VigorSwitch PX2060 / X2060

L2+ Managed Switch

User's Guide

Version: 1.0

Firmware Version: V2.9.9

Date: 17 June 2026

Intellectual Property Rights (IPR) Information

Copyrights

Trademarks

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows 8, 10, 11 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.

Safety Instructions and Approval

Safety Instructions

- Read the installation guide thoroughly before you set up the device.
- The switch is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the switch yourself.
- Do not place the switch in a damp or humid place, e.g. a bathroom.
- The switch should be used in a sheltered area, within a temperature range of 0 to +50 Celsius.
- Do not expose the switch to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.
- Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards.
- Keep the package out of reach of children.
- When you want to dispose of the modem, please follow local regulations on conservation of the environment.

Warranty

We warrant to the original end user (purchaser) that the switch will be free from any defects in workmanship or materials for a period of two (2) years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary tore-store the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

Be a Registered Owner

Web registration is preferred. You can register your Vigor router via https://myvigor.draytek.com.

Firmware & Tools Updates

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

https://www.draytek.com

Table of Contents

Chapter I Introduction

I-1 Introduction

This is a generic International version of the user guide. Specification, compatibility and features vary by region. For specific user guides suitable for your region or product, please contact local distributor.

I-1-1 Key Features

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

Below shows key features of this device:

QoS

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

VLAN

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

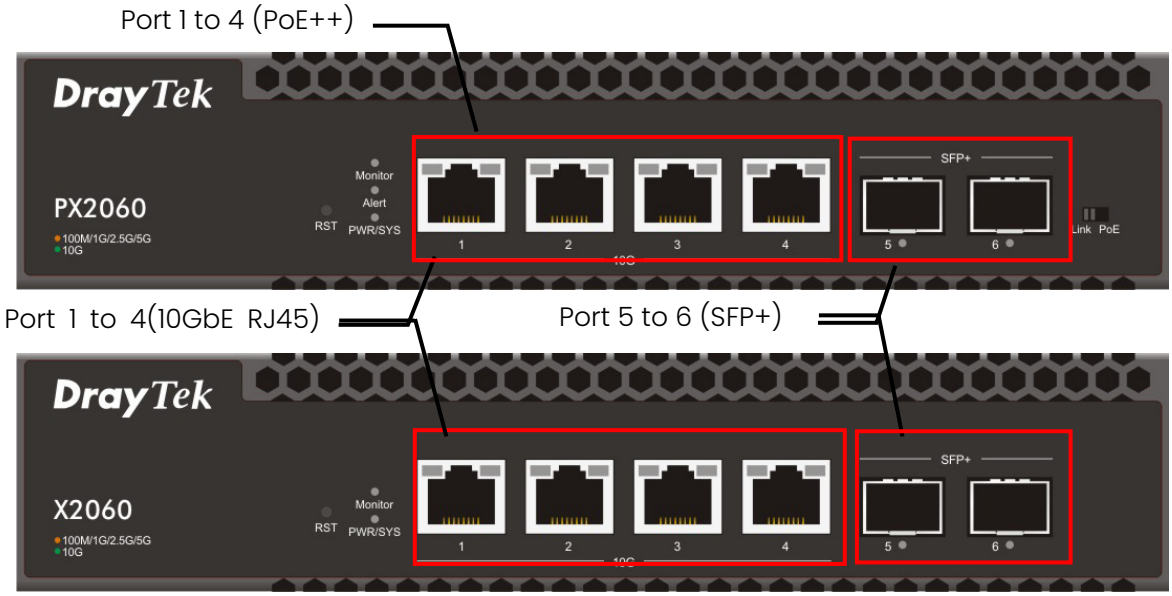
Port Trunking

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

Power Saving

The Power saving using the IEEE 802.3az, Energy-Efficient Ethernet to detect the client idle and cable length automatically and provides the different power. It could efficient to save the switch power and reduce the power consumption.

I-1-2 LED Indicators and Connectors



LED	Status	Explanation
Monitor	On (Red)	An alert for system failure due to overheating or wrong voltage.
	Off	The device is in normal condition and running normally.
Alert (for PX2060)	Blinking (Green)	The power is over (>) 80% watts PoE power budget.
	Off	The power is under (<) 80% watts PoE power budget.
PWR/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.
Port 1 ~ 4 (PoE, for PX2060)	On (Amber)	The port is supplied with PoE power.
	Off	No PoE power is supplied on the port.
Port 1 ~ 4 (GbE RJ45)	On (Green)	The device is connected with 10Gbps.
	On (Amber)	The device is connected with 5G/2.5G/1G/ 100Mbps.
	Blinking	The system is sending or receiving data through the port.
	Off	The port is disconnected or the link is failed.
Port 5 ~6 (SFP+)	On (Amber)	The device is connected with 1Gbps.
	On (Green)	The device is connected with 10Gbps.
	Blinking	The system is sending or receiving data through the port.
	Off	The port is disconnected or the link is failed.

Interface	Description
RST	Factory reset button. Press it to reboot the system. (<5 seconds)

	Press it to reset the system with factory default settings. (>5 seconds)
Port 1 ~ 4 (10GbE RJ45)	Port 1 to Port 4 can be used for Ethernet connection and PoE connection, depending on the device connected.
Port 1 ~ 4 (PoE 802.3af/at/bt, for PX2060)	
Port 5 ~ 6 (SFP+)	Port 5 to Port 6 are used for fiber connection.

Note

The following limitation is suitable for VigorSwitch PX2060

Power Output --

- IEEE 802.3bt Type 3 Max. 60W Output Supported

PoE Power Budget --

- 140 Watts (Max)

I-2 Installation

Before starting to configure the switch, you have to connect your devices correctly.

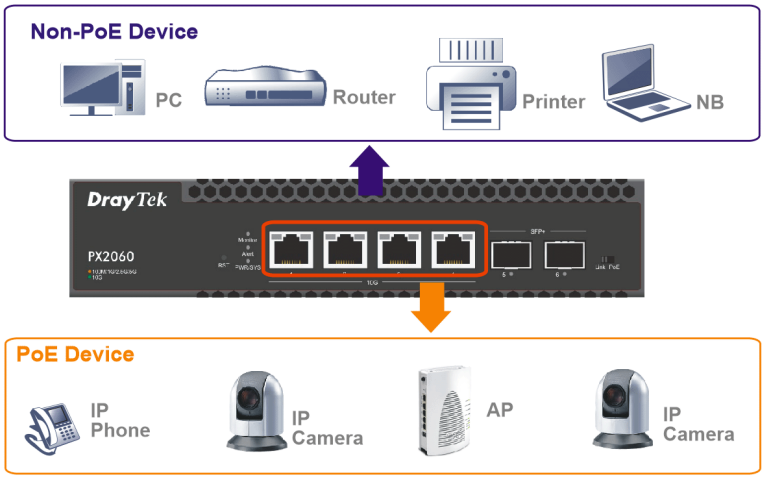
Note:

For the sake of personal safety, only trained and qualified personnel should install this device.

I-2-1 Network Connection

Allowance for connecting Non-PoE devices and PoE devices

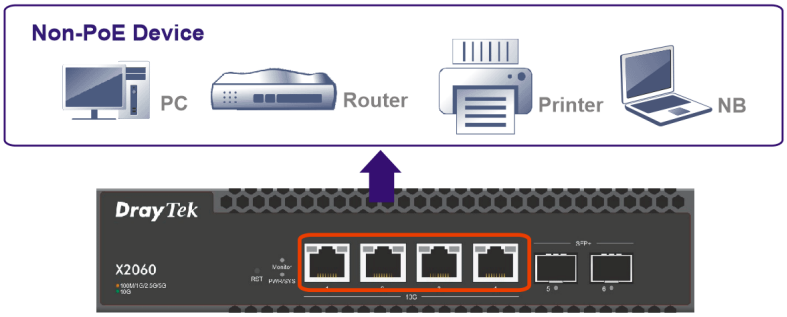
- Use a Category 5e, 6, 6a, or 7 twisted-pair cable to connect a PoE device to ports 1–4 on this switch. Category 5e and 6 cables support 100M, 1G, 2.5G, and 5G transmission speeds, while Category 6a and 7 cables support 10G transmission speeds.
- The switch will supply power to PoE Device over the twisted-pair cable.
- Please note that Power Device must comply with IEEE 802.3af/at.
- Other PCs, servers and network devices can be connected to the switch using a standard 'straight through' twisted pair cable.



Allowance for connecting Non-PoE devices

- Use the Ethernet cable(s) to connect None-PoE devices to the Vigor switch.
- All device ports are in the same local area network.

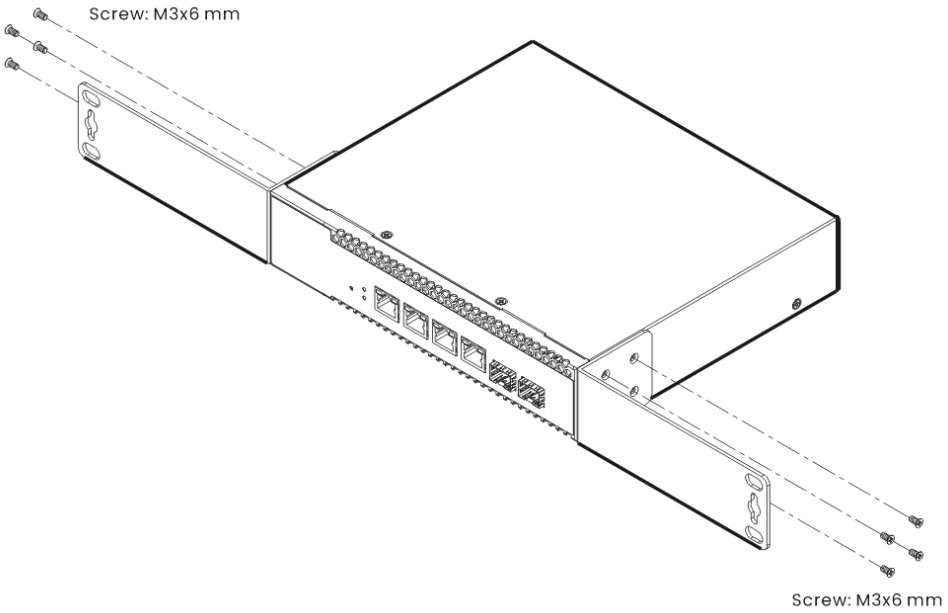
Here, we take VigorSwitch X2060 as an example.



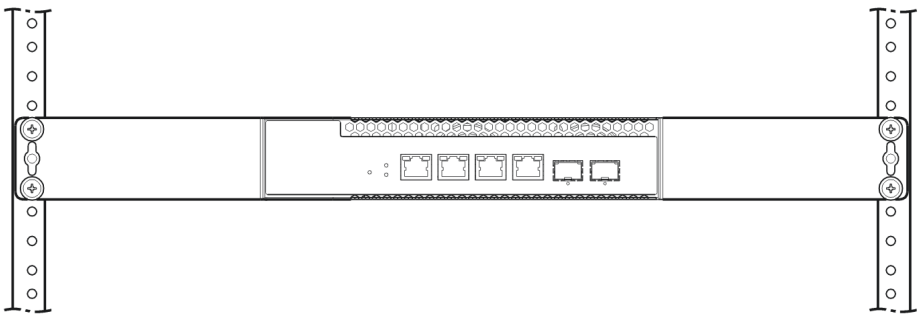
I-2-2 Single-Switch Rack-Mount Installation

The switch can be installed easily by using **rack mount kit**.

1. Fasten the rack mount kit on both sides of the VigorSwitch using specific screws.



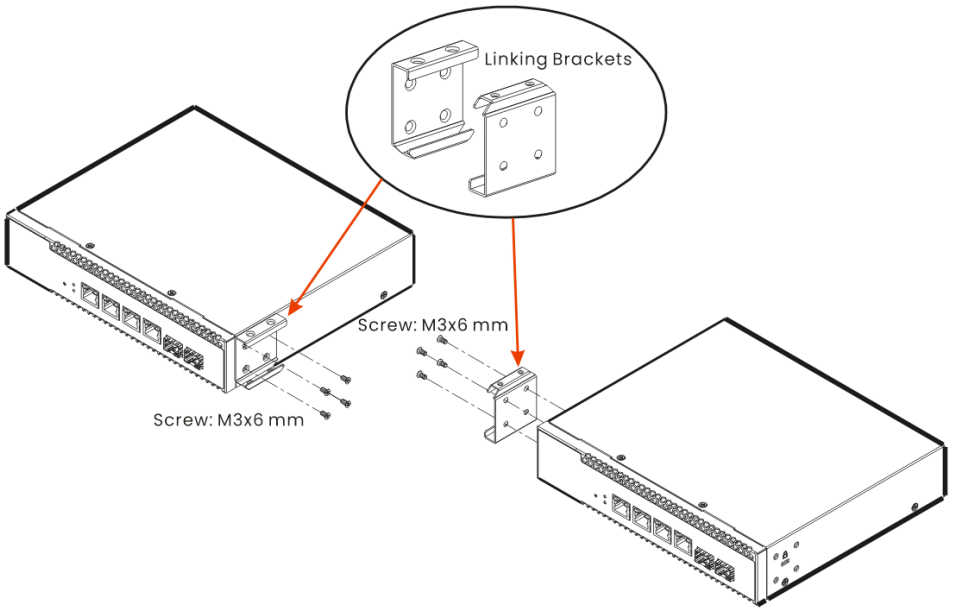
2. Then, install the VigorSwitch (with rack mount kit) on the 19-inch chassis by using other four screws.



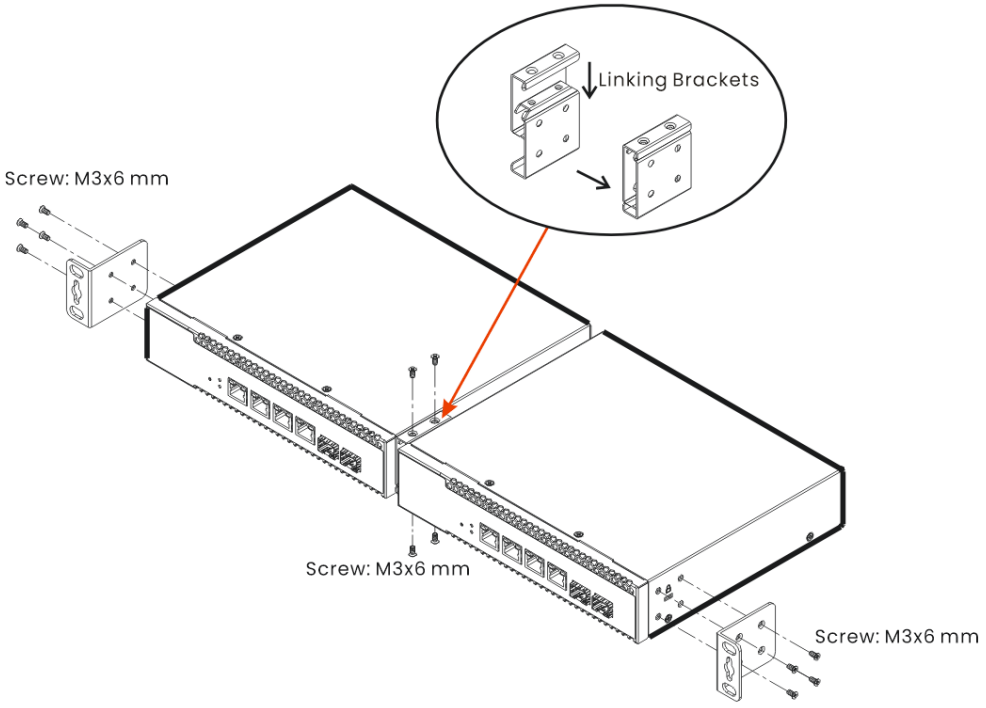
I-2-2 Single-Switch Rack-Mount Installation

Two switches can be installed side by side on the chassis. Please install them as follows:

1. Secure the switch linking brackets to the sides of both switches.



2. Assemble the switch linking brackets and tighten the screws. Then install the short rack mount kit and tighten the screws.



Now, both switches have been mounted to the chassis firmly.

Note that the linking brackets and the short rack mount kit are optional. Please contact your dealer to purchase them if needed.

I-2-3 Typical Applications

The VigorSwitch implements many 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:

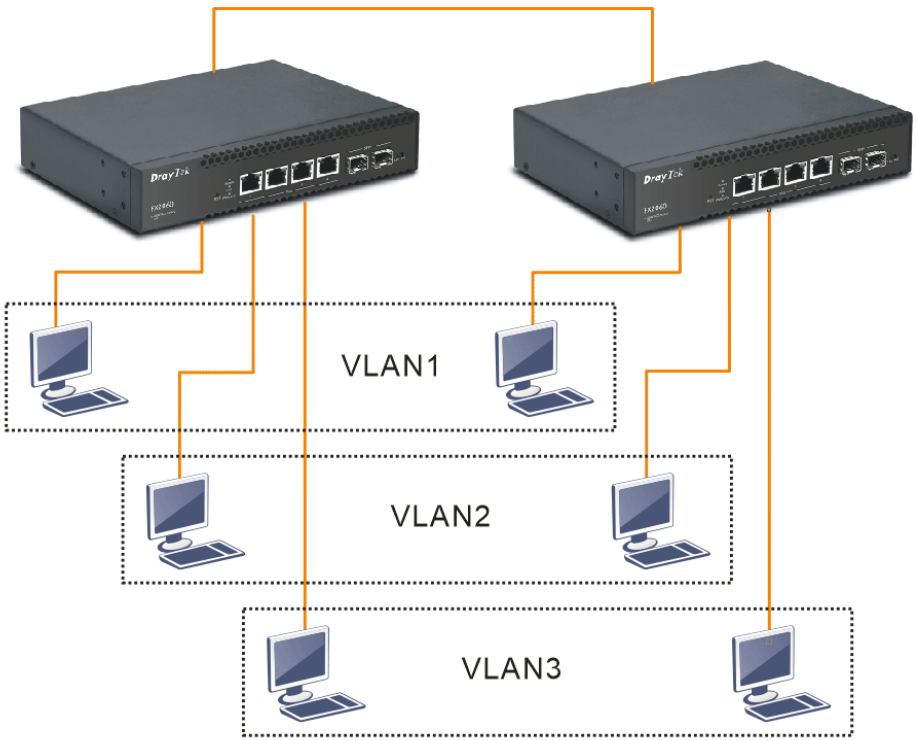
Case 1: All switch ports are in the same local area network.

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.

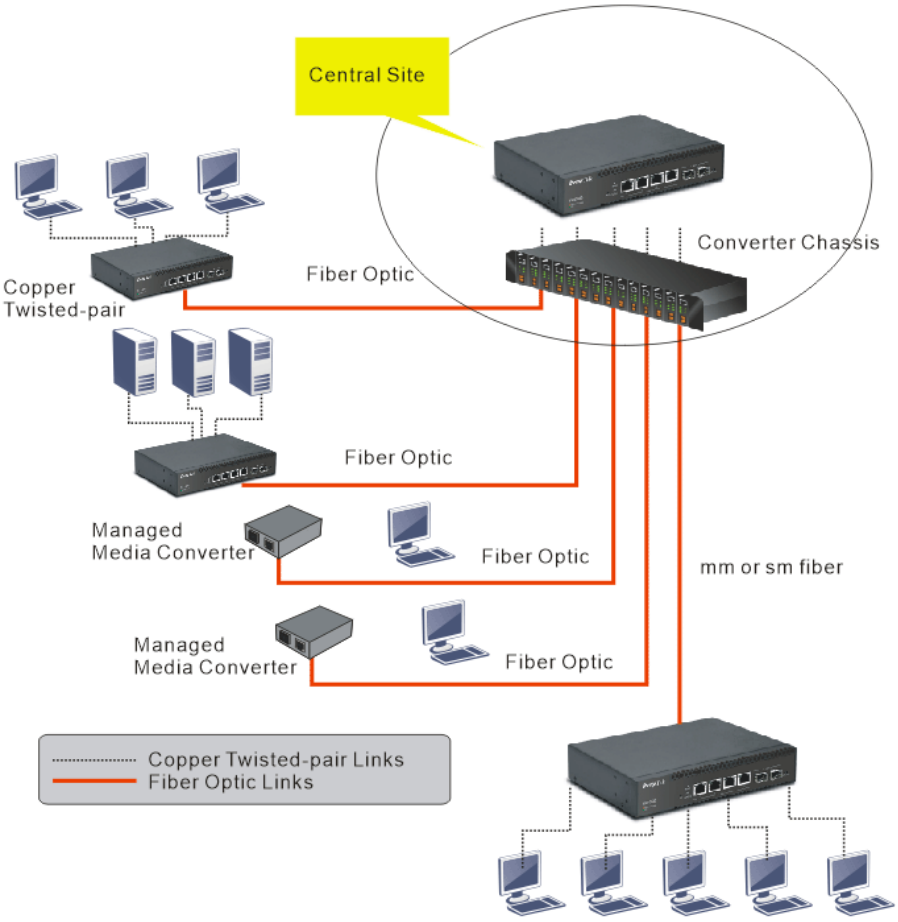
Case 2: The same VLAN members can be at different switches with the same VID



Case 3: 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 4: Central Site/Remote site application is used in carrier or ISP



I-2-4 Managing VigorSwitch 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.

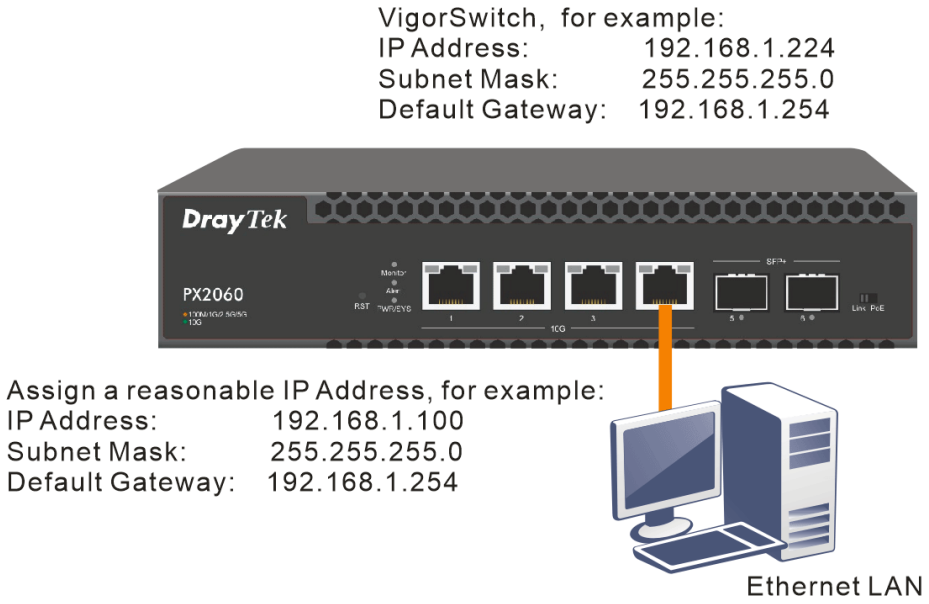
Note:

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.



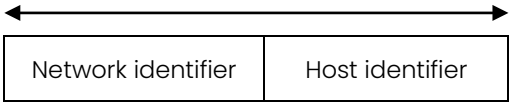
I-2-5 IP Address Assignment

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.

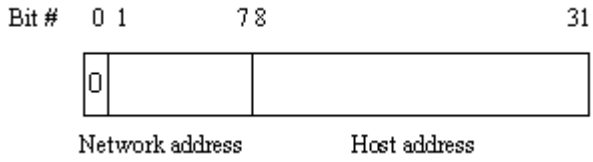


32 bits

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.

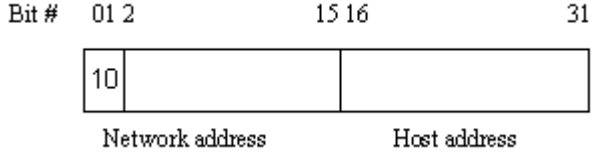
Class A:

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.



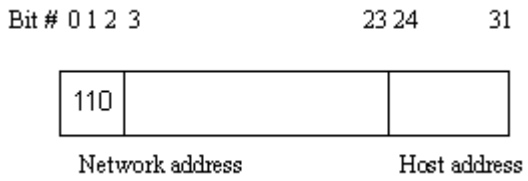
Class B:

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

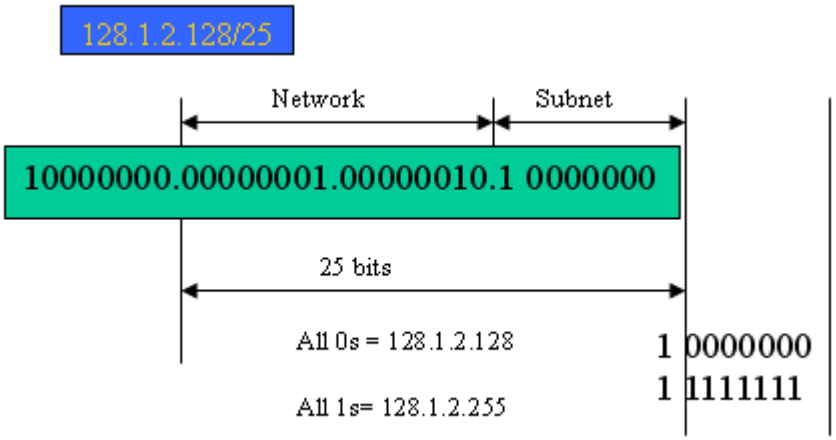
Please refer to RFC 1597 and RFC 1466 for more information.

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.

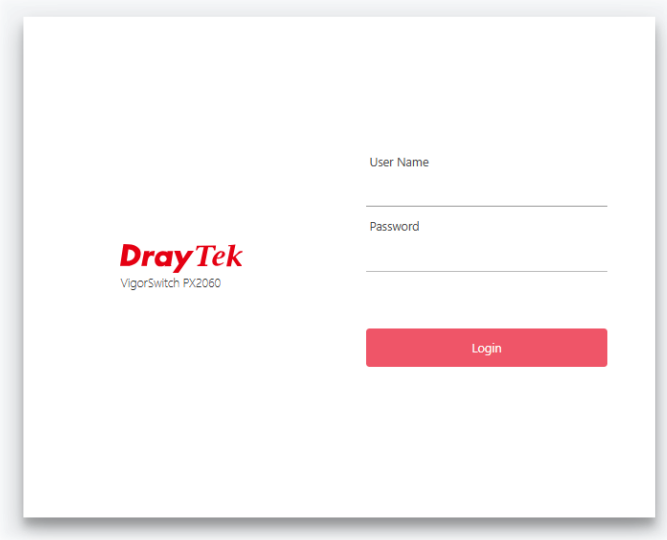
- First, IP Address: as shown above, enter "**192.168.1.224**", for instance. For sure, an IP address such as 192.168.1.x must be set on your PC.
- Second, Subnet Mask: as shown above, enter "255.255.255.0". Choose a subnet mask suitable for your network.

Note:

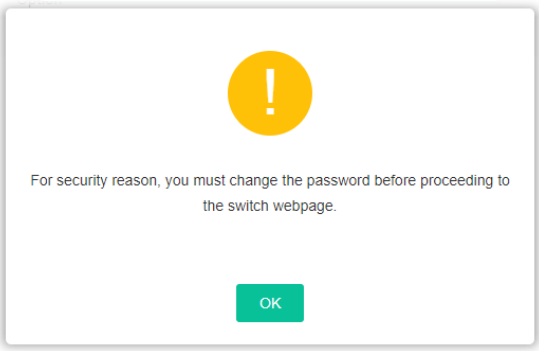
The DHCP Setting is enabled in default. Therefore, if a DHCP server presented on network connected to the switch, check before accessing your switch is essential.

I-3 Accessing Web Page of VigorSwitch

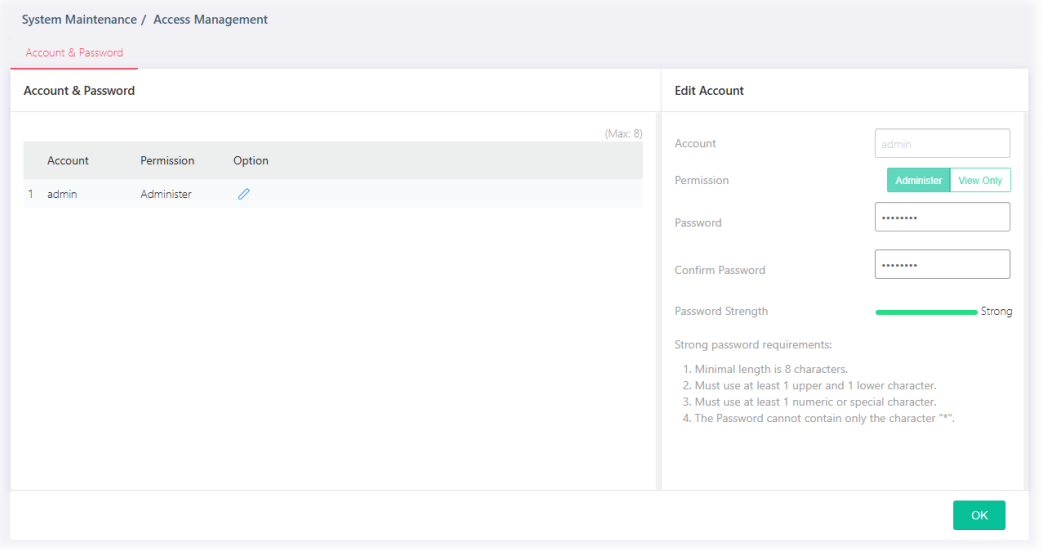
1. Open any browser (e.g., Firefox) and type "192.168.1.224" as URL.
2. Please enter "admin/admin" as the Username/Password and click **Login**.



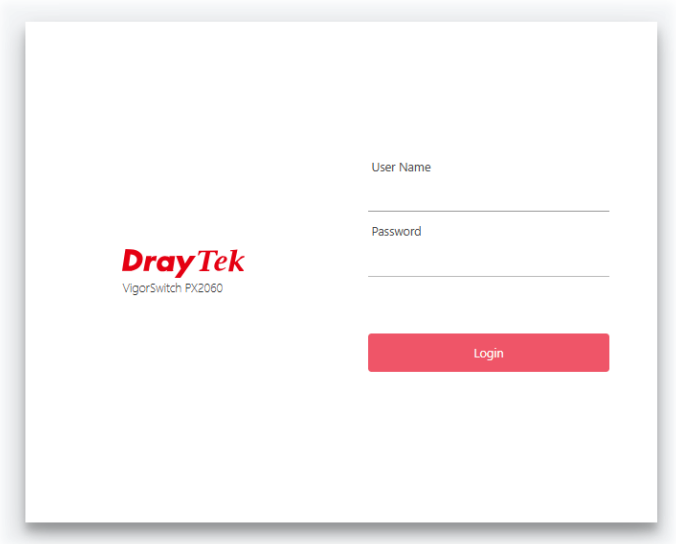
3. Next, a page will appear to guide you change the login password. You MUST change the login password before accessing the web user interface. Please click **OK**.



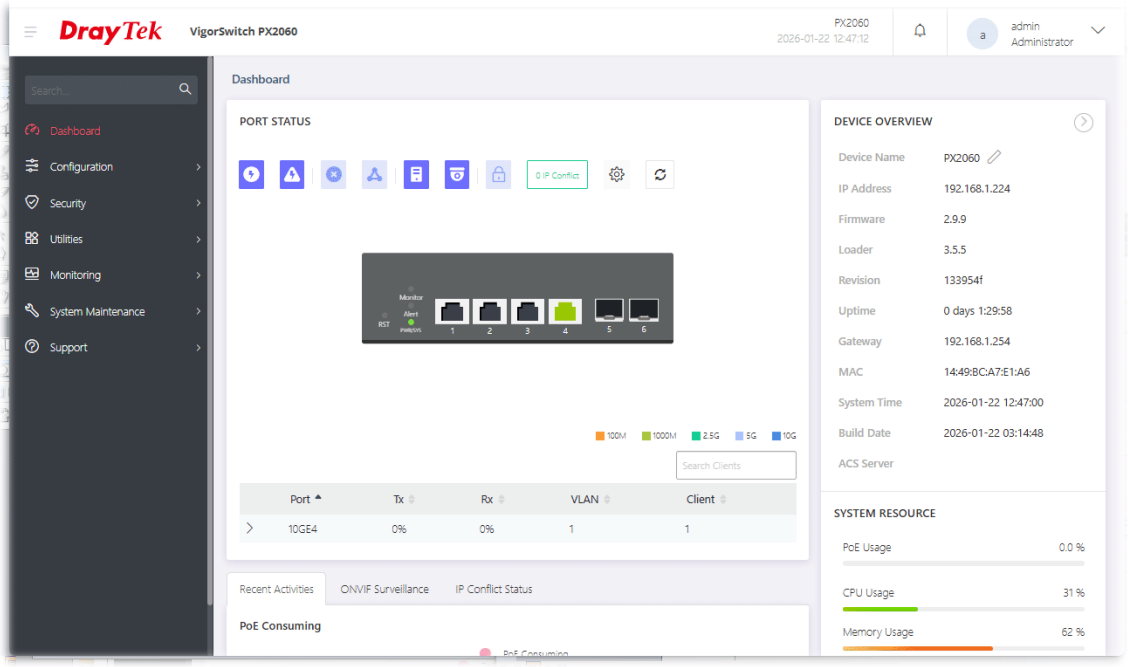
4. Set a new password with the highest level of strength for network security.



5. Click **OK**. Vigor system will guide you to login with the new password again. Enter the new Username/Password and click **Login**.



6. Later, the home page of VigorSwitch will be shown on the screen.

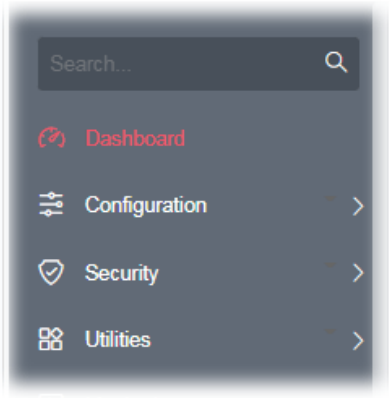


Info:

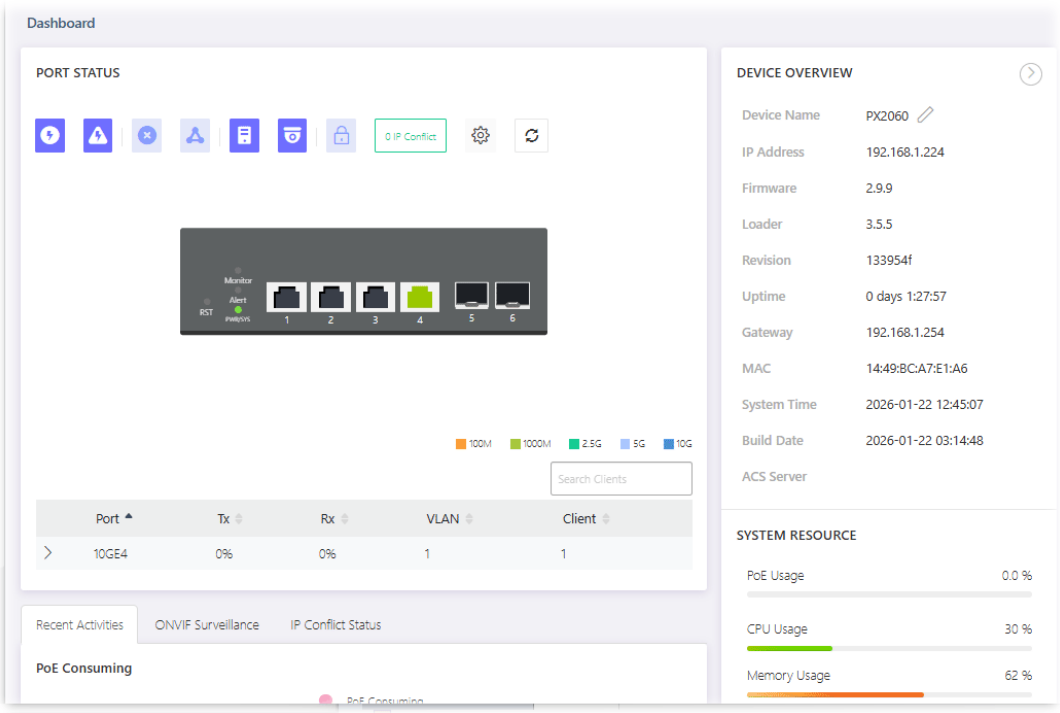
The DHCP Setting is enabled in default. Therefore, if a DHCP server presented on network connected to VigorSwitch, checking before accessing VigorSwitch is essential.

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:



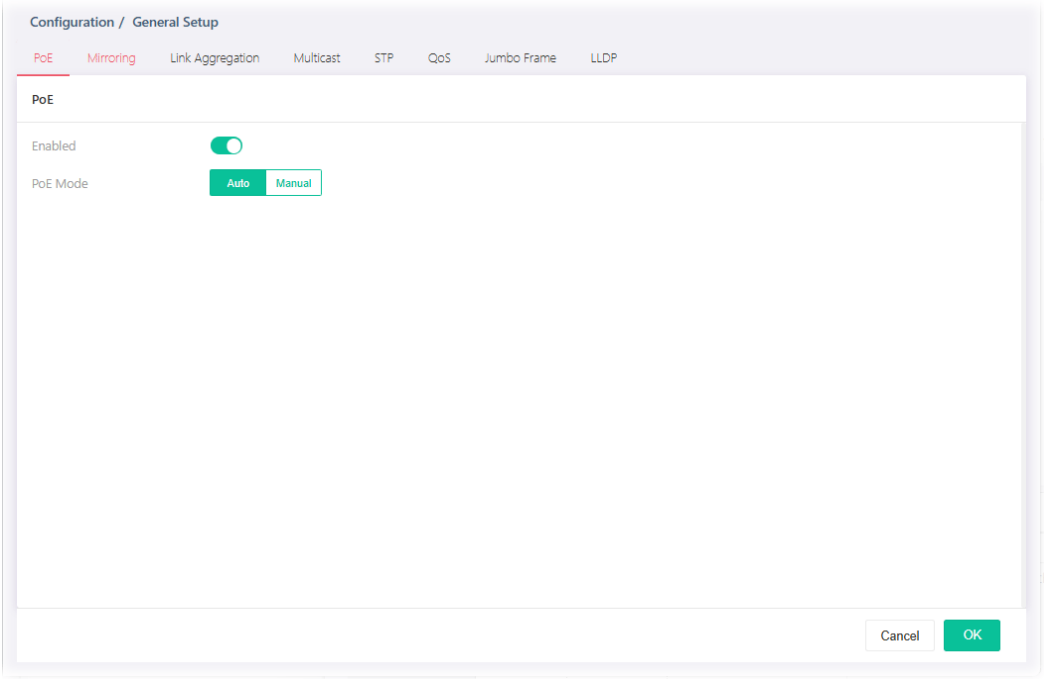
This page is left blank.

Chapter II Configuration

II-1 General Setup

II-1-1 PoE

This page allows a user to configure general settings for supplying PoE power for all PoE ports.



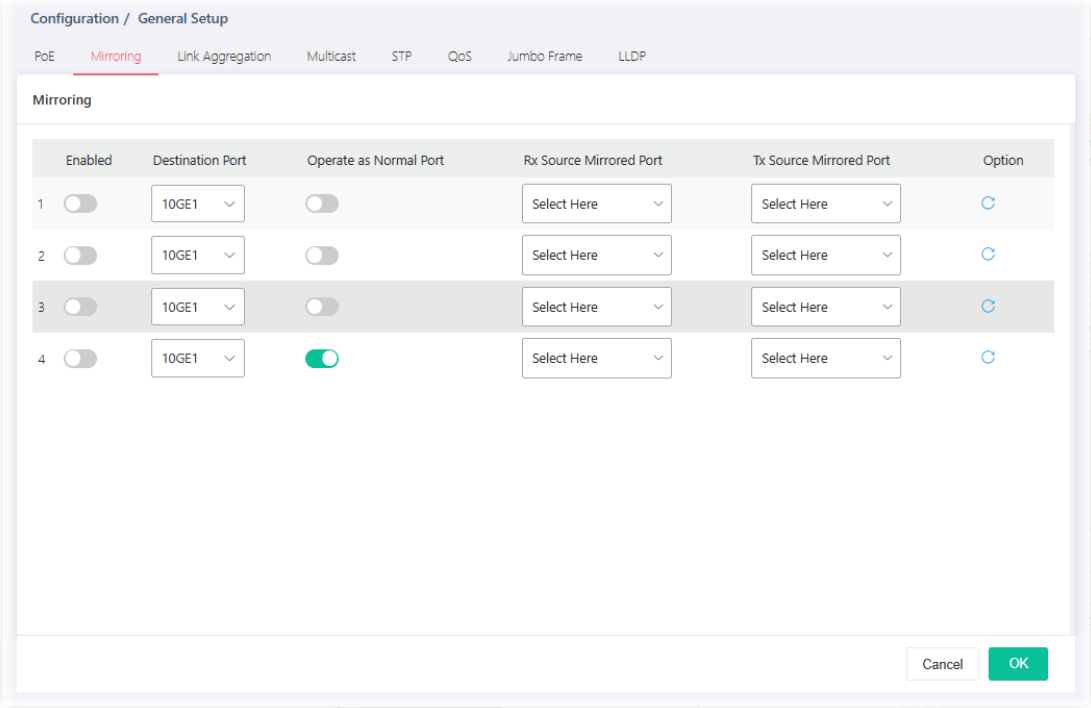
Available settings are explained as follows:

Item	Description
Enabled	**Enable / Disable** – Switch the toggle to enable / disable this function. - means "Enable". - means "Disable".
PoE Mode	**Auto** – Provides plug and play PoE function. PoE schedule and Power Limit are disabled in this mode. **Manual** – Before using scheduled PoE, set **Manual** as PoE mode.

After finishing this web page configuration, please click **OK** to save the settings.

II-1-2 Mirroring

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 convenient for system administrator to monitor / understand the traffic operation.



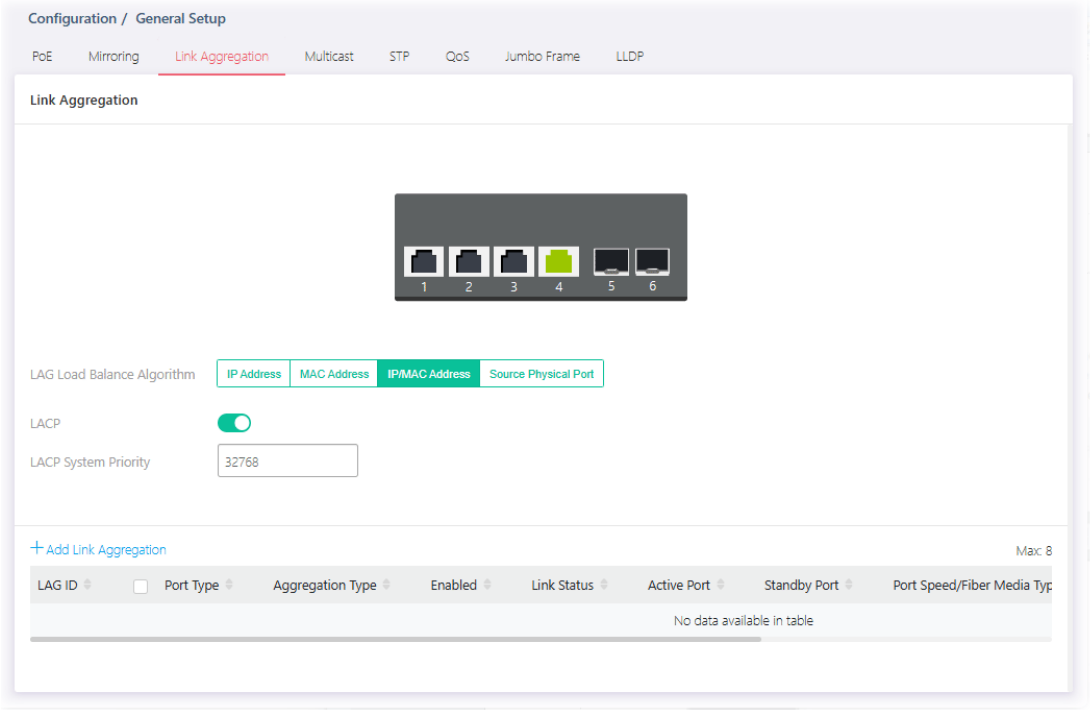
Available settings are explained as follows:

Item	Description
Enabled	**Enable / Disable** – Switch the toggle to enable / disable this function. - means "Enable". - means "Disable".
Destination Port	Specify the port where you wish to observe the mirrored packets.
Operate as Normal Port	**Enable / Disable** – Switch the toggle to enable / disable this function. - means "Enable". - means "Disable".
Rx/Tx Source Mirrored Port	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.
Option	- Clear current settings and return to factory default settings.

After finishing this web page configuration, please click **OK** to save the settings.

II-1-3 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.

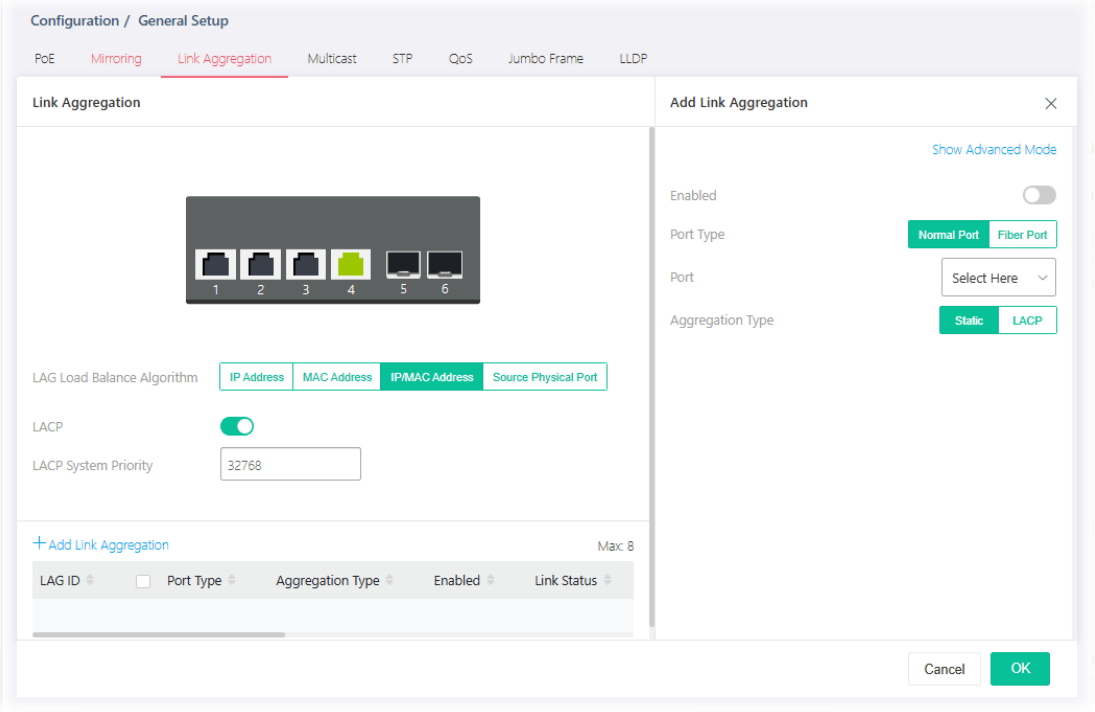


Available settings are explained as follows:

Item	Description
Link Aggregation	
LAG Load Balance Algorithm	Select your Load balance algorithm. **IP Address** - Aggregated group will balance the traffic based on different IP addresses. Therefore, the packets from different IP addresses will be sent to different links. **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. **Source Physical Port** - Aggregated group will balance the traffic based on the source physical port. Therefore, the packets from different physical ports will be sent to different links.
LACP	**Enable / Disable** – Switch the toggle to enable / disable this function.  - means “Enable”. - means “Disable”.
LACP 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 VigorSwitch 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.
+Add Link Aggregation	Click to open the setting page of creating Link Aggregation.

To add a link aggregation, click the "**+Add Link Aggregation**" to open the edit page.

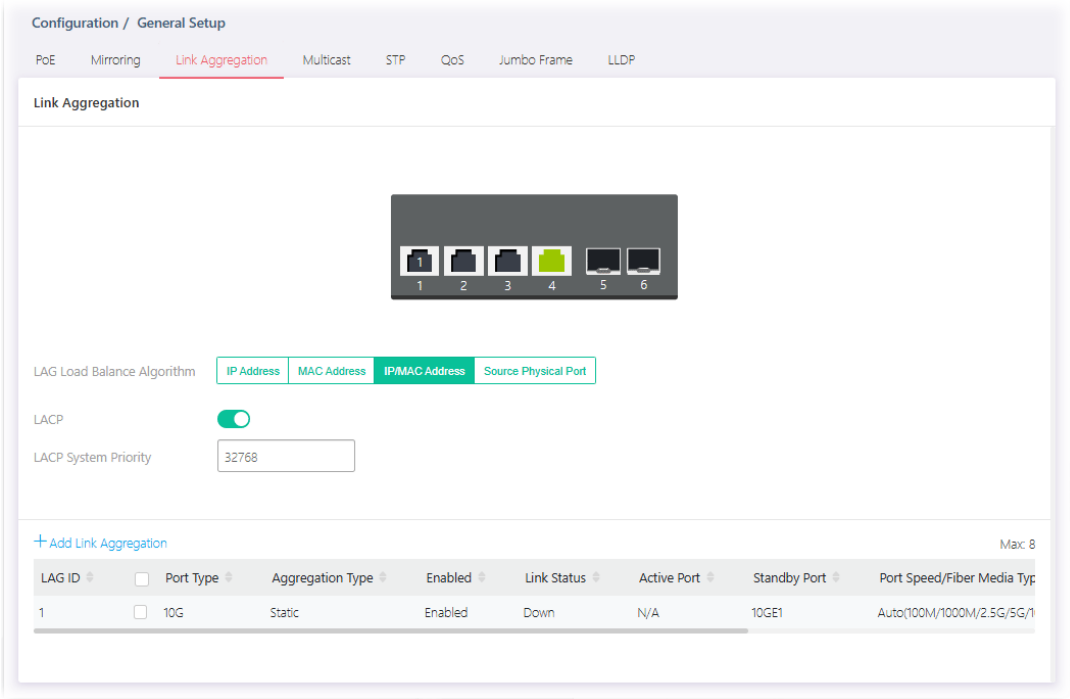


Available settings are explained as follows:

Item	Description
Add/Edit Link Aggregation	
Show/Hide Advanced Mode	Click to switch different modes.
Enabled	**Enable / Disable** – Switch the toggle to enable / disable this function.  - means "Enable". - means "Disable".
Port Type	Select **Normal Port** for Ethernet connection or **Fiber Port** for fiber connection.
Port	Select the physical port number for adding the function.
Aggregation Type	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.
Port Speed	It is available when one or more physical ports are selected.

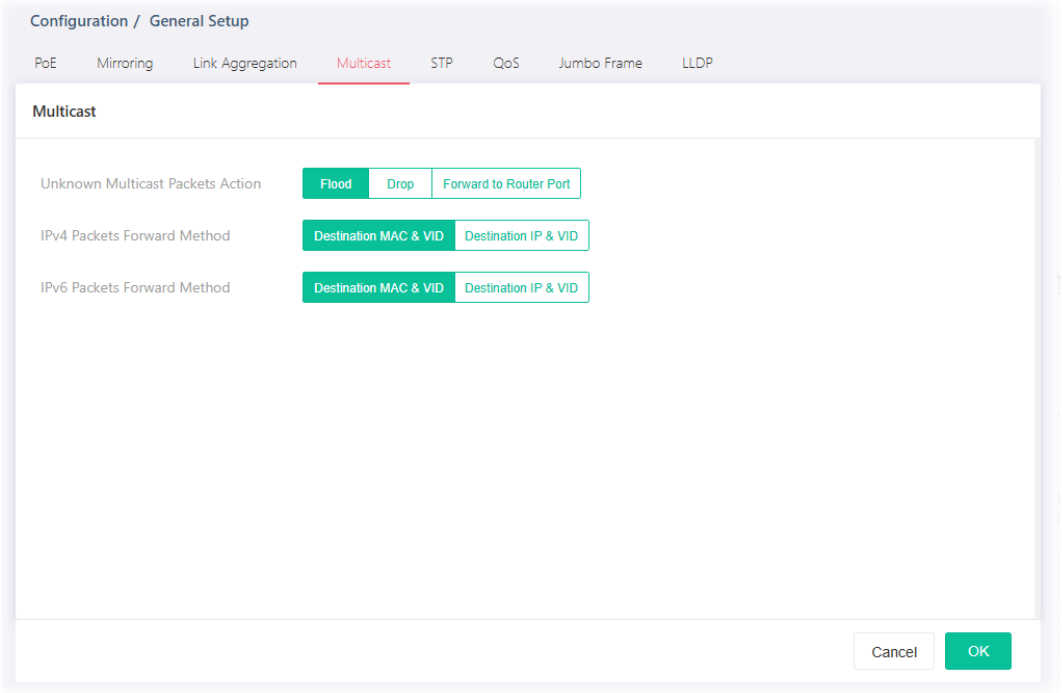
	Port speed capabilities: • **Auto(100/1000M/2.5G/5G/10G):** Auto speed withdifferent ability only. • **Auto(100M):** Auto speed with 100M ability only. • **Auto(1000M):** Auto speed with 1000M ability only. • **Auto(2.5G):** Auto speed with 2.5G ability. Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect. For SFP fiber module, you might need to manually configure the speed to match fiber module speed.
Flow Control	**Enable / Disable** – Switch the toggle to enable / disable this function.  - means "Enable". - means "Disable". 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.
OK	Save the settings.

After finishing this web page configuration, please click **OK** to save the settings. The new link aggregation group will be shown on the page.


Configuration / General Setup
PoE
Mirroring
Link Aggregation
Multicast
STP
QoS
Jumbo Frame
LLDP
Link Aggregation
1
2
3
4
5
6
LAG Load Balance Algorithm
IP Address
MAC Address
IP/MAC Address
Source Physical Port
LACP
LACP System Priority
32768
Add Link Aggregation
Max: 8
LAG ID
Port Type
Aggregation Type
Enabled
Link Status
Active Port
Standby Port
Port Speed/Fiber Media Typ
1
10G
Static
Enabled
Down
N/A
10GE1
Auto(100M/1000M/2.5G/5G/1

II-1-4 Multicast

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



Available settings are explained as follows:

Item	Description
Unknown Multicast Packets 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/IPv6 Packets Forward Method	Set the IPv4/IPv6 multicast forward method. **Destination MAC & VID** - Forward using destination multicast MAC address and VLAN IDs. **Destination IP & VID** - Forward using destination multicast IP address and VLAN ID.

After finishing this web page configuration, please click **OK** to save the settings.

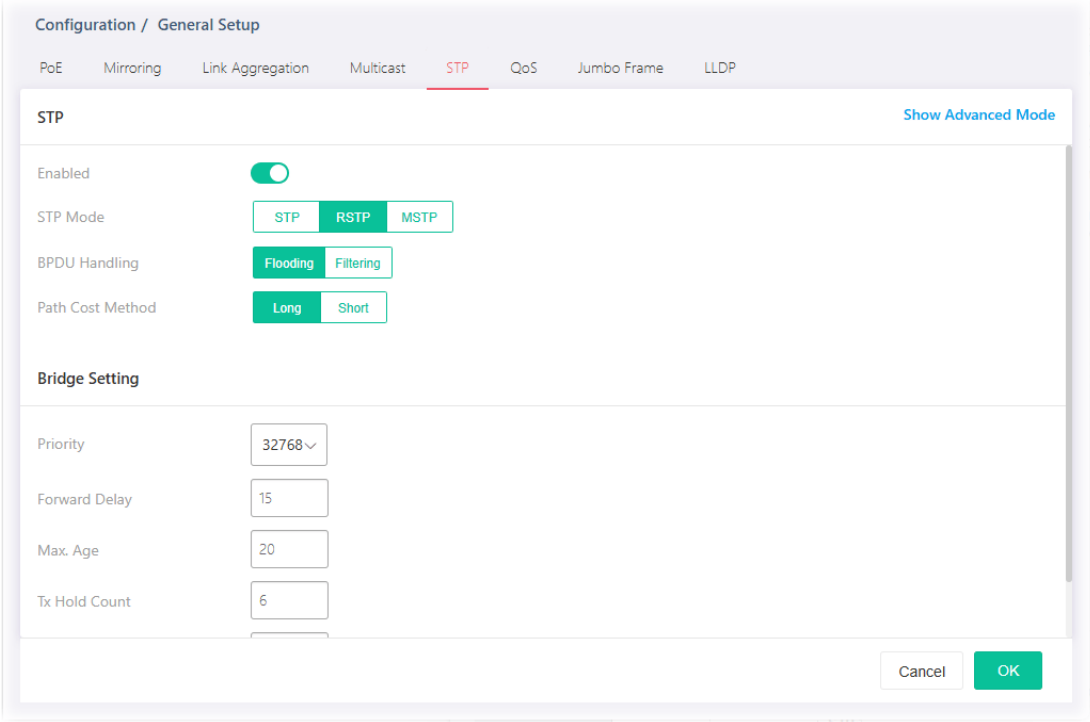
II-1-5 STP

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.



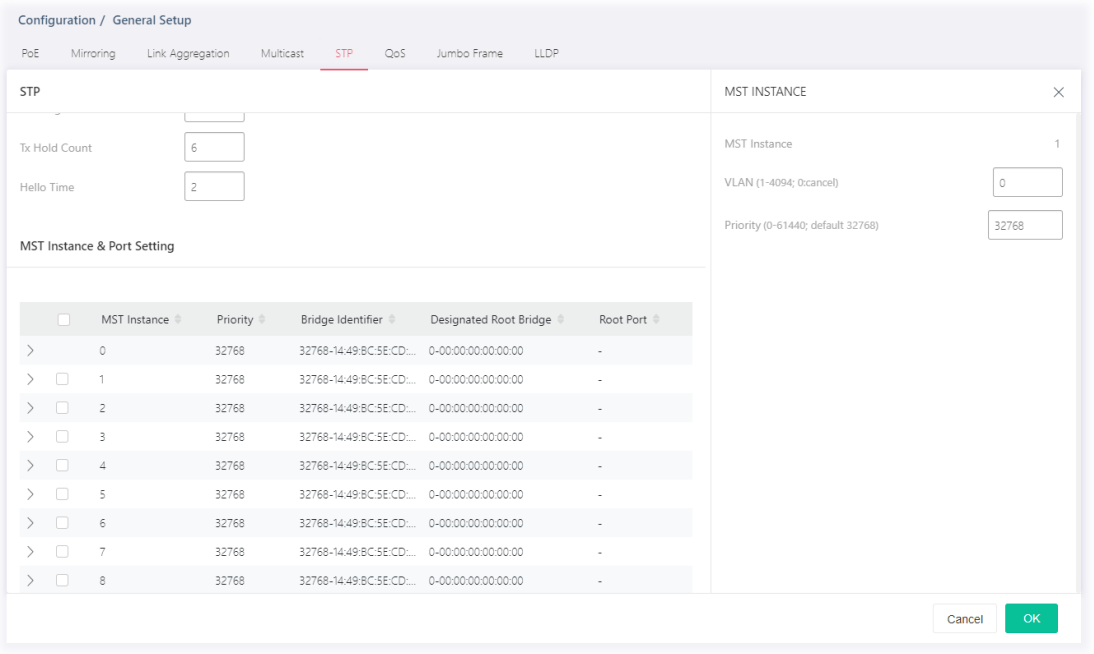
Available settings are explained as follows:

Item	Description
STP	
Enabled	Switch the toggle to enable / disable this function. - means "Enable". - means "Disable".
STP Mode	Set the operating mode of Spanning Tree (STP). **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.
Path Cost 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.
Bridge Setting - Negotiate with other VigorSwitch for determining the bridge switch.	
Priority	Specify the bridge priority. The valid range is from 0 to 61440, and the value should be the multiple of 4096. It ensures the probability that the switch is selected as the root bridge, and the lower value has the higher priority for the switch to be selected as the root bridge of the topology.
Forward Delay	Specify the STP forward delay time, which is the amount of time that a port remains in the Listening and Learning states before it enters the Forwarding state. Its valid range is from 4 to 10 seconds.
Max. Age	Specify the time interval in seconds for a switch to wait the configuration messages, without attempting to redefine its own configuration.
Tx Hold Count	Specify the tx-hold-count used to limit the maximum numbers of packets transmission per second. The valid range is from 1 to 10.
Hello Time	Specify the STP hello time in second to broadcast its hello message to other bridge by Designated Ports. Its valid range is from 1 to 10 seconds.
MSTP Properties	It appears if the Show Advanced Mode link is selected. To make all Vigor switchs within the same MST area, the following two settings must be the same and used for all switches. **Region Name** – Default value is the MAC address of the VigorSwitch. It is used for identifying the MST area. Define the name if required. **Revision** – Default value is "0" (range from 0 to 65535). It is used for the system administrator to identify the version of the MST allocation.
MST Instance & Port Setting	It appears if the Show Advanced Mode link is selected. MST instance 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. **Bridge Identifiter** – Displays the priority of MST instance number + MAC address of the switch. **Designated Root Bridge** – Displays the Bridge Identifier of the root bridge. **Root Port** – Displays the port toward the root. **Root Path Cost** – Displays the path cost toward the root. **Remaining Hop** – Displays the remaining hop count in BPDU. **VLAN –**Displays the ID of the VLAN which should be associated with this MST instance. **Option -**

	- Click to modify the setting page of the selected VLAN. - Clear settings of the selected port and return to factory default settings.

Click to open the MST editing page.



Available settings are explained as follows:

Item	Description
VLAN	Enter the ID (1-4094) of the VLAN which should be associated with this MST.
Priority	The switch priority for this MST instance. A lower number gives the switch higher chance to be chosen as the root bridge.
OK	Save the settings.

After finishing this web page configuration, please click **OK** to save the settings.

II-1-6 QoS

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

Queue Setting

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

- 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.

CoS Mapping

It allows users 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.

DSCP Mapping

It 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.

IP Precedence Mapping

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

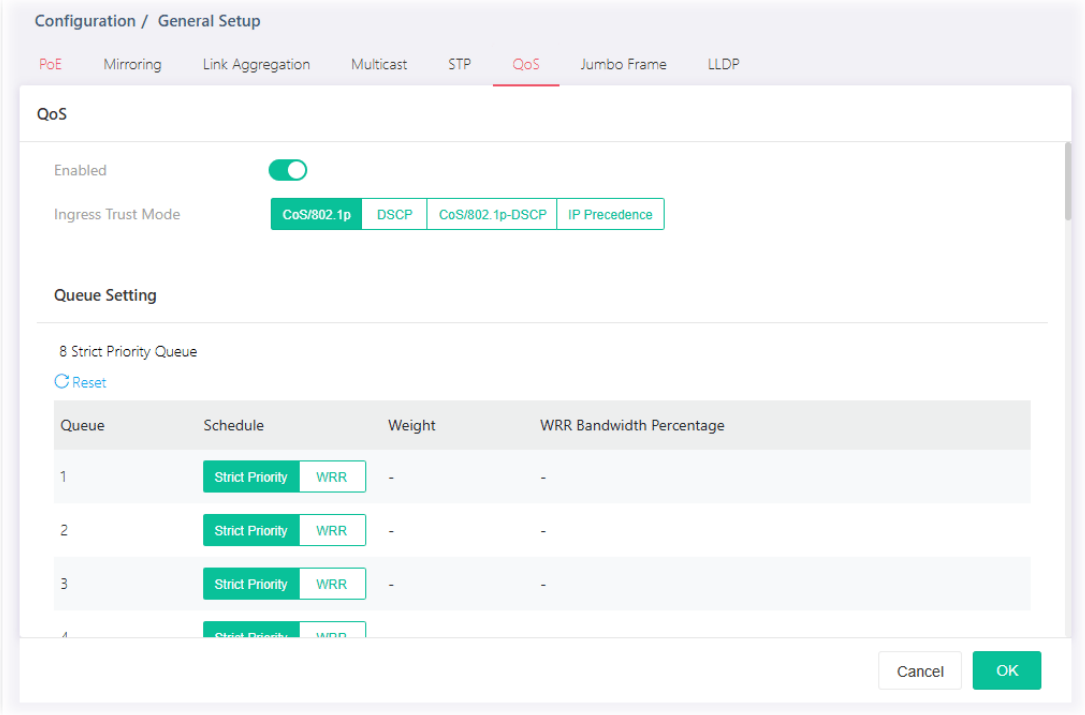
Actual effectiveness is based on how QoS is configured in previous QoS section. This page provides settings for user to configure mapping only.

Egress Shaping Rate

It allows a user to configure the 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 per Queue

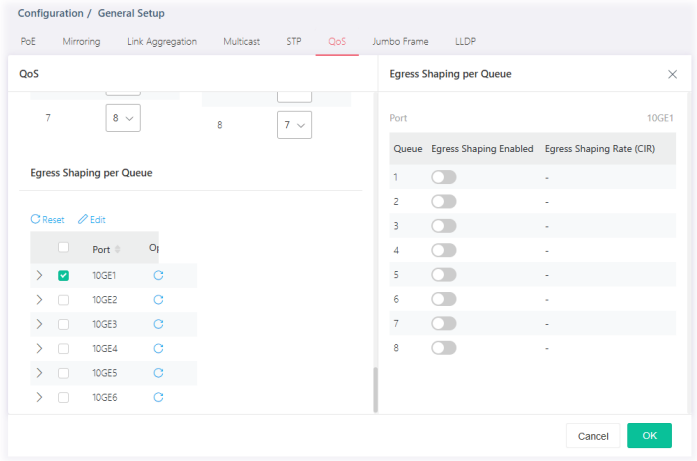
It allows users to configure the maximum egress bandwidth not only by the port but also by specific QoS queues. The configuration result for each port will be displayed on the table listed on the lower side of this web page.



Available settings are explained as follows:

Item	Description

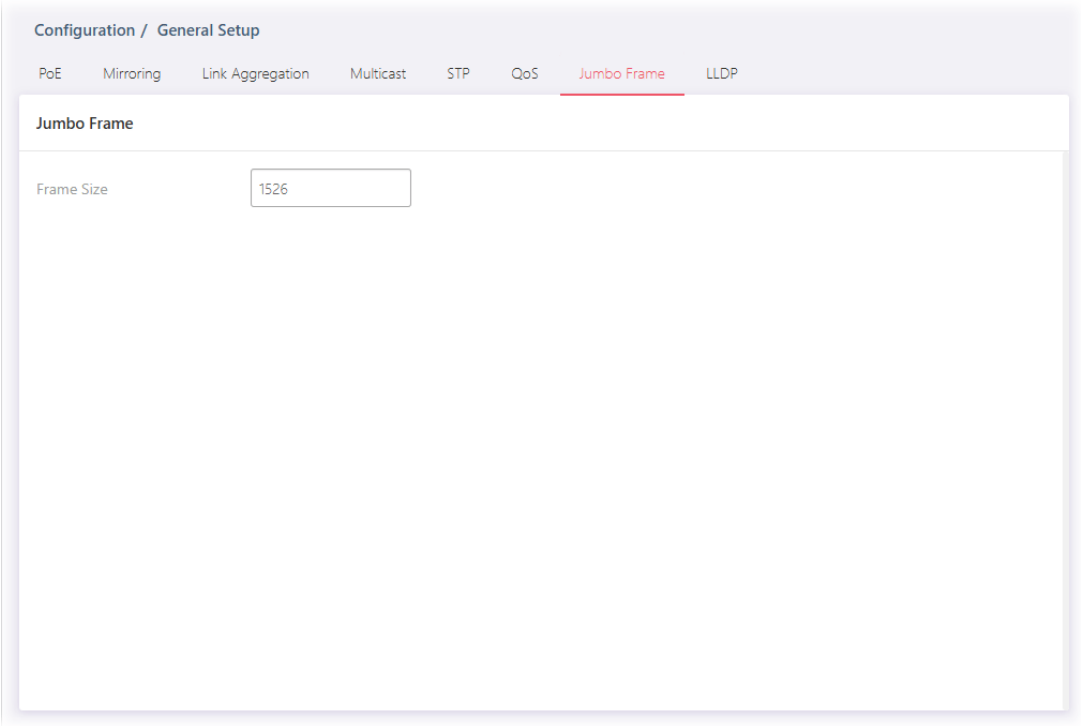
QoS	
Enabled	**Enable / Disable** – Switch the toggle to enable / disable the function of QoS mode.  - means “Enable”. - means “Disable”.
Ingress Trust Mode	Select the QoS operation mode. **CoS/802.1p** –Traffic is mapped to queues based on the CoS field in the VLAN tag, or based on the per-port default 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.
Queue Setting	
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
WRR Bandwidth Percentage	Displays the percentage of traffic which can be sent by current queue compared to total WRR queues.
CoS Mapping	
Class of Service Mapping to Queue (for Ingress Traffic)	Defines the queue ID (level 1 to 8) for different class of service values. **Reset** - Clear current settings and return to factory default settings.
Queue Mapping to Class of Service (for Egress Traffic Remarking)	Defines the class of service value (0 to 7). **Reset** - Clear current settings and return to factory default settings.
DSCP Mapping	
DSCP Mapping to Queue (for Ingress Traffic)	Define the queue ID (level 1 to 8) for different DSCP values. **Reset** - Clear current settings and return to factory default settings.
Queue Mapping to DSCP (for Egress Traffic Remarking)	Define the DSCP value (0 to 63). **Reset** - Clear current settings and return to factory default settings.
IP Precedence Mapping	
IP Precedence Mapping to Queue (for	Defines the queue ID (level 1 to 8) for different IP Precedence values.

Ingress Traffic)	**Reset** - Clear current settings and return to factory default settings.
Queue Mapping to IP Precedence (for Egress Traffic Remarking)	Defines the IP Precedence value (0 to 7). **Reset** - Clear current settings and return to factory default settings.
Egress Shaping per Queue	Configure the maximum egress bandwidth not only by port but also by specific QoS queues. **Reset** - Clear all settings and return to factory default settings. **Port** - Display the port (GE1 to GE16, 10GE1 to 10GE6) profiles.  - Clear settings of the selected port and return to factory default settings. **Edit** - To modify the egress shaping rate for port profiles, select **two** (at least) GE ports to display the Edti button. Cllick the **Edit** button to configure the port setting.  • **Egress Shaping Enabled**- Switch the toggle to enable/disable the setting. • **Egress Shaping Rate (CIR)** - Enter the rate value,<16-1000000>, unit:16 Kbps.

After finishing this web page configuration, please click **OK** to save the settings.

II-1-7 Jumbo Frame

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



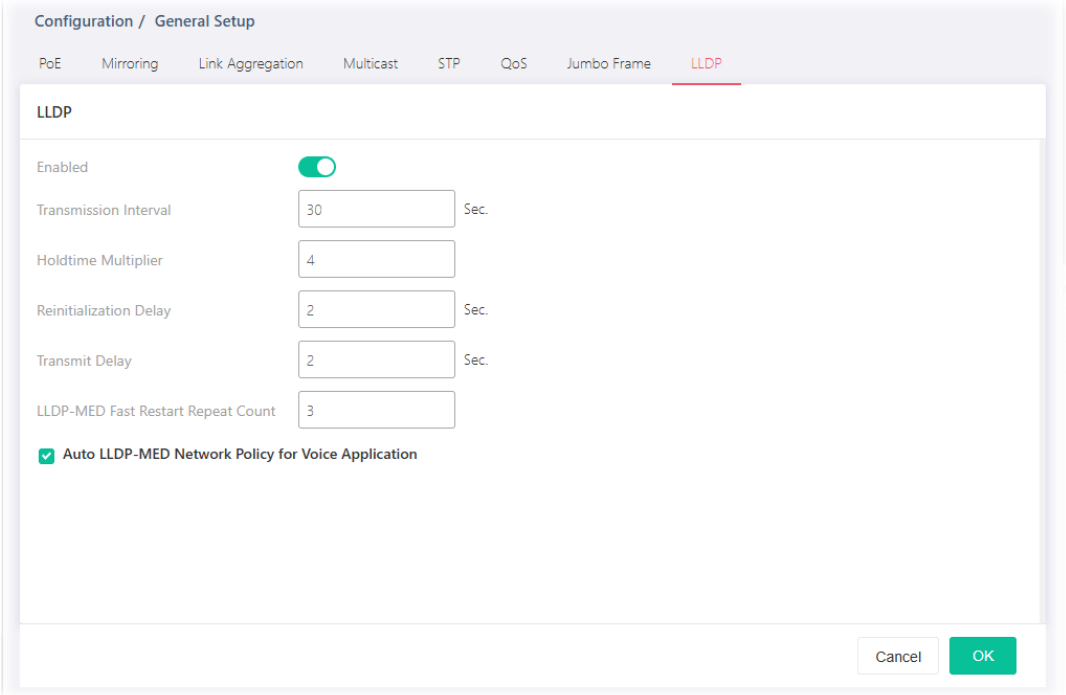
Available settings are explained as follows:

Item	Description
Jumbo Frame	
Frame Size	Enter Jumbo frame size. The valid range is 1526 bytes – 10000 bytes.

After finishing this web page configuration, please click **OK** to save the settings.

II-1-8 LLDP

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



Available settings are explained as follows:

Item	Description
LLDP	
Enabled	**Enable / Disable** – Switch the toggle to enable / disable this function. - means "Enable". - means "Disable". If LLDP function is disabled, specify an action for the LLDP PDU packets. • **Filtering** - The LLDP packets will be filtered and deleted when LLDP is disabled. • **Bridging** - The LLDP packets will be bridging when LLDP is disabled. • **Flooding** - The LLDP packets will be flooded and forwarded to all interfaces when LLDP is disabled.
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 Restart	Select the number of LLDP packets that will be sent during

Repeat Count	LLDP-MED Fast Start period. The default is 3. Available range is from 1 to 10.
Auto LLDP-MED Network Policy for Voice Application	The default value is Enable.

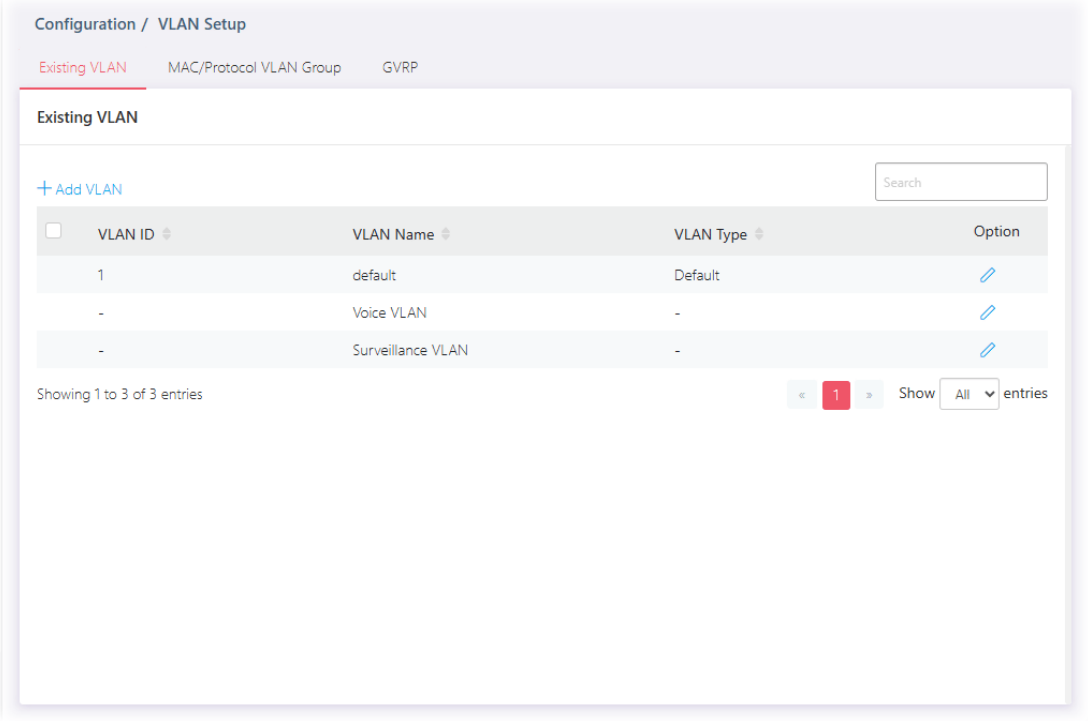
After finishing this web page configuration, please click **OK** to save the settings.

II-2 VLAN Setup

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-2-1 Existion VLAN

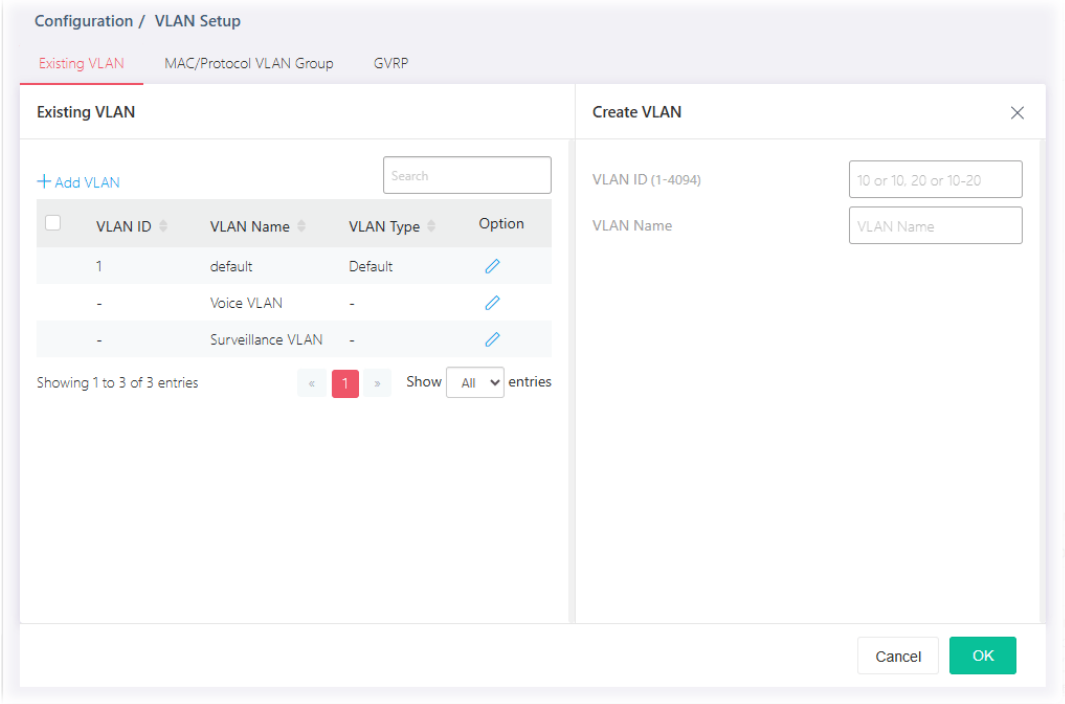
II-2-1-1 Default VLAN



Available settings are explained as follows:

Item	Description
+Add VLAN	Click to open the setting page of creating a new VLAN (with the same type of default VLAN).
VLAN ID	Displays the ID number of the VLAN.
VLAN Name	Displays the name of the VLAN.
VLAN Type	Displays the type of the VLAN.
Option	- Click to modify the setting page of the selected VLAN.

To create a new VLAN, click **+Add VLAN** to open the following page.



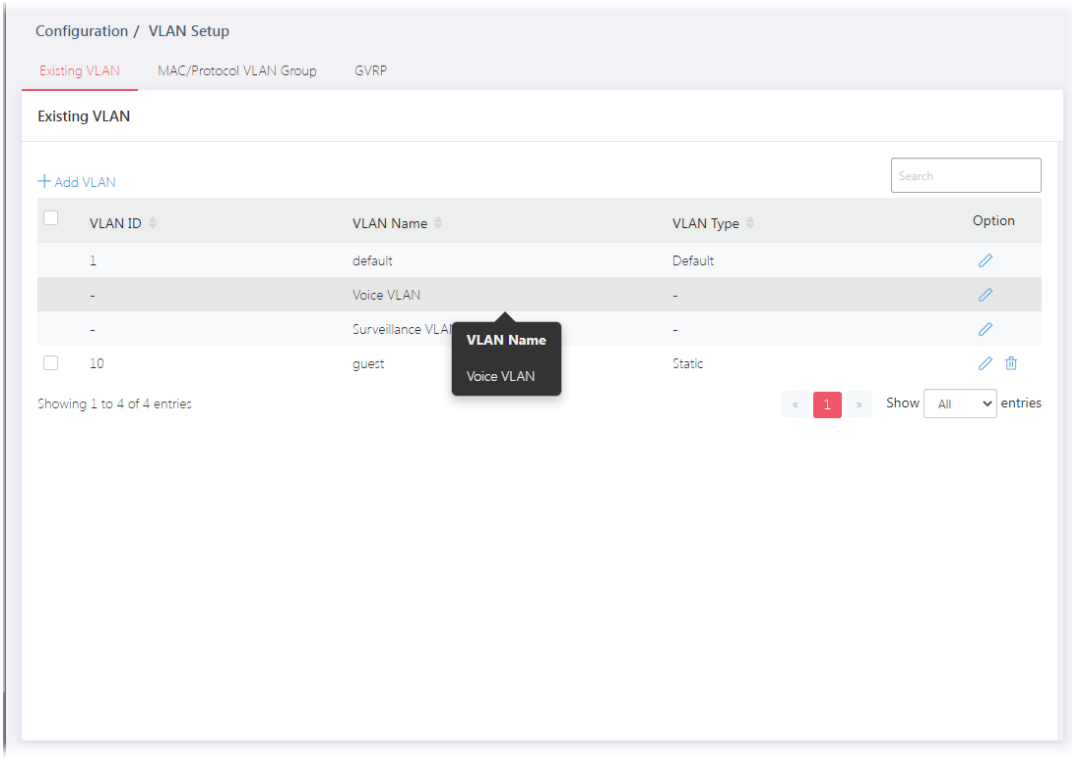
Available settings are explained as follows:

Item	Description
Create VLAN	
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".
OK	Save the settings.

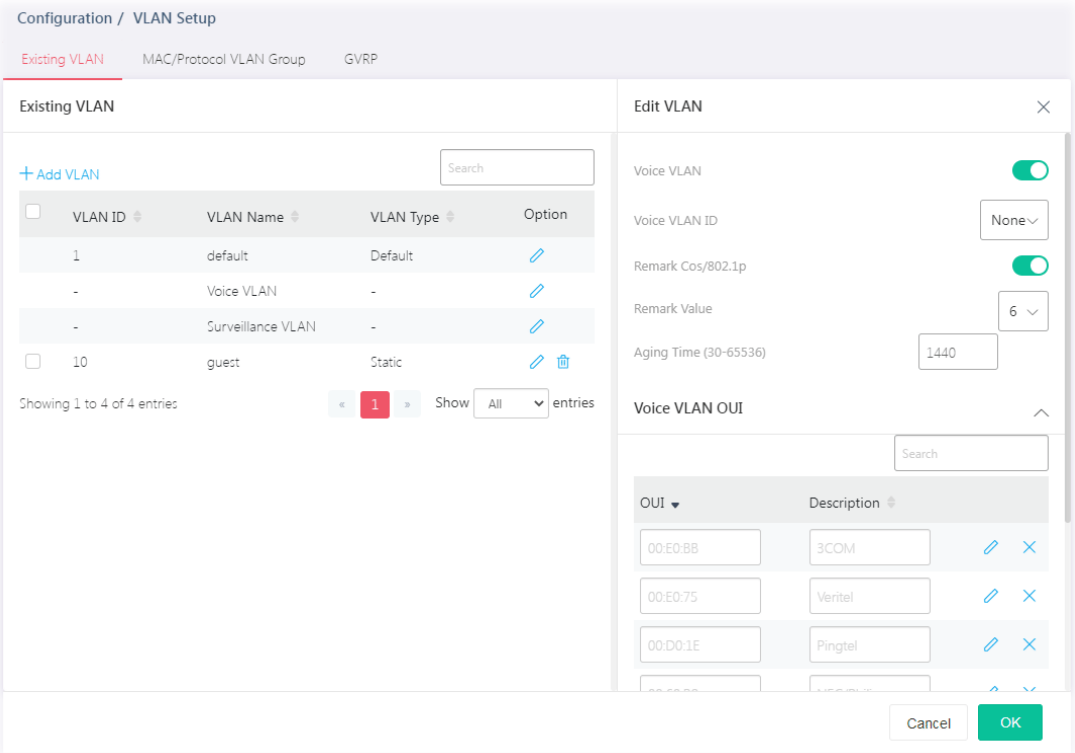
After finishing this web page configuration, please click **OK** to save the settings. A new VLAN will be shown on the page.

II-2-1-2 Voice VLAN

With this 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 priority 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.



Click  to open the editing page.



Available settings are explained as follows:

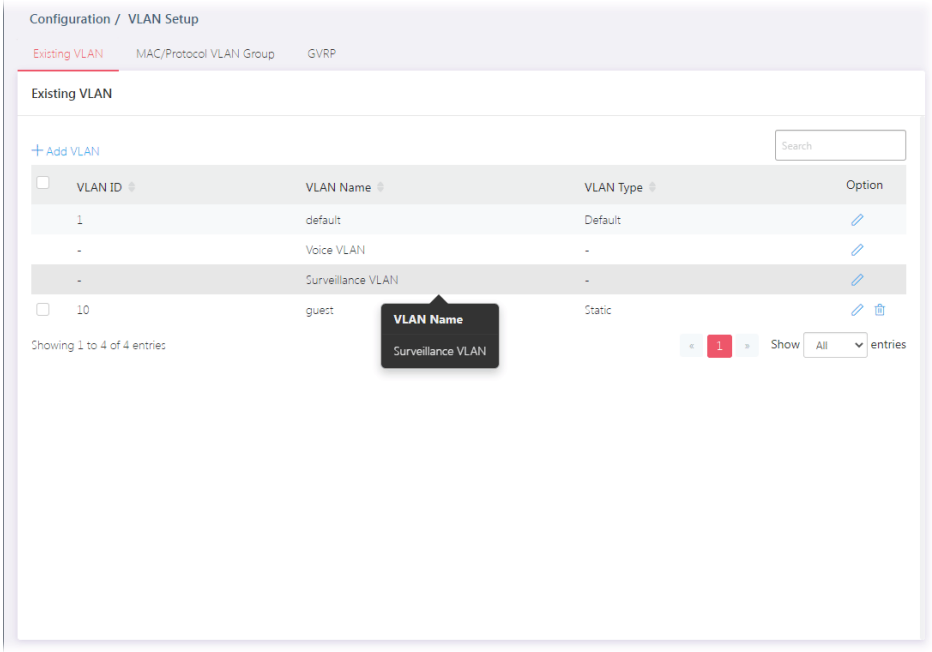
Item	Description
Edit VLAN	
Voice VLAN	**Enable / Disable** – Switch the toggle to enable / disable this function.

	- means “Enable”. - means “Disable”.
Voice VLAN ID	Select Voice VLAN ID profile.
Remark Cos/802.1p	Switch the toggle to enable / disable this function. **Remark Value** - If enabled, qualified packets will be remarked by this value. Specify the number of packets to be remarked. (0 to 7). The VoIP packets will be tagged with this number, 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.
Voice VLAN OUI	Click the to display advanced settings. Default has 8 pre-defined OUI MAC. **+Add** - Click to create a new voice OUI. • **OUI** - Enter the OUI address. • **Description** - Enter a description of the specified MAC address to the voice VLAN OUI table. - Click it to modify the OUI settings and the description.
OK	Save the settings.

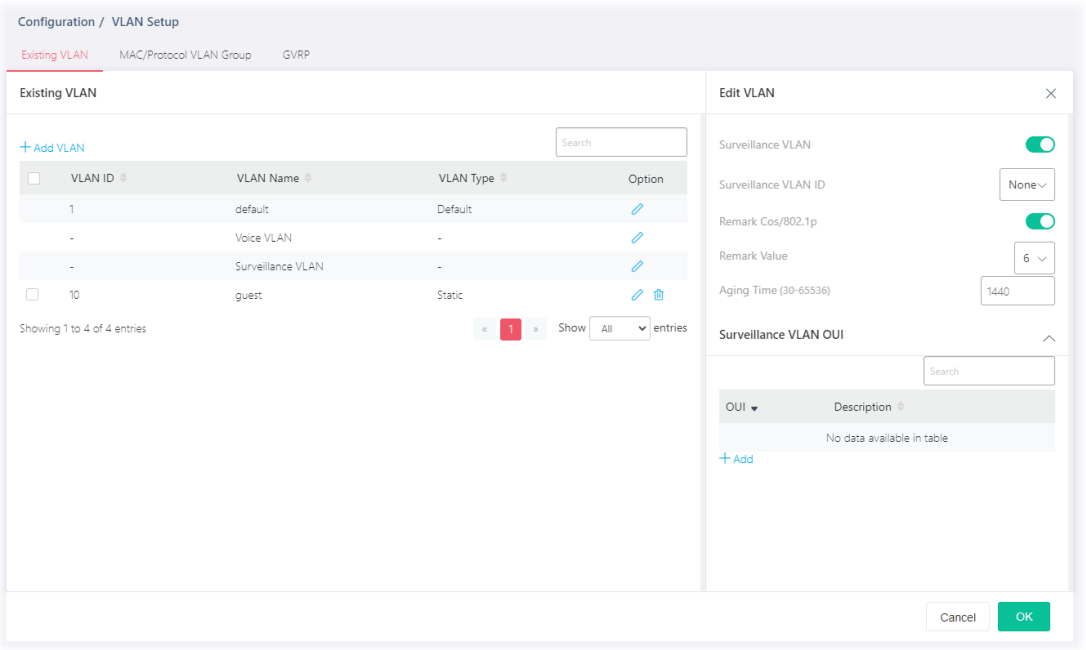
After finishing this web page configuration, please click **OK** to save the settings.

II-2-1-3 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.



Click to open the editing page.



Available settings are explained as follows:

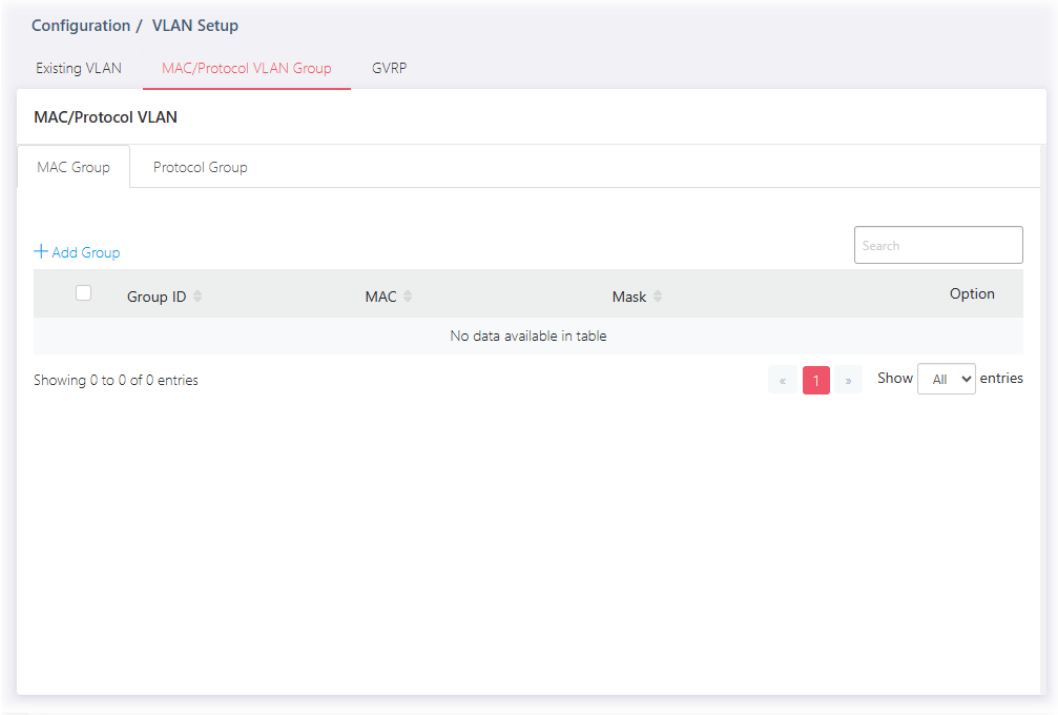
Item	Description
Edit VLAN	
Surveillance VLAN	**Enable / Disable** – Switch the toggle to enable / disable this function.  - means “Enable”. - means “Disable”. Enable the function to configure surveillance VLAN.
Surveillance VLAN ID	Choose a VLAN profile as Surveillance VLAN.
Remark Cos/802.1p	Switch the toggle to enable / disable this function. **Remark Value** - If enabled, qualified packets will be remarked by this value. Specify the number of packets to be remarked. (0 to 7). The VoIP packets will be tagged with this number, 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.
Surveillance VLAN OUI	Filtering Surveillance traffic is based on the OUI of the IP cameras. Click the to display advanced settings. **+Add** - Click to create a new OUI. • **OUI** - Enter OUI MAC address of monitored IP camera. • **Description** - Enter a description of the specified MAC address to the surveillance VLAN OUI table.  - Click to modify the OUI settings and the description.
OK	Save the settings.

After finishing this web page configuration, please click **OK** to save the settings.

II-2-2 MAC/Protocol VLAN Group

II-2-2-1 MAC Group

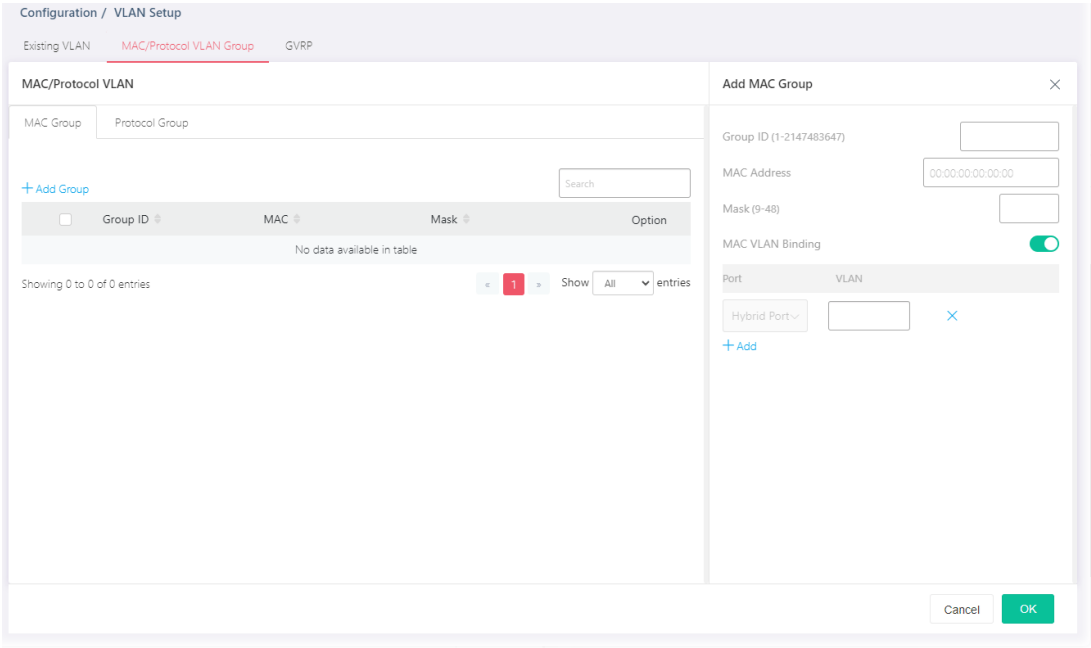
The MAC VLAN allows you to statically assign a VLAN ID to a host with specific MAC address(es). VigorSwitch allows you configure multiple groups with configured MAC address and mask to be active on ports and to be bound with VLAN ID. This page allows the network administrator to define groups with specific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



Available settings are explained as follows:

Item	Description
MAC Group	
+Add Group	Click to open the setting page of creating a new group.
Group ID	It is a number for identification later, while chosen to be bound with VLAN/Port.
MAC	Displays the MAC address of the device grouped under this VLAN profile.
Mask	Displays the number of the mask.

To add a MAC VLAN group, click the "**+Add Group**" to open the setting page.

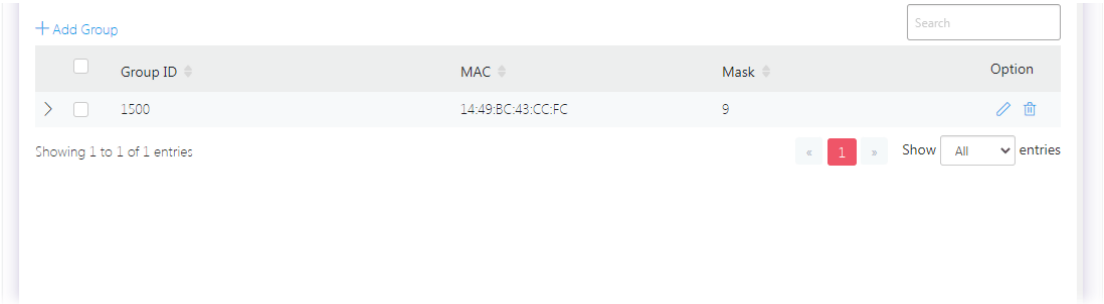


Available settings are explained as follows:

Item	Description
Add MAC Group	
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.
MAC VLAN 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. **Enable / Disable** – Switch the toggle to enable / disable this function.  - means “Enable”. - means “Disable”. **+Add** - Click to enter a port number and VLAN ID number. ● **Port** - Select the ports you wish to be bound with specified MAC address group. ● **VLAN** - Enter the VLAN ID that you wish to be bound with.

After finishing this web page configuration, please click **OK** to save the settings.

A new group will be shown on the page.



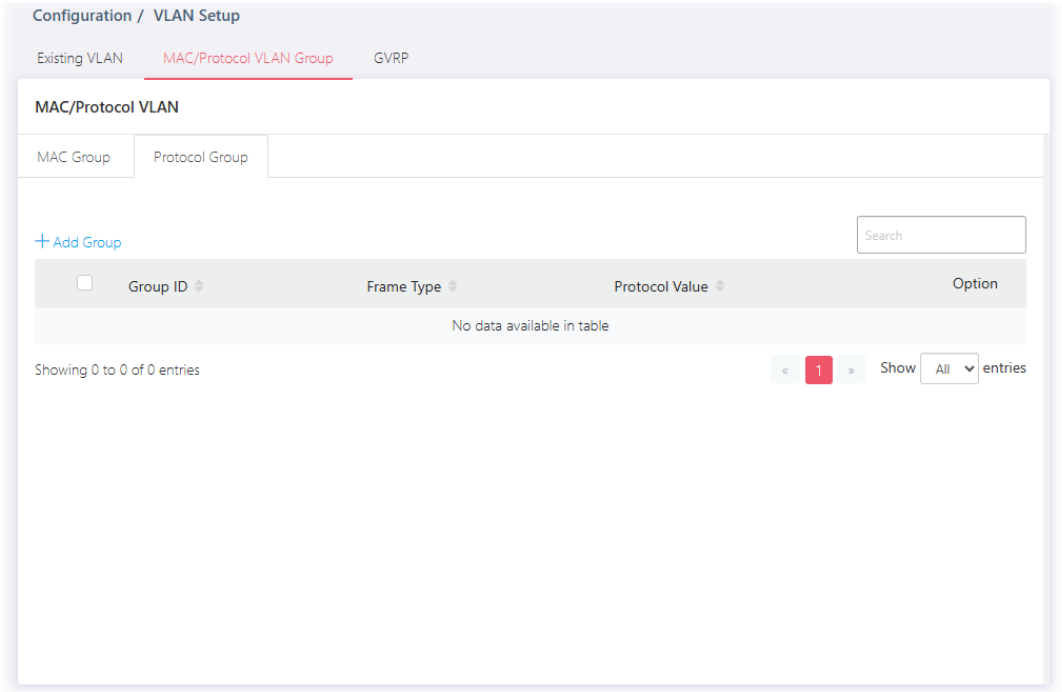
Available settings are explained as follows:

Item	Description
	Click to modify the settings of the selected group.
	Click it to remove the selected entry.

II-2-2-2 Protocol Group

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

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

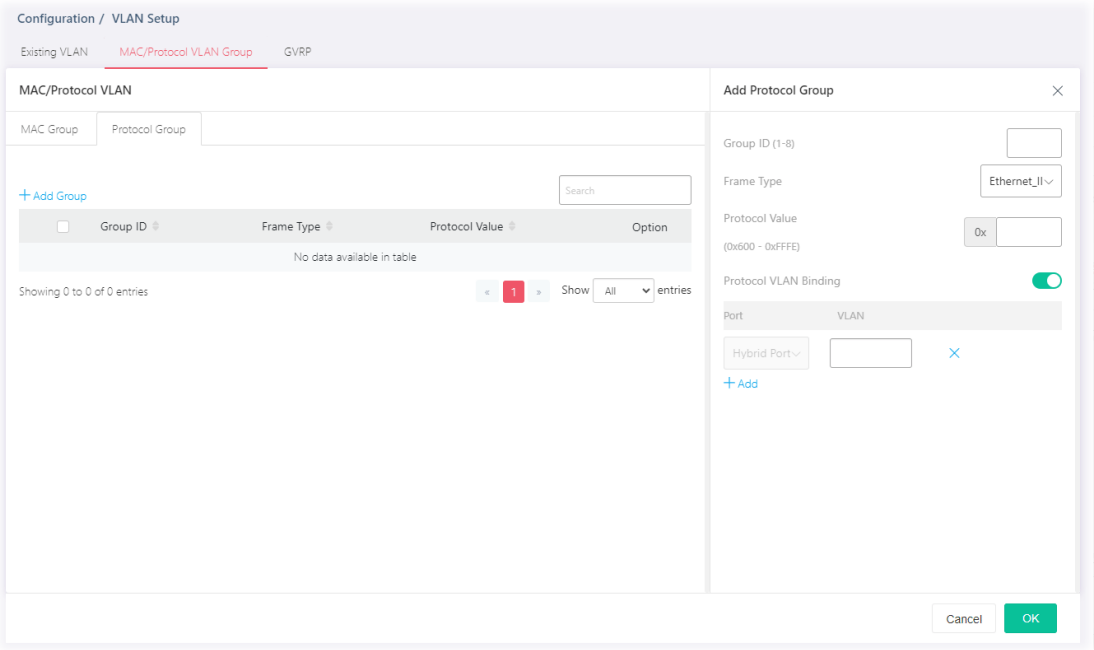


Available settings are explained as follows:

Item	Description
Protocol Group	
+Add Group	Click to open the setting page of creating a new group.

Group ID	It is a number for identification later, while chosen to be bound with VLAN/Port.
Frame Type	Displays the frame type which you would like to filter.
Protocol Value	Displays the value (ranging from 0x600 ~0xFFFE). Packets match with the value will be classified into this group.

To add a Protocol VLAN group, click the "**+Add Group**" to open the setting page.



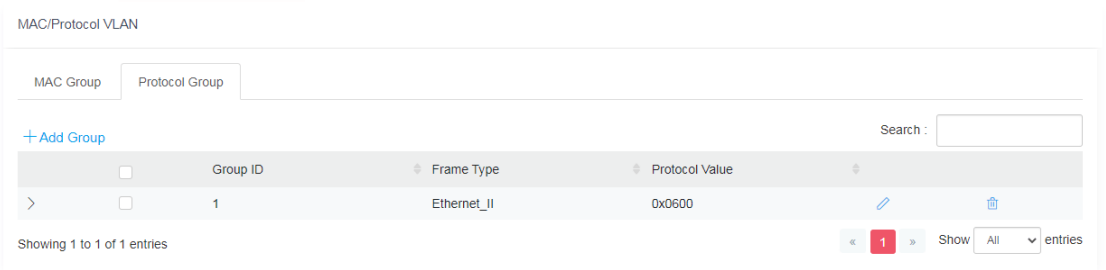
Available settings are explained as follows:

Item	Description
Add Protocol Group	
Group ID	It is a number for identification later, while chosen to be bound with VLAN/Port.
Frame Type	Use the drop-down list to specify the frame type which you would like to filter. **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.
Protocol VLAN Binding	It is for setting up the ports and protocol group that we would like to filter, and the VLAN ID we would like to assign. **Enable / Disable** – Switch the toggle to enable / disable this function.  - means “Enable”. - means “Disable”. **+Add** - Click to enter a port number and VLAN ID number. • **Port** - Select the ports you wish to be bound with specified MAC

	address group. ● **VLAN** - Enter the VLAN ID that you wish to be bound with.

After finishing this web page configuration, please click **OK** to save the settings.

A new group will be shown on the page.

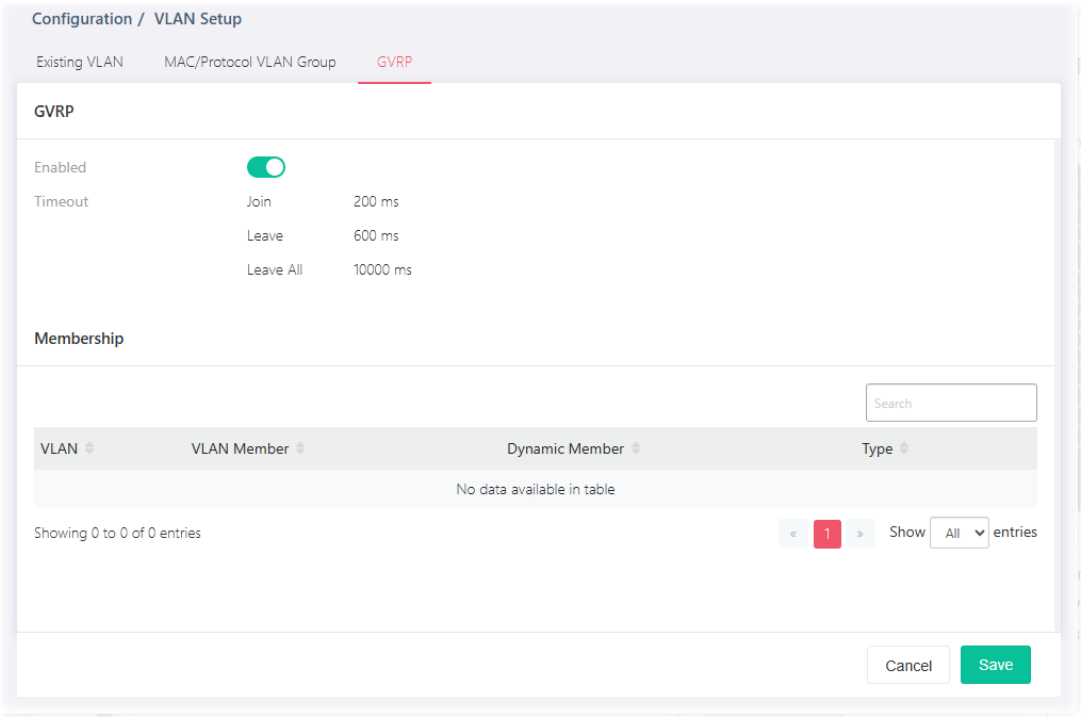


Available settings are explained as follows:

Item	Description
	Click to modify the settings of the selected group.
	Click it to remove the selected entry.

II-2-3 GVRP

This page allows to enable/disable the GVRP function and displays the information for the membership for GVRP (GARP VLAN Registration Protocol).



Available settings are explained as follows:

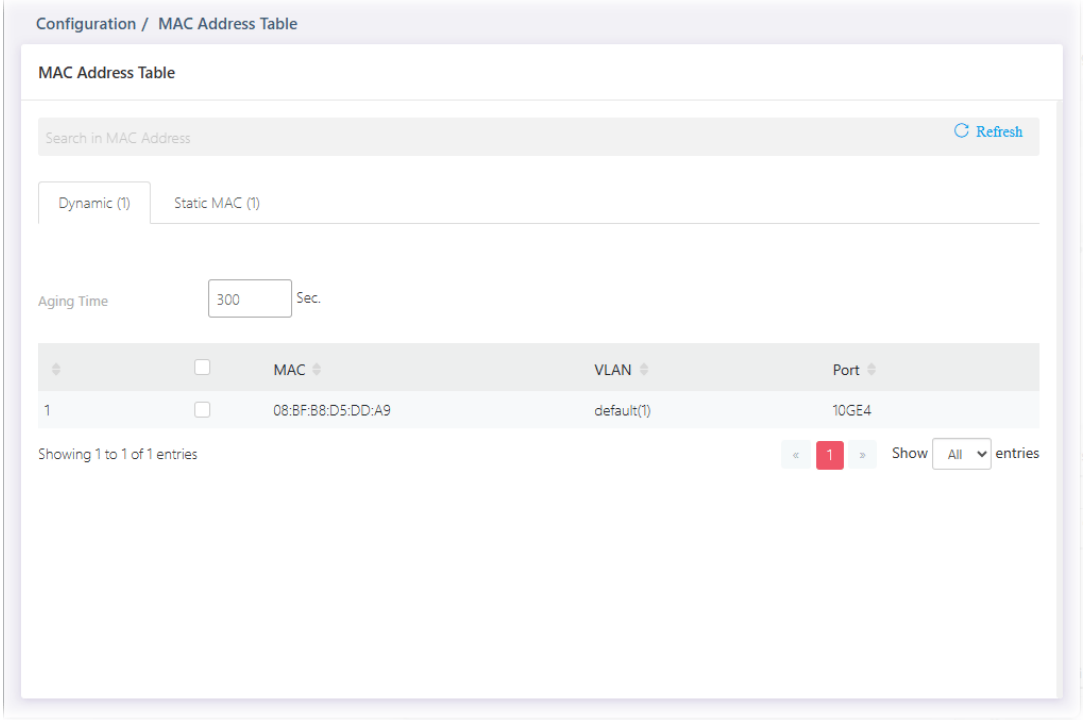
Item	Description
GVRP	

Enable	Switch the toggle to enable / disable this function.  - means “Enable”. - means “Disable”.

II-3 MAC Address Table

II-3-1 Dynamic

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

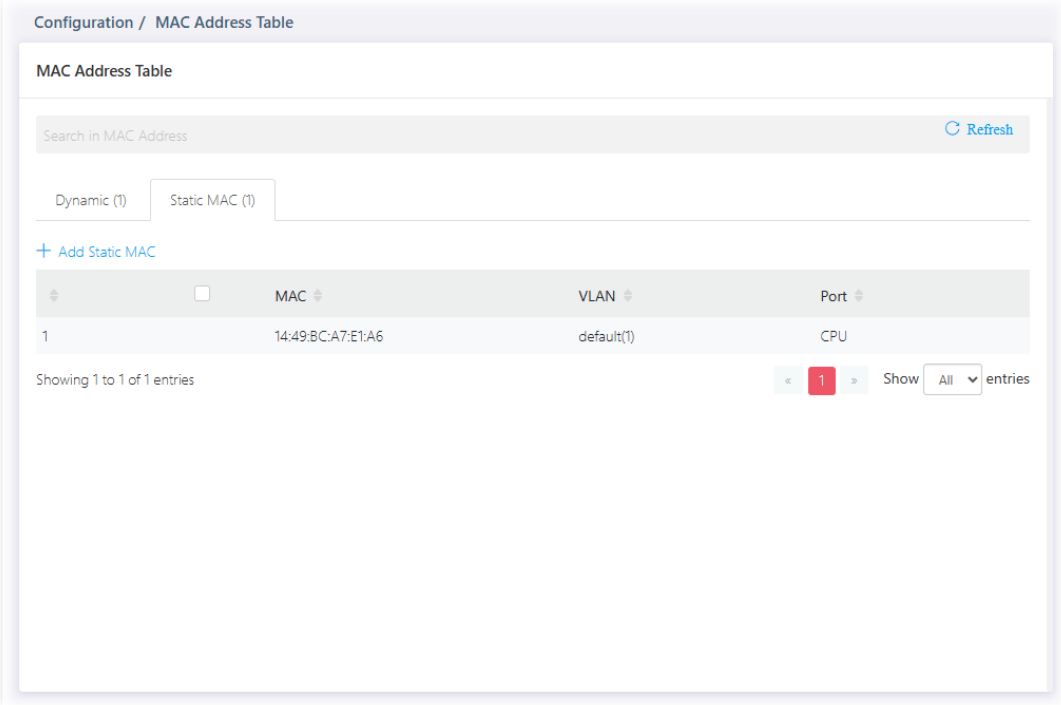


Available settings are explained as follows:

Item	Description
Aging Time	Enter the MAC address aging out value (5-32767 seconds).

II-3-2 Static MAC

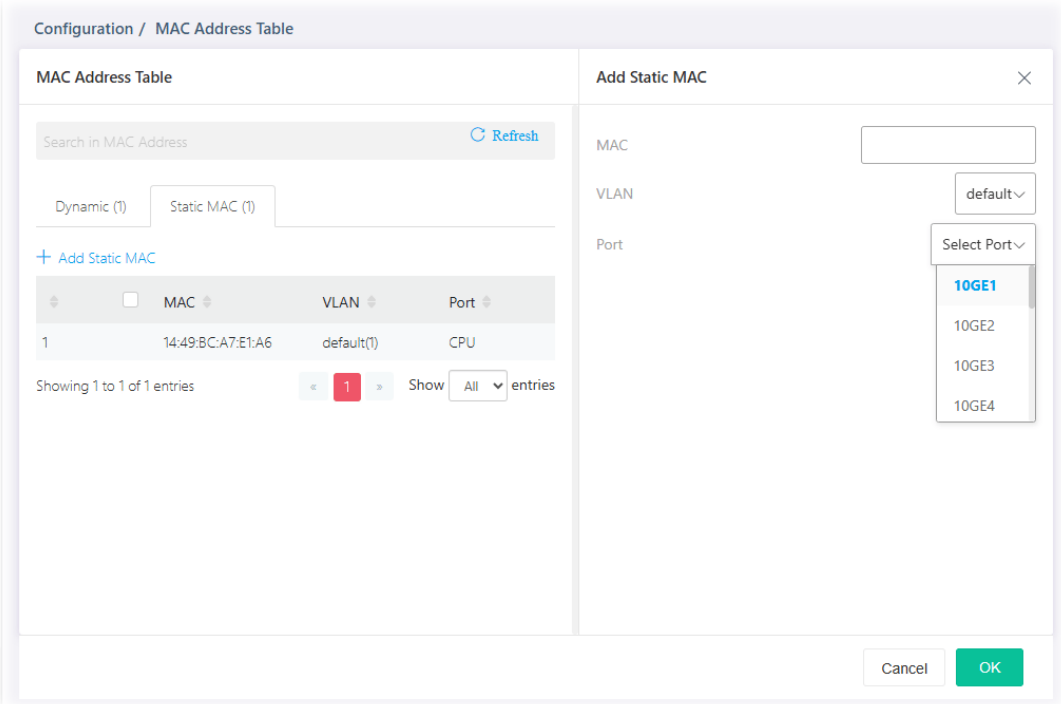
This section allows user to view the static MAC address entries in the MAC table, change related setting, and assign MAC address into MAC table.



Available settings are explained as follows:

Item	Description
+Add Static MAC	Click it to add any port into the static MAC table.
MAC	Displays the MAC address that will be forwarded.
VLAN	Displays the VLAN group to which the MAC address belongs.
Port	Displays the port to which this MAC address belongs.

To add a static MAC, click the "**+Add Static MAC**" to open the edit page.



Available settings are explained as follows:

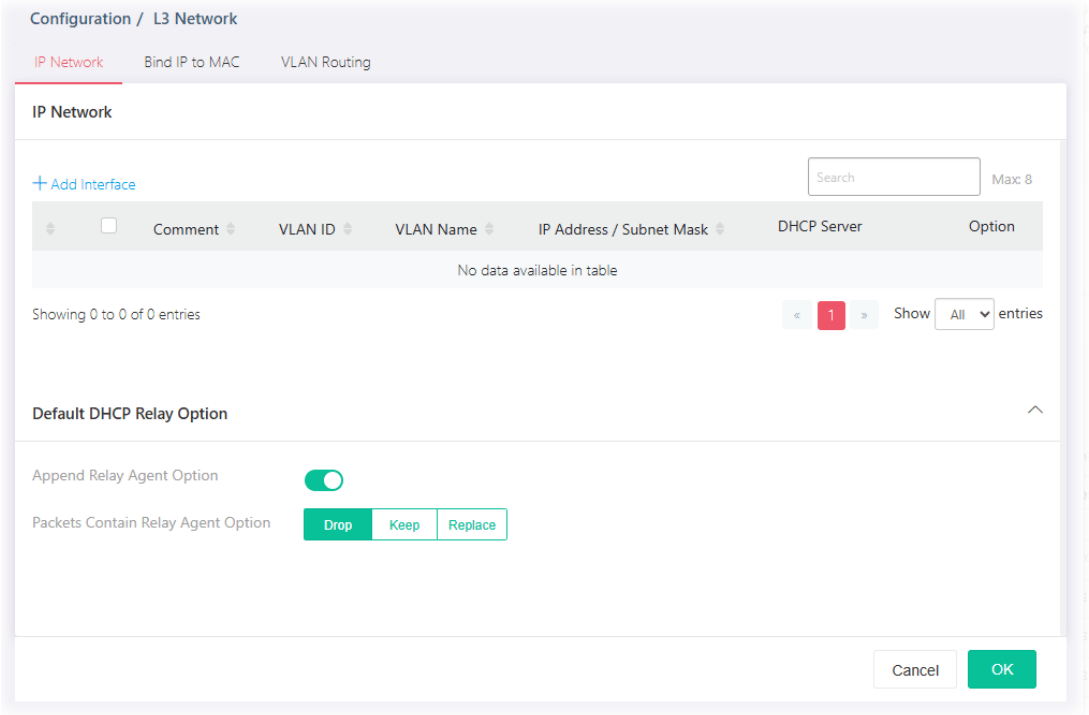
Item	Description
Add Static MAC	
MAC	Enter the MAC address that will be forwarded.
VLAN	Select the VLAN group to which the MAC address belongs.
Port	Select the port to which this MAC address belongs.
OK	Save the settings.

After finishing this web page configuration, please click **OK** to save the settings

II-4 L3 Network

II-4-1 IP Network

Different VLANs can communicate with each other. With the VLAN routing function, computers (or clients) under different VLANs (created from Configuration>>VLAN Setup) can access the Internet and share data or information with each other.

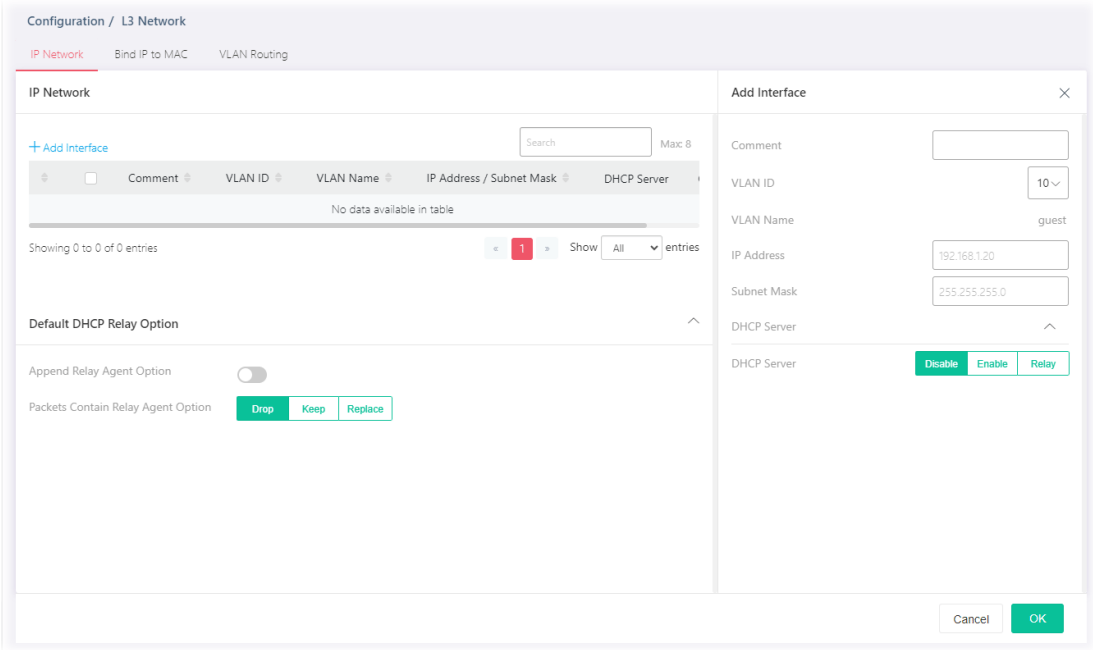


Available settings are explained as follows:

Item	Description
IP Network	
+Add Interface	Click to create a new VLAN interface profile.
Comment	Displays the brief comment for the VLAN ID.
VLAN ID	Displays the ID number of VLAN profile.
VLAN Name	Displays the name of the VLAN profile.
IP Address/Subnet Mask	Displays the IP address and the subnet mask of the selected VLAN profile.
DHCP Server	Displays the status of the server.
Default DHCP Relay Option	
Append Relay Agent Option	Switch the toggle to enable / disable the built-in DHCP server on Vigor switch.  - means “Enable”.

	- means “Disable”.
Packets Contain Relay Agent Option	Set the packet processing method. **Drop** - Received packets which already contain relay information will be discarded. **Keep** - All packets are forwarded, relay information already present will be ignored. **Replace** - Relay information already present in a packet is stripped and replaced with the router’s own relay information.

To add a new interface, click the "**+Add Interface**" to open the edit page.



Available settings are explained as follows:

Item	Description
Add Interface	
Comment	Enter a brief comment for the VLAN ID.
VLAN ID	Use the drop down list to select one VLAN ID.
VLAN Name	Displays the name of the VLAN profile related to the VLAN ID number selected above.
IP Address	Enter the IP address for the selected VLAN ID.
Subnet Mask	Enter the subnet mask for the IP address set above.
DHCP Server	**Disable** - Select to disable the DHCP server function. **Enable** - Select to enable the DHCP server function. **Relay** - If you want to use another DHCP server in the network other than the Vigor switch’s, you can let DHCP Relay help you to redirect the DHCP request to the specified location.
OK	Save the settings.

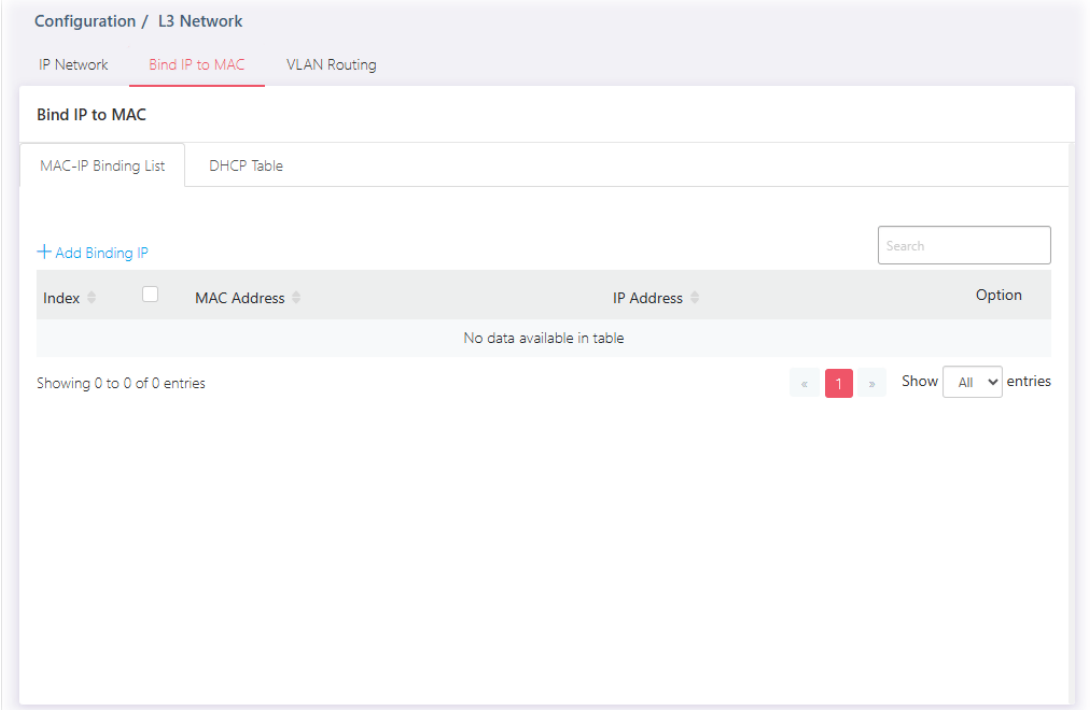
After finishing this web page configuration, please click **OK** to save the settings.

II-4-2 Bind IP to MAC

This function is used to bind the IP and MAC address in LAN to have a strengthening control in network. With the Bind IP to MAC feature you can reserve LAN IP addresses for LAN clients. Each reserved IP address is associated with a Media Access Control (MAC) address.

II-4-2-1 MAC-IP Binding List

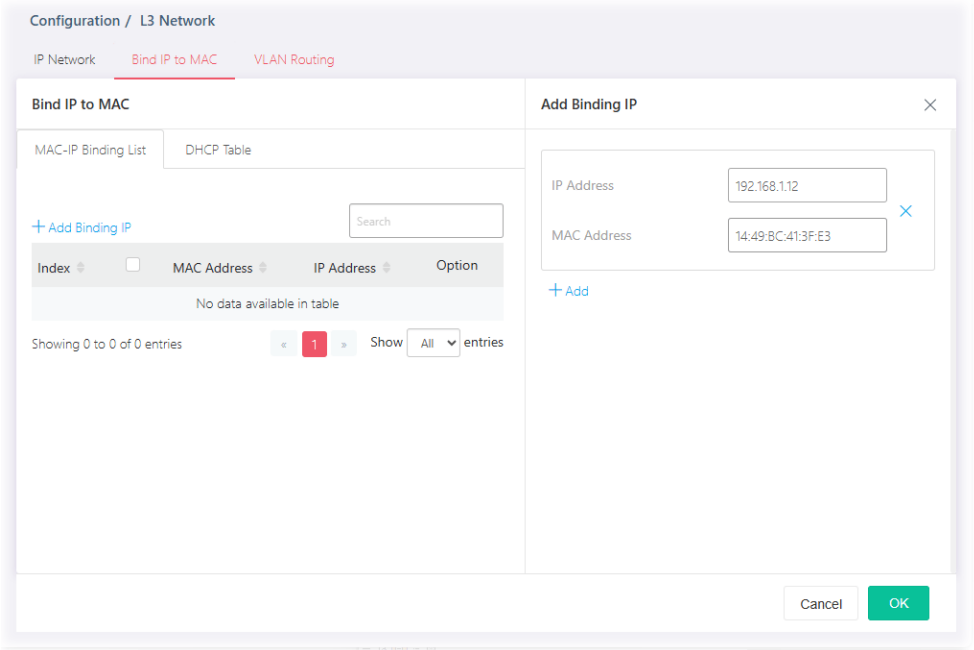
This page displays the MAC-IP Binding List and allows the user to add a new profile or edit/ delete an existed profile.



Available settings are explained as follows:

Item	Description
+Add Binding IP	Click to create a new binding list profile.
Index	Displays the index number of the binding list profile.
MAC Address	Displays the MAC address of the binding list profile.
IP Address	Displays the IP address of the binding list profile.
Option	- Click to modify the settings of the selected entry. - Click it to remove the selected entry.

To add a new binding IP, click the "**+Add Binding IP**" to open the edit page.



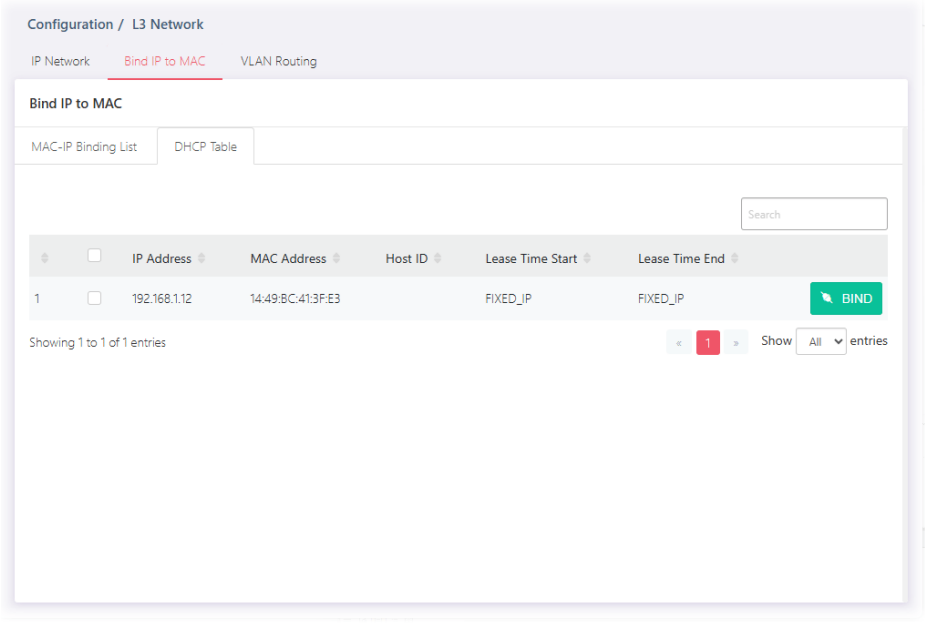
Available settings are explained as follows:

Item	Description
IP Address	Enter the IP address.
MAC Address	Enter the MAC address of the device to be bound with the IP address.
+Add	Click to create more binding IP settings.
OK	Save the settings.

After finishing this web page configuration, please click **OK** to save the settings.

II-4-2-2 DHCP Table

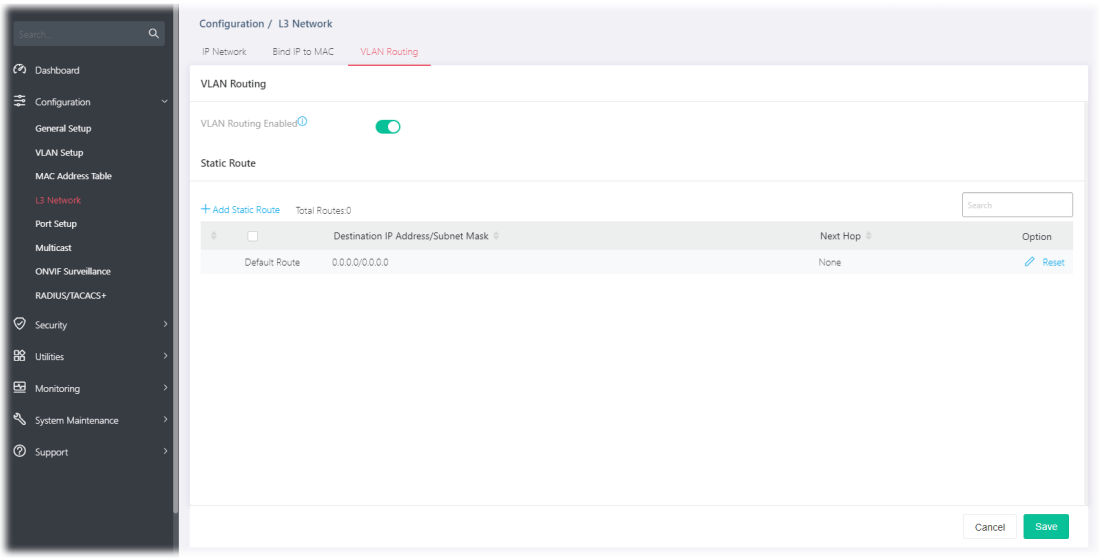
This page displays a table of DHCP servers used by "Bind IP to MAC".



Item	Description
IP Address	Displays the IP address of the DHCP server.
MAC Address	Displays the MAC address of the DHCP server.
Host ID	Displays the name of the DHCP server.
Lease Time Start	Displays the starting point of the lease time.
Lease Time End	Displays the ending point of the lease time.

II-4-3 VLAN Routing

Static routing is a process that the system network administrator can configure the network with all the required information for packet forwarding. Each VLAN can include several IP address with the same subnet. The network administrator can specify some IP addresses (with different subnets) and different VLANs for establishing a communication channel.

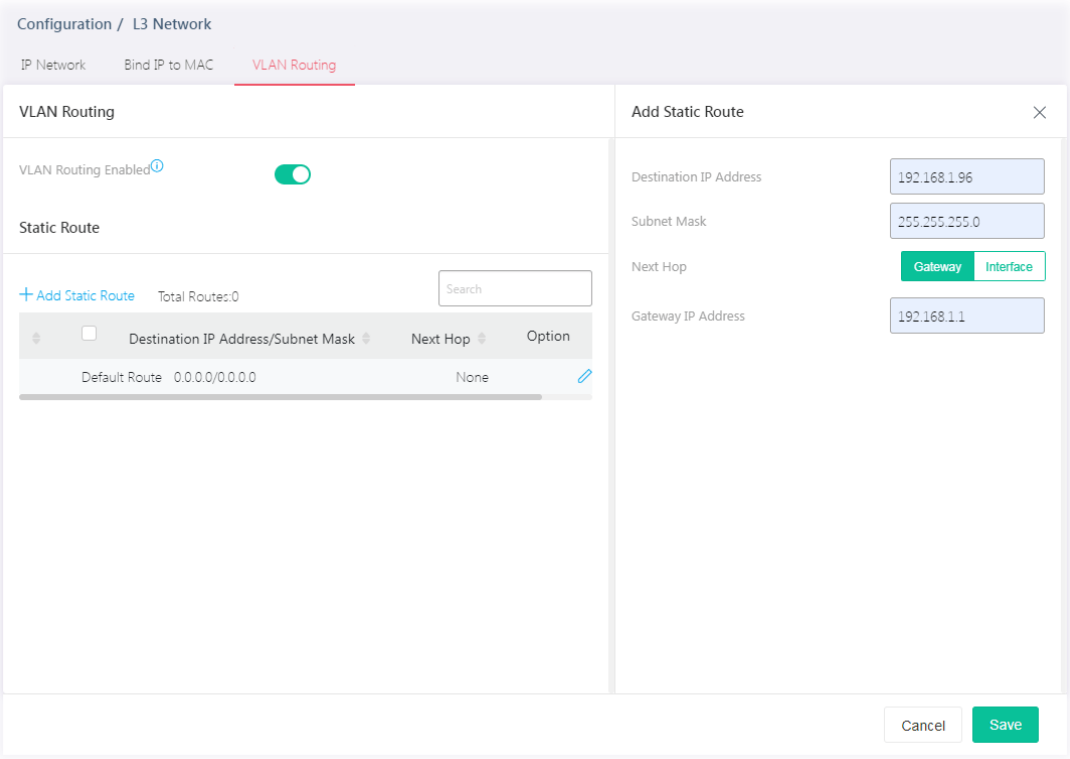


Available settings are explained as follows:

Item	Description
Vlan Routing	
VLAN Routing Enabled	Switch the toggle to enable / disable this function. - means "Enable". - means "Disable".
Static Route	
+Add Static Route	Create a new static route.
Destination IP Address/Subnet Mask	Displays the IP address/subnet mask of the static route.
Next Hop	Displays the type (none, gateway, interface) of the next hop.
Option	- Click to modify the settings of the selected entry.

	Reset - Click it to return to the factory default setting.

To add a new static route setting, click the "**+Add Static Route** " to open the edit page.



Available settings are explained as follows:

Item	Description
Destination IP Address	Enter the IP address.
Subnet Mask	Enter the subnet mask for the above IP address.
Next Hop	Select **Gateway** or **Interface** to enter the IP address or choose VLAN ID number.
Gateway IP Address	It is available when **Gateway** is selected as the Next Hop. Enter the IP address of the gateway.
Interface	It is available when **Interface** is selected as the Next Hop. Use the drop down list to specify the VLAN ID number.
OK	Save the settings.

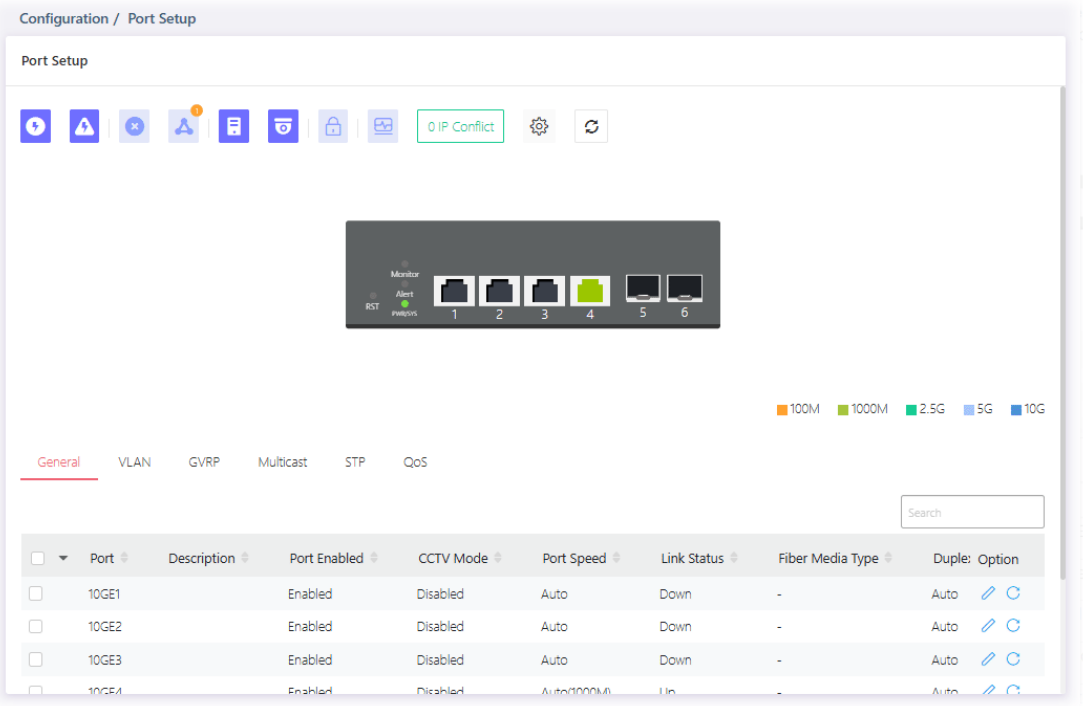
After finishing this web page configuration, please click **OK** to save the settings.

II-5 Port Setup

II-5-1 General

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

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

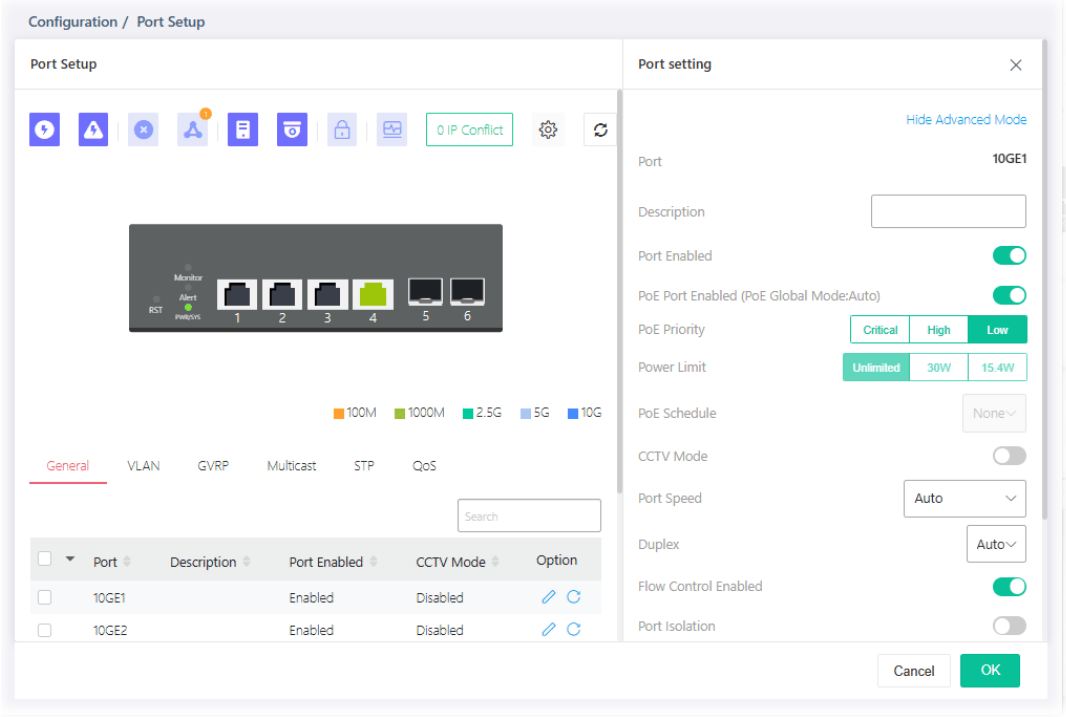


Available settings are explained as follows:

Item	Description
Port	Displays the LAN ports (2.5GE1 to 2.5GE24, 10GE1 to 10GE6).
Description	Displays the comment of the selected port.
Port Enabled	Displays the status (Enabled or Disabled) of the LAN port.
Port Speed	Displays the port speed capability.
Link Status	Displays the connection status.
Fiber Media Type	Displays the fiber media type of the LAN port.
Duplex	Displays the port duplex (auto/half/full) capability.
Flow Control Config	Displays if the function of Flow Control Config is enabled or disabled.
Flow Control Status	Displays the current operational status of Flow Control Config.

EEE Enable	Displays if the function of EEE is enabled or disabled.
EEE State	Displays the current operational status of EEE.
Option	- Click it to modify the port setting. - Clear current settings and return to factory default settings.

To modify settings for a port, click the link to open the setting page.



Available settings are explained as follows:

Item	Description
Port Setting	
Show / Hide Advanced Mode	Click to display or hide the advanced settings.
Port	Displays the port number.
Description	Enter a brief explanation for the selected port.
Port Enabled	Enable/disable the settings of the selected port.
PoE Port Enabled (PoE Global Mode: Auto)	Enable/disable the PoE feature of the selected port. If enabled, this port can be used for connecting the PoE device.
PoE Priority	Select Priority for PoE device. **Critical** - Set PoE device to highest priority connection. **High** –Set PoE device to high priority connection. **Low** –Set PoE device to low priority connection.
Power Limit	This setting is available when Manual is selected as PoE Mode. Enter the value (30W / 15.4W) as the maximum limit of power given to each physical port.

PoE Schedule	Specify the PoE port for applying the schedule. Before choosing, the PoE mode must be set as **Manual**. Use the drop down list to choose the schedule profile (from 1 to 15).
CCTV Mode	Enable/disable the settings of CCTV Mode.
Port Speed	Port speed capabilities: • **Auto:** Auto speed with all capabilities. • **Auto(100M):** Auto speed with 100M ability only. • **Auto(1000M):** Auto speed with 1000M ability only. • **Auto(2.5G):** Auto speed with 2.5G ability only. • **Auto(5G):** Auto speed with 5G ability only. • **Auto(10G):** Auto speed with 10G ability only. • **100M:** Force speed with 100M ability. • **1000M:** Force speed with 1000M ability. • **2.5G:** Force speed with 2.5G ability. • **5G:** Force speed with 5G 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 ability only.
Flow Control Enabled	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 / Disable** – Switch the toggle to enable / disable this function.  - means "Enable". - means "Disable".

Port Isolation	It allows the network administrator to configure protected port setting to prevent the selected ports from communication with each other. Port isolation is only allowed to communicate with unprotected port. For example, GE1 and GE3 are selected in Port List and Enable is clicked as port isolation, then users behind GE1 and GE3 are separated and can not communicate with each other. Enable / Disable – Switch the toggle to enable / disable this function.
LACP Priority	Enter a port priority number for the port.
LACP 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. Short - LACP PDU will be sent per second. If port member is not seen over 3 seconds, it will cause port member timeout. Long - LACP PDU will be sent every 30 seconds. If port member is not seen over 90 seconds, it will cause port member timeout.
EEE	Enable or disable port EEE (Energy Efficient Ethernet) function for the selected port.

After finishing this web page configuration, please click OK to save the settings.

II-5-2 VLAN

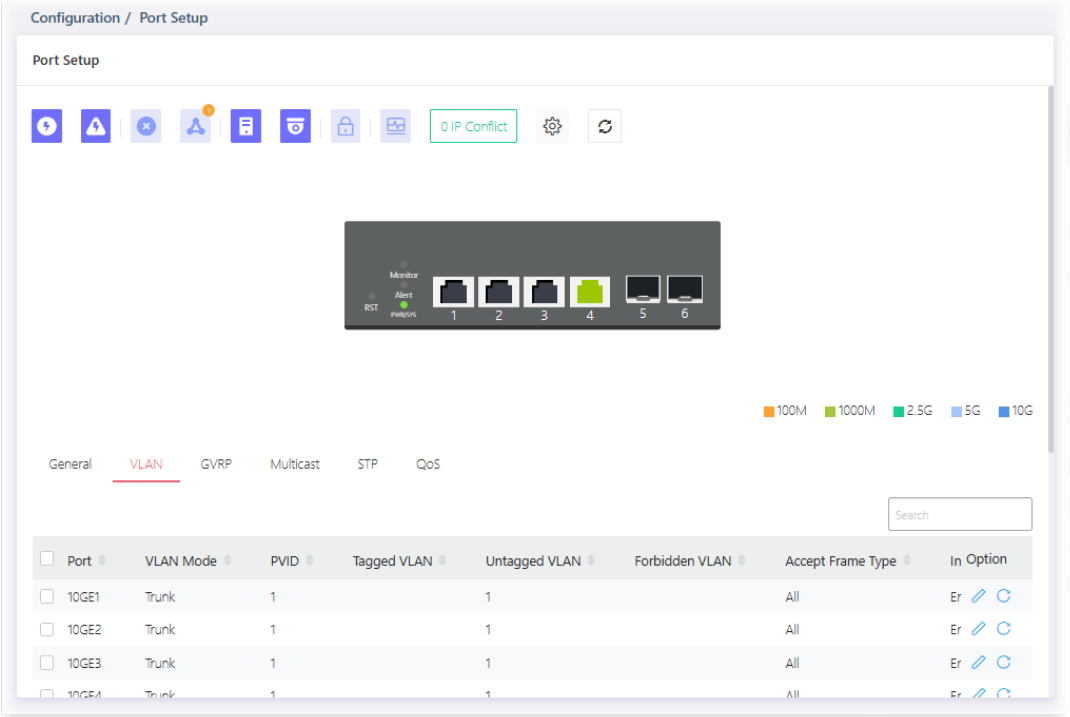
This page allows a user to configure interface (GE) settings related to VLAN.

Voice VLAN

With voice VLAN, 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 priority tag to speed up the packet transmission. The voice VLAN is only active inside VigorSwitch for packet transmission. After these packets leave VigorSwitch, the Voice VLAN tag will be removed immediately.

Surveillance VLAN

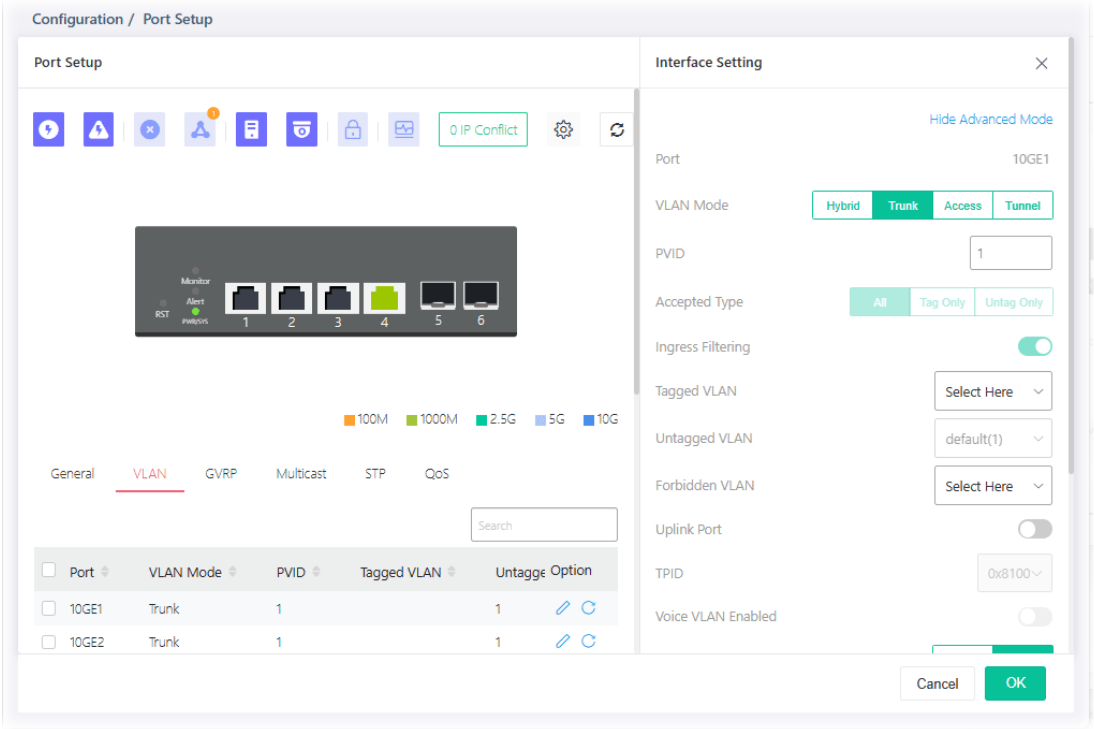
Surveillance VLAN can be configured for VigorSwitch to identify the packets coming from an IP camera automatically and assign those traffics to a specific VLAN ID and CoS/802.1p value, this helps you to prioritize those traffics and improve video quality.



Available settings are explained as follows:

Item	Description
Port	Displays the LAN port number.
VLAN Mode	Displays VLAN mode of the interface.
PVID	Displays the Port VLAN ID of the interface.
Tagged VLAN	Displays the VLAN profile (ID number) tagged in the VLAN interface.
Untagged VLAN	Displays the VLAN profile (ID number) untagged in the VLAN interface.
Forbidden VLAN	Displays the VLAN profile (ID number) used by the VLAN interface.
Accept Frame Type	Displays the acceptable-frame-type of the specified interfaces.
Ingress Filtering	Displays the status (enabled/disabled) of ingress filtering.
Option	- Click it to modify the VLAN interface settings. - Clear current settings and return to factory default settings.

To modify settings for a port, click the link to open the setting page.



Available settings are explained as follows:

Item	Description
Interface Setting	
Show / Hide Advanced Mode	Click to display or hide the advanced settings.
Port	Displays the selected LAN port number.
VLAN Mode	Select the VLAN mode of the interface. **Hybrid** – Support all functions as defined in IEEE 802.1Qspecification. **Trunk** - An untagged member of one VLAN at most, and is a tagged member of zero or more VLANs. **Access** – Accepts only untagged frames and join an untagged VLAN. **Tunnel** - Accepts only untagged frames and join an untagged VLAN.
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.

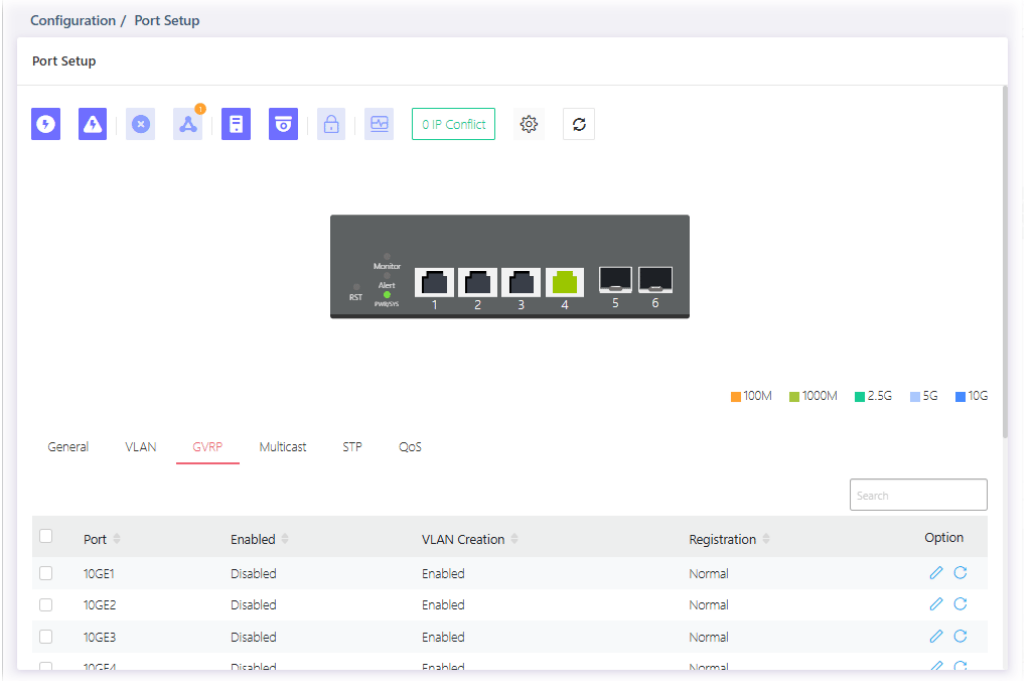
Tagged VLAN	Specify the VLAN profile tagged in the VLAN.
Untagged VLAN	Specify the VLAN profile untagged in the VLAN.
Below shows settings for Advanced Mode	
Forbidden VLAN	The selected GE port only allows default VLAN packet to pass through. **Enable / Disable** – Switch the toggle to enable / disable the LAN port(s) as forbidden VLAN port.  - means "Enable". - means "Disable".
Voice VLAN Enabled	**Enable / Disable** – Switch the toggle to enable / disable the LAN port(s) as Voice VLAN port.
Voice VLAN CoS Mode	**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.
Surveillance VLAN Enabled	**Enable / Disable** – Switch the toggle to enable / disable the LAN port(s) as Surveillance VLAN port.  - means "Enable". - means "Disable".
Surveillance VLAN 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.
Surveillance VLAN 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.
MAC VLAN Binding	Enable/disable the function of MAC VLAN Binding. **+Add -** Click to create a new MAC VLAN binding profile.
Protocol VLAN Binding	Click to create a new protocol VLAN binding profile. **+Add -** Click to create a new protocol VLAN binding profile.

After finishing this web page configuration, please click **OK** to save the settings.

II-5-3 GVRP

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.

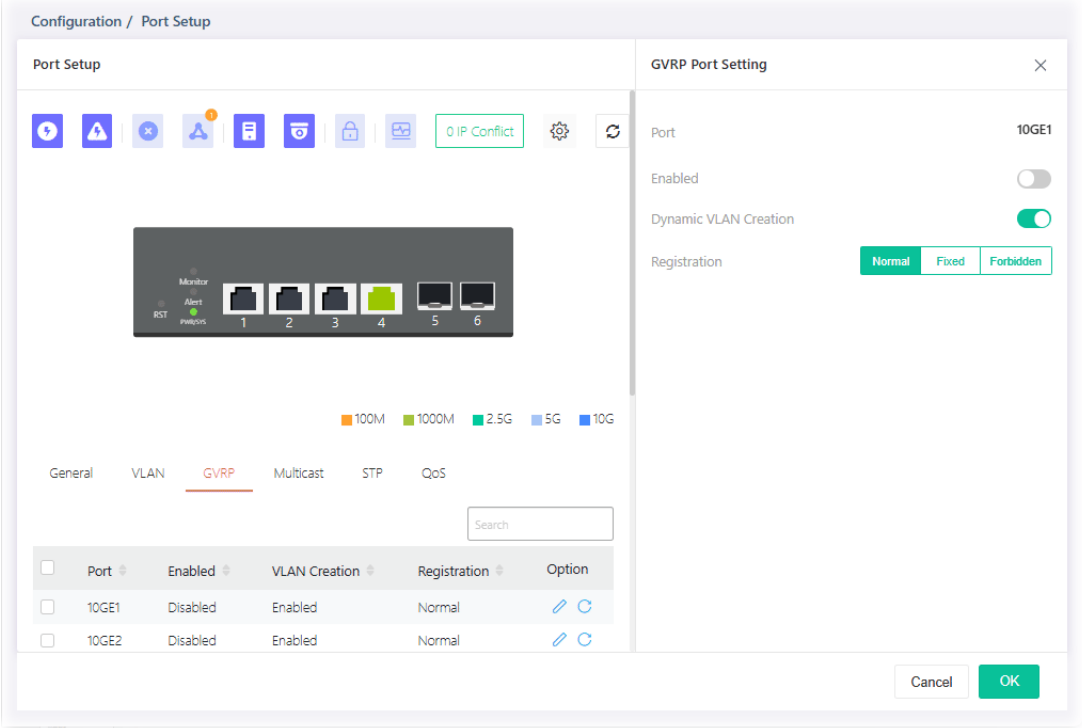
Such function can eliminate unnecessary network traffic and prevent any attempt to transmit information to unregistered users.



Available settings are explained as follows:

Item	Description
Port	Displays the LAN port number.
Enabled	Displays the status (Enabled/Disabled) of the GVRP port setting.
VLAN Creation	Displays the status (Enabled/Disabled) of the VLAN Creation.
Registration	Displays the registration mode for each GE/LAG port.
Option	- Click it to modify the GVRP settings. - Clear current settings and return to factory default settings.

To modify settings for a port, click the link to open the setting page.



Available settings are explained as follows:

Item	Description
GVRP Portsetting	
Port	Displays the port number.
Enabled	**Enable / Disable** – Switch the toggle to enable / disable the GVRP port setting. - means "Enable". - means "Disable".
Dynamic VLAN Creation	Switch the toggle to enable / disable the VLAN creation.
Registration	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.
OK	Save the settings.

After finishing this web page configuration, please click **OK** to save the settings.

II-5-4 Multicast

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.

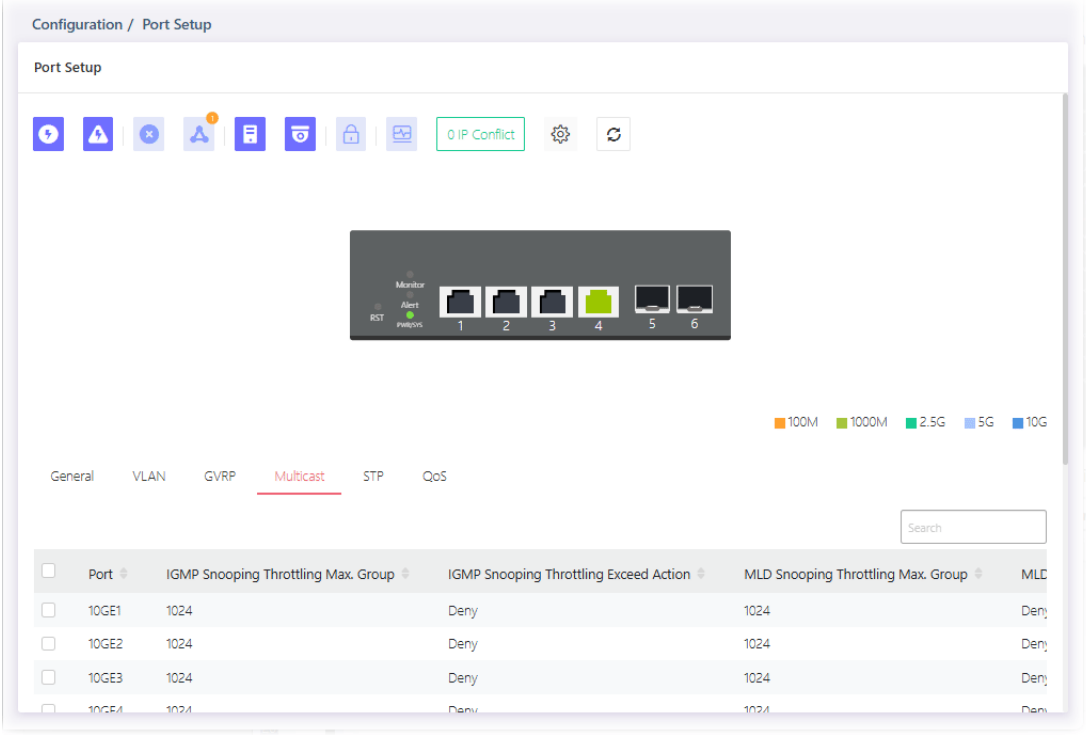
MLD Snooping

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.

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 (0~256) 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.

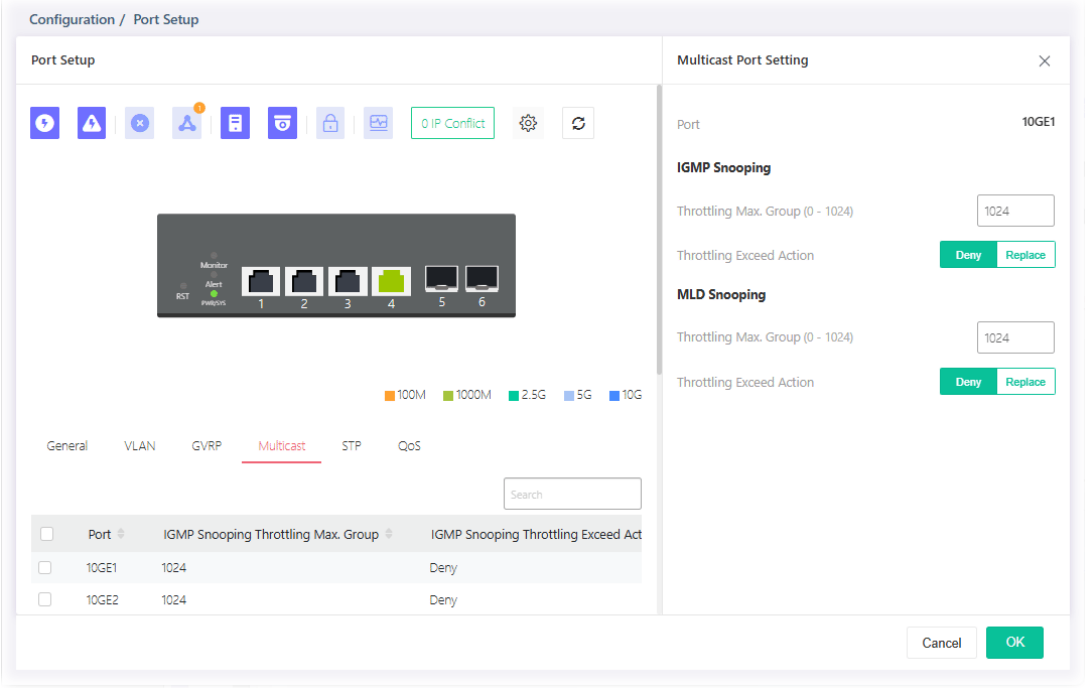


Available settings are explained as follows:

Item	Description
Port	Displays the GE/LAG port number.
IGMP Snooping Throttling Max. Group	Displays the maximum number of IGMP group profile.

IGMP Snooping Throttling Exceed Action	Displays the action performed when the number of IGMP join reports for the specified interface exceeds the value defined in Max Group.
MLD Snooping Throttling Max. Group	Displays the maximum number of MLD group profile.
MLD Snooping Throttling Exceed Action	Displays the action performed when the number of MLD join reports for the specified interface exceeds the value defined in Max Group.
Option	- Click it to modify the multicast settings for each port. - Clear current settings and return to factory default settings.

To modify settings for a port, click the link to open the setting page.



Available settings are explained as follows:

Item	Description
Multicast Port Setting	
Port	Displays the port number.
IGMP Snooping	
Throttling 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).
Throttling Exceed Action	VigorSwitch will perform the action defined below when the number of IGMP join reports for the specified interface exceeds the 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.
MLD Snooping	
Throttling 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).
Throttling Exceed Action	VigorSwitch will perform the action defined below when the number of MLD join reports for the specified interface exceeds the 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.
OK	Save the settings.

After finishing this web page configuration, please click OK to save the settings.

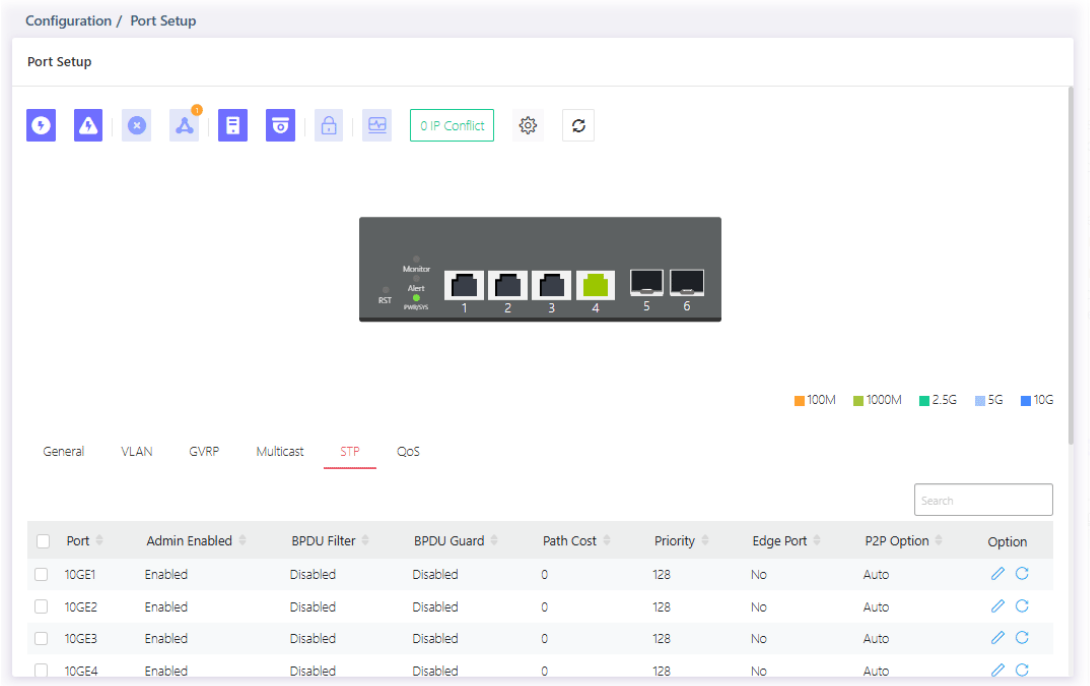
II-5-5 STP

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.

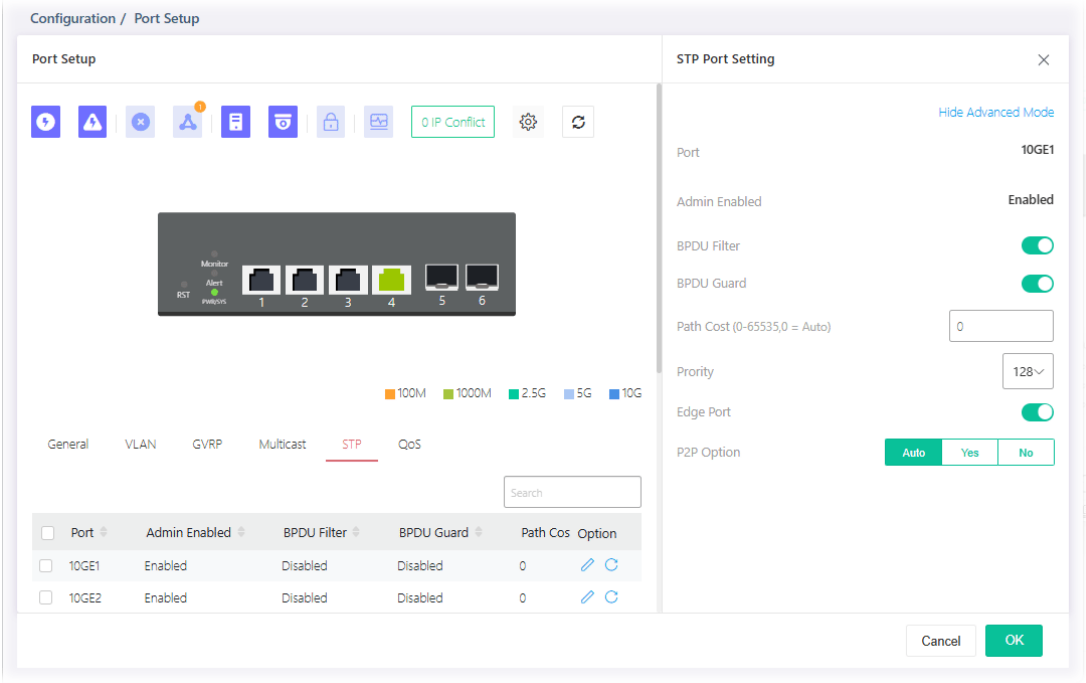


Available settings are explained as follows:

Item	Description
Port	Displays the LAN port number (10GE1 to 10GE6, LAG1 to LAG8).
Admin Enabled	Displays the status (enabled/disabled) of Admin Enabled.
BPDU Filter	Displays the status (enabled/disabled) of BPDU Filter function.
BPDU Guard	Displays the status (enabled/disabled) of BPDU Guard function.
Path Cost	Displays the value of transmitting a frame onto a LAN through that port.
Priority	Displays the priority value for the port interface.
Edge Port	Displays the status (enabled/disabled) of Edge Port function.

P2P Option	Displays the STP of link type (All, Yes, No) on this port.
Option	- Click it to modify the STP port setting. - Clear current settings and return to factory default settings.

To modify settings for a port, click the link to open the setting page.



Available settings are explained as follows:

Item	Description
STP Port Setting	
Show / Hide Advanced Mode	Click to display or hide the advanced settings.
Port	Displays the selected LAN port number.
Admin Enabled	Displays the status of Admin Enabled.
BPDU Filter	Switch the toggle to enable / disable the function of dropping all BPDU packets and no BPDU will be sent. - means "Enable". - means "Disable".
BPDU Guard	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.
Path Cost	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. Switch the toggle to enable / 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.

After finishing this web page configuration, please click **OK** to save the settings.

II-5-4 QoS

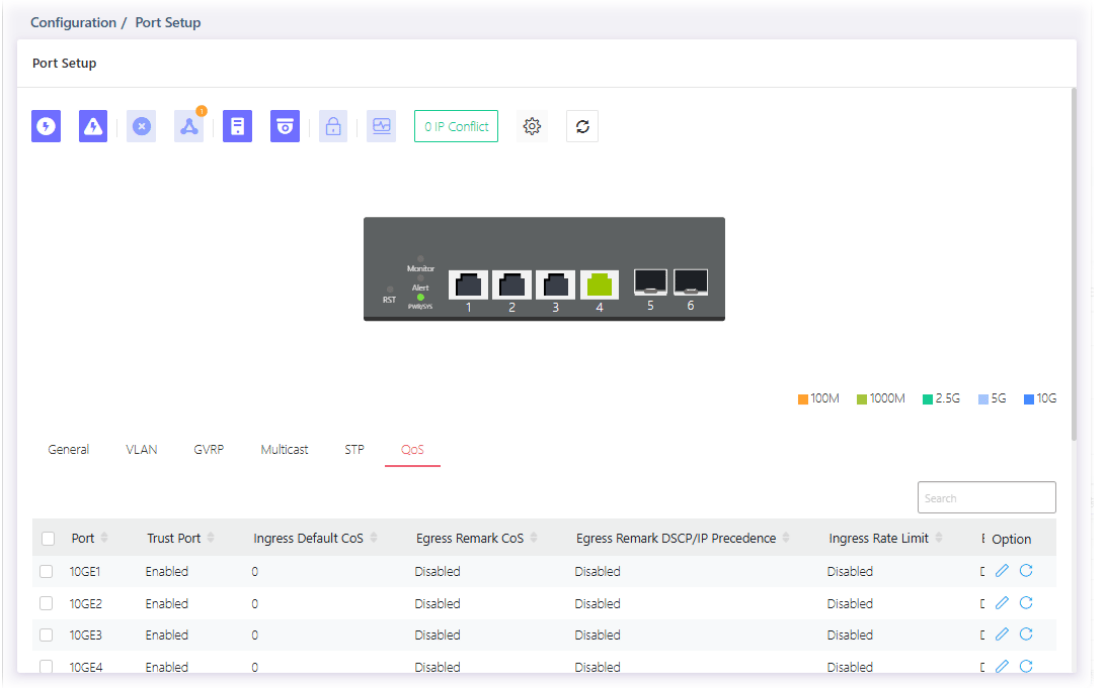
This page is used to configure port settings for QoS. The configuration result for each port will be displayed on the table listed on the lower side of this web page.

Ingress Rate Limit

It 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.

Egress Shaping Rate

It 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.

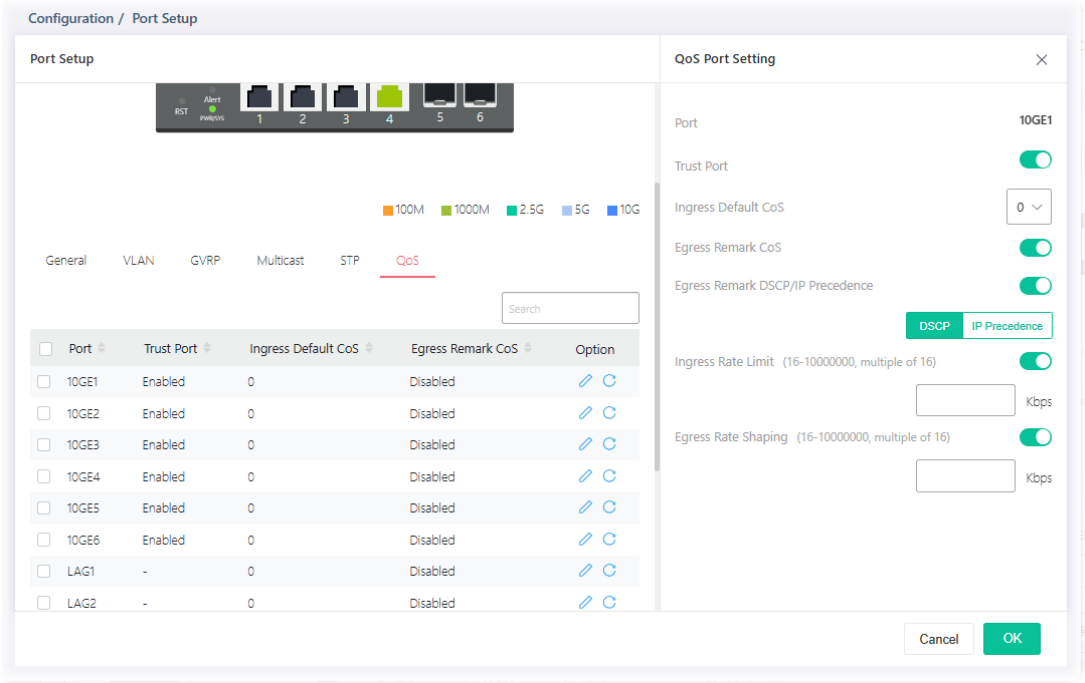


Available settings are explained as follows:

Item	Description
Port	Displays the port profiles (10GE1 to 10GE6, LAG1 to LAG8).
Trust Port	Displays if the traffic follow the trust mode in general setting (Enabled/Disabled).
Ingress Default CoS	Displays the default CoS priority value for those ingress frames.
Egress Remark CoS	Displays the status (Enabled/Disabled) of the function.
Egress Remark DHCP/IP Precedence	Displays the status (Enabled/Disabled) of the function.
Ingress Rate Limit	Displays the value of the ingress rate limit. If this function is disabled, then Off will be shown instead.
Egress Rate Shaping	Displays the value of the egress rate shaping. If this function is disabled, then Off will be shown instead.

Option	- Click it to modify the QoS port setting. - Clear current settings and return to the factory default settings.

To modify settings for a port, click the link to open the setting page.



Available settings are explained as follows:

Item	Description
QoS Port Setting	
Port	Displays the port profiles (10GE1 to 10GE6, LAG1 to LAG8).
Trust Port	Switch the toggle to enable / disable this function. - Traffic will follow trust mode in general setting. - No QoS service for this port.
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).
Egress Remark CoS	**Enable / Disable** – Switch the toggle to enable / disable this function.
Egress Remark DSCP/IP Precedence	Switch the toggle to enable / disable this function. **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.
Ingress 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.

	Switch the toggle to enable / disable this function. Enter the rate value,<16-1000000>,unit:16 Kbps.
Egress Rate Shaping	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. Switch the toggle to enable / disable this function. Enter the rate value,<16-1000000>,unit:16 Kbps.

After finishing this web page configuration, please click **OK** to save the settings.

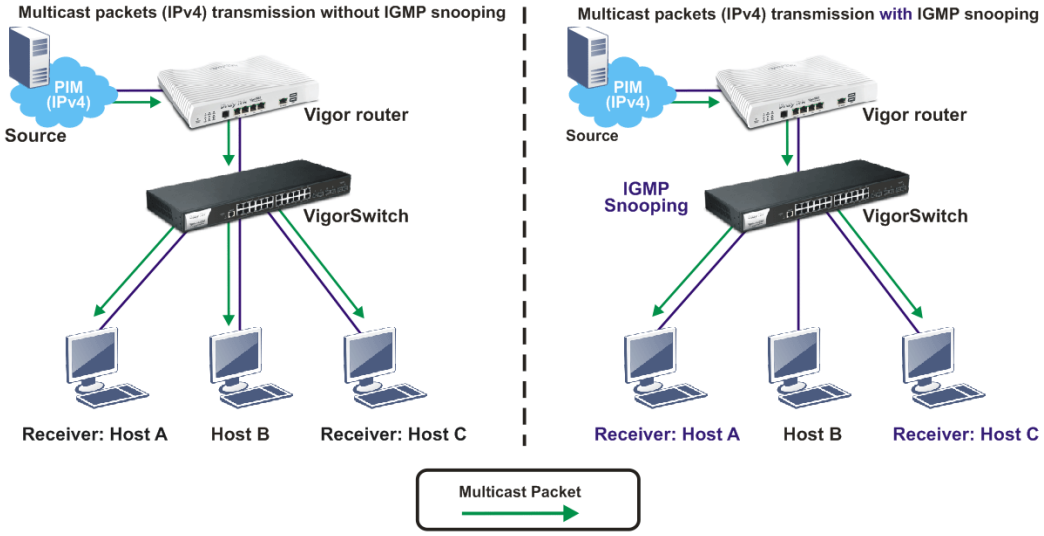
II-6 Multicast

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

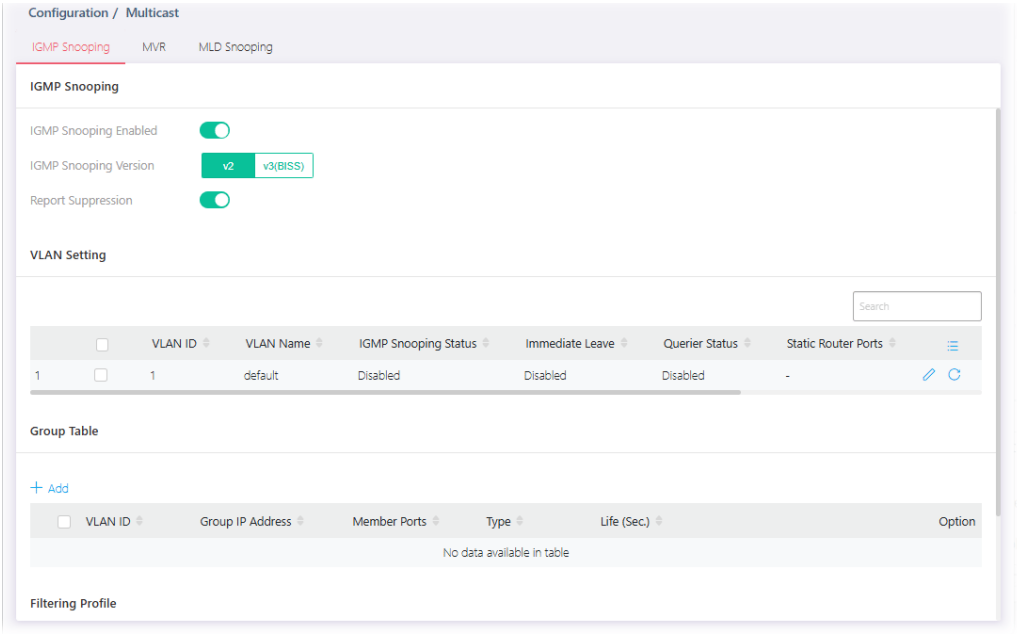
To avoid the incoming data broadcasting to all GE ports, multicast is useful to transfer the data/message to specified GE ports for IGMP snooping. When VigorSwitch receives a message "subscribed" by the client, it must decide to transfer the data to specified GE ports according to the location of the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

II-6-1 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-6-1-1 IGMP Snooping

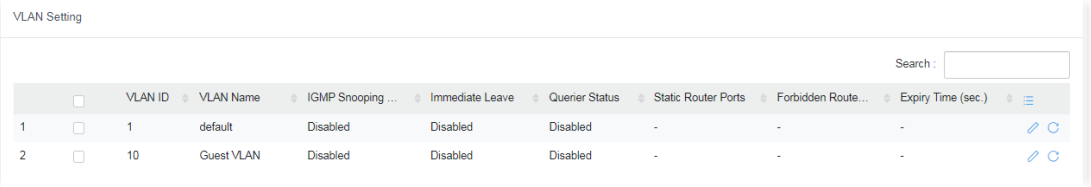


Available settings are explained as follows:

Item	Description
IGMP Snooping Enable	**Enable / Disable** – Switch the toggle to enable / disable this function. - means "Enable". - means "Disable".
IGMP Snooping Version	Set the IGMP snooping version. **v2 -** Only support process IGMP v2 packet. **v3** - Support v3 basic and v2.
Report Suppression	It allows the switch to handle IGMP reports between router and host, suppressing bandwidth used by IGMP. Switch the toggle to enable / disable this function. - means "Enable". - means "Disable".

II-6-1-2 VLAN Setting

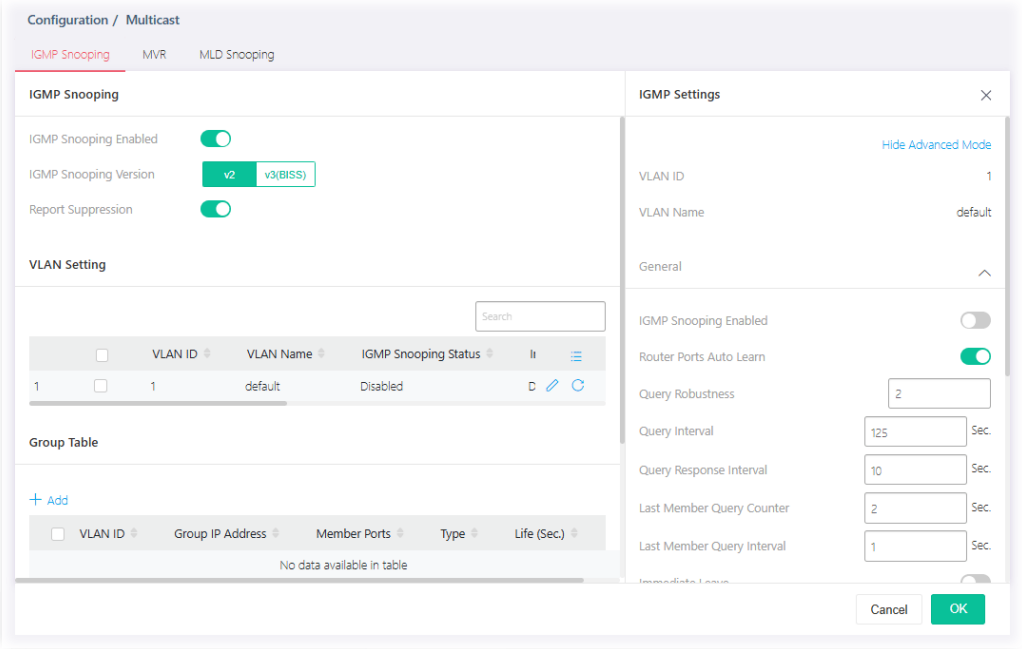
This page allows you to enable/disable IGMP function, select snooping version, and enable/disable snooping report suppression.



Available settings are explained as follows:

Item	Description
VLAN ID	Displays the VLAN ID number of the VLAN profile.
VLAN Name	Displays the name of the VLAN profile.
IGMP Snooping Status	Displays the status (Enabled/Disabled) of the IGMP function.
Immediate Leave	Displays the status (Enabled/Disabled)
Querier Status	Displays the status (Enabled/Disabled) of IGMP querier function.
Static Router Ports	Displays the LAN Port (GE/LAG) to send out query to remote host.
Forbidden Router Ports	Displays the forbidden LAN Port (GE/LAG).
Expiry Time (sec.)	Displays the time before querier is considered no longer existed.
	Click it to modify the IGMP setting.
	Clear current settings and return to factory default settings.

To modify settings for a port, click the link to open the setting page.



Available settings are explained as follows:

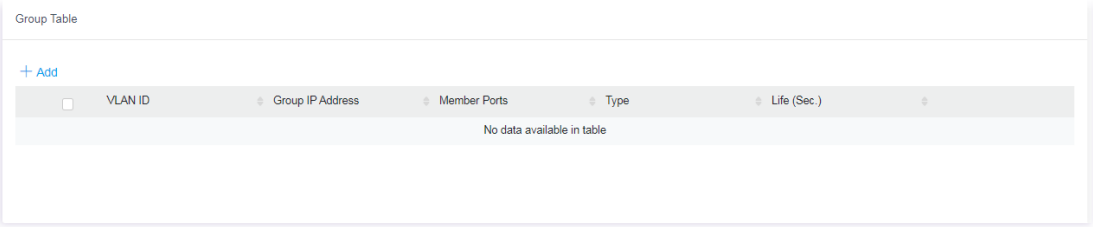
Item	Description
IGMP Setting	
Show / Hide Advanced Mode	Click to display or hide the advanced settings.
VLAN ID	Displays the VLAN ID number of the VLAN profile.
VLAN Name	Displays the name of the VLAN profile.
General	**IGMP Snooping Enabled** – Switch the toggle to enable / disable this IGMP snooping function.  - means “Enable”. - means “Disable”.
Below shows settings for Advanced Mode	
Router Ports Auto Learn	Switch the toggle to enable / disable this function. Set the enabling status of IGMP router port learning. The server will 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 to send the 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 querying 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.
IGMP Querier	**IGMP Querier Enable -** Switch the toggle to enable / disable this function. In **Advanced Mode,** **Querier Version** - Set the IGMP snooping version. ● **v2 -** Only support process IGMP v2 packet. ● **v3** - Support v3 basic and v2. For maximum compatibility, it is suggested to use querier version lower than IGMP snooping version, for there is possible network mixed with IGMP v2/v3 client and v2 query message is widely understandable for those clients.
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. **Enable / Disable** – Switch the toggle to enable / disable this function. **+Add** - Click to create a new group. ● **Group IP Address** - Specify the IPv4 multicast address you wish to assign for the static group (defined in VLAN ID).

	• **Member Ports** - Specify the port(s) that static group with given IPv4 multicast address shall include.
IGMP Router	**Static Router Ports** - Specify LAN Port (GE/LAG) to send out query to remote host. **Forbidden Router Ports** - Use the drop down list to specify forbidden LAN Port (GE/LAG).
IGMP Forward All	**Static Forward All 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 Forward All 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.

After finishing this web page configuration, please click **OK** to save the settings.

II-6-1-3 Group Table

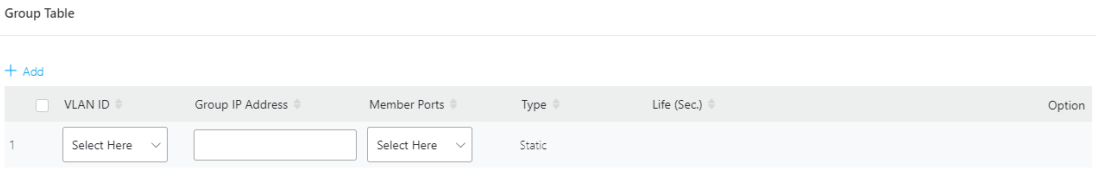
This page shows currently known and dynamically learned by IGMP snooping or shows the assigned IPv4 multicast address group in operation.



Available settings are explained as follows:

Item	Description
+Add	Click to create a new profile.
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.

To add a new group, click the **+Add** link to open the setting page.



Available settings are explained as follows:

Item	Description
VLAN ID	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.

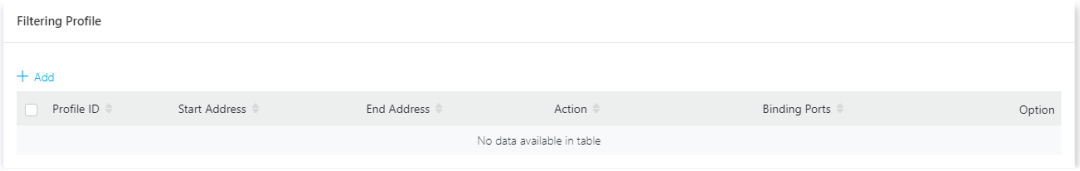
After finishing this web page configuration, please click **OK** to save the settings.

II-6-1-4 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.

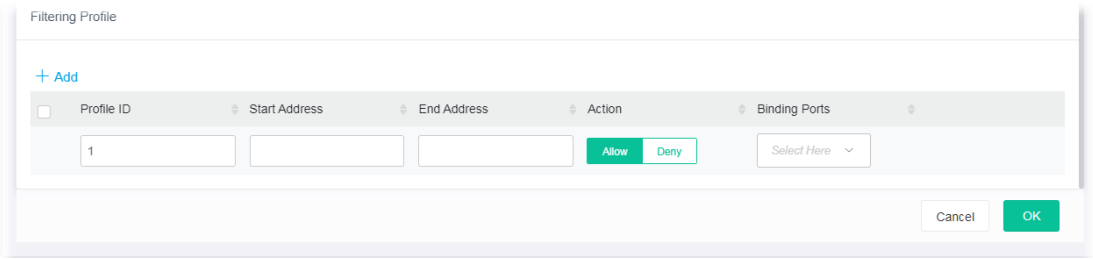
In addition, such filtering profile is only effective for controlling the query for multicast. It has nothing to do with the general IGMP query.



Available settings are explained as follows:

Item	Description
+Add	Click to create a new profile.
Profile ID	Displays the index number of a filtering profile.
Start Address	Displays the starting point for the IP range.
End Address	Displays the ending point for the IP range.
Action	Displays the action performed for this profile.
Binding Ports	Displays the interface (GE/LAG) selected for this profile.

To add a new profile, click the **+Add** link to open the setting page.



Available settings are explained as follows:

Item	Description

+Add	Click to have new fields for creating a new profile.
Profile ID	Enter 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	**Allow** – When it is selected, the request for multicast traffic will be forwarded to the multicast group normally. **Deny –** It is default setting. The forwarding request of multicast traffic will be discarded.
Binding Ports	Select the GE/LAG port(s) (interfaces) for filtering profile to process multicast traffic.
OK	Save the settings.

After finishing this web page configuration, please click **OK** to save the settings.

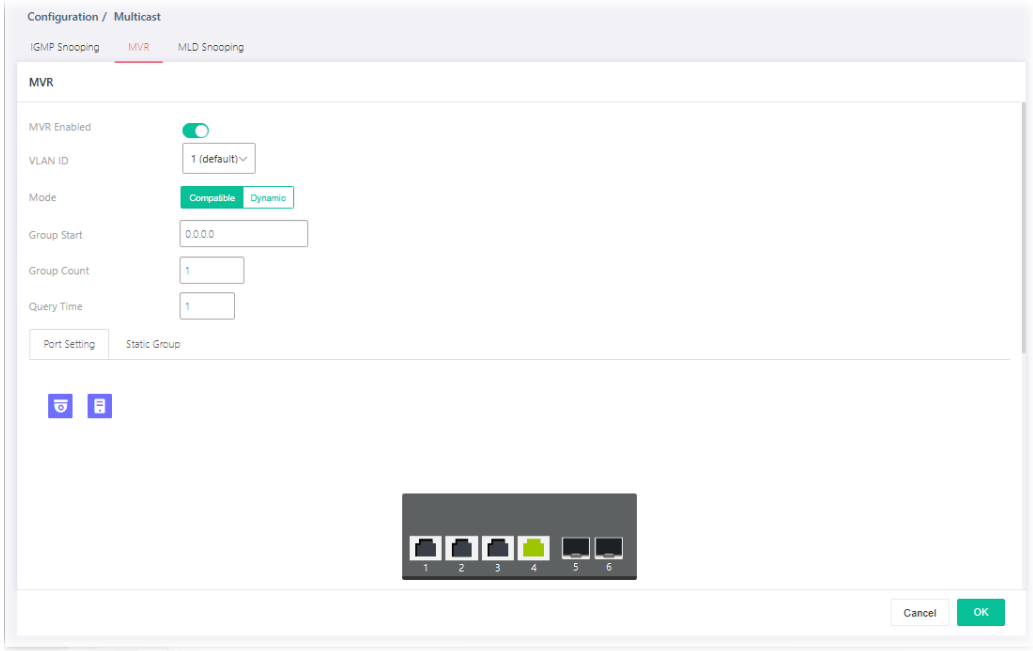
II-6-2 MVR

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



Available settings are explained as follows:

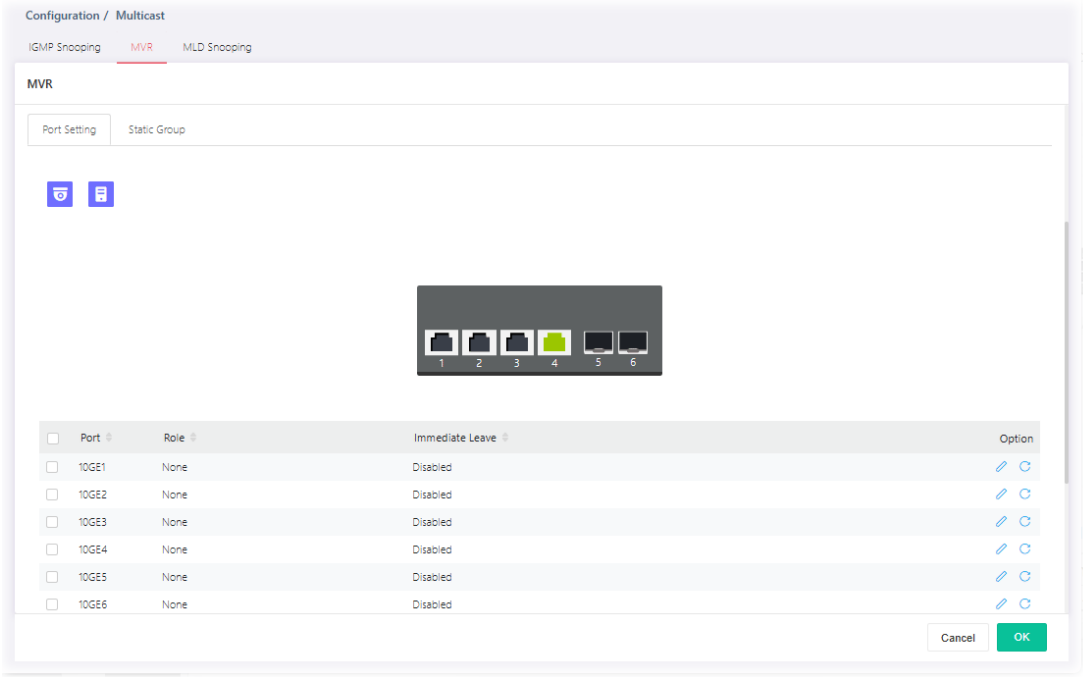
Item	Description

MVR Enabled	Switch the toggle to enable / disable the MVR function.  - means “Enable”. - means “Disable”.
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.
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 VigorSwitch 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 VigorSwitch; 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.
OK	Save the settings.

After finishing this web page configuration, please click **OK** to save the settings.

II-6-2-1 Port Setting

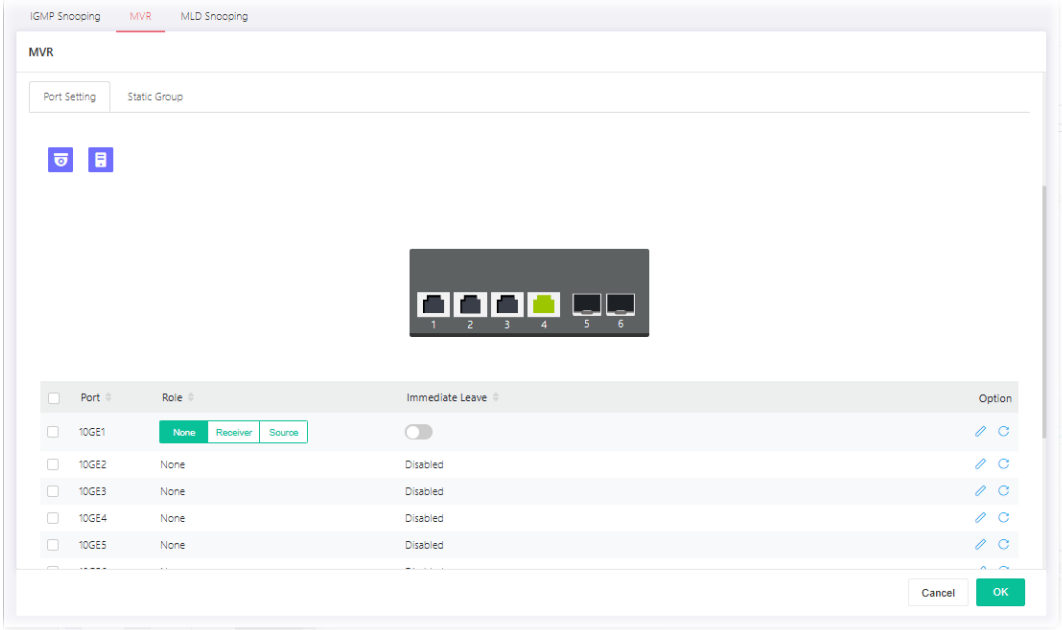
It is necessary to specify destination port and source port (GE/LAG) for Vigor system to perform MVR operation.



Available settings are explained as follows:

Item	Description
Port	Displays the index number of the LAN Port (GE/LAG).
Role	Displays the role (None, Receiver or Source) of the port.
Immediate Leave	Displays the status (enable/disable) of the immediate leave function.
Option	- Click it to modify the port setting for MVR. - Clear current settings and return to factory default settings.

To modify settings for a port, click the link to open the setting page.



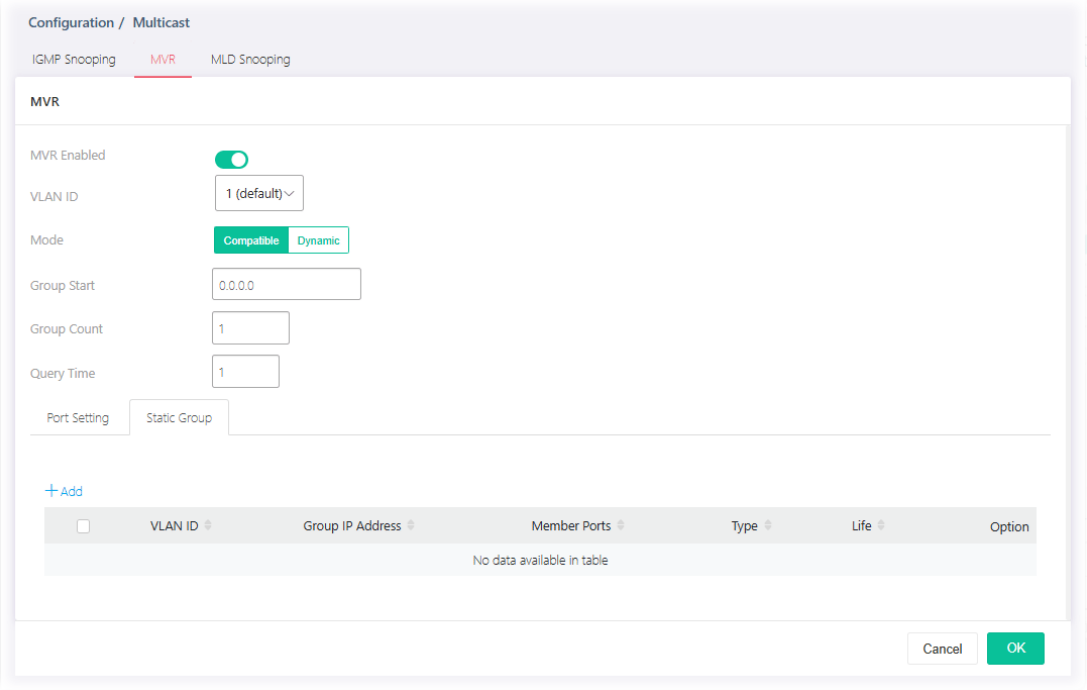
Available settings are explained as follows:

Item	Description
Port	Each port can be set as Receiver or Source port respectively.
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	**Enable** – Enable the function of the 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. **Disable** – Disable the function of immediate leave.
OK	Save the settings.

After finishing this web page configuration, please click **OK** to save the settings.

II-6-2-2 Static Group

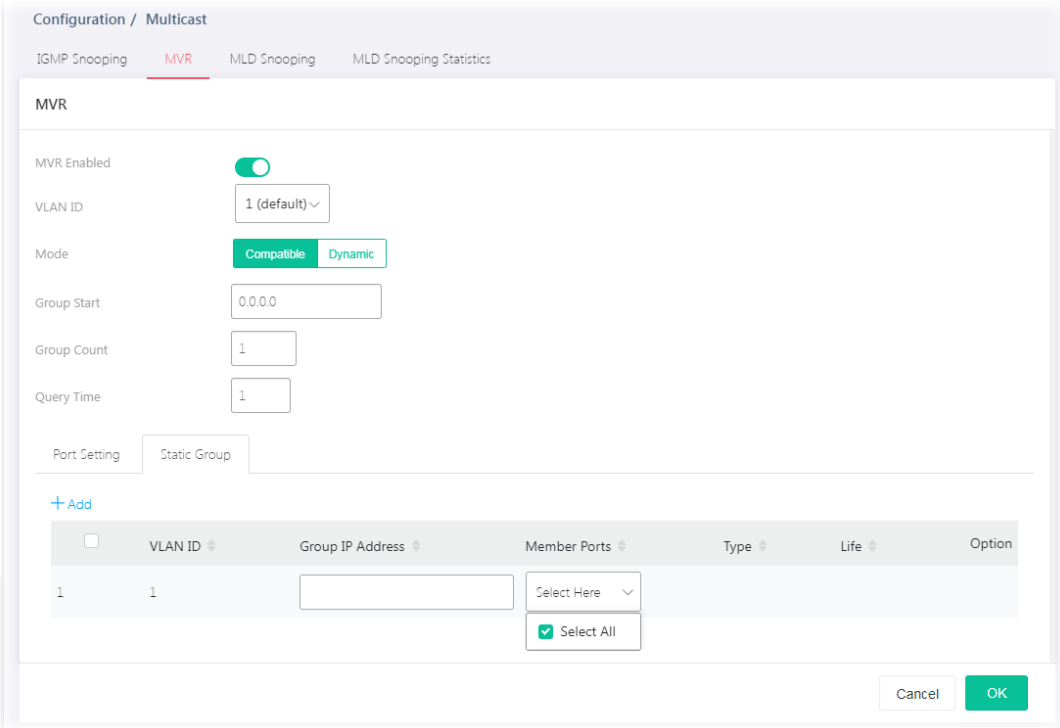
The MLD static group is allowed to assign a VLAN/port as a specific IP multicast member. Every IP multicast stream that belongs to the specified group IP address will be forwarded to the specified port/VLAN member.



Available settings are explained as follows:

Item	Description
+Add	Click to have new fields for creating a new profile.
VLAN ID	Displays the ID number of the VLAN.
Group IP Address	Displays the IP address(es).
Member Ports	Displays the GE/LAG port to be grouped under the selected VLAN.
Type	Displays if it is dynamically learned or statically assigned.
Life	Displays the life time of this multicast member left if no membership report sent again.

To add a new profile, click the **+Add** link to open the setting page.

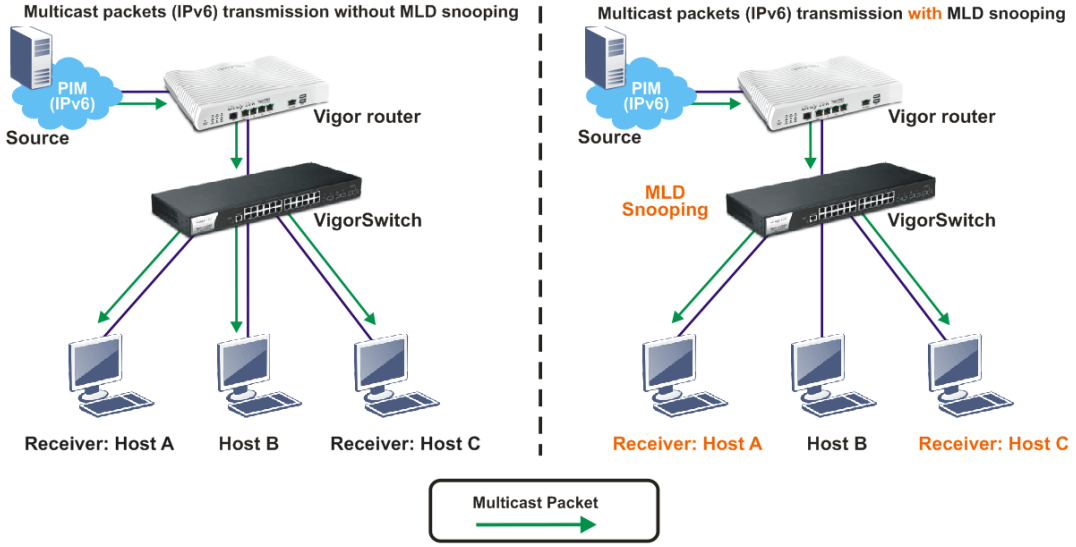


Available settings are explained as follows:

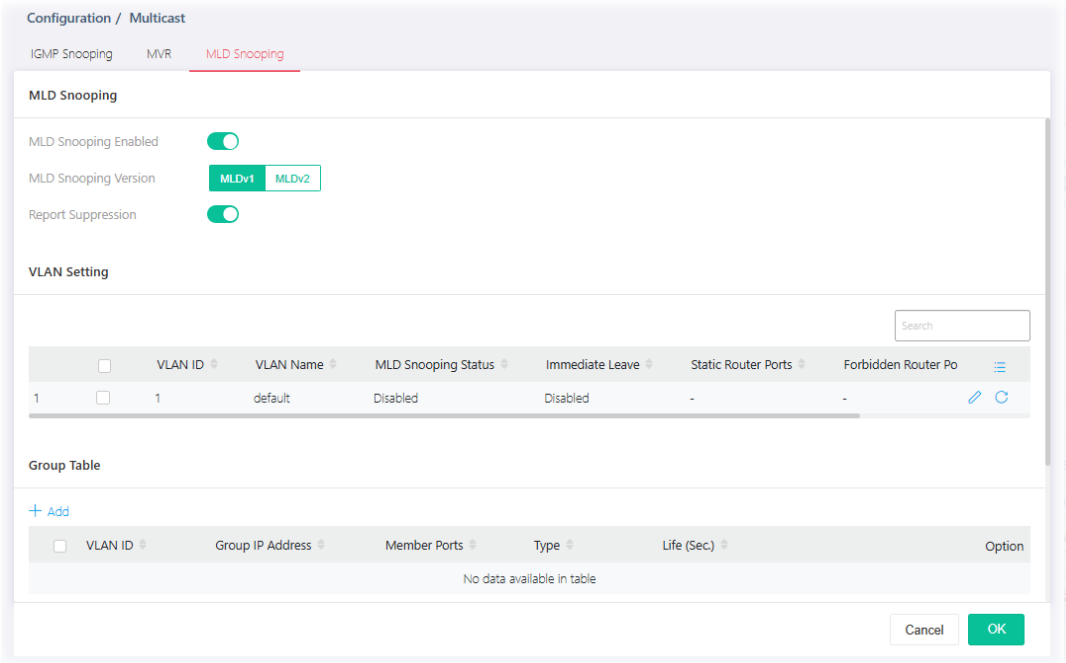
Item	Description
VLAN ID	Display the ID number of the VLAN.
Group IP Address	Define a range of IP address(es) with the format of "xxx.xxx.xxx.xxx – xxx.xxx.xxx.xxx".
Member Ports	Choose GE/LAG port to be grouped under the selected VLAN.
OK	Save the settings.

II-6-3 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-6-3-1 MLD Snooping



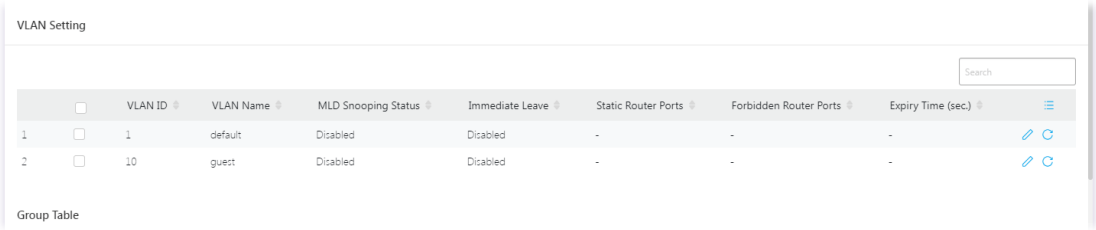
Available settings are explained as follows:

Item	Description
MLD Snooping Enabled	**Enable / Disable** – Switch the toggle to enable / disable this function. - means "Enable".

	- means “Disable”.
MLD Snooping 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	It allows the switch to handle MLD reports between router and host, suppressing bandwidth used by MLD. Switch the toggle to enable / disable this function. - means “Enable”. - means “Disable”.
OK	Save the settings.

II-6-3-2 VLAN Setting

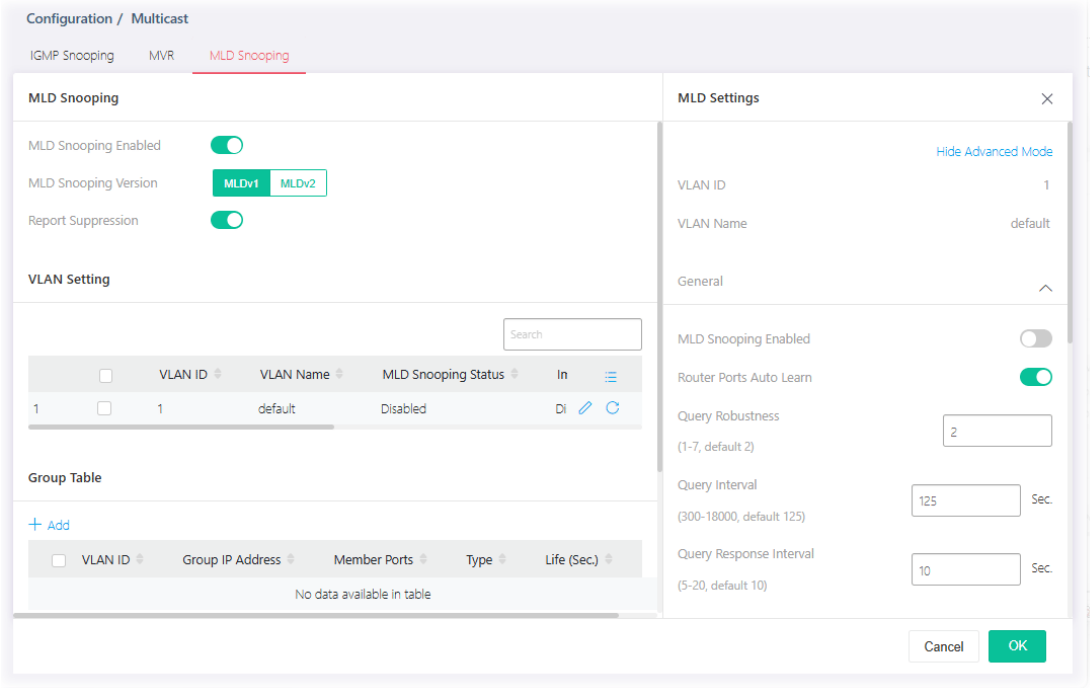
This page allows you to enable/disable MLD snooping function, select snooping version, and enable/disable snooping report suppression.



Available settings are explained as follows:

Item	Description
VLAN ID	Displays the VLAN ID number of the VLAN profile.
VLAN Name	Displays the name of the VLAN profile.
MLD Snooping Status	Displays the status (Enabled/Disabled) of the MLD snooping function.
Immediate Leave	Displays the status (Enabled/Disabled) of the immediate leave function.
Static Router Ports	Displays the LAN Port (GE/LAG) to send out query to remote host.
Forbidden Router Ports	Displays the forbidden LAN Port (GE/LAG).
Expiry Time (sec.)	Displays the time before querier is considered no longer existed.
	Click it to modify the MLD setting.
	Clear current settings and return to factory default settings.

To modify settings for a port, click the link to open the setting page.



Available settings are explained as follows:

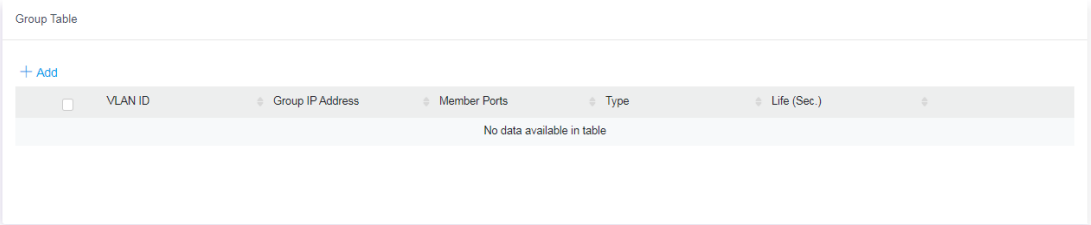
Item	Description
MLD Setting	
Show / Hide Advanced Mode	Click to display or hide the advanced settings.
VLAN ID	Displays the VLAN ID number of the VLAN profile.
VLAN Name	Displays the name of the VLAN profile.
General	**MLD Snooping Enabled** – Switch the toggle to enable / disable this MLD snooping function. - means "Enable". - means "Disable".
Below shows settings for Advanced Mode	
Router Ports Auto Learn	Switch the toggle to enable / disable this function. Set the enabling status of MLD router port learning. The server will 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 to send the 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 querying 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. Switch the toggle to enable Fastleave function.
MLD Static Group	The MLD static group is allowed to assign a VLAN/port as a specific IPv4 multicast member. Every IPv6 multicast stream that belongs to the specified group IP address will be forwarded to the specified port/VLAN member. **+Add** - Click to create a new group. ● **Group IP Address** - Specify the IPv6 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 IPv6 multicast address shall include.
MLD Router	**Static Router Ports** - Specify LAN Port (GE/LAG) to send out query to remote host. **Forbidden Router Ports** - Use the drop down list to specify forbidden LAN Port (GE/LAG).
MLD Forward All	**Static Forward All 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 Forward All 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.

After finishing this web page configuration, please click **OK** to save the settings.

II-6-3-3 Group Table

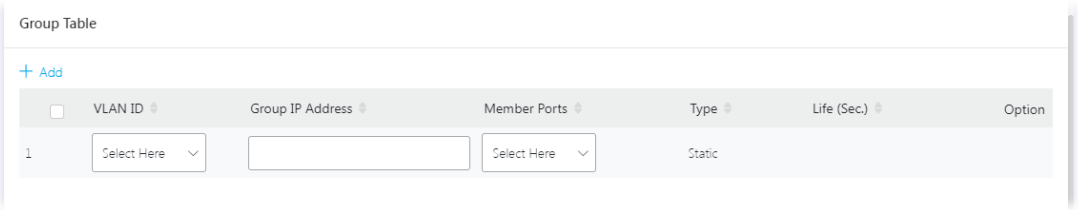
This page shows currently known and dynamically learned by IGMP snooping or shows the assigned IPv4 multicast address group in operation.



Available settings are explained as follows:

Item	Description
+Add	Click to create a new profile.
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.

To add a new group, click the **+Add** link to open the setting page.



Available settings are explained as follows:

Item	Description
VLAN ID	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 IPv6 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.

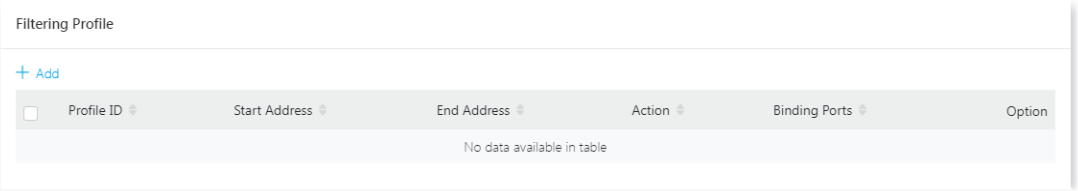
After finishing this web page configuration, please click **OK** to save the settings.

II-6-3-4 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.

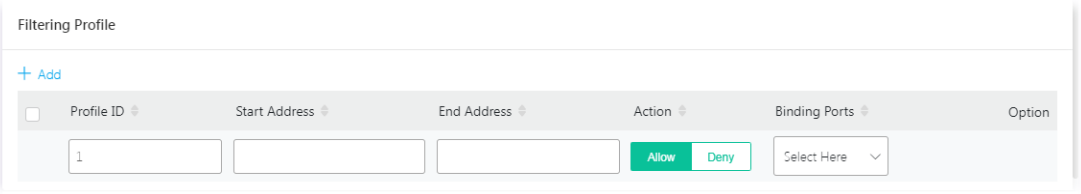
In addition, such filtering profile is only effective for controlling the query for multicast. It has nothing to do with the general IGMP query.



Available settings are explained as follows:

Item	Description
+Add	Click to create a new profile.
Profile ID	Displays the index number of a filtering profile.
Start Address	Displays the starting point for the IP range.
End Address	Displays the ending point for the IP range.
Action	Displays the action performed for this profile.
Binding Ports	Displays the interface (GE/LAG) selected for this profile.

To add a new profile, click the **+Add** link to open the setting page.



Available settings are explained as follows:

Item	Description
+Add	Click to have new fields for creating a new profile.
Profile ID	Enter 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	**Allow** – When it is selected, the request for multicast traffic will be forwarded to the multicast group normally. **Deny** – It is default setting. The forwarding request of multicast traffic will be discarded.
Binding Ports	Select the GE/LAG port(s) (interfaces) for filtering profile to process multicast traffic.
OK	Save the settings.

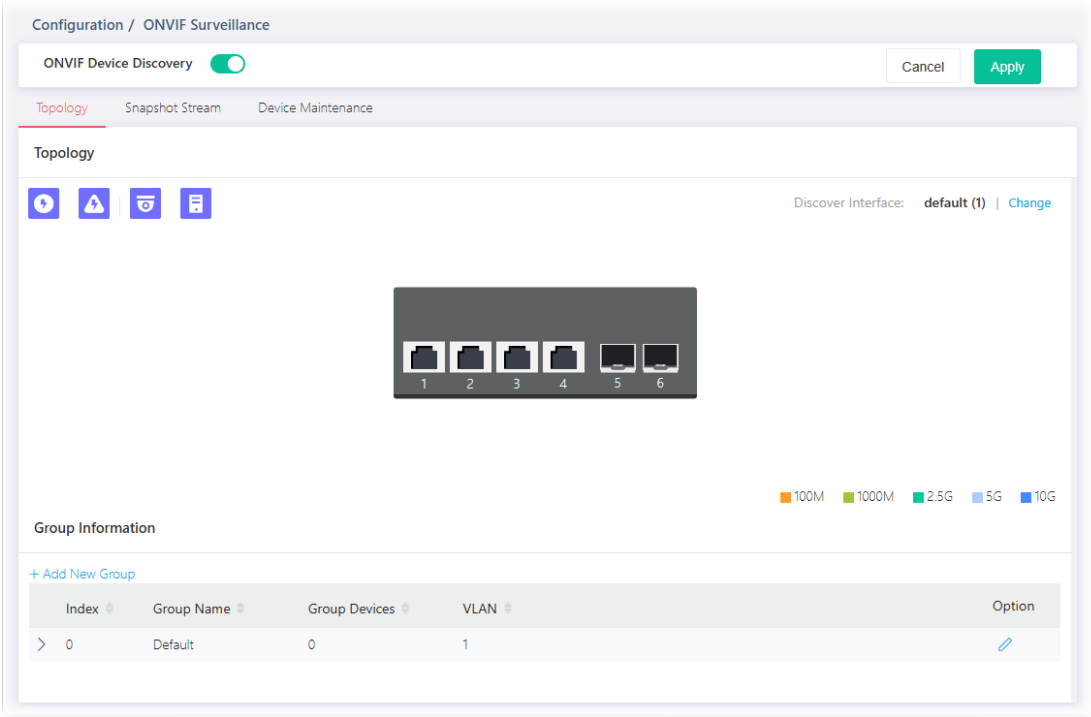
After finishing this web page configuration, please click **OK** to save the settings.

II-7 ONVIF Surveillance

ONVIF (Open Network Video Interface Forum), an International standard for current surveillance system industry, focuses on security products based on network IP address.

With this feature, VigorSwitch can:

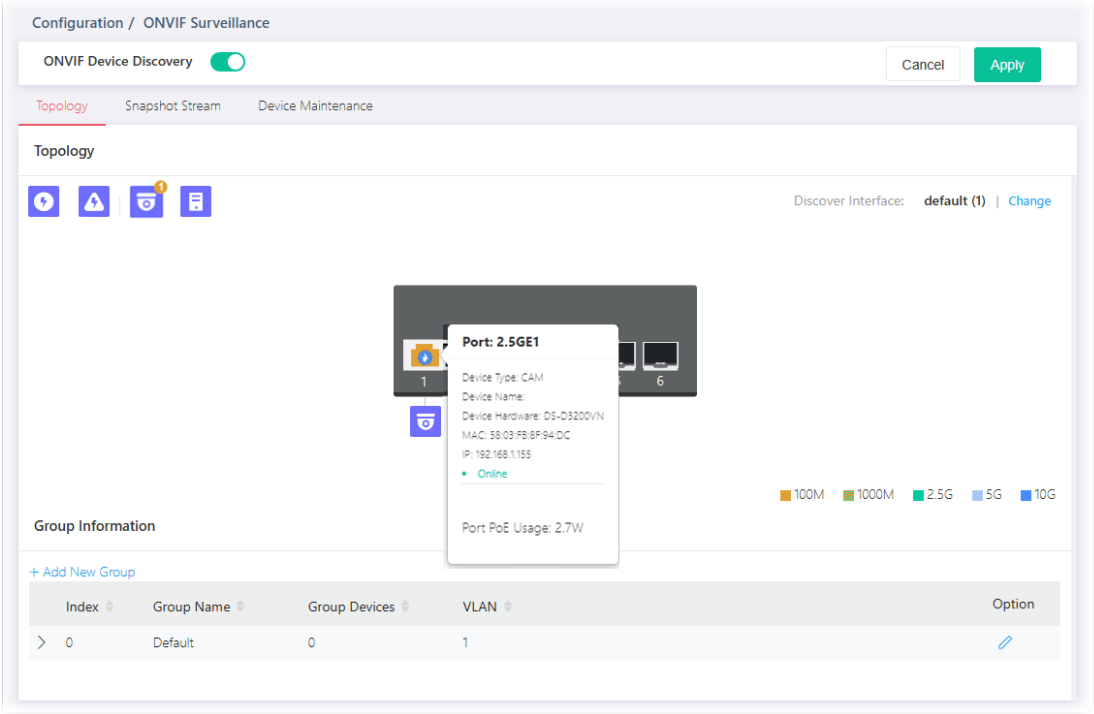
- Integrate the ONVIF device and surveillance network
- Centralize management of IP video products
- View video images directly on VigorSwitch WUI
- Offer remote IP video products maintenance



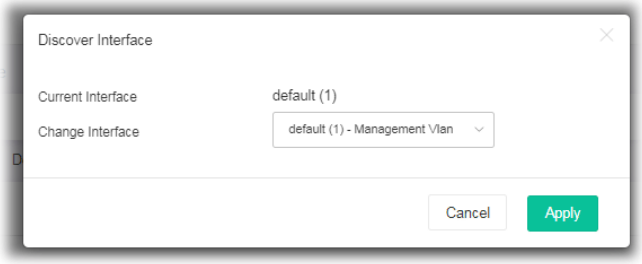
Switch the toggle to enable the **ONVIF Device Discovery** function. Then click **Apply**.

II-7-1 Topology

ONVIF devices can be centralized and managed remotely via VigorSwitch. With a hierarchy view, the administrator can manage several ONVIF devices and check abnormal traffic detected by the Vigor system.

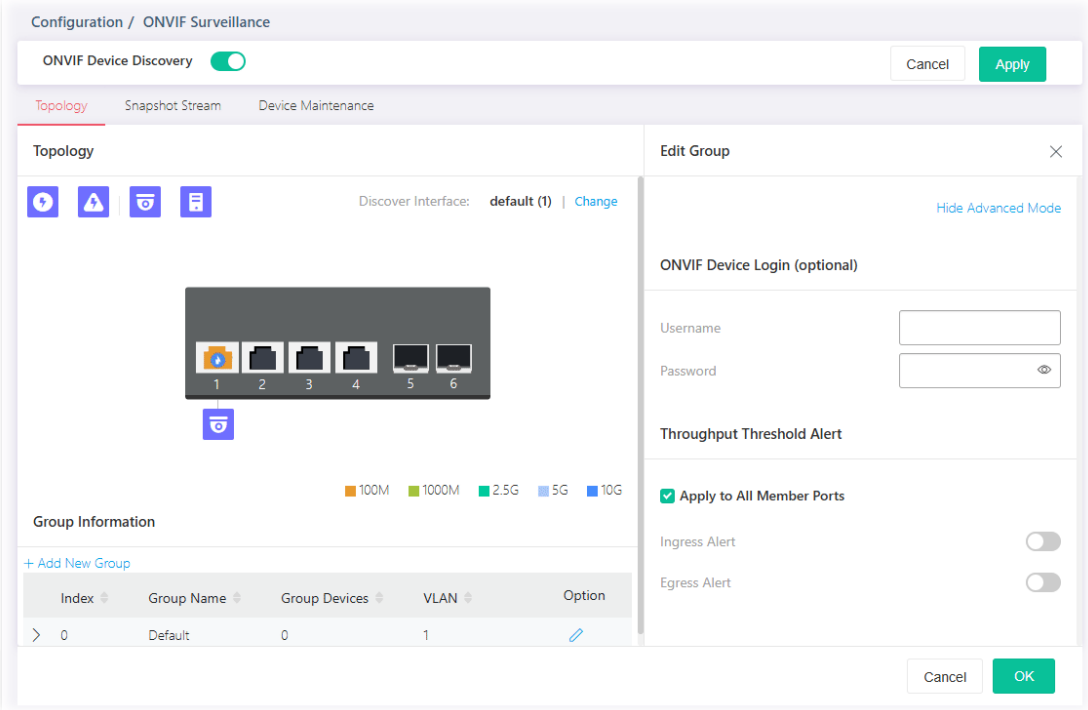


Available settings are explained as follows:

Item	Description
	**Camera -** Displays the number of IP camera(s) connected to VigorSwitch. The panel sketch on the screen will display which LAN port that the IP camera connected. **NVR -** Displays the number of NVR device(s) connected to VigorSwitch. The panel sketch on the screen will display which LAN port that the NVR device connected.
Change	VigorSwitch will detect the ONVIF device based on the interface selected. 
+Add New Group	A group can contain one (IP camera or NVR, as group leader) to several devices (IP cameras as group devices). Click to create a new group for managing multiple devices.
Index	Displays the index number of the group profile.

Group Name	Displays the name of the group profile.
Group Devices	Displays the number of the devices grouped under this profile.
VLAN	Displays the VLAN profile.
Option	- Click it to modify the group setting.

To modify settings for a port, click the link to open the setting page.



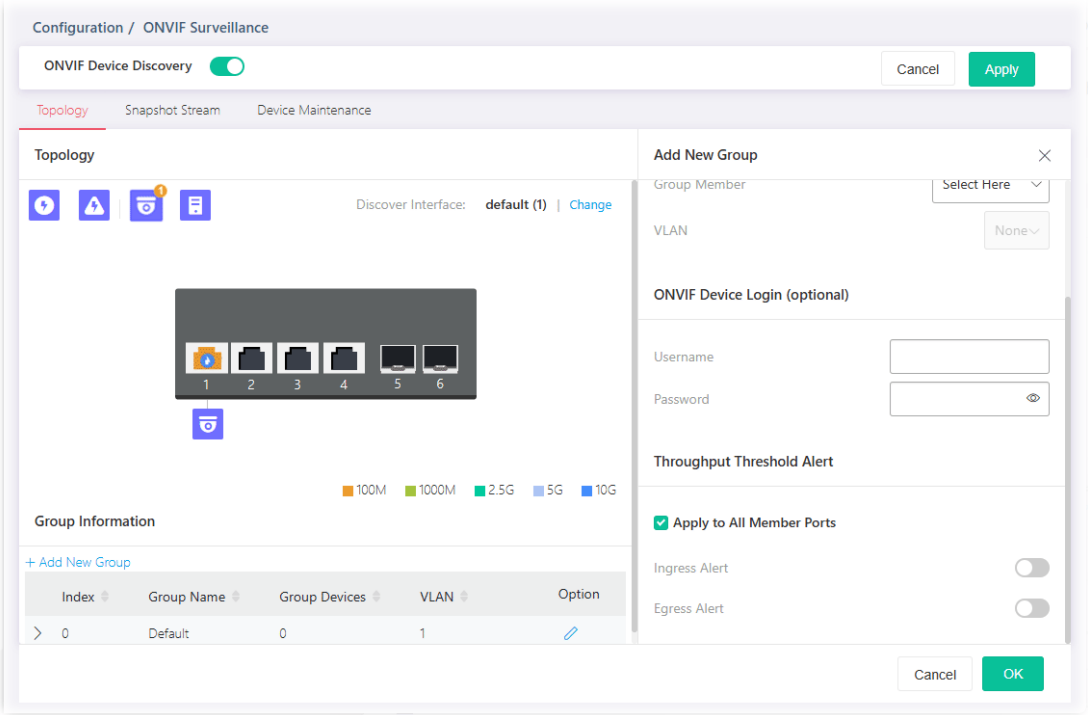
Available settings are explained as follows:

Item	Description
Edit Group	
Show / Hide Advanced Mode	Click to display or hide the advanced settings.
ONVIF Device Login (optional)	
Username / Password	Enter a name / password as the default value. In the entire ONVIF Surveillance menu, VigorSwitch will input this value in advanced and retrieve data. System administrator can access the IP device in which the username and password are as same as the default values. However, you can also input another username/password manually if the IP device username/password is different from the one you enter in Default Username/Default Password.
Advanced Mode - Throughput Threshold Alert	
Apply to All Member Ports	Check the box to apply the throughput threshold setting to all member ports.
Ingress Alert	Toggle the switch to enable the function. Set the ingress limit value. When the incoming traffic (packet) of the GE port reaches

	the limit, the Vigor System will send an alert email to the system administrator. **Rate Limit** - Enter the ingress rate as a threshold to send mail alert.
Egress Alert	Toggle the switch to enable the function. **Rate Limit** - Enter the egress rate as a threshold to send mail alert.

After finishing this web page configuration, please click **OK** to save the settings.

To create a new group, click the **+Add New Group** link to open the setting page.



Available settings are explained as follows:

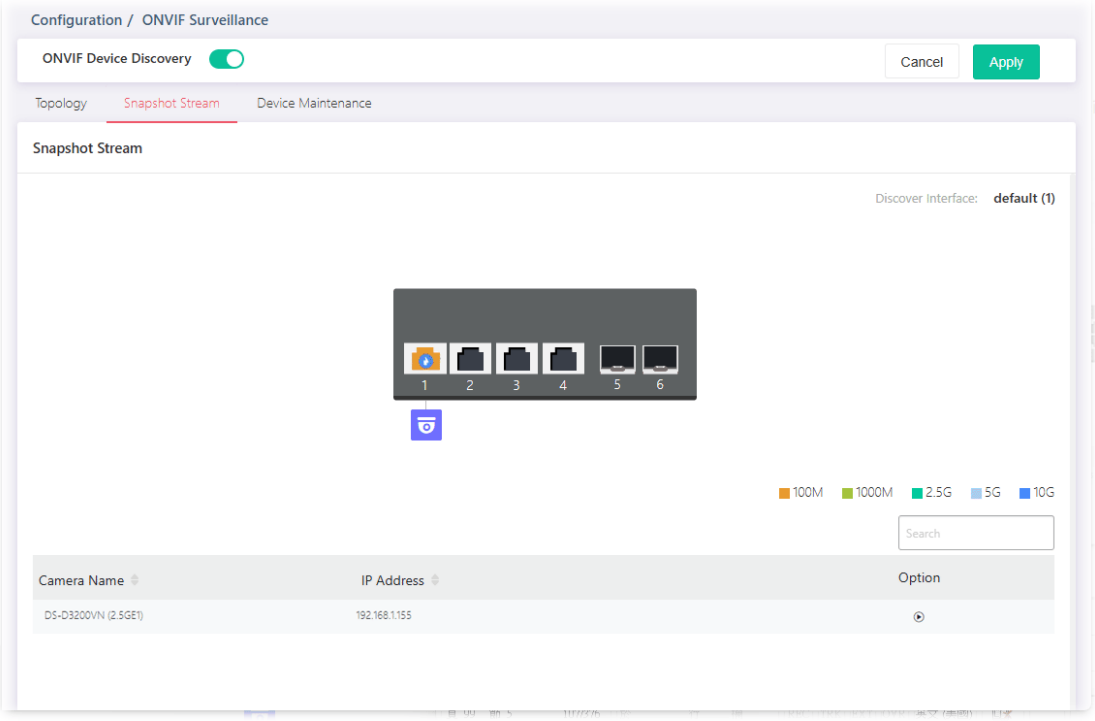
Item	Description
Add New Group	
Show / Hide Advanced Mode	Click to display or hide the advanced settings.
Group Name	Enter the name of a group.
Group Leader	The system will detect the NVR or IP cameras, and list them on the field of NVR or Group Leader.
Group Member	This field lists all devices (IP cameras) not included by other group. Select one IP device to multiple devices or select all the devices for managed by this group.
VLAN	Select a VLAN.
ONVIF Device Login (optional)	
Username / Password	Enter a name / password as the default value. In the entire ONVIF Surveillance menu, VigorSwitch will input this value in advanced and retrieve data. System administrator can access the IP device in which the username and password are as same as the default values. However, you can also input another username/password

	manually if the IP device username/password is different from the one you enter in Default Username/Default Password.
Throughput Threshold Alert	
Apply to All Member Ports	Check the box to apply the throughput threshold setting to all member ports.
Ingress Alert	Toggle the switch to enable the function. Set the ingress limit value. When the incoming traffic (packet) of the GE port reaches the limit, the Vigor System will send an alert email to the system administrator. **Rate Limit** - Enter the ingress rate as a threshold to send mail alert.
Egress Alert	Toggle the switch to enable the function. Set the egress limit value. When the incoming traffic (packet) of the GE port reaches the limit, the Vigor System will send an alert email to the system administrator. **Rate Limit** - Enter the ingress rate as a threshold to send mail alert.

After finishing this web page configuration, please click **OK** to save the settings.

II-7-2 Snapshot Stream

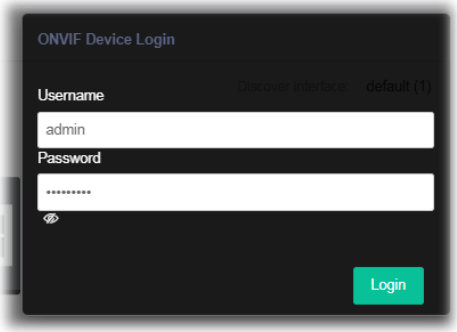
This page can offer a real-time video of specified IP camera for monitoring and control environments.



Available settings are explained as follows:

Item	Description
Snapshot Stream	
Camera Name	Displays the device name of the IP camera.
IP Address	Displays the IP address of the IP camera.
	After authenticated with correct username and password, the image of the specified IP camera (supported by VigorSwitch) will

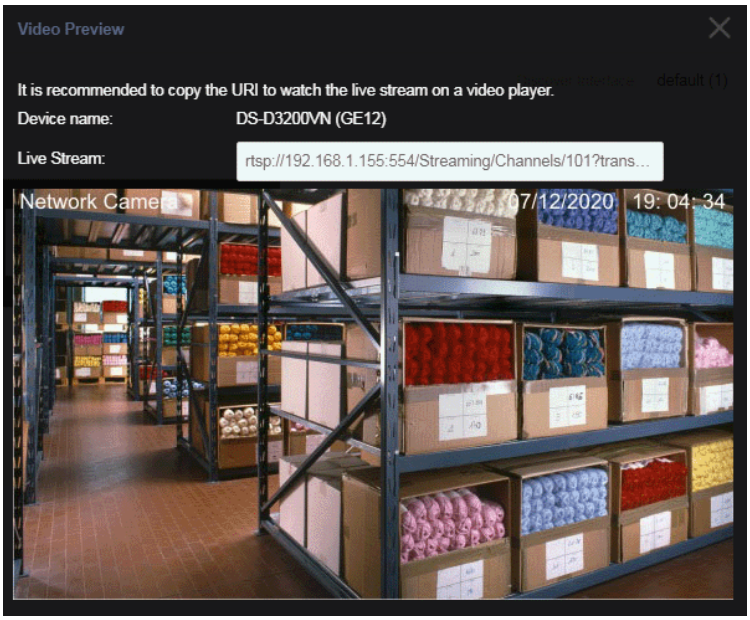
be shown immediately.



Usename / Password - The default username/password will be input if it is configured on the Topology page. However, if the default input is not the correct username/password, enter the correct one of the IP camera instead.

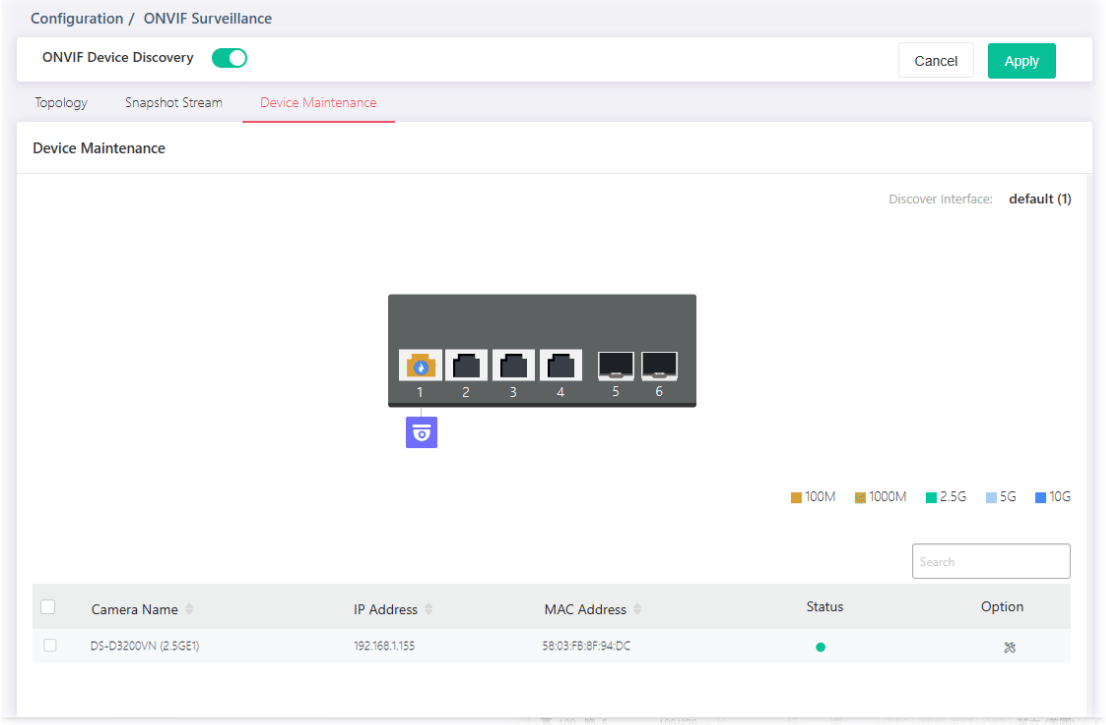
Login - Click it to authenticate the username and password for the specified IP camera.

A pop-up window (Video Preview) appears to display a live image on the screen.



II-7-3 Device Maintenance

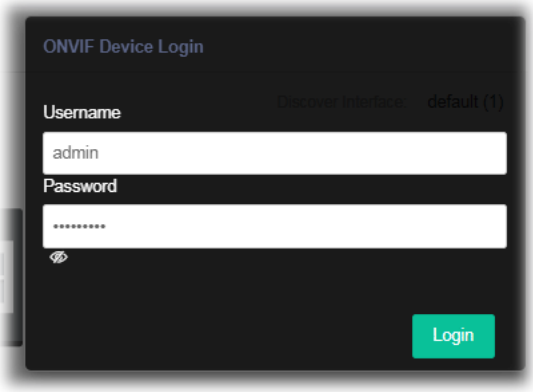
The system administrator can remotely configure time setting, security settings and reboot the devices (IP cameras or NVRs) managed by Vigor switch.



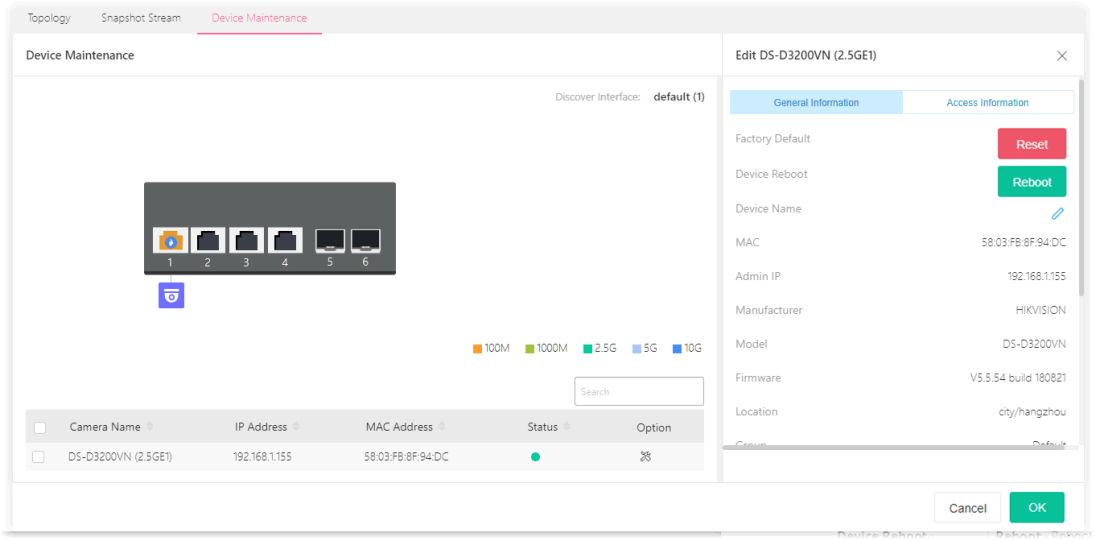
Available settings are explained as follows:

Item	Description
Device Maintenance	
Camera Name	Displays the device name of the IP camera.
IP Address	Displays the IP address of the IP camera.
MAC Address	Displays the MAC address of the IP camera.
Status	Displays the status (enabled or disabled) of the IP camera.
	Click to configure detailed settings for the selected device.

Click to configure detailed settings. First you have to login the ONVIF device.



After entering the correct username and password of the device, the detailed settings page will be shown as follows:



Available settings are explained as follows:

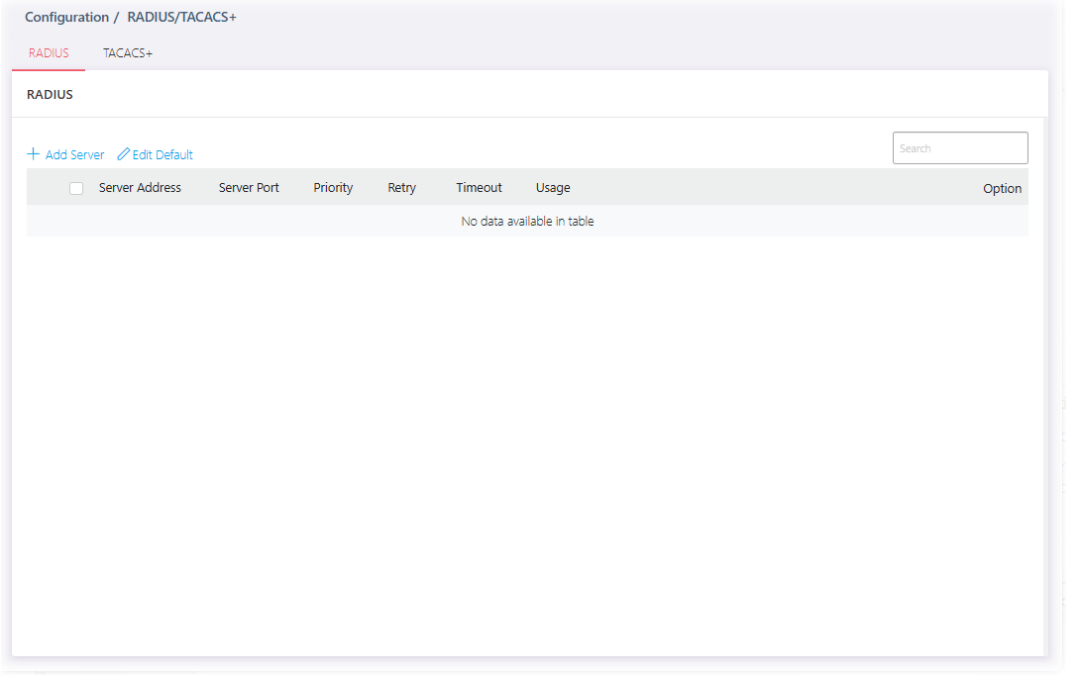
Item	Description
General Information	
Factory Default	**Reset** - Reset the factory default to the IP device.
Device Reboot	**Reboot** - Reboot the IP device immediately.
Device Name	Click  to modify the name of the device.
MAC	Displays the MAC address of the device.
Admin IP	Displays the IP address of the device.
Manufacturer	Displays the manufacturer of the device.
Model	Displays the model name of the device.
Firmware	Displays the firmware version used by the device.
Location	Displays the location of the device.
Group	Displays the name of the group.
Current Time	Displays the time set for the device.
UTC Time	Display the time and date information related to the selected device.
Time Zone	Displays the time zone based on the location of the device.
Daylight Saving	Displays the status (enabled/disabled) of the daylight saving function.
Auto Device Check	Switch the toggle to enable / disable this function.  - means “Enable”. - means “Disable”. **Failure Action** - Configure the power behavior for each LAN port. • **Power Cycle -** Once the device is offline, Vigorswitch will power off the device and then power on the device again. • **Power Off** - When the device is offline, power off the device immediately. • **Nothing** - When the device is offline, no action will be

	performed. **Note**: When a PoE hub connecting to LAN port of VigorSwitch, the power behavior (on/off) to the PoE hub also will apply to all the devices connecting to the PoE hub. **Mail Alert** - Switch the toggle to enable / disable this function. When the device is offline, Vigor system will send an alert mail to notify the recipient. • **With Snapshot** - If enabled, the switch will try to get snapshot from the device per half hour. Before using this feature, set the group authentication information when adding group or configure Default Username/Password in the Topology page first. When the device is offline, no action will be performed.
Access Information	
Mode	Change the connection mode for this device. **Static -** When it is selected, you have to enter value for network setting manually for the IP device. • **IP Address** - Enter an IPv4 address for the IP device. • **Prefix Length** - Specify the subnet mask for the IP address. • **Gateway** - Enter the IPv4 address for the gateway. • **DNS Server1/2** - Enter the IP address for primary / secondary DNS server. **DHCP -** When it is selected, the IP device will be assigned with the settings by the network's DHCP server automatically to access the Internet. • **Hostname** - Display the hostname of the DHCP server.
Zero Configuration	Switch the toggle to enable / disable this function. **Enable -** The network settings for the IP device will be configured automatically. **Disable -** The network settings for the IP device must be configured manually.
HTTP Port	Switch the toggle to enable / disable this function. **Enable -** Click it to enable the HTTP port configuration and enter a port value if required. **Disable -** Disable the HTTP port configuration.
HTTPS Port	Switch the toggle to enable / disable this function. **Enable -** Click it to enable the HTTPS port configuration and enter a port value if required. **Disable -** Disable the HTTPS port configuration.
RTSP Port	Switch the toggle to enable / disable this function. **Enable -** Click it to enable the RTSP port configuration and enter a port value if required. **Disable -** Disable the RTSP port configuration.

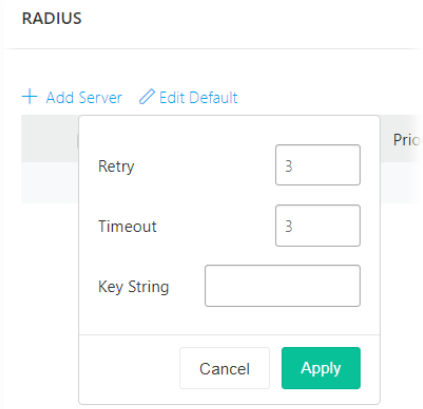
II-8 RADIUS/TACACS+

II-8-1 RADIUS

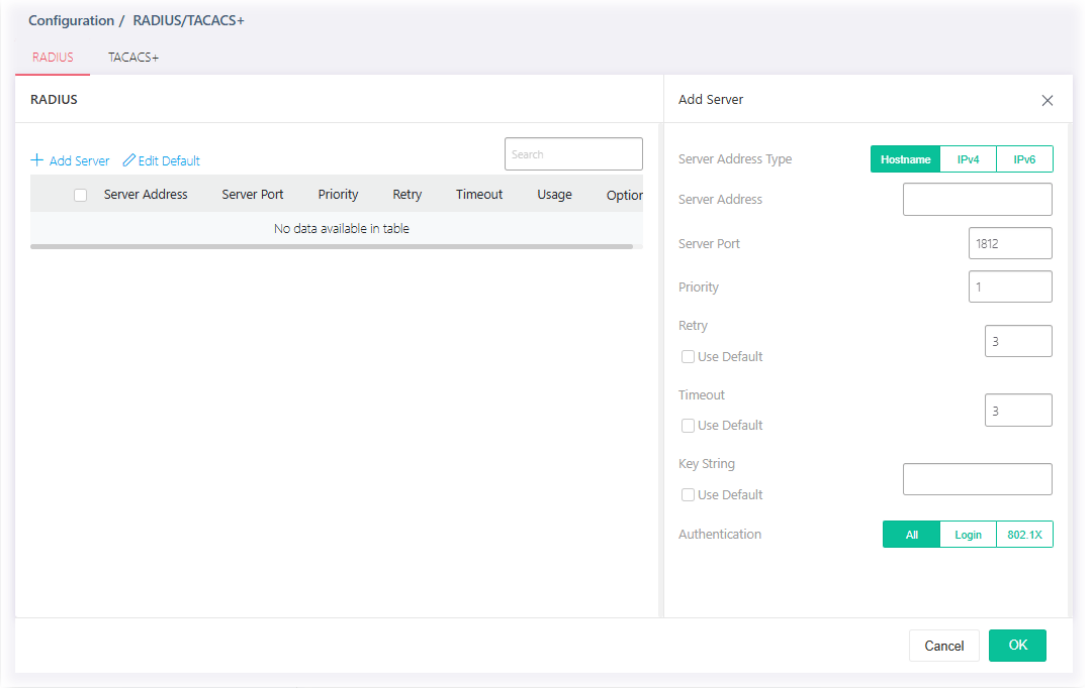
This page allows the network administrator to add and configure multiple RADIUS servers.



Available settings are explained as follows:

Item	Description
+Add Server	Click to create a new server profile.
Edit Default	Click to modify the value(s) for Retry, Timeout and Key String. These values will be saved as default settings. 

To create a new profile, click the **+ Add Server** link to open the setting page.



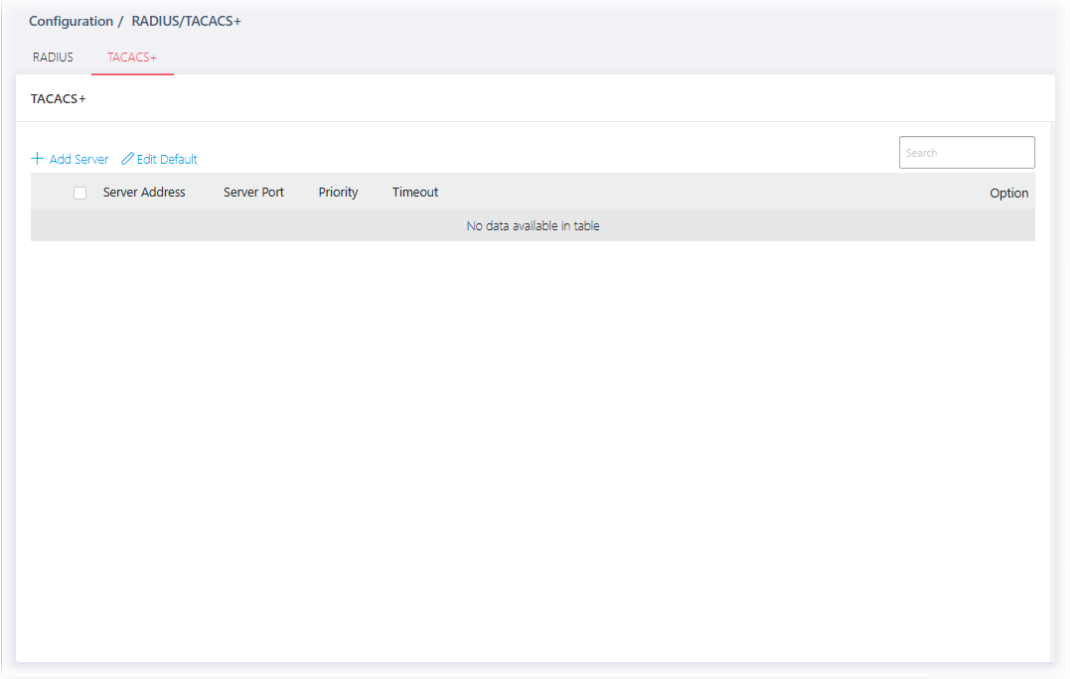
Available settings are explained as follows:

Item	Description
Add Server	
Server Address Type	Specify whether switch uses a hostname to resolve address by DNS to connect to server, or directly connect using IPv4 address. • Hostname • IPv4 • IPv6
Server Address	Enter the server's address corresponding with address type given.
Server Port	Enter the port number used by RADIUS server.
Priority	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 retry time before this server being considered not-reachable. **Use Default** - Use the default value.
Timeout	Set the time (in seconds) before this server being considered lost connection. **Use Default** - Use the default value.
Key String	Enter the string used to encrypt and authenticate with RADIUS server. **Use Default** - Use the default setting.
Authentication	Specify whether you would like to use this server for switch login authentication or 802.1x access port authentication, or both. • All • Login • 802.1X
OK	Save the settings.

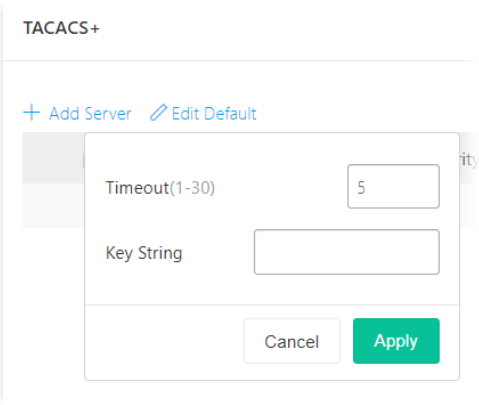
After finishing this web page configuration, please click **OK** to save the settings.

II-8-2 TACACS+

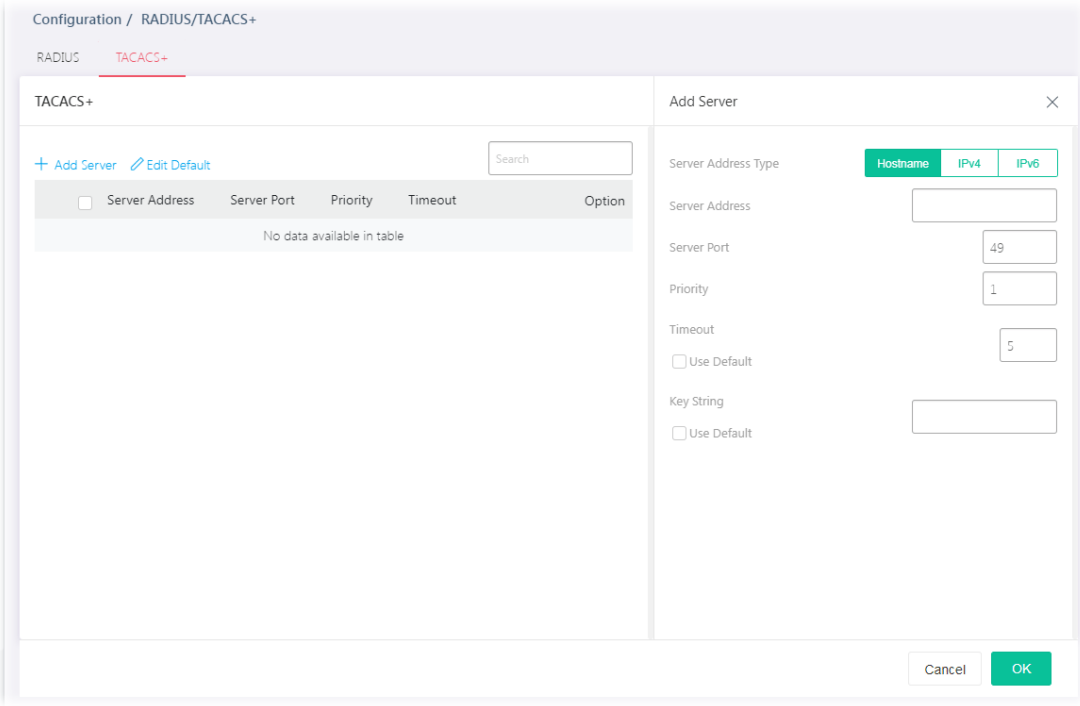
This page allows the network administrator to add and configure multiple TACACS+ server.



Available settings are explained as follows:

Item	Description
+Add Server	Click to create a new server profile.
Edit Default	Click to modify the value(s) for Timeout and Key String. These values will be saved as default settings. 

To create a new profile, click the **+ Add Server** link to open the setting page.



Item	Description
Add Server	
Server Address Type	Specify whether switch uses a hostname to resolve address by DNS to connect to server, or directly connect using IPv4 address. • Hostname • IPv4 • IPv6
Server Address	Enter the server's address corresponding with address type given.
Server Port	Enter the port number used by TACACS+ server.
Priority	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. **Use Default** - Use the default value.
Key String	Enter the string used to encrypt and authenticate with TACACS+ server. **Use Default** - Use the default setting.
OK	Save the settings.

After finishing this web page configuration, please click **OK** to save the settings.

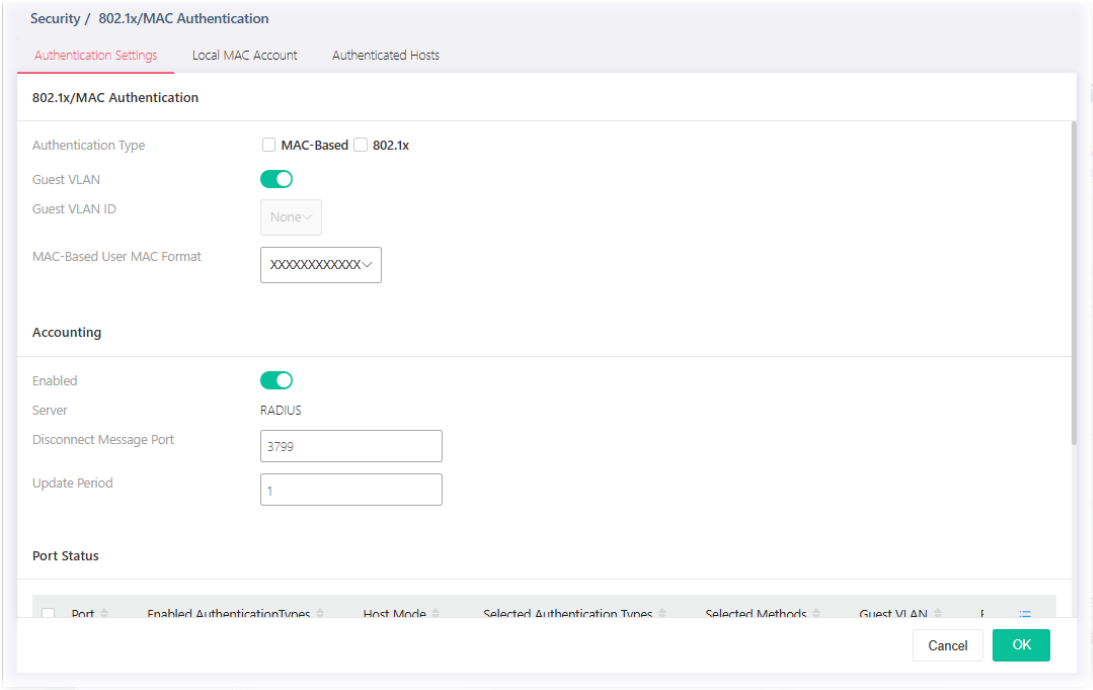
This page is left blank.

Chapter III Security

III-1 802.1x/MAC Authentication

III-1-1 802.1x/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.

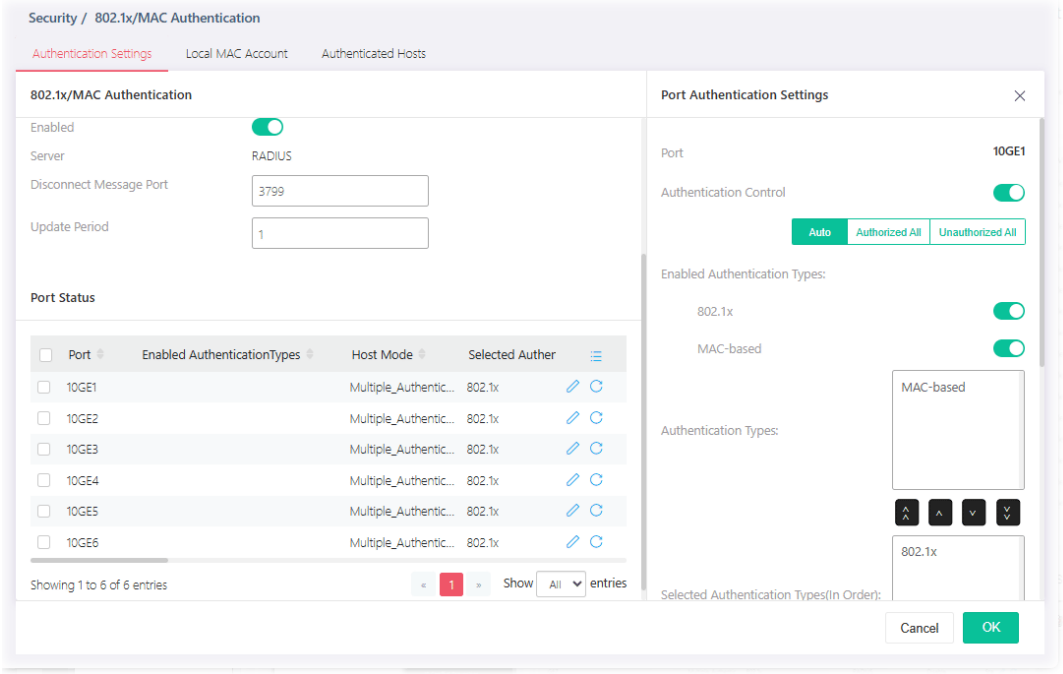


Available settings are explained as follows:

Item	Description
802.1x/MAC Authentication	
Authentication Type	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. • MAC-Based • 802.1x
Guest VLAN	Switch the toggle to enable/disable a Guest VLAN for those who have not successfully authenticated with any given methods. - means "Enable". If enabled, specify a VLAN ID number. - means "Disable". **Guest VLAN ID** - Choose one of the VLAN ID as a Guest VLAN.
MAC-Based User MAC Format	Specify how the MAC-based user ID should be expressed in EAP message between AAA server and switch.
Accounting	

Enabled	Switch the toggle to enable / disable this function. **Server** - Displays the type of the server. **Disconnect Message Port** - Enter a port value (1~65535). **Update Period** - Set the time period for accounting update.
Port Status	
Port	Displays the index number of the GE ports. Select physical port(s) for applying settings. Note that port authentication will not be effective if none of them were enabled.
Enabled Authentication Types	Displays the authentication type (802.1x and/or MAC-based) used by this port.
Host Mode	Displays the host mode used by this port.
Selected Authentication Types	Displays the authentication type (e.g., 802.1x) used by this port.
Selected Methods	Displays the authentication method (e.g., RADIUS) used by this port.
Guest VLAN	Displays the status (enable/disable) of guest VLAN function.
	Click it to modify the port setting.
	Clear current settings and return to factory default settings.

To modify settings for a port, click the link to open the setting page.



Available settings are explained as follows:

Item	Description
Port Authentication Settings	
Port	Displays the GE port number.
Authentication Control	Switch the toggle to enable / disable this function.

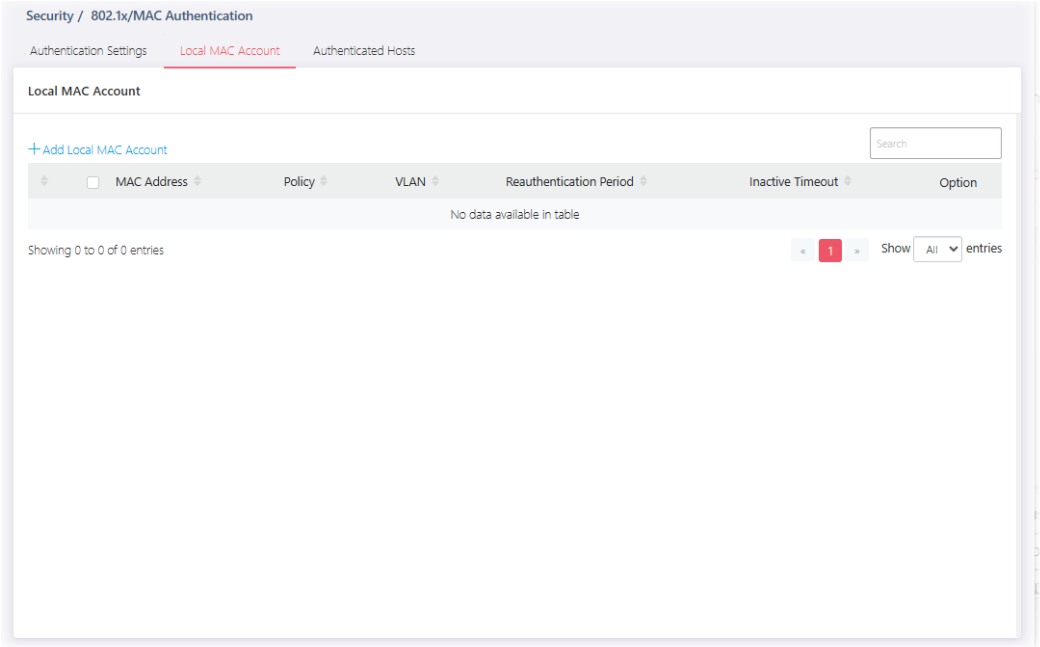
	 - means “Enable”. - means “Disable”. If enabled, select **Auto**, **Authorized All** or **Unauthorized** All as the control mode.
Enabled Authentication Types	Select 802.1x and/or MAC-based authenticate method for host connecting to this port. • 802.1x • MAC-based
Authentication Types	Displays available authentication types of AAA server (or local) you wish to have on this port.
Selected Authentication Types (In Order)	Specify the order of authentication type (e.g., 802.1x) you wish to have on this port.
Available Methods For TACACS+	Display available methods of AAA server (or local) you wish to have on this port.
Selected Methods (In Order)	Specify the order of authentication methods (e.g., RADIUS) you wish to have on this port.
Host Mode	**Multi-Auth** - Each host are authenticated individually. **Multi 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.
Advanced Mode	
Guest VLAN	Switch the toggle to enable / disable this function. Select **Enable** to enable Guest VLAN on this port for those didn't authenticated successfully.
RADIUS VLAN Assignment	**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. **Disabled** - Switch will ignore the VLAN assignment from the RADIUS server and keep the original VLAN of the host. **Reject** - Switch will reject the host if it does not receive the VLAN information from the RADIUS server.
Max. Hosts	If **Multi-Auth** mode is selected as Host Mode, the total number of hosts cannot exceed the maximum number of hosts configured here.
Periodic Reauthentication	The hosts via the selected GE port will be re-authenticated periodically. Switch the toggle to enable / disable this function. If enabled, specify the time setting. **Periodic 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.
Inactive 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 **Multi Hosts** mode, 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 will be allowed to perform authentication again.
EAP Resent Period	Set the period for host to re-send EAP (Ethernet Automatic Protection) requests. Default value is 30 (seconds).
Supplicant Timeout	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	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	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.
OK	Save the settings.

After finishing this web page configuration, please click **OK** to save the settings.

III-1-2 Local MAC Account

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

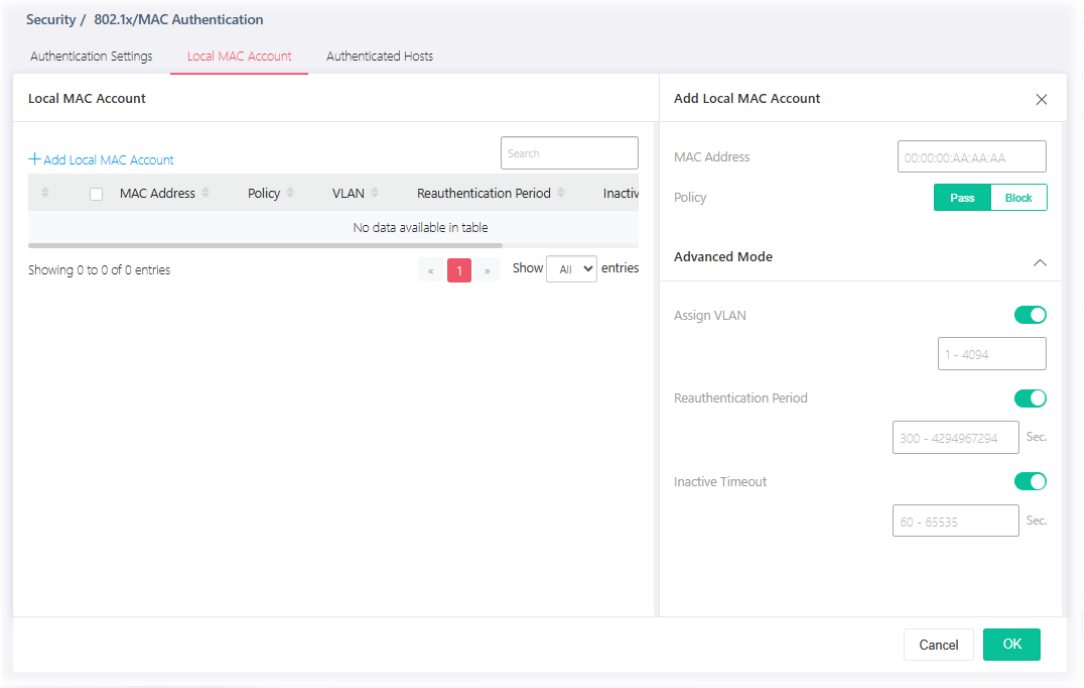


Available settings are explained as follows:

Item	Description

+Add Local MAC Account	Click to create a new MAC account.
MAC Address	Displays the MAC address of the host.
Policy	Displays the policy (pass or block) of the host.
VLAN	Displays the VLAN ID assigned by the host.
Reauthentication Period	Displays the time this account is required to be authenticated again.
Inactive Timeout	Displays the time to log off this account.

To add a new profile, click the **+Add Local MAC Account** link to open the setting page.



Available settings are explained as follows:

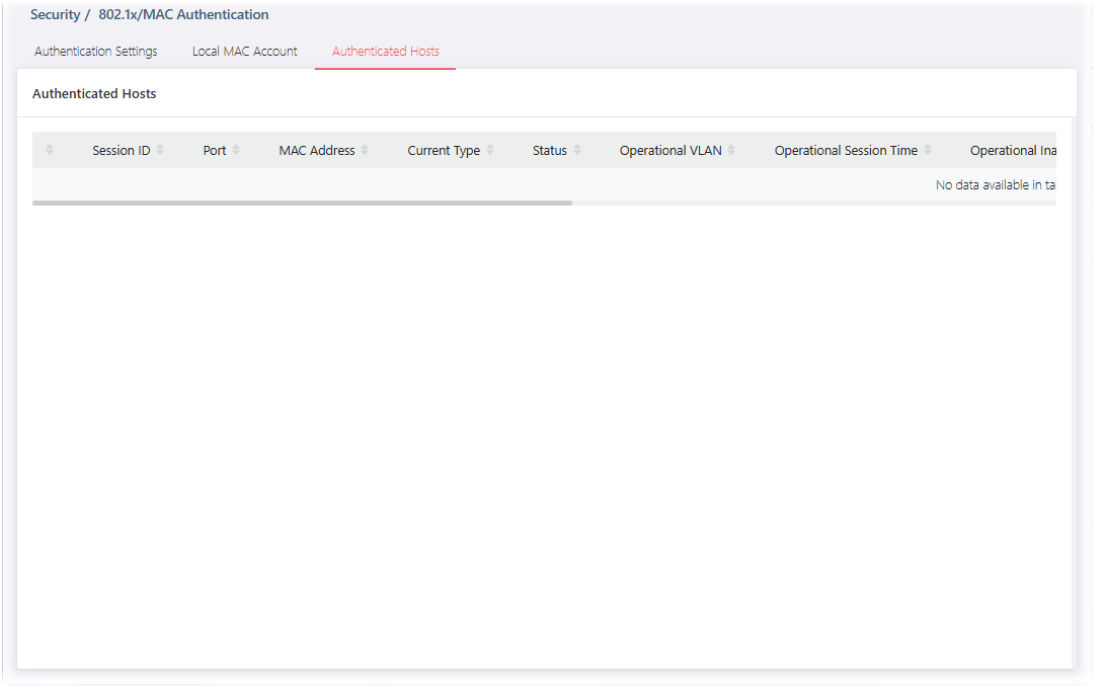
Item	Description
Local MAC Account	
MAC Address	Enter the MAC address of the host.
Policy	**Pass** - Click it to forcefully authenticate the host specified above. **Block** - The host specified above will not be authenticated by VigorSwitch. If **Pass** is selected, advanced mode will be shown below.
Advanced Mode	
Assign VLAN	Switch the toggle to enable / disable this function.  - means "Enable". - means "Disable". Specify which VLAN will be assigned by the host of this account.
Reauthentication Period	Switch the toggle to enable / disable this function. Set the time this account is required to be authenticated again

	after authentication has taken place.
Inactive Timout	Switch the toggle to enable / disable this function. Set a time. When the account is still inactive after the set time, it will be logged out by the system.

After finishing this web page configuration, please click **OK** to save the settings.

III-1-3 Authentication Hosts

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



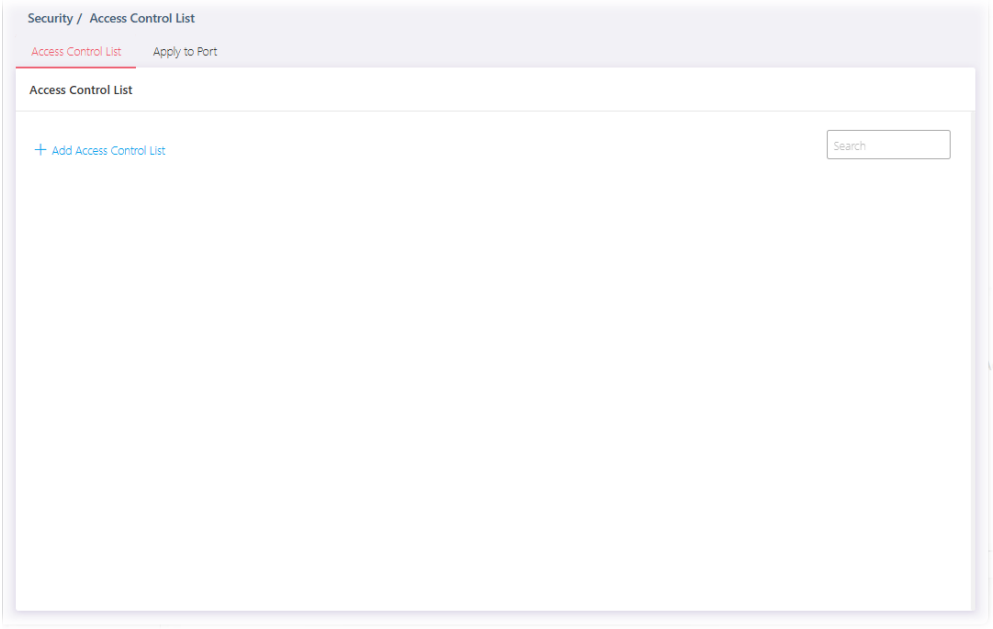
III-2 Access Control List

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.

Users can create the Access Control List (ACL) based on Layer 2 filtering, the MAC layer, Layer 2 to Layer 4 filtering, the IPv4, and Layer 2 to Layer 4 filtering, the IPv6. The ACL is composed by many Access Control Element (ACE) rules. You can create a new ACL here; then add multiple ACEs.

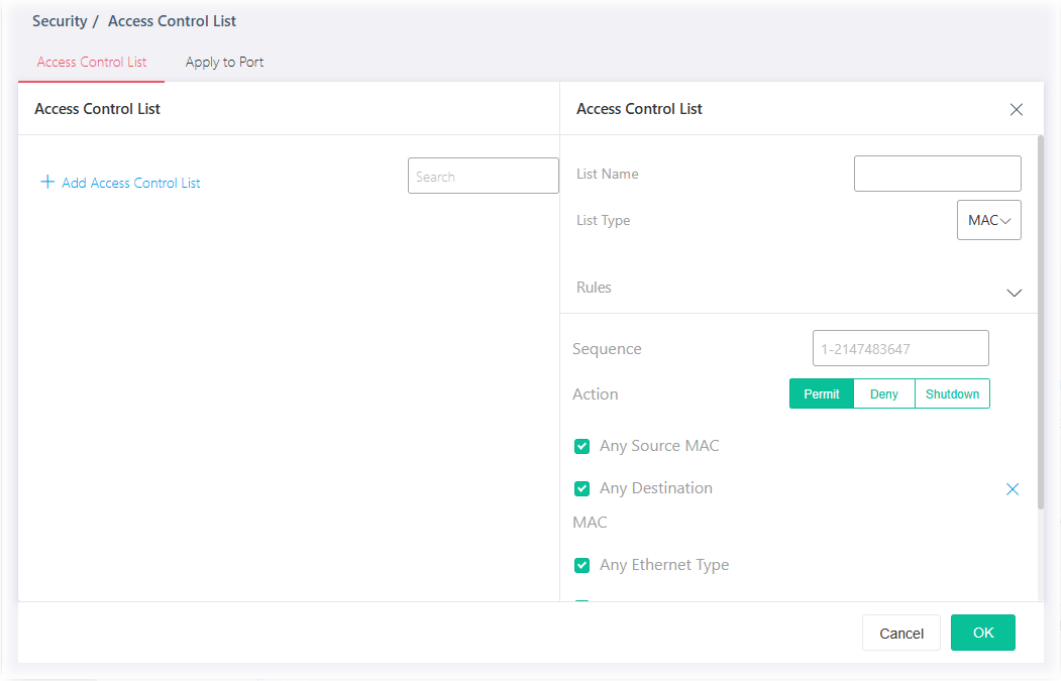
You may provide filtering/matching criteria for one or more packet characteristics (such as Source/Destination MAC, Ethertype, VLAN, 802.1p) for this ACE to identify the packet.

III-2-1 Access Control List



List Type - MAC

To create a new access control list, click the **+Add Access Control List** link to open the setting page.

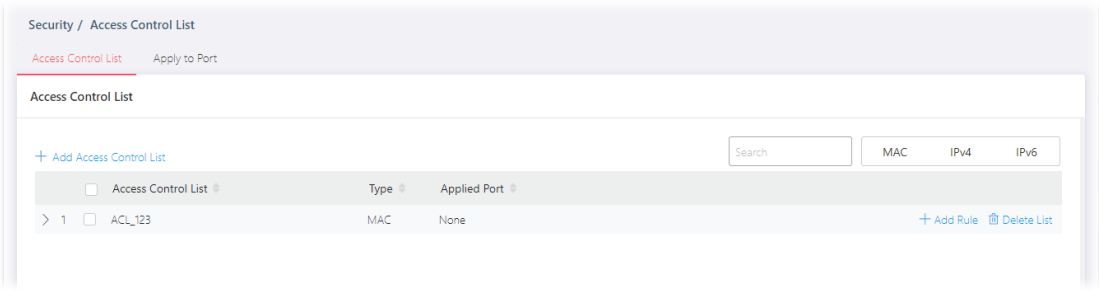


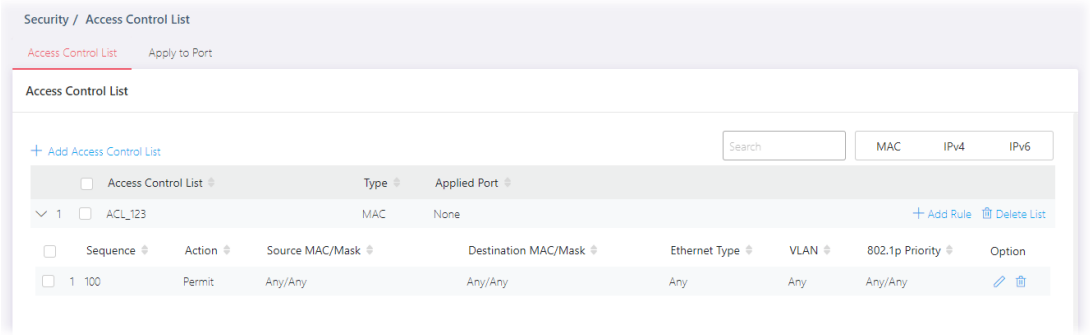
Available settings are explained as follows:

Item	Description
Access Control List	
List Name	Enter a name for creating a new ACL profile.
List Type	Specify the filtering type (MAC/IPv4/IPv6).
Rules	
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**
Any Source MAC	If disabled, please enter IP address with the subnet mask. 
Any Destination MAC	If disabled, please enter IP address with the subnet mask.
Any Ethernet Type	Specify Ethernet type for filtering. Select **Any Ethernet**. Or, enter the value with the format of "0x600 ~ 0xFFF". 

Any VLAN	Specify VLAN profile for filtering. Select **Any VLAN**. Or, enter a VLAN number. The packets coming from the VLAN specified here will be filtered by Vigor device. 
Any 802.1p Priority	Specify the 802.1p priority value for filtering. Select **Any 802.1p Priority**. Or, enter a number from 0 to 7. 
+Add Rule	Click it to create a new ACE rule. Each ACL profile can be added with 8 ACE rules.

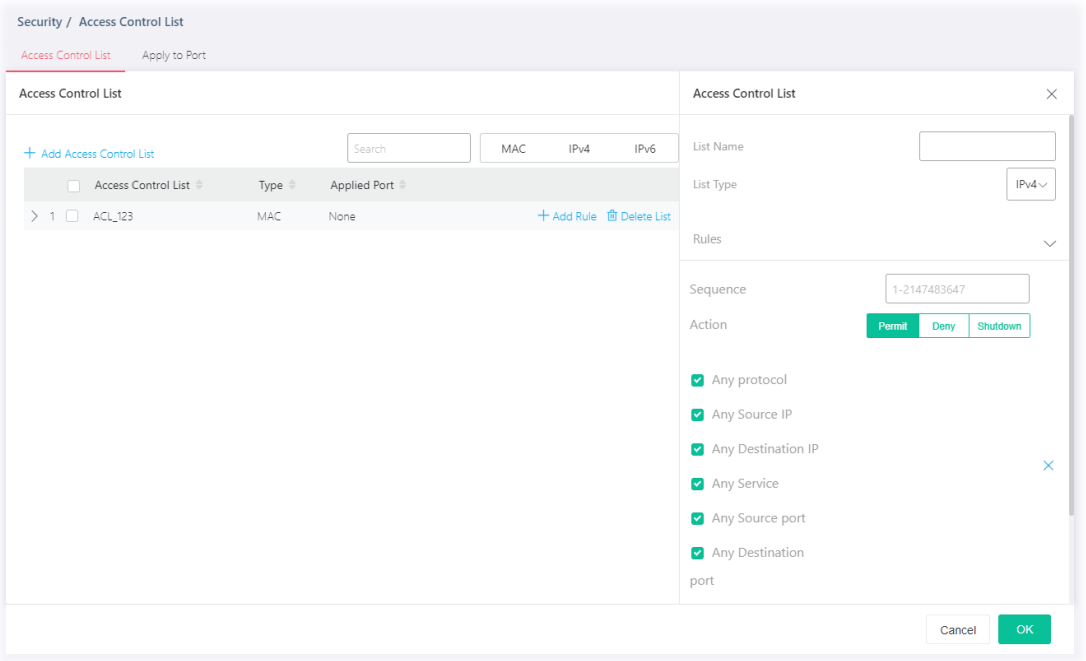
After finishing this web page configuration, please click **OK** to save the settings.





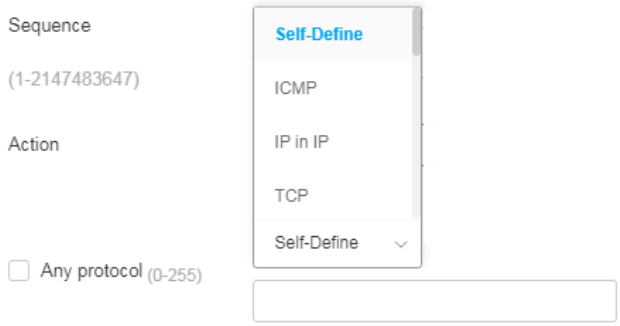
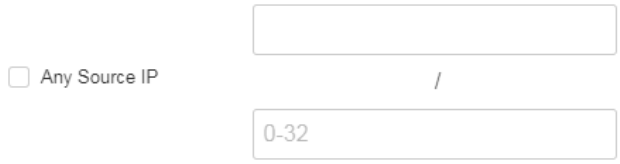
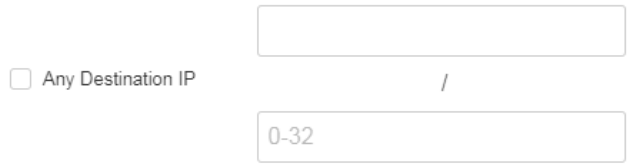
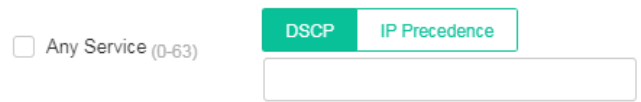
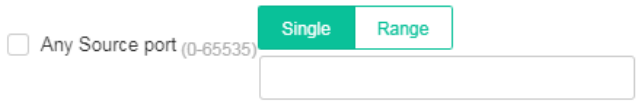
List Type - IPv4

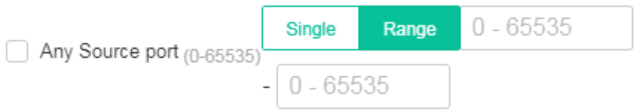
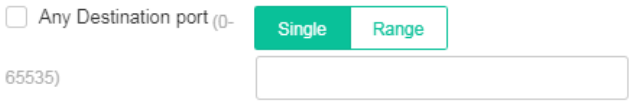
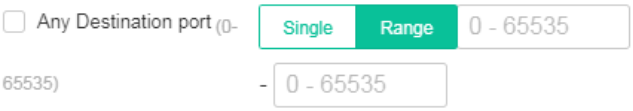
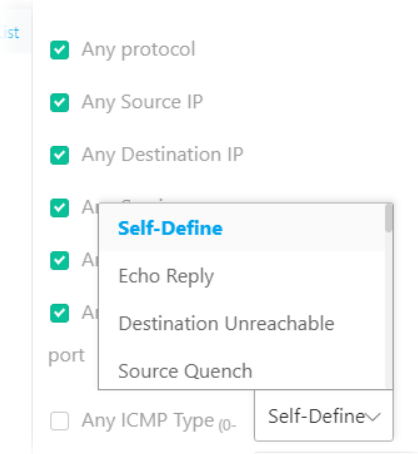
To create a new access control list, click the **+Add Access Control List** link to open the setting page.



Available settings are explained as follows:

Item	Description
Access Control List	
List Name	Enter a name for creating a new ACL profile.
List Type	Specify the filtering type (IPv4).
Rules	
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**
Any Protocol	Specify the protocol for filtering. **Any Protocol** – Default setting. All packets will be filtered. **Self-Define** – Enter a number (0 – 255) to specify a protocol. For example, 1 means "Internet Control Message"; 6 means "Transmission Control". **ICMP, IP in IP,...** – Choose one of the protocols (e.g., ICMP, IP in IP, TCP, EGP, IGP...) from the drop down list. Packets passing through the selected protocol will be filtered.

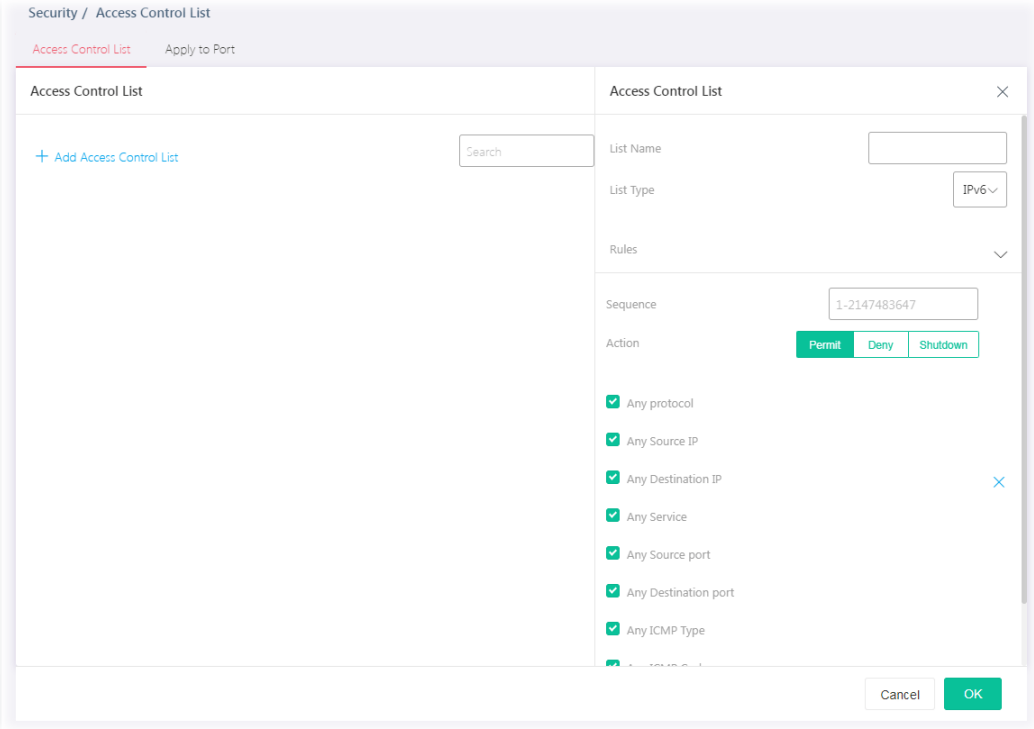
	
Any Source IP	Specify the source IPv4 address for filtering. **Any Source IP** – Default setting. All packets will be filtered. Select Any Source IP. Or, enter the IP address to filter the packets coming from that address. 
Any Destination IP	Specify the destination IPv4 address for filtering. **Any Destination IP** – Default setting. All packets will be filtered. Select Any Destination IP. Or, enter the IP address to filter the packets coming from that address. 
Any Service	**Any Service** – Default setting. 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. 
Any Source Port	Specify the source port number for filtering the packets. **Any Source Port** – Default setting. All packets will be filtered. Select Any Source Port. Or, enter the port number. **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. 
Any Destination Port	Specify the destination port number for filtering the packets. **Any Destination Port** – Default setting. All packets will be filtered. Select Any Destination Port. Or, enter the port number. **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. 
Any ICMP Type	**Any ICMP Type** – Default setting. All packets will be filtered. **Echo Reply, Destination Unreachable....** – Choose one of the type (e.g., Destination Unreachable, Echo Reply, MLD Query....) from the drop down list. **Self-Define** – Specify a type number (0 – 255) for ICMP code. For example, 0 means "Echo Reply"; 254 means "RFC3692-style Experiment 2". 
Any ICMP Code	ach 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 ICMP Code** – Default setting. All packets will be filtered. Select Any ICMP Code. Or, enter 0 to 255 based on the ICMP type specified. 

+Add Rule	Click it to create a new ACE rule. Each ACL profile can be added with 8 ACE rules.

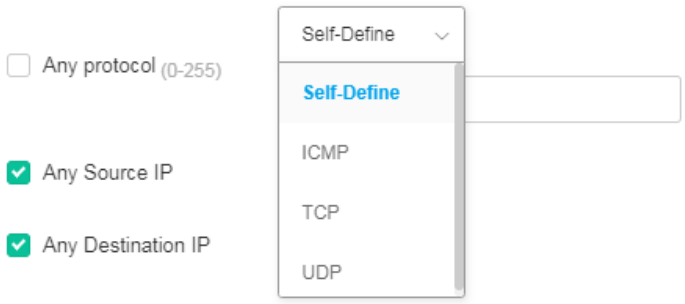
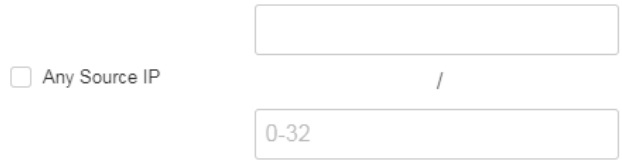
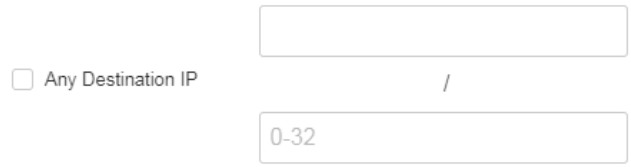
List Type - IPv6

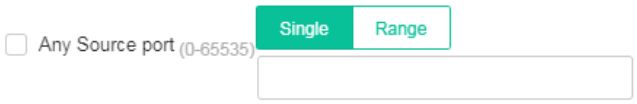
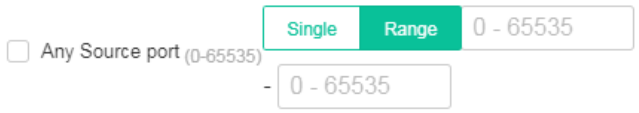
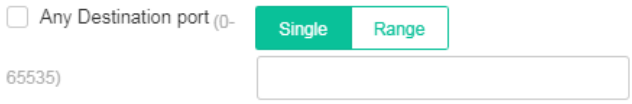
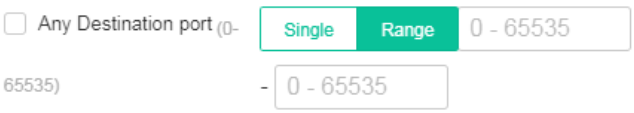
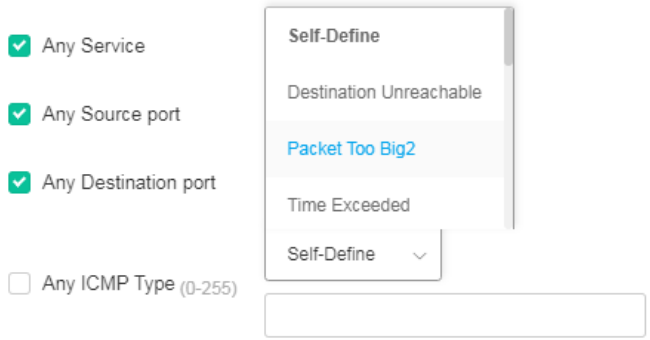
To create a new access control list, click the **+Add Access Control List** link to open the setting page.



Available settings are explained as follows:

Item	Description
Access Control List	
List Name	Enter a name for creating a new ACL profile.
List Type	Specify the filtering type (IPv6).
Rules	
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**
Any Protocol	Specify the protocol for filtering. **Any Protocol** – Default setting. All packets will be filtered. **Self-Define** – Enter a number (0 – 255) to specify a protocol. For

	example, 1 means “Internet Control Message”; 6 means “Transmission Control”. **ICMP, IP in IP,...** – Choose one of the protocol (e.g., ICMP, TCP, EGP...) from the drop down list. Packets passing through the selected protocol will be filtered. 
Any Source IP	Specify the source IPv6 address for filtering. **Any Source IP** – Default setting. All packets will be filtered. Select Any Source IP. Or, enter the IP address to filter the packets coming from that address. 
Any Destination IP	Specify the destination IPv6 address for filtering. **Any Destination IP** – Default setting. All packets will be filtered. Select Any Destination IP. Or, enter the IP address to filter the packets coming from that address. 
Any Service	**Any Service** – Default setting. 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. 
Any Source Port	Specify the source port number for filtering the packets. **Any Source Port** – Default setting. All packets will be filtered. Select Any Source Port. Or, enter the port number. **Single** – Only the packets passing through the number defined here will be filtered.

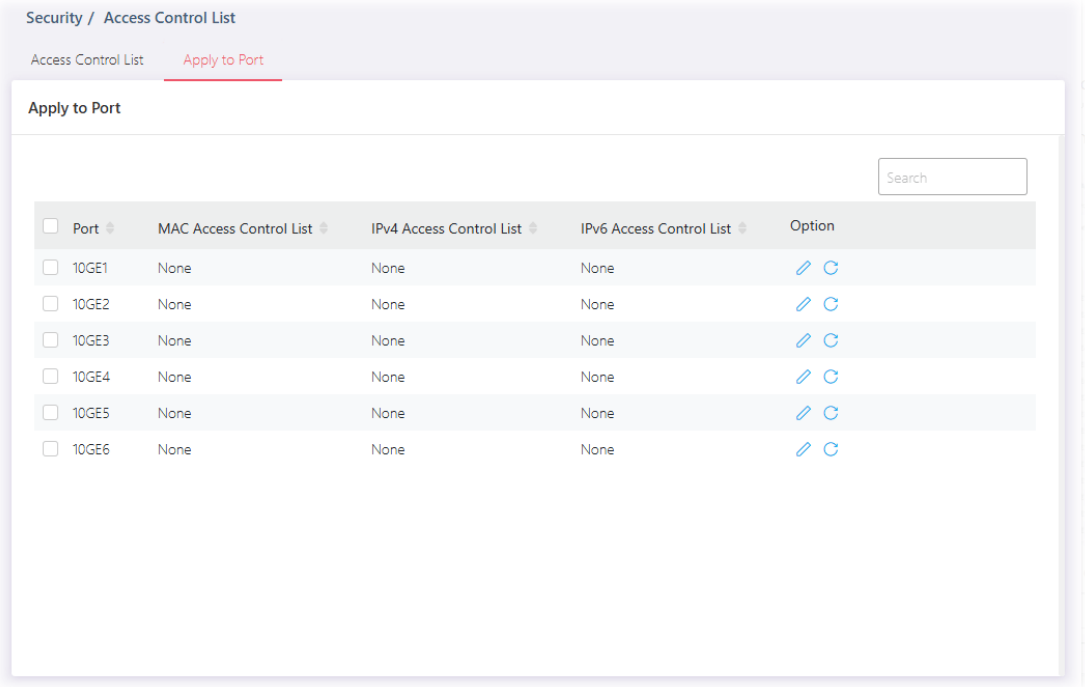
	 **Range** – Only the packets passing through the port range defined here will be filtered. 
Any Destination Port	Specify the destination port number for filtering the packets. **Any Destination Port** – Default setting. All packets will be filtered. Select Any Destination Port. Or, enter the port number. **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. 
Any ICMP Type	**Any ICMP Type** – Default setting. All packets will be filtered. **Echo Reply, Destination Unreachable….** – Choose one of the type (e.g., Destination Unreachable, Echo Reply, MLD Query….) from the drop down list. **Self-Define** – Specify a type number (0 – 255) for ICMP code. For example, 0 means “Echo Reply”; 254 means “RFC3692-style Experiment 2”. 
Any 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 ICMP Code** – Default setting. All packets will be filtered. Select Any ICMP Code. Or, enter 0 to 255 based on the ICMP type specified.

	
+Add Rule	Click it to create a new ACE rule. Each ACL profile can be added with 8 ACE rules.

III-1-2 Apply to Port

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

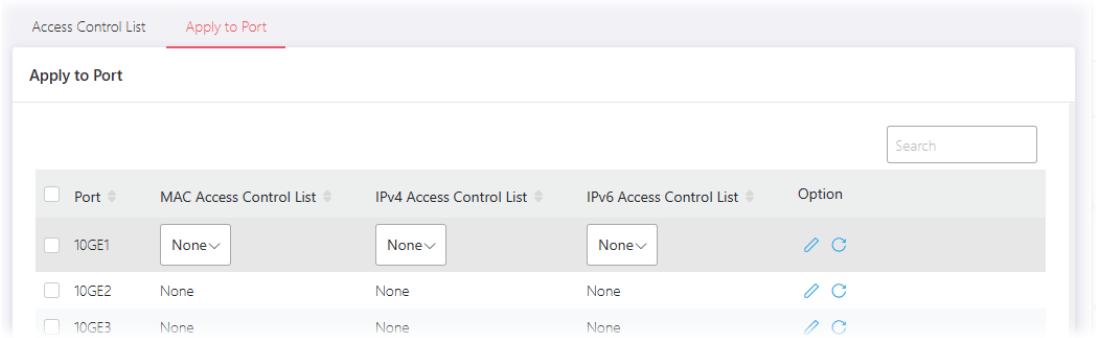
A physical port can only be bound with one of the **IPv4 and IPv6** ACLs, not both.



Available settings are explained as follows:

Item	Description
Port	Select the port profiles (10GE1 to 10GE6) for binding ACL.
MAC Access Control List	Displays the ACL (MAC) to be bound on this interface (port), so the switch may filter packets by using it.
IPv4 Access Control List	Displays the ACL (IPv4) to be bound on this interface (port), so the switch may filter packets by using it.
IPv6 Access Control List	Displays the ACL (IPv6) to be bound on this interface (port), so the switch may filter packets by using it.
Option	- Click it to modify the port setting. - Clear current settings and return to factory default settings.

To modify settings for a port, click the link to open the setting page.



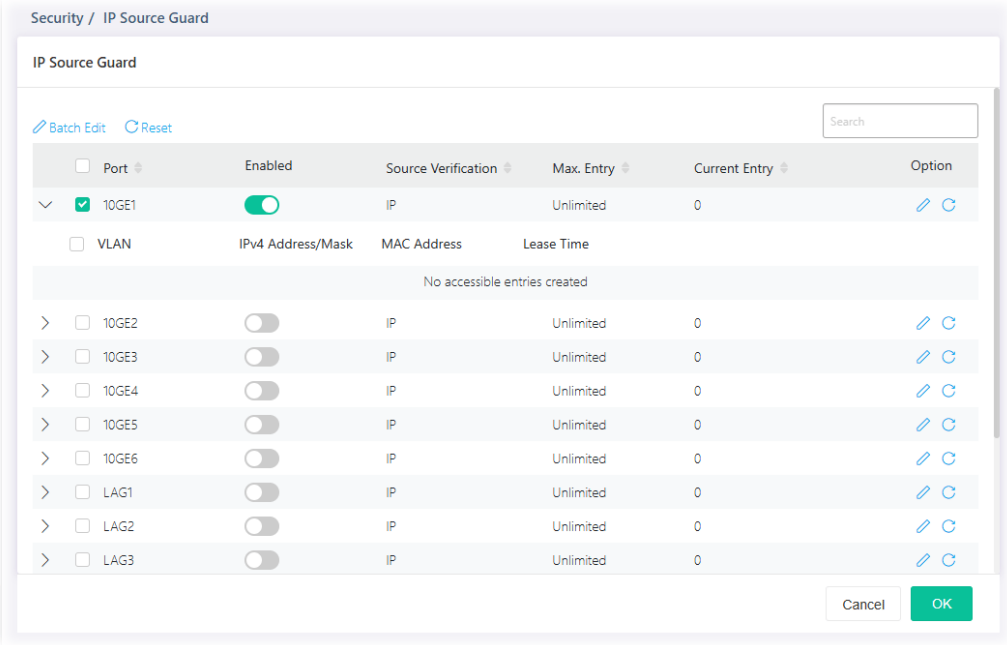
Available settings are explained as follows:

Item	Description
MAC Access Control List	Select an ACL (MAC) to be bound on this interface (port).
IPv4 Access Control List	Select an ACL (IPv4) to be bound on this interface (port).
IPv6 Access Control List	Select an ACL (IPv6) to be bound on this interface (port).

III-3 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.

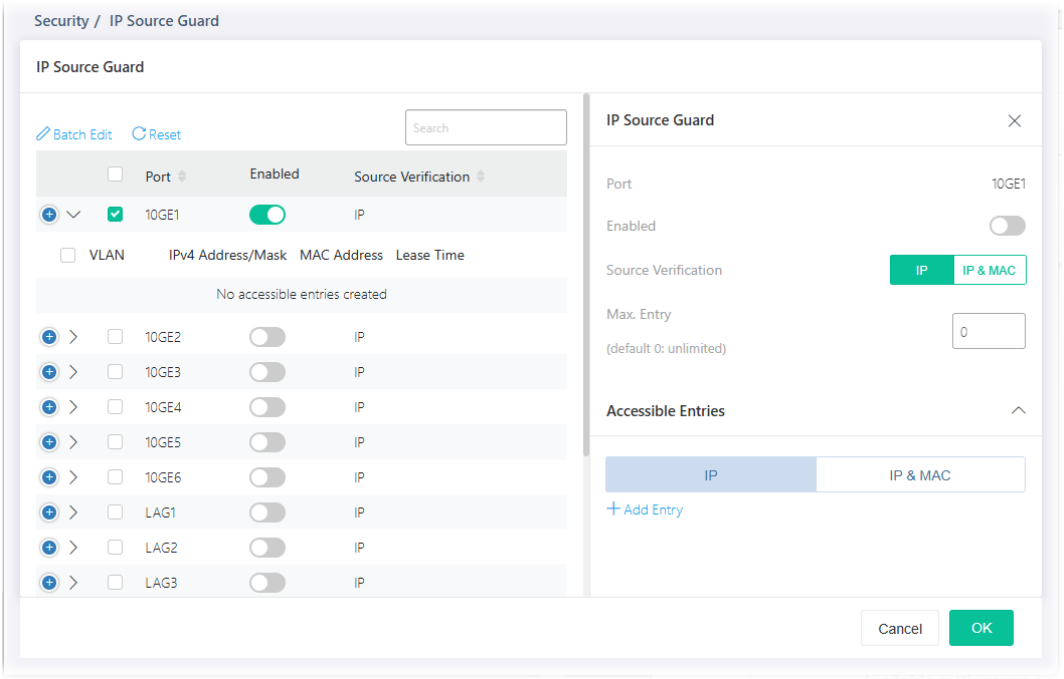
IP source guard is a port-based feature. Therefore, it is necessary to configure detailed settings for each GE/LAG port interface separately.



Available parameters are explained as follows:

Item	Description
Port	Displays the port profile (2.5GE1 to 2.5GE24, 10GE1 to 10GE6, LAG1 to LAG8). Check the box to the left side for applying the IP source guard function.
Enabled	Switch the toggle to enable / disable this profile. - means "Enable". - means "Disable".
Source Verification	Displays the type of source IP for the packet coming from.
Max. Entry	Displays the total number (0~50) of accessible entries allowed for this port.
Current Entry	Displays the number of accessible entries of this port.
Option	- Click it to modify the IP Source Guard setting of the selected port. - Clear current settings and return to factory default settings.

To modify settings for a port, click the link to open the setting page.



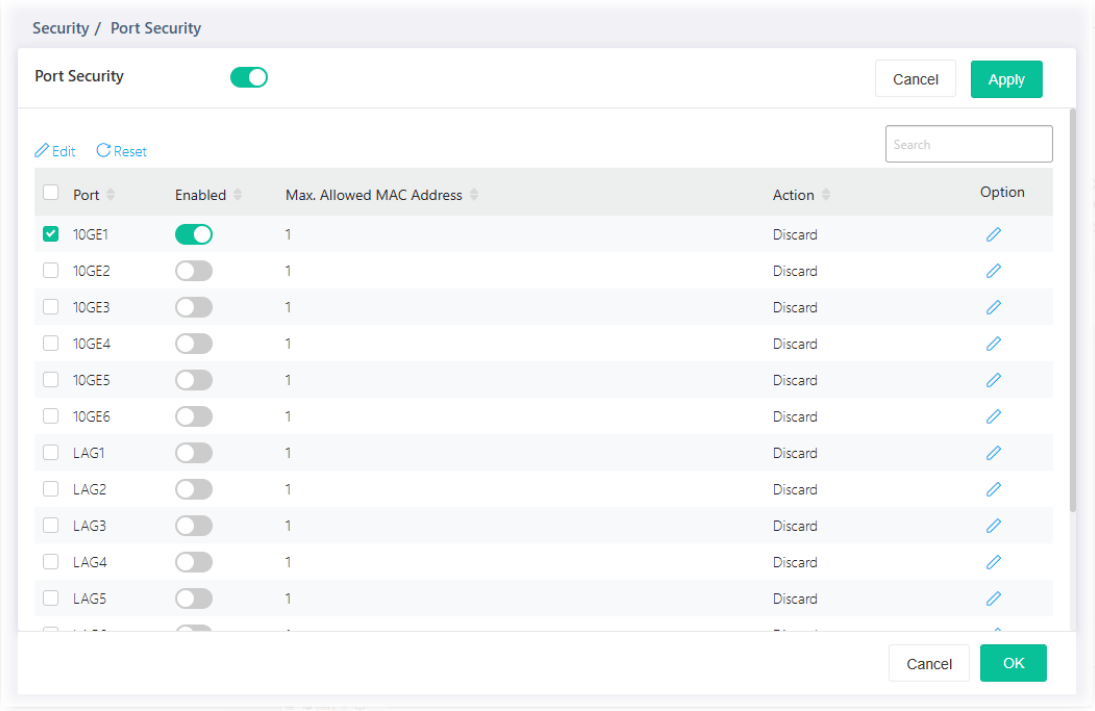
Available settings are explained as follows:

Item	Description
IP Source Guard	
Port	Displays the port profile (10GE1 to 10GE6, LAG1 to LAG8).
Enabled	Switch the toggle to enable / disable this function. - means "Enable". - means "Disable".
Source Verification	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 total number (0~50) of accessible entries allowed for this port. The default is 0 (no limit).
Accessible Entries	Define the entry for applying the IP source guard function. **IP** - Select this type to enter an IPv4 address and set a VLAN ID. **IP & MAC** - Select this type to enter an IP address, MAC address and IPv4 address. **+Add Entry** - Click to display blank entry boxes for configuring a new IP address, MAC address, and VLAN ID.

After finishing this web page configuration, please click **OK** to save the settings.

III-4 Port Security

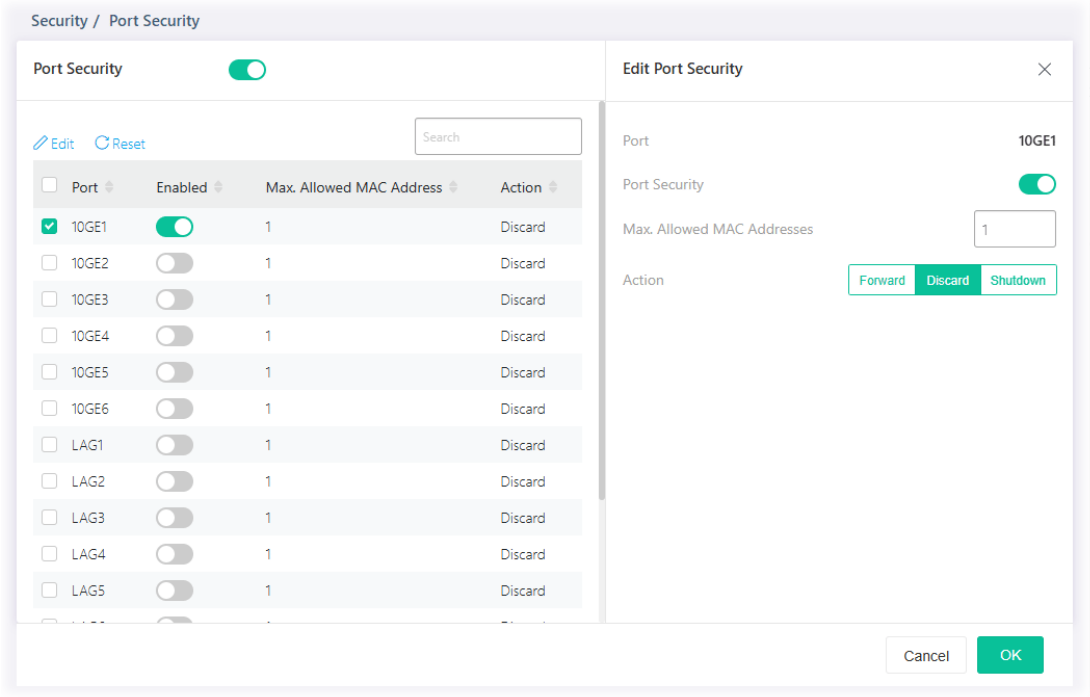
This page allows the network administrator to configure security settings for each port interface (GE port /LAG group). When port security is enabled for each interface, related action will be performed once detecting that the number of MAC address exceeds the limit.



Available settings are explained as follows:

Item	Description
Port Security	Switch the toggle to enable / disable this function. After clicking, press **Apply** to open the configuration page.  - means "Enable". - means "Disable". Enable this function to configure the settings.
Port	Displays the index number of the GE/LAG port.
Enabled	Switch the toggle to enable / disable this function. **Enabled –** The selected port applies the port security settings. **Disabled –** The selected port does not apply the port security settings.
Max. Allowed MAC Address	Displays the maximum number of MAC addresses that the port is allowed to learn.
Action	Displays the action performed by the selected port.
Option	 - Click it to modify the port security setting of the selected port.

To modify settings for a port, click the link to open the setting page.



Available settings are explained as follows:

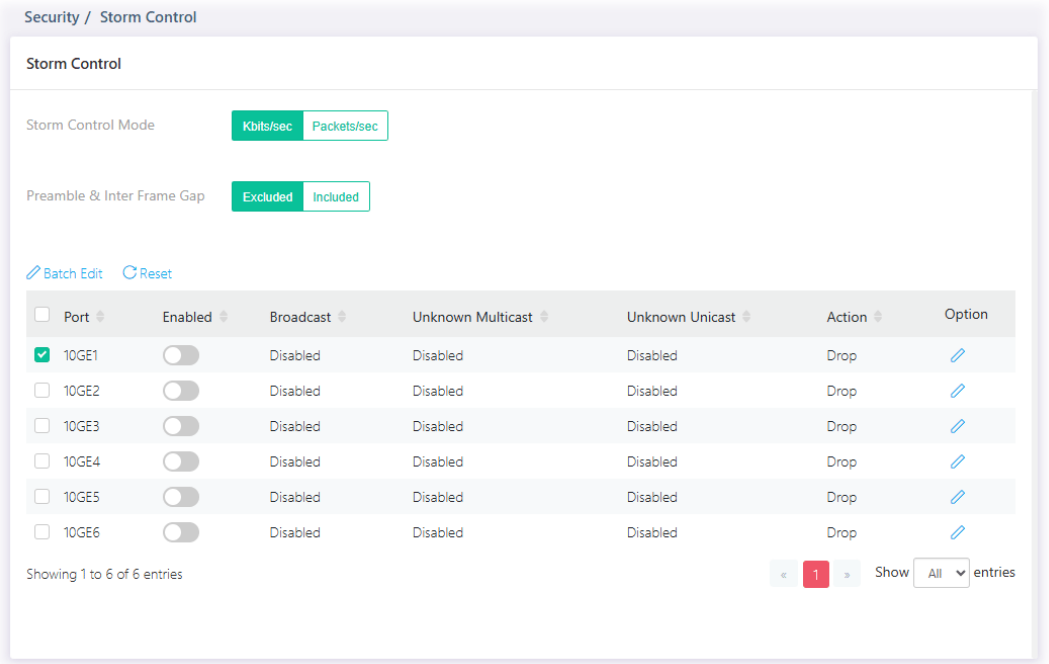
Item	Description
Edit Port Security	
Port	Displays the index number of the GE/LAG port.
Port Security	Switch the toggle to enable / disable this function. **Enabled –** The selected port applies the port security settings. **Disabled –** The selected port does not apply the port security settings.
Max. Allowed 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.
OK	Save the settings.

After finishing this web page configuration, please click **OK** to save the settings.

III-5 Storm Control

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

This page allows a user to configure general settings for Storm Control. In addition, it is used to configure port settings for Storm Control. The configuration result for each port will be displayed on the table listed on the lower side of this web page.

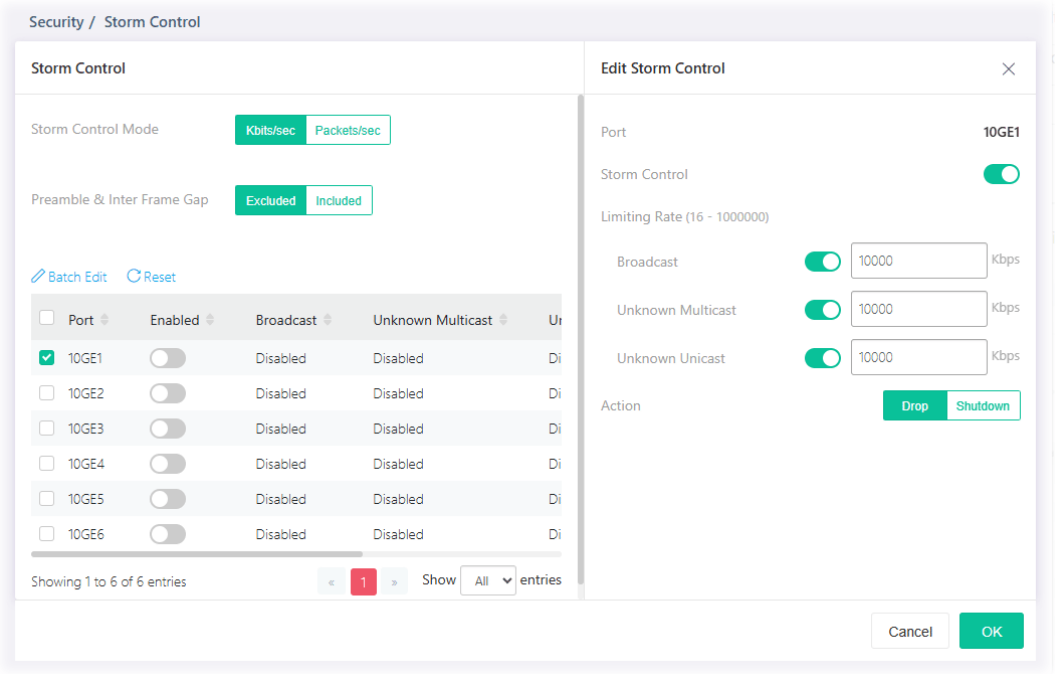


Available settings are explained as follows:

Item	Description
Storm Control Mode	Select the mode of storm control. **Kbits/sec** - Storm control rate will be calculated by octet-based. **Packet/sec** – Storm control rate will be calculated by packet-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.
Batch Edit	Allow to modify settings for more than one port at a time.
Port	Enable/disable the port (GE1 to GE28) profiles.
Enabled	Switch the toggle to enable / disable this profile.  - means “Enable”. - means “Disable”.
Broadcast	Displays the storm control rate limited for broadcast.

Unknown Multicast	Displays the storm control rate limited for unknown multicast.
Unknown Unicast	Displays the storm control rate limited for unknown unicast.
Action	Displays the action performed.
Option	- Click to modify the storm control settings of the selected port.

To modify settings for a port, click the link to open the setting page.



Available settings are explained as follows:

Item	Description
Edit Storm Control	
Port	Display the port profile selected to be modified.
Storm Control	Switch the toggle to enable / disable this function. - means "Enable". - means "Disable".
Limiting Rate	**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.

After finishing this web page configuration, please click **OK** to save the settings.

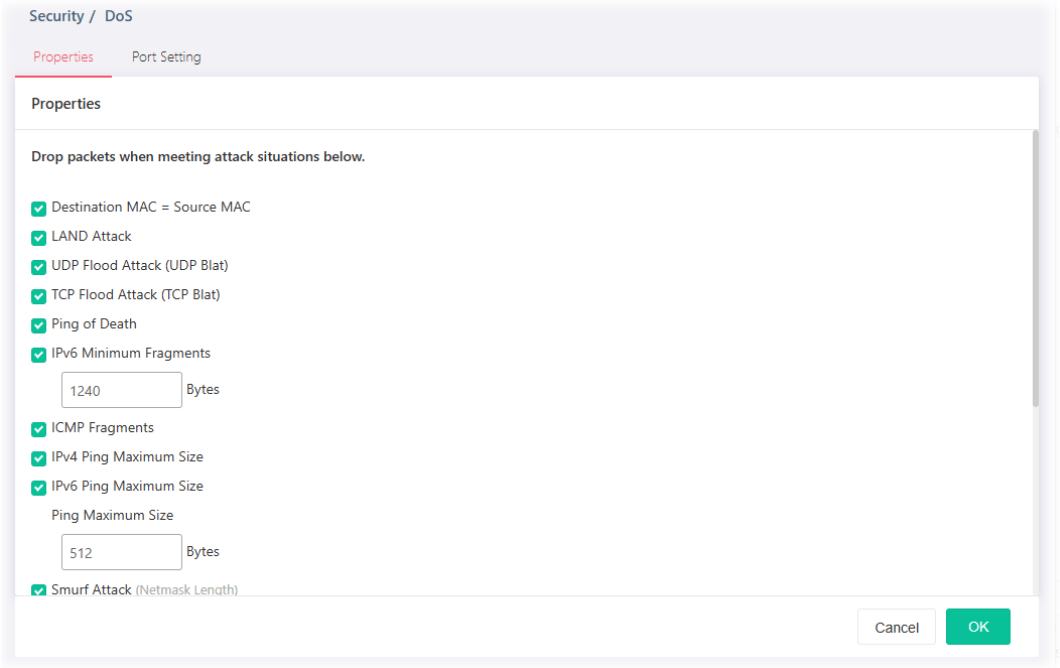
III-6 DoS

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-6-1 Properties

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



Available settings are explained as follows:

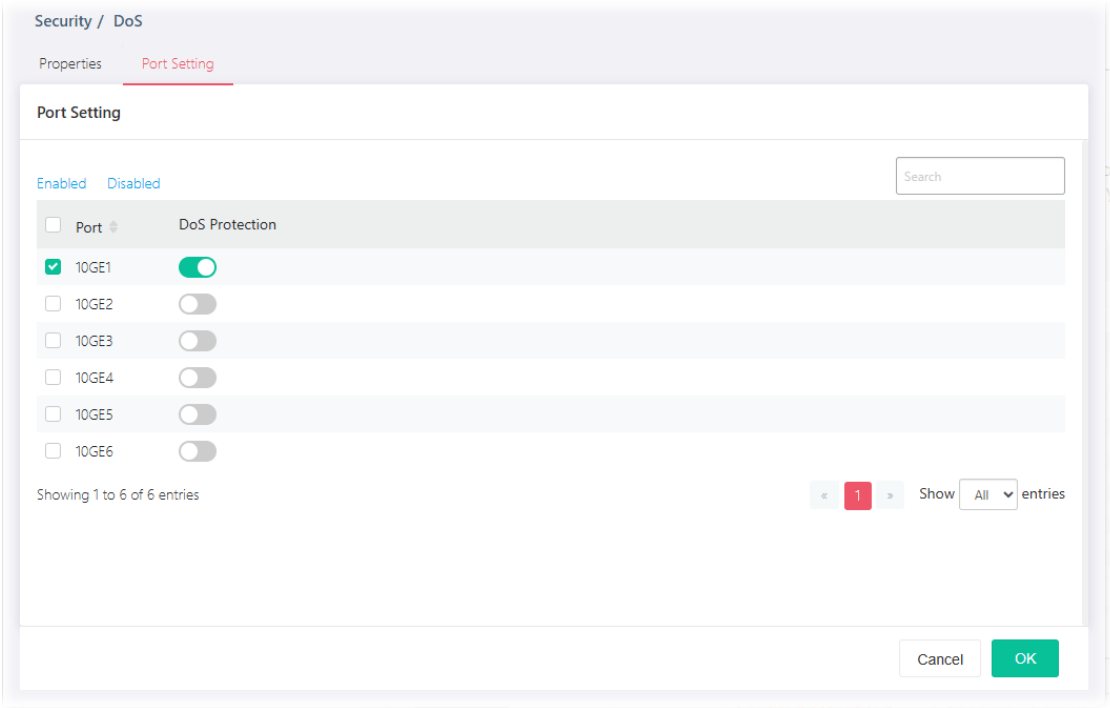
Item	Description
Destination MAC=Source MAC	Drops the packets if the destination MAC address is equal to the source MAC address. Check/uncheck the box to enable/disable the function.
LAND Attack	Drops the packets if the source IP address is equal to the destination IP address. Check/uncheck the box to enable/disable the function.
UDP Flood Attack (UDP Blat)	Drops the packets if the UDP source port equals to the UDP destination port. Check/uncheck the box to enable/disable the function.
TCP Flood Attack (TCP Blat)	Drops the packages if the TCP source port is equal to the TCP destination port. Check/uncheck the box to enable/disable the function.
Ping to Death	Avoids ping of death attack. Ping packets that length are larger than 65535 bytes.

	Check/uncheck the box to enable/disable the function.
IPv6 Minimum Fragments	Checks 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. Check/uncheck the box to enable/disable the function.
ICMP Fragments	Drops the fragmented ICMP packets. Check/uncheck the box to enable/disable the function.
IPv4 Ping Maximum Size	Determines the IPv4 PING packet with the length. Check/uncheck the box to enable/disable the function.
IPv6 Ping Maximum Size	Determines the IPv6 PING packet with the length. Check/uncheck the box to enable/disable the function. **Ping Maximum Size** - 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	Avoids smurf attack. The length range of the netmask is from 0 to 323 bytes, and default length is 0 byte. Check/uncheck the box to enable/disable the function.
TCP Minimum Header Size	Checks 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. Check/uncheck the box to enable/disable the function.
TCP-SYN (SPORT<1024)	Drops SYN packets with sport less than 1024. Check/uncheck the box to enable/disable the function.
Null Scan Attack	Drops the packets with NULL scan. Check/uncheck the box to enable/disable the function.
X-mas Scan Attack	Drops the packets if the sequence number is zero, and the FIN, URG and PSH bits are set. Check/uncheck the box to enable/disable the function.
TCP SYN-FIN Attack	Drops the packets with SYN and FIN bits set. Check/uncheck the box to enable/disable the function.
TCP SYN-RST Attack	Drops the packets with SYN and RST bits set. Check/uncheck the box to enable/disable the function.
TCP Fragment (Offset=1)	Drops the fragmented ICMP packets. Check/uncheck the box to enable/disable the function.

After finishing this web page configuration, please click **OK** to save the settings.

III-6-2 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.



Available settings are explained as follows:

Item	Description
Enabled / Disabled	Appears when one or more of the following ports are selected. Enabled – Click to enable the DoS Protection function for the selected port. Disabled – Cllick to disable the DoS Protection function for the selected port.
Port	Displays the port profile (10GE1 to 10GE6). Check the box to the left side to select the port profile.
DoS Protection	Switch the toggle to enable / disable the function of DoS Protection. - means "Enable". - means "Disable".

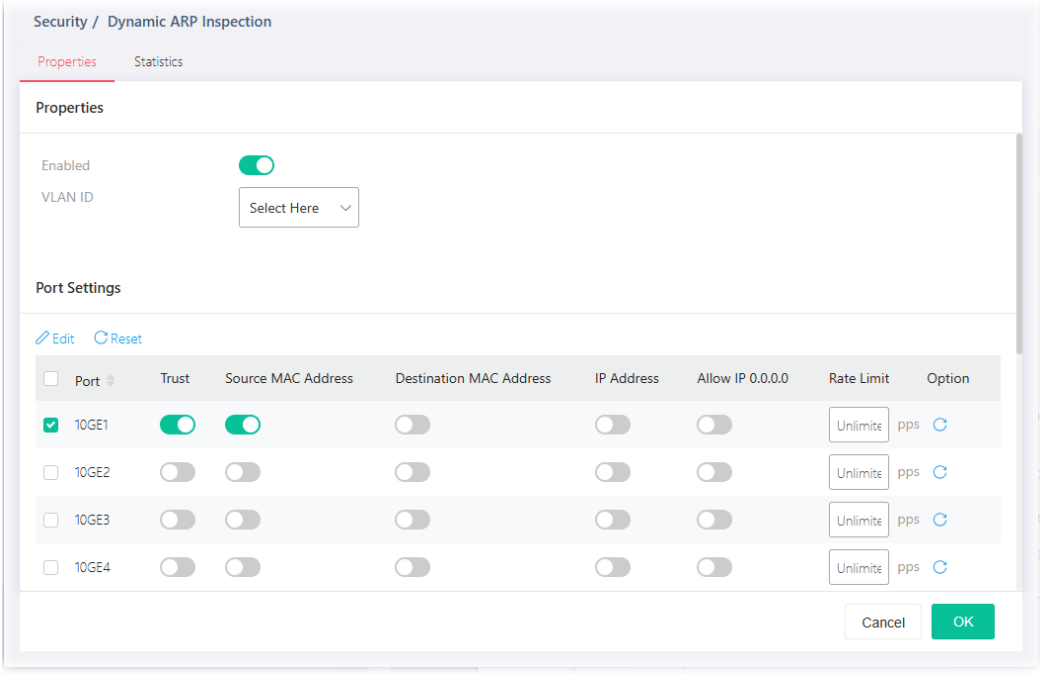
After finishing this web page configuration, please click **OK** to save the settings.

III-7 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-7-1 Properties

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

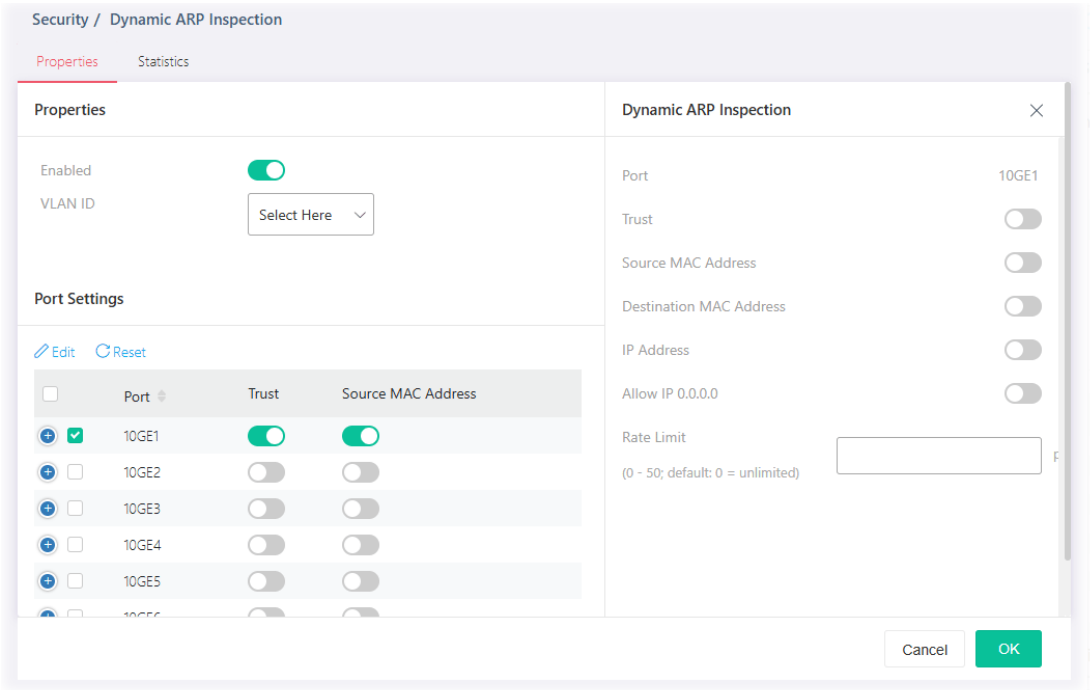


Available settings are explained as follows:

Item	Description
Enabled	Switch the toggle to enable / disable the function of Dynamic ARP Inspection. - means "Enable". - means "Disable".
VLAN ID	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.
Port Settings	
Edit	Appears when one or more of the following ports are selected.
Reset	Clear current settings and return to factory default settings.
Port	Displays the port (10GE1 to 10GE6, LAG1 to LAG8) or ports for applying DAI function.

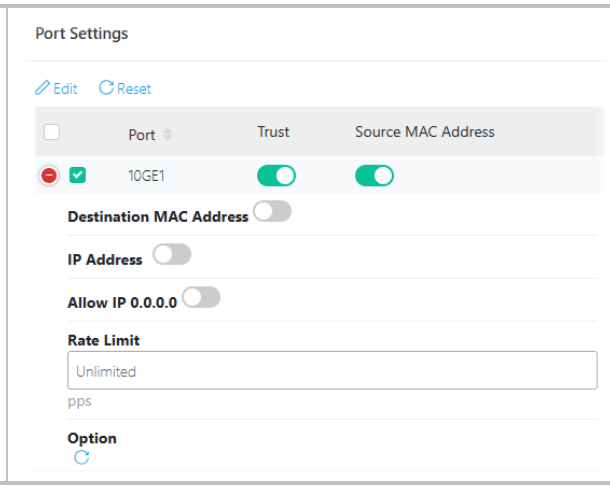
Trust	Switch the toggle to enable/disable the function of DAI for this port.
Source MAC Address	Switch the toggle to enable/disable the function of the source MAC address validation mechanism for this port.
Destination MAC Address	Switch the toggle to enable/disable the function of the destination MAC address validation mechanism for this port.
IP Address	Switch the toggle to enable/disable the function of IP address validation mechanism for this port.
Allow IP 0.0.0.0	Switch the toggle to enable/disable the function. The IP address of "0.0.0.0" can be applied to this port if it is enabled.
Rate Limit	Enter a rate limitation value (0~50) for this port.
Option	- Clear current settings and return to factory default settings.
OK	Save the settings.

In addition, you may click the Edit link to open the setting page for modifying the above settings.



Available settings are explained as follows:

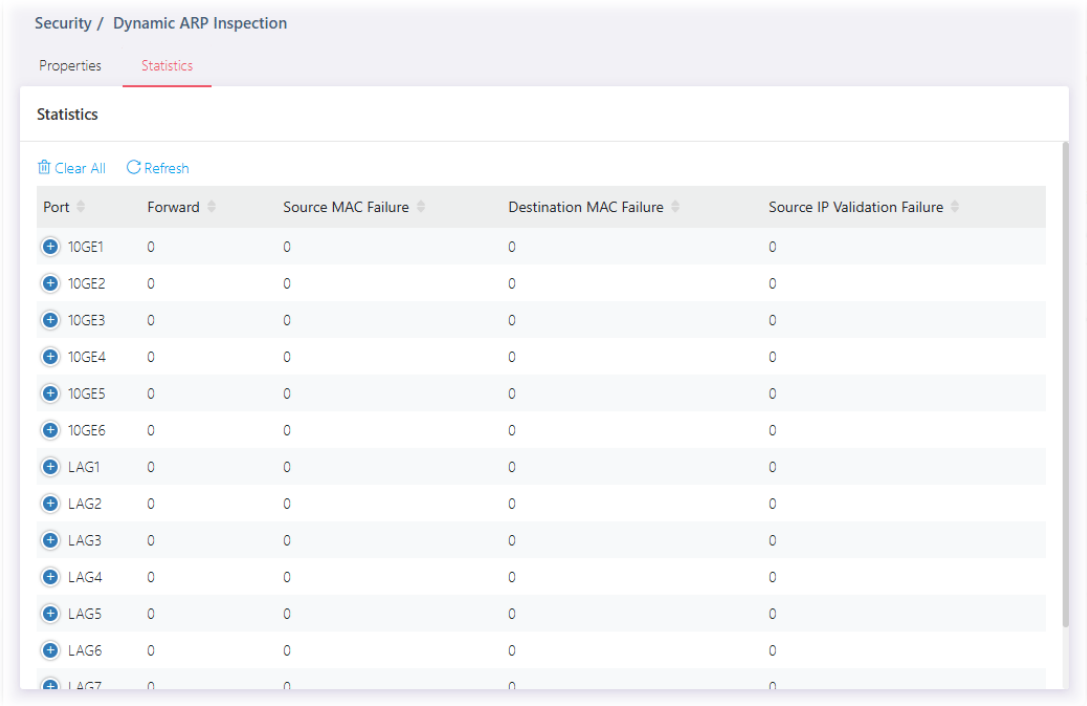
Item	Description
	Click to modify the Destination MAC Address, IP Address, Allow IP 0.0.0.0 and Rate Limit value.



After finishing this web page configuration, please click **OK** to save the settings.

III-7-2 Statistics

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



III-8 DHCP Snooping

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

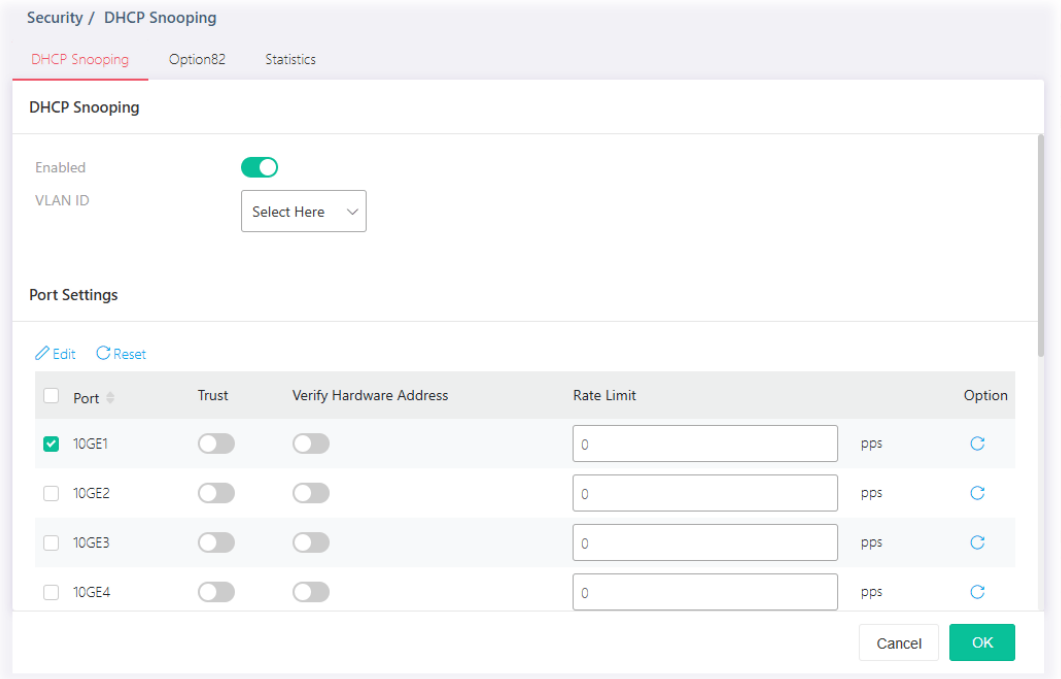
For DHCP snooping to function properly, it is suggested to connect DHCP servers to VigorSwitch through trusted interfaces; because untrusted DHCP messages will be forwarded to trusted interfaces only.

III-8-1 DHCP Snooping

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

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 a trusted device by configuring the trust state of its connecting port.



Available settings are explained as follows:

Item	Description
Enabled	Switch the toggle to enable / disable the function of DHCP Snooping. - means "Enable". - means "Disable".
VLAN ID	Select VLAN profile(s) to apply the function of DHCP Snooping

	function. Only the GE/LAG port within the selected VLAN will apply DHCP Snooping function.
Port Settings	
Port	Displays the port (10GE1 to 10GE6, LAG1 to LAG8) or ports for applying the DHCP snooping function.
Edit	It is available if one of the Ports is selected. Click to modify the settings of Trust, Verify Hardware Address, and the rate limit value.
Trust	Switch the toggle to enable/disable the function of DHCP snooping for this port.
Verify Hardware Address	Switch the toggle to enable/disable 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 the source MAC in Ethernet header or not. Default is disabled.
Rate Limit	Enter the rate limitation (0~300) of DHCP packets. The unit is “pps”. “0” means unlimited. Default is unlimited.
Option	- Clear current settings and return to factory default settings.
OK	Save the settings.

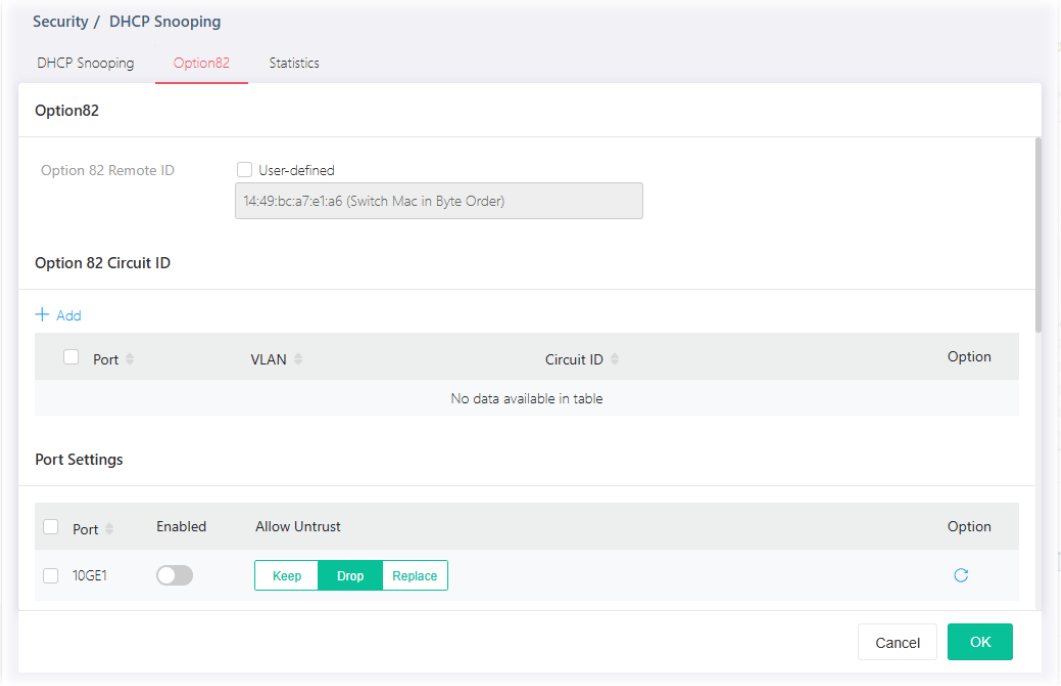
After finishing this web page configuration, please click **OK** to save the settings.

III-8-2 Option82

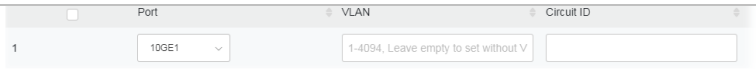
You can use information settings including Remote ID and Circuit ID for Option82, also known as the DHCP relay agent, to protect VigorSwitch against spoofing attacks.

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

In addition, it 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).



Available settings are explained as follows:

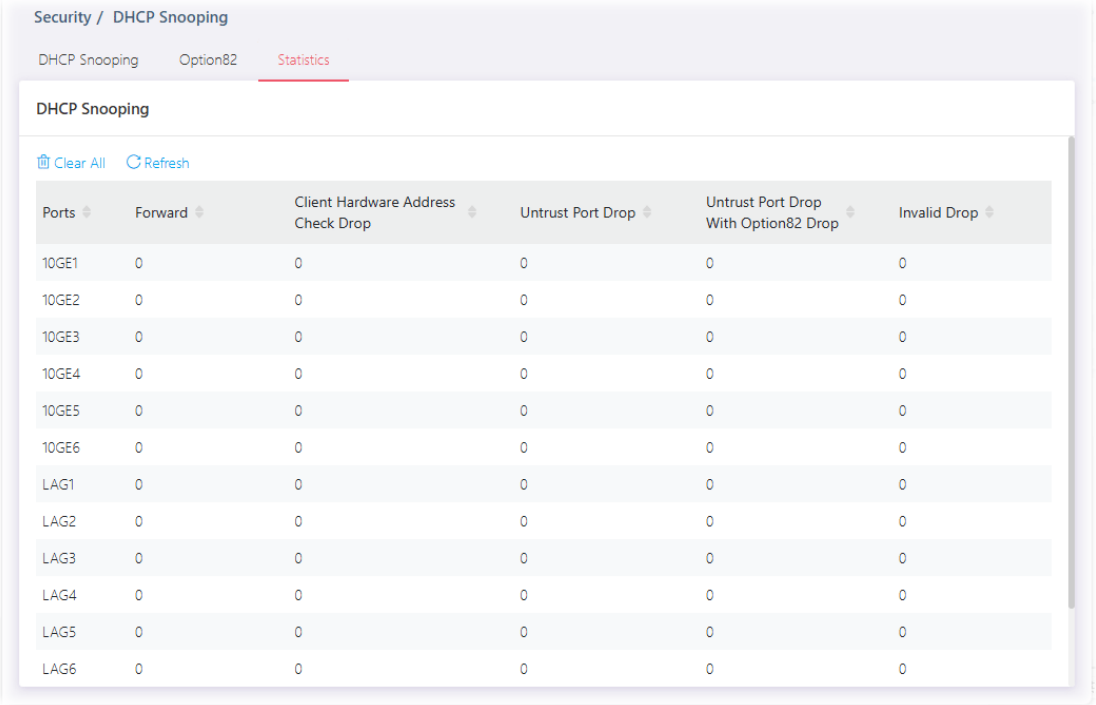
Item	Description
Option82	
Option 82 Remote ID	The string specified here is used to identify the remote host. **User-defined -** Check it and manually enter switch MAC in byte order in the entry box.
Option 82 Circuit ID	
+Add	 **Port -** Use the drop down list to select the port (10GE1 to 10GE12, LAG1 to LAG8) or ports for applying DHCP snooping, Option82 function. **VLAN** - Choose a number as VLAN ID which is easy to be identified for a packet containing with it. **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.
Port Settings	
Port	Displays the port (10GE1 to 10GE6, LAG1 to LAG8) or ports for applying the Option82 function.
Enabled	Switch the toggle to enable / disable the function of Option82 Property.  - means “Enable”. - means “Disable”.
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.
Option	- Clear current settings and return to factory default settings.
OK	Save the settings.

After finishing this web page configuration, please click **OK** to save the settings.

III-8-3 Statistics

This page displays all statistics recorded by DHCP snooping function.

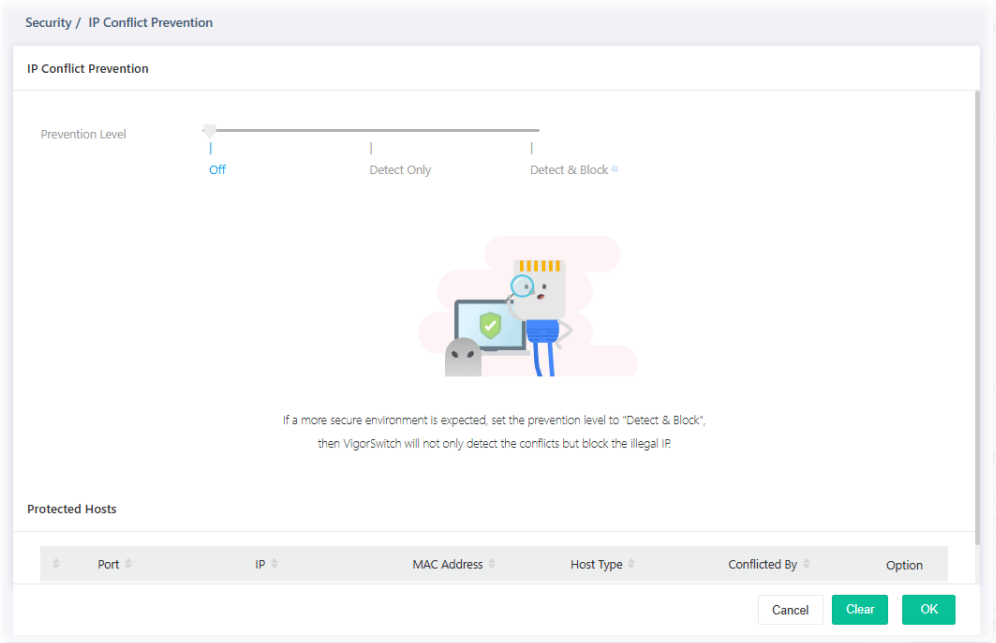


III-9 IP Conflict Prevention

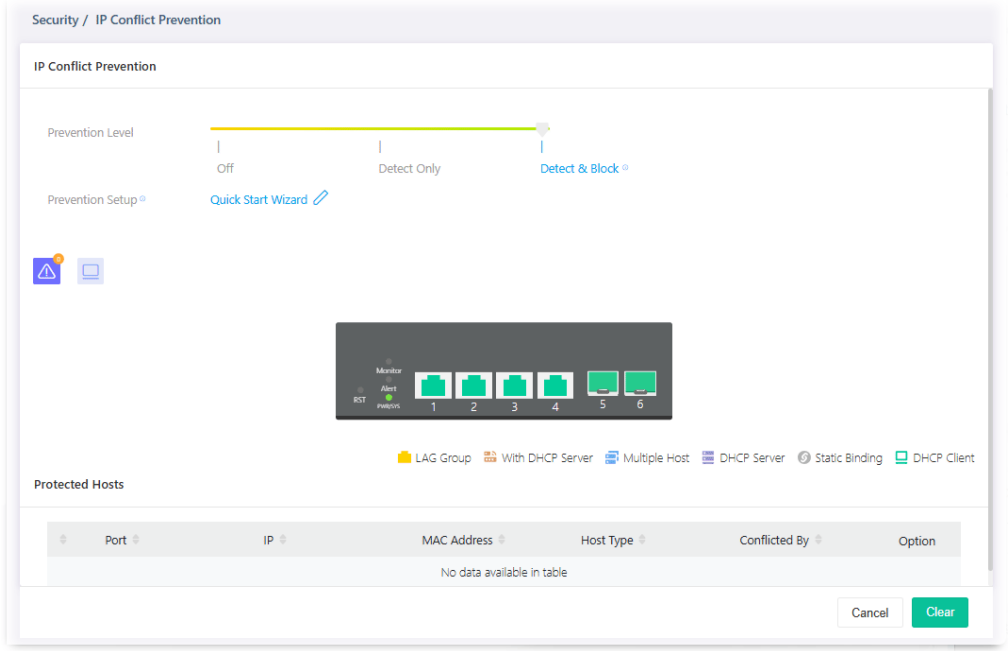
A user can configure IP addresses for network devices manually. However, it might result in conflict between different devices due to using the same IP address, and cause the devices not working correctly.

IP Conflict Prevention allows you to prevent IP conflict by binding the port with the specified IP address.

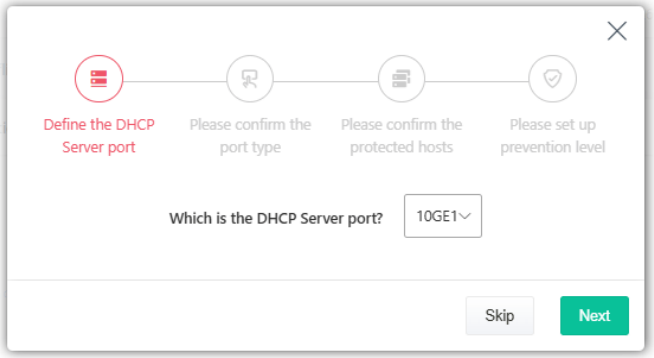
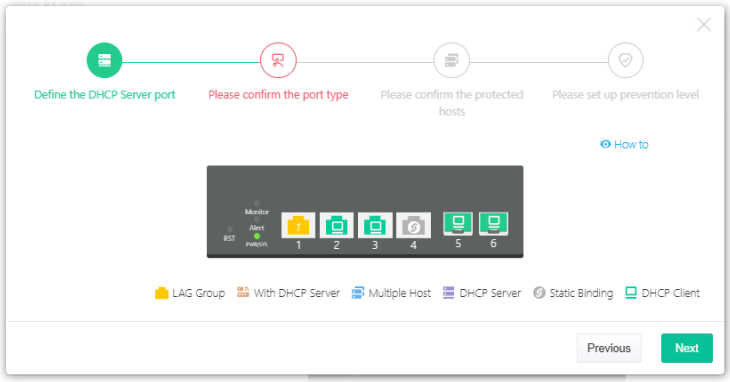
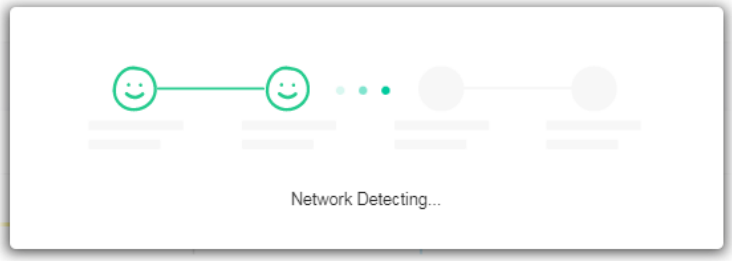
Prevention Level: Off

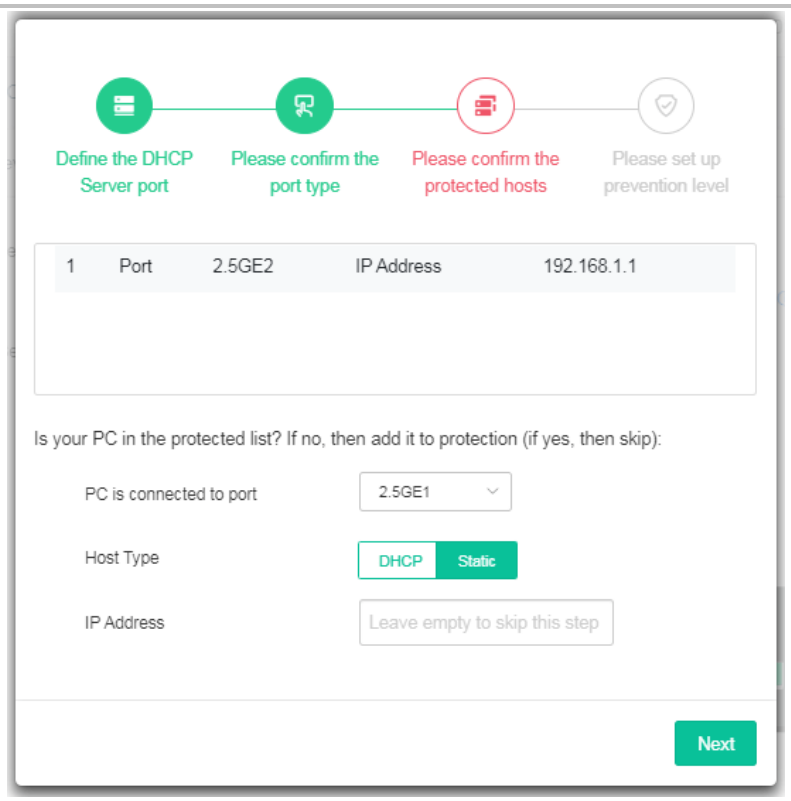


Prevention Level: Detect & Block

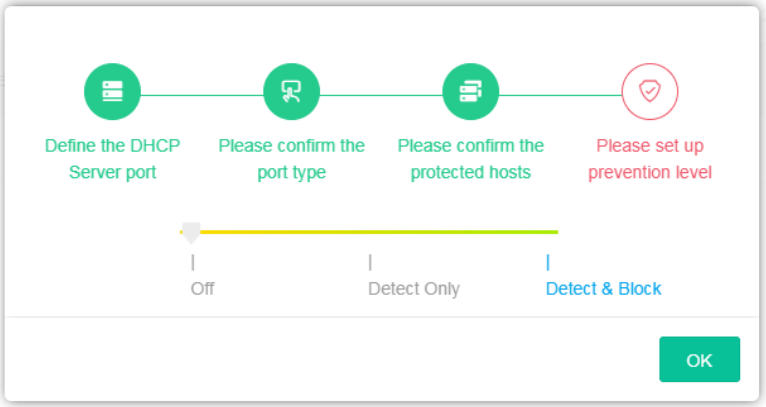


Available settings are explained as follows:

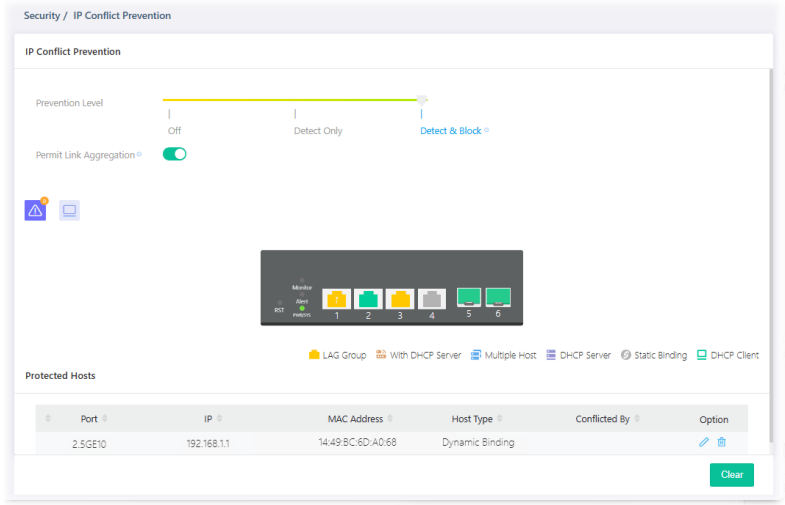
Item	Description
IP Conflict Prevention	
Prevention Level	**Off** - The function of IP conflict prevention is disabled. **Detect Only** - VigorSwitch will detect the host but no further action executed. **Detect & Block** - VigorSwitch will detect the host and block the host if it meets the configuration on this page.
Prevention Setup	**Quick Setup Wizard** - It is available only when **Detect & Block** is selected as Prevention Level. The system will guide to bind server port with an IP address step by step. Step 1: Choose a server port. Click Next.  Step 2: Confirm the port type. Click Next.  Step 3: Wait for the network detection.  Step 4: Confirm / modify the protected host. Click Next.



Step 5: Set up the prevention level. Click Next.



After clicking **OK**, the IP address specified for the GE port will be unavailable for other network devices.

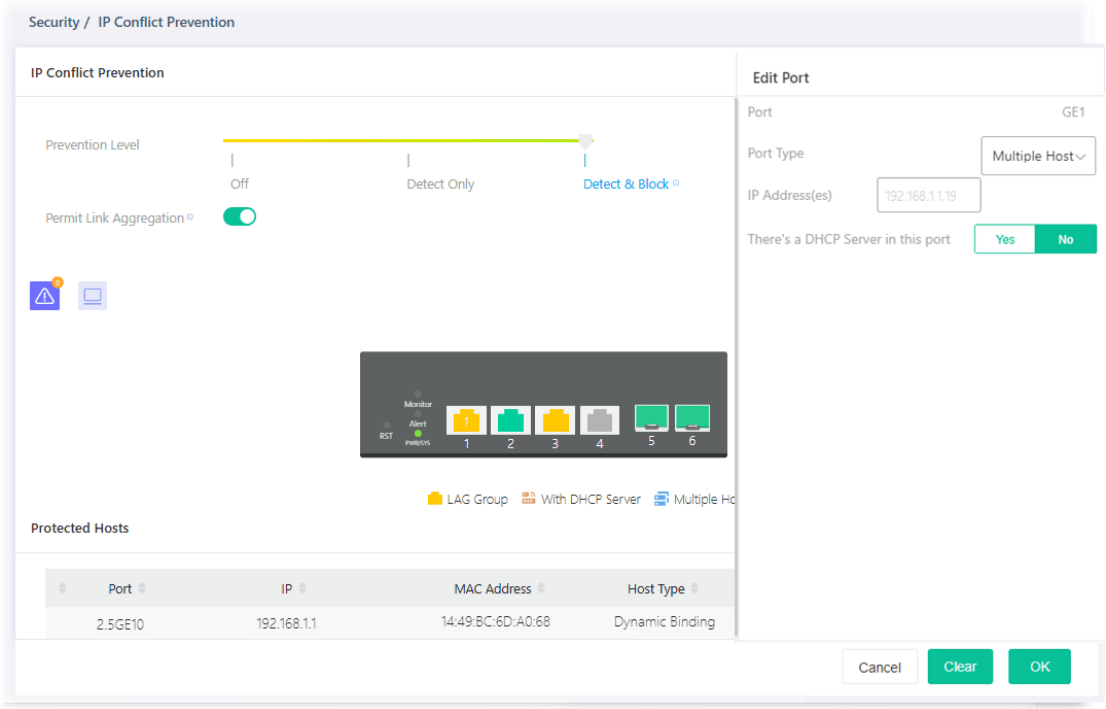


Permit Link	It appears after running the quick start wizard for IP conflict

Aggregation	prevention. The devices connected to the LAG ports will not be blocked due to using the same IP.
Protected Host	
Port	Displays the LAN port number (2.5GE1 to 2.5GE24, 10GE1 to 10GE6, LAG1 to LAG8) of the DHCP server.
IP	Displays the IP address of the DHCP server.
MAC Address	Displays the MAC address of the DHCP server.
Host Type	Displays the result of host type (e.g., Dynamic Binding) of the DHCP server.
Conflicted By	Displays the object conflicting with the host.
Option	- Click to modify the settings of the selected port. - Click it to remove the selected entry.
Clear	Click it to remove all entries.

After finishing this web page configuration, please click **OK** to save the settings.

To modify settings for a host, click the link of each port to open the setting page.



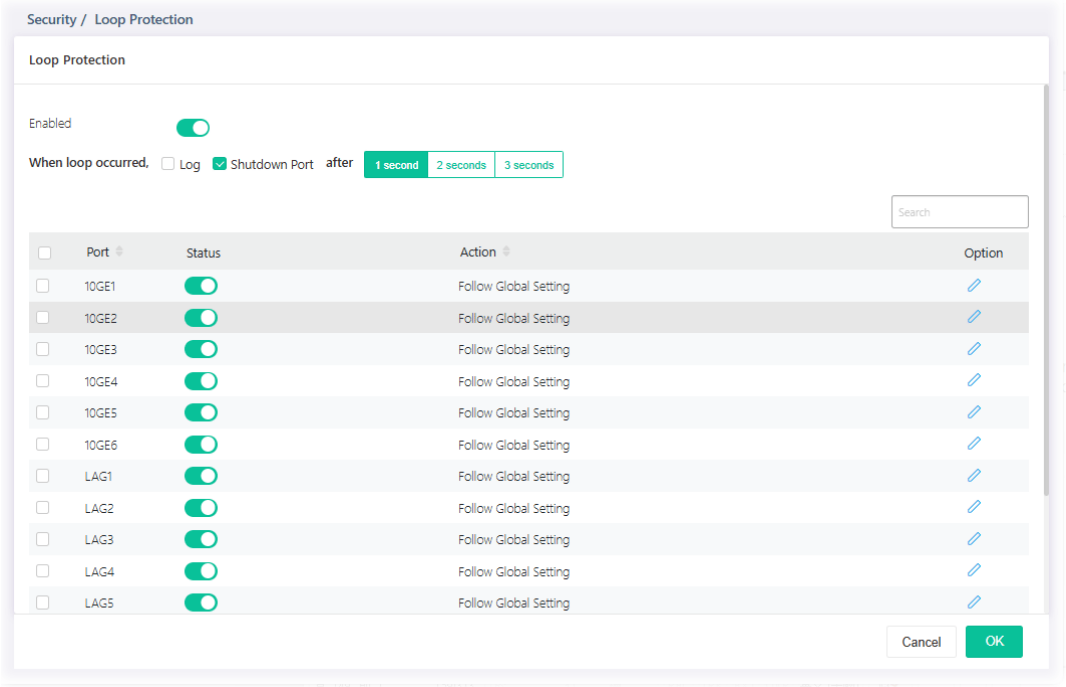
Available settings are explained as follows:

Item	Description
Edit Port	
Port	Displays the LAN port number (10GE1 to 10GE6, LAG1 to LAG8) of the selected host.
Port Type	Specify the port type for the selected host.

	• DHCP Client • Static Binding • Multiple Host • DHCP Server
IP Address(es)	Enter the IP address based on the port type.
There's a DHCP Server in this port	Yes - If there is a DHCP server in this port already, click Yes. No - If there is no DHCP server in this port already, click No.

III-10 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 looped packet.

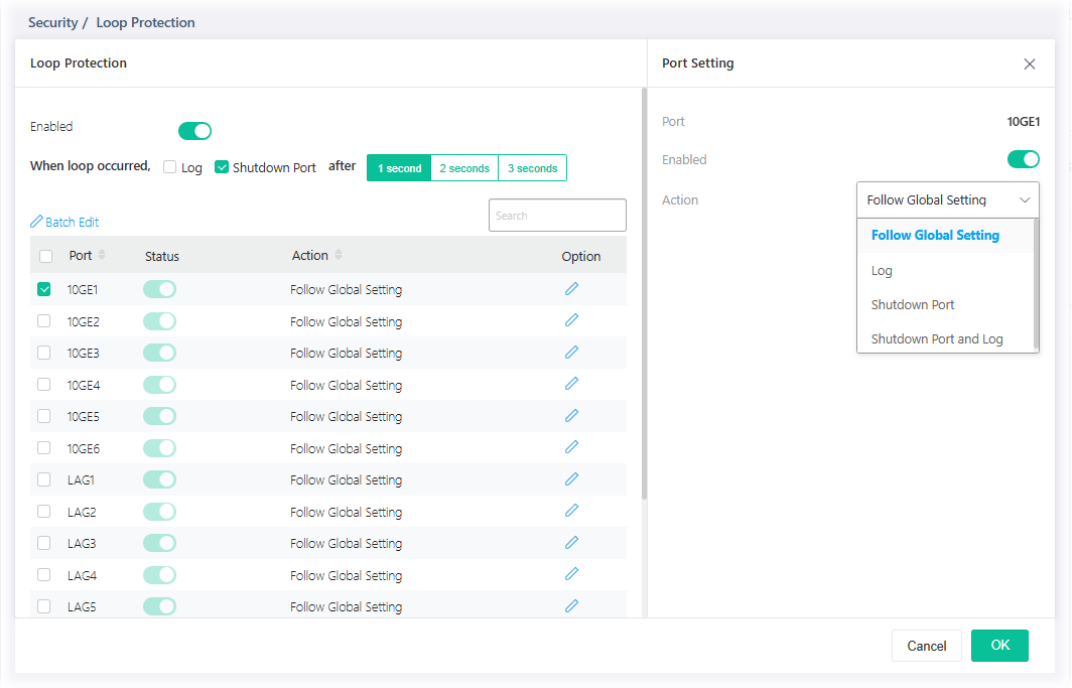


Available settings are explained as follows:

Item	Description
Loop Protection	
☐ / Status	**Enable / Disable** – Switch the toggle to enable / disable this function. VigorSwitch will detect the loop event of the GE port automatically. - means "Enable". - means "Disable".
When loop occurred..	When the switch detects loop situation occurred to a port; it will perform the action selected in this field. **Log** - The switch will record such event as a log. **Shutdown Port** - The switch will shut down the port. **After 1 second/2 seconds/3 seconds** - Determine the time to record the event and / or shutdown the port. The settings configured here will be treated as global setting for all GE ports.
Port	Displays the port number (2.5GE1 to 2.5GE24, 10GE1 to 10GE6, LAG1 to LAG8). Check the box to the left to enable the selected port.
Status	**Enable / Disable** – Switch the toggle to enable / disable this function.
Action	Display the specified action for the selected port.

Option	- Click to modify the loop protection settings of the selected port.

To modify settings for a port, click the link to open the setting page.



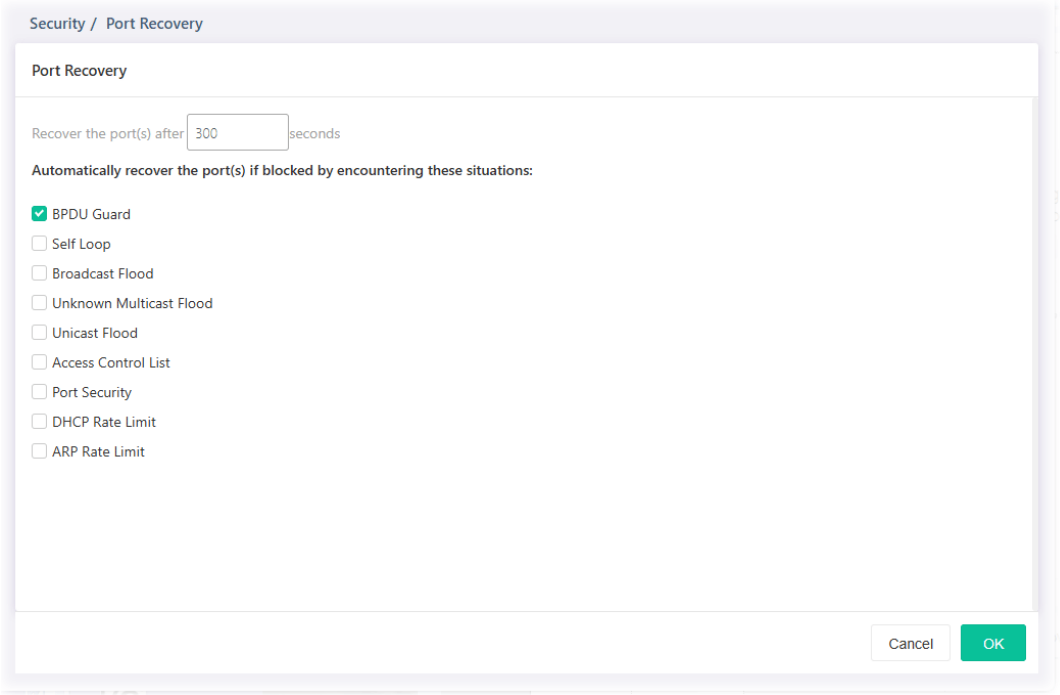
Available settings are explained as follows:

Item	Description
Port Setting	
Port	Displays the port number (10GE1 to 10GE6, LAG1 to LAG8).
Enabled	**Enable / Disable** – Switch the toggle to enable / disable this function. VigorSwitch will detect the loop event of the GE port automatically. - means "Enable". - means "Disable".
Action	**Follow Global Setting** - Adopts the settings configured for **When loop occurred**. **Log** - The switch will record 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.

After finishing this web page configuration, please click **OK** to save the settings.

III-11 Port Recovery

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.



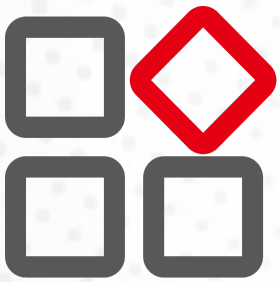
Available settings are explained as follows:

Item	Description
Port Recovery	
Recover the port(s) after	The port being blocked will be able to receive and send traffic after the time period configured here.
Check the box to block the port(s) if encountering the situations listed below.	
BPDU Guard	**Checked** - Recover the port being blocked by BPDU Guard after the time set in Recovery Interval.
Self Loop	**Checked** - Recover the port being blocked by self loop Guard after the time set in Recovery Interval.
Broadcast Flood	**Checked** - Recover the port being blocked by broadcast flood after the time set in Recovery Interval.
Unknown Multicast Flood	**Checked** - Recover the port being blocked by unknown multicast flood after the time set in Recovery Interval.
Unicast Flood	**Checked** - Recover the port being blocked by unicast flood after the time set in Recovery Interval.
Access Control List	**Checked** - Recover the port being blocked by ACL after the time set in Recovery Interval.
Port Security	**Checked** - Recover the port being blocked by port security after the time set in Recovery Interval.

DHCP Rate Limit	**Checked** - Recover the port being blocked by DHCP rate limit after the time set in Recovery Interval.
ARP Rate Limit	**Checked** - Recover the port being blocked by ARP rate limit after the time set in Recovery Interval.

This page is left blank.

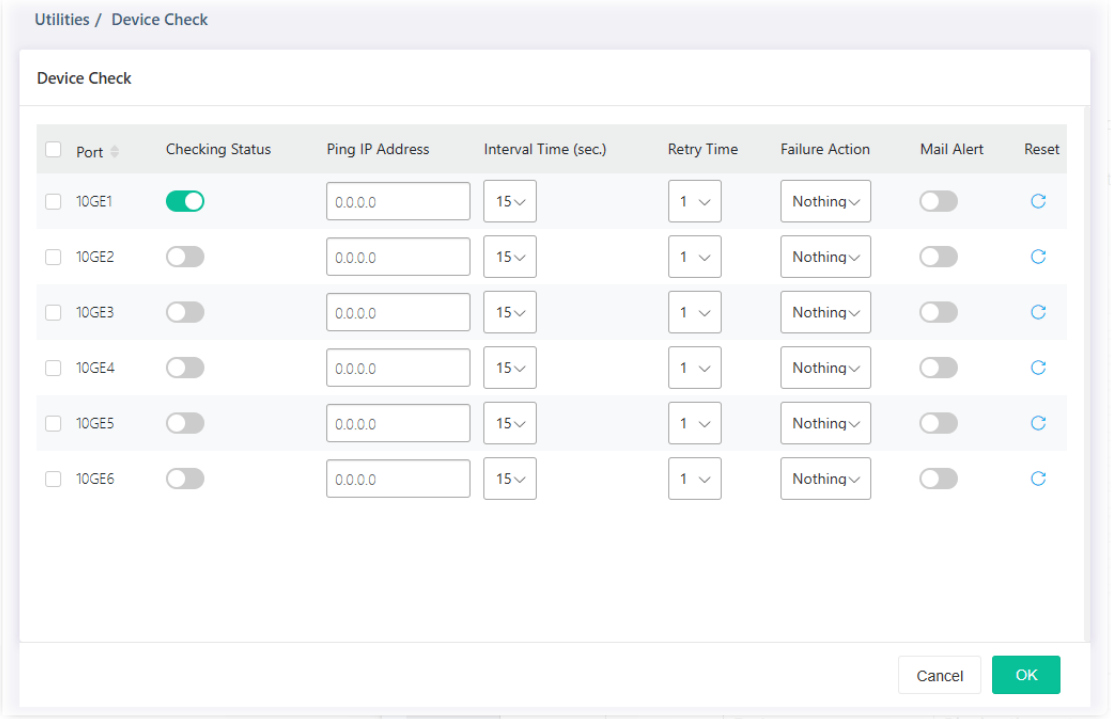
Chapter IV Utilities



IV-1 Device Check

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

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



Available settings are explained as follows:

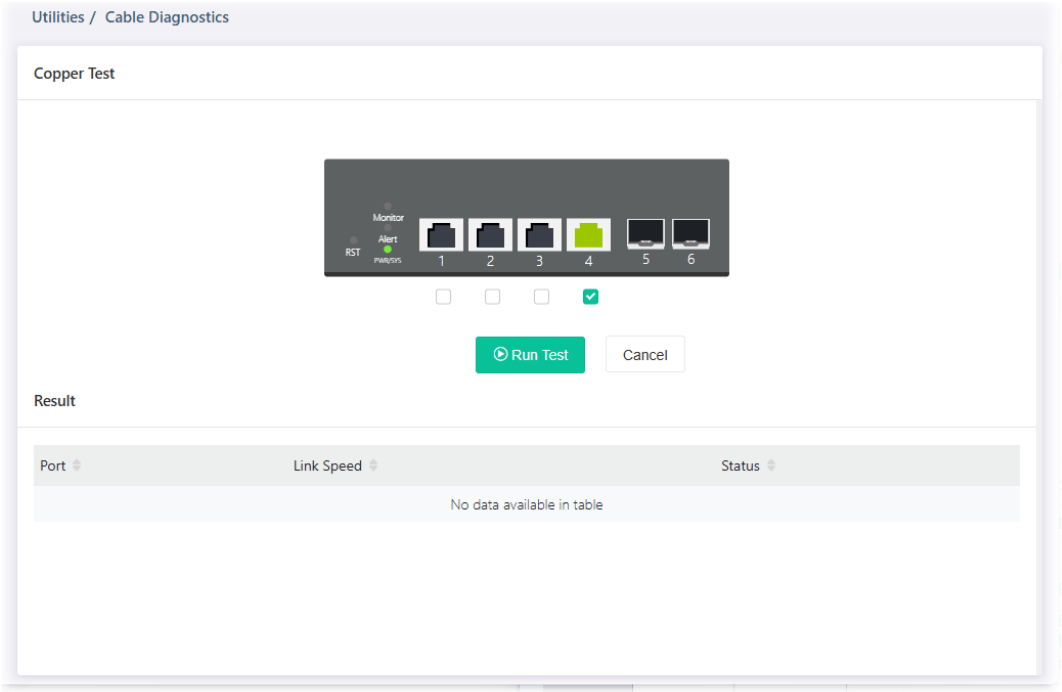
Item	Description
Port	Display the port number (10GE1 to 10GE6). Check the box to the left to enable the port settings.
Checking Status	**Enable / Disable** – Switch the toggle to enable / disable this function. - means "Enable". - means "Disable".
Ping IP Address	Enter the IP address of the PoE device for check.
Interval Time (sec.)	The ping check will be performed every 15, 30, 60 or 120 seconds for the selected port (PoE device).
Retry Time	The system will perform the ping check the selected port (PoE device) for 1, 3 or 5 times.
Failure Action	Specify the action performed for PoE device when there is no number of retry time of echo from given IP address. • **Power Cycle** - Force reboot the device by cycling the power given to the PoE device.

	• **Power Off** - The PoE device will be powered off. • **Nothing** - Log this event only, no action is taken on PoE device.
Mail Alert	**Enable / Disable** – Switch the toggle to enable / disable this function.
Reset	- Clear current settings and return to factory default settings.

After finishing this web page configuration, please click **OK** to save the settings.

IV-2 Cable Diagnostics

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



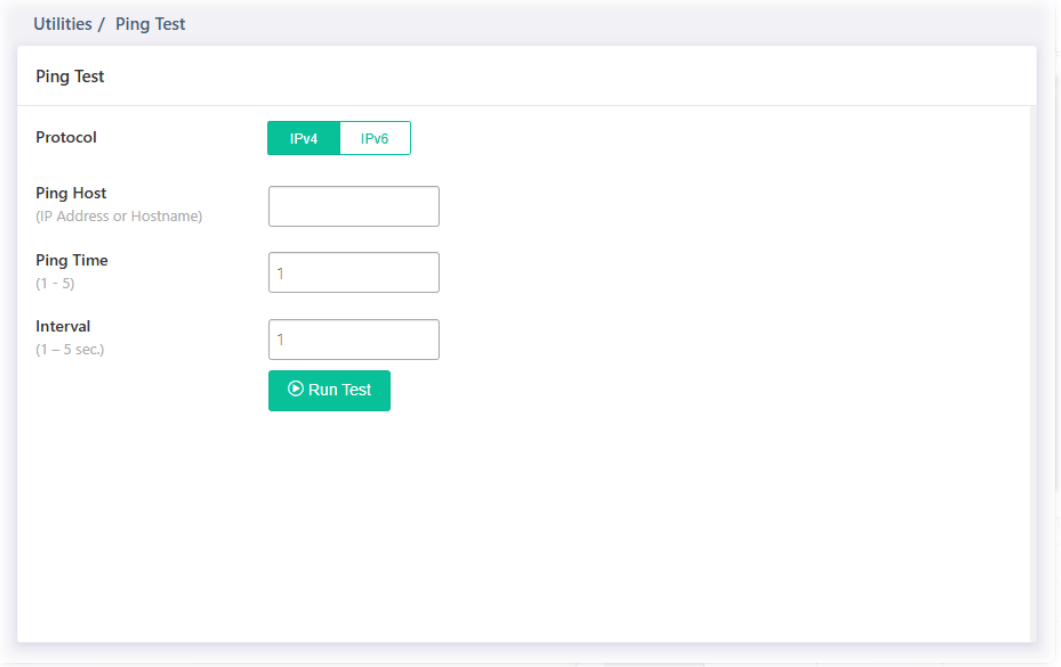
Available settings are explained as follows:

Item	Description
Cooper Test	
Run Test	Perform the copper test action. Before clicking Run Test, select the port or ports (2.5GE1 to 2.5GE24, 10GE1 to 10GE6) on the panel figure for performing cable diagnostics.
Result	
Show details	Click to display more detailed information about the scanning result.
Port	Displays the port number that has been performed with cable diagnostics.
Link Speed	Displays the link speed of the port(s).
Status	Displays the connection status of the port(s).

After finishing this web page configuration, please click **OK** to save the settings.

IV-3 Ping Test

This page is used for configuring the ping test and perform the ping test.

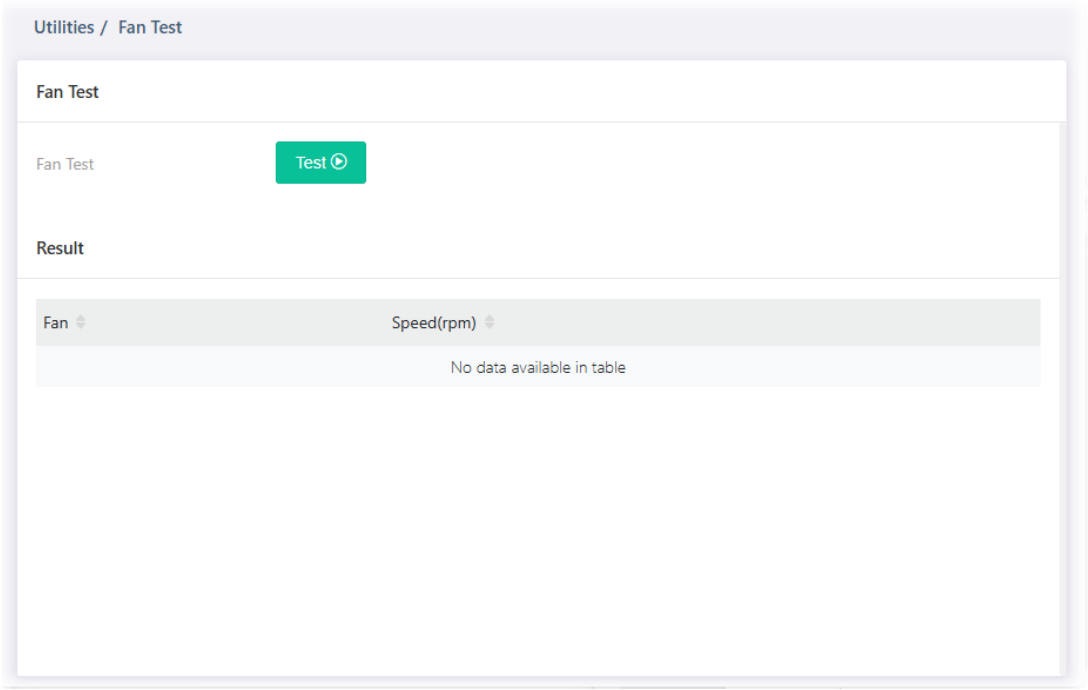


Available settings are explained as follows:

Item	Description
Ping Test	
Protocol	Choose IPv4/IPv6 to specify IP address for sending ping to check if network path is ok.
Ping Host	Enter the IP address of SNMP server based on the protocol selected above.
Ping Time	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	Defines the interval to perform ping action. For example, "1" means the ping action will be performed per second.
Run Test	Perform ping action.

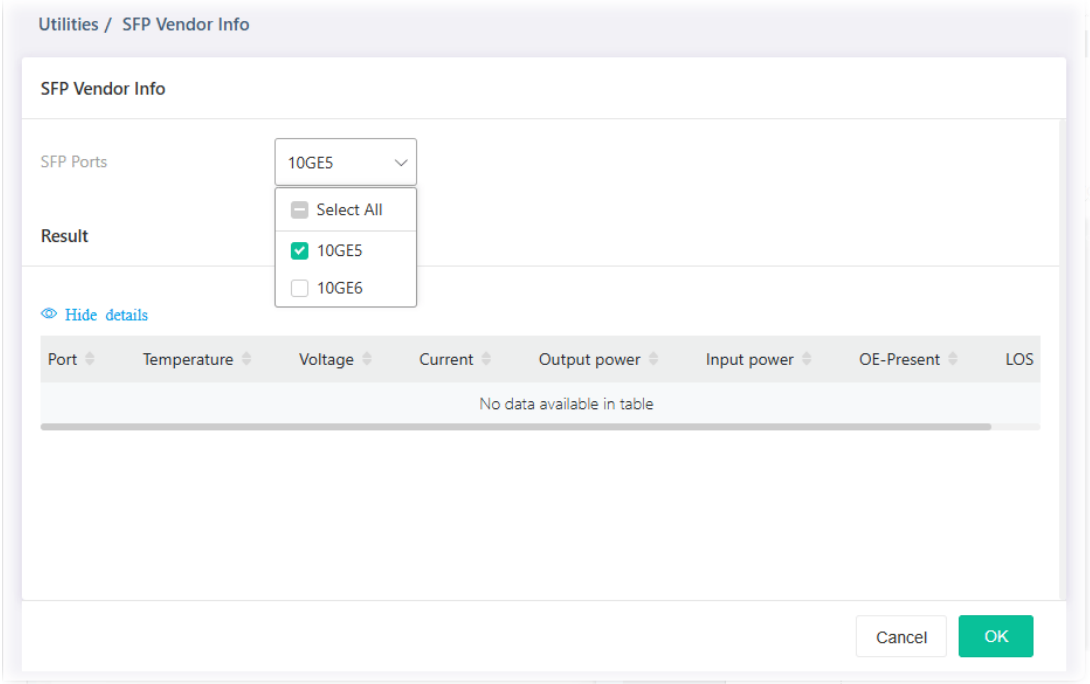
IV-4 Fan Test

The built-in fan in the VigorSwitch can be tested if it runs normally or not. Simply click **Test** to perform the fan test.



IV-5 SFP Vendor Info

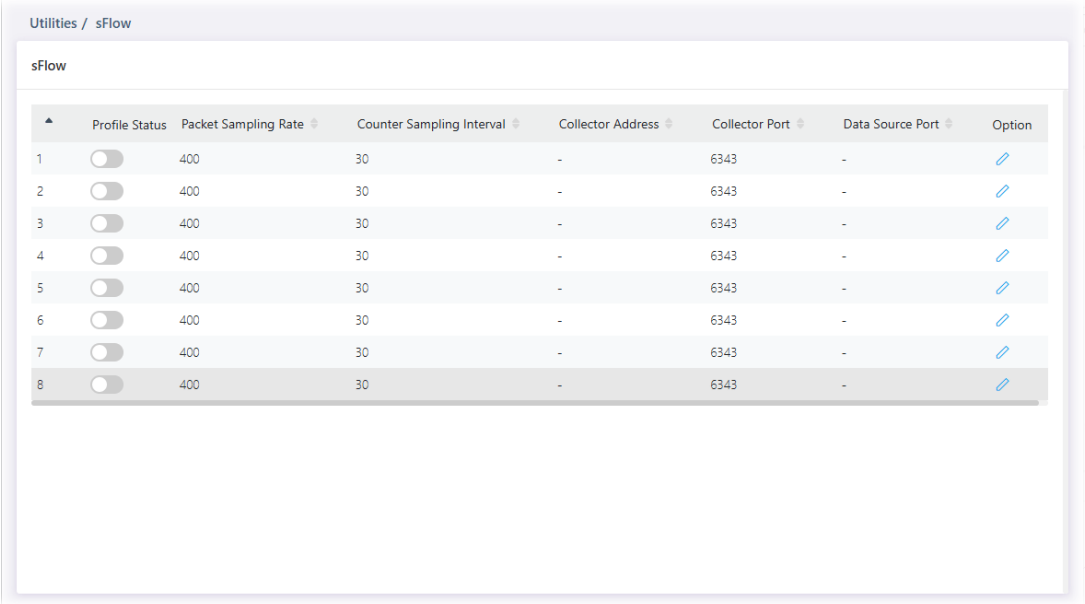
To get general information about the SFP vendor, select **Utilities>>SFP Vendor Info**.



IV-6 sFlow

sFlow (Sampled Flow) is a method which uses sampling to get the network packets information for the system administrator understanding the network operation and the network congestion.

VigorSwitch plays the role of sFlow agent which collects and sends the collected data to a sFlow controller (e.g., an external monitoring software) for executing data analysis. The system administrator shall install the sFlow controller on the device which can communicate with VigorSwitch. When the administrator wants to monitor the data traffic via VigorSwitch and get the statistics, he/she can configure VigorSwitch as sFlow agent by configuring the settings listed below. Later, the sFlow controller can analyze the data and offer statistics for the system administrator.

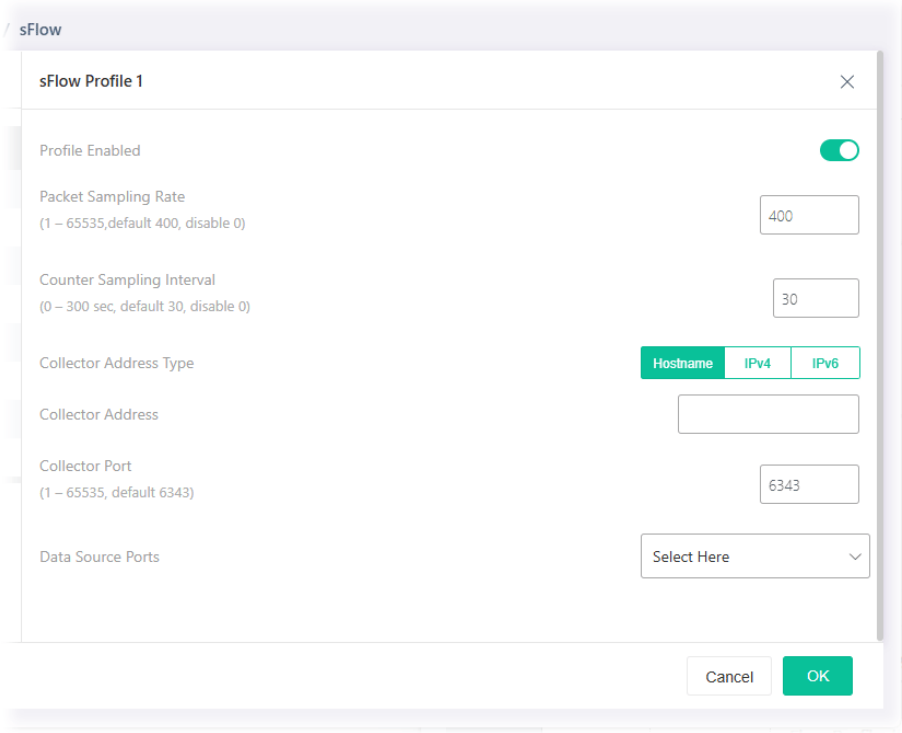


Available settings are explained as follows:

Item	Description
Profile Status	**Enable / Disable** – Switch the toggle to enable / disable this function. - means "Enable". - means "Disable".
Packet Sampling Rate	Displays the sampling rate of the packets for the server to capture.
Counter Sampling Interval	Displays the time (sec.) for the sFlow server to obtain the traffic on the interface (LAN port) periodically.
Collector Address	Displays the hostname, IPv4 address, or IPv6 address of the data collector device.
Collector Port	Displays the port number used for real-time monitoring traffic status.
Data Source Port	Displays the LAN interface (10GE1 to 10GE6) of the data source port.

Option	- Click to modify the loop protection settings of the selected port.

To modify settings for a port, click the link to open the setting page.



Available settings are explained as follows:

Item	Description
sFlow Profile #	
Profile Enabled	**Enable / Disable** – Switch the toggle to enable / disable the settings for the selected profile. - means "Enable". - means "Disable".
Packet Sampling Rate	Set the sampling rate of the packets for the server to capture.
Counter Sampling Interval	Set a time for the sFlow server to obtain the traffic on the interface (LAN port) periodically. Then, the sever will make statistics and transmit the data to the collector device. The default value is 30 (seconds).
Collector Address Type	Usually, you can specify a server or an IP address as a data collector device. Specify the role of the server (hostname, IPv4 or IPv6).
Collector Address	Enter the hostname, IPv4 address or IPv6 address according to the collector type selected.
Collector Port	The port number is the basic sampling unit which can be used for real-time monitoring traffic status. The default port number is 6343.

Data Source Ports	Specify the LAN interface (10GE1 to 10GE6) as the data source port.
OK	Save the settings.

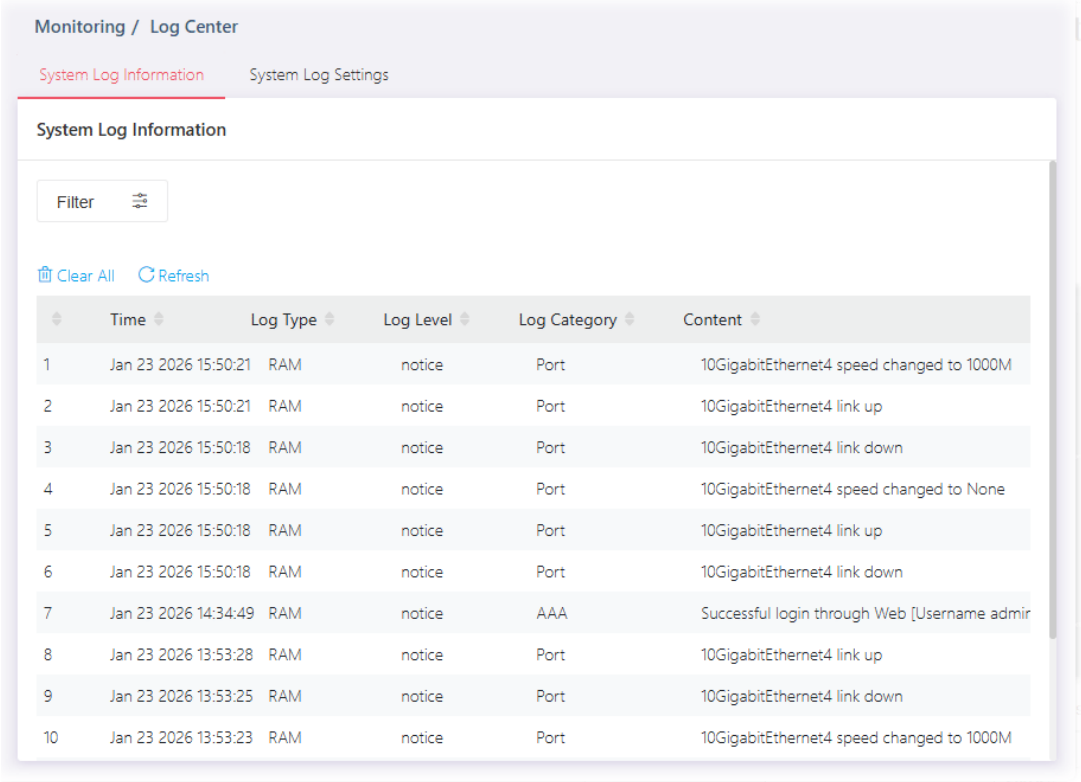
After finishing this web page configuration, please click **OK** to save the settings.

Chapter V Monitoring

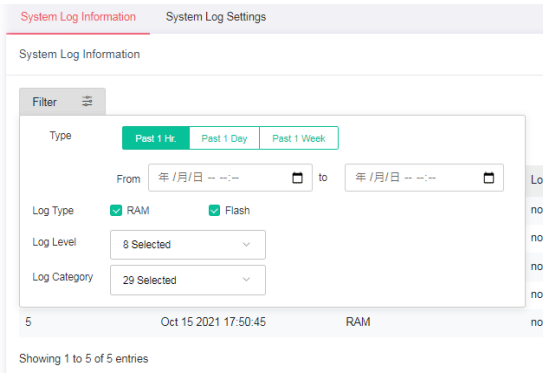
V-1 Log Center

V-1-1 System Log Information

This page allows the user to set filtering conditions and displays the filtering result.



Available settings are explained as follows:

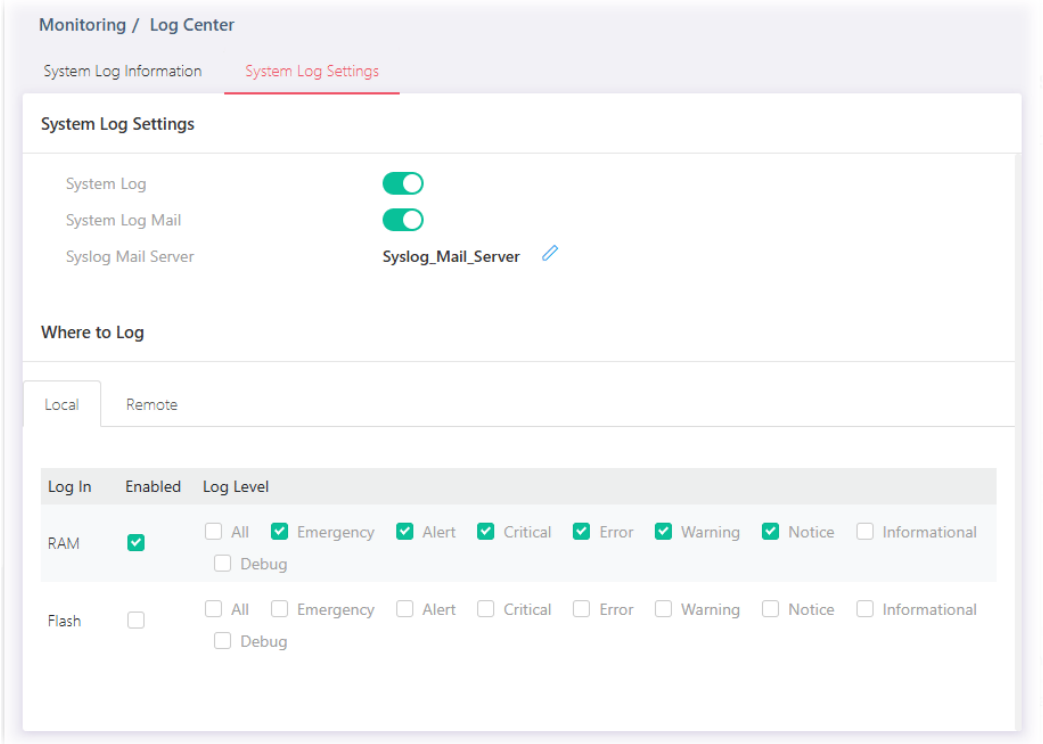
Item	Description
Filter	Click to set the conditions for filtering.  **Type** - Specify the time (Past 1 Hour, Past 1 Day, Past 1 Week) for filtering. **Log Type** - Select RAM (explore the logs contained in volatile memory (also known as RAM) or Flash (explore the logs contained

	in non-volatile memory). **Log Level** - Select severity (emerg, alert, crit, error, warning, notice, info and debug) of log messages which you wish to filter out for review. **Log Category** - Select the categories (related features) of logs you wish to review.
Clear All	Clear it to remove all logs displayed in this page.
Refresh	Click it to refresh the log.
Time	Displays the filtering time type.
Log Type	Displays the log type (RAM or Flash).
Log Level	Displays the severity of the log.
Log Category	Displays the category of the log.
Content	Displays the brief explanation of the log.

V-1-2 System Log Settings

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

V-1-2-1 Local

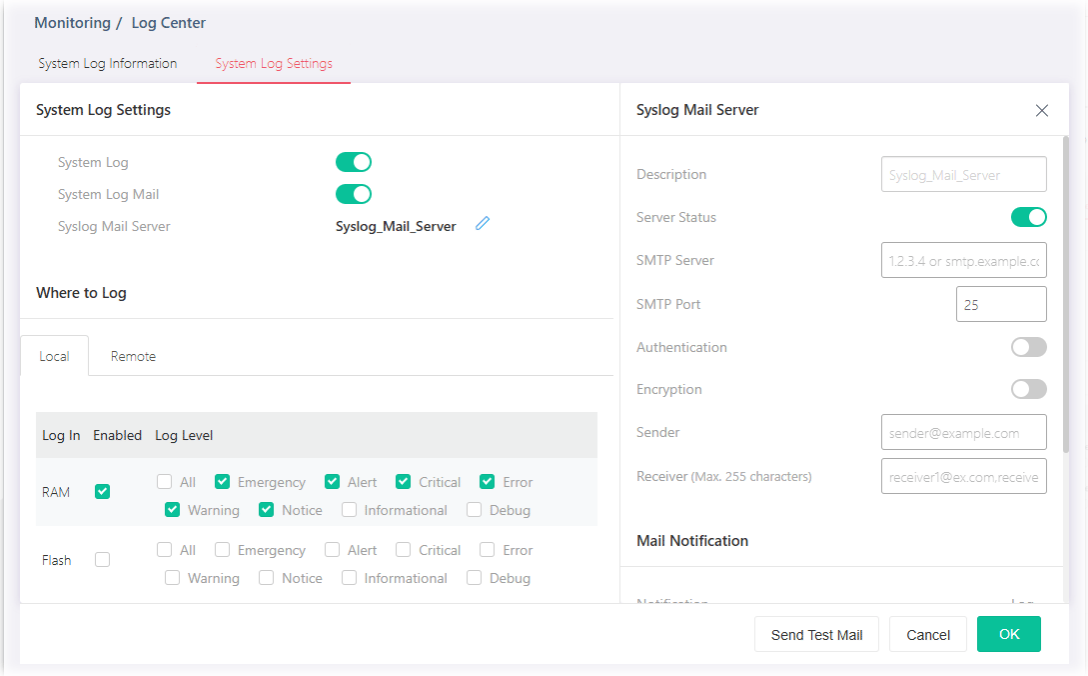


Available settings are explained as follows:

Item	Description
System Log Settings	

System Log	**Enable / Disable** – Switch the toggle to enable / disable this function. - means "Enable". - means "Disable".
System Log Mail	**Enable / Disable** – Switch the toggle to enable / disable this function. • **Syslog Mail Server** - Click to configure Syslog Mail Server.
Where to Log	
Local	**Log in** - Displays the log type. **Enabled** - Select the box to enable the log type (RAM/Flash). **Log Level** - Select the box(es) to select the severity of the log.

To modify settings for the **Syslog Mail Server,** click the link to open the setting page.



Available settings are explained as follows:

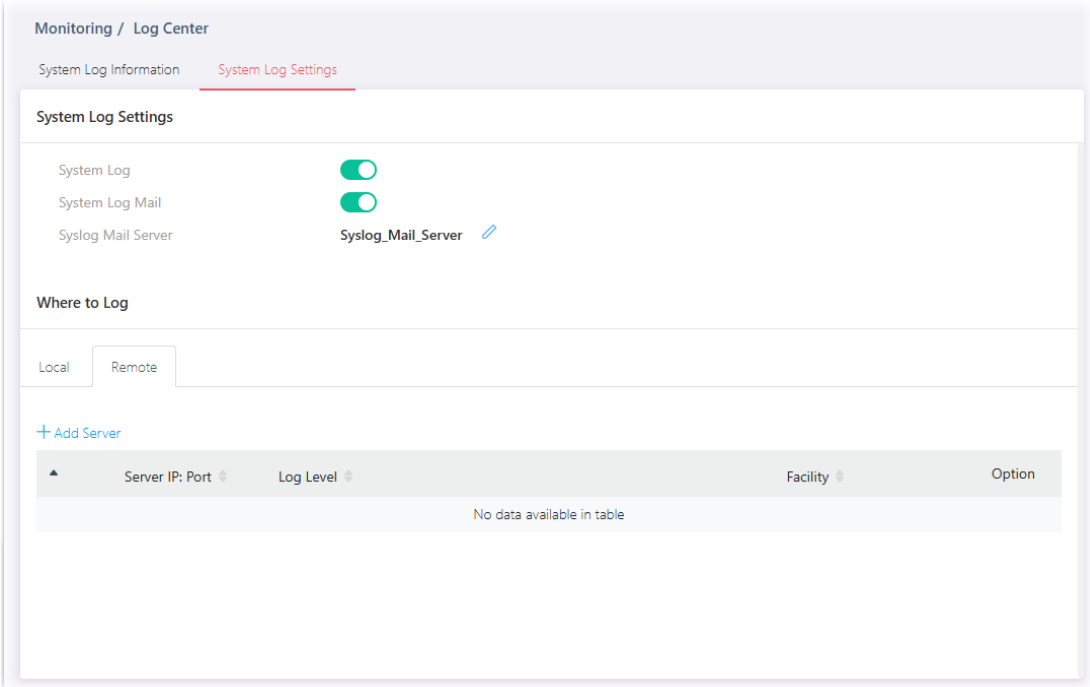
Item	Description
Syslog Mail Server	
Description	Displays the name of the Syslog Mail Server.
Server Status	**Enable / Disable** – Switch the toggle to enable / disable the Syslog Mail Server settings. - means "Enable". - means "Disable".
SMTP Server	Enter IP address or URL of the SMTP server.
SMTP Port	Enter the port number for the SMTP server.

Authentication	**Enable / Disable** – Switch the toggle to enable / disable the authentication mechanism. • **Username** - Enter a user name for authentication. • **Password** - Enter a password for authentication.
Encryption	**Enable / Disable** – Switch the toggle to enable / disable this function. 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 StartTLS.
Sender	Enter the email address which will send the syslog mail out.
Receiver	Enter the email address which will receive the syslog mail.
Mail Notification	
Log Type	Vigor system will send the e-mail related to the selected feature(e.g., AAA, ACL) to the recipient.
Send Test Mail	After clicking this button, VigorSwitch system will send a test mail to the recipient.

After finishing this web page configuration, please click **OK** to save the settings.

V-1-2-2 Remote

This page allows users to enable system logging into a specific remote Syslog server for storage.

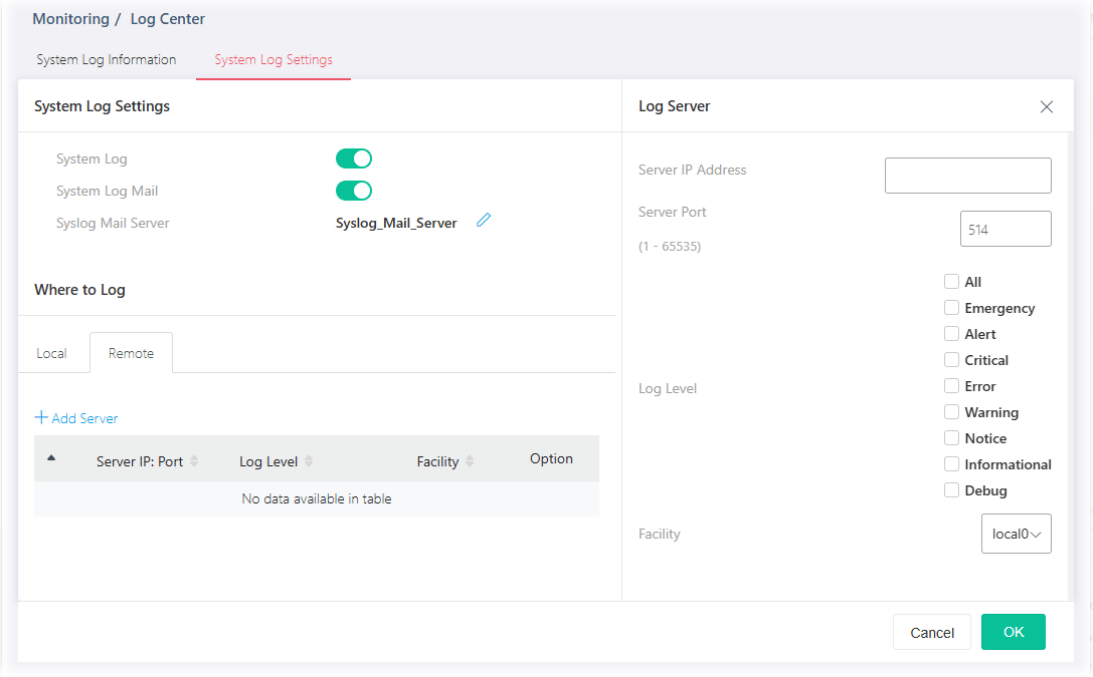


Available settings are explained as follows:

Item	Description
System Log Settings	
System Log	**Enable / Disable** – Switch the toggle to enable / disable this

	function.  - means “Enable”. - means “Disable”.
System Log Mail	**Enable / Disable** – Switch the toggle to enable / disable this function. • **Syslog Mail Server** - Click to configure Syslog Mail Server.
Where to Log	
+Add Server	Click to create a new remote server.
Log In	Displays the index number of the remote server.
Server IP: Port	Displays the IP address and port number used by the server.
Log Level	Displays the severity of the system log.
Facility	Displays the facility of the remote Syslog server.

To add a remote server, click the "**+Add Server**" to open the edit page.



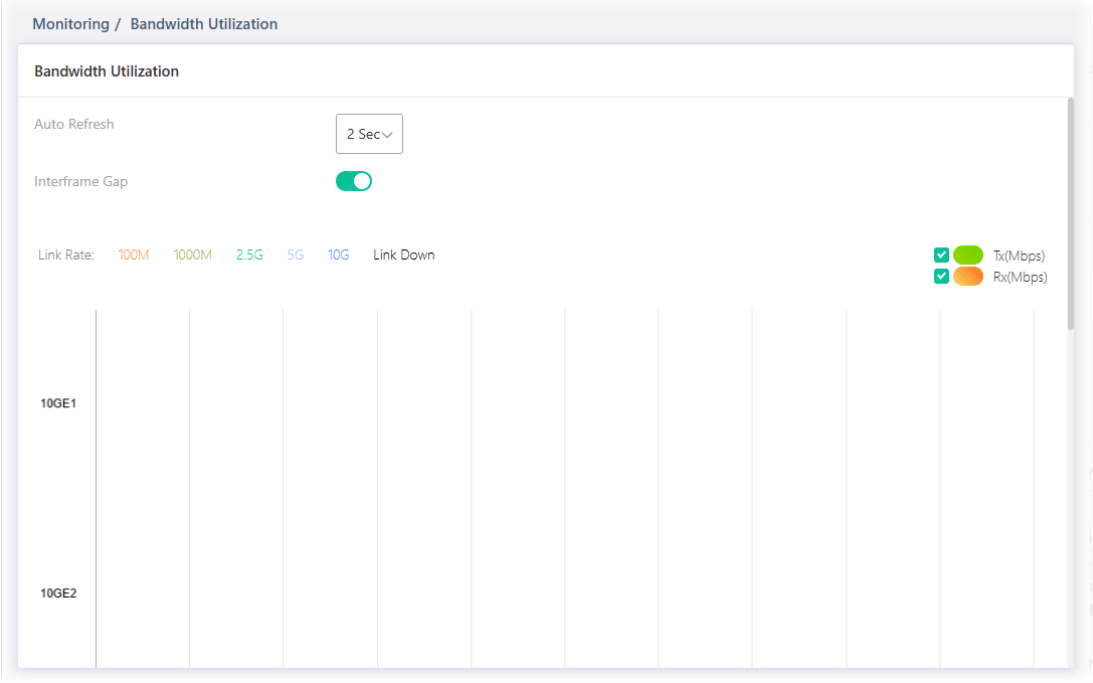
Available settings are explained as follows:

Item	Description
Log Server	
Server IP Address	Enter IP address of the Syslog server.
Server Port	Specify the port that syslog should be sent to.
Log Level	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 this Syslog server.

After finishing this web page configuration, please click **OK** to save the settings.

V-2 Bandwidth Utilization

This page offers the traffic statistics including data information and data of interframe gap for each port.

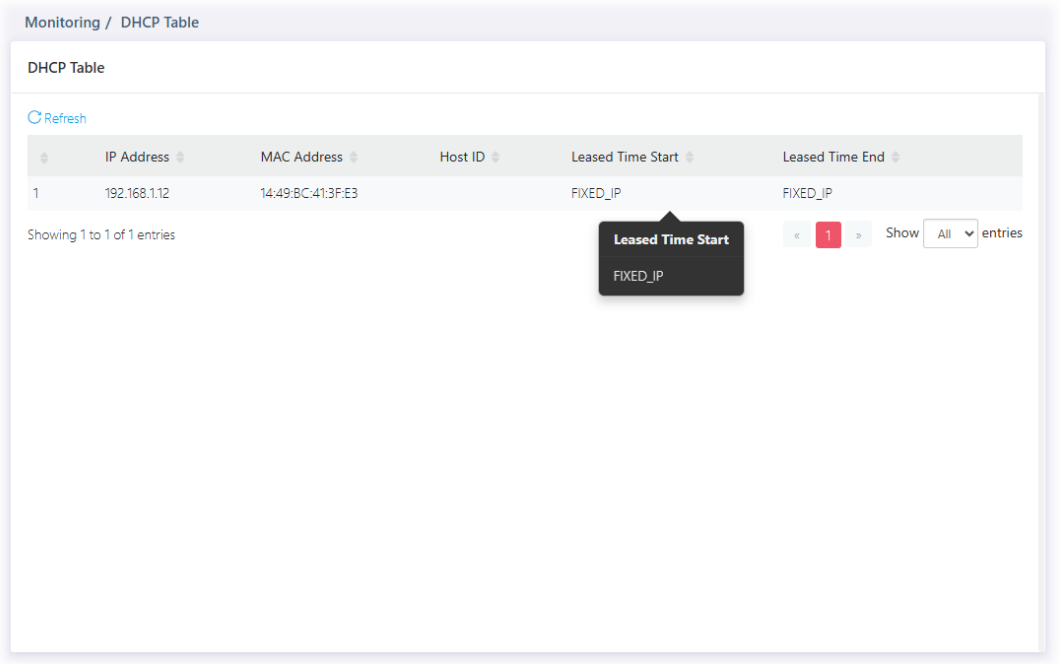


Available settings are explained as follows:

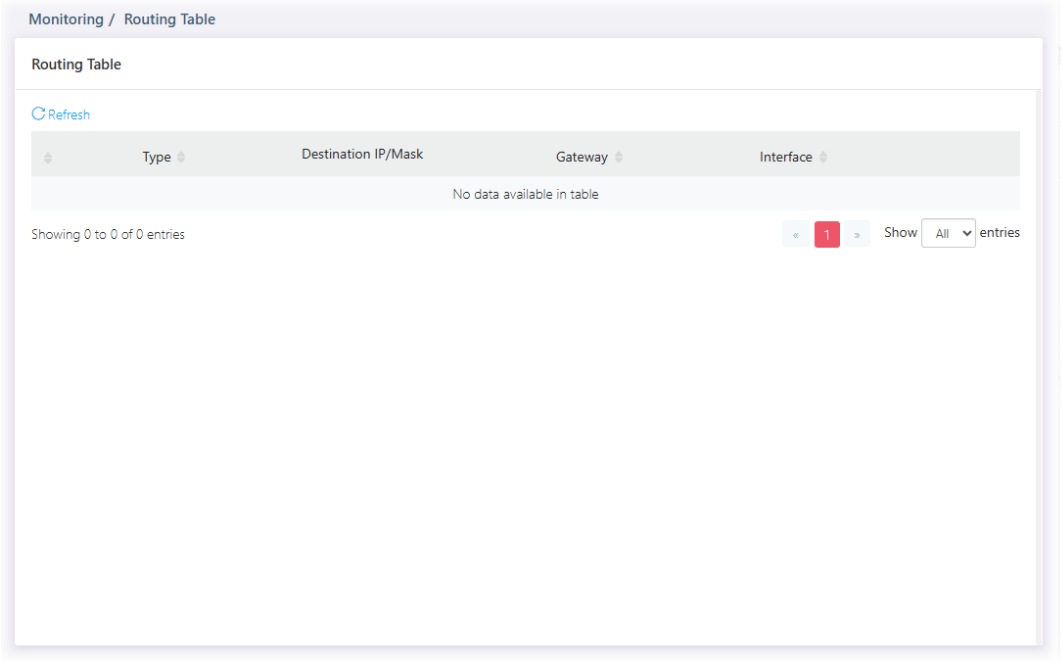
Item	Description
Auto Refresh	Select the time interval for refreshing this page.
Interframe Gap	The data of the interframe gap can be displayed or hidden by enabling/disabling for Interframe Gap. **Enable / Disable** – Switch the toggle to enable / disable this function. - means "Enable". - means "Disable".

V-3 DHCP Table

This page shows the IP list assigned by the DHCP server.

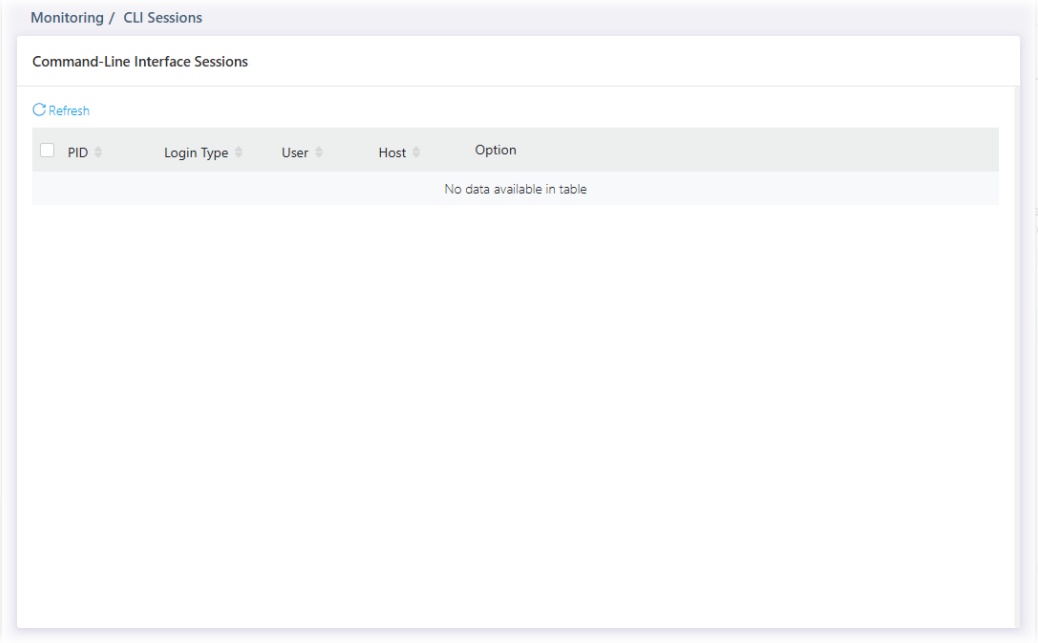


V-4 Routing Table



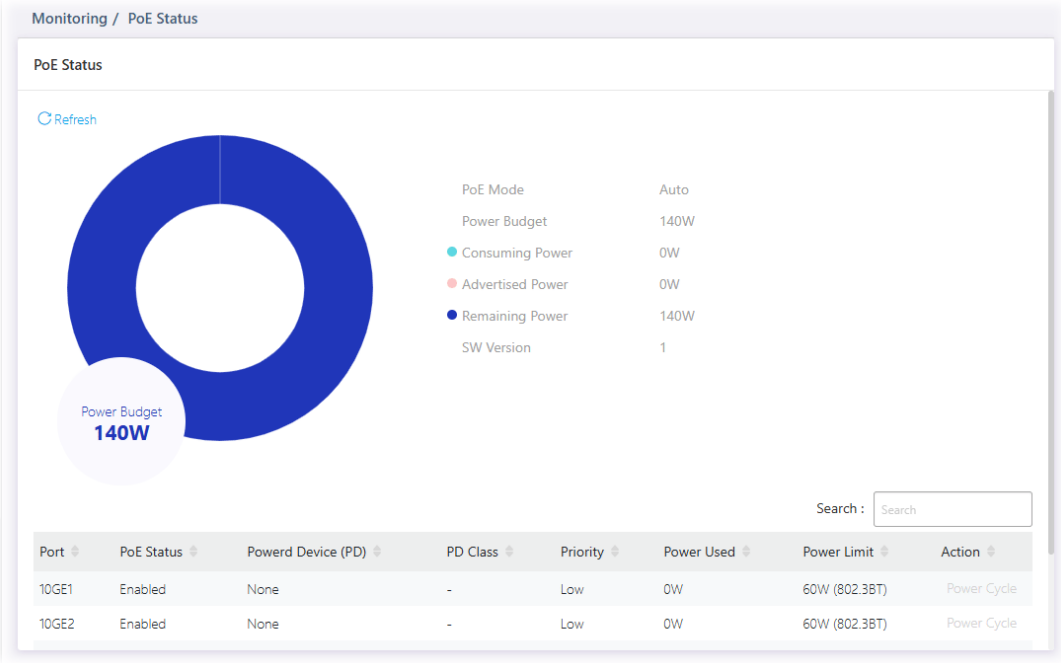
V-5 CLI Sessions

This page shows a list of CLI command executed. You can delete the selected CLI session by click the Remove button under the Edit item.



V-6 PoE Status

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



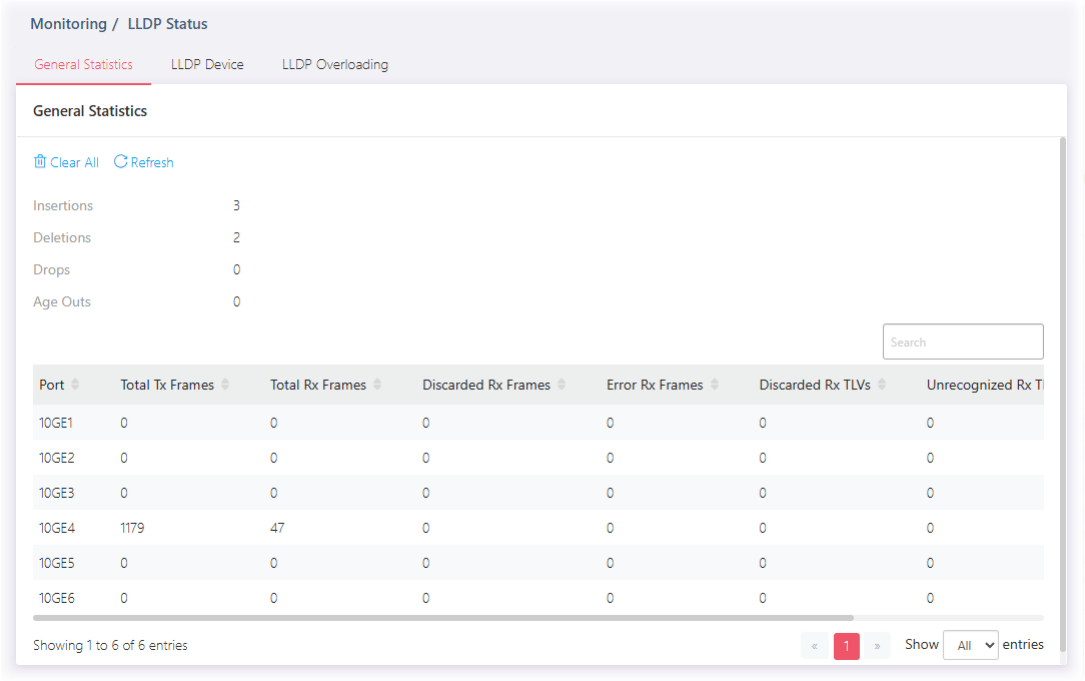
Available settings are explained as follows:

Item	Description
PoE Status	
Refresh	Click it to refresh the status page.
PoE Mode	Displays the PoE Mode (Manual/Auto) selected for the LAN port.
Power Budget(W)	Displays the maximum power this switch can supply over PoE.
Consuming Power(W)	Displays current power being consumed by all devices over PoE.
Remaining Power(W)	Displays remaining power that can be supplied to additional devices over PoE.
Port	Displays the PoE port number (10GE1 to 10GE4).
PoE Status	Displays the status (Enabled / Disabled) of the PoE port.
Powered Device (PD)	Displays the status (ON/None) of the PoE device.
PD Class	Displays the power limit (15.4W/30W) of the PoE device.
Priority	Displays the priority of the PoE port.
Power Used	Displays the consuming power of the PoE port.
Power Limit	Displays the total power for all PoE port.
Action	If the PoE device connects to VigorSwitch, it will be available for you to manually perform the cold boot for the PoE device by cycling the power supply.

V-7 LLDP Status

V-7-1 General Statistics

This page offers the statistics of LLDP packets of each port (10GE1 to 10GE6).



Available settings are explained as follows:

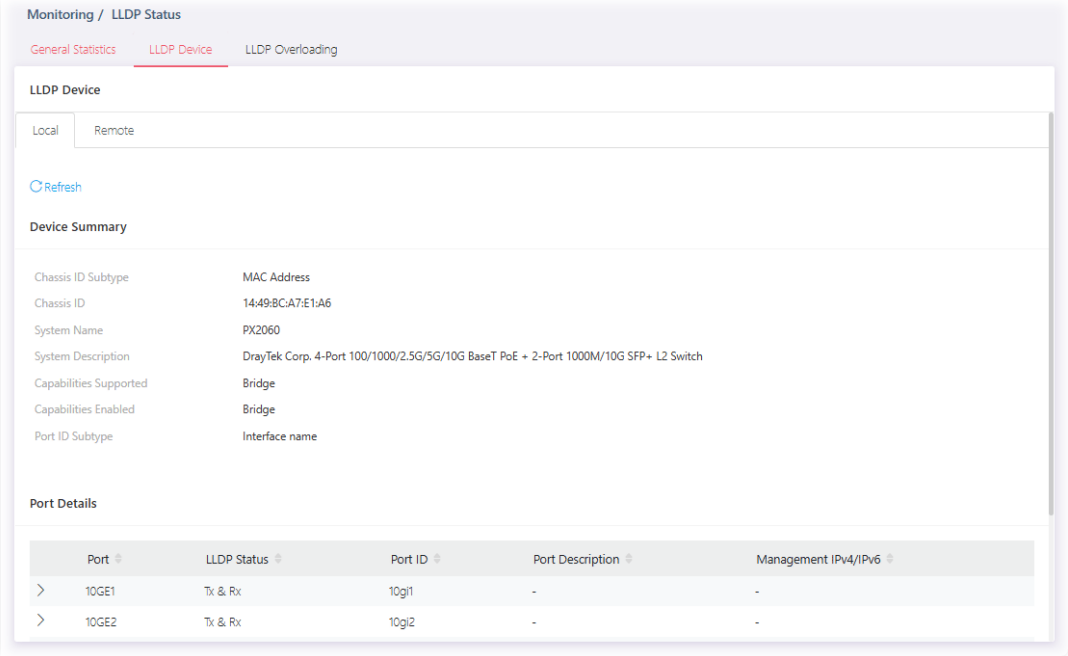
Item	Description
General Statistics	
Clear All	Clear it to remove all logs displayed in this page.
Refresh	Click it to refresh the status page.

V-7-2 LLDP Device

This page displays information for LLDP local and remote devices.

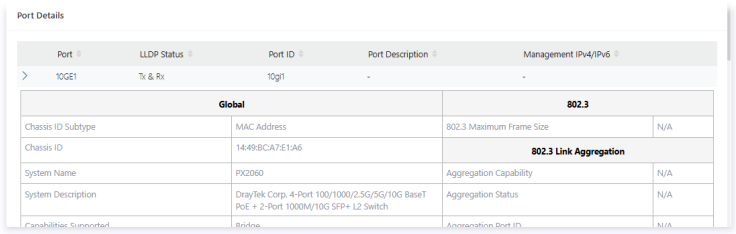
V-7-2-1 Local

This page displays information for LLDP local device.



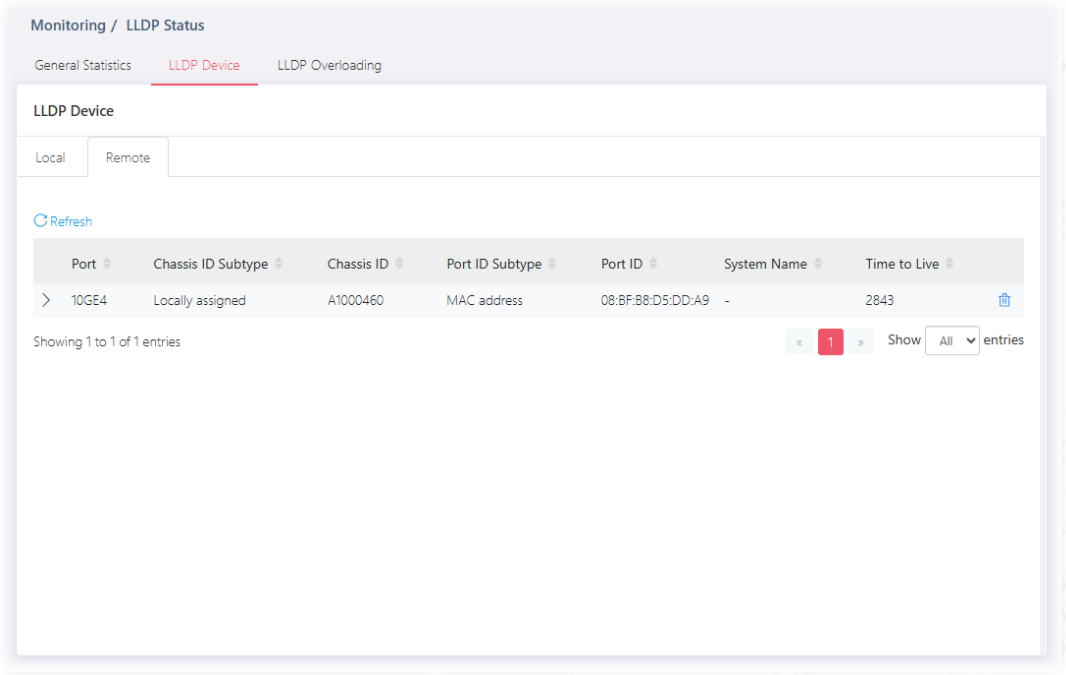
Available settings are explained as follows:

Item	Description
Refresh	Click it to refresh the status page.
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. Click > 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 (10GE1 to 10GE6).



V-7-2-2 Remote

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

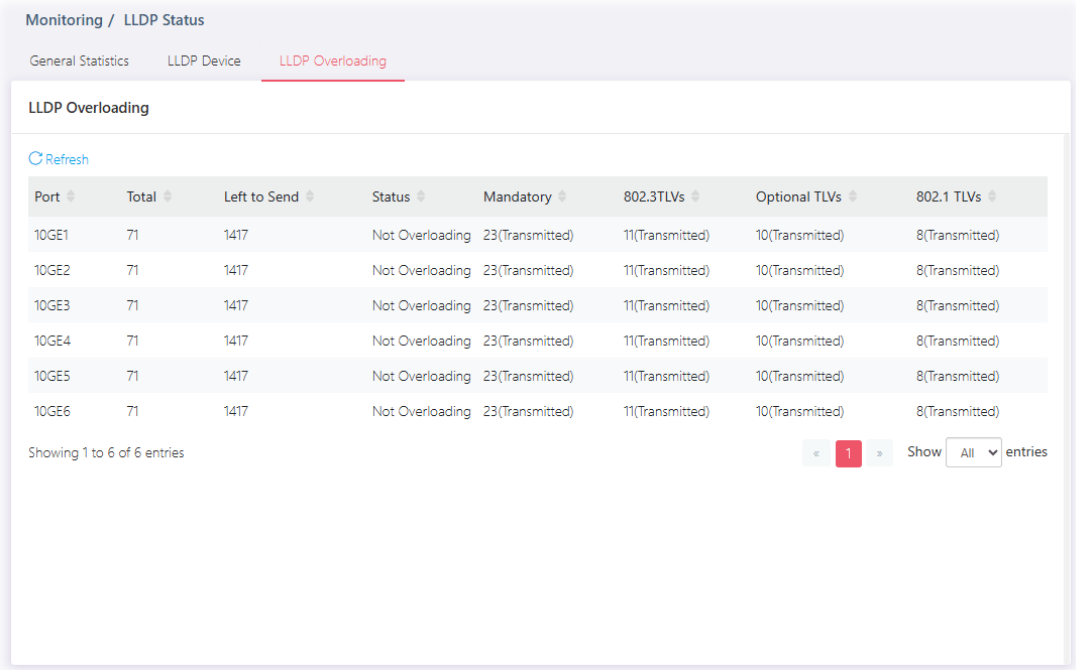


Available settings are explained as follows:

Item	Description
Refresh	Click it to refresh the status page.
Port	Displays the number of the local port to which the neighbor is connected.
Chassis ID Subtype	Displays the type of chassis ID (for example, MAC address).
Chassis ID	Displays the identifier of the 802 LAN neighboring device's chassis.
Port ID Subtype	Displays the type of port identifier.
Port ID	Displays the number of port identifier.
System Name	Displays the name of the switch.
Time to Live	Displays the time interval in seconds after which the information for remote device will be deleted.

V-7-3 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.

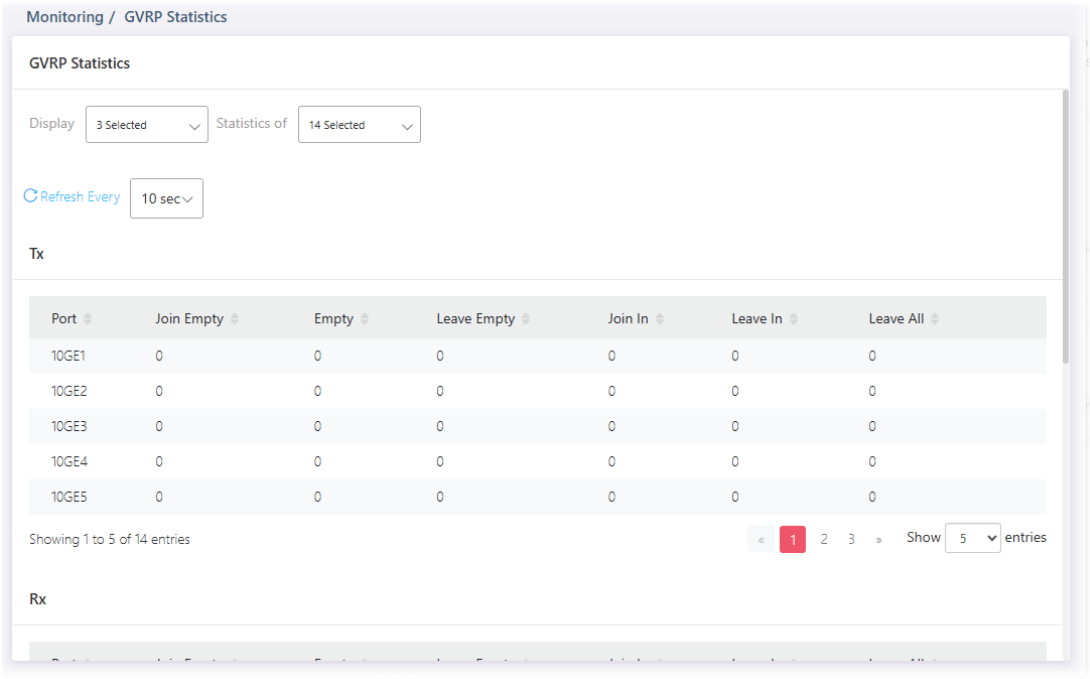


Available settings are explained as follows:

Item	Description
Refresh	Click it to refresh the status page.
Port	Displays the name of the port.
Total	Displays the total number of bytes of LLDP information in each packet.
Left to Send	Displays the total number of available bytes left for additional LLDP information in each packet.
Status	Displays if LLDP TLVs has overloaded the PDU maximum size or not.
Mandatory	Displays how many bytes used by mandatory TLVs.
802.3TLVs	Displays 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.

V-8 GVRP Statistics

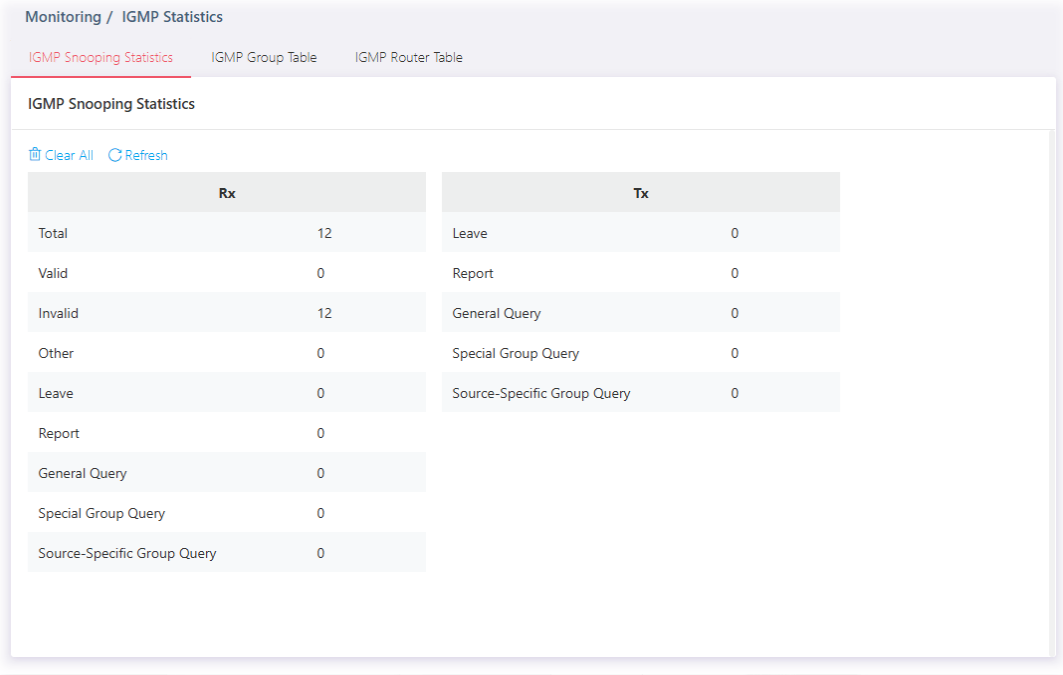
GVRP (Generic Attribute Registration Protocol) is used automatically for exchanging information for VLAN membership between switches. This page counts the GVRP information received on each port.



V-9 IGMP Statistics

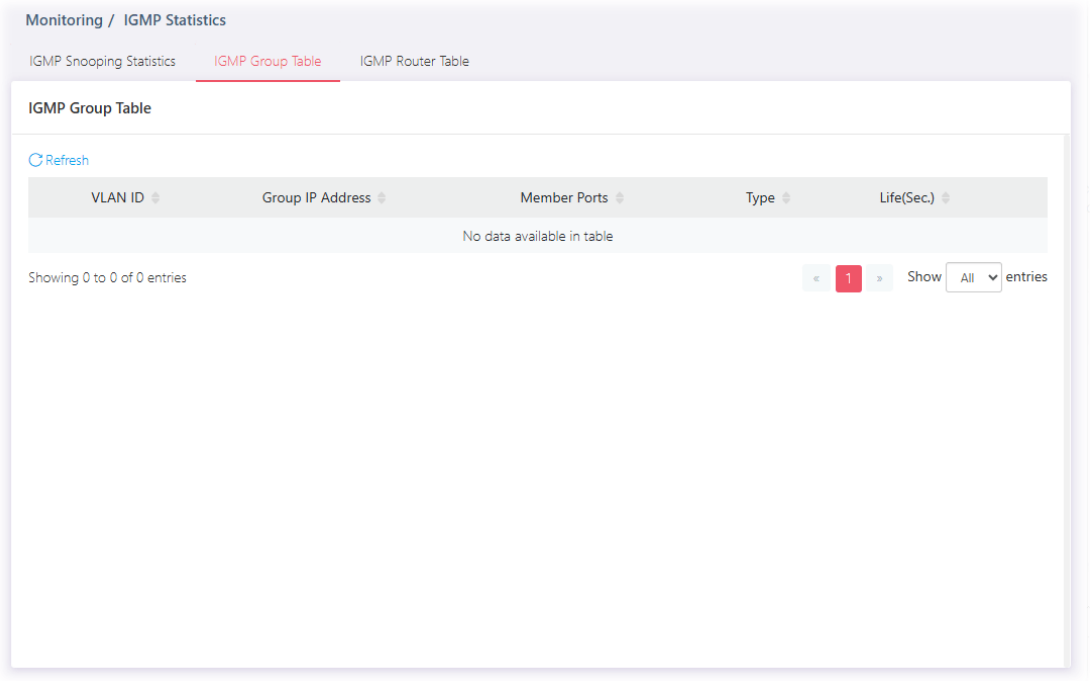
V-9-1 IGMP Snooping Statistics

This page counts the IGMP snooping traffic received or transmitted on the network.



V-9-2 IGMP Group Table

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

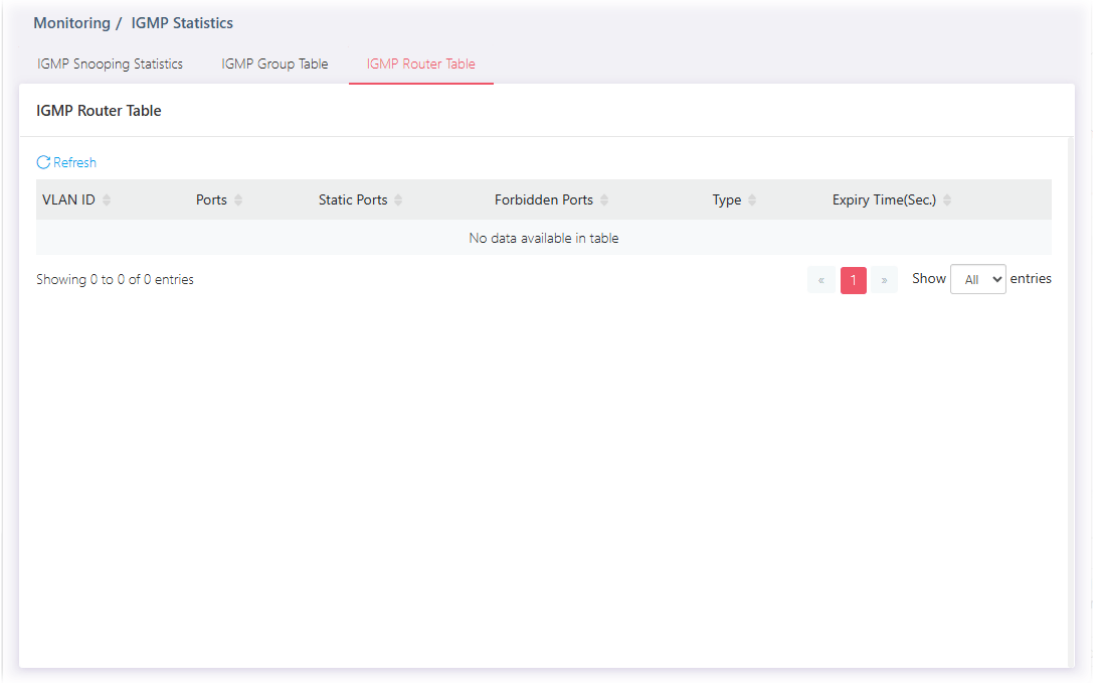


Available settings are explained as follows:

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.

V-9-3 IGMP Router Table

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

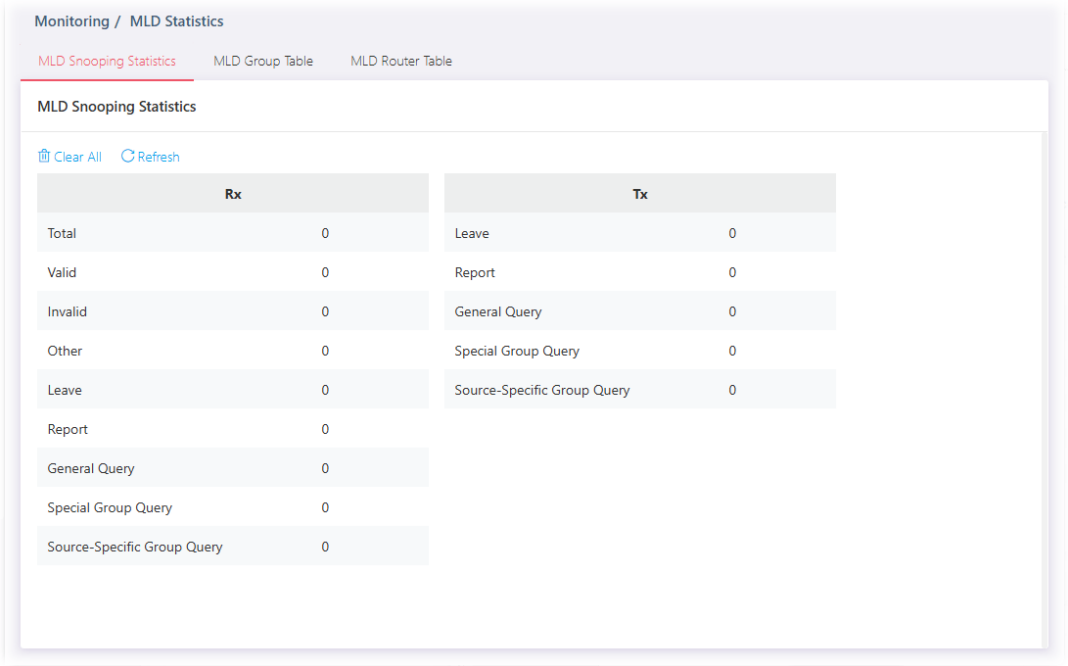


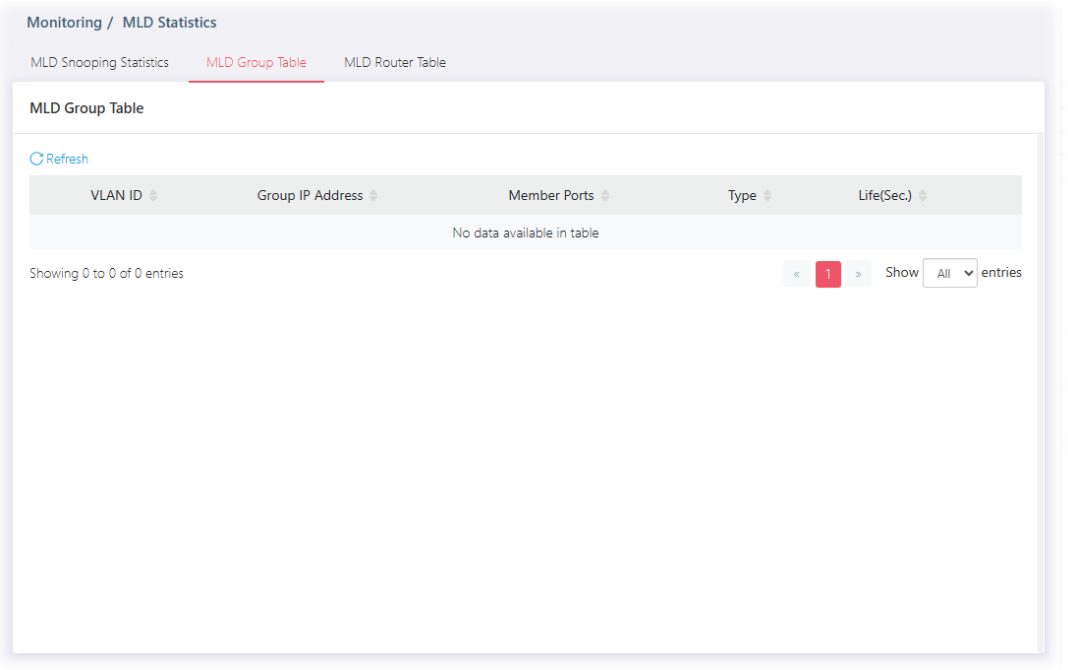
Available settings are explained as follows:

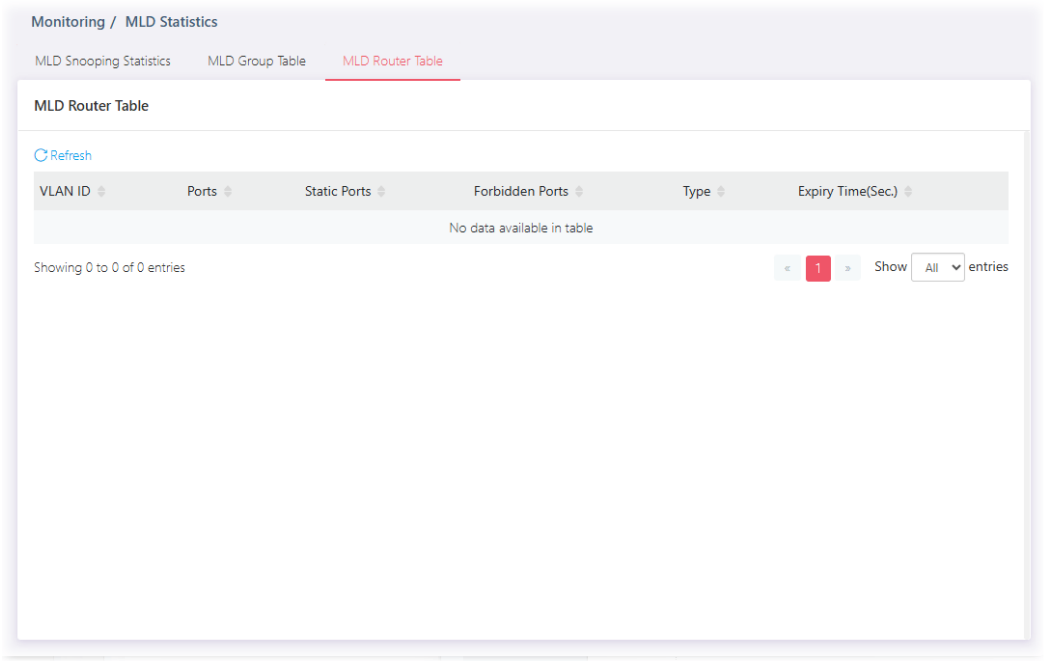
Item	Description
VLAN ID	Use the drop down list to specify a VLAN profile (created in **Switch LAN>>VLAN Management>>Create Vlan**) that the MLD querier belongs to.
Port	Display the static port member specified in Member Ports.
Static Ports	Display the LAN Port (GE/LAG) sending out query to remote host.
Forbidden Ports	Display the forbidden LAN Port (GE/LAG).
Expire Time (sec.)	Display the time before querier is considered no longer existed.

V-10 MLD Statistics

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



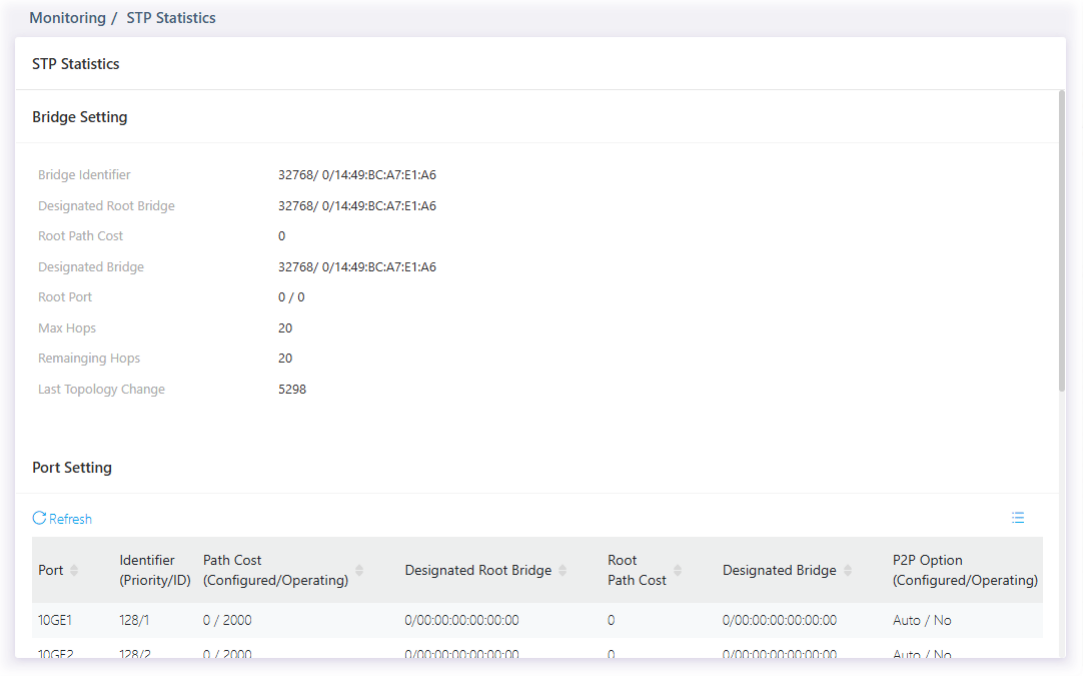



Monitoring / MLD Statistics
MLD Snooping Statistics
MLD Group Table
MLD Router Table
MLD Router Table
Refresh
VLAN ID
Ports
Static Ports
Forbidden Ports
Type
Expiry Time(Sec.)
No data available in table
Showing 0 to 0 of 0 entries
1
Show
All
entries

V-11 STP Statistics

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges, or routers.

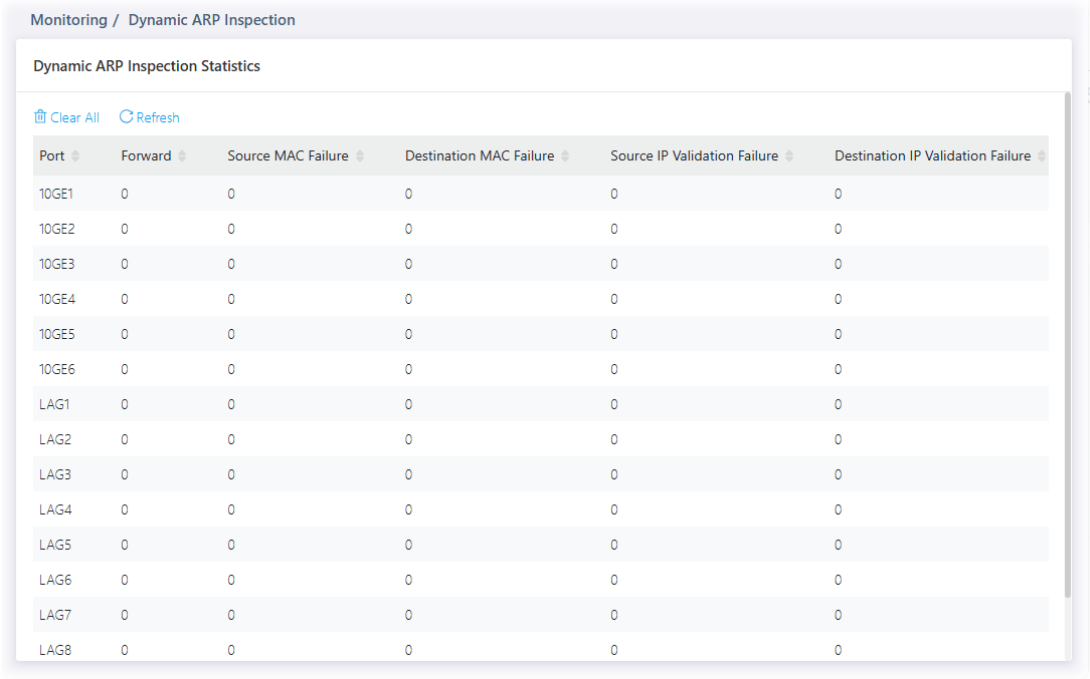
This page allows users to edit the general setting of the STP CIST port and browser CIST port status.



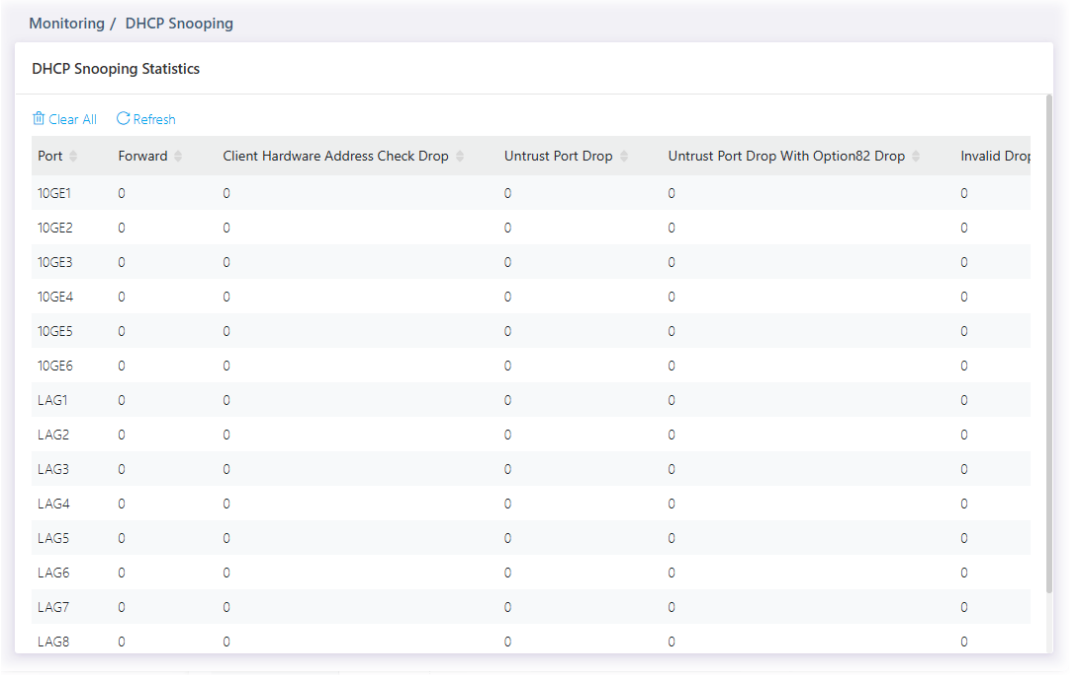
Available settings are explained as follows:

Item	Description
Refresh	Click it to refresh the status page.
Port	Displays the interface number for GE and LAG.
Identifier	Displays the spanning tree port identifier.
Path Cost	Displays current path cost of given port.
Designated Root Bridge	Displays the identifier of designated root bridge.
Root Path Cost	Displays the operational root path cost.
Designated Bridge	Displays the identifier of next bridge on this port.
Configure BPDUs Rx	Displays the counts of the received CONFIG BPDU.
TCN BPDUs Rx.	Displays the counts of the received TCN BPDU.
Configure BPDUs Tx.	Displays the counts of the transmitted CONFIG BPDU.
TCN BPDUs Tx	Displays the counts of the transmitted TCN BPDU.

V-12 Dynamic ARP Statistics

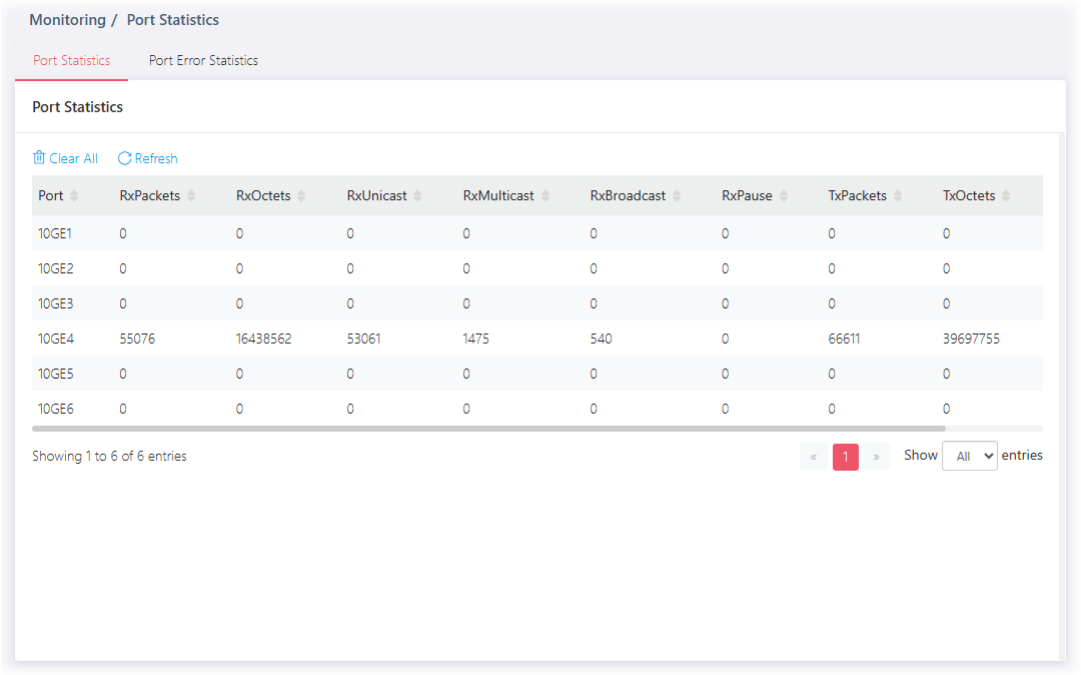


V-13 DHCP Snooping



V-14 Port Statistics

This page displays statistics for GE/LAG ports.



Available settings are explained as follows:

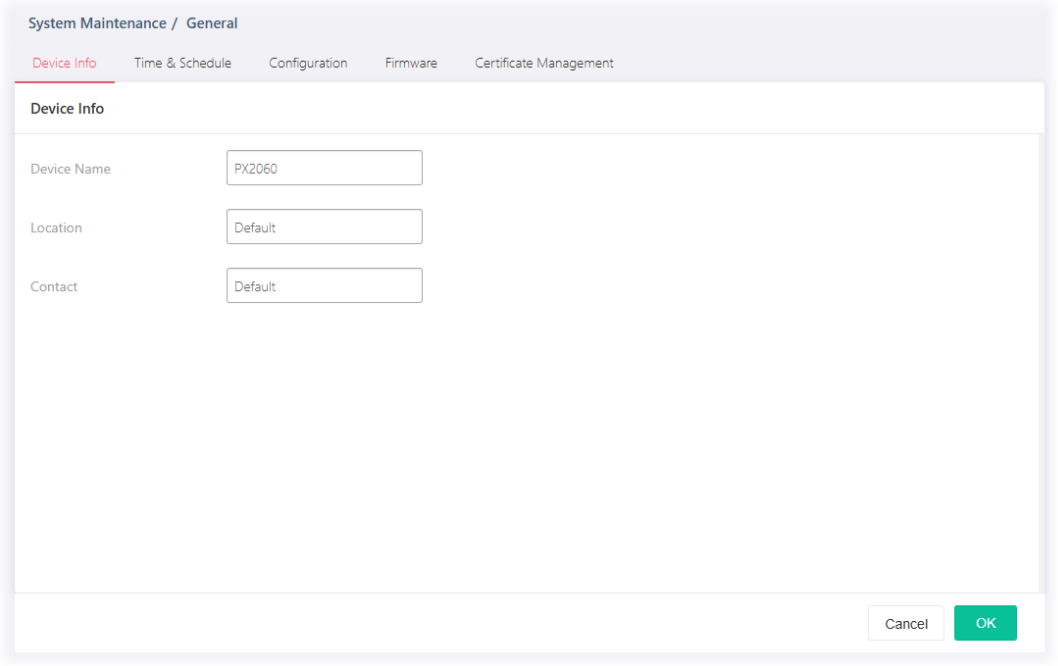
Item	Description
Clear All	Clear it to remove all logs displayed in this page.
Refresh	Click it to refresh the status page.
Port	Displays the port number.

Chapter VI System Maintenance

VI-1 General

VI-1-1 Device Info

This page displays general information (name, location and contact) for the VigorSwitch.



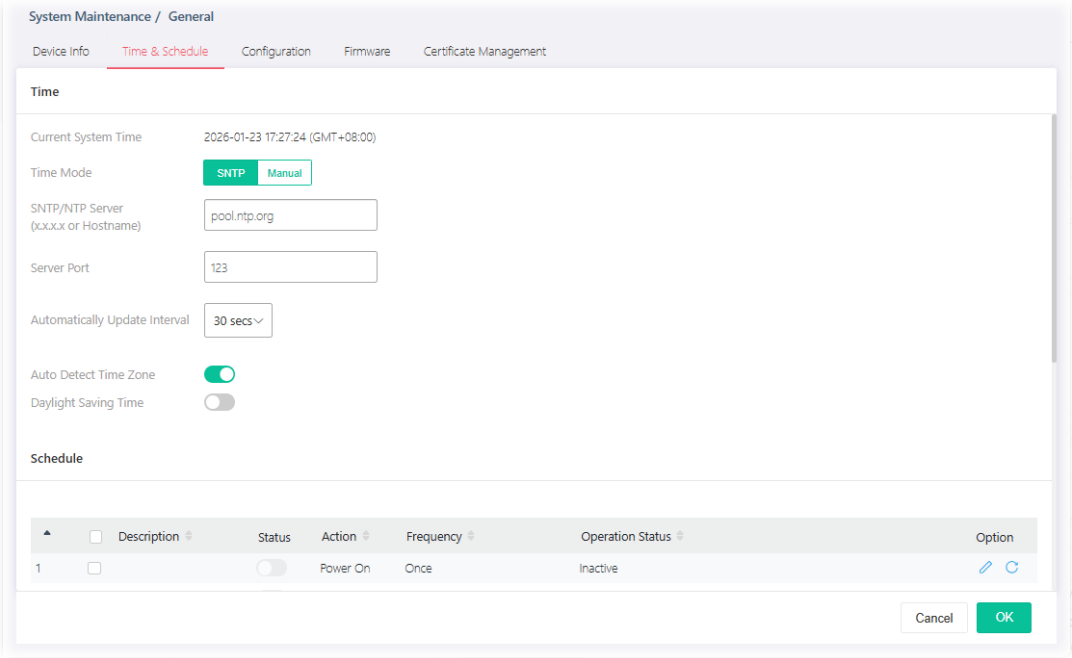
Available settings are explained as follows:

Item	Description
Device Name	Displays the name of this VigorSwitch. Change the name if required.
Location	Define the location of this VigorSwitch.
Contact	Define the contact information of this VigorSwitch.

After finishing this web page configuration, please click **OK** to save the settings.

VI-1-2 Time & Schedule

This page allows users to configure maximum 15 schedule rules.



Available settings are explained as follows:

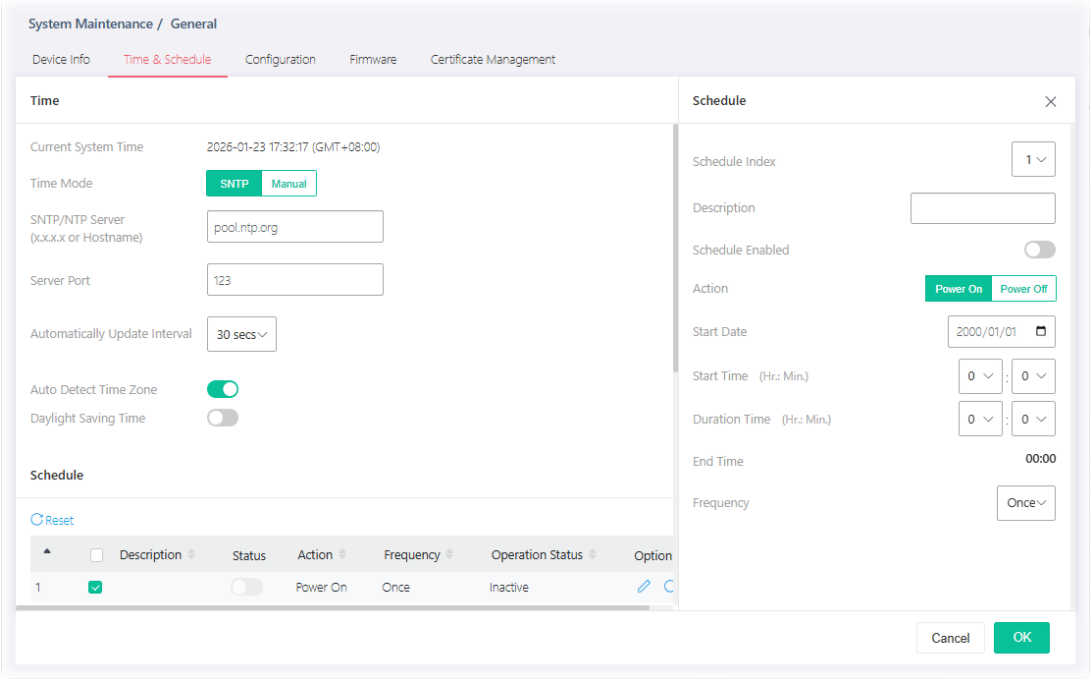
Item	Description
Time	
Current System Time	Display current system time based on the time server.
Time Mode	Select **SNTP** or **Manual**. If SNTP is selected, configure: • **SNTP/NTP Server** - Enter the web site of the time server or the IP address of the server. • **Server Port** - Enter the port number use by the time server. • **Automatically Update Interval** - Set the interval (30 secs, 1 min, 3 mins, 5 mins, 10 mins and etc.) for the system to update the time automatically. If Manual is selected, configure: • **Manual Time** - Specify static time (year, month, day, hours, minutes and seconds) manually. **Auto Detect Time Zone** - Switch the toggle to enable / disable this function.  - means "Enable". - means "Disable". **Daylight Saving Time** - Switch the toggle to enable / disable this function. If enabled, select the mode of 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.
when **Recurring** is selected	**Daylight Saving Time Offset -** Specify the adjust offset of daylight saving time. **Recurring From** - Specify the starting time of recurring daylight saving time. **Recurring To** - Specify the ending time of recurring daylight saving time.
when **Non-Recurring** is selected	**Daylight Saving Time Offset -** Specify the adjust offset of daylight saving time. **Non-recurring From** - Specify the starting time of non-recurring daylight saving time. **Non-recurring To** - Specify the ending time of recurring daylight saving time.
Schedule	
Description	Displays a short comment for the schedule profile.
Status	Displays the status (enable / disable) the schedule profile.
Action	Displays the action adopted by the schedule profile.
Frequency	Displays how often the schedule will be applied.
Operation Status	Displays the status (active / inactive) of the schedule profile.
Option	- Click to modify the setting page of the selected schedule profile. - Clear current settings and return to factory default settings.

After finishing this web page configuration, please click **OK** to save the settings.

Up to 15 schedule profiles are allowed to be set to meet various situations.

Click the " " to open the edit page.



Available settings are explained as follows:

Item	Description
Schedule	
Schedule Index	Use the drop down list to choose one schedule profile.
Description	Enter a brief comment for such schedule.
Schedule Enabled	Switch the toggle to enable / disable this function.  - means "Enable". The selected schedule profile will take action as configured. - means "Disable". The selected schedule profile will not take action but be saved for future use.
Action	Specify which action should perform during the period of the schedule. **Power On** – PoE connection is always on. **Power Off** - PoE connection is always down.
Start Date	Specify the starting date of the schedule by choosing from a drop down calendar.
Start Time	Specify the starting time of the schedule by using the drop down list to specify the starting hours and minutes.
Duration Time	Specify the ending time of the schedule by using the drop down list to specify the ending hours and minutes.
End Time	Displays the time period setting.
Frequency	Specify how often the schedule will be applied. **Once** - The schedule will be applied just once. **Weekdays Routine** - Specify which days in one week should perform the schedule.

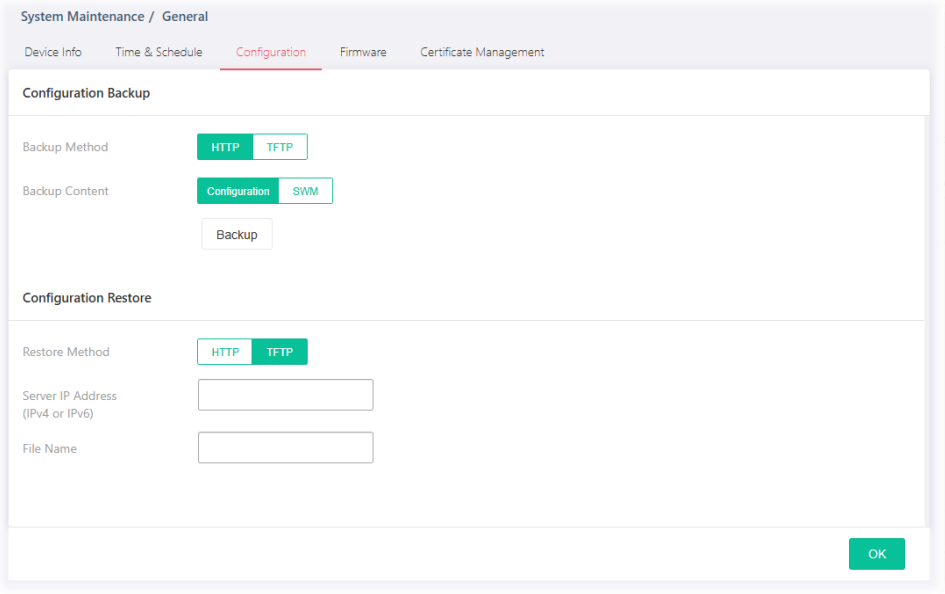
	• **Every** - Check to select the days in a week. **Monthly Routine** - Specify the day in a month as the starting point. • **Duration Time** - Use the drop down list to select the date in a month. **Few Days Routine** - The period of cycle duration is between 1 day and 31 days. For example, 7 means the whole cycle is 7 days; 20 means the whole cycle is 20 days. When the time is up, the PoE device will be turned on of off automatically. • **Every** - Use the drop down list to select the date in a month.

After finishing this web page configuration, please click **OK** to save the settings. A new schedule profile will be shown on the page.

VI-1-3 Configuration

Configuration Backup 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.

Configuration Restore 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.



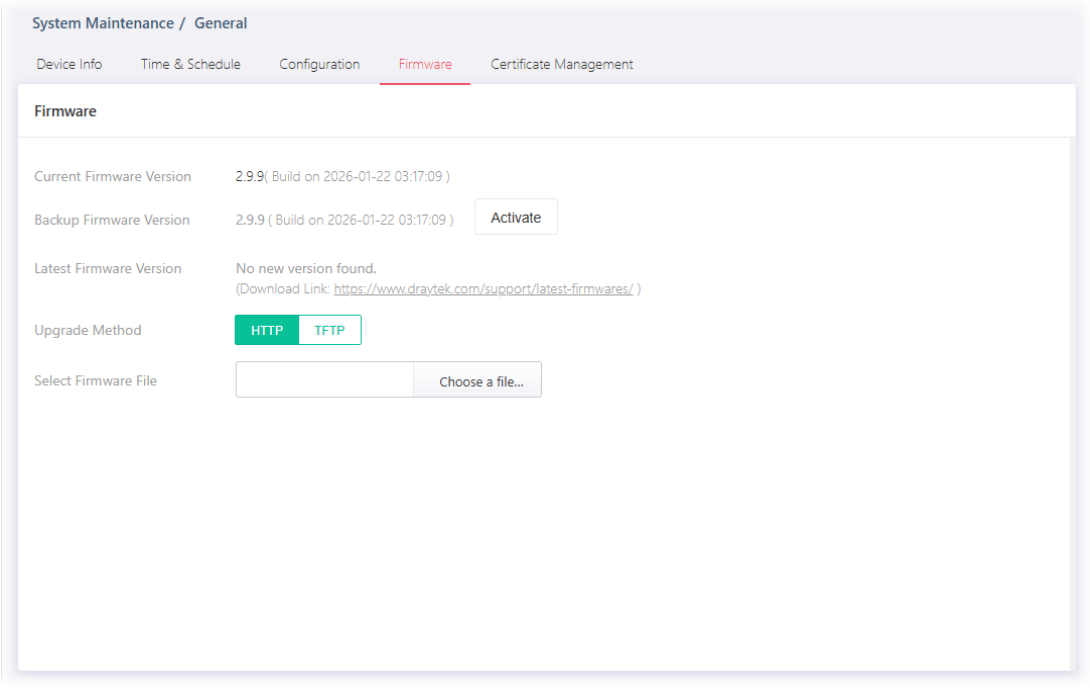
Available settings are explained as follows:

Item	Description
Configuration Backup	
Backup Method	Select Backup method. **HTTP** - Use WEB browser to backup firmware. **TFTP** - Use TFTP to backup firmware. ● **Server IP Address** - Enter the IPv4/IPv6 address for the TFTP server.
Backup Content	**Backup** - Make a backup copy for the configurations for VigorSwitch.
Configuration Restore	
Restore Method	Select **Restore** method. **HTTP** - Use WEB browser to restore firmware. ● **Select Configuration File** - Choose the file which will be used to restore the configuration settings. **TFTP** - Use TFTP to restore firmware. ● **Server IP Address** - Enter the IPv4/IPv6 address for the TFTP server. ● **File Name** - Enter the firmware image or configuration file name on the TFTP server.

After finishing this web page configuration, please click **OK** to save the settings.

VI-1-4 Firmware

This page 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.



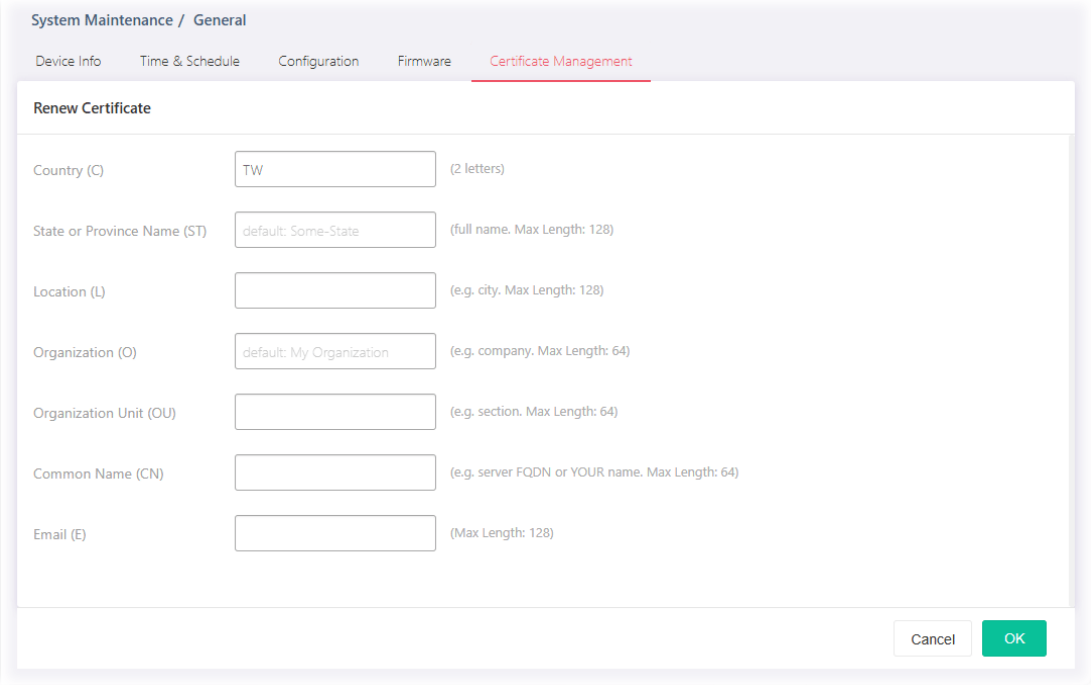
Available settings are explained as follows:

Item	Description
Firmware	
Current Firmware Version	Display current used firmware.
Upgrade Method	Select Upgrade method: **HTTP** - Use WEB browser to upgrade firmware. • **Select Firmware File -** Choose the firmware file located in your computer. **TFTP** - Use TFTP to upgrade firmware. • **Server IP Address** - Enter the IPv4/IPv6 address for the TFTP server. • **File Name** - Enter the firmware image or configuration file name on the TFTP server.

After finishing this web page configuration, please click **OK** to save the settings.

VI-1-5 Certificate Manager

Use this page to renew the certificate that your root CA generated before.



Item	Description
Renew Certificate	
Country (C)	Country in which your organization is located.
State or Province Name (DT)	State or province where your organization is located.
Location (L)	City where you're your organization is located.
Organization (O)	Legal name of your organization.
Organization Unit (OU)	Department within your organization that you wish to be associated with this certificate.
Common Name (CN)	Fully-qualified domain name / WAN IP that will be used to reach your server.
Email (E)	Email address of the entry.

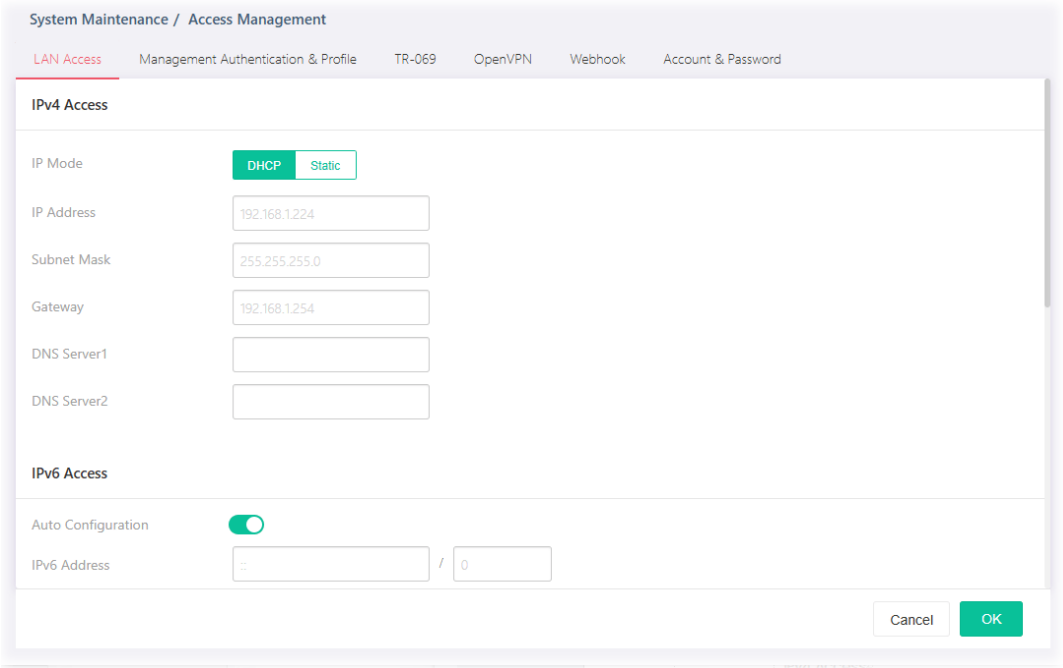
After finishing this web page configuration, please click **OK** to save the settings.

VI-2 Access Management

VI-2-1 LAN Access

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.

Use the IP Address (IPv4/IPv6) 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. In addition, 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.



Available settings are explained as follows:

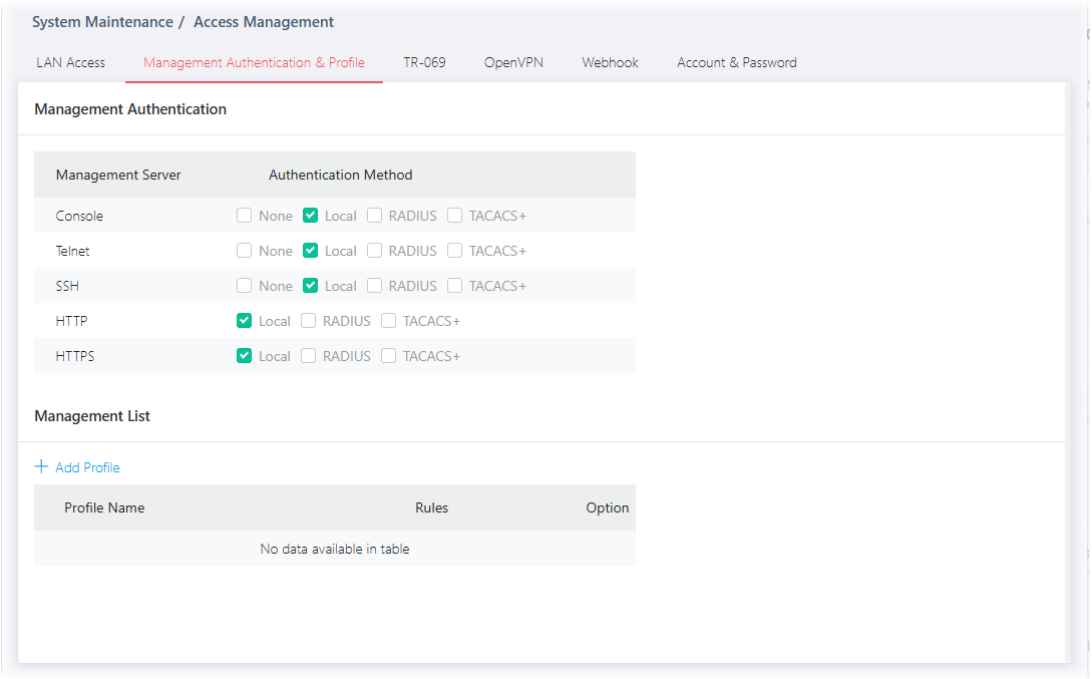
Item	Description
IPv4 Access	
IP Mode	Select the mode of network connection. **DHCP** - Use static IPv4 address. **Static** - Use DHCP provisioned IP address and Gateway if feasible. • **IP Address** - Enter the IP address of your switch in dotted decimal notation for example 192.168.1.224. If static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

	address in this field. • **DNS Server1/2** - Enter primary/ secondary DNS server address in this field.
IPv6 Access	
Auto Configuration	Switch the toggle to enable / disable this function.  - means “Enable”. Let the switch automatically configure IPv6 address. • **DHCPv6 Client** - Enable this feature if there is a DHCPv6 server on your network for assigning IPv6 Address, instead of using Router Advertisement. - means “Disable”. • **IPv6 Address** - Enter the IPv6 address of your switch. If auto configuration mode is disabled, enter IPv6 address in this field. • **Gateway** - Enter the IPv6 address of the router as your default IPv6 gateway to access IPv6 Internet or other IPv6 network. • **DNS Server1/2** - Enter primary/ secondary DNS server address in this field.
Management VLAN	
Management VLAN	Select the VLAN ID as management VLAN.
Protocol Access	
HTTP Server, **HTTPS Server,** **Enforce HTTPS Server,** **Telnet Server,** **SSH Server,** **SSH Key Authentication with No Password**	Select the protocol(s) for remote access.

After finishing this web page configuration, please click **OK** to save the settings.

VI-2-2 Management Authentication & Profile

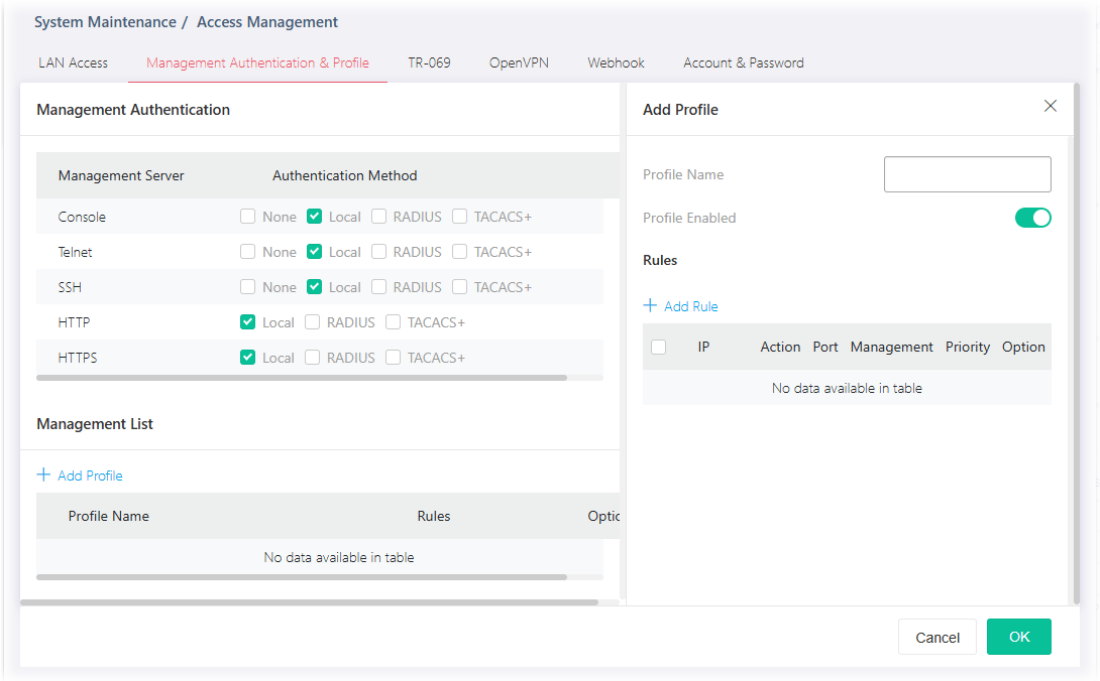
The system administrator can log in VigorSwitch from profiles defined on this page. All profiles will apply the configuration of management server(s) and authentication method(s) settings.



Available settings are explained as follows:

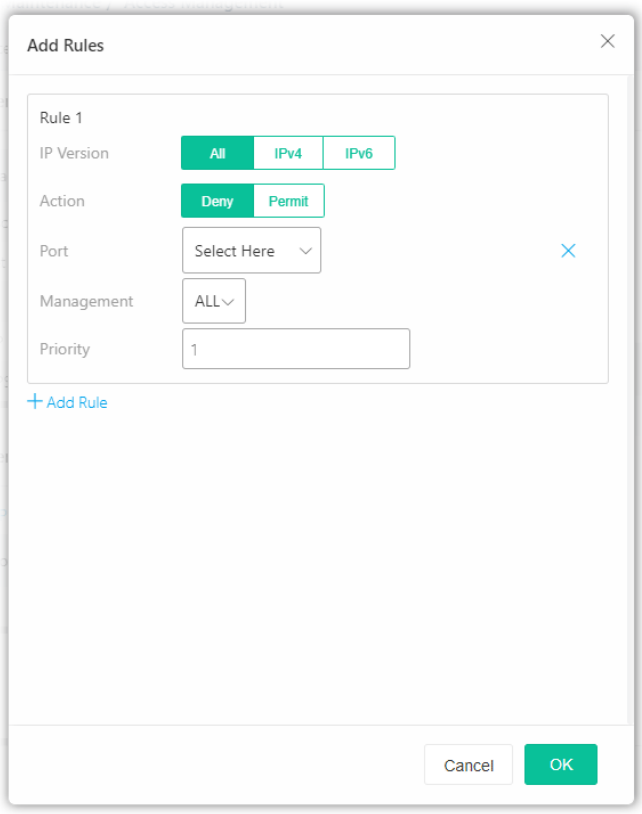
Item	Description
Management Authentication	
Management Server	Displays available servers set as management server.
Authentication Method	Displays available protocols for different management servers. Select one or more protocols for each server.
Management List	Displays a list of profiles that will apply the settings of server and authentication defined above. **+ Add Profile** - Click to create a new management profile.

To add a remote server, click the "**+Add Profile**" to open the edit page.



Available settings are explained as follows:

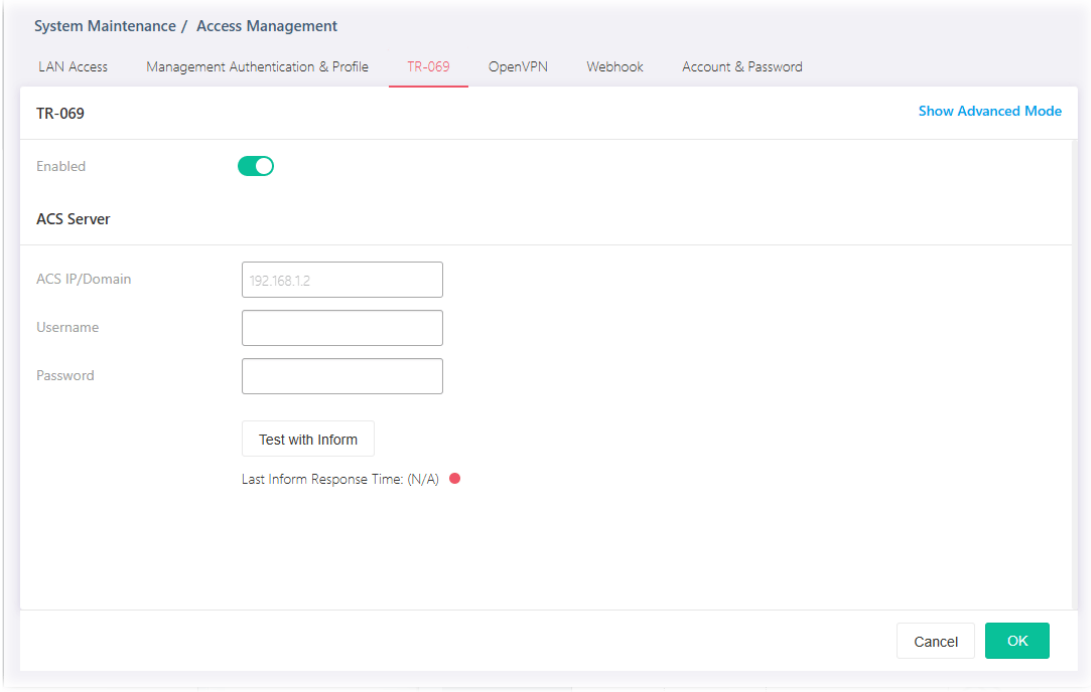
Item	Description
Add Profile	
Profile Name	Enter a name for an authentication profile.
Profile Enabled	Switch the toggle to enable / disable this profile. - means "Enable". - means "Disable".
+Add Rule	Click to create rules.

	 **IP Version** - 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. Enter the IPv4 address/subnet to which the ACE rule should apply. • **IPv6** –Specify the IPv6 address /subnet. Enter the IPv6 address/subnet to which the ACE rule should apply. **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. **Port** - Select the ports to which the ACL profile should be applied. **Management** - Specify a management server for this rule. **Priority** - Specify a priority number (1 to 65535) for such rule. The lower the number, the higher the priority.
OK	Save the settings.

After finishing this web page configuration, please click **OK** to save the settings.

VI-2-3 TR-069

This page allows a user to configure TR-069 settings for connecting to VigorACS 3.



Available settings are explained as follows:

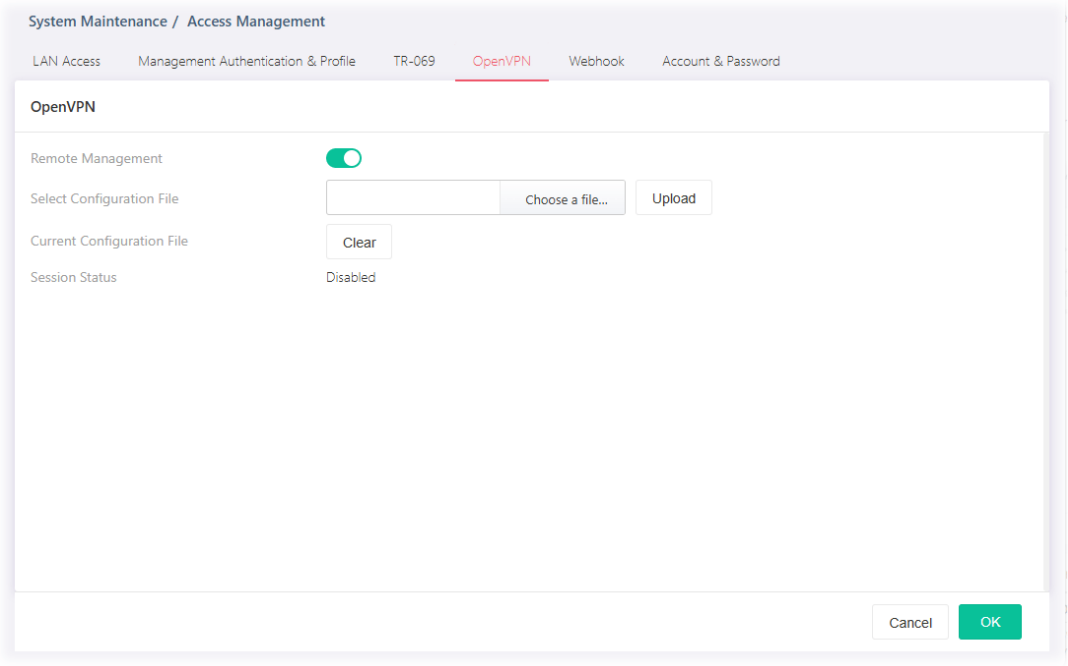
Item	Description
Show/Hide Advanced Mode	Click to display / hide the advanced mode settings.
TR-069	**Enabled** - Switch the toggle to enable / disable this function.  - means "Enable". - means "Disable".
Basic Mode - ACS Server	
ACS IP/Domain	Enter the IP address or domain name of the server.
Username	Enter the username that you wan to link with the VigorACS (Auto Configuration Server).
Password	Enter the password that you wan to link with the VigorACS (Auto Configuration Server).
Test with Inform	Click to send a message to test if this CPE is able to communicate with VigorACS server.
Advanced Mode - ACS Server	
Protocol	Choose **HTTP** or **HTTPS** for connecting with VigorACS.
Port	Enter a value that VigorACS can use to access to this switch.
ACS IP/Domain	Enter the IP address or domain name of the server.
Handler	Enter the URL that you wan to link with the VigorACS (Auto Configuration Server).

Username	Enter the username that you wan to link with the VigorACS (Auto Configuration Server).
Password	Enter the password that you wan to link with the VigorACS (Auto Configuration Server).
Test with Inform	Click to send a message to test if this 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	Enter a value that VigorACS can use to access to 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 switch.
TLS Version	
TLS Minimum Protocol Version	Due to security consideration, the built-in HTTPS VPN server of the router had upgraded to TLS1.x protocol (TLS1.2/TLS1.3). Select one of the versions.
Periodic Inform	
Enabled	Switch the toggle to enable/disable the function.
Interval Time	Set the interval time for the switch to send notification to CPE.
STUN Settings	
Enabled	Switch the toggle to enable / disable this function.  - means “Enable”. - means “Disable”.
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 the STUN server 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 the STUN server 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.
Notification	
Port Link Up/Down	Vigor system will check the health status of LAN ports including link up /down, speed change or PoE power disconnection. 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.
PoE Port Warning	Select LAN port(s) to do the health check of PoE power.

After finishing this web page configuration, please click **OK** to save the settings.

VI-2-4 OpenVPN

Devices connecting to VigorSwitch can transmit data to remote end via OpenVPN to ensure the information security.



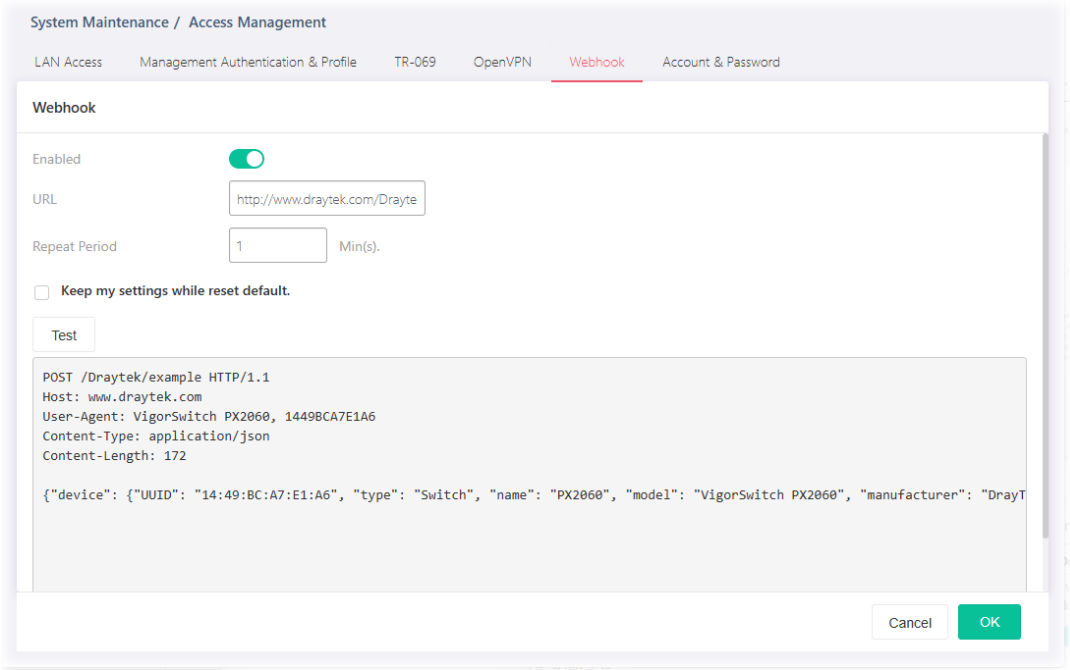
Available settings are explained as follows:

Item	Description
Remote Management	Switch the toggle to enable / disable OpenVPN tunnel between VigorSwitch with the remote end.  - means "Enable". - means "Disable".
Select Configuration File	It is available when remote management is enabled. As a VPN client, please import the OpenVPN config file coming from OpenVPN server.
Current Configuration File	Click to remove current configuration file.
Session Status	Display current OpenVPN status (Disabled, Connecting or Success).

After finishing this web page configuration, please click **OK** to save the settings.

VI-2-5 Webhook

Without getting any request, VigorSwitch will send the data (if available) that a user concerned to the specified URL (provided by remote client) automatically.



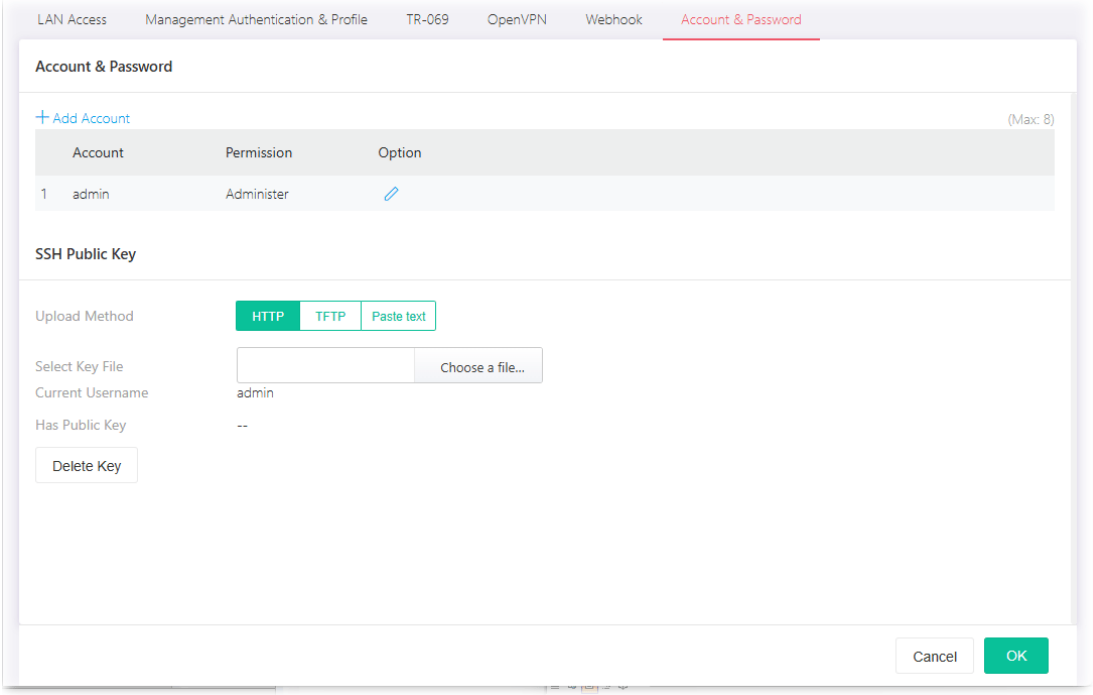
Available settings are explained as follows:

Item	Description
Enabled	Switch the toggle to enable / disable the webhook service. The data will be transmitted to the specified URL.  - means “Enable”. - means “Disable”.
URL	Specify the destination to receive the real-time data by entering the URL. Please get the URL from the client who wants to obtain the newest and available data automatically from the Vigor switch.
Repeat Period	Set the transmission interval (unit is minute).
Keep my settings while reset default	Check the box to keep the webhook configuration when resetting VigorSwitch with default settings.
Test	Vigor system will send a test report to the remote address.

After finishing this web page configuration, please click **OK** to save the settings.

VI-2-6 Account & Password

This page allows a user to add or delete local user on switch database for authentication.



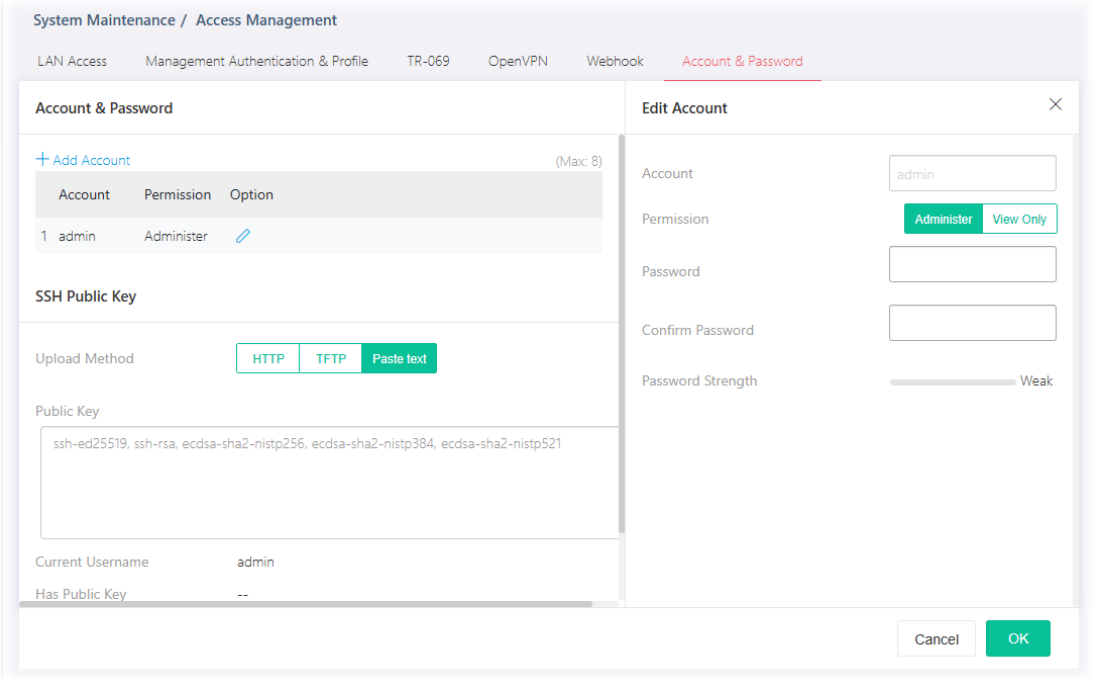
Available settings are explained as follows:

Item	Description
Account & Password	
+Add Account	Click to create a new account.
Account	Displays the name of the account.
Permission	Displays the privilege level (Admin or View Only) of the account.
Option	- Click to modify the account settings.
SSH Public Key	
Upload Method	Any client will be authenticated by SSH public key for using the SSH service. Please select the upload method for uploading the SSH public key. **HTTP** - Use WEB browser to upload the public key. • **Select Key File -** Choose the key file located in your computer. **TFTP** - Use TFTP to upload the public key. • **Server IP Address** - Enter the IPv4/IPv6 address for the TFTP server. • **File Name** - Enter the name of the public key on the TFTP server. **Paste text -** Use text to upload the public key. • **Public Key** - Enter the text composing the public key.

Current Username	Displays current username used for accessing the switch's web userinfterface.
Has Public Key	Displays if the user owns the SSH public key or not (v means YES; -- means NO).
Delete Key	Remove the public key for the selected user account.

To modify an existing schedule profile, click the link of  of the one to be changed.

To add a schedule profile, click the "**+ Add Account**" to open the edit page.



Available settings are explained as follows:

Item	Description
Add Account	
Account	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.
Permission	**Administer** - Allow to change switch settings. **View Only** - See switch settings only. Not allow to change it.
Password	Enter a password for new account.
Confirm Password	Enter the password again for confirmation.
Password Strength	Displays the strength of the password, indicated by the words "weak", "medium" or "strong".

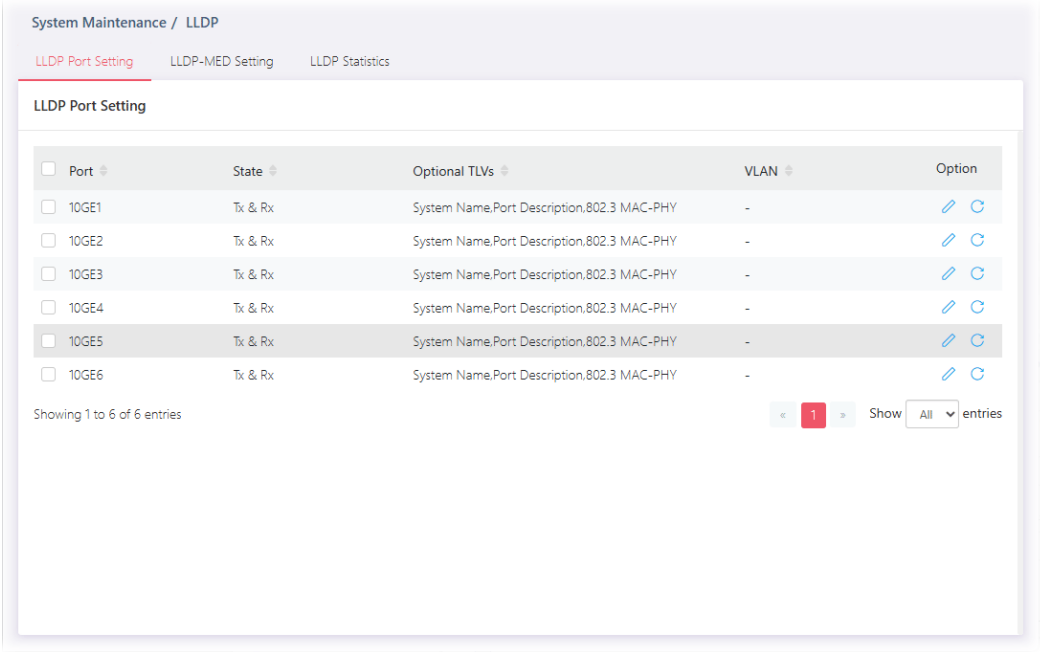
After finishing this web page configuration, please click **OK** to save the settings.

VI-3 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-3-1 LLDP Port Setting

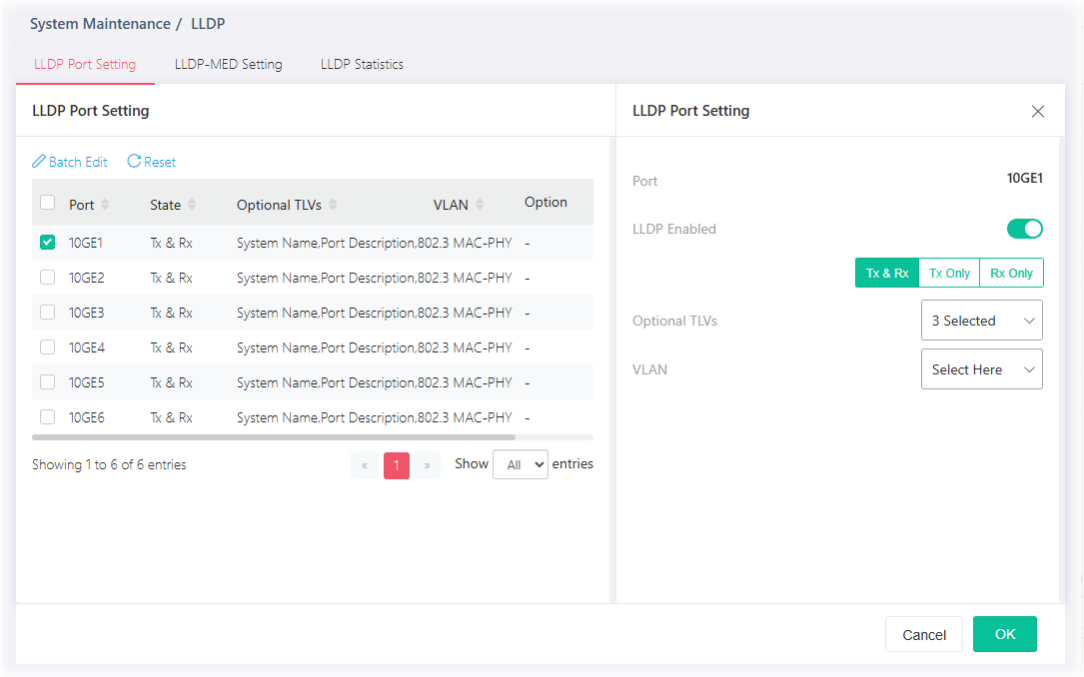
This page allows a user to select specified port or all ports to configure LLDP state.



Available settings are explained as follows:

Item	Description
Port	Displays the index number of GE ports (10GE1 to 10GE6).
State	Displays the transmission of LLDP PDUs.
Optional TLVs	Displays the data communication protocols and optional information.
VLAN	Displays the VLAN ID number.
Option	- Click to modify the LLDP port settings of the selected port. - Clear current settings and return to factory default settings.

To modify the port settings for the selected port, click the link of of the one to be changed.



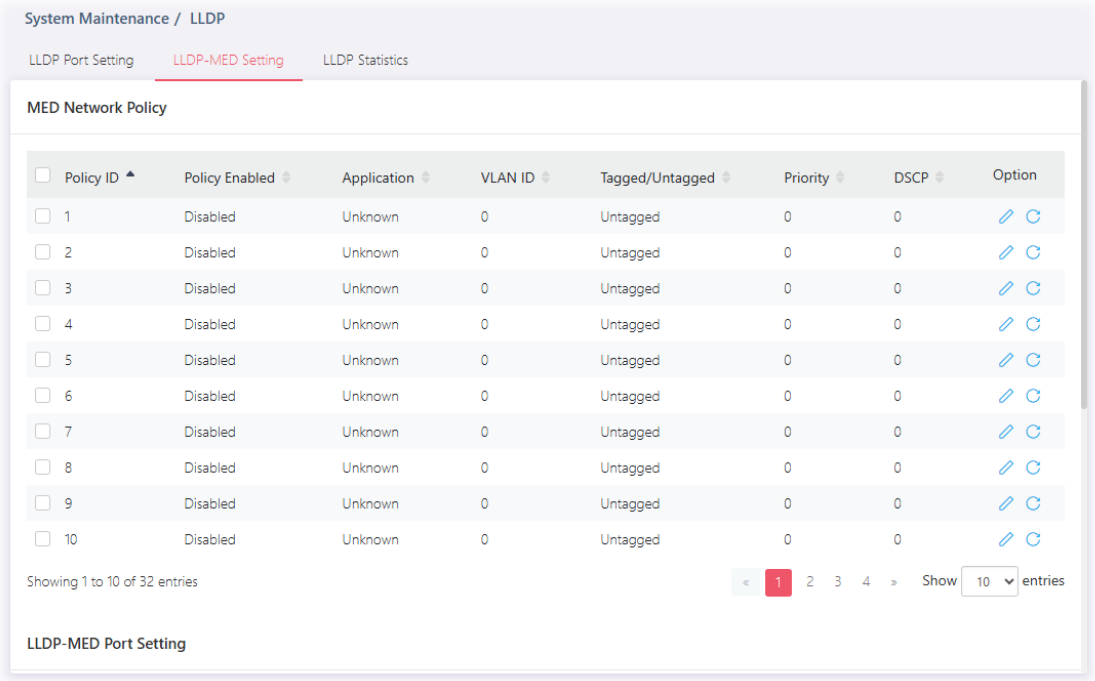
Available settings are explained as follows:

Item	Description
Port	Displays the index number of GE ports (10GE1 to 10GE6).
LLDP Enabled	Switch the toggle to enable / disable this function.  - means "Enable". - means "Disable". **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).

After finishing this web page configuration, please click **OK** to save the settings.

VI-3-2 LLDP-MED Setting

This page allows the network administrator to set MED (Media Endpoint Discovery) network policy and configure TLV (Type / Length / Value) settings for each port.

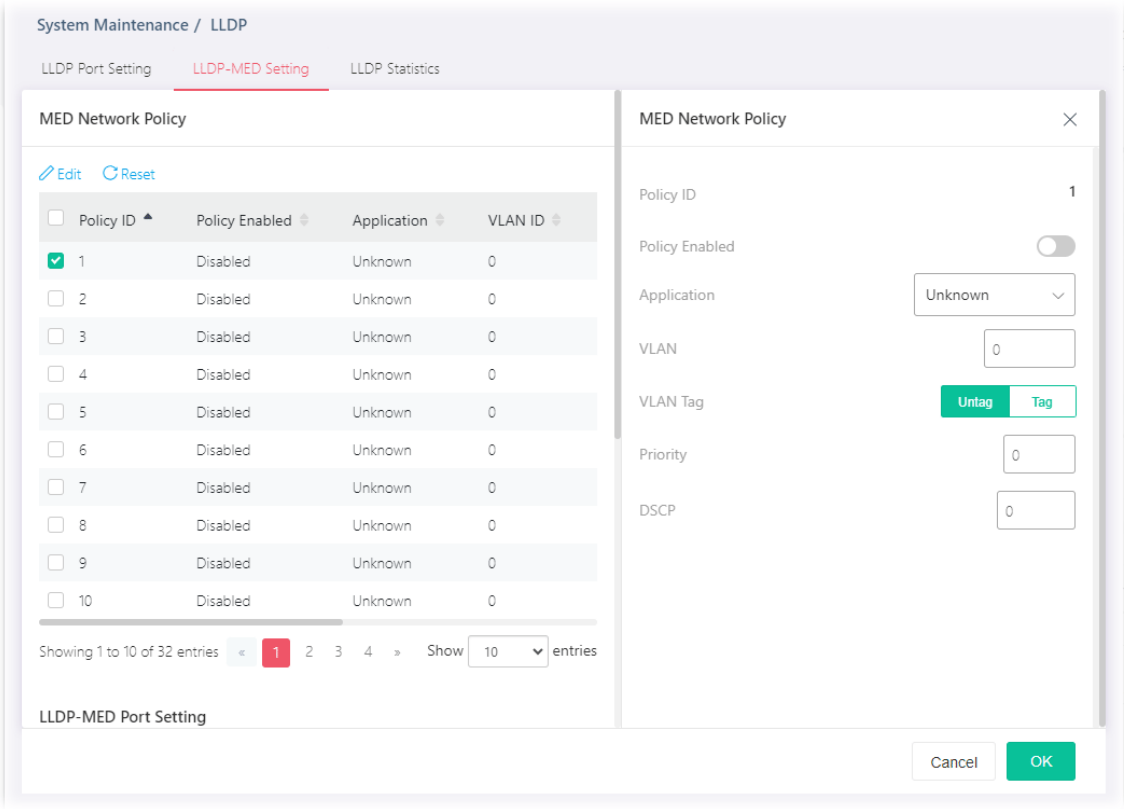


Available settings are explained as follows:

Item	Description
Option	- Click to modify the LLDP port settings of the selected policy. - Clear current settings and return to factory default settings.

VI-3-2-1 MED Network Policy

To modify the port settings for the selected MED network policy, click the link of  of the one to be changed.



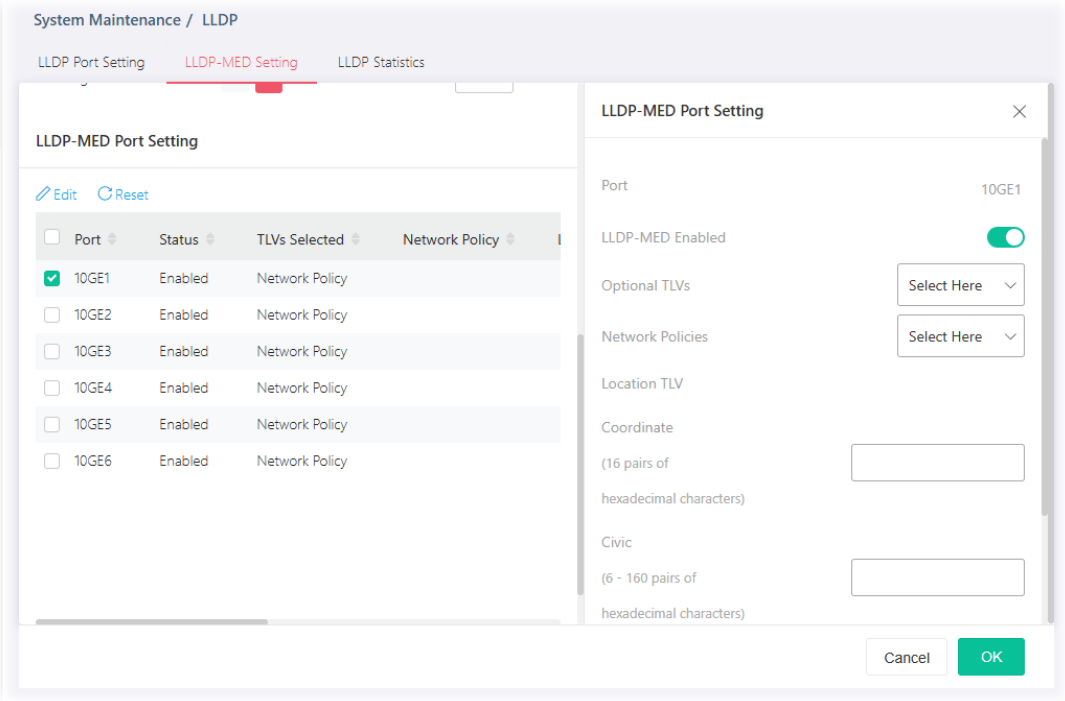
Available settings are explained as follows:

Item	Description
Policy ID	Choose a number for configuring the policy profile. Available selections include 1 to 32.
Policy Enabled	Switch the toggle to enable / disable this function.  - means “Enable”. - means “Disable”.
Application	There are several applications which can be used for MED network. Selections include Voice, 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 4094) for this 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).
OK	Save the settings.

After finishing this web page configuration, please click **OK** to save the settings.

VI-3-2-2 LLDP-MED Port Setting

To modify the port settings for the selected MED port setting, click the link of of the one to be changed.



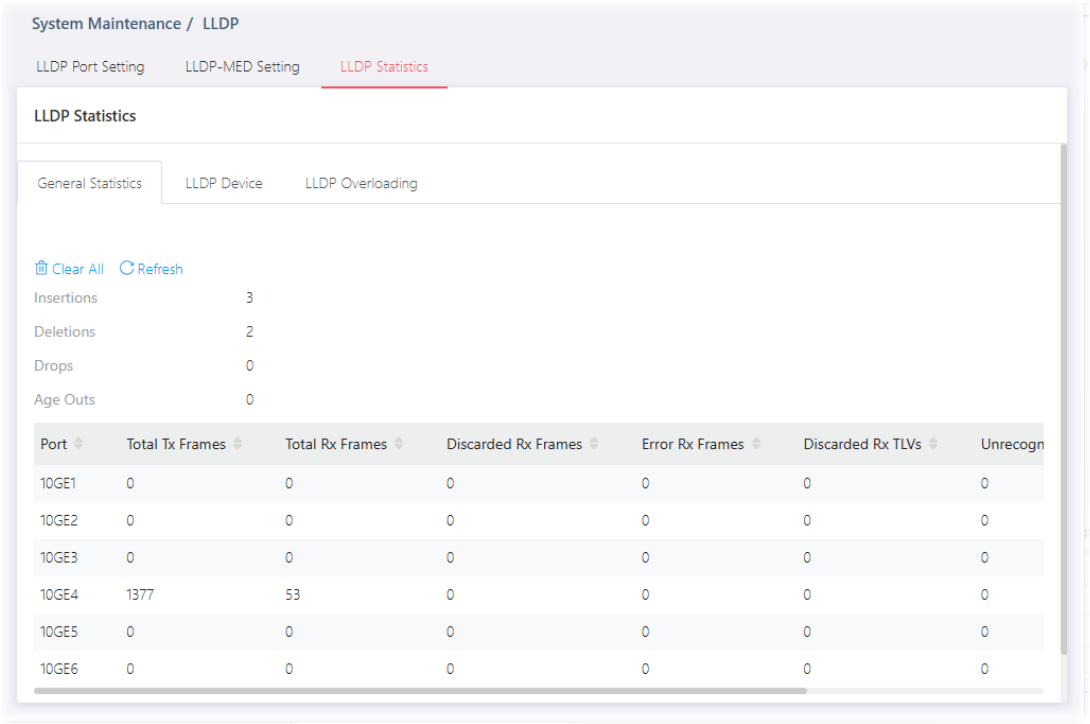
Available settings are explained as follows:

Item	Description
LLDP-MED Port Setting	
Port	Displays the index number of LAN port.
LLDP-MED Enable	Switch the toggle to enable / disable the LLDP MED on the selected port. - means "Enable". - means "Disable".
Optional TLVs	There are three TLVs (Type / Length / Value) for choosing: **Location**, **Inventory**, **Network Policy** and **Select All.** Select the one(s) for this profile.
Network Policies	Select network policy profiles for applying onto the selected port.
Location TLV 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.
OK	Save the settings.

After finishing this web page configuration, please click **OK** to save the settings.

VI-3-3 LLDP Statistics

This page offers the statistics of LLDP packets (in, out and error) of each port (10GE1 to 10GE6).



Available settings are explained as follows:

Item	Description
Clear All	Clear it to remove all logs displayed in this page.
Refresh	Click it to refresh the log.
Port	Displays the port number.

VI-4 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

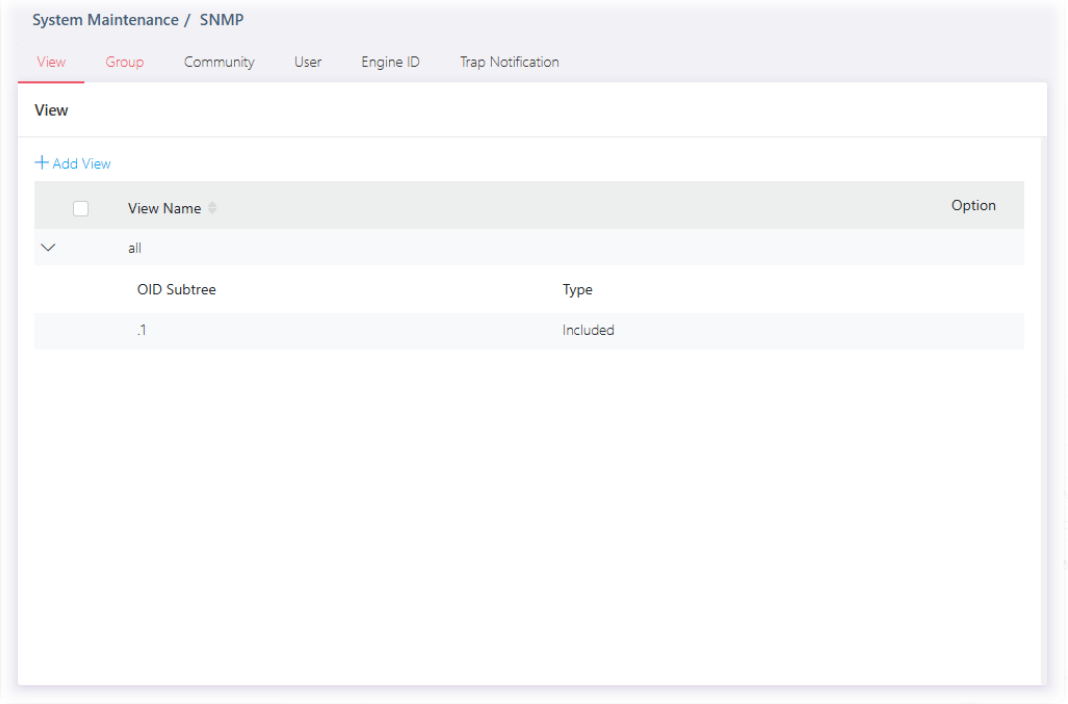
A managed device is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional (read and write) access to node-specific information. Managed devices exchange node-specific information with the NMSs. Sometimes called network elements, the managed devices can 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-4-1 View

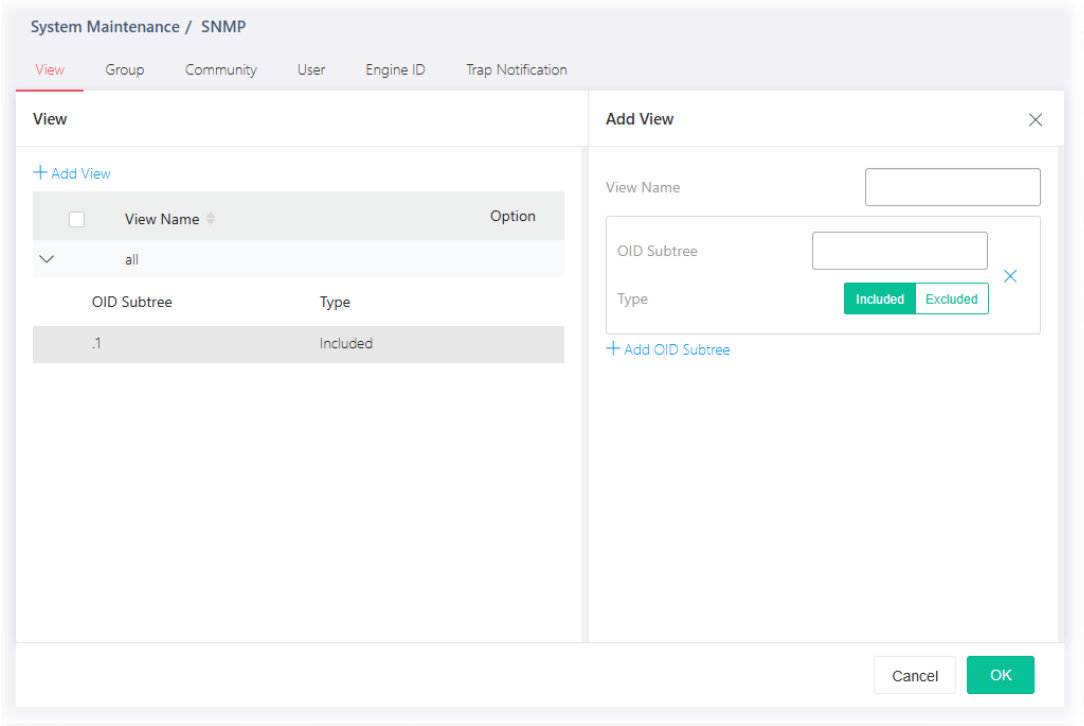
This page allows the network administrator to create MIB views (Management information base) and then include or exclude OID (Object Identifier) in a view.



Available settings are explained as follows:

Item	Description
+Add View	Click it to add a new MIB view profile.
View Name	Displays the name of the MIB view.

To add a schedule profile, click the "**+ Add View**" to open the edit page.



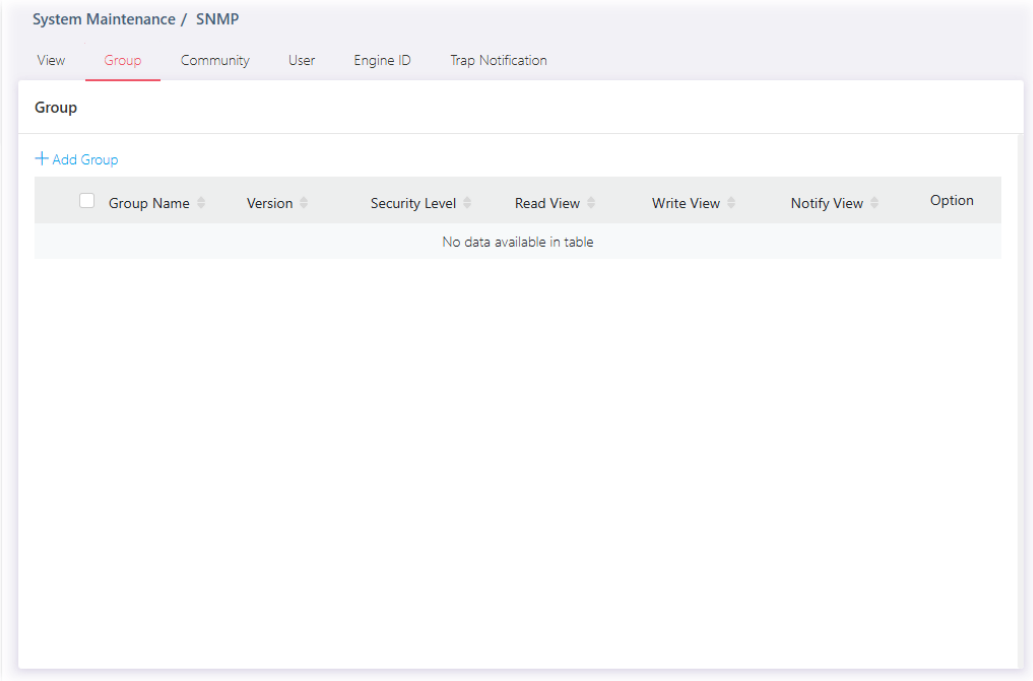
Available settings are explained as follows:

Item	Description
View Name	Enter a name of the MIB view.
OID Subtree	Enter an OID string to be included or excluded (based on the view type setting) from the MIB view.
Type	Determine to include or exclude the selected MIBs. • Include • Exclude
+Add OID Subtree	Click it to add a new MIB view profile.

After finishing this web page configuration, please click **OK** to save the settings.

VI-4-2 Group

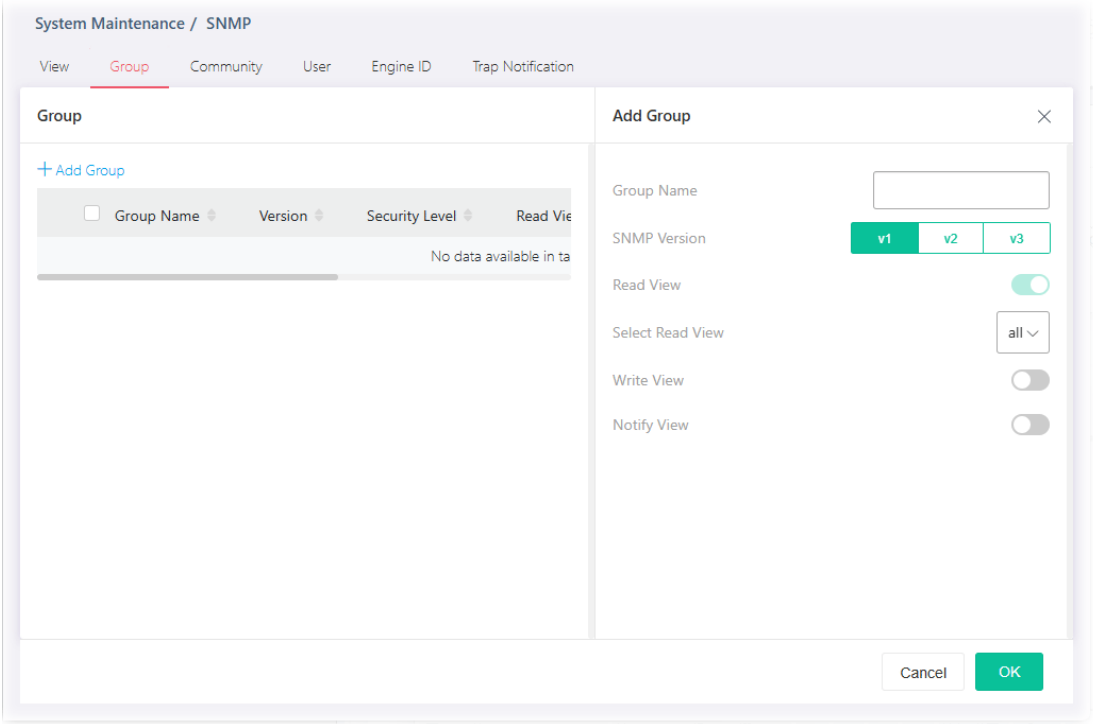
This page allows the network administrator to group SNMP users and assign different authorization and access privileges.



Available settings are explained as follows:

Item	Description
+Add Group	Click it to create a new group profile.
Group Name	Displays the name for the group.
Version	Displays the SNMP version adopted by the group.
Security Level	Displays the SNMP security level for the group.
Read View	Displays the read view profile.
Write View	Displays the write view profile.
Notify View	Displays the notify view profile.

To add a schedule profile, click the "**+ Add Group**" to open the edit page.



Available settings are explained as follows:

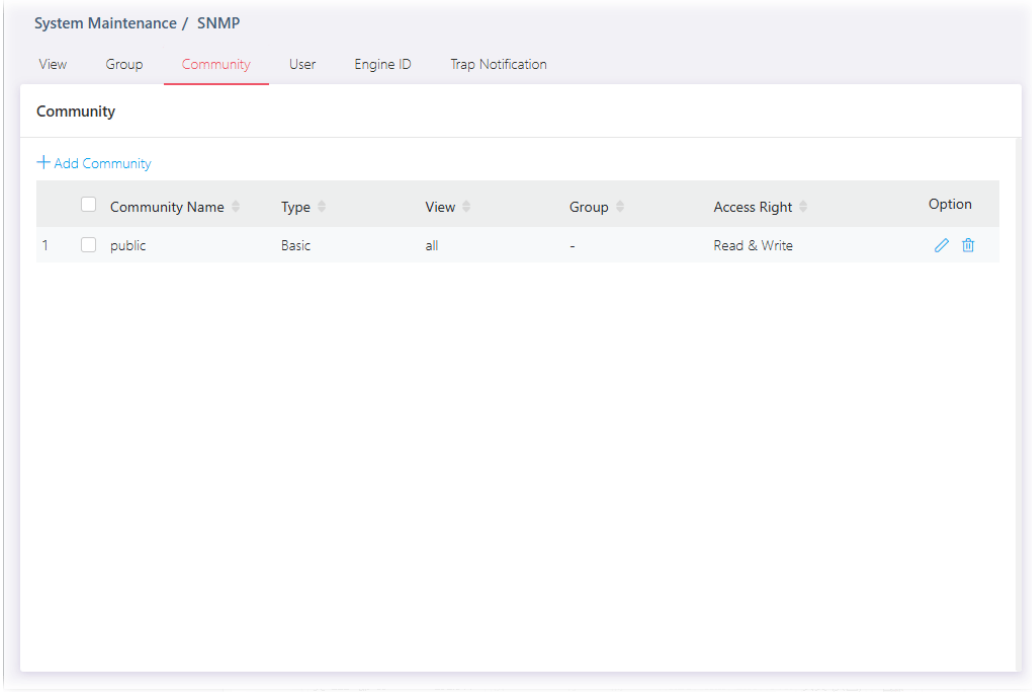
Item	Description
Add Group	
Group Name	Enter a name for the group.
SNMP Version	Specify SNMP version (v1, v2 or v3).
Security Level	Specify SNMP security level for the group. It is available when **SNMPv3** is selected. ● **No Security** – No authentication. ● **Authentication** – Authentication without encryption will be performed for packets. ● **Authentication and Privacy** – Authentication with encryption will be performed for packets.
Read View	Switch the toggle to enable / disable this function. If it is enabled, users of this group have the right to read the selected MIB view.  - means "Enable". - means "Disable".
Select Read 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	Switch the toggle to enable / disable this function. If it is enabled, users of this group have the right to write the selected MIB view. **Select Write 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	Switch the toggle to enable / disable this function. If it is enabled, users of this group have the right to send notifications for the

	selected MIB view. **Select Notify 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.

After finishing this web page configuration, please click **OK** to save the settings.

VI-4-3 Community

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

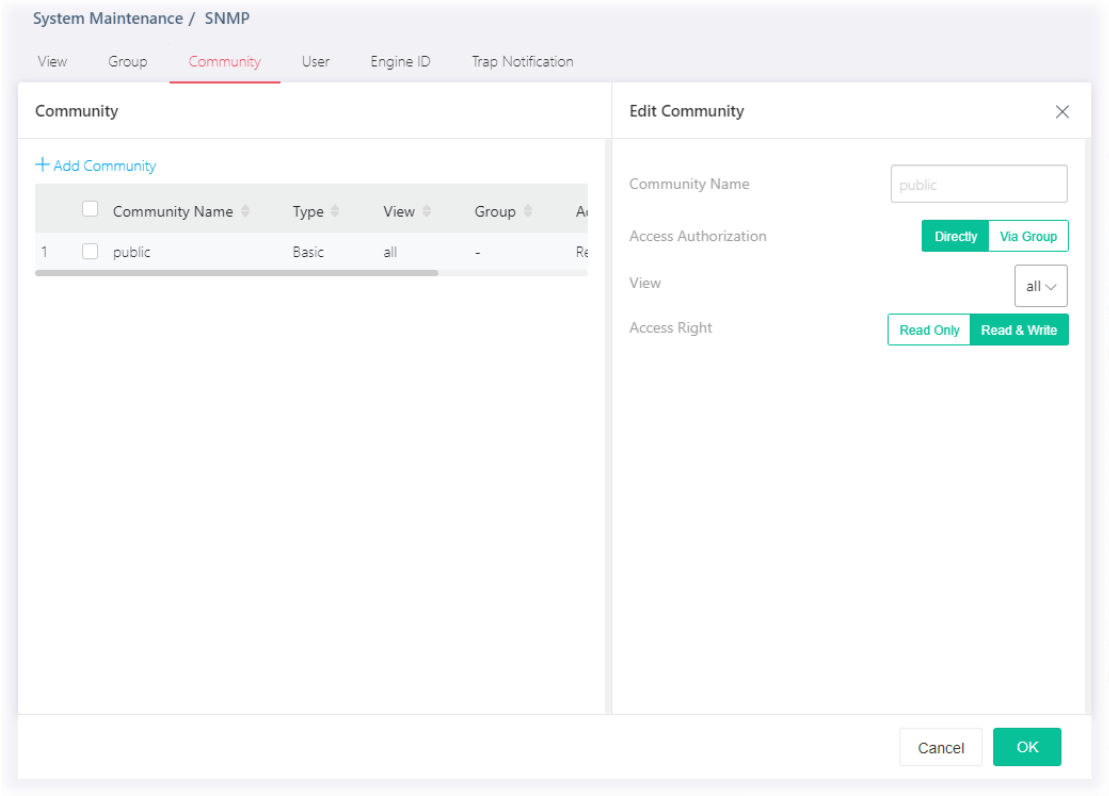


Available settings are explained as follows:

Item	Description
+Add Community	Click it to add a new community.
Community Name	Displays the community name.
View	Displays the name of the view profile.
Group	Displays the name of the group.
Access Right	Displays the accessing right (read, read and write) that this community has.
Option	- Click to modify the settings of the community. - Remove the selected entry.

To modify an existing community profile, click the link of of the one to be changed.

To add a schedule profile, click the "**+ Add Community**" to open the edit page.



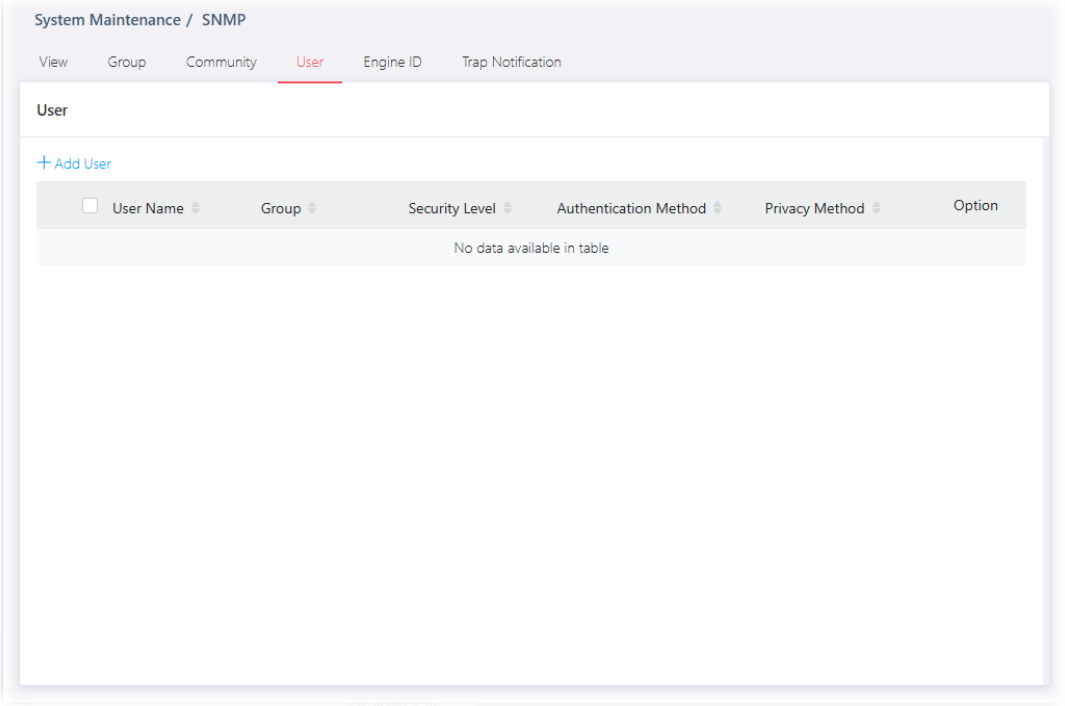
Available settings are explained as follows:

Item	Description
Add Community	
Community Name	Enter a name as community name. The maximum length of the text is limited to 23 characters.
Access Authorization	**Directly -** View and access right can be specified for this SNMP community profile. **Via Group -** Specify one of the SNMP groups for this SNMP community profile.
View	Simply specify one of the view profiles from the drop down list.
Group	It is available when **Via Group** is selected as access authorization. Specify a SNMP group to define the object available to the community.
Access Right	Define the access right of the community group. **Read Only -** It allows unidirectional access to node-specific information. **Read & Write -** It allows bidirectional access to node-specific information.

After finishing this web page configuration, please click **OK** to save the settings.

VI-4-4 User

This page allows a user to configure SNMP user profile(s).

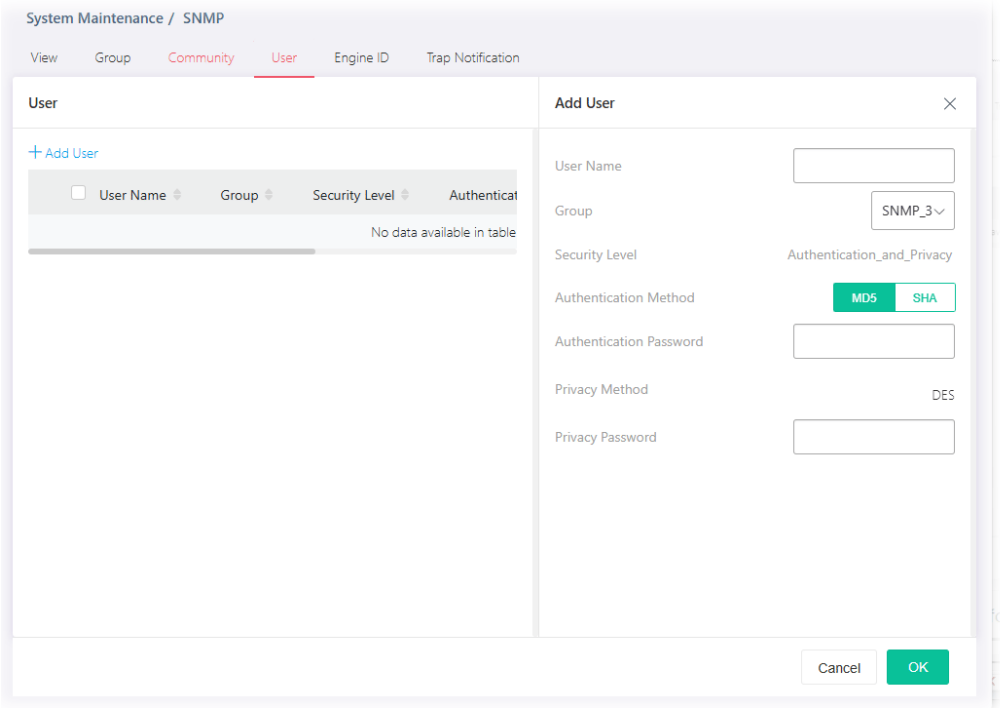


Available settings are explained as follows:

Item	Description
+Add User	Click it to add a new user profile.
User Name	Displays the name of this user profile.
Group	Displays the group name to which this user profile belongs.
Security Level	Displays the security method used by this user profile.
Authentication Method	Displays the authentication method used by this user profile.
Privacy Method	Displays the privacy method used by this user profile.
Option	- Click to modify the server setting. - Clear the selected entry.

To modify an existing user profile, click the link of of the one to be changed.

To add a user profile, click the "**+ Add User**" to open the edit page.



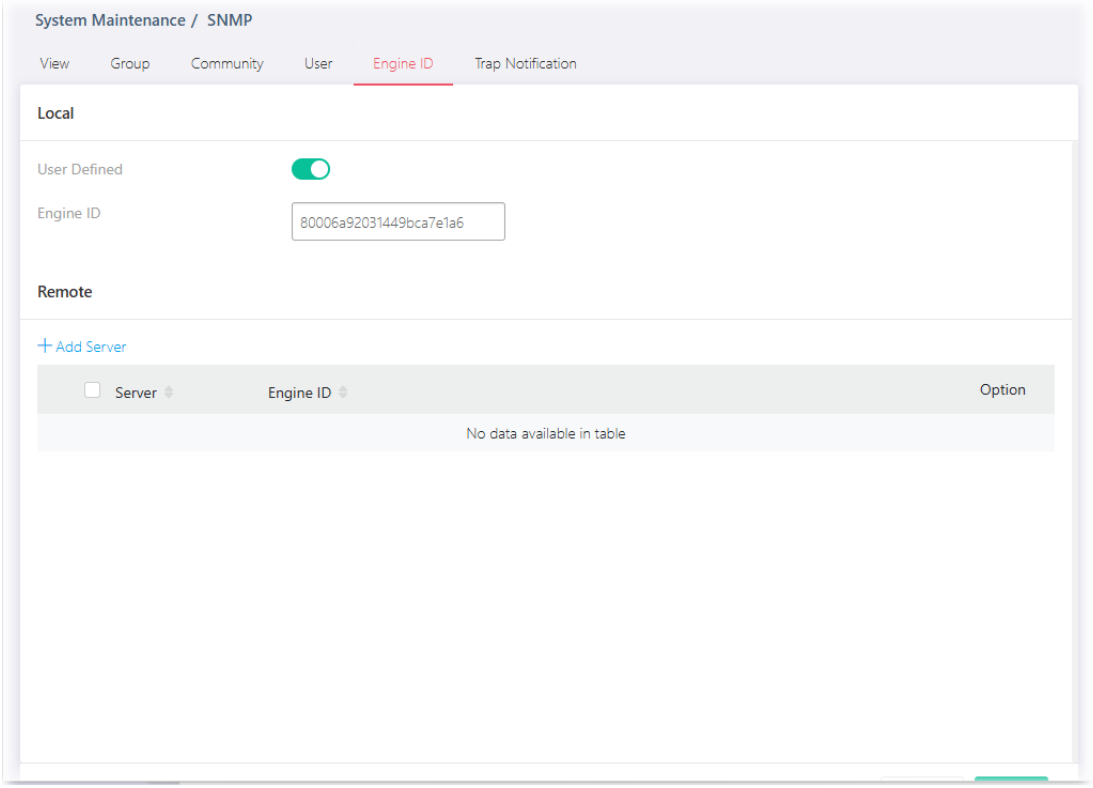
Available settings are explained as follows:

Item	Description
Add User	
User Name	Enter a name for creating new SNMP user.
Group	Select one of the **SNMP** groups from the drop down list. Then, this user profile will be grouped under the selected SNMP group.
Security Level	Displays the security level configured for the selected SNMP group. If the selected group is not a **SNMPv3** group, nothing will be displayed in this field.
For SNMPv3 group only	
Authentication Method	It is available only when the Security Level is set with "Authentication", or "Authentication_and_Privacy". You can change the methods (None, MD5, SHA) for the selected SNMPv3 group. If no method is available for you to select, that means the selected SNMPv3 group is set with No Security.
Authentication Password	It is available only when the Security Level is set with "Authentication", or "Authentication_and_Privacy". Enter a string as the password for authentication.
Privacy Method	It is available only when the Security Level is set with "Authentication_and_Privacy". You can change the methods (None, DES) for the selected SNMPv3 group. If no method is available for you to select, that means the selected SNMPv3 group is set with No privacy.
Privacy Password	It is available only when the Security Level is set with "Authentication_and_Privacy". Enter a string as the password for authentication.

After finishing this web page configuration, please click **OK** to save the settings.

VI-4-5 Engine ID

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

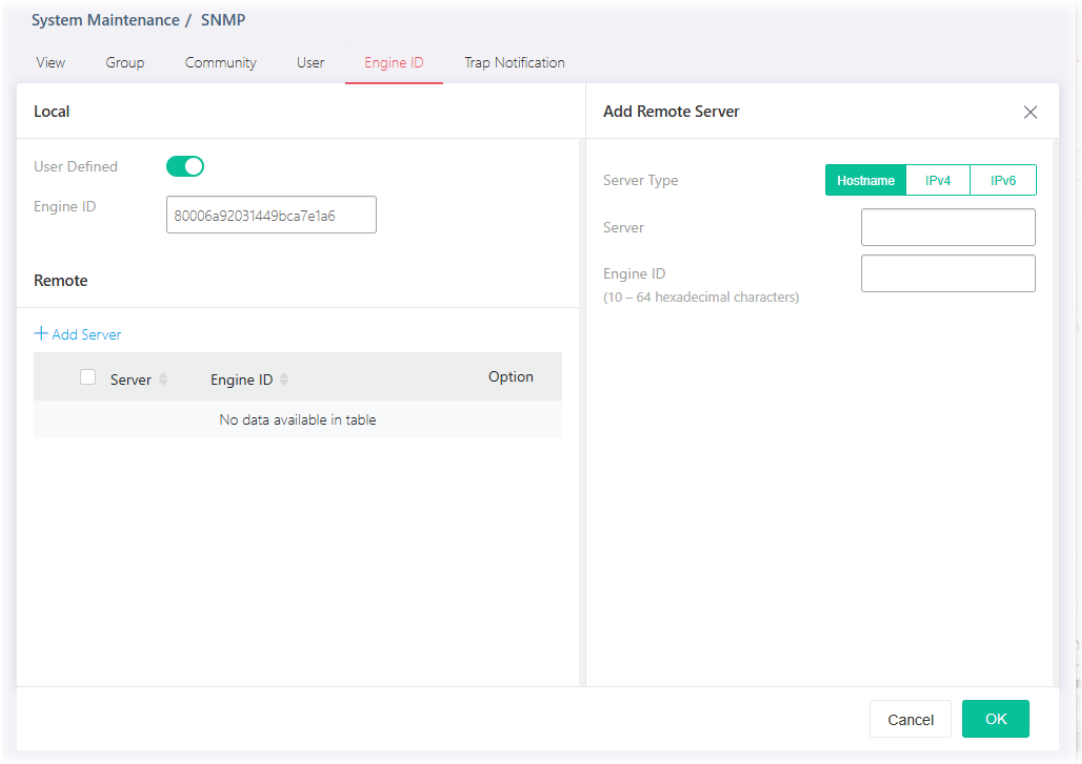


Available settings are explained as follows:

Item	Description
Local	
User Defined	Switch the toggle to enable / disable this function. - means "Enable". - means "Disable".
Engine ID	Displays the engine ID of the local server. The default Engine ID which is made up of MAC and Enterprise ID will be used instead.
Remote	
+Add Server	Click it to create a new remote server profile.
Server	Displays the hostname/IP address of the server.
Engine ID	Displays the engine ID of the remote server.
Option	- Click to modify the server setting. - Clear the selected entry.

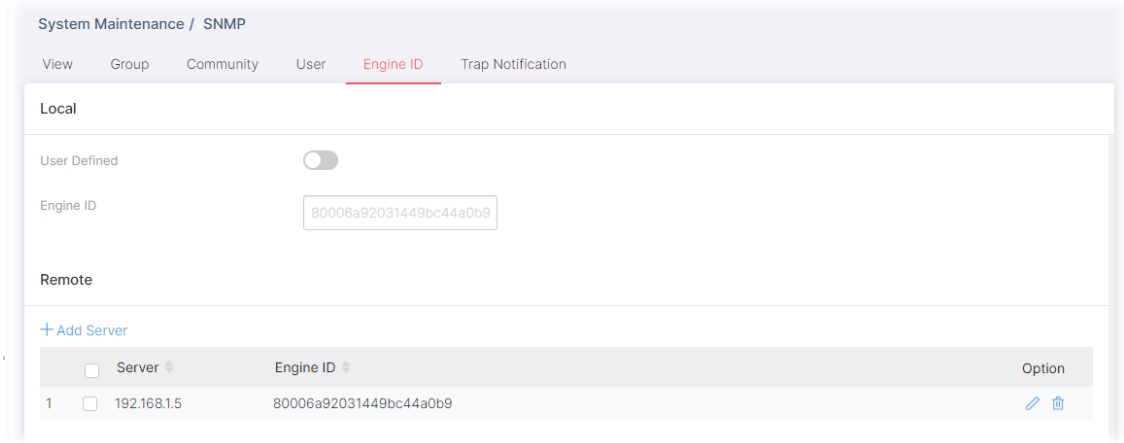
To modify an existing server profile, click the link of of the one to be changed.

To add a remote server profile, click the "**+ Add Server**" to open the page.



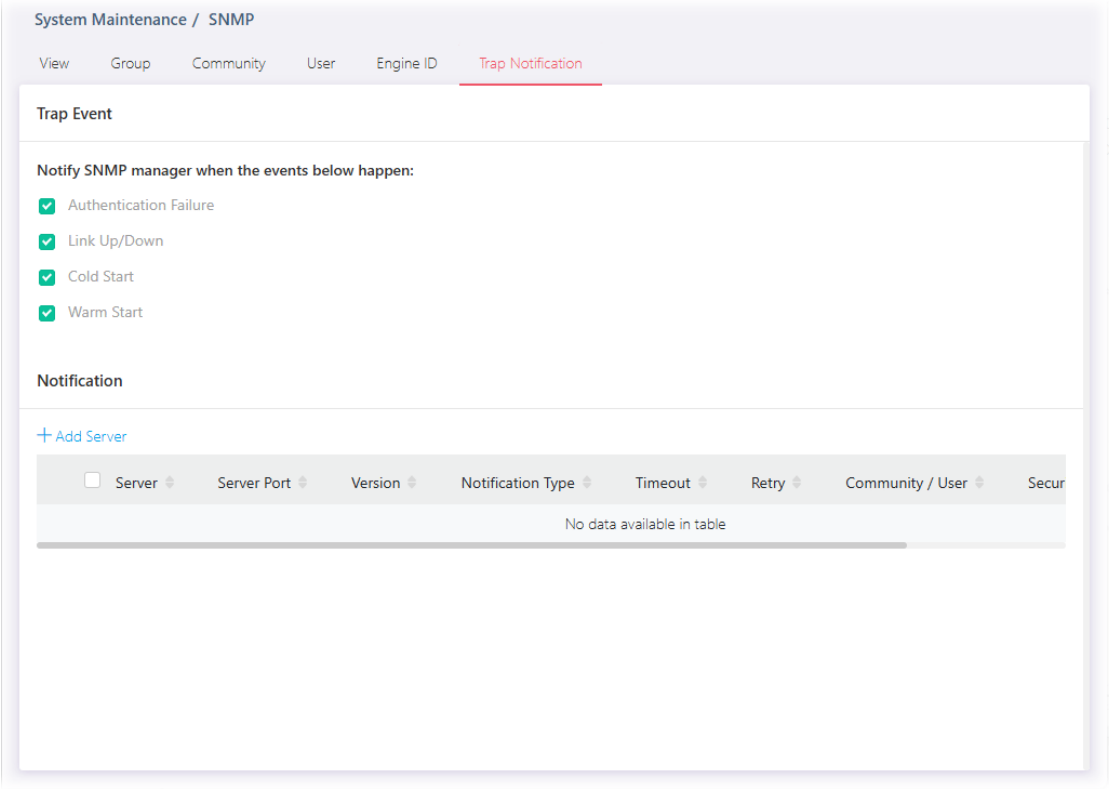
Available settings are explained as follows:

Item	Description
Add Remote Server	



VI-4-6 Trap Notification

This page allows a user to add or delete the SNMP trap receiver IP address and community name. In addition, it allows a user to configure a host to receive SNMPv1/v2/v3 notification.



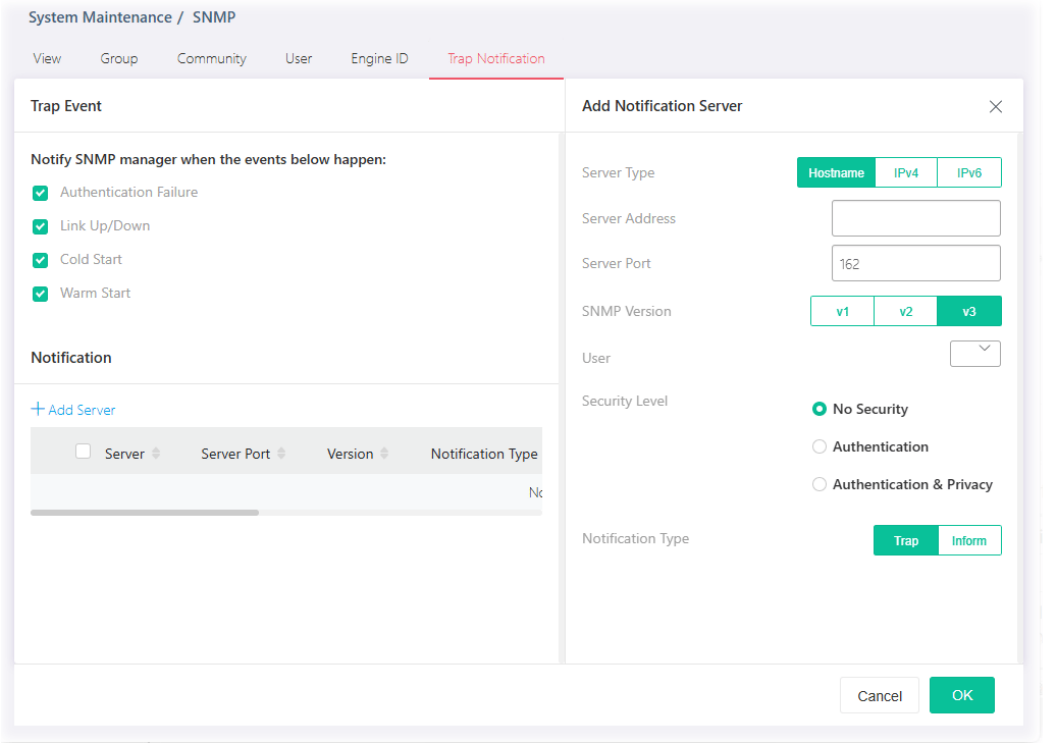
Available settings are explained as follows:

Item	Description
Trap Event	
Authentication Failure, Link Up/Down, Cold Start, Warm Start	Check the box to enable the function. **Authentication Failure** - VigorSwitch will reboot when encountering authentication failure (including community not match or user password not match). **Link Up/Down** - VigorSwitch will reboot while encountering port link up or down trap. **Cold Start** - VigorSwitch will reboot while encountering user trap. **Warm Start** - VigorSwitch will reboot while encountering power down trap.
Notification	
+Add Server	Click it to create a new notification server profile.
Server	Displays IPv4/IPv6/Hostname of the SNMP trap recipients.
Server Port	Displays the UDP port number for the recipient's server.
Version	Displays the notification SNMP version.
Notification Type	Displays the notification type (Trap or Inform).
Timeout	Displays the number of SNMP informs timeout.
Retry	Displays the number of SNMP informs retry count.

Community/User	Displays the community profile.
Security Level	Displays the security level for SNMP notification packet.
Option	- Click to modify the setting page of the server profile. - Remove the selected entry.

To modify an existing server profile, click the link of of the one to be changed.

To add a user profile, click the "**+ Add Server**" to open the edit page.



Available settings are explained as follows:

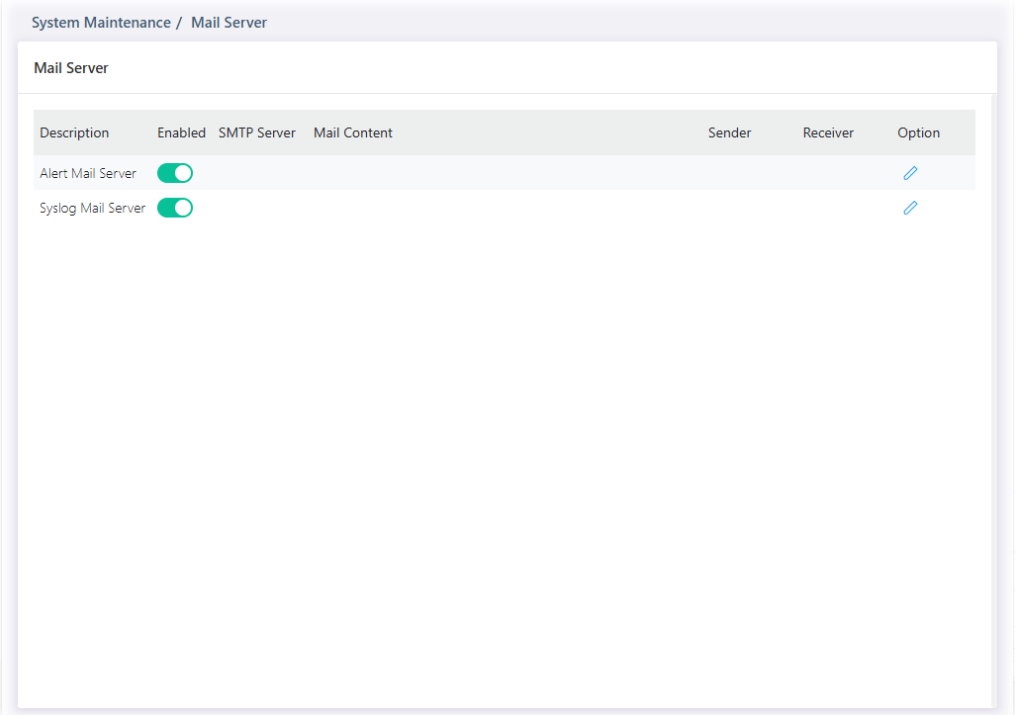
Item	Description
Add Notification Server	
Server Type	Choose IPv4/IPv6/Hostname to specify IP address or the hostname of the SNMP trap recipients. • **Hostname** • **IPv4** • **IPv6**
Server Address	Specify SNMP notification version (SNMPv1/v2/v3).
Server Port	Specify a port number for the server.
SNMP Version	Specify SNMP notification version (SNMPv1/v2/v3).
Community	Select v2 or v3 as SNMP Version. Use the drop down list to choose one of the community profiles.
Notification Type	Displays the notification type. To specify Notification Type, select v2 or v3 as SNMP Version. • **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.
Timeout	Specify the SNMP informs timeout. It is available when **Inform** is selected as **Type**.
Retry	Specify the SNMP informs retry count. It is available when **Inform** is selected as Type.
User	It is available when v3 is selected as SNMP Version.
Security Level	It is available when v3 is selected as SNMP Version. 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.

After finishing this web page configuration, please click **OK** to save the settings.

VI-5 Mail Server

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

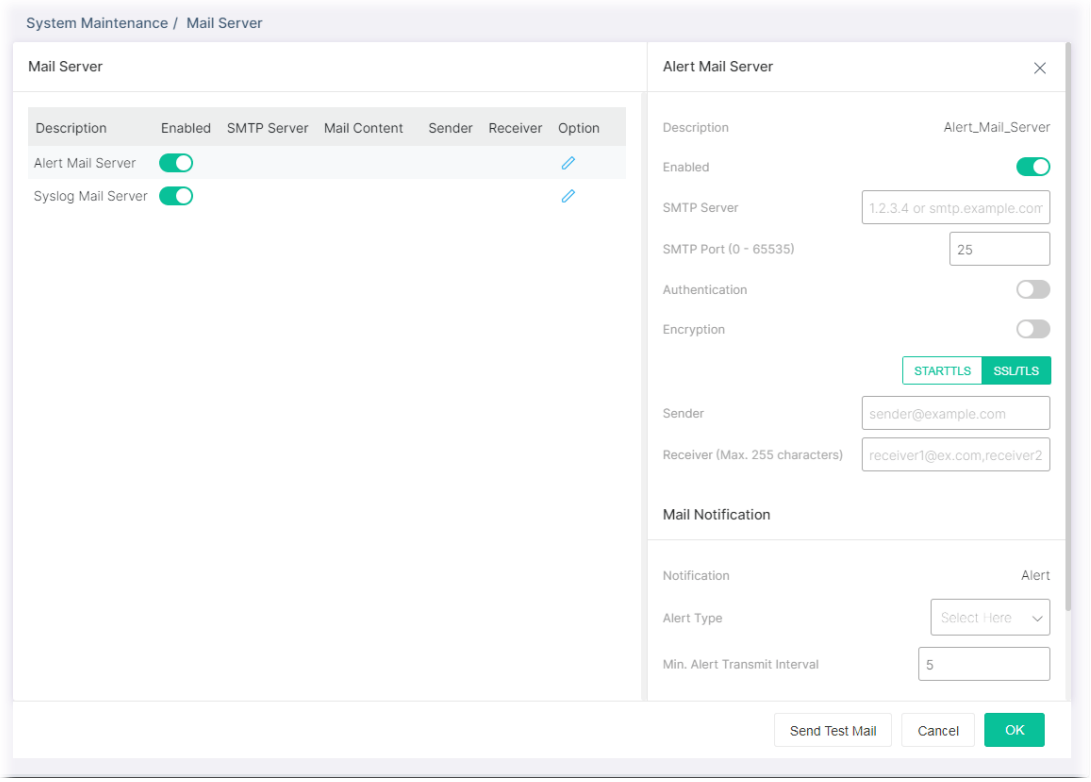


Available settings are explained as follows:

Item	Description
Mail Server	
Description	Displays the name of the mail server.
Enabled	Switch the toggle to enable / disable this function. - means "Enable". - means "Disable".
SMTP Server	Displays the IP address / host of the SMTP server.
Mail Content	Displays the condition(s) for VigorSwitch system to send a mail out.
Sender	Displays the email address sending the alert/syslog mail.
Receiver	Displays the email address receiving the alert/syslog mail.
Option	- Click to modify the setting page of the server profile.

Alert Mail Server

To modify the alert mail server profile, click the link of  of **Alert Mail Server** to be changed.



Available settings are explained as follows:

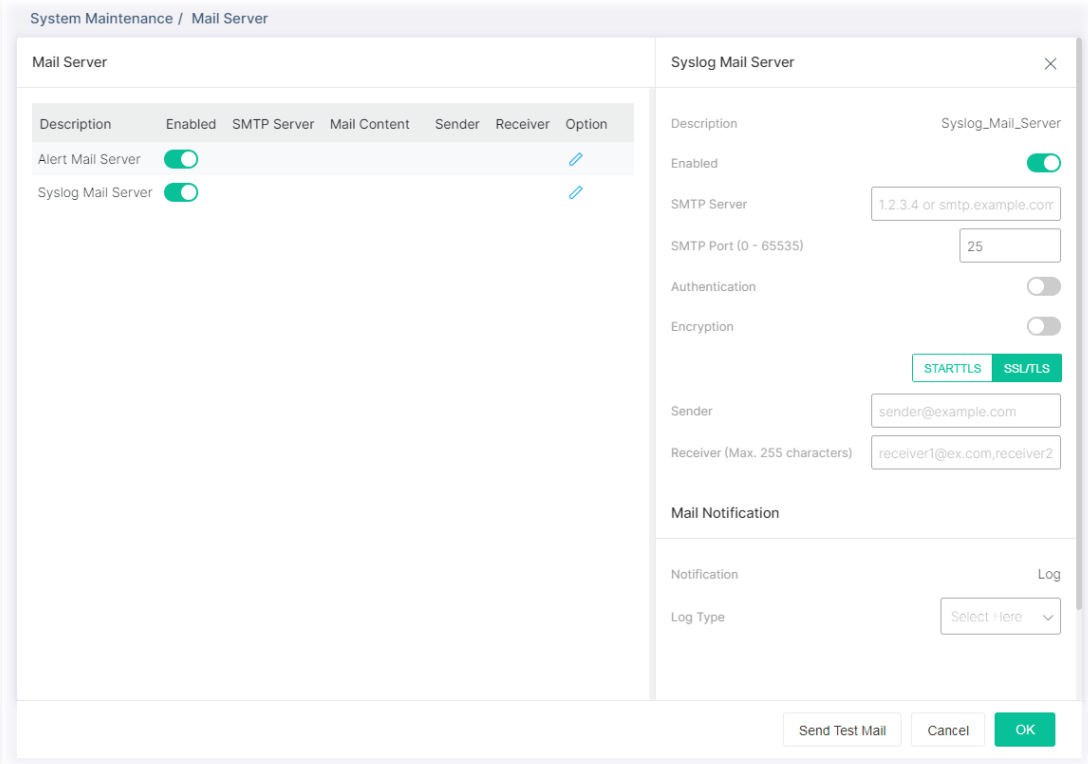
Item	Description
Alert Mail Server	
Description	Displays the name (Alert or Syslog) of the mail server.
Server Status	Switch the toggle to enable / disable the mail server.  - means “Enable”. - means “Disable”.
SMTP Server	Enter IP address or URL of the SMTP server.
SMTP Port	Enter the port number for the SMTP server.
Authentication	Switch the toggle to enable / disable this function. • **User Name** - Enter a user name for authentication. • **Password** - Enter a password for authentication.
Encryption	Switch the toggle to enable / disable this function. 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.
Sender	Enter the email address which will send the alert mail out.
Receiver	Enter the email address which will receive the alert mail.
Mail Notification	

Alert Type	Specify the condition(s) for VigorSwitch system to send an alert out. • Port Link Status • Port Link Speed • System Restarted • PoE Warning Status • IP Conflict • Hardware Monitor • Device Check • ONVIF Throughput Threshold
Min. Alert Transmit Interval	Set a time interval for VigorSwitch system to send an alert out from the specified sender.
Send Test Mail	After clicking this button, VigorSwitch system will send a test mail to the recipient.

After finishing this web page configuration, please click **OK** to save the settings.

Syslog Mail Server

To modify the Syslog mail server profile, click the link of  of **Syslog Mail Server** to be changed.



Available settings are explained as follows:

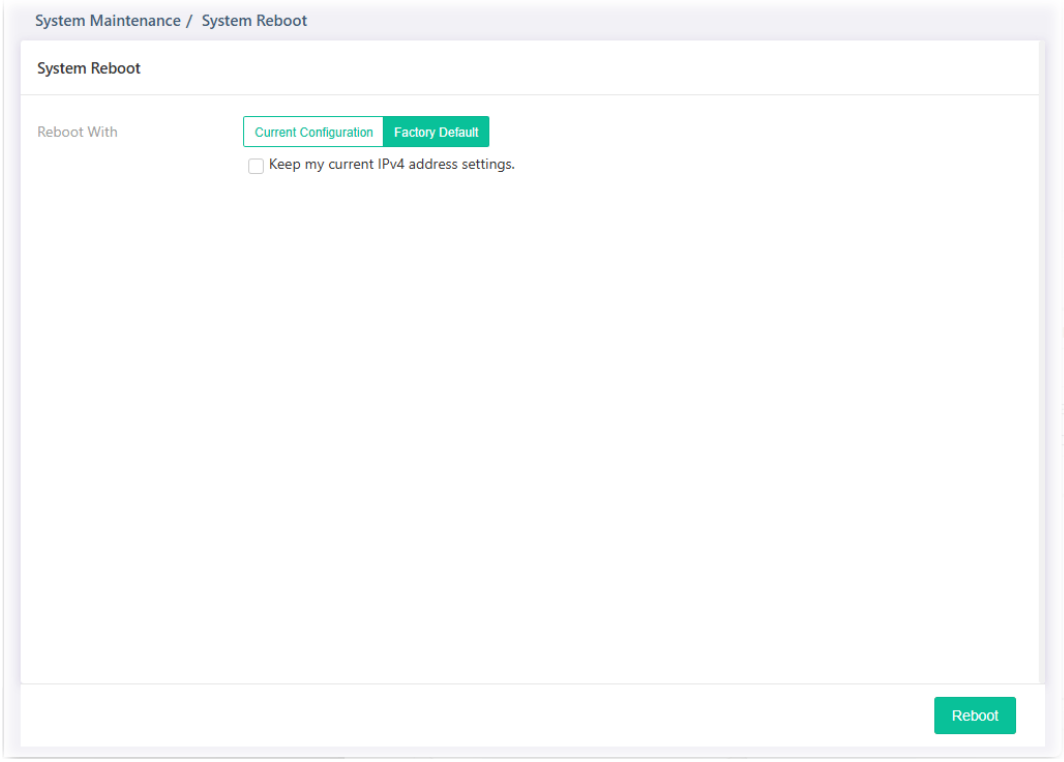
Item	Description
Alert Mail Server	
Description	Displays the name (Alert or Syslog) of the mail server.
Server Status	Switch the toggle to enable / disable this function.

	 - means “Enable”. - means “Disable”.
SMTP Server	Enter IP address or URL of the SMTP server.
SMTP Port	Enter the port number for the SMTP server.
Authentication	Switch the toggle to enable / disable this function. • User Name - Enter a user name for authentication. • Password - Enter a password for authentication.
Encryption	Switch the toggle to enable / disable this function. 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.
Sender	Enter the email address which will send the syslog mail out.
Receiver	Enter the email address which will receive the syslog mail.
Mail Notification	
Log Type	Vigor system will send the e-mail related to the selected feature(e.g., AAA, ACL) to the recipient.
Send Test Mail	After clicking this button, VigorSwitch system will send a test mail to the recipient.

After finishing this web page configuration, please click **OK** to save the settings.

VI-6 System Reboot

This page allows you to reboot VigorSwitch with current settings or return to factory default settings for VigorSwitch.



Available settings are explained as follows:

Item	Description
System Reboot	
Reboot With	**Current Configuration** - Use current configuration settings. **Factory Default** - Use the default configuration settings. ● **Keep my current IPv4 address settings**
Reboot	Click to reboot the device immediately.

This page is left blank.

Chapter VII Troubleshooting

VII-1 Backing to Factory Default Setting

Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the modem by software or hardware.

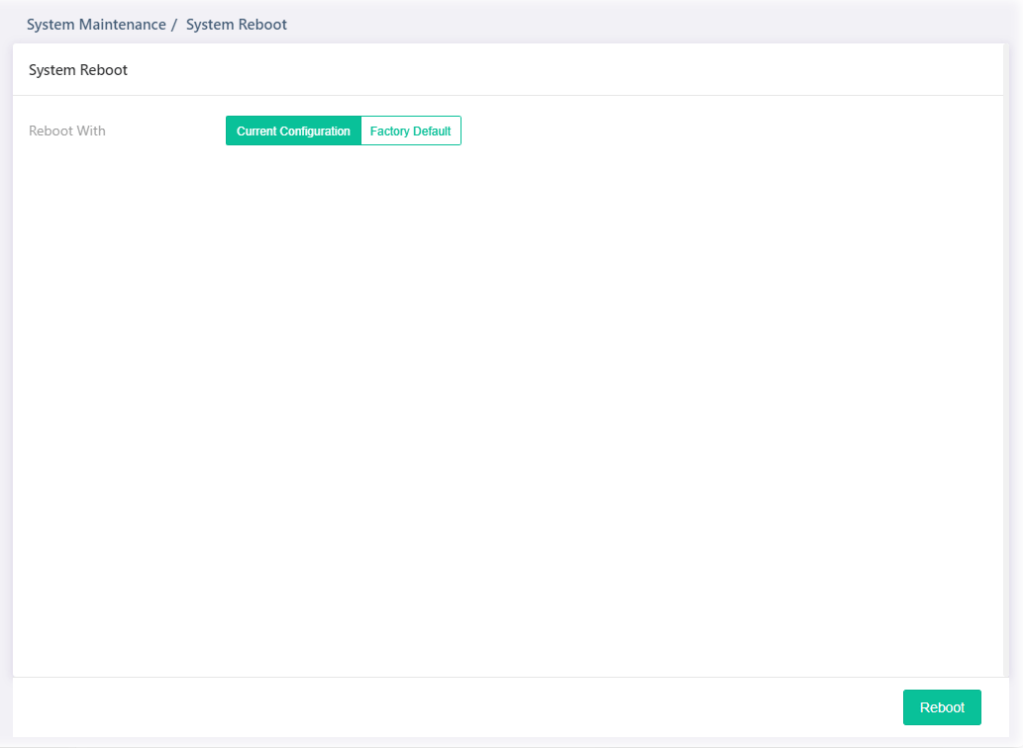
Warning:

After pressing **factory default setting**, you will loose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of factory default is null.

VII-1-1 Software Reset

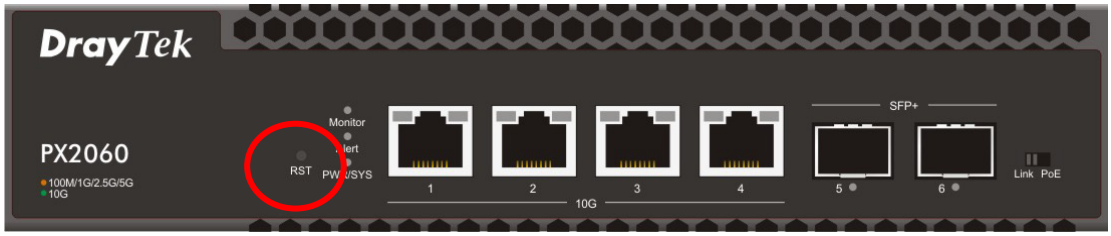
You can reset the modem to factory default via Web page.

Go to **System Maintenance** and choose **System Reboot** on the web page. The following screen will appear. Choose **Factory Default** and click **OK**. After few seconds, the modem will return all the settings to the factory settings.



VII-1-2 Hardware Reset

While the modem is running, press the **RST** button and hold for more than 5 seconds. When you see the **ACT** LED blinks rapidly, please release the button. Then, the modem will restart with the default configuration.



After restore the factory default setting, you can configure the settings for the modem again to fit your personal request.

VII-2 Contacting DrayTek

If the modem still cannot work correctly after trying many efforts, please contact your dealer for further help right away. For any questions, please feel free to send e-mail to support@draytek.com.