DrayTek

VigorSwitch G2240

User's Guide

Version: 1.0

Date: 2009/1/20

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 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 24 Gigabit L2 plus Switch 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

The 24-port Gigabit L2 Managed Switch, is a standard switch that meets all IEEE 802.3/u/x/z Gigabit, Fast Ethernet specifications. The switch included 20-Port 10/100/1000Mbps TP and 4-Port Gigabit TP/SFP Fiber management Ethernet switch. The switch can be managed through RS-232 serial port via directly connection, or through Ethernet port using CLI 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 ACL, IP-MAC Binding, DHCP Option 82, QoS (Quality of Service), Spanning Tree, VLAN, Port Trunking, Bandwidth Control, Port Security, SNMP/RMON, IGMP Snooping capability via the intelligent software. It is suitable for both metro-LAN and office application.

In this switch, Port 21 and Port 24 include 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.

- 1000Mbps LC, Multi-Mode, SFP Fiber transceiver
- 1000Mbps LC, 10km, SFP Fiber transceiver
- 1000Mbps LC, 30km, SFP Fiber transceiver
- 1000Mbps LC, 50km, SFP Fiber transceiver
- 1000Mbps BiDi LC, 20km, 1550nm SFP Fiber WDM transceiver
- 1000Mbps BiDi LC, 20km, 1310nm SFP Fiber WDM transceiver

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 2.21.2** 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.

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.

IGMP Proxy

The implementation of IP multicast processing. The switch supports IGMP version 1 and IGMP version 2, efficient use of network bandwidth, and fast response time for channel changing. IGMP version 1 (IGMPv1) is described in RFC1112 ,and IGMP version 2 (IGMPv2) is described in RFC 2236. Hosts interact with the system through the exchange of IGMP messages. Similarly, when you configure IGMP proxy, the system interacts with the router on its upstream interface through the exchange of IGMP messages. However, when acting as the proxy, the system performs the host portion of the IGMP task on the upstream interface as follows:

- When queried, sends group membership reports to the group.

- When one of its hosts joins a multicast address group to which none of its other hosts belong, sends unsolicited group membership reports to that group.
- When the last of its hosts in a particular multicast group leaves the group, sends an unsolicited leave group membership report to the all-routers group (244.0.0.2).

1.2 Features

The VigorSwitch G2240, 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

- 20 10/100/1000Mbps Auto-negotiation Gigabit Ethernet TP ports
- 4 10/100/1000Mbps TP or 1000Mbps SFP Fiber dual media auto sense
- 1392KB on-chip frame buffer
- Support jumbo frame up to 9600 bytes
- Programmable classifier for QoS (Layer 4/Multimedia)
- 8K MAC address and 4K VLAN support (IEEE802.1Q)
- Per-port shaping, policing, and Broadcast Storm Control
- IEEE802.1Q Q-in-Q nested VLAN support
- Full-duplex flow control (IEEE802.3x) and half-duplex backpressure
- Extensive front-panel diagnostic LEDs; System: Power, TP Port1-24: LINK/ACT, 10/100/1000Mbps, SFP Port 21-24: SFP(LINK/ACT)

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
- Supports user management and limits three users to login
- Maximal packet length can be up to 9600 bytes for jumbo frame application
- 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 Quality of Service (QoS) for real time applications based on the information taken from Layer 2 to Layer 4, such as VoIP
- 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 multiple spanning tree (802.1s MSTP)
- Supports 802.1X port security on a VLAN
- Supports IP-MAC-Port Binding for LAN security
- 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 with a resolution of 1Mbps
- The trap event and alarm message can be transferred via e-mail
- Supports diagnostics to let administrator knowing the hardware status
- Supports loop detection to protect the switch crash when the networking has looping issue
- HTTP and TFTP for firmware upgrade, system log upload and configuration file import/export
- Supports remote boot the device through user interface and SNMP
- Supports NTP 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 G2240
- AC Power Cord
- CD
- Console Cable
- Rubber feet
- Rack mount kit

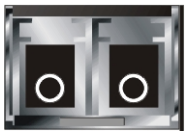
Please notify your sales representative immediately if any of the aforementioned items is missing or damaged.

Optional Modules

In the switch, Port 21~24 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

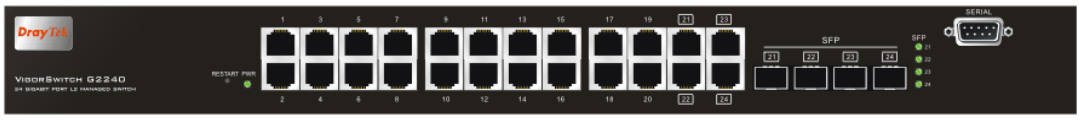
Front View of 1000Base-LX BiDi LC, SFP Fiber Transceiver

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
PWR	Green	Lit when +5V DC power is on and good
LAN P1 – P24	Green/ Amber	Lit green when 1000Mbps speed is active Lit ember when 100Mbps speed is active Off when 10Mbps speed is active
SF (21-24)	Green	Lit when connection with the remote device is good Blinks when any traffic is present Off when module connection is not good

Connector Explanation

Interface	Description
RESTART	Used to restart the management system.
LAN P1 – P24	Fast Ethernet Port
SFP (21 – 24)	SFP Fiber Port
RS-232	DB-9 connector

User Interfaces on the Rear Panel

One socket on the rear panel is for AC power input.

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

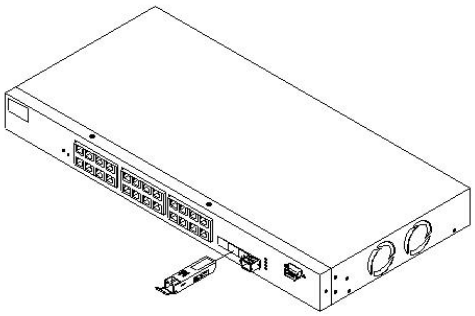
The switch supports 100-240 VAC, 50-60 Hz power supply. The power supply will automatically convert the local AC power source to DC power. It does not matter whether any connection plugged into the switch or not when power on, even modules as well. After the power is on, all LED indicators will light 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

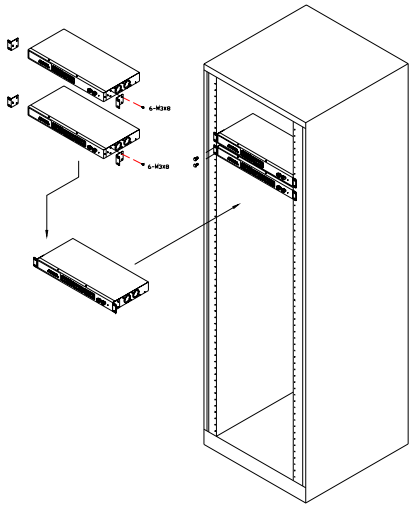
If you have no modules, please skip this section.



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.
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.

<table>
<tr><td rowspan="4">IEEE 802.3z
Gigabit Ethernet
1000SX 850nm</td><td colspan="4">Multi-mode Fiber Cable and Modal Bandwidth</td></tr>
<tr><td colspan="2">Multi-mode 62.5/125μm</td><td colspan="2">Multi-mode 50/125μm</td></tr>
<tr><td>Modal Bandwidth</td><td>Distance</td><td>Modal Bandwidth</td><td>Distance</td></tr>
<tr><td>160MHz-Km</td><td>220m</td><td>400MHz-Km</td><td>500m</td></tr>
<tr><td>200MHz-Km</td><td>275m</td><td>500MHz-Km</td><td>550m</td></tr>
<tr><td rowspan="3">1000Base-LX/LHX/XD/ZX</td><td colspan="4">Single-mode Fiber 9/125μm</td></tr>
<tr><td colspan="4">Single-mode transceiver 1310nm 10Km</td></tr>
<tr><td colspan="4">Single-mode transceiver 1550nm 30, 50Km</td></tr>
<tr><td rowspan="4">1000Base-LX
Single Fiber
(BIDI LC)</td><td colspan="2" rowspan="2">Single-Mode *20Km</td><td colspan="2">TX(Transmit) 1310nm</td></tr>
<tr><td colspan="2">RX(Receive) 1550nm</td></tr>
<tr><td colspan="2" rowspan="2">Single-Mode *20Km</td><td colspan="2">TX(Transmit) 1550nm</td></tr>
<tr><td colspan="2">RX(Receive) 1310nm</td></tr>
</table>

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:

<table>
<tr><th colspan="2">1000Base-X TP, Fiber</th><th colspan="4">100Base-TX TP/100Base-FX Fiber</th></tr>
<tr><td colspan="2">Round trip Delay: 4096</td><td colspan="4">Round trip Delay: 512</td></tr>
<tr><td>Cat. 5 TP Wire:</td><td>11.12/m</td><td>Cat. 5 TP Wire:</td><td>1.12/m</td><td>Fiber Cable:</td><td>1.0/m</td></tr>
</table>

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

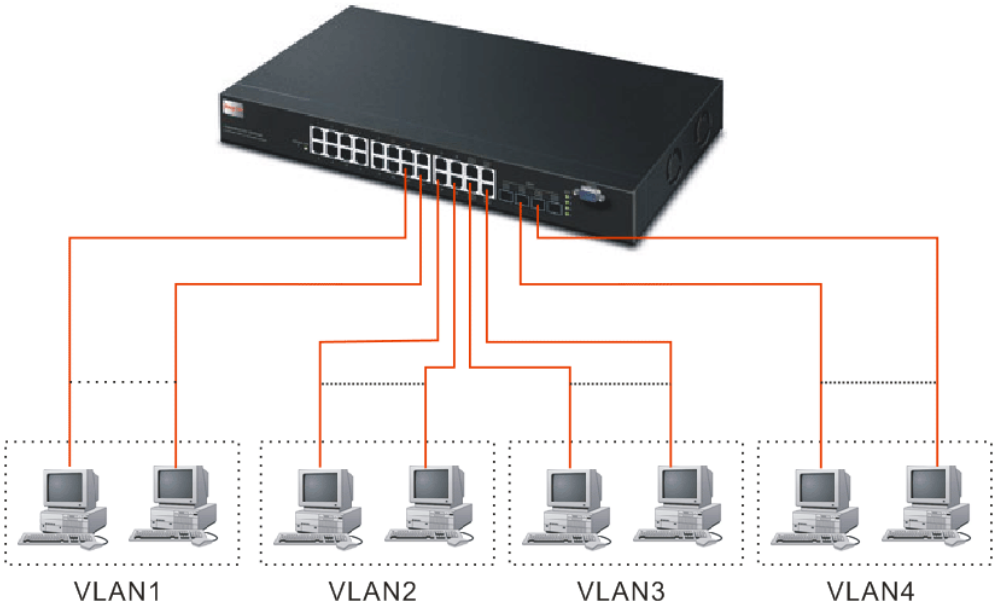
A hierarchical network with minimum levels of switch may reduce the timing delay between server and client station. Basically, with this approach, it will minimize the number of switches in any one path; will lower the possibility of network loop and will improve network efficiency. If more than two 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

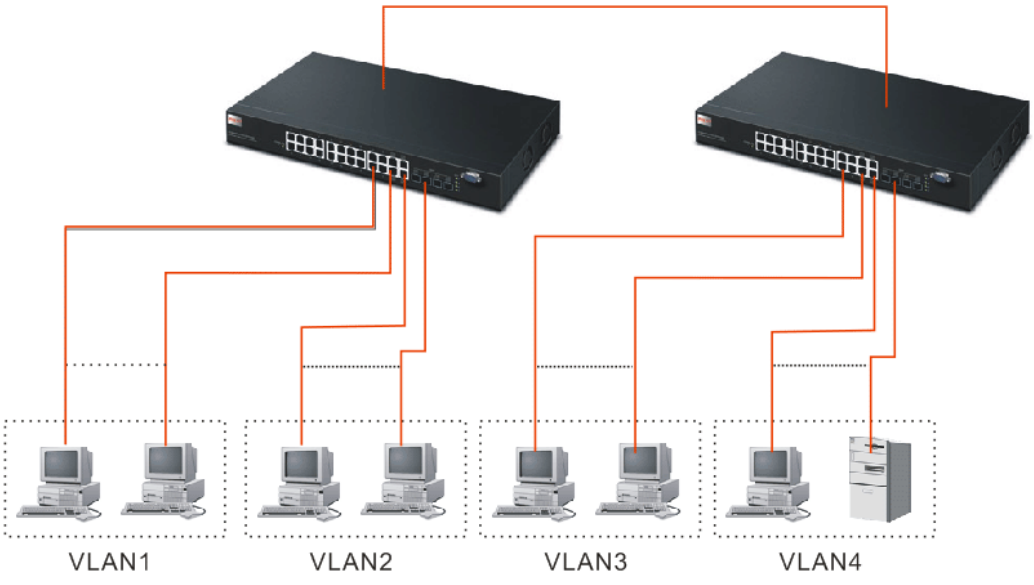


The same VLAN members could not be in different switches.

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



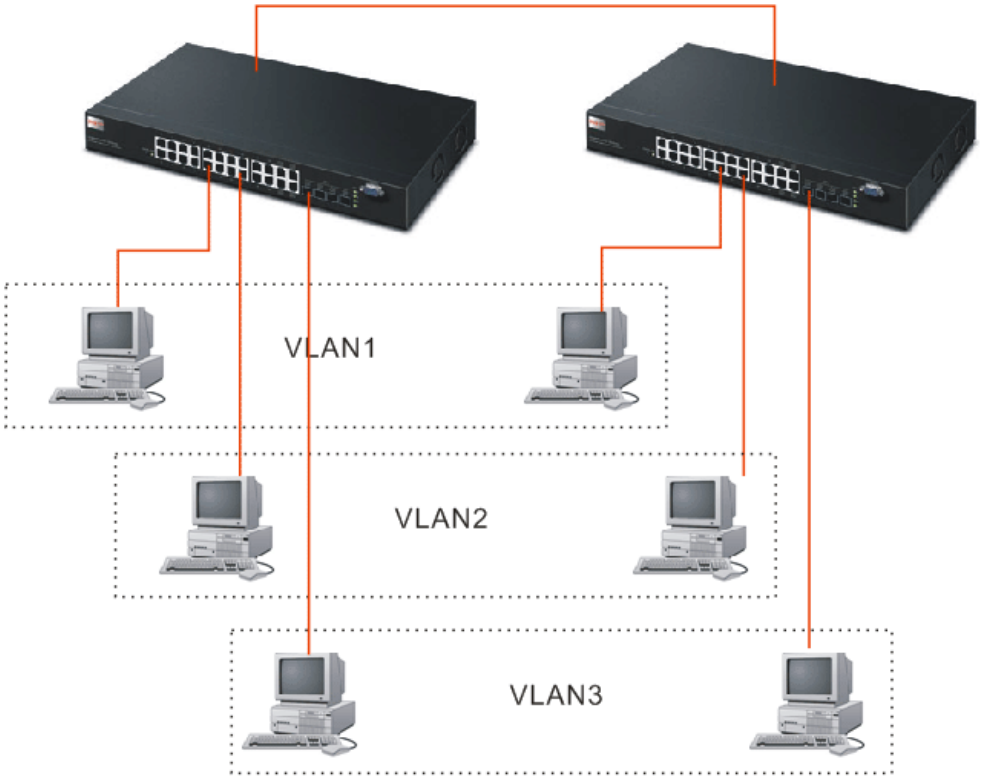
VLAN1 members could not access VLAN2, VLAN3 and VLAN4 members.

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.

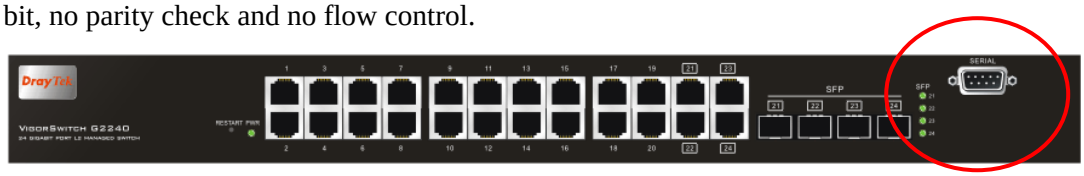
- Configuring the Management Agent of VigorSwitch G2240 through the Serial RS-232 Port
- Configuring the Management Agent of VigorSwitch G2240 through the Ethernet Port

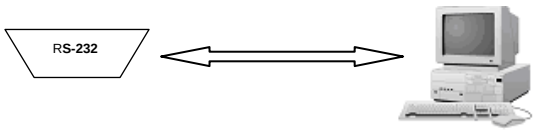
Note: Please first modify the IP address, Subnet mask, Default gateway and DNS through RS-232 console, and then do the next.

Configuring the Management Agent of VigorSwitch G2240 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 G2240
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.

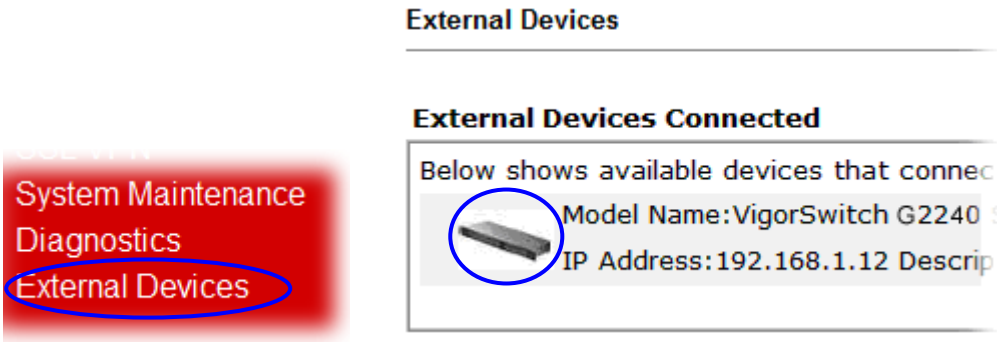
Note: The switch's serial port default settings are listed as follows:

Baud rate	115200
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.



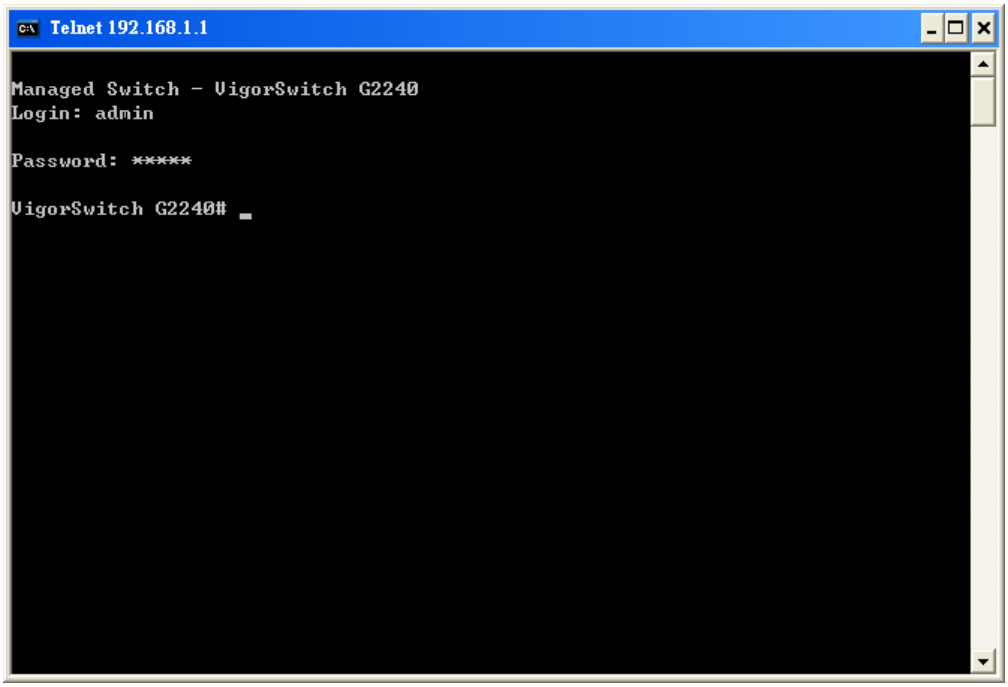
Set IP Address, Subnet Mask and Default Gateway IP Address

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.

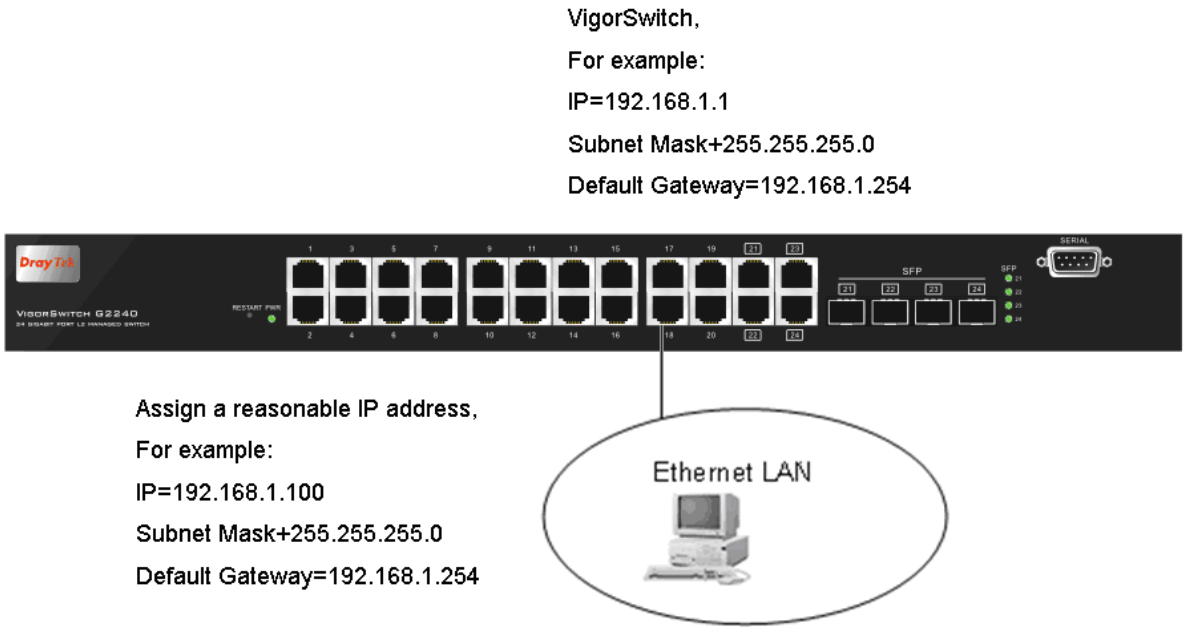
Default Value	VigorSwitch G2240	Your Network Setting
IP Address	192.168.1.1	10.1.1.1
Subnet	255.255.255.0	255.255.255.0
Default Gateway	192.168.1.254	10.1.1.254

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).



Configuring the Management Agent of VigorSwitch G2240 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.



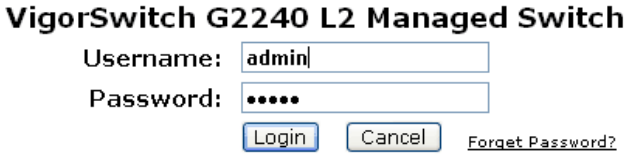
Managing VigorSwitch G2240 through Ethernet Port

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.



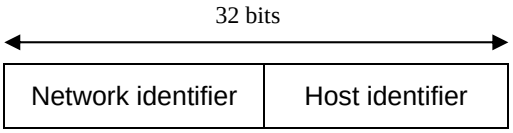
1.5.6 IP Address Assignment

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.

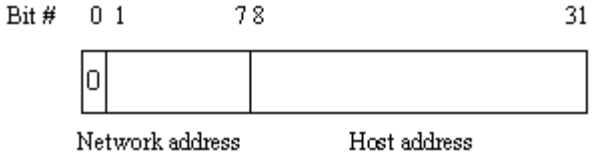
Each class has its own network range between the network identifier and host identifier in the 32 bits address. Each IP address comprises two parts: network identifier (address) and host identifier (address). The former indicates the network where the addressed host resides, and the latter indicates 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.

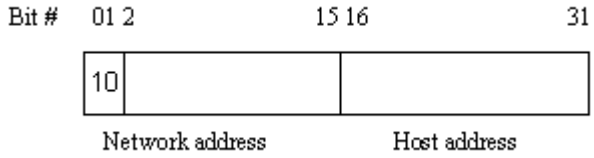
Class A:

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.



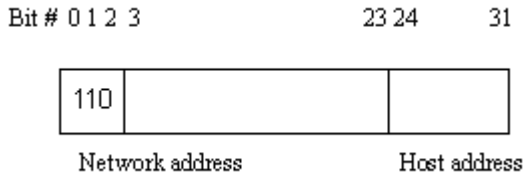
Class B:

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

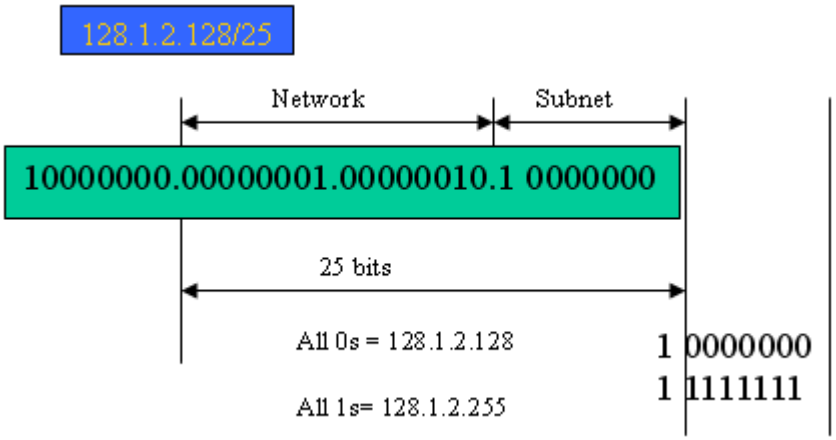
Please refer to RFC 1597 and RFC 1466 for more information.

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.

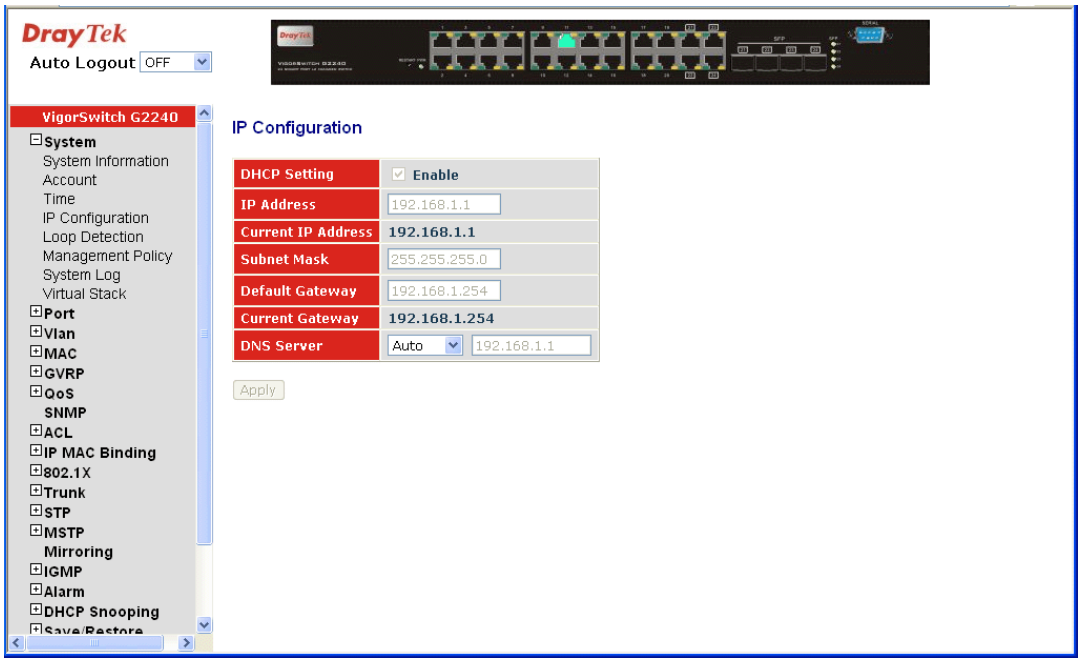
With the subnet mask, a bigger network can be cut into small pieces of network. If we want to have more than two independent networks in a worknet, a partition to the network must be performed. In this case, subnet mask must be applied.

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.



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:

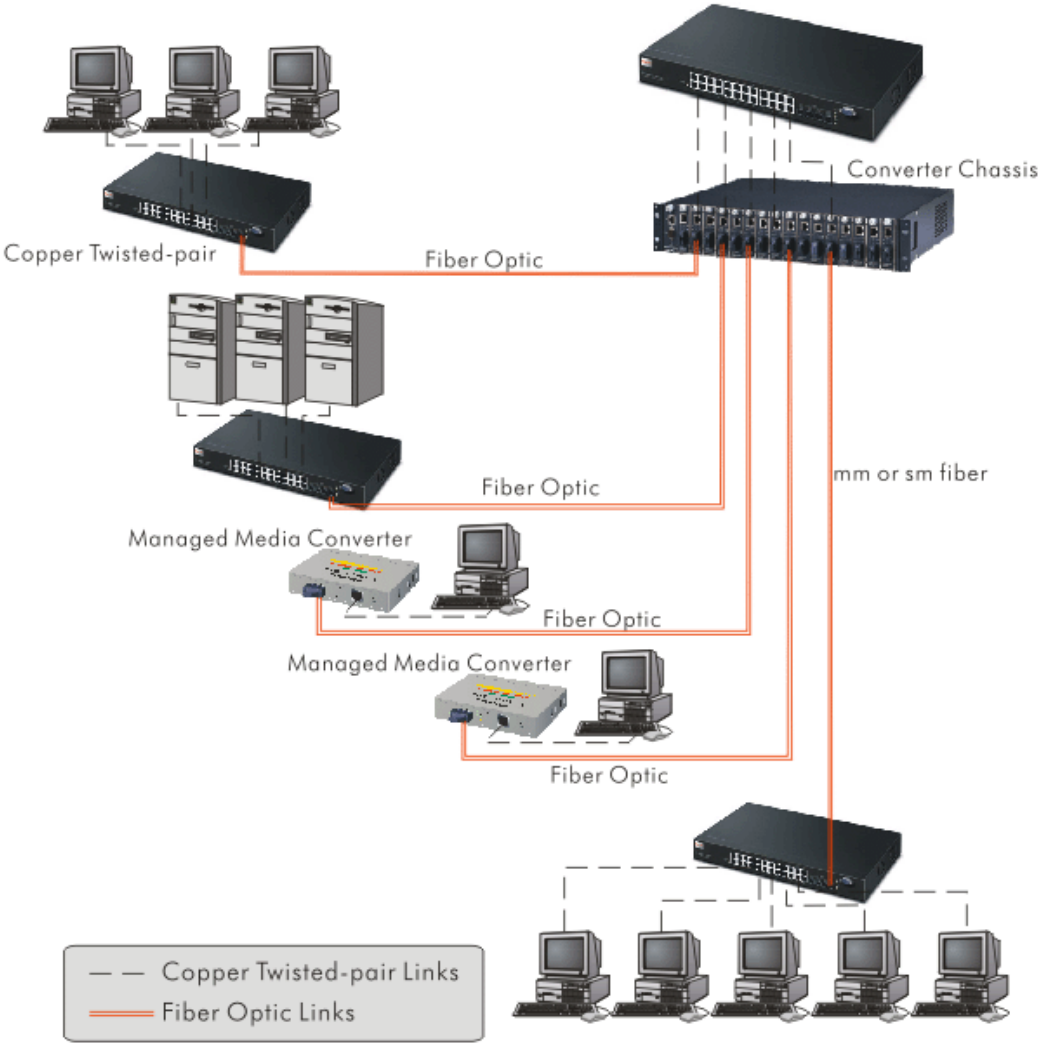
The Domain Name Server translates human readable machine name to IP address. Every machine on the Internet has a unique IP address. A server generally has a static IP address. To connect to a server, the client needs to know the IP of the server. However, user generally uses the name to connect to the 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.

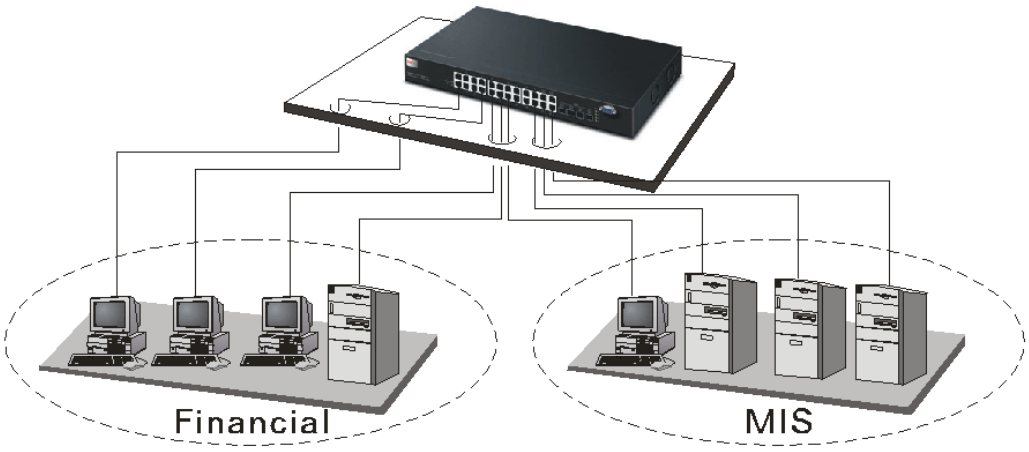
The switch is suitable for the following applications.

- Central Site/Remote site application is used in carrier or ISP

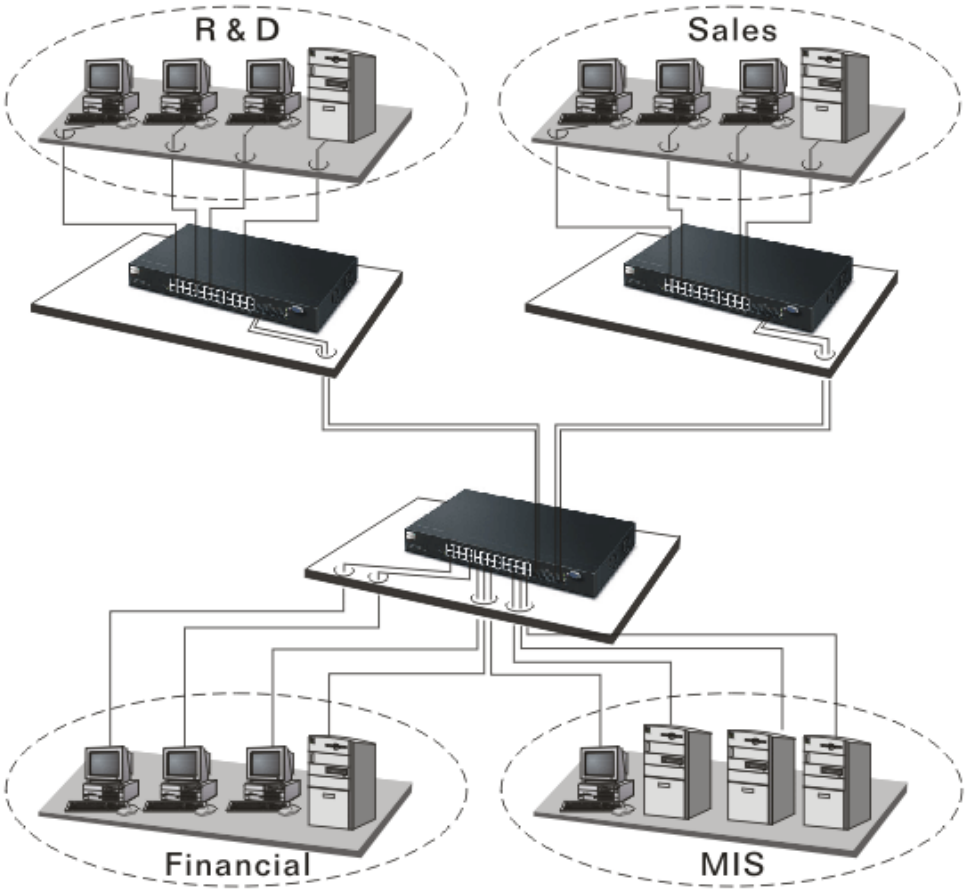


It is a system wide basic reference connection diagram. This diagram demonstrates how the switch connects with other network devices and hosts.

- Peer-to-peer application is used in two remote offices



- Office Network Connection



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 22-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

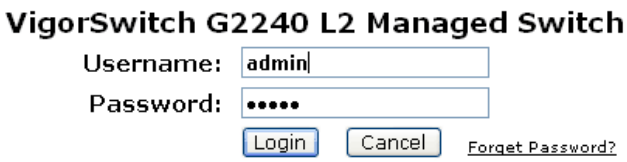
After the managed switch has been finished configuration in the CLI via the switch's serial interface, you can browse it. For example, type http://192.168.1.1 in the address row in a browser, it will show the following screen (see Figure below) and ask you inputting username and password in order to 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.

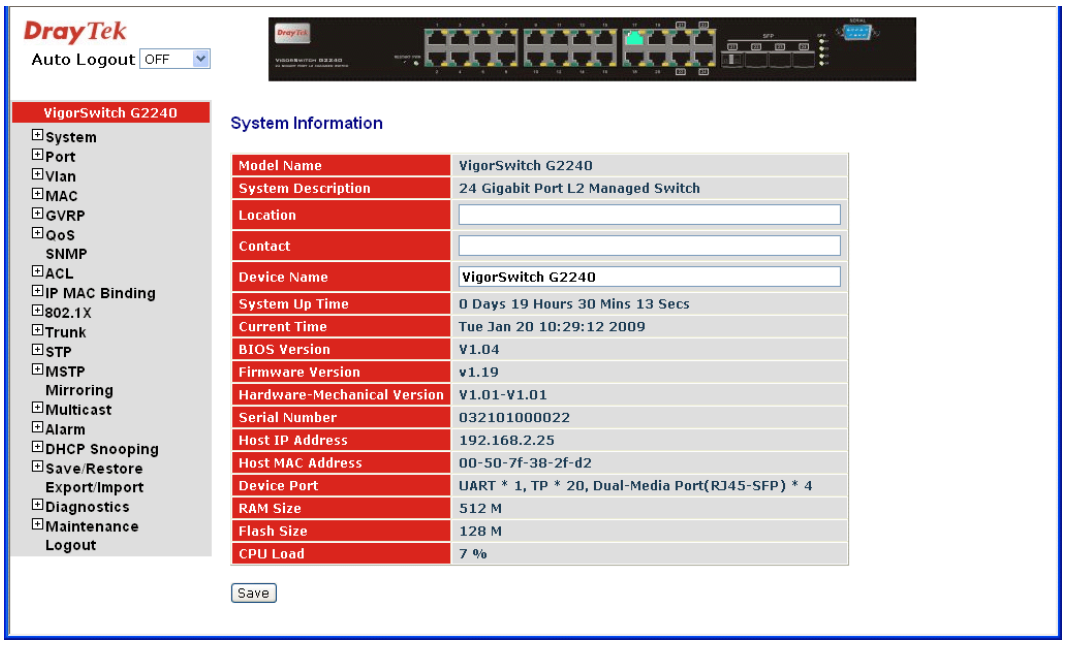
To optimize the display effect, we recommend you use Microsoft IE 6.0 above, Netscape V7.1 above or FireFox V1.00 above and have the resolution 1024x768. The switch supported neutral web browser interface.



2.1 Web Management Home Overview

After you login, the switch shows you the system information as 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”, “Flash Size” and “CPU Load”**. 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.

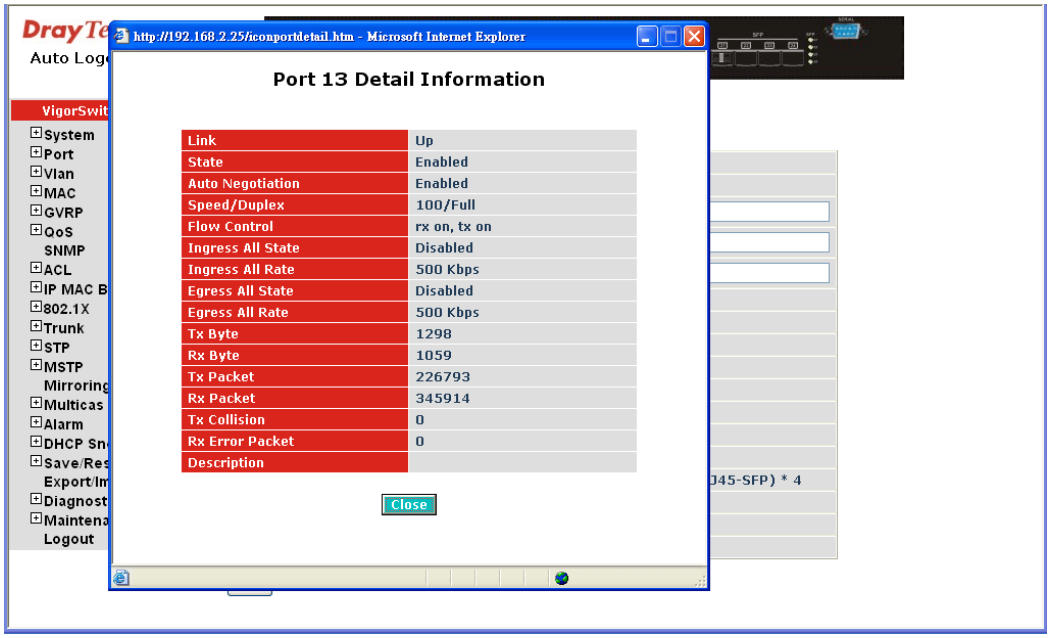
In the following figure, left section is the whole function tree with web user interface and we will travel it through this chapter.



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.

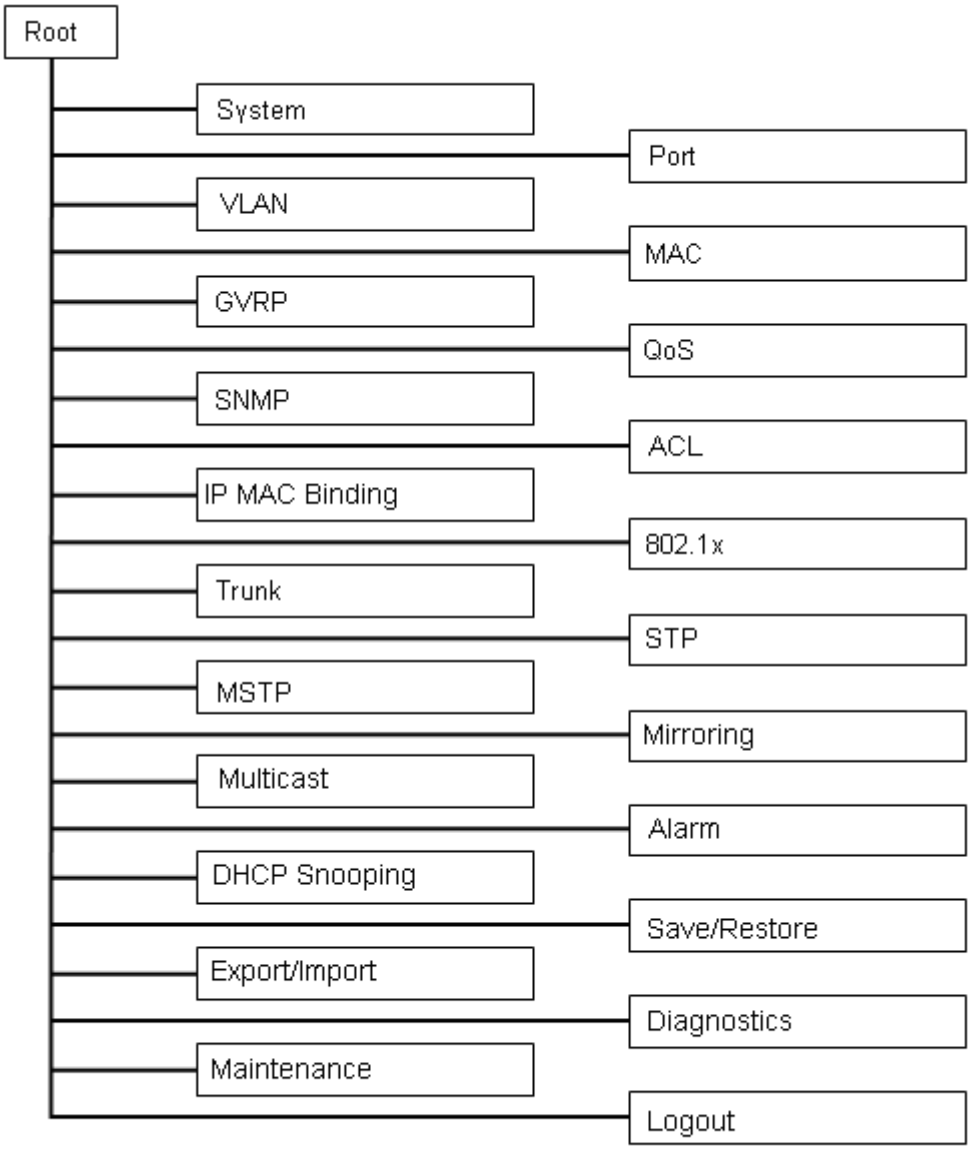
In this device, there are clicking functions on the panel provided for the information of the ports. These are very convenient functions for browsing the information of a single port. When clicking the port on the front panel, an information window for the port will be pop out.



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.



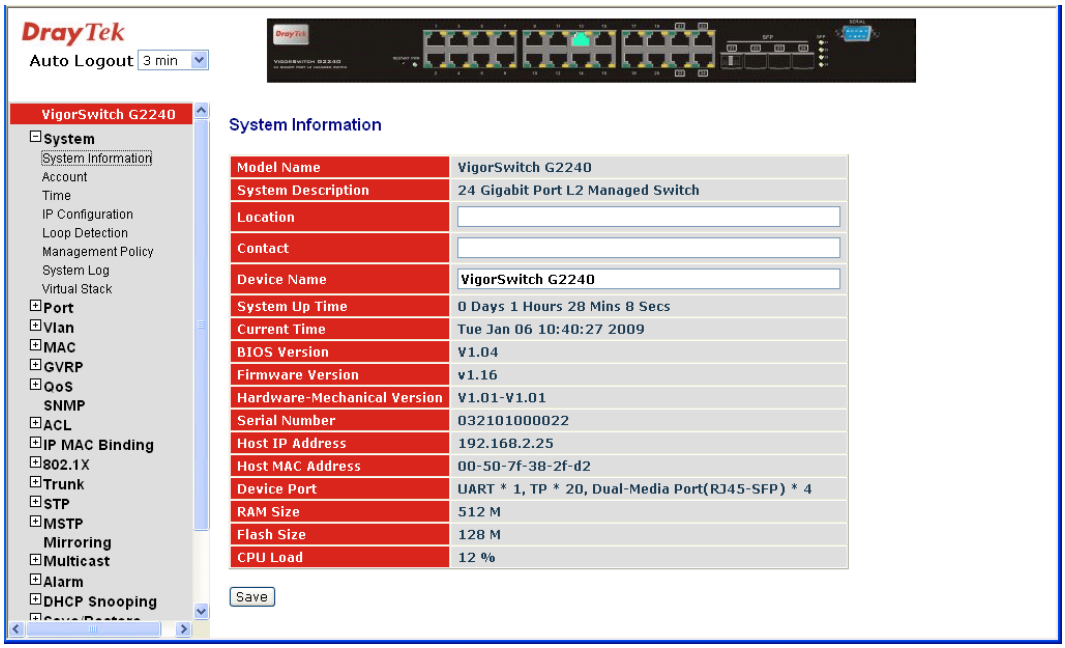
2.1.2 System Information

Function name:

System Information

Function description:

Show the basic system information.



Parameter description:

Model name:	The model name of this device.
System description:	Display what the device's description.
Location:	Set the location of the switch where it was located.
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 G2240.
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.

CPU Load: The loading of the CPU on this switch.

2.1.3 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:

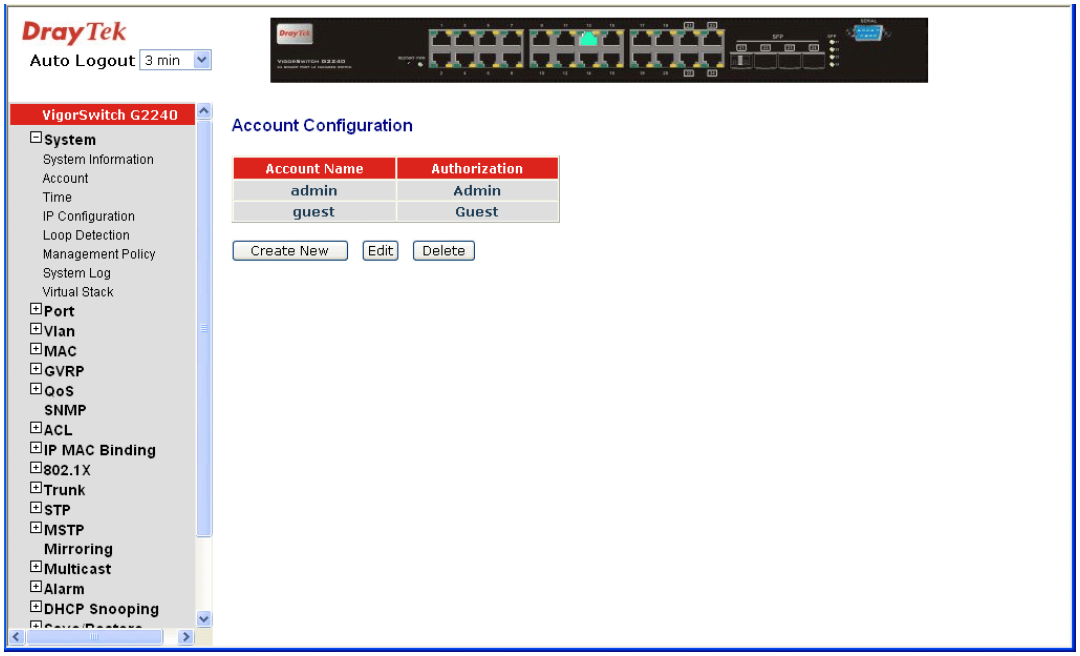
Username: admin

Password: admin

The default setting for guest user account is:

Username: guest

Password: guest



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.

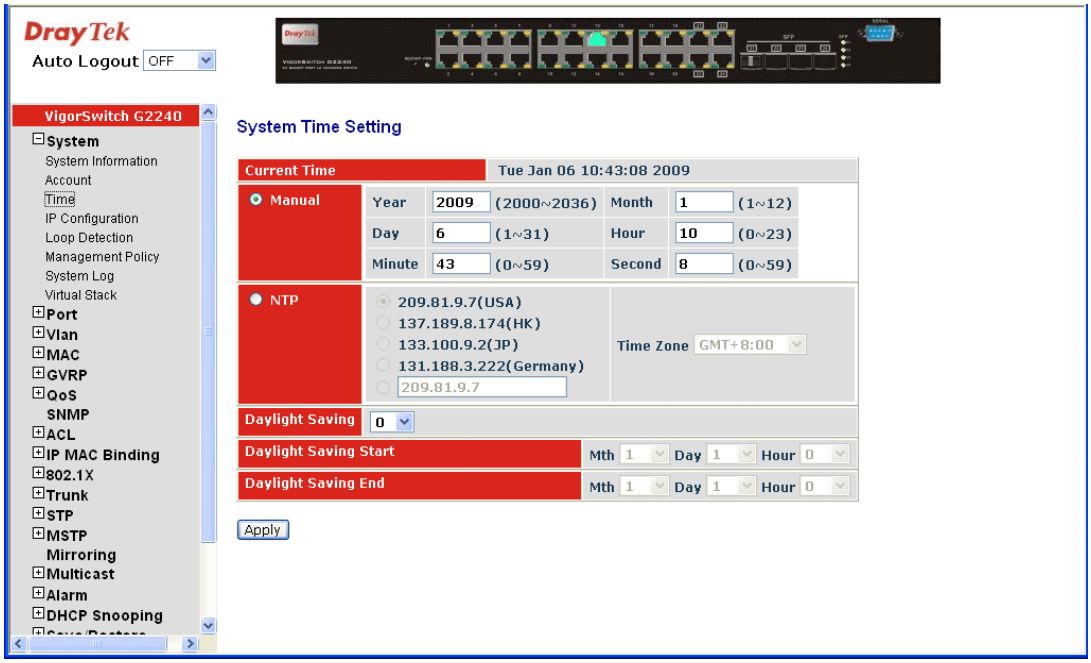
NTP is a well-known protocol used to synchronize the clock of the switch system time over a network. NTP, an internet draft standard formalized in RFC 1305, has been adopted on the system is version 3 protocol. The switch provides four built-in NTP server IP addresses resided in the Internet and a user-defined 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.



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 IP Configuration

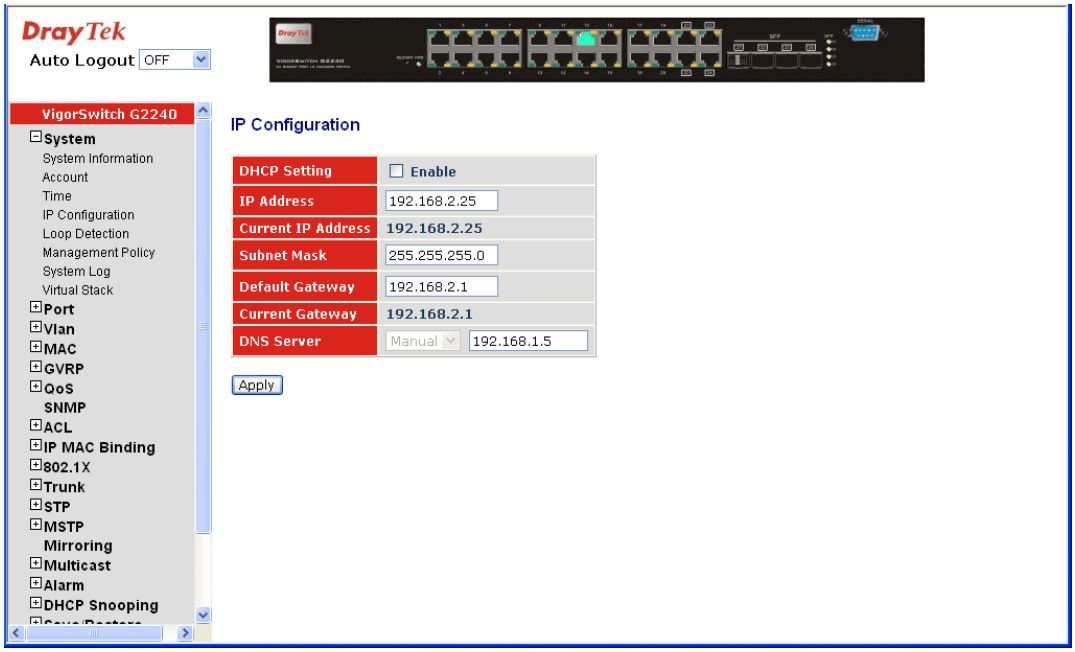
IP configuration is one of the most important configurations in the switch. Without the proper setting, network manager will not be able to manage or view the device. The switch supports both manual IP address setting and automatic IP address setting via DHCP server. When IP address is changed, you must 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.



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

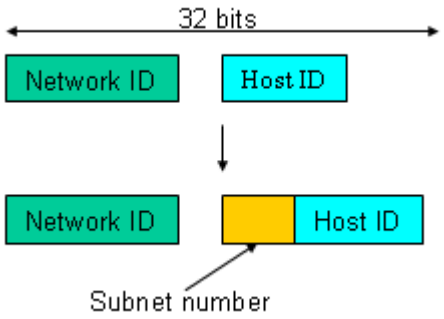
IP address: Users can configure the IP settings and fill in new values if users set the DHCP function “Disable”. Then, click **<Apply>** button to update.

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.

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.

2.1.6 Loop Detection

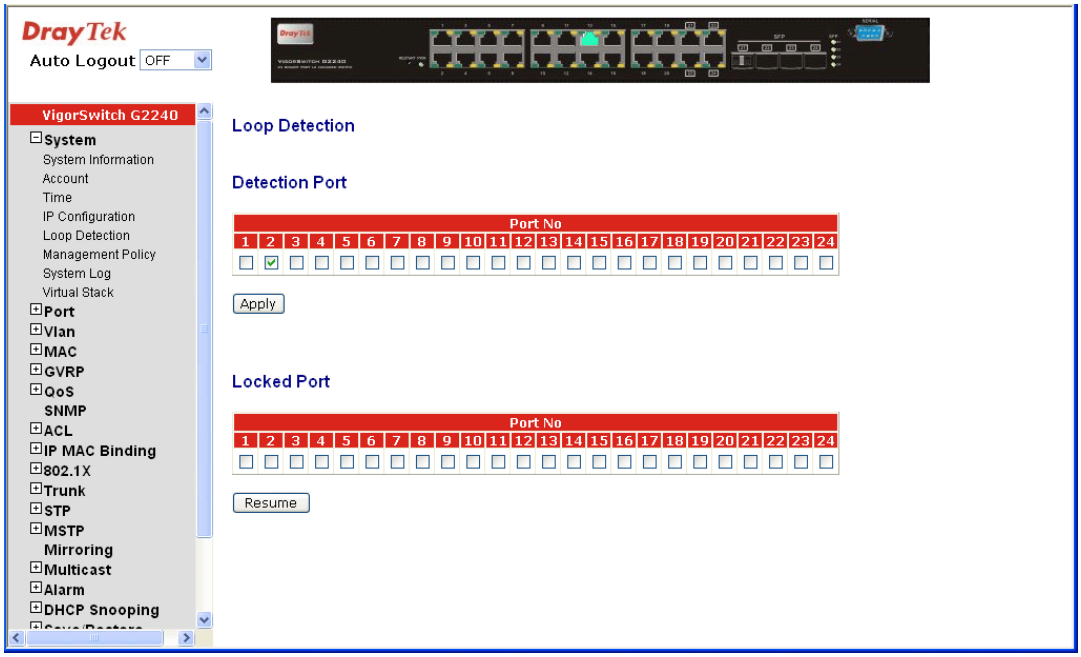
The loop detection is used to detect the presence of traffic. When switch receives packet’s (looping detection frame) MAC address the same as oneself from port, show Loop detection happens. The port will be locked when it received the looping detection frames. If you want to resume the locked port, please find out the looping path and take off the looping path, then select the resume the locked port and click on “Resume” to turn on the locked ports.

Function name:

Loop Detection

Function description:

Display whether switch opens Loop detection.



Parameter description:

Port No:	Display the port number. The number is 1 – 24.
Detection Port - Enable:	When Port No is chosen, and enable port's Loop detection, the port can detect loop happens. When Port-No is chosen, enable port's Loop detection, and the port detects loop happen, port will be locked. If Loop did not happen, port maintains Unlocked.
Locked Port - Resume:	When Port No is chosen, enable port's Loop detection, and the port detects loop happen, the port will be locked. When choosing **Resume**, port locked will be opened and turned into unlocked. If not choosing Resume, Port maintains locked.

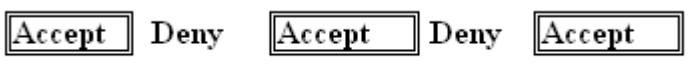
2.1.7 Management Policy

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

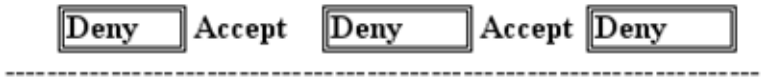
The following rules are offered for the administrator to manage the switch:

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

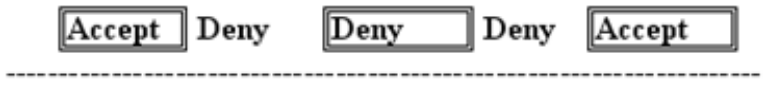
Rule 2): When only "accept lists" exist, then it will deny all connections, excluding the connection inside of the accepting range.



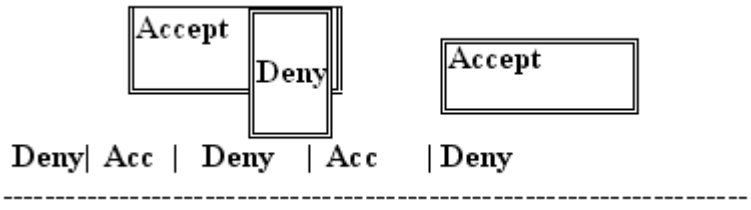
Rule 3): When only "deny lists" exist, then it will accept all connections, excluding the connection inside of the denying range.



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 Policy List

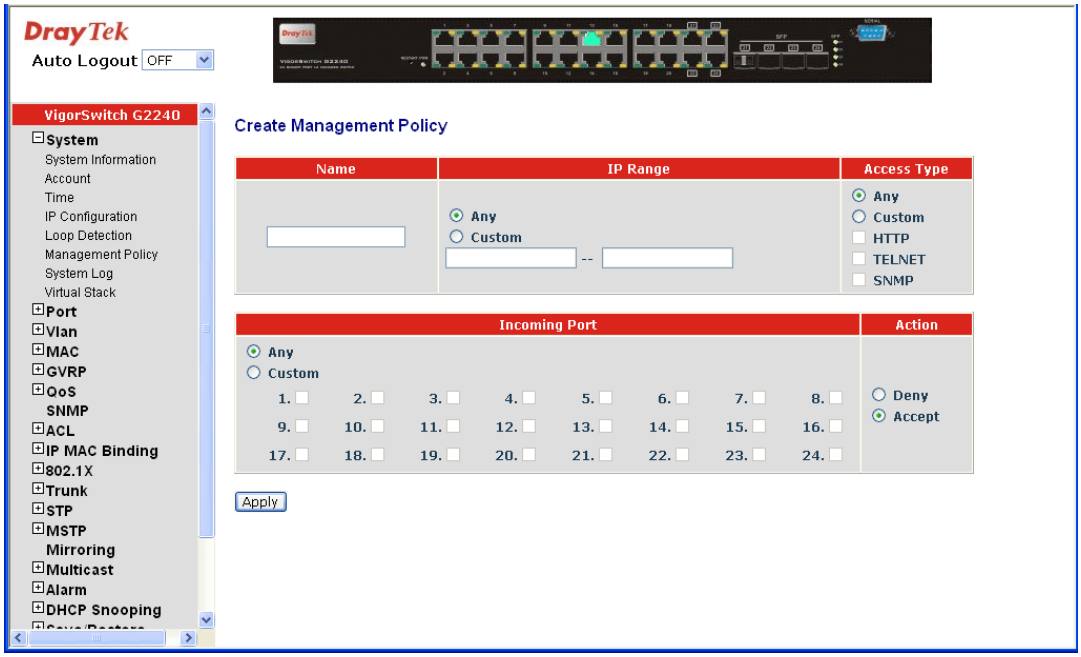
Function description:

The switch offers Management Policy List 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.

Parameter description:

Add:	A new entry of Management Policy List can be created after the parameters as mentioned above had been setup and then press <**Add**> button. Of course, the existed entry also can be modified by pressing this button.
Delete:	Remove the existed entry of Management Policy List from the management security table.

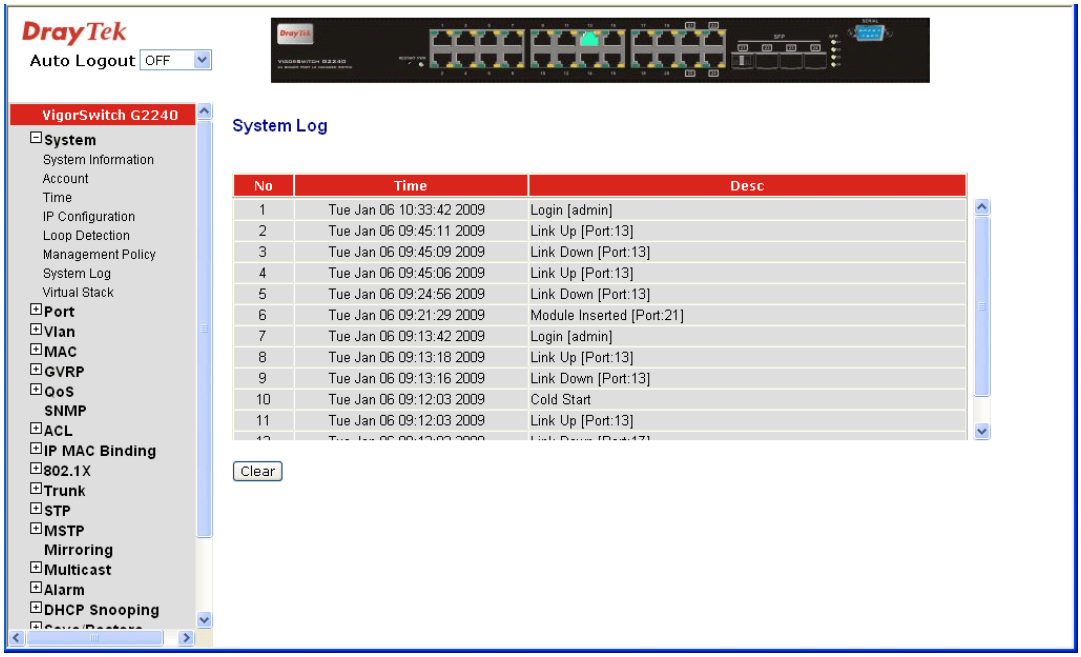
Click **Add** to get the following page:



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

2.1.8 System Log

The System Log provides information about system logs, including information when the device was booted, how the ports are operating, when users logged in, when sessions timed out, as well as other system information.



Function name:

System Log

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.

Parameter description:

No:	Display the order number that the trap happened.
Time:	Display the time that the trap happened.
Desc:	Display a description event recorded in the System Log.
Clear:	Clear log data.

2.1.9 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.

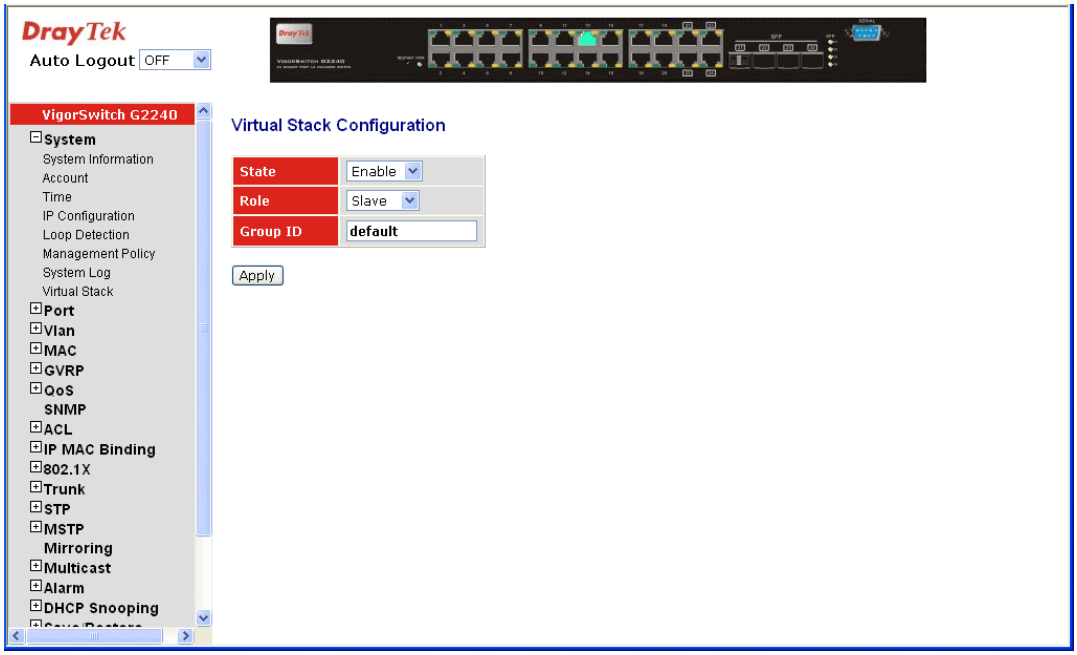
The most top-left button is only for Master device. The background color of the button you press will be changed to represent that the device is under your management.

> **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. 10_VigorSw), 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.



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

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 Configuration

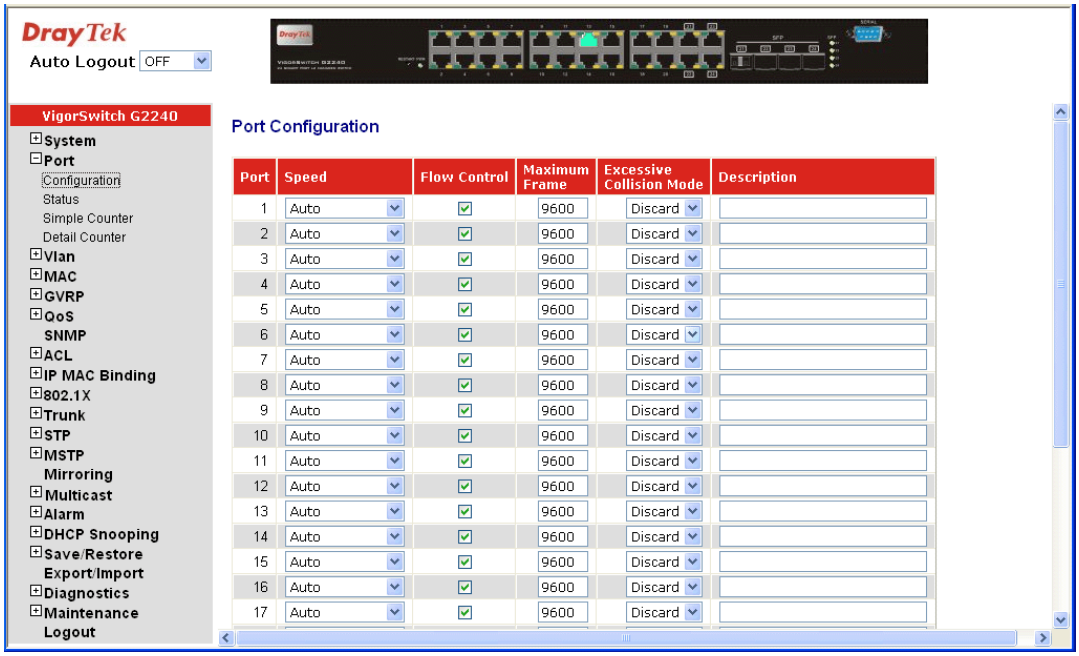
Port Configuration is applied to change the setting of each port. In this configuration function, you can set/reset the following functions. All of them are described in detail below.

Function name:

Port Configuration

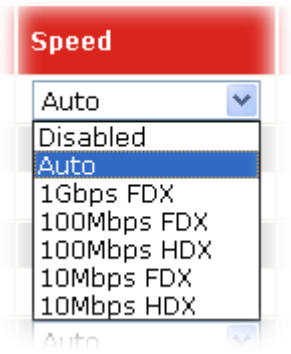
Function description:

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.



Parameter description:

Speed: Set the speed and duplex of the port. In speed, 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
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 Enable and Disable. If flow control is set Enable, both parties can send PAUSE frame to the transmitting device(s) if the receiving port is too busy to handle. When it is set Disable, there will be no flow control in the port. It drops the packet if too much to handle.

Maximum Frame: This module offers 1518~9600 (Bytes) length to make the long packet.

Excessive Collision Mode: There are two modes to choose when excessive collision happened in half-duplex condition as below:

Discard: The “Discard” mode determines whether the MAC drop frames after an excessive collision has occurred. If yes, a frame is dropped after excessive collision. This is IEEE Standard 802.3 half-duplex flow control operation.

Restart: The “Restart” mode determines whether the MAC retransmits frames after an excessive collision has occurred. If set, a frame is not dropped after excessive collisions, but the backoff sequence is restarted. This is a violation of IEEE Standard 802.3, but is useful in non-dropping half-duplex flow control operation.

Description: Description of device ports can not include “ # % & ‘ + \.

2.2.2 Port Status

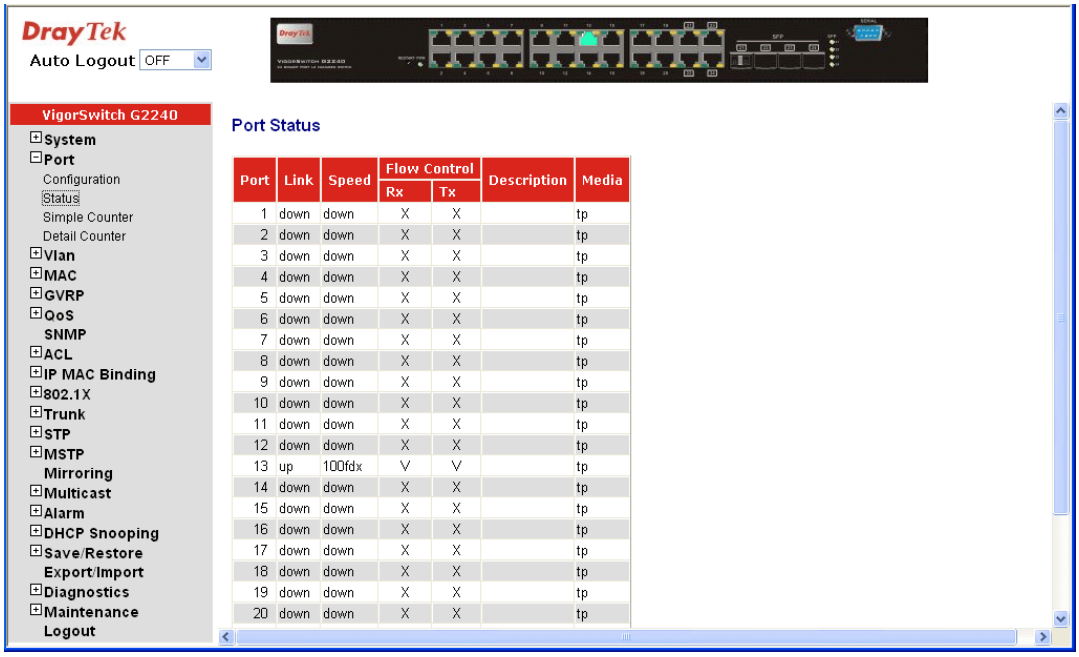
The function Port Status gathers the information of all ports’ current status and reports it by the order of port number, media, link status, port state, Auto-Negotiation status, speed/duplex, Rx Pause and Tx Pause. An extra media type information for the module ports 21 and 24 is also offered.

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.

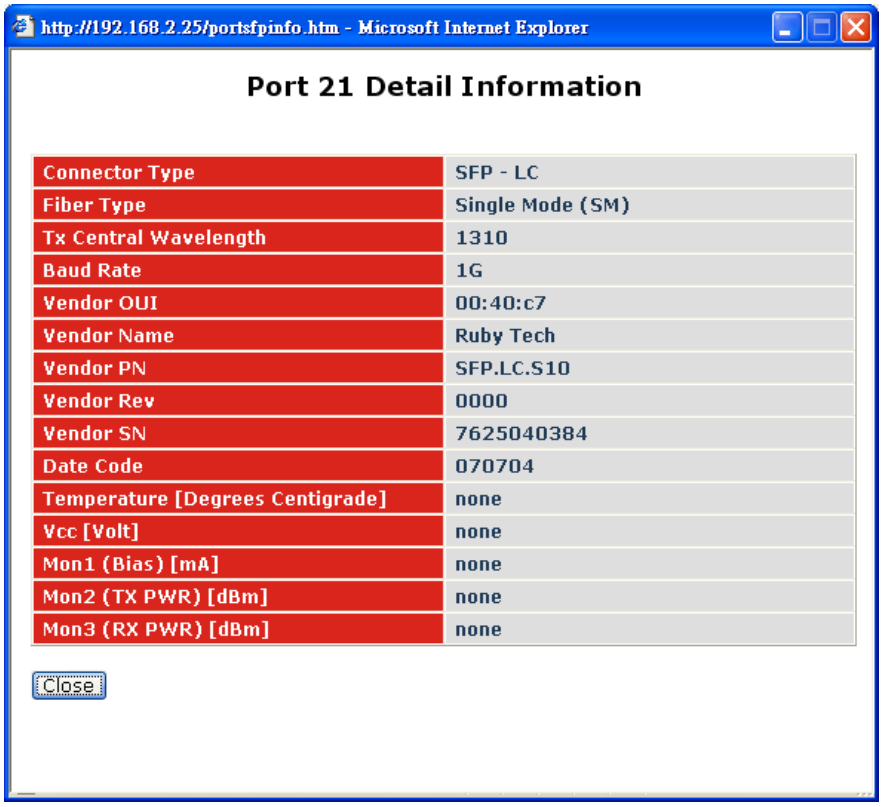


Parameter Description:

Port:	Display the port number. The number is 1 – 24. Both port 21 ~ 24 are optional modules.
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.
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. Default: None, depends on the result of the negotiation.
Flow Control:	Show each port’s flow control status. There are two types of flow control in Ethernet, Backpressure for half-duplex operation and Pause flow control (IEEE802.3x) for full-duplex operation. The switch supports both of them. Default: None, depends on the result of the negotiation.
Port Description:	Network managers provide a description of device ports.

***Parameter description of Port 21 ~ Port 24**:*

Note: If you want to get the below detail information then you need to click right button of mouse on SFP icon.



Connector Type:	Display the connector type, for instance, UTP, SC, ST, LC and so on.
Fiber Type:	Display the fiber mode, for instance, Multi-Mode, Single-Mode.
Tx Central Wavelength:	Display the fiber optical transmitting central wavelength, for instance, 850nm, 1310nm, 1550nm and so on.
Baud Rate:	Display the maximum baud rate of the fiber module supported, for instance, 10M, 100M, 1G and so on.
Vendor OUI:	Display the Manufacturer's OUI code which is assigned by IEEE.
Vendor Name:	Display the company name of the module manufacturer.
Vendor P/N:	Display the product name of the naming by module manufacturer.
Vendor Rev (Revision):	Display the module revision.
Vendor SN (Serial Number):	Show the serial number assigned by the manufacturer.
Date Code:	Show the date this SFP module was made.
Temperature:	Show the current temperature of SFP module.
Vcc:	Show the working DC voltage of SFP module.
Mon1(Bias) mA:	Show the Bias current of SFP module.
Mon2(TX PWR):	Show the transmit power of SFP module.

Mon3(RX PWR): Show the receiver power of SFP module.

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.

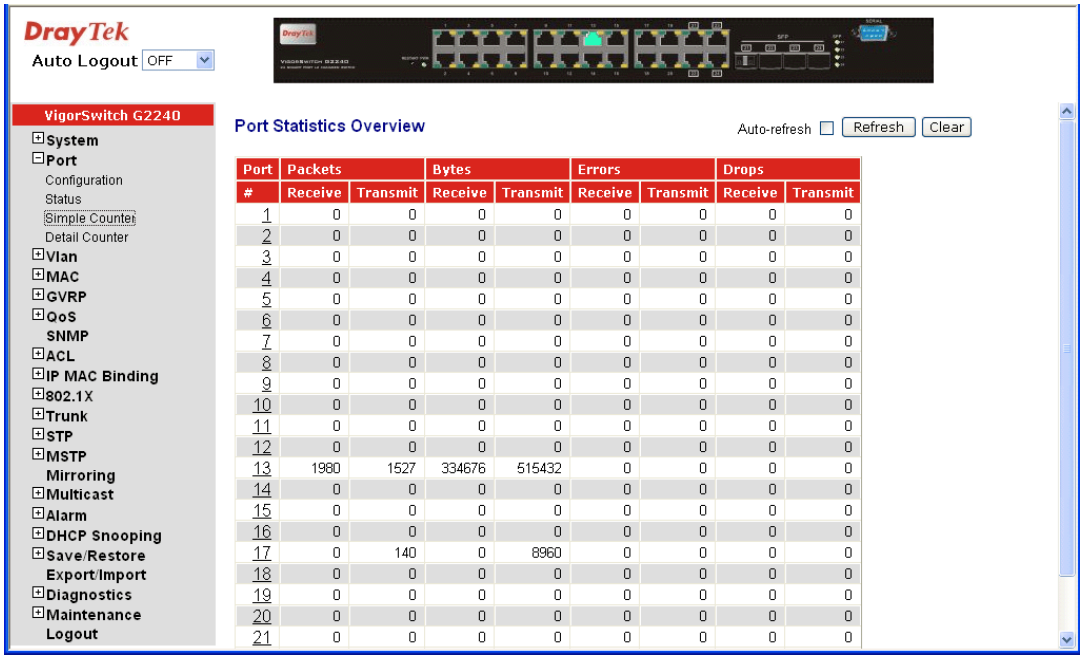
In the following figure, the window can show all ports' counter information at the same time. Each data field has 20-digit long. If the counting is overflow, the counter will be reset and restart counting. The data is updated every time interval defined by the user. The Refresh Interval is used to set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

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.



Port	Packets		Bytes		Errors		Drops	
#	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	1980	1527	334676	515432	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0
17	0	140	0	8960	0	0	0	0
18	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0

Parameters description:

Packet:	Transmit - The counting number of the packet transmitted. Receive - The counting number of the packet received.
Bytes:	Transmit - Total transmitted bytes. Receive - Total received bytes.
Error:	Transmit - Number of bad packets transmitted. Receive - Number of bad packets received.
Drops:	Transmit - Number of packets transmitted drop. Receive - Number of packets received drop.
Auto-refresh:	The simple counts will be refreshed automatically on the UI screen.
Refresh:	The simple counts will be refreshed manually when user use mouse to click on "Refresh" button.
Clear:	The simple counts will be reset to zero when user use mouse to click on "Clear" button.

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.

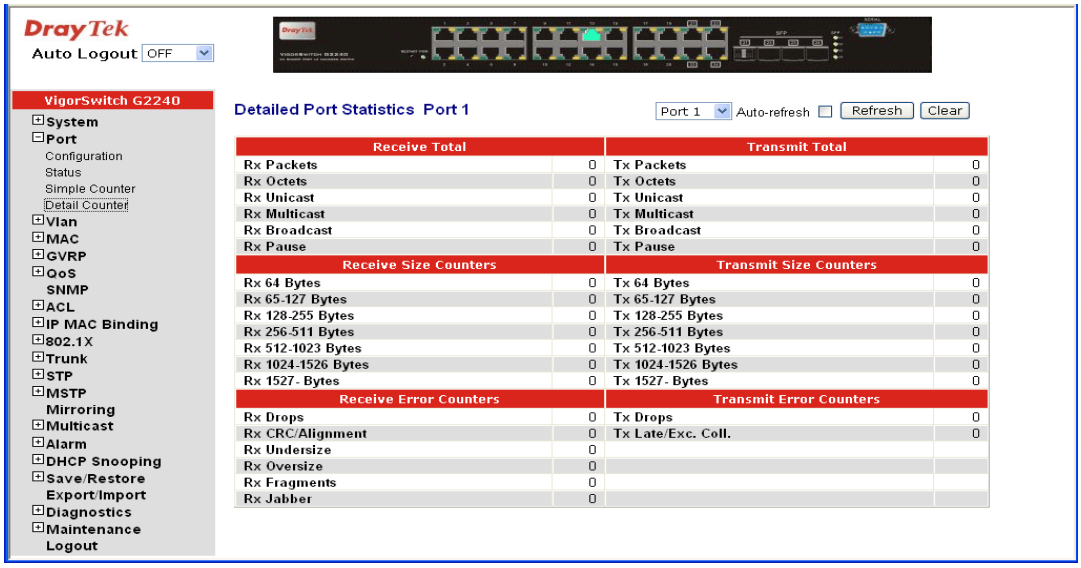
Each data field has 20-digit long. If the counting is overflow, the counter will be reset and restart counting. The data is updated every time interval defined by the user. The valid range is 3 to 10 seconds. The Refresh Interval is used to set the update frequency. Default update time is 3 seconds.

Function name:

Detail Counter

Function description:

Display the detailed counting number of each port's traffic. In the following figure, the window can show all counter information of each port at one time.



Parameter description:

Rx Packets:	The counting number of the packet received.
Rx Octets:	Total received bytes.
Rx Unicast:	Show the counting number of the received unicast packet.
Rx Broadcast:	Show the counting number of the received broadcast packet.
Rx Pause:	Show the counting number of the received pause packet.
RX 64 Bytes:	Number of 64-byte frames in good and bad packets received.
RX 65-127 Bytes:	Number of 65 ~ 127-byte frames in good and bad packets received.
RX 128-255 Bytes:	Number of 128 ~ 255-byte frames in good and bad packets received.
RX 256-511 Bytes:	Number of 256 ~ 511-byte frames in good and bad packets received.

RX 512-1023 Bytes:	Number of 512 ~ 1023-byte frames in good and bad packets received.
RX 1024- 1522 Bytes:	Number of 1024-1522-byte frames in good and bad packets received.
RX 1527 Bytes:	Number of 1527-byte frames in good and bad packets received.
Rx Drops:	Number of frames dropped due to the lack of receiving buffer.
Rx CRC/Alignment:	Number of Alignment errors packets received.
Rx Undersize:	Number of short frames (<64 Bytes) with valid CRC.
Rx Oversize:	Number of long frames (according to max_length register) with valid CRC.
Rx Fragments:	Number of short frames (< 64 bytes) with invalid CRC.
Rx Jabber:	Number of long frames (according tomax_length register) with invalid CRC.
Tx Packets:	The counting number of the packet transmitted.
TX Octets:	Total transmitted bytes.
Tx Unicast s:	Show the counting number of the transmitted unicast packet.
Tx Multicast:	Show the counting number of the transmitted multicast packet.
Tx Broadcast:	Show the counting number of the transmitted broadcast packet.
Tx Pause:	Show the counting number of the transmitted pause packet.
TX 64 Bytes:	Number of 64-byte frames in good and bad packets transmitted.
TX 65-127 Bytes:	Number of 65 ~ 127-byte frames in good and bad packets transmitted.
TX 128-255 Bytes:	Number of 128 ~ 255-byte frames in good and bad packets transmitted.
TX 256-511 Bytes:	Number of 256 ~ 511-byte frames in good and bad packets transmitted.
TX 512-1023 Bytes:	Number of 512 ~ 1023-byte frames in good and bad packets transmitted.
TX 1024- 1522 Bytes:	Number of 1024 ~ 1522-byt frames in good and bad packets transmitted.
TX 1527 Bytes:	Number of 1527-byte frames in good and bad packets transmitted.
Tx Drops:	Number of frames dropped due to excessive collision, late collision, or frame aging.
Tx lat/Exc.Coll.	Number of Frames late collision or excessive collision Error, which switch transmitted

2.3 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.

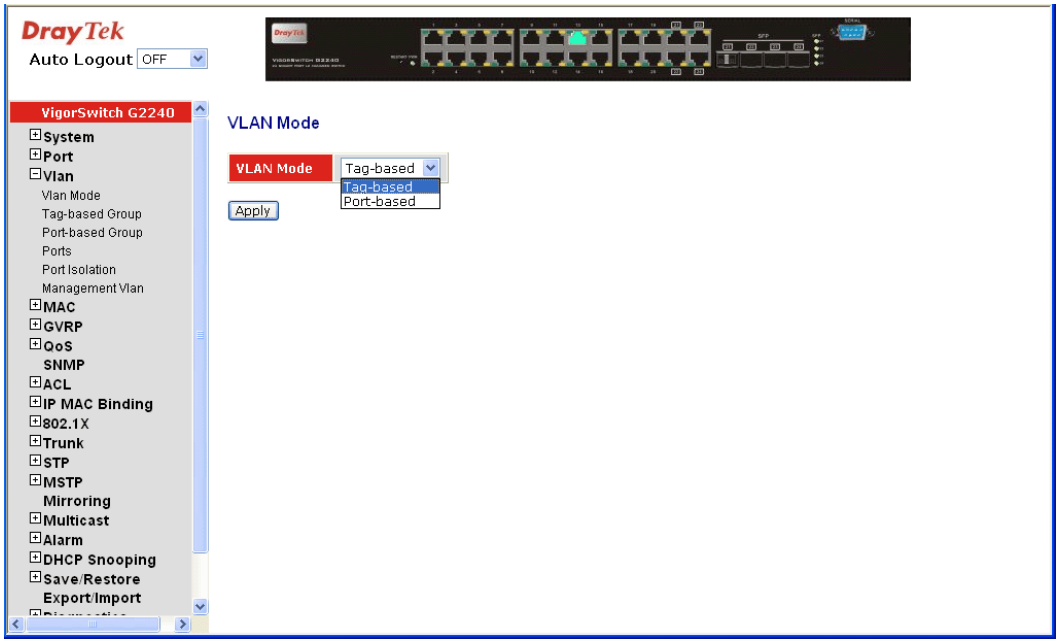
2.3.1 VLAN Mode

Function name:

VLAN Mode

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.



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.

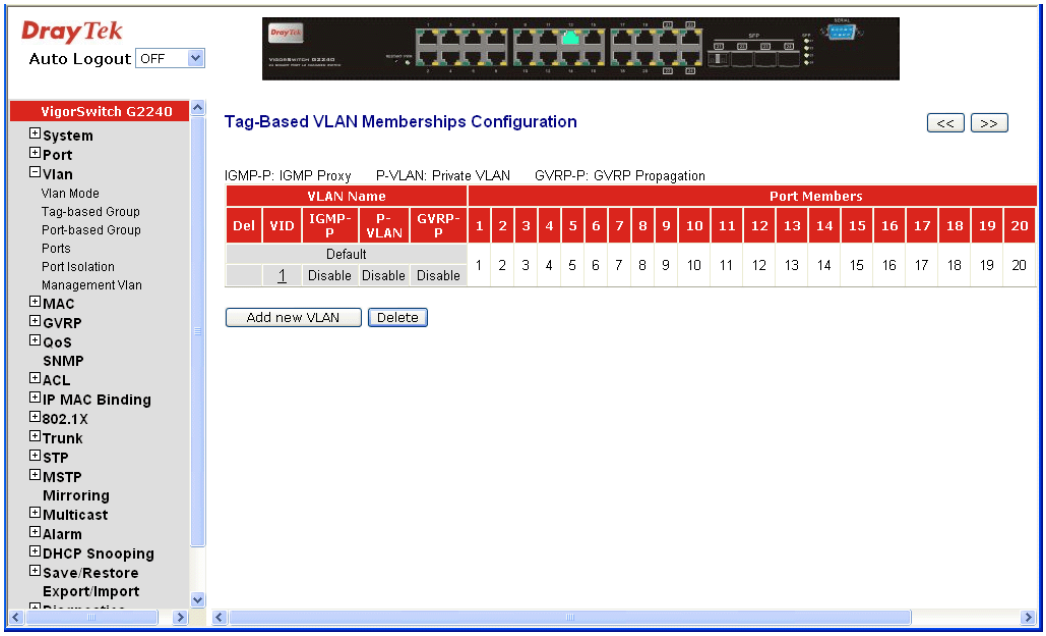
2.3.2 Tag-based Group

Function name:

Tag-based Group

Function description:

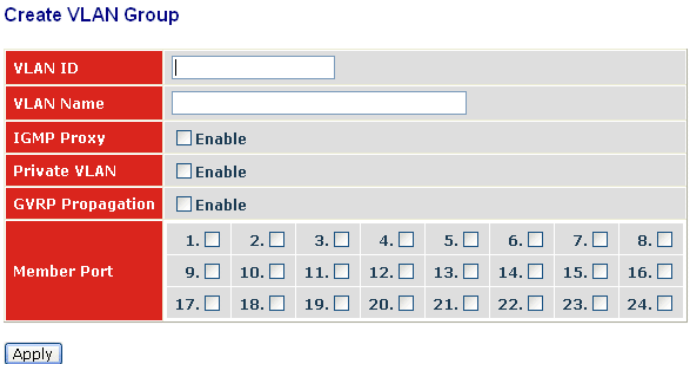
It shows the information of existed Tag-based VLAN Groups, You can also easily create, edit and delete a Tag-based VLAN group by pressing **<Add>**, **<Edit>** and **<Delete>** function buttons. User can add a new VLAN group by inputting a new VLAN name and VLAN ID.



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.
IGMP:	IGMP proxy enables the switch to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts. This switch can be set IGMP function **"Enable" or "Disable"** by VLAN group. If the VLAN group IGMP proxy is disabled, the switch will stop the exchange of IGMP messages in the VLAN group members. If the VLAN group IGMP proxy is enabled, the switch will support the exchange of IGMP messages in the VLAN group members and follow up IGMP proxy router port configuration, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

	You enable IGMP on the interfaces that connect the system to its hosts that are farther away from the root of the tree. These interfaces are known as downstream interfaces.
PVLAN:	Private VLAN ID identifier. Each Private VLAN group has a unique VID. Private VLAN contains switch ports that cannot communicate with each other but can access another network. It appears only in tag-based and Double-tag mode.
GVRP-P:	GVRP Propagation identifier. GVRP allows the propagation of VLAN information from device to device. With GVRP, a single switch is manually configured with all the desired VLANs for the network, and all other switches on the network learn those VLANs dynamically.
Port Members:	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.
Add new VLAN:	Please click on **<Add new VLAN>** to create a new Tag-based VLAN. Input the VLAN name as well as VID, configure the SYM-VLAN function and choose the member by ticking the check box beside the port No., then, press the **<Apply>** button to have the setting taken effect.



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

Note: If you need to use PVLAN(Private VLAN) function on Switch, you need to follow up the process as below:

1. Create a VLAN as primary VLAN and the VLAN ID is 2 and evoke the Private VLAN to enable Private VLAN service.

2. Assign port member to the VLAN2.

3. You need to assign these ports for member of port isolation.

4. Press the **"Save"** to complete the PVLAN configuration process.

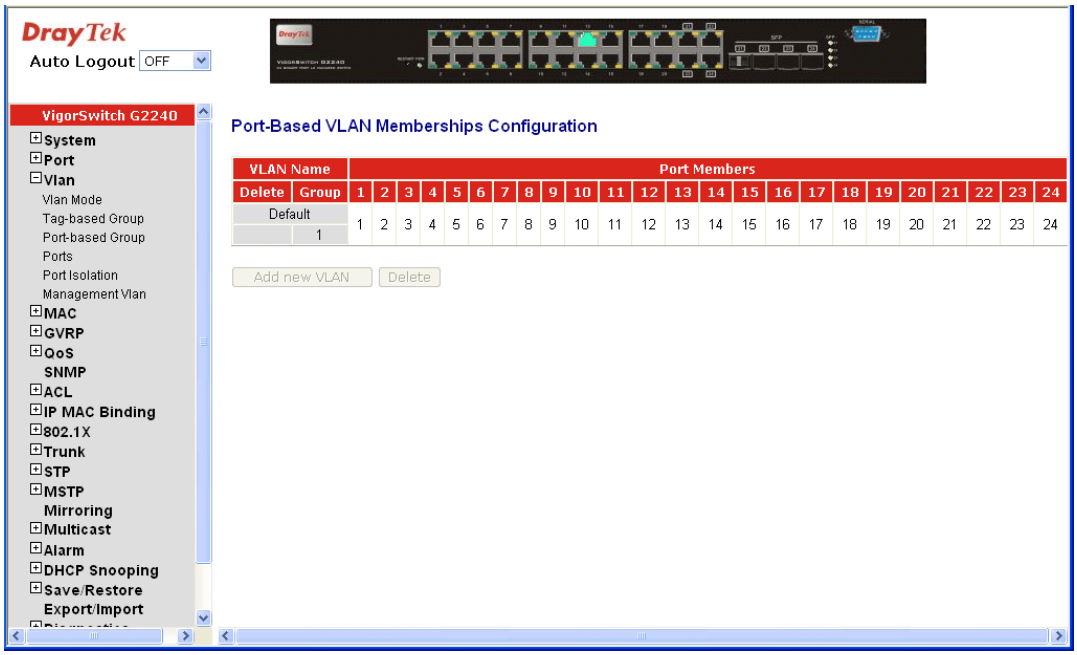
2.3.3 Port-based Group

Function name:

Port-based Group

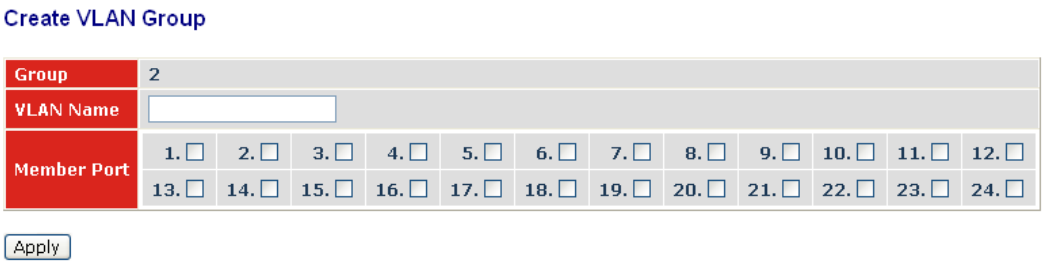
Function description:

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.



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.
Port Members:	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.
Add new VLAN	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.



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

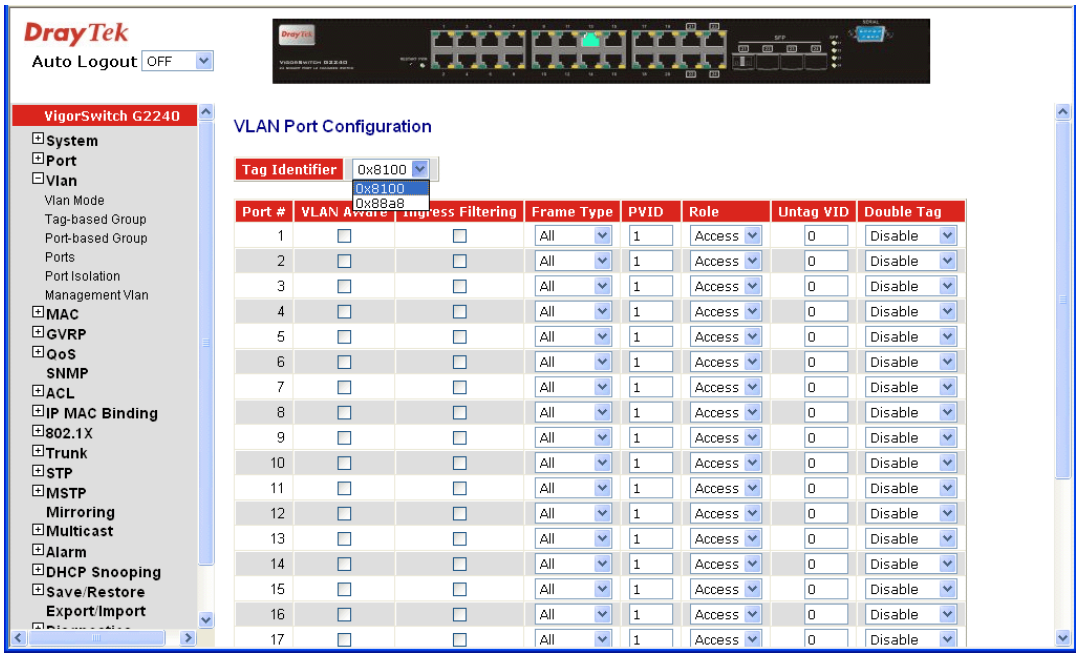
2.3.4 Ports

Function name:

VLAN Port Configuration

Function description:

In VLAN Tag Rule 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 rules to each port. There are two ingress filtering rules which can be applied to the switch. The Ingress Filtering Rule 1 is “forward only packets with VID matching this port’s configured VID”. The Ingress Filtering Rule 2 is “drop untagged frame”. You can also select the Role of each port as Access, Trunk, or Hybrid.



Parameter description:

Port 1-24:	Port number.
VLAN Aware:	Based on IEEE 802.1Q VLAN tag to forward packet.
Ingress Filtering:	Discard other VLAN group packets, only forward this port joined VLAN group packets.
Frame Type:	All: Forward all tagged and untagged packets. Tagged: Forward tagged packets only and discard untagged packets.
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.
Role:	This is an egress rule of the port. Here you can choose Access, Trunk or Hybrid. Trunk means the outgoing packets must carry VLAN tag header. Access means the outgoing packets carry no VLAN tag header. If packets have double VLAN tags, one will be dropped and the other will still be left. As to Hybrid, it is similar to Trunk, and both of them

will tag-out. When the port is set to Hybrid, its packets will be untagged out if the VID of the outgoing packets with tag is the same as the one in the field of Untag VID of this port.

Untag VID: Valid range is 1~4094. It works only when Role is set to Hybrid.

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. Scroll to enable the function and default is Disable.

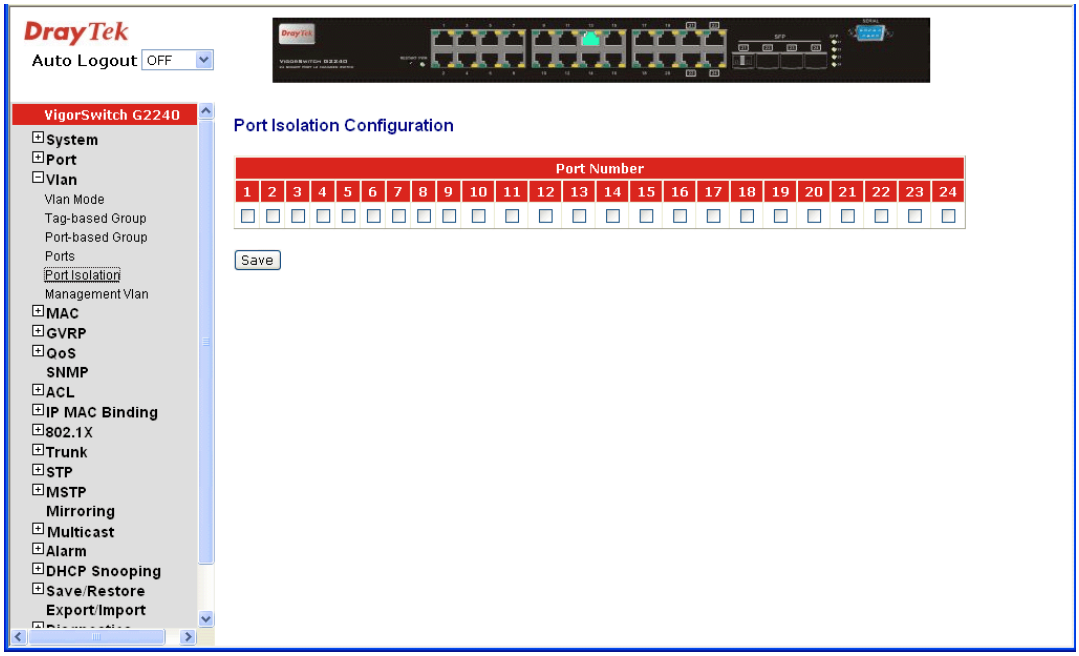
2.3.5 Port Isolation

Function name:

Port Isolation Configuration

Function description:

Port Isolation is the function what used on a layer 2 switch comprises configuring each of the ports on the layer 2 switch as a protected port or a non-protected port. A destination address on an data packet is matched with a physical address on said layer 2 switch and a forwarding map is generated for the data packet based upon the destination address on the data packet.



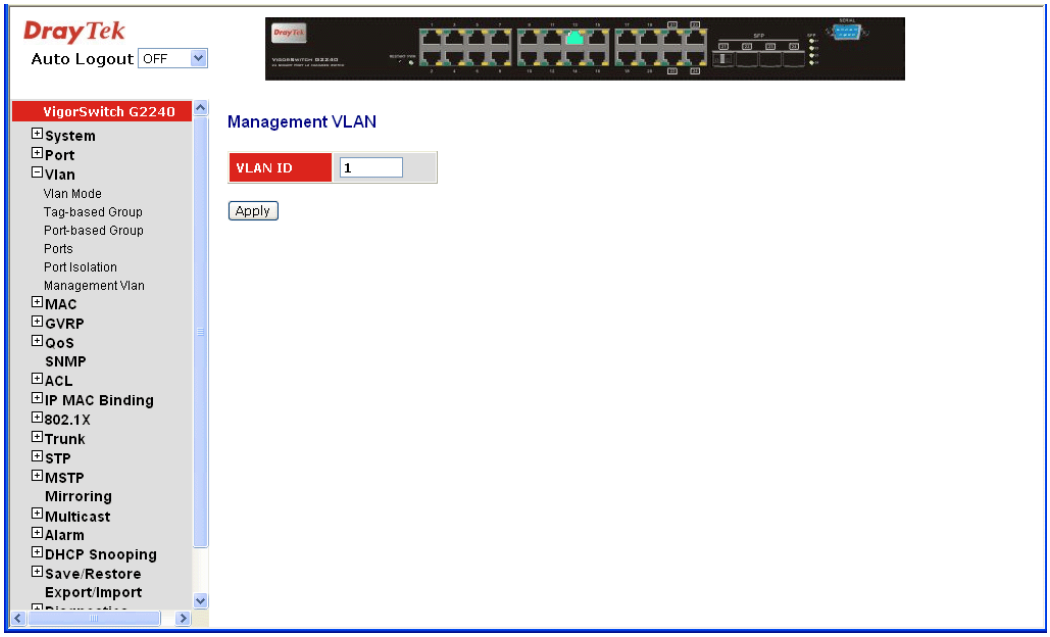
2.3.6 Management VLAN

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.



Parameter description:

VID: Valid range 1~4094.

2.4 MAC

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.

2.4.1 MAC Address Table Configuration

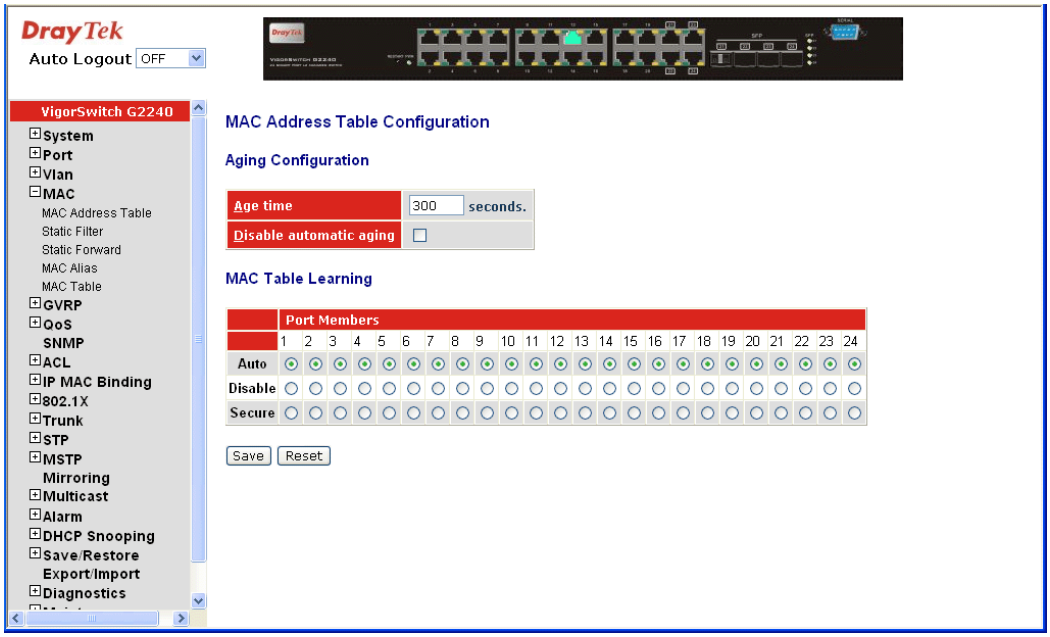
Function name:

MAC Address Table Configuration

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 10-1000000 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.



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 10-1000000 seconds. The default Aging Time is 300 seconds.
Disable automatic aging:	Stop the MAC table aging timer, the learned MAC address will not age out automatically
Auto:	Enable this port MAC address dynamic learning mechanism.
Disable:	Disable this port MAC address dynamic learning mechanism, only support static MAC address setting.
Secure:	Disable this port MAC address dynamic learning mechanism and copy the dynamic learning packets to CPU
Save:	Save MAC Address Table configuration
Reset:	Reset MAC Address Table configuration

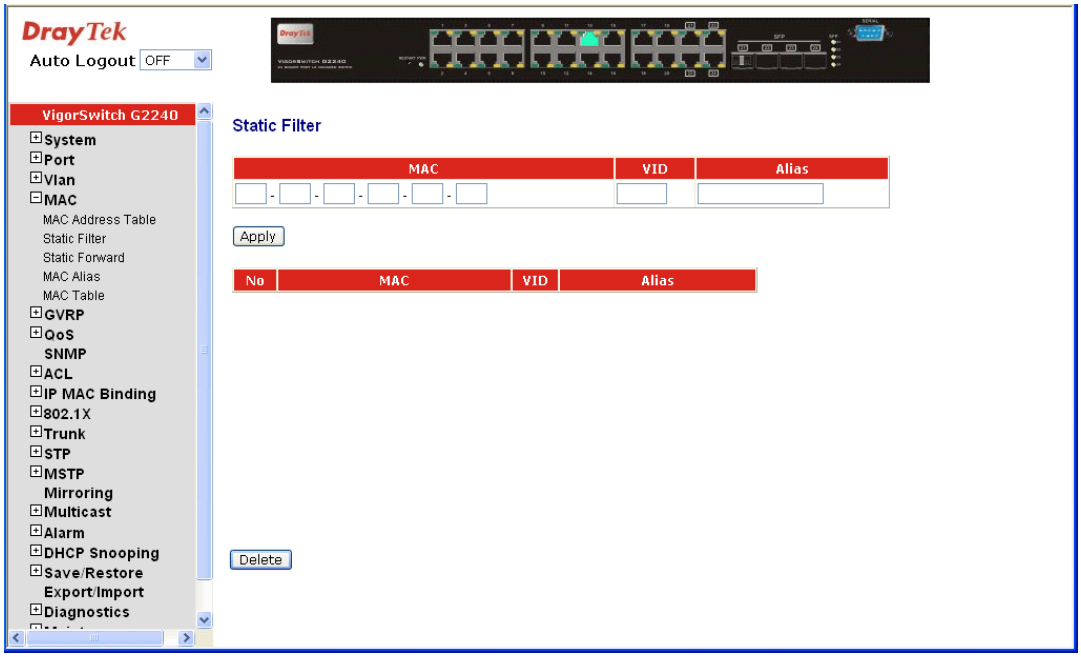
2.4.2 Static Filter

Function Name:

Static Filter

Function Description:

Static Filter is a function that denies the packet forwarding if the packet's MAC Address is listed in the filtering Static Filter table. User can very easily maintain the table by filling in MAC Address, VID (VLAN ID) and Alias fields individually. User also can delete the existed entry by clicking **<Delete>** button.



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 - 02
VID:	VLAN identifier. This will be filled only when tagged VLAN is applied. Valid range is 1 ~ 4094.
Alias:	MAC alias name you assign.

2.4.3 Static Forward

Function Name:

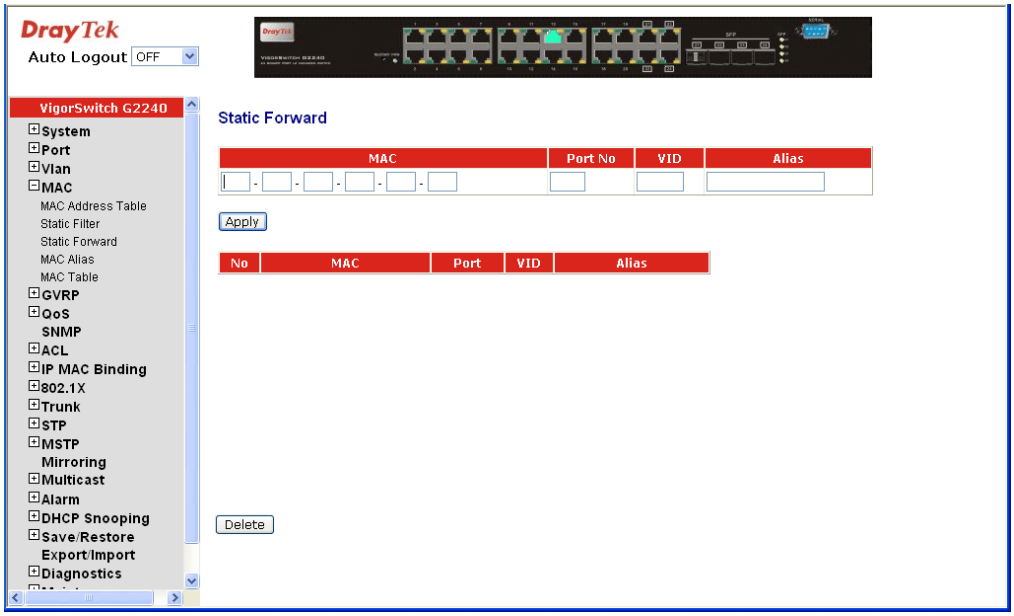
Static Forward

Function Description:

Static Forward is a function that allows the user in the static forward table to access a specified port of the switch. Static Forward table associated with a specified port of a switch is set up by manually inputting MAC address and its alias name.

When 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.

For adding a MAC address entry in the allowed table, you just need to fill in four parameters: MAC address, associated port, VID and Alias. Just select the existed MAC address entry you want and click **<Delete>** button, you also can remove it.



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
Port No:	Port number of the switch. It is 1 ~24.
VID:	VLAN identifier. This will be filled only when tagged VLAN is applied. Valid range is 1 ~ 4094.
Alias:	MAC alias name you assign.

2.4.4 MAC Alias

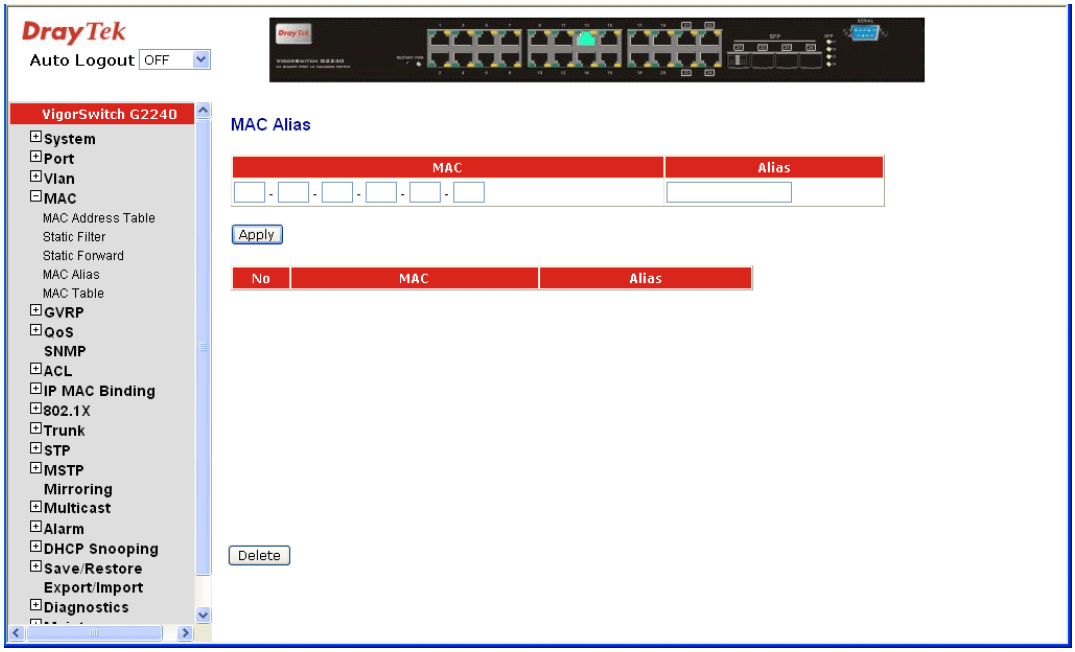
Function name:

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.



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.

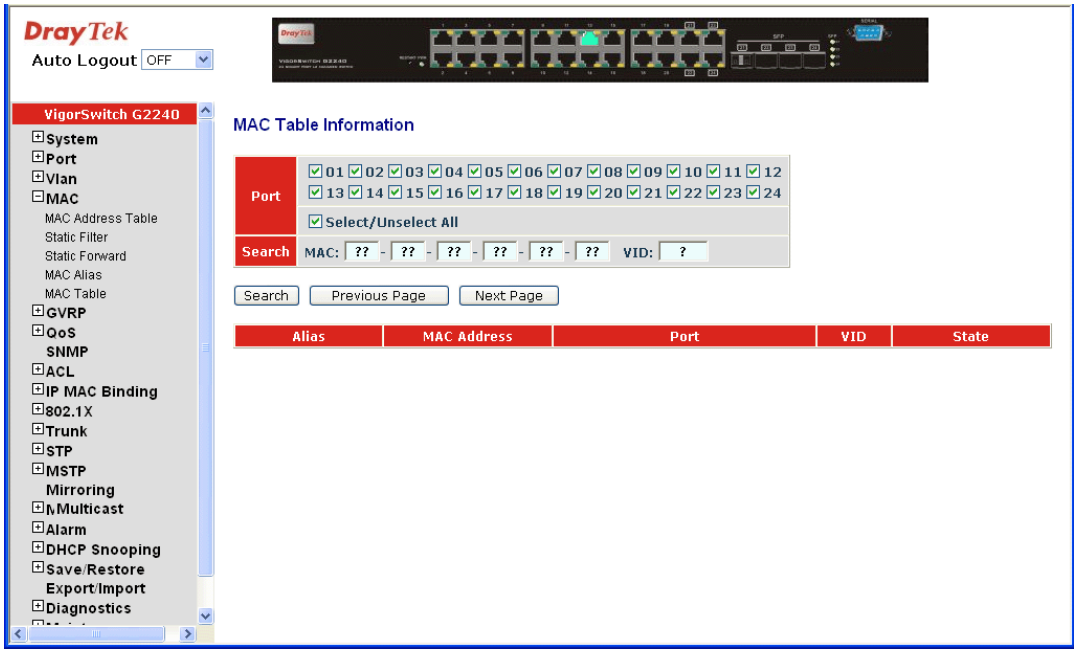
2.4.5 MAC Table

Function name:

MAC Table

Function description:

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



Parameters description:

Port:	The port that exists in the searched MAC Entry.
Search:	Find the specific MAC address what you input for search.
Previous Page:	Move to the previous page.
Next Page:	Move to the next page.

2.5

2.5 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.

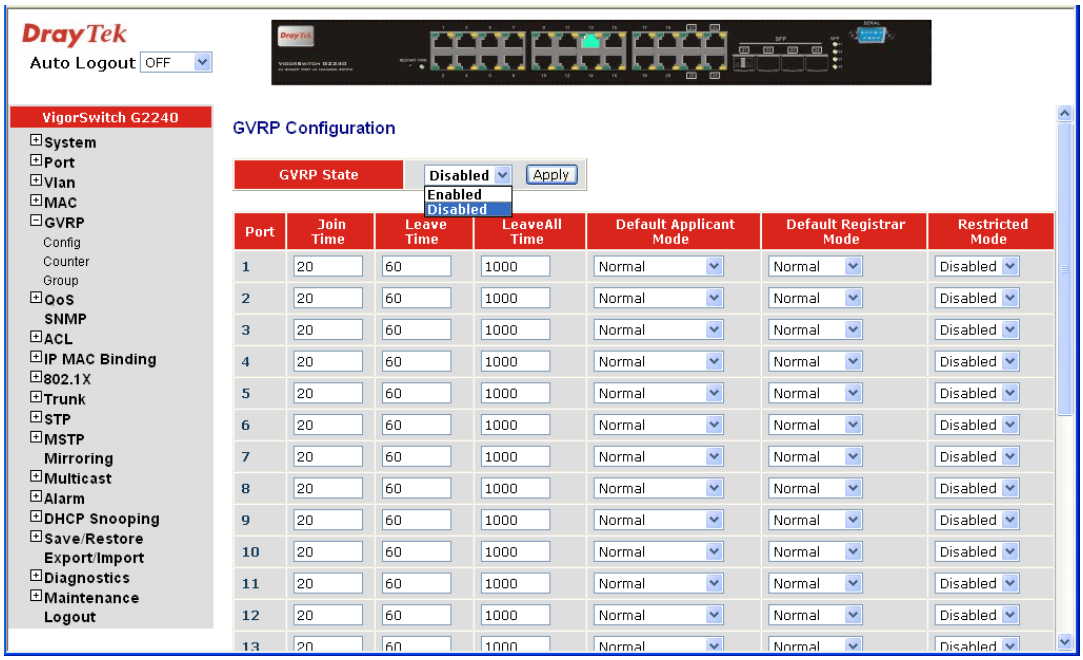
2.5.1 GVRP Config

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.



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.

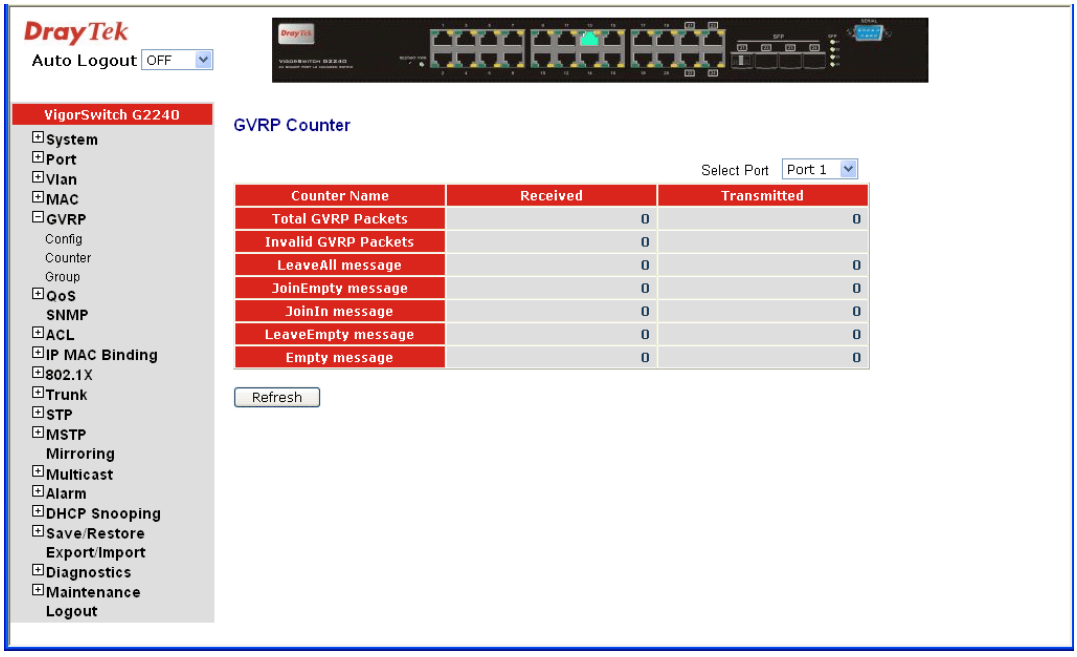
2.5.2 Counter

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.



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.

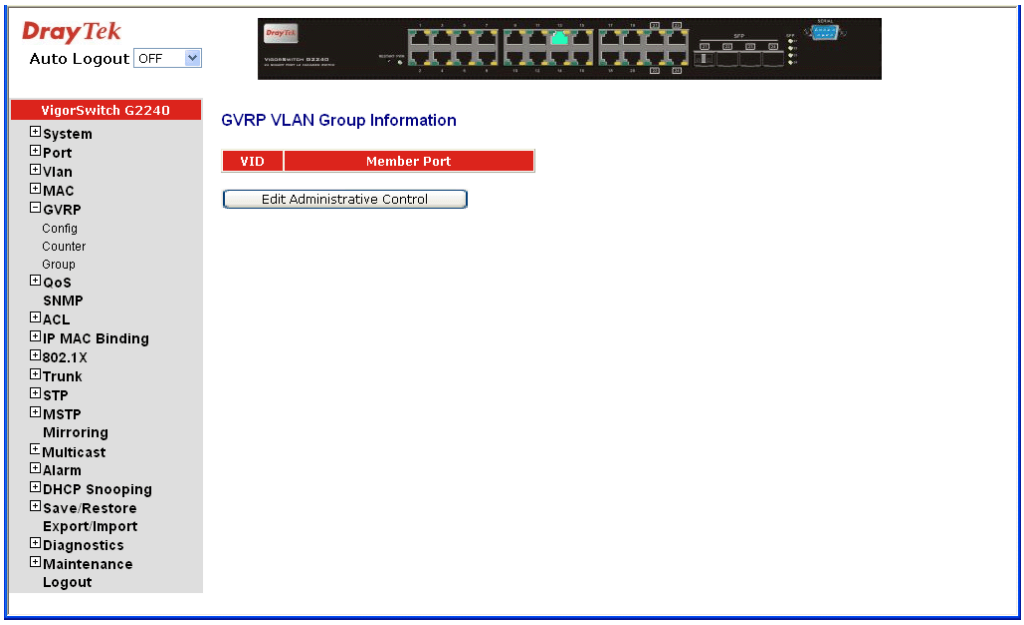
2.5.3 Group

Function name:

GVRP VLAN Group Information

Function description:

Show the dynamic group member and their information.



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.

2.6 QoS (Quality of Service) Configuration

The switch support four QoS queues per port with strict or weighted fair queuing scheduling. There are 24 QoS Control Lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP and UDP/TCP ports and ranges.

High flexibility in the classification of incoming frames to a QoS class. The QoS classification looks for information up to Layer 4, including IPv4 and IPv6 DSCP, IPv4 TCP/UDP port numbers, and user priority of tagged frames. This QoS classification mechanism is implemented in a QoS control list (QCL). The QoS class assigned to a frame is used throughout the device for providing queuing, scheduling, and congestion control guarantees to the frame according to what was configured for that specific QoS class.

The switch supports advanced memory control mechanisms providing excellent performance of all QoS classes under any traffic scenario, including jumbo frame, a super priority queue with dedicated memory and strict highest priority in the arbitration. The ingress super priority queue allows traffic recognized as CPU traffic to be received and queued for transmission to the CPU even when all the QoS class queues are congested.

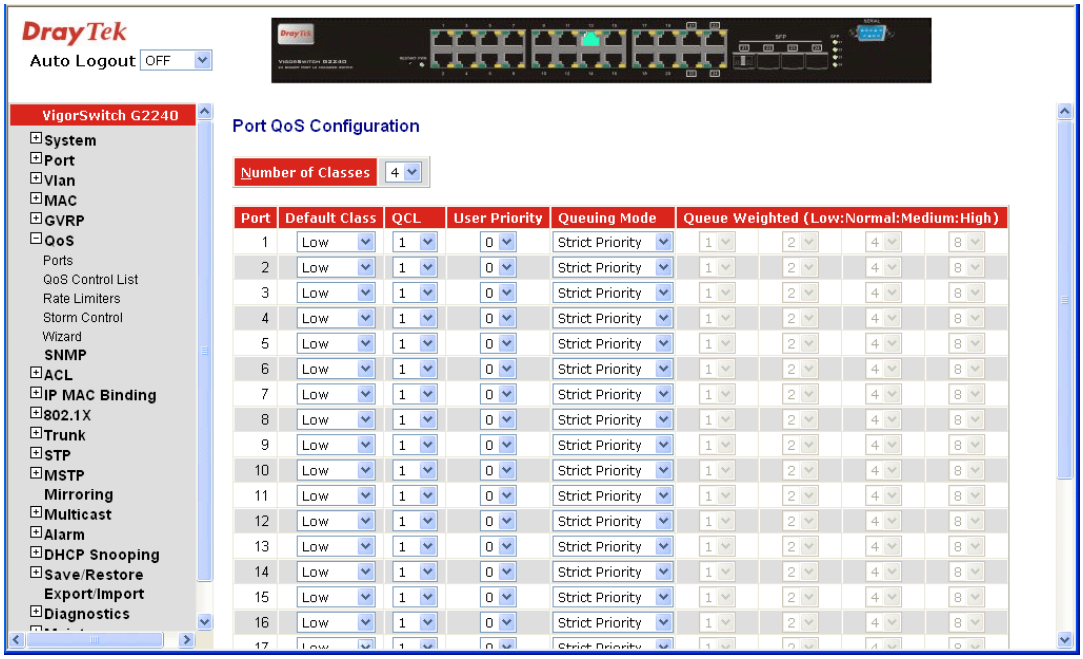
2.6.1 Ports

Function name:

Port QoS Configuration

Function description:

Configure each port QoS behavior. Four QoS queue per port with strict or weighted fair queuing scheduling. There are 24 QoS Control Lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP and UDP/TCP ports and ranges.



Parameter description:

Number of Classes:	1 / 2 / 4
Port:	User can choose the port (1~24) respectively with Priority Class on Per Port Priority function.
Default Class:	User can set up High Priority or Low Priority for each port respectively. Low / Normal / Medium / High
QCL:	The number of QCL rule 1~24, each port have to apply one of the QCL rule for QoS behavior
User Priority:	The user priority value 0~7 (3 bits) is used as an index to the eight QoS class values for VLAN tagged or priority tagged frames.
Queuing Mode:	There are two Scheduling Method, Strict Priority and Weighted Fair. Default is Strict Priority. After you choose any of Scheduling Method, please click Apply button to be in operation.
Queue Weighted:	There are four queues per port and four classes weighted number (1 / 2 / 4 / 8) for each queues, you can select the weighted number when the scheduling method be set to “Weighted Fair” mode.

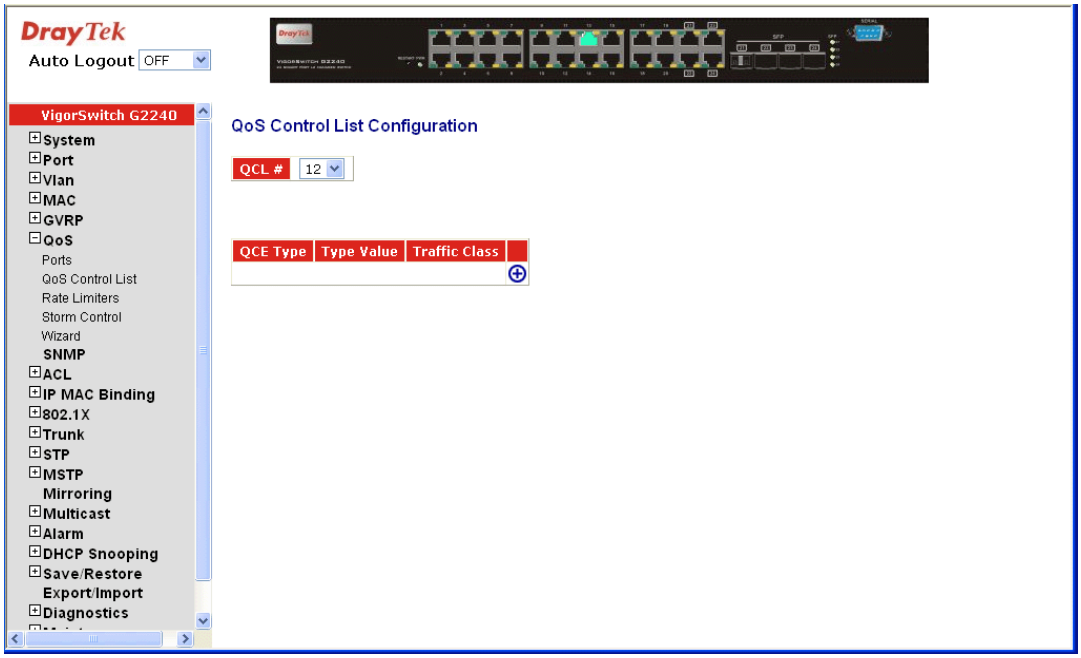
2.6.2 Qos Control List

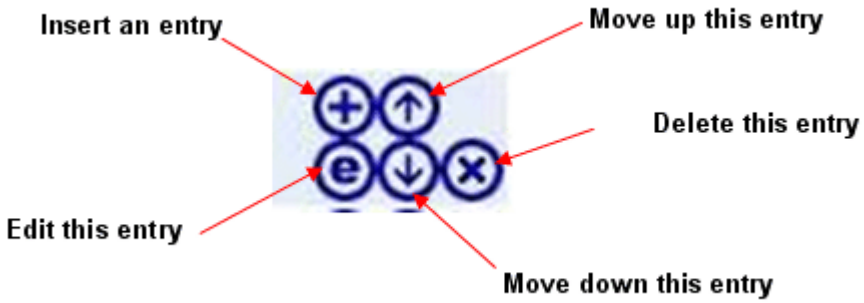
Function name:

Qos Control List Configuration

Function description:

The switch supports four QoS queues per port with strict or weighted fair queuing scheduling. There are 24 QoS Control Lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ether Type, VID, IPv4/IPv6 DSCP and UDP/TCP ports and ranges.





Parameter description:

QCL#: QCL number : 1~24

QCE Type: Ethernet Type / VLAN ID / UDP/TCP Port / DSCP / ToS / Tag Priority

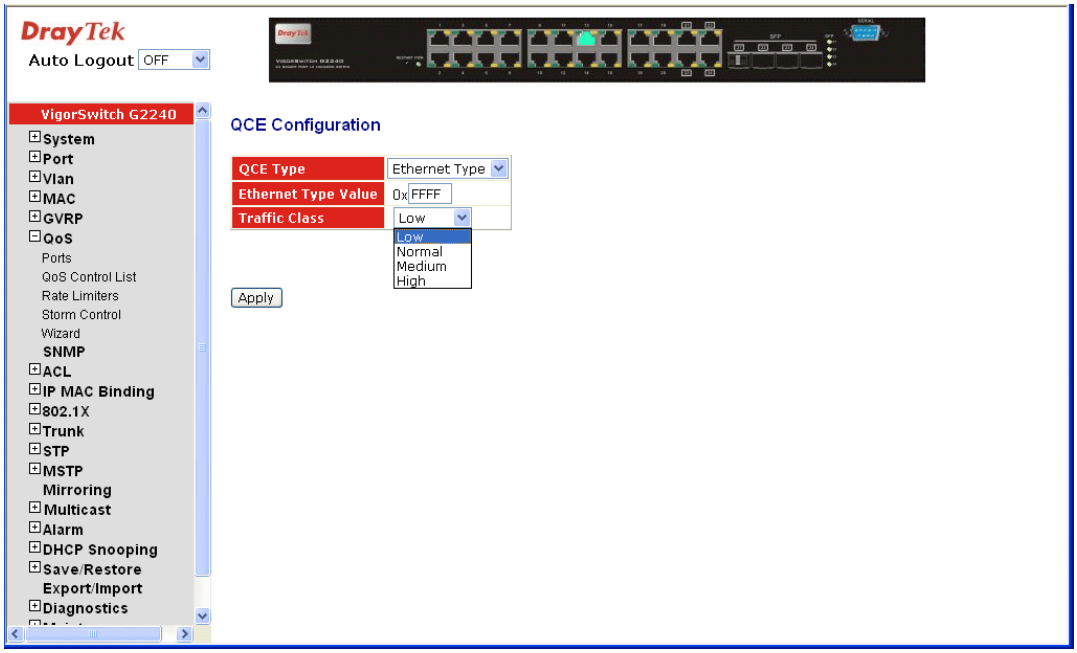
Ethernet Type Value: The configurable range is 0x600~0xFFFF. Well known protocols already assigned EtherType values. The commonly used values in the EtherType field and corresponding protocols are listed below:

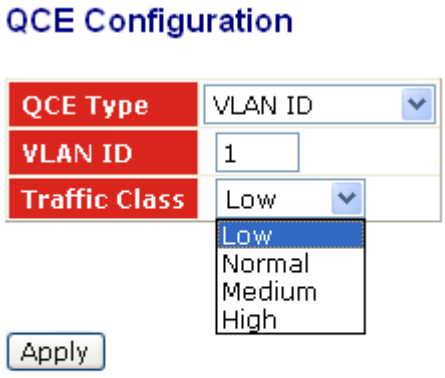
Ethertype (Hexadecimal)	Protocol
0x0800	IP, Internet Protocol
0x0801	X.75 Internet
0x0802	NBS Internet
0x0803	ECMA Internet

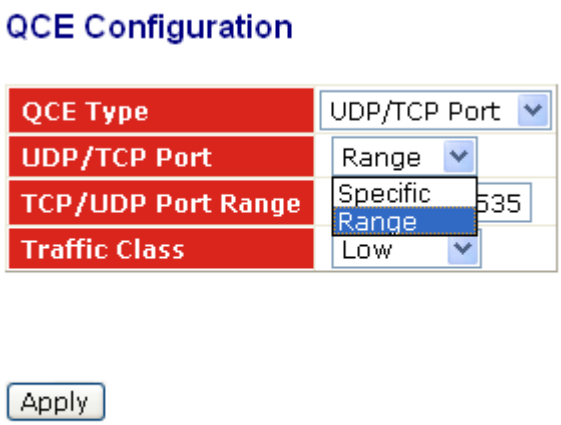
0x0804	Chaosnet
0x0805	X.25 Level 3
0x0806	ARP, Address Resolution Protocol.
0x0808	Frame Relay ARP [RFC1701]
0x6559	Raw Frame Relay [RFC1701]
0x8035	DRARP, Dynamic RARP. RARP, Reverse Address Resolution Protocol.
0x8037	Novell Netware IPX
0x809B	EtherTalk (AppleTalk over Ethernet)
0x80D5	IBM SNA Services over Ethernet
0x 80F3	AARP, AppleTalk Address Resolution Protocol.
0x8100	IEEE Std 802.1Q - Customer VLAN Tag Type.
0x8137	IPX, Internet Packet Exchange.
0x 814C	SNMP, Simple Network Management Protocol.
0x86DD	IPv6, Internet Protocol version 6.
0x880B	PPP, Point-to-Point Protocol.
0x 880C	GSMP, General Switch Management Protocol.
0x8847	MPLS, Multi-Protocol Label Switching (unicast).
0x8848	MPLS, Multi-Protocol Label Switching (multicast).
0x8863	PPPoE, PPP Over Ethernet (Discovery Stage).
0x8864	PPPoE, PPP Over Ethernet (PPP Session Stage).
0x88BB	LWAPP, Light Weight Access Point Protocol.
0x88CC	LLDP, Link Layer Discovery Protocol.
0x8E88	EAPOL, EAP over LAN.
0x9000	Loopback (Configuration Test Protocol)
0xFFFF	reserved.

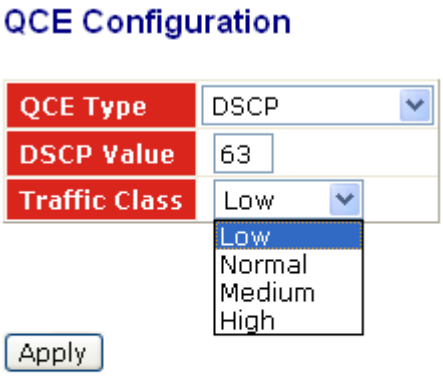
QCE Configuration

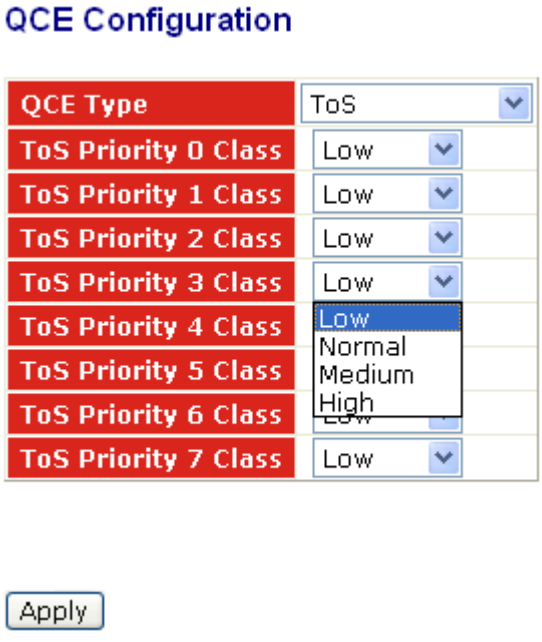
The QCL consists of several QoS Control Entries (QCEs) that are searched from the top of the list to the bottom of the list for a match. The first matching QCE determines the QoS classification of the frame. The QCE ordering is therefore important for the resulting QoS classification algorithm. If no matching QCE is found, the default QoS class is used in the port QoS configuration.

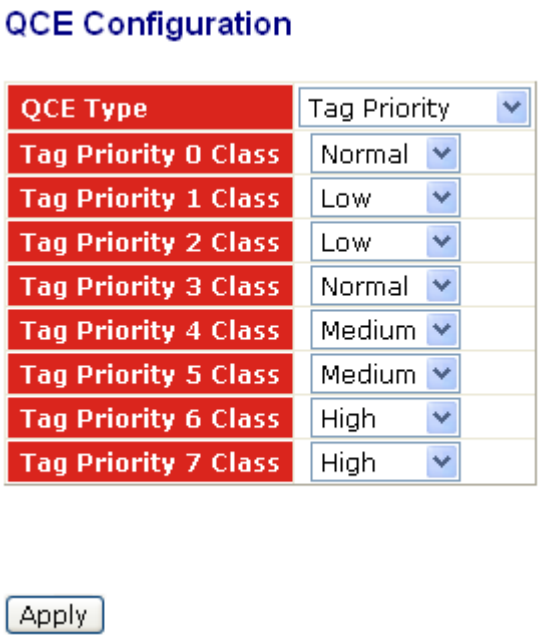

DrayTek
Auto Logout OFF
VigorSwitch G2240
System
Port
Vlan
MAC
GVRP
QoS
Ports
QoS Control List
Rate Limiters
Storm Control
Wizard
SNMP
ACL
IP MAC Binding
802.1X
Trunk
STP
MSTP
Mirroring
Multicast
Alarm
DHCP Snooping
Save/Restore
Export/Import
Diagnostics
QCE Configuration
QCE Type
Ethernet Type
Ethernet Type Value
0x FFFF
Traffic Class
Low
Low
Normal
Medium
High
Apply


QCE Configuration
QCE Type
VLAN ID
VLAN ID
1
Traffic Class
Low
Low
Normal
Medium
High
Apply


QCE Configuration
QCE Type
UDP/TCP Port
UDP/TCP Port
Range
TCP/UDP Port Range
Specific
Range
535
Traffic Class
Low
Apply


QCE Configuration
QCE Type
DSCP
DSCP Value
63
Traffic Class
Low
Low
Normal
Medium
High
Apply


QCE Configuration
QCE Type
ToS
ToS Priority 0 Class
ToS Priority 1 Class
ToS Priority 2 Class
ToS Priority 3 Class
ToS Priority 4 Class
ToS Priority 5 Class
ToS Priority 6 Class
ToS Priority 7 Class
Low
Low
Normal
Medium
High
Apply



Parameter description:

VLAN ID:	The configurable VID range:1~4094
UDP/TCP Port:	To select the UDP/TCP port classification method by Range or Specific.
UDP/TCP Port Range:	The configurable ports range: 0~65535 You can refer to following UDP/TCP port-numbers information. http://www.iana.org/assignments/port-numbers
UDP/TCP Port No.:	The configurable specific port value: 0~65535
DSCP Value:	The configurable DSCP value: 0~63
Traffic Class:	Low / Normal / Medium / High

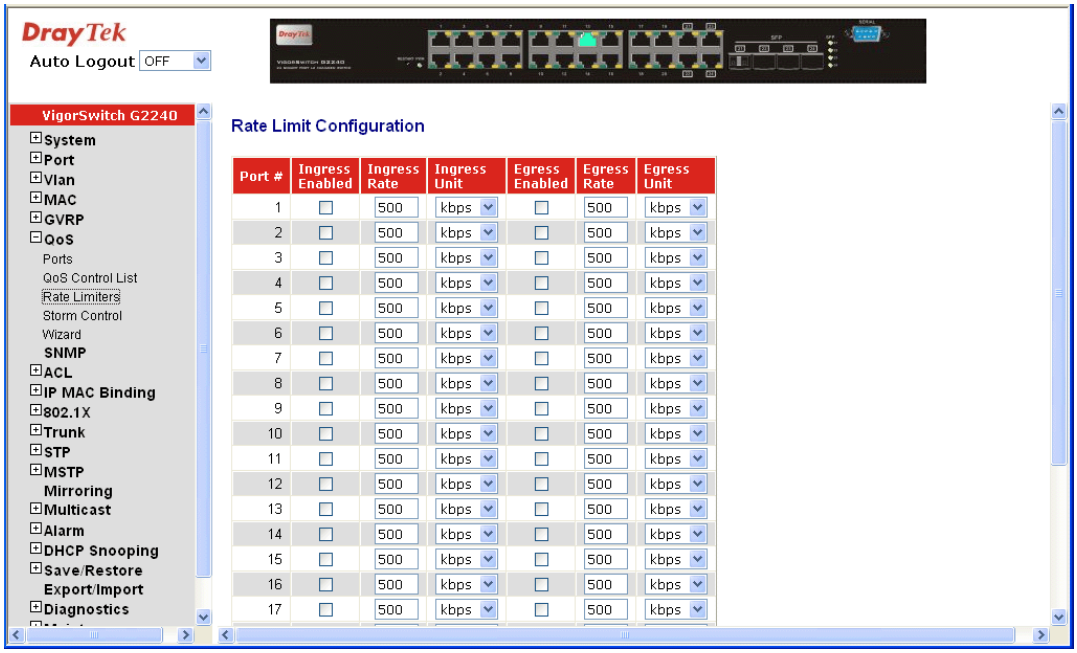
2.6.3 Rate Limiters

Function name:

Rate Limit Configuration

Function description:

Each port includes an ingress policer, and an egress shaper, which can limit the bandwidth of received and transmitted frames. Ingress policer or egress shaper operation is controlled per port in the Rate Limit Configuration.



Parameter description:

Port #:	Port number.
Ingress Enabled:	Ingress enabled to limit ingress bandwidth by ingress rate.
Ingress Rate:	The configurable ingress rate range: 500 Kbps ~ 1000000 Kbps |1 Mbps ~ 1000 Mbps
Ingress Unit:	There are two units for ingress rate limit: kbps / Mbps
Egress Enabled:	Shaper enabled to limit egress bandwidth by egress rate.
Egress Rate:	The configurable shaper rate range: 500 Kbps ~ 1000000 Kbps 1 Mbps ~ 1000 Mbps
Egress Unit:	There are two units for egress shaper rate limit: kbps / Mbps

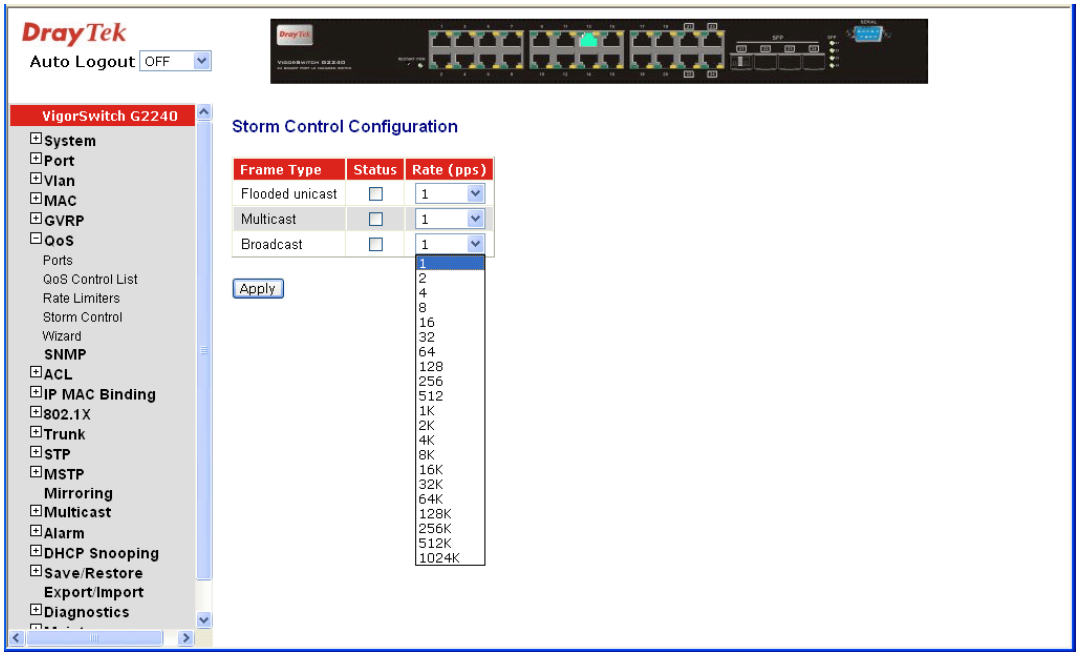
2.6.4 Storm Control

Function name:

Storm Control Configuration

Function description:

The switch support storm ingress control function to limit the Flooded, Multicast and Broadcast to prevent storm event happen.



Parameter description:

Port #:	Port number.
Frame Type:	There three frame types of storm can be controlled: Flooded unicast / Multicast / Broadcast.
Status:	The function means to enable the frame type for Storm control.
Rate (pps):	Refer to the following rate configurable value list, the unit is Packet Per Second (pps). 1 / 2 / 4 / 8 / 16 / 32 / 64 / 128 / 256 / 512 / 1K / 2K / 4K / 8K / 16K / 32K / 64K / 128K / 256K / 512K / 1024K

2.6.5 Wizard

Function name:

Wizard

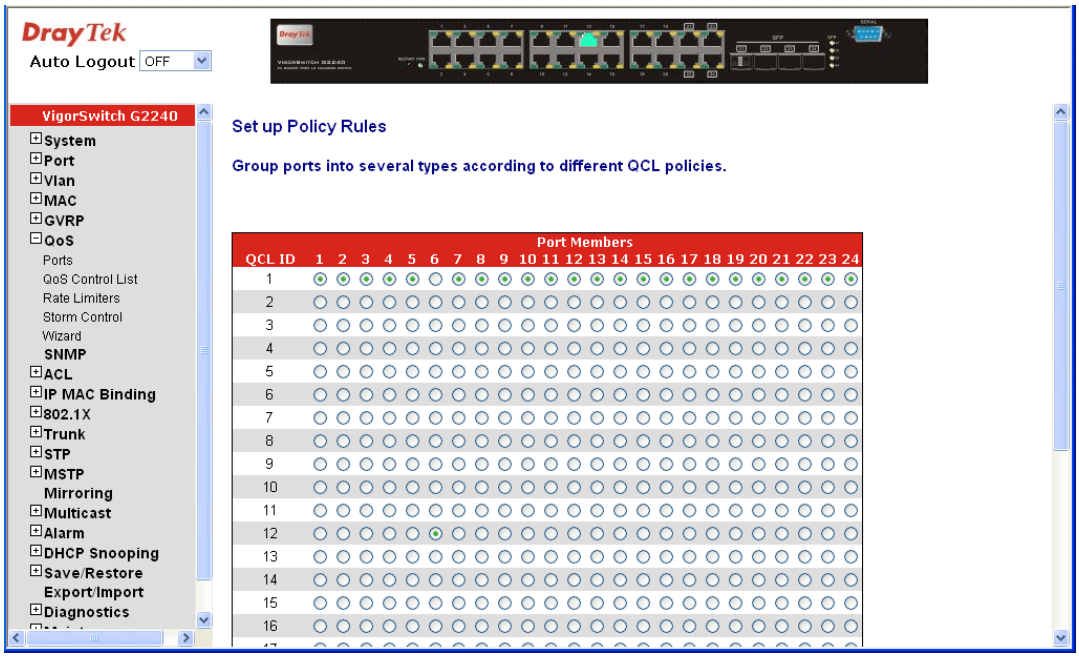
Function description:

The QCL configuration Wizard is targeted on user can easy to configure the QCL rules for QoS configuration. The wizard provide the typical network application rules, user can apply these application easily.

Parameter description:

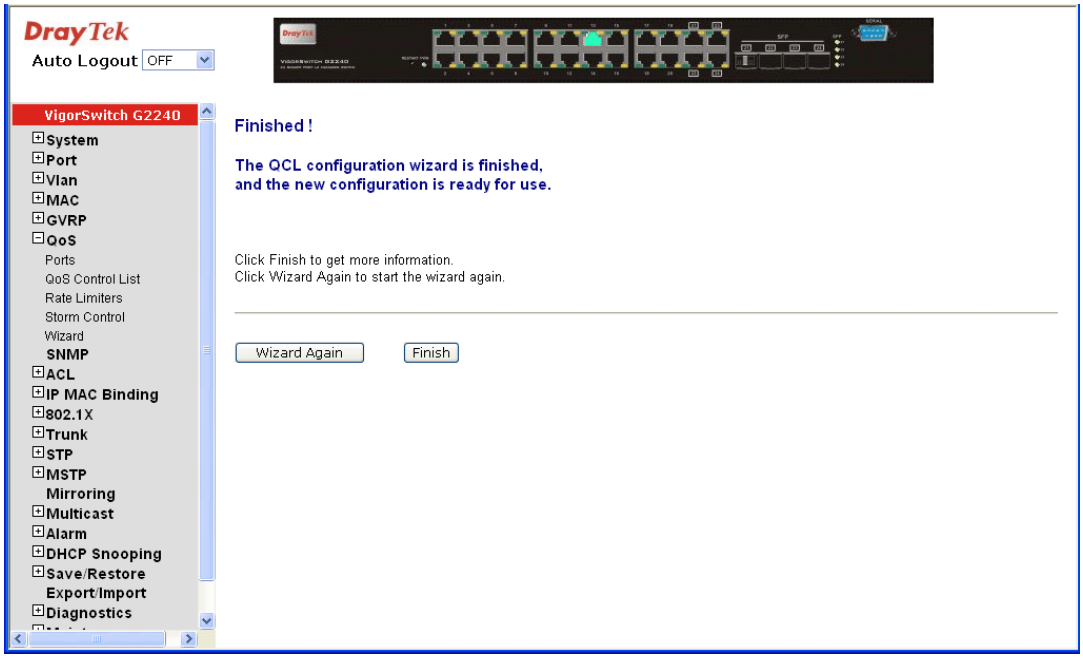
Please select an Action:	User need to select one of action from following items, then click on <Next> to finish QCL configuration: ● Set up Port Policies ● Set up Typical Network Application Rules ● Set up TOS Precedence Mapping ● Set up VLAN Tag Priority Mapping
Next:	Go to next step.
Cancel:	Abort current configuration back to previous step.
Back:	Back to previous screen.

- **Set up Port Policies**

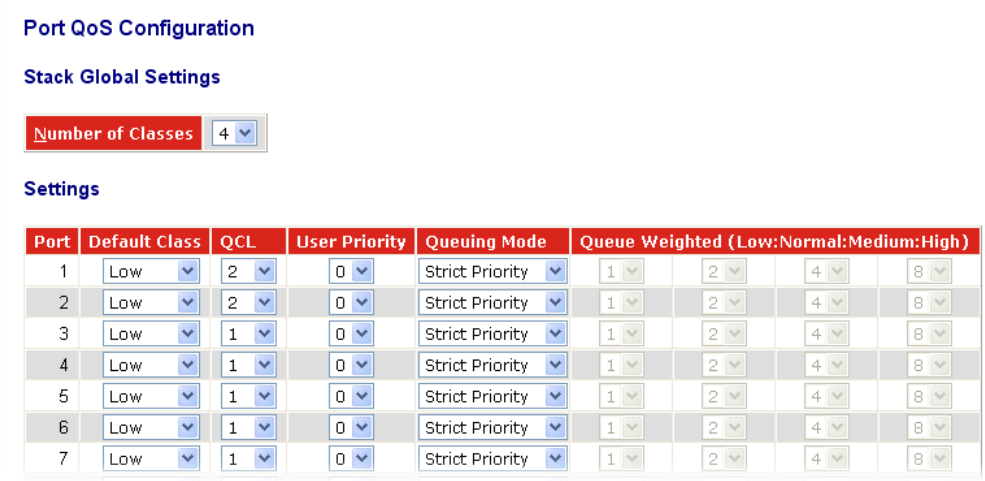


Parameter description:

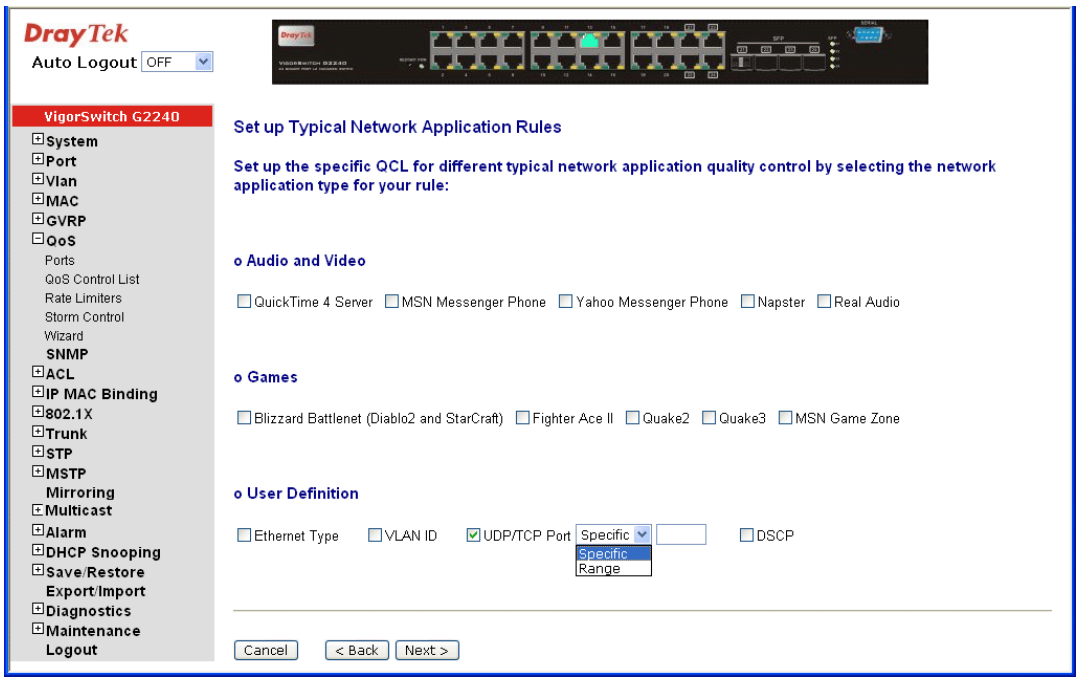
QCL ID:	QoS Control List (QCL): 1~24
Port Member:	Port Member: 1~24
Next:	Go to next step.
Cancel:	Abort current configuration back to previous step.
Back:	Back to previous screen.



Wizard Again:	Click on the <Wizard Again>, back to QCL Configuration Wizard.
Finish:	When you click on <Finish>, the parameters will be set according to the wizard configuration and shown on the screen, then ask you to click on <Apply> for changed parameters confirmation.

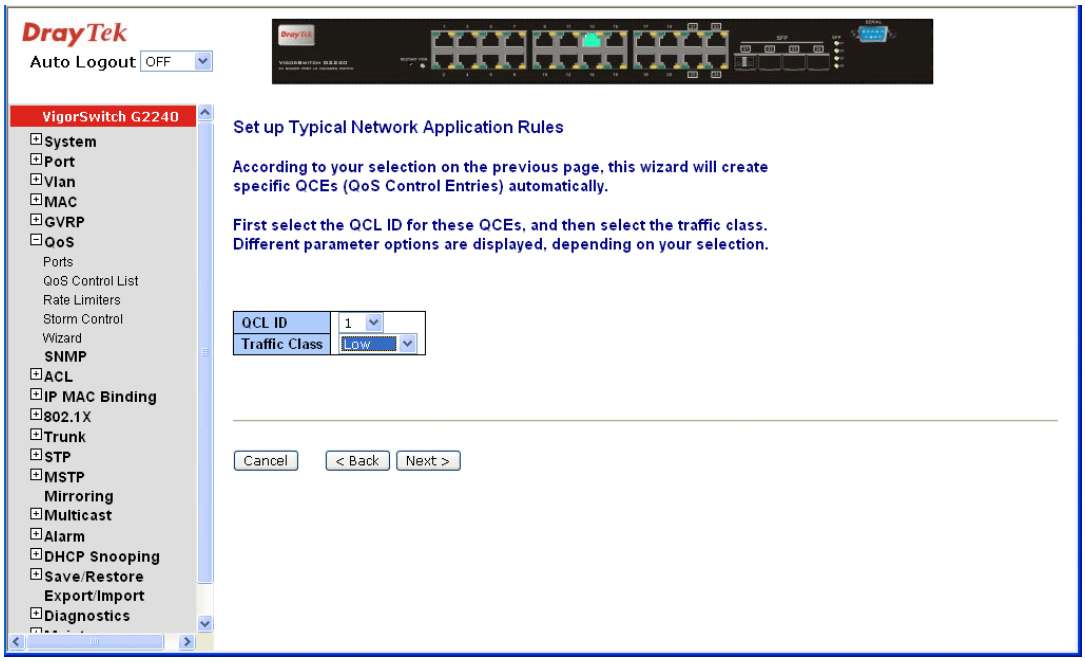


- **Set up Typical Network Application Rules**

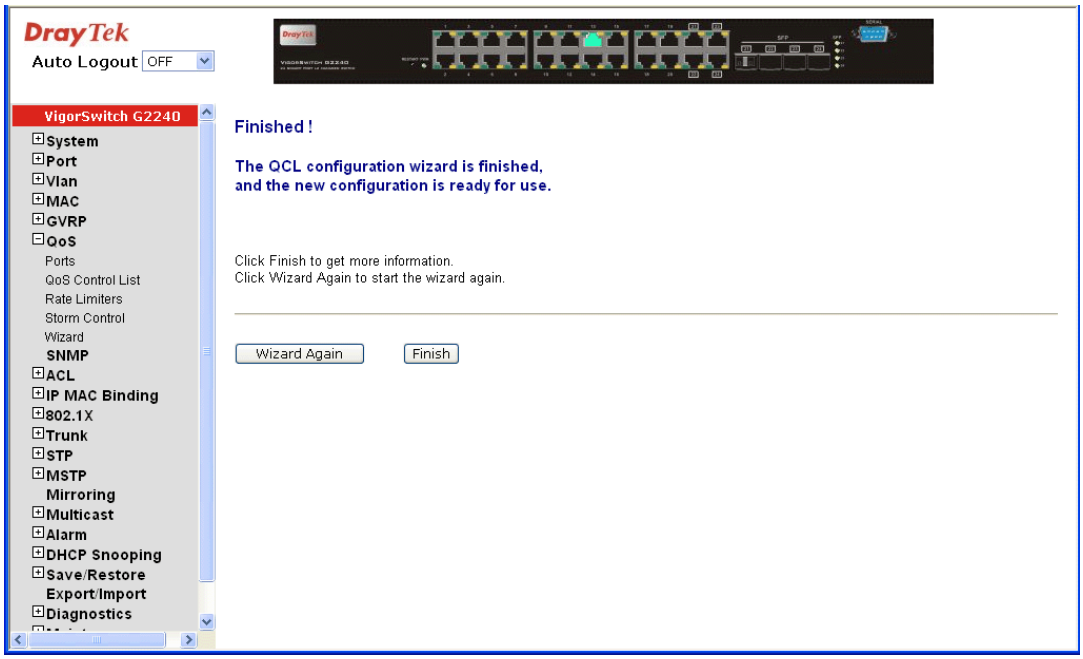


Parameter description:

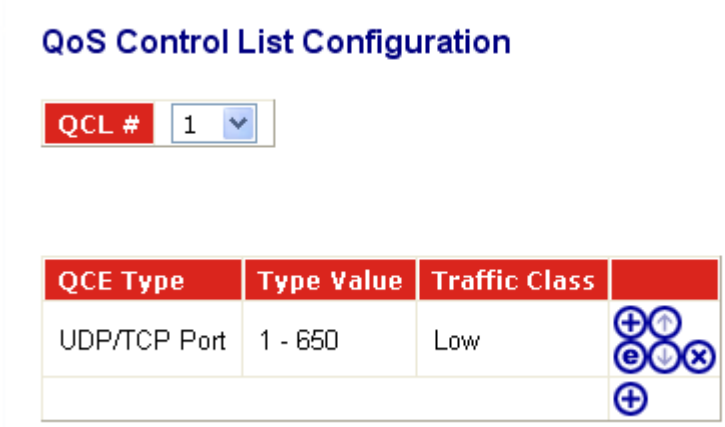
Audio and Video:	QuickTime 4 Server / MSN Messenger Phone / Yahoo Messenger Phone / Napster / Real Audio
Games:	Blizzard Battlenet (Diablo2 and StarCraft) / Fighter Ace II / Quake2 / Quake3 / MSN Game Zone
User Definition:	Ethernet Type / VLAN ID / UDP/TCP Port / DSCP
	Ethernet Type Value: Type Range: 0x600~0xFFFF
	VLAN ID: VLAN ID Range: 1~4094
	UDP/TCP Port: Two Mode: Range / Specific
	UDP/TCP Port Range: Port Range: 0~65535
	UDP/TCP Port No.: Port Range: 0~65535
	DSCP Value: DSCP Value Range: 0~63
Next:	Go to next step.
Cancel:	Abort current configuration back to previous step.
Back:	Back to previous screen.



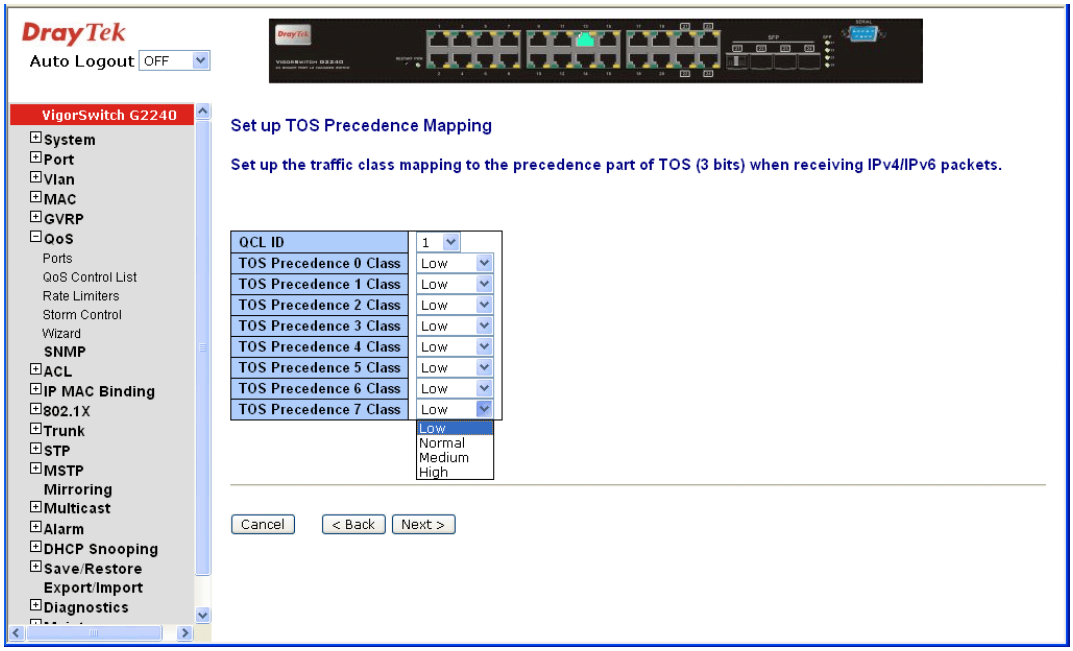
QCL ID:	QCL ID Range: 1~24
Traffic Class:	There are four classes: Low / Normal / Medium / High
Next:	Go to next step.
Cancel:	Abort current configuration back to previous step.
Back:	Back to previous screen.



Wizard Again:	Click on the <Wizard Again>, back to QCL Configuration Wizard.
Finish:	When you click on <Finish>, the parameters will be set according to the wizard configuration and shown on the screen, then ask you to click on <Apply> for changed parameters confirmation.

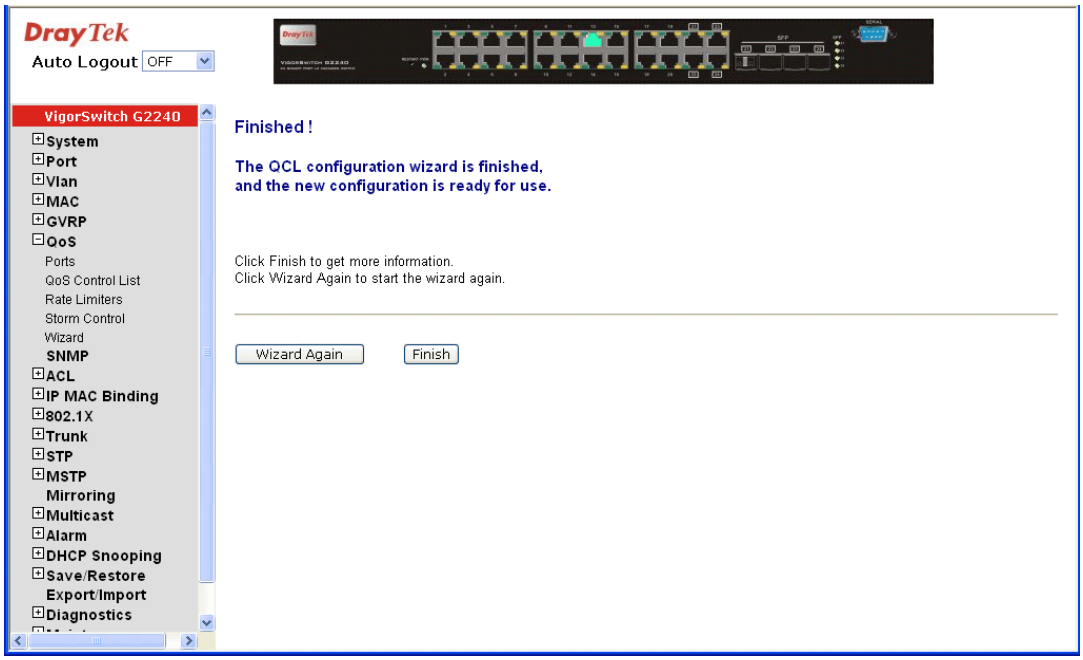


- **Set up TOS Precedence Mapping**



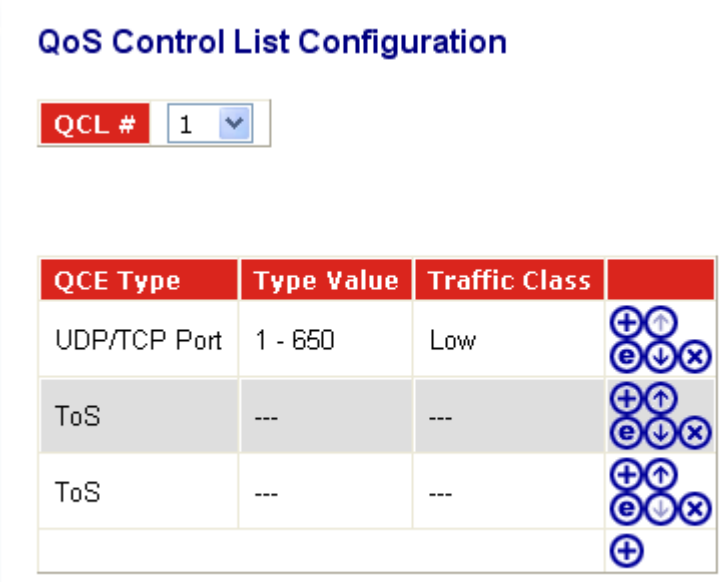
Parameter description:

QCL ID:	QoS Control List (QCL): 1~24
TOS Precedence 0~7 Class:	Low / Normal / Medium / High
Next:	Go to next step.
Cancel:	Abort current configuration back to previous step.
Back:	Back to previous screen.

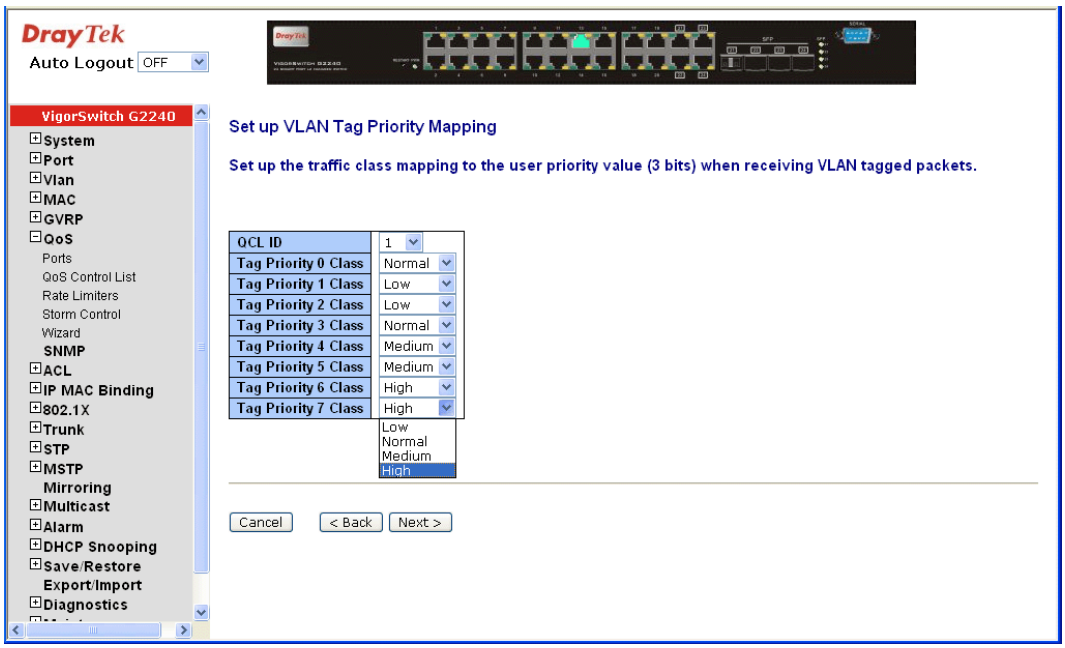


Wizard Again: Click on the <Wizard Again>, back to QCL Configuration Wizard.

Finish: When you click on <Finish>, the parameters will be set according to the wizard configuration and shown on the screen, then ask you to click on <Apply> for changed parameters confirmation.

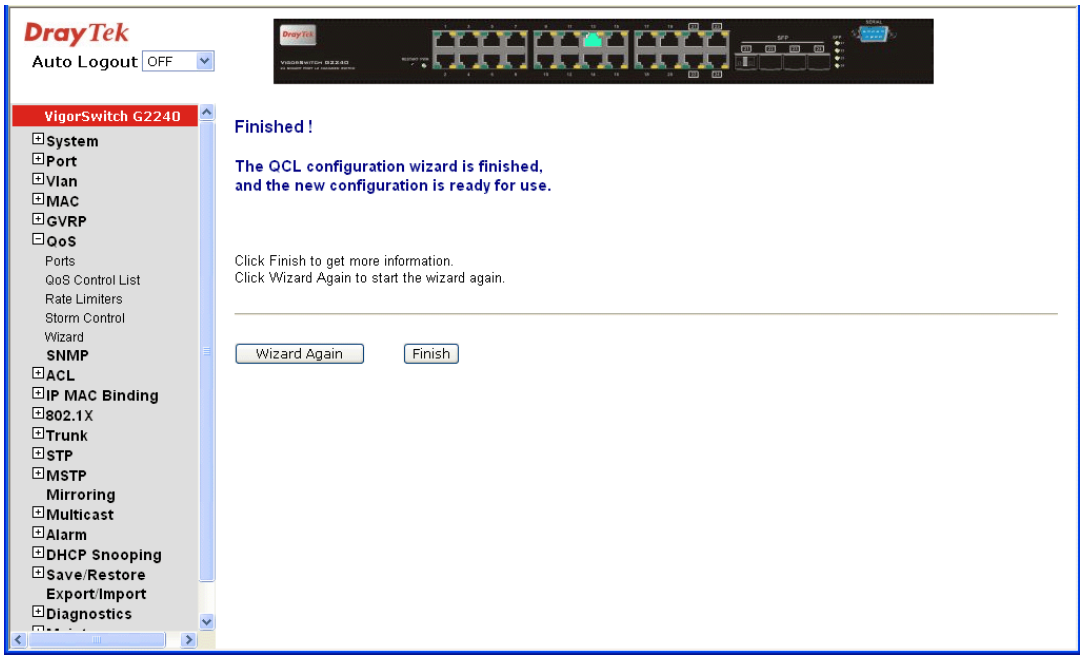


- **Set up VLAN Tag Priority Mapping**



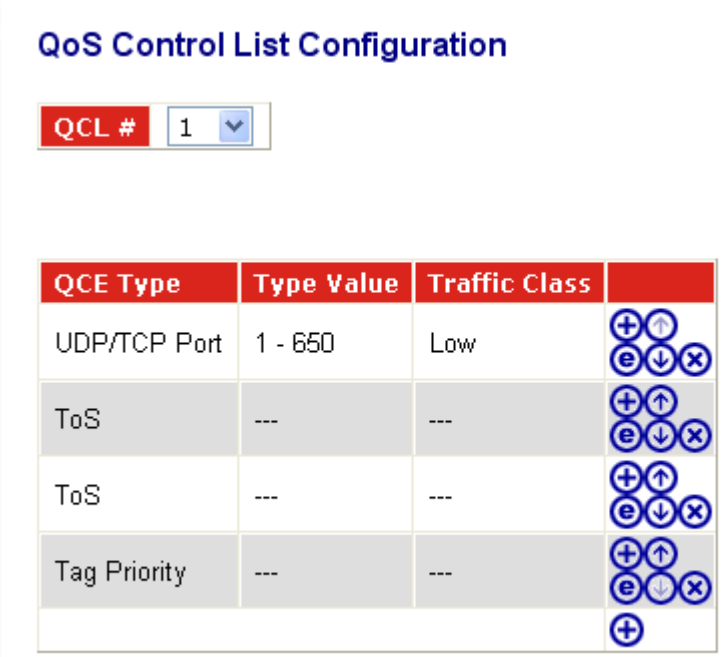
Parameter description:

QCL ID:	QoS Control List (QCL): 1~24
Tag Priority 0~7 Class:	Low / Normal / Medium / High
Next:	Go to next step.
Cancel:	Abort current configuration back to previous step.
Back:	Back to previous screen.



Wizard Again:	Click on the <Wizard Again>, back to QCL Configuration Wizard.
Finish:	When you click on <Finish>, the parameters will be set according to the wizard configuration and shown on the

screen, then ask you to click on <Apply> for changed parameters confirmation.



2.7 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.

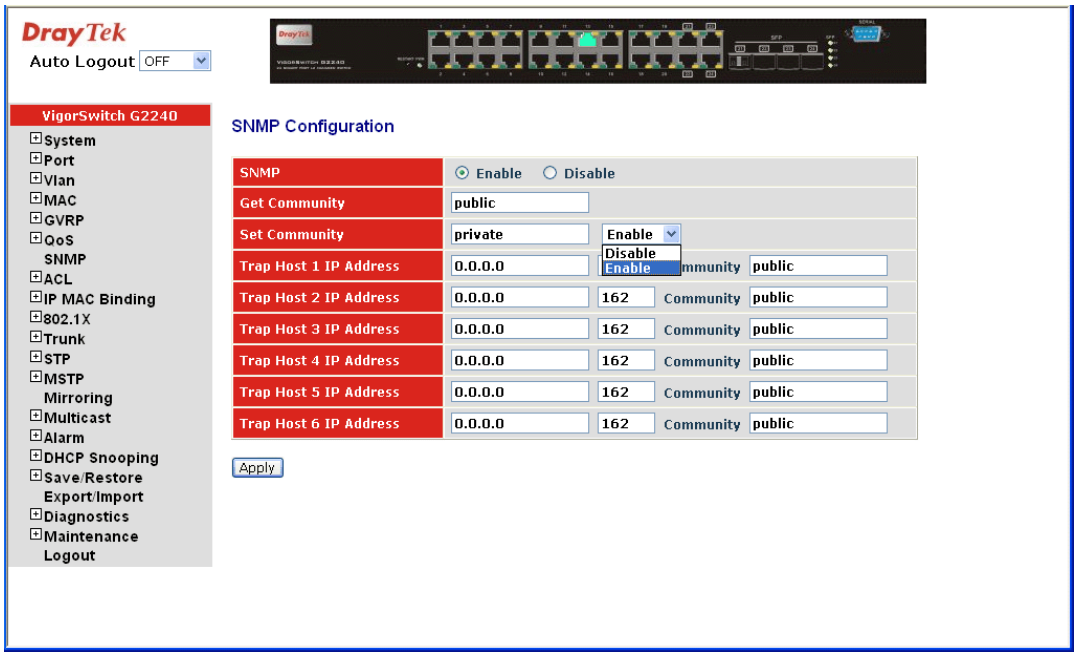
Basically, it is passive except issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP “Enable”, SNMP agent will be started up. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set “Disable”, 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.



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.

2.8 ACL

The 24 Gigabit L2 Managed Switch access control list (ACL) is probably the most commonly used object in the IOS. It is used for packet filtering but also for selecting types of traffic to be analyzed, forwarded, or influenced in some way.

The ACLs are divided into EtherTypes. IPv4, ARP protocol, MAC and VLAN parameters etc. Here we will just go over the standard and extended access lists for TCP/IP. As you create ACEs for ingress classification, you can assign a policy for each port, the policy number is 1-8, however, each policy can be applied to any port. This makes it very easy to determine what type of ACL policy you will be working with.

2.8.1 Ports

Function name:

ACL Ports Configuration

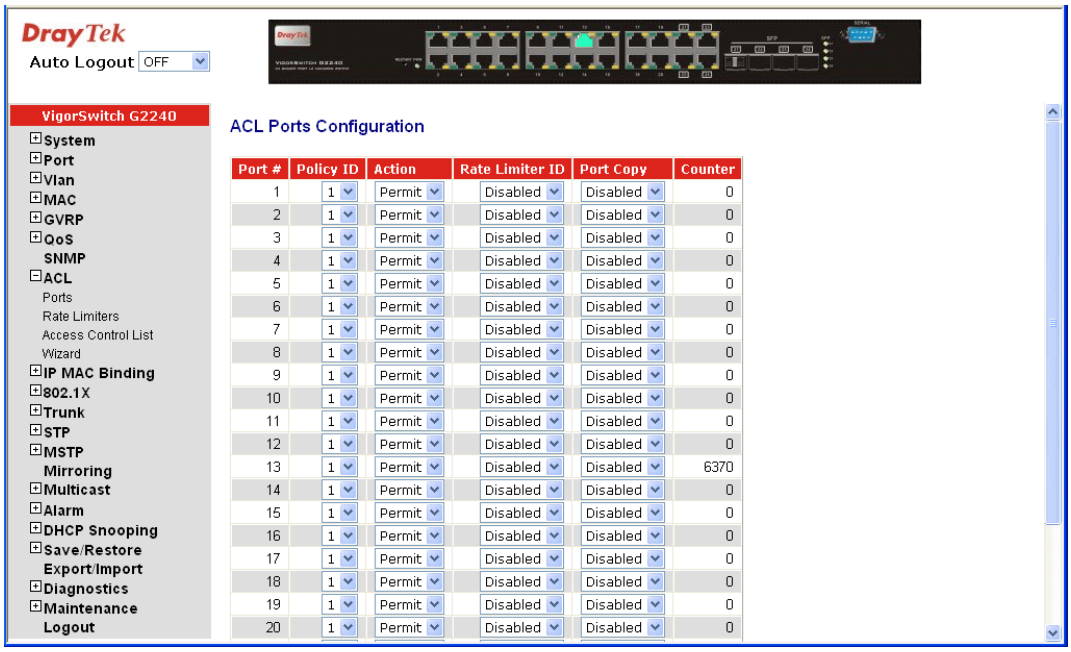
Function description:

The switch ACL function support up to 128 Access Control Entries (ACEs), using the shared 128 ACEs for ingress classification. You can create an ACE and assign this ACE for each port with <Any> or assign this ACE for a policy or assign this ACE for a port. There are 8 policies, each port can select one of policy, then decides which of the following actions would take according to the packet's IPv4, EtherType, ARP Protocol, MAC Parameters and VLAN parameters:

Packet Deny or Permit

Rate Limiter (Unit: pps)

Port Copy (1 – 24)



Parameters description:

Port #:	Port number: 1~24
Policy ID:	Policy ID range: 1~8
Action:	Permit or Deny forwarding the met ACL packets
Rate Limiter ID:	Disabled: Disable Rate Limitation Rate Limiter ID Range: 1~16. To select one of rate limiter ID for this port, it will limit met ACL packets by rate limiter ID configuration.
Port Copy:	Disabled: Disable to copy the met ACL packets to specific port Port number: 1~24. Copy the met ACL packets to the selected port
Counter:	The counter will increase from initial value 0, when this port received one of the met ACL packet the counter value will increase +1

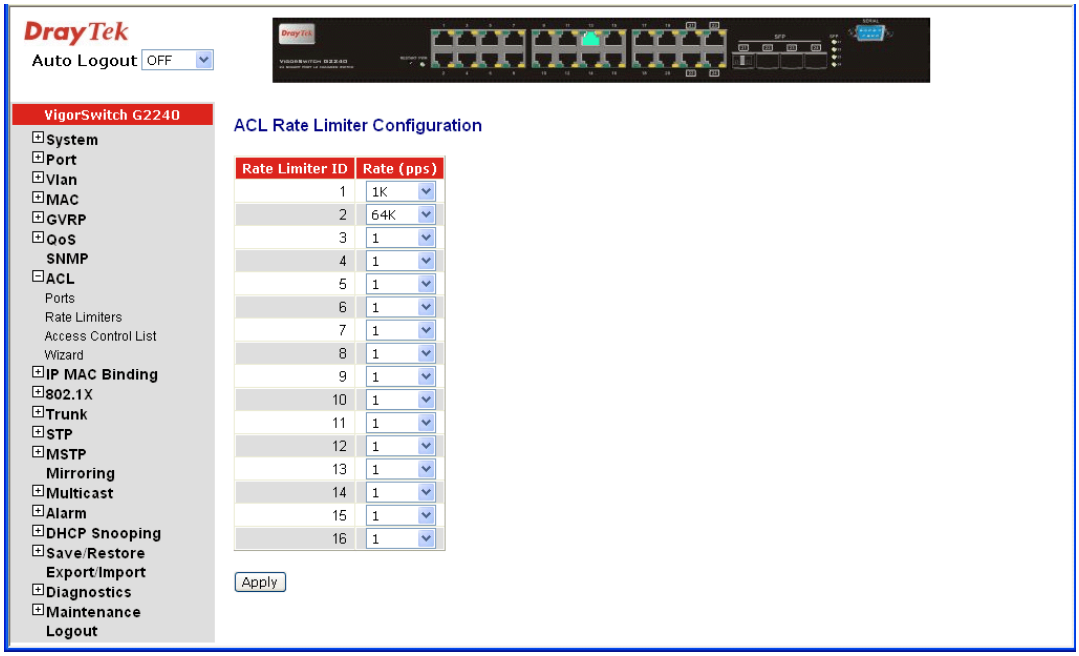
2.8.2 Rate Limiters

Function name:

ACL Rate Limiter Configuration

Function description:

There are 16 rate limiter IDs. You can assign one of the limiter ID for each port. The rate limit configuration unit is Packet Per Second (pps).



Parameters description:

Rate Limiter ID: ID Range: 1~16

Rate(pps): 1 / 2 / 4 / 8 / 16 / 32 / 64 / 128 / 256 / 512 / 1K / 2K / 4K / 8K / 16K / 32K / 64K / 128K / 256K / 512K / 1024K

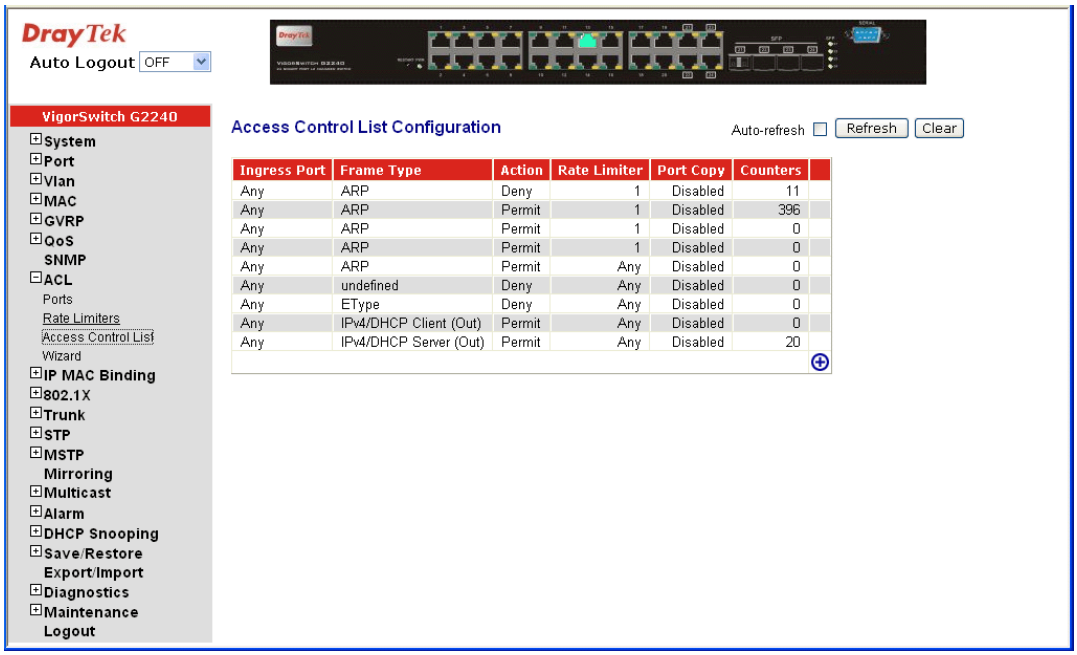
2.8.3 Access Control List

Function name:

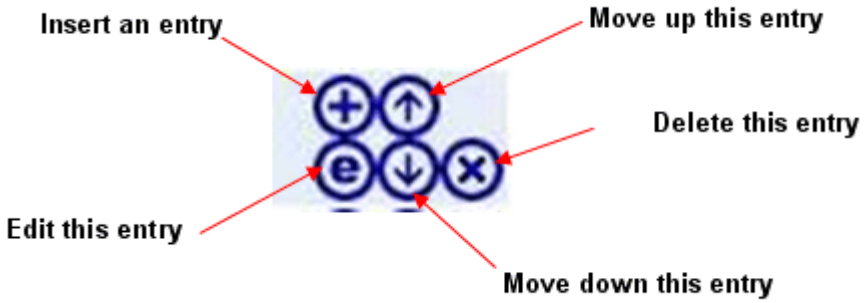
ACL Control List Configuration

Function description:

The switch ACL function support up to 128 Access Control Entries (ACEs), using the shared 128 ACEs for ingress classification. You can create an ACE and assign this ACE for each port with <Any> or assign this ACE for a policy or assign this ACE for a port. There are 8 policies, each port can select one of policy, then decides which of the Permit/Deny, Rate Limitation and Port Copy actions would take according to the ACL configuration packet's IPv4, EtherType, ARP Protocol, MAC Parameters and VLAN parameters.



Ingress Port	Frame Type	Action	Rate Limiter	Port Copy	Counters
Any	ARP	Deny	1	Disabled	11
Any	ARP	Permit	1	Disabled	396
Any	ARP	Permit	1	Disabled	0
Any	ARP	Permit	1	Disabled	0
Any	ARP	Permit	Any	Disabled	0
Any	undefined	Deny	Any	Disabled	0
Any	EType	Deny	Any	Disabled	0
Any	IPv4/DHCP Client (Out)	Permit	Any	Disabled	0
Any	IPv4/DHCP Server (Out)	Permit	Any	Disabled	20

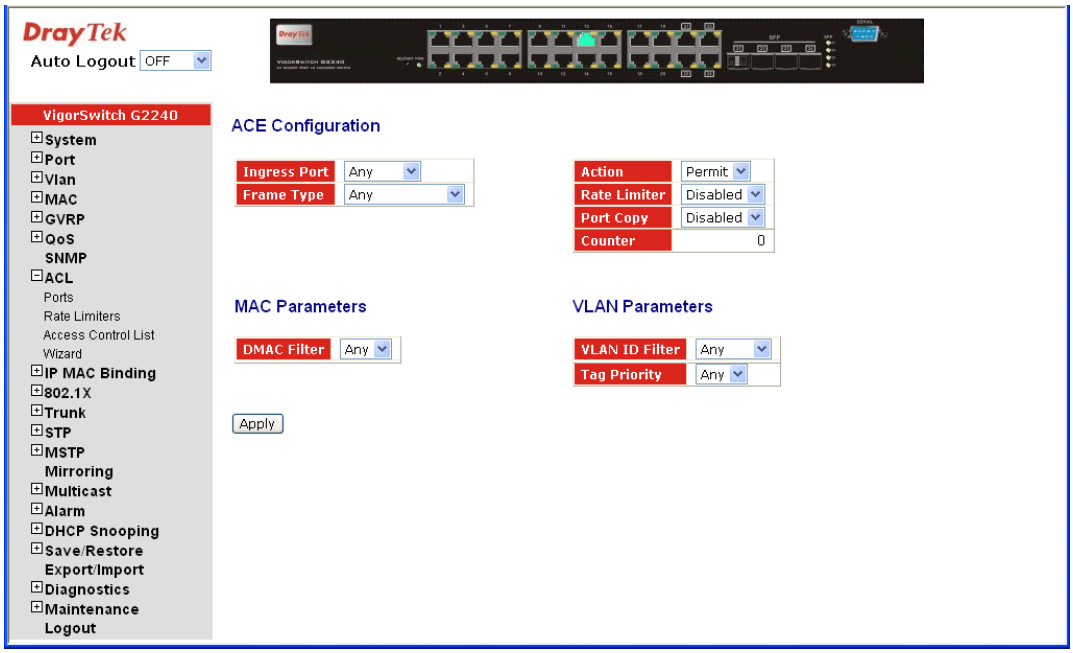


Parameters description:

Ingress Port:	Configurable Range: Any / Policy 1-8 / Port 1-24 Any: Apply this ACE rule for each port ingress classification Policy 1-8: Apply this ACE rule for specific policy Port 1-24: Apply this ACE rule for specific port ingress classification
Frame Type:	Range: Any / Ethernet Type / ARP / IPv4 Any: It is including all frame type Ethernet Type: It is including all Ethernet frame type

ARP: It is including all ARP protocol frame type
IPv4: It is including all IPv4 protocol frame type

To insert an entry, click the icon of inserting an entry, the following page will be shown as below.



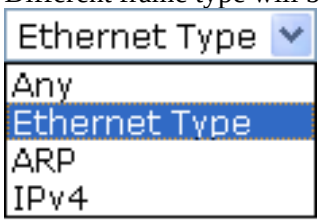
The switch ACL function support up to 128 Access Control Entries (ACEs), using the shared 128 ACEs for ingress classification. You can create an ACE and assign this ACE for each port with <Any> or assign this ACE for a policy or assign this ACE for a port. There are 8 policies, each port can select one of policy, then decides which of the Permit/Deny, Rate Limitation and Port Copy actions would take according to the ACL configuration packet's IPv4, EtherType, ARP Protocol, MAC Parameters and VLAN parameters.

Ingress Port:

Range: Any / Policy 1-8 / Port 1-24
Any: Apply this ACE rule for each port ingress classification
Policy 1-8: Apply this ACE rule for specific policy
Port 1-24: Apply this ACE rule for specific port ingress classification

Frame Type:

Different frame type will bring different web pages.

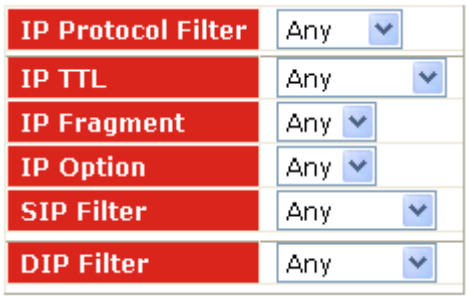


Any: It is including all frame type

Ethernet Type: It is including all Ethernet frame type. When you choose this one, the following selection will appear.

ARP: It is including all ARP protocol frame type. When you choose this one, the following selection will appear.

IPv4: It is including all IPv4 protocol frame type. When you choose this one, the following selection will appear.



MAC Parameters:

This section will change slightly based on the frame type selected.
(When Frame Type = **Any**)
DMAC Filter: Range: Any / MC / BC / UC
Any: It is including all destination MAC address
MC: It is including all Multicast MAC address
BC: It is including all Broadcast MAC address
UC: It is including all Unicast MAC address

(When Frame Type = **Ethernet Type**)
SMAC Filter: Range: Any / Specific
Any: It is including all source MAC address
Specific: It is according to SMAC Value specific the source MAC address
DMAC Filter: Range: Any / MC / BC / UC / Specific
Any: It is including all destination MAC address
MC: It is including all Multicast MAC address
BC: It is including all Broadcast MAC address
UC: It is including all Unicast MAC address
Specific: It is according to DMAC Value specific the destination MAC address

(When Frame Type = **ARP**)
SMAC Filter: Range: Any / Specific
Any: It is including all source MAC address
Specific: It is according to SMAC Value specific the source MAC address

DMAC Filter: Range: Any / MC / BC / UC
Any: It is including all destination MAC address
MC: It is including all Multicast MAC address
BC: It is including all Broadcast MAC address
UC: It is including all Unicast MAC address

(When Frame Type = **IPv4**)
DMAC Filter: Range: Any / MC / BC / UC
Any: It is including all destination MAC address

	MC: It is including all Multicast MAC address BC: It is including all Broadcast MAC address UC: It is including all Unicast MAC address (When Frame Type = **Ethernet Type**) *EtherType Filter*: Range: Any / Specific Any: It is including all Ethernet frame type Specific: It is according to specific Ethernet Type Value. Ethernet Type Value: The Ethernet Type Range: 0x600-0xFFFF
ARP Parameters:	This selection appears when Frame Type = **ARP**. *ARP/RARP*: Range: Any / ARP / RARP / Other Any: Including all ARP/RARP protocol frame types ARP: Including all ARP protocol frame types RARP: Including all RARP frame types Other: Including other frame types except ARP/RARP protocol *Request/Reply*: Range: Any / Request / Reply Any: Including all ARP/RARP Request and Reply Request: Including all ARP/RARP request frames Reply: Including all ARP/RARP reply frames *Sender IP Filte*r: Range: Any / Host / Network Any: Including all sender IP address Host: Only one specific sender host IP address Network: A specific IP subnet segment under the sender IP mask Sender IP Address: Default: 192.168.1.1 Sender IP Mask: Default: 255.255.255.0 *Target IP Filter*: Range: Any / Host / Network Any: Including all target IP address Host: Only one specific target host IP address Network: A specific IP subnet segment under the target IP mask Target IP Address: Default: 192.168.1.254 Target IP Mask: Default: 255.255.255.0 *ARP SMAC Match*: Range: Any / 0 / 1 Any: Both 0 and 1 0: The ingress ARP frames where the source MAC address is not equal SMAC under MAC parameter setting 1: The ingress ARP frames where the source MAC address is equal SMAC address under MAC parameter setting *RARP DMAC Match*: Range: Any / 0 / 1 Any: Both 0 and 1 0: The ingress RARP frames where the Destination MAC address is not equal DMAC address under MAC parameter setting 1: The ingress RARP frames where the Destination MAC address is equal DMAC address under MAC parameter setting *IP/Ethernet Length*: Range: Any / 0 / 1 Any: Both 0 and 1

0: The ingress ARP/PARP frames where the Hardware size is not equal "0x6" or the Protocol size is not equal "0x4"
1: The ingress ARP/PARP frames where the Hardware size is equal "0x6" and the Protocol size is "0x4"

IP: Range: Any / 0 / 1
Any: Both 0 and 1
0: The ingress ARP/PARP frames where Protocol type is not equal "0x800"
1: The ingress ARP/PARP frames where Protocol type is equal "0x800"

Ethernet: Range: Any / 0 / 1
Any: Both 0 and 1
0: The ingress ARP/PARP frames where Hardware type is not equal "0x100"
1: The ingress ARP/PARP frames where Hardware type is equal "0x100"

IP Parameters: This selection appears when Frame Type = **IPv4** and IP Protocol Filter = **Any**)

IPTT: (Time To Live): How many routers a datagram can pass through. Each router decrements this value by 1 until it reaches 0 when the datagram is discarded. This keeps misrouted datagram from remaining on the Internet forever
Range: Any / Non-zero / Zero
Any: Including all conditions for IPTTL
Non-Zero: Including IPTTL is Non-Zero
Zero: Including IPTTL is zero

IP Fragment (IP Fragmentation Flag): Controls datagram fragmentation together with the identification field. The flags indicate whether the datagram may be fragmented, whether the datagram is fragmented, and whether the current fragment is the final one.
Range: Any / Yes / No
Any: Including all IP fragment case
Yes: The ingress frame is fragmented packet
No: The ingress frames is not fragmented packet

*IP Optio*n: A list of optional specifications for security restrictions, route recording, and source routing. Not every datagram specifies an options field.
Range: Any / Yes / No
Any: Including all IP option case
Yes: The ingress frame is specified IP options
No: The ingress frame is not specified IP options

SIP Filter: (SIP Source IP Address)
Range: Any / Host / Network
Any: Including all source IP address
Host: Only one specific source host IP address
Network: A specific IP subnet segment under the source IP mask
SIP Address: Default: 192.168.1.1
SIP Mask: Default: 255.255.255.0

DIP Filter: (DIP Destination IP Address)
Range: Any / Host / Network
Any: Including all destination IP address
Host: Only one specific destination host IP address
Network: A specific IP subnet segment under the destination IP mask
DIP Address: Default: 192.168.1.254
DIP Mask: Default: 255.255.255.0

When Frame Type = **IPv4** and IP Protocol Filter = **ICMP**, ICMP Parameters will appear and contain the following options:

ICMP Type Filter:
Range: Any / Specific
Any: Including all types of ICMP type values
Specific: According to following ICMP type value setting for ingress classification

ICMP Type Value:
Range: 0-255

ICMP Code Filter:
Range: Any / Specific
Any: Including all of ICMP code values
Specific: According to following ICMP code value setting for ingress classification

ICMP Code Value:
Range: 0-255

When Frame Type = **IPv4** and IP Protocol Filter = **UDP**, UDP Parameters will appear and contain the following options:

Source Port Filter: Range: Any / Specific / Range
Any: Including all UDP source ports
Specific: According to following Source Port No. setting for ingress classification
Range: According to following Source Port Range setting for ingress classification
Source Port No/Range.: Range: 0-65535
Dest. Port Filter: Range: Any / Specific / Range
Any: Including all UDP destination ports
Specific: According to following Dest. Port No. setting for ingress classification
Range: According to following Dest. Port Range setting for ingress classification
Dest. Port No.: (Destination Port Number) Range: 0-65535
Dest. Port Range.: (Destination Port Range) Range: 0-65535

When Frame Type = **IPv4** and IP Protocol Filter = **TCP**, the TCP Parameters will appear and contain the following options:
Source Port Filter: Range: Any / Specific / Range
Any: Including all TCP source ports
Specific: According to following Source Port No. setting for ingress classification
Range: According to following Source Port Range setting

for ingress classification
Source Port No.: Range: 0-65535
Source Port Range.: Range: 0-65535
Dest. Port Filter: Range: Any / Specific / Range
Any: Including all TCP destination ports
Specific: According to following Dest. Port No. setting for ingress classification
Range: According to following Dest. Port Range setting for ingress classification
Dest. Port No.: Range: 0-65535
Dest. Port Range.: Range: 0-65535

*TCP FIN: (*TCP Control Bit FIN) Means No more data from sender
Range: Any / 0 / 1
Any: Including all TCP FIN case
0: The TCP control bit FIN is 0
1: The TCP control bit FIN is 1

TCP SYN: (TCP Control Bit SYN) Means Synchronize sequence numbers
Range: Any / 0 / 1
Any: Including all TCP SYN case
0: The TCP control bit SYN is 0
1: The TCP control bit SYN is 1

TCP RST: (TCP Control Bit RST) Means Reset the connection
Range: Any / 0 / 1
Any: Including all TCP RST case
0: The TCP control bit RST is 0
1: The TCP control bit RST is 1

TCP PSH: (TCP Control Bit PSH) Means Push Function
Range: Any / 0 / 1
Any: Including all TCP PSH case
0: The TCP control bit PSH is 0
1: The TCP control bit PSH is 1

TCP ACK: (TCP Control Bit ACK) Means Acknowledgment field significant
Range: Any / 0 / 1
Any: Including all TCP ACK case
0: The TCP control bit ACK is 0
1: The TCP control bit ACK is 1

TCP URG: (TCP Control Bit URG) Means Urgent Pointer field significant
Range: Any / 0 / 1
Any: Including all TCP URG case
0: The TCP control bit URG is 0
1: The TCP control bit URG is 1

When Frame Type = **IPv4** and IP Protocol Filter = **Other**, The IP Parameters will be as follows:

IP Protocol Value: Default: 255
IPTTL: (Time To Live) How many routers a datagram can pass through. Each router decrements this value by 1 until it reaches 0 when the datagram is discarded. This keeps misrouted datagrams from remaining on the Internet forever.
Range: Any / Non-zero / Zero
Any: Including all conditions for IPTTL
Non-Zero: Including IPTTL is Non-Zero
Zero: Including IPTTL is zero

IP Fragment: (IP Fragmentation Flag) Controls datagram fragmentation together with the identification field. The flags indicate whether the datagram may be fragmented, whether the datagram is fragmented, and whether the current fragment is the final one.
Range: Any / Yes / No
Any: Including all IP fragment case
Yes: The ingress frame is fragmented packet
No: The ingress frame is not fragmented packet

IP Option: A list of optional specifications for security restrictions, route recording, and source routing. Not every datagram specifies an options field.
Range: Any / Yes / No
Any: Including all IP option case
Yes: The ingress frame is specified IP options
No: The ingress frame is not specified IP options

SIP Filter: (SIP Source IP Address)
Range: Any / Host / Network
Any: Including all source IP address
Host: Only one specific source host IP address
Network: A specific IP subnet segment under the source IP mask
SIP Address: Default: 192.168.1.1
SIP Mask: Default: 255.255.255.0

DIP Filter: (DIP Destination IP Address)
Range: Any / Host / Network
Any: Including all destination IP address
Host: Only one specific destination host IP address
Network: A specific IP subnet segment under the destination IP mask
DIP Address: Default: 192.168.1.254
DIP Mask: Default: 255.255.255.0

VLAN Parameters:

VLAN ID Filter: Range: Any / Specific
Any: Including all VLAN IDs
Specific: According to following VLAN ID and Tag Priority setting for ingress classification

VLAN ID: Range: 1-4094

Tag Priority: Range: Any / 0-7
Any: Including all Tag Priority values
0-7: The Tag Priority Value is one of number (0-7)

Action Parameters:

When the ingress frame meets above ACL ingress classification rule you can do the following actions:

Action: Range: Permit / Deny
Permit: Permit the met ACL ingress classification rule packets forwarding to other ports on the switch
Deny: Discard the met ACL ingress classification rule packets

Rate Limiter: Range: Disabled / 1-16
Disable: Disable Rate Limiter function
1-16: Apply the Rate Limiter Number setting for met ACL ingress rule packets

Port Copy: Range: Disabled / 1-24
Disable: Disable the Port Copy function
1-24: The packets will be copied to the selected port when they met ACL ingress rule.

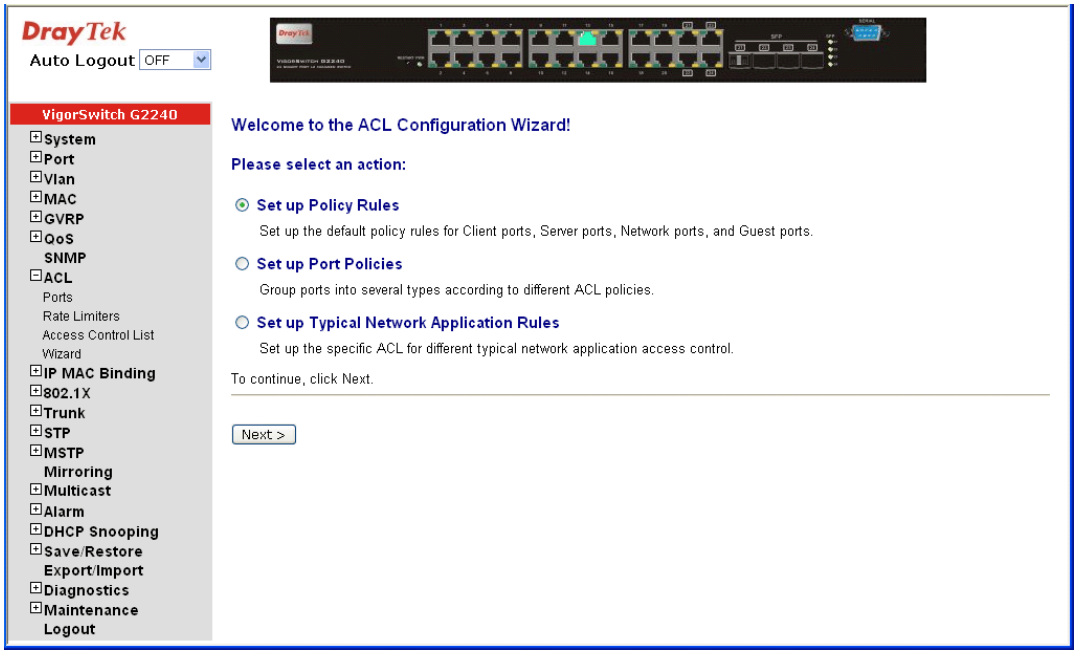
2.8.4 Wizard

Function name:

Wizard

Function description:

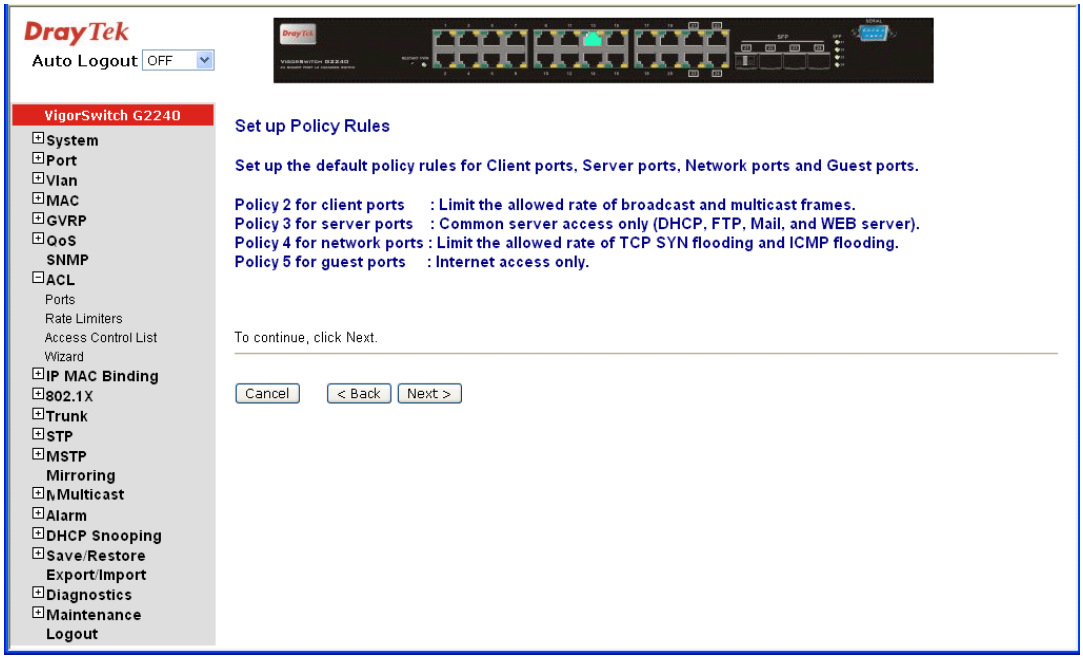
The wizard function provides 4 type of typical application for user easy to configure their application with ACL function.



Parameter description:

Please select an Action:	Set up Policy Rules / Set up Port Policies / Set up Typical Network Application Rules.
Next:	Click on <Next> to confirm current setting and go to next step automatically.

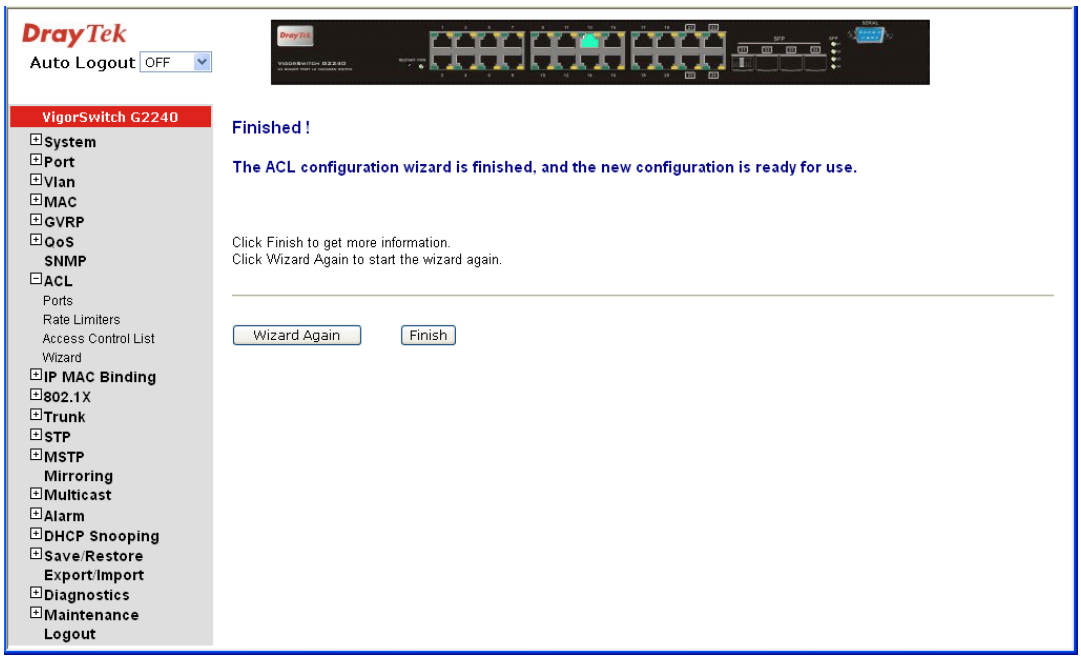
- **Set up Policy Rules**



Cancel: Cancel current setting back to top layer in the ACL wizard function.

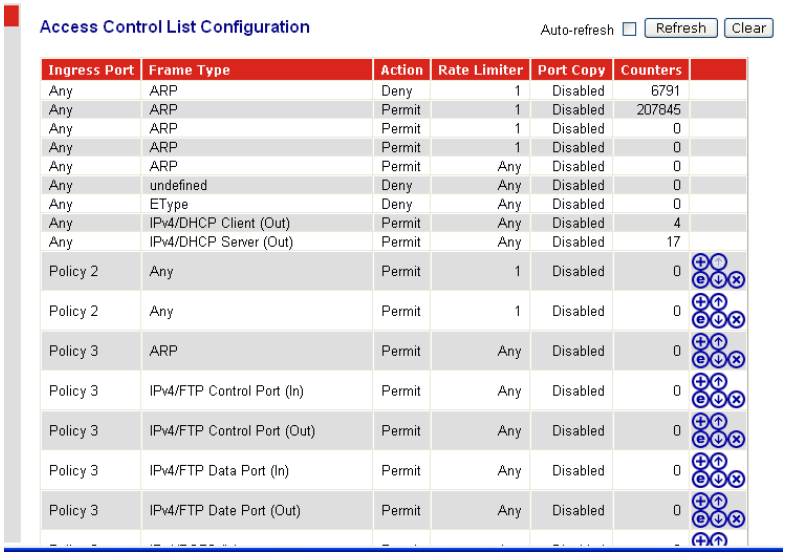
Back: Click on <Back> to back to previous step.

Next: Click on <Next> to go to the next step.



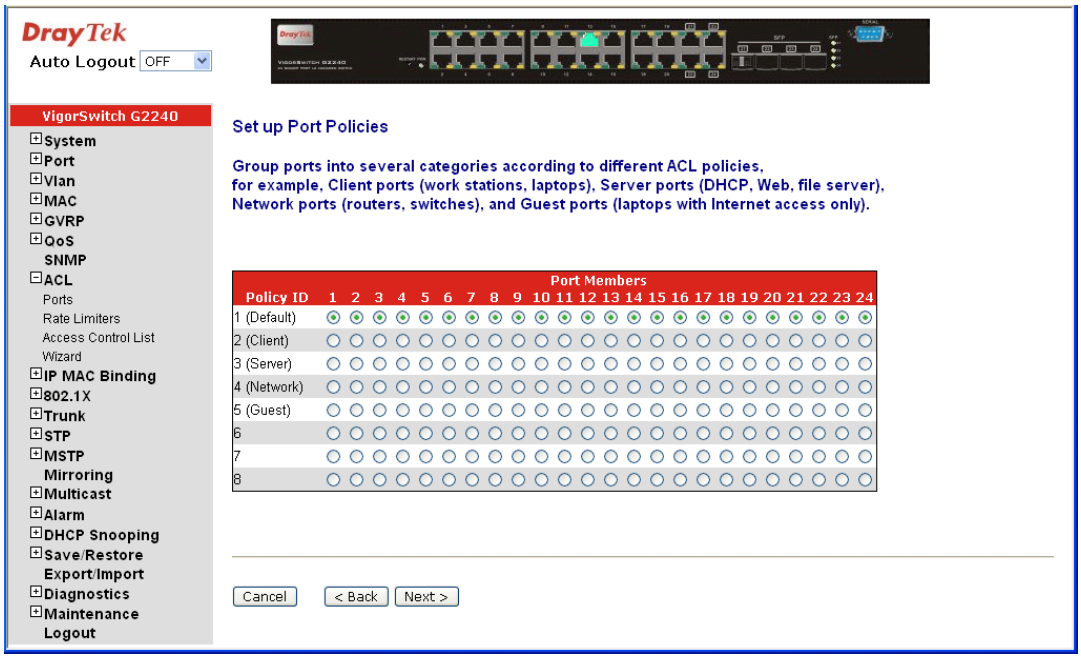
Wizard Again: Click on <Wizard Again> the UI will back to top layer in the wizard function.

Finish: Click in <Finish> to finish the ACL Wizard setting, it will according the selection items to change the related parameters, then you have to click on <Apply> to confirm the all changed parameters setting.

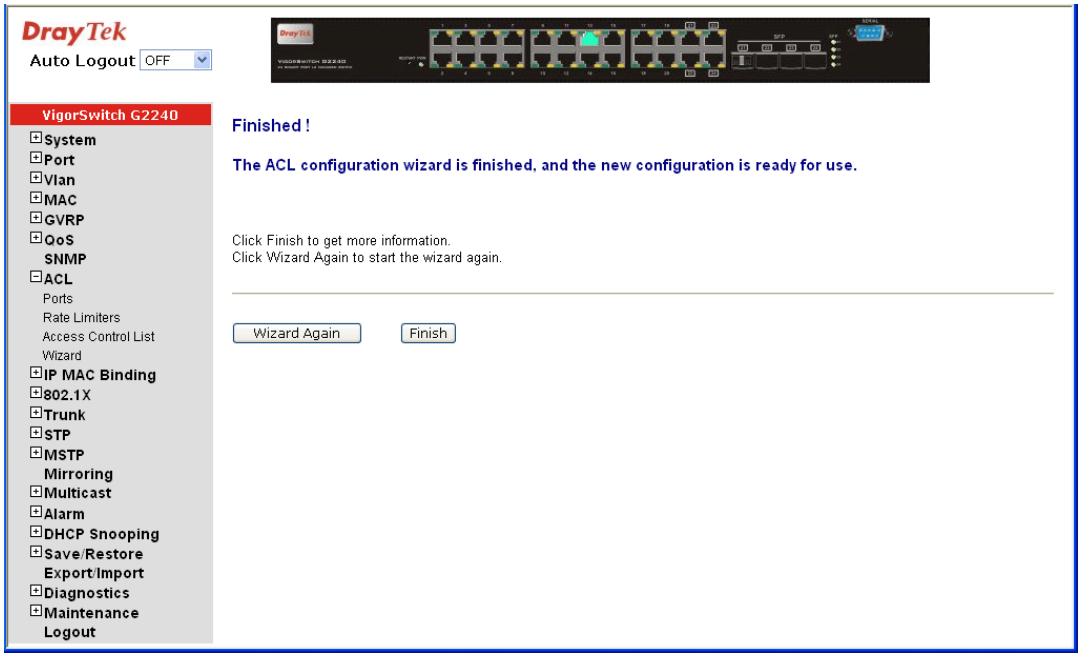


Ingress Port	Frame Type	Action	Rate Limiter	Port Copy	Counters
Any	ARP	Deny	1	Disabled	6791
Any	ARP	Permit	1	Disabled	207845
Any	ARP	Permit	1	Disabled	0
Any	ARP	Permit	1	Disabled	0
Any	ARP	Permit	Any	Disabled	0
Any	undefined	Deny	Any	Disabled	0
Any	EType	Deny	Any	Disabled	0
Any	IPv4/DHCP Client (Out)	Permit	Any	Disabled	4
Any	IPv4/DHCP Server (Out)	Permit	Any	Disabled	17
Policy 2	Any	Permit	1	Disabled	0
Policy 2	Any	Permit	1	Disabled	0
Policy 3	ARP	Permit	Any	Disabled	0
Policy 3	IPv4/FTP Control Port (In)	Permit	Any	Disabled	0
Policy 3	IPv4/FTP Control Port (Out)	Permit	Any	Disabled	0
Policy 3	IPv4/FTP Data Port (In)	Permit	Any	Disabled	0
Policy 3	IPv4/FTP Date Port (Out)	Permit	Any	Disabled	0

- **Set up Port Policies**

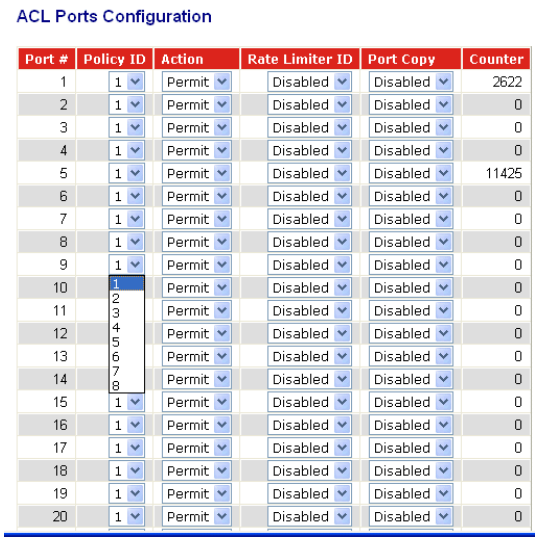


Cancel:	Cancel current setting back to top layer in the ACL wizard function.
Back:	Click on <Back> to back to previous step.
Next:	Click on <Next> to go to the next step.

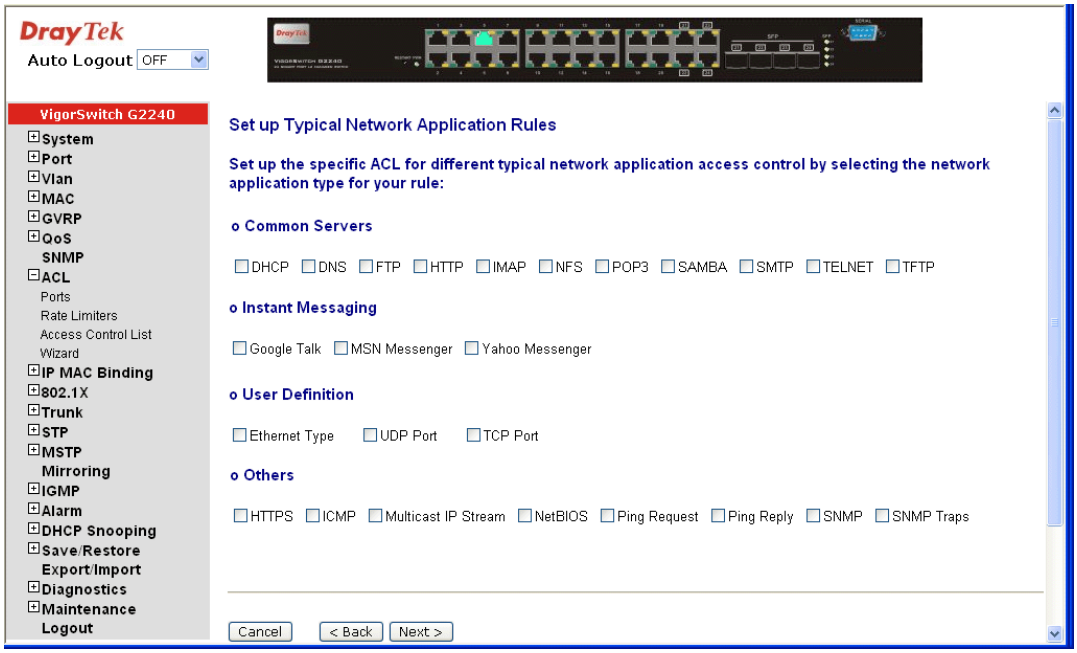


Wizard Again: Click on <Wizard Again> the UI will back to top layer in the wizard function.

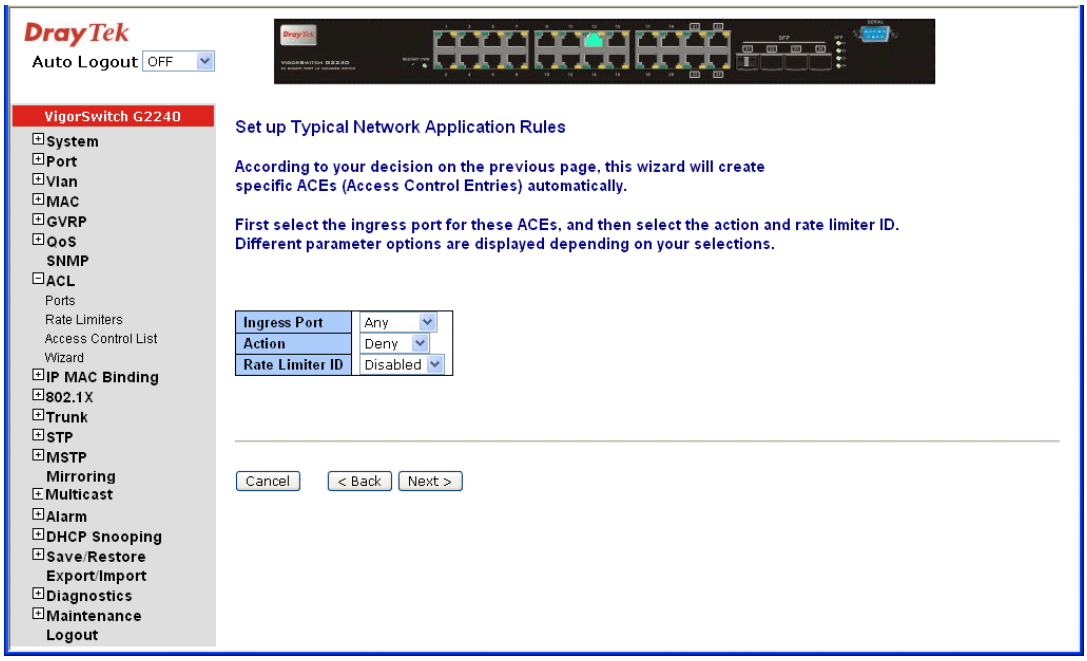
Finish: Click in <Finish> to finish the ACL Wizard setting, it will according the selection items to change the related parameters, then you have to click on <Apply> to confirm the all changed parameters setting.



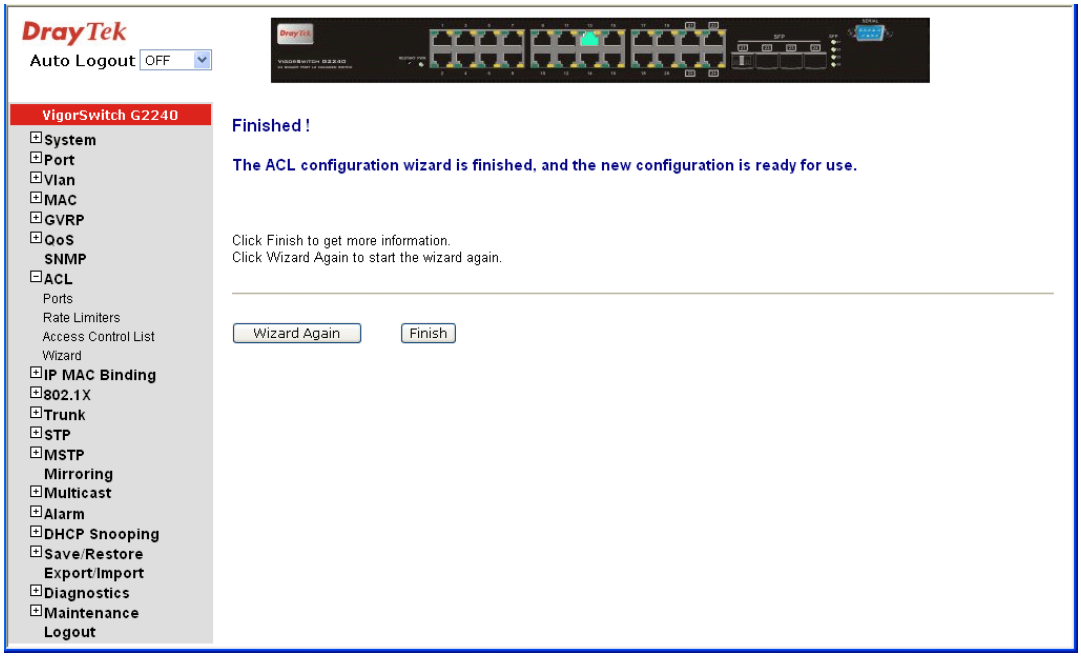
- **Set up Typical Network Application Rules**



Common Server:	DHCP / DNS / FTP / HTTP / IMAP / NFS / POP3 / SAMBA / SMTP / TELNET / TFTP
Instant Messaging:	Google Talk / MSN Messenger / Yahoo Messenger
User Definition:	Ethernet Type / UDP Port / TCP Port
Others:	TCP Port / ICMP / Multicast IP Stream / NetBIOS / Ping Request / Ping Reply / SNMP / SNMP Traps
Cancel:	Cancel current setting back to top layer in the ACL wizard function.
Back:	Click on <Back> to back to previous step.
Next:	Click on <Next> to go to the next step.

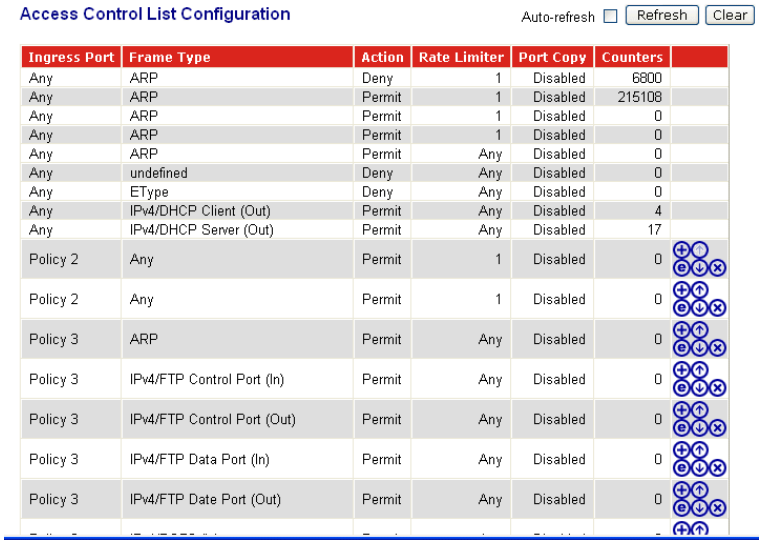


Ingress Port:	Any / Policy1-8 / Port1-24
Action:	Permit / Deny
Rate Limiter ID:	Disabled / 1-16
Cancel:	Cancel current setting back to top layer in the ACL wizard function.
Back:	Click on <Back> to back to previous step.
Next:	Click on <Next> to go to the next step.



Wizard Again:	Click on <Wizard Again> the UI will back to top layer in the wizard function.
Finish:	Click in <Finish> to finish the ACL Wizard setting, it will change the related parameters according the selection items,

then you have to click on <Apply> to confirm the changed parameters setting.



Ingress Port	Frame Type	Action	Rate Limiter	Port Copy	Counters	
Any	ARP	Deny	1	Disabled	6800	
Any	ARP	Permit	1	Disabled	215108	
Any	ARP	Permit	1	Disabled	0	
Any	ARP	Permit	1	Disabled	0	
Any	ARP	Permit	Any	Disabled	0	
Any	undefined	Deny	Any	Disabled	0	
Any	EType	Deny	Any	Disabled	0	
Any	IPv4/DHCP Client (Out)	Permit	Any	Disabled	4	
Any	IPv4/DHCP Server (Out)	Permit	Any	Disabled	17	
Policy 2	Any	Permit	1	Disabled	0	
Policy 2	Any	Permit	1	Disabled	0	
Policy 3	ARP	Permit	Any	Disabled	0	
Policy 3	IPv4/FTP Control Port (In)	Permit	Any	Disabled	0	
Policy 3	IPv4/FTP Control Port (Out)	Permit	Any	Disabled	0	
Policy 3	IPv4/FTP Data Port (In)	Permit	Any	Disabled	0	
Policy 3	IPv4/FTP Date Port (Out)	Permit	Any	Disabled	0	

2.9 IP MAC Binding

2.9.1 IP MAC Binding Configuration

The IP network layer uses a four-byte address. The Ethernet link layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC binding is to restrict the access to a switch to a number of authorized users. Only the authorized client can access the Switch's port by checking the pair of IP-MAC

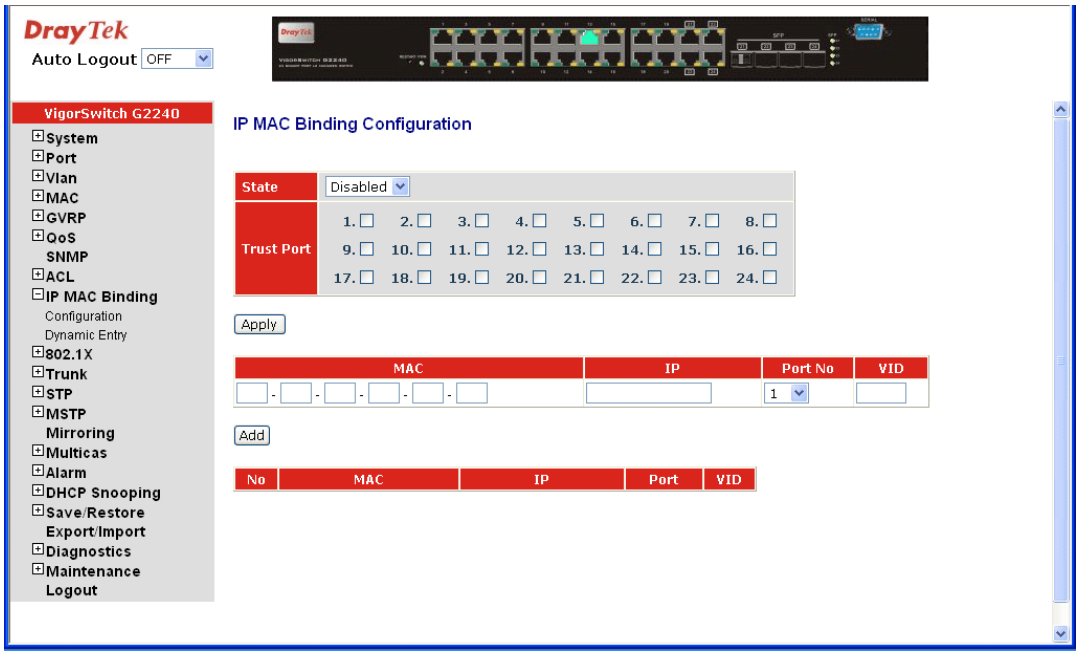
Addresses and port number with the pre-configured database. If an unauthorized user tries to access an IP-MAC binding enabled port, the system will block the access by dropping its packet.

Function name:

IP MAC Binding Configuration

Function description:

The switch has client and server two classes of IP-MAC Binding table. The maximum number of IP-MAC binding client table is 512 entries. The maximum number of IP-MAC Binding server table is 64 entries. The creation of authorized users can be manually. The function is global, this means a user can enable or disable the function for all ports on the switch.



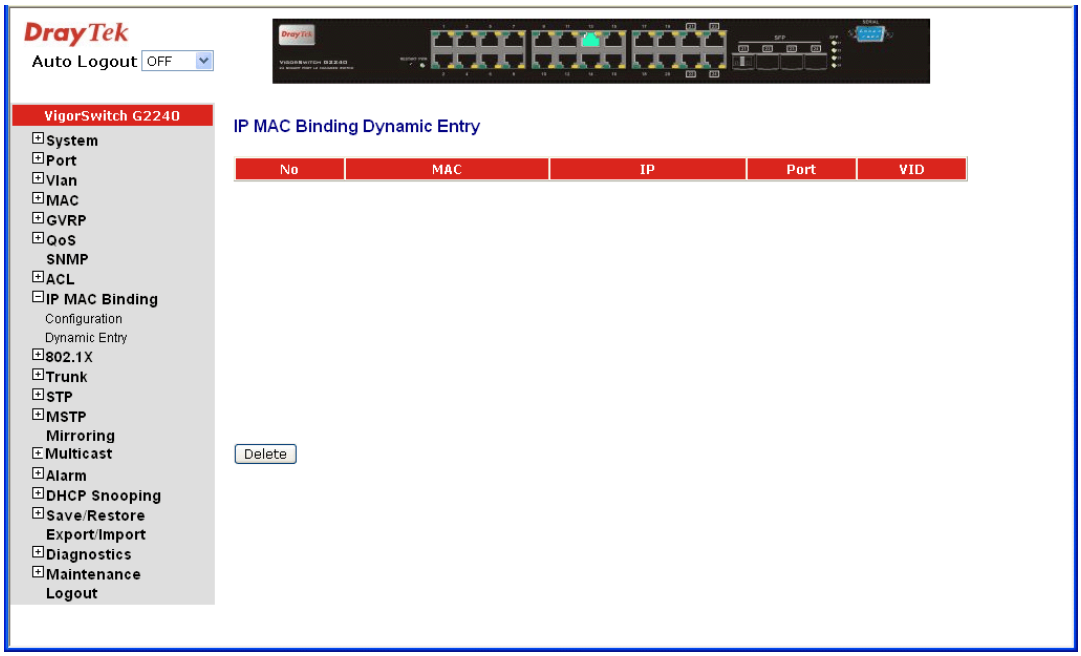
Parameter description:

State:	Disabled / Enabled
Trust Port:	**If DHCP snooping is enabled globally and enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a trusted port. The available ports are from 0 to 24.** Number of IP-MAC Binding server table is 64 entries.
MAC:	Six-byte MAC Address: xx-xx-xx-xx-xx-xx For example: 00-40-c7-00-00-01

IP:	Four-byte IP Address: xxx.xxx.xxx.xxx For example: 192.168.1.100
Port No:	Port no.: 1-24
VID:	VLAN ID: 1-4094
Add:	Input MAC, IP, Port and VID, then click on <Add> to create a new entry into the IP MAC Binding table
Delete:	Select one of entry from the table, then click on <Delete> to delete this entry.

2.9.2 IP MAC Binding Dynamic Entry

定義?請提供說明



The function must combine with IP-MAC Binding and DHCP Snooping Enable.

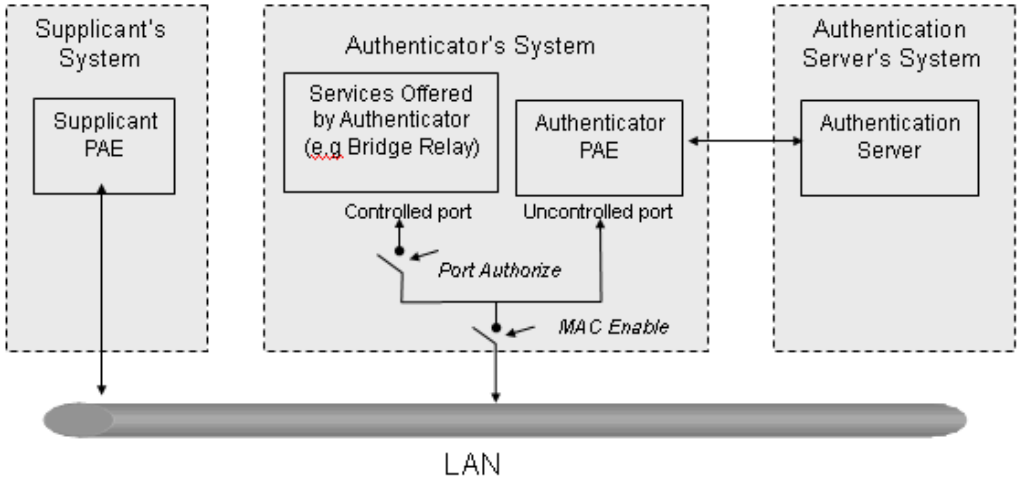
No:	**The IP-MAC Binding entry Index**
MAC:	**Six-byte MAC Address: xx-xx-xx-xx-xx-xx For example: 00-40-c7-00-00-01**
IP:	**Four-byte IP Address: xxx.xxx.xxx.xxx For example: 192.168.1.100**
Port No:	**Port no.: 1-24**
VID:	**VLAN ID: 1-4094**
Add:	**Input MAC, IP, Port and VID, then click on <Add> to create a new entry into the IP MAC Binding table**
Delete:	**Select one of entry from the table, then click on <Delete> to delete this entry.**

2.10 802.1X 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.

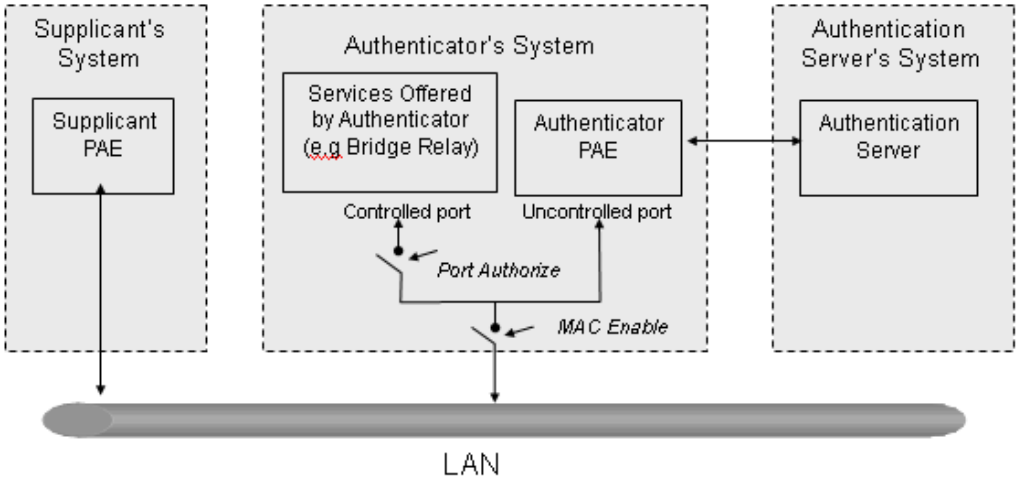
A port acting as an authenticator is thought to be two logical ports, a controlled port and an uncontrolled port. A controlled port can only pass the packets when the authenticator PAE is authorized, and otherwise, an uncontrolled port will unconditionally pass the packets with PAE group MAC address,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

Authentication server:

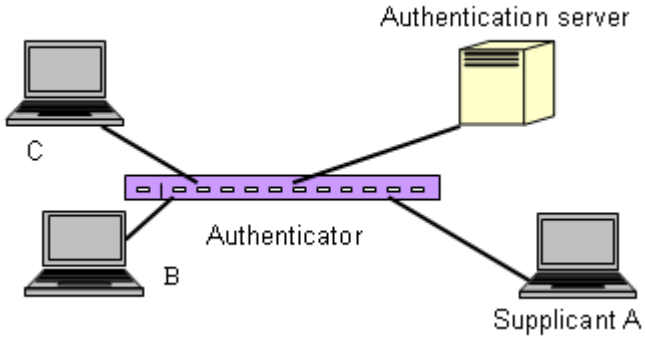
A device provides authentication service, through EAP, to an authenticator by using authentication credentials supplied by the supplicant to determine if the supplicant is authorized to access the network resource.

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.

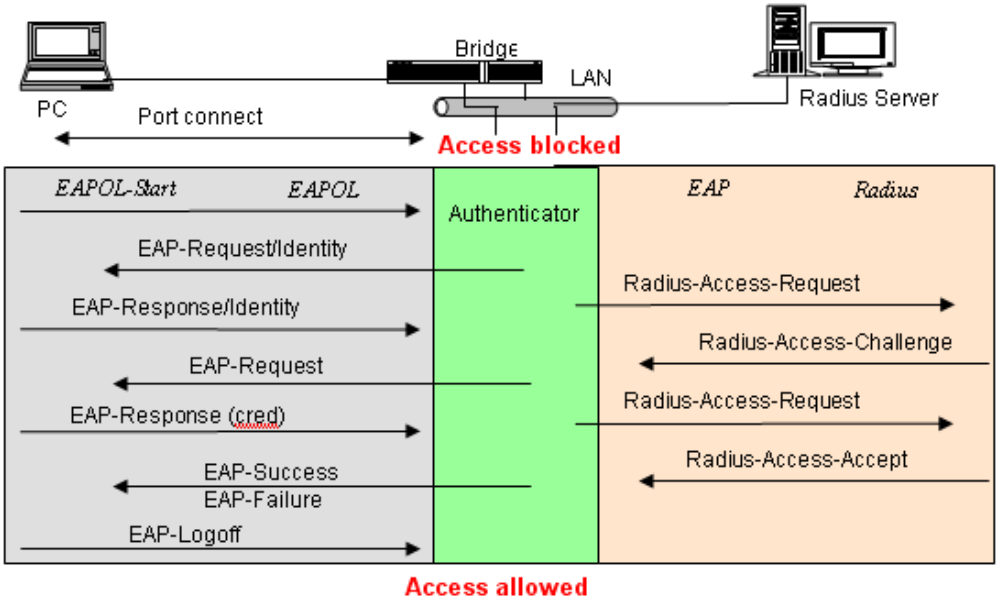
While in the authentication process, the message packets, encapsulated by Extensible Authentication Protocol over LAN (EAPOL), are exchanged between an authenticator PAE and a supplicant PAE. The Authenticator exchanges the message to authentication server using EAP encapsulation. Before successfully 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

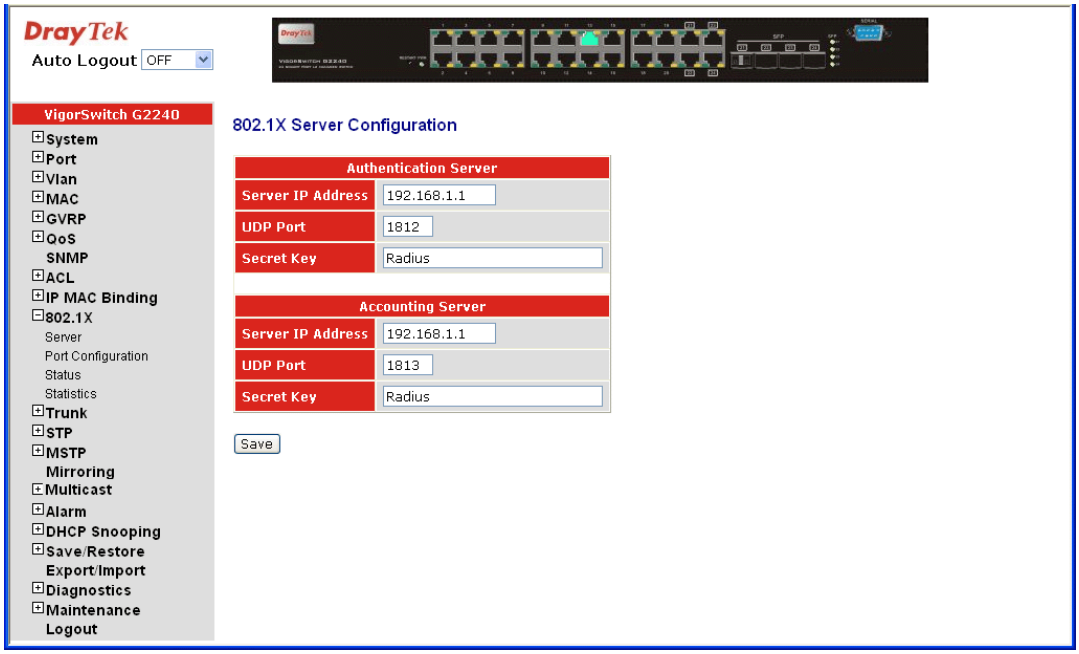
2.10.1 Server

Function name:

802.1X Server Configuration

Function description:

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



Authentication Server	*Server IP Server* - Server IP address for authentication. Default: 192.168.1.1 *UDP Port* -Default port number is 1812. *Secret Key* - The secret key should be 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 Server	*Server IP Server* - Server IP address for authentication. Default: 192.168.1.1 *UDP Port* - Default port number is 1812. *Secret Key* - The secret key should be 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

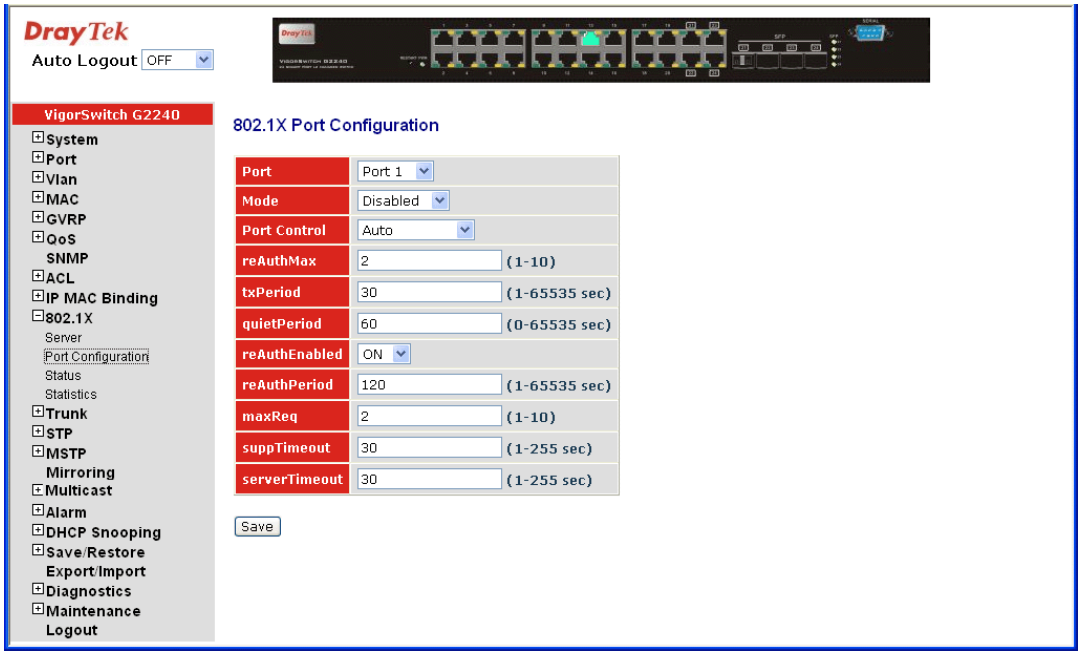
2.10.2 Port Configuration

Function name:

802.1X Port Configuration

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.



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.

Mode: Range: Disable / Normal / Advanced / Clientless
Disable: Disable IEEE 802.1X for this port.
Normal: All clients under this port will be authorized when one of the client do 802.1X authentication successfully.
Advanced: Each client under this port have to do 802.1X authentication by himself.
Clientless: The clients don't need to install 802.1X client function. It means the client PC (for example WINDOW XP) which does not need to enable 802.1X client function also can do 802.1X authentication. But the network maintainer needs to configure the Radius server using each client's MAC address for Radius account ID and password.

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

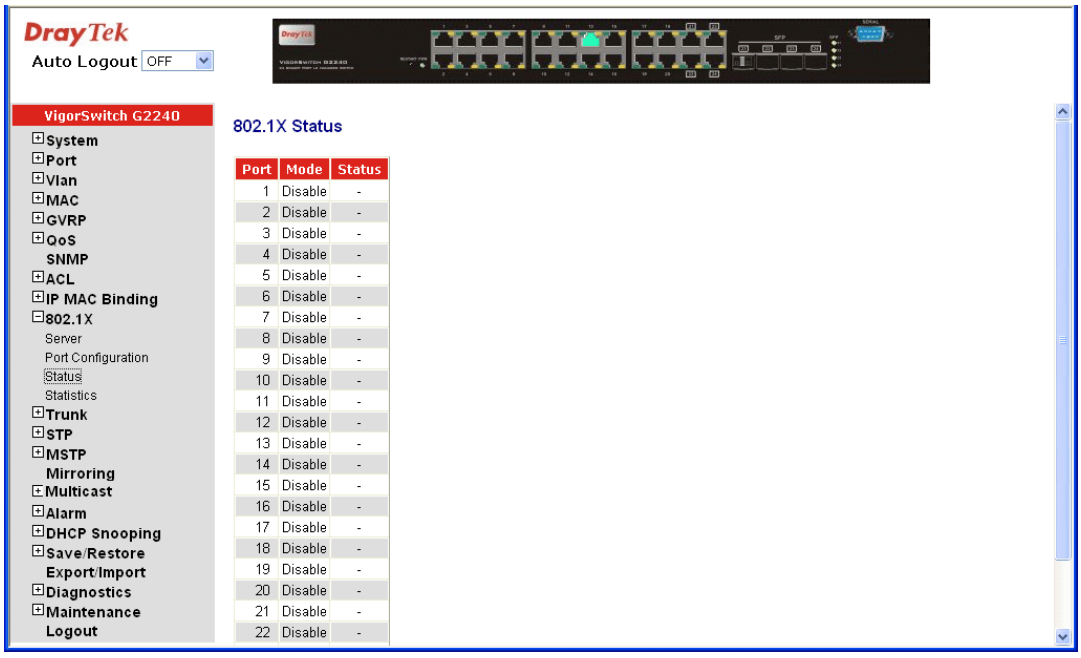
2.10.3 Status

Function name:

802.1X Status

Function description:

Show the each port IEEE 802.1X authentication current operating mode and status.



Parameter description:

Port:	Port number: 1-24
Mode:	Show this port IEEE 802.1X operating mode: There are four modes Disable, Normal, Advance and Clientless.
Status:	Show this port IEEE 802.1X security current status: Authorized or Unauthorized.

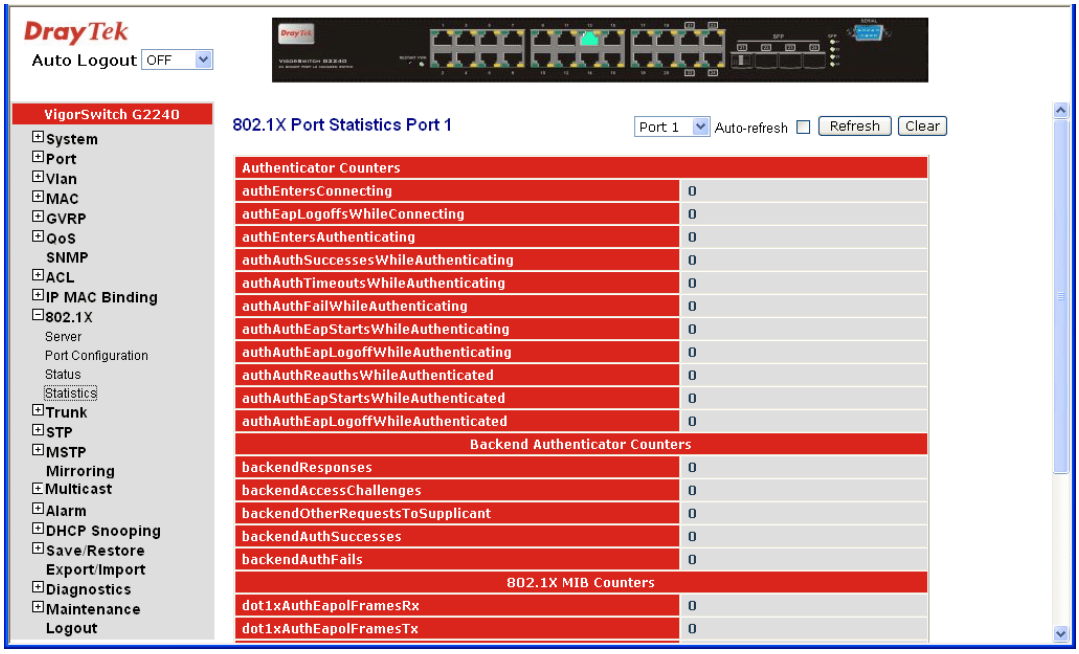
2.10.4 Statistics

Function name:

802.1X Port Statistics Port 1

Function description:

Show the IEEE 802.1X authentication related counters for manager monitoring authenticator status.



Parameter description:

Port:	Port Number: 1-24
Auto - refresh:	Refresh the authenticator counters in the web UI automatically
Refresh:	Click on the <Refresh> to update the authenticator counters in the web UI
Clear:	Click on the <Clear> to clear all authenticator counters in the web UI

2.11 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:

- 12 ports have already used Static Trunk Group ID 1, the 13th port willing to use the same Static Trunk Group ID will be automatically set to use the “None” trunking method and its Group ID will turn to 0. This means the port won’t aggregate with other ports.
- 14 ports all use LACP Trunk Group ID 1 at most 12 ports can aggregate together and transit into the ready state.
- A port using the “None“ trunking method or Group ID 0 will be automatically set to use the “None” trunking method with Group ID 0.

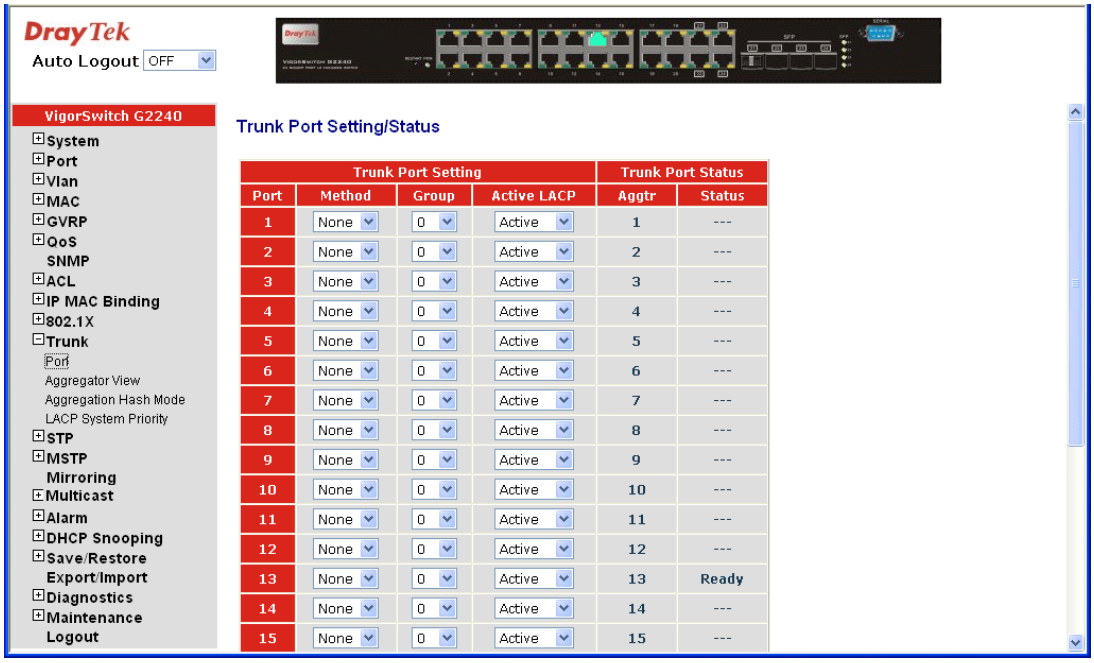
2.11.1 Port

Function name:

Trunk Port Setting/Status

Function description:

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



Parameter description:

Port : Port Number: 1-24

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.

Active - 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”

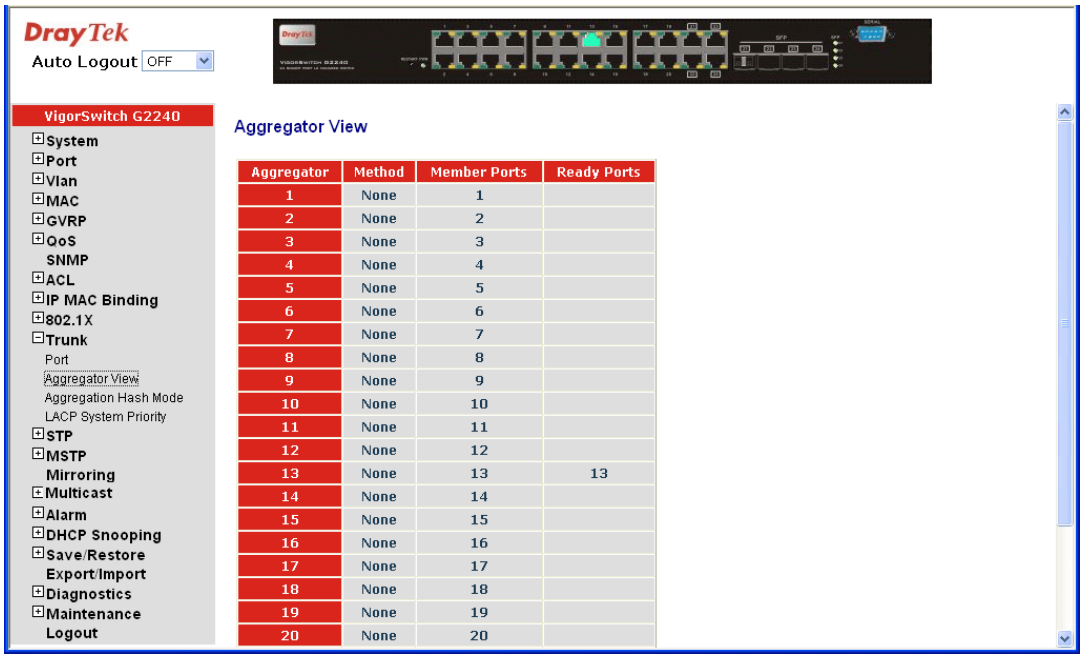
2.11.2 Aggregator View

Function name:

Aggregator View

Function description:

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



Parameter description:

Aggregator: It shows the aggregator ID (from 1 to 24) 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).

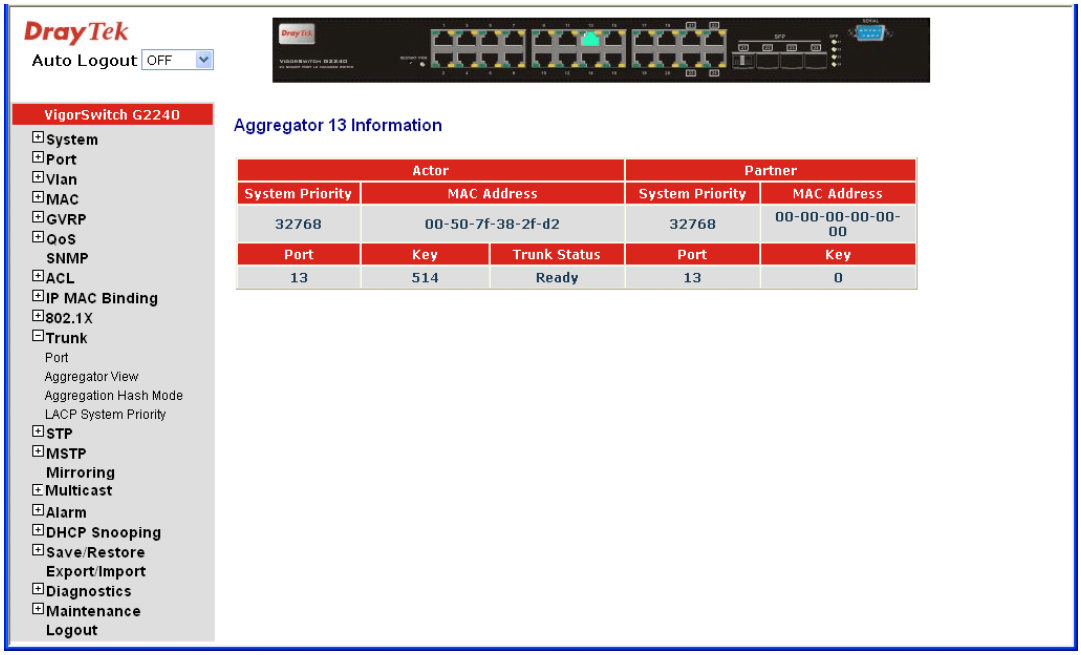
LACP Detail

Function name:

LACP Detail (LACP Aggregator Detailed Information)

Function description:

Show the detailed information of the LACP trunking group.



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"

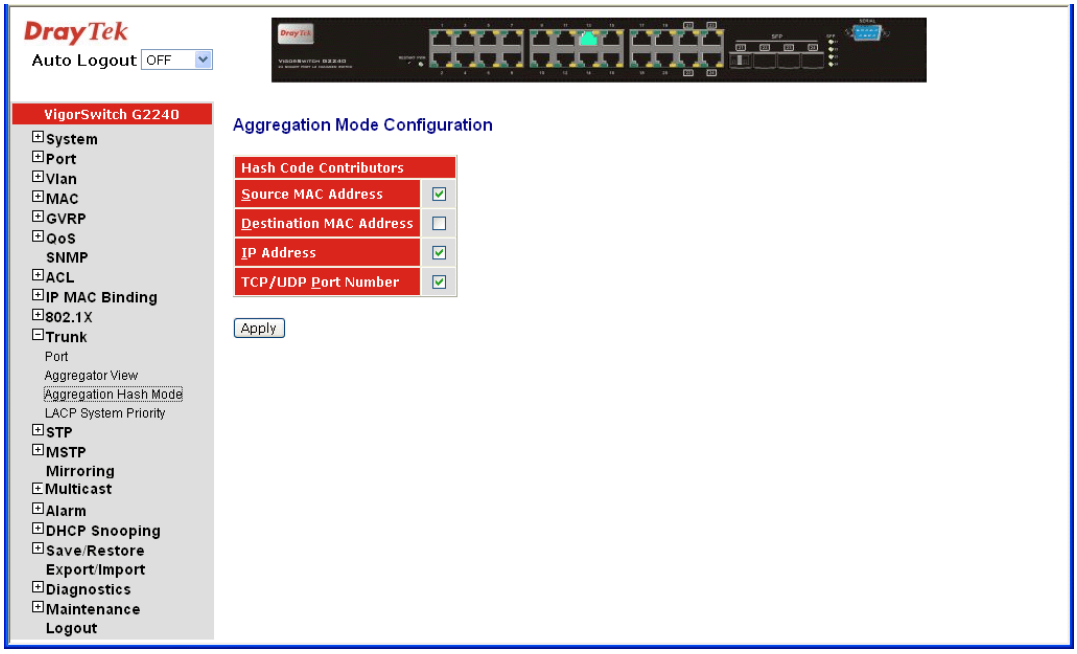
2.11.3 Aggregation Hash Mode

Function name:

Aggregation Hash Mode

Function description:

Configure the current port aggregate mode with 4 types.



Parameter description:

Source MAC Address:	Check this box to evoke to enable source MAC address for Aggregate Mode.
Destination MAC Address:	Check this box to evoke to enable destination MAC address for Aggregate Mode.
IP Address:	Check this box to evoke to enable IP address for Aggregate Mode.
TCP/UDP Port Number:	Check this box to evoke to enable TCP/UDP Port Number for Aggregate Mode.

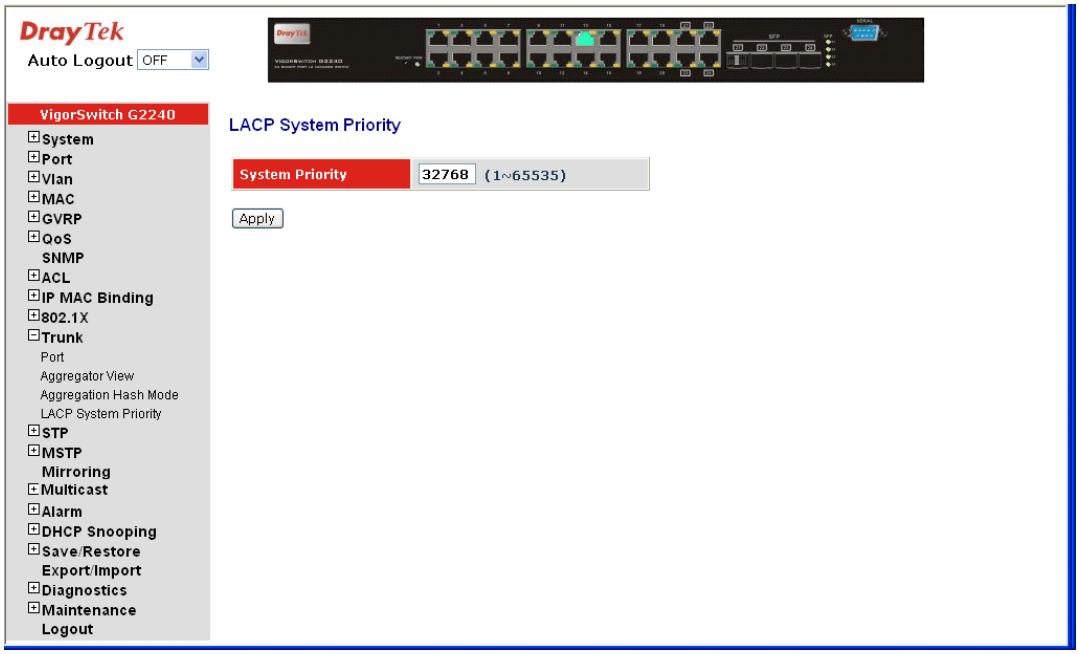
2.11.4 LACP System Priority

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



Parameter description:

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

2.12 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.

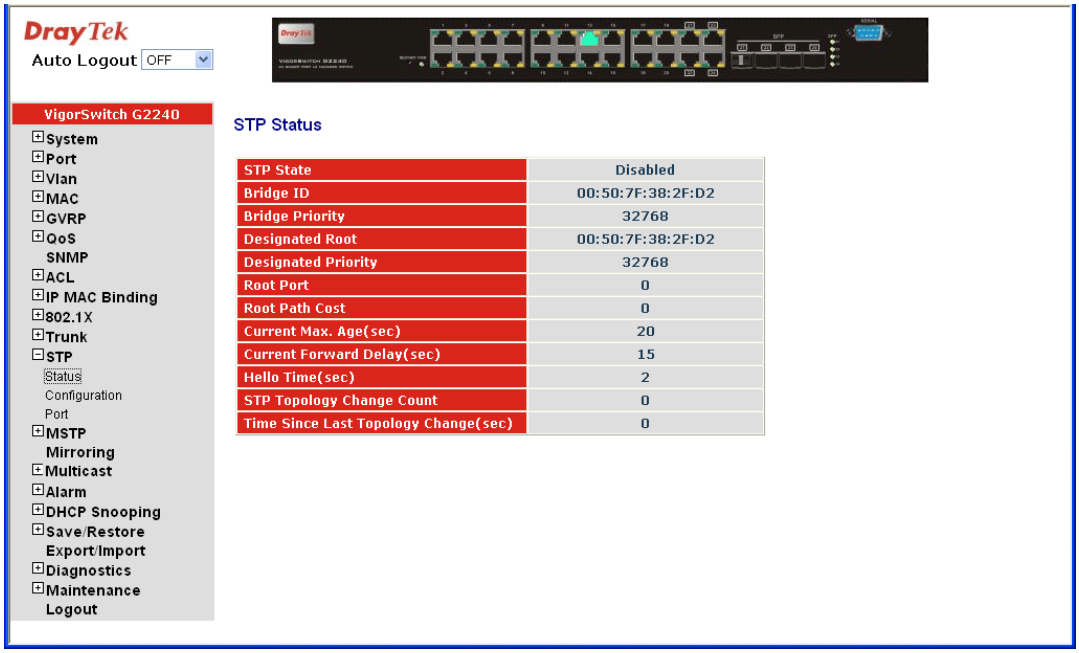
2.12.1 STP Status

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.



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.

2.12.2 STP Configuration

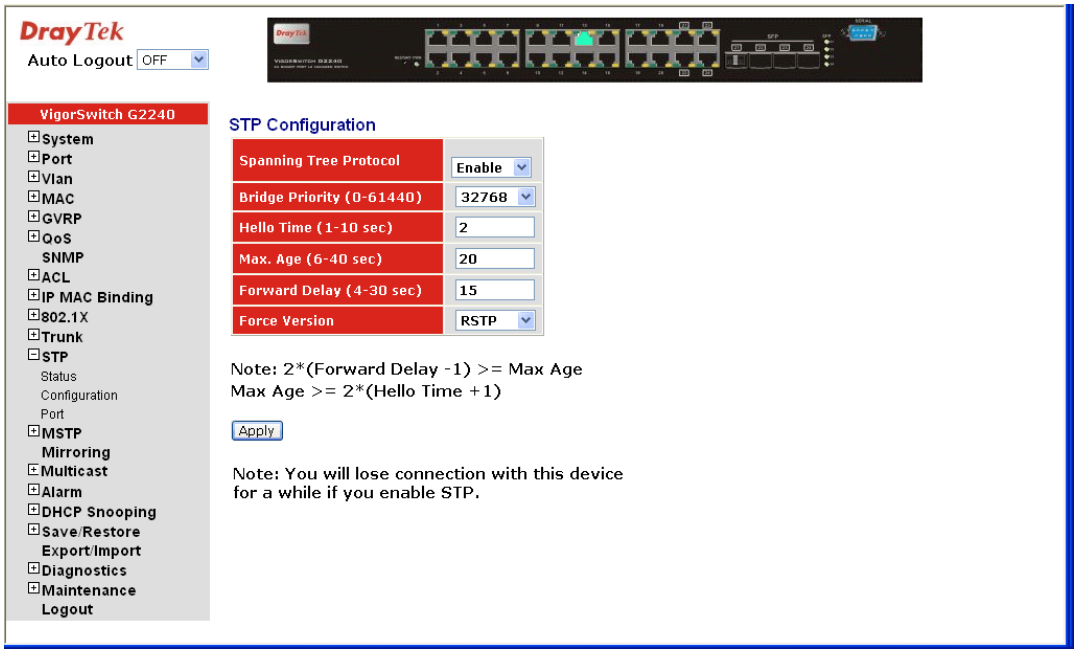
The STP, Spanning Tree Protocol, actually includes RSTP. In the Spanning Tree Configuration, there are six parameters open for the user to configure as user’s idea. Each parameter description is listed below.

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”.



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 switch 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 switch 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 switch 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).

2.12.3 Port

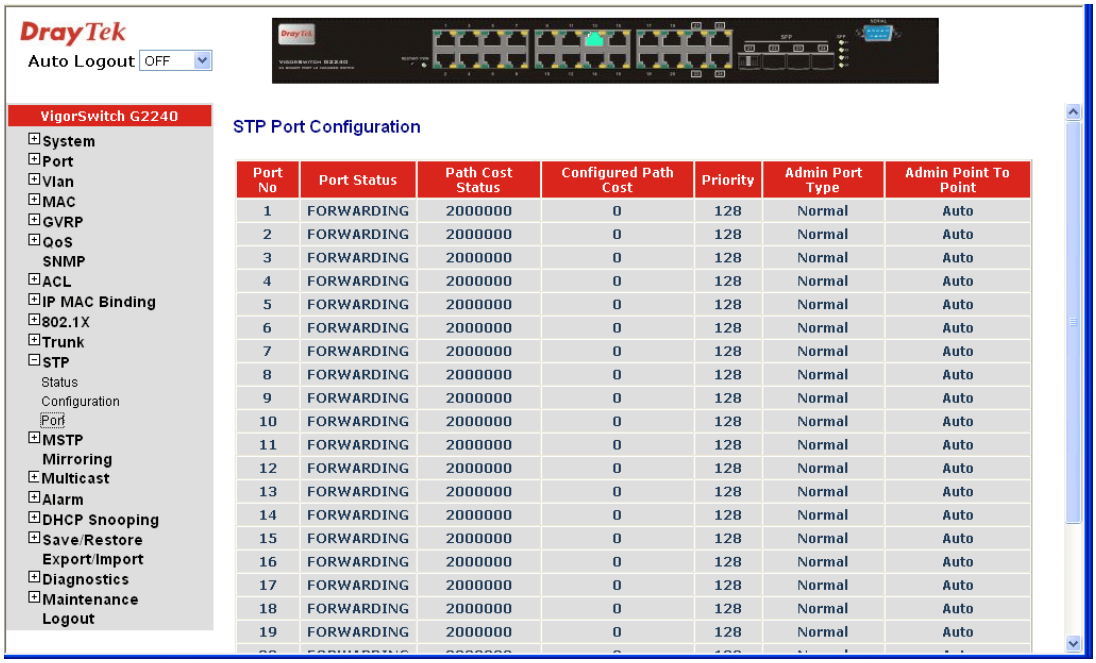
Function name:

STP Port Configuration

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.



Port No	Port Status	Path Cost Status	Configured Path Cost	Priority	Admin Port Type	Admin Point To Point
1	FORWARDING	2000000	0	128	Normal	Auto
2	FORWARDING	2000000	0	128	Normal	Auto
3	FORWARDING	2000000	0	128	Normal	Auto
4	FORWARDING	2000000	0	128	Normal	Auto
5	FORWARDING	2000000	0	128	Normal	Auto
6	FORWARDING	2000000	0	128	Normal	Auto
7	FORWARDING	2000000	0	128	Normal	Auto
8	FORWARDING	2000000	0	128	Normal	Auto
9	FORWARDING	2000000	0	128	Normal	Auto
10	FORWARDING	2000000	0	128	Normal	Auto
11	FORWARDING	2000000	0	128	Normal	Auto
12	FORWARDING	2000000	0	128	Normal	Auto
13	FORWARDING	2000000	0	128	Normal	Auto
14	FORWARDING	2000000	0	128	Normal	Auto
15	FORWARDING	2000000	0	128	Normal	Auto
16	FORWARDING	2000000	0	128	Normal	Auto
17	FORWARDING	2000000	0	128	Normal	Auto
18	FORWARDING	2000000	0	128	Normal	Auto
19	FORWARDING	2000000	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:	To display the Admin port type with “normal”, “None-STP” and “Edge”
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.

2.13 MSTP

The implementation of MSTP is according to IEEE 802.1Q 2005 Clause 13 – Multiple Spanning Tree Protocol. MSTP allows frames assigned to different VLANs to follow separate paths, each based on an independent Multiple Spanning Tree Instance (MSTI), within Multiple Spanning Tree (MST) Regions composed of LANs and or MST Bridges. Proper configuration of MSTP in an 802.1Q VLAN environment can ensure a loop-free data path for a group of vlans within an MSTI. Redundant path and load balancing in vlan environment is also achieved via this feature. A spanning tree instance called CIST (Common and Internal Spanning Tree) always exists. Up to 64 more spanning tree instances (MSTIs) can be provisioned.

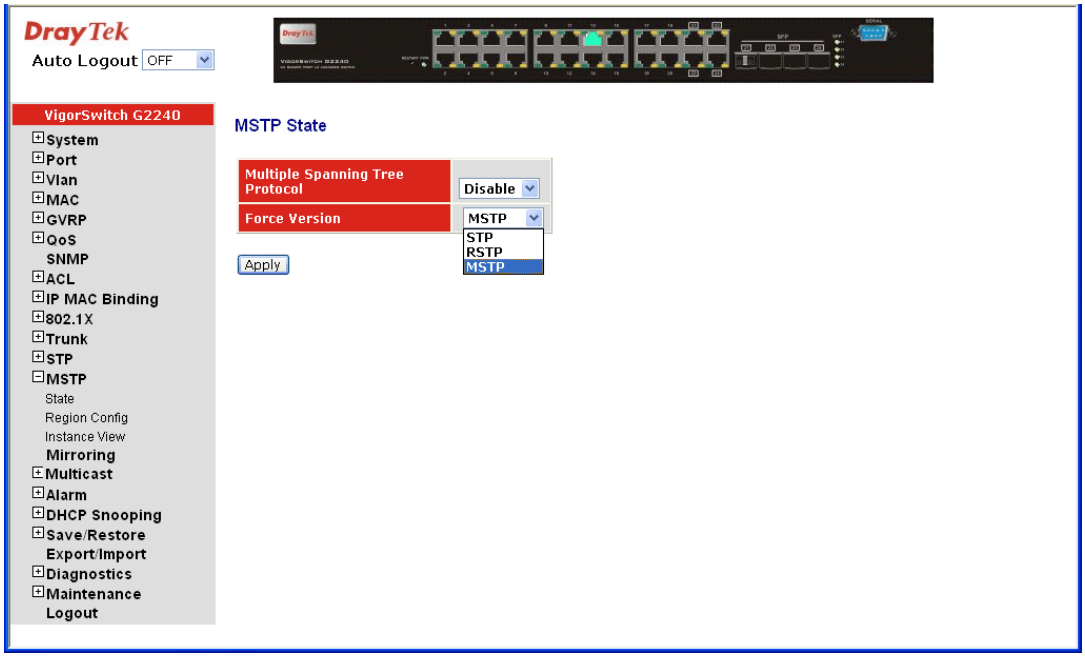
2.13.1 State

Function name:

MSTP State

Function description:

Enable or disable MSTP. And to select a version of Spanning Tree protocol which MSTP should operate on.



Parameter description:

Multiple Spanning Tree Protocol: Disabled / Enabled

Force Version: STP / RSTP / MSTP

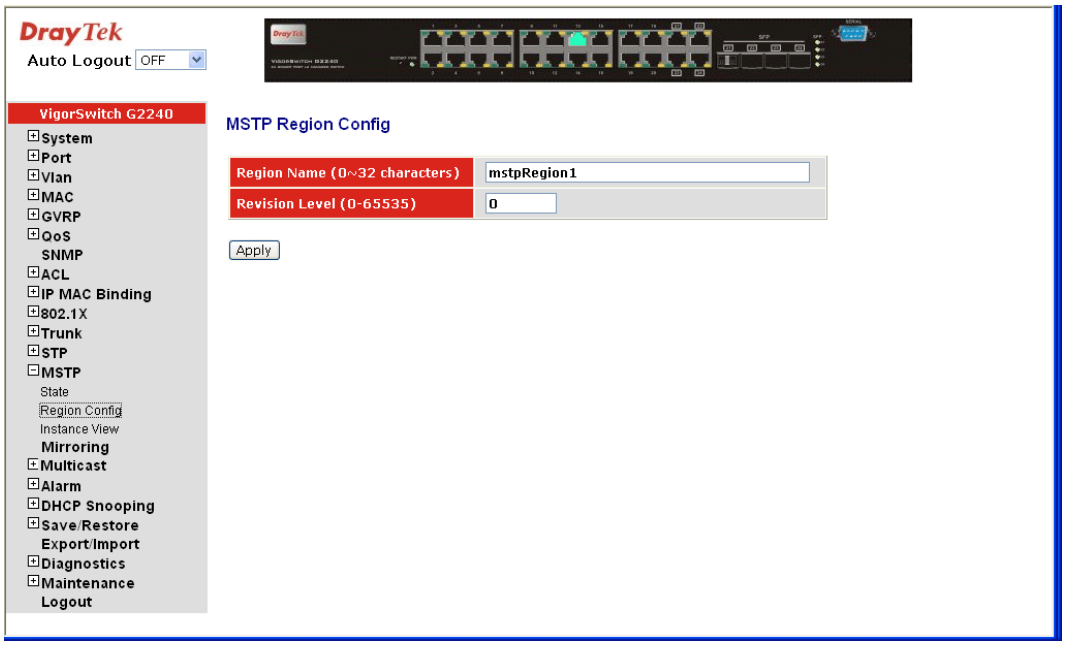
2.13.2 Region Config

Function name:

MSTP Region Config

Function description:

Configure the basic identification of a MSTP bridge. Bridges participating in a common MST region must have the same Region Name and Revision Level.



Parameter description:

Region Name:	0-32 characters (A variable length text string encoded within a fixed field of 32 octets, conforming to RFC 2271's definition of SnmpAdminString.)
Revision Level:	0-65535

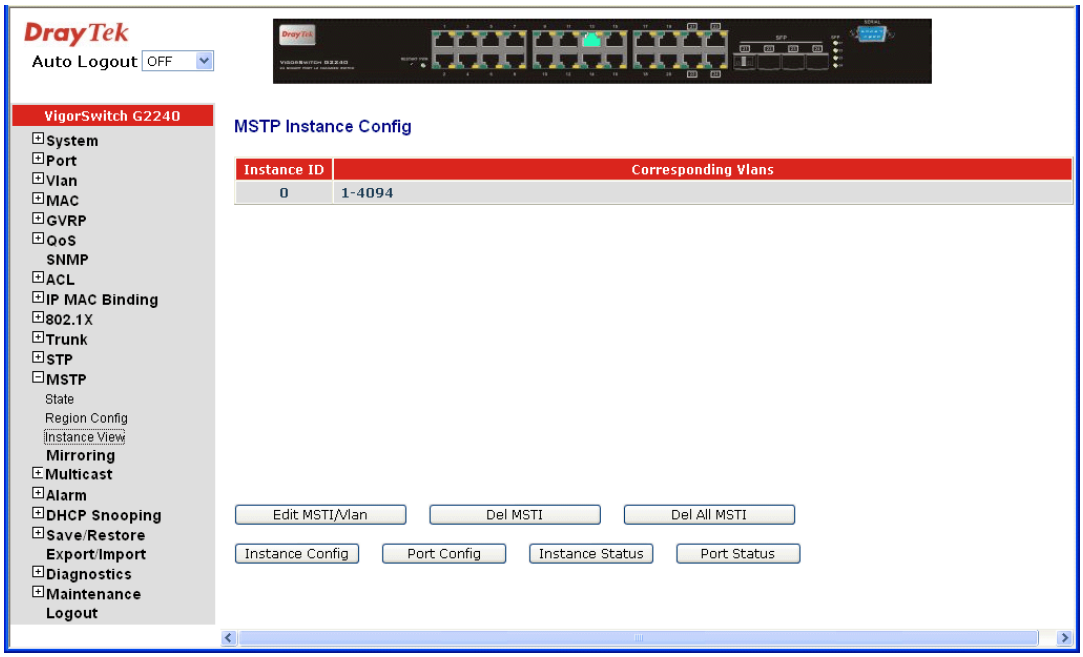
2.13.3 Instance View

Function name:

MSTP Instance View

Function description:

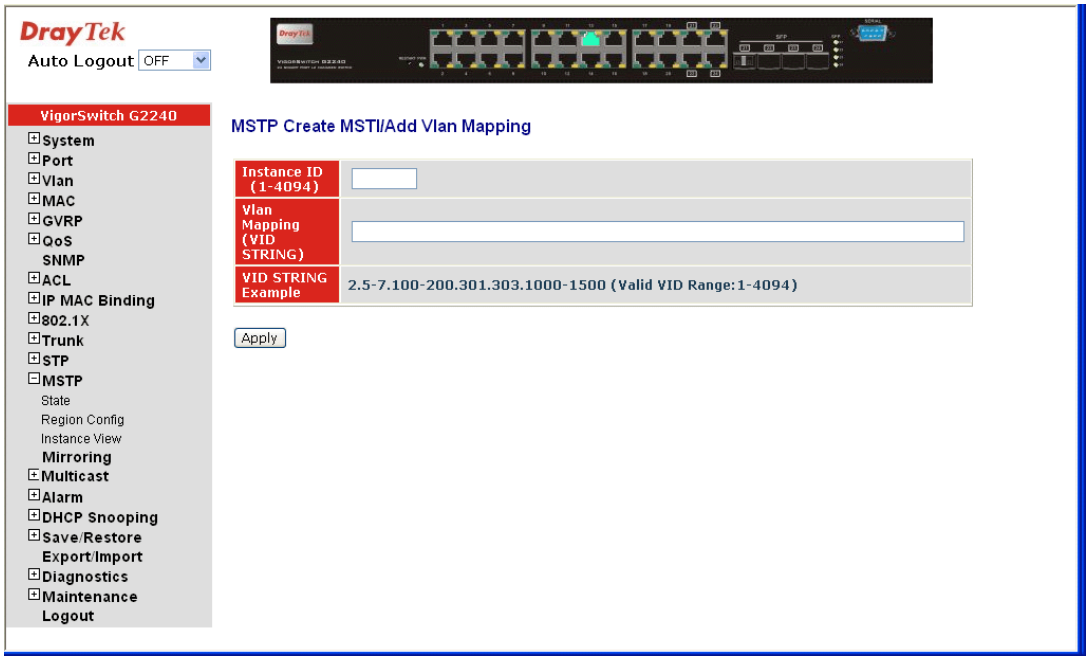
Provide an MST instance table which includes information (vlan membership of a MSTI) of all spanning instances provisioned in the particular MST region which the bridge belongs to. Through this table, additional MSTP configuration data can be applied and MSTP status can be retrieved.



Parameter description:

Instance ID:	Every spanning tree instance need to have a unique instance ID within 0~4095. Instance 0 (CIST) always exists and can not be deleted. Additional spanning instances (MSTIs) can be added or deleted. At least one vlan must be provisioned for an MSTI to declare the need for the MSTI to be existent.
Corresponding Vlans:	0-4095. Multiple vlans can belong to an MSTI. All vlans that are not provisioned through this will be automatically assigned to Instance 0(CIST).
Edit MSTI / Vlan:	Add an MSTI and provide its vlan members or modify vlan members for a specific MSTI.
Del MSTI:	Delete an MSTI.
Del All MSTI:	Delete all provisioned MSTIs at a time.
Instance Config:	Provision spanning tree performance parameters per instance.
Port Config:	Provision spanning tree performance parameters per instance per port.
Instance Status:	Show the status report of a particular spanning tree instance.
Port Status:	Show the status report of all ports regarding a specific spanning tree instance.

- **Edit MSTI / Vlan**

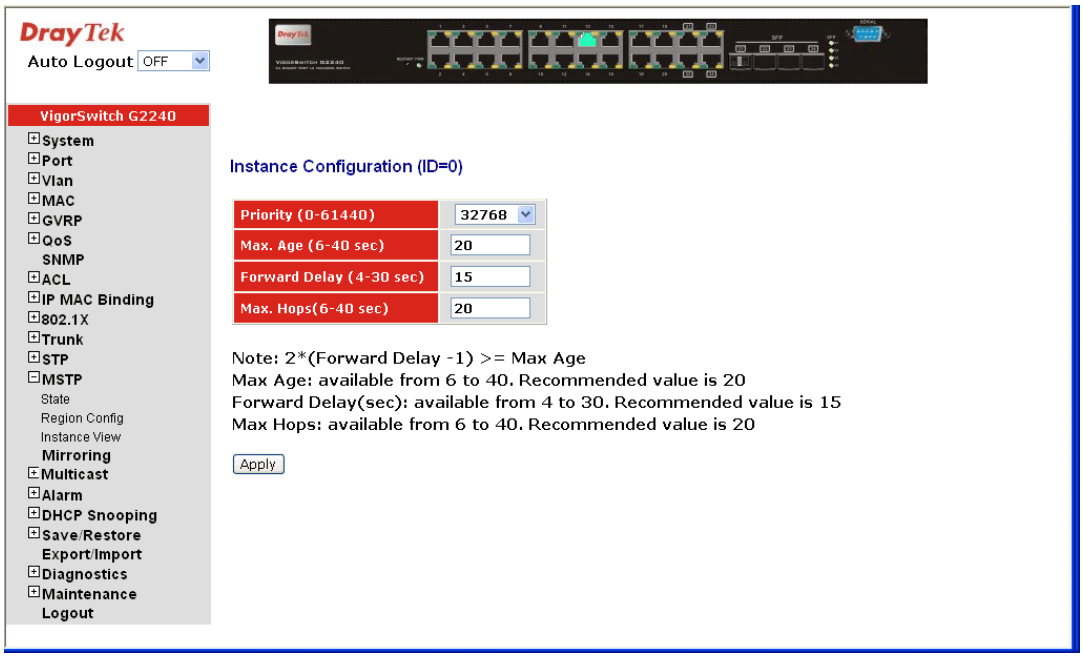


Instance ID: Every spanning tree instance need to have a unique instance ID within 0~4095. Instance 0 (CIST) always exists and can not be deleted. Additional spanning instances (MSTIs) can be added or deleted. At least one vlan must be provisioned for an MSTI to declare the need for the MSTI to be existent.

Vlan Mapping: VID STRING

VID STRING Example: 2.5-7.100-200.301.303.1000-1500 (Valid VID Range:1-4094)

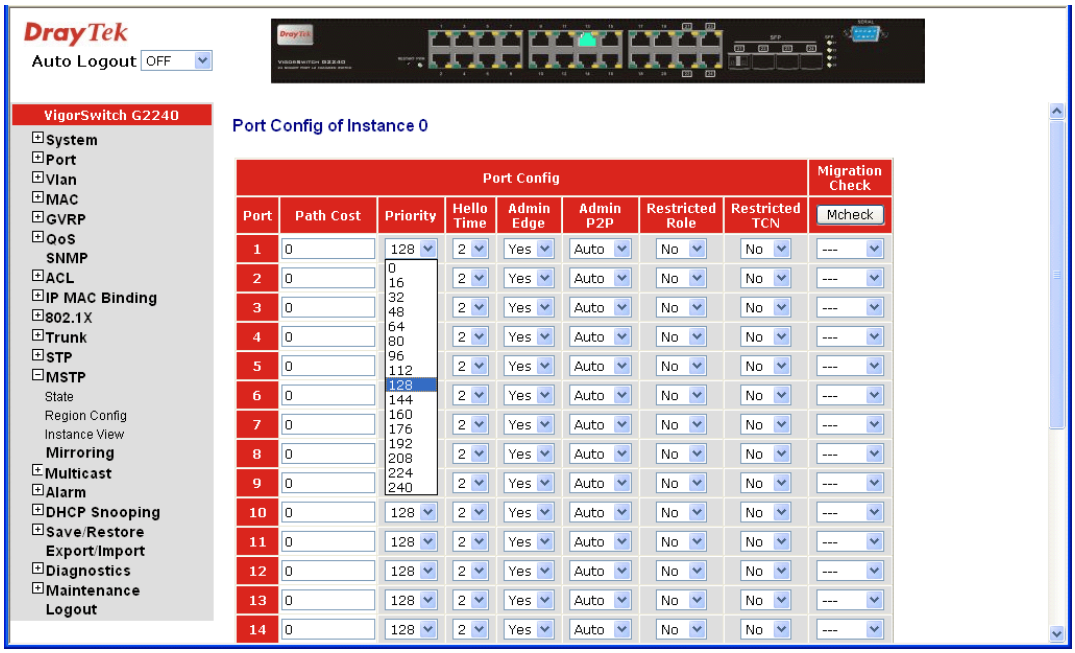
- **Instance Config**



Priority: The priority parameter used in the CIST (Common and Internal Spanning Tree) connection.
0 / 4096 / 8192 / 12288 / 16384 / 20480 / 24576 / 28672 /

	32768 / 36864 / 40960 / 45056 / 49152 / 53248 / 57344 / 61440
MAX. Age:	6-40sec, same definition as in the RSTP protocol.
Forward Delay:	4-30sec, same definition as in the RSTP protocol.
MAX. Hops:	6-40sec. It's a new parameter for the multiple spanning tree protocol. It is used in the internal spanning tree instances. "CIST Remaining Hops" or "MSTI Remaining Hops" in the Spanning tree protocol message would decreased by one when the message is propagated to the neighboring bridge. If the Remaining Hops in a message is zero, the message (BPDU) would be regarded as invalid. Max Hops is used to specify the initial value of the Remaining Hops for Regional Root Bridge (Either CIST Regional Root or MSTI Regional Root)

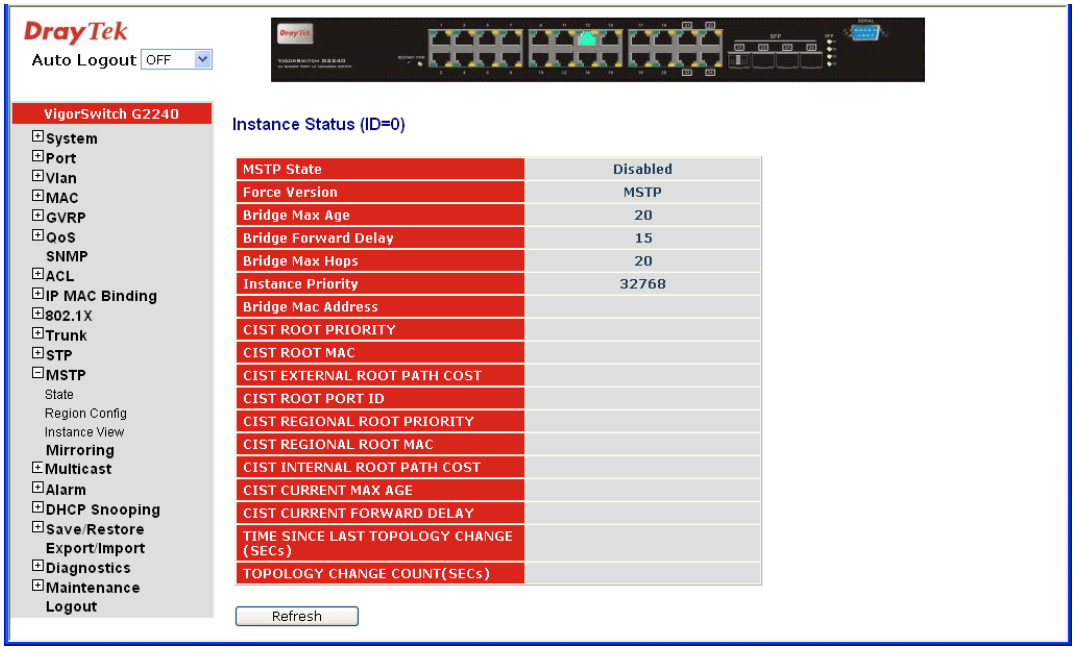
- **Port Config**



Port:	1-24
Path Cost:	1 – 200,000,000 The same definition as in the RSTP specification. But in MSTP, this parameter can be respectively applied to ports of CIST and ports of any MSTI.
Priority:	0 / 16 / 32 / 48 / 64 / 80 / 96 / 112 / 128 / 144 / 160 / 176 / 192 / 208 / 224 / 240 The same definition as in the RSTP specification. But in MSTP, this parameter can be respectively applied to ports of CIST and ports of any MSTI.
Hello Time:	1 / 2 In contrast with RSTP, Hello Time in MSTP is a per port setting for the CIST.
Admin Edge:	Yes / No The same definition as in the RSTP specification for the CIST ports.

Admin P2P:	Auto / True / False The same definition as in the RSTP specification for the CIST ports.
Restricted Role:	Yes / No If “Yes” causes the Port not to be selected as Root Port for the CIST or any MSTI, even it has the best spanning tree priority vector. Such a Port will be selected as an Alternate Port after the Root Port has been selected. This parameter is “No” by default. If set, it can cause lack of spanning tree connectivity. It is set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator.
Restricted TCN:	Yes / No If “Yes” causes the Port not to propagate received topology change notifications and topology changes to other Ports. This parameter is “No” by default. If set it can cause temporary loss of connectivity after changes in a spanning trees active topology as a result of persistent incorrectly learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator. or the status of MAC operation for the attached LANs transitions frequently.
Mcheck:	The same definition as in the RSTP specification for the CIST ports.

- **Instance Status**



MSTP State:	MSTP protocol is Enable or Disable.
Force Version:	It shows the current spanning tree protocol version configured.
Bridge Max Age:	It shows the Max Age setting of the bridge itself.

Bridge Forward Delay: It shows the Forward Delay setting of the bridge itself.

Bridge Max Hops: It shows the Max Hops setting of the bridge itself.

Instance Priority: Spanning tree priority value for a specific tree instance (CIST or MSTI)

Bridge Mac Address: The Mac Address of the bridge itself.

CIST ROOT PRIORITY: Spanning tree priority value of the CIST root bridge

CIST ROOT MAC: Mac Address of the CIST root bridge

CIST EXTERNAL ROOT PATH COST: Root path cost value from the point of view of the bridge's MST region.

CIST ROOT PORT ID: The port ID of the bridge's root port. In MSTP, peer port of a root port may reside in different MST region or in the same MST region. The first case indicates that the root port's owner is the CIST regional root bridge.

CIST REGIONAL ROOT PRIORITY: Spanning tree priority value of the CIST regional root bridge. Note that CIST Regional Root bridge is different from CIST Root bridge. One exception is that when a bridge belonging to an MST region happens to be the root bridge of the CST (Common Spanning Tree). An MST Region in the CST can be regarded as a common RSTP bridge. The IST(Internal Spanning Tree) and MSTIs are transparent to bridges outside this region.

CIST REGIONAL ROOT MAC: Mac Address of the CIST regional root bridge.

CIST INTERNAL ROOT PATH COST: Root path cost value from the point of view of the bridges inside the IST.

CIST CURRENT MAX AGE: Max Age of the CIST Root bridge.

CIST CURRENT FORWARD DELAY: Forward Delay of the CIST Root bridge.

TIME SINCE LAST TOPOLOGY CHANGE (SECs): Time Since Last Topology Change is the elapsed time in unit of seconds for a bunch of "Topology Change and(or) Topology Change Notification receiving" to occur. When new series of Topology Changes occur again, this counter will be reset to 0.

TOPOLOGY CHANGE COUNT(SECs): The per spanning tree instance 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 there is no topology change occurring and no more topology change notification received, the Topology Change count will be reset to 0.

2.14 Mirroring

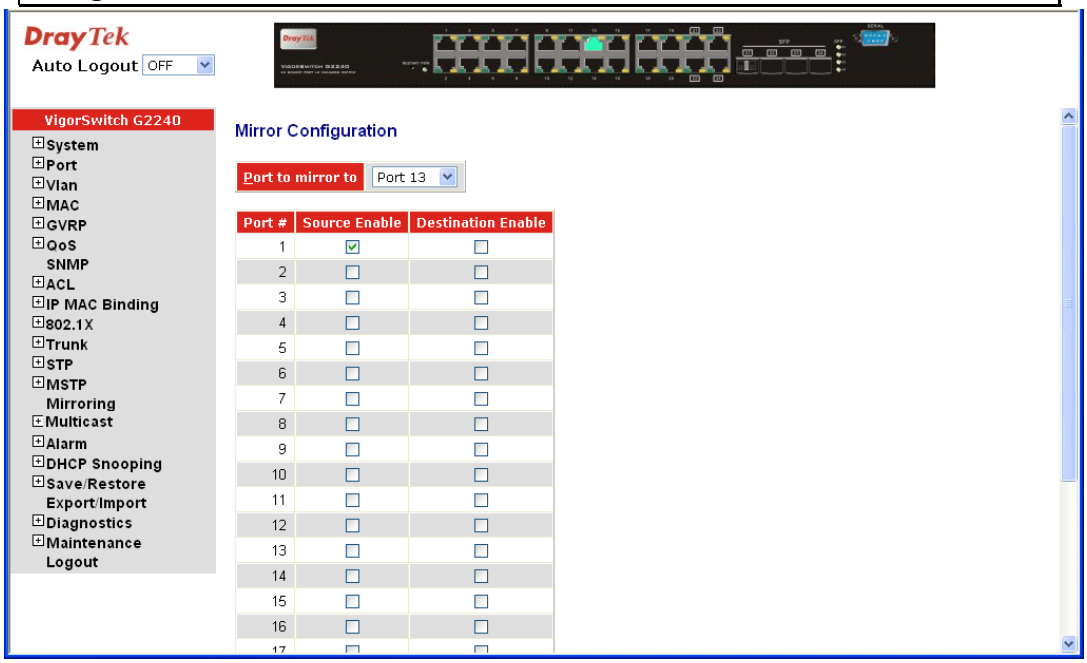
Function name:

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.

> **Note:** When configure the mirror function, you should avoid setting a port to be a sniffer port and aggregated port at the same time. It will cause something wrong.



Parameter description:

Port to mirror to:	Set the monitoring port. Range: Disabled / Port 1-24
Port #:	Range: 1-24, select the monitored ports.
Source Enable:	The source enable means the monitored port ingress traffic will be copied to monitoring port.
Destination Enable:	The destination enable means the monitored port egress traffic will be copied to monitoring port

2.15 Multicast

The function is used 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.

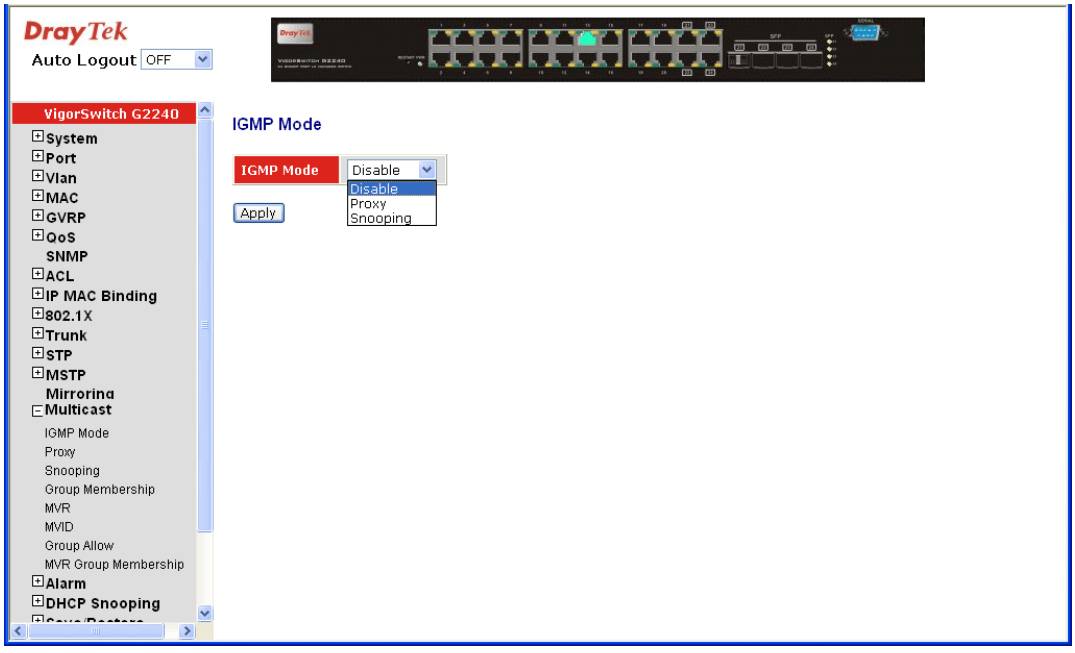
2.15.1 IGMP Mode

Function name:

IGMP Mode

Function description:

IGMP mode enables the switch to issue IGMP function that you enable IGMP proxy or snooping on the switch, which connects to a router closer to the root of the tree. This interface is the *upstream interface*. The router on the upstream interface should be running IGMP.



Parameter description:

IGMP Mode: Scroll the IGMP mode with **"Disable"**, **"Proxy"** or **"Snooping".**

2.15.2 Proxy

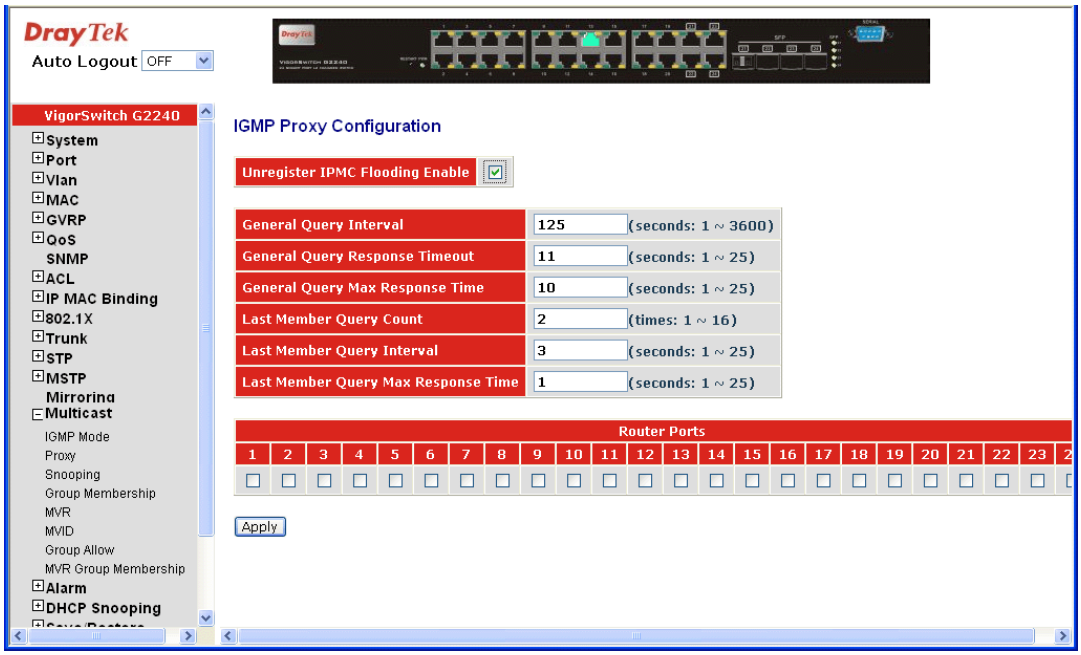
Function name:

IGMP Proxy Configuration

Function description:

IGMP proxy enables the switch to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The switch acts as a *proxy* for its hosts.

You enable IGMP proxy on the switch, which connects to a router closer to the root of the tree. This interface is the *upstream interface*. The router on the upstream interface should be running IGMP.



Parameter description:

Unregister IPMC Flooding Enable: Enable to control the traffic that doesn't appear in the multicast table for flooding

General Query Interval: Set the switch sending general query period time. (Available: 1~3600 secs)

General Query Response Timeout: Make the switch to determine the client living time. (Available: 1~25 secs)

General Query Max Response Time: Set max response code value of the general query packet. (Available: 1~25 secs)

Last Member Query Count: Set the frequency. When Switch received IGMP leave, the switch will send specific query frequency. (Available: 1~16 secs)

Last Member Query Interval: Set the frequency that the Switch sends specific query period time. (Available: 1~25 secs)

Last Member Query Max Response Time: Set the max response code value in the specific query packet (Available: 1~25 secs)

Update Interval of Router Port: Set the period time for the interface ever received IGMP query packet. (Available: 1~3600 secs)

Router Ports: Set the interface that connects to IGMP Router. IGMP packets can be received and sent out via the router port of this switch.Router ports may be only or more than one.

Apply: Save all configurations.

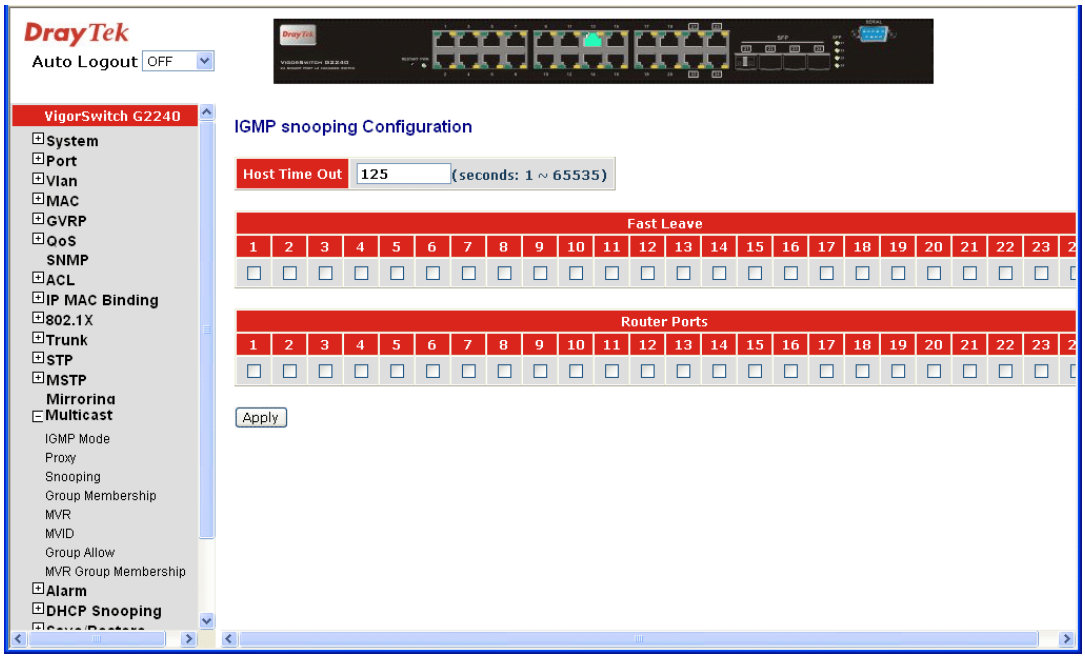
2.15.3 Snooping

Function name:

IGMP Snooping Configuration

Function description:

IGMP Snooping enables the switch to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The switch acts with Snooping mode for its hosts. You enable IGMP Snooping on the switch.



Parameter description:

Host Time Out:	Set the IGMP Snooping enable and the Host packet received by Switch timeout period. The unit is second and time range is from 1 to 65535. The default is 125 seconds.
Fast Leave:	Set which port wants to enable the Fast leave mode with IGMP snooping mode.
Router Ports:	Set which port wants to be a Router Port with IGMP snooping mode.

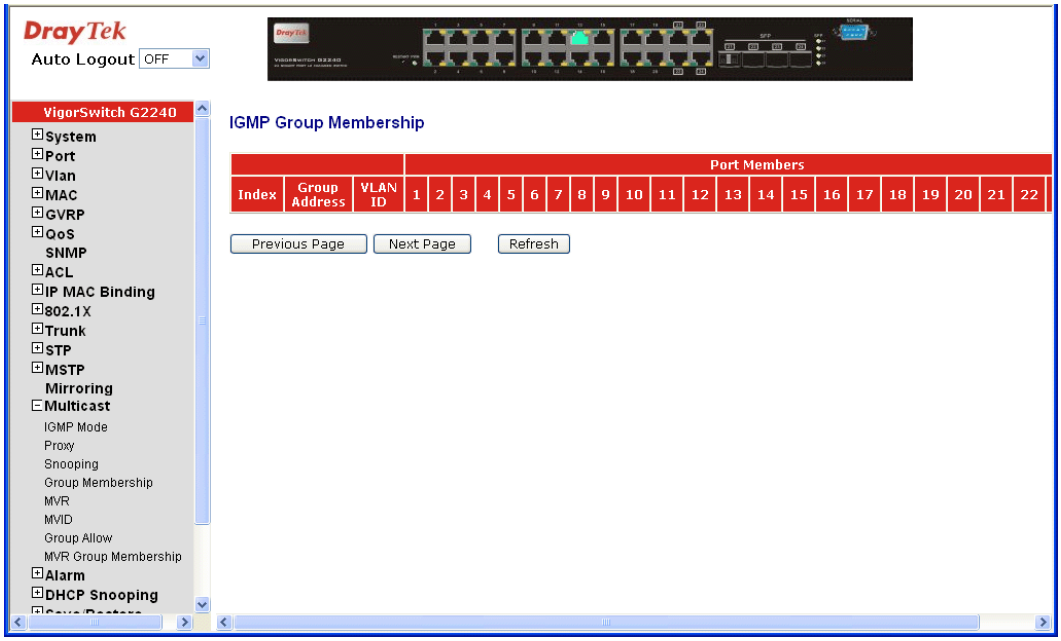
2.15.4 IGMP Group Membership

Function name:

IGMP Group Membership

Function description:

Show the information for IGMP group members, the you can edit the parameters for IGMP groups and members in the web user interface.



Parameter description:

Index:	Display current built-up multicast group entry index.
Group Address:	Display current built-up multicast Group Address.
VLAN ID:	Display current built-up multicast VLAN ID.
Port Members:	Display current built-up multicast port members
Previous Page:	Display previous page context.
Next Page:	Display next page context.
Refresh:	Update multicast group membership.

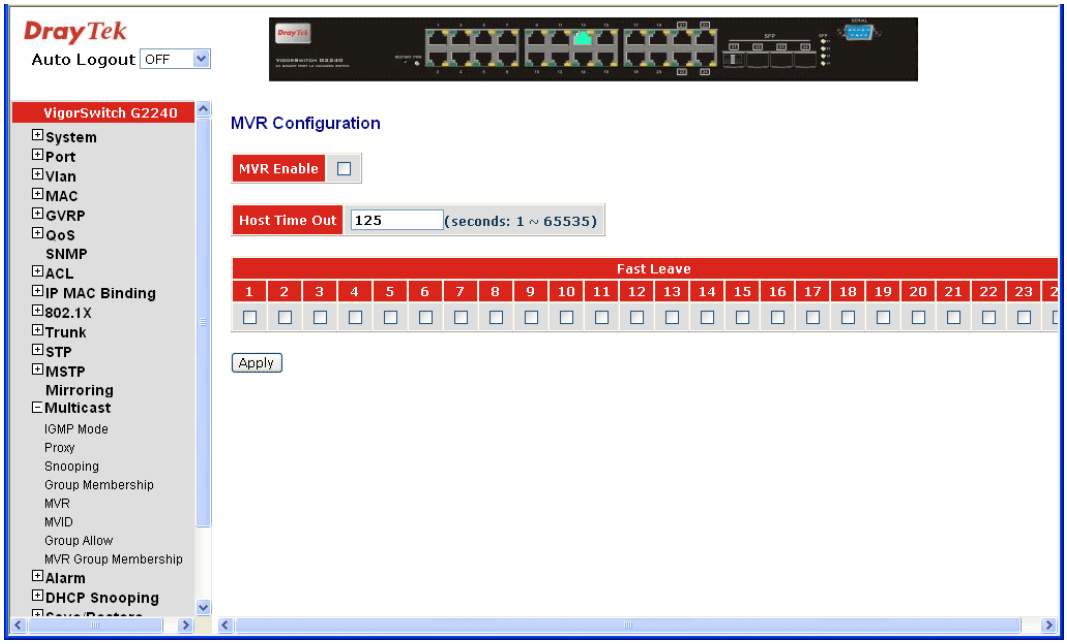
2.15.5 MVR

Function name:

MVR Configuration

Function description:

Multicast VLAN Registration (MVR) routes packets received in a multicast source VLAN to one or more receive VLANs. Clients are in the receive VLANs and the multicast server is in the source VLAN. Multicast routing has to be disabled when MVR is enabled. Refer to the configuration guide at Understanding Multicast VLAN Registration for more information on MVR.



Parameter description:

MVR Enable:	Set the MVR function enable.
Host Time Out:	Set the MVR function enable and the Host packet received by Switch timeout period. The unit is second and time range is from 1 to 65535. The default is 125 seconds.
Fast Leave:	Set which port want to enable the Fast leave mode with IGMP snooping mode.

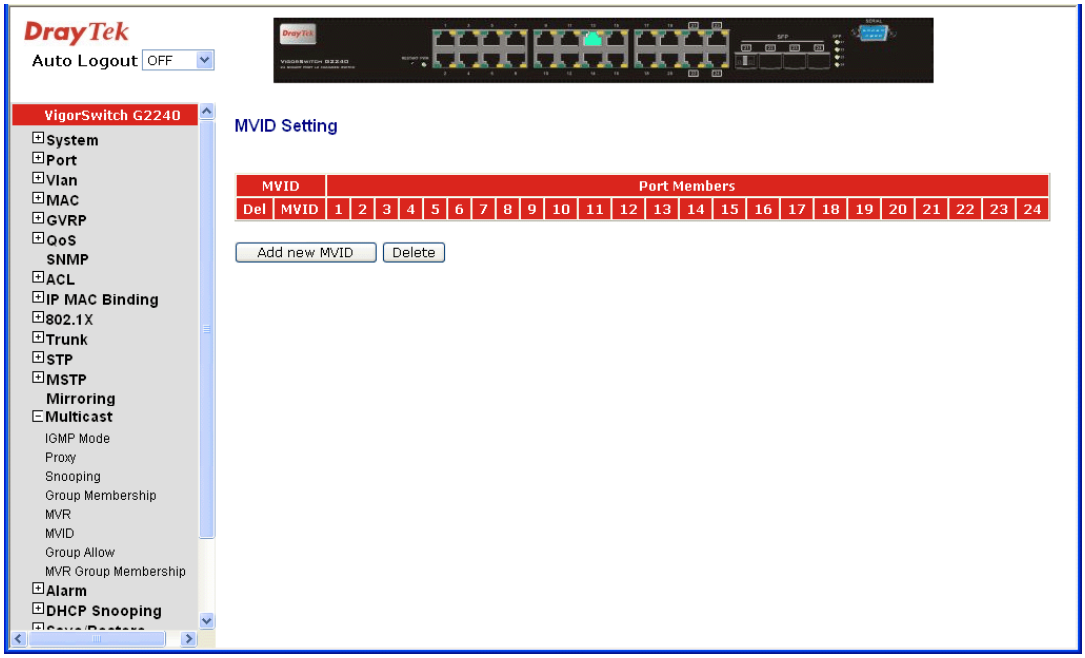
2.15.6 MVID

Function name:

MVID Setting

Function description:

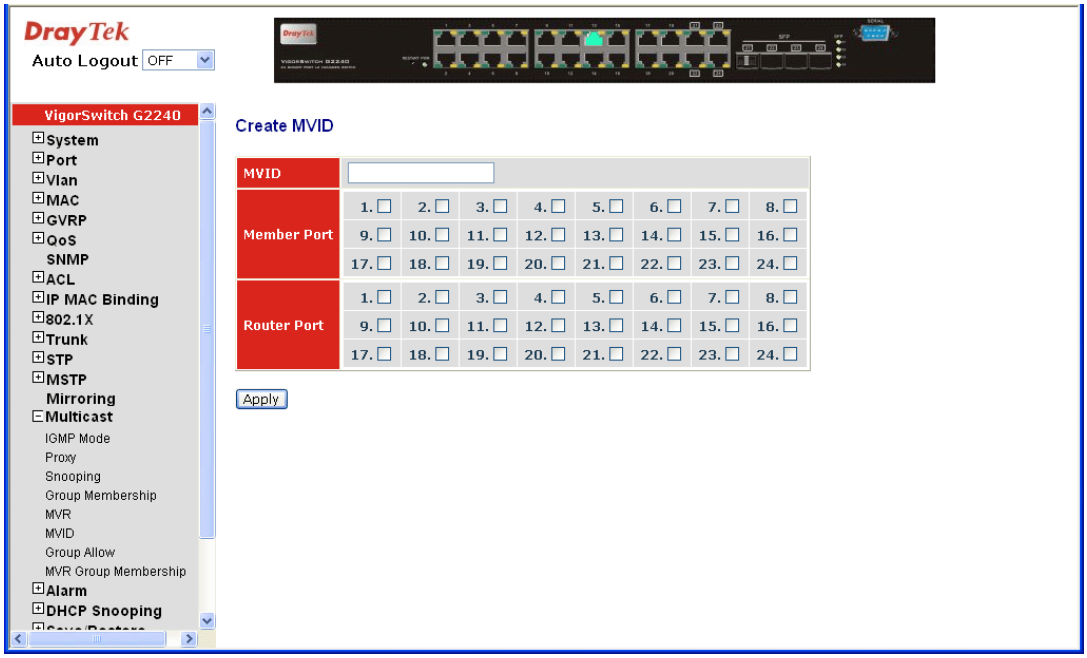
Set the MVR Group member ID (MVID) entry with the Member port and Router Port.



Parameter description:

MVID:	Display the MVR Group ID.
Port Members:	Display which port will join the MVR Group member
Add new MVID:	Create a new MVID entry.
Delete:	Delete the existed MVID entry.

To add a new MVID, click Add new MVID. The following screen will appear.



Parameter description:

MVID:	Input MVR group ID for MVID.
Member Port:	Evoke which port will join the MVR Group member.
Router Port:	Evoke which port will become the MVR Group router port.

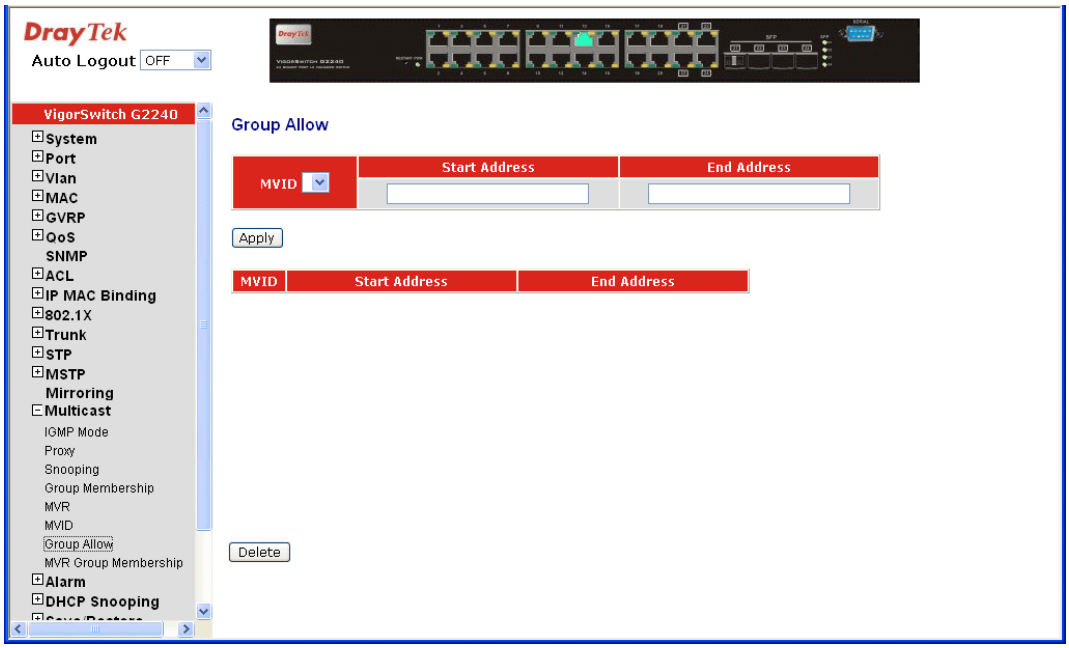
2.15.7 Group Allow

Function name:

Group Allow

Function description:

The Group Allow function allows the Multicast VLAN Registration to set up the IP multicast group filtering conditions. IGMP join behavior that meet the items you set up will be joined or formed the multicast group.



Parameter description:

MVID:	Evoke the valid MVID which you set on the Switch.
Start Address:	The switch supports managed valid IP range. You can assign effective IP range. The valid start Address is 224.0.0.0~239.255.255.254.
End Address:	The switch supports managed valid IP range. You can assign effective IP range. The valid End Address is 224.0.0.1~239.255.255.255.

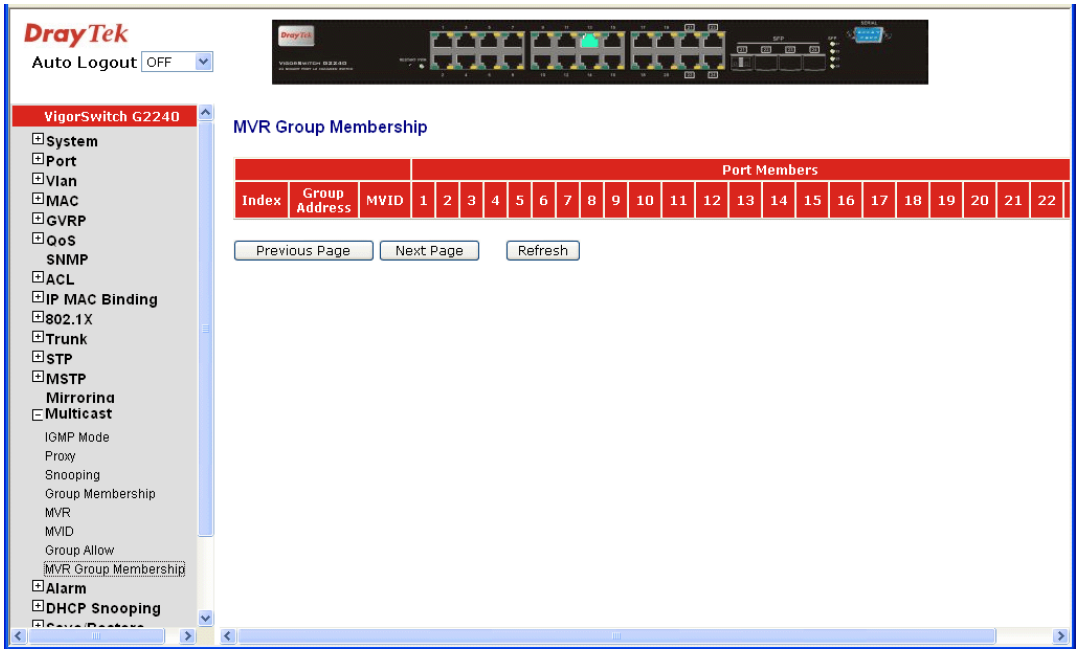
2.15.8 MVR Group Membership

Function name:

MVR Group Membership

Function description:

Display the MVR Group Membership information.



Parameter description:

Index:	Display the MVR Group entry index which you create on the Switch.
Group Address:	Display the MVR Group Address which you set on the Switch.
MVID:	Display the MVR Group ID which you set on the Switch.
Previous Page:	Display previous page context.
Next Page:	Display next page context.
Refresh:	Update multicast group membership.

2.16 Alarm Configuration

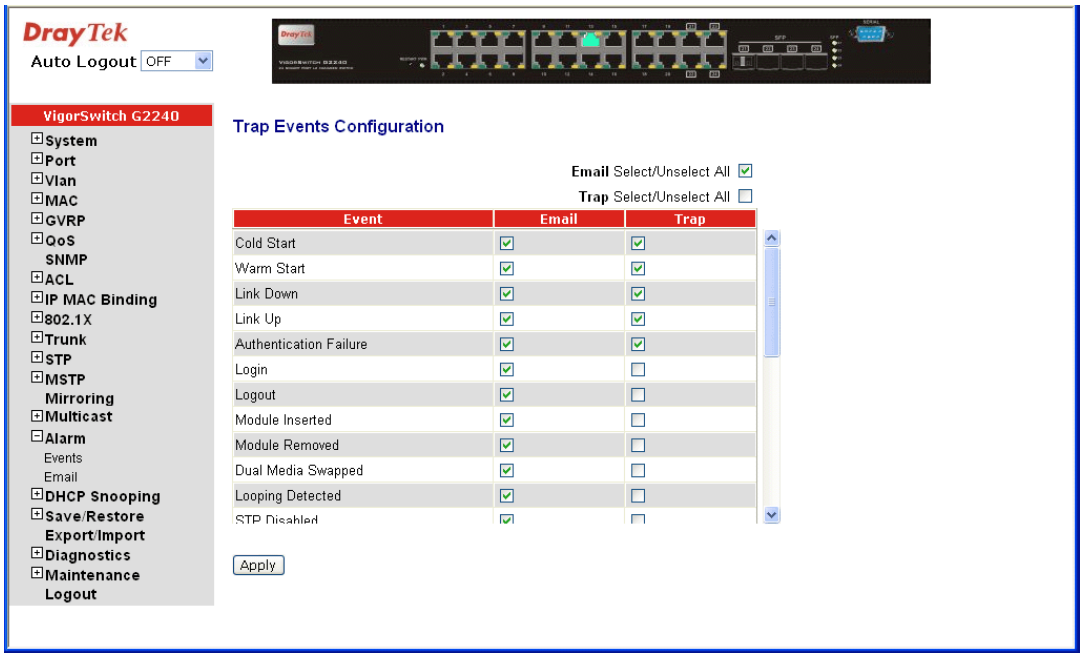
2.16.1 Events Configuration

Function name:

Trap 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.



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

2.16.2 Email

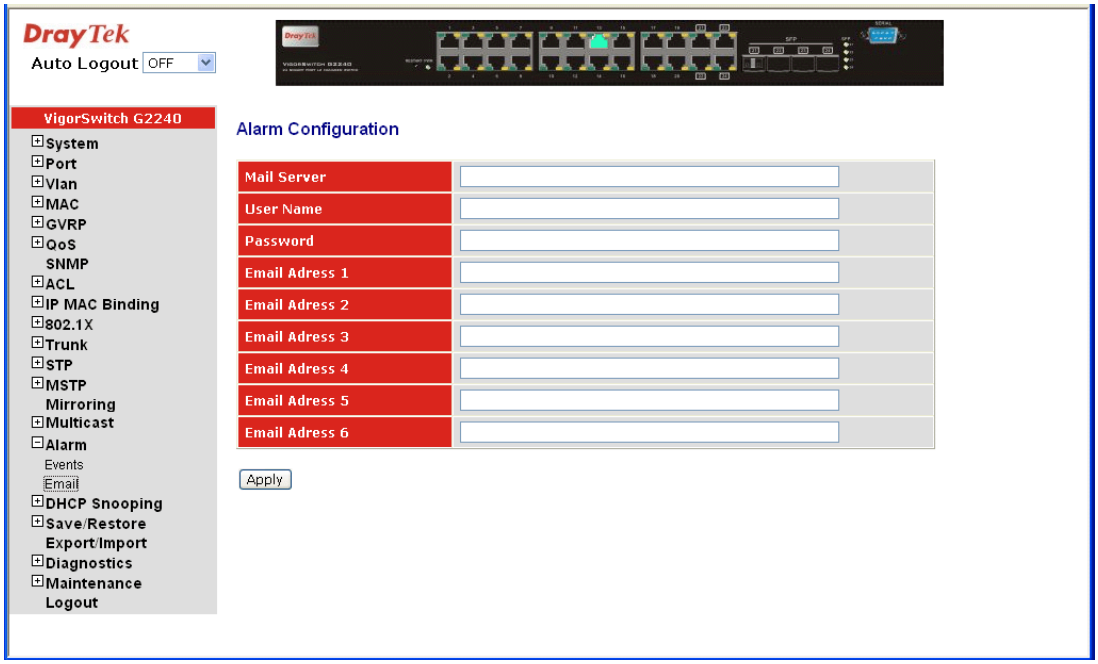
Function name:

Email Configuration

Function description:

Alarm configuration is used to configure the persons who should receive the alarm message via either email. It depends on your settings. An email address or a mobile phone number has to be set in the web page of alarm configuration. 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.



Parameter description:

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.

2.17 DHCP Snooping

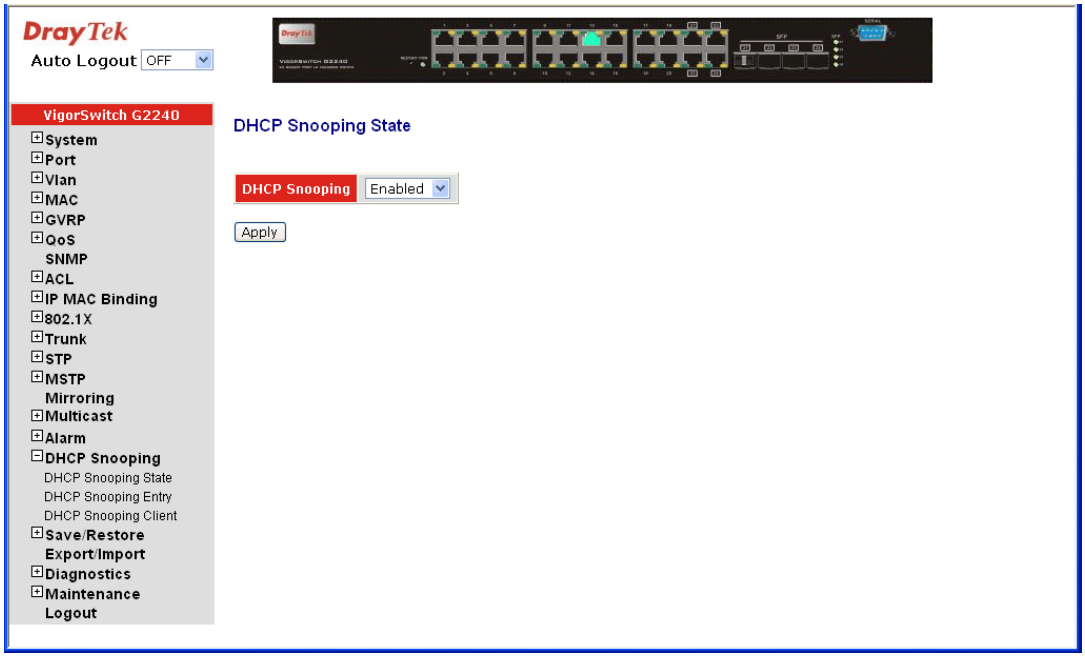
2.17.1 DHCP Snooping State

Function name:

DHCP Snooping State

Function description:

The addresses assigned to DHCP clients on unsecure ports can be carefully controlled using the dynamic bindings registered with DHCP Snooping. DHCP snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port.



DHCP Snooping: Set to disable or enable the DHCP snooping function on the switch, the default is ***Disabled.***

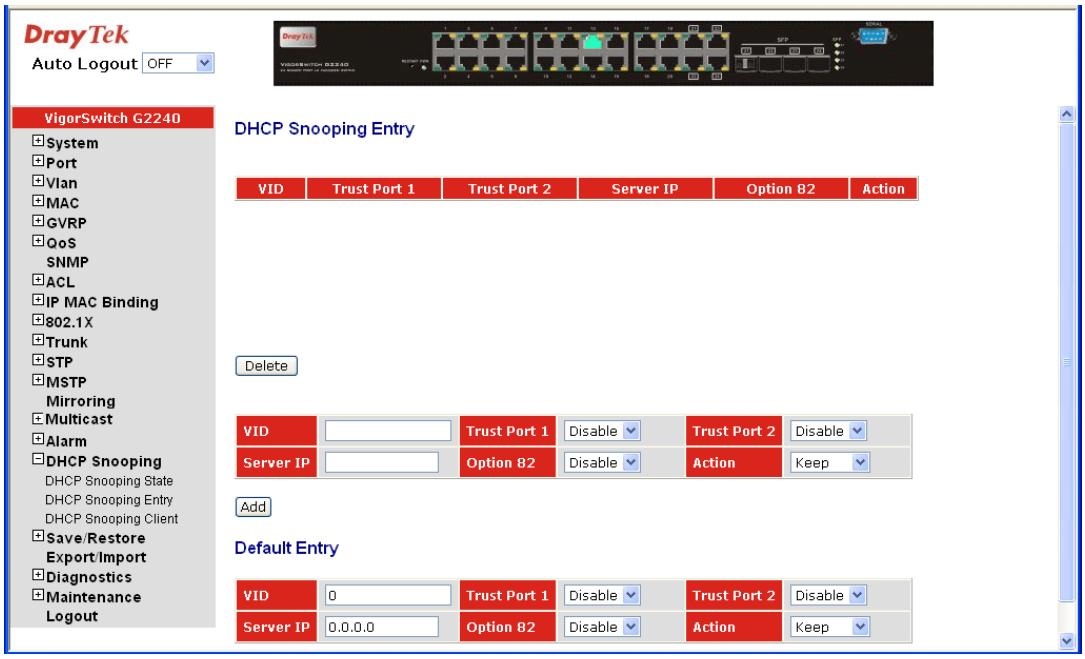
2.17.2 DHCP Snooping Entry

Function name:

DHCP Snooping Entry

Function description:

DHCP snooping Entry allows a switch to add the a trust DHCP server and 2 trust port to build the DHCP snooping available entry. This information can be useful in tracking an IP address back to a physical port and enable or disable the DHCP Option 82.



VID: When DHCP snooping is enabled, and enabled on the specified VLAN, DHCP packet filtering will be performed on any un-trusted ports within the VLAN. It set a available

	VLAN ID to enable the DHCP snooping on VLAN interface.
Trust Port 1:	If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a trusted por. Available ports are from 1 to 24.
Trust port 2	It sets a trust port 2. Available ports are from 1 to 24.
Server IP:	Set a trust DHCP Server IP address for DHCP Snooping.
Option 82:	Set the DHCP Option 82 function on the switch, default is Disable.
Action:	Set the switch when received a client DHCP request packet then action for filtering. Available action: keep/ drop / replace.
Delete:	To delete a DHCP snooping entry which you set on the Switch.
Add:	To create a DHCP snooping entry on the Switch
Apply:	To save the configuration to Switch RAM.

Note: Filtering rules are implemented as follows:

- If the DHCP snooping is disabled, all DHCP packets are forwarded.
- If DHCP snooping is enabled and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a trusted port.
- If DHCP snooping is enabled and also enabled on the VLAN where the DHCP packet is received, but the port is not trusted, it is processed as follows:
  - If the DHCP packet is a reply packet from a DHCP server, the packet is dropped.

  - If the DHCP packet is from a client, such as a DISCOVER, REQUEST INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled. However, if MAC address verification is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.

  - If the DHCP packet is not a recognizable type, it is dropped.
- If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.
- If a DHCP packet is from server is received on a trusted port, it will be forwarded to both trusted and un-trusted ports in the same VLAN.

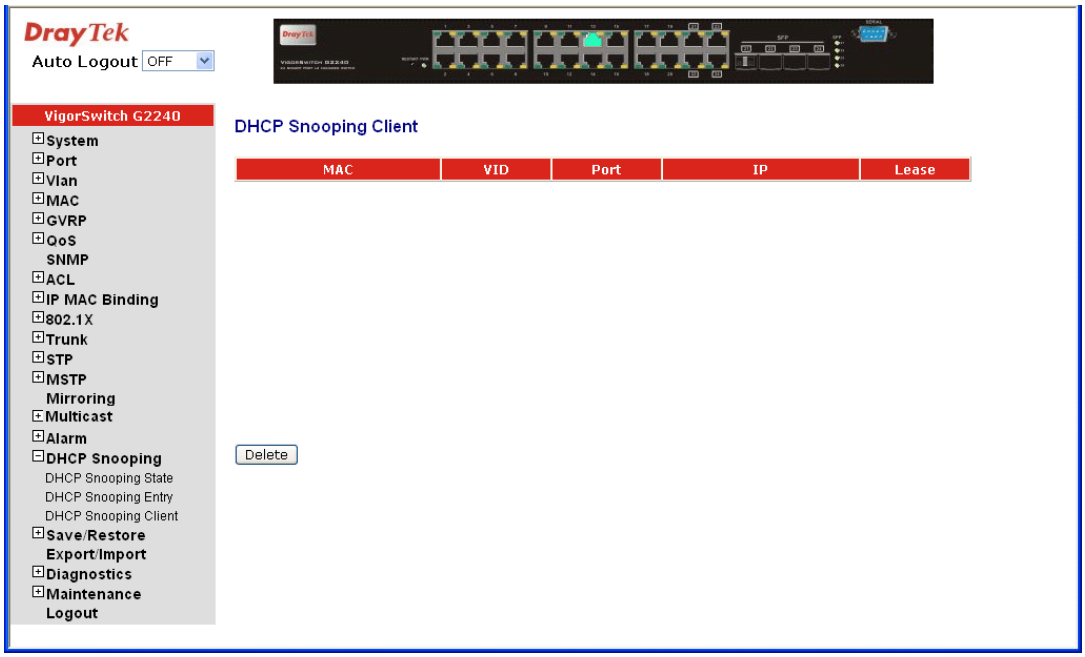
2.17.3 DHCP Snooping Client

Function name:

DHCP Snooping Client

Function description:

Display the DHCP snooping client.



MAC:	Display the DHCP snooping client's MAC address
VID:	Display the DHCP snooping client's VLAN ID.
Port:	Display the DHCP snooping client's port.
IP:	Display the DHCP snooping client's IP address.
Lease:	Display the DHCP snooping client's lease.
Delete:	Delete a DHCP snooping Client's entry which you set on the Switch. When you choice an entry want to delete.

2.18 Save/Restore

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.

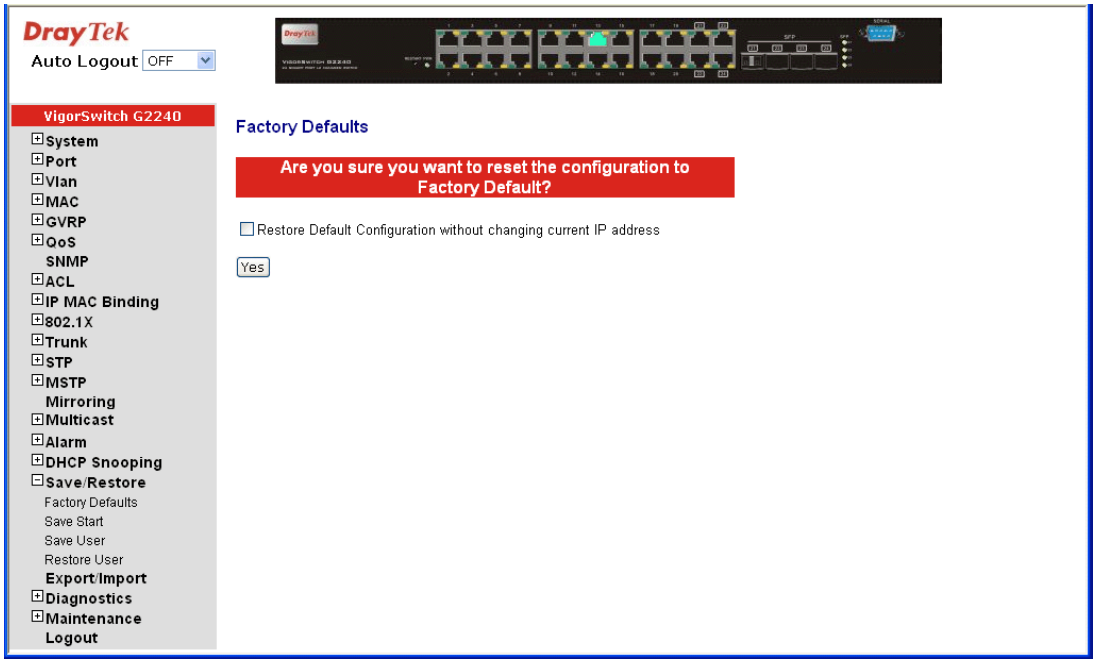
2.18.1 Factory Defaults

Function name:

Restore Default Configuration (includes default IP address)

Function description:

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



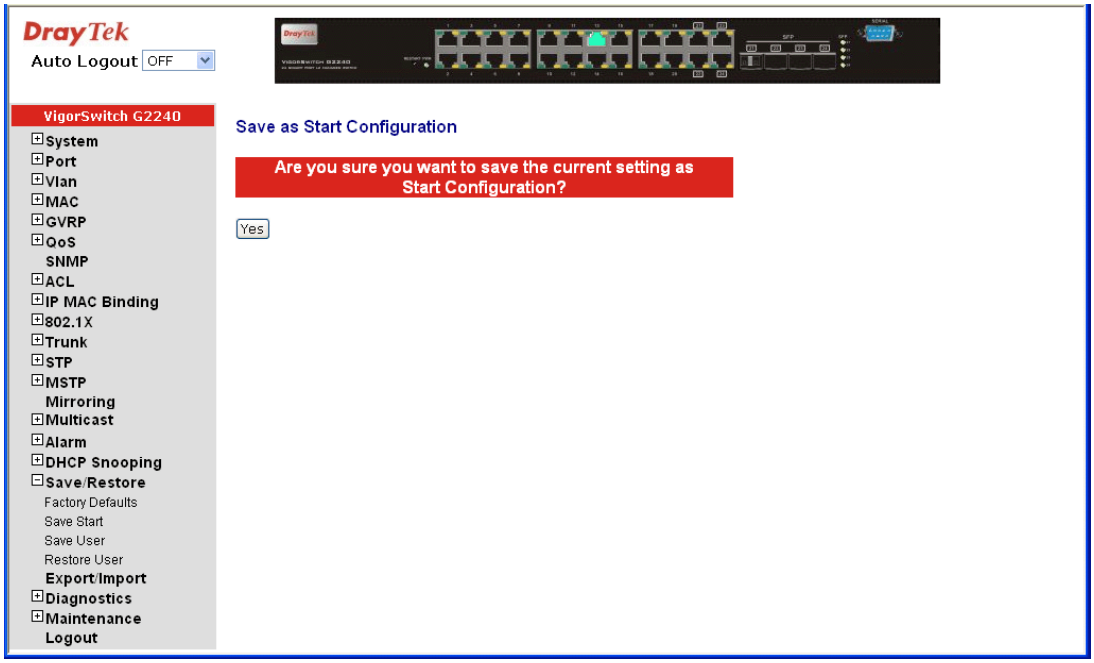
2.18.2 Save Start

Function name:

Save As Start Configuration

Function description:

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



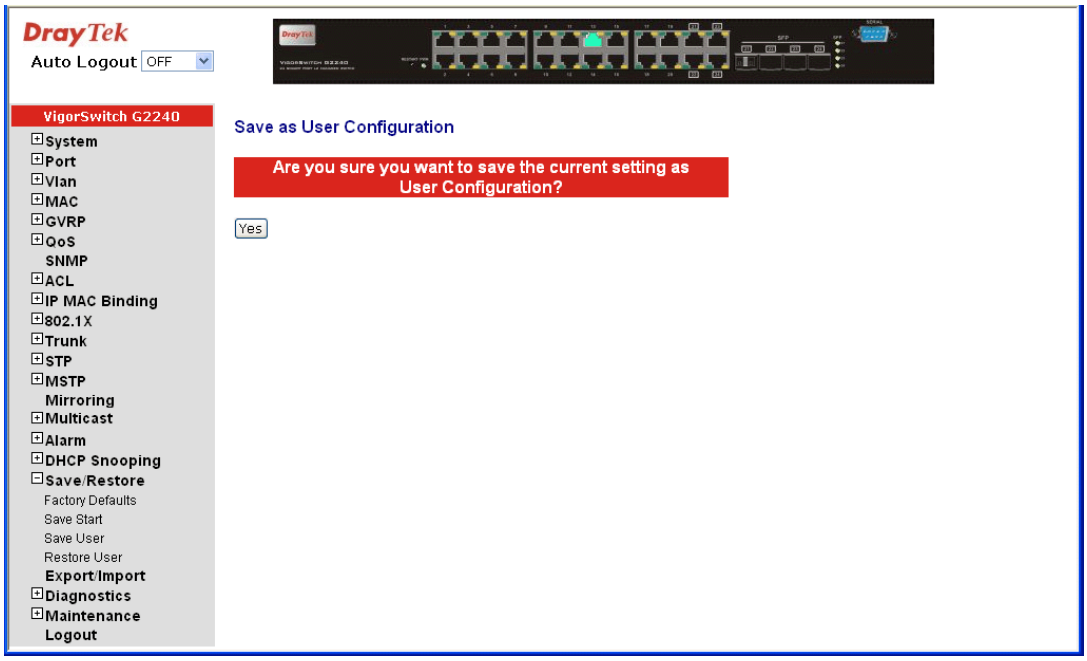
2.18.3 Save User

Function name:

Save As User Configuration

Function description:

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



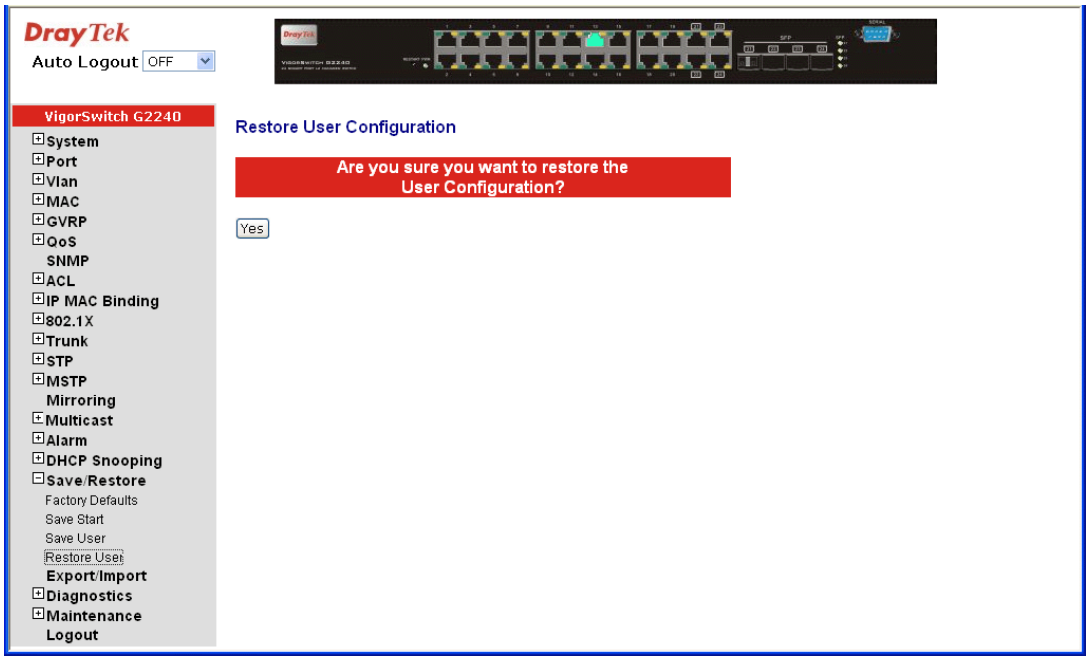
2.18.4 Restore User

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.



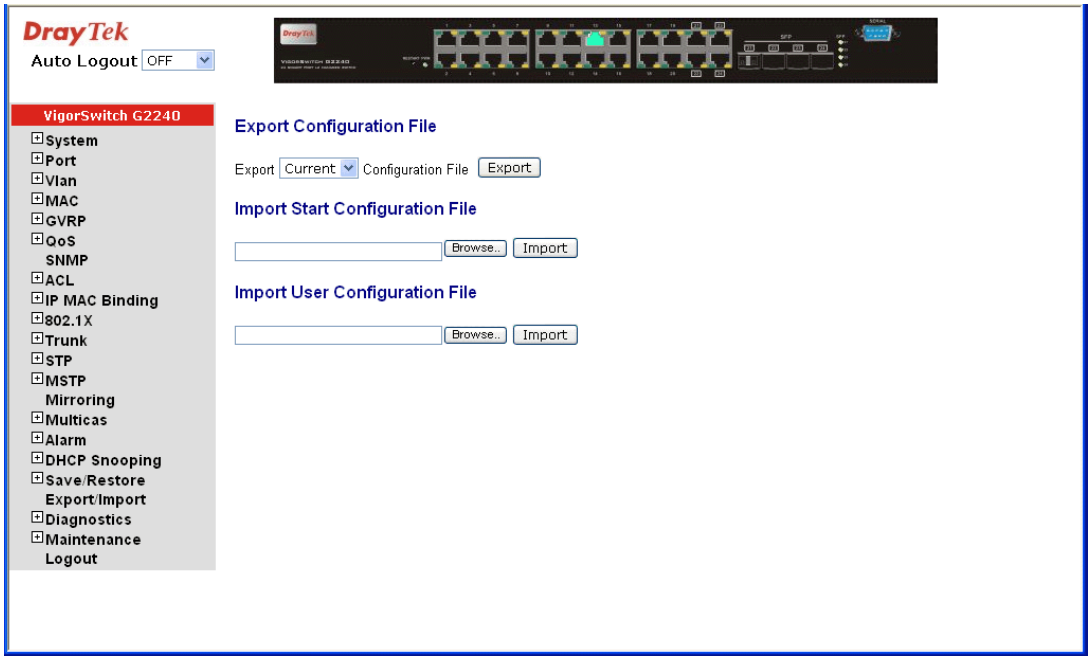
2.19 Export/Import

Function name:

Export/Import Configuration

Function description:

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



Parameter description:

Export:	Current – Export the current configuration on switch from Flash. User – Export the configuration what user just configure on switch without save to Flash.
Import Start Configuration:	Import “Save As Start’s configuration” file stored in the flash.
Import User Configuration:	Import “Save As User’s configuration” file stored in the flash.

2.20 Diagnostics

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

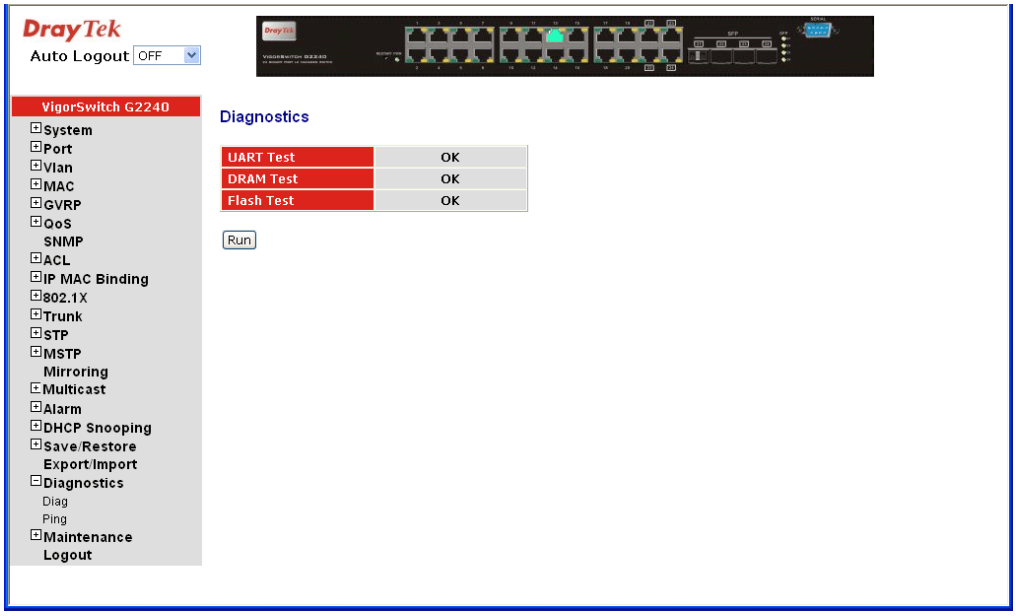
2.20.1 Diagnostics

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 UART test, DRAM test and Flash test.



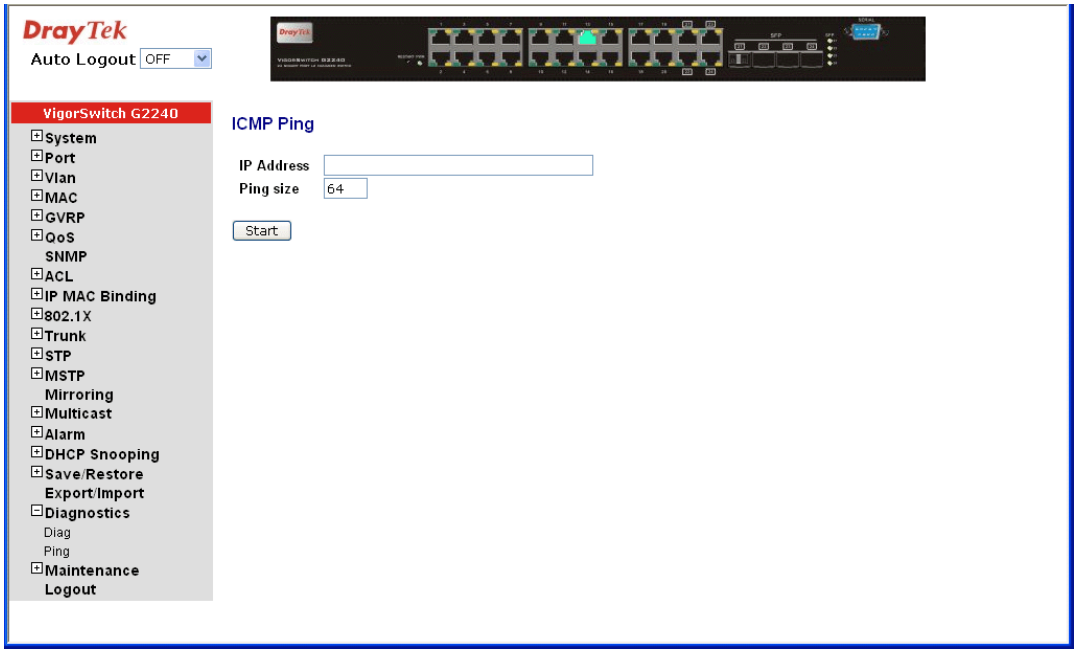
2.20.2 Ping

Function name:

ICMP Ping

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.



Parameter description:

IP Address:	An IP address with the version of v4, e.g. 192.168.1.1.
Ping size:	Identify what ping packet size and unit is bytes.

2.21 Maintenance

This chapter will introduce the reset and firmware upgrade function for the firmware upgrade and key parameters change system maintenance requirements.

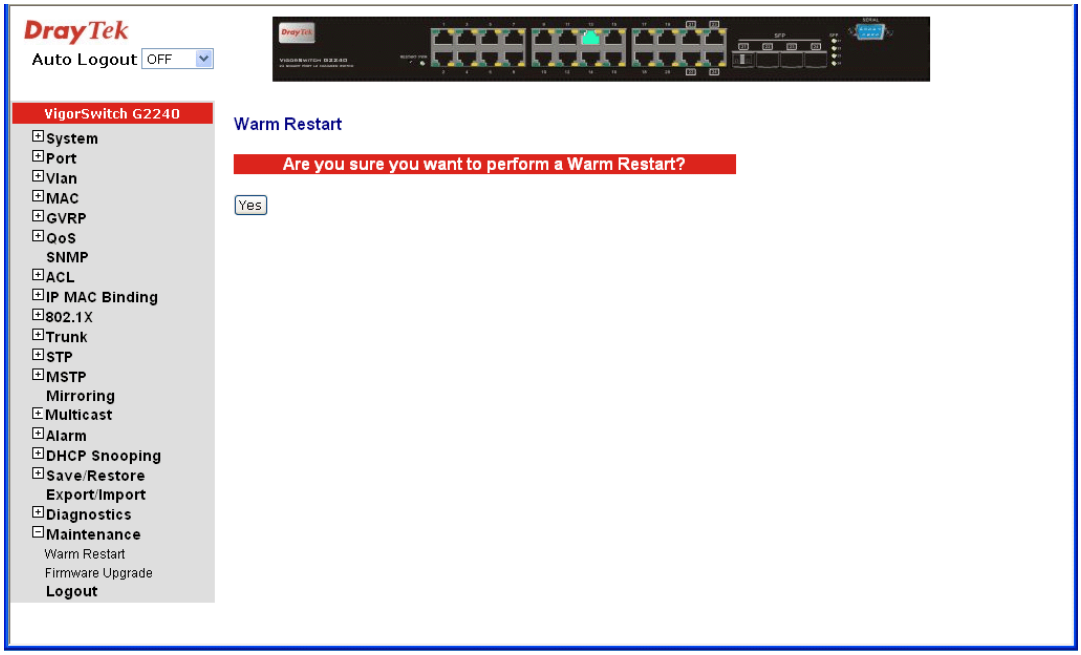
2.21.1 Warm Restart

Function name:

Warm Restart

Function description:

We offer you many ways to reset 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 “Warm Restart” in the main menu.



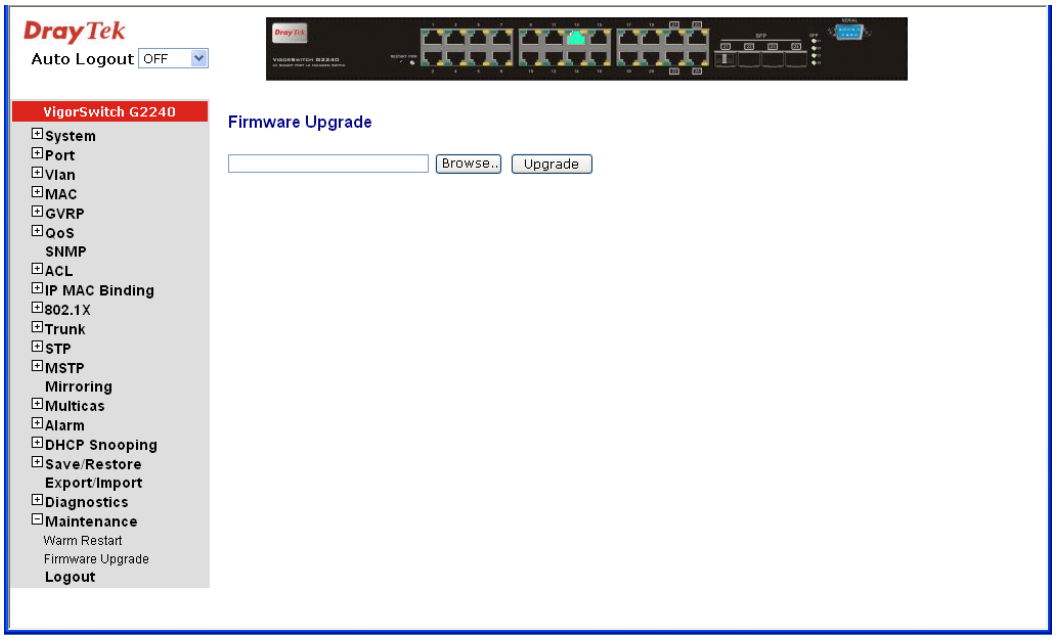
2.21.2 Firmware Upgrade

Function name:

Firmware Upgrade

Function description:

Click on <Browse> to select a specific 24 GIGABIT L2 MANAGED SWITCH firmware file from the Web management PC, then click on <Upload> to confirm the upgrade firmware action. The new firmware will be uploaded into the switch and write into flash memory. You have to reboot the switch for new firmware take effect after the firmware upgrade successfully.



2.22 Logout

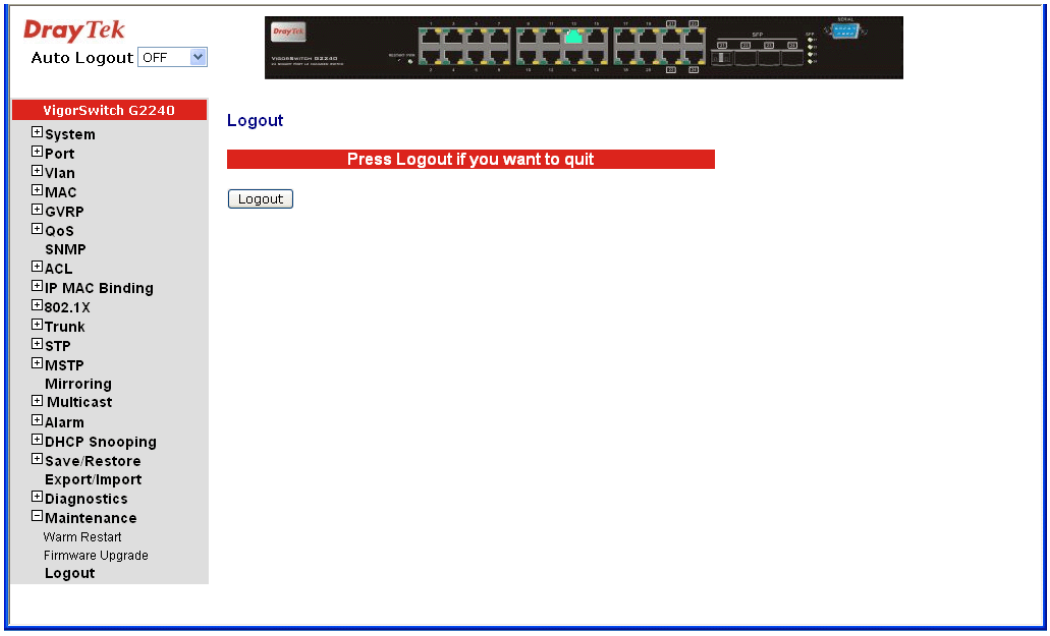
You can manually logout by performing Logout function. In the switch, it provides another way to logout. You can configure it to logout automatically.

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 in five minutes. Besides, you can manually logout.



Parameter description:

Logout: Click on Logout to leave the web UI management function.

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: 115200, 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.