DrayTek

VigorSwitch P1280

PoE Web Smart Giga Switch

Your reliable networking solutions partner

User's Guide

V1.1

VigorSwitch P1280

PoE Gigabit Ports Web Smart Switch

User's Guide

Version: 1.1

Firmware Version: V2.0.0

(For future update, please visit DrayTek web site)

Date: October 13, 2017

Copyrights

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, Vista, 7, 8, 10 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

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

Be a Registered Owner

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

Firmware & Tools Updates

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

More update, please visit www.draytek.com.

Table of Contents

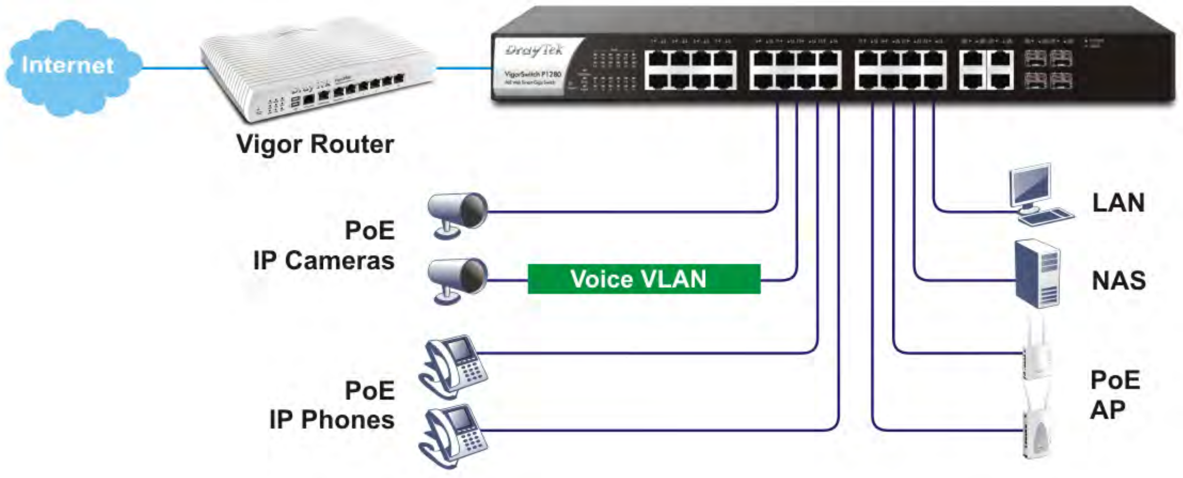
Part I Introduction

I-1 Introduction

24 ports + 4 Combo UTP/SFP ports, PoE Gigabit Ports Web Smart Switch is a standard switch that meets all IEEE 802.3/u/x/z Gigabit, Fast Ethernet specifications. The switch has 24 10/100/1000Mbps TP ports. It supports telnet, http, https, SSH 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.

Vigor switch supports IEEE 802.3az, Energy-Efficient Ethernet, and provides power saving feature. It can efficiently save the switch power with auto detect the client idle and cable length to provide different power.

1000Mbps SFP Fiber port fully complies with all IEEE 802.3z and 1000Base-SX/LX standards.



I-1-1 Key Features

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 IEEE 802.3az, Energy-Efficient Ethernet 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.

I-1-2 Specifications

The VigorSwitch P1280, 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

- 24 10/100/1000Mbps Auto-negotiation Gigabit Ethernet TP ports with PoE+
- Jumbo frame support 9KB
- 4 UTP/SFP Combo Ethernet Ports
- 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 IEEE 802.3az, Energy-Efficient Ethernet
- Full-duplex flow control (IEEE802.3x) and half-duplex backpressure
- Extensive front-panel diagnostic LEDs; Power, System, PoE fail and PoE/link activity
- Hardware reset button for resetting configuration to factory default by pressing over 5 seconds

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

I-1-3 Packing List

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

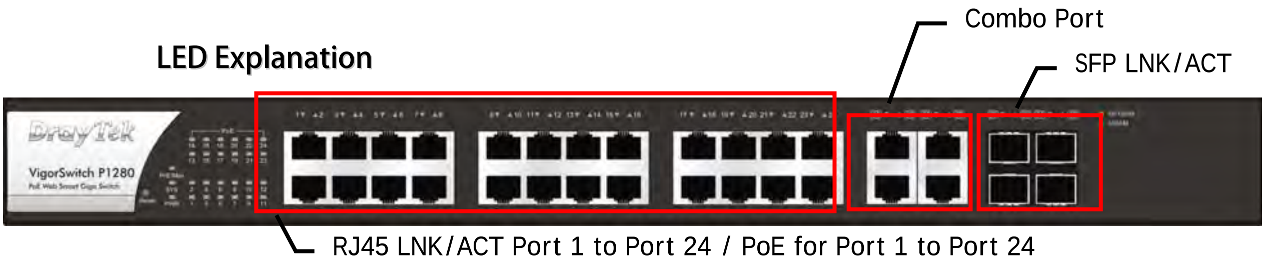
- VigorSwitch P1280
- AC Power Cord
- Quick Start Guide
- Rubber feet
- Rack mount kit

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

I-1-4 LED Indicators and Connectors

Before you use the Vigor device, please get acquainted with the LED indicators and connectors first. There are 8 Ethernet ports and SFP ports on the front panel of the switch. LED display area, locating on the front panel, contains an ACT, Power LED and ports working status of the switch.

LED Explanation



LED	Color	Explanation
PoE /Max	On (Green)	Connected over the PoE maximum power budget.
	Off	Connected within the PoE maximum power budget.
SYS	On (Green)	The switch finishes system booting and the system is ready.
	Blinking (Green)	The switch is powered on and starts system booting.
	Off	The power is off or the system is not ready / malfunctioning.
PWR	On (Green)	The device is powered on and running normally.
	Off	The device is not ready or is failed.
PoE 1~24	On (Green)	The port is supplied with PoE power.
	Off	No PoE power is supplied on the port.
RJ 45 LNK/ACT	On (Green)	The device is connected with 1000Mbps.
	On (Amber)	The device is connected with 10/100Mbps.

Port 1 ~ 24	Blinking	The system is sending or receiving data through the port.
	Off	The port is disconnected or the link is failed.
Combo for Port 25 ~ 28 (RJ 45 LNK/ACT)	On (Green)	The device is connected with 1000Mbps.
	On (Amber)	The device is connected with 10/100Mbps.
	Blinking	The system is sending or receiving data through the port.
	Off	The port is disconnected or the link is failed.
SFP LNK/ACT	On (Green)	The device is connected with 1000Mbps.
	On (Amber)	The device is connected with 10/100Mpps.
	Blinking	The system is sending or receiving data through the port.
	Off	The port is disconnected or the link is failed.

Connector Explanation

Interface	Description
RJ 45 LNK/ACT Port 1 ~ 24	Port 1 to Port 24 can be used for Ethernet connection and PoE connection, depending on the device connected.
PoE for Port 1 ~ 24	
	Power inlet for AC input (100~240V/AC, 50/60Hz).

Power Output	--	IEEE 802.3af Max. 15.4W Output Supported; IEEE 802.3at Max. 30W Output Supported
PoE Power Budget	--	340 Watts (Max)

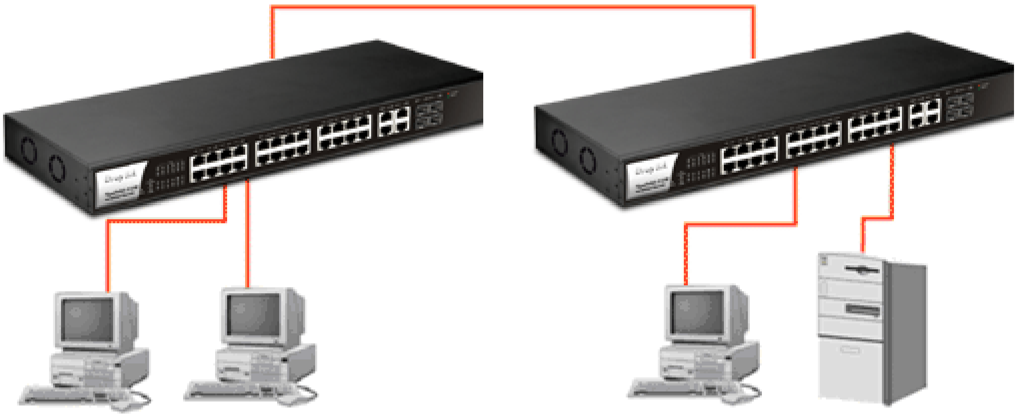
I-2 Installation

I-2-1 Typical Applications

The VigorSwitch implements 24 Gigabit Ethernet TP ports with auto MDIX and four slots for the removable module supporting comprehensive fiber types of connection, including LC and BiDi-LC SFP modules. The switch is suitable for the following applications:

Case 1: All switch ports are in the same local area network.

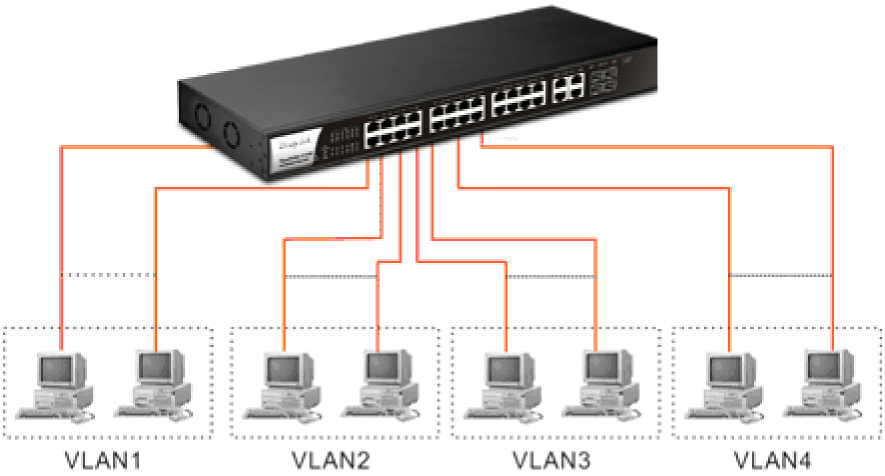
Every port can access each other. (*The switch image is sample only.)



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.

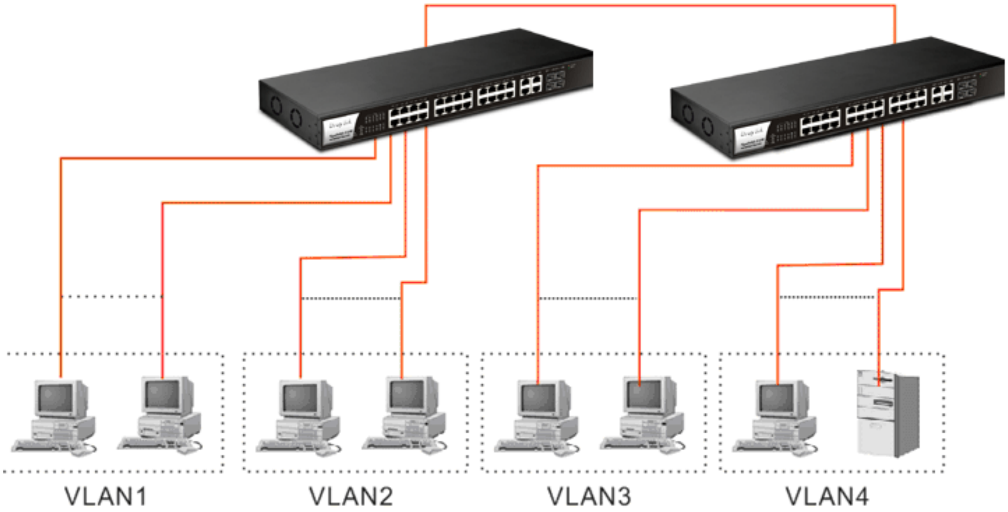
Case 2: Port-based VLAN -1 (*The switch image is sample only.)



- ❖ The same VLAN members could not be in different switches.

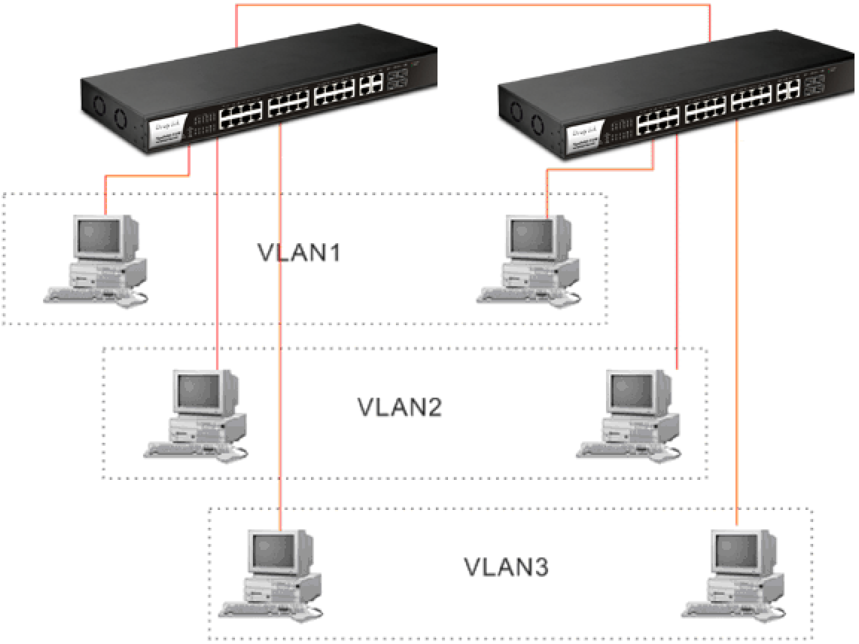
- Every VLAN members could not access VLAN members each other.
- The switch manager has to assign different names for each VLAN groups at one switch.

Case 3: Port-based VLAN - 2



- 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



Case 5: Desktop Installation

1. Install the switch on a level surface that can support the weight of the unit and the relevant components.
2. Plug the switch with the female end of the provided power cord and plug the male end to the power outlet.

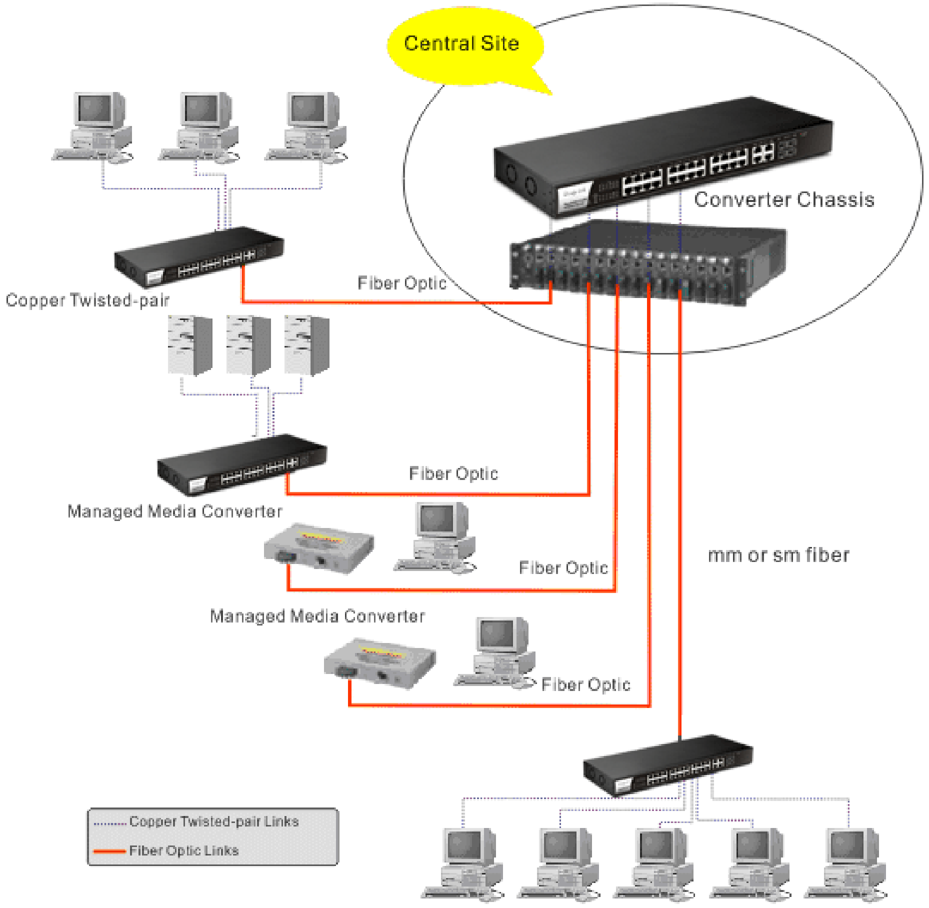
Case 6: Rack-mount Installation

The switch may be standalone, or mounted in a rack. Rack mounting facilitate to an orderly installation when you are going to install series of networking devices.

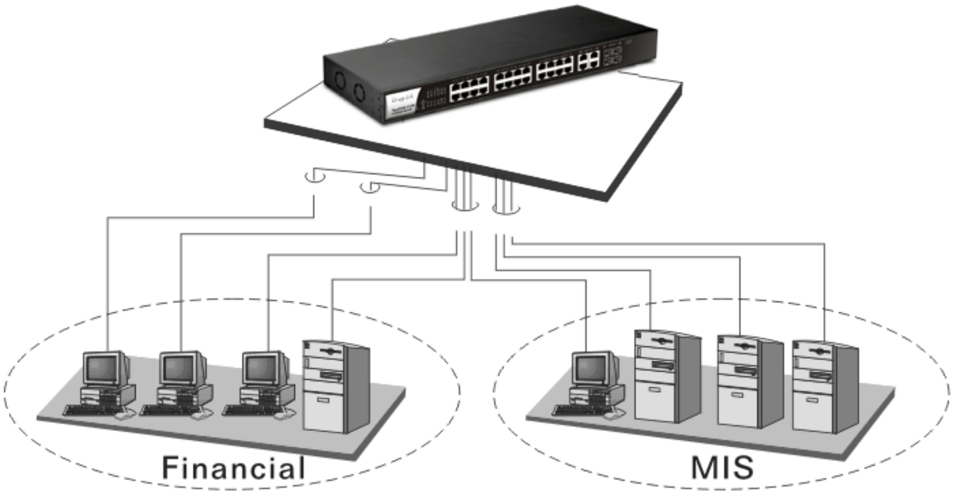
Procedures to Rack-mount the switch:

1. Disconnect all the cables from the switch before continuing.
2. Place the unit the right way up on a hard, flat surface with the front facing you.
3. Locate a mounting bracket over the mounting holes on one side of the unit.
4. Insert the screws and fully tighten with a suitable screwdriver.
5. Repeat the two previous steps for the other side of the unit.
6. Insert the unit into the rack and secure with suitable screws.
7. Reconnect all the cables.

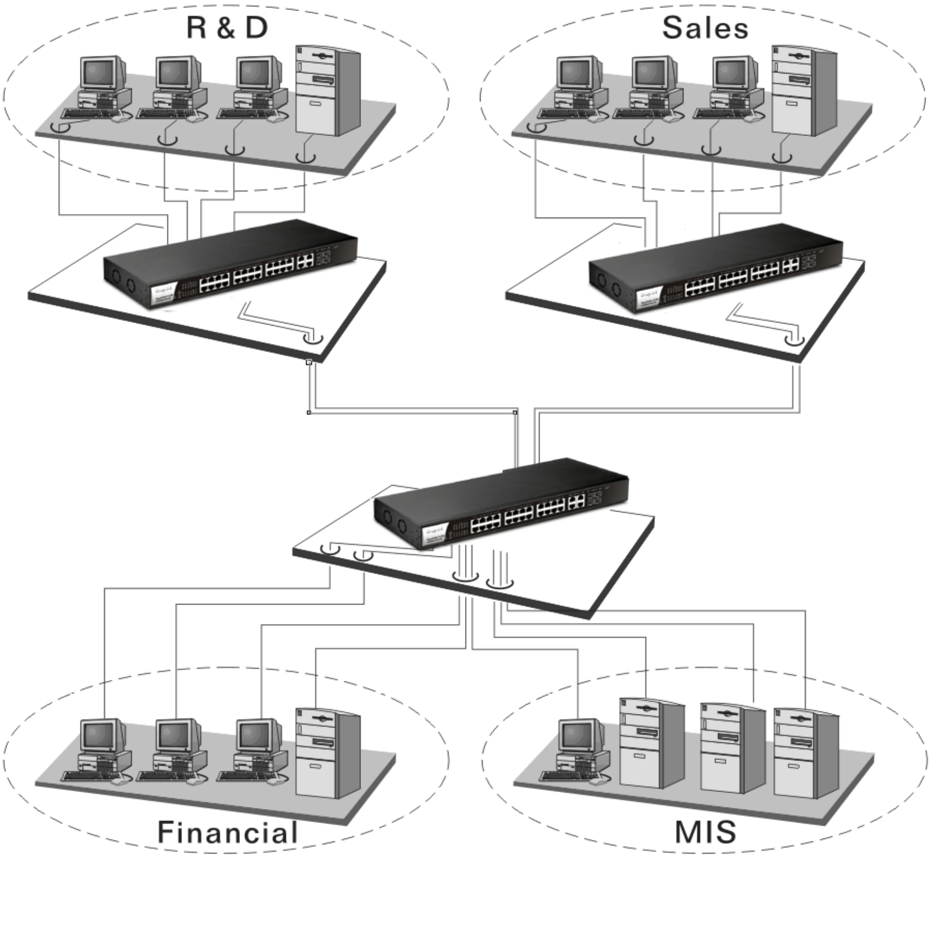
Case 7: Central Site/Remote site application is used in carrier or ISP



Case 8: Peer-to-peer application is used in two remote offices



Case 9: Office network



I-2-2 Installing Network Cables

Crossover or straight-through cable: All the ports on the switch support Auto-MDI/MDI-X functionality. Both straight-through or crossover cables can be used as the media to connect the switch with PCs as well as other devices like switches, hubs or router.

Category 3, 4, 5 or 5e, 6 UTP/STP cable: To make a valid connection and obtain the optimal performance, an appropriate cable that corresponds to different transmitting/receiving speed is required. To choose a suitable cable, please refer to the following table.

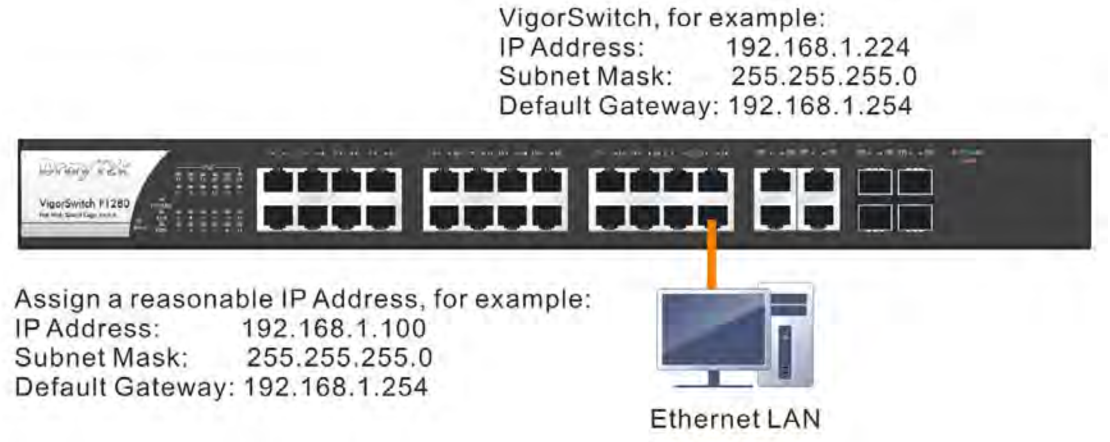
Media	Speed	Wiring
10/100/1000 Mbps copper	10 Mbps	Category 3,4,5 UTP/STP
	100Mbps	Category 5 UTP/STP
	1000 Mbps	Category 5e, 6 UTP/STP

I-2-3 Configuring the Management Agent of Switch

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

Configuring the Management Agent of VigorSwitch P1280 through the Ethernet Port.

There are several ways to configure and monitor the switch through Ethernet port, includes Web-UI and SNMP.


VigorSwitch, for example:
IP Address: 192.168.1.224
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.254
VigorSwitch P1280
Assign a reasonable IP Address, for example:
IP Address: 192.168.1.100
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.254
Ethernet LAN

I-2-4 Managing VigorSwitch P1280 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. 5e 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 Web Smart Switch default IP address information.

2. After configuring correct IP address on your PC, open your web browser and access switch's IP address.

Default system account is "admin", with password "admin" in default. Switch IP address is "192.168.1.224" by default with DHCP client enabled.

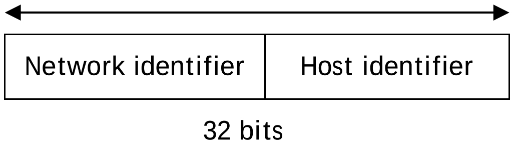
I-2-5 IP Address Assignment

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.

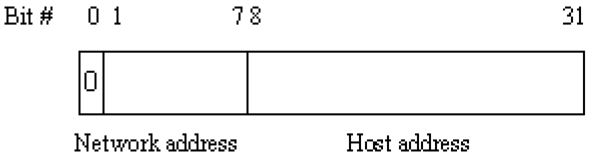
Each class has its own network range between the network identifier and host identifier in the 32 bits address. Each IP address comprises two parts: network identifier (address) and host identifier (address). The former indicates the network where the addressed host resides, and the latter indicates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

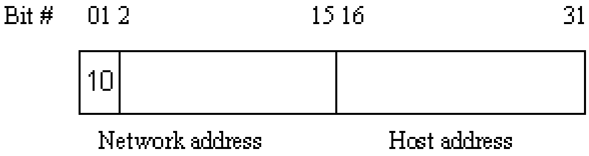
Class A:

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.



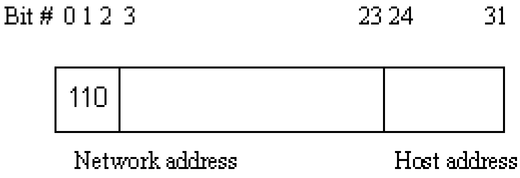
Class B:

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

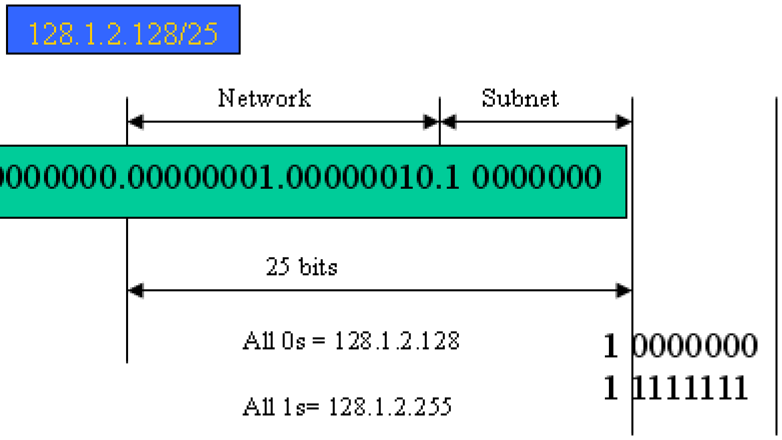
Please refer to RFC 1597 and RFC 1466 for more information.

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.

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

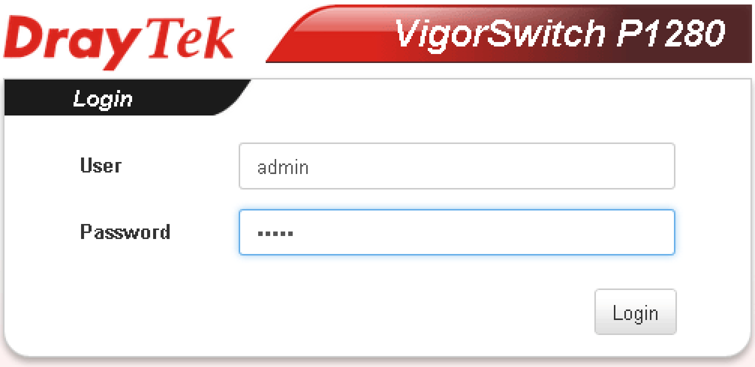
❖ First, IP Address: as shown above, enter "**192.168.1.224**", for instance. For sure, an IP address such as 192.168.1.x must be set on your PC.

❖ Second, Subnet Mask: as shown above, enter "255.255.255.0". Choose a subnet mask suitable for your network.

Note: The DHCP Setting is enabled in default. Therefore, if a DHCP server presented on network connected to the switch, check before accessing your switch is essential.

I-3 Accessing Web Page of VigorSwitch

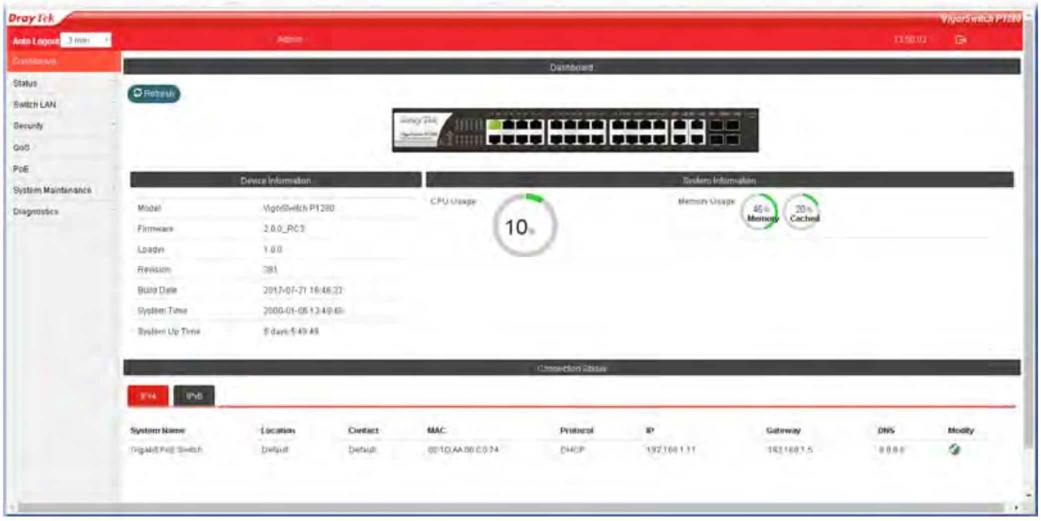
1. Open any browser (e.g., Firefox) and type “192.168.1.224” as URL.
2. Please type “admin/admin” as the Username/Password and click **Login**.



User admin

Password •••••

3. Now, the **Main Screen** will appear.



Model	VigorSwitch P1280
Firmware	2.0.0_RC3
Loader	1.0.0
Revision	381
Build Date	2017-07-21 16:46:33
System Time	2000-01-05 13:49:45
System Up Time	5 days 5:49:49

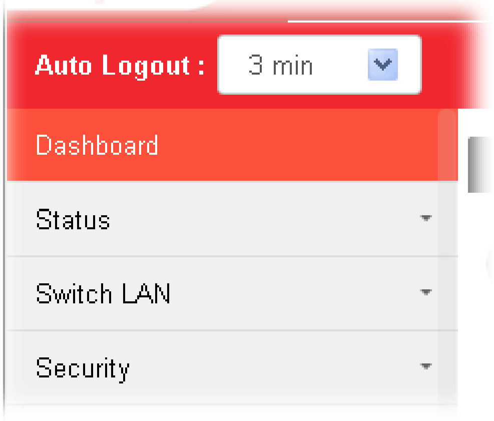
System Name	Location	Contact	MAC	Protocol	IP	Gateway	DNS	Modify
Gigabit PoE Switch	Default	Default	00:1D:AA:00:C0:74	DHCP	192.168.1.11	192.168.1.5	8.8.8.8	

Info

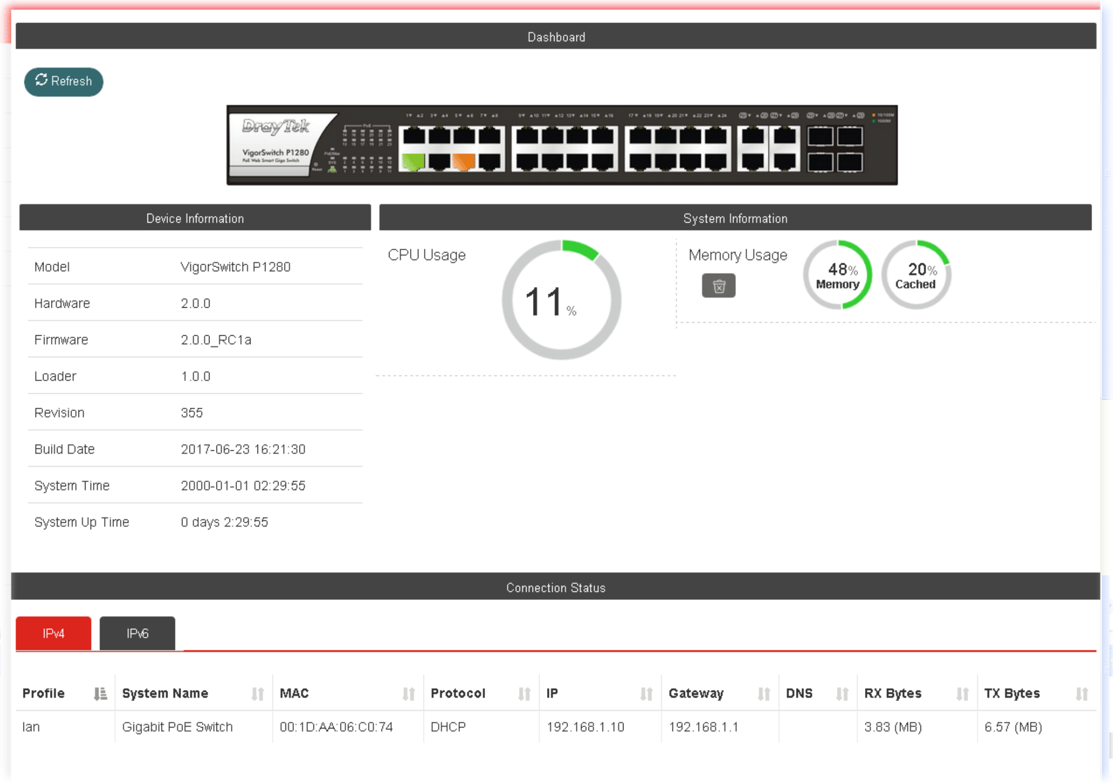
The DHCP Setting is enabled in default. Therefore, if a DHCP server presented on network connected to VigorSwitch, checking before accessing VigorSwitch is essential.

I-4 Dashboard

Click **Dashboard** from the main menu on the left side of the main page.



A web page with default selections will be displayed on the screen. Refer to the following figure:



Device Information

Model	VigorSwitch P1280
Hardware	2.0.0
Firmware	2.0.0_RC1a
Loader	1.0.0
Revision	355
Build Date	2017-06-23 16:21:30
System Time	2000-01-01 02:29:55
System Up Time	0 days 2:29:55

System Information

CPU Usage 11%

Memory Usage 48% Memory 20% Cached

Connection Status

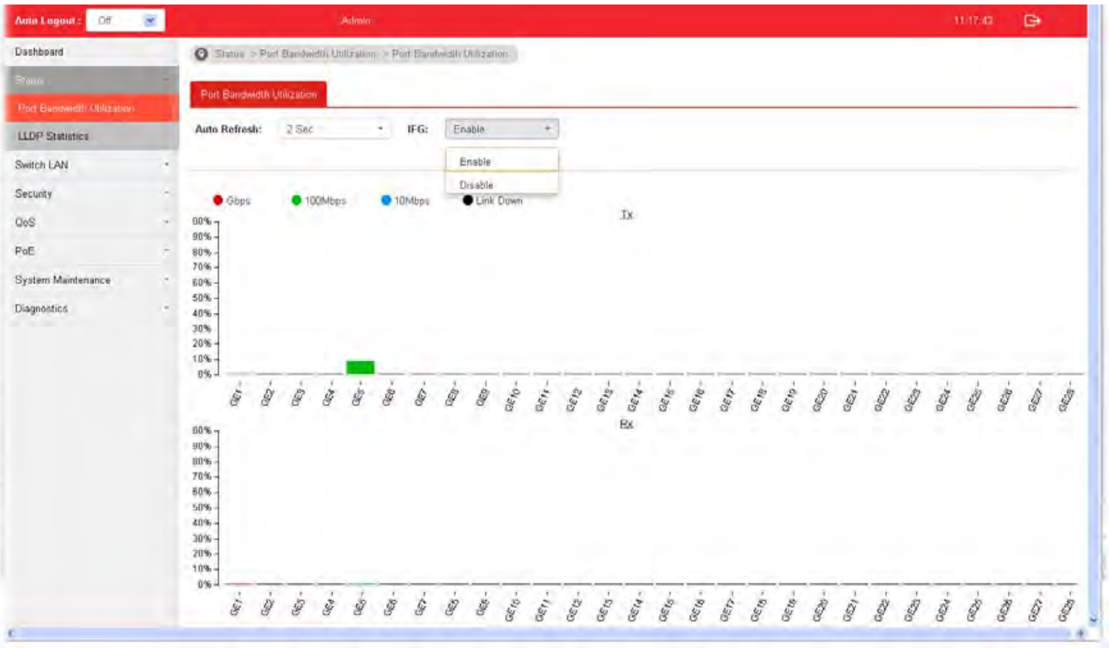
IPv4 IPv6

Profile	System Name	MAC	Protocol	IP	Gateway	DNS	RX Bytes	TX Bytes
lan	Gigabit PoE Switch	00:1D:AA:06:C0:74	DHCP	192.168.1.10	192.168.1.1		3.83 (MB)	6.57 (MB)

I-5 Status

I-5-1 Port Bandwidth Utilization

This page offers the traffic statistics inlcuding data information and data of interframe gap for each port (GE1 to GE28). In which, data of interframe gap can be displayed or hidden by choose **Enable / Disable** for IFG.



Auto Logout : Off

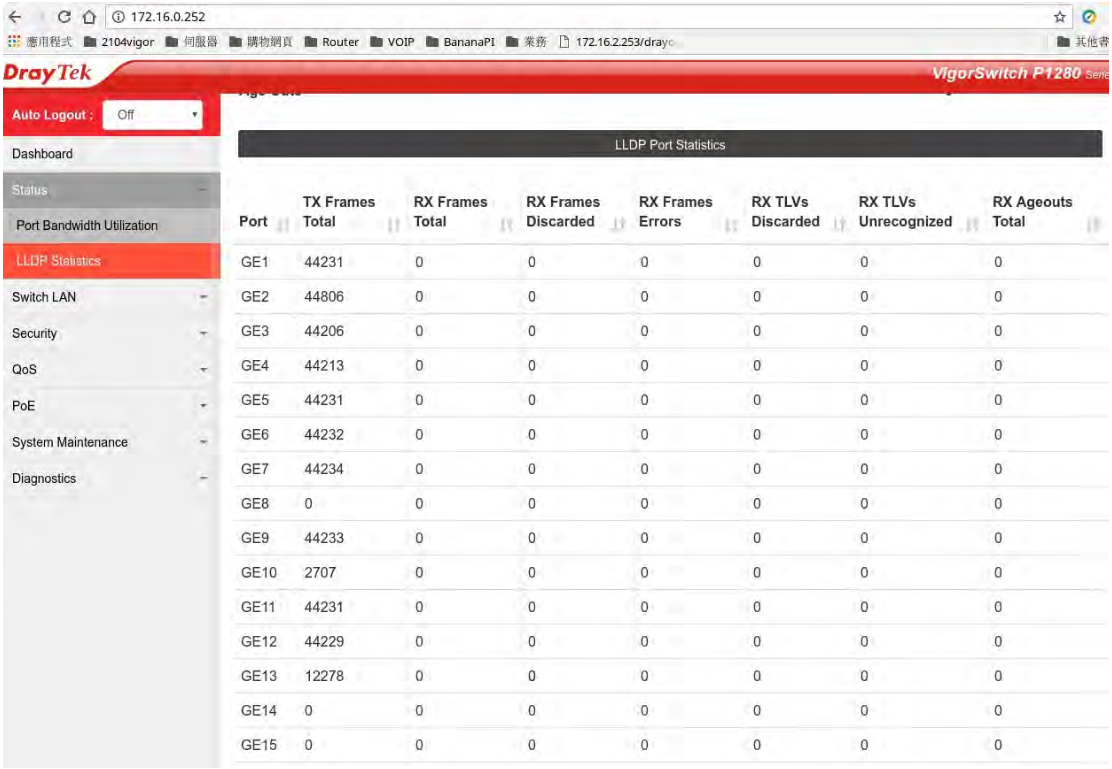
Auto Refresh: 2 Sec

IFG: Enable

Admin
11:17:42
Dashboard
Status
Port Bandwidth Utilization
LLDP Statistics
Switch LAN
Security
QoS
PoE
System Maintenance
Diagnostics
Status > Port Bandwidth Utilization > Port Bandwidth Utilization
Port Bandwidth Utilization
Enable
Disable
● Gbps
● 100Mbps
● 10Mbps
● Link Down
Tx
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8 GE9 GE10 GE11 GE12 GE13 GE14 GE15 GE16 GE17 GE18 GE19 GE20 GE21 GE22 GE23 GE24 GE25 GE26 GE27 GE28
Rx

I-5-2 LLDP Statistics

This page offers the statistics of LLDP packets (in, out and error) of each port (GE1 to GE28).



LLDP Port Statistics

Port	TX Frames Total	RX Frames Total	RX Frames Discarded	RX Frames Errors	RX TLVs Discarded	RX TLVs Unrecognized	RX Ageouts Total
GE1	44231	0	0	0	0	0	0
GE2	44806	0	0	0	0	0	0
GE3	44206	0	0	0	0	0	0
GE4	44213	0	0	0	0	0	0
GE5	44231	0	0	0	0	0	0
GE6	44232	0	0	0	0	0	0
GE7	44234	0	0	0	0	0	0
GE8	0	0	0	0	0	0	0
GE9	44233	0	0	0	0	0	0
GE10	2707	0	0	0	0	0	0
GE11	44231	0	0	0	0	0	0
GE12	44229	0	0	0	0	0	0
GE13	12278	0	0	0	0	0	0
GE14	0	0	0	0	0	0	0
GE15	0	0	0	0	0	0	0

This page is left blank.

Part II Switch LAN

II-1 General Setup

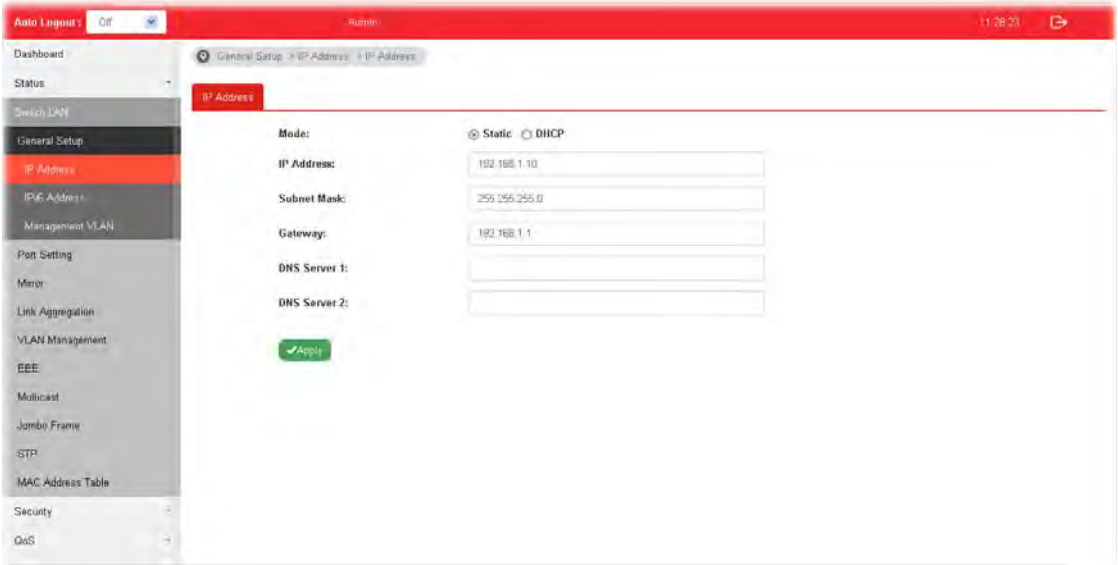
General setup is used to configure settings for the switch network interface and offers how the switch connects to a remote server to get services.

II-1-1 IP Address

Use the IP Address screen to configure the switch IP address and the default gateway device. The gateway field specifies the IP address of the gateway (next hop) for outgoing traffic.

The switch needs an IP address for it to be managed over the network. The factory default IP address is 192.168.1.224. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.

Info	If VigorSwitch has connected to Vigor router, it will use the IP address obtained from the DHCP server on Vigor router. Thus, the user must type the assigned IP as URL for accessing into the web user interface of VigorSwitch. If not, 192.168.1.224 shall be the default IP.



Mode: ● Static ○ DHCP

IP Address: 192.168.1.10

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

DNS Server 1:

DNS Server 2:

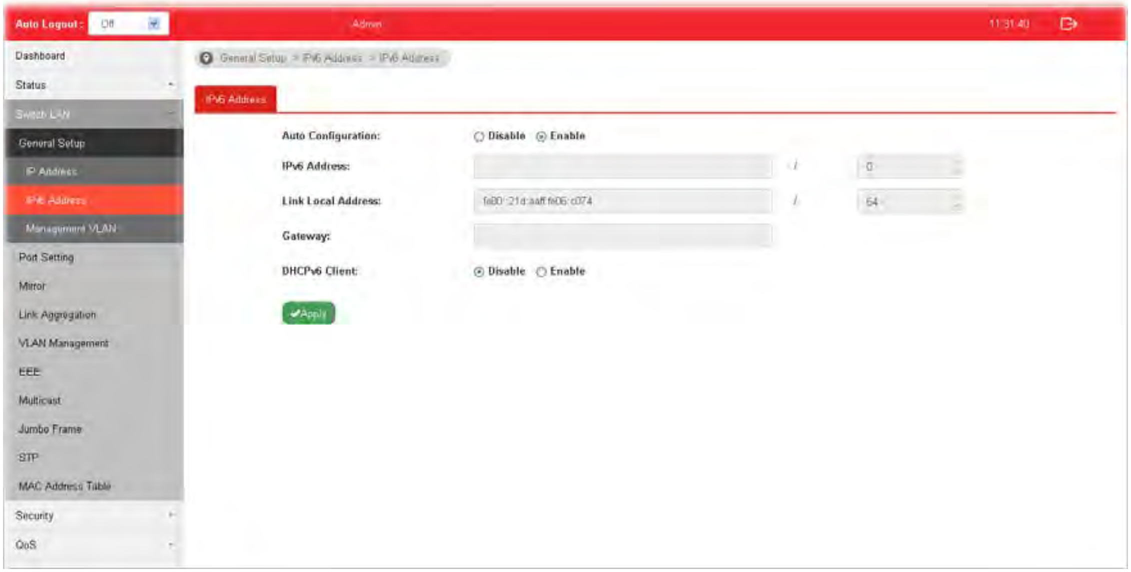
Available settings are explained as follows:

Item	Description
Mode	Select the mode of network connection**.** **Static**- Use static IPv4 address. **DHCP** – Use DHCP provisioned IP address and Gateway if feasible.
IP Address	It is available when **Static** is selected as **Mode**. Enter the IP address of your switch in dotted decimal notation for example 192.168.1.224. If static mode is enabled, enter IP address in this field.
Subnet Mask	It is available when **Static** is selected as **Mode**. Enter the IP subnet mask of your switch in dotted decimal

	notation for example 255.255.255.0. If static mode is enabled, enter subnet mask in this field.
Gateway	It is available when **Static** is selected as **Mode**. Enter the IP address of the gateway in dotted decimal notation. If static mode is enabled, enter gateway address in this field.
DNS Server 1	It is available when **Static** is selected as **Mode**. If static mode is enabled, enter primary DNS server address in this field.
DNS Server 2	It is available when **Static** is selected as **Mode**. If static mode is enabled, enter secondary DNS server address in this field.
Apply	Save the settings or changes to the switch.

II-1-2 IPv6 Address

Use the IPv6 Address screen to configure the switch IPv6 address and the default gateway device. The gateway field specifies the IPv6 address of the gateway (next hop) for outgoing traffic.



Auto Configuration: ○ Disable ● Enable

IPv6 Address: / 0

Link Local Address: fe80::21d:aaff:fe06:c074 / 64

Gateway:

DHCPv6 Client: ● Disable ○ Enable

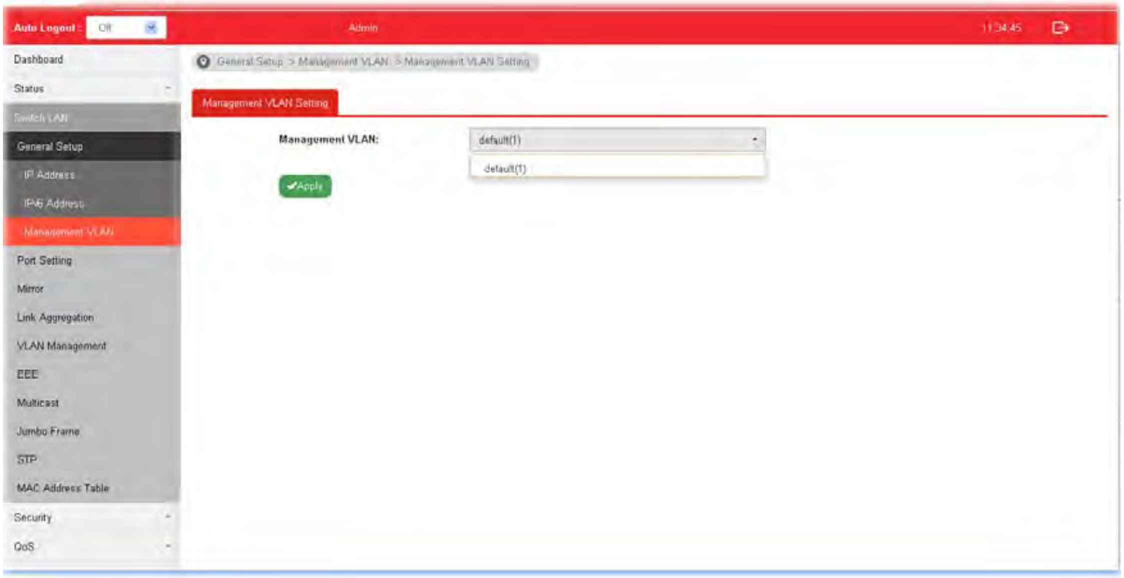
Available settings are explained as follows:

Item	Description
Auto Configuration	**Enable** - Check it to let switch automatically configure IPv6 address.
IPv6 Address	It is available when **Auto Configuration** is **Disable**. Enter the IPv6 address of your switch. If auto configuration mode is disabled, enter IPv6 address in this field.
Link Local Address	It is available when **Auto Configuration** is **Disable**. Type
Gateway	It is available when **Auto Configuration** is **Disable**. Enter the IPv6 address of the router as your default IPv6

	gateway to access IPv6 Internet or other IPv6 network.
DHCPv6 Client	Enable this feature if there is a DHCPv6 server on your network for assigning IPv6 Address, instead of using Router Advertisement.
Apply	Save the settings or changes to the switch.

II-1-3 Management VLAN

This page allows users to change the VLAN ID of management access. Management access protocols such as http, https, SNMP and etc., are only accessible from the VLAN specified as management VLAN.



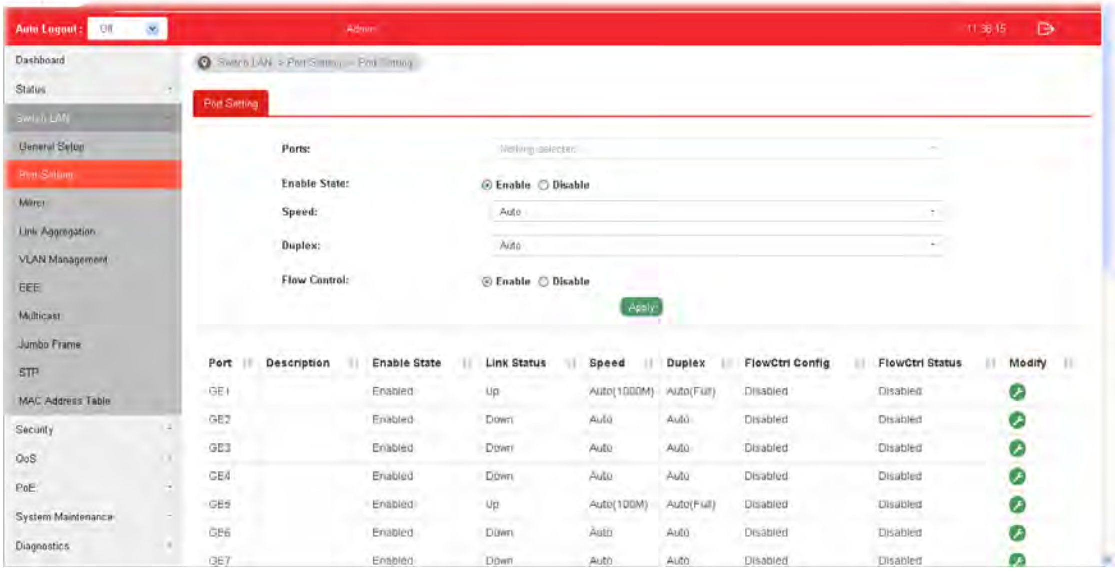
Management VLAN: default(1)

Available settings are explained as follows:

Item	Description
Management VLAN	Select the VLAN ID as management VLAN. You can create additional VLAN profiles by **Switch LAN>>VLAN management>> Create VLAN**.
Apply	Save the settings or changes to the switch.

II-2 Port Setting

Port Setting is used to configure settings for the switch ports, trunk, Layer 2 protocols and other switch features.



Ports: Nothing selected

Enable State: ◉ Enable ○ Disable

Speed: Auto

Duplex: Auto

Flow Control: ◉ Enable ○ Disable

Port	Description	Enable State	Link Status	Speed	Duplex	FlowCtrl Config	FlowCtrl Status	Modify
GE1		Enabled	Up	Auto(1000M)	Auto(Full)	Disabled	Disabled	✎
GE2		Enabled	Down	Auto	Auto	Disabled	Disabled	✎
GE3		Enabled	Down	Auto	Auto	Disabled	Disabled	✎
GE4		Enabled	Down	Auto	Auto	Disabled	Disabled	✎
GE5		Enabled	Up	Auto(100M)	Auto(Full)	Disabled	Disabled	✎
GE6		Enabled	Down	Auto	Auto	Disabled	Disabled	✎
GE7		Enabled	Down	Auto	Auto	Disabled	Disabled	✎

Available settings are explained as follows:

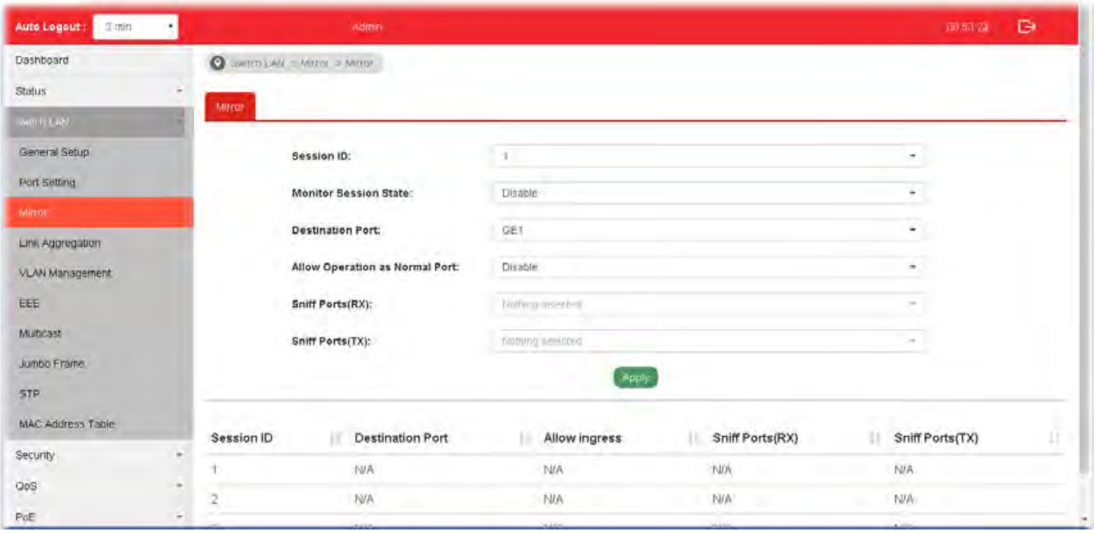
Item	Description
Ports	Use the drop down list to selelct one or more LAN port(s).
Enable State	**Enable -**Click it to enable the port. **Disable -** Click it to disable the port.
Speed	Port speed capabilities: ● **Auto:** Auto speed with all capabilities. ● **Auto-10M:** Auto speed with 10M ability only. ● **Auto-100M:** Auto speed with 100M ability only. ● **Auto-1000M:** Auto speed with 1000M ability only. ● **Auto-10/100M:** Auto speed with 10/100M ability. ● **10M:** Force speed with 10M ability. ● **100M:** Force speed with 100M ability. ● **1000M:** Force speed with 1000M ability. Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect. For SFP fiber module, you might need to manually configure

	the speed to match fiber module speed.
Duplex	Port duplex capabilities: ● **Auto:** Auto duplex with all capabilities. ● **Half:** Auto speed with 10/100M ability only. ● **Full:** Auto speed with 10/100/1000M ability only.
Flow Control	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port. The switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. **Enable -** Click it to enable such function. **Disable -** Click it to disable such function.
Apply	Save the settings or changes to the switch.

II-3 Mirror

This section provides ability to mirror packets coming in or going out on any port to a destination port. Through the packet duplication in the destination port, this feature is convinent for system administrator to monitor / understand the traffic operation.

Session ID 1 to 4 can be enabled simultaneously and operate independently.



Session ID: 1

Monitor Session State: Disable

Destination Port: GE1

Allow Operation as Normal Port: Disable

Sniff Ports(RX): Nothing selected

Sniff Ports(TX): Nothing selected

Session ID	Destination Port	Allow ingress	Sniff Ports(RX)	Sniff Ports(TX)
1	N/A	N/A	N/A	N/A
2	N/A	N/A	N/A	N/A

Available settings are explained as follows:

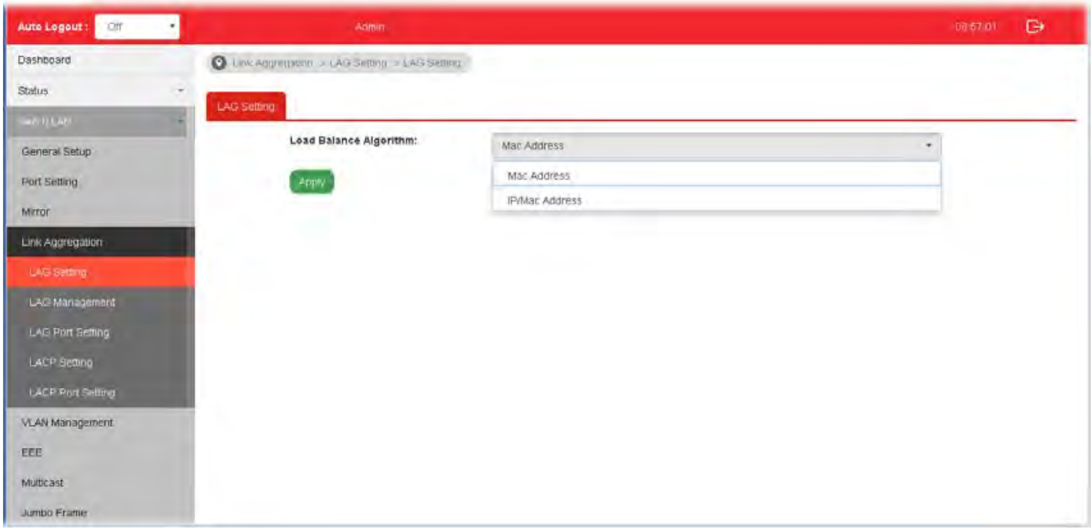
Item	Description
Session ID	Select the session ID (profile 1 to 4) of mirror operation you wish to configure.
Monitor Session State	**Enable** – Enable specified mirror session. **Disable** - Disable specified mirror session.
Destination Port	Specify the port where you wish to observe the mirrored packets.
Allow Operation as Normal Port	**Enable** – The destination port is able to function as a port connecting to network, communicating with other network devices. **Disable** - Only observe the mirrored packets.
Sniff Ports (RX) / (TX)	Select the port(s) which you wish to mirror the traffic, Rx for mirror the packets into the port, Tx for mirror the packets going out from the port.
Apply	Save the settings or changes to the switch.

II-4 Link Aggregation

LAG means Link Aggregation Group which groups some physical ports together to make a single high-bandwidth data path. Thus it can implement traffic load sharing among the member ports in a group to enhance the connection reliability.

II-4-1 LAG Setting

This page allows to configure Load Balance Algorithm for Link Aggregation.



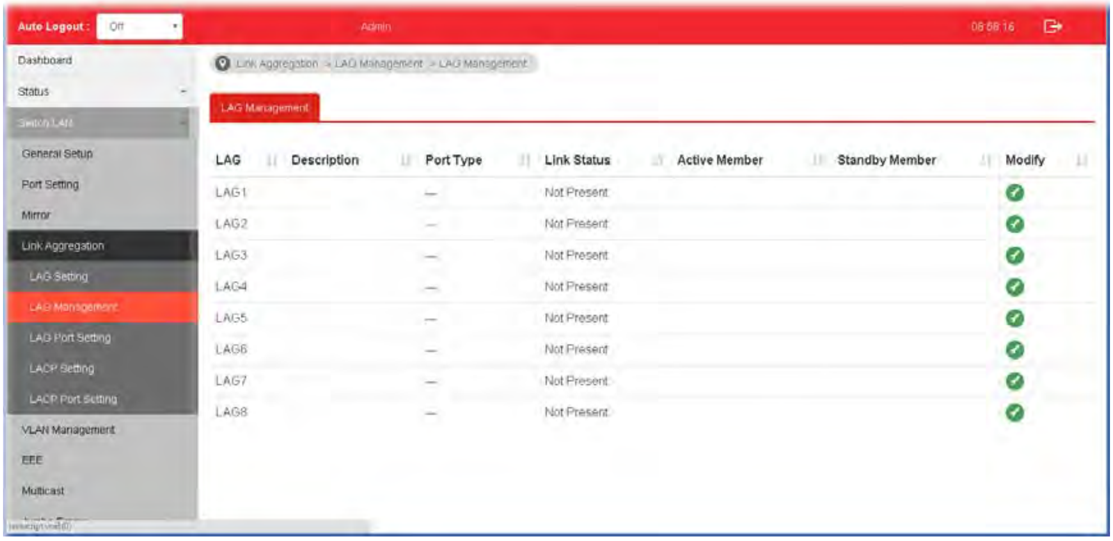
Load Balance Algorithm: Mac Address

Available settings are explained as follows:

Item	Description
Load Balance Algorithm	Select your Load balance algorithm. **MAC address** - Aggregated group will balance the traffic based on different MAC addresses. Therefore, the packets from different MAC addresses will be sent to different links. **IP/Mac Address** - Aggregated group will balance the traffic based on MAC addresses and IP addresses. Therefore, the packets from same MAC addresses but different IP addresses will be sent to different links.
Apply	Save the settings or changes to the switch.

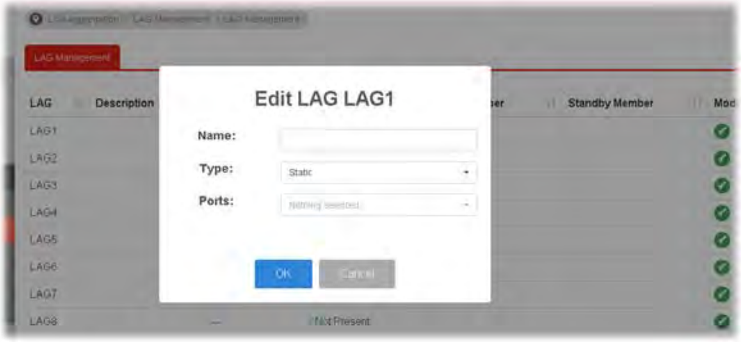
II-4-2 LAG Management

There are eight LAG profiles allowed to group different physical ports (GE1 to GE28). The system will assign certain port(s) as Active Member and Standby Member according to the GE selections.



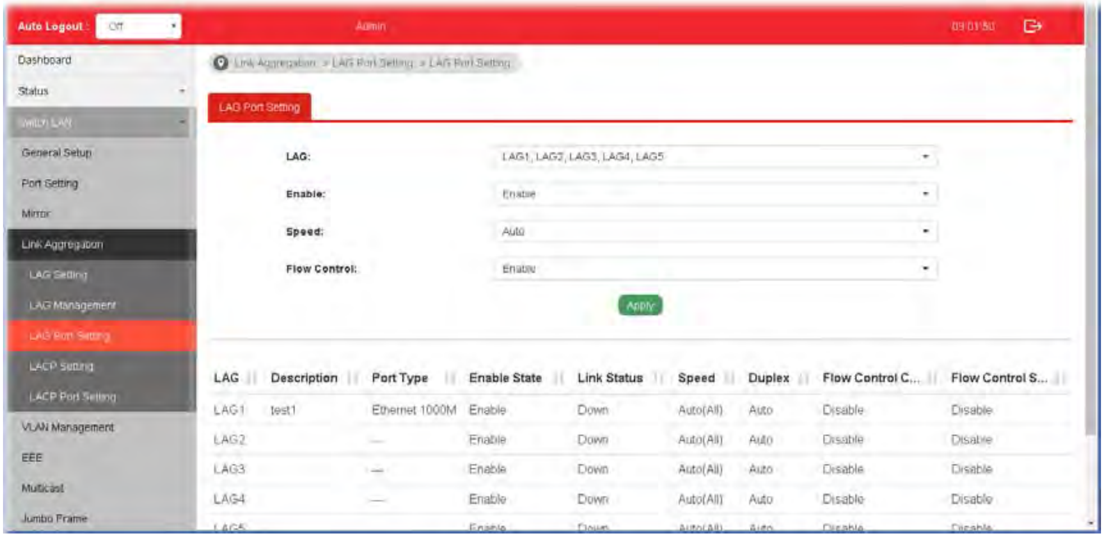
LAG	Description	Port Type	Link Status	Active Member	Standby Member	Modify
LAG1		—	Not Present			✓
LAG2		—	Not Present			✓
LAG3		—	Not Present			✓
LAG4		—	Not Present			✓
LAG5		—	Not Present			✓
LAG6		—	Not Present			✓
LAG7		—	Not Present			✓
LAG8		—	Not Present			✓

Available settings are explained as follows:

Item	Description
Description	Display the port description.
Port Type	Display the type of the LAG.
Link Status	Display LAG port link status.
Active Member	Display active member ports of the LAG.
Standby Member	Display inactive or candidate member ports of the LAG.
Modify	It is used to edit the name, type and port number for each link aggregation profile.  Edit LAG LAG1 Name: Type: Static Ports: Nothing selected OK Cancel **Name-** Enter a string as LAG name. **Type -** Use the drop down menu to specify the type for LAG. ● **Static-** The static aggregated port sends packets over active member without detecting or negotiating with remote aggregated port. ● **LACP-** The LACP aggregated ports place member into active only after negotiated with remote aggregated port for best reliability.

II-4-3 LAG Port Setting

This page defines port setting for each LAG profile (LAG1 to LAG8), including data speed and enabling/disabling the flow control.



LAG: LAG1, LAG2, LAG3, LAG4, LAG5

Enable: Enable

Speed: Auto

Flow Control: Enable

LAG	Description	Port Type	Enable State	Link Status	Speed	Duplex	Flow Control C...	Flow Control S...
LAG1	test1	Ethernet 1000M	Enable	Down	Auto(All)	Auto	Disable	Disable
LAG2		—	Enable	Down	Auto(All)	Auto	Disable	Disable
LAG3		—	Enable	Down	Auto(All)	Auto	Disable	Disable
LAG4		—	Enable	Down	Auto(All)	Auto	Disable	Disable
LAG5			Enable	Down	Auto(All)	Auto	Disable	Disable

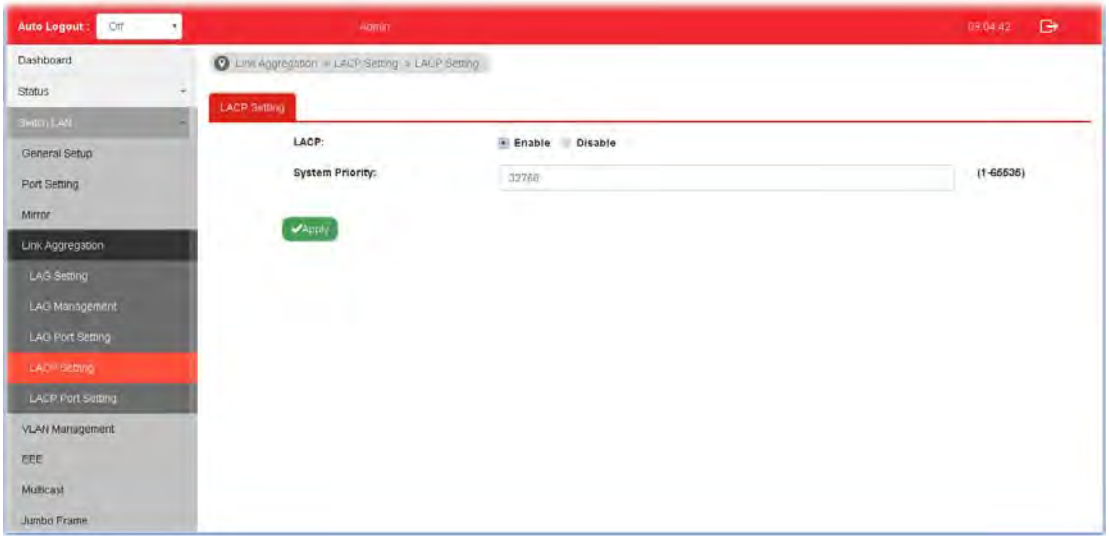
Available settings are explained as follows:

Item	Description
LAG	Use the drop down list to selelct one or more LAG profiles.
Enable	**Enable -**Click it to enable the profile. **Disable -** Click it to disable the profile.
Speed	Port speed capabilities: ● **Auto:** Auto speed with all capabilities. ● **Auto-10M:** Auto speed with 10M ability only. ● **Auto-100M:** Auto speed with 100M ability only. ● **Auto-1000M:** Auto speed with 1000M ability only. ● **Auto-10/100M:** Auto speed with 10/100M ability. ● **10M:** Force speed with 10M ability. ● **100M:** Force speed with 100M ability. ● **1000M:** Force speed with 1000M ability. Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect. For SFP fiber module, you might need to manually configure the speed to match fiber module speed.

Flow Control	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port. The switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. **Enable -** Click it to enable such function. **Disable -** Click it to disable such function.
Apply	Save the settings or changes to the switch.

II-4-4 LACP Setting

This page is used to enable or disable the LACP function.



Auto Logout : Off

LACP: ● Enable ○ Disable

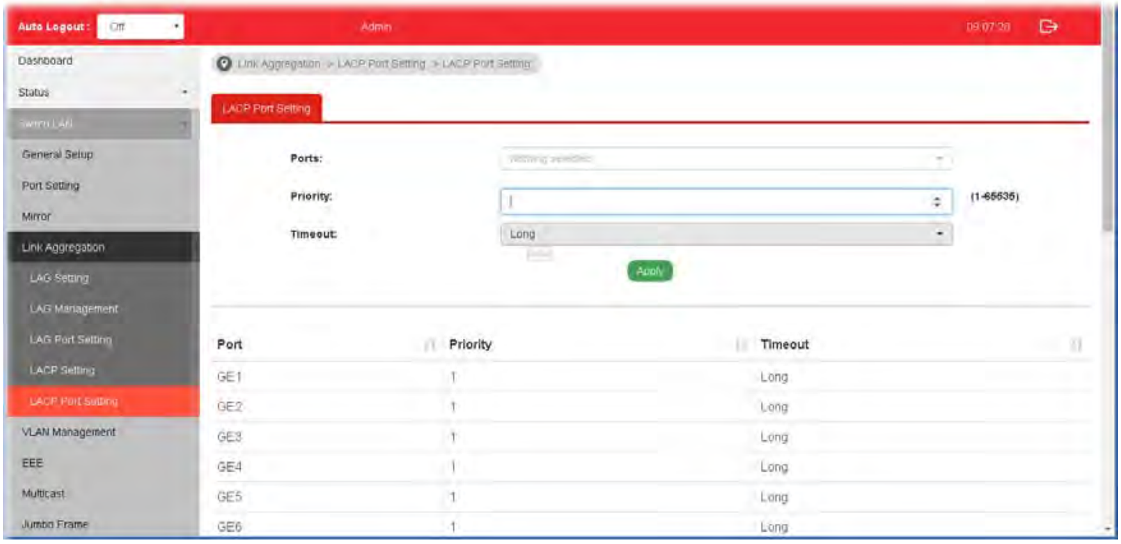
System Priority: 32768 (1-65536)

Available settings are explained as follows:

Item	Description
LACP	**Enable** – Click it to enable such function. **Disable** – Click it to disable the function.
System Priority	The priority is used to determine which switch (local or remote) on the LAG connection is able to decide LACP activities. The lower the number is, the higher the priority for Vigorwitch will be. Therefore, the switch with the highest system priority (e.g., 1) can make decisions about which ports actively participate in LAG at a given time.
Apply	Save the settings or changes to the switch.

II-4-5 LACP Port Setting

This section provides few detailed configuration regarding to Ports under LACP protocol.



Ports: Nothing selected

Priority: 1 (1-65535)

Timeout: Long

Port	Priority	Timeout
GE1	1	Long
GE2	1	Long
GE3	1	Long
GE4	1	Long
GE5	1	Long
GE6	1	Long

Available settings are explained as follows:

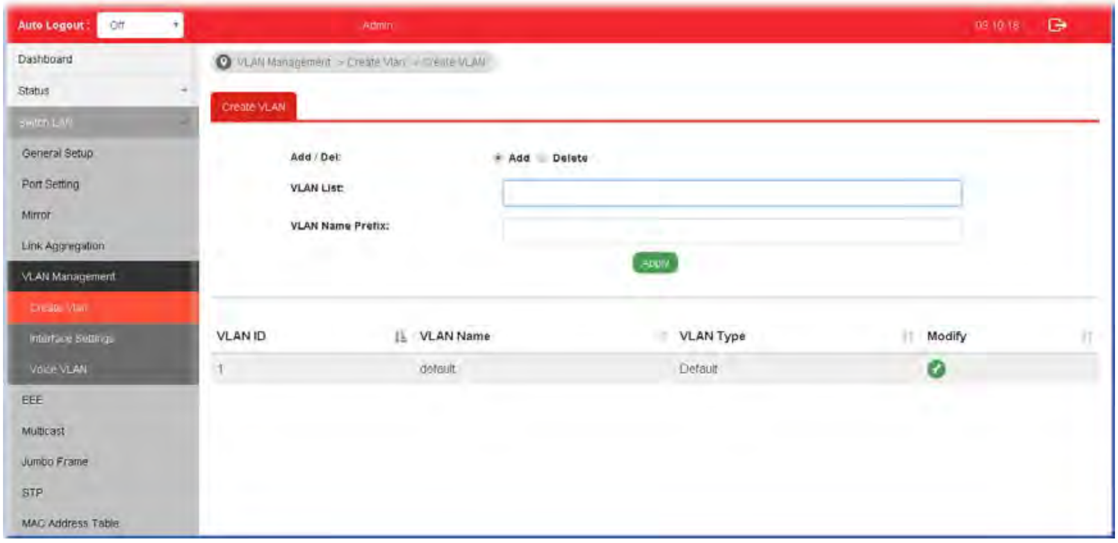
Item	Description
Ports	Use the drop down list to specify LAN Port.
Priority	Enter a port priority number for the port.
Timeout	The timeout option decides how local switch of LAG connection determines connection to be lost. Switch would also notify the remote switch about this setting value, so that remote switch can send LACP PDU in correct timing. **Long** - LACP PDU will be sent every 30 seconds. If port member is not seen over 90 seconds, it will cause port member timeout. **Short** - LACP PDU will be sent per second. If port member is not seen over 3 seconds, it will cause port member timeout.
Apply	Save the settings or changes to the switch.

II-5 VLAN Management

A virtual local area network, virtual LAN or VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together even if they are not located on the same network switch. VLAN membership can be configured through software instead of physically relocating devices or connections.

II-5-1 Create VLAN

This page allows a user to add, edit or delete VLAN settings.



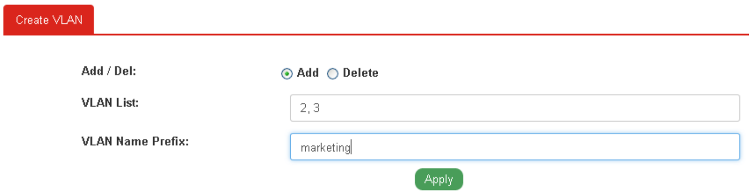
Add / Del: ● Add ○ Delete

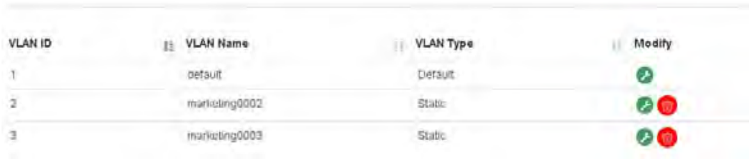
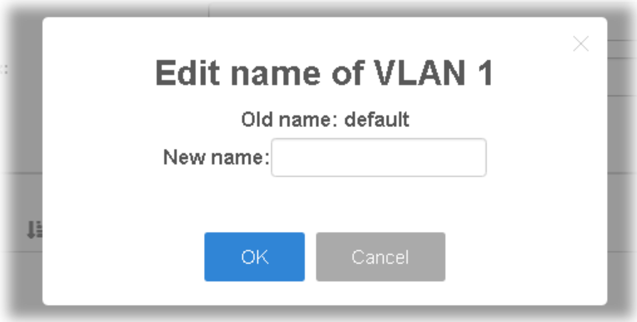
VLAN List:

VLAN Name Prefix:

VLAN ID	VLAN Name	VLAN Type	Modify
1	default	Default	✓

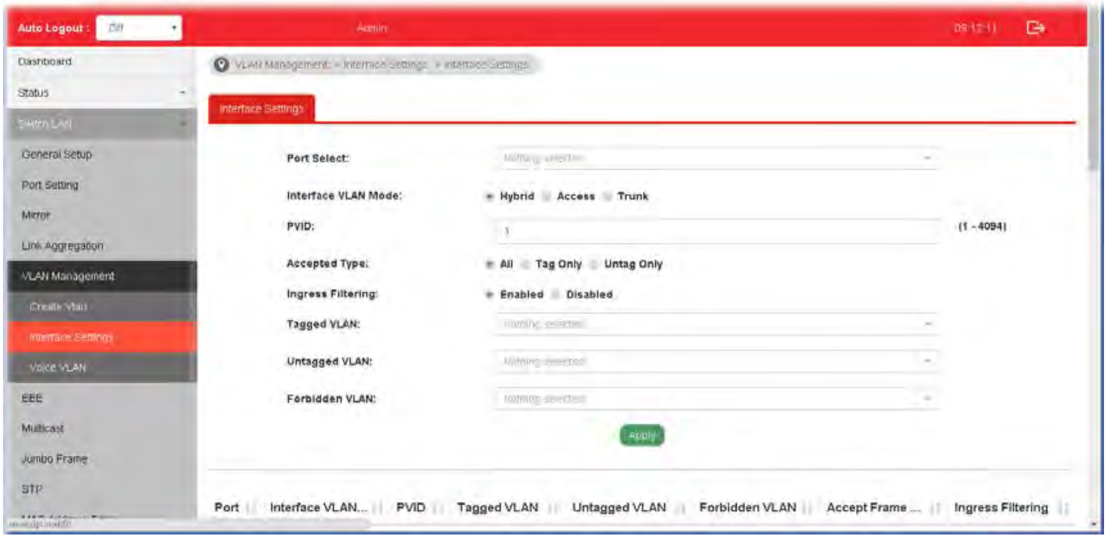
Available settings are explained as follows:

Item	Description
Add / Del	Select which action to perform, add VLANs or delete VLANs. **Add** – Create a new VLAN profile. **Delete** – Delete an existed VLAN profile.
VLAN List	Enter the number as VLAN ID to be created or deleted. If you want to create / delete multiple VLAN profiles, simply enter multiple VLAN ID separated by comma, and/or range of VLAN ID using hyphen.
VLAN Name Prefix	Enter the prefix you wish to add followed by VLAN ID as VLAN name. Leave it empty for using default "VLAN".  Add / Del: ● Add ○ Delete VLAN List: 2, 3 VLAN Name Prefix: marketing After clicking Apply, you will see:

	 VLAN ID / VLAN Name / VLAN Type / Modify 1 / default / Default 2 / marketing0002 / Static 3 / marketing0003 / Static
Apply	Save the settings or changes to the switch.
Modify	🔧 - Modify the name of the selected VLAN ID.  Edit name of VLAN 1 Old name: default New name: OK Cancel **New Name -** Type a name for such VLAN profile. **OK** - Save the settings or changes to the switch. **Cancel -** Close the page and return to previous page. 🗑 - Delete the selected VALN ID.

II-5-2 Interface Settings

This page allows a user to configure interface setting related to VLAN.



Port Select: Nothing selected

Interface VLAN Mode: ● Hybrid ○ Access ○ Trunk

PVID: 1 (1 - 4094)

Accepted Type: ● All ○ Tag Only ○ Untag Only

Ingress Filtering: ● Enabled ○ Disabled

Tagged VLAN: Nothing selected

Untagged VLAN: Nothing selected

Forbidden VLAN: Nothing selected

Available settings are explained as follows:

Item	Description
Port Select	Select LAN ports to configure VLAN Settings.
Interface VLAN Mode	Select the VLAN mode of the interface. **Hybrid** – Support all functions as defined in IEEE

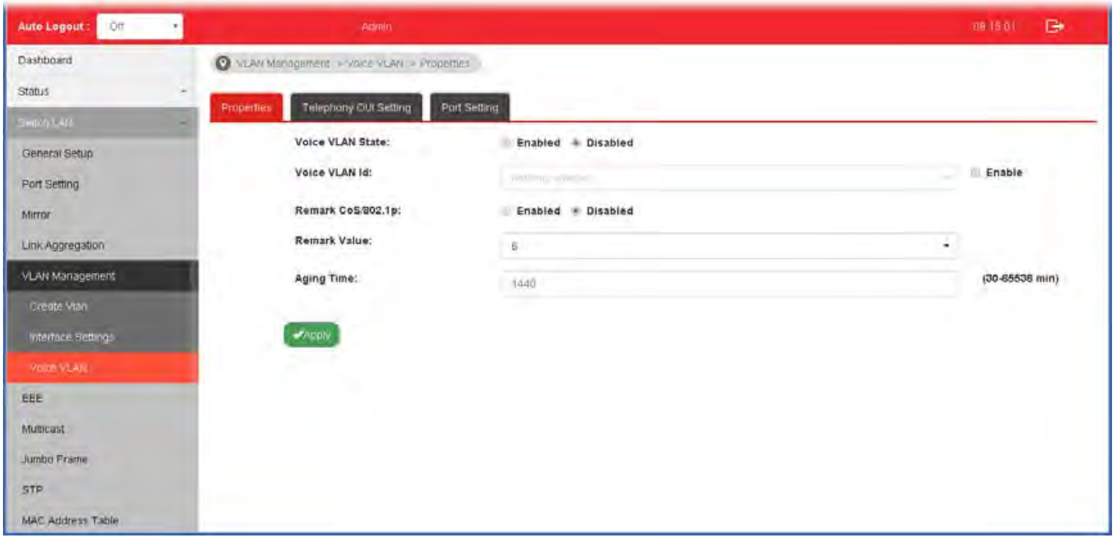
	802.1Qspecification. **Access** – Accepts only untagged frames and join an untagged VLAN. **Trunk** - An untagged member of one VLAN at most, and is a tagged member of zero or more VLANs.
PVID	A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines. For port under **Access** Mode, VLAN ID provided as PVID would automatically be selected as the untagged VLAN.
Accepted Type	Specify the acceptable-frame-type of the specified interfaces. It's only available with Hybrid mode. **All** - Accept frames regardless it's tagged with 802.1q or not. **Tag Only** - Accept frames only with 802.1q tagged. **Untag Only** - Accept frames untagged.
Ingress Filtering	Enable the ingress filtering to filter out any packets not belong to any VLAN members of this port. It is enabled automatically while operating in Access and Trunk mode. **Enabled** – Click it to enable the function. **Disabled** - Click it to disable the function.
Tagged VLAN	Specify the VLAN profile tagged in the VLAN.
Untagged VLAN	Specify the VLAN profile untagged in the VLAN.
Forbidden VLAN	Specify the VLAN profile forbidden in the VLAN.
Apply	Save the settings or changes to the switch.

II-5-3 Voice VLAN

With such feature, a VLAN will be created temporarily and when the specified OUI device delivers protocol packets related to "VoIP", VigorSwitch will guide these packets into the specified Voice LAN with specified priorioty tag to speed up the packet transmission. Such voice VLAN is only active inside VigorSwitch for packet transmission. After these packets leave VigorSwitch, the Voice VLAN tag will be removed immediately.

II-5-3-1 Properties

This page allows a user to configure global and per interface setting of voice VLAN.



Voice VLAN State: ○ Enabled ● Disabled

Voice VLAN Id: □ Enable

Remark CoS/802.1p: ○ Enabled ● Disabled

Remark Value: 6

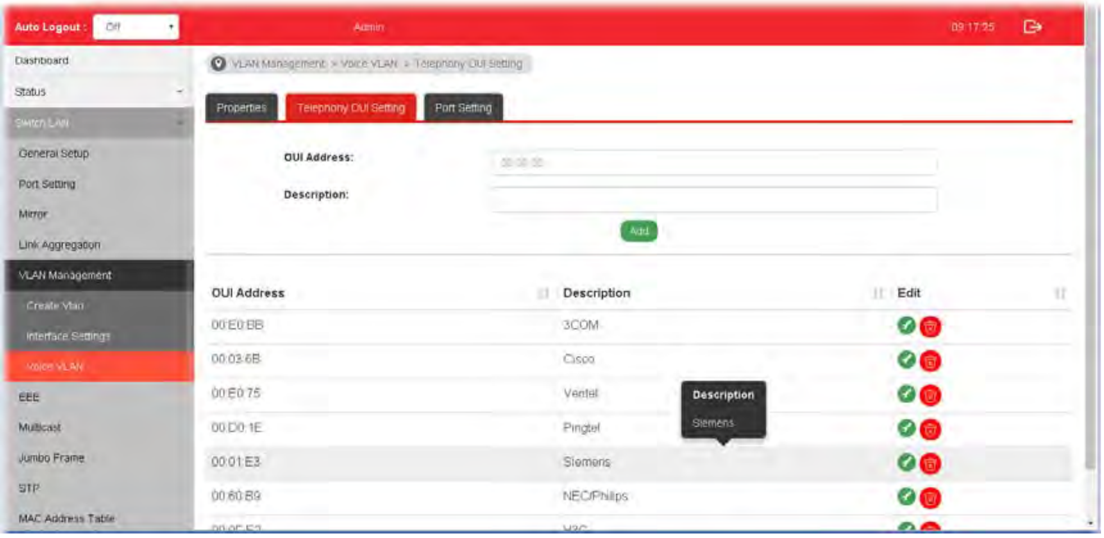
Aging Time: 1440 (30-65536 min)

Available settings are explained as follows:

Item	Description
Voice VLAN State	**Enabled** – Click it to enable Voice VLAN. **Disabled** - Click it to disable Voice VLAN.
Voice VLAN Id	Check the box of Enable first and then select Voice VLAN ID profile.
Remark CoS/802.1p	Click **Enabled / Disabled** to enable or disable 1p remarking. If enabled, qualified packets will be remarked by this value.
Remark Value	Specify the number of packets to be remarked. Specify the CoS/802.1p number you wish ingress VoIP packets be tagged with, so that QoS can prioritize it correctly.
Aging Time	Select value of aging time (30~65536 min). Default is 1440 minutes. A voice VLAN entry will be age out after this time if without any packet pass through.
Apply	Save the settings or changes to the switch.

II-5-3-2 Telephony OUI Setting

This page allows a user to add, edit or delete OUI MAC addresses. Default has 8 pre-defined OUI MAC.

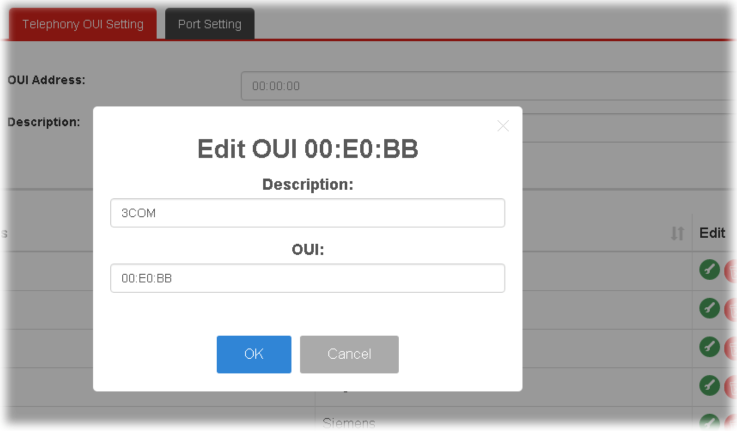


OUI Address: 00:00:00

Description:

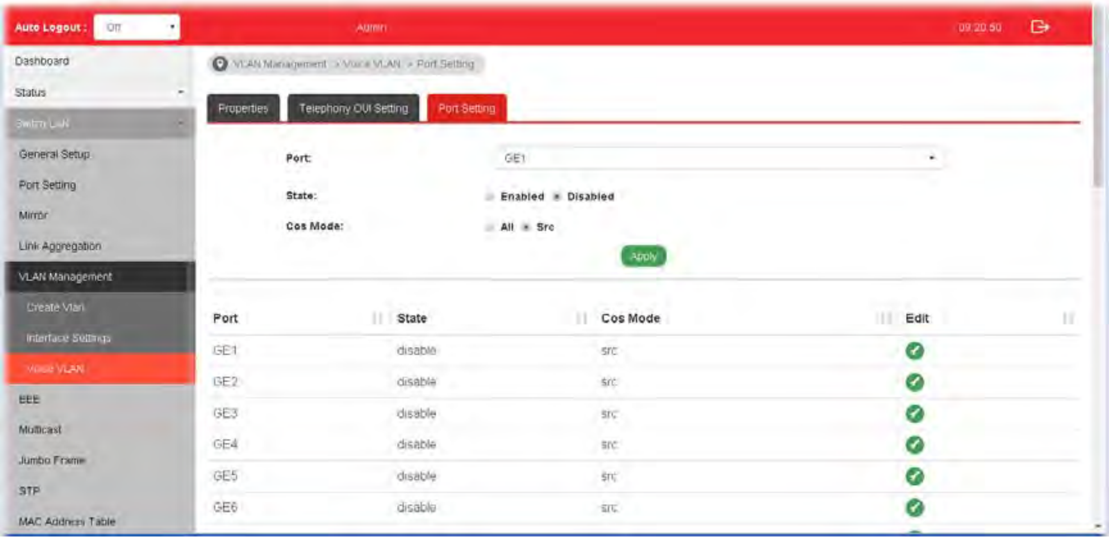
OUI Address	Description	Edit
00:E0:BB	3COM	
00:03:6B	Cisco	
00:E0:75	Veritel	
00:D0:1E	Pingtel	
00:01:E3	Siemens	
00:60:B9	NEC/Philips	
00:0F:E2	H3C	

Available settings are explained as follows:

Item	Description
OUI Address	Type OUI address.
Description	Enter a description of the specified MAC address to the voice VLAN OUI table.
Add	Click it to create a new voice OUI based on the settings configured above.
Edit	Click **Edit** for one entry to modify OUI setting for voice VLAN.  Edit OUI 00:E0:BB Description: 3COM OUI: 00:E0:BB OK Cancel
Delete	Click it to remove the selected OUI entry.

II-5-3-3 Port Setting

This page allows a user to specify LAN port(s) as Voice LAN port.



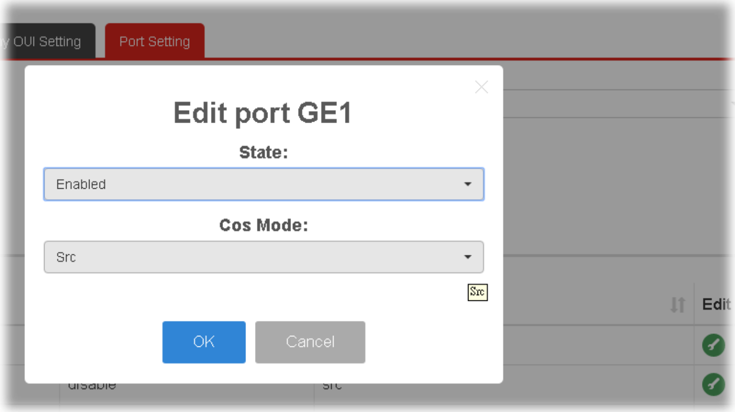
Port: GE1

State: ○ Enabled ● Disabled

Cos Mode: ○ All ● Src

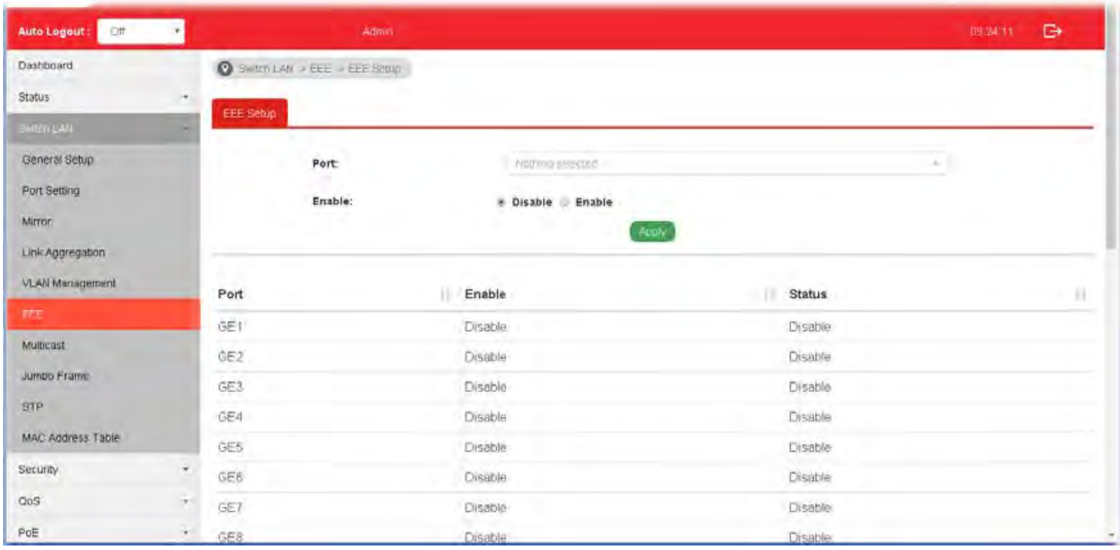
Port	State	Cos Mode	Edit
GE1	disable	src	✓
GE2	disable	src	✓
GE3	disable	src	✓
GE4	disable	src	✓
GE5	disable	src	✓
GE6	disable	src	✓

Available settings are explained as follows:

Item	Description
Port	Use the drop down list to specify one or more LAN ports.
State	**Enabled** – Click it to enable the port settings for Voice LAN. **Disabled** – Click it to disable the port settings for Voice LAN.
Cos Mode	If **Remark CoS/802.1p** is enabled in **Voice VLAN>>Propertie**s, settings in this page shall be applied. Otherwise, this option will not take effect. **All** - Once this port is identified as Voice VLAN by frame with matched OUI, remark CoS/802.1p shall tag for all ingress frame regardless of remarked frame matched with pre-configured OUI or not. **Src (Source)** - Once this port is identified as Voice VLAN by frame with matched OUI, remark CoS/802.1p shall tag for only the matched ingress frame with pre-configured OUI.
Apply	Save the settings or changes to the switch.
Edit	Click **Edit** for one entry to modify port settings (State, Cos Mode) for voice VLAN.  Edit port GE1 State: Enabled Cos Mode: Src

II-6 EEE

This page allows a user to enable or disable port EEE (Energy Efficient Ethernet) function.



Auto Logout : Off

Port: Nothing selected

Enable: ● Disable ○ Enable

Port	Enable	Status
GE1	Disable	Disable
GE2	Disable	Disable
GE3	Disable	Disable
GE4	Disable	Disable
GE5	Disable	Disable
GE6	Disable	Disable
GE7	Disable	Disable
GE8	Disable	Disable

Available settings are explained as follows:

Item	Description
Port	Select one or multiple ports to configure (GE1 to GE28).
Enable	**Enable -**Click it to enable the EEE function. **Disable -** Click it to disable the EEE function.
Apply	Save the settings or changes to the switch.

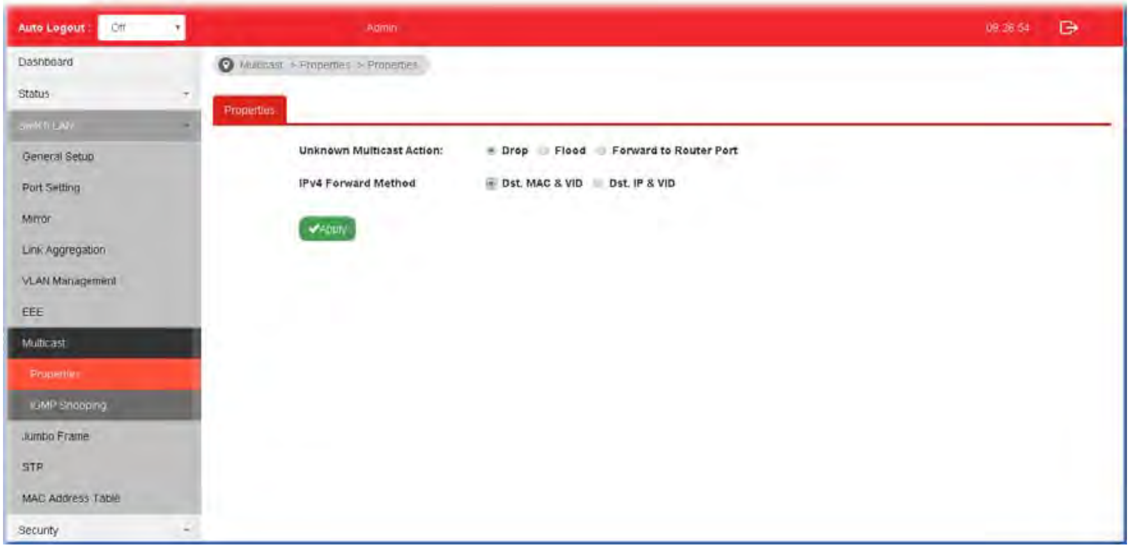
II-7 Multicast

IP multicast is a technique for one-to-many communication over an IP infrastructure in a network.

To avoid the incoming data broadcasting to all GE ports, multicast is useful to transfer the data/message to specified GE ports for IGMP snooping. When VigorSwitch receives a message “subscribed” by the client, it must decide to transfer the data to specified GE ports according to the location of the client (subscribed member).

II-7-1 Properties

For the multicast packets, this page allows the administrator to choose actions for processing the unknown muliticast packets and for handling known packets with MAC address, IP address and VLAN ID.



Unknown Multicast Action: ● Drop ○ Flood ○ Forward to Router Port

IPv4 Forward Method ● Dst. MAC & VID ○ Dst. IP & VID

Available settings are explained as follows:

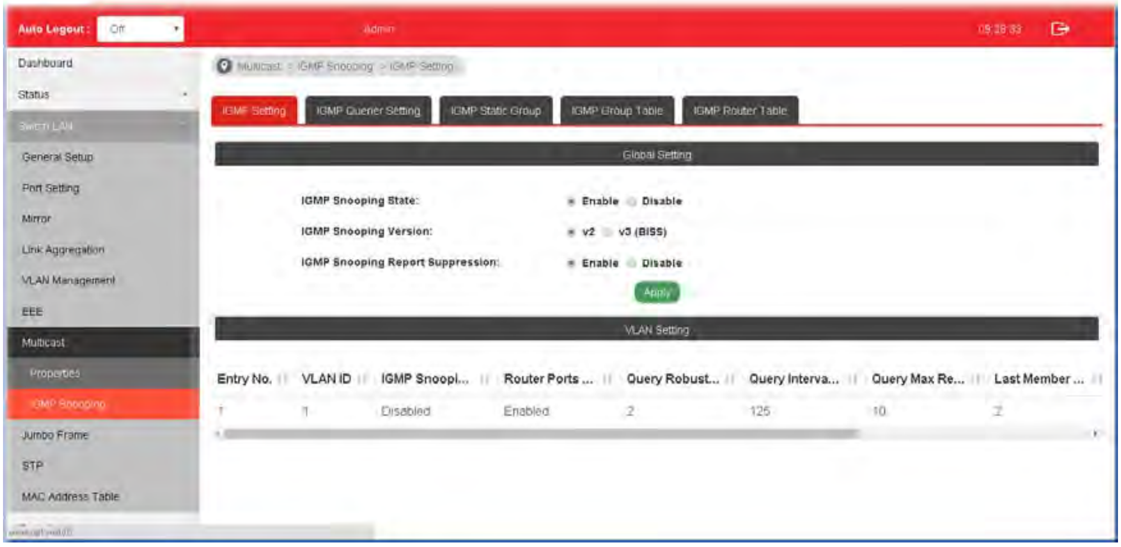
Item	Description
Unknown Multicast Action	Select an action for switch to handle with unknown multicast packet. **Drop:** Drop the unknown multicast data. **Flood:** Flood the unknown multicast data. **Forward to Router port:** Forward the unknown multicast data to router port.
IPv4 Forward Method	Set the IPv4 multicast forward method. **Dst. MAC & VID:** Forward using destination multicast MAC address and VLAN IDs. **Dst. IP & VID:** Forward using destination multicast IP address and VLAN ID.
Apply	Save the settings or changes to the switch.

II-7-2 IGMP Snooping

IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.

II-7-2-1 IGMP Setting

This page allows you to enable/disable IGMP function, select snooping version, and enable/disable snooping report suppression.



IGMP Snooping State: ● Enable ○ Disable

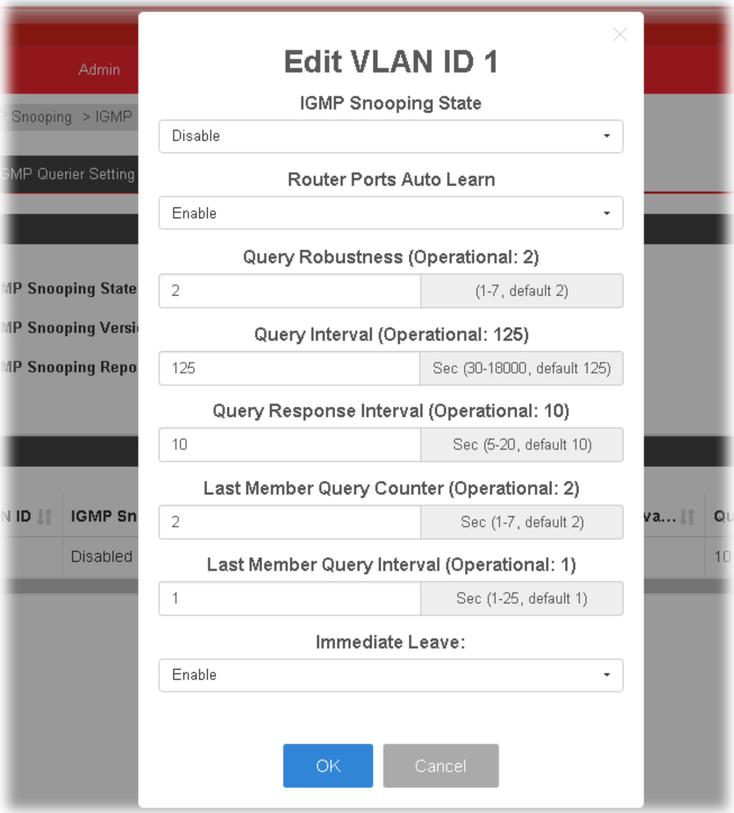
IGMP Snooping Version: ● v2 ○ v3 (BISS)

IGMP Snooping Report Suppression: ● Enable ○ Disable

Entry No.	VLAN ID	IGMP Snoopi...	Router Ports ...	Query Robust...	Query Interva...	Query Max Re...	Last Member ...
1	1	Disabled	Enabled	2	125	10	2

Available settings are explained as follows:

Item	Description
IGMP Snooping State	**Enable** – Click it to set enabling IGMP function. **Disable** - Click it to disable IGMP function.
IGMP Snooping Version	Set the IGMP snooping version. **v2 -** Only support process IGMP v2 packet. **v3** - Support v3 basic and v2.
IGMP Snoopign Report Suppression	Click **Enable** to allow the switch to handle IGMP reports between router and host, suppressing bandwidth used by IGMP.
Apply	Save the settings or changes to the switch.
Edit	Click it to modify IGMP settings for selected VLAN profile.



Edit VLAN ID 1

IGMP Snooping State: Disable

Router Ports Auto Learn: Enable

Query Robustness (Operational: 2): 2 (1-7, default 2)

Query Interval (Operational: 125): 125 Sec (30-18000, default 125)

Query Response Interval (Operational: 10): 10 Sec (5-20, default 10)

Last Member Query Counter (Operational: 2): 2 Sec (1-7, default 2)

Last Member Query Interval (Operational: 1): 1 Sec (1-25, default 1)

Immediate Leave: Enable

IGMP Snooping State -Choose **Enable** to enable IGMP snooping function.

Router Ports Auto Learn - Set the enabling status of IGMP router port learning. Choose Enable to learn router port by IGMP query.

Query Robustness - Set a number which allows tuning for the expected packet loss on a subnet.

Query Interval - Set the interval of querier send general query.

Query Response Interval - It specifies the maximum allowed time before sending a responding report in units of 1/10 second.

Last Member Query Counter - After quering for specified times (defined here) and still not receiving any response from the subscribed member, VigorSwitch will stop transmitting data to the related GE port(s).

Last Member Query Interval - The maximum time interval between counting each member query message with no responses from any subscribed member.

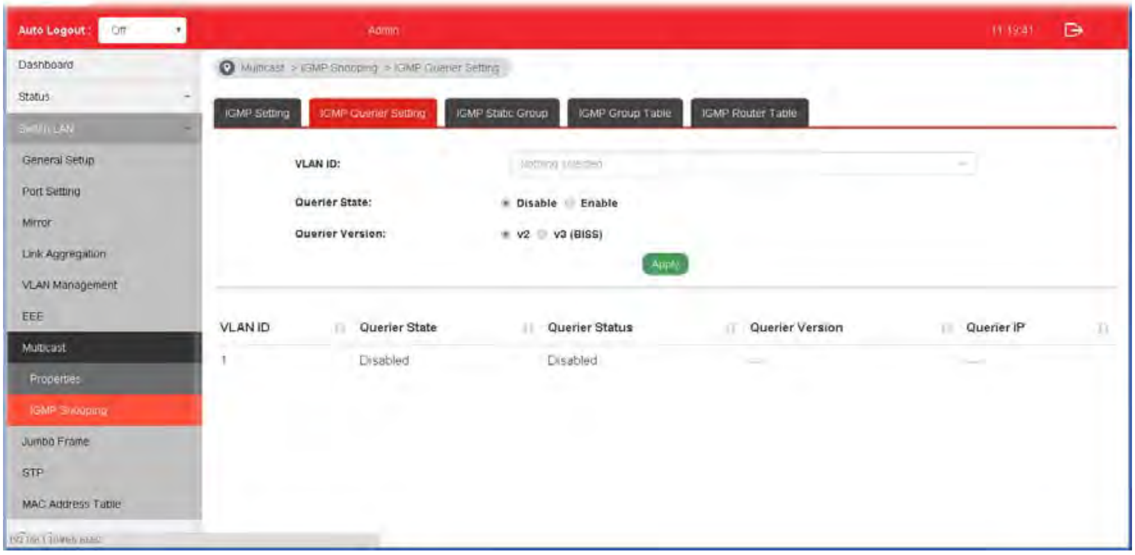
Immediate Leave - Leave the multicast group immediately on the port & VLAN where leave message is sent from, regardless there is still a subscribed member or not. Click Enable to enable Fastleave function.

OK - Save the settings or changes to the switch.

Cancel - Close the page and return to previous page.

II-7-2-2 IGMP Querier Setting

This page allows a user to configure querier settings on specific VLAN of IGMP Snooping.



VLAN ID: Nothing selected

Querier State: ● Disable ○ Enable

Querier Version: ● v2 ○ v3 (BISS)

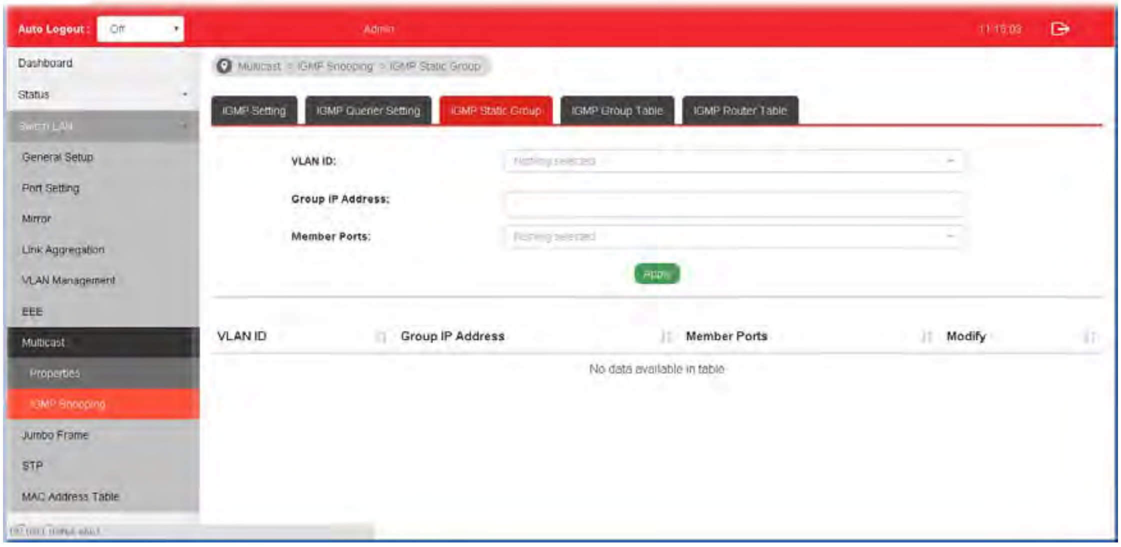
VLAN ID	Querier State	Querier Status	Querier Version	Querier IP
1	Disabled	Disabled	---	---

Available settings are explained as follows:

Item	Description
VLAN ID	Use the drop down list to specify a VLAN profile as IGMP Snooping querier.
Querier State	**Enable -** Click **Enable** to set the enabling status of IGMP Querier on the chosen VLAN profile. **Disable -** Click it to disable the function.
Querier Version	Set the query version of IGMP Querier Election on the chosen VLANs. **v2**: Querier version 2. **v3**: Querier version 3. **Note:** For maximum compatibility, it is suggested to use querier version lower than IGMP snooping version, for there is possibile network mixed with IGMP v2/v3 client and v2 query message is widerly understandable for those clients.
Apply	Save the settings or changes to the switch.

II-7-2-3 IGMP Static Group

The IGMP static group is allowed to assign a VLAN/port as a specific IPv4 multicast member. Every IPv4 multicast stream that belongs to the specified group IP address will be forwarded to the specified port/VLAN member.



VLAN ID: Nothing selected

Group IP Address:

Member Ports: Nothing selected

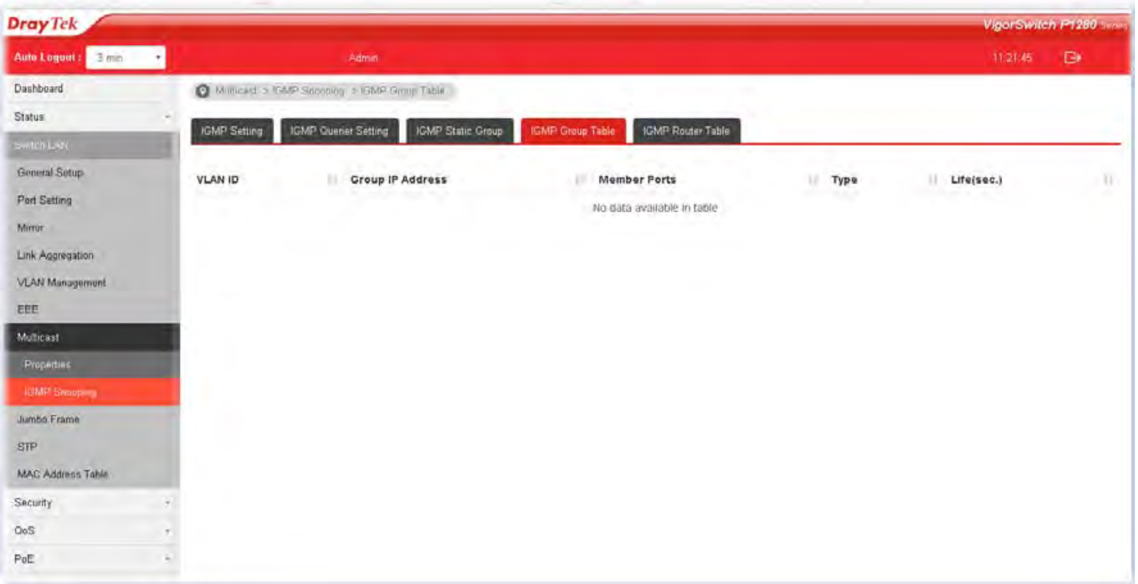
VLAN ID	Group IP Address	Member Ports	Modify
No data available in table			

Available settings are explained as follows:

Item	Description
VLAN ID	Use the drop down list to specify a VLAN profile as IGMP Static Group.
Group IP Address	Specify the IPv4 multicast address you wish to assign for the static group (defined in VLAN ID).
Member Ports	Specify the port(s) that static group with given IPv4 multicast address shall include.
Apply	Save the settings or changes to the switch.

II-7-2-4 IGMP Group Table

This page shows currently known and dynamically learned by IGMP snooping or shows the assigned IPv4 multicast address group in operation.



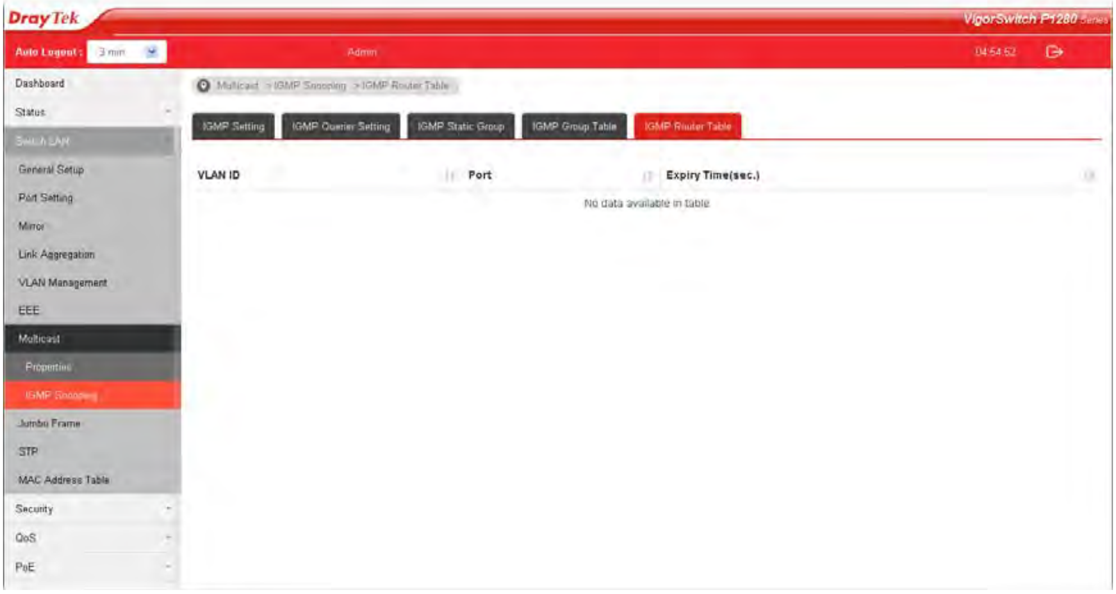
VLAN ID	Group IP Address	Member Ports	Type	Life(sec.)
		No data available in table		

Available settings are explained as follows:

Item	Description
VLAN ID	Display the VLAN of this multicast group belongs to.
Group IP Address	Display the multicast address of this multicast group.
Member Ports	Display the port(s) where subscribing member of this multicast group belongs to.
Type	Display if it is dynamically learned or statically assigned.
Life(sec.)	Display the life time of this multicast member left if no membership report sent again.

II-7-2-5 IGMP Router Table

This page shows the IGMP querier router known to this switch.



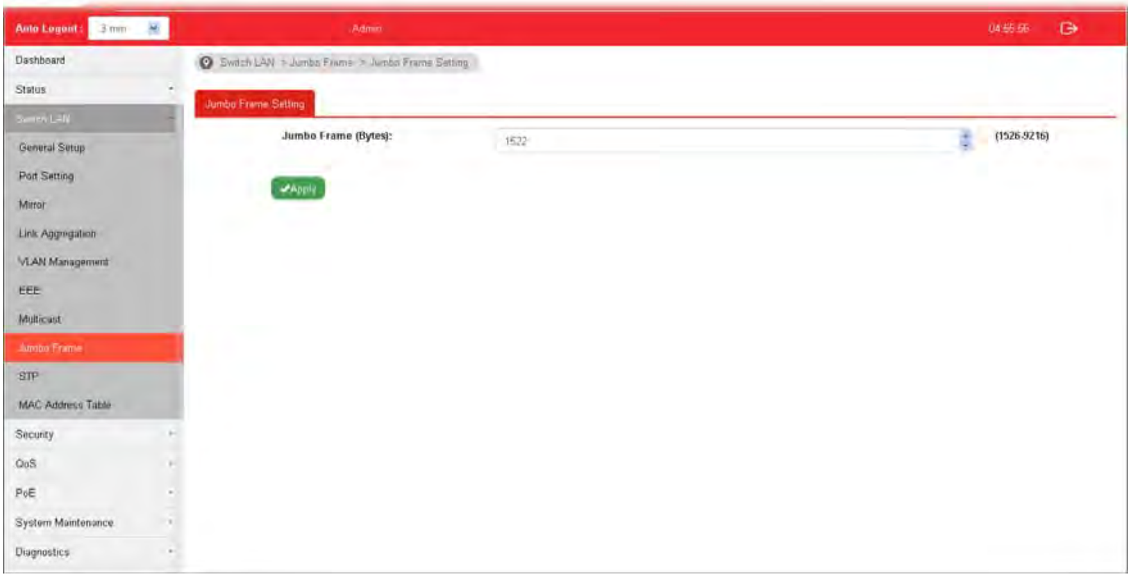
VLAN ID	Port	Expiry Time(sec.)
No data available in table		

Available settings are explained as follows:

Item	Description
VLAN ID	Display the VLAN profile that the IGMP querier belongs to.
Port	Display the uplink ports where querier router exists.
Expire Time (sec.)	Display the time before querier is considered no longer existed.

II-8 Jumbo Frame

This page allows a user to configure switch port jumbo frame settings.



Jumbo Frame (Bytes): 1522 (1526-9216)

Available settings are explained as follows:

Item	Description
Jumbo Frame (Bytes)	Enter Jumbo frame size. The valid range is 1526 bytes – 9216 bytes.
Apply	Save the settings or changes to the switch.

II-9 STP

The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network.

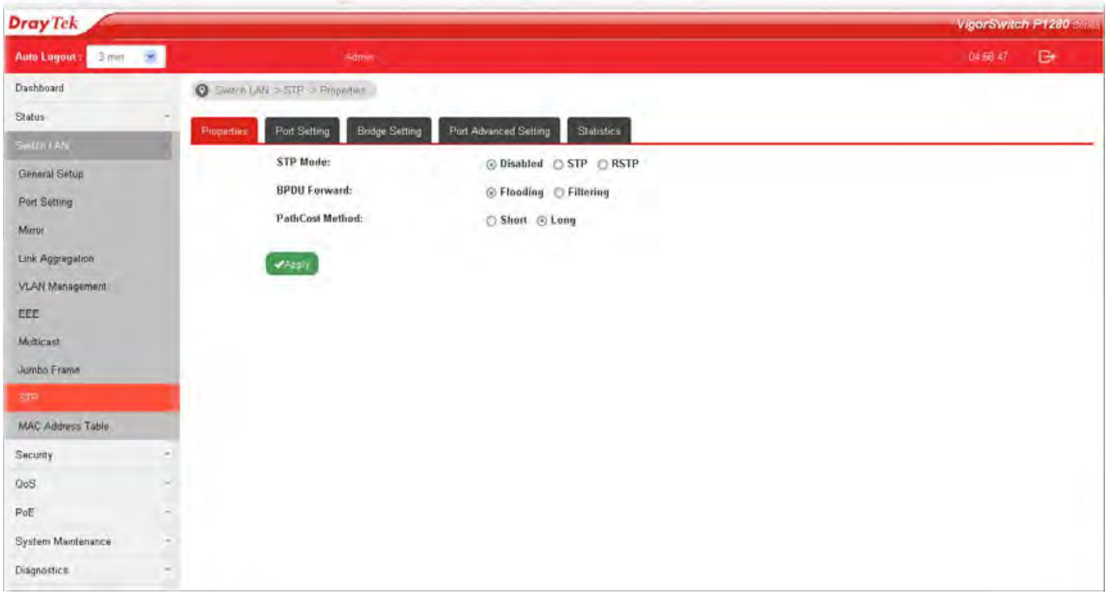
Bridge Protocol Data Units (BPDUs) are frames that contain information about the Spanning Tree Protocol (STP). Switches send BPDUs using a unique MAC address from its origin port and a multicast address as destination MAC (01:80:C2:00:00:00, or 01:00:0C:CC:CC:CD for Per VLAN Spanning Tree).

For STP algorithms to function, the switches need to share information about themselves and their connections. What they share are bridge protocol data units (BPDUs).

BPDUs are sent out as multicast frames to which only other layer 2 switches or bridges are listening. If any loops (multiple possible paths between switches) are found in the network topology, the switches will co-operate to disable a port or ports to ensure that there are no loops; that is, from one device to any other device in the layer 2 network, only one path can be taken.

II-9-1 Properties

This page allows a user to configure and display STP property configuration.



STP Mode: ● Disabled ○ STP ○ RSTP

BPDU Forward: ● Flooding ○ Filtering

PathCost Method: ○ Short ● Long

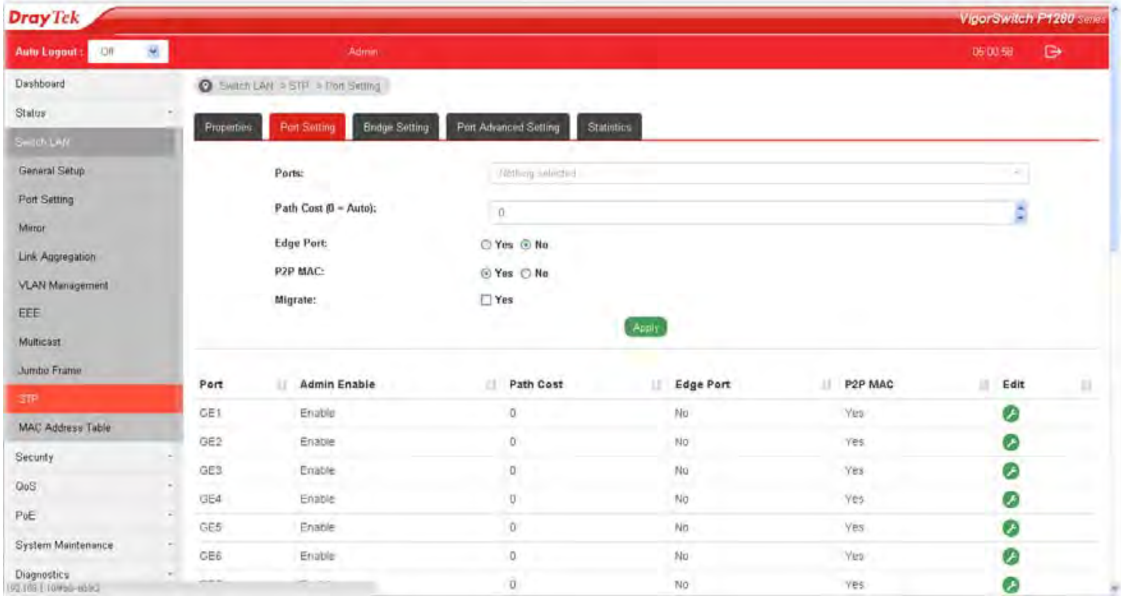
Available settings are explained as follows:

Item	Description
STP Mode	Set the operating mode of Spanning Tree (STP). **Disabled -** Disable the STP operation. **STP -** Enable the Spanning Tree (STP) operation. **RSTP -** Enable the Rapid Spanning Tree (RSTP) operation.
BPDU Forward	Specify the BPDU forward method when the STP is disabled. **Filtering -** Filter the BPDU when STP is disabled. **Flooding -** Flood the BPDU when STP is disabled.
PathCost Method	Specify the path cost method. **Long -** Specifies that the default port path costs are within the

	range: 1~200,000,000. **Short -** Specifies that the default port path costs are within the range: 1~65,535.
Apply	Save the settings or changes to the switch.

II-9-2 Port Setting

This page allows the user to configure and display STP port settings.



Ports: Nothing selected

Path Cost (0 = Auto): 0

Edge Port: ○ Yes ● No

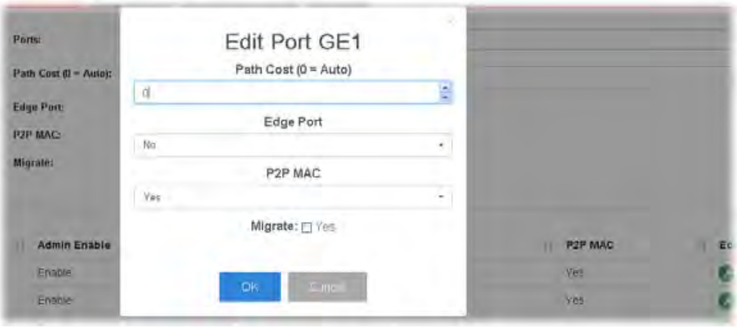
P2P MAC: ● Yes ○ No

Migrate: □ Yes

Port	Admin Enable	Path Cost	Edge Port	P2P MAC	Edit
GE1	Enable	0	No	Yes	✎
GE2	Enable	0	No	Yes	✎
GE3	Enable	0	No	Yes	✎
GE4	Enable	0	No	Yes	✎
GE5	Enable	0	No	Yes	✎
GE6	Enable	0	No	Yes	✎
		0	No	Yes	✎

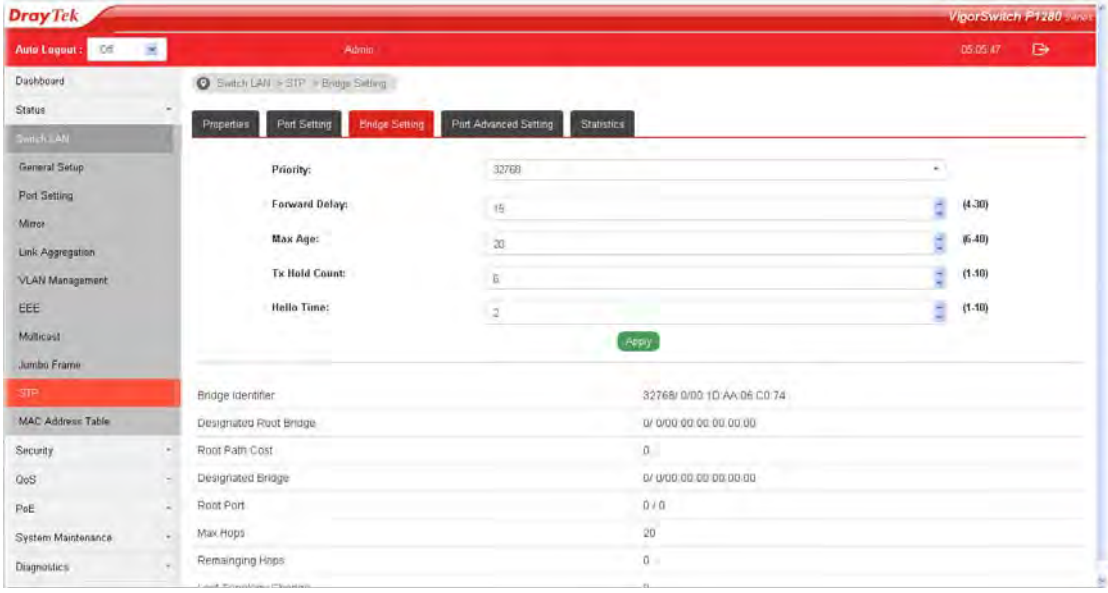
Available settings are explained as follows:

Item	Description
Ports	Use the drop down to specify the interface ID or the list of interface IDs.
Path Cost (0=Auto)	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost. Entering 0 means the switch will automatically assign a value.
Edge Port	In the edge mode, the interface would be put into the Forwarding state immediately upon link up. If the edge mode is enabled for the interface and there are BPDUs received on the interface, the loop might be occurred in the short time before the STP state change. **Yes -** Enable the function. **No -** Disable the function.
P2P MAC	**Yes -** It means the STP of link type on this port is full-duplex and directly connect to another switch or host. **No -** It means the STP of link type on this port is "not" full-duplex and "does not" directly connect to another switch or host.
Migrate	**Yes -** Check it to force the specified port to send one RSTP BPDU (Rapid Spanning Tree Protocol Bridge Protocol Data Unit).

Apply	Save the settings or changes to the switch. After clicking it, the settings configured above will be shown on the table below.
Admin Enable	**YES -** Such port is managed by VigorSwitch.
Edit	Click it to modify the settings for the selected GE port.  Edit Port GE1 Path Cost (0 = Auto): 0 Edge Port: No P2P MAC: Yes Migrate: □ Yes OK Cancel

II-9-3 Bridge Setting

This page allows you to configure required information to negotiate with other VigorSwitch for determining the bridge switch.



Priority: 32768

Forward Delay: 15 (4-30)

Max Age: 20 (6-40)

Tx Hold Count: 6 (1-10)

Hello Time: 2 (1-10)

Bridge Identifier	32768/ 0/00:1D:AA:06:C0:74
Designated Root Bridge	0/ 0/00:00:00:00:00:00
Root Path Cost	0
Designated Bridge	0/ 0/00:00:00:00:00:00
Root Port	0 / 0
Max Hops	20
Remainging Hops	0

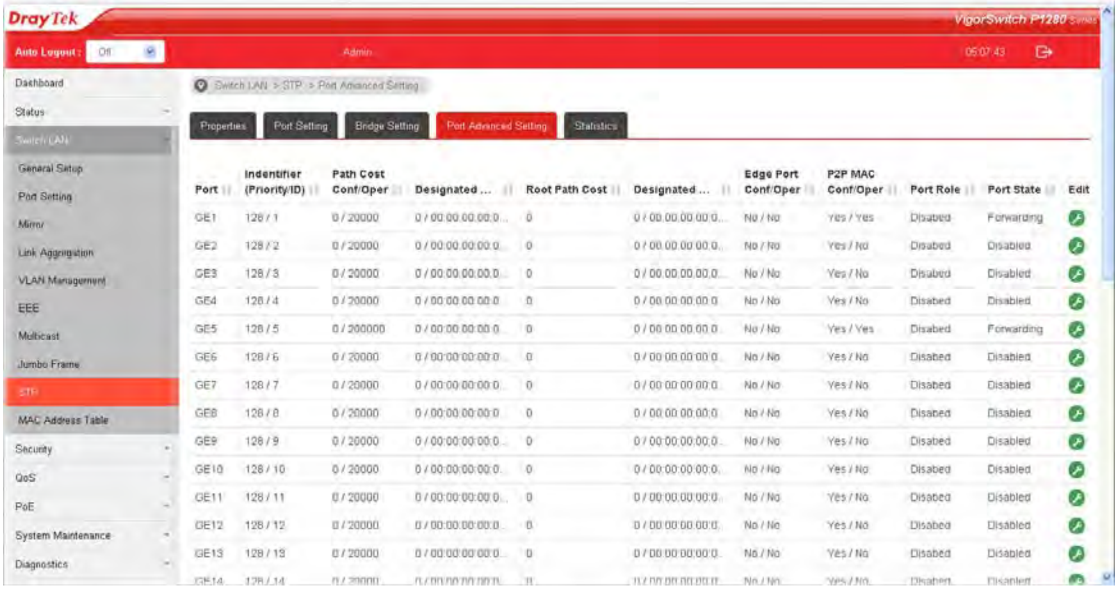
Available settings are explained as follows:

Item	Description
Priority	Specify the bridge priority. The valid range is from 0 to 61440, and the value should be the multiple of 4096. It ensures the probability that the switch is selected as the root bridge, and the lower value has the higher priority for the switch to be selected as the root bridge of the topology.
Forward Delay	Specify the STP forward delay time, which is the amount of time that a port remains in the Listening and Learning states before it enters the Forwarding state. Its valid range is from 4 to 10 seconds.

Max Age	Specify the time interval in seconds for a switch to wait the configuration messages, without attempting to redefine its own configuration.
Tx Hold Count	Specify the tx-hold-count used to limit the maximum numbers of packets transmission per second. The valid range is from 1 to 10.
Hello Time	Specify the STP hello time in second to broadcast its hello message to other bridge by Designated Ports. Its valid range is from 1 to 10 seconds.
Apply	Save the settings or changes to the switch.

II-9-4 Port Advanced Setting

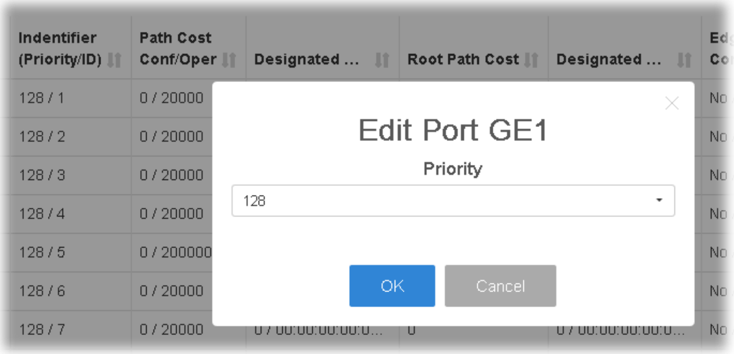
This page allows user to edit general setting of STP CIST port and browser CIST port status.



Port	Indentifier (Priority/ID)	Path Cost Conf/Oper	Designated ...	Root Path Cost	Designated ...	Edge Port Conf/Oper	P2P MAC Conf/Oper	Port Role	Port State	Edit
GE1	128 / 1	0 / 20000	0 / 00:00:00:00:0...	0	0 / 00:00:00:00:0...	No / No	Yes / Yes	Disabed	Forwarding	
GE2	128 / 2	0 / 20000	0 / 00:00:00:00:0...	0	0 / 00:00:00:00:0...	No / No	Yes / No	Disabed	Disabled	
GE3	128 / 3	0 / 20000	0 / 00:00:00:00:0...	0	0 / 00:00:00:00:0...	No / No	Yes / No	Disabed	Disabled	
GE4	128 / 4	0 / 20000	0 / 00:00:00:00:0...	0	0 / 00:00:00:00:0...	No / No	Yes / No	Disabed	Disabled	
GE5	128 / 5	0 / 200000	0 / 00:00:00:00:0...	0	0 / 00:00:00:00:0...	No / No	Yes / Yes	Disabed	Forwarding	
GE6	128 / 6	0 / 20000	0 / 00:00:00:00:0...	0	0 / 00:00:00:00:0...	No / No	Yes / No	Disabed	Disabled	
GE7	128 / 7	0 / 20000	0 / 00:00:00:00:0...	0	0 / 00:00:00:00:0...	No / No	Yes / No	Disabed	Disabled	
GE8	128 / 8	0 / 20000	0 / 00:00:00:00:0...	0	0 / 00:00:00:00:0...	No / No	Yes / No	Disabed	Disabled	
GE9	128 / 9	0 / 20000	0 / 00:00:00:00:0...	0	0 / 00:00:00:00:0...	No / No	Yes / No	Disabed	Disabled	
GE10	128 / 10	0 / 20000	0 / 00:00:00:00:0...	0	0 / 00:00:00:00:0...	No / No	Yes / No	Disabed	Disabled	
GE11	128 / 11	0 / 20000	0 / 00:00:00:00:0...	0	0 / 00:00:00:00:0...	No / No	Yes / No	Disabed	Disabled	
GE12	128 / 12	0 / 20000	0 / 00:00:00:00:0...	0	0 / 00:00:00:00:0...	No / No	Yes / No	Disabed	Disabled	
GE13	128 / 13	0 / 20000	0 / 00:00:00:00:0...	0	0 / 00:00:00:00:0...	No / No	Yes / No	Disabed	Disabled	
GE14	128 / 14	0 / 20000	0 / 00:00:00:00:0...	0	0 / 00:00:00:00:0...	No / No	Yes / No	Disabed	Disabled	

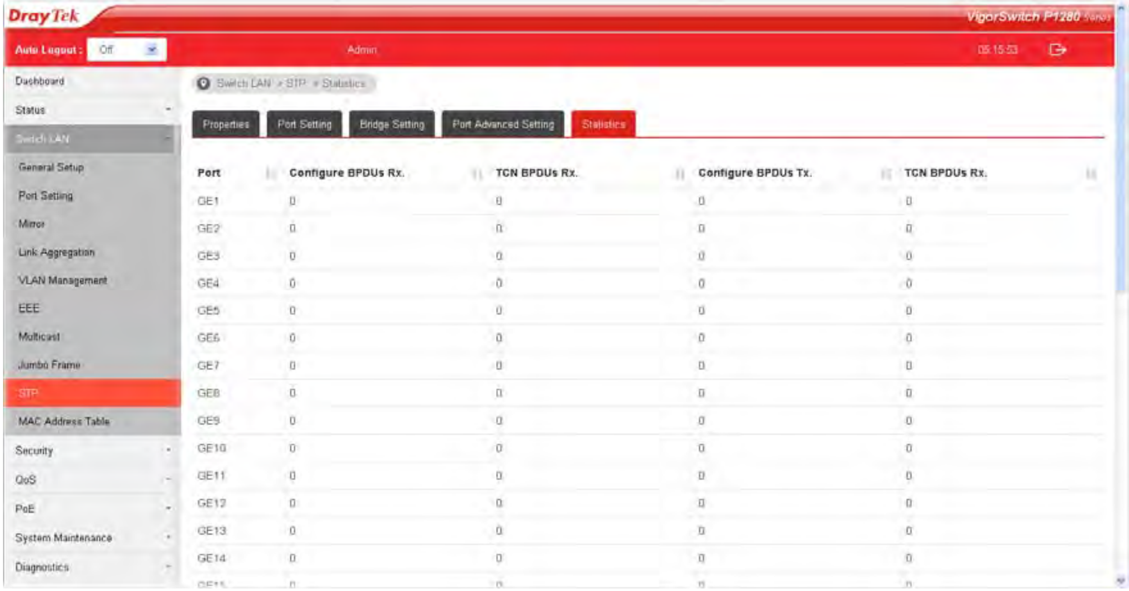
Available settings are explained as follows:

Item	Description
Port	Display the interface number for GE and LAG.
Indentifier(Priority/ID)	Display the spanning tree port identifier.
Path Cost Conf/Oper	Display current path cost of given port.
Designated Root Bridge	Display the identifier of designated root bridge.
Root Path Cost	Display the operational root path cost.
Designated Bridge	Display the identifier of next bridge on this port.
Edge Port Conf/Oper	Display if this port is configured as Edge of STP network, for speed up link up.
P2P MAC Conf/Oper	Display if this port is configured as point to point link to another switch or host.
Port Role	Display current port role on the specified port. The possible values will be: “Disabled”, “Root”, “Designated”, “Alternative”, and “Backup”.

Port State	Display current port state on the specified port. The possible values will be: “Disabled”, “Discarding”, “Learning”, and “Forwarding”.
Edit	Click it to modify the settings for the selected GE port / LAG port.  Edit Port GE1 Priority: 128 OK Cancel

II-9-5 Statistics

This page displays STP statistics.



Port	Configure BPDUs Rx.	TCN BPDUs Rx.	Configure BPDUs Tx.	TCN BPDUs Rx.
GE1	0	0	0	0
GE2	0	0	0	0
GE3	0	0	0	0
GE4	0	0	0	0
GE5	0	0	0	0
GE6	0	0	0	0
GE7	0	0	0	0
GE8	0	0	0	0
GE9	0	0	0	0
GE10	0	0	0	0
GE11	0	0	0	0
GE12	0	0	0	0
GE13	0	0	0	0
GE14	0	0	0	0

Available settings are explained as follows:

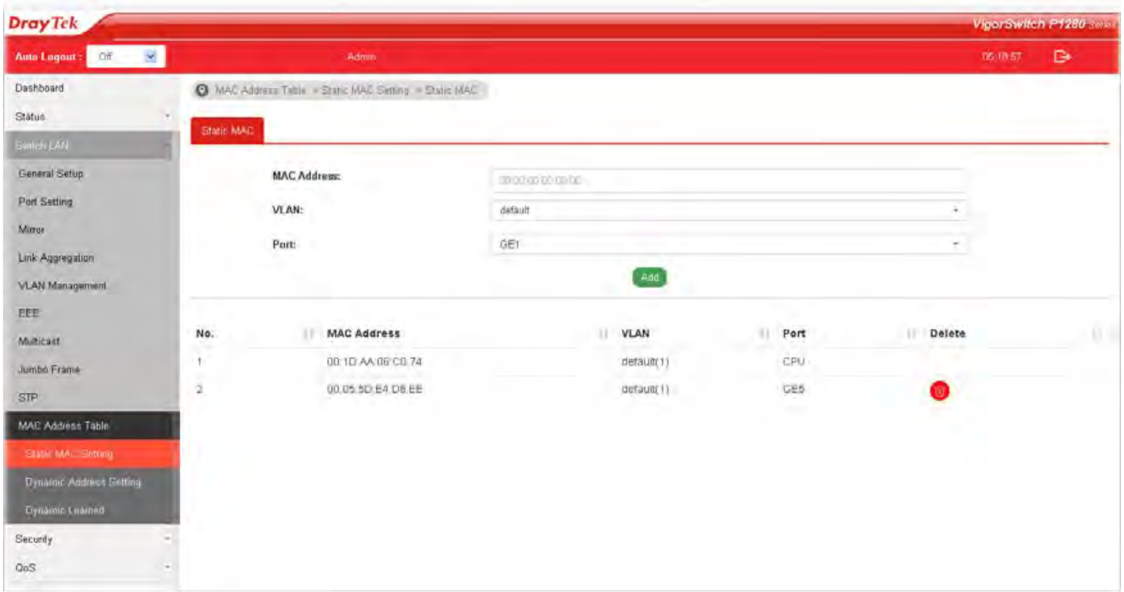
Item	Description
Port	Display the port number (GE / LAG).
Configure BPDUs Rx.	Display the counts of the received CONFIG BPDU.
TCN BPDUs Rx.	Display the counts of the received TCN BPDU.
Configure BPDUs Tx.	Display the counts of the transmitted CONFIG BPDU.
TCN BPDUs Rx	Display the counts of the transmitted TCN BPDU.

II-10 MAC Address Table

This section allows user to view the dynamic MAC address entries in the MAC table, change related setting, and assign MAC address into MAC table.

II-10-1 Static MAC Setting

This section allows user to manually assign MAC address into MAC table. The configuration result will be displayed on the table listed on the lower side of this web page.



MAC Address: 00:00:00:00:00:00

VLAN: default

Port: GE1

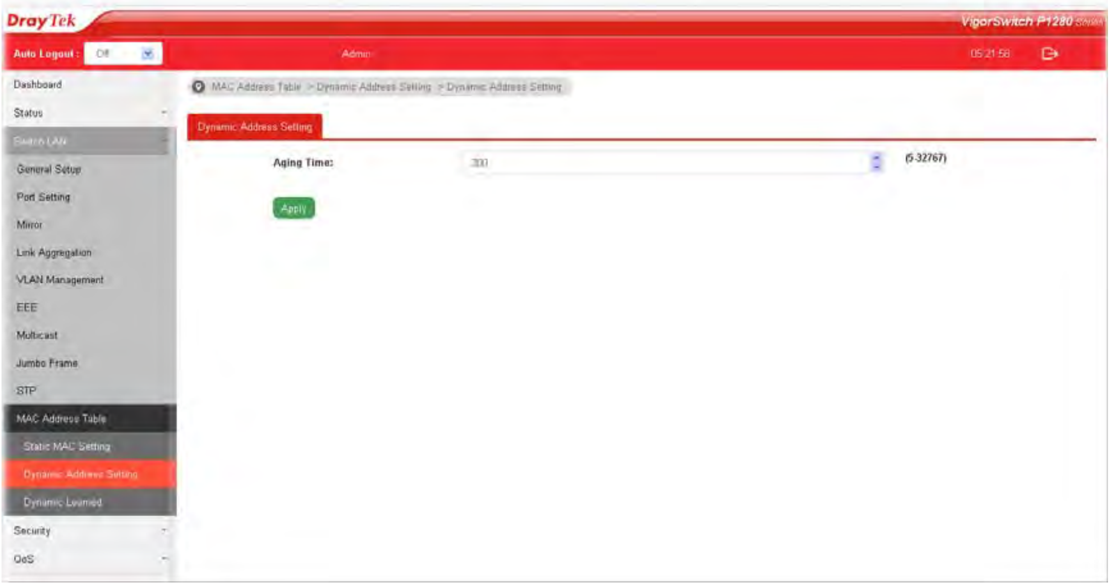
No.	MAC Address	VLAN	Port	Delete
1	00:1D:AA:06:C0:74	default(1)	CPU	
2	00:05:5D:E4:D8:EE	default(1)	GE5	●

Available settings are explained as follows:

Item	Description
MAC Address	Enter the MAC address that will be forwarded.
VLAN	This is the VLAN group to which the MAC address belongs.
Port	Select the port where received frame of matched destination MAC address will be forwarded to.
Add	Click it to add any port into the static MAC table.
Delete	Click it to remove the selected port from the static MAC table.

II-10-2 Dynamic Address Setting

This page allows a user to configure aging time for dynamic MAC address.



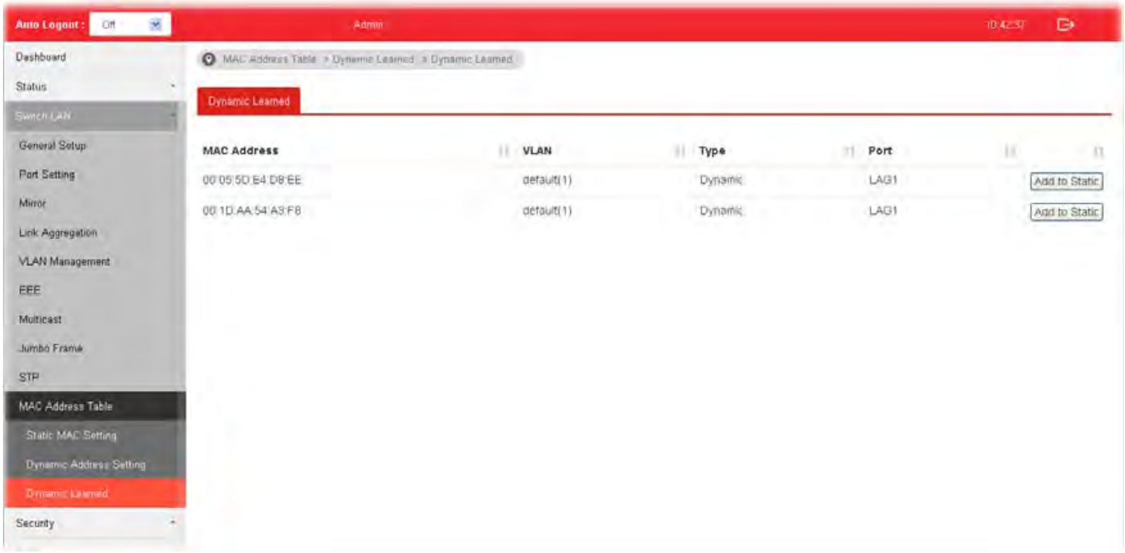
Aging Time: 300 (5-32767)

Available settings are explained as follows:

Item	Description
Aging Time	Enter the Dynamic MAC address aging out value (5-32767 seconds).
Apply	Save the settings or changes to the switch.

II-10-3 Dynamic Learned

This page displays the MAC address and port number automatically learned by VigorSwitch.



MAC Address	VLAN	Type	Port	
00:05:5D:E4:D8:EE	default(1)	Dynamic	LAG1	Add to Static
00:1D:AA:54:A3:F8	default(1)	Dynamic	LAG1	Add to Static

Available settings are explained as follows:

Item	Description
MAC Address	Display the MAC address that will be forwarded.
VLAN	Display the VLAN group to which the MAC address belongs.
Type	Display whether the MAC address is **Dynamic** (learned by the Switch) or **Static Unicast** (manually entered in the **Static MAC Forwarding** screen).
Port	Display the port to which this MAC address belongs.
Add to Static	Click this button to add any port into the static MAC table.

This page is left blank.

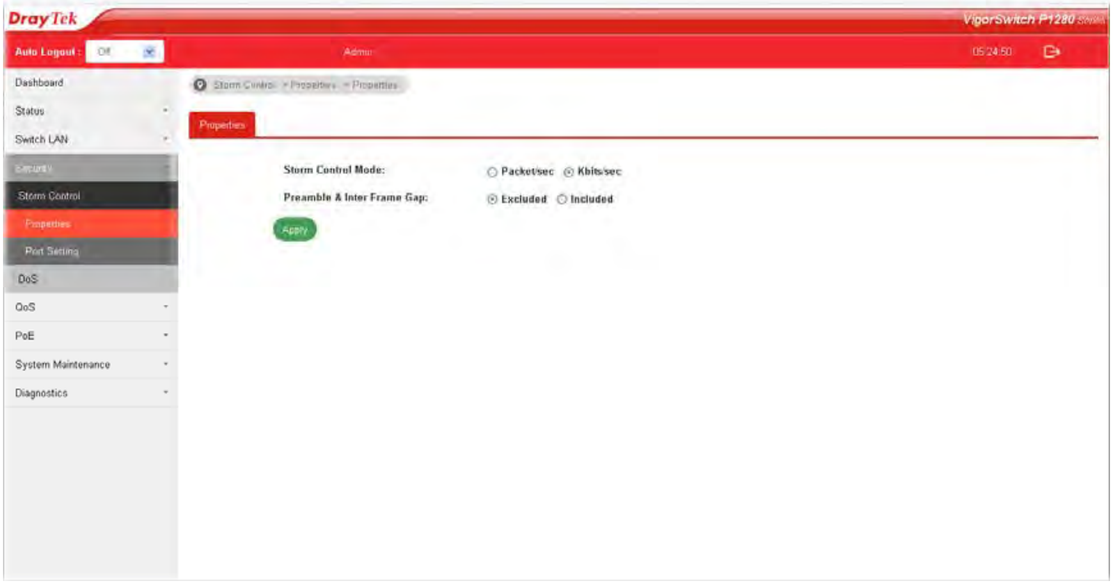
Part III Security

III-1 Storm Control

Storm Control helps to suppress possible broadcast, unknown multicast or unknown unicast storm by applying a rate limit on those packets.

III-1-1 Properties

This page allows a user to configure general settings for Storm Control.



Storm Control Mode: ○ Packet/sec ● Kbits/sec

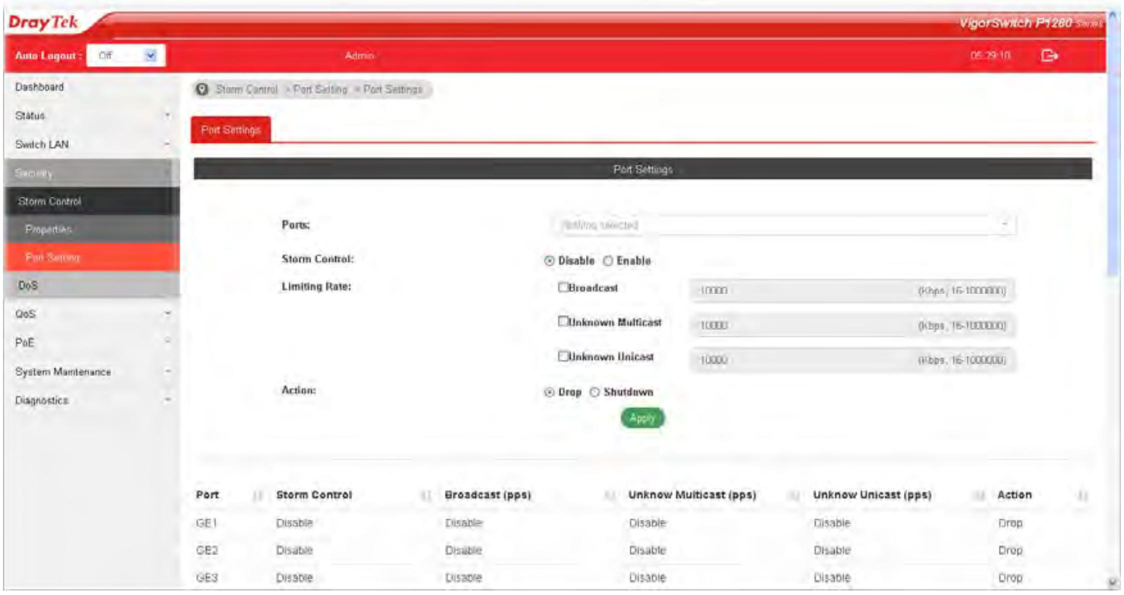
Preamble & Inter Frame Gap: ● Excluded ○ Included

Available settings are explained as follows:

Item	Description
Storm Control Mode	Select the mode of storm control. **Packet/sec** – Storm control rate will be calculated by packet-based. **Kbits/sec** - Storm control rate will be calculated by octet-based.
Preamble & Inter Frame Gap	Select the rate calculation with/without preamble & IFG (20 bytes). **Excluded** – Exclude preamble & IFG (20 bytes) when count ingress storm control rate. **Included** - Include preamble & IFG (20 bytes) when count ingress storm control rate.
Apply	Save the settings or changes to the switch.

III-1-2 Port Setting

This page is used to configure port settings for Storm Control. The configuration result for each port will be displayed on the table listed on the lower side of this web page.



Port Settings

Ports: Nothing selected

Storm Control: ● Disable ○ Enable

Limiting Rate:

- □ Broadcast 10000 (Kbps, 16-1000000)
- □ Unknown Multicast 10000 (Kbps, 16-1000000)
- □ Unknown Unicast 10000 (Kbps, 16-1000000)

Action: ● Drop ○ Shutdown

Port	Storm Control	Broadcast (pps)	Unknow Multicast (pps)	Unknow Unicast (pps)	Action
GE1	Disable	Disable	Disable	Disable	Drop
GE2	Disable	Disable	Disable	Disable	Drop
GE3	Disable	Disable	Disable	Disable	Drop

Available settings are explained as follows:

Item	Description
Ports	Use the drop down list to select the port profile (GE1 to GE28) or profiles.
Storm Control	**Disable** – Disable the storm control configuration for the selected port profile. **Enable** – Enable the storm control configuration for the selected port profile.
Limiting Rate	Check the box(es) to enable strom control rate limited for Broadcast, Unknown Multicast and/or Unknow Unicast packet. **Broadcast** – Specify the storm control rate for Broadcast packet. Value of storm control rate, Unit: Kbps (Kbits per-second). The range is from 16 to 1000000. **Unknown Multicast** – Specify the storm control rate for unknown multicast packet. Value of storm control rate, Unit: Kbps (Kbits per-second). The range is from 16 to 1000000. **Unknown Unicast** - Specify the storm control rate for unknown multicast packet. Value of storm control rate, Unit: Kbps (Kbits per-second). The range is from 16 to 1000000.
Action	Select the state of setting. **Drop** – Packets exceed storm control rate will be dropped. **Shutdown** - Port exceeds storm control rate will be shutdown.
Apply	Save the settings or changes to the switch.

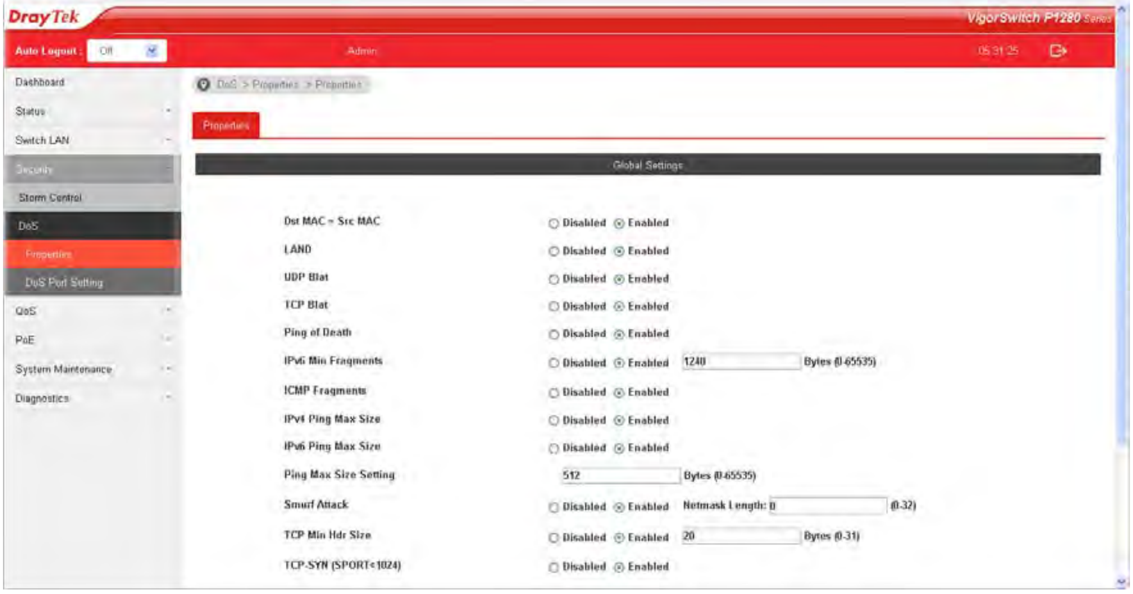
III-2 DoS

A Denial of Service (DoS) attack is a hacker attempt to make a device unavailable to its users. DoS attacks saturate the device with external communication requests, so that it cannot respond to legitimate traffic. These attacks usually lead to a device CPU overload.

The DoS protection feature is a set of predefined rules that protect the network from malicious attacks. The DoS Security Suite Setting enables activating the security suite.

III-2-1 Properties

This page allows a user to configure DoS setting to enable/disable DoS function for global setting.



Dst MAC = Src MAC ○ Disabled ● Enabled
LAND ○ Disabled ● Enabled
UDP Blat ○ Disabled ● Enabled
TCP Blat ○ Disabled ● Enabled
Ping of Death ○ Disabled ● Enabled
IPv6 Min Fragments ○ Disabled ● Enabled 1240 Bytes (0-65535)
ICMP Fragments ○ Disabled ● Enabled
IPv4 Ping Max Size ○ Disabled ● Enabled
IPv6 Ping Max Size ○ Disabled ● Enabled
Ping Max Size Setting 512 Bytes (0-65535)
Smurf Attack ○ Disabled ● Enabled Netmask Length: 0 (0-32)
TCP Min Hdr Size ○ Disabled ● Enabled 20 Bytes (0-31)
TCP-SYN (SPORT<1024) ○ Disabled ● Enabled

Available settings are explained as follows:

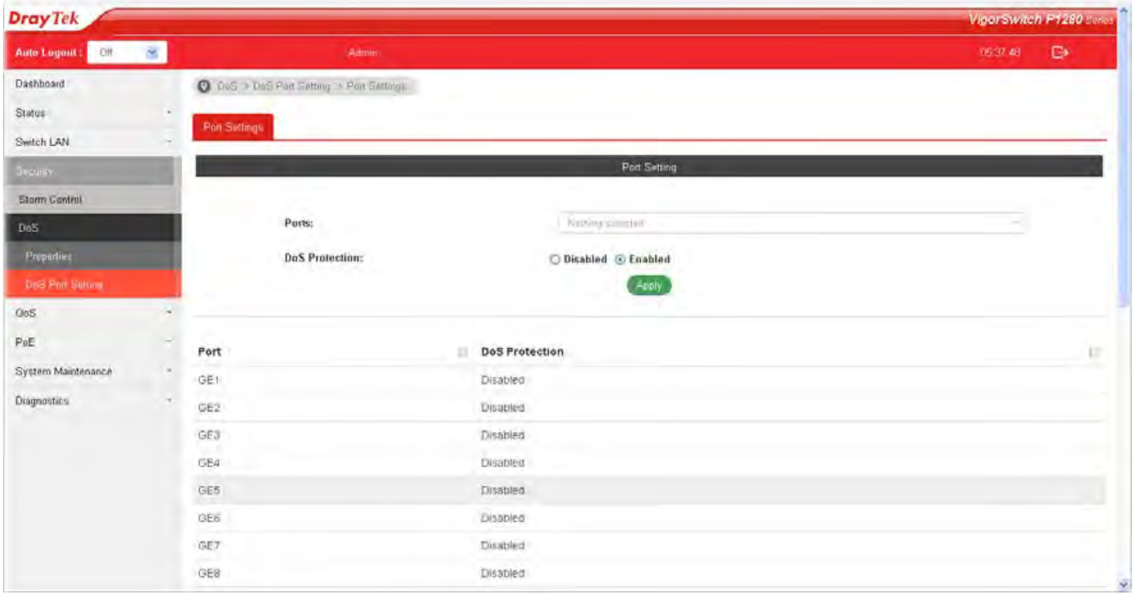
Item	Description
Dst MAC=Src MAC	Drop the packets if the destination MAC address is equal to the source MAC address. **Disabled** – Disable the item function. **Enabled** - Enable the item function.
LAND	Drop the packets if the source IP address is equal to the destination IP address. **Disabled** – Disable the item function. **Enabled** - Enable the item function.
UDP Blat	Drop the packets if the UDP source port equals to the UDP destination port. **Disabled** – Disable the item function. **Enabled** - Enable the item function.
TCP Blat	Drop the packages if the TCP source port is equal to the TCP destination port. **Disabled** – Disable the item function.

	Enabled - Enable the item function.
Ping of Death	Avoid ping of death attack. Ping packets that length are larger than 65535 bytes. **Disabled** – Disable the item function. **Enabled** - Enable the item function.
IPv6 Min Fragments	Check the minimum size of IPv6 fragments, and drop the packets smaller than the minimum size. The valid range is from 0 to 65535 bytes, and default value is 1240 bytes. **Disabled** – Disable the item function. **Enabled** - Enable the item function.
ICMP Fragments	Drop the fragmented ICMP packets. **Disabled** – Disable the item function. **Enabled** - Enable the item function.
IPv4 Ping Max Size	Determine the IPv4 PING packet with the length. **Disabled** – Disable the item function. **Enabled** - Enable the item function.-
IPv6 Ping Max Size	Determine the IPv6 PING packet with the length. **Disabled** – Disable the item function. **Enabled** - Enable the item function.
Ping Max Size Setting	Determine the IPv4/IPv6 PING packet with the length. Specify the maximum size of the ICMPv4/ICMPv6 ping packets. The valid range is from 0 to 65535 bytes, and the default value is 512 bytes.
Smurf Attack	Avoid smurf attack. The length range of the netmask is from 0 to 323 bytes, and default length is 0 byte. **Disabled** – Disable the item function. **Enabled** - Enable the item function.
TCP Min Hdr Size	Check the minimum TCP header and drops the TCP packets with the header smaller than the minimum size. The length range is from 0 to 31 bytes, and default length is 20 bytes. **Disabled** – Disable the item function. **Enabled** - Enable the item function.
TCP-SYN (SPORT<1024)	Drop SYN packets with sport less than 1024. **Disabled** – Disable the item function. **Enabled** - Enable the item function.
Null Scan Attack	Drop the packets with NULL scan. **Disabled** – Disable the item function. **Enabled** - Enable the item function.
X-mas Scan Attack	Drop the packets if the sequence number is zero, and the FIN, URG and PSH bits are set. **Disabled** – Disable the item function. **Enabled** - Enable the item function.
TCP SYN-FIN Attack	Drop the packets with SYN and FIN bits set. **Disabled** – Disable the item function. **Enabled** - Enable the item function.-
TCP SYN-RST Attack	Drop the packets with SYN and RST bits set. **Disabled** – Disable the item function.

	Enabled - Enable the item function.
TCP Fragment (Offset=1)	Drop the fragmented ICMP packets. **Disabled** – Disable the item function. **Enabled** - Enable the item function.
Apply	Save the settings or changes to the switch.

III-2-2 DoS Port Setting

This page allows a user to configure and display the state of DoS protection for interfaces. The configuration result for each port will be displayed on the table listed on the lower side of this web page.



Ports: Nothing selected

DoS Protection: ○ Disabled ● Enabled

Port	DoS Protection
GE1	Disabled
GE2	Disabled
GE3	Disabled
GE4	Disabled
GE5	Disabled
GE6	Disabled
GE7	Disabled
GE8	Disabled

Available settings are explained as follows:

Item	Description
Port	Use the drop down list to select the port profile (GE1 to GE28) or profiles.
DoS Protection	**Disabled** – Disable the function of DoS Protection. **Enabled** - Enable the function of DoS Protection.
Apply	Save the settings or changes to the switch.

Part IV QoS Configuration

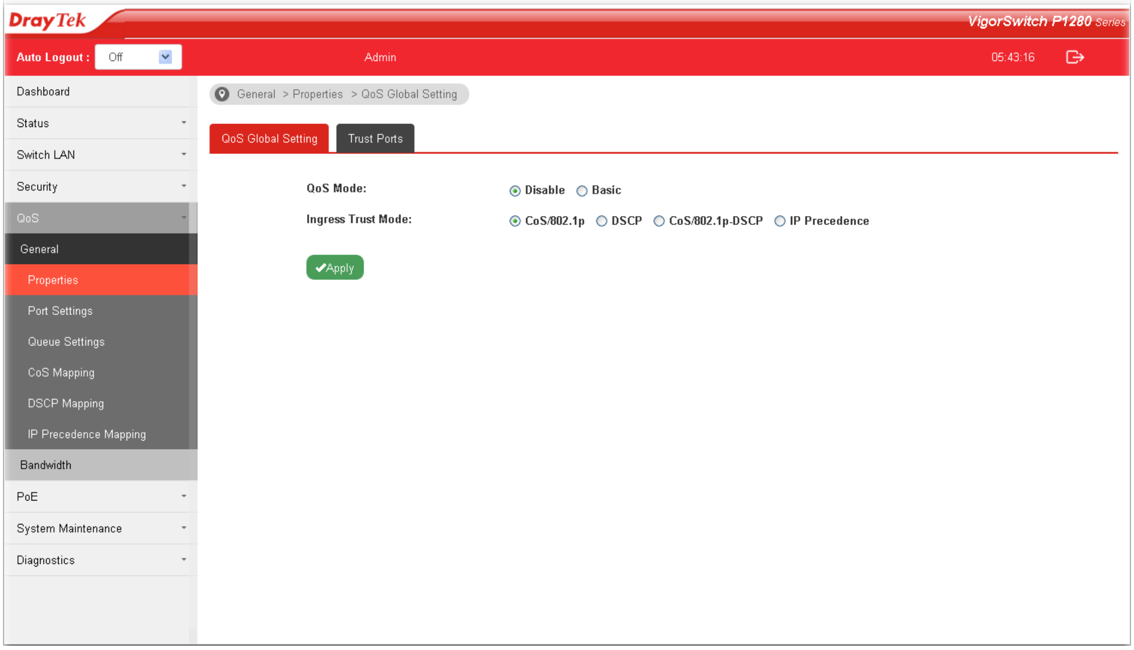
IV-1 General

QoS (Quality of Service) functions to provide different quality of service for various network applications and requirements and optimize the bandwidth resource distribution so as to provide a network service experience of a better quality.

IV-1-1 Properties

IV-1-1-1 QoS General Setting

This page is used to specify Ingress Trust Mode for basic QoS mode.



QoS Mode: ● Disable ○ Basic

Ingress Trust Mode: ● CoS/802.1p ○ DSCP ○ CoS/802.1p-DSCP ○ IP Precedence

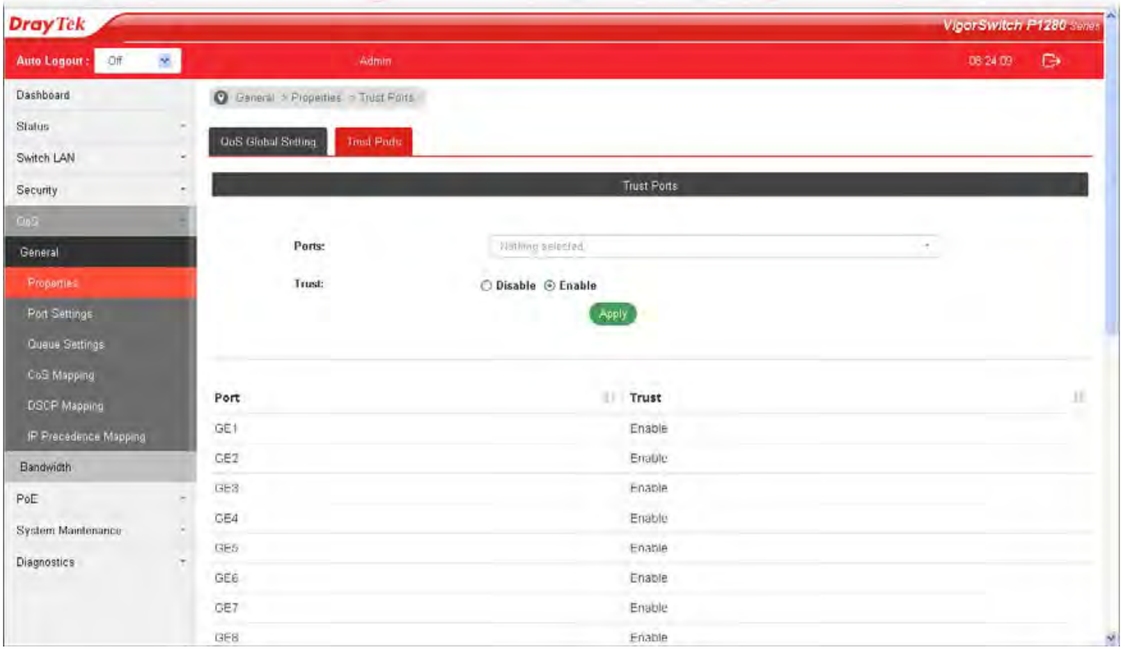
Available settings are explained as follows:

Item	Description
QoS Mode	**Disable** –Disable the function of QoS mode. **Basic** – Enable the function of QoS mode.
Ingress Trust Mode	Select the QoS operation mode. **CoS/802.1p** –Traffic is mapped to queues based on the CoS field in the VLAN tag, or based on the per-port default CoS value if there is no VLAN tag on the incoming packet. **DSCP** – All IP traffic is mapped to queues based on the DSCP field in the IP header. If traffic is not IP traffic, it is mapped to the lowest priority queue. **CoS/802.1p-DSCP** – All IP traffic is mapped to queues based on the DSCP field in the IP header. If traffic is not IP but has VLAN tag, mapped to queues based on the CoS value in the VLAN tag. **IP Precedence** - All IP traffic is mapped to queues based on the DSCP field in the IP header. If traffic is not IP but has VLAN tag, mapped to queues based on the CoS value in the VLAN tag.

Apply	Save the settings or changes to the switch.

IV-1-1-2 Trust Ports

This page is used to enable the trust mode of basic QoS on each port. Port that is trust disabled will be sent with lowest priority queue. The configuration result for each port will be displayed on the table listed on the lower side of this web page.



Trust Ports

Ports: Nothing selected

Trust: ○ Disable ● Enable

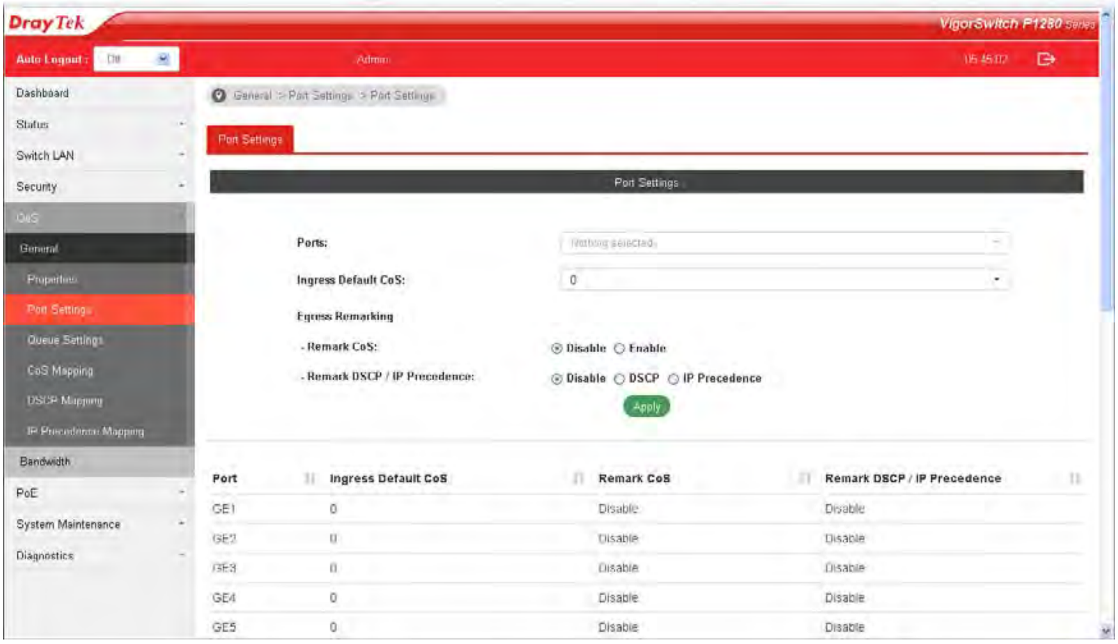
Port	Trust
GE1	Enable
GE2	Enable
GE3	Enable
GE4	Enable
GE5	Enable
GE6	Enable
GE7	Enable
GE8	Enable

Available settings are explained as follows:

Item	Description
Ports	Use the drop down list to select the port profile (GE1 to GE28) or profiles.
Trust	Click **Enable** to make traffic follow the trust mode in general setting. **Enable** - Traffic will follow trust mode in general setting. **Disable** – No QoS service for this port.
Apply	Save the settings or changes to the switch.

IV-1-2 Port Settings

This page is used to configure port settings for QoS. The configuration result for each port will be displayed on the table listed on the lower side of this web page.



Port Settings

Ports: Nothing selected.

Ingress Default CoS: 0

Egress Remarking

- Remark CoS: ● Disable ○ Enable
- Remark DSCP / IP Precedence: ● Disable ○ DSCP ○ IP Precedence

Port	Ingress Default CoS	Remark CoS	Remark DSCP / IP Precedence
GE1	0	Disable	Disable
GE2	0	Disable	Disable
GE3	0	Disable	Disable
GE4	0	Disable	Disable
GE5	0	Disable	Disable

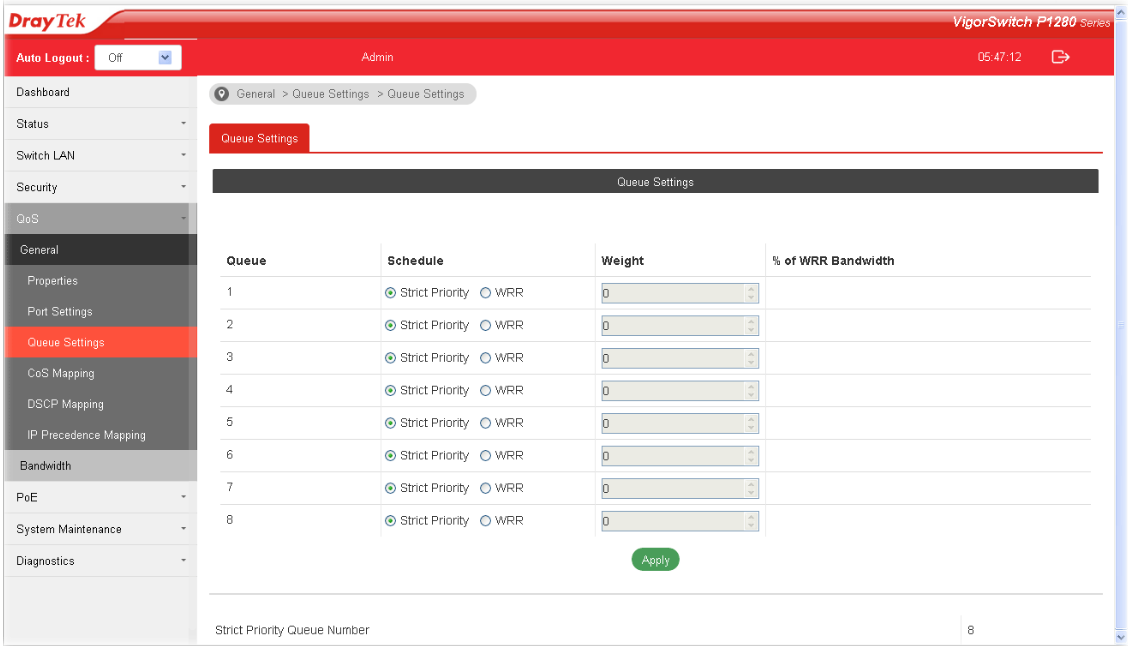
Available settings are explained as follows:

Item	Description
Ports	Use the drop down list to select the port profile (GE1 to GE28) or profiles.
Ingress Default CoS	Specify the default CoS priority value for those ingress frames without given trust QoS tag (802.1q/DSCP/IP Precedence, depending on configuration).
Engress Remarking	
Remark CoS	**Disable** – Disable CoS remarking function for outgoing packets. **Enable** - Egress traffic will be marked with CoS value according to the Queue to CoS mapping table.
Remark DSCP/IP Precedence	**Disable** – Disable DSCP/IP Precedence remarking function for outgoing packets. **DSCP** – Egress traffic will be marked with DSCP value according to the Queue to DSCP mapping table. **IP Precedence** - Egress traffic will be marked with IP Precedence value according to the Queue to IP Precedence mapping table.

IV-1-3 Queue Settings

VigorSwitch supports multiple queues for each interface. The higher numbered queue represents the higher priority. The following lists the types of supported priority queue:

- Strict Priority (SP) - Egress traffic from the higher priority queue will be transmitted first, lower priority queue shall wait until all traffic in SP queue is transmitted.
- Weighted Round Robin (WRR) - The number of packets sent from the queue is proportional to the weight of the queue.



Auto Logout : Off

Queue	Schedule	Weight	% of WRR Bandwidth
1	● Strict Priority ○ WRR	0	
2	● Strict Priority ○ WRR	0	
3	● Strict Priority ○ WRR	0	
4	● Strict Priority ○ WRR	0	
5	● Strict Priority ○ WRR	0	
6	● Strict Priority ○ WRR	0	
7	● Strict Priority ○ WRR	0	
8	● Strict Priority ○ WRR	0	

Strict Priority Queue Number 8

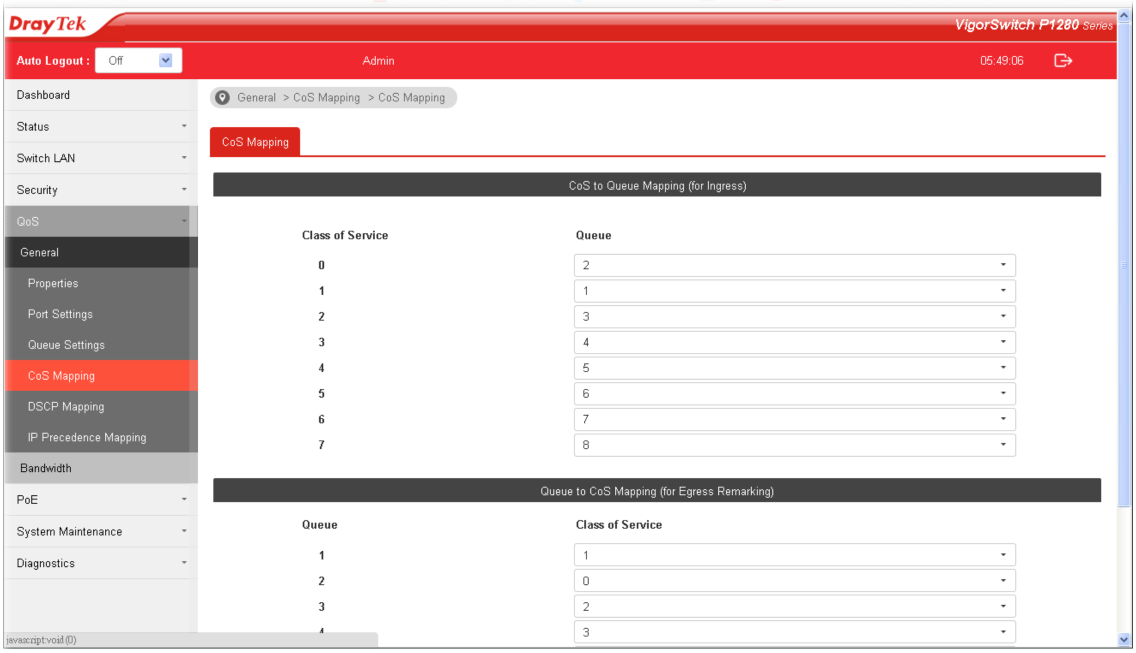
Available settings are explained as follows:

Item	Description
Queue	There are eight queue ID numbers allowed to be configured.
Schedule	**Strict Priority** – Click it to set queue to strict priority type. **WRR** – Click it to set queue to Weight round robin type.
Weight	If the queue type is WRR, set the queue weight for the queue.
% of WRR Bandwidth	Display the percentage of traffic which can be sent by current queue compared to total WRR queues.
Apply	Save the settings or changes to the switch.
Strict Priority Queue Number	Display the number of queues using Strict Priority method.

IV-1-4 CoS Mapping

This section allows user to configure how ingress frames with CoS/802.1p tag map to QoS queues, and QoS queues to CoS/802.1p on egress frames.

Actual effectiveness is based on how QoS is configured in previous QoS section. This page provides settings for user to configure mapping only.



CoS to Queue Mapping (for Ingress)

Class of Service	Queue
0	2
1	1
2	3
3	4
4	5
5	6
6	7
7	8

Queue to CoS Mapping (for Egress Remarking)

Queue	Class of Service
1	1
2	0
3	2
4	3

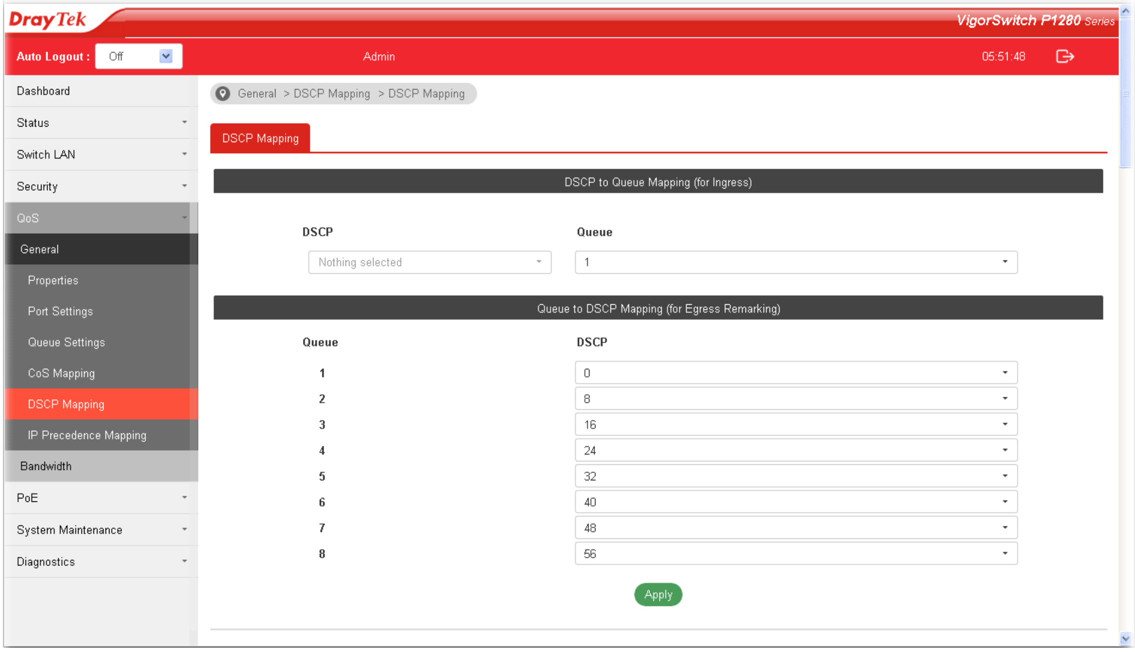
Available settings are explained as follows:

Item	Description
CoS to Queue Mapping (for Ingress) - Settings for incoming packets.	
Class of Service	Display the class of service value (0 to 7).
Queue	Define the queue ID (level 1 to 8) for different class of service values.
Queue to CoS Mapping (for Egress Remarking) - Settings for outgoing packets.	
Queue	Display the queue ID (level 1 to 8) for different class of service values.
Class of Service	Define the class of service value (0 to 7).
Apply	Save the settings or changes to the switch.

IV-1-5 DSCP Mapping

This section allows user to configure how ingress packets with DSCP tag map to QoS queues, and QoS queues to DSCP on egress packets.

Actual effectiveness is based on how QoS is configured in previous QoS section. This page provides settings for user to configure mapping only.



DSCP to Queue Mapping (for Ingress)

DSCP	Queue
Nothing selected	1

Queue to DSCP Mapping (for Egress Remarking)

Queue	DSCP
1	0
2	8
3	16
4	24
5	32
6	40
7	48
8	56

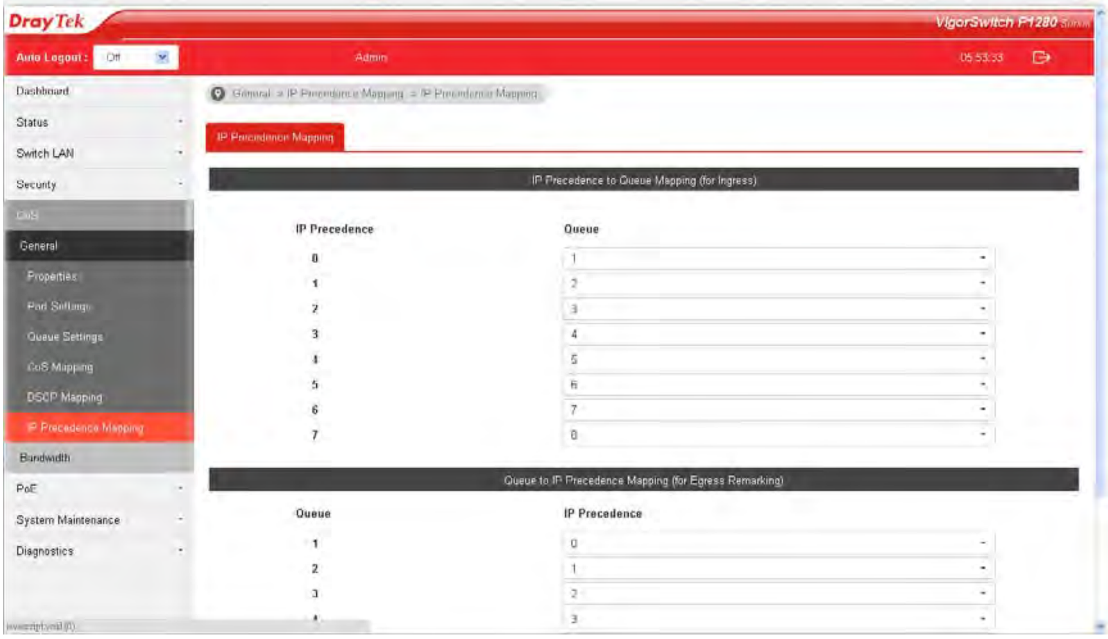
Available settings are explained as follows:

Item	Description
DSCP to Queue Mapping (for Ingress) - Settings for the incoming packets.	
DSCP	Display the DSCP value (0 to 7).
Queue	Define the queue ID (level 1 to 8) for different DSCP values.
Queue to DSCP Mapping (for Egress Remarking) - Settings for outgoing packets.	
Queue	Display the queue ID (level 1 to 8) for different DSCP values.
DSCP	Define the DSCP value (0 to 7).
Apply	Save the settings or changes to the switch.

IV-1-6 IP Precedence Mapping

This section allows user to configure how ingress packets with IP Precedence tag map to QoS queues, and QoS queues to IP Precedence on egress packets.

Actual effectiveness is based on how QoS is configured in previous QoS section. This page provides settings for user to configure mapping only.



IP Precedence to Queue Mapping (for Ingress)

IP Precedence	Queue
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

Queue to IP Precedence Mapping (for Egress Remarking)

Queue	IP Precedence
1	0
2	1
3	2
4	3

Available settings are explained as follows:

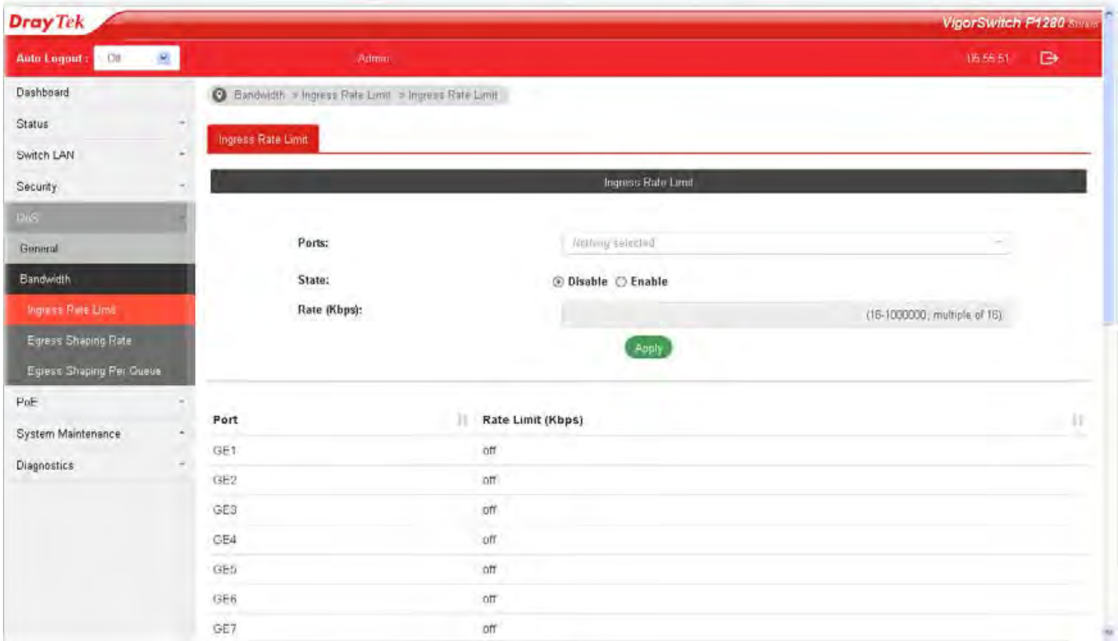
Item	Description
IP Precedence to Queue Mapping (for Ingress) - Settings for the incoming packets.	
IP Precedence	Display the IP Precedence value (0 to 7).
Queue	Define the queue ID (level 1 to 8) for different IP Precedence values.
Queue to IP Precedence Mapping (for Egress Remarking) - Settings for outgoing packets.	
Queue	Display the queue ID (level 1 to 8) for different IP Precedence values.
IP Precedence	Define the IP Precedence value (0 to 7).
Apply	Save the settings or changes to the switch.

IV-2 Bandwidth

Use the bandwidth setting pages to define values that determine how much traffic the switch can receive and send on specific port or queue.

IV-2-1 Ingress Rate Limit

This page allows a user to configure ingress port rate limit. The ingress rate limit is the number of bits per second that can be received from the ingress interface. Excess bandwidth above this limit is discarded. The configuration result for each port will be displayed on the table listed on the lower side of this web page.



Ports: Nothing selected

State: ● Disable ○ Enable

Rate (Kbps): (16-1000000, multiple of 16)

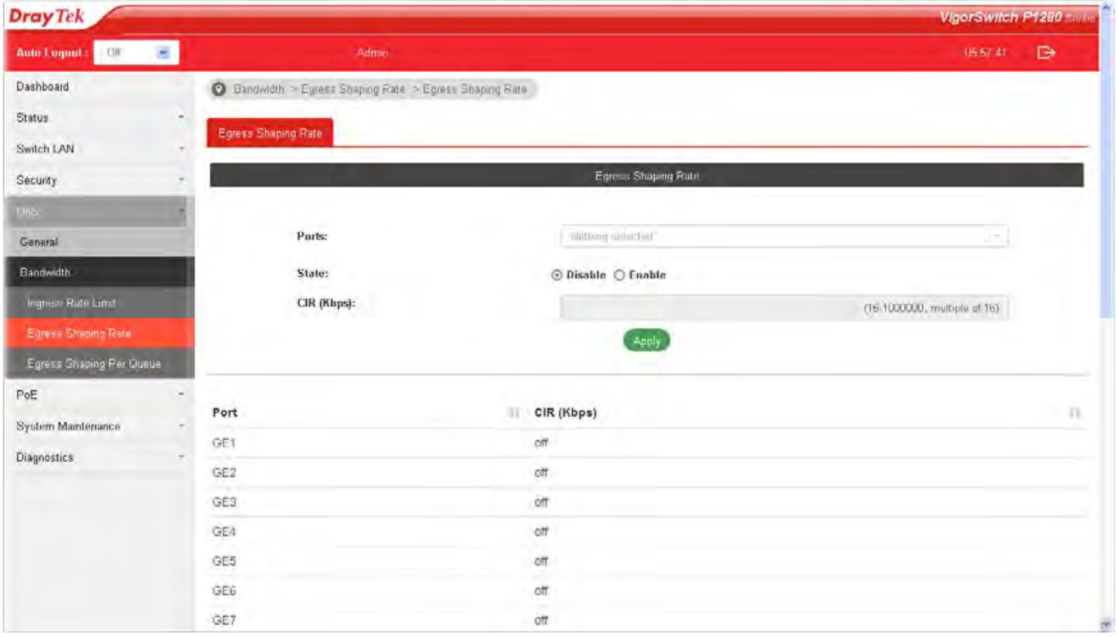
Port	Rate Limit (Kbps)
GE1	off
GE2	off
GE3	off
GE4	off
GE5	off
GE6	off
GE7	off

Available settings are explained as follows:

Item	Description
Ingress Rate Limit	
Ports	Use the drop down list to select the port profile (GE1 to GE28) or profiles.
State	**Disable** – Disable ingress bandwidth control. **Enable** - Enable ingress bandwidth control.
Rate (Kbps)	Enter the rate value,<16-1000000>,unit:16 Kbps.
Apply	Save the settings or changes to the switch.

IV-2-2 Egress Shaping Rate

This page allows a user to configure egress port rate limit. The egress rate limit is the number of bits per second that can be received from the egress interface. Excess bandwidth above this limit is discarded.



Egress Shaping Rate

Ports: Nothing selected

State: ● Disable ○ Enable

CIR (Kbps): (16-1000000, multiple of 16)

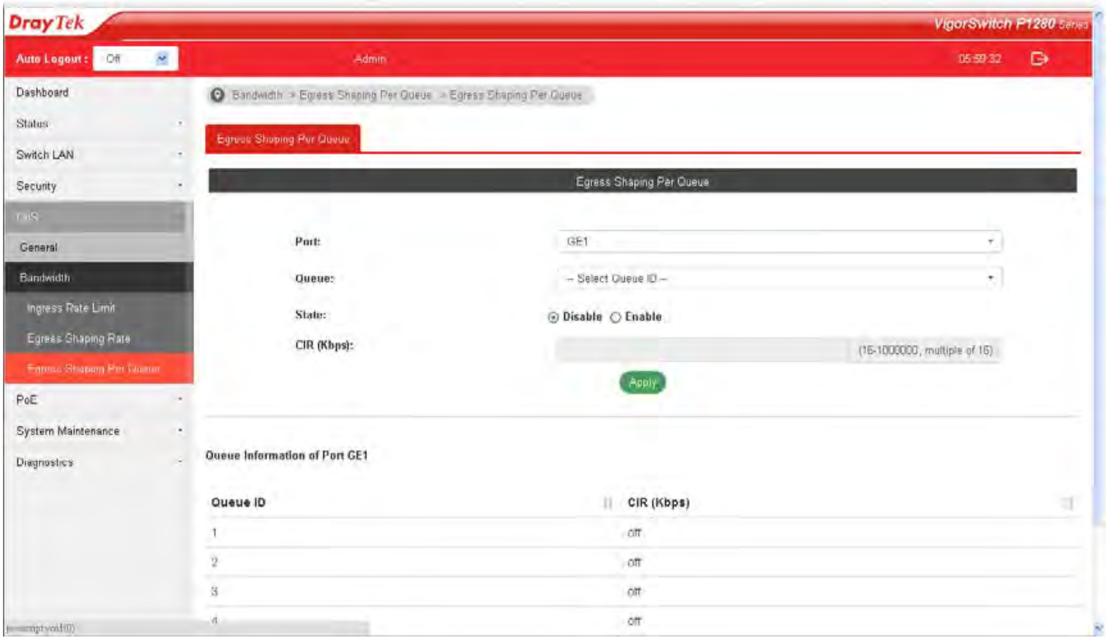
Port	CIR (Kbps)
GE1	off
GE2	off
GE3	off
GE4	off
GE5	off
GE6	off
GE7	off

Available settings are explained as follows:

Item	Description
Egress Shapping Rate	
Ports	Use the drop down list to select the port profile (GE1 to GE28) or profiles.
State	**Disable** – Disable egress bandwidth control. **Enable** - Enable egress bandwidth control.
CIR (Kbps)	Enter the rate value,<16-1000000>,unit:16 Kbps.
Apply	Save the settings or changes to the switch.

IV-2-3 Egress Shaping Per Queue

This page allows user to configure the maximum egress bandwidth not only by port but also by specific QoS queues. The configuration result for each port will be displayed on the table listed on the lower side of this web page.



Auto Logout : Off

Egress Shaping Per Queue

Port: GE1

Queue: -- Select Queue ID --

State: ● Disable ○ Enable

CIR (Kbps): (16-1000000, multiple of 16)

Queue Information of Port GE1

Queue ID	CIR (Kbps)
1	off
2	off
3	off
4	off

Available settings are explained as follows:

Item	Description
Egress Shapping Per Queue	
Port	Use the drop down list to select the port profile (GE1 to GE28) or profiles.
Queue	Use the drop down list to select queue number for the selected GE port.
State	**Disable** – Disable egress bandwidth control. **Enable** - Enable egress bandwidth control.
CIR (Kbps)	Enter the rate value,<16-1000000>,unit:16 Kbps.
Apply	Save the settings or changes to the switch.

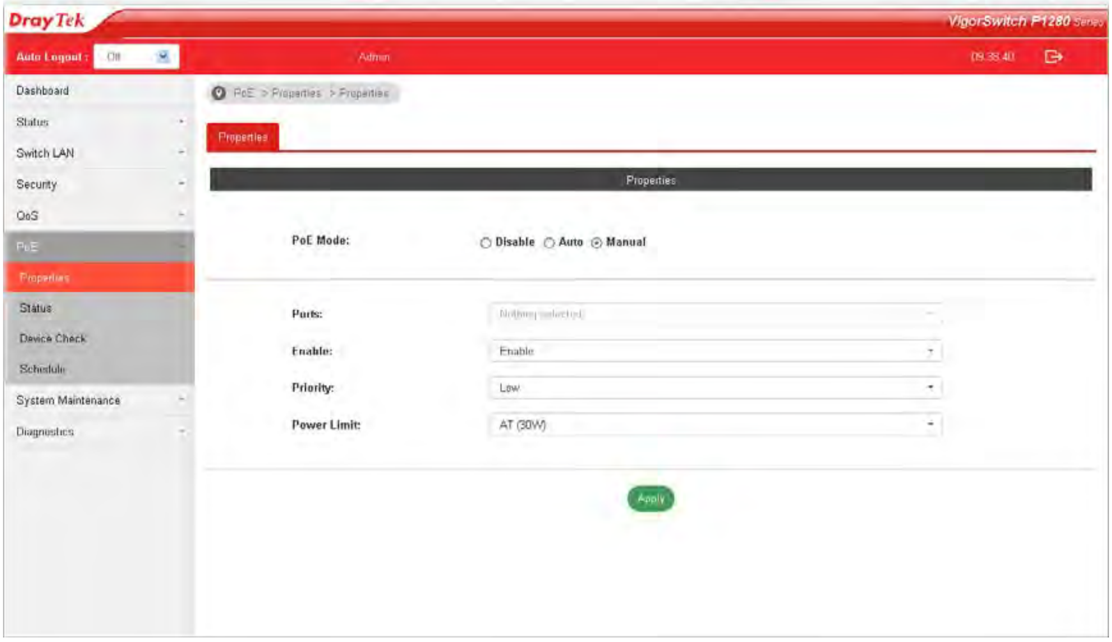
This page is left blank.

Part V PoE Configuration

V-1 Properties

This page allows a user to configure general settings for PoE and configure priority of each port for supplying PoE power. While maximum power budget is reached, power will be served starting with critical priority.

If the priority setting for all GE ports is configured as the same value (e.g., High); then, GE1 will have the highest priority to obtain PoE power in actual operation.



PoE Mode: ○ Disable ○ Auto ● Manual

Ports: Nothing selected

Enable: Enable

Priority: Low

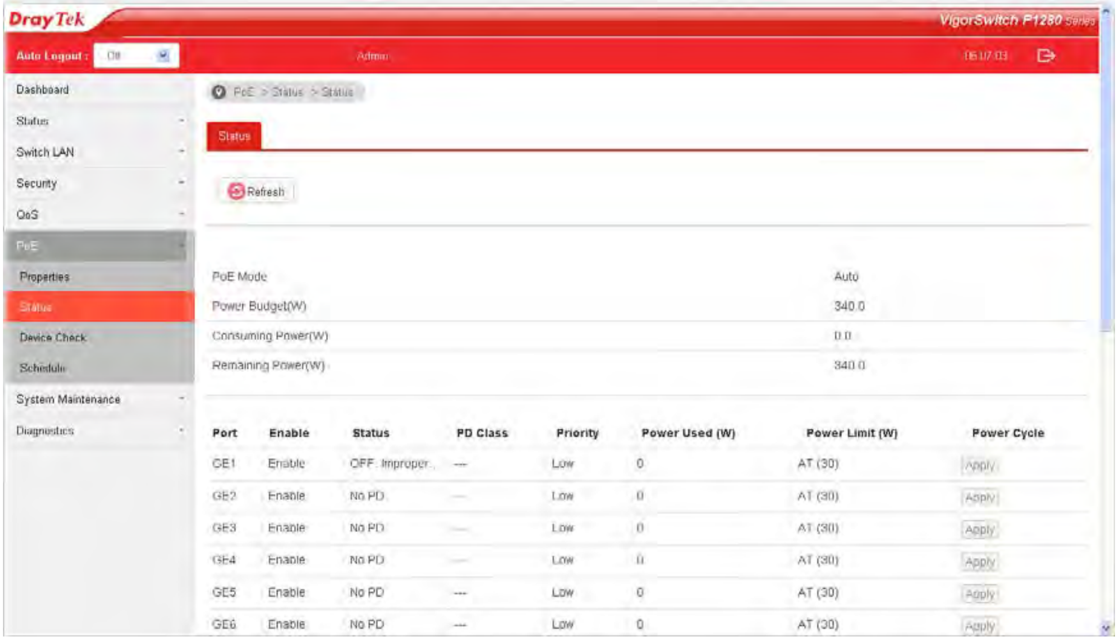
Power Limit: AT (30W)

Available settings are explained as follows:

Item	Description
PoE Mode	**Disable** – Disable the PoE function. **Auto** – Provides plug and play PoE function. PoE schedule and Power Limit are disabled in this mode. **Manual** – Before using **PoE>>Schedule**, set Manual as PoE mode.
Ports	Use the drop down list to select the port (GE1 to GE28) or ports for applying PoE configuration.
Enable	**Enable** – Make the selected ports be applied with PoE mode. **Disable** – Make the selected ports be not applied with PoE mode.
Priority	Select Priority for PoE device. **Low** –Set PoE device to low priority connection. **High** –Set PoE device to high priority connection. **Critical** - Set PoE device to highest priority connection.
Power Limit	This setting is available when Manual is selected as PoE Mode. Enter the value as the maximum limit of power given to each physical port.
Apply	Save the settings or changes to the switch.

V-2 Status

This page displays the current PoE status (configured in Properties, Device Check and Schedule) for each PoE port.



PoE Mode	Auto
Power Budget(W)	340.0
Consuming Power(W)	0.0
Remaining Power(W)	340.0

Port	Enable	Status	PD Class	Priority	Power Used (W)	Power Limit (W)	Power Cycle
GE1	Enable	OFF: Improper...	---	Low	0	AT (30)	Apply
GE2	Enable	No PD	---	Low	0	AT (30)	Apply
GE3	Enable	No PD	---	Low	0	AT (30)	Apply
GE4	Enable	No PD	---	Low	0	AT (30)	Apply
GE5	Enable	No PD	---	Low	0	AT (30)	Apply
GE6	Enable	No PD	---	Low	0	AT (30)	Apply

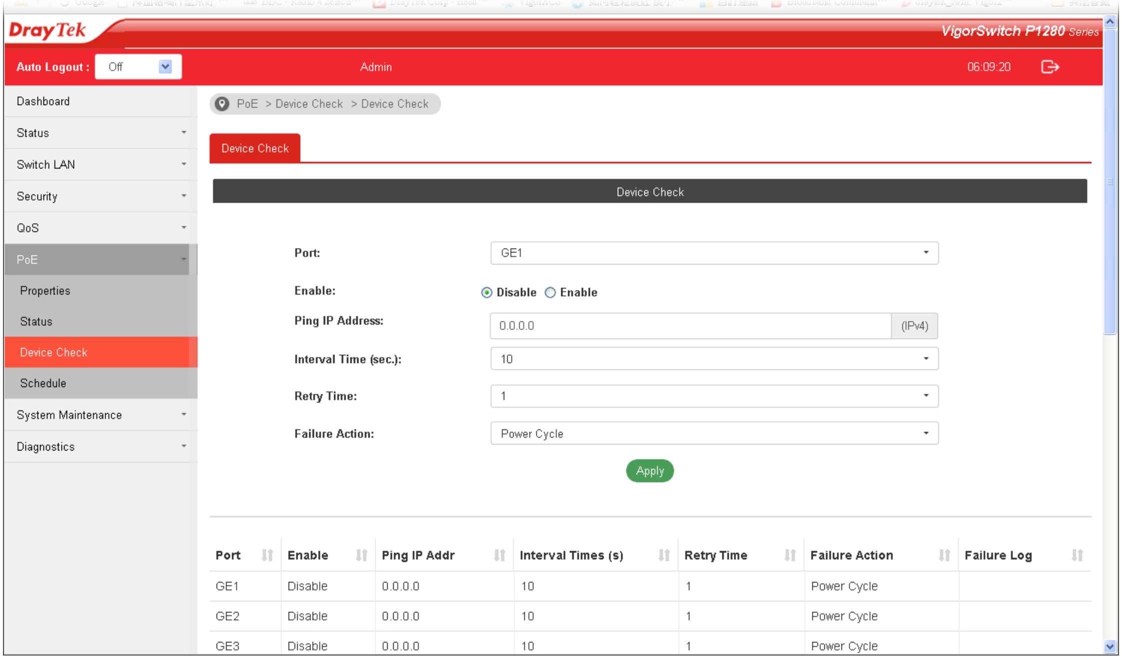
Available settings are explained as follows:

Item	Description
Refresh	Click it to refresh the status page.
PoE Mode	Display the PoE Mode (Manual, Auto or Disable) selected for the LAN port.
Power Budget(W)	Display the maximum power this switch can supply over PoE.
Consuming Power(W)	Display current power being consumed by all devices over PoE.
Remaining Power(W)	Display remaining power that can be supplied to additional devices over PoE.
Power Cycle	**Apply** – If PoE device connects to VigorSwitch, such button will be avaible for you to manually perform the cold boot for the PoE device by cycling the power supply.

V-3 Device Check

This page is used to configure device check of PoE PD devices. It can be applied to PoE PD devices connected directly, check ping echo status, and forcely reboot the device when meeting the preset health condition.

The configuration result for each port will be displayed on the table listed on the lower side of this web page.



Device Check

Port: GE1

Enable: ● Disable ○ Enable

Ping IP Address: 0.0.0.0 (IPv4)

Interval Time (sec.): 10

Retry Time: 1

Failure Action: Power Cycle

Apply

Port	Enable	Ping IP Addr	Interval Times (s)	Retry Time	Failure Action	Failure Log
GE1	Disable	0.0.0.0	10	1	Power Cycle	
GE2	Disable	0.0.0.0	10	1	Power Cycle	
GE3	Disable	0.0.0.0	10	1	Power Cycle	

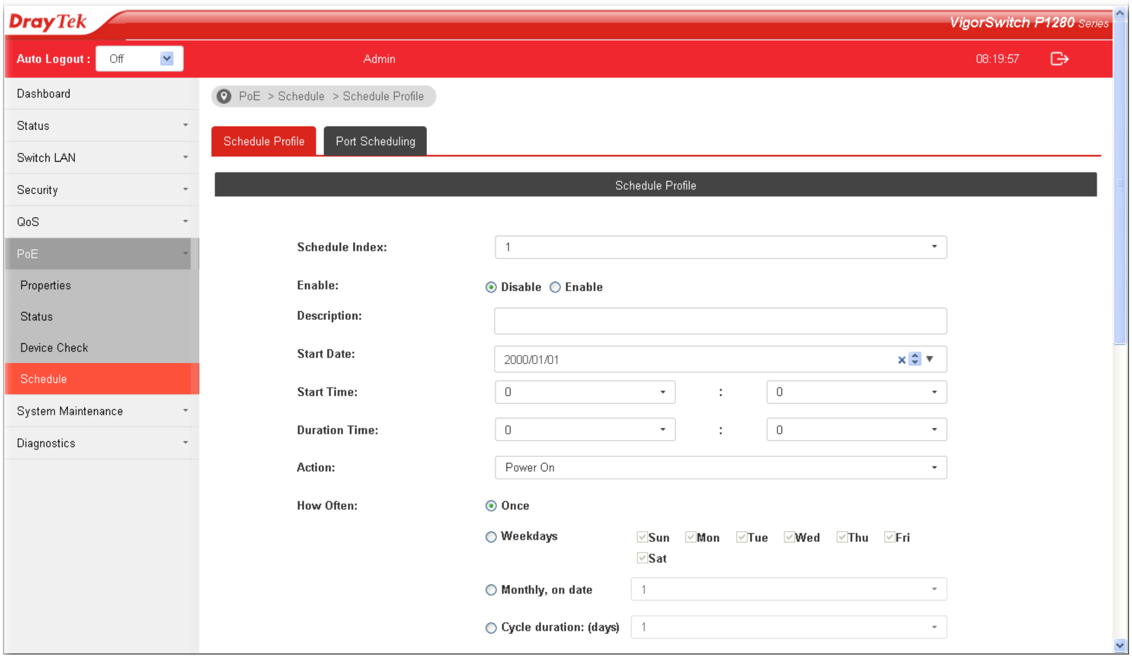
Available settings are explained as follows:

Item	Description
Port	Use the drop down list to select the port (GE1 to GE24) or ports for device check.
Enable	**Disable** – No PoE function for the selected GE port. **Enable** – PoE function will be enabled for the selected GE port.
Ping IP Address	Enter the IP address of the PoE device for check.
Interval Time (sec.)	The ping check will be performed every 10, 30, 60 or 120 seconds for the selected port (PoE device).
Retry Time	The system will perform the ping check the selected port (PoE device) for 1, 3 or 5 times.
Failure Action	Specify the action performed for PoE device when there is no number of retry time of echo from given IP address. **Power Cycle** – Forcely reboot the device by cycling the power given to PoE device. **Power Off** – The PoE divice will be powered off. **Nothing** – Log this event only, no action is taken on PoE device.
Apply	Save the settings or changes to the switch.

V-4 Schedule

V-4-1 Schedule Profile

This page allows users to configure maximum 15 PoE schedule rules.



Schedule Profile

Schedule Index: 1

Enable: ● Disable ○ Enable

Description:

Start Date: 2000/01/01

Start Time: 0 : 0

Duration Time: 0 : 0

Action: Power On

How Often: ● Once

○ Weekdays ☑Sun ☑Mon ☑Tue ☑Wed ☑Thu ☑Fri ☑Sat

○ Monthly, on date 1

○ Cycle duration: (days) 1

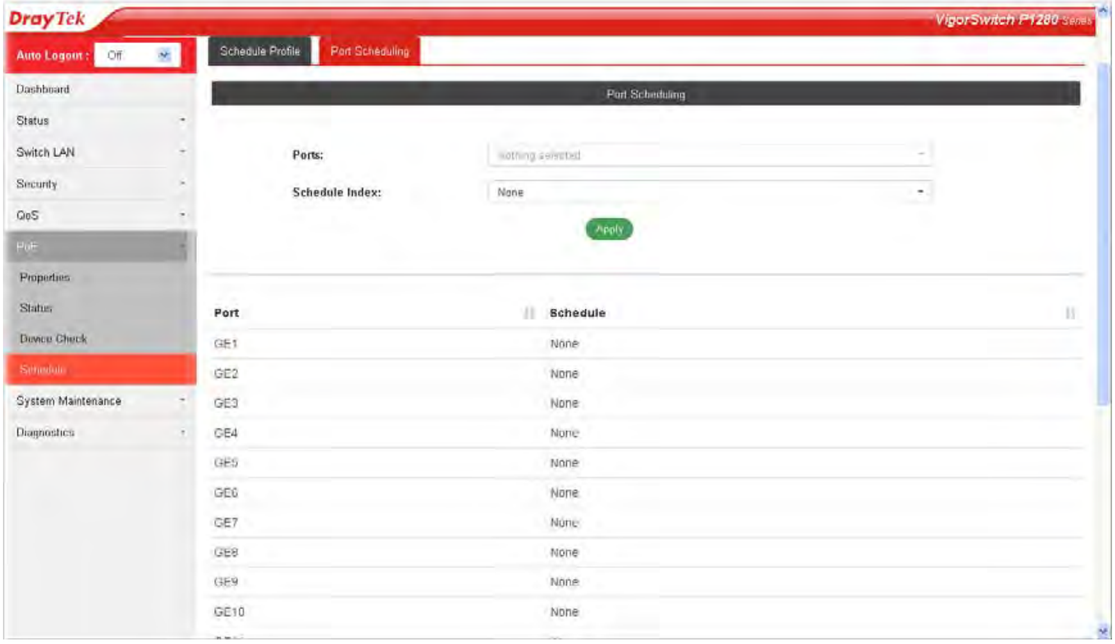
Available settings are explained as follows:

Item	Description
Schedule Index	Use the drop down list to choose one schedule profile.
Enable	**Disable** – The selected schedule profile will not take action but be saved for future use. **Enable** – The selected schedule profile will take action as configured.
Description	Enter a brief comment for such schedule.
Start Date	Specify the starting date of the schedule by choosing from a drop down calendar.
Start Time	Specify the starting time of the schedule by using the drop down list to specify the starting time (hours and minutes).
Duration Time	Define the time duration (hours and minutes).
Action	Specify which action should perform during the period of the schedule. **Power On** – PoE connection is always on. **Power Off** - PoE connection is always down.
How Often	Specify how often the schedule will be applied. **Once** – The schedule will be applied just once. **Weekdays** – Specify which days in one week should perform the schedule. **Monthly, on date** – Specify the day in a month as the starting

	point. **Cycle duration (days)** - The period of cycle duration is between 1 day and 31 days. For example, 7 means the whole cycle is 7 days; 20 means the whole cycle is 20 days. When the time is up, the PoE device will be turned on of off automatically.
Apply	Save the settings or changes to the switch.

V-4-2 Port Scheduling

This page is used to specify the PoE port for applying the schedule. The configuration result for each port will be displayed on the table listed on the lower side of this web page.



Port Scheduling

Ports: nothing selected

Schedule Index: None

Port	Schedule
GE1	None
GE2	None
GE3	None
GE4	None
GE5	None
GE6	None
GE7	None
GE8	None
GE9	None
GE10	None

Available settings are explained as follows:

Item	Description
Ports	Select the port or ports for applying the schedule.
Schedule Index	Use the drop down list to choose the schedule profile (from 1 to 15). After clicking **Apply**, the selected port(s) will be applied with the specified schedule.
Apply	Save the settings or changes to the switch.

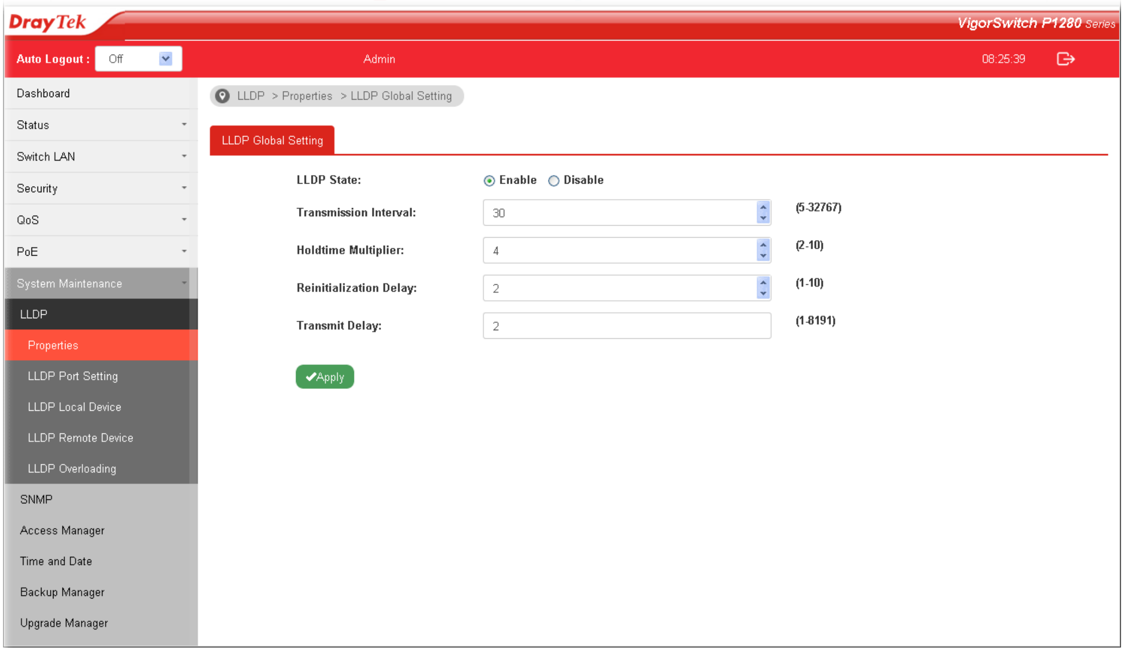
Part VI System Maintenance

VI-1 LLDP

LLDP is a one-way protocol; there are no request/response sequences. Information is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function. The LLDP category contains LLDP and LLDP-MED pages.

VI-1-1 Properties

This page allows a user to set general settings for LLDP.



LLDP State: ● Enable ○ Disable

Transmission Interval: 30 (5-32767)

Holdtime Multiplier: 4 (2-10)

Reinitialization Delay: 2 (1-10)

Transmit Delay: 2 (1-8191)

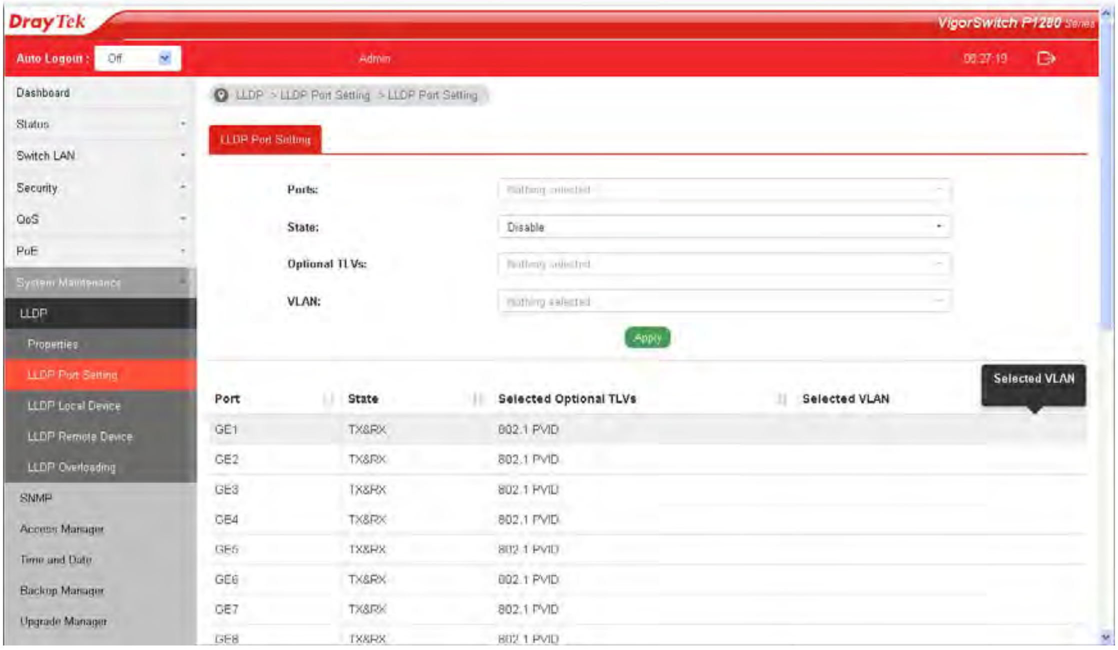
✓Apply

Available settings are explained as follows:

Item	Description
LLDP State	**Enable** – Enable LLDP protocol on this switch. **Disable** – Disable LLDP protocol on this switch.
Transmission Interval	Select the interval at which frames are transmitted. The default is 30 seconds, and the valid range is 5–32768seconds.
Holdtime Multiplier	Select the multiplier on the transmit interval to assign to TTL (range 2–10, default = 4).
Reinitialization Delay	Select the delay before a re-initialization (range 1–10 seconds, default = 2).
Transmit Delay	Select the delay after an LLDP frame is sent (range 1–8192 seconds, default = 3).
Apply	Save the settings or changes to the switch.

VI-1-2 LLDP Port Setting

This page allows a user to select specified port or all ports to configure LLDP state.



Ports: Nothing selected

State: Disable

Optional TLVs: Nothing selected

VLAN: Nothing selected

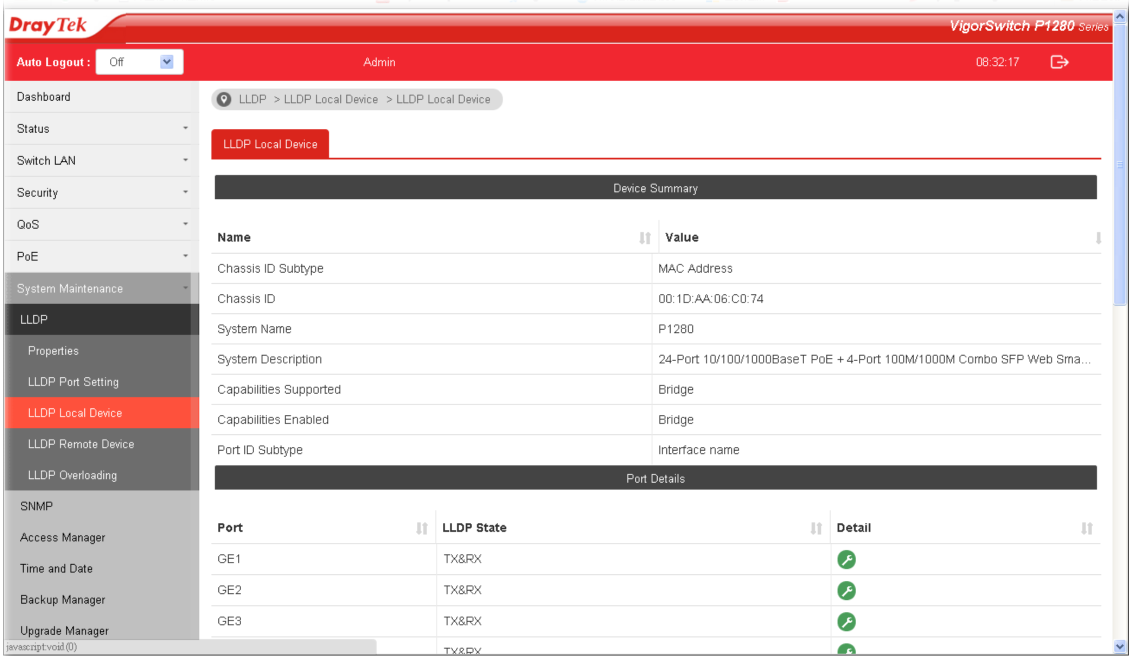
Port	State	Selected Optional TLVs	Selected VLAN
GE1	TX&RX	802.1 PVID	
GE2	TX&RX	802.1 PVID	
GE3	TX&RX	802.1 PVID	
GE4	TX&RX	802.1 PVID	
GE5	TX&RX	802.1 PVID	
GE6	TX&RX	802.1 PVID	
GE7	TX&RX	802.1 PVID	
GE8	TX&RX	802.1 PVID	

Available settings are explained as follows:

Item	Description
Ports	Use the drop down list to select the port (GE1 to GE28) or ports for device check.
State	**Disable** – Disable the transmission of LLDP PDUs. **TX&RX** – Transmit and receive LLDP PDUs both. **TX Only** – Transmit LLDP PDUs only. **RX Only** - Receive LLDP PDUs only.
Optional TLVs	Within data communication protocols, optional information may be encoded as a type-length-value or TLV element inside a protocol. TLV is also known as tag-length value. The type and length are fixed in size (typically 1-4 bytes), and the value field is of variable size. Select the LLDP optional TLVs to be carried (multiple selection is allowed). Available items include System Name, Port Description, System Description, System Capability, 802.3 MAC-PHY, 802.3 Link Aggregation, 802.3 Maximum Frame Size, Management Address and 802.1 PVID.
VLAN	Select the VLAN ID number to be performed (multiple selections are allowed).
Apply	Save the settings or changes to the switch.

VI-1-3 LLDP Local Device

This page displays information for LLDP Local Device.



Device Summary

Name	Value
Chassis ID Subtype	MAC Address
Chassis ID	00:1D:AA:06:C0:74
System Name	P1280
System Description	24-Port 10/100/1000BaseT PoE + 4-Port 100M/1000M Combo SFP Web Sma...
Capabilities Supported	Bridge
Capabilities Enabled	Bridge
Port ID Subtype	Interface name

Port Details

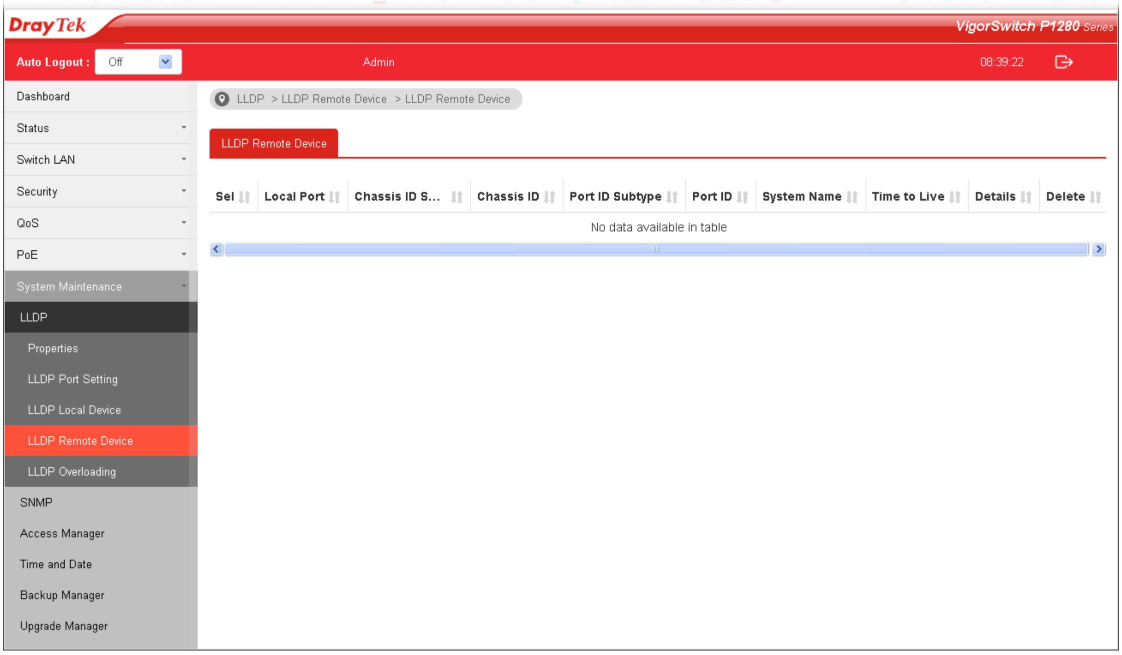
Port	LLDP State	Detail
GE1	TX&RX	🔧
GE2	TX&RX	🔧
GE3	TX&RX	🔧
	TX&RX	

Available settings are explained as follows:

Item	Description
Device Summary	Display a summary of the LLDP information for this switch. **Chassis ID Subtype -** Display the type of chassis ID, such as the MAC address. **Chassis ID -** Display Identifier of chassis. Where the chassis ID subtype is a MAC address, the MAC address of the switch is displayed. **System Name -** Display model name of switch. **System Description -** Display description of switch. **Capabilities Supported -** Display the primary functions of the device, such as Bridge, WLAN AP, or Router. **Capabilities Enabled -** Primary enabled functions of the device. **Port ID Subtype -** Display the type of the port identifier that is shown.
Port Details	Display detailed information of the selected GE port. **Detail** - Click it to review the detailed information contained in TLVs sent out from each interface, containing MAC/PHY, 802.3, 802.3 Link Aggregation, 802.1 VLAN and Protocol for each LAN port (GE1 to GE28).

VI-1-4 LLDP Remote Device

This page is used to view the information sent from neighboring devices by LLDP protocol.



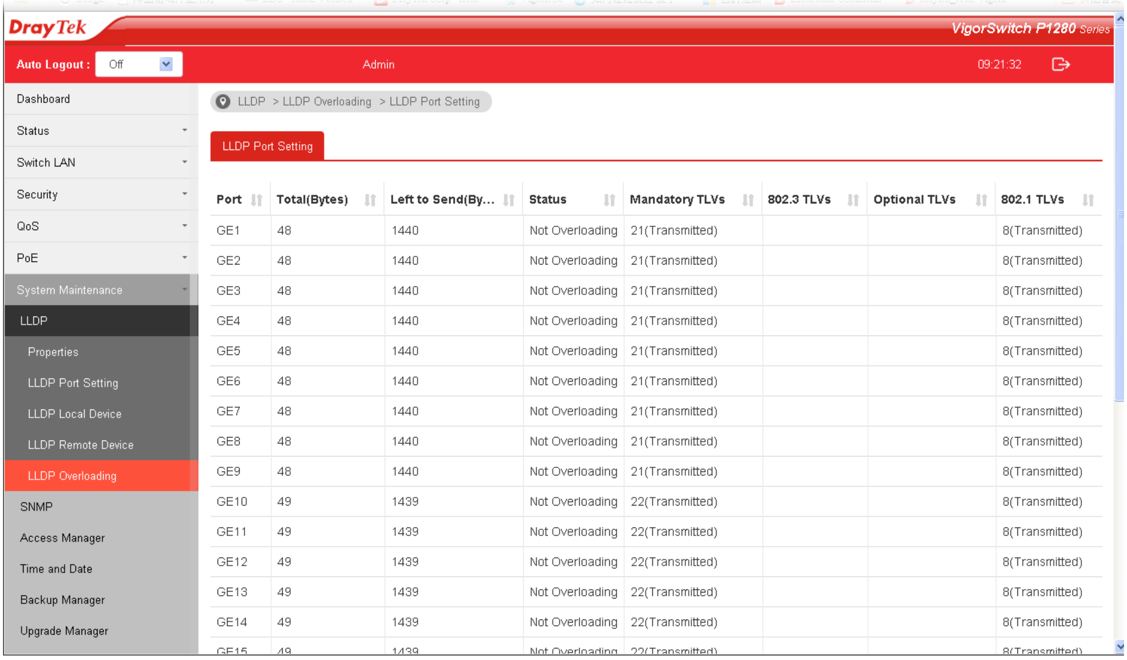
Sel	Local Port	Chassis ID S...	Chassis ID	Port ID Subtype	Port ID	System Name	Time to Live	Details	Delete
No data available in table									

Available settings are explained as follows:

Item	Description
Local Port	Display the number of the local port to which the neighbor is connected.
Chassis ID Subtype	Display the type of chassis ID (for example, MAC address).
Chassis ID	Display the identifier of the 802 LAN neighboring device's chassis.
Port ID Subtype	Display the type of port identifier.
Port ID	Display the number of port identifier.
System Name	Display the name of the switch.
Time to Live	Display the time interval in seconds after which the information for remote device will be deleted.
Details	Display detailed information contained in TLVs sent out from neighboring devices.
Delete	Click it to remove information of the selected port.

VI-1-5 LLDP Overloading

This page allows user to review current size, overall size of LLDP packet and whether it is to exceed maximum allowed size of single LLDP packet.



Port	Total(Bytes)	Left to Send(By...	Status	Mandatory TLVs	802.3 TLVs	Optional TLVs	802.1 TLVs
GE1	48	1440	Not Overloading	21(Transmitted)			8(Transmitted)
GE2	48	1440	Not Overloading	21(Transmitted)			8(Transmitted)
GE3	48	1440	Not Overloading	21(Transmitted)			8(Transmitted)
GE4	48	1440	Not Overloading	21(Transmitted)			8(Transmitted)
GE5	48	1440	Not Overloading	21(Transmitted)			8(Transmitted)
GE6	48	1440	Not Overloading	21(Transmitted)			8(Transmitted)
GE7	48	1440	Not Overloading	21(Transmitted)			8(Transmitted)
GE8	48	1440	Not Overloading	21(Transmitted)			8(Transmitted)
GE9	48	1440	Not Overloading	21(Transmitted)			8(Transmitted)
GE10	49	1439	Not Overloading	22(Transmitted)			8(Transmitted)
GE11	49	1439	Not Overloading	22(Transmitted)			8(Transmitted)
GE12	49	1439	Not Overloading	22(Transmitted)			8(Transmitted)
GE13	49	1439	Not Overloading	22(Transmitted)			8(Transmitted)
GE14	49	1439	Not Overloading	22(Transmitted)			8(Transmitted)
GE15	49	1439	Not Overloading	22(Transmitted)			8(Transmitted)

Available settings are explained as follows:

Item	Description
Port	Display the name of the port.
Total(Bytes)	Display the total number of bytes of LLDP information in each packet.
Left to Send(By..)	Display the total number of available bytes left for additional LLDP information in each packet.
Status	Display if LLDP TLVs has overloaded the PDU maximum size or not.
Mandatory TLVs	Display how many bytes used by mandatory TLVs.
802.3 TLVs	Display how many bytes used by 802.3 TLVs.
Optional TLVs	Displays how many bytes used by optional TLVs.
802.1 TLVs	Displays how many bytes used by 802.1 TLVs.

VI-2 SNMP

Simple Network Management Protocol (SNMP) is an "Internet-standard protocol for managing devices on IP networks". Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more.

SNMP is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

An SNMP-managed network consists of three key components:

- Managed device
- Agent - software which runs on managed devices
- Network management station (NMS) - software which runs on the manager

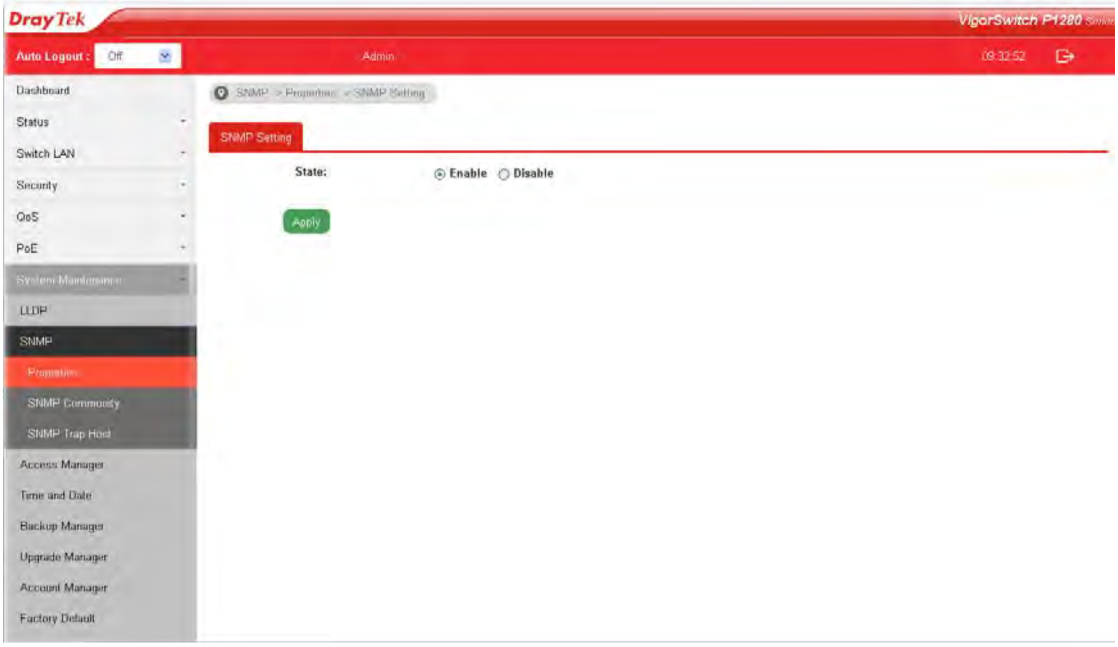
A managed device is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional (read and write) access to node-specific information. Managed devices exchange node-specific information with the NMSs. Sometimes called network elements, the managed devices can be any type of device, including, but not limited to, routers, access servers, switches, bridges, hubs, IP telephones, IP video cameras, computer hosts, and printers.

An agent is a network-management software module that resides on a managed device. An agent has local knowledge of management information and translates that information to or from an SNMP-specific form.

A network management station (NMS) executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs may exist on any managed network.

VI-2-1 Properties

This page allows a user to enable the function of SNMP for VigorSwitch.



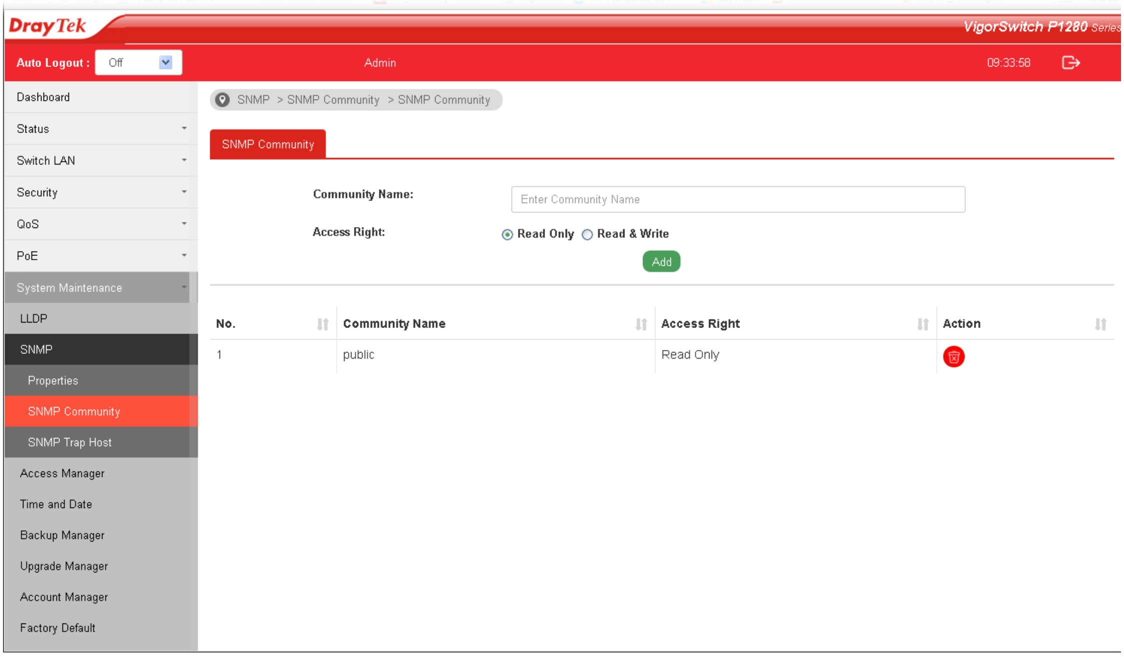
State: ● Enable ○ Disable

Available settings are explained as follows:

Item	Description
State	**Enable** – Enable the function of SNMP. **Disable** – Disable the function of SNMP.
Apply	Save the settings or changes to the switch.

VI-2-2 SNMP Community

This page allows a user to add/remove multiple communities of SNMP.



Community Name: Enter Community Name

Access Right: ● Read Only ○ Read & Write

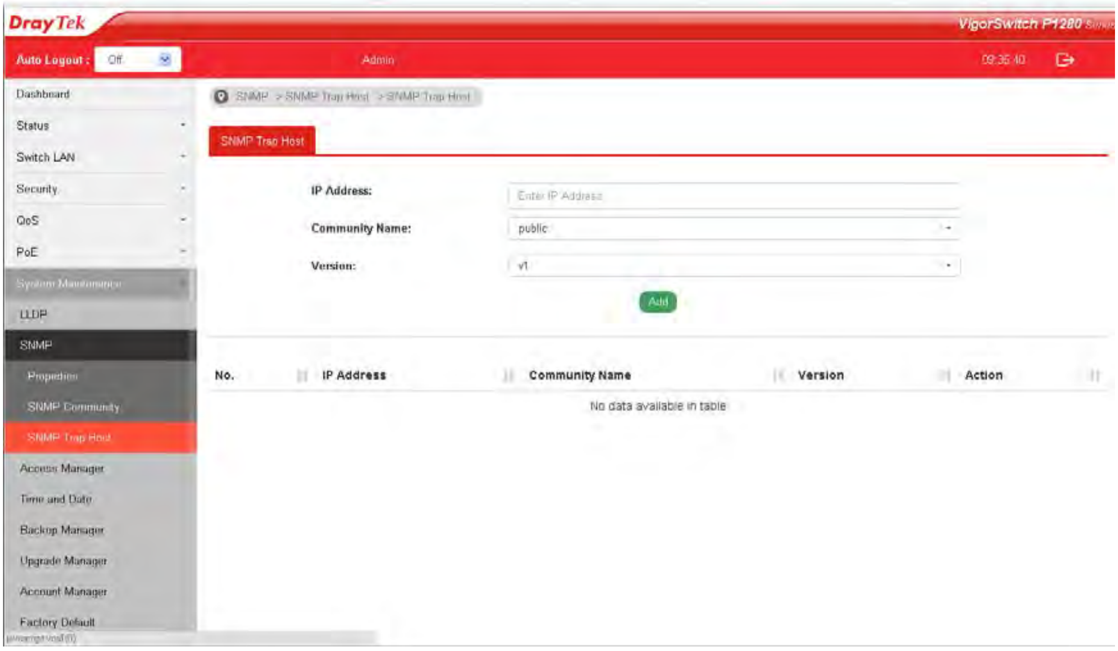
No.	Community Name	Access Right	Action
1	public	Read Only	🗑

Available settings are explained as follows:

Item	Description
Community Name	Enter a name as community name. The maximum length of the text is limited to 23 characters.
Access Right	**Read Only** – It allows unidirectional access to node-specific information. **Read & Write** - It allows bidirectional access to node-specific information.
Add	Click it to add a new community.
Action	**Delete** – Remove the selectd community strings.

VI-2-3 SNMP Trap Host

This page allows user to register where the SNMP agent should send trap to when triggered.



IP Address: Enter IP Address

Community Name: public

Version: v1

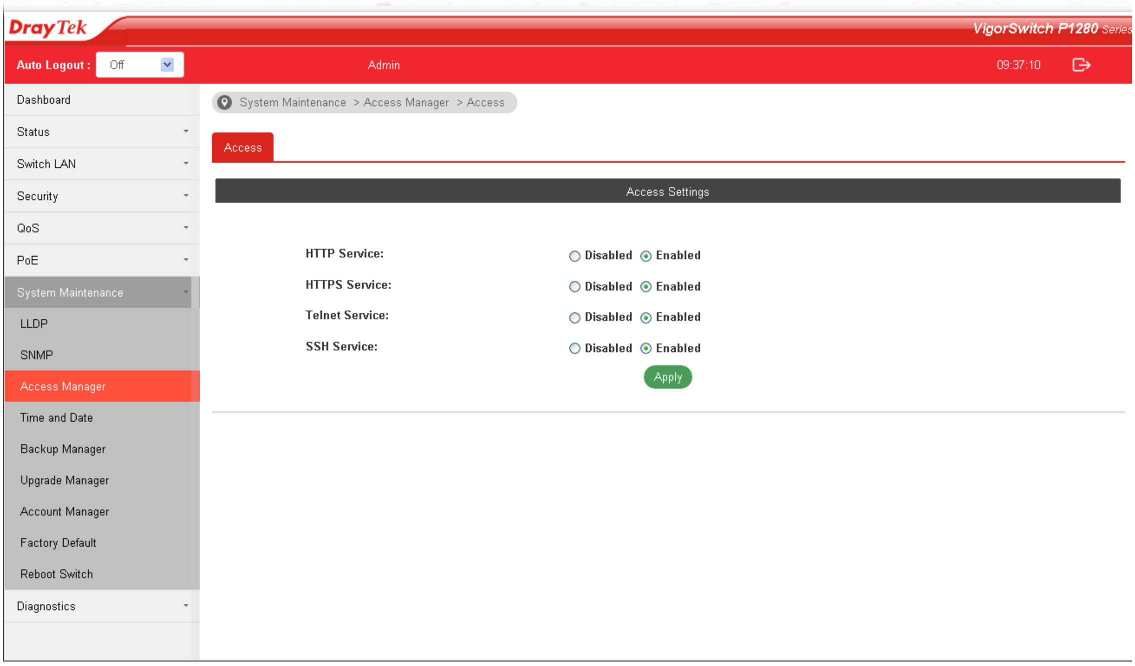
No.	IP Address	Community Name	Version	Action
No data available in table				

Available settings are explained as follows:

Item	Description
IP Address	Enter IPv4 address to receive the trap notification.
Community Name	Use the drop down list to select one existed community name for notification.
Version	Specify SNMP notification version. **v1 or v2c** – Specify the SNMP Version 1 notification or SNMP Version 2 notification.
Add	Click it to add a new community.
Action	**Delete** – Remove the selected community strings.

VI-3 Access Manager

This page allows users to control availability of management services such as HTTP, HTTPS, Telent and SSH.



HTTP Service: ○ Disabled ● Enabled

HTTPS Service: ○ Disabled ● Enabled

Telnet Service: ○ Disabled ● Enabled

SSH Service: ○ Disabled ● Enabled

Apply

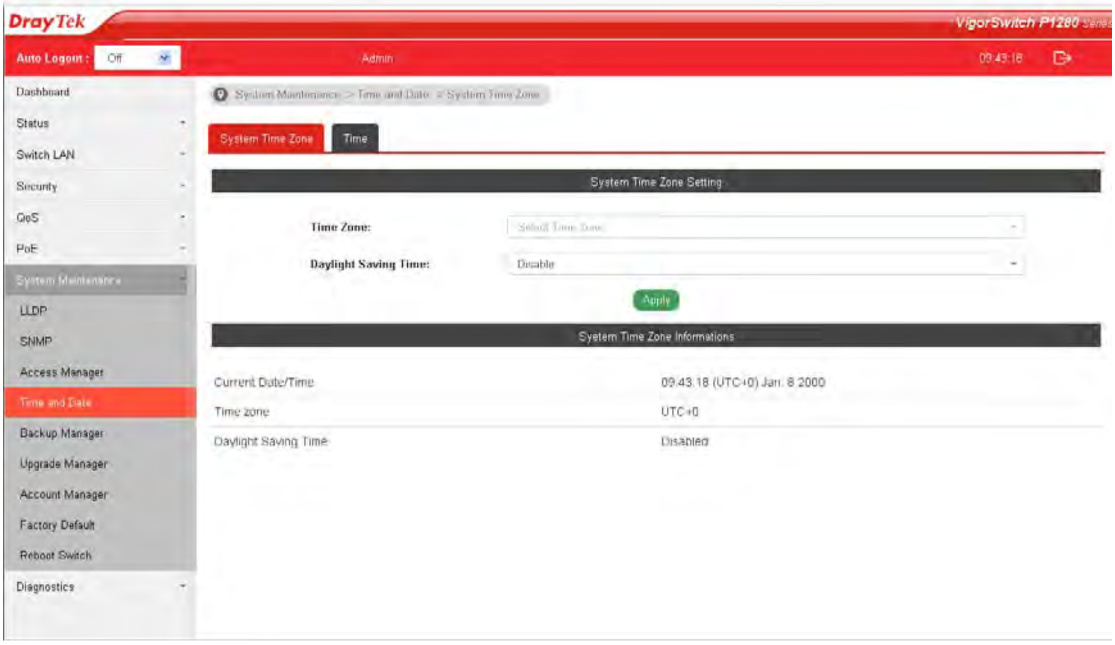
Available settings are explained as follows:

Item	Description
HTTP Service	HTTP is the acronym of HyperText Transfer Protocol. **Enabled** –Click it to enable HTTP service.
HTTPS Service	HTTPS is the acronym of Hypertext Transfer Protocol over Secure Socket Layer. **Enabled** - Click it to enable HTTPS service.
Telnet Service	Telnet is the TCP/IP standard protocol for remote terminal service. TELNET allows a user at one site to interact with a remote timesharing system at another site as if the user's keyboard and display connected directly to the remote machine. **Disabled** – Click it for not accessing telnet service. **Enabled** – Click it to access telnet service.
SSH Service	**Enabled** – Enable SSH service.
Apply	Save the settings or changes to the switch.

VI-4 Time and Date

VI-4-1 System Time Zone

This page allows a user to specify where the time of VigorSwitch should be inquired from.



System Time Zone Setting

Time Zone: Select Time Zone

Daylight Saving Time: Disable

System Time Zone Informations

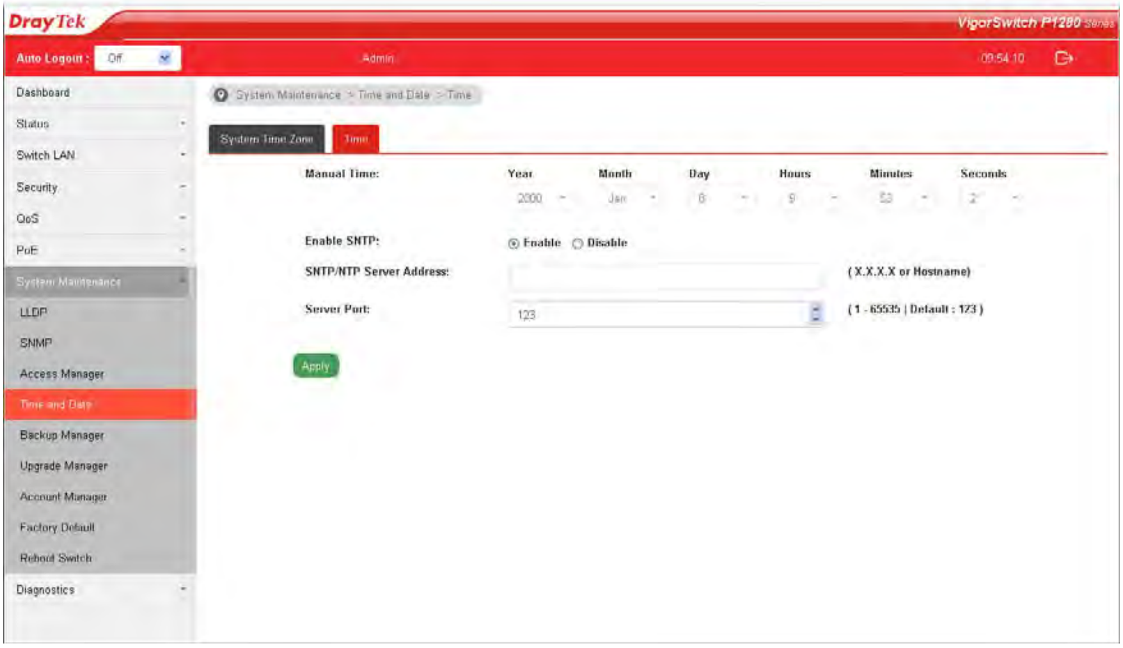
Current Date/Time	09:43:18 (UTC+0) Jan. 8 2000
Time zone	UTC+0
Daylight Saving Time	Disabled

Available settings are explained as follows:

Item	Description
System Time Zone Setting	
Time Zone	Use the drop down menu to select a time zone that VigorSwitch is located.
Daylight Saving Time	Select the mode of daylight saving time. **Disable** –Disable daylight saving time. **Recurring** - Using recurring mode of daylight saving time. **Non-Recurring** – Using non-recurring mode of daylight saving time. **USA** –Using daylight saving time in the United States that starts on the second Sunday of March and ends on the first Sunday of November. **European** - Using daylight saving time in the Europe that starts on the last Sunday.
Daylight Saving Time Offse	It is available when **Recurring** is selected as Daylight Saving Time. Specify the adjust offset of daylight saving time.
Recurring From / To	It is available when **Recurring** is selected as Daylight Saving Time. **From** - Specify the starting time of recurring daylight saving

	time. **To** - Specify the ending time of recurring daylight saving time.
Non-recurring From / To	It is available when **Non-Recurring** is selected as Daylight Saving Time. **From** - Specify the starting time of non-recurring daylight saving time. **To** - Specify the ending time of recurring daylight saving time.
Apply	Save the settings or changes to the switch.
System Time Zone Informations	Display the status of system time zone.

VI-4-2 Time



Manual Time: Year 2000 Month Jan Day 6 Hours 9 Minutes 53 Seconds 2

Enable SNTP: ● Enable ○ Disable

SNTP/NTP Server Address: (X.X.X.X or Hostname)

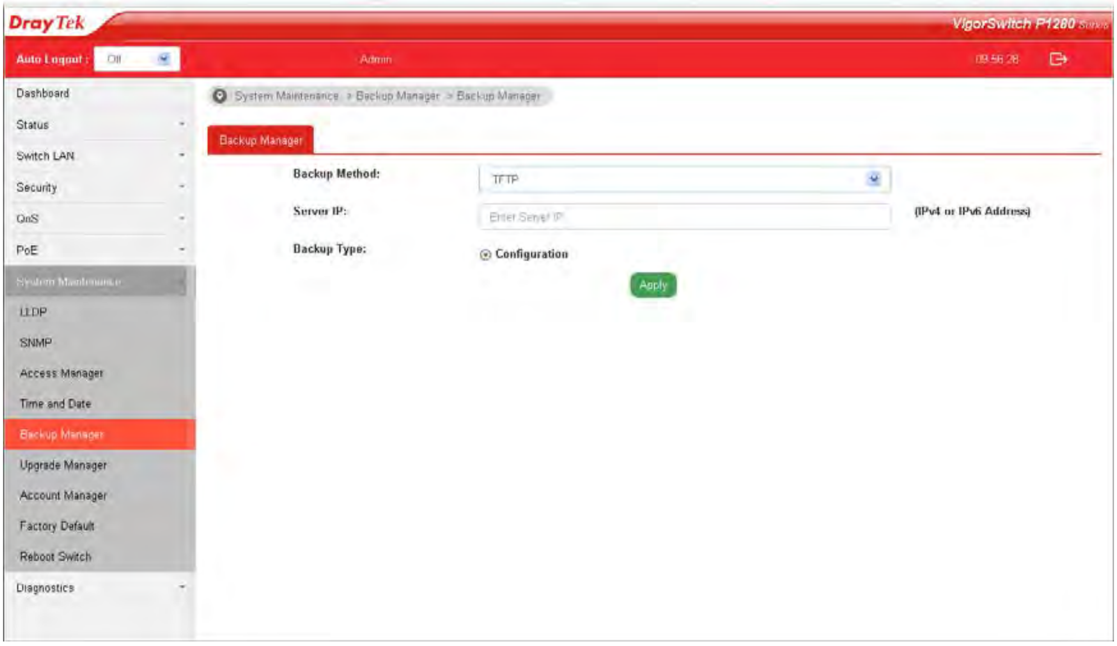
Server Port: 123 (1 - 65535 | Default : 123)

Available settings are explained as follows:

Item	Description
Manual Time	Specify static time (year, month, day, hours, miniutes and seconds) manually.
Enable SNTP	**Enable** – Click it to enable SNTP time server. **Disable** – Click to disable the time server.
SNTP/NTP Server Address	Enter the web site of the time server or the IP address of the server.
Server Port	Enter the port number use by the time server.
Apply	Save the settings or changes to the switch.

VI-5 Backup Manager

Backup Manager allows a user to backup the firmware image or configuration file on the switch to remote TFTP server or host file system through HTTP protocol.



Auto Logout : Off

Backup Method: TFTP

Server IP: Enter Server IP (IPv4 or IPv6 Address)

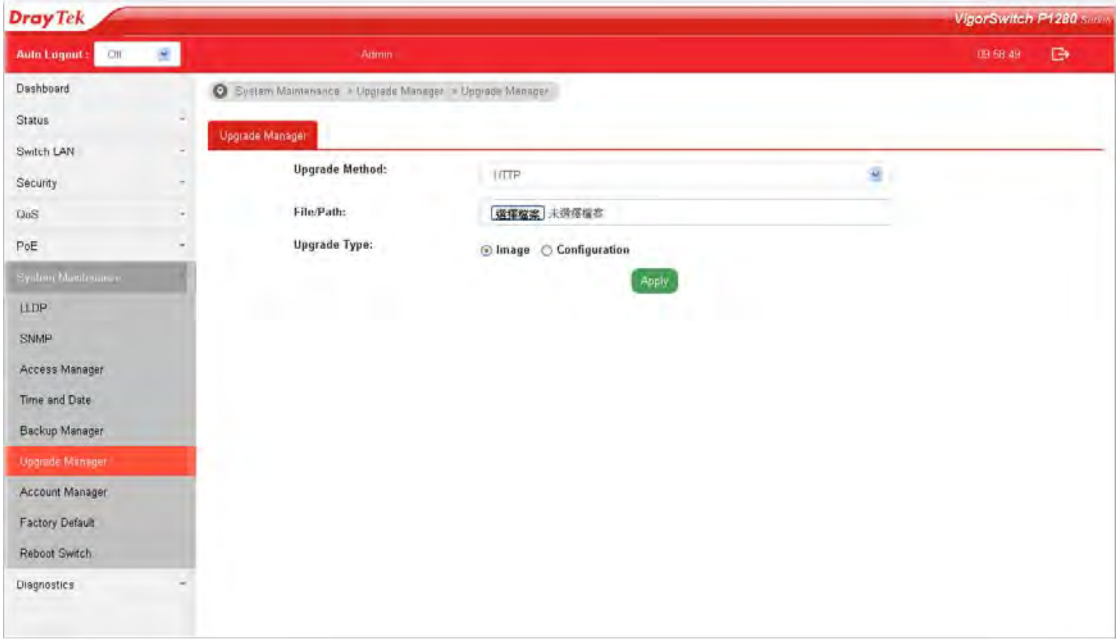
Backup Type: ● Configuration

Available settings are explained as follows:

Item	Description
Backup Method	Select Backup method. **TFTP** - Using TFTP to backup firmware. **HTTP** - Using WEB browser to ubackup firmware.
Server IP	It is available when TFTP is selected as Backup Method. Enter the IPv4/IPv6 address for the TFTP server.
Backup Type	**Configuration** – Make a backup copy for the configurations for VigorSwitch.
Apply	Save the settings or changes to the switch.

VI-6 Upgrade Manager

Backup Manager allows a user to upgrade the firmware image or configuration file on the switch to remote TFTP server or host file system through HTTP protocol.



Upgrade Method: HTTP

File/Path: 選擇檔案 未選擇檔案

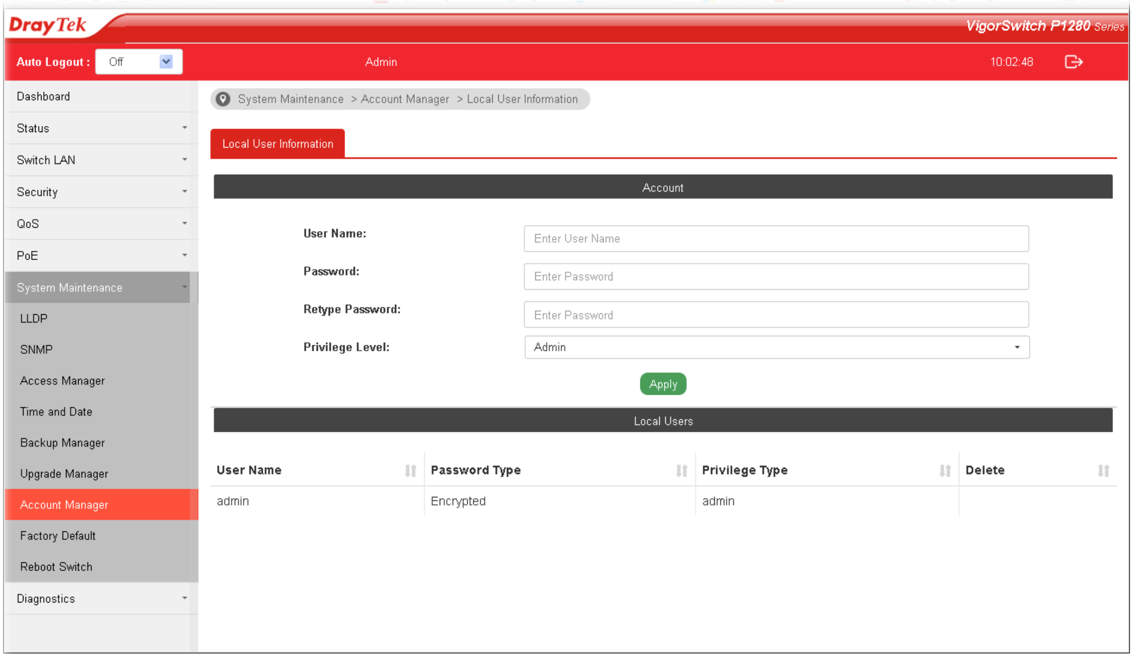
Upgrade Type: ● Image ○ Configuration

Available settings are explained as follows:

Item	Description
Upgrade Method	Select Upgrade method: **TFTP** - Using TFTP to upgrade firmware. **HTTP** - Using WEB browser to upgrade firmware.
Server IP	It is available when TFTP is selected as Upgrade Method. Enter the IPv4/IPv6 address for the TFTP server.
File Name	It is available when **TFTP** is selected as Upgrade Method. Enter the firmware image or configuration file name on the TFTP server.
File/Path	It is available when **HTTP** is selected as Upgrade Method. Choose the firmware file located in your computer.
Upgrade Type	It is available when TFTP is selected as Upgrade Method. **Image** – Click it to upgrade the firmware image. **Configuration** – Click ito to upgrade the configurations for VigorSwitch.
Apply	Save the settings or changes to the switch.

VI-7 Account Manager

This page allows a user to add or delete local user on switch database for authentication. The configuration result for each port will be displayed on the table listed on the lower side of this web page.



User Name: Enter User Name

Password: Enter Password

Retype Password: Enter Password

Privilege Level: Admin

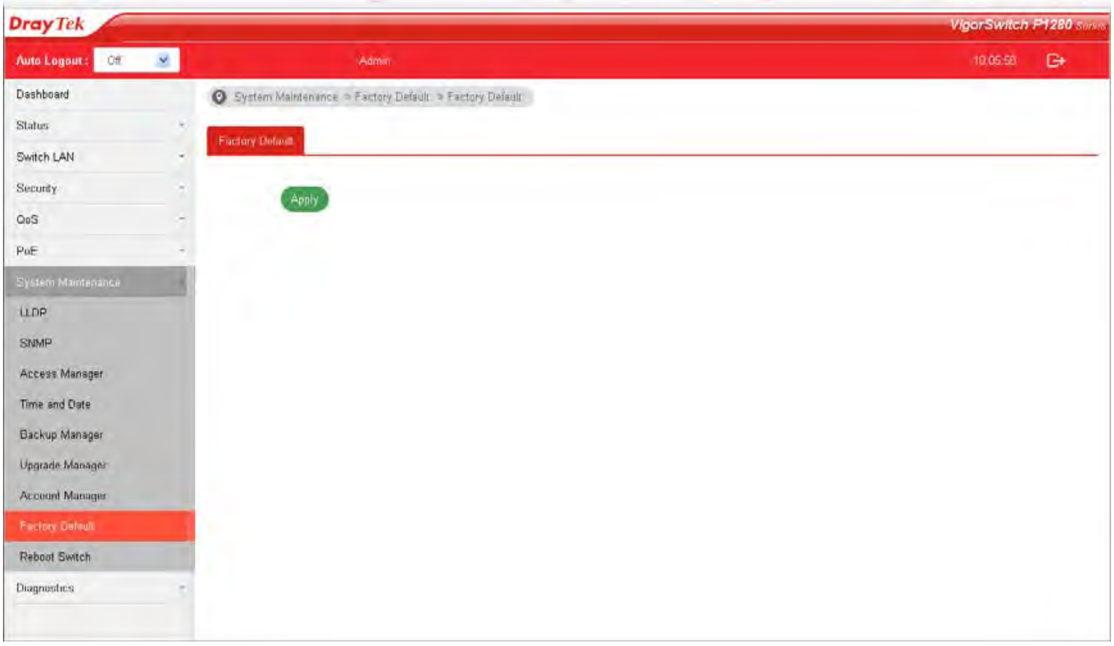
User Name	Password Type	Privilege Type	Delete
admin	Encrypted	admin	

Available settings are explained as follows:

Item	Description
User Name	Enter a username for new account. If you want to modify an existed user account, simply enter the same string in this field. Then, modify the password and choose privilege level. After clicking **Apply**, the existed user name will be modified with different values.
Password	Enter a password for new account.
Retype Password	Retype password to make sure the password is exactly you typed before in “Password” field.
Privilege Level	Use the drop down list to select privilege level (Admin/User) for new account. **Admin** - Allow to change switch settings. **User** - See switch settings only. Not allow to change it.
Apply	Save the settings or changes to the switch.
Delete	Remove the selected account.

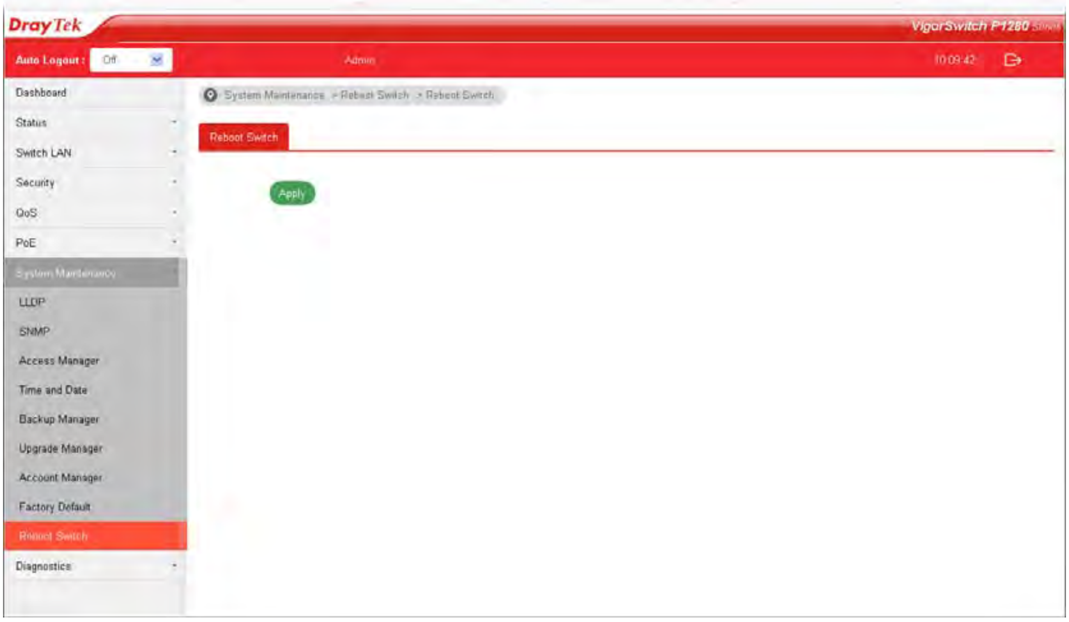
VI-8 Factory Default

Click **Apply** to return to factory default settings for VigorSwitch.



VI-9 Reboot Switch

Click **Apply** to reboot VigorSwitch with current settings.

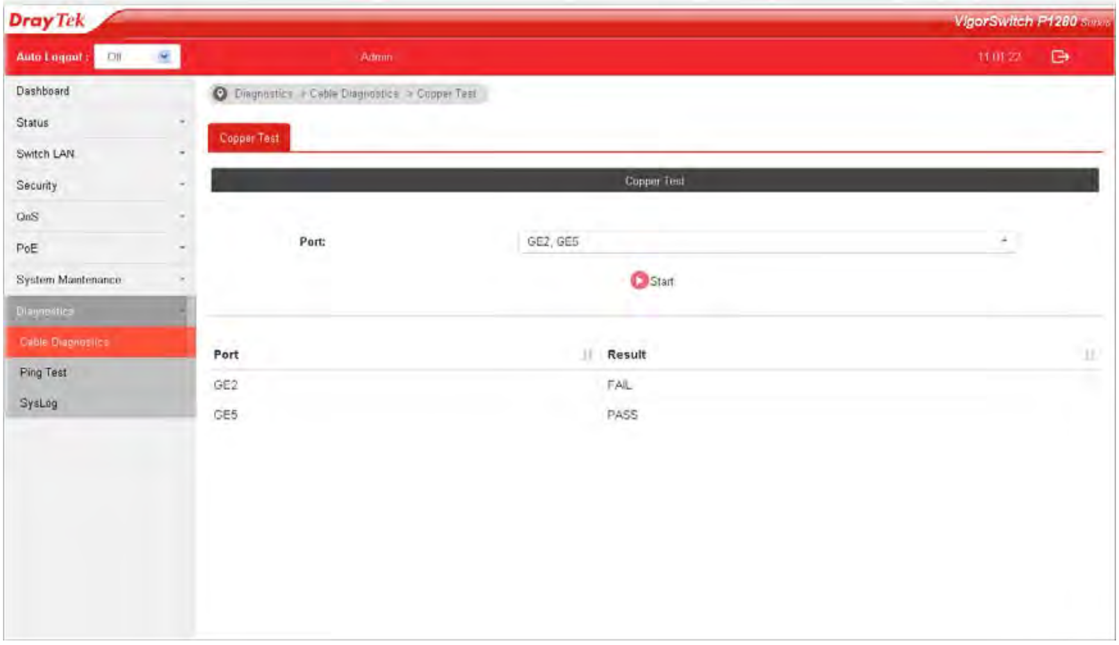


Auto Logout : Off

Part VII Diagnostics

VII-1 Cable Diagnostics

After finished copper test, the results will be shown on the lower side of this web page.



Port: GE2, GE5

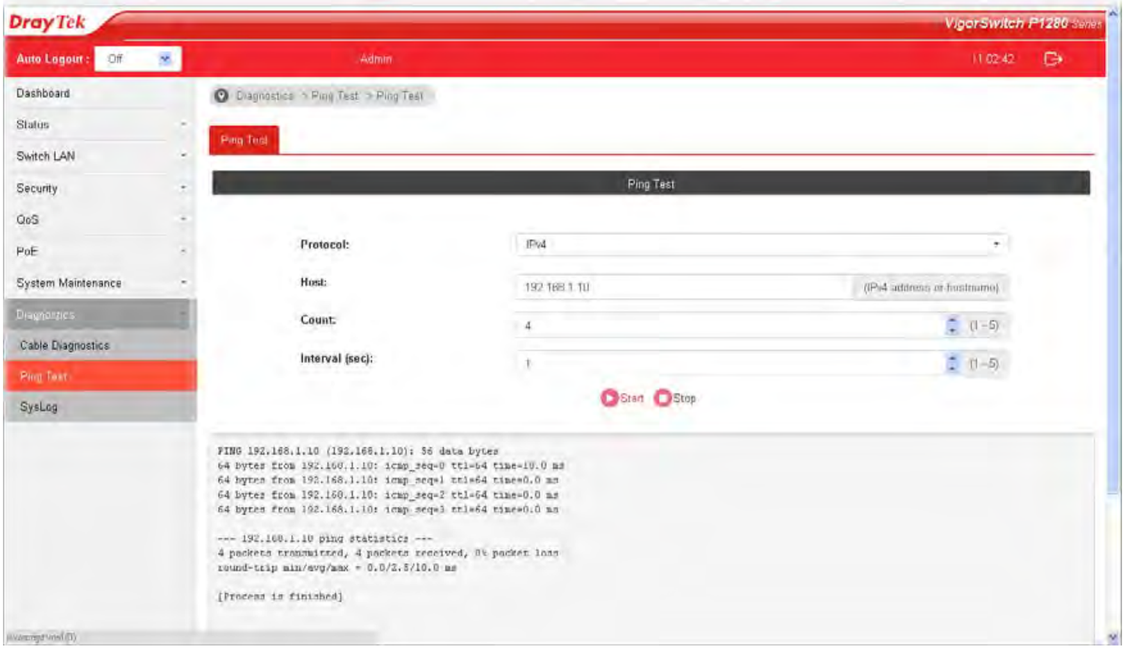
Port	Result
GE2	FAIL
GE5	PASS

Available settings are explained as follows:

Item	Description
Port	Use the drop down list to select the port (GE1 to GE28) or ports for performing cable diagnostics.
Start	Perform the copper test action.

VII-2 Ping Test

After finished the ping test, the results will be shown on the lower side of this web page.



Ping Test

Protocol: IPv4

Host: 192.168.1.10 (IPv4 address or hostname)

Count: 4 (1 - 5)

Interval (sec): 1 (1 - 5)

```
PING 192.168.1.10 (192.168.1.10): 56 data bytes
64 bytes from 192.168.1.10: icmp_seq=0 ttl=64 time=10.0 ms
64 bytes from 192.168.1.10: icmp_seq=1 ttl=64 time=0.0 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=64 time=0.0 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=64 time=0.0 ms

--- 192.168.1.10 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.0/2.5/10.0 ms

[Process is finished]
```

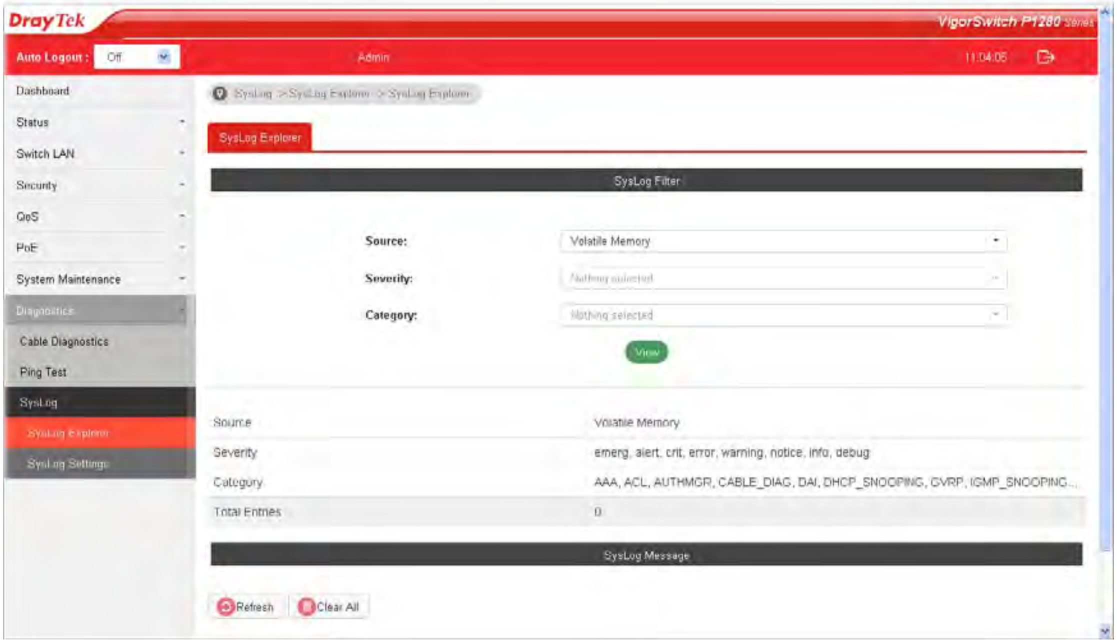
Available settings are explained as follows:

Item	Description
Protocol	Choose IPv4/IPv6 to specify IP address for sending ping to check if network path is ok.
Host	Enter the IP address of SNMP server based on the protocol selected above.
Count	It means how many times to send ping request packet. Enter a number between 1 and 5 as the count and the default configuration is 4.
Interval(sec)	Define the interval to perform ping action. For example, "1" means the ping action will be performed per second.
Start	Perform ping action.
Stop	Terminate ping action.

VII-3 SysLog

VII-3-1 SysLog Explorer

After clicking View, the results will be shown on the lower side of this web page.



Source: Volatile Memory

Severity: Nothing selected

Category: Nothing selected

Source	Volatile Memory
Severity	emerg, alert, crit, error, warning, notice, info, debug
Category	AAA, ACL, AUTHMGR, CABLE_DIAG, DAI, DHCP_SNOOPING, GVRP, IGMP_SNOOPING...
Total Entries	0

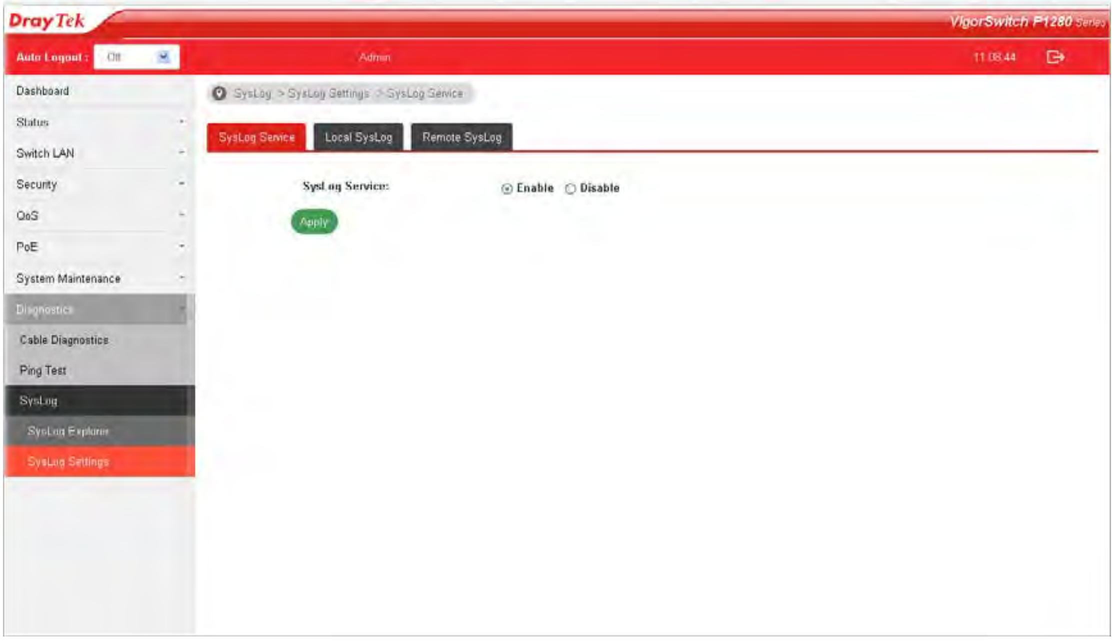
Available settings are explained as follows:

Item	Description
Source	**Volatile Memory** – Explore the logs contained in volatile memory (also known as RAM). **Non-Volatile Memory** - Explore the logs contained in non-volatile memory (also known as Flash).
Severity	Select severity (emerg, alert, crit, error, warning, notice, info and debug) of log messages which you wish to filter out for review.
Category	Select the categories (related features) of logs you wish to review. Category contains AAA, ACL, AUTHMGR, CABLE_DIAG, DAI, DHCP_SNOOPING, GVRP, IGMP_SNOOPING, IPSG, L2, LLDP, Mac-based VLAN, Mirror, MLD_SNOOPING, Platform, PM, Port, PORT_SECURITY, QoS, Rate, SNMP, STP, Security suite, System, Surveillance VLAN, Trunk, UDLD and VLAN.
View	Click it to display logs based on the settings configured above.
Refresh	Click it to refresh the log.
Clear All	Clear it to remove all logs displayed in this page.

VII-3-2 SysLog Settings

VII-3-2-1 SysLog Service

This page allows user to enable system logging into local syslog and specific remote syslog server for storage.



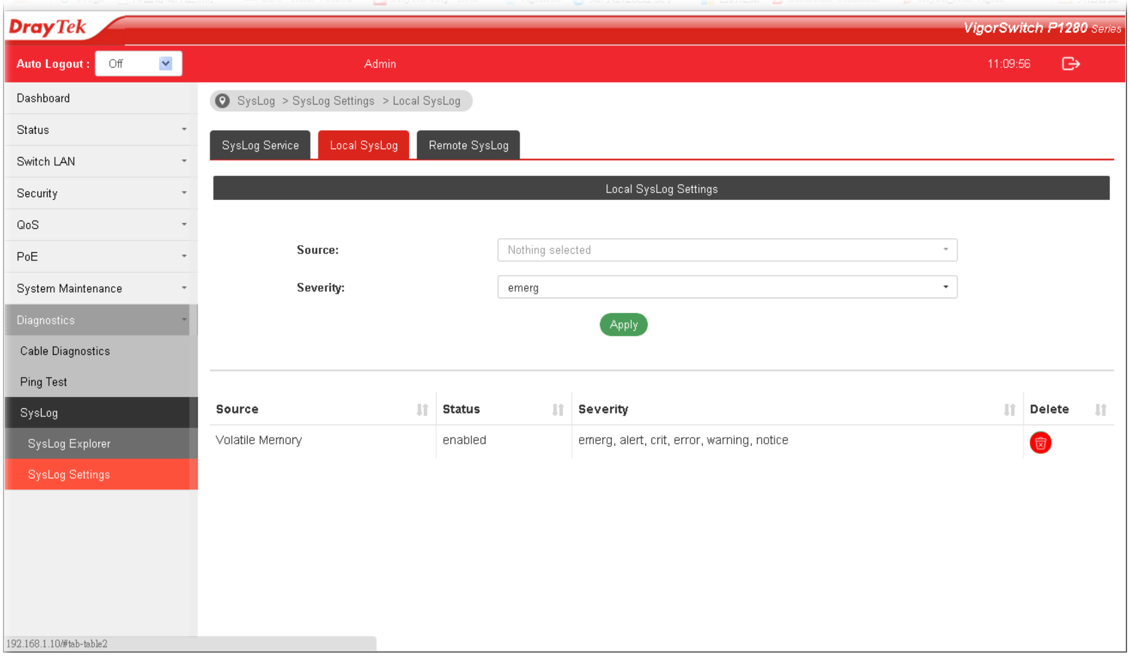
SysLog Service: ● Enable ○ Disable

Available settings are explained as follows:

Item	Description
SysLog Service	**Enable** – Click it to activate function of syslog. **Disable** – Click it to inactivate the function.
Apply	Save the settings or changes to the switch.

VII-3-2-2 Local SysLog

This page allows user to enable logging into volatile memory or non-volatile memory.



Source: Nothing selected

Severity: emerg

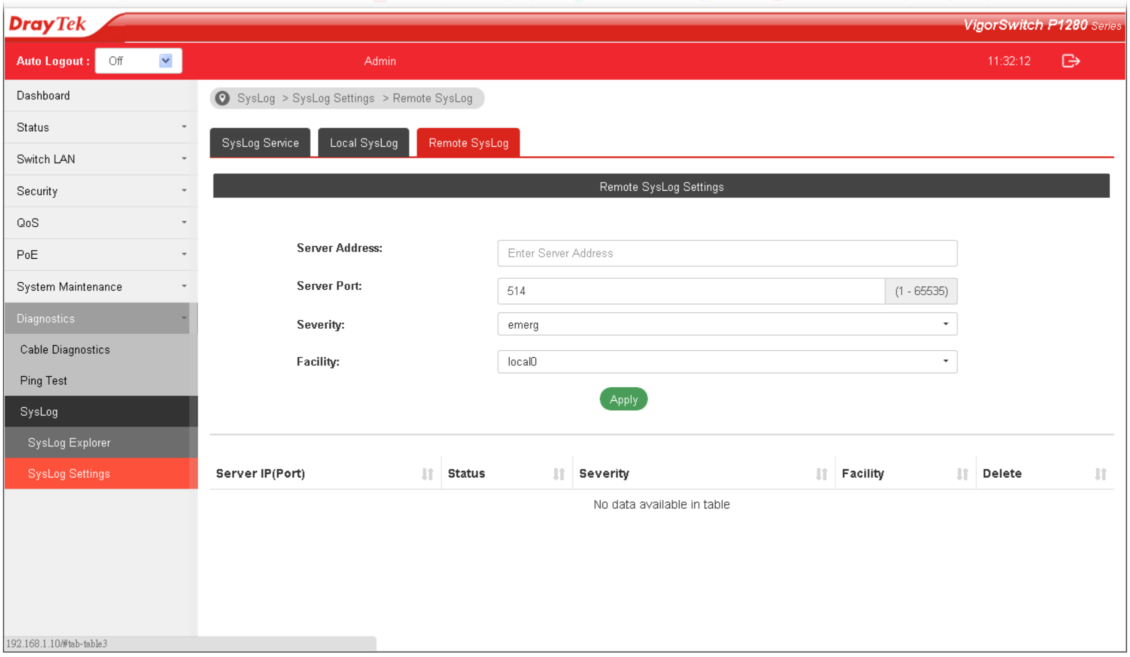
Source	Status	Severity	Delete
Volatile Memory	enabled	emerg, alert, crit, error, warning, notice	

Available settings are explained as follows:

Item	Description
Source	**Volatile Memory** – Select the volatile memory for saving local log. Volatile memory does not hold the log after reboot or power off. **Non-Volatile Memory** - Select the non-volatile memory for saving. If you want to modify **Volatile Memory / Non-Volatile Memory**, select **Volatile Memory / Non-Volatile Memory** in this field. Then, use the drop down list of severity to specify type of log message. After clicking **Apply**, the **Volatile Memory / Non-Volatile Memory** will be modified with new configured severity level.
Severity	Select severity (emerg, alert, crit, error, warning, notice, info and debug) of log messages which will be stored.
Apply	Save the settings or changes to the switch.
Delete	Remove all logs displayed in this page.

VII-3-2-3 Remote SysLog

This page allows user to enable system logging into specific remote syslog server for storage. After clicking **Apply**, the results will be shown on the lower side of this web page.



Remote SysLog Settings

Server Address: Enter Server Address

Server Port: 514 (1 - 65535)

Severity: emerg

Facility: local0

Apply

Server IP(Port)	Status	Severity	Facility	Delete
No data available in table				

Available settings are explained as follows:

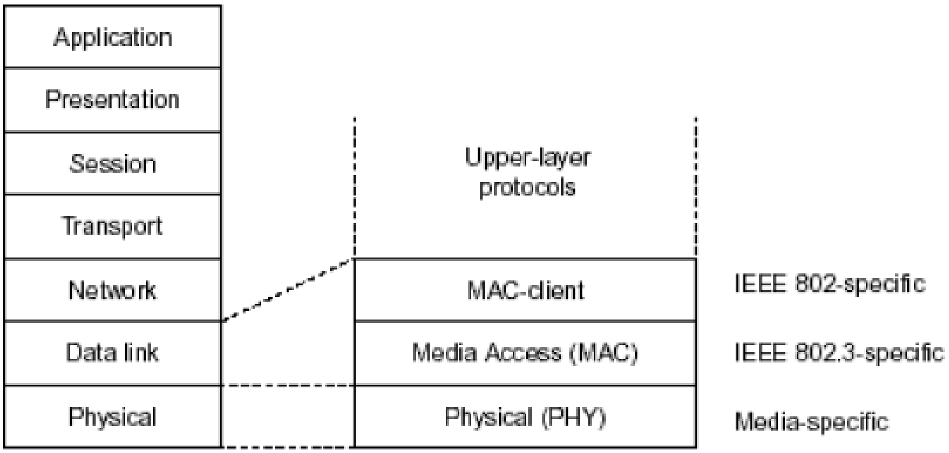
Item	Description
Server Address	Enter the IP address of Syslog server.
Server Port	Specify the port that syslog should be sent to.
Severity	Select severity (emerg, alert, crit, error, warning, notice, info and debug) of log messages which will be stored.
Facility	One device supports multiple facilities (represented with facility ID, local0 to local7) of remote Syslog server. For each facility ID contains different syslog server configuration, please choose a facility ID for such Syslog server.
Apply	Save the settings or changes to the switch.
Delete	Remove specific remote syslog entry.

Appendix: Reference

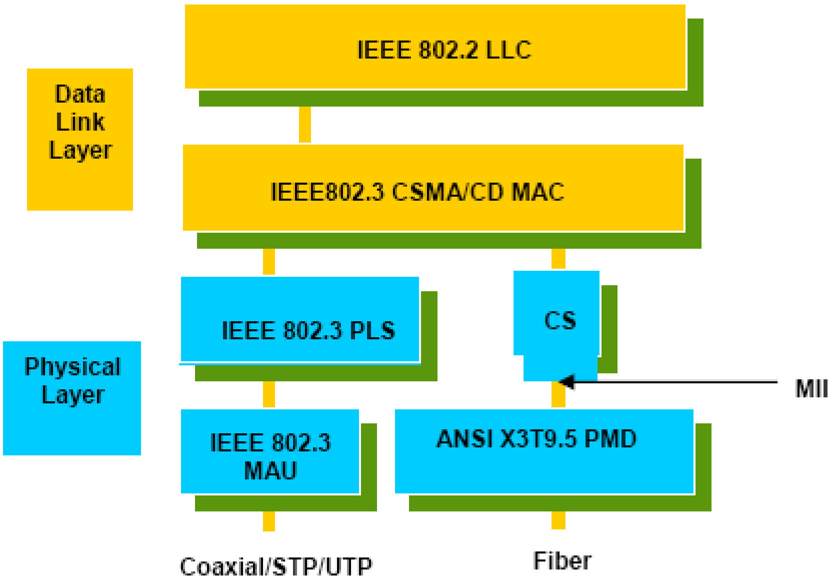
This chapter will tell you the basic concept of features to manage this switch and how they work.

A-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.

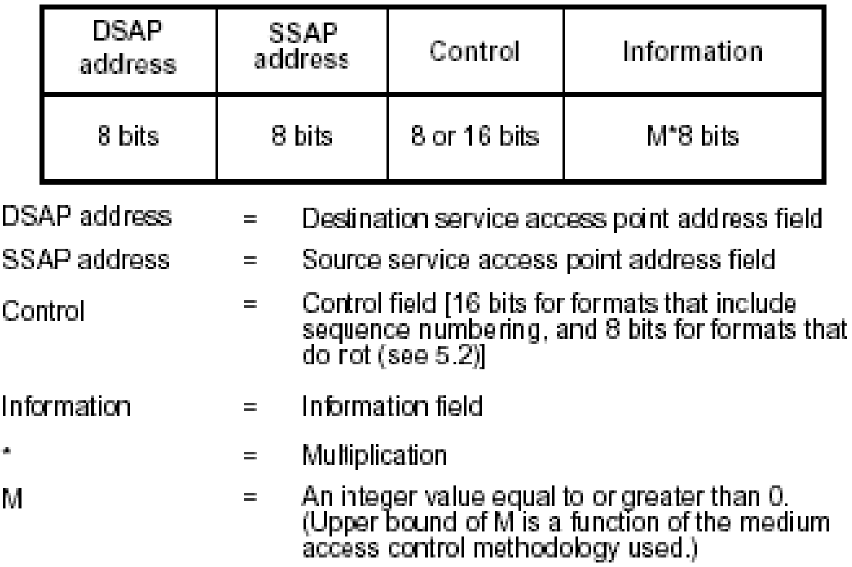


This above diagram shows the Ethernet architecture, LLC sub-layer and MAC sub-layer, which are responded to the Data Link layer, and transceivers, which are responded to the Physical layer in OSI model. In this section, we are mainly describing the MAC sub-layer.

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.

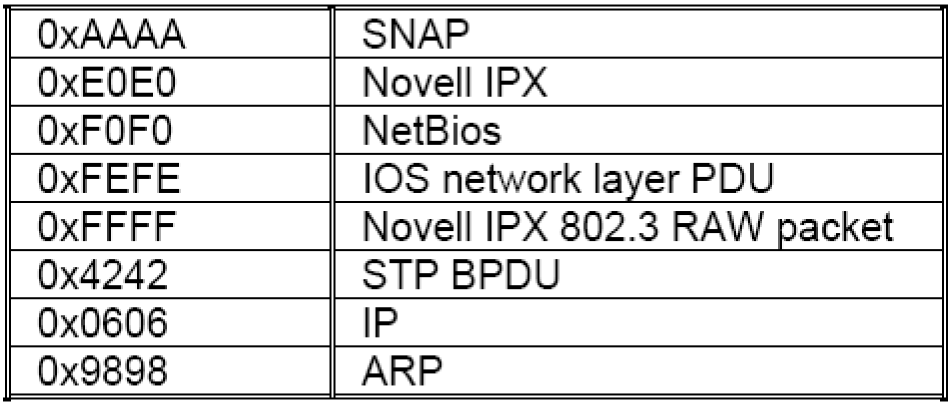
Logical link control supports the interface between the Ethernet MAC and upper layers in the protocol stack, usually Network layer, which is nothing to do with the nature of the LAN. So it can operate over other different LAN technology such as Token Ring, FDDI and so on. Likewise, for the interface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

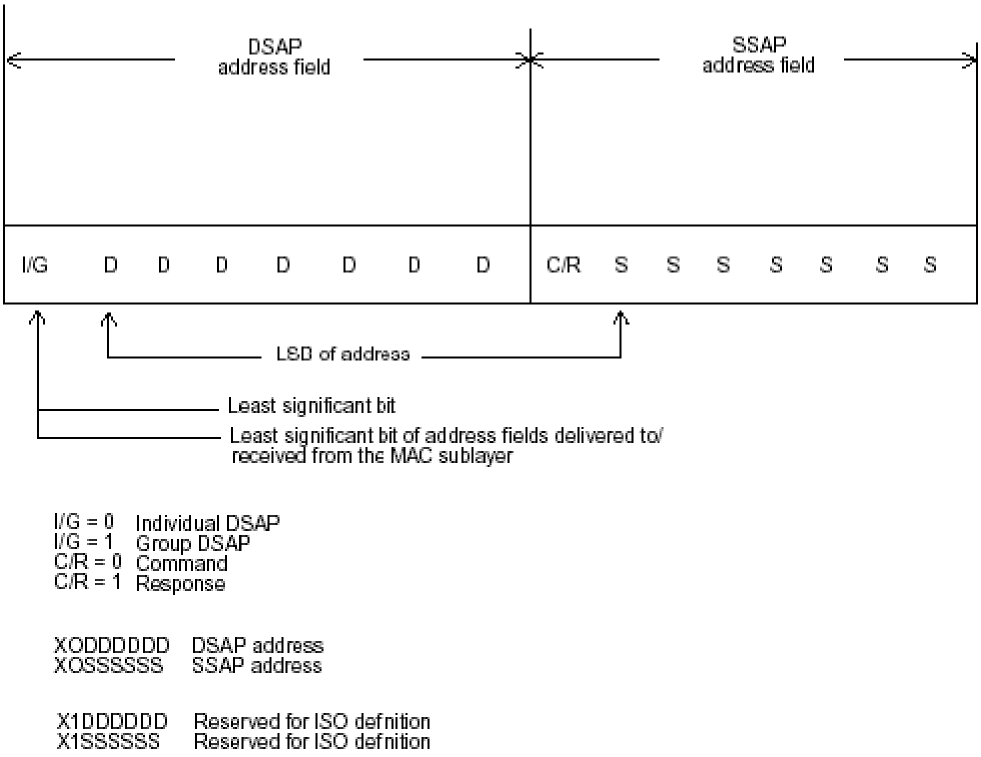
DSAP address	=	Destination service access point address field
SSAP address	=	Source service access point address field
Control	=	Control field [16 bits for formats that include sequence numbering, and 8 bits for formats that do rot (see 5.2)]
Information	=	Information field
*	=	Mulliplication
M	=	An 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.



A-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
1st byte	2nd byte	3rd byte	4th byte	5th byte	6th 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.

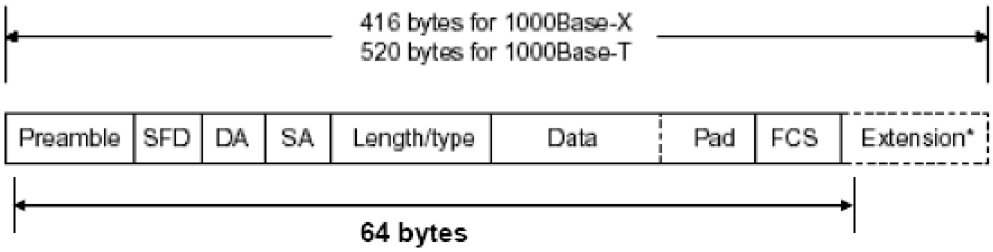
1. MAC will assemble the frame. First, the preamble and Start-of-Frame delimiter will be put in the fields of PRE and SFD, followed DA, SA, tag ID if tagged VLAN is applied, Ethertype or the value of the data length, and payload data field, and finally put the FCS data in order into the responded fields.
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.

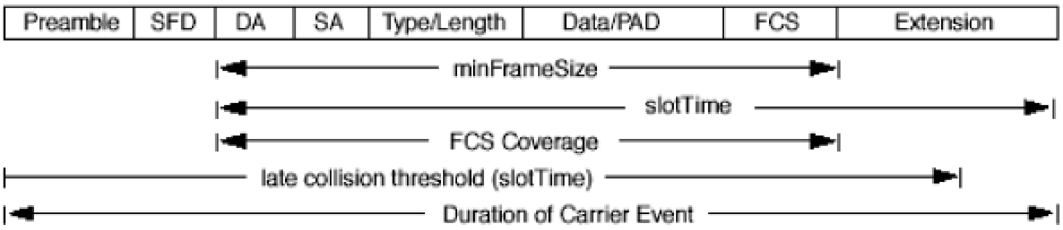
As the transmission of a MAC frame with the half-duplex operation exists only in the same collision domain, the carrier signal needs to spend time to travel to reach the targeted device. For two most-distant devices in the same collision domain, when one sends the frame first, and the second sends the 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
Max. collision domain DTE to DTE	100 meters	100 meters for UTP 412 meters for fiber	100 meters for UTP 316 meters for fiber
Max. collision domain with repeater	2500 meters	205 meters	200 meters
Slot time	512 bit times	512 bit times	512 bit times
Interframe Gap	9.6us	0.96us	0.096us
AttemptLimit	16	16	16
BackoffLimit	10	10	10
JamSize	32 bits	32 bits	32 bits
MaxFrameSize	1518	1518	1518
MinFrameSize	64	64	64
BurstLimit	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.

A-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.

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

where

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

Frame Reception

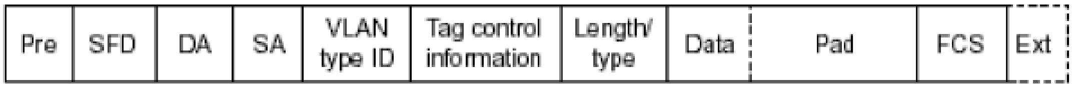
In essence, the frame reception is the same in both operations of half duplex and full duplex, except that full-duplex operation uses two buffers to transmit and receive the frame independently. The receiving node always “listens” if there is traffic running over the medium when it is not receiving a 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.

Bits 15-13	User Priority 7-0, 0 is lowest priority
Bit 12	CFI (Canonical Format Indicator) 1: RIF field is present in the tag header 0: No RIF field is present
Bits 11-0	VID (VLAN Identifier) 0x000: Null VID. No VID is present and only user priority is present. 0x001: Default VID 0xFFF: 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.

Index