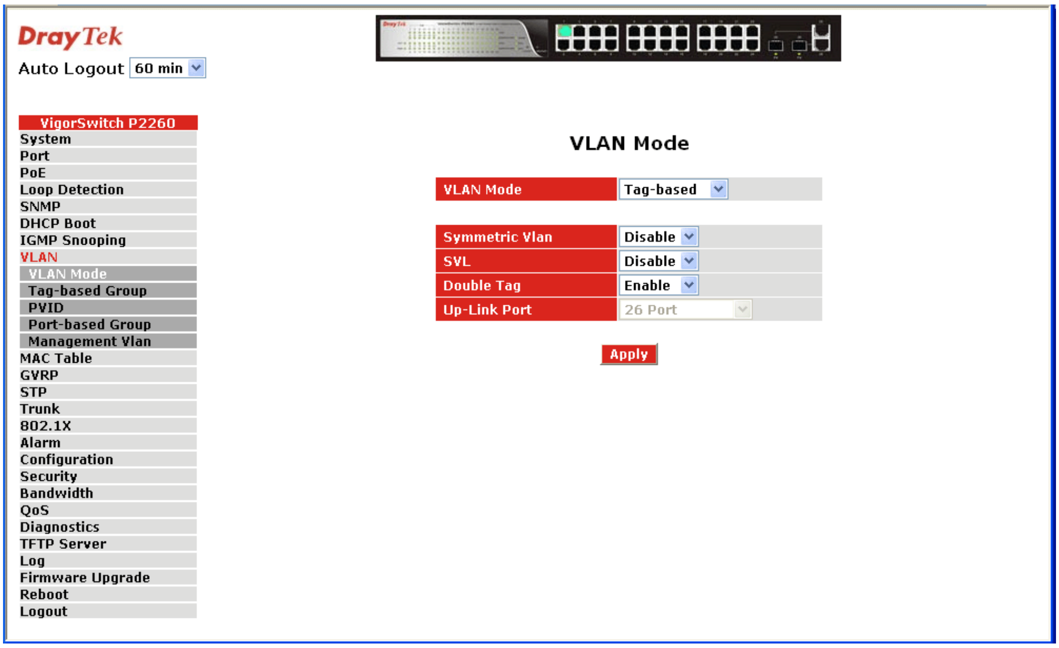
2.8.1 VLAN Mode

Function name:

VLAN Mode Setting

Function description:

The VLAN Mode Selection function includes five modes: Port-based, Tag- based, Metro Mode, Double-tag and Disable, you can choose one of them by pulling down list and selecting an item. Then, click <**Apply**> button, the settings will take effect immediately.

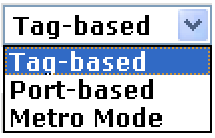


VLAN Mode

VLAN Mode	Tag-based
Symmetric Vlan	Disable
SVL	Disable
Double Tag	Enable
Up-Link Port	26 Port

Parameter description:

VLAN Mode:



Port-based -
Port-based VLAN is defined by port. Any packet coming in or outgoing from any one port of a port-based VLAN will be accepted. No filtering criterion applies in port-based VLAN. The only criterion is the physical port you connect to. For example, for a port-based VLAN named PVLAN-1 contains port members Port 1&2&3&4. If you are on the port 1, you can communicate with port 2&3&4. If you are on the port 5, then you cannot talk to them. Each port-based VLAN you built up must be assigned a group name. This switch can support up to maximal 8 port-based VLAN groups.

Tag-based -
Tag-based VLAN identifies its member by VID. This is quite different from port-based VLAN. If there are any more rules in ingress filtering list or egress filtering list, the packet will be screened with more filtering criteria to determine if it can be forwarded. The switch supports supplement of 802.1q.

Each tag-based VLAN you built up must be assigned VLAN name and VLAN ID. Valid VLAN ID is 1-4094. User can create total up to 64 Tag VLAN groups.

Metro Mode -
The Metro Mode is a quick configuration VLAN environment method on Port-based VLAN. It will create 6 or 7 Port-based VLAN groups.

Symmetric Vlan

This is a Ingress Rule (Rule 1, The Ingress Filtering Rule 1 is “forward only packets with VID matching this port’s configured VID”.). For example, if port 1 receives a tagged packet with VID=100 (VLAN name=VLAN100), and if Symmetric-Vlan function is enabled, the switch will check if port 1 is a member of VLAN100. If yes, the received packet is forwarded; otherwise, the received packet is dropped.

> Note: If Symmetric is enabled and port 1, for example, receives an untagged packet, the switch will apply the PVID of port 1 to tag this packet, the packet then will be forwarded. But if the PVID of port 1 is not 100, the packet will be dropped.

SVL

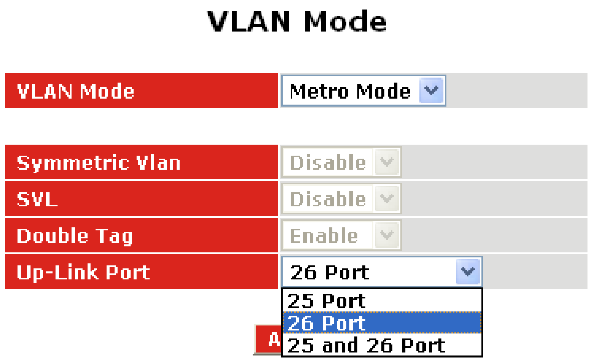
While SVL is enable, all VLANs use the same filtering database storing the membership information of the VLAN to learn or look up the membership information of the VLAN. While SVL is disable, it means learning mode is IVL. In this mode, different VLAN uses different filtering database storing the membership information of the VLAN to learn or look up the information of a VLAN member.

Double Tag

Double-tag mode belongs to the tag-based mode, however, it would treat all frames as the untagged ones, which means that tag with PVID will be added into all packets. Then, these packets will be forwarded as Tag-based VLAN. So, the incoming packets with tag will become the double-tag ones.

Up-link Port:

This function is enabled only when metro mode is chosen in VLAN mode.



VLAN Mode

VLAN Mode: Metro Mode

Symmetric Vlan: Disable

SVL: Disable

Double Tag: Enable

Up-Link Port: 26 Port

25 -
Except Port 25, each port of the switch cannot transmit packets with each other. Each port groups a VLAN with Port 25, thus, total 25 groups consisting of 2 members are formed.
26 -
Except Port 8, each port of the switch cannot transmit packets with each other. Each port groups a VLAN with Port 8, thus, total 26 groups consisting of 2 members are formed.
25 and 26 Port -

Except Port 25 and Port 26, each port of the switch cannot transmit packets with each other. Each port groups a VLAN with Port 25 and Port 26, thus, total 6 groups consisting of 3 members are formed.4

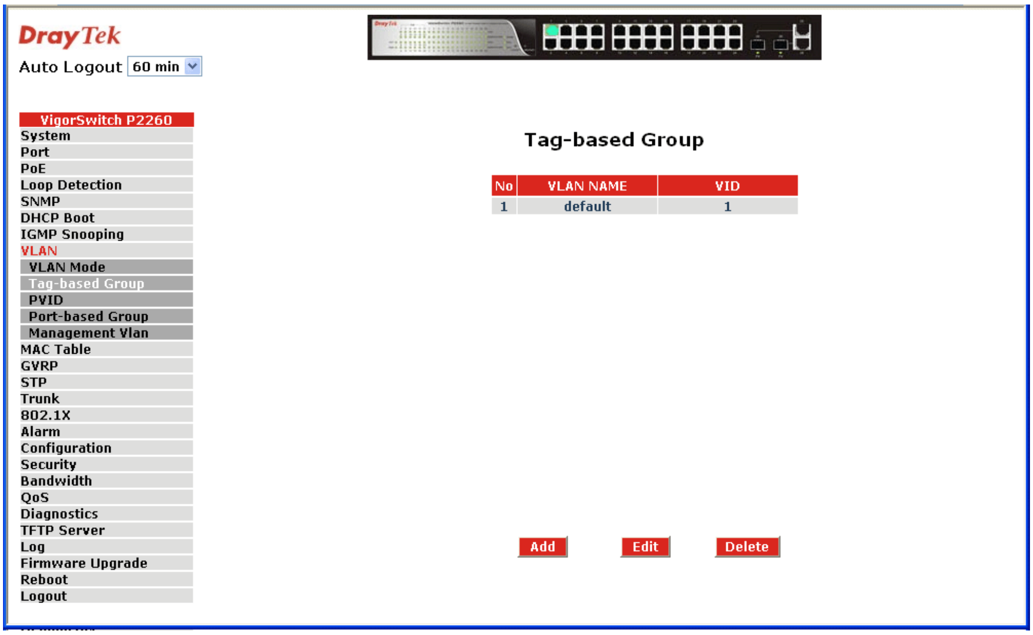
2.8.2 Tag-based Group

Function name:

Tag-based Group Configuration

Function description:

It shows the information of existed Tag-based VLAN Groups, You can also easily create, edit and delete a Tag-based VLAN group by pressing <**Add**>, <**Edit**> and <**Delete**> function buttons. User can add a new VLAN group by inputting a new VLAN name and VLAN ID.



Tag-based Group

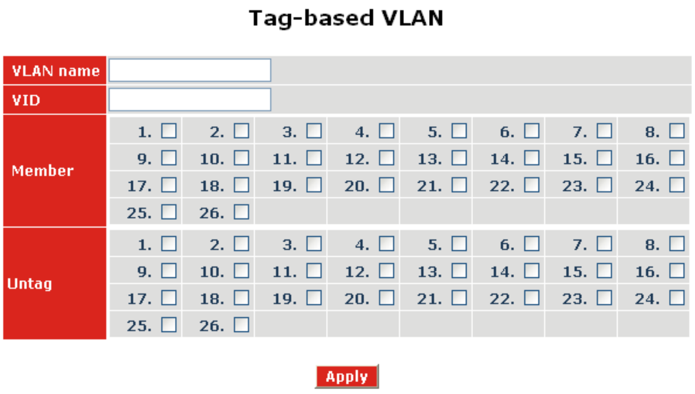
No	VLAN NAME	VID
1	default	1

Parameter description:

VLAN Name: The name defined by administrator is associated with a VLAN group. Valid letters are A-Z, a-z, 0-9, “ - “ and “_” characters. The maximal length is 15 characters.

VID: VLAN identifier. Each tag-based VLAN group has a unique VID. It appears only in tag-based and Double-tag mode.

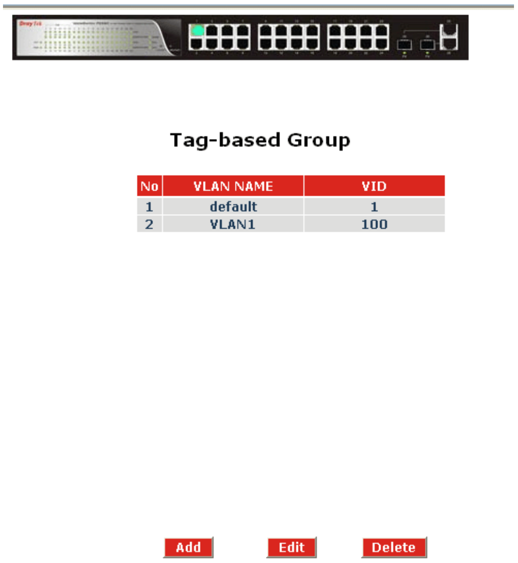
Add Input the VLAN name, VID and then choose the member by ticking the check box beside the port No. to create a new Tag-based VLAN. As to the parameter of Untag, it stands for an egress rule of the port. If you tick the check box beside the port No., packets with this VID outgoing from this port will be untagged. Finally, press the <**Apply**> button to have the setting taken effect.



Tag-based VLAN

VLAN name								
VID								
Member	1. □	2. □	3. □	4. □	5. □	6. □	7. □	8. □
	9. □	10. □	11. □	12. □	13. □	14. □	15. □	16. □
	17. □	18. □	19. □	20. □	21. □	22. □	23. □	24. □
	25. □	26. □						
Untag	1. □	2. □	3. □	4. □	5. □	6. □	7. □	8. □
	9. □	10. □	11. □	12. □	13. □	14. □	15. □	16. □
	17. □	18. □	19. □	20. □	21. □	22. □	23. □	24. □
	25. □	26. □						

Delete Just press the <**Delete**> button to remove the selected group entry from the Tag-based group table.



Tag-based Group

No	VLAN NAME	VID
1	default	1
2	VLAN1	100

Edit Just select a group entry and press the <Edit> button, then you can modify a group’s description.

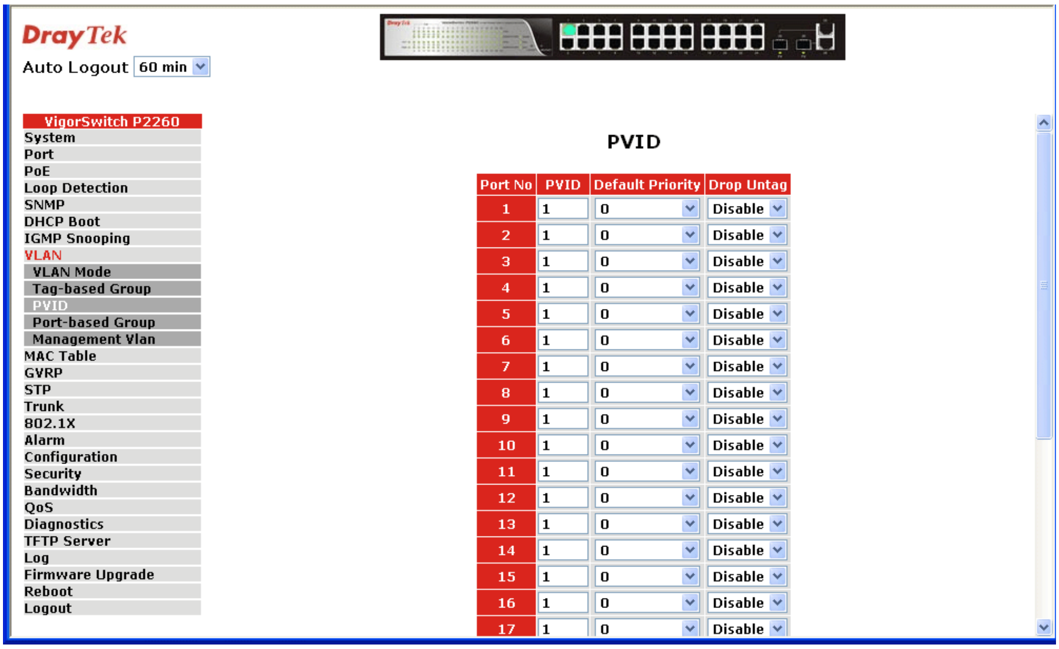
2.8.3 PVID

Function name:

PVID

Function description:

In PVID Setting, user can input VID number to each port. The range of VID number is from 1 to 4094. User also can choose ingress filtering rule (Rule 2) to each port. The Ingress Filtering Rule 2 is “drop untagged frame”. While Rule 2 is enabled, the port will discard all Untagged-frames.



PVID

Port No	PVID	Default Priority	Drop Untag
1	1	0	Disable
2	1	0	Disable
3	1	0	Disable
4	1	0	Disable
5	1	0	Disable
6	1	0	Disable
7	1	0	Disable
8	1	0	Disable
9	1	0	Disable
10	1	0	Disable
11	1	0	Disable
12	1	0	Disable
13	1	0	Disable
14	1	0	Disable
15	1	0	Disable
16	1	0	Disable
17	1	0	Disable

Parameter description:

Port 1-26: Port number.

PVID: This PVID range will be 1-4094. Before you set a number x as PVID, you have to create a Tag-based VLAN with VID x. For example, if port x receives an untagged packet, the switch will apply the PVID (assume as VID y) of port x to tag this packet, the packet then will be forwarded as the tagged packet with VID y.

Default Priority It bases on 802.1p QoS and affects untagged packets. When the packets enter the switch, it would get the priority precedence according to your Default Priority setting and map to 802.1p priority setting in QoS function. For example, while you set Default Priority of port 2 with 2 and transmit untagged packets to port 2, these packets will own priority 2 precedence due to your default 802.1p Priority Mapping setting in QoS function and be put into Queue 1.

Drop Untag: Drop untagged frame. You can configure a given port to accept all frames (Tagged and Untagged) or just receive tagged frame. If the former is the case, then the packets with tagged or untagged will be processed. If the later is the case, only the packets carrying VLAN tag will be processed, the rest packets will be discarded.

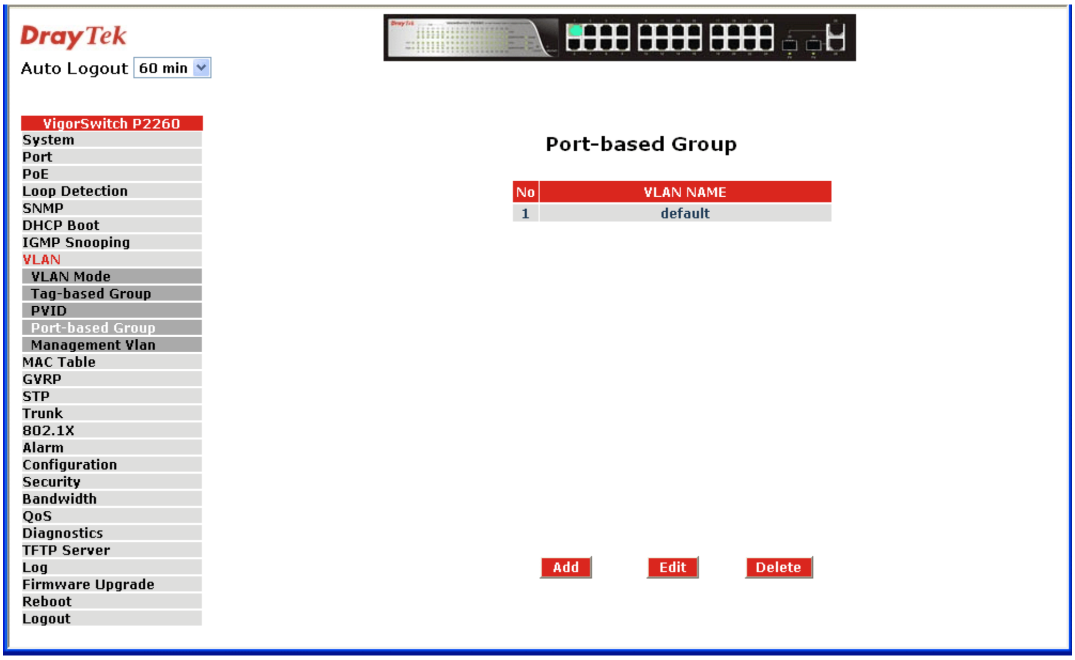
2.8.4 Port-based Group

Function name:

Port-based Group Configuration

Function description:

It shows the information of the existed Port-based VLAN Groups. You can easily create, edit and delete a Port-based VLAN group by pressing **<Add>**, **<Edit>** and **<Delete>** function buttons. User can add a new VLAN group by inputting a new VLAN name.



Port-based Group

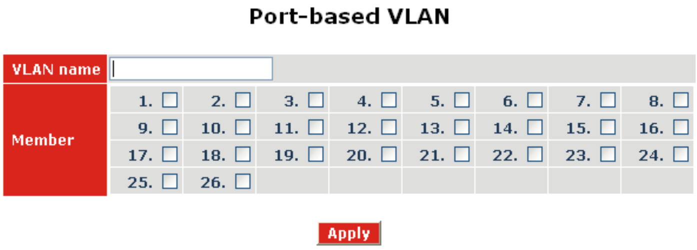
No	VLAN NAME
1	default

Parameter description:

VLAN Name: The name defined by administrator is associated with a VLAN group. Valid letters are A-Z, a-z, 0-9, " - " and "_" characters. The maximal length is 15 characters.

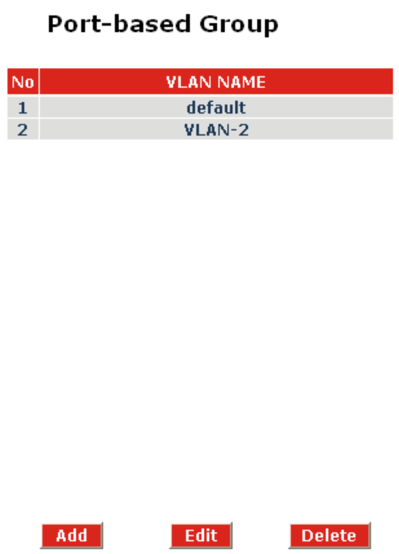
Add Create a new Port-based VLAN. Input the VLAN name and choose the member by ticking the check box beside the port No., then, press the <**Apply**> button to have the setting taken effect.

Member: This is used to enable or disable if a port is a member of the new added VLAN, "Enable" means it is a member of the VLAN. Just tick the check box (☑) beside the port x to enable it.


Port-based VLAN

VLAN name								
Member	1. □	2. □	3. □	4. □	5. □	6. □	7. □	8. □
	9. □	10. □	11. □	12. □	13. □	14. □	15. □	16. □
	17. □	18. □	19. □	20. □	21. □	22. □	23. □	24. □
	25. □	26. □						

Delete Just press the <**Delete**> button to remove the selected group entry from the Port-based group table.



Port-based Group

No	VLAN NAME
1	default
2	VLAN-2

Edit a group Just select a group entry and press the **<Edit>** button, then you can modify a group‘s description and member set.

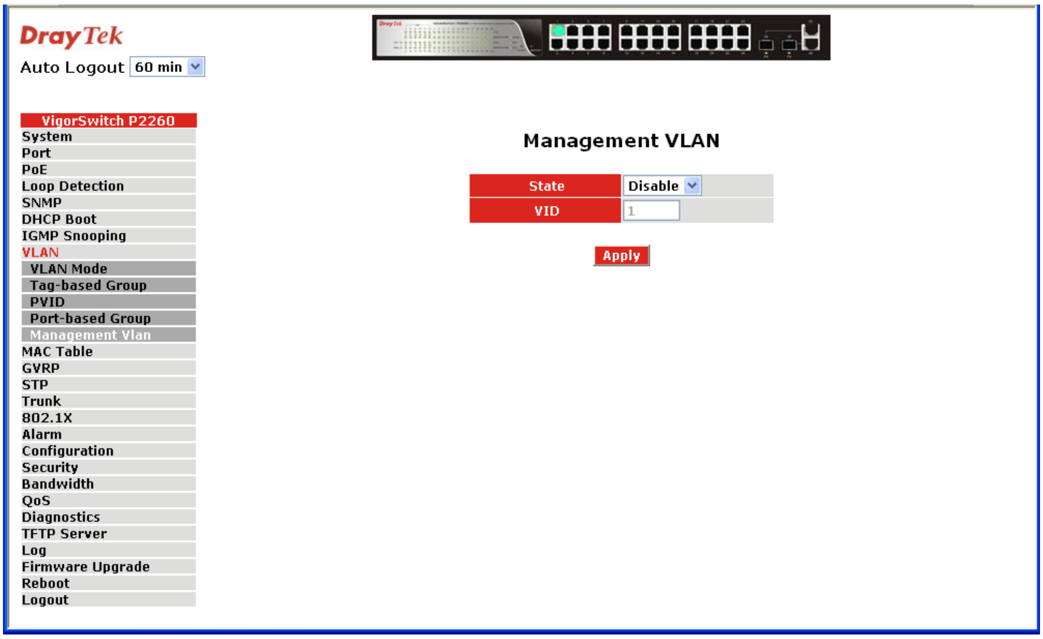
2.8.5 Management VLAN

Function name:

Management VLAN

Function description:

To create a secure VLAN for the switch management interface, all of the management traffic will be sent via an isolated VLAN. This is a security function. It can protect switch management interface, it also can avoid the switch CPU DoS by network attacking.



Management VLAN

State	Disable
VID	1

Parameter description:

State: *Enable-*
This function is based on tag-based VLAN mode. When this function is enabled, only the tagged packets with this VID can manage the switch.
Disable –

	The management VLAN function default setting is disabled. The management traffic can belong to any VLAN groups.
VID:	Valid range 1~4094.

2.9 MAC Table

MAC Table Configuration gathers many functions, including MAC Table Information, MAC Table Maintenance, Static Forward, Static Filter and MAC Alias, which cannot be categorized to some function type. They are described below.

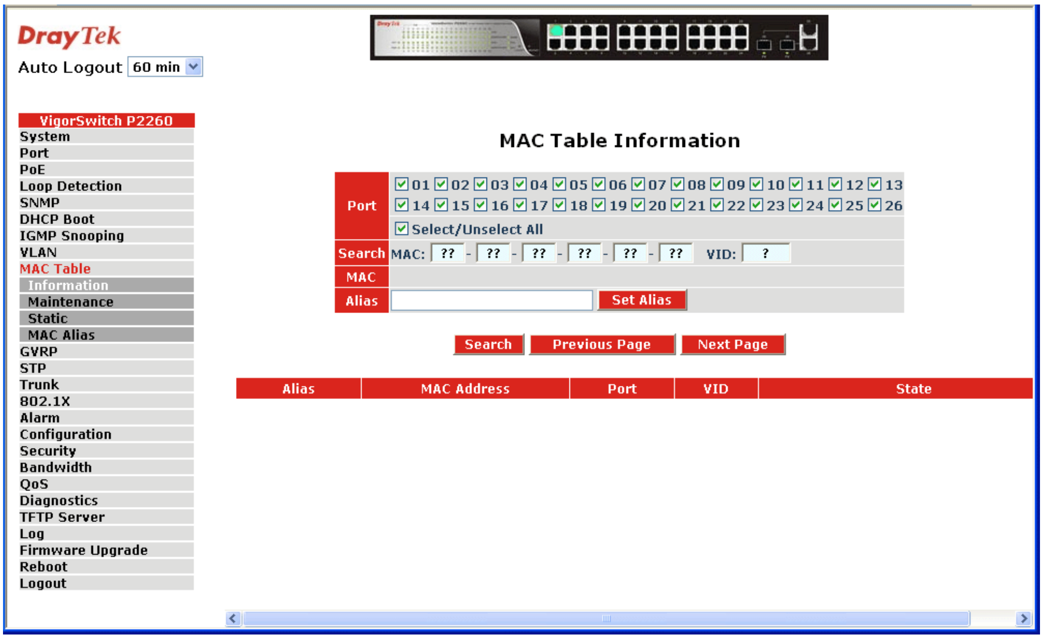
2.9.1 MAC Table Information

Function name:

MAC Table Information

Function Description:

Display the static or dynamic learning MAC entry and the state for the selected port.



MAC Table Information

Port	☑01 ☑02 ☑03 ☑04 ☑05 ☑06 ☑07 ☑08 ☑09 ☑10 ☑11 ☑12 ☑13 ☑14 ☑15 ☑16 ☑17 ☑18 ☑19 ☑20 ☑21 ☑22 ☑23 ☑24 ☑25 ☑26 ☑Select/Unselect All
Search	MAC: ?? - ?? - ?? - ?? - ?? - ?? VID: ?
MAC	
Alias	Set Alias

Alias	MAC Address	Port	VID	State

Parameter description:

Port:	Select the port you would like to inquire.
Search:	Set up the MAC entry you would like to inquire. The default is ??-??-??-??-??-??
MAC:	Display the MAC address of one entry you selected from the searched MAC entries table.
Alias:	Set up the Alias for the selected MAC entry.
Set Alias:	Save the Alias of MAC entry you set up.
Search:	Find the entry that meets your setup.
Previous Page:	Move to the previous page.
Next Page:	Move to the next page.
Alias:	The Alias of the searched entry.
MAC Address:	The MAC address of the searched entry.

Port:	The port that exists in the searched MAC Entry.
VID:	VLAN Group that MAC Entry exists.
State:	Display the method that this MAC Entry is built. It may show “Dynamic MAC” or “Static MAC”.

2.9.2 MAC Table Maintenance

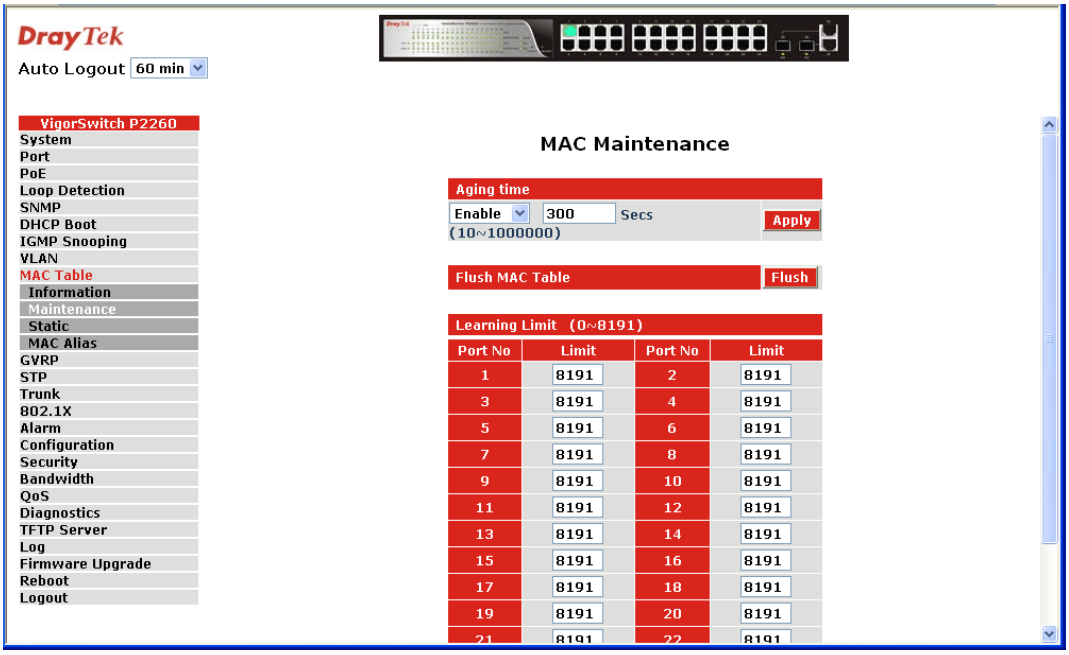
Function Name:

MAC Table Maintenance

Function Description:

This function can allow the user to set up the processing mechanism of MAC Table. An idle MAC address exceeding MAC Address Age-out Time will be removed from the MAC Table. The range of Age-out Time is 10-65535 seconds, and the setup of this time will have no effect on static MAC addresses.

In addition, the learning limit of MAC maintenance is able to limit the amount of MAC that each port can learn.



MAC Maintenance

Aging time

Enable 300 Secs (10~1000000) Apply

Flush MAC Table Flush

Learning Limit (0~8191)

Port No	Limit	Port No	Limit
1	8191	2	8191
3	8191	4	8191
5	8191	6	8191
7	8191	8	8191
9	8191	10	8191
11	8191	12	8191
13	8191	14	8191
15	8191	16	8191
17	8191	18	8191
19	8191	20	8191
21	8191	22	8191

Parameter description:

Aging Time:	Delete a MAC address idling for a period of time from the MAC Table, which will not affect static MAC address. Range of MAC Address Aging Time is 10-65535 seconds. The default Aging Time is 300 seconds.
Flush:	Remove all entries that do not belong to the static Mac Entry from the MAC Table.
Learning Limit	To set up the maximum amount of MAC that each port can learn. Valid value of learning limit for port 1~24 ranges from 0-8191. As to port 25~port 26, only the fixed value “8192” is assigned to these two ports and user cannot configure this value.

2.9.3 Static Forward

Function Name:

Static MAC

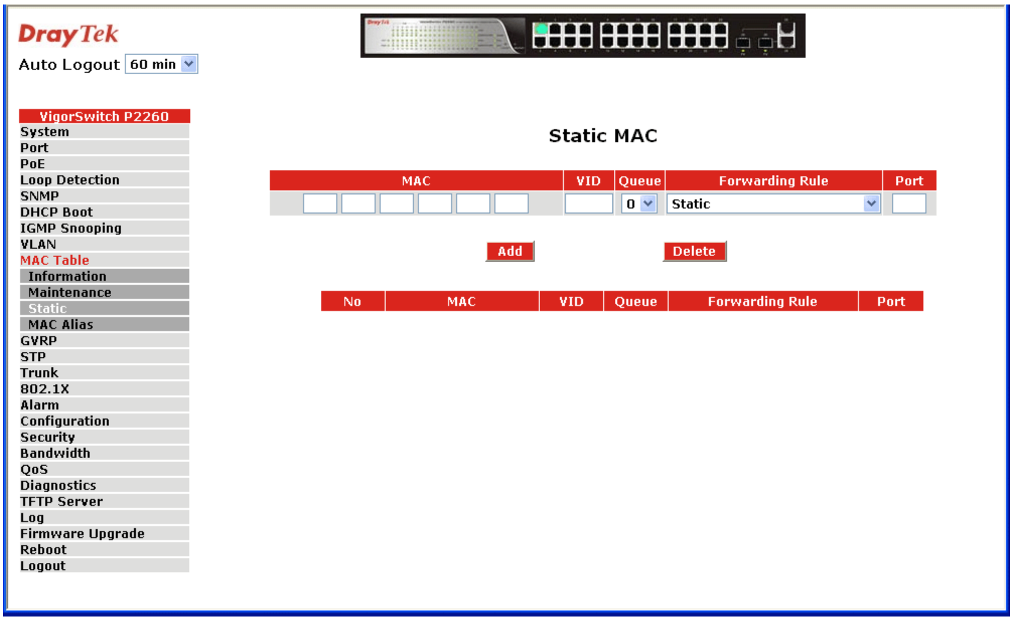
Function Description:

The function of Static is used to configure MAC's real manners inside of the switch. Three kinds of manners including static, static with destination drop and static with source drop are contained in this function.

As "static" is chosen, assign a MAC address to a specific port, all of the switch's traffics sent to this MAC address will be forwarded to this port.

As "static with destination drop" is chosen, the packet will be dropped if its DA is equal to the value you set up. Due to this setting belongs to the global one, so, it may affect all ports' transmission of the packets.

As "static with source drop" is chosen, the packet will be dropped if its SA is equal to the value you set up. Due to this setting belongs to the global one, so, it may affect all ports' transmission of the packets.



MAC	VID	Queue	Forwarding Rule	Port
		0	Static	

No	MAC	VID	Queue	Forwarding Rule	Port

Parameter description:

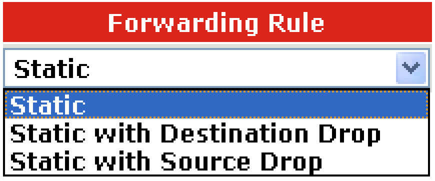
MAC: It is a six-byte long Ethernet hardware address and usually expressed by hex and separated by hyphens. For example, 00 – 40 - C7 - D6 – 00 - 01

VID: VLAN identifier. This will be filled only when tagged VLAN is applied. Valid range is 1 ~ 4094.

Queue: Set up the priority(0~3) for the MAC.

Forwarding Rule Static - A MAC address is assigned to a specific port, all of the switch's traffics sent to this MAC address will be forwarded to this port.
Static with Destination Drop - While the DA of the incoming packets meets the value you set up, these packets will be dropped.
Static with Source Drop - While the SA of the incoming packets meets the value you set up, these packets will be

dropped.



Port: Select the port No. you would like to do setup in the switch. It is 1~26.

2.9.4 MAC Alias Create/Edit or Delete

Function name:

MAC Alias

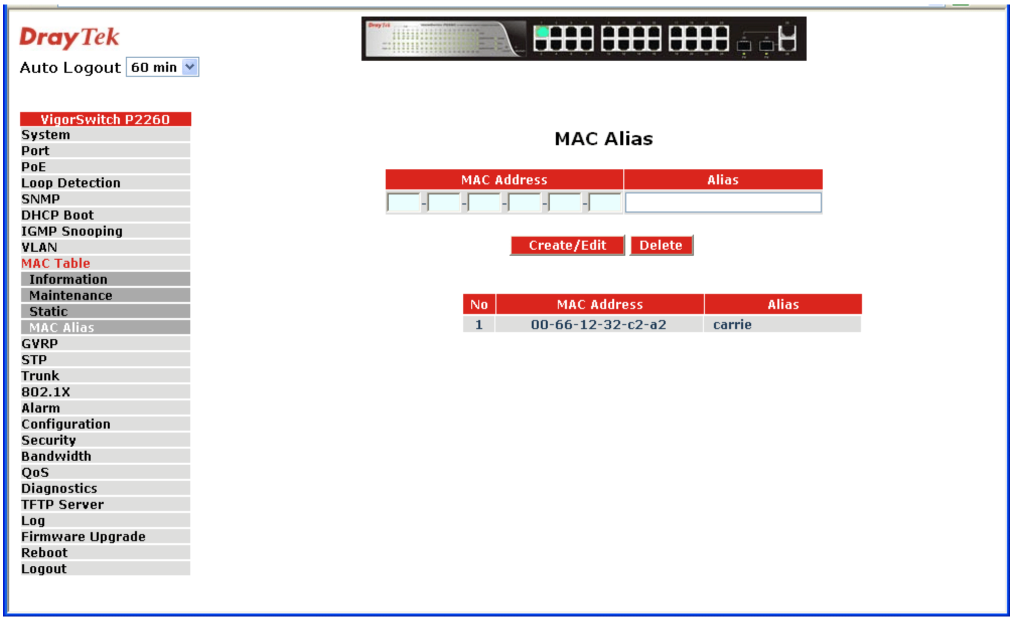
Function description:

MAC Alias function is used to let you assign MAC address a plain English name. This will help you tell which MAC address belongs to which user in the illegal access report. At the initial time, it shows all pairs of the existed alias name and MAC address.

There are three MAC alias functions in this function folder, including MAC Alias Add, MAC Alias Edit and MAC Alias Delete. You can click **<Create/Edit>** button to add/modify a new or an existed alias name for a specified MAC address, or mark an existed entry to delete it. Alias name must be composed of A-Z, a-z and 0-9 only and has a maximal length of 15 characters.

In the MAC Alias function, MAC Alias Add/Edit function is used to let you add or modify an association between MAC address and a plain English name. User can click **<Create/Edit>** button to add a new record with name.

As to MAC Alias Delete function is used to let you remove an alias name to a MAC address. You can select an existed MAC address or alias name to remove.



No	MAC Address	Alias
1	00-66-12-32-c2-a2	carrie

Parameter description:

MAC Address: It is a six-byte long Ethernet hardware address and usually expressed by hex and separated by hyphens. For example, 00 – 40 - C7 - D6 – 00 - 01

Alias: MAC alias name you assign.

Note: If there are too many MAC addresses learned in the table, we recommend you inputting the MAC address and alias name directly.

2.10 GVRP Configuration

GVRP is an application based on Generic Attribute Registration Protocol (GARP), mainly used to automatically and dynamically maintain the group membership information of the VLANs. The GVRP offers the function providing the VLAN registration service through a GARP application. It makes use of GARP Information Declaration (GID) to maintain the ports associated with their attribute database and GARP Information Propagation (GIP) to communicate among switches and end stations. With GID information and GIP, GVRP state machine maintain the contents of Dynamic VLAN Registration Entries for each VLAN and propagate these information to other GVRP-aware devices to setup and update their knowledge database, the set of VLANs associated with currently active members, and through which ports these members can be reached.

In GVRP Configuration function folder, there are three functions supported, including GVRP Config, GVRP Counter and GVRP Group explained below.

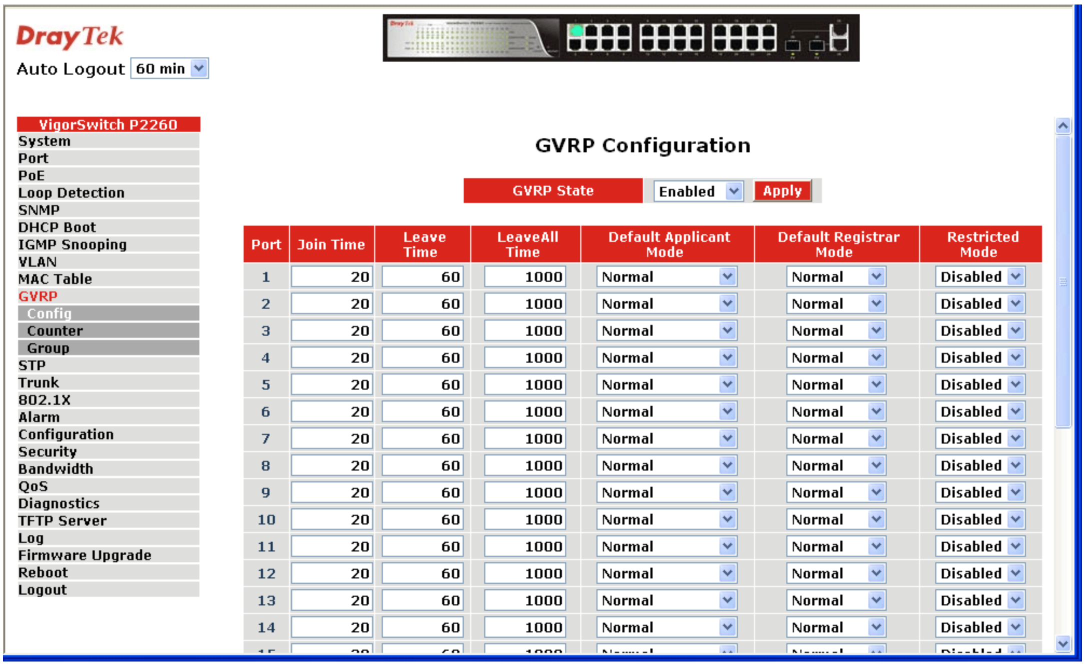
2.10.1 GVRP Config

Function name:

GVRP Config

Function description:

In the function of GVRP Config, it is used to configure each port's GVRP operation mode, in which there are seven parameters needed to be configured described below.



Auto Logout 60 min

GVRP Configuration

GVRP State: Enabled

Port	Join Time	Leave Time	LeaveAll Time	Default Applicant Mode	Default Registrar Mode	Restricted Mode
1	20	60	1000	Normal	Normal	Disabled
2	20	60	1000	Normal	Normal	Disabled
3	20	60	1000	Normal	Normal	Disabled
4	20	60	1000	Normal	Normal	Disabled
5	20	60	1000	Normal	Normal	Disabled
6	20	60	1000	Normal	Normal	Disabled
7	20	60	1000	Normal	Normal	Disabled
8	20	60	1000	Normal	Normal	Disabled
9	20	60	1000	Normal	Normal	Disabled
10	20	60	1000	Normal	Normal	Disabled
11	20	60	1000	Normal	Normal	Disabled
12	20	60	1000	Normal	Normal	Disabled
13	20	60	1000	Normal	Normal	Disabled
14	20	60	1000	Normal	Normal	Disabled

Parameter description:

GVRP State Setting: This function is simply to let you enable or disable GVRP function. You can pull down the list and click the **<Downward>** arrow key to choose "Enable" or "Disable".

Then, click the **<Apply>** button, the system will take effect immediately.

Join Time: Used to declare the Join Time in unit of centisecond. Valid time range: 20 –100 centisecond, Default: 20 centisecond.

Leave Time: Used to declare the Leave Time in unit of centisecond. Valid time range: 60 –300 centisecond, Default: 60 centisecond.

Leave All Time: A time period for announcement that all registered device is going to be de-registered. If someone still issues a new join, then a registration will be kept in the switch. Valid range: 1000-5000 unit time, Default: 1000 unit time.

Default Applicant Mode: The mode here means the type of participant. There are two modes, normal participant and non-participant, provided for the user’s choice.

Normal - It is Normal Participant. In this mode, the switch participates normally in GARP protocol exchanges. The default setting is Normal.

Non-Participant - It is Non-Participant. In this mode, the switch does not send or reply any GARP messages. It just listens messages and reacts for the received GVRP BPDU.

Default Registrar Mode: The mode here means the type of Registrar. There are three types of parameters for registrar administrative control value, normal registrar, fixed registrar and forbidden registrar, provided for the user’s choice.

Normal - It is Normal Registration. The Registrar responds normally to incoming GARP messages. The default setting is Normal.

Fixed - It is Registration Fixed. The Registrar ignores all GARP messages, and all members remain in the registered (IN) state.

Forbidden - It is Registration Forbidden. The Registrar ignores all GARP messages, and all members remain in the unregistered (EMPTY) state.

Restricted Mode: This function is used to restrict dynamic VLAN be created when this port received GVRP PDU. There are two modes, disable and enable, provided for the user’s choice.

Disabled - In this mode, the switch dynamic VLAN will be created when this port received GVRP PDU. The default setting is Normal.

Enabled - In this mode, the switch does not create dynamic VLAN when this port received GVRP PDU. Except received dynamic VLAN message of the GVRP PDU is an existed static VLAN in the switch, this port will be added into the static VLAN members dynamically.

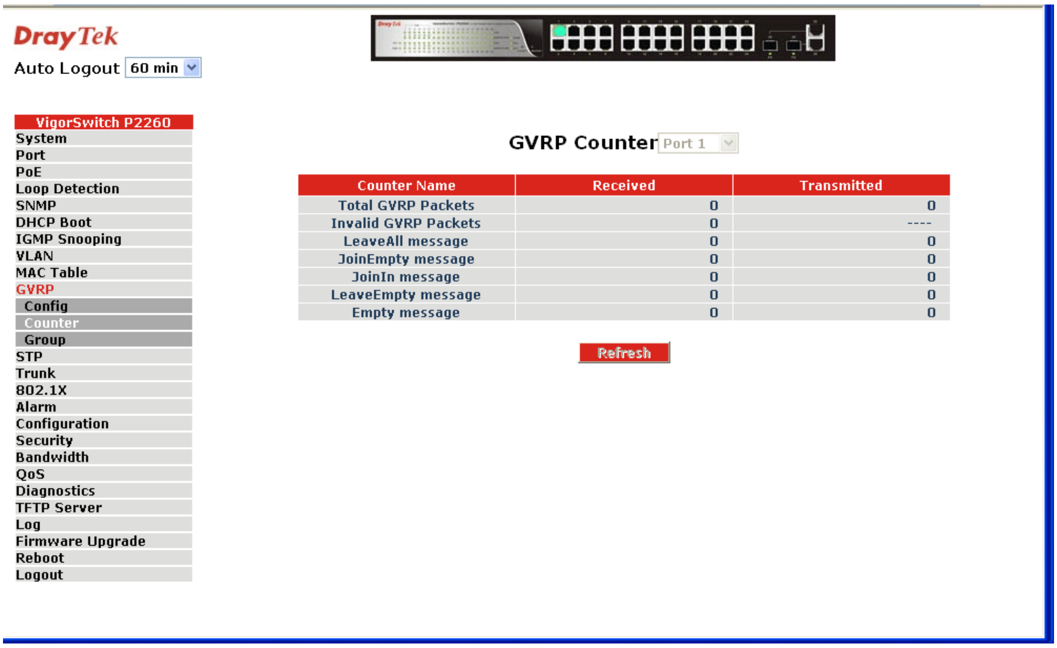
2.10.2 GVRP Counter

Function name:

GVRP Counter

Function description:

All GVRP counters are mainly divided into Received and Transmitted two categories to let you monitor the GVRP actions. Actually, they are GARP packets.



GVRP Counter Port 1

Counter Name	Received	Transmitted
Total GVRP Packets	0	0
Invalid GVRP Packets	0	----
LeaveAll message	0	0
JoinEmpty message	0	0
JoinIn message	0	0
LeaveEmpty message	0	0
Empty message	0	0

Parameter description:

Received:

Total GVRP Packets - Total GVRP BPDU is received by the GVRP application.

Invalid GVRP Packets - Number of invalid GARP BPDU is received by the GARP application.

LeaveAll Message Packets - Number of GARP BPDU with Leave All message is received by the GARP application.

JoinEmpty Message Packets - Number of GARP BPDU with Join Empty message is received by the GARP application.

JoinIn Message Packets - Number of GARP BPDU with Join In message is received by the GARP application.

LeaveEmpty Message Packets - Number of GARP BPDU with Leave Empty message is received by the GARP application.

Empty Message Packets - Number of GARP BPDU with Empty message is received by the GARP application.

Transmitted:

Total GVRP Packets - Total GARP BPDU is transmitted by the GVRP application.

Invalid GVRP Packets - Number of invalid GARP BPDU is transmitted by the GVRP application.

LeaveAll Message Packets - Number of GARP BPDU with Leave All message is transmitted by the GARP application.

JoinEmpty Message Packets - Number of GARP BPDU with Join Empty message is transmitted by the GARP application.

JoinIn Message Packets - Number of GARP BPDU with Join In message is transmitted by the GARP application.

LeaveEmpty Message Packets - Number of GARP BPDU with Leave Empty message is transmitted by the GARP application.

Empty Message Packets - Number of GARP BPDU with Empty message is transmitted by the GARP application.

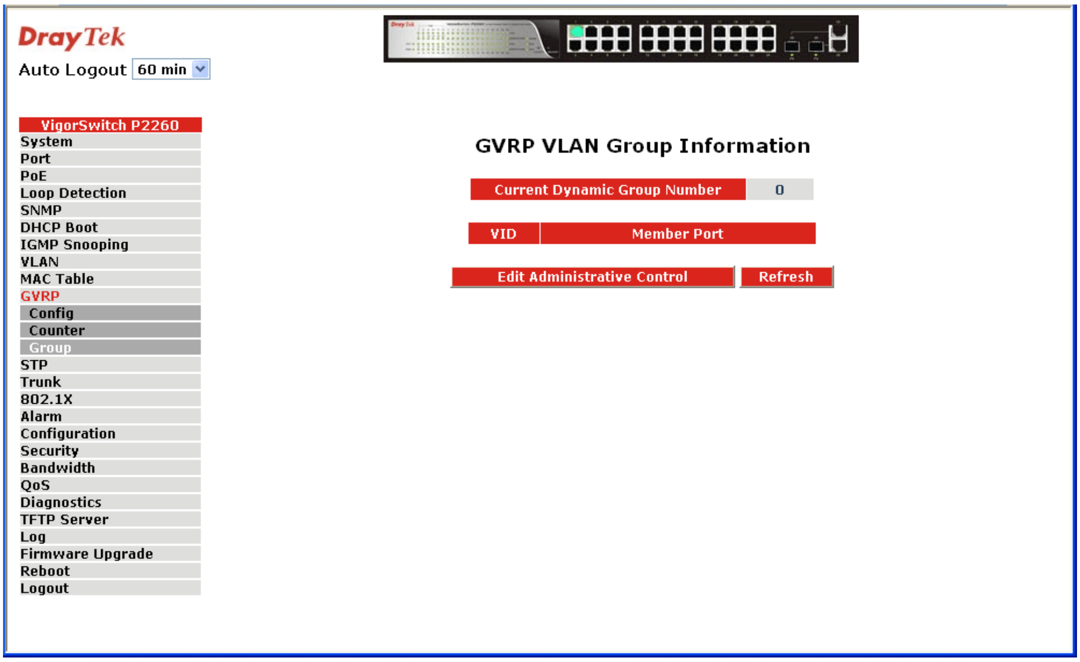
2.10.3 GVRP Group Information

Function name:

GVRP Group Information

Function description:

Show the dynamic group member and their information.



GVRP VLAN Group Information

Current Dynamic Group Number	0

VID	Member Port

Parameter description:

VID: VLAN identifier. When GVRP group creates, each dynamic VLAN group owns its VID. Valid range is 1 ~ 4094.

Member Port: Those are the members belonging to the same dynamic VLAN group.

Edit Administrative Control: When you create GVRP group, you can use Administrative Control function to change Applicant Mode and Registrar Mode of GVRP group member.

Refresh: Refresh function can help you to see current GVRP group status.

2.11 STP Configuration

The Spanning Tree Protocol (STP) is a standardized method (IEEE 802.1D) for avoiding loops in switched networks. When STP is enabled, ensure that only one path is active between any two nodes on the network at a time. User can enable Spanning Tree Protocol on switch's web management and then set up other advanced items. We recommend that you enable STP on all switches to ensure a single active path on the network.

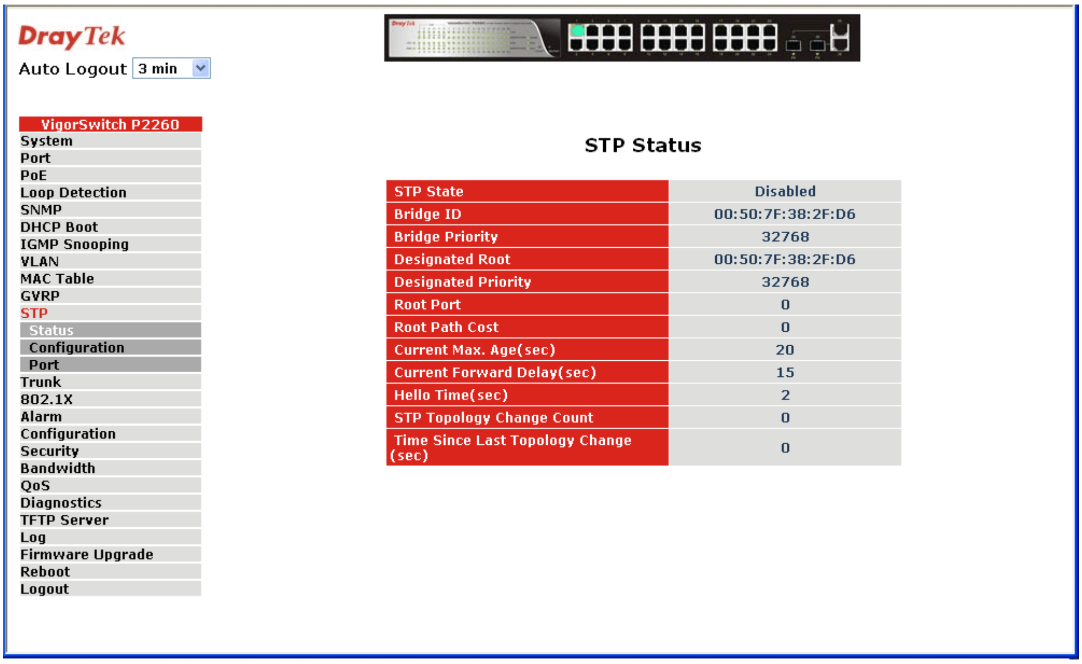
2.11.1 STP Status

Function name:

STP Status

Function description:

In the Spanning Tree Status, user can read 12 parameters to know STP current status. The 12 parameters' description is listed in the following table.



STP Status

STP State	Disabled
Bridge ID	00:50:7F:38:2F:D6
Bridge Priority	32768
Designated Root	00:50:7F:38:2F:D6
Designated Priority	32768
Root Port	0
Root Path Cost	0
Current Max. Age(sec)	20
Current Forward Delay(sec)	15
Hello Time(sec)	2
STP Topology Change Count	0
Time Since Last Topology Change (sec)	0

Parameter description:

STP State: Show the current STP Enabled / Disabled status. Default is "Disabled".

Bridge ID: Show switch's bridge ID which stands for the MAC address of this switch.

Bridge Priority: Show this switch's current bridge priority setting. Default is 32768.

Designated Root: Show root bridge ID of this network segment. If this switch is a root bridge, the "Designated Root" will show this switch's bridge ID.

Designated Priority: Show the current root bridge priority.

Root Port: Show port number connected to root bridge with the lowest path cost.

Root Path Cost: Show the path cost between the root port and the designated port of the root bridge.

Current Max. Age: Show the current root bridge maximum age time. Maximum age time is used to monitor if STP topology needs to change. When a bridge does not receive a hello message from root bridge until the maximum age time is counted down to 0, the bridge will treat the root bridge malfunctioned and issue a Topology Change Notification (TCN) BPDU to all other bridges.

All bridges in the LAN will re-learn and determine which the root bridge is. Maximum Age time is assigned by root bridge in unit of seconds. Default is 20 seconds.

Current Forward Delay: Show the current root bridge forward delay time. The value of Forward Delay time is set by root. The Forward Delay time is defined as the time spent from Listening state moved to Learning state or from Learning state moved to Forwarding state of a port in bridge.

Hello Time: Show the current hello time of the root bridge. Hello time is a time interval specified by root bridge, used to request all other bridges periodically sending hello message every “hello time” seconds to the bridge attached to its designated port.

STP Topology Change Count: STP Topology Change Count expresses the time spent in unit of seconds since the beginning of the Spanning Tree Topology Change to the end of the STP convergence. Once the STP change is converged, the Topology Change count will be reset to 0. The figures showing in the screen may not be the exact time it spent but very close to, because the time is eclipsing.

Time Since Last Topology Change: Time Since Last Topology Change is the accumulated time in unit of seconds the STP has been since the last STP Topology Change was made. When Topology Change is initiated again, this counter will be reset to 0. And it will also count again once STP topology Change is completed.

2.11.2 STP Configuration

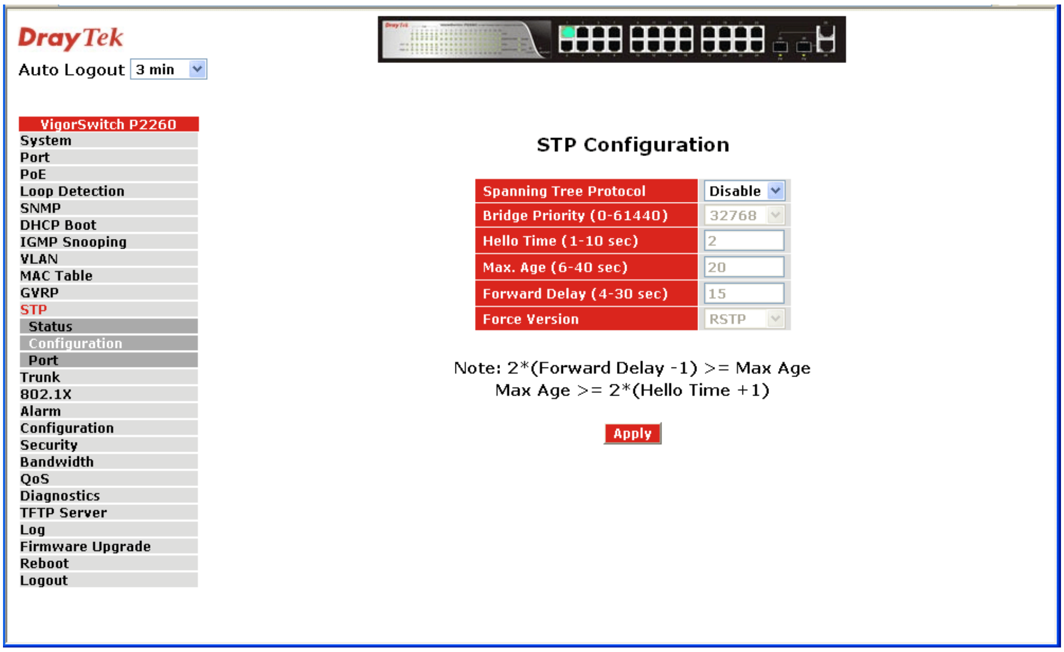
The STP, Spanning Tree Protocol, actually includes RSTP. In the Spanning Tree Configuration, there are six parameters open for the user to configure as user’s idea. Each parameter description is listed below.

Function name:

STP Configuration

Function description:

User can set the following Spanning Tree parameters to control STP function enable/disable, select mode RSTP/STP and affect STP state machine behavior to send BPDU in this switch. The default setting of Spanning Tree Protocol is “Disable”.



Auto Logout: 3 min

STP Configuration

Spanning Tree Protocol	Disable
Bridge Priority (0-61440)	32768
Hello Time (1-10 sec)	2
Max. Age (6-40 sec)	20
Forward Delay (4-30 sec)	15
Force Version	RSTP

Note: 2*(Forward Delay -1) >= Max Age
Max Age >= 2*(Hello Time +1)

Parameter description:

Spanning Tree Protocol: Set 802.1W Rapid STP function Enable / Disable. Default is “Disable”

Bridge Priority: The lower the bridge priority is, the higher priority it has. Usually, the bridge with the highest bridge priority is the root. If you want to have the GEL2-SW8 as root bridge, you can set this value lower than that of bridge in the LAN. The valid value is 0 ~ 61440. The default is 32768.

Hello Time: Hello Time is used to determine the periodic time to send normal BPDU from designated ports among bridges. It decides how long a bridge should send this message to other bridge to tell I am alive. When the GEL2-SW8 is the root bridge of the LAN, for example, all other bridges will use the hello time assigned by this switch to communicate with each other. The valid value is 1 ~ 10 in unit of second.

Default is 2 seconds.

Max. Age: When the GEL2-SW8 is the root bridge, the whole LAN will apply this figure set by this switch as their maximum age time. When a bridge received a BPDU originated from the root bridge and if the message age conveyed in the BPDU exceeds the Max. Age of the root bridge, the bridge will treat the root bridge malfunctioned and issue a Topology Change Notification (TCN) BPDU to all other bridges. All bridges in the LAN will re-calculate and determine who the root bridge is. The valid value of Max. Age is 6 ~ 40 seconds. Default is 20 seconds.

Forward Delay: You can set the root bridge forward delay time. This figure is set by root bridge only. The forward delay time is defined as the time spent from Listening state moved to Learning state and also from Learning state moved to Forwarding state of a port in bridge. The forward delay time contains two states, Listening state to Learning state and Learning state to Forwarding state. It assumes that forward delay time is 15 seconds, then total forward delay time will be 30 seconds. This has much to do with the STP convergent time which will be more than 30 seconds because some other factors.

The valid value is 4 ~ 30 seconds, default is 15 seconds.

Force Version: Two options are offered for the user's choosing STP algorithm. One is RSTP and the other is STP. If STP is chosen, RSTP will run as a legacy STP. The switch supports RSTP (802.1w) which is backward compatible with STP (802.1d).

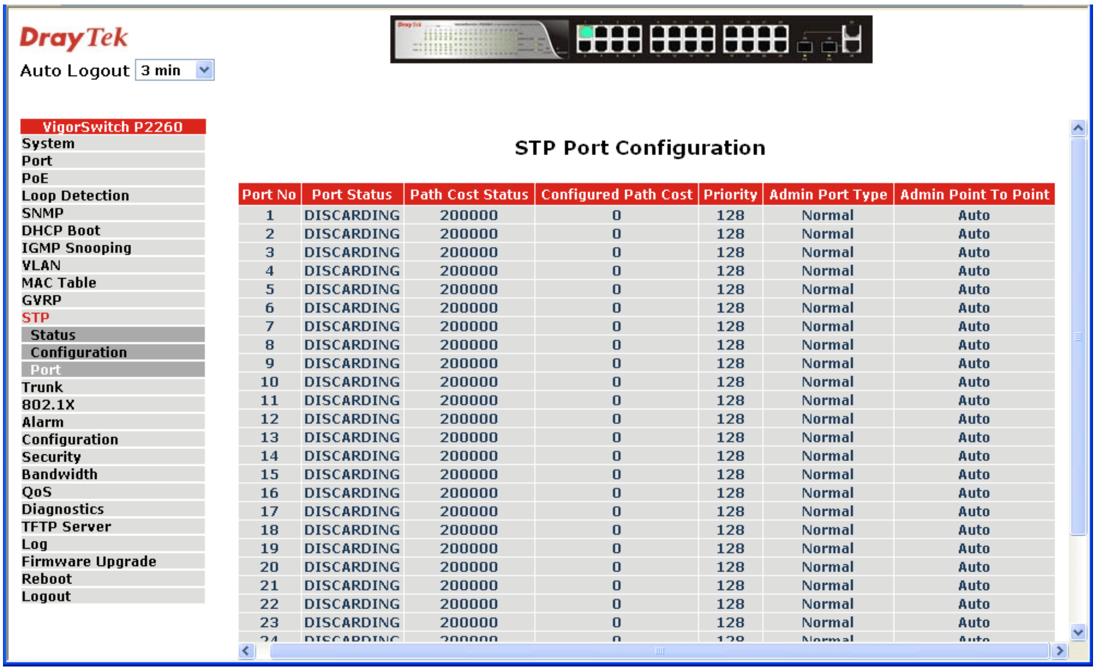
2.11.3 STP Port Configuration

Function name:

STP Port Setting

Function description:

In the STP Port Setting, one item selection and five parameters settings are offered for user's setup. User can disable and enable each port by selecting each Port Status item. User also can set "Path Cost" and "Priority" of each port by filling in the desired value and set "Admin Edge Port" and "Admin Point To Point" by selecting the desired item.



Auto Logout 3 min

STP Port Configuration

Port No	Port Status	Path Cost Status	Configured Path Cost	Priority	Admin Port Type	Admin Point To Point
1	DISCARDING	200000	0	128	Normal	Auto
2	DISCARDING	200000	0	128	Normal	Auto
3	DISCARDING	200000	0	128	Normal	Auto
4	DISCARDING	200000	0	128	Normal	Auto
5	DISCARDING	200000	0	128	Normal	Auto
6	DISCARDING	200000	0	128	Normal	Auto
7	DISCARDING	200000	0	128	Normal	Auto
8	DISCARDING	200000	0	128	Normal	Auto
9	DISCARDING	200000	0	128	Normal	Auto
10	DISCARDING	200000	0	128	Normal	Auto
11	DISCARDING	200000	0	128	Normal	Auto
12	DISCARDING	200000	0	128	Normal	Auto
13	DISCARDING	200000	0	128	Normal	Auto
14	DISCARDING	200000	0	128	Normal	Auto
15	DISCARDING	200000	0	128	Normal	Auto
16	DISCARDING	200000	0	128	Normal	Auto
17	DISCARDING	200000	0	128	Normal	Auto
18	DISCARDING	200000	0	128	Normal	Auto
19	DISCARDING	200000	0	128	Normal	Auto
20	DISCARDING	200000	0	128	Normal	Auto
21	DISCARDING	200000	0	128	Normal	Auto
22	DISCARDING	200000	0	128	Normal	Auto
23	DISCARDING	200000	0	128	Normal	Auto
24	DISCARDING	200000	0	128	Normal	Auto

Parameter description:

Port Status: It displays the current state of a port. We cannot manually set it because it displays the status only. There are three possible states (according to 802.1w specification).

- DISCARDING state indicates that this port can neither forward packets nor contribute learning knowledge.

> Notice: Three other states (Disable state, BLOCKING state and LISTENING state) defined in the 802.1d specification are now all represented as DISCARDING state.

- LEARNING state indicates this port can now contribute its learning knowledge but cannot forward packets still.
- FORWARDING state indicates this port can both contribute its learning knowledge and forward packets normally.

Path Cost Status: It is the contribution value of the path through this port to Root Bridge. STP algorithm determines a best path to Root Bridge by calculating the sum of path cost contributed by all ports on this path. A port with a smaller path cost value would become the Root Port more possibly.

Configured Path Cost: The range is 0 – 200,000,000. In the switch, if path cost is set to be zero, the STP will get the recommended value resulted from auto-negotiation of the link accordingly and display this value in the field of Path Cost Status. Otherwise, it may show the value that the administrator set up in Configured Path Cost and Path Cost Status.

802.1w RSTP recommended value: (Valid range: 1 – 200,000,000)

10 Mbps: 2,000,000

100 Mbps: 200,000

1 Gbps: 20,000

Default: 0

Priority: Priority here means Port Priority. Port Priority and Port Number are mixed to form the Port ID. Port IDs are often compared in order to determine which port of a bridge would become the Root Port. The range is 0 – 240.

Default is 128.

Admin Port Type: The Admin Port Type has three modes - “Normal”, “Edge” and “None-STP”. An “Edge” Port is a port connected to a device that knows nothing about STP or RSTP. Usually, the connected device is an end station. “Edge” Ports will immediately transit to forwarding state and skip the listening and learning state because the edge ports cannot create bridging loops in the network. This will expedite the convergence. When the link on the edge port toggles, the STP topology keeps unchanged. Unlike the designate port or root port though, an “edge” port will transit to a normal spanning-tree port immediately if it receives a BPDU. “None-STP” means per port does not join STP calculation.

Admin Point To Point: We say a port is a point-to-point link, from RSTP's view, if it is in full-duplex mode but is shared link if it is in half-duplex mode. RSTP fast convergence can only happen on point-to-point links and on edge ports. This can expedite the convergence because this will have the port fast transited to forwarding state.

There are three parameters, Auto, True and False, used to configure the type of the point-to-point link. If configure this parameter to be Auto, it means RSTP will use the duplex mode resulted from the auto-negotiation. In today's switched networks, most links are running in full-duplex mode. For sure, the result may be half-duplex, in this case, the port will not fast transit to Forwarding state. If it is set as True, the port is treated as point-to-point link by RSTP and unconditionally transited to Forwarding state. If it is set as False, fast transition to Forwarding state will not happen on this port.

Default: Auto

MCheck: Migration Check. It forces the port sending out an RSTP BPDU instead of a legacy STP BPDU at the next transmission. The only benefit of this operation is to make the port quickly get back to act as an RSTP port. Click **<M Check>** button to send a RSTP BPDU from the port you specified.

2.12 Trunking Configuration

The Port Trunking Configuration is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipments to build the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single Fast Ethernet port has.

The switch supports two kinds of port trunking methods:

LACP

Ports using Link Aggregation Control Protocol (according to IEEE 802.3ad specification) as their trunking method can choose their unique LACP GroupID (1~8) to form a logic "trunked port". The benefit of using LACP is that a port makes an agreement with its peer port before it becomes a ready member of a "trunk group" (also called aggregator). LACP is safer than the other trunking method - static trunk.

The switch LACP does not support the followings:

- Link Aggregation across switches
- Aggregation with non-IEEE 802.3 MAC link
- Operating in half-duplex mode
- Aggregate the ports with different data rates

Static Trunk

Ports using Static Trunk as their trunk method can choose their unique Static GroupID (also 1~8, this Static groupID can be the same with another LACP groupID) to form a logic “trunked port”. The benefit of using Static Trunk method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of your static trunk group may not know that they should be aggregate together to form a “logic trunked port”. Using Static Trunk on both end of a link is strongly recommended. Please also note that low speed links will stay in “not ready” state when using static trunk to aggregate with high speed links.

As to system restrictions about the port aggregation function on the switch, in the management point of view, the switch supports maximum 8 trunk groups for LACP and additional 8 trunk groups for Static Trunk. But in the system capability view, only 8 “real trunked” groups are supported. An LACP trunk group with more than one ready member-pors is a “real trunked” group. An LACP trunk group with only one or less than one ready member-port is not a “real trunked” group. Any Static trunk group is a “real trunked” group.

Per Trunking Group supports a maximum of 12 ready member-ports. Please note that some decisions will automatically be made by the system while you are configuring your trunking ports. Some configuration examples are listed below:

Rule1: Maximum 3 groups are allowed

Rule 2: The members of each group cannot exceed more than 4 ports

Rule 3: Group 1 and 2 cannot exist member 25 and 26 port

Rule 4: Group 3 cannot exist member from 1 to 24 port

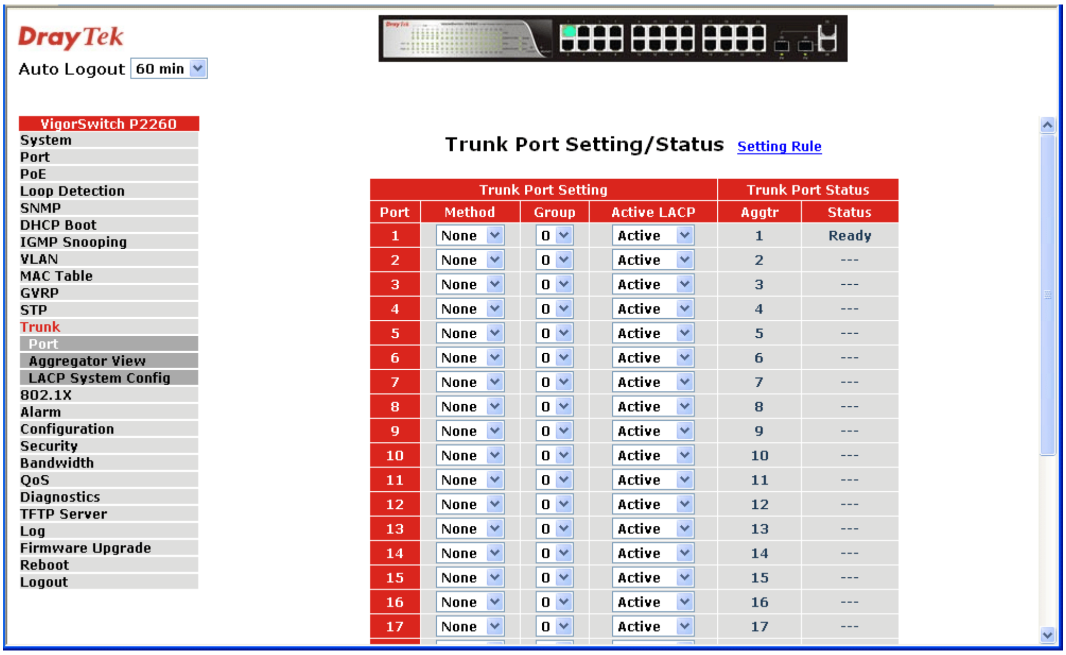
2.12.1 Port Setting/Status

Function name:

Port Setting/Status

Function description:

Port setting/status is used to configure the trunk property of each and every port in the switch system.



Auto Logout 60 min

Trunk Port Setting/Status

Trunk Port Setting				Trunk Port Status	
Port	Method	Group	Active LACP	Aggtr	Status
1	None	0	Active	1	Ready
2	None	0	Active	2	---
3	None	0	Active	3	---
4	None	0	Active	4	---
5	None	0	Active	5	---
6	None	0	Active	6	---
7	None	0	Active	7	---
8	None	0	Active	8	---
9	None	0	Active	9	---
10	None	0	Active	10	---
11	None	0	Active	11	---
12	None	0	Active	12	---
13	None	0	Active	13	---
14	None	0	Active	14	---
15	None	0	Active	15	---
16	None	0	Active	16	---
17	None	0	Active	17	---

Parameter description:

Method: This determines the method a port uses to aggregate with other ports.

None - A port does not want to aggregate with any other port should choose this default setting.

LACP - A port use LACP as its trunk method to get aggregated with other ports also using LACP.

Static - A port use Static Trunk as its trunk method to get aggregated with other ports also using Static Trunk.

Group: Ports choosing the same trunking method other than “None” must be assigned a unique Group number (i.e. Group ID, valid value is from 1 to 8) in order to declare that they wish to aggregate with each other.

Active LACP: This field is only referenced when a port’s trunking method is LACP.

Activer - An Active LACP port begins to send LACPDU to its link partner right after LACP protocol entity started to take control of this port.

Passive - A Passive LACP port will not actively send LACPDU out before it receives an LACPDU from its link partner.

Aggtr: Aggtr is an abbreviation of “aggregator”. Every port is also an aggregator, and its own aggregator ID is the same as its own Port No. We can regard an aggregator as a representative of a trunking group. Ports with same Group ID and using same trunking method will have the opportunity to aggregate to a particular aggregator port. This aggregator port is usually the port with the smallest Port No. within the trunking group.

Status: This field represents the trunking status of a port which uses a trunking method other than “None”. It also represents the management link status of a port which uses the “None” trunking method. “---“ means “not ready”

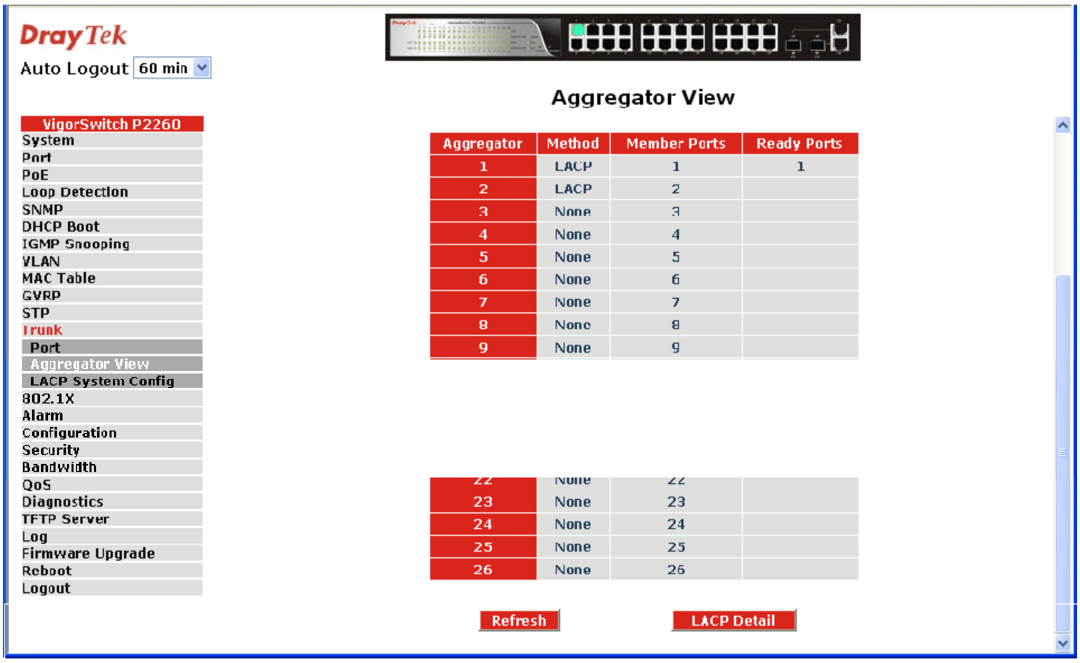
2.12.2 Aggregator View

Function name:

Aggregator View

Function description:

To display the current port trunking information from the aggregator point of view.



Aggregator View

Aggregator	Method	Member Ports	Ready Ports
1	LACP	1	1
2	LACP	2	
3	None	3	
4	None	4	
5	None	5	
6	None	6	
7	None	7	
8	None	8	
9	None	9	
22	None	22	
23	None	23	
24	None	24	
25	None	25	
26	None	26	

Parameter description:

Aggregator: It shows the aggregator ID (from 1 to 8) of every port. In fact, every port is also an aggregator, and its own aggregator ID is the same as its own Port No..

Method: Show the method a port uses to aggregate with other ports.

Member Ports: Show all member ports of an aggregator (port).

Ready Ports: Show only the ready member ports within an aggregator (port).

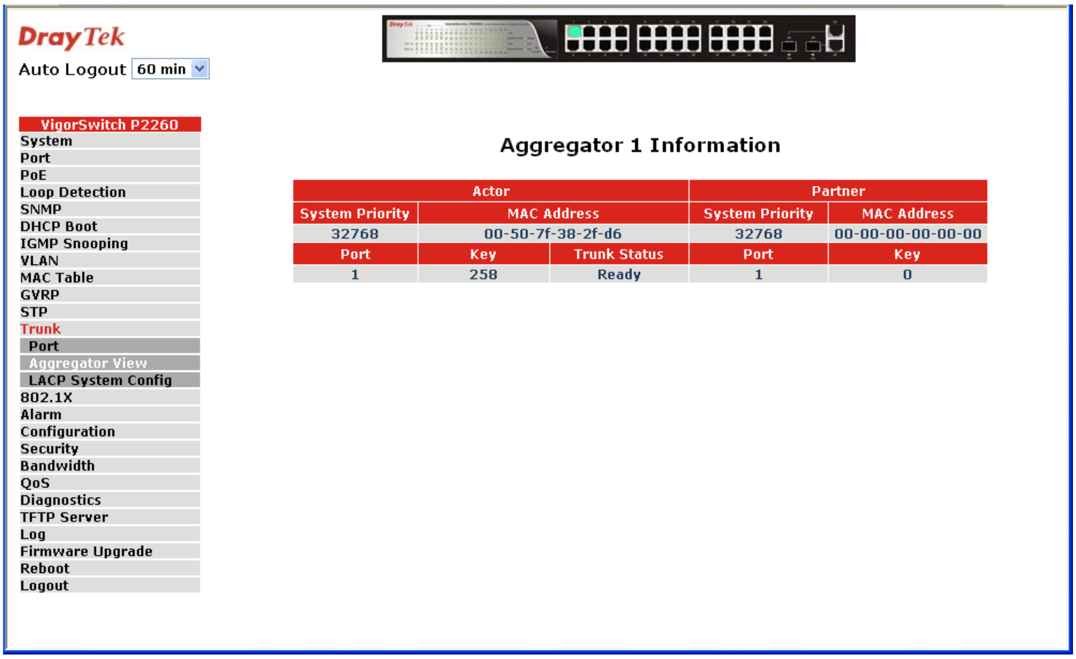
LACP Detail

Function name:

LACP Detail (LACP Aggregator Detailed Information)

Function description:

Show the detailed information of the LACP trunking group.



Auto Logout 60 min

Aggregator 1 Information

Actor			Partner	
System Priority	MAC Address		System Priority	MAC Address
32768	00-50-7f-38-2f-d6		32768	00-00-00-00-00-00
Port	Key	Trunk Status	Port	Key
1	258	Ready	1	0

Parameter description:

Actor: The switch you are watching on.

Partner: The peer system from this aggregator’s view.

System Priority: Show the System Priority part of a system ID.

MAC Address: Show the MAC Address part of a system ID.

Port: Show the port number part of an LACP port ID.

Key: Show the key value of the aggregator. The key value is determined by the LACP protocol entity and can’t be set through management.

Trunk Status: Show the trunk status of a single member port. “---” means “not ready”

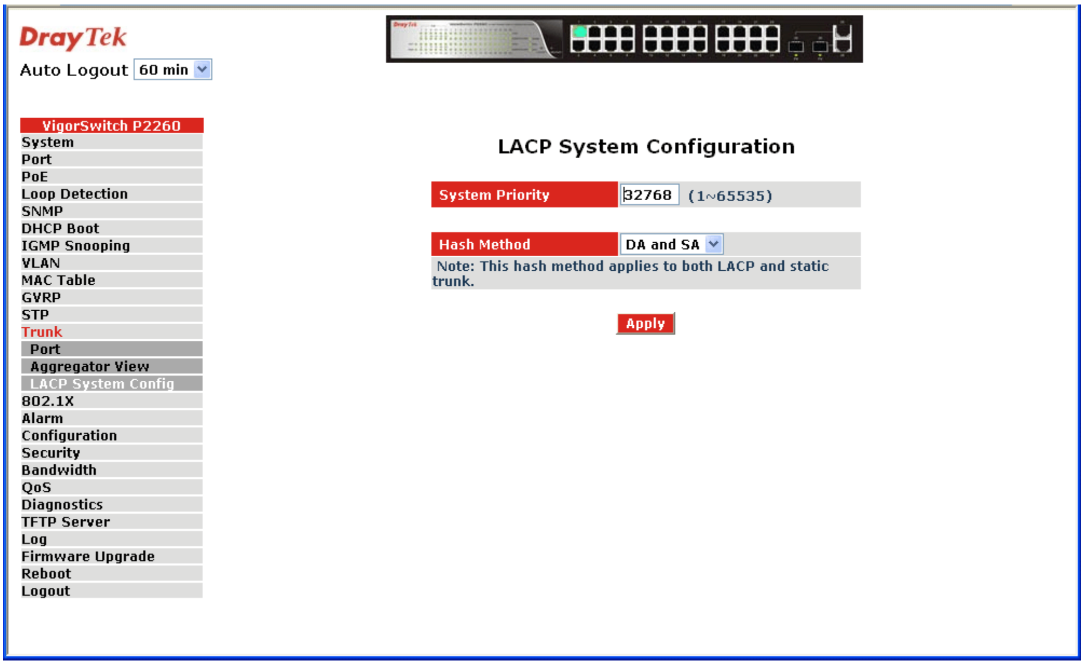
2.12.3 LACP System Priority

Function name:

LACP System Priority

Function description:

It is used to set the priority part of the LACP system ID. LACP will only aggregate together the ports whose peer link partners are all on a single system. Each system supports LACP will be assigned a globally unique System Identifier for this purpose. A system ID is a 64-bit field comprising a 48-bit MAC Address and 16-bit priority value.



LACP System Configuration

System Priority	32768 (1~65535)
Hash Method	DA and SA

Note: This hash method applies to both LACP and static trunk.

Parameter description:

System Priority: The System Priority can be set by the user. Its range is from 1 to 65535. Default: 32768.

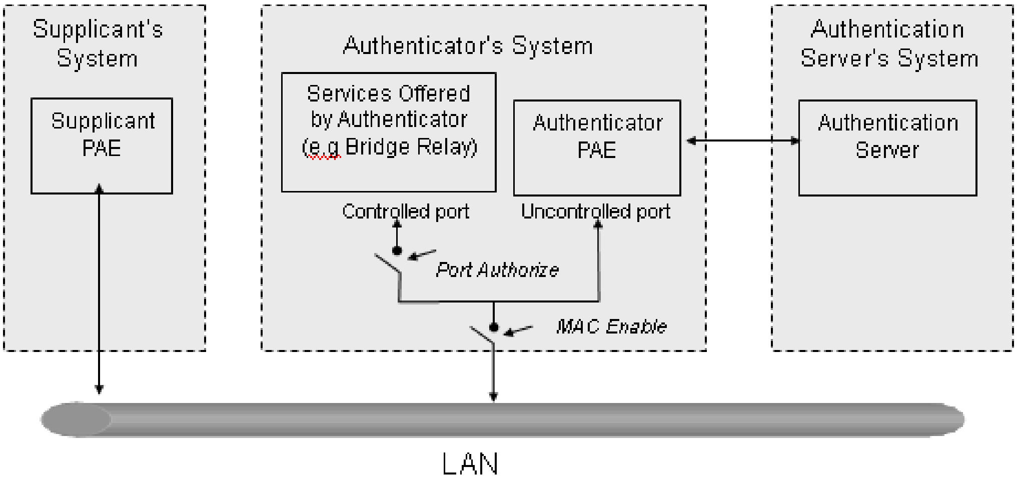
Hash Method: DA+SA, DA and SA are three Hash methods offered for the Link Aggregation of the switch. Packets will decide the path to transmit according to the mode of Hash you choose. Default: DA and SA

2.13 802.1X Configuration

802.1X port-based network access control provides a method to restrict users to access network resources via authenticating user’s information. This restricts users from gaining access to the network resources through a 802.1X-enabled port without authentication. If a user wishes to touch the network through a port under 802.1X control, he (she) must firstly input his (her) account name for authentication and waits for gaining authorization before sending or receiving any packets from a 802.1X-enabled port.

Before the devices or end stations can access the network resources through the ports under 802.1X control, the devices or end stations connected to a controlled port send the authentication request to the authenticator, the authenticator pass the request to the authentication server to authenticate and verify, and the server tell the authenticator if the request get the grant of authorization for the ports.

According to IEEE802.1X, there are three components implemented. They are Authenticator, Supplicant and Authentication server shown in figure below.



Supplicant:

It is an entity being authenticated by an authenticator. It is used to communicate with the Authenticator PAE (Port Access Entity) by exchanging the authentication message when the Authenticator PAE request to it.

Authenticator:

An entity facilitates the authentication of the supplicant entity. It controls the state of the port, authorized or unauthorized, according to the result of authentication message exchanged between it and a supplicant PAE. The authenticator may request the supplicant to re-authenticate itself at a configured time period. Once start re-authenticating the supplicant, the controlled port keeps in the authorized state until re-authentication fails.

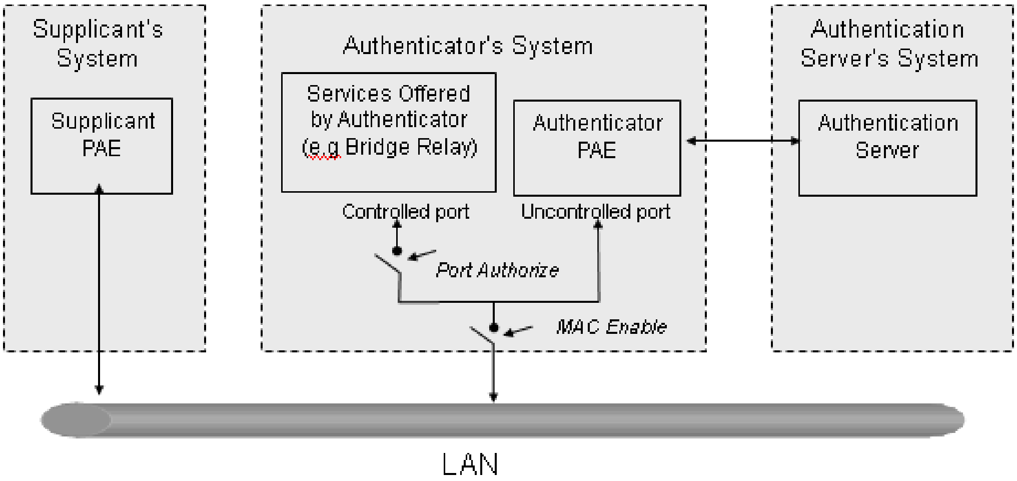
A port acting as an authenticator is thought to be two logical ports, a controlled port and an uncontrolled port. A controlled port can only pass the packets when the authenticator PAE is authorized, and otherwise, an uncontrolled port will unconditionally pass the packets with PAE group MAC address, which has the value of 01-80-c2-00-00-03 and will not be forwarded by MAC bridge, at any time.

Authentication server:

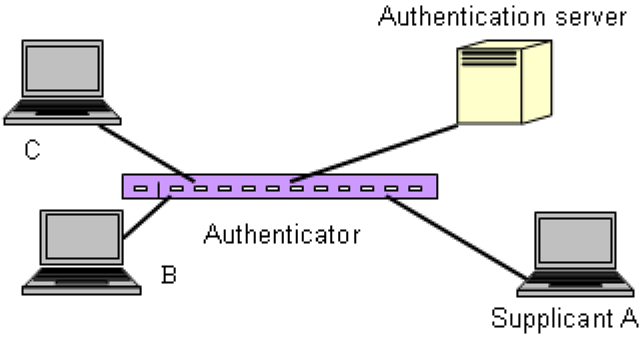
A device provides authentication service, through EAP, to an authenticator by using authentication credentials supplied by the supplicant to determine if the supplicant is authorized to access the network resource.

The overview of operation flow for the Fig. 3-52 is quite simple. When Supplicant PAE issues a request to Authenticator PAE, Authenticator and Supplicant exchanges authentication message. Then, Authenticator passes the request to RADIUS server to verify. Finally, RADIUS server replies if the request is granted or denied.

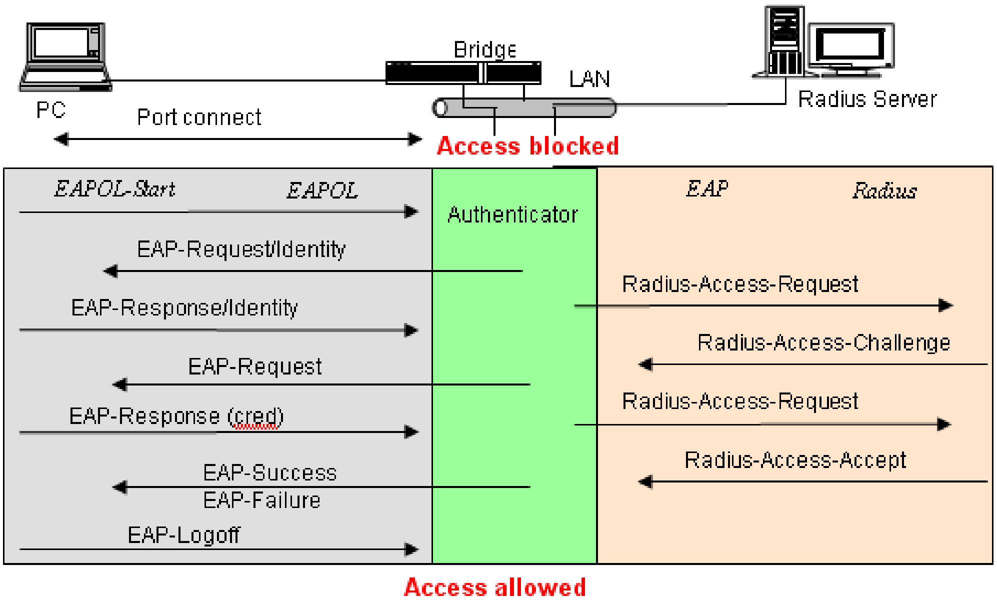
While in the authentication process, the message packets, encapsulated by Extensible Authentication Protocol over LAN (EAPOL), are exchanged between an authenticator PAE and a supplicant PAE. The Authenticator exchanges the message to authentication server using EAP encapsulation. Before successfully authenticating, the supplicant can only touch the authenticator to perform authentication message exchange or access the network from the uncontrolled port.



In the following figure, this is the typical configuration, a single supplicant, an authenticator and an authentication server. B and C is in the internal network, D is Authentication server running RADIUS, switch at the central location acts Authenticator connecting to PC A and A is a PC outside the controlled port, running Supplicant PAE. In this case, PC A wants to access the services on device B and C, first, it must exchange the authentication message with the authenticator on the port it connected via EAPOL packet. The authenticator transfers the supplicant's credentials to Authentication server for verification. If success, the authentication server will notice the authenticator the grant. PC A, then, is allowed to access B and C via the switch. If there are two switches directly connected together instead of single one, for the link connecting two switches, it may have to act two port roles at the end of the link: authenticator and supplicant, because the traffic is bi-directional.



The figure below shows the procedure of 802.1X authentication.



There are steps for the login based on 802.1X port access control management. The protocol used in the right side is EAPOL and the left side is EAP.

1. At the initial stage, the supplicant A is unauthenticated and a port on switch acting as an authenticator is in unauthorized state. So the access is blocked in this stage.
2. Initiating a session. Either authenticator or supplicant can initiate the message exchange. If supplicant initiates the process, it sends EAPOL-start packet to the authenticator PAE and authenticator will immediately respond EAP-Request/Identity packet.
3. The authenticator always periodically sends EAP-Request/Identity to the supplicant for requesting the identity it wants to be authenticated.
4. If the authenticator doesn't send EAP-Request/Identity, the supplicant will initiate EAPOL-Start the process by sending to the authenticator.
5. And next, the Supplicant replies an EAP-Response/Identity to the authenticator. The authenticator will embed the user ID into Radius-Access-Request command and send it to the authentication server for confirming its identity.
6. After receiving the Radius-Access-Request, the authentication server sends Radius-Access-Challenge to the supplicant for asking for inputting user password via the authenticator PAE.
7. The supplicant will convert user password into the credential information, perhaps, in MD5 format and replies an EAP-Response with this credential information as well as the specified authentication algorithm (MD5 or OTP) to Authentication server via the authenticator PAE. As per the value of the type field in message PDU, the authentication server knows which algorithm should be applied to authenticate the credential information, EAP-MD5 (Message Digest 5) or EAP-OTP (One Time Password) or other else algorithm.
8. If user ID and password is correct, the authentication server will send a Radius-Access-Accept to the authenticator. If not correct, the authentication server will send a Radius-Access-Reject.
9. When the authenticator PAE receives a Radius-Access-Accept, it will send an EAP-Success to the supplicant. At this time, the supplicant is authorized and the port

connected to the supplicant and under 802.1X control is in the authorized state. The supplicant and other devices connected to this port can access the network. If the authenticator receives a Radius-Access-Reject, it will send an EAP-Failure to the supplicant. This means the supplicant is failed to authenticate. The port it connected is in the unauthorized state, the supplicant and the devices connected to this port won't be allowed to access the network.

10. When the supplicant issue an EAP-Logoff message to Authentication server, the port you are using is set to be unauthorized.

Only MultiHost 802.1X is the type of authentication supported in the switch. In this mode, for the devices connected to this port, once a supplicant is authorized, the devices connected to this port can access the network resource through this port.

802.1X Port-based Network Access Control function supported by the switch is little bit complex, for it just support basic Multihost mode, which can distinguish the device's MAC address and its VID. The following table is the summary of the combination of the authentication status and the port status versus the status of port mode, set in 802.1X Port mode, port control state, set in 802.1X port setting. Here Entry Authorized means MAC entry is authorized.

Port Mode	**Port Control**	**Authentication**	**Port Status**
Disable	Don't Care	Don't Care	Port Uncontrolled
Multihost	Auto	Successful	Port Authorized
Multihost	Auto	Failure	Port Unauthorized
Multihost	ForceUnauthorized	Don't Care	Port Unauthorized
Multihost	ForceAuthorized	Don't Care	Port Authorized

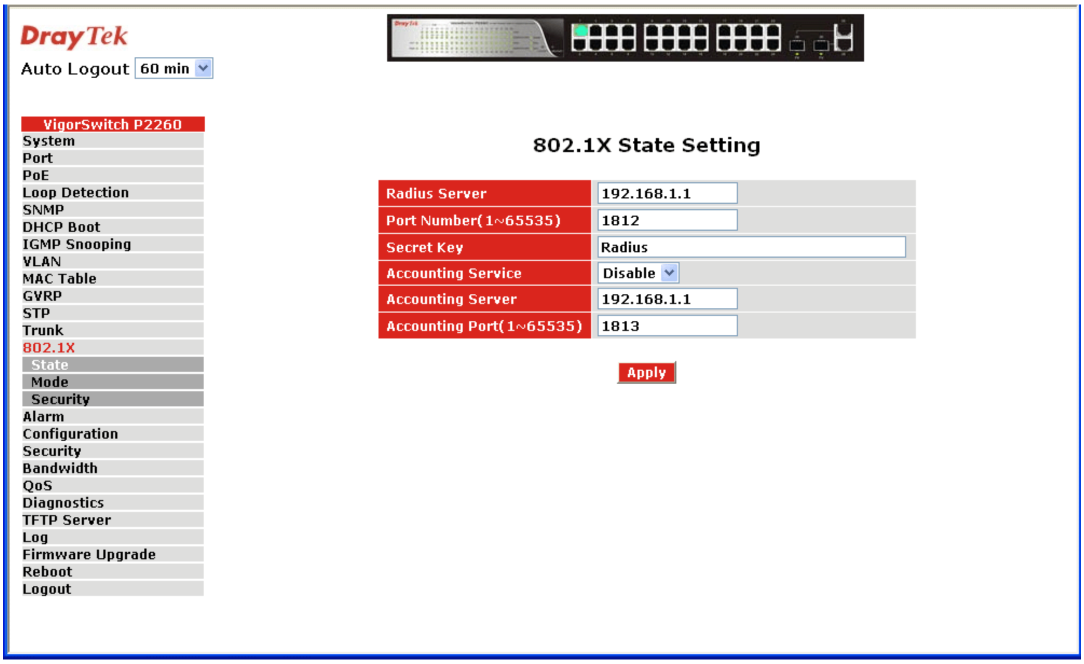
2.13.1 802.1X State Setting

Function name:

802.1X State Setting

Function description:

This function is used to configure the global parameters for RADIUS authentication in 802.1X port security application.



802.1X State Setting

Radius Server	192.168.1.1
Port Number(1~65535)	1812
Secret Key	Radius
Accounting Service	Disable
Accounting Server	192.168.1.1
Accounting Port(1~65535)	1813

Parameter description:

Radius Server:	RADIUS server IP address for authentication. Default: 192.168.1.1
Port Number:	The port number to communicate with RADIUS server for the authentication service. The valid value ranges 1-65535. Default port number is 1812.
Secret Key:	The secret key between authentication server and authenticator. It is a string with the length 1 – 31 characters. The character string may contain upper case, lower case and 0-9. It is character sense. It is not allowed for putting a blank between any two characters. Default: Radius
Accounting Service	Enable or disable the Accounting service for client accounting with Accounting Server.
Accounting Server	Indicate the Accounting Server IP address for accounting.
Accounting Port	Type the UDP Port. Default port number is 1812.

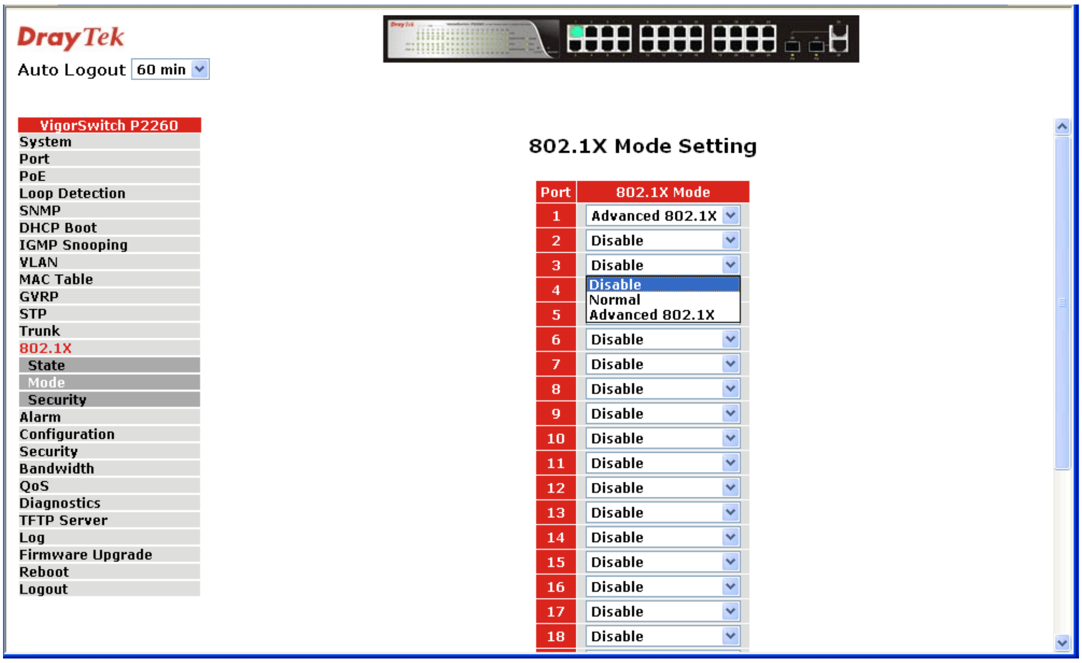
2.13.2 802.1X Mode Setting

Function name:

802.1X Mode Setting

Function description:

Set the operation mode of 802.1X for each port. In this device, it supports only Multi-host operation mode.



802.1X Mode Setting

Port	802.1X Mode
1	Advanced 802.1X
2	Disable
3	Disable
4	Disable Normal Advanced 802.1X
5	
6	Disable
7	Disable
8	Disable
9	Disable
10	Disable
11	Disable
12	Disable
13	Disable
14	Disable
15	Disable
16	Disable
17	Disable
18	Disable

Parameter description:

Port Number: Indicate which port is selected to configure the 802.1X operation mode.

802.1X Mode: 802.1X operation mode. There are three options, including Disable, Normal and Advanced 802.1x mode. Default is Disable.

- Disable - It will have the chosen port acting as a plain port, that is no 802.1X port access control works on the port.

- Normal - In this mode, for the devices connected to this port, once a supplicant is authorized, the devices connected to this port can access the network resource through this port.

- Advanced 802.1x – In this mode, each client under this port has to do 802.1X authentication by himself.

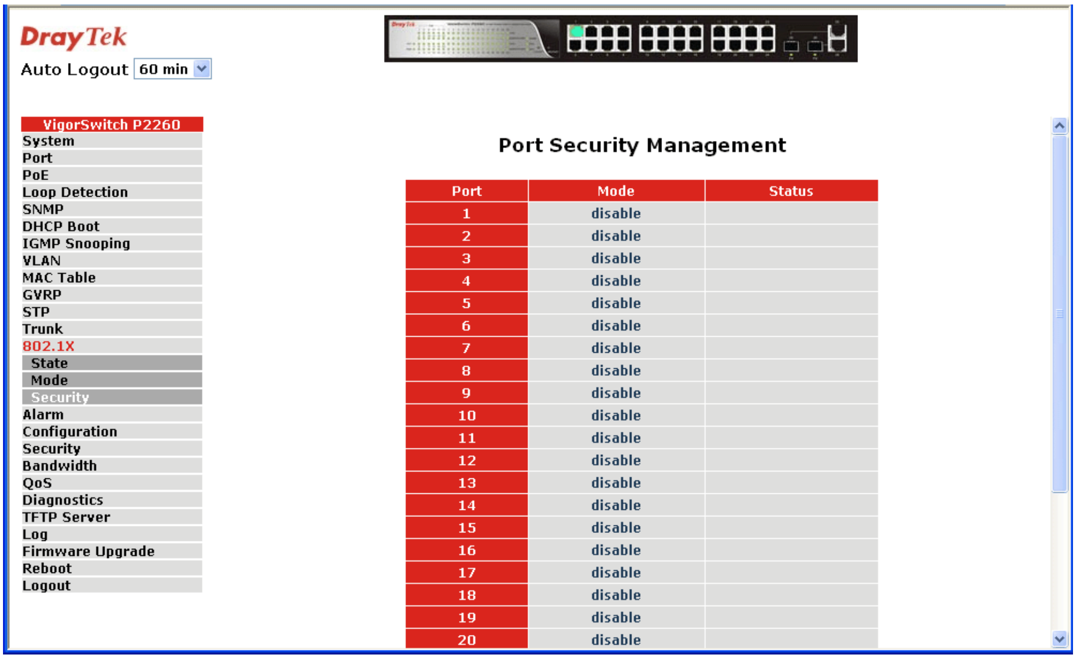
2.13.3 Port Security Management

Function name:

Port Security Management

Function description:

Show each port status. In Multi-host mode, it shows the port number and its status, authorized or unauthorized.



Port Security Management

Port	Mode	Status
1	disable	
2	disable	
3	disable	
4	disable	
5	disable	
6	disable	
7	disable	
8	disable	
9	disable	
10	disable	
11	disable	
12	disable	
13	disable	
14	disable	
15	disable	
16	disable	
17	disable	
18	disable	
19	disable	
20	disable	

Parameter description:

Port Number: The port number to be chosen to show its 802.1X Port Status. The valid number is Port 1 – 26.

Disable Mode: When selecting Disable mode for a port in the function 802.1X Port Mode Configuration, the port is in the uncontrolled port state and does not apply 802.1X authenticator on it. Any node attached on this port can access the network without the admittance of 802.1X authenticator. The Port Status will show the following screen.

Port Status: The current 802.1X status of the port. In Disable mode, this field is disabled.

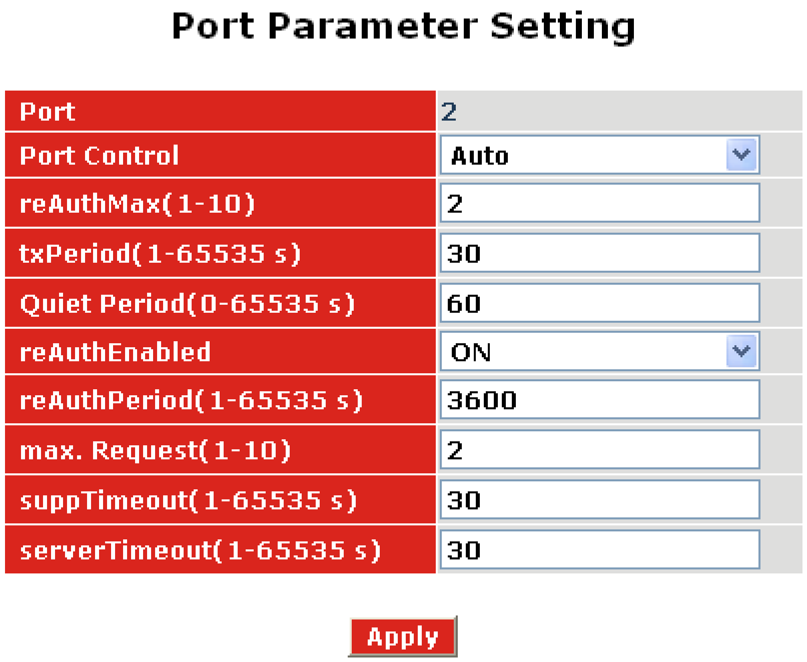
Param. Setting

Function name:

Param. Setting

Function description:

This function is used to configure the parameters for each port in 802.1X port security application. Refer to the following parameters description for details.



Port Parameter Setting

Port	2
Port Control	Auto
reAuthMax(1-10)	2
txPeriod(1-65535 s)	30
Quiet Period(0-65535 s)	60
reAuthEnabled	ON
reAuthPeriod(1-65535 s)	3600
max. Request(1-10)	2
suppTimeout(1-65535 s)	30
serverTimeout(1-65535 s)	30

Parameter description:

Port: It is the port number to be selected for configuring its associated 802.1X parameters which are Port control, reAuthMax, txPeriod, Quiet Period, reAuthEnabled, reAuthPeriod, max. Request, suppTimeout, serverTimeout and Controlled direction.

Port Control: This is used to set the operation mode of authorization. There are three type of operation mode supported, ForceUnauthorized, ForceAuthorized, Auto.

ForceUnauthorized - The controlled port is forced to hold in the unauthorized state.

ForceAuthorized - The controlled port is forced to hold in the authorized state.

Auto - The controlled port is set to be in authorized state or unauthorized state depends on the result of the authentication exchange between the authentication server and the supplicant.
Default: Auto

reAuthMax (1-10): The number of authentication attempt that is permitted before the port becomes unauthorized.
Default: 2

txPeriod (1-65535 s): A time period to transmitted EAPOL PDU between the authenticator and the supplicant.
Default: 30

Quiet Period (0-65535 s): A period of time during which we will not attempt to access the supplicant.
Deafult: 60 seconds

reAuthEnabled: Choose whether regular authentication will take place in this port.
Default: ON

reAuthPeriod (1-65535 s): A non-zero number seconds between the periodic re-authentication of the supplicant.
Default: 3600

max. Request (1-10): The maximum of number times that the authenticator will retransmit an EAP Request to the supplicant before it times out the authentication session. The valid range: 1 – 10.
Default: 2 times

suppTimeout (1-65535 s): A timeout condition in the exchange between the authenticator and the supplicant. The valid range: 1 –65535.
Default: 30 seconds.

serverTimeout (1-65535 s): A timeout condition in the exchange between the authenticator and the authentication server. The valid range: 1 –65535.
Default: 30 seconds

2.14 Alarm Configuration

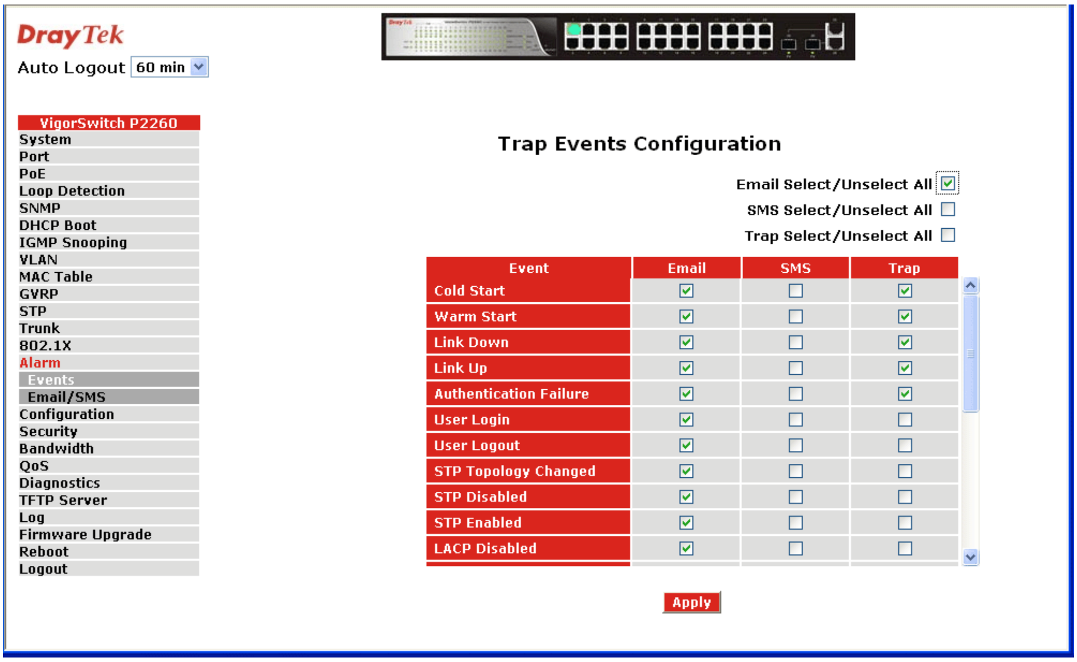
2.14.1 Events Configuration

Function name:

Events Configuration

Function description:

The Trap Events Configuration function is used to enable the switch to send out the trap information while pre-defined trap events occurred. The switch offers 24 different trap events to users for switch management. The trap information can be sent out in three ways, including email, mobile phone SMS (short message system) and trap. The message will be sent while users tick (☑) the trap event individually on the web page shown as below.



Trap Events Configuration

Email Select/Unselect All ☑
SMS Select/Unselect All □
Trap Select/Unselect All □

Event	Email	SMS	Trap
Cold Start	☑	□	☑
Warm Start	☑	□	☑
Link Down	☑	□	☑
Link Up	☑	□	☑
Authentication Failure	☑	□	☑
User Login	☑	□	□
User Logout	☑	□	□
STP Topology Changed	☑	□	□
STP Disabled	☑	□	□
STP Enabled	☑	□	□
LACP Disabled	☑	□	□

Parameter description:

Trap:	Cold Start, Warm Start, Link Down, Link Up, Authentication Failure, User login, User logout
STP:	STP Topology Changed, STP Disabled, STP Enabled
LACP:	LACP Disabled, LACP Enabled, LACP Member Added, LACP Port Failure
GVRP:	GVRP Disabled, GVRP Enabled
VLAN:	VLAN Disabled, Port-based VLAN Enabled, Tag-based VLAN Enabled, Metro-mode Vlan Enabled, Double-tag Vlan Enabled
Module Swap:	Module Inserted, Module Removed, Dual Media Swapped

This page only provides fixed event table for user to select and asks device sending the trap when the event happens**.**

2.14.2 Email/SMS Configuration

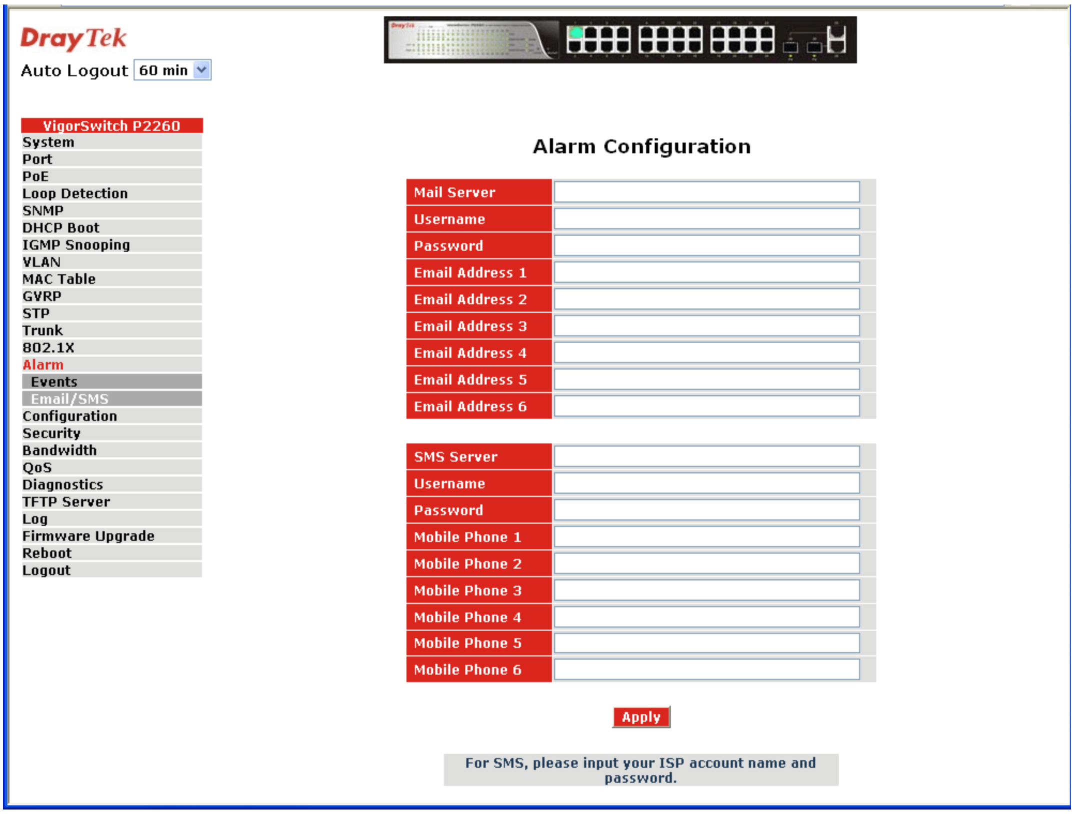
Function name:

Email/SMS Configuration

Function description:

Alarm configuration is used to configure the persons who should receive the alarm message via either email or SMS, or both. It depends on your settings. An email address or a mobile phone number has to be set in the web page of alarm configuration (See Fig. 3-60). Then, user can read the trap information from the email or the mobile phone. This function provides 6 email addresses and 6 mobile phone numbers at most. The 24 different trap events will be sent out to SNMP Manager when trap event occurs. After ticking trap events, you can fill in your desired email addresses and mobile phone numbers. Then, please click **<Apply>** button to complete the alarm configuration. It will take effect in a few seconds.

> **Note:** SMS may not work in your mobile phone system. It is customized for different systems.



Alarm Configuration

Mail Server	
Username	
Password	
Email Address 1	
Email Address 2	
Email Address 3	
Email Address 4	
Email Address 5	
Email Address 6	

SMS Server	
Username	
Password	
Mobile Phone 1	
Mobile Phone 2	
Mobile Phone 3	
Mobile Phone 4	
Mobile Phone 5	
Mobile Phone 6	

Apply

For SMS, please input your ISP account name and password.

Parameter description:

Email:	Mail Server: the IP address of the server transferring your email. Username: your username on the mail server. Password: your password on the mail server. Email Address 1 – 6: email address that would like to receive the alarm message.
SMS:	SMS Server: the IP address of the server transferring your SMS. Username: your username in ISP.

Password: your username in ISP.

Mobile Phone 1-6: the mobile phone number that would like to receive the alarm message.

2.15 Configuration

The switch supports three copies of configuration, including the default configuration, working configuration and user configuration for your configuration management. All of them are listed and described below respectively.

Default Configuration

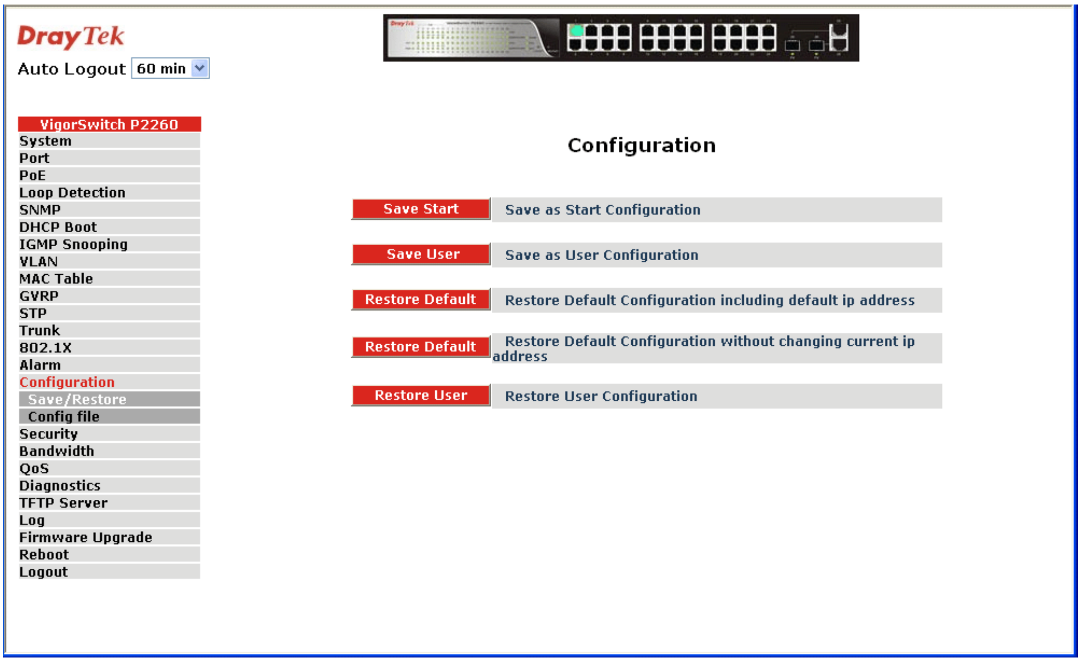
This is the ex-factory setting and cannot be altered. In Web UI, two restore default functions are offered for the user to restore to the default setting of the switch. One is the function of "Restore Default Configuration included default IP address", the IP address will restore to default "192.168.1.1" as you use it. The other is the function of "Restore Default Configuration without changing current IP address", the IP address will keep the same one that you had saved before by performing this function.

Working Configuration

It is the configuration you are using currently and can be changed any time. The configurations you are using are saved into this configuration file. This is updated each time as you press <**Apply**> button.

User Configuration

It is the configuration file for the specified or backup purposes and can be updated while having confirmed the configuration. You can retrieve it by performing Restore User Configuration.



Configuration

Save Start	Save as Start Configuration
Save User	Save as User Configuration
Restore Default	Restore Default Configuration including default ip address
Restore Default	Restore Default Configuration without changing current ip address
Restore User	Restore User Configuration

2.15.1 Save/Restore

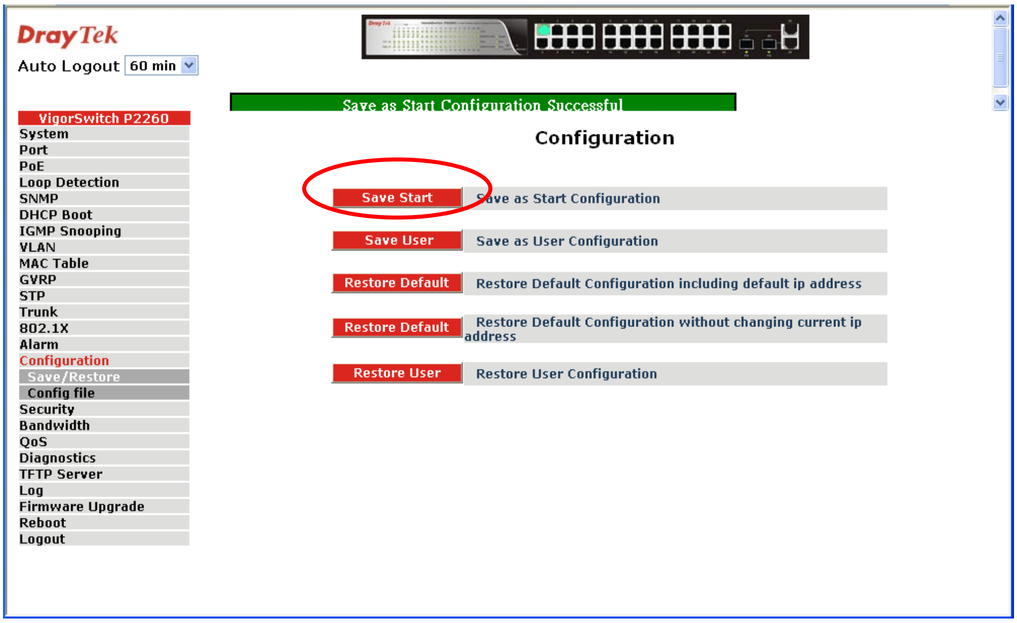
Save As Start Configuration

Function name:

Save As Start Configuration

Function description:

Save the current configuration as a start configuration file in flash memory.



Save as Start Configuration Successful

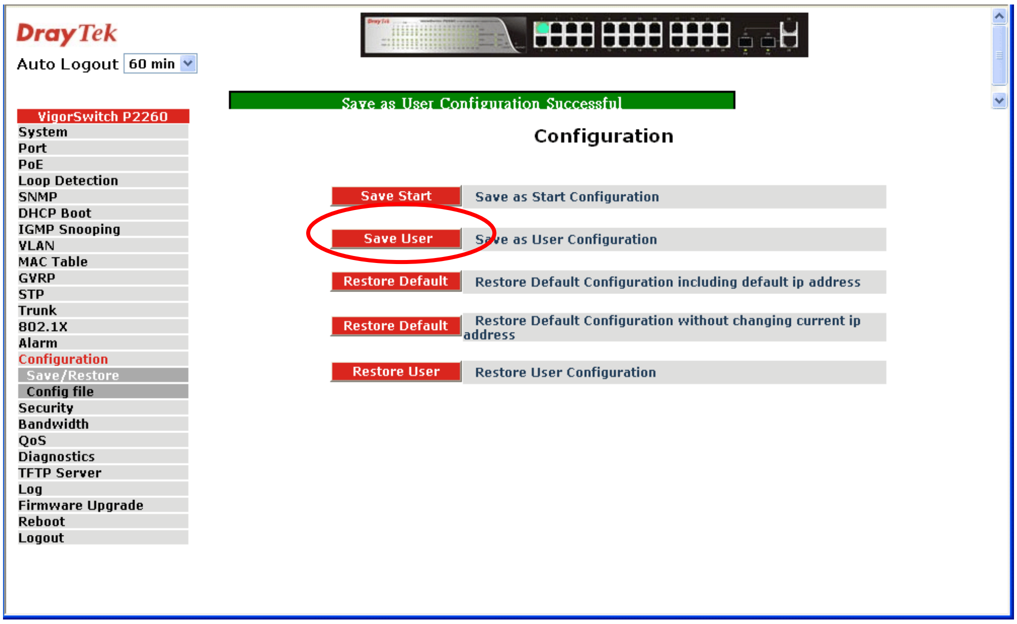
Save As User Configuration

Function name:

Save As User Configuration

Function description:

Save the current configuration as a user configuration file in flash memory.



Save as User Configuration Successful

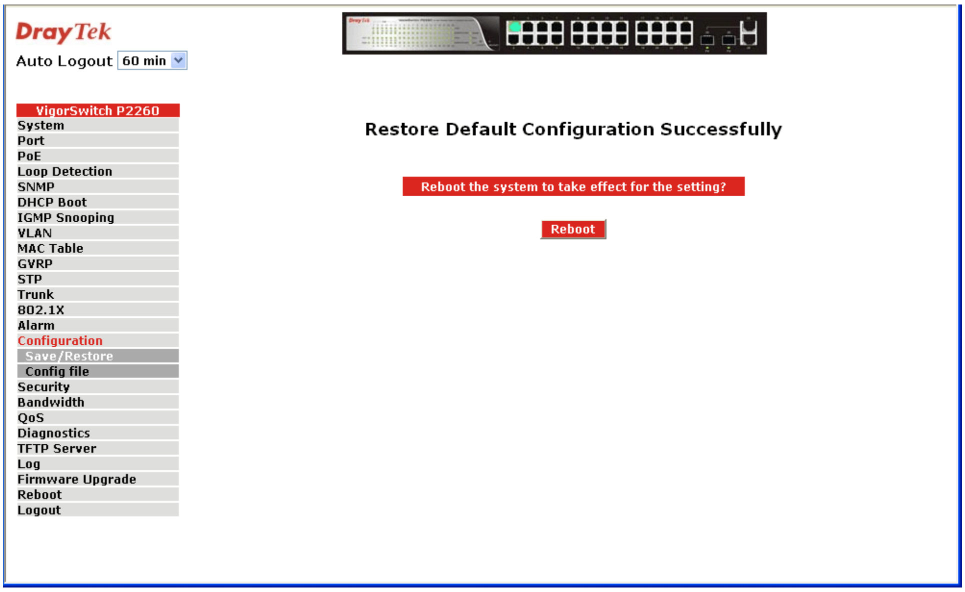
Restore Default Configuration (includes default IP address)

Function name:

Restore Default Configuration (includes default IP address)

Function description:

Restore Default Configuration function can retrieve the ex-factory setting to replace the start configuration. And the IP address of the switch will also be restored to 192.168.1.1.



Restore Default Configuration Successfully

Reboot the system to take effect for the setting?

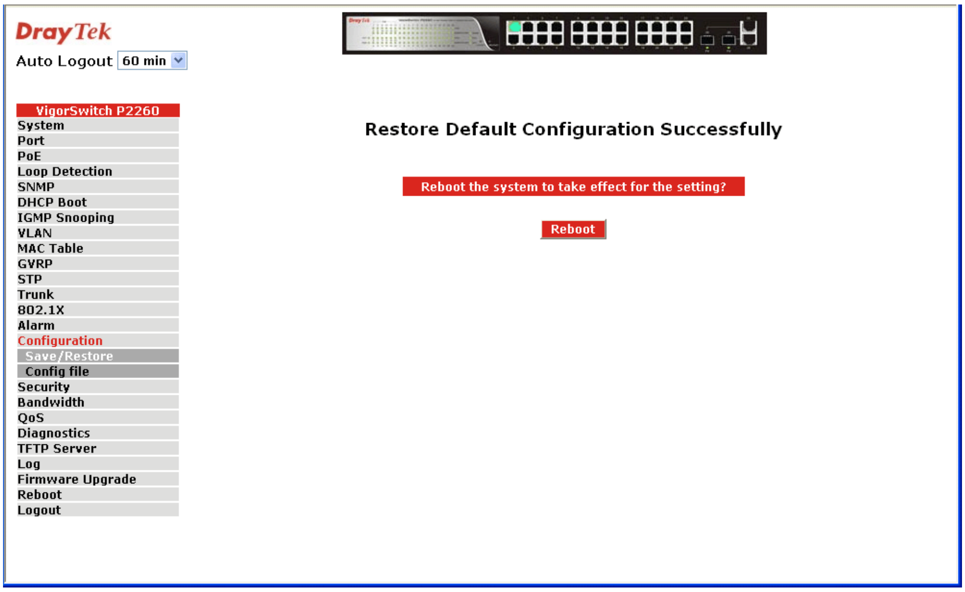
Restore Default Configuration (excludes current IP address)

Function name:

Restore Default Configuration (excludes current IP address)

Function description:

Restore Default Configuration function can retrieve the ex-factory setting to replace the start configuration. However, the switch’s current IP address that the user set up will not be changed and will NOT be restored to 192.168.1.1 as well.



Restore Default Configuration Successfully

Reboot the system to take effect for the setting?

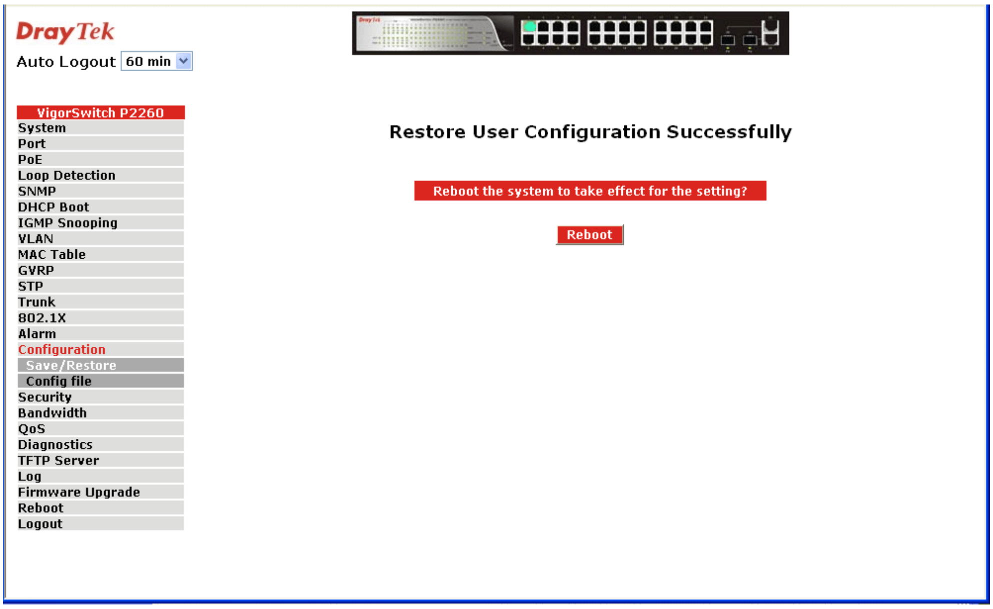
Restore User Configuration

Function name:

Restore User Configuration

Function description:

Restore User Configuration function can retrieve the previous confirmed working configuration stored in the flash memory to update start configuration. When completing to restore the configuration, the system's start configuration is updated and will be changed its system settings after rebooting the system.



Restore User Configuration Successfully

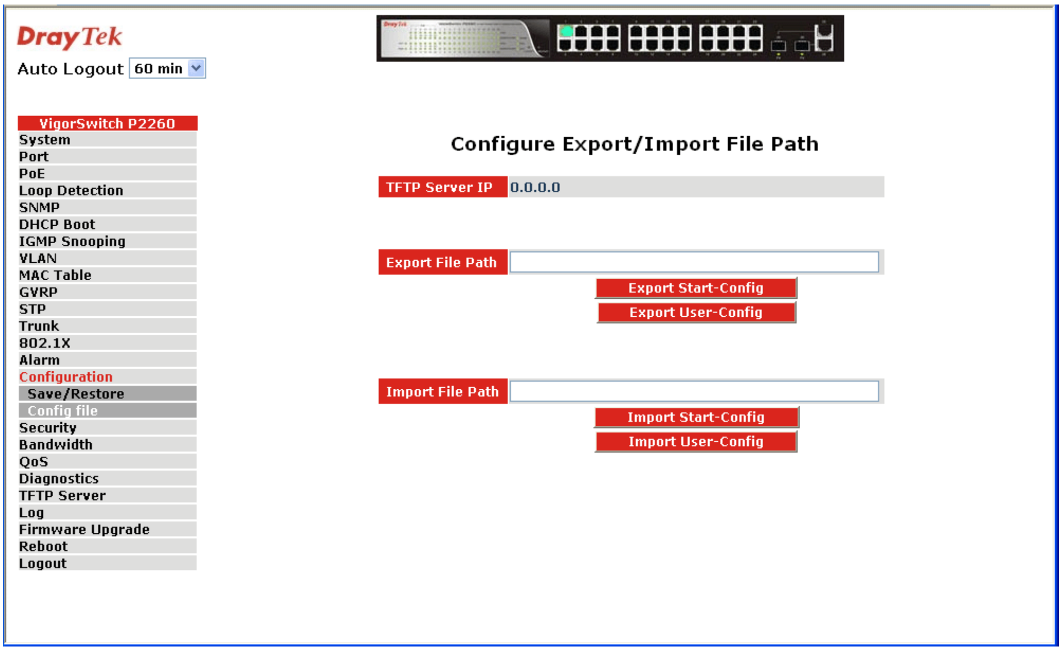
2.15.2 Config File

Function name:

Config File

Function description:

With this function, user can back up or reload the config files of Save As Start or Save As User via TFTP.



Configure Export/Import File Path

TFTP Server IP 0.0.0.0

Export File Path

Import File Path

Parameter description:

Export File Path:	*Export Start* -Export Save As Start's config file stored in the flash. *Export User-Conf* - Export Save As User's config file stored in the flash.
Import File Path:	*Import Start* -Import Save As Start's config file stored in the flash. *Import User-Conf* - Import Save As User's config file stored in the flash.

2.16 Security

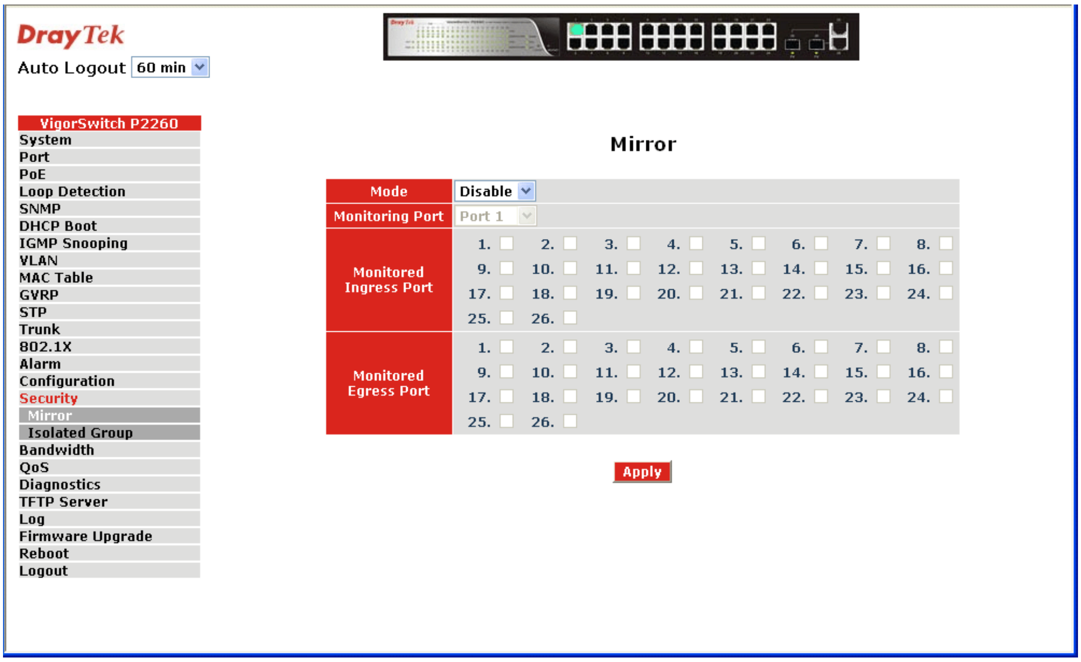
2.16.1 Mirror

Function name:

Mirror Configuration

Function description:

Mirror Configuration is to monitor the traffic of the network. For example, we assume that Port A and Port B are Monitoring Port and Monitored Port respectively, thus, the traffic received by Port B will be copied to Port A for monitoring.



Mirror

Mode	Disable							
Monitoring Port	Port 1							
Monitored Ingress Port	1. □	2. □	3. □	4. □	5. □	6. □	7. □	8. □
	9. □	10. □	11. □	12. □	13. □	14. □	15. □	16. □
	17. □	18. □	19. □	20. □	21. □	22. □	23. □	24. □
	25. □	26. □						
Monitored Egress Port	1. □	2. □	3. □	4. □	5. □	6. □	7. □	8. □
	9. □	10. □	11. □	12. □	13. □	14. □	15. □	16. □
	17. □	18. □	19. □	20. □	21. □	22. □	23. □	24. □
	25. □	26. □						

Apply

Parameter description:

Mode:	Used for the activation or de-activation of Port Mirror function. Default is “Disable”.
Monitoring Port:	Set up the port for monitoring. Valid port is Port 1~26 and default is Port 1.
Monitored Ingress Port:	Set up the port for being monitored. It only monitor the packets received by the port you set up. Just tick the check box (☑) beside the port x and valid port is Port 1~26.
Monitored Egress Port:	Set up the port for being monitored. It only monitor the packets transmitted by the port you set up. Just tick the check box (☑) beside the port x and valid port is Port 1~26.

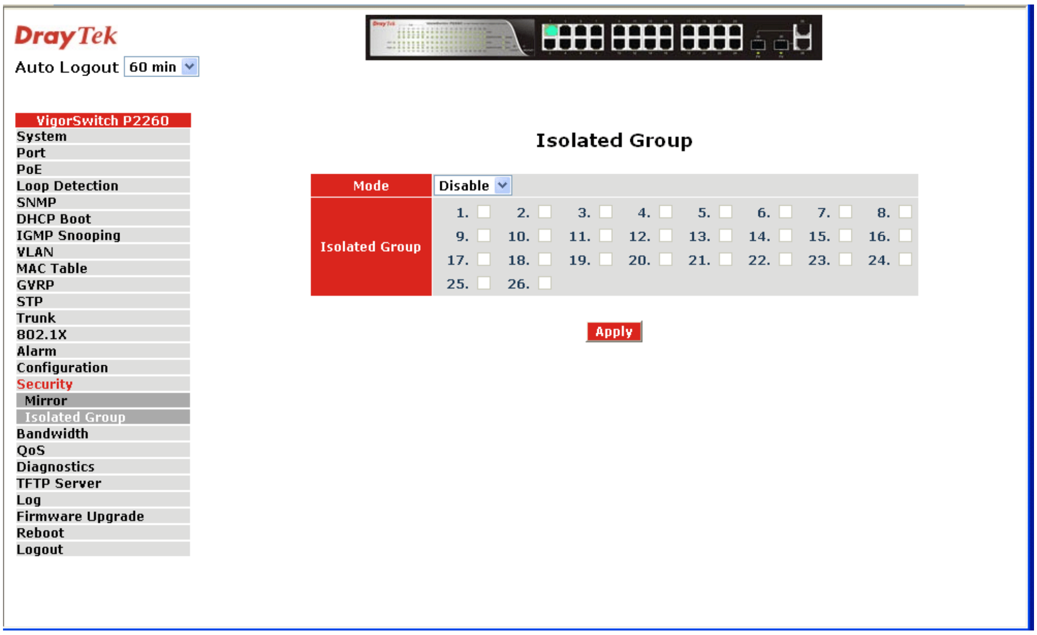
2.16.2 Isolated Group

Function name:

Isolated Group

Function description:

Isolated Group function can let the port be independent of other ports in the Isolated group, and the communication is also forbidden between these ports. But, the ports of the Isolated group are still able to communicate with the ports of the non-Isolated group. With this design, it will be helpful to the administrator to immediately find and solve the port that results in the occurrence of looping problems in the network.



Isolated Group

Mode	Disable							
Isolated Group	1. □	2. □	3. □	4. □	5. □	6. □	7. □	8. □
	9. □	10. □	11. □	12. □	13. □	14. □	15. □	16. □
	17. □	18. □	19. □	20. □	21. □	22. □	23. □	24. □
	25. □	26. □						

Apply

Parameter description:

Mode: Used for the activation or de-activation of Isolated Group function. Default is “Disable”.

Isolated Group: User can choose any port to be the member of this group. Just tick the check box (☑) beside the port x and valid port is Port 1~26. In this group, all of these member ports cannot forward packets with each other. Thus, the switch will not be capable of forwarding any packets in case its all ports become the members of the Isolated group.

2.17 Bandwidth Management

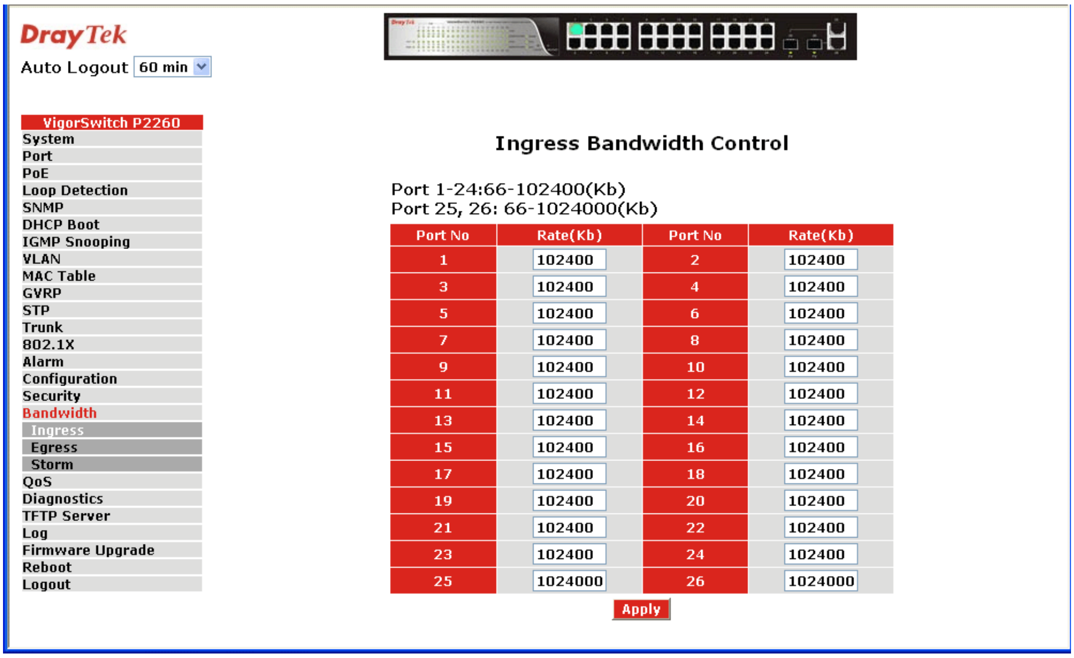
2.17.1 Ingress

Function name:

Ingress Bandwidth Control

Function description:

Ingress Bandwidth Setting function is used to set up the limit of Ingress bandwidth for each port.



Ingress Bandwidth Control

Port 1-24:66-102400(Kb)
Port 25, 26: 66-1024000(Kb)

Port No	Rate(Kb)	Port No	Rate(Kb)
1	102400	2	102400
3	102400	4	102400
5	102400	6	102400
7	102400	8	102400
9	102400	10	102400
11	102400	12	102400
13	102400	14	102400
15	102400	16	102400
17	102400	18	102400
19	102400	20	102400
21	102400	22	102400
23	102400	24	102400
25	1024000	26	1024000

Parameter description:

Port Number: Choose the port that you would like this function to work on it. Valid range of the port is 1~26.

Rate: Set up the limit of Ingress bandwidth for the port you choose. Incoming traffic will be discarded if the rate exceeds the value you set up in Data Rate field. Pause frames are also generated if flow control is enabled. The format of the packet limits to unicast, broadcast and multicast. Valid value of Port 1~24 ranges from 66~102400, and Port 25~26 ranges from 66~1024000 with the minimum unit of 1. Default value of Port 1~24 is 102400 and Port 25~26 is 1024000.

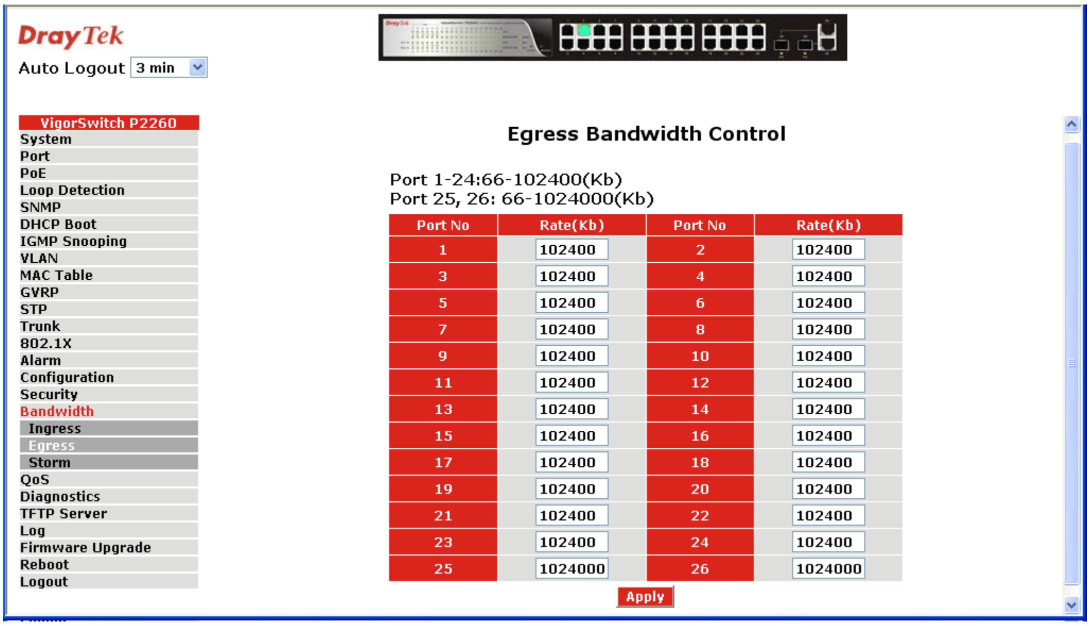
2.17.2 Egress

Function name:

Ingress Bandwidth Control/Egress Bandwidth Control

Function description:

Egress Bandwidth Setting function is used to set up the limit of Egress bandwidth for each port.



Egress Bandwidth Control

Port 1-24:66-102400(Kb)
Port 25, 26: 66-1024000(Kb)

Port No	Rate(Kb)	Port No	Rate(Kb)
1	102400	2	102400
3	102400	4	102400
5	102400	6	102400
7	102400	8	102400
9	102400	10	102400
11	102400	12	102400
13	102400	14	102400
15	102400	16	102400
17	102400	18	102400
19	102400	20	102400
21	102400	22	102400
23	102400	24	102400
25	1024000	26	1024000

Parameter description:

Port Number: Choose the port that you would like this function to work on it. Valid range of the port is 1~26.

Rate: Set up the limit of Egress bandwidth for the port you choose. Packet transmission will be delayed if the rate exceeds the value you set up in Data Rate field. Traffic may be lost if egress buffers run full. The format of the packet limits to unicast, broadcast and multicast. Valid value of Port 1~24 ranges from 66~102400, and Port 25~26 ranges from 66~1024000 with the minimum unit of 1. Default value of Port 1~24 is 102400 and Port 25~26 is 1024000.

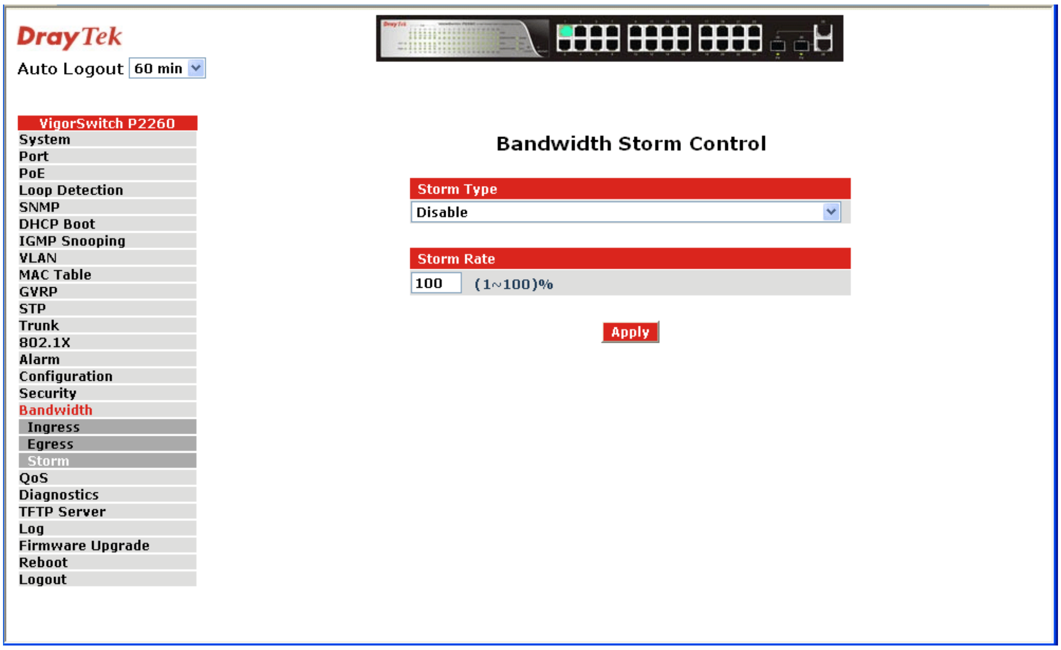
2.17.3 Storm

Function name:

Bandwidth Storm Control

Function description:

Bandwidth Management function is used to set up the limit of Ingress and Egress bandwidth for each port.



Bandwidth Storm Control

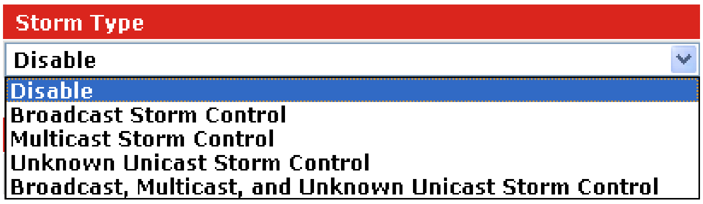
Storm Type: Disable

Storm Rate: 100 (1~100)%

Parameter description:

Storm Type:

Disable - Disable the function of the bandwidth storm control.
Broadcast Storm Control - Enable the function of bandwidth storm control for broadcast packets.
Multicast Storm Control - Enable the function of bandwidth storm control for multicast packets.
Unknown Unicast Storm Control- Enable the function of bandwidth storm control for unknown unicast packets. These packets are the MAC address that had not completed the learning process yet.
Broadcast, Multicast, Unknown Unicast Storm Control - Enable the function of bandwidth storm control for all packets in transmission.


Storm Type
Disable
Disable
Broadcast Storm Control
Multicast Storm Control
Unknown Unicast Storm Control
Broadcast, Multicast, and Unknown Unicast Storm Control

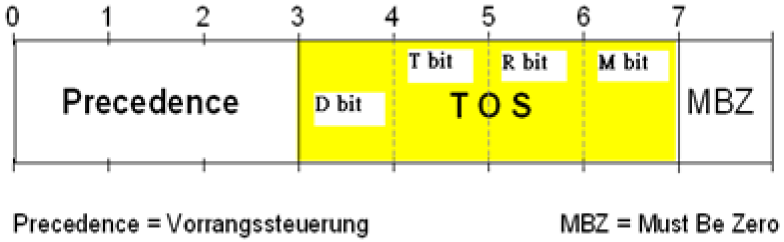
Storm Rate:

Set up the limit of bandwidth for storm type you choose. Valid value of the storm rate ranges from 1-100 with the minimum unit of 1. And only integer is acceptable. Default is 100.

2.18 QoS(Quality of Service) Configuration

The switch supports 5 kinds of QoS, are as follows, MAC Priority, 802.1p Priority, IP TOS Priority, and DiffServ DSCP Priority. Port Based Priority has a special name called VIP Port in the switch. Any packets enter VIP Port will have highest transmitting priority. MAC Priority act on the destination address of MAC in packets. VLAN tagged Priority field is effected by 802.1p Priority setting. IP TOS Priority affects TOS fields of IP header, and you can find it has 8-bit SERVICE TYPE field that specifies how the datagram should be handled. The field could be divided into six subfields as follows, PRECEDENCE (3 bits), D-Type (Delay Priority, 1 bit), T-Type (Throughput Priority, 1bit), R-Type (Reliability Priority, 1bit), M-Type (Monetary Cost Priority, 1bit), and UNUSED (1bit).

User can randomly control these fields to achieve some special QoS goals. When bits D, T, R, or M set, the D bit requests low delay, the T bit requests high throughput, the R bit requests high reliability, and the M bit requests low cost.



DiffServ DSCP Priority act on DSCP field of IP Header. In the late 1990s, the IETF redefined the meaning of the 8-bit SERVICE TYPE field to accommodate a set of differentiated services (DS). Under the differentiated services interpretation, the first six bits comprise a codepoint, which is sometimes abbreviated DSCP, and the last two bits are left unused.

High Priority Packet streams will experience less delay into the switch. For handing different priority packets, each egress port has designed up to 4 queues. Each QoS is influenced by two scheduling, WRR (Weighted Round Robin) and Strict Priority as well. When you finish setting the priority mapping to the queue, WRR scheduling will distribute the bandwidth according to the weight you set for 4 queues (queue 0 to queue 3). Another scheduling is Strict Priority dedicated for the function named VIP Port of QoS. While we select some ports as the VIP Port, these ports will own the highest transmitting priority in egress queue of the switch.

The QoS functions as we mentioned above are able to be enabled at the same time. But, the following precedence will decide whether these functions work or not.

1. enable both VIP and TOS

   Choose priorities of VIP and TOS.

2. enable both VIP and DSCP

   Choose priorities of VIP and DSCP.

3. enable both TOS and DSCP

   Choose "DSCP".

4. enable both VIP and DSCP

   Choose priorities of VIP and DSCP.

5. enable both 802.1p and TOS

   Choose "TOS".

6. enable both 802.1p and DSCP

   Choose "DSCP".

7. enable both 802.1p and DSCP and TOS

   Choose "DSCP".

8. enable both 802.1p and DSCP and TOS and VIP

   Choose priorities of VIP and DSCP.

** VIP/DSCP > TOS > 802.1p (Final result)

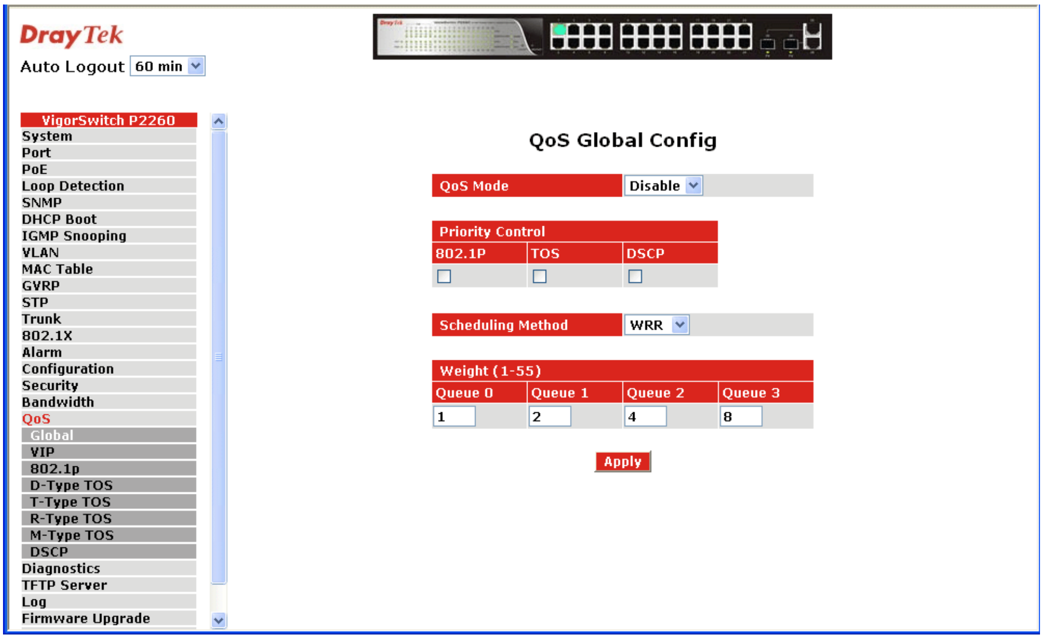
2.18.1 Global

Function name:

QoS Global Config

Function description:

When you want to use QoS function, please enable QoS Mode in advance. Then you can use MAC Priority, 802.1p Priority, IP TOS Priority, DiffServ DSCP Priority, or VIP Port functions and take effect. In this function, you can Enable QoS Mode. Choose any of Priority Control, such as 802.1p, TOS, DSCP. Moreover, you can select Scheduling Method of WRR (Weighted Round Robin) or Strict Priority. Next, you can arrange Weight values for queue 0 to queue 3.



Auto Logout 60 min

QoS Global Config

QoS Mode: Disable

Priority Control

802.1P	TOS	DSCP
□	□	□

Scheduling Method: WRR

Weight (1-55)

Queue 0	Queue 1	Queue 2	Queue 3
1	2	4	8

Parameter description:

QoS Mode:	You can Enable QoS Mode and let QoS function become effective. Default is Disable.
Priority Control:	Just tick the check box (☑) of 802.1P, TOS, or DSCP Qos and click Apply button to be in operation.
Scheduling Method:	There are two Scheduling Method, WRR and Strict Priority. Default is WRR. After you choose any of Scheduling Method, please click Apply button to be in operation.
Weight:	Over here, you can make an arrangement to Weight values of Queue 0 to Queue 3. The range of Weight you can set is 1~55. In default, the weight of Queue 0 is 1, the weight of Queue 1 is 2, the weight of Queue 2 is 4, and the weight of Queue 3 is 8.

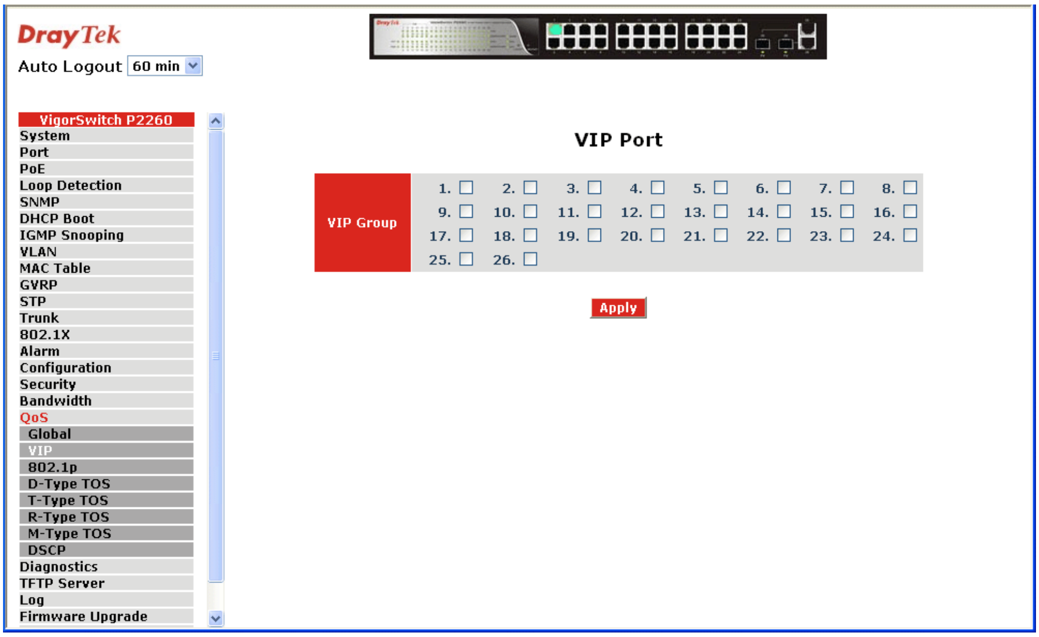
2.18.2 VIP

Function name:

VIP Port

Function description:

When the port is set as VIP Port, the packets enter this port and will have highest transmitting priority. For example, as you choose port 2 is VIP Port, simultaneously transmit packets from port 2 and port 3 to port 1 at speed of 100MB and let congestion happen. The packets for port 3 will be dropped because the packets from port 2 owns highest precedence. For the sake of this function taking effect, you must choose Scheduling Method of Strict Priority ahead.



VIP Port

VIP Group	1. □	2. □	3. □	4. □	5. □	6. □	7. □	8. □
	9. □	10. □	11. □	12. □	13. □	14. □	15. □	16. □
	17. □	18. □	19. □	20. □	21. □	22. □	23. □	24. □
	25. □	26. □						

Apply

Parameter description:

VIP Group: Just tick the check box (☑) to select any port(port 1~26) as the VIP Port. Then, click the <**Apply**> button to have the setting taken effect.

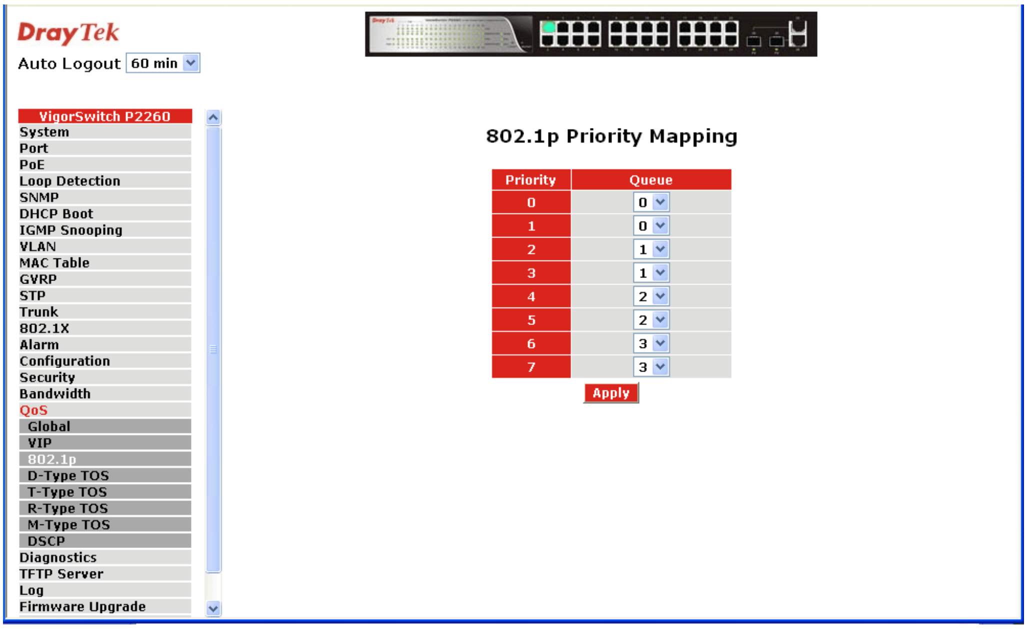
2.18.3 802.1p

Function name:

802.1p Priority Mapping

Function description:

This function will affect the priority of VLAN tag. Based on priority of VLAN tag, it can arrange 0~8 priorities, priorities can map to 4 queues of the switch (queue 0~3) and possess different bandwidth distribution according to your weight setting.



Auto Logout 60 min

802.1p Priority Mapping

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

Parameter description:

Queue:	Each Priority can select any of Queue 0 ~ Queue 3. In Default, Priority 0 is mapping to Queue 0, Priority 1 is mapping to Queue 0, Priority 2 is mapping to Queue 1, Priority 3 is mapping to Queue 1, Priority 4 is mapping to Queue 2, Priority 5 is mapping to Queue 2, Priority 6 is mapping to Queue 3, and Priority 0 is mapping to Queue 3.

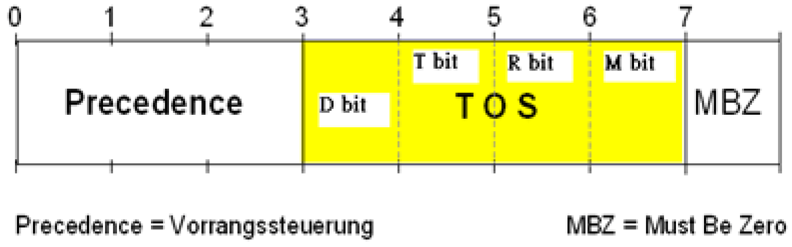
2.18.4 D-Type TOS

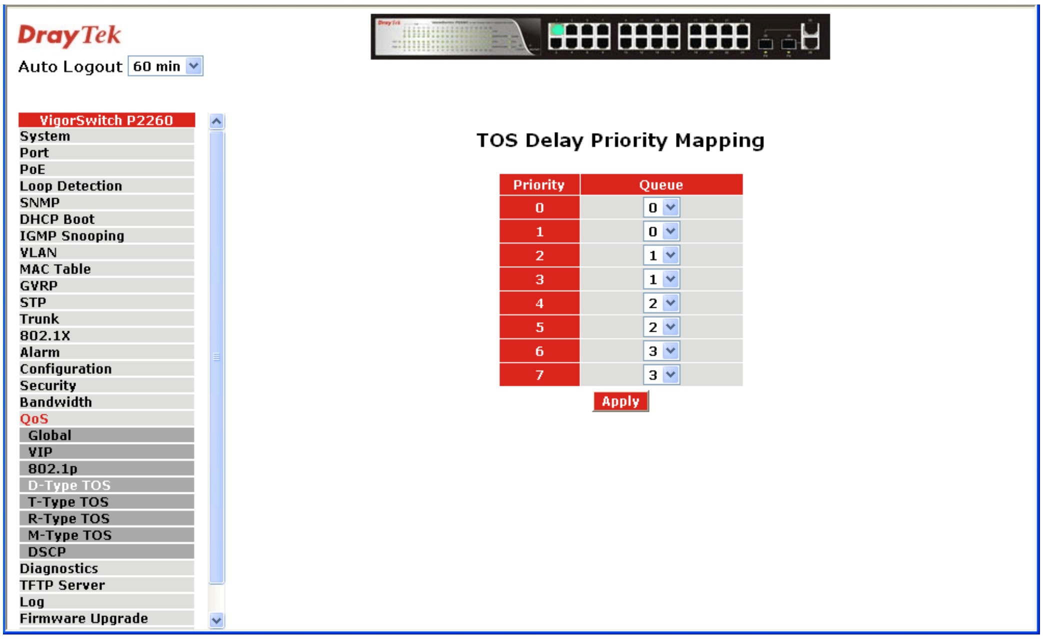
Function name:

TOS Delay Priority Mapping

Function description:

IP TOS Priority affect TOS fields of IP header, you can find it has 8-bit SERVICE TYPE field that specifies how the datagram should be handled. The field could be divided into six subfields as follows, PRECEDENCE (3 bits), D-Type (Delay Priority, 1 bit), T-Type (Throughput Priority, 1bit), R-Type (Reliability Priority, 1bit), M-Type (Monetary Cost Priority, 1bit), and UNUSED. PRECEDENCE 3-bits can arrange 8 kinds of priorities corresponding to the 0~7 priority in the following priority diagram. TOS Delay Priority Mapping works while D-TYPE in TOS field of IP header of the packets received by the switch is configured.





TOS Delay Priority Mapping

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

Apply

Parameter description:

Queue:	Each Priority can select any of Queue 0 ~ Queue 3. In Default, Priority 0 is mapping to Queue 0, Priority 1 is mapping to Queue 0, Priority 2 is mapping to Queue 1, Priority 3 is mapping to Queue 1, Priority 4 is mapping to Queue 2, Priority 5 is mapping to Queue 2, Priority 6 is mapping to Queue 3, and Priority 0 is mapping to Queue 3.

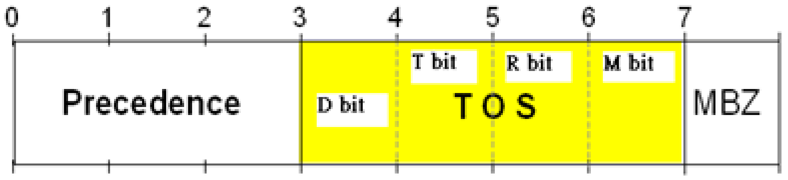
2.18.5 T-Type TOS

Function name:

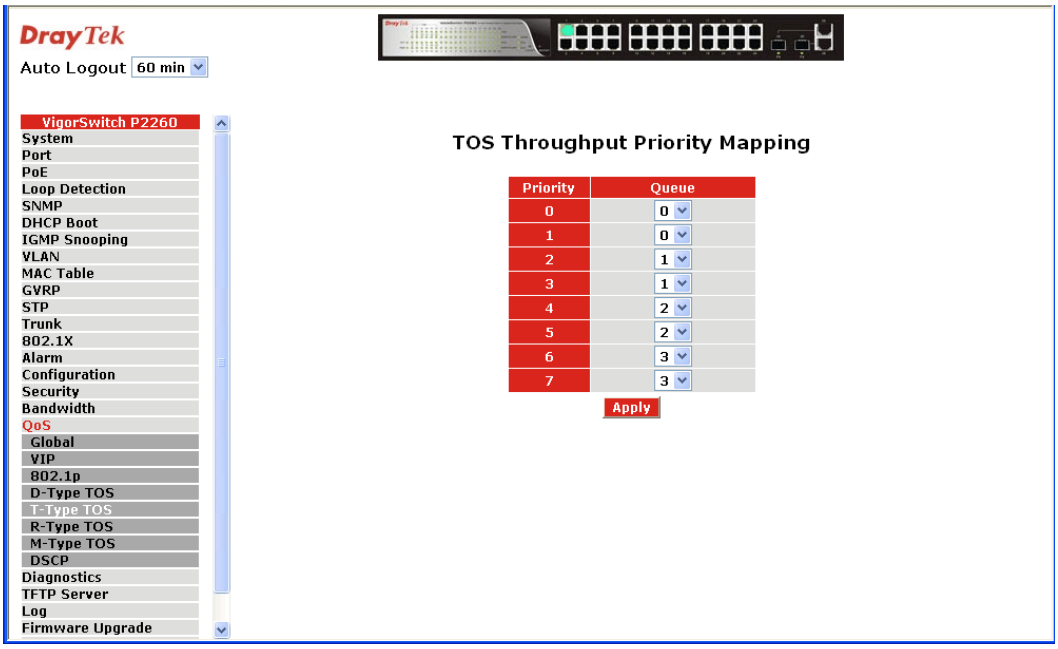
TOS Throughput Priority Mapping

Function description:

IP TOS Priority affect TOS fields of IP header, you can find it has 8-bit SERVICE TYPE field that specifies how the datagram should be handled. The field could be divided into six subfields as follows, PRECEDENCE (3 bits), D-Type (Delay Priority, 1 bit), T-Type (Throughput Priority, 1bit), R-Type (Reliability Priority, 1bit), M-Type (Monetary Cost Priority, 1bit), and UNUSED. PRECEDENCE 3-bits can arrange 8 kinds of priorities corresponding to the 0~7 priority in the following priority diagram. TOS Throughput Priority Mapping works while T-TYPE in TOS field of IP header of the packets received by the switch is configured.



Precedence = Vorrangssteuerung MBZ = Must Be Zero



TOS Throughput Priority Mapping

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

Parameter description:

Queue:	Each Priority can select any of Queue 0 ~ Queue 3. In Default, Priority 0 is mapping to Queue 0, Priority 1 is mapping to Queue 0, Priority 2 is mapping to Queue 1, Priority 3 is mapping to Queue 1, Priority 4 is mapping to Queue 2, Priority 5 is mapping to Queue 2, Priority 6 is mapping to Queue 3, and Priority 0 is mapping to Queue 3.

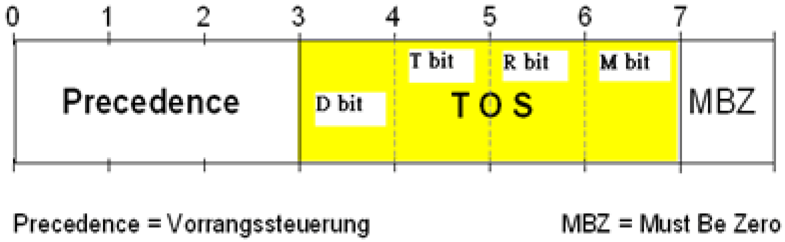
2.18.6 R-Type TOS

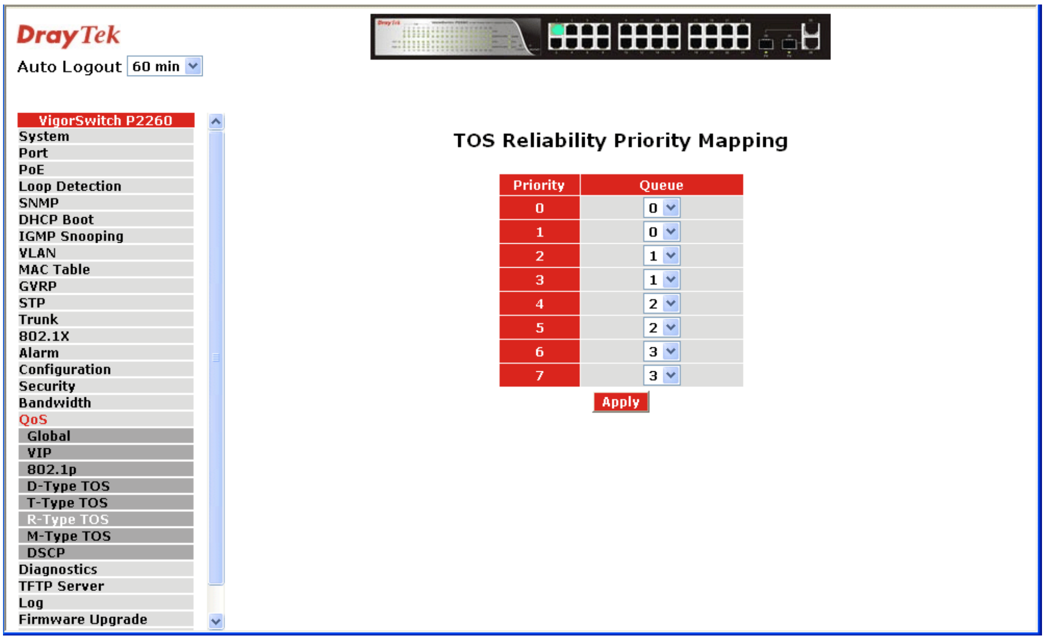
Function name:

TOS Reliability Priority Mapping

Function description:

IP TOS Priority affect TOS fields of IP header, you can find it has 8-bit SERVICE TYPE field that specifies how the datagram should be handled. The field could be divided into six subfields as follows, PRECEDENCE (3 bits), D-Type (Delay Priority, 1 bit), T-Type (Throughput Priority, 1bit), R-Type (Reliability Priority, 1bit), M-Type (Monetary Cost Priority, 1bit), and UNUSED. PRECEDENCE 3-bits can arrange 8 kinds of priorities corresponding to the 0~7 priority in the following priority diagram. TOS Reliability Priority Mapping works while R-TYPE in TOS field of IP header of the packets received by the switch is configured.





TOS Reliability Priority Mapping

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

Parameter description:

Queue:	Each Priority can select any of Queue 0 ~ Queue 3. In Default, Priority 0 is mapping to Queue 0, Priority 1 is mapping to Queue 0, Priority 2 is mapping to Queue 1, Priority 3 is mapping to Queue 1, Priority 4 is mapping to Queue 2, Priority 5 is mapping to Queue 2, Priority 6 is mapping to Queue 3, and Priority 0 is mapping to Queue 3.

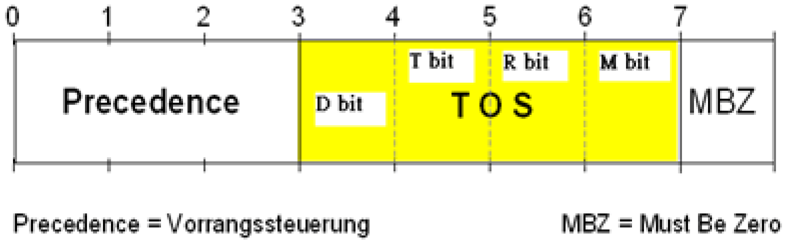
2.18.7 M-Type TOS

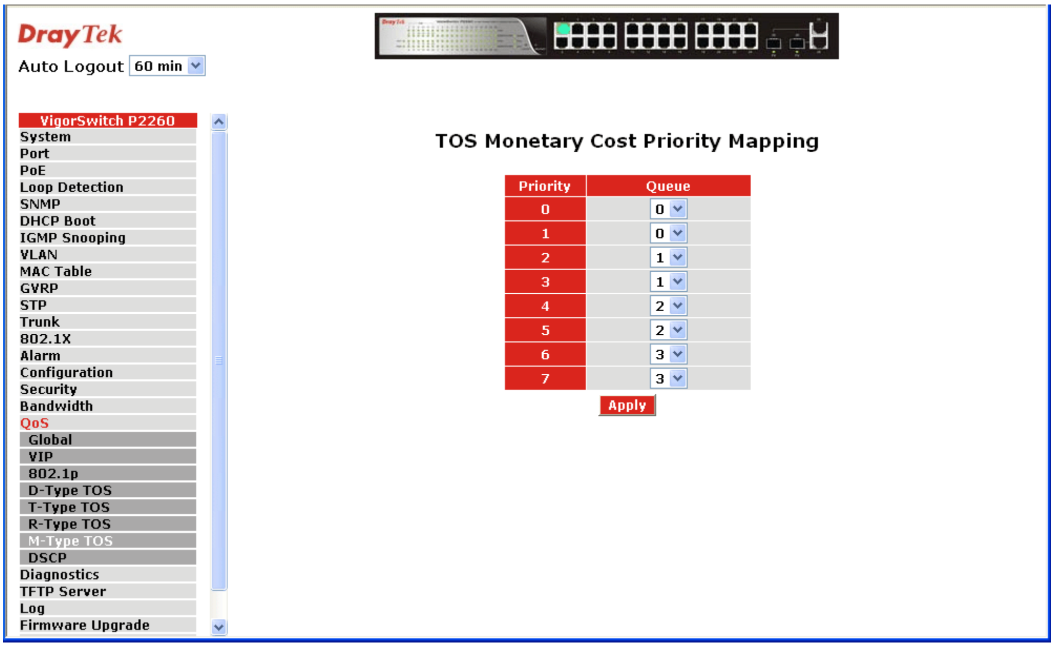
Function name:

TOS Monetary Cost Priority Mapping

Function description:

IP TOS Priority affect TOS fields of IP header, you can find it has 8-bit SERVICE TYPE field that specifies how the datagram should be handled. The field could be divided into six subfields as follows, PRECEDENCE (3 bits), D-Type (Delay Priority, 1 bit), T-Type (Throughput Priority, 1bit), R-Type (Reliability Priority, 1bit), M-Type (Monetary Cost Priority, 1bit), and UNUSED. PRECEDENCE 3-bits can arrange 8 kinds of priorities corresponding to the 0~7 priority in the following priority diagram. TOS Monetary Cost Priority Mapping works while M-TYPE in TOS field of IP header of the packets received by the switch is configured.





TOS Monetary Cost Priority Mapping

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

Parameter description:

Queue: Each Priority can select any of Queue 0 ~ Queue 3. In Default, Priority 0 is mapping to Queue 0, Priority 1 is mapping to Queue 0, Priority 2 is mapping to Queue 1, Priority 3 is mapping to Queue 1, Priority 4 is mapping to Queue 2, Priority 5 is mapping to Queue 2, Priority 6 is mapping to Queue 3, and Priority 0 is mapping to Queue 3.

2.18.8 DSCP

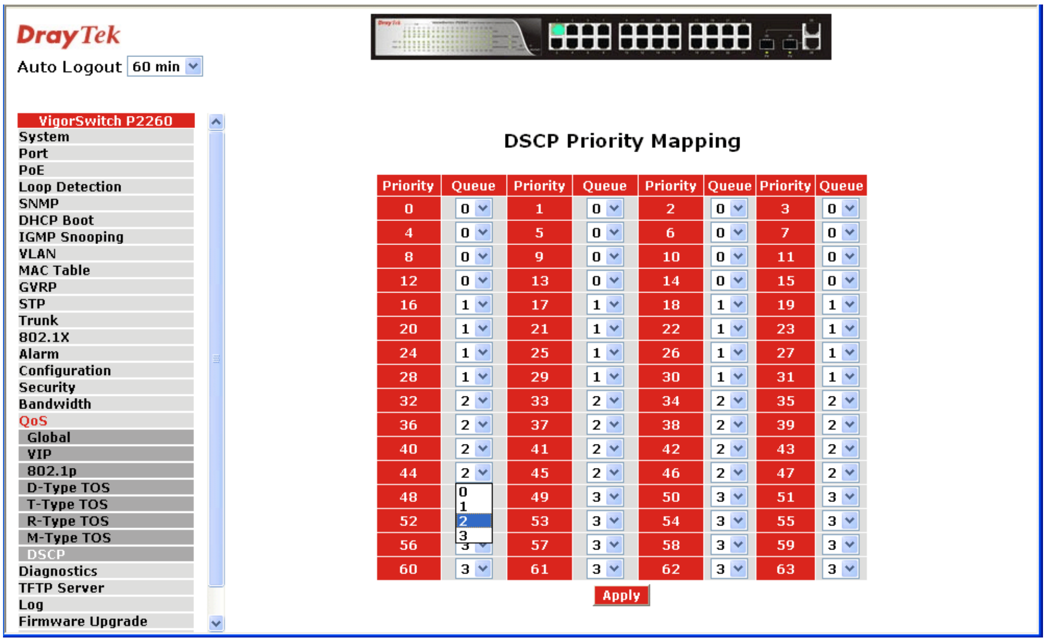
Function name:

DSCP Priority Mapping

Function description:

In the late 1990s, the IETF redefined the meaning of the 8-bit SERVICE TYPE field to accommodate a set of differentiated services (DS). Under the differentiated services interpretation, the first six bits comprise a codepoint, which is sometimes abbreviated DSCP, and the last two bits are left unused.

DSCP can form total 64 (0~63) kinds of Traffic Class based on the arrangement of 6-bit field in DSCP of the IP packet. In the switch, user is allowed to set up these 64 kinds of Class that belong to any of queue 0~3.



DSCP Priority Mapping

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

Parameter description:

Queue: 64 kinds of priority traffic as mentioned above, user can set up any of Queue 0~3. In default, Priority 0~15 are mapping to Queue 0, Priority 16~31 are mapping to Queue 1, Priority 32~47 are mapping to Queue 0, Priority 48~63 are mapping to Queue 0.

2.19 Diagnostics

Three functions, including Diagnostics, Loopback Test and Ping Test are contained in this function folder for device self-diagnostics.

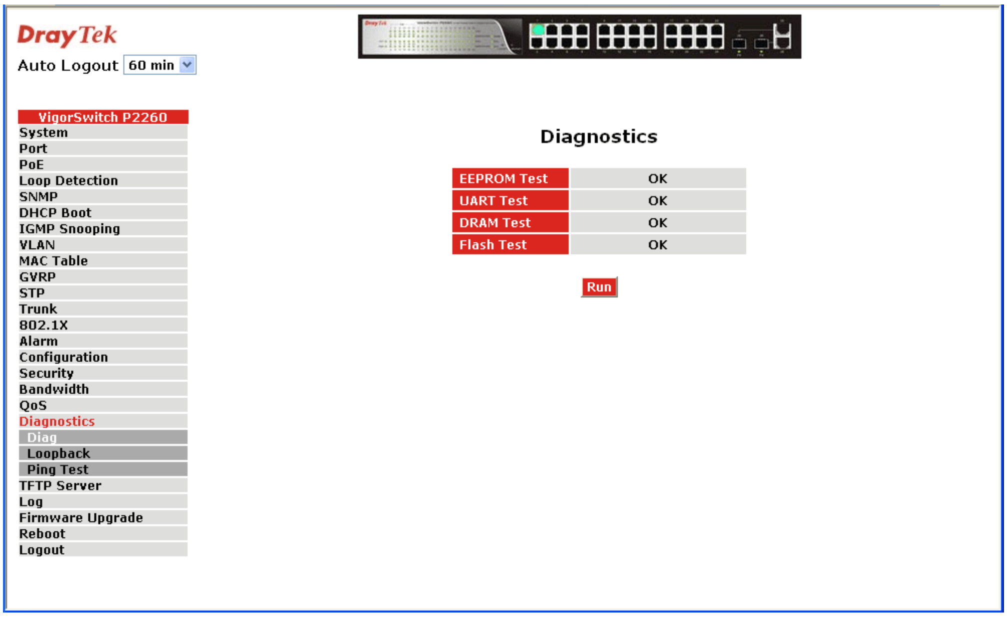
2.19.1 Diagnostics

Function name:

Diagnostics

Function description:

Diagnostics function provides a set of basic system diagnosis. It let users know that whether the system is health or needs to be fixed. The basic system check includes EEPROM test, UART test, DRAM test and Flash test.



Diagnostics

EEPROM Test	OK
UART Test	OK
DRAM Test	OK
Flash Test	OK

2.19.2 Loopback Test

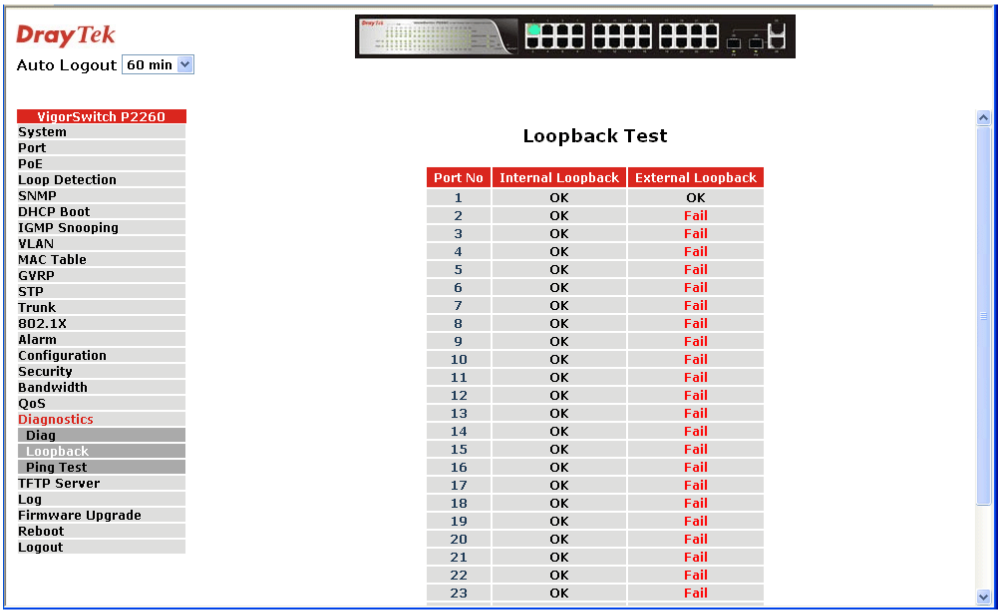
Function name:

Loopback Test

Function description:

In the Loopback Test function, there are two different loopback tests. One is Internal Loopback Test and the other is External Loopback Test. The former test function will not send the test signal outside the switch box. The test signal only wraps around in the switch box. As to the latter test function, it will send the test signal to its link partner. If you do not have them connected to active network devices, i.e. the ports are link down, the switch will report the port numbers failed. If they all are ok, it just shows OK.

Note: Whatever you choose Internal Loopback Test or External Loopback Test, these two functions will interfere with the normal system working, and all packets in sending and receiving also will stop temporarily.



Loopback Test

Port No	Internal Loopback	External Loopback
1	OK	OK
2	OK	Fail
3	OK	Fail
4	OK	Fail
5	OK	Fail
6	OK	Fail
7	OK	Fail
8	OK	Fail
9	OK	Fail
10	OK	Fail
11	OK	Fail
12	OK	Fail
13	OK	Fail
14	OK	Fail
15	OK	Fail
16	OK	Fail
17	OK	Fail
18	OK	Fail
19	OK	Fail
20	OK	Fail
21	OK	Fail
22	OK	Fail
23	OK	Fail

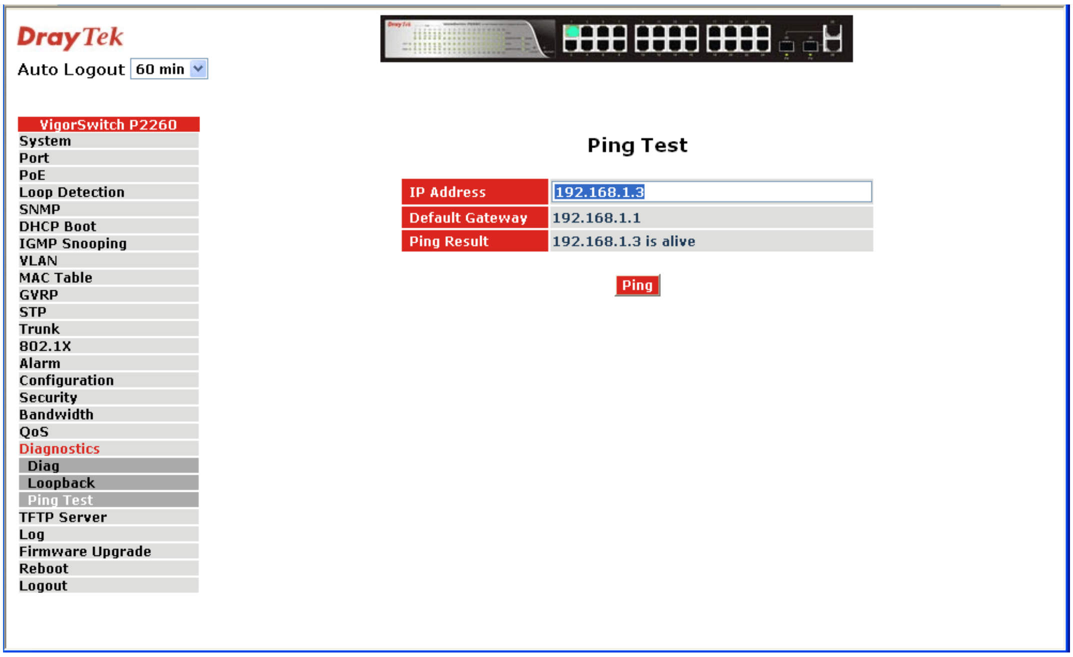
2.19.3 Ping Test

Function name:

Ping Test

Function description:

Ping Test function is a tool for detecting if the target device is alive or not through ICMP protocol which abounds with report messages. The switch provides Ping Test function to let you know that if the target device is available or not. You can simply fill in a known IP address and then click **<Ping>** button. After a few seconds later, the switch will report you the pinged device is alive or dead in the field of Ping Result.



Ping Test

IP Address	192.168.1.3
Default Gateway	192.168.1.1
Ping Result	192.168.1.3 is alive

Parameter description:

IP Address:	An IP address with the version of v4, e.g. 192.168.1.1.
Default Gateway:	IP address of the default gateway.

2.20 TFTP Server

Function name:

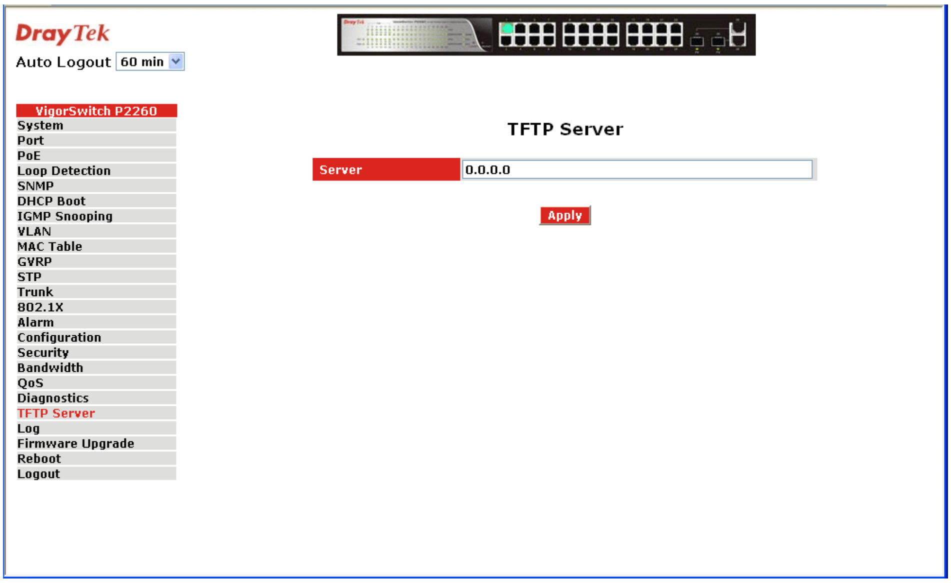
TFTP Server

Function description:

Set up IP address of TFTP server.

Parameter description:

Specify the IP address where the TFTP server locates. Fill in the IP address of your TFTP server, then press <**Apply**> button to have the setting taken effect.



TFTP Server

Server	0.0.0.0

2.21 Log

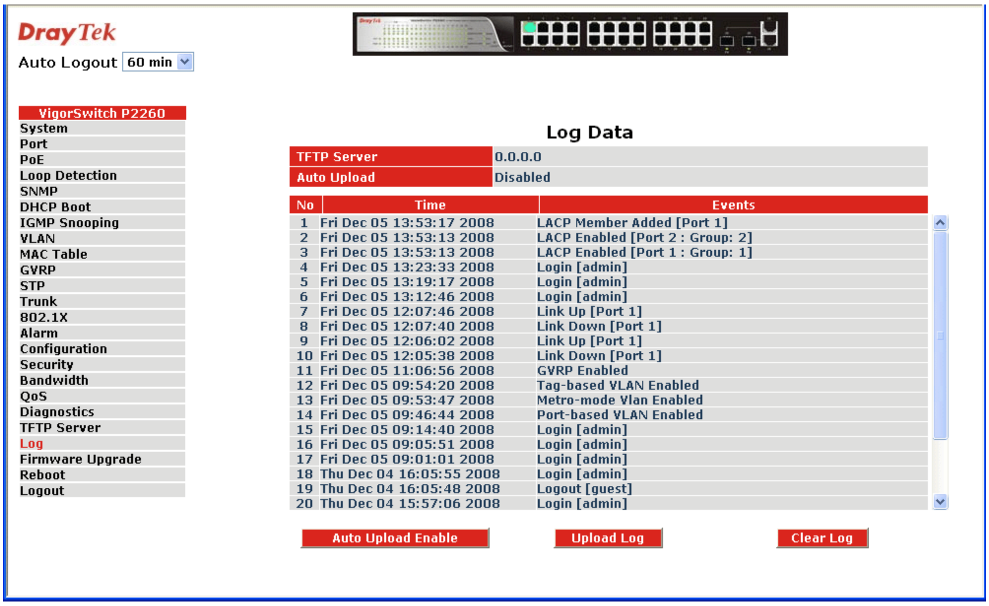
This function shows the log data. The switch provides system log data for users. There are 19 private trap logs, 5 public trap logs. The switch supports total 120 log entries. For more details on log items, please refer to the section of Trap/Alarm Configuration and SNMP Configuration.

Function name:

Log Data

Function description:

The Trap Log Data is displaying the log items including all SNMP Private Trap events, SNMP Public traps and user logs occurred in the system. In the report table, No., Time and Events are three fields contained in each trap record.



Log Data

TFTP Server	0.0.0.0
Auto Upload	Disabled

No	Time	Events
1	Fri Dec 05 13:53:17 2008	LACP Member Added [Port 1]
2	Fri Dec 05 13:53:13 2008	LACP Enabled [Port 2 : Group: 2]
3	Fri Dec 05 13:53:13 2008	LACP Enabled [Port 1 : Group: 1]
4	Fri Dec 05 13:23:33 2008	Login [admin]
5	Fri Dec 05 13:19:17 2008	Login [admin]
6	Fri Dec 05 13:12:46 2008	Login [admin]
7	Fri Dec 05 12:07:46 2008	Link Up [Port 1]
8	Fri Dec 05 12:07:40 2008	Link Down [Port 1]
9	Fri Dec 05 12:06:02 2008	Link Up [Port 1]
10	Fri Dec 05 12:05:38 2008	Link Down [Port 1]
11	Fri Dec 05 11:06:56 2008	GVRP Enabled
12	Fri Dec 05 09:54:20 2008	Tag-based VLAN Enabled
13	Fri Dec 05 09:53:47 2008	Metro-mode Vlan Enabled
14	Fri Dec 05 09:46:44 2008	Port-based VLAN Enabled
15	Fri Dec 05 09:14:40 2008	Login [admin]
16	Fri Dec 05 09:05:51 2008	Login [admin]
17	Fri Dec 05 09:01:01 2008	Login [admin]
18	Thu Dec 04 16:05:55 2008	Login [admin]
19	Thu Dec 04 16:05:48 2008	Logout [guest]
20	Thu Dec 04 15:57:06 2008	Login [admin]

Parameter description:

No.: Display the order number that the trap happened.

Time: Display the time that the trap happened.

Events: Display the trap event name.

Auto Upload Enable: Switch the enabled or disabled status of the auto upload function.

Upload Log: Upload log data through tftp.

Clear Log: Clear log data.

2.22 Firmware Upgrade

Software upgrade tool is used to help upgrade the software function in order to fix or improve the function. The switch provides a TFTP client for software upgrade. This can be done through Ethernet.

Function name:

Firmware Upgrade

Function description:

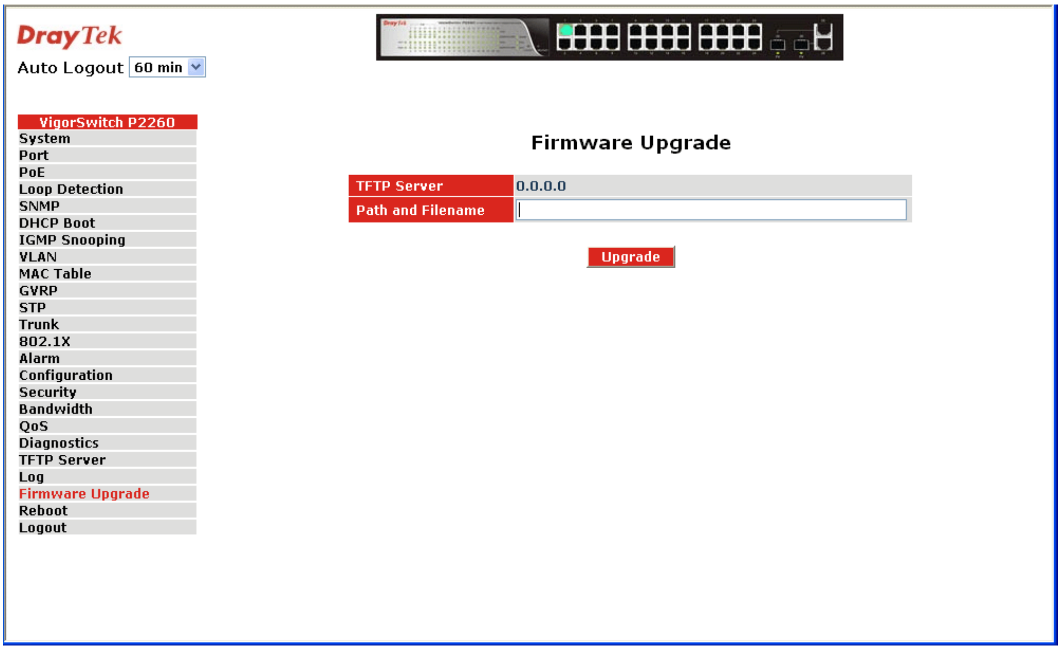
The switch supports TFTP upgrade tool for upgrading software. If you assure to upgrade software to a newer version one, you must follow two procedures:

1. Specifying the IP address where TFTP server locates. In this field, the IP address of your TFTP server should be filled in.
2. Specifying what the filename and where the file is. You must specify full path and filename.

Then, press <**Upgrade**> button if your download is not successful, the switch will also be back to "Software Upgrade", and it will not upgrade the software as well.

When download is completed, the switch starts upgrading software. A reboot message will be prompted after completing upgrading software. At this time, you must reboot the switch to have new software worked.

Note: Software upgrade is hazardous if power is off. You must do it carefully.



Firmware Upgrade

TFTP Server	0.0.0.0
Path and Filename	

Parameter description:

TFTP Server: A TFTP server stored the image file you want to upgrade.

Path and Filename: File path and filename stored the image file you want to upgrade.

2.23 Reboot

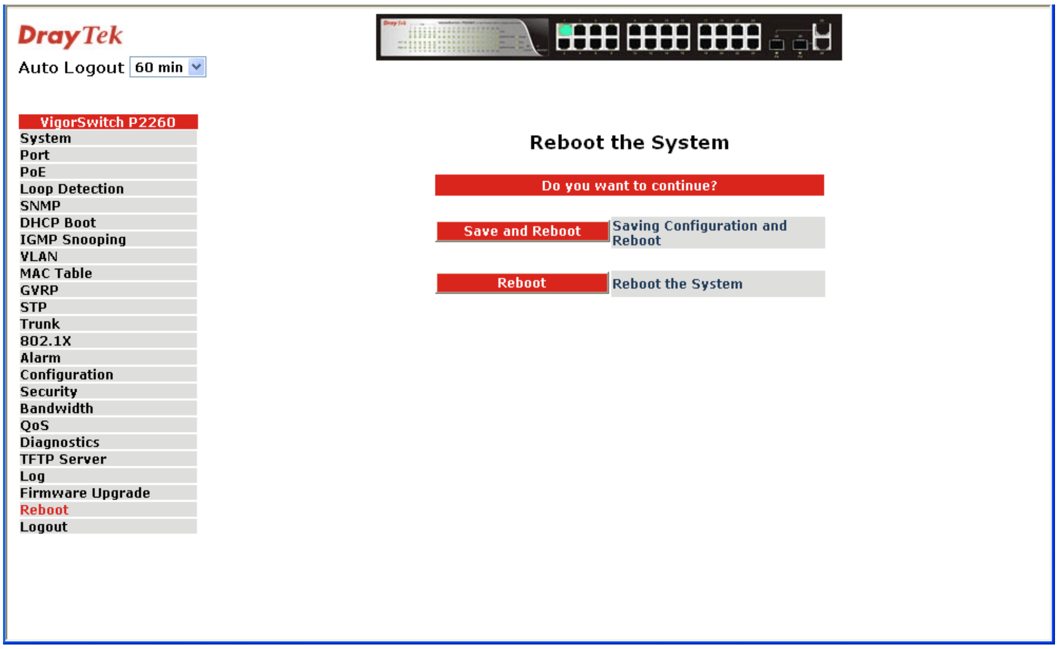
We offer you many ways to reboot the switch, including power up, hardware reset and software reset. You can press the RESET button in the front panel to reset the switch. After upgrading software, changing IP configuration or changing VLAN mode configuration, then you must reboot to have the new configuration taken effect. Here we are discussing is software reset for the "reboot" in the main menu.

Function name:

Reboot

Function description:

Reboot the switch. Reboot takes the same effect as the RESET button on the front panel of the switch. It will take around thirty (30) seconds to complete the system boot.



Reboot the System

Do you want to continue?

Saving Configuration and Reboot

Reboot the System

Parameter description:

Save and Reboot: Save the current settings as start configuration before rebooting the switch.

Reboot: Reboot the system directly.

2.24 Logout

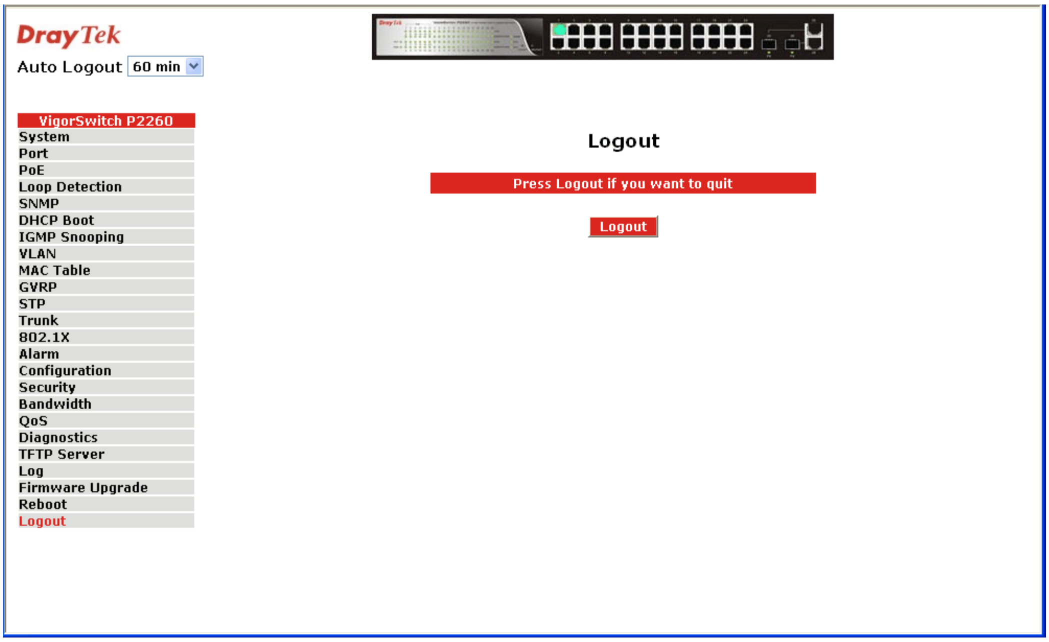
You can manually logout by performing Logout function. In the switch, it provides another way to logout. You can configure it to logout automatically.

Function name:

Logout

Function description:

The switch allows you to logout the system to prevent other users from the system without the permission. If you do not logout and exit the browser, the switch will automatically have you logout. Besides this manually logout and implicit logout, you can pull down the **<Auto Logout>** list at the top-left corner to explicitly ON/OFF this logout function.



Parameter description:

Auto Logout:	Default is ON. If it is "ON", and no action and no key is stroke as well in any function screen more than 3 minutes, the switch will have you logout automatically.

3 Trouble Shooting

This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the device and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the device from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

If all above stages are done and the device still cannot run normally, it is the time for you to contact your dealer for advanced help.

3.1 Resolving No Link Condition

The possible causes for a no link LED status are as follows:

- The attached device is not powered on
- The cable may not be the correct type or is faulty
- The installed building premise cable is faulty
- The port may be faulty

3.2 Q & A

1. Computer A can connect to Computer B, but cannot connect to Computer C through the Managed Switch.

- The network device of Computer C may fail to work. Please check the link/act status of Computer C on the LED indicator. Try another network device on this connection.
- The network configuration of Computer C may be something wrong. Please verify the network configuration on Computer C.

2. The uplink connection function fails to work.

- The connection ports on another must be connection ports. Please check if connection ports are used on that Managed Switch.
- Please check the uplink setup of the Managed Switch to verify the uplink function is enabled.

3. The console interface cannot appear on the console port connection.

- The COM port default parameters are [Baud Rate: 57600, Data Bits: 8, Parity Bits: None, Stop Bit: A, Flow Control: None]. Please check the COM port property in the terminal program. And if the parameters are changed, please set the COM configuration to the new setting.

- Check the RS-232 cable is connected well on the console port of the Managed Switch and COM port of PC.
- Check if the COM of the PC is enabled.

4. How to configure the Managed Switch?

The “Hyperterm” is the terminal program in Win95/98/NT. Users can also use any other terminal programs in Linux/Unix to configure the Managed Switch. Please refer to the user guide of that terminal program. But the COM port parameters (baud rate/ data bits/ parity bits/ flow control) must be the same as the setting of the console port of the Managed Switch.