DrayTek

# VigorSwitch PQ2200xb

## L2+ Managed Switch

# *User's Guide*

**V1.1**

# VigorSwitch PQ2200xb

L2+ Managed Switch

User's Guide

Version: 1.1

Firmware Version: V2.8.1

Date: February 17, 2023

# Intellectual Property Rights (IPR) Information

**Copyrights**

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

**Trademarks**

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows 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 +5 to +45 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 ..... IX**

I-1 Introduction ..... 1

I-1-1 Key Features ..... 1
I-1-2 LED Indicators and Connectors ..... 2

I-2 Installation ..... 4

I-2-1 Network Connection ..... 4
I-2-2 Rack-Mounted Installation ..... 5
I-2-3 Typical Applications ..... 5
I-2-4 Configuring the Management Agent of Switch ..... 9
I-2-5 Managing VigorSwitch PQ2200xb through Ethernet Port ..... 9
I-2-6 IP Address Assignment ..... 10

I-3 Accessing Web Page of VigorSwitch ..... 14

I-4 Dashboard ..... 16

**Chapter II Configuration ..... 17**

II-1 General Setup ..... 18

II-1-1 PoE ..... 18
II-1-2 Mirroring ..... 19
II-1-3 Link Aggregation ..... 20
II-1-4 Multicast ..... 23
II-1-5 STP ..... 24
II-1-6 QoS ..... 26
II-1-7 Jumbo Frame ..... 29
II-1-8 LLDP ..... 30

II-2 VLAN Setup ..... 31

II-2-1 Existion VLAN ..... 31
II-2-1-1 Default VLAN ..... 31
II-2-1-2 Voice VLAN ..... 32
II-2-1-3 Surveillance VLAN ..... 34
II-2-2 MAC VLAN Group ..... 36
II-2-2-1 MAC Group ..... 36
II-2-2-2 Protocol Group ..... 38
II-2-3 GVRP ..... 40

II-3 MAC Address Table ..... 41

II-4 L3 Network ..... 43

II-4-1 IP Network ..... 43
II-4-2 Bind IP to MAC ..... 45
II-4-2-1 MAC-IP Binding List ..... 45
II-4-2-2 DHCP Table ..... 46
II-4-3 VLAN Routing ..... 47

II-5 Port Setup ..... 50

II-5-1 General ..... 50
II-5-2 VLAN ..... 53
II-5-3 GVRP ..... 56
II-5-4 Multicast ..... 59
II-5-5 STP ..... 62
II-5-4 QoS ..... 65

II-6 Multicast ..... 68

II-6-1 IGMP Snooping ..... 68
II-6-1-1 IGMP Snooping ..... 68
II-6-1-2 VLAN Setting ..... 69

II-6-1-3 Group Table ..... 72
II-6-1-4 Filtering Profile ..... 73
II-6-2 MVR ..... 74
II-6-2-1 Port Setting ..... 76
II-6-2-2 Static Group ..... 77
II-6-3 MLD Snooping ..... 79
II-6-3-1 MLD Snooping ..... 80
II-6-3-2 VLAN Setting ..... 81
II-6-3-3 Group Table ..... 83
II-6-3-4 Filtering Profile ..... 84
II-6-4 MLD Snooping Statistics ..... 86
II-7 ONVIF Surveillance ..... 87
II-7-1 Topology ..... 87
II-7-2 Snapshot Stream ..... 91
II-7-3 Device Maintenance ..... 92
II-8 RADIUS/TACACS+ ..... 96
II-8-1 RADIUS ..... 96
II-8-2 TACACS+ ..... 98

**Chapter III Security ..... 101**

III-1 802.1x/MAC Authentication ..... 102
III-1-1 802.1x/MAC Authentication ..... 102
III-1-2 Local/MAC Account ..... 105
III-1-3 Authentication Hosts ..... 107
III-2 Access Control List ..... 108
III-2-1 Access Control List ..... 108
III-1-2 Apply to Port ..... 118
III-3 IP Source Guard ..... 120
III-4 Port Security ..... 122
III-5 Storm Control ..... 124
III-6 DoS ..... 126
III-6-1 Properties ..... 126
III-6-2 Port Setting ..... 128
III-7 Dynamic ARP Inspection ..... 129
III-7-1 Properties ..... 129
III-7-2 Statistics ..... 130
III-8 DHCP Snooping ..... 131
III-8-1 DHCP Snooping ..... 131
III-8-2 Option82 ..... 132
III-8-3 Statistics ..... 134
III-9 IP Conflict Prevention ..... 135
III-10 Loop Protection ..... 140
III-11 Port Recovery ..... 142

**Chapter IV Utilities ..... 145**

IV-1 Device Check ..... 146
IV-2 Cable Diagnostics ..... 148
IV-3 Ping Test ..... 149
IV-4 Fan Test ..... 150
IV-5 SFP Vendor Info ..... 151

IV-6 sFlow ..... 152

**Chapter V Monitoring ..... 155**

V-1 Log Center ..... 156

V-1-1 System Log Information ..... 156
V-1-2 System Log Settings ..... 157
V-1-2-1 Local ..... 157
V-1-2-2 Remote ..... 159

V-2 Bandwidth Utilization ..... 161

V-3 DHCP Table ..... 162

V-4 Routing Table ..... 163

V-5 CLI Sessions ..... 164

V-6 PoE Status ..... 165

V-7 LLDP Status ..... 166

V-7-1 General Statistics ..... 166
V-7-2 LLDP Device ..... 167
V-7-2-1 Local ..... 167
V-7-2-2 Remote ..... 168
V-7-3 LLDP Overloading ..... 169

V-8 GVRP Statistics ..... 170

V-9 MLD Snooping Statistics ..... 171

V-10 STP Statistics ..... 172

V-11 Dynamic ARP Statistics ..... 173

V-12 DHCP Snooping ..... 174

V-13 Port Statistics ..... 175

**Chapter VI System Maintenance ..... 177**

VI-1 General ..... 178

VI-1-1 Device Info ..... 178
VI-1-2 Time & Schedule ..... 179
VI-1-3 Configuration ..... 182
VI-1-4 Firmware ..... 183

VI-2 Access Management ..... 184

VI-2-1 LAN Access ..... 184
VI-2-2 Management Authentication & Profile ..... 186
VI-2-3 TR-069 ..... 189
VI-2-4 OpenVPN ..... 191
VI-2-5 Webhook ..... 192
VI-2-6 Account & Password ..... 193

VI-3 LLDP ..... 195

VI-3-1 LLDP Port Setting ..... 195
VI-3-2 LLDP-MED Setting ..... 197
VI-3-3 LLDP Statistics ..... 200

VI-4 SNMP ..... 201

VI-4-1 VIew ..... 201
VI-4-2 Group ..... 204
VI-4-3 Community ..... 206
VI-4-4 User ..... 208
VI-4-5 Engine ID ..... 210
VI-4-6 Trap Notification ..... 212

VI-5 Mail Server ..... 215

VI-6 System Reboot ..... 219

**Chapter VII Troubleshooting ..... 221**

VII-1 Backing to Factory Default Setting ..... 222

VII-1-1 Software Reset ..... 222
VII-1-2 Hardware Reset ..... 223

VII-2 Contacting DrayTek ..... 224

**Appendix Telnet Commands ..... 225**

A-1 Accessing Telnet of Vigor Switch ..... 226

A-2 Available Commands ..... 228

A-2-1 Clear Configuration ..... 228
A-2-2 Clock Configuration ..... 237
A-2-3 Configure Configuration ..... 237
A-2-4 Copy Configuration ..... 340
A-2-5 Delete Configuration ..... 341
A-2-6 Disable Configuration ..... 341
A-2-7 End Configuration ..... 342
A-2-8 Exit Configuration ..... 342
A-2-9 Hardware-Monitor Configuration ..... 342
A-2-10 Ping Configuration ..... 343
A-2-11 Reboot Configuration ..... 343
A-2-12 Renew Configuration ..... 343
A-2-13 Restore-defaults Configuration ..... 344
A-2-14 Save Configuration ..... 344
A-2-15 Show Configuration ..... 344
A-2-16 SSL Configuration ..... 345
A-2-17 Terminal Configuration ..... 346
A-2-18 Traceroute Configuration ..... 346
A-2-19 UDLD Configuration ..... 347

# 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.

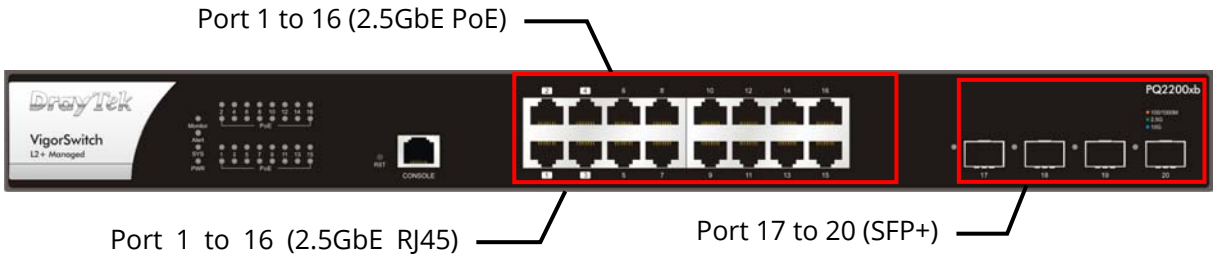
### Port Trunking

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 | Blinking (Green) | The power is over (>) 80% watts PoE power budget. |
| | Off | The power is under (<) 80% watts PoE power budget. |
| SYS | On (Green) | The switch finishes system booting and the system is ready. |
| | Blinking (Green) | The switch is powered on and starts system booting. |
| | Off | The power is off or the system is not ready / malfunctioning. |
| PWR | On (Green) | The device is powered on and running normally. |
| | Off | The device is not ready or is failed. |
| Port 1 ~ 16 (PoE) | On (Green) | The port is supplied with PoE power. |
| | Off | No PoE power is supplied on the port. |
| Port 1 ~ 16 (2.5GbE RJ45) | On (Green) | The device is connected with 2500Mbps. |
| | On (Amber) | The device is connected with 10/100/1000Mbps. |
| | Blinking | The system is sending or receiving data through the port. |
| | Off | The port is disconnected or the link is failed. |
| Port 17 ~ 20 (SFP+) | On (Green) | The device is connected with 1000Mbps. |
| | On (Blue) | 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 |
|---|---|
| Port 1 ~ 16 (2.5GbE RJ45) | Used for Ethernet connection (10/100/1000/2500Mbps).<br>For VigorSwitch PQ2200xb, PoE supports:<br>Port 1 ~ 4 : 802.3af/at/bt, up to 90W.<br>Port 5 ~ 16: 802.3af/at, up to 30W.<br>See the following note for detail. |
| Port 17 ~ 20 (SFP+) | Port 17 to Port 20 are used for fiber connection. |
| Console | Used to perform telnet command control. |

| | |
|---|---|
| | Power inlet for AC input (100~240V/AC, 50/60Hz). |

**Note**

The following limitation is suitable for VigorSwitch PQ2200xb
Power Output --

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

PoE Power Budget –-

- 400 Watts (Max)

# I-2 Installation

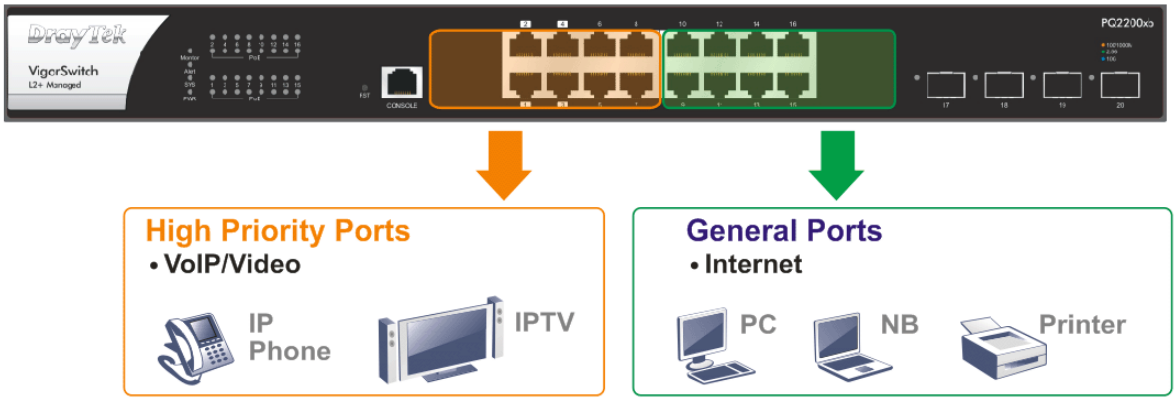
Before starting to configure the switch, you have to connect your devices correctly.

**Note:**

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

## I-2-1 Network Connection

- Use a Cat. 5e twisted-pair cable to connect a PoE device to the port (1~24) of this switch.
- 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.



## I-2-2 Rack-Mounted Installation

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

1. Attach the brackets to the chassis of a 19-inch rack. The second bracket attaches the other side of the chassis as above procedure.
2. After the bracket installation, the VigorSwitch's chassis can be installed in a rack by using four screws for each side of the rack.

## 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:

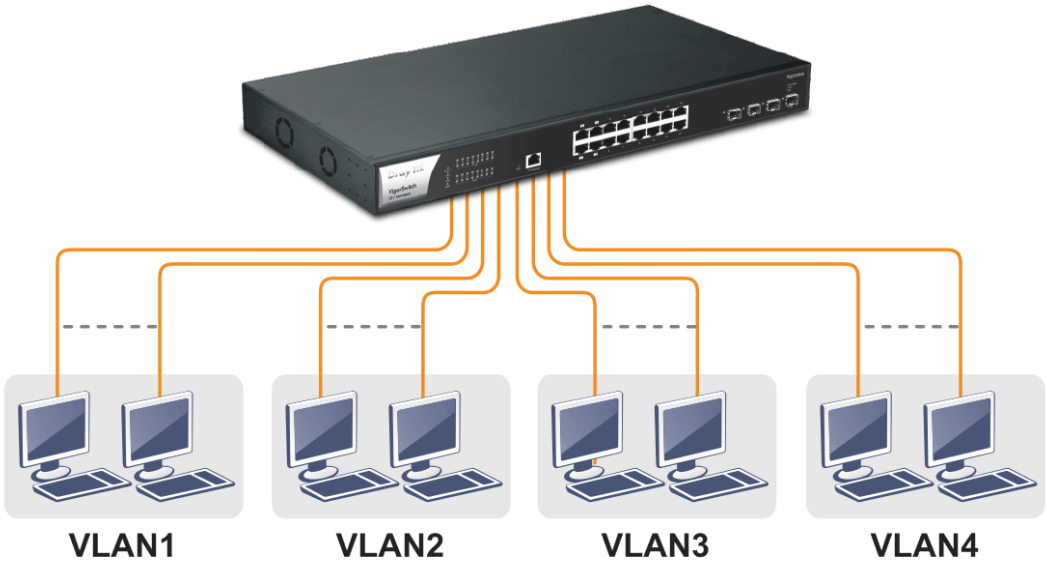
**Case 1: All switch ports are in the same local area network.**

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.

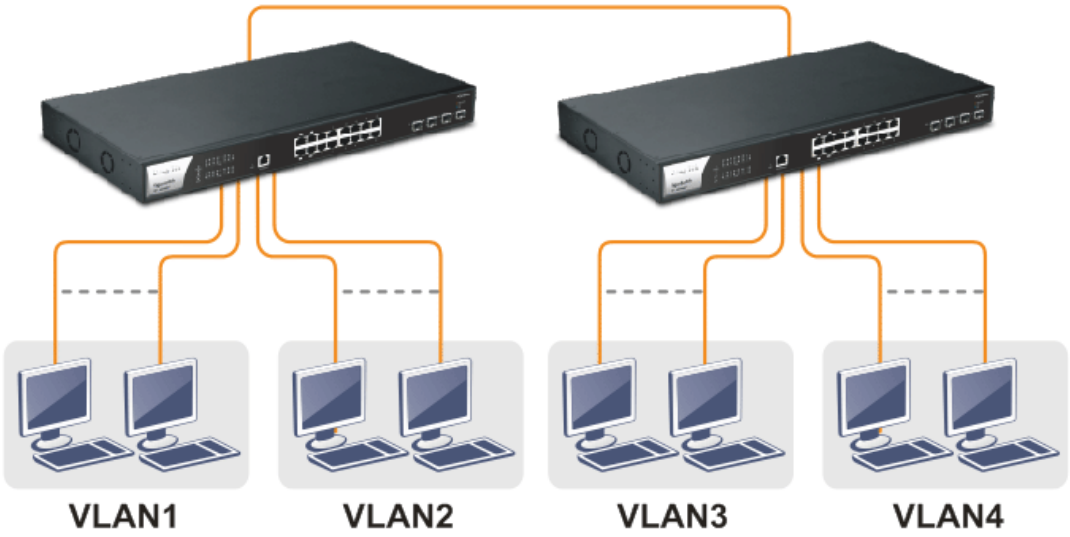
Here VLAN area is defined by what VLAN you are using. The switch supports both port-based VLAN and tag-based VLAN. They are different in practical deployment, especially in physical location. The following diagram shows how it works and what the difference they are.

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



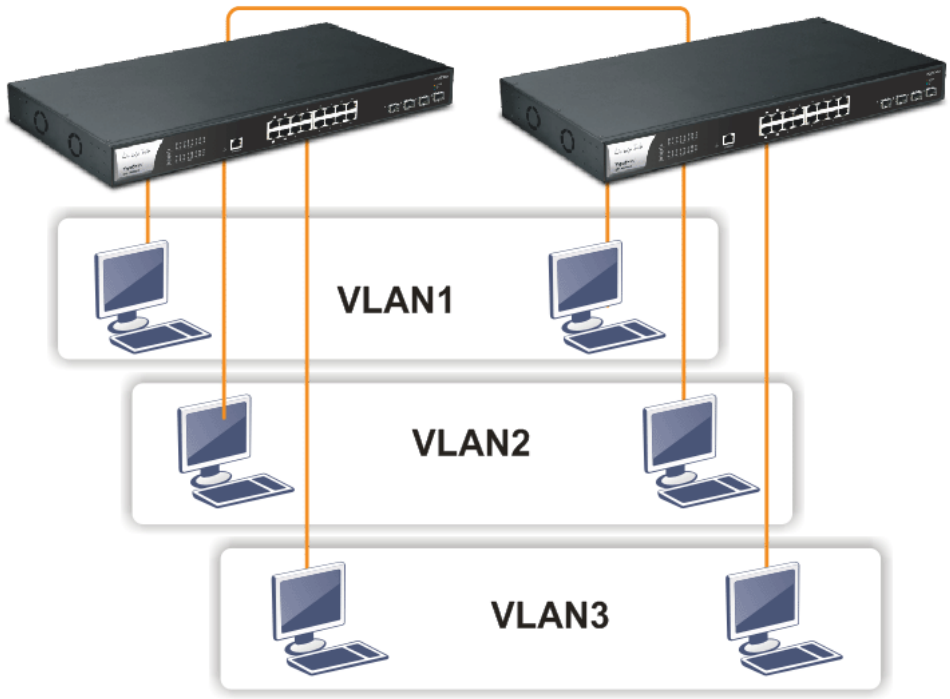

- The same VLAN members could not be in different switches.
- Every VLAN members could not access VLAN members each other.
- The switch manager has to assign different names for each VLAN groups at one switch.

**Case 3: Port-based VLAN - 2**




- VLAN1 members could not access VLAN2, VLAN3 and VLAN4 members.
- VLAN2 members could not access VLAN1 and VLAN3 members, but they could access VLAN4 members.
- VLAN3 members could not access VLAN1, VLAN2 and VLAN4.
- VLAN4 members could not access VLAN1 and VLAN3 members, but they could access VLAN2 members.

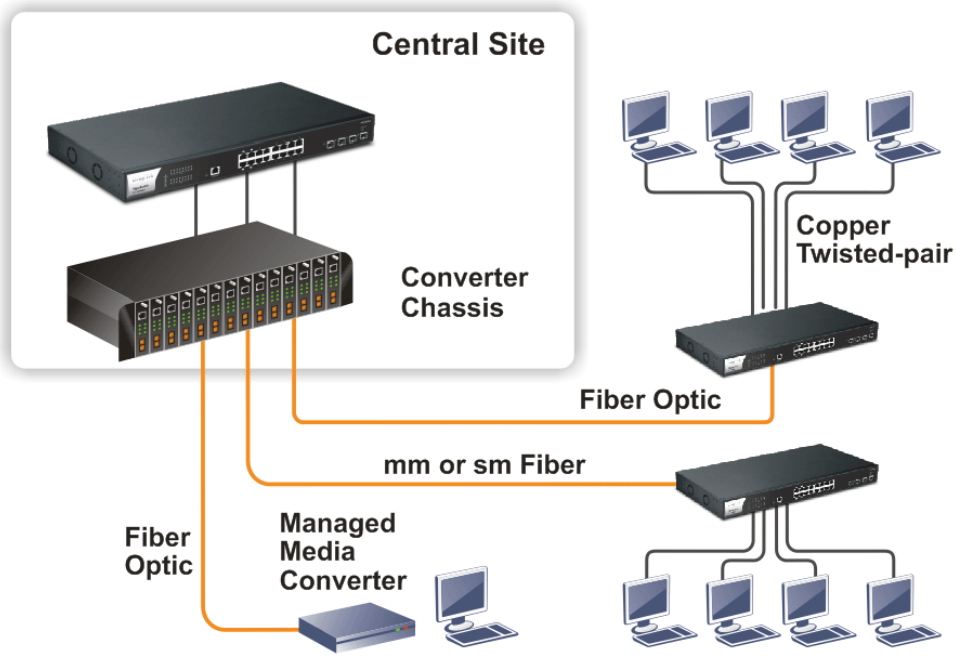
**Case 4: The same VLAN members can be at different switches with the same VID**



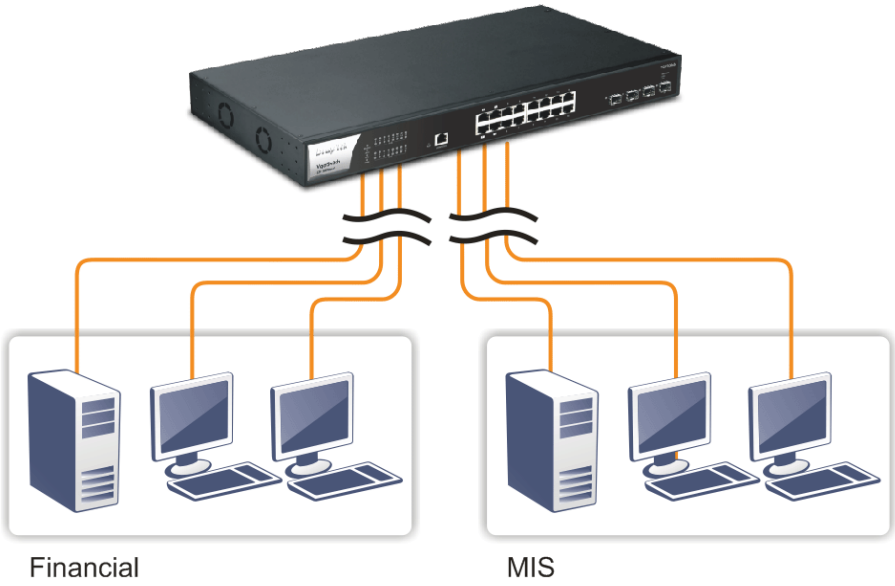

**Case 5: Desktop Installation**

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

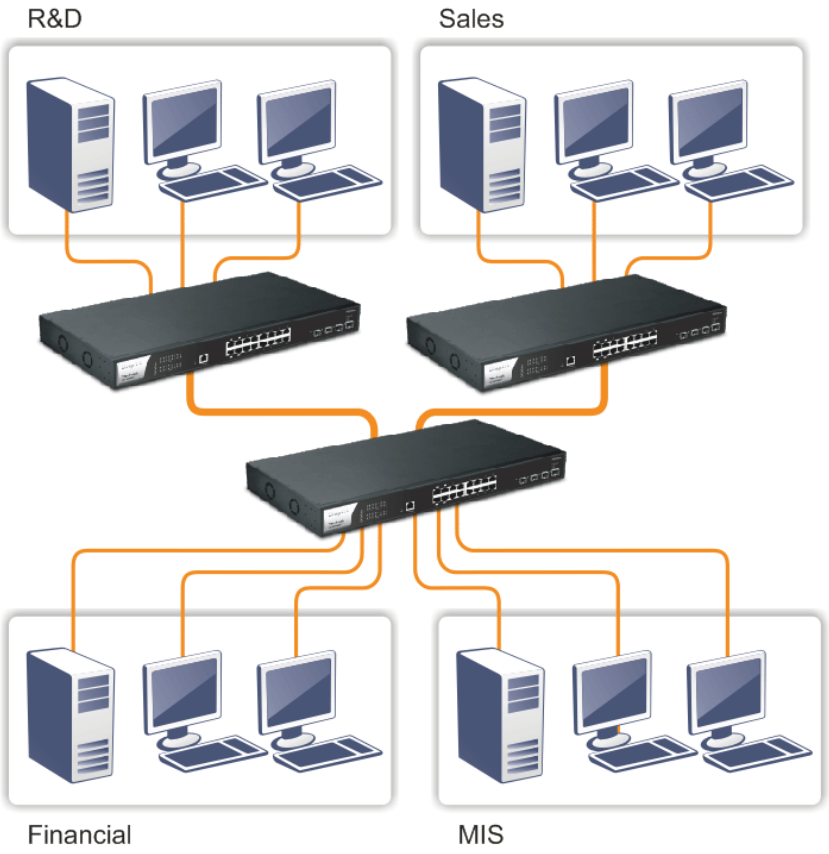
**Case 6: Central Site/Remote site application is used in carrier or ISP**



**Case 7: Peer-to-peer application is used in two remote offices**




**Case 8: Office network**

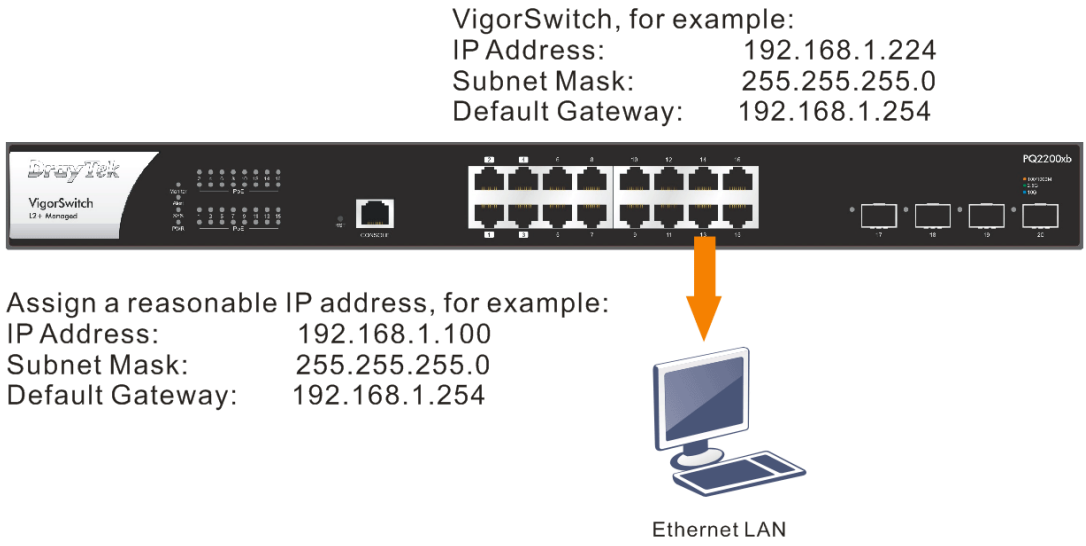


## I-2-4 Configuring the Management Agent of Switch

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

Configuring the Management Agent of VigorSwitch PQ2200XBthrough the Ethernet Port.

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




## I-2-5 Managing VigorSwitch PQ2200xb 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.

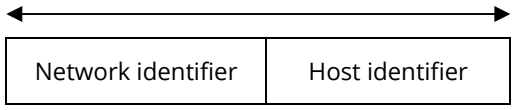
# I-2-6 IP Address Assignment

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

**IP address:**

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

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

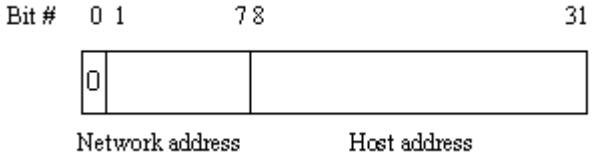



32 bits

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.

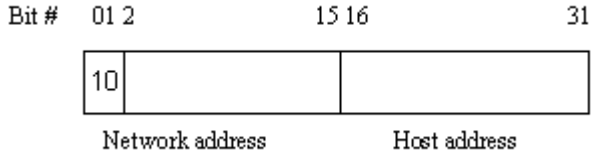
**Class A:**

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.



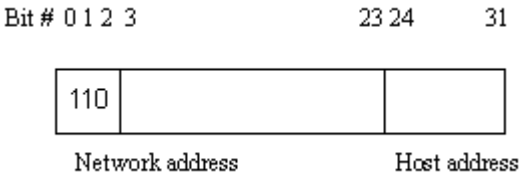

**Class B:**

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 |

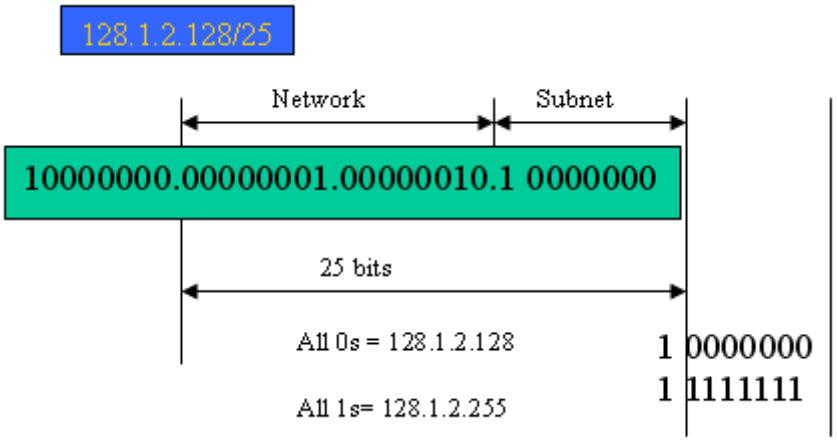
Please refer to RFC 1597 and RFC 1466 for more information.

**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.

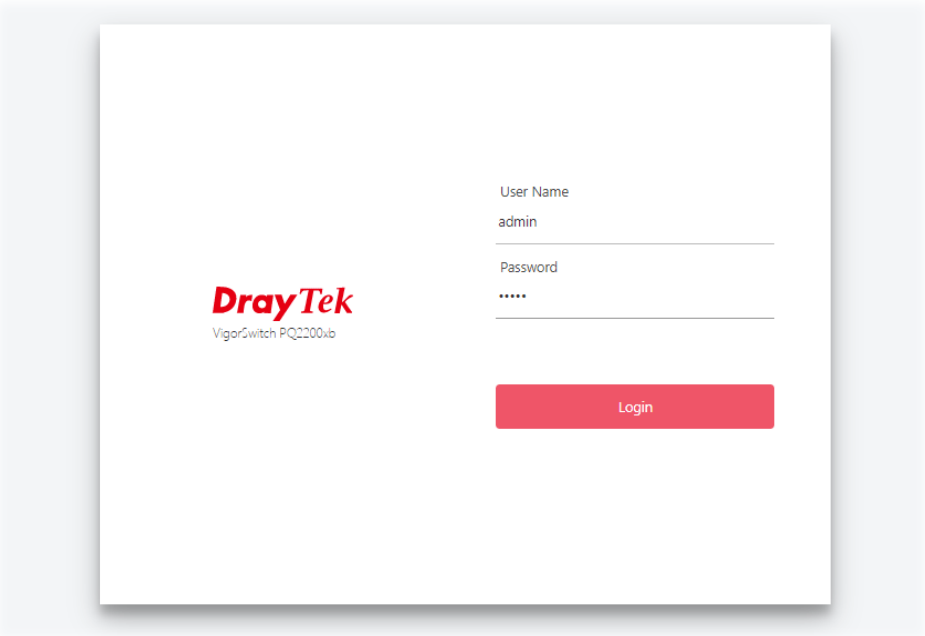
- First, IP Address: as shown above, enter "**192.168.1.224**", for instance. For sure, an IP address such as 192.168.1.x must be set on your PC.
- Second, Subnet Mask: as shown above, enter "255.255.255.0". Choose a subnet mask suitable for your network.

**Note:**

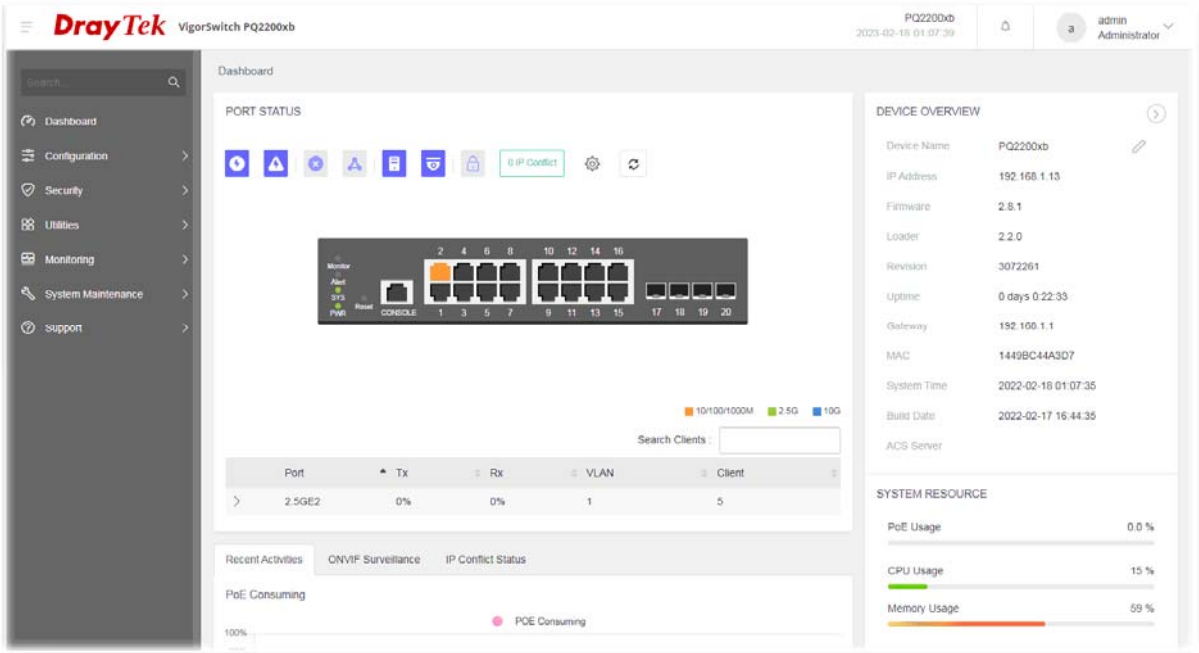
The DHCP Setting is enabled in default. Therefore, if a DHCP server presented on network connected to the switch, check before accessing your switch is essential.

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

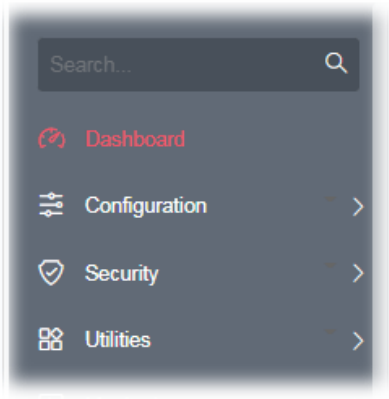


**Info:**

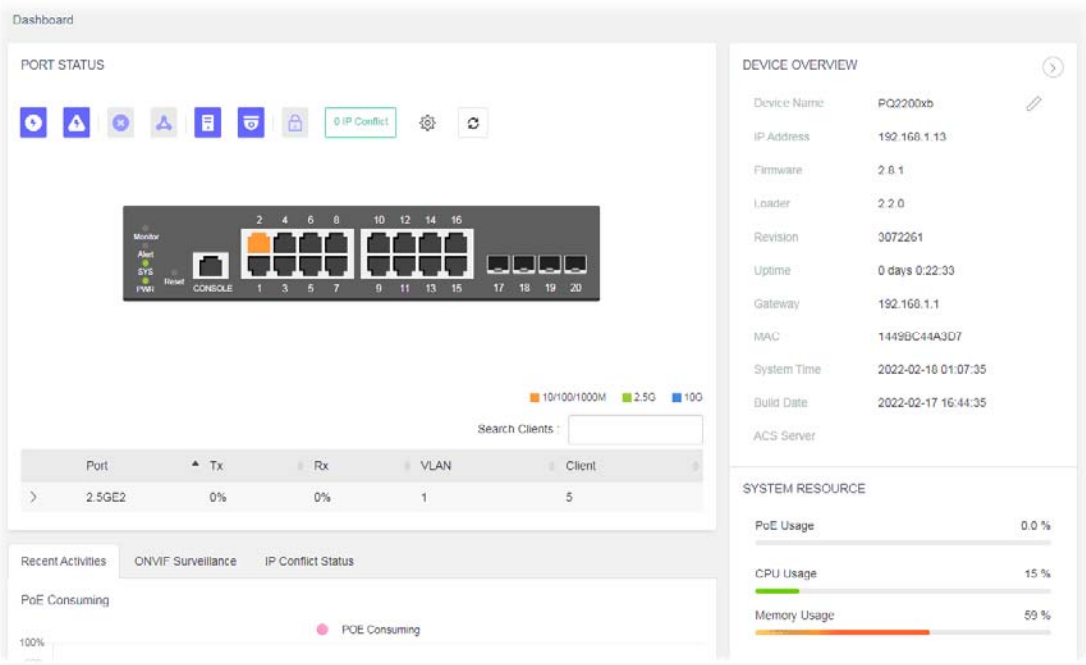
The DHCP Setting is enabled in default. Therefore, if a DHCP server presented on network connected to VigorSwitch, checking before accessing VigorSwitch is essential.

# 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:

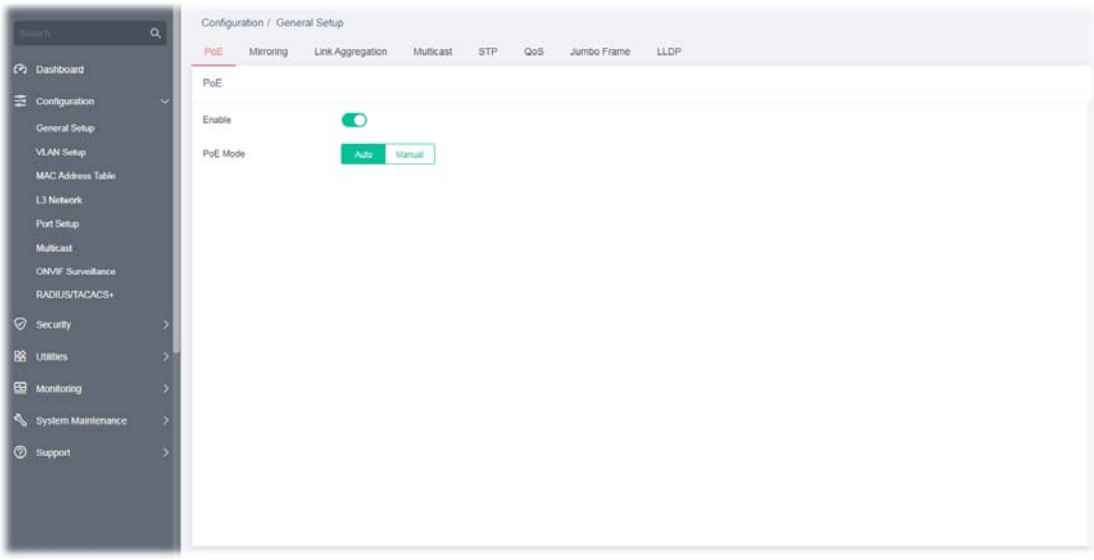


# Chapter II Configuration

# 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.



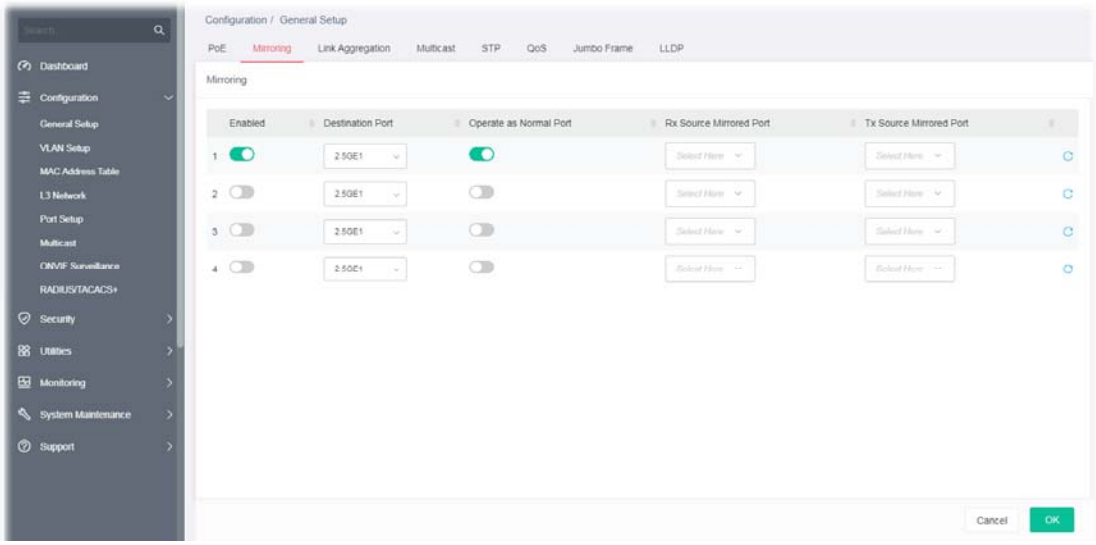

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable** | **Enable / Disable** – Click the toggle to enable / disable this function.<br> - means “Enable”.<br> - means “Disable”. |
| **PoE Mode** | **Auto** – Provides plug and play PoE function. PoE schedule and Power Limit are disabled in this mode.<br>**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.



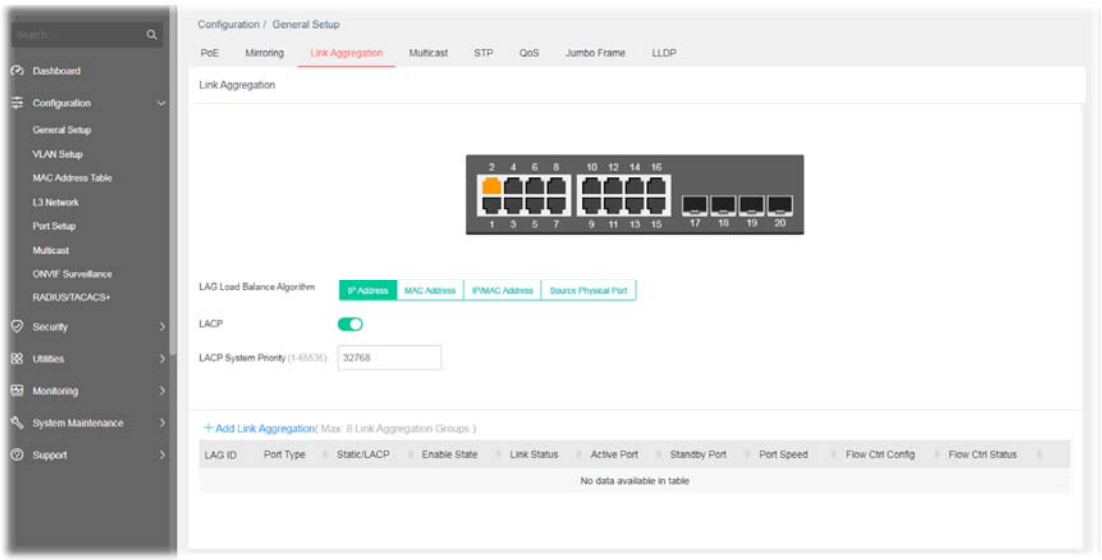

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enabled** | **Enable / Disable** – Click the toggle to enable / disable this function.<br>- means “Enable”.<br>- means “Disable”. |
| **Destination Port** | Specify the port where you wish to observe the mirrored packets. |
| **Operate as Normal Port** | **Enable / Disable** – Click the toggle to enable / disable this function.<br>- means “Enable”.<br>- 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. |
| | 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

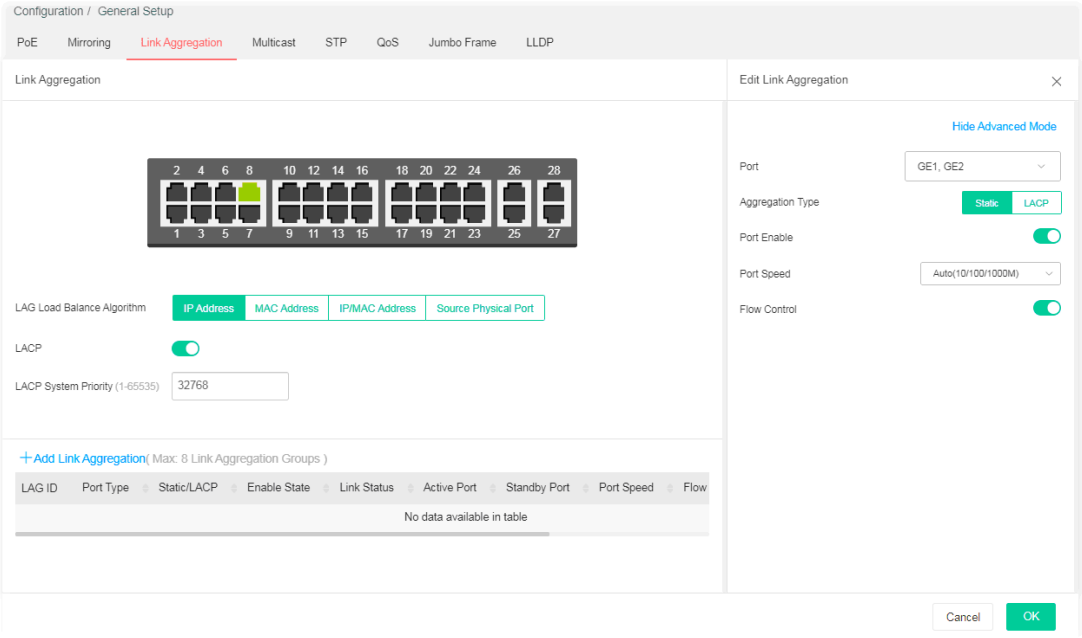
LAG means Link Aggregation Group which groups some physical ports together to make a single high-bandwidth data path. Thus it can implement traffic load sharing among the member ports in a group to enhance the connection reliability.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Link Aggregation** | |
| **LAG Load Balance Algorithm** | Select your Load balance algorithm.<br>**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.<br>**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.<br>**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.<br>**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** – Click the toggle to enable / disable this function.<br> - means “Enable”.<br> - 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.

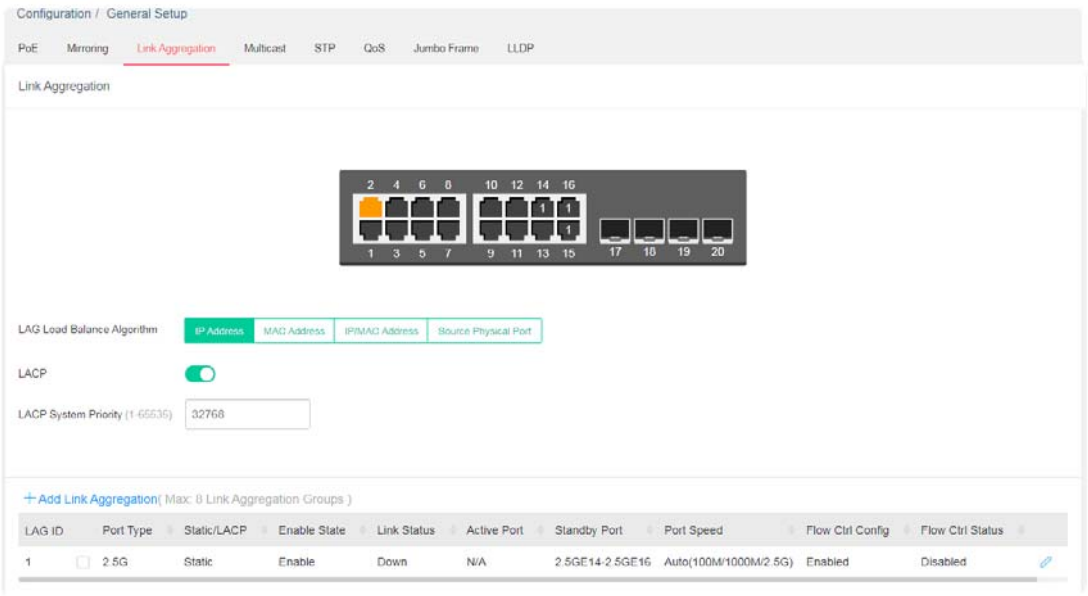



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Edit Link Aggregation** | |
| **Show/Hide Advanced Mode** | Click to switch different modes. |
| **Aggregation Type** | Specify the type for LAG.<br>**Static** - The static aggregated port sends packets over active member without detecting or negotiating with remote aggregated port.<br>**LACP** - The LACP aggregated ports place member into active only after negotiated with remote aggregated port for best reliability. |
| **Port Enable** | **Enable / Disable** – Click the toggle to enable / disable this function.<br>- means “Enable”.<br>- means “Disable”. |
| **Port Speed** | Port speed capabilities:<br>● **Auto(100/1000M/2.5G):** Auto speed with 2.5G ability only.<br>● **Auto(100M):** Auto speed with 100M ability only.<br>● **Auto(1000M):** Auto speed with 1000M ability only.<br>● **Auto(2.5G):** Auto speed with 2.5G ability.<br>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 |

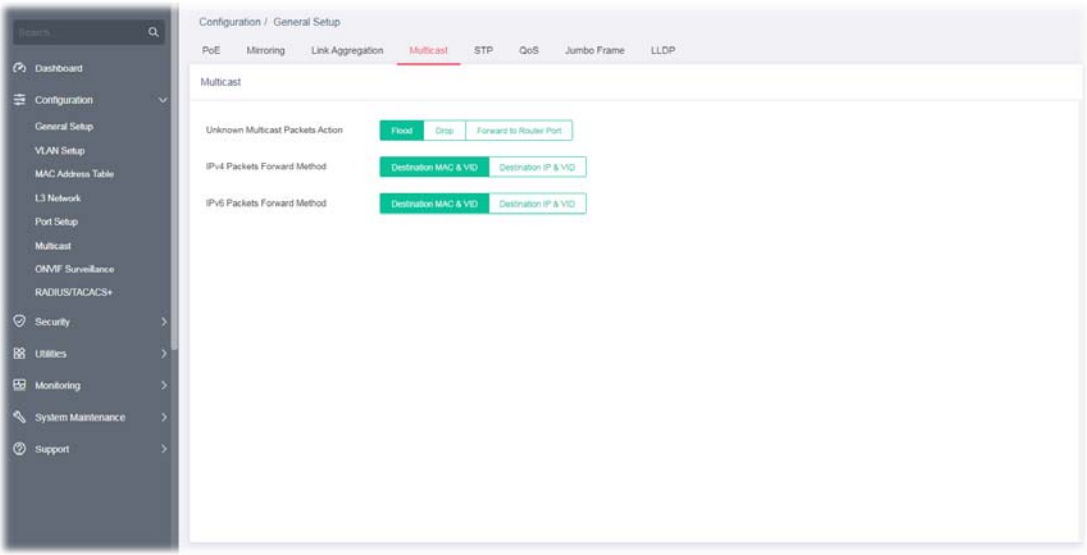
| | |
|---|---|
| | settings of the peer port are the same in order to connect.<br>For SFP fiber module, you might need to manually configure the speed to match fiber module speed. |
| **Flow Control** | **Enable / Disable** – Click the toggle to enable / disable this function.<br> - means “Enable”.<br> - means “Disable”.<br>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.



# 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.<br>**Drop** - Drop the unknown multicast data.<br>**Flood** - Flood the unknown multicast data.<br>**Forward to Router Port** - Forward the unknown multicast data to router port. |
| **IPv4/IPv6 Packets Forward Method** | Set the IPv4/IPv6 multicast forward method.<br>**Dst. MAC & VID** - Forward using destination multicast MAC address and VLAN IDs.<br>**Dst. IP & VID** - Forward using destination multicast IP address and VLAN ID. |

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

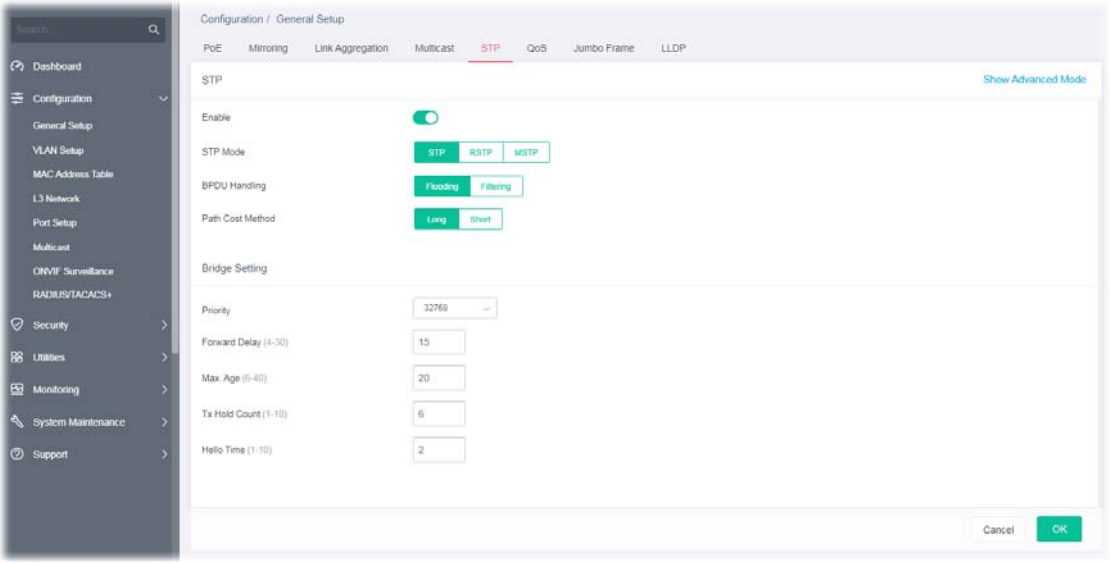
# II-1-5 STP

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.

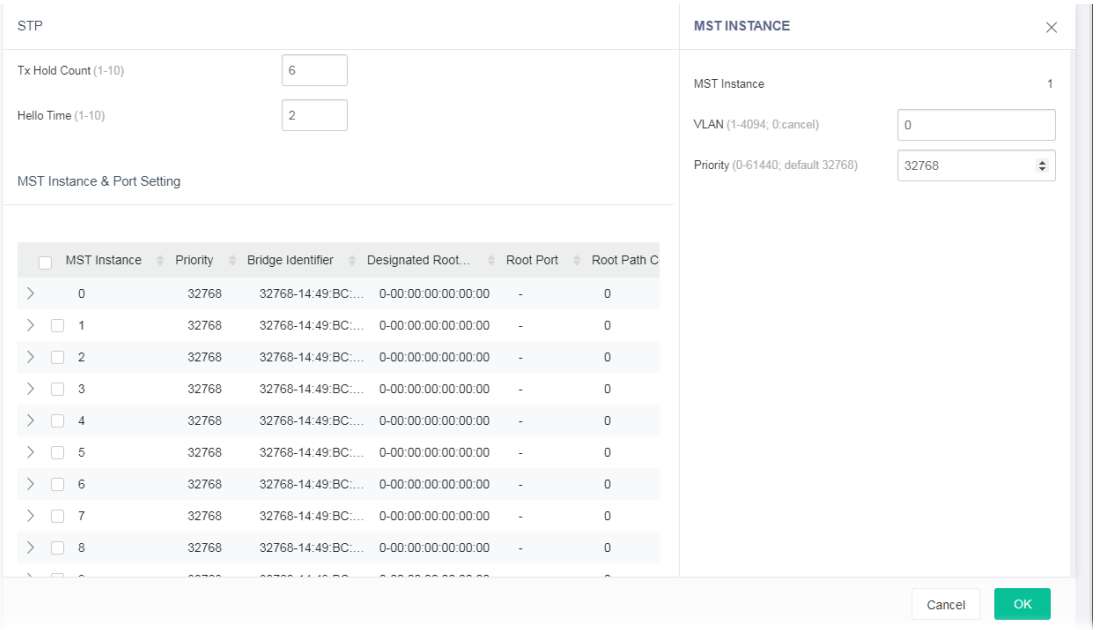



Available settings are explained as follows:

| Item | Description |
|---|---|
| **STP** | |
| **Enable** | **Enable / Disable** – Click the toggle to enable / disable this function.<br> - means “Enable”.<br> - means “Disable”. |
| **STP Mode** | Set the operating mode of Spanning Tree (STP).<br>**STP -** Enable the Spanning Tree (STP) operation.<br>**RSTP -** Enable the Rapid Spanning Tree (RSTP) operation. |
| **BPDU Handling** | Specify the BPDU forward method when the STP is disabled.<br>**Filtering -** Filter the BPDU when STP is disabled.<br>**Flooding -** Flood the BPDU when STP is disabled. |
| **Path Cost Method** | Specify the path cost method.<br>**Long -** Specifies that the default port path costs are within the range: 1~200,000,000.<br>**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. |
| **MST Instance & Port Setting** | It appears if the Show Advanced Mode link is selected.<br>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.<br>**Bridge Identifiter** – Displays the priority of MST instance number + MAC address of the switch.<br>**Designated Root Bridge** – Displays the Bridge Identifier of the root bridge.<br>**Root Port** – Displays the port toward the root.<br>**Root Path Cost** – Displays the path cost toward the root.<br>**Remaining Hop** – Displays the remaining hop count in BPDU.<br>**VLAN –**Displays the ID of the VLAN which should be associated with this MST instance.<br> - Click to modify the setting page of the selected VLAN.<br> - 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.

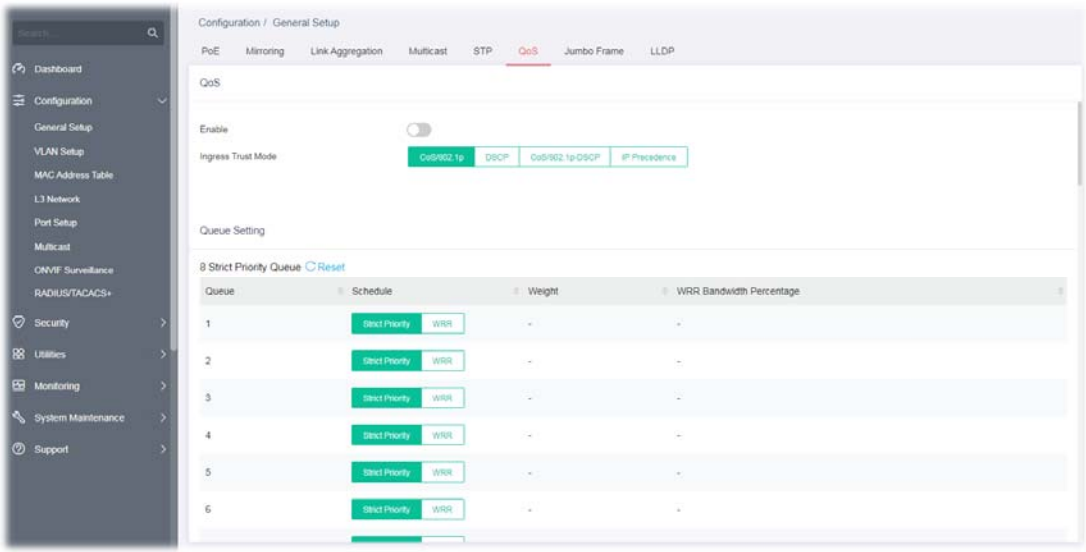
Actual effectiveness is based on how QoS is configured in previous QoS section. This page provides settings for user to configure mapping only.

**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**

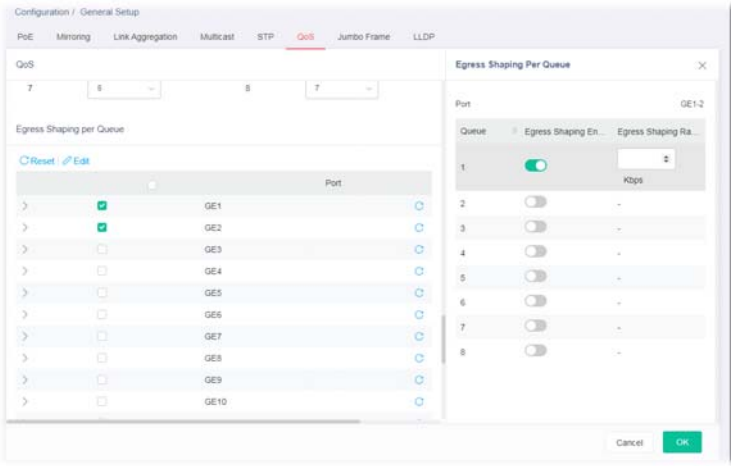
It allows users to configure the maximum egress bandwidth not only by the port but also by specific QoS queues. The configuration result for each port will be displayed on the table listed on the lower side of this web page.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **QoS** | |
| **Enable** | **Enable / Disable** – Click the toggle to enable / disable the function of QoS mode.<br> - means “Enable”.<br> - means “Disable”. |
| **Ingress Trust Mode** | Select the QoS operation mode.<br>**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.<br>**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. |

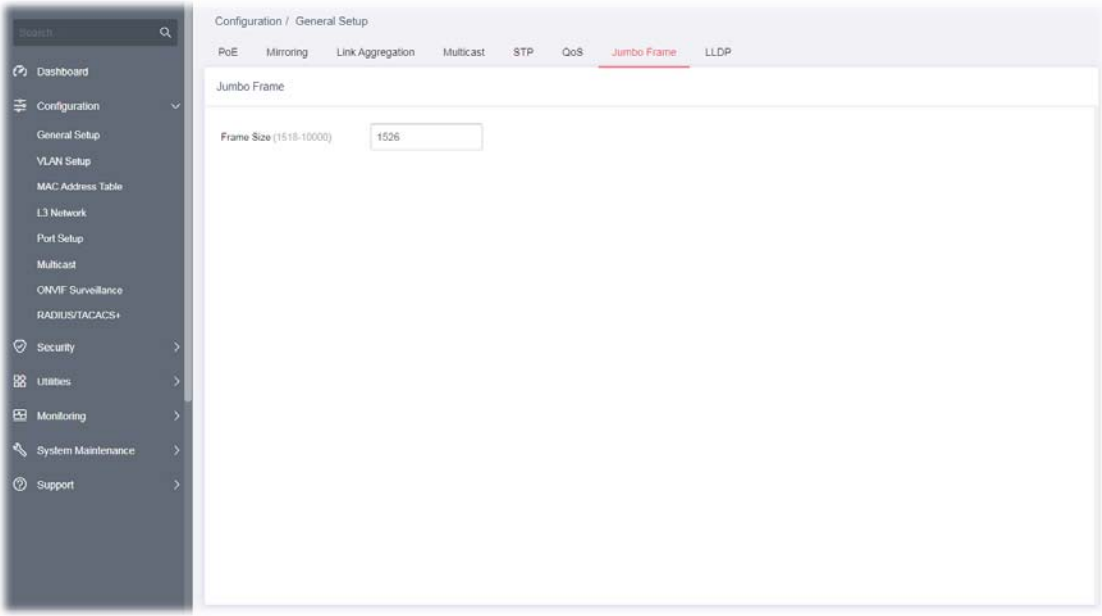
| | |
|---|---|
| | **CoS/802.1p-DSCP** – All IP traffic is mapped to queues based on the DSCP field in the IP header. If traffic is not IP but has VLAN tag, mapped to queues based on the CoS value in the VLAN tag.<br>**IP Precedence** - All IP traffic is mapped to queues based on the DSCP field in the 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.<br>**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.<br>**Reset** - Clear current settings and return to factory default settings. |
| **Queue Mapping to Class of Service (for Ingress Traffic)** | Defines the class of service value (0 to 7).<br>**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.<br>**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).<br>**Reset** - Clear current settings and return to factory default settings. |
| **IP Precedence Mapping** | |
| **IP Precedence Mapping to Queue (for Ingress Traffic)** | Defines the queue ID (level 1 to 8) for different IP Precedence values.<br>**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).<br>**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.<br>**Reset** - Clear all settings and return to factory default settings.<br>**Port** - Display the port (GE1 to GE16, 10GE1 to 10GE4) profiles.<br>- Clear settings of the selected port and return to factory default settings.<br>**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. |

| | |
|---|---|
| |  <br>• **Egress Shaping Enabled**- Switch the toggle to enable/disable the setting.<br>• **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.



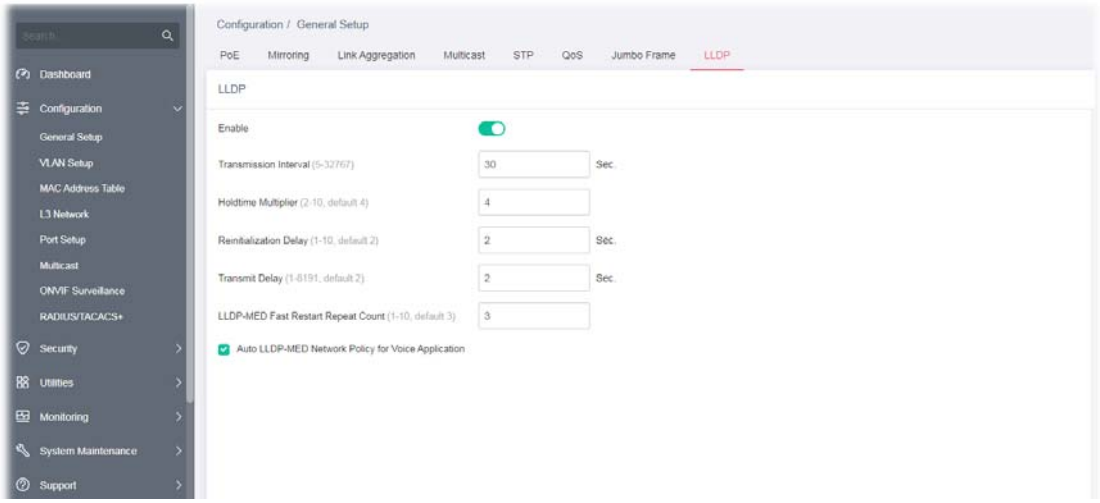

Available settings are explained as follows:

| 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** | |
| **Enable** | **Enable / Disable** – Click the toggle to enable / disable this function.<br>- means “Enable”.<br>- means “Disable”.<br>If LLDP function is disabled, specify an action for the LLDP PDU packets.<br>• **Filtering** - The LLDP packets will be filtered and deleted when LLDP is disabled.<br>• **Bridging** - The LLDP packets will be bridging when LLDP is disabled.<br>• **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 Repeat Count** | Select the number of LLDP packets that will be sent during LLDP-MED Fast Start period.<br>The default is 3. Available range is from 1 to 10. |
| **Auto LLDP-MED Network Policy for Voice Application** | The default value is Enable. |

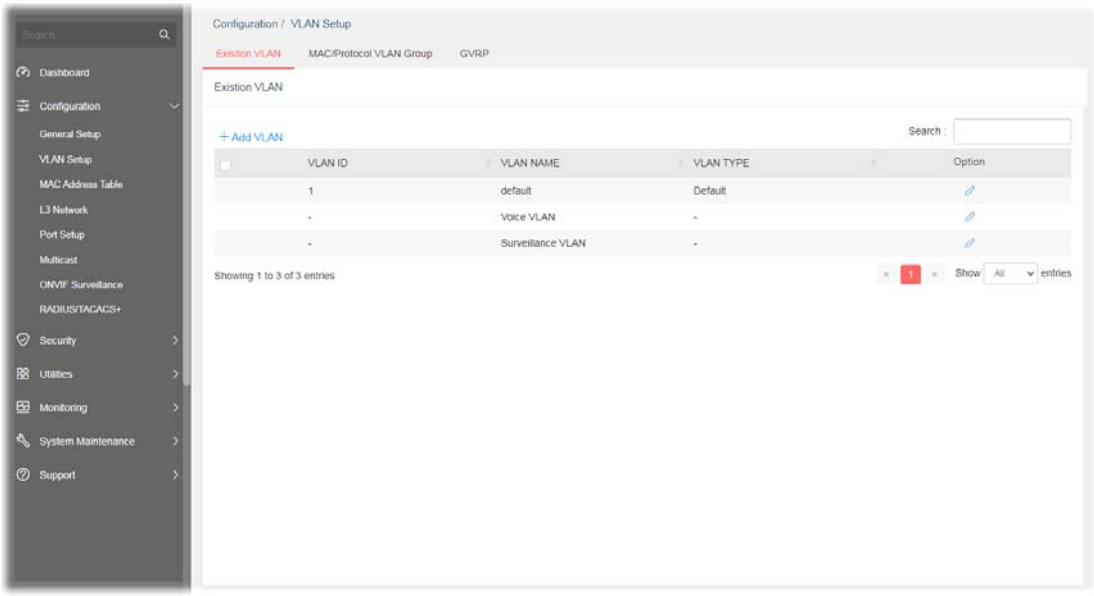
After finishing this web page configuration, please click **OK** to save the settings.

# 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

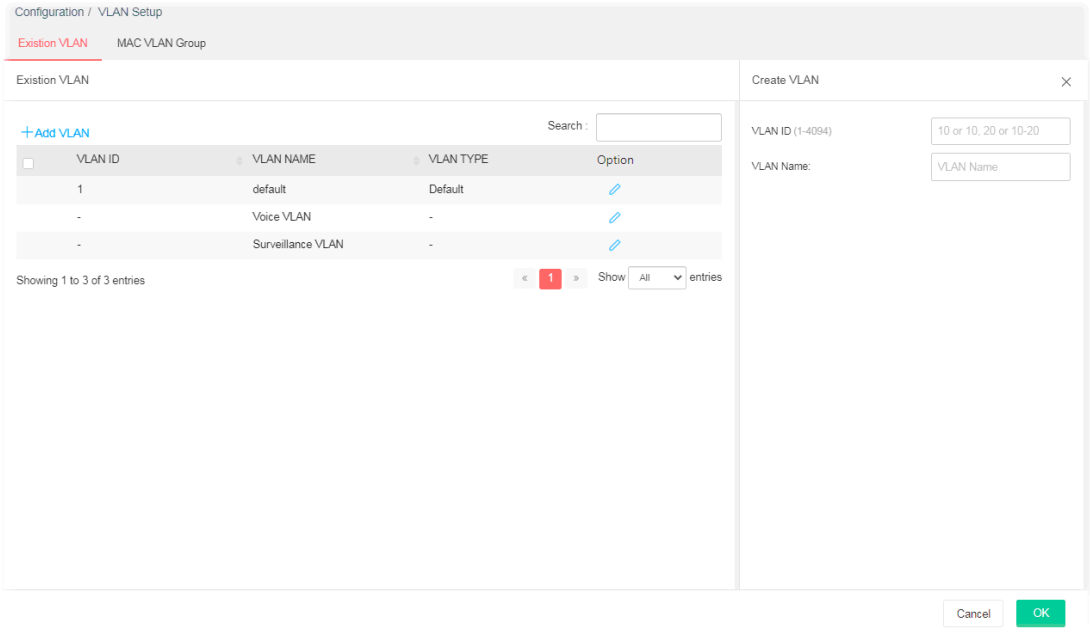
### II-2-1-1 Default VLAN




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.



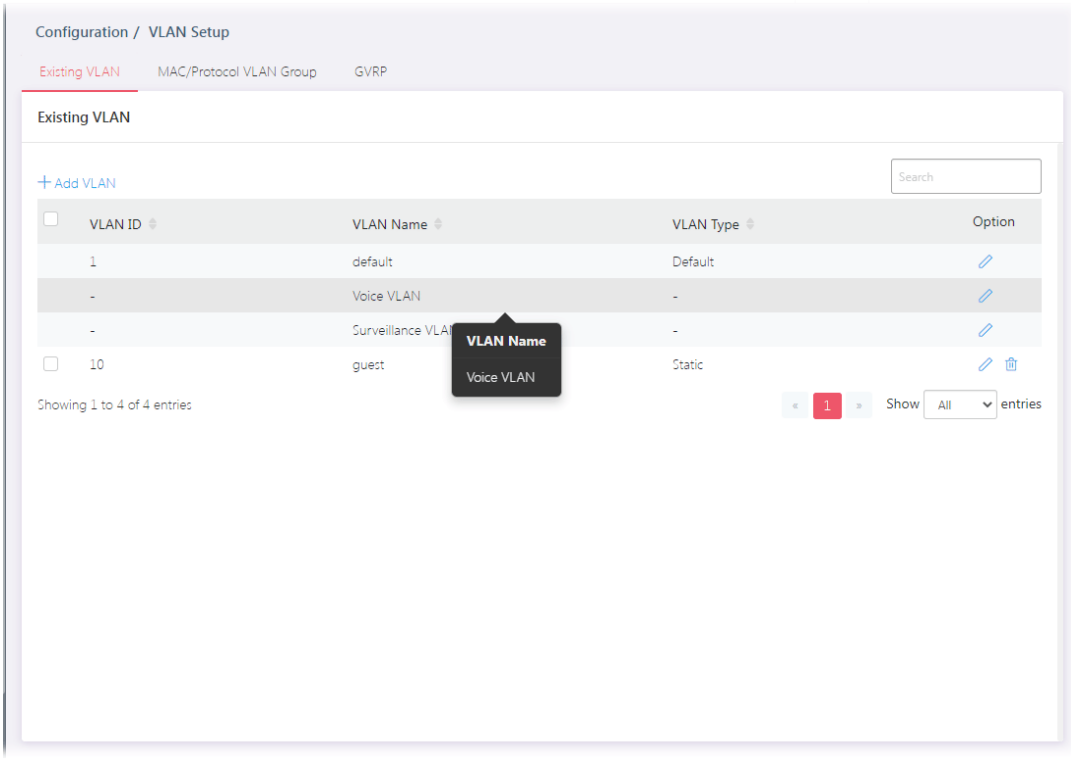

Available settings are explained as follows:

| 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. |

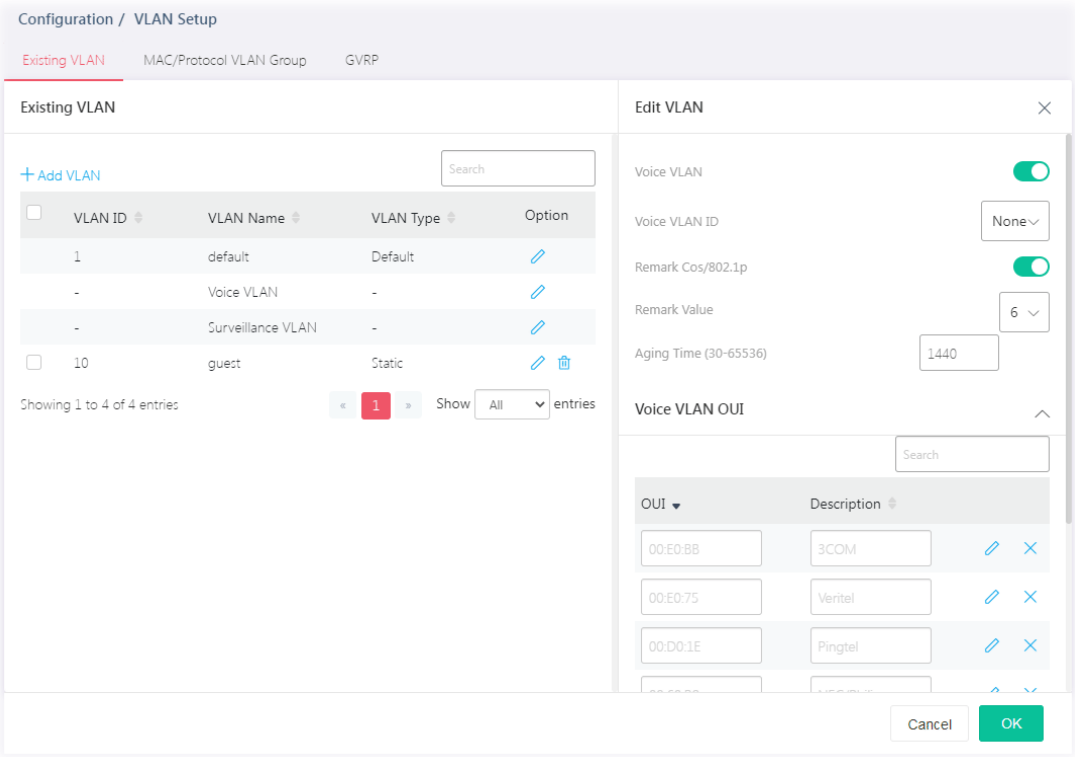
After finishing this web page configuration, please click **OK** to save the settings. A new VLAN will be shown on the page.

## 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:

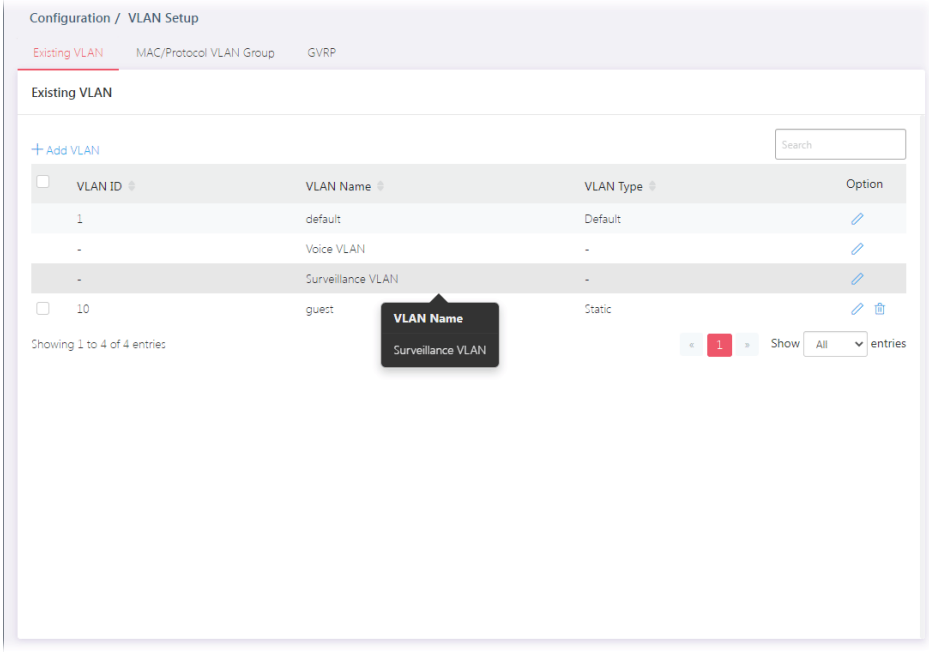
| Item | Description |
|---|---|
| **Edit VLAN** | |

| | |
|---|---|
| **Voice VLAN** | **Enable / Disable** – Click the toggle to enable / disable this function.<br> - means “Enable”.<br> - means “Disable”. |
| **Voice VLAN ID** | Select Voice VLAN ID profile. |
| **Remark Cos/802.1p** | Click the toggle to enable / disable this function.<br>**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).<br>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.<br>**+Add** - Click to create a new voice OUI.<br>• **OUI** - Enter the OUI address.<br>• **Description** - Enter a description of the specified MAC address to the voice VLAN OUI table.<br> - Click it to modify the OUI settings and the description. |
| **OK** | Save the settings. |

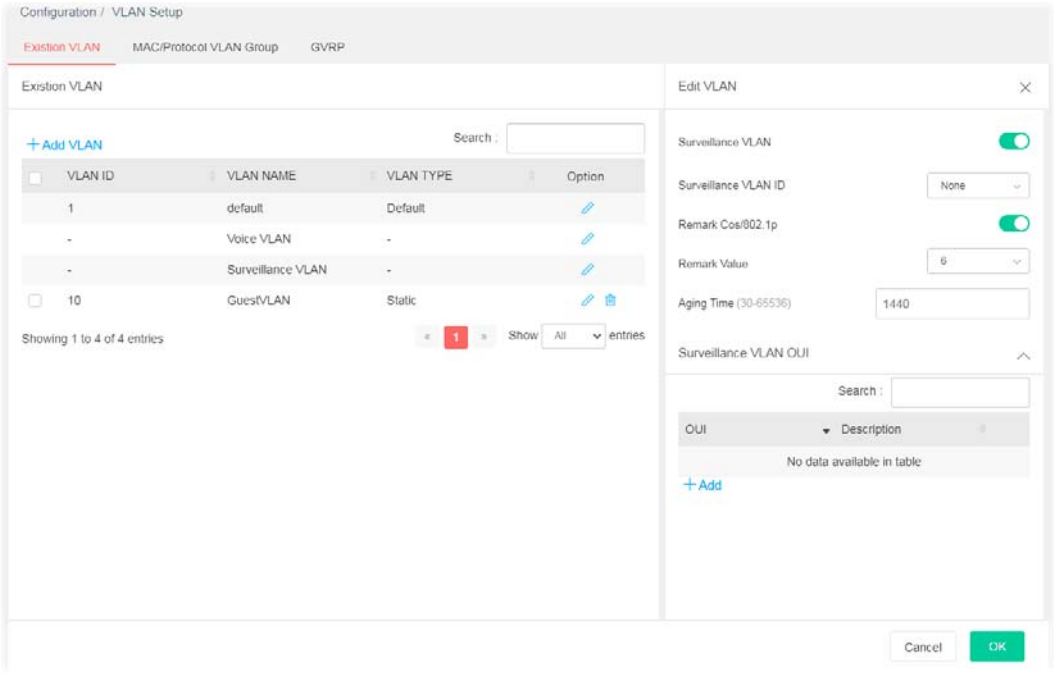
After finishing this web page configuration, please click **OK** to save the settings.

## 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** – Click the toggle to enable / disable this function.<br>- means “Enable”.<br>- means “Disable”.<br>Enable the function to configure surveillance VLAN. |
| **Surveillance VLAN ID** | Choose a VLAN profile as Surveillance VLAN. |
| **Remark Cos/802.1p** | Click the toggle to enable / disable this function.<br>**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).<br>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.<br>Click the to display advanced settings.<br>**+Add** - Click to create a new OUI.<br>• **OUI** - Enter OUI MAC address of monitored IP camera.<br>• **Description** - Enter a description of the specified MAC address to the surveillance VLAN OUI table.<br>- Click to modify the OUI settings and the description. |

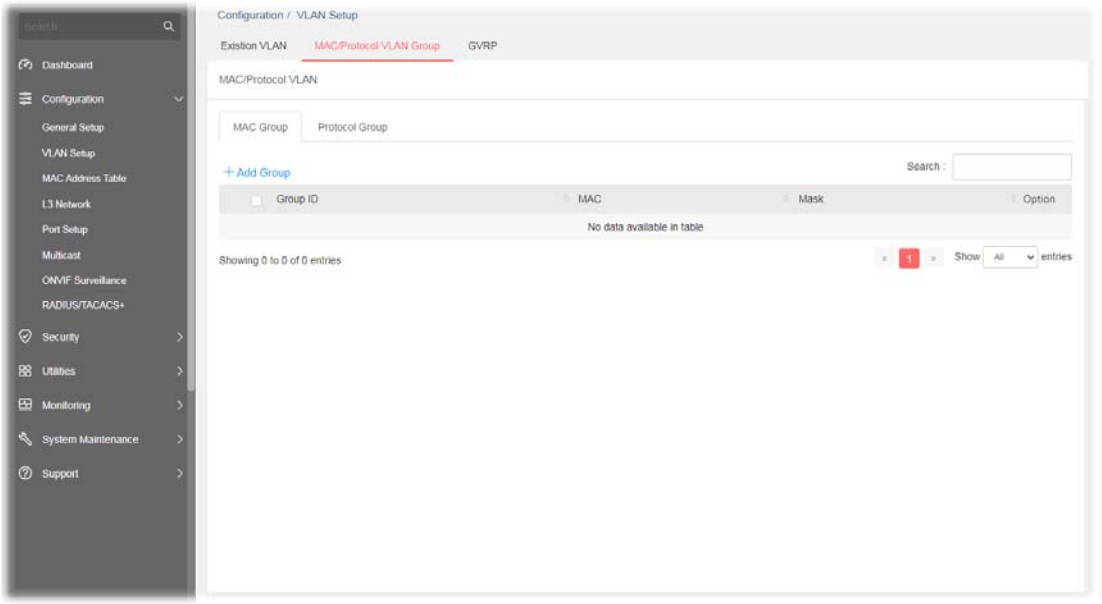
| | |
|---|---|
| **OK** | Save the settings. |

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

# II-2-2 MAC VLAN Group

## II-2-2-1 MAC Group

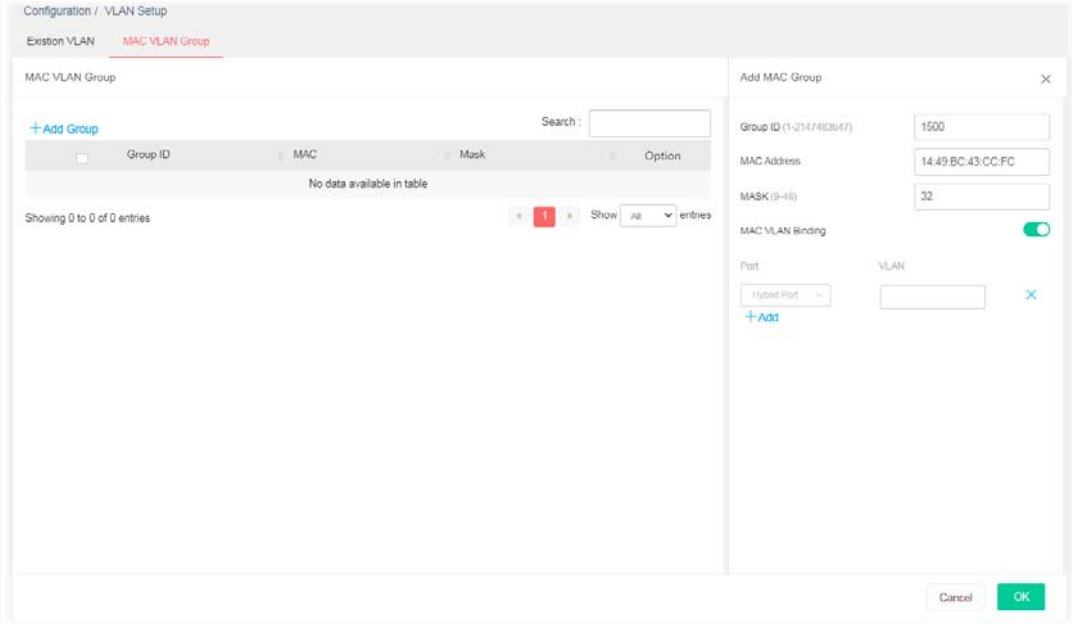
The MAC VLAN allows you to statically assign a VLAN ID to a host with specific MAC address(es). VigorSwitch allows you configure multiple groups with configured MAC address and mask to be active on ports and to be bound with VLAN ID. This page allows the network administrator to define groups with specific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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **MAC VLAN 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.

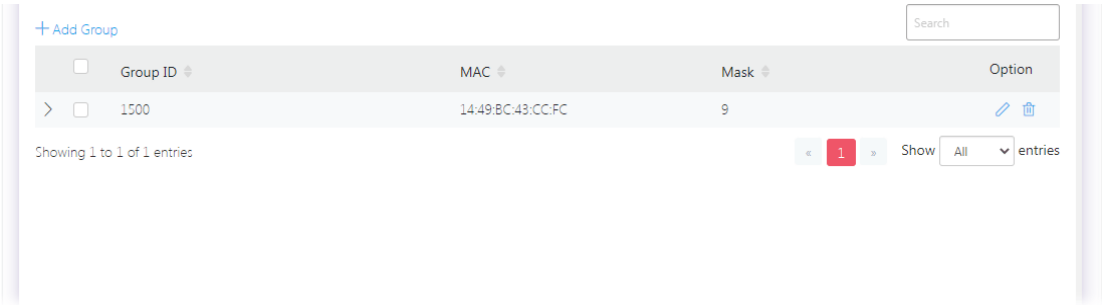



Available settings are explained as follows:

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



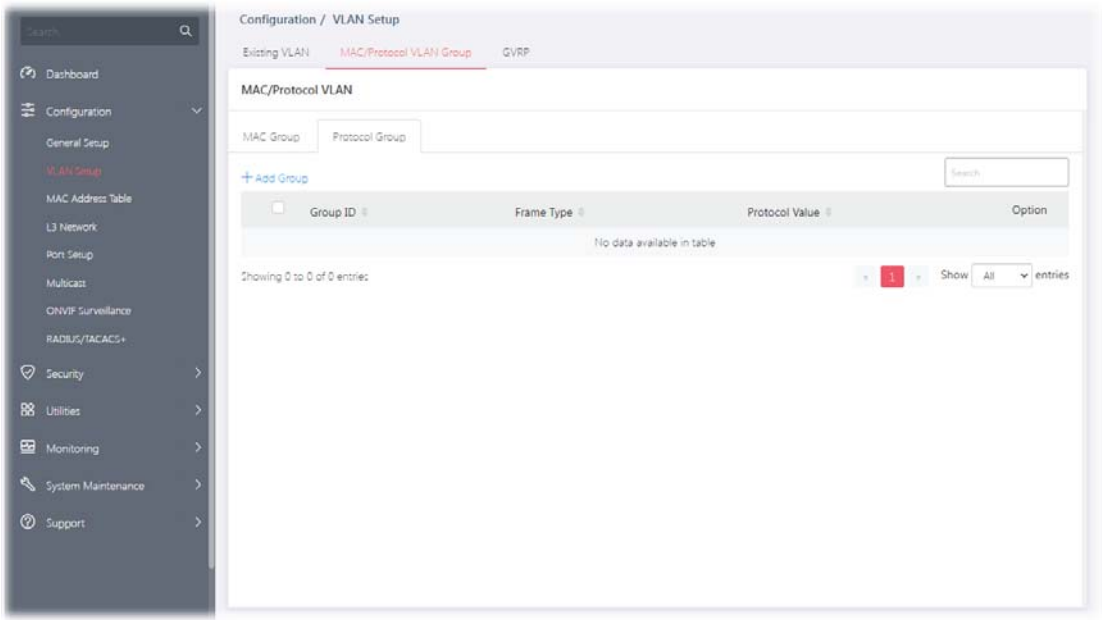

Available settings are explained as follows:

| 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.

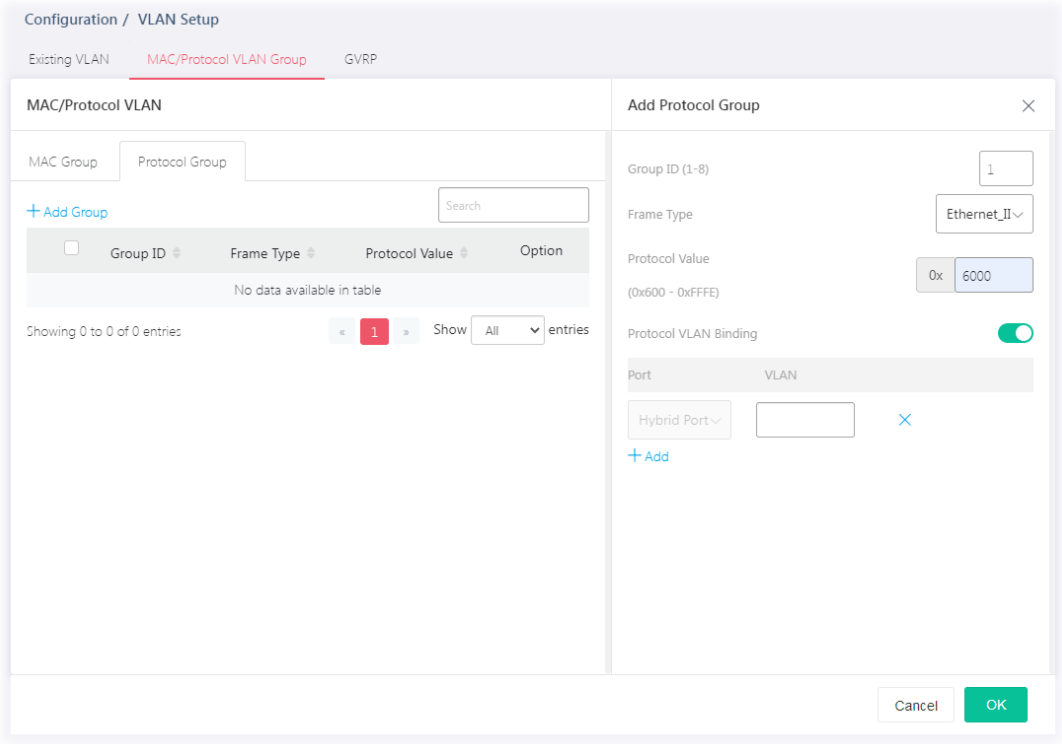



Available settings are explained as follows:

| 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.

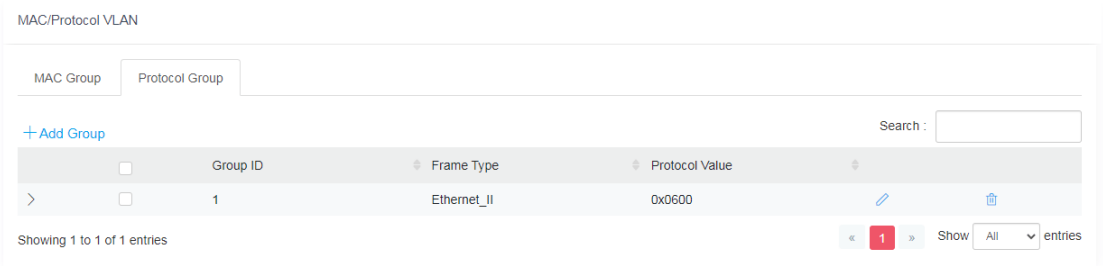



Available settings are explained as follows:

| 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.<br>**Ethernet_II** - Packet will be mapped based on Ethernet version 2.<br>**IEEE802.3_LLC_Other** –Packet will be mapped based on 802.3 packet with LLC other header.<br>**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.<br>**Enable / Disable** – Click the toggle to enable / disable this function.<br> - means “Enable”.<br> - means “Disable”.<br>**+Add** - Click to enter a port number and VLAN ID number.<br>• **Port** - Select the ports you wish to be bound with specified MAC address group.<br>• **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.

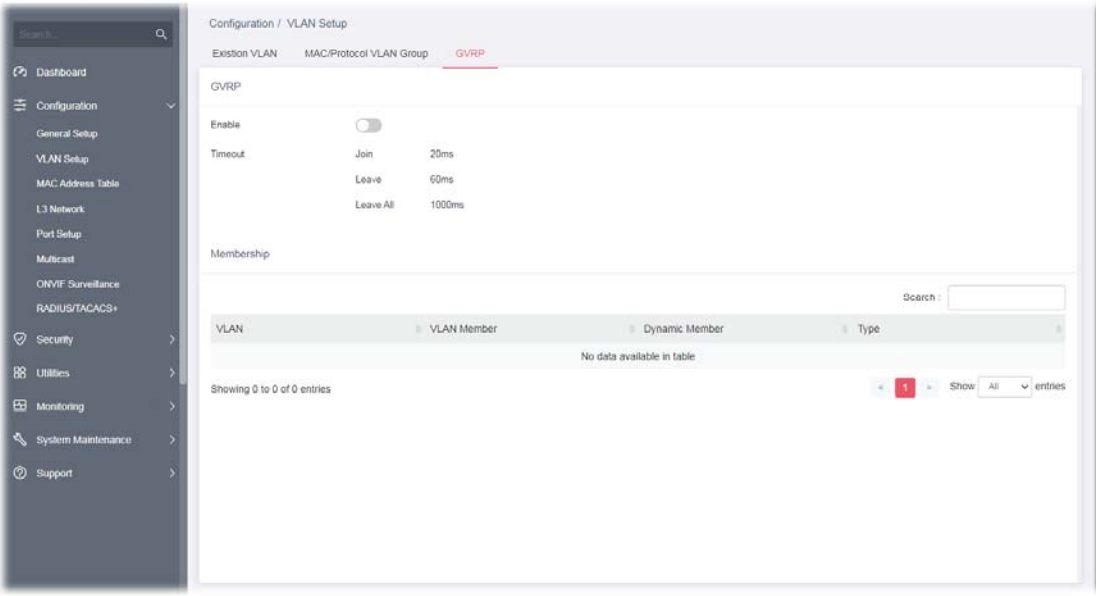



Available settings are explained as follows:

| 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).

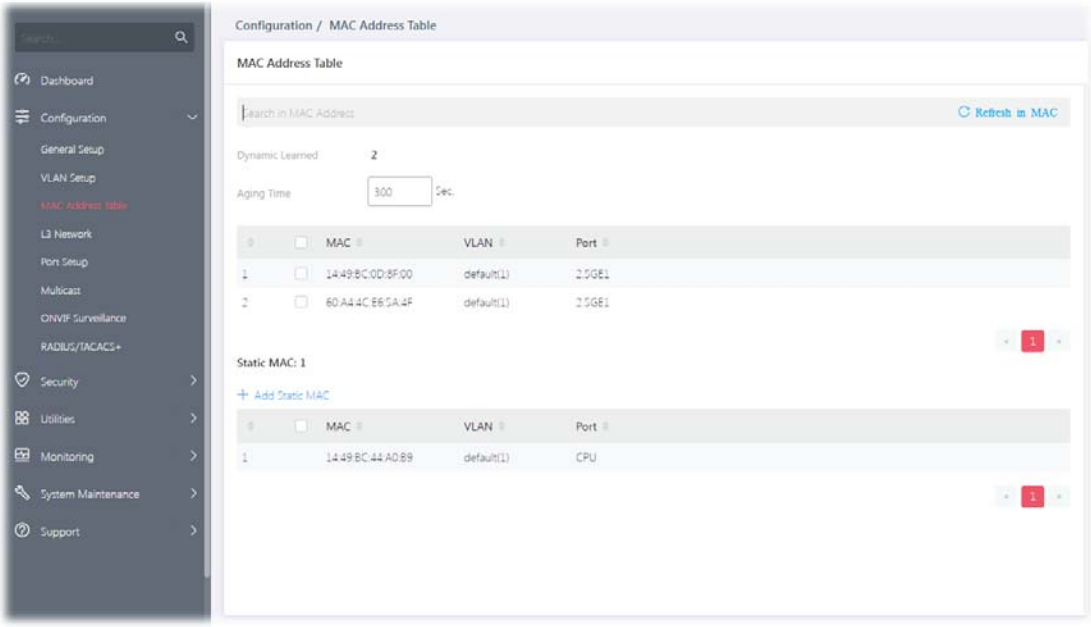



Available settings are explained as follows:

| Item | Description |
|---|---|
| **GVRP** | |
| **Enable** | Click the toggle to enable / disable this function.<br> - means “Enable”.<br> - means “Disable”. |

# II-3 MAC Address Table

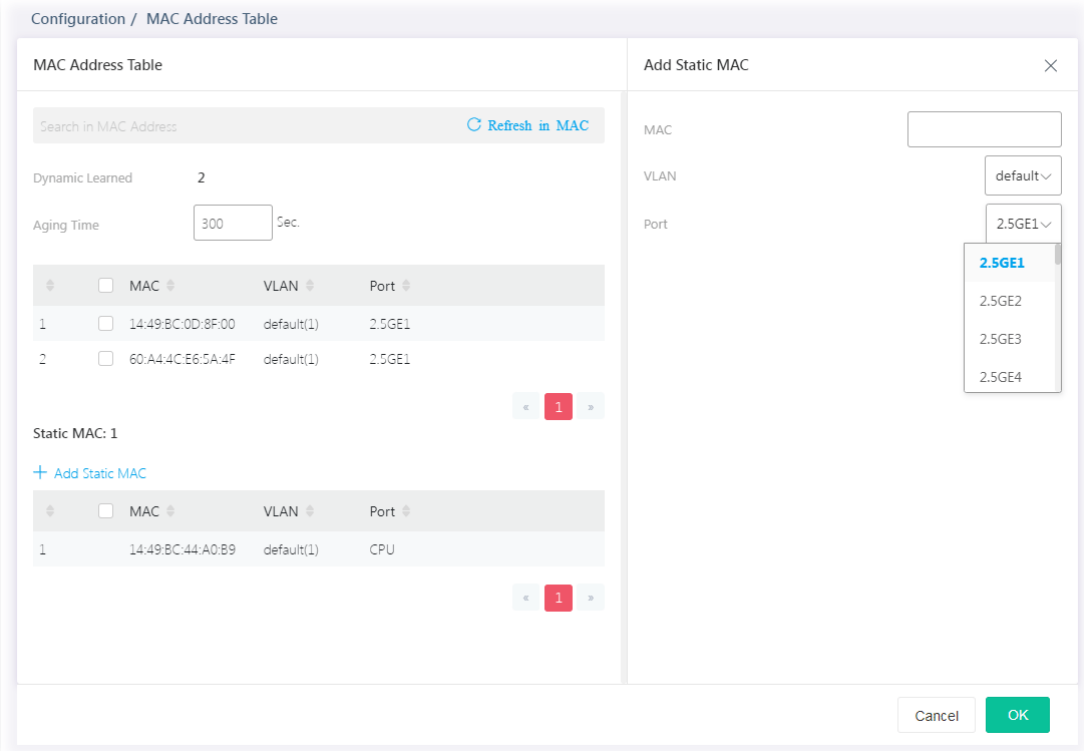
This section allows user to view the static MAC address entries in the MAC table, change related setting, and assign MAC address into MAC table.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Dynamic Learned** | Displays the port number automatically learned by VigorSwitch. |
| **Aging Time** | Enter the MAC address aging out value (5-32767 seconds). |
| **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. |
| **+Add Static MAC** | Click it to add any port into the static MAC table. |

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




Available settings are explained as follows:

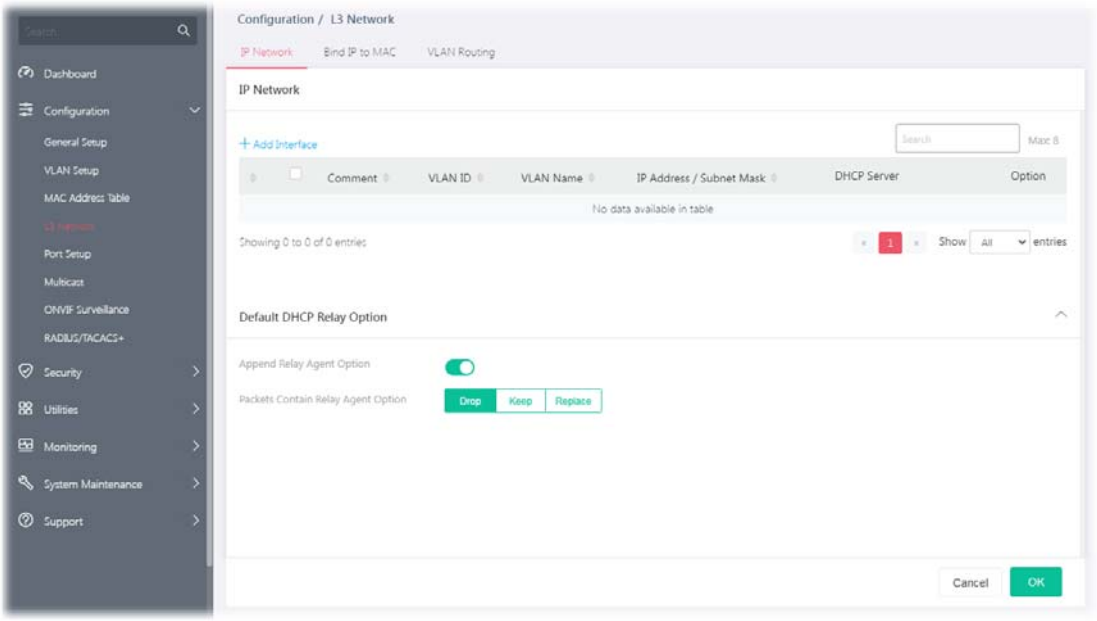
| Item | Description |
|---|---|
| **Add Static MAC** | |
| **MAC** | Enter the MAC address that will be forwarded. |
| **VLAN** | Select the VLAN group to which the MAC address belongs. |
| **Port** | Select the port to which this MAC address belongs. |
| **OK** | Save the settings. |

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.

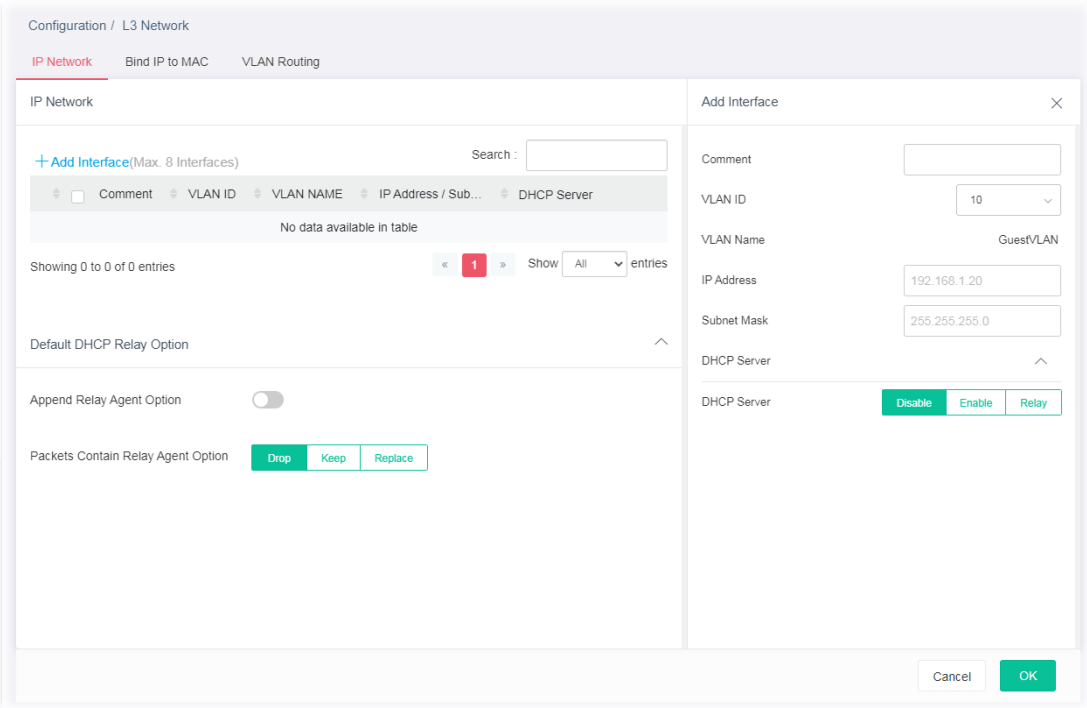



Available settings are explained as follows:

| 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** | Click the toggle to enable / disable the built-in DHCP server on Vigor switch.<br>- means “Enable”.<br>- means “Disable”. |
| **Packets Contain Relay** | Set the packet processing method. |

| | |
|---|---|
| **Agent Option** | **Drop** - Received packets which already contain relay information will be discarded.<br>**Keep** - All packets are forwarded, relay information already present will be ignored.<br>**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.<br>**Enable** - Select to enable the DHCP server function.<br>**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. |

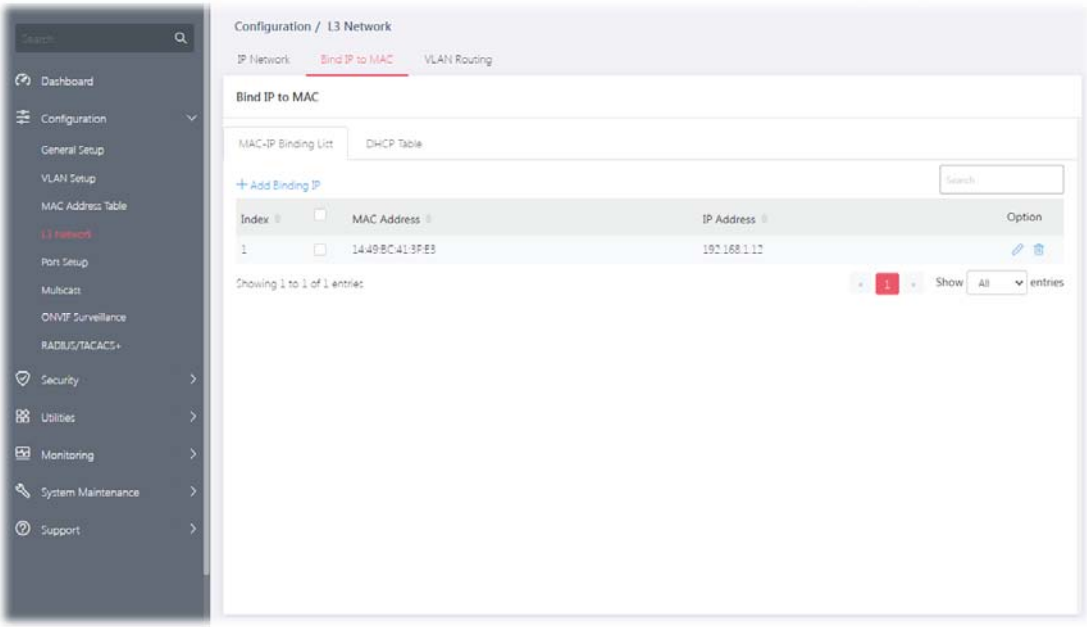
After finishing this web page configuration, please click **OK** to save the settings.

# 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

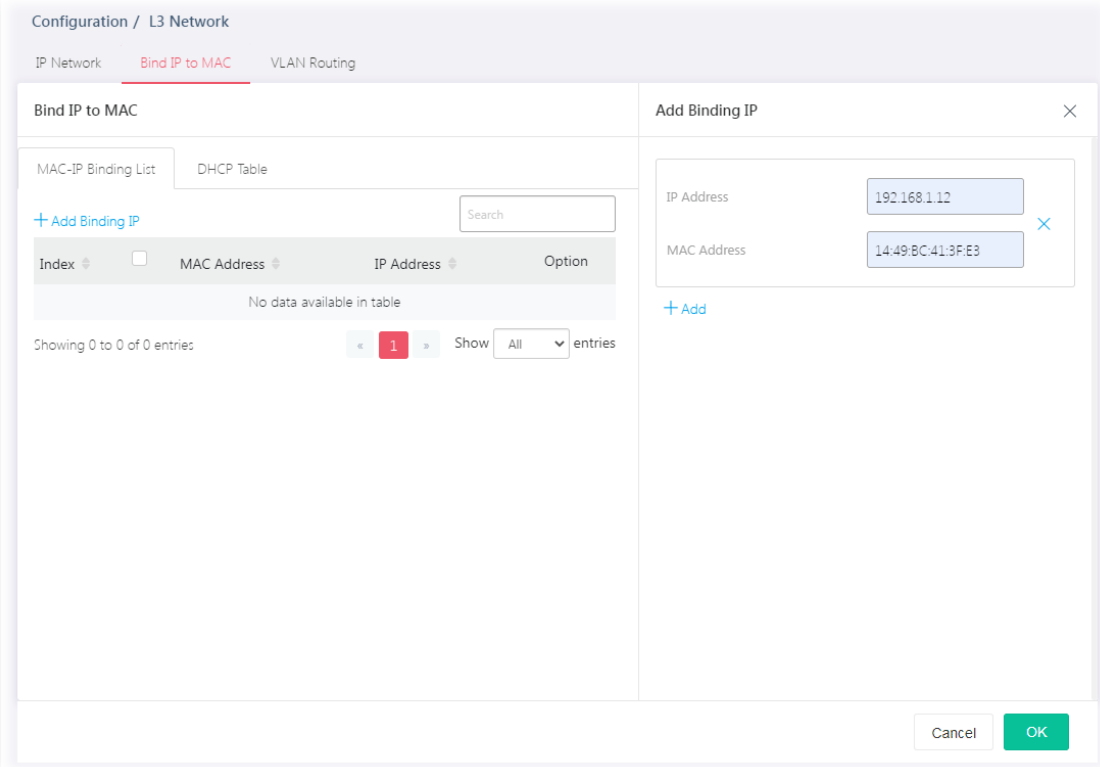
This page displays the MAC-IP Binding List and allows the user to add a new profile or edit/ delete an existed profile.




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.<br>- Click it to remove the selected entry. |

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



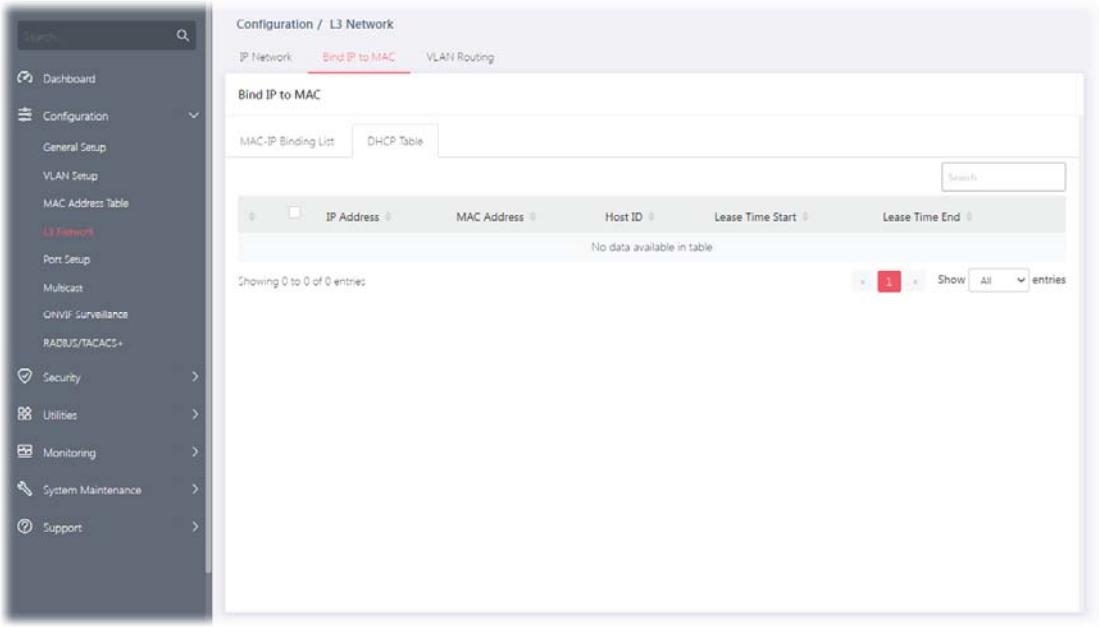

Available settings are explained as follows:

| 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

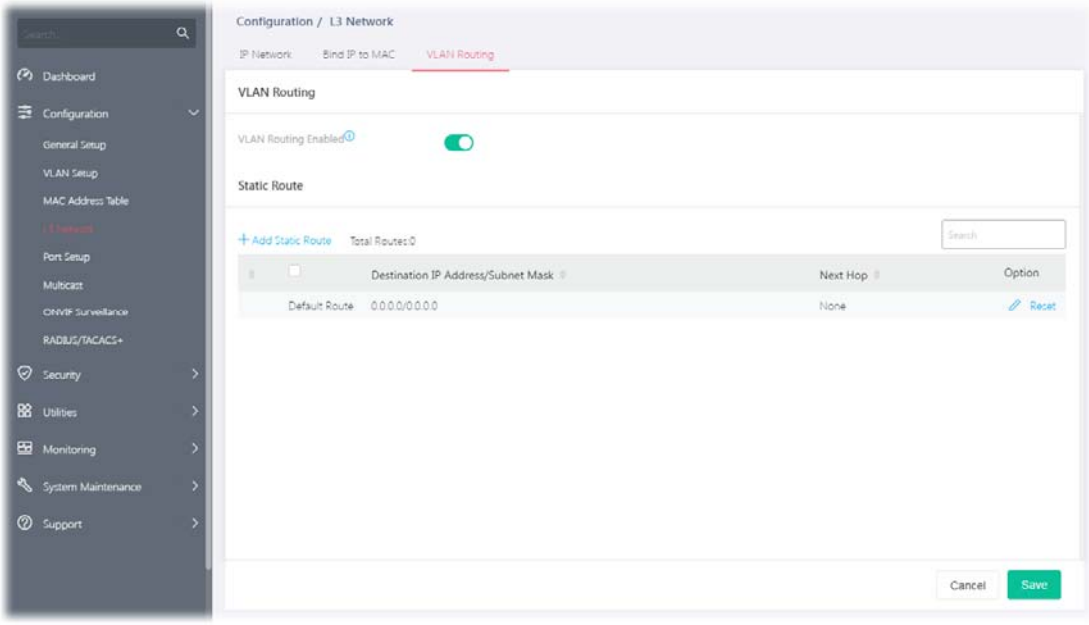
This page displays a table of DHCP servers used by "Bind IP to MAC".




| 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

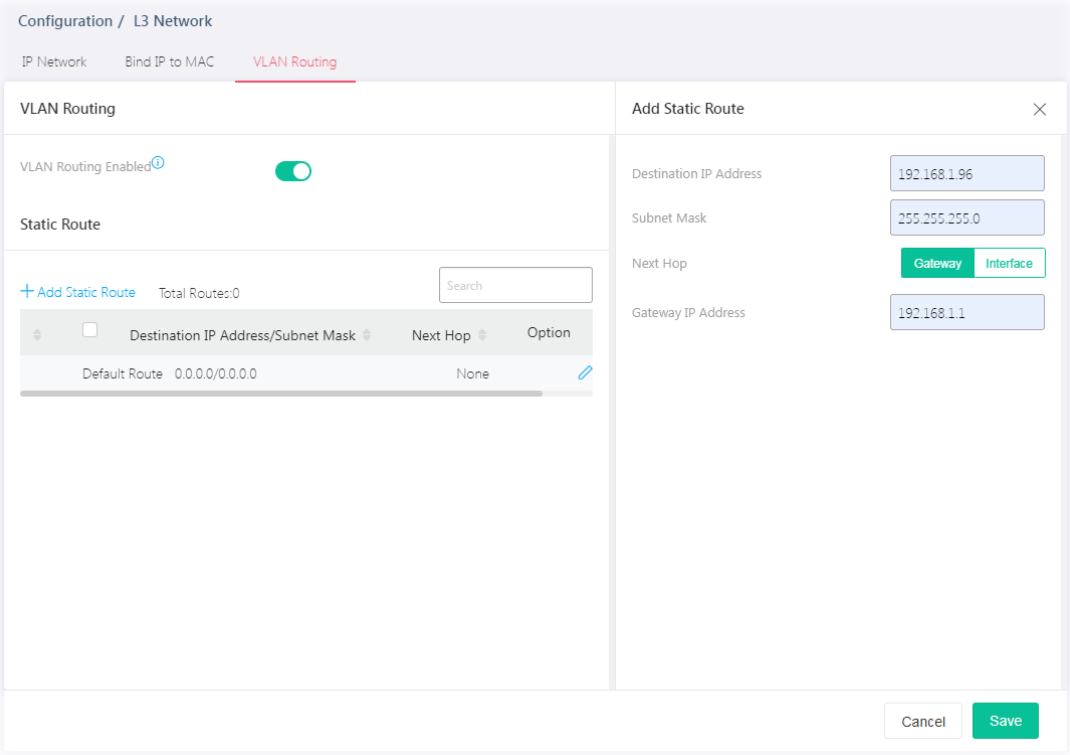
Static routing is a process that the system network administrator can configure the network with all the required information for packet forwarding. Each VLAN can include several IP address with the same subnet. The network administrator can specify some IP addresses (with different subnets) and different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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Vlan Routing** | |
| **VLAN Routing Enable** | Click the toggle to enable / disable this function.<br>- means “Enable”.<br>- 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.<br>**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.<br>Enter the IP address of the gateway. |
| **Interface** | It is available when **Interface** is selected as the Next Hop.<br>Use the drop down list to specify the VLAN ID number. |
| **OK** | Save the settings. |

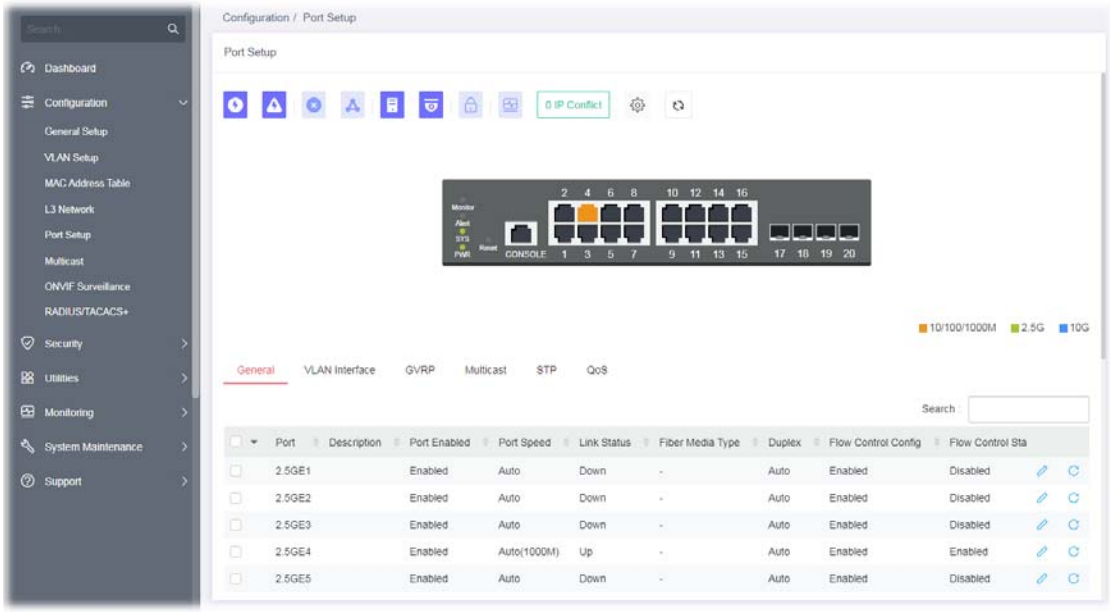
After finishing this web page configuration, please click **OK** to save the settings.

# 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.

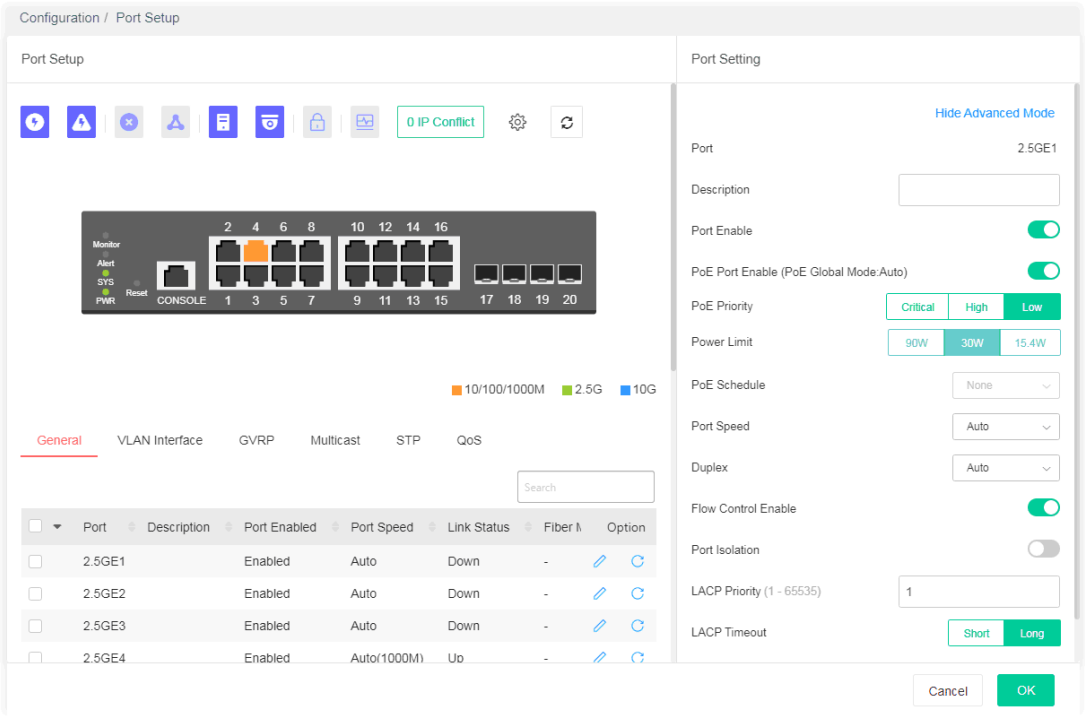


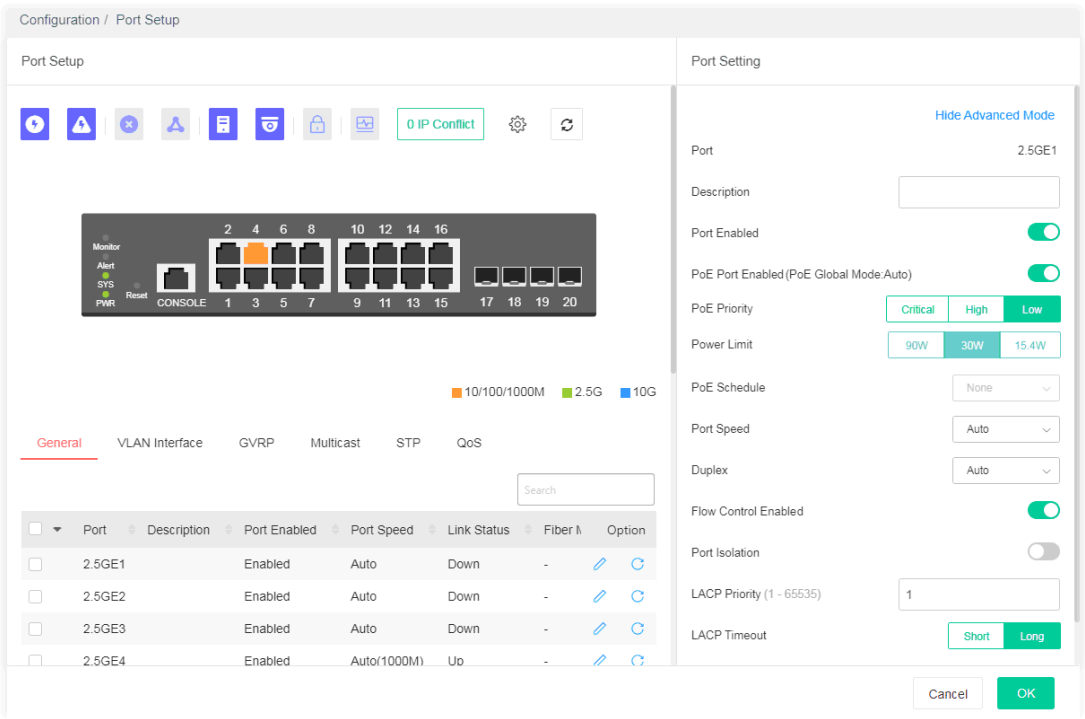

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Port** | Displays the LAN ports (2.5GE1 to 2.5GE16, 10GE1 to 10GE4). |
| **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.<br>- 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.<br>**Critical** - Set PoE device to highest priority connection.<br>**High** –Set PoE device to high priority connection.<br>**Low** –Set PoE device to low priority connection. |
| **Power Limit** | This setting is available when Manual is selected as PoE Mode.<br>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**.<br>Use the drop down list to choose the schedule profile (from 1 to 15). |
| **Port Speed** | Port speed capabilities:<br>• **Auto:** Auto speed with all capabilities.<br>• **Auto(10M):** Auto speed with 10M ability only.<br>• **Auto(100M):** Auto speed with 100M ability only.<br>• **Auto(1000M):** Auto speed with 1000M ability only.<br>• **Auto(10/100M):** Auto speed with 10/100M ability.<br>• **Auto(2.5G):** Auto speed with 2.5G ability only.<br>• **10M:** Force speed with 10M ability.<br>• **100M:** Force speed with 100M ability.<br>• **1000M:** Force speed with 1000M ability.<br>• **2.5G:** Force speed with 2.5G ability.<br>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.<br>For SFP fiber module, you might need to manually configure the speed to match fiber module speed. |
| **Duplex** | Port duplex capabilities:<br>• **Auto:** Auto duplex with all capabilities.<br>• **Half:** Auto speed with 10/100M ability only.<br>• **Full:** Auto speed with 10/100/1000M ability only. |
| **Flow Control Enable** | 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.<br>**Enable / Disable** – Click the toggle to enable / disable this function.<br> - means “Enable”.<br> - 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.<br>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.<br>**Enable / Disable** – Click 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.<br>**Short** - LACP PDU will be sent per second. If port member is not seen over 3 seconds, it will cause port member timeout.<br>**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

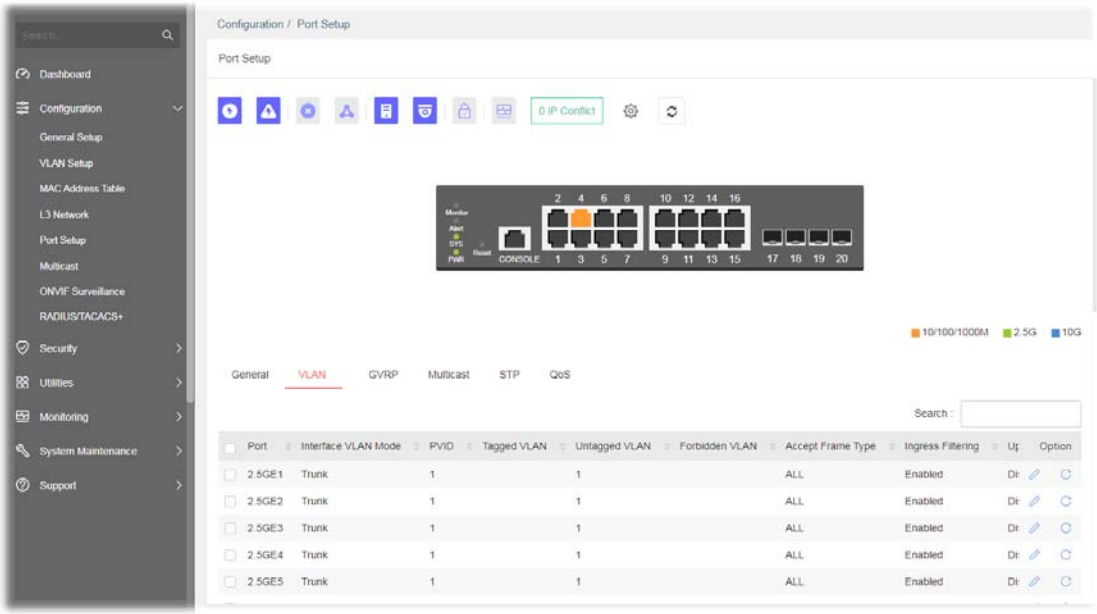
This page allows a user to configure interface (GE) settings related to VLAN.

**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**

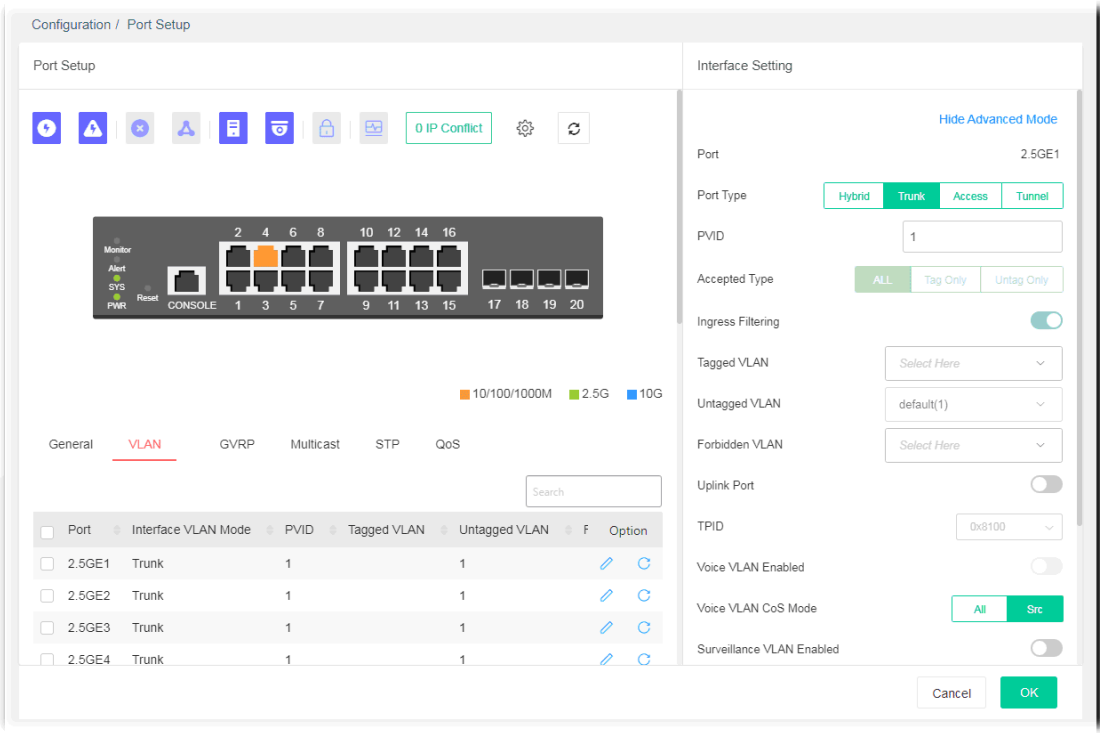
Surveillance VLAN can be configured for VigorSwitch to identify the packets coming from an IP camera automatically and assign those traffics to a specific VLAN ID and CoS/802.1p value, this helps you to prioritize those traffics and improve video quality.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Port** | Displays the LAN port number. |
| **Interface 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.<br>- 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. |
| **Port Type** | Select the VLAN mode of the interface.<br>**Hybrid** – Support all functions as defined in IEEE 802.1Qspecification.<br>**Access** – Accepts only untagged frames and join an untagged VLAN.<br>**Trunk** - An untagged member of one VLAN at most, and is a tagged member of zero or more VLANs. |
| **PVID** | A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines.<br>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.<br>**All** - Accept frames regardless it's tagged with 802.1q or not.<br>**Tag Only** - Accept frames only with 802.1q tagged.<br>**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. |

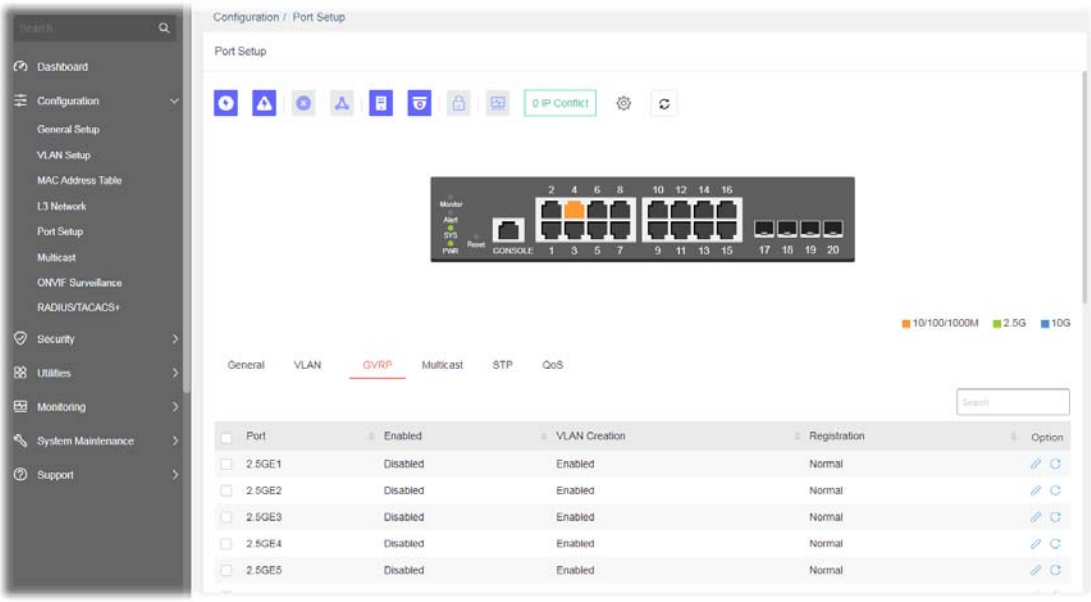
| Below shows settings for Advanced Mode | |
|---|---|
| **Forbidden VLAN** | The selected GE port only allows default VLAN packet to pass through.<br>**Enable / Disable** – Click the toggle to enable / disable the LAN port(s) as forbidden VLAN port.<br> - means “Enable”.<br> - means “Disable”. |
| **Voice VLAN Enable** | **Enable / Disable** – Click 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.<br>**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 Enable** | **Enable / Disable** – Click the toggle to enable / disable the LAN port(s) as Surveillance VLAN port.<br> - means “Enable”.<br> - means “Disable”. |
| **Surveillance VLAN Mode** | Select port surveillance VLAN mode.<br>**Auto** - Surveillance VLAN auto detect packets that match OUI table and add received port into surveillance VLAN ID tagged member.<br>**Manual** - User need add interface to VLAN ID tagged member manually. |
| **Surveillance VLAN QoS Policy** | Select port QoS Policy mode.<br>**Video Packet** - QoS attributes are applied to packets with OUI in the source MAC address.<br>**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 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.

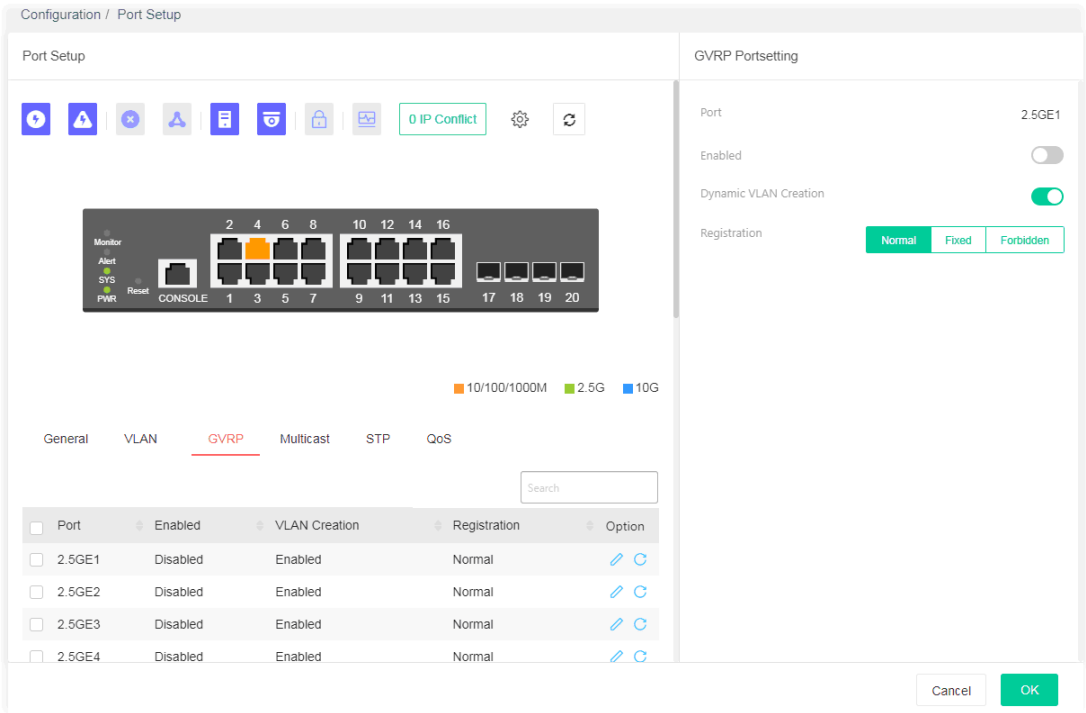
Such function can eliminate unnecessary network traffic and prevent any attempt to transmit information to unregistered users.




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.<br>- 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** – Click the toggle to enable / disable the GVRP port setting.<br>- means “Enable”.<br>- means “Disable”. |
| **Dynamic VLAN Creation** | Click the toggle to enable / disable the VLAN creation. |
| **Registration** | There are three modes to be specified.<br>**Normal** – Default setting. All packets can pass through the selected GE port.<br>**Fixed** – The selected GE port only sends static VLAN information to neighboring device and allows static VLAN packet to pass through.<br>**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.

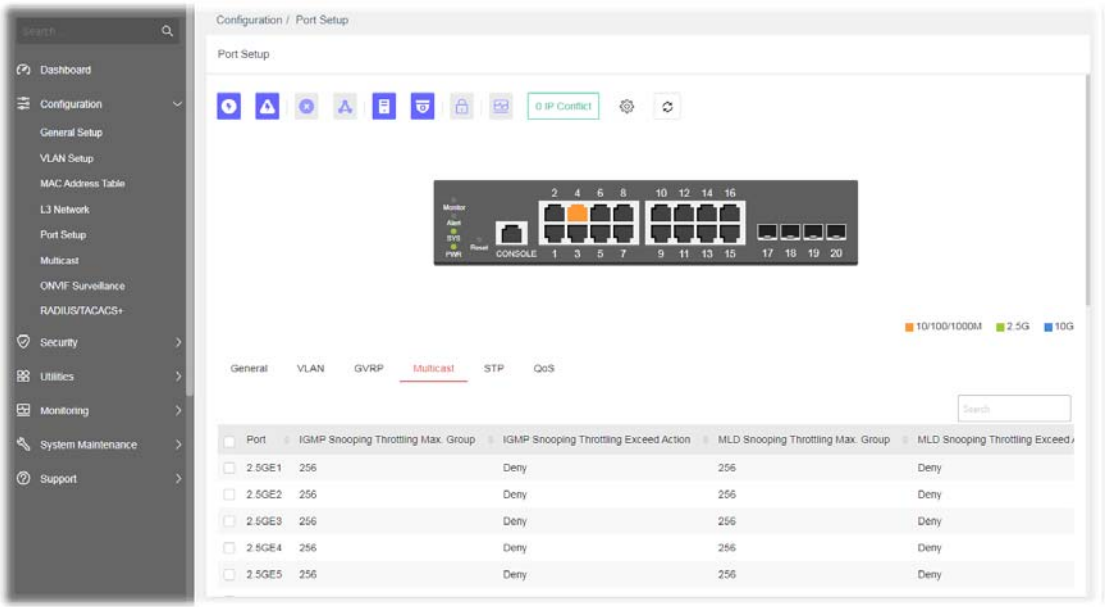
### MLD Snooping

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.

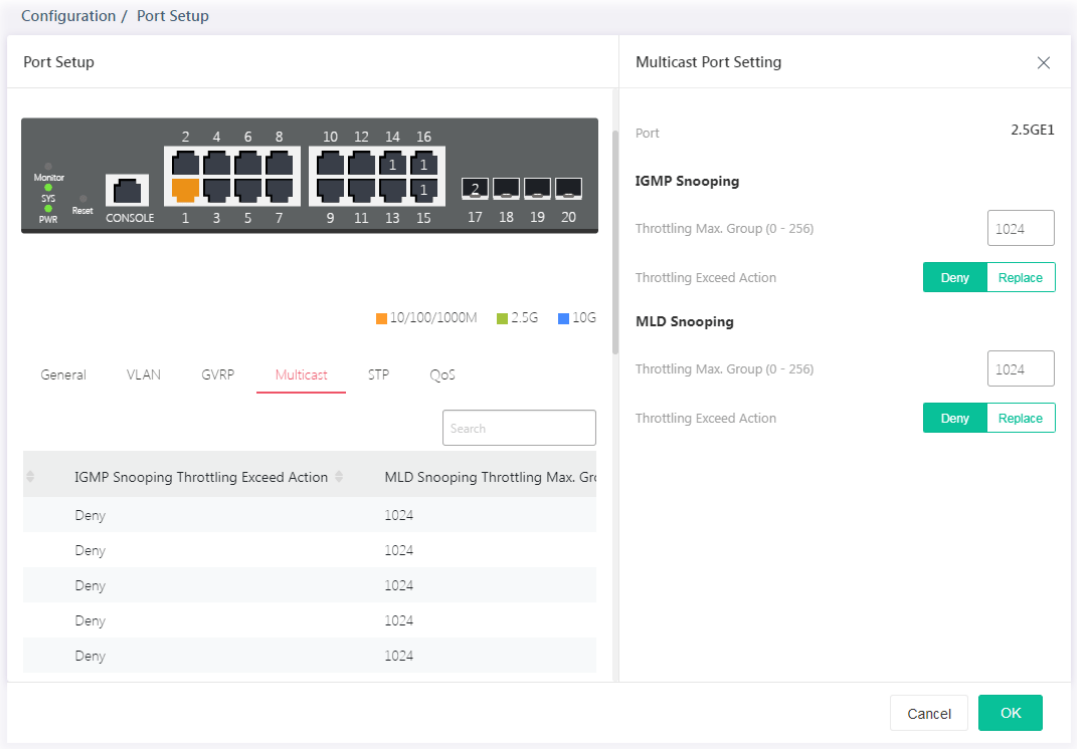



Available settings are explained as follows:

| 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.<br>- 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.<br>**Deny –** It is default setting. The IGMP join report (for multicast service) received by such interface will be discarded.<br>**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.<br>**Deny –** It is default setting. The MLD join report (for multicast service) received by such interface will be discarded.<br>**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.

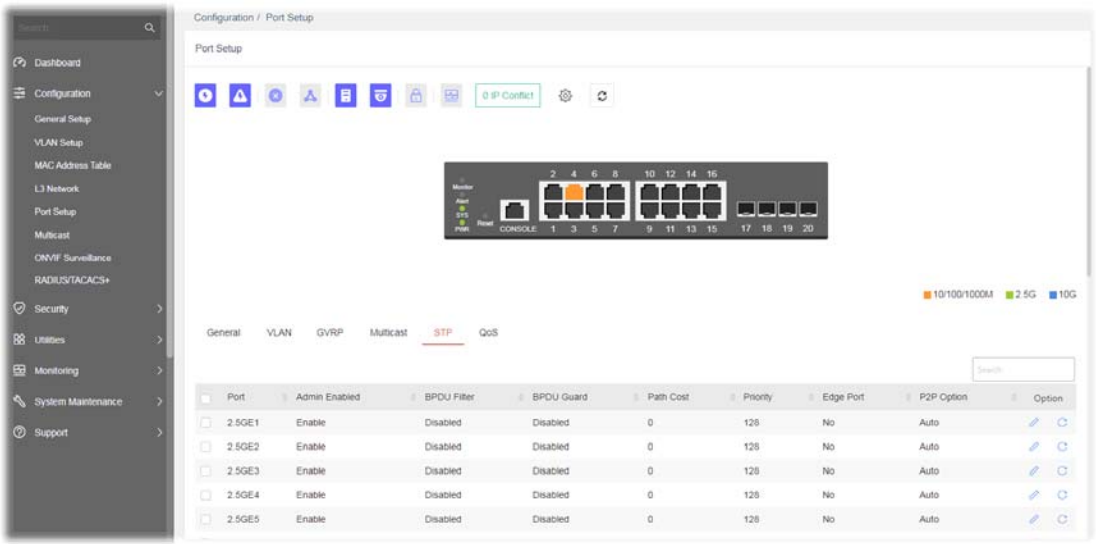
# II-5-5 STP

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).

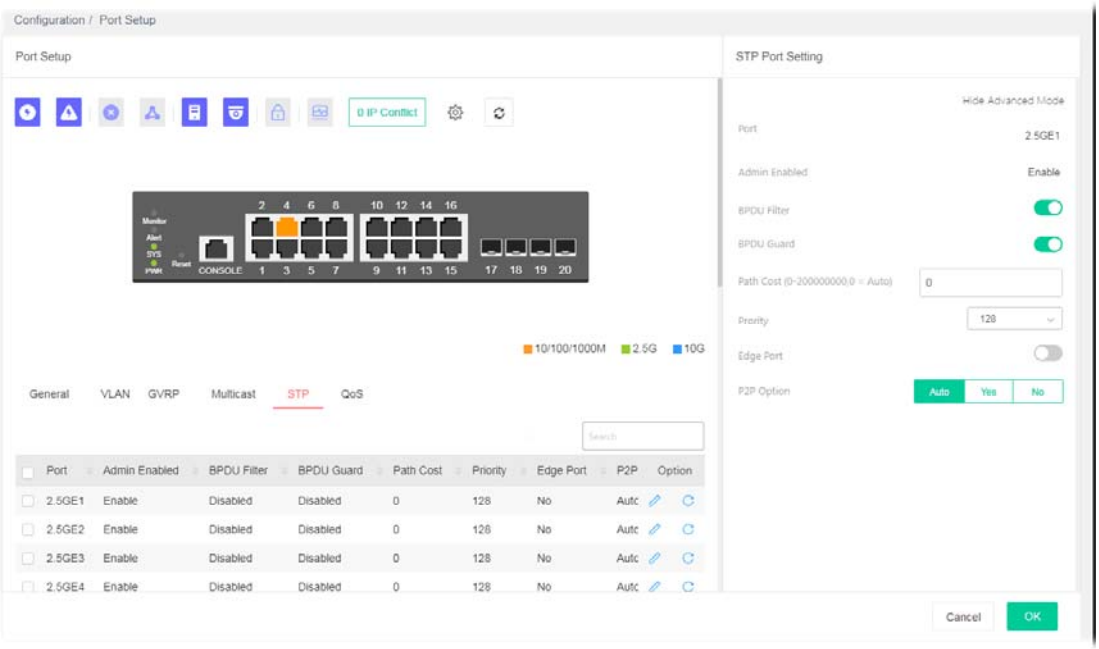
BPDUs are sent out as multicast frames to which only other layer 2 switches or bridges are listening. If any loops (multiple possible paths between switches) are found in the network topology, the switches will co-operate to disable a port or ports to ensure that there are no loops; that is, from one 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 (2.5GE1 to 2.5GE16, 10GE1 to 10GE4, 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.<br>- 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** | Click the toggle to enable / disable the function of dropping all BPDU packets and no BPDU will be sent.<br>- means “Enable”.<br>- 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.<br>Click the toggle to enable / disable the function. |
| **P2P Option** | • **Auto –** VigorSwitch determines the STP of link type for this port |

| | |
|---|---|
| | automatically.<br>• **Yes –** It means the STP of link type on this port is full-duplex and directly connect to another switch or host.<br>• **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

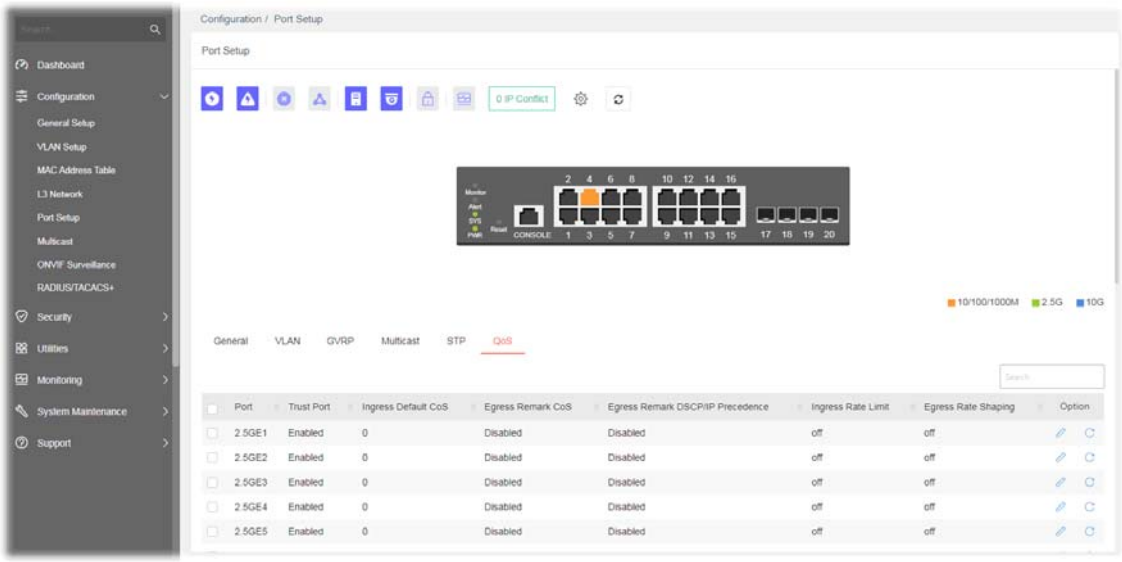
This page is used to configure port settings for QoS. The configuration result for each port will be displayed on the table listed on the lower side of this web page.

**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**

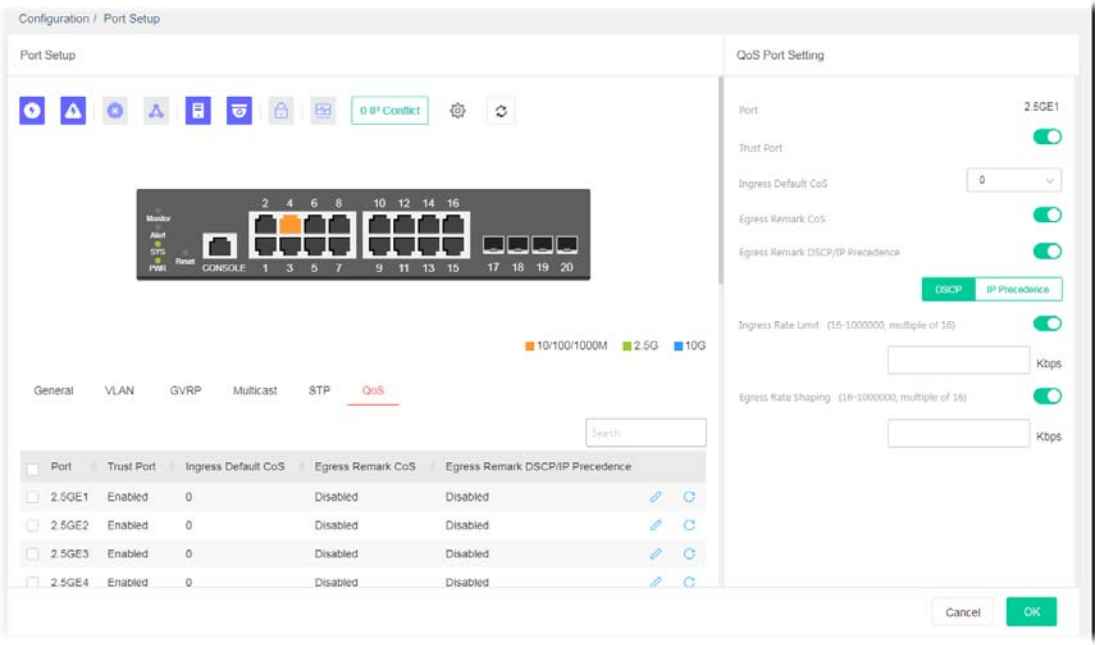
It allows a user to configure egress port rate limit. The egress rate limit is the number of bits per second that can be received from the egress interface. Excess bandwidth above this limit is discarded.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Port** | Displays the port profiles (2.5GE1 to 2.5GE16, 10GE1 to 10GE4, 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.<br>- 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 (2.5GE1 to 2.5GE16, 10GE1 to 10GE4, LAG1 to LAG8). |
| **Trust Port** | **Enable / Disable** – Click the toggle to enable / disable this function.<br>- Traffic will follow trust mode in general setting.<br>- 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** – Click the toggle to enable / disable this function. |
| **Egress Remark DSCP/IP Precedence** | Click the toggle to enable / disable this function.<br>**DSCP** - Egress traffic will be marked with DSCP value according to the Queue to DSCP mapping table.<br>**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.<br>Click the toggle to enable / disable this function.<br>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.<br>Click 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.

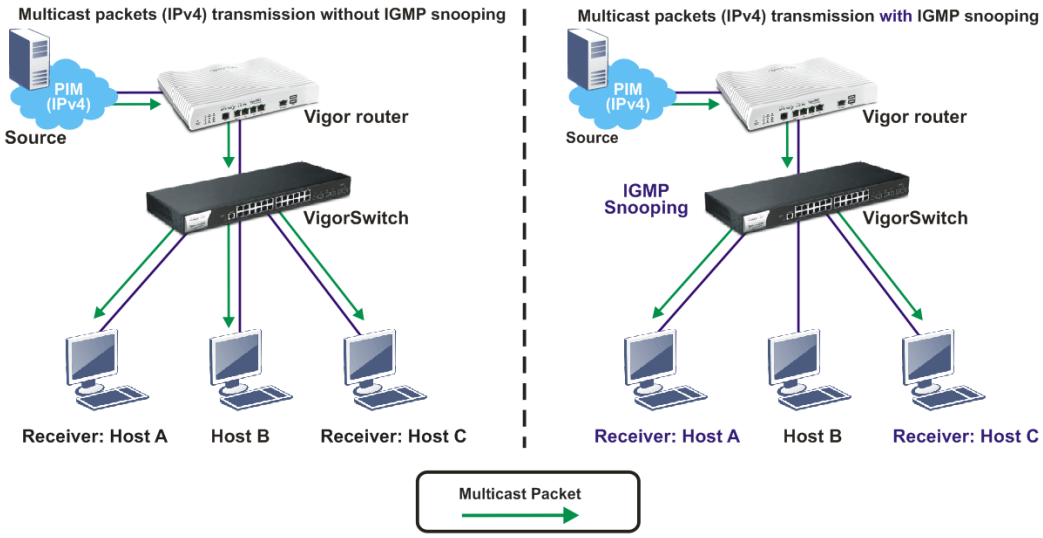
# II-6 Multicast

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

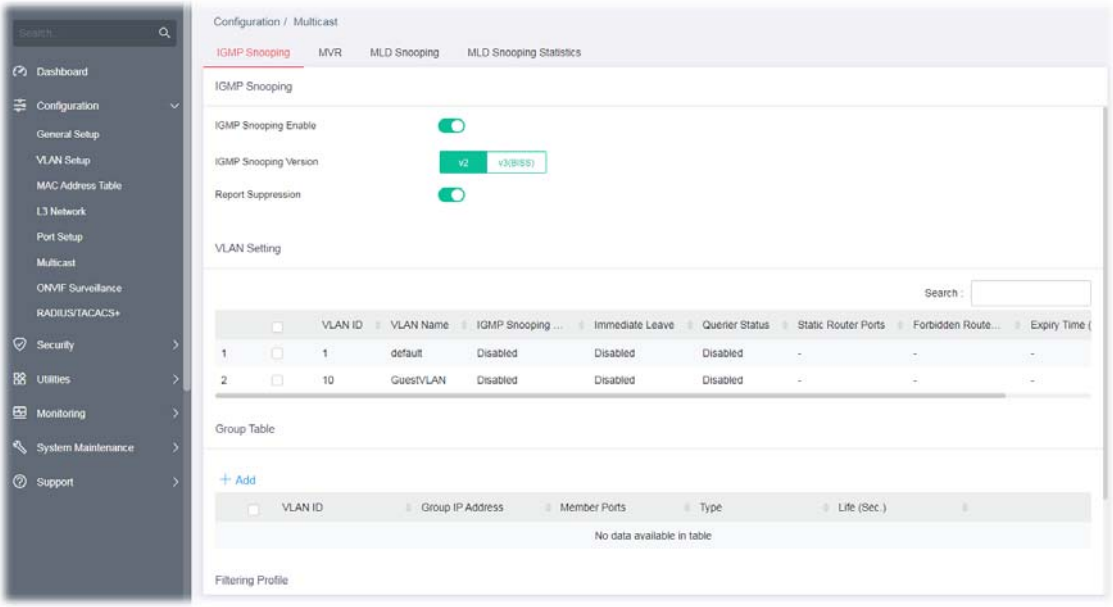
To avoid the incoming data broadcasting to all GE ports, multicast is useful to transfer the data/message to specified GE ports for IGMP snooping. When VigorSwitch receives a message “subscribed” by the client, it must decide to transfer the data to specified GE ports according to the location of the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

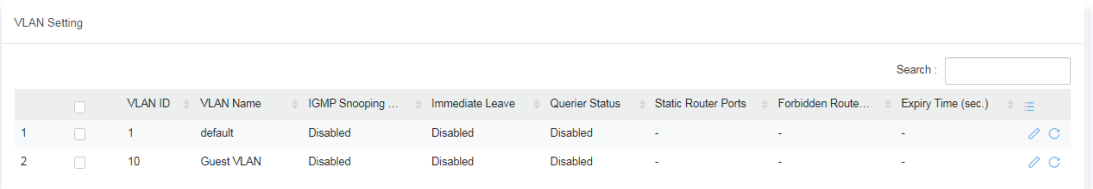



Available settings are explained as follows:

| Item | Description |
|---|---|
| **IGMP Snooping Enable** | **Enable / Disable** – Click the toggle to enable / disable this function.<br> - means “Enable”.<br> - means “Disable”. |
| **IGMP Snooping Version** | Set the IGMP snooping version.<br>**v2 -** Only support process IGMP v2 packet.<br>**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.<br>**Enable / Disable** – Click the toggle to enable / disable this function.<br> - means “Enable”.<br> - 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.

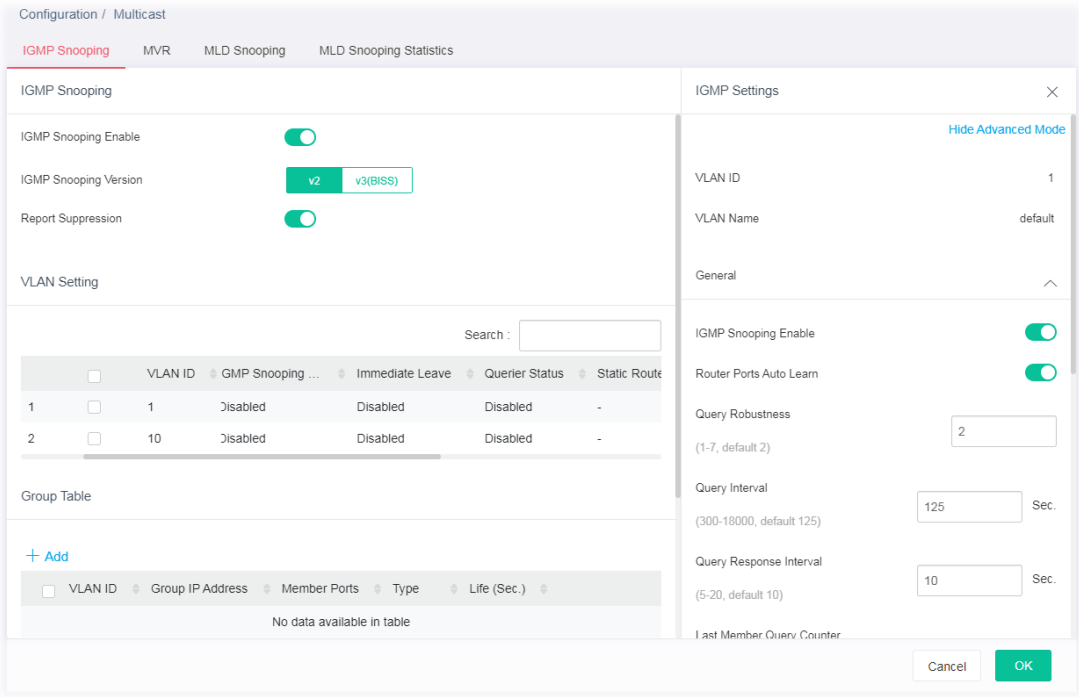



Available settings are explained as follows:

| 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. |

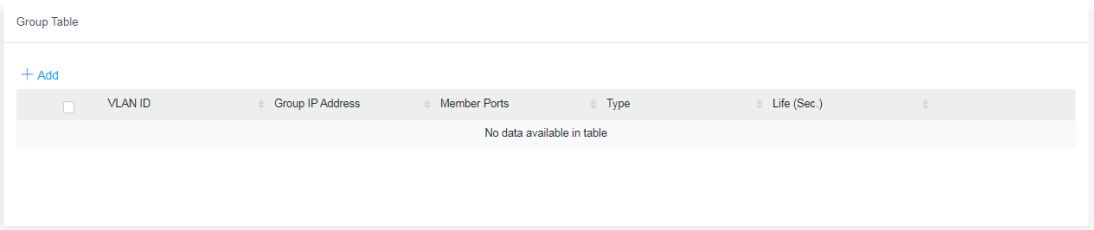
| | |
|---|---|
| **General** | **IGMP Snooping Enable** – Click the toggle to enable / disable this IGMP snooping function.<br> - means “Enable”.<br> - means “Disable”. |
| **Below shows settings for Advanced Mode** | |
| **Router Ports Auto Learn** | Click the toggle to enable / disable this function. 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 -** Click the toggle to enable / disable this function.<br>In **Advanced Mode,**<br>**Querier Version** - Set the IGMP snooping version.<br>• **v2 -** Only support process IGMP v2 packet.<br>• **v3** - Support v3 basic and v2.<br>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.<br>**Enable / Disable** – Click the toggle to enable / disable this function.<br>**+Add** - Click to create a new group.<br>• **Group IP Address** - Specify the IPv4 multicast address you wish to assign for the static group (defined in VLAN ID).<br>• **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.<br>**Forbidden Router Ports** - Use the drop down list to specify forbidden LAN Port (GE/LAG). |
| **IGMP Forward All** | **Static Forward 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.<br>**Forbidden Forward 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

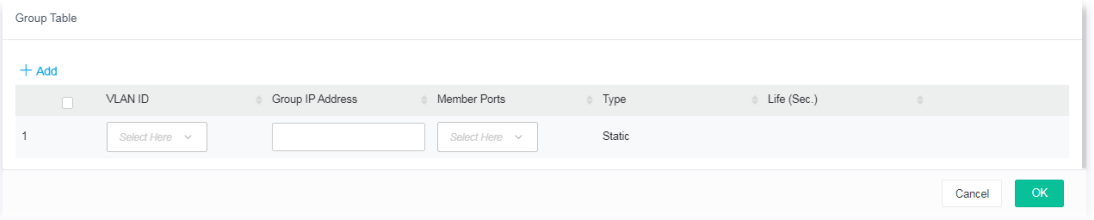
This page shows currently known and dynamically learned by IGMP snooping or shows the assigned IPv4 multicast address group in operation.




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.<br>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. |

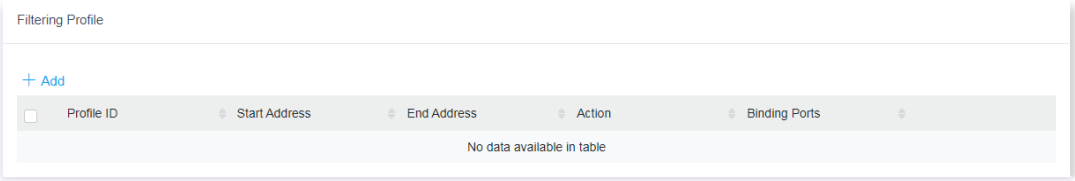
After finishing this web page configuration, please click **OK** to save the settings.

## 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.

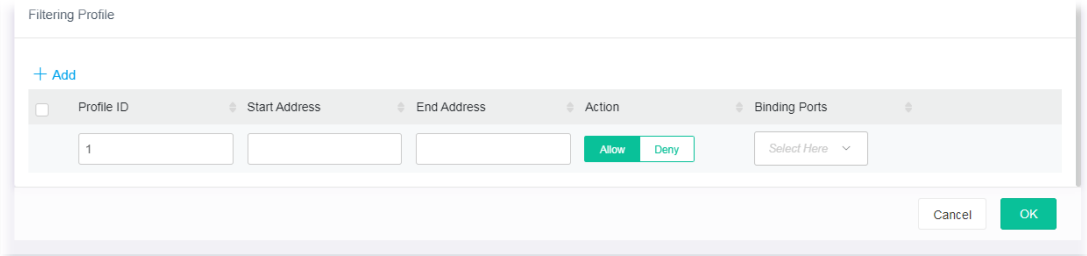
In addition, such filtering profile is only effective for controlling the query for multicast. It has nothing to do with the general IGMP query.




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.

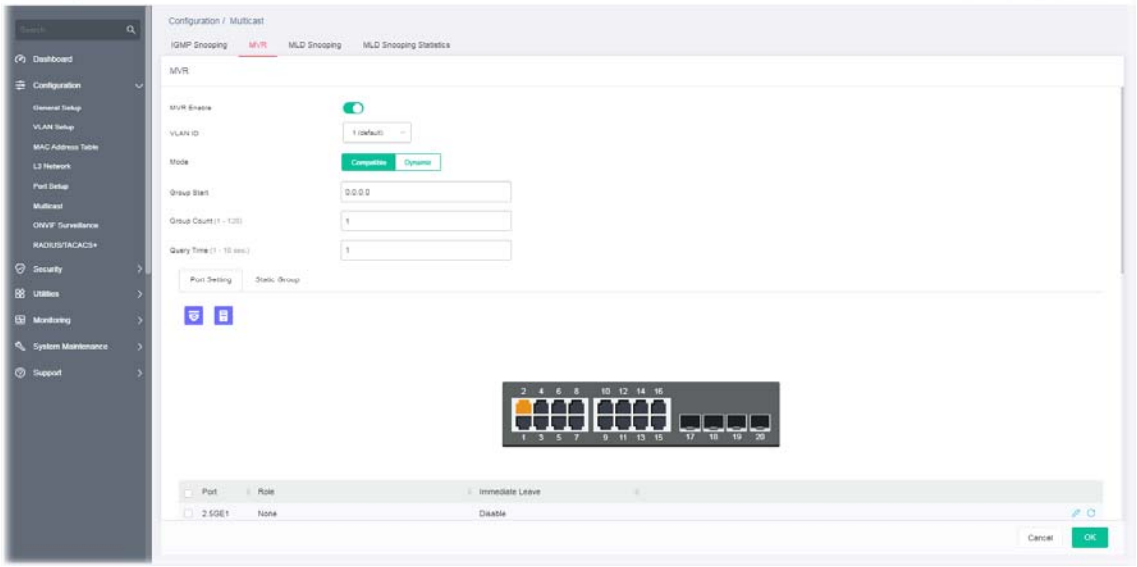
## II-6-2 MVR

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:

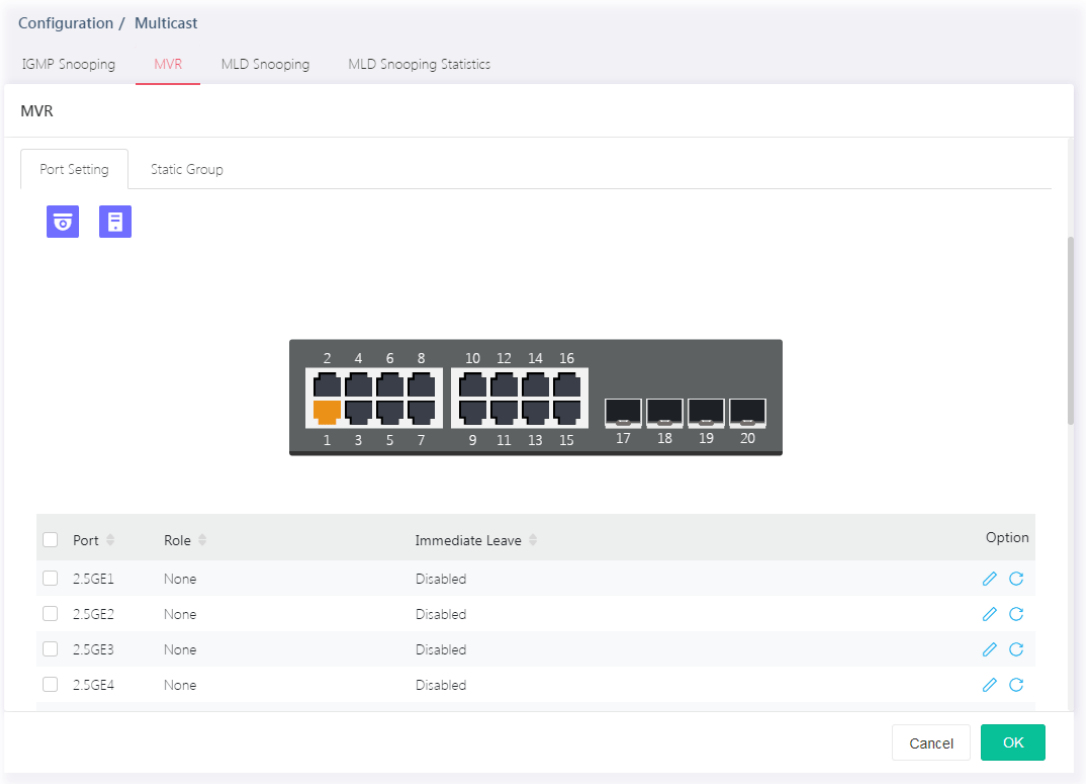
| Item | Description |
|---|---|
| **MVR Enable** | Click the toggle to enable / disable the MVR function.<br>- means “Enable”.<br>- means “Disable”. |
| **VLAN ID** | Choose one VLAN profile from the drop down list as multicast source VLAN which will receive multicast data. All source ports must belong to this VLAN. The default is VLAN 1.<br>Note: Each VLAN ID shall be configured with group address and member port. |
| **Mode** | There are two modes offered for MVR operation.<br>**Comaptible –** Multicast data received by MVR hosts (multicast server) |

| | |
|---|---|
| | will be forwarded to all MVR receiver ports.<br>**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

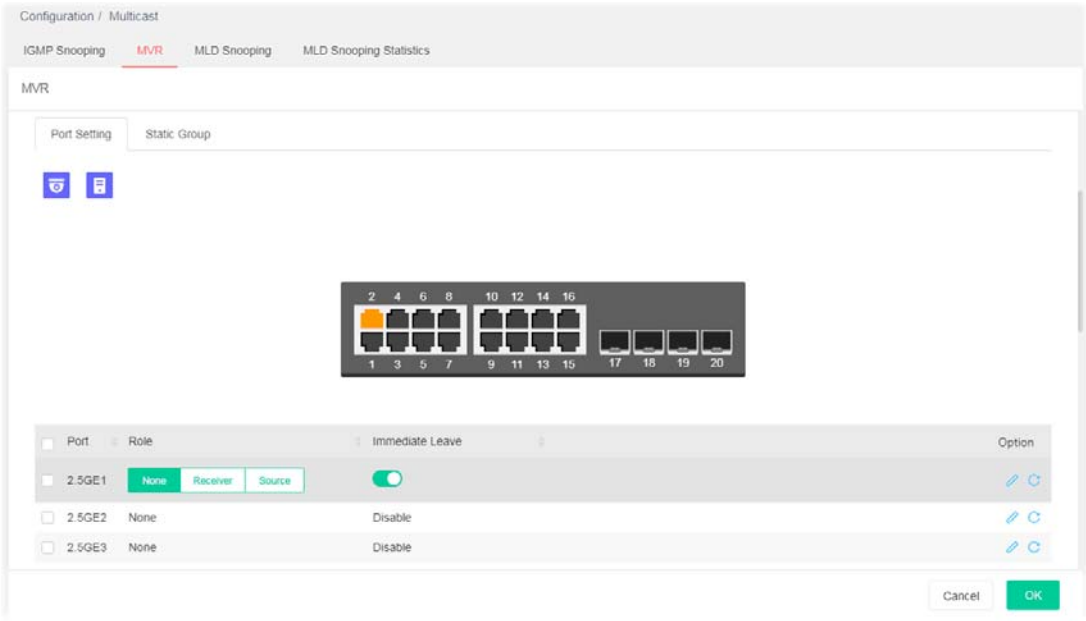
It is necessary to specify destination port and source port (GE/LAG) for Vigor system to perform MVR operation.




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.<br>- Clear current settings and return to factory default settings. |

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



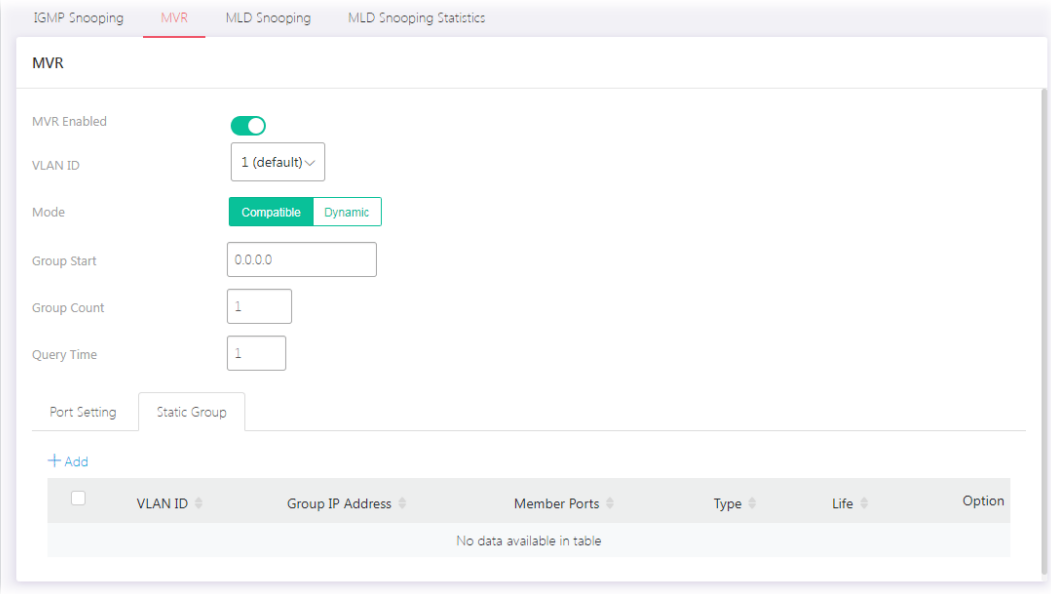

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Port** | Each port can be set as Receiver or Source port respectively. If you do not satisfy with the port setting, simply click to make the modification. |
| **Role** | **None –** Noting will be happed to the selected LAN port in MVR operation.<br>**Receiver –** The selected port will be treated as destination port which will receive multicast data from the multicast server.<br>**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.<br>**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

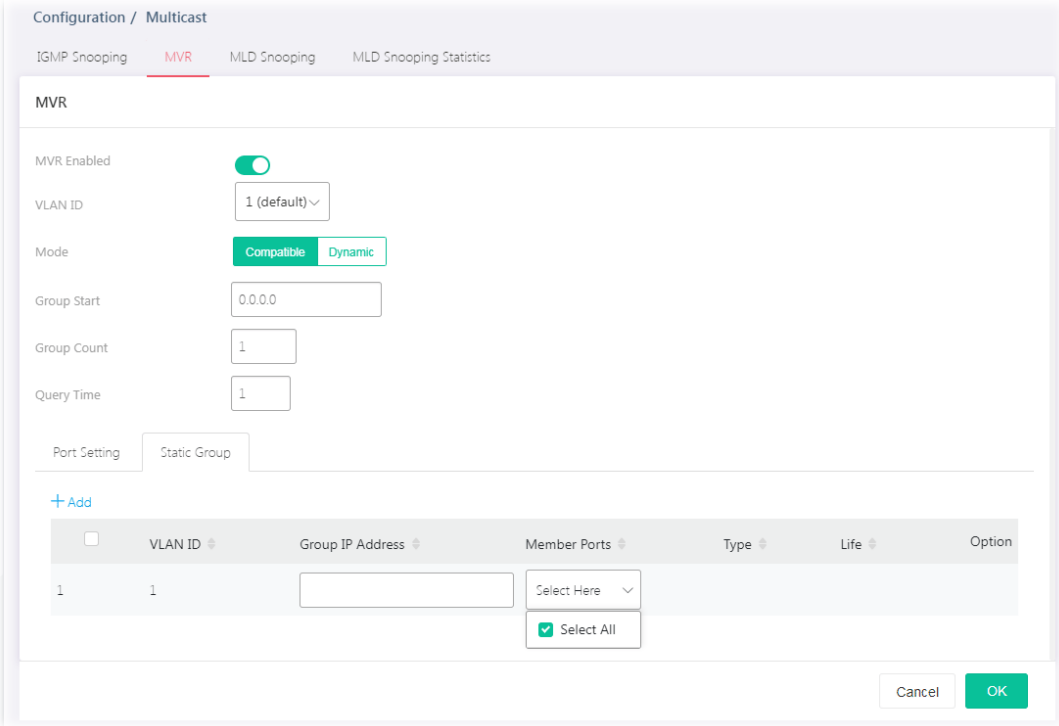
The MLD static group is allowed to assign a VLAN/port as a specific IP multicast member. Every IP multicast stream that belongs to the specified group IP address will be forwarded to the specified port/VLAN member.




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 Address** | Displays the IP address(es). |
| **Member** | 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.

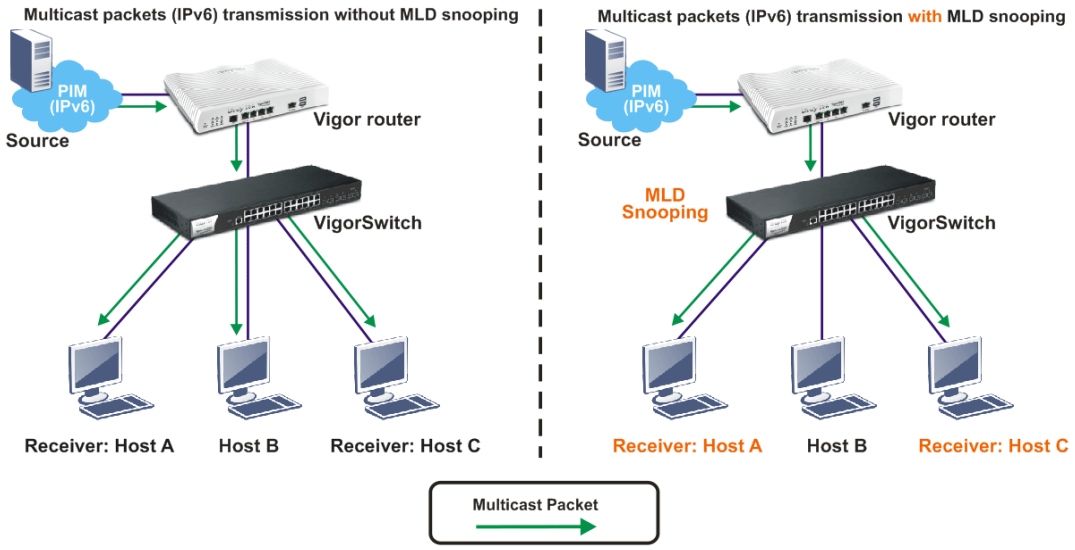



Available settings are explained as follows:

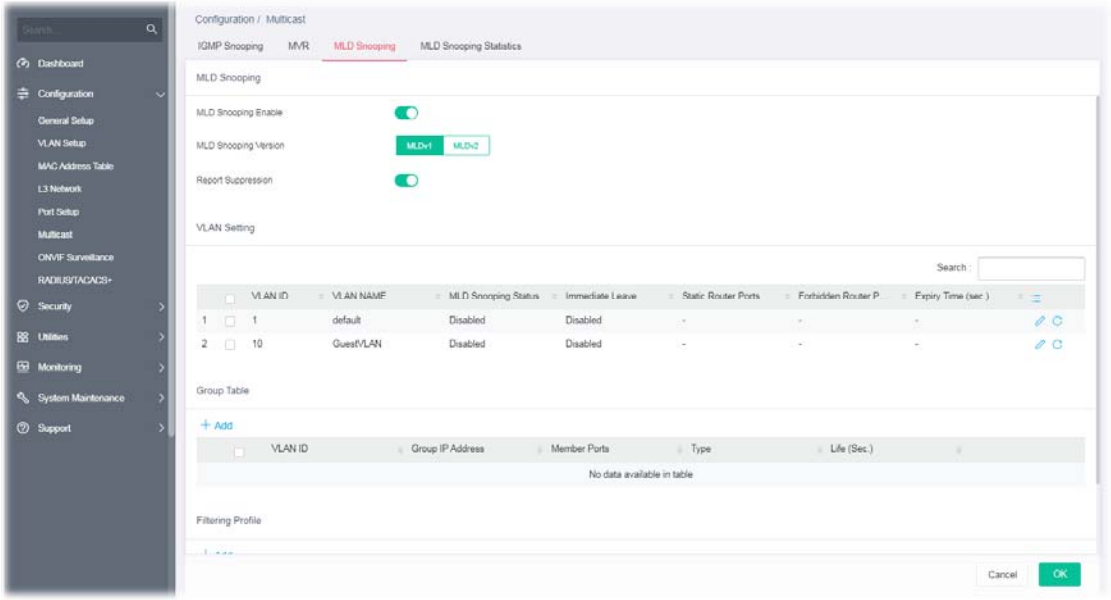
| Item | Description |
|---|---|
| **VLAN ID** | Display the ID number of the VLAN. |
| **Group Address** | Define a range of IP address(es) with the format of "xxx.xxx.xxx.xxx – xxx.xxx.xxx.xxx". |
| **Member Ports** | Choose GE/LAG port to be grouped under the selected VLAN. |
| **OK** | Save the settings.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

## 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



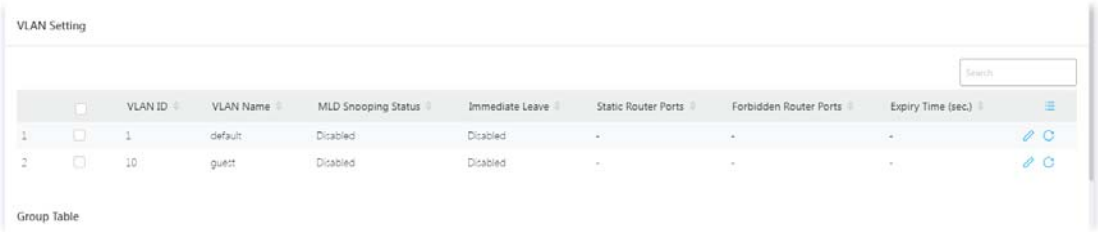

Available settings are explained as follows:

| Item | Description |
|---|---|
| **MLD Snooping Enable** | **Enable / Disable** – Click the toggle to enable / disable this function.<br>- means “Enable”.<br>- means “Disable”. |
| **MLD Snooping Version** | VigorSwitch supports two versions of MLD snooping.<br>**MLDv1 –** When it is selected, VigorSwitch will detect packets controlled by MLDv1 and *bridge* the traffic to IPv6 destination defined with multicast address(es).<br>**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.<br>**Enable / Disable** – Click the toggle to enable / disable this function.<br> - means “Enable”.<br> - means “Disable”. |
| **OK** | Save the settings. |

## II-6-3-2 VLAN Setting

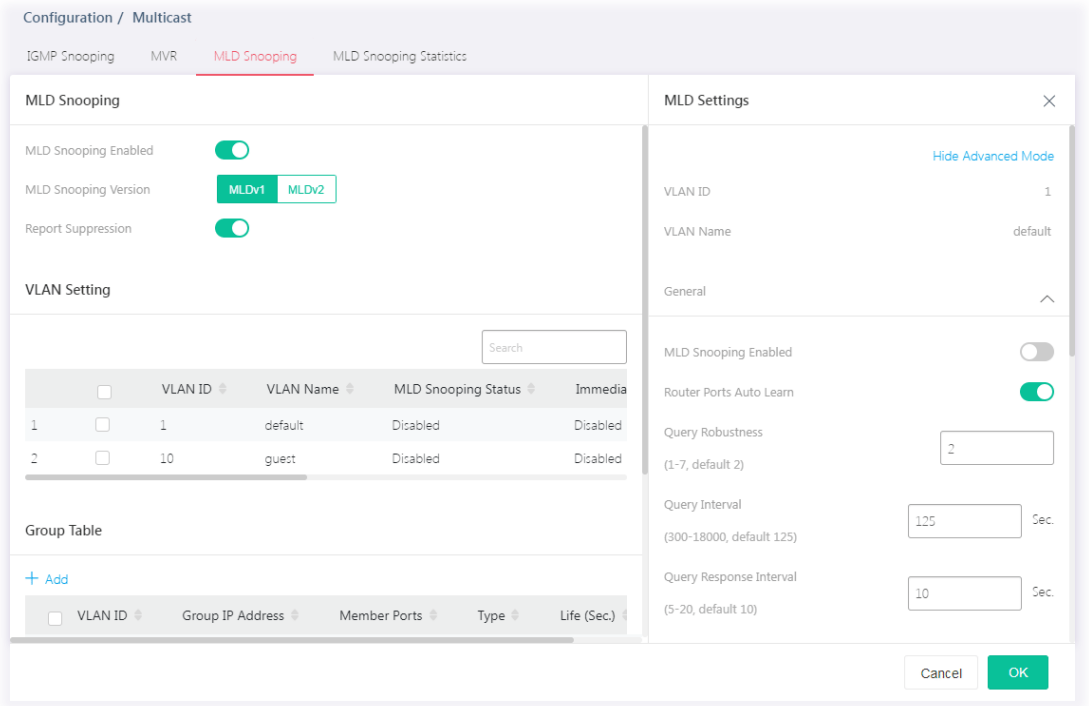
This page allows you to enable/disable MLD snooping function, select snooping version, and enable/disable snooping report suppression.




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:

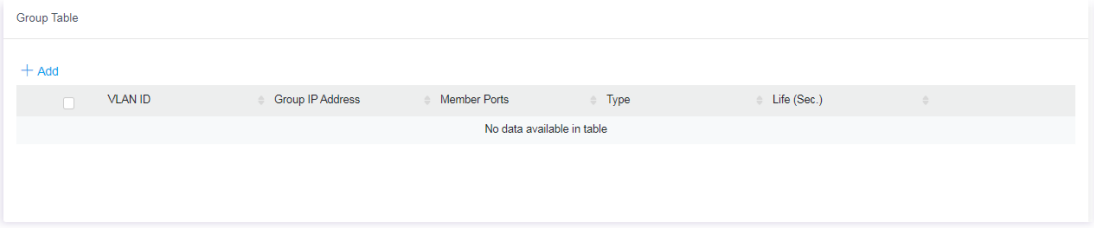
| Item | Description |
|---|---|
| **MLD Setting** | |
| **Show / Hide Advanced Mode** | Click to display or hide the advanced settings. |
| **VLAN ID** | Displays the VLAN ID number of the VLAN profile. |
| **VLAN Name** | Displays the name of the VLAN profile. |
| **General** | **MLD Snooping Enable** – Click the toggle to enable / disable this MLD snooping function.<br>- means “Enable”.<br>- means “Disable”. |
| **Below shows settings for Advanced Mode** | |
| **Router Ports Auto Learn** | Click 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. Click 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.<br>**+Add** - Click to create a new group.<br>• **Group IP Address** - Specify the IPv6 multicast address you wish to assign for the static group (defined in VLAN ID).<br>• **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.<br>**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.<br>**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

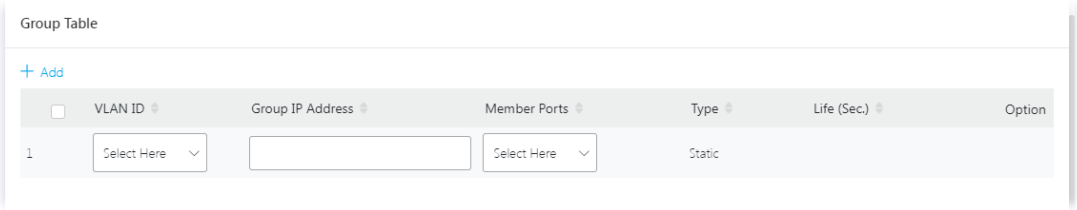
This page shows currently known and dynamically learned by IGMP snooping or shows the assigned IPv4 multicast address group in operation.




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.<br>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. |

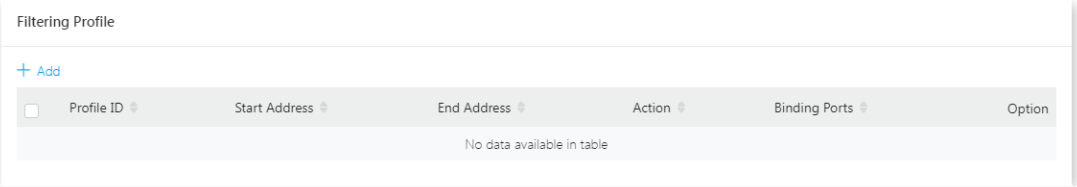
After finishing this web page configuration, please click **OK** to save the settings.

## 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.

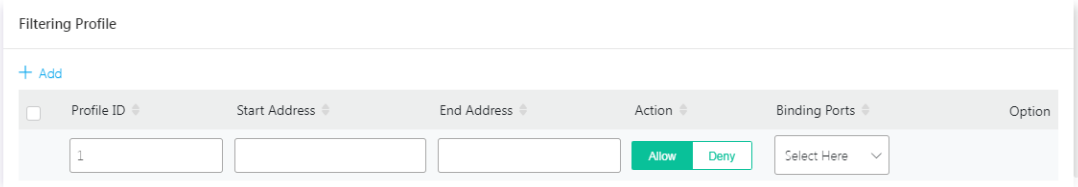
In addition, such filtering profile is only effective for controlling the query for multicast. It has nothing to do with the general IGMP query.




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.



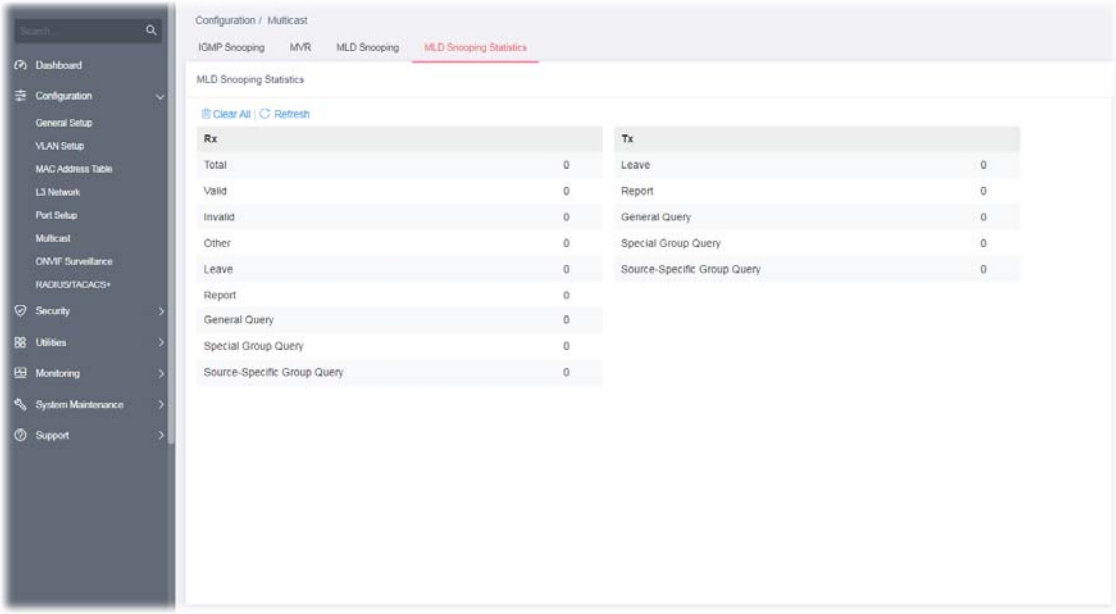

Available settings are explained as follows:

| 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.<br>**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-6-4 MLD Snooping Statistics

This page displays the MLD snooping statistics.

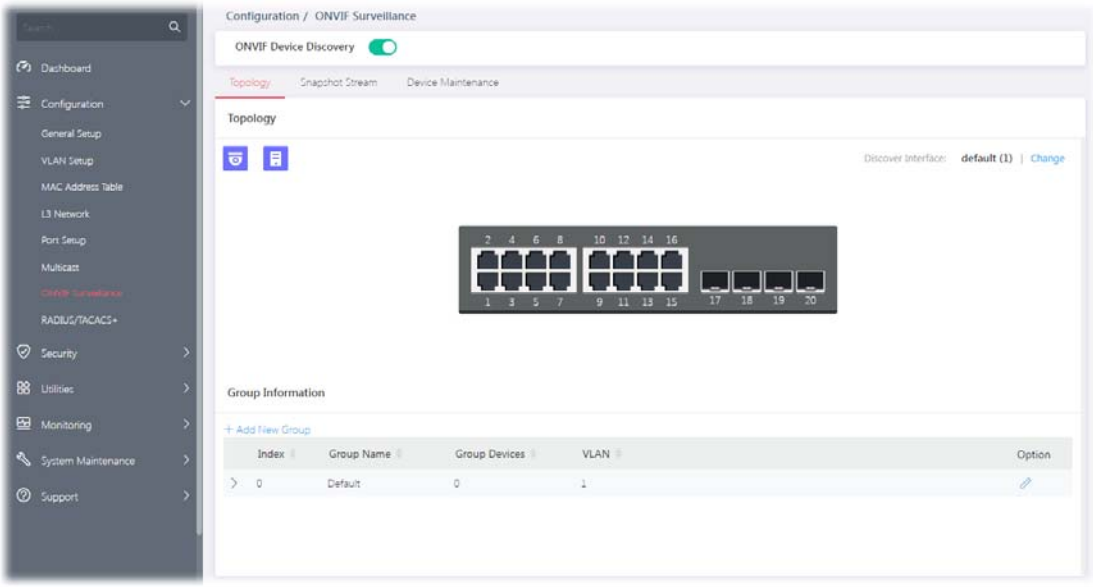


# II-7 ONVIF Surveillance

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:

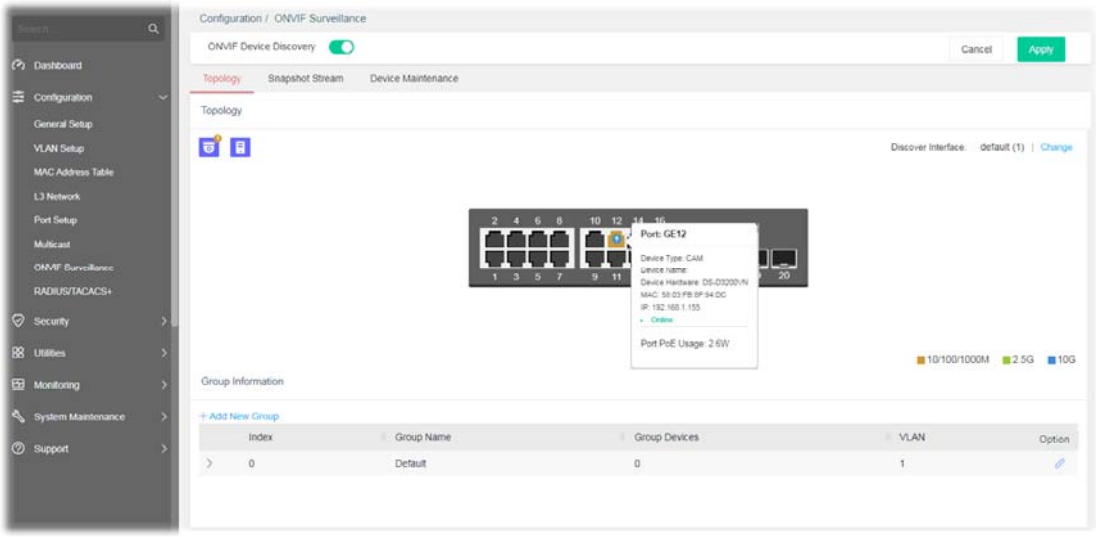
- Integrate the ONVIF device and surveillance network
- Centralize management of IP video products
- View video images directly on VigorSwitch WUI
- Offer remote IP video products maintenance



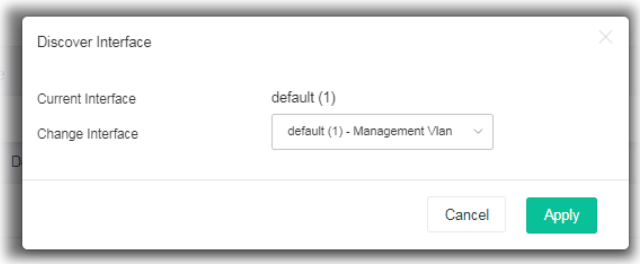

Switch the toggle to enable the **ONVIF Device Discovery** function. Then click **Apply**.

## 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.

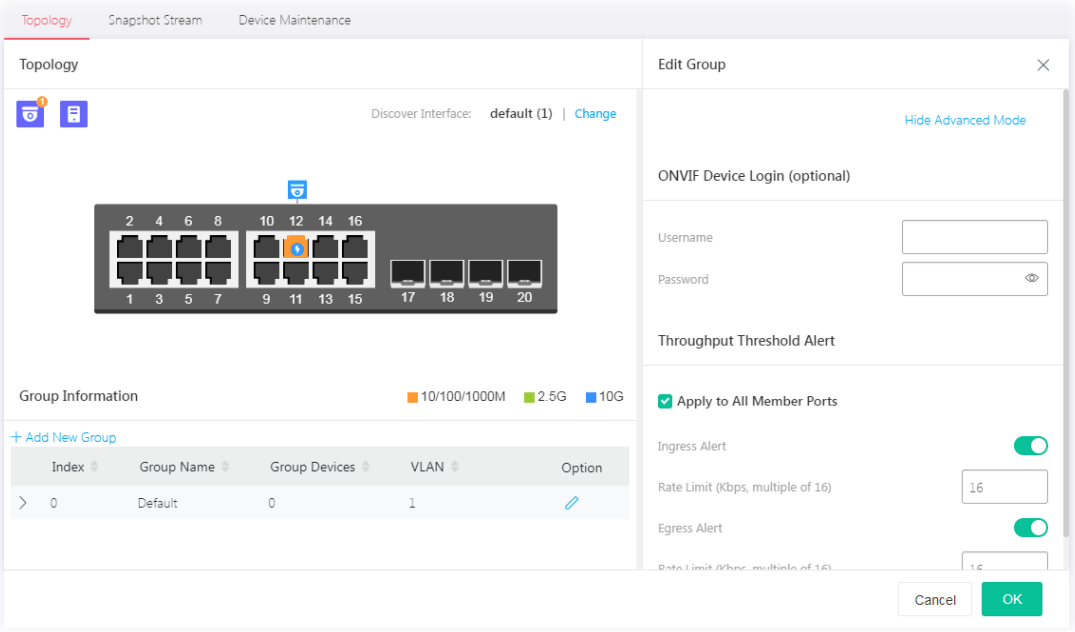



Available settings are explained as follows:

| 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.<br>**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.<br>  |
| **+Add New Group** | A group can contain one (IP camera or NVR, as group leader) to several devices (IP cameras as group devices).<br>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.

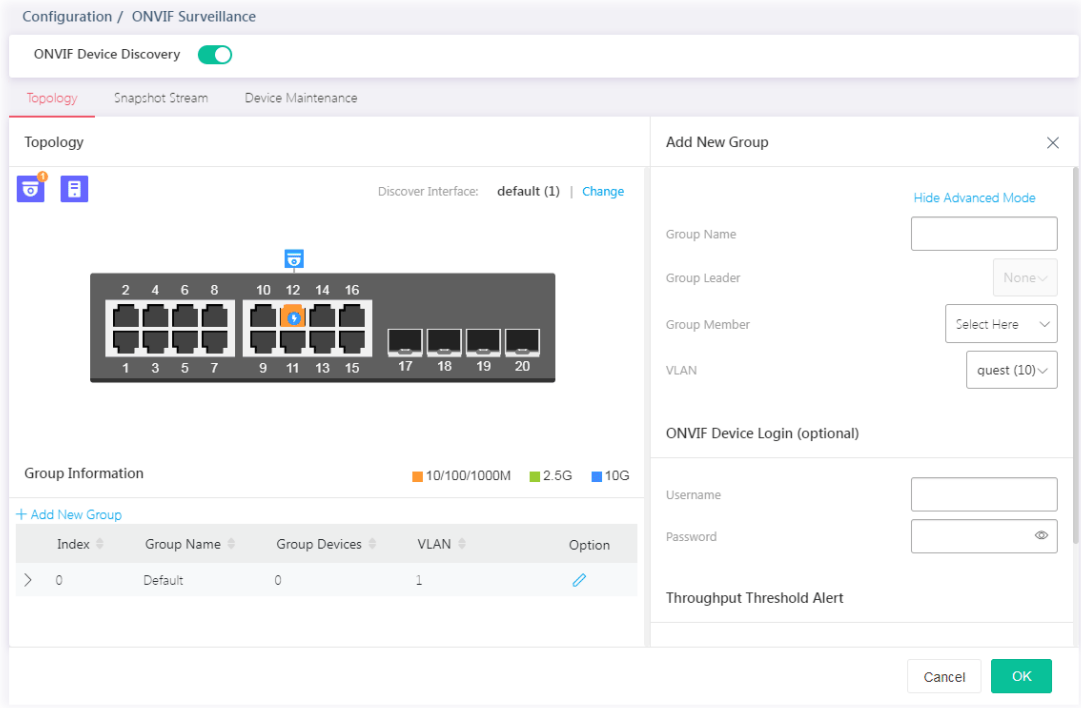



Available settings are explained as follows:

| 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.<br>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.<br>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.<br>**Rate Limit** - Enter the ingress rate as a threshold to send mail alert. |
| **Egress Alert** | Toggle the switch to enable the function.<br>**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:

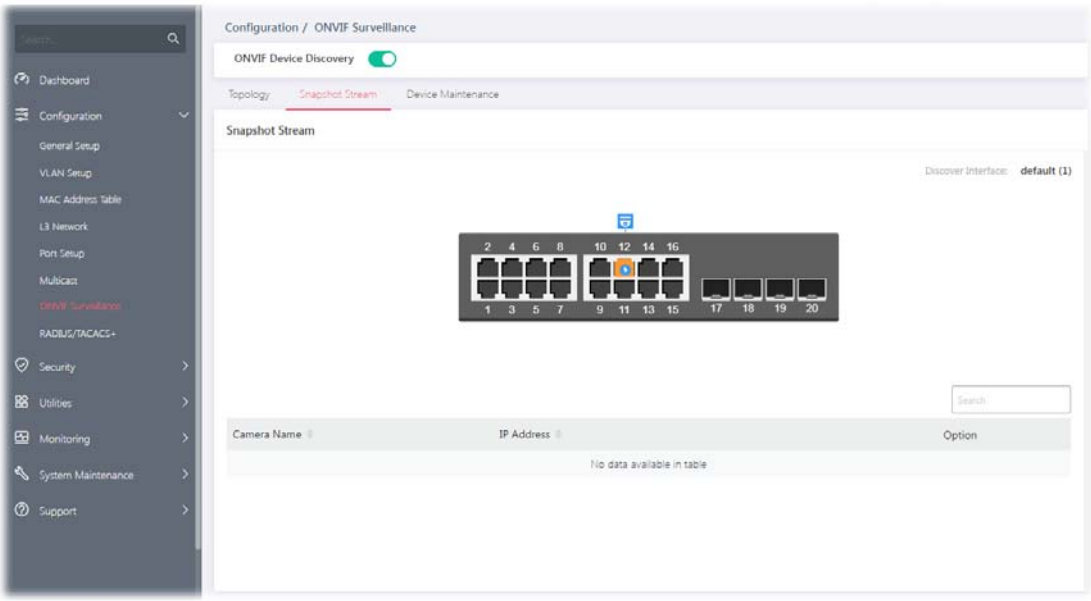
| Item | Description |
|---|---|
| **Add New Group** | |
| **Show / Hide Advanced Mode** | Click to display or hide the advanced settings. |
| **Group Name** | Enter the name of a group. |
| **Group Leader** | The system will detect the NVR or IP cameras, and list them on the field of NVR or Group Leader. |
| **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. |
| **ONVIF Device Login (optional)** | |
| **Username / Password** | Enter a name / password as the default value.<br>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.<br>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.<br>**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.<br>**Rate Limit** - Enter the ingress rate as a threshold to send mail alert. |

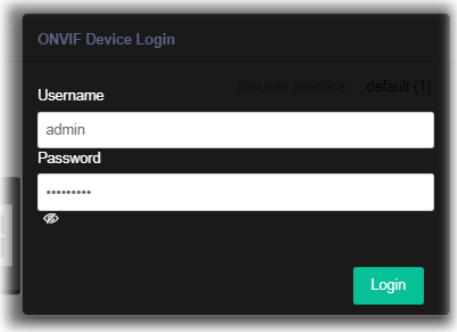
After finishing this web page configuration, please click **OK** to save the settings.

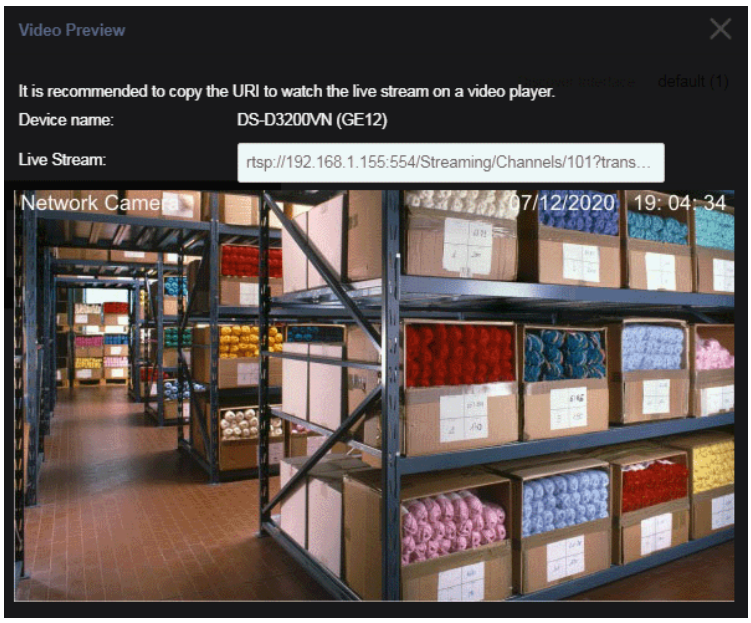
## II-7-2 Snapshot Stream

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



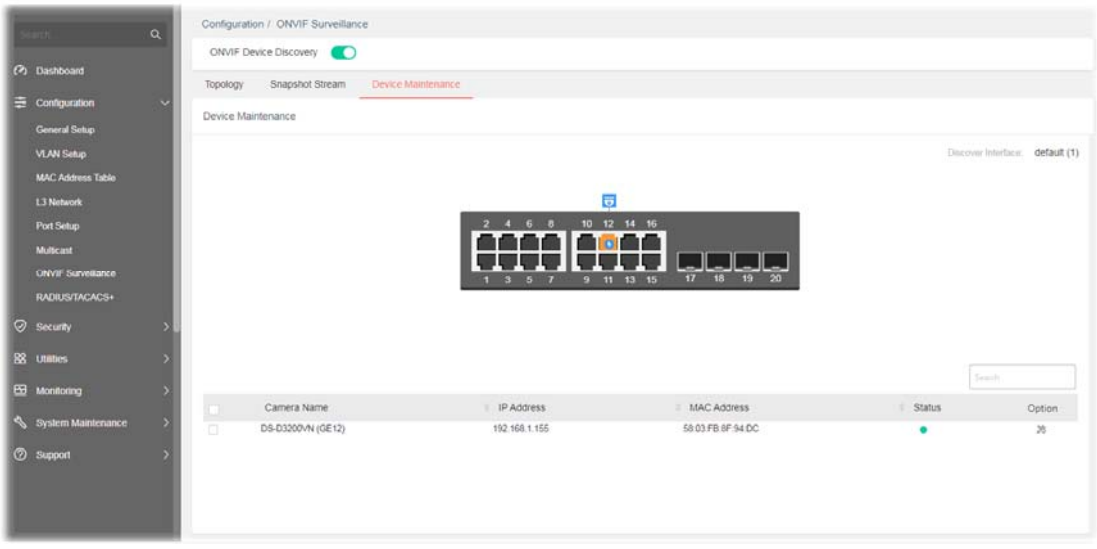

Available settings are explained as follows:

| 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.<br>  <br>**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.<br>A pop-up window (Video Preview) appears to display a live image on the screen.<br>  |

## 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.

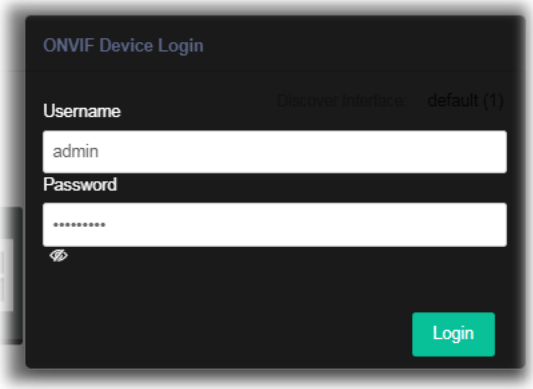



Available settings are explained as follows:

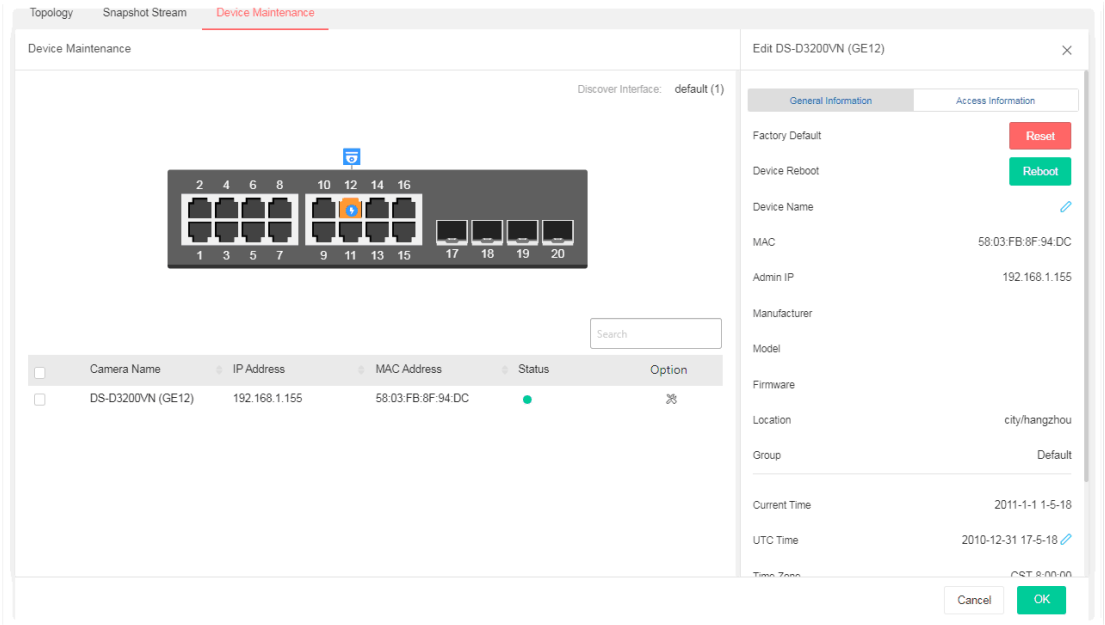
| Item | Description |
|---|---|
| **Device Maintenance** | |
| **Camera Name** | Displays the device name of the IP camera. |
| **IP Address** | Displays the IP address of the IP camera. |
| **MAC Address** | Displays the MAC address of the IP camera. |

| | |
|---|---|
| **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. |

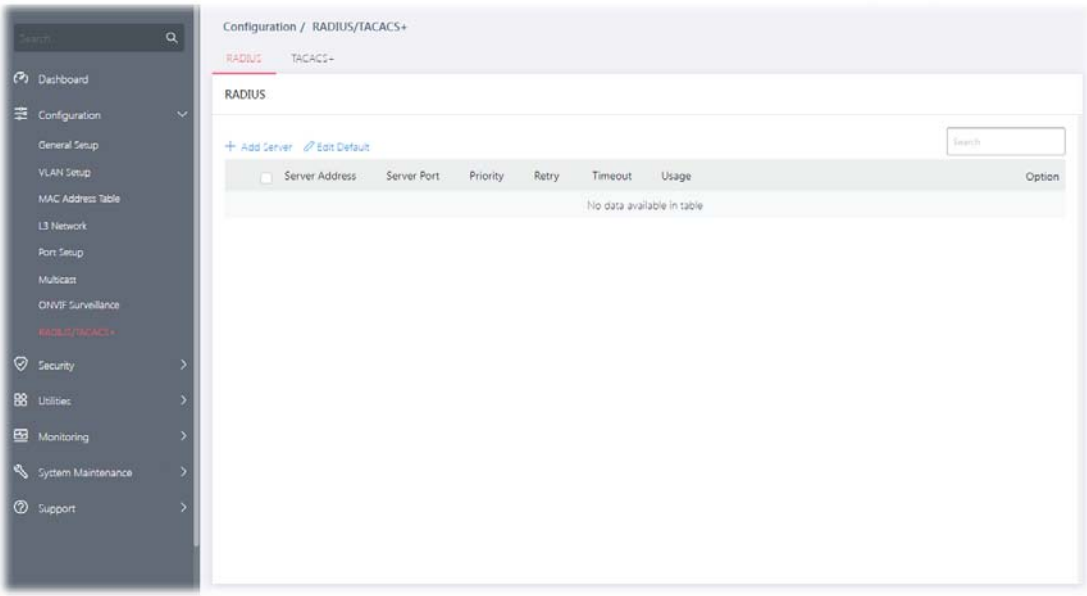
| | |
|---|---|
| **Firmware** | Displays the firmware version used by the device. |
| **Location** | Displays the location of the device. |
| **Group** | Displays the name of the group. |
| **Current Time** | Displays the time set for the device. |
| **UTC Time** | Display the time and date information 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** | Click the toggle to enable / disable this function.<br> - means “Enable”.<br> - means “Disable”.<br>**Failure Action** - Configure the power behavior for each LAN port.<br>• **Power Cycle -** Once the device is offline, Vigorswitch will power off the device and then power on the device again.<br>• **Power Off** - When the device is offline, power off the device immediately.<br>• **Nothing** - When the device is offline, no action will be performed.<br>**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.<br>**Mail Alert** - Click the toggle to enable / disable this function. When the device is offline, Vigor system will send an alert mail to notify the recipient.<br>• **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.<br>When the device is offline, no action will be performed. |
| **Access Information** | |
| **Mode** | Change the connection mode for this device.<br>**Static -** When it is selected, you have to enter value for network setting manually for the IP device.<br>• **IP Address** - Enter an IPv4 address for the IP device.<br>• **Prefix Length** - Specify the subnet mask for the IP address.<br>• **Gateway** - Enter the IPv4 address for the gateway.<br>• **DNS Server1/2** - Enter the IP address for primary / secondary DNS server.<br>**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.<br>• **Hostname** - Display the hostname of the DHCP server. |
| **Zero Configuration** | Click the toggle to enable / disable this function.<br>**Enable -** The network settings for the IP device will be configured automatically.<br>**Disable -** The network settings for the IP device must be configured |

| | |
|---|---|
| | manually. |
| **HTTP Port** | Click the toggle to enable / disable this function.<br>**Enable -** Click it to enable the HTTP port configuration and enter a port value if required.<br>**Disable -** Disable the HTTP port configuration. |
| **HTTPS Port** | Click the toggle to enable / disable this function.<br>**Enable -** Click it to enable the HTTPS port configuration and enter a port value if required.<br>**Disable -** Disable the HTTPS port configuration. |
| **RTSP Port** | Click the toggle to enable / disable this function.<br>**Enable -** Click it to enable the RTSP port configuration and enter a port value if required.<br>**Disable -** Disable the RTSP port configuration. |

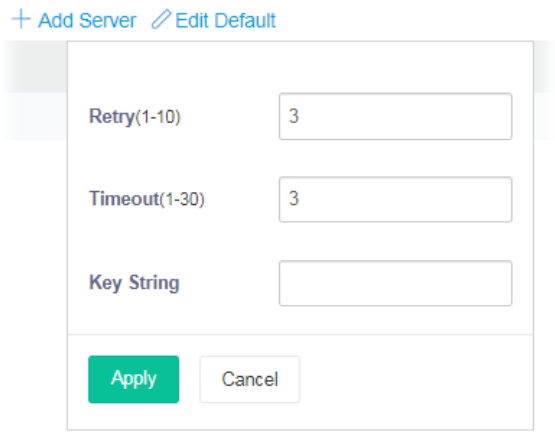
# II-8 RADIUS/TACACS+

## II-8-1 RADIUS

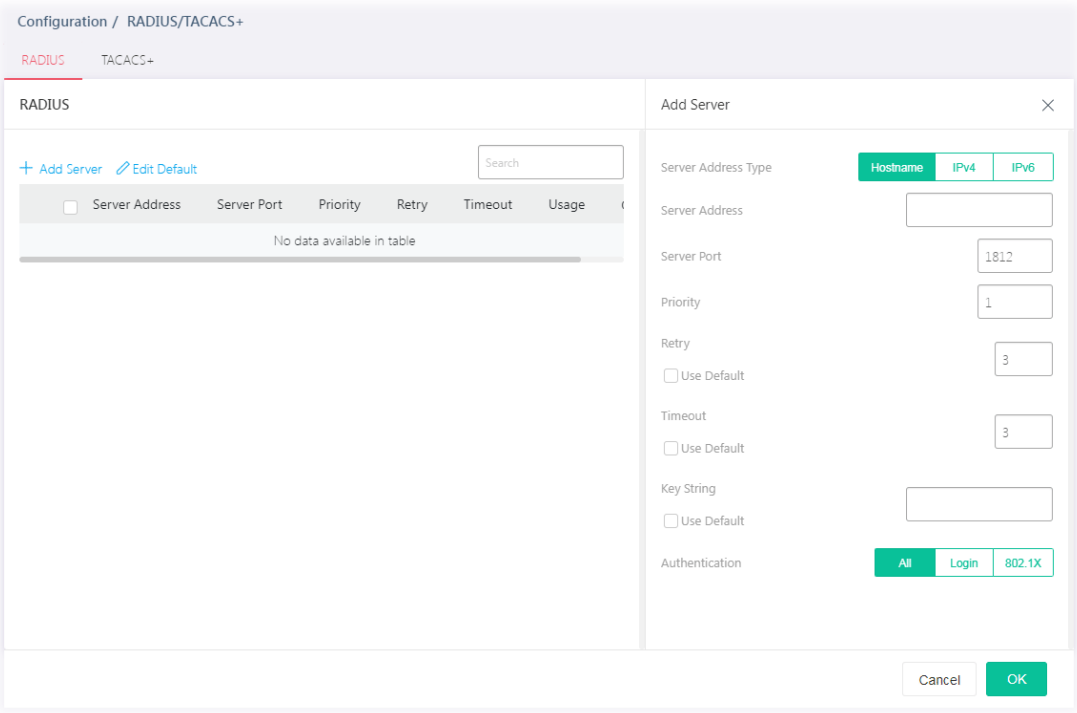
This page allows the network administrator to add and configure multiple RADIUS servers.




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.<br>  |

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



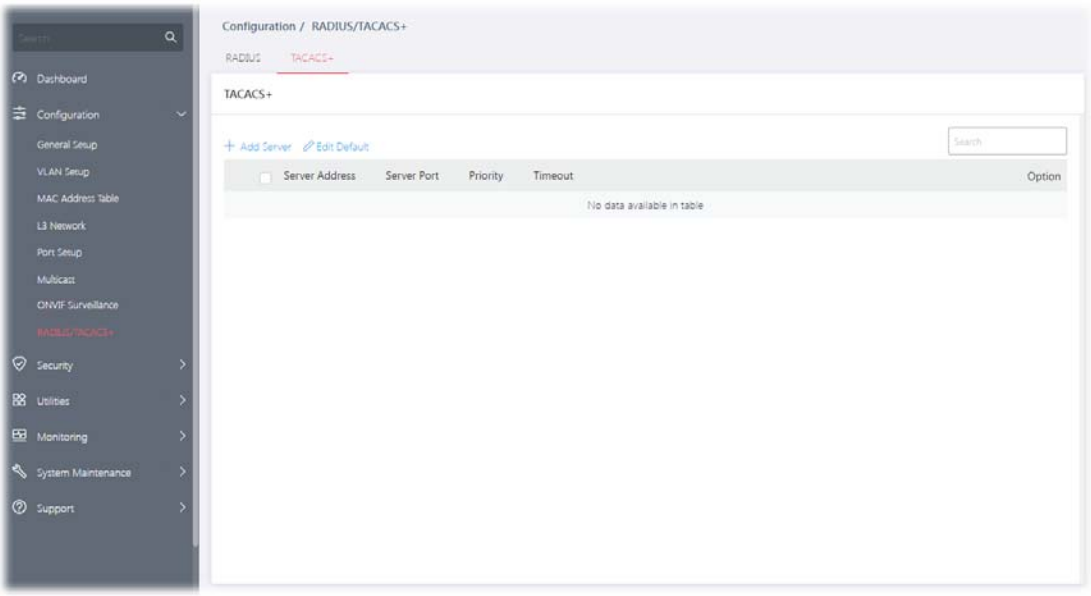

Available settings are explained as follows:

| 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.<br>• Hostname<br>• IPv4<br>• 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.<br>**Use Default** - Use the default value. |
| **Timeout** | Set the time (in seconds) before this server being considered lost connection.<br>**Use Default** - Use the default value. |
| **Key String** | Enter the string used to encrypt and authenticate with RADIUS server.<br>**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.<br>• All<br>• Login<br>• 802.1X |
| **OK** | Save the settings. |

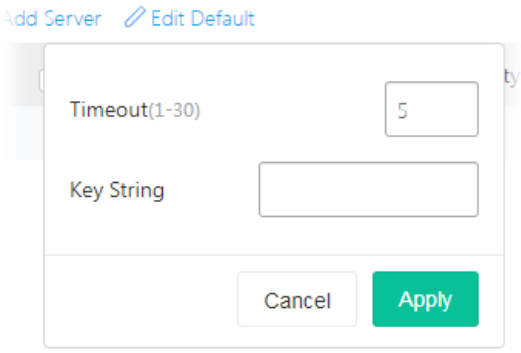
After finishing this web page configuration, please click **OK** to save the settings.

## II-8-2 TACACS+

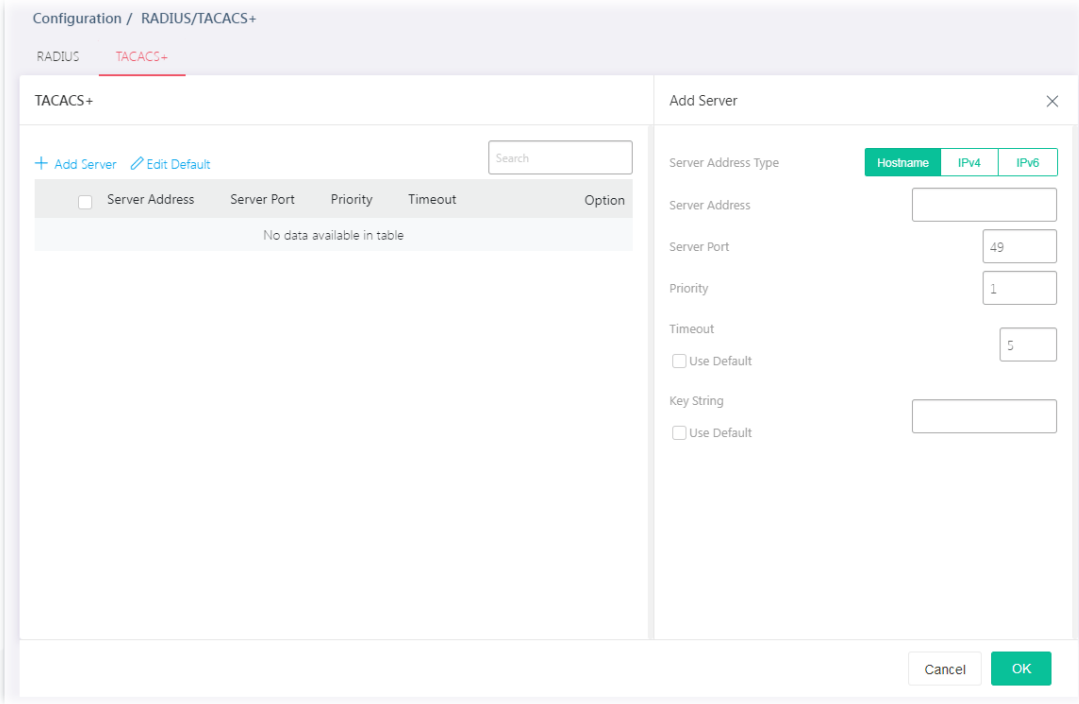
This page allows the network administrator to add and configure multiple TACACS+ server.




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.<br>  |

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.<br>• Hostname<br>• IPv4<br>• 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.<br>**Use Default** - Use the default value. |
| **Key String** | Enter the string used to encrypt and authenticate with TACACS+ server.<br>**Use Default** - Use the default setting. |
| **OK** | Save the settings. |

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

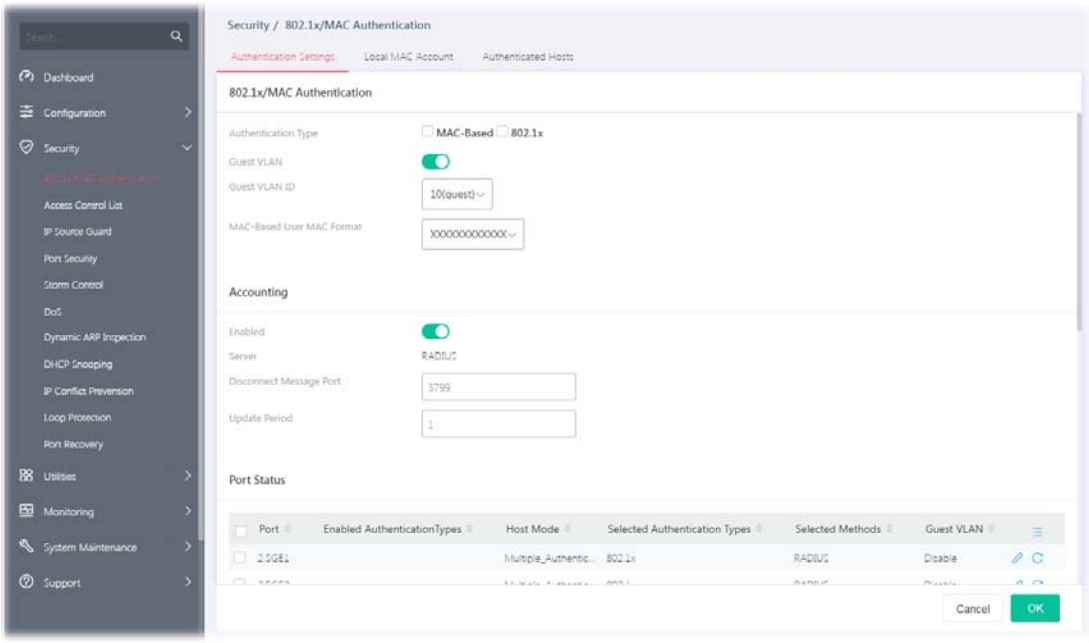
This page is left blank.

# 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.

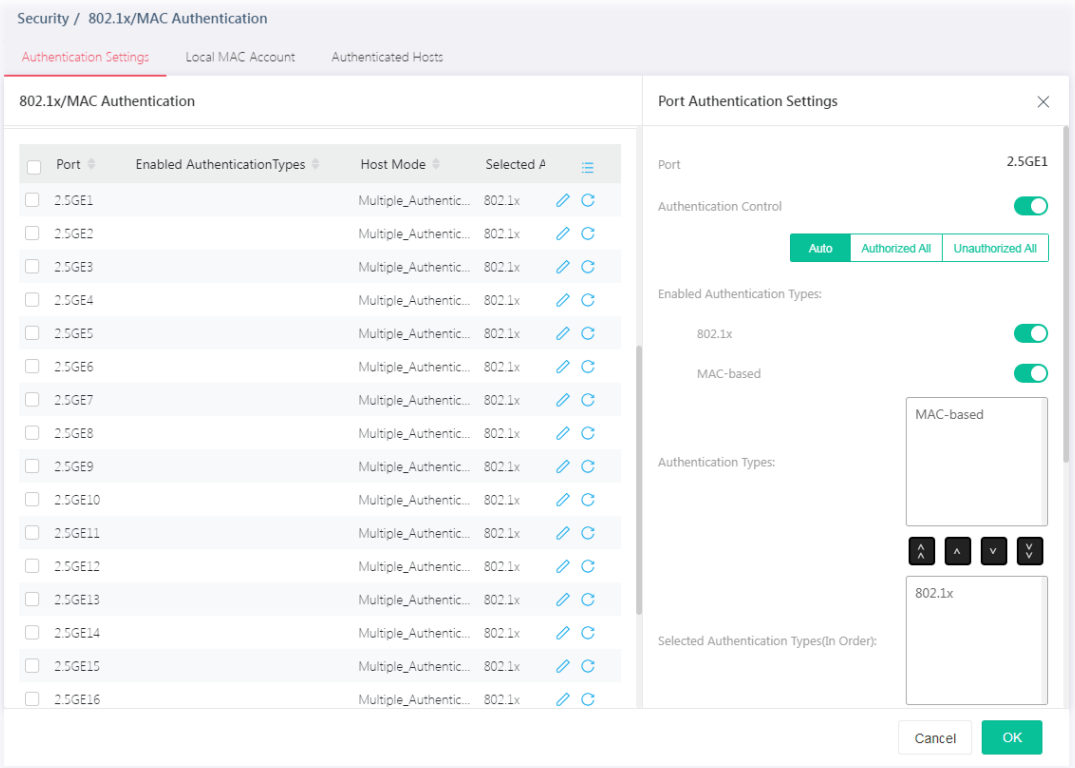



Available settings are explained as follows:

| 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.<br>• MAC-Based<br>• 802.1x |
| **Guest VLAN** | Click the toggle to enable/disable a Guest VLAN for those who have not successfully authenticated with any given methods.<br>- means "Enable". If enabled, specify a VLAN ID number.<br>- means "Disable".<br>**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** | |
| **Enable** | Click the toggle to enable / disable this function.<br>**Server** - Displays the type of the server. |

| Port Status | |
|---|---|
| **Port** | Displays the index number of the GE ports.<br>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** | Click the toggle to enable / disable this function.<br>- means “Enable”.<br>- means “Disable”. |

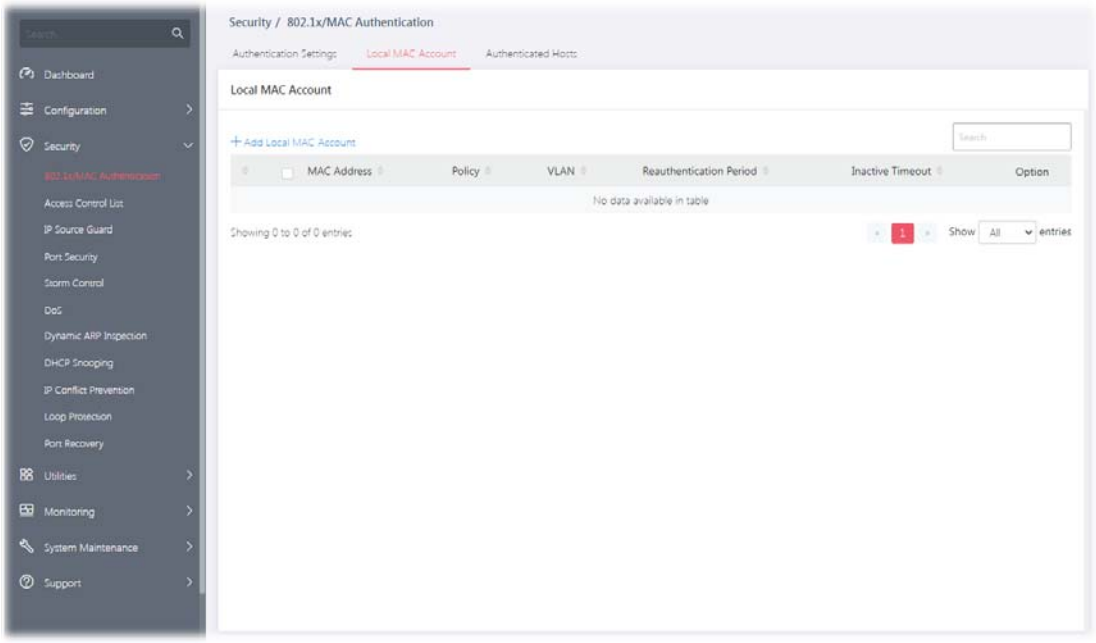
| | |
|---|---|
| | If enabled, select **Auto**, **Authorized All** or **Unauthorized** All as the control mode. |
| **Enable Authentication Types** | Select 802.1x and/or MAC-based authenticate method for host connecting to this port.<br>• 802.1x<br>• MAC-based |
| **Authentication Types** | Displays 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.<br>**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.<br>**Single Host** - Only one host can be authenticated, and access the port. |
| **Advanced Mode** | |
| **Guest VLAN** | Click 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.<br>**Disabled** - Switch will ignore the VLAN assignment from the RADIUS server and keep the original VLAN of the host.<br>**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.<br>Click the toggle to enable / disable this function. If enabled, specify the time setting.<br>**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.<br>Later, after the time period set in this field, the host will be allowed to perform authentication again. |
| **Supplicant Timeout** | Set a period of time for the maximum number of EAP requests will be sent.<br>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.

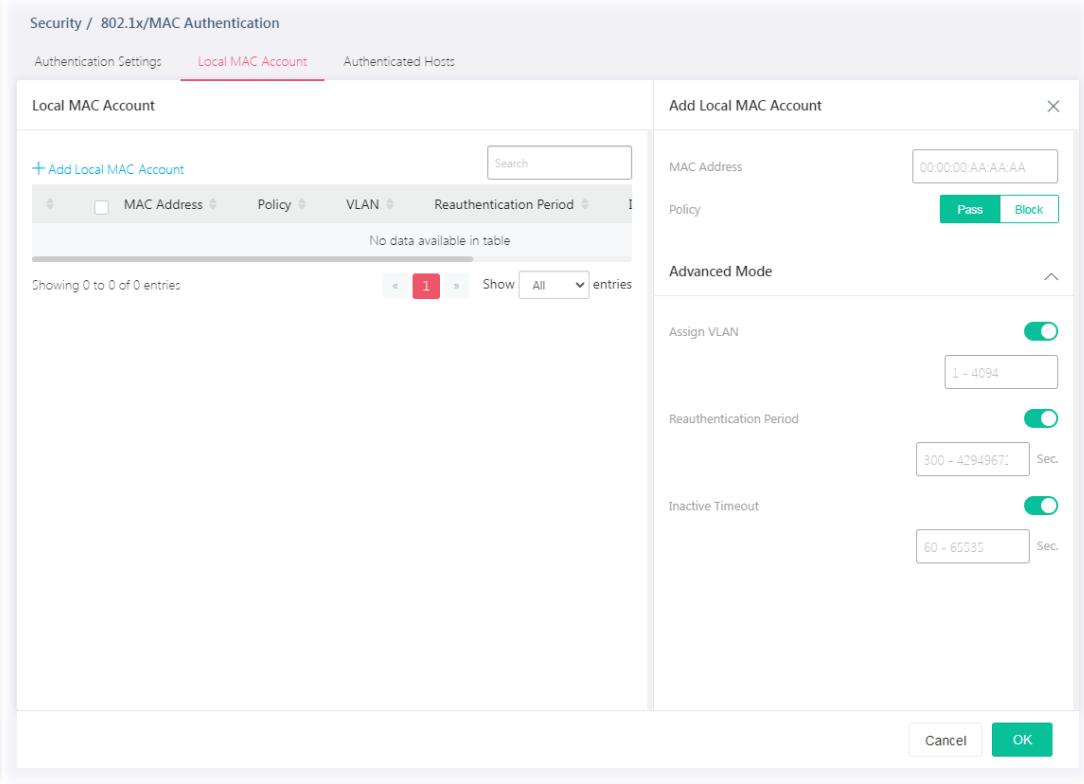



Available settings are explained as follows:

| 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** | Displays the time this account is required to be authenticated again. |

| | |
|---|---|
| **Period** | |
| **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.



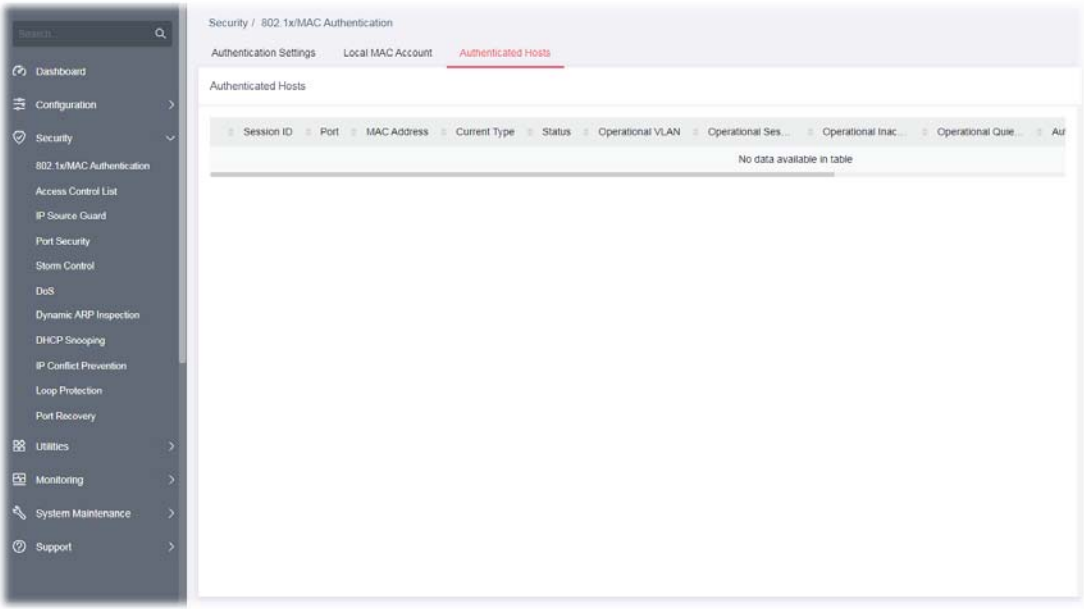

Available settings are explained as follows:

| 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.<br>**Block** - The host specified above will not be authenticated by VigorSwitch.<br>If **Pass** is selected, advanced mode will be shown below. |
| **Advanced Mode** | |
| **Assign VLAN** | Click the toggle to enable / disable this function.<br> - means “Enable”.<br> - means “Disable”.<br>Specify which VLAN will be assigned by the host of this account. |
| **Reauthentication Period** | Click the toggle to enable / disable this function.<br>Set the time this account is required to be authenticated again after authentication has taken place. |
| **Inactive Timout** | Click the toggle to enable / disable this function.<br>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.



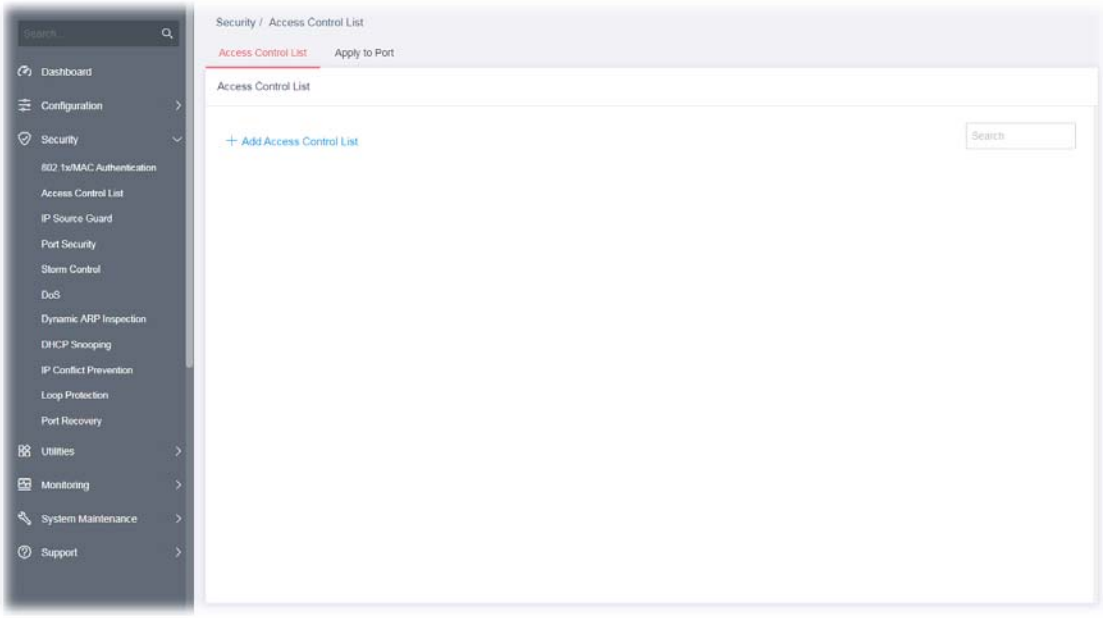
# III-2 Access Control List

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.

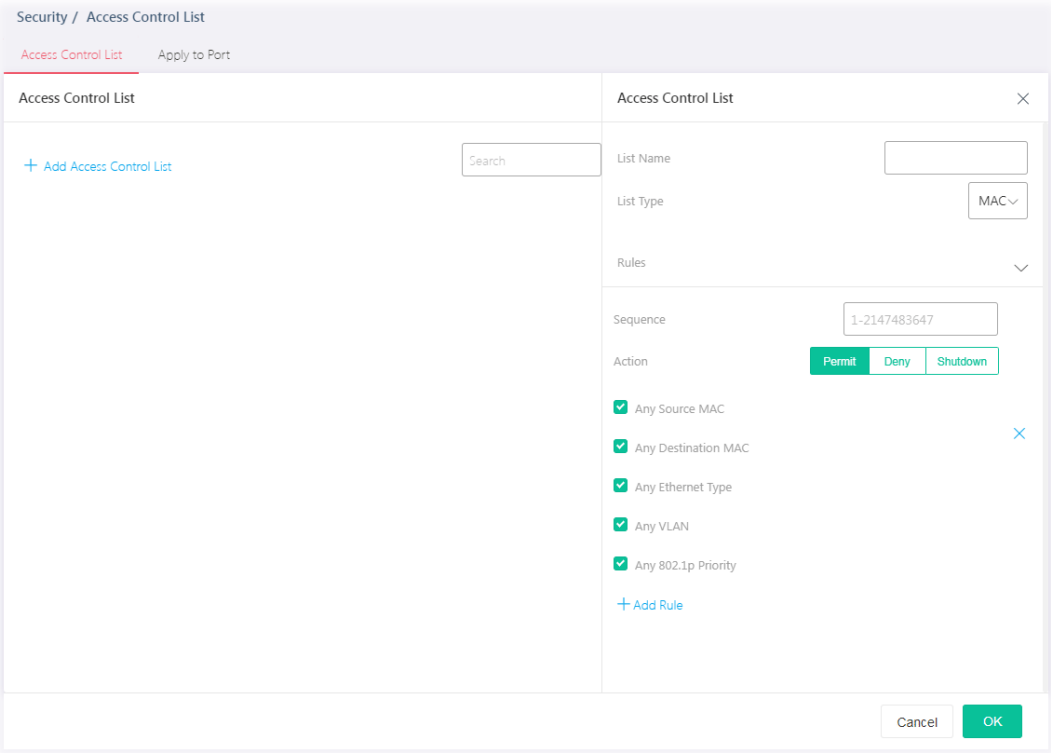
You may provide filtering/matching criteria for one or more packet characteristics (such as Source/Destination MAC, Ethertype, VLAN, 802.1p) for this ACE to identify the packet.

## 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.

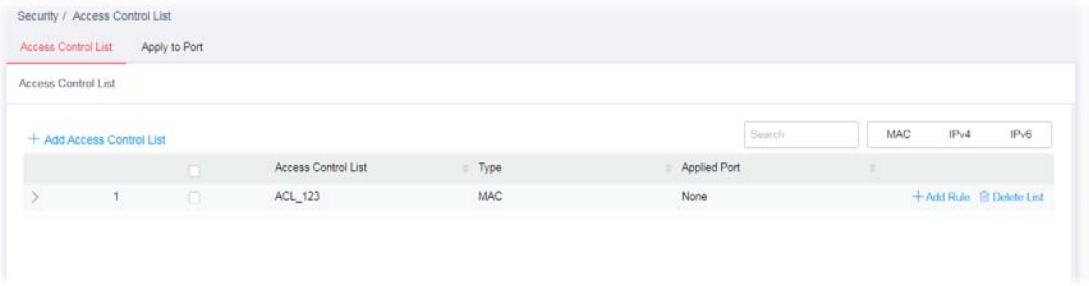


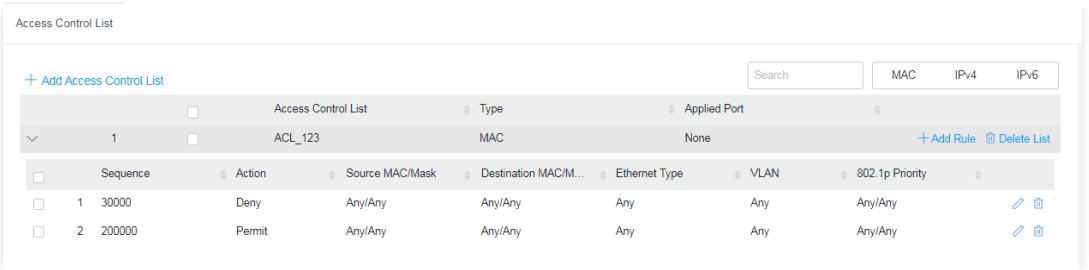

Available settings are explained as follows:

| 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.<br>• **Permit**<br>• **Deny**<br>• **Shutdown** |
| **Any Source MAC** | If disabled, please enter IP address with the subnet mask.<br> |
| **Any Destination MAC** | If disabled, please enter IP address with the subnet mask. |
| **Any Ethernet Type** | Specify Ethernet type for filtering. Select **Any Ethernet**.<br>Or, enter the value with the format of “0x600 ~ 0xFFF”. |

| | |
|---|---|
| | Any Ethernet<br>Type (0x600-0xFFFF) |
| **Any VLAN** | Specify VLAN profile for filtering. Select **Any VLAN**.<br>Or, enter a VLAN number. The packets coming from the VLAN specified here will be filtered by Vigor device.<br>Any VLAN (1-4094) |
| **Any 802.1p Priority** | Specify the 802.1p priority value for filtering. Select **Any 802.1p Priority**.<br>Or, enter a number from 0 to 7.<br>Any 802.1p Priority (0-7) / |
| **+Add Rule** | Click it to create a new ACE rule.<br>Each ACL profile can be added with 8 ACE rules. |

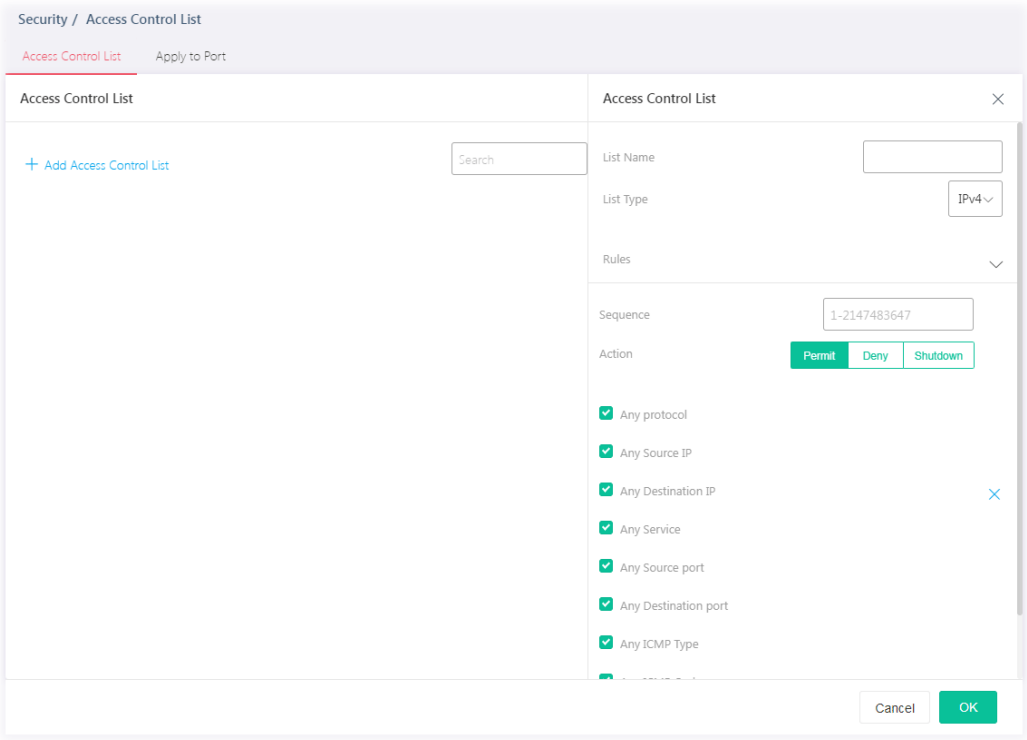
After finishing this web page configuration, please click **OK** to save the settings.



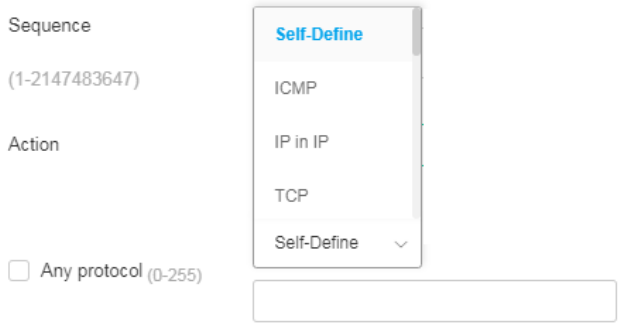
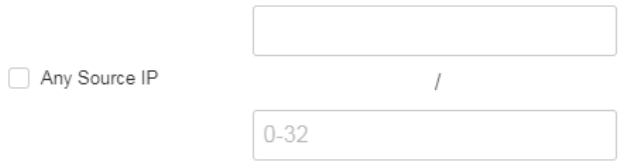
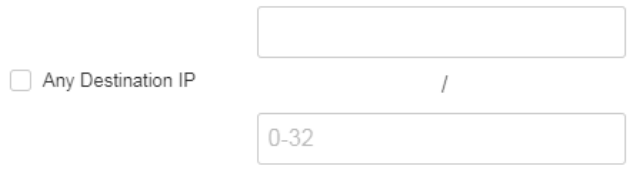
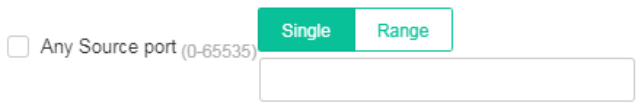
## List Type - IPv4

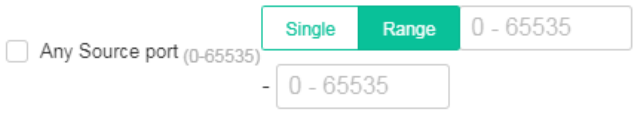
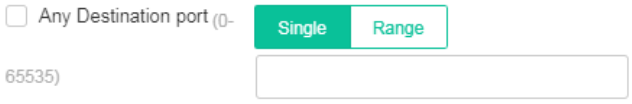
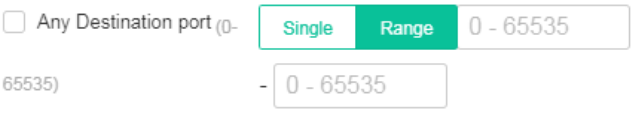
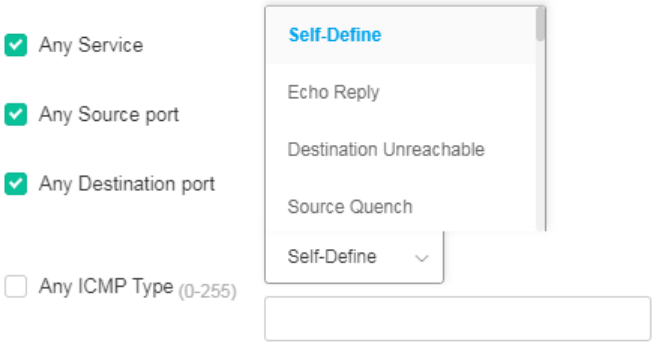
To create a new access control list, click the **+Add Access Control List** link to open the setting page.




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.<br>• **Permit**<br>• **Deny**<br>• **Shutdown** |
| **Any Protocol** | Specify the protocol for filtering.<br>**Any Protocol** – Default setting. All packets will be filtered.<br>**Self-Define** – Enter a number (0 – 255) to specify a protocol. For example, 1 means “Internet Control Message”; 6 means “Transmission Control”.<br>**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 |

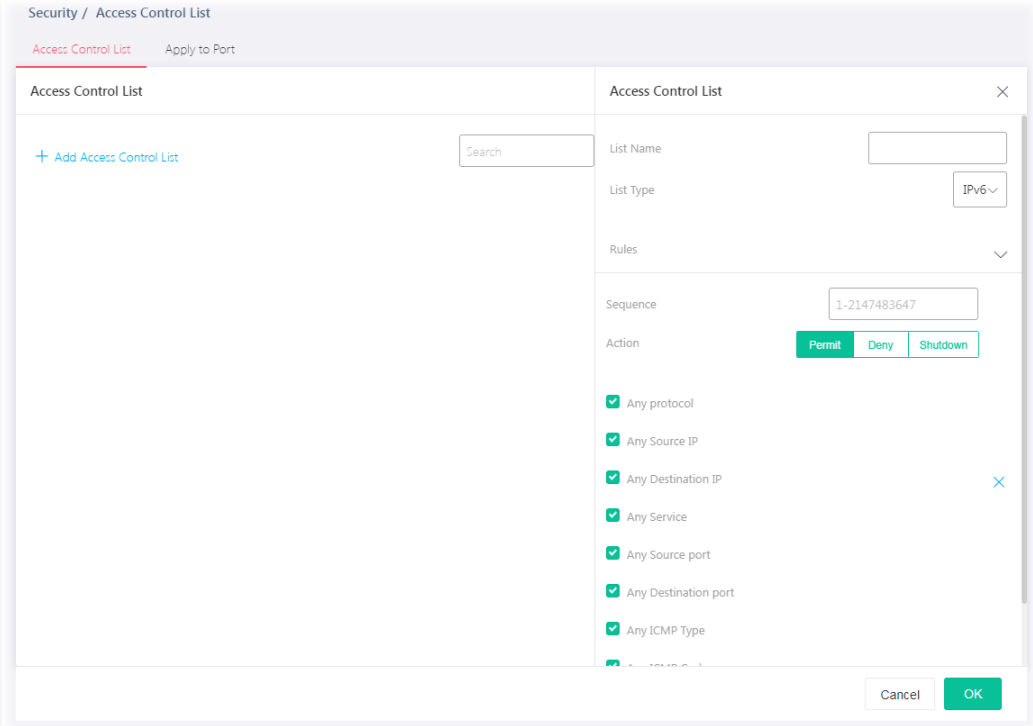
| | |
|---|---|
| | selected protocol will be filtered.<br>  |
| **Any Source IP** | Specify the source IPv4 address for filtering.<br>**Any Source IP** – Default setting. All packets will be filtered.<br>Select Any Source IP. Or, enter the IP address to filter the packets coming from that address.<br>  |
| **Any Destination IP** | Specify the destination IPv4 address for filtering.<br>**Any Destination IP** – Default setting. All packets will be filtered.<br>Select Any Destination IP. Or, enter the IP address to filter the packets coming from that address.<br>  |
| **Any Service** | **Any Service** – Default setting. All packets will be filtered.<br>**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.<br>**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.<br> |
| **Any Source Port** | Specify the source port number for filtering the packets.<br>**Any Source Port** – Default setting. All packets will be filtered.<br>Select Any Source Port. Or, enter the port number.<br>**Single** – Only the packets passing through the number defined here will be filtered.<br>  |

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

| | |
|---|---|
| | Each ACL profile can be added with 8 ACE rules. |

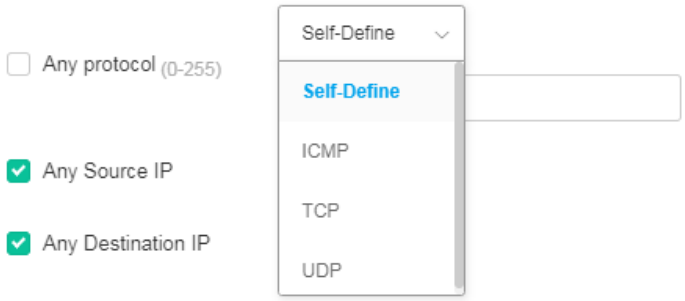
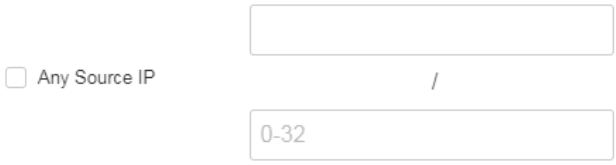
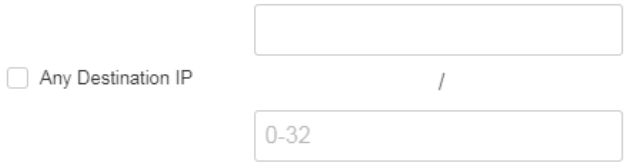
## List Type - IPv6

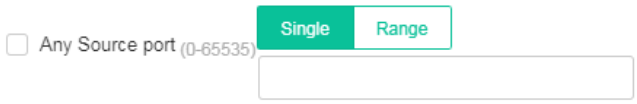
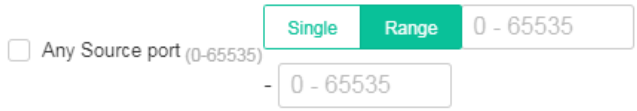
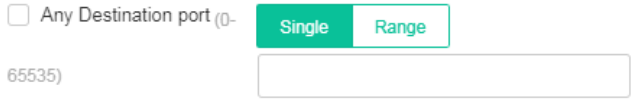
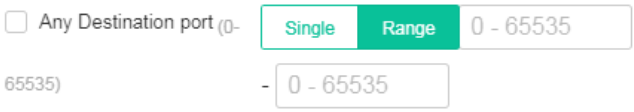
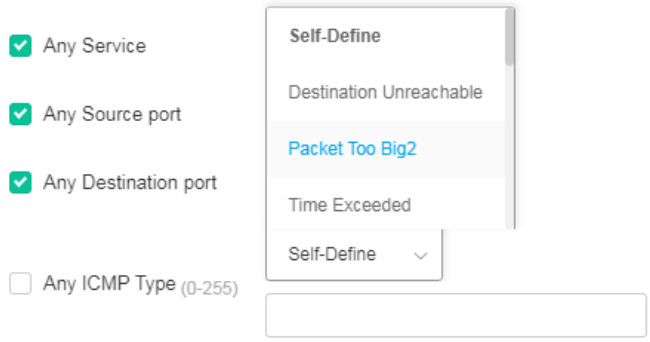
To create a new access control list, click the **+Add Access Control List** link to open the setting page.




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.<br>• **Permit**<br>• **Deny**<br>• **Shutdown** |
| **Any Protocol** | Specify the protocol for filtering.<br>**Any Protocol** – Default setting. All packets will be filtered.<br>**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.<br>  |
| **Any Source IP** | Specify the source IPv6 address for filtering.<br>**Any Source IP** – Default setting. All packets will be filtered.<br>Select Any Source IP. Or, enter the IP address to filter the packets coming from that address.<br>  |
| **Any Destination IP** | Specify the destination IPv6 address for filtering.<br>**Any Destination IP** – Default setting. All packets will be filtered.<br>Select Any Destination IP. Or, enter the IP address to filter the packets coming from that address.<br>  |
| **Any Service** | **Any Service** – Default setting. All packets will be filtered.<br>**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.<br>**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.<br> |
| **Any Source Port** | Specify the source port number for filtering the packets.<br>**Any Source Port** – Default setting. All packets will be filtered.<br>Select Any Source Port. Or, enter the port number.<br>**Single** – Only the packets passing through the number defined here will be filtered. |

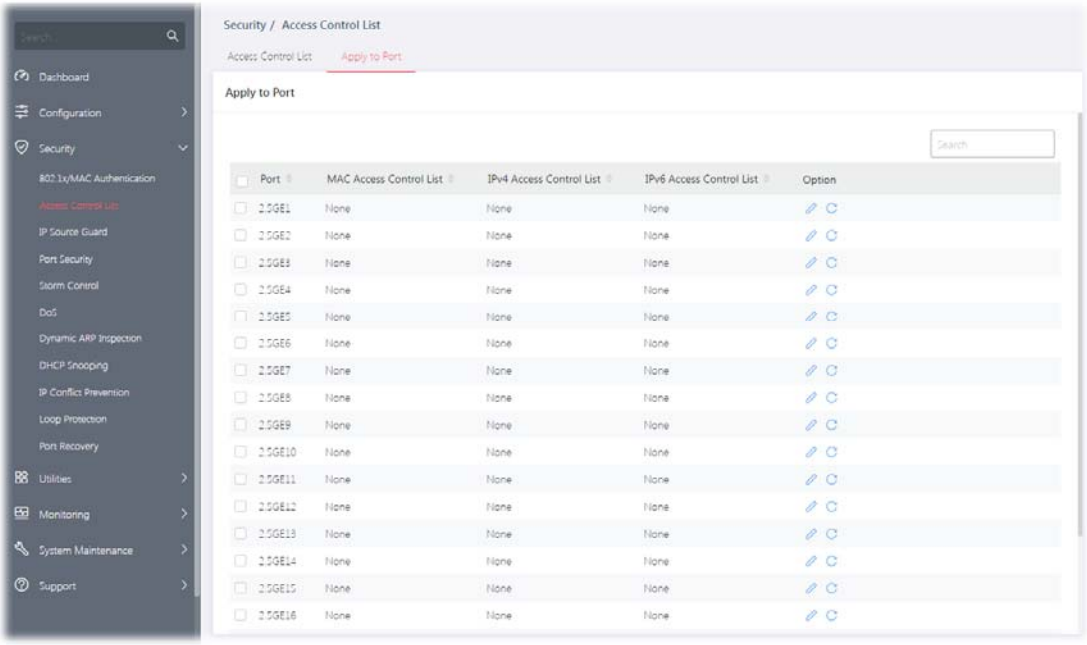
| | |
|---|---|
| |  <br>**Range** – Only the packets passing through the port range defined here will be filtered.<br>  |
| **Any Destination Port** | Specify the destination port number for filtering the packets.<br>**Any Destination Port** – Default setting. All packets will be filtered.<br>Select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

| | |
|---|---|
| | Any ICMP Code (0-255) |
| **+Add Rule** | Click it to create a new ACE rule.<br>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).

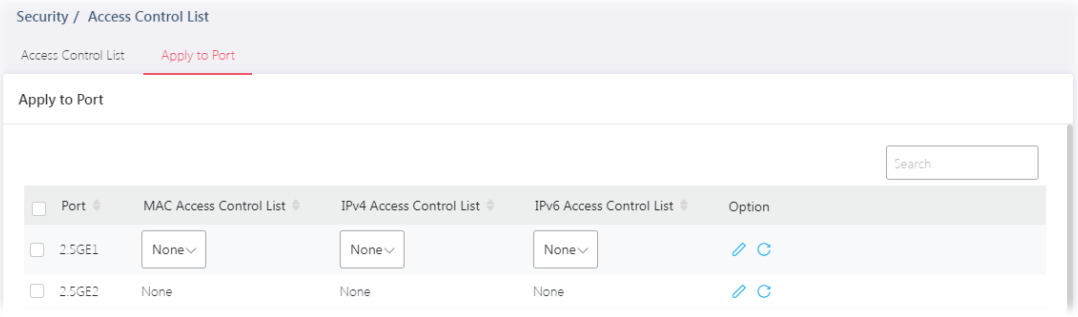
A physical port can only be bound with one of the **IPv4 and IPv6** ACLs, not both.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Port** | Select the port profiles (GE1 to GE28) 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.<br>- Clear current settings and return to factory default settings. |

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



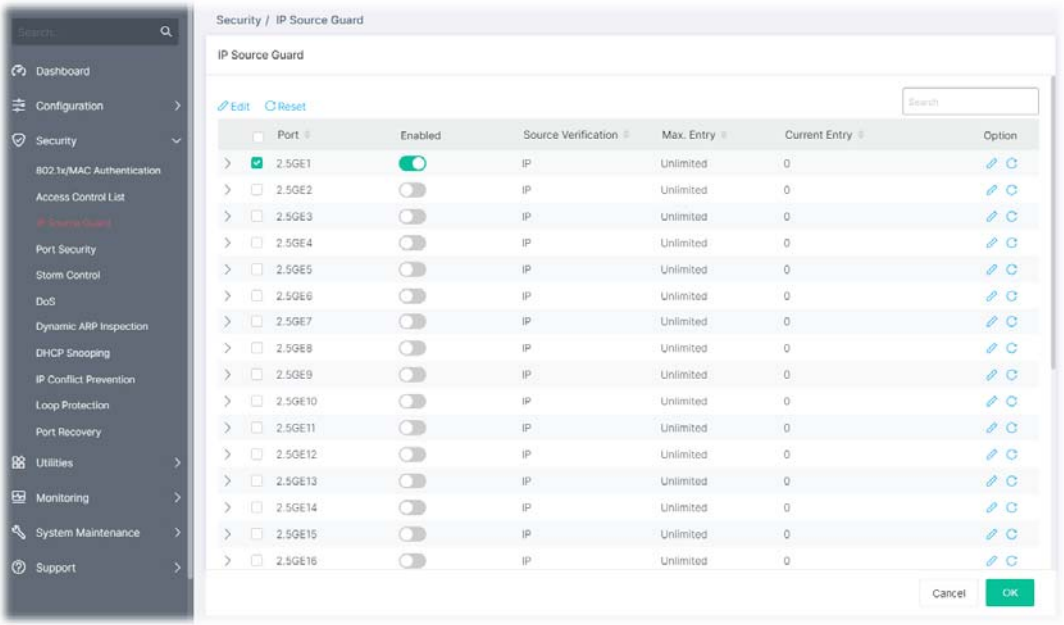
Available settings are explained as follows:

| 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.

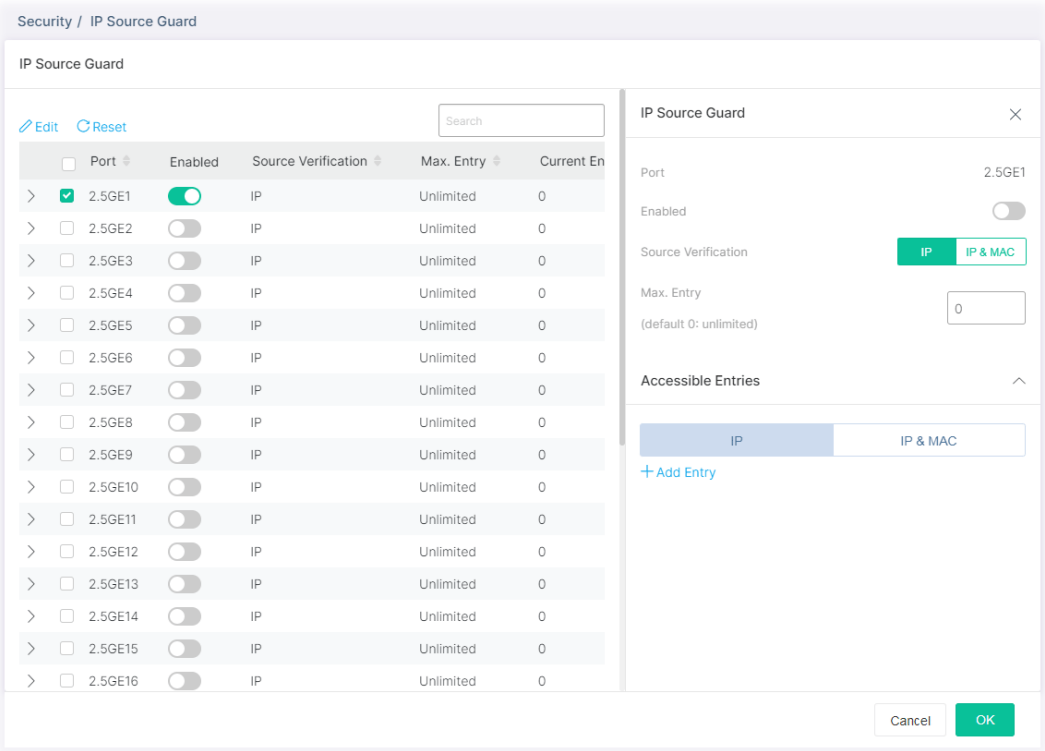
IP source guard is a port-based feature. Therefore, it is necessary to configure detailed settings for each GE/LAG port interface separately.




Available parameters are explained as follows:

| Item | Description |
|---|---|
| **Port** | Displays the port profile (2.5GE1 to 2.5GE16, 10GE1 to 10GE4, LAG1 to LAG8). Check the box to the left side for applying the IP source guard function. |
| **Enabled** | Click the toggle to enable / disable this profile.<br>- means “Enable”.<br>- 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.<br>- Clear current settings and return to factory default settings. |

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



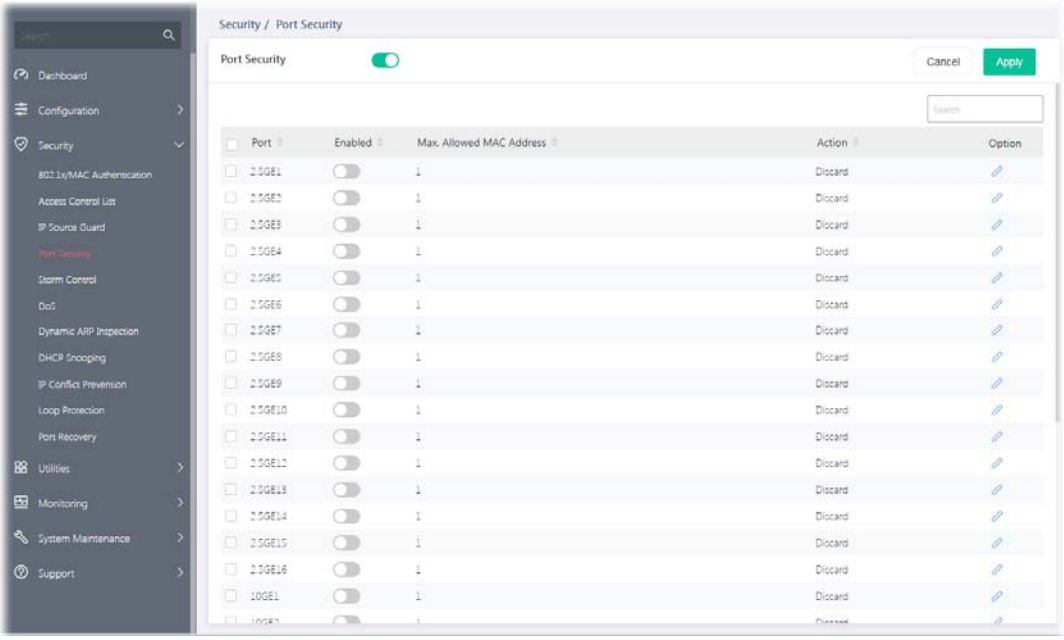

Available settings are explained as follows:

| Item | Description |
|---|---|
| **IP Source Guard** | |
| **Port** | Displays the port profile (2.5GE1 to 2.5GE16, 10GE1 to 10GE4, LAG1 to LAG8). |
| **Enable** | Click the toggle to enable / disable this function.<br> - means “Enable”.<br> - means “Disable”. |
| **Source Verification** | Specify the type of source IP for the packet coming from.<br>**IP** - Only the packet with specified IP address will be verified.<br>**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.<br>**IP** - Select this type to enter an IPv4 address and set a VLAN ID.<br>**IP & MAC** - Select this type to enter an IP address, MAC address and IPv4 address.<br>**+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

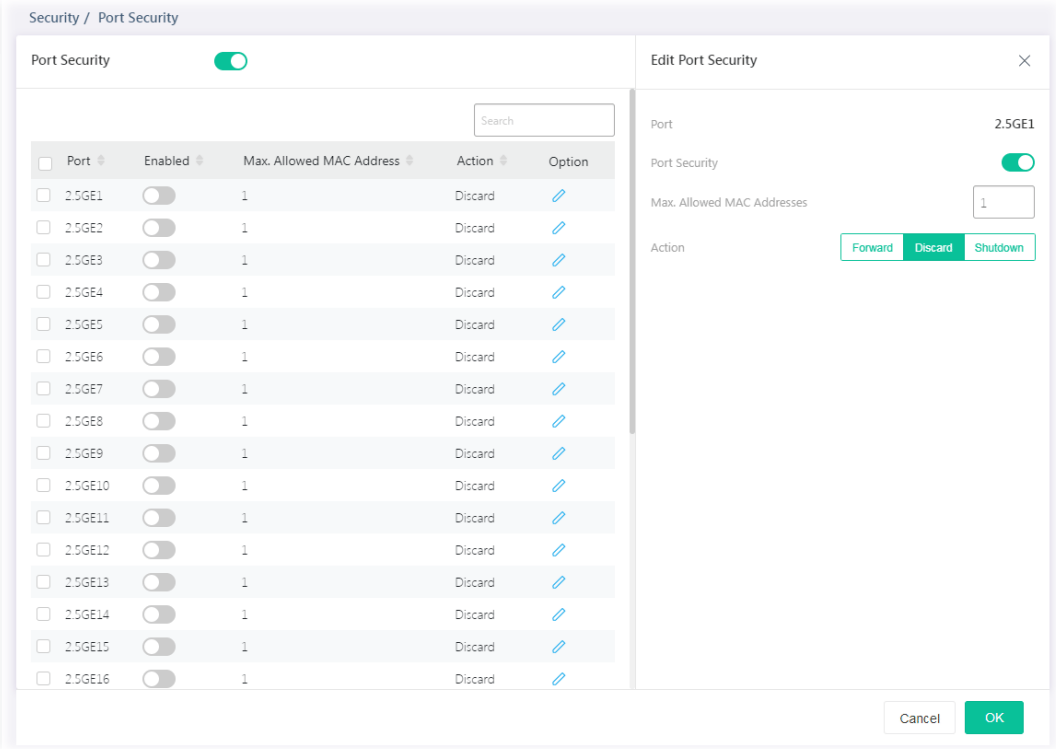
This page allows the network administrator to configure security settings for each port interface (GE port /LAG group). When port security is enabled for each interface, related action will be performed once detecting that the number of MAC address exceeds the limit.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Port Security** | Click the toggle to enable / disable this function. After clicking, press **Apply** to open the configuration page.<br>- means “Enable”.<br>- means “Disable”.<br>Enable this function to configure the settings. |
| **Port** | Displays the index number of the GE/LAG port. |
| **Enabled** | Click the toggle to enable / disable this function.<br>**Enabled –** The selected port applies the port security settings.<br>**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:

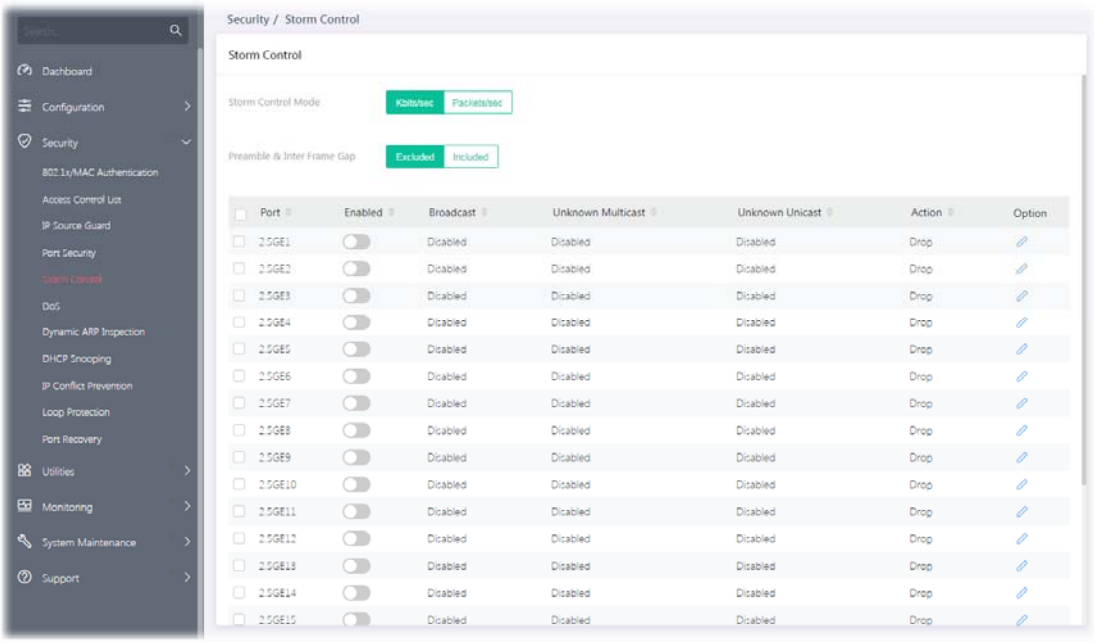
| Item | Description |
|---|---|
| **Edit Port Security** | |
| **Port** | Displays the index number of the GE/LAG port. |
| **Port Security** | Click the toggle to enable / disable this function.<br>**Enabled –** The selected port applies the port security settings.<br>**Disabled –** The selected port 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.<br>**Forward**- Forward a packet whose source MAC is unknown to the switch.<br>**Discard**- Discard a packet whose source MAC is unknown to the switch.<br>**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.

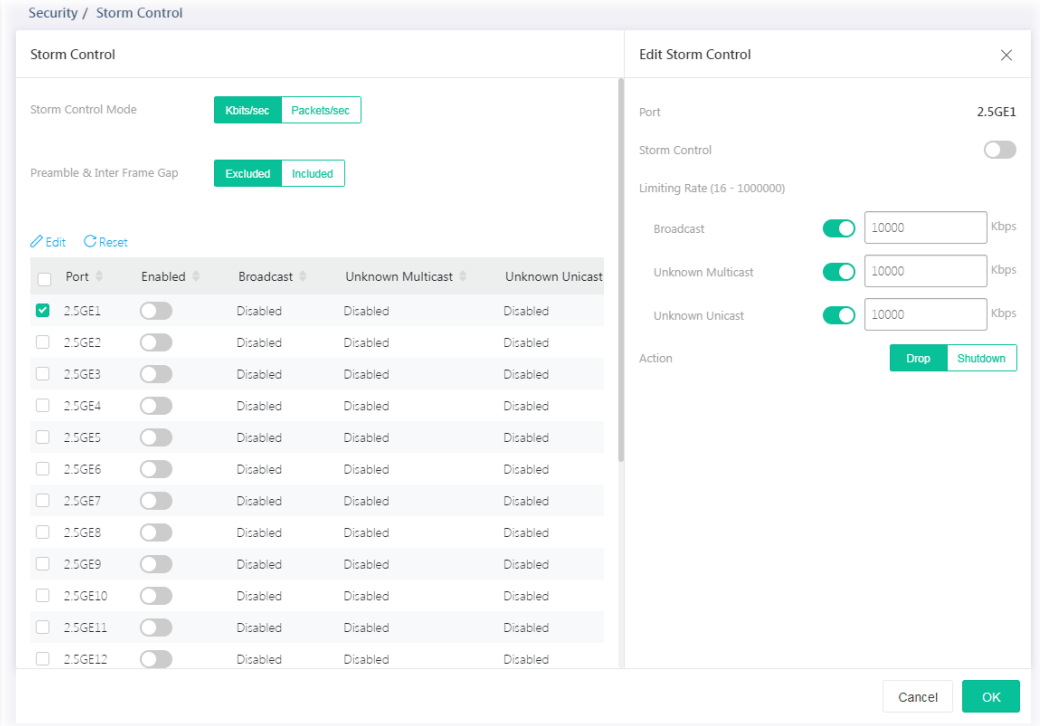



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Storm Control Mode** | Select the mode of storm control.<br>**Kbits/sec** - Storm control rate will be calculated by octet-based.<br>**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).<br>**Excluded** – Exclude preamble & IFG (20 bytes) when count ingress storm control rate.<br>**Included** - Include preamble & IFG (20 bytes) when count ingress storm control rate. |
| **Port** | Enable/disable the port (GE1 to GE28) profiles. |
| **Enabled** | Click the toggle to enable / disable this profile.<br> - means “Enable”.<br> - 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** | Click the toggle to enable / disable this function.<br>- means “Enable”.<br>- 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.<br>**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.<br>**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.<br>**Drop** – Packets exceed storm control rate will be dropped.<br>**Shutdown** - Port exceeds storm control rate will be shutdown. |

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

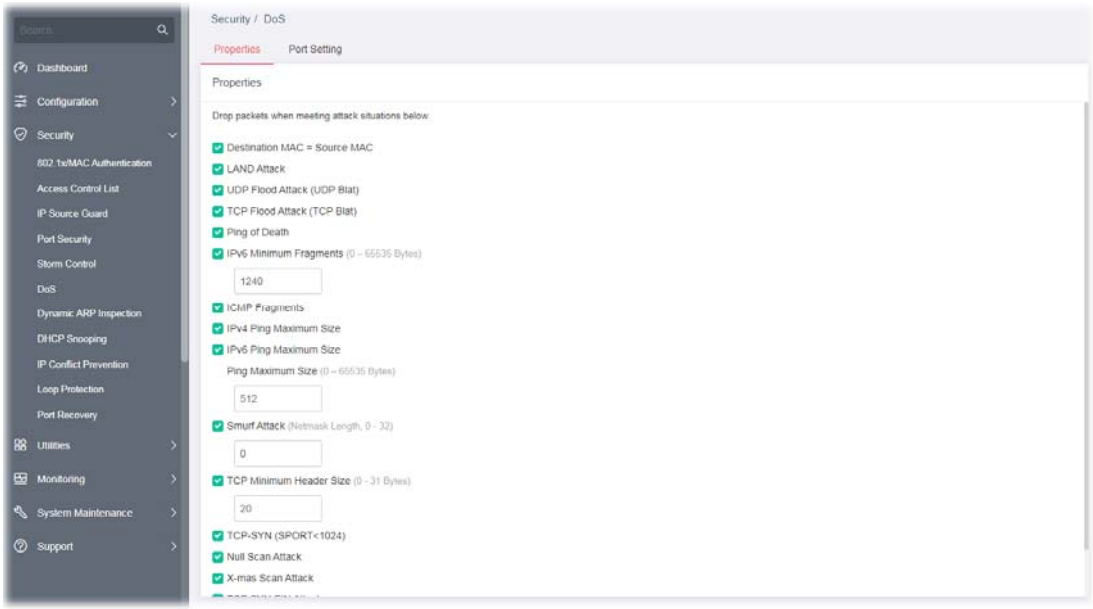
# III-6 DoS

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:

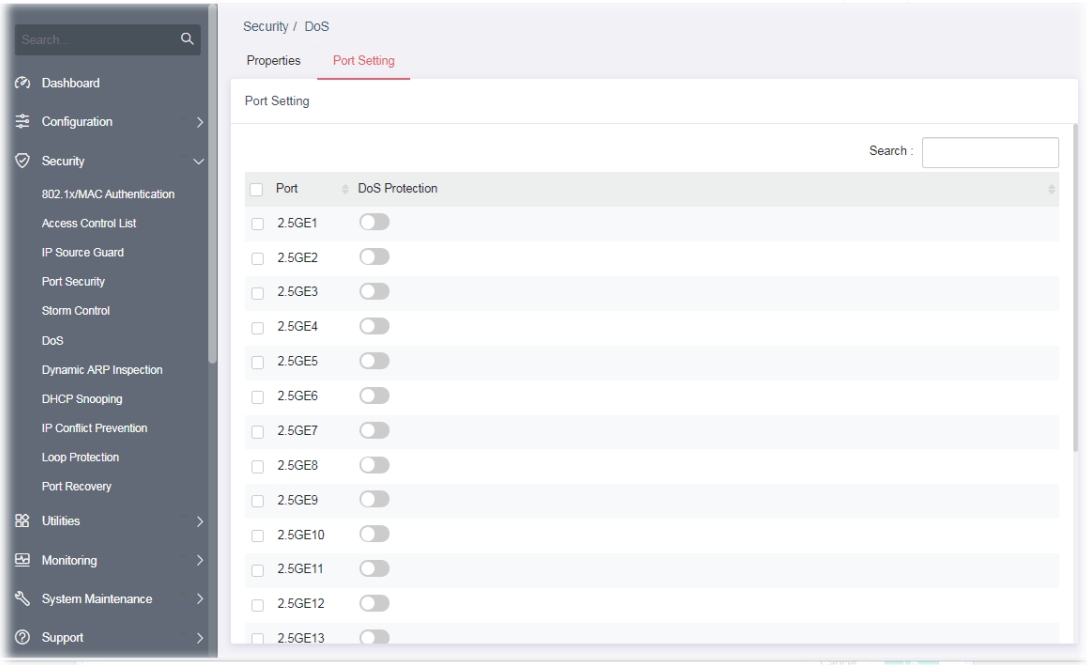
| Item | Description |
|---|---|
| **Destination MAC=Source MAC** | Drops the packets if the destination MAC address is equal to the source MAC address.<br>Check/uncheck the box to enable/disable the function. |
| **LAND Attack** | Drops the packets if the source IP address is equal to the destination IP address.<br>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.<br>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.<br>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.<br>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.<br>Check/uncheck the box to enable/disable the function. |
| **ICMP Fragments** | Drops the fragmented ICMP packets.<br>Check/uncheck the box to enable/disable the function. |
| **IPv4 Ping Maximum Size** | Determines the IPv4 PING packet with the length.<br>Check/uncheck the box to enable/disable the function. |
| **IPv6 Ping Maximum Size** | Determines the IPv6 PING packet with the length.<br>Check/uncheck the box to enable/disable the function.<br>**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.<br>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.<br>Check/uncheck the box to enable/disable the function. |
| **TCP-SYN (SPORT<1024)** | Drops SYN packets with sport less than 1024.<br>Check/uncheck the box to enable/disable the function. |
| **Null Scan Attack** | Drops the packets with NULL scan.<br>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.<br>Check/uncheck the box to enable/disable the function. |
| **TCP SYN-FIN Attack** | Drops the packets with SYN and FIN bits set.<br>Check/uncheck the box to enable/disable the function. |
| **TCP SYN-RST Attack** | Drops the packets with SYN and RST bits set.<br>Check/uncheck the box to enable/disable the function. |
| **TCP Fragment (Offset=1)** | Drops the fragmented ICMP packets.<br>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 |
|---|---|
| **Port** | Displays the port profile (GE1 to GE28). Check the box to the left side to select the port profile. |
| **DoS Protection** | Click the toggle to enable / disable the function of DoS Protection.<br> - means “Enable”.<br> - means “Disable”. |

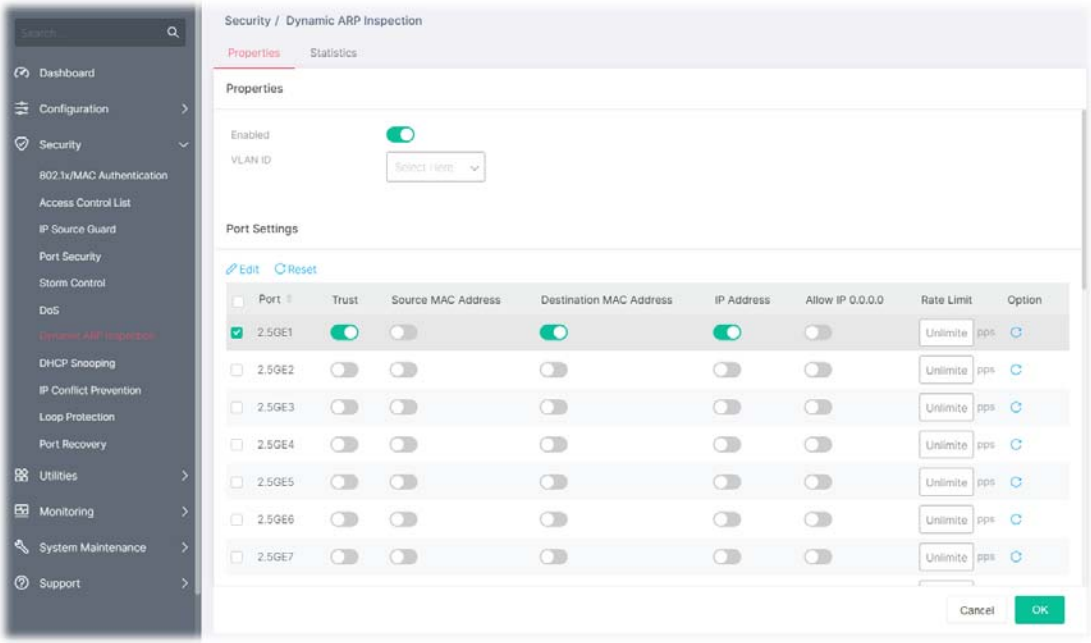
After finishing this web page configuration, please click **OK** to save the settings.

# 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:

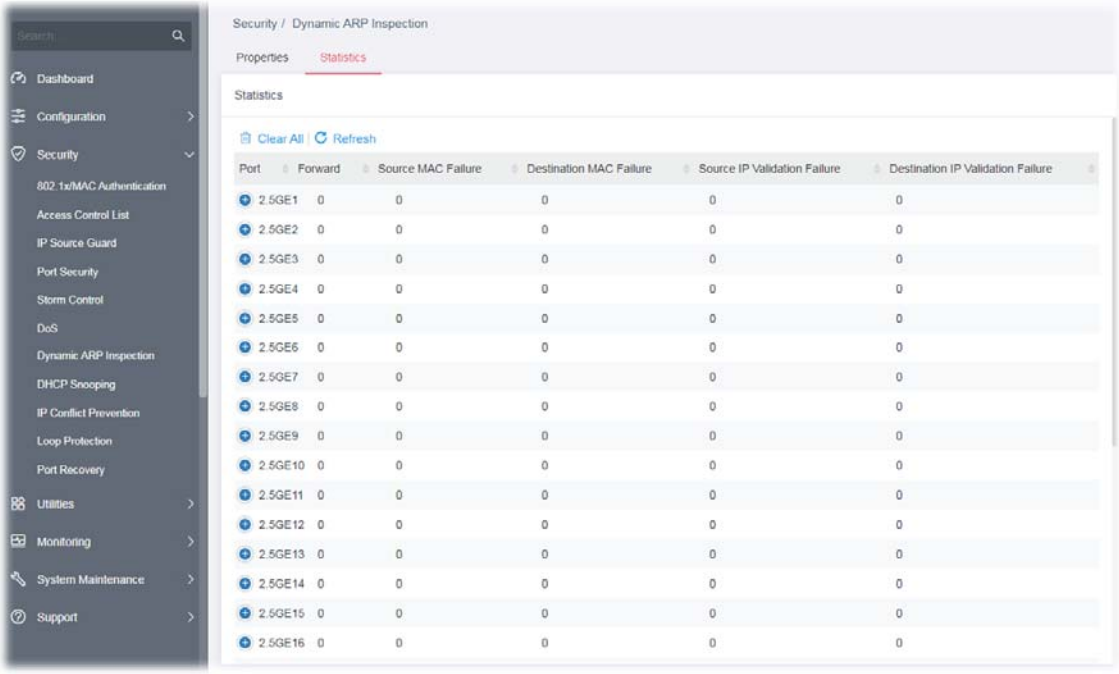
| Item | Description |
|---|---|
| **Enable** | Click the toggle to enable / disable the function of Dynamic ARP Inspection.<br> - means “Enable”.<br> - means “Disable”. |
| **VLAN ID** | Select VLAN profile(s) to apply the function of Dynamic ARP Inspection.<br>Only the GE/LAG port within the selected VLAN will apply DAI function. |
| **Port Settings** | |
| **Port** | Displays the port (2.5GE1 to 2.5GE16, 10GE1 to 10GE4, LAG1 to LAG8) or ports for applying DAI function. |
| **Trust** | Click the toggle to enable/disable the function of DAI for this port. |
| **Source MAC Address** | Click the toggle to enable/disable the function of the source MAC address validation mechanism for this port. |

| | |
|---|---|
| **Destination MAC Address** | Click the toggle to enable/disable the function of the destination MAC address validation mechanism for this port. |
| **IP Address** | Click the toggle to enable/disable the function of IP address validation mechanism for this port. |
| **Allow IP 0.0.0.0** | Click the toggle to enable/disable the function.<br>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. |

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.

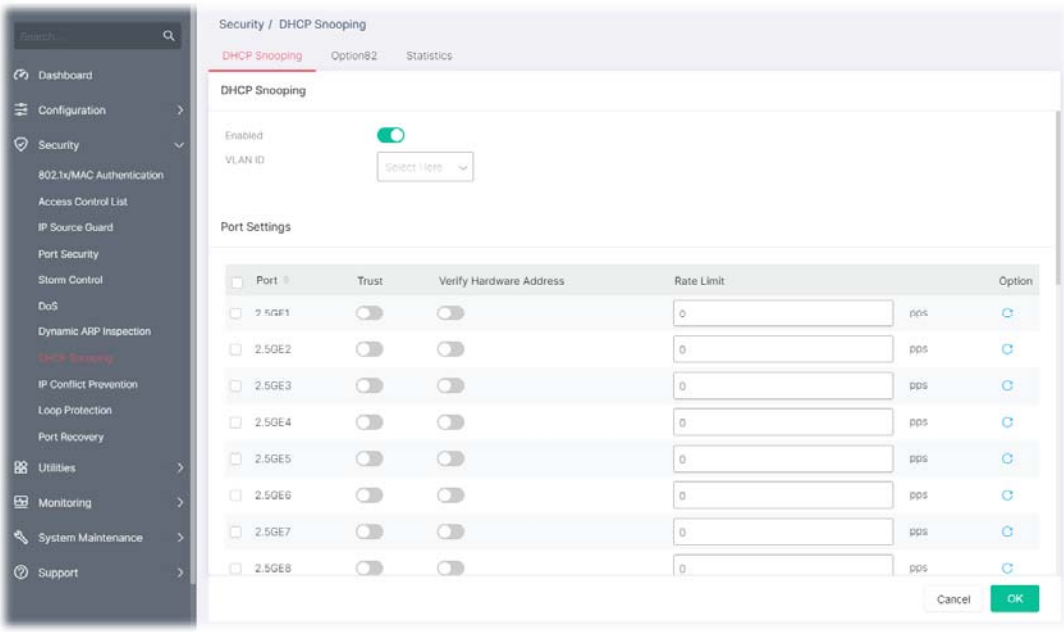
For DHCP snooping to function properly, it is suggested to connect DHCP servers to VigorSwitch through trusted interfaces; because untrusted DHCP messages will be forwarded to trusted interfaces only.

## 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 |
|---|---|
| **Enable** | Click the toggle to enable / disable the function of DHCP Snooping.<br>- means “Enable”.<br>- means “Disable”. |
| **VLAN ID** | Select VLAN profile(s) to apply the function of DHCP Snooping function.<br>Only the GE/LAG port within the selected VLAN will apply DHCP Snooping function. |
| **Port Settings** | |

| | |
|---|---|
| **Port** | Displays the port (2.5GE1 to 2.5GE16, 10GE1 to 10GE4, LAG1 to LAG8) or ports for applying the DHCP snooping function. |
| **Trust** | Click the toggle to enable/disable the function of DHCP snooping for this port. |
| **Verify Hardware Address** | Click 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. |

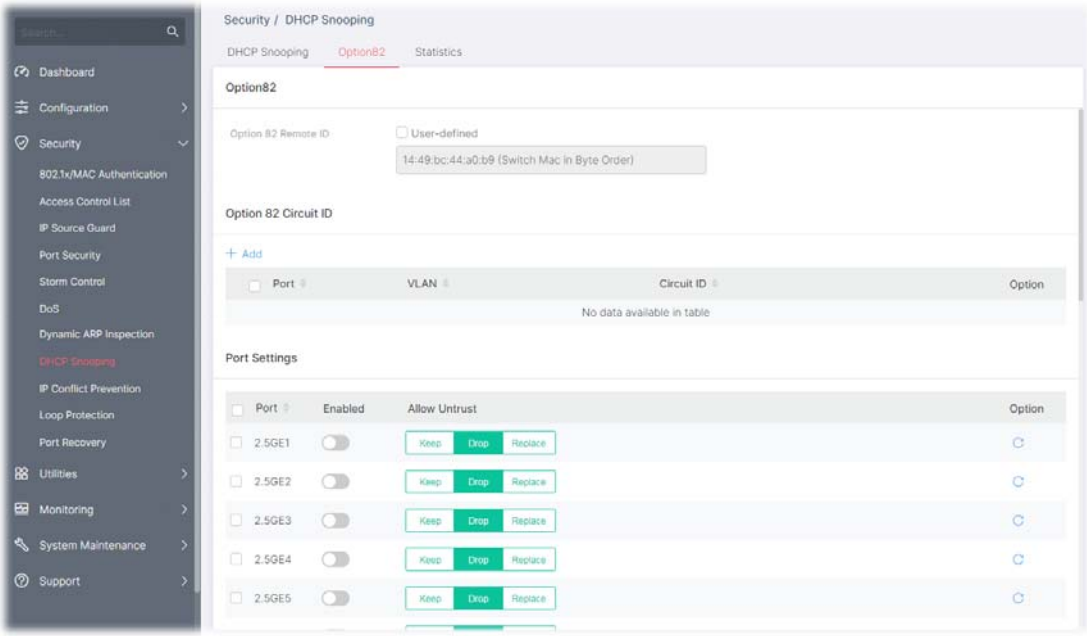
After finishing this web page configuration, please click **OK** to save the settings.

## 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.

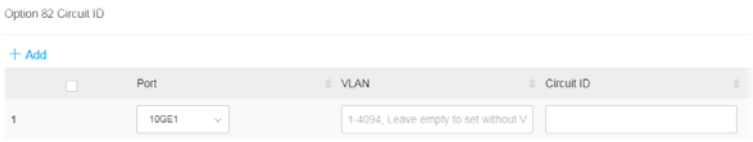
This page allows a user to set a string as remote ID for DHCP option82. For example, use a switch-configured hostname or specify an ASCII text string as remote ID.

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:

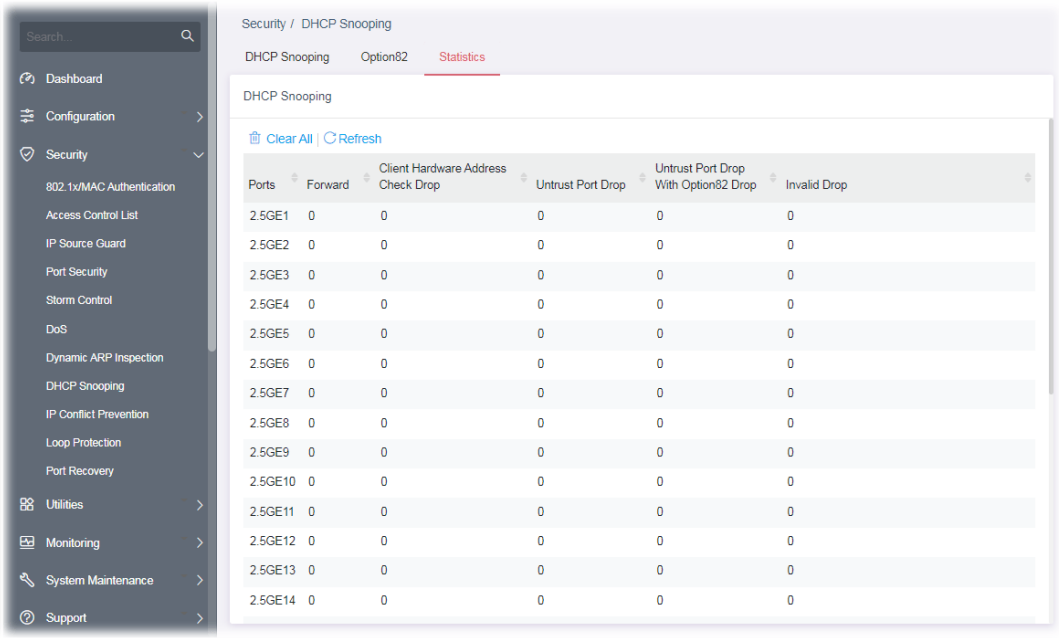
| Item | Description |
|---|---|
| **Option82** | |
| **Option 82 Remote ID** | The string specified here is used to identify the remote host.<br>**User-defined -** Check it and manually enter switch MAC in byte order |

| | |
|---|---|
| | in the entry box. |
| **Option 82 Circuit ID** | |
| **+Add** | Click to have new fields for creating a new profile.<br>  <br><br>**Port -** Use the drop down list to select the port (10GE1 to 10GE12, LAG1 to LAG8) or ports for applying DHCP snooping, Option82 function.<br>**VLAN** - Choose a number as VLAN ID which is easy to be identified for a packet containing with it.<br>**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 (2.5GE1 to 2.5GE16, 10GE1 to 10GE4, LAG1 to LAG8) or ports for applying the Option82 function. |
| **Enabled** | Click the toggle to enable / disable the function of Option82 Property.<br> - means “Enable”.<br> - means “Disable”. |
| **Allow Untrust** | Untrusted packets detected by VigorSwitch will be performed by the action determined here.<br>**Keep** – Packets are allowed to pass through.<br>**Drop** – Packets are blocked and discarded.<br>**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.

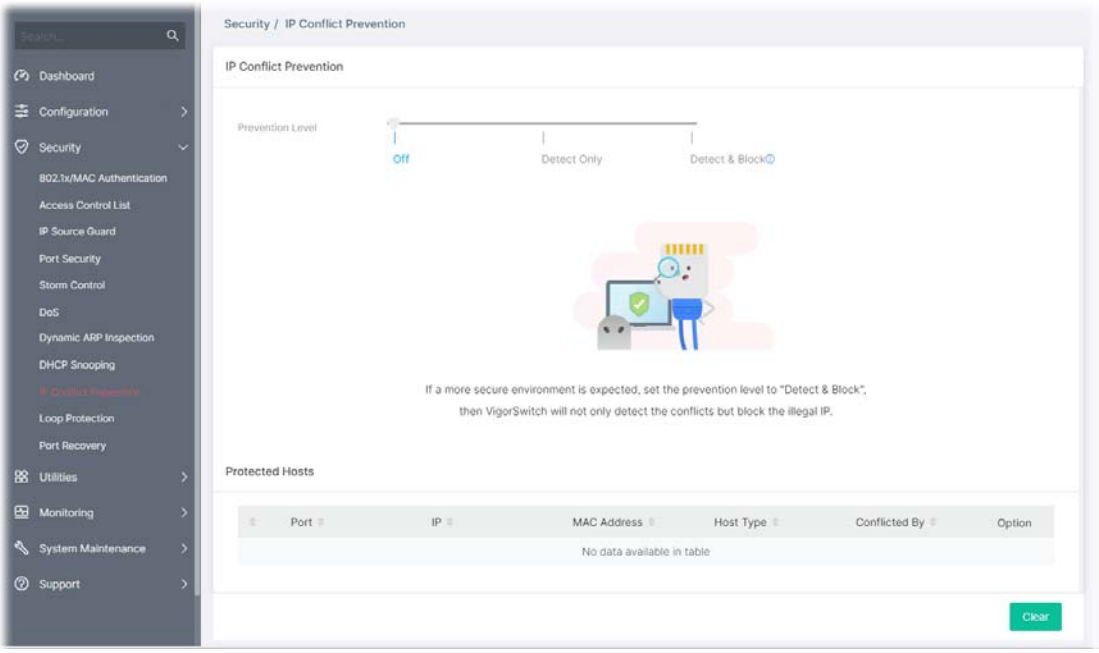


# III-9 IP Conflict Prevention

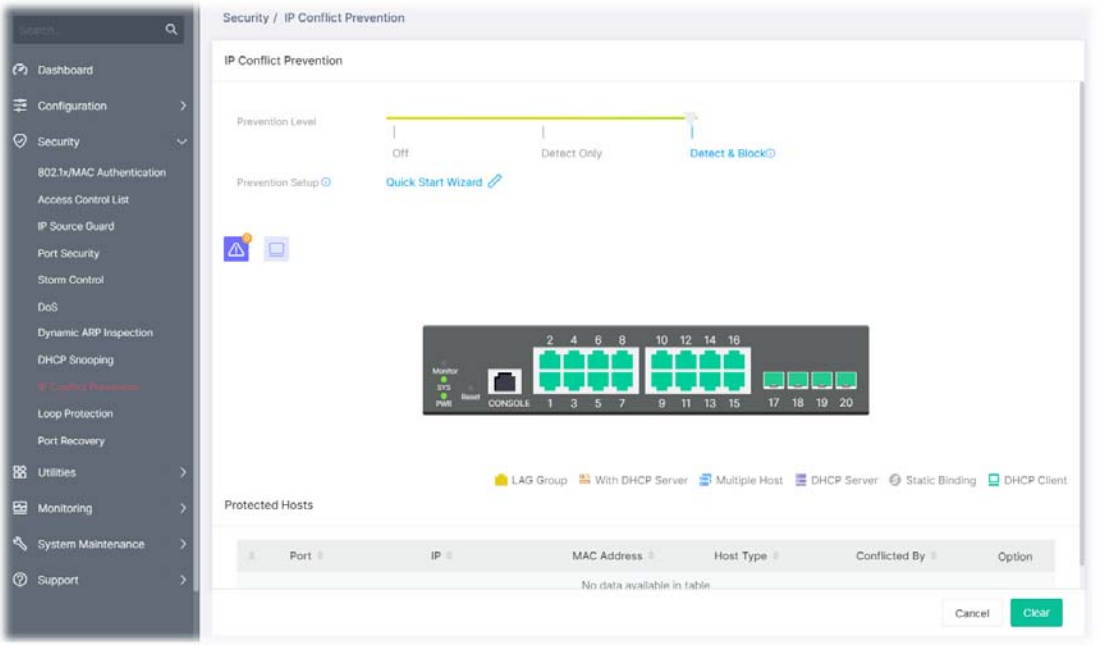
A user can configure IP addresses for network devices manually. However, it might result in conflict between different devices due to using the same IP address, and cause the devices not working correctly.

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

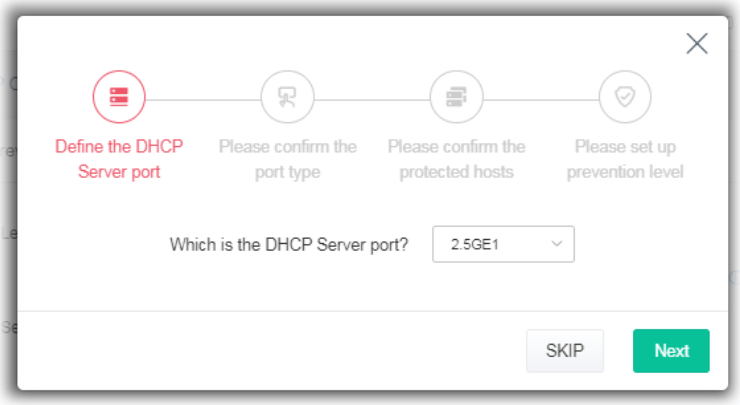
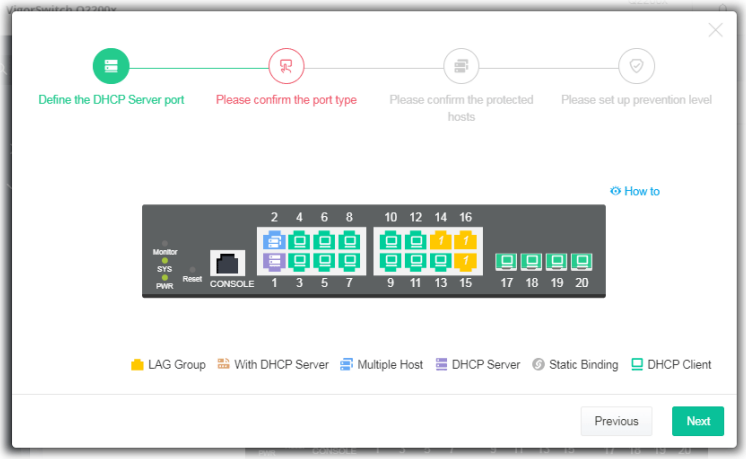
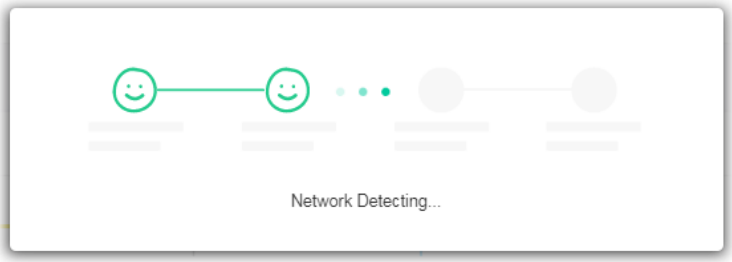
**Prevention Level: Off**

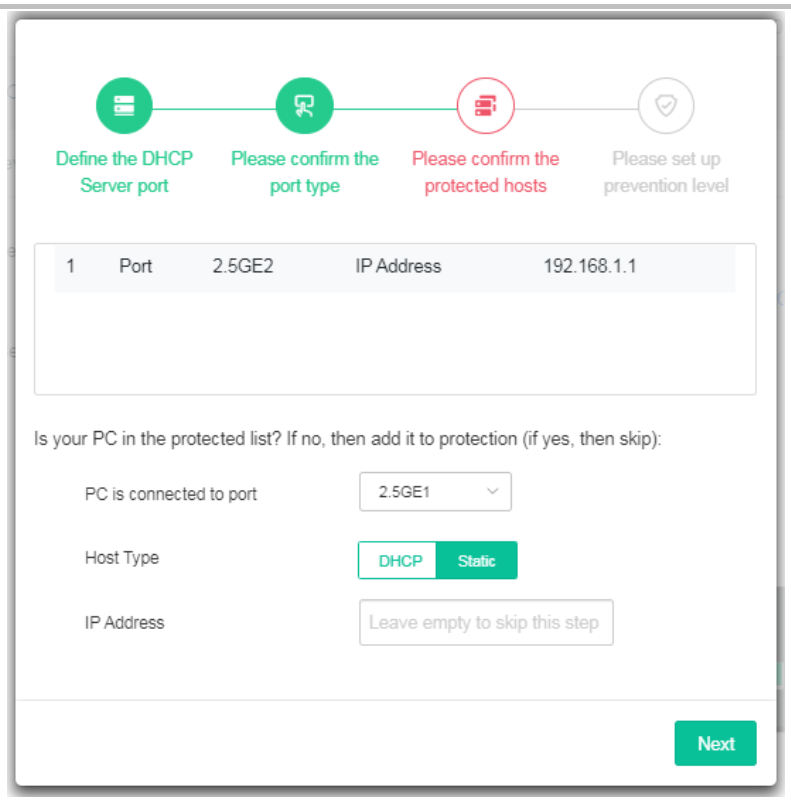



**Prevention Level: Detect & Block**

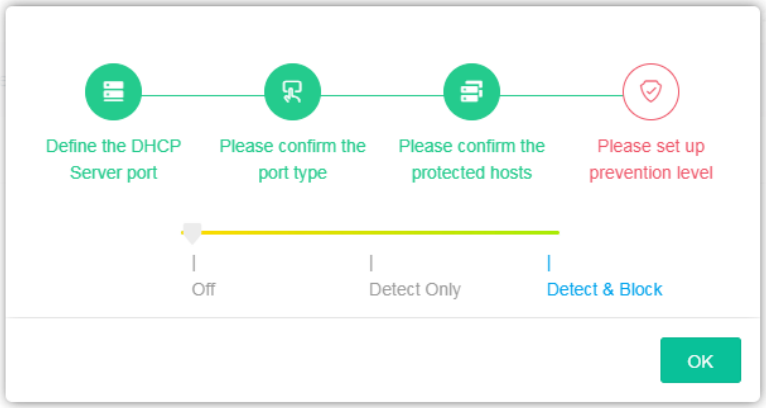



Available settings are explained as follows:

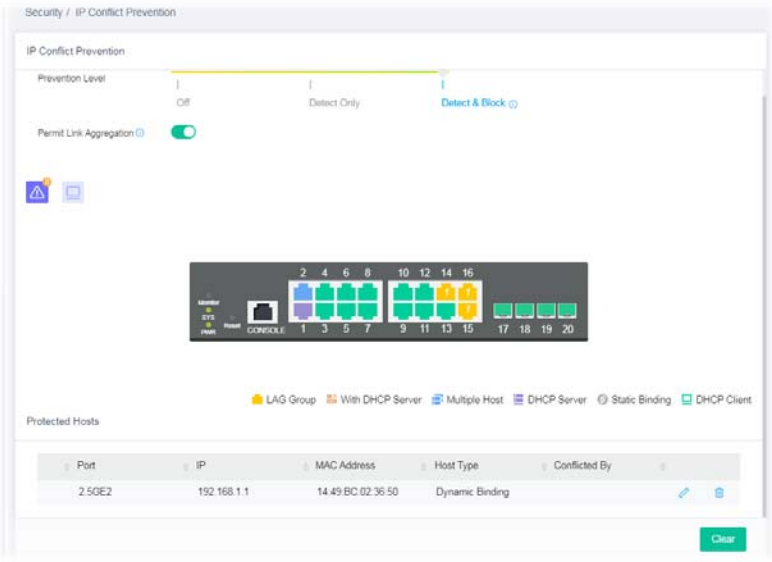
| Item | Description |
| --- | --- |
| **IP Conflict Prevention** | |
| **Prevention Level** | **Off** - The function of IP conflict prevention is disabled.<br>**Detect Only** - VigorSwitch will detect the host but no further action executed.<br>**Detect & Block** - VigorSwitch will detect the host and 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.<br>Step 1: Choose a server port. Click Next.<br>  <br>Step 2: Confirm the port type. Click Next.<br>  <br>Step 3: Wait for the network detection.<br>  <br>Step 4: Confirm / modify the protected host. Click Next. |




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



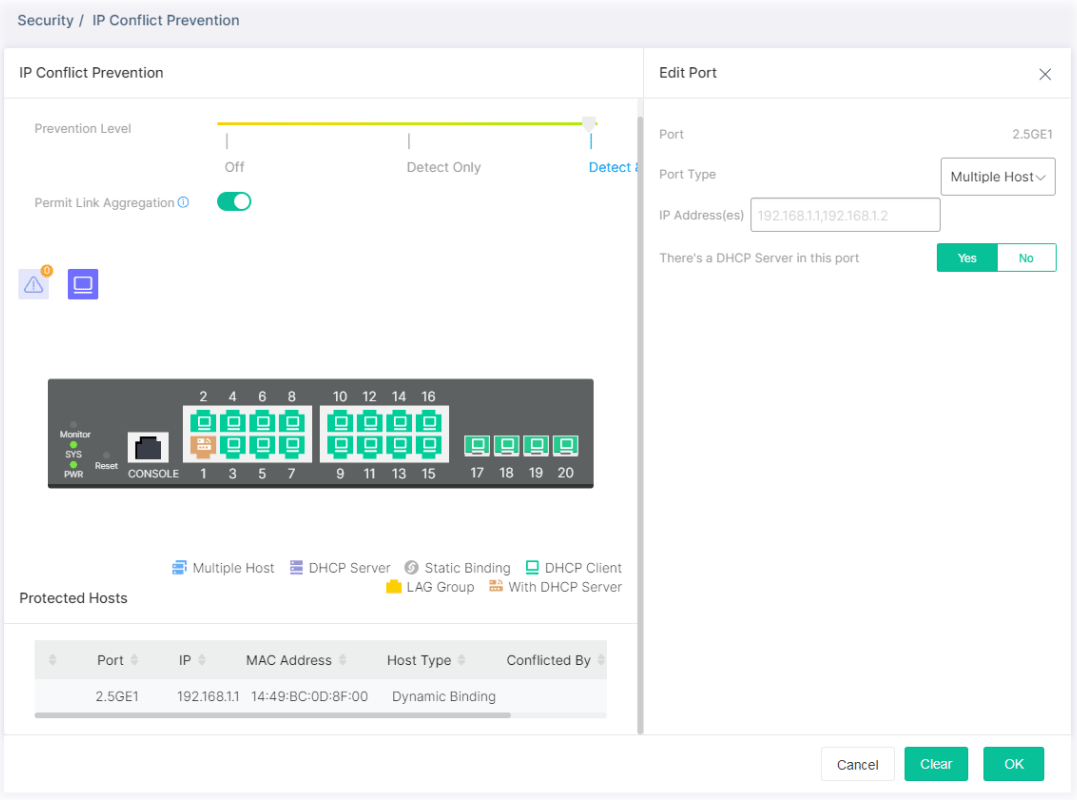

After clicking **OK**, the IP address specified for the GE port will be unavailable for other network devices.



| | |
|---|---|
| **Permit Link Aggregation** | It appears after running the quick start wizard for IP conflict prevention.<br>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 2.5GE16, 10GE1 to 10GE4, 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.<br>- 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.



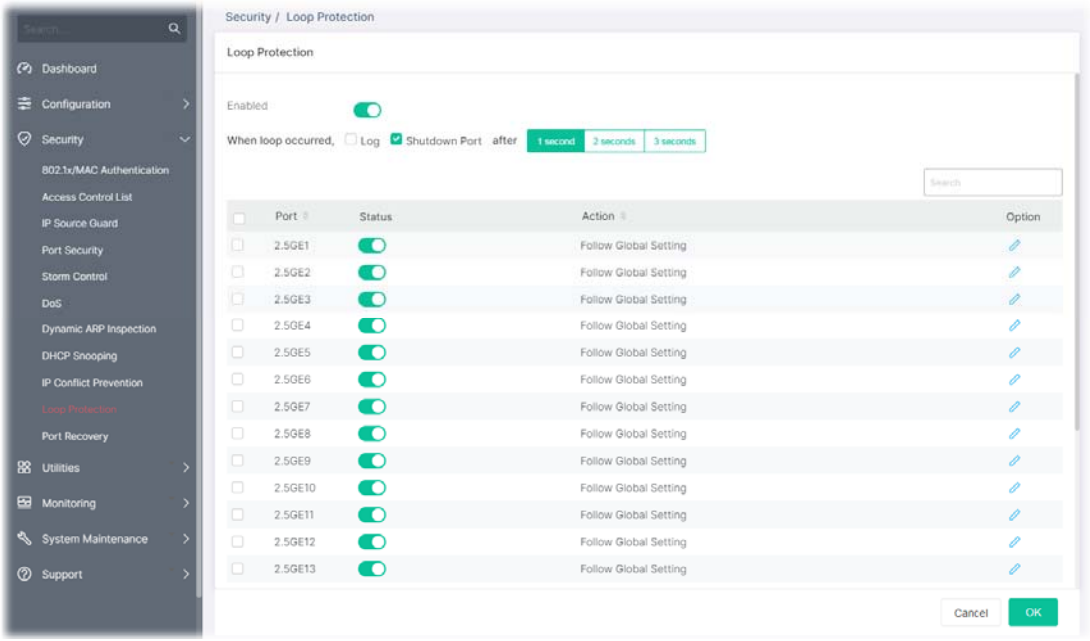

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Edit Port** | |

| | |
|---|---|
| **Port** | Displays the LAN port number (2.5GE1 to 2.5GE16, 10GE1 to 10GE4, LAG1 to LAG8) of the selected host. |
| **Port Type** | Specify the port type for the selected host.<br>• **DHCP Client**<br>• **Static Binding**<br>• **Multiple Host**<br>• **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.<br>**No** - If there is no DHCP server in this port already, click No. |

# III-10 Loop Protection

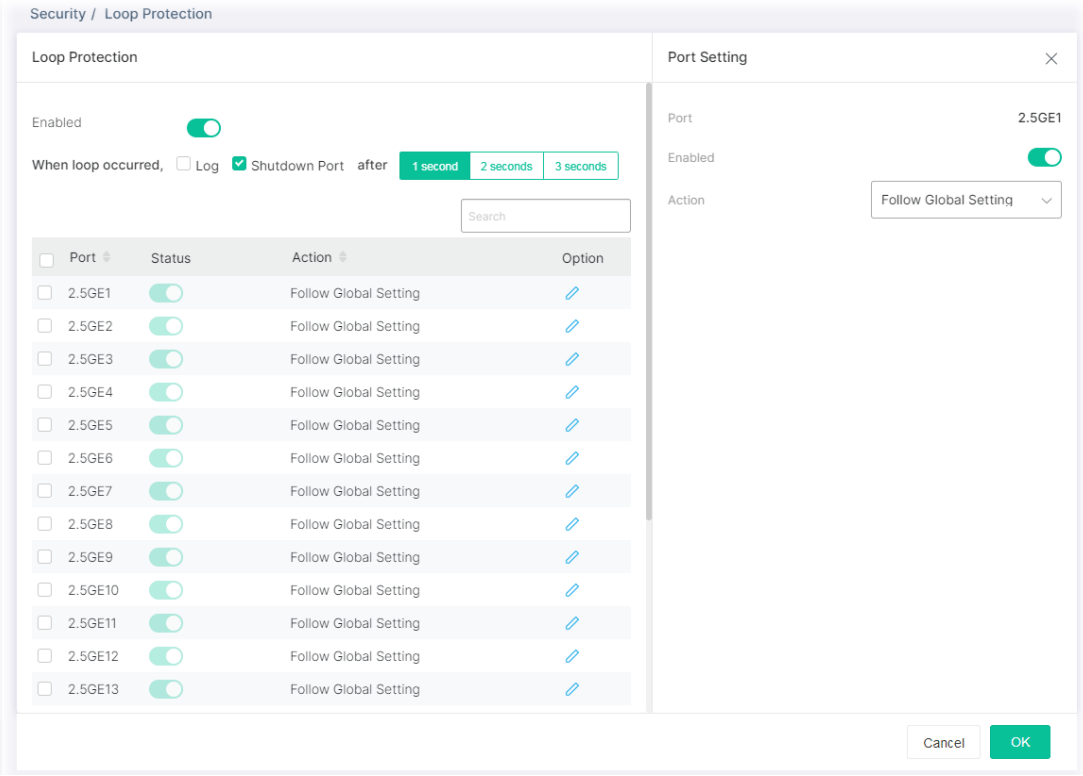
Loop event might be caused due to wrong hardware connection. VigorSwitch will periodically send packets out to check if they loopback or not. This page allows you to set conditions and perform an action when VigorSwitch detects the looped packet.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Loop Protection** | |
| **Enable** | **Enable / Disable** – Click the toggle to enable / disable this function. VigorSwitch will detect the loop event of the GE port automatically.<br> - means “Enable”.<br> - means “Disable”. |
| **When loop occurred..** | When the switch detects loop situation occurred to a port; it will perform the action selected in this field.<br>**Log** - The switch will record such event as a log.<br>**Shutdown Port** - The switch will shut down the port.<br>**After 1 second/2 seconds/3 seconds** - Determine the time to record the event and / or shutdown the port.<br>The settings configured here will be treated as global setting for all GE ports. |
| **Port** | Displays the port number (2.5GE1 to 2.5GE16, 10GE1 to 10GE4, LAG1 to LAG8). Check the box to the left to enable the selected port. |
| **Status** | **Enable / Disable** – Click 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.



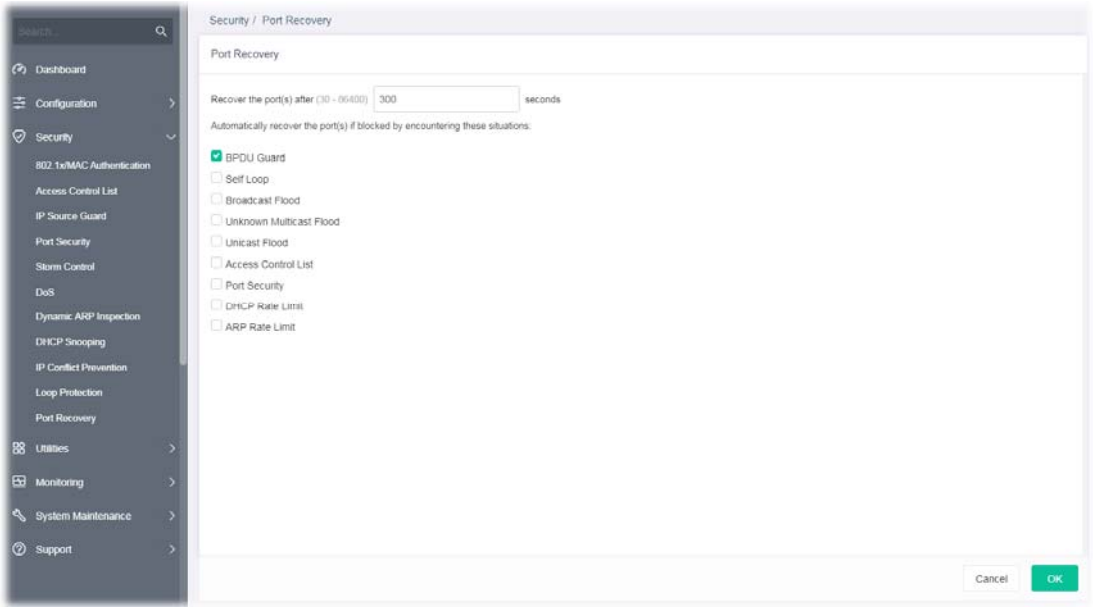

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Port** | Displays the port number (2.5GE1 to 2.5GE16, 10GE1 to 10GE4, LAG1 to LAG8). |
| **Enable** | **Enable / Disable** – Click the toggle to enable / disable this function. VigorSwitch will detect the loop event of the GE port automatically.<br>- means “Enable”.<br>- means “Disable”. |
| **Action** | **Follow Global Setting** - Adopts the settings configured for **When loop occurred**.<br>**Log** - The switch will record such event as a log.<br>**Shutdown Port** - The switch will shut down the port.<br>**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.



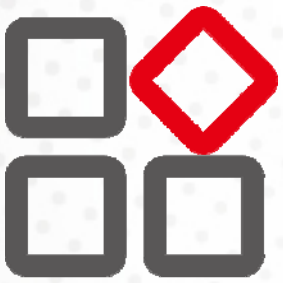

Available settings are explained as follows:

| 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.

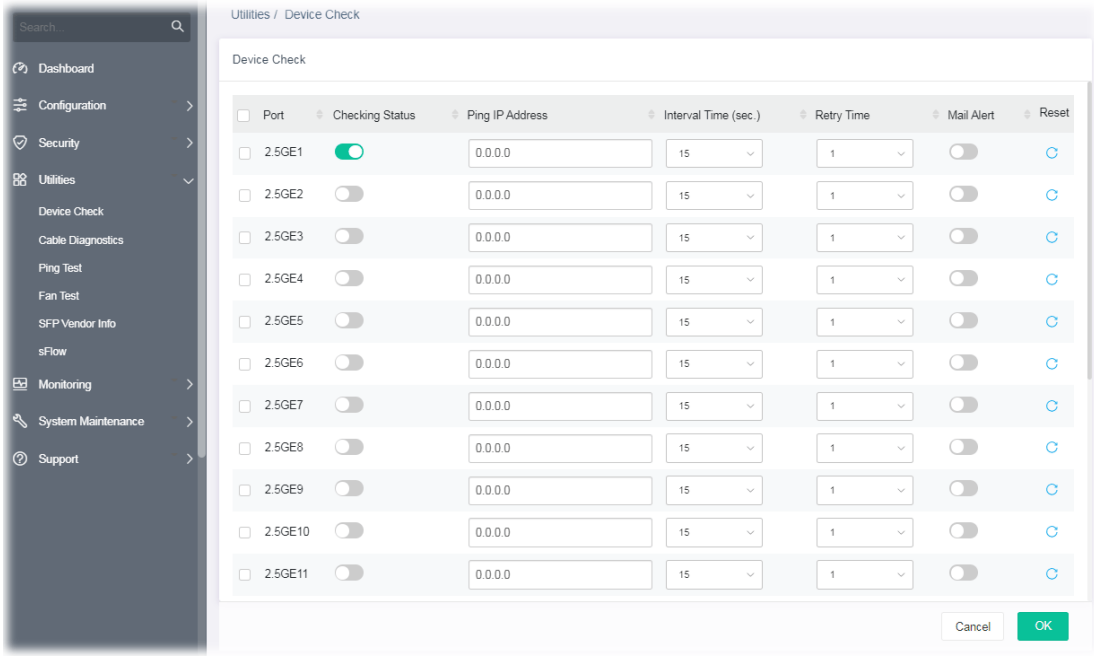
# Chapter IV Utilities



# 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:

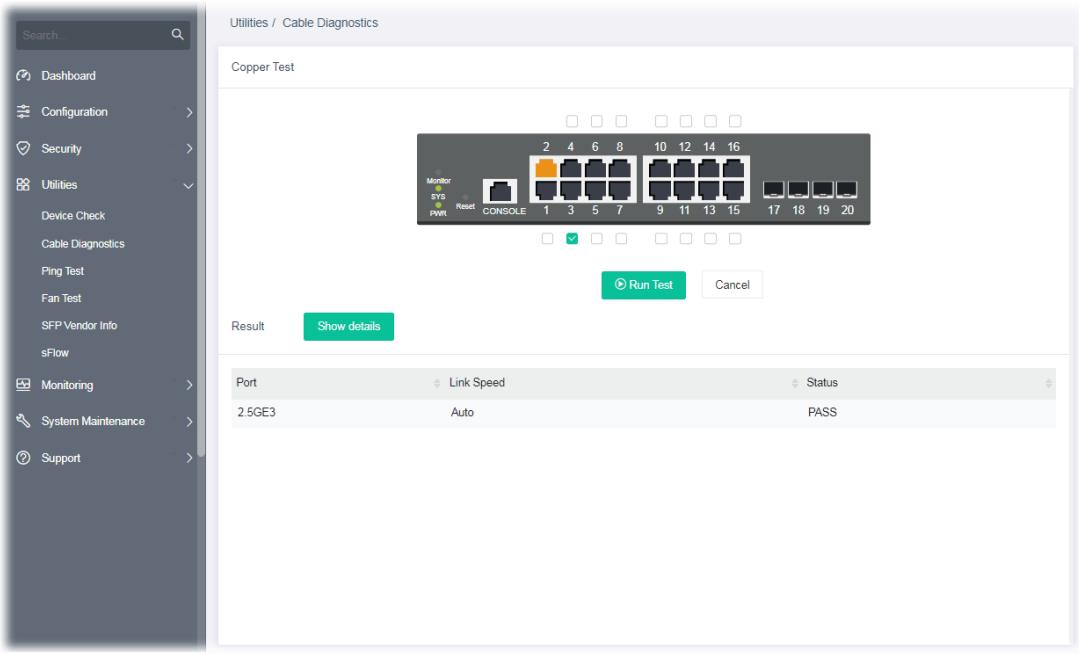
| Item | Description |
|---|---|
| **Port** | Display the port number (2.5GE1 to 2.5GE16, 10GE1 to 10GE4).<br>Check the box to the left to enable the port settings. |
| **Checking Status** | **Enable / Disable** – Click the toggle to enable / disable this function.<br> - means “Enable”.<br> - means “Disable”. |
| **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.<br>• **Power Cycle** - Force reboot the device by cycling the power given to the PoE device.<br>• **Power Off** - The PoE device will be powered off.<br>• **Nothing** - Log this event only, no action is taken on PoE device. |

| | |
|---|---|
| **Mail Alert** | **Enable / Disable** – Click 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.



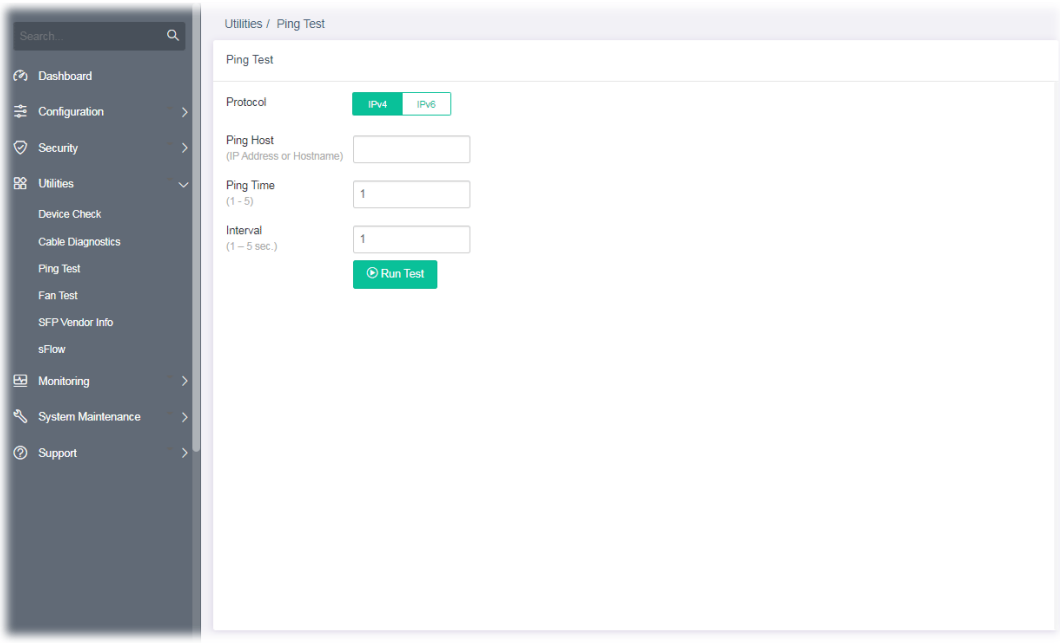

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Cooper Test** | |
| **Run Test** | Perform the copper test action.<br>Before clicking Run Test, select the port or ports (2.5GE1 to 2.5GE16, 10GE1 to 10GE4) on the panel figure for performing cable diagnostics. |
| **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.

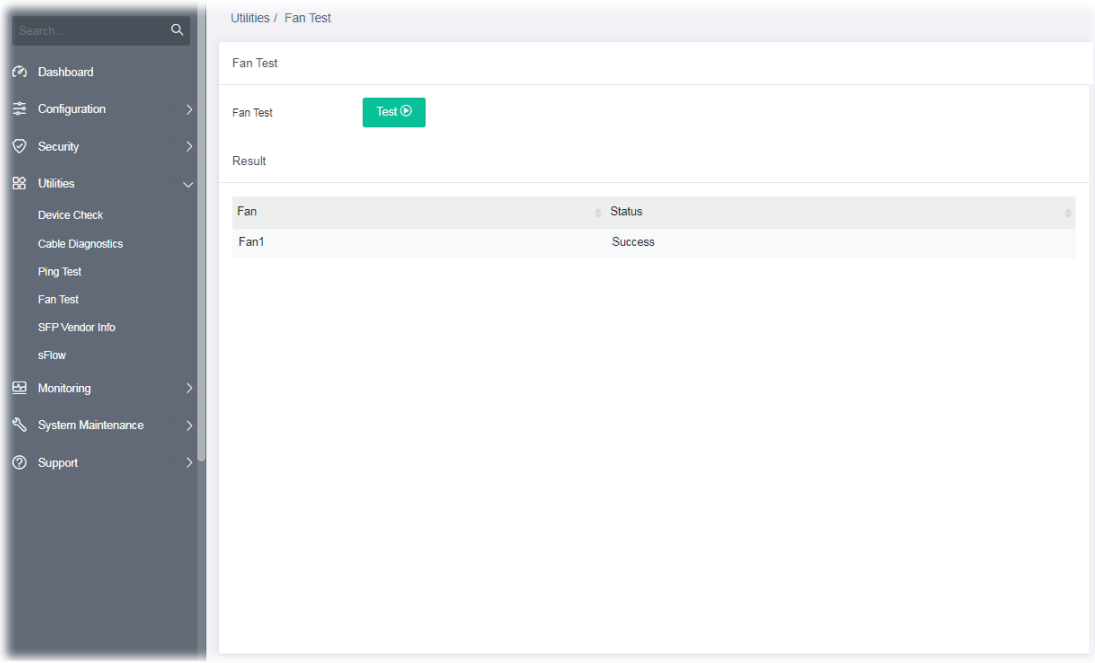



Available settings are explained as follows:

| 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.<br>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. |

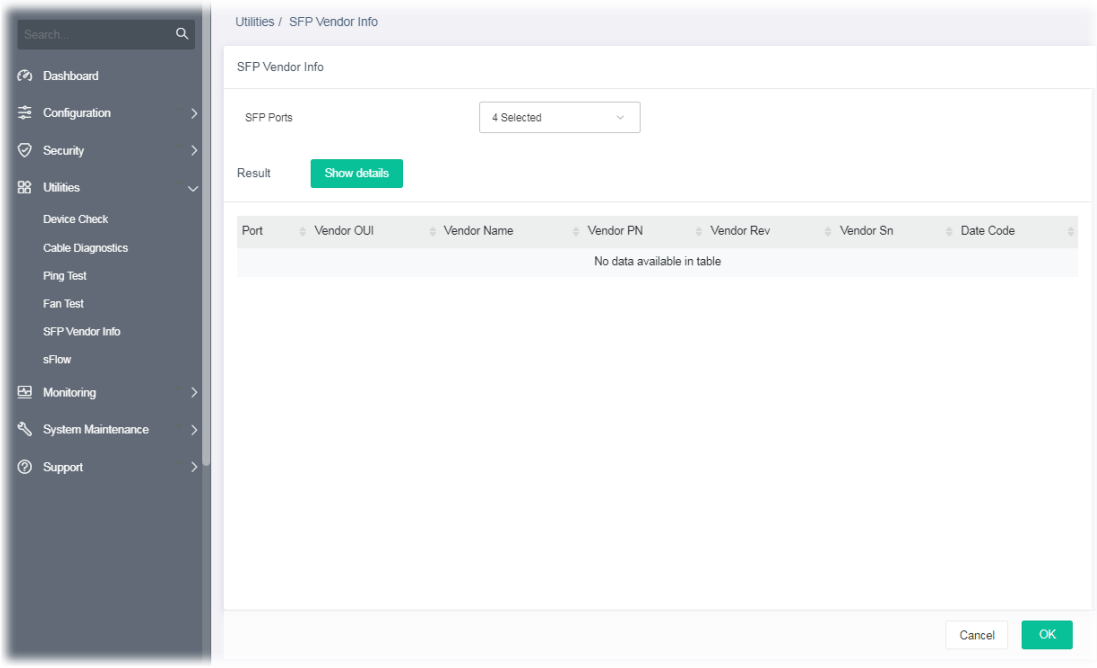
# IV-4 Fan Test

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

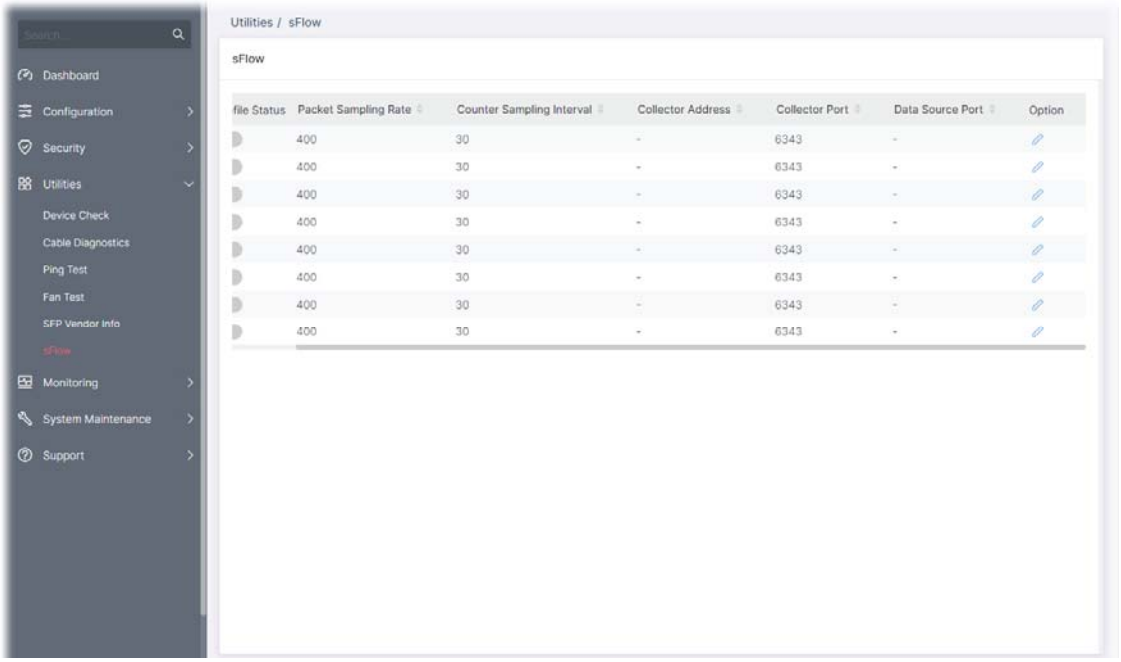
To get general information about the SFP vendor, select **Utilities>>SFP Vendor Info**.



# 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.

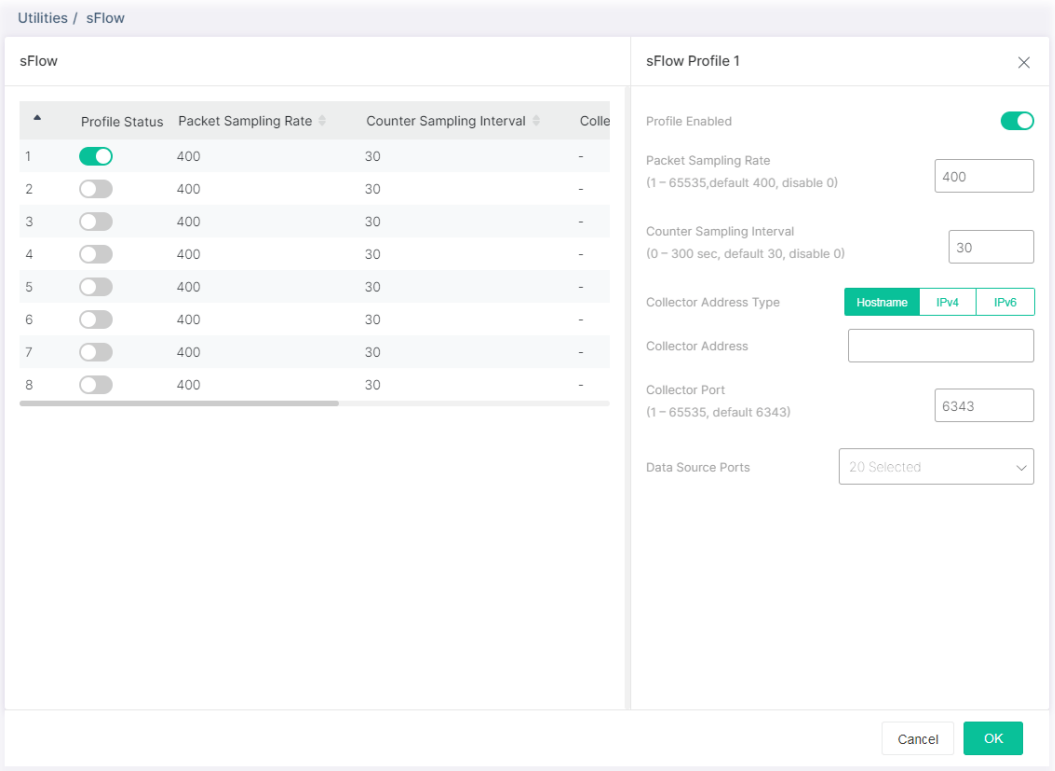
VigorSwitch plays the role of sFlow agent which collects and sends the collected data to a sFlow controller (e.g., an external monitoring software) for executing data analysis. The system administrator shall install the sFlow controller on the device which can communicate with VigorSwitch. When the administrator 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** – Click the toggle to enable / disable this function.<br>- means “Enable”.<br>- 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 (2.5GE1 to 2.5GE16, 10GE1 to 10GE4) 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 Enable** | **Enable / Disable** – Click the toggle to enable / disable the settings for the selected profile.<br>- means “Enable”.<br>- 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 (2.5GE1 to 2.5GE16, 10GE1 to 10GE4) as the data source port. |
| **OK** | Save the settings. |

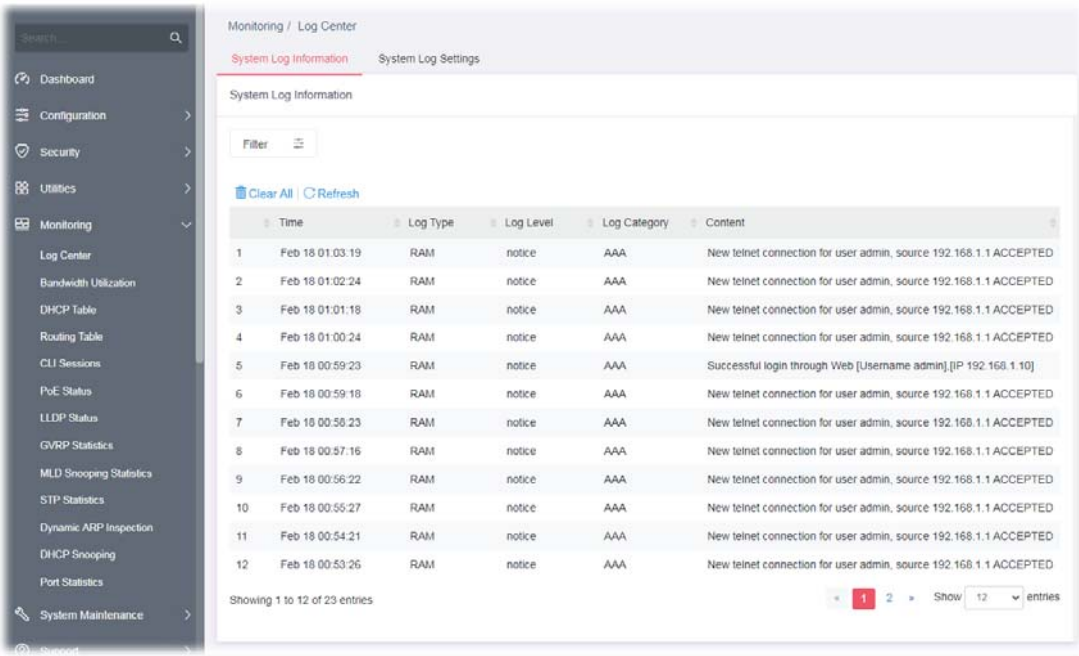
After finishing this web page configuration, please click **OK** to save the settings.

# Chapter V Monitoring

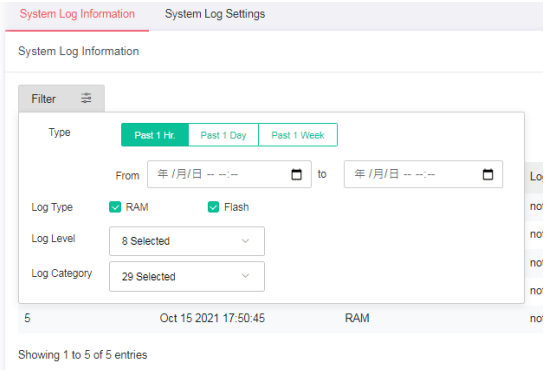
# V-1 Log Center

## 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:

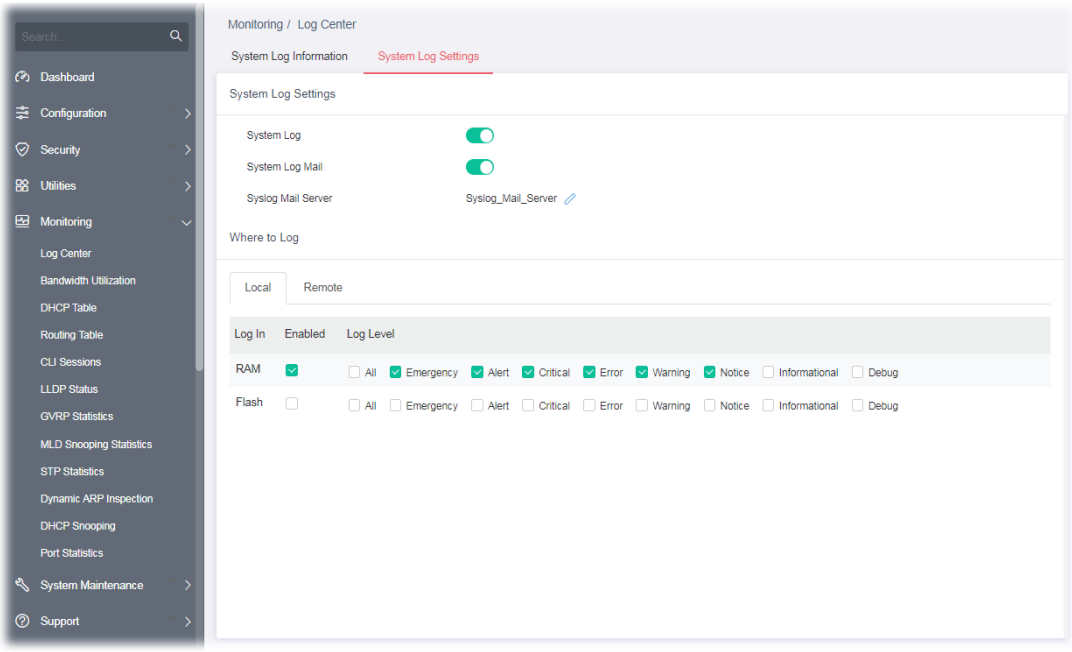
| Item | Description |
|---|---|
| **Filter** | Click to set the conditions for filtering.<br>  <br>**Type** - Specify the time (Past 1 Hour, Past 1 Day, Past 1 Week) for filtering.<br>**Log Type** - Select RAM (explore the logs contained in volatile memory (also known as RAM) or Flash (explore the logs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

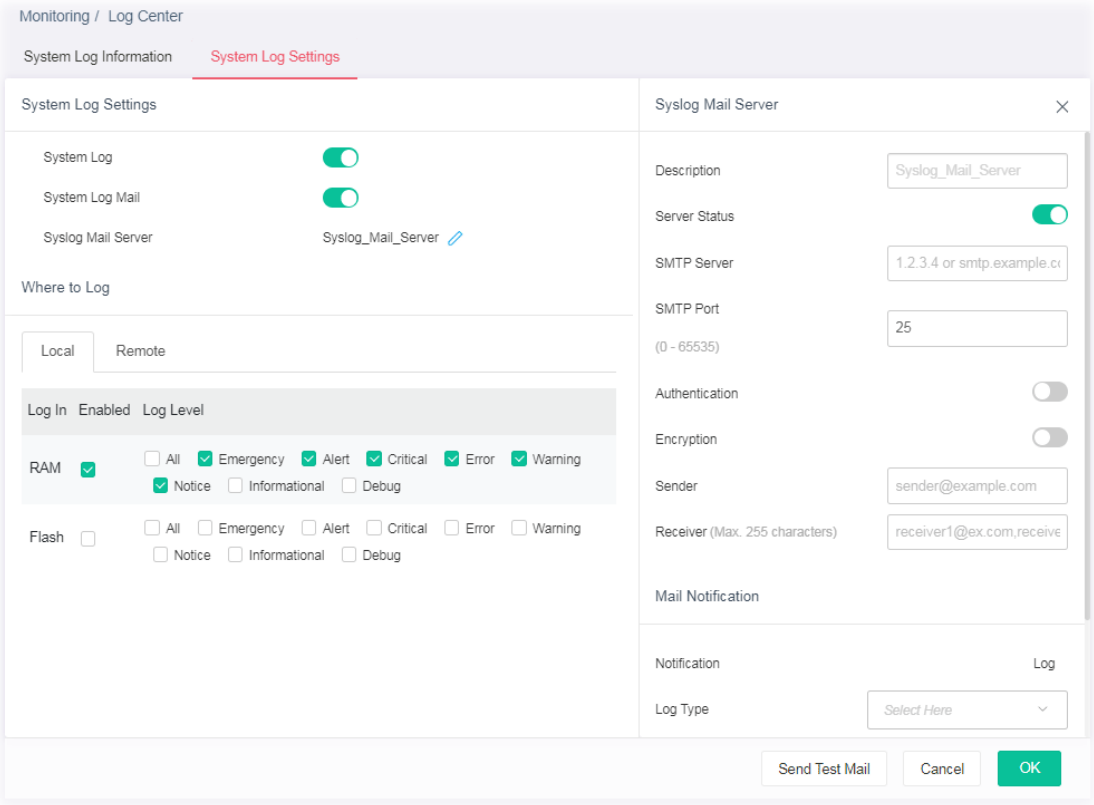



Available settings are explained as follows:

| Item | Description |
|---|---|
| **System Log Settings** | |
| **System Log** | **Enable / Disable** – Click the toggle to enable / disable this function.<br>- means “Enable”.<br>- means “Disable”. |
| **System Log Mail** | **Enable / Disable** – Click 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.<br>**Enable** - Select the box to enable the log type (RAM/Flash).<br>**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:

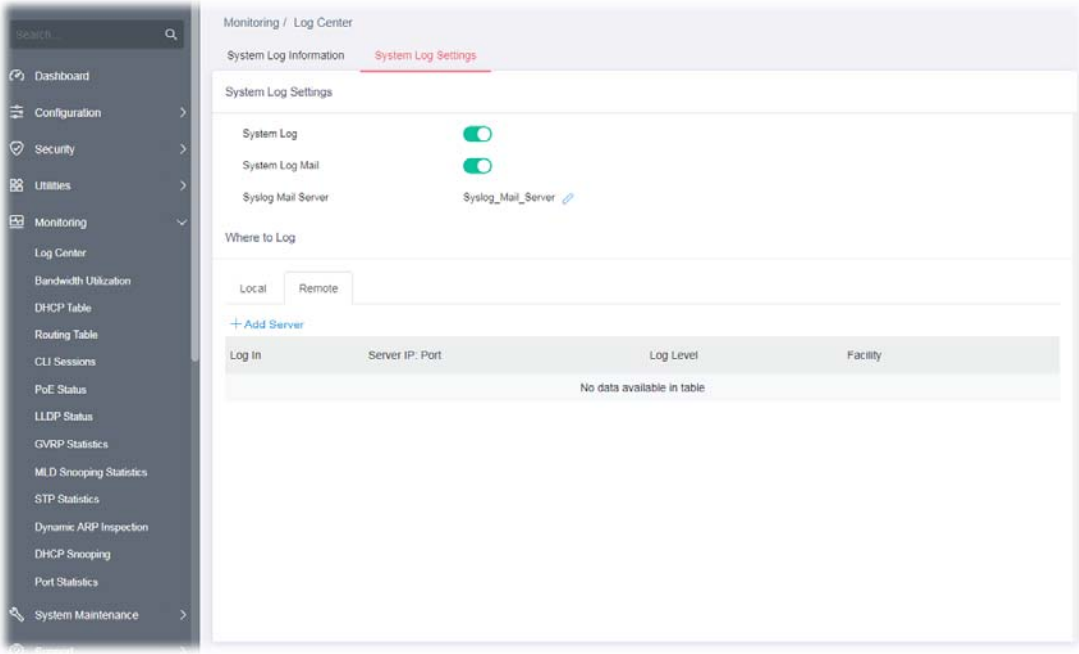
| Item | Description |
|---|---|
| **Syslog Mail Server** | |
| **Description** | Displays the name of the Syslog Mail Server. |
| **Server Status** | **Enable / Disable** – Click the toggle to enable / disable the Syslog Mail Server settings.<br>- means “Enable”.<br>- means “Disable”. |
| **SMTP Server** | Enter IP address or URL of the SMTP server. |
| **SMTP Port** | Enter the port number for the SMTP server. |
| **Authentication** | **Enable / Disable** – Click the toggle to enable / disable the authentication mechanism.<br>• **Username** - Enter a user name for authentication.<br>• **Password** - Enter a password for authentication. |

| | |
|---|---|
| **Encryption** | **Enable / Disable** – Click the toggle to enable / disable this function. After enabling Authentication, choose one of the encryption servers for data encryption.<br>● **STARTTLS** - The mail will be encrypted with StartTLS.<br>● **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.

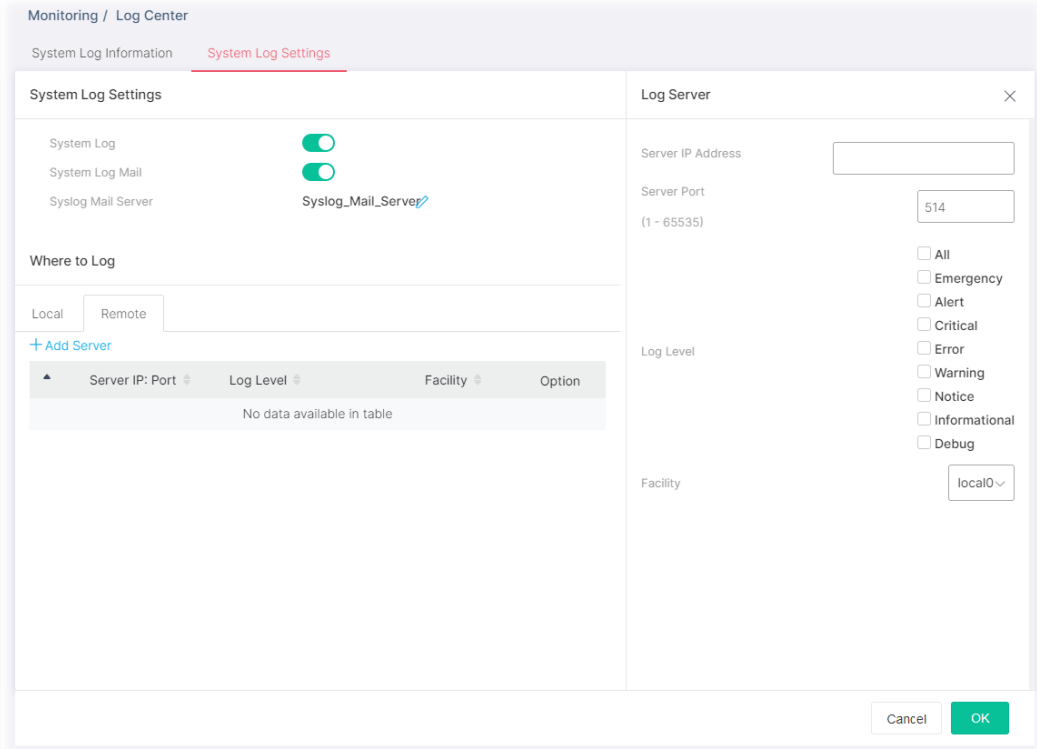



Available settings are explained as follows:

| Item | Description |
|---|---|
| **System Log Settings** | |
| **System Log** | **Enable / Disable** – Click the toggle to enable / disable this function.<br> - means “Enable”.<br> - means “Disable”. |
| **System Log Mail** | **Enable / Disable** – Click the toggle to enable / disable this function.<br>● **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.



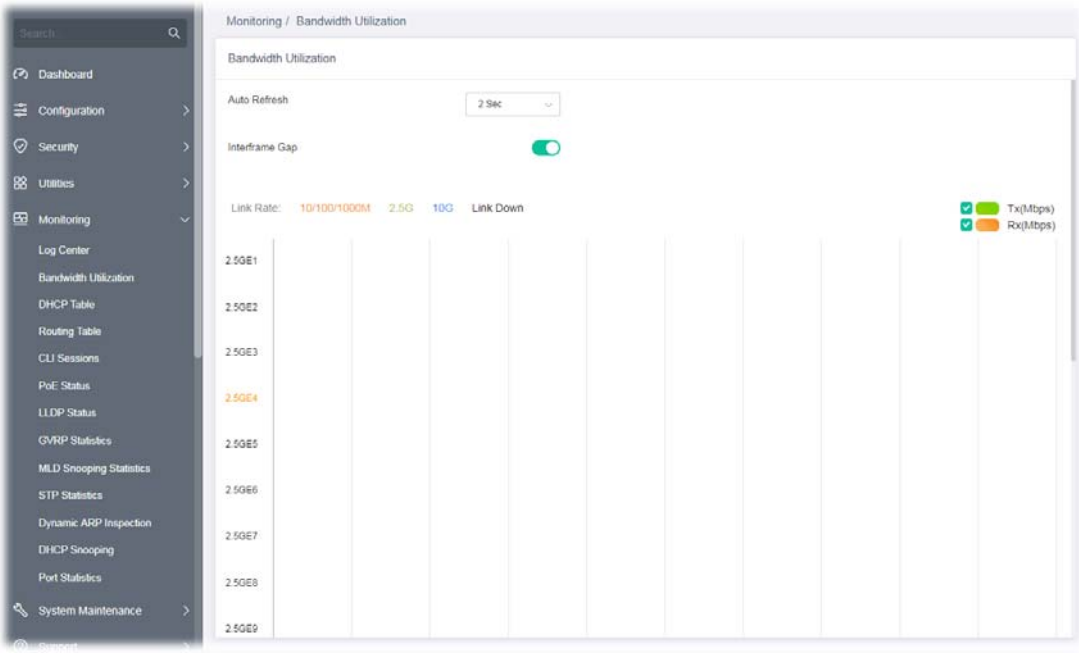

Available settings are explained as follows:

| 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.

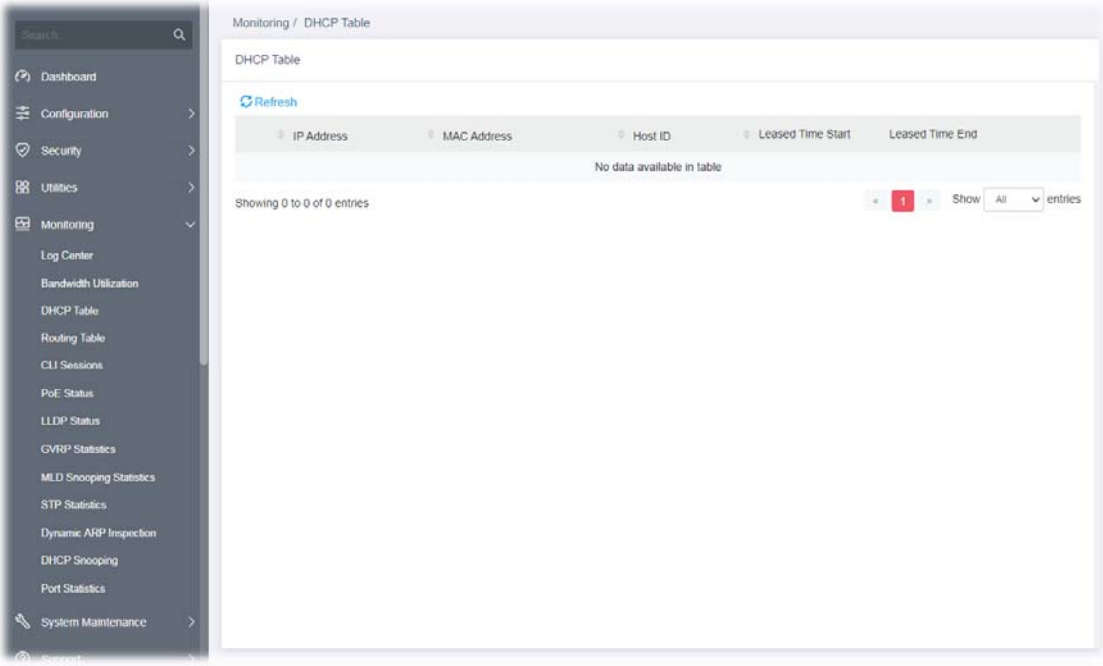



Available settings are explained as follows:

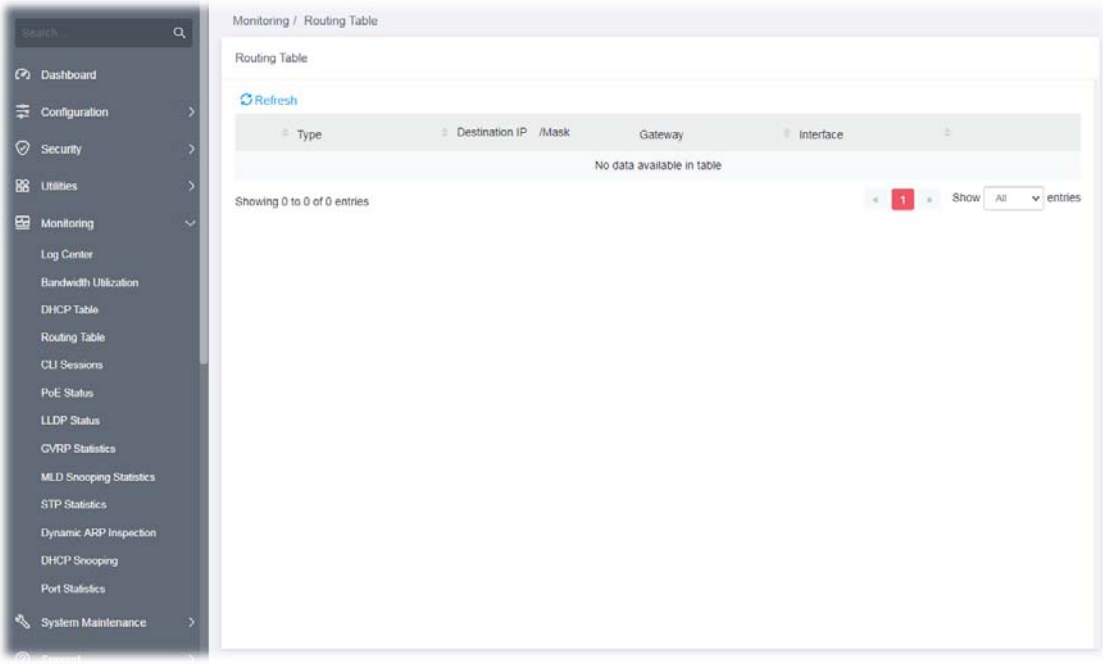
| Item | Description |
|---|---|
| **Auto Refresh** | Select the time interval for refreshing this page. |
| **Interframe Gap** | The data of the interframe gap can be displayed or hidden by enabling/disabling for Interframe Gap.<br>**Enable / Disable** – Click the toggle to enable / disable this function.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

# V-3 DHCP Table

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

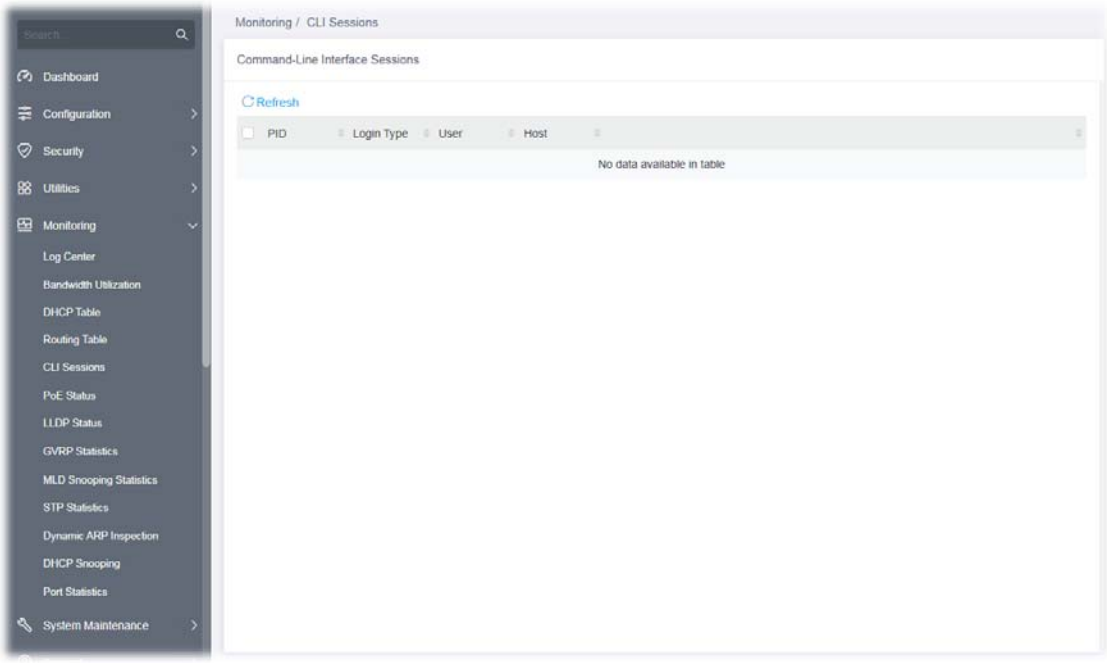


# V-4 Routing Table



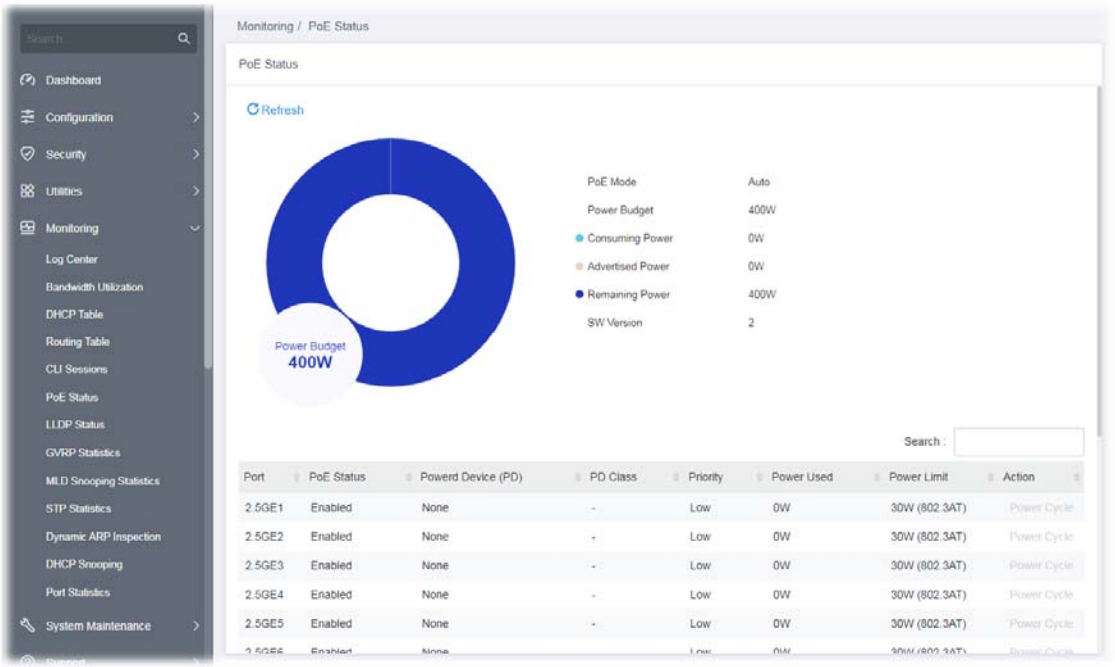
# V-5 CLI Sessions

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.



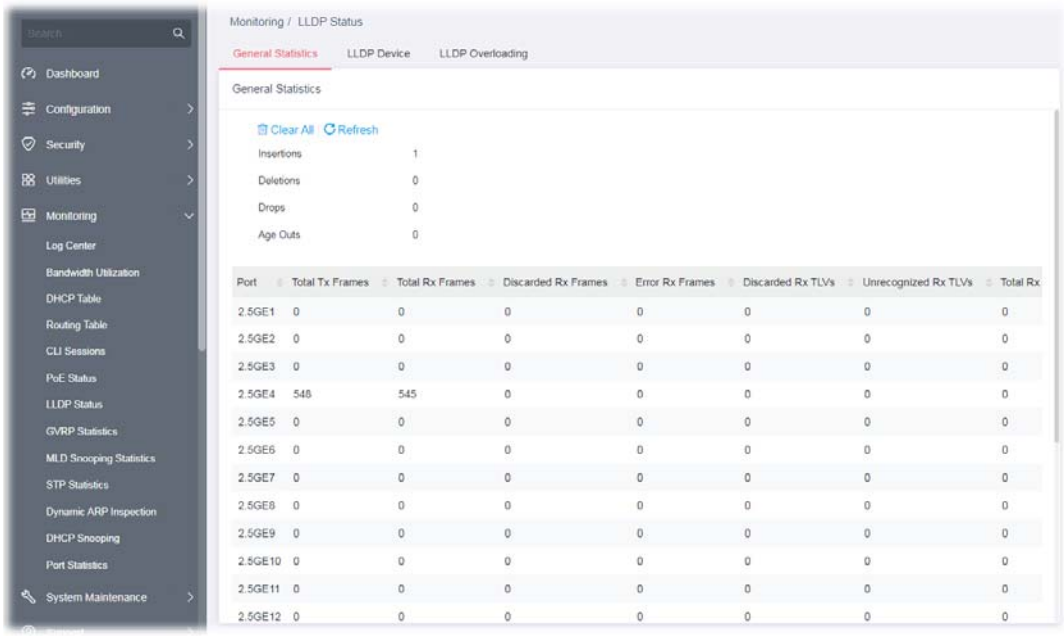

Available settings are explained as follows:

| 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 (GE1 to GE28). |
| **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 (2.5GE1 to 2.5GE16, 10GE1 to 10GE4).




Available settings are explained as follows:

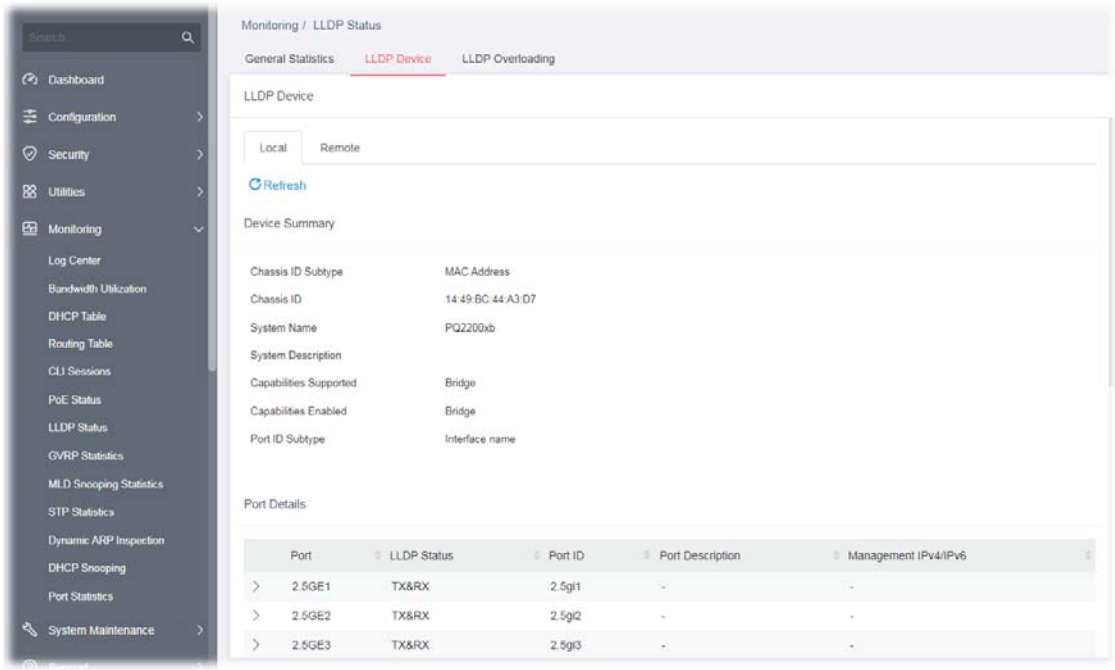
| Item | Description |
|---|---|
| **General Statistics** | |
| **Clear All** | Clear it to remove all logs displayed in this page. |
| **Refresh** | Click it to refresh the status page. |

# V-7-2 LLDP Device

This page displays information for LLDP local and remote devices.

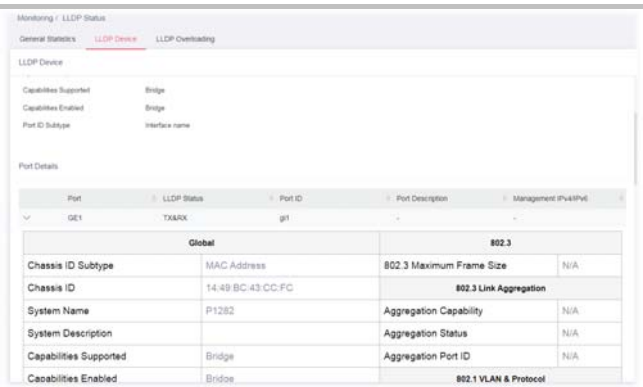
## V-7-2-1 Local

This page displays information for LLDP local device.



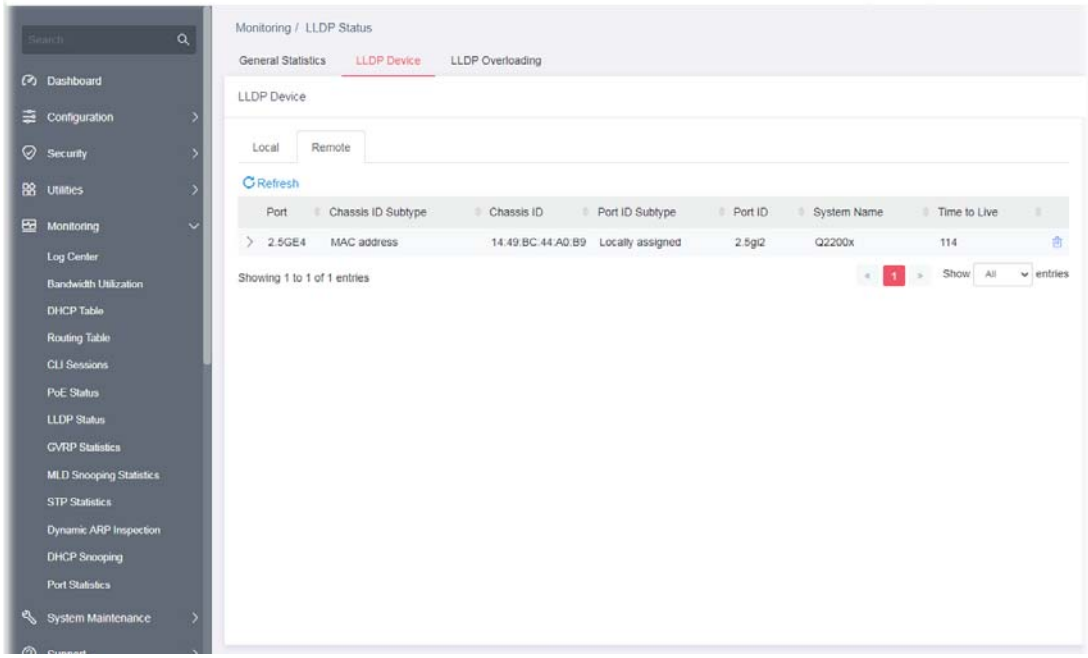

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Refresh** | Click it to refresh the status page. |
| **Device Summary** | Display a summary of the LLDP information for this switch.<br>**Chassis ID Subtype -** Display the type of chassis ID, such as the MAC address.<br>**Chassis ID -** Display Identifier of chassis. Where the chassis ID subtype is a MAC address, the MAC address of the switch is displayed.<br>**System Name -** Display model name of switch.<br>**System Description -** Display description of switch.<br>**Capabilities Supported -** Display the primary functions of the device, such as Bridge, WLAN AP, or Router.<br>**Capabilities Enabled -** Primary enabled functions of the device.<br>**Port ID Subtype -** Display the type of the port identifier that is shown. |
| **Port Details** | Display detailed information of the selected GE port.<br>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 (2.5GE1 to 2.5GE16, 10GE1 to 10GE4). |



## V-7-2-2 Remote

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

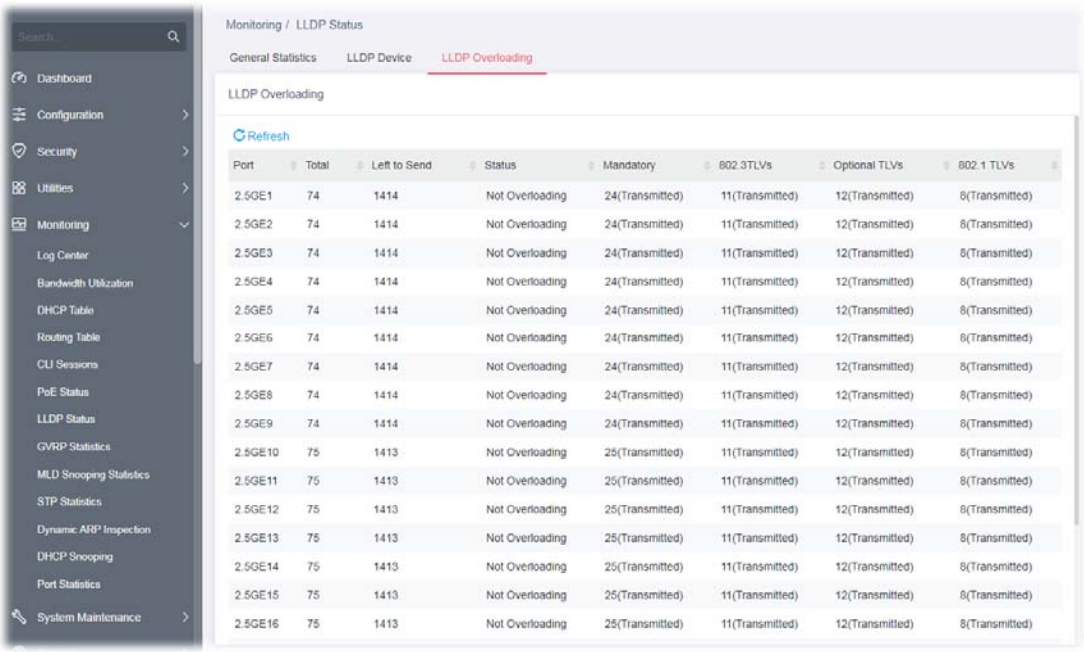



Available settings are explained as follows:

| 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.



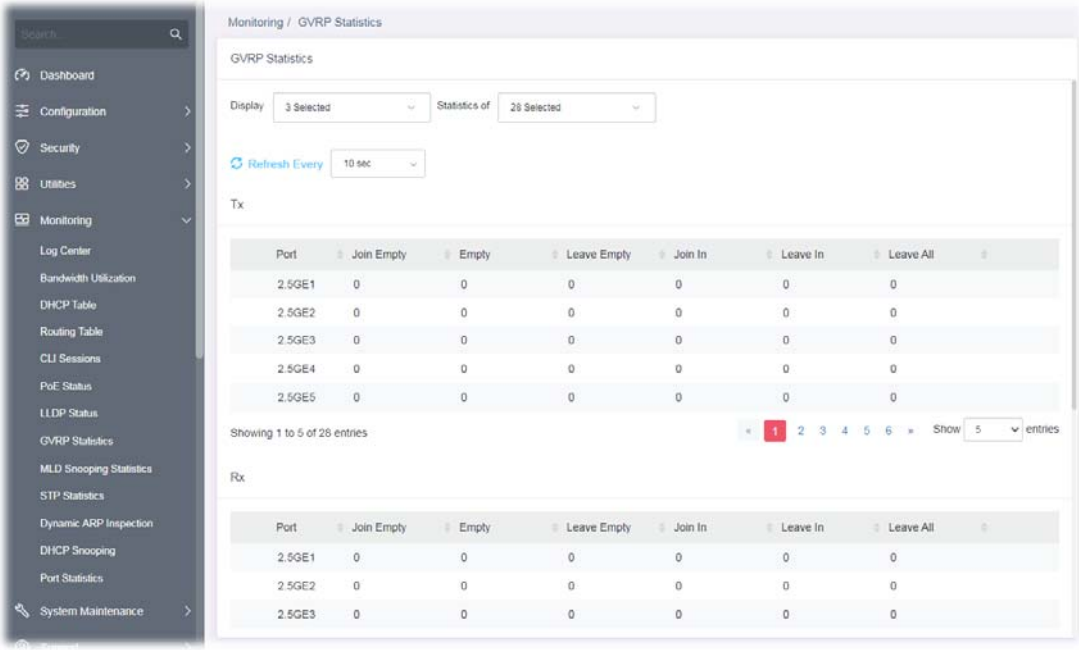

| Port | Total | Left to Send | Status | Mandatory | 802.3TLVs | Optional TLVs | 802.1 TLVs |
|---|---|---|---|---|---|---|---|
| 2.5GE1 | 74 | 1414 | Not Overloading | 24(Transmitted) | 11(Transmitted) | 12(Transmitted) | 8(Transmitted) |
| 2.5GE2 | 74 | 1414 | Not Overloading | 24(Transmitted) | 11(Transmitted) | 12(Transmitted) | 8(Transmitted) |
| 2.5GE3 | 74 | 1414 | Not Overloading | 24(Transmitted) | 11(Transmitted) | 12(Transmitted) | 8(Transmitted) |
| 2.5GE4 | 74 | 1414 | Not Overloading | 24(Transmitted) | 11(Transmitted) | 12(Transmitted) | 8(Transmitted) |
| 2.5GE5 | 74 | 1414 | Not Overloading | 24(Transmitted) | 11(Transmitted) | 12(Transmitted) | 8(Transmitted) |
| 2.5GE6 | 74 | 1414 | Not Overloading | 24(Transmitted) | 11(Transmitted) | 12(Transmitted) | 8(Transmitted) |
| 2.5GE7 | 74 | 1414 | Not Overloading | 24(Transmitted) | 11(Transmitted) | 12(Transmitted) | 8(Transmitted) |
| 2.5GE8 | 74 | 1414 | Not Overloading | 24(Transmitted) | 11(Transmitted) | 12(Transmitted) | 8(Transmitted) |
| 2.5GE9 | 74 | 1414 | Not Overloading | 24(Transmitted) | 11(Transmitted) | 12(Transmitted) | 8(Transmitted) |
| 2.5GE10 | 75 | 1413 | Not Overloading | 25(Transmitted) | 11(Transmitted) | 12(Transmitted) | 8(Transmitted) |
| 2.5GE11 | 75 | 1413 | Not Overloading | 25(Transmitted) | 11(Transmitted) | 12(Transmitted) | 8(Transmitted) |
| 2.5GE12 | 75 | 1413 | Not Overloading | 25(Transmitted) | 11(Transmitted) | 12(Transmitted) | 8(Transmitted) |
| 2.5GE13 | 75 | 1413 | Not Overloading | 25(Transmitted) | 11(Transmitted) | 12(Transmitted) | 8(Transmitted) |
| 2.5GE14 | 75 | 1413 | Not Overloading | 25(Transmitted) | 11(Transmitted) | 12(Transmitted) | 8(Transmitted) |
| 2.5GE15 | 75 | 1413 | Not Overloading | 25(Transmitted) | 11(Transmitted) | 12(Transmitted) | 8(Transmitted) |
| 2.5GE16 | 75 | 1413 | Not Overloading | 25(Transmitted) | 11(Transmitted) | 12(Transmitted) | 8(Transmitted) |

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. |

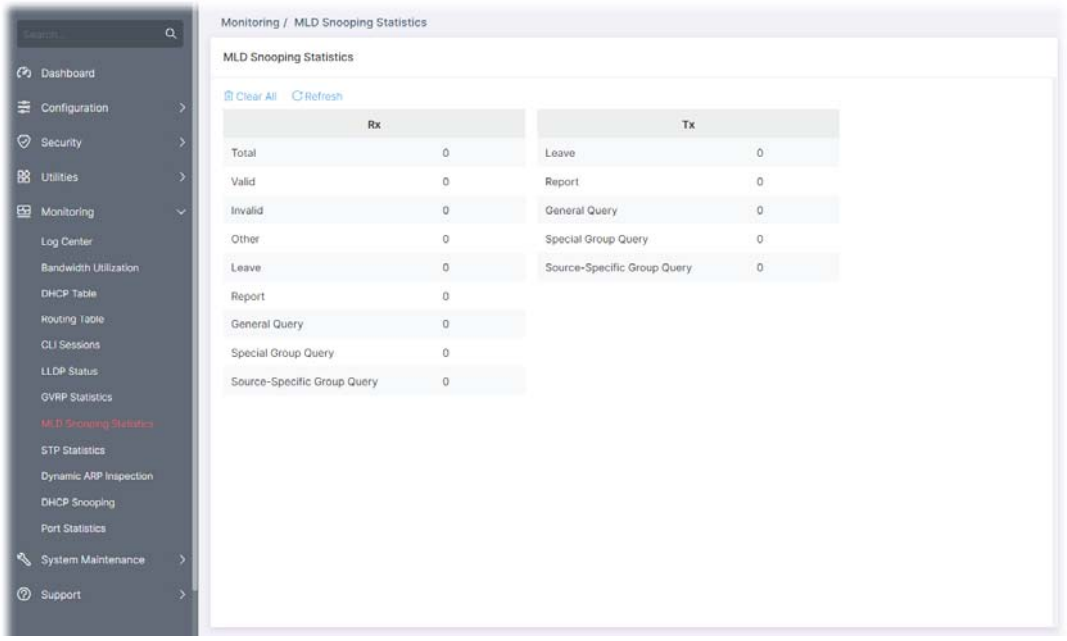
# V-8 GVRP Statistics

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 MLD Snooping Statistics

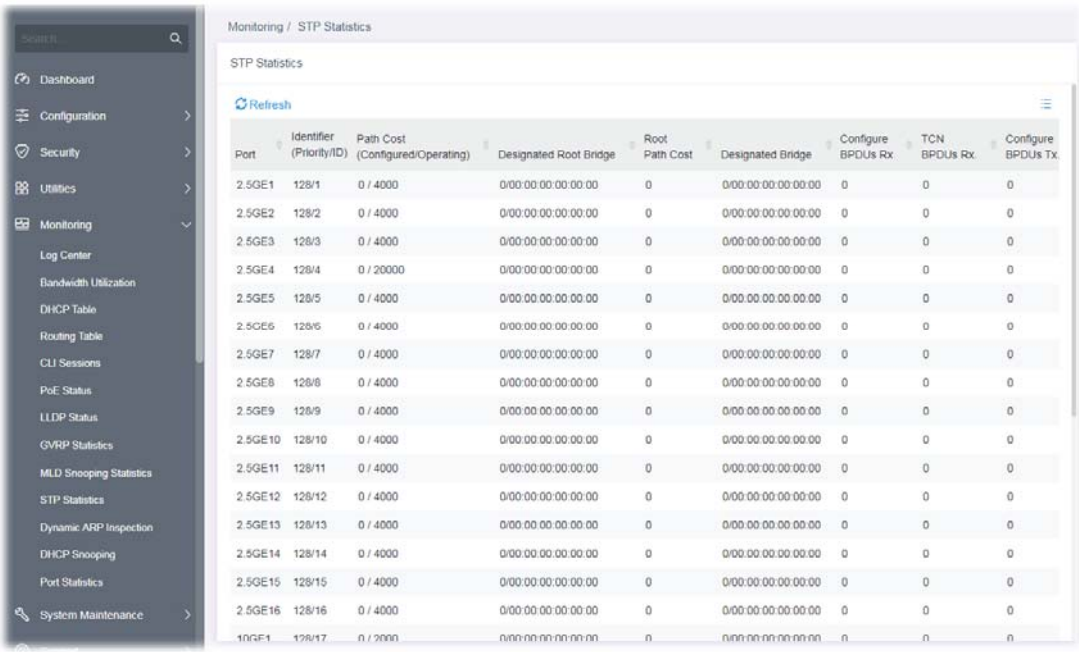
This page counts the MLD messages received or transmitted on the network.



# V-10 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.

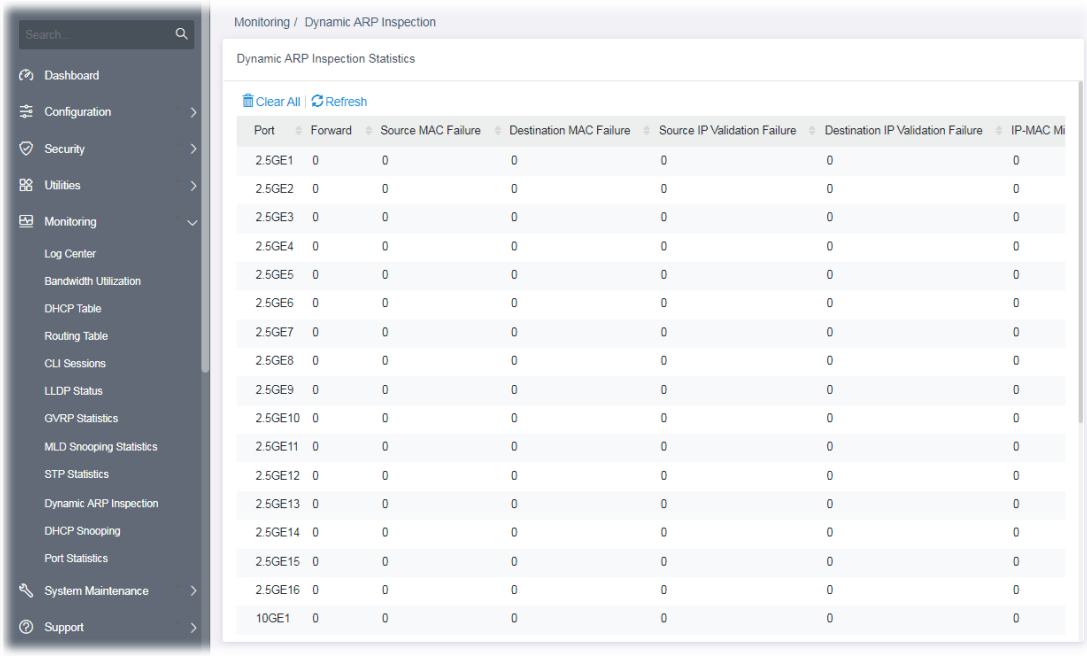
This page allows users to edit the general setting of the STP CIST port and browser CIST port status.



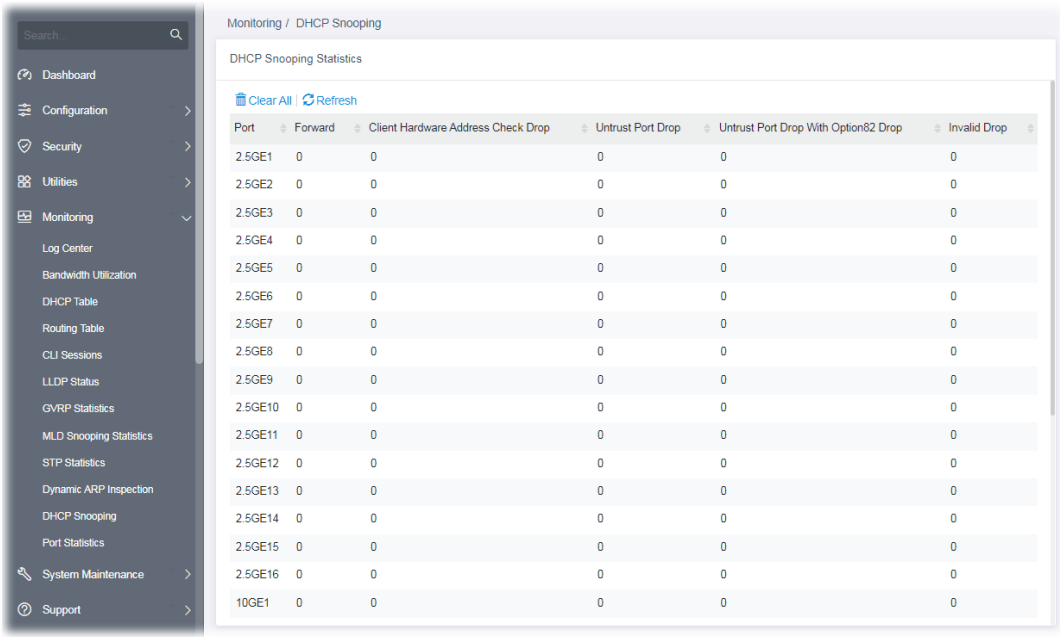

Available settings are explained as follows:

| 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-11 Dynamic ARP Statistics

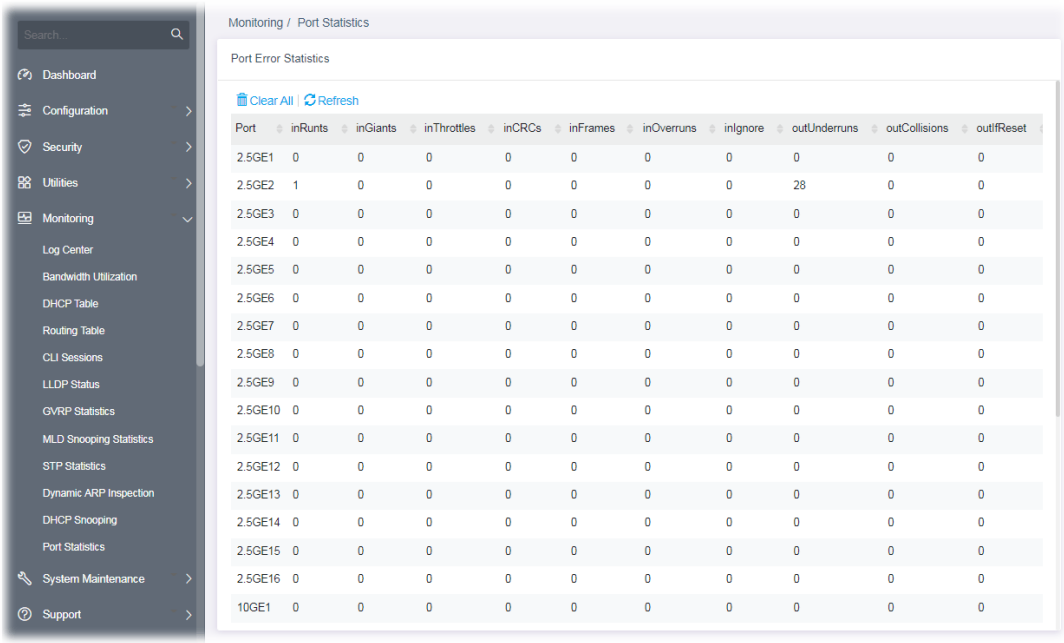


# V-12 DHCP Snooping



# V-13 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. |

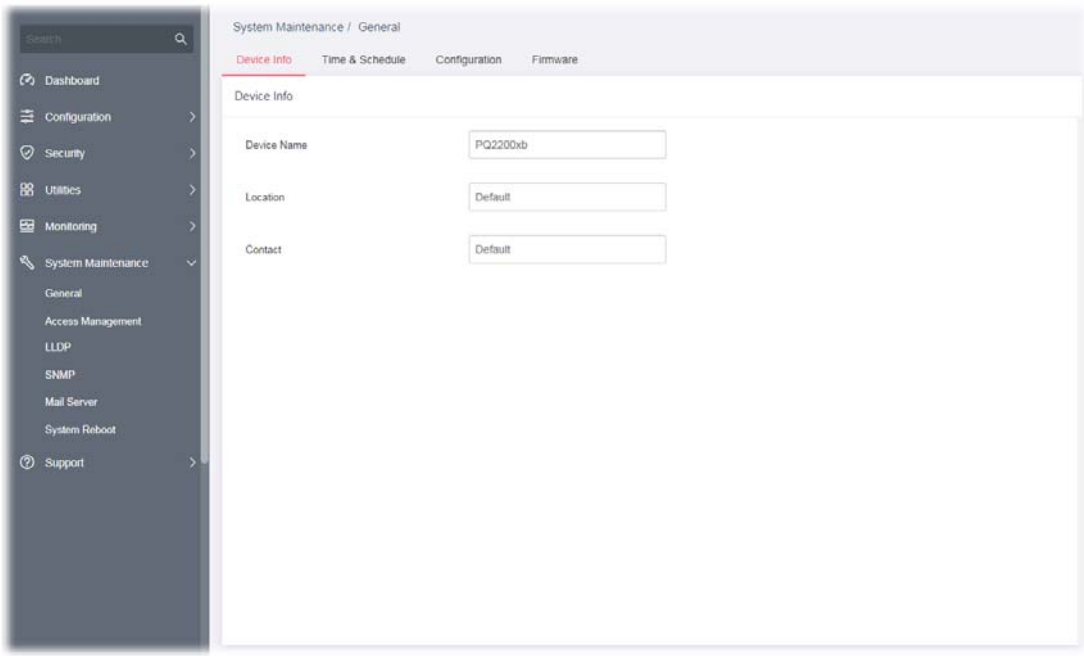
This page is left blank.

# Chapter VI System Maintenance

# VI-1 General

## VI-1-1 Device Info

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



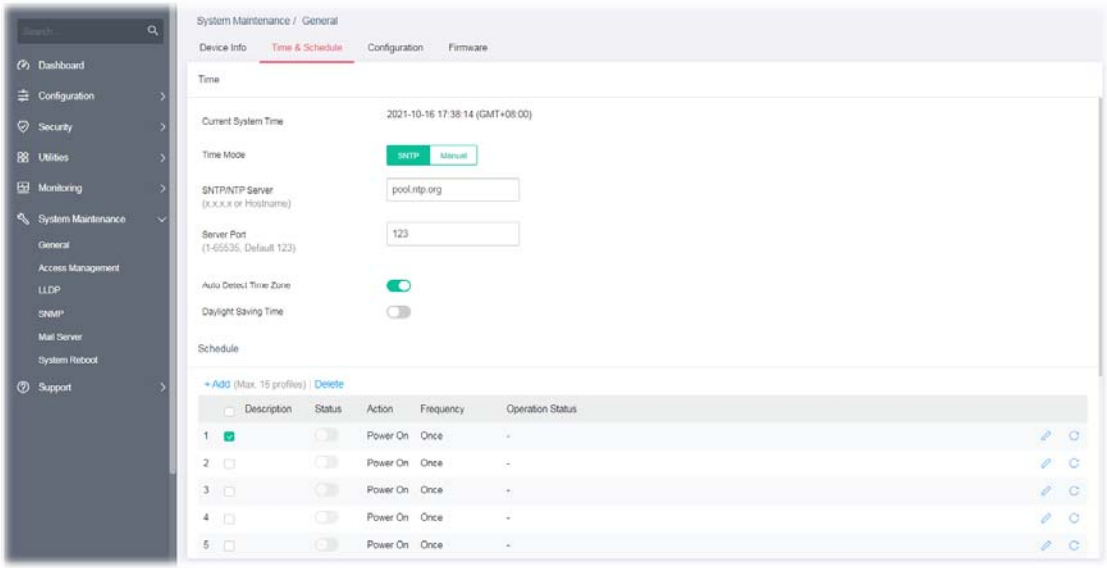

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Device Name** | Displays the name of this VigorSwitch.<br>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.



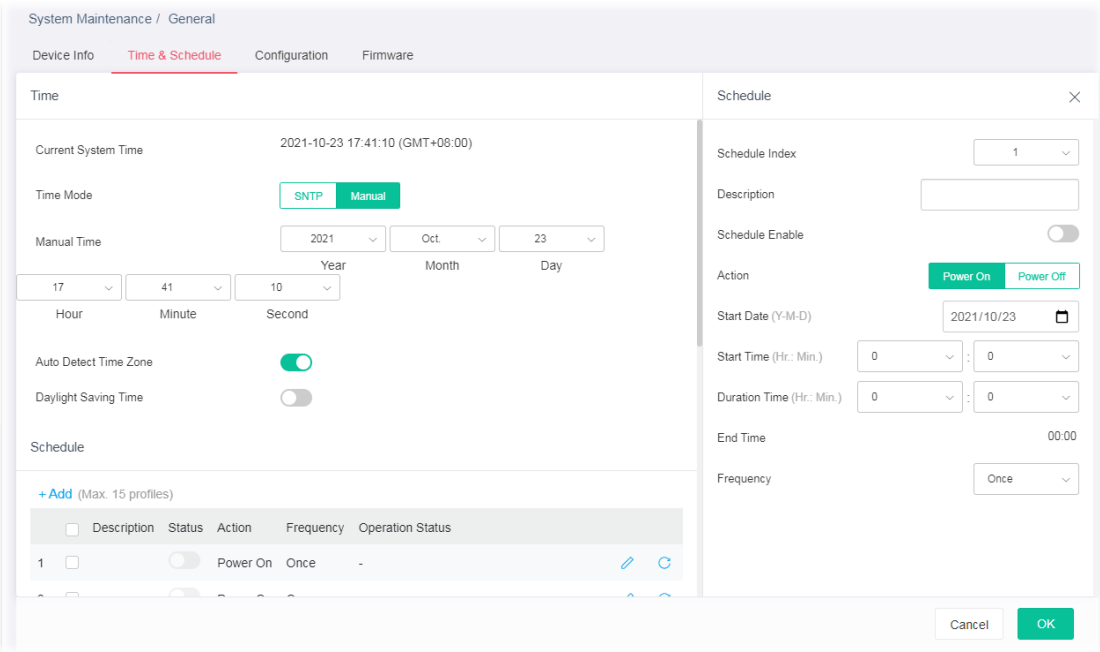

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Time** | |
| **Current System Time** | Display current system time based on the time server. |
| **Time Mode** | Select **SNTP** or **Manual**.<br>If SNTP is selected, configure:<br>• **SNTP/NTP Server** - Enter the web site of the time server or the IP address of the server.<br>• **Server Port** - Enter the port number use by the time server.<br>If Manual is selected, configure:<br>• **Manual Time** - Specify static time (year, month, day, hours, minutes and seconds) manually.<br>**Auto Detect Time Zone** - Click the toggle to enable / disable this function.<br> - means “Enable”.<br> - means “Disable”.<br>**Daylight Saving Time** - Click the toggle to enable / disable this function. If enabled, select the mode of daylight saving time.<br>• **Recurring** - Using recurring mode of daylight saving time.<br>• **Non-Recurring** – Using non-recurring mode of daylight saving time.<br>• **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.<br>• **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.<br>**Recurring From** - Specify the starting time of recurring daylight saving time.<br>**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.<br>**Non-recurring From** - Specify the starting time of non-recurring daylight saving time.<br>**Non-recurring To** - Specify the ending time of recurring daylight saving time. |
| **Schedule** | |
| **+Add** | Click to add a new schedule (up to 15).<br>**Delete** - Click to remove a selected schedule profile. |
| **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. |
| | 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.

To add a schedule profile, click the "**+Add**" 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 Enable** | Click the toggle to enable / disable this function.<br> - means “Enable”. The selected schedule profile will take action as configured.<br> - 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.<br>**Power On** – PoE connection is always on.<br>**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.<br>**Once** - The schedule will be applied just once.<br>**Weekdays Routine** - Specify which days in one week should perform the schedule.<br>• **Every** - Check to select the days in a week.<br>**Monthly Routine** - Specify the day in a month as the starting point.<br>• **Duration Time** - Use the drop down list to select the date in a month.<br>**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.<br>• **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.

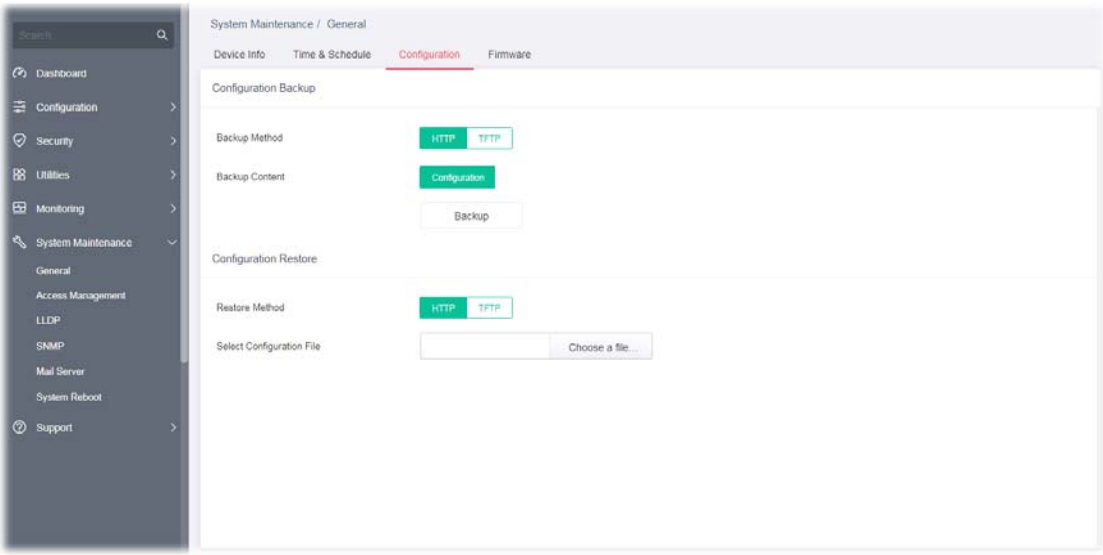
To modify an existing schedule profile, click the link of of the one to be changed.

After clicking **OK**, the existed schedule profile will be changed.

# 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.



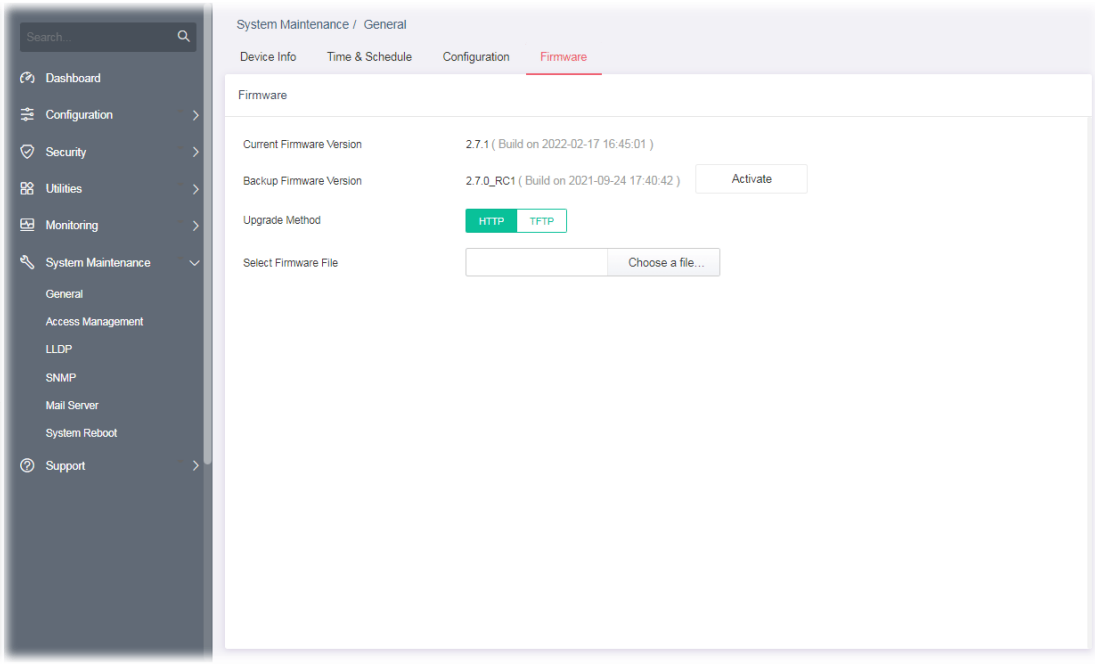

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Configuration Backup** | |
| **Backup Method** | Select Backup method.<br>**HTTP** - Use WEB browser to backup firmware.<br>**TFTP** - Use TFTP to backup firmware.<br>● **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.<br>**HTTP** - Use WEB browser to restore firmware.<br>● **Select Configuration File** - Choose the file which will be used to restore the configuration settings.<br>**TFTP** - Use TFTP to restore firmware.<br>● **Server IP Address** - Enter the IPv4/IPv6 address for the TFTP server.<br>● **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:<br>**HTTP** - Use WEB browser to upgrade firmware.<br>• **Select Firmware File -** Choose the firmware file located in your computer.<br>**TFTP** - Use TFTP to upgrade firmware.<br>• **Server IP Address** - Enter the IPv4/IPv6 address for the TFTP server.<br>• **File Name** - Enter the firmware image or configuration file name on the TFTP server. |

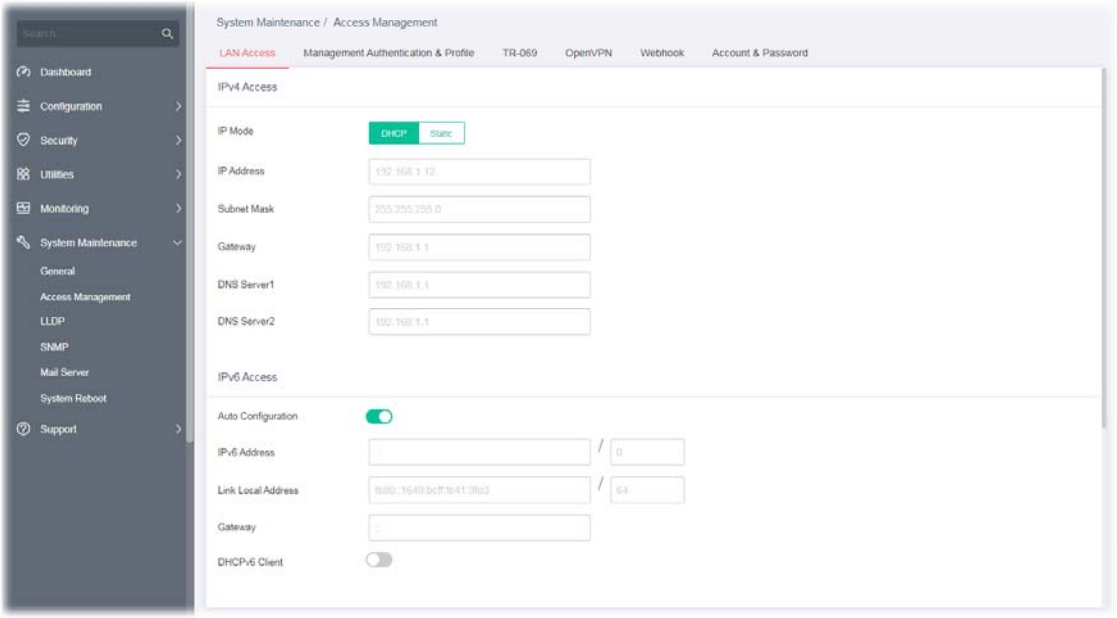
After finishing this web page configuration, please click **OK** to save the settings.

# VI-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:

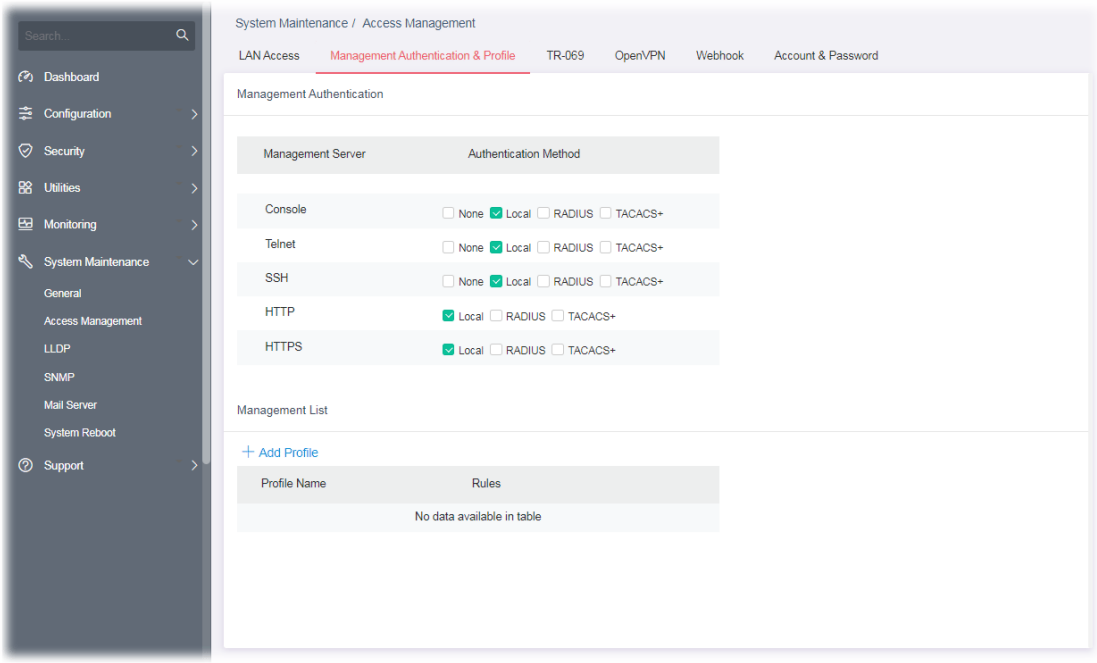
| Item | Description |
|---|---|
| **IPv4 Access** | |
| **IP Mode** | Select the mode of network connection**.**<br>**DHCP** - Use static IPv4 address.<br>**Static** - Use DHCP provisioned IP address and Gateway if feasible.<br>• **IP Address** - Enter the IP address of your switch in dotted decimal notation for example 192.168.1.224. If static mode is enabled, enter IP address in this field.<br>• **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.<br>• **Gateway** - Enter the IP address of the gateway in dotted decimal notation. If static mode is enabled, enter gateway address in this field.<br>• **DNS Server1/2** - Enter primary/ secondary DNS server address |

| | |
|---|---|
| | in this field. |
| **IPv6 Access** | |
| **Auto Configuration** | **Enabled** - Let the switch automatically configure IPv6 address.<br>Click the toggle to enable / disable this function.<br> - means “Enable”.<br> - means “Disable”.<br>• **DHCPv6 Client** - Enable this feature if there is a DHCPv6 server on your network for assigning IPv6 Address, instead of using Router Advertisement.<br>**Disabled** -<br>• **IPv6 Address** - Enter the IPv6 address of your switch. If auto configuration mode is disabled, enter IPv6 address in this field.<br>• **Gateway** - Enter the IPv6 address of the router as your default IPv6 gateway to access IPv6 Internet or other IPv6 network.<br>• **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, Telnet Server, SSH Server, Enforce HTTPS Server** | 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

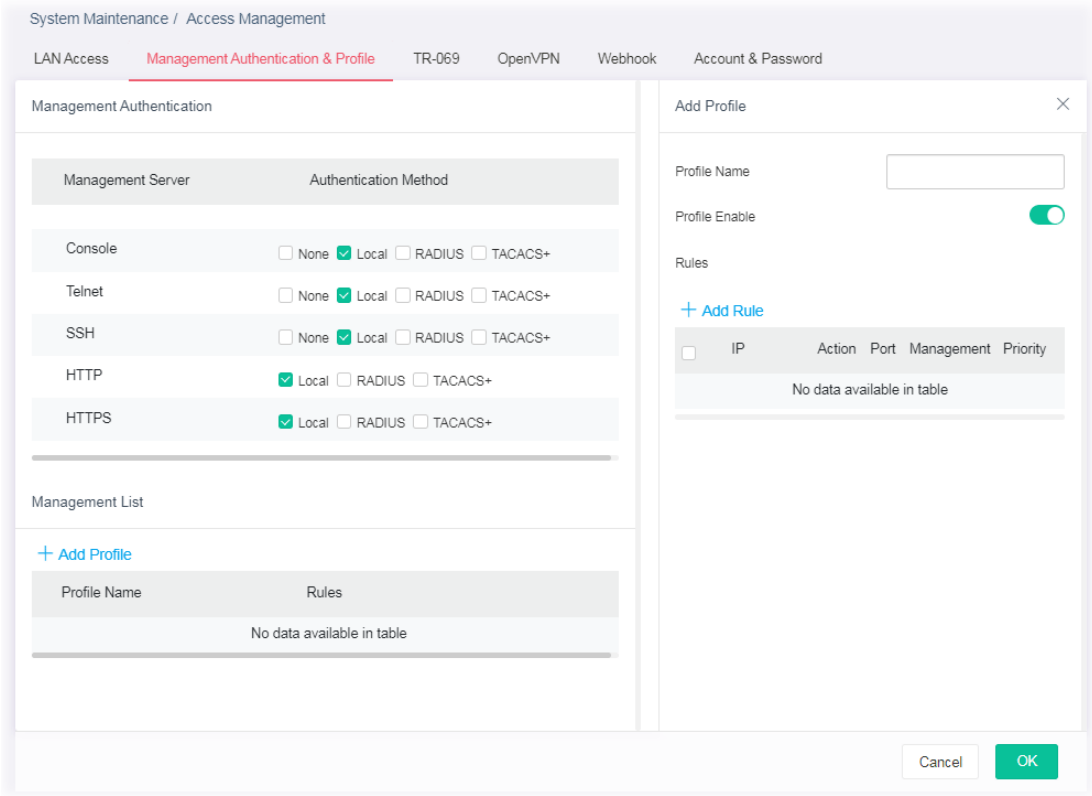
The system administrator can log in VigorSwitch from profiles defined on this page. All profiles will apply the configuration of management server(s) and authentication method(s) settings.




Available settings are explained as follows:

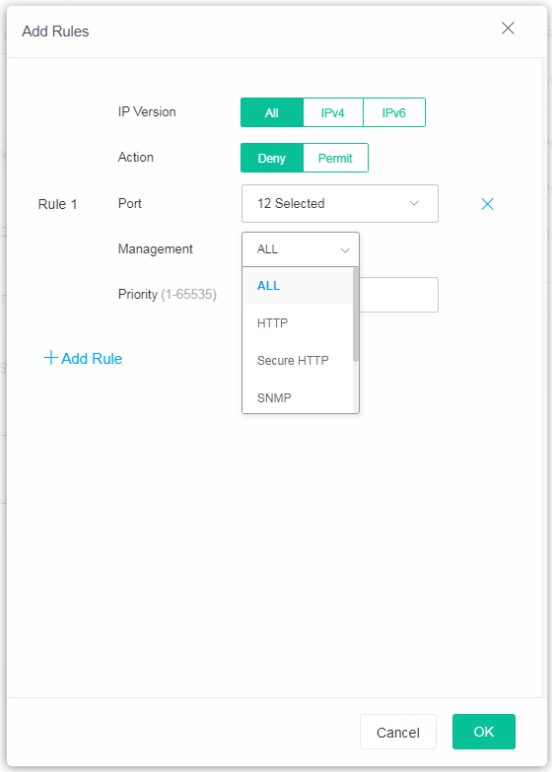
| Item | Description |
|---|---|
| **Management Authentication** | |
| **Management Server** | Displays available servers set as management server. |
| **Authentication Method** | Displays available protocols for different management servers.<br>Select one or more protocols for each server. |
| **Management List** | Displays a list of profiles that will apply the settings of server and authentication defined above.<br>**+ 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 |
|---|---|
| **MANAGEMENT ACCESS PROFILE** | |
| **Profile Name** | Enter a name for an authentication profile. |
| **Profile Enable** | Click the toggle to enable / disable this profile.<br>- means “Enable”.<br>- means “Disable”. |
| **+Add Rule** | Click to create a rule. |




**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.

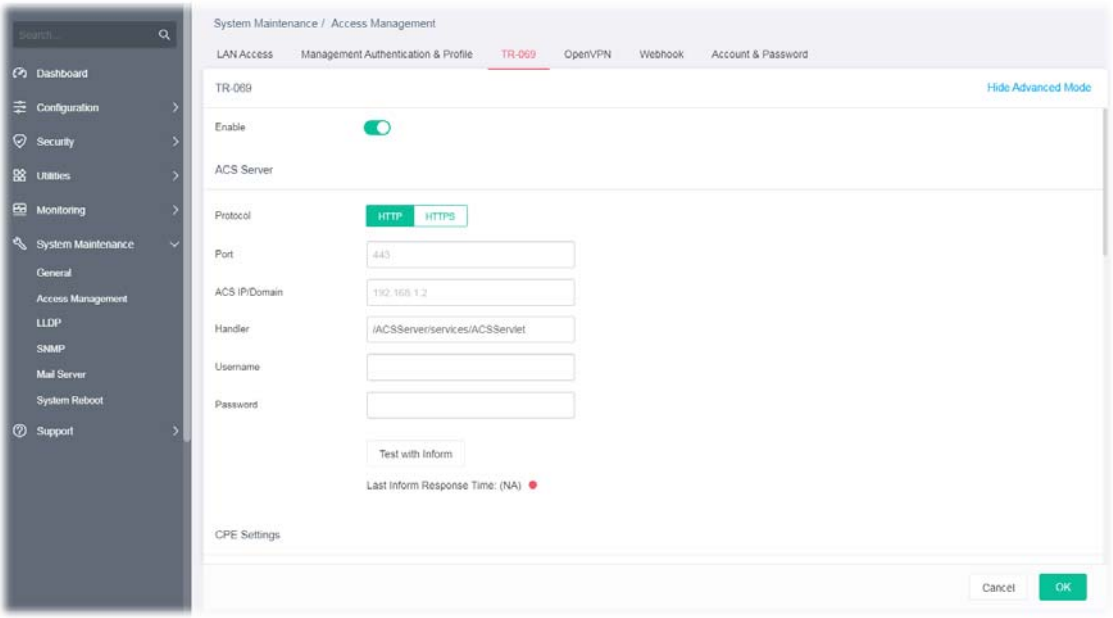
**Priority** - Specify a priority number (1 to 65535) for such rule. The lower the number, the higher the priority.

| | |
|---|---|
| **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:

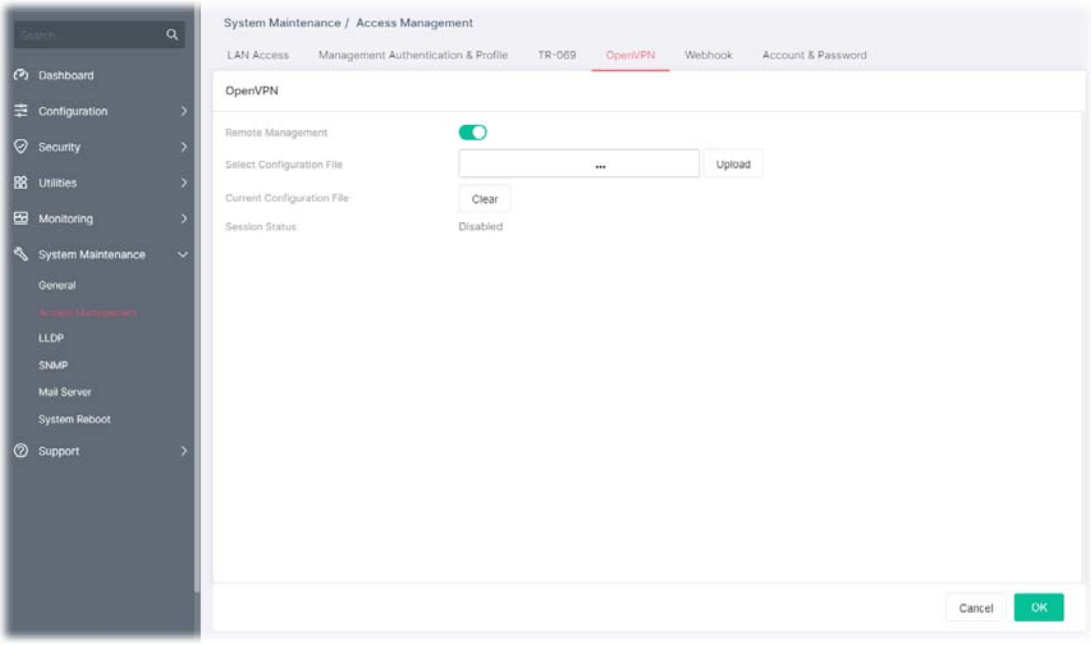
| Item | Description |
|---|---|
| **Show/Hide Advanced Mode** | Click to display / hide the advanced mode settings. |
| **TR-069** | Click the toggle to enable / disable this function.<br>- means “Enable”.<br>- means “Disable”. |
| **Basic Mode - ACS Server** | |
| **ACS IP/Domain** | Enter the IP address 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** | Click the toggle to enable/disable the function. |
| **Interval Time** | Set the interval time for the switch to send notification to CPE. |
| **STUN Settings** | |
| **Enabled** | Click the toggle to enable / disable this function.<br> - means “Enable”.<br> - 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.<br>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.



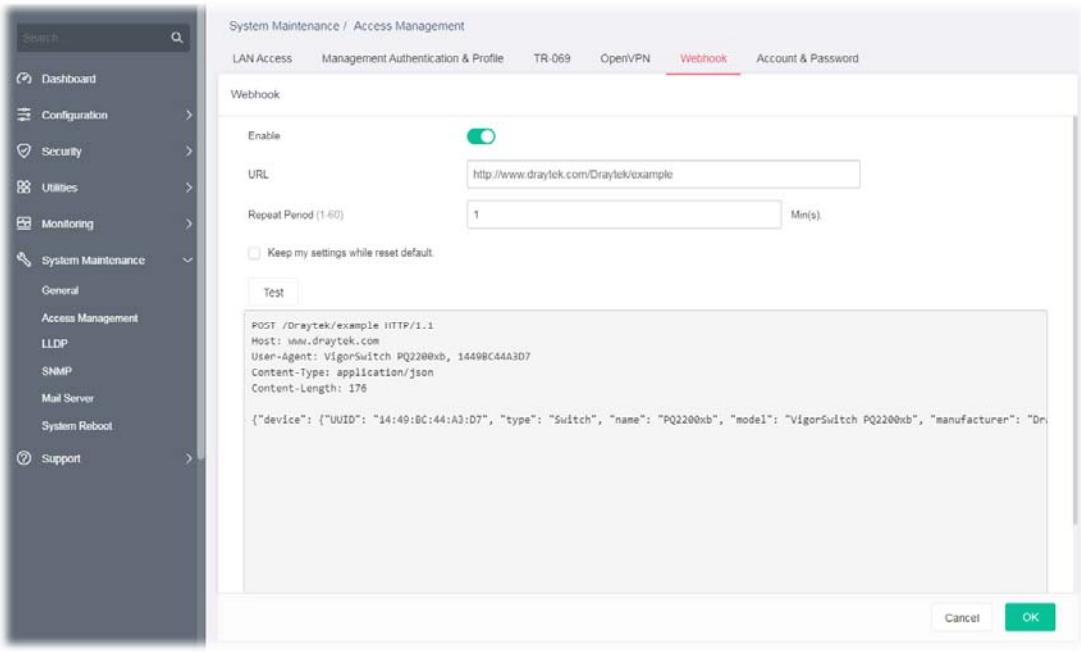

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Remote Management** | Click the toggle to enable / disable OpenVPN tunnel between VigorSwitch with the remote end.<br> - means “Enable”.<br> - means “Disable”. |
| **Select Configuration File** | It is available when remote management is enabled.<br>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.



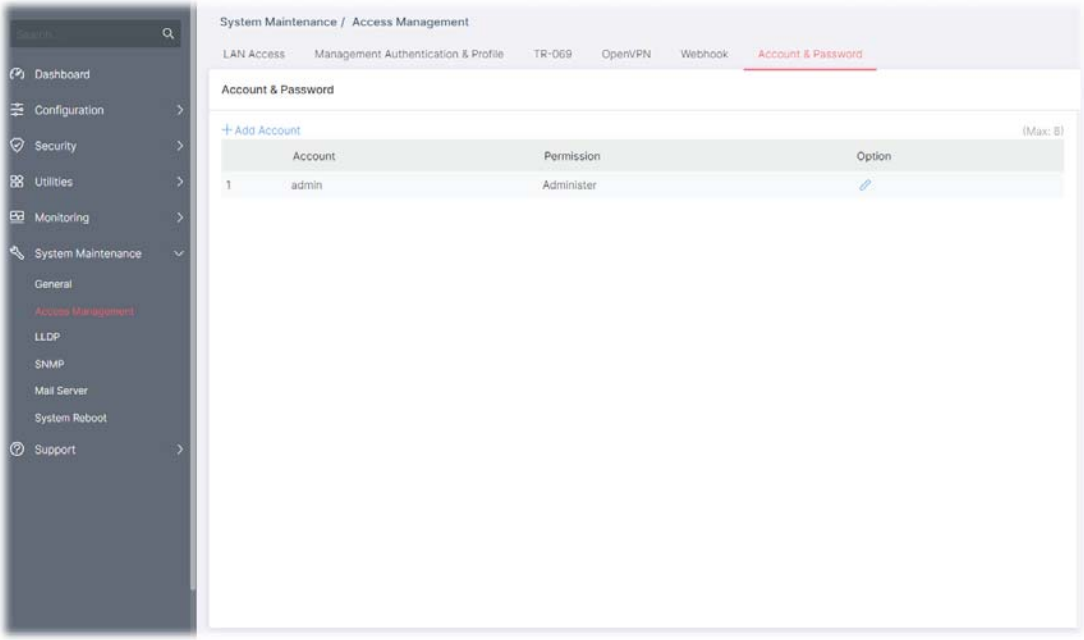

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Click the toggle to enable / disable the webhook service. The data will be transmitted to the specified URL.<br> - means “Enable”.<br> - means “Disable”. |
| **URL** | Specify the destination to receive the real-time data by entering the URL.<br>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.

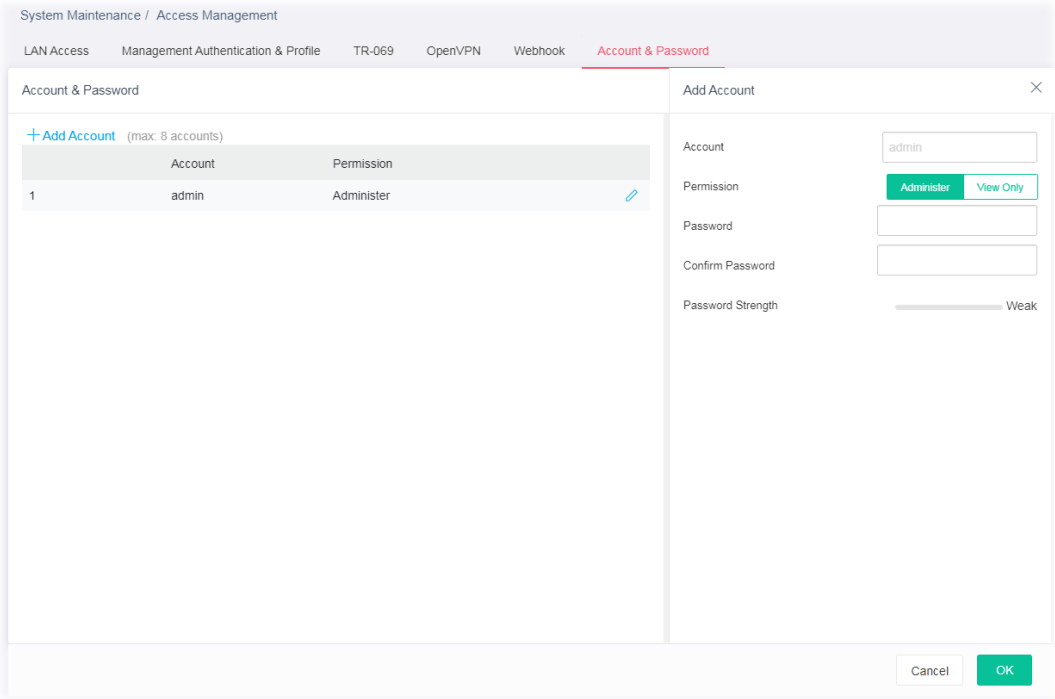



Available settings are explained as follows:

| Item | Description |
|---|---|
| **+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. |

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.<br>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.<br>**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”. |

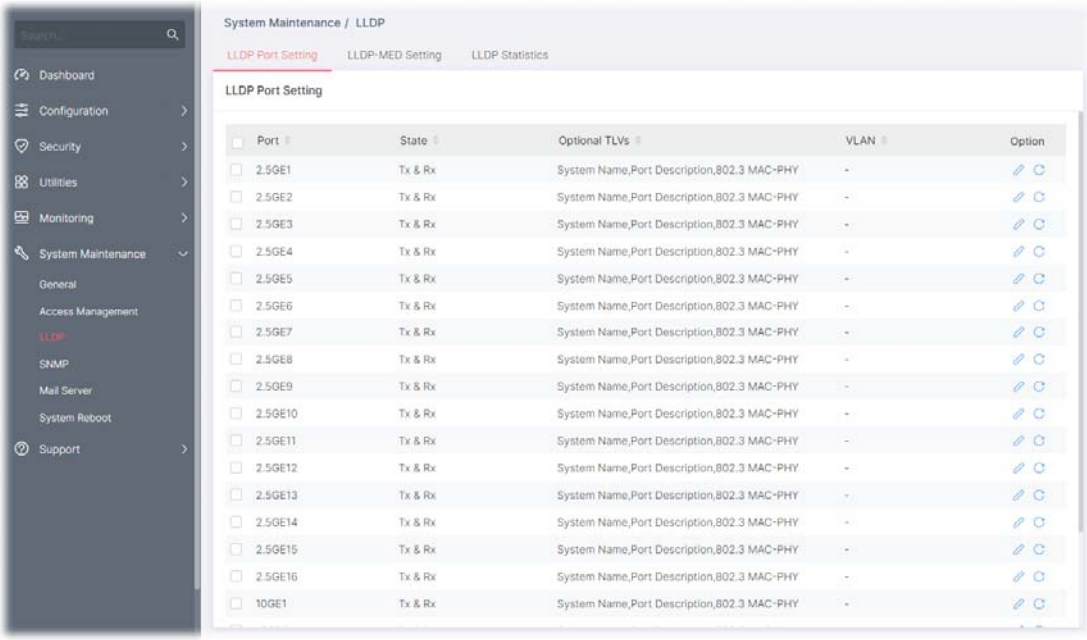
After finishing this web page configuration, please click **OK** to save the settings.

# 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

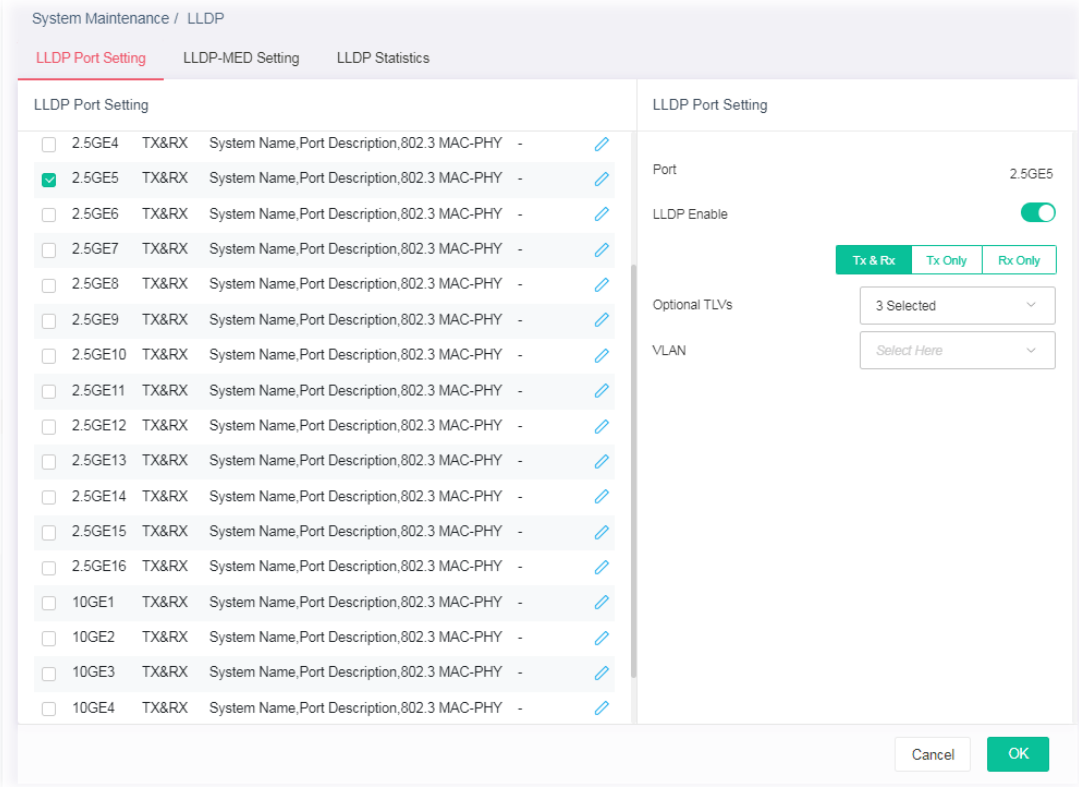
This page allows a user to select specified port or all ports to configure LLDP state.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Port** | Displays the index number of GE ports (2.5GE1 to 2.5GE16, 10GE1 to 10GE4). |
| **Status** | 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.<br>- 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.



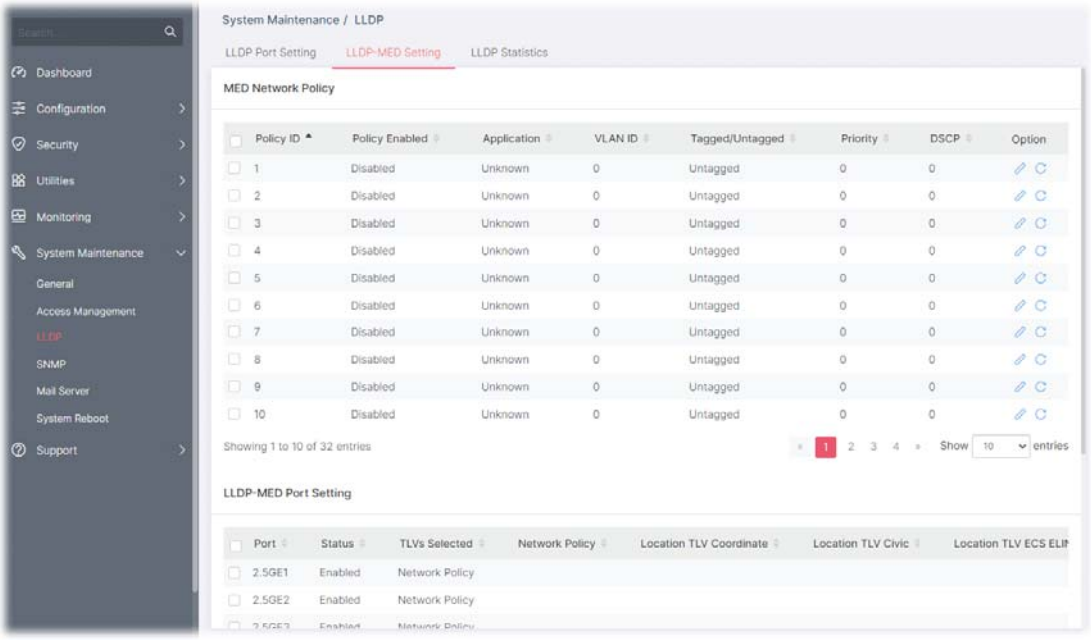

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Port** | Displays the index number of GE ports (2.5GE1 to 2.5GE16, 10GE1 to 10GE4). |
| **LLDP Enable** | Click the toggle to enable / disable this function.<br>- means “Enable”.<br>- means “Disable”.<br>**TX&RX** – Transmit and receive LLDP PDUs both.<br>**TX Only** – Transmit LLDP PDUs only.<br>**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.<br>The type and length are fixed in size (typically 1-4 bytes), and the value field is of variable size.<br>Select the LLDP optional TLVs to be carried (multiple selection is allowed).<br>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.

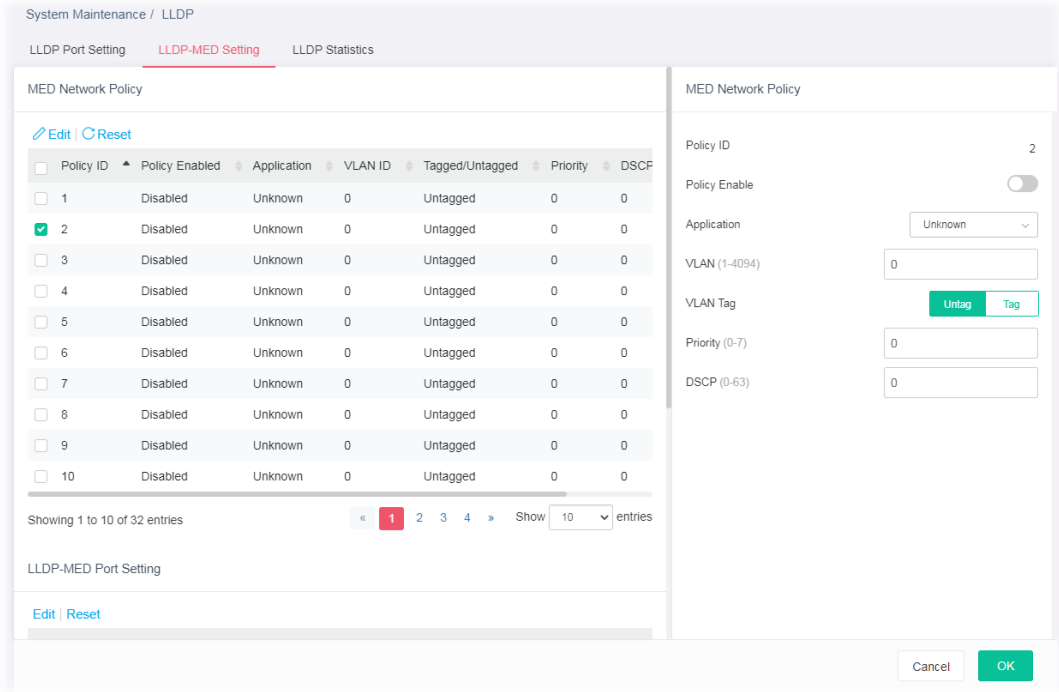



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Option** | - Click to modify the LLDP port settings of the selected policy.<br>- 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.



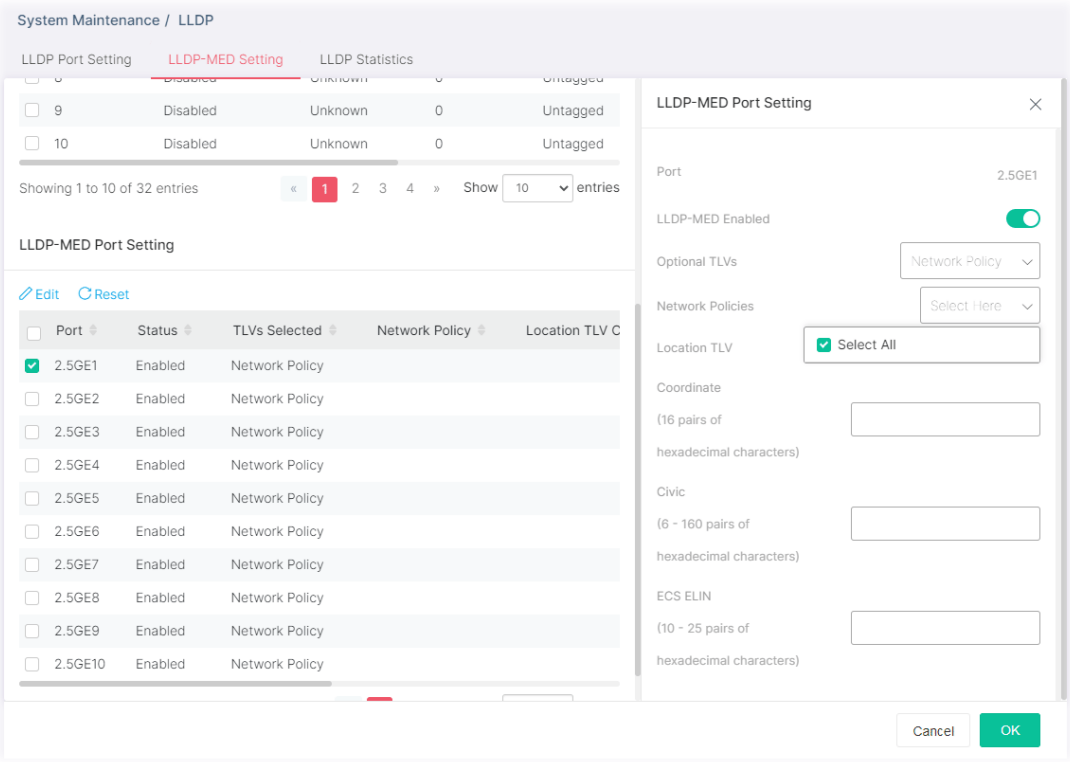

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Policy ID** | Choose a number for configuring the policy profile.<br>Available selections include 1 to 32. |
| **Policy Enable** | Click the toggle to enable / disable this function.<br>- means “Enable”.<br>- means “Disable”. |
| **Application** | There are several applications which can be used for MED network.<br>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.<br>**Untag** – Packets will be sent out without any tag.<br>**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.



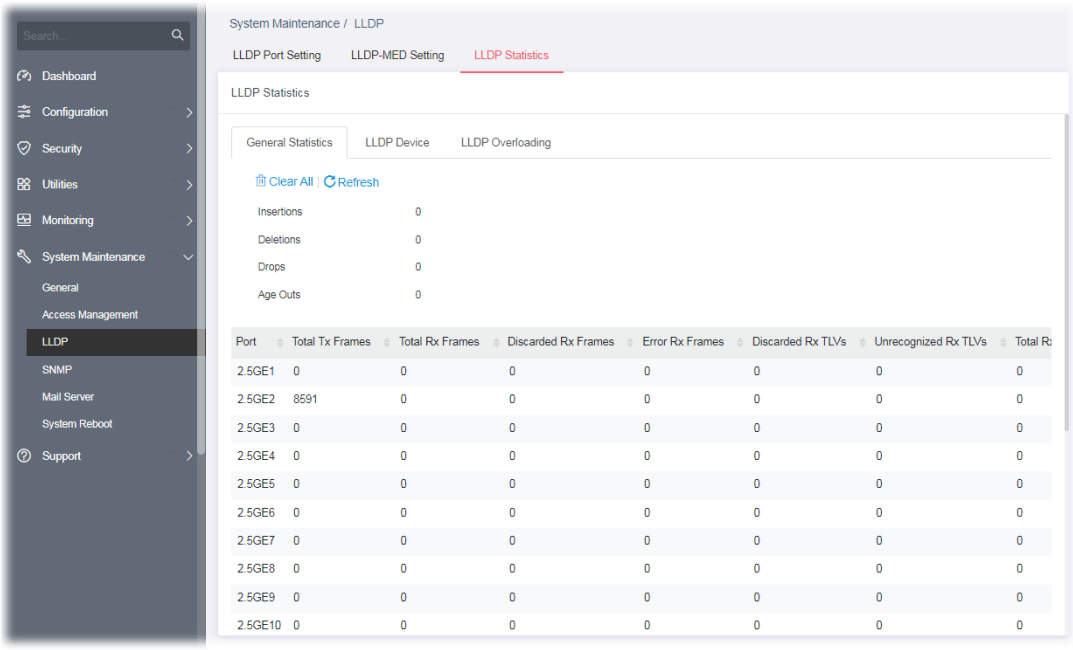

Available settings are explained as follows:

| Item | Description |
|---|---|
| **LLDP-MED Port Setting** | |
| **Port** | Displays the index number of LAN port. |
| **LLDP-MED Enable** | Click the toggle to enable / disable the LLDP MED on the selected port.<br> - means “Enable”.<br> - 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 (2.5GE1 to 2.5GE16, 10GE1 to 10GE4).




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 (GE1 to GE28). |

# 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

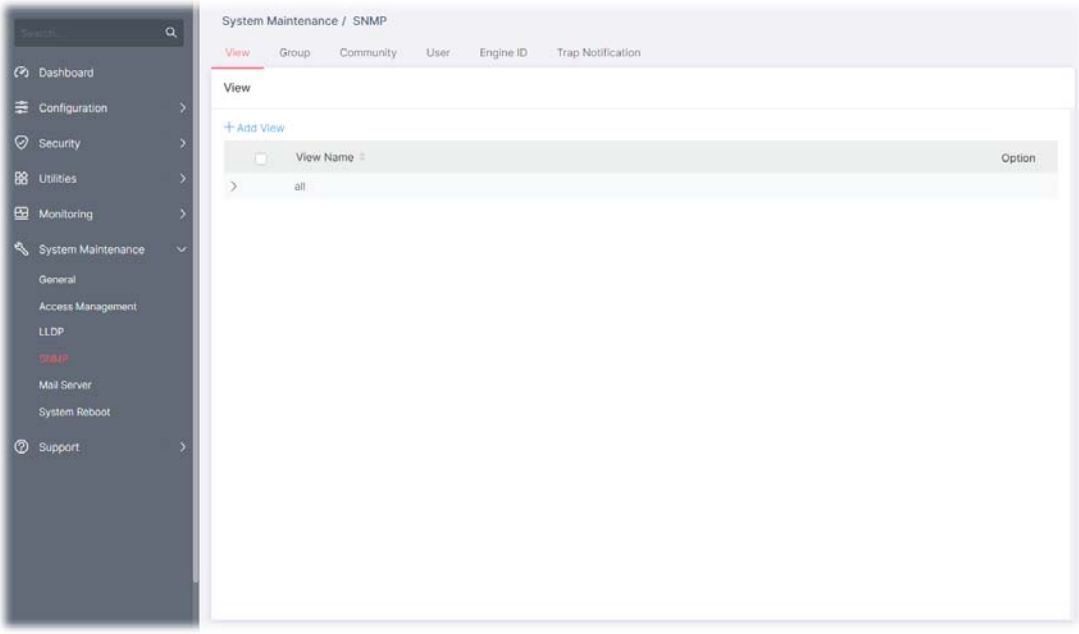
A managed device is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional (read and write) access to node-specific information. Managed devices exchange node-specific information with the NMSs. Sometimes called network elements, the managed devices can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

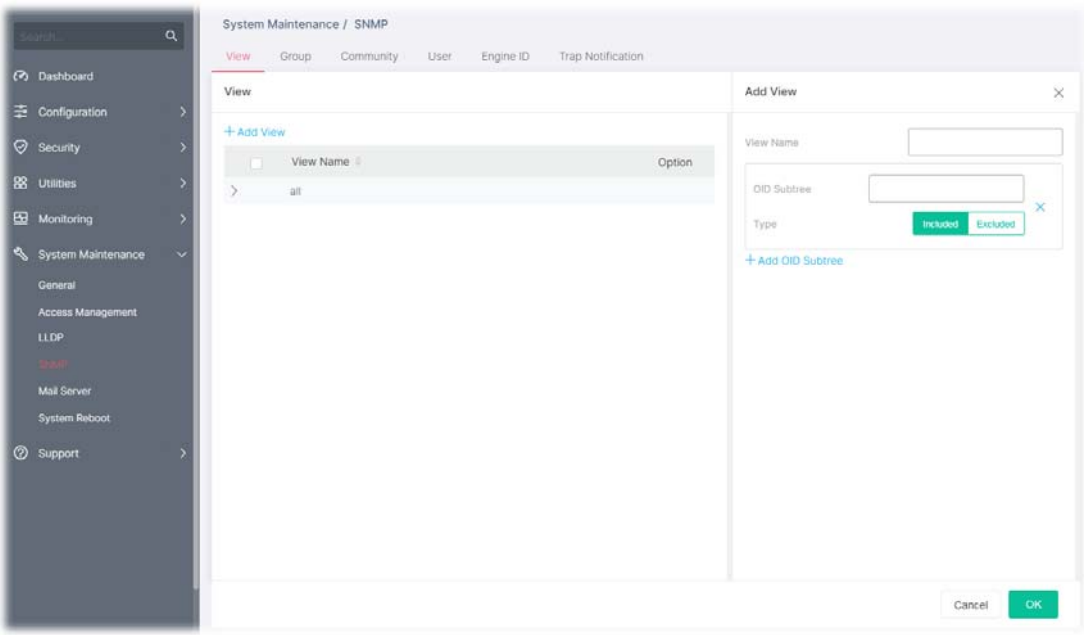
This page allows the network administrator to create MIB views (Management information base) and then include or exclude OID (Object Identifier) in a view.




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:

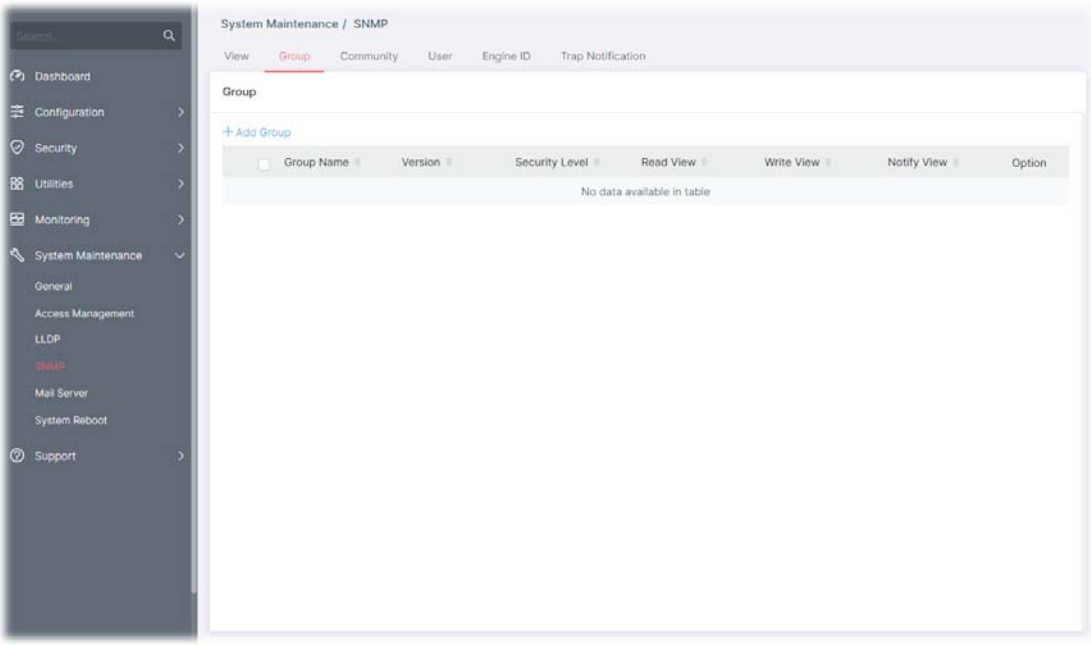
| Item | Description |
|---|---|
| **View Name** | Enter a name of the MIB view. |
| **OID Subtree** | Enter an OID string to be included or excluded (based on the view type setting) from the MIB view. |
| **Type** | Determine to include or exclude the selected MIBs. |

| | |
|---|---|
| | • **Include**<br>• **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

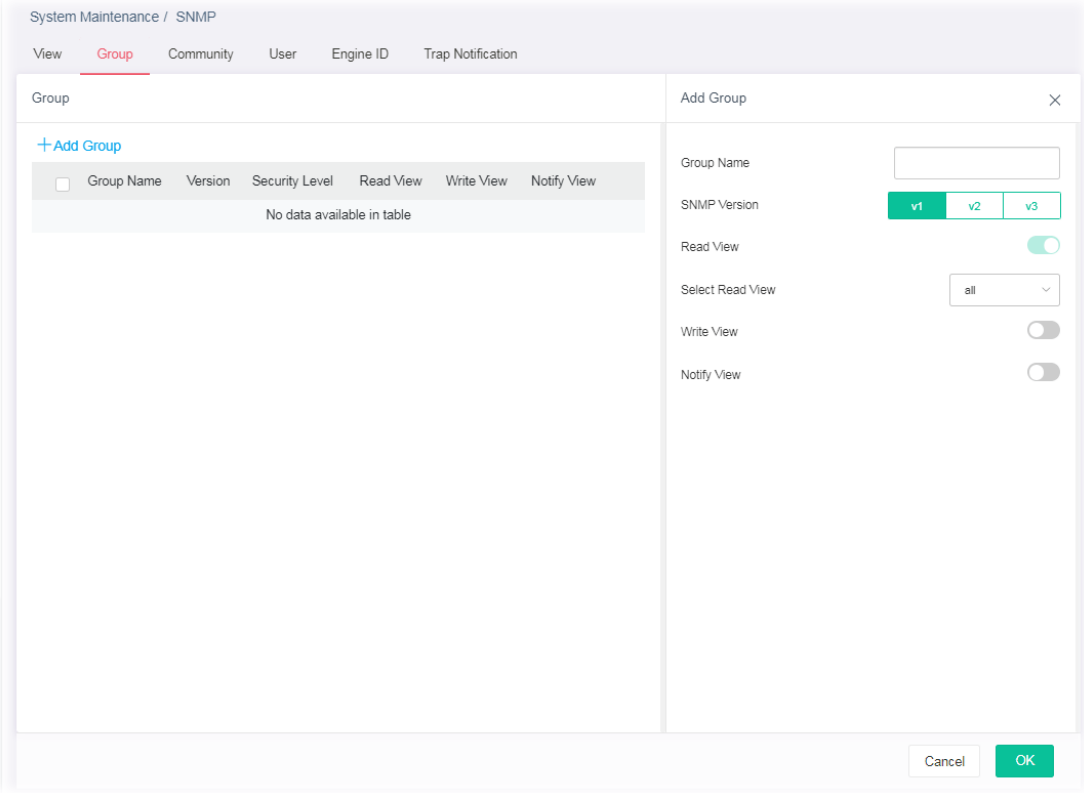
This page allows the network administrator to group SNMP users and assign different authorization and access privileges.




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:

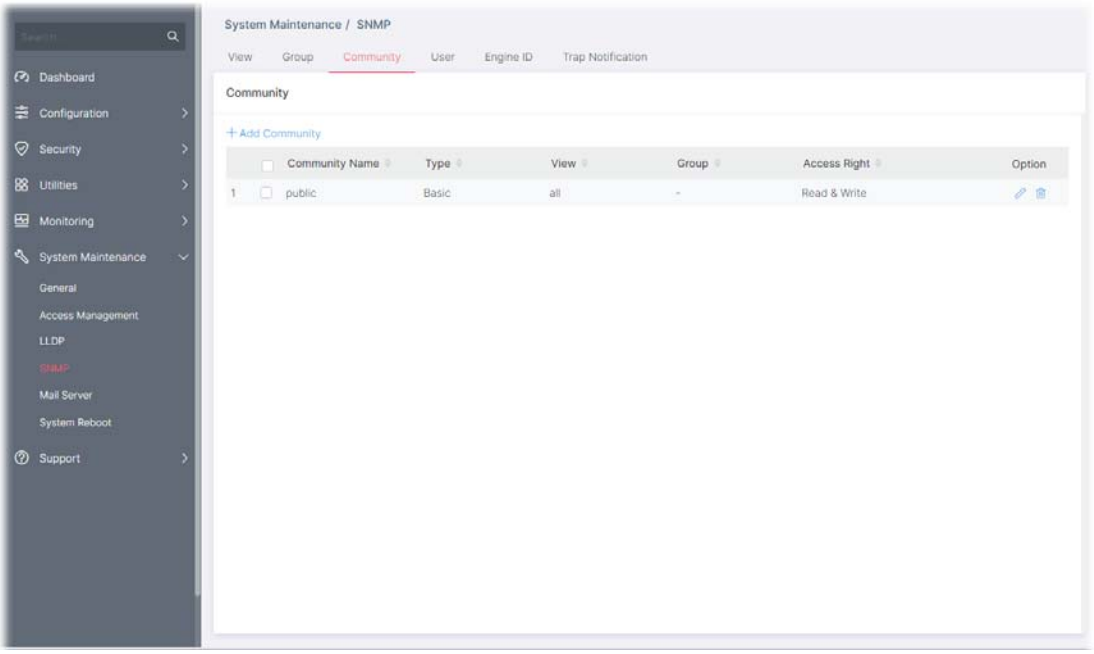
| Item | Description |
|---|---|
| **Add Group** | |
| **Group Name** | Enter a name for the group. |
| **SNMP Version** | Specify SNMP version (v1, v2 or v3). |
| **Security Level** | Specify SNMP security level for the group. It is available when **SNMPv3** is selected.<br>● **No Security** – No authentication.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

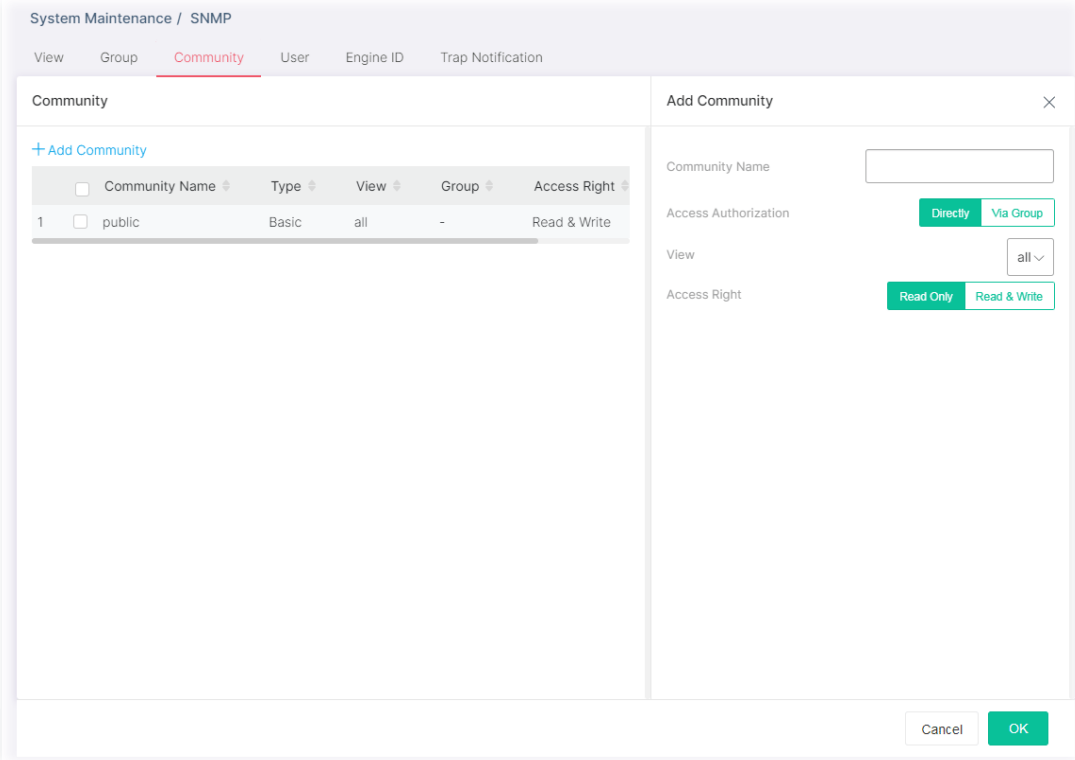



Available settings are explained as follows:

| Item | Description |
|---|---|
| **+Add Community** | Click it to add a new community. |
| **Community Name** | Displays the community name. |
| **Type** | Displays |
| **View** | Displays |
| **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.<br>- 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.



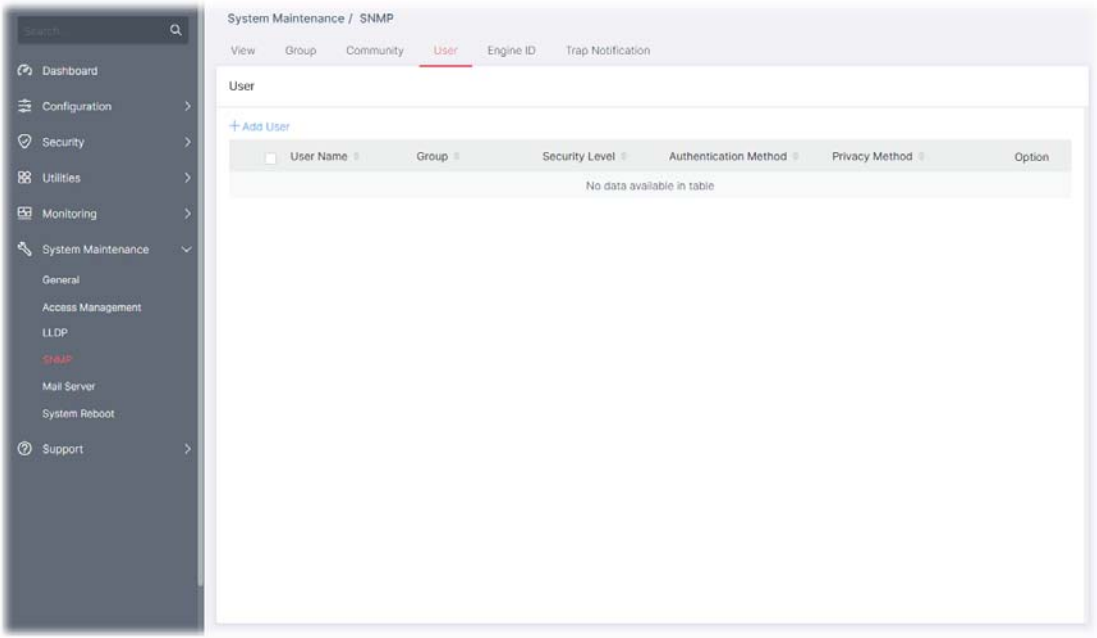

Available settings are explained as follows:

| 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.<br>**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**.**<br>Specify a SNMP group to define the object available to the community. |
| **Access Right** | Define the access right of the community group.<br>**Read Only -** It allows unidirectional access to node-specific information.<br>**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).

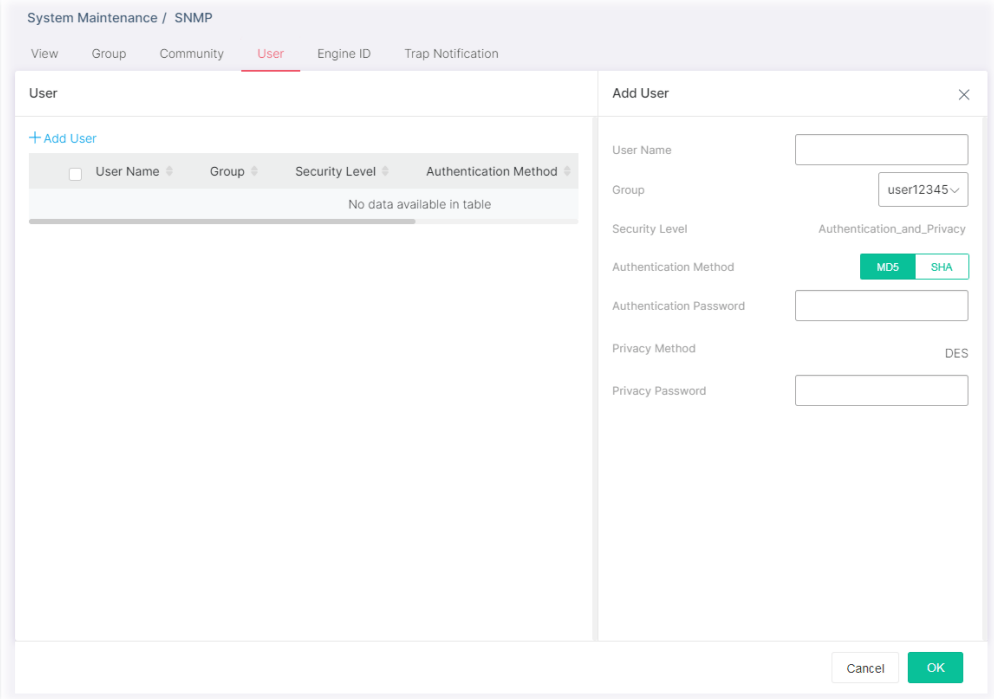



Available settings are explained as follows:

| 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. |

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.



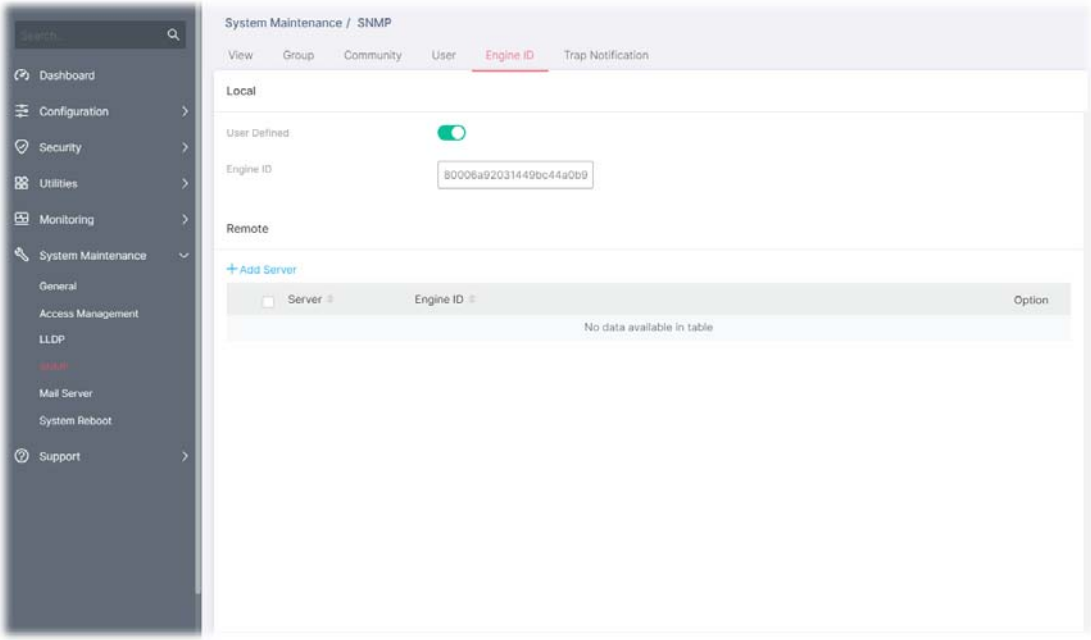

Available settings are explained as follows:

| 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.<br>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".<br>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".<br>Enter a string as the password for authentication. |
| **Privacy Method** | It is available only when the Security Level is set with "Authentication_and_Privacy".<br>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".<br>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.

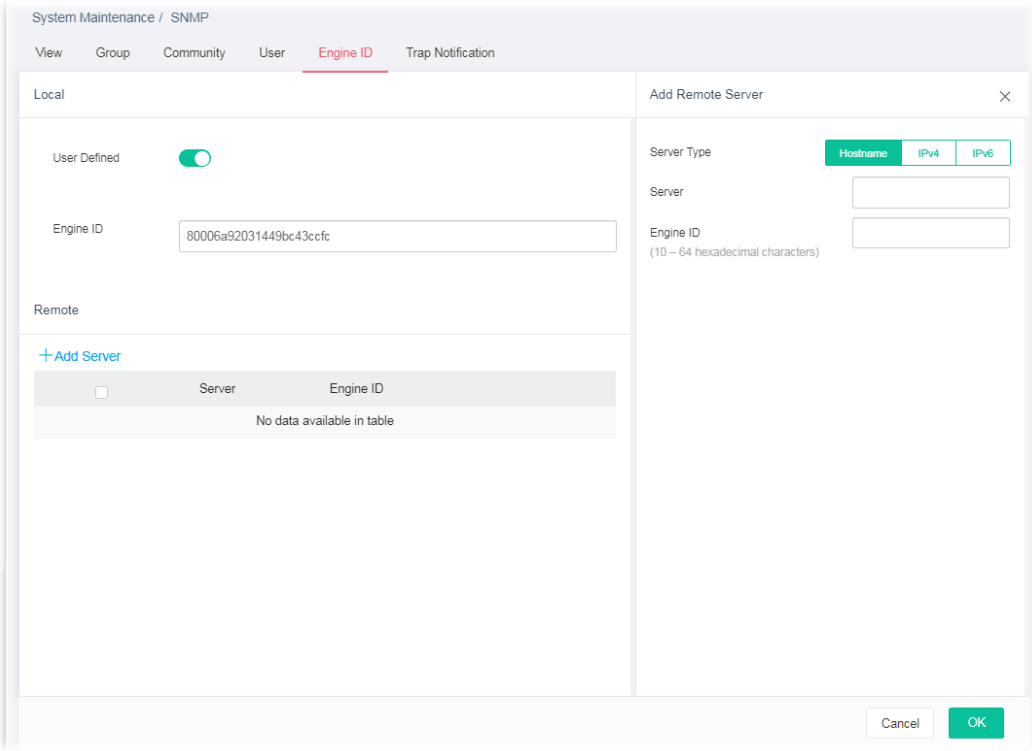



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Local** | |
| **User Defined** | Click the toggle to enable / disable this function.<br>- means “Enable”.<br>- means “Disable”. |
| **Engine ID** | Displays the engine ID of the local server.<br>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.<br>- Clear the selected entry. |

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

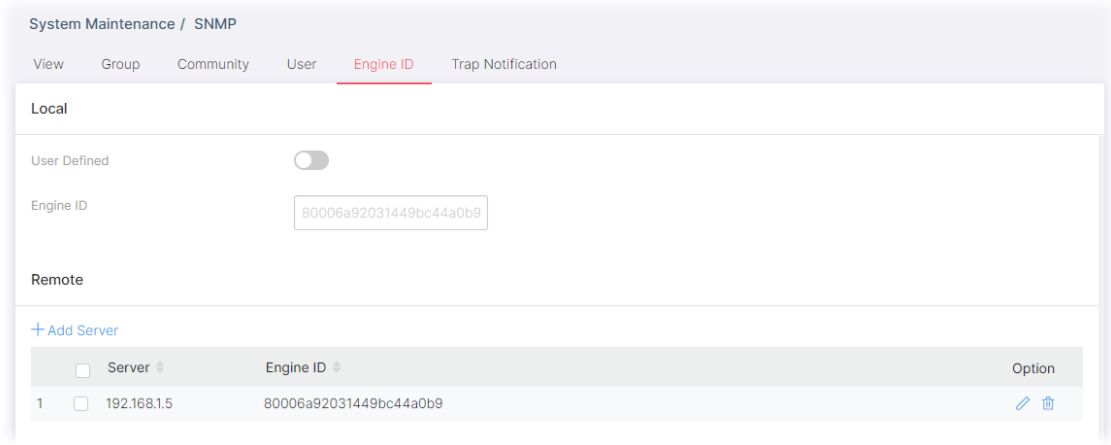
To add a remote server profile, click the "**+ Add Server** " to open the page.




Available settings are explained as follows:

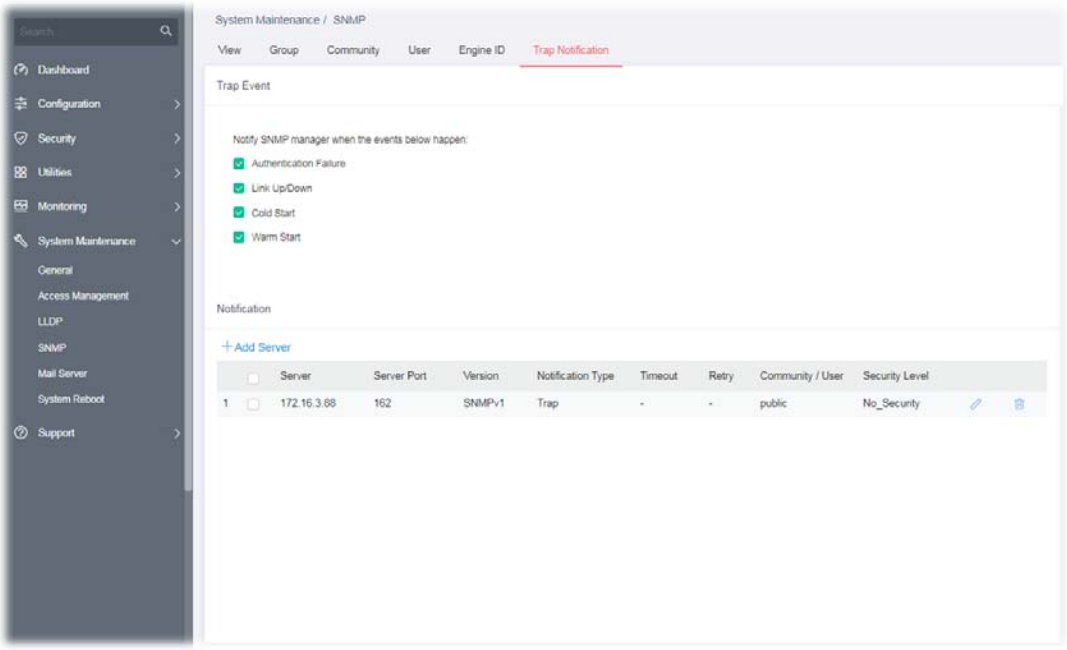
| Item | Description |
|---|---|
| **Add Remote Server** | |
| **Server Type** | Specify the address type for entering hostname or IPv4/IPv6 address.<br>• **Hostname**<br>• **IPv4**<br>• **IPv6** |
| **Server** | Enter the IP address or the hostname of the remote SNMP server. |
| **Engine ID** | Specify the engine ID for remote SNMP server.<br>The engine ID ranges from 10 to 64 hexadecimal characters, and the hexadecimal number must be divided by “2”. |

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



# 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.



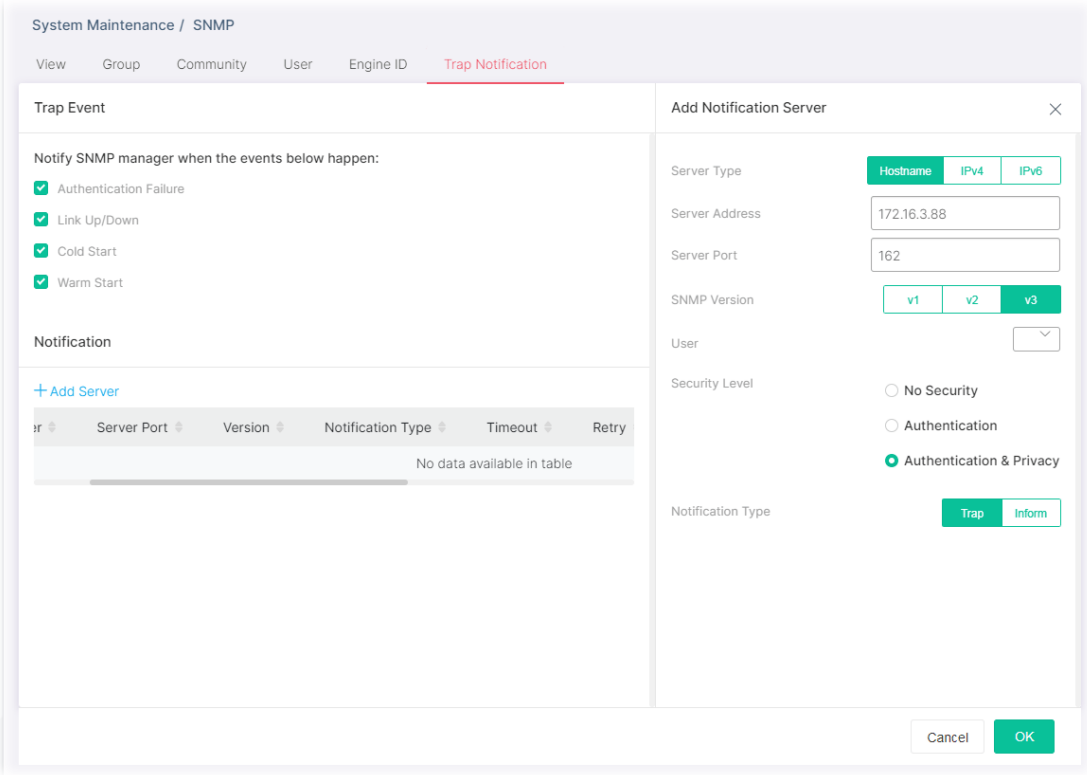

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Trap Event** | |
| **Authentication Failure, Link Up/Down, Cold Start, Warm Start** | Check the box to enable the function.<br>**Authentication Failure** - VigorSwitch will reboot when encountering authentication failure (including community not match or user password not match).<br>**Link Up/Down** - VigorSwitch will reboot while encountering port link up or down trap.<br>**Cold Start** - VigorSwitch will reboot while encountering user trap.<br>**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.<br>- 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:

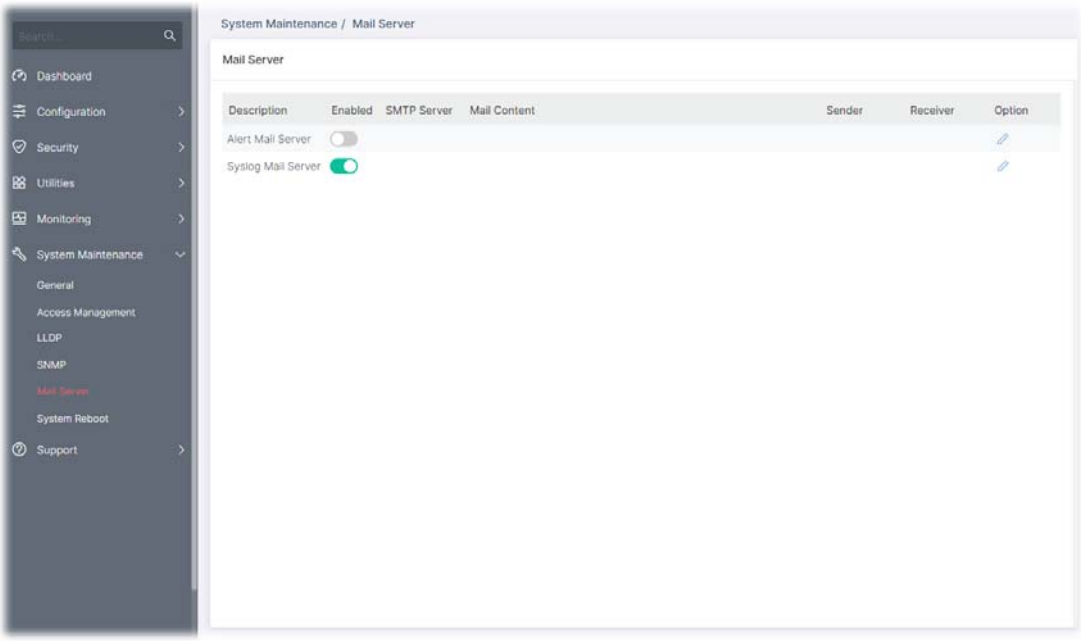
| Item | Description |
|---|---|
| **Add Notification Server** | |
| **Server Type** | Choose IPv4/IPv6/Hostname to specify IP address or the hostname of the SNMP trap recipients.<br>• **Hostname**<br>• **IPv4**<br>• **IPv6** |
| **Server Address** | Specify SNMP notification version (SNMPv1/v2/v3). |
| **Server Port** | Specify a port number for the server. |
| **SNMP Version** | Specify SNMP notification version (SNMPv1/v2/v3). |
| **Community** | Use the drop down list to choose one of the community profiles. |
| **Notification Type** | Displays the notification type.<br>To specify Notification Type, select v2 or v3 as SNMP Version.<br>• **Trap** –Send SNMP traps to the host.<br>• **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.<br>Specify SNMP security level for SNMP notification packet. It is available when SNMPv3 is selected.<br>• **No Security** – No authentication.<br>• **Authentication** – Authentication without encryption will be performed for packets.<br>• **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.

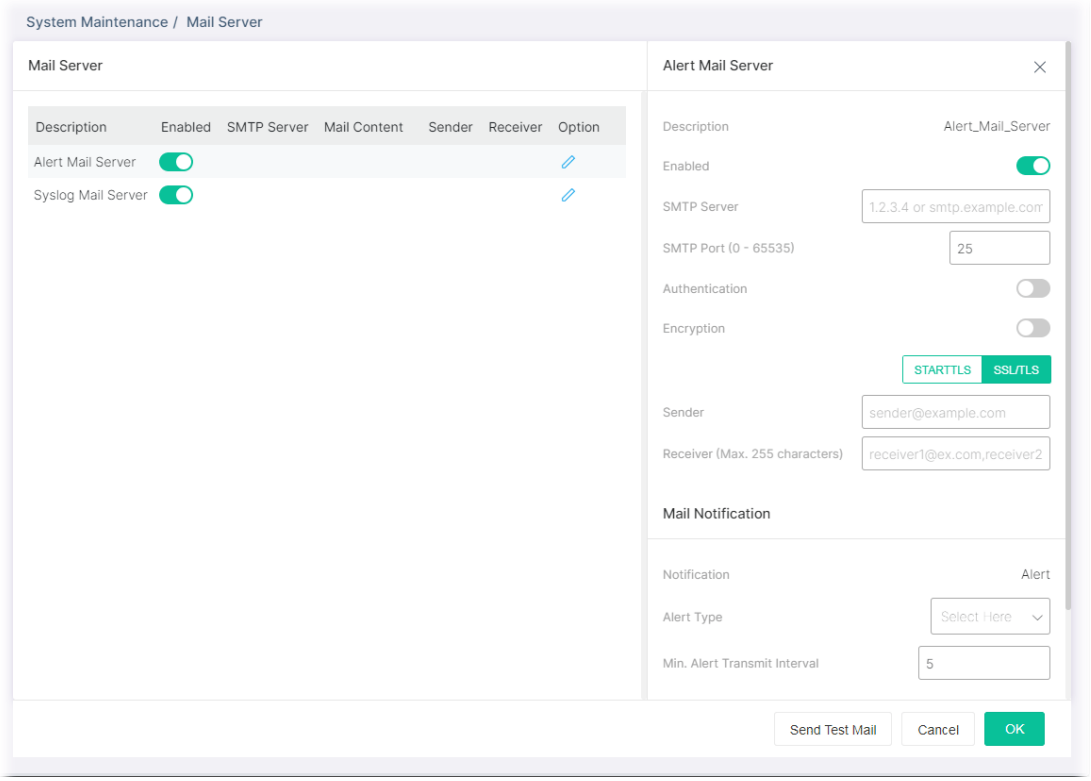



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Mail Server** | |
| **Description** | Displays the name of the mail server. |
| **Status** | Click the toggle to enable / disable this function.<br>- means “Enable”.<br>- 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:

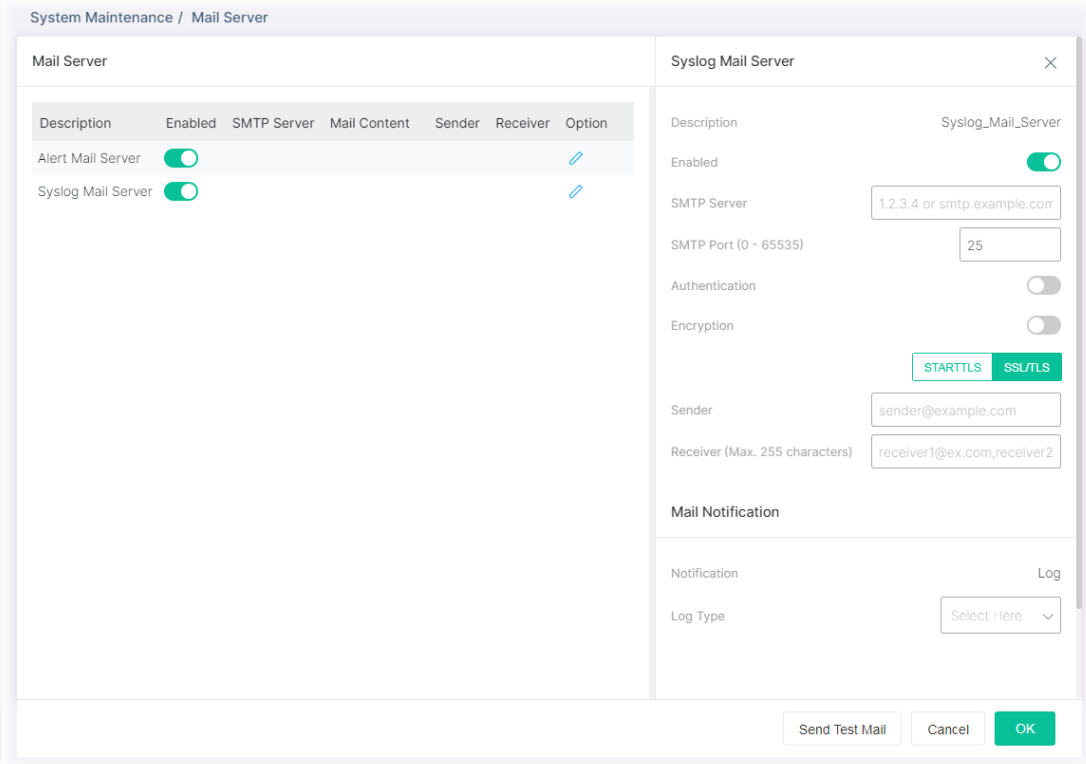
| Item | Description |
|---|---|
| **Alert Mail Server** | |
| **Description** | Displays the name (Alert or Syslog) of the mail server. |
| **Server Status** | Click the toggle to enable / disable the mail server.<br> - means “Enable”.<br> - means “Disable”. |
| **SMTP Server** | Enter IP address or URL of the SMTP server. |
| **SMTP Port** | Enter the port number for the SMTP server. |
| **Authentication** | Click the toggle to enable / disable this function.<br>• **User Name** - Enter a user name for authentication.<br>• **Password** - Enter a password for authentication. |
| **Encryption** | Click the toggle to enable / disable this function.<br>After enabling Authentication, choose one of the encryption servers for data encryption.<br>• **STARTTLS -** The mail will be encrypted with StartTLS.<br>• **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.<br>• Port Link Status<br>• Port Link Speed<br>• System Restarted<br>• PoE Warning Status<br>IP Conflict |
| **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:

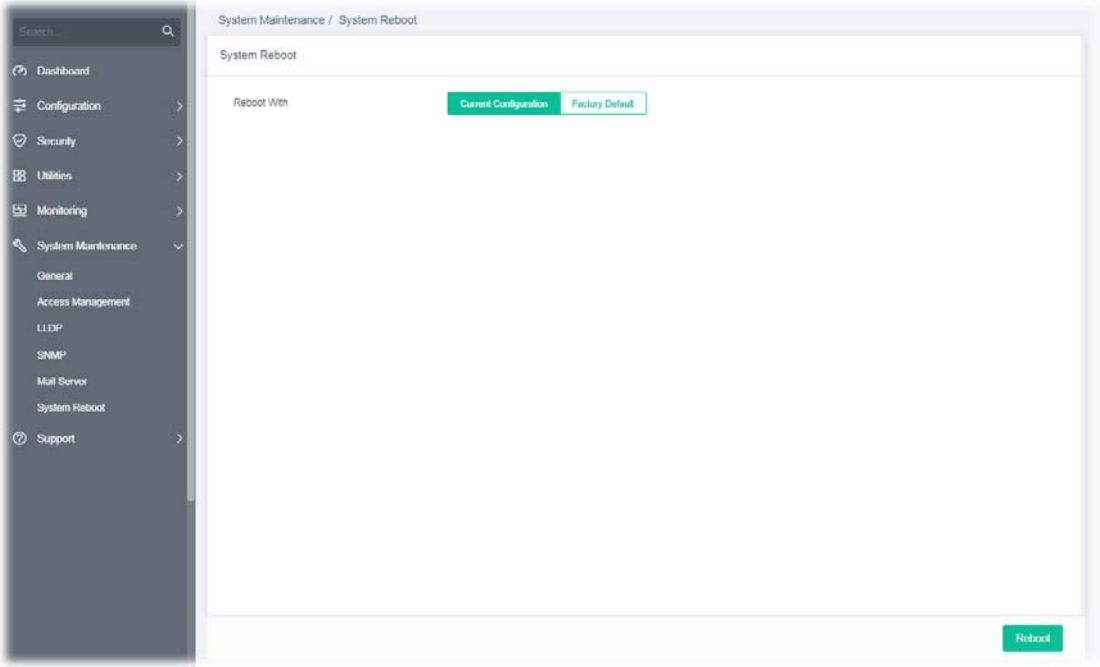
| Item | Description |
|---|---|
| **Alert Mail Server** | |
| **Description** | Displays the name (Alert or Syslog) of the mail server. |
| **Server Status** | Click the toggle to enable / disable this function.<br> - means “Enable”.<br> - means “Disable”. |
| **SMTP Server** | Enter IP address or URL of the SMTP server. |
| **SMTP Port** | Enter the port number for the SMTP server. |

| | |
|---|---|
| **Authentication** | Click the toggle to enable / disable this function.<br>• **User Name** - Enter a user name for authentication.<br>• **Password** - Enter a password for authentication. |
| **Encryption** | Click the toggle to enable / disable this function.<br>After enabling Authentication, choose one of the encryption servers for data encryption.<br>• **STARTTLS -** The mail will be encrypted with StartTLS.<br>• **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.<br>**Factory Default** - Use the default configuration 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:**

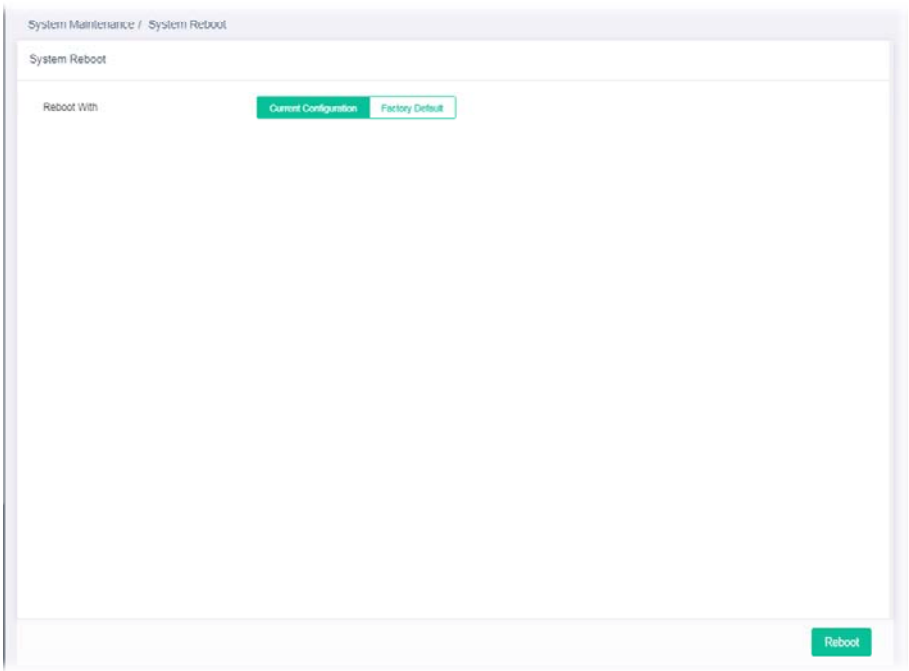
After pressing **factory default setting**, you will loose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of factory default is null.

---

## VII-1-1 Software Reset

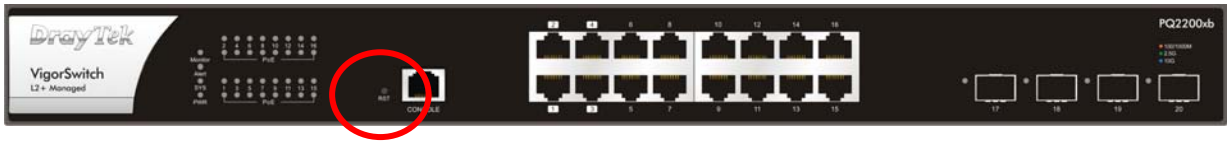
You can reset the modem to factory default via Web page.

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.

# Appendix Telnet Commands

# A-1 Accessing Telnet of Vigor Switch

This chapter also gives you a general description for accessing telnet and describes the firmware versions for the routers explained in this manual.

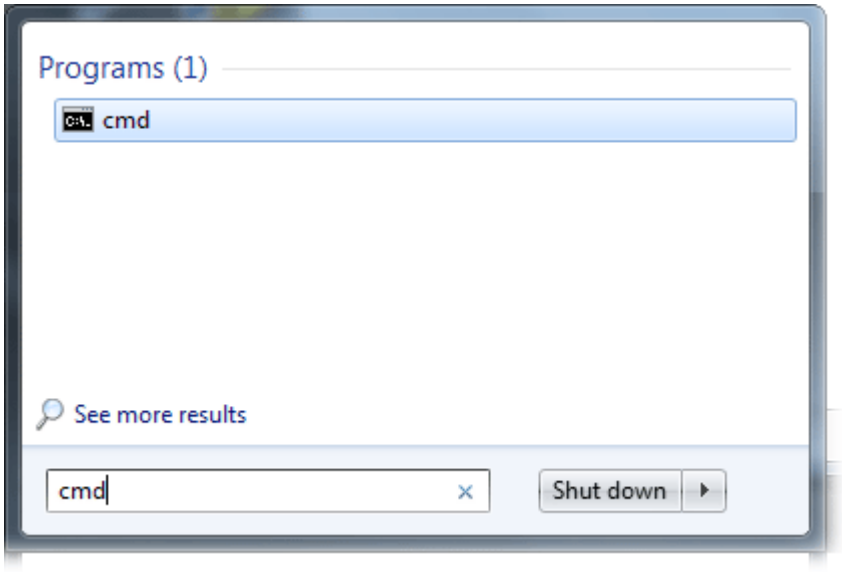
---

**Note:**

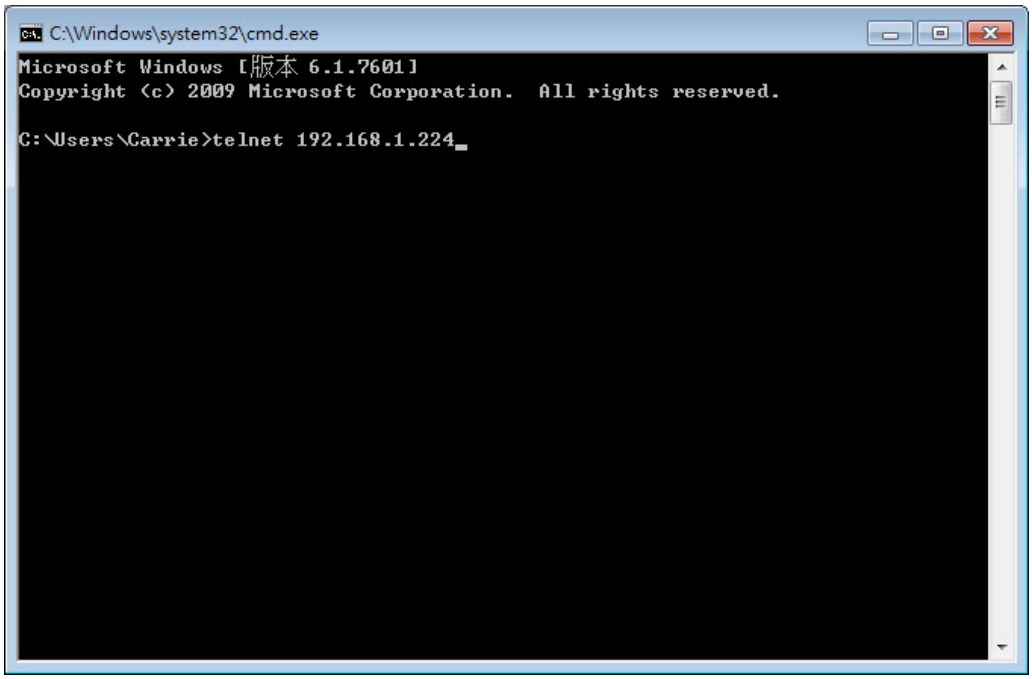
For Windows 7 user, please make sure the Windows Features of Telnet Client has been turned on under Control Panel>>Programs.

---

Type **cmd** and press Enter. The Telnet terminal will be open later.

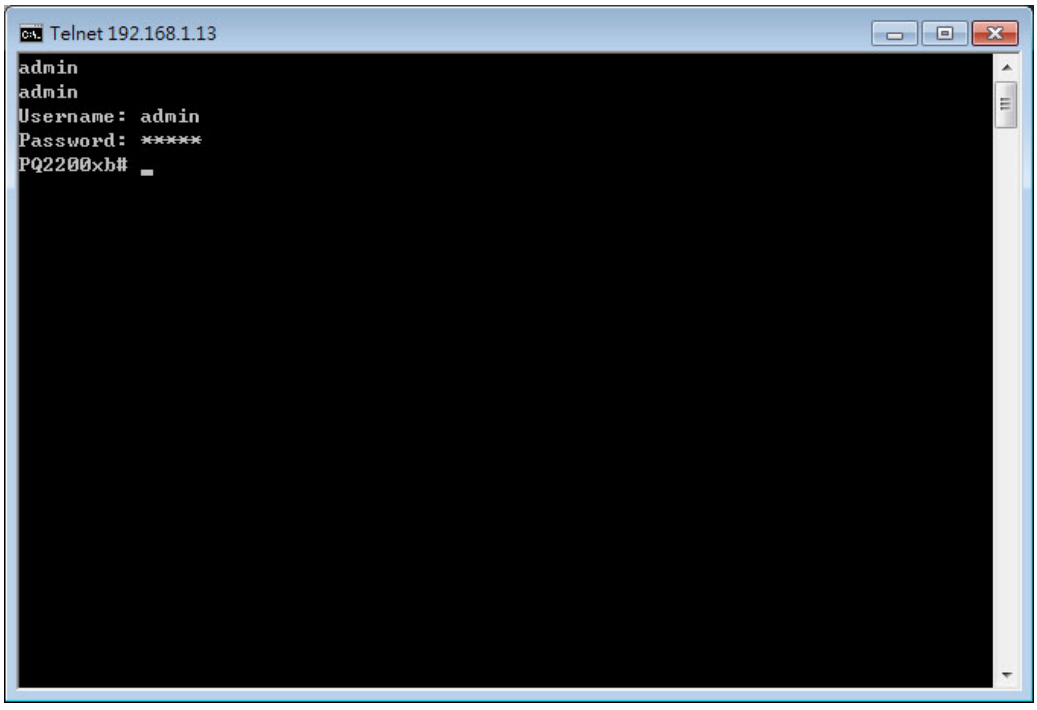



In the following window, type Telnet 192.168.1.224 as below and press Enter. Note that the IP address in the example is the default address of the router. If you have changed the default, enter the current IP address of the router and press Enter.



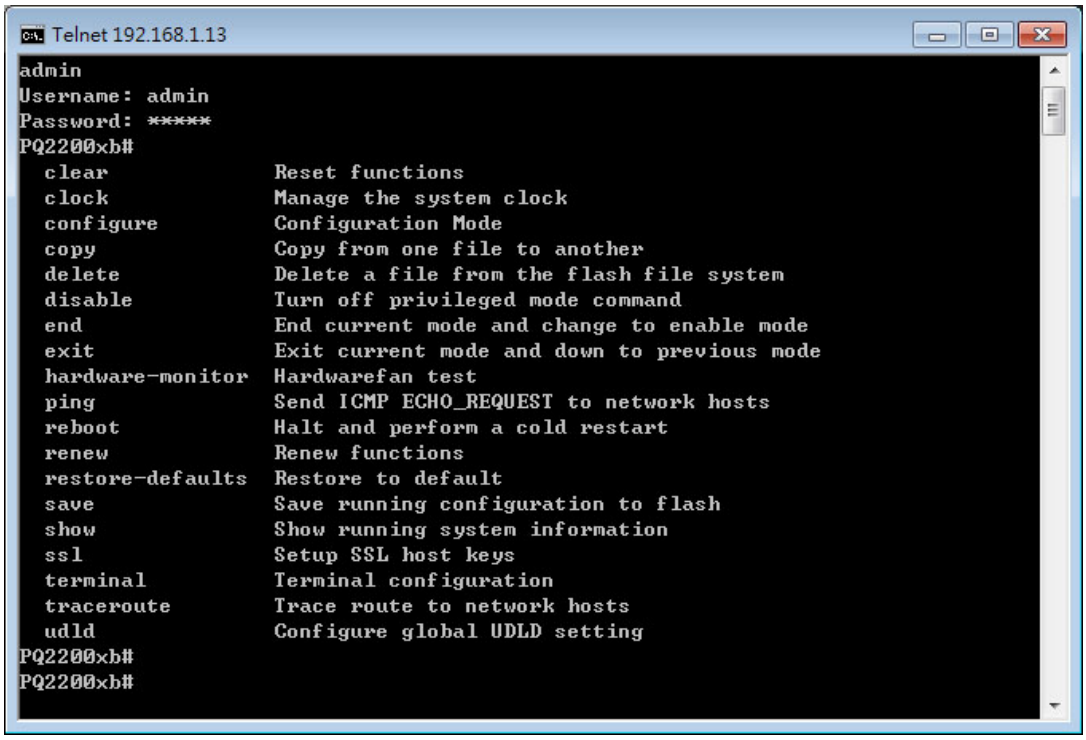

For users using previous Windows system (e.g., XP), simply click Start >> Run and type Telnet 192.168.1.224 in the Open box.

Next, enter admin/admin for Account/Password.



# A-2 Available Commands

Enter ? to get a list of available commands.




The available commands contain – clear, clock, configure, copy, delete, disable, end, exit, hardware-monitor, ping, reboot, renew, restore-defaults, save, show, ssl, terminal, traceroute and udld. Each command will be explained as follows.

**Note**: You can also enter ? to check if there are subcommands under current command.

## A-2-1 Clear Configuration

This command allows resetting the functions of ARP, interface, IP, IPv6, LACP, Line, LLDP, Logging, MAC, and Spanning Tree.

### Telnet Command: clear arp

Use this command to clear entries in the ARP cache.

**Syntax Items**

clear arp

**Description**

| Syntax Items | Description |
|---|---|
| clear arp | <A.B.C.D> - Enter the IP address of the device (e.g., 192.168.1.224).<br>Related Syntax:<br>• # clear arp |

| | |
|---|---|
| | • # clear arp <A.B.C.D> |

**Example**

```
PQ2200xb# clear arp 192.168.1.224
PQ2200xb#
```

## Telnet Command: clear authentication

Use this command to clear authentication sessions based on LAN port, MAC address, or authentication type for 802.1x/MAC authentication.

**Syntax Items**

clear authentication sessions

clear authentication sessions interfaces 10GigabitEthernet

clear authentication sessions interfaces 2.5GigabitEthernet

clear authentication sessions mac

clear authentication sessions session-id

clear authentication sessions type

**Description**

| Syntax Items | Description |
|---|---|
| clear authentication sessions | Clear all of the sessions related to authentication.<br>Related Syntax:<br>• # clear authentication sessions |
| clear authentication sessions interfaces 10GigabitEthernet | Clear the sessions of a specific interface.<br><1-4> - Enter the number of LAN port.<br>Related Syntax:<br>• # clear authentication sessions interfaces 10GigabitEthernet <1-4> |
| clear authentication sessions interfaces 2.5GigabitEthernet | Clear the sessions of a specific interface.<br><1-16> - Enter the number of LAN port.<br>Related Syntax:<br>• # clear authentication sessions interfaces 2.5GigabitEthernet <1-16> |
| clear authentication sessions mac | Clear the sessions with the MAC address set here.<br><A:B:C:D:E:F> - Enter the MAC address of the device that you want to clear the authentication information.<br>Related Syntax:<br>• # clear authentication sessions mac <A:B:C:D:E:F> |
| clear authentication sessions session-id | Clear the sessions with the string set here.<br><WORD> - Enter a string of a session that you want to clear.<br>Related Syntax:<br>• # clear authentication sessions session-id <WORD> |

| | |
|---|---|
| clear authentication sessions type | Clear the sessions with authentication type selected here.<br><dot1x> - Use 802.1x authentication.<br><mac> - Use mac-based authentication.<br><web> - Use web-based authentication.<br>Related Syntax:<br>• # clear authentication sessions type <dot1x><mac><web> |

**Example**

```
PQ2200xb# clear authentication sessions
No Auth Manager sessions currently exist
PQ2200xb# clear authentication sessions mac 48:5B:39:2F:A8:66
PQ2200xb# clear authentication sessions interfaces 10GigabitEthernet 2
PQ2200xb# clear authentication sessions session-id 0000000B002AFBE8
PQ2200xb#
```

## Telnet Command: clear gvrp

Use this command to clear statistics or port error statistics for all interfaces or a specific interface (LAN or LAG).

**Syntax Items**

clear gvrp error-statistics

clear gvrp statistics

**Description**

| Syntax Items | Description |
|---|---|
| clear gvrp error-statistics | Specify a LAN/LAG interface for clearing error statistics for GVRP.<br><1-4> - Enter the number (1 to 4) of LAN port (10G).<br><1-16> - Enter the number (1 to 12) of LAN port (2.5G).<br><1-8> - Enter the number (1 to 8) of LAG interface (IEEE 802.3 Link Aggregation Interface) that you want to clear the GVRP setting.<br>Related Syntax:<br>• # clear gvrp error-statistics interfaces 10GigabitEthernet <1-4><br>• # clear gvrp error-statistics interfaces 2.5GigabitEthernet <1-16><br>• # clear gvrp error-statistics interfaces LAG <1-8> |
| clear gvrp statistics | Specify a LAN/LAG interface for clearing statistics for GVRP.<br><1-4> - Specify an interface (10G) for clearing statistics for GVRP.<br><1-16> - Specify an interface (2.5G) for clearing statistics for GVRP.<br><1-8> - Specify LAG interface for clearing statistics for GVRP.<br>Related Syntax: |

| | |
|---|---|
| | • # clear gvrp statistics interfaces 10GigabitEthernet <1-4><br>• # clear gvrp statistics interfaces 2.5GigabitEthernet <1-16><br>• # clear gvrp statistics interfaces LAG <1- 8> |

**Example**

```
PQ2200xb# clear gvrp error-statistics interfaces 10GigabitEthernet 2
PQ2200xb#
PQ2200xb# clear gvrp error-statistics interfaces LAG 2
PQ2200xb#
```

## Telnet Command: clear interfaces

Use this command to clear statistics counters for all interfaces or a specific interface (10GB LAN, 2.5GB LAN or LAG).

**Syntax Items**

clear interfaces 10GigabitEthernet

clear interfaces 2.5GigabitEthernet

clear interfaces LAG

**Description**

| Syntax Items | Description |
|---|---|
| clear interfaces 10GigabitEthernet | Specify a LAN interface (10G) for clearing statistics counters on that port.<br><1-4> - Enter the number (1 to 4) of LAN port.<br>Related Syntax:<br>• # clear interfaces 10GigabitEthernet <1-4> counters |
| clear interfaces 2.5GigabitEthernet | Specify a LAN interface (2.5G) for clearing statistics counters on that port.<br><1-16> - Enter the number (1 to 16) of LAN port.<br>Related Syntax:<br>• # clear interfaces 2.5GigabitEthernet <1-16> counters |
| clear interfaces LAG | Specify a LAG interface for clearing statistics counters on that port.<br><1-8> - Enter the number (1 to 8) of LAG interface (IEEE 802.3 Link Aggregation Interface).<br>Related Syntax:<br>• # clear interfaces LAG <1-8> counters |

**Example**

```
PQ2200xb# clear interfaces gigabitethernet 3 counters
PQ2200xb# clear interfaces
PQ2200xb# clear interfaces lag 2 counters
PQ2200xb#
```

## Telnet Command: clear ip

Use this command to clear IGMP snooping groups (dynamic or static) information for all interfaces or a specific interface (LAN or LAG) with IP address.

**Syntax Items**

clear ip arp

clear ip dhcp

clear ip igmp

**Description**

| Syntax Items | Description |
|---|---|
| clear ip arp | <1-4> - Enter the number (1 to 4) of LAN port (10GB).<br><1-16> - Enter the number (1 to 16) of LAN port (2.5GB).<br><1-8> - Specify a LAG interface for clearing ARP inspection information.<br>statistics - Clear the statistics for ARP inspection.<br>Related Syntax:<br>• # clear ip arp inspection interfaces 10GigabitEthernet <1-4><br>• #clear ip arp inspection interfaces 2.5GigabitEthernet <1-16><br>• # clear ip arp inspection interfaces LAG <1-8> statistics |
| clear ip dhcp | snooping database statistics - Clear snooping database statistics for DHCP server.<br>snooping interfaces 10GigabitEthernet / LAG- Specify a LAN / LAG interface for clearing DHCP snooping information.<br><1-4> - Enter the number (1 to 4) of LAN port (10GB).<br><1-16> - Enter the number (1 to 16) of LAN port (2.5GB).<br><1-8> - Specify a LAG interface for clearing DHCP snooping information.<br>Related Syntax:<br>• # clear ip dhcp snooping database statistics<br>• # clear ip dhcp snooping interfaces 10GigabitEthernet <1-4> statistics<br>• # clear ip dhcp snooping interfaces 2.5GigabitEthernet <1-16> statistics<br># clear ip dhcp snooping interfaces LAG <1-8> statistics |
| clear ip igmp | snooping groups dynamic - Clear dynamic snooping groups of IGMP server.<br>snooping groups static - Clear static snooping groups of IGMP server.<br>snooping statistics - Clear snooping statistics for IGMP server.<br>Related Syntax:<br>• # clear ip igmp snooping groups dynamic<br>• # clear ip igmp snooping groups static<br>• # clear ip igmp snooping statistics |

**Example**

```
PQ2200xb# clear ip igmp snooping groups dynamic
PQ2200xb#
```

## Telnet Command: clear ipv6

Use this command to clear MLD snooping configuration for dynamic / static group(s) with IPv6 address.

**Syntax Items**

clear ipv6 mld

**Description**

| Syntax Items | Description |
|---|---|
| clear ipv6 mld | snooping groups dynamic - Clear dynamic snooping groups of MLD.<br>snooping groups static - Clear static snooping groups of MLD.<br>Related Syntax:<br>• # clear ipv6 mld snooping groups dynamic<br>• # clear ipv6 mld snooping groups static<br>• # clear ipv6 mld snooping statistics |

**Example**

```
PQ2200xb# clear ipv6
PQ2200xb# clear ipv6 mld snooping groups dynamic
PQ2200xb# clear ipv6 mld snooping groups dynamic?
  <cr>
PQ2200xb# clear ipv6 mld snooping groups static
PQ2200xb#
```

## Telnet Command: clear lacp

Use this command to clear LACP configuration for specified LAG interface or all LAG interfaces.

**Syntax Items**

clear lacp <1-8> counters

clear lacp counters

**Description**

| Syntax Items | Description |
|---|---|
| clear lacp <1-8> | <1-8> - Enter the number (1 to 8) of LAG interface (IEEE 802.3 Link Aggregation Interface).<br>Related Syntax:<br>• # clear lacp <1-8> counters |
| clear lacp counters | Clear LACP configuration for all LAG interfaces.<br>Related Syntax:<br>• # clear lacp counters |

**Example**

```
PQ2200xb# clear lacp 1 counters
No interfaces configured in the channel group
PQ2200xb#
```

## Telnet Command: clear line

Use this command to clear line settings including SSH (Secure Shell) configuration and telnet daemon configuration.

**Syntax Items**

clear line ssh

clear line telnet

**Description**

| Syntax Items | Description |
|---|---|
| clear line ssh | Clear SSH configuration for line connection.<br>Related Syntax:<br>• # clear line ssh |
| clear line telnet | Clear SSH Telnet configuration for line connection.<br>Related Syntax:<br>• # clear line telnet |

**Example**

```
PQ2200xb# clear line ssh
PQ2200xb# clear line telnet
```

## Telnet Command: clear lldp

Use this command to clear LLDP statistics or reset LLDP information.

**Syntax Items**

clear lldp global

clear lldp interfaces

**Description**

| Syntax Items | Description |
|---|---|
| clear lldp global | Clear all of the statistics related to LLDP.<br>Related Syntax:<br>• # clear lldp global statistics |
| clear lldp interfaces | Specify a LAN / LAG interface for clearing LLDP information.<br><1-4> - Enter the number (1 to 4) of LAN port (10GB).<br><1-16> - Enter the number (1 to 16) of LAN port (2.5GB).<br><1-8> - Enter the number (1 to 8) of LAG interface (IEEE 802.3 Link Aggregation Interface).<br>Related Syntax:<br>• # clear lldp interfaces 10GigabitEthernet <1-4> statistics<br>• # clear lldp interfaces 2.5GigabitEthernet <1-16> statistics<br>• # clear lldp interfaces LAG <1-8> statistics |

**Example**

```
PQ2200xb# clear lldp global statistics
PQ2200xb#
PQ2200xb# clear lldp interfaces LAG 1 statistics
PQ2200xb# clear lldp interfaces gigabitethernet 1 statistics
PQ2200xb#
```

## Telnet Command: clear logging

Use this command to clear log messages from the internal logging buffer and flash.

**Syntax Items**

clear logging buffered

clear logging file

**Description**

| Syntax Items | Description |
|---|---|
| clear logging buffered | Clear the log stored in RAM.<br>Related Syntax:<br>• # clear logging buffered |
| clear logging file | Clear the log stored in flash.<br>Related Syntax:<br>• # clear logging file |

**Example**

```
PQ2200xb# clear logging buffered
PQ2200xb# clear logging file
PQ2200xb#
```

## Telnet Command: clear mac

Use this command to clear MAC configuration related to VLAN, LAG, and LAN port.

**Syntax Items**

clear mac

**Description**

| Syntax Items | Description |
|---|---|
| clear mac address-table | <1-4> - Enter the number (1 to 4) of LAN port (10GB).<br><1-16> - Enter the number (1 to 16) of LAN port (2.5GB).<br><1-8>- Enter the number (1 to 8) of LAG interface (IEEE 802.3 Link Aggregation Interface).<br><1-4094> - Specify a VLAN ID by entering its number.<br>Related Syntax:<br>• # clear mac adderss-table dynamic interfaces 10GigabitEthernet <1-4><br>• clear mac adderss-table dynamic interfaces 2.5GigabitEthernet <1-16><br>• # clear mac adderss-table dynamic interfaces LAG <1-8> |

| | |
|---|---|
| | • # clear mac adderss-table dynamic vlan <1-4094> |

**Example**

```
PQ2200xb# clear mac address-table dynamic vlan 2038
PQ2200xb# clear mac address-table dynamic interfaces gigabitethernet 3
PQ2200xb#
```

## Telnet Command: clear mvr

Use this command to clear information for all members (including dynamic, static) of MVR.

**Syntax Items**

clear mvr members

**Description**

| Syntax Items | Description |
|---|---|
| clear mvr members | Clear information for dynamic / static members.<br>Related Syntax:<br>• # clear mvr members dynamic<br>• # clear mvr members static |

**Example**

```
PQ2200xb # clear mvr members dynamic
PQ2200xb # clear mvr members static
PQ2200xb #
```

## Telnet Command: clear spanning-tree

Use this command to clear running system information.

**Syntax Items**

clear spanning-tree

**Description**

| Syntax Items | Description |
|---|---|
| clear spanning-tree interfaces | Specify a LAN interface for clearing its running information.<br><1-4> - Enter the number (1 to 4) of LAN port (10GB).<br><1-16> - Enter the number (1 to 16) of LAN port (2.5GB).<br><1-8>- Enter the number (1 to 8) of LAG interface (IEEE 802.3 Link Aggregation Interface).<br>Related Syntax:<br>• # clear spanning-tree interfaces 10GigabitEthernet <1-4> statistics<br>• # clear spanning-tree interfaces 2.5GigabitEthernet <1-16> statistics<br>• # clear spanning-tree interfaces LAG <1-8> statistics |

**Example**

```
PQ2200xb# clear spanning-tree interfaces 10GigabitEthernet
  <1-4>  10GigabitEthernet device number
PQ2200xb# clear spanning-tree interfaces 10gigabitethernet 3 statistics
PQ2200xb# clear spanning-tree interfaces LAG 1 statistics
PQ2200xb#
```

## A-2-2 Clock Configuration

This command allows managing the system clock.

### Telnet Command: clock set

Use this command to configure the system clock manually.

**Syntax Items**

clock set

**Description**

| Syntax Items | Description |
|---|---|
| clock set | Set current by entering hours, minutes, seconds, month, date and year with the format listed below:<br><HH:MM:SS> - Hour, minute, second (e.g., 08:10:30).<br><Jan> - January.<br><feb> - February<br><mar> - March<br><apr> - April<br><may> - May<br><jun> - June<br><jul> - July<br><aug> - August<br><sep> - September<br><oct> - October<br><nov> - November<br><dec> - December<br><1-31> - Date 1 to 31.<br><2000-2035> - Year of 2000 to 2035.<br>Related Syntax:<br>• # clock set HH:MM:SS jan/feb/mar/apr/may/jun/jul/aug/sep/oct/nov/dec <1-31> <2000-2035> |

**Example**

```
PQ2200xb# clock set 12:10:30 jan 1 2019
2019-01-01 12:10:30 UTC+8
```

## A-2-3 Configure Configuration

This command allows configuring the settings related to VigorSwitch.

Available sub-commands under Configure include:

aaa, acct, authentication, boot, clock, custom, dhcp-server, dos, dot1x, do, dray_surveillence, enable, end, errdisable, exit, gvrp, hostname, http, interface, ip, ipv6, jumbo-frame, lacp, lag, line, lldp, logging, logmail, loop-protection, mac, mailalert, management, management-vlan, mirror, mvr, no, openvpn, poe, port-security, qos, radius, schedule, sflow, snmp, sntp, spanning-tree, start-up, storm-control, surveillance-vlan, system, tacacs, tr069, udld, username, vlan, voice-vlan and webhook

Before configuration, you have to enter “configure” to access into next phase.

To return to previous phase, enter “exit”

Example

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# exit
PQ2200xb#
```

## Telnet Command: aaa

Use this command to add a login authentication list to authenticate with local, tacacs+, radius, and none service.

**Syntax Items**

aaa authentication enable

aaa authentication login

**Description**

| Syntax Items | Description |
|---|---|
| aaa authentication enable | Enable authentication is used only on CLI for a user trying to switch from User EXEC (>) mode to Privileged EXEC (#) mode.<br>enable – Enable the authentication list.<br><LISTNAME> – Enter a string as the list name for authentication type. Default value is “default”.<br><none, enable, tacacs+, radius> – Specify the authentication method by entering none, enable, tacacs+ or radius.<br>• None: Do nothing and just make user be authenticated.<br>• Enable: Use local password to authenticate.<br>• Tacacs+: Use remote Tacas+ server to authenticate.<br>• Radius: Use remote Radius server to authenticate.<br>default - It is used to configure default enable authentication.<br>**Related Syntax:**<br>• <config>#aaa authentication enable <LISTNAME> <none, enable, tacacs+, radius><br>• <config>#aaa authentication enable default <none, enable, tacacs+, radius> |
| aaa authentication login | Login authentication is used when a user tries to login into the switch.<br><none, enable, tacacs+, radius> –Specify the authentication method by entering none, enable, tacacs+ or radius. |

| | |
|---|---|
| | default - It is used to configure default login authentication.<br>**Related Syntax:**<br>● <config>#aaa authentication login <none, enable, tacacs+, radius><br>● <config>#aaa authentication login default <none, enable, tacacs+, radius> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# aaa authentication enable LISTNAME enable
PQ2200xb(config)#
PQ2200xb(config)# exit
PQ2200xb# show aaa authentication enable lists
  Enable List Name      Authentication Method List
------------------ --------------------------------
                default         enable
              LISTNAME              enable
PQ2200xb#
```

## Telnet Command: acct

Use this command to set RADIUS / TACACS server.

**Syntax Items**

acct server radius

acct server tacacs

**Description**

| Syntax Items | Description |
|---|---|
| server radius | <1-65535> - Set a value to wait for a packet retransmission to the authentication server.<br><1-60> - Set the transmission interval (unit is second).<br>● # acct server radius disconnect message port <1-65535> interval <1-60> |
| server tacacs | <1-65535> - Set a value to wait for a packet retransmission to the authentication server.<br><1-60> - Set the transmission interval (unit is second).<br>● # acct server tacacs disconnect message port <1-65535> interval <1-60> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# acct server radius disconnect message port 3030 interval 30
PQ2200xb(config)#
```

## Telnet Command: authentication

Use this command to enable the global setting of 802.1x/MAC/WEB authentication network access control (default is disabled for all).

**Syntax Items**

authentication dot1x

authentication guest-vlan

authentication mac

authentication web

**Description**

| Syntax Items | Description |
|---|---|
| authentication dot1x | Enable 802.1x authentication by entering the word, dot1x after authentication.<br>Related Syntax:<br>● <config># authentication dot1x |
| authentication guest-vlan | Configure the guest VLAN.<br><1-4094> - Specify a guest VLAN ID by entering its number.<br>Related Syntax:<br>● <config># authentication guest-vlan <1-4094> |
| authentication mac | Enable MAC authentication by entering the word, mac after authentication.<br>mac local - Local database for MAC-Based authentication. It can add local MAC authentication hosts in database.<br><A:B:C:D:E:F> - Enter the MAC address to be added for authentication.<br>control auth – Set a local entry control mode, auth (the host will be set to authorized) or unauth (the host will be set to unauthorized).<br>vlan <1~4094> - Specify a VLAN ID by entering its number<br>reauth-period <300~4294967294> - Set a time to initiate automatic re-authentication.<br>inactive-timeout <60~65535>- Set the inactive timeout for MAC authentication host. After the time interval, if there is no activity from the client, then it will be unauthorized by Vigor system.<br>control unauth - Set a local entry control mode as “unauth” to let the host set as unauthorized.<br>radius mac-case <lower / upper> - Set RADIUS user ID with lower case or upper case.<br>radius mac-delimiter <colon/dot/hyphen/none> - Select RADIUS user ID delimiter. In which,<br>colon: XX:XX:XX:XX:XX:XX<br>dot: XX.XX.XX.XX.XX.XX<br>hyphen: XX-XX-XX-XX-XX-XX<br>none: XXXXXXXXXXXX<br>gap <2/4/6> - Select delimiter gap.<br>Related Syntax:<br>● <config>#authentication mac |

| | |
|---|---|
| | • <config>#authentication mac local <A:B:C:D:E:F> control auth inactive-timeout <60~65535><br>• <config>#authentication mac local <A:B:C:D:E:F> control auth reauth-period <300~4294967294><br>• <config>#authentication mac local <A:B:C:D:E:F> control auth vlan <1~4094><br>• <config>#authentication mac local <A:B:C:D:E:F> control auth vlan<1~4094> reauth-period <300~4294967294><br>• <config>#authentication mac local <A:B:C:D:E:F> control auth vlan<1~4094> reauth-period <300~4294967294> inactive-timeout <60~65535><br>• <config>#authentication mac local <A:B:C:D:E:F> control unauth<br>• <config>#authentication mac radius mac-case <lower / upper><br>• <config>#authentication mac radius mac-delimiter <colon/dot/hyphen/none><br>• <config>#authentication mac radius mac-delimiter <colon/dot/hyphen/none> gap <2/4/6> |
| authentication web | Web - Enable web authentication by entering the word “web” after “authentication”.<br>username <WORD> - Specify a username.<br>password <string> - Set a password.<br>vlan <1~4094> - Specify a VLAN ID by entering its number.<br>reauth-period <30~4294967294> - Set a time to initiate automatic re-authentication.<br>inactive-timeout <60~65535>- Set the inactive timeout for MAC authentication host. After the time interval, if there is no activity from the client, then it will be unauthorized by Vigor system.<br>Related Syntax:<br>• <config>#authentication web<br>• <config>#authentication web local username <WORD> password <string> inactive-timeout <60~65535><br>• <config>#authentication web local username <WORD> password <string> reauth-period <300~4294967294><br>• <config>#authentication web local username <WORD> password <string> reauth-period <300~4294967294> inactive-timeout <60~65535><br>• <config>#authentication web local username <WORD> password <string> vlan<1~4094><br>• <config>#authentication web local username <WORD> password <string> inactive-timeout <60~65535><br>• <config>#authentication web local username <WORD> password <string> reauth-period <30~4294967294> inactive-timeout <60~65535><br>• <config>#authentication web local username <WORD> password <string> vlan<1~4094> reauth-period <30~4294967294> inactive-timeout <60~65535> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)# authentication dot1x
PQ2200xb(config)# vlan 3
PQ2200xb(config-vlan)# exit
PQ2200xb(config)# authentication guest-vlan 3
PQ2200xb(config)#
PQ2200xb(config)# exit
PQ2200xb # show authentication
Autentication dot1x state          : enabled
Autentication mac state            : disabled
Autentication web state            : disabled
Guest VLAN                              : enabled (3)
Mac-auth Radius User ID Format   : XXXXXXXXXXX
Mac-auth Local Entry               :
Web-auth Local Entry               :
Interface Configurations
Interface GigabitEthernet1
   Admin Control             : disable
   Host Mode                 : multi-auth
   Type dot1x State          : disabled
   Type mac State            : disabled
   Type web State            : disabled
   Type Order                : dot1x
   MAC/WEB Method Order      : radius
   Guest VLAN                : disabled
   Reauthentication          : disabled
   Max Hosts                 : 256
   VLAN Assign Mode          : static
--More—
.....
PQ2200xb# configure
PQ2200xb(config)# authentication mac local 00:11:22:33:00:01 control auth vlan 3
reauth-period 500 inactive-timeout 300
PQ2200xb(config)#
PQ2200xb(config)# authentication mac local 00:11:22:33:00:01 control unauth
PQ2200xb(config)#
PQ2200xb(config)# authentication web local username user_1 password 1234tw vlan 3
reauth-period 600 inactive-timeout 700
PQ2200xb(config)#
```

## Telnet Command: boot

Use this command to have a backup image in the flash partition. Select the active firmware image, and another firmware image will become a backup one.

**Syntax Items**

boot system

**Description**

| Syntax Items | Description |
|---|---|
| boot system | Boot the system from flash image partition 0 / 1.<br>Related Syntax:<br>● <config># boot system image0<br>● <config># boot system image1 |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# boot system image0
Select "image0" Success
PQ2200xb(config)# exit
PQ2200xb#
PQ2200xb # show boot
Image   Version      Date                    Status       File Name
-----   ----------   ---------------------   -----------  ----------
0        1.0.2       2017-08-29 09:44:57     Not active*  2120_r442_220RC1.all
1        2.3.2       2018-05-16 09:14:31     Active       p2280_r734_230RC4.all

"*" designates that the image was selected for the next boot

PQ2200xb#
```

## Telnet Command: clock

Use this command to configure time zone, summer-time and external time source for the system clock.

**Syntax Items**

clock auto timezone

clock source local

clock source sntp

clock summer-time

clock timezone

**Description**

| Syntax Items | Description |
|---|---|
| clock auto timezone | VigorSwitch sets the time zone automatically. |
| clock source local | Configure an external time source for the system clock.<br>“local” means to use static time. It is the default setting.<br>Related Syntax:<br>● <config># clock source local |
| clock source sntp | Configure an external time source for the system clock. “sntp” means to use SNTP time. |

| | |
|---|---|
| | Related Syntax:<br>• <config># clock source sntp |
| clock summer-time | Configure the system to automatically switch to summer time (daylight saving time).<br>ACRONYM – Specify the acronym name of time zone. The acronym of the time zone will be displayed when summer time is in effect. If unspecified, the time zone acronym will be used in default. (1-4 chars)<br><jan/feb/mar/apr/may/jun/jul/aug/sep/oct/nov/dec> - Indicate January, February, March, April, May, June, July, August, September, October, November, December.<br><1-31> means date 1 to 31.<br><2000-2037> - means year of 2000 to 2035.<br><HH:MM> - means hours and minutes.<br>recurring - Summer time should start and end on the corresponding specified days every year.<br><1-1440>- Set the number of minutes to add during the summer time. The default number is 60.<br>eu - The summer time is based on the European Union rules. (Start point – last Sunday in March, End point – last Sunday in October)<br>usa - The summer time is based on the United States rules. (Start point – second Sunday in March, End point – first Sunday in November)<br>first - The first week of the month.<br>last - The last week of the month.<br><sun/mon/tue/wed/thu/fri/sat> - Indicate Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday.<br><jan/feb/mar/apr/may/jun/jul/aug/sep/oct/nov/dec> - Indicate January, February, March, April, May, June, July, August, September, October, November, December.<br><first/last>- Specify the first week or the last week of the month.<br><1-5> - Specify the number of the week in the month.<br>Note that the first group of month, date, hour and minute is used for configuring starting time, and the second group is used for configuring ending time.<br>Related Syntax:<br>• <config># clock summer-time ACRONYM date <jan/feb/mar/apr/may/jun/jul/aug/sep/oct/nov/dec> <1-31> <2000-2037> <HH:MM> <jan/feb/mar/apr/may/jun/jul/aug/sep/oct/nov/dec><1-31><2000-2037> <HH:MM><br>• <config># clock summer-time ACRONYM recurring eu <1-1440><br>• <config># clock summer-time ACRONYM recurring usa <1-1440><br>• <config># clock summer-time ACRONYM recurring first <sun/mon/tue/wed/thu/fri/sat>< jan / feb / mar / apr / may / jun/jul/aug/sep/oct/nov/dec> <HH:MM> <first/last> <sun/mon/tue/wed/thu/fri/sat>< jan /feb /mar /apr/may/ jun/jul/aug/sep/oct/nov/dec> <HH:MM> <1-14400><br>• <config># clock summer-time ACRONYM recurring last <sun/mon/tue/wed/thu/fri/sat>< jan /feb /mar /apr /may /jun/jul/aug/sep/oct/nov/dec> <HH:MM> <first/last><sun/mon/tue/wed/thu/fri/sat>< jan /feb /mar /apr/may/ |

| | |
|---|---|
| | jun/jul/aug/sep/oct/nov/dec> <HH:MM> <1-14400><br>• <config># clock summer-time ACRONYM recurring <1-5> <sun/mon/tue/wed/thu/fri/sat>< jan /feb /mar /apr /may /jun/jul/aug/sep/oct/nov/dec> <HH:MM> <1-5> <sun/mon/tue/wed/thu/fri/sat>< jan /feb /mar /apr /may/jun/jul/aug/sep/oct/nov/dec> <HH:MM> <1-14400> |
| clock timezone ACRONYM <-12-13> minutes <0-59> | Set the time zone for display purposes.<br>ACRONYM – Specify the acronym name of time zone. The acronym of the time zone will be displayed when summer time is in effect. If unspecified, the time zone acronym will be used in default. (1-4 chars)<br><-12-13> – Specify the hour offset (from -12 to +13) of time zone.<br>minutes <0-59> – Specify the minute difference from UTC.<br>Related Syntax:<br>• <config># clock timezone ACRONYM <-12-13> minutes <0-59> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)# clock source sntp
PQ2200xb(config)# exit
PQ2200xb# show clock detail
2019-01-05 06:51:23 UTC+8
Time source is sntp
Time zone:
Acronym is
Offset is UTC+8
PQ2200xb# configure
PQ2200xb(config)# clock summer-time tw date jan 30 2019 23:30 feb 1 2019 20:50
PQ2200xb(config)# exit
PQ2200xb# show clock detail
2019-01-05 07:13:49 UTC+8
Time source is sntp
Time zone:
Acronym is ACRONYM
Offset is UTC-10:08
Summertime:
Acronym is tw
Starting and ending on a specific date.
Begins at 1 30 19 23:30
Ends at 2 1 19 20:50
Offset is 60 minutes.
PQ2200xb# configure
PQ2200xb(config)# clock summer-time ACRONYM recurring eu 1200
PQ2200xb(config)# clock summer-time ACRONYM recurring first mon jan 10:10 first sun feb 10:10 1000
PQ2200xb(config)# exit
PQ2200xb# show clock detail
```

```
2019-01-05 11:37:18 UTC+8
Time source is sntp
Time zone:
Acronym is
Offset is UTC+8
Summertime:
Acronym is ACRONYM
Recurring every year.
Begins at 1 1 1 10:10
Ends at 1 0 2 10:10
Offset is 1000 minutes.
```

## Telnet Command: custom

Use this command to enable the module settings.

**Syntax Items**

custom enable

**Description**

| Syntax Items | Description |
| --- | --- |
| custom enable | Enable the module settings.<br>Related Syntax:<br>• <config># custom enable |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)# custom enable
PQ2200xb(config)#
```

## Telnet Command: dos

Use this command to enable specific Denial of Service (DoS) protection.

**Syntax Items**

dos daeqsa-deny
dos icmp-frag-pkts-deny
dos icmp-ping-max-length
dos icmpv4-ping-max-check
dos icmpv6-ping-max-check
dos ipv6-min-frag-size-check
dos ipv6-min-frag-size-length
dos land-deny
dos nullscan-deny
dos pod-deny
dos smurf-deny
dos smurf-netmask
dos syn-sportl1024-deny

dos synfin-deny

dos synrst-deny

dos tcp-frag-off-min-check

dos tcpblat-deny

dos tcphdr-min-check

dos tcphdr-min-length

dos udpblat-deny

dos xma-deny

**Description**

| Syntax Items | Description |
|---|---|
| dos daeqsa-deny | Drop the packets if the destination MAC address equals to the source MAC address.<br>Related Syntax:<br>• <config># dos daeqsa-deny |
| dos icmp-frag-pkts-deny | Drop the fragmented ICMP packets.<br>Related Syntax:<br>• <config># dos icmp-frag-pkts-deny |
| dos icmp-ping-max-length | Set the maximum packet size for ICMPv4/ICMPv6 ping operation.<br><0-65535> - Specify a packet number.<br>Related Syntax:<br>• <config># dos icmp-ping-max-length <0-65535> |
| dos icmpv4-ping-max-check | Check ICMPv4 ping maximum packets size and drop the packets larger than the maximum packet size defined by the command, dos icmp-ping-max-length.<br>Related Syntax:<br>• <config># dos icmpv4-ping-max-check |
| dos icmpv6-ping-max-check | Check ICMPv6 ping maximum packets size and drop the packets larger than the maximum packet size defined by the command, icmp-ping-max-length.<br>Related Syntax:<br>• <config># dos icmpv6-ping-max-check |
| dos ipv6-min-frag-size-check | Check minimum size of IPv6 fragments.<br>Related Syntax:<br>• <config># dos ipv6-min-frag-size-check |
| dos ipv6-min-frag-size-length <0-65535> | Set the minimum packet size of IPv6 fragmented packets.<br><0-65535> - Specify a packet number.<br>Related Syntax:<br>• <config># dos ipv6-min-frag-size-length <0-65535> |
| dos land-deny | Drop the packets if the source IP address equals to destination IP address.<br>Related Syntax:<br>• <config># dos land-deny |
| dos nullscan-deny | Drop the packets if attacked by NULL Scan. |

| | |
|---|---|
| | Related Syntax:<br>• <config># dos nullscan-deny |
| dos pod-deny | Drop the packets if attacked by Ping of Death.<br>Related Syntax:<br>• <config># dos pod-deny |
| dos smurf-deny | Drop the packets if encountered Smurf attack.<br>Related Syntax:<br>• <config># dos smurf-deny |
| dos smurf-netmask | Set the smurf attack size.<br><0-32> - Enter a number as smurf attacks size.<br>Related Syntax:<br>• <config># dos smurf-netmask <0-32> |
| dos syn-sportl1024-deny | Drop SYN packets with sport less than 1024.<br>Related Syntax:<br>• <config># dos syn-sportl1024-deny |
| dos synfin-deny | Drop the packets with SYN and FIN bits set.<br>Related Syntax:<br>• <config># dos synfin-deny |
| dos synrst-deny | Drop the packets with SYNC and RST bits set.<br>Related Syntax:<br>• <config># dos synrst-deny |
| dos tcp-frag-off-min-check | Drop the TCP fragmented packet with offset equals to the minimum packet size.<br>Related Syntax:<br>• <config># dos tcp-frag-off-min-check |
| dos tcpblat-deny | Drop the packets if the source TCP port equals to destination TCP port.<br>Related Syntax:<br>• <config># dos tcpblat-deny |
| dos tcphdr-min-check | Check the minimum TCP header and drop the TCP packets with the header smaller than the minimum size defined.<br>Related Syntax:<br>• <config># dos tcphdr-min-check |
| dos tcphdr-min-length | Set the minimum size of TCP header.<br><0-65535> - Specify a packet number.<br>Related Syntax:<br>• <config># dos tcphdr-min-length <0-65535> |
| dos udpblat-deny | Drop the packets if the source UDP port equals to destination UDP port.<br>Related Syntax:<br>• <config># dos udpblat-deny |
| dos xma-deny | Drop the packets if the sequence number is zero and the FIN, URG and PSH bits are set already. |

| | |
|---|---|
| | Related Syntax:<br>• <config># dos xma-deny |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# dos icmp-ping-max-length 25252
PQ2200xb(config)# dos icmpv4-ping-max-check
PQ2200xb(config)#
```

## Telnet Command: dot1x

Use this command to set 802.1x configuration.

**Syntax Items**

dot1x

**Description**

| Syntax Items | Description |
|---|---|
| dot1x guest-vlan | <0-4094> - Enter a number as guest VLAN ID.<br>Related Syntax:<br>• <config># dot1x guest-vlan <0-4094> |

**Example**

```
PQ2200xb # configure
PQ2200xb(config)#
PQ2200xb(config)# dot1x guest-vlan 33
VLAN does not exist
PQ2200xb(config)#
```

## Telnet Command: do

Use this command to execute a command immediately.

**Syntax Items**

do SEQUENCE

**Description**

| Syntax Items | Description |
|---|---|
| SEQUENCE | Enter the command that you want to execute immediately.<br>Related Syntax: (for example)<br>• <config># do show info |

**Example**

```
PQ2200xb(config)# do show info
System Name          : PQ2200xb
System Location      : Default
System Contact       : Default
MAC Address          : 14:49:BC:43:CC:FC
IP Address           : 192.168.1.11
Subnet Mask          : 255.255.255.0
Loader Version       : 2.1.0
Loader Date          : Jun 30 2021 - 13:11:14
Firmware Version     : 2.7.0
Firmware Date        : Oct 15 2021 - 09:50:07
Firmware Revision    : 95993d5
System Object ID     : 1.3.6.1.4.1.7367
System Up Time       : 0 days, 23 hours, 6 mins, 44 secs
PoE SW Version       : 2
PQ2200xb(config)#
```

## Telnet Command: dray_surveillence

Use this command to enable / disable the ONVIF.

**Syntax Items**

dray_surveillence add

dray_surveillence direct-add

dray_surveillence set

**Description**

| Syntax Items | Description |
|---|---|
| dray_surveillence add | Add an IP device for surveillance.<br>WORD <36-36> - Enter the UUID string of the IP camera or IP-based device.<br>Related Syntax:<br>● <config># dray_surveillence add device uuid WORD <36-36><br>● <config># dray_surveillence add group uuid WORD <36-36> |
| dray_surveillence direct-add | WORD <36-36> - Enter the UUID string of the IP camera or IP-based device.<br>Related Syntax:<br>● <config># dray_surveillence direct-add device uuid WORD <36-36> |
| dray_surveillence set | username WORD<1-32> - Enter a string as the default user name.<br>password WORD<1-32>> - Enter a string as the default password.<br>encptpwd WORD <1-128> - Enter a string as the encrypted key.<br>WORD <36-36> - Enter the UUID string of the IP camera or the IP-based device.<br>ip <A.B.C.D> - Enter the IP address of the IP camera or the |

| | |
|---|---|
| | IP-based device.<br>Mask <A.B.C.D> - Enter the subnet mask of the IP camera or the IP-based device.<br>vlan <1-4094> - Enter a value representing the VLAN ID.<br>Related Syntax:<br>● <config># dray_surveillence set default username WORD<1-32> password WORD<1-32><br>● <config># dray_surveillence set default username WORD<1-32>encptpwd WORD <1-128><br>● <config># dray_surveillence set device uuid WORD <36-36><br>● <config># dray_surveillence set group uuid WORD <36-36><br>● <config># dray_surveillence set interface ip <A.B.C.D><br>● <config># dray_surveillence set interface mask <A.B.C.D><br>● <config># dray_surveillence set vlan <1-4094> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# dray_surveillence
PQ2200xb(config)#
PQ2200xb(config)# dray_surveillence add device uuid 53d7762a-c52b-4bb9-8000-305501e0f35f
PQ2200xb(config)#
```

## Telnet Command: enable

Use this command to configure local password with encrypted string or not.

**Syntax Items**

enable password

enable privilege

enable secret

**Description**

| Syntax Items | Description |
|---|---|
| enable password | Edit the password for each privilege level for activating authentication.<br><1-15> - Enter a number for specifying a privilege level. Default value is 15.<br>Related Syntax:<br>● <config># enable password <1-15> |
| enable privilege | Edit the privilege level of the password for local user.<br><1-15> - Enter a number for specifying a privilege level. Default value is 15.<br><string> - Enter a new string as the password.<br>Related Syntax:<br>● <config># enable privilege <1-15> password <string> (This password will NOT be encrypted.)<br>● <config># enable privilege <1-15> secret <string> |

| | |
|---|---|
| | (This password will BE encrypted.)<br>• <config># enable privilege <1-15> secret encrypted <string><br>(This password is copied from another configuration file. So, enter an existed and encrypted password.) |
| enable secret | <PASSWORD> - Enter a new string as the encrypted password.<br>Related Syntax:<br>• <config># enable secret PASSWORD<br>• <config># enable secret encrypted PASSWORD |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)# enable secret encrypted testtest
PQ2200xb(config)# exit
PQ2200xb# show running-config
PQ2200xb# ...
enable privilege 2 secret "OTE5ZTY4MmNhYzgyNWQ0MzBhNTgwZTg0MmZmMGJiYzQ="
enable secret "testtest"
vlan 2
  name "test0002"
vlan 3
  name "test0003"
vlan 5
  name "test_carrie"
voice-vlan oui-table 00:E0:BB "3COM"
voice-vlan oui-table 00:03:6B "Cisco"
voice-vlan oui-table 00:E0:75 "Veritel"
.......
```

## Telnet Command: end

Use this command to end current mode.

**Syntax Items**

end

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#end
PQ2200xb#
```

## Telnet Command: errdisable

Use this command to enable the auto recovery timer for port error.

**Syntax Items**

errdisable recovery cause

errdisable recovery interval

**Description**

| Syntax Items | Description |
| --- | --- |
| errdisable recovery cause | Enable the auto recovery timer for port error disabled from ACL,all, ARP rate limit, STP BPDU guard, broadcast flooding, DHCP rate limit, port security, STP self-loop, unicast flooding, or unknown multicast flooding causes.<br>Related Syntax:<br>● <config># erridisable recovery cause < acl /all /arp-inspection /bpduguard /broadcast-flood /dhcp-rate-limit /psecure-violation /selfloop /unicast-flood /unknown-multicast-flood > |
| errdisable recovery interval | Set the recovery time of the error disabled port.<br><30-86400> - The default value is 300 seconds.<br>Related Syntax:<br>● <config># errdisable recovery interval <30-86400> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# errdisable recovery interval 600
PQ2200xb(config)#
```

## Telnet Command: exit

Use this command to exit current mode and return to previous mode/phase.

**Syntax Items**

exit

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# exit
PQ2200xb#
```

## Telnet Command: gvrp

Use this command to enable the GVRP configuration. In default, the GVRP is disabled.

**Syntax Items**

gvrp

**Example**

```
PQ2200xb# configure
PQ2200xb(config)# gvrp
PQ2200xb(config)#
PQ2200xb(config)# exit
PQ2200xb# show gvrp
                    GVRP       Status
                    ----------------------
```

```
    GVRP                    : Enabled
    Join time               : 200 ms
    Leave time              : 600 ms
    LeaveAll time           : 10000 ms
PQ2200xb #
```

## Telnet Command: hostname

Use this command to modify the network name of VigorSwitch.

**Syntax Items**

hostname WORD

**Description**

| Syntax Items | Description |
|---|---|
| Hostname WORD | <WORD> - Enter a string as the network name for VigorSwitch.<br>Related Syntax:<br><config># hostname WORD |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)# hostname Switch_3F
Switch_3F(config)#
```

## Telnet Command: interface

Use this command to configure interface settings.

Before configuring, you have to access into next phase. See the following example:

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# interface 10GigabitEthernet 3
PQ2200xb(config-if)#
```

Or

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# interface range LAG 3
PQ2200xb(config-if-range)#
```

**Syntax Items**

interface 10GigabitEthernet

interface 2.5GigabitEthernet

interface VLAN

interface LAG

interface range

**Description**

| Syntax Items | Description |
|---|---|

| | |
|---|---|
| interface 10GigabitEthernet | <1-4> - Specify the number of Ethernet LAN port.<br>Related Syntax:<br>● <config># interface 10GigabitEthernet <1-4> |
| interface 2.5GigabitEthernet | <1-16> - Specify the number of Ethernet LAN port.<br>Related Syntax:<br>● <config># interface 2.5GigabitEthernet <1-16> |
| Interface vlan | <1-4094> - Specify the number of VLAN ID.<br>Related Syntax:<br>● <config># interface vlan <1-4094> |
| interface LAG | <1-8> - Specify the number of LAG interface.<br>Related Syntax:<br>● <config># interface LAG <1-8> |
| Interface range | Specify an interface ranges for configuring detailed settings.<br>Related Syntax:<br>● <config># interface range 10GigabitEthernet <1-4><br>● <config># interface range 2.5GigabitEthernet <1-16><br>● <config># interface range LAG <1-8> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)# interface LAG 1
PQ2200xb(config-if)#
```

Under (config-if)#, available sub-commands for LAN, VLAN or LAG will be different. Below shows the items under Ethernet LAN:

<config-if>#10g-media
<config-if># authentication
<config-if># back-pressure
<config-if># cctv
<config-if># custom
<config-if># description
<config-if># device-check
<config-if># dos
<config-if># dot1x
<config-if># do
<config-if># dray_surveillence
<config-if># duplex
<config-if># eee
<config-if># end
<config-if># exit
<config-if># flowcontrol
<config-if># gvrp
<config-if># ip
<config-if># ipv6
<config-if># lacp

<config-if># lag
<config-if># lldp
<config-if># loop-protection
<config-if># mac
<config-if># mvr
<config-if># no
<config-if># poe
<config-if># port-security
<config-if># power
<config-if># protected
<config-if># qos
<config-if># rate-limit
<config-if># shutdown
<config-if># spanning-tree
<config-if># speed
<config-if># storm-control
<config-if># surveillance-vlan
<config-if># switchport
<config-if># udld
<config-if># vlan
<config-if># voice-vlan

**Description**

| Syntax Items | Description |
|---|---|
| 10g-media | It is used for configuring 10G media type**.**<br>dac100cm - Set the media type as 100cm DAC.<br>dac300cm - Set the media type as 300cm DAC.<br>dac500cm - Set the media type as 500cm DAC.<br>dac50cm - Set the media type as 50cm DAC.<br>fiber10g - Set the media type as 10G Fiber.<br>fiber1g - Set the media type as 1G Fiber.<br>none - Set the media type to NONE media.<br>Related Syntax:<br>• <config-if># 10g-media dac100cm<br>• <config-if># 10g-media dac300cm<br>• <config-if># 10g-media dac500cm<br>• <config-if># 10g-media dac50cm<br>• <config-if># 10g-media fiber10g<br>• <config-if># 10g-media fiber1g<br>• <config-if># 10g-media none |
| authentication | Apply Auth Manager Port Configuration Commands to the specified interface (Ethernet port/LAG port).<br>dot1x – Execute the 802.1x authentication.<br>guest-vlan – Authenticate the guest VLAN configuration.<br>host-mode <multi-auth / multi-host / single-host> - Set the host |

| | |
|---|---|
| | mode for authentication on this port.<br>max-hosts <1-256> - Set the maximum number of authenticated hoss allowed on this port.<br>method <local/radius> - Set authentication method by using local or RADIUS server.<br>order <dot1x / mac /web> - Add an authentication type to the order list.<br>port-control <auto / force-auth / force-unauth> - Set the port state of this port as AUTO, Authorized or Unauthorized.<br>radius-attributes vlan reject – If the Radius server authorizes the supplicant, but does not provide a supplicant VLAN, the supplicant will be rejected. If the parameter is omitted, the option is applied by default.<br>radius-attributes vlan static - If the Radius server authorizes the supplicant but does not provide asupplicant VLAN, the supplicant will be accepted.<br>reauth – Enable/Disabel Reauthentication for this port<br>timer <inactive> <60-65535> – Set the time value for authentication. After the time interval, if there is no activity from the client, it will be unauthorized.<br>timer quiet <0-65535> - Set the time value to wait failed authentication exchange.<br>timer reauth <300-4294967294> - Set the time value. After the time interval, an automatic re-authentication should be initiated.<br>web – Execute the web-based authentication.<br>web max-login-attempts <3-10> – Set a maximum number of login attemps on the port.<br>web max-login-attempts infinite – No limit for login attempts.<br>Related Syntax:<br>● <config-if># authentication dot1x<br>● <config-if># authentication guest-vlan<br>● <config-if># authentication host-mode <multi-auth / multi-host / single-host><br>● <config-if># authentication mac<br>● <config-if># authentication max-hosts <1-256><br>● <config-if># authentication method <local/radius><br>● <config-if># authentication order <dot1x / mac /web><br>● <config-if># authentication port-control <auto / force-auth / force-unauth><br>● <config-if># authentication radius-attributes vlan reject<br>● <config-if># authentication radius-attributes vlan static<br>● <config-if># authentication reauth<br>● <config-if># authentication timer inactive <60-65535><br>● <config-if># authentication timer quiet <0-65535><br>● <config-if># authentication timer reauth <300-4294967294><br>● <config-if># authentication web<br>● <config-if># authentication web max-login-attempts <3-10> |

| | |
|---|---|
| | • <config-if># authentication web max-login-attempts infinite |
| back-pressure | Enable back-pressure for the specified interface (Ethernet port/LAG port).<br>Related Syntax:<br>• <config-if># back-pressure |
| custom | <enable> - Enable the custom module configuration for the specified interface (Ethernet port/LAG port).<br>Related Syntax:<br>• <config-if># custom enable |
| description | Write a description for the specified interface (Ethernet port/LAG port).<br><WORD> - Enter a description (up to 32 characters).<br>Related Syntax:<br>• <config-if># description <WORD> |
| device-check | Perform a device check the specified interface (Ethernet port/LAG port).<br>ip-address<A.B.C.D> - Enter the IP address of the device.<br>interval <120/15/30/60>– Check the device interval by entering the time value. Unit is second.<br>retry <1/3/5> - Enter the retry time during a checking period.<br>failure-action <nothing/powercycle/poweroff> – Set the power cycle.<br>alert <disable/enable> - Enable or disable the alert function.<br><STRING> - Enter multiple IP addresses separated by ",".<br>Related Syntax:<br>• <config-if># device-check ip-address <A.D.C.D> interval <120/15/30/60> retry <1/3/5> failure-action <nothing/powercycle/poweroff><br>• <config-if># device-check ip-address <A.D.C.D> interval <120/15/30/60> retry <1/3/5> failure-action <nothing/powercycle/poweroff> alert <disable/enable><br>• <config-if># device-check multi ip-address <STRING> interval <120/15/30/60> retry <1/3/5> failure-action <nothing/powercycle/poweroff> alert <disable/enable> |
| dos | Apply DoS to the specified interface (Ethernet port/LAG port). |
| dot1x | It is available for GigabitEthernet port only.<br>guest-vlan – Set guest VLAN configuration.<br>max-req <1-10>– Set the maximum request retries. Default is 2.<br>Port-control <auto/force-auth/force-unauth>– Set the port control value (auto, authorized or unauthorized)<br>reauth – Enable/disable the reauthenctication for this port.<br>timeout <quiet-period / reauth-period / server-timeout /supp-timeout /tx-period>– Set timeout value for this port.<br><0-65535> - Set a value as quiet period (default is 60-second).<br><300-4294967294> - Set a value as re-authentication period. (default is 3600-second). |

| | |
|---|---|
| | <1-65535> - Set a value to wait for a packet retransmission to the authentication server.<br>supp-timeout <1-65535> – Set a vale as supplicant timeout period.<br>tx-period <1-65535> - Set a value to wait for a response to an EAP-request / identity before resending the request.<br>Related Syntax:<br>● <config-if># dot1x guest-vlan<br>● <config-if># dot1x max-req <1-10><br>● <config-if># dot1x port-control <auto /force-auth /force-unauth ><br>● <config-if># dot1x reauth<br>● <config-if># dot1x timeout quiet-period <0-65535><br>● <config-if># dot1x timeout reauth-period <300-4294967294><br>● <config-if># dot1x timeout server-timeout <1-65535><br>● <config-if># dot1x timeout supp-timeout <1-65535><br>● <config-if># dot1x timeout tx-period <1-65535> |
| do | Run execution commands in current mode. |
| dray_surveillence | Use this command to set the ONVIF throughput alert threshold.<br><16-1000000> - Specify a number as the alert threshold for egress /ingress throughput.<br>Related Syntax:<br>● <config-if>#dray_surveillence set threshold alert egress <16-1000000><br>● <config-if>#dray_surveillence set threshold alert ingress <16-1000000> |
| duplex | Apply the duplex configuration to the specified interface (Ethernet port/LAG port).<br><Auto> – Auto duplex configuration.<br><Full>– Force full duplex operation.<br><Half> – Force half-duplex operation.<br>Related Syntax:<br>● <config-if># duplex <auto/full/half> |
| eee | Apply the EEE configuration to the specified interface (Ethernet port). |
| end | End current mode, change to enable mode and return to previous phase. |
| exit | Exit from current mode. |
| flowcontrol | Configure flow-control mode to the specified interface (Ethernet port/LAG port).<br><Auto> – Enable AUTO flow-control configuration.<br><Off> – Disable the force flow-control.<br><On> – Enable the force flow-control.<br>Related Syntax: |

| | |
|---|---|
| | • <config-if># flowcontrol <auto/off/on> |
| gvrp | Apply the GVRP configuration to the specified interface (Ethernet port/LAG port).<br>registration-mode <fixed / forbidden / normal>- Set registration mode for GVRP. When registration-mode is fixed or forbidden, it will remove the dynamic port from VLAN.<br>vlan-creation-forbid – Do not remove dynamic port from VLAN.<br>Related Syntax:<br>• <config-if># gvrp registration-mode <fixed / forbidden / normal><br>• <config-if># gvrp vlan-creation-forbid |
| ip | Apply IP configuration to the specified interface (Ethernet port/LAG port).<br>acl <NAME> - Specify an ACL for packets. Enter the name of the ACL.<br>bind-ip <A.B.C.D> - Enter an IP address for binding with the port type.<br>conflict prevention bind-ip <A.B.C.D> - Enter the IP address for the binding.<br>conflict prevention port-type DHCP-Client – Set DHCP Client as the port type.<br>conflict prevention port-type DHCP-Server –Set DHCP Server as the port type.<br>conflict prevention port-type Multiple-Hosts – Set Multiple-Hosts as the port type.<br>conflict prevention port-type Multiple-Hosts has-server – Use this string if there is a DHCP server in this port.<br>conflict prevention port-type Static-Binding –Set Static-Binding as the port type.<br>igmp filter <1-128> - Use it to bind a profile for a port. Specify a profile ID.<br>igmp max-groups <0-256> - Use it to limit port learning max group number (0-256).<br>igmp max-groups action <deny/replace> - Use it to set the action (deny or replace) when the number of groups reach the limitation.<br>source binding max-entry <1-50> - Set the maximum dynamic binding entry number.<br>source binding max-entry no-limit - No limit to binding entry.<br>source verify mac-and-ip – Use it to enable IP source guard function.<br>Related Syntax:<br>• <config-if># ip acl <NAME><br>• <config-if># ip conflict prevention bind-ip <A.B.C.D><br>• <config-if># ip conflict prevention port-type DHCP-Client<br>• <config-if># ip conflict prevention port-type DHCP-Client has-server<br>• <config-if># ip conflict prevention port-type DHCP-Server<br>• <config-if># ip conflict prevention port-type DHCP-Server |

| | |
|---|---|
| | has-server<br>• <config-if># ip conflict prevention port-type Multiple-Hosts<br>• <config-if># ip conflict prevention port-type Multiple-Hosts has-server<br>• <config-if># ip conflict prevention port-type Static-Binding<br>• <config-if># ip conflict prevention port-type Static-Binding has-server<br>• <config-if># ip igmp filter <1-128><br>• <config-if># ip igmp max-groups <0-256><br>• <config-if># ip igmp max-groups action <deny/replace><br>• <config-if># ip source binding max-entry <1-50><br>• <config-if># ip source binding max-entry no-limit<br>• <config-if># ip source verify mac-and-ip |
| ipv6 | Apply IPv6 configuration to the specified interface (Ethernet port/LAG port).<br>acl <NAME> - Specify the ACL name for packets<br>mld <filter> – Set IPv6 filter for MLD configuration.<br>mld max-groups – Specify the number for maximum group.<br><0-256> - MLD snooping group number.<br>action <deny /replace> – Define the action to be performed when excessing the maximum group.<br>Related Syntax:<br>• <config-if># ipv6 acl <NAME><br>• <config-if># ipv6 mld filter<br>• <config-if># ipv6 mld max-groups <0-256><br>• <config-if># ipv6 mld max-groups action <deny / replace> |
| lacp | Apply LACP Configuration to the specified interface (Ethernet port/LAG port).<br><1-65535> - Set a number for IEEE 802.3 link aggregation port priority.<br><long/short> – Set long or short timeout value.<br>Related Syntax:<br>• <config-if># lacp port-priority <1-65535><br>• <config-if># lacp timeout <long/short> |
| lag | Apply Link Aggregation Group Configuration the specified interface (Ethernet port/LAG port).<br><1-8> - Specify LAG number.<br>Related Syntax:<br>• <config-if># lag <1-8> |
| lldp | med location - Configure the LLDP MED location data. The “coordinate”, “civic-address”, “ecs-elin” locations are independent, so at most three location TLVs could be sent if their data are not empty.<br>med network-policy add / remove - Configure the LLDP MED network policy table. Add /remove a network policy entry that can be bind to ports.<br>med tlv-select - Configure LLDP MED TLVs selection. Available |

| | |
|---|---|
| | optional TLVs are network-policy, location, inventory and poe-pse.<br>tlv-select - Select LLDP TLVs to send.<br><civic-address> - The location is specified as civic address.<br><ADDR> - Range from 6 to 160 hexadecimal bytes.<br><Coordinate> - The location is specified as coordinates.<br><ADDR> - 16 hexadecimal bytes exactly.<br><ecs-elin> - The location is specified as ECS ELIN.<br><ADDR> - 10 to 25 hexadecimal bytes.<br><IDX_LIST> - Range from 1 to 32.<br><TLV> - LLDP optional TLV, pick from: port-desc, sys-name, sys-desc, sys-cap, mac-phy, lag, max-frame-size, management-addr.<br>pvid <disable/enable> - Enable or disable the TX optional-TLV 802.1 PVID.<br>vlan-name <add/remove> <2-4094> - Add/remove a selected VLAN. Enter the VLAN ID number.<br><rx> - Enable LLDP reception on interface.<br><tx> - Enable LLDP transmission on interface.<br>Related Syntax:<br>● <config-if># lldp med location <civic-address/coordinate/ecs-elin> <ADDR><br>● <config-if># lldp med network-policy add <IDX_LIST><br>● <config-if># lldp med network-policy remove <IDX_LIST><br>● <config-if># lldp med tlv-select <network-policy/location/inventory/poe-pse> <network-policy/location/inventory/poe-pse> <network-policy/location/inventory/poe-pse><br>● <config-if># lldp tlv-select <TLV/pvid/vlan-name><br>● <config-if># lldp tlv-select pvid <disable/enable><br>● <config-if># lldp tlv-select vlan-name <add/remove> <2-4094><br>● <config-if># lldp <rx/tx> |
| loop-protection | Record the log, shutdown the port or follow the global loop-protection settings for each port.<br>Related Syntax:<br>● <config-if># loop-protection action all<br>● <config-if># loop-protection action global<br>● <config-if># loop-protection action log<br>● <config-if># loop-protection action shutdown |
| mac | Specify an access control list for packets.<br>Before configuring, you have to create an ACL based on MAC address. For example,<br><config># mac acl CA_ACL<br><config-mac-acl>#<br><NAME> - Enter a name for ACL.<br>Related Syntax: |

| | |
|---|---|
| | • <config-if># mac acl <NAME> |
| mvr | Make MVR configuration.<br>immediate - Enable MVR function.<br>type <receiver/source> - Specify MVR port type as receiver or source.<br>Related Syntax:<br>• <config-if># mvr immediate<br>• <config-if># mvr type <receiver/source> |
| no | Negate command. Such command can disable current setting of command executed and return to the factory setting of that command.<br>Example:<br><config-if> # no mvr<br>The operation will make mvr setting is default. Continue? [yes/no]:yes<br><config-if> #<br>Related Syntax:<br>• <config-if># no <command> |
| poe | Enable or disable the PoE port. |
| port-security | port-security - Enable the port security functionality. Default is disabled.<br>address-limit <1-256>- Enter the number as limitation for MAC address.<br>action <discard / forward / shutdown> – Speicfy an action to be performed.<br>Related Syntax:<br>• <config-if># port-security<br>• <config-if># port-security adderss-limit <1-256> action <discard / forward / shutdown> |
| power | Configure the inline power for the PoE device.<br>inline auto - Turn on the PoE device discovery protocol and apply the power to the devcie.<br>inline never - Turn off the PoE device power.<br>power-limit <15.4w/30w/MW> - Set the power limit for the PoE device.<br>priority <1-3/critical/high/low> - Set the priority of power application for the PoE device.<br>schedule-index - Specify the index number (1 to 15) of the schedule profile.<br>Related Syntax:<br>• <config-if># power inline auto<br>• <config-if># power inline never<br>• <config-if># power power-limit <15.4w/30w/MW><br>• <config-if># power priority <1-3/critical/high/low><br>• <config-if># power schedule-index <1-15> |
| protected | Configure an interface to be a protected port. |

| | |
|---|---|
| | Related Syntax:<br>• <config-if>#protected |
| qos | cos - Configure the default CoS value for an Ethernet port.<br><0-7> - Specify a CoS value for the selected interface. Default value is 0.<br>remark - Configure remarking state of each port.<br>trust - Configure each port to trust state while the system is in “basic” mode. There are four trust types for a device to judge the appropriate queue of the packets.<br><cos> - Enable cos remarking.<br><dscp> - Enable DSCP remarking.<br><cos-dscp> - Enable cos and DSCP remarking.<br><precedence> - Enable IP precedence remarking.<br>Related Syntax:<br>• <config-if>#qos cos <0-7><br>• <config-if>#qos remark <cos/dscp/precedence><br>• <config-if>#qos trust <cos/cos-dscp/ dscp/precedence> |
| rate-limit | It is effective for Ethernet port only.<br>egress - Configure the egress port shaper.<br>ingress - Configure the ingress port shaper.<br>egress queue – Configure queue for egress port shaper.<br><0-1000000> - Enter a number as the average traffic rate in Kbps. It must be a multiple of 16.<br><16-1000000> - Enter a number as the average traffic rate in Kbps. It must be a multiple of 16.<br><1-8> - Specify a number as queue ID.<br>Related Syntax:<br>• <config-if># rate-limit egress <0-1000000><br>• <config-if># rate-limit egress queue <1-8> <16-1000000><br>• <config-if># rate-limit ingress <16-1000000> |
| shutdown | Disable the selected interface.<br>Example:<br>(config)# interface gigabitethernet 3<br>(config-if)# shutdown<br>(config-if)# exit<br>(config)# exit<br># show interface Gigabitethernet 3<br>GigabitEthernet3 is down<br>Related Syntax:<br>• <config-if># shutdown |
| spanning-tree | Configure spanning-tree settings.<br>bpdu-filter - Set the BPDU-Filter for specified port.<br>bpdu-guard - Set the BPDU-Guard for specified port.<br>edge - Set the edge-port for specified port.<br>cost - Change an interface’s spanning tree path cost. |

| | |
|---|---|
| | link-type - Specify a link type for spanning tree protocol use.<br>mcheck - Set the mcheck for specified port to migrate.<br>mst - Set spanning-tree parameters of instance.<br>port-priority- Set the priority for specified instance.<br><0-200000000> - Specify a value of internal path cost (0 means Auto).<br><point-to-point> - The selected port will be treated as point-to-point.<br><shared> - The selected port will be treated as shared.<br><0-15> - Specify an instance ID.<br><0-240> - Specify a priority number for the selected port.<br>Related Syntax:<br>● <config-if># spanning-tree <bpdu-filter /bpdu-guard/ edge><br>● <config-if># spanning-tree cost <0-200000000><br>● <config-if># spanning-tree link-type <point-to-point/shared><br>● <config-if>#spanning-tree mcheck<br>● <config-if>#spanning-tree mst <0-15> cost <0-200000000><br>● <config-if># spanning-tree port-priority <0-240> |
| speed | Configure speed operation.<br><10/100/1000> - Force 10/100/1000 Mbps operation.<br><auto> - Enable Auto speed configuration.<br>Related Syntax:<br>● <config-if># speed<10/100/1000><br>● <config-if># speed auto |
| storm-control | action - Select an action for storm control after exceeding the threshold.<br>broadcast level - Enable the storm control type of broadcast for the selected port.<br>unknown-multicast level - Enable the storm control type of unknown-multicast for the selected port.<br>unknown-unicast level- Enable the storm control type of unknown-unicast for the selected port.<br><drop> - Drop packets after exceeding storm control threshold.<br><shutdown> - Disable the port after exceeding storm control threshold.<br><1-1000000> - Specify the rate value.<br>Related Syntax:<br>● <config-if># storm-control action <drop/shutdown><br>● <config-if># storm-control broadcast level <1-1000000><br>● <config-if># storm-control unknown-multicast level <1-1000000><br>● <config-if># storm-control unknown-unicast level <1-1000000> |
| surveillance-vlan | cos - Set surveillance VLAN configuration.<br>mode - Set surveillance member port join mode. |

| | |
|---|---|
| | <all> - QoS attributes are applied to all packets that are classified to the Surveillance VLAN.<br><src> - QoS attributes are applied only on packets from IP phones.<br><auto> - Make surveillance member port join voice VLAN automatically.<br><manual> - The administrator manually makes surveillance member port join voice VLAN.<br>Related Syntax:<br>• <config-if># surveillance-vlan cos <all/src><br>• <config-if># surveillance-vlan mode <auto/manual> |
| switchport | Set switching mode characteristics.<br>access vlan –Use it to set a native VLAN on the interface.<br>default-vlan tagged – Use it to make the selected port interface to become the default VLAN tagged member.<br>forbidden default-vlan – Use it to forbid the defult-vlan on the interface.<br>forbidden vlan - Use it to forbid a vlan on the interface.<br>hybrid acceptable-frame-type – Use it to choose which type of frame will be accepted.<br>hybrid allowed – Use it to allow a VALN set on the interface.<br>hybrid ingress-filtering – Use it to enable VLAN ingress filter.<br>hybrid pvid – Use it to set PVID of the interface.<br>mode access - Use it to configure the selected port as the role of access. Only untagged frames will be accepted.<br>mode hybrid - Use it to configure the selected port as the role of hybrid. Support all functions defined in IEEE 802.1Q specification.<br>mode trunk uplink – Use it to configure the selected port as the role of trunk. It can recognize double tagging on the interface.<br>trunk allowed – Use it to allow a VALN on the interface.<br>trunk native – Use it to set a native VLAN on the interface.<br>tunnel vlan – Use it to set a Dot1q tunnel VLAN on the interface.<br>vlan tpid – Use it to set TPID on the interface.<br><1-4094> - Specify a VLAN ID.<br><add/remove> - Add or remove the allowed VLAN list.<br><all/tagged-only/untagged-only> - Specify an option for accepting all frames, only tagged frames or only untagged frames.<br><1-4094/all> - Specify a VLAN ID or all VLAN IDs.<br>< 0x8100 / 0x88A8 / 0x9100 / 0x9200> - Specify one tag-protocol-id.<br>Related Syntax:<br>• <config-if># switchport access vlan <1-4094><br>• <config-if># switchport default-vlan tagged<br>• <config-if># switchport forbidden default-vlan<br>• <config-if># switchport forbidden vlan <add/remove> |

| | |
|---|---|
| | <1-4094><br>• <config-if># switchport hybrid acceptable-frame-type <all/tagged-only/untagged-only><br>• <config-if># switchport hybrid allowed vlan add <1-4094><br>• <config-if># switchport hybrid allowed vlan add <1-4094> <tagged/ untagged><br>• <config-if># switchport hybrid allowed vlan remove <1-4094><br>• <config-if># switchport hybrid ingress-filtering<br>• <config-if># switchport hybrid pvid <1-4094><br>• <config-if># switchport mode <access/hybrid><br>• <config-if># switchport mode trunk uplink<br>• <config-if># switchport trunk allowed vlan <add /remove> <1-4094/all><br>• <config-if># switchport trunk native <1-4094><br>• <config-if># switchport tunnel vlan <1-4094><br>• <config-if># switchport vlan tpid < 0x8100/0x88A8 / 0x9100 / 0x9200> |
| udld | Configure UDLD enabled or disabled and ignore global UDLD setting.<br>aggressive - Enable UDLD protocol on such interface.<br>Related Syntax:<br>• <config-if># udld<br>• <config-if># udld aggressive |
| vlan | mac-vlan group - Set a MAC-based VLAN configuration.<br>protocol-vlan group - Set a protocol-based VLAN configuration.<br><1-2147483647> - Specify a group ID to map.<br><1-4094> - Specify a VLAN ID.<br>Related Syntax:<br>• <config-if># vlan mac-vlan group <1-2147483647> vlan <1-4094><br>• <config-if># vlan protocol-vlan group<1-2147483647> vlan <1-4094> |
| voice-vlan | cos - Set voice VLAN configuration as COS mode.<br>mode - Set voice member port join mode.<br><all> - QoS attributes are applied on all packets that are classified to the Voice VLAN.<br><src> - QoS attributes are applied only on packets from IP phones.<br><auto> - Make voice member port join voice VLAN automatically.<br><manual> - The administrator manually makes voice member port join voice VLAN.<br>Related Syntax:<br>• <config-if># voice-vlan cos <all/src><br>• <config-if># voice-vlan mode <auto/manual> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)# interface LAG 1
PQ2200xb(config-if)# speed 100
PQ2200xb(config-if)# backpressure
PQ2200xb(config-if)# lldp med location ecs-elin 112233445566778899AA
PQ2200xb(config-if)# vlan mac-vlan group 35 vlan 1000
PQ2200xb(config-if)#
```

## Telnet Command: ip

Use this command to create an IPv4 access list (ACL) which performs classification on layer 3 fields and enters ip-access configuration mode.

**Syntax Items**

ip acl

ip address

ip arp

ip conflict

ip default-gateway

ip dhcp

ip dns

ip forcedhttps

ip http

ip https

ip igmp

ip route

ip source

ip ssh

ip telnet

**Description**

| Syntax Items | Description |
|---|---|
| ip acl | acl <NAME> - Set the name of the access list (ACL) based on IPv4.<br>To configure detailed settings, enter the name of ACL to access into next level.<br><config>#ip acl <NAME><br>Then, available sub-command includes:<br><config-ip-acl>#deny<br><config-ip-acl>#do<br><config-ip-acl>#end<br><config-ip-acl>#exit<br><config-ip-acl>#permit<br><config-ip-acl>#sequence<br><config-ip-acl>#show |
| | Use the “deny” command to create deny rules for the IPv4 access list. |

| | |
|---|---|
| | <0-255/egp/hmp/icmp/igp/ipinip/ipv6 /ipv6:frag /ipv6:icmp /ipv6:rout / ip / l2tp /ospf /pim / rdp / rsvp /tcp /udp > - Specify the IP protocol number or enter the name of the protocol.<br>\<A.B.C.D>/\<A.B.C.D> \<A.B.C.D>/\<A.B.C.D> - Specify the source and destination IPv4 addresses and subnet masks.<br>dscp <0-63> - Set the DSCP filtering by specifying a value for DSCP.<br>precedence <0-7> - Set the cos value and the cos mask for a packet.<br>shutdown – Disable the Ethernet interface.<br>any – Any IP address (as source or destination).<br>Related Syntax:<br>• \<config-ip-acl >#deny <0-255> \<A.B.C.D>/\<A.B.C.D> \<A.B.C.D>/\<A.B.C.D> dscp <0-63><br>• \<config-ip-acl >#deny <0-255> \<A.B.C.D>/\<A.B.C.D> \<A.B.C.D>/\<A.B.C.D> dscp <0-63> shutdown<br>• \<config-ip-acl >#deny <0-255> \<A.B.C.D>/\<A.B.C.D> \<A.B.C.D>/\<A.B.C.D> precedence <0-7><br>• \<config-ip-acl >#deny <0-255> \<A.B.C.D>/\<A.B.C.D> \<A.B.C.D>/\<A.B.C.D> precedence <0-7> shutdown<br>• \<config-ip-acl >#deny <0-255> any \<A.B.C.D>/\<A.B.C.D> dscp <0-63><br>• \<config-ip-acl >#deny <0-255> any \<A.B.C.D>/\<A.B.C.D> dscp <0-63> shutdown<br>• \<config-ip-acl >#deny <0-255> any \<A.B.C.D>/\<A.B.C.D> precedence <0-7><br>• \<config-ip-acl >#deny <0-255> any \<A.B.C.D>/\<A.B.C.D> precedence <0-7> shutdown<br>• \<config-ip-acl >#deny <0-255> any any dscp <0-7><br>• \<config-ip-acl >#deny <0-255> any any dscp <0-7> shutdown<br>• \<config-ip-acl >#deny <0-255> any any precedence <0-7><br>• \<config-ip-acl >#deny <0-255> any any precedence <0-7> shutdown |
| | Use the “do” command to run execution command in current mode.<br><SEQUENCE> -<br>Related Syntax:<br>• \<config-ip-acl>#do <SEQUENCE> |
| | Use the “end” command to finish current mode. Any changes in current mode will be saved.<br>Related Syntax:<br>• \<config-ip-acl>#end |
| | Use the “exit” command to close the current CLI session or return to the previous mode without saving the settings.<br>Related Syntax:<br>• \<config-ip-acl>#exit |
| | Use the “no sequence” command to delete any entry in |

| | |
|---|---|
| | management ACL.<br><1-2147483647>- Specify an index number of the ACL.<br>Related Syntax:<br>• <config-ip-acl>#no sequence <1-2147483647> |
| | Use the “sequence” command to deny or permit the ACL.<br><1-2147483647> - Enter the sequence of ACL entry. The sequence represents the priority of the ACE in the ACL.<br>Related Syntax:<br>• <config-ip-acl >#sequence <1-2147483647> deny<br>• <config-ip-acl >#sequence <1-2147483647> permit |
| | Use the “show acl” command to list current status of the selected ACL. |
| ip address | Use this command to modify the administration IPv4 address.<br>adddress <A.B.C.D> - Specify the IPv4 addresses. This IP is required when the administer wants to access into VigorSwitch through Telnet, SSH, HTTP, HTTPS, SNMP and so on.<br>mask <A.B.C.D> - Specify the netmask of the IP address.<br>Related Syntax:<br>• <config>#ip address <A.B.C.D><br>• <config>#ip address <A.B.C.D> mask <A.B.C.D> |
| Ip arp | Use this command to enable the function of dynamic ARP inspection.<br>vlan <1-4094> - Specify the VLAN ID number.<br>Related Syntax:<br>• <config>#ip arp inspection<br>• <config>#ip arp inspection vlan <1-4094> |
| ip conflict | Use this command to do IP conflict prevention.<br>lag - Enable/disable the function.<br><A.B.C.D> - Specify the IPv4 addresses.<br><1-16> - Specify a physical port (2.5G).<br><1-4> - Specify a physical port (10G).<br><1-8> - Specify a LAG port.<br><1-4094> - Specify a VLAN ID number.<br>Related Syntax:<br>• <config>#ip conflict detection<br>• <config>#ip conflict lag<br>• <config>#ip conflict prevention<br>• <config>#ip conflict prevention binding <A:B:C:D:E:F> vlan <1-4094> <A.B.C.D> 10GigabitEthernet <1-4> server<br>• <config>#ip conflict prevention binding <A:B:C:D:E:F> vlan <1-4094> <A.B.C.D> 2.5GigabitEthernet <1-16> server<br>• <config>#ip conflict prevention binding <A:B:C:D:E:F> vlan <1-4094> <A.B.C.D> LAG <1-8> server<br>• <config>#ip conflict prevention binding <A:B:C:D:E:F> vlan <1-4094> <A.B.C.D> 10GigabitEthernet <1-4> static<br>• <config>#ip conflict prevention binding <A:B:C:D:E:F> vlan |

| | |
|---|---|
| | <1-4094> <A.B.C.D> 2.5GigabitEthernet <1-16> static<br>• <config>#ip conflict prevention binding <A:B:C:D:E:F> vlan <1-4094> <A.B.C.D> LAG <1-8> static<br>• <config>#ip conflict prevention binding vlan <1-4094> <A.B.C.D> <A.B.C.D> interface 10GigabitEthernet <1-4> server<br>• <config>#ip conflict prevention binding vlan <1-4094> <A.B.C.D> <A.B.C.D> interface 10GigabitEthernet <1-4> static<br>• <config>#ip conflict prevention binding vlan <1-4094> <A.B.C.D> <A.B.C.D> interface 2.5GigabitEthernet <1-16> sterver<br>• <config>#ip conflict prevention binding vlan <1-4094> <A.B.C.D> <A.B.C.D> interface 2.5GigabitEthernet <1-16> static<br>• <config>#ip conflict prevention binding vlan <1-4094> <A.B.C.D> <A.B.C.D> interface LAG<1-8> server<br>• <config>#ip conflict prevention binding vlan <1-4094> <A.B.C.D> <A.B.C.D> interface LAG<1-8> static<br>• <config>#ip conflict prevention clear<br>• <config>#ip conflict prevention server-ip <A.B.C.D> interface 10GigabitEthernet <1-4><br>• <config>#ip conflict prevention server-ip <A.B.C.D> interface 2.5GigabitEthernet <1-16><br>• <config>#ip conflict prevention server-ip <A.B.C.D> interface LAG <1-8> |
| ip default-gateway | Use this command to modify default gateway address.<br>address <A.B.C.D> - Specify the IPv4 addresses.<br>Related Syntax:<br>• <config>#ip default-gateway <A.B.C.D> |
| ip dhcp | Use this command to enable DHCP client to get IP address from remote DHCP server.<br>Related Syntax:<br>• <config>#ip dhcp |
| ip dns | Use this command to modify DNS server configuration.<br><A.B.C.D> - Specify the IP address as primary DNS server.<br><A.B.C.D> <A.B.C.D> - Sepcify two IP addresses as primary and secondary DNS server.<br><X:X:XX:X:X> - Specify the MAC address as primary DNS server.<br><X:X:XX:X:X><X:X::X:X> - Specify two MAC addresses as primary and secondary DNS server.<br>lookup – Enable the IP domain naming system lookup.<br>Related Syntax:<br>• <config>#ip dns <A.B.C.D><br>• <config>#ip dns <A.B.C.D> <A.B.C.D><br>• <config>#ip dns <X:X:XX:X:X><br>• <config>#ip dns <X:X:XX:X:X><X:X::X:X><br>• <config>#ip dns lookup |

| | |
|---|---|
| ip forcedhttps | Use this command to enable the function of forced HTTPS configuration.<br>Related Syntax:<br>• <config>#ip forcedhttps |
| ip http | Use this command to enable the function of HTTP configuration.<br>Session-timeout – Set the session timeout.<br><0-86400> - Set the timeout value. 0 means no timeout.<br>Related Syntax:<br>• <config>#ip http session-timeout <0-86400> |
| ip https | Use this command to enable the function of HTTPS configuration.<br>session-timeout – Set the session timeout.<br><0-86400> - Set the timeout value. 0 means no timeout.<br>tls version <tls1.2/tls1.3> - Set the TLS version.<br>Related Syntax:<br>• <config>#ip https session-timeout <0-86400><br>• <config>#ip https tls version <tls1.2/tls1.3> |
| ip igmp | Use this command to set IGMP profile and enable IGMP snooping function.<br>Profile – Set IGMP profile.<br><1-128> - Enter the index number of IGMP profile to access into next phase for configuring detailed settings.<br><A.B.C.D><A.B.C.D> - Specify the source and destination IPv4 addresses<br>action <deny/permit> - Specify the rule (deny/permit) for the IGMP profile.<br>snooping forward-method <dip/mac> - Set the forward method.<br>snooping report-suppression - Set the IGMP v1 or v2 report suppression.<br>snooping unknown-multicast action drop /flood/router-port- Set unknown multicast. The packets will be dropped, flood, or forwarded to the router ports.<br>snooping version <2/3> - Set the IGMP snooping operation version.<br>snooping vlan <VLAN-LIST>- Set a VLAN ID (1 to 4094) for the IGMP VLAN configuration.<br>forbidden-port 10GigabitEthernt <1 -4> / 2.5GigabitEthernt <1 -16> / LAG <1 - 8> - Specify an interface for the IPv4 forbidden port configuration.<br>immediate-leave - Enable the IGMP snooping immediate-leave function.<br>last-member-query-count <1-7> - Set a value as the Last Member Query Count.<br>last-member-query-interval <1-25> - Set the time interval.<br>querier - Enable the querier for the IGMP VLAN configuration.<br>querier <2/3> - Set the querier version (Version 2 or Version 3). |

| | |
|---|---|
| | query-interval <30-18000> - Set the time interval for the query.<br>response-time <5-20> - Set the response time.<br>robustness-variable <1-7> - Set the robustness variable.<br>router learn pim-dvmrp - Enable the IGMP snooping router port learn by PIM, DVMRP and IGMP messages.<br>static-group <A.B.C.D> - Specify the IPv4 multicast address.<br>interfaces 10GigabitEthernt <1 -4> / 2.5GigabitEthernt <1 -16> / LAG <1 - 8> - Specify an interface.<br>static-port 10GigabitEthernt <1 -4> / 2.5GigabitEthernt <1 -16> / LAG <1 - 8> - Set the static port for an interface.<br>static-router-port 10GigabitEthernt <1 -4> / 2.5GigabitEthernt <1 -16> / LAG <1 - 8> - Set the static router port for an interface.<br>Related Syntax:<br>• <config>#ip igmp profile <1-128><br>• <config-igmp-profile># do<br>• <config-igmp-profile># end<br>• <config-igmp-profile># exit<br>• <config-igmp-profile># profile range ip <A.B.C.D><A.B.C.D><br>• <config-igmp-profile># profile range ip <A.B.C.D><A.B.C.D> action <deny/permit><br>• <config-igmp-profile># profile range ip <A.B.C.D> action <deny/permit><br>• <config-igmp-profile># show ip igmp profile <1-128><br>• <config>#ip igmp snooping<br>• <config>#ip igmp snooping forward-method <dip/mac><br>• <config>#ip igmp snooping report-suppression<br>• <config>#ip igmp snooping unknown-multicast action <drop / flood / router-port><br>• <config>#ip igmp snooping version <2/3><br>• <config>#ip igmp snooping vlan <VLAN-LIST> forbidden-port 10GigabitEthernt <1 -4><br>• <config>#ip igmp snooping vlan <VLAN-LIST> forbidden-port 2.5GigabitEthernt <1 -16><br>• <config>#ip igmp snooping vlan <VLAN-LIST> forbidden-port LAG <1 to 8><br>• <config>#ip igmp snooping vlan <VLAN-LIST> forbidden-router-port 10GigabitEthernt <1 -4><br>• <config>#ip igmp snooping vlan <VLAN-LIST> forbidden-router-port 2.5GigabitEthernt <1 -16><br>• <config>#ip igmp snooping vlan <VLAN-LIST> forbidden-router-port LAG <1 to 8><br>• <config>#ip igmp snooping vlan <VLAN-LIST> immediate-leave<br>• <config>#ip igmp snooping vlan <VLAN-LIST> last-member-query-count <1-7><br>• <config>#ip igmp snooping vlan <VLAN-LIST> last-member-query-interval <1-25> |

| | |
|---|---|
| | • <config>#ip igmp snooping vlan <VLAN-LIST> querier<br>• <config>#ip igmp snooping vlan <VLAN-LIST> querier version <2/3><br>• <config>#ip igmp snooping vlan <VLAN-LIST> query-interval <30-18000><br>• <config>#ip igmp snooping vlan <VLAN-LIST> response-time <5-20><br>• <config>#ip igmp snooping vlan <VLAN-LIST> robustness-variable <1-7><br>• <config>#ip igmp snooping vlan <VLAN-LIST> router learn pim-dvmrp<br>• <config>#ip igmp snooping vlan <VLAN-LIST> static-group <A.B.C.D> interfaces 10GigabitEthernt <1 - 4><br>• <config>#ip igmp snooping vlan <VLAN-LIST> static-group <A.B.C.D> interfaces 2.5GigabitEthernt <1 - 16><br>• <config>#ip igmp snooping vlan <VLAN-LIST> static-group <A.B.C.D> interfaces LAG <1- 8><br>• <config>#ip igmp snooping vlan <VLAN-LIST> static-port 10GigabitEthernt <1 - 4><br>• <config>#ip igmp snooping vlan <VLAN-LIST> static-port 2.5GigabitEthernt <1 - 16><br>• <config>#ip igmp snooping vlan <VLAN-LIST> static-port LAG <1- 8><br>• <config>#ip igmp snooping vlan <VLAN-LIST> static-router-port 10GigabitEthernt <1 - 4><br>• <config>#ip igmp snooping vlan <VLAN-LIST> static-router-port 2.5GigabitEthernt <1 - 16><br>• <config>#ip igmp snooping vlan <VLAN-LIST> static-router-port LAG <1 - 8> |
| ip route | Use this command to create a static route.<br><A.B.C.D> - Specify the source IPv4 address.<br>vlan <1-4094> - Specify the VLAN ID number.<br>mask <A.B.C.D> - Specify the subnet mask.<br>Related Syntax:<br>• <config>#ip route<br>• <config>#ip route <A.B.C.D><br>• <config>#ip route <A.B.C.D> gateway <A.B.C.D><br>• <config>#ip route <A.B.C.D> mask <A.B.C.D> gateway <A.B.C.D> |
| ip source | Use this command to create a static IP source binding entry.<br><A:B:C:D:E:F> - Enter the MAC address for the binding entry (e.g., 14:49:BC:44:A3:D7).<br>vlan <1-4094> - Specify the VLAN ID number.<br><A.B.C.D><A.B.C.D> - Specify the IPv4 addresses and the netmask address.<br><1-16> - Specify a physical port (2.5G GigabitEthernet port).<br><1-4> - Specify a physical port (10G GigabitEthernet port).<br><1-8> - Specify a LAG port. |

| | |
|---|---|
| | Related Syntax:<br>• <config>#ip source binding <A:B:C:D:E:F> vlan <1-4094> <A.B.C.D> interface 10GigabitEthernet <1-4><br>• <config>#ip source binding <A:B:C:D:E:F> vlan <1-4094> <A.B.C.D> interface 2.5GigabitEthernet <1-16><br>• <config>#ip source binding <A:B:C:D:E:F> vlan <1-4094> <A.B.C.D> interface LAG <1-8><br>• <config>#ip source binding vlan <1-4094> <A.B.C.D> <A.B.C.D> interface 10GigabitEthernet <1-4><br>• <config>#ip source binding vlan <1-4094> <A.B.C.D> <A.B.C.D> interface 2.5GigabitEthernet <1-16><br>• <config>#ip source binding vlan <1-4094> <A.B.C.D> <A.B.C.D> interface LAG <1-8> |
| ip ssh | Use this command to generate the key files for SSH connection.<br><all/v1/v2> - Select the key files for SSH connection.<br>Related Syntax:<br>• <config>#ip ssh <all/v1/v2> |
| ip telnet | Use this command to enable telnet service.<br>Related Syntax:<br>• <config>#ip telnet |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)# ip acl market_1
PQ2200xb(config-ip-acl)#
PQ2200xb(config-ip-acl)# deny 20 192.168.2.55/255.255.255.0 192.168.2.85/255.255.255.0
PQ2200xb(config)#
```

## Telnet Command: ipv6

Use this command to create an IPv6 access list (ACL).

**Syntax Items**

ipv6

ipv6 acl

ipv6 address

ipv6 autoconfig

ipv6 default-gateway

ipv6 dhcp

ipv6 mld

**Description**

| Syntax Items | Description |
|---|---|
| ipv6 acl | <NAME> - Set the name of the access list (ACL) based on IPv6.<br>To configure detailed settings, enter the name of ACL to access into next level.<br><config>#ipv6 acl <NAME> |

| | |
|---|---|
| | Then, available sub-command includes:<br><config-ipv6-acl>#deny<br><config-ipv6-acl>#do<br><config-ipv6-acl>#end<br><config-ipv6-acl>#exit<br><config-ipv6-acl>#no<br><config-ipv6-acl>#permit<br><config-ipv6-acl>#sequence<br><config-ipv6-acl>#show |
| | Use the “deny” command to create deny rules for the IPv4 access list.<br><0-255/icmp/ipv6/tcp /udp > - Specify the IP protocol number or enter the name of the protocol.<br><0-255/any> - Specify ICMPv6 number.<br><X:X::X:X>/<0-128> <X:X::X:X>/<0-128> - Specify the source/destination IPv6 addresses and subnet masks.<br>dscp <0-63> - Set the DSCP filtering by specifying a value for DSCP.<br>precedence <0-7> - Set the cos value and the cos mask for a packet.<br>shutdown – Disable the Ethernet interface.<br>any – Any IP address (as source or destination).<br><0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> - Set TCP port.<br>match-all <TCP_FLAG> - Set TCP flags. List of TCP flags that should occur. If a flag should be set, it is prefixed by "+".If a flag should be unset, it is prefixed by "-". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack).<br><0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> <X:X::X:X>/<0-128> <0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> - Set UDP port.<br>Related Syntax:<br>● <config-ipv6-acl >#deny <0-255> <X:X::X:X>/<0-128> <X:X::X:X>/<0-128><br>● <config-ipv6-acl >#deny <0-255> <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> dscp <0-63><br>● <config-ipv6-acl >#deny <0-255> <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> dscp <0-63> shutdown |

| | |
|---|---|
| | • <config-ipv6-acl >#deny <0-255> <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> precedence <0-7><br>• <config-ipv6-acl >#deny <0-255> <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> precedence <0-7> shutdown<br>• <config-ipv6-acl >#deny <0-255> <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> shutdown<br>• <config-ipv6-acl >#deny <0-255> <X:X::X:X>/<0-128> any dscp <0-63><br>• <config-ipv6-acl >#deny <0-255> <X:X::X:X>/<0-128> any dscp <0-63> shutdown<br>• <config-ipv6-acl >#deny <0-255> <X:X::X:X>/<0-128> any precedence <0-7><br>• <config-ipv6-acl >#deny <0-255> <X:X::X:X>/<0-128> any precedence <0-7>shutdown<br>• <config-ipv6-acl >#deny <0-255> <X:X::X:X>/<0-128> any shutdown<br>• <config-ipv6-acl >deny icmp <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> <0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255/any> dscp <0-63><br>• <config-ipv6-acl >#deny icmp <X:X::X:X>/<0-128> <X:X::X:X>/<0-128><0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255/any> dscp <0-63> shutdown<br>• <config-ipv6-acl >#deny icmp <X:X::X:X>/<0-128> <X:X::X:X>/<0-128><0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255/any> precedence <0-7><br>• <config-ipv6-acl >#deny icmp <X:X::X:X>/<0-128> <X:X::X:X>/<0-128><0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255/any> precedence <0-7> shutdown<br>• <config-ipv6-acl >#deny icmp <X:X::X:X>/<0-128> <X:X::X:X>/<0-128><0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255/any> shutdown<br>• <config-ipv6-acl >#deny icmp <X:X::X:X>/<0-128> any <0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255 /any> dscp <0-63><br>• <config-ipv6-acl >#deny icmp <X:X::X:X>/<0-128> any <0-255 / any / destination-unreachable / echo-reply / |

| | |
|---|---|
| | echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255 /any> dscp <0-63> shutdown<br>• <config-ipv6-acl >#deny icmp <X:X::X:X>/<0-128> any <0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255 /any> precedence <0-7><br>• <config-ipv6-acl >#deny icmp <X:X::X:X>/<0-128> any <0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255 /any> precedence <0-7> shutdown<br>• <config-ipv6-acl >#deny icmp <X:X::X:X>/<0-128> any <0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255 /any> shutdown<br>• <config-ipv6-acl >#deny ipv6 <X:X::X:X>/<0-128> <X:X::X:X>/<0-128><br>• <config-ipv6-acl >#deny ipv6 <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> dscp <0-63><br>• <config-ipv6-acl >#deny ipv6 <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> dscp <0-63> shutdown<br>• <config-ipv6-acl >#deny ipv6 <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> precedence <0-7><br>• <config-ipv6-acl >#deny ipv6 <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> precedence <0-7> shutdown<br>• <config-ipv6-acl >#deny ipv6 <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> shutdown<br>• <config-ipv6-acl >#deny ipv6 <X:X::X:X>/<0-128> any dscp <0-63><br>• <config-ipv6-acl >#deny ipv6 <X:X::X:X>/<0-128> any dscp <0-63> shutdown<br>• <config-ipv6-acl >#deny ipv6 <X:X::X:X>/<0-128> any precedence <0-7><br>• <config-ipv6-acl >#deny ipv6 <X:X::X:X>/<0-128> any precedence <0-7>shutdown<br>• <config-ipv6-acl >#deny ipv6 <X:X::X:X>/<0-128> any shutdown<br>• <config-ipv6-acl >#deny ipv6 any <X:X::X:X>/<0-128><br>• <config-ipv6-acl >#deny ipv6 any <X:X::X:X>/<0-128> dscp <0-63><br>• <config-ipv6-acl >#deny ipv6 any <X:X::X:X>/<0-128> dscp <0-63> shutdown<br>• <config-ipv6-acl >#deny ipv6 any <X:X::X:X>/<0-128> precedence <0-7><br>• <config-ipv6-acl >#deny ipv6 any <X:X::X:X>/<0-128> |

| | |
|---|---|
| | precedence <0-7> shutdown<br>• <config-ipv6-acl >#deny ipv6 any <X:X::X:X>/<0-128> shutdown<br>• <config-ipv6-acl >#deny ipv6 any any<br>• <config-ipv6-acl >#deny ipv6 any any dscp <0-63><br>• <config-ipv6-acl >#deny ipv6 any any dscp <0-63> shutdown<br>• <config-ipv6-acl >#deny ipv6 any any precedence <0-7><br>• <config-ipv6-acl >#deny ipv6 any any precedence <0-7> shutdown<br>• <config-ipv6-acl >#deny ipv6 any any shutdown<br>• <config-ipv6-acl >#deny tcp <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www><br>• <config-ipv6-acl >#deny tcp <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> dscp <0-63><br>• <config-ipv6-acl >#deny tcp <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> dscp <0-63> shutdown<br>• <config-ipv6-acl >#deny tcp <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> match-all <TCP_FLAG> dscp <0-63><br>• <config-ipv6-acl >#deny tcp <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / |

| | |
|---|---|
| | echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> match-all <TCP_FLAG> dscp <0-63> shutdown<br>• <config-ipv6-acl >#deny tcp <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> match-all <TCP_FLAG> precedence <0-7><br>• <config-ipv6-acl >#deny tcp <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> match-all <TCP_FLAG> precedence <0-7> shutdown<br>• <config-ipv6-acl >#deny tcp <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> match-all <TCP_FLAG> shutdown<br>• <config-ipv6-acl >#deny tcp <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> precedence <0-7><br>• <config-ipv6-acl >#deny tcp <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> precedence <0-7> shutdown<br>• <config-ipv6-acl >#deny tcp <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X:X>/<0-128> <0-65535 / |

| | |
|---|---|
| | PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> shutdown<br>• <config-ipv6-acl >#deny udp <X:X::X:X>/<0-128> <0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> <X:X::X:X>/<0-128> <0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who><br>• <config-ipv6-acl >#deny udp <X:X::X:X>/<0-128> <0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> <X:X::X:X>/<0-128> <0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> dscp <0-63><br>• <config-ipv6-acl >#deny udp <X:X::X:X>/<0-128> <0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> <X:X::X:X>/<0-128> <0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> dscp <0-63> shutdown<br>• <config-ipv6-acl >#deny udp <X:X::X:X>/<0-128> <0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> <X:X::X:X>/<0-128> <0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> dscp <0-63> precedence <0-7><br>• <config-ipv6-acl >#deny udp <X:X::X:X>/<0-128> <0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> <X:X::X:X>/<0-128> <0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> dscp <0-63> precedence <0-7> shutdown<br>• <config-ipv6-acl >#deny udp <X:X::X:X>/<0-128> <0-65535> any |
| | Use the “do” command to run execution command in current mode.<br><SEQUENCE> -<br>Related Syntax:<br>• <config-ipv6-acl>#do <SEQUENCE> |

| | |
|---|---|
| | Use the “end” command to finish current mode. Any changes in current mode will be saved.<br>Related Syntax:<br>• <config-ipv6-acl>#end |
| | Use the “exit” command to close the current CLI session or return to the previous mode without saving the settings.<br>Related Syntax:<br>• <config-ipv6-acl>#exit |
| | Use the “no sequence” command to delete any entry in management ACL.<br><1-2147483647>- Specify an index number of the ACL.<br>Related Syntax:<br>• <config-ip-acl>#no sequence <1-2147483647> |
| | Use the “permit” command to create permit rules which bypass the packets meet the rule.<br><0-255/icmp/ipv6/tcp /udp > - Specify the IP protocol number or enter the name of the protocol.<br><0-255/any> - Specify ICMPv6 number.<br><X:X::X:X>/<0-128> <X:X::X:X>/<0-128> - Specify the source/destination IPv6 addresses and subnet masks.<br>dscp <0-63> - Set the DSCP filtering by specifying a value for DSCP.<br>precedence <0-7> - Set the cos value and the cos mask for a packet.<br>shutdown – Disable the Ethernet interface.<br>any – Any IP address (as source or destination).<br><0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> - Set TCP port.<br>match-all <TCP_FLAG> - Set TCP flags. List of TCP flags that should occur. If a flag should be set, it is p refixed by "+".If a flag should be unset, it is prefixed by "-". Avai lable options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin.To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack).<br><0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> <X:X::X:X>/<0-128> <0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> - Set UDP port.<br>Related Syntax:<br>• <config-ipv6-acl >#permit <0-255> <X:X::X:X>/<0-128> |

| | |
|---|---|
| | <X:X::X:X>/<0-128><br>• <config-ipv6-acl >\# permit <0-255> <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> dscp <0-63><br>• <config-ipv6-acl >\# permit <0-255> <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> dscp <0-63> shutdown<br>• <config-ipv6-acl >\# permit <0-255> <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> precedence <0-7><br>• <config-ipv6-acl >\# permit <0-255> <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> precedence <0-7> shutdown<br>• <config-ipv6-acl >\# permit <0-255> <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> shutdown<br>• <config-ipv6-acl >\# permit <0-255> <X:X::X:X>/<0-128> any dscp <0-63><br>• <config-ipv6-acl >\# permit <0-255> <X:X::X:X>/<0-128> any dscp <0-63> shutdown<br>• <config-ipv6-acl >\# permit <0-255> <X:X::X:X>/<0-128> any precedence <0-7><br>• <config-ipv6-acl >\# permit <0-255> <X:X::X:X>/<0-128> any precedence <0-7>shutdown<br>• <config-ipv6-acl >\# permit <0-255> <X:X::X:X>/<0-128> any shutdown<br>• <config-ipv6-acl > permit icmp <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> <0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255/any> dscp <0-63><br>• <config-ipv6-acl >\# permit icmp <X:X::X:X>/<0-128> <X:X::X:X>/<0-128><0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255/any> dscp <0-63> shutdown<br>• <config-ipv6-acl >\# permit icmp <X:X::X:X>/<0-128> <X:X::X:X>/<0-128><0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255/any> precedence <0-7><br>• <config-ipv6-acl >\# permit icmp <X:X::X:X>/<0-128> <X:X::X:X>/<0-128><0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255/any> precedence <0-7> shutdown<br>• <config-ipv6-acl >\# permit icmp <X:X::X:X>/<0-128> <X:X::X:X>/<0-128><0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255/any> shutdown<br>• <config-ipv6-acl >\# permit icmp <X:X::X:X>/<0-128> any <0-255 / any / destination-unreachable / echo-reply / |

| | |
|---|---|
| | echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255 /any> dscp <0-63><br>• <config-ipv6-acl ># permit icmp <X:X::X:X>/<0-128> any <0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255 /any> dscp <0-63> shutdown<br>• <config-ipv6-acl ># permit icmp <X:X::X:X>/<0-128> any <0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255 /any> precedence <0-7><br>• <config-ipv6-acl ># permit icmp <X:X::X:X>/<0-128> any <0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255 /any> precedence <0-7> shutdown<br>• <config-ipv6-acl ># permit icmp <X:X::X:X>/<0-128> any <0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255 /any> shutdown<br>• <config-ipv6-acl ># permit ipv6 <X:X::X:X>/<0-128> <X:X::X:X>/<0-128><br>• <config-ipv6-acl ># permit ipv6 <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> dscp <0-63><br>• <config-ipv6-acl ># permit ipv6 <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> dscp <0-63> shutdown<br>• <config-ipv6-acl ># permit ipv6 <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> precedence <0-7><br>• <config-ipv6-acl ># permit ipv6 <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> precedence <0-7> shutdown<br>• <config-ipv6-acl ># permit ipv6 <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> shutdown<br>• <config-ipv6-acl ># permit ipv6 <X:X::X:X>/<0-128> any dscp <0-63><br>• <config-ipv6-acl ># permit ipv6 <X:X::X:X>/<0-128> any dscp <0-63> shutdown<br>• <config-ipv6-acl ># permit ipv6 <X:X::X:X>/<0-128> any precedence <0-7><br>• <config-ipv6-acl ># permit ipv6 <X:X::X:X>/<0-128> any precedence <0-7>shutdown<br>• <config-ipv6-acl ># permit ipv6 <X:X::X:X>/<0-128> any shutdown<br>• <config-ipv6-acl ># permit ipv6 any <X:X::X:X>/<0-128><br>• <config-ipv6-acl ># permit ipv6 any <X:X::X:X>/<0-128> dscp |

| | |
|---|---|
| | <0-63><br>• <config-ipv6-acl ># permit ipv6 any <X:X::X:X>/<0-128> dscp <0-63> shutdown<br>• <config-ipv6-acl ># permit ipv6 any <X:X::X:X>/<0-128> precedence <0-7><br>• <config-ipv6-acl ># permit ipv6 any <X:X::X:X>/<0-128> precedence <0-7> shutdown<br>• <config-ipv6-acl ># permit ipv6 any <X:X::X:X>/<0-128> shutdown<br>• <config-ipv6-acl ># permit ipv6 any any<br>• <config-ipv6-acl ># permit ipv6 any any dscp <0-63><br>• <config-ipv6-acl ># permit ipv6 any any dscp <0-63> shutdown<br>• <config-ipv6-acl ># permit ipv6 any any precedence <0-7><br>• <config-ipv6-acl ># permit ipv6 any any precedence <0-7> shutdown<br>• <config-ipv6-acl ># permit ipv6 any any shutdown<br>• <config-ipv6-acl ># permit tcp <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www><br>• <config-ipv6-acl ># permit tcp <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> dscp <0-63><br>• <config-ipv6-acl ># permit tcp <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> dscp <0-63> shutdown<br>• <config-ipv6-acl >#deny tcp <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> match-all <TCP_FLAG> dscp <0-63> |

| | |
|---|---|
| | • <config-ipv6-acl ># permit tcp <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> match-all <TCP_FLAG> dscp <0-63> shutdown<br>• <config-ipv6-acl ># permit tcp <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> match-all <TCP_FLAG> precedence <0-7><br>• <config-ipv6-acl ># permit tcp <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> match-all <TCP_FLAG> precedence <0-7> shutdown<br>• <config-ipv6-acl ># permit tcp <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> match-all <TCP_FLAG> shutdown<br>• <config-ipv6-acl ># permit tcp <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> precedence <0-7><br>• <config-ipv6-acl ># permit tcp <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time |

| | |
|---|---|
| | / whois / www> precedence <0-7> shutdown<br>• <config-ipv6-acl ># permit tcp <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X:X>/<0-128> <0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> shutdown<br>• <config-ipv6-acl ># permit udp <X:X::X:X>/<0-128> <0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> <X:X::X:X>/<0-128> <0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who><br>• <config-ipv6-acl ># permit udp <X:X::X:X>/<0-128> <0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> <X:X::X:X>/<0-128> <0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> dscp <0-63><br>• <config-ipv6-acl ># permit udp <X:X::X:X>/<0-128> <0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> <X:X::X:X>/<0-128> <0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> dscp <0-63> shutdown<br>• <config-ipv6-acl ># permit udp <X:X::X:X>/<0-128> <0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> <X:X::X:X>/<0-128> <0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> dscp <0-63> precedence <0-7><br>• <config-ipv6-acl ># permit udp <X:X::X:X>/<0-128> <0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> <X:X::X:X>/<0-128> <0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> dscp <0-63> precedence <0-7> shutdown<br>• <config-ipv6-acl ># permit udp <X:X::X:X>/<0-128> <0-65535> any |

| | |
|---|---|
| | Use the “sequence” command to deny or permit the ACL.<br><1-2147483647> - Enter the sequence of ACL entry. The sequence represents the priority of the ACE in the ACL.<br>Related Syntax:<br>● <config-ipv6-acl >#sequence <1-2147483647> deny<br>● <config-ipv6-acl >#sequence <1-2147483647> permit |
| | Use the “show acl” command to list current status of the selected ACL. |
| Ipv6 address | Use this command to modify the administration IPv6 address.<br>address <X:X::X:X> - Specify the IPv6 addresses. This IP is required when the administer wants to access into VigorSwitch through Telnet, SSH, HTTP, HTTPS, SNMP and so on.<br>prefix <0-128> - Specify the prefix length of the IPv6 address.<br>Related Syntax:<br>● <config>#ipv6 address <X:X::X:X> prefix <0-128> |
| ipv6 autoconfig | Use this command to enable IPv6 auto configuration feature. |
| Ipv6 default-gateway | Use this command to modify default gateway address.<br>default-address <X:X::X:X> - Specify the IPv6 addresses of the gateway.<br>Related Syntax:<br>● <config>#ipv6 default-gateway <X:X::X:X> |
| ipv6 dhcp | Use this command to enable DHCPv6 client to get IP address from remote DHCPv6 server.<br>Related Syntax:<br>● <config>#ipv6 dhcp |
| ipv6 mld | Use this command to set MLD configuration.<br>profile <1-128> - Use it to enter profile configuration.<br>snooping – Use it to enable MLD snooping function.<br>forward-method <dip/mac> - Specify a method to forward the packets.<br>report-suppression – Use it to enable MLD snooping report-suppression function.<br>unknown-multicast action <drop/flood/router-port> - Use it to set unknown multicast action.<br>version <1/2> – Use it to change MLD support version.<br>vlan <1-4094> - Use it to enable MLD on VLAN. Specify a VLAN ID for configuration.<br>forbidden-port 10GigabitEthernet <1-4> - Specify a physical port.<br>forbidden-port 2.5GigabitEthernet <1-16> - Specify a physical port.<br>forbidden-port LAG <1-8> - Specify a LAG port.<br>forbidden-router-port 10GigabitEthernet <1-4> - Use it to add static forbidden router port. Specify a physical port.<br>forbidden-router-port 2.5GigabitEthernet <1-16> - Use it to add static forbidden router port. Specify a physical port. |

| | |
|---|---|
| | forbidden-router-port LAG <1-8> - Use it to add static forbidden router port. Specify a LAG port.<br>immediate-leave – Use it to enable fastleave function.<br>last-member-query-count <1-7> - Use it to change how many query packets will send. Specify the last member query count. Default is 2.<br>last-member-query-interval <1-25> - Use it to set interval between each query packet. Specify the last member query interval. Default is 1.<br>query-interval <30-18000> - Use it to set interval between each query. Specify the query interval. Default is 125.<br>response-time <5-20> - Use it to set response time. Specify a time value. Default is 10.<br>robustness-variable <1-7> - Specify a robustness-variable value. Default is 2.<br>router learn pim-dvmrp – Use it to enable learning router port by rouing protocol packets (DVMRP).<br>static-group <X:X::X:X> interfaces 10Gigabitethernet <1-4> - Use it to add a static group. Specify a physical port.<br>static-group <X:X::X:X> interfaces 2.5Gigabitethernet <1-16> - Use it to add a static group. Specify a physical port.<br>static-group <X:X::X:X> interfaces LAG <1-8> - Use it to add a static group. Specify a LAG port.<br>static-port 10Gigabitethernet <1-4> - Use it to add static forwarding port. Specify a physical port.<br>static-port 2.5Gigabitethernet <1-16> - Use it to add static forwarding port. Specify a physical port.<br>static-port LAG <1-8>- Use it to add static forwarding port. Specify a LAG port.<br>static-router-port 10GigabitEthernet <1-4> - Use it to add static router port. All query packets wil forward to the specified port. Specify a physical port.<br>static-router-port 2.5GigabitEthernet <1-16> - Use it to add static router port. All query packets wil forward to the specified port. Specify a physical port.<br>static-router-port LAG <1-8> - Use it to add static router port. All query packets wil forward to the specified port. Specify a LAG port.<br>Related Syntax:<br>● <config>#ipv6 mld profile <1-128><br><config-mld-profile># do<br><config-mld-profile># end<br><config-mld-profile># exit<br><config-mld-profile># profile range ipv6 <X:X::X:X> action <deny/permit><br><config-mld-profile># profile range ipv6 <X:X::X:X> <X:X::X:X><br><config-mld-profile># profile range ipv6 <X:X::X:X> <X:X::X:X> action <deny/permit><br><config-mld-profile># show |

| | |
|---|---|
| | • <config>#ipv6 mld snooping<br>• <config>#ipv6 mld snooping forward-method <dip/mac><br>• <config>#ipv6 mld snooping report-suppression<br>• <config>#ipv6 mld snooping unknown-multicast action <drop/flood/router-port><br>• <config>#ipv6 mld snooping version <1/2><br>• <config>#ipv6 mld snooping vlan <1-4094><br>• <config>#ipv6 mld snooping vlan <1-4094> forbidden-port 10GigabitEthernet <1-4><br>• <config>#ipv6 mld snooping vlan <1-4094> forbidden-port 2.5GigabitEthernet <1-16><br>• <config>#ipv6 mld snooping vlan <1-4094> forbidden-port LAG <1-8><br>• <config>#ipv6 mld snooping vlan <1-4094> forbidden-router-port 10GigabitEthernet <1-4><br>• <config>#ipv6 mld snooping vlan <1-4094> forbidden-router-port 2.5GigabitEthernet <1-16><br>• <config>#ipv6 mld snooping vlan <1-4094> forbidden-router-port LAG <1-8><br>• <config>#ipv6 mld snooping vlan <1-4094> immediate-leave<br>• <config>#ipv6 mld snooping vlan <1-4094> last-member-query-count <1-7><br>• <config>#ipv6 mld snooping vlan <1-4094> last-member-query-interval <1-25><br>• <config>#ipv6 mld snooping vlan <1-4094> query-interval <30-18000><br>• <config>#ipv6 mld snooping vlan <1-4094> response-time <5-20><br>• <config>#ipv6 mld snooping vlan <1-4094> robustness-variable <1-7><br>• <config>#ipv6 mld snooping vlan <1-4094> router learn pim-dvmrp<br>• <config>#ipv6 mld snooping vlan <1-4094> static-group <X:X::X:X> interfaces 10Gigabitethernet <1-4><br>• <config>#ipv6 mld snooping vlan <1-4094> static-group <X:X::X:X> interfaces 2.5Gigabitethernet <1-16><br>• <config>#ipv6 mld snooping vlan <1-4094> static-group <X:X::X:X> interfaces LAG <1-8><br>• <config>#ipv6 mld snooping vlan <1-4094> static-port 10Gigabitethernet <1-4><br>• <config>#ipv6 mld snooping vlan <1-4094> static-port 2.5Gigabitethernet <1-16><br>• <config>#ipv6 mld snooping vlan <1-4094> static-port LAG <1-8><br>• <config>#ipv6 mld snooping vlan <1-4094> static-router-port 10Gigabitethernet <1-4><br>• <config>#ipv6 mld snooping vlan <1-4094> static-router-port 2.5Gigabitethernet <1-16><br>• <config>#ipv6 mld snooping vlan <1-4094> |

| | |
|---|---|
| | static-router-port LAG <1-8> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# ipv6 mld snooping vlan 33
PQ2200xb(config)# ipv6 acl CA_v6
PQ2200xb(config-ipv6-acl)# deny 3 00:50::32:ff/24 00:50::78:aa/32
```

## Telnet Command: jumbo-frame

Use this command to modify the maximum frame size of jumbo frame.

**Syntax Items**

jumbo-frame

**Description**

| Syntax Items | Description |
|---|---|
| jumbo-frame | Enable the function of jumbo frame.<br>Set the maximum frame size.<br><1518-10000> - The default value is 1522.<br>Related Syntax:<br>• <config># jumbo-frame<br>• <config># jumbo-frame <1518-10000> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# jumbo-frame 8000
PQ2200xb(config)#
```

## Telnet Command: lacp

Use this command to set the system priority of the switch.

**Syntax Items**

lacp

lacp system-priority

**Description**

| Syntax Items | Description |
|---|---|
| lacp | Enable the function. |
| lacp system-priority | It is used for selecting a master switch between two devices. Lower system priority has higher priority. The device with higher priority value can determine which port is able to join LAG.<br><1-65535> - Specify the system priority value.<br>Related Syntax: |

| | |
|---|---|
| | • <config># lacp<br>• <config># lacp system-priority <1-65535> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# lacp system-priority 1000
PQ2200xb(config)#
```

## Telnet Command: lag

LAG port can transmit packets to all ports for balancing the traffic loading. Use this command to change the load balance algorithm to src-dst-mac or src-dst-mac-ip as the Load Balance policy.

**Syntax Items**

lag load-balance

**Description**

| Syntax Items | Description |
|---|---|
| lag load-balance | LAG load balancing is based on source and destination MAC address and/or IP address.<br>Related Syntax:<br>• <config># lag load-balance src-dst-mac<br>• <config># lag load-balance src-dst-mac-ip |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
```

## Telnet Command: line

Use this command to select line configuration mode.

**Syntax Items**

line console

line ssh

line telent

**Description**

| Syntax Items | Description |
|---|---|
| console/ssh/telnet | Select console configuration mode.<br>To configure detailed settings, access into next level.<br><config>#line <console/ssh/telnet><br>console - Select the console line to configure. Then, available sub-commands are:<br><config-line>#do<br><config-line>#exec-timeout<br><config-line>#exit |

| | |
|---|---|
| | <config-line>#lhistory<br><config-line>#no<br><config-line>#password-thresh<br><config-line>#silent-time |
| | Select SSH line to configure. Then, available sub-commands are:<br><config-line>#do<br><config-line>#end<br><config-line>#exec-timeout<br><config-line>#exit<br><config-line>#password-thresh<br><config-line>#silent-time |
| | telnet - Select telnet line to configure. Then, available sub-commands are:<br><config-line>#do<br><config-line>#end<br><config-line>#exec-timeout<br><config-line>#exit<br><config-line>#password-thresh<br><config-line>#silent-time |
| #do | Use the “do” command to run execution command in current mode.<br><SEQUENCE> -<br>Related Syntax:<br>● <config-line>#do <SEQUENCE> |
| #exec-timeout | Use the “exec-timeout” to set the session timeout configuration.<br><0-65535> - Enter the number.<br>Related Syntax:<br>● <config-line>#exec-timeout <0-65535> |
| #exit | Use the “exit” command to close the current CLI session or return to the previous mode without saving the settings.<br>Related Syntax:<br>● <config-line>#exit |
| #history | Use the “history” command to specify the index number of history.<br><1-256> - Enter a number.<br>Related Syntax:<br>● <config-line>#history <1-256> |
| #no | Use the “no” command to negate line command.<br>Related Syntax:<br>● <config-line>#no enable<br>● <config-line>#no history<br>● <config-line>#no login |

| | |
|---|---|
| #password-thresh | Use the “password-thresh” command to set the login password intrusion threshold.<br><0-120> - Set a number of allowed password attempts. 0 means no threshold.<br>Related Syntax:<br>● <config-line>#password-thresh <0-120> |
| #silent-time | Use the “silent-time” command to set fail silent time.<br><0-65535> - Set the time to disable the console response.<br>Related Syntax:<br>● <config-line>#silent-time <0-65535> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# line telnet
PQ2200xb(config-line)#
```

## Telnet Command: lldp

Use this command to set LLDP function.

**Syntax Items**

lldp

lldp holdtime-multiplier

lldp lldpdu

lldp reinit-delay

lldp tx-delay

lldp tx-interval

**Description**

| Syntax Items | Description |
|---|---|
| lldp | Enable the function of LLDP. |
| lldp holdtime-multiplier | Set the multiplier used for calculating the LLDP discovery packet hold time.<br><2-10> - Set the LLDP hold time multiplier.<br>Related Syntax:<br>● <config># lldp holdtime-multiplier <2-10> |
| lldp lldpdu | bridging - The LLDP packets will be bridging when LLDP is disabled.<br>filtering - The LLDP packets will be filtered and deleted when LLDP is disabled.<br>flooding - The LLDP packets will be flooded and forwarded to all interfaces when LLDP is disabled.<br>Related Syntax:<br>● <config># lldp lldpdu bridging<br>● <config># lldp lldpdu filtering<br>● <config># lldp lldpdu flooding |

| | |
|---|---|
| lldp reinit-delay | Set the LLDP re-initial delay to avoid LLDP generating too many PDU.<br><1-10> - Specify a number for LLDP server to initialize.<br>Related Syntax:<br>● <config># lldp reinit-delay <1-10> |
| lldp tx-delay | Set the delay time between the successful LLDP frame transmissions.<br><1-8191> - Enter the number of delay time.<br>Note that both tx-interval and tx-delay will affect the LLDP PDU TX time.<br>Related Syntax:<br>● <config># lldp tx-delay <1-8191> |
| lldp tx-interval | Set the LLDP TX interval.<br><5-32767> - Enter the interval in unit of second.<br>Related Syntax:<br>● <config># lldp tx-interval <5-32767> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# lldp holdtime-multiplier 5
PQ2200xb(config)#
```

## Telnet Command: logging

Use this command to set logging service on VigorSwitch.

**Syntax Items**

logging
logging buffered
logging console
logging file
logging host

**Description**

| Syntax Items | Description |
|---|---|
| logging | Enable the logging service. |
| logging buffered | Store the log message in the RAM. |
| logging console | Specify the logging level.<br><0-7> - Specify the logging level by entering a number (from EMEGR-DEBUG).<br>Related Syntax:<br>● <config># logging console<br>● <config># logging console severity <0-7> |
| logging file | Store the log message in the flash.<br><0-7> - Specify the logging level by entering a number (from |

| | |
|---|---|
| | EMEGR-DEBUG).<br>Related Syntax:<br>• <config># logging file severity <0-7> |
| logging host | Define the logging server.<br>host <A.B.C.D> - Enter an IP address of the remote (or local) server.<br>facility <local0-local7> - Specify the facility parameter for the syslog message.<br>port <1-65535> - Enter a number for the remote server. Default is 514.<br>severity <0-7> - Specify the logging level by entering a number (from EMEGR-DEBUG).<br><HOSTNAME> - Define a name as the host.<br>Related Syntax:<br>• <config>#logging host <A.B.C.D> facility <local0-local7><br>• <config>#logging host <A.B.C.D> port <1-65535><br>• <config>#logging host <A.B.C.D> port <1-65535> facility <local0-local7><br>• <config>#logging host <A.B.C.D> port <1-65535> severity <0-7> facility <local0-local7><br>• <config>#logging host <A.B.C.D> severity <0-7> facility <local0-local7><br>• <config>#logging host <HOSTNAME> facility <local0-local7><br>• <config>#logging host <HOSTNAME> port <1-65535><br>• <config>#logging host <HOSTNAME> port <1-65535> facility <local0-local7><br>• <config>#logging host <HOSTNAME> port <1-65535> severity <0-7> facility <local0-local7><br>• <config>#logging host <HOSTNAME> severity <0-7> facility <local0-local7><br>• <config>#logging host <X:X::X:X> facility <local0-local7><br>• <config>#logging host <X:X::X:X> port <1-65535><br>• <config>#logging host <X:X::X:X> port <1-65535> facility <local0-local7><br>• <config>#logging host <X:X::X:X> port <1-65535> severity <0-7> facility <local0-local7> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# logging host aa:00::1a:FF facility local1
```

## Telnet Command: logmail

Use this command to configure log mail.

**Syntax Items**

logmail active

logmail auth

logmail category
logmail encpassword
logmail encry
logmail password
logmail port
logmail receiver
logmail sender
logmail server
logmail username

**Description**

| Syntax Items | Description |
|---|---|
| logmail active | <disable/enable> - Enable or disable the function of log mail.<br>Related Syntax:<br>• <config># logmail active <disable/enable> |
| logmail auth | <disable/enable> - Enable or disable the function of SMTP server authentication.<br>Related Syntax:<br>• <config># logmail auth <disable/enable> |
| logmail category | <AAA, ACL, AUTHMGR,CABLE_DIAG, DAI, DHCP_SNOOPING, GVRP, IGMP_SNOOPING, IPSG, L2, LLDP, Mac-based, Mirror, MLD_SNOOPING, Platform, PM, POE, Port, PORT_SECURITY, QoS, Rate, SNMP, STP, Security, System, Surveillance, Trunk, UDLD, VLAN, CLEAR> - Specify one type for the logmail.<br>Related Syntax:<br>• <config># logmail category <AAA, ACL, AUTHMGR,CABLE_DIAG, DAI, DHCP_SNOOPING, GVRP, IGMP_SNOOPING, IPSG, L2, LLDP, Mac-based, Mirror, MLD_SNOOPING, Platform, PM, POE, Port, PORT_SECURITY, QoS, Rate, SNMP, STP, Security, System, Surveillance, Trunk, UDLD, VLAN, CLEAR> |
| logmail encpassword | Set SMTP encrypt authentication password.<br><PASSWORD> - Enter the password for SMTP server encrypt authentication.<br>Related Syntax:<br>• <config># logmail encpassword <PASSWORD> |
| logmail encry | <disable/ssltls/starttls> - Specify the encryption type for mail alert.<br>Related Syntax:<br>• <config># logmail encry <disable/ ssltls/starttls> |
| logmail password | <PASSWORD> - Enter the password for SMTP server authentication.<br>Related Syntax:<br>• <config># logmail password <PASSWORD> |
| logmail port | <0-65535>- Enter a port number.<br>Related Syntax: |

| | |
|---|---|
| | • <config># logmail port <0-65535> |
| logmail receiver | Specify an address for receiving the alart mail.<br><ADDRESS> - Enter the email address of the receiver.<br>Related Syntax:<br>• <config># logmail receiver <ADDRESS> |
| logmail sender | Specify an address which sends out the alert mail.<br><ADDRESS> - Enter the email address of the sender.<br>Related Syntax:<br>• <config># logmail |
| logmail server | Set the IP address of the server.<br><ADDRESS> - Enter the IP address of the SMTP server.<br>Related Syntax:<br>• <config># logmail server <ADDRESS> |
| logmail username | <NAEM> - Enter the username authenticated by STMP server.<br>Related Syntax:<br>• <config># logmail username <NAME> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# logmail receiver carrie_ni@draytek.com
PQ2200xb(config)#
```

## Telnet Command: loop-protection

Use this command to set loop-protection.

**Syntax Items**

loop-protection action
loop-protection periodicTime
loop-protection state

**Description**

| Syntax Items | Description |
|---|---|
| loop-protection action | Specify an action to be taken when the loop is happened.<br><all/log/shutdown> - Specify one action to be executed.<br>Related Syntax:<br>• <config># loop-protection action <all/log/shutdown> |
| loop-protection periodicTime | Send the loop protection packets to the network hosts.<br><1-3> - Enter the number of the packet.<br>Related Syntax:<br>• <config># Related Syntax:<br>• <config># loop-protection periodicTime <1-3> |
| loop-protection state | <enable/disable> - Enable or disable the function of loop protection. |

| | |
|---|---|
| | Related Syntax:<br>• <config># loop-protection state <enable/disable> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# loop-protection state enable
PQ2200xb(config)#
```

## Telnet Command: mac

Use this command to create a MAC access list.

**Syntax Items**

mac acl

mac address-table

**Description**

| Syntax Items | Description |
|---|---|
| mac acl | <NAME> - Set the name of the access list (ACL).<br>To configure detailed settings, enter the name of ACL to access into next level.<br><config>#mac acl <NAME><br>Then, available sub-commands are:<br><config-mac-acl>#deny<br><config-mac-acl>#do<br><config-mac-acl>#end<br><config-mac-acl>#exit<br><config-mac-acl>#permit<br><config-mac-acl>#sequence |
| | Use the “deny” command to add deny rules for the MAC access list:<br><A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> - Specify the source and destination MAC addresses and subnet masks.<br>cos <0-7><0-7> - Set the cos value and the cos mask for a packet.<br><0x0600-0xFFFF> - Set the EtherType of the packet.<br>Shutdown – Disable the Ethernet interface.<br>vlan <1-4094> - Specify the VLAN ID of the packet.<br>any – Any MAC address.<br>Related Syntax:<br>• <config-mac-acl >#deny <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7><br>• <config-mac-acl >#deny <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#deny <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> ethtype |

| | |
|---|---|
| | <0x0600-0xFFFF> shutdown<br>• <config-mac-acl >#deny <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> shutdown<br>• <config-mac-acl >#deny <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> ethtype <0x0600-0xFFFF><br>• <config-mac-acl ># deny <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> ethtype <0x0600-0xFFFF> shutdown<br>• <config-mac-acl ># deny <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> shutdown<br>• <config-mac-acl >#deny any <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7><br>• <config-mac-acl >#deny any <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#deny any <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> ethtype <0x0600-0xFFFF> shutdown<br>• <config-mac-acl >#deny any <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> shutdown<br>• <config-mac-acl >#deny any any cos <0-7><0-7><br>• <config-mac-acl >#deny any any cos <0-7><0-7> ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#deny any any cos <0-7><0-7> ethtype <0x0600-0xFFFF> shutdown<br>• <config-mac-acl >#deny any any cos <0-7><0-7> shutdown<br>• <config-mac-acl >#deny any any ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#deny any any ethtype <0x0600-0xFFFF> shutdown<br>• <config-mac-acl >#deny any any shutdown<br>• <config-mac-acl >#deny any any vlan <1-4094><br>• <config-mac-acl >#deny any any vlan <1-4094> cos <0-7><0-7><br>• <config-mac-acl >#deny any any vlan <1-4094> cos <0-7><0-7> ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#deny any any vlan <1-4094> cos <0-7><0-7> ethtype <0x0600-0xFFFF> shutdown<br>• <config-mac-acl >#deny any any vlan <1-4094> ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#deny any any vlan <1-4094> ethtype <0x0600-0xFFFF> shutdown<br>• <config-mac-acl >#deny any any vlan <1-4094> shutdown |
| | Use the “do” command to run execution command in current mode.<br><SEQUENCE> -<br>Related Syntax:<br>• <config-mac-acl>#do <SEQUENCE> |
| | Use the “end” command to finish current mode. Any changes in current mode will be saved. |

| | |
|---|---|
| | Related Syntax:<br>• <config-mac-acl>#end |
| | Use the “exit” command to close the current CLI session or return to the previous mode without saving the settings.<br>Related Syntax:<br>• <config-mac-acl>#exit |
| | Use the “no sequence” command to delete any entry in management ACL.<br><1-65535>- Specify an index number of the ACL.<br>Related Syntax:<br>• <config-mac-acl>#no sequence <1-65535> |
| | Use the “permit” command to add permit rules which bypass the packets meet the rule.<br><A:B:C:D:E:F>/<A:B:C:D:E:F >- Specify the source and destination MAC addresses and subnet masks.<br>cos <0-7><0-7> - Set the cos value and the cos mask for a packet.<br><0x0600-0xFFFF> - Set the EtherType of the packet.<br>Shutdown – Disable the Ethernet interface.<br>vlan <1-4094> - Specify the VLAN ID of the packet.<br>any – Any MAC address.<br>Related Syntax:<br>• <config-mac-acl >#permit <A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7><br>• <config-mac-acl >#permit <A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#permit <A:B:C:D:E:F>/<A:B:C:D:E:F> ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#permit <A:B:C:D:E:F>/<A:B:C:D:E:F> vlan <1-4094><br>• <config-mac-acl >#permit <A:B:C:D:E:F>/<A:B:C:D:E:F> vlan <1-4094>cos <0-7><0-7><br>• <config-mac-acl >#permit <A:B:C:D:E:F>/<A:B:C:D:E:F> vlan <1-4094>cos <0-7><0-7> ethtype <0x0600-0xFFFF><br>• <config-mac-acl>#permit <A:B:C:D:E:F>/<A:B:C:D:E:F> vlan <1-4094>ethtype <0x0600-0xFFFF><br>• <config-mac-acl>#permit any <A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7><br>• <config-mac-acl>#permit any <A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7>ethtype <0x0600-0xFFFF><br>• <config-mac-acl>#permit any <A:B:C:D:E:F>/<A:B:C:D:E:F> ethtype <0x0600-0xFFFF><br>• <config-mac-acl>#permit any <A:B:C:D:E:F>/<A:B:C:D:E:F> vlan <1-4094><br>• <config-mac-acl>#permit any <A:B:C:D:E:F>/<A:B:C:D:E:F> vlan <1-4094> cos <0-7><0-7><br>• <config-mac-acl>#permit any <A:B:C:D:E:F>/<A:B:C:D:E:F> vlan <1-4094> cos <0-7><0-7>ethtype <0x0600-0xFFFF> |

| | |
|---|---|
| | • <config-mac-acl>#permit any <A:B:C:D:E:F>/<A:B:C:D:E:F> vlan <1-4094> ethtype <0x0600-0xFFFF> |
| | Use the “sequence” command to deny or permit the ACL.<br><1-2147483647> - Enter the sequence index ACE. The sequence represents the priority of the ACE in the ACL.<br><A:B:C:D:E:F>/<A:B:C:D:E:F >- Specify the source and destination MAC addresses and subnet masks.<br>cos <0-7><0-7> - Set the cos value and the cos mask for a packet.<br><0x0600-0xFFFF> - Set the EtherType of the packet.<br>shutdown – Disable the Ethernet interface.<br>vlan <1-4094> - Specify the VLAN ID of the packet.<br>any – Any MAC address.<br>Related Syntax:<br>• <config-mac-acl >#sequence <1-2147483647>deny <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7><br>• <config-mac-acl >#sequence <1-2147483647>deny <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#sequence <1-2147483647>deny <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> ethtype <0x0600-0xFFFF> shutdown<br>• <config-mac-acl >#sequence <1-2147483647>deny <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> shutdown<br>• <config-mac-acl >#sequence <1-2147483647>deny <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#sequence <1-2147483647>deny <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> ethtype <0x0600-0xFFFF> shutdown<br>• <config-mac-acl >#sequence <1-2147483647>deny <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> shutdown<br>• <config-mac-acl >#sequence <1-2147483647>deny any <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7><br>• <config-mac-acl >#sequence <1-2147483647>deny any <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#sequence <1-2147483647>deny any <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> ethtype <0x0600-0xFFFF> shutdown<br>• <config-mac-acl >#sequence <1-2147483647>deny any <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> shutdown<br>• <config-mac-acl >#sequence <1-2147483647>deny any any cos <0-7><0-7><br>• <config-mac-acl >#sequence <1-2147483647>deny any any |

| | |
|---|---|
| | cos <0-7><0-7> ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#sequence <1-2147483647>deny any any cos <0-7><0-7> ethtype <0x0600-0xFFFF> shutdown<br>• <config-mac-acl >#sequence <1-2147483647>deny any any cos <0-7><0-7> shutdown<br>• <config-mac-acl >#sequence <1-2147483647>deny any any ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#sequence <1-2147483647>deny any any ethtype <0x0600-0xFFFF> shutdown<br>• <config-mac-acl >#sequence <1-2147483647>deny any any shutdown<br>• <config-mac-acl >#sequence <1-2147483647>deny any any vlan <1-4094><br>• <config-mac-acl >#sequence <1-2147483647>deny any any vlan <1-4094> cos <0-7><0-7><br>• <config-mac-acl >#sequence <1-2147483647>deny any any vlan <1-4094> cos <0-7><0-7> ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#sequence <1-2147483647>deny any any vlan <1-4094> cos <0-7><0-7> ethtype <0x0600-0xFFFF> shutdown<br>• <config-mac-acl >#sequence <1-2147483647>deny any any vlan <1-4094> ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#sequence <1-2147483647>deny any any vlan <1-4094> ethtype <0x0600-0xFFFF> shutdown<br>• <config-mac-acl >#sequence <1-2147483647>deny any any vlan <1-4094> shutdown<br>• <config-mac-acl >#sequence <1-2147483647>permit <A:B:C:D:E:F>/<A:B:C:D:E:F> <A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7><br>• <config-mac-acl >#sequence <1-2147483647>permit <A:B:C:D:E:F>/<A:B:C:D:E:F> <A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#sequence <1-2147483647>permit <A:B:C:D:E:F>/<A:B:C:D:E:F> <A:B:C:D:E:F>/<A:B:C:D:E:F> ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#sequence <1-2147483647>permit <A:B:C:D:E:F>/<A:B:C:D:E:F> <A:B:C:D:E:F>/<A:B:C:D:E:F> vlan <1-4094><br>• <config-mac-acl >#sequence <1-2147483647>permit <A:B:C:D:E:F>/<A:B:C:D:E:F> <A:B:C:D:E:F>/<A:B:C:D:E:F> vlan <1-4094> cos <0-7><0-7><br>• <config-mac-acl >#sequence <1-2147483647>permit <A:B:C:D:E:F>/<A:B:C:D:E:F> <A:B:C:D:E:F>/<A:B:C:D:E:F> vlan <1-4094> cos <0-7><0-7> ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#sequence <1-2147483647>permit <A:B:C:D:E:F>/<A:B:C:D:E:F> <A:B:C:D:E:F>/<A:B:C:D:E:F> vlan <1-4094> ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#sequence <1-2147483647>permit any <A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7><br>• <config-mac-acl >#sequence <1-2147483647>permit any |

| | |
|---|---|
| | <A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#sequence <1-2147483647>permit any <A:B:C:D:E:F>/<A:B:C:D:E:F> vlan <1-4094><br>• <config-mac-acl >#sequence <1-2147483647>permit any <A:B:C:D:E:F>/<A:B:C:D:E:F> vlan <1-4094> cos <0-7><0-7><br>• <config-mac-acl >#sequence <1-2147483647>permit any <A:B:C:D:E:F>/<A:B:C:D:E:F> vlan <1-4094> cos <0-7><0-7> ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#sequence <1-2147483647>permit any <A:B:C:D:E:F>/<A:B:C:D:E:F> vlan <1-4094> ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#sequence <1-2147483647>permit any any cos <0-7><0-7><br>• <config-mac-acl >#sequence <1-2147483647>permit any any cos <0-7><0-7> ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#sequence <1-2147483647>permit any any ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#sequence <1-2147483647>permit any any vlan <1-4094><br>• <config-mac-acl >#sequence <1-2147483647>permit any any vlan <1-4094> cos <0-7><0-7><br>• <config-mac-acl >#sequence <1-2147483647>permit any any vlan <1-4094> cos <0-7><0-7> ethtype <0x0600-0xFFFF><br>• <config-mac-acl >#sequence <1-2147483647>permit any any vlan <1-4094> ethtype <0x0600-0xFFFF> |
| mac address-table | Set the aging time for an entry remains in the MAC address table.<br>address-table static - Add a static address to the MAC address table to drop the packets with the specified source or destination MAC address.<br><10-630> - Unit is second. Default is 300.<br>static <A:B:C:D:E:F> - Enter the MAC address (e.g., 14:49:BC:44:A3:D7).<br>vlan <1-4094> - Specify the VLAN ID of the packet.<br>10GigabitEthernet <1-4> - Specify a physical port.<br>2.5GigabitEthernet <1-16> - Specify a physical port.<br>LAG <1-8> - Specify a LAG port.<br>Related Syntax:<br>• <config># mac address-table aging-time <10-630><br>• <config># mac address-table static <A:B:C:D:E:F> vlan <1-4094> drop<br>• <config># mac address-table static <A:B:C:D:E:F> vlan <1-4094> interfaces 10GigabitEthernet <1-4><br>• <config># mac address-table static <A:B:C:D:E:F> vlan <1-4094> interfaces 2.5GigabitEthernet <1-16><br>• <config># mac address-table static <A:B:C:D:E:F> vlan <1-4094> interfaces LAG <1-8> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)# mac acl test_CA
PQ2200xb(config-mac-acl)# deny 00:50:00:7f:12:11/00:00:00:00:10:20
00:50:00:aa:bb:cc/00:00:00:00:12:00 cos 3 2 ethtype 0x0600
PQ2200xb(config-mac-acl)# deny any 00:50:00:7f:12:11/00:00:00:00:10:20 cos 5 6 ethtype
0x0600
PQ2200xb(config-mac-acl)# deny any
PQ2200xb(config)# mac address-table static 00:50:07:12:ff:aa vlan 300 drop
```

## Telnet Command: mailalert

Use this command to configure mail alert for various conditions.

**Syntax Items**

mailalert active
mailalert auth
mailalert devicecheck
mailalert encpassword
mailalert encry
mailalert hwmon
mailalert interval
mailalert ipconfilict
mailalert password
mailalert poestatus
mailalert port
mailalert portlink
mailalert portspeed
mailalert receiver
mailalert sender
mailalert server
mailalert sysrestart
mailalert throughputcheck
mailalert username

**Description**

| Syntax Items | Description |
|---|---|
| mailalert active | <disable/enable> - Enable or disable the function of mail alert.<br>Related Syntax:<br>• <config># mailalert active <disable/enable> |
| mailalert auth | <disable/enable> - Enable or disable the function of SMTP server authentication.<br>Related Syntax:<br>• <config># mailalert auth <disable/enable> |
| mailalert devicecheck | <disable/enable> - Enable or disable the function of sending a mail alert when encountering a device check error.<br>Related Syntax: |

| | |
|---|---|
| | • <config># mailalert devicecheck <disable/enable> |
| mailalert encpassword | <PASSWORD> - Set a encryption authentication password for the mail alert.<br>Related Syntax:<br>• <config># mailalert encpassword <PASSWORD> |
| mailalert encry | Specify the encryption type for mail alert.<br><disable/ssltls/starttls> -<br>Related Syntax:<br>• <config># mailalert encry <disable/ ssltls/starttls> |
| mailalert hwmon | Send a mail alert when hardware monitor error.<br><disable/enable> - Enable or disable the function.<br>Related Syntax:<br>• <config># mailalert hwmon <disable/enable> |
| mailalert interval | Set the transmission interval for the mail alert.<br><1-60> - Unit is second.<br>Related Syntax:<br>• <config># mailalert interval <1-60> |
| mailalert ipconflict | <disable/enable> - Enable or disable the function of sending a mail alert if encountering the IP conflict.<br>Related Syntax:<br>• <config># mailalert ipconflict <disable/enable> |
| mailalert password | <PASSWORD> - Enter the password for SMTP server authentication.<br>Related Syntax:<br>• <config># mailalert password <PASSWORD> |
| mailalert poestatus | <disable/enable> - Enable or disable the function of sending a mail alert when PoE status is changed.<br>Related Syntax:<br>• <config># mailalert poestatus <disable/enable> |
| mailalert port | <0-65535>- Enter a port number.<br>Related Syntax:<br>• <config># mailalert port <0-65535> |
| mailalert portlink | <disable/enable> - Enable or disable the function of sending an alert when the port lnik status changes.<br>Related Syntax:<br>• <config># mailalert portlink <disable/enable> |
| mailalert portspeed | <disable/enable> - Enable or disable the function of sending an alert when the port link speed changes.<br>Related Syntax:<br>• <config># mailalert portspeed <disable/enable> |
| mailalert receiver | Specify an address for receiving the alart mail.<br><ADDRESS> - Enter the email address of the receiver.<br>Related Syntax:<br>• <config># mailalert receiver <ADDRESS> |

| | |
|---|---|
| mailalert sender | Specify an address which sends out the alert mail.<br><ADDRESS> - Enter the email address of the sender.<br>Related Syntax:<br>• <config># mailalert sender <ADDRESS> |
| mailalert server | Set the IP address of the server.<br><ADDRESS> - Enter the IP address of the SMTP server.<br>Related Syntax:<br>• <config># mailalert server <ADDRESS> |
| mailalert sysrestart | <disable/enable> -Enable or disable the function of sending a mail alert when the system restarts.<br>Related Syntax:<br>• <config># mailalert sysrestart <disable/enable> |
| mailalert throughputcheck | <disable/enable> - Enable or disable the function of sending a mail alert when reaching the throughput threshold.<br>Related Syntax:<br>• <config># mailalert throughputcheck <disable/enable> |
| mailalert username | <NAEM> - Enter the username authenticated by STMP server.<br>Related Syntax:<br>• <config># mailalert username <NAME> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# mailalert receiver carrie_ni@draytek.com
```

## Telnet Command: management

Use this command to create a management access list and set configuration mode.

**Syntax Items**

management access-list

management access-class

**Description**

| Syntax Items | Description |
|---|---|
| management access-list | <NAME> - Enter the name of the access list.<br>To configure detailed settings, enter the name of ACL to access into next level.<br><config>#management access-list <NAME><br>Then, available sub-commands are:<br><config-macl>#deny<br><config-macl>#do<br><config-macl>#end<br><config-macl>#exit<br><config-macl>#permit<br><config-macl>#sequence |

| | |
|---|---|
| | Use the “deny” command to add deny rules for the management access list:<br>10GigabitEthernet <1-4> - Specify a physical port.<br>2.5GigabitEthernet <1-16> - Specify a physical port.<br>LAG <1-8> - Specify a LAG port.<br>service <all/http/https/snmp/ssh/telnet> - Specify the servcie type.<br>ip <A.B.C.D>/<A.B.C.D> - Specify the source IP address with mask for the packets.<br>ipv6 <X:X::X:X>/<0-128> - Specify the source IPv6 address and prefix length of the packet.<br>Related Syntax:<br>● <config-macl>#deny interfaces 10GigabitEthernet <1-4> service <all/http/https/snmp/ssh/telnet><br>● <config-macl>#deny interfaces 2.5GigabitEthernet <1-16> service <all/http/https/snmp/ssh/telnet><br>● <config-macl>#deny interfaces LAG <1-8> service <all/http/https/snmp/ssh/telnet><br>● <config-macl>#deny ip <A.B.C.D>/<A.B.C.D> interfaces 10GigabitEthernet <1-4> service <all/http/https/snmp/ssh/telnet><br>● <config-macl>#deny ip <A.B.C.D>/<A.B.C.D> interfaces 2.5GigabitEthernet <1-16> service <all/http/https/snmp/ssh/telnet><br>● <config-macl>#deny ip <A.B.C.D>/<A.B.C.D> interfaces LAG <1-8> service <all/http/https/snmp/ssh/telnet><br>● <config-macl>#deny ipv6 <X:X::X:X>/<0-128> interfaces 10GigabitEthernet <1-4> service <all/http/https/snmp/ssh/telnet><br>● <config-macl>#deny ipv6 <X:X::X:X>/<0-128> interfaces 2.5GigabitEthernet <1-16> service <all/http/https/snmp/ssh/telnet><br>● <config-macl>#deny ipv6 <X:X::X:X>/<0-128> interfaces LAG <1-8> service <all/http/https/snmp/ssh/telnet> |
| | Use the “do” command to run execution command in current mode.<br><SEQUENCE> -<br>Related Syntax:<br>● <config-macl>#do <SEQUENCE> |
| | Use the “end” command to finish current mode. Any changes in current mode will be saved.<br>Related Syntax:<br>● <config-macl>#end |
| | Use the “exit” command to close the current CLI session or return to the previous mode without saving the settings.<br>Related Syntax:<br>● <config-macl>#exit |
| | Use the “no sequence” command to delete any entry in |

| | |
|---|---|
| | management ACL.<br><1-65535>- Specify an index number of the ACL.<br>Related Syntax:<br>• <config-macl>#no sequence <1-65535> |
| | Use the “permit” command to add permit rules which bypass the packets meet the rule.<br>10GigabitEthernet <1-4> - Specify a physical port.<br>2.5GigabitEthernet <1-16> - Specify a physical port.<br>LAG <1-8> - Specify a LAG port.<br>service <all/http/https/snmp/ssh/telnet> - Specify the servcie type.<br>ip <A.B.C.D>/<A.B.C.D> - Specify the source IP address with mask for the packets.<br>ipv6 <X:X::X:X>/<0-128> - Specify the source IPv6 address and prefix length of the packet.<br>Related Syntax:<br>• <config-macl>#permit interfaces 10GigabitEthernet <1-4> service <all/http/https/snmp/ssh/telnet><br>• <config-macl>#permit interfaces 2.5GigabitEthernet <1-16> service <all/http/https/snmp/ssh/telnet><br>• <config-macl>#permit interfaces LAG <1-8> service <all/http/https/snmp/ssh/telnet><br>• <config-macl>#permit ip <A.B.C.D>/<A.B.C.D> interfaces 10GigabitEthernet <1-4> service <all/http/https/snmp/ssh/telnet><br>• <config-macl>#permit ip <A.B.C.D>/<A.B.C.D> interfaces 2.5GigabitEthernet <1-16> service <all/http/https/snmp/ssh/telnet><br>• <config-macl>#permit ip <A.B.C.D>/<A.B.C.D> interfaces LAG <1-8> service <all/http/https/snmp/ssh/telnet><br>• <config-macl>#permit ipv6 <X:X::X:X>/<0-128> interfaces 10GigabitEthernet <1-4> service <all/http/https/snmp/ssh/telnet><br>• <config-macl>#permit ipv6 <X:X::X:X>/<0-128> interfaces 2.5GigabitEthernet <1-16> service <all/http/https/snmp/ssh/telnet><br>• <config-macl>#permit ipv6 <X:X::X:X>/<0-128> interfaces LAG <1-8> service <all/http/https/snmp/ssh/telnet> |
| | Use the “sequence” command to deny or permit the ACL.<br><1-65535>- Specify an index number of the ACL.<br>10GigabitEthernet <1-4> - Specify a physical port.<br>2.5GigabitEthernet <1-16> - Specify a physical port.<br>LAG <1-8> - Specify a LAG port.<br>service <all/http/https/snmp/ssh/telnet> - Specify the servcie type.<br>ip <A.B.C.D>/<A.B.C.D> - Specify the source IP address with mask for the packets.<br>ipv6 <X:X::X:X>/<0-128> - Specify the source IPv6 address and prefix length of the packet. |

| | |
|---|---|
| | Related Syntax:<br>• <config-macl>#sequence <1-65535>deny interfaces 10GigabitEthernet <1-4> service <all/http/https/snmp/ssh/telnet><br>• <config-macl>#sequence <1-65535>deny interfaces 2.5GigabitEthernet <1-16> service <all/http/https/snmp/ssh/telnet><br>• <config-macl>#sequence <1-65535>deny interfaces LAG <1-8> service <all/http/https/snmp/ssh/telnet><br>• <config-macl>#sequence <1-65535>deny ip <A.B.C.D>/<A.B.C.D> interfaces 10GigabitEthernet <1-4> service <all/http/https/snmp/ssh/telnet><br>• <config-macl>#sequence <1-65535>deny ip <A.B.C.D>/<A.B.C.D> interfaces 2.5GigabitEthernet <1-16> service <all/http/https/snmp/ssh/telnet><br>• <config-macl>#sequence <1-65535>deny ip <A.B.C.D>/<A.B.C.D> interfaces LAG <1-8> service <all/http/https/snmp/ssh/telnet><br>• <config-macl>#sequence <1-65535>deny ipv6 <X:X::X:X>/<0-128> interfaces 10GigabitEthernet <1-4> service <all/http/https/snmp/ssh/telnet><br>• <config-macl>#sequence <1-65535>deny ipv6 <X:X::X:X>/<0-128> interfaces 2.5GigabitEthernet <1-16> service <all/http/https/snmp/ssh/telnet><br>• <config-macl>#sequence <1-65535>deny ipv6 <X:X::X:X>/<0-128> interfaces LAG <1-8> service <all/http/https/snmp/ssh/telnet><br>• <config-macl>#sequence <1-65535> permit 10GigabitEthernet <1-4> service <all/http/https/snmp/ssh/telnet><br>• <config-macl>#sequence <1-65535> permit 2.5GigabitEthernet <1-16> service <all/http/https/snmp/ssh/telnet><br>• <config-macl>#sequence <1-65535> permit interfaces LAG <1-8> service <all/http/https/snmp/ssh/telnet><br>• <config-macl>#sequence <1-65535> permit ip <A.B.C.D>/<A.B.C.D> interfaces 10GigabitEthernet <1-4> service <all/http/https/snmp/ssh/telnet><br>• <config-macl>#sequence <1-65535> permit ip <A.B.C.D>/<A.B.C.D> interfaces 2.5GigabitEthernet <1-16> service <all/http/https/snmp/ssh/telnet><br>• <config-macl>#sequence <1-65535> permit t ip <A.B.C.D>/<A.B.C.D> interfaces LAG <1-8> service <all/http/https/snmp/ssh/telnet><br>• <config-macl>#sequence <1-65535> permit ipv6 <X:X::X:X>/<0-128> interfaces 10GigabitEthernet <1-4> service <all/http/https/snmp/ssh/telnet><br>• config-macl>#sequence <1-65535> permit ipv6 <X:X::X:X>/<0-128> interfaces 2.5GigabitEthernet <1-16> service <all/http/https/snmp/ssh/telnet><br>• <config-macl>#sequence <1-65535> permit <X:X::X:X>/<0-128> interfaces LAG <1-8> service |

| | |
|---|---|
| | <all/http/https/snmp/ssh/telnet> |
| management access-class | Specify an ACL as active access-list.<br><NAME> - Enter the name of the access list.<br>Related Syntax:<br>● <config># management access-class <NAME> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# management access-list CA_ACL
PQ2200xb(config-macl)# deny ip 192.168.2.56/255.255.255.0 interfaces gigabitethernet 3 service telnet
PQ2200xb(config-macl)#
PQ2200xb(config-macl)# deny ipv6 00:50::7f:3b/24
```

## Telnet Command: management-vlan

Use this command to set VLAN ID for management VLAN.

**Syntax Items**

management-vlan vlan

**Description**

| Syntax Items | Description |
|---|---|
| management-vlan vlan | Set the management VLAN ID.<br><1-4094>- Specify the VLAN ID number of management VLAN.<br>Related Syntax:<br>● <config># management-vlan vlan <1-4094> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# management-vlan vlan 200
VLAN 200: VLAN does not exist
PQ2200xb(config)#
```

## Telnet Command: mirror

Use this command to set the source / destination interface of a port mirror session.

**Syntax Items**

mirror session

**Description**

| Syntax Items | Description |
|---|---|
| mirror session | Set the destination/source interface of a port mirror session.<br><1-4> - Specify the mirror session ID number.<br>10GigabitEthernet <1-4> - Specify a physical port as the SPAN |

| | |
|---|---|
| | destination.<br>2.5GigabitEthernet <1-16> - Specify a physical port as the SPAN destination.<br>allow-ingress – Enable the ingress traffic forwarding.<br>Related Syntax:<br>● <config># mirror session <1-4> destination interface 10GigabitEthernet <1-4><br>● <config># mirror session <1-4> destination interface 2.5GigabitEthernet <1-16><br>● <config># mirror session <1-4> destination interface 10GigabitEthernet <1-4> allow-ingress<br>● <config># mirror session <1-4> destination interface 2.5GigabitEthernet <1-16> allow-ingress |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# mirror session 3 destination interface 10GigabitEthernet 3 allow
PQ2200xb(config)#
```

## Telnet Command: mvr

Use this command to enable MVR function and configure related settings.

**Syntax Items**

mvr

mvr group

mvr mode

mvr query-time

mvr vlan

**Description**

| Syntax Items | Description |
|---|---|
| mvr | Enable MVR function.<br>Related Syntax:<br>● <config># mvr |
| mvr group | Set MVR group address.<br><A.B.C.D> - Enter an IP address.<br><1-128> - Specify a number for contiguous series of IPv4 multicast address.<br>Related Syntax:<br>● <config># mvr group <A.B.C.D><1-128> |
| mvr mode | Set MVR mode as compatible or dynamic.<br><compatible> - The switch does not support IGMP dynamic joins on the source ports.<br><dynamic> - The switch supports MVR membership on the source ports.<br>Related Syntax: |

| | |
|---|---|
| | • <config># mvr mode <compatible/dynamic> |
| mvr query-time | Set query response time for MVR.<br><1-10> - Specify the response time (second).<br>Related Syntax:<br>• <config># mvr query-time <1-10> |
| mvr vlan | Set a VLAN ID for MVR.<br><1-4094> - Specify the existed static VLAN ID.<br>Related Syntax**:**<br>• <config># mvr vlan <1-4094> |

**Example**

```
PQ2200xb x# configure
PQ2200xb (config)#
PQ2200xb (config)#mvr group 192.168.2.33
The operation will delete the MVR VLAN groups include static MVR groups.Continue
? [yes/no]:y
Input Parameter Error
PQ2200xb (config)#
```

## Telnet Command: no

Use this command to disable specific command.

**Syntax Items**

no <command>

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# no port-security
PQ2200xb(config)#
```

## Telnet Command: openvpn

Use this command to enable/disable the OpenVPN tunnel.

**Syntax Items**

openvpn enable

openvpn disable

openvpn filename

**Description**

| Syntax Items | Description |
|---|---|
| enable | Enable the OpenVPN tunnel. |
| disable | Disable the OpenVPN tunnel. |
| filename | <NAME> - Define a name for OpenVPN configuration.<br>Related Syntax:<br>• <config># openvpn filename <NAME> |

**Example**

```
PQ2200xb# configure
PQ2200xb (config)#openvpn enable
killall: openvpn: no process killed
PQ2200xb(config)#
```

## Telnet Command: poe

Use this command configure settings for PoE device.

**Syntax Items**

poe mode

poe schedule

**Description**

| Syntax Items | Description |
|---|---|
| poe mode | auto - VigorSwitch determines the power watts for PoE device based on actual demand.<br>manual - VigorSwitch will supply actual power demand for the PoE device and reserved PD class power for the PoE device.<br>none - VigorSwitch does not supply any power for the PoE device.<br>Related Syntax:<br>• <config># poe mode auto<br>• <config># poe mode manual<br>• <config># poe mode none |
| poe schedule | Specify a schedule for PoE device.<br>global-enable - Enable the global setting.<br>index <1-24> - Specify the index number of the schedule profiles.<br>Related Syntax:<br>• <config># poe schedule global-enable<br>• <config># poe schedule index <1-24> |

**Example**

```
PQ2200xb(config)# poe mode auto
  <cr>
PQ2200xb(config)# poe mode auto
PQ2200xb(config)#
```

## Telnet Command: port-security

Use this command to enable the function of port security.

**Syntax Items**

port-security

**Example**

```
PQ2200xb# configure
PQ2200xb(config)# port-security
PQ2200xb(config)#
```

## Telnet Command: qos

Use this command to configure QoS settings.

**Syntax Items**

qos

qos map

qos queue

qos trust

**Description**

| Syntax Items | Description |
|---|---|
| qos | Enable the quality of service based on basic trust type to assign the queue for packets.<br>Related Syntax:<br>• <config># qos |
| qos map | map cos-queue - Set the CoS to queue map.<br>map dscp-queue - Set the DSCP to queue map.<br>map precedence-queue - Set the IP Precedence to queue map.<br>map queue-cos - Modify the queue to CoS map.<br>map queue-dscp - Modify the queue to DSCP map.<br>map queue-precedence - Modify the queue to IP precedence map.<br><1-8> - Specify the queue number for the following CoS values mapped.<br><1-8> - Specify the queue number to which the DSCP value shall correspond.<br><1-8> - Specify the queue number to which the IP precedence value shall correspond.<br><0-7> - Enter the cos value to which the queue ID shall correspond.<br><0-7> - Enter the DSCP value to which the queue ID shall correspond.<br><0-7> - Enter the IP precedence value to which the queue ID shall correspond.<br>Related Syntax:<br>• <config># qos map cos-queue SEQUENCE to <1-8><br>• <config># qos map dscp-queue SEQUENCE to <1-8><br>• <config># qos map precedence-queue SEQUENCE to <1-8><br>• <config># qos map queue-cos SEQUENCE to <0-7><br>• <config># qos map queue-dscp SEQUENCE to <0-7><br>• <config># qos map queue-precedence SEQUENCE to <0-7> |
| qos queue | queue strict-priority-num - Set the number of strict priority queue. |

| | |
|---|---|
| | queue weight SEQUENCE - Set the number of non-strict priority queue.<br><0-8> - Specify the queue number.<br><weight1-weight8> <1-127> - Specify a number (1~127) representing queue weight value.<br>Related Syntax:<br>● <config># qos queue strict-priority-num <0-8><br>● <config># qos queue weight SEQUENCE <weight1 – weight8> <1-127> |
| qos trust | Set the trust type, cos, for the device to judge the appropriate queue of the packets.<br>Related Syntax:<br>● <config># qos trust <cos/cos-dscp/ dscp/ip-precedence> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# qos map cos-queue SEQUENCE to 3
PQ2200xb(config)#
```

## Telnet Command: radius

Use this command to configure settings for RADIUS server.

**Syntax Items**

radius default-config

radius host

**Description**

| Syntax Items | Description |
|---|---|
| radius default-config | Key <RADIUSKEY> - Specify key string for RADIUS server.<br>Retransmit <1-10> - Specify the retransmit times (from 1 to 10) for RADIUS server.<br>Timeout <1-30> - Specify the time out value (from 1 to 30) for RADIUS server.<br>Related Syntax:<br>● <config># radius default-config key <RADIUSKEY><br>● <config># radius default-config key <RADIUSKEY> retransmit <1-10><br>● <config># radius default-config key <RADIUSKEY> retransmit <1-10> timeout <1-30><br>● <config># radius default-config retransmit <1-10><br>● <config># radius default-config retransmit <1-10> timeout <1-30><br>● <config># radius default-config timeout <1-30> |
| radius host | host <HOSTNAME> - Specify a domain name or IP address for RADIUS server host.<br>auth-port <0~65535> - Speicfy a UDP port number for RADIUS server. |

| | |
|---|---|
| | key <RADIUSKEY> - Specify key string for RADIUS server.<br>priority <0~65535> - Specify the priority for RADIUS server.<br>retransmit <1-10> - Specify the retransmit times (from 1 to 10) for RADIUS server.<br>timeout <1-30> - Specify the time out value (from 1 to 30) for RADIUS server.<br>type <802.1x / all / login> - Choose the usage type for 802.1X authentication, or login, or both 802.1X authentication and login of RADIUS type.<br>Related Syntax:<br>● <config># radius host <HOSTNAME> auth-port <0~65535><br>● <config># radius host <HOSTNAME> auth-port <0~65535> key <RADIUSKEY><br>● <config># radius host <HOSTNAME> auth-port <0~65535> key <RADIUSKEY> priority <0~65535><br>● <config># radius host <HOSTNAME> auth-port <0~65535> key <RADIUSKEY> priority <0~65535> retransmit <1-10><br>● <config># radius host <HOSTNAME> auth-port <0~65535> key <RADIUSKEY> priority <0~65535> retransmit <1-10> timeout <1-30> type <802.1x / all / login><br>● <config># radius host <HOSTNAME> key <RADIUSKEY><br>● <config># radius host <HOSTNAME> key <RADIUSKEY> priority <0~65535><br>● <config># radius host <HOSTNAME> key <RADIUSKEY> priority <0~65535> retransmit <1-10><br>● <config># radius host <HOSTNAME> key <RADIUSKEY> priority <0~65535> retransmit <1-10> timeout <1-30><br>● <config># radius host <HOSTNAME> key <RADIUSKEY> priority <0~65535> retransmit <1-10> timeout <1-30> type <802.1x / all / login><br>● <config># radius host <HOSTNAME> priority <0~65535><br>● <config># radius host <HOSTNAME> priority <0~65535> retransmit <1-10><br>● <config># radius host <HOSTNAME> priority <0~65535> retransmit <1-10> timeout <1-30><br>● <config># radius host <HOSTNAME> priority <0~65535> retransmit <1-10> timeout <1-30> type <802.1x / all / login><br>● <config># radius host <HOSTNAME> retransmit <1-10><br>● <config># radius host <HOSTNAME> retransmit <1-10> timeout <1-30><br>● <config># radius host <HOSTNAME> retransmit <1-10> timeout <1-30> type <802.1x / all / login><br>● <config># radius host <HOSTNAME> timeout <1-30><br>● <config># radius host <HOSTNAME> timeout <1-30> type <802.1x / all / login><br>● <config># radius host <HOSTNAME> type <802.1x / all / login> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# radius default-config key 123456789 retransmit 3 timeout 10
PQ2200xb(config)# radius host radius auth-port 3000
```

## Telnet Command: schedule

Use this command to set schedule.

**Syntax Items**

schedule index

**Description**

| Syntax Items | Description |
|---|---|
| schedule index | Specify an index number for configuring detailed settings of a schedule profile.<br><1-15> - Enter a number to select a schedule profile.<br><DESCRIPTION> - Give a brief description for such profile.<br>cycle-days - The action applied with the schedule will take place every few days.<br>monthly-date - The action applied with the schedule will take place in specified day within a month.<br>once - The action applied with the schedule will take place for one time.<br>weekdays - The action applied with the schedule will take place on a certain day within a week.<br><1-31> - Enter a number to make action repeat.<br><apr / aug / dec / feb /jan / jul / jun /jul / mar / may / nov / oct / sep > - Represent month of April, August, December, February, January, July, June, March, May, November, October, and September.<br><sun /mon /tue /wed / thu / fri / sat> - Represent Sunday, Monday, Tuesday, Wednesday, Thursday, Friday and Saturday.<br><1-31> - Enter a number as the start date within a month.<br><2000-2035> - Enter the number as the year of start date.<br><HH:MM> - Enter the hours and the miniutes.<br><on/off> - Enable (on) or disable (off) the action applied with such profile.<br>Related Syntax:<br>• <config># schedule index <1-15> description <DESCRIPTION><br>• <config># schedule index <1-15> how-often cycle-days <1-31> start-date <apr / aug / dec / feb /jan / jul / jun / mar / may / nov / oct / sep > <1-31> <2000-2035> start-time <HH:MM> duration <HH:MM> action <on/off><br>• <config># schedule index <1-15> how-often monthly-date <1-31> start-date <apr / aug / dec / feb /jan / jul / jun / mar / may / nov / oct / sep > <1-31> <2000-2035> start-time <HH:MM> duration <HH:MM> action <on/off><br>• <config># schedule index <1-15> how-often once |

| | |
|---|---|
| | start-date<apr / aug / dec / feb /jan / jul / jun / mar / may / nov / oct / sep > <1-31> <2000-2035> start-time <HH:MM> duration <HH:MM> action <on/off><br>• <config># schedule index <1-15> how-often weekdays <sun /mon /tue /wed / thu / fri / sat> start-date <apr / aug / dec / feb /jan / jul / jun / mar / may / nov / oct / sep > <1-31> <2000-2035> start-time <HH:MM> duration <HH:MM> action <on/off> |

**Example**

PQ2200xb# configure

PQ2200xb(config)#

PQ2200xb(config)# schedule index 1 how-often cycle-days 3 start-date jan 1 2019 start-time 08:01 duraton 17:30 action on

PQ2200xb(config)# schedule index 2 how-often weekdays sun start-date may 11 2019 start-time 02:10 duration 12:10 action on

PQ2200xb(config)#

## Telnet Command: sflow

Use this command to configure sflow profile.

**Syntax Items**

sflow profile

**Description**

| Syntax Items | Description |
|---|---|
| sflow profile | profile <1-8> - Enter the ID number (1 to 8) of the profile.<br>rate <0-65535> - Set the sampling rate for the sFlow profile. 0 means to disable the sampling rate.<br>interval <0-65535> - Set the time interval for the sFlow profile.<br>collector <HOSTNAME> - Set the collector hostname.<br>data_sources interfaces 10GigabitEthernet <1-4> - Speicfy the LAN port.<br>data_sources interfaces 2.5GigabitEthernet <1-16> - Speicfy the LAN port.<br>port <0-65535> - Set the TCP/UDP port number for the profile.<br>Related Syntax:<br>• <config># sflow profile <1-8> rate <0-65535> interval <0-65535> collector <HOSTNAME> data_sources interfaces 10GigabitEthernet <1-4><br>• <config># sflow profile <1-8> rate <0-65535> interval <0-65535> collector <HOSTNAME> data_sources interfaces 2.5GigabitEthernet <1-16><br>• <config># sflow profile <1-8> rate <value> interval <0-65535> collector <HOSTNAME> port <0-65535> data_sources interfaces 10GigabitEthernet <1-4><br>• <config># sflow profile <1-8> rate <value> interval <0-65535> collector <HOSTNAME> port <0-65535> data_sources interfaces 2.5GigabitEthernet <1-16> |

**Example**

PQ2200xb # configure

PQ2200xb(config)#

PQ2200xb(config)# sflow profile 3 rate 2558 interval 9600 collector sHost port 1000 data_source interfaces 10GigabitEthernet 2

DNS resolution failed. Please check DNS server setting or host name

PQ2200xb(config)#

PQ2200xbconfig)# sflow profile 3 rate 2558 interval 9600 collector sHost data_sources interfaces 10GigabitEthernet 2

PQ2200xb(config)#

## Telnet Command: snmp

Use this command to define SNMP community.

**Syntax Items**

snmp community

snmp engineid

snmp group

snmp host

snmp trap

snmp user

snmp view

**Description**

| Syntax Items | Description |
|---|---|
| snmp community | snmp community - Set community name for SNMP v1 and v2, and access group name.<br>Available parameters for SNMP community:<br><NAME> after community - Enter a string (maximum length: 20 characters) as community name.<br><NAME> after group - Enter a string (maximum length: 30 characters) as access group.<br>ro - Set the community as read only.<br>rw - Set the community as read and write.<br>Related Syntax:<br>• <config># snmp community <NAME> group <NAME><br>• <config># snmp community <NAME> ro<br>• <config># snmp community <NAME> rw<br>• <config># snmp community <NAME> view <NAME> ro<br>• <config># snmp community <NAME> view <NAME> rw |
| snmp engineid | snmp engineid - Set the remote host for SNMP engine.<br>default - Reset to default setting of engine ID for SNMP server.<br><ENGINEID> - Such number must be 10 ~ 64 hexadecimal.<br><A.B.C.D> - Enter the IP address of the remote SNMP server.<br><HOSTNAME> - Enter the host name of the remote SNMP server. |

| | |
|---|---|
| | <X:X::X:X> - Enter the IPv6 address for remote SNMP server.<br>Related Syntax:<br>• <config># snmp engineid <ENGINEID><br>• <config># snmp engineid default<br>• <config># snmp engineid remote <A.B.C.D> <ENGINEID><br>• <config># snmp engineid remote <HOSTNAME> <ENGINEID><br>• <config># snmp engineid remote <X:X::X:X><ENGINEID> |
| snmp group | snmp group - Set the SNMP group.<br><NAME> - Specify the name of SNMP group.<br>version <1/2c/3> - Specify the version of SNMP service.<br><auth/noauth/priv> - Specify the packet authentication mode. “auth” means to perform packet authentication without encryption. It is applicable for SNMPv3 only. “noauth” means no packet authentication performed. “priv” means to perform packet authentication with encryption and also it is applicable for SNMPv3 only.<br>read-view <NAME> - Set the view name to enable agent configuration.<br>notify-view <NAME> - Set the view name to send only trap included in SNMP view for notification.<br>write-view <NAME> - Set the view name to enable viewing.<br>Related Syntax:<br>• <config># snmp group <NAME> version <1/2c/3> <auth/noauth/priv> read-view <NAME><br>• <config># snmp group <NAME> version <1/2c/3> <auth/noauth/priv> read-view <NAME> notify-view <NAME><br>• <config># snmp group <NAME> version <1/2c/3> <auth/noauth/priv> read-view <NAME> notify-view <NAME> write-view <NAME> |
| snmp host | snmp host - Set a host to receive SNMP notifications.<br><A.B.C.D> - Enter the IPv4/IPv6 address or host name of the receipt.<br>version <1/2c/3> - Specify the version of SNMP service.<br><NAME> - Set the community name sent with the notification.<br>udp-port <1-65535> - Set the UDP port number.<br>timeout <1-300> - Set the timeout of V2c informs.<br>retries <1-255> - Enter the retry counter of V2c informs.<br>Related Syntax:<br>Set a host to receive SNMP notifications.<br>• <config># snmp host <A.B.C.D> <NAME> retries <1-255><br>• <config># snmp host <A.B.C.D> <NAME> timeout <1-300> retries <1-255><br>• <config># snmp host <A.B.C.D> <NAME> udp-port <1-65535> retries <1-255><br>• <config># snmp host <A.B.C.D> <NAME> udp-port <1-65535> timeout <1-300> |

| | |
|---|---|
| | Set a host to receive SNMP notifications. Notification type is informs.<br>• <config># snmp host <A.B.C.D> informs <NAME> retries <1-255><br>• <config># snmp host <A.B.C.D> informs <NAME> timeout <1-300><br>• <config># snmp host <A.B.C.D> informs <NAME> timeout <1-300> retries <1-255><br>• <config># snmp host <A.B.C.D> informs <NAME> udp-port <1-65535><br>• <config># snmp host <A.B.C.D> informs <NAME> udp-port <1-65535> retries <1-255><br>• <config># snmp host <A.B.C.D> informs <NAME> udp-port <1-65535> timeout <1-300><br>• <config># snmp host <A.B.C.D> informs <NAME> udp-port <1-65535> timeout <1-300> retries <1-255><br>• <config># snmp host <A.B.C.D> informs version <1/2c/3><br>• <config># snmp host <A.B.C.D> informs version <1/2c/3><NAME> retries <1-255><br>• <config># snmp host <A.B.C.D> informs version <1/2c/3><NAME> timeout <1-300><br>• <config># snmp host <A.B.C.D> informs version <1/2c/3><NAME> timeout <1-300> retries <1-255><br>• <config># snmp host <A.B.C.D> informs version <1/2c/3><NAME> udp-port <1-65535><br>• <config># snmp host <A.B.C.D> informs version <1/2c/3><NAME> udp-port <1-65535> retries <1-255><br>• <config># snmp host <A.B.C.D> informs version <1/2c/3><NAME> udp-port <1-65535> timeout <1-300><br>• <config># snmp host <A.B.C.D> informs version <1/2c/3><NAME> udp-port <1-65535> timeout <1-300> retries <1-255> |
| | Set a host to receive SNMP notifications. Notification type is traps.<br>• <config># snmp host <A.B.C.D> traps <NAME><br>• <config># snmp host <A.B.C.D> traps <NAME> retries <1-255><br>• <config># snmp host <A.B.C.D> traps <NAME> timeout <1-300><br>• <config># snmp host <A.B.C.D> traps <NAME> timeout <1-300> retries <1-255><br>• <config># snmp host <A.B.C.D> traps version <1/2c/3><NAME> retries <1-255><br>• <config># snmp host <A.B.C.D> traps version <1/2c/3><NAME> timeout <1-300> retries <1-255><br>• <config># snmp host <A.B.C.D> traps version <1/2c/3><NAME> udp-port <1-65535><br>• <config># snmp host <A.B.C.D> traps version <1/2c/3><NAME> udp-port <1-65535> retries <1-255> |

| | |
|---|---|
| | • <config># snmp host <A.B.C.D> traps version <1/2c/3><NAME> udp-port <1-65535> timeout <1-300><br>• <config># snmp host <A.B.C.D> traps version <1/2c/3><NAME> udp-port <1-65535> timeout <1-300> retries <1-255><br>• <config># snmp host <A.B.C.D> version <1/2c/3><NAME> retries <1-255><br>• <config># snmp host <A.B.C.D> version <1/2c/3><NAME> timeout <1-300><br>• <config># snmp host <A.B.C.D> version <1/2c/3><NAME> timeout <1-300> retries <1-255><br>• <config># snmp host <A.B.C.D> version <1/2c/3><NAME> udp-port <1-65535><br>• <config># snmp host <A.B.C.D> version <1/2c/3><NAME> udp-port <1-65535> retries <1-255><br>• <config># snmp host <A.B.C.D> version <1/2c/3><NAME> udp-port <1-65535> timeout <1-300><br>• <config>#snmp host <A.B.C.D> version <1/2c/3><NAME> udp-port <1-65535> timeout <1-300> retries <1-255> |
| | • <config># snmp host HOSTNAME <NAME><br>• <config># snmp host HOSTNAME <NAME> retries <1-255><br>• <config># snmp host HOSTNAME <NAME> timeout <1-300><br>• <config># snmp host HOSTNAME <NAME> timeout <1-300> retries <1-255><br>• <config># snmp host HOSTNAME <NAME> udp-port <1-65535><br>• <config># snmp host HOSTNAME <NAME> udp-port <1-65535> retries <1-255><br>• <config># snmp host HOSTNAME <NAME> udp-port <1-65535> timeout <1-300><br>• <config># snmp host HOSTNAME <NAME> udp-port <1-65535> timeout <1-300> retries <1-255><br>• <config># snmp host HOSTNAME informs <NAME><br>• <config># snmp host HOSTNAME informs <NAME> retries <1-255><br>• <config># snmp host HOSTNAME informs <NAME> timeout <1-300><br>• <config># snmp host HOSTNAME informs <NAME> retries <1-255> timeout <1-300> retries <1-255><br>• <config># snmp host HOSTNAME informs <NAME> udp-port <1-65535><br>• <config># snmp host HOSTNAME informs <NAME> udp-port <1-65535> retries <1-255><br>• <config># snmp host HOSTNAME informs <NAME> udp-port <1-65535> timeout <1-300><br>• <config># snmp host HOSTNAME informs <NAME> udp-port <1-65535> timeout <1-300> retries <1-255><br>• <config># snmp host HOSTNAME traps <NAME><br>• <config># snmp host HOSTNAME traps <NAME> retries |

| | |
|---|---|
| | <1-255><br>• <config># snmp host HOSTNAME traps <NAME> timeout <1-300><br>• <config># snmp host HOSTNAME traps <NAME> timeout <1-300> retries <1-255><br>• <config># snmp host HOSTNAME traps <NAME> udp-port <1-65535><br>• <config># snmp host HOSTNAME traps <NAME> udp-port <1-65535> retries <1-255><br>• <config># snmp host HOSTNAME traps <NAME> udp-port <1-65535> timeout <1-300><br>• <config># snmp host HOSTNAME traps <NAME> udp-port <1-65535> timeout <1-300> retries <1-255><br>• <config># snmp host HOSTNAME traps version <1/2c/3> <NAME> retries <1-255><br>• <config># snmp host HOSTNAME traps version <1/2c/3> <NAME> timeout <1-300><br>• <config># snmp host HOSTNAME traps version <1/2c/3> <NAME> timeout <1-300> retries <1-255><br>• <config># snmp host HOSTNAME traps version <1/2c/3> <NAME> udp-port <1-65535><br>• <config># snmp host HOSTNAME traps version <1/2c/3> <NAME> udp-port <1-65535> retries <1-255><br>• <config># snmp host HOSTNAME traps version <1/2c/3> <NAME> udp-port <1-65535> timeout <1-300><br>• <config># snmp host HOSTNAME traps version <1/2c/3> <NAME> udp-port <1-65535> timeout <1-300> retries <1-255><br>• <config># snmp host HOSTNAME version <1/2c/3> <NAME><br>• <config># snmp host HOSTNAME version <1/2c/3> <NAME> retries <1-255><br>• <config># snmp host HOSTNAME version <1/2c/3> <NAME> timeout <1-300><br>• <config># snmp host HOSTNAME version <1/2c/3> <NAME> timeout <1-300> retries <1-255><br>• <config># snmp host HOSTNAME version <1/2c/3> <NAME> udp-port <1-65535><br>• <config># snmp host HOSTNAME version <1/2c/3> <NAME> udp-port <1-65535> retries <1-255><br>• <config># snmp host HOSTNAME version <1/2c/3> <NAME> udp-port <1-65535> timeout <1-300><br>• <config># snmp host HOSTNAME version <1/2c/3> <NAME> udp-port <1-65535> timeout <1-300> retries <1-255> |
| | • <config># snmp host <X:X::X:X> <NAME><br>• <config># snmp host <X:X::X:X> <NAME> retries <1-255><br>• <config># snmp host <X:X::X:X> <NAME> retries <1-255> timeout <1-300><br>• <config># snmp host <X:X::X:X> <NAME> retries <1-255> |

| | |
|---|---|
| | timeout <1-300> retries <1-255><br>• <config># snmp host <X:X::X:X> <NAME> udp-port <1-65535><br>• <config># snmp host <X:X::X:X> <NAME> udp-port <1-65535> retries <1-255><br>• <config># snmp host <X:X::X:X> <NAME> udp-port <1-65535> timeout <1-300><br>• <config># snmp host <X:X::X:X> <NAME> udp-port <1-65535> timeout <1-300> retries <1-255><br>• <config># snmp host <X:X::X:X> informs <NAME><br>• <config># snmp host <X:X::X:X> informs <NAME> retries <1-255><br>• <config># snmp host <X:X::X:X> informs <NAME> timeout <1-300><br>• <config># snmp host <X:X::X:X>informs <NAME> retries <1-255> timeout <1-300> retries <1-255><br>• <config># snmp host <X:X::X:X> informs <NAME> udp-port <1-65535><br>• <config># snmp host <X:X::X:X> informs <NAME> udp-port <1-65535> retries <1-255><br>• <config># snmp host <X:X::X:X> informs <NAME> udp-port <1-65535> timeout <1-300><br>• <config># snmp host <X:X::X:X> informs <NAME> udp-port <1-65535> timeout <1-300> retries <1-255><br>• <config># snmp host <X:X::X:X> traps <NAME><br>• <config># snmp host <X:X::X:X> traps <NAME> retries <1-255><br>• <config># snmp host <X:X::X:X> traps <NAME> timeout <1-300><br>• <config># snmp host <X:X::X:X> traps <NAME> timeout <1-300> retries <1-255><br>• <config># snmp host <X:X::X:X> traps <NAME> udp-port <1-65535><br>• <config># snmp host <X:X::X:X> traps <NAME> udp-port <1-65535> retries <1-255><br>• <config># snmp host <X:X::X:X> traps <NAME> udp-port <1-65535> timeout <1-300><br>• <config># snmp host <X:X::X:X> traps <NAME> udp-port <1-65535> timeout <1-300> retries <1-255><br>• <config># snmp host <X:X::X:X> version <1/2c/3> <NAME><br>• <config># snmp host <X:X::X:X> version <1/2c/3> <NAME> retries <1-255><br>• <config># snmp host <X:X::X:X> version <1/2c/3> <NAME> timeout <1-300><br>• <config># snmp host <X:X::X:X> version <1/2c/3> <NAME> timeout <1-300> retries <1-255><br>• <config># snmp host <X:X::X:X> version <1/2c/3> <NAME> udp-port <1-65535> |

| | |
|---|---|
| | • <config># snmp host <X:X::X:X> version <1/2c/3> <NAME> udp-port <1-65535> retries <1-255><br>• <config># snmp host <X:X::X:X> version <1/2c/3> <NAME> udp-port <1-65535> timeout <1-300><br>• <config># snmp host <X:X::X:X> version <1/2c/3> <NAME> udp-port <1-65535> timeout <1-300> retries <1-255> |
| snmp trap | snmp trap - Send the SNMP traps.<br>auth – Enable the SNMP authentication failure trap.<br>cold-start – Enable the SNMP cold startup failure trap.<br>linkUpDown – Enable the SNMP link up and down failure trap.<br>wort-security – Enable the SNMP port security trap.<br>Warm-start – Enable the SNMP warm startup failure trap.<br>Related Syntax:<br>• <config># snmp trap <auth / cold-start / linkUpDown / port-security / warm-start> |
| snmp user | snmp user - Set SNMP user account.<br><username> - Specify a name of SNMP user.<br><groupNAME> - Sepcify a name of SNMP group.<br>auth <md5/sha> - Specify the authentication mode, md5 or sha.<br><AUTHPASSWD> - Enter the password for the md5/sha mode.<br>Pri <PRIVPASSWD> - Enter a password as a privacy key.<br>Related Syntax:<br>• <config># snmp user <username> <groupNAME><br>• <config># snmp user <username> <groupNAME> auth <md5/sha> <AUTHPASSWD><br>• <config># snmp user <username> <groupNAME> auth <md5/sha> <AUTHPASSWD> priv <PRIVPASSWD> |
| snmp view | snmp view - Set the SNMP view.<br><NAME> - Enter the SNMP view name.<br>Subtree <OID> - Specify the ASN.1 subtree object identifier (OID).<br>oid-mask <mask/all> - Speicfy the OID mask, or use all for all masks.<br>viewtype <exluded/included> - Let the selected MIBs include or exclude in the SNMP view.<br>Related Syntax:<br>• <config># snmp view <NAME> subtree <OID> oid-mask <mask> viewtype <excluded/included> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# snmp engineid remote 192.168.2.38 00036D001188
PQ2200xb(config)# snmp engineid remote 00:50::16:88 00036D002288
PQ2200xb(config)# snmp host 192.168.2.89 CAR_community udp-port 1500 timeout 200
PQ2200xb(config)# snmp host 192.168.2.88 informs version 2c CAR_community udp-port 3000
```

```
timeout 180 retries 35
PQ2200xb(config)# snmp host 192.168.2.88 traps version 2c CAR_traps udp-port 6500 timeout 60 retries 2
PQ2200xb(config)# snmp host 192.168.2.88 version 2c CAR_version udp-port 3000 timeout 60 retries 2
PQ2200xb(config)# snmp host HOSTNAME CAR_host udp-port 3000 timeout 60 retries
PQ2200xb(config)# snmp host HOSTNAME informs HA_informs udp-port 3000 timeout 60 retries 2
PQ2200xb(config)# snmp host HOSTNAME version 2c HT_verstion udp-port 3000 timeout 60 retries 2
PQ2200xb(config)# snmp user CA_user_1 CA_group_1 auth md5 CA12345678 priv PR12345678
PQ2200xb(config)# snmp view CAR_community subtree 10 oid-mask 9 viewtype included
PQ2200xb(config)#
```

## Telnet Command: sntp

Use this command to configure settings for remote SNTP server.

**Syntax Items**

sntp host

**Description**

| Syntax Items | Description |
|---|---|
| sntp host | Set the remote SNTP server by specifying IP address or hostname.<br><HOSTNAME> - Enter the IP address or hostname of SNTP server.<br><1-65535> - Specify the port number for the SNTP server.<br>Related Syntax:<br>• <config># sntp host <HOSTNAME><br>• <config># sntp host <HOSTNAME>> port <1-65535> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# sntp host KEY1245 port 3000
PQ2200xb(config)#
```

## Telnet Command: spanning-tree

Use this command to configure settings for spanning-tree.

**Syntax Items**

spanning-tree

spanning-tree bpdu

spanning-tree forward-delay

spanning-tree hello-time

spanning-tree maximum-age

spanning-tree mode

spanning-tree pathcost

spanning-tree priority

spanning-tree tx-hold-count

**Description**

| Syntax Items | Description |
|---|---|
| spanning-tree | Enable the function of spanning-tree.<br>Related Syntax:<br>● <config># spanning-tree |
| spanning-tree bpdu | Filter/flood the BPDU packets.<br><filtering> - Packets will be filtered when STP is disabled on specified interface.<br><flooding> - Packets will be flooded to all interfaces with STP disabled and flooding mode.<br>Related Syntax:<br>● <config># spanning-tree bpdu<filtering/flooding> |
| spanning-tree forward-delay | Set the STP forward delay time.<br><4-30> - Default value is 15 (seconds).<br>Related Syntax:<br>● <config># spanning-tree forward-delay <4-30> |
| spanning-tree hello-time | Set the hello time interval to broadcast the message to other bridges.<br><1-10> - Default value is 2 (seconds).<br>Related Syntax:<br>● <config># spanning-tree hello-time <1-10> |
| spanning-tree maximum-age | Set the time interval for VigorSwitch to wait without receiving the configuration message.<br><6-40> - Default value is 20 (seconds).<br>Related Syntax:<br>● <config># spanning-tree maximum-age <6-40> |
| spanning-tree mode | <mstp/rstp/stp> - Specify the operation mode for spanning tree, such as multiple spanning tree (MSTP), rapid spanning tree (RSTP) or spanning tree (STP).<br>Related Syntax:<br>● <config># spanning-tree mode <mstp/rstp/stp> |
| spanning-tree pathcost | Set the path-cost method for spanning tree.<br><long/short> - Long means the path cost ranging from 1 to 200000000; short means the path cost ranging from 1 to 65535.<br>Related Syntax:<br>● <config># spanning-tree pathcost method <long/short> |
| spanning-tree priority | Set the priority for the specified instance ID.<br><0-61440> - The number must be multiple of 4096.<br>Related Syntax:<br>● <config># spanning-tree priority <0-61440> |

| | |
|---|---|
| spanning-tree tx-hold-count | Set the maximum number of packets transmission per second.<br><1-10> - Valid range is from 1 to 10.<br>Related Syntax:<br>● <config># spanning-tree tx-hold-count <1-10> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# spanning-tree forward-delay 20
PQ2200xb(config)#
PQ2200xb(config)# spanning-tree maximum-age 38
PQ2200xb(config)#
PQ2200xb(config)# spanning-tree tx-hold-count 3
PQ2200xb(config)#
```

## Telnet Command: start-up

Use this command to restart ICP status after rebooting VigorSwitch.

**Syntax Items**

start-up icp

**Description**

| Syntax Items | Description |
|---|---|
| start-up icp | Related Syntax:<br>● <config># start-up icp enable |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# start-up icp enable
PQ2200xb(config)#
```

## Telnet Command: storm-control

Use this command to configure settings for Storm Control.

**Syntax Items**

storm-control ifg exclude

storm-control ifg include

storm-control unit bps

storm-control unit pps

**Description**

| Syntax Items | Description |
|---|---|
| storm-control ifg exclude | Exclude the preamble and IFG (inter frame gap) into the calculating.<br>Related Syntax: |

| | |
|---|---|
| | • <config># storm-control ifg exclude |
| storm-control ifg include | Include the preamble and IFG (inter frame gap) into the calculating.<br>Related Syntax:<br>• <config># storm-control ifg include |
| storm-control unit bps | Change the unit of calculating method for storm-control.<br>bps – Calculate the storm control rate by octet-based.<br>Related Syntax:<br>• <config># storm-control unit bps |
| storm-control unit pps | Change the unit of calculating method for storm-control.<br>pps – Calculate the storm control rate by packet-based.<br>Related Syntax:<br>• <config># storm-control unit pps |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# storm-control ifg exclude
PQ2200xb(config)#
PQ2200xb(config)# storm-control unit bps
PQ2200xb(config)#
```

## Telnet Command: surveillance-vlan

Use this command to configure settings for surveillance-VLAN.

**Syntax Items**

surveillance-vlan
surveillance-vlan aging-time
surveillance-vlan cos
surveillance-vlan oui-table
surveillance-vlan vlan

**Description**

| Syntax Items | Description |
|---|---|
| surveillance-vlan | Enable the function of surveillance VLAN on VigorSwitch.<br>Related Syntax:<br>• <config># surveillance-vlan |
| surveillance-vlan aging-time | Set the aging time for surveillance VLAN.<br><30-65536> - Enter a value as aging time.<br>Related Syntax:<br>• <config># surveillance-vlan aging-time <30-65536> |
| surveillance-vlan cos | Set the class of service (0~7) for surveillance VLAN.<br><0-7>- Enter a number.<br>Related Syntax:<br>• <config># surveillance-vlan cos <0-7> remark |

| | |
|---|---|
| surveillance-vlan oui-table | Enable OUI surveillance VLAN configuration for specified interface.<br><A:B:C> - Enter the OUI address (e.g., 00:50:12).<br><DESCRIPTION> - Enter a string to briefly explain the surveillance VLAN.<br>Related Syntax:<br>● <config># surveillance-vlan oui-table <A:B:C> <DESCRIPTION> |
| surveillance-vlan vlan | Specify a VLAN profile as surveillance VLAN.<br><2-4094> - Specify the surveillance VLAN ID.<br>Related Syntax:<br>● <config># surveillance-vlan vlan <2-4094> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)#
PQ2200xb(config)# surveillance-vlan aging-time 60
PQ2200xb(config)#
PQ2200xb(config)# surveillance-vlan oui-table 00:50:12 fortestonly
PQ2200xb(config)#
```

## Telnet Command: system

Use this command to modify the contact information of VigorSwitch.

**Syntax Items**

system contact

system location

system name

**Description**

| Syntax Items | Description |
|---|---|
| system contact | <CONTACT> - Enter a string (maximum length: 256 characters).<br>Related Syntax:<br>● <config># system contact <CONTACT> |
| system location | <LOCATION> - Specify the location of the host.<br>Related Syntax:<br>● <config># system location <LOCATION> |
| system name | <NAME> - Change the name of the system. The default name is “PQ2200xb”.<br>Related Syntax:<br>● <config># system name <NAME> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
```

```
PQ2200xb(config)# system contact callMIS
PQ2200xb(config)#
PQ2200xb(config)# system location DrayTek
PQ2200xb(config)# system name UPDATEFRIM
UPDATEFRIM(config)#
```

## Telnet Command: tacacs

Use this command to configure TACACS+ server.

**Syntax Items**

tacacs default-config

tacacs host

**Description**

| Syntax Items | Description |
|---|---|
| tacacs default-config | Set the default parameters for the TACACS+ server.<br>Modify the default parameters of server key and timeout setting for the TACACS+ server.<br><TACPLUSKEY> - Enter a string as the TACACS+ server key.<br><1-30> - Enter a value as the TACACS+ server timeout.<br>Related Syntax:<br>● <config># tacacs default-config<br>● <config># tacacs default-config key <TACPLUSKEY><br>● <config># tacacs default-config key <TACPLUSKEY> timeout <1-30> |
| tacacs host | Set host name for the TACACS+ server or set host name, server key and priority for the TACACS+ server.<br><HOSTNAME> - Enter the host name of the TACACS+ server.<br><TACPLUSKEY> - Enter a string as the TACACS+ server key.<br><1-65535> - Enter a value as server priority in server group.<br><1-30> - Enter a timeout setting.<br>Related Syntax:<br>● <config># tacacs host <HOSTNAME><br>● <config># tacacs host <HOSTNAME> key <TACPLUSKEY><br>● <config># tacacs host <HOSTNAME> key <TACPLUSKEY> priority <1-65535><br>● <config># tacacs host <HOSTNAME> key <TACPLUSKEY> priority <0-65535> timeout <1-30> |

**Example**

```
PQ2200xb # configure
PQ2200xb(config)#
PQ2200xb(config)# tacacs default-config key tce00056 timeout 25
DNS resolution failed. Please check DNS server setting or host name
PQ2200xb(config)# tacacs host carrie02 key TA012345 priority 3000 timeout 10
PQ2200xb(config)#
```

## Telnet Command: tr069

Use this command to configure parameter settings of TR-069.

**Syntax Items**

tr069 acsPwd
tr069 acsUsername
tr069 acsurl
tr069 cpeEnable
tr069 cpePwd
tr069 cpeUsername
tr069 cpeport
tr069 healthlinkstatus
tr069 healthpoewarning
tr069 healthspeedstatus
tr069 periodicInfo
tr069 periodicTime
tr069 ssl
tr069 stun
tr069 stunMAXkeepalive
tr069 stunMINkeepalive
tr069 stunaddr
tr069 stunport
tr069 tls

**Description**

| Syntax Items | Description |
|---|---|
| tr069 acsPwd | <PASSWORD> - Enter the password used for registering to VigorACS server.<br>Related Syntax:<br>• <config># tr069 acsPwd<PASSWORD> |
| tr069 acsUsername | <NAME> - Enter the username used for registering to VigorACS server.<br>Related Syntax:<br>• <config># tr069 acsUsername<NAME> |
| tr069 acsurl | <ADDRESS> - Enter the URL for VigorACS server.<br>Related Syntax:<br>• <config># tr069 acsurl <ADDRESS> |
| tr069 cpeEnable | <disable/enable> - Enter Enable for VigorACS controlling such CPE through the Internet.<br>Related Syntax:<br>• <config># tr069 cpeEnable <disable/enable> |
| tr069 cpePwd | <PASSWORD> - Enter the password that VigorACS server can use it to authenticate and control the CPE device.<br>Related Syntax:<br>• <config># tr069 cpePwd <PASSWORD> |

| | |
|---|---|
| tr069 cpeUsername | <NAME> - Enter the username that VigorACS server can use it to authenticate and control the CPE device.<br>Related Syntax:<br>● <config># tr069 cpeUsername <NAME> |
| tr069 cpeport | <0-65535> - Enter the port number for CPE.<br>Related Syntax:<br>● <config># tr069 cpeport <0-65535> |
| tr069 healthlinkstatus | Perform the health check for the link status of specified interface(s).<br><PORTLIST> - Specify the interface, such as GE1, GE3-GE5 and so on.<br>Related Syntax:<br>● <config># tr069 healthlinkstatus <PORTLIST> |
| tr069 healthpoewarning | Perform the health check for PoE port warning status.<br><PORTLIST> - Specify the interface, such as GE1, GE3-GE5 and so on.<br>Related Syntax:<br>● <config># tr069 healthpoewarning <PORTLIST> |
| tr069 healthspeedstatus | Perform the health check for link speed status of specified interface(s).<br><PORTLIST> - Specify the interface, such as GE1, GE3-GE5 and so on.<br>Related Syntax:<br>● <config># tr069 healthspeedstatus <PORTLIST> |
| tr069 periodicInfo | <disable/enable> - Enter Enable to activate periodic information setting.<br>Related Syntax:<br>● <config># tr069 periodicInfo <disable/enable> |
| tr069 periodicTime | TIME Update the CPE information to VigorACS server.<br>Related Syntax:<br>● <config># tr069 periodicTime TIME |
| tr069 ssl | <disable/enable> - Enter Enable to enable CPE management protocol with SSL.<br>Related Syntax:<br>● <config># tr069 ssl <disable/enable> |
| tr069 stun | <disable/enable> - Enter Enable to enable CPE management protocol with STUN server.<br>Related Syntax:<br>● <config># tr069 stun <disable/enable> |
| tr069 stunMAXkeepalive | Set the maximum time period for CPE to send the binding request to VigorACS server.<br><0-65535> - Enter a number.<br>Related Syntax:<br>● <config># tr069 stunMAXkeepalive <0-65535> |
| tr069 stunMINkeepalive | Set the minimum time period for CPE to send the binding |

| | |
|---|---|
| | request to VigorACS server.<br><0-65535> - Enter a number.<br>Related Syntax:<br>• <config># tr069 stunMINkeepalive <0-65535> |
| tr069 stunaddr | <ADDRESS> - Enter the URL/IP address of STUN server.<br>Related Syntax:<br>• <config># tr069 stunaddr <ADDRESS> |
| tr069 stunport | <0-65535> - Set the port number for STUN server.<br>Related Syntax:<br>• <config># tr069 stunport <0-65535> |
| tr069 tls | Set TLS version (1.2 or 1.3).<br>Related Syntax:<br>• <config># tr069 tls version <tls1.2/tls1.3> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# tr069 stunaddr 192.168.3.99
PQ2200xb(config)#
```

## Telnet Command: udld

Use this command to set the time interval of UniDirectional Link Detection (UDLD) sent message.

**Syntax Items**

udld

**Description**

| Syntax Items | Description |
|---|---|
| udld message time | <1-90> - Specify a time interval (unit: second) for sending message.<br>Related Syntax:<br>• <config>#udld message time <1-90> |

**Example**

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# udld message time 35
PQ2200xb(config)#
```

## Telnet Command: username

Use this command to add a new user account or edit an existing user account.

**Syntax Items**

username

**Description**

| Syntax Items | Description |
| --- | --- |
| username | privilege - Set a user account with the privilege of admin, user or customized level.<br>secret - Set a user account with unencrypted password.<br>secret encrypted - Set a user account with encrypted password.<br><WORD> - Enter the name (0~32 characters) of the local user profile.<br><admin/ user> - Specify the privilege level to be admin (privilege 15) / user (privilege 1).<br><PASSWORD> - Enter a string as the password for the local user.<br>Related Syntax:<br>● <config># username <WORD> privilege <admin/user> secret <PASSWORD><br>● <config># username <WORD> secret <PASSWORD><br>● <config># username <WORD> secret encrypted <PASSWORD> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# username carrie_1 privilege admin secret md123456
PQ2200xb(config)#
PQ2200xb(config)# username carrie_1 secret encrypted ca123456
Old password: ********
PQ2200xb(config)#
```

## Telnet Command: vlan

Use this command to configure detailed settings for VLAN profile.

Before configuring, you have to access into next phase. See the following example:

```
PQ2200xb# configure
PQ2200xb(config)#
PQ2200xb(config)# vlan 3
PQ2200xb(config-vlan)#
```

**Syntax Items**

vlan vlan-list

vlan mac-vlan group

**Description**

| Syntax Items | Description |
| --- | --- |
| vlan vlan-list | Specify the index number of VLAN profile. To configure detailed settings, access into next level.<br><vlan-list> - The available range is 1 to 4094.<br><config># vlan 33 |

| | |
|---|---|
| | <config-vlan>#<br>Then, available sub-commands are:<br><config-vlan>#do<br><config-vlan>#end<br><config-vlan>#exit<br><config-vlan>#name |
| | Use the “do” command to run execution command in current mode.<br><SEQUENCE> -<br>Related Syntax:<br>● <config-vlan>#do <SEQUENCE> |
| | Use the “end” command to finish current mode. Any changes in current mode will be saved.<br>Related Syntax:<br>● <config-vlan>#end |
| | Use the “exit” command to close the current CLI session or return to the previous mode without saving the settings.<br>Related Syntax:<br>● <config-macl>#exit |
| | Use the “name” command to add a VLAN profile.<br><string> - Enter the name of the VLAN profile.<br>Related Syntax:<br>● <config-vlan>#name <string> |
| vlan mac-vlan group | Create a MAC-vlan group.<br><1-2147483647> - Specify a group ID.<br><A:B:C:D:E:F> - Enter the MAC address to be mapped.<br><9-48> - Enter a number representing the subnet mask.<br>Related Syntax:<br>● <config># vlan mac-vlan group <1-2147483647> <A:B:C:D:E:F> mask <9-48> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)# vlan 3
PQ2200xb(config-vlan)#
PQ2200xb(config-vlan)# name vlan_friends
PQ2200xb(config-vlan)#
…
PQ2200xb(config)# vlan mac-vlan group 33 00:50:17:22:12:ff mask 10
PQ2200xb(config)# vlan group 1 frame-type ethernet_ii protocol-value 0x0600
PQ2200xb(config)#
```

## Telnet Command: voice-vlan

Use this command to enable voice VLAN and configure settings for voice VLAN.

**Syntax Items**

voice-vlan aging-time

voice-vlan cos

voice-vlan oui-table

voice-vlan vlan

**Description**

| Syntax Items | Description |
|---|---|
| voice-vlan aging-time | Set the voice VLAN aging timeout interval.<br><30-65536> - The unit is minute. Default is 1440 (minutes).<br><string> - Enter the name of the VLAN profile.<br>Related Syntax:<br>● <config># voice-vlan aging-time <30-65536> |
| voice-vlan cos | Set the voice VLAN cos value and remark function.<br>Specify the class of service for voice VLAN.<br><0-7> - CoS value. Default is 6. Remark is disabled.<br>remark – L2 user priority is remarked with the CoS value.<br>Related Syntax:<br>● <config># voice-vlan cos <0-7> remark |
| voice-vlan oui-table | Add or remove the selected OUI to/from the OUI table. In default, there are 8 OUI addresses.<br><A:B:C> - Enter the OUI address.<br><DESCRIPTION> - Enter a brief description for the specified MAC address to the voice VLAN OUI table.<br>Related Syntax:<br>● <config># voice-vlan cos <0-7> remark |
| voice-vlan vlan | Set the VLAN identifier of the voice VLAN.<br><2-4094> - Enter the number of VLAN ID.<br>Related Syntax:<br>● <config># voice-vlan vlan <2-4094> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)# voice-vlan aging-time 1000
PQ2200xb(config)#
PQ2200xb(config)# voice-vlan oui-table 22:30:ff test_01
PQ2200xb(config)#
PQ2200xb(config)# voice-vlan oui-table 00:01:E2 STAMP
PQ2200xb(config)# exit
PQ2200xb# show voice-vlan interfaces gigabitEthernet 1
Voice VLAN Aging       : 1000 minutes
Voice VLAN CoS         : 6
Voice VLAN 1p Remark: disabled

OUI table
    OUI MAC       |     Description
```

```
--------------+-----------------
    00:E0:BB     | 3COM
    00:03:6B     | Cisco
    00:E0:75     | Veritel
    00:D0:1E     | Pingtel
    00:01:E3     | Siemens
    00:60:B9     | NEC/Philips
    00:0F:E2     | H3C
    00:09:6E     | Avaya
    22:30:FF     | test_01
    00:01:E2     | STAMP

   Port | State       | Port Mode     | Cos Mode
-------+----------+-------------+-----------
gi1       | Disabled |       Auto        | Src
PQ2200xb#
```

## Telnet Command: webhook

Use this command to enable or disable the webhook service.

**Syntax Items**

webhook active

webhook host

webhook interval

webhook keep

**Description**

| Syntax Items | Description |
|---|---|
| webhook active | <enable/disable> - Enable or disable the webhook application.<br>Related Syntax:<br>● <config># webhook active <enable/disable> |
| webhook host | Specify the destination (URL, domain name, IP address) to receive the data transferred by VigorSwitch.<br>ip <ADDRESS> - Enter the IP address of the destination.<br>path <PATH> - Enter the path string (part of the composition of the URL) of the destination.<br>port <number> - Enter a port number (1-65535).<br>service <http/https> - Specify the protocol (http or https) of the destination.<br>url <domain name> - Enter the domain name (e.g., draytek.com) of the destination. Note that it is not necessary to enter this information if IP address has been set first.<br>Related Syntax:<br>● <config># webhook host ip <ADDRESS><br>● <config># webhook host path <PATH><br>● <config># webhook host port <number> |

| | |
|---|---|
| | • <config># webhook host service <http/https><br>• <config># webhook host url <domain name> |
| webhook interval | <1-60> - Set the transmission interval (unit is minute).<br>Related Syntax:<br>• <config># webhook interval <1-60> |
| webhook keep | setings <enable/disable> - Enable or disable the function of keep webhook settings.<br>Related Syntax:<br>• <config># webhook keep setings <enable/disable> |

**Example**

```
PQ2200xb# configure
PQ2200xb(config)# webhook host service https
PQ2200xb(config)# webhook host url www.demo.com
PQ2200xb(config)# webhook host path Draytek/demo
PQ2200xb(config)# webhook host port 443
PQ2200xb(config)# webhook interval 2
```

## A-2-4 Copy Configuration

Use this command to upgrade firmware image, configuration file, syslog file, language file and security certificate.

**Syntax Items**

copy flash://

copy tftp://

copy startup-config

**Description**

| Syntax Items | Description |
|---|---|
| copy flash:// | Related Syntax:<br>• # copy flash:// flash://<br>• # copy flash:// tftp:// |
| copy startup-config | running-config - Copy the startup configuration file to the running configuration.<br>tftp://- Copy the startup configuration file to remote TFTP server with a filename.<br><IP address> - Enter the IP address of TFTP sever.<br><filename> - Create a name to save the configuration file.<br>Related Syntax:<br>• # copy startup-config tftp:// |
| copy tftp:// | running-config - Get the running configuration from specified TFTP server.<br>startup-config - Get the startup configuration from specified TFTP server.<br>Related Syntax: |

| | |
|---|---|
| | • # copy tftp:// flash://<br>• # copy tftp:// startup-config<br>• # copy tftp:// tftp:// |

**Example**

```
PQ2200xb# copy startup-config tftp://172.16.3.8/test_da.cfg
Uploading file. Please wait...
Save configuration done.
PQ2200xb#
```

## A-2-5 Delete Configuration

Use this command to delete a file from the FLASH file system or restore the factory default settings of VigorSwitch.

**Syntax Items**

delete flash:// startup-config

delete startup-config

**Description**

| Syntax Items | Description |
|---|---|
| delete flash://startup-config | Delete the startup configuration file in FLASH file system.<br>Related Syntax:<br>• # delete flash://startup-config |
| delete startup-config | Restore the factory default settings of VigorSwitch.<br>Related Syntax:<br>• # delete startup-config |

**Example**

```
PQ2200xb# delete flash://startup-config
Delete flash://startup-config [y/n] y
Do you want to reload the system to take effect? [y/n] y
…
```

## A-2-6 Disable Configuration

All commands used will be divided into EXEC mode and Privileged EXEC mode. This command is to turn off privileged mode command.

Default privilege level is 15 if no privilege level is specified on enable command.

Default privilege level is 1 if no privilege level is specified on disable command.

**Syntax Items**

disable

**Description**

| Syntax Items | Description |
|---|---|

| | |
|---|---|
| disable | Enter a number to specify the privilege level.<br>Related Syntax:<br>• # disable <1-14> |

**Example**

```
PQ2200xb# disable ?
<1-14>  Privilege level
<cr>
PQ2200xb# disable 3
PQ2200xb#
<1-14>  Privilege level
<cr>
PQ2200xb# disable 3
PQ2200xb#
```

## A-2-7 End Configuration

Use this command to end current mode.

**Syntax Items**

end

**Example**

```
PQ2200xb(config)# interface GigabitEthernet 3
PQ2200xb(config-if)# end
PQ2200xb#
```

## A-2-8 Exit Configuration

Use this command to close current CLI session or return to previous mode.

**Syntax Items**

exit

**Example**

```
PQ2200xb(config)# interface GigabitEthernet 3
PQ2200xb(config-if)# exit
PQ2200xb(config)#
```

## A-2-9 Hardware-Monitor Configuration

Use this command to execute the hardware fan test.

**Syntax Items**

hardware-monitor fan-test

**Example**

```
PQ2200xb# hardware-monitor fan-test
PQ2200xb#
```

## A-2-10 Ping Configuration

Use this command to send ICMP ECHO_REQUEST to network hosts.

**Syntax Items**

ping

**Description**

| Syntax Items | Description |
|---|---|
| ping | <HOSTNAME> - Enter an IPv4/IPv6 address or a domain name to ping.<br><1-999999999> - Specify the number of repetitions of ping operation.<br>Related Syntax:<br>● # ping <HOSTNAME><br>● # ping <HOSTNAME> count <1-999999999> |

**Example**

```
PQ2200xb# ping 192.168.1.11 count 3
PING 192.168.1.11 (192.168.1.11): 56 data bytes
64 bytes from 192.168.1.11: icmp_seq=0 ttl=64 time=0.0 ms
64 bytes from 192.168.1.11: icmp_seq=1 ttl=64 time=0.0 ms
64 bytes from 192.168.1.11: icmp_seq=2 ttl=64 time=0.0 ms
--- 192.168.1.11 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
PQ2200xb#
```

## A-2-11 Reboot Configuration

Use this command to perform a cold restart of VigorSwitch.

**Syntax Items**

reboot

**Example**

```
PQ2200xb# reboot
PQ2200xb#
```

## A-2-12 Renew Configuration

Use this command to renew DHCP Snooping database from backup file.

**Syntax Items**

renew ip dhcp snooping database

**Example**

```
PQ2200xb # renew ip dhcp snooping database
PQ2200xb #
```

## A-2-13 Restore-defaults Configuration

Use this command to restore the factory default settings for the system or for the selected port.

**Syntax Items**

restore-defaults

**Description**

| Syntax Items | Description |
|---|---|
| restore-defaults | <1-4> - Enter the number (1 to 4) of LAN port.<br><1-16> - Enter the number (1 to 16) of LAN port.<br><1-8> - Enter the number of LAG port.<br>Related Syntax:<br>• # restore-defaults<br>• # restore-defaults interfaces 10GigabitEthernet <1-4><br>• # restore-defaults interfaces 2.5GigabitEthernet <1-16><br>• # restore-defaults interfaces LAG <1-8> |

**Example**

```
PQ2200xb# restore-defaults interfaces 10gigabitethernet 3
Interface 10gi3: restore factory defaults.
PQ2200xb#
PQ2200xb# restore-default
System: restore factory defaults. Do you want to reboot now? (y/n)y
```

## A-2-14 Save Configuration

Use this command to save configuration and activate the settings.

Note that this command has the same effect as "copy running-config startup-config".

**Syntax Items**

save

**Example**

```
PQ2200xb# save
Success
PQ2200xb#
```

## A-2-15 Show Configuration

After finished the command setting, use this command to display the configuration for all commands.

**Syntax Items**

show <command>

**Example**

```
PQ2200xb# show acl utilization
Type: sys                                usage: 256
Type: IPSG                               usage: 128
Type: Auth                               usage: 128
PQ2200xb#
PQ2200xb#
PQ2200xb# show arp
Address              HWtype   HWaddress           Flags Mask            Iface
192.168.1.55         ether    00:1D:AA:F0:26:08   C                     eth0
192.168.1.10         ether    00:05:5D:E4:D8:EE   C                     eth0
PQ2200xb# show voice-vlan interfaces gigabitethernet 3
Voice VLAN Aging       : 1440 minutes
Voice VLAN CoS         : 6
Voice VLAN 1p Remark: disabled
OUI table
    OUI MAC       |     Description
--------------+-----------------
    00:E0:BB     | 3COM
    00:03:6B     | Cisco
    00:E0:75     | Veritel
    00:D0:1E     | Pingtel
    00:01:E3     | Siemens
    00:60:B9     | NEC/Philips
    00:0F:E2     | H3C
    00:09:6E     | Avaya

   Port | State       | Port Mode     | Cos Mode
-------+----------+-------------+-----------
gi3      | Disabled |       Auto        | Src
PQ2200xb#
```

# A-2-16 SSL Configuration

Use this command to generate security certificate files such as RSA, DSA.

After entering the command of SSL, follow the onscreen questions to give the required information.

**Syntax Items**

ssl

**Example**

```
PQ2200xb# ssl
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to '/mnt/ssh/ssl_key.pem_tmp'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a D
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:tw
State or Province Name (full name) [Some-State]:hs
Locality Name (eg, city) []:hschu
Organization Name (eg, company) [Internet Widgits Pty Ltd]:draytek
Organizational Unit Name (eg, section) []:marketing
Common Name (e.g. server FQDN or YOUR name) []:draytek
Email Address []:carrie_ni@draytek.com
PQ2200xb#
```

## A-2-17 Terminal Configuration

Use this command to set the maximum line number that the terminal is able to print.

**Syntax Items**

terminal

**Description**

| Syntax Items | Description |
|---|---|
| terminal | <0-24> - Enter the length value. 0 means no limit.<br>Related Syntax:<br>• # terminal length <0-24> |

**Example**

```
PQ2200xb# terminal length 15
PQ2200xb# show running-config
......
```

## A-2-18 Traceroute Configuration

Use this command to execute network trace route diagnostic.

**Syntax Items**

traceroute

**Description**

| Syntax Items | Description |
| --- | --- |
| traceroute | <HOSTNAME>- Enter the IP address or the hostname of the device for VigorSwitch to perform traceroute diagnostic.<br>Related Syntax:<br>● # traceroute <HOSTNAME> |

**Example**

```
PQ2200xb# traceroute 192.168.1.224
traceroute to 192.168.1.224 (192.168.1.224), 30 hops max, 40 byte packets
 1  192.168.1.224 (192.168.1.224)  0 ms  0 ms  0 ms
PQ2200xb#
```

## A-2-19 UDLD Configuration

Use this command to reset all interfaces disabled by the UniDirectional Link Detection (UDLD) and make data traffic begin passing through the interfaces again.

**Syntax Items**

traceroute

**Description**

| Syntax Items | Description |
| --- | --- |
| udld | Reset all the interfaces which have been shut down by UDLD.<br>Related Syntax:<br>● # udld reset |

**Example**

```
PQ2200xb # udld reset
PQ2200xb #
```