DrayTek

VigorSwitch G2500

L2 Managed Gigabit Switch

Your reliable networking solutions partner

User's Guide

V1.0

VigorSwitch G2500

L2 Managed Gigabit Switch

User's Guide

Version: 1.0

Firmware Version: V2.4.1

(For future update, please visit DrayTek web site)

Date: March 20, 2019

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

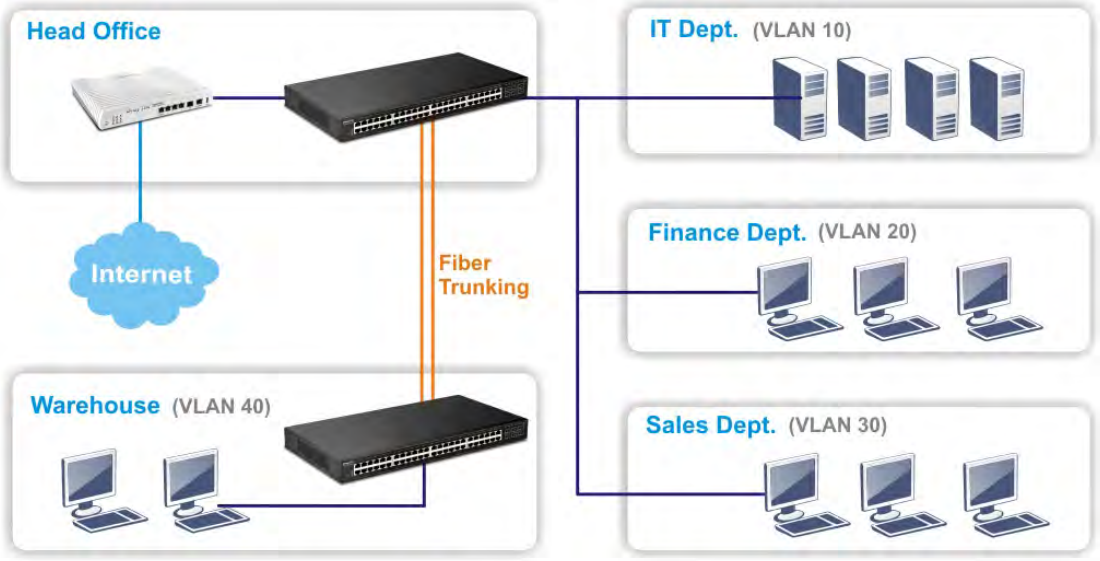
Part I Introduction

I-1 Introduction

VigorSwitch G2500, L2 Managed Gigabit 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 login 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 coulld be used in 1000Base-X/100Base-FX interface applications.



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.

I-1-2 Specifications

The VigorSwitch G2500, 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

- 44 10/100/1000Mbps Auto-negotiation Gigabit Ethernet TP ports
- 4 TP/SFP Combo Ethernet Ports
- 2 SFP Ports
- Jumbo frame support 9KB
- Programmable classifier for QoS (Layer 2/Layer 3)
- 8K MAC address and support VLAN ID(1~4094)
- Per-port shaping, policing, and Broadcast Storm Control
- Power Saving with IEEE 802.3az, Energy-Efficient Ethernet
- Full-duplex flow control (IEEE802.3x) and half-duplex backpressure
- Extensive front-panel diagnostic LEDs; Power, System
- 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:

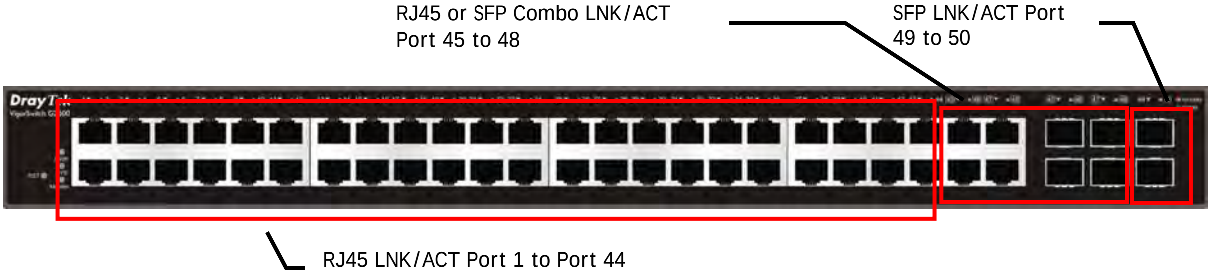
- VigorSwitch G2500
- AC Power Cord
- Quick Start Guide
- Rubber feet
- Rack mount kit

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


RJ45 or SFP Combo LNK/ACT Port 45 to 48
SFP LNK/ACT Port 49 to 50
RJ45 LNK/ACT Port 1 to Port 44

LED	Color	Explanation
PWR	On (Green)	The device is powered on and running normally.
	Off	The device is not ready or is failed.
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.
Monitor	On (Red)	An alert for system failure due to overheating or wrong voltage.
	Off	The device is in normal condition and running normally.
Port 1 ~ 44	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.
Port 45 ~ 48 (RJ45 or SFP)	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.
Port 49 ~ 50 (SFP)	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.

Connector Explanation

Interface	Description
Port 1 ~ 44 (RJ45)	Port 1 to Port 44 can be used for Ethernet connection.
Port 45 ~ 48 (RJ45 or SFP)	Port 45 to Port 48 are used either for Ethernet or fiber connection.
Port 49 ~ 50 (SFP)	Port 49 to Port 50 are used for fiber connection.
Console	Used to perform telnet command control.
	Power inlet for AC input (100~240V/AC, 50/60Hz).

Note:

Power Output –

- IEEE 802.3af Max. 15.4W Output Supported
- IEEE 802.3at Max. 30W Output Supported

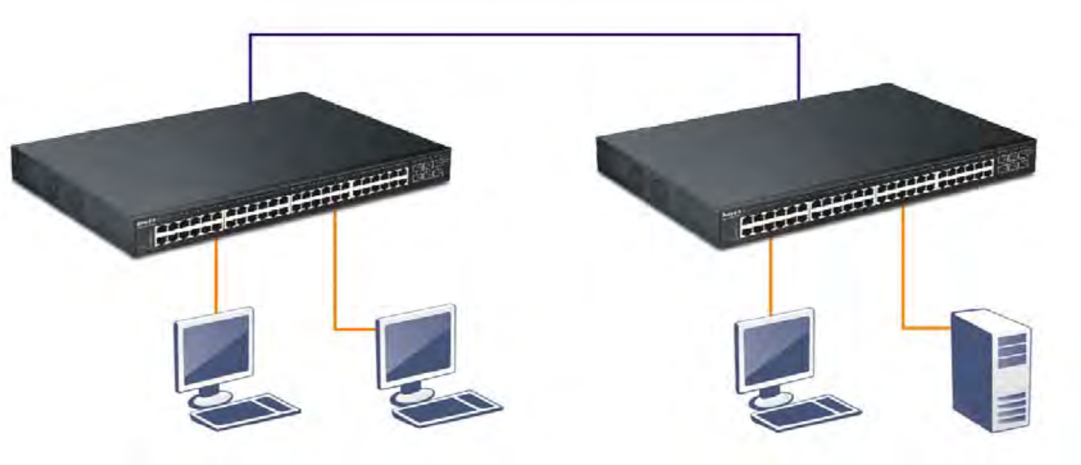
I-2 Installation

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.

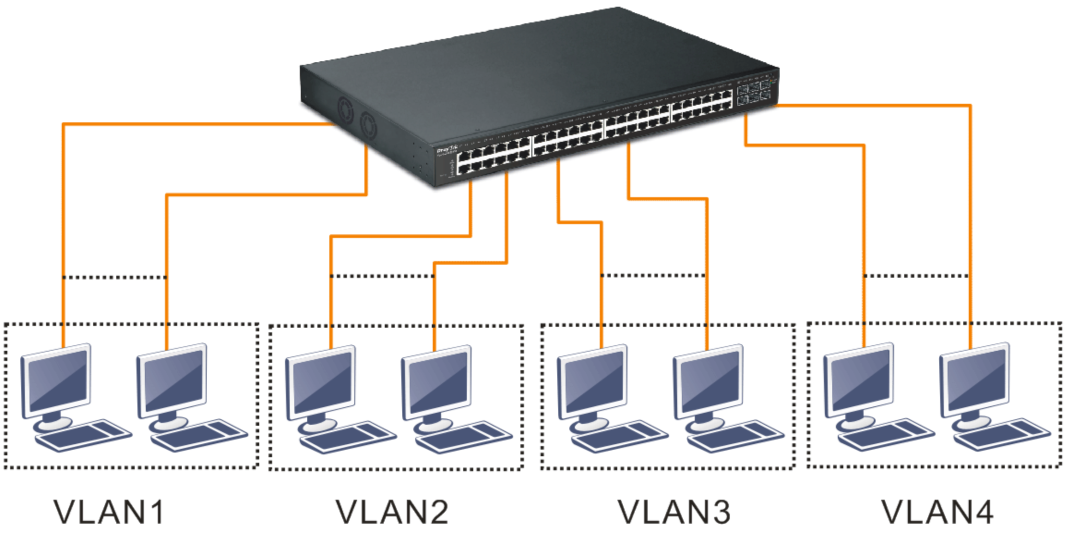
Every port can access each other. (*The switch image is sample only.)



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.

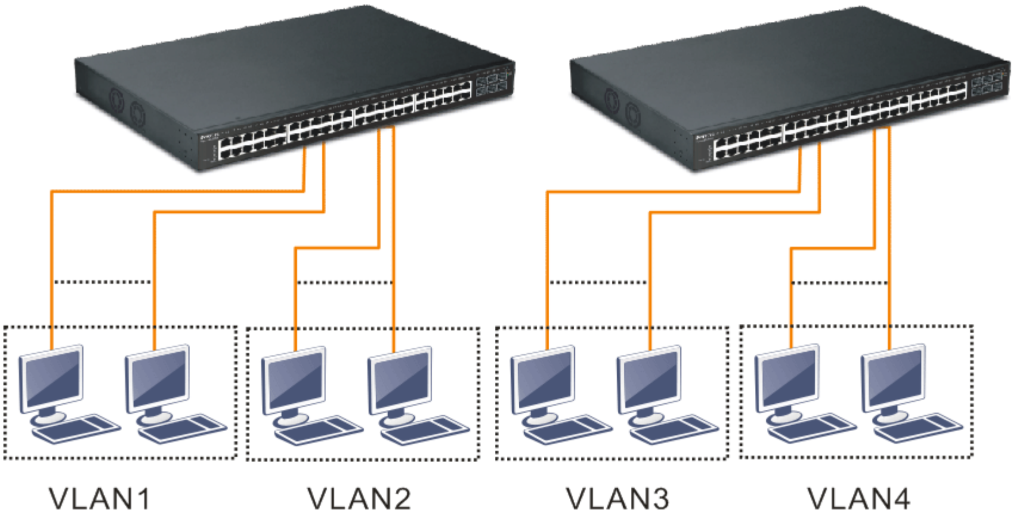
Case 2: Port-based VLAN -1 (*The switch image is sample only.)



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

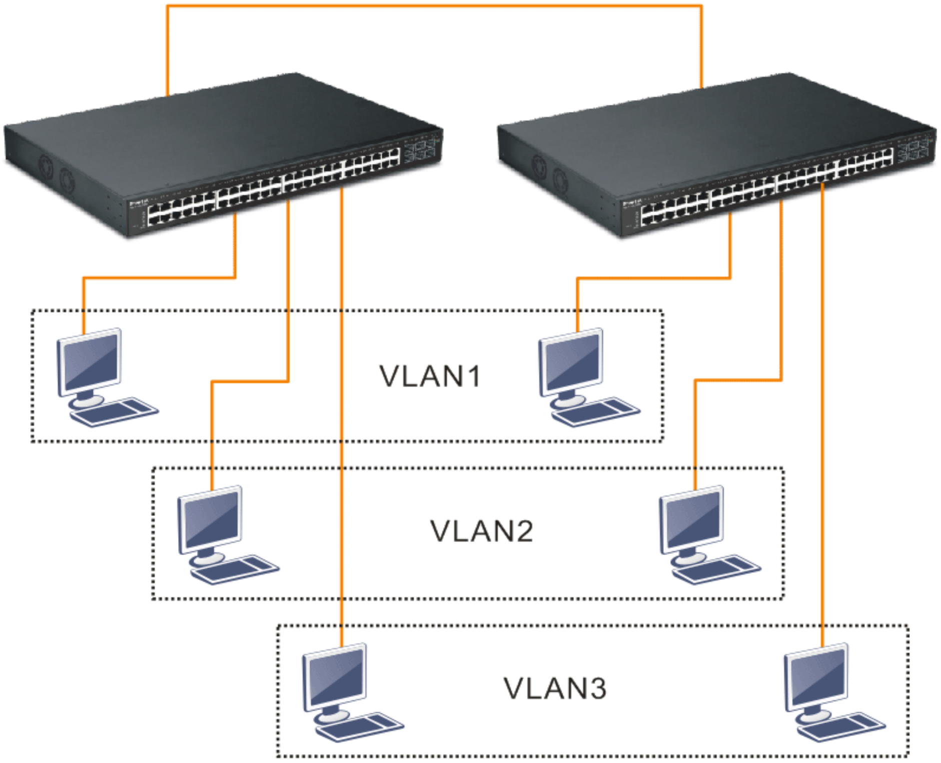
- Every VLAN members could not access VLAN members each other.
- The switch manager has to assign different names for each VLAN groups at one switch.

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.

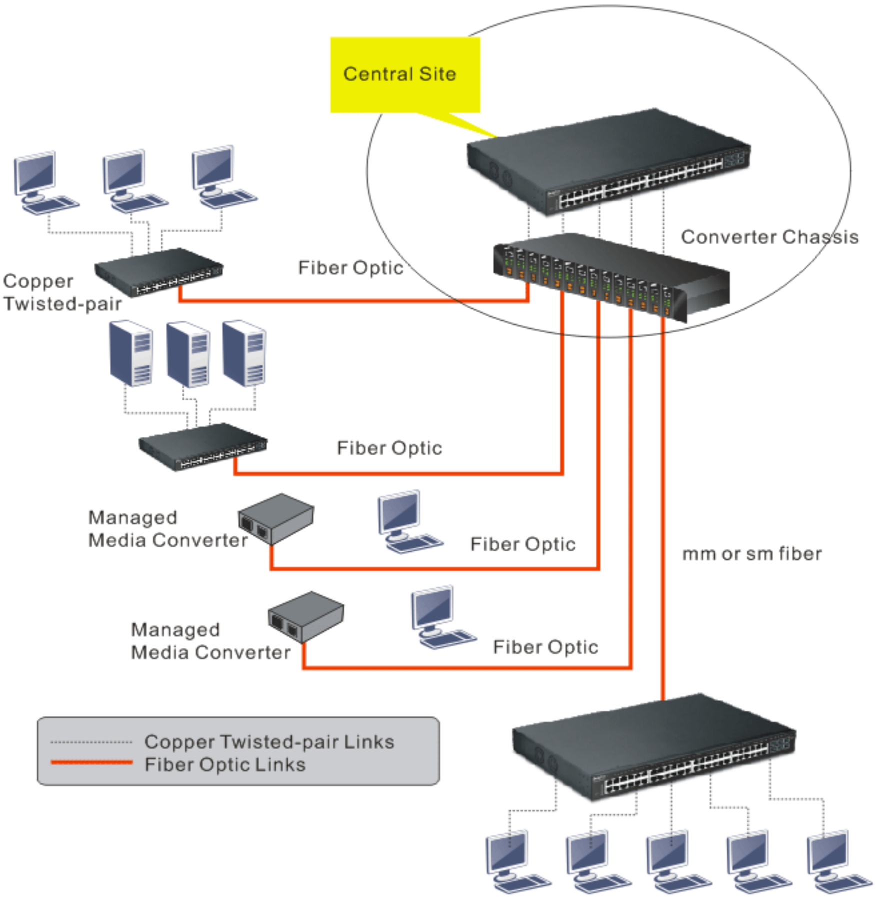
Case 6: Rack-mount Installation

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.

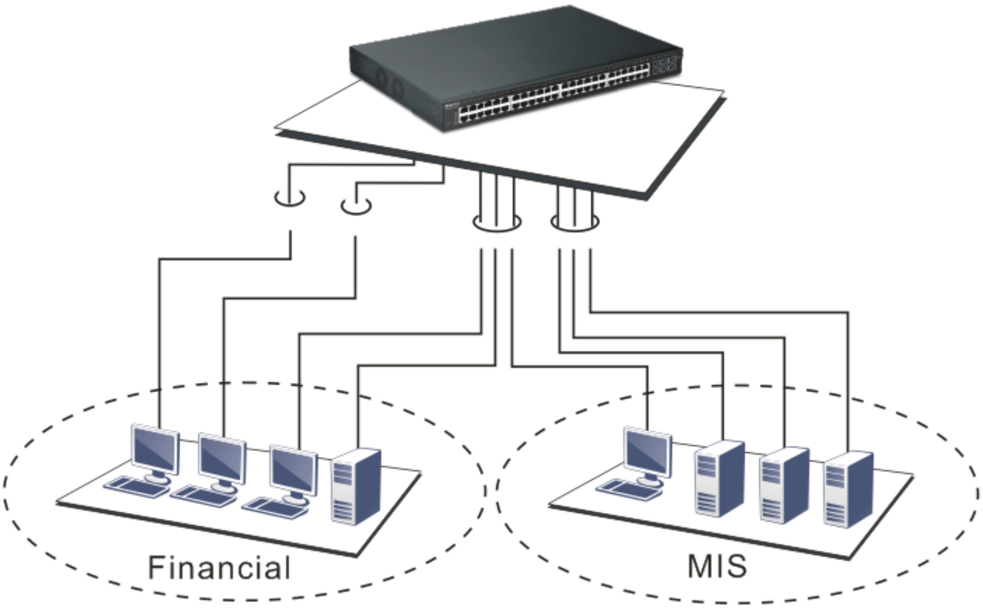
Procedures to Rack-mount the switch:

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.

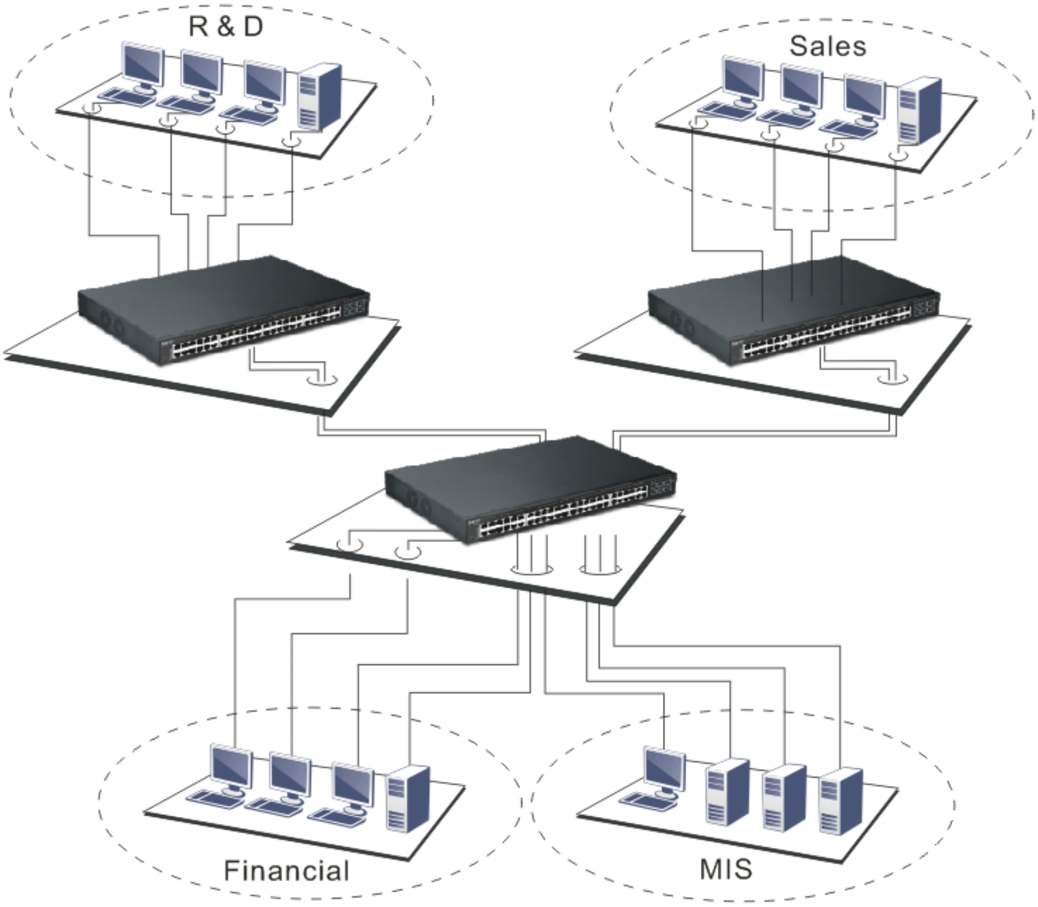
Case 7: Central Site/Remote site application is used in carrier or ISP



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.

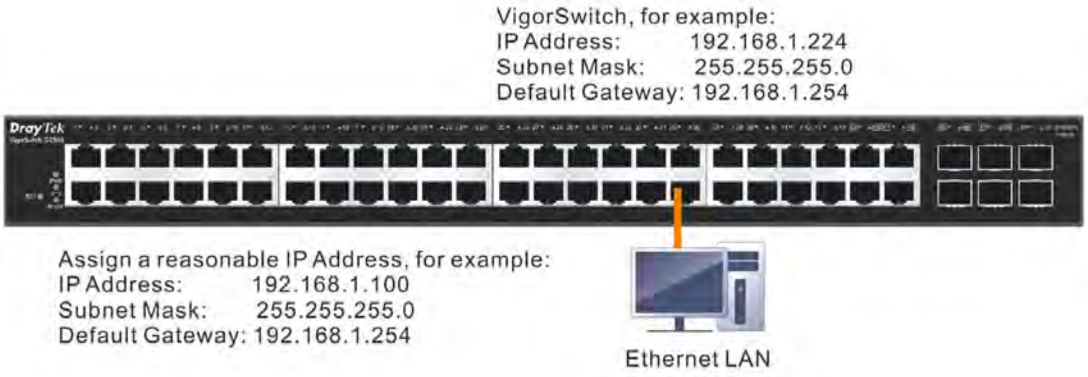
Media	Speed	Wiring
10/100/1000 Mbps copper	10 Mbps	Category 3,4,5 UTP/STP
	100Mbps	Category 5 UTP/STP
	1000 Mbps	Category 5e, 6 UTP/STP

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 G2500 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
DrayTek
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 G2500 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.

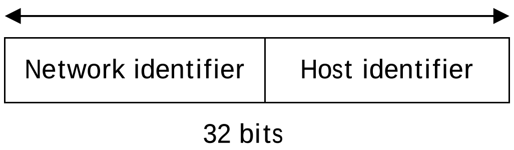
I-2-5 IP Address Assignment

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.

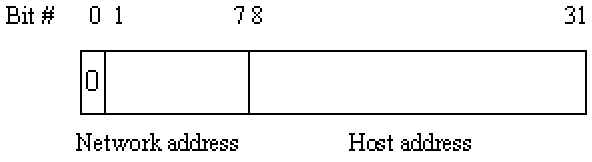
Each class has its own network range between the network identifier and host identifier in the 32 bits address. Each IP address comprises two parts: network identifier (address) and host identifier (address). The former indicates the network where the addressed host resides, and the latter indicates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

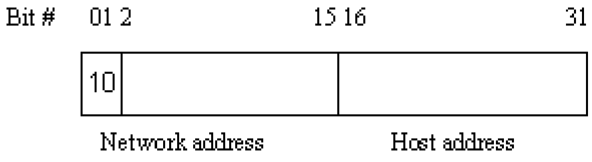
Class A:

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.



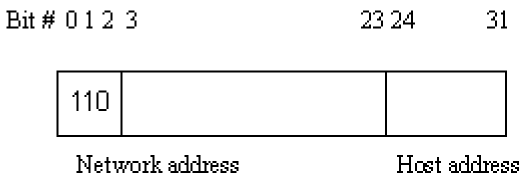
Class B:

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

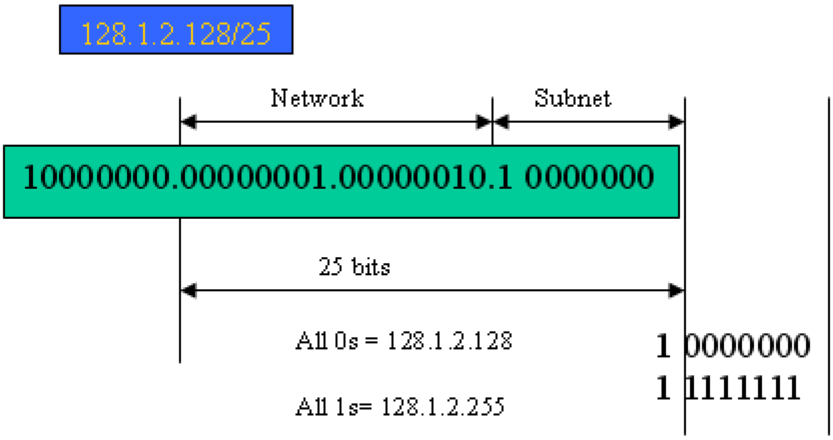
Please refer to RFC 1597 and RFC 1466 for more information.

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.

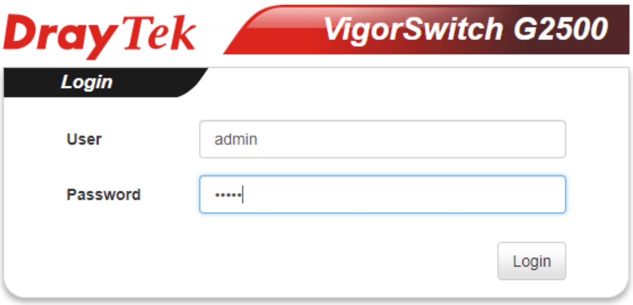
For assigning an IP address to the switch, you just have to check what the IP address of the network will be connected with the switch. Use the same network address and append your host address to it.

- 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.

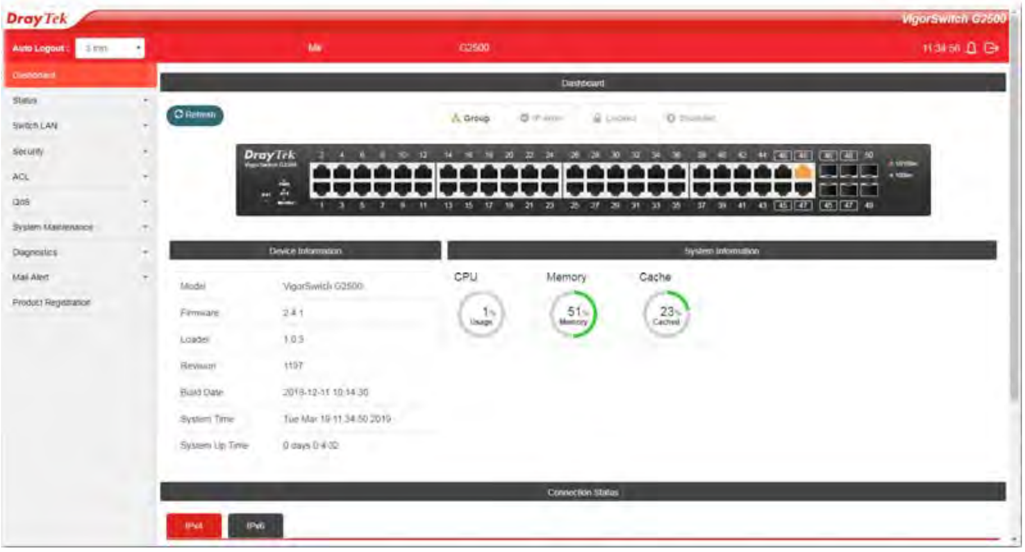
I-3 Accessing Web Page of VigorSwitch

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.



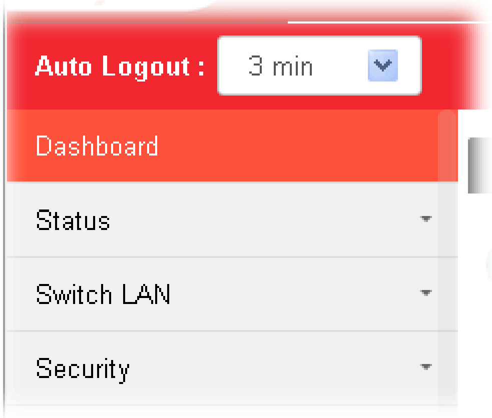
Model	VigorSwitch G2500
Firmware	2.4.1
Loader	1.0.3
Revision	1197
Build Date	2018-12-11 10:14:30
System Time	Tue Mar 19 11:34:50 2019
System Up Time	0 days 0:4:32

Info

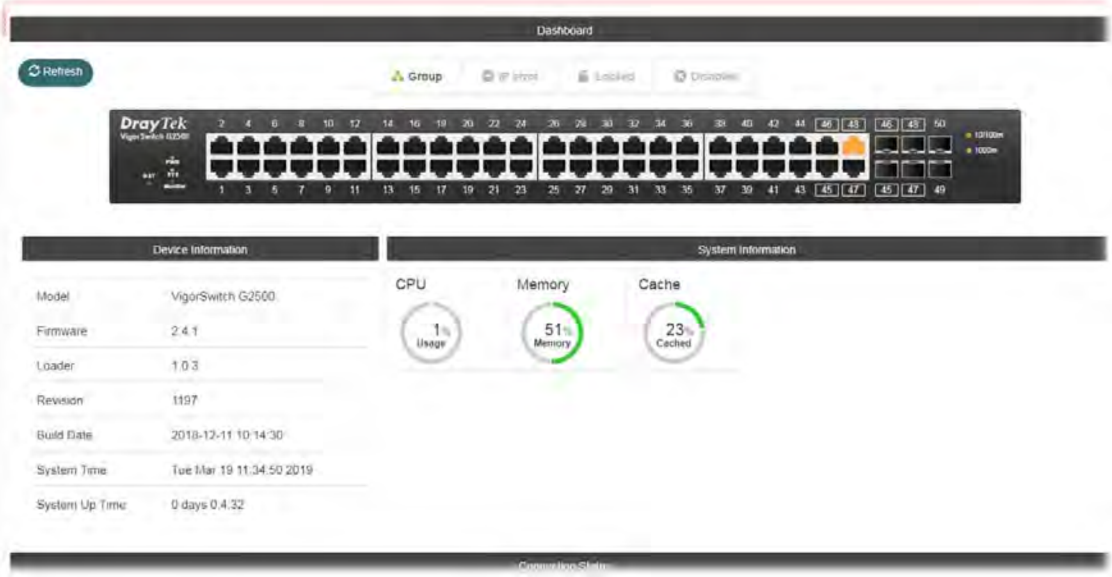
The DHCP Setting is enabled in default. Therefore, if a DHCP server presented on network connected to VigorSwitch, checking before accessing VigorSwitch is essential.

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 G2500

Firmware 2.4.1

Loader 1.0.3

Revision 1197

Build Date 2018-12-11 10:14:30

System Time Tue Mar 19 11:34:50 2019

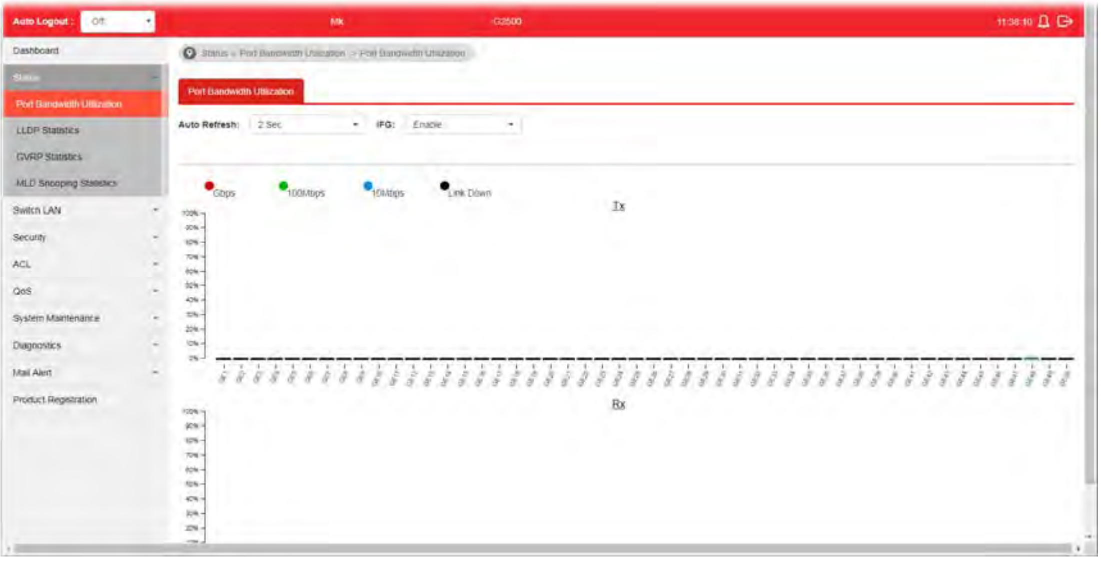
System Up Time 0 days 0:4:32

System Information

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.

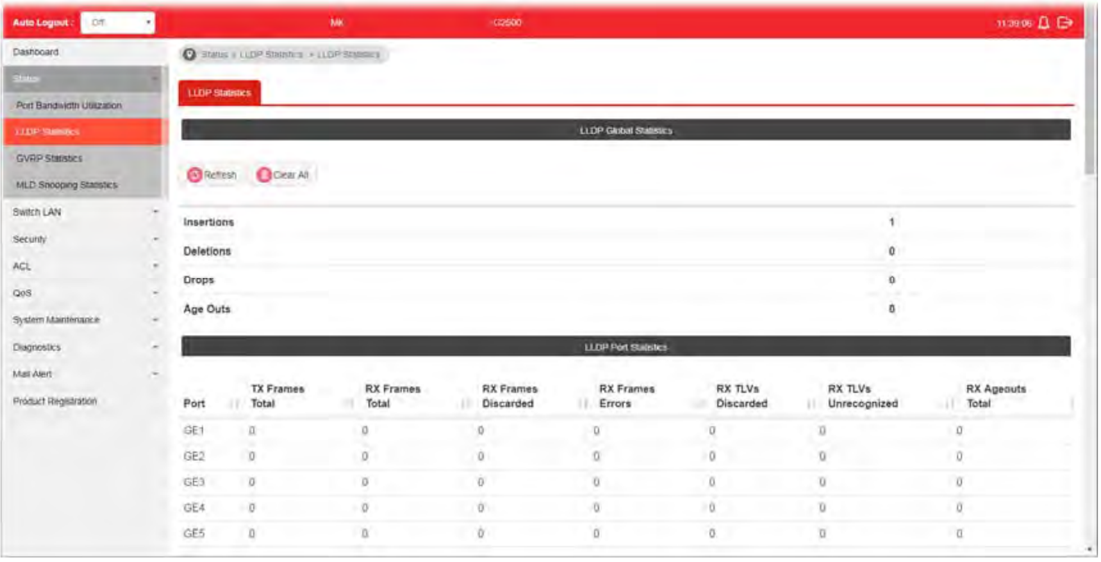


Auto Refresh: 2 Sec

IFG: Enable

I-5-2 LLDP Statistics

This page offers the statistics of LLDP packets (in, out and error) of each port (GE1 to GE50).



LLDP Global Statistics

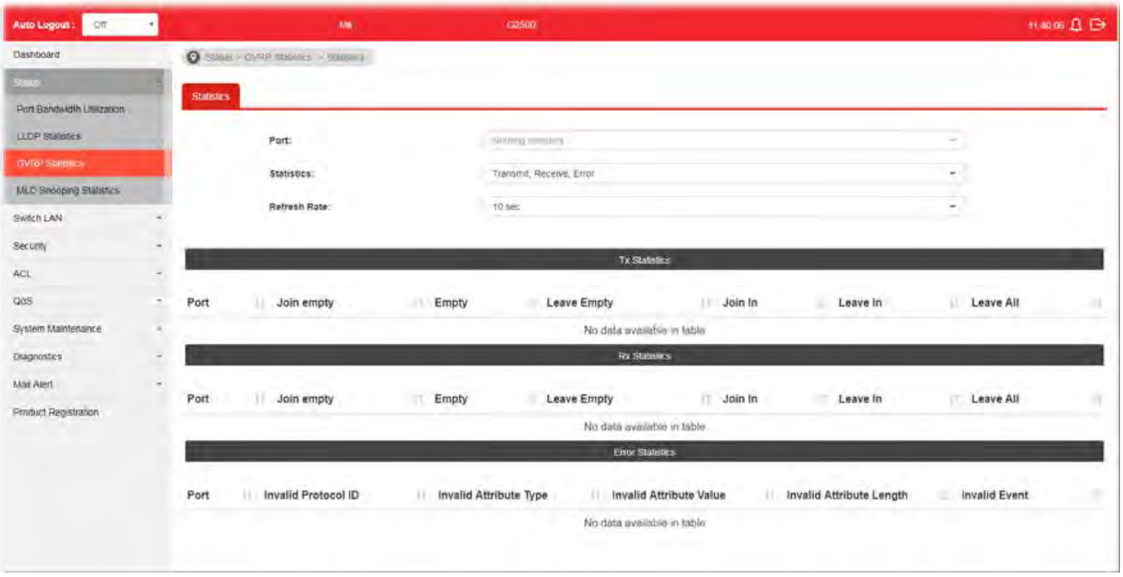
Insertions	1
Deletions	0
Drops	0
Age Outs	0

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	0	0	0	0	0	0	0
GE2	0	0	0	0	0	0	0
GE3	0	0	0	0	0	0	0
GE4	0	0	0	0	0	0	0
GE5	0	0	0	0	0	0	0

I-5-3 GVRP Statistics

GVRP (Generic Attribute Registration Protocol) is used automatically for exchanging information for VLAN membership between switches. This page counts the GVRP information received on each port.



Port:

Statistics: Transmit, Receive, Error

Refresh Rate: 10 sec

Tx Statistics

Port	Join empty	Empty	Leave Empty	Join In	Leave In	Leave All
No data available in table						

Rx Statistics

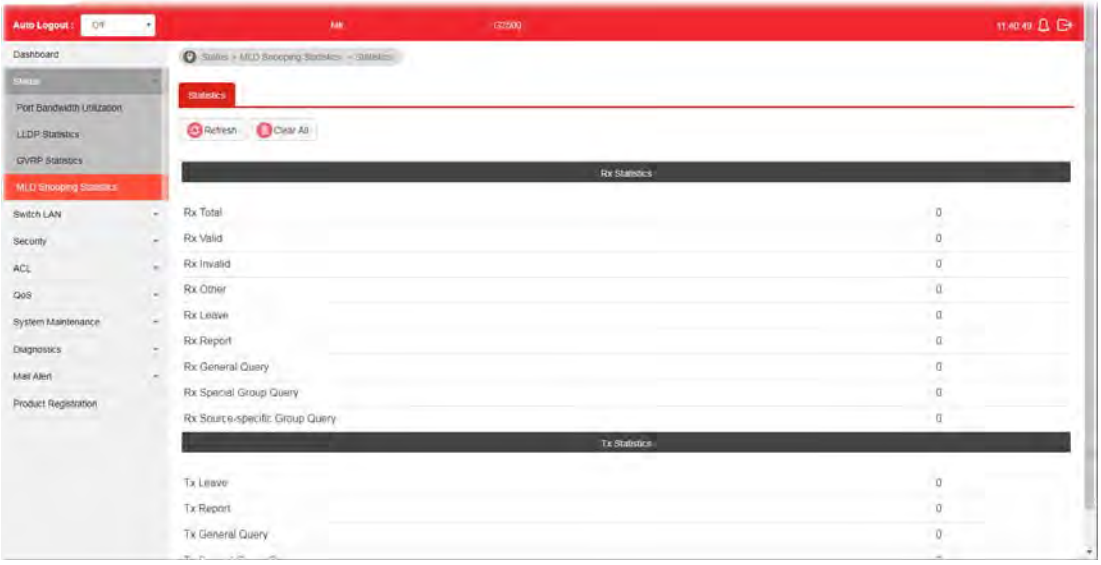
Port	Join empty	Empty	Leave Empty	Join In	Leave In	Leave All
No data available in table						

Error Statistics

Port	Invalid Protocol ID	Invalid Attribute Type	Invalid Attribute Value	Invalid Attribute Length	Invalid Event
No data available in table					

I-5-4 MLD Snooping Statistics

This page counts the MLD messages received or transmitted on the network.



Rx Statistics

Rx Total	0
Rx Valid	0
Rx Invalid	0
Rx Other	0
Rx Leave	0
Rx Report	0
Rx General Query	0
Rx Special Group Query	0
Rx Source-specific Group Query	0

Tx Statistics

Tx Leave	0
Tx Report	0
Tx General Query	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.

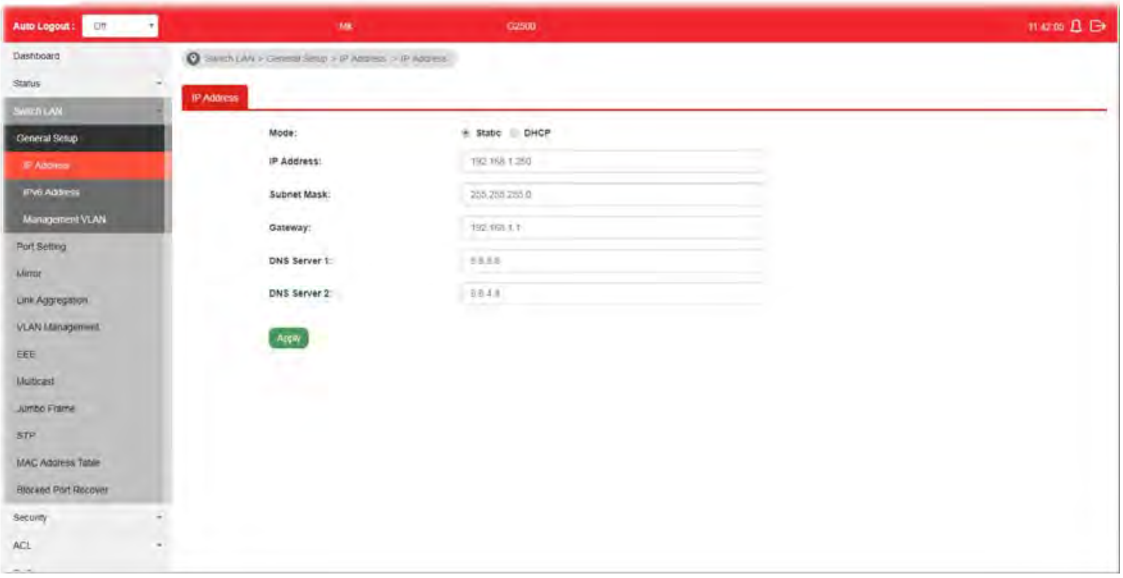
II-1-1 IP Address

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: 192.168.1.250

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

DNS Server 1: 8.8.8.8

DNS Server 2: 8.8.4.4

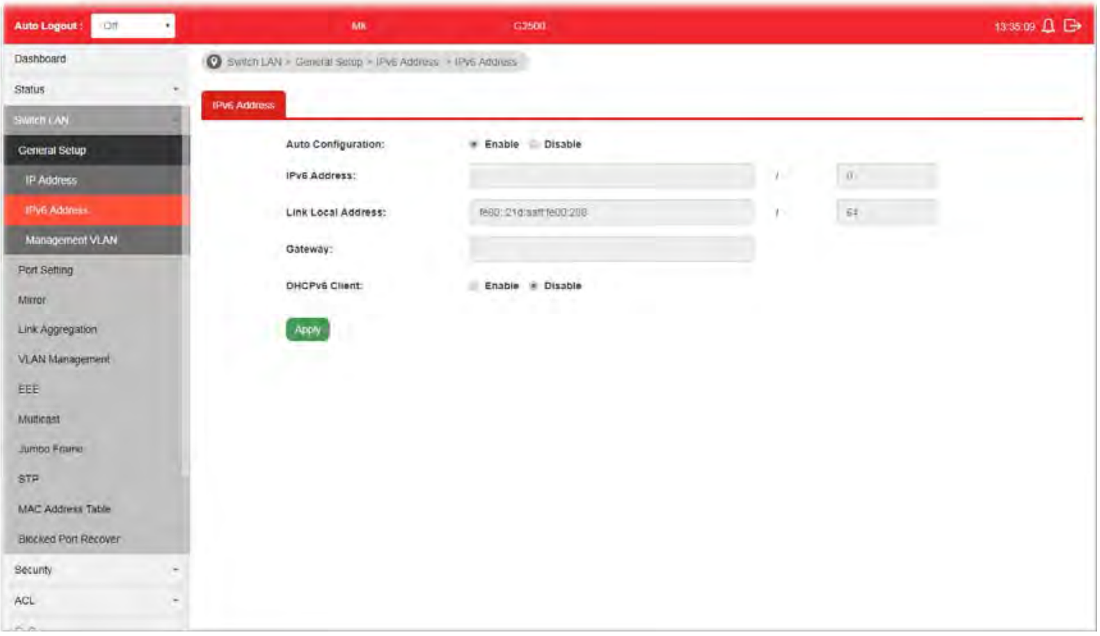
Available settings are explained as follows:

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	Apply the settings 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: ● Enable ○ Disable

IPv6 Address: / 0

Link Local Address: fe80::21d:aaff:fe00:208 / 64

Gateway:

DHCPv6 Client: ○ Enable ● Disable

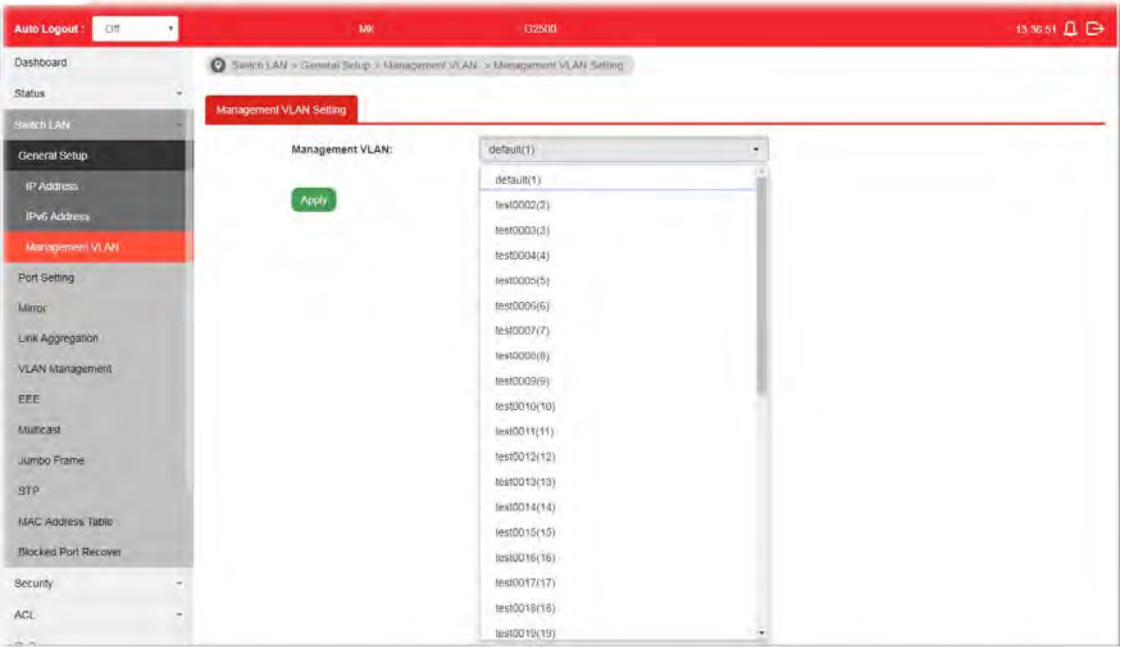
Available settings are explained as follows:

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

	gateway to access IPv6 Internet or other IPv6 network.
DNS Server 1	It is available when **Auto Configuration** is set as **Disable**. If static mode is enabled, enter primary DNS server address in this field.
DNS Server 2	It is available when **Auto Configuration** is set as **Disable**. If static mode is enabled, enter secondary DNS server address in this field.
DHCPv6 Client	It is available when **Auto Configuration** is set as **Enable.** Enable this feature if there is a DHCPv6 server on your network for assigning IPv6 Address, instead of using Router Advertisement.
Apply	Apply the settings to the switch.

II-1-3 Management VLAN

This page allows the network administrator 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 Setting

Management VLAN: default(1)

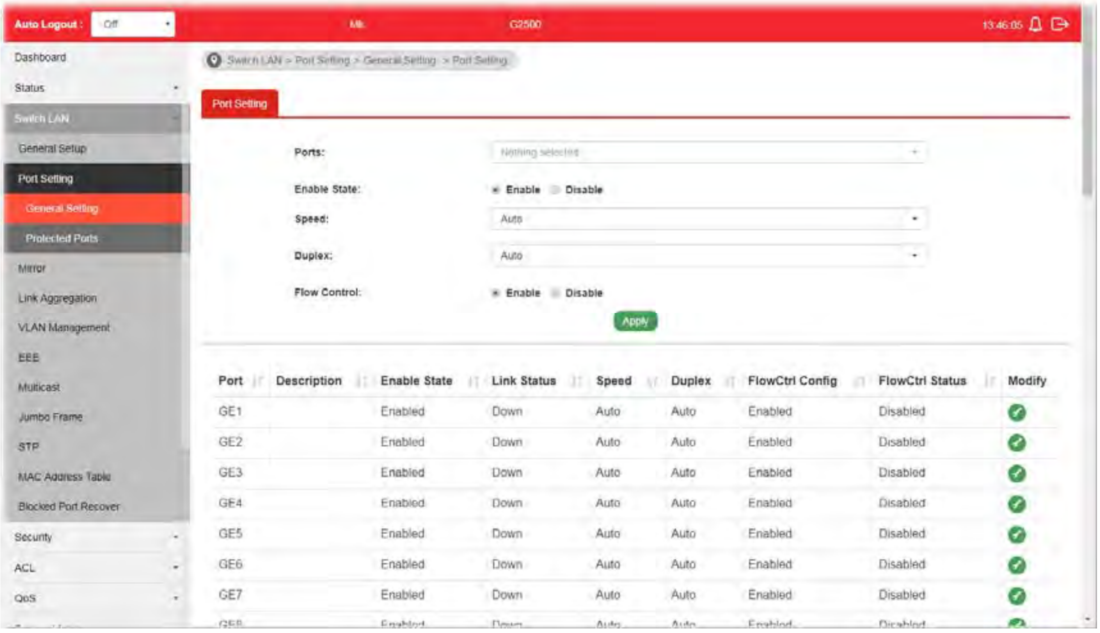
Available settings are explained as follows:

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	Apply the settings to the switch.

II-2 Port Setting

II-2-1 General 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

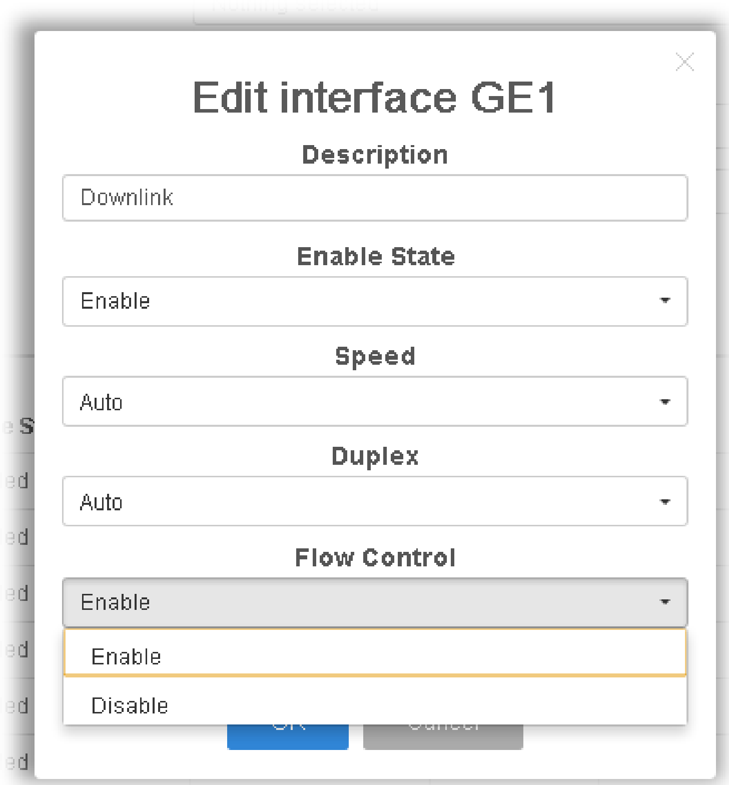
Duplex: Auto

Flow Control: ● Enable ○ Disable

Port	Description	Enable State	Link Status	Speed	Duplex	FlowCtrl Config	FlowCtrl Status	Modify
GE1		Enabled	Down	Auto	Auto	Enabled	Disabled	✓
GE2		Enabled	Down	Auto	Auto	Enabled	Disabled	✓
GE3		Enabled	Down	Auto	Auto	Enabled	Disabled	✓
GE4		Enabled	Down	Auto	Auto	Enabled	Disabled	✓
GE5		Enabled	Down	Auto	Auto	Enabled	Disabled	✓
GE6		Enabled	Down	Auto	Auto	Enabled	Disabled	✓
GE7		Enabled	Down	Auto	Auto	Enabled	Disabled	✓
GE8		Enabled	Down	Auto	Auto	Enabled	Disabled	✓

Available settings are explained as follows:

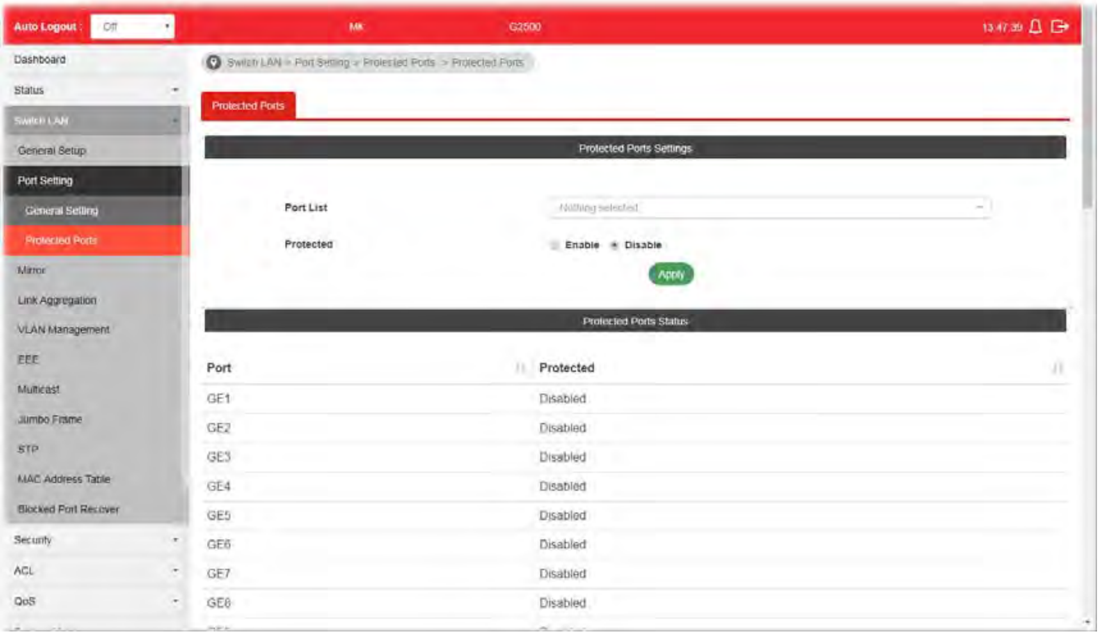
Item	Description
Ports	Use the drop down list to selelct one or more LAN port(s).
Enable State	**Enable -**Click it to enable the port. **Disable -** Click it to disable the port.
Speed	Port speed capabilities: ● **Auto:** Auto speed with all capabilities. ● **Auto-10M:** Auto speed with 10M ability 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	Apply the settings to the switch.
Modify	It is used to manually enter the description, state, speed, duplex, flow control for the port.  Edit interface GE1 Description: Downlink Enable State: Enable Speed: Auto Duplex: Auto Flow Control: Enable

II-2-2 Protected Ports

This page allows the network administrator to configure protected port setting to prevent the selected ports from communication with each other. Protected port is only allowed to communicate with unprotected port.

For example, GE1 and GE3 are selected in Port List and Enable is clicked as Protected, then users behind GE1 and GE3 are separated and can not communicate with each other.



Protected Ports Settings

Port List: Nothing selected

Protected: ○ Enable ● Disable

Apply

Protected Ports Status

Port	Protected
GE1	Disabled
GE2	Disabled
GE3	Disabled
GE4	Disabled
GE5	Disabled
GE6	Disabled
GE7	Disabled
GE8	Disabled

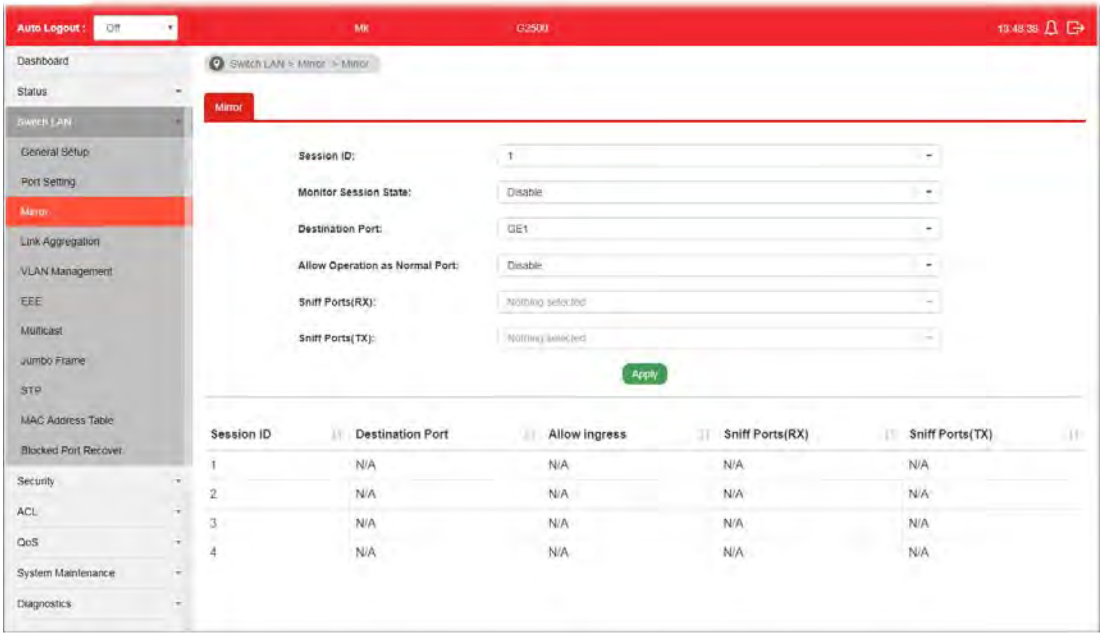
Available settings are explained as follows:

Item	Description
Protected Ports Settings	● **Port List -** Use the drop down list to select the port(s) (GE1 to GE50) for applying the settings configured in this page. ● **Protected -** Click **Enable** to activate the protected port function. ● **Apply** - The modification made above can be applied on to the selected GE port immediately.
Protected Port Status	Display current status for each GE port.

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
3	N/A	N/A	N/A	N/A
4	N/A	N/A	N/A	N/A

Available settings are explained as follows:

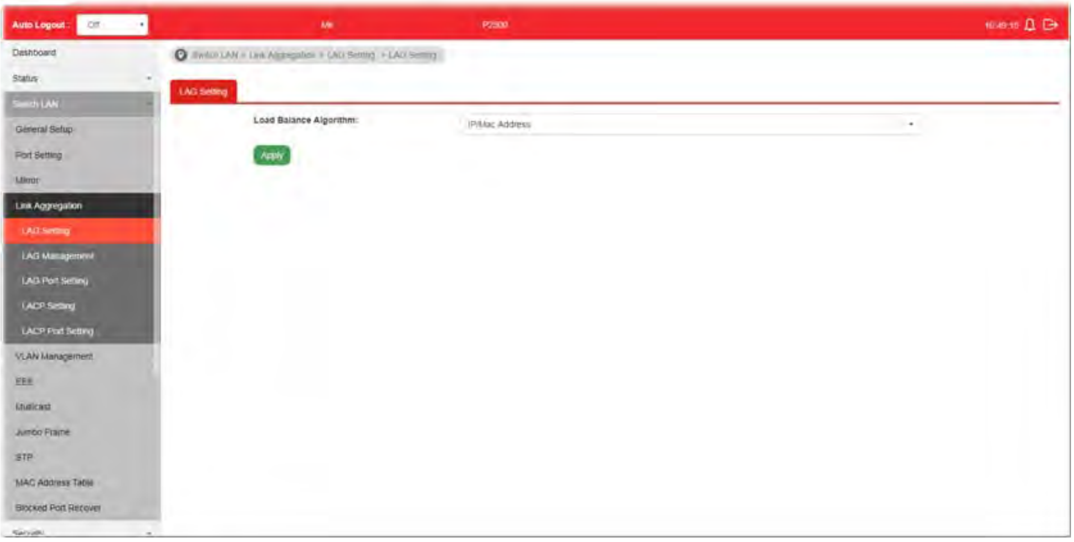
Item	Description
Session ID	Select the session ID (profile 1 to 4) of mirror operation you wish to configure.
Monitor Session State	● **Enable** – Enable specified mirror session. ● **Disable** - Disable specified mirror session.
Destination Port	Specify the port where you wish to observe the mirrored 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	Apply the settings 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.



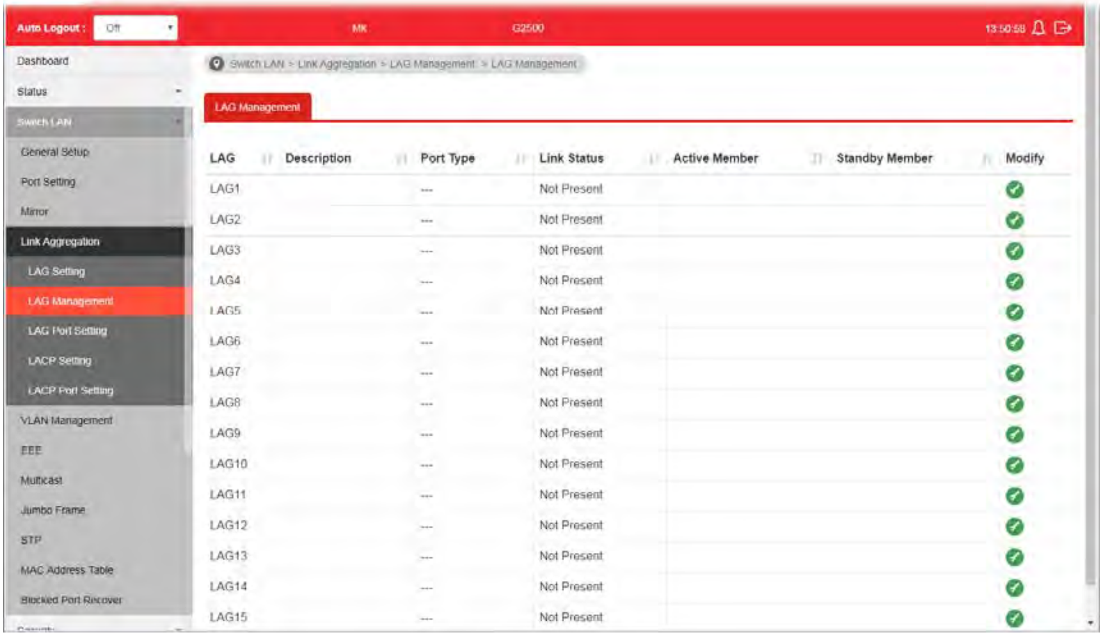
Load Balance Algorithm: IP/Mac Address

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	Apply the settings to the switch.

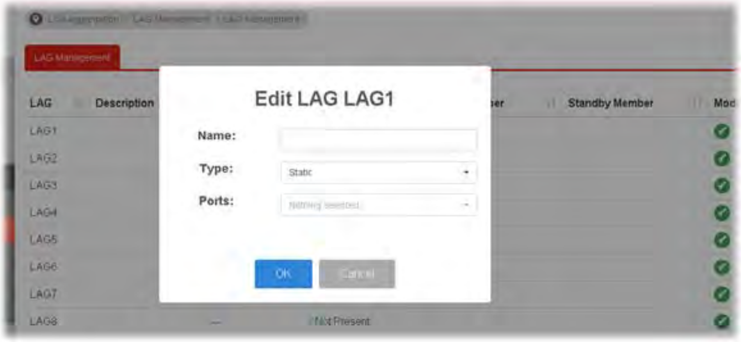
II-4-2 LAG Management

There are eight LAG profiles allowed to group different physical ports (GE1 to GE50). 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			✓
LAG9		---	Not Present			✓
LAG10		---	Not Present			✓
LAG11		---	Not Present			✓
LAG12		---	Not Present			✓
LAG13		---	Not Present			✓
LAG14		---	Not Present			✓
LAG15		---	Not Present			✓

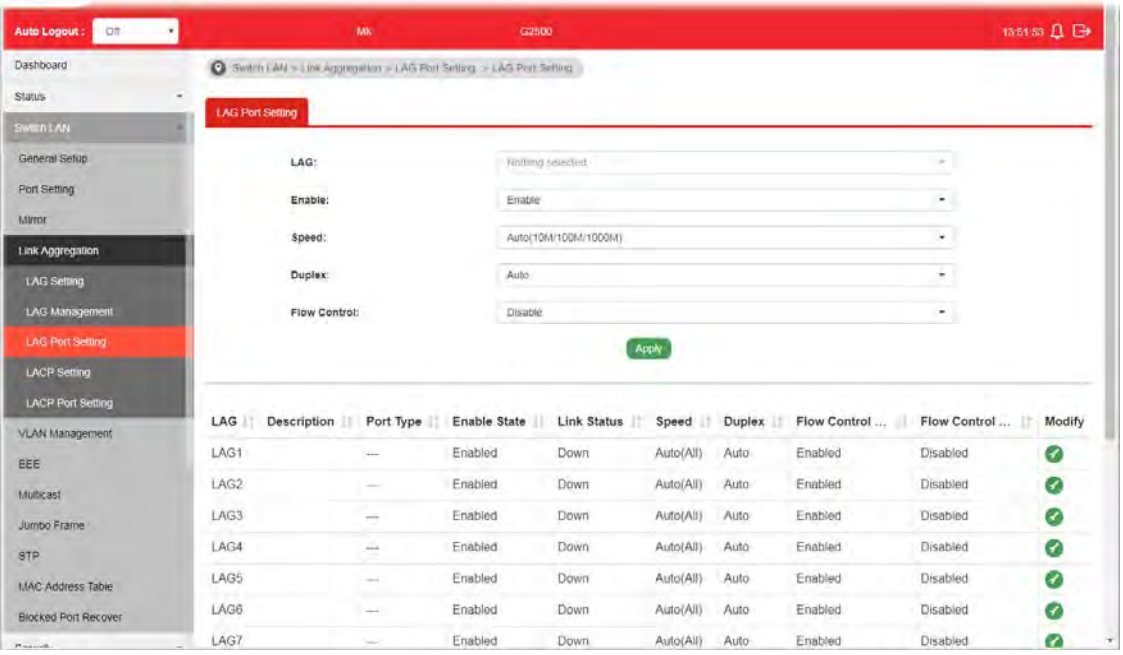
Available settings are explained as follows:

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 LAG16), including data speed and enabling/disabling the flow control.



LAG: Nothing selected

Enable: Enable

Speed: Auto(10M/100M/1000M)

Duplex: Auto

Flow Control: Disable

LAG	Description	Port Type	Enable State	Link Status	Speed	Duplex	Flow Control ...	Flow Control ...	Modify
LAG1		—	Enabled	Down	Auto(All)	Auto	Enabled	Disabled	✓
LAG2		—	Enabled	Down	Auto(All)	Auto	Enabled	Disabled	✓
LAG3		—	Enabled	Down	Auto(All)	Auto	Enabled	Disabled	✓
LAG4		—	Enabled	Down	Auto(All)	Auto	Enabled	Disabled	✓
LAG5		—	Enabled	Down	Auto(All)	Auto	Enabled	Disabled	✓
LAG6		—	Enabled	Down	Auto(All)	Auto	Enabled	Disabled	✓
LAG7		—	Enabled	Down	Auto(All)	Auto	Enabled	Disabled	✓

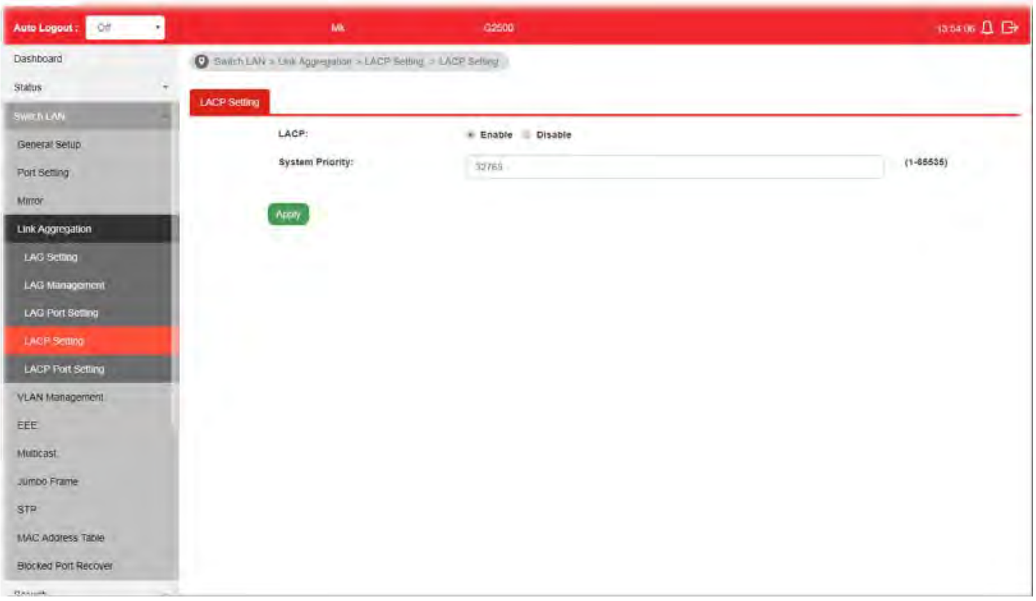
Available settings are explained as follows:

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. ● 10G: Force speed with 10G 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 /10G 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	Apply the settings to the switch.
Modify	It is used to edit status, speed, and flow control for the LAG.

II-4-4 LACP Setting

This page allows the network administrator to enable or disable the LACP function.



LACP: ● Enable ○ Disable

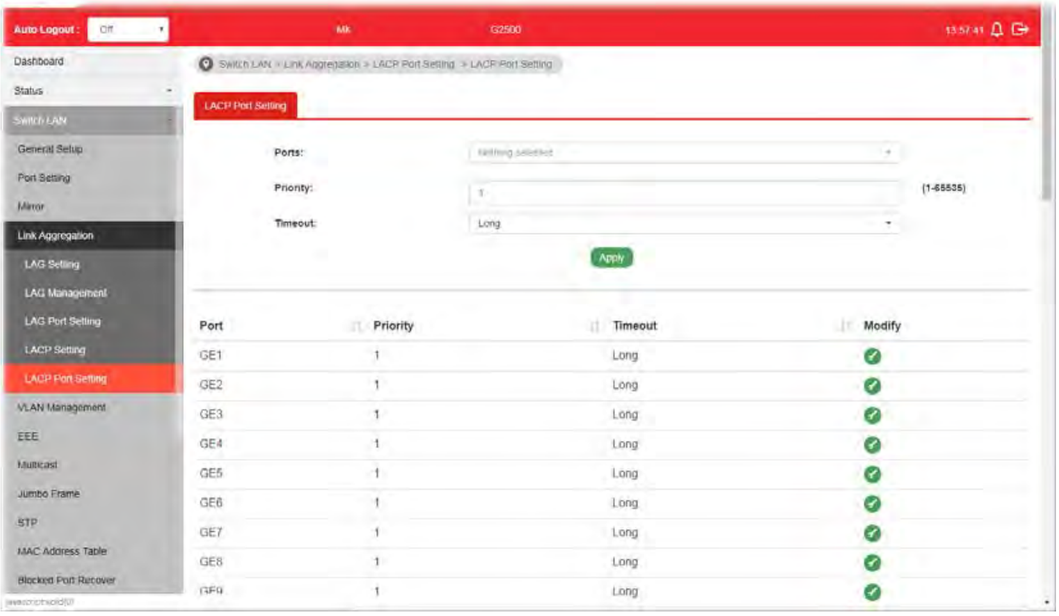
System Priority: 32768 (1-65535)

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	Apply the settings 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	Modify
GE1	1	Long	✓
GE2	1	Long	✓
GE3	1	Long	✓
GE4	1	Long	✓
GE5	1	Long	✓
GE6	1	Long	✓
GE7	1	Long	✓
GE8	1	Long	✓
GE9	1	Long	✓

Available settings are explained as follows:

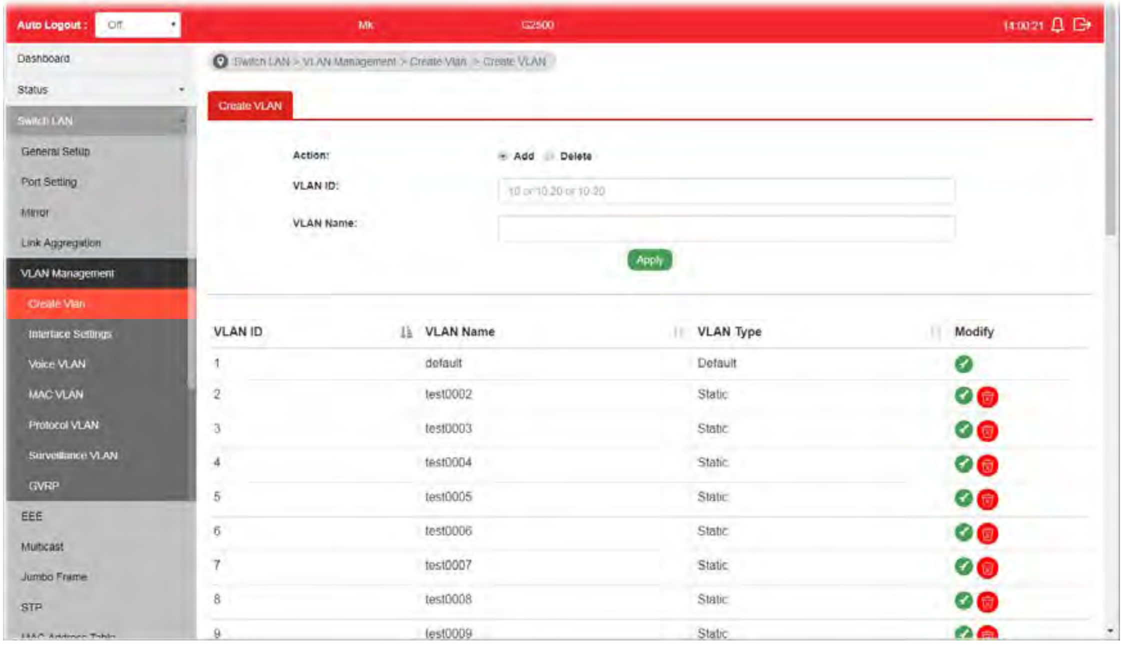
Item	Description
Ports	Use the drop down list to specify LAN Port.
Priority	Enter a port priority number for the port.
Timeout	The timeout option decides how local switch of LAG connection determines connection to be lost. Switch would also notify the remote switch about this setting value, so that remote 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	Apply the settings to the switch.
Modify	It is used to edit settings (priority and timeout) for LACP port.

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.



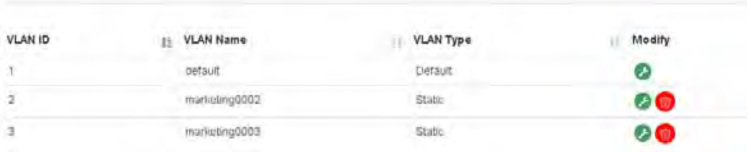
Action: ● Add ○ Delete

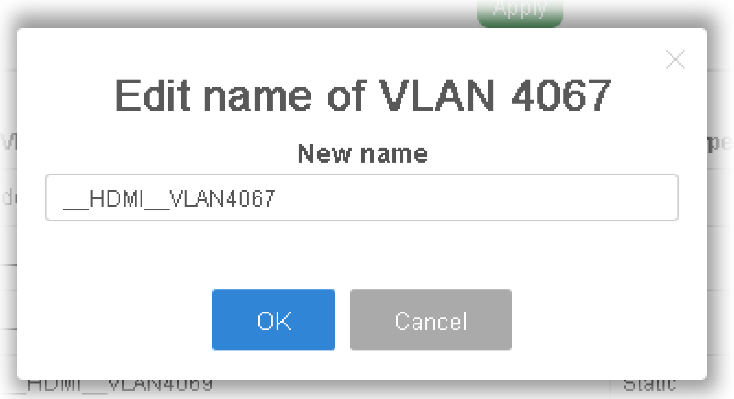
VLAN ID: 10 or 10,20 or 10-20

VLAN Name:

VLAN ID	VLAN Name	VLAN Type	Modify
1	default	Default	✓
2	test0002	Static	✓ 🗑
3	test0003	Static	✓ 🗑
4	test0004	Static	✓ 🗑
5	test0005	Static	✓ 🗑
6	test0006	Static	✓ 🗑
7	test0007	Static	✓ 🗑
8	test0008	Static	✓ 🗑
9	test0009	Static	✓ 🗑

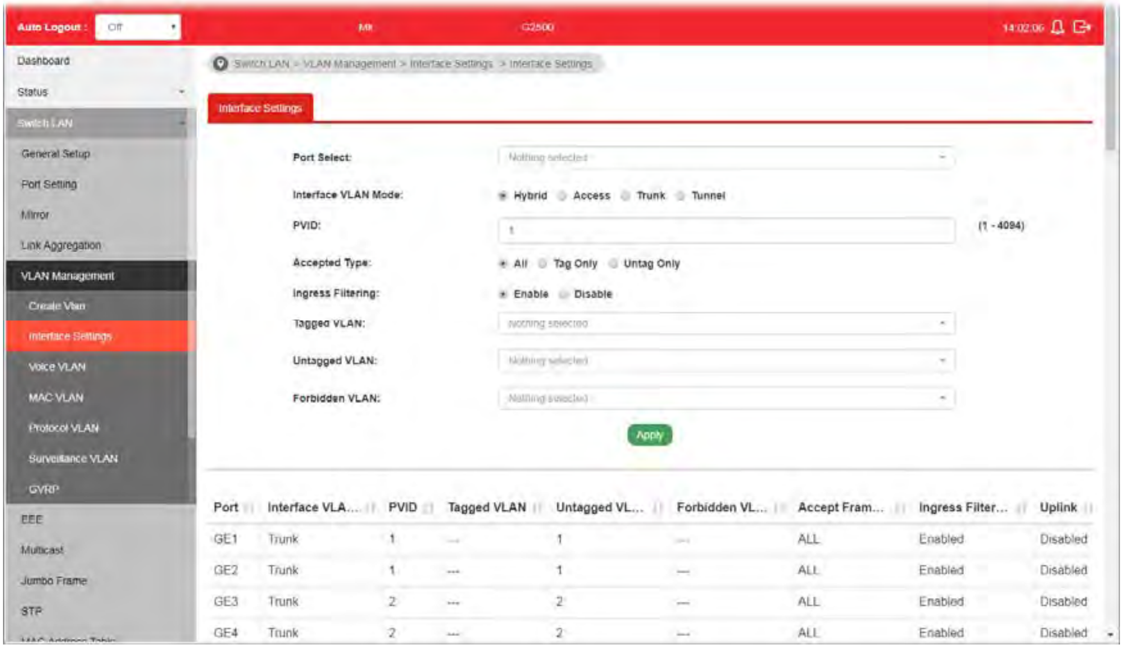
Available settings are explained as follows:

Item	Description
Action	Select which action to perform, add VLANs or delete VLANs. ● **Add** – Create a new VLAN profile. ● **Delete** – Delete an existed VLAN profile.
VLAN ID	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	Enter the prefix you wish to add followed by VLAN ID as VLAN name. Leave it empty for using default "VLAN". After clicking Apply, you will see:  VLAN ID – VLAN Name – VLAN Type – Modify 1 – default – Default – ✓ 2 – marketing0002 – Static – ✓ 🗑 3 – marketing0003 – Static – ✓ 🗑

Apply	Apply the settings to the switch.
Modify	🔧 - Modify the name of the selected VLAN ID.  Edit name of VLAN 4067 New name: __HDMI__VLAN4067 ● **New Name -** Type a name for such VLAN profile. ● **OK** - Apply the settings 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 ○ Tunnel

PVID: 1 (1 - 4094)

Accepted Type: ● All ○ Tag Only ○ Untag Only

Ingress Filtering: ● Enable ○ Disable

Tagged VLAN: Nothing selected

Untagged VLAN: Nothing selected

Forbidden VLAN: Nothing selected

Port	Interface VLA...	PVID	Tagged VLAN	Untagged VL...	Forbidden VL...	Accept Fram...	Ingress Filter...	Uplink
GE1	Trunk	1	---	1	---	ALL	Enabled	Disabled
GE2	Trunk	1	---	1	---	ALL	Enabled	Disabled
GE3	Trunk	2	---	2	---	ALL	Enabled	Disabled
GE4	Trunk	2	---	2	---	ALL	Enabled	Disabled

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 802.1Q

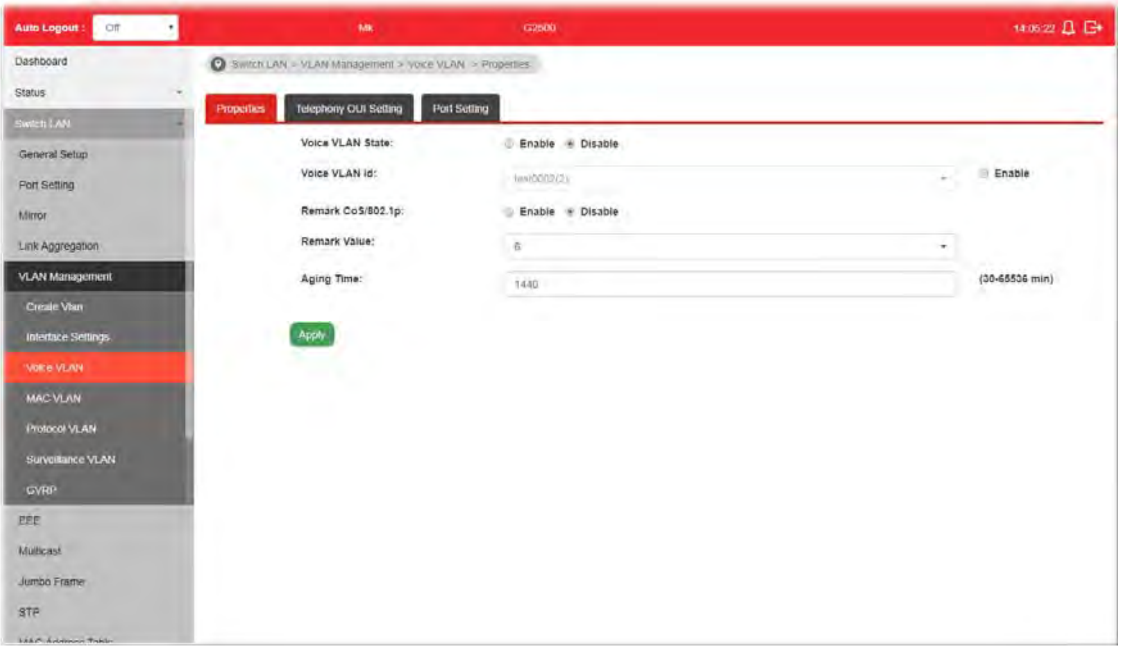
	specification. ● **Access** – Accept only untagged frames and join an untagged VLAN. ● **Trunk** - An untagged member of one VLAN at most, and is a tagged member of zero or more VLANs.
PVID	A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are 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	Apply the settings to the switch.
Modify	🔧 - It is used to edit settings for the selected port.

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: ○ Enable ● Disable

Voice VLAN id: test0002(2) □ Enable

Remark CoS/802.1p: ○ Enable ● Disable

Remark Value: 6

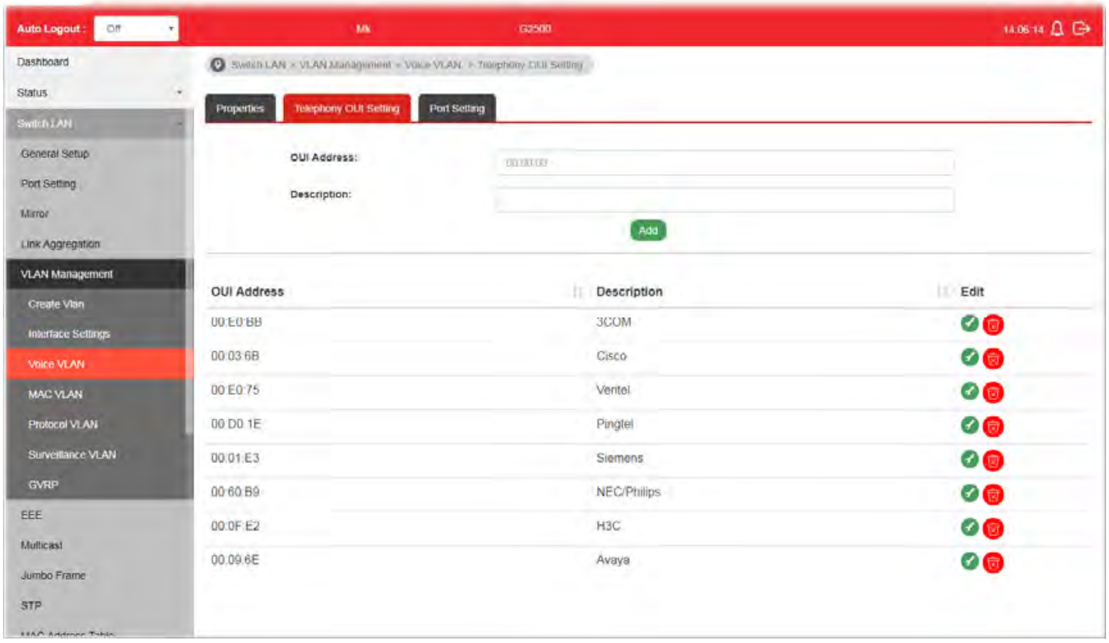
Aging Time: 1440 (30-65536 min)

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	Apply the settings 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.

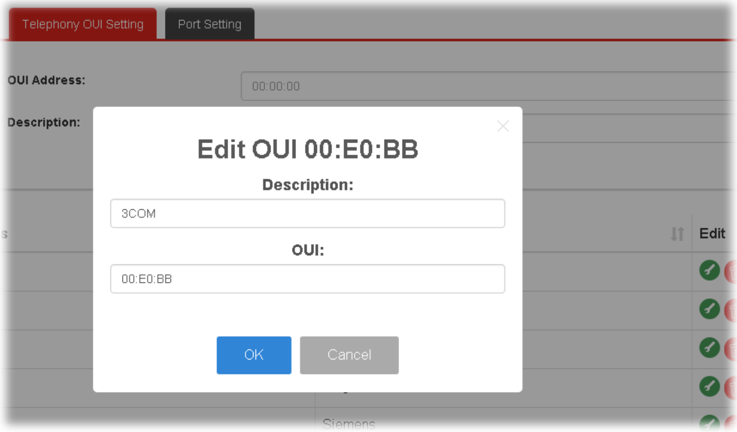


OUI Address: 00:00:00

Description:

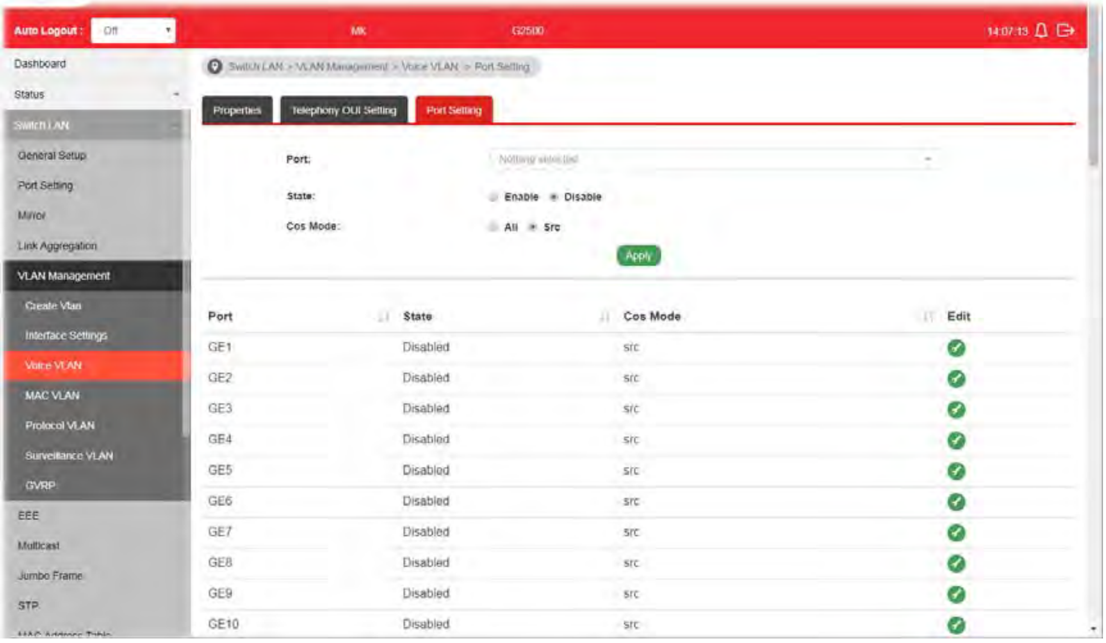
OUI Address	Description	Edit
00:E0:BB	3COM	✓ 🗑
00:03:6B	Cisco	✓ 🗑
00:E0:75	Veritel	✓ 🗑
00:D0:1E	Pingtel	✓ 🗑
00:01:E3	Siemens	✓ 🗑
00:60:B9	NEC/Philips	✓ 🗑
00:0F:E2	H3C	✓ 🗑
00:09:6E	Avaya	✓ 🗑

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.
Modify	🔧 - Modify OUI setting for voice VLAN.  Telephony OUI Setting Port Setting OUI Address: 00:00:00 Description: Edit OUI 00:E0:BB Description: 3COM OUI: 00:E0:BB OK Cancel 🗑 - 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: Nothing selected

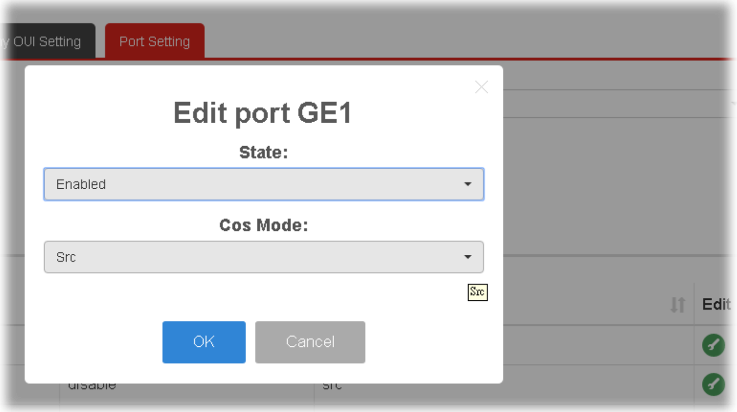
State: ○ Enable ● Disable

Cos Mode: ○ All ● Src

Port	State	Cos Mode	Edit
GE1	Disabled	src	✓
GE2	Disabled	src	✓
GE3	Disabled	src	✓
GE4	Disabled	src	✓
GE5	Disabled	src	✓
GE6	Disabled	src	✓
GE7	Disabled	src	✓
GE8	Disabled	src	✓
GE9	Disabled	src	✓
GE10	Disabled	src	✓

Available settings are explained as follows:

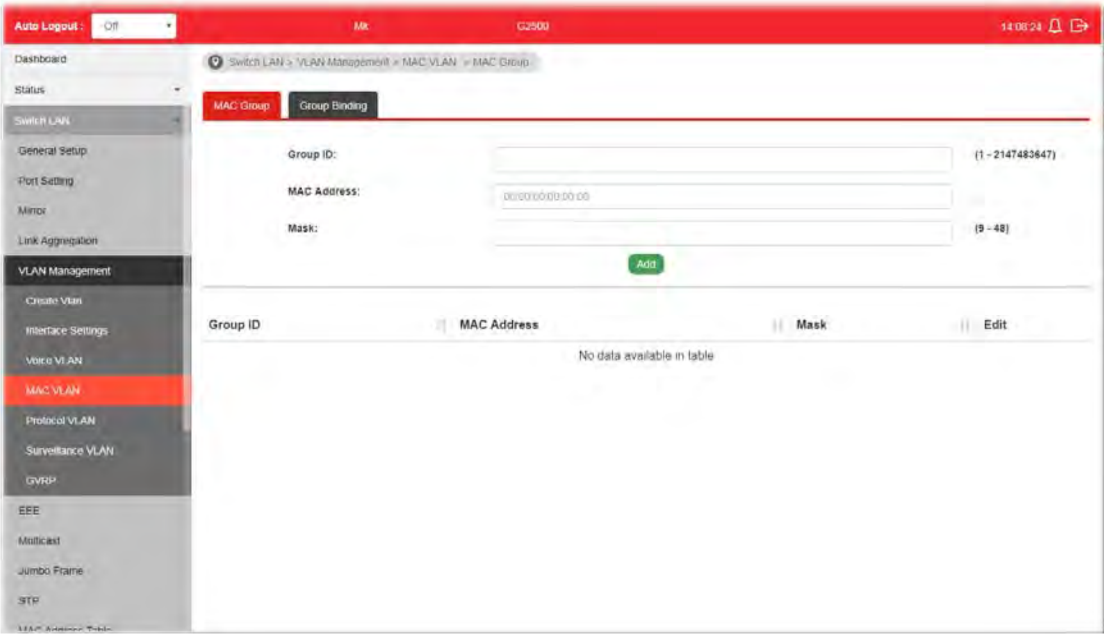
Item	Description
Port	Use the drop down list to specify one or more LAN ports.
State	● **Enabled** – Click it to enable the port settings for Voice LAN. ● **Disabled** – Click it to disable the port settings for Voice LAN.
Cos Mode	If **Remark CoS/802.1p** is enabled in **Voice VLAN>>Propertie**s, settings 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	Apply the settings to the switch.
Edit	Click the icon under **Edit** for one entry to modify port settings (State, Cos Mode) for voice VLAN.

	 Edit port GE1 State: Enabled Cos Mode: Src

II-5-4 MAC VLAN

II-5-4-1 MAC Group

The MAC VLAN allows you to statically assign a VLAN ID to a host with specific MAC address(es). VigorSwitch allows you configure multiple groups with configured MAC address and mask to be active on ports and to be bound with VLAN ID. This page allows the network administrator to define groups with specific MAC addresses for later binding with VLAN and Port.



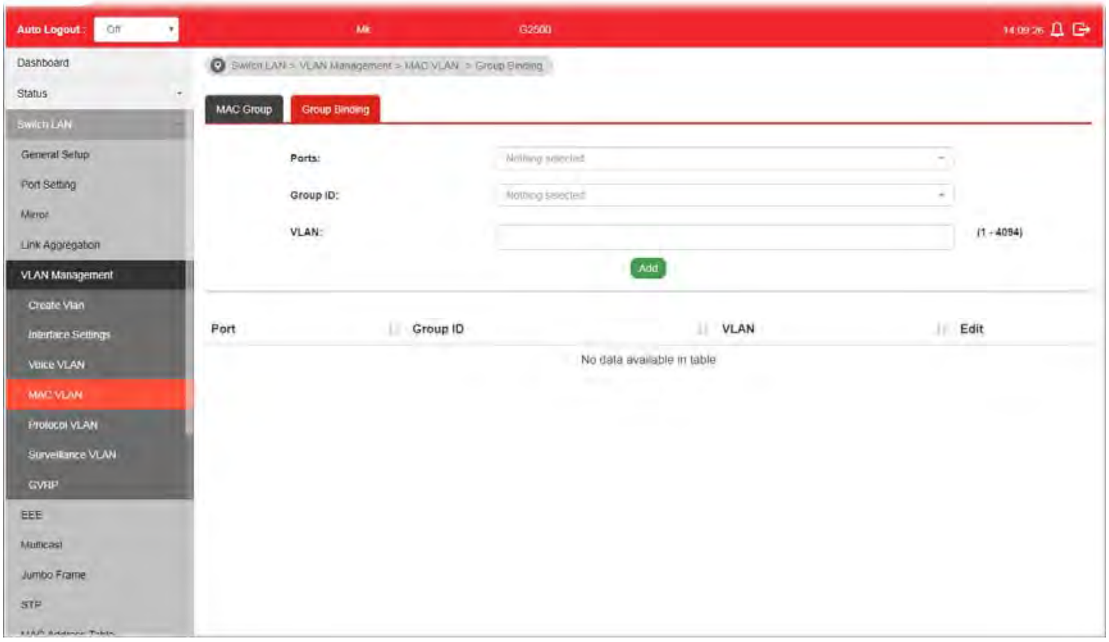
Available settings are explained as follows:

Item	Description
Group ID	It is a number for identification later, while chosen to be bound with VLAN/Port.
MAC Address	Enter the MAC address you wish to be classified in this group
Mask	The mask is the length of matching prefix you wish to have on MAC address. For example, configure mask in 10. It means a host with beginning of the 10-digit of MAC address will be checked, and classified into this group if matched.

Add	Click it to create a new MAC group profile based on the settings configured above.
Edit	Click the icon under **Edit** for one entry to modify settings for group ID.

II-5-4-2 Group Binding

The MAC VLAN allows you to statically assign a VLAN ID to a host with specific MAC address(es). VigorSwitch allows you to configure multiple groups with configured MAC address and mask to be active on ports and to be bound with VLAN ID. This page allows the network administrator to bind the group of specified MAC addresses with VLAN and Port.



Ports: Nothing selected

Group ID: Nothing selected

VLAN: (1 - 4094)

Port	Group ID	VLAN	Edit
No data available in table			

Available settings are explained as follows:

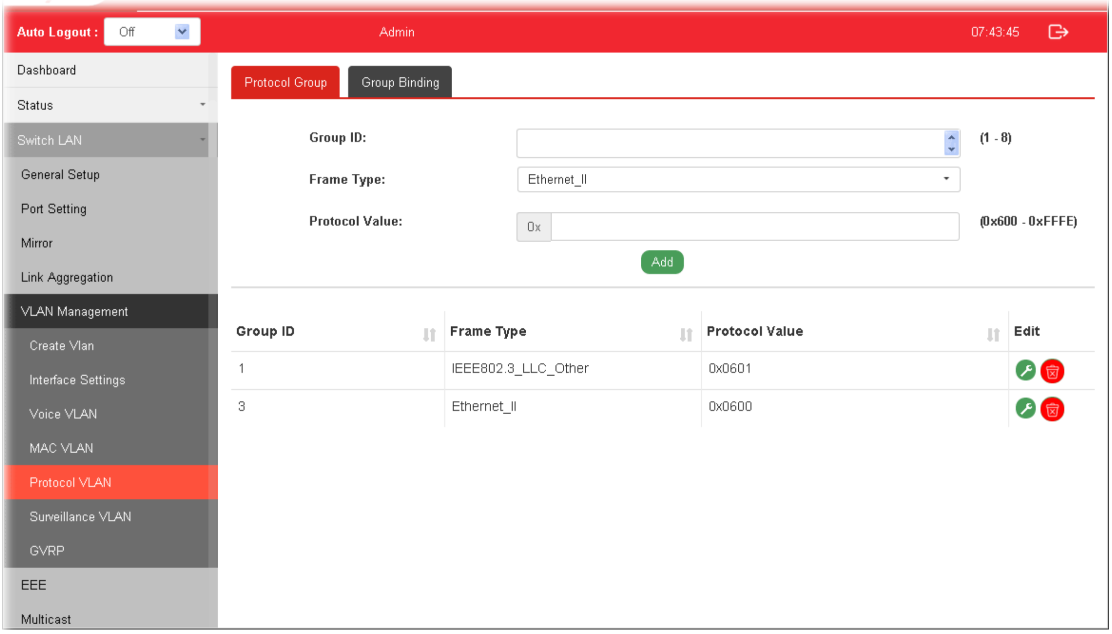
Item	Description
Ports	Select the ports you wish to be bound with specified MAC address group.
Group ID	Choose the group ID you have created in earlier section, which specified a group of host by MAC address and its mask.
VLAN	Enter the VLAN ID that you wish to be bound with.
Add	Click it to create a new MAC group binding profile based on the settings configured above.
Edit	Click the icon under **Edit** for one entry to modify settings for selected port profile.

II-5-5 Protocol VLAN

VigorSwitch offers protocol VLANs which allows Network Administrator to filter out untagged traffic of certain protocol and then assign them a specific VLAN ID.

II-5-5-1 Protocol Group

Up to eight protocol groups can be defined, each of them can have a unique filtering criteria such as frame type and protocol value.



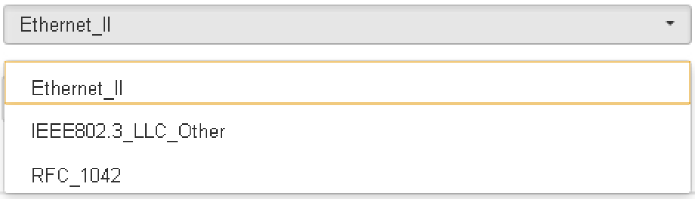
Group ID: (1 - 8)

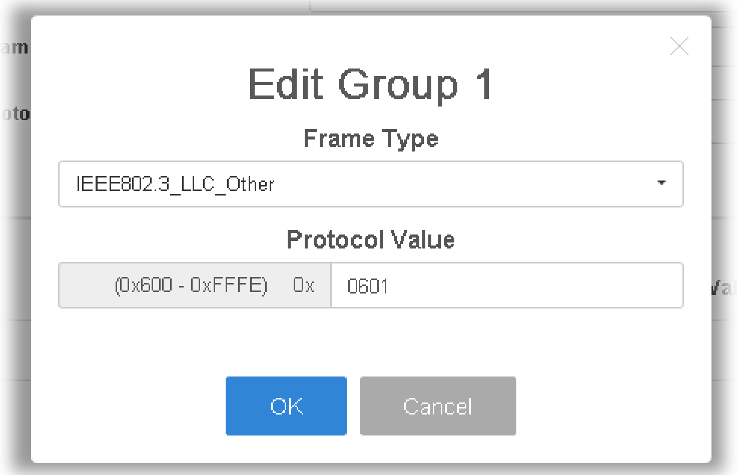
Frame Type: Ethernet_II

Protocol Value: 0x (0x600 - 0xFFFE)

Group ID	Frame Type	Protocol Value	Edit
1	IEEE802.3_LLC_Other	0x0601	
3	Ethernet_II	0x0600	

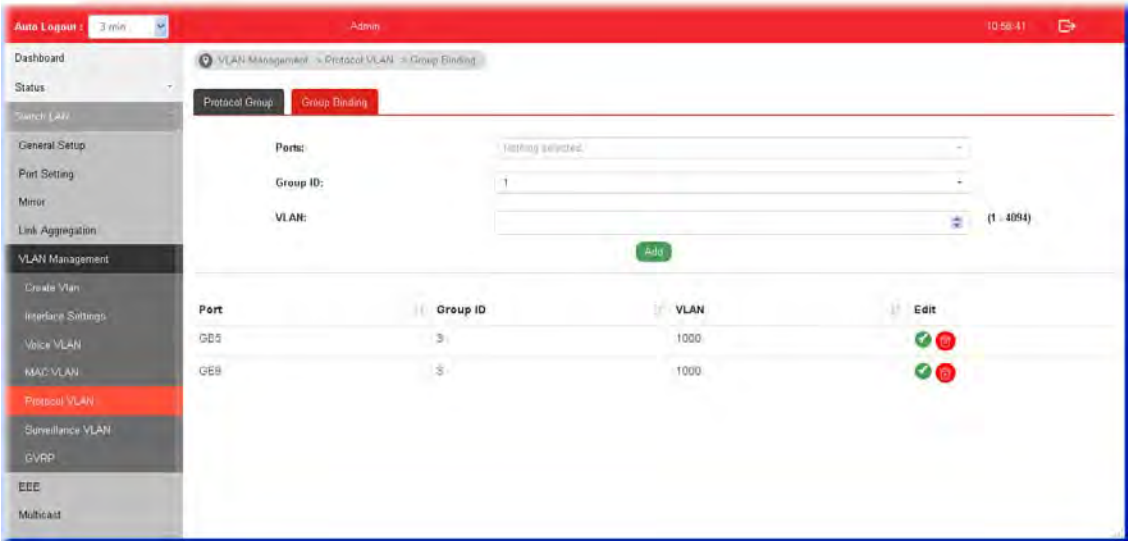
Available settings are explained as follows:

Item	Description
Group ID	It is a number for identification while bounding with VLAN/Port.
Frame Type	Use the drop-down list to specify the frame type which you would like to filter.  Ethernet_II Ethernet_II IEEE802.3_LLC_Other RFC_1042 ● Ethernet_II - Packet will be mapped based on Ethernet version 2. ● IEEE802.3_LLC_Other –Packet will be mapped based on 802.3 packet with LLC other header. ● RFC_1042 - Packet will be mapped based on RFC 1042.
Protocol Value	Input a value (ranging from 0x600 ~0xFFFE). Packets match with such value will be classified into this group.
Add	Click it to create a new protocol group profile based on the settings configured above.

Edit	- Modify setting for selected group.  Edit Group 1 Frame Type: IEEE802.3_LLC_Other Protocol Value: (0x600 - 0xFFFE) 0x 0601 - Click it to remove the group.

II-5-5-2 Group Binding

This page is for setting up the ports and protocol group that we would like to filter, and the VLAN ID we would like to assign.



Ports: Nothing selected

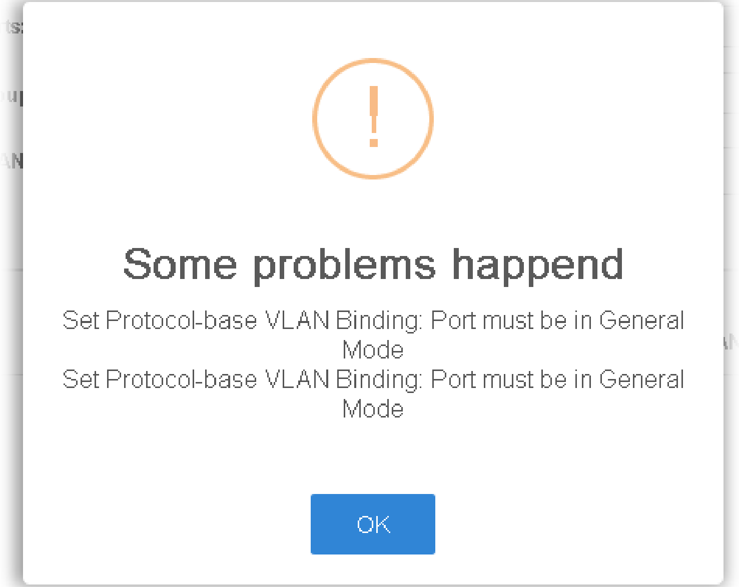
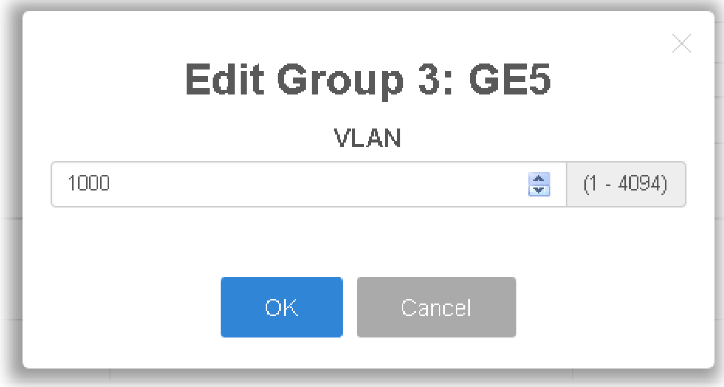
Group ID: 1

VLAN: (1 - 4094)

Port	Group ID	VLAN	Edit
GE5	3	1000	
GE8	3	1000	

Available settings are explained as follows:

Item	Description
Ports	Use the drop-down list to select one or more ports for applying protocol-based VLAN. Note that protocol-based VLAN can only be applied to the ports of which Interface VLAN Mode (at VLAN Management >> Interface Settings) is set to "Hybrid".
Group ID	Select the protocol group defined in Protocol Group setup.
VLAN	Use drop down list to choose a value as VLAN number.
Add	Add the above settings to the switch. Before using **Add**, open **Switch LAN>>VLAN**

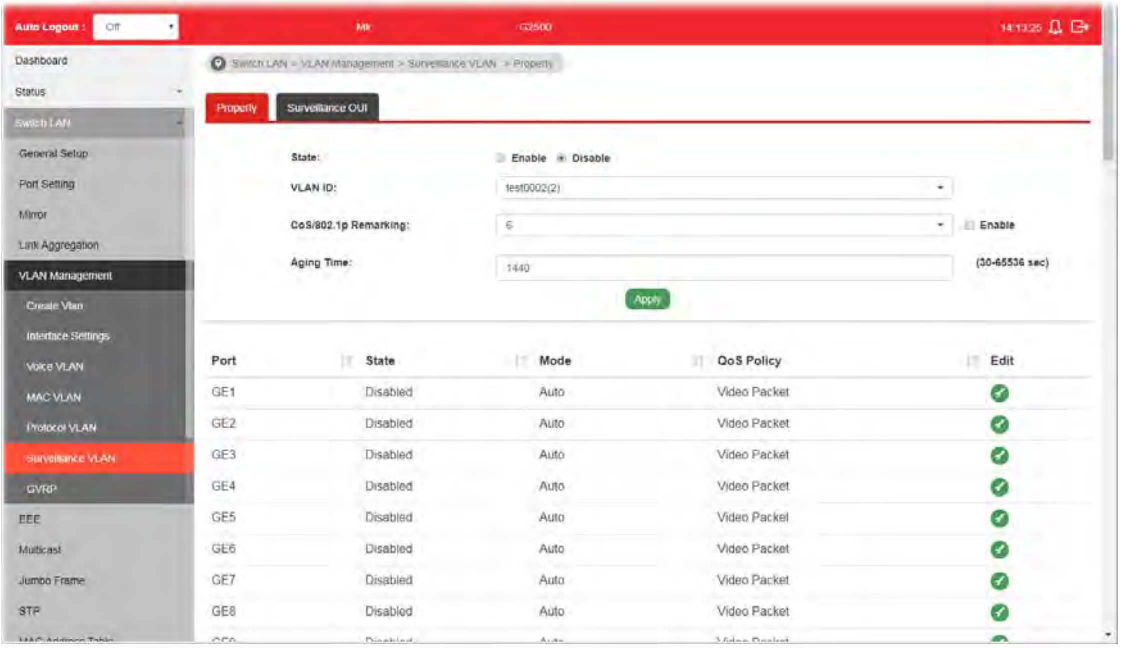
	Management>>Interface Settings to specify **Hybrid** as **Interface VLAN Mode** for the GE ports first. Otherwise, the following error message will appear.  Some problems happend Set Protocol-base VLAN Binding: Port must be in General Mode Set Protocol-base VLAN Binding: Port must be in General Mode
Edit	🔧 - Modify setting for the selected group.  Edit Group 3: GE5 VLAN: 1000 (1 - 4094) 🗑 - Click it to remove the selected group.

II-5-6 Surveillance VLAN

Surveillance VLAN can be configured for VigorSwitch to identify the packets coming from an IP camera automatically and assign those traffics to a specific VLAN ID and CoS/802.1p value, this helps you to prioritize those traffics and improve video quality.

II-5-6-1 Property

This page is for setting up the VLAN to which the video traffic should be assigned and to enable/disable Surveillance VLAN on each port.



State: ○ Enable ● Disable

VLAN ID: test0002(2)

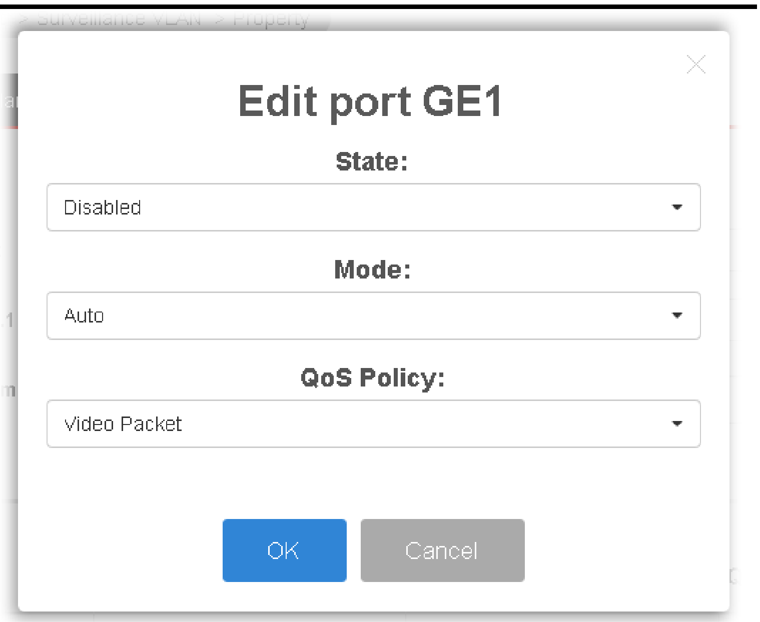
CoS/802.1p Remarking: 6 □ Enable

Aging Time: 1440 (30-65536 sec)

Port	State	Mode	QoS Policy	Edit
GE1	Disabled	Auto	Video Packet	✓
GE2	Disabled	Auto	Video Packet	✓
GE3	Disabled	Auto	Video Packet	✓
GE4	Disabled	Auto	Video Packet	✓
GE5	Disabled	Auto	Video Packet	✓
GE6	Disabled	Auto	Video Packet	✓
GE7	Disabled	Auto	Video Packet	✓
GE8	Disabled	Auto	Video Packet	✓

Available settings are explained as follows:

Item	Description
State	● **Enabled** – Click it to enable the port settings for such VLAN. ● **Disabled** – Click it to disable the port settings for such VLAN.
VLAN ID	Choose a VLAN profile (created in **Switch LAN>>VLAN Management>>Create Vlan**) as Surveillance VLAN.
CoS/802.1p Remarking	Specify the CoS/802.1p number you wish ingress packets be tagged with, so that QoS can prioritize it correctly. ● **Enable** - If enabled, qualified packets will be remarked by this value.
Aging Time	Unit is second. Select value of aging time (30~65536 seconds). Default is 1440 seconds. VLAN entry will be aged out after this time if no packet passes through.
Apply	Apply the settings to the switch.
Edit	✓ - Click it to modify port setting status.



Edit port GE1

State: Disabled

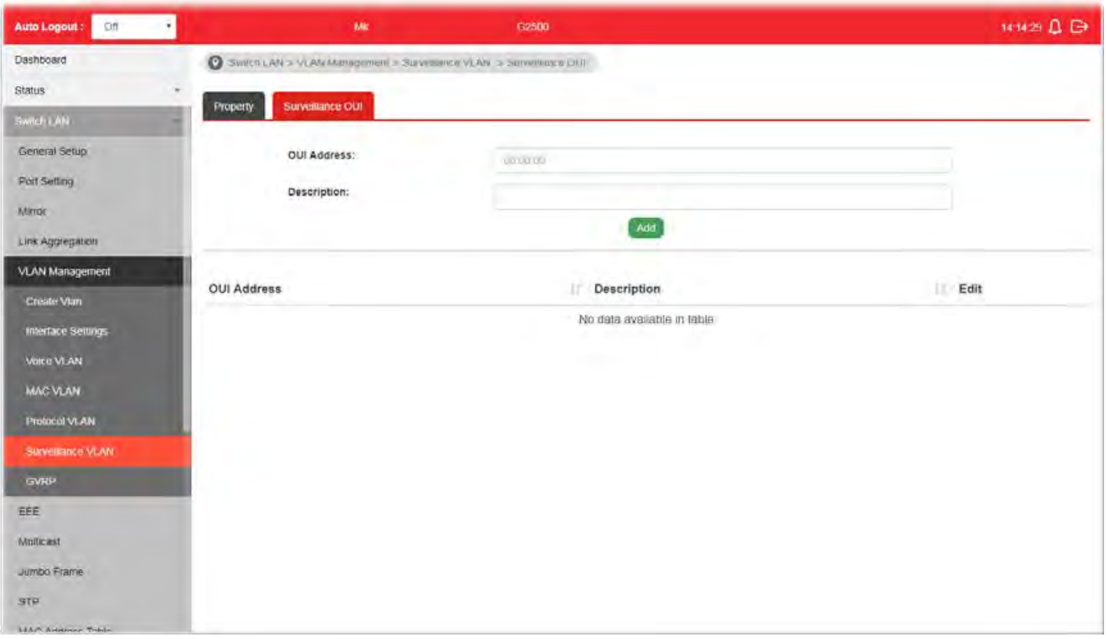
Mode: Auto

QoS Policy: Video Packet

- **State** –Set it to enable surveillance VLAN function of interface.
- **Mode** –Select port surveillance VLAN mode.
  - **Auto**: Surveillance VLAN auto detect packets that match OUI table and add received port into surveillance VLAN ID tagged member.
  - **Manual**: User need add interface to VLAN ID tagged member manually.
- **QoS Policy** - Select port QoS Policy mode.
  - **Video Packet**: QoS attributes are applied to packets with OUI in the source MAC address.
  - **All**: QoS attributes are applied to packets that are classified to the Surveillance VLAN.
- **OK -** Apply the settings to the switch.
- **Cancel -** Abandon the changes and return to previous page.

II-5-6-1 Surveillance OUI

Filtering Surveillance traffic is based on the OUI of the IP cameras. Users can add, edit, and delete OUI on this page.



Available settings are explained as follows:

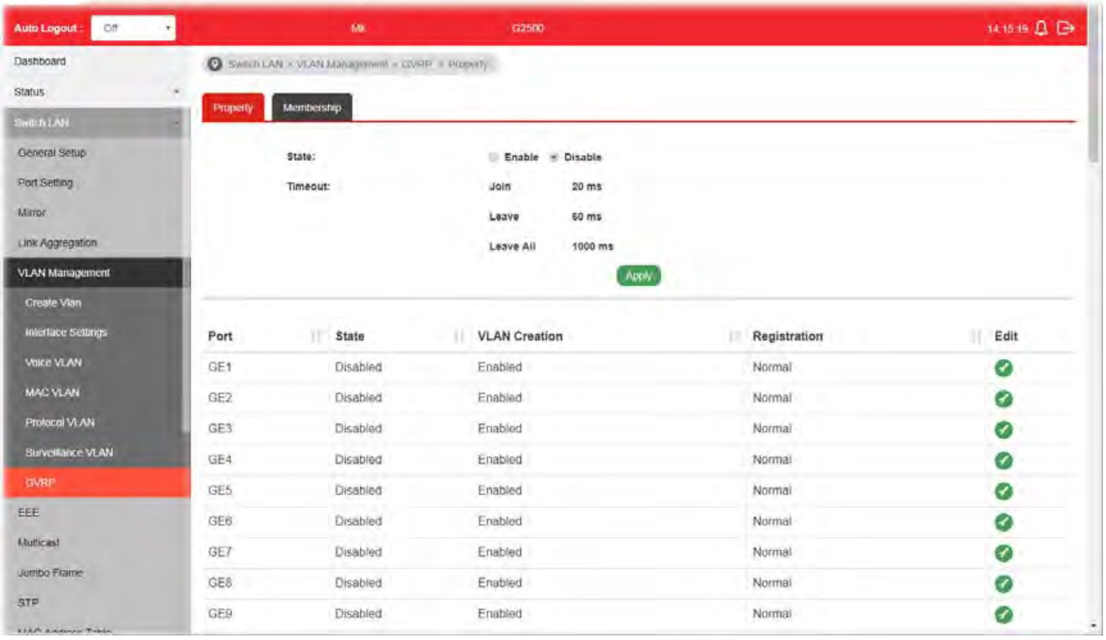
Item	Description
OUI Address	Enter OUI MAC address of monitored IP camera. It can't be edited in edit dialog.
Description	Enter a description of the specified MAC address to the surveillance VLAN OUI table.
Add	Click it to create a new voice OUI based on the settings configured above.
Edit	🔧 - Modify OUI setting for surveillance VLAN. 🗑 - Click it to remove the selected OUI entry.

II-5-7 GVRP

II-5-7-1 Property

This page allows the network administrator to configure registration mode (e.g., Normal, Fixed or Forbidden) of GVRP (GARP VLAN Registration Protocol) for each GE port.

Such function can eliminate unnecessary network traffic and prevent any attempt to transmit information to unregistered users.



State: ○ Enable ● Disable

Timeout:

Join 20 ms

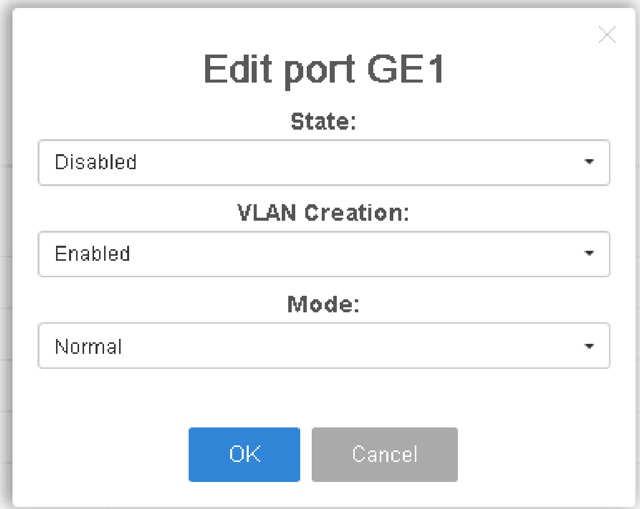
Leave 60 ms

Leave All 1000 ms

Port	State	VLAN Creation	Registration	Edit
GE1	Disabled	Enabled	Normal	✓
GE2	Disabled	Enabled	Normal	✓
GE3	Disabled	Enabled	Normal	✓
GE4	Disabled	Enabled	Normal	✓
GE5	Disabled	Enabled	Normal	✓
GE6	Disabled	Enabled	Normal	✓
GE7	Disabled	Enabled	Normal	✓
GE8	Disabled	Enabled	Normal	✓
GE9	Disabled	Enabled	Normal	✓

Available settings are explained as follows:

Item	Description
State	● **Enabled** – Click it to enable the port settings for such VLAN. ● **Disabled** – Click it to disable the port settings for such VLAN.
Timeout	Display the current time status for GVRP.
Apply	Apply the settings to the switch.
Edit	🔧 - Click it to modify settings for the selected port.



Edit port GE1

State: Disabled

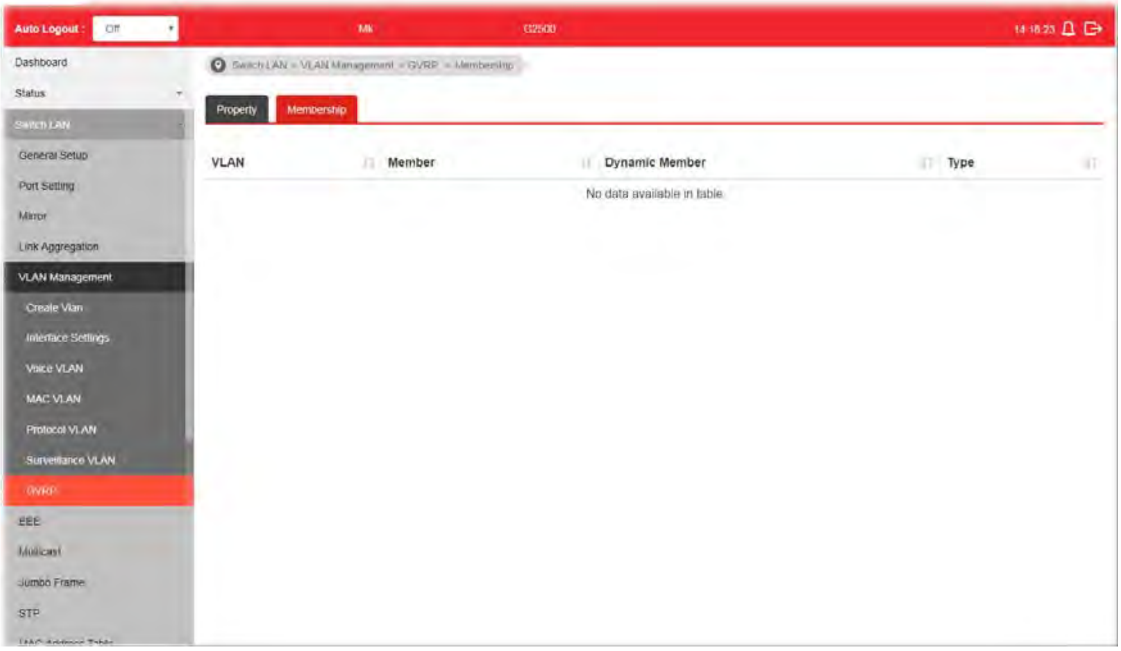
VLAN Creation: Enabled

Mode: Normal

- **State** – Select Enabled or Disabled for such port.
- **VLAN Creation** –Select Enabled or Disabled.
- **Mode** – There are three modes to be specified.
  - Normal – Default setting. All packets can pass through the selected GE port.
  - Fixed – The selected GE port only sends static VLAN information to neighboring device and allows static VLAN packet to pass through.
  - Forbidden – The selected GE port only allows default VLAN packet to pass through.

II-5-7-2 Membership

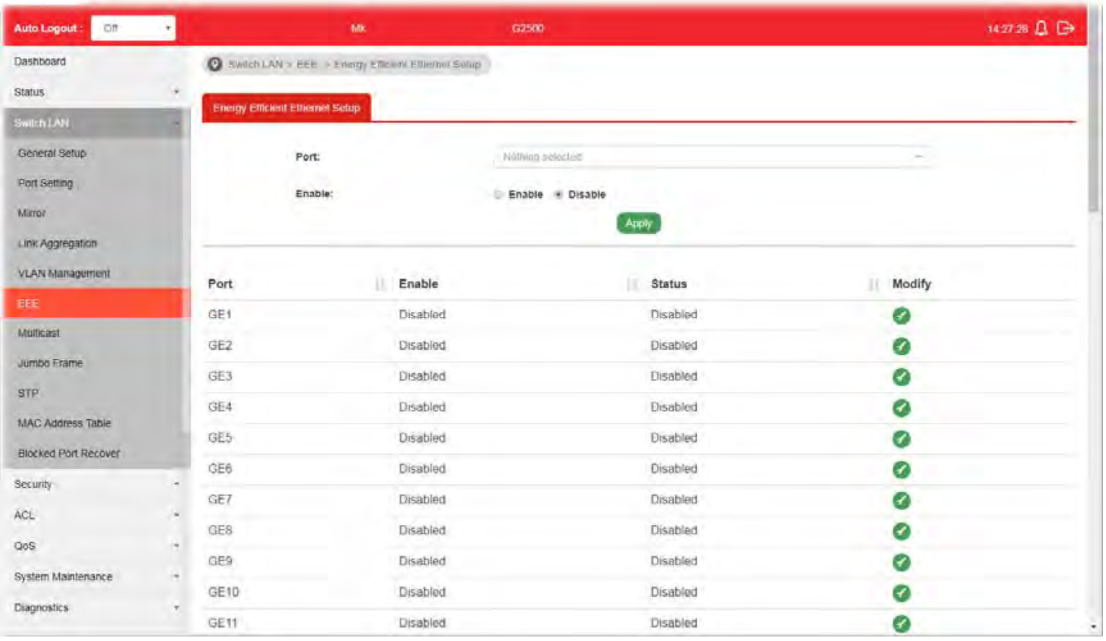
This page display information about membership for GVRP.



VLAN	Member	Dynamic Member	Type
No data available in table			

II-6 EEE

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



Port: Nothing selected

Enable: ○ Enable ● Disable

Port	Enable	Status	Modify
GE1	Disabled	Disabled	✓
GE2	Disabled	Disabled	✓
GE3	Disabled	Disabled	✓
GE4	Disabled	Disabled	✓
GE5	Disabled	Disabled	✓
GE6	Disabled	Disabled	✓
GE7	Disabled	Disabled	✓
GE8	Disabled	Disabled	✓
GE9	Disabled	Disabled	✓
GE10	Disabled	Disabled	✓
GE11	Disabled	Disabled	✓

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	Apply the settings to the switch.
Modify	🔧 - Click it to modify port setting status.

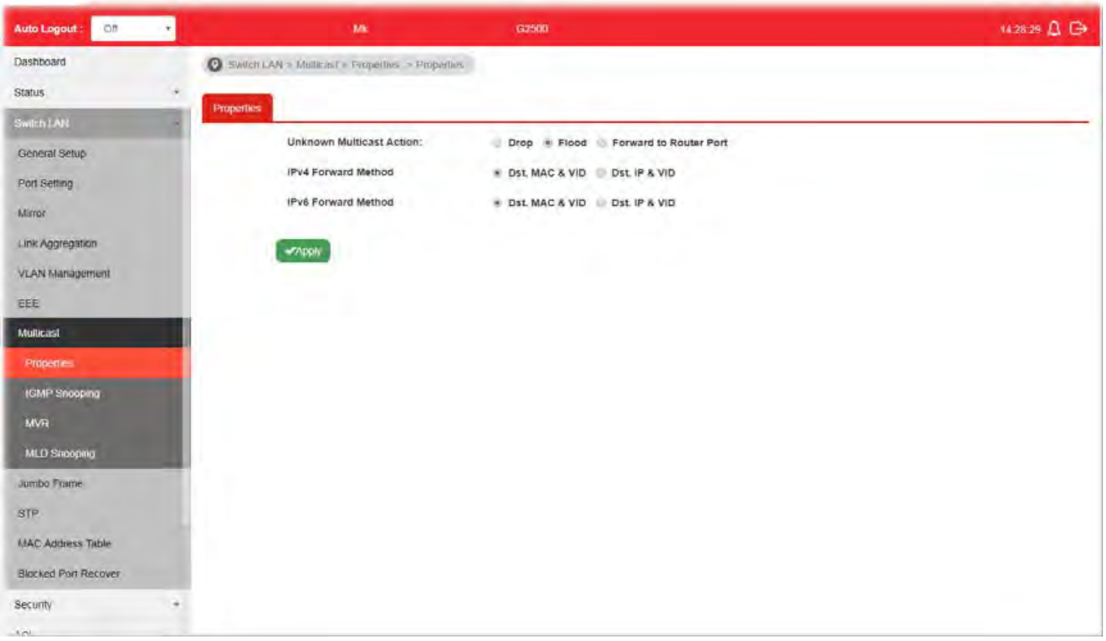
II-7 Multicast

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 network administrator to choose actions for processing the unknown mulititcast 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

IPv6 Forward Method ● Dst. MAC & VID ○ Dst. IP & VID

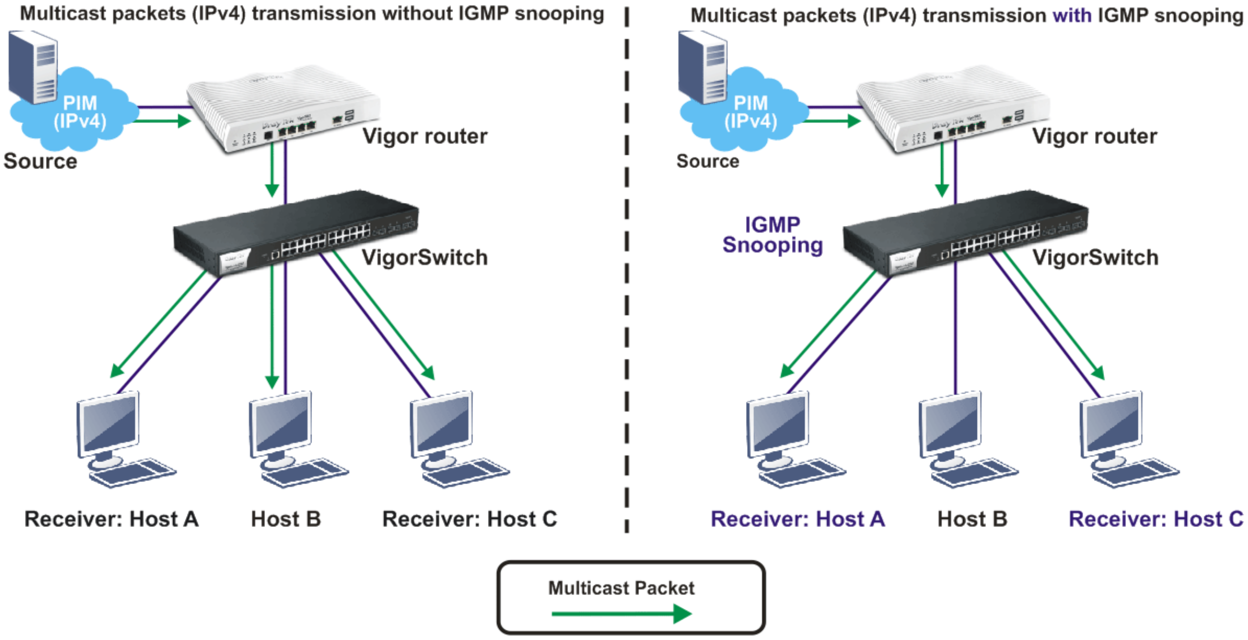
Available settings are explained as follows:

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.
IPv6 Forward Method	Set the IPv6 multicast forward method. ● **Dst. MAC & VID:** Forward using destination multicast MAC

	address and VLAN IDs. ● **Dst. IP & VID:** Forward using destination multicast IPv6 address and VLAN ID.
Apply	Apply the settings to the switch.

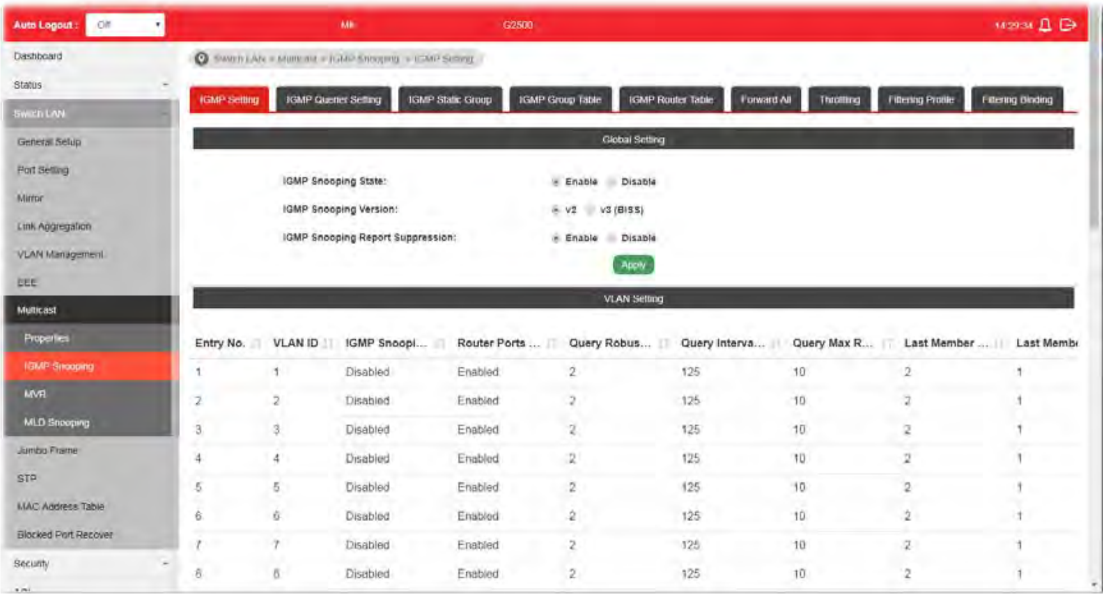
II-7-2 IGMP Snooping

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 the network administrator to enable/disable IGMP function, select snooping version, and enable/disable snooping report suppression.



Global Setting

IGMP Snooping State: ● Enable ○ Disable

IGMP Snooping Version: ● v2 ○ v3 (BISS)

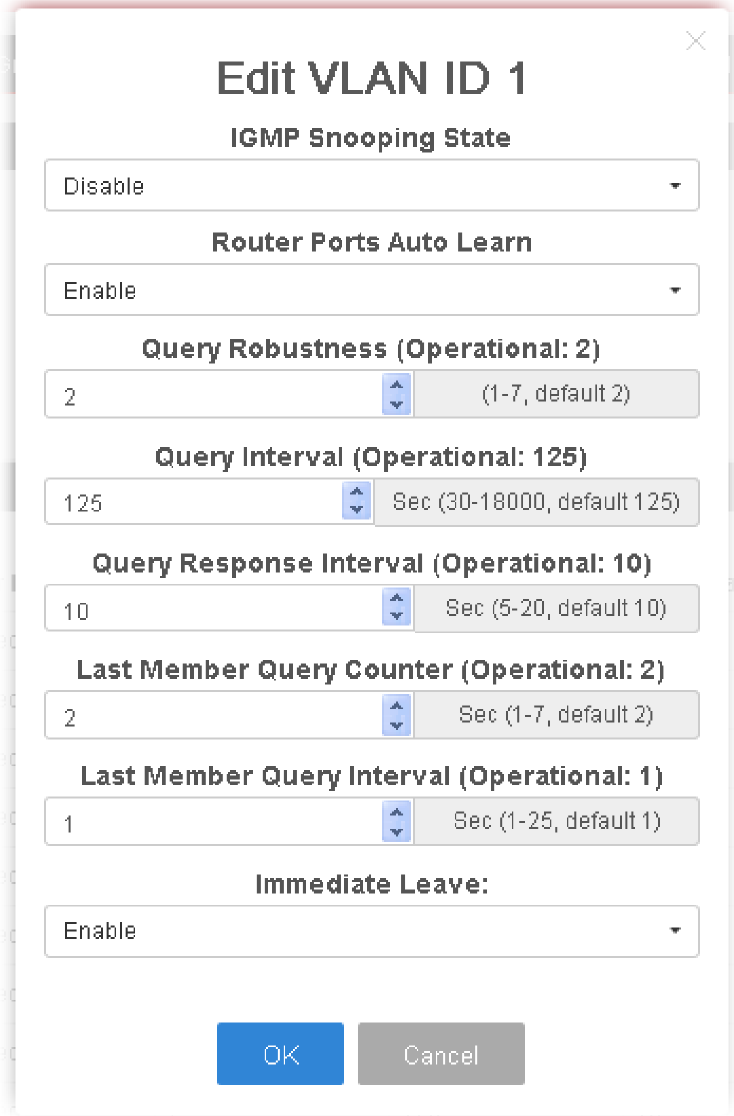
IGMP Snooping Report Suppression: ● Enable ○ Disable

VLAN Setting

Entry No.	VLAN ID	IGMP Snoopi...	Router Ports ...	Query Robus...	Query Interva...	Query Max R...	Last Member ...	Last Membe
1	1	Disabled	Enabled	2	125	10	2	1
2	2	Disabled	Enabled	2	125	10	2	1
3	3	Disabled	Enabled	2	125	10	2	1
4	4	Disabled	Enabled	2	125	10	2	1
5	5	Disabled	Enabled	2	125	10	2	1
6	6	Disabled	Enabled	2	125	10	2	1
7	7	Disabled	Enabled	2	125	10	2	1
8	8	Disabled	Enabled	2	125	10	2	1

Available settings are explained as follows:

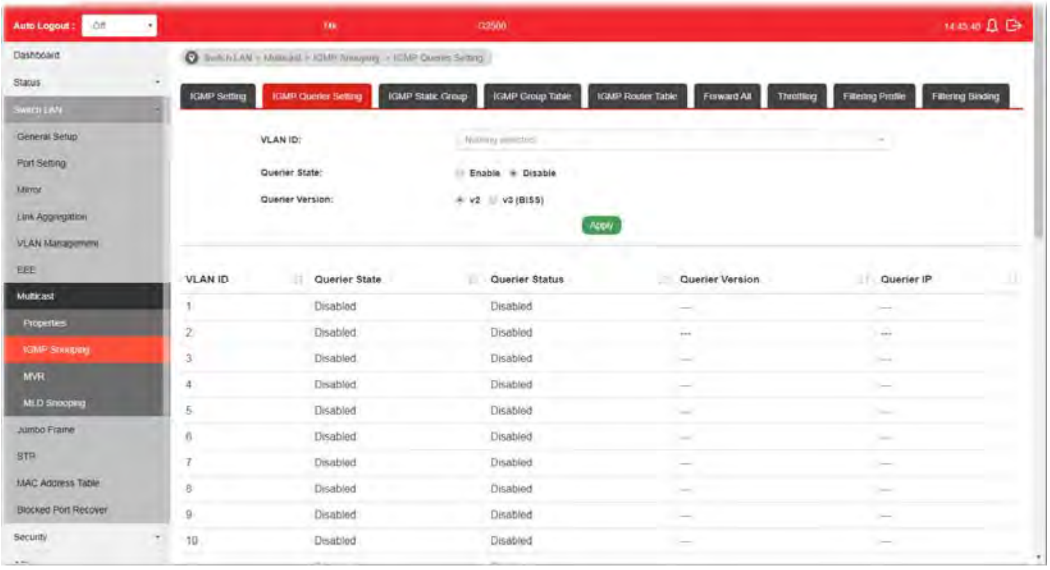
Item	Description
IGMP Snooping State	● **Enable** – Click it to set enabling IGMP function.

	● **Disable** - Click it to disable IGMP function.
IGMP Snooping Version	Set the IGMP snooping version. ● **v2 -** Only support process IGMP v2 packet. ● **v3 (BISS)** - 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	Apply the settings to the switch.
Modify	🔧 - Click it to modify IGMP settings for selected profile. However, if **IGMP Snooping State** is not set as **Enable**, such option will be disabled.  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** - Apply the settings 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: ○ Enable ● Disable

Querier Version: ● v2 ○ v3 (BISS)

VLAN ID	Querier State	Querier Status	Querier Version	Querier IP
1	Disabled	Disabled	---	---
2	Disabled	Disabled	---	---
3	Disabled	Disabled	---	---
4	Disabled	Disabled	---	---
5	Disabled	Disabled	---	---
6	Disabled	Disabled	---	---
7	Disabled	Disabled	---	---
8	Disabled	Disabled	---	---
9	Disabled	Disabled	---	---
10	Disabled	Disabled	---	---

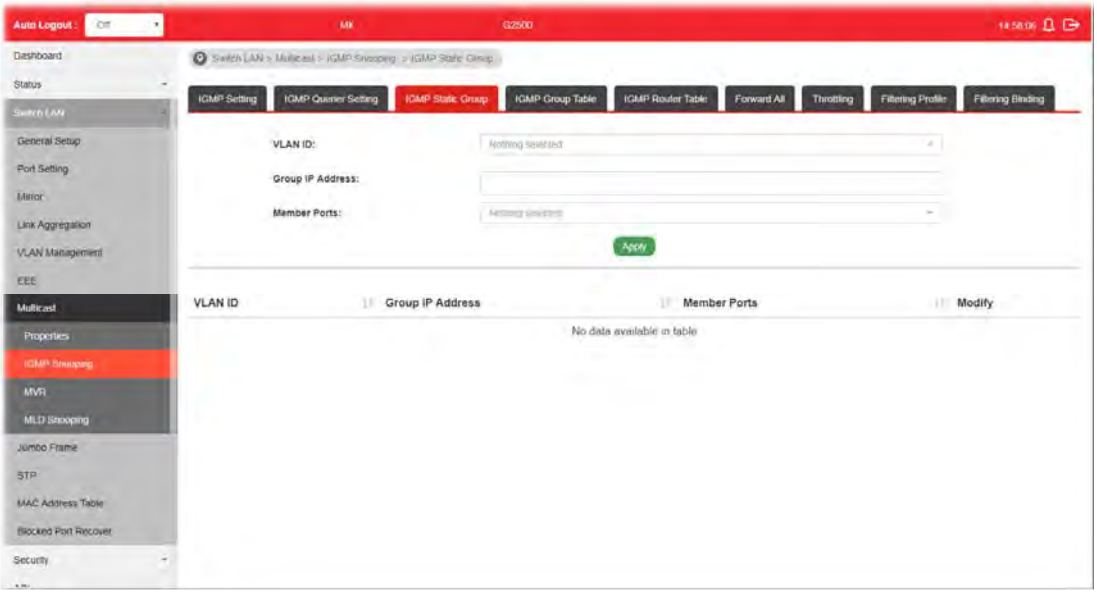
Available settings are explained as follows:

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	Apply the settings 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

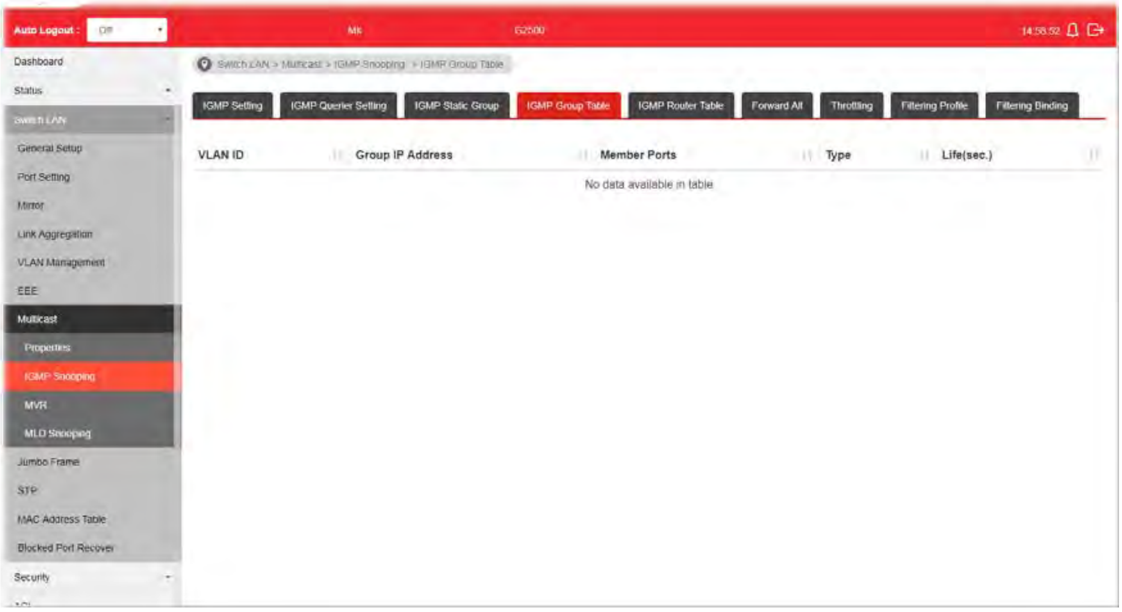
VLAN ID	Group IP Address	Member Ports	Modify
No data available in table			

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	It is an identifier for the group member. Packets sent to such address will be transferred to all interfaces defined in Member Ports. 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	Apply the settings to the switch.
Modify	🔧 - Click it to modify settings.

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.



Auto Logout : Off

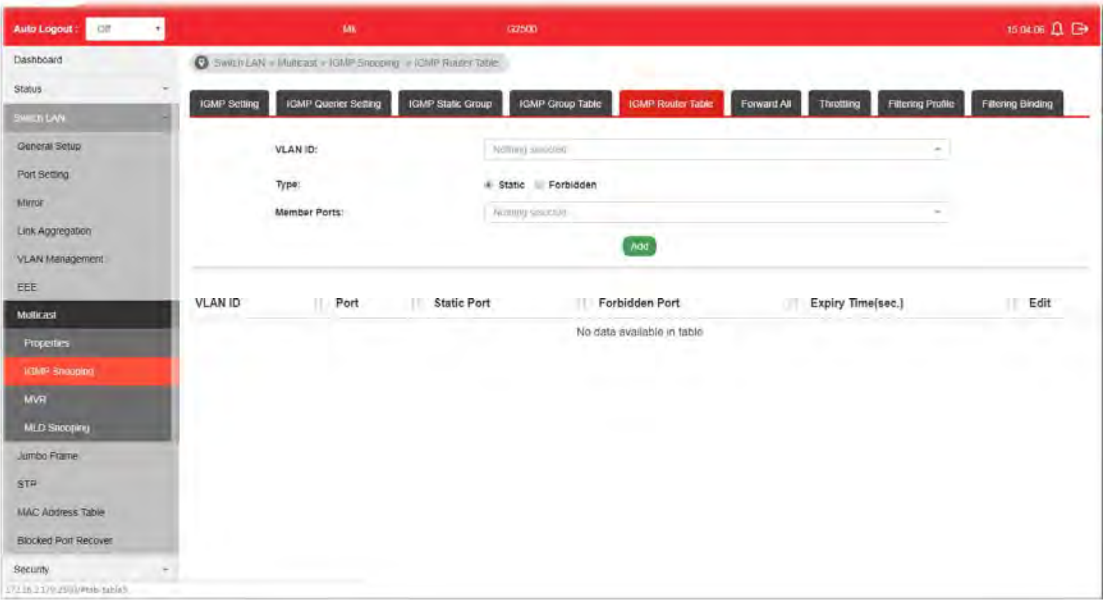
VLAN ID	Group IP Address	Member Ports	Type	Life(sec.)
		No data available in table		

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: Nothing selected

Type: ● Static ○ Forbidden

Member Ports: Nothing selected

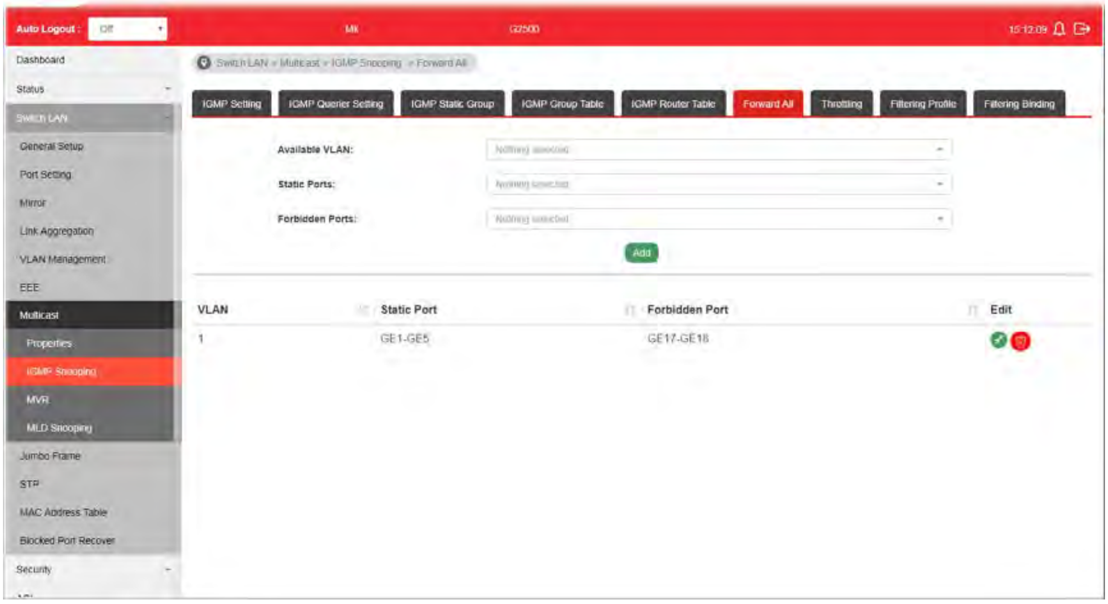
VLAN ID	Port	Static Port	Forbidden Port	Expiry Time(sec.)	Edit
No data available in table					

Available settings are explained as follows:

Item	Description
VLAN ID	Use the drop down list to specify a VLAN profile (created in **Switch LAN>>VLAN Management>>Create Vlan**) that the MLD querier belongs to.
Type	**Static** - Specify LAN Port (GE/LAG) to send out query to remote host. **Forbidden** - Use the drop down list to specify forbidden LAN Port (GE/LAG).
Member Ports	Use the drop down list to choose the uplink ports where querier router exists.
Add	Click it to display the result based on the settings configured above.
Port	Display the static port member specified in Member Ports.
Expire Time (sec.)	Display the time before querier is considered no longer existed.
Edit	Click the icon under Edit to modify the settings for the selected VLAN profile.

II-7-2-6 Forward All

This page is allowed to determine which port(s) would like to receive the data (multicast packets) that forwarded by VigorSwitch.



Available VLAN: Nothing selected

Static Ports: Nothing selected

Forbidden Ports: Nothing selected

VLAN	Static Port	Forbidden Port	Edit
1	GE1-GE5	GE17-GE18	✎ 🗑

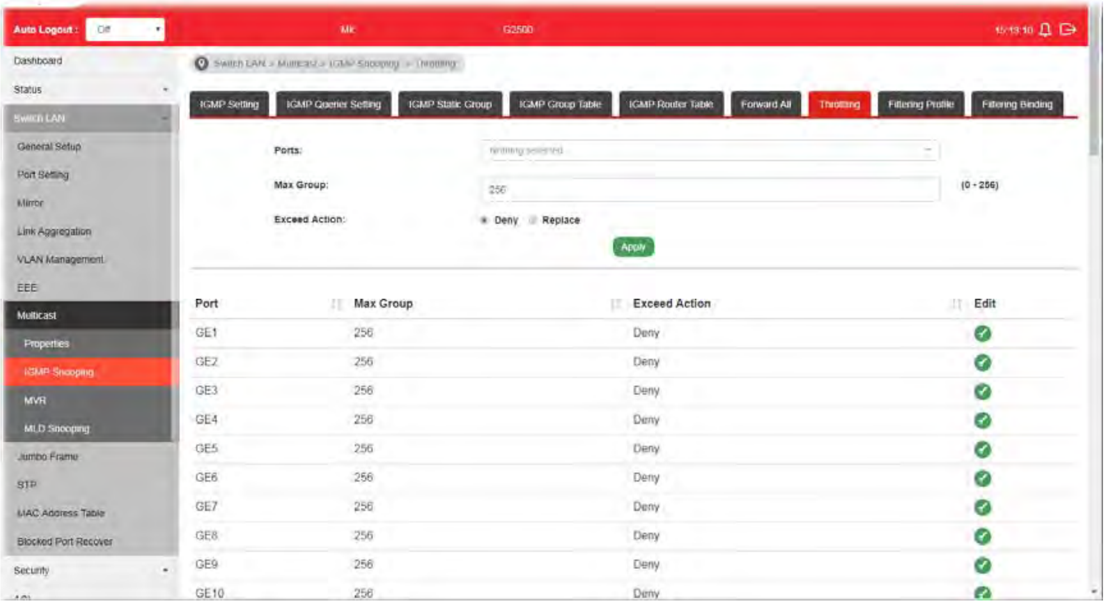
Available settings are explained as follows:

Item	Description
Available VLAN	To display all of the available VLAN, the **State** must be set as **Enabled** in **MLD Setting** first. Use the drop down list to specify a VLAN profile (created in **Switch LAN>>VLAN Management>>Create Vlan**) that multicast packets will be forwarded to.
Static Ports	Use the drop down list to specify LAN Port (GE/LAG). Later, the multicast packets will be delivered to the network device connected by these ports.
Forbidden Ports	Use the drop down list to specify forbidden LAN Port (GE/LAG). Later, the multicast packets will not be delivered to the network device connected by these ports.
Add	Click it to display the result based on the settings configured above.
Edit	✎ - Click it to modify port setting (static port and forbidden port). 🗑 - Click it to remove the selected entry.

II-7-2-7 Throttling

The administrator can configure the user on a switch port (GE/LAG port) belonging to which multicast group and restrict the number of multicast group that the user on the switch can join. Then the administrator is able to control the network service (e.g, IP/TV service) that the user can enjoy.

The Throttling page is used for configuring the maximum number (0~255) of IGMP group that a user on a switch port can join. After defined the maximum number, each switch port interface can be set to deny the IGMP join report or set to replace randomly selected multicast interface with received IGMP join report.



Ports: nothing selected

Max Group: 256 (0 - 256)

Exceed Action: ● Deny ○ Replace

Port	Max Group	Exceed Action	Edit
GE1	256	Deny	✓
GE2	256	Deny	✓
GE3	256	Deny	✓
GE4	256	Deny	✓
GE5	256	Deny	✓
GE6	256	Deny	✓
GE7	256	Deny	✓
GE8	256	Deny	✓
GE9	256	Deny	✓
GE10	256	Deny	✓

Available settings are explained as follows:

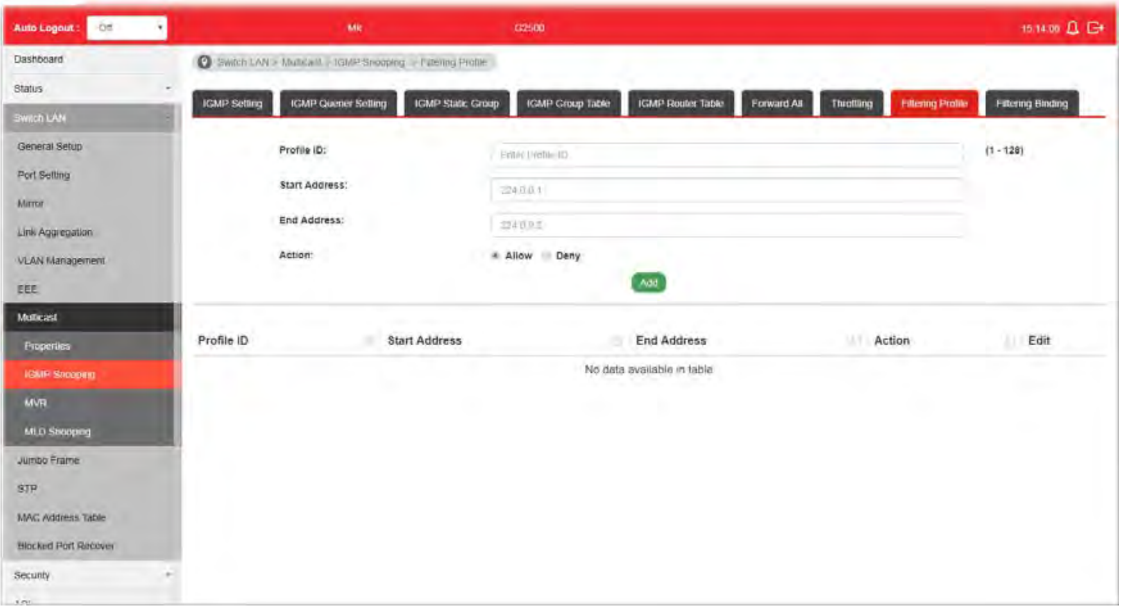
Item	Description
Ports	Use the drop down list to specify LAN Port (GE/LAG).
Max Group	Define the maximum number of IGMP group profile that a user on the switch can join. If "0" is selected, then such interface (port) can join all of the IGMP group profiles (defined in Filtering Profile).
Exceed Action	VigorSwitch will perform the action defined below when the number of IGMP join report for the specified interface exceeds value defined in Max Group. ● **Deny -** It is default setting. The IGMP join report (for multicast service) received by such interface will be discarded. ● **Replace -** When it is selected, a new group with IGMP report received will replace the existing group.
Apply	Apply the settings to the switch.
Edit	🔧 - Click it to modify port setting (max group and exceed action).

II-7-2-8 Filtering Profile

The administrator can configure the user on a switch port (GE/LAG port) belonging to which multicast group and restrict the number of multicast group that the user on the switch can join. Then the administrator is able to control the network service (e.g, IP/TV service) that the user can enjoy.

The filtering profile page allows to configure up to 128 IP-group (for multicast servie) profiles (starting and ending point within an IP range shall be specified). Each IP group profile can be set for permission of / denial of network service respectively.

In addition, such filtering profile is only effective for controlling the query for multicast. It has nothing to do with the general IGMP query.



Profile ID: Enter Profile ID (1 - 128)

Start Address: 224.0.0.1

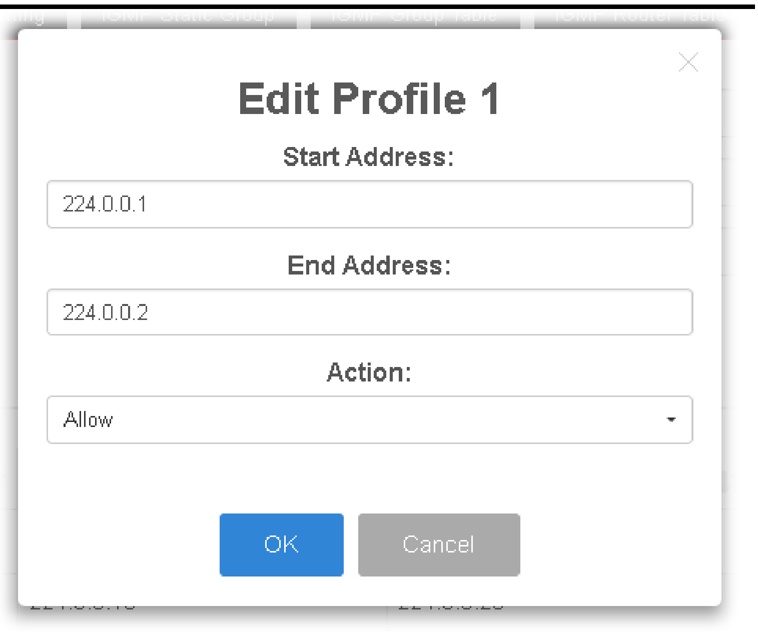
End Address: 224.0.0.2

Action: ● Allow ○ Deny

Profile ID	Start Address	End Address	Action	Edit
No data available in table				

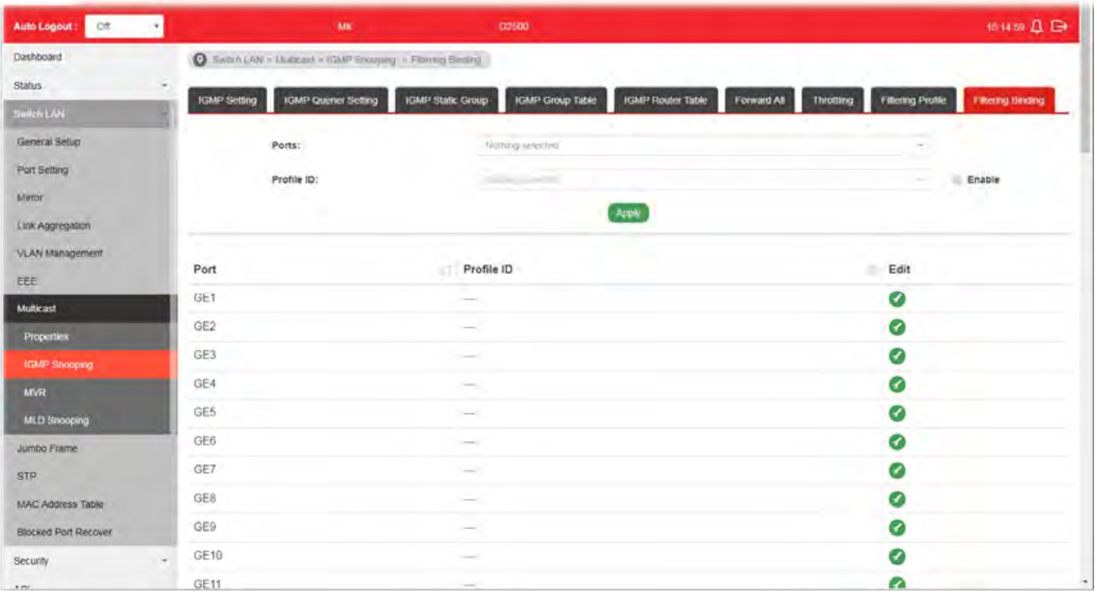
Available settings are explained as follows:

Item	Description
Profile ID	Use the drop down list to select one filtering profile (1~128) for IGMP snooping.
Start Address	Enter an IP address as the starting point for the IP range.
End Address	Enter an IP address as the ending point for the IP range.
Action	● **Deny -** It is default setting. The forwarding request of multicast traffic will be discarded. ● **Allow** – When it is selected, the request for multicast traffic will be forwarded to the multicast group normally.
Add	Click it to display the result based on the settings configured above.
Edit	🔧 - Click it to modify port setting (max group and exceed action).

	 Edit Profile 1 Start Address: 224.0.0.1 End Address: 224.0.0.2 Action: Allow OK Cancel

II-7-2-9 Filtering Binding

This page allows the network administrator to select a filtering profile for LAN/GE port to process multicast traffic.



Switch LAN > Multicast > IGMP Snooping > Filtering Binding

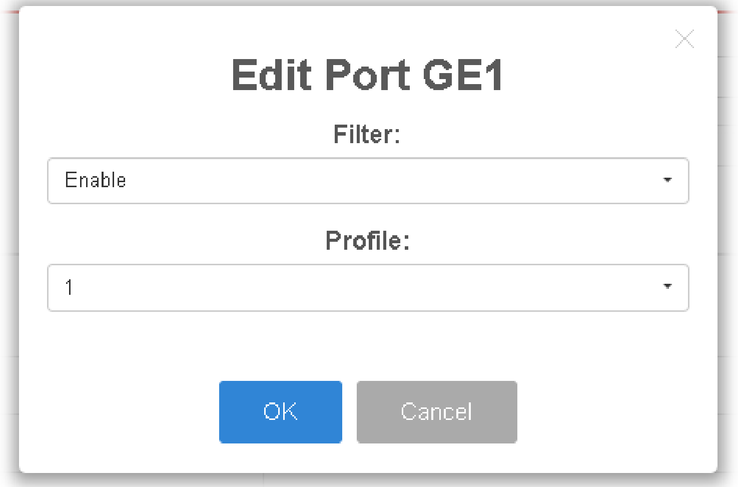
Ports: Nothing selected

Profile ID: ☐ Enable

Port	Profile ID	Edit
GE1	—	✓
GE2	—	✓
GE3	—	✓
GE4	—	✓
GE5	—	✓
GE6	—	✓
GE7	—	✓
GE8	—	✓
GE9	—	✓
GE10	—	✓
GE11	—	✓

Available settings are explained as follows:

Item	Description
Ports	Use the drop down list to specify LAN Port (GE/LAG).
Profile ID	Use the drop down list to choose the filtering profile for the select port/interface. ● **Enable -** Check this box first to make profile ID selection be available for choosing.
Apply	Apply the settings to the switch.
Edit	🔧 - Click it to modify port setting (enabling / disabling filter function and choosing a profile for such interface).

	 Edit Port GE1 Filter: Enable Profile: 1

II-7-3 MVR

Multicast VLAN Registration (MVR) can route packets received in a multicast source VLAN to one or more desination VLANs. LAN users are in the destination VLANs and the multicast server is in the source VLAN.

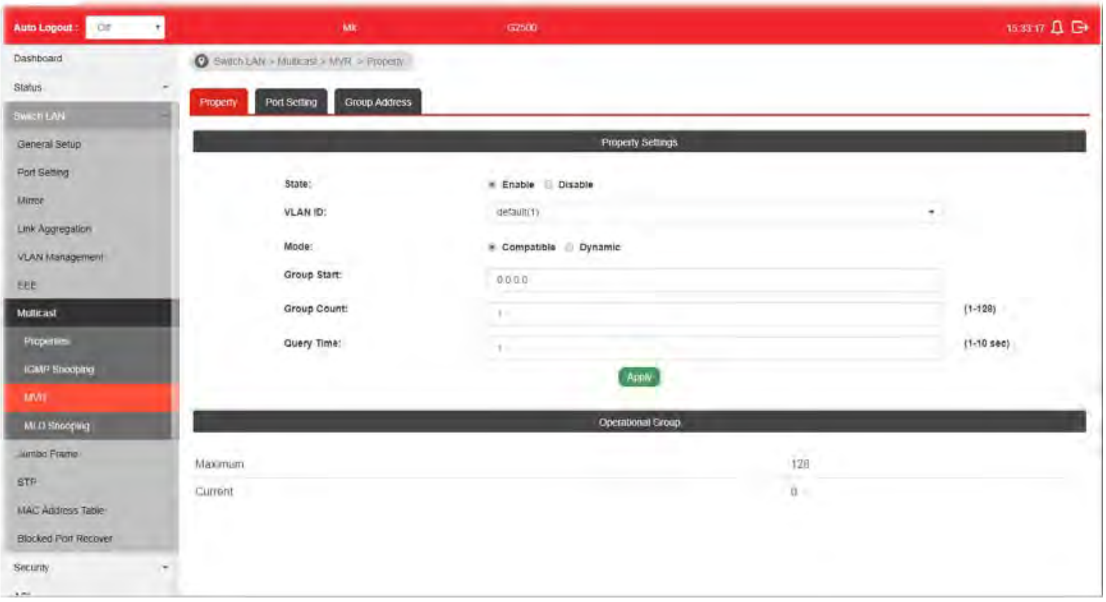
MVR can continuously send multicast stream for traffic in the multicast VLAN, but isolate the streams from the source VLANs for bandwidth and security reasons.

In general, MVR is able to:

- Identify the MVR IP multicast streams and their associated IP multicast group.
- Intercept the IGMP messages

II-7-3-1 Property

This page allows the network administrator to configure general settings for MVR, such as enabling function, selecting VLAN ID (as source VLAN) and specify IP address(es) for receiver/LAN users.



Property Settings

State: ● Enable ○ Disable

VLAN ID: default(1)

Mode: ● Compatible ○ Dynamic

Group Start: 0.0.0.0

Group Count: 1 (1-128)

Query Time: 1 (1-10 sec)

Operational Group

Maximum	128
Current	0

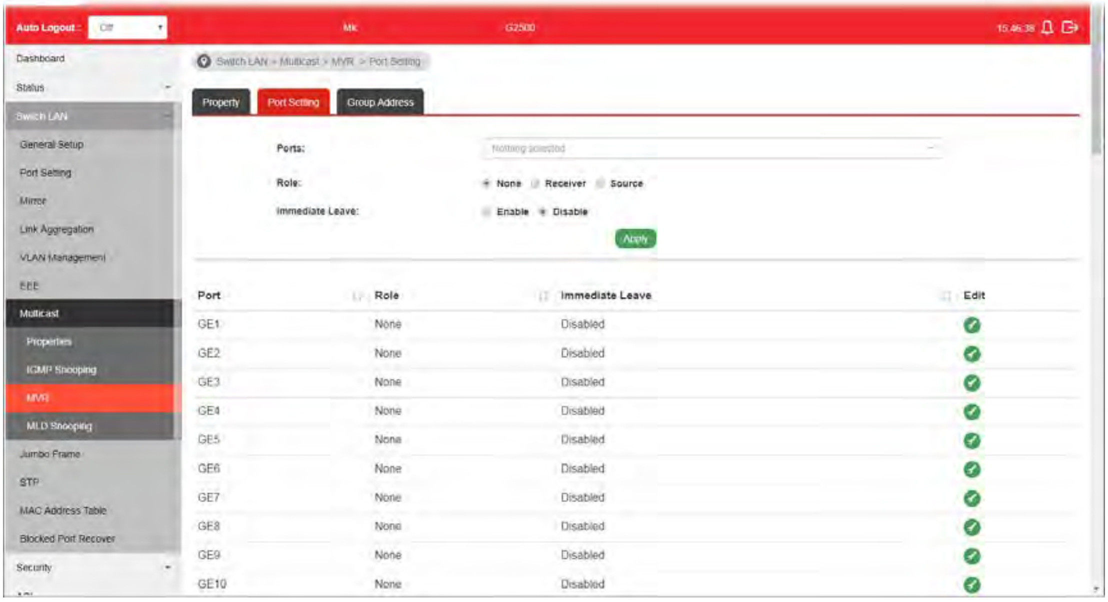
Available settings are explained as follows:

Item	Description
State	● **Enabled** – Click it to enable the MVR function. ● **Disabled** – Click it to disable the MVR function.
VLAN ID	Choose one VLAN profile from the drop down list as multicast source VLAN which will receive multicast data. All source ports must belong to this VLAN. The default is VLAN 1. Note: Each VLAN ID shall be configured with group address and member port (defined in **MVR>>Group Address** page).
Mode	There are two modes offered for MVR operation. ● **Comaptible -** Multicast data received by MVR hosts (multicast server) will be forwarded to all MVR receiver ports. ● **Dynamic -** Multicast data received by MVR hosts (multicast server) on Vigor switch will be forwarded

	from those MVR data and client ports grouped under MVR server.
Group Start	Enter an IP address. Any multicast data sent to this IP address will be sent to all source ports on Vigor switch; and all receiver ports will accept /receive data from that multicast address.
Group Count	Select a number to configure a contiguous series of MVR group addresses (the range for count is 1 to 128; the default is 1).
Query Time	Use the drop down list to define the maximum time (1 - 10 seconds) to wait for IGMP report members on a receiver port before the port is removed from multicast group.
Apply	Apply the settings to the switch.
Operation Group	Display group information for MVR operation.

II-7-3-2 Port Setting

It is necessary to specify destination port and source port (GE/LAG) for Vigor system to perform MVR operation.



Ports: Nothing selected

Role: ● None ○ Receiver ○ Source

Immediate Leave: ○ Enable ● Disable

Port	Role	Immediate Leave	Edit
GE1	None	Disabled	✓
GE2	None	Disabled	✓
GE3	None	Disabled	✓
GE4	None	Disabled	✓
GE5	None	Disabled	✓
GE6	None	Disabled	✓
GE7	None	Disabled	✓
GE8	None	Disabled	✓
GE9	None	Disabled	✓
GE10	None	Disabled	✓

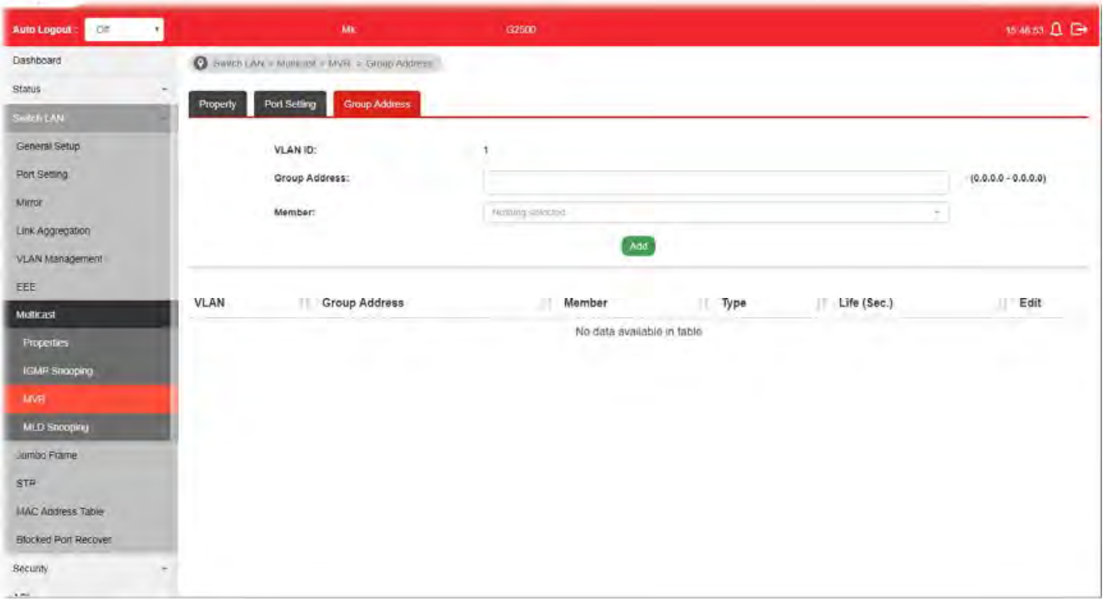
Available settings are explained as follows:

Item	**Description**
Ports	Use the drop down list to select LAN Port (GE/LAG). Later, each port can be set as Recevier or Source port respectively. If you do not satisfy with the port setting, simply click the Edit button to make the modification.
Role	● **None -** Noting will be happed to the selected LAN port in MVR operation. ● **Receiver -** The selected port will be treated as destination port which will receive multicast data from the multicast server. ● **Source -** The selected port will be treated as source port which will send multicast data to the receiver port.
Immediate Leave	● **Enabled -** Enable the function fo immediate leave**.** When

	the port (with the role of receiver) receives the leave message, it will be removed from multicast group to speed up leave latency. ● **Disabled -** Disable the function of immediate leave.
Apply	Apply the settings to the switch.
Edit	🔧 - Click it to modify port setting (role and immediate leave).

II-7-3-3 Group Address

This page allows the network administrator to configure IP address and specify port member for VLAN selected in **MVR>>Property** page.



VLAN ID: 1

Group Address: (0.0.0.0 - 0.0.0.0)

Member: Nothing selected

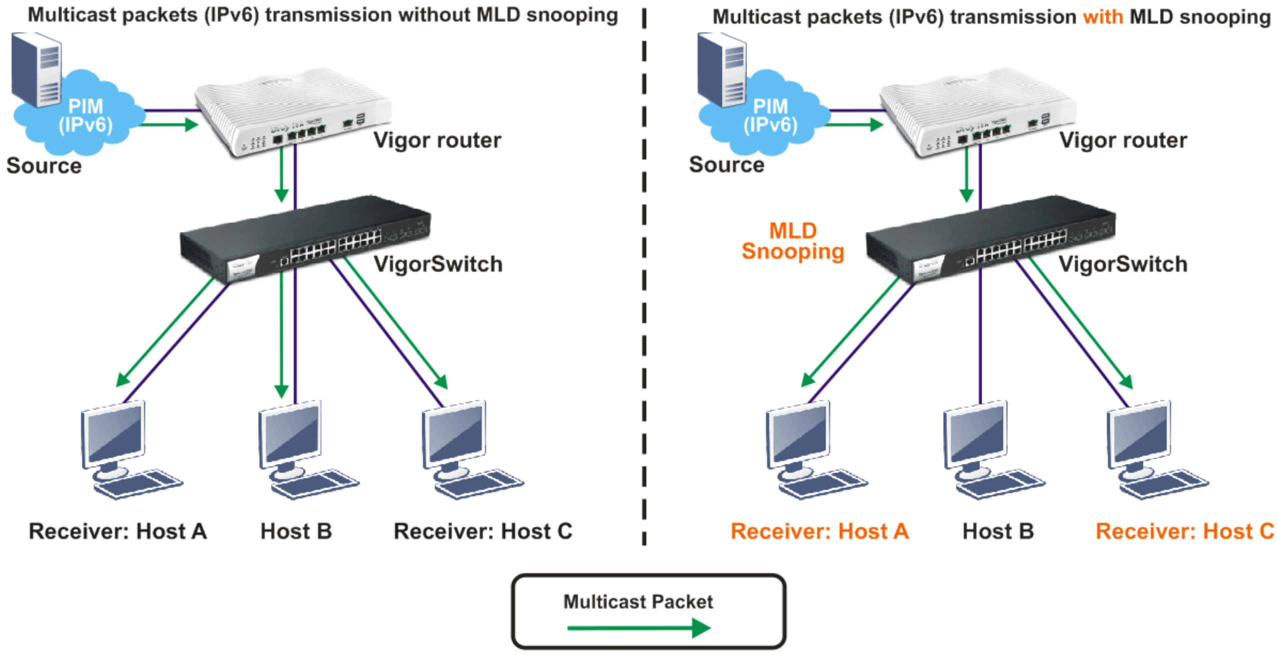
VLAN	Group Address	Member	Type	Life (Sec.)	Edit
No data available in table					

Available settings are explained as follows:

Item	Description
VLAN ID	Display the ID number of the VLAN.
Group Address	Define a range of IP address(es) with the format of “xxx.xxx.xxx.xxx – xxx.xxx.xxx.xxx”.
Member	Choose GE/LAG port to be grouped under the selected VLAN.
Add	Click it to display the result based on the settings configured above.
Edit	🔧 - Click it to modify the settings.

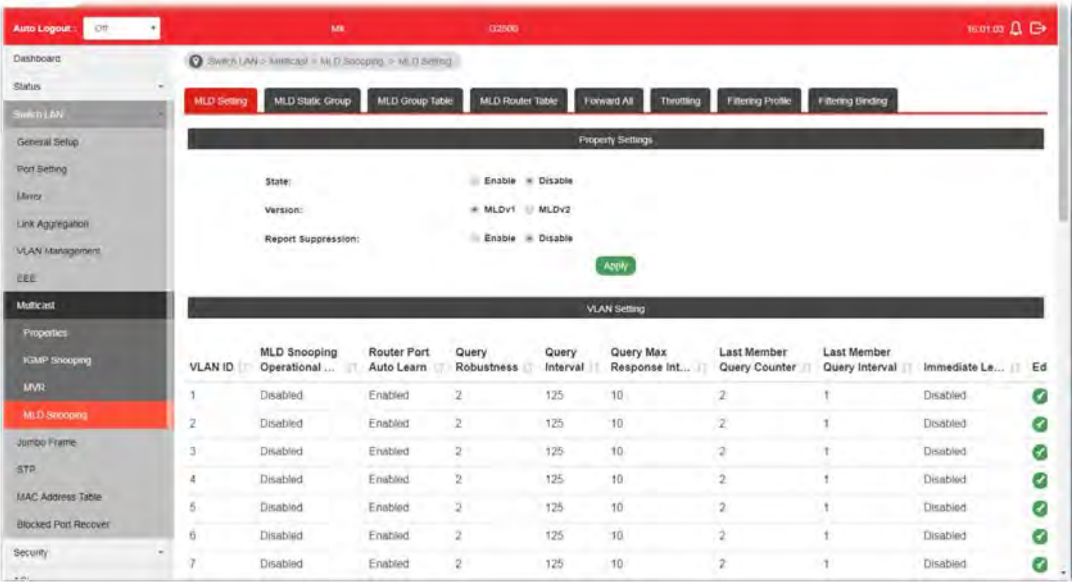
II-7-4 MLD Snooping

MLD snooping does the same thing as IGMP snooping. The difference is that IGMP snooping acts on IPv4 packets; MLD snooping acts on IPv6 packets. MLD snooping is the process of listening to Multicast Listener Discovery network traffic. It can examine IPv6 packets and forward these packets to designate location via VLAN port members.



II-7-4-1 MLD Setting

This page allows the network administrator to enable/disable MLD Snooping function, select snooping version, and enable/disable snooping report suppression.



Property Settings

State: ○ Enable ● Disable

Version: ● MLDv1 ○ MLDv2

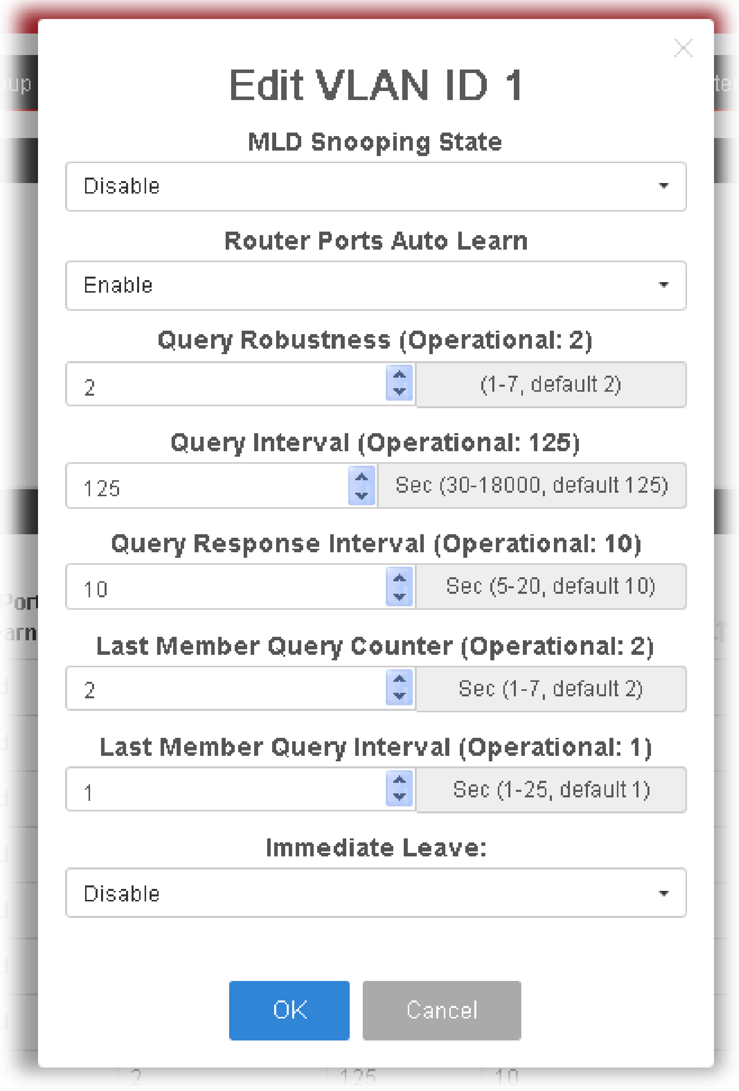
Report Suppression: ○ Enable ● Disable

VLAN Setting

VLAN ID	MLD Snooping Operational ...	Router Port Auto Learn	Query Robustness	Query Interval	Query Max Response Int...	Last Member Query Counter	Last Member Query Interval	Immediate Le...	Ed
1	Disabled	Enabled	2	125	10	2	1	Disabled	✓
2	Disabled	Enabled	2	125	10	2	1	Disabled	✓
3	Disabled	Enabled	2	125	10	2	1	Disabled	✓
4	Disabled	Enabled	2	125	10	2	1	Disabled	✓
5	Disabled	Enabled	2	125	10	2	1	Disabled	✓
6	Disabled	Enabled	2	125	10	2	1	Disabled	✓
7	Disabled	Enabled	2	125	10	2	1	Disabled	✓

Available settings are explained as follows:

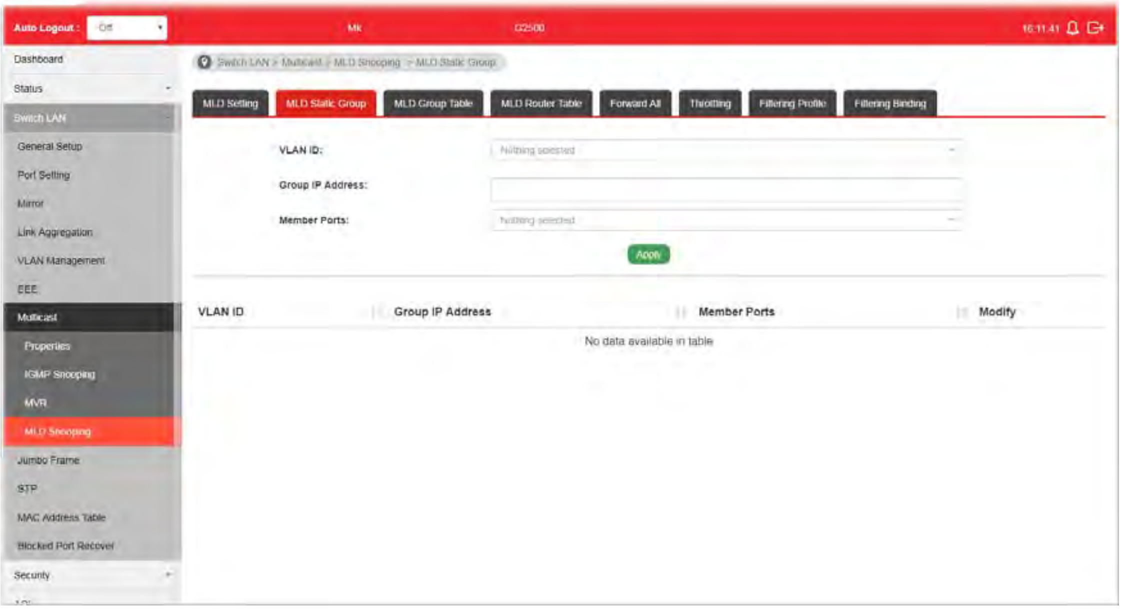
Item	Description
State	● **Enabled** – Click it to enable the MLD snooping function.

	● **Disabled** – Click it to disable the MLD snooping function.
Version	VigorSwitch supports two versions of MLD snooping. ● **MLDv1 -** When it is selected, VigorSwitch will detect packets controlled by MLDv1 and *bridge* the traffic to IPv6 destination defined with multicast address(es). ● **MLDv2 -** When it is selected, VigorSwitch will detect packets controlled by MLDv1 and *forward* the traffic to destination defined with multicast address(es).
Report Suppression	● **Enabled** – Click it to allow the switch to handle MLD reports between router and host, suppressing bandwidth used by MLD. ● **Disabled** – Click it to disable the function.
Apply	Click it to display the result based on the settings configured above.
Edit	🔧 - Click it to modify the settings for the selected VLAN ID (GE/LAG port).  Edit VLAN ID 1 MLD 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: Disable OK Cancel ● **MLD Snooping State** – Enable/disable the MLD snooping function for the selected port. ● **Router Ports Auto Learn** –Set the enabling status of IGMP router port learning. Choose **Enable** to learn router port

	by MLD query. ● **Query Robustness** – Set a number which allows tuning for the expected packet loss on a subnet. ● **Query Interval** – Specify the time interval for VigorSwitch to send out general MLD query to the host (responsible for responding). Later, based on the response, VigorSwitch can forward the traffic through ports in VLAN. ● **Query Response Interval** – Specify the time interval for VigorSwitch to receive the query response from the host. If time is up and no response received, the packets will be blocked and discarded. ● **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** – Click **Enable** to enable the function of immediate leave. When the GE/LAG port receives the leave message, it will be removed from multicast group to speed up leave latency. ● **OK** - Apply the settings to the switch. ● **Cancel -** Close the page and return to previous page.

II-7-4-2 MLD Static Group

The MLD static group is allowed to assign a VLAN/port as a specific IPv6 multicast member. Every IPv6 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			

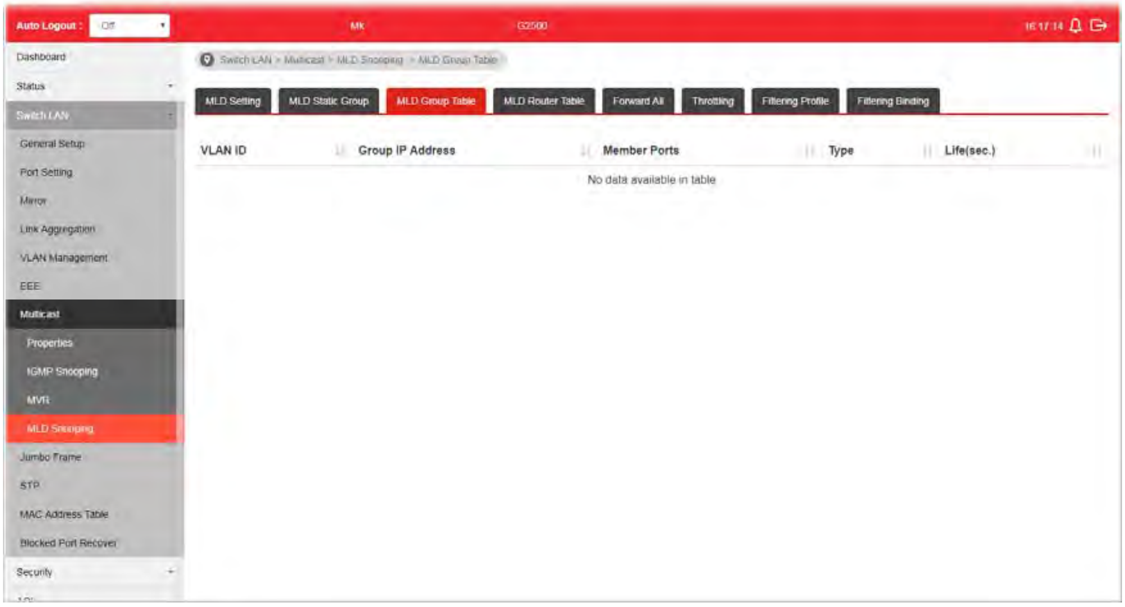
Available settings are explained as follows:

Item	Description
VLAN ID	Use the drop down list to specify a VLAN profile (created in **Switch LAN>>VLAN Management>>Create Vlan)** as MLD

	Static Group. However, if **State** in **MLD Setting** is not set as **Enabled**, such option will be disabled and no ID can be selected.
Group IP Address	It is an identifier for the group member. Packets sent to such address will be transferred to all interfaces defined in Member Ports. Specify the IPv6 multicast address you wish to assign for the static group (defined in VLAN ID).
Member Ports	Use the drop down list to specify interaces (GE/LAG) for receiving the packets from group IP address.
Add	Click it to display the result based on the settings configured above.

II-7-4-3 MLD Group Table

This page shows currently known and dynamically learned by MLD snooping or shows the assigned IP6 multicast address group in operation.



VLAN ID	Group IP Address	Member Ports	Type	Life(sec.)

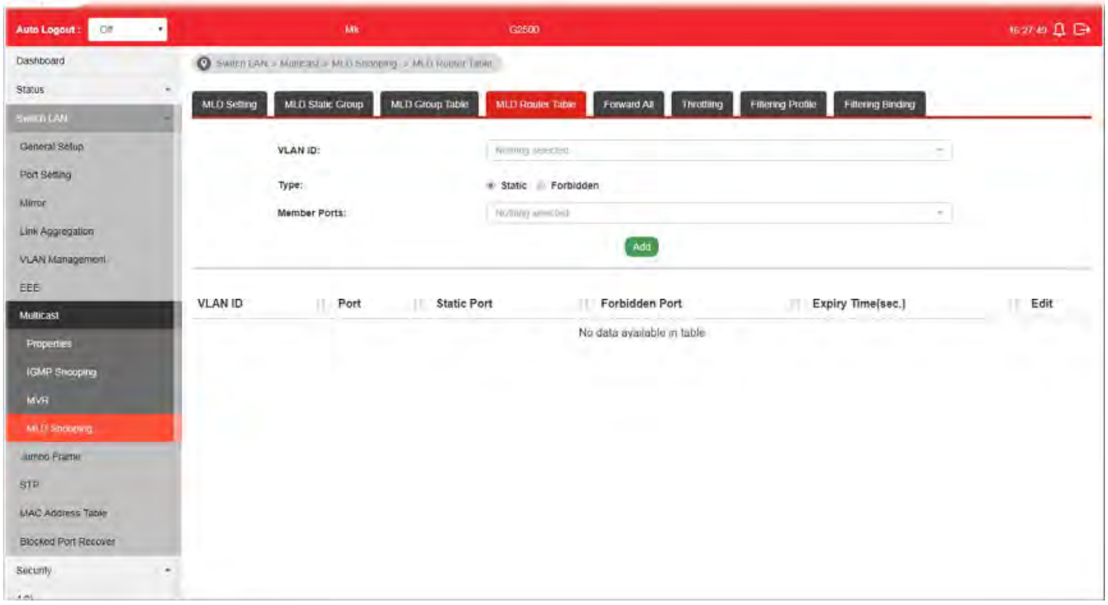
No data available in table

Available settings are explained as follows:

Item	**Description**
VLAN ID	Display the name of VLAN configured in MLD Static Group.
Group IP Address	Display the IP adderss defined in MLD Static Group.
Member Ports	Display all of the interfaces defined in MLD Static Group.
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-7-4-4 MLD Router Table

This page is allowed to configure VLAN profile by specifying static/forbidden ports for the router (MLD querier).



VLAN ID: Nothing selected

Type: ● Static ○ Forbidden

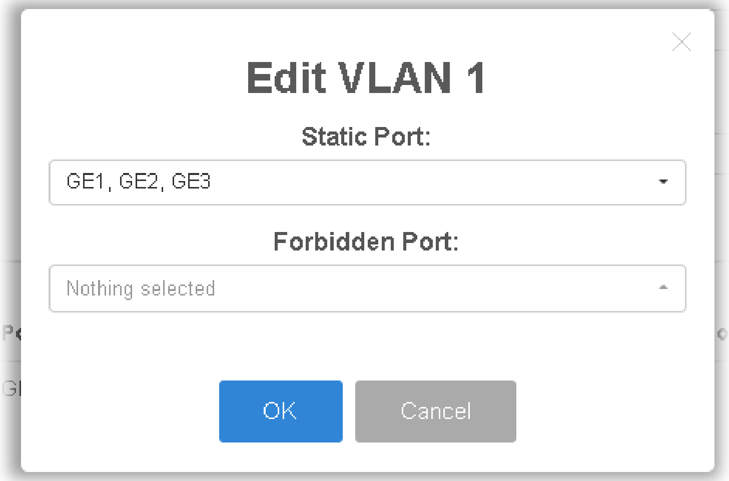
Member Ports: Nothing selected

Add

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

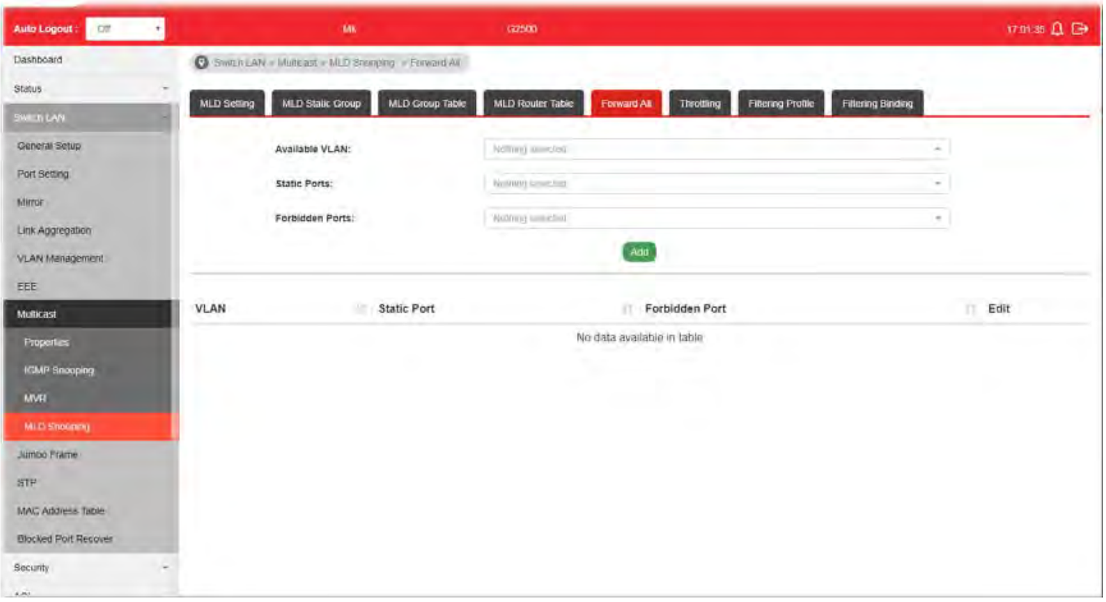
Available settings are explained as follows:

Item	Description
VLAN ID	Use the drop down list to specify a VLAN profile (created in **Switch LAN>>VLAN Management>>Create Vlan**) that the MLD querier belongs to.
Type	● **Static** - Specify LAN Port (GE/LAG) to send out query to remote host. ● **Forbidden** - Use the drop down list to specify forbidden LAN Port (GE/LAG).
Member Ports	Use the drop down list to choose the uplink ports where querier router exists.
Add	Click it to display the result based on the settings configured above.
Static Port / Forbidden Port	Display the static port / forbidden port member specified in Member Ports.
Expire Time (sec.)	Display the time before querier is considered no longer existed.
Edit	🔧 - Click it to modify the settings for the selected entry.

	 Edit VLAN 1 Static Port: GE1, GE2, GE3 Forbidden Port: Nothing selected OK Cancel

II-7-4-5 Forward All

This page is allowed to determine which port(s) would like to receive the data (multicast packets) that forwarded by VigorSwitch.



Available VLAN: Nothing selected

Static Ports: Nothing selected

Forbidden Ports: Nothing selected

VLAN	Static Port	Forbidden Port	Edit
No data available in table			

Available settings are explained as follows:

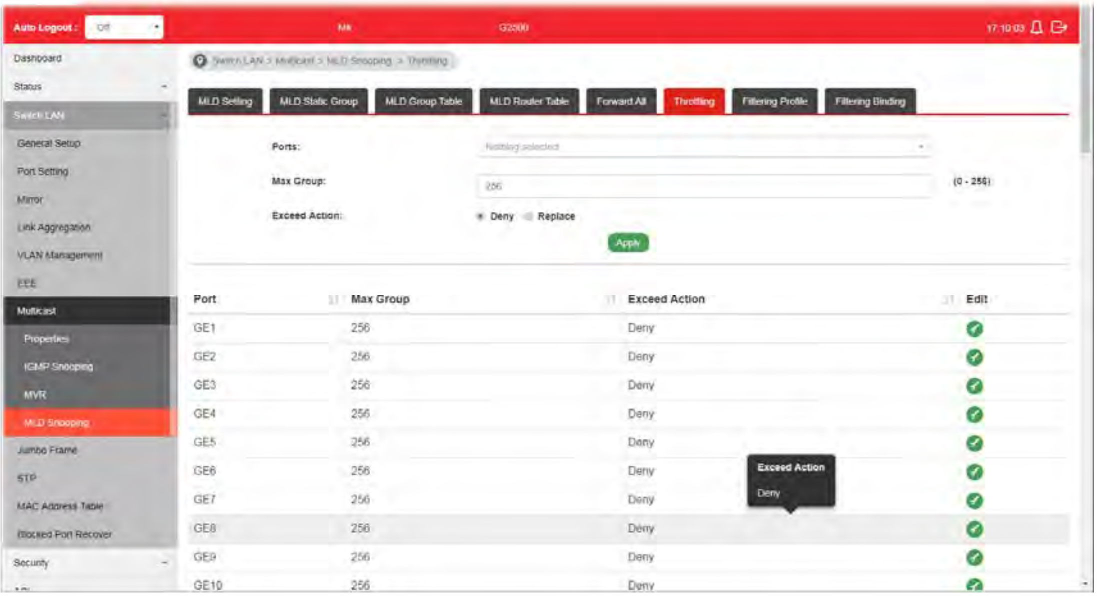
Item	Description
Available VLAN	To display all of the available VLAN, the **State** must be set as **Enabled** in **MLD Setting** first. Use the drop down list to specify a VLAN profile (created in **Switch LAN>>VLAN Management>>Create Vlan**) that multicast packets will be forwarded to.
Static Ports	Use the drop down list to specify LAN Port (GE/LAG). Later, the multicast packets will be delivered to the network device connected by these ports.
Forbidden Ports	Use the drop down list to specify forbidden LAN Port (GE/LAG). Later, the multicast packets will not be delivered to the network device connected by these ports.

Add	Click it to display the result based on the settings configured above.
Edit	🔧 - Click it to modify port setting (static port and forbidden port). 🗑 - Click it to remove the selected entry.

II-7-4-6 Throttling

The administrator can configure the user on a switch port (GE/LAG port) belonging to which multicast group and restrict the number of multicast group that the user on the switch can join. Then the administrator is able to control the network service (e.g, IP/TV service) that the user can enjoy.

The Throttling page is used for configuring the maximum number (0~255) of MLD group that a user on a switch port can join. After defined the maximum number, each switch port interface can be set to deny the MLD join report or set to replace randomly selected multicast interface with received MLD join report.



Ports: Nothing selected

Max Group: 256 (0 - 256)

Exceed Action: ● Deny ○ Replace

Port	Max Group	Exceed Action	Edit
GE1	256	Deny	🔧
GE2	256	Deny	🔧
GE3	256	Deny	🔧
GE4	256	Deny	🔧
GE5	256	Deny	🔧
GE6	256	Deny	🔧
GE7	256	Deny	🔧
GE8	256	Deny	🔧
GE9	256	Deny	🔧
GE10	256	Deny	🔧

Available settings are explained as follows:

Item	Description
Ports	Use the drop down list to specify LAN Port (GE/LAG) for applying throttling feature.
Max Group	Define the maximum number of MLD group profile that a user on the switch can join. If "0" is selected, then such interface (port) can join all of the MLD group profiles (defined in Filtering Profile).
Exceed Action	VigorSwitch will perform the action defined below when the number of MLD join report for the specified interface exceeds value defined in Max Group. ● **Deny -** It is default setting. The MLD join report (for multicast service) received by such interface will be discarded. ● **Replace -** When it is selected, a new group with MLD report received will replace the existing group.

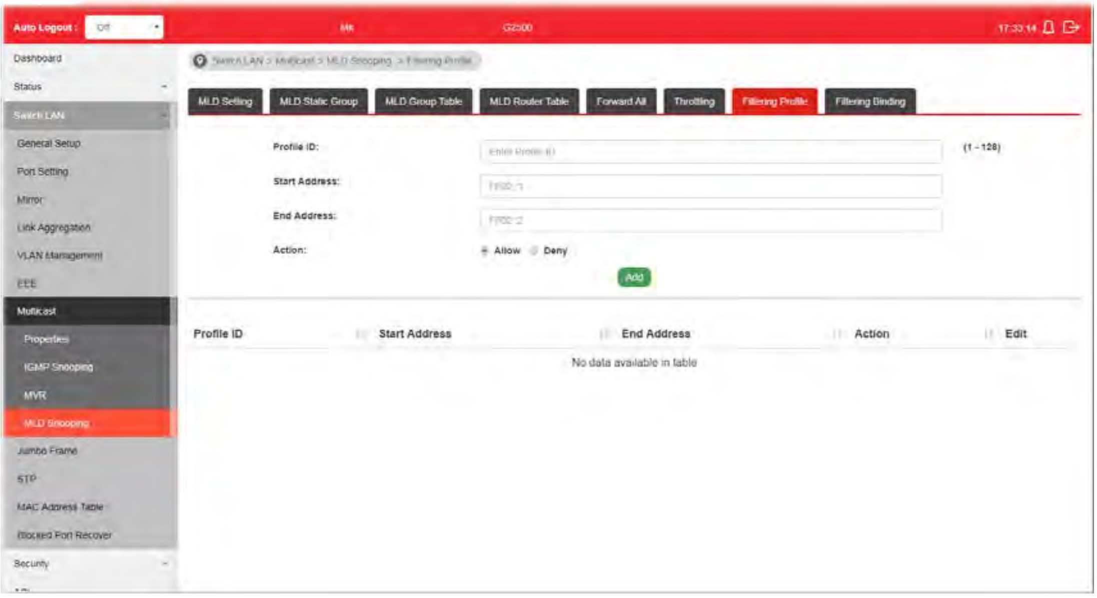
Apply	Apply the settings to the switch.
Edit	- Click it to modify the settings for the selected entry.

II-7-4-7 Filtering Profile

The administrator can configure the user on a switch port (GE/LAG port) belonging to which multicast group and restrict the number of multicast group that the user on the switch can join. Then the administrator is able to control the network service (e.g, IP/TV service) that the user can enjoy.

The filtering profile page allows to configure up to 128 IP-group (for multicast servie) profiles (starting and ending point within an IP range shall be specified). Each IP group profile can be set for permission of / denial of network service respectively.

In addition, such filtering profile is only effective for controlling the query for multicast traffic. It has nothing to do with the general MLD query.



Profile ID: Enter Profile ID (1 - 128)

Start Address: FF00::1

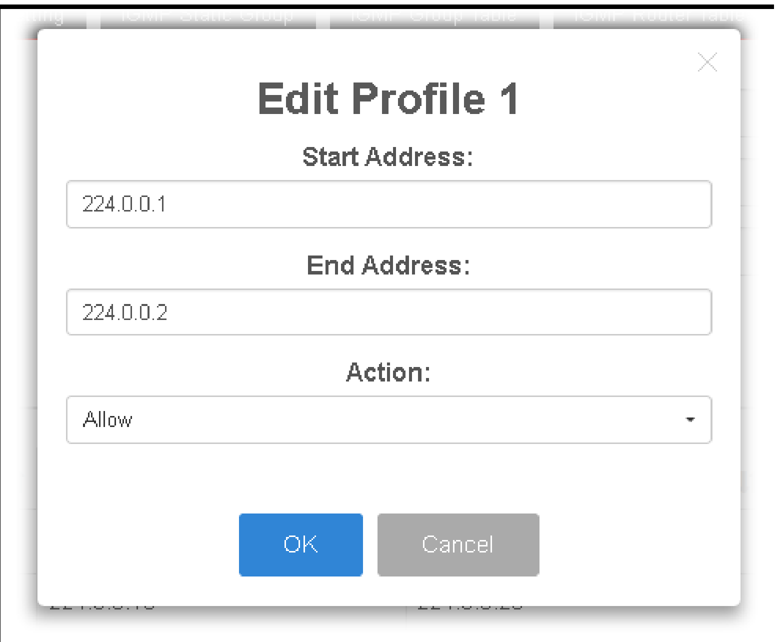
End Address: FF00::2

Action: ● Allow ○ Deny

Profile ID	Start Address	End Address	Action	Edit
No data available in table				

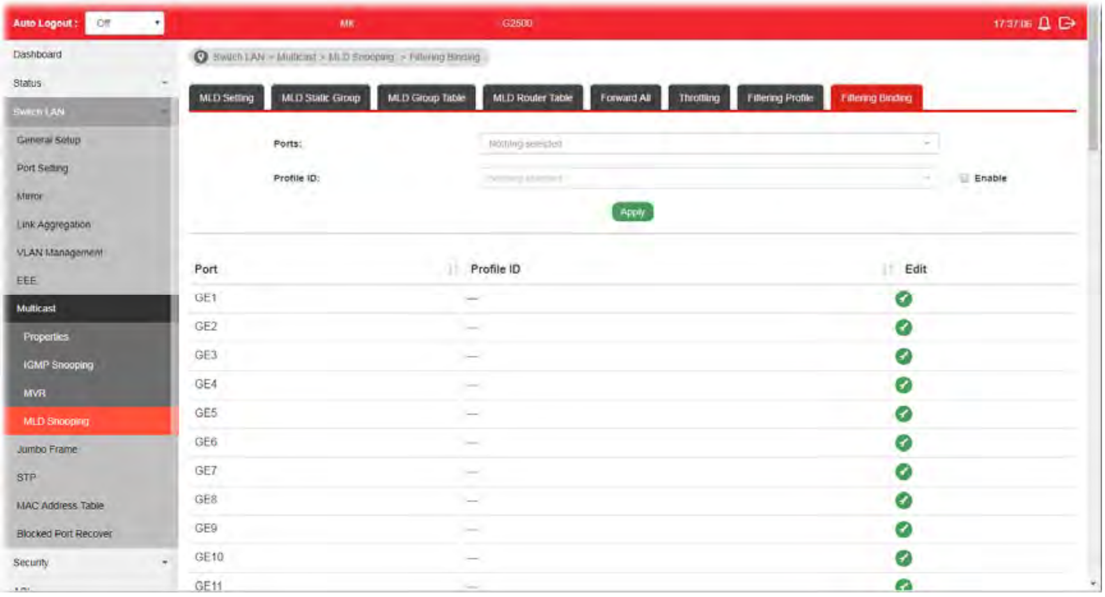
Available settings are explained as follows:

Item	Description
Profile ID	Use the drop down list to select one filtering profile (1~128) for MLD snooping.
Start Address	Enter an IP address as the starting point for the IP range.
End Address	Enter an IP address as the ending point for the IP range.
Action	● **Deny -** It is default setting. The forwarding request of multicast traffic will be discarded. ● **Allow** – When it is selected, the request for multicast traffic will be forwarded to the multicast group normally.
Add	Click it to display the result based on the settings configured above.
Edit	- Click it to modify the settings for the selected entry.

	 Edit Profile 1 Start Address: 224.0.0.1 End Address: 224.0.0.2 Action: Allow

II-7-4-8 Filtering Binding

This page allows the network administrator to select a filtering profile for LAN/GE port to process multicast traffic.



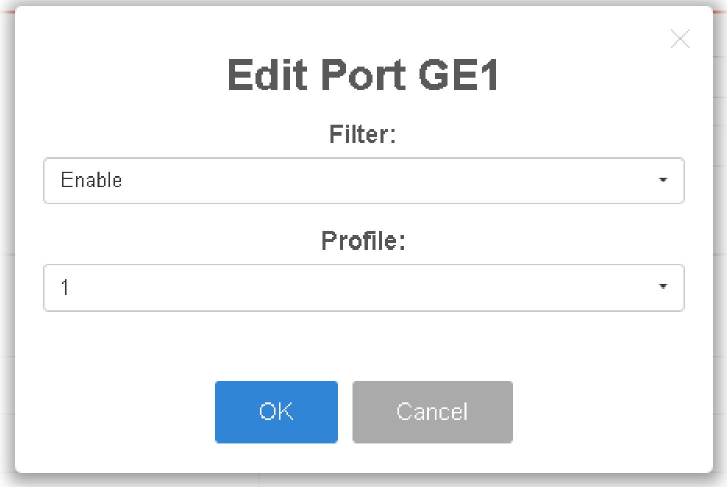
Ports: Nothing selected

Profile ID: Nothing selected □ Enable

Port	Profile ID	Edit
GE1	—	✓
GE2	—	✓
GE3	—	✓
GE4	—	✓
GE5	—	✓
GE6	—	✓
GE7	—	✓
GE8	—	✓
GE9	—	✓
GE10	—	✓
GE11	—	✓

Available settings are explained as follows:

Item	Description
Ports	Use the drop down list to specify LAN Port (GE/LAG).
Profile ID	Use the drop down list to choose the filtering profile for the select port/interface. ● **Enable -** Check this box first to make profile ID selection be available for choosing.
Apply	Apply the settings to the switch.
Edit	✓ - Click it to modify port setting (enabling / disabling filter function and choosing a profile for such interface).



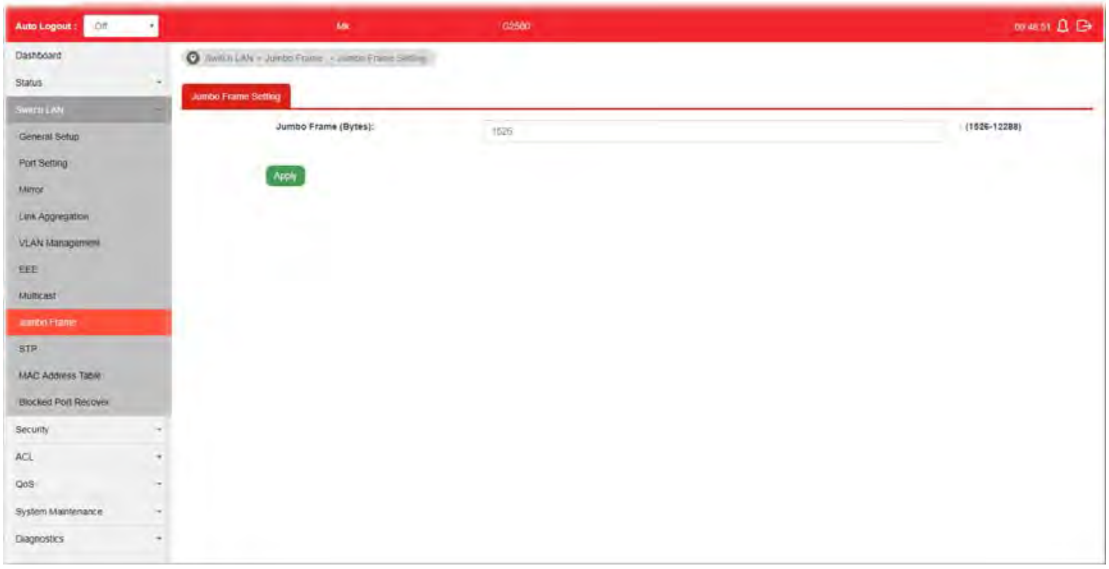
Edit Port GE1

Filter: Enable

Profile: 1

II-8 Jumbo Frame

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



Jumbo Frame (Bytes): 1526 (1526-12288)

Available settings are explained as follows:

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

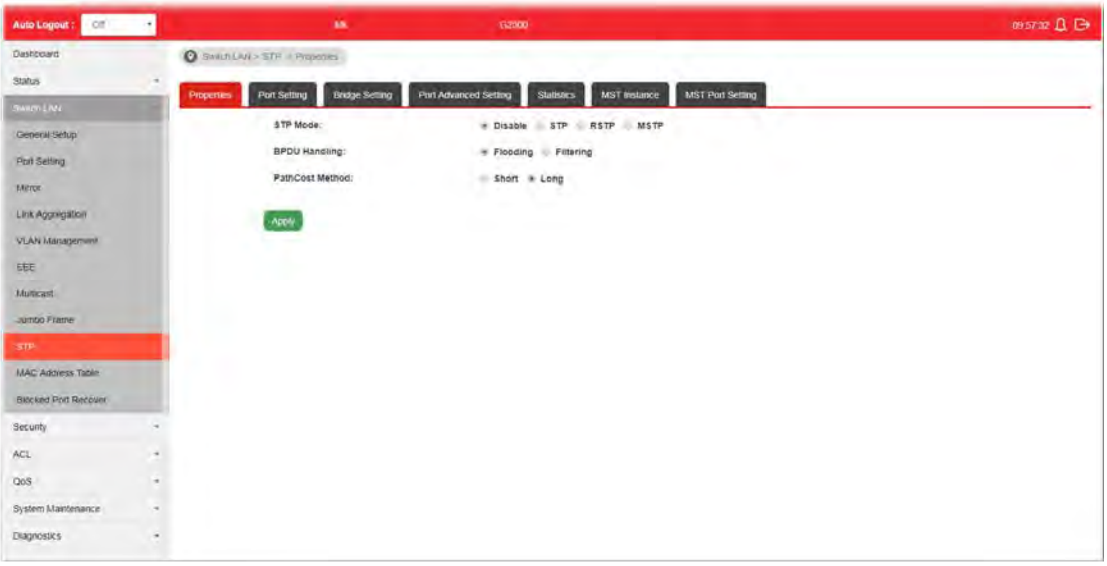
Bridge Protocol Data Units (BPDUs) are frames that contain information about the Spanning Tree Protocol (STP). Switches send BPDUs using a unique MAC address from its origin port and a multicast address as destination MAC (01:80:C2:00:00:00, or 01:00:0C:CC:CC:CD for Per VLAN Spanning Tree).

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 Spanning Tree Protocol (STP) property configuration.



STP Mode: ● Disable ○ STP ○ RSTP ○ MSTP

BPDU Handling: ● Flooding ○ Filtering

PathCost Method: ○ Short ● Long

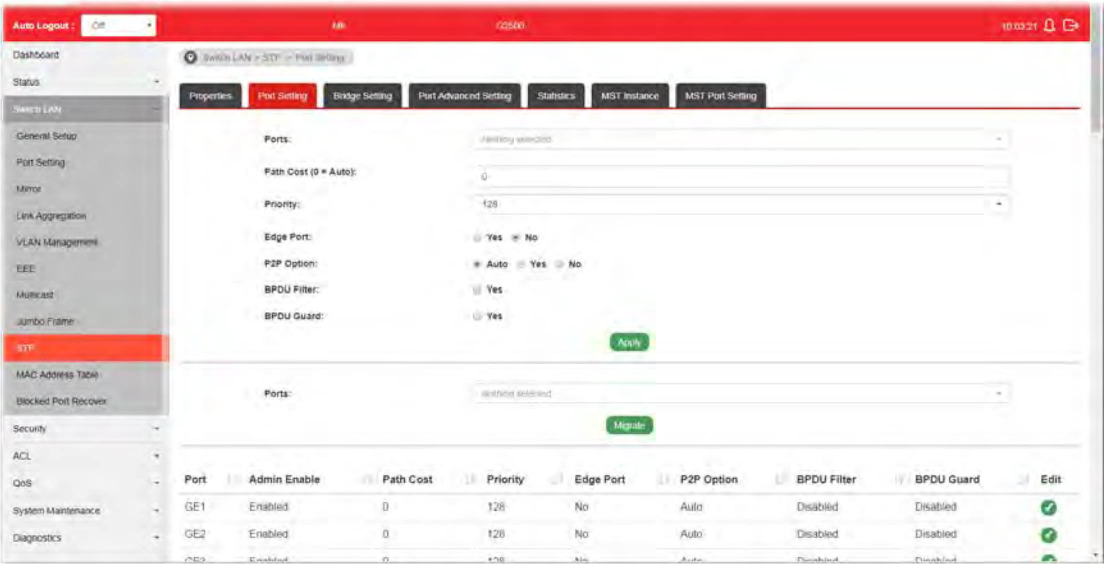
Available settings are explained as follows:

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. ● **MSTP** – Enable the Multiple Spanning Tree Protocol (MSTP) operation.
BPDU Handling	● 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	Apply the settings to the switch.

II-9-2 Port Setting

This page allows the user to configure and display Spanning Tree Protocol (STP) port settings.



Ports: Nothing selected

Path Cost (0 = Auto): 0

Priority: 128

Edge Port: ○ Yes ● No

P2P Option: ● Auto ○ Yes ○ No

BPDU Filter: □ Yes

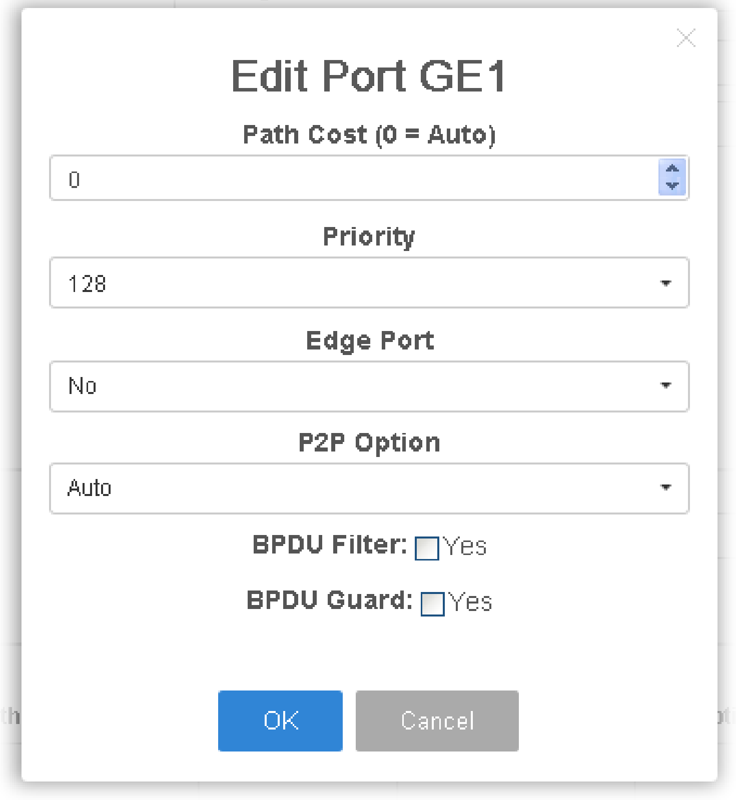
BPDU Guard: □ Yes

Ports: Nothing selected

Port	Admin Enable	Path Cost	Priority	Edge Port	P2P Option	BPDU Filter	BPDU Guard	Edit
GE1	Enabled	0	128	No	Auto	Disabled	Disabled	✓
GE2	Enabled	0	128	No	Auto	Disabled	Disabled	✓
GE3	Enabled	0	128	No	Auto	Disabled	Disabled	✓

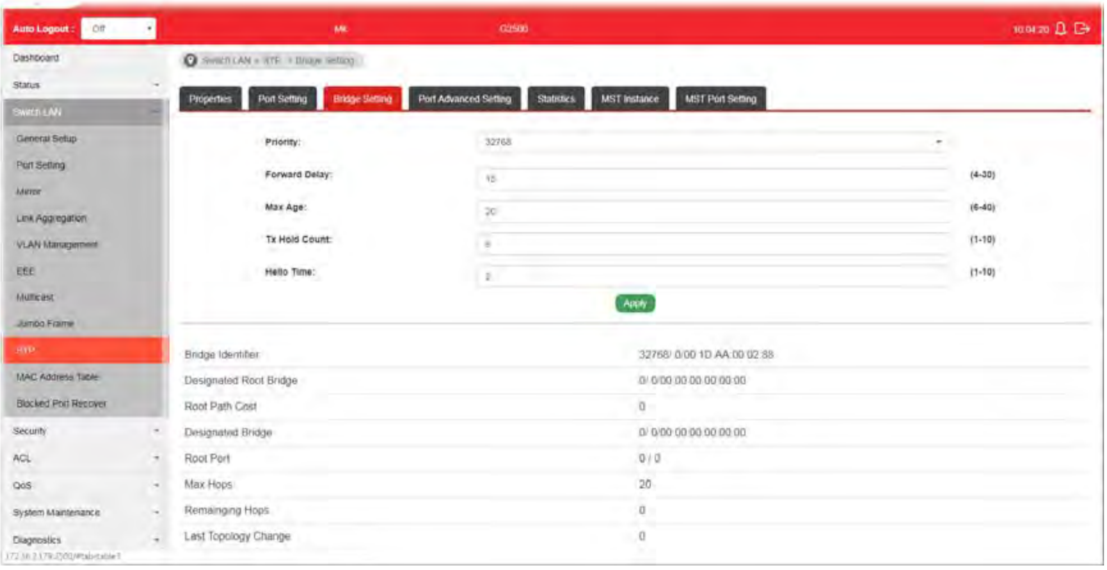
Available settings are explained as follows:

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.
Priority	Specify a priority value for the switch. The smaller the priority value, the higher the priority and greater chance of becoming the root.
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 Option	● **Auto -** VigorSwitch determines the STP of link type for this port automatically. ● **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.
BPDU Filter	**Yes -** Drop all BPDU packets and no BPDU will be sent.
BPDU Guard	**Yes -** BPDU Guard further protects your switch by turning this port into error state and shutdown if any BPDU received from this port. Check it to enable such function.
Apply	Apply the settings to the switch. After clicking it, the settings configured above will be shown on the table below.
Ports	Use the drop down to specify the interface(s) for applying the function of **Migrate**.
Migrate	Click it to force the port(s) specified above to send one RSTP BPDU (Rapid Spanning Tree Protocol Bridge Protocol Data Unit).
Edit	Click it to modify the settings for the selected GE port.  Edit Port GE1 Path Cost (0 = Auto): 0 Priority: 128 Edge Port: No P2P Option: Auto BPDU Filter: □Yes BPDU Guard: □Yes

II-9-3 Bridge Setting

This page allows the network administrator 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)

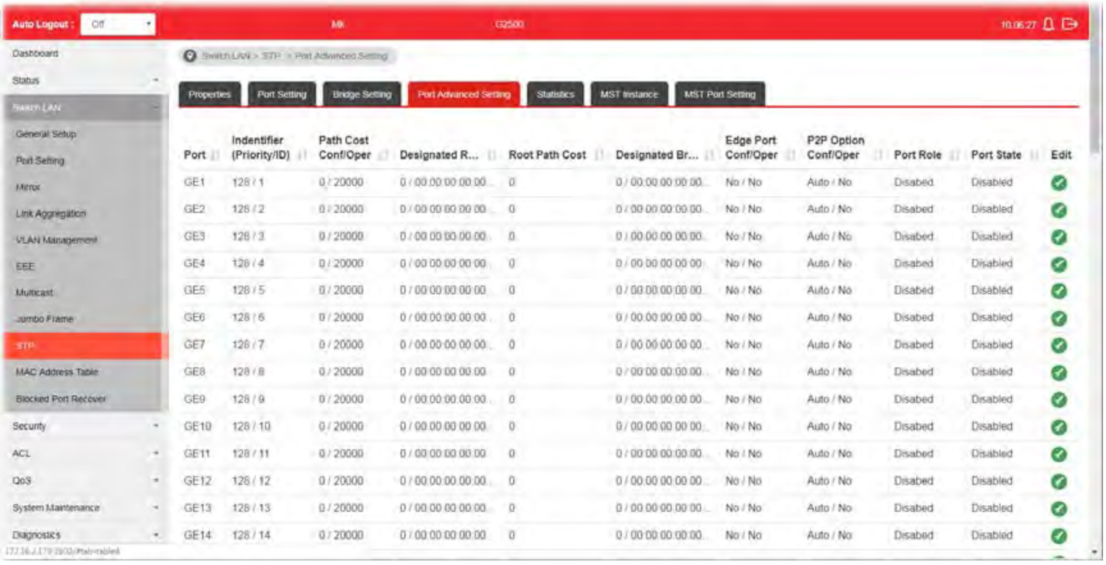
Bridge Identifier	32768/ 0:00 1D AA 00 02 88
Designated Root Bridge	0/ 0/00 00 00 00 00 00
Root Path Cost	0
Designated Bridge	0/ 0/00 00 00 00 00 00
Root Port	0 / 0
Max Hops	20
Remainging Hops	0
Last Topology Change	0

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 30 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	Apply the settings to the switch.

II-9-4 Port Advanced Setting

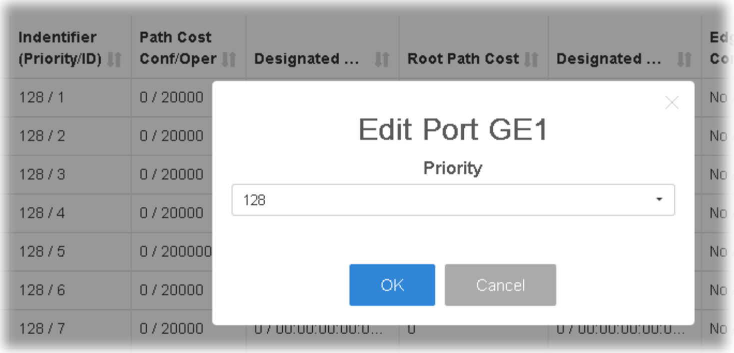
This page allows user to edit general setting of STP CIST port and browser CIST port status.



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

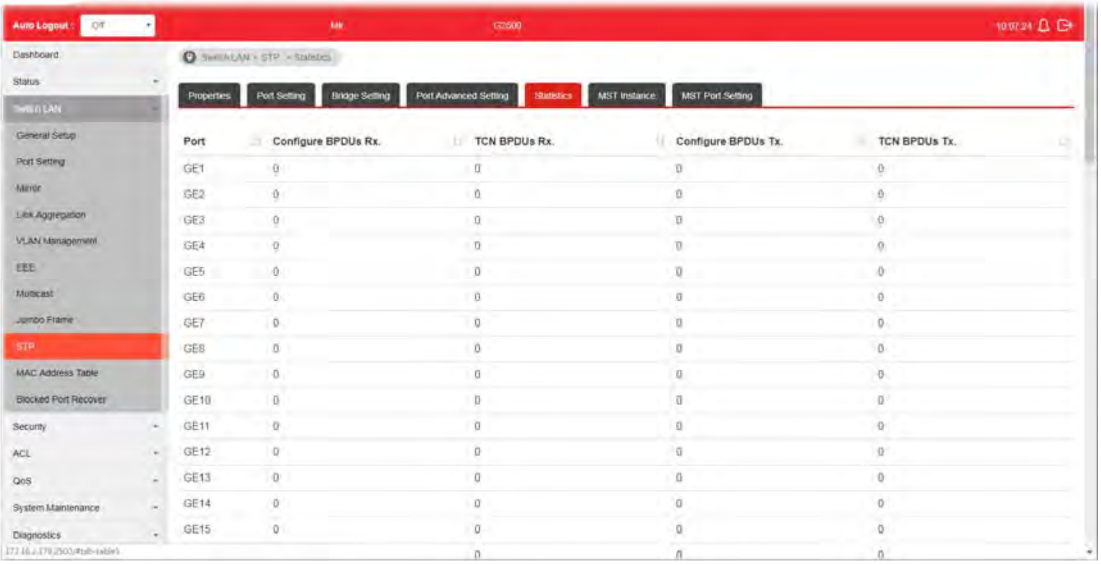
Available settings are explained as follows:

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 priority setting for the selected GE port / LAG port.

	 Edit Port GE1 Priority: 128

II-9-5 Statistics

This page displays STP statistics.



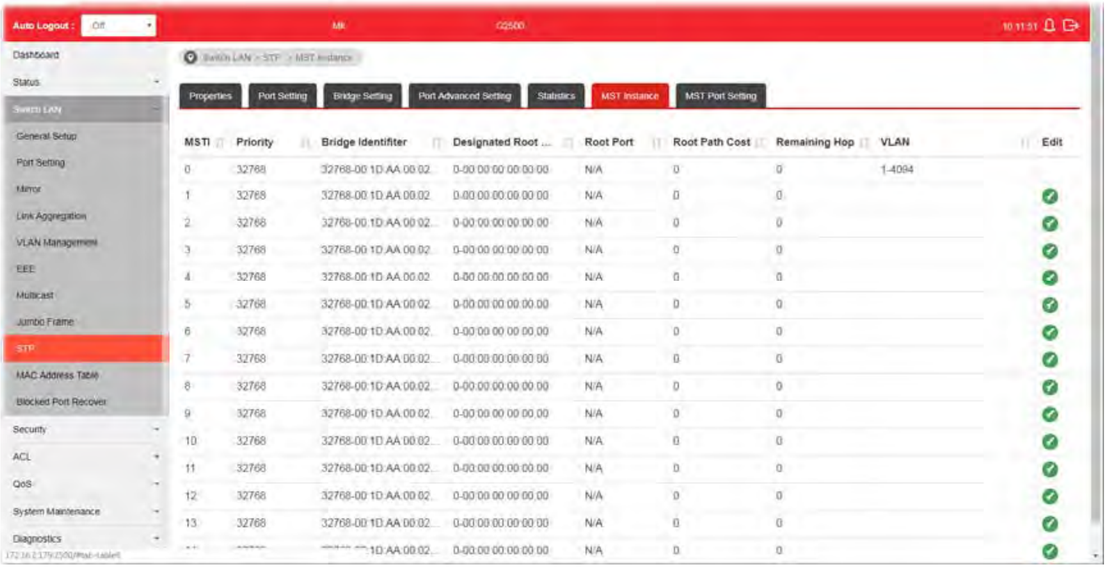
Port	Configure BPDUs Rx.	TCN BPDUs Rx.	Configure BPDUs Tx.	TCN BPDUs Tx.
GE1	0	0	0	0
GE2	0	0	0	0
GE3	0	0	0	0
GE4	0	0	0	0
GE5	0	0	0	0
GE6	0	0	0	0
GE7	0	0	0	0
GE8	0	0	0	0
GE9	0	0	0	0
GE10	0	0	0	0
GE11	0	0	0	0
GE12	0	0	0	0
GE13	0	0	0	0
GE14	0	0	0	0
GE15	0	0	0	0

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.

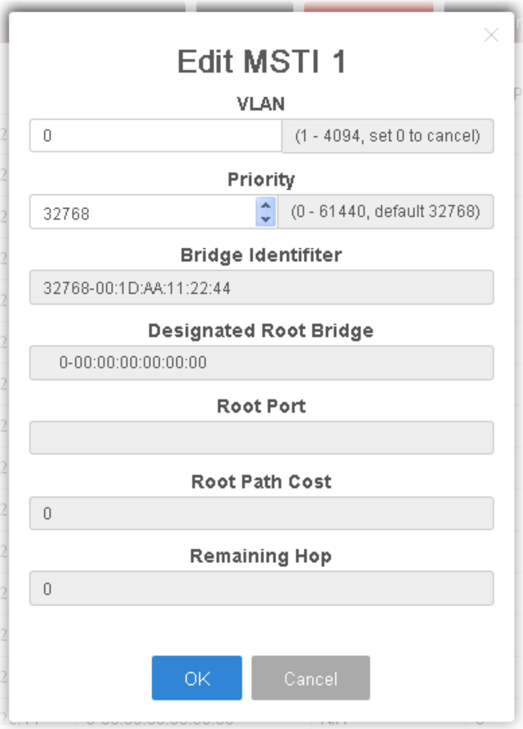
II-9-6 MST Instance

MSTP allows traffic of different VLAN to be mapped into different MST Instances. VigorSwitch supports up to 16 independent MST instances (0~15) with which the VLAN can be associated.



MSTI	Priority	Bridge Identifiter	Designated Root ...	Root Port	Root Path Cost	Remaining Hop	VLAN	Edit
0	32768	32768-00:1D:AA:00:02...	0-00:00:00:00:00:00	N/A	0	0	1-4094	
1	32768	32768-00:1D:AA:00:02	0-00:00:00:00:00:00	N/A	0	0		✓
2	32768	32768-00:1D:AA:00:02...	0-00:00:00:00:00:00	N/A	0	0		✓
3	32768	32768-00:1D:AA:00:02...	0-00:00:00:00:00:00	N/A	0	0		✓
4	32768	32768-00:1D:AA:00:02	0-00:00:00:00:00:00	N/A	0	0		✓
5	32768	32768-00:1D:AA:00:02...	0-00:00:00:00:00:00	N/A	0	0		✓
6	32768	32768-00:1D:AA:00:02...	0-00:00:00:00:00:00	N/A	0	0		✓
7	32768	32768-00:1D:AA:00:02...	0-00:00:00:00:00:00	N/A	0	0		✓
8	32768	32768-00:1D:AA:00:02...	0-00:00:00:00:00:00	N/A	0	0		✓
9	32768	32768-00:1D:AA:00:02...	0-00:00:00:00:00:00	N/A	0	0		✓
10	32768	32768-00:1D:AA:00:02...	0-00:00:00:00:00:00	N/A	0	0		✓
11	32768	32768-00:1D:AA:00:02...	0-00:00:00:00:00:00	N/A	0	0		✓
12	32768	32768-00:1D:AA:00:02...	0-00:00:00:00:00:00	N/A	0	0		✓
13	32768	32768-00:1D:AA:00:02...	0-00:00:00:00:00:00	N/A	0	0		✓
[illegible]	[illegible]	[illegible]1D:AA:00:02...	0-00:00:00:00:00:00	N/A	0	0		✓

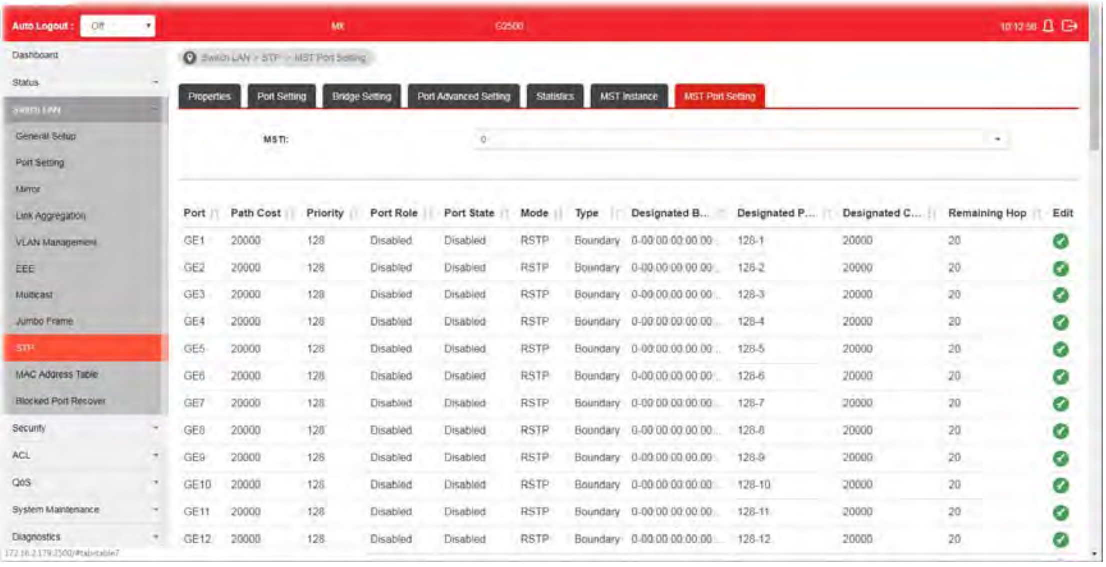
Available settings are explained as follows:

Item	Description
MSTI	Display the index number of MST Instance. Each MSTI can have one or multiple VLANs.
Edit	✓ - Click it to modify the priority setting for the selected GE port / LAG port.  Edit MSTI 1 VLAN: 0 (1 - 4094, set 0 to cancel) Priority: 32768 (0 - 61440, default 32768) Bridge Identifiter: 32768-00:1D:AA:11:22:44 Designated Root Bridge: 0-00:00:00:00:00:00 Root Port: Root Path Cost: 0 Remaining Hop: 0 ● **VLAN -** Enter the ID (1-4094) of the VLAN which should be

	associated with this MSTI. ● **Priority -** The switch priority for this MST instance. A lower number gives the switch higher chance to be chosen as the root bridge. ● **Bridge Identifiter -** Display the priority of MSTI instance number + MAC address of the switch. ● **Designated Root Bridge -** Display the Bridge Identifier of the root bridge. ● **Root Port -** Display the port toward the root. ● **Root Path Cost -** Display the path cost toward the root. ● **Remaining Hop** – Display the remaining hop count in BPDU. ● VLAN - Display the range of VLAN ID numbers. ● **OK** – Save the modifications.

II-9-7 MST Port Setting

MST Port Settings is used to configure the GE port / LAG group settings for each MST instance. The table displays the MST parameters for each port.

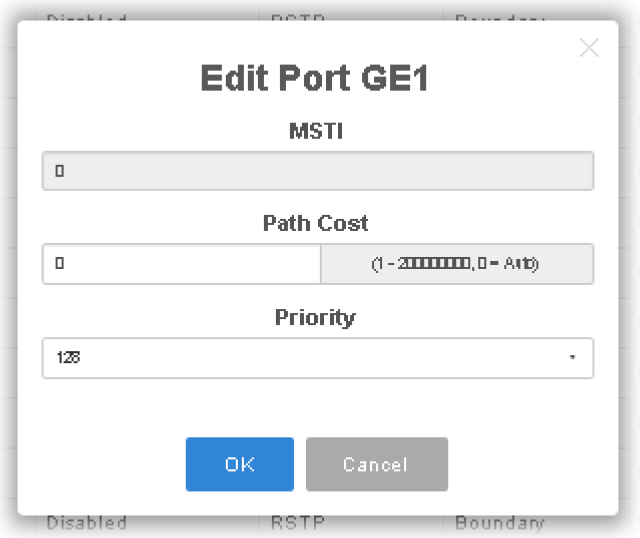


MSTI: 0

Port	Path Cost	Priority	Port Role	Port State	Mode	Type	Designated B...	Designated P...	Designated C...	Remaining Hop	Edit
GE1	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00...	128-1	20000	20	✓
GE2	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00...	128-2	20000	20	✓
GE3	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00...	128-3	20000	20	✓
GE4	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00...	128-4	20000	20	✓
GE5	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00...	128-5	20000	20	✓
GE6	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00...	128-6	20000	20	✓
GE7	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00...	128-7	20000	20	✓
GE8	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00...	128-8	20000	20	✓
GE9	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00...	128-9	20000	20	✓
GE10	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00...	128-10	20000	20	✓
GE11	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00...	128-11	20000	20	✓
GE12	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00...	128-12	20000	20	✓

Available settings are explained as follows:

Item	Description
MSTI	Select one of the MST instances.
Edit	🔧 - Click it to modify the path cost and priority setting for the port.



Edit Port GE1

MSTI: 0

Path Cost: 0 (1 - 200000000, 0 = Auto)

Priority: 128

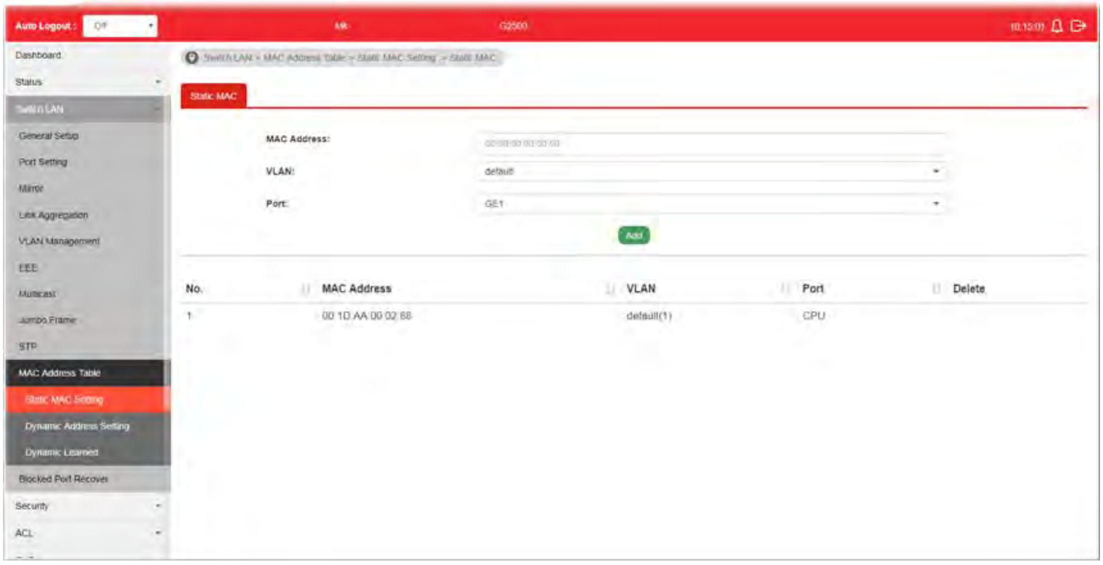
- **MSTI** – Display the selected MST instance.
- **Path Cost** – Set path cost value for the port. A port with lowest value will be used as the forwarding port by spanning tree. Default value was set according to the bandwidth of the port.
- **Priority** – Among the ports with same path cost, port with lower priority will have higher chance to be used as the forwarding port by spanning tree. Use the drop down list to choose desired priority value.

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

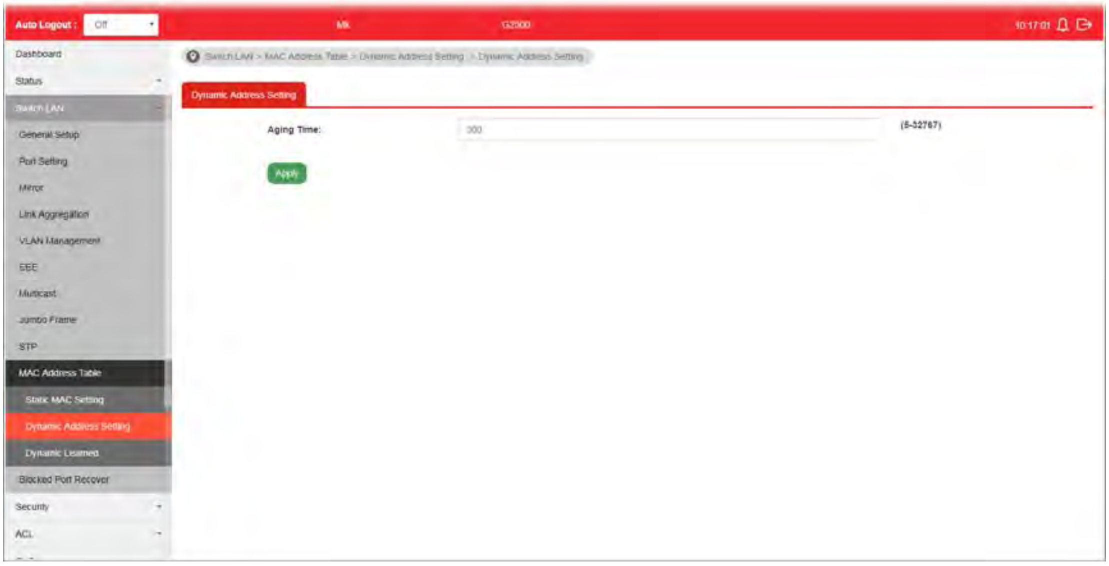
No.	MAC Address	VLAN	Port	Delete
1	00:1D:AA:00:02:68	default(1)	CPU	

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.



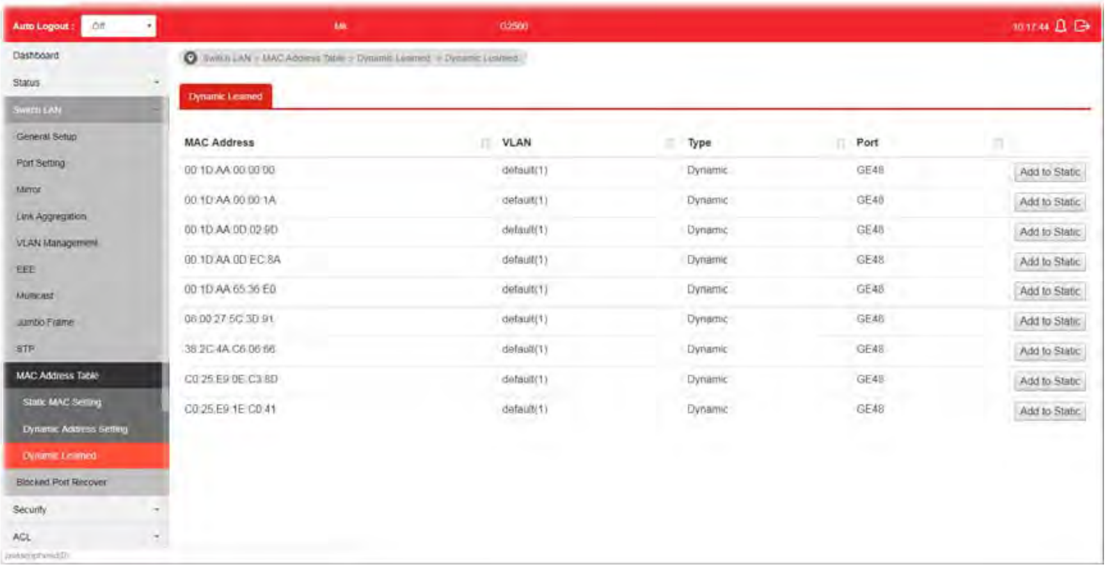
Aging Time: 300 (5-32767)

Available settings are explained as follows:

Item	Description
Aging Time	Enter the Dynamic MAC address aging out value (5-32767 seconds).
Apply	Apply the settings 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	
00:1D:AA:00:00:00	default(1)	Dynamic	GE48	Add to Static
00:1D:AA:00:00:1A	default(1)	Dynamic	GE48	Add to Static
00:1D:AA:0D:02:9D	default(1)	Dynamic	GE48	Add to Static
00:1D:AA:0D:EC:8A	default(1)	Dynamic	GE48	Add to Static
00:1D:AA:65:36:E0	default(1)	Dynamic	GE48	Add to Static
08:00:27:5C:3D:91	default(1)	Dynamic	GE48	Add to Static
38:2C:4A:C6:06:66	default(1)	Dynamic	GE48	Add to Static
C0:25:E9:0E:C3:8D	default(1)	Dynamic	GE48	Add to Static
C0:25:E9:1E:C0:41	default(1)	Dynamic	GE48	Add to Static

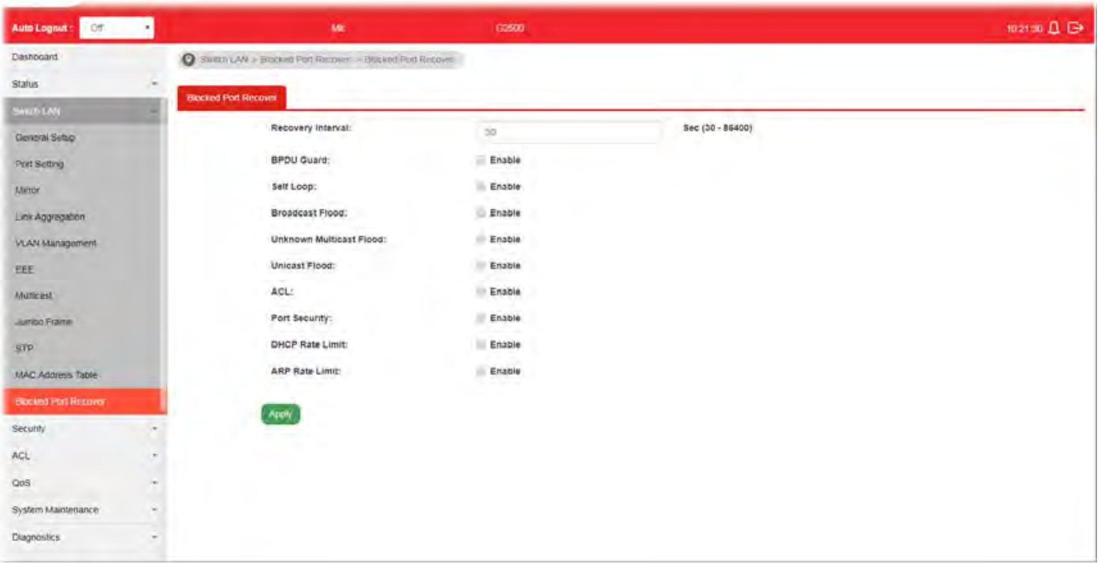
Available settings are explained as follows:

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.

II-11 Blocked Port Recover

This page is used for configuring settings to recover the port which is being blocked by the following functions after a defined period of time.



Recovery Interval: 30 Sec (30 - 86400)

BPDU Guard: □ Enable

Self Loop: □ Enable

Broadcast Flood: □ Enable

Unknown Multicast Flood: □ Enable

Unicast Flood: □ Enable

ACL: □ Enable

Port Security: □ Enable

DHCP Rate Limit: □ Enable

ARP Rate Limit: □ Enable

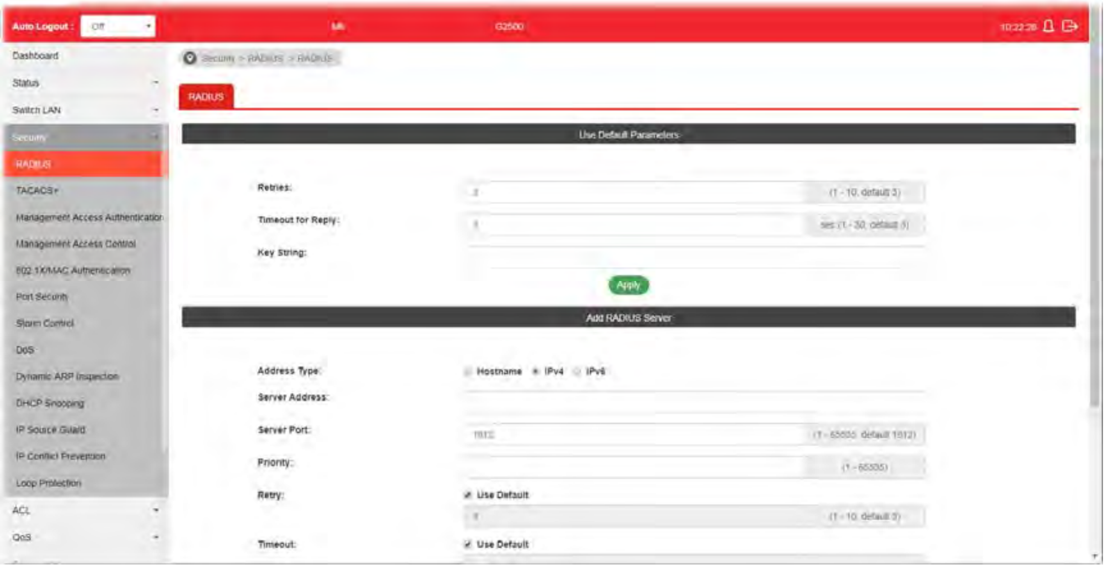
Available settings are explained as follows:

Item	Description
Recovery Interval	The port being blocked will be able to receive and send traffic after the time period configured here.
BPDU Guard	**Enable** – Recover the port being blocked by BPDU Guard after the time set in Recovery Interval.
Self Loop	**Enable** – Recover the port being blocked by self loop Guard after the time set in Recovery Interval.
Broadcast Flood	**Enable** –Recover the port being blocked by broadcast flood after the time set in Recovery Interval.
Unknown Multicast Flood	**Enable** – Recover the port being blocked by unknown multicast flood after the time set in Recovery Interval.
Unicast Flood	**Enable** – Recover the port being blocked by unicast flood after the time set in Recovery Interval.
ACL	**Enable** – Recover the port being blocked by ACL after the time set in Recovery Interval.
Port Security	**Enable** – Recover the port being blocked by port security after the time set in Recovery Interval.
DHCP Rate Limit	**Enable** – Recover the port being blocked by DHCP rate limit after the time set in Recovery Interval.
ARP Rate Limit	**Enable** – Recover the port being blocked by ARP rate limit after the time set in Recovery Interval.
Apply	Apply the settings to the switch.

Part III Security

III-1 RADIUS

This page allows the network administrator to add and configure multiple RADIUS servers.



Retries: (1 - 10, default 3)

Timeout for Reply: sec (1 - 30, default 5)

Key String:

Address Type: ○ Hostname ● IPv4 ○ IPv6

Server Address:

Server Port: 1812 (1 - 65535, default 1812)

Priority: (1 - 65535)

Retry: ☑ Use Default (1 - 10, default 3)

Timeout: ☑ Use Default

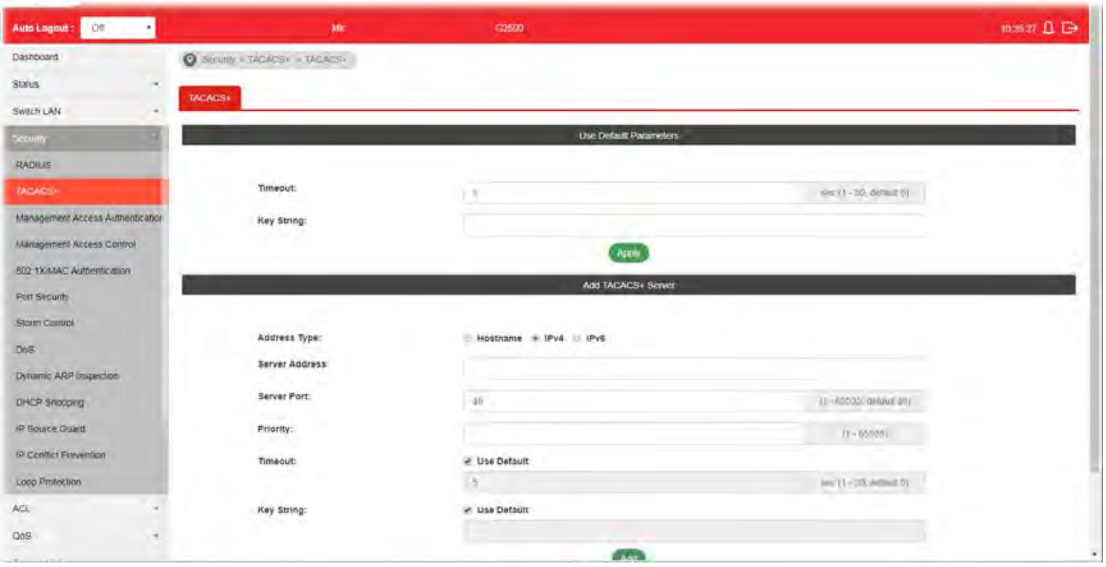
Available settings are explained as follows:

Item	Description
Use Default Parameters	● **Retries** - The retry time before this server being considered not-reachable. ● **Timeout for Reply** – Set the time (in seconds) before this server being considered lost connection. ● **Key String** – Enter the string used to encrypt and authenticate with RADIUS server. ● **Apply** - Save the settings.
Add RADIUS Server	● **Address Type** – Specify whether switch uses a hostname to resolve address by DNS to connect to server, or directly connect using IPv4 address. ● **Sever Address** – Enter the server's address corresponding with address type given. ● **Server Port** – Enter the port number used by RADIUS server. ● **Priorty** - Specify the priority that switch uses this server. The higher number, the lower priority. Switch will start with server with lowest priority. ● **Retry** – Set the time before this server being considered not-reachable ● **Timeout** – Set the time (in seconds) before this server being considered lost connection. ● **Key String** – Enter the key string used for encrypting and authenticating with server. Unless Key String is specified here, the default string will be used. ● **Usage** –Specify whether you would like to use this server for switch login authentication or 802.1x access port authentication, or both. ● **Add** – Click it to add a new RADIUS server and display in

	this page. 🔧 under **Edit**- Click it to modify the priority setting for the selected GE port / LAG port.

III-2 TACACS+

This page allows the network administrator to add and configure multiple TACACS+ server.



Timeout: 5 sec (1 - 30, default 5)

Key String:

Address Type: ○ Hostname ● IPv4 ○ IPv6

Server Address:

Server Port: 49 (1 - 65535, default 49)

Priority: (1 - 65535)

Timeout: ☑ Use Default 5 sec (1 - 30, default 5)

Key String: ☑ Use Default

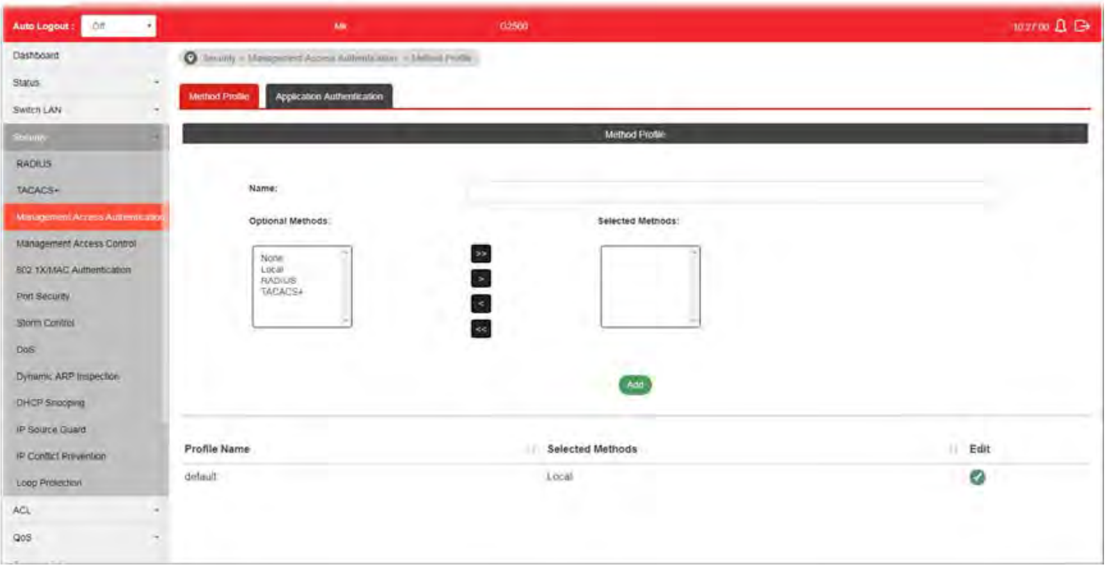
Available settings are explained as follows:

Item	Description
Use Default Parameters	● **Timeout** –Set the time (in seconds) before this server being considered lost connection. ● **Key String** – Enter the string used to encrypt and authenticate with TACACS+ server. ● **Apply** - Save the settings.
Add TACACS+ Server	● **Address Type** – Specify whether switch use a hostname to resolve address by DNS to connect to server, or directly connect using IPv4 address. ● **Sever Address** – Enter the server's address corresponding with address type given. ● **Server Port** – Enter the port number used by TACACS+ server. ● **Priorty** - Specify the priority that switch uses this server. The higher number, the lower priority. Switch will start with server with lowest priority. ● **Timeout** –Set the time (in seconds) before this server being considered lost connection. ● **Key String** – Enter the key string used for encrypting and authenticating with server. Unless Key String is specified here, the default string will be used. ● **Add** – Click it to add a new RADIUS server and display in this page. 🔧 under **Edit**- Click it to modify the priority setting for the selected GE port / LAG port.

III-3 Management Access Authentication

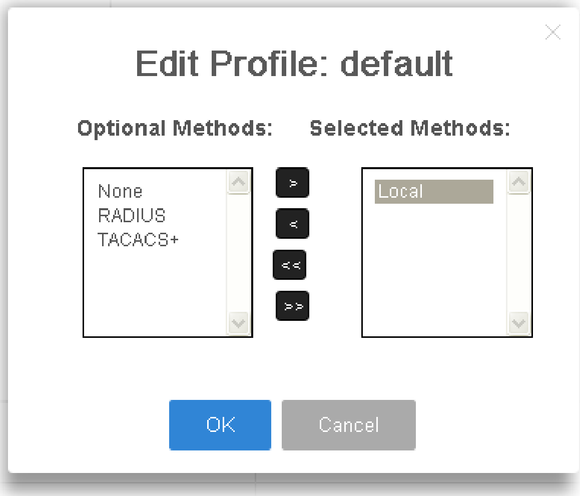
III-3-1 Method Profile

This page allows a user to create method list for applying on management service.



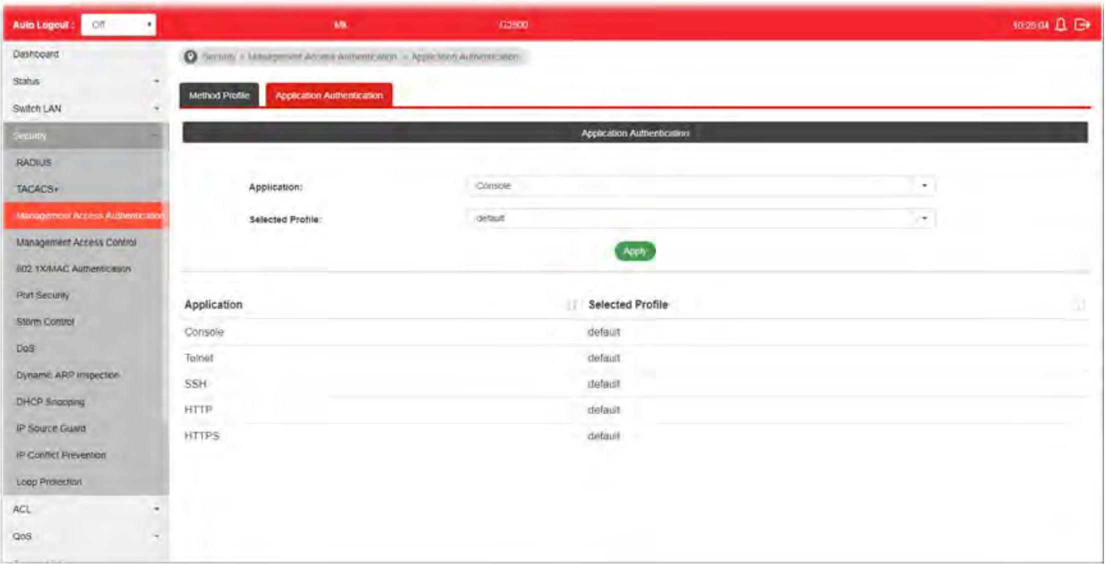
Profile Name	Selected Methods	Edit
default	Local	✓

Available settings are explained as follows:

Item	Description
Method Profile	● **Name** – Enter a name for creating a method. ● **Optional Methods** – Available methods include Local, RADIUS and TACACS+. ● **Selected Methods** – The method listed in this field will be applied for such method profile. ● **Add** – Click it to add a method from Optional Method onto Selected Method.
🔧 under **Edit**	Click it to modify the optional methods/selected methods for the selected profile.  Edit Profile: default Optional Methods: Selected Methods: None RADIUS TACACS+ > < << >> Local OK Cancel

III-3-2 Application Authentication

This page allows the network administrator to select the customized Method List to apply to any management service, for management access control.



Application Authentication

Application: Console

Selected Profile: default

Application	Selected Profile
Console	default
Telnet	default
SSH	default
HTTP	default
HTTPS	default

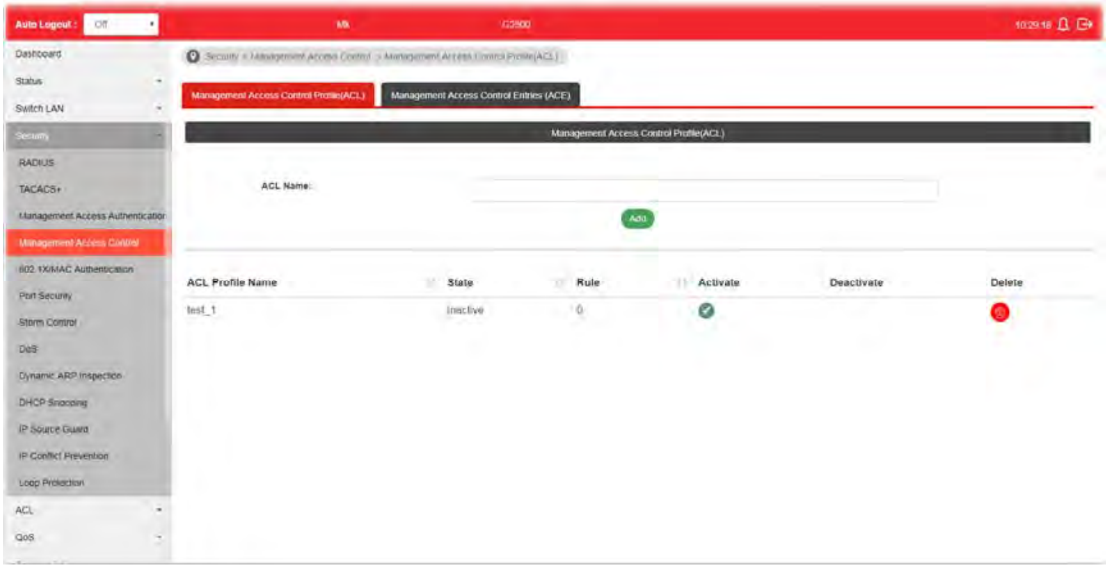
Available settings are explained as follows:

Item	Description
Application	There are five methods to be configured with different profile respectively. ● Console/Telnet/SSH/HTTP/HTTPS
Selected Profile	Specify one of customized method profiles to apply to any management service, for management access control.
Apply	Save the settings.

III-4 Management Access Control

III-4-1 Management Access Control Profile (ACL)

This page allows a user to add, edit, and delete Management Access Control profiles.


Auto Logout : Off
MA
G2500
10:29:18
Dashboard
Status
Switch LAN
Security
RADIUS
TACACS+
Management Access Authentication
Management Access Control
802.1X/MAC Authentication
Port Security
Storm Control
DoS
Dynamic ARP Inspection
DHCP Snooping
IP Source Guard
IP Conflict Prevention
Loop Protection
ACL
QoS
Security > Management Access Control > Management Access Control Profile(ACL)
Management Access Control Profile(ACL)
Management Access Control Entries (ACE)
Add

Management Access Control Profile(ACL)

ACL Name:

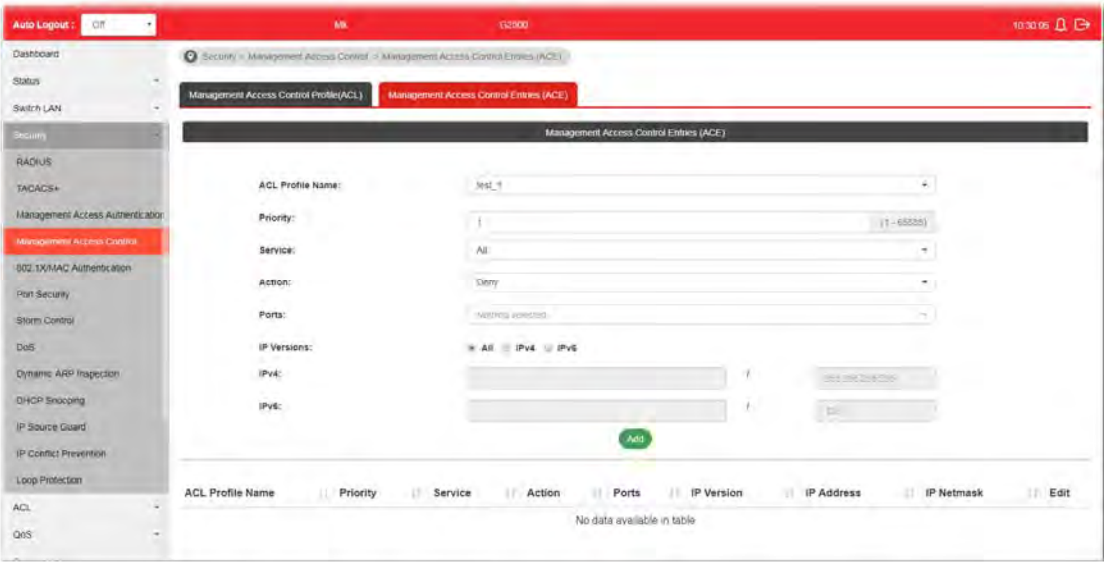
ACL Profile Name	State	Rule	Activate	Deactivate	Delete
test_1	Inactive	0	✓		●

Available settings are explained as follows:

Item	Description
ACL Name	Enter a name to create a profile for ACL. Once a profile is created, it will be displayed on this page.
Add	Click it to create a new ACL profile after entering the ACL name.
ACL Profile Name	Display the name of the ACL profile.
State	Display if such ACL profile is active or inactive.
Rule	Display the number of ACE used by this ACL profile.
Activate / Deactivate	🔧 **-** Click it to activate / deactivate such entry. To configure detailed settings for the selected ACL profile, do not click Activate for that profile.
Delete	Click the icon under Delete to remove the selected entry.

III-4-2 Management Access Control Entries (ACE)

This page allows a user to add, edit, or remove Access Control Entries (ACE) of the Management Access Control profiles. However, only the ACE of inactive profiles can be modified, and before configuring ACE, at least one ACL profile should be created.


Auto Logout : Off
Mk
G2500
10:30:05
Dashboard
Status
Switch LAN
Security
RADIUS
TACACS+
Management Access Authentication
Management Access Control
802.1X/MAC Authentication
Port Security
Storm Control
DoS
Dynamic ARP Inspection
DHCP Snooping
IP Source Guard
IP Conflict Prevention
Loop Protection
ACL
QoS
Security > Management Access Control > Management Access Control Entries (ACE)
Management Access Control Profile(ACL)
Management Access Control Entries (ACE)
Add

Management Access Control Entries (ACE)

ACL Profile Name: test_1

Priority: 1 (1 - 65535)

Service: All

Action: Deny

Ports: Nothing selected

IP Versions: ● All ○ IPv4 ○ IPv6

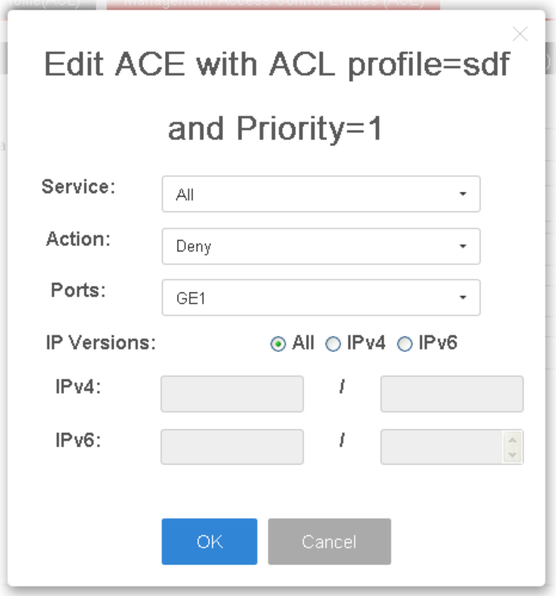
IPv4: /

IPv6: /

ACL Profile Name	Priority	Service	Action	Ports	IP Version	IP Address	IP Netmask	Edit
No data available in table								

Available settings are explained as follows:

Item	Description
ACL Profile Name	Use the drop-down list to select the inactive ACL profile you would like to modify.
Priority	Specify a priority number (1 to 65535) for such rule. The lower the number, the higher the priority.
Service	Choose the service type you would like to control the access.
Action	Select the action to be taken on the traffic of selected service type. ● **Deny** – Incoming / outgoing data which meets ACE rules will be blocked. ● **Permit** – Incoming / outgoing data which meets ACE rule is allowed to pass through.
Ports	Select the ports to which the ACL should be applied.
IP Versions	Specify the IP address/subnet to which the ACL should be applied. ● **All** – All the IP address should be applied. ● **IPv4** – Specify the IPv4 address /subnet. **IPv6** –Specify the IPv6 address /subnet.
IPv4	Enter the IPv4 address/subnet to which the ACE rule should apply.
IPv6	Enter the IPv6 address/subnet to which the ACE rule should apply.
Add	Click it to create an ACE rule profile. Then, such ACE rule profile will be shown on the table below.

Edit	🔧 - click it to modify the settings for the selected entry.  Edit ACE with ACL profile=sdf and Priority=1 Service: All Action: Deny Ports: GE1 IP Versions: ● All ○ IPv4 ○ IPv6 IPv4: / IPv6: / 🗑 - click it to remove the selected entry.

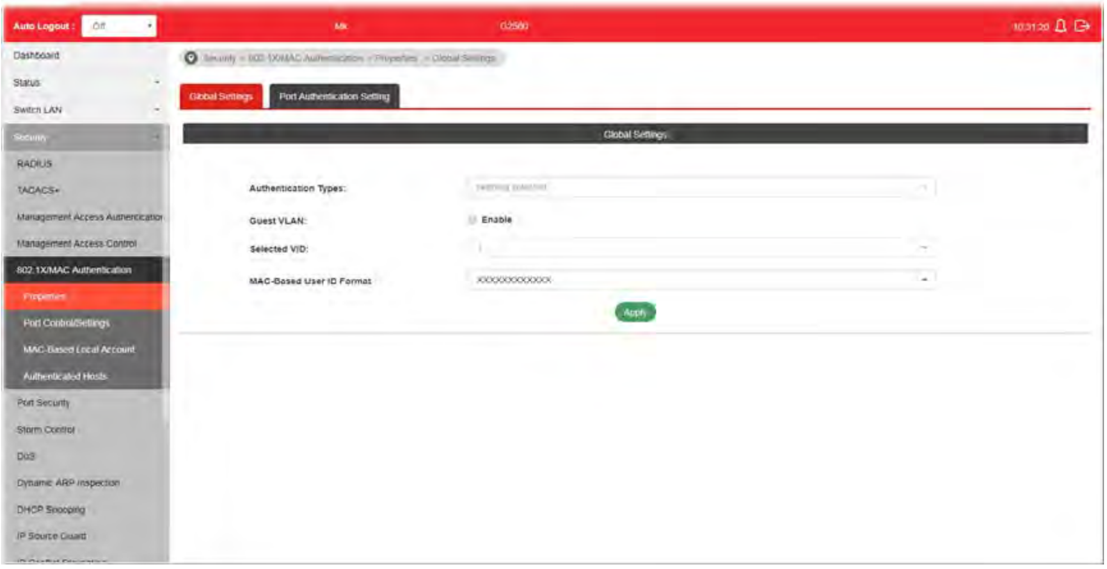
III-5 802.1X/MAC Authentication

The authentication manager allows you to configure securely access from any host connected to physical ports. You may apply multiple ways of authentication to each port.

III-5-1 Properties

III-5-1-1 Global Settings

VigorSwitch G2500 supports 802.1x and MAC-based authentication methods. In Global Settings page, you can specify authentication type, enable Guest VLAN function, specify a VID and select format for MAC address entry.



Authentication Types: Nothing selected

Guest VLAN: □ Enable

Selected VID: 1

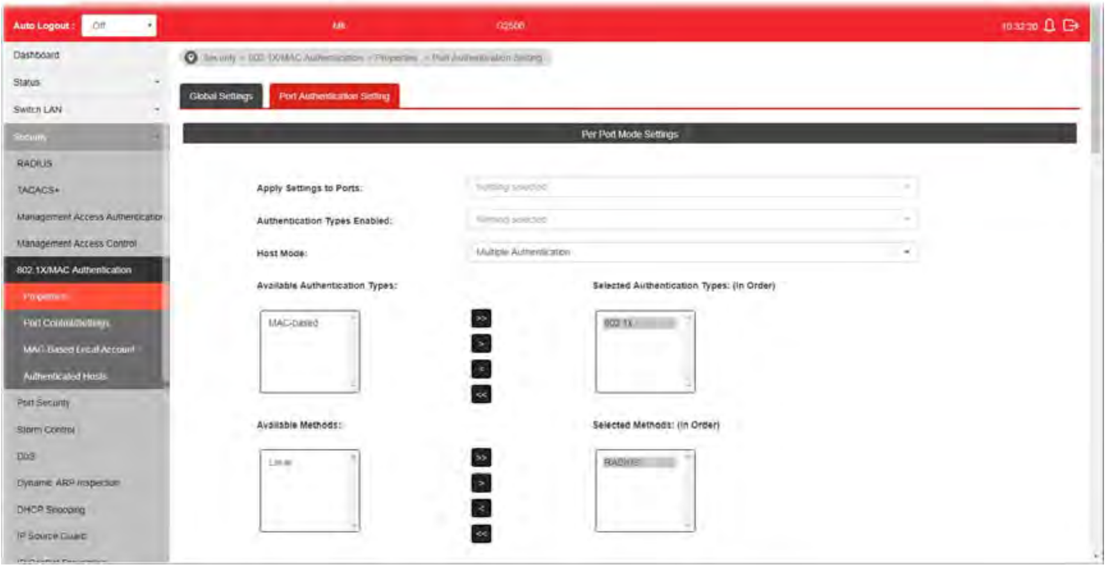
MAC-Based User ID Format: XXXXXXXXXXXX

Available settings are explained as follows:

Item	Description
Authentication Types	Use the drop down list to specify which type (802.1x, MAC-based) will be used for authentication. Choose to enable 802.1x or MAC-based authenticate method for host connecting to Ethernet port. You may configure which type to be used per port, but enabling any per port without enabling here will not be effective.
Guest VLAN	Check to enable a Guest VLAN for those have not successfully authenticated with any given methods. Choose one of the VLAN ID as a Guest VLAN.
Selected VID	If Guest VLAN is enabled, use the drop down list to specify one VID number.
MAC-Based User ID Format	Specify how the MAC-based user ID should be expressed in EAP message between AAA server and switch.
Apply	Save and activate the settings configured above.

III-5-1-2 Port Authentication Setting

This page allows the network administrator to configure detailed authentication settings for each port.



Apply Settings to Ports: Nothing selected

Authentication Types Enabled: Nothing selected

Host Mode: Multiple Authentication

Available Authentication Types: MAC-based

Selected Authentication Types: (In Order) 802.1X

Available Methods: Local

Selected Methods: (In Order) RADIUS

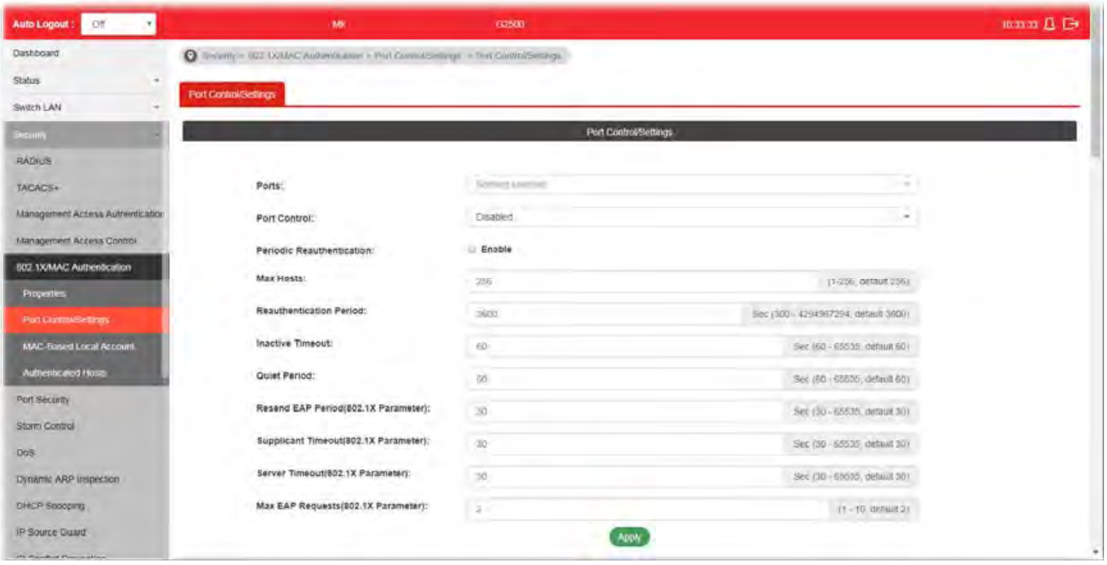
Available settings are explained as follows:

Item	Description
Apply Settings to Ports	Select physical port(s) for applying settings. Note that port authentication will not be effective if none of them were enabled.
Authentication Types Enabled	Select 802.1x and/or MAC-based authenticate method for host connecting to this port.
Host Mode	● **Multiple Authentication** - Each host are authenticated individually. ● **Multiple Hosts** - Authentication is done on port basis, only one authenticated host is required; other hosts connected to this port can access freely as authenticated host. ● **Single Host** - Only one host can be authenticated, and access the port.
Available Authentication Types	Display available authentication types of AAA server (or local) you wish to have on this port.
Selected Authentication Types	Specify the order of authentication type you wish to have on this port.
Available Methods	Display available methods of AAA server (or local) you wish to have on this port.
Selected Methods	Specify the order of authentication methods you wish to have on this port.
Guest VLAN	Check **Enable** to enable Guest VLAN on this port for those didn't authenticated successfully.
RADIUS VLAN Assignment	● **Disable -** Switch will ignore the VLAN assignment from the RADIUS server and keep the original VLAN of the host. ● **Static** – Switch will use the VLAN assignment from the RADIUS server if it receives the information. If there is not VLAN information, it will keep the original VLAN of

	the host. ● **Reject** - Switch will reject the host if it does not receive the VLAN information from RADIUS server.
Apply	The modification made above can be applied on to the selected GE port immediately.

III-5-2 Port Control/Settings

This page allows the network administrator to controls port setting, based on 802.1X, for ethernet port authentication.



Port Control/Settings

Ports:

Port Control: Disabled

Periodic Reauthentication: □ Enable

Max Hosts: 256 (1-256, default 256)

Reauthentication Period: 3600 Sec (300 - 4294967294, default 3600)

Inactive Timeout: 60 Sec (60 - 65535, default 60)

Quiet Period: 60 Sec (60 - 65535, default 60)

Resend EAP Period(802.1X Parameter): 30 Sec (30 - 65535, default 30)

Supplicant Timeout(802.1X Parameter): 30 Sec (30 - 65535, default 30)

Server Timeout(802.1X Parameter): 30 Sec (30 - 65535, default 30)

Max EAP Requests(802.1X Parameter): 2 (1 - 10, default 2)

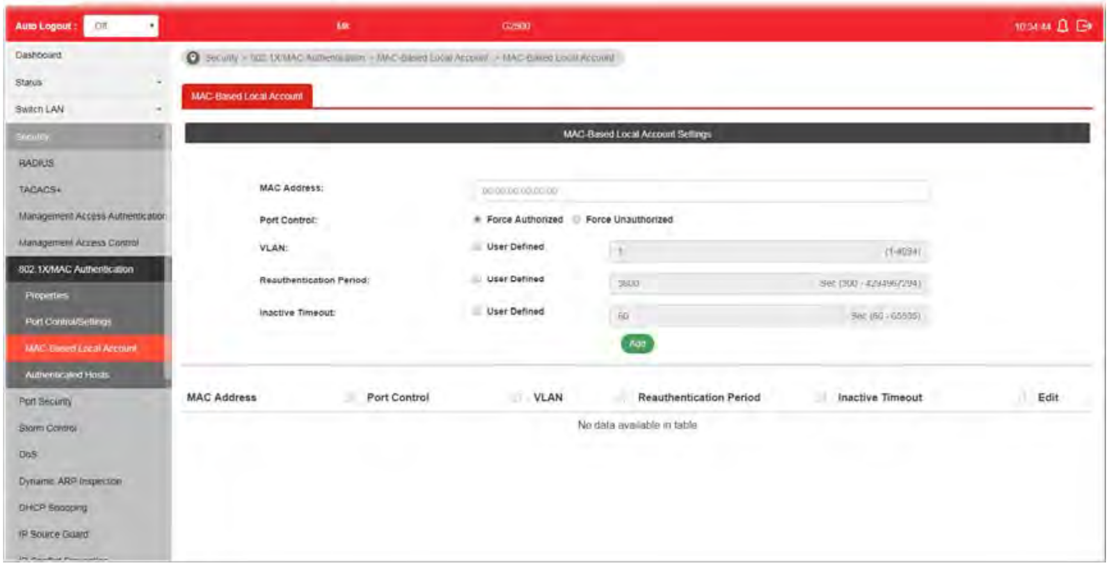
Available settings are explained as follows:

Item	Description
Ports	Select the ports to modify the port control settings.
Port Control	Specify if you wish this account to be allowed (Authorized) or blocked (Unauthorized) or determined by VigorSwtich (Auto). ● **Disabled** - Disable any authentication requirement for port access. All clients are allowed to access the network. ● **Force Authorized-** Port will be considered authorized. All clients are allowed to access the network. ● **Force Unauthorized -** Port will be considered un-authorized. All clients are NOT allowed to access the network. ● **Auto -** Port will be considered authorized or unauthorized based on the authentication results of the host.
Periodic Reauthentication	**Enable** – The hosts via the selected GE port will be re-authenticated periodically.
Max Hosts	If Multiple Authentication mode is selected as Host Mode (802.1X/MAC Authenticaion>>Properties>>Port Authentication Setting), the total number of hosts cannot exceed the maximum numer of hosts configured here.

Reauthentication Period	Enter a time period. When the time is up, the host shall return to initial state and prepare to pass authentication procedure again. Default is 3600 seconds.
Inactivate Timeout	When there is no packet coming from the authenticated host, the system will start the inactive timer. After inactive timeout, the host will be unauthorized and corresponding session will be deleted. In Multiple Hosts mode (configured in 802.1X/MAC Authenticaion>>Properties>>Port Authentication Setting), the packet is counted on the authorized host only and not all packets on the port.
Quiet Period	When a GE port is disabled just because authentication fails several times, the host connected to that port will be blocked for a period of time configured in quiet period. Later, after the time period set in this field, the host wll be allowed to perform authentication again.
Resend EAP Period (802.1X Parameter)	Set the period for host to re-send EAP (Ethernet Automatic Protection) requests. Default value is 30 (seconds).
Supplicant Timeout(802.1X Parameter)	Set a period of time for the maximum number of EAP requests will be sent. If a response from the host is not received by VigorSwitch after the defined period (supplicant timeout), the authentication process will be started again.
Server Timeout (802.1X Parameter)	Set a period of time for the server. The EAP requests shall be resent to the supplicant within the time; otherwise, the time setting will lapse and the requests won't be sent out.
MAX EAP Request (802.1X Parameter)	Set the maximum time interval for EAP request sent out.
Apply	The modification made above can be applied on to the selected GE port immediately.

III-5-3 MAC-Based Local Account

This page allows the network administrator to create profiles by entering MAC address of the hosts to be authenticated.



MAC-Based Local Account Settings

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

Port Control: ● Force Authorized ○ Force Unauthorized

VLAN: □ User Defined 1 (1-4094)

Reauthentication Period: □ User Defined 3600 Sec (300 - 4294967294)

Inactive Timeout: □ User Defined 60 Sec (60 - 65535)

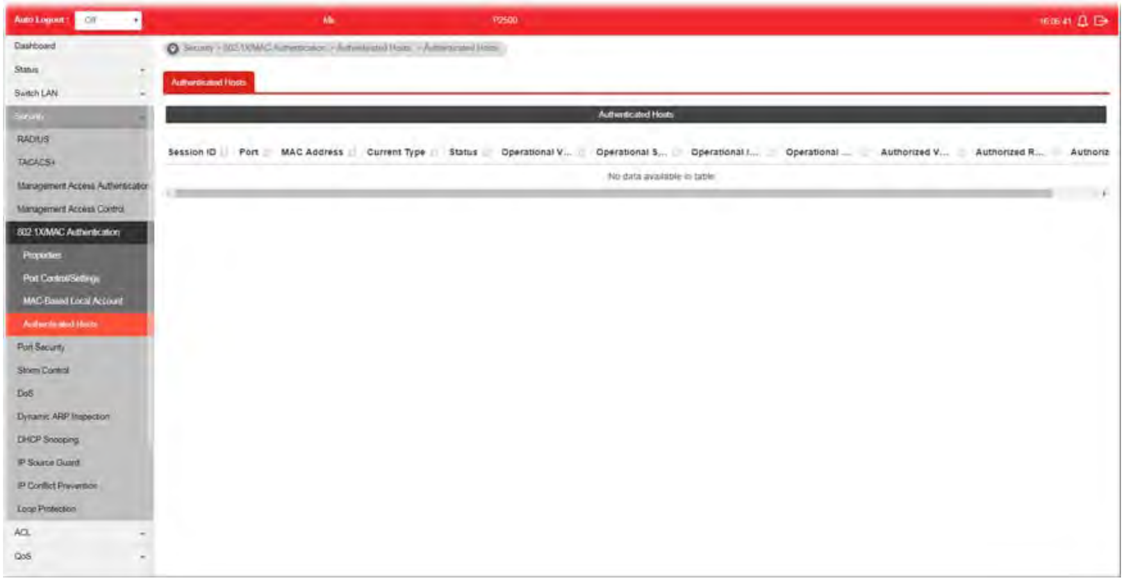
MAC Address	Port Control	VLAN	Reauthentication Period	Inactive Timeout	Edit
No data available in table					

Available settings are explained as follows:

Item	Description
MAC Address	Enter the MAC address of the host.
Port Control	Specify a control type for the host. ● Force Authorized – Click it to forcefully authenticate the host specified above. ● Force Unauthorized - The host specified above will not be authenticated by VigorSwitch.
VLAN	**User Defined** – Check it to specify which VLAN will be assigned by the host of this account.
Reauthentication Period	**User Defined** – Check it to specify the time this account required to be authenticated again after authentication taken place.
Inactive Timeout	**User Defined** – Check it to specify the time of inactive this account becoming log-off.
Add	Click it to create a new account.
Edit	It is available when there is one profile existed. 🔧 - Click it to modify the settings for the selected entry.

III-5-4 Authenticated Hosts

This page displays information related to the host authenticated by VigorSwitch.

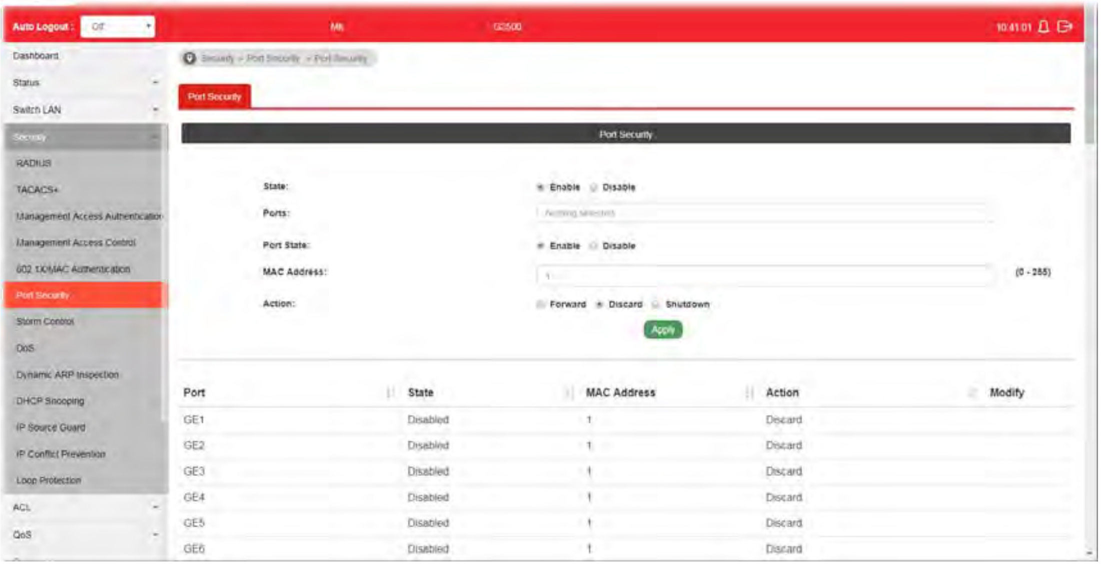


Authenticated Hosts

Session ID	Port	MAC Address	Current Type	Status	Operational V...	Operational S...	Operational I...	Operational ...	Authorized V...	Authorized R...	Authoriz
No data available in table											

III-6 Port Security

This page allows the network administrator to configure security settings for each port interface (GE port /LAG group). When port security is enabled for each interface, releated action will be performed once detecting that the number of MAC address exceeds the limit.



State: ● Enable ○ Disable

Ports: Nothing selected

Port State: ● Enable ○ Disable

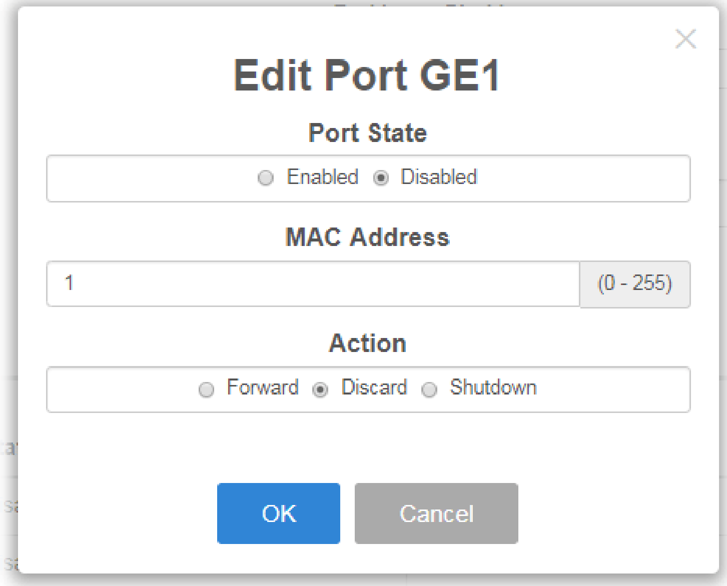
MAC Address: 1 (0 - 255)

Action: ○ Forward ● Discard ○ Shutdown

Port	State	MAC Address	Action	Modify
GE1	Disabled	1	Discard	
GE2	Disabled	1	Discard	
GE3	Disabled	1	Discard	
GE4	Disabled	1	Discard	
GE5	Disabled	1	Discard	
GE6	Disabled	1	Discard	

Available settings are explained as follows:

Item	Description
State	Enable or disable port security function on the switch. ● **Enabled -** Enable the port security function. ● **Disabled -** Disable the port security function.
Ports	Select the port(s) you would like to configure the port security settings.
Port State	Enable or disable port security function on the ports selected above. ● **Enabled -** The selected port applies the port security settings. ● **Disabled -** The selected port does not apply the port security settings.
MAC Address	Enter the maximum number of MAC addresses that the port is allowed to learn.
Action	Select an action to perform when there is an unknown MAC address on the port. ● **Forward**- Forward a packet whose source MAC is unknown to the switch. ● **Discard**- Discard a packet whose source MAC is unknown to the switch. ● **Shutdown**- Shutdown this port when a packet with unknown source MAC is received.
Apply	The modification made above can be applied on to the selected GE/LAG port immediately.

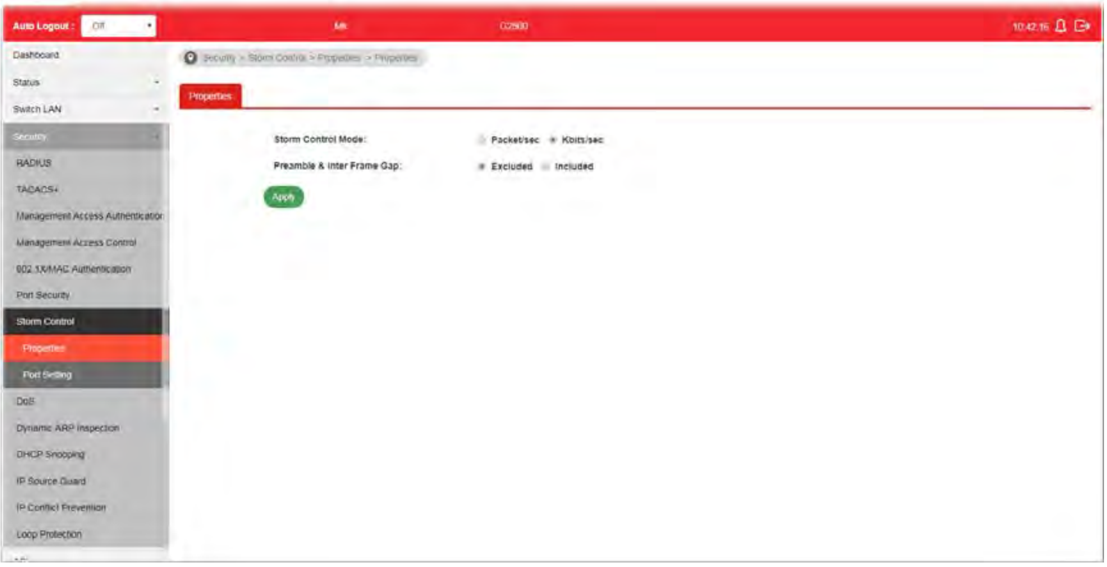
Edit	- click it to modify the settings for the selected entry.  Edit Port GE1 Port State ○ Enabled ● Disabled MAC Address 1 (0 - 255) Action ○ Forward ● Discard ○ Shutdown

III-7 Storm Control

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

III-7-1 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

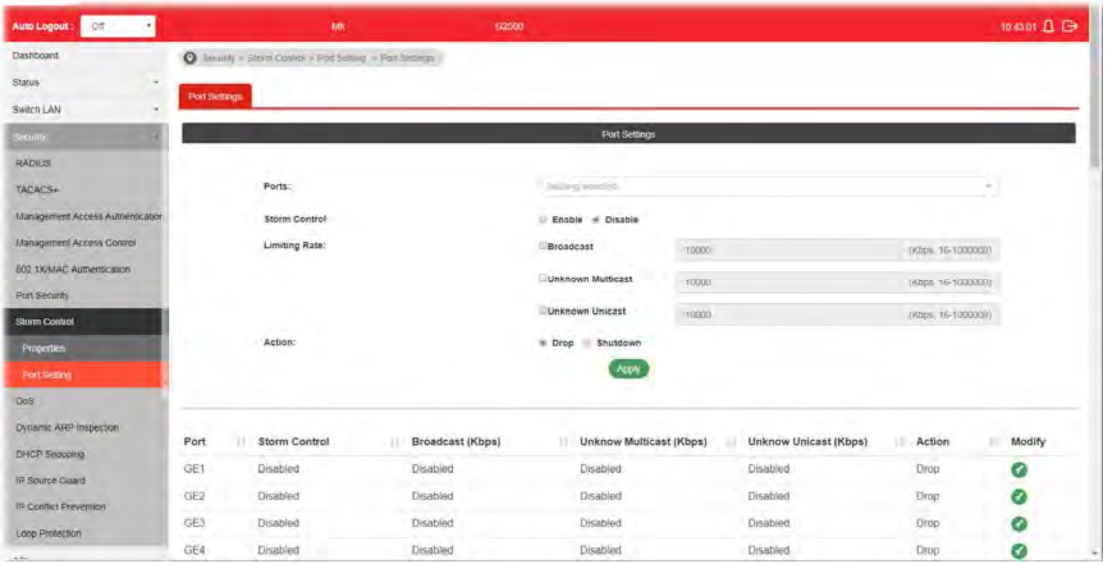
Apply

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	Apply the settings to the switch.

III-7-2 Port Setting

This page allows the network administrator 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.



Ports: Nothing selected

Storm Control ○ Enable ● Disable

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 (Kbps)	Unknow Multicast (Kbps)	Unknow Unicast (Kbps)	Action	Modify
GE1	Disabled	Disabled	Disabled	Disabled	Drop	✓
GE2	Disabled	Disabled	Disabled	Disabled	Drop	✓
GE3	Disabled	Disabled	Disabled	Disabled	Drop	✓
GE4	Disabled	Disabled	Disabled	Disabled	Drop	✓

Available settings are explained as follows:

Item	Description
Ports	Use the drop down list to select the port profile (GE1 to GE28).
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	Apply the settings to the switch.

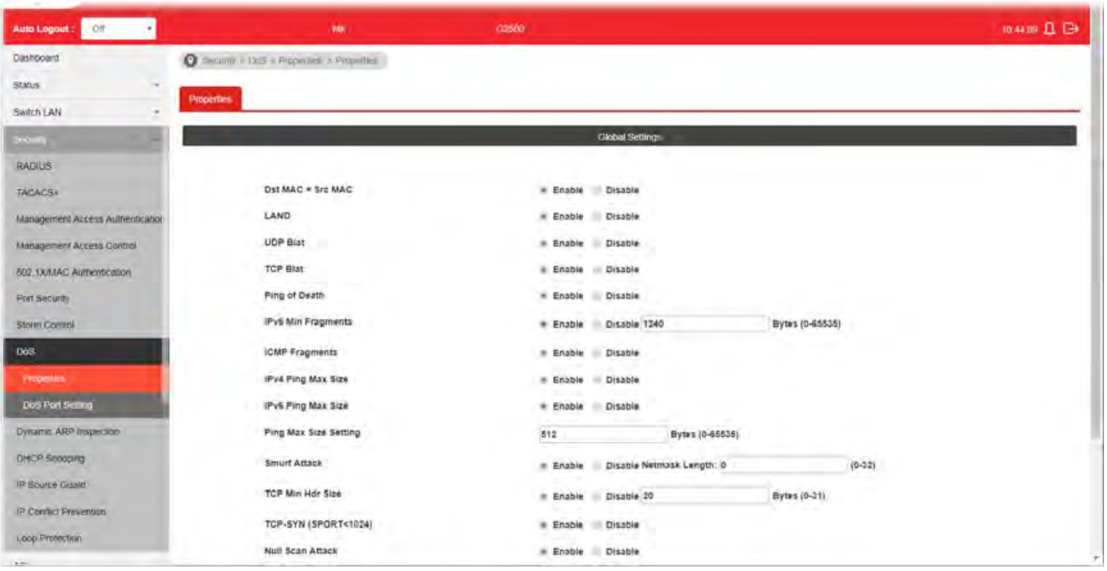
III-8 DoS

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-8-1 Properties

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



Dst MAC = Src MAC ● Enable ○ Disable

LAND ● Enable ○ Disable

UDP Blat ● Enable ○ Disable

TCP Blat ● Enable ○ Disable

Ping of Death ● Enable ○ Disable

IPv6 Min Fragments ● Enable ○ Disable 1240 Bytes (0-65535)

ICMP Fragments ● Enable ○ Disable

IPv4 Ping Max Size ● Enable ○ Disable

IPv6 Ping Max Size ● Enable ○ Disable

Ping Max Size Setting 512 Bytes (0-65535)

Smurf Attack ● Enable ○ Disable Netmask Length: 0 (0-32)

TCP Min Hdr Size ● Enable ○ Disable 20 Bytes (0-31)

TCP-SYN (SPORT<1024) ● Enable ○ Disable

Null Scan Attack ● Enable ○ Disable

Available settings are explained as follows:

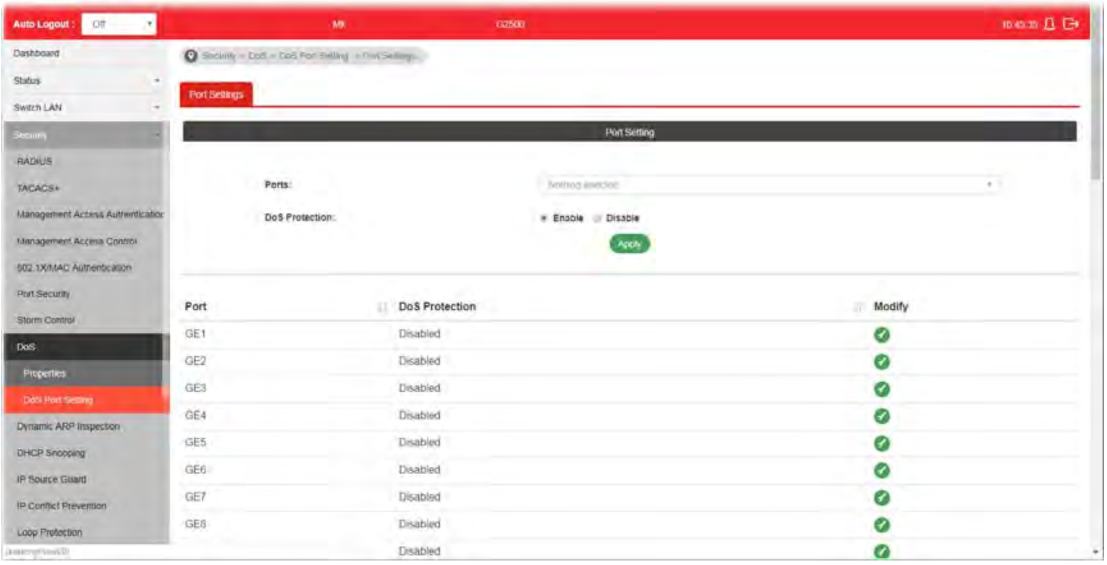
Item	Description
Dst MAC=Src MAC	Drop the packets if the destination MAC address is equal to the source MAC address. ● **Disabled** – Disable the item function. ● **Enabled** - Enable the item function.
LAND	Drop the packets if the source IP address is equal to the destination IP address. ● **Disabled** – 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	Apply the settings to the switch.

III-8-2 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: ● Enable ○ Disable

Port	DoS Protection	Modify
GE1	Disabled	✓
GE2	Disabled	✓
GE3	Disabled	✓
GE4	Disabled	✓
GE5	Disabled	✓
GE6	Disabled	✓
GE7	Disabled	✓
GE8	Disabled	✓
	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	Apply the settings to the switch.
Modify	🔧 - Click it to modify settings.

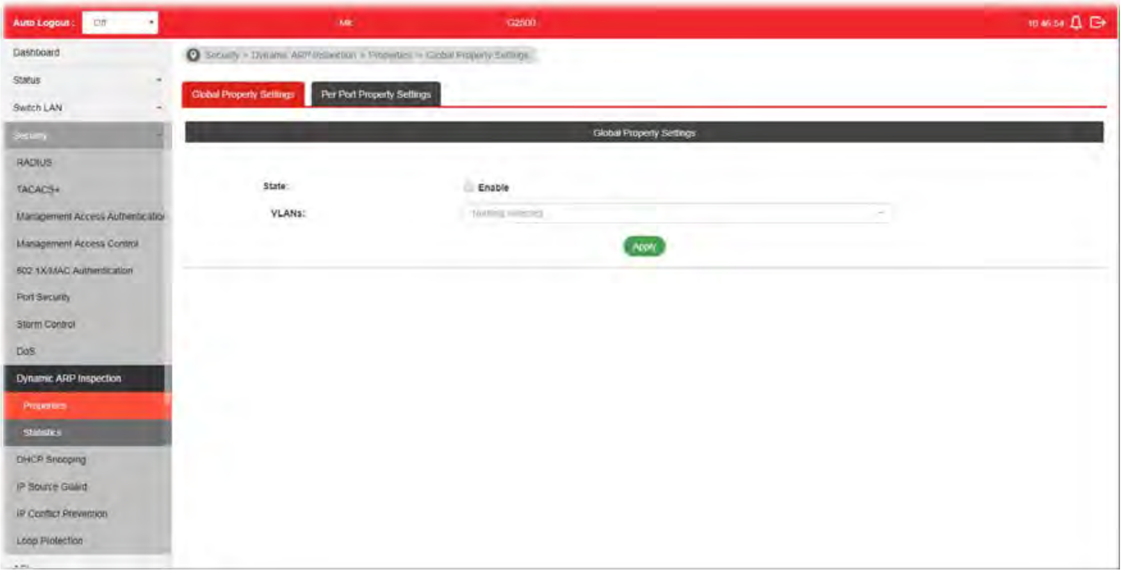
III-9 Dynamic ARP Inspection

Dynamic ARP inspection (DAI) can prevent ARP spoofing attacks by validating ARP packet in a network. It can intercept, record, and discard ARP packets with invalid IP-to-MAC address bindings; and then protect the network against malicious attacks.

III-9-1 Properties

III-9-1-1 Global Property Settings

This page allows a user to configure global property settings for the fuction of Dynamic ARP Inspection.



State: □ Enable

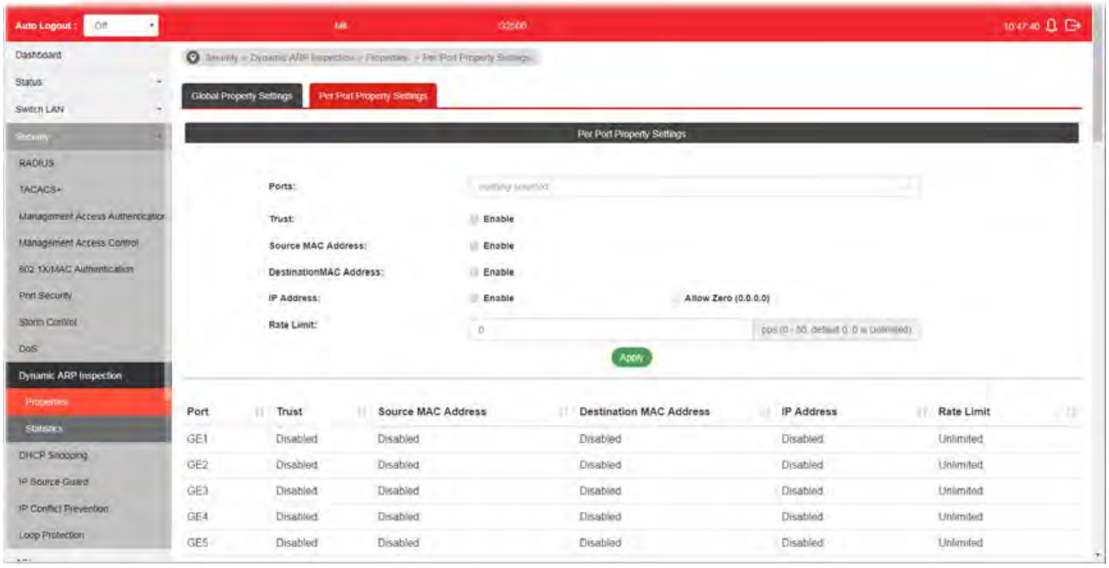
VLANs: Nothing selected

Available settings are explained as follows:

Item	Description
State	**Enable** – Check the box to enable global property settings.
VLANs	Select VLAN profile(s) to apply the function of Dynamic ARP Inspection. Only the GE/LAG port within the selected VLAN will apply DAI function.
Apply	Apply the settings to the switch.

III-9-1-2 Per Port Property Settings

This page allows a user to configure detailed settings of DAI for each port (GE/LAG).



Per Port Property Settings

Ports: nothing selected

Trust: □ Enable

Source MAC Address: □ Enable

DestinationMAC Address: □ Enable

IP Address: □ Enable □ Allow Zero (0.0.0.0)

Rate Limit: 0 pps (0 - 50, default 0, 0 is Unlimited)

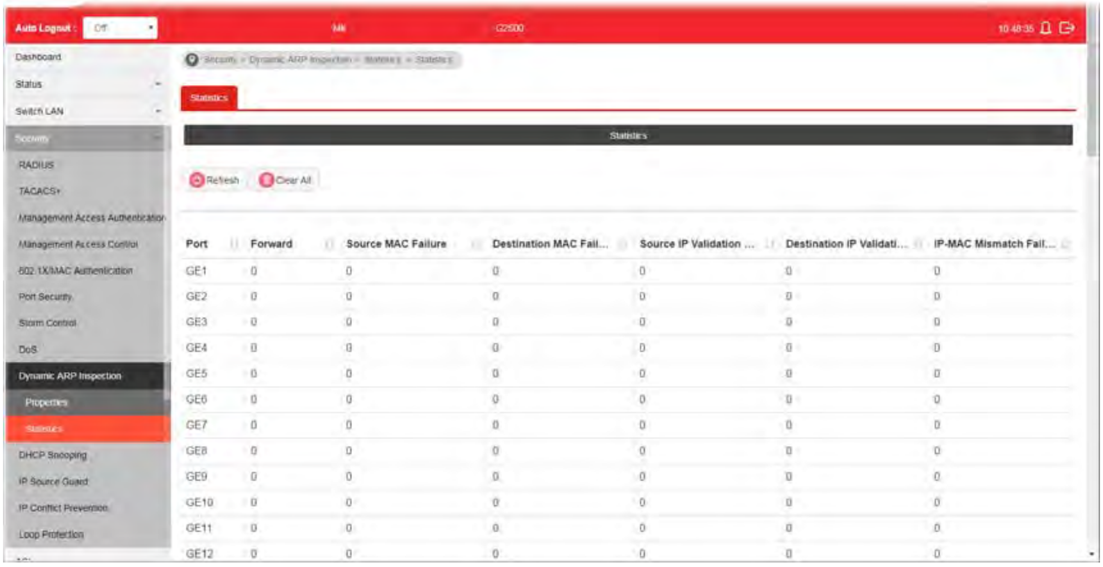
Port	Trust	Source MAC Address	Destination MAC Address	IP Address	Rate Limit
GE1	Disabled	Disabled	Disabled	Disabled	Unlimited
GE2	Disabled	Disabled	Disabled	Disabled	Unlimited
GE3	Disabled	Disabled	Disabled	Disabled	Unlimited
GE4	Disabled	Disabled	Disabled	Disabled	Unlimited
GE5	Disabled	Disabled	Disabled	Disabled	Unlimited

Available settings are explained as follows:

Item	Description
Ports	Use the drop down list to select the port (GE1 to GE28, LAG1 to LAG8) or ports for applying DAI function.
Trust	**Enable** – Enable the function of DAI for the port(s) selected above.
Source MAC Address	**Enable** – Check it to enable the function of source MAC address validation mechanism for the selected port(s).
Destination MAC Address	**Enable** - Check it to enable the function of destination MAC address validation mechanism for the selected port(s).
IP Address	● **Enable** - Check it to enable the function of IP address validation mechanism for the selected port(s). ● **Allow Zero** – The IP address of “0.0.0.0” can be applied to the selected port(s) if it is enabled.
Rate Limit	Use the drop down list to choose a rate limitation value (0~50) for the selected port(s).
Apply	Apply the settings to the switch.

III-9-2 Statistics

This page displays all statistics recorded by Dynamic ARP Inspection function.



Port	Forward	Source MAC Failure	Destination MAC Fail...	Source IP Validation ...	Destination IP Validati...	IP-MAC Mismatch Fail...
GE1	0	0	0	0	0	0
GE2	0	0	0	0	0	0
GE3	0	0	0	0	0	0
GE4	0	0	0	0	0	0
GE5	0	0	0	0	0	0
GE6	0	0	0	0	0	0
GE7	0	0	0	0	0	0
GE8	0	0	0	0	0	0
GE9	0	0	0	0	0	0
GE10	0	0	0	0	0	0
GE11	0	0	0	0	0	0
GE12	0	0	0	0	0	0

III-10 DHCP Snooping

DHCP snooping is able to validate DHCP messages obtained from untrusted sources and filter out invalid message.

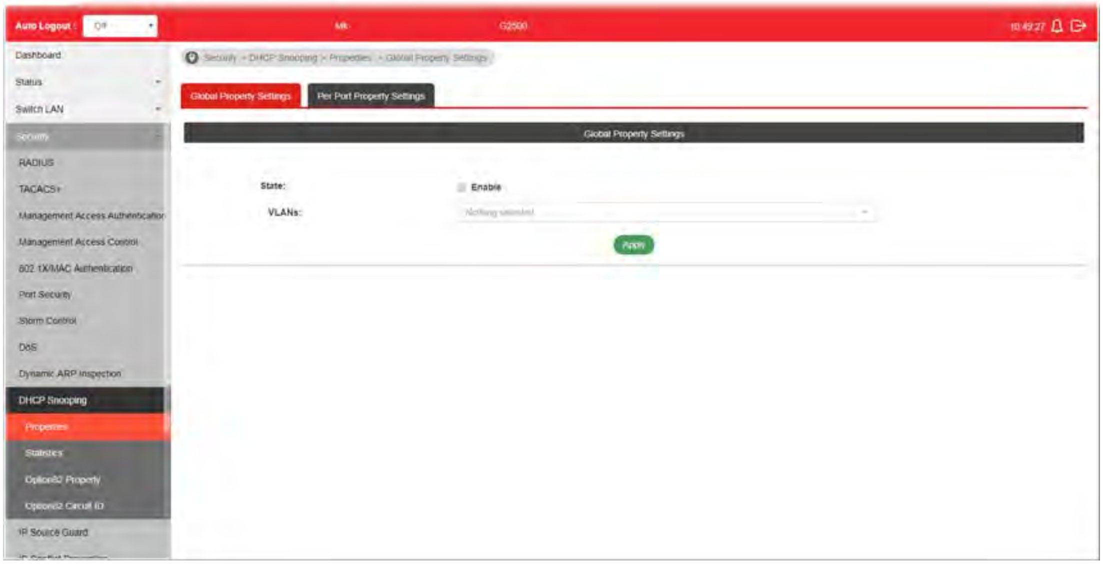
For DHCP snooping to function properly, it is suggested to connect DHCP servers to VigorSwitch through trusted interfaces; because untrusted DHCP messages will be forwarded to trusted interfaces only.

III-10-1 Properties

III-10-1-1 Global Property Settings

This page allows a user to configure global property settings for the fuction of DHCP snooping Inspection.

In default, DHCP snooping is inactive on all VLANs. You can enable such feature on a single VLAN or a range of VLANs.



Global Property Settings

State: □ Enable

VLANs: Nothing selected

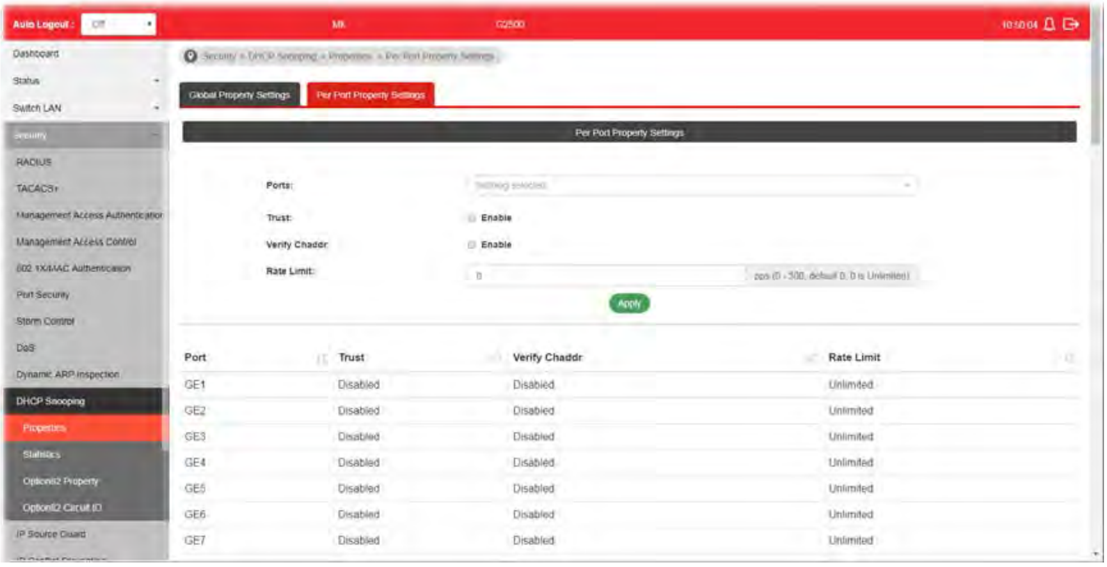
Available settings are explained as follows:

Item	Description
State	**Enable** – Check the box to enable global property settings.
VLANs	Select VLAN profile(s) to apply the function of DHCP Snooping Inspection. Only the GE/LAG port within the selected VLAN will apply DHCP Snooping function.
Apply	Apply the settings to the switch.

III-10-1-2 Per Port Property Settings

This page allows a user to configure detailed settings of DHCP Snooping for each port (GE/LAG).

Any device that is not in the service provider network will be regarded as an untrusted source (such as a customer switch). Host ports are untrusted sources. In VigorSwitch, you can assign a source as trusted device by configuring the trust state of its connecting port.



Per Port Property Settings

Ports: Nothing selected

Trust: □ Enable

Verify Chaddr: □ Enable

Rate Limit: 0 pps (0 - 300, default 0, 0 is Unlimited)

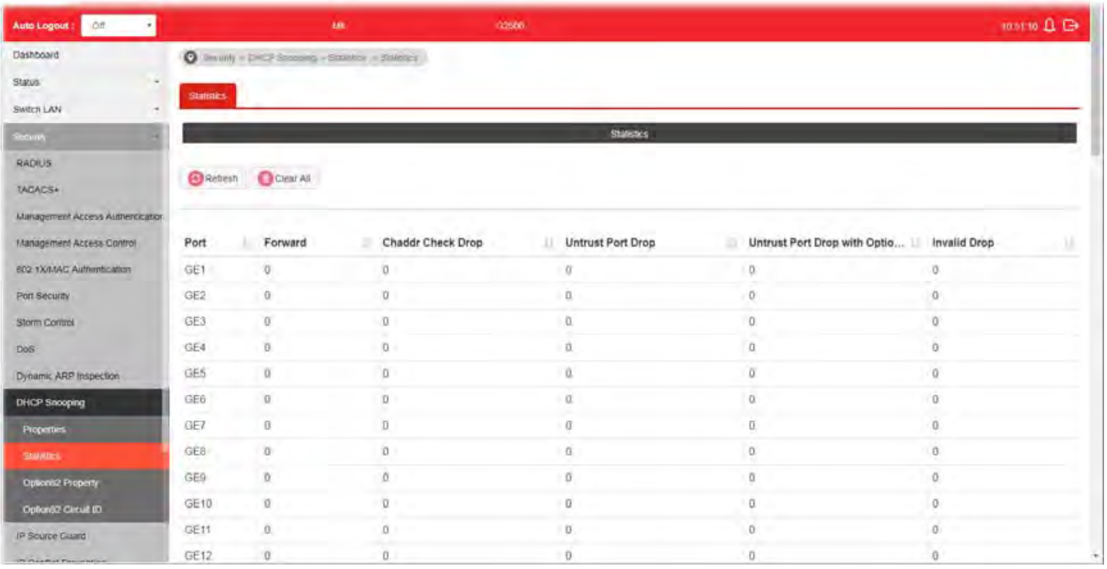
Port	Trust	Verify Chaddr	Rate Limit
GE1	Disabled	Disabled	Unlimited
GE2	Disabled	Disabled	Unlimited
GE3	Disabled	Disabled	Unlimited
GE4	Disabled	Disabled	Unlimited
GE5	Disabled	Disabled	Unlimited
GE6	Disabled	Disabled	Unlimited
GE7	Disabled	Disabled	Unlimited

Available settings are explained as follows:

Item	Description
Ports	Use the drop down list to select the port (GE1 to GE28, LAG1 to LAG8) or ports for applying DHCP snooping function.
Trust	**Enable** – Check it to make the port(s) selected above as trusted interface.
Verify Chaddr	**Enable** - Check it to enable chaddr (client hardware address) validation of GE/LAG port. All DHCP packets will be checked if the client hardware MAC address is the same as source MAC in Ethernet header or not. Default is disabled.
Rate Limit	Input rate limitation (0~300) of DHCP packets. The unit is "pps". "0" means unlimited. Default is unlimited.
Apply	Apply the settings to the switch.

III-10-2 Statistics

This page displays all statistics recorded by DHCP snooping function.



Statistics

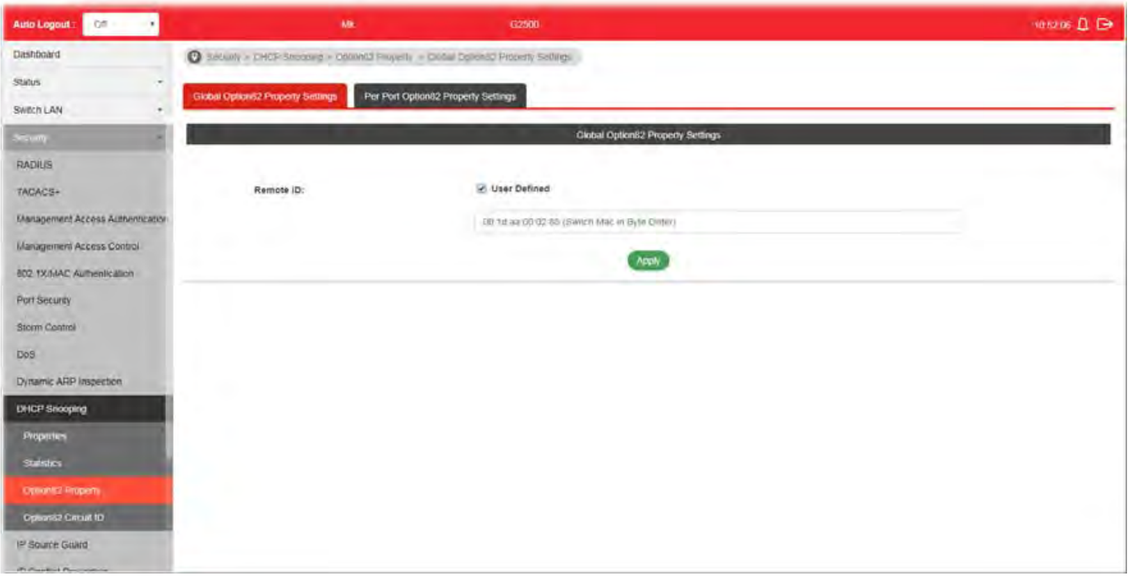
Port	Forward	Chaddr Check Drop	Untrust Port Drop	Untrust Port Drop with Optio...	Invalid Drop
GE1	0	0	0	0	0
GE2	0	0	0	0	0
GE3	0	0	0	0	0
GE4	0	0	0	0	0
GE5	0	0	0	0	0
GE6	0	0	0	0	0
GE7	0	0	0	0	0
GE8	0	0	0	0	0
GE9	0	0	0	0	0
GE10	0	0	0	0	0
GE11	0	0	0	0	0
GE12	0	0	0	0	0

III-10-3 Option82 Property

You can use information settings including Remote ID and Circuit ID for Option82 Property, also known as the DHCP relay agent, to protect VigorSwitch against spoofing attacks.

III-10-3-1 Global Option82 Property Settings

This page allows a user to set string as remote ID for DHCP option82. For example, use a switch-configured hostname or specify an ASCII text string as remote ID.


Auto Logout : Off
Mk
G2500
10:52:06
Dashboard
Status
Switch LAN
Security
RADIUS
TACACS+
Management Access Authentication
Management Access Control
802.1X/MAC Authentication
Port Security
Storm Control
DoS
Dynamic ARP Inspection
DHCP Snooping
Properties
Statistics
Option82 Property
Option82 Circuit ID
IP Source Guard
Security > DHCP Snooping > Option82 Property > Global Option82 Property Settings
Global Option82 Property Settings
Per Port Option82 Property Settings
Apply

Global Option82 Property Settings

Remote ID: ☑ User Defined

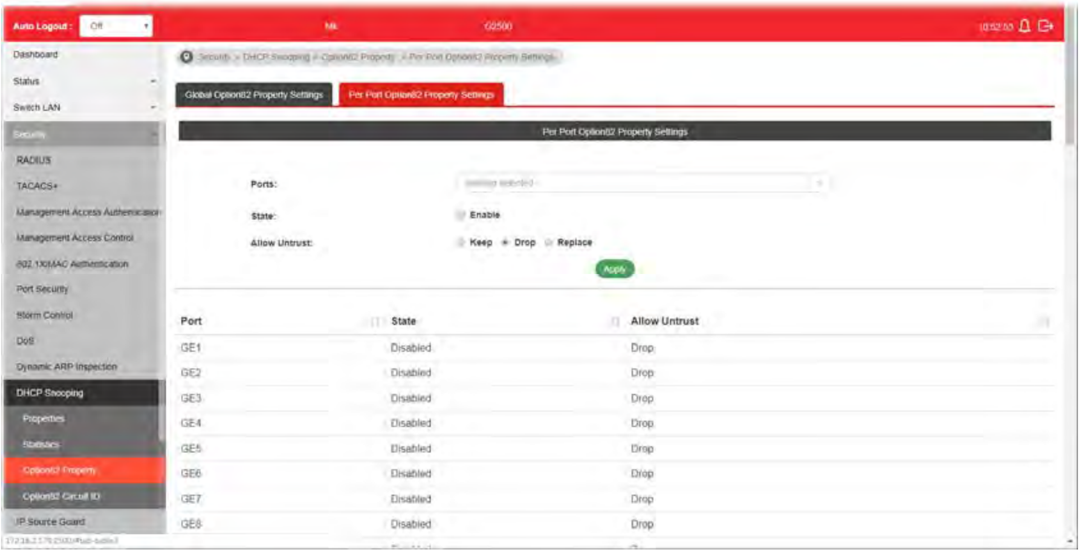
00:1d:aa:00:02:60 (Switch Mac in Byte Order)

Available settings are explained as follows:

Item	Description
Remote ID	The string specified here is used to identify the remote host. **User Defined** – Check it and manually enter ASCII text string in the entry box.
Apply	Apply the settings to the switch.

III-10-3-2 Per Port Option82 Property Settings

This page allows a user to configure detailed settings of DHCP Snooping, Option82 for each port (GE/LAG).



Auto Logout : Off
G2500
Dashboard
Status
Switch LAN
Security
RADIUS
TACACS+
Management Access Authentication
Management Access Control
802.1X/MAC Authentication
Port Security
Storm Control
DoS
Dynamic ARP Inspection
DHCP Snooping
Properties
Statistics
Option82 Property
Option82 Circuit ID
IP Source Guard
Security > DHCP Snooping > Option82 Property > Per Port Option82 Property Settings
Global Option82 Property Settings
Per Port Option82 Property Settings
Apply

Per Port Option82 Property Settings

Ports:

State: □ Enable

Allow Untrust: ○ Keep ● Drop ○ Replace

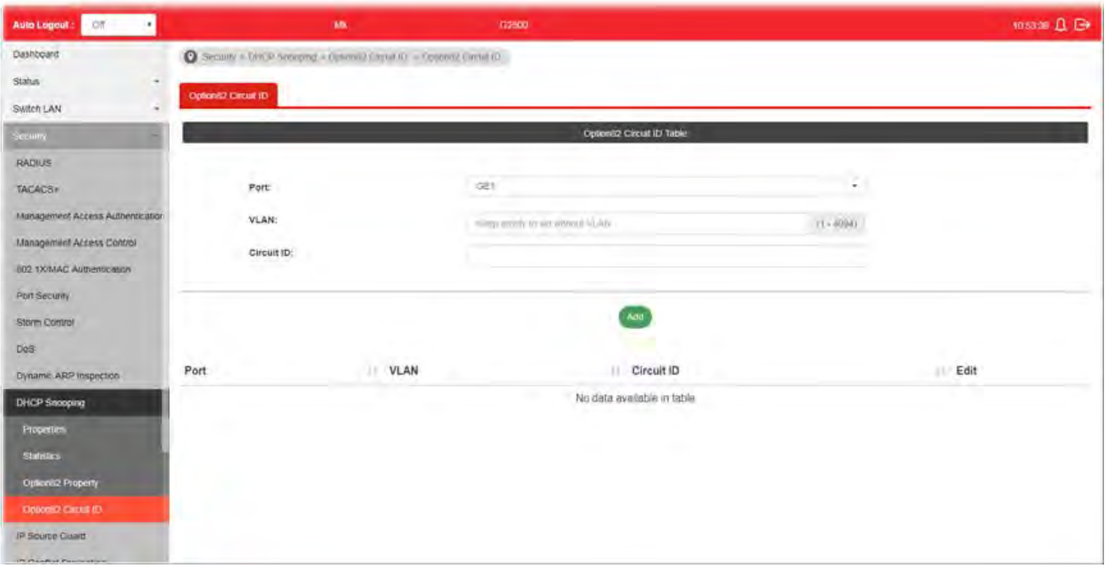
Port	State	Allow Untrust
GE1	Disabled	Drop
GE2	Disabled	Drop
GE3	Disabled	Drop
GE4	Disabled	Drop
GE5	Disabled	Drop
GE6	Disabled	Drop
GE7	Disabled	Drop
GE8	Disabled	Drop

Available settings are explained as follows:

Item	Description
Ports	Use the drop down list to select the port (GE1 to GE28, LAG1 to LAG8) or ports for applying DHCP snooping, Option82 Property function.
State	**Enable** – Check it to make the port(s) selected above apply the settings configured in this page.
Allow Untrust	Untrusted packets detected by VigorSwitch will be performed by the action determined here. ● **Keep** – Packets are allowed to pass through. ● **Drop** – Packets are blocked and discarded. ● **Replace** – Packets will be replaced.
Apply	Apply the settings to the switch.

III-10-4 Option82 Circuit ID

This page allows a user to set string as circuit ID for DHCP option82 setting. Circuit ID shall be combined with VLAN name (or VLAN ID number) and interface name (GE/LAG port).



Port: GE1

VLAN: Keep empty to set without VLAN (1 - 4094)

Circuit ID:

Port	VLAN	Circuit ID	Edit
No data available in table			

Available settings are explained as follows:

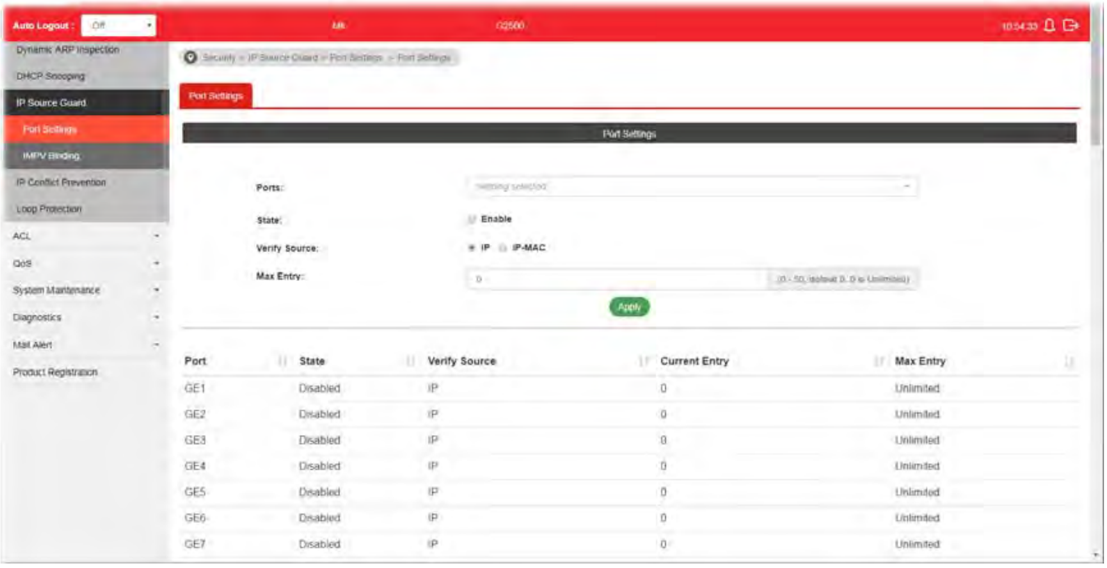
Item	Description
Port	Use the drop down list to select the port (GE1 to GE28, LAG1 to LAG8) or ports for applying DHCP snooping, Option82 Property function.
VLAN	Choose a number as VLAN ID which is easy to be identified for a packet containing with it. It is optional setting.
Circuit ID	Enter ASCII text string in the entry box. Later, any packet passes through the specified interface (GE/LAG port) will be inserted with such information.
Add	Click it to create a profile.
Edit	🔧 - click it to modify the circuit ID value for the selected entry. 🗑 - click it to remove the selected entry.

III-11 IP Source Guard

By using the source IP address filtering function, IP source guard can prevent a malicious host from feigning a legal host with its IP address and performing malicious attack.

III-11-1 Port Settings

IP source guard is a port-based feature. Therefore, it is necessary to configure detailed settings for each GE/LAG port interface separately.



Port Settings

Ports: Nothing selected

State: □ Enable

Verify Source: ● IP ○ IP-MAC

Max Entry: 0 (0 - 50, default 0, 0 is Unlimited)

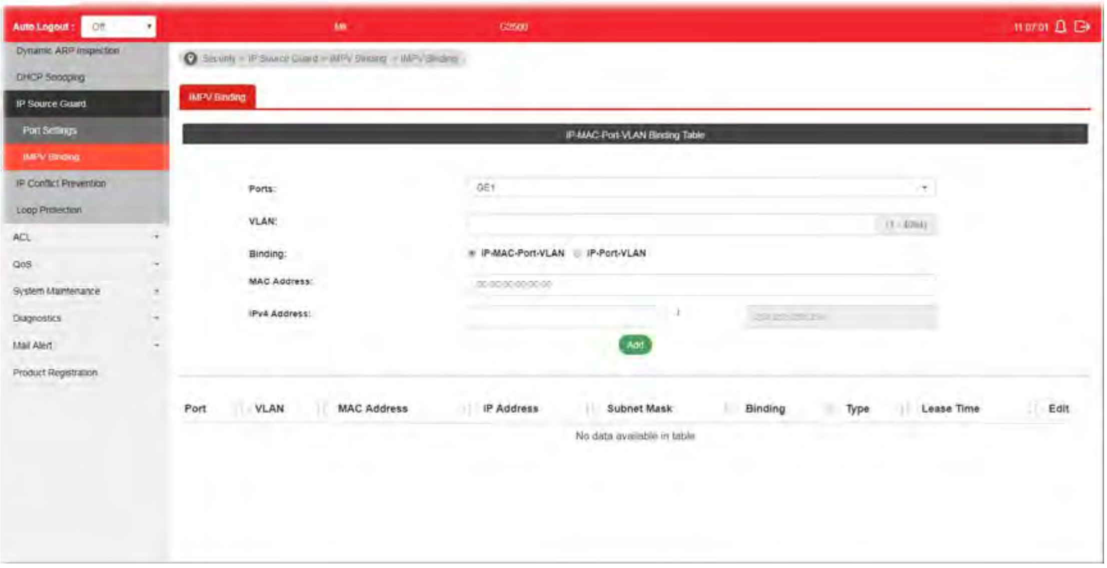
Port	State	Verify Source	Current Entry	Max Entry
GE1	Disabled	IP	0	Unlimited
GE2	Disabled	IP	0	Unlimited
GE3	Disabled	IP	0	Unlimited
GE4	Disabled	IP	0	Unlimited
GE5	Disabled	IP	0	Unlimited
GE6	Disabled	IP	0	Unlimited
GE7	Disabled	IP	0	Unlimited

Available settings are explained as follows:

Item	Description
Ports	Use the drop down list to select the port (GE1 to GE28, LAG1 to LAG8) or ports for applying IP source guard function.
State	**Enable** – Check it to make the port(s) selected above apply the settings configured in this page.
Verify Source	Specify the type of source IP for the packet coming from. ● **IP** – Only the packet with specified IP address will be verified. ● **IP-MAC** – Only the packet with specified IP address and MAC address will be verified.
Max Entry	Define the number (0~50) for the port. The default is 0 (no limit).
Apply	Apply the settings to the switch.

III-11-2 IMPV Binding

This page allows the network administrator to set the filtering conditions (binding type, MAC address, IPv4 address) for packets through the specified LAN port.



IP-MAC-Port-VLAN Binding Table

Ports: GE1

VLAN: (1 - 4094)

Binding: ● IP-MAC-Port-VLAN ○ IP-Port-VLAN

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

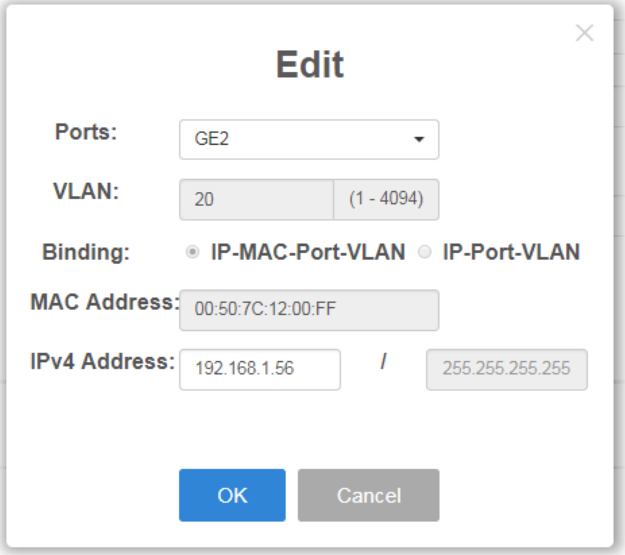
IPv4 Address: / 255.255.255.255

Port	VLAN	MAC Address	IP Address	Subnet Mask	Binding	Type	Lease Time	Edit

No data available in table

Available settings are explained as follows:

Item	Description
Ports	Use the drop down list to select the port (GE1 to GE28, LAG1 to LAG8) or ports for applying IMPV Binding function.
VLAN	Choose a number as VLAN ID which is easy to be identified for a packet containing with it. It is optional setting.
Binding	Select the binding type for such feature. ● **IP-MAC-Port-VLAN** – Packets will be allowed to pass through the port interface if they meet the conditions specified by IP address, MAC address, Port setting and VLAN ID setting. ● **IP-Port-VLAN** – Packets will be allowed to pass through the port interface if they meet the conditions specified by IP address, Port setting and VLAN ID setting.
MAC Address	Enter the MAC address of the device connecting to the port interface selected above.
IPv4 Address	Enter the IP address with mask address of the device connecting to the port interface selected above.
Add	Click it to create a new binding profile.
Edit	🔧 - Click it to modify the settings for the selected entry.



Edit

Ports: GE2

VLAN: 20 (1 - 4094)

Binding: ● IP-MAC-Port-VLAN ○ IP-Port-VLAN

MAC Address: 00:50:7C:12:00:FF

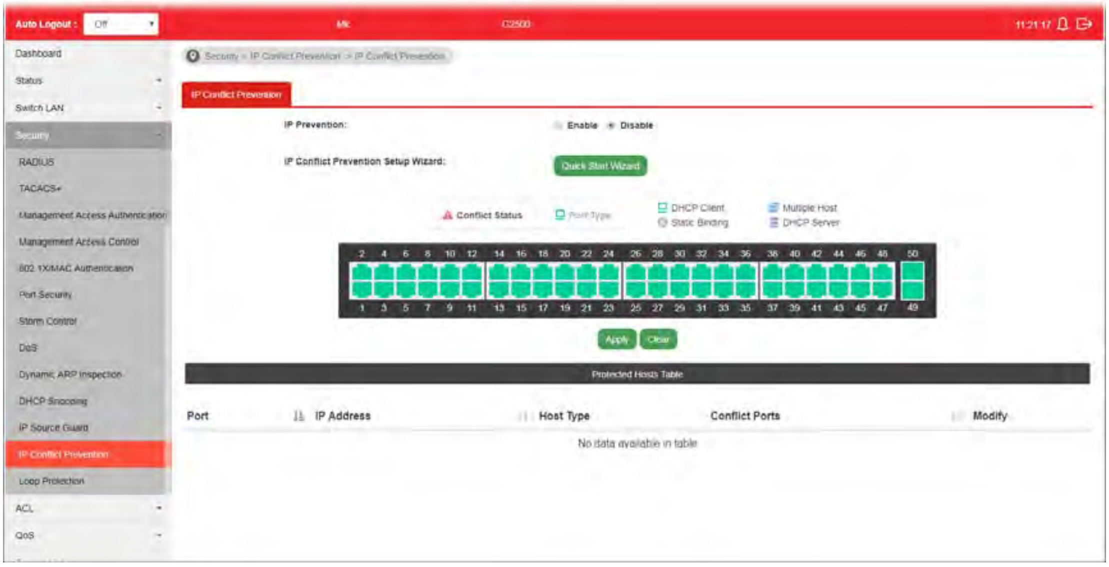
IPv4 Address: 192.168.1.56 / 255.255.255.255

🗑 - click it to remove the selected entry.

III-12 IP Conflict Prevention

A user can configure IP addresses for network devices manually. However, it might result in conflict between different devices due to using the same IP address, and cause the devices not working correctly.

This page allows you to prevent IP conflict by binding the port with the specified IP address.

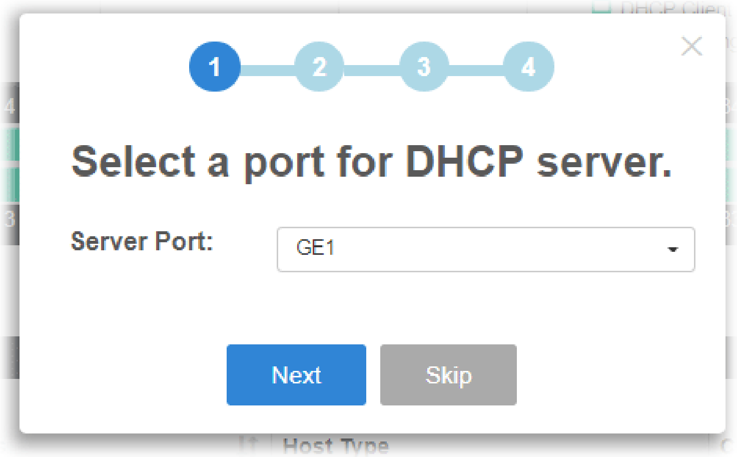


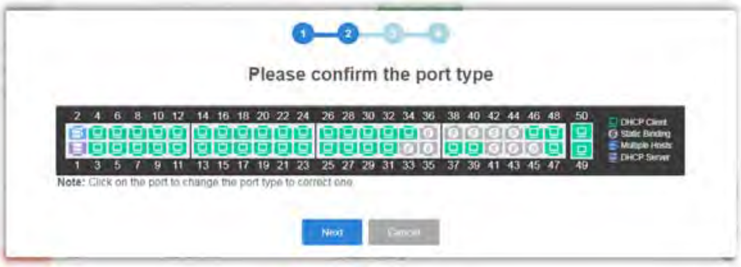
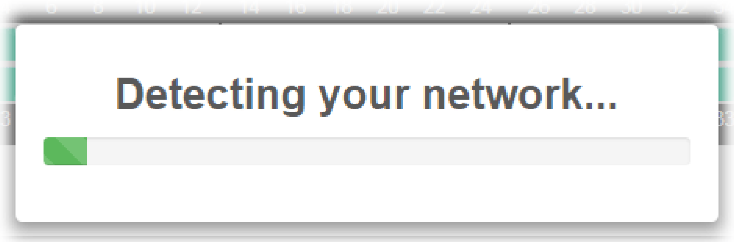
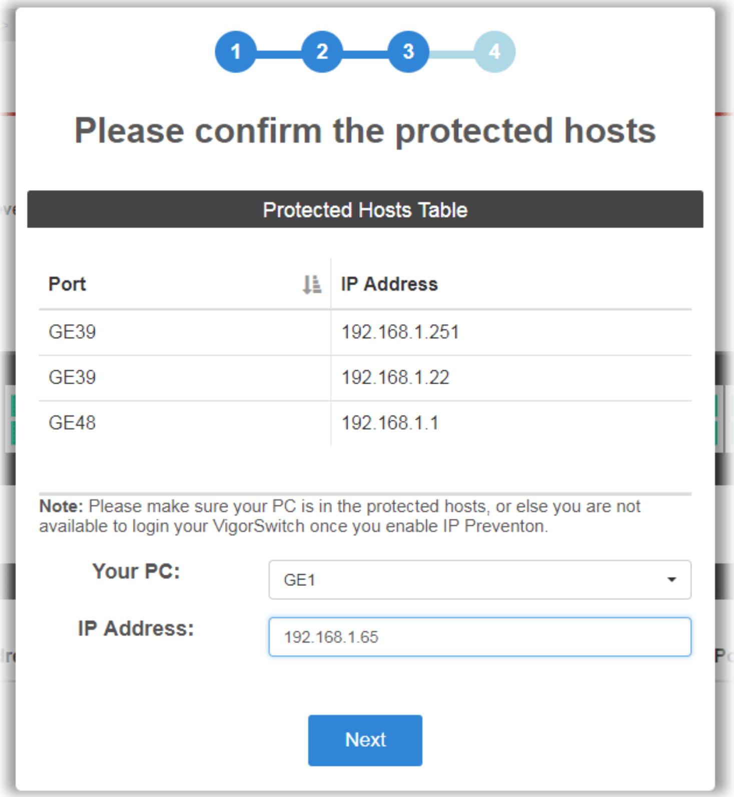
IP Prevention: ○ Enable ● Disable

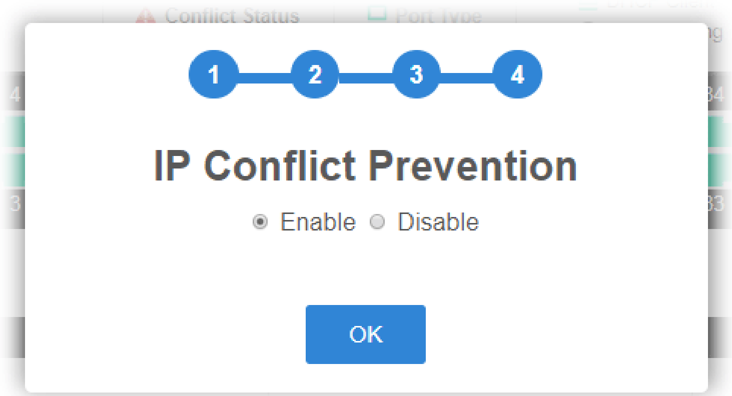
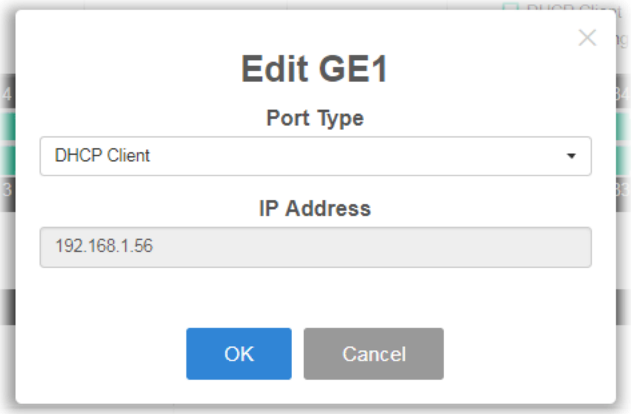
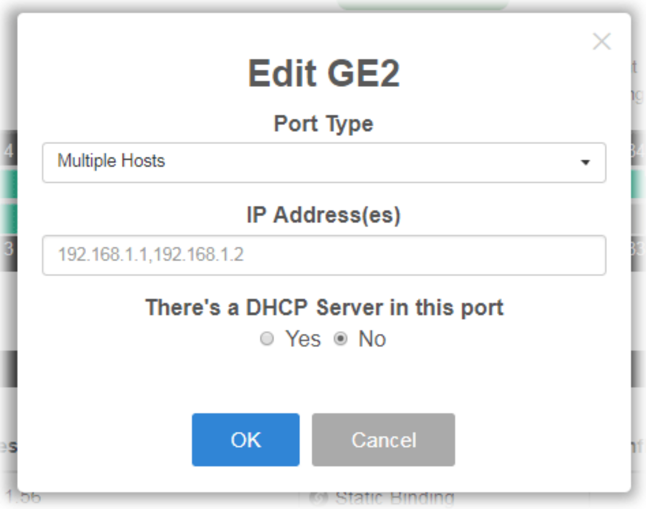
IP Conflict Prevention Setup Wizard: Quick Start Wizard

Port	IP Address	Host Type	Conflict Ports	Modify
No data available in table				

Available settings are explained as follows:

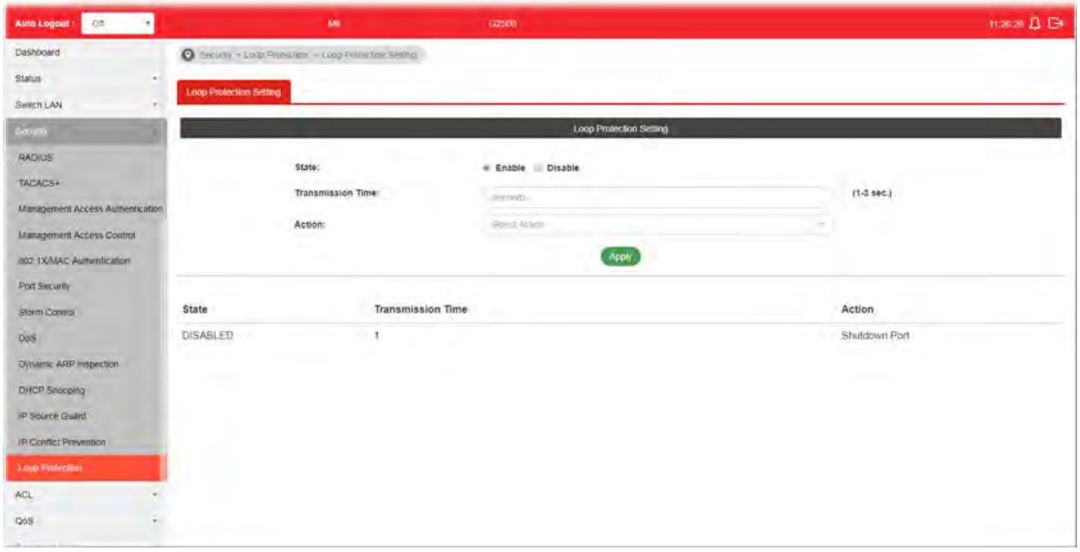
Item	Description
IP Prevention	**Enable** - Click it to activate the function of IP prevention. **Disable** - Click it to deactivate the function of IP prevention.
IP Conflict Prevention Setup Wizard	**Quick Start Wizard** - The system will guide to bind server port with an IP address step by step. Step 1  Select a port for DHCP server. Server Port: GE1 Next Skip Step 2

	 Please confirm the port type 1 2 3 4 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 50 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 49 DHCP Client Static Binding Multiple Hosts DHCP Server Next Cancel **Note:** Click on the port to change the port type to correct one  Detecting your network... Step 3  Please confirm the protected hosts Protected Hosts Table Port | IP Address GE39 | 192.168.1.251 GE39 | 192.168.1.22 GE48 | 192.168.1.1 **Note:** Please make sure your PC is in the protected hosts, or else you are not available to login your VigorSwitch once you enable IP Preventon. Your PC: GE1 IP Address: 192.168.1.65 Step 4

	 1 2 3 4 IP Conflict Prevention ● Enable ○ Disable OK After clicking **OK**, the IP address specified for the GE port will be unavailable for other network devices.
Apply	Apply the settings to the switch.
Clear	Remove all settings of IP source guard DHCP snooping and dynamic ARP inspection.
Modify	🔧 - Click it to modify the settings for the selected entry.  Edit GE1 Port Type: DHCP Client IP Address: 192.168.1.56 OK Cancel  Edit GE2 Port Type: Multiple Hosts IP Address(es): 192.168.1.1,192.168.1.2 There's a DHCP Server in this port ○ Yes ● No OK Cancel **Port Type** - There are four selections - DHCP Client, Static Binding, Multiple Hosts and DHCP Server. Each type will bring out different IP address(es) settings. **OK** - Click it to save the settings. 🗑 - Click it to remove the selected entry.

III-13 Loop Protection

Loop event might be caused due to wrong hardware connection. VigorSwitch will periodically send packets out to check if they loopback or not. This page allows you to set conditions and perform an action when VigorSwitch detects the loopped packet.



Loop Protection Setting

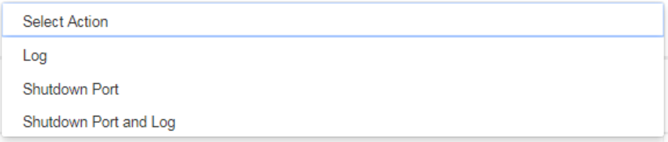
State: ● Enable ○ Disable

Transmission Time: (1-3 sec.)

Action: Select Action

State	Transmission Time	Action
DISABLED	1	Shutdown Port

Available settings are explained as follows:

Item	Description
State	● **Enable** - VigorSwitch detects the loop event of GE ports/LAG ports automaticlly. ● **Disable** - VigorSwitch will not detect the loop event.
Transmission Time	When the loop event occurred, VigorSwitch will perform the action after a period of time.
Action	When the switch detects loop situation occurred to a port; it will perform the action selected in this field.  Select Action Log Shutdown Port Shutdown Port and Log ● **Log** - The switch will reord such event as a log. ● **Shutdown Port** - The switch will shut down the port. ● **Shutdown Port and Log** - The switch will shut down the port and record the event as a log. The system administrator will view the content from system log.
Apply	Apply the settings to the switch.

This page is left blank.

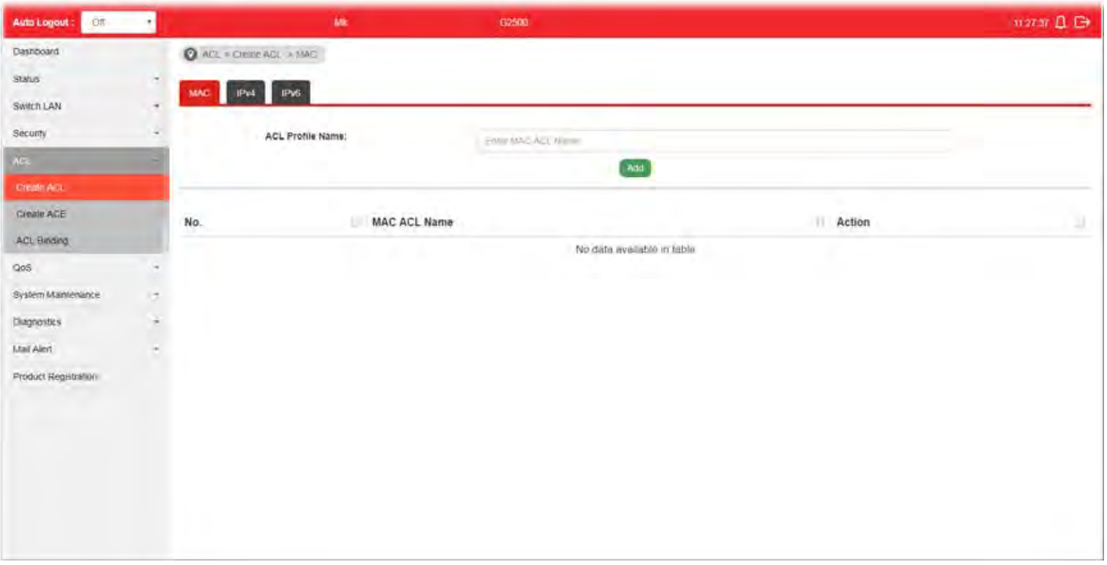
Part IV ACL Configuration

IV-1 Create ACL

An Access Control List (ACL) is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the frame is accepted.

IV-1-1 MAC

The function is used to show the Access Control List (ACL) based on Layer 2 filtering, the MAC layer. The ACL is composed by many Access Control Element (ACE) rules. You can create a new ACL here; then add multiple ACEs.



ACL Profile Name: Enter MAC ACL Name

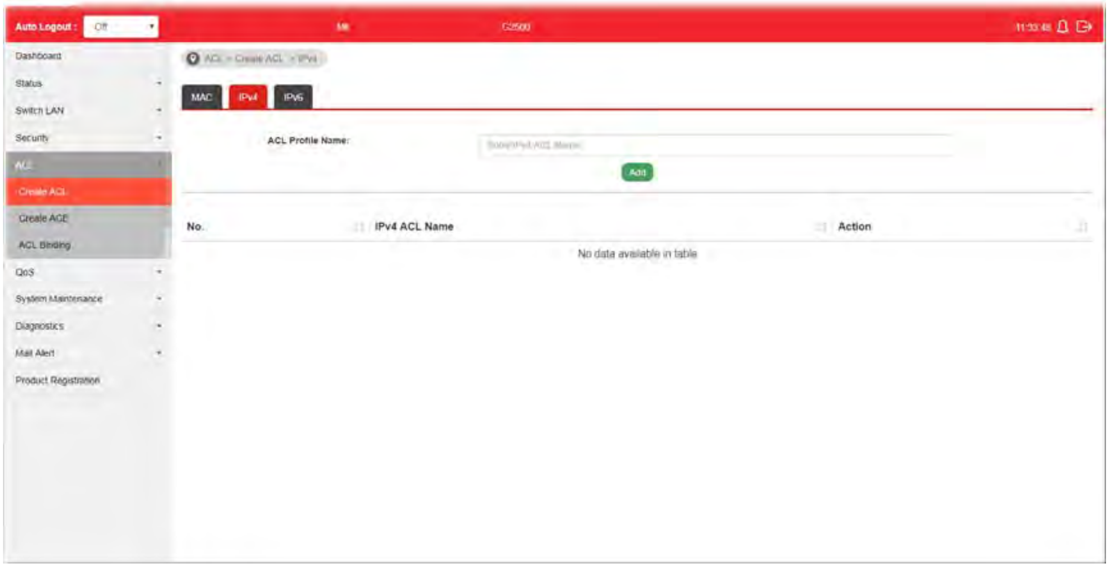
No.	MAC ACL Name	Action
No data available in table		

Available settings are explained as follows:

Item	Description
ACL Profile Name	Enter a name for creating a new ACL profile.
Add	Add a new ACL entry using given ACL name.
Action	🗑 - click it to remove the selected entry.

IV-1-2 IPv4

The function is used to show the Access Control List (ACL) based on Layer 2 to Layer 4 filtering, the IPv4. The ACL is composed by many Access Control Element (ACE) rules. You may create a new ACL here; then add multiple ACEs.



ACL Profile Name:

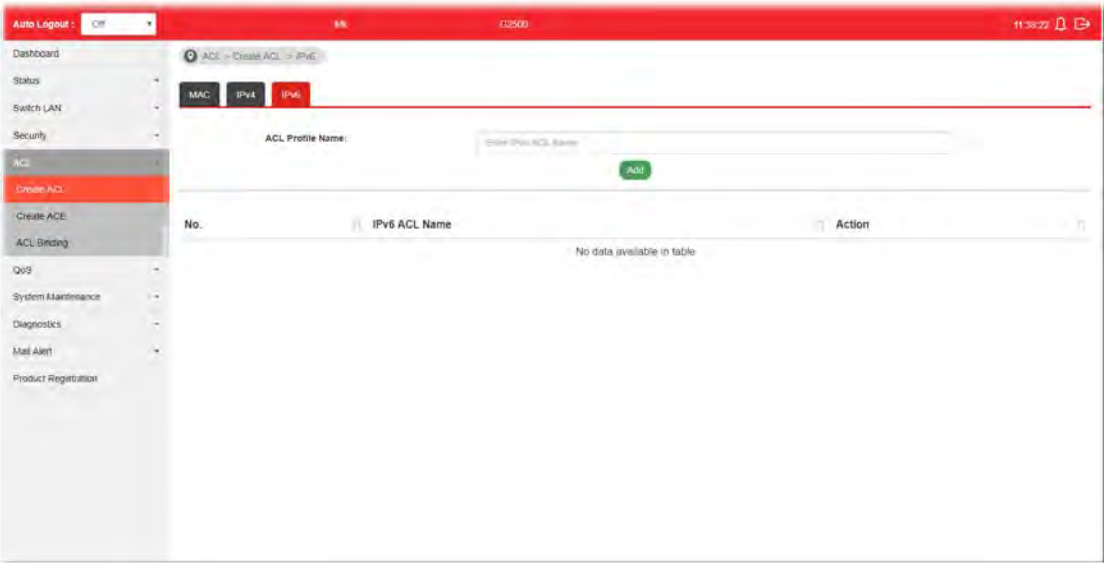
No.	IPv4 ACL Name	Action
No data available in table		

Available settings are explained as follows:

Item	Description
ACL Profile Name	Enter a name for creating a new ACL profile.
Add	Add a new ACL entry using given ACL name.
Action	🗑 - click it to remove the selected entry.

IV-1-3 IPv6

The function is used to show the Access Control List (ACL) based on Layer 2 to Layer 4 filtering, the IPv6. The ACL is composed by many Access Control Element (ACE) rules. You may create a new ACL here; then add multiple ACEs.



ACL Profile Name: Enter IPv6 ACL Name

No.	IPv6 ACL Name	Action
No data available in table		

Available settings are explained as follows:

Item	Description
ACL Profile Name	Enter a name for creating a new ACL profile.
Add	Add a new ACL entry using given ACL name.
Action	🗑 - click it to remove the selected entry.

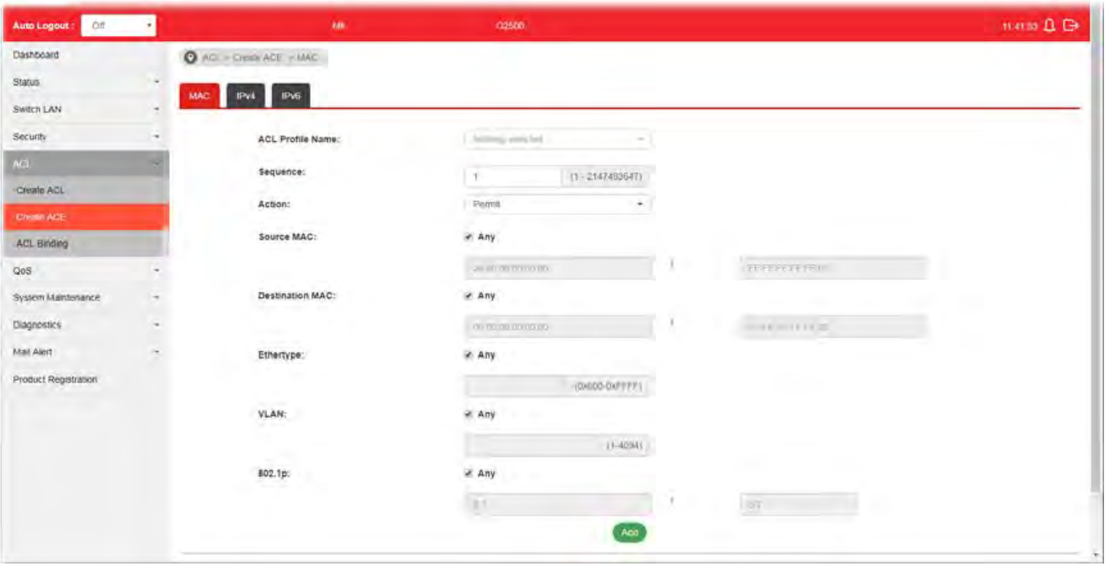
IV-2 Create ACE

Since ACL based on MAC, IPv4 and/or IPv4 has been created on the section of IV-1, now you can add multiple ACE rules for each ACL.

IV-2-1 MAC

This page shows ACE based on MAC address. You may choose ACL, permit, and deny particular packet or frame, even shutdown the port.

You may provide filtering/matching criteria for one or more of packet characteristic (such as Source/Destination MAC, Ethertype, VLAN, 802.1p) for this ACE to identify the packet.



ACL Profile Name:

Sequence: 1 (1 - 2147483647)

Action: Permit

Source MAC: ☑ Any

Destination MAC: ☑ Any

Ethertype: ☑ Any (0x600-0xFFFF)

VLAN: ☑ Any (1-4094)

802.1p: ☑ Any

Available settings are explained as follows:

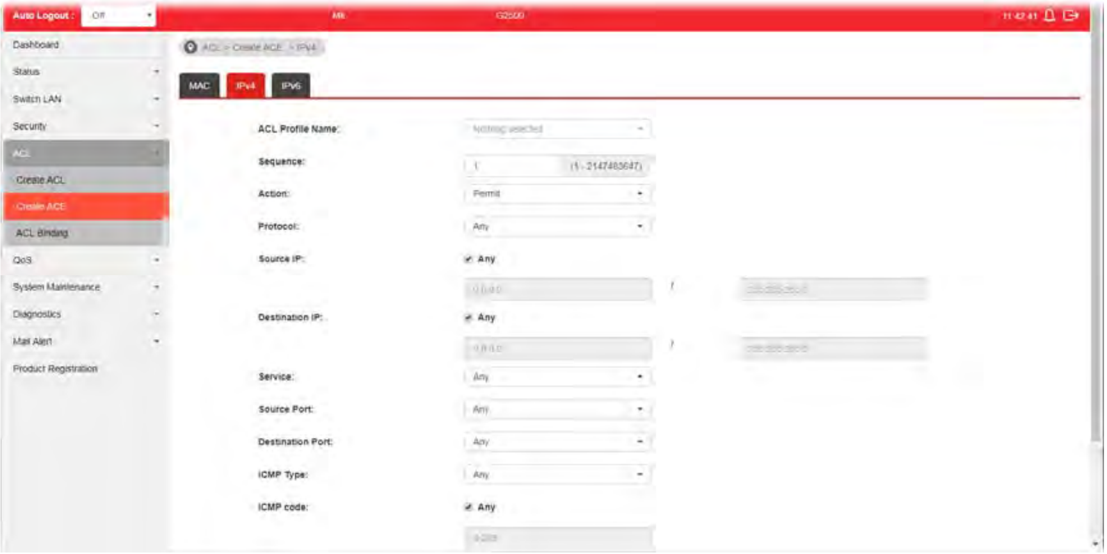
Item	Description
ACL Profile Name	Use the drop down list to selected one of the user defined ACL profiles.
Sequence	Assign a sequence number to this ACE. The sequence is used to identify which one of ACEs in an ACL is firstly used to match ingress packets. The switch port bound with an ACL use the contained ACE rules, start with the one with lower sequence number to match the packet first.
Action	Select the action applied to the packet matched this ACE. Permit or deny the packets into switch core, or shutdown the port for stopping further transmission. ● **Permit** ● **Deny** ● **Shutdown**
Source MAC / Destination MAC	Specify the source and the destination MAC address for filtering. **Any** – All packets will be filtered. Or, enter the IP address to filter the packets coming from that

	address.
Ethertype	Specify ethernet type for filtering. Select **Any**. Or, enter the value with the format of “0x600 ~ 0xFFF”.
VLAN	Specify VLAN profile for filtering. Select **Any**. Or, enter a VLAN number. The packets coming from the VLAN specified here will be filtered by Vigor device.
802.1p	Specify the 802.1p priority value for filtering. Select Any, or a number from 0 to 7.
Add	Click it to create a new ACE rule.
Modify	🔧 - click it to modify the settings for the selected entry. 🗑 - click it to remove the selected entry.

IV-2-2 IPv4

This page shows ACE based on IPv4 address. You may choose ACL, permit, and deny particular packet or frame, even shutdown the port.

You may provide filtering/matching criteria for one or more of following packet characteristic (such as Protocol over the IP layer, Source/Destination IPv4 address, Type of Service, Source/Destination port number, TCP flags, ICMP Type, if chosen protocol contains ICMP), for this ACE to identify the packet.



ACL Profile Name: Nothing selected

Sequence: 1 (1 - 2147483647)

Action: Permit

Protocol: Any

Source IP: ✓ Any

Destination IP: ✓ Any

Service: Any

Source Port: Any

Destination Port: Any

ICMP Type: Any

ICMP code: ✓ Any

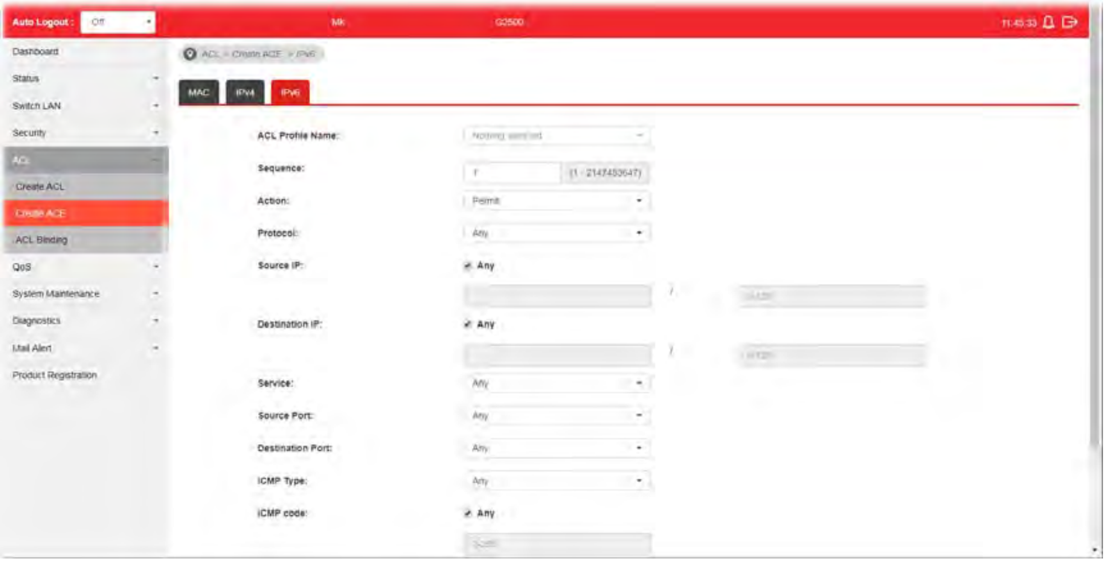
Available settings are explained as follows:

Item	Description
ACL Profile Name	Use the drop down list to selected one of the user defined ACL profiles.
Sequence	Assign a sequence number to this ACE. The sequence is used to identify which one of ACEs in an ACL is firstly used to match ingress packets. The switch port bound with an ACL use the contained ACE rules, start with the one with lower sequence

	number to match the packet first.
Action	Select the action applied to the packet matched this ACE. Permit or deny the packets into switch core, or shutdown the port for stopping further transmission. ● **Permit** ● **Deny** ● **Shutdown**
Protocol	Specify the protocol for filtering. ● **Any** – All packets will be filtered. ● **Select** – Choose one of the protocol (e.g., ICMP, IP in IP, TCP, EGP, IGP…) from the drop down list. Packets passing through the selected protocol will be filtered. ● **Define** – Specify a type number (0 – 255) for ICMP code. For example, 0 means "Echo Reply"; 254 means "RFC3692-style Experiment 2".
Source IP / Destination IP	Specify the source and the destination IPv4 address for filtering. **Any** – All packets will be filtered. Or, enter the IP address to filter the packets coming from that address.
Service	● **Any** – All packets will be filtered. ● **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. ● **IP Precedence** - All IP traffic is mapped to queues based on the IP Precedence field in the IP header. If traffic is not IP traffic, it is mapped to the lowest priority queue.
Source Port / Destination Port	Specify the source and destination port number for filtering the packets. ● **Any** – All packets will be filtered. ● **Single** – Only the packets passing through the number defined here will be filtered. ● **Range** – Only the packets passing through the port range defined here will be filtered.
ICMP Type	● **Any** – All packets will be filtered. ● **Select** – Choose one of the type (e.g., Destination Unreachable Echo Reply, MLD Query….) from the drop down list. ● **Define** – Specify a type number (0 – 255) for ICMP code. For example, 0 means "Echo Reply"; 254 means "RFC3692-style Experiment 2".
ICMP code	Each ICMP type can be defined with different codes. For example, if you define ICMP Type as "3", then the available codes for Type 3 will be 0-15. **Any** – All packets will be filtered. Or, enter 0 to 255 based on the ICMP type specifed.
Add	Click it to create a new binding profile.
Modify	🔧 - click it to modify the settings for the selected entry. 🗑 - click it to remove the selected entry.

IV-2-3 IPv6

This page allows the network administrator to create ACE based on IPv6 address.



ACL Profile Name: Nothing selected

Sequence: 1 (1 - 2147483647)

Action: Permit

Protocol: Any

Source IP: ☑ Any

Destination IP: ☑ Any

Service: Any

Source Port: Any

Destination Port: Any

ICMP Type: Any

ICMP code: ☑ Any

Available settings are explained as follows:

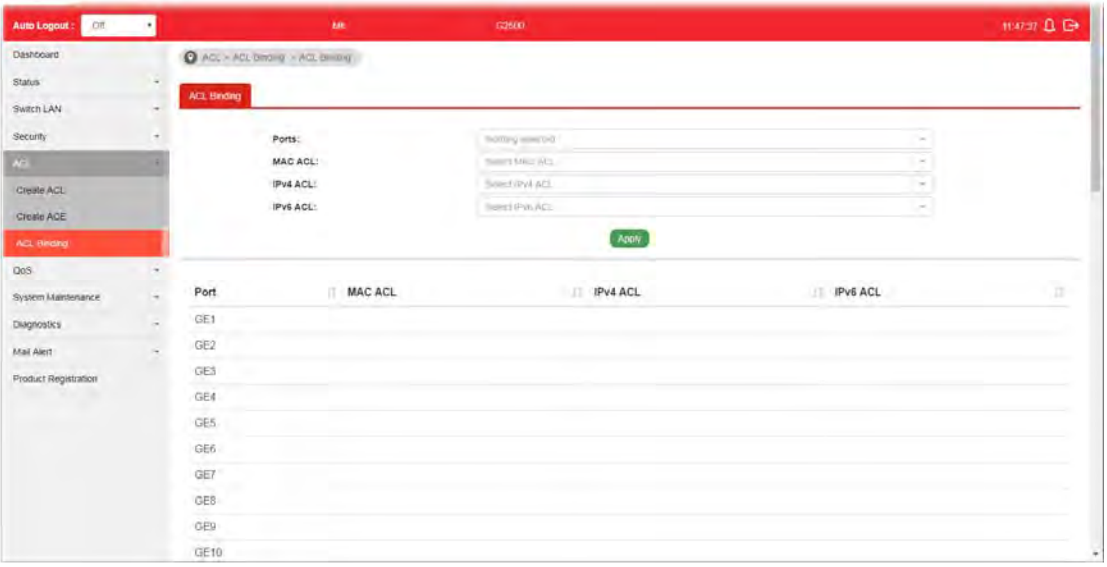
Item	Description
ACL Profile Name	Use the drop down list to selected one of the user defined ACL profiles.
Sequence	Assign a sequence number to this ACE. The sequence is used to identify which one of ACEs in an ACL is firstly used to match ingress packets. The switch port bound with an ACL use the contained ACE rules, start with the one with lower sequence number to match the packet first.
Action	Select the action applied to the packet matched this ACE. Permit or deny the packets into switch core, or shutdown the port for stopping further transmission. ● **Permit** ● **Deny** ● **Shutdown**
Protocol	Specify the protocol for filtering. ● **Any** – All packets will be filtered. ● **Select** – Choose one of the protocol (e.g., ICMP, TCP, EGP...) from the drop down list. Packets passing through the selected protocol will be filtered. ● **Define** – Specify a type number (0 – 255) for ICMP code. For example, 0 means "Echo Reply"; 254 means "RFC3692-style Experiment 2".
Source IP / Destination IP	Specify the source and the destination IPv6 address for filtering. **Any** – All packets will be filtered. Or, enter the IPv6 address to filter the packets coming from that address.
Service	● **Any** – All packets will be filtered. ● **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. ● **IP Precedence** - All IP traffic is mapped to queues based on the IP Precedence field in the IP header. If traffic is not IP traffic, it is mapped to the lowest priority queue.
Source Port / Destination Port	Specify the source and destination port number for filtering the packets. ● **Any** – All packets will be filtered. ● **Single** – Only the packets passing through the number defined here will be filtered. ● **Range** – Only the packets passing through the port range defined here will be filtered.
ICMP Type	● **Any** – All packets will be filtered. ● **Select** – Choose one of the type (e.g., Destination Unreachable Echo Reply, MLD Query….) from the drop down list. ● **Define** – Specify a type number (0 – 255) for ICMP code. For example, 0 means “Echo Reply”; 254 means “RFC3692-style Experiment 2”.
ICMP code	Each ICMP type can be defined with different codes. For example, if you define ICMP Type as “3”, then the available codes for Type 3 will be 0-15. **Any** – All packets will be filtered. Or, enter 0 to 255 based on the ICMP type specifed.
Add	Click it to create a new binding profile.
Modify	🔧- Click it to modify the settings for the selected profile. 🗑- Click it to remove the selected entry.

IV-3 ACL Binding

This section allows you to bind Access Control Lists created in previous section to an interface (physical port or aggregation).

A physical port can only be bound with one of the IPv4 and IPv6 ACL, not both.



Ports: Nothing selected

MAC ACL: Select MAC ACL

IPv4 ACL: Select IPv4 ACL

IPv6 ACL: Select IPv6 ACL

Port	MAC ACL	IPv4 ACL	IPv6 ACL
GE1			
GE2			
GE3			
GE4			
GE5			
GE6			
GE7			
GE8			
GE9			
GE10			

Available settings are explained as follows:

Item	Description
Ports	Use the drop down list to select the port profiles (GE1 to GE28) for binding ACL.
MAC ACL / IPv4 ACL / IPv6 ACL	Select ACLs (MAC, IPv4, and/or IPv6) to be bound on this interface (port), so Switch may filter packets by using it.
Apply	Apply the settings to the switch.

Part V QoS Configuration

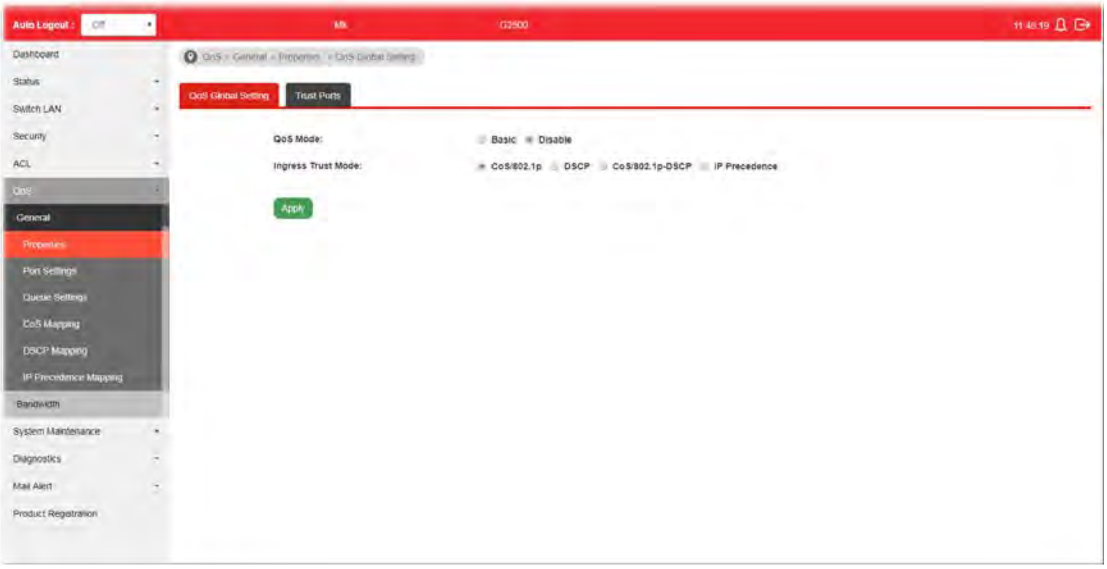
V-1 General

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.

V-1-1 Properties

V-1-1-1 QoS General Setting

This page allows the network administrator to specify Ingress Trust Mode for basic QoS mode.



QoS Mode: ○ Basic ● Disable

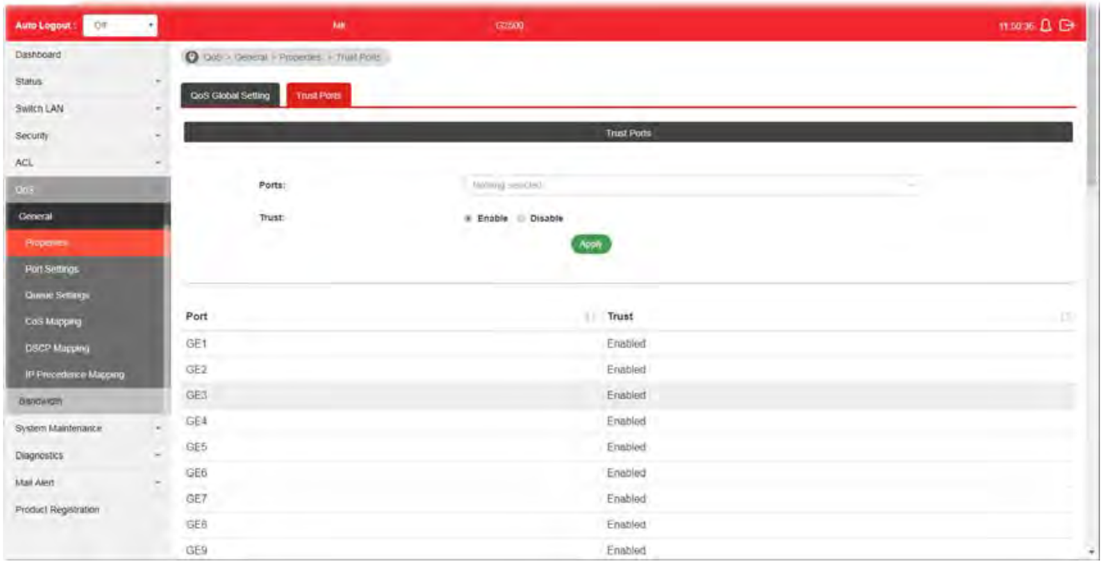
Ingress Trust Mode: ● CoS/802.1p ○ DSCP ○ CoS/802.1p-DSCP ○ IP Precedence

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	Apply the settings to the switch.

V-1-1-2 Trust Ports

This page allows the network administrator 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: ● Enable ○ Disable

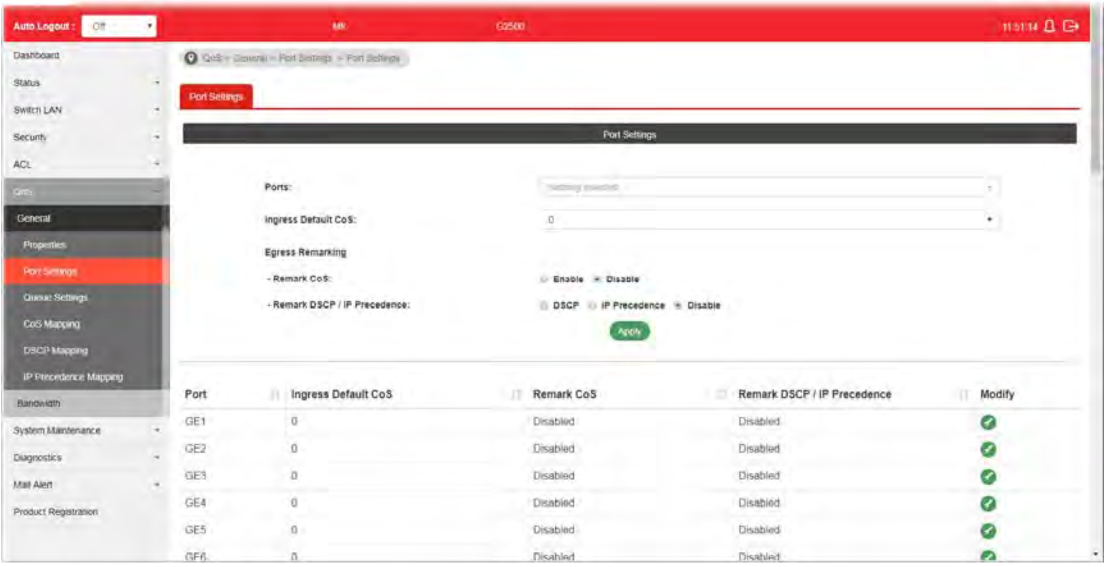
Port	Trust
GE1	Enabled
GE2	Enabled
GE3	Enabled
GE4	Enabled
GE5	Enabled
GE6	Enabled
GE7	Enabled
GE8	Enabled
GE9	Enabled

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	Apply the settings to the switch.

V-1-2 Port Settings

This page allows the network administrator 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: ○ Enable ● Disable

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

Port	Ingress Default CoS	Remark CoS	Remark DSCP / IP Precedence	Modify
GE1	0	Disabled	Disabled	✓
GE2	0	Disabled	Disabled	✓
GE3	0	Disabled	Disabled	✓
GE4	0	Disabled	Disabled	✓
GE5	0	Disabled	Disabled	✓
GE6	0	Disabled	Disabled	✓

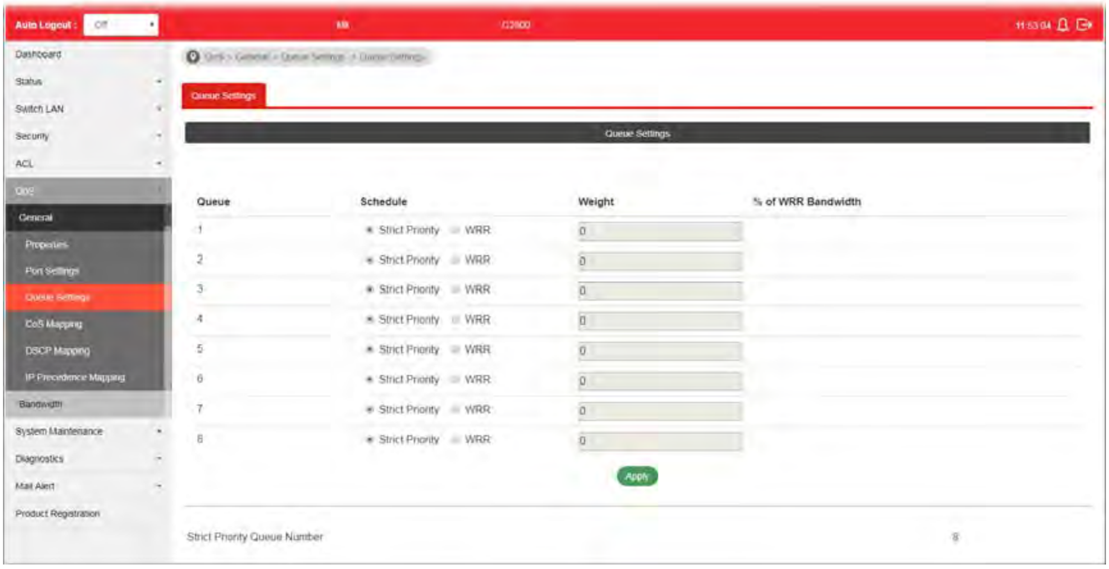
Available settings are explained as follows:

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.
Apply	Apply the settings to the switch.
Modify	- Click it to modify the settings for the selected port profile.

V-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.



Queue Settings

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

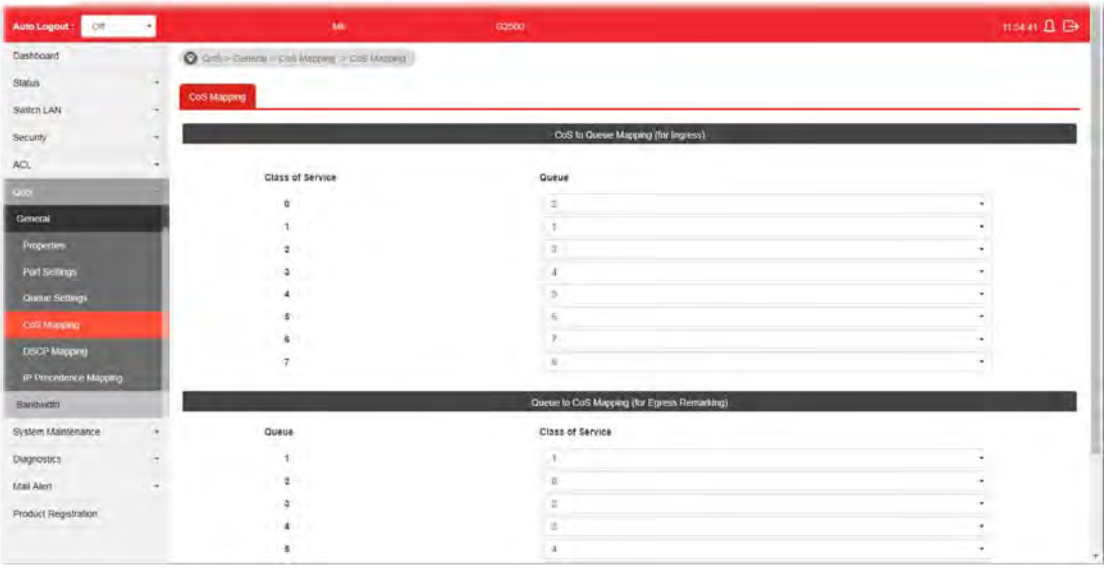
Available settings are explained as follows:

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	Apply the settings to the switch.
Strict Priority Queue Number	Display the number of queues using Strict Priority method.

V-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
5	4

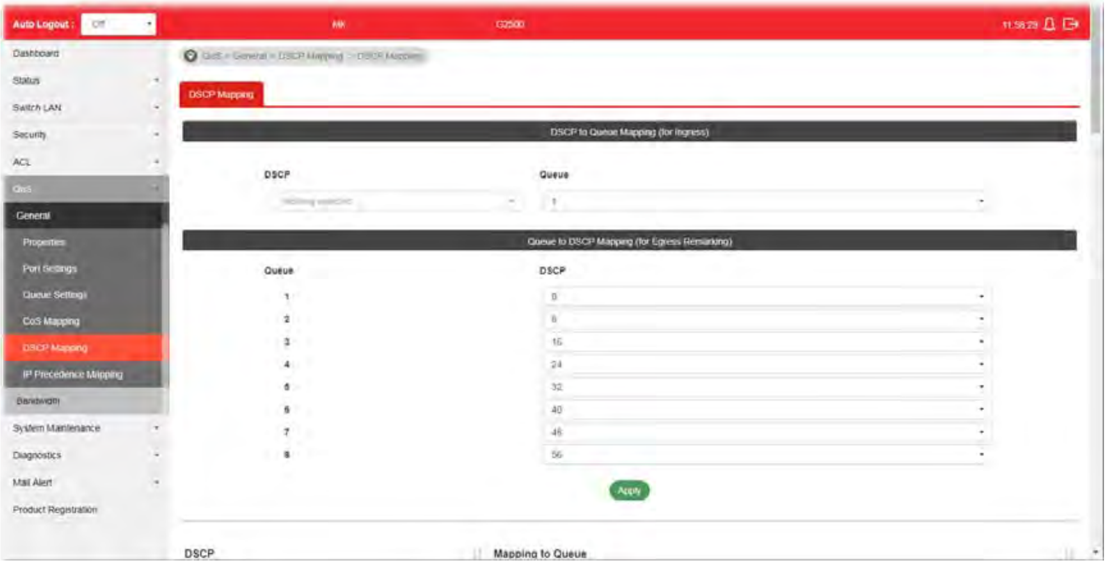
Available settings are explained as follows:

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	Apply the settings to the switch.

V-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

DSCP | Mapping to Queue

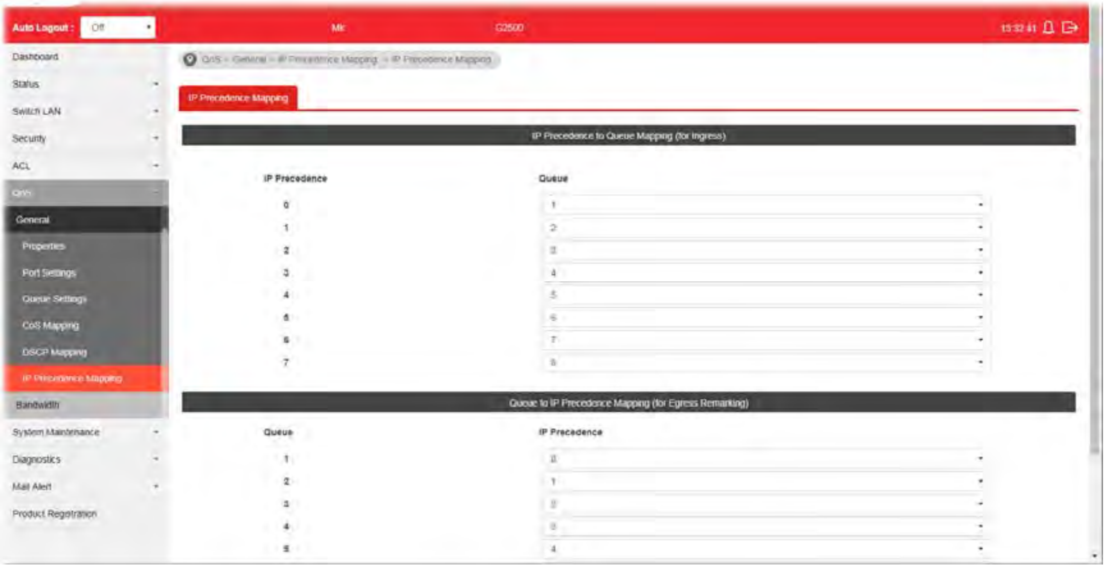
Available settings are explained as follows:

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	Apply the settings to the switch.

V-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
5	4

Available settings are explained as follows:

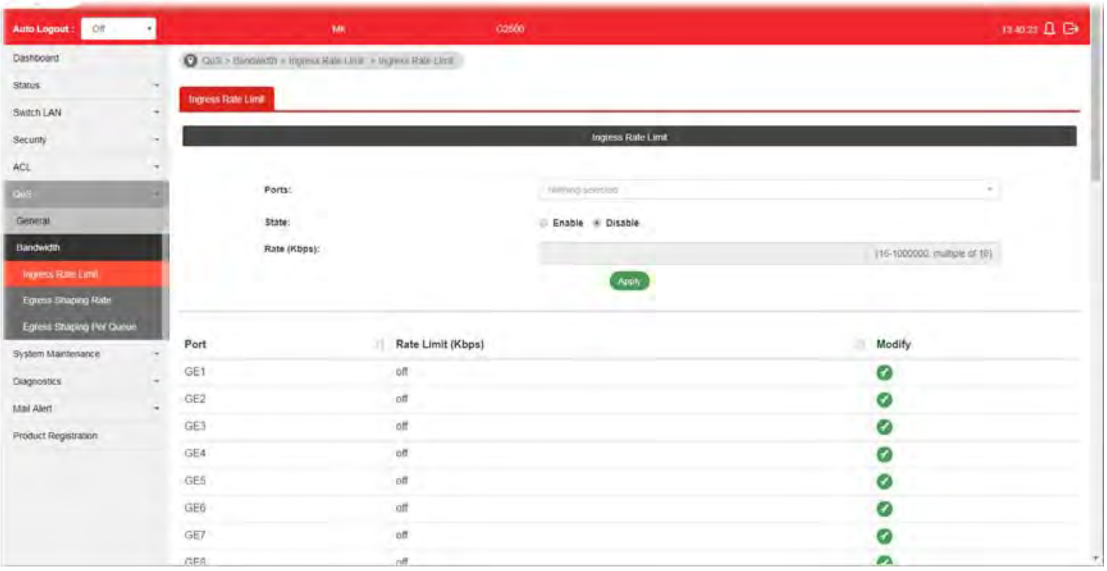
Item	Description
IP Precedence to Queue Mapping (for Ingress) - Settings for the incoming packets.	
IP Precedence	Display the IP Precedence value (0 to 7).
Queue	Define the queue ID (level 1 to 8) for different IP Precedence values.
Queue to IP Precedence Mapping (for Egress Remarking) - Settings for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

V-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.

V-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: ○ Enable ● Disable

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

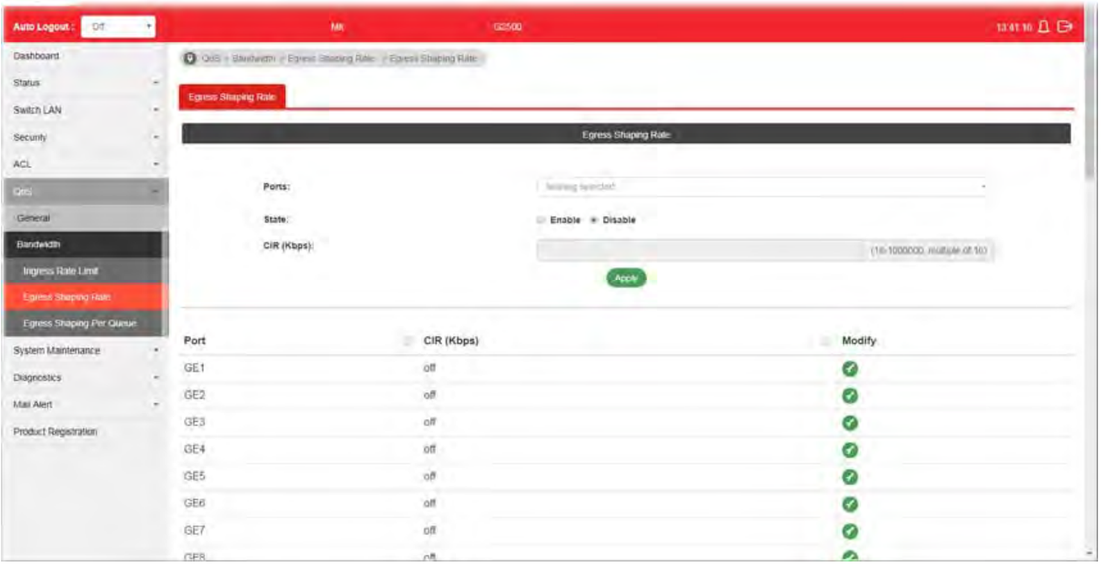
Port	Rate Limit (Kbps)	Modify
GE1	off	✓
GE2	off	✓
GE3	off	✓
GE4	off	✓
GE5	off	✓
GE6	off	✓
GE7	off	✓
GE8	off	✓

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	Apply the settings to the switch.
Modify	🔧 - Click it to modify the settings for the selected port profile.

V-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: ○ Enable ● Disable

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

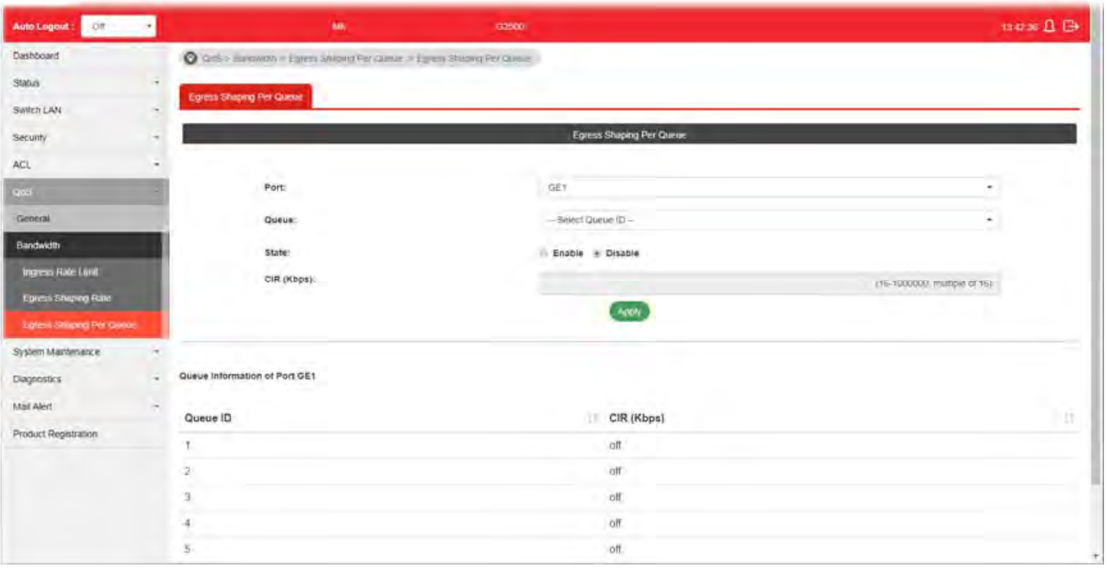
Port	CIR (Kbps)	Modify
GE1	off	✓
GE2	off	✓
GE3	off	✓
GE4	off	✓
GE5	off	✓
GE6	off	✓
GE7	off	✓
GE8	off	✓

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	Apply the settings to the switch.
Modify	🔧 - Click it to modify the settings for the selected port profile.

V-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.



Egress Shaping Per Queue

Port: GE1

Queue: -- Select Queue ID --

State: ○ Enable ● Disable

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

Queue Information of Port GE1

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

Available settings are explained as follows:

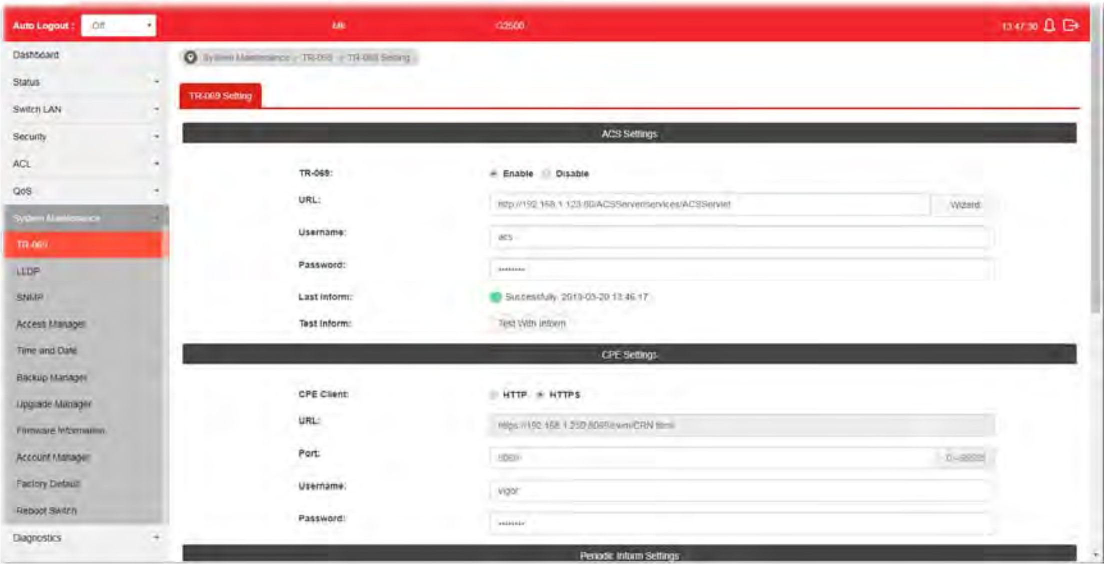
Item	Description
Egress Shapping Per Queue	
Port	Use the drop down list to select the port profile (GE1 to GE28) or profiles.
Queue	Use the drop down list to select queue number (1 to 8) for the selected GE port.
State	● **Disable** – Disable egress bandwidth control. ● **Enable** - Enable egress bandwidth control.
CIR (Kbps)	Enter the rate value,<16-1000000>,unit:16 Kbps.
Apply	Apply the settings to the switch.

This page is left blank.

Part VI System Maintenance

VI-1 TR-069

This page allows a user to configure TR-069 settings for connecting to VigorACS 2.



ACS Settings

TR-069: ● Enable ○ Disable

URL: http://192.168.1.123:80/ACSServer/services/ACSServlet Wizard

Username: acs

Password: ••••••••

Last Inform: Successfully. 2019-03-20 13:46:17

Test Inform: Test With Inform

CPE Settings

CPE Client: ○ HTTP ● HTTPS

URL: https://192.168.1.250:8069/cwm/CRN.html

Port: 8069 (1~65535)

Username: vigor

Password: ••••••••

Available settings are explained as follows:

Item	Description
ACS Settings	● **TR-069** - Click **Enable** to activate the settings on this page. ● **URL** - The URL must be entered according to the ACS (Auto Configuration Server) you want to link. ● **Wizard** - Click it to enter the IP address of VigorACS server, port number and the handler. ● **Username** - The string of username must be entered according to the VigorACS (Auto Configuration Server) you want to link. ● **Password** - The password must be entered according to the VigorACS (Auto Configuration Server) you want to link. ● **Last Inform** - Display the time that VigorACS server makes a response while receiving Inform message from CPE last time. ● **Test Inform** - Click **Test With Inform** to send a message to test if such CPE is able to communicate with VigorACS server.
CPE Settings	● **CPE Client** - Choose **HTTP** or **HTTPS** for connecting with VigorACS. ● **URL** - Display the URL of VigorSwitch. ● **Port** - Type the username and password that VigorACS can use to access into this switch. ● **Username** - Enter the username that VigorACS can use to access into this switch. ● **Password** - Enter the password that VigorACS can use to access into this swtich.
Periodic Inform Settings	● **Periodic Inform Settings** - Click **Enable** to configure the

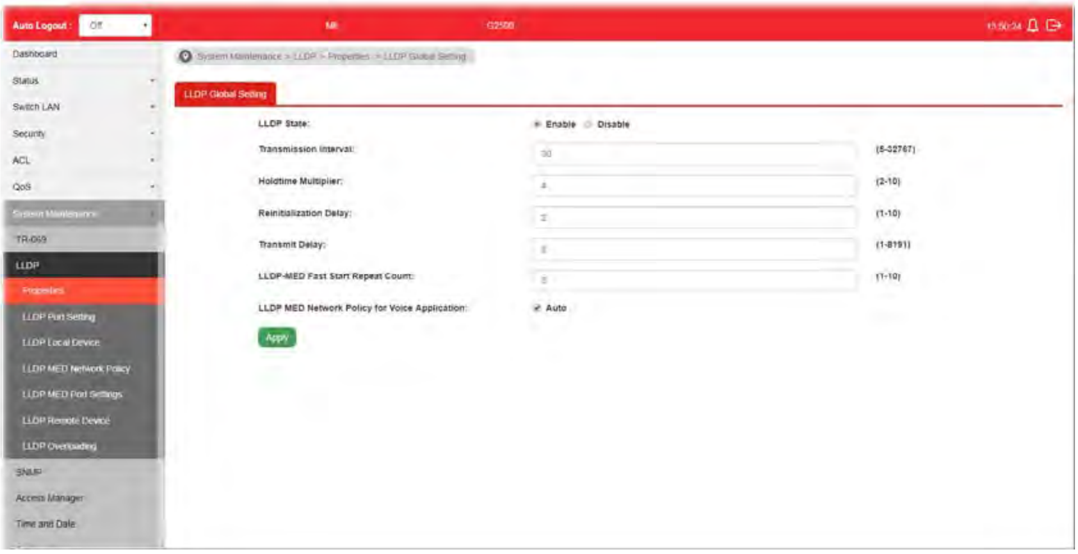
	interval time. ● **Interval Time** - Set the interval time for the switch to send notification to CPE.
STUN Settings	● **STUN Settings** - Click **Enable** to configure STUN settings. ● **Server Address** - Enter the IP address of the STUN server. ● **Server Port** - Enter the port number of the STUN server. ● **Minimum Keep Alive Period** - If STUN is enabled, the switch must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds". ● **Maximum Keep Alive Period** - If STUN is enabled, the switch must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.
Health Check	Vigor system will check the health status of LAN ports including link up /down or speed change. ● **Port Link Up/Down** - Select LAN port(s) to do the health check of port link. ● **Link Speed Change** - Select LAN port(s) to do the health check of speed change.
Apply	Apply the settings to the switch.
Clear	Discard current settings.

VI-2 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-2-1 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: 3 (1-8191)

LLDP-MED Fast Start Repeat Count: 3 (1-10)

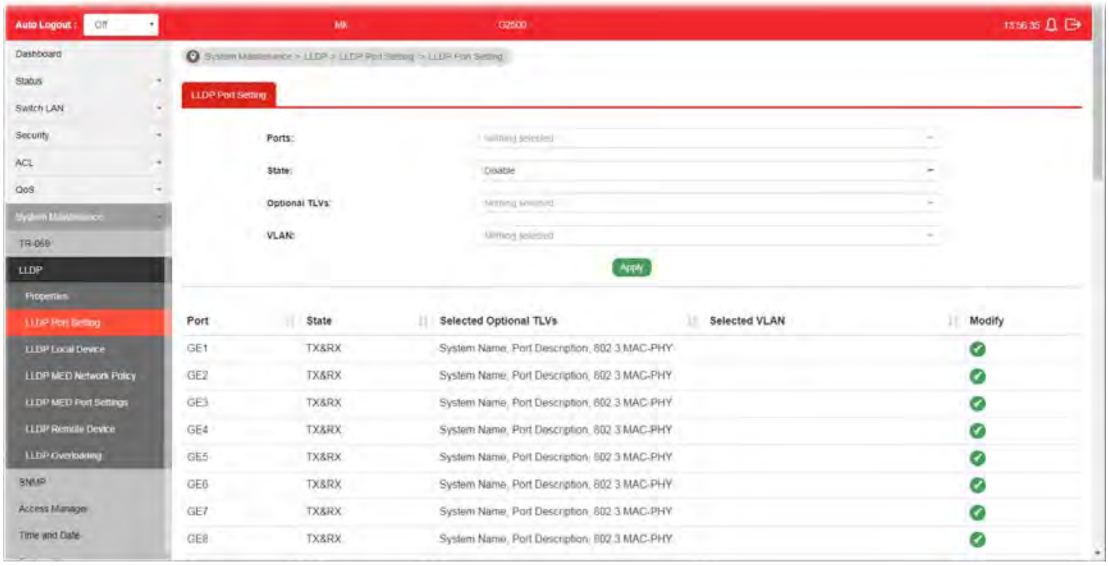
LLDP MED Network Policy for Voice Application: ☑ Auto

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).
LLDP-MED Fast Start Repeat Count	Select the number of LLDP packets that will be sent during LLDP-MED Fast Start period. The default is 3. Available range is from 1 to 10.
LLDP MED Network Policy for Voice Application	The default is Auto.
Apply	Apply the settings to the switch.

VI-2-2 LLDP Port Setting

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



Ports: Nothing selected

State: Disable

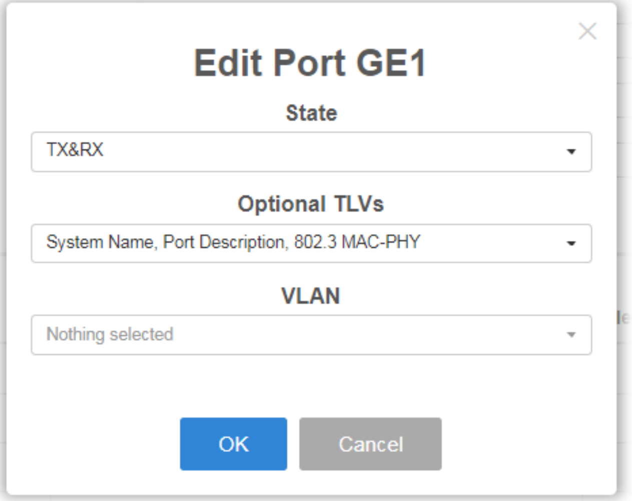
Optional TLVs: Nothing selected

VLAN: Nothing selected

Port	State	Selected Optional TLVs	Selected VLAN	Modify
GE1	TX&RX	System Name, Port Description, 802.3 MAC-PHY		✓
GE2	TX&RX	System Name, Port Description, 802.3 MAC-PHY		✓
GE3	TX&RX	System Name, Port Description, 802.3 MAC-PHY		✓
GE4	TX&RX	System Name, Port Description, 802.3 MAC-PHY		✓
GE5	TX&RX	System Name, Port Description, 802.3 MAC-PHY		✓
GE6	TX&RX	System Name, Port Description, 802.3 MAC-PHY		✓
GE7	TX&RX	System Name, Port Description, 802.3 MAC-PHY		✓
GE8	TX&RX	System Name, Port Description, 802.3 MAC-PHY		✓

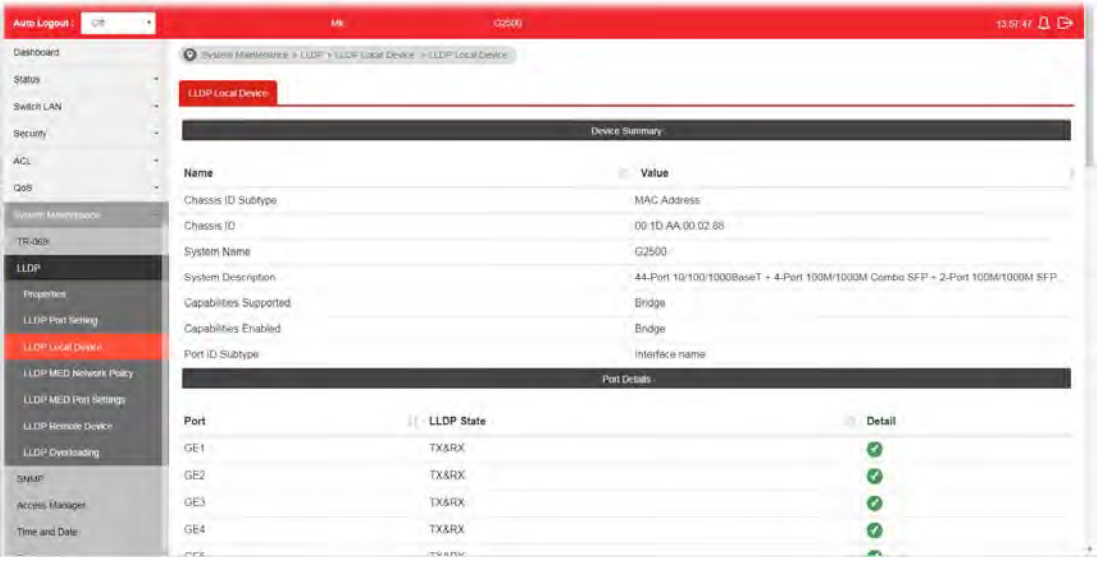
Available settings are explained as follows:

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	Apply the settings to the switch.
Modify	✓ - Click it to modify the settings for the selected port profile.

	 Edit Port GE1 State TX&RX Optional TLVs System Name, Port Description, 802.3 MAC-PHY VLAN Nothing selected

VI-2-3 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:00:02:88
System Name	G2500
System Description	44-Port 10/100/1000BaseT + 4-Port 100M/1000M Combo SFP + 2-Port 100M/1000M SFP
Capabilities Supported	Bridge
Capabilities Enabled	Bridge
Port ID Subtype	Interface name

Port Details

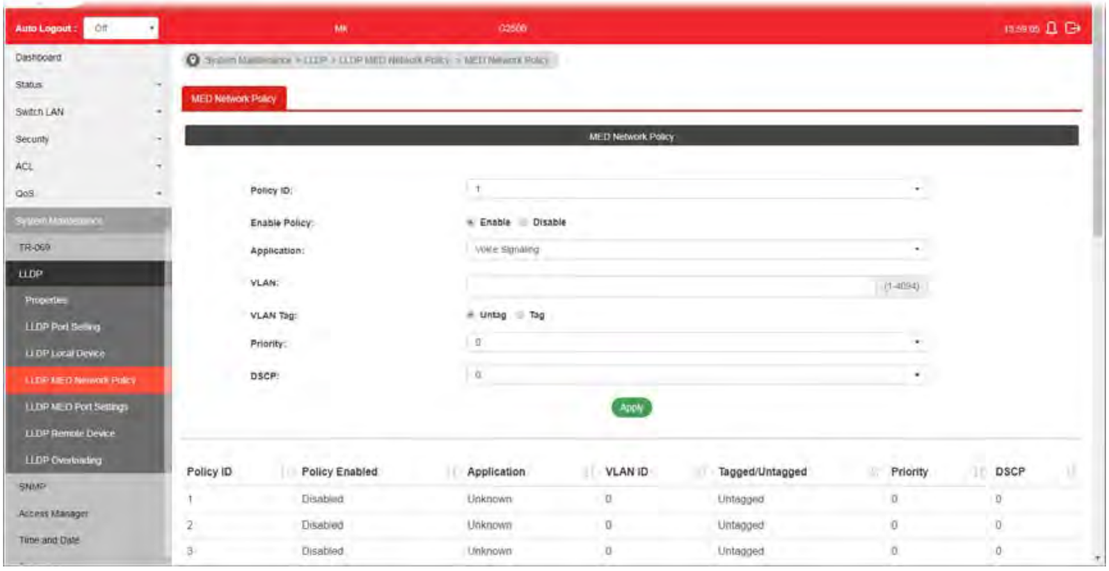
Port	LLDP State	Detail
GE1	TX&RX	✓
GE2	TX&RX	✓
GE3	TX&RX	✓
GE4	TX&RX	✓

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 the button under 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-2-4 MED Network Policy

This page allows the network administrator to set MED (Media Endpoint Discovery) network policy.



Policy ID: 1

Enable Policy: ● Enable ○ Disable

Application: Voice Signaling

VLAN: (1-4094)

VLAN Tag: ● Untag ○ Tag

Priority: 0

DSCP: 0

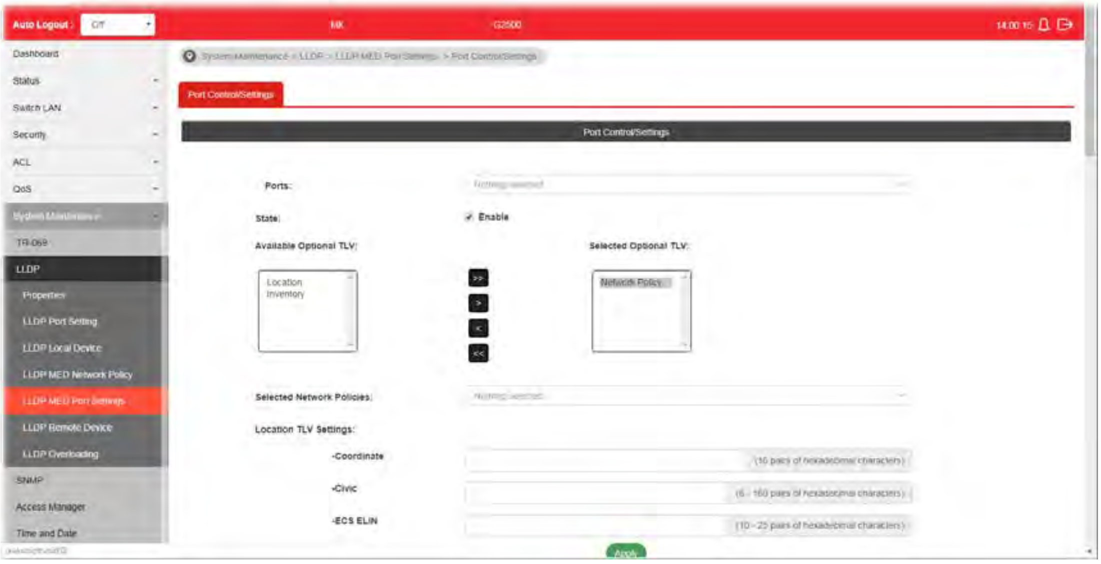
Policy ID	Policy Enabled	Application	VLAN ID	Tagged/Untagged	Priority	DSCP
1	Disabled	Unknown	0	Untagged	0	0
2	Disabled	Unknown	0	Untagged	0	0
3	Disabled	Unknown	0	Untagged	0	0

Available settings are explained as follows:

Item	Description
Policy ID	Choose a number for configuring the policy profile. Available selections include 1 to 32.
Enable Policy	**Enable** – Click it to enable such function.
Application	There are several applications which can be used for MED network. Selections include Voice Signaling, Guest Voice, Guest Voice Signaling, Softphone Voice, Video Conferencing, Stream Video and Video Signaling.
VLAN	Set a VLAN ID (ranging from 1 to 4095) for such profile.
VLAN Tag	Specify if the outgoing packets will be tagged or not. ● **Untag** – Packets will be sent out without any tag. ● **Tag** – Packets will be sent out with a number tagged.
Priority	Set Layer2 priority (range from 0 to 7).
DSCP	Set DSCP value (range form 0 to 63).
Apply	Apply the settings to the switch.

VI-2-5 LLDP MED Port Settings

This page allows the network administrator to configure TLV (Type / Length / Value) settings for each port.



Port Control/Settings

Ports: Nothing selected

State: ☑ Enable

Available Optional TLV: Location, Inventory

Selected Optional TLV: Network Policy

Selected Network Policies: Nothing selected

Location TLV Settings:

-Coordinate (16 pairs of hexadecimal characters)

-Civic (6 - 160 pairs of hexadecimal characters)

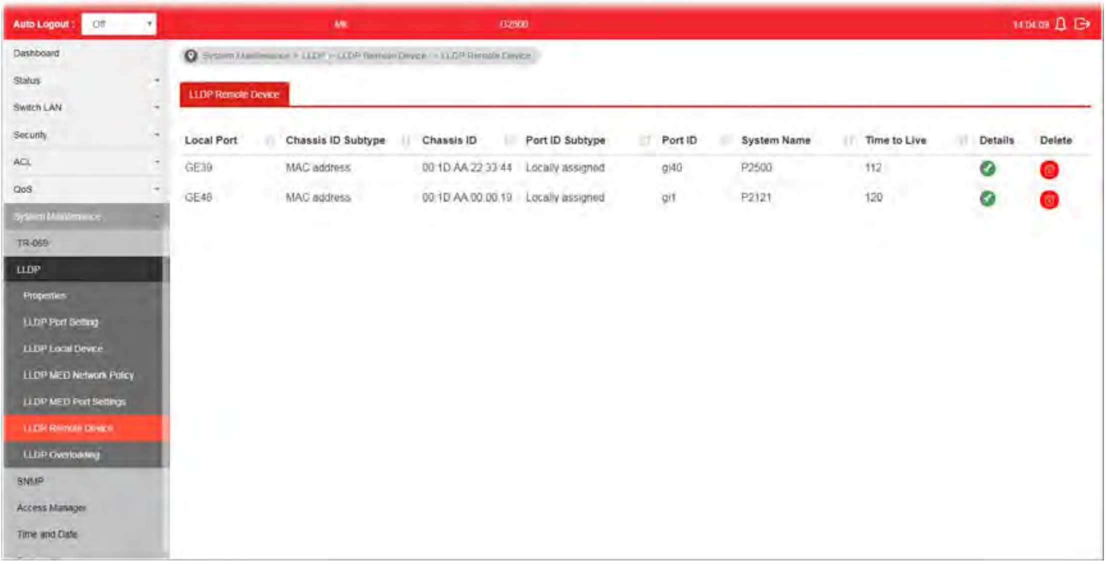
-ECS ELIN (10 - 25 pairs of hexadecimal characters)

Available settings are explained as follows:

Item	Description
Ports	Choose the port(s) for configuring TLV settings.
State	**Enable** – Click it to enable LLDP MED on the selected port.
Available Optional TLV	Available TLV items will be shown in this field. Choose the one(s) you want and click the >> arrow to transfer the selection(s) to the field of "Selected Optional TLV".
Selected Optional TLV	Display the selected TLV items.
Selected Network Policies	Select network policy profiles (created in **LLDP>>LLDP MED Network Policy**) for applying onto the selected port.
Location TLV Settings	Define the location, civic address and ECS ELIN for LLDP protocol. ● **Coordinate** –Enter the coordinate location in 16 pairs of hexadecimal characters. ● **Civic** – Enter the civic address in 6 ~ 160 pairs of hexadecimal characters. ● **ECS ELIN** - Enter the ECS (Emergency Call Service) ELIN (Emergency Location Identification Number) in 10 ~ 25 pairs of hexadecimal characters.
Apply	Apply the settings to the switch.

VI-2-6 LLDP Remote Device

This page allows the network administrator to view the information sent from neighboring devices by LLDP protocol.



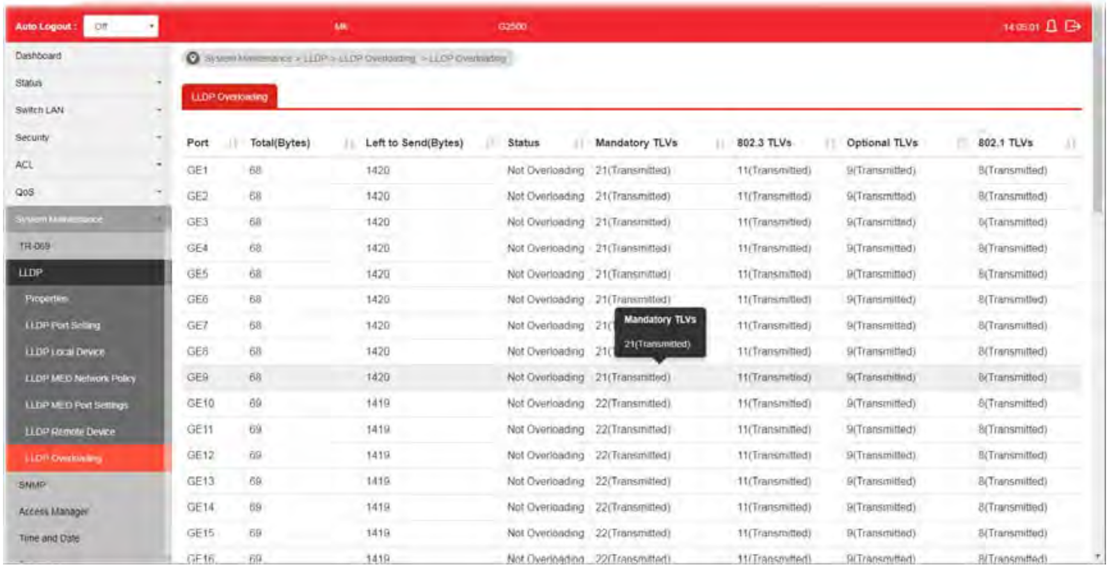
Local Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	System Name	Time to Live	Details	Delete
GE39	MAC address	00:1D:AA:22:33:44	Locally assigned	gi40	P2500	112	✓	●
GE48	MAC address	00:1D:AA:00:00:19	Locally assigned	gi1	P2121	120	✓	●

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-2-7 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(Bytes)	Status	Mandatory TLVs	802.3 TLVs	Optional TLVs	802.1 TLVs
GE1	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE2	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE3	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE4	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE5	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE6	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE7	68	1420	Not Overloading	21(	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE8	68	1420	Not Overloading	21(	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE9	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE10	69	1419	Not Overloading	22(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE11	69	1419	Not Overloading	22(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE12	69	1419	Not Overloading	22(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE13	69	1419	Not Overloading	22(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE14	69	1419	Not Overloading	22(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE15	69	1419	Not Overloading	22(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE16	69	1419	Not Overloading	22(Transmitted)	11(Transmitted)	9(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(Bytes)	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-3 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

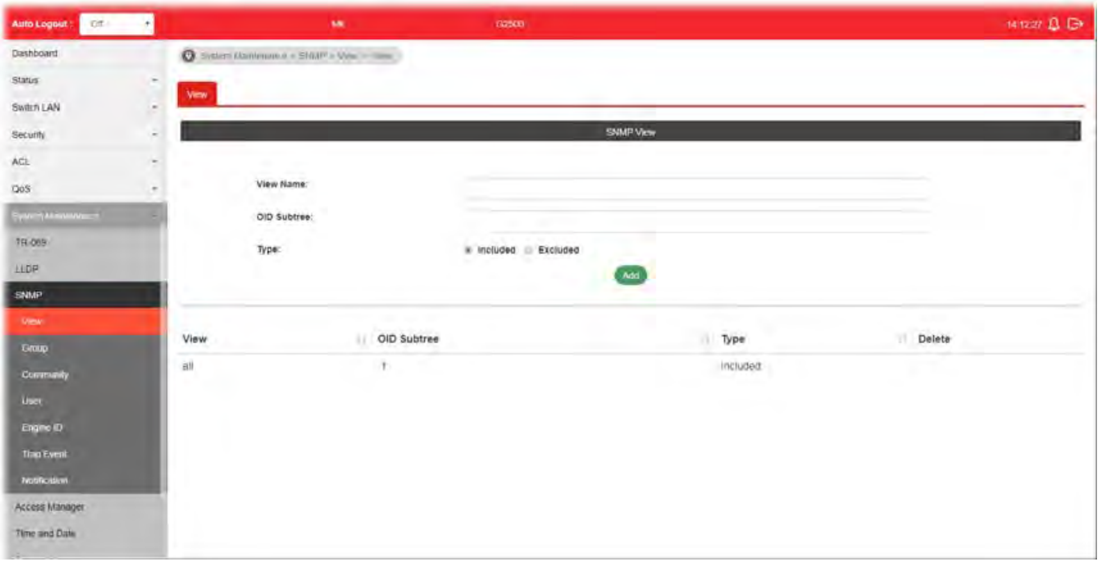
A managed device is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional (read and write) access to node-specific information. Managed devices exchange node-specific information with the NMSs. Sometimes called network elements, the managed devices can 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-3-1 View

This page allows the network administrator to create MIB views (Management information base) and then include or exclude OID (Object Identifier) in a view.



View Name:

OID Subtree:

Type: ● Included ○ Excluded

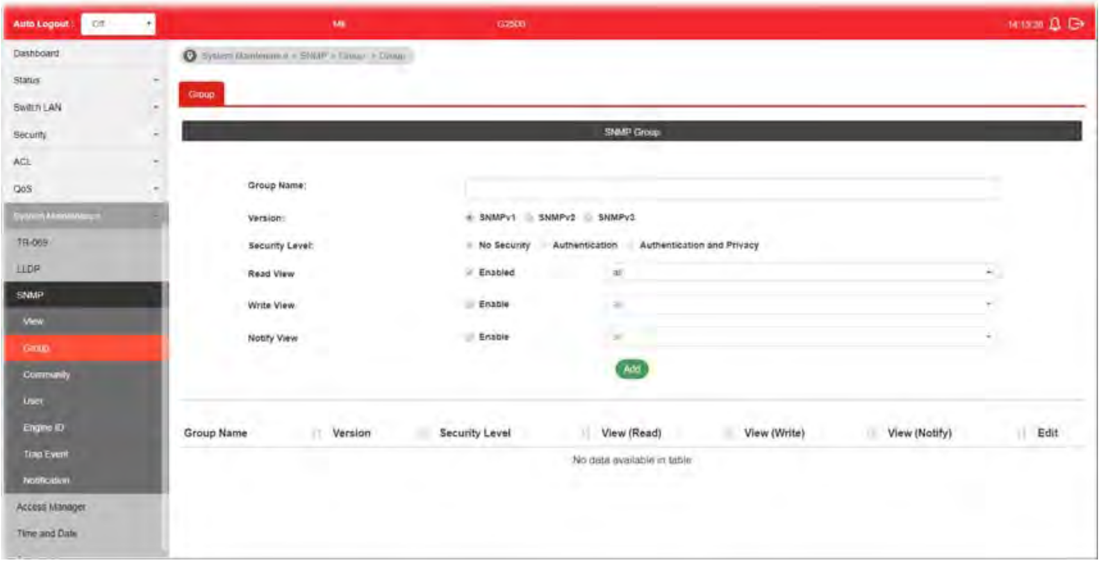
View	OID Subtree	Type	Delete
all	1	Included	

Available settings are explained as follows:

Item	Description
View Name	Enter a name of the MIB view.
OID Subtree	Enter an OID string to be included or excluded from the MIB view.
Type	Determine to include or exclude the selected MIBs.
Apply	Apply the settings to the switch.

VI-3-2 Group

This page allows the network administrator to group SNMP users and assign different authorization and access privileges.



Group Name:

Version: ● SNMPv1 ○ SNMPv2 ○ SNMPv3

Security Level: ● No Security ○ Authentication ○ Authentication and Privacy

Read View ☑ Enabled all

Write View ☐ Enable all

Notify View ☐ Enable all

Group Name	Version	Security Level	View (Read)	View (Write)	View (Notify)	Edit
No data available in table						

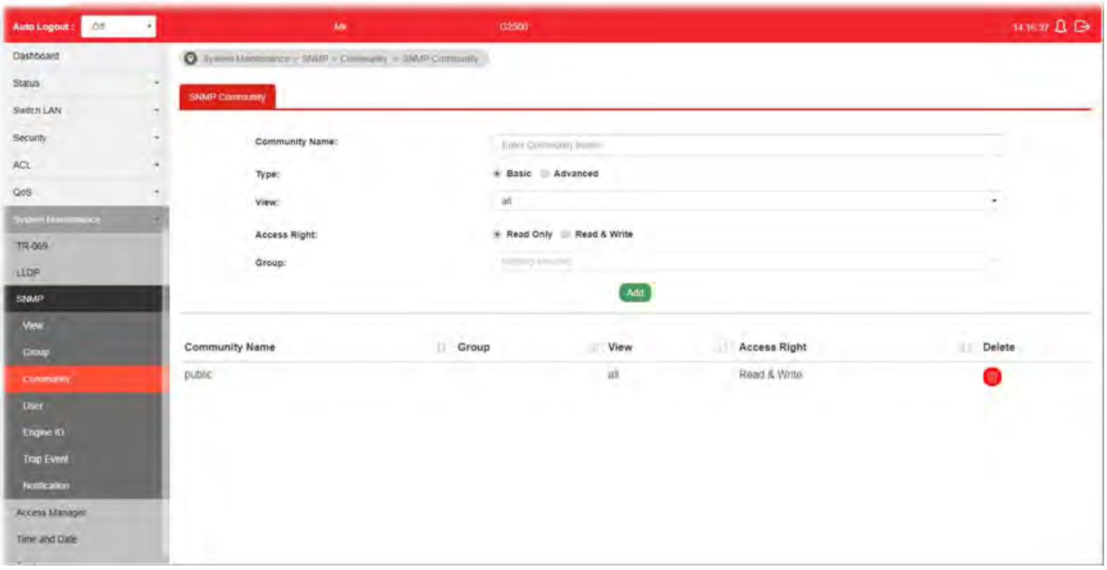
Available settings are explained as follows:

Item	Description
Group Name	Enter a name for the group.
Version	Specify SNMP version.
Security Level	Specify SNMP security level for the group. It is available when SNMPv3 is selected. ● **No Security** – No authentication and no encryption. ● **Authentication** – Requires authentication but no encryption. ● **Authentication and Privacy** –Requires authentication and encryption.
Read View	**Enabled** – Users of this group have the right to read the selected MIB view. Use the drop down list to select one of the views. The default is “all”, which means the group user can read all MIB views.
Write View	**Enabled** – Users of this group have the right to write the selected MIB view. Use the drop down list to select one of the views. The default is “all”, which means the group user can write all MIB views.
Notify View	**Enabled** – Users of this group have the right to send notification for the selected MIB view. Use the drop down list to select one of the views. The default is “all”, which means the group user have the right to send notification for all MIB views.
Add	Click it to create a new group profile.
Edit	🔧 - Click it to modify the settings for the selected group.

	🗑- click it to remove the selected group.

VI-3-3 Community

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



Community Name: Enter Community Name

Type: ● Basic ○ Advanced

View: all

Access Right: ● Read Only ○ Read & Write

Group:

Add

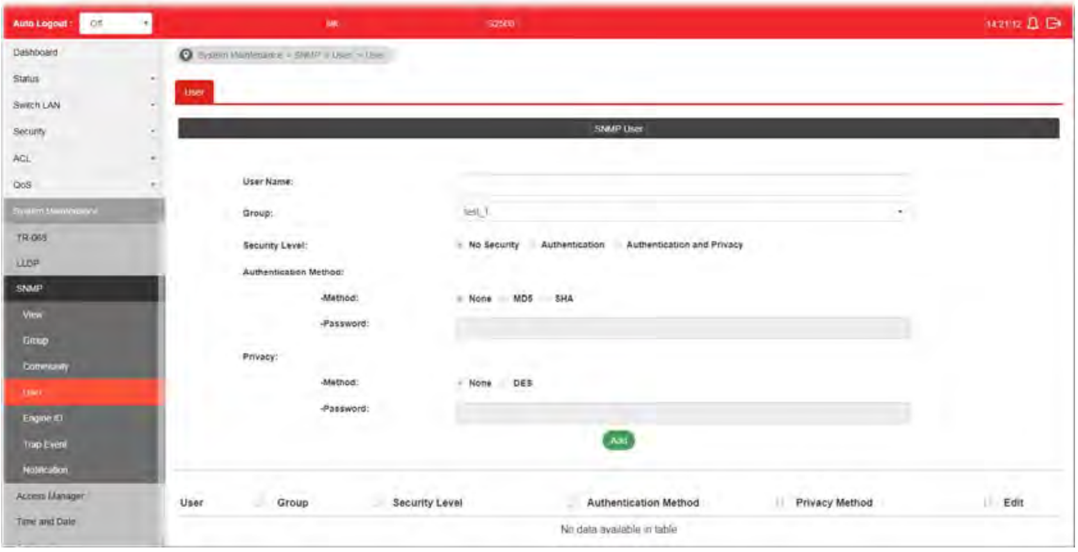
Community Name	Group	View	Access Right	Delete
public		all	Read & Write	●

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.
Type	● **Basic** – View and access right can be specified for such SNMP community profile. ● **Advanced** – Specify one of the SNMP groups for such SNMP community profile.
View	Simply specify one of the view profiles (created in **SNMP>>View**) from the drop down list.
Access Right	● **Read Only** – It allows unidirectional access to node-specific information. ● **Read & Write** - It allows bidirectional access to node-specific information.
Group	Specify the SNMP group configured by user (**SNMP>>Group**) to define the object available to the community.
Add	Click it to add a new community.
Delete	Click the icon to remove the selectd community strings.

VI-3-4 User

This page allows a user to configure SNMP user profile.



User Name:

Group: test_1

Security Level: ● No Security ○ Authentication ○ Authentication and Privacy

Authentication Method:

-Method: ● None ○ MD5 ○ SHA

-Password:

Privacy:

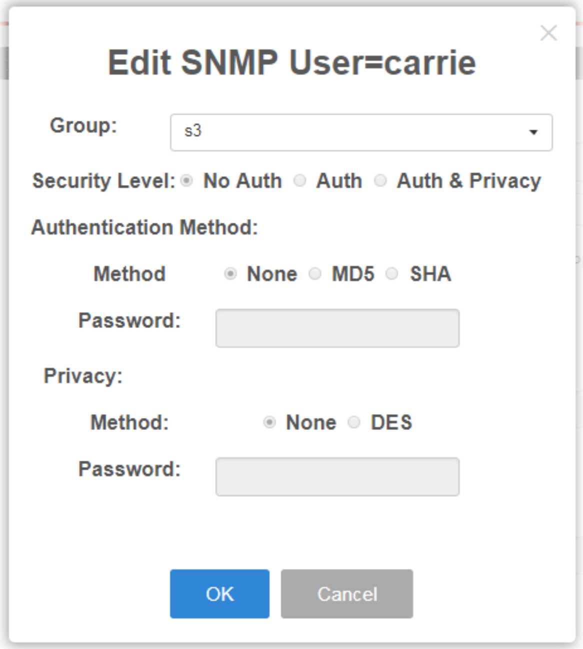
-Method: ● None ○ DES

-Password:

User	Group	Security Level	Authentication Method	Privacy Method	Edit
No data available in table					

Available settings are explained as follows:

Item	Description
User Name	Enter a name for creating new SNMP user.
Group	Choose one of the SNMP group from the drop down list. Then, this user profile will be grouped under the selected SNMP group.
Security Level	Specify SNMP security level for the group. It is available when SNMPv3 is selected. ● **No Security** – No authentication. ● **Authentication** – Authentication without encryption will be performed for packets. ● **Authentication and Privacy** – Authentication with encryption will be performed for packets.
Authentication Method	It is available when **Authentication** or **Authentication and Privacy** is selected as security level. ● **Method** – At present, available methods include None, MD5 and SHA. ● **Password** – Enter a password for the selected method.
Privacy	It is available when **Authentication** or **Authentication and Privacy** is selected as security level. ● **Method** –At present, available methods include DES and None. ● **Password** - Enter a password for the selected method.
Add	Click it to add a new user profile.
Edit	🔧 - click it to modify the settings for the selected profile. 🗑 - click it to remove the selected entry.



Edit SNMP User=carrie

Group: s3

Security Level: ● No Auth ○ Auth ○ Auth & Privacy

Authentication Method:

Method ● None ○ MD5 ○ SHA

Password:

Privacy:

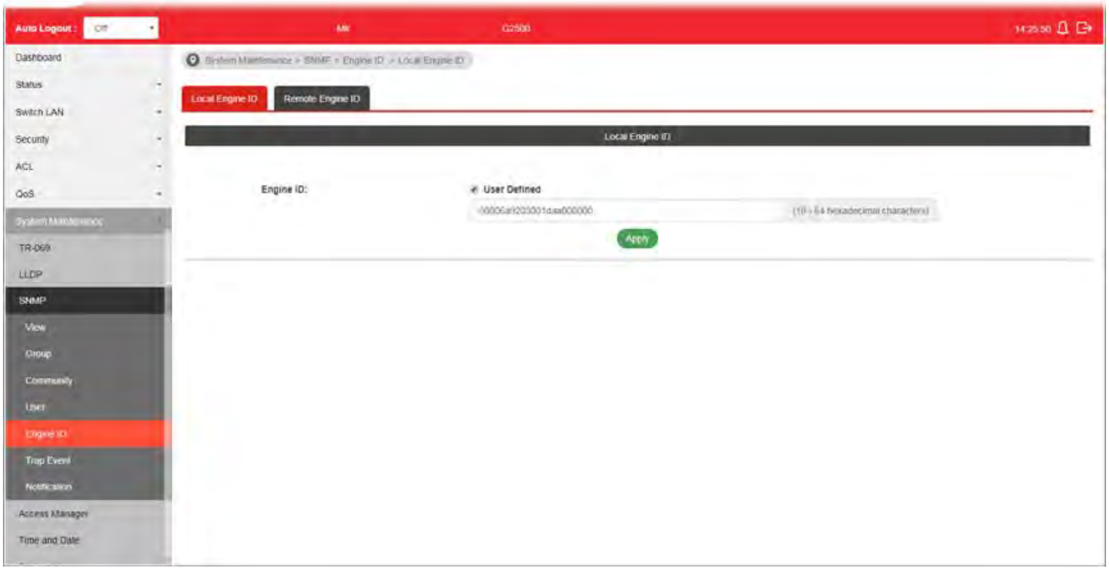
Method: ● None ○ DES

Password:

VI-3-5 Engine ID

VI-3-5-1 Local Engine ID

This page allows a user to configure and display SNMP local engine ID.



Engine ID: ☑ User Defined

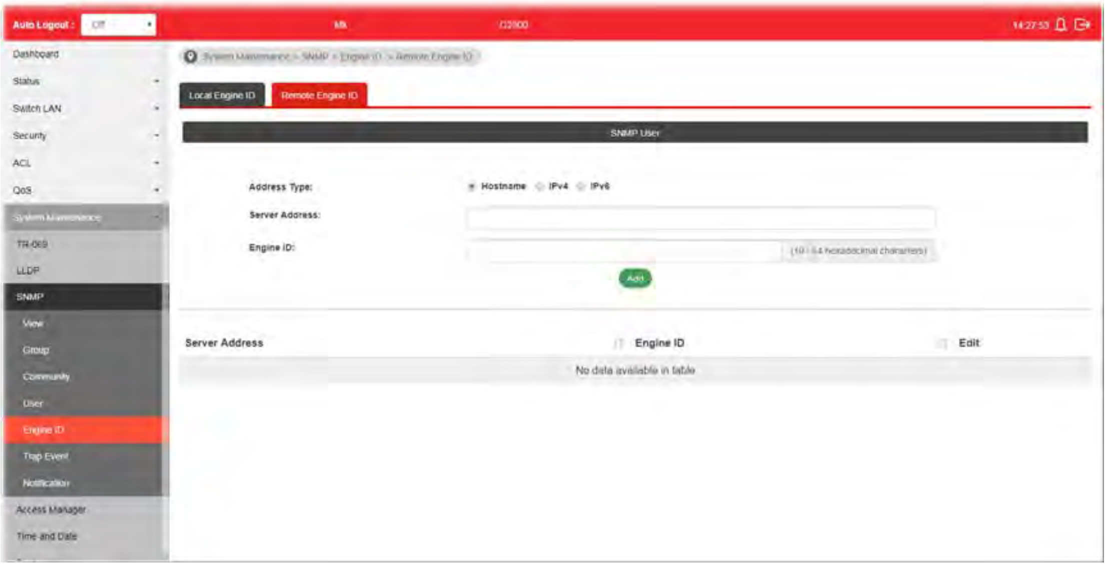
00006a9203001daa000000 (10 - 64 hexadecimal characters)

Available settings are explained as follows:

Item	Description
Engine ID	The user defined engine ID is range 10 to 64 hexadecimal characters, and the hexadecimal number must be divided by "2". **User Defined** - If it is checked, the local engine ID will be configured manually. If not, the default Engine ID which is made up of MAC and Enterprise ID will be used instead.
Apply	Apply the settings to the switch.

VI-3-5-2 Remote Engine ID

This page allows a user to configure and display SNMP remote engine ID.



Address Type: ● Hostname ○ IPv4 ○ IPv6

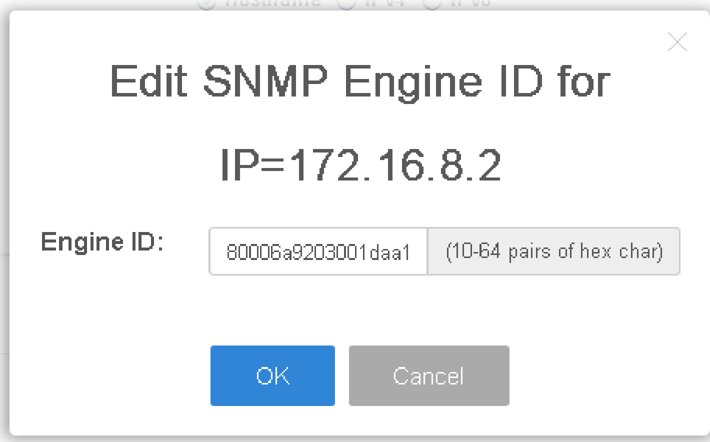
Server Address:

Engine ID: (10 - 64 hexadecimal characters)

Add

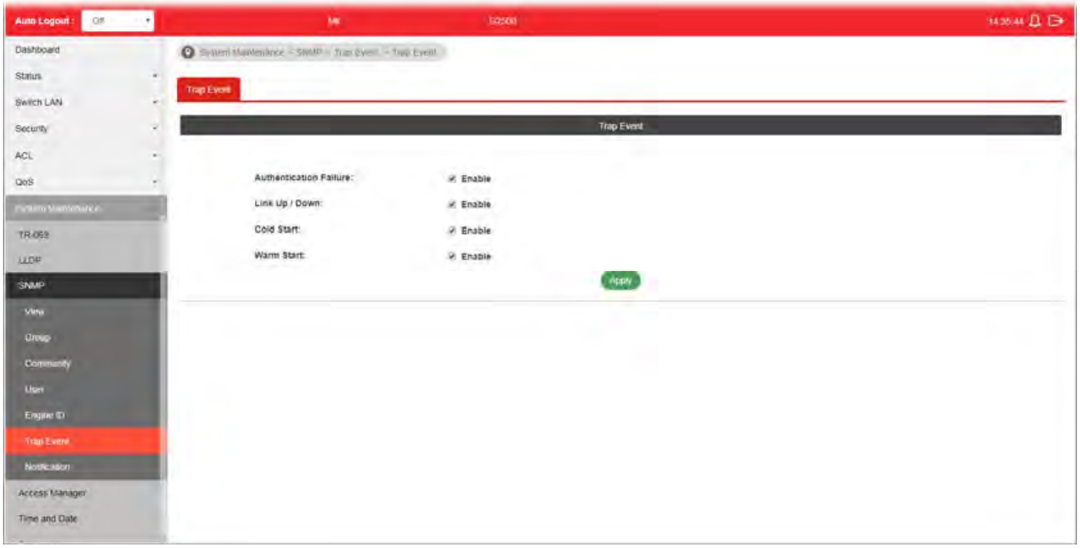
Server Address	Engine ID	Edit
No data available in table		

Available settings are explained as follows:

Item	Description
Address Type	Specify the address type for entering hostname or IPv4/IPv6 address.
Server Address	Enter the IP address or the host name of the SNMP server.
Engine ID	Specify the engine ID for remote SNMP server. The engine ID is range10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.
Add	Click it to create a new profile.
Edit	🔧 - click it to modify the settings for the selected server profile. 🗑 - click it to remove the selected entry.  Edit SNMP Engine ID for IP=172.16.8.2 Engine ID: 80006a9203001daa1 (10-64 pairs of hex char) OK Cancel

VI-3-6 Trap Event

This page allows a user to add or delete SNMP trap receiver IP address and community name.



Trap Event

Authentication Failure: ☑ Enable

Link Up / Down: ☑ Enable

Cold Start: ☑ Enable

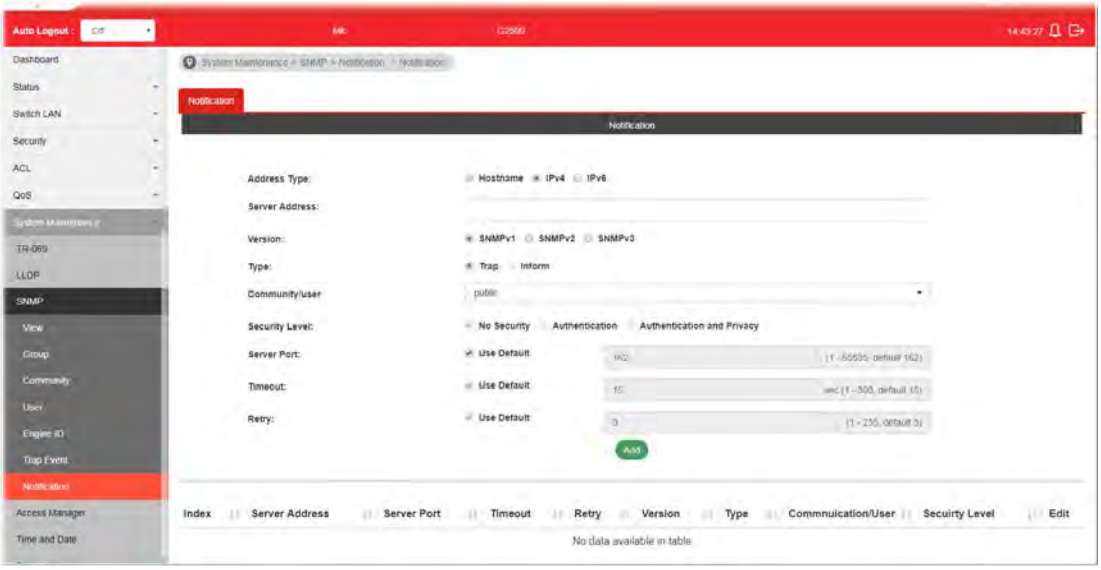
Warm Start: ☑ Enable

Available settings are explained as follows:

Item	Description
Authentication Failure	**Enable** – VigorSwtich will reboot when encountering authentication failure (including community not match or user password not match).
Link Up / Down	**Enable** – VigorSwtich will reboot while encountering port link up or down trap.
Cold Start	**Enable** – VigorSwtich will reboot while encountering user trap.
Warm Start	**Enable** – VigorSwtich will reboot while encountering power down trap.
Apply	Apply the settings to the switch.

VI-3-7 Notification

This page allows a user to configure a host to receive SNMPv1/v2/ve notification.



Notification

Address Type: ○ Hostname ● IPv4 ○ IPv6

Server Address:

Version: ● SNMPv1 ○ SNMPv2 ○ SNMPv3

Type: ● Trap ○ Inform

Community/user: public

Security Level: ○ No Security ○ Authentication ○ Authentication and Privacy

Server Port: ☑ Use Default 162 (1 - 65535, default 162)

Timeout: ☑ Use Default 15 sec (1 - 300, default 15)

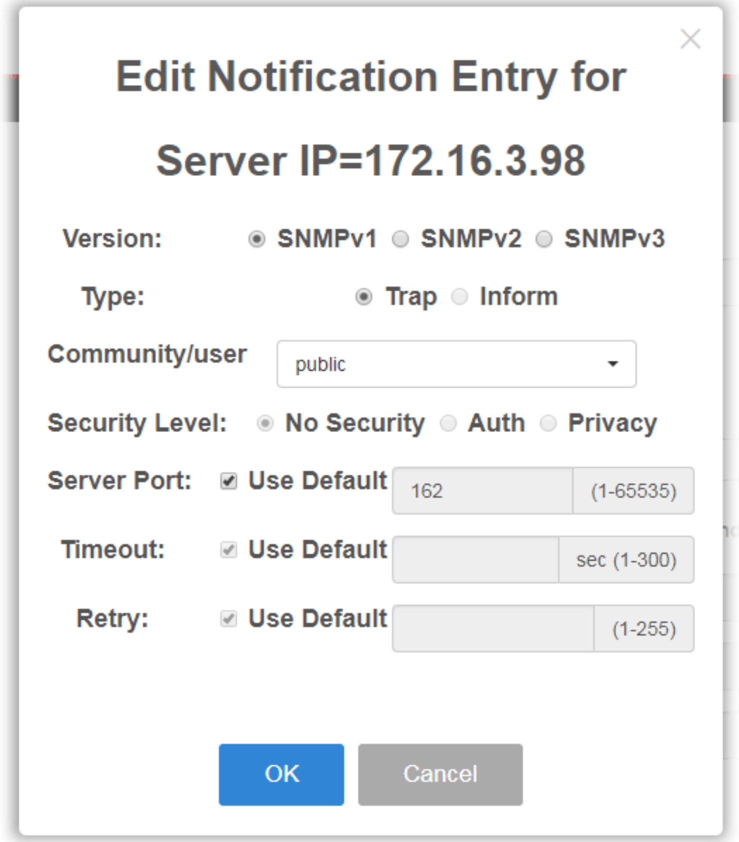
Retry: ☑ Use Default 3 (1 - 255, default 3)

Index	Server Address	Server Port	Timeout	Retry	Version	Type	Commnuication/User	Secuirty Level	Edit

No data available in table

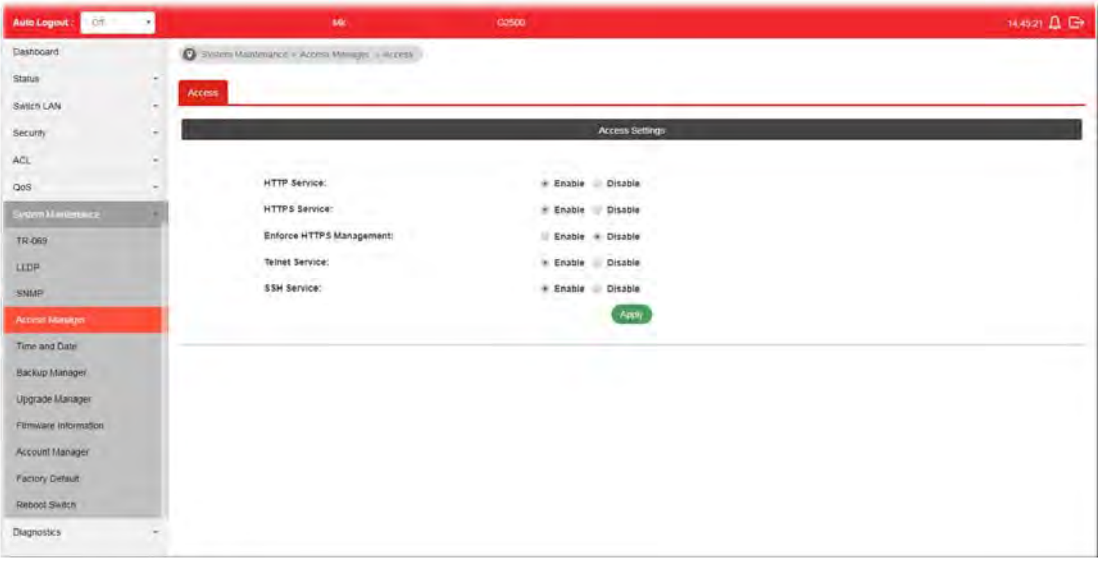
Available settings are explained as follows:

Item	Description
Address Type	Choose IPv4/IPv6/Hostname to specify IP address or the hostname of the SNMP trap recipients.
Server Address	Enter the IP address of SNMP server based on the address type selected above.
Version	Specify SNMP notification version (SNMPv1/v2/v3).
Type	Specify Notification Type. ● **Trap** -Send SNMP traps to the host. ● **Inform** - Send SNMP informs to the host. If it is used, Timeout and Retry also shall be defined.
Community/user	Use the drop down list to choose one of the community profiles.
Security Level	Specify SNMP security level for SNMP notification packet. It is available when SNMPv3 is selected. ● **No Security** – No authentication. ● **Authentication** – Authentication without encryption will be performed for packets. ● **Authentication and Privacy** – Authentication with encryption will be performed for packets.
Server Port	Specify the UDP port number for the recipient's server. **Use Default** – If it is checked, the default number (162) will be used automaticallty.
Timeout	Specify the SNMP informs timeout. It is available when **Inform** is selected as **Type**. **Use Default** - If it is checked, the default number (15) will be used automaticallty.
Retry	Specify the SNMP informs retry count. It is available when

	Inform is selected as Type. **Use Default** - If it is checked, the default number (3) will be used automaticallty.
Add	Click it to create a new notification profile.
Edit	🔧 - Click it to modify the settings for the selected server profile. 🗑 - Click it to remove the selected entry.  Edit Notification Entry for Server IP=172.16.3.98 Version: ● SNMPv1 ○ SNMPv2 ○ SNMPv3 Type: ● Trap ○ Inform Community/user: public Security Level: ● No Security ○ Auth ○ Privacy Server Port: ☑ Use Default 162 (1-65535) Timeout: ☑ Use Default sec (1-300) Retry: ☑ Use Default (1-255)

VI-4 Access Manager

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



HTTP Service: ● Enable ○ Disable
HTTPS Service: ● Enable ○ Disable
Enforce HTTPS Management: ○ Enable ● Disable
Telnet Service: ● Enable ○ Disable
SSH Service: ● Enable ○ Disable

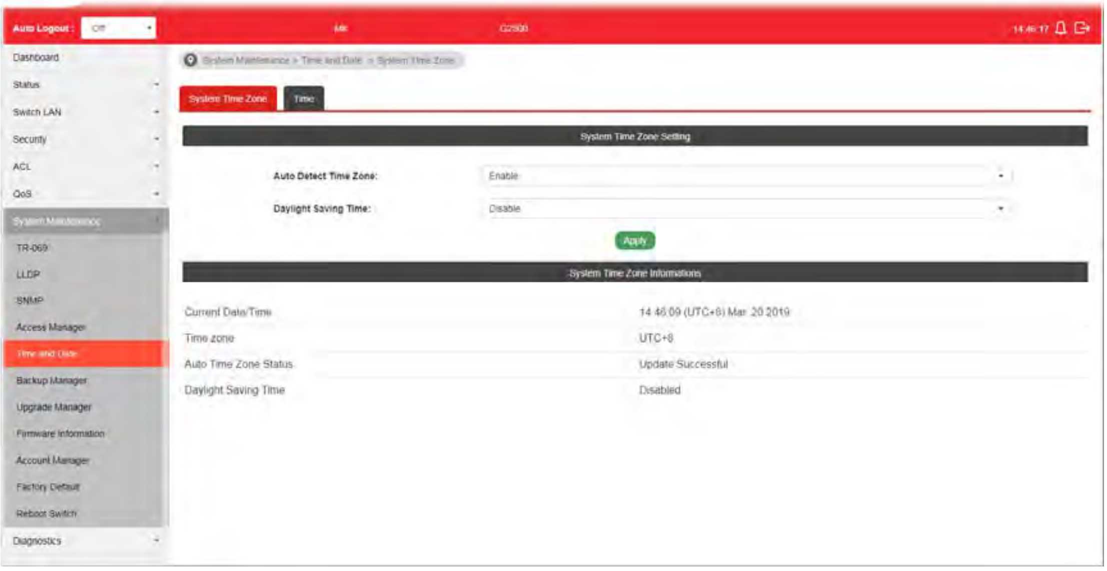
Available settings are explained as follows:

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.
Enforce HTTPS Management	**Enabled** - Users will be forced to access into the web user interface of VigorSwitch by HTTPS protocol.
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	Apply the settings to the switch.

VI-5 Time and Date

VI-5-1 System Time Zone

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



System Time Zone Setting

Auto Detect Time Zone: Enable

Daylight Saving Time: Disable

System Time Zone Informations

Current Date/Time	14:46:09 (UTC+8) Mar 20 2019
Time zone	UTC+8
Auto Time Zone Status	Update Successful
Daylight Saving Time	Disabled

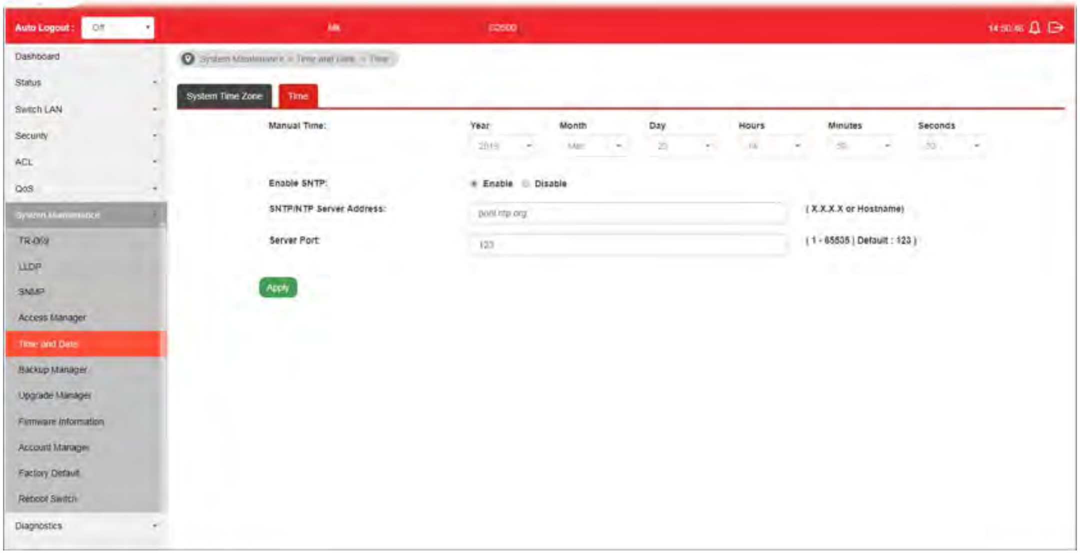
Available settings are explained as follows:

Item	Description
System Time Zone Setting	
Auto Detect Time Zone	Select **Enable** to make Vigor router detect the time zone that VigorSwitch is located automatically.
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 Offset	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	Apply the settings to the switch.
System Time Zone Informations	Display the status of system time zone.

VI-5-2 Time

This page allows a user to specify time and activate SNTP server manually.



Manual Time: Year 2019, Month Mar, Day 20, Hours 14, Minutes 58, Seconds 30

Enable SNTP: ● Enable ○ Disable

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

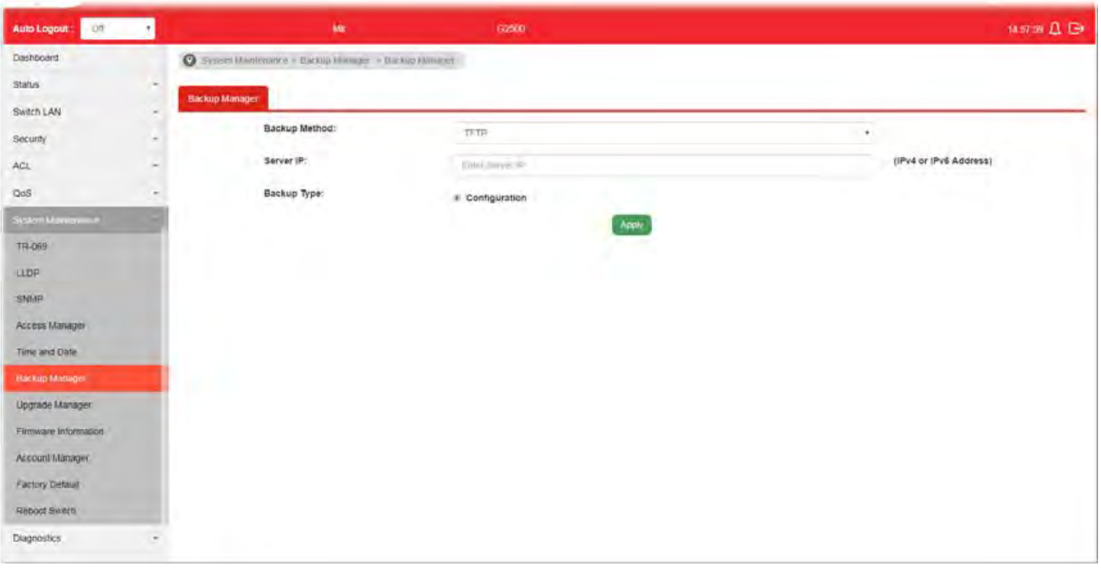
Server Port: 123 (1 - 65535 | Default : 123)

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	Apply the settings to the switch.

VI-6 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.



Backup Method: TFTP

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

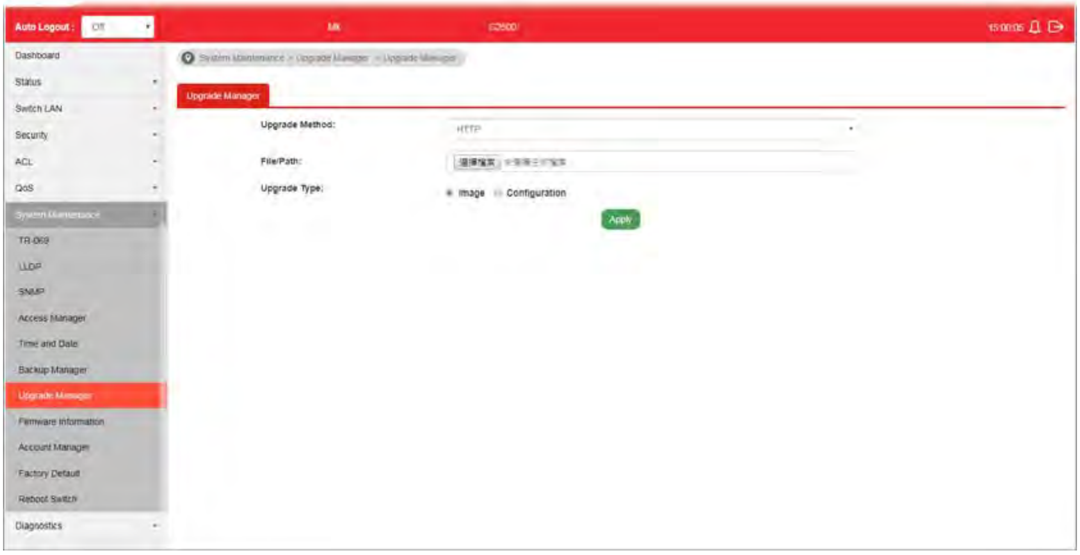
Backup Type: ● Configuration

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	Apply the settings to the switch.

VI-7 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 未選擇任何檔案

Upgrade Type: ● Image ○ Configuration

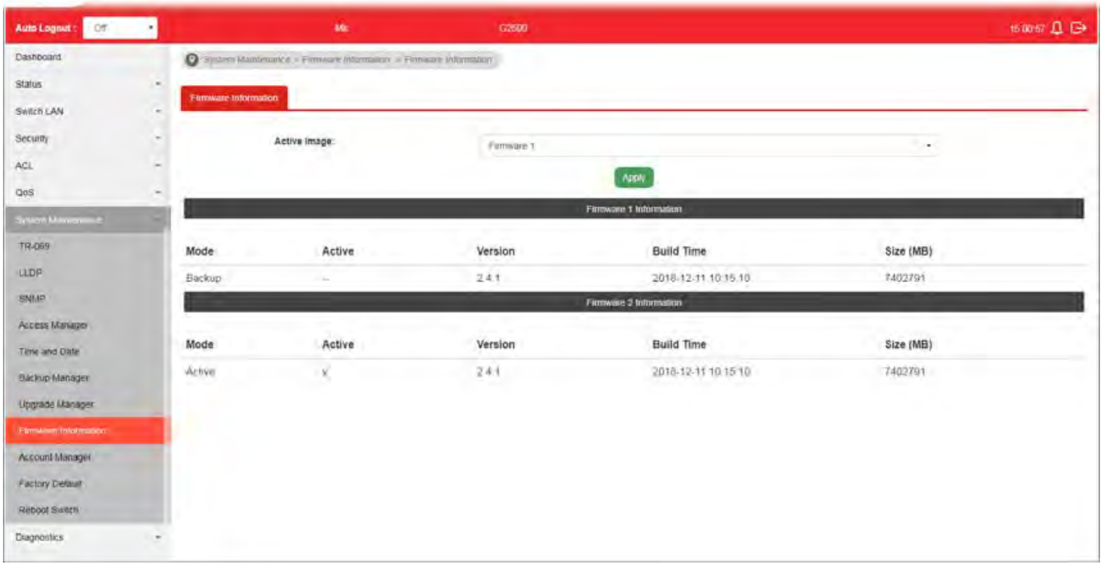
Apply

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	Apply the settings to the switch.

VI-8 Firmware Information

This page allows a user to choose the active firmware and backup firmware.



Active Image: Firmware 1

Firmware 1 Information

Mode	Active	Version	Build Time	Size (MB)
Backup	--	2.4.1	2018-12-11 10:15:10	7402791

Firmware 2 Information

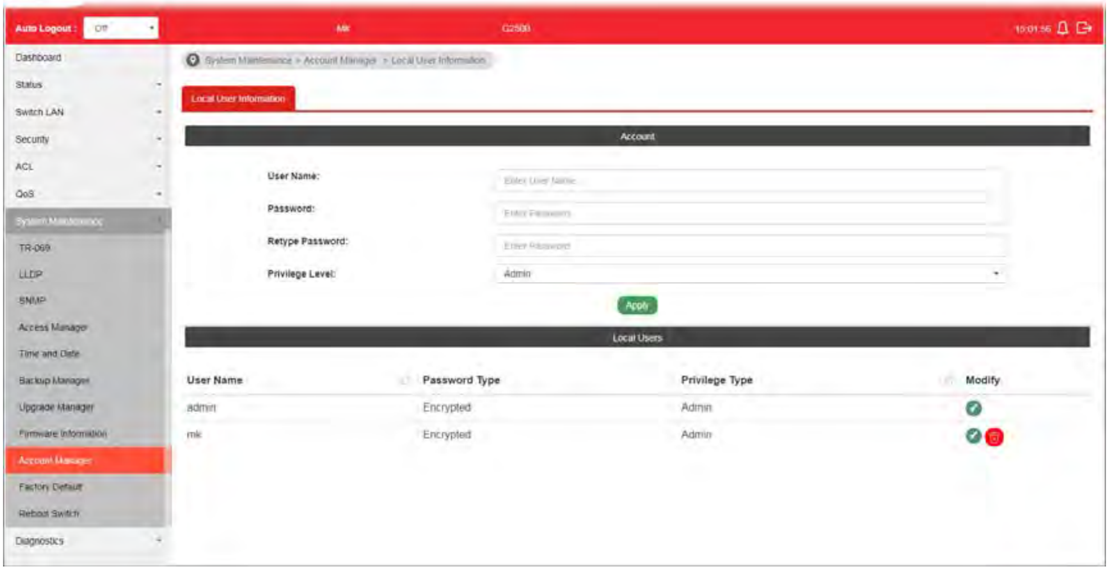
Mode	Active	Version	Build Time	Size (MB)
Active	v	2.4.1	2018-12-11 10:15:10	7402791

Available settings are explained as follows:

Item	Description
Active Image	There are two versions of firmware. Simply choose the one you want as primary firmware.
Apply	Apply the settings to the switch.
Firmware 1 Information **Firmware 2 Information**	● **Mode** - Display the mode (Active or Backup) of the firmware. ● **Active** –Display the status (in use or not) of the firmware. ● **Version** – Display the switch version. ● **Build Time** – Display the built time of the firmware. ● **Size (MB)** – Display the size of the firmware.

VI-9 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.



Auto Logout : Off

Account

User Name: Enter User Name

Password: Enter Password

Retype Password: Enter Password

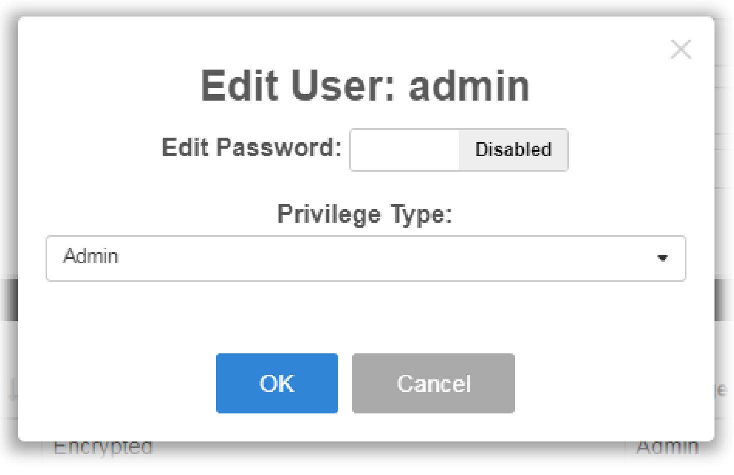
Privilege Level: Admin

Local Users

User Name	Password Type	Privilege Type	Modify
admin	Encrypted	Admin	✎
mk	Encrypted	Admin	✎ 🗑

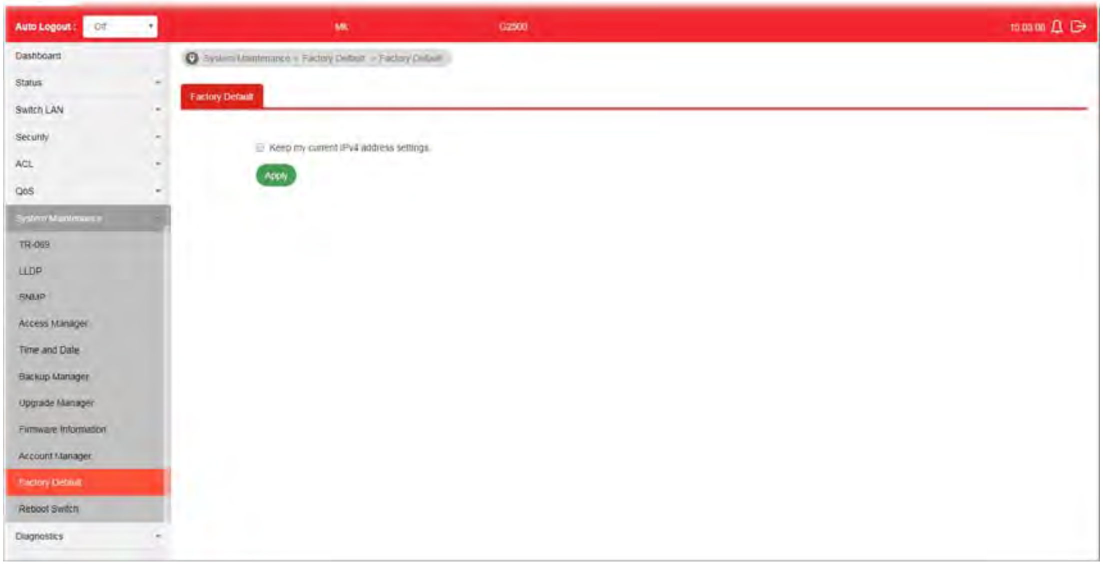
Available settings are explained as follows:

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	Apply the settings to the switch.
Delete	Remove the selected account.
Edit	🔧 - Click it to modify the settings for the selected user profile. 🗑 - Click it to remove the selected entry.

	 Edit User: admin Edit Password: Disabled Privilege Type: Admin

VI-10 Factory Default

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

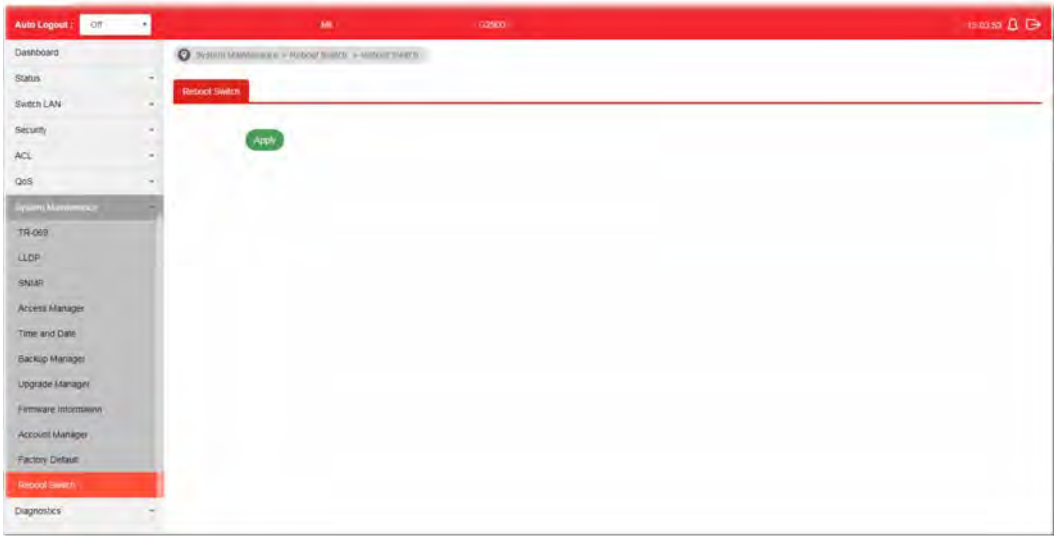


□ Keep my current IPv4 address settings.

If **Keep my current IPv4 address setting**s is checked, after clicking Apply, the original configuration for IP address will be kept.

VI-11 Reboot Switch

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

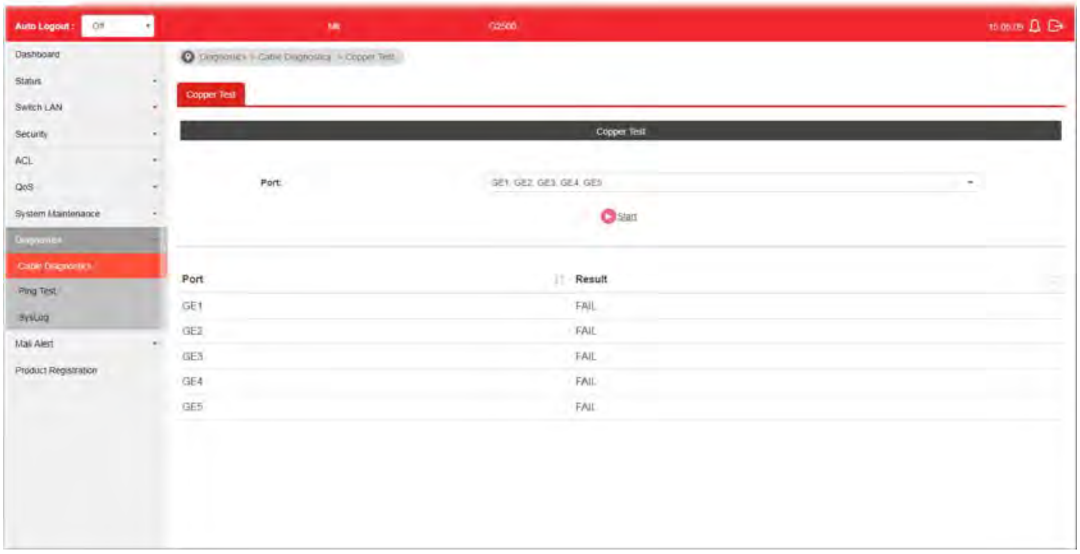


This page is left blank.

Part VII Diagnostics

VII-1 Cable Diagnostics

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



Copper Test

Port: GE1, GE2, GE3, GE4, GE5

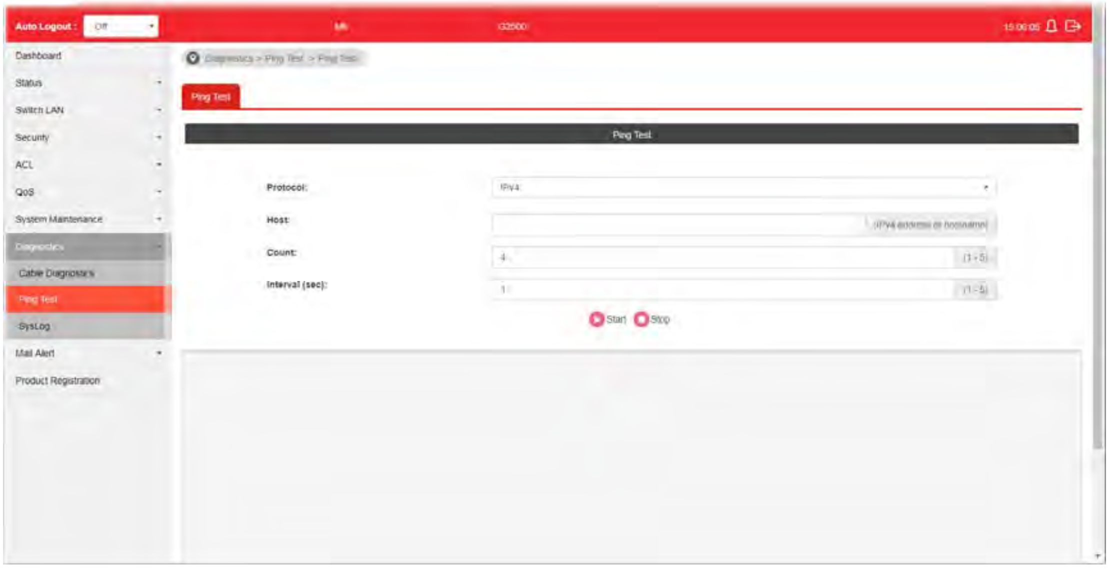
Port	Result
GE1	FAIL
GE2	FAIL
GE3	FAIL
GE4	FAIL
GE5	FAIL

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.



Protocol: IPv4

Host: (IPv4 address or hostname)

Count: 4 (1 - 5)

Interval (sec): 1 (1 - 5)

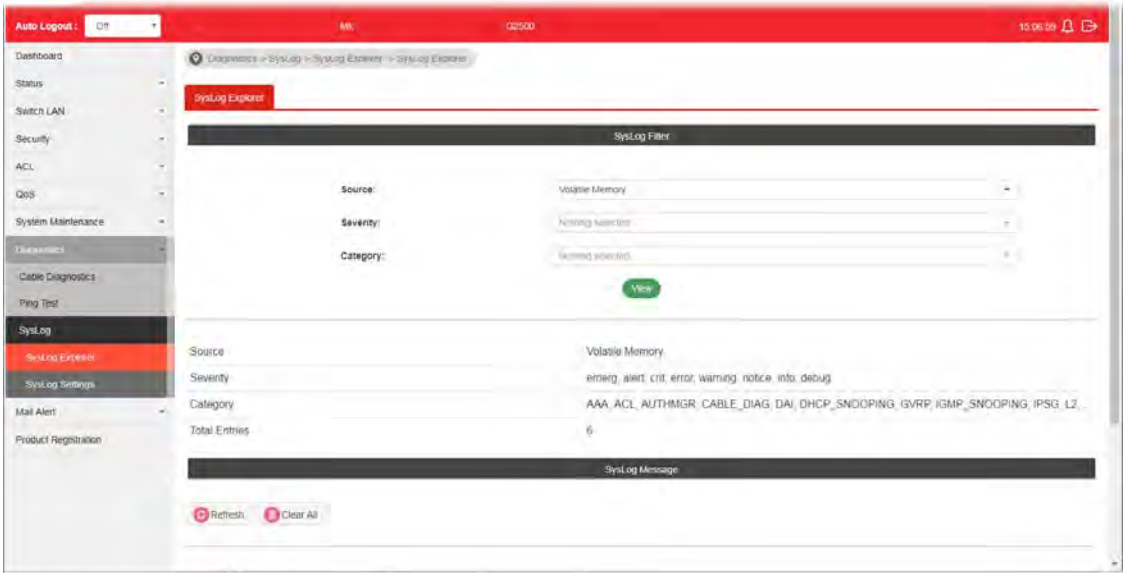
Available settings are explained as follows:

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, IPSG, L2,...
Total Entries	6

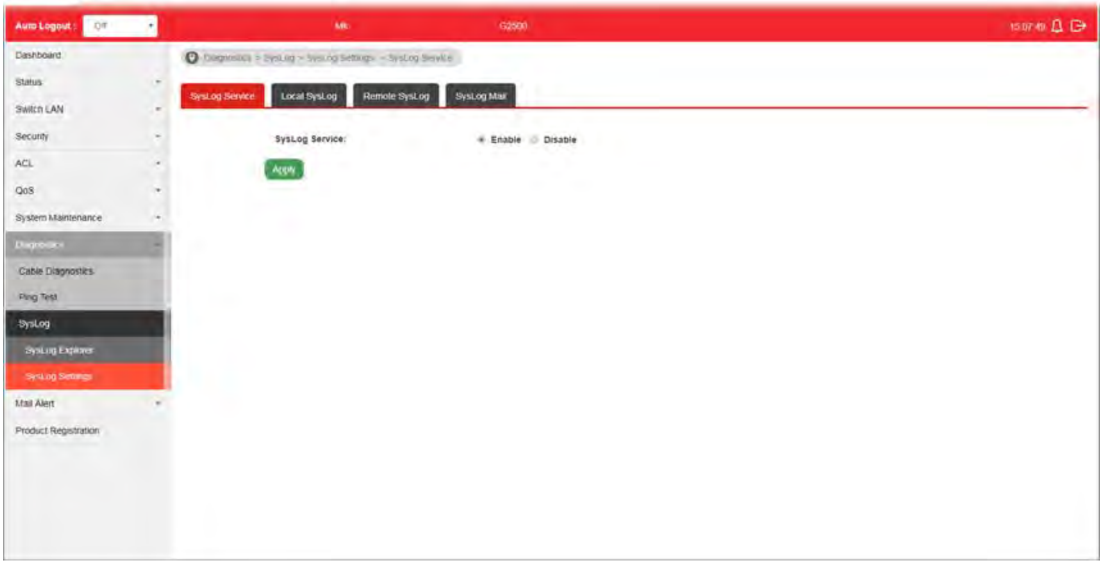
Available settings are explained as follows:

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.



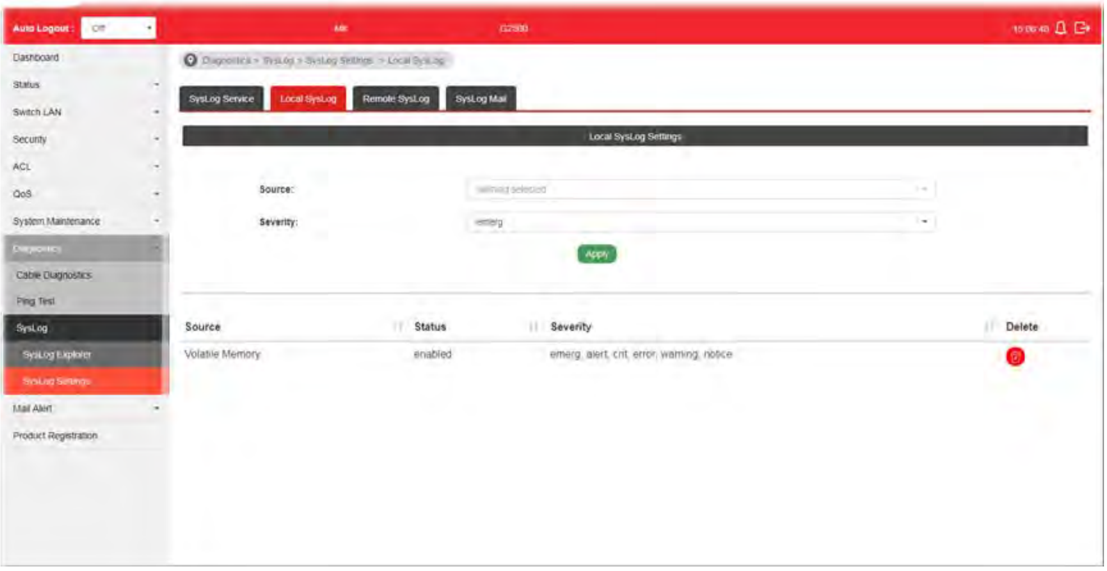
SysLog Service: ● Enable ○ Disable

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	Apply the settings to the switch.

VII-3-2-2 Local SysLog

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



Local SysLog Settings

Source: nothing selected

Severity: emerg

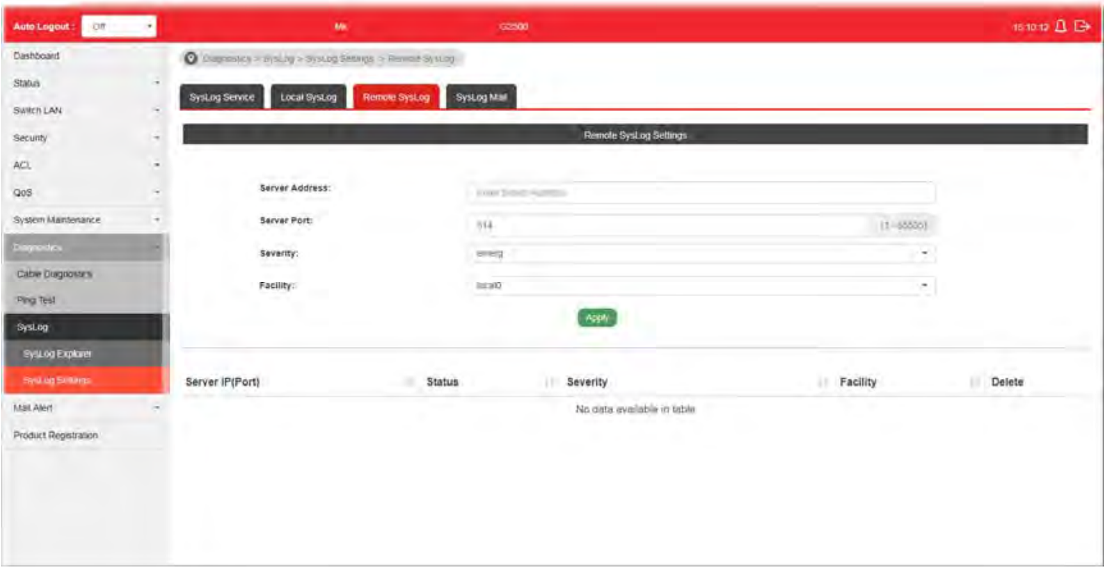
Source	Status	Severity	Delete
Volatile Memory	enabled	emerg, alert, crit, error, warning, notice	

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	Apply the settings 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

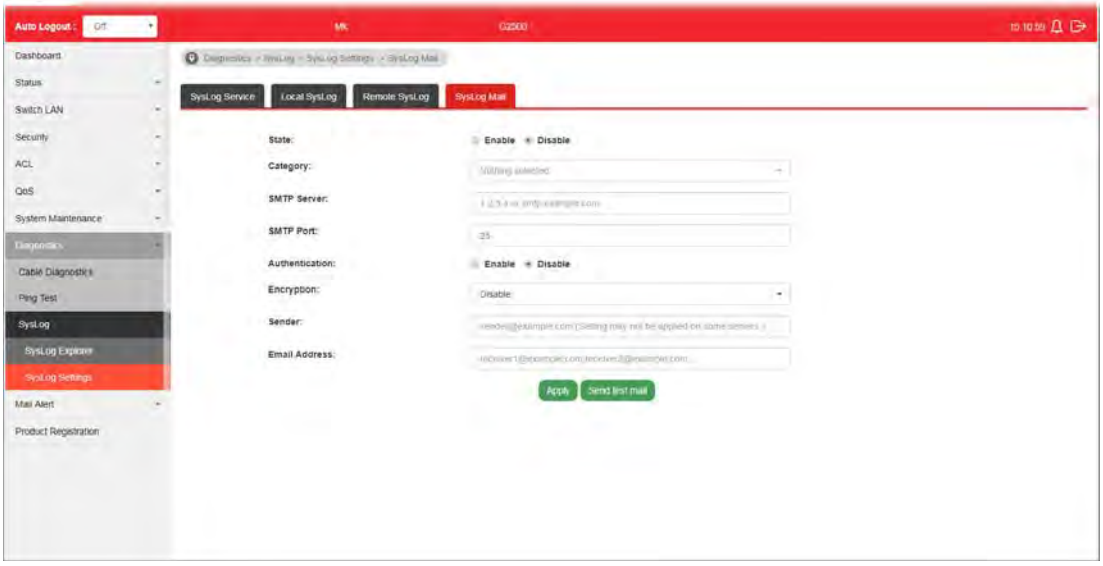
Server IP(Port)	Status	Severity	Facility	Delete
No data available in table				

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	Apply the settings to the switch.
Delete	Remove specific remote syslog entry.

VII-3-2-4 SysLog Mail

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.



State: ○ Enable ● Disable

Category: Nothing selected

SMTP Server: 1.2.3.4 or smtp.example.com

SMTP Port: 25

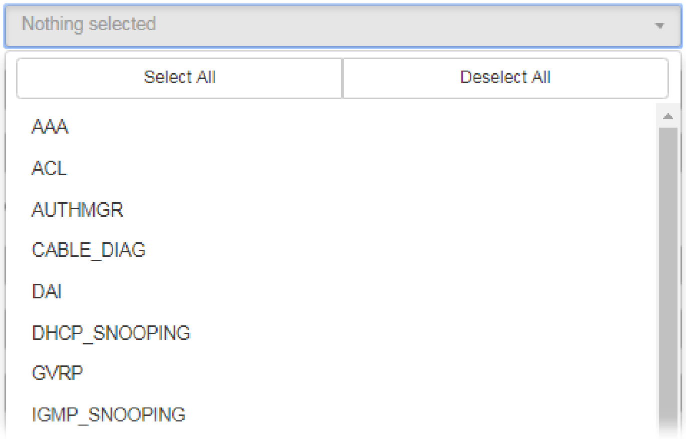
Authentication: ○ Enable ● Disable

Encryption: Disable

Sender: sender@example.com (Setting may not be applied on some servers.)

Email Address: receiver1@example.com,receiver2@example.com

Available settings are explained as follows:

Item	Description
State	**Enable** - Enable the function of Syslog Mail. **Disable** - Disable the function of Syslog Mail.
Category	Vigor sytem will send the e-mail related to the selected feature(s) to the recipient.  Nothing selected Select All Deselect All AAA ACL AUTHMGR CABLE_DIAG DAI DHCP_SNOOPING GVRP IGMP_SNOOPING
SMTP Server	Enter IP address or URL of the SMTP server.
SMTP Port	Enter the port number for the SMTP server.
Authentication	**Enable** - Click it to enable authentication mechanism. ● **User Name** - Enter a user name for authentication. ● **Password** - Enter a password for authentication.
Encryption	After enabling Authentication, choose one of the encryption servers for data encryption. ● **StartTLS** - The mail will be encrypted with StartTLS. ● **SSL/TLS** - The mail will be encrypted with SSL/TLS.

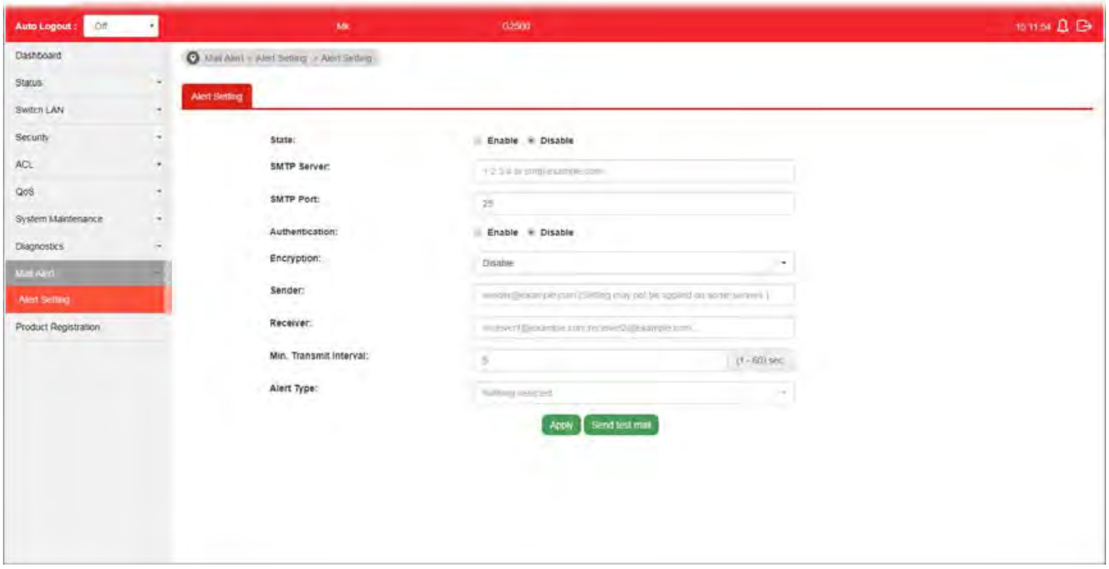
	● **Disable** - The mail sent out will not be encrypted.
Sender	Enter the email address which will send the syslog mail out.
Email Address	Enter the email address which will receive the syslog mail.
Apply	Apply the settings to the switch.
Send test mail	After clicking this button, VigorSwitch system will send a test mail to the recipient.

This page is left blank.

Part VIII Mail Alert

VIII-1 Alert Setting

This page allows a user to configure settings for VigorSwitch to send alert mail when encountering certain sitaution.



State: ○ Enable ● Disable

SMTP Server: 1.2.3.4 or smtp.example.com

SMTP Port: 25

Authentication: ○ Enable ● Disable

Encryption: Disable

Sender: sender@example.com (Setting may not be applied on some servers)

Receiver: receiver1@example.com,receiver2@example.com...

Min. Transmit Interval: 5 (1 - 60) sec

Alert Type: Nothing selected

Available settings are explained as follows:

Item	Description
State	● **Enable** - Click it to enable the mail alert function. ● **Disable** - Click it to disable the mail alert funciton.
SMTP Server	Enter IP address or URL of the SMTP server.
SMTP Port	Enter the port number for the SMTP server.
Authentication	**Enable** - Click it to enable authentication mechanism. ● **User Name** - Enter a user name for authentication. ● **Password** - Enter a password for authentication.
Encryption	After enabling Authentication, choose one of the encryption servers for data encryption. ● **StartTLS** - The mail will be encrypted with StartTLS. ● **SSL/TLS** - The mail will be encrypted with SSL/TLS. ● **Disable** - The mail sent out will not be encrypted.
Sender	Enter the email address which will send the alert mail out.
Receiver	Enter the email address which will receive the alert mail.
Min. Transmit Interval	Set a time interval for VigorSwitch system to send an alert out from the specified sender.
Alert Type	Specify the condition(s) for VigorSwitch system to send an alert out. ● Port Link Status ● Port Link Speed ● System Restarted
Apply	Apply the settings to the switch.

Send test mail	After clicking this button, VigorSwitch system will send a test mail to the recipient.

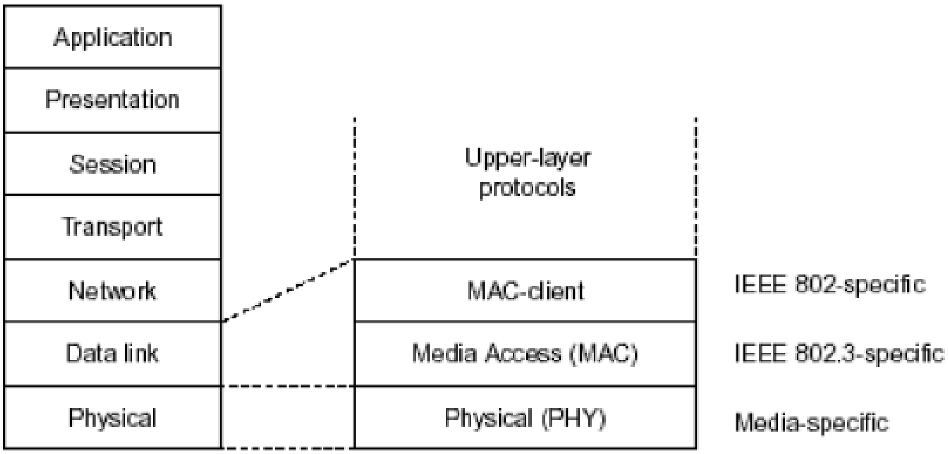
This page is left blank.

Appendix: Reference

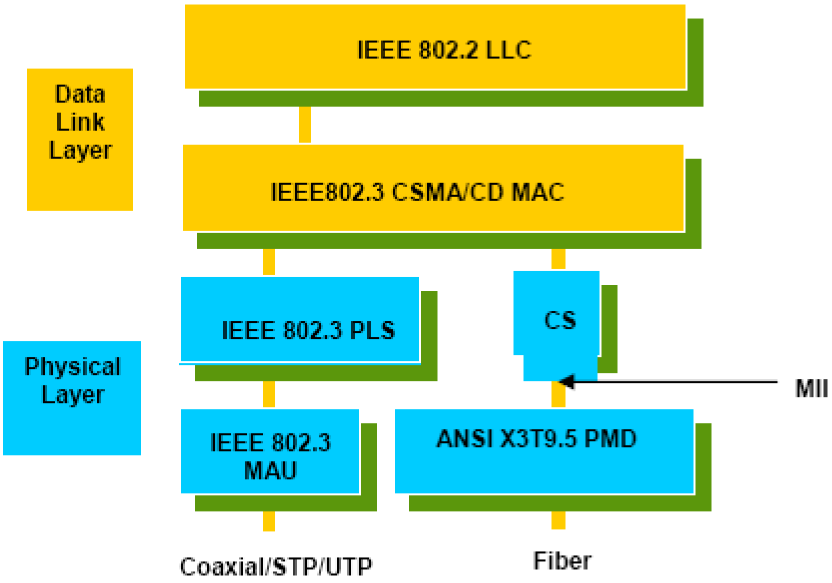
This chapter will tell you the basic concept of features to manage this switch and how they work.

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.

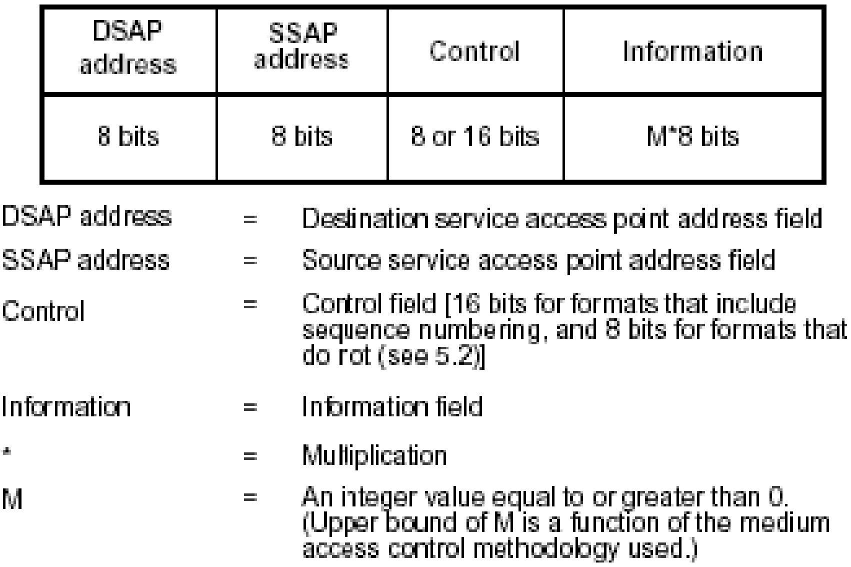


This above diagram shows the Ethernet architecture, LLC sub-layer and MAC sub-layer, which are responded to the Data Link layer, and transceivers, which are responded to the Physical layer in OSI model. In this section, we are mainly describing the MAC sub-layer.

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

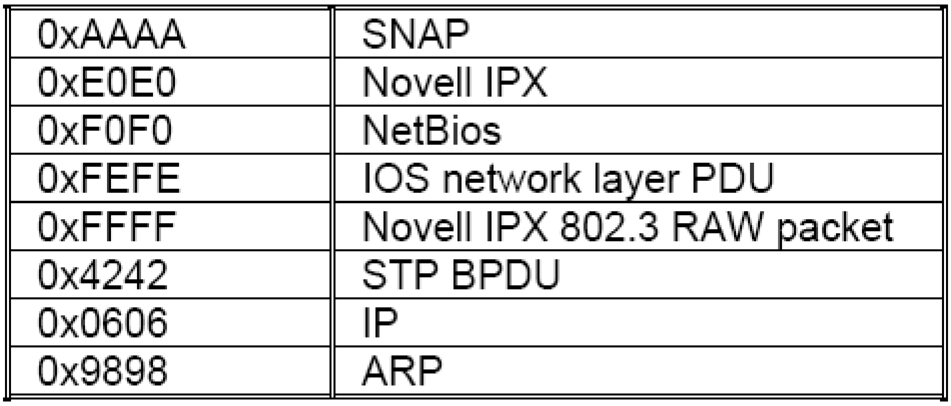
Control = Control field [16 bits for formats that include sequence numbering, and 8 bits for formats that do rot (see 5.2)]

Information = Information field

* = Mulliplication

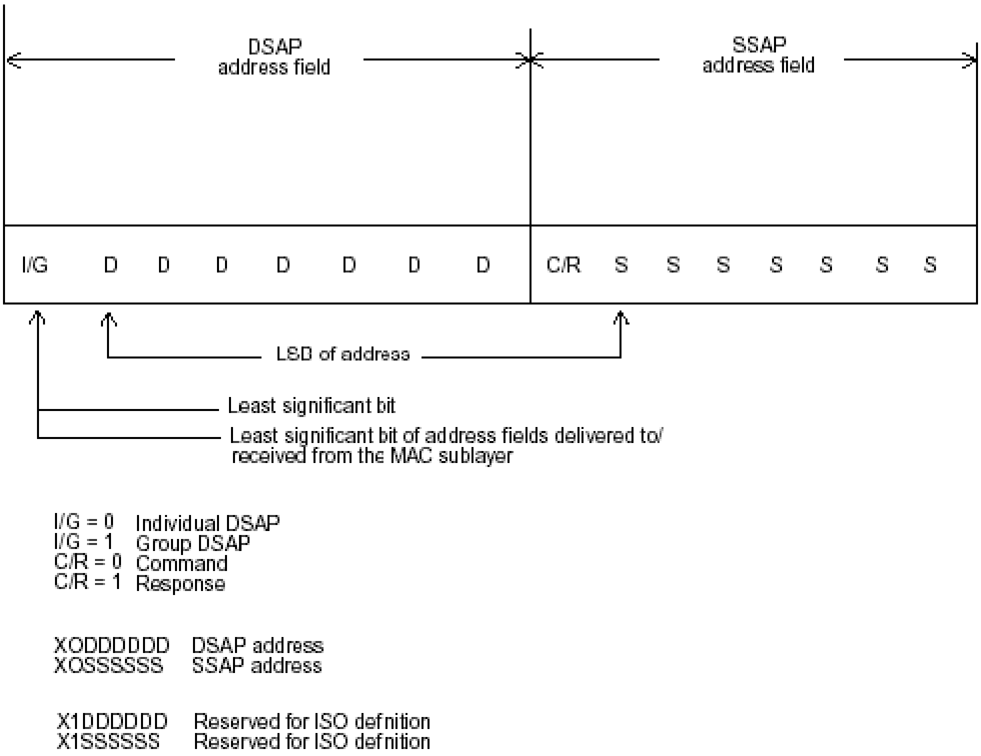
M = An integer value equal to or greater than 0. (Upper bound of M is a function of the medium access control methodology used.)

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.

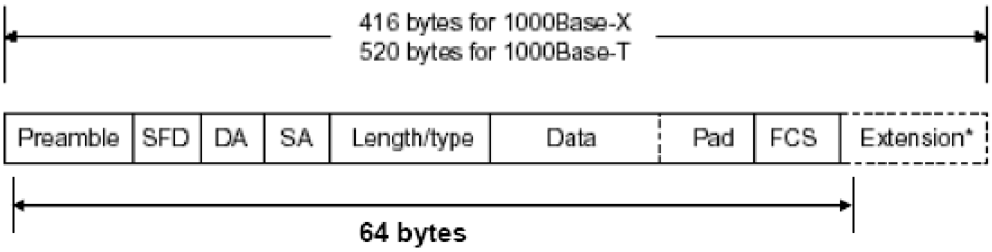
1. MAC will assemble the frame. First, the preamble and Start-of-Frame delimiter will be put in the fields of PRE and SFD, followed DA, SA, tag ID if tagged VLAN is applied, Ethertype or the value of the data length, and payload data field, and finally put the FCS data in order into the responded fields.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

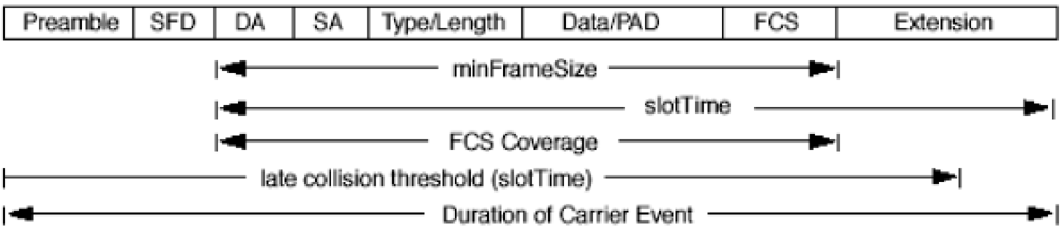
As the transmission of a MAC frame with the half-duplex operation exists only in the same collision domain, the carrier signal needs to spend time to travel to reach the targeted device. For two most-distant devices in the same collision domain, when one sends the frame first, and the second sends the 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.

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

where

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

Frame Reception

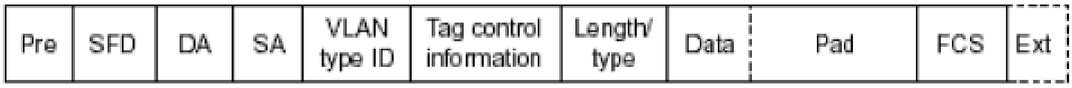
In essence, the frame reception is the same in both operations of half duplex and full duplex, except that full-duplex operation uses two buffers to transmit and receive the frame independently. The receiving node always "listens" if there is traffic running over the medium when it is not receiving a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

For a received frame, the MAC will check:

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

What if a VLAN tagging is applied?

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



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

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

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

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