

# DrayTek

## VigorSwitch G1260

Web Smart Giga Switch



*Your reliable networking solutions partner*

# User's Guide

**V1.1**

# **VigorSwitch G1260**

## ***24 Gigabit Port Web Smart Switch***

### **User's Guide**

**Version: 1.1**

**Firmware Version: V1.21**

**Date: March 31, 2016**

## Copyright Information

### Copyright Declarations

Copyright 2013 All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.

### 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 to restore 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 township, 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.

## Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a class A computing device pursuant to Subpart J of part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment.

## GPL Notice

This DrayTek product uses software partially or completely licensed under the terms of the GNU GENERAL PUBLIC LICENSE. The author of the software does not provide any warranty. A Limited Warranty is offered on DrayTek products. This Limited Warranty does not cover any software applications or programs.

To download source codes please visit:

<http://gplsource.draytek.com>

GNU GENERAL PUBLIC LICENSE:

<https://gnu.org/licenses/gpl-2.0>

Version 2, June 1991

For any question, please feel free to contact DrayTek technical support at [support@draytek.com](mailto:support@draytek.com) for further information.



## Table of Contents

# 1

<b>Introduction .....</b>	<b>1</b>
1.1 Overview .....	1
1.2 Features .....	2
1.3 Packing List .....	3
1.4 LED Indicators and Connectors .....	4
1.5 Hardware Installation .....	5
1.5.1 Connecting the SFP Fiber Transceiver to the Chassis .....	5
1.5.2 Installing Optional SFP Fiber Transceivers to the switch .....	6
1.5.3 Installing Chassis to a 19-Inch Wiring Closet Rail .....	6
1.5.4 Cabling Requirements .....	6
1.5.5 Configuring the Management Agent of Switch .....	11
1.5.6 IP Address Assignment .....	12
1.6 Typical Applications .....	16

# 2

<b>Basic Concept and Management .....</b>	<b>19</b>
2.1 What's the Ethernet.....	19
2.2 Media Access Control (MAC).....	21
2.3 Flow Control .....	26
2.4 How does a switch work?.....	28
Terminology .....	28
2.5 Virtual LAN .....	31
2.6 Link Aggregation .....	36

# 3

<b>Operation of Web-based Management .....</b>	<b>39</b>
3.1 Web Management Home Overview .....	40
3.1.1 The Information of Page Layout .....	40
3.2 System .....	41
3.2.1 System Information and IP Configuration.....	41
3.3 Port.....	44
3.3.1 Port Configuration.....	44
3.4 VLANs .....	46
3.4.1 VLAN Mode .....	46
3.4.2 VLAN Group – Tag-based .....	48
3.4.3 VLAN Group - Port-based.....	52

3.4.4 VLAN Isolation .....	54
3.5 Aggregation .....	55
3.6 802.1X .....	56
3.7 IGMP Snooping .....	61
3.8 Mirroring .....	62
3.9 Quality of Service .....	62
3.10 Loop Detection .....	65
3.11 Broadcast Storm Protection.....	66
3.12 SNMP .....	67
3.13 Statistics Overview .....	69
3.14 Detailed Statistics .....	70
3.15 IGMP Status .....	72
3.16 Ping .....	73
3.17 Warm Restart .....	74
3.18 Factory Default.....	74
3.19 Firmware Upgrade .....	75
3.20 Configuration File Transfer.....	76
3.21 Logout .....	77

# 4

<b>Trouble Shooting.....</b>	<b>79</b>
4.1 Resolving No Link Condition.....	79
4.2 Q & A.....	79

# 1

# Introduction

## 1.1 Overview

The 24-port Gigabit Web Smart Switch is a standard switch that meets all IEEE 802.3/u/x/z Gigabit, Fast Ethernet specifications. The switch has 20 10/100/1000Mbps TP ports and 4 Gigabit TP/SFP transceiver slots. It supports console, telnet, http and SNMP interface for switch management. The network administrator can logon the switch to monitor, configure and control each port's activity. In addition, the switch implements the QoS (Quality of Service), VLAN, and Trunking. It is suitable for office application.

Others the switch increases support the Power saving for reduce the power consumption with "ActiPHY Power Management" and "PerfectReach Power Management" two techniques. It could efficient saving the switch power with auto detect the client idle and cable length to provide different power.

In this switch, Port 21, 22, 23, 24 includes two types of media --- TP and SFP Fiber (LC, BiDi-SC...); 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.

Below shows key features of this device:

### **QoS**

The switch offers powerful QoS function. This function supports 802.1p VLAN tag priority and DSCP on Layer 3 of network framework.

### **VLAN**

Support Port-based VLAN and IEEE802.1Q Tag VLAN. Support 24 active VLANs and VLAN ID 1~4094.

### **Port Trunking**

Allows one or more links to be aggregated together to form a Link Aggregation Group by the static setting.

## Power Saving

The Power saving using the "ActiPHY Power Management" and "PerfectReach Power Management" two techniques to detect the client idle and cable length automatically and provides the different power. It could efficient to save the switch power and reduce the power consumption.

## 1.2 Features

The VigorSwitch G1260, 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
- 512KB on-chip frame buffer
- Jumbo frame support 9KB
- Programmable classifier for QoS (Layer 2/Layer 3)
- 8K MAC address and support VLAN ID(1~4094)
- Per-port shaping, policing, and Broadcast Storm Control
- Power Saving with "ActiPHY Power Management" and "Perfect Reach Power Management" techniques.
- 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 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 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 UI and Reset button of the switch
- 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 3



- Built-in web-based management and CLI management, providing a more convenient UI for the user

## 1.3 Packing List

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

- VigorSwitch G1260
- AC Power Cord
- CD
- 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 include two types of media --- TP and SFP Fiber (LC, BiDi-SC...); they support 10/100/1000Mbps TP or 1000Mbps SFP Fiber with auto-detected function. 1000Mbps SFP Fiber transceiver is used for high-speed connection expansion; nine optional SFP types provided for the switch are listed below:

- 1000Mbps LC, MM, SFP Fiber transceiver (SFP.0LC.202)
- 1000Mbps LC, SM 10km, SFP Fiber transceiver (SFP.0LC.212.10)
- 1000Mbps LC, SM 30km, SFP Fiber transceiver (SFP.0LC.212.30)
- 1000Mbps LC, SM 50km, SFP Fiber transceiver (SFP.0LC.212.50)
- 1000Mbps LC, SM 70km, SFP Fiber transceiver (SFP.0LC.212.70)
- 1000Mbps LC, SM 110km, SFP Fiber transceiver (SFP.0LC.212.B0)
- 1000Mbps BiDi SC, type 1, SM 20km, SFP Fiber WDM transceiver (SFP.0BS.621.201)
- 1000Mbps BiDi SC, type 2, SM 20km, SFP Fiber WDM transceiver (SFP.0BS.621.202)
- 1000Mbps LC, SM 10km, SFP Fiber transceiver with DDM (SFP.DLC.212.10)



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 24 ports working status of the switch.

### LED Explanation



LED	Color	Explanation
System	Green	Lit when +3.3V power is coming up
	Red	Lit when The voltage is smaller than 10.8V or greater than 13.2V. When the temperature of the switch near power supply is greater than 45°C or the temperature near fan entrance is greater than 70°C. When looping occurs.
<b>10/100/1000 Ethernet TP Port 1 to 24 LED</b>		
LINK/ACT	Green	Lit when connection with remote device is good. Blinks when any traffic is present.
Speed	Green/ Yellow/ Off	Lit Green when TP link on 1000Mbps speed. Lit Amber when TP link on 10/100Mbps speed. Off when no link occur.
<b>1000SX/LX Gigabit Fiber Port 21, 22, 23, 24 LED</b>		
LINK/ACT	Green	Lit when SFP connection with remote device is good. Blinks when any traffic is present.
Speed	Green/ Yellow/ Off	Lit Green when SFP link on 1000Mbps speed. Lit Yellow when SFP link on 100Mbps speed. Off when no link occur.

### Connector Explanation

Interface	Description
Mode	<ul style="list-style-type: none"> <li>● Switch the status display among System, Link/Act and Speed.</li> <li>● Press and hold for 3~5 seconds to reboot the router.</li> <li>● Press until all the LEDs light on for returning to factory default settings.</li> </ul>
LAN P1 – P24	Giga Ethernet Port.
SFP (21 – 24)	SFP Fiber Port.

## User Interfaces on the Rear Panel



24-PORT GBE WEB SMART SWITCH

## 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

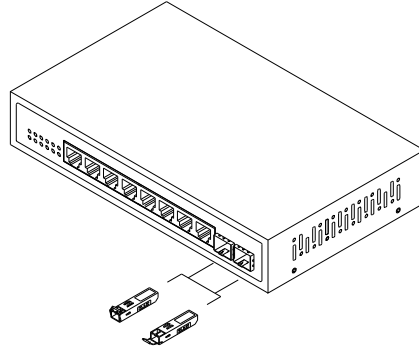
The switch supports 100-240 VAC, 50-60 Hz power supply. The power supply will automatically convert the local AC power source to DC power. It does not matter whether any connection plugged into the switch or not when power on, even modules as well. After the power is on, all LED indicators will light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

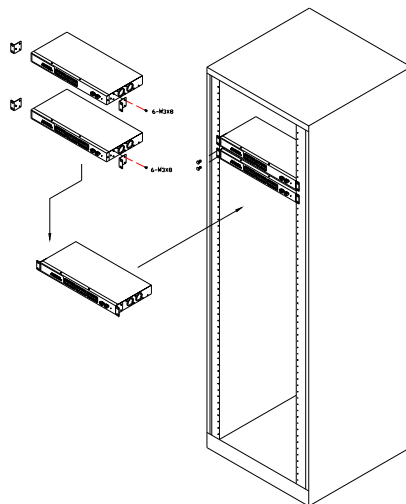
If you have no modules, please skip this section.



### 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.

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

**Switch Cascading in Topology**

**Takes the Delay Time into Account**

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

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

1000Base-X TP, Fiber	100Base-TX TP/100Base-FX Fiber
Round trip Delay: 4096	Round trip Delay: 512

Cat. 5 TP Wire:	11.12/m	Cat. 5 TP Wire:	1.12/m	Fiber Cable:	1.0/m
Fiber Cable:	10.10/m	TP to fiber Converter: 56			
Bit Time unit: 1ns (1sec./1000 Mega bit)			Bit Time unit: 0.01 $\mu$ s (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.

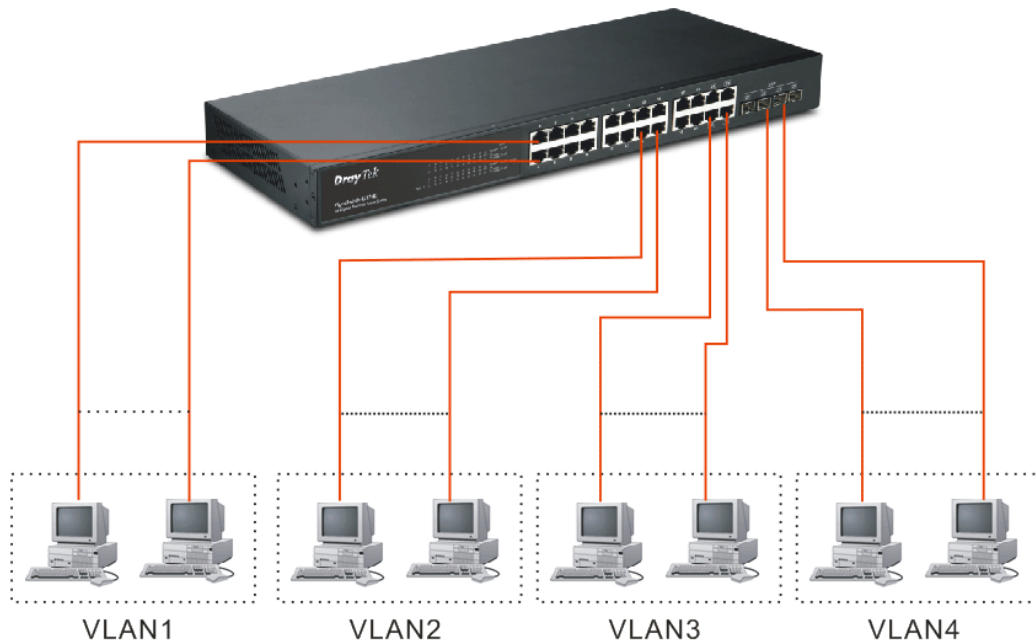
Every port can access each other. (\*The switch image is sample only.)



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

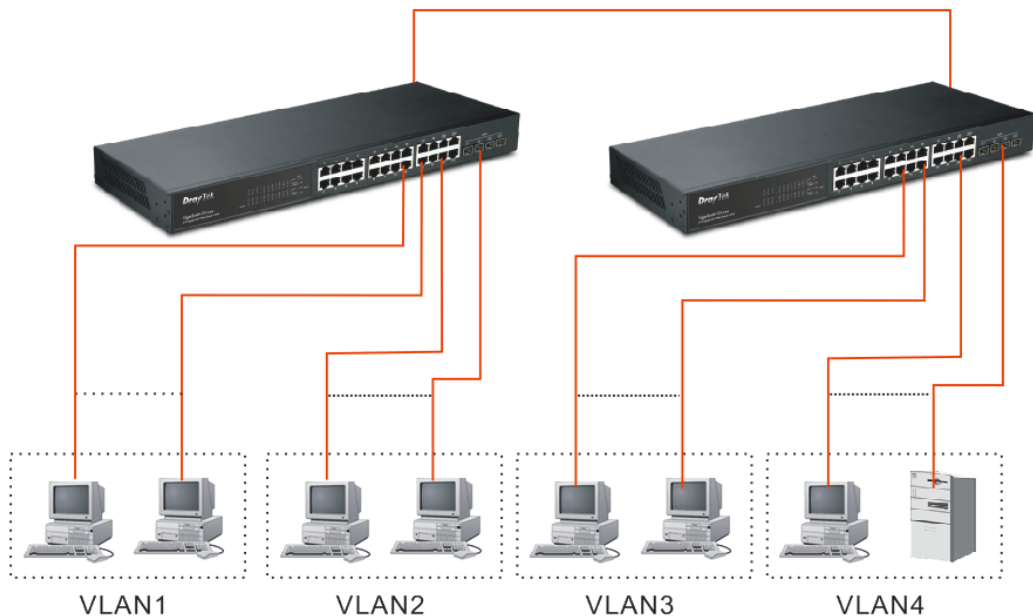
Here VLAN area is defined by what VLAN you are using. The switch supports both port-based VLAN and tag-based VLAN. They are different in practical deployment, especially in physical location. The following diagram shows how it works and what the difference they are.

**Case 2: Port-based VLAN -1** (\*The switch image is sample only.)



- 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.

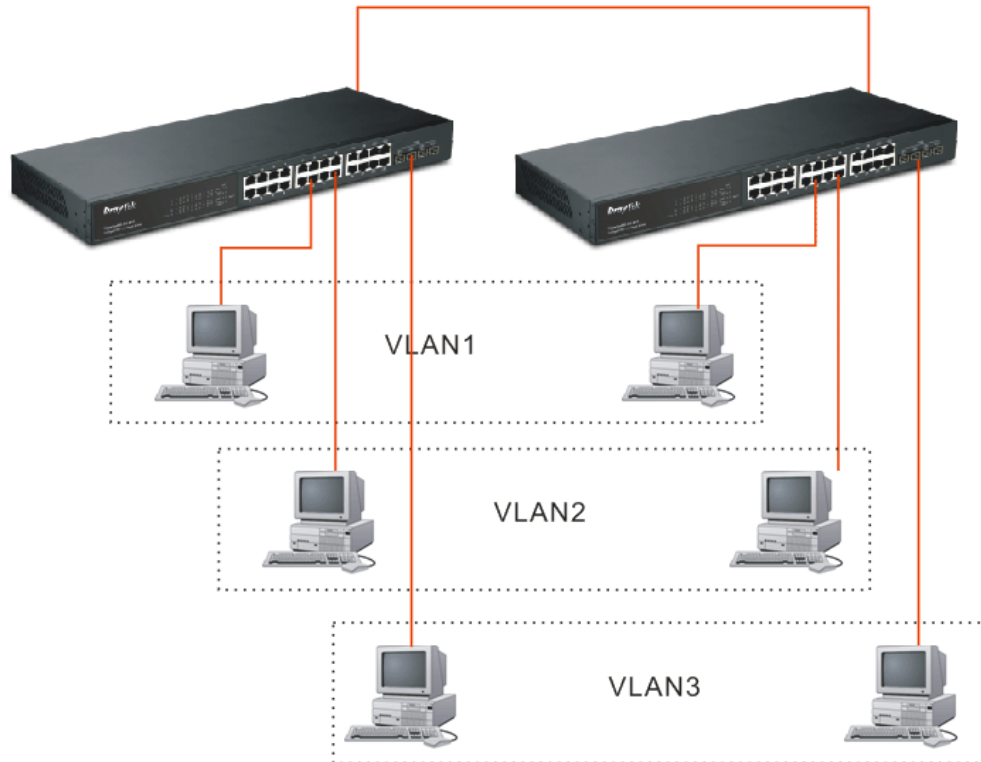
**Case 3: Port-based VLAN – 2** (\*The switch image is sample only.)



- 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**  
(\*The switch image is sample only.)





## 1.5.5 Configuring the Management Agent of Switch

Users can monitor and configure the switch through the following procedures.

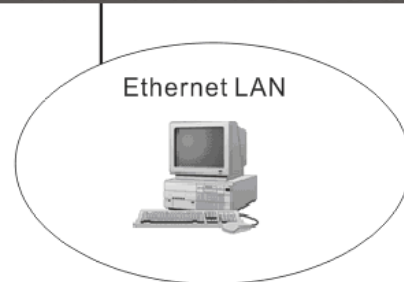
### Configuring the Management Agent of VigorSwitch G1260 through the Ethernet Port

There are two ways to configure and monitor the switch through the switch's Ethernet port. They are Web browser and SNMP manager. We just introduce the first type of management interface. Web-based UI for the switch is an interface in a highly friendly way.

VigorSwitch  
For example:  
IP=192.168.1.1  
Subnet Mask =255.255.255.0  
Default Gateway=192.168.1.254



Assign a reasonable IP address,  
For example:  
IP=192.168.1.100  
Subnet Mask =255.255.255.0  
Default Gateway=192.168.1.254



### Managing VigorSwitch G1260 through Ethernet Port

Before start using the switch, the IP address setting of the switch should be done, then perform the following steps:

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. Please refer to the above figure about the 24-Port GbE Web Smart Switch default IP address information.

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



Password

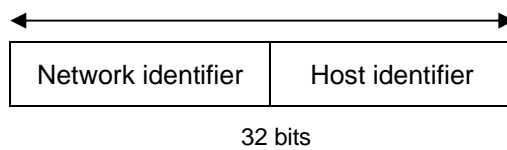
## 1.5.6 IP Address Assignment

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

### *IP address:*

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

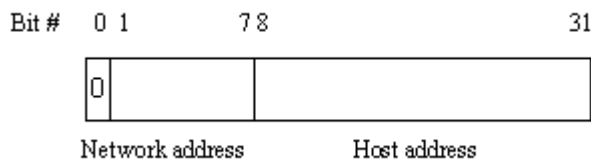
Each class has its own network range between the network identifier and host identifier in the 32 bits address. Each IP address comprises two parts: network identifier (address) and host identifier (address). The former indicates the network where the addressed host resides, and the latter indicates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



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

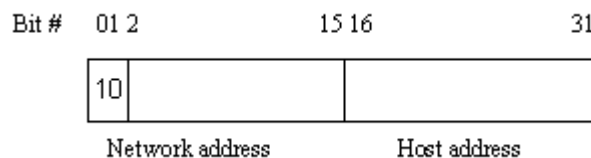
### *Class A:*

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



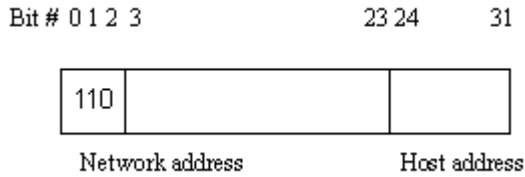
### *Class B:*

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



### *Class C:*

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



**Class D and E:**

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

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

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

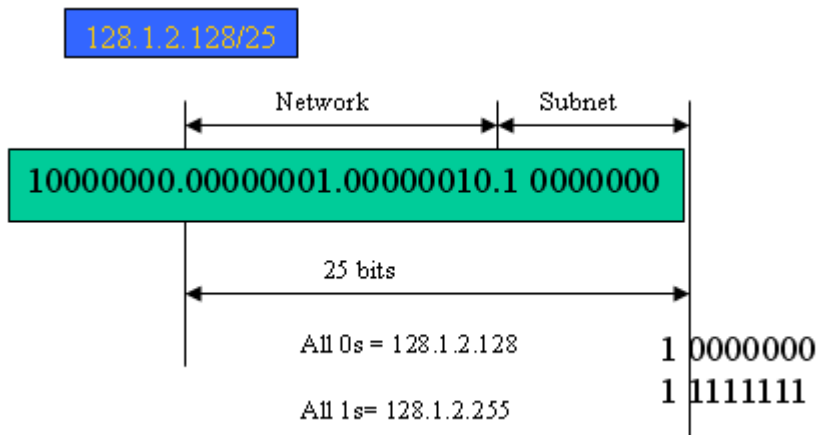
Please refer to RFC 1597 and RFC 1466 for more information.

**Subnet mask:**

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

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

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



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

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

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

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

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

**Default gateway:**

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

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

<b>Configuration</b>	MAC Address	00-40-c7-00-00-01
System Information	Serial Number	999999999999
Ports	Temperature	39°C(102.2°F) / 38°C(100.4°F)
VLANs	Voltage	12.42 / 1.03 / 1.02
--VLAN Mode	Active IP Address	192.168.1.11
--VLAN Group	Active Subnet Mask	255.255.255.0
--VLAN Isolation	Active Gateway	192.168.1.3
Aggregation	DHCP Server	192.168.1.3
802.1X	Lease Time Left	64361 secs
IGMP Snooping	Device Name	VigorSwitch G1260
Mirroring	System Contact	admin@localhost
Quality of Service	System Location	Taiwan
Loop Detection	DHCP Enabled	<input checked="" type="checkbox"/>
Broadcast Storm Protection	Fallback IP Address	192.168.1.224
SNMP	Fallback Subnet Mask	255.255.255.0
<b>Monitoring</b>	Fallback Gateway	192.168.1.1
Statistics Overview	Management VLAN	1
Detailed Statistics	Password	.....
IGMP Status		
Ping		
<b>Maintenance</b>		
Warm Restart		
Factory Default		
Firmware Upgrade		
Configuration File Transfer		
Logout		

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.

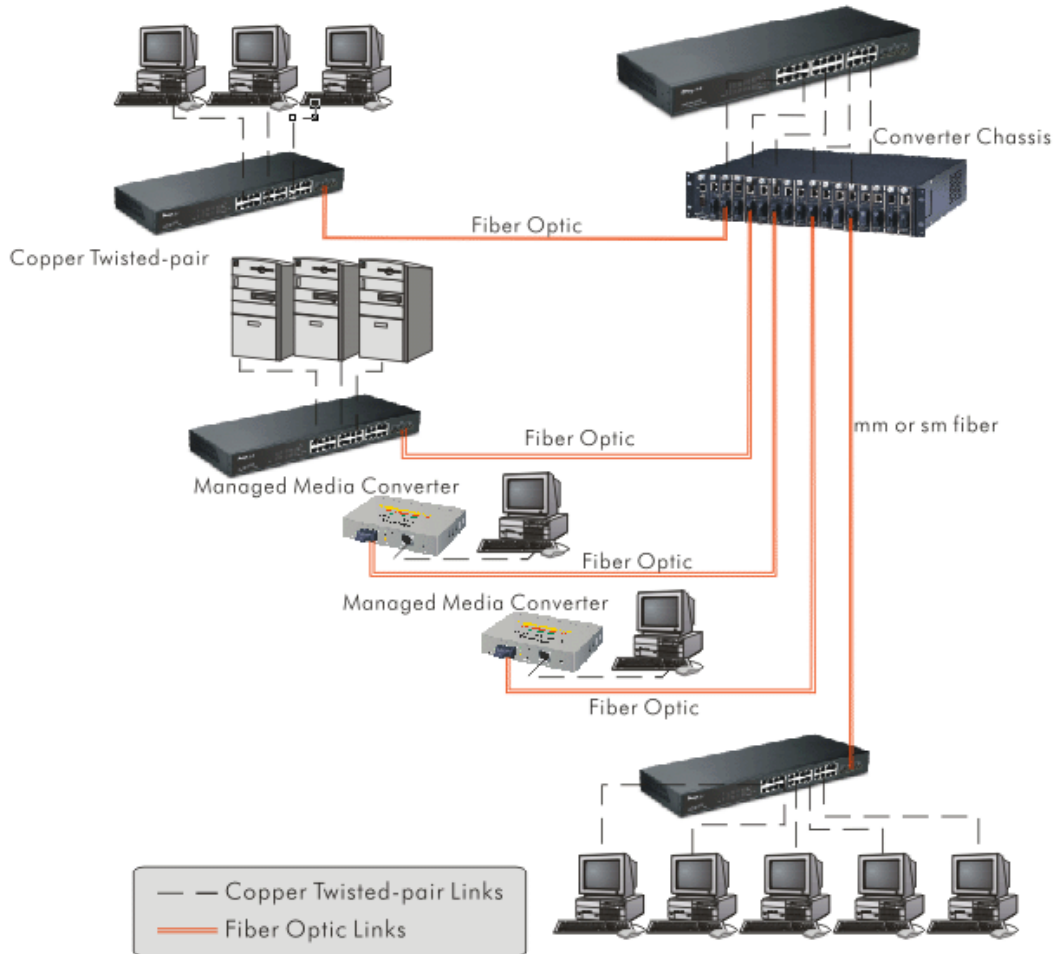
**Note:** The DHCP Setting is enabled in default.

## 1.6 Typical Applications

The 24-Port 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.

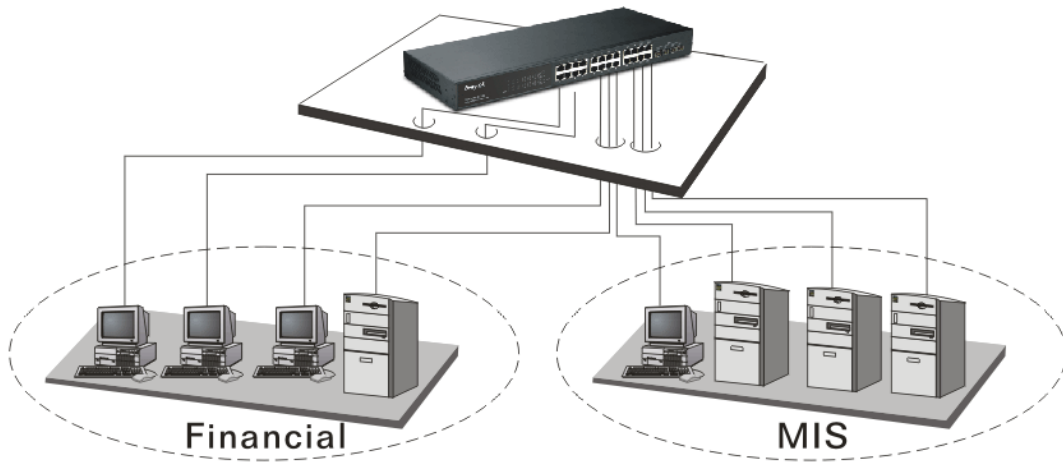
The switch is suitable for the following applications.

- Central Site/Remote site application is used in carrier or ISP  
(\* The switch image is sample only)



It is a system wide basic reference connection diagram. This diagram demonstrates how the switch and the various devices form the network infrastructure in a large-scale network.

- Peer-to-peer application is used in two remote offices  
(\* The switch image is sample only.)



- Office Network Connection  
(\* The switch image is sample only.)



This page is left blank.



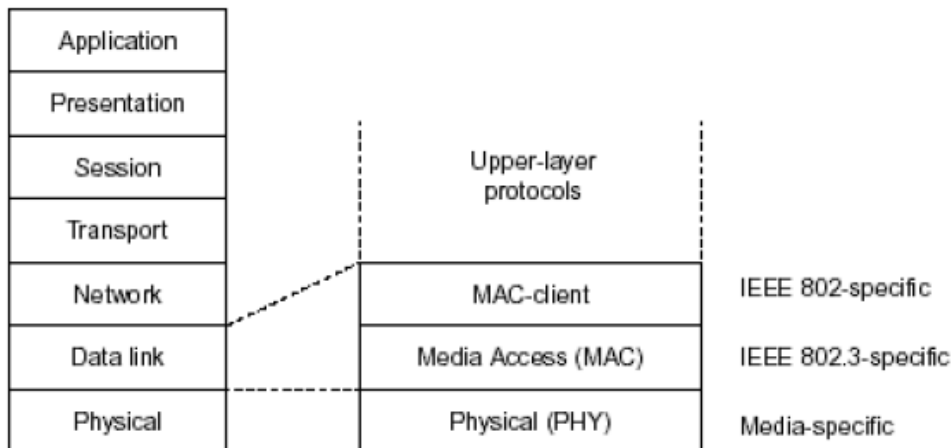
# 2

## Basic Concept and Management

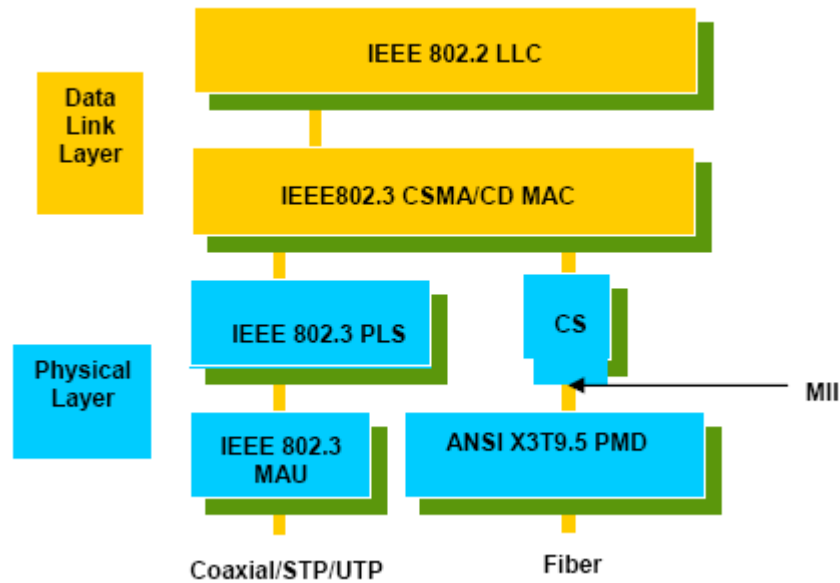
This chapter will tell you the basic concept of features to manage this switch and how they work.

### 2.1 What's the Ethernet

Ethernet originated and was implemented at Xerox in Palo Alto, CA in 1973 and was successfully commercialized by Digital Equipment Corporation (DEC), Intel and Xerox (DIX) in 1980. In 1992, Grand Junction Networks unveiled a new high speed Ethernet with the same characteristic of the original Ethernet but operated at 100Mbps, called Fast Ethernet now. This means Fast Ethernet inherits the same frame format, CSMA/CD, software interface. In 1998, Gigabit Ethernet was rolled out and provided 1000Mbps. Now 10G/s Ethernet is under approving. Although these Ethernet have different speed, they still use the same basic functions. So they are compatible in software and can connect each other almost without limitation. The transmission media may be the only problem.



In the above figure, we can see that Ethernet locates at the Data Link layer and Physical layer and comprises three portions, including logical link control (LLC), media access control (MAC), and physical layer. The first two comprises Data link layer, which performs splitting data into frame for transmitting, receiving acknowledge frame, error checking and re-transmitting when not received correctly as well as provides an error-free channel upward to network layer.



This above diagram shows the Ethernet architecture, LLC sub-layer and MAC sub-layer, which are responded to the Data Link layer, and transceivers, which are responded to the Physical layer in OSI model. In this section, we are mainly describing the MAC sub-layer.

### Logical Link Control (LLC)

Data link layer is composed of both the sub-layers of MAC and MAC-client. Here MAC client may be logical link control or bridge relay entity.

Logical link control supports the interface between the Ethernet MAC and upper layers in the protocol stack, usually Network layer, which is nothing to do with the nature of the LAN. So it can operate over other different LAN technology such as Token Ring, FDDI and so on. Likewise, for the interface to the MAC layer, LLC defines the services with the interface independent of the medium access technology and with some of the nature of the medium itself.

DSAP address	SSAP address	Control	Information
8 bits	8 bits	8 or 16 bits	M*8 bits

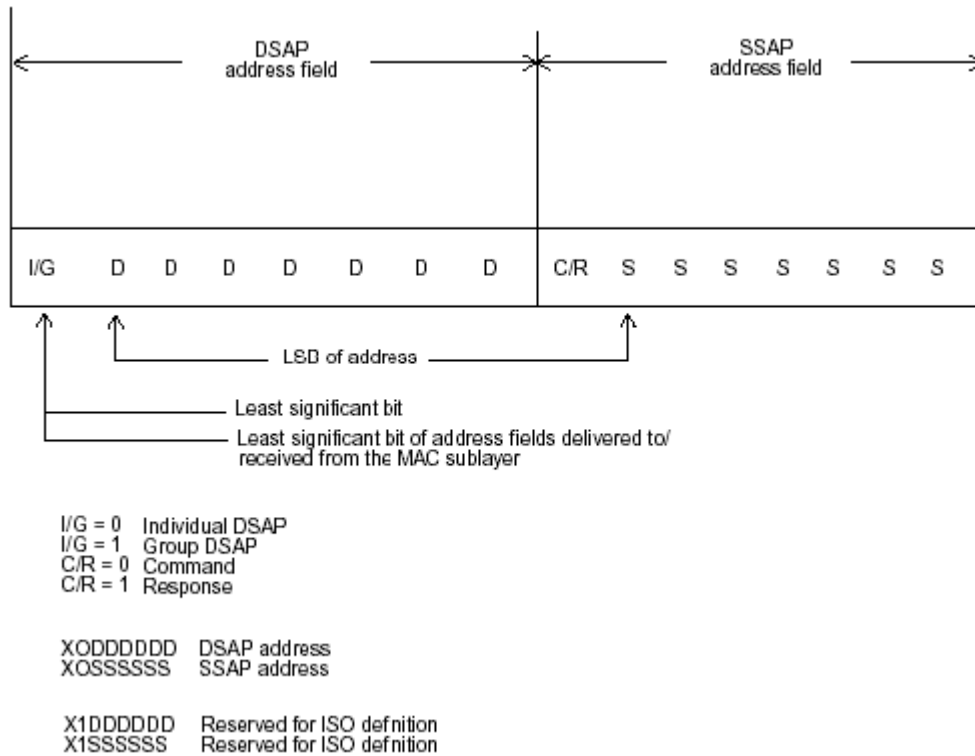
- DSAP address = Destination service access point address field
- SSAP address = Source service access point address field
- Control = Control field [16 bits for formats that include sequence numbering, and 8 bits for formats that do not (see 5.2)]
- Information = Information field
- \* = Multiplication
- M = An integer value equal to or greater than 0. (Upper bound of M is a function of the medium access control methodology used.)

The table above is the format of LLC PDU. It comprises four fields, DSAP, SSAP, Control and Information. The DSAP address field identifies the one or more service access points, in which the I/G bit indicates it is individual or group address. If all bit of DSAP is 1s, it's a global address. The SSAP address field identifies the specific services indicated by C/R bit

(command or response). The DSAP and SSAP pair with some reserved values indicates some well-known services listed in the table below.

0xAAAA	SNAP
0xE0E0	Novell IPX
0xF0F0	NetBios
0xFEFE	IOS network layer PDU
0xFFFF	Novell IPX 802.3 RAW packet
0x4242	STP BPDU
0x0606	IP
0x9898	ARP

LLC type 1 connectionless service, LLC type 2 connection-oriented service and LLC type 3 acknowledge connectionless service are three types of LLC frame for all classes of service. In Fig 3-2, it shows the format of Service Access Point (SAP). Please refer to IEEE802.2 for more details.



## 2.2 Media Access Control (MAC)

### MAC Addressing

Because LAN is composed of many nodes, for the data exchanged among these nodes, each node must have its own unique address to identify who should send the data or should receive the data. In OSI model, each layer provides its own mean to identify the unique address in some form, for example, IP address in network layer.

The MAC is belonged to Data Link Layer (Layer 2), the address is defined to be a 48-bit long and locally unique address. Since this type of address is applied only to the Ethernet LAN media access control (MAC), they are referred to as MAC addresses.

The first three bytes are Organizational Unique Identifier (OUI) code assigned by IEEE. The last three bytes are the serial number assigned by the vendor of the network device. All these six bytes are stored in a non-volatile memory in the device. Their format is as the following table and normally written in the form as aa-bb-cc-dd-ee-ff, a 12 hexadecimal digits separated by hyphens, in which the aa-bb-cc is the OUI code and the dd-ee-ff is the serial number assigned by manufacturer.

Bit 47					Bit 0
1 <sup>st</sup> byte	2 <sup>nd</sup> byte	3 <sup>rd</sup> byte	4 <sup>th</sup> byte	5 <sup>th</sup> byte	6 <sup>th</sup> byte
OUI code			Serial number		

The first bit of the first byte in the Destination address (DA) determines the address to be a Unicast (0) or Multicast frame (1), known as I/G bit indicating individual (0) or group (1). So the 48-bit address space is divided into two portions, Unicast and Multicast. The second bit is for global-unique (0) or locally-unique address. The former is assigned by the device manufacturer, and the later is usually assigned by the administrator. In practice, global-unique addresses are always applied.

A unicast address is identified with a single network interface. With this nature of MAC address, a frame transmitted can exactly be received by the target an interface the destination MAC points to.

A multicast address is identified with a group of network devices or network interfaces. In Ethernet, a many-to-many connectivity in the LANs is provided. It provides a mean to send a frame to many network devices at a time. When all bit of DA is 1s, it is a broadcast, which means all network device except the sender itself can receive the frame and response.

### Ethernet Frame Format

There are two major forms of Ethernet frame, type encapsulation and length encapsulation, both of which are categorized as four frame formats 802.3/802.2 SNAP, 802.3/802.2, Ethernet II and Netware 802.3 RAW. We will introduce the basic Ethernet frame format defined by the IEEE 802.3 standard required for all MAC implementations. It contains seven fields explained below.

PRE	SFD	DA	SA	Type/Length	Data	Pad bit if any	FCS
7	7	6	6	2		46-1500	4

**Preamble (PRE)** - The PRE is 7-byte long with alternating pattern of ones and zeros used to tell the receiving node that a frame is coming, and to synchronize the physical receiver with the incoming bit stream. The preamble pattern is:

10101010 10101010 10101010 10101010 10101010 10101010 10101010

**Start-of-frame delimiter (SFD)** - The SFD is one-byte long with alternating pattern of ones and zeros, ending with two consecutive 1-bits. It immediately follows the preamble and uses the last two consecutive 1s bit to indicate that the next bit is the start of the data packet and the left-most bit in the left-most byte of the destination address. The SFD pattern is 10101011.

**Destination address (DA)** - The DA field is used to identify which network device(s) should receive the packet. It is a unique address. Please see the section of MAC addressing.

**Source addresses (SA)** - The SA field indicates the source node. The SA is always an individual address and the left-most bit in the SA field is always 0.

**Length/Type** - This field indicates either the number of the data bytes contained in the data field of the frame, or the Ethernet type of data. If the value of first two bytes is less than or equal to 1500 in decimal, the number of bytes in the data field is equal to the Length/Type value, i.e. this field acts as Length indicator at this moment. When this field acts as Length, the frame has optional fields for 802.3/802.2 SNAP encapsulation, 802.3/802.2 encapsulation and Netware 802.3 RAW encapsulation. Each of them has different fields following the Length field.

If the Length/Type value is greater than 1500, it means the Length/Type acts as Type. Different type value means the frames with different protocols running over Ethernet being sent or received.

For example,

0x0800	IP datagram
0x0806	ARP
0x0835	RARP
0x8137	IPX datagram
0x86DD	IPv6

**Data** - Less than or equal to 1500 bytes and greater or equal to 46 bytes. If data is less than 46 bytes, the MAC will automatically extend the padding bits and have the payload be equal to 46 bytes. The length of data field must equal the value of the Length field when the Length/Type acts as Length.

**Frame check sequence (FCS)** - This field contains a 32-bit cyclic redundancy check (CRC) value, and is a check sum computed with DA, SA, through the end of the data field with the following polynomial.

$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

It is created by the sending MAC and recalculated by the receiving MAC to check if the packet is damaged or not.

## How does a MAC work?

The MAC sub-layer has two primary jobs to do:

1. Receiving and transmitting data. When receiving data, it parses frame to detect error; when transmitting data, it performs frame assembly.
2. Performing Media access control. It prepares the initiation jobs for a frame transmission and makes recovery from transmission failure.

## Frame transmission

As Ethernet adopted Carrier Sense Multiple Access with Collision Detect (CSMA/CD), it detects if there is any carrier signal from another network device running over the physical medium when a frame is ready for transmission. This is referred to as sensing carrier, also "Listen". If there is signal on the medium, the MAC defers the traffic to avoid a transmission collision and waits for a random period of time, called backoff time, then sends the traffic again.

After the frame is assembled, when transmitting the frame, the preamble (PRE) bytes are inserted and sent first, then the next, Start of frame Delimiter (SFD), DA, SA and through

the data field and FCS field in turn. The followings summarize what a MAC does before transmitting a frame.

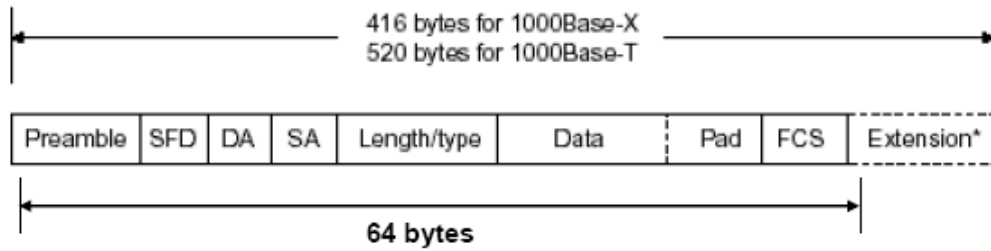
1. MAC will assemble the frame. First, the preamble and Start-of-Frame delimiter will be put in the fields of PRE and SFD, followed DA, SA, tag ID if tagged VLAN is applied, Ethertype or the value of the data length, and payload data field, and finally put the FCS data in order into the responded fields.
2. Listen if there is any traffic running over the medium. If yes, wait.
3. If the medium is quiet, and no longer senses any carrier, the MAC waits for a period of time, i.e. inter-frame gap time to have the MAC ready with enough time and then start transmitting the frame.
4. During the transmission, MAC keeps monitoring the status of the medium. If no collision happens until the end of the frame, it transmits successfully. If there is a collision happened, the MAC will send the patterned jamming bit to guarantee the collision event propagated to all involved network devices, then wait for a random period of time, i.e. backoff time. When backoff time expires, the MAC goes back to the beginning state and attempts to transmit again. After a collision happens, MAC increases the transmission attempts. If the count of the transmission attempt reaches 16 times, the frame in MAC's queue will be discarded.

Ethernet MAC transmits frames in half-duplex and full-duplex ways. In halfduplex operation mode, the MAC can either transmit or receive frame at a moment, but cannot do both jobs at the same time.

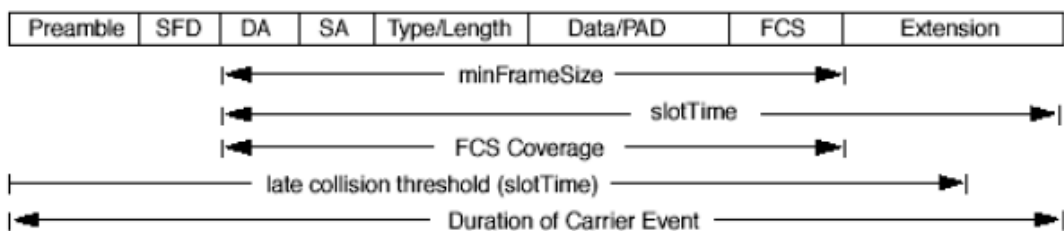
As the transmission of a MAC frame with the half-duplex operation exists only in the same collision domain, the carrier signal needs to spend time to travel to reach the targeted device. For two most-distant devices in the same collision domain, when one sends the frame first, and the second sends the frame, in worstcase, just before the frame from the first device arrives. The collision happens and will be detected by the second device immediately. Because of the medium delay, this corrupted signal needs to spend some time to propagate back to the first device. The maximum time to detect a collision is approximately twice the signal propagation time between the two most-distant devices. This maximum time is traded-off by the collision recovery time and the diameter of the LAN.

In the original 802.3 specification, Ethernet operates in half duplex only. Under this condition, when in 10Mbps LAN, it's 2500 meters, in 100Mbps LAN, it's approximately 200 meters and in 1000Mbps, 200 meters. According to the theory, it should be 20 meters. But it's not practical, so the LAN diameter is kept by using to increase the minimum frame size with a variable-length non-data extension bit field which is removed at the receiving MAC. The following tables are the frame format suitable for 10M, 100M and 1000M Ethernet, and some parameter values that shall be applied to all of these three types of Ethernet.

Actually, the practice Gigabit Ethernet chips do not feature this so far. They all have their chips supported full-duplex mode only, as well as all network vendors' devices. So this criterion should not exist at the present time and in the future. The switch's Gigabit module supports only full-duplex mode.



Parameter value/LAN	10Base	100Base	1000Base
<b>Max. collision domain DTE to DTE</b>	100 meters	100 meters for UTP 412 meters for fiber	100 meters for UTP 316 meters for fiber
<b>Max. collision domain with repeater</b>	2500 meters	205 meters	200 meters
<b>Slot time</b>	512 bit times	512 bit times	512 bit times
<b>Interframe Gap</b>	9.6us	0.96us	0.096us
<b>AttemptLimit</b>	16	16	16
<b>BackoffLimit</b>	10	10	10
<b>JamSize</b>	32 bits	32 bits	32 bits
<b>MaxFrameSize</b>	1518	1518	1518
<b>MinFrameSize</b>	64	64	64
<b>BurstLimit</b>	Not applicable	Not applicable	65536 bits



In full-duplex operation mode, both transmitting and receiving frames are processed simultaneously. This doubles the total bandwidth. Full duplex is much easier than half duplex because it does not involve media contention, collision, retransmission schedule, padding bits for short frame. The rest functions follow the specification of IEEE802.3. For example, it must meet the requirement of minimum inter-frame gap between successive frames and frame format the same as that in the half-duplex operation.

Because no collision will happen in full-duplex operation, for sure, there is no mechanism to tell all the involved devices. What will it be if receiving device is busy and a frame is coming at the same time? Can it use “backpressure” to tell the source device? A function flow control is introduced in the full-duplex operation.



## 2.3 Flow Control

Flow control is a mechanism to tell the source device stopping sending frame for a specified period of time designated by target device until the PAUSE time expires. This is accomplished by sending a PAUSE frame from target device to source device. When the target is not busy and the PAUSE time is expired, it will send another PAUSE frame with zero time-to-wait to source device. After the source device receives the PAUSE frame, it will again transmit frames immediately. PAUSE frame is identical in the form of the MAC frame with a pause-time value and with a special destination MAC address 01-80-C2-00-00-01. As per the specification, PAUSE operation can not be used to inhibit the transmission of MAC control frame.

Normally, in 10Mbps and 100Mbps Ethernet, only symmetric flow control is supported. However, some switches (e.g. 24-Port GbE Web Smart Switch) support not only symmetric but asymmetric flow controls for the special application. In Gigabit Ethernet, both symmetric flow control and asymmetric flow control are supported. Asymmetric flow control only allows transmitting PAUSE frame in one way from one side, the other side is not but receipt-and-discard the flow control information. Symmetric flow control allows both two ports to transmit PASUE frames each other simultaneously.

### Inter-frame Gap time

After the end of a transmission, if a network node is ready to transmit data out and if there is no carrier signal on the medium at that time, the device will wait for a period of time known as an inter-frame gap time to have the medium clear and stabilized as well as to have the jobs ready, such as adjusting buffer counter, updating counter and so on, in the receiver site. Once the inter-frame gap time expires after the de-assertion of carrier sense, the MAC transmits data. In IEEE802.3 specification, this is 96-bit time or more.

### Collision

Collision happens only in half-duplex operation. When two or more network nodes transmit frames at approximately the same time, a collision always occurs and interferes with each other. This results the carrier signal distorted and undiscriminated. MAC can afford detecting, through the physical layer, the distortion of the carrier signal. When a collision is detected during a frame transmission, the transmission will not stop immediately but, instead, continues transmitting until the rest bits specified by jamSize are completely transmitted. This guarantees the duration of collision is enough to have all involved devices able to detect the collision. This is referred to as Jamming. After jamming pattern is sent, MAC stops transmitting the rest data queued in the buffer and waits for a random period of time, known as backoff time with the following formula. When backoff time expires, the device goes back to the state of attempting to transmit frame. The backoff time is determined by the formula below. When the times of collision is increased, the backoff time is getting long until the collision times excess 16. If this happens, the frame will be discarded and backoff time will also be reset.

$$0 \leq r < 2^k$$

where

$$k = \min(n, 10)$$



## Frame Reception

In essence, the frame reception is the same in both operations of half duplex and full duplex, except that full-duplex operation uses two buffers to transmit and receive the frame independently. The receiving node always “listens” if there is traffic running over the medium when it is not receiving a frame. When a frame destined for the target device comes, the receiver of the target device begins receiving the bit stream, and looks for the PRE (Preamble) pattern and Start-of-Frame Delimiter (SFD) that indicates the next bit is the starting point of the MAC frame until all bit of the frame is received.

For a received frame, the MAC will check:

1. If it is less than one slotTime in length, i.e. short packet, and if yes, it will be discarded by MAC because, by definition, the valid frame must be longer than the slotTime. If the length of the frame is less than one slotTime, it means there may be a collision happened somewhere or an interface malfunctioned in the LAN. When detecting the case, the MAC drops the packet and goes back to the ready state.
2. If the DA of the received frame exactly matches the physical address that the receiving MAC owns or the multicast address designated to recognize. If not, discards it and the MAC passes the frame to its client and goes back to the ready state.
3. If the frame is too long. If yes, throws it away and reports frame Too Long.
4. If the FCS of the received frame is valid. If not, for 10M and 100M Ethernet, discards the frame. For Gigabit Ethernet or higher speed Ethernet, MAC has to check one more field, i.e. extra bit field, if FCS is invalid. If there is any extra bits existed, which must meet the specification of IEEE802.3. When both FCS and extra bits are valid, the received frame will be accepted, otherwise discards the received frame and reports frameCheckError if no extra bits appended or alignmentError if extra bits appended.
5. If the length/type is valid. If not, discards the packet and reports lengthError.
6. If all five procedures above are ok, then the MAC treats the frame as good and de-assembles the frame.

## What if a VLAN tagging is applied?

VLAN tagging is a 4-byte long data immediately following the MAC source address. When tagged VLAN is applied, the Ethernet frame structure will have a little change shown as follows.

Pre	SFD	DA	SA	VLAN type ID	Tag control information	Length/ type	Data	Pad	FCS	Ext
-----	-----	----	----	--------------	-------------------------	--------------	------	-----	-----	-----

Only two fields, VLAN ID and Tag control information are different in comparison with the basic Ethernet frame. The rest fields are the same.

The first two bytes is VLAN type ID with the value of 0x8100 indicating the received frame is tagged VLAN and the next two bytes are Tag Control Information (TCI) used to provide user priority and VLAN ID, which are explained respectively in the following table.

<b>Bits 15-13</b>	User Priority 7-0, 0 is lowest priority
<b>Bit 12</b>	CFI (Canonical Format Indicator) 1: RIF field is present in the tag header 0: No RIF field is present

<b>Bits 11-0</b>	VID (VLAN Identifier) 0x000: Null VID. No VID is present and only user priority is present. 0x001: Default VID 0xFFFF: Reserved
------------------	--

**Note:** RIF is used in Token Ring network to provide source routing and comprises two fields, Routing Control and Route Descriptor.

When MAC parses the received frame and finds a reserved special value 0x8100 at the location of the Length/Type field of the normal non-VLAN frame, it will interpret the received frame as a tagged VLAN frame. If this happens in a switch, the MAC will forward it, according to its priority and egress rule, to all the ports that is associated with that VID. If it happens in a network interface card, MAC will deprive of the tag header and process it in the same way as a basic normal frame. For a VLAN-enabled LAN, all involved devices must be equipped with VLAN optional function.

At operating speeds above 100 Mbps, the slotTime employed at slower speeds is inadequate to accommodate network topologies of the desired physical extent. Carrier Extension provides a means by which the slotTime can be increased to a sufficient value for the desired topologies, without increasing the minFrameSize parameter, as this would have deleterious effects. Nondata bits, referred to as extension bits, are appended to frames that are less than slotTime bits in length so that the resulting transmission is at least one slotTime in duration. Carrier Extension can be performed only if the underlying physical layer is capable of sending and receiving symbols that are readily distinguished from data symbols, as is the case in most physical layers that use a block encoding/decoding scheme.

The maximum length of the extension is equal to the quantity (slotTime - minFrameSize). The MAC continues to monitor the medium for collisions while it is transmitting extension bits, and it will treat any collision that occurs after the threshold (slotTime) as a late collision.

## 2.4 How does a switch work?

The switch is a layer 2 Ethernet Switch equipped with 24 Fast Ethernet ports and 2 optional modules which support Gigabit Ethernet or 100M Ethernet. Each port on it is an independent LAN segment and thus has 26 LAN segments and 26 collision domains, contrast to the traditional shared Ethernet HUB in which all ports share the same media and use the same collision domain and thus limit the bandwidth utilization. With switch's separated collision domain, it can extend the LAN diameter farther than the shared HUB does and highly improve the efficiency of the traffic transmission.

Due to the architecture, the switch can provide full-duplex operation to double the bandwidth per port and many other features, such as VLAN, bandwidth aggregation and so on, not able to be supported in a shared hub.

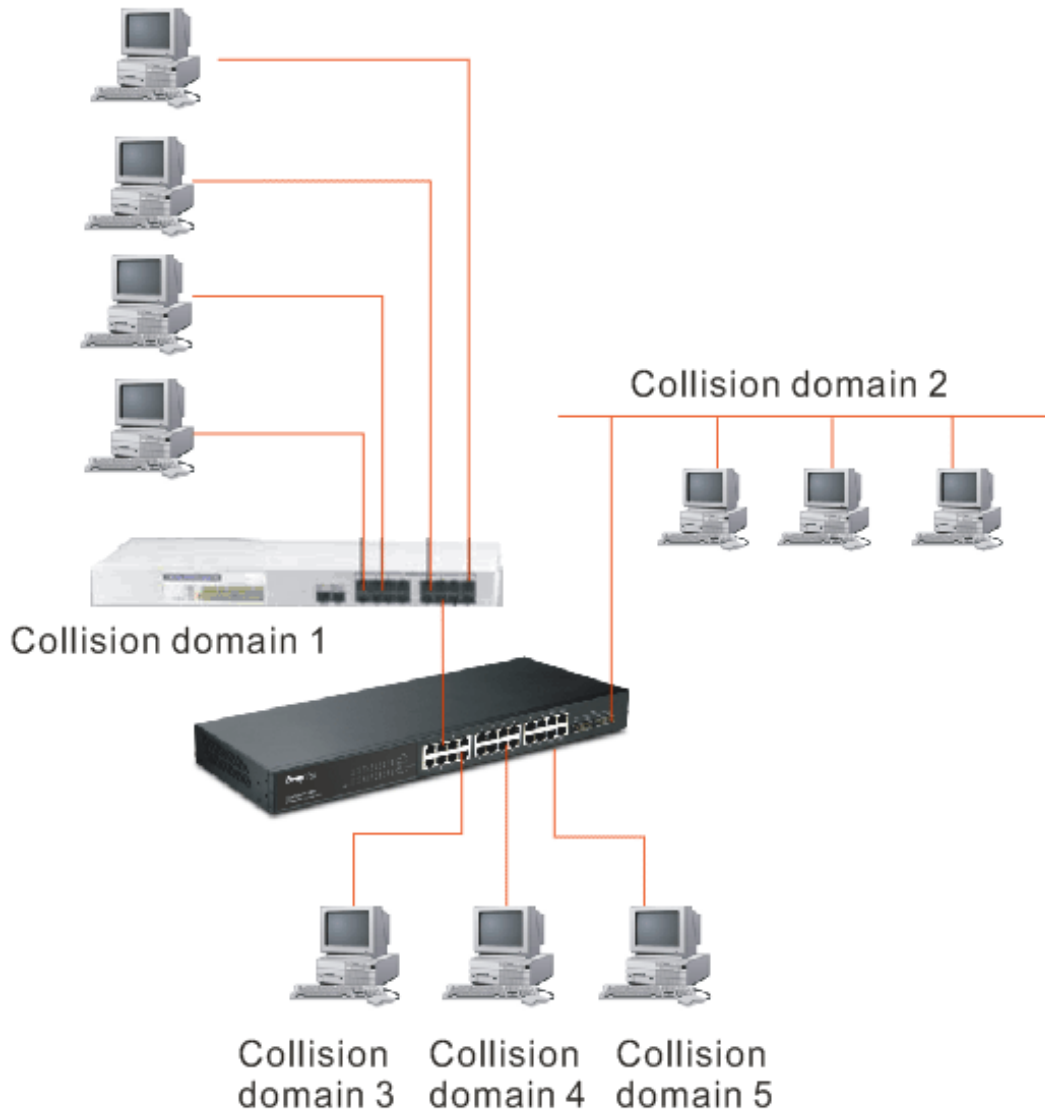
### Terminology

#### Separate Access Domains:

As per the description in the section of "What's the Ethernet", Ethernet utilizes CSMA/CD to arbitrate who can transmit data to the station(s) attached in the LAN. When more than one station transmits data within the same slot time, the signals will collide, referred to as

collision. The arbitrator will arbitrate who should gain the media. The arbitrator is a distributed mechanism in which all stations contend to gain the media. Please refer to “What’s the Ethernet” for more details.

In the figure listed below, assumed in half duplex, you will see some ports of the switch are linked to a shared HUB, which connects many hosts, and some ports just are individually linked to a single host. The hosts attached to a shared hub will be in the same collision domain, separated by the switch, and use CSMA/CD rule. For the host directly attached to the switch, because no other host(s) joins the traffic contention, hence it will not be affected by CSMA/CD. These LAN segments are separated in different access domains by the switch. (\* The switch image is sample only.)



### Micro-segmentation:

To have a port of the switch connected to a single host is referred to as micro-segmentation. It has the following interesting characteristics.

- There is no need the access contention (e.g. Collision). They have their own access domain. But, collision still could happen between the host and the switch port.
- When performing the full duplex, the collision vanishes.
- The host owns a dedicated bandwidth of the port.

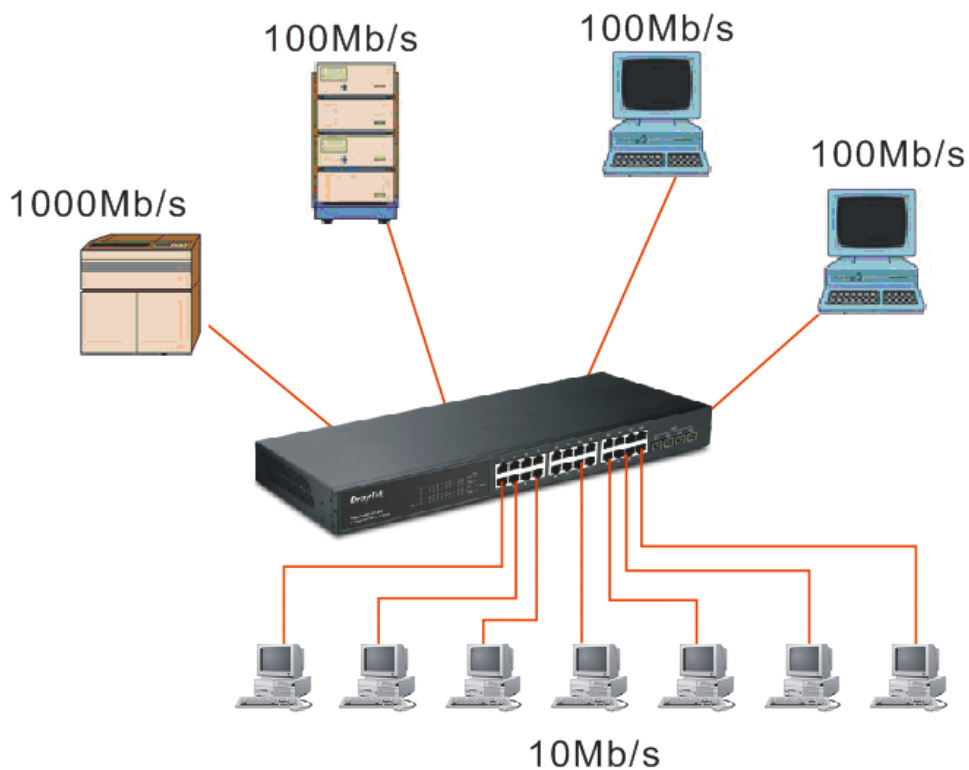
The switch port can run at different speed, such as 10Mbps, 100Mbps or 1000Mbps. A shared hub cannot afford this.

### Extended Distance Limitations:

Traffic aggregation is to aggregate the bandwidth of more than one port and treat it as a single port in the LAN. This single port possesses the features of a normal port but loading balance. This is a great feature for the port needing more bandwidth but cannot afford paying much cost for high bandwidth port. (\* The switch image is sample only.)

### Traffic Aggregation:

Traffic aggregation is to aggregate the bandwidth of more than one port and treat it as a single port in the LAN. This single port possesses the features of a normal port but loading balance. This is a great feature for the port needing more bandwidth but cannot afford paying much cost for high bandwidth port. (\* The switch image is sample only.)



### How does a switch operate?

A Layer 2 switch uses some features of the Data Link layer in OSI model to forward the packet to the destination port(s). Here we introduce some important features of a switch and how they work.

### MAC address table

When a packet is received on a port of switch, the switch first checks if the packet good or bad and extracts the source MAC address (SA) and destination MAC address (DA) to find 1) if SA is existed in the MAC address table, if no, puts it in the MAC address table, if yes, 2) looks up DA and its associated port to which the traffic is forwarded. If DA does not exist, have the packet broadcasted.

Due to the size of the MAC address limited, MAC address aging function is applied. When the MAC address has resided and keeps no update in the table for a long time, this means

the traffic using that entry has yet come for a while. If this time period is more than the aging time, the entry will be marked invalid. The vacancy is now available for other new MAC.

Both learning and forwarding are the most important functions in a switch. Besides that, VLAN can be one of the rules to forward the packet. There are ingress rule and egress rule applied. The ingress rule is used to filter the incoming packet by VLAN ID and so on and to decide whether the packet is allowed to enter the switch or not. The egress rule is used to forward the packet to the proper port.

### **Mac address aging**

There is a field in MAC address table used to put the entry's Age time which determines how long a MAC entry can reside in a switch. The age time is refreshed when a packet with that SA. Usually, the age time is programmable.

### **Transmission schedule**

In most layer 2 switches, the QoS is supported. QoS in a switch must associate a transmission schedule to transmit the packet. This function is much to do with the priority level a packet has. With the given priority, the scheduler will do the proper action on it. The scheduler has many ways to implement, and different chips may support different schedule algorithms. Most common schedulers are:

FCFS: First Come First Service.

Strictly Priority: All High before Low.

Weighted Round Robin:

Set a weight figure to the packet with a priority level, say 5-7, and next, set another weight to the packet with a priority level, say 2-4 and so on. The WRR will transmit the packet with the weight. So the packet of each priority level can be allocated a fixed bandwidth.

### **Bandwidth rating**

Bandwidth rating is the limitation set by administrator, and it can be applied to those with SLA. Bandwidth rating can be total bandwidth, types of service of a port with many steps. The switch supports by-port Ingress and Egress total bandwidth rate control capacity. The bandwidth rate resolution is 0.1 Mbps (100Kbps) and ranges from 0 to 100Mbps.

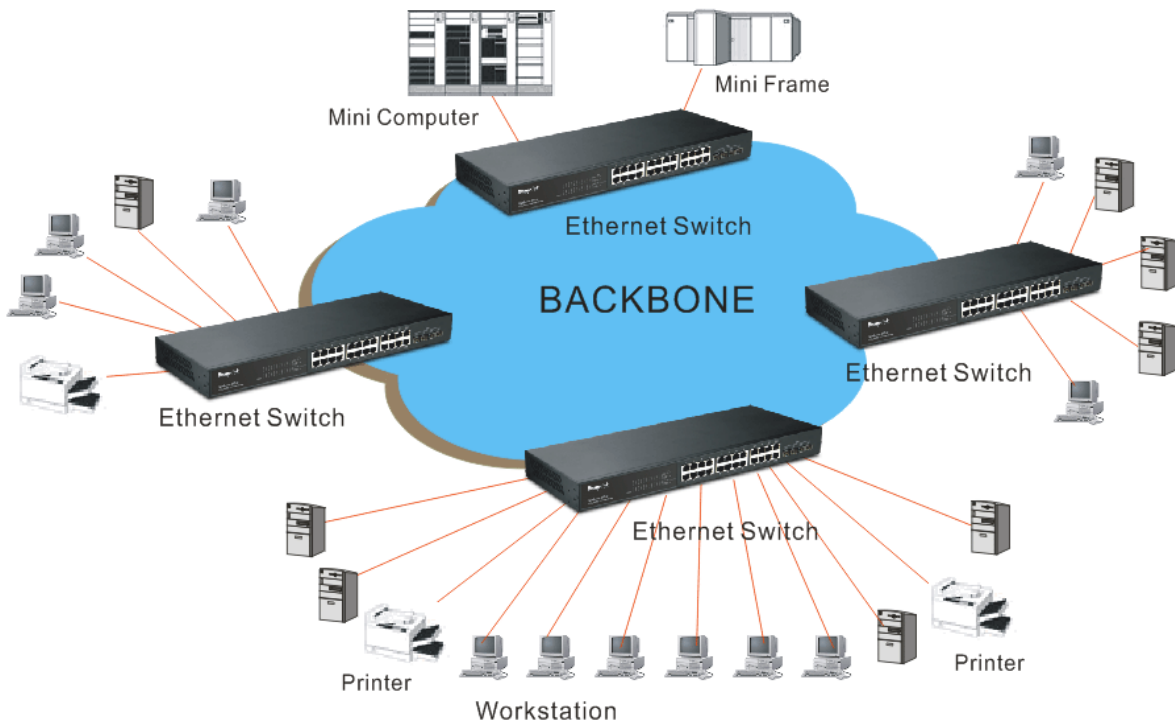
## **2.5 Virtual LAN**

### **What is a VLAN?**

It is a subset of a LAN. Before we discuss VLAN, we must understand what LAN is. In general, a LAN is composed of different physical network segments bridged by switches or bridges which attach to end stations in the same broadcast domain. The traffic can reach any station on the same LAN. Beyond this domain, the traffic cannot go without router's help. This also implies that a LAN is limited. If you need to communicate with the station outside the LAN, a router is needed which always lies on the edge of the LAN.

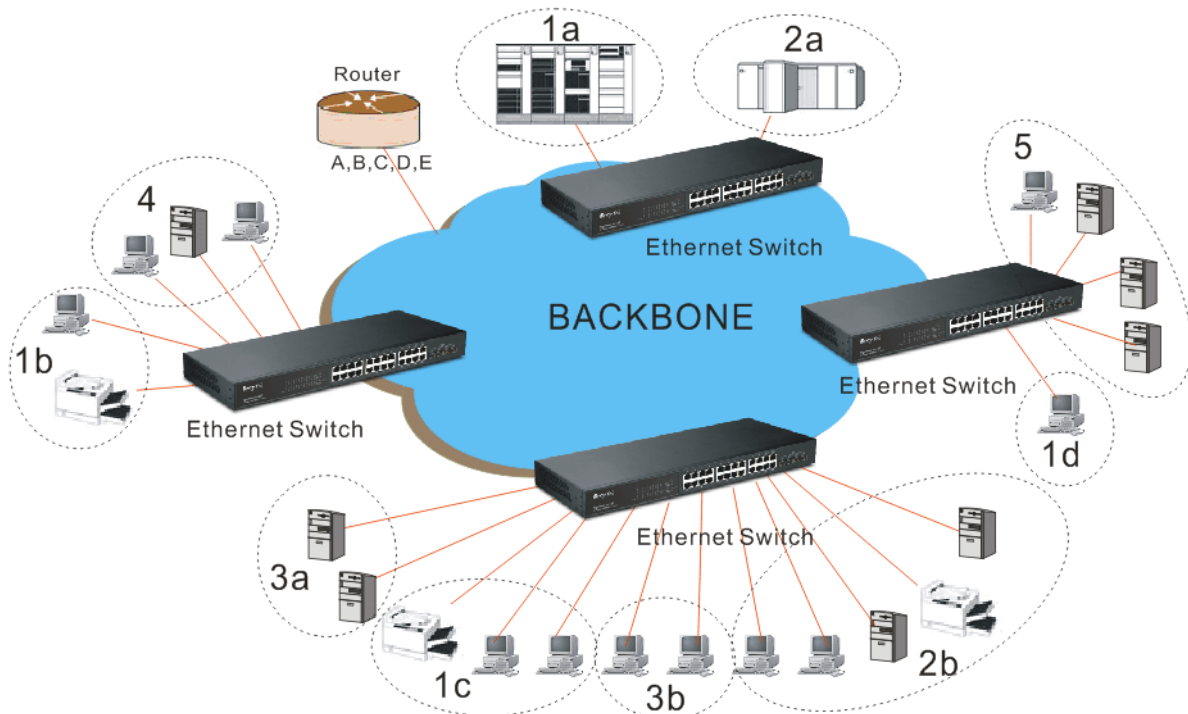
For a layer 2 VLAN, it assumes it is a logical subset of a physical LAN separated by specific rules such as tag, port, MAC address and so on. In other words, they can communicate with each other between separated small physical LANs within a LAN but can not be between any two separated logical LANs.

(\* The switch image is sample only.)



In the figure above, all stations are within the same broadcast domain. For these stations, it is obviously that the traffic is getting congested while adding more stations on it. With the more and more users joining the LAN, broadcast traffic will rapidly decrease the performance of the network. Finally, the network may get down.

(\* The switch image is sample only.)



Now we apply VLAN technology to configure the system shown as the figure above. We can partition the users into the different logical networks which have their own broadcast domain. The traffic will not disturb among these logical networks. The users 1x (x denotes a ~ d) are members of VLAN 1. Any traffic within VLAN 1 does not flow to VLAN 2 and



others. This helps us configure the network easily according to the criteria needed, for example, financial, accounting, R&D and whatever you think it necessary. You can also easily move a user to a different location or join a new user somewhere in the building to VLAN. Without VLAN, it is very hard to do. Basically, VLAN can afford offering at least 3 benefits: move and change users, reduce broadcast traffic and increase performance, Security.

Besides, VLAN can highly reduce the traffic congestion and increase total performance because there are no more too many users in the same broadcast domain.

There are many types of VLAN applied. Most popular is port-based VLAN, tag-based VLAN and protocol-based VLAN.

➤ **Port-based VLAN**

Some physical ports are configured as members of a VLAN. All stations attached on these ports can communicate with each other.

➤ **Tag-based VLAN**

It identifies the membership by VLAN ID, no matter where the packet comes from. It is also referred to as 802.1Q VLAN.

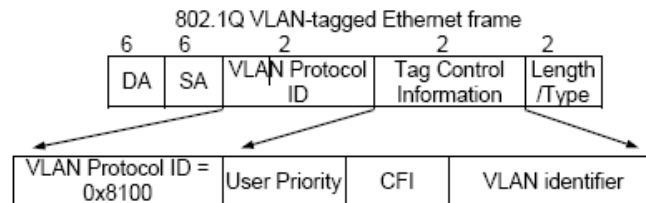
➤ **Protocol-based VLAN**

It identifies the VLAN membership by layer 3 protocol types, for example IPX, Appletalk, IP, etc.

Other VLAN technologies not mentioned above are MAC-based VLAN, IP-based VLAN and so on.

### Terminology

**Tagged Frame:** A frame, carrying a tag field following the source MAC address, is four bytes long and contains VLAN protocol ID and tag control information composed of user priority, Canonical Format Indicator (CFI) and optional VLAN identifier (VID). Normally, the maximal length of a tagged frame is 1522 bytes.



**VLAN Protocol ID:** 8100 is reserved for VLAN-tagged frame.

**User Priority:** 3 bits long. User priority is defined to 7 – 0. 0 is the lowest priority.

**CFI:** Canonical Format Indicator. 1 bit long. It is used to encapsulate a token ring packet to let it travel across the Ethernet. Usually, it is set to 0.

**VLAN ID:** 12 bits long. 0 means no VLAN ID is present. 1 means default VLAN, 4095 reserved.

**VLAN-tagged frame:** An Ethernet frame, carrying VLAN tag field, contains VLAN identification without the value of 0 and 4095, and priority information.

**Priority-tagged frame:** An Ethernet frame, carrying VLAN tag field, contains VLAN identification with the value of 0 and priority information.

- Untagged frame: An Ethernet frame carries no VLAN tag information.
- VLAN Identifier: Also referred to as VID. It is used to identify a member whether it belongs to the VLAN group with the VID. The assignable number is 1- 4094. If VID=0, the tagged frame is a priority packet. Both the value of 0 and 4095 also cannot be assigned in VLAN management.
- Port VLAN Identifier: VLAN identifier of a port. It also can be referred to as PVID. When an untagged frame or a priority-tagged frame is received, the frame will be inserted the PVID of that port in the VLAN tag field. The frame with VID assigned by a port is called PVID. Each port can only be assigned a PVID. The default value for PVID is 1, the same as VID.
- Ingress filtering: The process to check a received packet and compare its VID to the VLAN membership of the ingress port. The ingress filtering can be set by per port. When receiving a packet, VLAN bridge examines if the VID in the frame's header presents.
- If the VID of the received packet presents, the VID of the packet is used. And VLAN bridge will check its MAC address table to see if the destination ports are members of the same VLAN. If both are members of the tagged VLAN, then the packet will be forwarded.
- If the packet is an untagged or a null tag packet, the ingress port's PVID is applied to the packet. VLAN bridge will then look up the MAC address table and determine to which ports the packet should be forwarded. Next, it will check to see if the destination ports belong to the same VLAN with that PVID. If the destination ports are members of the VLAN used by ingress port, the packet will be forwarded.
- Note: VID can not be 0 or 4095.
- Ingress Rule: Each packet received by a VLAN-aware bridge will be classified to a VLAN.
- The classification rule is described as follows.
1. If the VID of the packet is null VID (VID=0) or this packet is an untagged packet:
    - a. If there are still some other ways (e.g. protocol, MAC address, application, IP-subnet, etc.) to classify the incoming packets beside port-based classification in implement and these approaches can offer non-zero VID, then, use the value of VID offered by other classifications for VLAN's classification.
    - b. If there is only port-based classification in implement or other classification approaches cannot offer non-zero VID for the incoming packets, then assign the PVID to the incoming packets as VID for the classification of the VLAN group.
  2. If the VID is not a null VID (VID≠0), then use the value to classify the VLAN group.
- Egress Rule: An egress list is used to make the tagging and forwarding decision on an outgoing port. It specifies the VLANs whose packets can be transmitted out and specifies if the packet should be tagged or not. It can be configured for port's VLAN membership, and tagged or



untagged for a transmitted packet. When a packet is transmitted out, the VLAN bridge checks the port's egress list. If the VLAN of the packet is on the egress list of the port on which the packet transmits out, the packet will be transmitted with the priority accordingly. If enabled, an egress port will transmit out a tagged packet if the port is connected to a 802.1Q-compliant device.

If an egress port is connected to a non-802.1Q device or an end station, VLAN bridge must transmit out an untagged packet, i.e. the tag has been stripped off in an egress port. Egress rule can be set by per port.

**Independent VLAN Learning (IVL):** It specifies the mode how to learn MAC address. For a specified VLAN, it will use an independent filtering database (FID) to learn or look up the membership information of the VLAN and decide where to go.

**Shared VLAN Learning (SVL):** It specifies the mode how to learn MAC address. In this mode, some VLAN or all VLANs use the same filtering database storing the membership information of the VLAN to learn or look up the membership information of the VLAN. In 24-Port GbE Web Smart Switch, you can choose a VID for sharing filtering database in Shared VID field if you wish to use the existed filtering database. For a specified VLAN, when a MAC address is learned by a switch, VLAN will use this formation to make forwarding decision.

**Filtering Database:** Referred to as FID. It can provide the information where the packet will be sent to. Filtering database will supply the outgoing port according to the request from forwarding process with VID and DA. When a packet is received, if it has a non-zero VID, then FID will offer the associated outgoing ports information to the packet.

In SVL, VLANs use the same Filtering Database. In IVL, VLANs use different FIDs. Any VID can be assigned to the same FID by administrator.

## **How does a Tagged VLAN work?**

If the ingress filtering is enabled and when a packet is received, VLAN bridge will first check if the VID of the packet presents.

- 1.) If the packet has a non-zero VID, VLAN bridge will apply this VID as the VLAN ID of the packet in the network.
- 2.) For a packet with null tag or no VLAN tag, if VLAN bridge provides rules to decide its VID, then apply this VID to the packet.

If VLAN bridge does not support any rule for VID, then apply the PVID of the port to the packet which came from that port. VLAN bridge checks to see if the ingress port and the received packet are on the same VLAN. If not, drops it. If yes, forwards it to the associated ports. Meanwhile, this VLAN must be applied to the egress port, or the packet will be dropped.

If ingress filtering is disabled, VLAN bridge will only check the MAC address table to see if the destination VLAN exists. If VLAN does not exist, then drop the packet, and if both DA and VLAN do not exist, forwards the packet. If just knows VLAN existed, then floods the packet to all the ports the VLAN covers.

If we plan to deploy four VLANs in an office and use a switch to partition them, we should check which ports belong to which VLAN first. Assuming a 24-port switch is applied.

Name	VID	Port Members
Marketing	2	1,2,3,4,5
Service	3	6,7,20,21,22
Sales	4	8,9,10,11,12,13,14,15,16
Administration	1	17,18,19,23,24

Next, assigns IP address to each VLAN. Usually, we use 10.x.x.x as internal IP block. Because there are total four VLANs in the network, we must assign 4 IP blocks to each of them.

Name	VID	Port Members
Marketing	2	10.1.2.0/24
Service	3	10.1.3.0/24
Sales	4	10.1.4.0/24
Administration	1	10.1.1.0/24

Here we apply the subnet mask 255.255.255, and each VLAN is capable of supporting 254 nodes.

## 2.6 Link Aggregation

Basically, Link Aggregation is to aggregate the bandwidth of more than one port to an assigned logical link. This highly increases total bandwidth to the targeted device. There is more than one Link Aggregation technology in many vendors' switch products already, which may cause the problem of interoperability. This is the reason why now we have 802.3ad Link Aggregation Control Protocol (LACP).

### Why 802.3ad (LACP)?

Network is varying. For example, if a port malfunctioned or unplugged accidentally in a static trunk port, administrator has to reconfigure it, or the network will get trouble. Therefore, offering a tool with automatic recovery capability is necessary for an administrator. LACP is a protocol that allows a switch able to know whether its partner has the capability to co-setup a trunk between them.

Usually, if administrator wishes to increase the bandwidth of a specific link, he may:

1. Buy new network equipments with higher throughput, or
2. Aggregate the bandwidth of more than one port to a logical link.

If the item 1 is the case, you will pay much more cost beyond your budget, and the solution caused by the limitation of hardware performance may not be scalable.

If the item 2 is the case, now you do not have to pay much more extra cost and can keep flexible according to the demand of bandwidth because all equipments are there already. And what's more, you can avoid worrying about the interoperability issue. Applying LACP in your network, you will not only gain benefits below to improve the performance of your network but also have these investments usable to future new products.

1. Public standardized specification
2. No interoperability issue
3. No change to IEEE 802.3 frame format, no change in software and management.
4. Increased bandwidth and availability
5. Load sharing and redundancy
6. Automatic configuration
7. Rapid configuration and reconfiguration
8. Deterministic behavior
9. Low risk of duplication or mis-ordering
10. Support existing IEEE 802.3 MAC Clients
11. Backwards compatibility with aggregation-unaware devices

There are also some constraints when applying LACP.

1. LACP does not support inter-switch bandwidth aggregation.
2. The ports aggregated must operate in full-duplex mode.
3. The ports in the same Link Aggregation Group must have the same speed, for example, all with 100Mbps or all 1000Mbps. You cannot aggregate a 1000Mbps and two 100Mbps for a 1.2Gbps trunk port.

## Terminology

**Link Aggregation:** It is a method to have multiple physical links with the same media and speed bundled to be a logical link forming a Link Aggregation Group with a group ID. With the viewpoint of MAC client, each Link Aggregation Group is an independent link.

There are three cases of link used in the network, which are switch to switch, switch to station and station to station. Here station may be a host or a router.

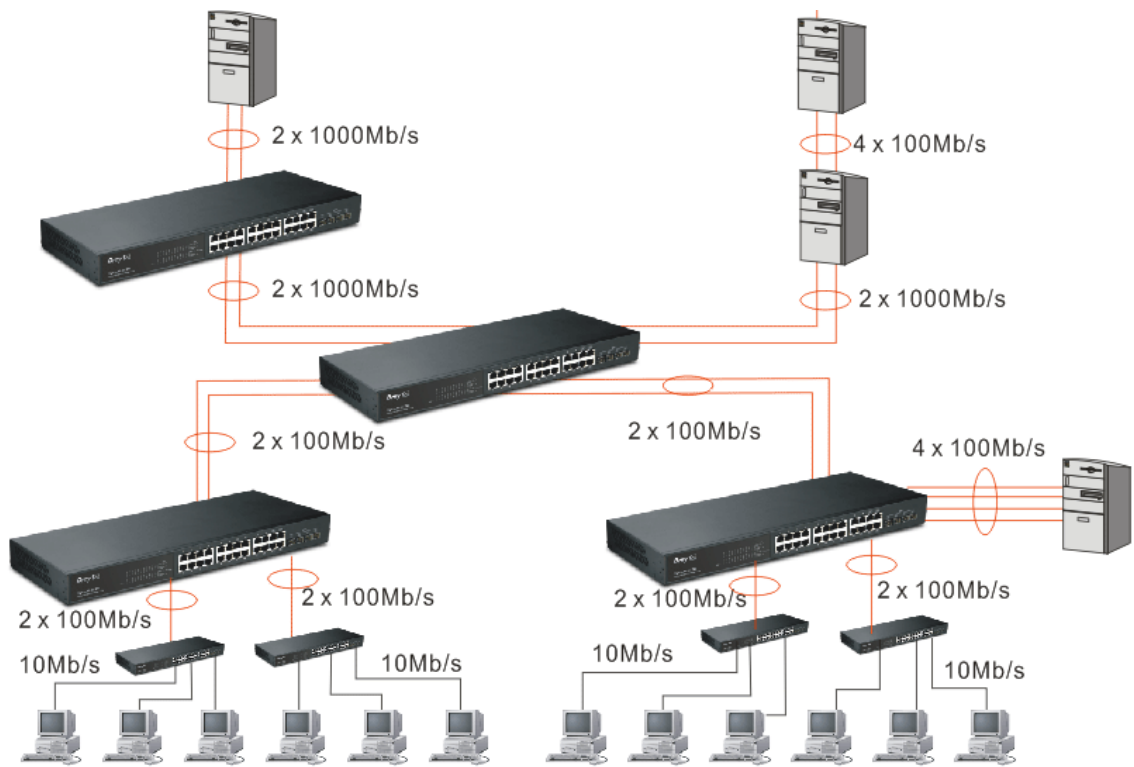
Link Aggregation, called port trunking sometimes, has two types of link configuration, including static port trunk and dynamic port trunk.

➤ **Static Port Trunk:**

When physical links are changed, administrator needs to manually configure the switches one by one.

➤ **Dynamic Port Trunk:**

When physical links are changed, LACP takes over and automatically reconfigure. Administrator does not have to do anything and may see the trap message of LACP changed in NMS.

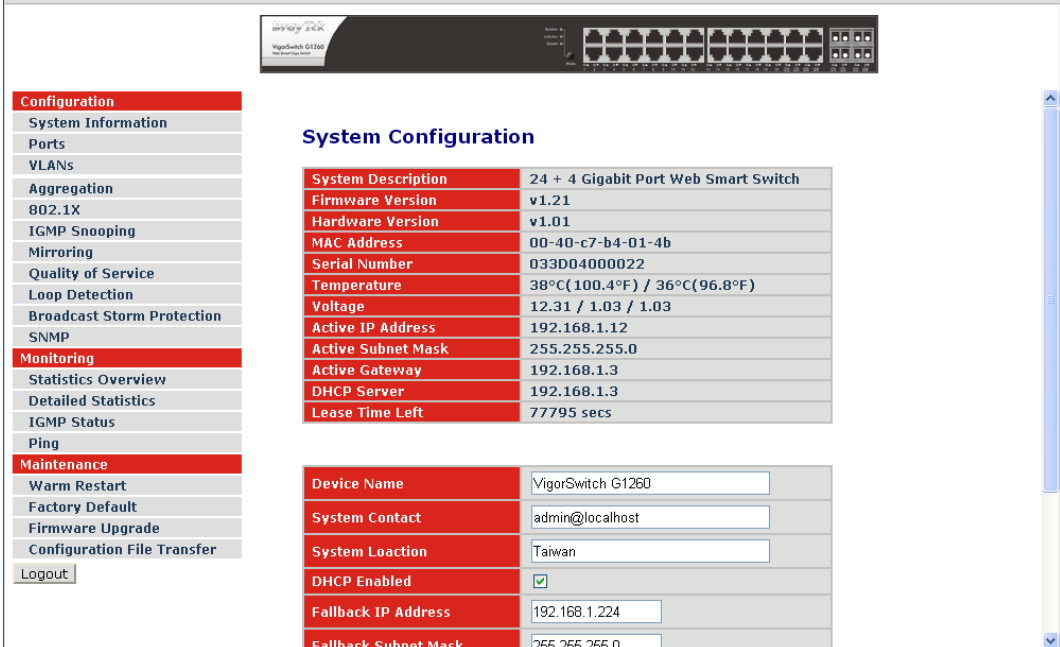


# 3

## Operation of Web-based Management

This chapter would introduce how to manage your Web Smart Switch and how to configure the 10/100/1000Mbps TP Ports and Gigabit TP/SFP Fiber dual media ports on the switch via web user interfaces. Web Smart Switch provides 20 fixed Gigabit Ethernet TP ports and 4 optional Gigabit dual media ports. With this facility, you can easily access and monitor the status like MIBs, port activity, and multicast traffic through any ports on the switch.

The default values of the Switch are listed in the figure below:



The screenshot displays the web management interface for a VigorSwitch G1260. At the top, there is a navigation menu with categories: Configuration, Monitoring, and Maintenance. Under Configuration, options include System Information, Ports, VLANs, Aggregation, 802.1X, IGMP Snooping, Mirroring, Quality of Service, Loop Detection, Broadcast Storm Protection, and SNMP. Under Monitoring, options include Statistics Overview, Detailed Statistics, IGMP Status, and Ping. Under Maintenance, options include Warm Restart, Factory Default, Firmware Upgrade, and Configuration File Transfer. A Logout button is also present.

The main content area is titled "System Configuration" and contains two tables of system information and configuration fields.

System Configuration	
System Description	24 + 4 Gigabit Port Web Smart Switch
Firmware Version	v1.21
Hardware Version	v1.01
MAC Address	00-40-c7-b4-01-4b
Serial Number	033D04000022
Temperature	38°C(100.4°F) / 36°C(96.8°F)
Voltage	12.31 / 1.03 / 1.03
Active IP Address	192.168.1.12
Active Subnet Mask	255.255.255.0
Active Gateway	192.168.1.3
DHCP Server	192.168.1.3
Lease Time Left	77795 secs

Device Name	VigorSwitch G1260
System Contact	admin@localhost
System Location	Taiwan
DHCP Enabled	<input checked="" type="checkbox"/>
Fallback IP Address	192.168.1.224
Fallback Subnet Mask	255.255.255.0

When the configuration of your Web Smart Switch is finished, you can browse it by the IP address you set up. For instance, uncheck the **Enable** box of DHCP Setting first (it is enabled in default). Next, type `http://192.168.1.1` in the address row in a browser, then the following screen (see Fig.4-1) would show up and ask for your password input for login and access authentication. The default password is "admin". For the first time access, please enter the default password, and click <Apply> button. The login process now would be completed.

Web Smart Switch supports a simplified user management function which allows only one administrator to configure the switch at one time.

To optimize the display effect, we recommend Microsoft IE and 1024x768 display resolution.

Password

.....

Login

## 3.1 Web Management Home Overview

After login, System Information would be displayed as the following illustration. This page lists default values and shows you the basic information of the switch, including “Switch Status”, “TP Port Status”, “Fiber Port Status”, “Aggregation”, “VLAN”, “Mirror”, “SNMP”, and “Maximum Packet Length”. With this information, you will know the software version, MAC address, ports available and so on. It would be helpful while malfunction occurred. For more details, please refer to Section 3.1.1.

### 3.1.1 The Information of Page Layout

On the top part of the information page, it shows the front panel of the switch. Linked ports will be displayed in green color, and linked-off ones will be in black. For the optional modules, the slots with no module will only show covered plates, the other slots with installed modules would present modules. The images of modules would depend on the ones you insert. Vice versa, if ports are disconnected, they will show just in black.

On the left side, the main menu tree for web is listed in the page. The functions of each folder are described in its corresponded section respectively. As to the function names in normal type are the sub-functions. When clicking it, the function is performed. The following list is the main function tree for web user interface.

## 3.2 System

### 3.2.1 System Information and IP Configuration

System configuration is one of the most important functions. Without a proper setting, network administrator would not be able to manage the device. The switch supports manual IP address setting.

**Function name:**

System configuration

**Function description:**

Show system description, firmware version, hardware version, MAC address, serial number, host IP address, host MAC address, active subnet mask, active gateway, and DHCP server.

Set device name, uncheck DHCP setting, IP address, subnet mask, default gateway, management VLAN, password and auto logout.

#### System Configuration

System Description	24 + 4 Gigabit Port Web Smart Switch
Firmware Version	v1.21
Hardware Version	v1.01
MAC Address	00-40-c7-b4-01-4b
Serial Number	033D04000022
Temperature	38°C(100.4°F) / 36°C(96.8°F)
Voltage	12.31 / 1.03 / 1.03
Active IP Address	192.168.1.12
Active Subnet Mask	255.255.255.0
Active Gateway	192.168.1.3
DHCP Server	192.168.1.3
Lease Time Left	77795 secs

Device Name	VigorSwitch G126U
System Contact	admin@localhost
System Location	Taiwan
DHCP Enabled	<input checked="" type="checkbox"/>
Fallback IP Address	192.168.1.224
Fallback Subnet Mask	255.255.255.0
Fallback Gateway	192.168.1.1
Management VLAN	1
Password	*****
Auto Logout (0, 60-10000 Secs)	300

Apply Refresh

---

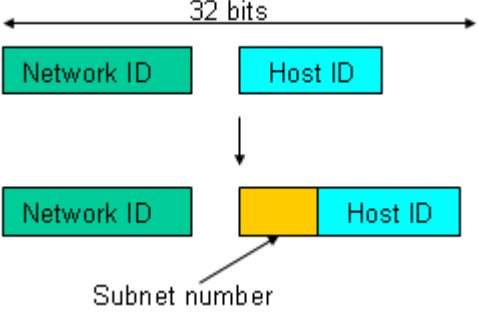
#### Parameter description:

System description	Display what the device's description.
--------------------	--

---

Firmware version	The firmware version in this switch.
Hardware Version	The hardware version of this switch.
MAC address	It is the Ethernet MAC address of the management agent in this switch.
Serial number	The serial number is assigned by the manufacturer.
Temperature	The Temperature of this switch (near power supply/ near fan Entrance).
Voltage	The voltage of this switch.(power supply/MAC/PHY)
Active IP address	The IP address of the switch.
Active Subnet Mask	Show the active subnet mask of this switch.
Active Gateway	Show the active gateway of this switch.
DHCP Server	Show the IP address of the DHCP server. Default: 0.0.0.0
Lease Time Left	Show the lease time left of DHCP client.
Device name	The name of the switch, User-defined. Default is VigorSwitch G1260.
System 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.
System Location	Set the location of the switch where it was located.
DHCP Enabled	Enable DHCP snooping, Just tick the check box ( <input checked="" type="checkbox"/> ) to enable it. Default: disable
Fallback IP Address	Users can configure the IP settings and fill in new values. Then, click <Apply> button to update. Default: 192.168.1.224
Fallback 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 ( $2^{(\text{bit number of subnet number})}$ ).



	 <p>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.</p> <p>For more information, please also see the Section 2-1-4 “IP Address Assignment” in this manual.</p> <p>Default: 255.255.255.0</p>
Fallback Gateway	<p>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.</p> <p>Default: 192.168.1.1</p>
Management VLAN	<p>Set the management VLAN number.</p>
Password	<p>Set a password for this switch. Up to 16 characters are allowed in this parameter. Any alphanumeric character is acceptable.</p> <p>Default: admin</p>
Auto Logout	<p>Set the auto-logout timer. The valid value is 0, 60 ~ 10000 in the unit of minute and a decimal point is not allowed. The value OFF means auto-logout timer is disabled.</p> <p>Default: OFF</p>

## 3.3 Port

### 3.3.1 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:**

Port Configuration is applied for the settings of the ports (TP Ports and Fiber Ports) on the switch. By this function, you can set or reset the values for Mode and Flow Control.

### Port Configuration

Enable Jumbo Frames(Up to 9600 bytes)

Power Saving

Drop frames after excessive collisions  
(Use in Half Duplex flow control environment)

#### TP Ports

Port	Link	Mode	Flow Control
1	Down	Auto Speed	✓
2	Down	Auto Speed	✓
3	1000FDX	Auto Speed	✓
4	Down	Auto Speed	✓
...	...	...	...
24	Down	Auto Speed	✓

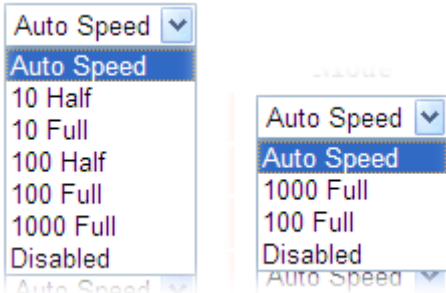
#### Fiber Ports

Port	Link	Mode	Flow Control
21	Down	Auto Speed	✓
22	Down	Auto Speed	✓
23	Down	Auto Speed	✓
24	Down	Auto Speed	✓

---

**Parameter description:**

---

Enable Jumbo Frames	This function support jumbo frames of up to 9600 bytes, Just tick the check box (☑) to enable it. Default: disable
Power Saving	This function supports Power Saving. Default: disable
Drop frames after excessive collisions	Drop frames after excessive collisions. After an excessive collision, the MAC drop frames might occur. If yes, a frame is dropped after excessive collision. This is IEEE Standard 802.3 half-duplex flow control operation.
Link	Show link status of this port.
Mode	Set the speed and duplex of the port. If the media is 1Gbps fiber, there are three modes to choose: <b>Auto Speed, 1000/100 Full</b> and <b>Disable</b> . If the media is TP, the speed is <b>Auto Speed, 10 /100 /1000 Mbps (Full/Half)</b> and <b>Disabled</b> . The following table summarized the function the media supports. In Auto mode, no default value. 
Flow Control	You can Just tick the check box (☐) to enable flow control. 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. Default: Disable

## 3.4 VLANs

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.

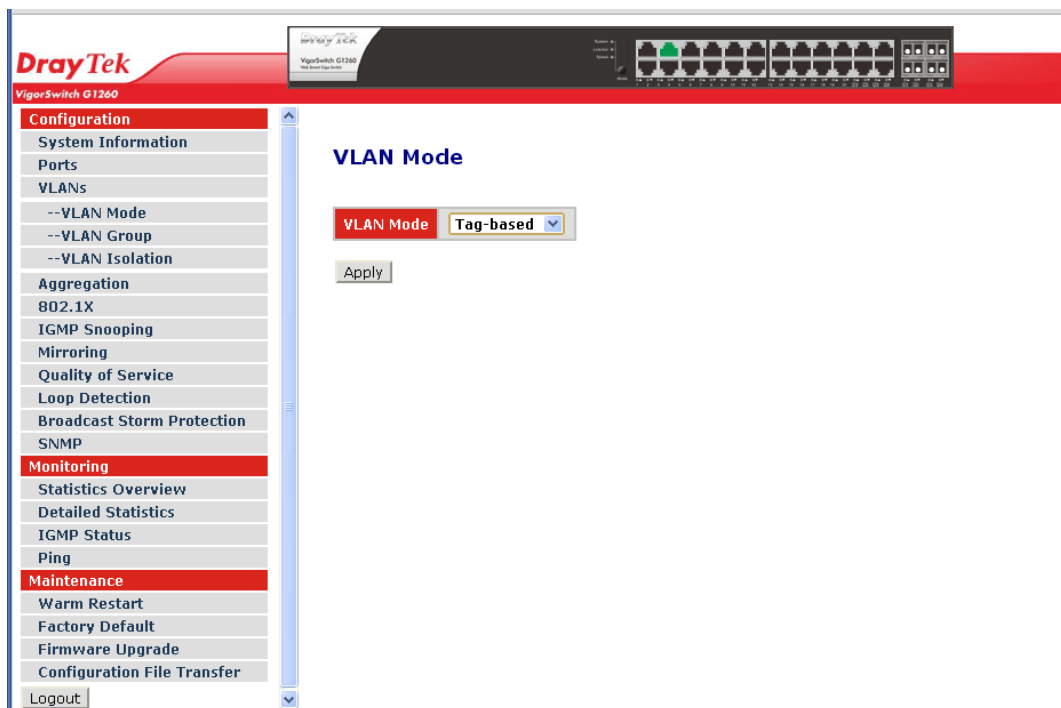
### 3.4.1 VLAN Mode

**Function name:**

VLAN Mode

**Function description:**

The VLAN Mode Selection function includes two modes: Port-based, Tag-based, 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:**

<p>VLAN Mode</p>	<p><i>Port-based</i> –  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&amp;2&amp;3&amp;4. If you are on the port 1, you can communicate with port 2&amp;3&amp;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.</p> <p><i>Tag-based</i> –  Tag-based VLAN identifies its member by VID. This is</p>
------------------	---

---

<p>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.</p>
--

<p>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.</p>
--

---

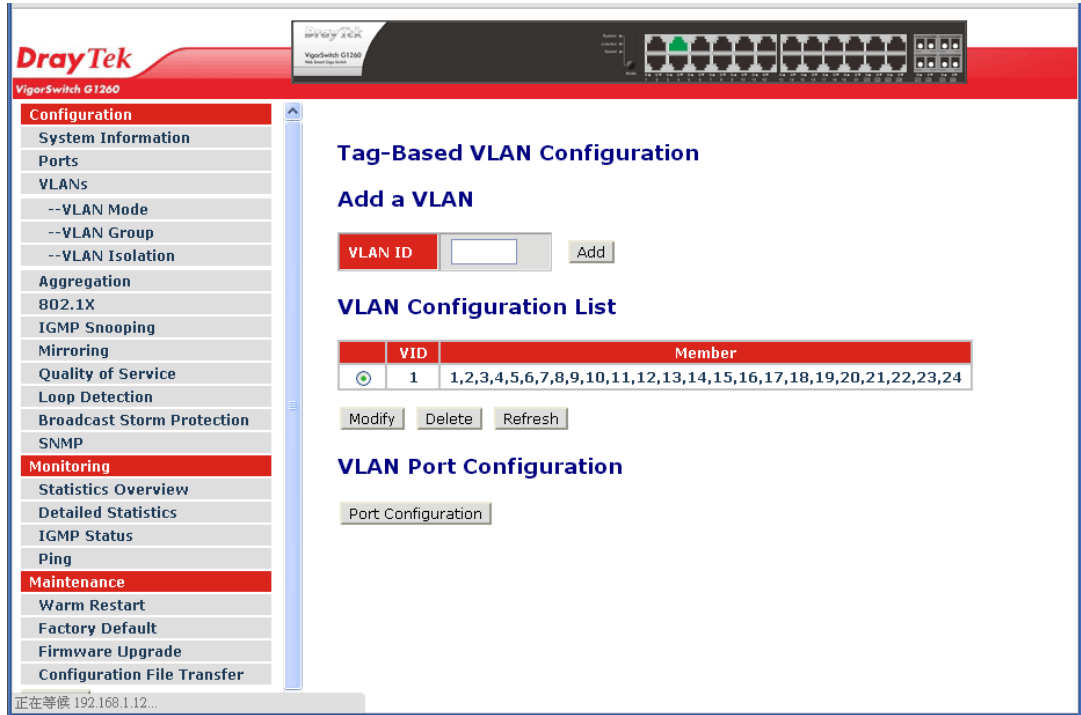
### 3.4.2 VLAN Group – Tag-based

**Function name:**

VLAN Group - Tag-based VLAN Configuration

**Function description:**

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



**Parameter description:**

Add a VLAN	<p>Create a new port-based VLAN or tag-based VLAN, which depends on the VLAN mode you choose in VLAN mode function.</p> <p>Please input the VLAN ID first, then click on &lt;Add &gt; to create a new Tag-based VLAN with the ID specified.</p>
------------	---

## VLAN Setup

VLAN ID: 20			
Port	Member	Port	Member
Port 1	<input checked="" type="checkbox"/>	Port 13	<input type="checkbox"/>
Port 2	<input checked="" type="checkbox"/>	Port 14	<input type="checkbox"/>
Port 3	<input checked="" type="checkbox"/>	Port 15	<input type="checkbox"/>
Port 4	<input checked="" type="checkbox"/>	Port 16	<input type="checkbox"/>
Port 5	<input checked="" type="checkbox"/>	Port 17	<input type="checkbox"/>
Port 6	<input type="checkbox"/>	Port 18	<input type="checkbox"/>
Port 7	<input type="checkbox"/>	Port 19	<input type="checkbox"/>
Port 8	<input type="checkbox"/>	Port 20	<input type="checkbox"/>
Port 9	<input type="checkbox"/>	Port 21	<input type="checkbox"/>
Port 10	<input type="checkbox"/>	Port 22	<input type="checkbox"/>
Port 11	<input type="checkbox"/>	Port 23	<input type="checkbox"/>
Port 12	<input type="checkbox"/>	Port 24	<input type="checkbox"/>

Port Member 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.

Click <**Apply**> to have the setting taken effect.

### VLAN Configuration List

	VID	Member
<input type="radio"/>	1	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24
<input checked="" type="radio"/>	20	1,2,3,4,5,

### VLAN Port Configuration

VLAN ID	Type an ID number for identification.
VLAN Configuration List	<p><i>VID</i> - VLAN identifier. Each tag-based VLAN group has a unique VID. It appears only in tag-based and Double-tag mode.</p> <p><i>Member</i> - Display the selected port members that will apply to such VLAN group.</p> <p><i>Modify</i> - Just press the &lt;Modify&gt; button to edit the selected group entry.</p> <p><i>Delete</i> - Just press the &lt;Delete&gt; button to remove the selected group entry from the Tag-based group table.</p>
VLAN Port Configuration	Press the < <b>Port Configuration</b> > button to open the following page to configure tag-based VLAN group in

detail.

## Detailed for Port Configuration

### VLAN Per Port Configuration

Port#	Ingress Filtering	Frame Type	PVID	Role	Untagged VID
1	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	<input type="text" value="1"/>	Access	<input type="text" value="1"/>
2	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	<input type="text" value="1"/>	Access	<input type="text" value="1"/>
3	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	<input type="text" value="1"/>	Access	<input type="text" value="1"/>
4	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	<input type="text" value="1"/>	Access	<input type="text" value="1"/>
5	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	<input type="text" value="1"/>	Access	<input type="text" value="1"/>
6	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	<input type="text" value="1"/>	Access	<input type="text" value="1"/>
7	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	<input type="text" value="1"/>	Access	<input type="text" value="1"/>
8	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	<input type="text" value="1"/>	Access	<input type="text" value="1"/>
9	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	<input type="text" value="1"/>	Access	<input type="text" value="1"/>
10	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	<input type="text" value="1"/>	Access	<input type="text" value="1"/>
11	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	<input type="text" value="1"/>	Access	<input type="text" value="1"/>
12	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	<input type="text" value="1"/>	Access	<input type="text" value="1"/>
13	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	<input type="text" value="1"/>	Access	<input type="text" value="1"/>
14	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	<input type="text" value="1"/>	Access	<input type="text" value="1"/>
15	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	<input type="text" value="1"/>	Access	<input type="text" value="1"/>
16	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	<input type="text" value="1"/>	Access	<input type="text" value="1"/>
17	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	<input type="text" value="1"/>	Access	<input type="text" value="1"/>
18	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	<input type="text" value="1"/>	Access	<input type="text" value="1"/>
19	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	<input type="text" value="1"/>	Access	<input type="text" value="1"/>
20	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	<input type="text" value="1"/>	Access	<input type="text" value="1"/>
21	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	<input type="text" value="1"/>	Access	<input type="text" value="1"/>
22	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	<input type="text" value="1"/>	Access	<input type="text" value="1"/>
23	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	<input type="text" value="1"/>	Access	<input type="text" value="1"/>
24	<input type="checkbox"/>	<input checked="" type="radio"/> All <input type="radio"/> Tagged Only	<input type="text" value="1"/>	Access	<input type="text" value="1"/>

Apply Cancel

#### Parameter description:

Port	Display the number of the LAN port in the switch.
Ingress Filtering	You can check this box to discard other VLAN group packets, but only forward this port joined VLAN group packets.
Frame Type	Specify a frame type to forward packets. <i>All</i> - Forward all tagged and untagged packets. <i>Tagged Only</i> - Forward tagged packets only and discard untagged packets.
PVID	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.
Role	It is an egress rule for the port. Choose Access, Trunk or Hybrid.



	<div data-bbox="699 197 842 322" style="border: 1px solid black; padding: 2px;"> <b>Access</b> ▾  <b>Access</b>  <b>Trunk</b>  <b>Hybrid</b> </div> <p><i>Trunk</i> - means the outgoing packets must carry VLAN tag header.</p> <p><i>Access</i> - 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.</p> <p><i>Hybrid</i> - 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.</p>
Untag VID	Valid range is 1~4094. It works only when Role is set to Hybrid.

### 3.4.3 VLAN Group - Port-based

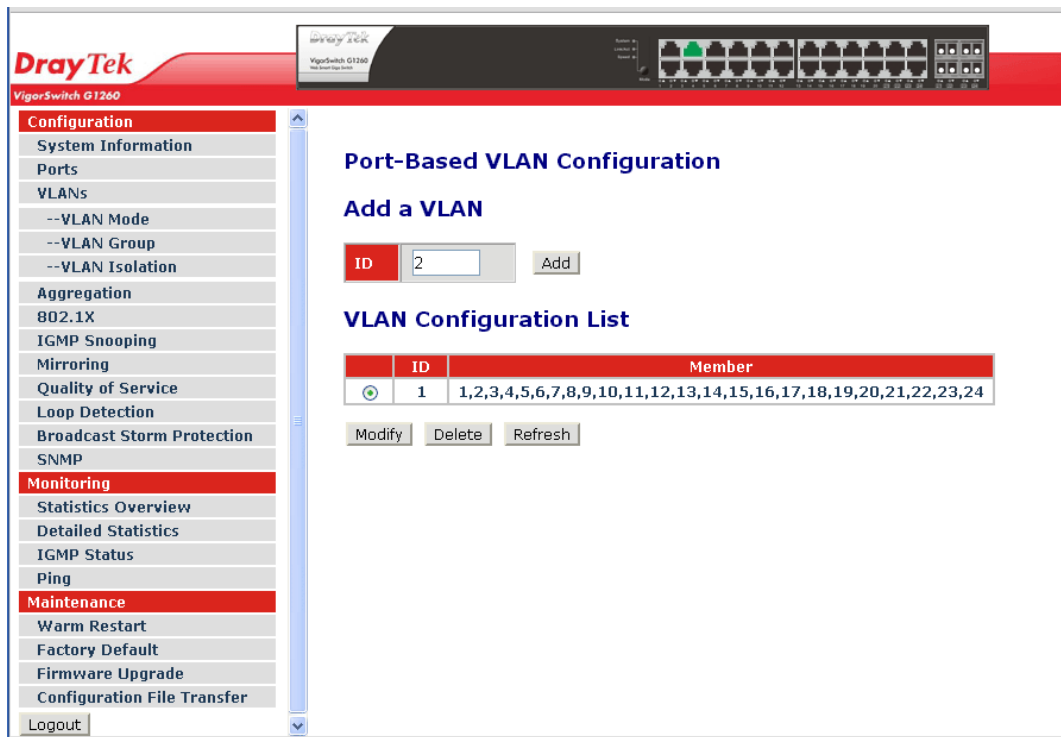
**Function name:**

VLAN Group - Port-based VLAN Configuration

**Function description:**

It shows the information of VLAN Groups, and allows administrators to maintain them by modifying and deleting each VLAN group. User also can add a new VLAN group by inputting a new VLAN name and VLAN ID.

If you are in port-based VLAN, it will just show the ID · Member of the existed port-based VLAN group. If you are in tag-based VLAN, it will show the ID · VID · Member of the existed tag-based VLAN group. The switch can store the configuration of port-based VLAN and tag-based VLAN separately. When you choose one of VLAN mode, the switch will bring you the responded VLAN configuration which keeps the default data. You can easily create and delete a VLAN group by pressing <Add> and <Delete> buttons; or click the Group ID directly to edit it.



**Parameter description:**

Add a VLAN	<p>Create a new port-based VLAN or tag-based VLAN, which depends on the VLAN mode you choose in VLAN mode function.</p> <p>Please input the VLAN ID first, then click on &lt;Add &gt; to create a new Port-Based VLAN with specified VLAN name.</p>
------------	---

## Port-Based Vlan Setup

ID: 2			
Port	Member	Port	Member
Port 1	<input checked="" type="checkbox"/>	Port 13	<input type="checkbox"/>
Port 2	<input type="checkbox"/>	Port 14	<input type="checkbox"/>
Port 3	<input type="checkbox"/>	Port 15	<input type="checkbox"/>
Port 4	<input type="checkbox"/>	Port 16	<input type="checkbox"/>
Port 5	<input checked="" type="checkbox"/>	Port 17	<input type="checkbox"/>
Port 6	<input type="checkbox"/>	Port 18	<input type="checkbox"/>
Port 7	<input type="checkbox"/>	Port 19	<input type="checkbox"/>
Port 8	<input type="checkbox"/>	Port 20	<input type="checkbox"/>
Port 9	<input type="checkbox"/>	Port 21	<input type="checkbox"/>
Port 10	<input type="checkbox"/>	Port 22	<input type="checkbox"/>
Port 11	<input type="checkbox"/>	Port 23	<input type="checkbox"/>
Port 12	<input type="checkbox"/>	Port 24	<input type="checkbox"/>

Select All Apply Refresh

Port Members 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.

Click <Apply> to have the setting taken effect.

### VLAN Configuration List

ID	Member
<input type="radio"/> 1	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24
<input checked="" type="radio"/> 2	1,5

Modify Delete Refresh

### VLAN Configuration List

*ID* - When you want to edit a VLAN group, you must select the Group ID field. Then, you will enter Tag Base VLAN Group Setting or Port Base VLAN Group Setting page, which depends on your VLAN mode selection.

*Member* - Display the selected port members that will apply to such VALN group.

*Modify* - Just press the <Modify> button to edit the selected group entry.

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

*Refresh* – Just press it to refresh current page.

### 3.4.4 VLAN Isolation

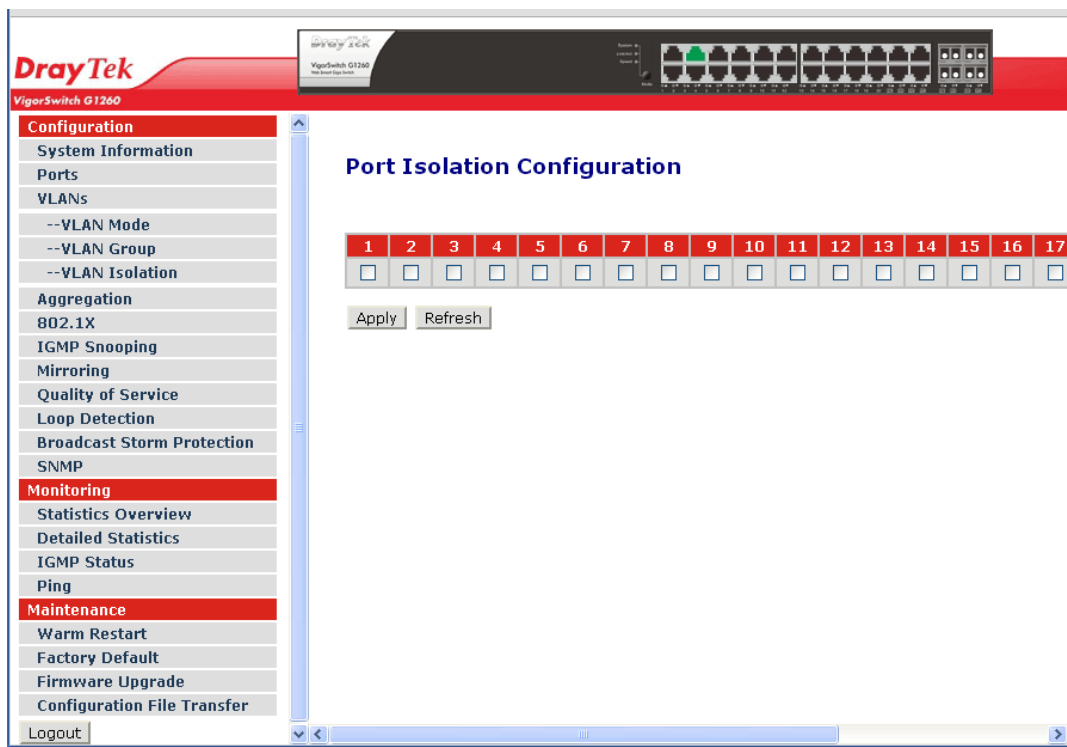
**Function name:**

Port Isolation Configuration

**Function description:**

Port Isolation provides for an apparatus and method to isolate ports on layer 2 switches on the same VLAN to restrict traffic flow. The apparatus comprises a switch having said plurality of ports, each port configured as a protected port or a non-protected port. An address table memory stores an address table having a destination address and port number pair. A forwarding map generator generates a forwarding map which is responsive to a destination address of a data packet. The method for isolating ports 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 the 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. The data packet is then sent to the plurality of ports pursuant to the forwarding map generated based upon whether the ingress port was configured as a protected or non-protected port.

This page is used for enabling or disabling port isolation on ports in a Private VLAN. A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.



**Parameter description:**

Port Members	A check box is provided for each port of a private VLAN. When checked, port isolation is enabled on that port. When unchecked, port isolation is disabled on that port. By default, port isolation is disabled on all ports.
--------------	--

## 3.5 Aggregation

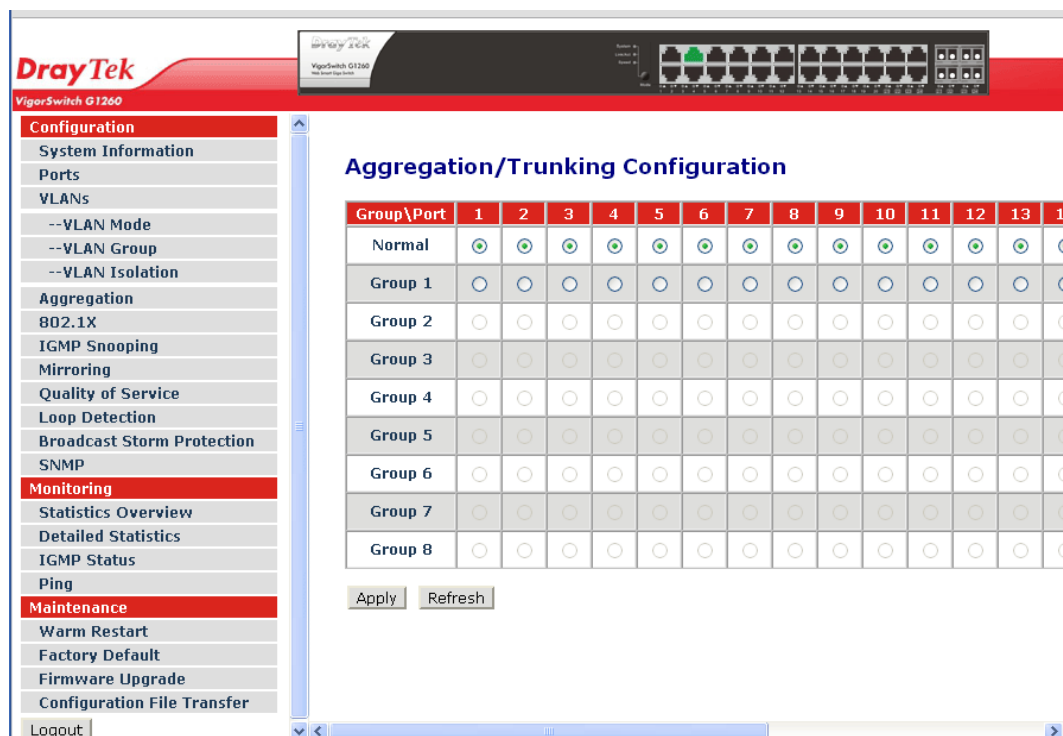
The Aggregation (Port Trunking) Configuration is used to configure the settings of Link Aggregation. You can bundle ports by same speed, MAC, and full duplex to be a single logical port, thus the logical port can aggregate the bandwidth of these ports. This means you can apply your current Ethernet equipments to build the bandwidth aggregation. For example, if three Fast Ethernet ports are aggregated into a logical port, then this logical port's bandwidth would be as three times high as a single Fast Ethernet port's.

**Function name:**

Aggregation Configuration

**Function description:**

Display the current setup of Aggregation Trunking. With this function, user is allowed to add a new trunking group or modify the members of an existed trunking group.



**Parameter description:**

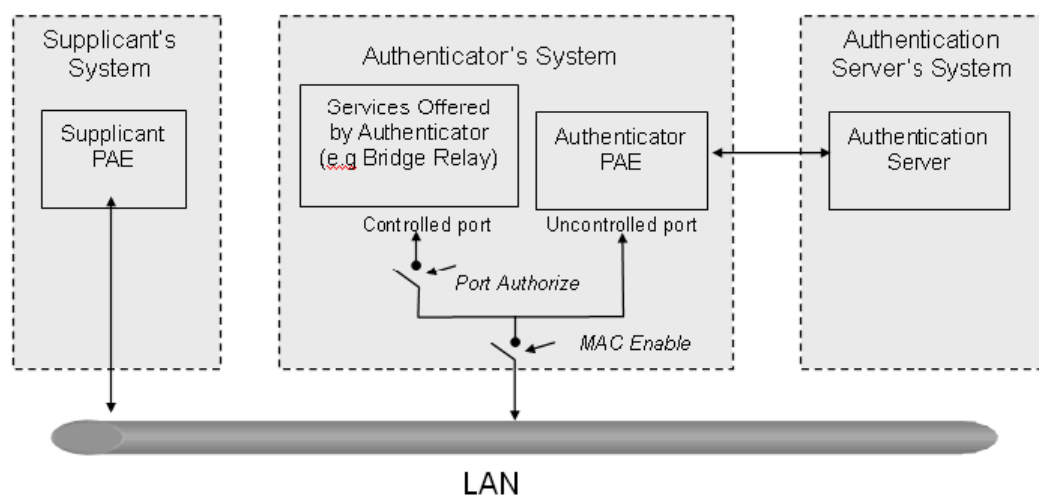
Group \ Port	<p><i>Normal</i> - Set up the ports that do not join any aggregation trunking group.</p> <p><i>Group 1 -8</i> - Group the ports you choose together. Up to 12 ports can be selected for each group.</p>
--------------	---

## 3.6 802.1X

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.

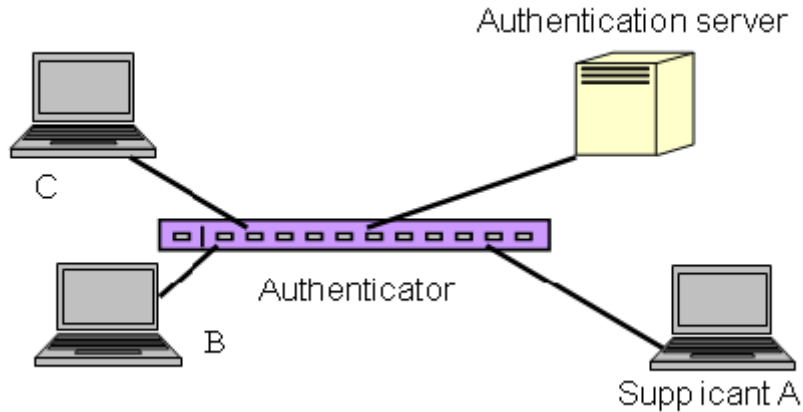
**Authenticator:** An entity facilitates the authentication of the supplicant entity. It controls the state of the port, authorized or unauthorized, according to the result of authentication message exchanged between it and a supplicant PAE. The authenticator may request the supplicant to re-authenticate 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.

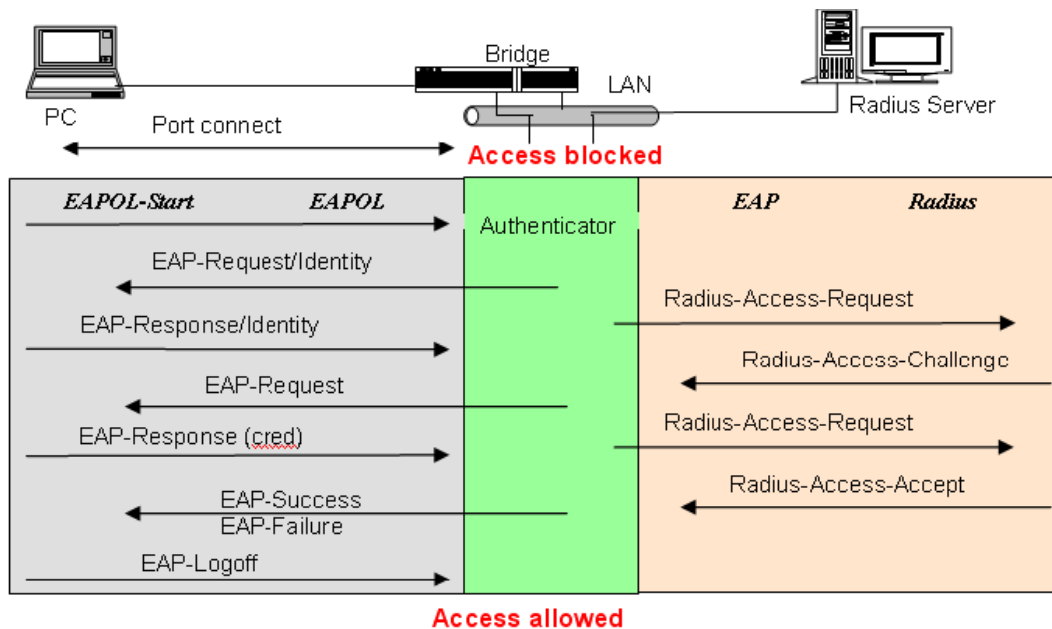
**Authentication server:** A device provides authentication service, through EAP, to an authenticator by using authentication credentials supplied by the supplicant to determine if the supplicant is authorized to access the network resource.

The overview of operation flow for the Figure above 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 above 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.



Above figure 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.

The 802.1X “Enabled” 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 “Enabled” 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
Enabled	Auto	Successful	Port Authorized



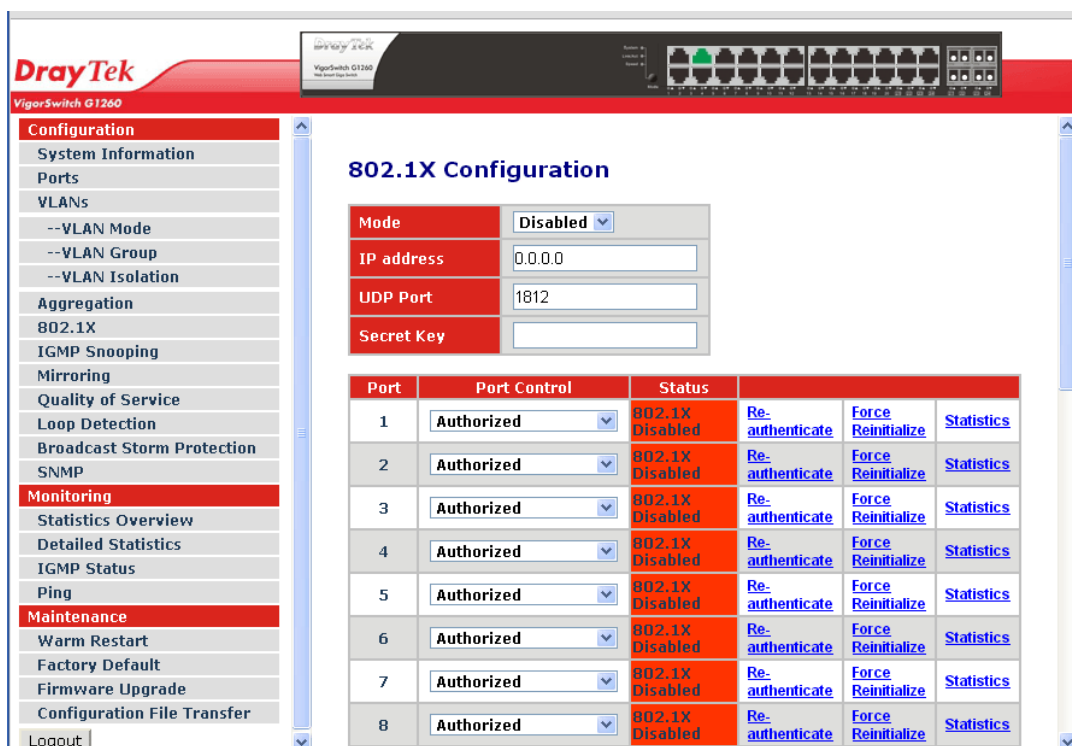
Enabled	Auto	Failure	Port Unauthorized
Enabled	ForceUnauthorized	Don't Care	Port Unauthorized
Enabled	ForceAuthorized	Don't Care	Port Authorized

**Function name:**

802.1X Configuration


**Function description:**

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



**Parameter description:**

Mode	Enable or disable 802.1X function.
IP Address	RADIUS server IP address for authentication. Default: 0.0.0.0
UDP Port	The port number to communicate with RADIUS server for the authentication service. The valid value ranges 1-65535. Default port number is 1812.
Secret Key	The secret key between authentication server and authenticator. It is a string with the length 1 – 15 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: None

Port Control	<p>This is used to set the operation mode of authorization. There are two type of operation mode supported, Authorized, Auto.</p> <p><i>Auto</i> - 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.</p> <p><i>Authorized</i> - The controlled port is forced to hold in the authorized state.</p> <p><i>Force Unauthorized</i> –The controlled port is forced to hold in the unauthorized state.</p>  <p>Default: Authorized</p>
Status	<p>Show the port status of authorization.</p> <p><i>Re-authenticate</i> - Specify if subscriber has to periodically re-enter his or her username and password to stay connected to the port.</p> <p><i>Re-authenticate All</i> - Re-authenticate for all ports in at once.</p> <p><i>Force Reinitialize</i> - Force the subscriber has to reinitialize connected to the port.</p> <p><i>Force Reinitialize All</i> - Force Reinitialize for all ports in at once.</p> <p><i>Statistics</i> - Choose the port which you want to show of 802.1X statistics, the screen include Authenticator counters, backend Authenticator counters, dot1x MIB counters and Other statistics.</p> <p>Press the &lt;<b>Refresh</b>&gt; button will fresh the screen and see the newer counters.</p>

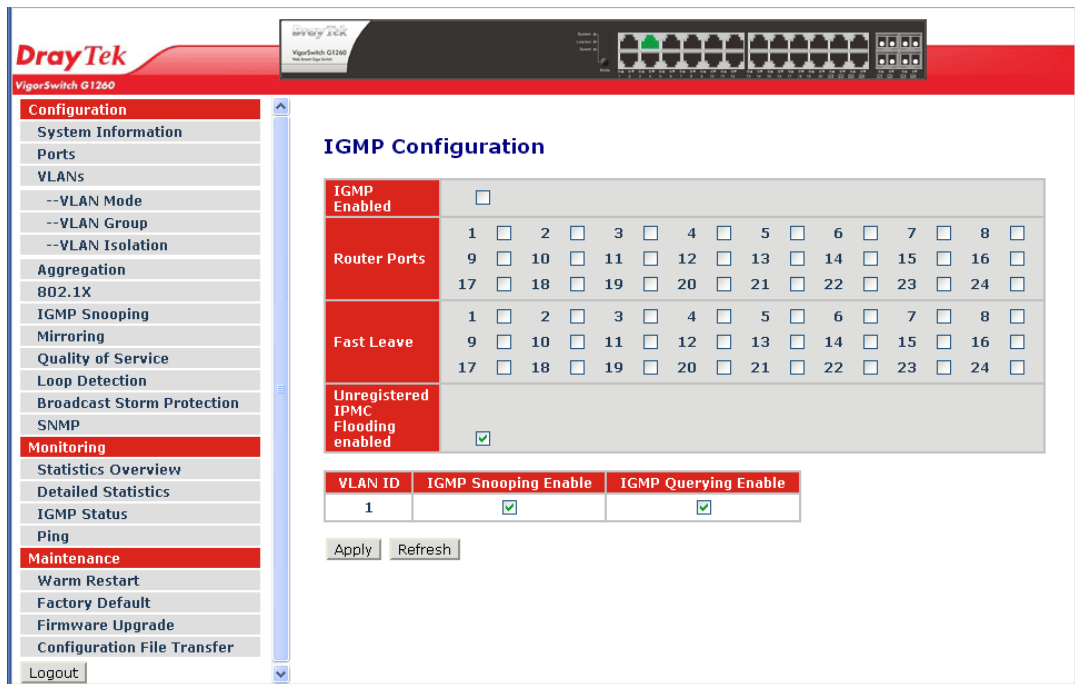
### 3.7 IGMP Snooping

**Function name:**

IGMP Snooping Configuration

**Function description:**

IGMP Snooping lets administrators configure a switch to constrain multicast traffic by listening to Internet Group Management Protocol (IGMP). After finishing the settings, please press <Apply> button to start up the function.



**Parameter description:**

IGMP Enabled:	Just tick the check box (☐) to enable this function. Default: disable.
Router Ports:	Just tick the check box (☐) beside the port x to enable router ports, then press the <Apply> button to start up. Default: none
Fast Leave	Enable the fast leave on the port.
Unregistered IPMC Flooding enabled:	Just tick the check box (☐) to enable this function. Default: enable
VLAN ID:	At the IGMP Enable mode being selected, it will list the VLAN ID number.
IGMP Snooping Enabled:	After IGMP Enabled function start up then user can tick the check box (☐) to enable this function. Default: enable
IGMP Querying Enabled:	After IGMP Enabled function start up then user can tick the check box (☐) to enable this function. Default: enable

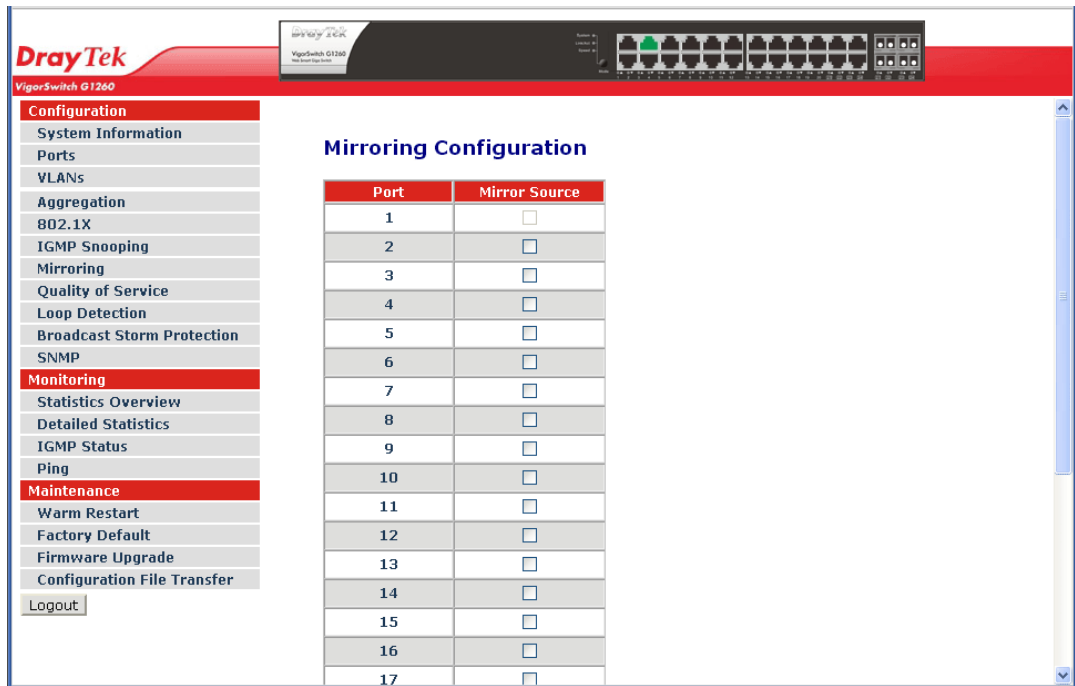
## 3.8 Mirroring

**Function name:**

Mirror Configuration

**Function description:**

Mirror Configuration is provided to monitor the traffic in the network. This switch supports one-port mirror multi-ports. For example, we assume that Port A and Port B are Source Ports, and Port C is Mirror Port respectively, thus, the traffic passing through Port A and Port B will be copied to Port C for monitor purpose.



**Parameter description:**

Port:	Use the drop-down menu to select a mirror port.
Mirror Source:	The source enable means the monitored port ingress traffic will be copied to monitoring port. Set up the port for being monitored. Just tick the check box ( <input type="checkbox"/> ) beside the port x and valid port is Port 1~24.

## 3.9 Quality of Service

The switch offers powerful QoS function.

This function supports VLAN-tagged priority that can make precedence of 8 priorities, and DSCP (Differentiated Services Code Point) on Layer 3 of network framework.

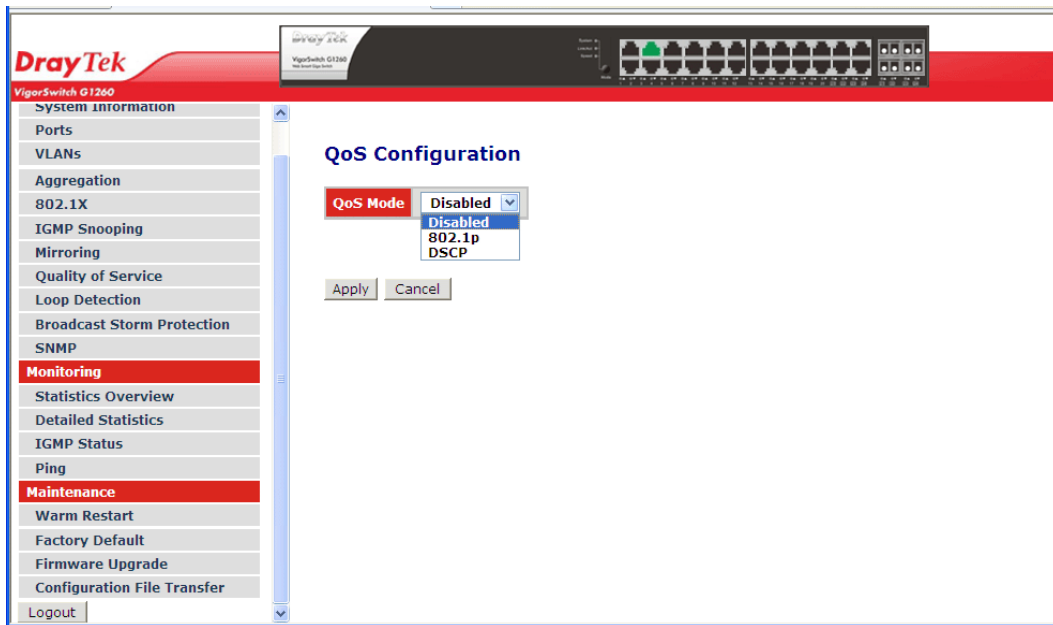
**Function name:**

QoS Configuration

**Function description:**

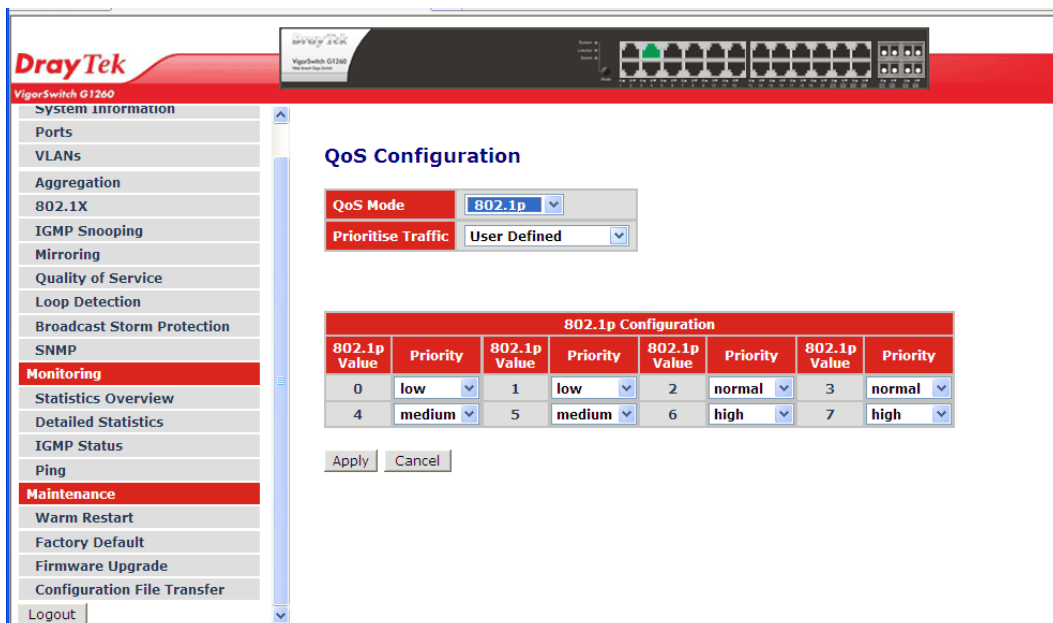
While setting QoS function, please select QoS Mode in drop-down menu at first. Then you can use 802.1p Priority and DSCP Priority functions. In this function, you can enable/disable QoS Mode and set Priority Control, such as: 802.1p and DSCP. The switch only supports Strict Priority. High priority queue is always passed first.

## QoS Mode - Disabled



## QoS Mode – 802.1p

Each Priority can select any of Queue. In Default, Priority 0 is mapping to Queue normal, Priority 1 is mapping to Queue low, Priority 2 is mapping to Queue low, Priority 3 is mapping to Queue normal, Priority 4 is mapping to Queue medium, Priority 5 is mapping to Queue medium, Priority 6 is mapping to Queue high, and Priority 7 is mapping to Queue high.



### Parameter description:

Prioritise Traffic

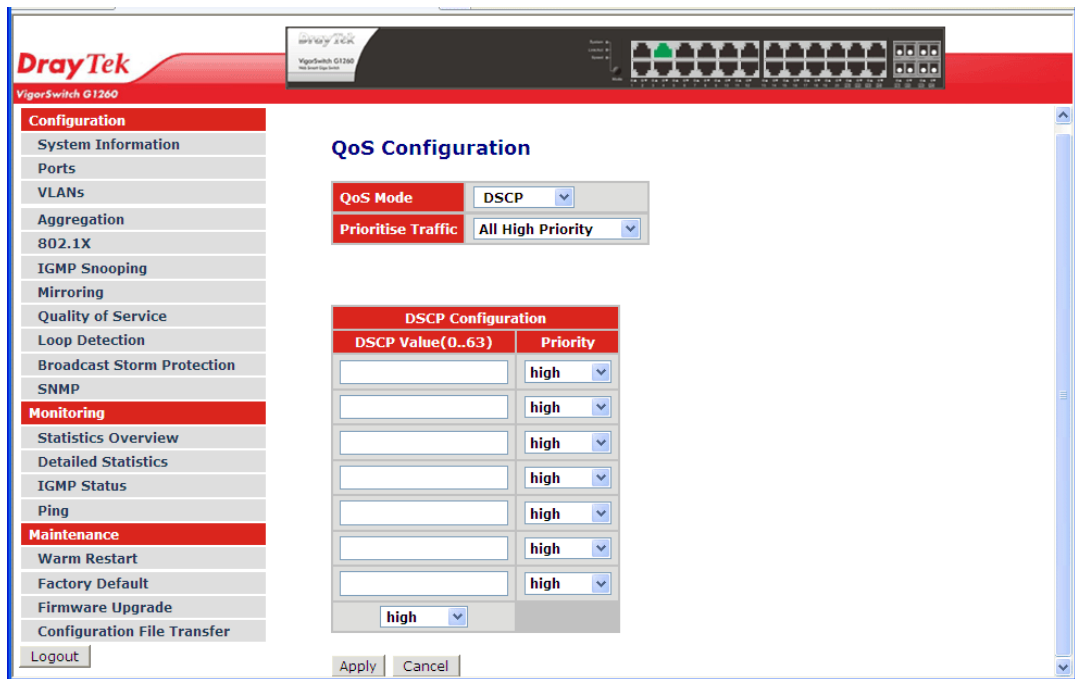
Five Prioritise Traffic values are provided: User Defined, All Low Priority, All Normal Priority, All Medium Priority, and All High Priority.

The QoS setting would apply to all ports on the switch if one of the following values is selected: All Low Priority, All Normal Priority, All Medium Priority, or All High

	Priority. <div style="border: 1px solid black; padding: 5px;"> <b>All High Priority</b> ▾  <b>User Defined</b>  <b>All Low Priority</b>  <b>All Normal Priority</b>  <b>All Medium Priority</b>  <b>All High Priority</b> </div>
Priority	<div style="border: 1px solid black; padding: 5px;"> <b>Medium</b> ▾  <b>Low</b>  <b>Normal</b>  <b>Medium</b>  <b>High</b> </div>

### QoS Mode – DSCP

In the late 1990s, the IETF redefined the meaning of the 8-bit SERVICE TYPE field to accommodate a set of differentiated services (DS). Under the differentiated services interpretation, the first six bits comprise a codepoint, which is sometimes abbreviated DSCP, and the last two bits are left unused. DSCP can form total 64 (0~63) kinds of Traffic Class based on the arrangement of 6-bit field in DSCP of the IP packet. In the switch, user is allowed to set up these 64 kinds of Class that belong to any of queue (low, normal, medium, high).



### Parameter description:

Prioritise Traffic	<p>Five Prioritize Traffic values are provided: User Defined, All Low Priority, All Normal Priority, All Medium Priority, and All High Priority.</p> <p>The QoS setting would apply to all ports on the switch if one of the following values is selected: All Low Priority, All Normal Priority, All Medium Priority, or All High Priority.</p>
--------------------	--

	<div style="border: 1px solid black; padding: 2px;"> <b>All High Priority</b> <span style="float: right;">▼</span>  <b>User Defined</b>  <b>All Low Priority</b>  <b>All Normal Priority</b>  <b>All Medium Priority</b>  <b>All High Priority</b> </div>
DSCP Value (0..63)	64 kinds of priority traffic as mentioned above, user can set up any of Queue (low, normal, medium, high). In default, Priority 0~63 are mapping to High.
Priority	User can set up any of Queue (low, normal, medium, high). <div style="border: 1px solid black; padding: 2px;"> <b>Medium</b> <span style="float: right;">▼</span>  <b>Low</b>  <b>Normal</b>  <b>Medium</b>  <b>High</b> </div>

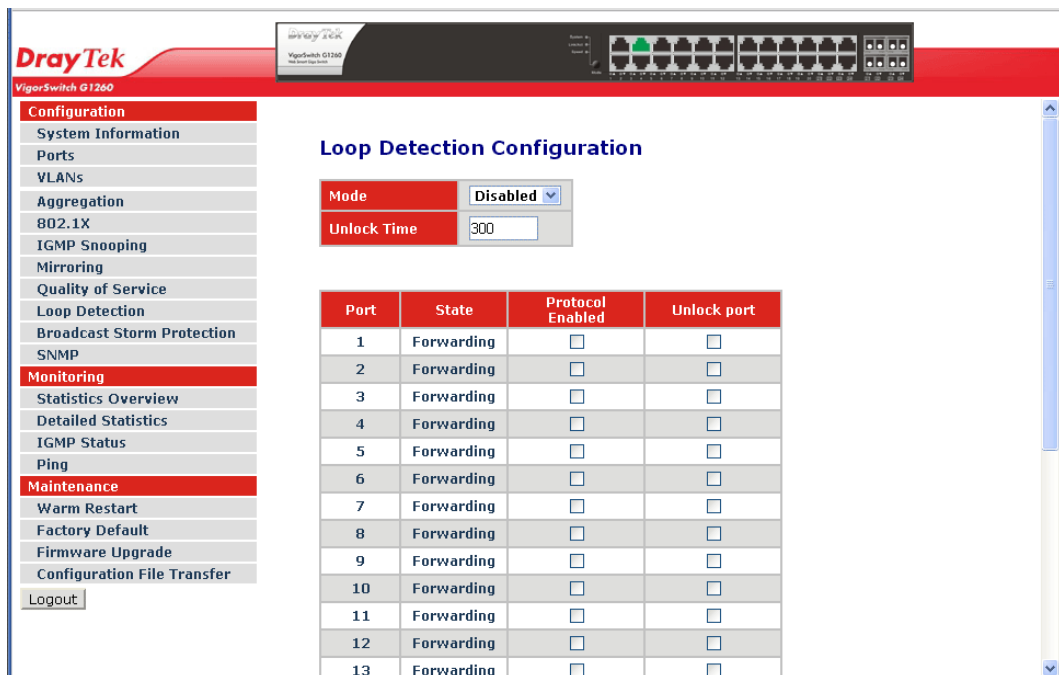
### 3.10 Loop Detection

**Function name:**

Loop Detection Configuration

**Function description:**

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 "Unlock port" and click on "Apply" to turn on the locked ports.



**Parameter description:**

Mode	Controls whether Loop Detection is enabled (as a whole).
------	--

Unlock Time	The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action is to shut down the port).
Port	Display the number of the ports on the switch.
State	Show the status on the port.
Protocol Enabled	Controls whether Loop Detection is enabled on this switch port. When Port No is chosen and enable port's Loop detection, the port can detect loop happens and port will be Locked. If Loop did not happen, port maintains Unlocked.
Unlock port	When ticking the port, port locked will be opened and turned into unlocked. If not ticking the port, Port maintains locked.

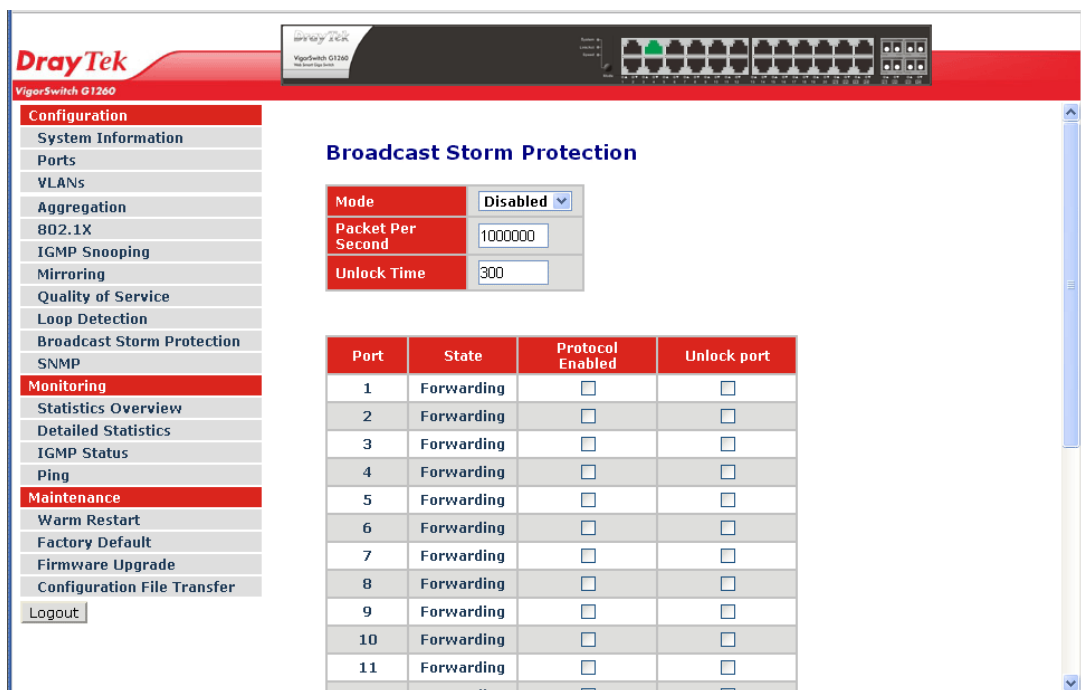
### 3.11 Broadcast Storm Protection

**Function name:**

Broadcast Storm Protection configuration

**Function description:**

When the broadcast packets received by the switch exceed the threshold configured, the port will be blocked for a period of time which can be set. After a configured time, the switch will detect whether the broadcast packets received on the port still exceed the threshold. If the broadcast traffic is still higher than, the port will be closed for a period of time again. If the broadcast traffic is under the threshold, the port will re-open and forward the packets normally.



**Parameter description:**

Mode	Controls whether Broadcast Storm Protection is enabled (as a whole).
------	--



Packet Per Second	It is a threshold. When the broadcast packet traffic in a second is higher than the threshold configured, the Broadcast Storm Protection enable.
Unlock Time	The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action is to shut down the port).
Port	Display the number of the ports on the switch.
State	Show the status on the port.
Protocol Enabled	Controls whether Broadcast Storm Protection is enabled on this switch port.
Unlock port	When ticking the port, port locked will be opened and turned into unlocked. If not ticking the port, Port maintains locked.

### 3.12 SNMP

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.

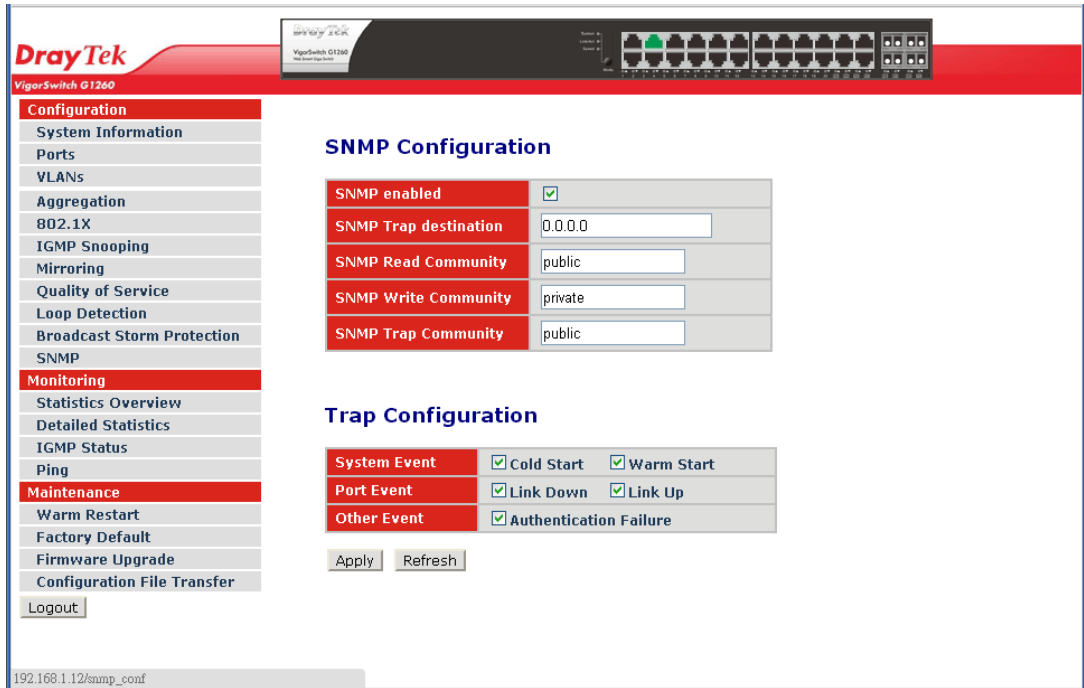
Basically, it is passive except issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP “Enable”, SNMP agent will be started up. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set “Disable”,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



**Parameter description:**

SNMP enabled	The term SNMP enable here is used for the activation or de-activation of SNMP. Default is Disable. Default SNMP function: Disable
SNMP Trap destination	Set the IP address for the SNMP Trap Host.
SNMP Get Community SNMP Set Community SNMP 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 Read only works for Read function and can't be applied to other function such as Write and Trap.  Default community name for Get: public Default community name for Set: private Default community name for Trap: public
System Event	There are two events (Cold Boot or Warm Boot) offered here for you to set.  When VigorSwitch is boot by "cold boot" or "warm boot", it will send notification to SNMP server to inform

	the user.
Port Event	The Port Event trap enable here is used for the “Link Up” or “Link Down” of system Event. Default is “Disable”.
Other Event	The Other Event trap enable here is used for the Authentication failure of system Event. Default is “Disable”.

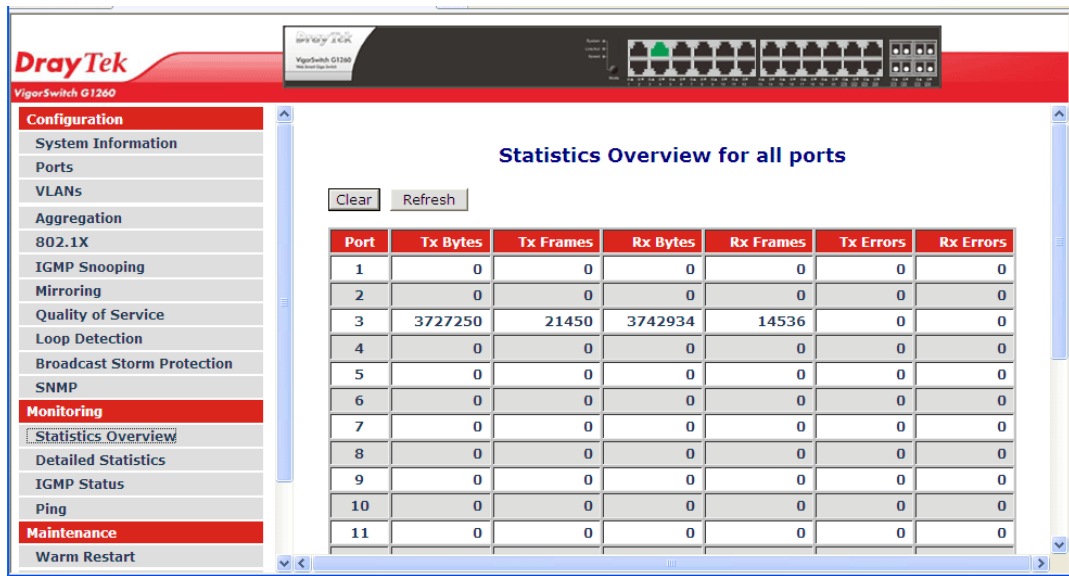
### 3.13 Statistics Overview

**Function name:**

Statistics Overview for all ports

**Function description:**

The section describes to the Port statistics information and provides overview of general traffic statistics for all switch ports.



**Parameter description:**

Tx Bytes / Rx Bytes	The number of received and transmitted bytes per port.
Tx Frames / Rx Frames	The number of received and transmitted frames per port.
Tx Errors / Rx Errors	The number of frames received in error and the number of incomplete transmissions per port.

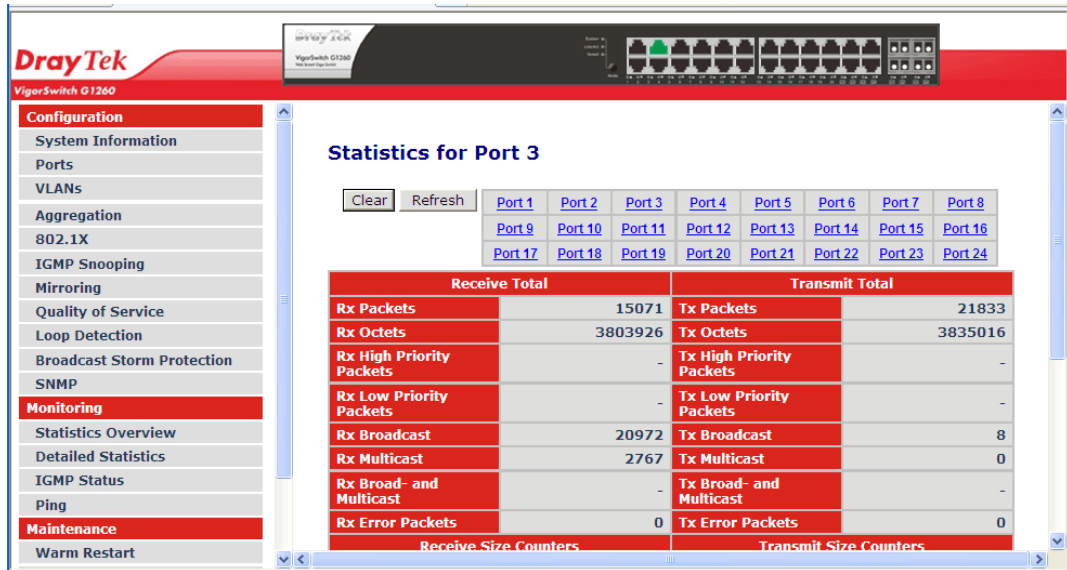
### 3.14 Detailed Statistics

**Function name:**

Detailed Statistics

**Function description:**

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



**Parameter description:**

Rx Packets:	The counting number of the packet received.
Rx Octets:	Total received bytes.
Rx High Priority Packets:	Number of Rx packets classified as high priority.
Rx Low Priority Packets:	Number of Rx packets classified as low priority.
Rx Broadcast:	Show the counting number of the received broadcast packet.
Rx Multicast:	Show the counting number of the received multicast packet.
Rx Broad- and Multicast:	Show the counting number of the received broadcast with multicast packet.
Rx Error Packets:	Show the counting number of the received error packets.
Tx Packets:	The counting number of the packet transmitted.
Tx Octets:	Total transmitted bytes.
Tx High Priority Packets:	Number of Tx packets classified as high priority.
Tx Low Priority Packets:	Number of Tx packets classified as low priority.
Tx Broadcast:	Show the counting number of the transmitted broadcast packet.
Tx Multicast:	Show the counting number of the transmitted multicast packet.

Tx Broad- and Multicast:	Show the counting number of the transmitted broadcast with multicast packet.
Tx Error Packets:	Show the counting number of the received error packets.
Rx 64 Bytes:	Number of 64-byte frames in good and bad packets received.
Rx 65-127 Bytes:	Number of 65 ~ 126-byte frames in good and bad packets received.
Rx 128-255 Bytes:	Number of 127 ~ 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-Bytes:	Number of 1024-max_length-byte frames in good and bad packets received.
Tx 64 Bytes:	Number of 64-byte frames in good and bad packets transmitted.
Tx 65-127 Bytes:	Number of 65 ~ 126-byte frames in good and bad packets transmitted.
Tx 128-255 Bytes:	Number of 127 ~ 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-Bytes:	Number of 1024-max_length-byte frames in good and bad packets transmitted.
Rx CRC/Alignment:	Number of Alignment errors and CRC error 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 to max_length register) with invalid CRC.
Rx Drops:	Frames dropped due to the lack of receiving buffer.
Tx Collisions:	Number of collisions transmitting frames experienced.
Tx Drops:	Number of frames dropped due to excessive collision, late collision, or frame aging.
Tx Overflow:	Number of frames dropped due to the lack of transmitting buffer.

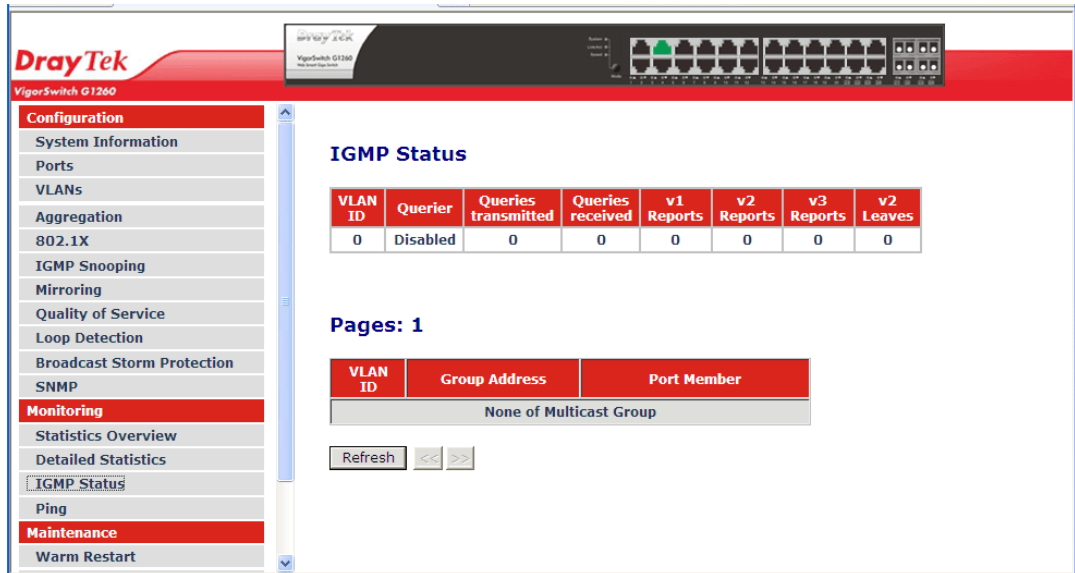
### 3.15 IGMP Status

**Function name:**

IGMP Status

**Function description:**

Display IGMP status. The window shows VLAN ID for each multicast group.



**Parameter description:**

VLAN ID:	Show VLAN ID for each multicast group.
Querier:	Show the group membership queries status.
Queries transmitted:	To count the group membership queries transmitted.
Queries received:	To count the group membership queries received.
V1 Reports:	When a host receives a group membership query, it identifies the groups associated with the query and determines to which groups it belongs. The host then sets a timer, with a value less than the <i>Max Response Time</i> field in the query, for each group to which it belongs. It Calculate the number of times of IGMPV1 report.
V2 Reports:	When a host receives a group membership query, it identifies the groups associated with the query and determines to which groups it belongs. The host then sets a timer, with a value less than the Max Response Time field in the query, for each group to which it belongs. It Calculate the number of times of IGMPV2 report.
V3 Reports:	When a host receives a group membership query, it identifies the groups associated with the query and determines to which groups it belongs. The host then sets a timer, with a value less than the Max Response Time field in the query, for each group to which it belongs. It Calculate the number of times of IGMPV3 report.
V2 Leaves:	When a host leaves a group, it sends a leave group membership message to multicast routers on the network,

	it show the leaves number.
VLAN ID:	Show VLAN ID for each multicast group.
Group Address:	Display the corresponding IP address for the VLAN ID multicast group.
Ports Member:	Display the corresponding port number for the VLAN ID multicast group.

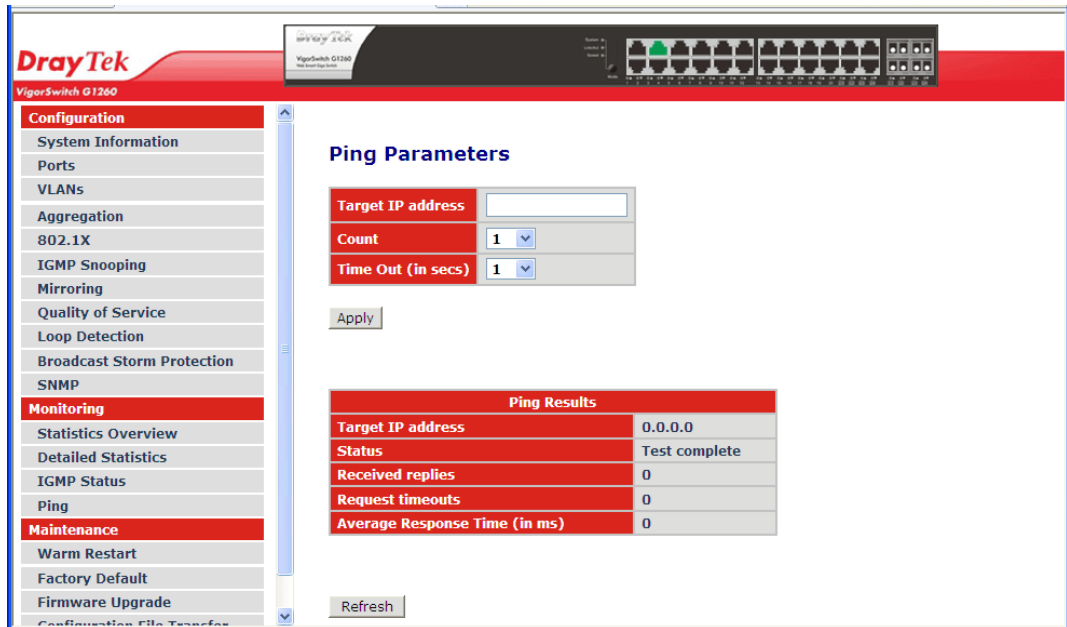
### 3.16 Ping

**Function name:**

Ping Configuration

**Function description:**

To set up target IP address for ping function and display ping status.



**Parameter description:**

Target IP Address	Set up a Target IP address to ping.
Count	Use drop-down menu to set number of echo requests to send. Four type of number can choose, there are 1, 5, 10 and 20. Default: 1
Time Out (in secs)	Use drop-down menu to set number of echo requests time out in second. Four type numbers can choose, there are 1,5,10 and 20. Default: 1
Target IP address	Show the active target IP address.
Status	Show the result of the ping status.
Received replies:	Show the received replies number of times.

Received timeouts:	Show the timeout of request.
Average Response Time (in ms)	Show the average response time in milliseconds.

**NOTE:** All the functions should press <Apply> button to start up after you set up the parameters.

### 3.17 Warm Restart

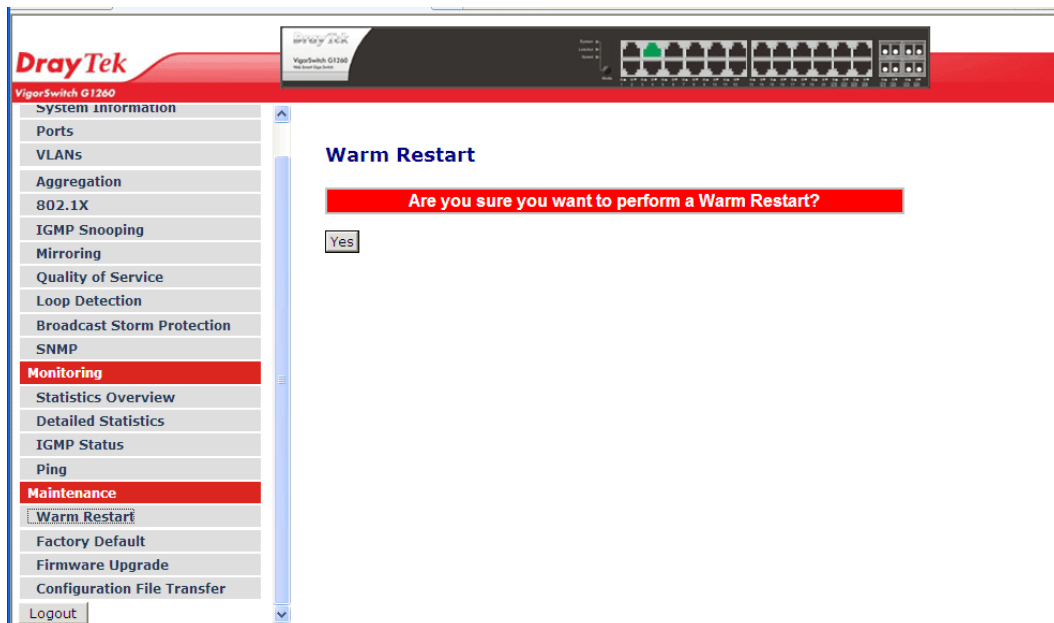
The device offers many approaches to reboot your switch, such as: power up, hardware reset and software reset. You can press RESET button in the front panel of your switch to reset the device and to retrieve default settings. After upgrading software, you have to reboot the device to have new configuration take effect. The function being discussed here is software reset.

**Function name:**

Warm Restart

**Function description:**

Reboot the switch. Reboot takes the same effect as the RESET button on the front panel of the switch. Press <Yes> button to confirm warm restart function, and it will take around thirty (30) seconds to complete the system boot.



### 3.18 Factory Default

**Function name:**

Factory Defaults

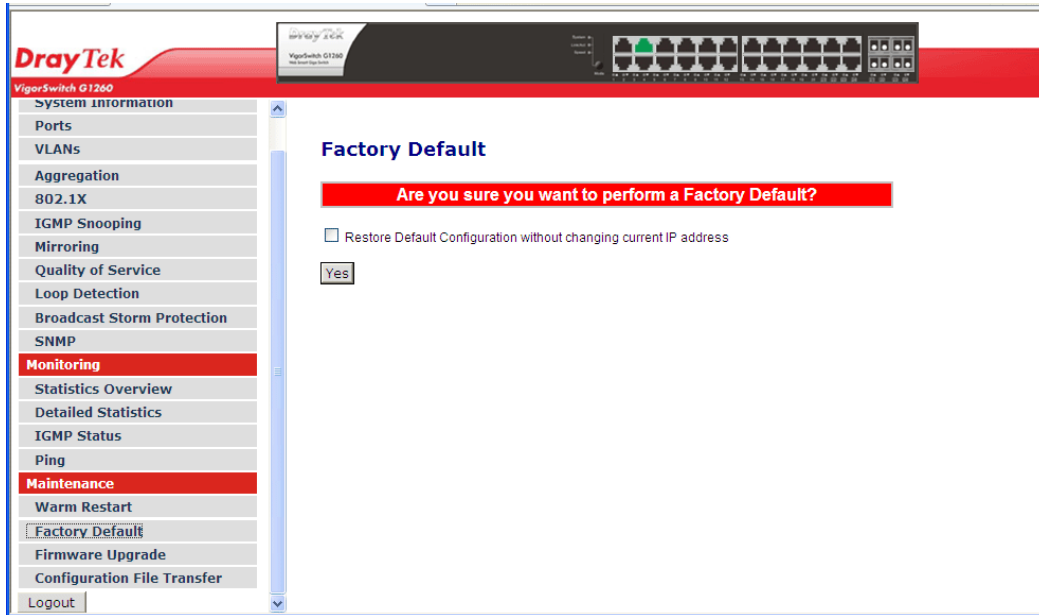
**Function description:**

Factory Default provides the function to retrieve default settings and replace current configuration. Except the IP address setting, all settings will be restored to the factory default values when “Factory Default” function is performed. If you want to restore all



configurations including the IP address setting to the factory default, please press the “**Mode**” button on the front panel.

You must press the “**Mode**” button over 3 seconds to restore the factory default setting.



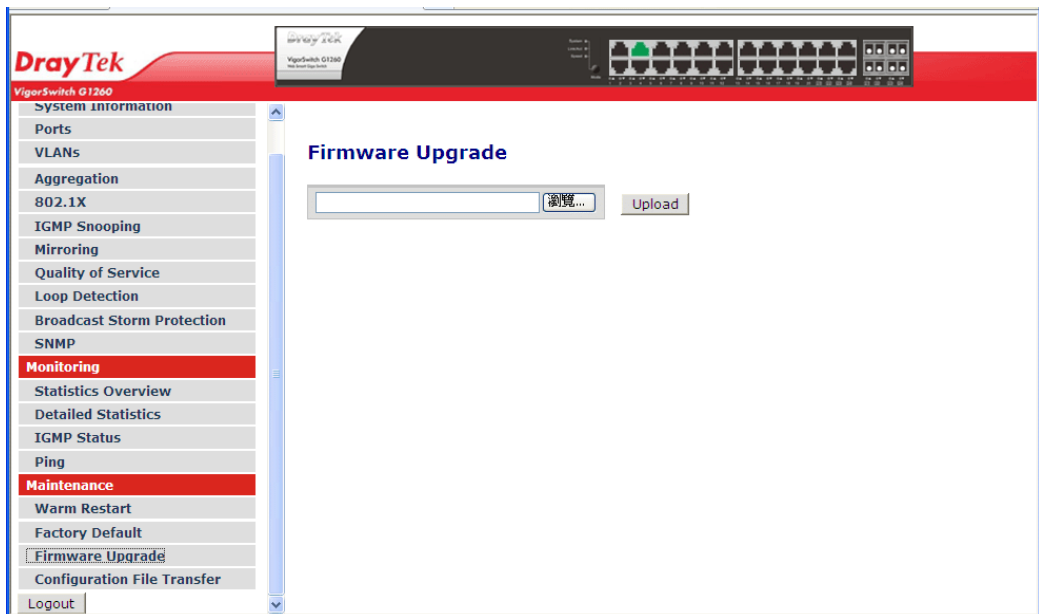
### 3.19 Firmware Upgrade

**Function name:**

Firmware Upgrade

**Function description:**

You can just click Browse button to retrieve the file you want in your system to upgrade your switch.



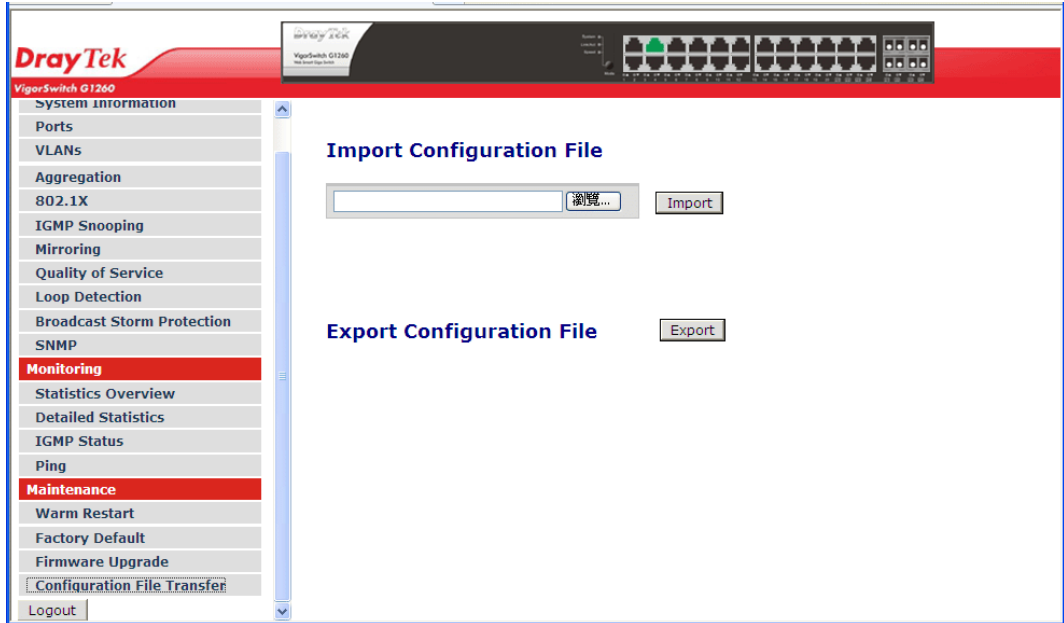
## 3.20 Configuration File Transfer

**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:**

Import:	Import a configuration file stored in the flash.
Export:	Export the current configuration on switch from Flash.

## 3.21 Logout

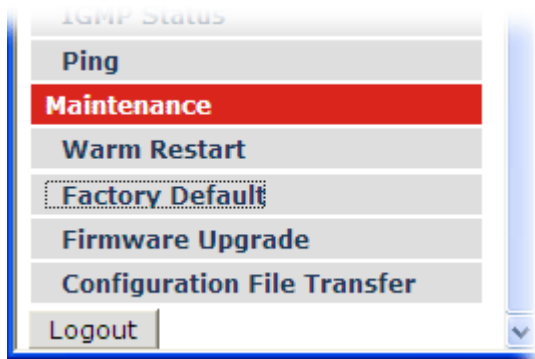
In addition to auto logout function we just mentioned in system configuration section, the switch also allows administrators to logout manually by Logout function.

**Function name:**

Logout

**Function description:**

The switch allows you to logout the system to prevent other users from the system without the permission. If you do not logout and exit the browser, the switch will automatically have you logout. Besides this manually logout and implicit logout, you can set up the parameter of Auto Logout Timer in system configuration function to explicitly ON/OFF this logout function.



This page is left blank.

# 4

## Trouble Shooting

### 4.1 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

### 4.2 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 the Switch.
- Please check the uplink setup of the Switch to verify the uplink function is enabled.

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

- The Switch has no console port, so you cannot use console interface to connect with the Switch.

#### **4. How to configure the Switch?**

- A user can use IE browser program in window series of computer to control the web smart functions in the Switch. First, choose any port in the Switch. Then, enable DHCP server setting. When the switch is assigned an IP address, use IE and type the obtained IP address to connect to 24 Gigabit with RJ45 network line. Finally, the login screen will appear at once.