DrayTek

VigorSwitch P1282

Web Smart Managed Switch

User's Guide

V1.0

VigorSwitch P1282

Web Smart Managed

User's Guide

Version: 1.0

Firmware Version: V2.7.0

Date: April 27, 2022

Intellectual Property Rights (IPR) Information

Copyrights

Trademarks

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows 8, 10 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 +40 Celsius.
- Do not expose the switch to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.
- Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards.
- Keep the package out of reach of children.
- When you want to dispose of the modem, please follow local regulations on conservation of the environment.

Warranty

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

Be a Registered Owner

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

Firmware & Tools Updates

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

https://www.draytek.com

Table of Contents

Chapter I Introduction

I-1 Introduction

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

Thank you for purchasing VigorSwitch.

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

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

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

I-1-1 Key Features

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.

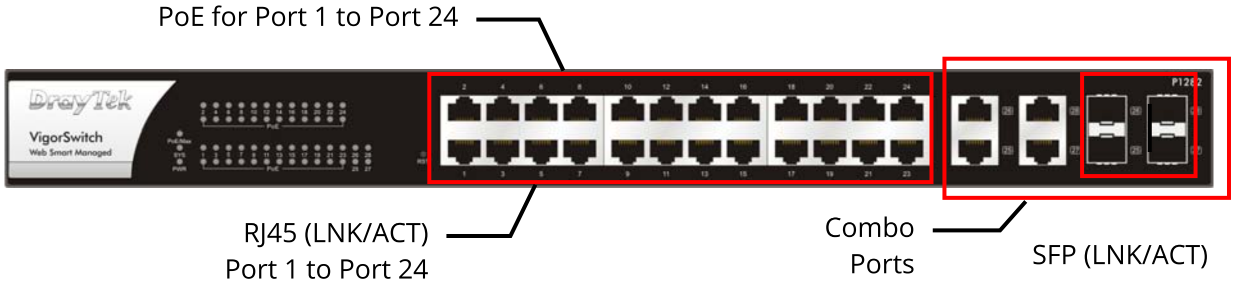
Port Trunking

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

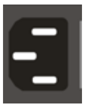
Power Saving

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
PoE/Max (for P1282)	On (Green)	Connected over the PoE maximum power budget.
	Off	Connected within the PoE maximum power budget.
SYS	On (Green)	The switch finishes system booting and the system is ready.
	Blinking (Green)	The switch is powered on and starts system booting.
	Off	The power is off or the system is not ready / malfunctioning.
PWR	On (Green)	The device is powered on and running normally.
	Off	The device is not ready or is failed.
PoE 1~24	On (Green)	The port is supplied with PoE power.
	Off	No PoE power is supplied on the port.
RJ45 (LNK/ACT) Port 1 ~ 24	On (Green)	The device is connected
	Blinking	The system is sending or receiving data through the port.
	Off	The port is disconnected or the link is failed.
Combo Ports 25 ~ 28 RJ45 / SFP (LNK/ACT)	On (Green)	The device is connected with 1000Mbps.
	On (Amber)	The device is connected with 10/100Mbps.
	Blinking	The system is sending or receiving data through the port.
	Off	The port is disconnected or the link is failed.

Interface	Description
RJ 45 LNK/ACT Port 1 ~ 24	Port 1 to Port 24 can be used for Ethernet connection and PoE connection, depending on the device connected.
PoE for Port 1 ~ 24	
SFP LNK/ACT Port 25 ~ 28	Port 25 to Port 28 are used for fiber connection.
	Power inlet for AC input (100~240V/AC, 50/60Hz).

Note

The following limitation is suitable for VigorSwitch P1282

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

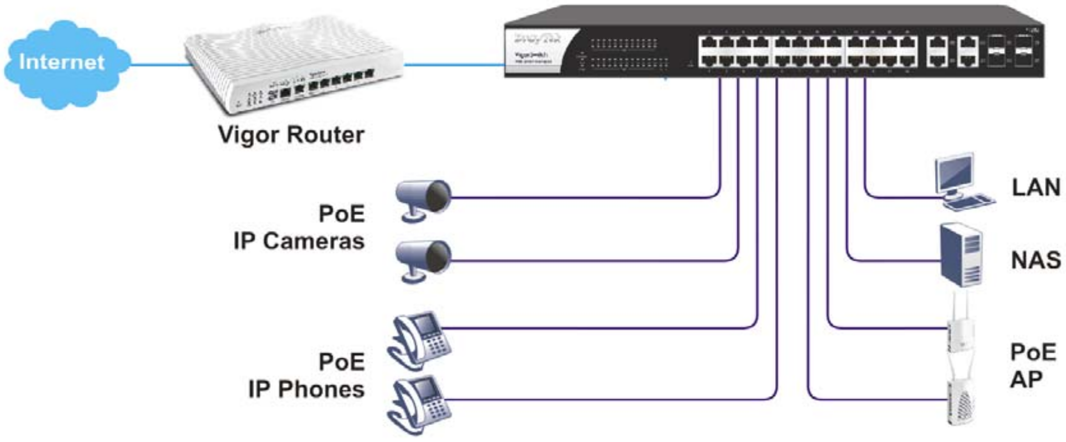
Before starting to configure the switch, you have to connect your devices correctly.

Note:

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

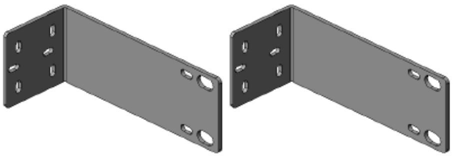
I-2-1 Network Connection

- 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.

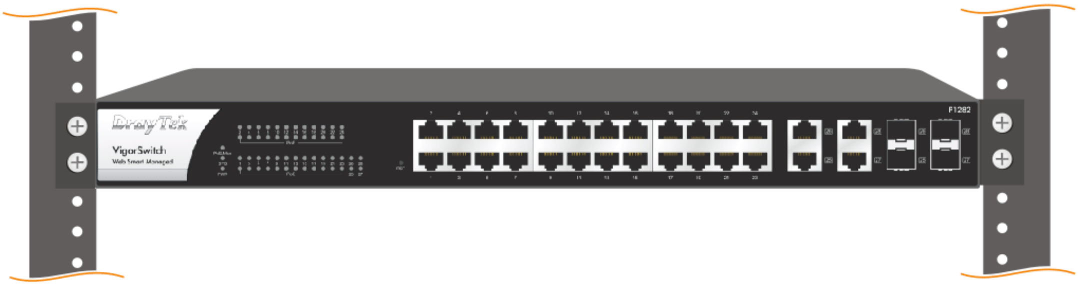


I-2-2 Rack-Mounted Installation

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.

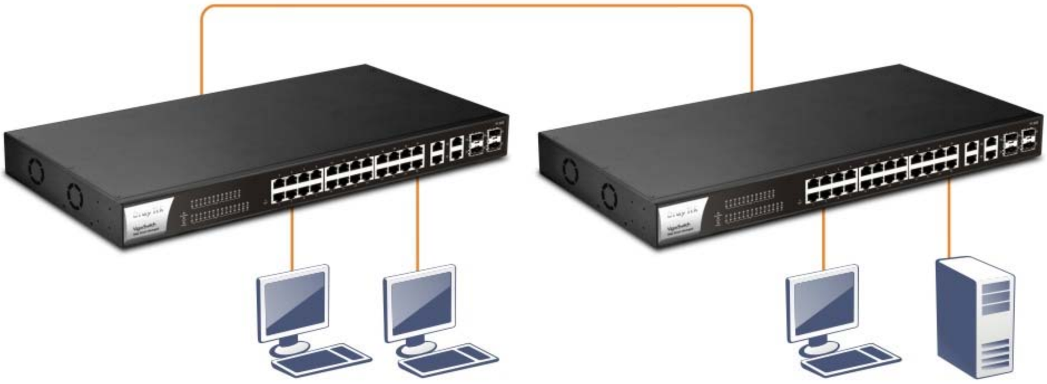


I-2-3 Typical Applications

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

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

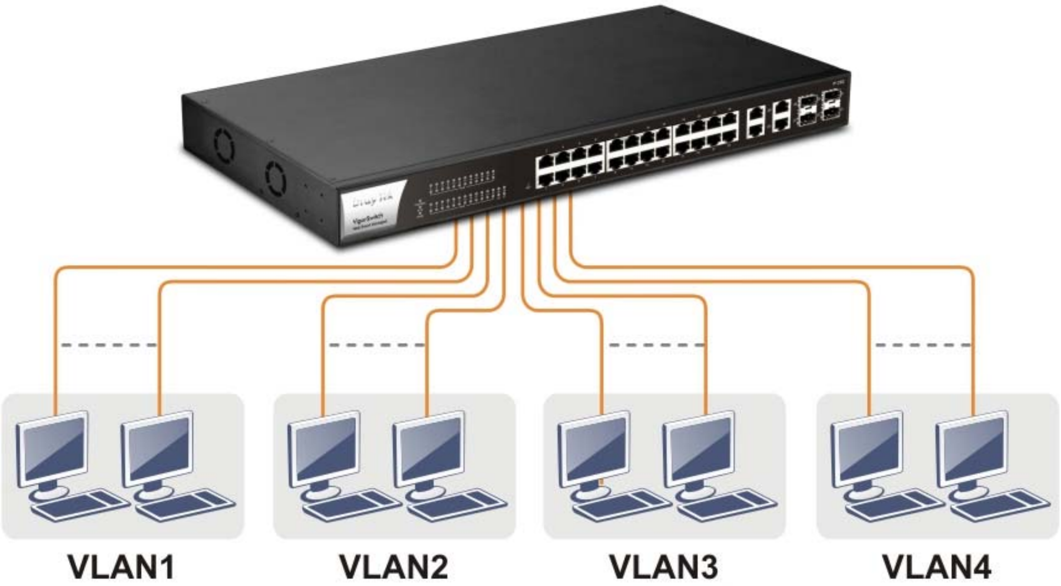
Every port can access each other. (*The switch image is sample only.)



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

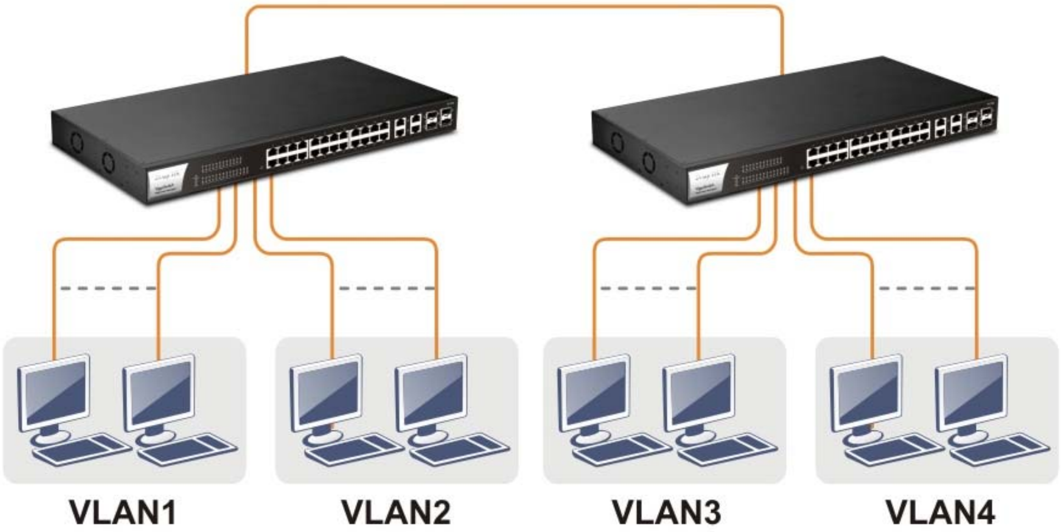
Here VLAN area is defined by what VLAN you are using. The switch supports both port-based VLAN and tag-based VLAN. They are different in practical deployment, especially in physical location. The following diagram shows how it works and what the difference they are.

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



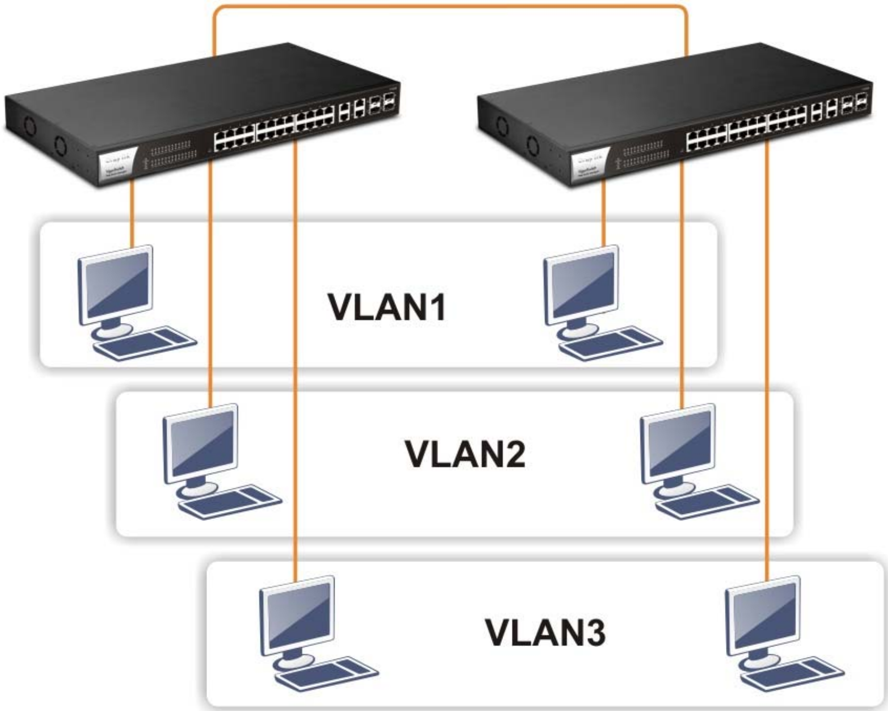
- The same VLAN members could not be in different switches.
- Every VLAN members could not access VLAN members each other.
- The switch manager has to assign different names for each VLAN groups at one switch.

Case 3: Port-based VLAN - 2



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

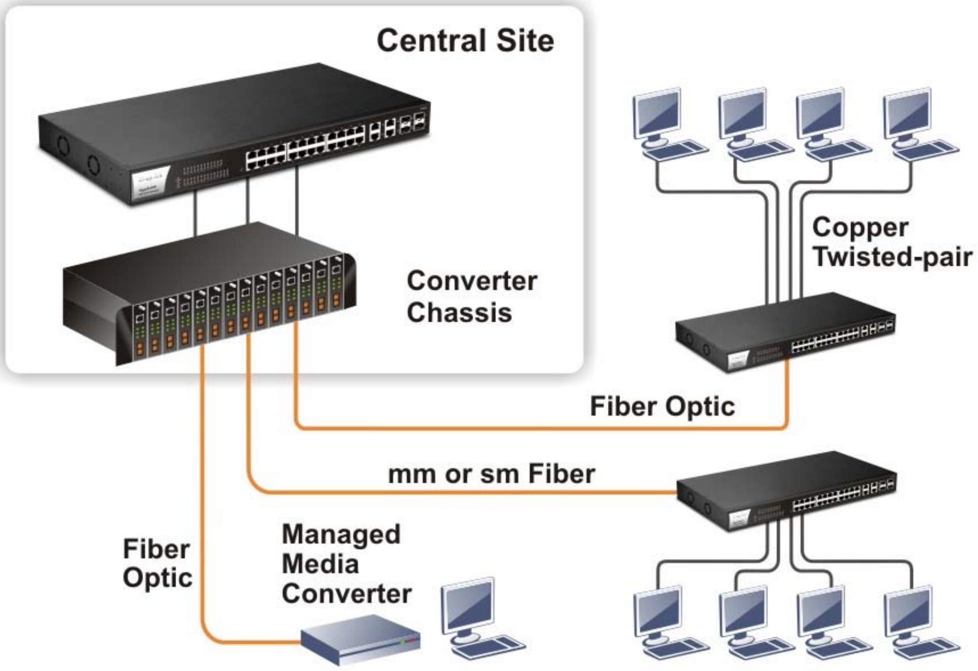
Case 4: The same VLAN members can be at different switches with the same VID



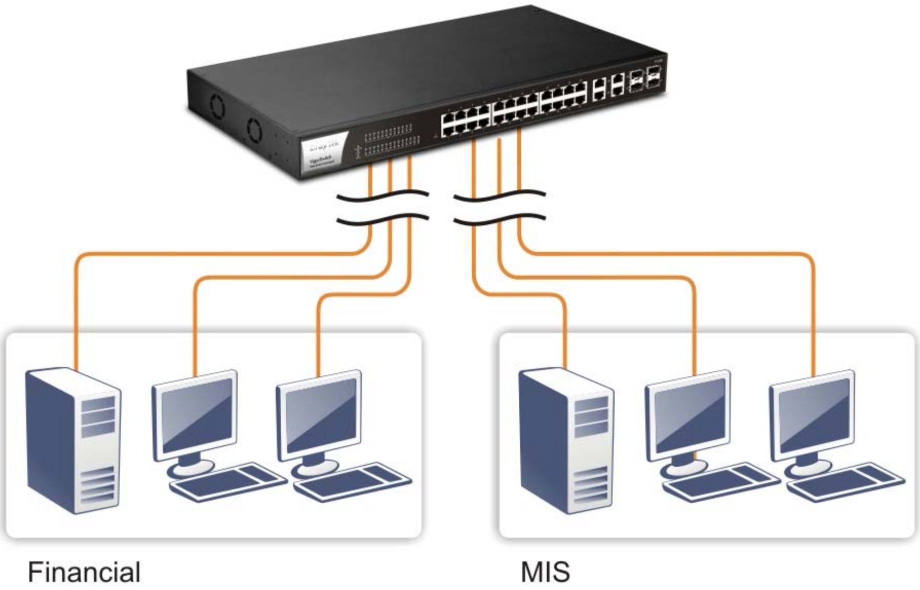
Case 5: Desktop Installation

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

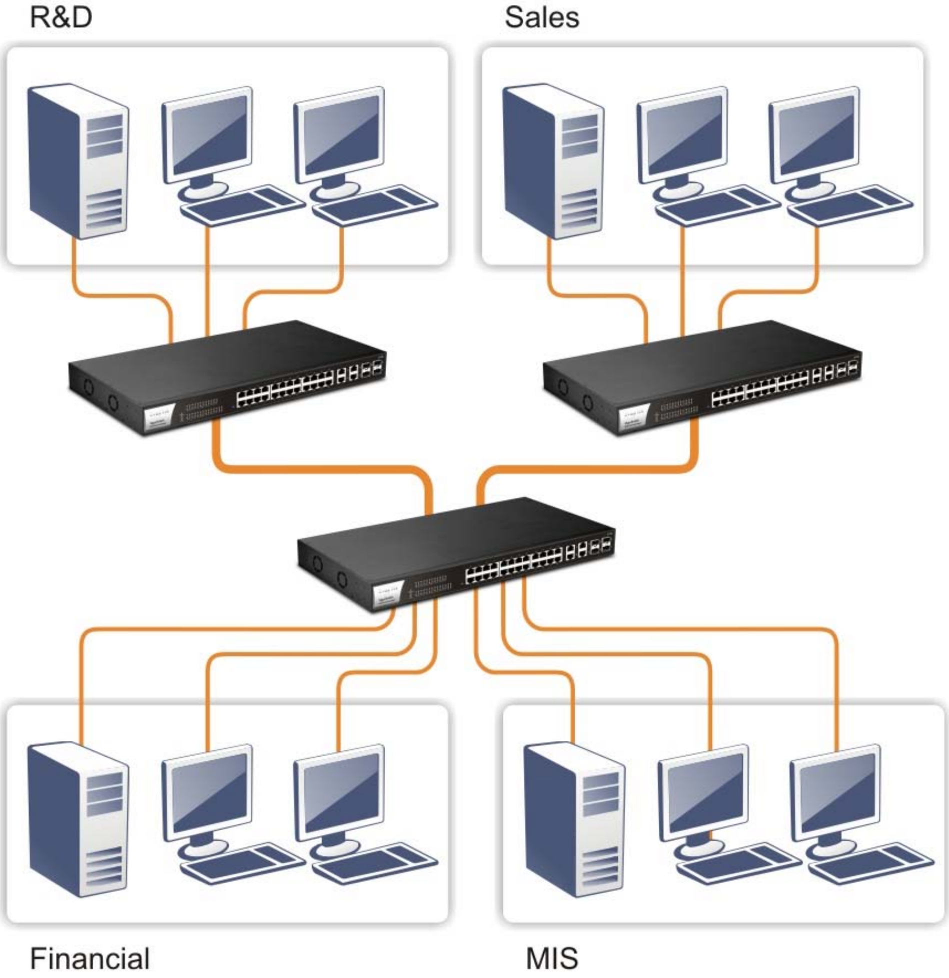
Case 6: Central Site/Remote site application is used in carrier or ISP



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



Case 8: Office network

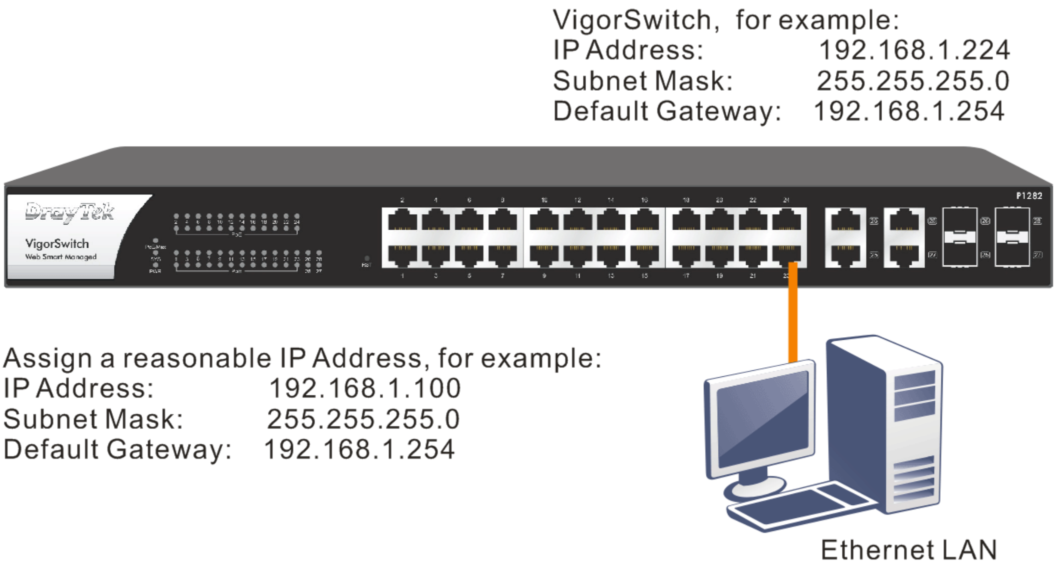


I-2-4 Configuring the Management Agent of Switch

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

Configuring the Management Agent of VigorSwitch P1282 through the Ethernet Port.

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



VigorSwitch, for example:
IP Address: 192.168.1.224
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.254
VigorSwitch
Web Smart Managed
P1282
Assign a reasonable IP Address, for example:
IP Address: 192.168.1.100
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.254
Ethernet LAN

I-2-5 Managing VigorSwitch P1282 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.

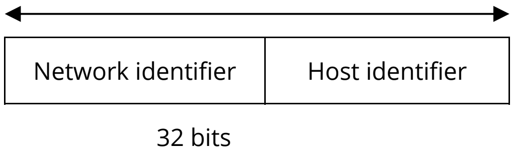
I-2-6 IP Address Assignment

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.

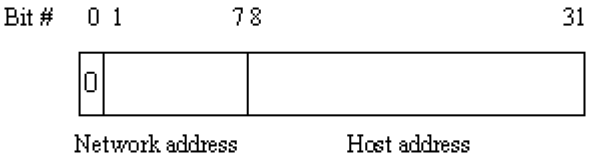
Each class has its own network range between the network identifier and host identifier in the 32 bits address. Each IP address comprises two parts: network identifier (address) and host identifier (address). The former indicates the network where the addressed host resides, and the latter indicates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



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.

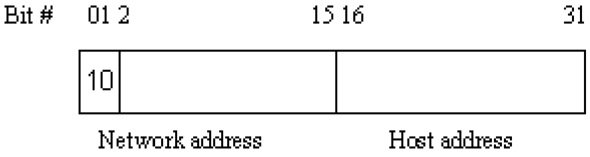
Class A:

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.



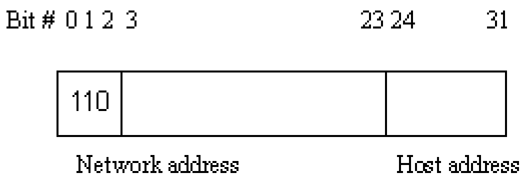
Class B:

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

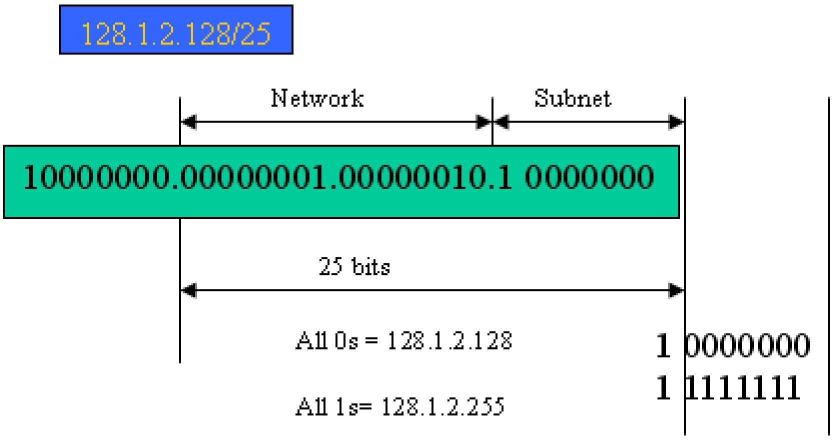
Please refer to RFC 1597 and RFC 1466 for more information.

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.

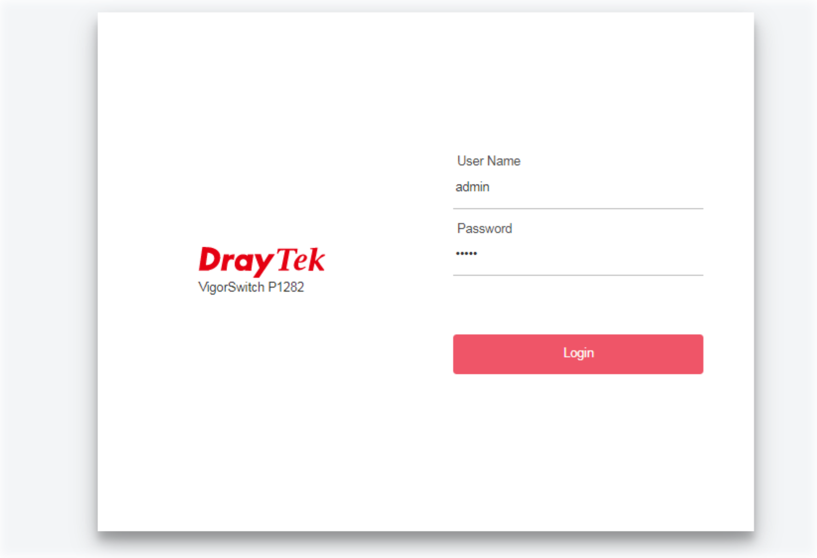
- First, IP Address: as shown above, enter “**192.168.1.224**”, for instance. For sure, an IP address such as 192.168.1.x must be set on your PC.
- Second, Subnet Mask: as shown above, enter “255.255.255.0”. Choose a subnet mask suitable for your network.

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

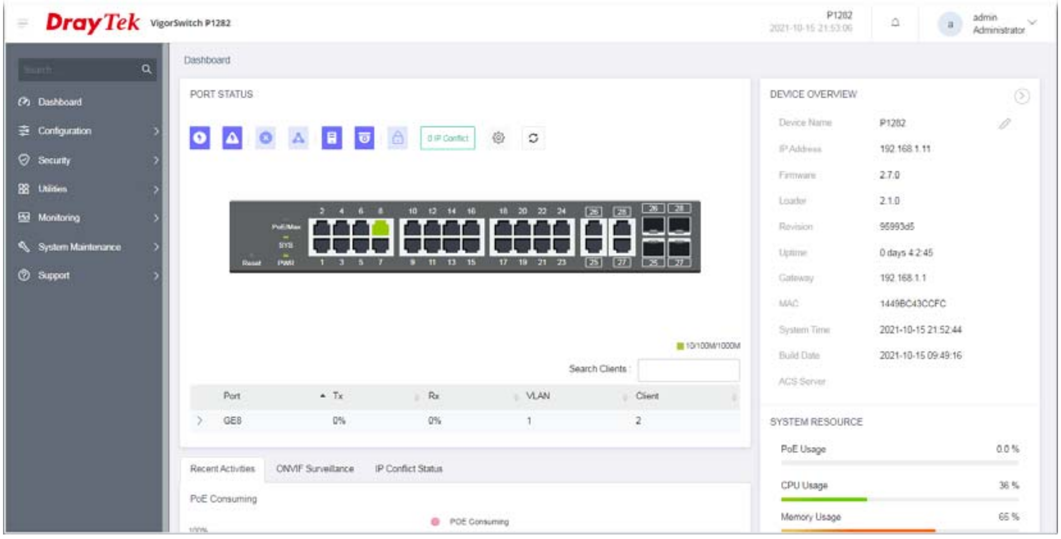
1. Open any browser (e.g., Firefox) and type “192.168.1.224” as URL.
2. Please enter “admin/admin” as the Username/Password and click **Login**.



User Name: admin

Password: •••••

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



Search Clients :

Port	Tx	Rx	VLAN	Client
GE8	0%	0%	1	2

DEVICE OVERVIEW

Device Name	P1282
IP Address	192.168.1.11
Firmware	2.7.0
Loader	2.1.0
Revision	95993d5
Uptime	0 days 4:2:45
Gateway	192.168.1.1
MAC	1449BC43CCFC
System Time	2021-10-15 21:52:44
Build Date	2021-10-15 09:49:16
ACS Server	

SYSTEM RESOURCE

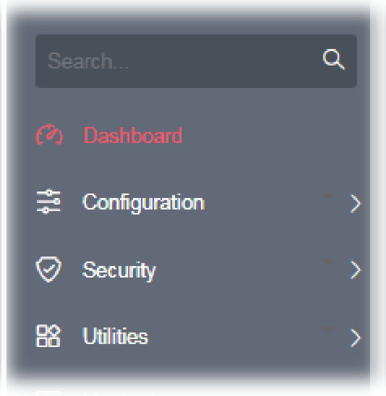
PoE Usage	0.0 %
CPU Usage	36 %
Memory Usage	65 %

Info:

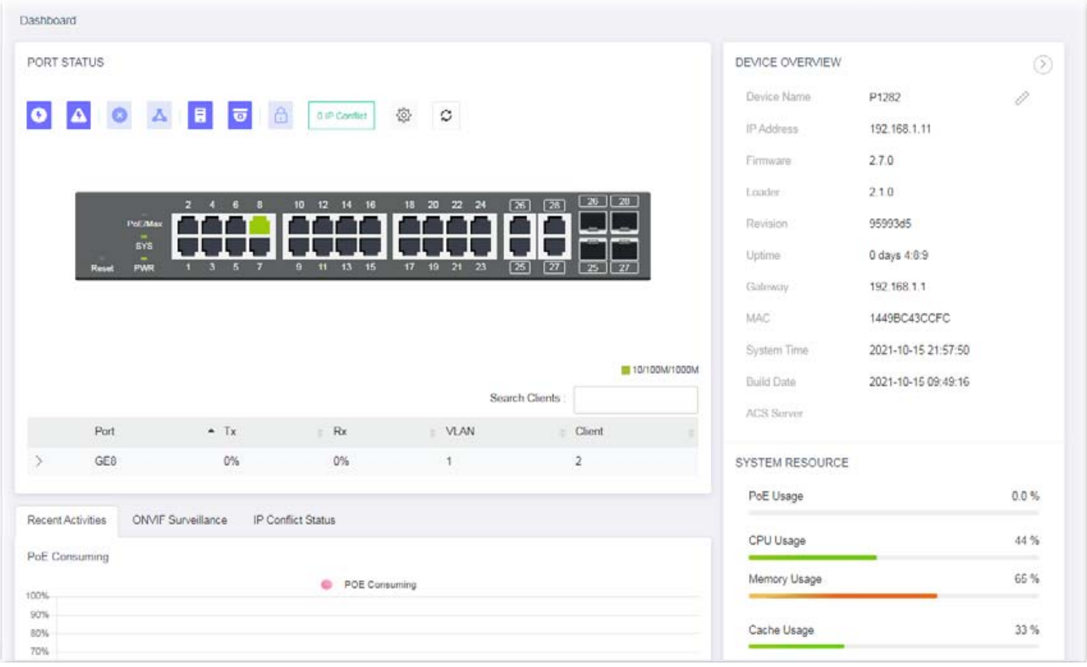
The DHCP Setting is enabled in default. Therefore, if a DHCP server presented on network connected to VigorSwitch, checking before accessing VigorSwitch is essential.

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:



	Port	Tx	Rx	VLAN	Client
>	GE8	0%	0%	1	2

Device Name	P1282
IP Address	192.168.1.11
Firmware	2.7.0
Loader	2.1.0
Revision	95993d5
Uptime	0 days 4:8:9
Gateway	192.168.1.1
MAC	1449BC43CCFC
System Time	2021-10-15 21:57:50
Build Date	2021-10-15 09:49:16
ACS Server	

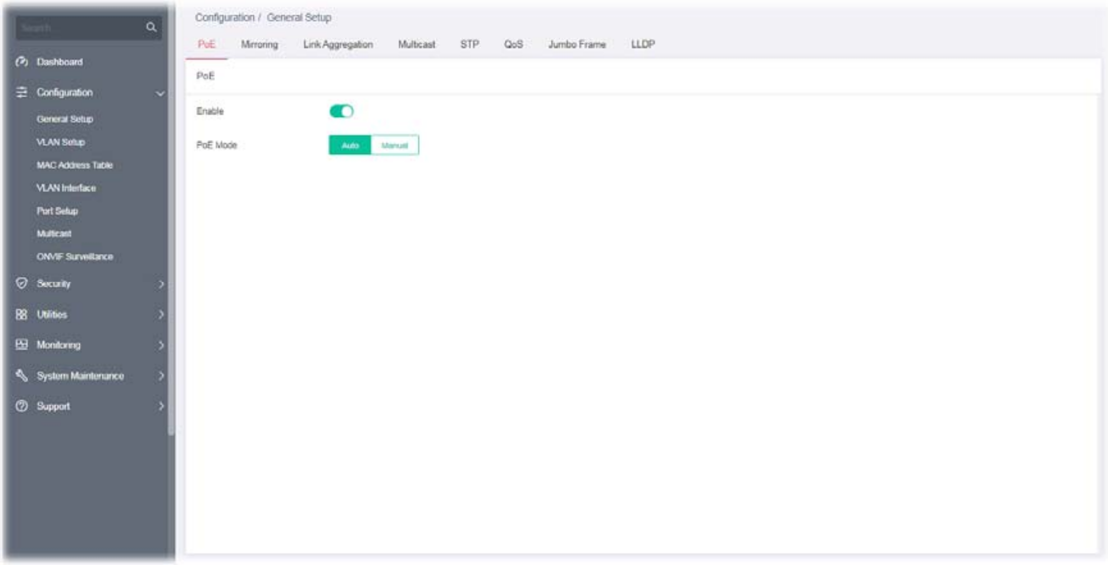
PoE Usage	0.0 %
CPU Usage	44 %
Memory Usage	65 %
Cache Usage	33 %

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.



Enable ●

PoE Mode [✓ Auto] Manual

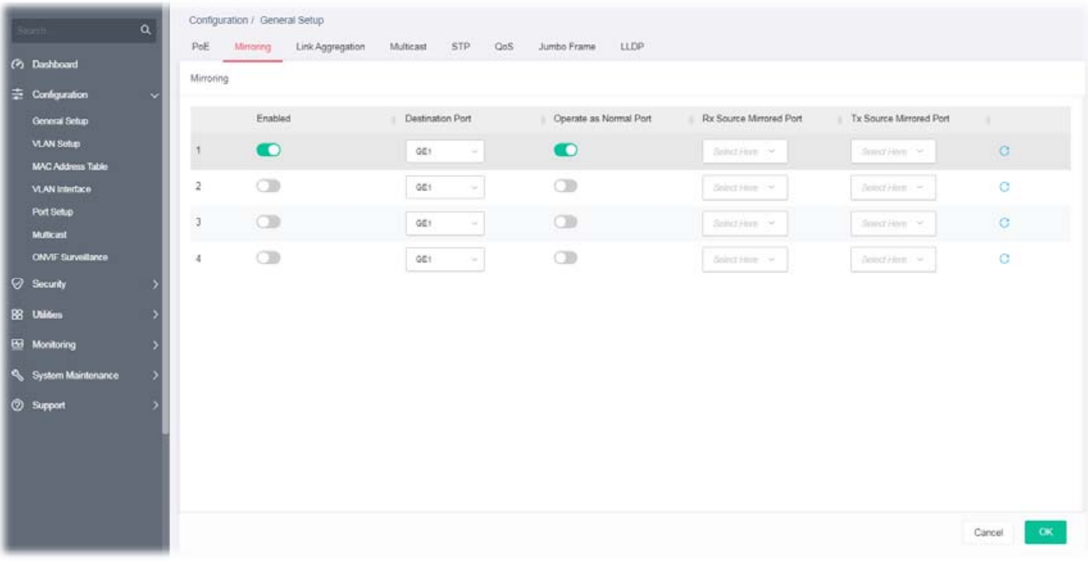
Available settings are explained as follows:

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

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

II-1-2 Mirroring

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



	Enabled	Destination Port	Operate as Normal Port	Rx Source Mirrored Port	Tx Source Mirrored Port	
1	●	GE1	●	Select Here	Select Here	↻
2	○	GE1	○	Select Here	Select Here	↻
3	○	GE1	○	Select Here	Select Here	↻
4	○	GE1	○	Select Here	Select Here	↻

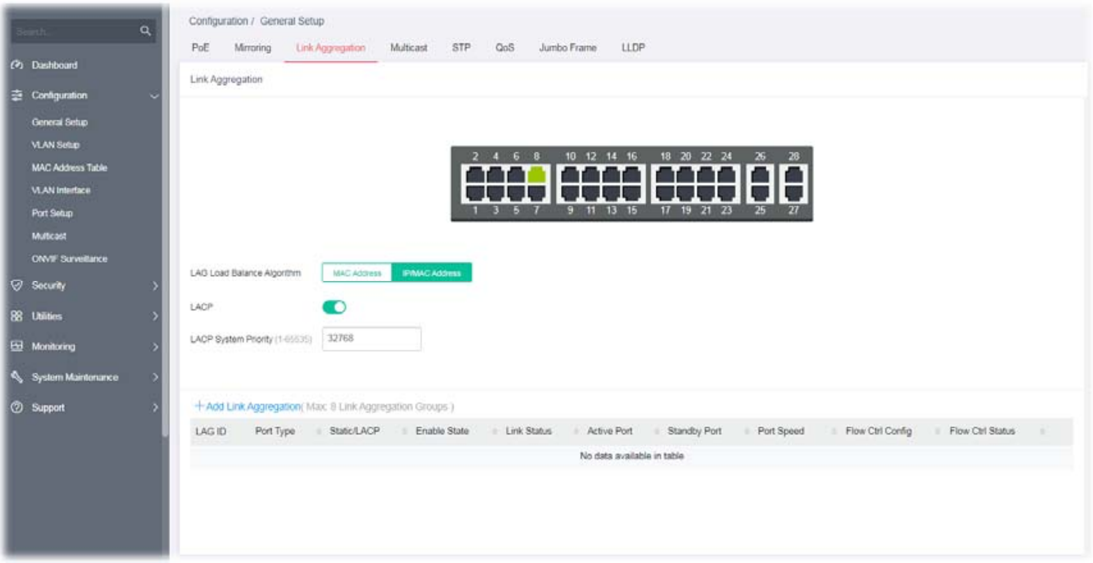
Available settings are explained as follows:

Item	Description
Enabled	**Enable / Disable** – Click the toggle to enable / disable this function. ● - means "Enable". ○ - means "Disable".
Destination Port	Specify the port where you wish to observe the mirrored packets.
Operate as Normal Port	**Enable / Disable** – Click the toggle to enable / disable this function. ● - means "Enable". ○ - means "Disable".
Rx/Tx Source Mirrored Port	Select the port(s) which you wish to mirror the traffic, Rx for mirror the packets into the port, Tx for mirror the packets going out from the port.
↻	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.



Link Aggregation

LAG Load Balance Algorithm: MAC Address [✓ IP/MAC Address]

LACP: ●

LACP System Priority (1-65535): 32768

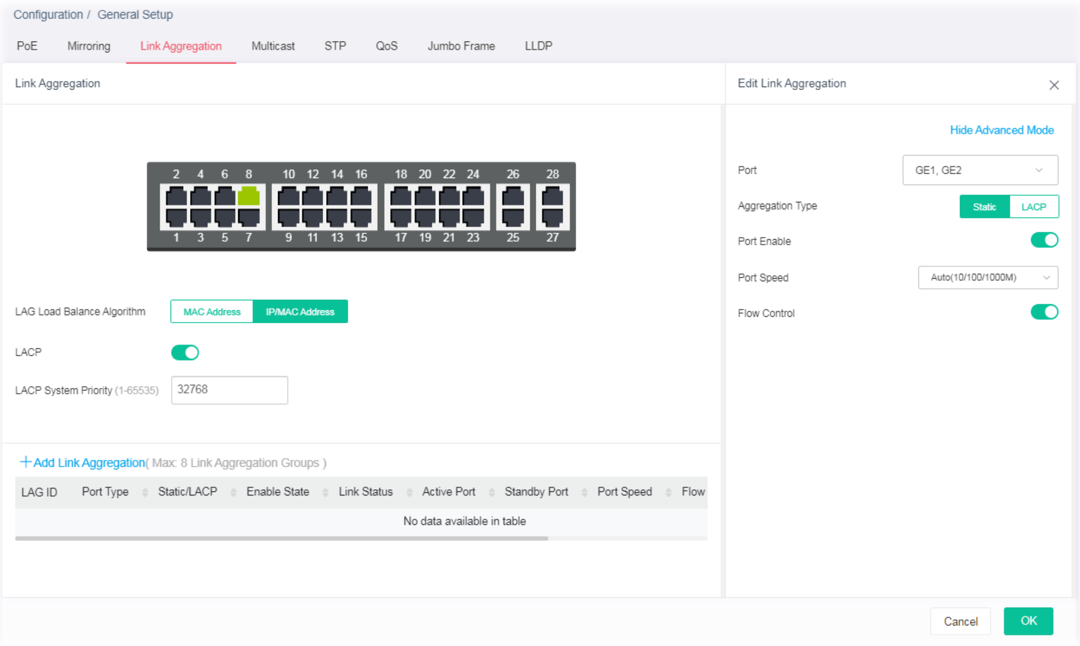
+Add Link Aggregation(Max: 8 Link Aggregation Groups)

LAG ID	Port Type	Static/LACP	Enable State	Link Status	Active Port	Standby Port	Port Speed	Flow Ctrl Config	Flow Ctrl Status
No data available in table									

Available settings are explained as follows:

Item	Description
Link Aggregation	
LAG Load Balance Algorithm	Select your Load balance algorithm. **MAC address** - Aggregated group will balance the traffic based on different MAC addresses. Therefore, the packets from different MAC addresses will be sent to different links. **IP/Mac Address** - Aggregated group will balance the traffic based on MAC addresses and IP addresses. Therefore, the packets from same MAC addresses but different IP addresses will be sent to different links.
LACP	**Enable / Disable** – Click the toggle to enable / disable this function. ● - means “Enable”. ○ - means “Disable”.
LACP System Priority	The priority is used to determine which switch (local or remote) on the LAG connection is able to decide LACP activities. The lower the number is, the higher the priority for VigorSwitch will be. Therefore, the switch with the highest system priority (e.g., 1) can make decisions about which ports actively participate in LAG at a given time.
+Add Link Aggregation	Click to open the setting page of creating Link Aggregation.

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



Configuration / General Setup

Link Aggregation

LAG Load Balance Algorithm: MAC Address | IP/MAC Address

LACP

LACP System Priority (1-65535): 32768

+Add Link Aggregation(Max: 8 Link Aggregation Groups)

LAG ID	Port Type	Static/LACP	Enable State	Link Status	Active Port	Standby Port	Port Speed	Flow
No data available in table								

Edit Link Aggregation

Hide Advanced Mode

Port: GE1, GE2

Aggregation Type: Static | LACP

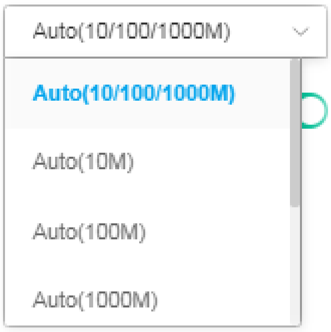
Port Enable

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

Flow Control

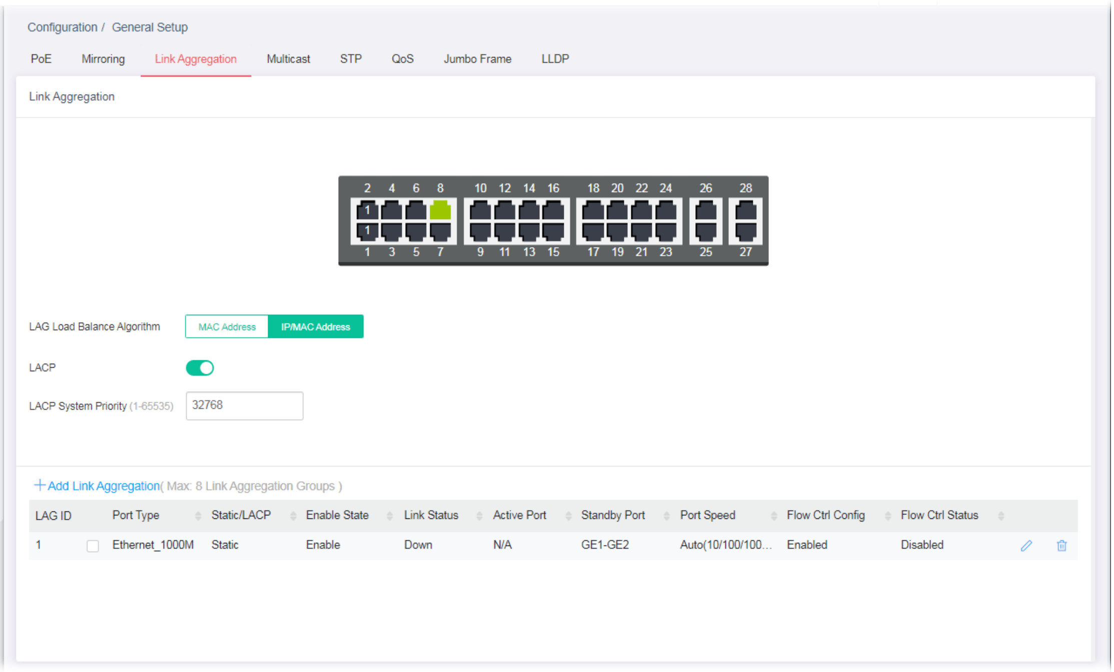
Available settings are explained as follows:

Item	Description
Edit Link Aggregation	
Show/Hide Advanced Mode	Click to switch different modes.
Aggregation Type	Specify the type for LAG. **Static** - The static aggregated port sends packets over active member without detecting or negotiating with remote aggregated port. **LACP** - The LACP aggregated ports place member into active only after negotiated with remote aggregated port for best reliability.
Port Enable	**Enable / Disable** – Click the toggle to enable / disable this function. ● - means “Enable”. ○ - means “Disable”.

Port Speed	Port speed capabilities:
	
	Auto(10/100/1000M)
	Auto(10/100/1000M)
	Auto(10M)
	Auto(100M)
	Auto(1000M)
	● **Auto(10/100/1000M):** Auto speed with all capabilities.
	● **Auto(10M):** Auto speed with 10M ability only.

	● **Auto(100M):** Auto speed with 100M ability only. ● **Auto(1000M):** Auto speed with 1000M ability only. ● **10M:** Force speed with 10M ability. ● **100M:** Force speed with 100M ability. ● **1000M:** Force speed with 1000M ability. Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect. For SFP fiber module, you might need to manually configure the speed to match fiber module speed.
Flow Control	**Enable / Disable** – Click the toggle to enable / disable this function. ● - means "Enable". ○ - means "Disable". A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port. The switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later.
OK	Save the settings.

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



LAG Load Balance Algorithm: IP/MAC Address

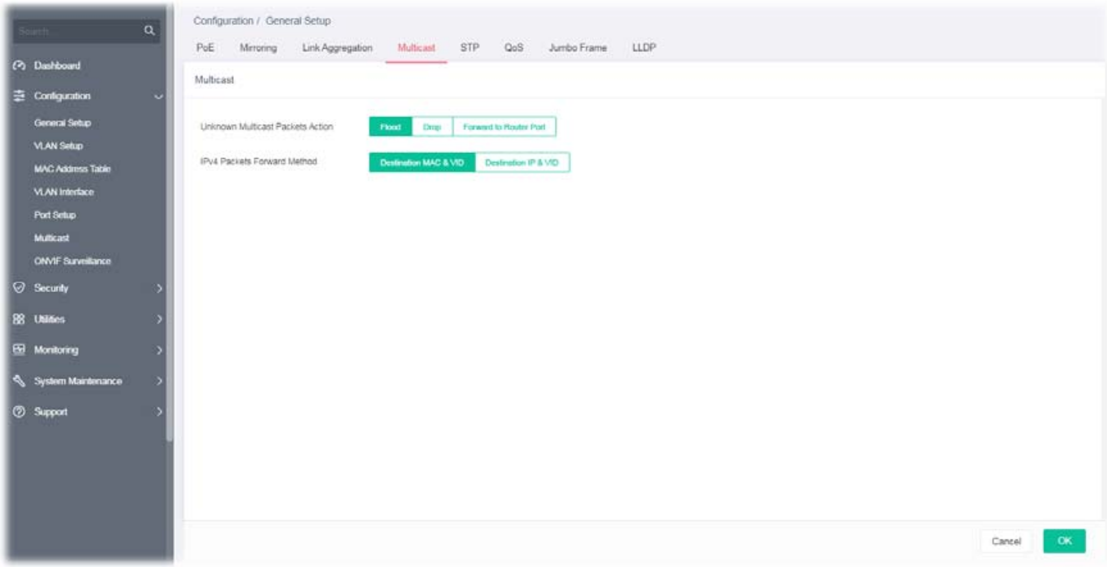
LACP: on

LACP System Priority (1-65535): 32768

LAG ID		Port Type	Static/LACP	Enable State	Link Status	Active Port	Standby Port	Port Speed	Flow Ctrl Config	Flow Ctrl Status
1	□	Ethernet_1000M	Static	Enable	Down	N/A	GE1-GE2	Auto(10/100/100...	Enabled	Disabled

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.



Unknown Multicast Packets Action: Flood

IPv4 Packets Forward Method: Destination MAC & VID

Available settings are explained as follows:

Item	Description
Unknown Multicast Packets Action	Select an action for switch to handle with unknown multicast packet. **Drop** - Drop the unknown multicast data. **Flood** - Flood the unknown multicast data. **Forward to Router Port** - Forward the unknown multicast data to router port.
IPv4 Packets Forward	Set the IPv4 multicast forward method.

Method	**Dst. MAC & VID** - Forward using destination multicast MAC address and VLAN IDs. **Dst. IP & VID** - Forward using destination multicast IP address and VLAN ID.

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

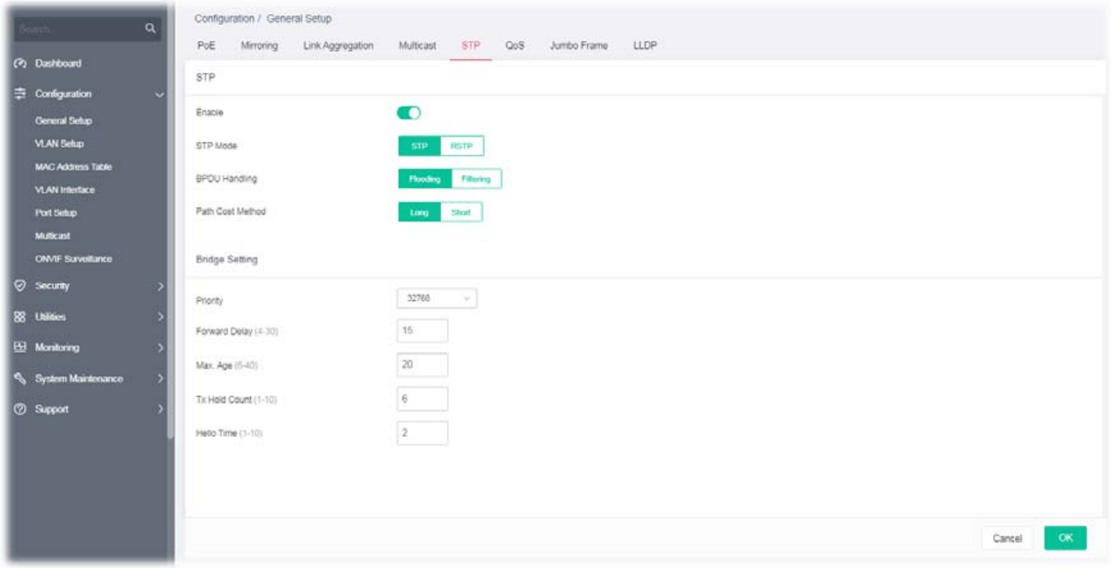
II-1-5 STP

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.



STP

Enable ●

STP Mode [✓ STP] RSTP

BPDU Handling [✓ Flooding] Filtering

Path Cost Method [✓ Long] Short

Bridge Setting

Priority 32768

Forward Delay (4-30) 15

Max. Age (6-40) 20

Tx Hold Count (1-10) 6

Hello Time (1-10) 2

Available settings are explained as follows:

Item	Description
STP	
Enable	**Enable / Disable** – Click the toggle to enable / disable this function. ● - means “Enable”. ○ - means “Disable”.
STP Mode	Set the operating mode of Spanning Tree (STP). **STP -** Enable the Spanning Tree (STP) operation. **RSTP -** Enable the Rapid Spanning Tree (RSTP) operation.
BPDU Handling	Specify the BPDU forward method when the STP is disabled.

	Filtering - Filter the BPDU when STP is disabled. **Flooding -** Flood the BPDU when STP is disabled.
Path Cost Method	Specify the path cost method. **Long -** Specifies that the default port path costs are within the range: 1~200,000,000. **Short -** Specifies that the default port path costs are within the range: 1~65,535.
Bridge Setting - Negotiate with other VigorSwitch for determining the bridge switch.	
Priority	Specify the bridge priority. The valid range is from 0 to 61440, and the value should be the multiple of 4096. It ensures the probability that the switch is selected as the root bridge, and the lower value has the higher priority for the switch to be selected as the root bridge of the topology.
Forward Delay	Specify the STP forward delay time, which is the amount of time that a port remains in the Listening and Learning states before it enters the Forwarding state. Its valid range is from 4 to 10 seconds.
Max. Age	Specify the time interval in seconds for a switch to wait the configuration messages, without attempting to redefine its own configuration.
Tx Hold Count	Specify the tx-hold-count used to limit the maximum numbers of packets transmission per second. The valid range is from 1 to 10.
Hello Time	Specify the STP hello time in second to broadcast its hello message to other bridge by Designated Ports. Its valid range is from 1 to 10 seconds.

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.

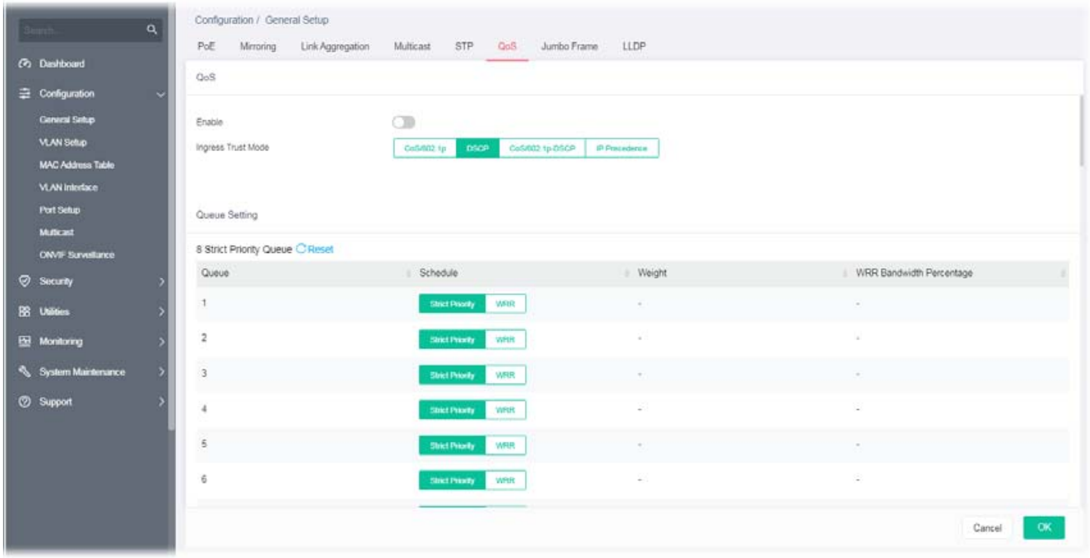
Actual effectiveness is based on how QoS is configured in previous QoS section. This page provides settings for user to configure mapping only.

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.



Enable ○

Ingress Trust Mode: CoS/802.1p | [✓ DSCP] | CoS/802.1p-DSCP | IP Precedence

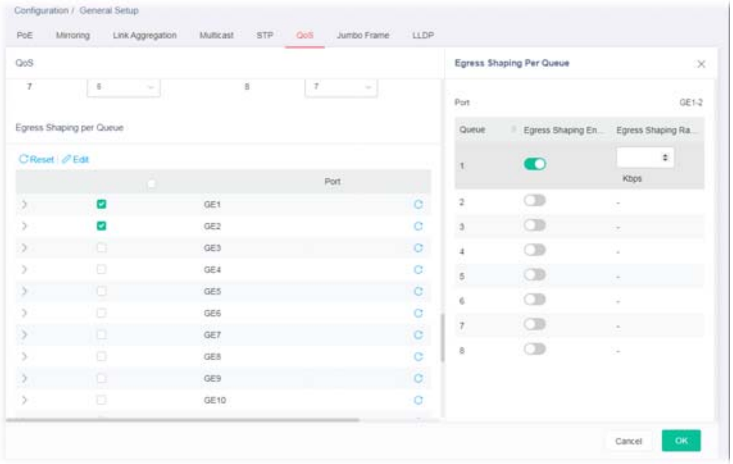
8 Strict Priority Queue

Queue	Schedule	Weight	WRR Bandwidth Percentage
1	[✓ Strict Priority] WRR	-	-
2	[✓ Strict Priority] WRR	-	-
3	[✓ Strict Priority] WRR	-	-
4	[✓ Strict Priority] WRR	-	-
5	[✓ Strict Priority] WRR	-	-
6	[✓ Strict Priority] WRR	-	-

Available settings are explained as follows:

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

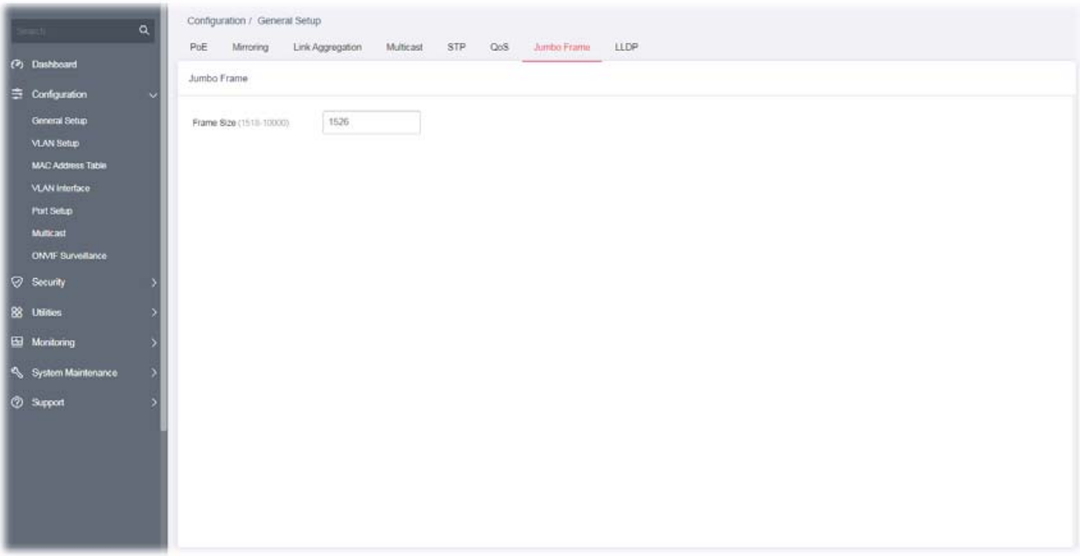
	mapped to queues based on the CoS value in the VLAN tag. **IP Precedence** - All IP traffic is mapped to queues based on the DSCP field in the IP header. If traffic is not IP but has VLAN tag, mapped to queues based on the CoS value in the VLAN tag.
Queue Setting	
Queue	There are eight queue ID numbers allowed to be configured.
Schedule	**Strict Priority** - Click it to set queue to strict priority type. **WRR** - Click it to set queue to Weight round robin type.
Weight	If the queue type is WRR, set the queue weight for the queue
WRR Bandwidth Percentage	Displays the percentage of traffic which can be sent by current queue compared to total WRR queues.
CoS Mapping	
Class of Service Mapping to Queue (for Ingress Traffic)	Defines the queue ID (level 1 to 8) for different class of service values. **Reset** - Clear current settings and return to factory default settings.
Class of Service Mapping to Queue (for Egress Traffic Remark)	Defines the class of service value (0 to 7). **Reset** - Clear current settings and return to factory default settings.
DSCP Mapping	
DSCP Mapping to Queue (for Ingress Traffic)	Define the queue ID (level 1 to 8) for different DSCP values. **Reset** - Clear current settings and return to factory default settings.
DSCP Mapping to Queue (for Egress Traffic Remarking)	Define the DSCP value (0 to 63). **Reset** - Clear current settings and return to factory default settings.
IP Precedence Mapping	
IP Precedence Mapping to Queue (for Ingress Traffic)	Defines the queue ID (level 1 to 8) for different IP Precedence values. **Reset** - Clear current settings and return to factory default settings.
IP Precedence Mapping to Queue (for Egress Traffic Remarking)	Defines the IP Precedence value (0 to 7). **Reset** - Clear current settings and return to factory default settings.
Egress Shaping per Queue	Configure the maximum egress bandwidth not only by port but also by specific QoS queues. **Reset** - Clear all settings and return to factory default settings. **Port** - Display the port (GE1 to GE28) profiles. ↻ - Clear settings of the selected port and return to factory default settings. **Edit** - To modify the egress shaping rate for port profiles, select two (at least) GE ports to display the link.

	 Configuration / General Setup PoE Mirroring Link Aggregation Multicast STP QoS Jumbo Frame LLDP QoS Egress Shaping per Queue Reset Edit Port GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8 GE9 GE10 Egress Shaping Per Queue Port GE1-2 Queue Egress Shaping En... Egress Shaping Ra... Kbps 1 2 3 4 5 6 7 8 Cancel OK ● **Egress Shaping Enabled**- Switch the toggle to enable/disable the setting. ● **Egress Shaping Rate (CIR)** - Enter the rate value,<16-1000000>, unit:16 Kbps.

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

II-1-7 Jumbo Frame

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



Frame Size (1518-10000) 1526

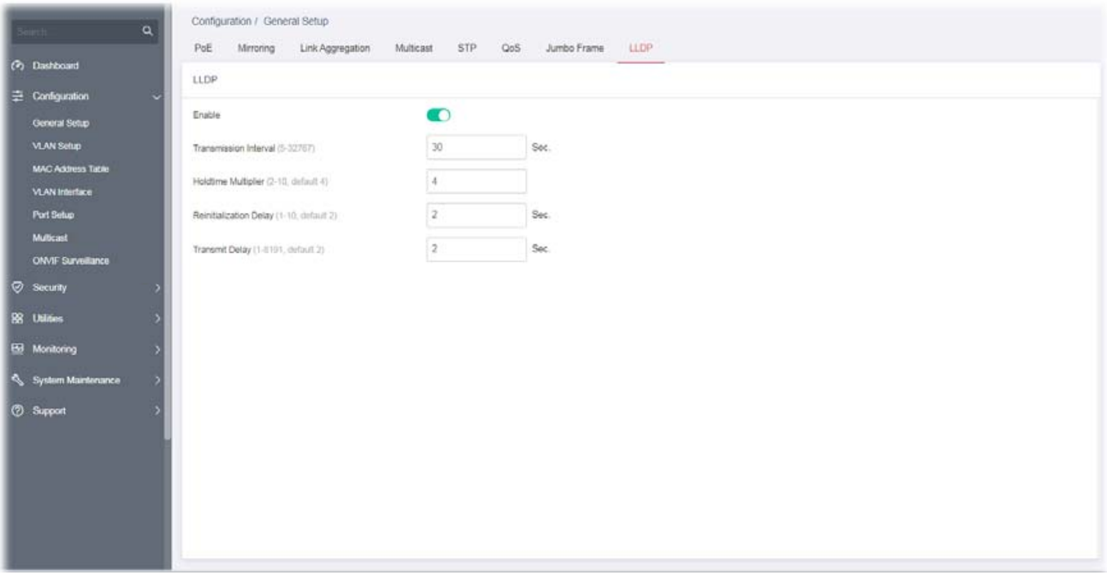
Available settings are explained as follows:

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.



Configuration / General Setup

LLDP

Enable ●

Transmission Interval (5-32767) 30 Sec.

Holdtime Multiplier (2-10, default 4) 4

Reinitialization Delay (1-10, default 2) 2 Sec.

Transmit Delay (1-8191, default 2) 2 Sec.

Available settings are explained as follows:

Item	Description
LLDP	
Enable	**Enable / Disable** – Click the toggle to enable / disable this function. ● - means “Enable”. ○ - means “Disable”. If LLDP function is disabled, specify an action for the LLDP PDU packets. ● **Filtering** - The LLDP packets will be filtered and deleted when LLDP is disabled. ● **Bridging** - The LLDP packets will be bridging when LLDP is disabled. ● **Flooding** - The LLDP packets will be flooded and forwarded to all interfaces when LLDP is disabled.
Transmission Interval	Select the interval at which frames are transmitted. The default is 30 seconds, and the valid range is 5–32768seconds.
Holdtime Multiplier	Select the multiplier on the transmit interval to assign to TTL (range 2–10, default = 4).
Reinitialization Delay	Select the delay before a re-initialization (range 1–10 seconds, default = 2).
Transmit Delay	Select the delay after an LLDP frame is sent (range 1–8192 seconds, default = 3).

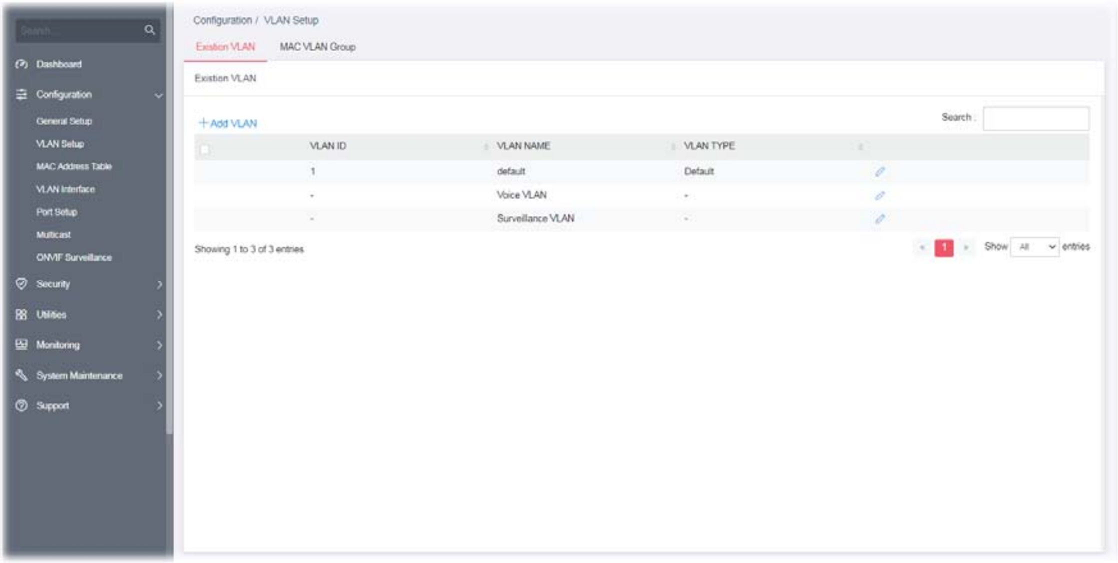
After finishing this web page configuration, please click **OK** to save the settings.

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



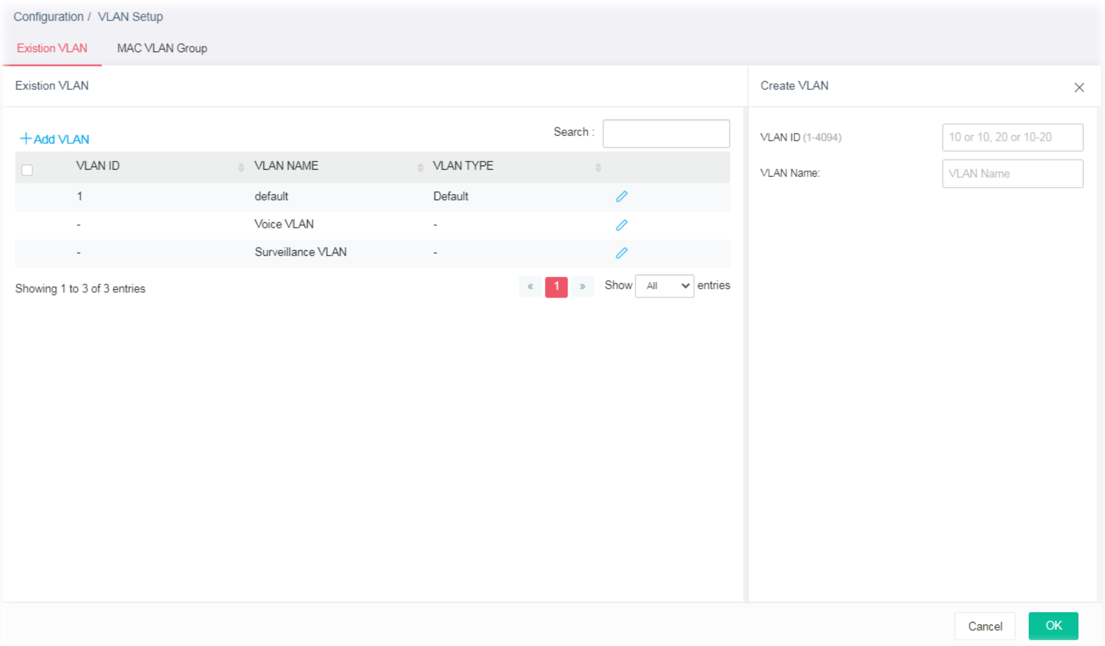
□	VLAN ID	VLAN NAME	VLAN TYPE	
	1	default	Default	✎
	-	Voice VLAN	-	✎
	-	Surveillance VLAN	-	✎

Showing 1 to 3 of 3 entries

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.
✎	Click to modify the setting page of the selected VLAN.

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



Configuration / VLAN Setup

Existion VLAN | MAC VLAN Group

Existion VLAN

+Add VLAN

Search :

□	VLAN ID	VLAN NAME	VLAN TYPE	
	1	default	Default	✎
	-	Voice VLAN	-	✎
	-	Surveillance VLAN	-	✎

Showing 1 to 3 of 3 entries

« 1 » Show All entries

Create VLAN

VLAN ID (1-4094): 10 or 10, 20 or 10-20

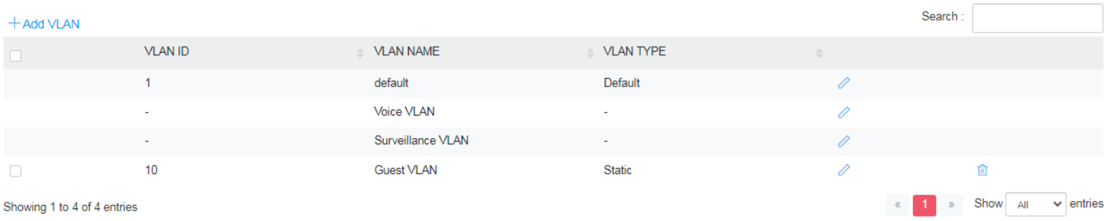
VLAN Name: VLAN Name

Cancel OK

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.



+Add VLAN

Search :

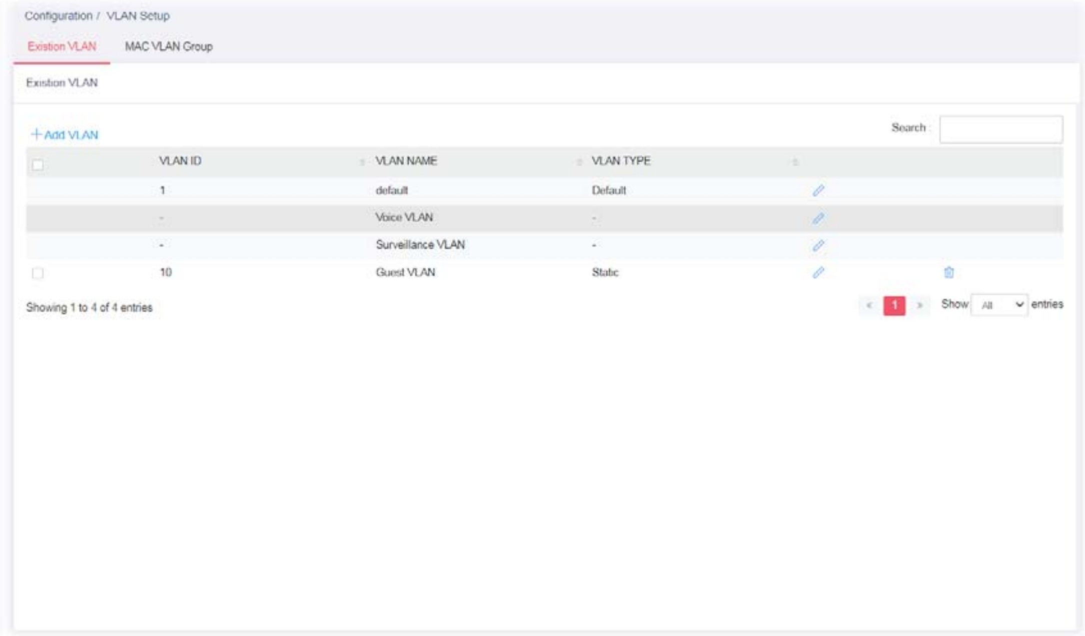
□	VLAN ID	VLAN NAME	VLAN TYPE		
	1	default	Default	✎	
	-	Voice VLAN	-	✎	
	-	Surveillance VLAN	-	✎	
□	10	Guest VLAN	Static	✎	🗑

Showing 1 to 4 of 4 entries

« 1 » Show All entries

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.



Configuration / VLAN Setup

Existion VLAN | MAC VLAN Group

Existion VLAN

+Add VLAN

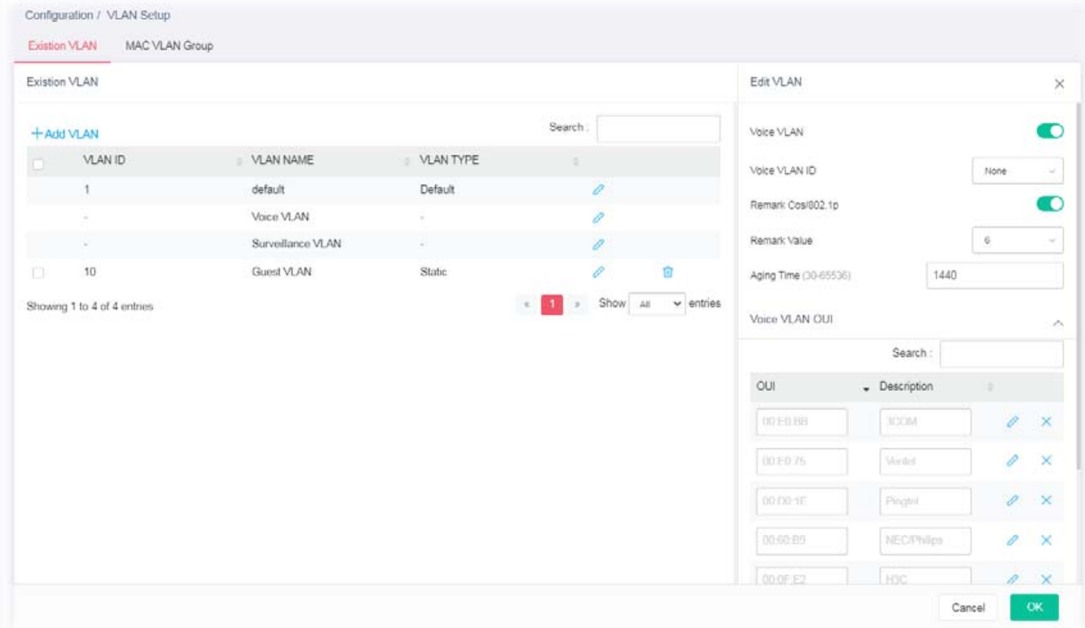
Search :

□	VLAN ID	VLAN NAME	VLAN TYPE		
	1	default	Default		
	-	Voice VLAN	-		
	-	Surveillance VLAN	-		
□	10	Guest VLAN	Static		

Showing 1 to 4 of 4 entries

‹ 1 › Show All entries

Click to open the editing page.



Configuration / VLAN Setup

Existion VLAN | MAC VLAN Group

Existion VLAN

+Add VLAN

Search :

□	VLAN ID	VLAN NAME	VLAN TYPE		
	1	default	Default		
	-	Voice VLAN	-		
	-	Surveillance VLAN	-		
□	10	Guest VLAN	Static		

Showing 1 to 4 of 4 entries

‹ 1 › Show All entries

Edit VLAN

Voice VLAN: enabled

Voice VLAN ID: None

Remark Cos/802.1p: enabled

Remark Value: 6

Aging Time (30-65536): 1440

Voice VLAN OUI

Search :

OUI	Description
00:E0:BB	3COM
00:E0:75	Verilel
00:D0:1E	Pingtel
00:60:B9	NEC/Philips
00:0F:E2	H3C

Cancel | OK

Available settings are explained as follows:

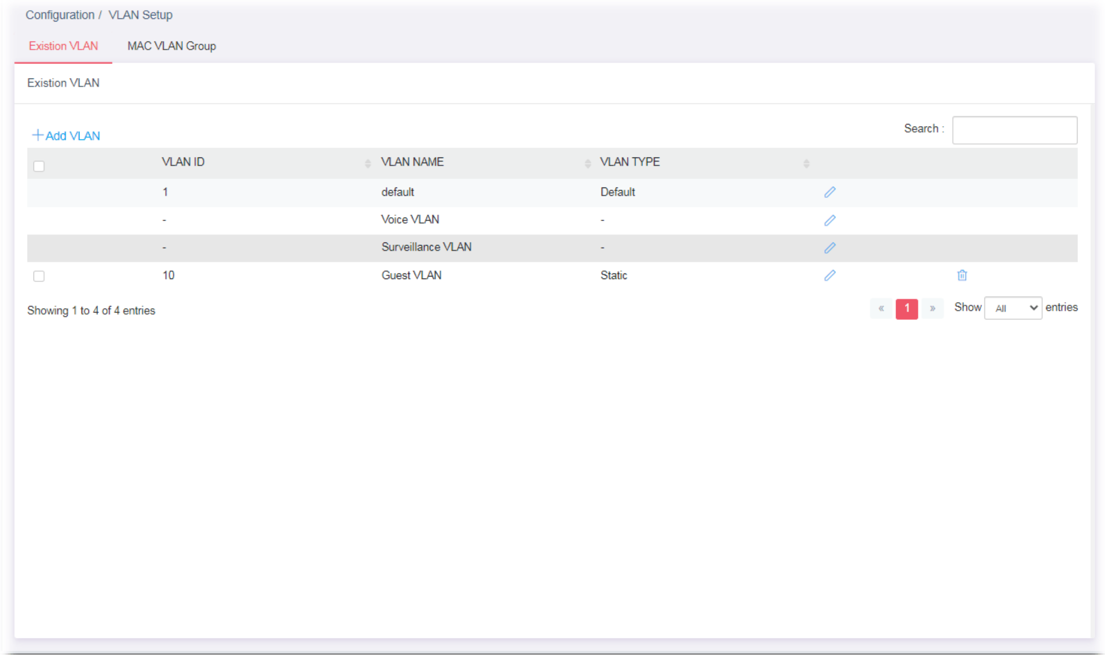
Item	Description
Edit VLAN	
Voice VLAN	**Enable / Disable** – Click the toggle to enable / disable this function. - means “Enable”. - means “Disable”.
Voice VLAN ID	Select Voice VLAN ID profile.
Remark Cos/802.1p	Click the toggle to enable / disable this function.

	Remark Value - If enabled, qualified packets will be remarked by this value. Specify the number of packets to be remarked. (0 to 7). The VoIP packets will be tagged with this number, so that QoS can prioritize it correctly.
Aging Time	Select value of aging time (30~65536 min). Default is 1440 minutes. A voice VLAN entry will be age out after this time if without any packet pass through.
Voice VLAN OUI	Click the ⌄ to display advanced settings. Default has 8 pre-defined OUI MAC. **+Add** - Click to create a new voice OUI. ● **OUI** - Enter the OUI address. ● **Description** - Enter a description of the specified MAC address to the voice VLAN OUI table. ✎ - Click it to modify the OUI settings and the description.
OK	Save the settings.

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

II-2-1-3 Surveillance VLAN

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



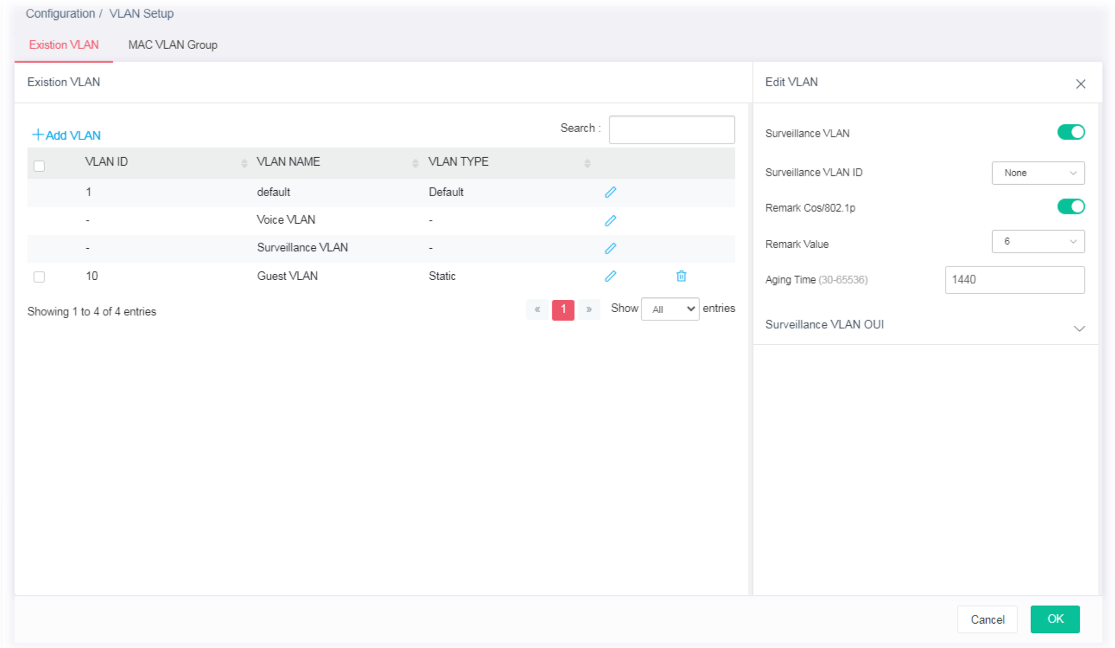
Configuration / VLAN Setup

Existion VLAN

□	VLAN ID	VLAN NAME	VLAN TYPE	
	1	default	Default	✎
	-	Voice VLAN	-	✎
	-	Surveillance VLAN	-	✎
□	10	Guest VLAN	Static	✎ 🗑

Showing 1 to 4 of 4 entries

Click ✎ to open the editing page.



Configuration / VLAN Setup

Existion VLAN | MAC VLAN Group

Existion VLAN

+Add VLAN

Search :

VLAN ID	VLAN NAME	VLAN TYPE	
1	default	Default	✎
-	Voice VLAN	-	✎
-	Surveillance VLAN	-	✎
10	Guest VLAN	Static	✎

Showing 1 to 4 of 4 entries

Show All entries

Edit VLAN

Surveillance VLAN: ●

Surveillance VLAN ID: None

Remark Cos/802.1p: ●

Remark Value: 6

Aging Time (30-65536): 1440

Surveillance VLAN OUI

Cancel OK

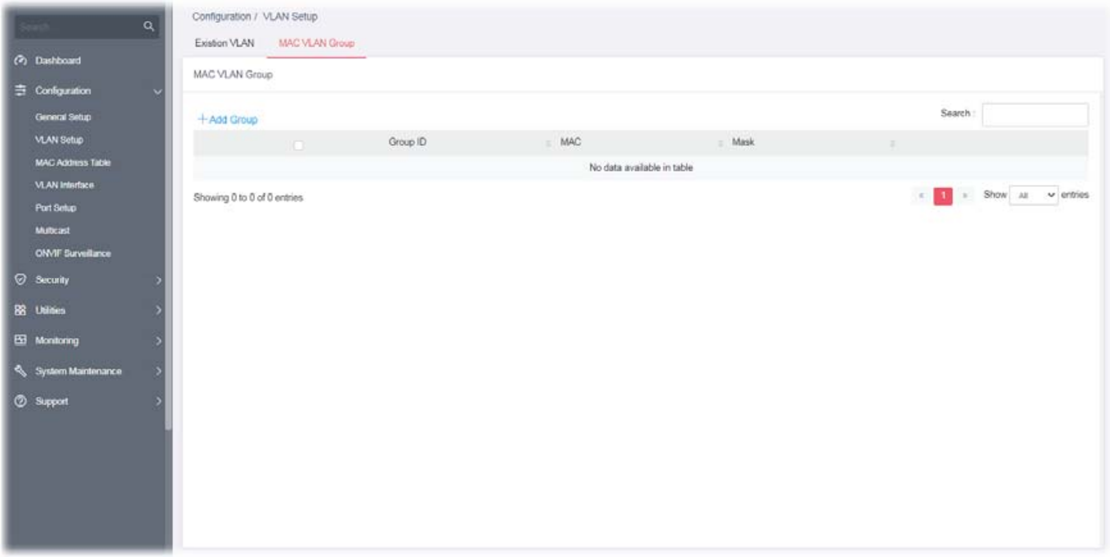
Available settings are explained as follows:

Item	Description
Edit VLAN	
Surveillance VLAN	**Enable / Disable** – Click the toggle to enable / disable this function. ● - means “Enable”. ○ - means “Disable”. Enable the function to configure surveillance VLAN.
Surveillance VLAN ID	Choose a VLAN profile as Surveillance VLAN.
Remark Cos/802.1p	Click the toggle to enable / disable this function. **Remark Value** - If enabled, qualified packets will be remarked by this value. Specify the number of packets to be remarked. (0 to 7). The VoIP packets will be tagged with this number, so that QoS can prioritize it correctly.
Aging Time	Select value of aging time (30~65536 min). Default is 1440 minutes. A voice VLAN entry will be age out after this time if without any packet pass through.
Surveillance VLAN OUI	Filtering Surveillance traffic is based on the OUI of the IP cameras. Click the ∨ to display advanced settings. **+Add** - Click to create a new OUI. ● **OUI** - Enter OUI MAC address of monitored IP camera. ● **Description** - Enter a description of the specified MAC address to the surveillance VLAN OUI table. ✎ - Click to modify the OUI settings and the description.
OK	Save the settings.

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

II-2-2 MAC VLAN 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.



MAC VLAN Group

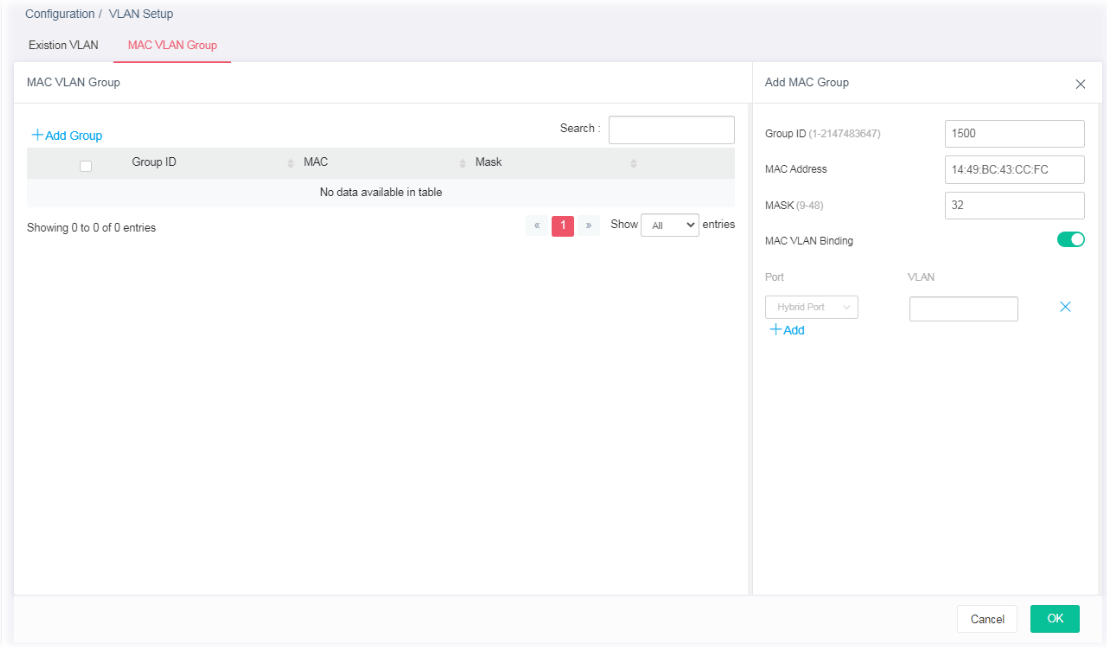
□	Group ID	MAC	Mask
No data available in table			

Showing 0 to 0 of 0 entries

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.



□	Group ID	MAC	Mask
No data available in table			

Group ID (1-2147483647): 1500

MAC Address: 14:49:BC:43:CC:FC

MASK (9-48): 32

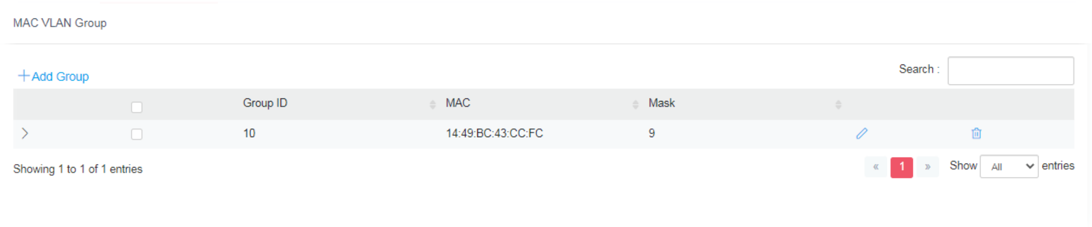
MAC VLAN Binding: ●

Available settings are explained as follows:

Item	Description
Add MAC Group	
Group ID	It is a number for identification later, while chosen to be bound with VLAN/Port.
MAC Address	Enter the MAC address you wish to be classified in this group.
MASK	The mask is the length of matching prefix you wish to have on MAC address. For example, configure mask in 10. It means a host with beginning of the 10-digit of MAC address will be checked, and classified into this group if matched.
MAC VLAN Binding	The MAC VLAN allows you to statically assign a VLAN ID to a host with specific MAC address(es). VigorSwitch allows you to configure multiple groups with configured MAC address and mask to be active on ports and to be bound with VLAN ID. This page allows the network administrator to bind the group of specified MAC addresses with VLAN and Port. **Enable / Disable** – Click the toggle to enable / disable this function. ● - means “Enable”. ○ - means “Disable”. **+Add** - Click to enter a port number and VLAN ID number. ● **Port** - Select the ports you wish to be bound with specified MAC address group. ● **VLAN** - Enter the VLAN ID that you wish to be bound with.

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

A new group will be shown on the page.



MAC VLAN Group

	□	Group ID	MAC	Mask		
>	□	10	14:49:BC:43:CC:FC	9	✎	🗑

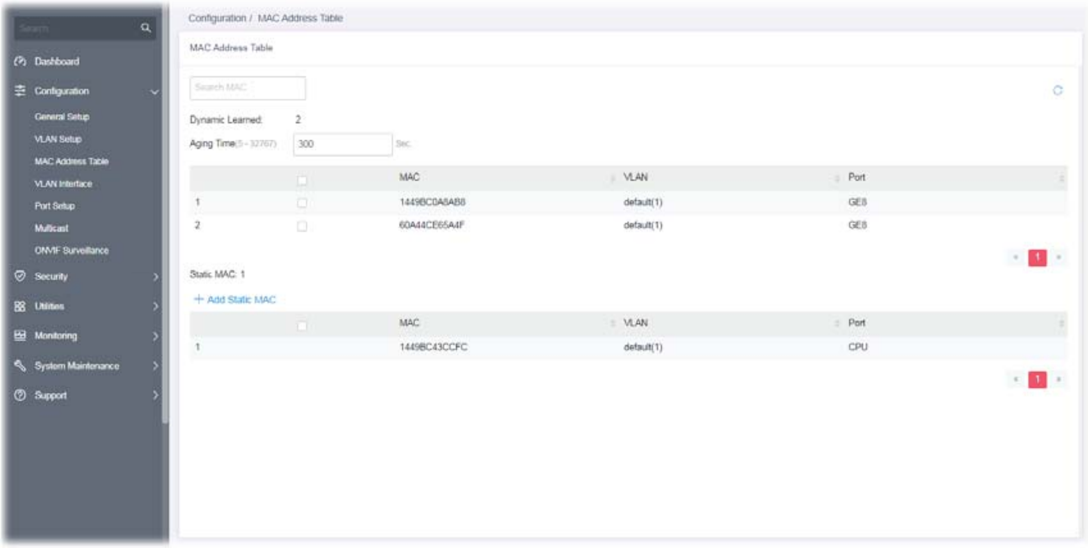
Showing 1 to 1 of 1 entries

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-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.



Configuration / MAC Address Table

MAC Address Table

Search MAC

Dynamic Learned: 2

Aging Time(5 - 32767) 300 Sec.

	□	MAC	VLAN	Port
1	□	1449BC0A8AB8	default(1)	GE8
2	□	60A44CE65A4F	default(1)	GE8

Static MAC: 1

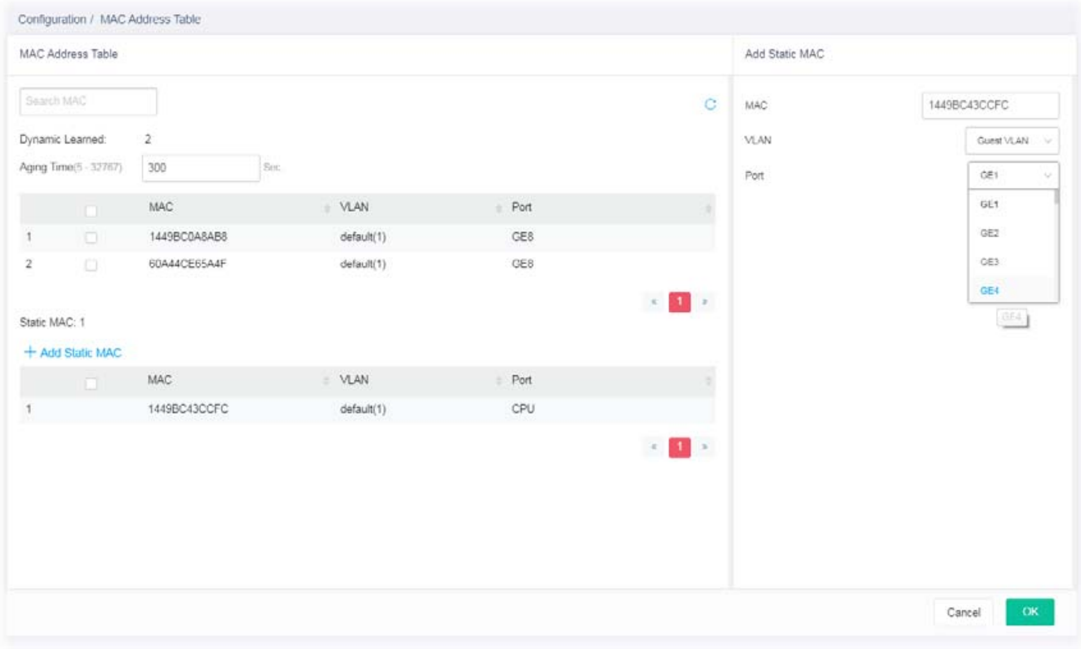
+ Add Static MAC

	□	MAC	VLAN	Port
1		1449BC43CCFC	default(1)	CPU

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.



Configuration / MAC Address Table

MAC Address Table

Dynamic Learned: 2

Aging Time(5 - 32767) 300 Sec

	□	MAC	VLAN	Port
1	□	1449BC0A8AB8	default(1)	GE8
2	□	60A44CE65A4F	default(1)	GE8

Static MAC: 1

	□	MAC	VLAN	Port
1		1449BC43CCFC	default(1)	CPU

Add Static MAC

MAC: 1449BC43CCFC

VLAN: Guest VLAN

Port: GE1

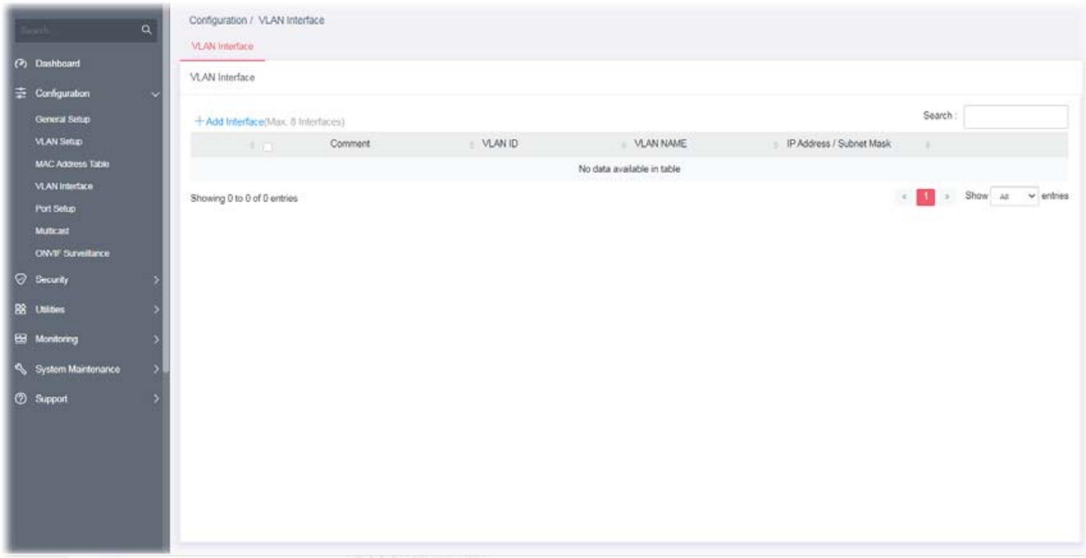
Available settings are explained as follows:

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 VLAN Interface

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.



VLAN Interface

+Add Interface(Max. 8 Interfaces)

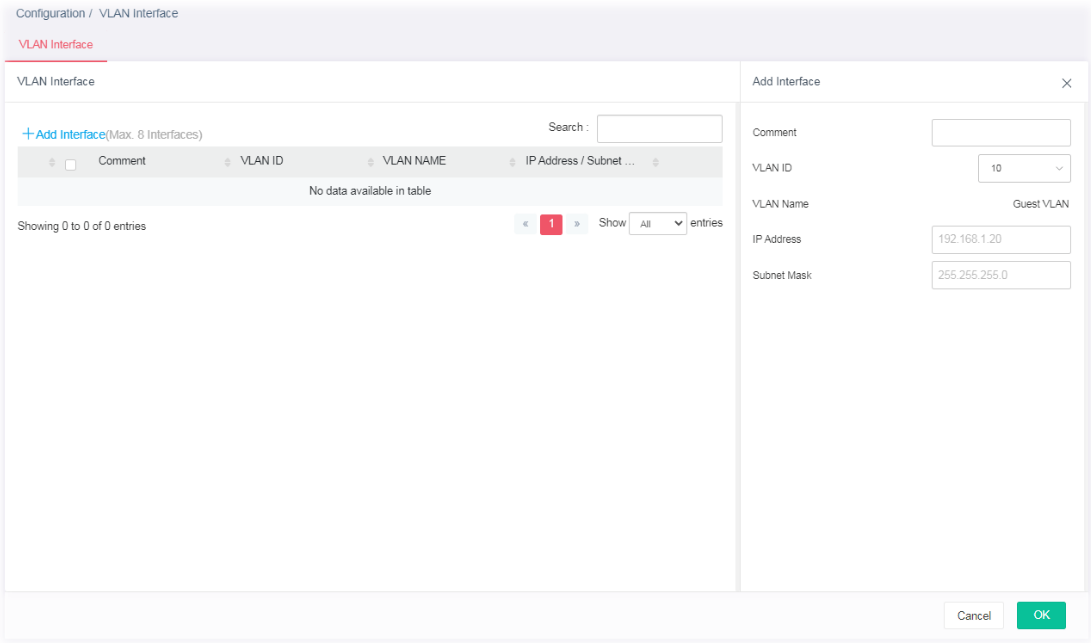
□	Comment	VLAN ID	VLAN NAME	IP Address / Subnet Mask
No data available in table				

Showing 0 to 0 of 0 entries

Available settings are explained as follows:

Item	Description
+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.

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



Configuration / VLAN Interface

VLAN Interface

Comment	VLAN ID	VLAN NAME	IP Address / Subnet ...
No data available in table			

Showing 0 to 0 of 0 entries

Add Interface

Comment:

VLAN ID: 10

VLAN Name: Guest VLAN

IP Address: 192.168.1.20

Subnet Mask: 255.255.255.0

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.

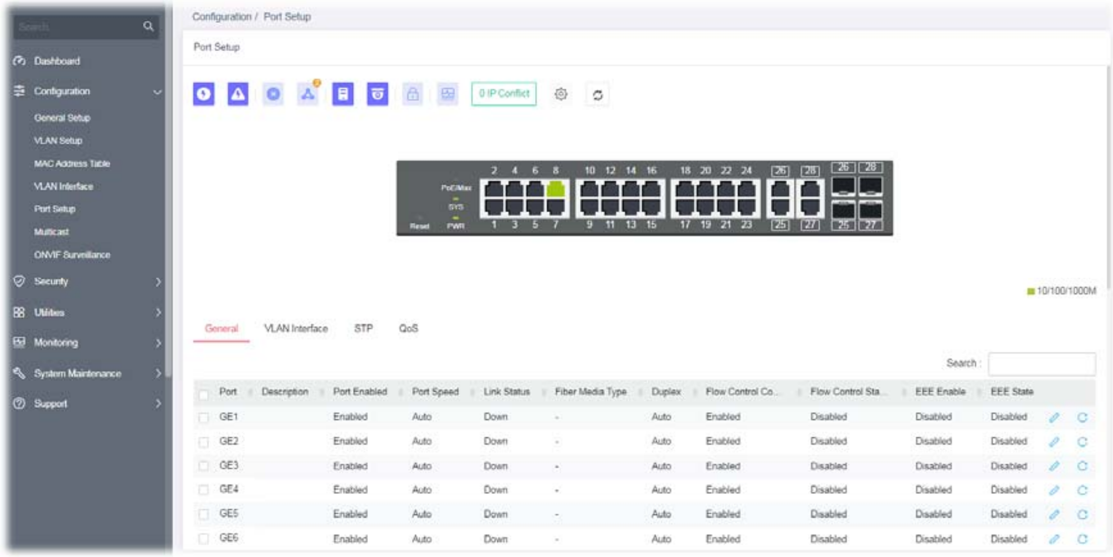
After finishing this web page configuration, please click **OK** to save the settings.

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.



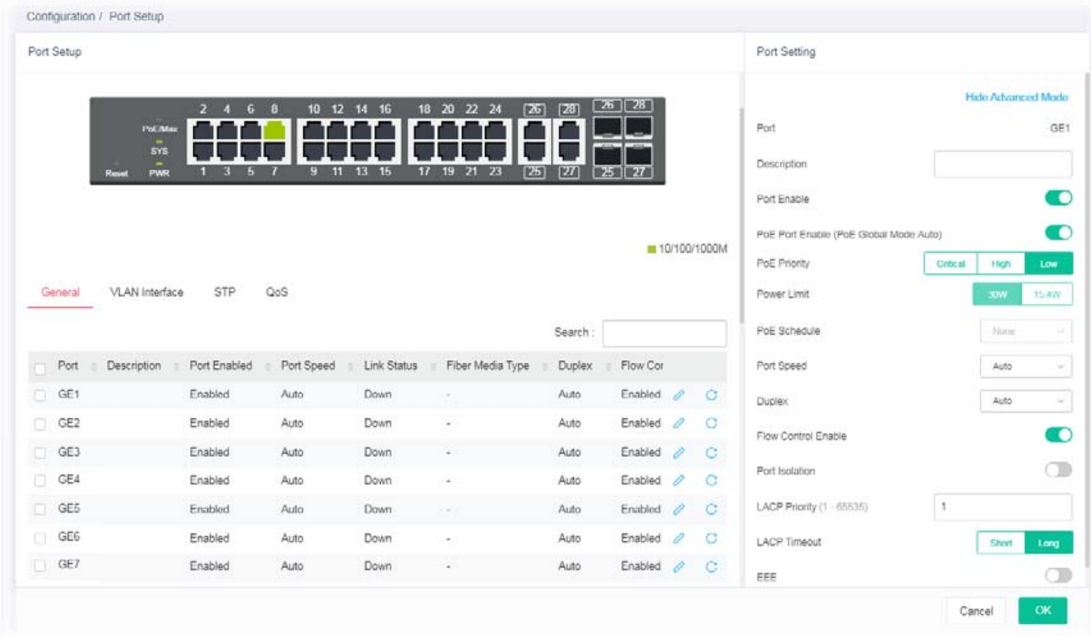
Port	Description	Port Enabled	Port Speed	Link Status	Fiber Media Type	Duplex	Flow Control Co...	Flow Control Sta...	EEE Enable	EEE State
GE1		Enabled	Auto	Down	-	Auto	Enabled	Disabled	Disabled	Disabled
GE2		Enabled	Auto	Down	-	Auto	Enabled	Disabled	Disabled	Disabled
GE3		Enabled	Auto	Down	-	Auto	Enabled	Disabled	Disabled	Disabled
GE4		Enabled	Auto	Down	-	Auto	Enabled	Disabled	Disabled	Disabled
GE5		Enabled	Auto	Down	-	Auto	Enabled	Disabled	Disabled	Disabled
GE6		Enabled	Auto	Down	-	Auto	Enabled	Disabled	Disabled	Disabled

Available settings are explained as follows:

Item	Description
Port	Displays the LAN ports (GE1 to GE28).
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.
✎	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.



Configuration / Port Setup

Port Setup

General | VLAN Interface | STP | QoS

Search :

□	Port	Description	Port Enabled	Port Speed	Link Status	Fiber Media Type	Duplex	Flow Cor		
□	GE1		Enabled	Auto	Down	-	Auto	Enabled	✎	↻
□	GE2		Enabled	Auto	Down	-	Auto	Enabled	✎	↻
□	GE3		Enabled	Auto	Down	-	Auto	Enabled	✎	↻
□	GE4		Enabled	Auto	Down	-	Auto	Enabled	✎	↻
□	GE5		Enabled	Auto	Down	-	Auto	Enabled	✎	↻
□	GE6		Enabled	Auto	Down	-	Auto	Enabled	✎	↻
□	GE7		Enabled	Auto	Down	-	Auto	Enabled	✎	↻

Port Setting

Hide Advanced Mode

Port: GE1

Description:

Port Enable: ● on

PoE Port Enable (PoE Global Mode:Auto): ● on

PoE Priority: Critical | High | [✓ Low]

Power Limit: [✓ 30W] | 15.4W

PoE Schedule: None

Port Speed: Auto

Duplex: Auto

Flow Control Enable: ● on

Port Isolation: ○ off

LACP Priority (1 - 65535): 1

LACP Timeout: Short | [✓ Long]

EEE: ○ off

Cancel | OK

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 Enable	Enable/disable the settings of the selected port.
PoE Port Enable (PoE Global Mode: Auto)	Enable/disable the PoE feature of the selected port. If enabled, this port can be used for connecting the PoE device.
PoE Priority	Select Priority for PoE device. **Critical** - Set PoE device to highest priority connection. **High** –Set PoE device to high priority connection. **Low** –Set PoE device to low priority connection.
Power Limit	This setting is available when Manual is selected as PoE Mode. Enter the value (30W / 15.4W) as the maximum limit of power given to each physical port.
PoE Schedule	Specify the PoE port for applying the schedule. Before choosing, the PoE mode must be set as **Manual**. Use the drop down list to choose the schedule profile (from 1 to 15).
Port Speed	Port speed capabilities: ● **Auto:** Auto speed with all capabilities. ● **Auto(10M):** Auto speed with 10M ability only. ● **Auto(100M):** Auto speed with 100M ability only.

	● **Auto(1000M):** Auto speed with 1000M ability only. ● **Auto(10/100M):** Auto speed with 10/100M ability. ● **10M:** Force speed with 10M ability. ● **100M:** Force speed with 100M ability. ● **1000M:** Force speed with 1000M ability. Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect. For SFP fiber module, you might need to manually configure the speed to match fiber module speed.
Duplex	Port duplex capabilities: ● **Auto:** Auto duplex with all capabilities. ● **Half:** Auto speed with 10/100M ability only. ● **Full:** Auto speed with 10/100/1000M ability only.
Flow Control 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. **Enable / Disable** – Click the toggle to enable / disable this function. ● - means "Enable". ○ - means "Disable".
Port Isolation	It allows the network administrator to configure protected port setting to prevent the selected ports from communication with each other. Port isolation is only allowed to communicate with unprotected port. For example, GE1 and GE3 are selected in Port List and Enable is clicked as port isolation, then users behind GE1 and GE3 are separated and can not communicate with each other. **Enable / Disable** – 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. **Short -** LACP PDU will be sent per second. If port member is not seen over 3 seconds, it will cause port member timeout.

	Long - LACP PDU will be sent every 30 seconds. If port member is not seen over 90 seconds, it will cause port member timeout.
EEE	Enable or disable port EEE (Energy Efficient Ethernet) function for the selected port.

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

II-5-2 VLAN Interface

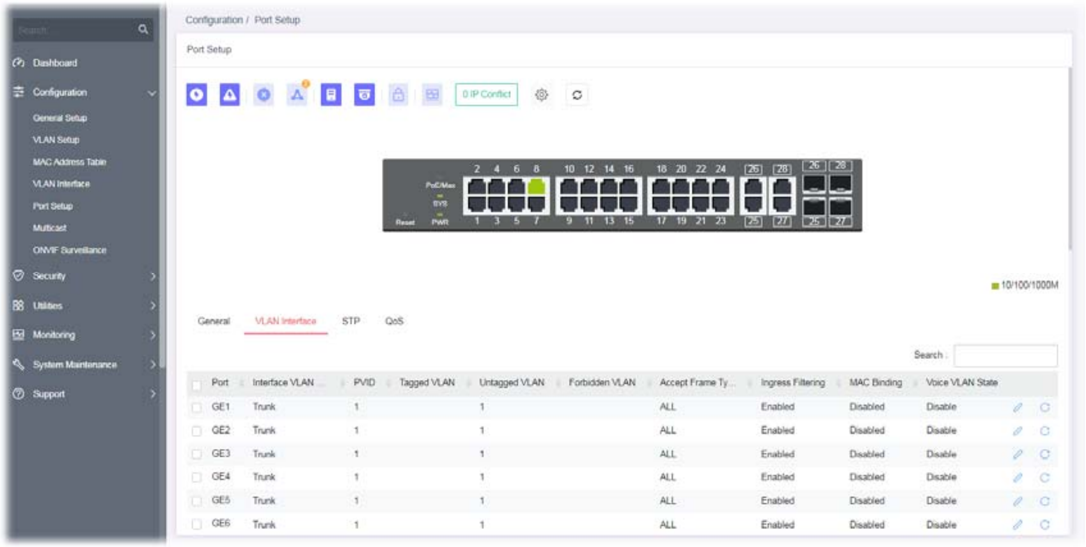
This page allows a user to configure interface (GE) settings related to VLAN.

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.



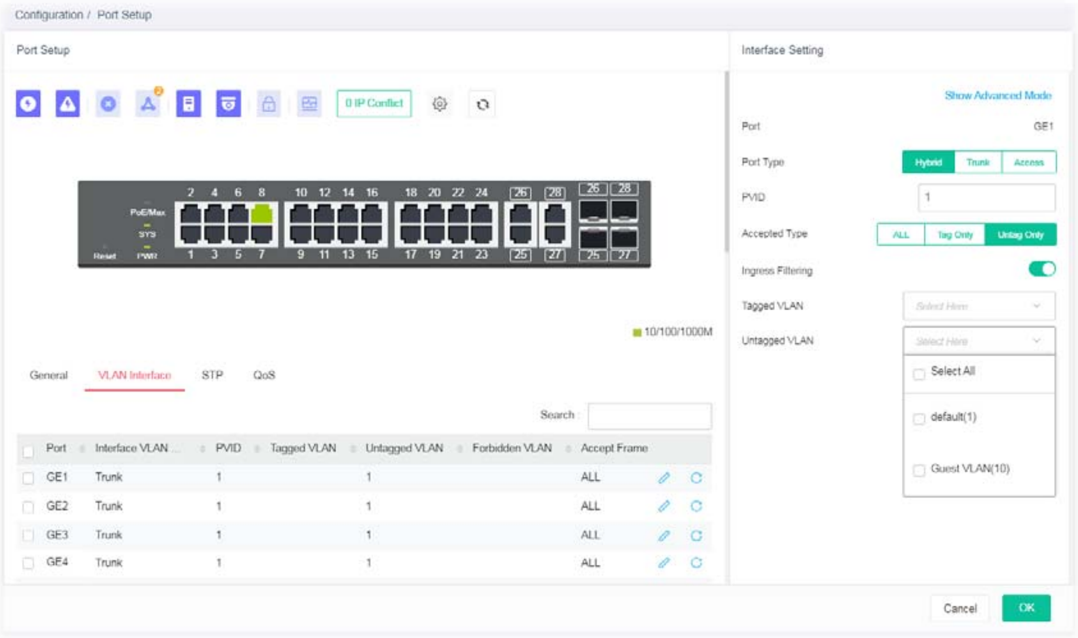
☐	Port	Interface VLAN ...	PVID	Tagged VLAN	Untagged VLAN	Forbidden VLAN	Accept Frame Ty...	Ingress Filtering	MAC Binding	Voice VLAN State
☐	GE1	Trunk	1		1		ALL	Enabled	Disabled	Disable
☐	GE2	Trunk	1		1		ALL	Enabled	Disabled	Disable
☐	GE3	Trunk	1		1		ALL	Enabled	Disabled	Disable
☐	GE4	Trunk	1		1		ALL	Enabled	Disabled	Disable
☐	GE5	Trunk	1		1		ALL	Enabled	Disabled	Disable
☐	GE6	Trunk	1		1		ALL	Enabled	Disabled	Disable

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.
✎	Click it to modify the VLAN interface settings.
↻	Clear current settings and return to factory default settings.

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



□	Port	Interface VLAN ...	PVID	Tagged VLAN	Untagged VLAN	Forbidden VLAN	Accept Frame		
□	GE1	Trunk	1		1		ALL	✎	↻
□	GE2	Trunk	1		1		ALL	✎	↻
□	GE3	Trunk	1		1		ALL	✎	↻
□	GE4	Trunk	1		1		ALL	✎	↻

Port: GE1

Port Type: [✓ Hybrid] Trunk Access

PVID: 1

Accepted Type: ALL Tag Only [✓ Untag Only]

Ingress Filtering: ●

Tagged VLAN: Select Here

Untagged VLAN: Select Here
- □ Select All
- □ default(1)
- □ Guest VLAN(10)

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. **Hybrid** – Support all functions as defined in IEEE 802.1Qspecification. **Access** – Accepts only untagged frames and join an untagged VLAN. **Trunk** - An untagged member of one VLAN at most, and is a tagged member of zero or more VLANs.
PVID	A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines. For port under **Access** Mode, VLAN ID provided as PVID would automatically be selected as the untagged VLAN.
Accepted Type	Specify the acceptable-frame-type of the specified interfaces. It's only available with Hybrid mode. **All** - Accept frames regardless it's tagged with 802.1q or not. **Tag Only** - Accept frames only with 802.1q tagged. **Untag Only** - Accept frames untagged.

Ingress Filtering	Enable the ingress filtering to filter out any packets not belong to any VLAN members of this port. It is enabled automatically while operating in Access and Trunk mode.
Tagged VLAN	Specify the VLAN profile tagged in the VLAN.
Untagged VLAN	Specify the VLAN profile untagged in the VLAN.
Below shows settings for Advanced Mode	
Forbidden VLAN	The selected GE port only allows default VLAN packet to pass through. **Enable / Disable** – Click the toggle to enable / disable the LAN port(s) as forbidden VLAN port. ● - means “Enable”. ○ - 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. **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. ● - means “Enable”. ○ - means “Disable”.
Surveillance VLAN Mode	Select port surveillance VLAN mode. **Auto** - Surveillance VLAN auto detect packets that match OUI table and add received port into surveillance VLAN ID tagged member. **Manual** - User need add interface to VLAN ID tagged member manually.
Surveillance VLAN QoS Policy	Select port QoS Policy mode. **Video Packet** - QoS attributes are applied to packets with OUI in the source MAC address. **All** - QoS attributes are applied to packets that are classified to the Surveillance VLAN.
MAC VLAN Binding	Enable/disable the function of MAC VLAN Binding.
+Add	Click to create a new MAC VLAN profile.

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

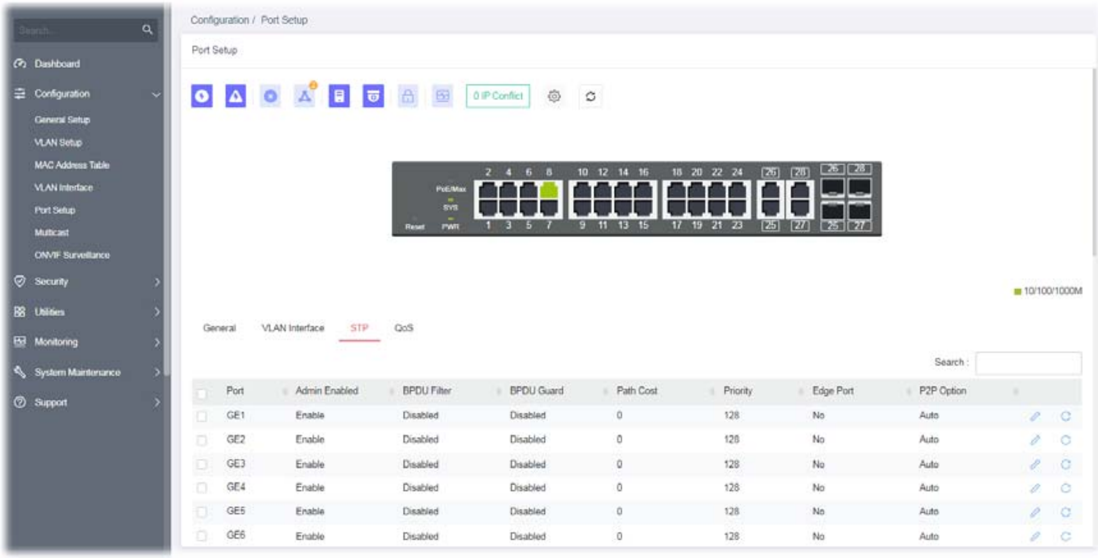
II-5-3 STP

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.

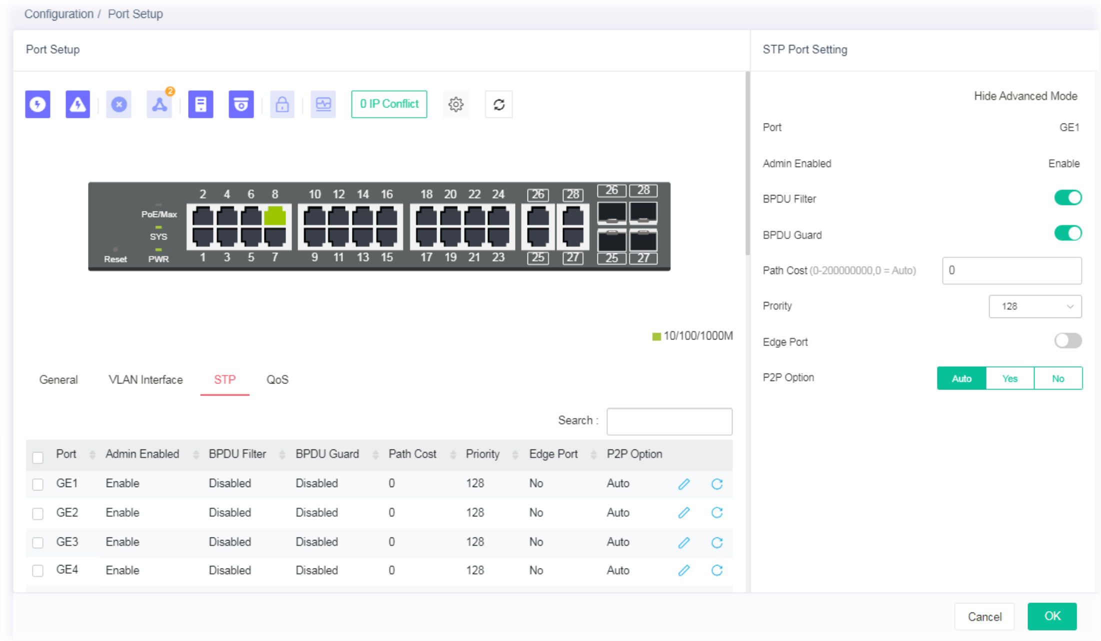


□	Port	Admin Enabled	BPDU Filter	BPDU Guard	Path Cost	Priority	Edge Port	P2P Option		
□	GE1	Enable	Disabled	Disabled	0	128	No	Auto	✎	↻
□	GE2	Enable	Disabled	Disabled	0	128	No	Auto	✎	↻
□	GE3	Enable	Disabled	Disabled	0	128	No	Auto	✎	↻
□	GE4	Enable	Disabled	Disabled	0	128	No	Auto	✎	↻
□	GE5	Enable	Disabled	Disabled	0	128	No	Auto	✎	↻
□	GE6	Enable	Disabled	Disabled	0	128	No	Auto	✎	↻

Available settings are explained as follows:

Item	Description
Port	Displays the LAN port number (GE1 to GE28).
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.
✎	Click it to modify the STP port setting.
↻	Clear current settings and return to factory default settings.

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



Configuration / Port Setup

Port Setup

0 IP Conflict

🟩 10/100/1000M

General | VLAN Interface | STP | QoS

Search :

	Port	Admin Enabled	BPDU Filter	BPDU Guard	Path Cost	Priority	Edge Port	P2P Option		
□	GE1	Enable	Disabled	Disabled	0	128	No	Auto	✎	↻
□	GE2	Enable	Disabled	Disabled	0	128	No	Auto	✎	↻
□	GE3	Enable	Disabled	Disabled	0	128	No	Auto	✎	↻
□	GE4	Enable	Disabled	Disabled	0	128	No	Auto	✎	↻

STP Port Setting

Hide Advanced Mode

Port	GE1
Admin Enabled	Enable
BPDU Filter	⬤
BPDU Guard	⬤
Path Cost (0-200000000,0 = Auto)	0
Prority	128
Edge Port	○
P2P Option	[✓ Auto] Yes No

Cancel OK

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. ⬤ - means "Enable". ○ - means "Disable".
BPDU Guard	BPDU Guard further protects your switch by turning this port into error state and shutdown if any BPDU received from this port. Check it to enable such function.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost. Entering 0 means the switch will automatically assign a value.
Priority	Specify a priority value for the switch. The smaller the priority value, the higher the priority and greater chance of becoming the root.
Edge Port	In the edge mode, the interface would be put into the Forwarding state immediately upon link up. If the edge mode is enabled for the interface and there are BPDUs received on the interface, the loop might be occurred in the short time before the STP state change. Click the toggle to enable / disable the function.
P2P Option	● **Auto –** VigorSwitch determines the STP of link type for this port

	automatically. ● **Yes –** It means the STP of link type on this port is full-duplex and directly connect to another switch or host. ● **No -** It means the STP of link type on this port is “not” full-duplex and “does not” directly connect to another switch or host.

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

II-5-4 QoS

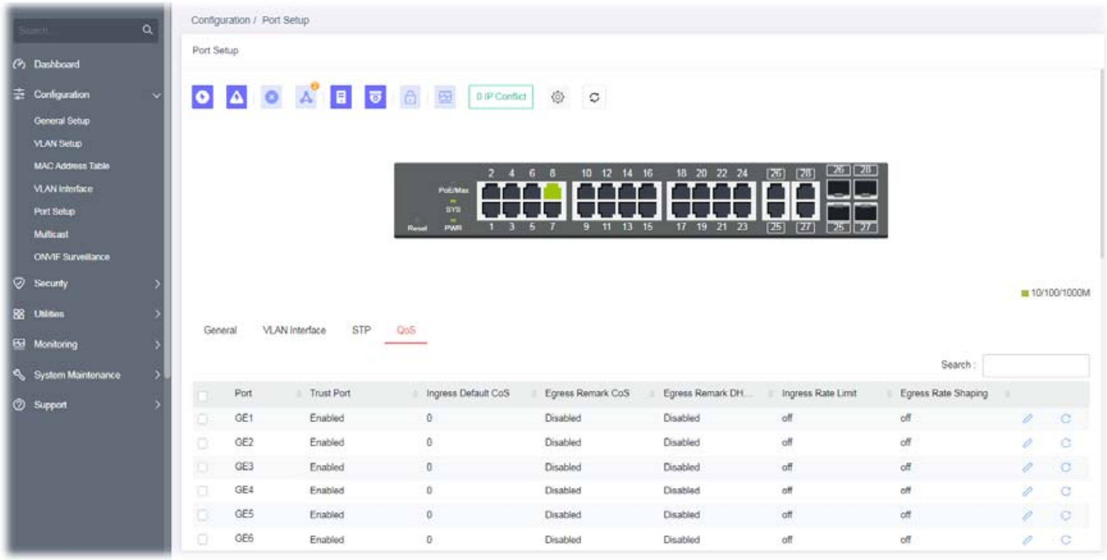
This page is used to configure port settings for QoS. The configuration result for each port will be displayed on the table listed on the lower side of this web page.

Ingress Rate Limit

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

Egress Shaping Rate

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

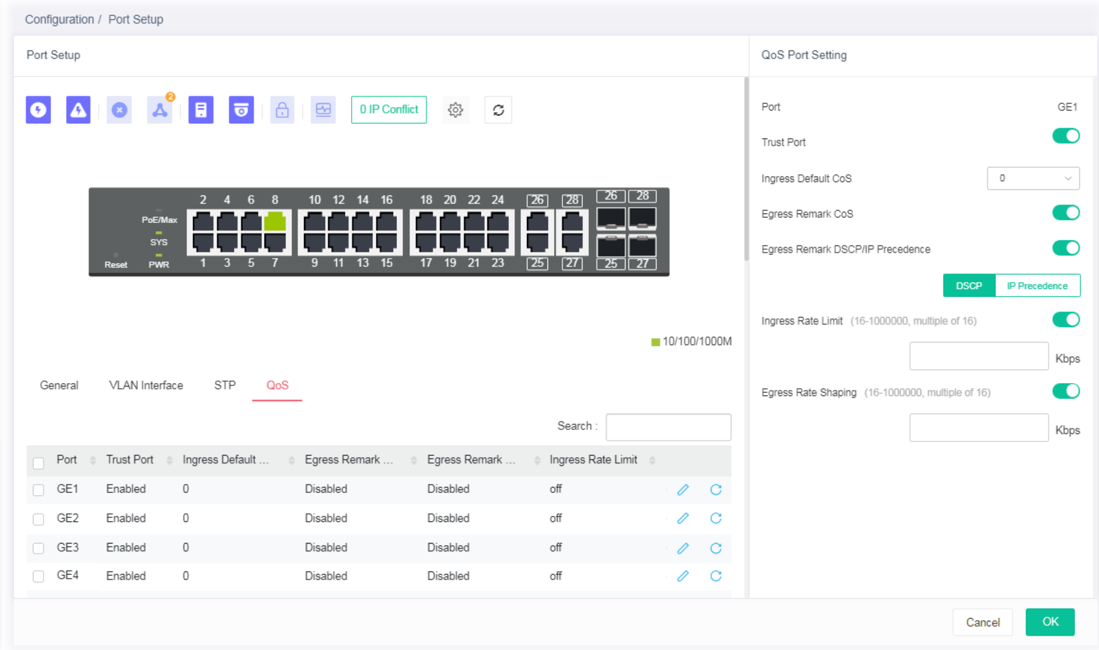


☐	Port	Trust Port	Ingress Default CoS	Egress Remark CoS	Egress Remark DH...	Ingress Rate Limit	Egress Rate Shaping
☐	GE1	Enabled	0	Disabled	Disabled	off	off
☐	GE2	Enabled	0	Disabled	Disabled	off	off
☐	GE3	Enabled	0	Disabled	Disabled	off	off
☐	GE4	Enabled	0	Disabled	Disabled	off	off
☐	GE5	Enabled	0	Disabled	Disabled	off	off
☐	GE6	Enabled	0	Disabled	Disabled	off	off

Available settings are explained as follows:

Item	Description
Port	Displays the port profiles (GE1 to GE28).
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.
✎	Click it to modify the QoS 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.



Configuration / Port Setup

Port Setup

0 IP Conflict

10/100/1000M

General VLAN Interface STP QoS

Search :

Port	Trust Port	Ingress Default ...	Egress Remark ...	Egress Remark ...	Ingress Rate Limit
GE1	Enabled	0	Disabled	Disabled	off
GE2	Enabled	0	Disabled	Disabled	off
GE3	Enabled	0	Disabled	Disabled	off
GE4	Enabled	0	Disabled	Disabled	off

QoS Port Setting

Port GE1

Trust Port ●

Ingress Default CoS 0

Egress Remark CoS ●

Egress Remark DSCP/IP Precedence ●

DSCP IP Precedence

Ingress Rate Limit (16-1000000, multiple of 16) ●

Kbps

Egress Rate Shaping (16-1000000, multiple of 16) ●

Kbps

Cancel OK

Available settings are explained as follows:

Item	Description
QoS Port Setting	
Port	Displays the port profiles (GE1 to GE28).
Trust Port	**Enable / Disable** – Click the toggle to enable / disable this function. ● - Traffic will follow trust mode in general setting. ○ - No QoS service for this port.
Ingress Default CoS	Specify the default CoS priority value for those ingress frames without given trust QoS tag (802.1q/DSCP/IP Precedence, depending on configuration).
Egress Remark CoS	**Enable / Disable** – Click the toggle to enable / disable this function.
Egress Remark DSCP/IP Precedence	Click the toggle to enable / disable this function. **DSCP** - Egress traffic will be marked with DSCP value according to the Queue to DSCP mapping table. **IP Precedence** - Egress traffic will be marked with IP Precedence value according to the Queue to IP Precedence mapping table.
Ingress Rate Limit	The ingress rate limit is the number of bits per second that can be received from the ingress interface. Excess bandwidth above this limit is discarded. Click the toggle to enable / disable this function. Enter the rate value,<16-1000000>,unit:16 Kbps.
Egress Rate Shaping	The egress rate limit is the number of bits per second that can be received from the egress interface. Excess bandwidth above this limit is discarded.

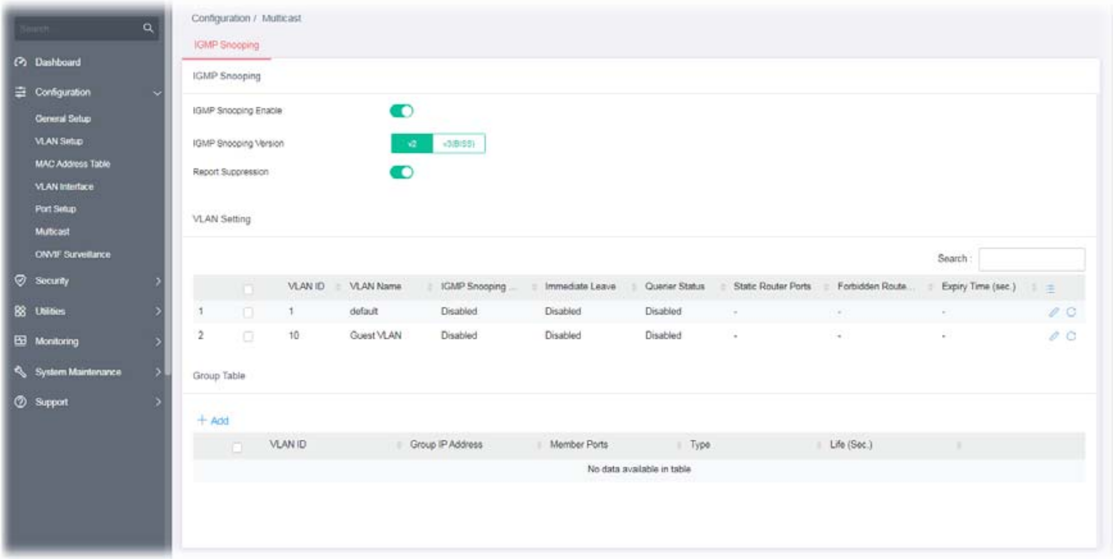
	Click the toggle to enable / disable this function. Enter the rate value,<16-1000000>,unit:16 Kbps.

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).



Configuration / Multicast

IGMP Snooping

IGMP Snooping

IGMP Snooping Enable

IGMP Snooping Version: v2 | v3(BISS)

Report Suppression

VLAN Setting

Search :

	□	VLAN ID	VLAN Name	IGMP Snooping ...	Immediate Leave	Querier Status	Static Router Ports	Forbidden Route...	Expiry Time (sec.)
1	□	1	default	Disabled	Disabled	Disabled	-	-	-
2	□	10	Guest VLAN	Disabled	Disabled	Disabled	-	-	-

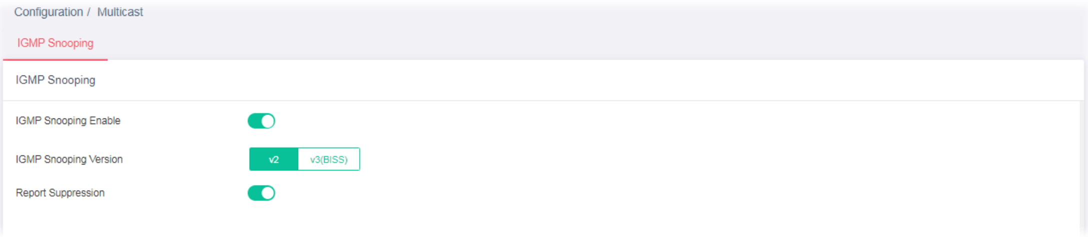
Group Table

+ Add

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

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.



Configuration / Multicast

IGMP Snooping

IGMP Snooping

IGMP Snooping Enable

IGMP Snooping Version: v2 | v3(BISS)

Report Suppression

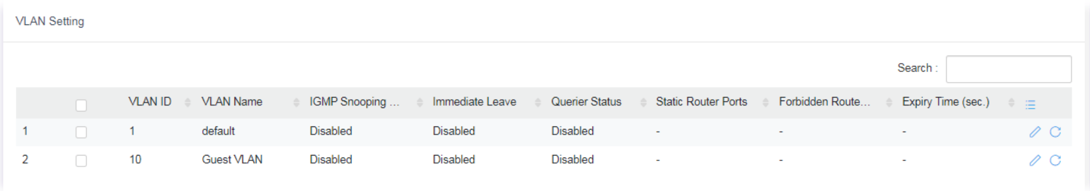
Available settings are explained as follows:

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

	v3 - Support v3 basic and v2.
Report Suppression	It allows the switch to handle IGMP reports between router and host, suppressing bandwidth used by IGMP. **Enable / Disable** – Click the toggle to enable / disable this function. ● - means "Enable". ○ - means "Disable".

II-6-2 VLAN Setting

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



VLAN Setting

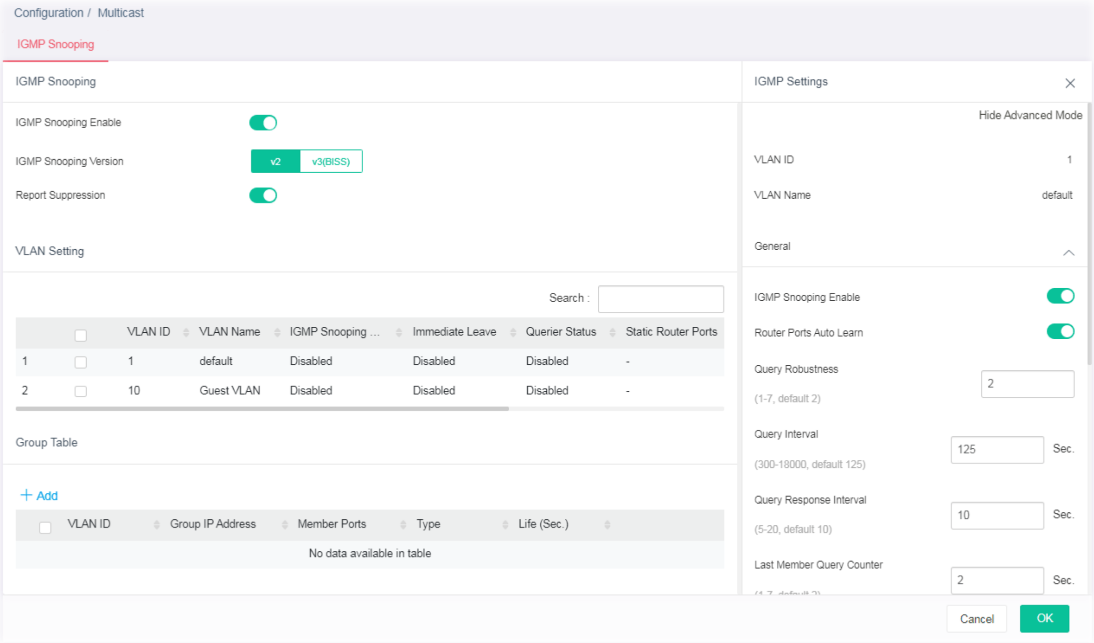
Search :

	□	VLAN ID	VLAN Name	IGMP Snooping ...	Immediate Leave	Querier Status	Static Router Ports	Forbidden Route...	Expiry Time (sec.)	☰
1	□	1	default	Disabled	Disabled	Disabled	-	-	-	✎ ↻
2	□	10	Guest VLAN	Disabled	Disabled	Disabled	-	-	-	✎ ↻

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.



Configuration / Multicast

IGMP Snooping

IGMP Snooping

IGMP Snooping Enable ●

IGMP Snooping Version [✓ v2] v3(BISS)

Report Suppression ●

VLAN Setting

Search :

	□	VLAN ID	VLAN Name	IGMP Snooping ...	Immediate Leave	Querier Status	Static Router Ports
1	□	1	default	Disabled	Disabled	Disabled	-
2	□	10	Guest VLAN	Disabled	Disabled	Disabled	-

Group Table

+ Add

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

IGMP Settings

Hide Advanced Mode

VLAN ID 1

VLAN Name default

General

IGMP Snooping Enable ●

Router Ports Auto Learn ●

Query Robustness (1-7, default 2) 2

Query Interval (300-18000, default 125) 125 Sec.

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

Last Member Query Counter 2 Sec.

Cancel OK

Available settings are explained as follows:

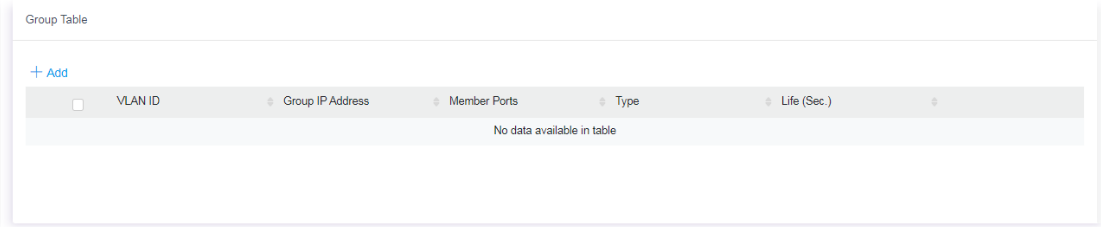
Item	Description
IGMP Setting	
Show / Hide Advanced Mode	Click to display or hide the advanced settings.
VLAN ID	Displays the VLAN ID number of the VLAN profile.
VLAN Name	Displays the name of the VLAN profile.
General	**IGMP Snooping Enable** – Click the toggle to enable / disable this IGMP snooping function. ● - means “Enable”. ○ - 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. In **Advanced Mode,** **Querier Version** - Set the IGMP snooping version. ● **v2 -** Only support process IGMP v2 packet. ● **v3** - Support v3 basic and v2. For maximum compatibility, it is suggested to use querier version lower than IGMP snooping version, for there is possible network mixed with IGMP v2/v3 client and v2 query message is widely understandable for those clients.
IGMP Static Group	The IGMP static group is allowed to assign a VLAN/port as a specific IPv4 multicast member. Every IPv4 multicast stream that belongs to the specified group IP address will be forwarded to the specified port/VLAN member. **Enable / Disable** – Click the toggle to enable / disable this function. **+Add** - Click to create a new group. ● **Group IP Address** - Specify the IPv4 multicast address you wish to assign for the static group (defined in VLAN ID). ● **Member Ports** - Specify the port(s) that static group with given IPv4 multicast address shall include.

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

II-6-3 Group Table

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



Group Table

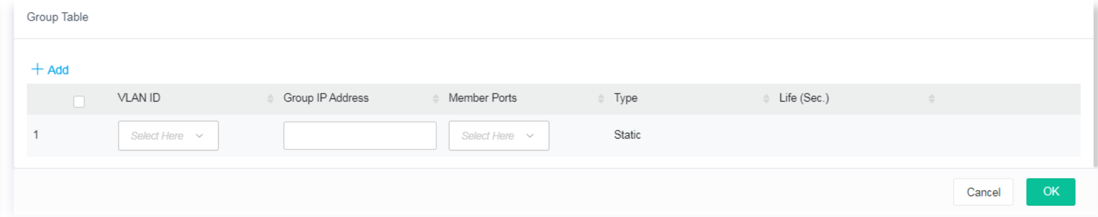
+ Add

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

Available settings are explained as follows:

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

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



Available settings are explained as follows:

Item	Description
VLAN ID	Specify a VLAN profile as IGMP Static Group.
Group IP Address	It is an identifier for the group member. Packets sent to such address will be transferred to all interfaces defined in Member Ports. Specify the IPv4 multicast address you wish to assign for the static group (defined in VLAN ID).
Member Ports	Specify the port(s) that static group with given IPv4 multicast address shall include.

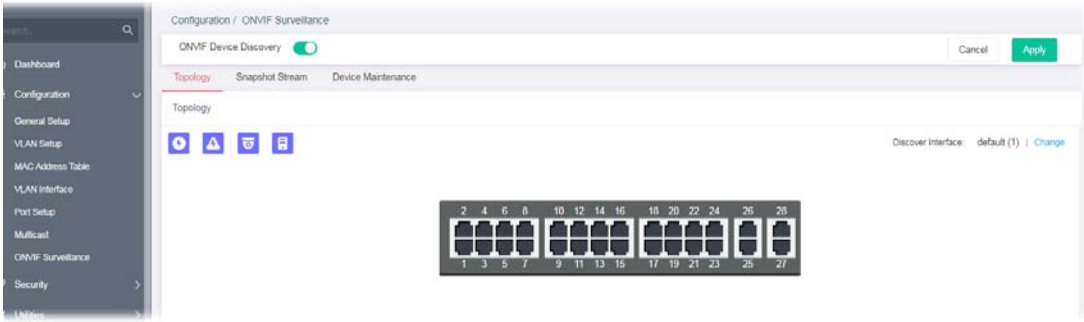
After finishing this web page configuration, please click **OK** to save the settings.

II-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:

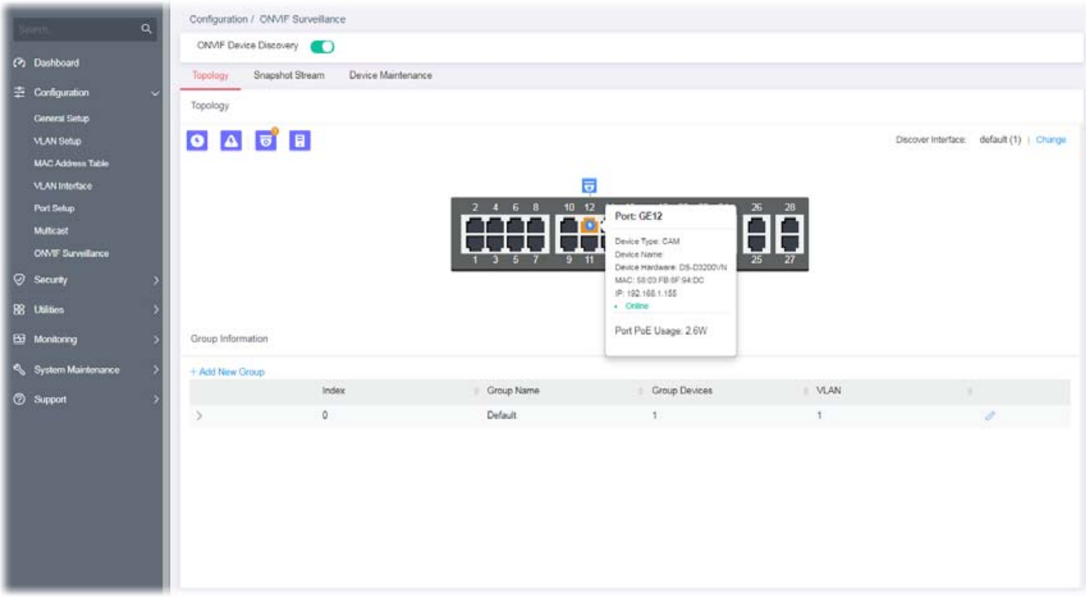
- Integrate the ONVIF device and surveillance network
- Centralize management of IP video products
- View video images directly on VigorSwitch WUI
- Offer remote IP video products maintenance



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.

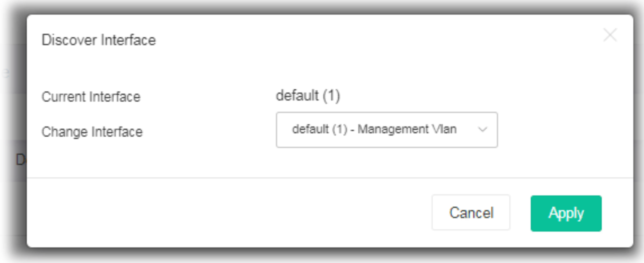


Port: GE12
Device Type: CAM
Device Name:
Device Hardware: DS-D3200VN
MAC: 58:03:FB:8F:94:DC
IP: 192.168.1.155
Online
Port PoE Usage: 2.6W

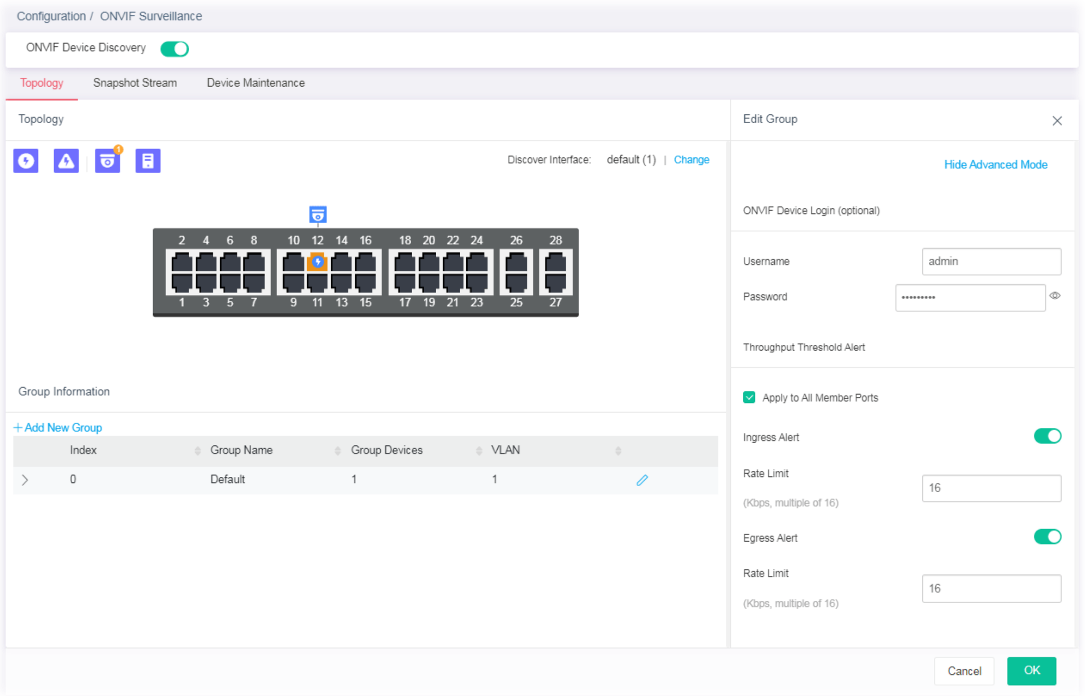
Index	Group Name	Group Devices	VLAN
0	Default	1	1

Available settings are explained as follows:

Item	Description

	Camera - Displays the number of IP camera(s) connected to VigorSwitch. The panel sketch on the screen will display which LAN port that the IP camera connected. **NVR -** Displays the number of NVR device(s) connected to VigorSwitch. The panel sketch on the screen will display which LAN port that the NVR device connected.
Change	VigorSwitch will detect the ONVIF device based on the interface selected.  Discover Interface Current Interface: default (1) Change Interface: default (1) - Management Vlan Cancel Apply
+Add New Group	A group can contain one (IP camera or NVR, as group leader) to several devices (IP cameras as group devices). Click to create a new group for managing multiple devices.
Index	Displays the index number of the group profile.
Group Name	Displays the name of the group profile.
Group Devices	Displays the number of the devices grouped under this profile.
VLAN	Displays the VLAN profile.
✎	Click it to modify the group setting.

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



Configuration / ONVIF Surveillance

ONVIF Device Discovery

Topology | Snapshot Stream | Device Maintenance

Topology

Discover Interface: default (1) | Change

Group Information

+ Add New Group

	Index	Group Name	Group Devices	VLAN	
>	0	Default	1	1	✎

Edit Group

Hide Advanced Mode

ONVIF Device Login (optional)

Username: admin

Password: ••••••••

Throughput Threshold Alert

☑ Apply to All Member Ports

Ingress Alert: ●

Rate Limit (Kbps, multiple of 16): 16

Egress Alert: ●

Rate Limit (Kbps, multiple of 16): 16

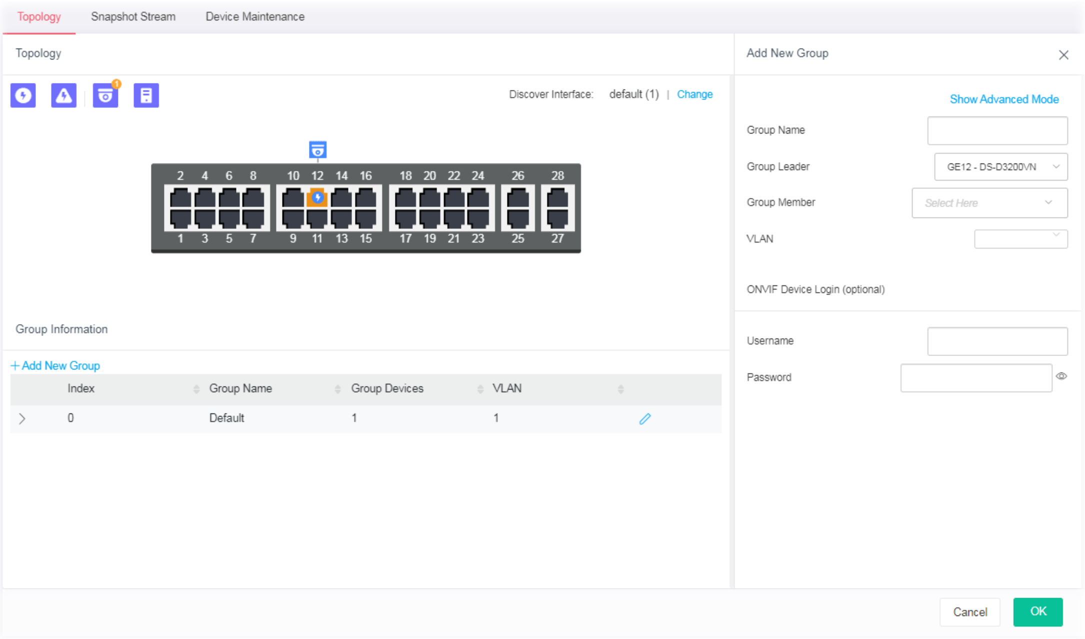
Cancel OK

Available settings are explained as follows:

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

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

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



Discover Interface: default (1)

Group Information

+ Add New Group

Index	Group Name	Group Devices	VLAN
0	Default	1	1

Add New Group

Group Name

Group Leader: GE12 - DS-D3200VN

Group Member: Select Here

VLAN

ONVIF Device Login (optional)

Username

Password

Available settings are explained as follows:

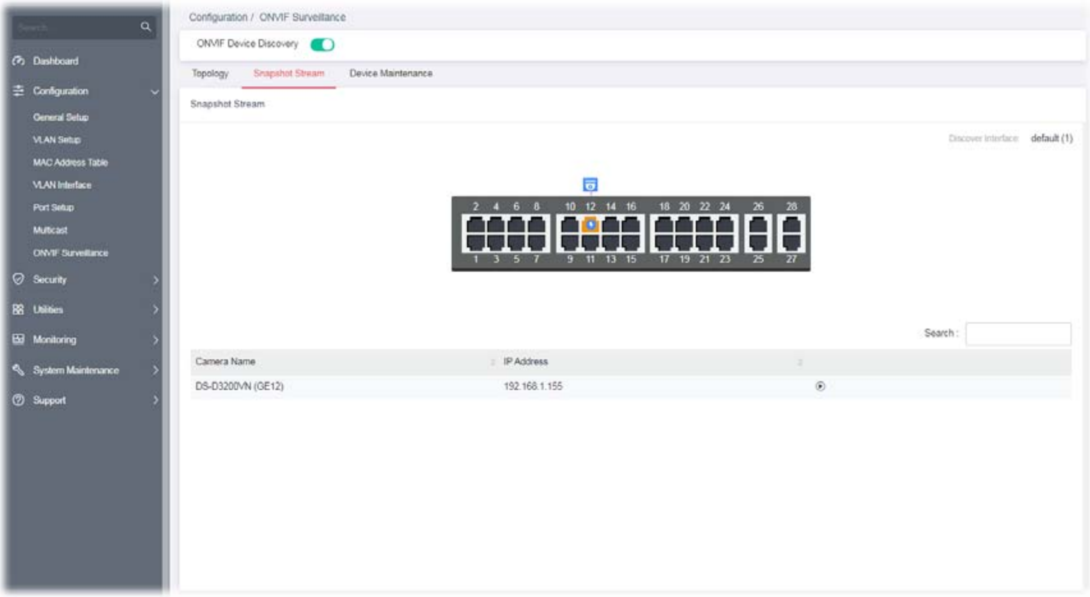
Item	Description
Add New Group	
Show / Hide Advanced Mode	Click to display or hide the advanced settings.
Group Name	Enter the name of a group.
Group Leader	The system will detect the NVR or IP cameras, and list them on the field of NVR or Group Leader.
Group Member	This field lists all devices (IP cameras) 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. In the entire ONVIF Surveillance menu, VigorSwitch will input this value in advanced and retrieve data. System administrator can access the IP device in which the username and password are as same as the default values. However, you can also input another username/password manually if the IP device username/password is different from the one you enter in Default Username/Default Password.
Throughput Threshold Alert	
Apply to All Member Ports	Check the box to apply the throughput threshold setting to all member ports.
Ingress Alert	Toggle the switch to enable the function. Set the ingress limit value. When the incoming traffic (packet) of the GE port reaches the limit, the Vigor System will send an alert email to the system administrator. **Rate Limit** - Enter the ingress rate as a threshold to send mail alert.
Egress Alert	Toggle the switch to enable the function. Set the egress limit value. When the incoming traffic (packet) of the GE port reaches the limit,

	the Vigor System will send an alert email to the system administrator. **Rate Limit** - Enter the ingress rate as a threshold to send mail alert.

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

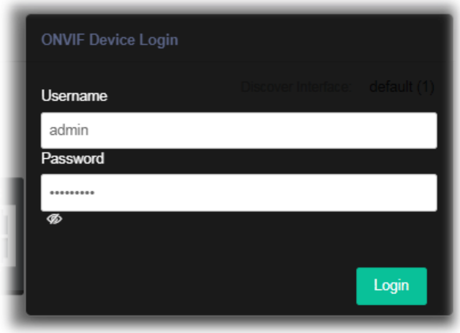
II-7-2 Snapshot Stream

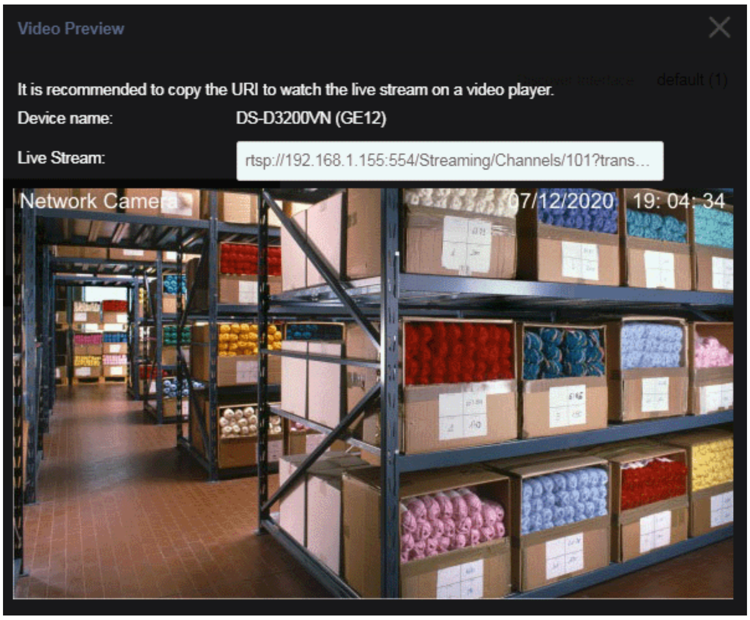
This page can offer a real-time video of specified IP camera for monitoring and control environments.



Camera Name	IP Address	
DS-D3200VN (GE12)	192.168.1.155	▶

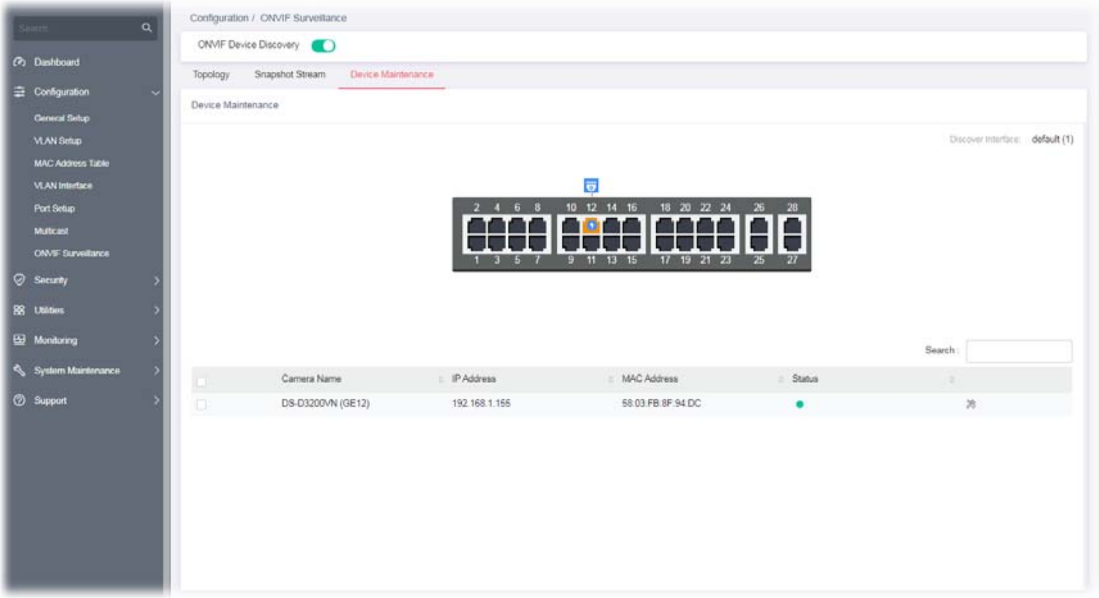
Available settings are explained as follows:

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.  ONVIF Device Login Username: admin Password: ········· Login **Usename / Password** - The default username/password will be input if it is configured on the Topology page. However, if the default input is not the correct username/password, enter the correct one of the IP camera instead. **Login** - Click it to authenticate the username and password for the specified IP camera.

	A pop-up window (Video Preview) appears to display a live image on the screen.  Video Preview It is recommended to copy the URI to watch the live stream on a video player. Device name: DS-D3200VN (GE12) Live Stream: rtsp://192.168.1.155:554/Streaming/Channels/101?trans...

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.



ONVIF Device Discovery: on

Device Maintenance

Discover Interface: default (1)

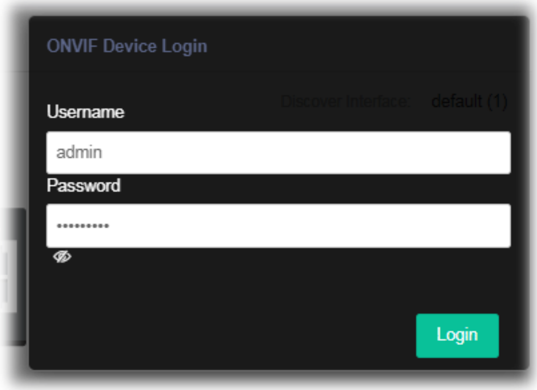
□	Camera Name	IP Address	MAC Address	Status	
□	DS-D3200VN (GE12)	192.168.1.155	58:03:FB:8F:94:DC	●	

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.



ONVIF Device Login

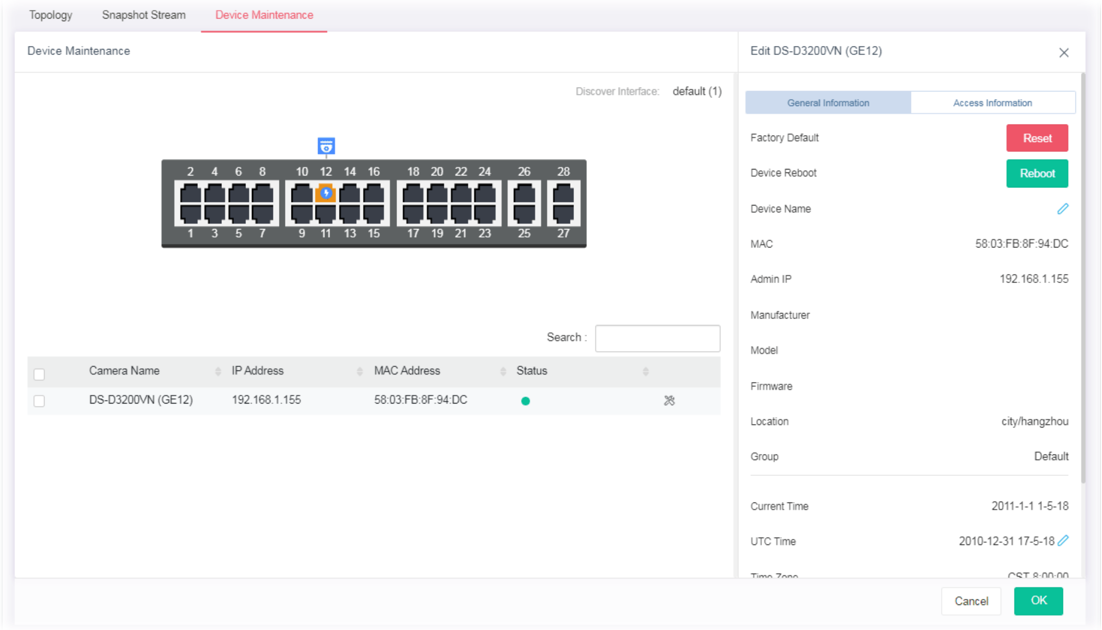
Username

admin

Password

•••••••••

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



Device Maintenance

Discover Interface: default (1)

Search :

□	Camera Name	IP Address	MAC Address	Status	
□	DS-D3200VN (GE12)	192.168.1.155	58:03:FB:8F:94:DC	●	⚒

Edit DS-D3200VN (GE12)

Factory Default	Reset
Device Reboot	Reboot
Device Name	✎
MAC	58:03:FB:8F:94:DC
Admin IP	192.168.1.155
Manufacturer	
Model	
Firmware	
Location	city/hangzhou
Group	Default
Current Time	2011-1-1 1-5-18
UTC Time	2010-12-31 17-5-18 ✎
Time Zone	CST 8:00:00

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. ● - means “Enable”. ○ - means “Disable”. **Failure Action** - Configure the power behavior for each LAN port. ● **Power Cycle -** Once the device is offline, Vigorswitch will power off the device and then power on the device again. ● **Power Off** - When the device is offline, power off the device immediately. ● **Nothing** - When the device is offline, no action will be performed. **Note**: When a PoE hub connecting to LAN port of VigorSwitch, the power behavior (on/off) to the PoE hub also will apply to all the devices connecting to the PoE hub. **Mail Alert** - Click the toggle to enable / disable this function. When the device is offline, Vigor system will send an alert mail to notify the recipient. ● **With Snapshot** - If enabled, the switch will try to get snapshot from the device per half hour. Before using this feature, set the group authentication information when adding group or configure Default Username/Password in the Topology page first. When the device is offline, no action will be performed.
Access Information	
Mode	Change the connection mode for this device. **Static -** When it is selected, you have to enter value for network setting manually for the IP device. ● **IP Address** - Enter an IPv4 address for the IP device. ● **Prefix Length** - Specify the subnet mask for the IP address. ● **Gateway** - Enter the IPv4 address for the gateway. ● **DNS Server1/2** - Enter the IP address for primary / secondary DNS server. **DHCP -** When it is selected, the IP device will be assigned with the settings by the network's DHCP server automatically to access the Internet. ● **Hostname** - Display the hostname of the DHCP server.
Zero Configuration	Click the toggle to enable / disable this function. **Enable -** The network settings for the IP device will be configured automatically. **Disable -** The network settings for the IP device must be configured

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

This page is left blank.

Chapter III Security

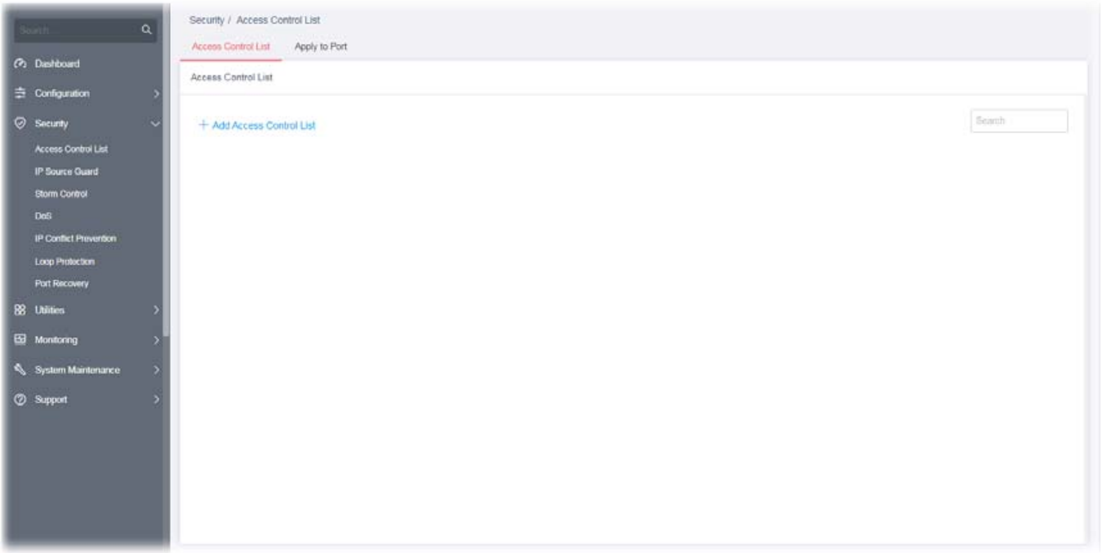
III-1 Access Control List

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.

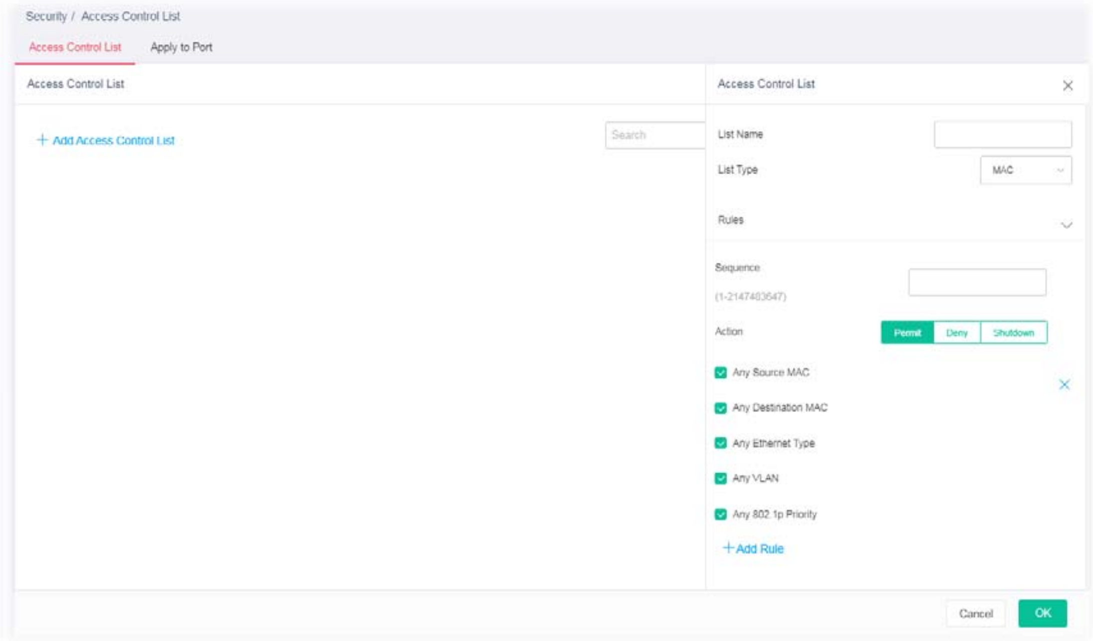
You may provide filtering/matching criteria for one or more packet characteristics (such as Source/Destination MAC, Ethertype, VLAN, 802.1p) for this ACE to identify the packet.

III-1-1 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.



Security / Access Control List

Access Control List | Apply to Port

Access Control List

+ Add Access Control List

Search

Access Control List

List Name

List Type: MAC

Rules

Sequence (1-2147483647)

Action: Permit | Deny | Shutdown

☑ Any Source MAC

☑ Any Destination MAC

☑ Any Ethernet Type

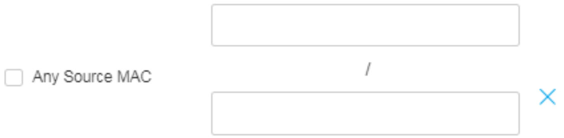
☑ Any VLAN

☑ Any 802.1p Priority

+Add Rule

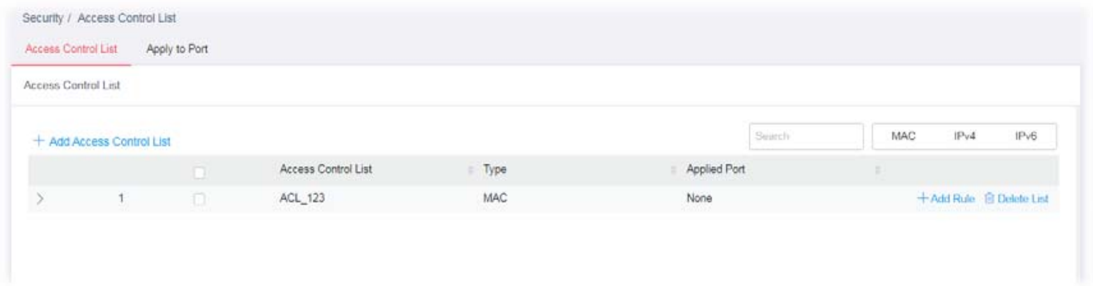
Cancel | OK

Available settings are explained as follows:

Item	Description
Access Control List	
List Name	Enter a name for creating a new ACL profile.
List Type	Specify the filtering type (MAC/IPv4/IPv6).
Rules	
Sequence	Assign a sequence number to this ACE. The sequence is used to identify which one of ACEs in an ACL is firstly used to match ingress packets. The switch port bound with an ACL use the contained ACE rules, start with the one with lower sequence number to match the packet first.
Action	Select the action applied to the packet matched this ACE. Permit or deny the packets into switch core, or shutdown the port for stopping further transmission. ● **Permit** ● **Deny** ● **Shutdown**
Any Source MAC	If disabled, please enter IP address with the subnet mask.  □ Any Source MAC /
Any Destination MAC	If disabled, please enter IP address with the subnet mask.
Any Ethernet Type	Specify Ethernet type for filtering. Select **Any Ethernet**. Or, enter the value with the format of “0x600 ~ 0xFFF”. □ Any Ethernet Type (0x600-0xFFFF)

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

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



Security / Access Control List

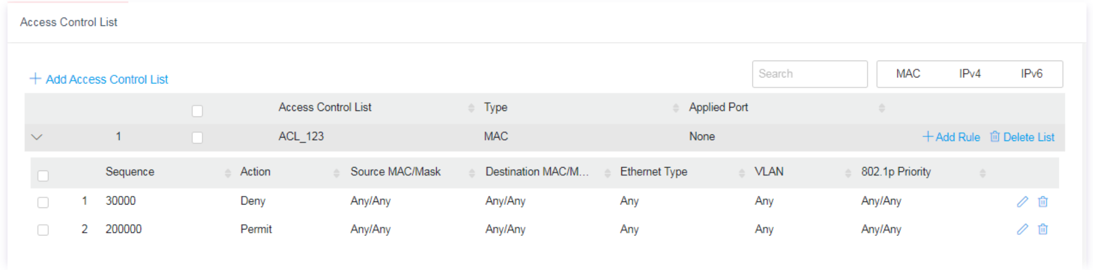
Access Control List | Apply to Port

Access Control List

+ Add Access Control List

Search | MAC | IPv4 | IPv6

			Access Control List	Type	Applied Port	
>	1	☐	ACL_123	MAC	None	+ Add Rule 🗑 Delete List



Access Control List

+ Add Access Control List

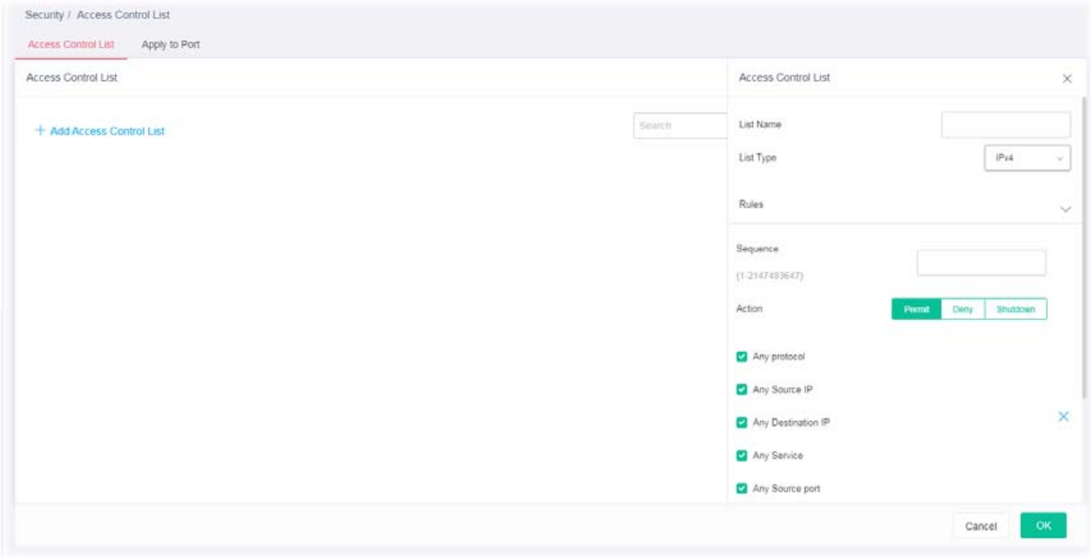
Search | MAC | IPv4 | IPv6

			Access Control List	Type	Applied Port	
∨	1	☐	ACL_123	MAC	None	+ Add Rule 🗑 Delete List

☐		Sequence	Action	Source MAC/Mask	Destination MAC/M...	Ethernet Type	VLAN	802.1p Priority	
☐	1	30000	Deny	Any/Any	Any/Any	Any	Any	Any/Any	✎ 🗑
☐	2	200000	Permit	Any/Any	Any/Any	Any	Any	Any/Any	✎ 🗑

List Type - IPv4

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



List Name

List Type IPv4

Sequence (1-2147483647)

Action Permit

☑ Any protocol

☑ Any Source IP

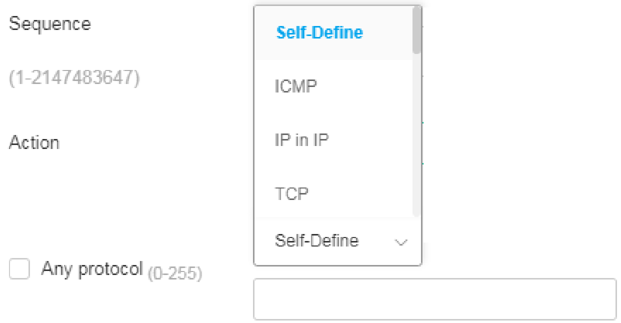
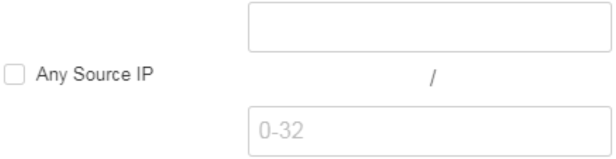
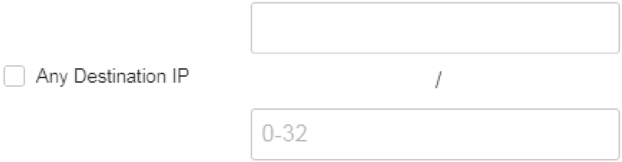
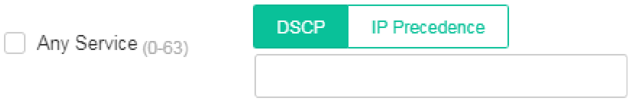
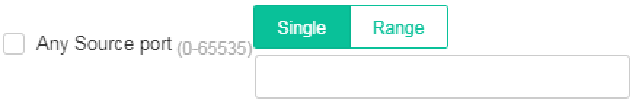
☑ Any Destination IP

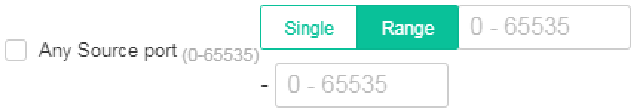
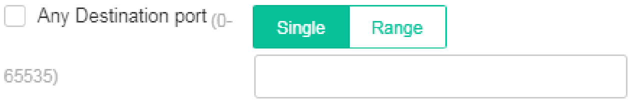
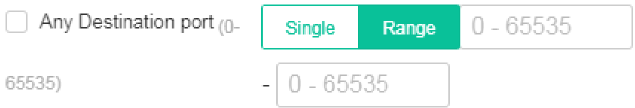
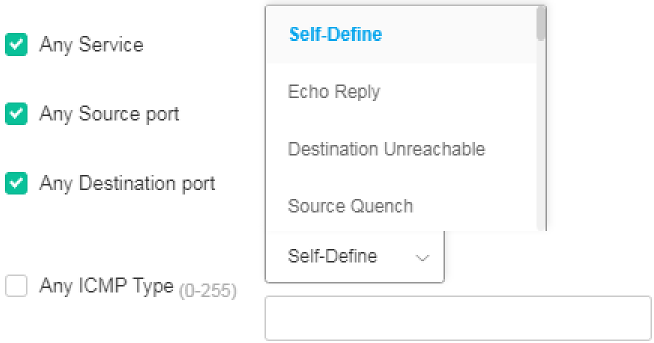
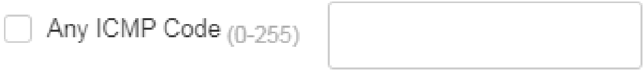
☑ Any Service

☑ Any Source port

Available settings are explained as follows:

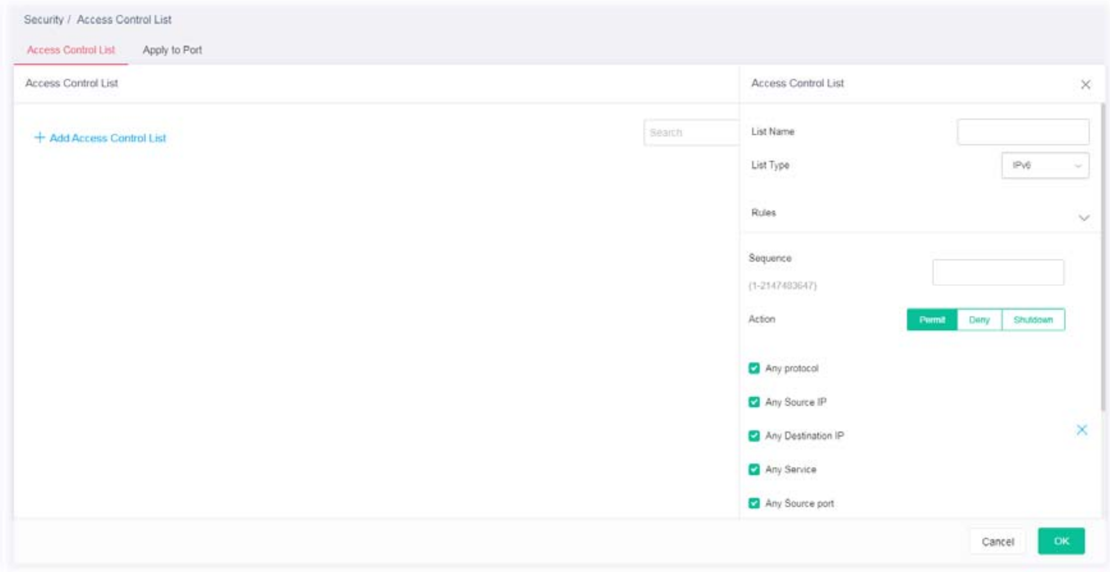
Item	Description
Access Control List	
List Name	Enter a name for creating a new ACL profile.
List Type	Specify the filtering type (IPv4).
Rules	
Sequence	Assign a sequence number to this ACE. The sequence is used to identify which one of ACEs in an ACL is firstly used to match ingress packets. The switch port bound with an ACL use the contained ACE rules, start with the one with lower sequence number to match the packet first.
Action	Select the action applied to the packet matched this ACE. Permit or deny the packets into switch core, or shutdown the port for stopping further transmission. ● **Permit** ● **Deny** ● **Shutdown**
Any Protocol	Specify the protocol for filtering. **Any Protocol** – Default setting. All packets will be filtered. **Self-Define** – Enter a number (0 – 255) to specify a protocol. For example, 1 means “Internet Control Message”; 6 means “Transmission Control”. **ICMP, IP in IP**,… – Choose one of the protocols (e.g., ICMP, IP in IP, TCP, EGP, IGP…) from the drop down list. Packets passing through the selected protocol will be filtered.

	 Sequence (1-2147483647) Action □ Any protocol (0-255) Self-Define ICMP IP in IP TCP Self-Define
Any Source IP	Specify the source IPv4 address for filtering. **Any Source IP** – Default setting. All packets will be filtered. Select Any Source IP. Or, enter the IP address to filter the packets coming from that address.  □ Any Source IP / 0-32
Any Destination IP	Specify the destination IPv4 address for filtering. **Any Destination IP** – Default setting. All packets will be filtered. Select Any Destination IP. Or, enter the IP address to filter the packets coming from that address.  □ Any Destination IP / 0-32
Any Service	**Any Service** – Default setting. All packets will be filtered. **DSCP** – All IP traffic is mapped to queues based on the DSCP field in the IP header. If traffic is not IP traffic, it is mapped to the lowest priority queue. **IP Precedence** - All IP traffic is mapped to queues based on the IP Precedence field in the IP header. If traffic is not IP traffic, it is mapped to the lowest priority queue.  □ Any Service (0-63) DSCP IP Precedence
Any Source Port	Specify the source port number for filtering the packets. **Any Source Port** – Default setting. All packets will be filtered. Select Any Source Port. Or, enter the port number. **Single** – Only the packets passing through the number defined here will be filtered.  □ Any Source port (0-65535) Single Range **Range** – Only the packets passing through the port range defined

	here will be filtered.  Any Source port (0-65535) Single Range 0 - 65535 - 0 - 65535
Any Destination Port	Specify the destination port number for filtering the packets. **Any Destination Port** – Default setting. All packets will be filtered. Select Any Destination Port. Or, enter the port number. **Single** – Only the packets passing through the number defined here will be filtered.  **Range** – Only the packets passing through the port range defined here will be filtered.  Any Destination port (0-65535) Single Range 0 - 65535 - 0 - 65535
Any ICMP Type	**Any ICMP Type** – Default setting. All packets will be filtered. **Echo Reply, Destination Unreachable….** – Choose one of the type (e.g., Destination Unreachable, Echo Reply, MLD Query….) from the drop down list. **Self-Define** – Specify a type number (0 – 255) for ICMP code. For example, 0 means "Echo Reply"; 254 means "RFC3692-style Experiment 2".  Any Service Any Source port Any Destination port Any ICMP Type (0-255) Self-Define Echo Reply Destination Unreachable Source Quench Self-Define
Any ICMP Code	ach ICMP type can be defined with different codes. For example, if you define ICMP Type as "3", then the available codes for Type 3 will be 0-15. **Any ICMP Code** – Default setting. All packets will be filtered. Select Any ICMP Code. Or, enter 0 to 255 based on the ICMP type specified. 
+Add Rule	Click it to create a new ACE rule. Each ACL profile can be added with 8 ACE rules.

List Type - IPv6

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



List Name

List Type: IPv6

Sequence (1-2147483647)

Action: Permit

☑ Any protocol

☑ Any Source IP

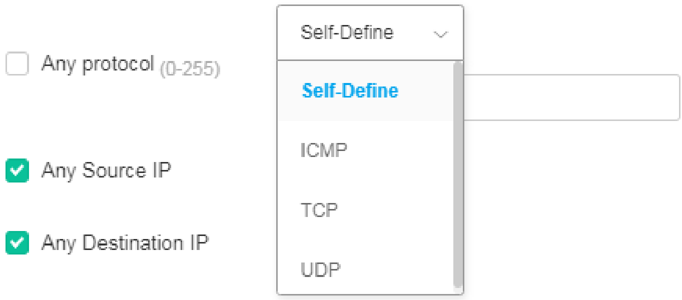
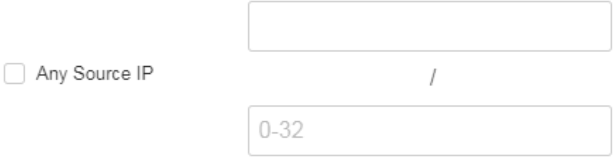
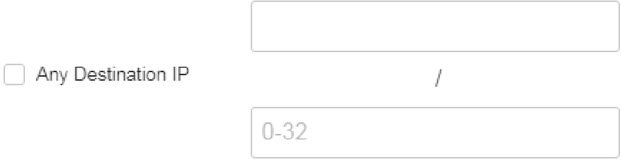
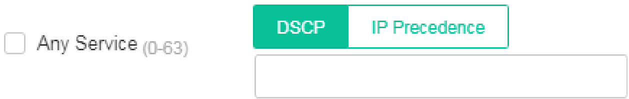
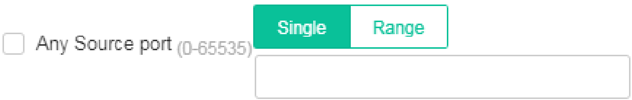
☑ Any Destination IP

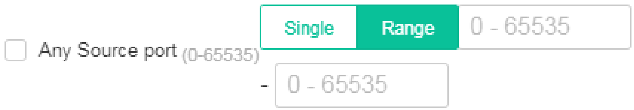
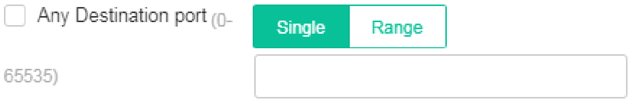
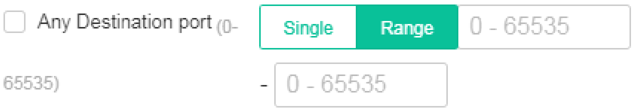
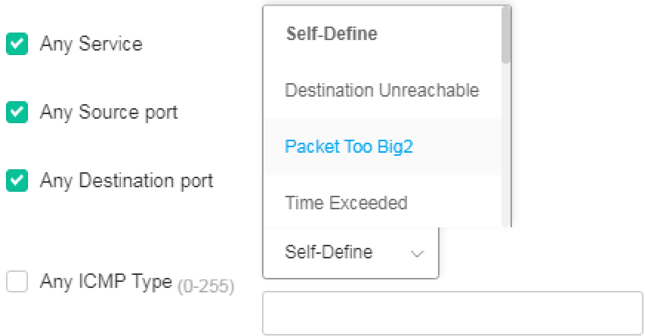
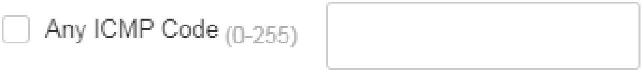
☑ Any Service

☑ Any Source port

Available settings are explained as follows:

Item	Description
Access Control List	
List Name	Enter a name for creating a new ACL profile.
List Type	Specify the filtering type (IPv6).
Rules	
Sequence	Assign a sequence number to this ACE. The sequence is used to identify which one of ACEs in an ACL is firstly used to match ingress packets. The switch port bound with an ACL use the contained ACE rules, start with the one with lower sequence number to match the packet first.
Action	Select the action applied to the packet matched this ACE. Permit or deny the packets into switch core, or shutdown the port for stopping further transmission. ● **Permit** ● **Deny** ● **Shutdown**
Any Protocol	Specify the protocol for filtering. **Any Protocol** – Default setting. All packets will be filtered. **Self-Define** – Enter a number (0 – 255) to specify a protocol. For example, 1 means “Internet Control Message”; 6 means “Transmission Control”. **ICMP, IP in IP**,… – Choose one of the protocol (e.g., ICMP, TCP, EGP…) from the drop down list. Packets passing through the selected protocol will be filtered.

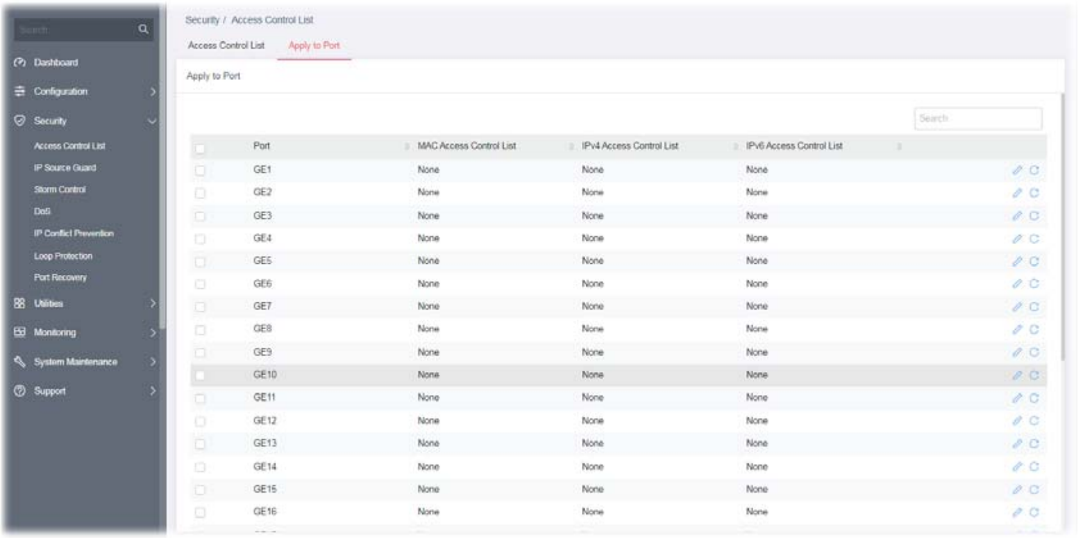
	 ☐ Any protocol (0-255) Self-Define Self-Define ICMP TCP UDP ☑ Any Source IP ☑ Any Destination IP
Any Source IP	Specify the source IPv6 address for filtering. **Any Source IP** – Default setting. All packets will be filtered. Select Any Source IP. Or, enter the IP address to filter the packets coming from that address.  ☐ Any Source IP / 0-32
Any Destination IP	Specify the destination IPv6 address for filtering. **Any Destination IP** – Default setting. All packets will be filtered. Select Any Destination IP. Or, enter the IP address to filter the packets coming from that address.  ☐ Any Destination IP / 0-32
Any Service	**Any Service** – Default setting. All packets will be filtered. **DSCP** – All IP traffic is mapped to queues based on the DSCP field in the IP header. If traffic is not IP traffic, it is mapped to the lowest priority queue. **IP Precedence** - All IP traffic is mapped to queues based on the IP Precedence field in the IP header. If traffic is not IP traffic, it is mapped to the lowest priority queue.  ☐ Any Service (0-63) DSCP IP Precedence
Any Source Port	Specify the source port number for filtering the packets. **Any Source Port** – Default setting. All packets will be filtered. Select Any Source Port. Or, enter the port number. **Single** – Only the packets passing through the number defined here will be filtered.  ☐ Any Source port (0-65535) Single Range **Range** – Only the packets passing through the port range defined

	here will be filtered.  □ Any Source port (0-65535) Single Range 0 - 65535 - 0 - 65535
Any Destination Port	Specify the destination port number for filtering the packets. **Any Destination Port** – Default setting. All packets will be filtered. Select Any Destination Port. Or, enter the port number. **Single** – Only the packets passing through the number defined here will be filtered.  **Range** – Only the packets passing through the port range defined here will be filtered.  □ Any Destination port (0-65535) Single Range 0 - 65535 - 0 - 65535
Any ICMP Type	**Any ICMP Type** – Default setting. All packets will be filtered. **Echo Reply, Destination Unreachable….** – Choose one of the type (e.g., Destination Unreachable, Echo Reply, MLD Query….) from the drop down list. **Self-Define** – Specify a type number (0 – 255) for ICMP code. For example, 0 means "Echo Reply"; 254 means "RFC3692-style Experiment 2".  ☑ Any Service ☑ Any Source port ☑ Any Destination port □ Any ICMP Type (0-255) Self-Define Destination Unreachable Packet Too Big2 Time Exceeded Self-Define
Any ICMP Code	ach ICMP type can be defined with different codes. For example, if you define ICMP Type as "3", then the available codes for Type 3 will be 0-15. **Any ICMP Code** – Default setting. All packets will be filtered. Select Any ICMP Code. Or, enter 0 to 255 based on the ICMP type specified. 
+Add Rule	Click it to create a new ACE rule. Each ACL profile can be added with 8 ACE rules.

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.

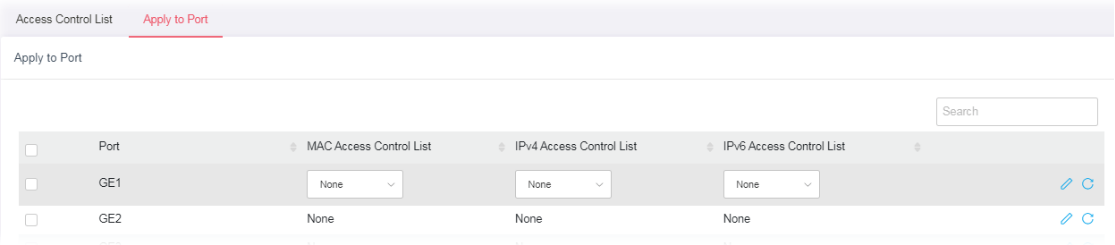


□	Port	MAC Access Control List	IPv4 Access Control List	IPv6 Access Control List	
□	GE1	None	None	None	✎ ↻
□	GE2	None	None	None	✎ ↻
□	GE3	None	None	None	✎ ↻
□	GE4	None	None	None	✎ ↻
□	GE5	None	None	None	✎ ↻
□	GE6	None	None	None	✎ ↻
□	GE7	None	None	None	✎ ↻
□	GE8	None	None	None	✎ ↻
□	GE9	None	None	None	✎ ↻
□	GE10	None	None	None	✎ ↻
□	GE11	None	None	None	✎ ↻
□	GE12	None	None	None	✎ ↻
□	GE13	None	None	None	✎ ↻
□	GE14	None	None	None	✎ ↻
□	GE15	None	None	None	✎ ↻
□	GE16	None	None	None	✎ ↻

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.
✎	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.



□	Port	MAC Access Control List	IPv4 Access Control List	IPv6 Access Control List	
□	GE1	None ⌄	None ⌄	None ⌄	✎ ↻
□	GE2	None	None	None	✎ ↻

Available settings are explained as follows:

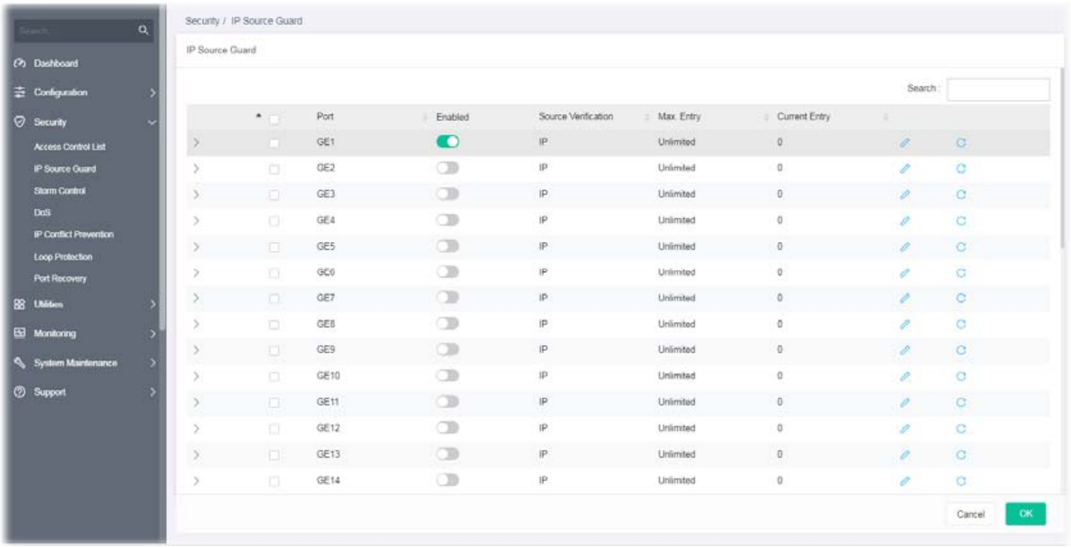
Item	Description
MAC Access Control List	Select an ACL (MAC) to be bound on this interface (port).

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-2 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.



Security / IP Source Guard

IP Source Guard

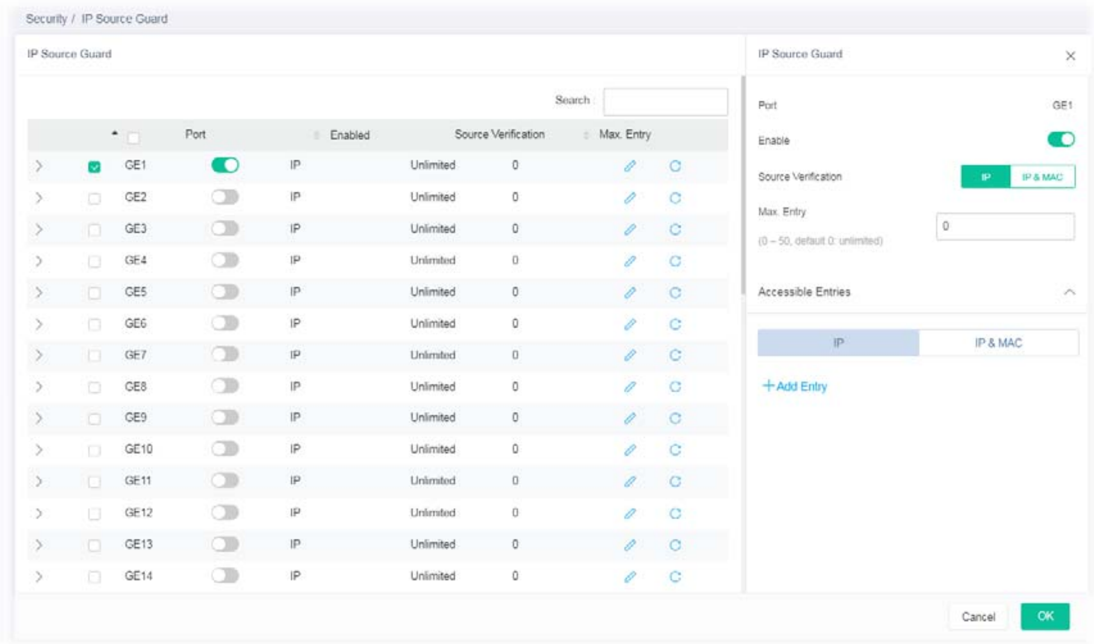
Search :

	□	Port	Enabled	Source Verification	Max. Entry	Current Entry		
›	□	GE1	●	IP	Unlimited	0	✎	↻
›	□	GE2	○	IP	Unlimited	0	✎	↻
›	□	GE3	○	IP	Unlimited	0	✎	↻
›	□	GE4	○	IP	Unlimited	0	✎	↻
›	□	GE5	○	IP	Unlimited	0	✎	↻
›	□	GE6	○	IP	Unlimited	0	✎	↻
›	□	GE7	○	IP	Unlimited	0	✎	↻
›	□	GE8	○	IP	Unlimited	0	✎	↻
›	□	GE9	○	IP	Unlimited	0	✎	↻
›	□	GE10	○	IP	Unlimited	0	✎	↻
›	□	GE11	○	IP	Unlimited	0	✎	↻
›	□	GE12	○	IP	Unlimited	0	✎	↻
›	□	GE13	○	IP	Unlimited	0	✎	↻
›	□	GE14	○	IP	Unlimited	0	✎	↻

Available parameters 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.
Enabled	Click the toggle to enable / disable this profile. ● - means “Enable”. ○ - means “Disable”.
Source Verification	Displays the type of source IP for the packet coming from.
Max. Entry	Displays the total number (0~50) of accessible entries allowed for this port.
Current Entry	Displays the number of accessible entries of this port.
✎	Click it to modify the IP Source Guard setting of the selected port.
↻	Clear current settings and return to factory default settings.

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



Security / IP Source Guard

IP Source Guard

Search :

☐	Port		Enabled	Source Verification	Max. Entry
☑	GE1	●	IP	Unlimited	0
☐	GE2	○	IP	Unlimited	0
☐	GE3	○	IP	Unlimited	0
☐	GE4	○	IP	Unlimited	0
☐	GE5	○	IP	Unlimited	0
☐	GE6	○	IP	Unlimited	0
☐	GE7	○	IP	Unlimited	0
☐	GE8	○	IP	Unlimited	0
☐	GE9	○	IP	Unlimited	0
☐	GE10	○	IP	Unlimited	0
☐	GE11	○	IP	Unlimited	0
☐	GE12	○	IP	Unlimited	0
☐	GE13	○	IP	Unlimited	0
☐	GE14	○	IP	Unlimited	0

IP Source Guard

Port GE1

Enable ●

Source Verification [✓ IP] IP & MAC

Max. Entry 0

(0 – 50, default 0: unlimited)

Accessible Entries

[✓ IP] IP & MAC

+Add Entry

Cancel OK

Available settings are explained as follows:

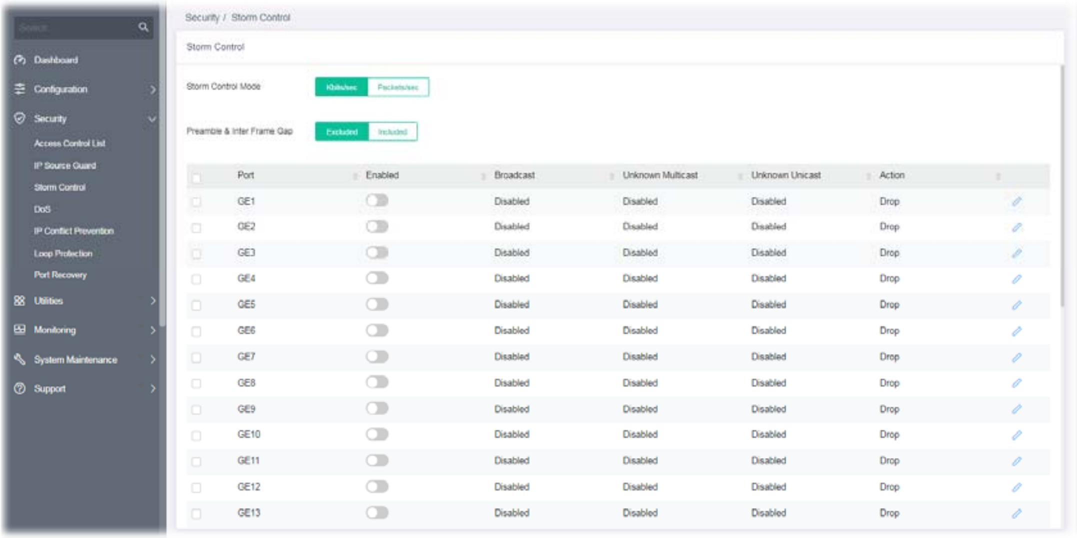
Item	Description
IP Source Guard	
Port	Displays the port profile (GE1 to GE28).
Enable	Click the toggle to enable / disable this function. ● - means “Enable”. ○ - means “Disable”.
Source Verification	Specify the type of source IP for the packet coming from. **IP** - Only the packet with specified IP address will be verified. **IP & MAC** - Only the packet with specified IP address and MAC address will be verified.
Max. Entry	Define the total number (0~50) of accessible entries allowed for this port. The default is 0 (no limit).
Accessible Entries	Define the entry for applying the IP source guard function. **IP** - Select this type to enter an IPv4 address and set a VLAN ID. **IP & MAC** - Select this type to enter an IP address, MAC address and IPv4 address. **+Add Entry** - Click to display blank entry boxes for configuring a new IP address, MAC address, and VLAN ID.

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

III-3 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.



Security / Storm Control

Storm Control

Storm Control Mode: Kbits/sec | Packets/sec

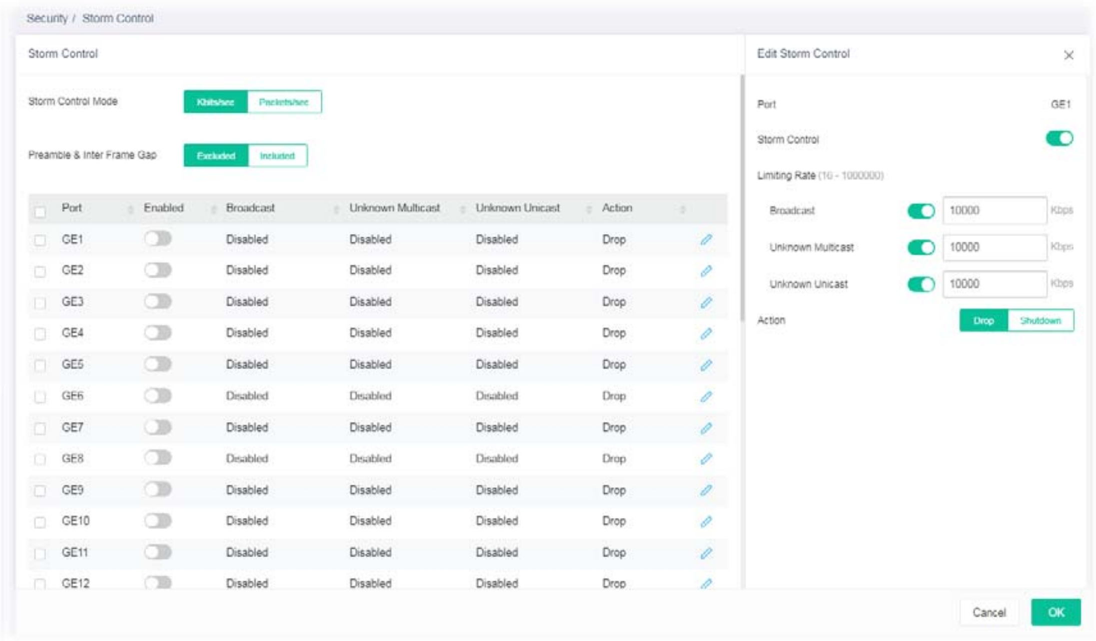
Preamble & Inter Frame Gap: Excluded | Included

□	Port	Enabled	Broadcast	Unknown Multicast	Unknown Unicast	Action	
□	GE1	○	Disabled	Disabled	Disabled	Drop	✎
□	GE2	○	Disabled	Disabled	Disabled	Drop	✎
□	GE3	○	Disabled	Disabled	Disabled	Drop	✎
□	GE4	○	Disabled	Disabled	Disabled	Drop	✎
□	GE5	○	Disabled	Disabled	Disabled	Drop	✎
□	GE6	○	Disabled	Disabled	Disabled	Drop	✎
□	GE7	○	Disabled	Disabled	Disabled	Drop	✎
□	GE8	○	Disabled	Disabled	Disabled	Drop	✎
□	GE9	○	Disabled	Disabled	Disabled	Drop	✎
□	GE10	○	Disabled	Disabled	Disabled	Drop	✎
□	GE11	○	Disabled	Disabled	Disabled	Drop	✎
□	GE12	○	Disabled	Disabled	Disabled	Drop	✎
□	GE13	○	Disabled	Disabled	Disabled	Drop	✎

Available settings are explained as follows:

Item	Description
Storm Control Mode	Select the mode of storm control. **Kbits/sec** - Storm control rate will be calculated by octet-based. **Packet/sec** – Storm control rate will be calculated by packet-based.
Preamble & Inter Frame Gap	Select the rate calculation with/without preamble & IFG (20 bytes). **Excluded** – Exclude preamble & IFG (20 bytes) when count ingress storm control rate. **Included** - Include preamble & IFG (20 bytes) when count ingress storm control rate.
Port	Enable/disable the port (GE1 to GE28) profiles.
Enabled	Click the toggle to enable / disable this profile. ● - means “Enable”. ○ - means “Disable”.
Broadcast	Displays the storm control rate limited for broadcast.
Unknown Multicast	Displays the storm control rate limited for unknown multicast.
Unknown Unicast	Displays the storm control rate limited for unknown unicast.
Action	Displays the action performed.
✎	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.



Security / Storm Control

Storm Control

Storm Control Mode: [✓ Kbits/sec] Packets/sec

Preamble & Inter Frame Gap: [✓ Excluded] Included

□	Port	Enabled	Broadcast	Unknown Multicast	Unknown Unicast	Action	
□	GE1	○	Disabled	Disabled	Disabled	Drop	🖉
□	GE2	○	Disabled	Disabled	Disabled	Drop	🖉
□	GE3	○	Disabled	Disabled	Disabled	Drop	🖉
□	GE4	○	Disabled	Disabled	Disabled	Drop	🖉
□	GE5	○	Disabled	Disabled	Disabled	Drop	🖉
□	GE6	○	Disabled	Disabled	Disabled	Drop	🖉
□	GE7	○	Disabled	Disabled	Disabled	Drop	🖉
□	GE8	○	Disabled	Disabled	Disabled	Drop	🖉
□	GE9	○	Disabled	Disabled	Disabled	Drop	🖉
□	GE10	○	Disabled	Disabled	Disabled	Drop	🖉
□	GE11	○	Disabled	Disabled	Disabled	Drop	🖉
□	GE12	○	Disabled	Disabled	Disabled	Drop	🖉

Edit Storm Control

Port: GE1

Storm Control: ●

Limiting Rate (16 - 1000000)

Broadcast: ● 10000 Kbps

Unknown Multicast: ● 10000 Kbps

Unknown Unicast: ● 10000 Kbps

Action: [✓ Drop] Shutdown

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. ● - means “Enable”. ○ - means “Disable”.
Limiting Rate	**Broadcast** – Specify the storm control rate for Broadcast packet. Value of storm control rate, Unit: Kbps (Kbits per-second). The range is from 16 to 1000000. **Unknown Multicast** – Specify the storm control rate for unknown multicast packet. Value of storm control rate, Unit: Kbps (Kbits per-second). The range is from 16 to 1000000. **Unknown Unicast** - Specify the storm control rate for unknown multicast packet. Value of storm control rate, Unit: Kbps (Kbits per-second). The range is from 16 to 1000000.
Action	Select the state of setting. **Drop** – Packets exceed storm control rate will be dropped. **Shutdown** - Port exceeds storm control rate will be shutdown.

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

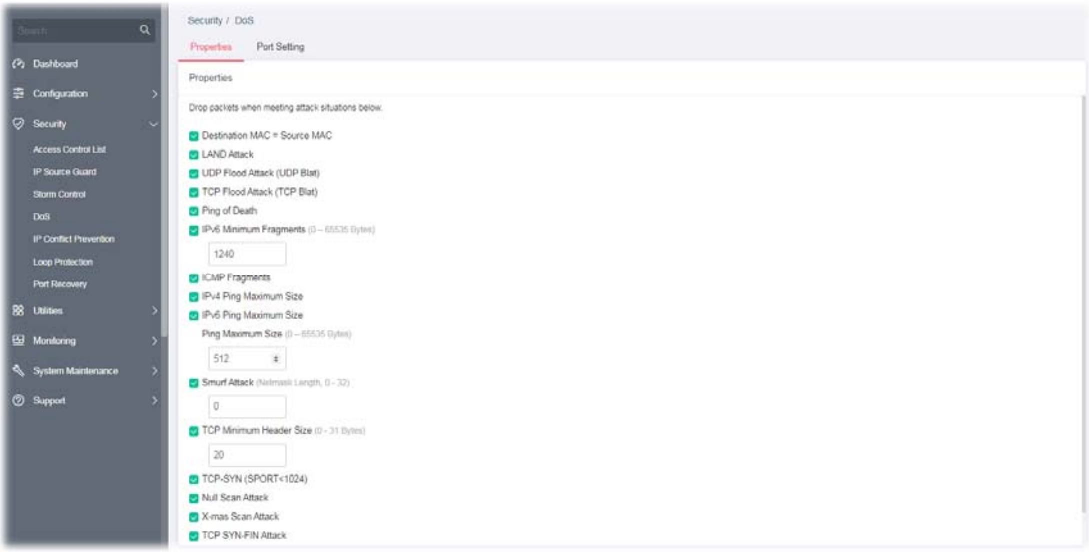
III-4 DoS

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-4-1 Properties

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



Properties

Drop packets when meeting attack situations below.

☑ Destination MAC = Source MAC
☑ LAND Attack
☑ UDP Flood Attack (UDP Blat)
☑ TCP Flood Attack (TCP Blat)
☑ Ping of Death
☑ IPv6 Minimum Fragments (0 – 65535 Bytes)
1240
☑ ICMP Fragments
☑ IPv4 Ping Maximum Size
☑ IPv6 Ping Maximum Size
Ping Maximum Size (0 – 65535 Bytes)
512
☑ Smurf Attack (Netmask Length, 0 - 32)
0
☑ TCP Minimum Header Size (0 - 31 Bytes)
20
☑ TCP-SYN (SPORT<1024)
☑ Null Scan Attack
☑ X-mas Scan Attack
☑ TCP SYN-FIN Attack

Available settings are explained as follows:

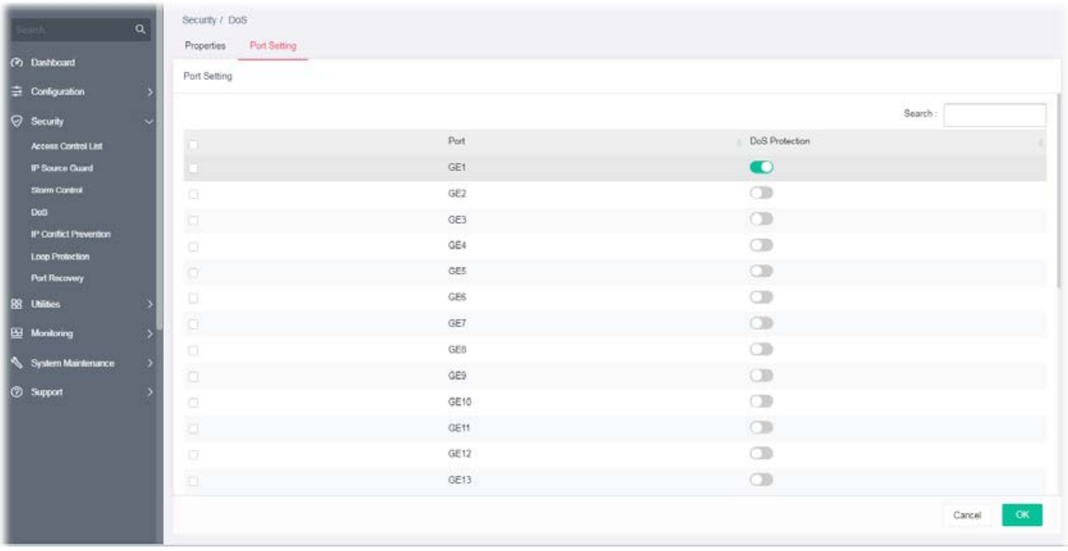
Item	Description
Destination MAC=Source MAC	Drops the packets if the destination MAC address is equal to the source MAC address. Check/uncheck the box to enable/disable the function.
LAND Attack	Drops the packets if the source IP address is equal to the destination IP address. Check/uncheck the box to enable/disable the function.
UDP Flood Attack (UDP Blat)	Drops the packets if the UDP source port equals to the UDP destination port. Check/uncheck the box to enable/disable the function.
TCP Flood Attack (TCP Blat)	Drops the packages if the TCP source port is equal to the TCP destination port. Check/uncheck the box to enable/disable the function.
Ping to Death	Avoids ping of death attack. Ping packets that length are larger than 65535 bytes. Check/uncheck the box to enable/disable the function.
IPv6 Minimum Fragments	Checks the minimum size of IPv6 fragments, and drop the packets smaller than the minimum size. The valid range is from 0 to 65535 bytes, and default value is 1240 bytes.

	Check/uncheck the box to enable/disable the function.
ICMP Fragments	Drops the fragmented ICMP packets. Check/uncheck the box to enable/disable the function.
IPv4 Ping Maximum Size	Determines the IPv4 PING packet with the length. Check/uncheck the box to enable/disable the function.
IPv6 Ping Maximum Size	Determines the IPv6 PING packet with the length. Check/uncheck the box to enable/disable the function. **Ping Maximum Size** - Determine the IPv4/IPv6 PING packet with the length. Specify the maximum size of the ICMPv4/ICMPv6 ping packets. The valid range is from 0 to 65535 bytes, and the default value is 512 bytes.
Smurf Attack	Avoids smurf attack. The length range of the netmask is from 0 to 323 bytes, and default length is 0 byte. Check/uncheck the box to enable/disable the function.
TCP Minimum Header Size	Checks the minimum TCP header and drops the TCP packets with the header smaller than the minimum size. The length range is from 0 to 31 bytes, and default length is 20 bytes. Check/uncheck the box to enable/disable the function.
TCP-SYN (SPORT<1024)	Drops SYN packets with sport less than 1024. Check/uncheck the box to enable/disable the function.
Null Scan Attack	Drops the packets with NULL scan. Check/uncheck the box to enable/disable the function.
X-mas Scan Attack	Drops the packets if the sequence number is zero, and the FIN, URG and PSH bits are set. Check/uncheck the box to enable/disable the function.
TCP SYN-FIN Attack	Drops the packets with SYN and FIN bits set. Check/uncheck the box to enable/disable the function.
TCP SYN-RST Attack	Drops the packets with SYN and RST bits set. Check/uncheck the box to enable/disable the function.
TCP Fragment (Offset=1)	Drops the fragmented ICMP packets. Check/uncheck the box to enable/disable the function.

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

III-4-2 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.



Port Setting

Search :

□	Port	DoS Protection
□	GE1	●
□	GE2	○
□	GE3	○
□	GE4	○
□	GE5	○
□	GE6	○
□	GE7	○
□	GE8	○
□	GE9	○
□	GE10	○
□	GE11	○
□	GE12	○
□	GE13	○

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. ● - means "Enable". ○ - means "Disable".

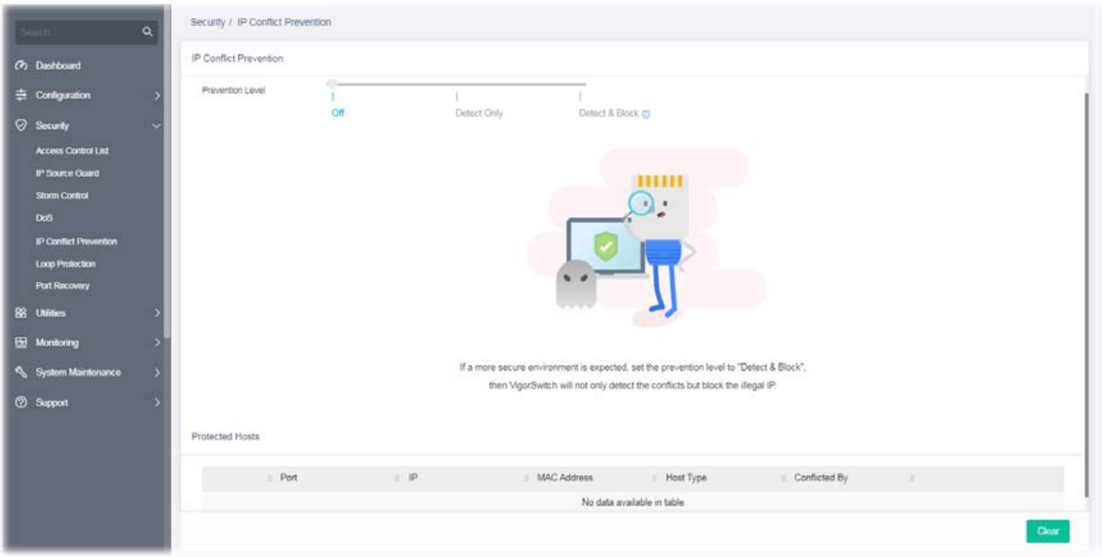
After finishing this web page configuration, please click **OK** to save the settings.

III-5 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



Security / IP Conflict Prevention

IP Conflict Prevention

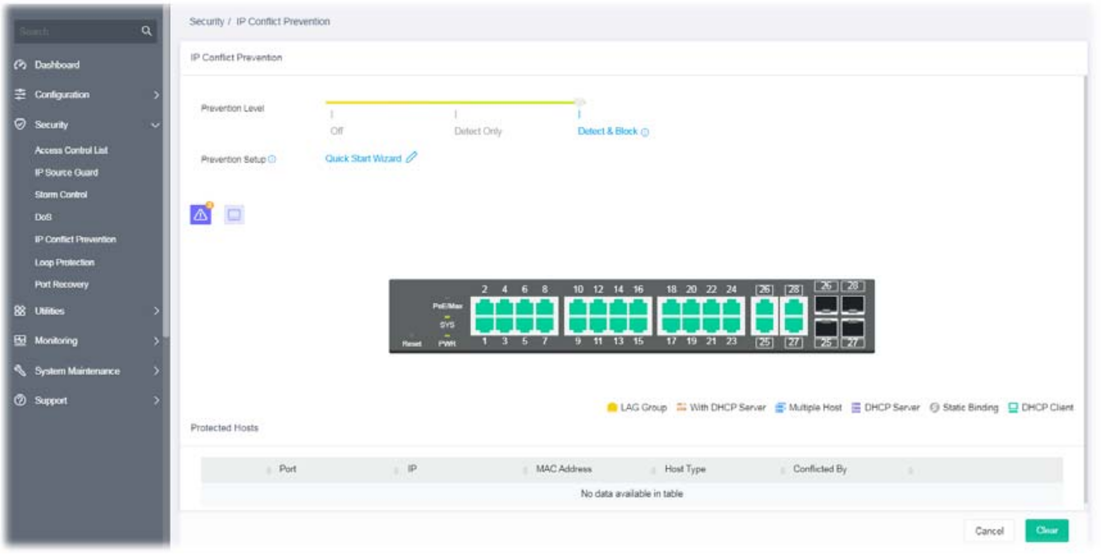
Prevention Level: Off | Detect Only | Detect & Block

If a more secure environment is expected, set the prevention level to "Detect & Block", then VigorSwitch will not only detect the conflicts but block the illegal IP.

Protected Hosts

Port	IP	MAC Address	Host Type	Conflicted By
No data available in table				

Prevention Level: Detect & Block



Security / IP Conflict Prevention

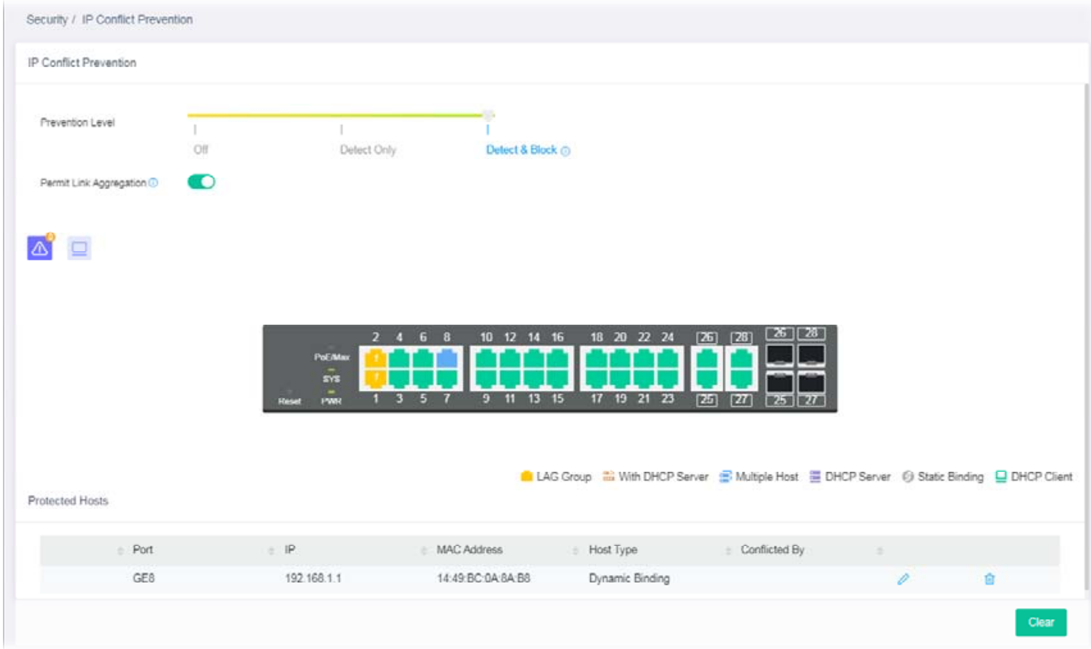
IP Conflict Prevention

Prevention Level: Off | Detect Only | Detect & Block

Prevention Setup: Quick Start Wizard

Protected Hosts

Port	IP	MAC Address	Host Type	Conflicted By
No data available in table				



Security / IP Conflict Prevention

IP Conflict Prevention

Prevention Level: Off | Detect Only | Detect & Block

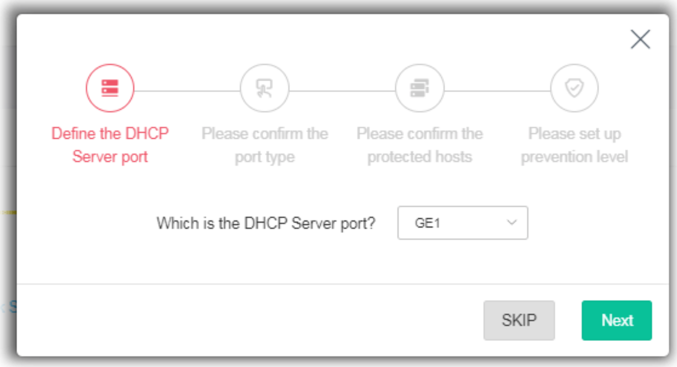
Permit Link Aggregation: on

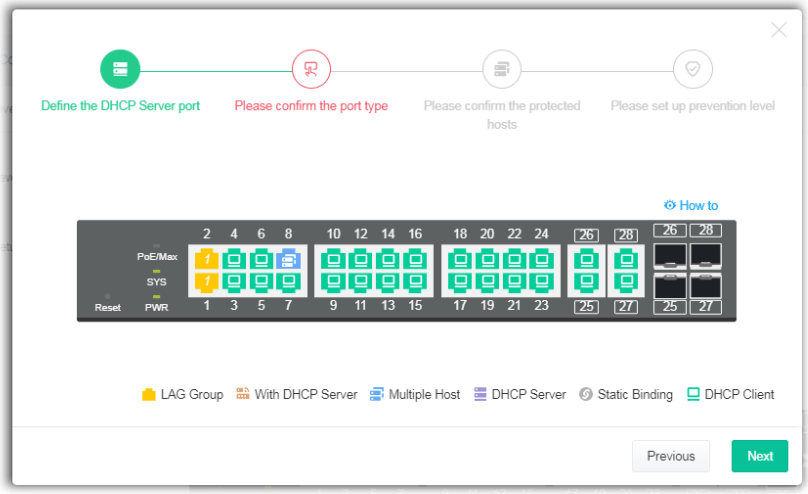
Protected Hosts

Port	IP	MAC Address	Host Type	Conflicted By
GE8	192.168.1.1	14:49:BC:0A:8A:B8	Dynamic Binding	

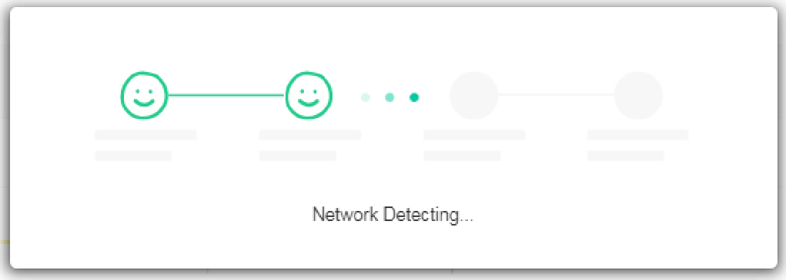
Clear

Available settings are explained as follows:

Item	Description
IP Conflict Prevention	
Prevention Level	**Off** - The function of IP conflict prevention is disabled. **Detect Only** - VigorSwitch will detect the host but no further action executed. **Detect & Block** - VigorSwitch will detect the host and block the host if it meets the configuration on this page.
Prevention Setup	**Quick Setup Wizard** - It is available only when **Detect & Block** is selected as Prevention Level. The system will guide to bind server port with an IP address step by step. Step 1: Choose a server port. Click Next.  Define the DHCP Server port — Please confirm the port type — Please confirm the protected hosts — Please set up prevention level Which is the DHCP Server port? GE1 SKIP Next Step 2: Confirm the port type. Click Next.

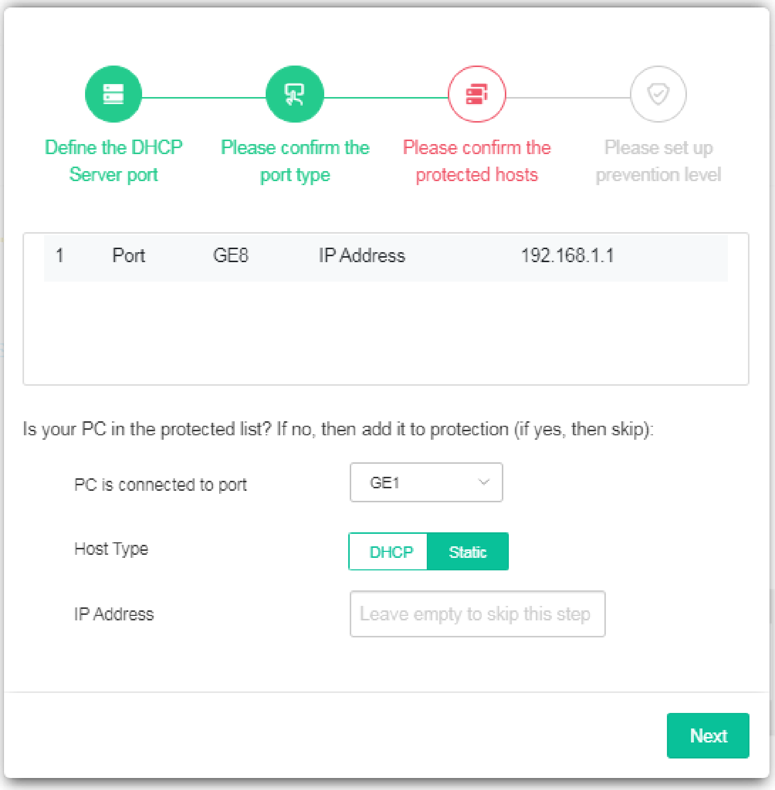


Step 3: Wait for the network detection.



Network Detecting...

Step 4: Confirm / modify the protected host. Click Next.


Define the DHCP Server port
Please confirm the port type
Please confirm the protected hosts
Please set up prevention level
Next

1	Port	GE8	IP Address	192.168.1.1

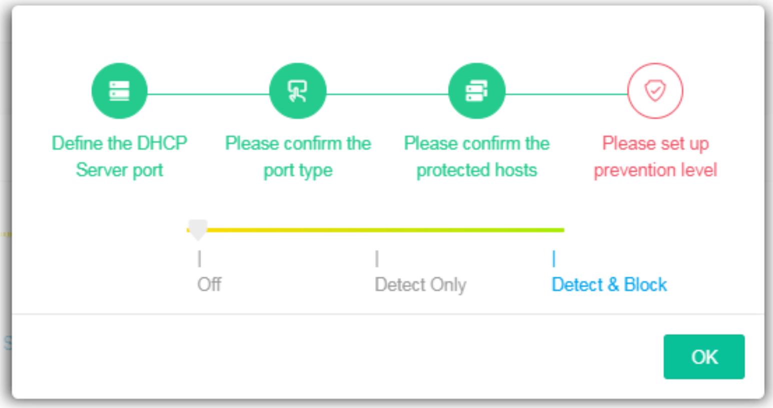
Is your PC in the protected list? If no, then add it to protection (if yes, then skip):

PC is connected to port: GE1

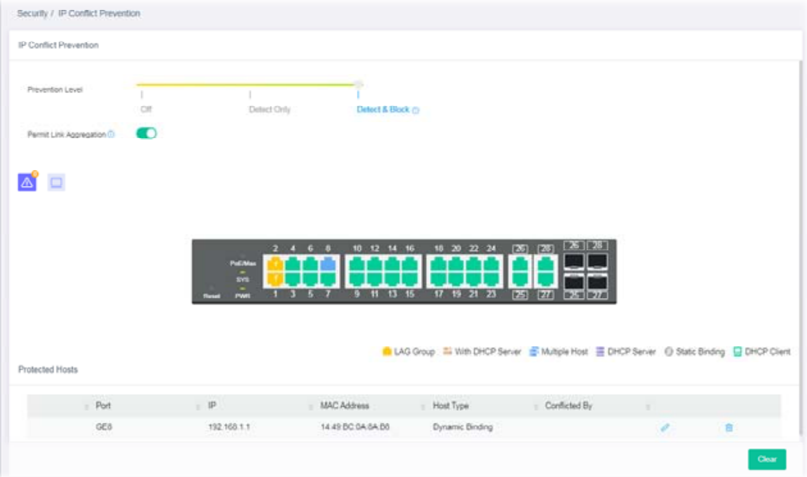
Host Type: DHCP [✓ Static]

IP Address: Leave empty to skip this step

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


Define the DHCP Server port
Please confirm the port type
Please confirm the protected hosts
Please set up prevention level
Off
Detect Only
Detect & Block
OK

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

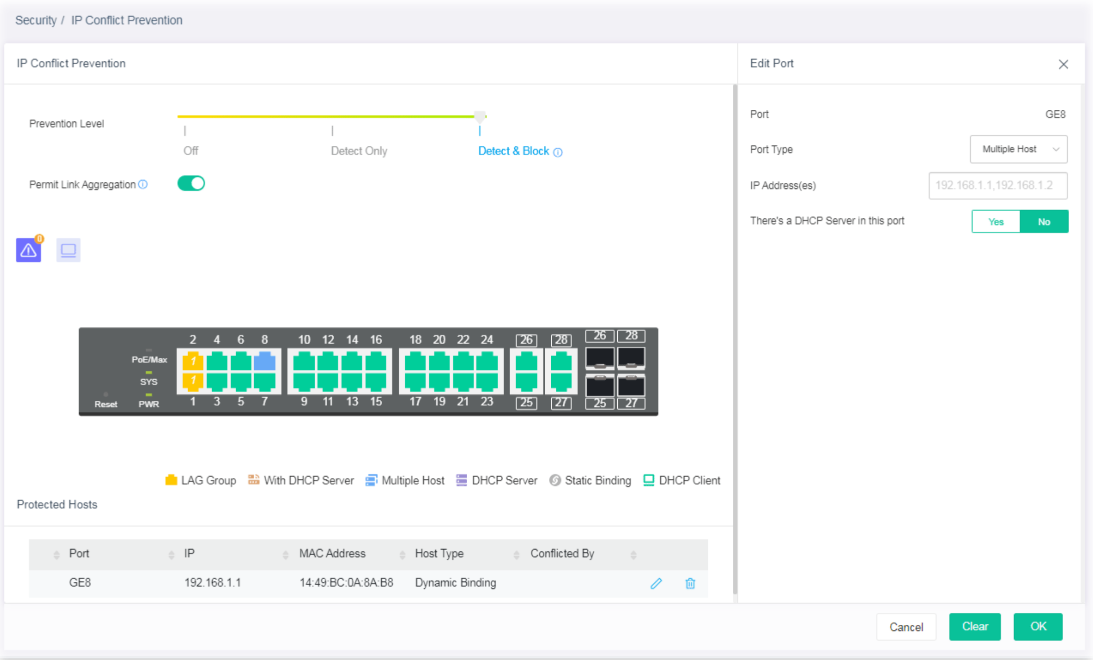


Port	IP	MAC Address	Host Type	Conflicted By
GE8	192.168.1.1	14:49:BC:0A:8A:B8	Dynamic Binding	

Permit Link Aggregation	It appears after running the quick start wizard for IP conflict prevention. The devices connected to the LAG ports will not be blocked due to using the same IP.
Protected Host	
Port	Displays the LAN port number (GE1 to GE28, 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.
✎	Click to modify the settings of the selected port.
🗑	Click it to remove the selected entry.
Clear	Click it to remove all entries.

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

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



Security / IP Conflict Prevention

IP Conflict Prevention

Prevention Level: Off | Detect Only | Detect & Block

Permit Link Aggregation ●

LAG Group | With DHCP Server | Multiple Host | DHCP Server | Static Binding | DHCP Client

Protected Hosts

Port	IP	MAC Address	Host Type	Conflicted By
GE8	192.168.1.1	14:49:BC:0A:8A:B8	Dynamic Binding	

Edit Port

Port: GE8

Port Type: Multiple Host

IP Address(es): 192.168.1.1,192.168.1.2

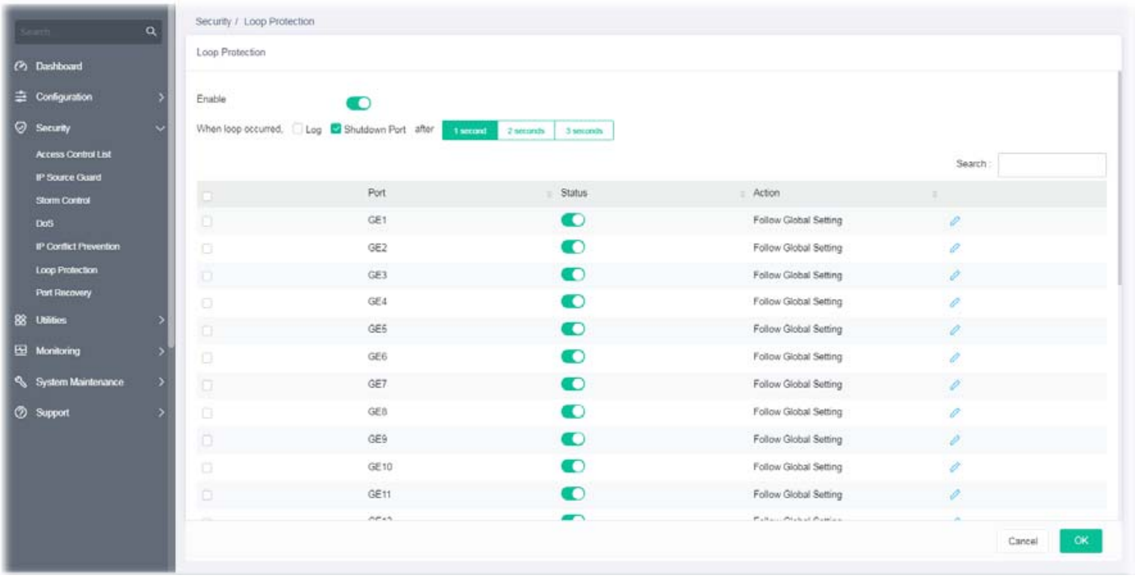
There's a DHCP Server in this port: Yes [✓ No]

Available settings are explained as follows:

Item	Description
Edit Port	
Port	Displays the LAN port number (GE1 to GE28, LAG1 to LAG8) of the selected host.
Port Type	Specify the port type for the selected host. ● **DHCP Client** ● **Static Binding** ● **Multiple Host** ● **DHCP Server**
IP Address(es)	Enter the IP address based on the port type.
There's a DHCP Server in this port	**Yes** - If there is a DHCP server in this port already, click Yes. **No** - If there is no DHCP server in this port already, click No.

III-6 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.



Security / Loop Protection

Loop Protection

Enable ●

When loop occurred, □ Log ☑ Shutdown Port after [✓ 1 second] 2 seconds 3 seconds

Search :

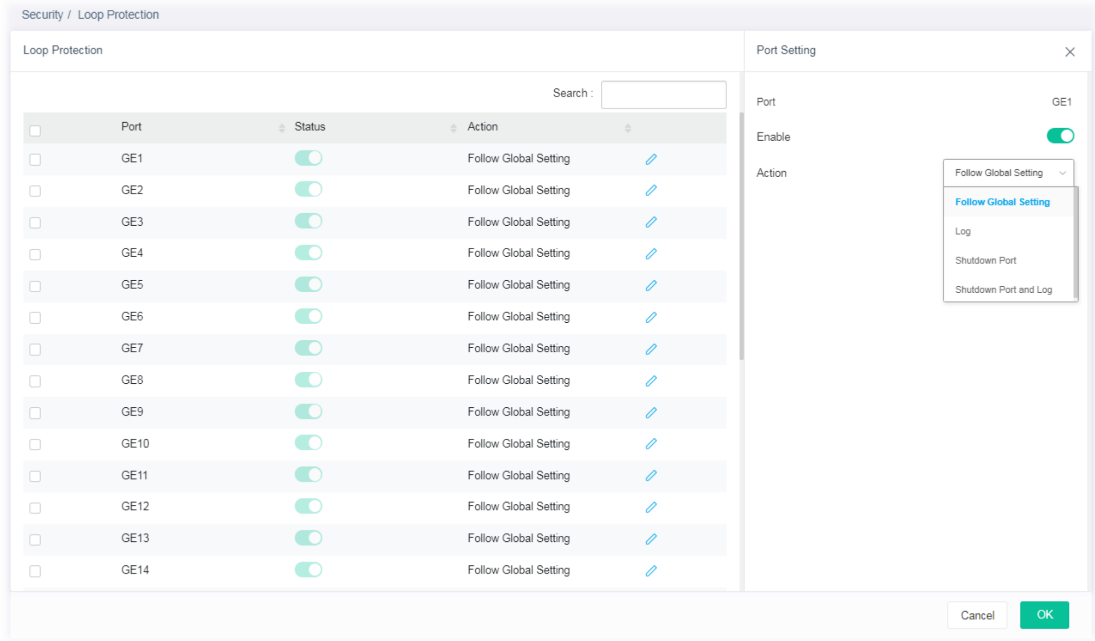
□	Port	Status	Action	
□	GE1	●	Follow Global Setting	✎
□	GE2	●	Follow Global Setting	✎
□	GE3	●	Follow Global Setting	✎
□	GE4	●	Follow Global Setting	✎
□	GE5	●	Follow Global Setting	✎
□	GE6	●	Follow Global Setting	✎
□	GE7	●	Follow Global Setting	✎
□	GE8	●	Follow Global Setting	✎
□	GE9	●	Follow Global Setting	✎
□	GE10	●	Follow Global Setting	✎
□	GE11	●	Follow Global Setting	✎

Cancel OK

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. ● - means “Enable”. ○ - means “Disable”.
When loop occurred..	When the switch detects loop situation occurred to a port; it will perform the action selected in this field. **Log** - The switch will record such event as a log. **Shutdown Port** - The switch will shut down the port. **After 1 second/2 seconds/3 seconds** - Determine the time to record the event and / or shutdown the port. The settings configured here will be treated as global setting for all GE ports.
Port	Displays the port number (GE1 to GE28). 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.
✎	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.



Security / Loop Protection

Loop Protection

Search :

Port	Status	Action
GE1		Follow Global Setting
GE2		Follow Global Setting
GE3		Follow Global Setting
GE4		Follow Global Setting
GE5		Follow Global Setting
GE6		Follow Global Setting
GE7		Follow Global Setting
GE8		Follow Global Setting
GE9		Follow Global Setting
GE10		Follow Global Setting
GE11		Follow Global Setting
GE12		Follow Global Setting
GE13		Follow Global Setting
GE14		Follow Global Setting

Port Setting

Port GE1

Enable

Action Follow Global Setting

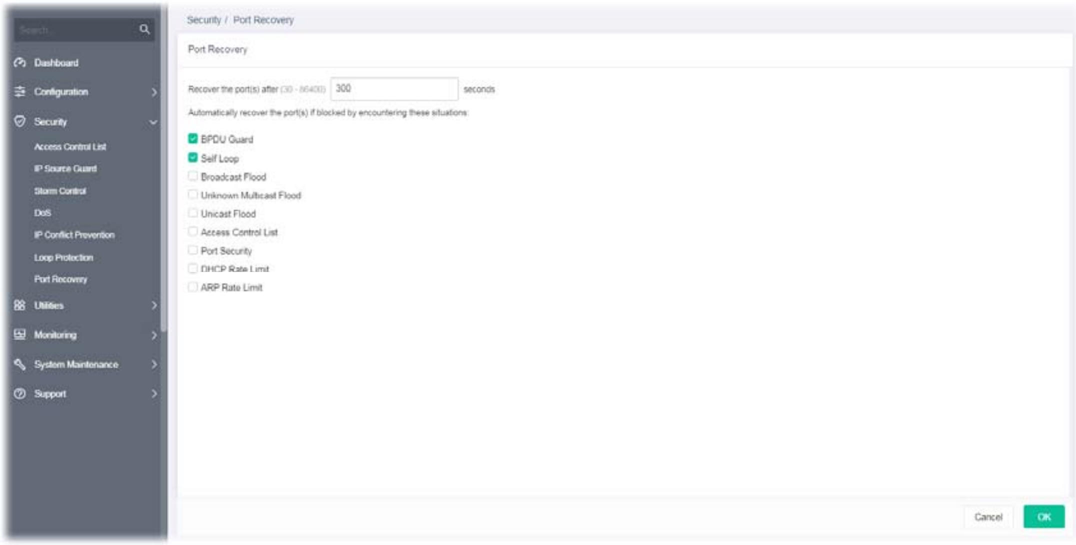
Available settings are explained as follows:

Item	Description
Port	Displays the port number (GE1 to GE28).
Enable	**Enable / Disable** – Click the toggle to enable / disable this function. VigorSwitch will detect the loop event of the GE port automatically. - means “Enable”. - means “Disable”.
Action	**Follow Global Setting** - Adopts the settings configured for **When loop occurred**. **Log** - The switch will record such event as a log. **Shutdown Port** - The switch will shut down the port. **Shutdown Port and Log** - The switch will shut down the port and record the event as a log. The system administrator will view the content from system log.

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

III-7 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.



Security / Port Recovery

Port Recovery

Recover the port(s) after (30 - 86400) 300 seconds

Automatically recover the port(s) if blocked by encountering these situations:

☑ BPDU Guard
☑ Self Loop
□ Broadcast Flood
□ Unknown Multicast Flood
□ Unicast Flood
□ Access Control List
□ Port Security
□ DHCP Rate Limit
□ ARP Rate Limit

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.

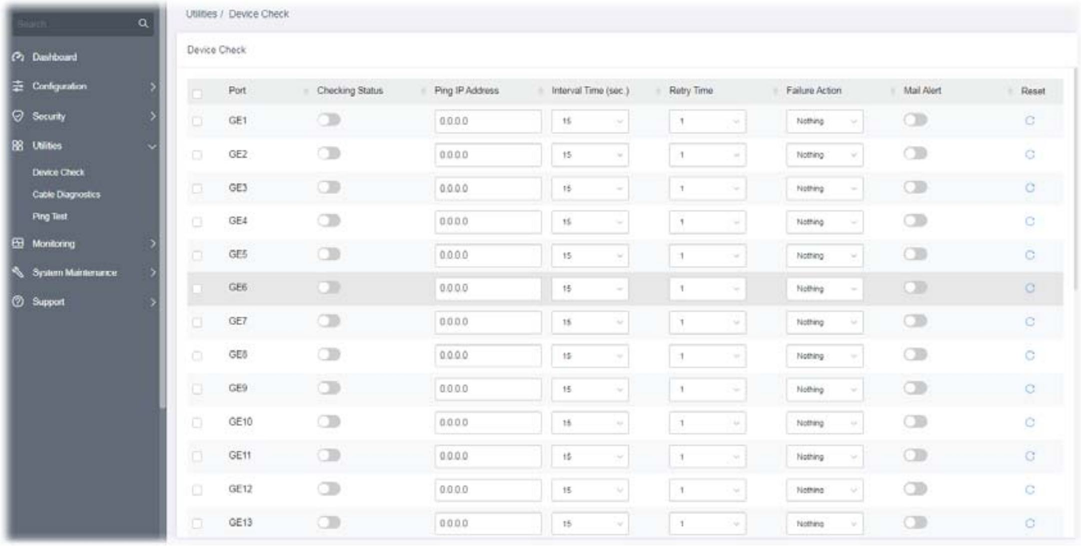
This page is left blank.

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.



Utilities / Device Check

Device Check

☐	Port	Checking Status	Ping IP Address	Interval Time (sec.)	Retry Time	Failure Action	Mail Alert	Reset
☐	GE1	○	0.0.0.0	15	1	Nothing	○	↻
☐	GE2	○	0.0.0.0	15	1	Nothing	○	↻
☐	GE3	○	0.0.0.0	15	1	Nothing	○	↻
☐	GE4	○	0.0.0.0	15	1	Nothing	○	↻
☐	GE5	○	0.0.0.0	15	1	Nothing	○	↻
☐	GE6	○	0.0.0.0	15	1	Nothing	○	↻
☐	GE7	○	0.0.0.0	15	1	Nothing	○	↻
☐	GE8	○	0.0.0.0	15	1	Nothing	○	↻
☐	GE9	○	0.0.0.0	15	1	Nothing	○	↻
☐	GE10	○	0.0.0.0	15	1	Nothing	○	↻
☐	GE11	○	0.0.0.0	15	1	Nothing	○	↻
☐	GE12	○	0.0.0.0	15	1	Nothing	○	↻
☐	GE13	○	0.0.0.0	15	1	Nothing	○	↻

Available settings are explained as follows:

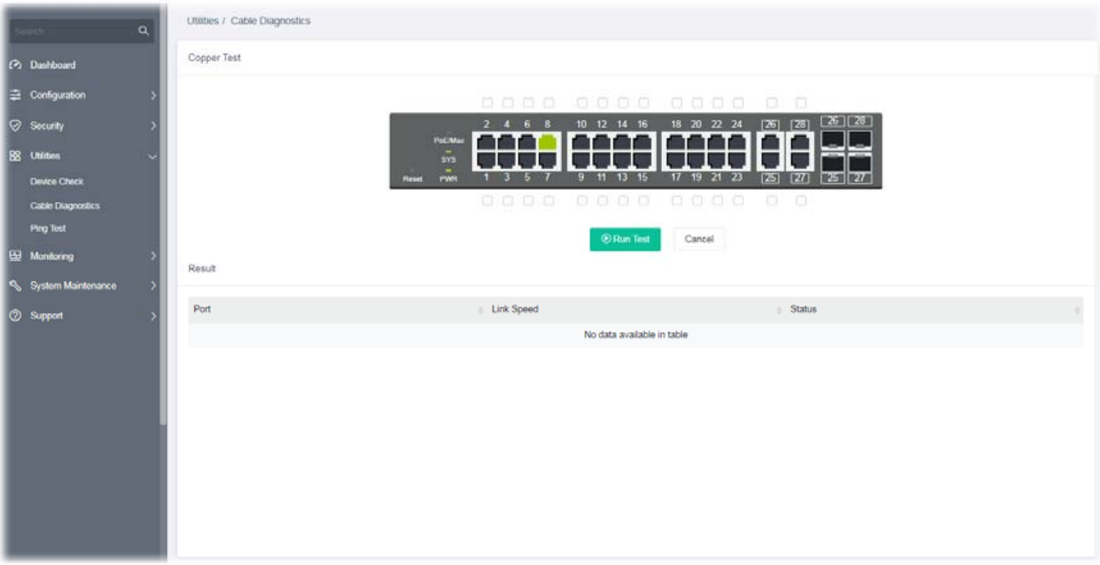
Item	Description
Port	Display the port number (GE1 to GE28). Check the box to the left to enable the port settings.
Checking Status	**Enable / Disable** – Click the toggle to enable / disable this function. ● - means “Enable”. ○ - means “Disable”.
Ping IP Address	Enter the IP address of the PoE device for check.
Interval Time(sec.)	The ping check will be performed every 15, 30, 60 or 120 seconds for the selected port (PoE device).
Retry Time	The system will perform the ping check the selected port (PoE device) for 1, 3 or 5 times.
Failure Action	Specify the action performed for PoE device when there is no number of retry time of echo from given IP address. ● **Power Cycle** - Force reboot the device by cycling the power given to the PoE device. ● **Power Off** - The PoE device will be powered off. ● **Nothing** - Log this event only, no action is taken on PoE device.
Mail Alert	**Enable / Disable** – 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.



Port	Link Speed	Status
No data available in table		

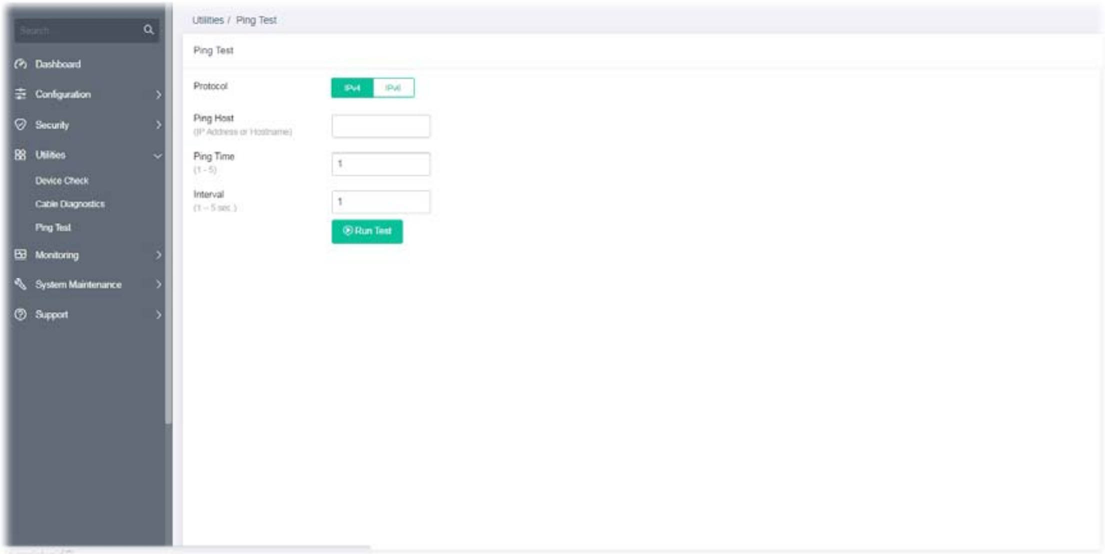
Available settings are explained as follows:

Item	Description
Cooper Test	
Run Test	Perform the copper test action. Before clicking Run Test, select the port or ports (GE1 to GE28) 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.



Protocol: IPv4

Ping Host (IP Address or Hostname):

Ping Time (1 - 5): 1

Interval (1 ~ 5 sec.): 1

Available settings are explained as follows:

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

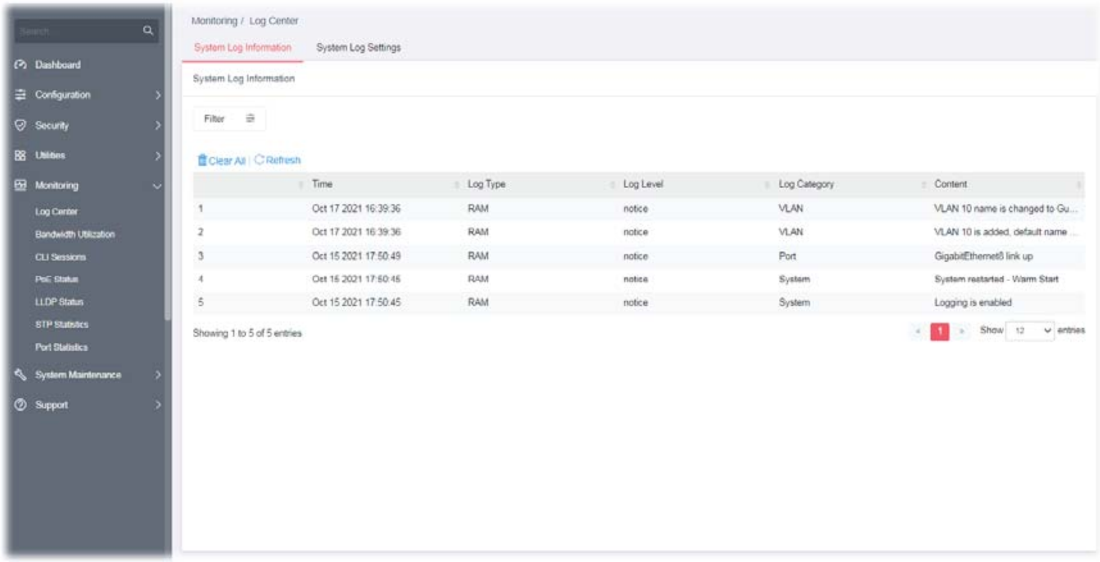
This page is left blank.

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.



Monitoring / Log Center

System Log Information | System Log Settings

System Log Information

Filter

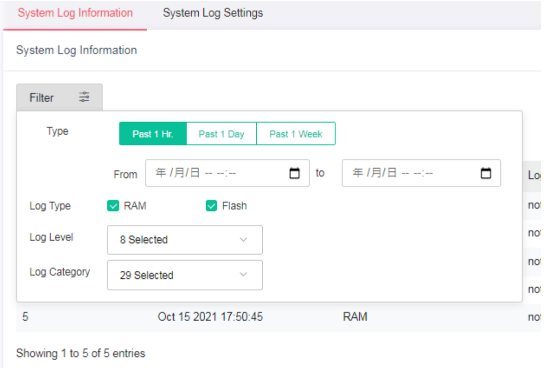
Clear All | Refresh

	Time	Log Type	Log Level	Log Category	Content
1	Oct 17 2021 16:39:36	RAM	notice	VLAN	VLAN 10 name is changed to Gu...
2	Oct 17 2021 16:39:36	RAM	notice	VLAN	VLAN 10 is added, default name ...
3	Oct 15 2021 17:50:49	RAM	notice	Port	GigabitEthernet8 link up
4	Oct 15 2021 17:50:45	RAM	notice	System	System restarted - Warm Start
5	Oct 15 2021 17:50:45	RAM	notice	System	Logging is enabled

Showing 1 to 5 of 5 entries

Show 12 entries

Available settings are explained as follows:

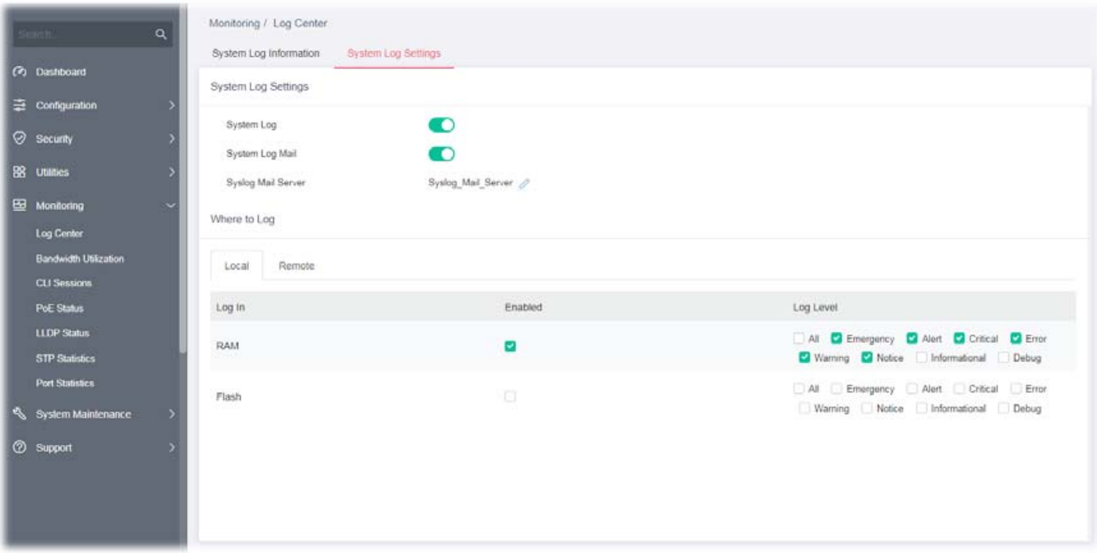
Item	Description
Filter	Click to set the conditions for filtering.  System Log Information | System Log Settings System Log Information Filter Type: Past 1 Hr. | Past 1 Day | Past 1 Week From 年/月/日 --:-- to 年/月/日 --:-- Log Type: ☑ RAM ☑ Flash Log Level: 8 Selected Log Category: 29 Selected 5 Oct 15 2021 17:50:45 RAM Showing 1 to 5 of 5 entries **Type** - Specify the time (Past 1 Hour, Past 1 Day, Past 1 Week) for filtering. **Log Type** - Select RAM (explore the logs contained in volatile memory (also known as RAM) or Flash (explore the logs contained in non-volatile memory). **Log Level** - Select severity (emerg, alert, crit, error, warning, notice, info and debug) of log messages which you wish to filter out for review. **Log Category** - Select the categories (related features) of logs you wish to review.

Clear All	Clear it to remove all logs displayed in this page.
Refresh	Click it to refresh the log.
Time	Displays the filtering time type.
Log Type	Displays the log type (RAM or Flash).
Log Level	Displays the severity of the log.
Log Category	Displays the category of the log.
Content	Displays the brief explanation of the log.

V-1-2 System Log Settings

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

V-1-2-1 Local



System Log Settings

System Log: on

System Log Mail: on

Syslog Mail Server: Syslog_Mail_Server

Where to Log

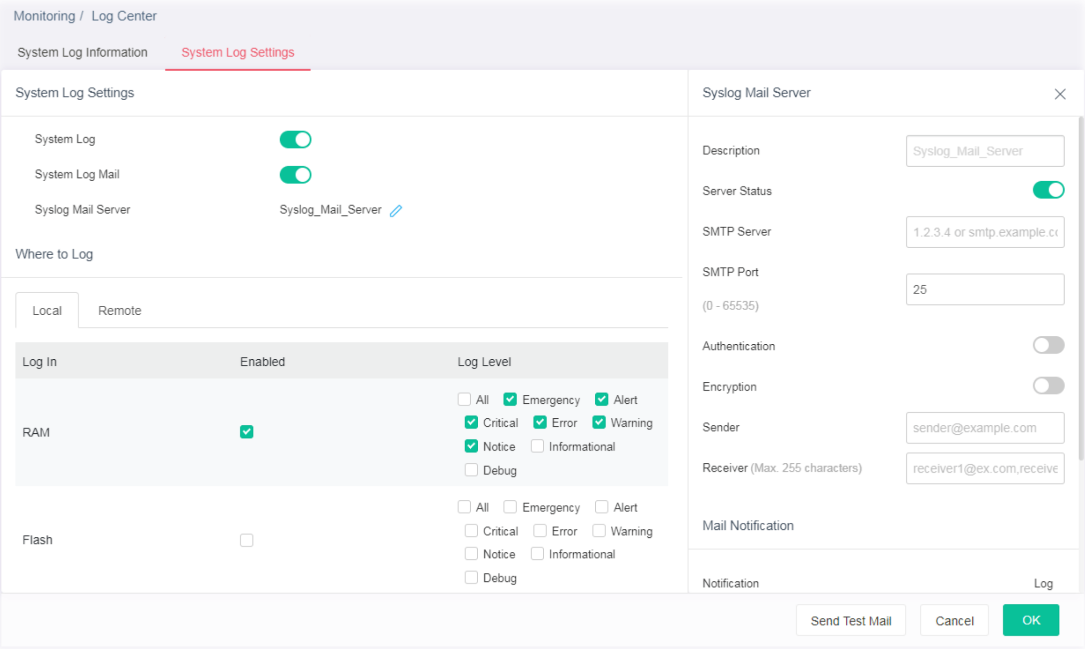
Log In	Enabled	Log Level
RAM	☑	□ All ☑ Emergency ☑ Alert ☑ Critical ☑ Error ☑ Warning ☑ Notice □ Informational □ Debug
Flash	□	□ All □ Emergency □ Alert □ Critical □ Error □ Warning □ Notice □ Informational □ Debug

Available settings are explained as follows:

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

	Log Level - Select the box(es) to select the severity of the log.

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



Monitoring / Log Center

System Log Information | System Log Settings

System Log Settings

System Log ●

System Log Mail ●

Syslog Mail Server: Syslog_Mail_Server ✎

Where to Log

Local | Remote

Log In	Enabled	Log Level
RAM	☑	☐ All ☑ Emergency ☑ Alert ☑ Critical ☑ Error ☑ Warning ☑ Notice ☐ Informational ☐ Debug
Flash	☐	☐ All ☐ Emergency ☐ Alert ☐ Critical ☐ Error ☐ Warning ☐ Notice ☐ Informational ☐ Debug

Syslog Mail Server

Description: Syslog_Mail_Server

Server Status: ●

SMTP Server: 1.2.3.4 or smtp.example.co

SMTP Port (0 - 65535): 25

Authentication: ○

Encryption: ○

Sender: sender@example.com

Receiver (Max. 255 characters): receiver1@ex.com,receive

Mail Notification

Notification: Log

Available settings are explained as follows:

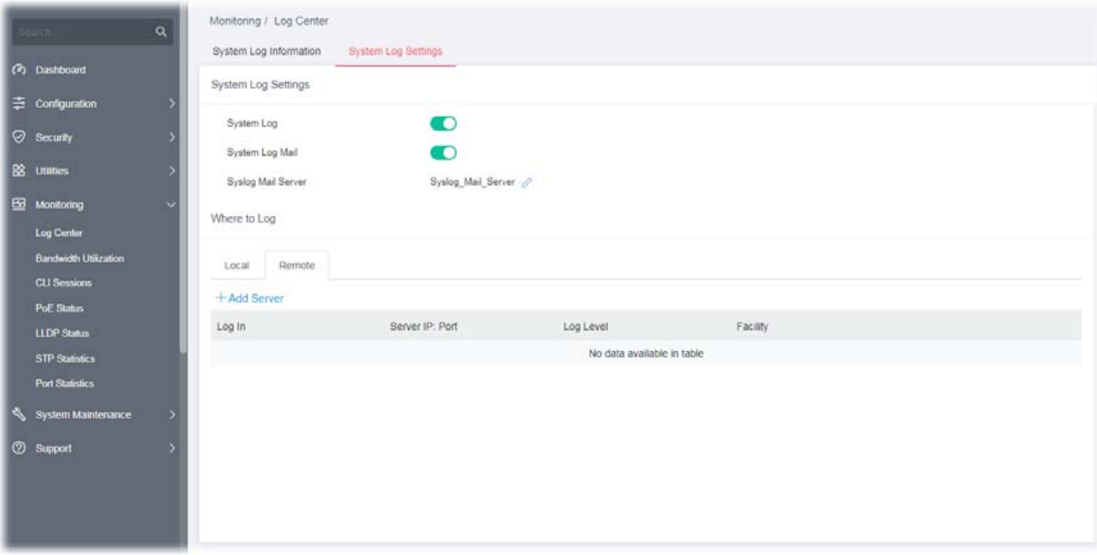
Item	Description
Syslog Mail Server	
Description	Displays the name of the Syslog Mail Server.
Server Status	**Enable / Disable** – Click the toggle to enable / disable the Syslog Mail Server settings. ● - means “Enable”. ○ - means “Disable”.
SMTP Server	Enter IP address or URL of the SMTP server.
SMTP Port	Enter the port number for the SMTP server.
Authentication	**Enable / Disable** – Click the toggle to enable / disable the authentication mechanism. ● **Username** - Enter a user name for authentication. ● **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. ● **STARTTLS** - The mail will be encrypted with StartTLS. ● **SSL/TLS** - The mail will be encrypted with StartTLS.
Sender	Enter the email address which will send the syslog mail out.
Receiver	Enter the email address which will receive the syslog mail.

Mail Notification	
Log Type	Vigor system will send the e-mail related to the selected feature(e.g., AAA, ACL) to the recipient.
Send Test Mail	After clicking this button, VigorSwitch system will send a test mail to the recipient.

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

V-1-2-2 Remote

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



System Log Settings

System Log ●
System Log Mail ●
Syslog Mail Server Syslog_Mail_Server

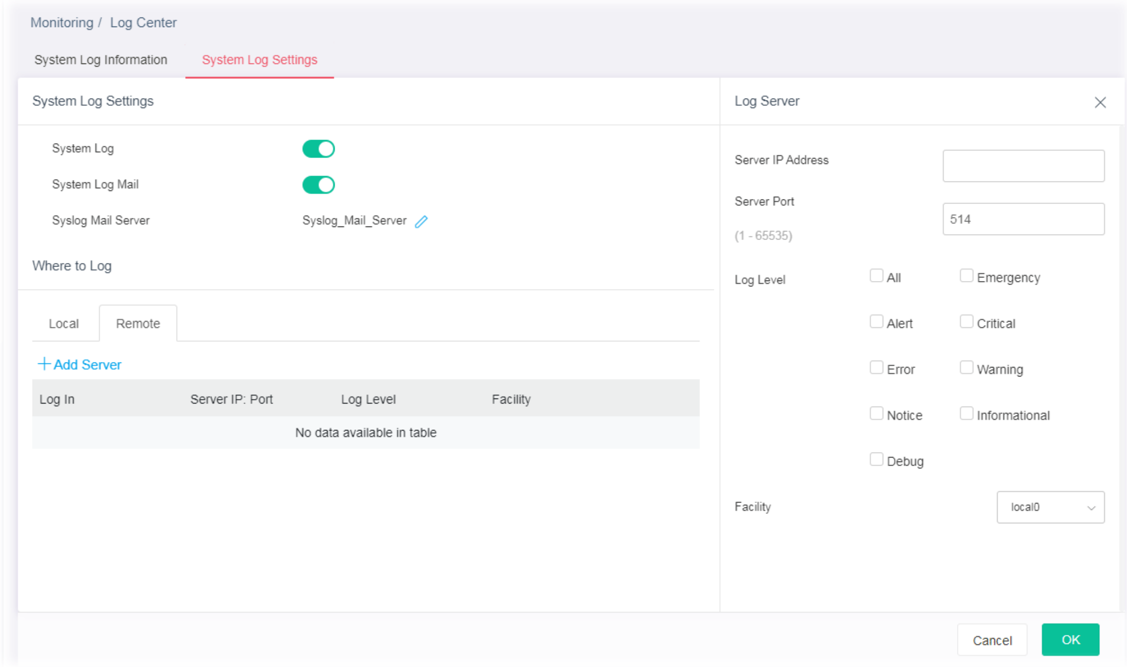
Where to Log

Log In	Server IP: Port	Log Level	Facility
No data available in table			

Available settings are explained as follows:

Item	Description
System Log Settings	
System Log	**Enable / Disable** – Click the toggle to enable / disable this function. ● - means “Enable”. ○ - 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	
+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.


Monitoring / Log Center

System Log Information | System Log Settings

System Log Settings

System Log: on

System Log Mail: on

Syslog Mail Server: Syslog_Mail_Server

Where to Log

Local | Remote

+ Add Server

Log In	Server IP: Port	Log Level	Facility
No data available in table			

Log Server

Server IP Address:

Server Port (1 - 65535): 514

Log Level: □ All □ Emergency □ Alert □ Critical □ Error □ Warning □ Notice □ Informational □ Debug

Facility: local0

Cancel | OK

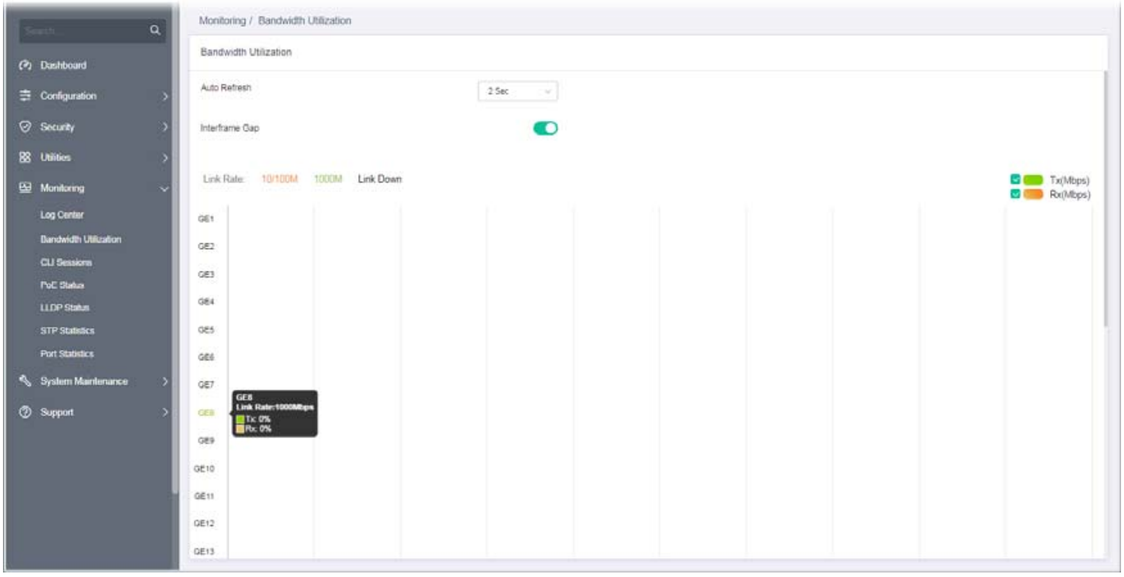
Available settings are explained as follows:

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 (GE1 to GE28).



Monitoring / Bandwidth Utilization

Bandwidth Utilization

Auto Refresh: 2 Sec

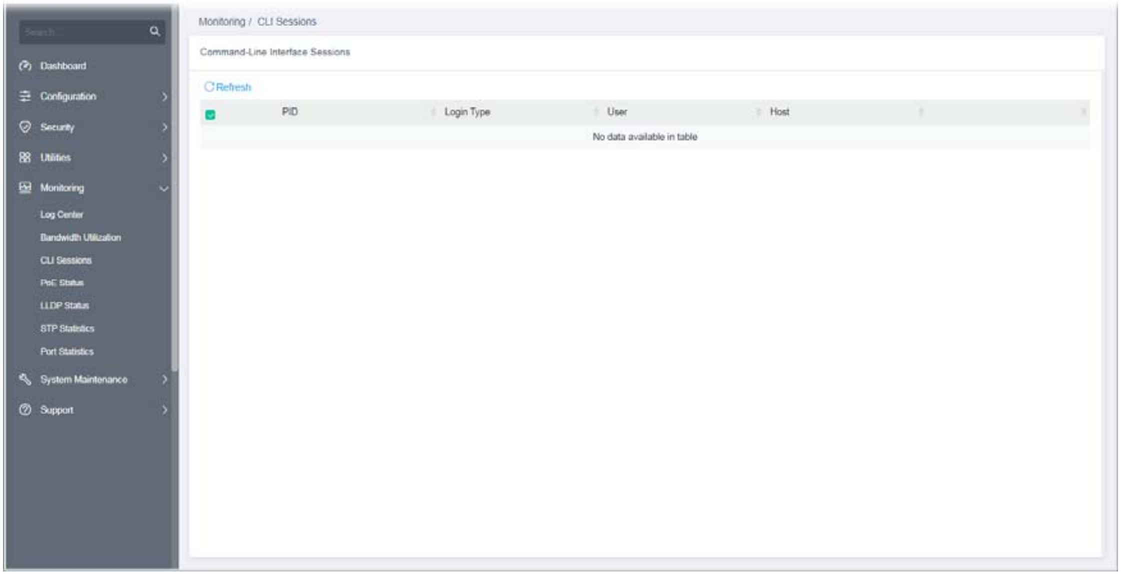
Interframe Gap: ●

Available settings are explained as follows:

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

V-3 CLI Sessions

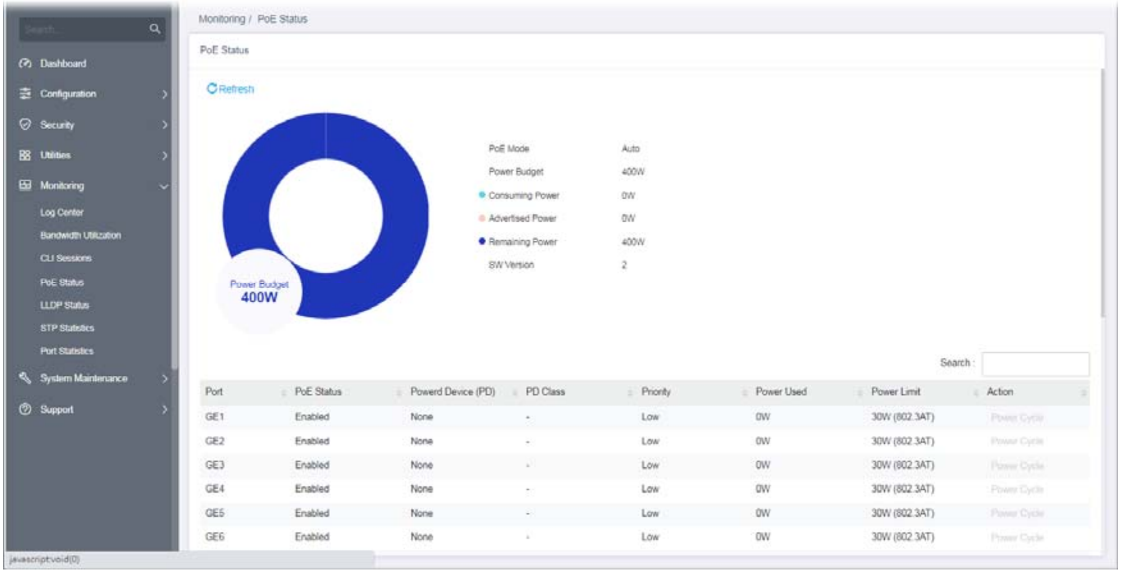
This page shows a list of CLI command executed. You can delete the selected CLI session by click the Remove button under the Edit item.



☑	PID	Login Type	User	Host
			No data available in table	

V-4 PoE Status

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



PoE Mode	Auto
Power Budget	400W
● Consuming Power	0W
● Advertised Power	0W
● Remaining Power	400W
SW Version	2

Port	PoE Status	Powerd Device (PD)	PD Class	Priority	Power Used	Power Limit	Action
GE1	Enabled	None	-	Low	0W	30W (802.3AT)	Power Cycle
GE2	Enabled	None	-	Low	0W	30W (802.3AT)	Power Cycle
GE3	Enabled	None	-	Low	0W	30W (802.3AT)	Power Cycle
GE4	Enabled	None	-	Low	0W	30W (802.3AT)	Power Cycle
GE5	Enabled	None	-	Low	0W	30W (802.3AT)	Power Cycle
GE6	Enabled	None	-	Low	0W	30W (802.3AT)	Power Cycle

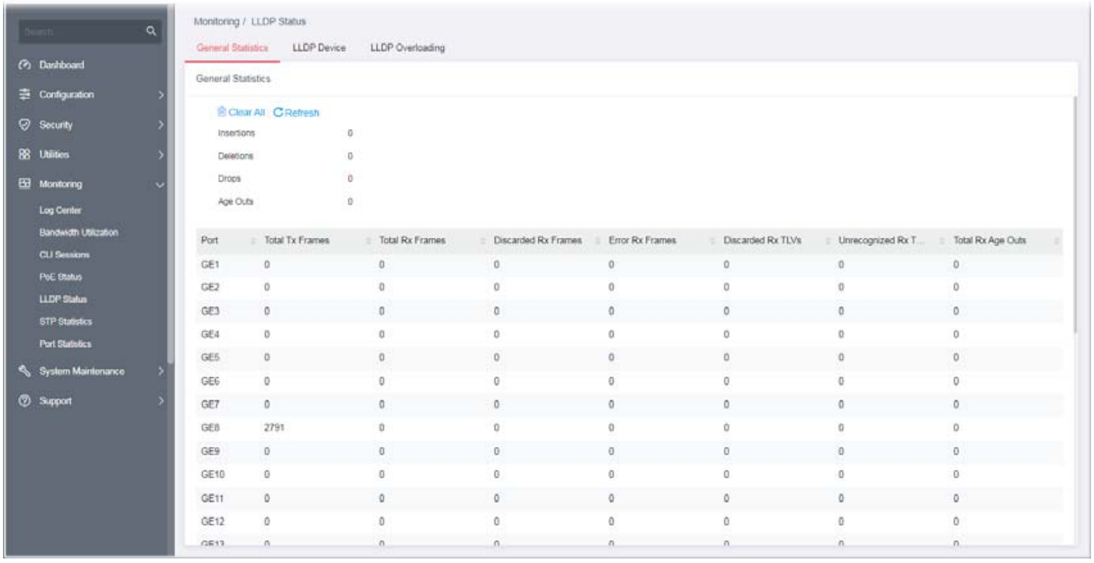
Available settings are explained as follows:

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-5 LLDP Status

V-5-1 General Statistics

This page offers the statistics of LLDP packets of each port (GE1 to GE28).



Insertions 0

Deletions 0

Drops 0

Age Outs 0

Port	Total Tx Frames	Total Rx Frames	Discarded Rx Frames	Error Rx Frames	Discarded Rx TLVs	Unrecognized Rx T...	Total Rx Age Outs
GE1	0	0	0	0	0	0	0
GE2	0	0	0	0	0	0	0
GE3	0	0	0	0	0	0	0
GE4	0	0	0	0	0	0	0
GE5	0	0	0	0	0	0	0
GE6	0	0	0	0	0	0	0
GE7	0	0	0	0	0	0	0
GE8	2791	0	0	0	0	0	0
GE9	0	0	0	0	0	0	0
GE10	0	0	0	0	0	0	0
GE11	0	0	0	0	0	0	0
GE12	0	0	0	0	0	0	0
GE13	0	0	0	0	0	0	0

Available settings are explained as follows:

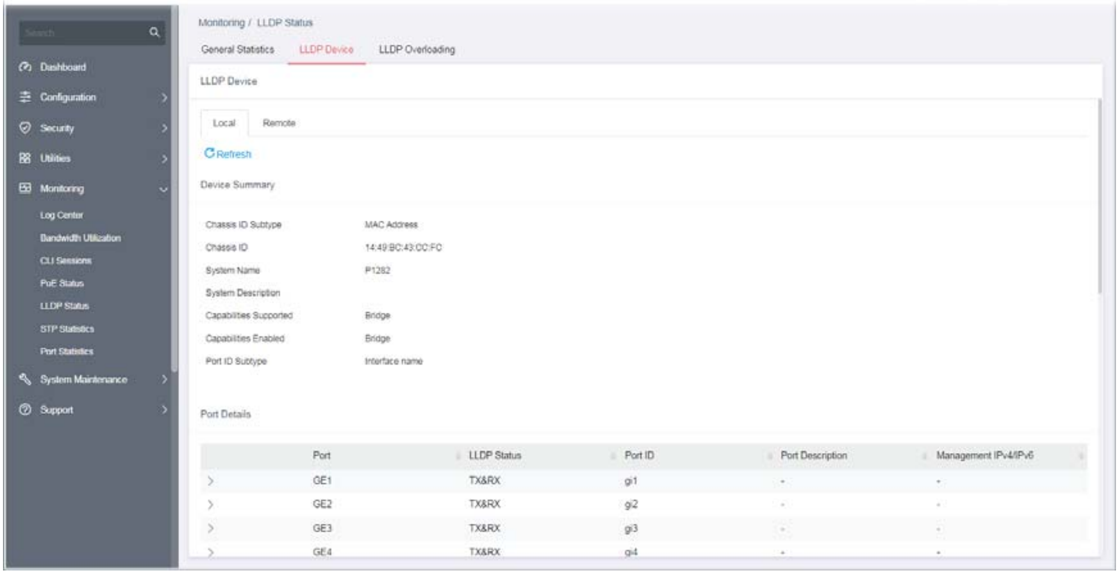
Item	Description
General Statistics	
Clear All	Clear it to remove all logs displayed in this page.
Refresh	Click it to refresh the status page.
Port	Displays the port number (GE1 to GE28).

V-5-2 LLDP Device

This page displays information for LLDP local and remote devices.

V-5-2-1 Local

This page displays information for LLDP local device.



Device Summary

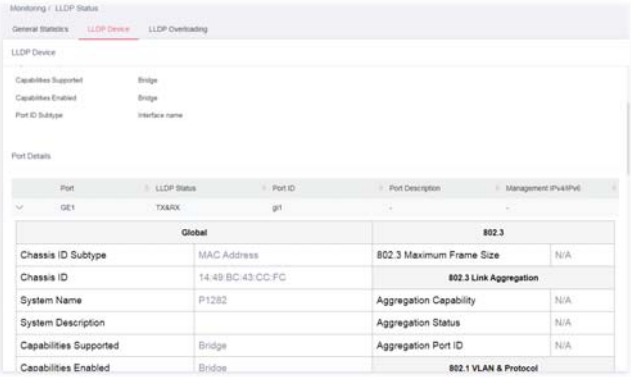
Chassis ID Subtype	MAC Address
Chassis ID	14:49:BC:43:CC:FC
System Name	P1282
System Description	
Capabilities Supported	Bridge
Capabilities Enabled	Bridge
Port ID Subtype	Interface name

Port Details

	Port	LLDP Status	Port ID	Port Description	Management IPv4/IPv6
>	GE1	TX&RX	gi1	-	-
>	GE2	TX&RX	gi2	-	-
>	GE3	TX&RX	gi3	-	-
>	GE4	TX&RX	gi4	-	-

Available settings are explained as follows:

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

Monitoring / LLDP Status

General Statistics | LLDP Device | LLDP Overloading

LLDP Device

Capabilities Supported	Bridge
Capabilities Enabled	Bridge
Port ID Subtype	Interface name

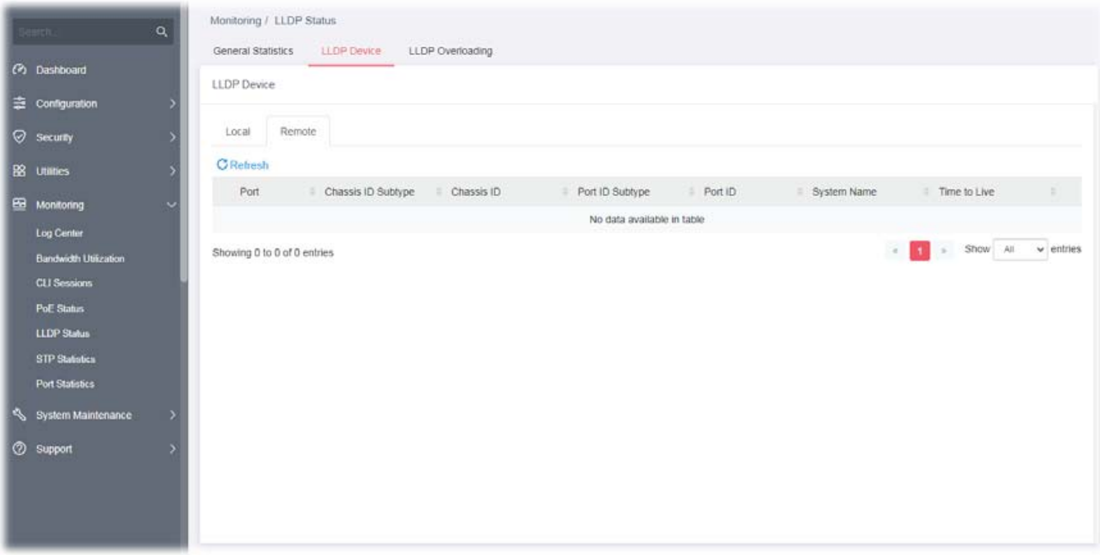
Port Details

Port	LLDP Status	Port ID	Port Description	Management IPv4/IPv6
GE1	TX&RX	gi1	-	-

Global		802.3	
Chassis ID Subtype	MAC Address	802.3 Maximum Frame Size	N/A
Chassis ID	14:49:BC:43:CC:FC	802.3 Link Aggregation	
System Name	P1282	Aggregation Capability	N/A
System Description		Aggregation Status	N/A
Capabilities Supported	Bridge	Aggregation Port ID	N/A
Capabilities Enabled	Bridge	802.1 VLAN & Protocol	

V-5-2-2 Remote

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



Monitoring / LLDP Status

General Statistics | LLDP Device | LLDP Overloading

LLDP Device

Local | Remote

Refresh

Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	System Name	Time to Live
No data available in table						

Showing 0 to 0 of 0 entries

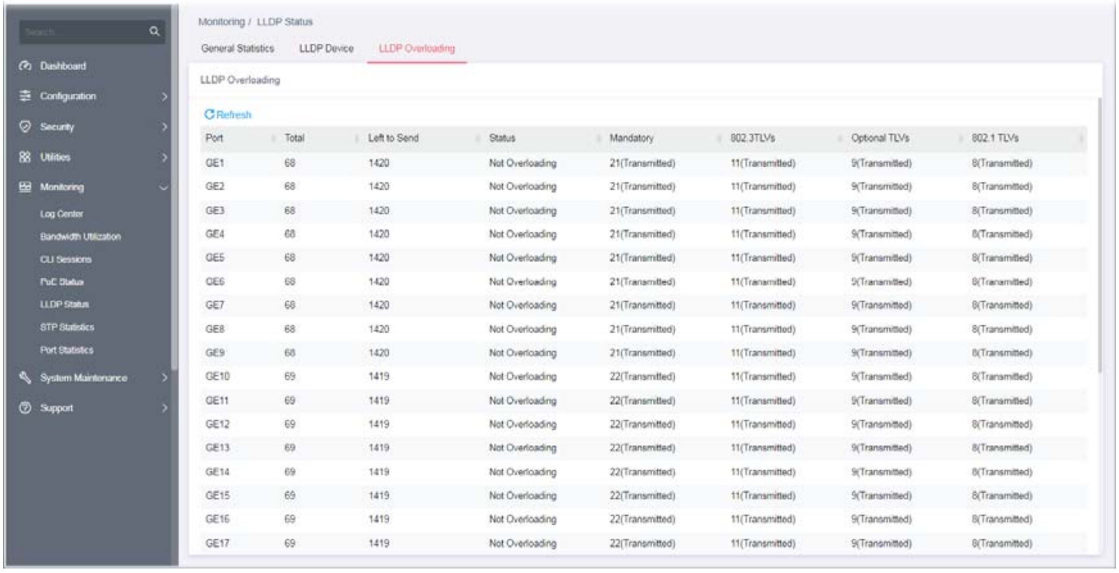
‹ 1 › Show All entries

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-5-3 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.



Monitoring / LLDP Status

LLDP Overloading

Port	Total	Left to Send	Status	Mandatory	802.3TLVs	Optional TLVs	802.1 TLVs
GE1	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE2	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE3	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE4	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE5	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE6	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE7	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE8	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE9	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE10	69	1419	Not Overloading	22(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE11	69	1419	Not Overloading	22(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE12	69	1419	Not Overloading	22(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE13	69	1419	Not Overloading	22(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE14	69	1419	Not Overloading	22(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE15	69	1419	Not Overloading	22(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE16	69	1419	Not Overloading	22(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
GE17	69	1419	Not Overloading	22(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)

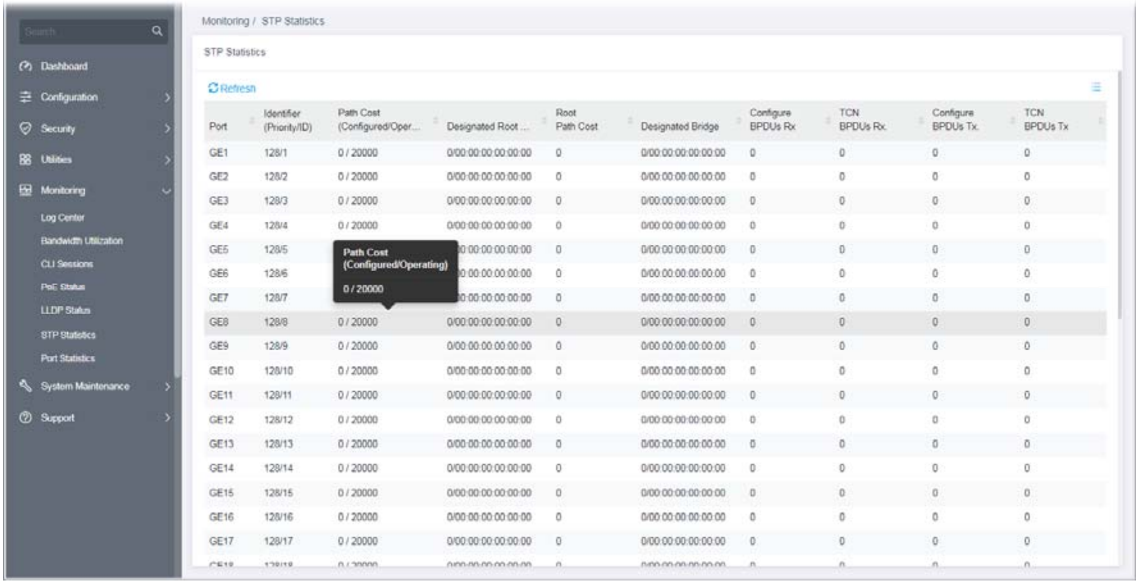
Available settings are explained as follows:

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-6 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.



Port	Identifier (Priority/ID)	Path Cost (Configured/Oper...	Designated Root ...	Root Path Cost	Designated Bridge	Configure BPDUs Rx	TCN BPDUs Rx.	Configure BPDUs Tx.	TCN BPDUs Tx
GE1	128/1	0 / 20000	0/00:00:00:00:00:00	0	0/00:00:00:00:00:00	0	0	0	0
GE2	128/2	0 / 20000	0/00:00:00:00:00:00	0	0/00:00:00:00:00:00	0	0	0	0
GE3	128/3	0 / 20000	0/00:00:00:00:00:00	0	0/00:00:00:00:00:00	0	0	0	0
GE4	128/4	0 / 20000	0/00:00:00:00:00:00	0	0/00:00:00:00:00:00	0	0	0	0
GE5	128/5		0:00:00:00:00:00	0	0/00:00:00:00:00:00	0	0	0	0
GE6	128/6		0:00:00:00:00:00	0	0/00:00:00:00:00:00	0	0	0	0
GE7	128/7		0:00:00:00:00:00	0	0/00:00:00:00:00:00	0	0	0	0
GE8	128/8	0 / 20000	0/00:00:00:00:00:00	0	0/00:00:00:00:00:00	0	0	0	0
GE9	128/9	0 / 20000	0/00:00:00:00:00:00	0	0/00:00:00:00:00:00	0	0	0	0
GE10	128/10	0 / 20000	0/00:00:00:00:00:00	0	0/00:00:00:00:00:00	0	0	0	0
GE11	128/11	0 / 20000	0/00:00:00:00:00:00	0	0/00:00:00:00:00:00	0	0	0	0
GE12	128/12	0 / 20000	0/00:00:00:00:00:00	0	0/00:00:00:00:00:00	0	0	0	0
GE13	128/13	0 / 20000	0/00:00:00:00:00:00	0	0/00:00:00:00:00:00	0	0	0	0
GE14	128/14	0 / 20000	0/00:00:00:00:00:00	0	0/00:00:00:00:00:00	0	0	0	0
GE15	128/15	0 / 20000	0/00:00:00:00:00:00	0	0/00:00:00:00:00:00	0	0	0	0
GE16	128/16	0 / 20000	0/00:00:00:00:00:00	0	0/00:00:00:00:00:00	0	0	0	0
GE17	128/17	0 / 20000	0/00:00:00:00:00:00	0	0/00:00:00:00:00:00	0	0	0	0
GE18	128/18	0 / 20000	0/00:00:00:00:00:00	0	0/00:00:00:00:00:00	0	0	0	0

Path Cost
(Configured/Operating)

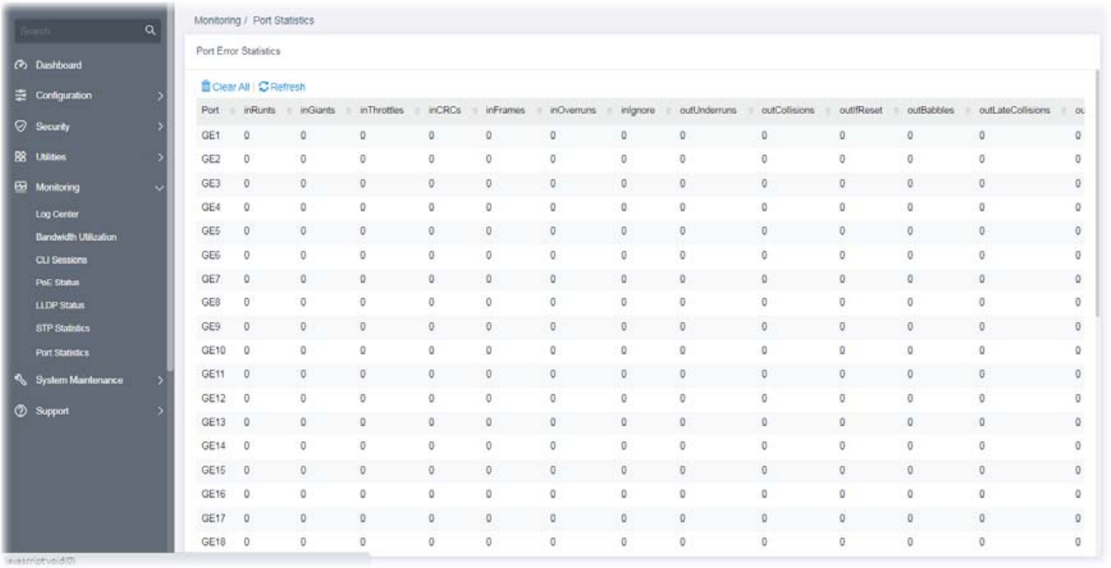
0 / 20000

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-7 Port Statistics

This page displays statistics for GE/LAG ports.



Monitoring / Port Statistics

Port Error Statistics

Clear All | Refresh

Port	inRunts	inGiants	inThrottles	inCRCs	inFrames	inOverruns	inIgnore	outUnderruns	outCollisions	outIfReset	outBabbles	outLateCollisions	ou
GE1	0	0	0	0	0	0	0	0	0	0	0	0	0
GE2	0	0	0	0	0	0	0	0	0	0	0	0	0
GE3	0	0	0	0	0	0	0	0	0	0	0	0	0
GE4	0	0	0	0	0	0	0	0	0	0	0	0	0
GE5	0	0	0	0	0	0	0	0	0	0	0	0	0
GE6	0	0	0	0	0	0	0	0	0	0	0	0	0
GE7	0	0	0	0	0	0	0	0	0	0	0	0	0
GE8	0	0	0	0	0	0	0	0	0	0	0	0	0
GE9	0	0	0	0	0	0	0	0	0	0	0	0	0
GE10	0	0	0	0	0	0	0	0	0	0	0	0	0
GE11	0	0	0	0	0	0	0	0	0	0	0	0	0
GE12	0	0	0	0	0	0	0	0	0	0	0	0	0
GE13	0	0	0	0	0	0	0	0	0	0	0	0	0
GE14	0	0	0	0	0	0	0	0	0	0	0	0	0
GE15	0	0	0	0	0	0	0	0	0	0	0	0	0
GE16	0	0	0	0	0	0	0	0	0	0	0	0	0
GE17	0	0	0	0	0	0	0	0	0	0	0	0	0
GE18	0	0	0	0	0	0	0	0	0	0	0	0	0

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 (GE1 to GE28).

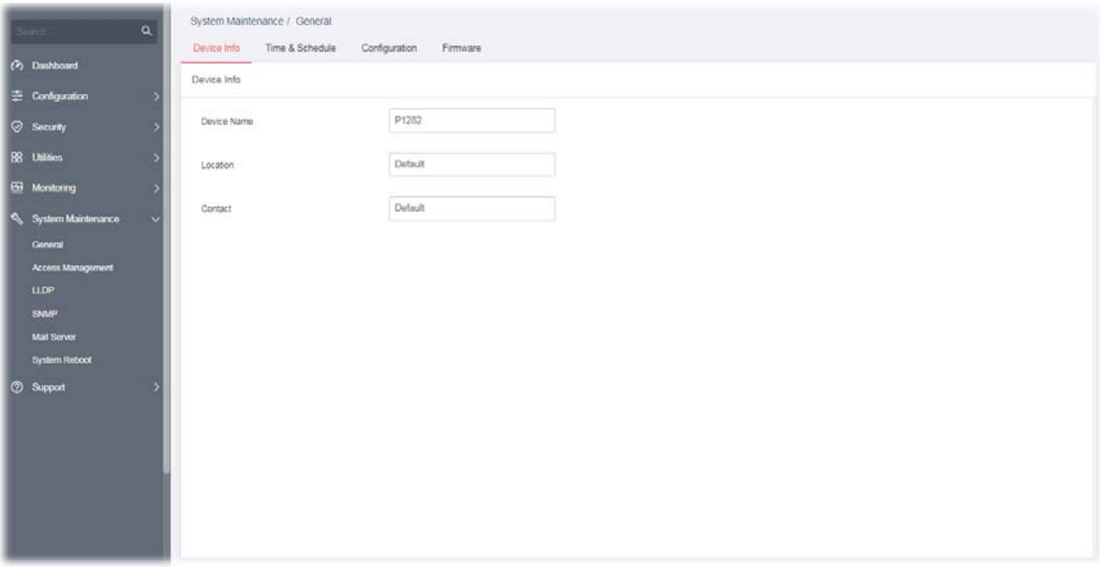
This page is left blank.

Chapter VI System Maintenance

VI-1 General

VI-1-1 Device Info

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



Device Info

Device Name: P1282

Location: Default

Contact: Default

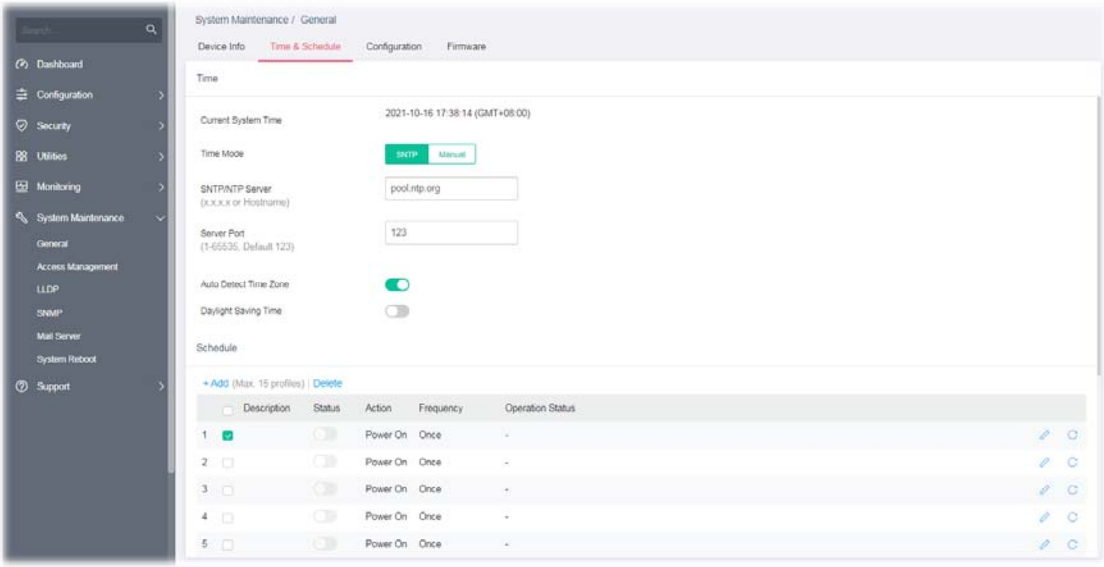
Available settings are explained as follows:

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

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

VI-1-2 Time & Schedule

This page allows users to configure maximum 15 schedule rules.



Time

Current System Time	2021-10-16 17:38:14 (GMT+08:00)
Time Mode	SNTP / Manual
SNTP/NTP Server (x.x.x.x or Hostname)	pool.ntp.org
Server Port (1-65535, Default 123)	123
Auto Detect Time Zone	●
Daylight Saving Time	○

Schedule

+ Add (Max. 15 profiles) | Delete

	□	Description	Status	Action	Frequency	Operation Status
1	☑		○	Power On	Once	-
2	□		○	Power On	Once	-
3	□		○	Power On	Once	-
4	□		○	Power On	Once	-
5	□		○	Power On	Once	-

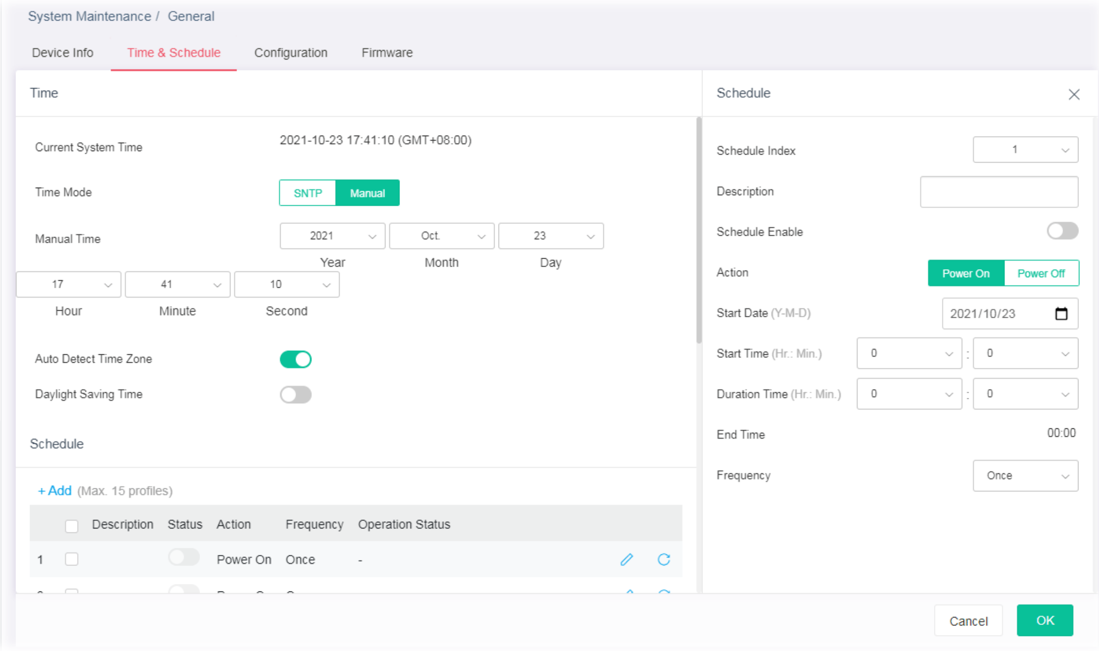
Available settings are explained as follows:

Item	Description
Time	
Current System Time	Display current system time based on the time server.
Time Mode	Select **SNTP** or **Manual**. If SNTP is selected, configure: ● **SNTP/NTP Server** - Enter the web site of the time server or the IP address of the server. ● **Server Port** - Enter the port number use by the time server. If Manual is selected, configure: ● **Manual Time** - Specify static time (year, month, day, hours, minutes and seconds) manually. **Auto Detect Time Zone** - Click the toggle to enable / disable this function. ● - means "Enable". ○ - means "Disable". **Daylight Saving Time** - Click the toggle to enable / disable this function. If enabled, select the mode of daylight saving time. ● **Recurring** - Using recurring mode of daylight saving time. ● **Non-Recurring** – Using non-recurring mode of daylight saving time. ● **USA** –Using daylight saving time in the United States that starts on the second Sunday of March and ends on the first Sunday of November. ● **European** - Using daylight saving time in the Europe that starts on the last Sunday.

when **Recurring** is selected	**Daylight Saving Time Offset -** Specify the adjust offset of daylight saving time. **Recurring From** - Specify the starting time of recurring daylight saving time. **Recurring To** - Specify the ending time of recurring daylight saving time.
when **Non-Recurring** is selected	**Daylight Saving Time Offset -** Specify the adjust offset of daylight saving time. **Non-recurring From** - Specify the starting time of non-recurring daylight saving time. **Non-recurring To** - Specify the ending time of recurring daylight saving time.
Schedule	
+Add	Click to add a new schedule (up to 15). **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.



Time

Current System Time 2021-10-23 17:41:10 (GMT+08:00)

Time Mode SNTP Manual

Manual Time 2021 Year, Oct. Month, 23 Day, 17 Hour, 41 Minute, 10 Second

Auto Detect Time Zone

Daylight Saving Time

Schedule

+ Add (Max. 15 profiles)

	Description	Status	Action	Frequency	Operation Status
1	□		Power On	Once	-

Schedule

Schedule Index 1

Description

Schedule Enable

Action Power On Power Off

Start Date (Y-M-D) 2021/10/23

Start Time (Hr.: Min.) 0 : 0

Duration Time (Hr.: Min.) 0 : 0

End Time 00:00

Frequency Once

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. ● - means “Enable”. The selected schedule profile will take action as configured. ○ - means “Disable”. The selected schedule profile will not take action but be saved for future use.
Action	Specify which action should perform during the period of the schedule. **Power On** – PoE connection is always on. **Power Off** - PoE connection is always down.
Start Date	Specify the starting date of the schedule by choosing from a drop down calendar.
Start Time	Specify the starting time of the schedule by using the drop down list to specify the starting hours and minutes.
Duration Time	Specify the ending time of the schedule by using the drop down list to specify the ending hours and minutes.
End Time	Displays the time period setting.
Frequency	Specify how often the schedule will be applied. **Once** - The schedule will be applied just once. **Weekdays Routine** - Specify which days in one week should perform the schedule. ● **Every** - Check to select the days in a week. **Monthly Routine** - Specify the day in a month as the starting point. ● **Duration Time** - Use the drop down list to select the date in a month. **Few Days Routine** - The period of cycle duration is between 1 day and 31 days. For example, 7 means the whole cycle is 7 days; 20 means the whole cycle is 20 days. When the time is up, the PoE device will be turned on of off automatically. ● **Every** - Use the drop down list to select the date in a month.

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

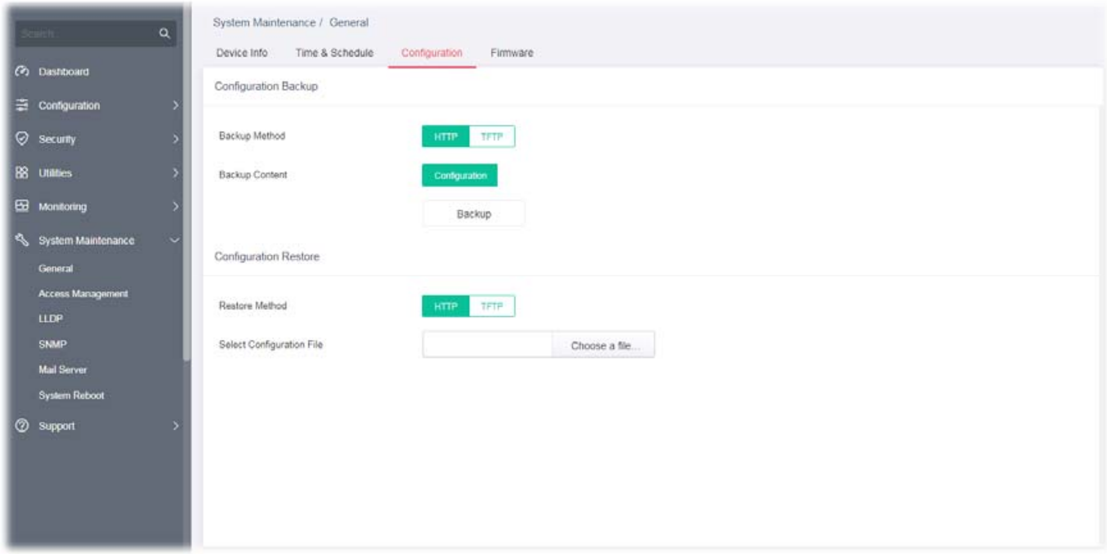
To modify an existing schedule profile, click the link of ✎ of the one to be changed.

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.



Configuration Backup

Backup Method: HTTP TFTP

Backup Content: Configuration

Configuration Restore

Restore Method: HTTP TFTP

Select Configuration File

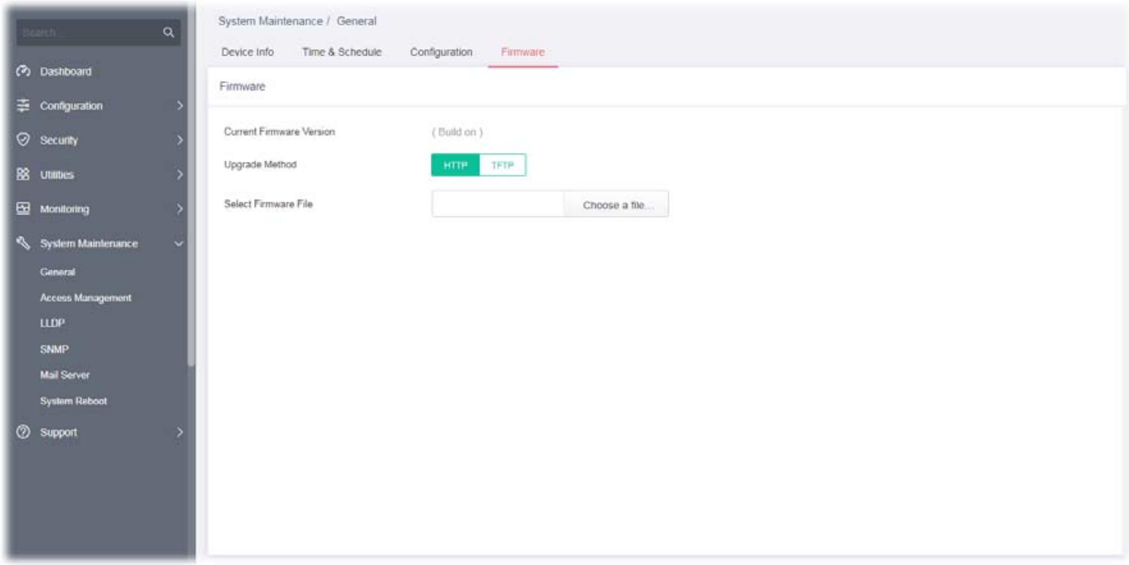
Available settings are explained as follows:

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

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

VI-1-4 Firmware

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



Firmware

Current Firmware Version (Build on)

Upgrade Method HTTP TFTP

Select Firmware File Choose a file...

Available settings are explained as follows:

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

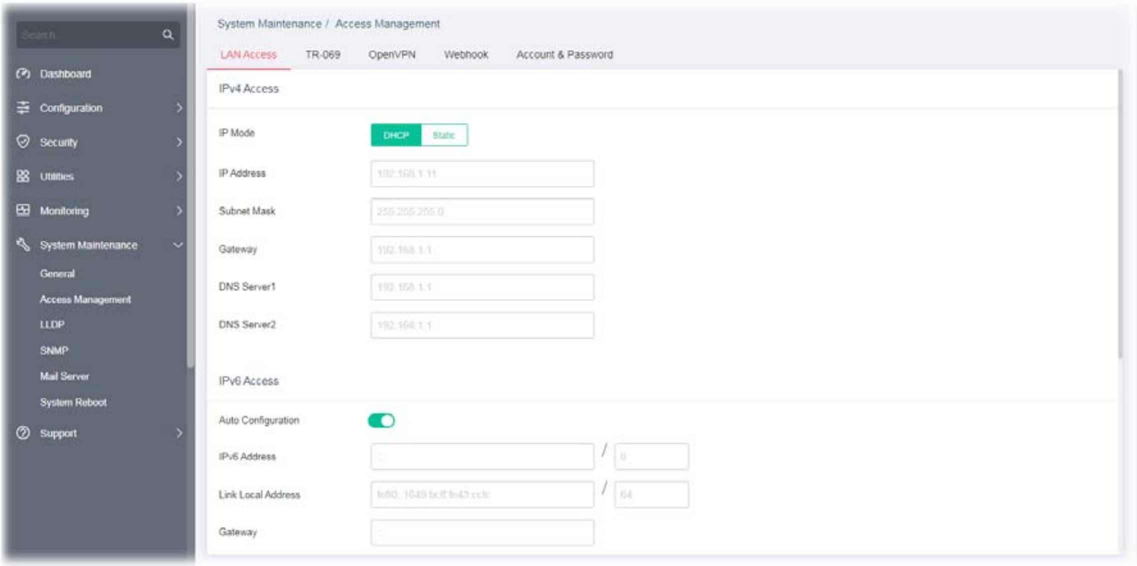
After finishing this web page configuration, please click **OK** to save the settings.

VI-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.



IPv4 Access

IP Mode: DHCP | Static

IP Address: 192.168.1.11

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

DNS Server1: 192.168.1.1

DNS Server2: 192.168.1.1

IPv6 Access

Auto Configuration: ●

IPv6 Address: :: / 0

Link Local Address: fe80::1649:bcff:fe43:ccfc / 64

Gateway: ::

Available settings are explained as follows:

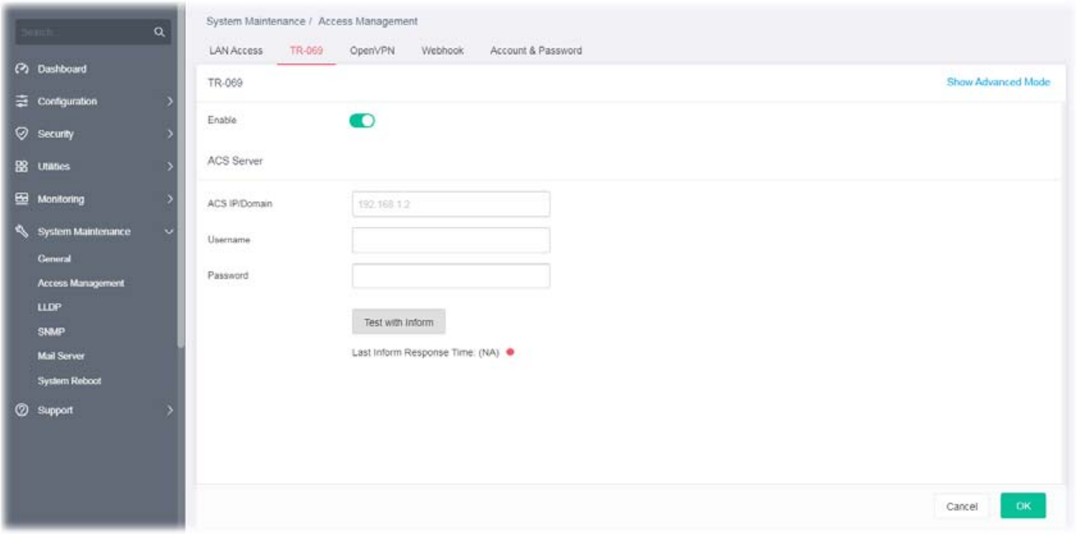
Item	Description
IPv4 Access	
IP Mode	Select the mode of network connection**.** **DHCP** - Use static IPv4 address. **Static** - Use DHCP provisioned IP address and Gateway if feasible. ● **IP Address** - Enter the IP address of your switch in dotted decimal notation for example 192.168.1.224. If static mode is enabled, enter IP address in this field. ● **Subnet Mask** - Enter the IP subnet mask of your switch in dotted decimal notation for example 255.255.255.0. If static mode is enabled, enter subnet mask in this field. ● **Gateway** - Enter the IP address of the gateway in dotted decimal notation. If static mode is enabled, enter gateway address in this field. ● **DNS Server1/2** - Enter primary/ secondary DNS server address in this field.

IPv6 Access	
Auto Configuration	**Enabled** - Let the switch automatically configure IPv6 address. Click the toggle to enable / disable this function. ● - means “Enable”. ○ - means “Disable”. ● **DHCPv6 Client** - Enable this feature if there is a DHCPv6 server on your network for assigning IPv6 Address, instead of using Router Advertisement. **Disabled** - ● **IPv6 Address** - Enter the IPv6 address of your switch. If auto configuration mode is disabled, enter IPv6 address in this field. ● **Gateway** - Enter the IPv6 address of the router as your default IPv6 gateway to access IPv6 Internet or other IPv6 network. ● **DNS Server1/2** - Enter primary/ secondary DNS server address in this field.
Management VLAN	
Management VLAN	Select the VLAN ID as management VLAN.
Protocol Access	
HTTP Server, HTTPS Server, 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 TR-069

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



TR-069

Enable ●

ACS Server

ACS IP/Domain: 192.168.1.2

Username:

Password:

Last Inform Response Time: (NA) ●

Available settings are explained as follows:

Item	Description

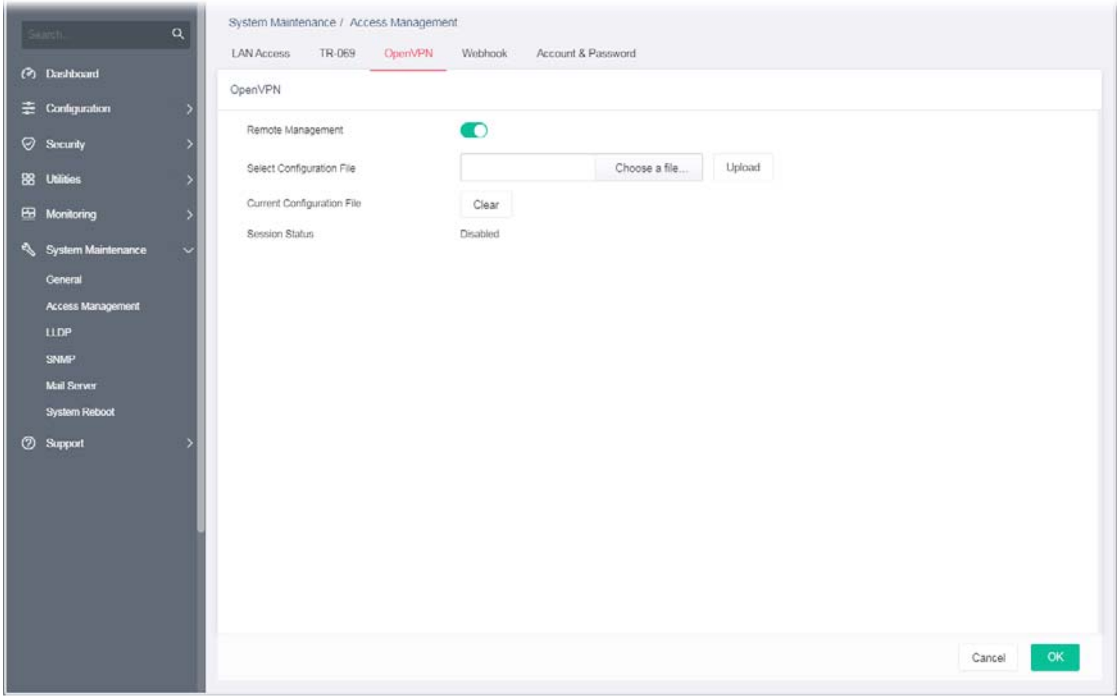
Show/Hide Advanced Mode	Click to display / hide the advanced mode settings.
TR-069	Click the toggle to enable / disable this function. ● - means “Enable”. ○ - means “Disable”.
Basic Mode - ACS Server	
ACS IP/Domain	Enter the IP address or domain name of the server.
Username	Enter the username that you wan to link with the VigorACS (Auto Configuration Server).
Password	Enter the password that you wan to link with the VigorACS (Auto Configuration Server).
Test with Inform	Click to send a message to test if this CPE is able to communicate with VigorACS server.
Advanced Mode - ACS Server	
Protocol	Choose **HTTP** or **HTTPS** for connecting with VigorACS.
Port	Enter a value that VigorACS can use to access to this switch.
ACS IP/Domain	Enter the IP address or domain name of the server.
Handler	Enter the URL that you wan to link with the VigorACS (Auto Configuration Server).
Username	Enter the username that you wan to link with the VigorACS (Auto Configuration Server).
Password	Enter the password that you wan to link with the VigorACS (Auto Configuration Server).
Test with Inform	Click to send a message to test if this CPE is able to communicate with VigorACS server.
CPE Settings	
CPE Client	Choose **HTTP** or **HTTPS** for connecting with VigorACS.
URL	Display the URL of VigorSwitch
Port	Enter a value that VigorACS can use to access to this switch.
Username	Enter the username that VigorACS can use to access into this switch.
Password	Enter the password that VigorACS can use to access into this switch.
TLS Version	
TLS Minimum Protocol Version	Due to security consideration, the built-in HTTPS VPN server of the router had upgraded to TLS1.x protocol (TLS1.2/TLS1.3). Select one of the versions.
Periodic Inform	
Enable	Click the toggle to enable/disable the function.
Interval Time	Set the interval time for the switch to send notification to CPE.
STUN Settings	

Enable	Click the toggle to enable / disable this function. ● - means "Enable". ○ - means "Disable".
Server Address	Enter the IP address of the STUN server.
Server port	Enter the port number of the STUN server.
Minimum Keep Alive Period	If the STUN server is enabled, the switch must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds".
Maximum Keep Alive Period	If the STUN server is enabled, the switch must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.
Notification	
Port Link Up/Down	Vigor system will check the health status of LAN ports including link up /down, speed change or PoE power disconnection. Select LAN port(s) to do the health check of port link.
Link Speed Change	Select LAN port(s) to do the health check of speed change.
PoE Port Warning	Select LAN port(s) to do the health check of PoE power.

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

VI-2-3 OpenVPN

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



OpenVPN

Remote Management ●

Select Configuration File

Current Configuration File

Session Status Disabled

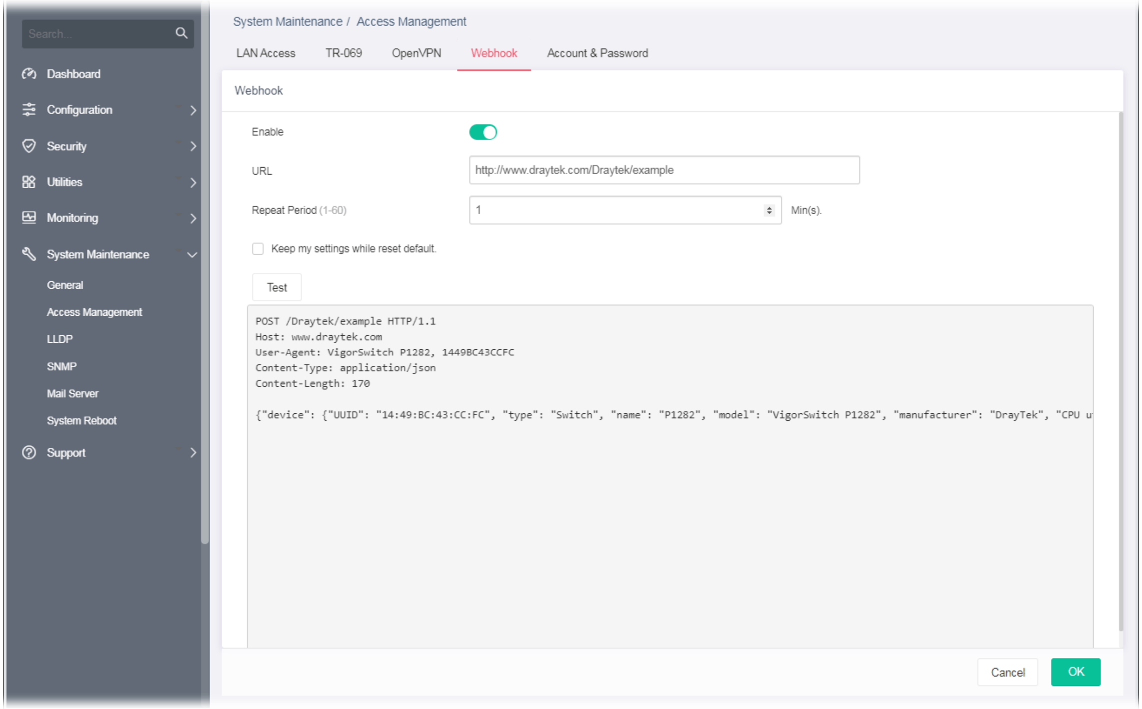
Available settings are explained as follows:

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

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

VI-2-4 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.



Enable ●

URL http://www.draytek.com/Draytek/example

Repeat Period (1-60) 1 Min(s).

□ Keep my settings while reset default.

```
POST /Draytek/example HTTP/1.1
Host: www.draytek.com
User-Agent: VigorSwitch P1282, 1449BC43CCFC
Content-Type: application/json
Content-Length: 170

{"device": {"UUID": "14:49:BC:43:CC:FC", "type": "Switch", "name": "P1282", "model": "VigorSwitch P1282", "manufacturer": "DrayTek", "CPU u
```

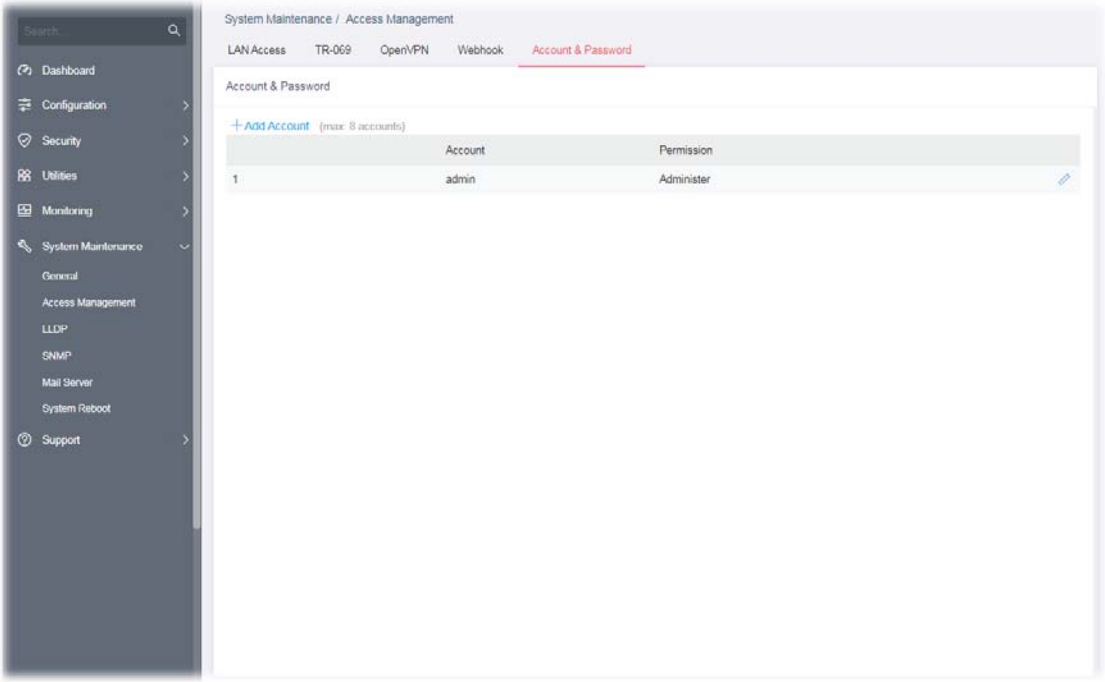
Available settings are explained as follows:

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

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

VI-2-5 Account & Password

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



System Maintenance / Access Management

Account & Password

+Add Account (max 8 accounts)

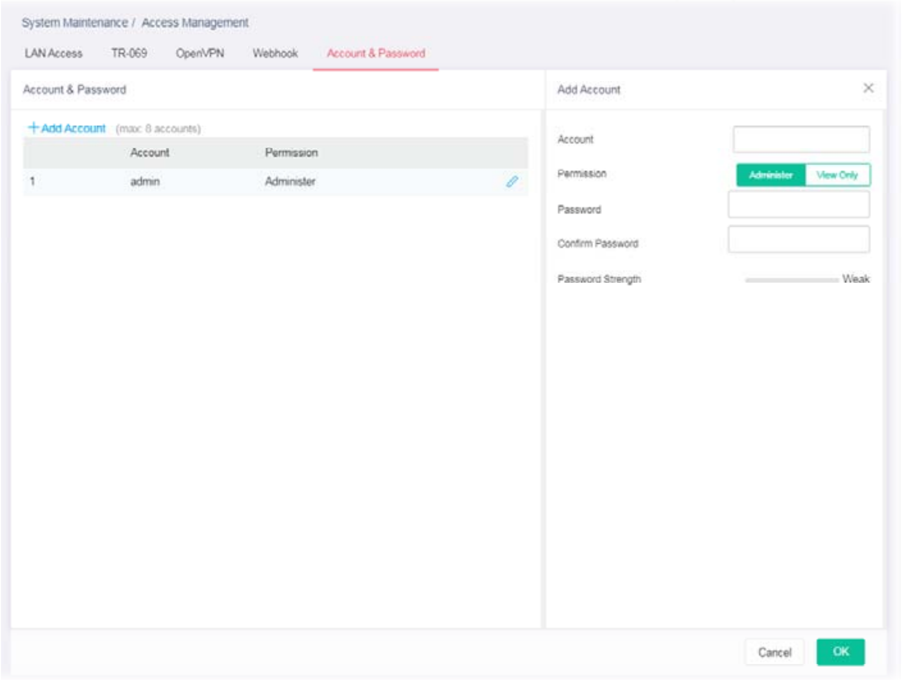
	Account	Permission	
1	admin	Administer	✎

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.
✎	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.



Account & Password

(max 8 accounts)

	Account	Permission
1	admin	Administer

Add Account

Account

Permission [✓ Administer] View Only

Password

Confirm Password

Password Strength Weak

Available settings are explained as follows:

Item	Description
Add Account	
Account	Enter a username for new account. If you want to modify an existed user account, simply enter the same string in this field. Then, modify the password and choose privilege level. After clicking **Apply**, the existed user name will be modified with different values.
Permission	**Administer** - Allow to change switch settings. **View Only** - See switch settings only. Not allow to change it.
Password	Enter a password for new account.
Confirm Password	Enter the password again for confirmation.
Password Strength	Displays the strength of the password, indicated by the words “weak”, “medium” or “strong”.

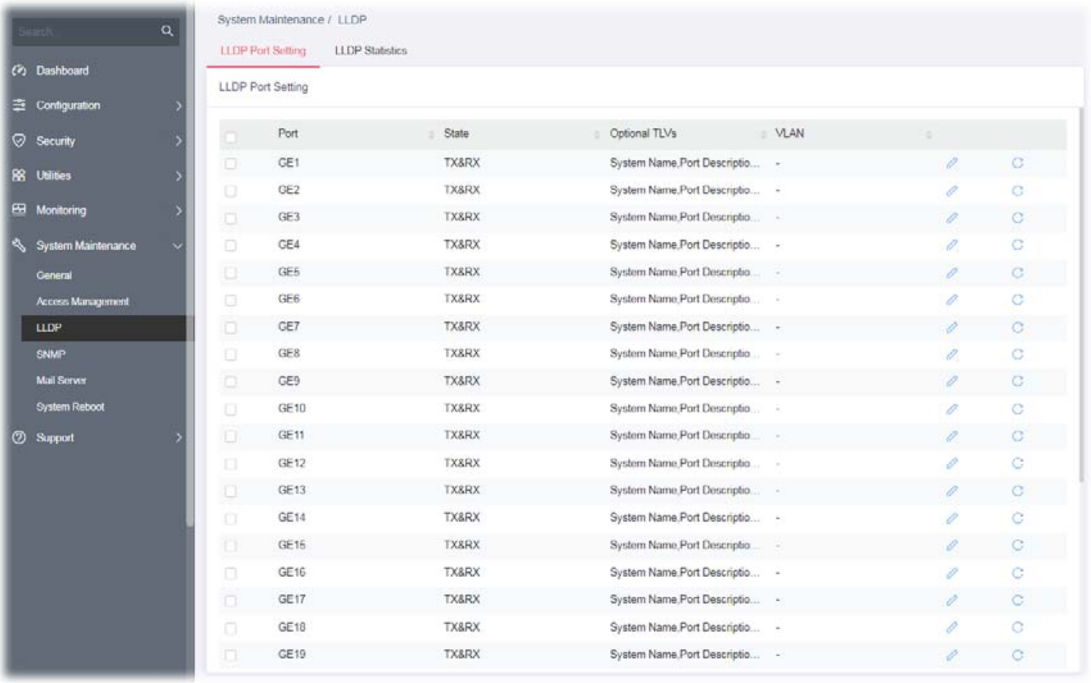
After finishing this web page configuration, please click **OK** to save the settings.

VI-3 LLDP

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

VI-3-1 LLDP Port Setting

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



System Maintenance / LLDP

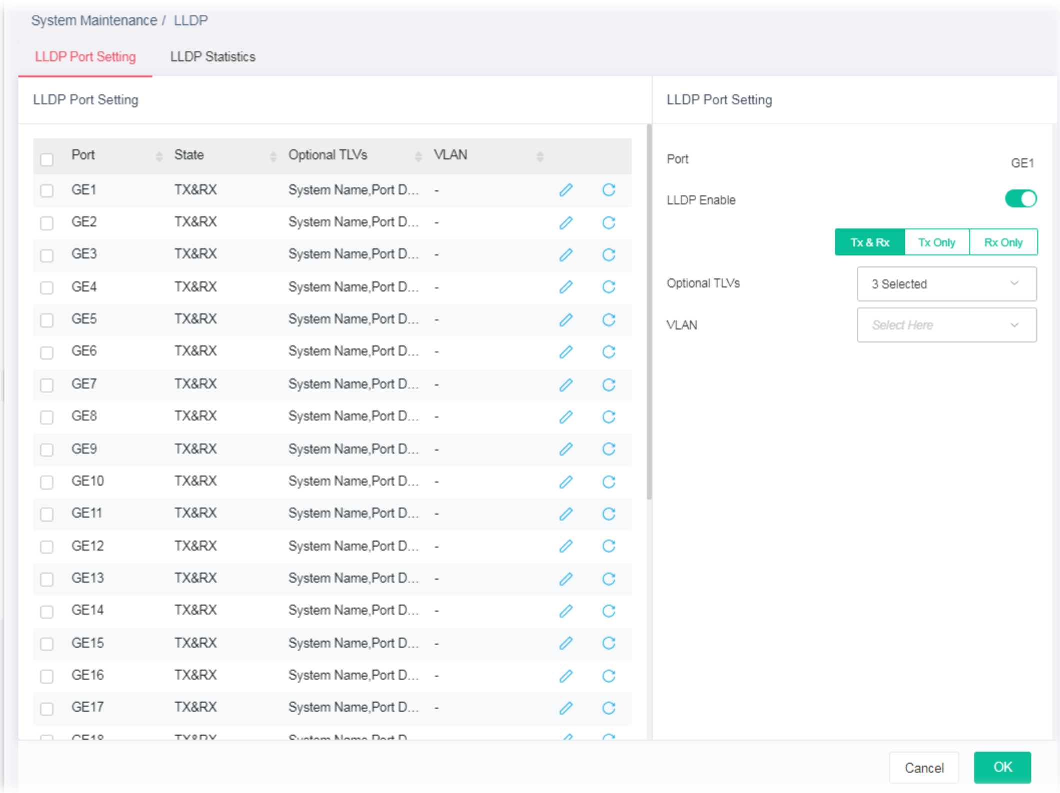
LLDP Port Setting

□	Port	State	Optional TLVs	VLAN		
□	GE1	TX&RX	System Name,Port Descriptio...	-	✎	↻
□	GE2	TX&RX	System Name,Port Descriptio...	-	✎	↻
□	GE3	TX&RX	System Name,Port Descriptio...	-	✎	↻
□	GE4	TX&RX	System Name,Port Descriptio...	-	✎	↻
□	GE5	TX&RX	System Name,Port Descriptio...	-	✎	↻
□	GE6	TX&RX	System Name,Port Descriptio...	-	✎	↻
□	GE7	TX&RX	System Name,Port Descriptio...	-	✎	↻
□	GE8	TX&RX	System Name,Port Descriptio...	-	✎	↻
□	GE9	TX&RX	System Name,Port Descriptio...	-	✎	↻
□	GE10	TX&RX	System Name,Port Descriptio...	-	✎	↻
□	GE11	TX&RX	System Name,Port Descriptio...	-	✎	↻
□	GE12	TX&RX	System Name,Port Descriptio...	-	✎	↻
□	GE13	TX&RX	System Name,Port Descriptio...	-	✎	↻
□	GE14	TX&RX	System Name,Port Descriptio...	-	✎	↻
□	GE15	TX&RX	System Name,Port Descriptio...	-	✎	↻
□	GE16	TX&RX	System Name,Port Descriptio...	-	✎	↻
□	GE17	TX&RX	System Name,Port Descriptio...	-	✎	↻
□	GE18	TX&RX	System Name,Port Descriptio...	-	✎	↻
□	GE19	TX&RX	System Name,Port Descriptio...	-	✎	↻

Available settings are explained as follows:

Item	Description
Port	Displays the index number of GE ports (GE1 to GE28).
Status	Displays the transmission of LLDP PDUs.
Optional TLVs	Displays the data communication protocols and optional information.
VLAN	Displays the VLAN ID number.
✎	Click to modify the LLDP port settings of the selected port.
↻	Clear current settings and return to factory default settings.

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



System Maintenance / LLDP

LLDP Port Setting | LLDP Statistics

LLDP Port Setting

□	Port	State	Optional TLVs	VLAN
□	GE1	TX&RX	System Name,Port D...	-
□	GE2	TX&RX	System Name,Port D...	-
□	GE3	TX&RX	System Name,Port D...	-
□	GE4	TX&RX	System Name,Port D...	-
□	GE5	TX&RX	System Name,Port D...	-
□	GE6	TX&RX	System Name,Port D...	-
□	GE7	TX&RX	System Name,Port D...	-
□	GE8	TX&RX	System Name,Port D...	-
□	GE9	TX&RX	System Name,Port D...	-
□	GE10	TX&RX	System Name,Port D...	-
□	GE11	TX&RX	System Name,Port D...	-
□	GE12	TX&RX	System Name,Port D...	-
□	GE13	TX&RX	System Name,Port D...	-
□	GE14	TX&RX	System Name,Port D...	-
□	GE15	TX&RX	System Name,Port D...	-
□	GE16	TX&RX	System Name,Port D...	-
□	GE17	TX&RX	System Name,Port D...	-
□	GE18	TX&RX	System Name,Port D	

LLDP Port Setting

Port: GE1

LLDP Enable: ●

Tx & Rx | Tx Only | Rx Only

Optional TLVs: 3 Selected

VLAN: Select Here

Cancel | OK

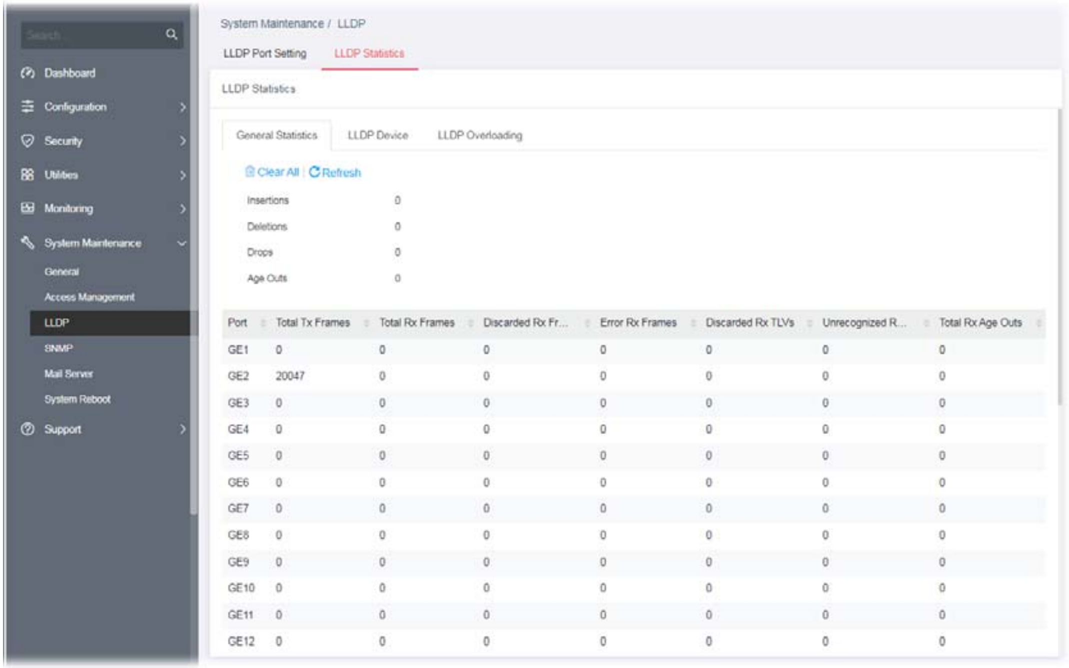
Available settings are explained as follows:

Item	Description
Port	Displays the index number of GE port.
LLDP Enable	Click the toggle to enable / disable this function. ● - means “Enable”. ○ - means “Disable”. **TX&RX** – Transmit and receive LLDP PDUs both. **TX Only** – Transmit LLDP PDUs only. **RX Only** - Receive LLDP PDUs only.
Optional TLVs	Within data communication protocols, optional information may be encoded as a type-length-value or TLV element inside a protocol. TLV is also known as tag-length value. The type and length are fixed in size (typically 1-4 bytes), and the value field is of variable size. Select the LLDP optional TLVs to be carried (multiple selection is allowed). Available items include System Name, Port Description, System Description, System Capability, 802.3 MAC-PHY, 802.3 Link Aggregation, 802.3 Maximum Frame Size, Management Address and 802.1 PVID.
VLAN	Select the VLAN ID number to be performed (multiple selections are allowed).

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

VI-3-2 LLDP Statistics

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



Insertions	0
Deletions	0
Drops	0
Age Outs	0

Port	Total Tx Frames	Total Rx Frames	Discarded Rx Fr...	Error Rx Frames	Discarded Rx TLVs	Unrecognized R...	Total Rx Age Outs
GE1	0	0	0	0	0	0	0
GE2	20047	0	0	0	0	0	0
GE3	0	0	0	0	0	0	0
GE4	0	0	0	0	0	0	0
GE5	0	0	0	0	0	0	0
GE6	0	0	0	0	0	0	0
GE7	0	0	0	0	0	0	0
GE8	0	0	0	0	0	0	0
GE9	0	0	0	0	0	0	0
GE10	0	0	0	0	0	0	0
GE11	0	0	0	0	0	0	0
GE12	0	0	0	0	0	0	0

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

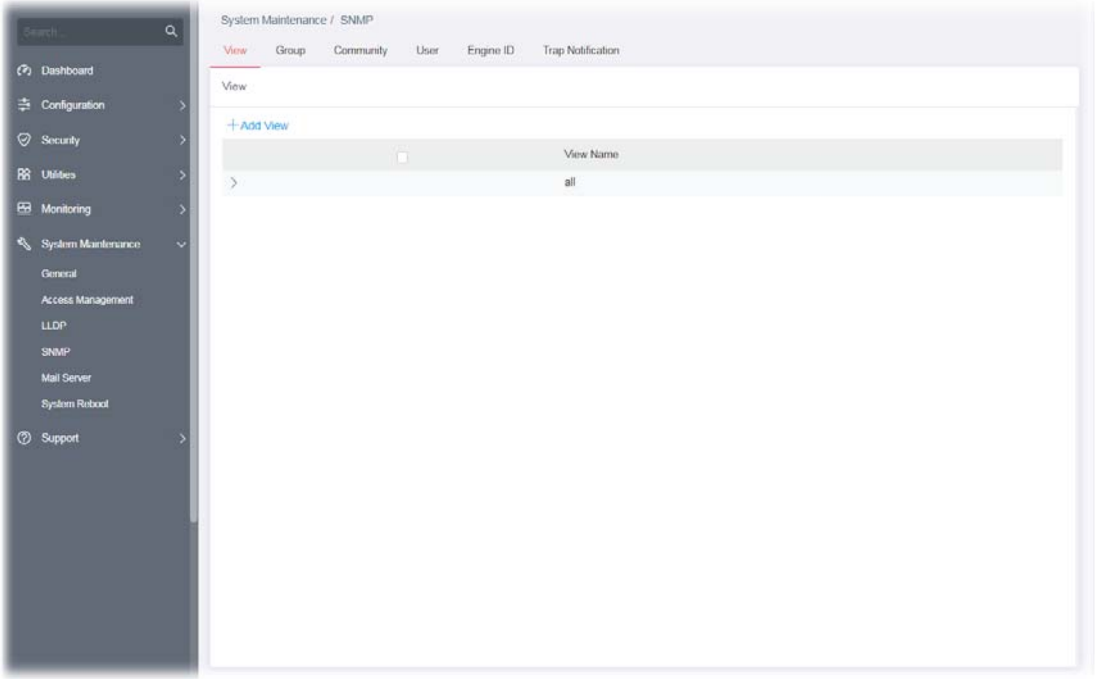
A managed device is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional (read and write) access to node-specific information. Managed devices exchange node-specific information with the NMSs. Sometimes called network elements, the managed devices can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

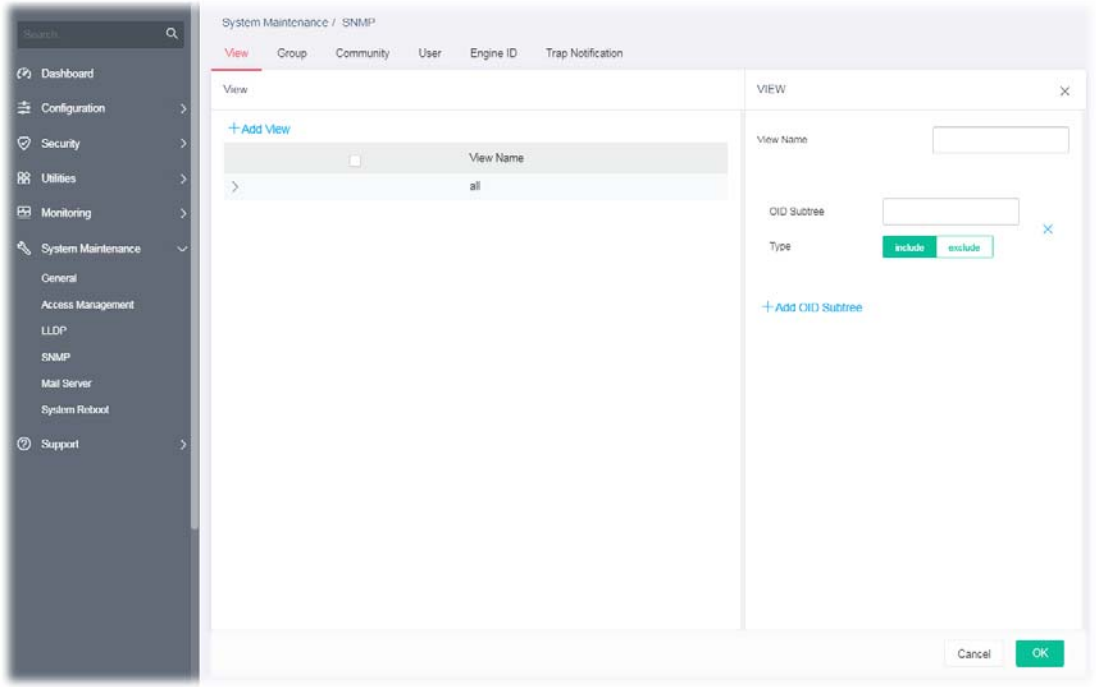
This page allows the network administrator to create MIB views (Management information base) and then include or exclude OID (Object Identifier) in a view.



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:

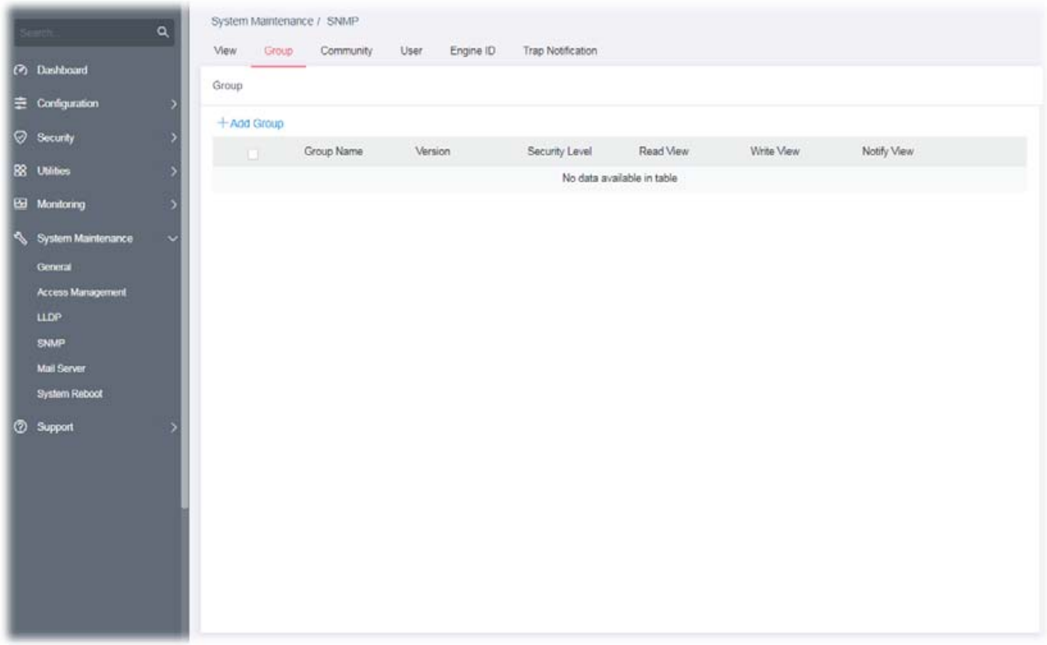
Item	Description
View Name	Enter a name of the MIB view.

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** ● **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

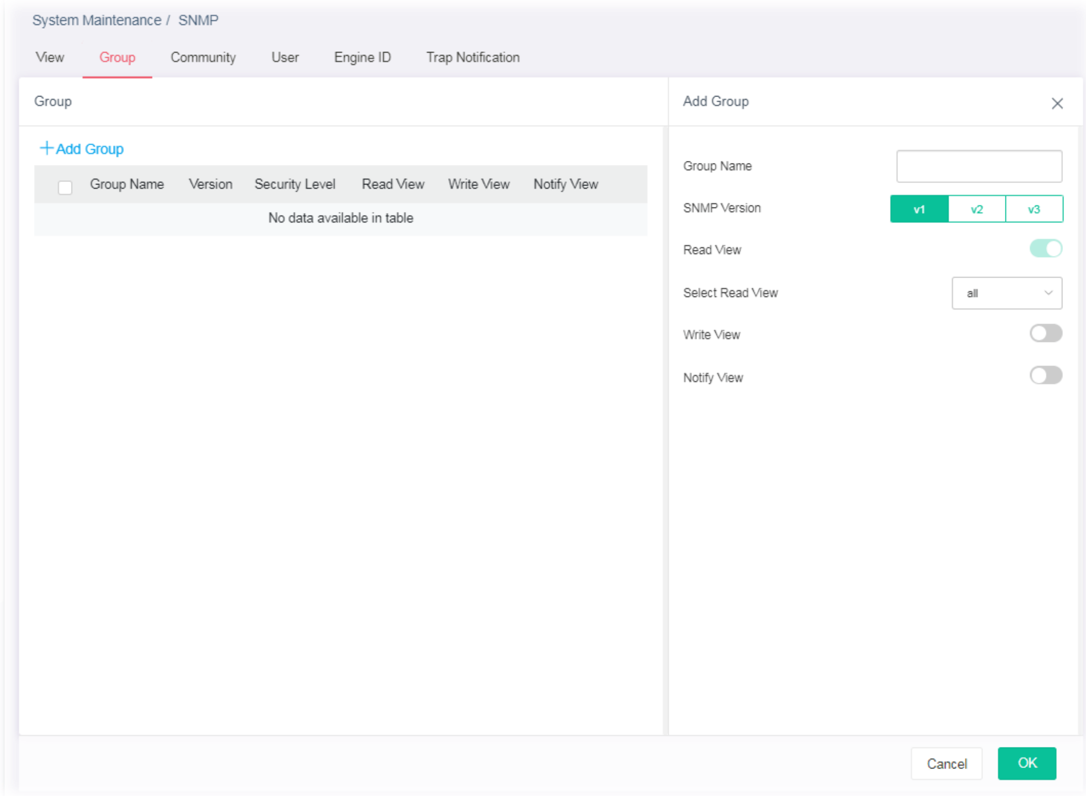
This page allows the network administrator to group SNMP users and assign different authorization and access privileges.



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.



System Maintenance / SNMP

View | Group | Community | User | Engine ID | Trap Notification

Group

+Add Group

□	Group Name	Version	Security Level	Read View	Write View	Notify View
No data available in table						

Add Group

Group Name:

SNMP Version: v1 (selected) v2 v3

Read View: ●

Select Read View: all

Write View: ○

Notify View: ○

Cancel OK

Available settings are explained as follows:

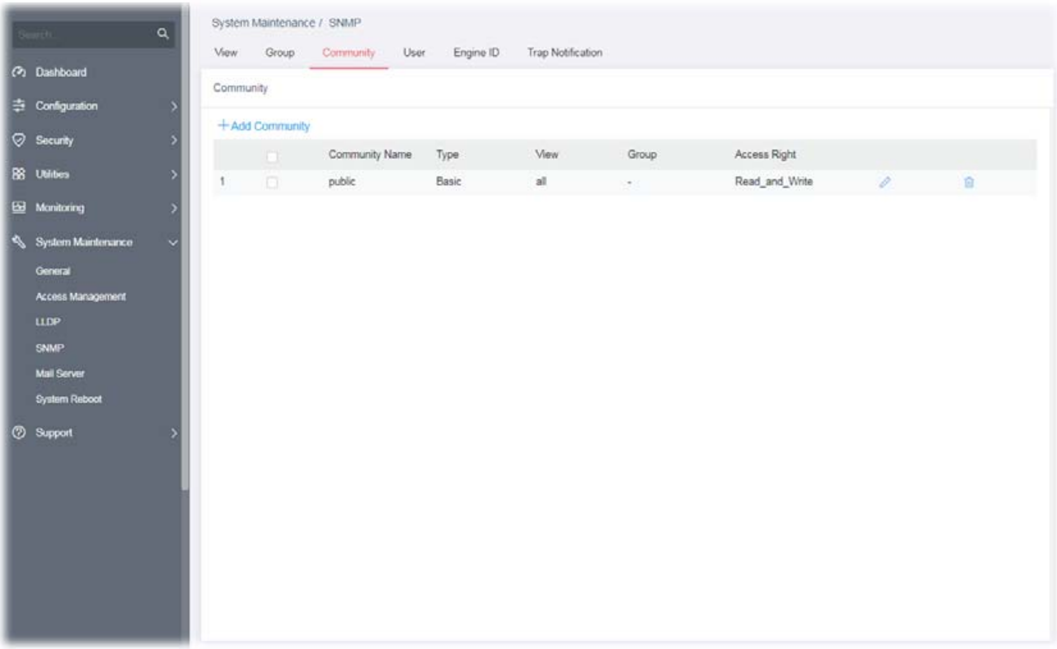
Item	Description
Add Group	
Group Name	Enter a name for the group.
SNMP Version	Specify SNMP version (v1, v2 or v3).
Security Level	Specify SNMP security level for the group. It is available when **SNMPv3** is selected. ● **No Security** – No authentication. ● **Authentication** – Authentication without encryption will be performed for packets. ● **Authentication and Privacy** – Authentication with encryption will be performed for packets.
Read View	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. ● - means “Enable”. ○ - means “Disable”.
Select Read View	Use the drop down list to select one of the views. The default is “all”, which means the group user can read all MIB views.
Write View	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. **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. **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.



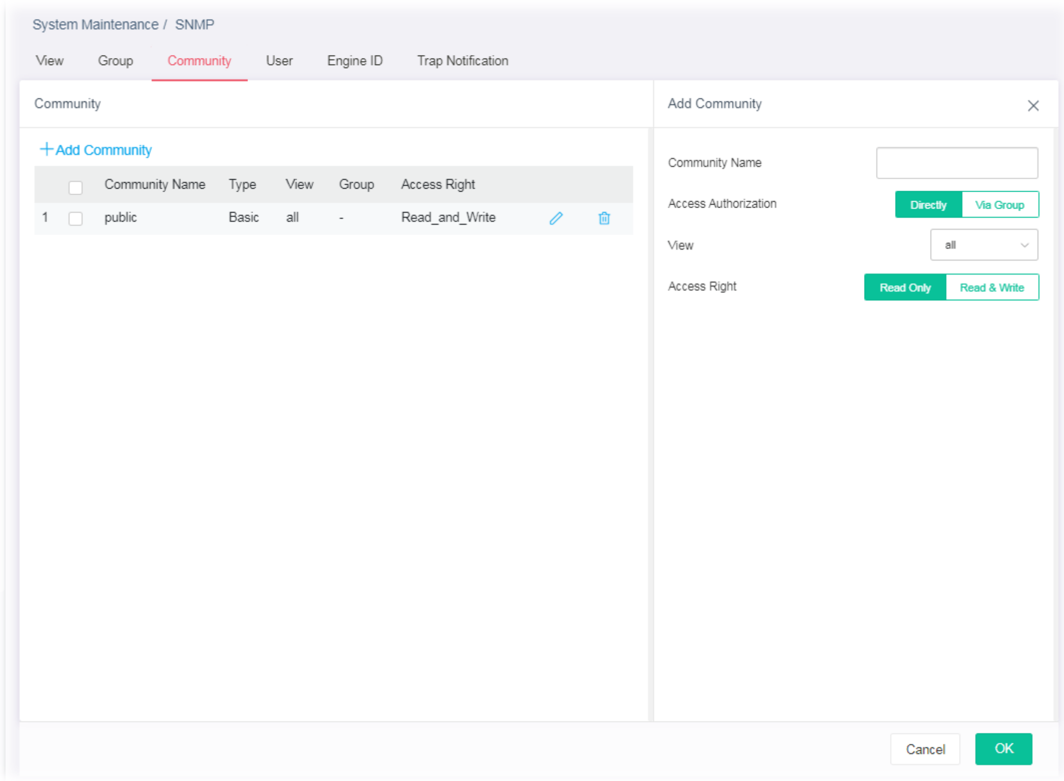
	□	Community Name	Type	View	Group	Access Right		
1	□	public	Basic	all	-	Read_and_Write	✎	🗑

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.
✎	Click to modify the settings of the community.
🗑	Remove the selected entry.

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

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



	Community Name	Type	View	Group	Access Right
1	public	Basic	all	-	Read_and_Write

Community Name:

Access Authorization: Directly

View: all

Access Right: Read Only

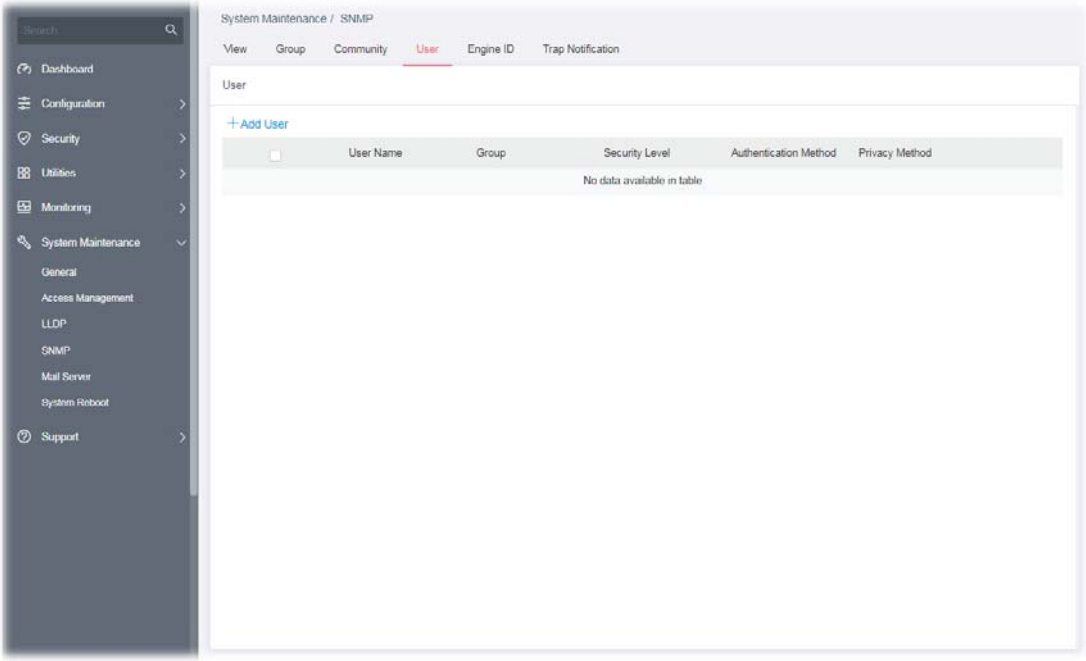
Available settings are explained as follows:

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

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

VI-4-4 User

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



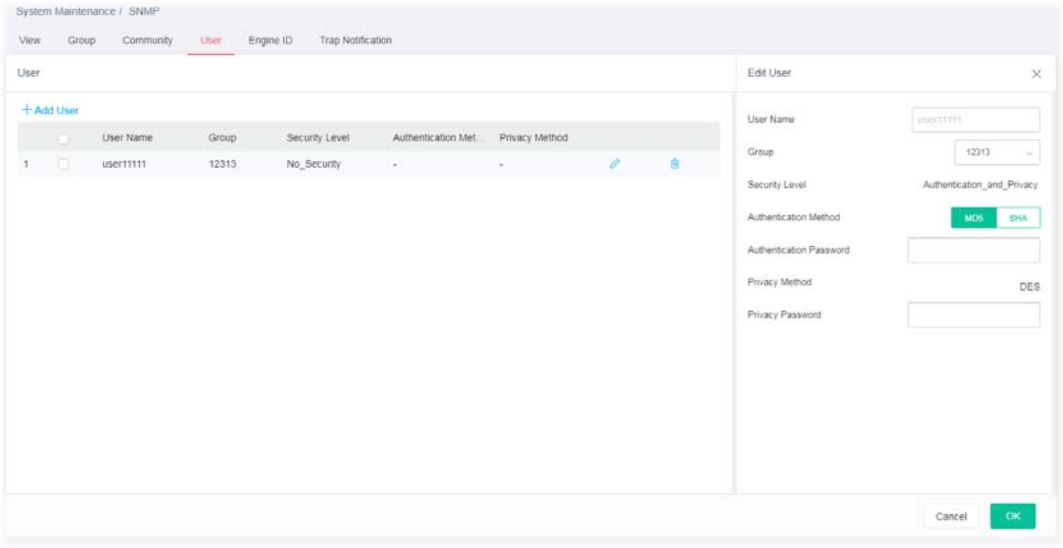
□	User Name	Group	Security Level	Authentication Method	Privacy Method
No data available in table					

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.



	User Name	Group	Security Level	Authentication Met...	Privacy Method
1	user11111	12313	No_Security	-	-

User Name	user11111
Group	12313
Security Level	Authentication_and_Privacy
Authentication Method	MD5 SHA
Authentication Password	
Privacy Method	DES
Privacy Password	

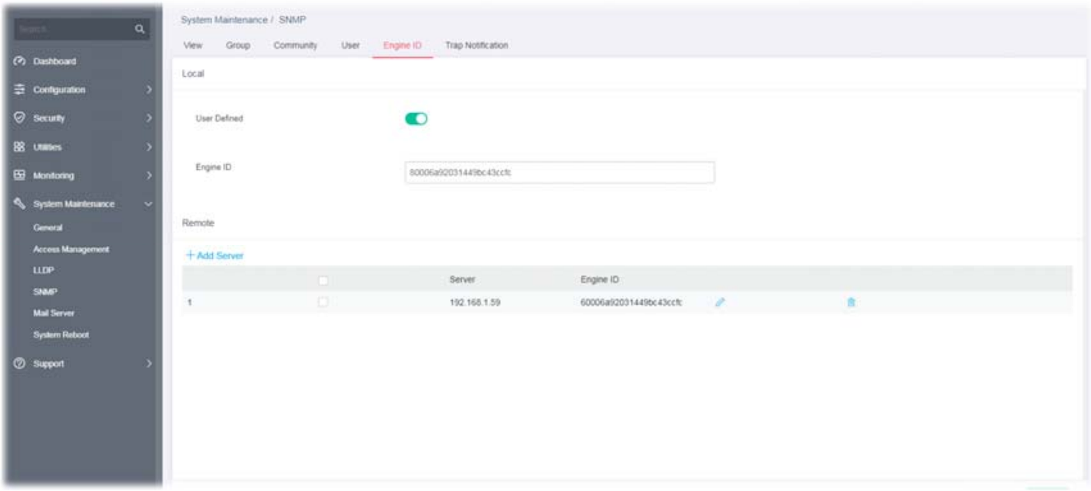
Available settings are explained as follows:

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

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

VI-4-5 Engine ID

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



User Defined ●

Engine ID 80006a92031449bc43ccfc

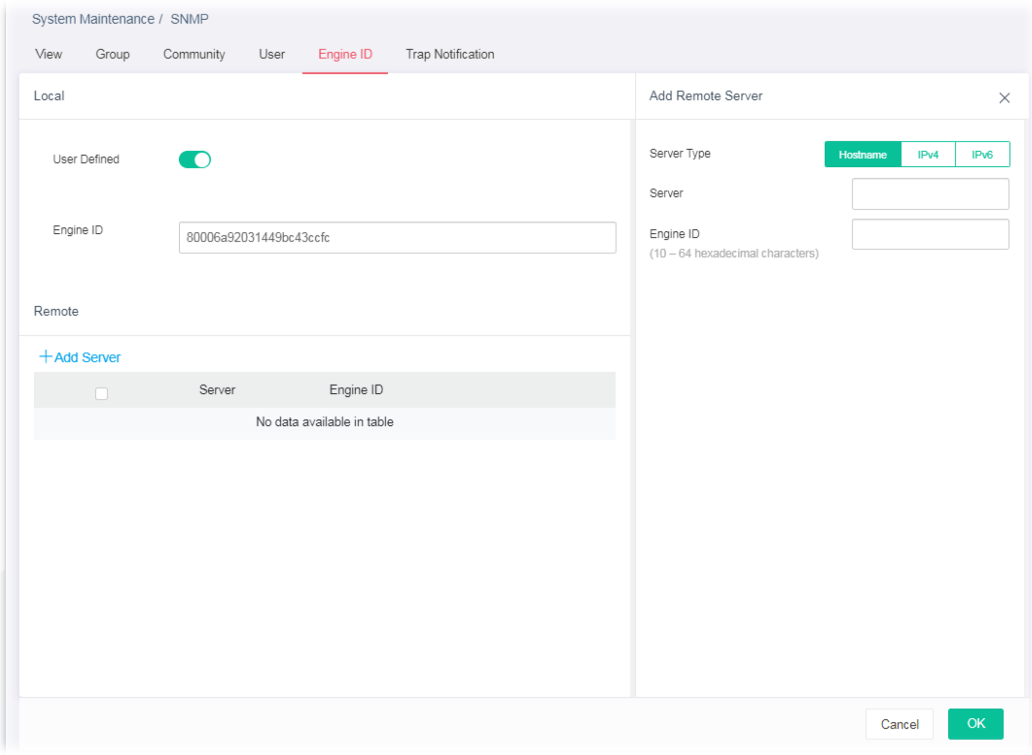
	□	Server	Engine ID		
1	□	192.168.1.59	60006a92031449bc43ccfc	✎	🗑

Available settings are explained as follows:

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

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

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


System Maintenance / SNMP

Engine ID: 80006a92031449bc43ccfc

□	Server	Engine ID
No data available in table		

Server Type: Hostname

Server:

Engine ID (10 – 64 hexadecimal characters):

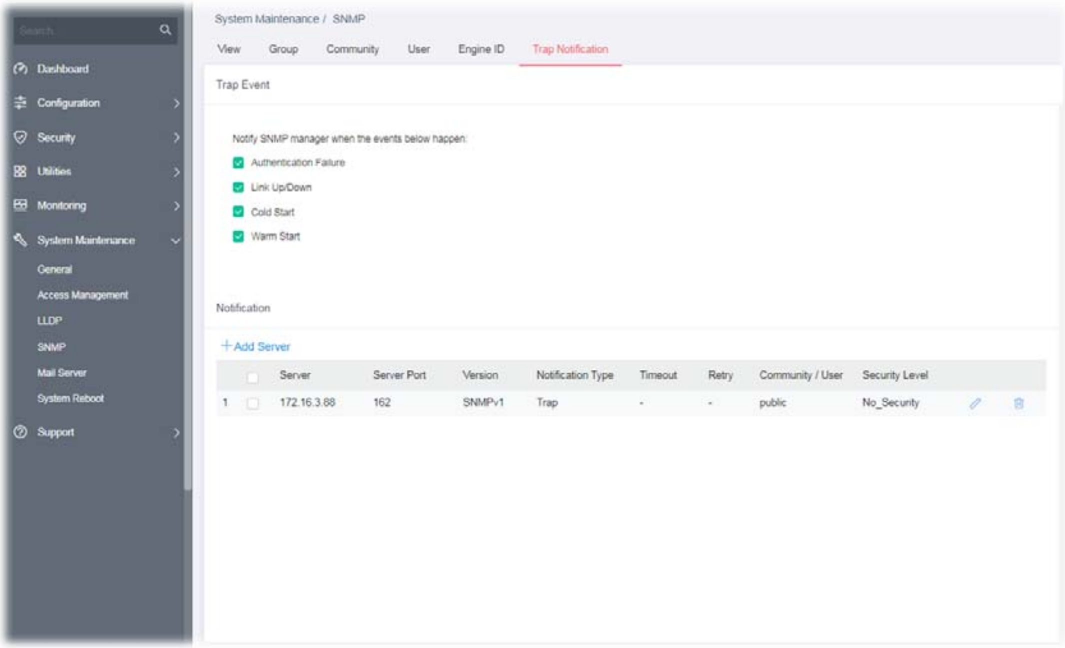
Available settings are explained as follows:

Item	Description
Add Remote Server	
Server Type	Specify the address type for entering hostname or IPv4/IPv6 address. ● **Hostname** ● **IPv4** ● **IPv6**
Server	Enter the IP address or the hostname of the remote SNMP server.
Engine ID	Specify the engine ID for remote SNMP server. 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/ve notification.



Notify SNMP manager when the events below happen:

☑ Authentication Failure
☑ Link Up/Down
☑ Cold Start
☑ Warm Start

	□	Server	Server Port	Version	Notification Type	Timeout	Retry	Community / User	Security Level
1	□	172.16.3.88	162	SNMPv1	Trap	-	-	public	No_Security

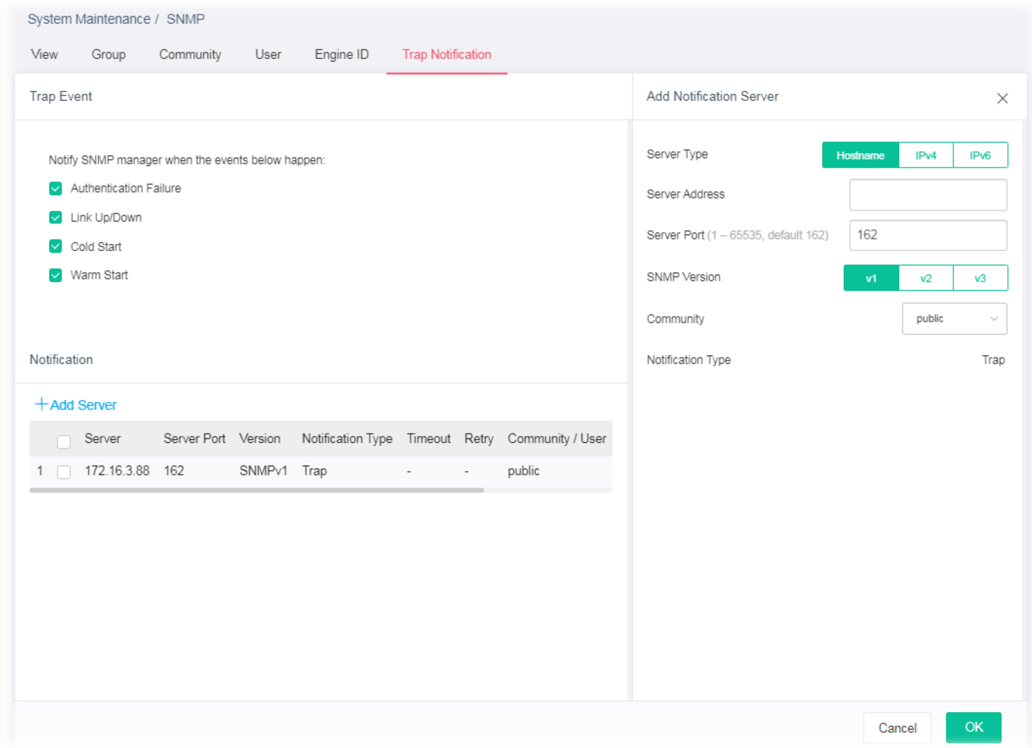
Available settings are explained as follows:

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

✎	Click to modify the setting page of the server profile.
🗑	Remove the selected entry.

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

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



Notify SNMP manager when the events below happen:

- ☑ Authentication Failure
- ☑ Link Up/Down
- ☑ Cold Start
- ☑ Warm Start

	Server	Server Port	Version	Notification Type	Timeout	Retry	Community / User
1 □	172.16.3.88	162	SNMPv1	Trap	-	-	public

Server Type: Hostname / IPv4 / IPv6 (Hostname selected)

Server Address:

Server Port (1 – 65535, default 162): 162

SNMP Version: v1 / v2 / v3 (v1 selected)

Community: public

Notification Type: Trap

Available settings are explained as follows:

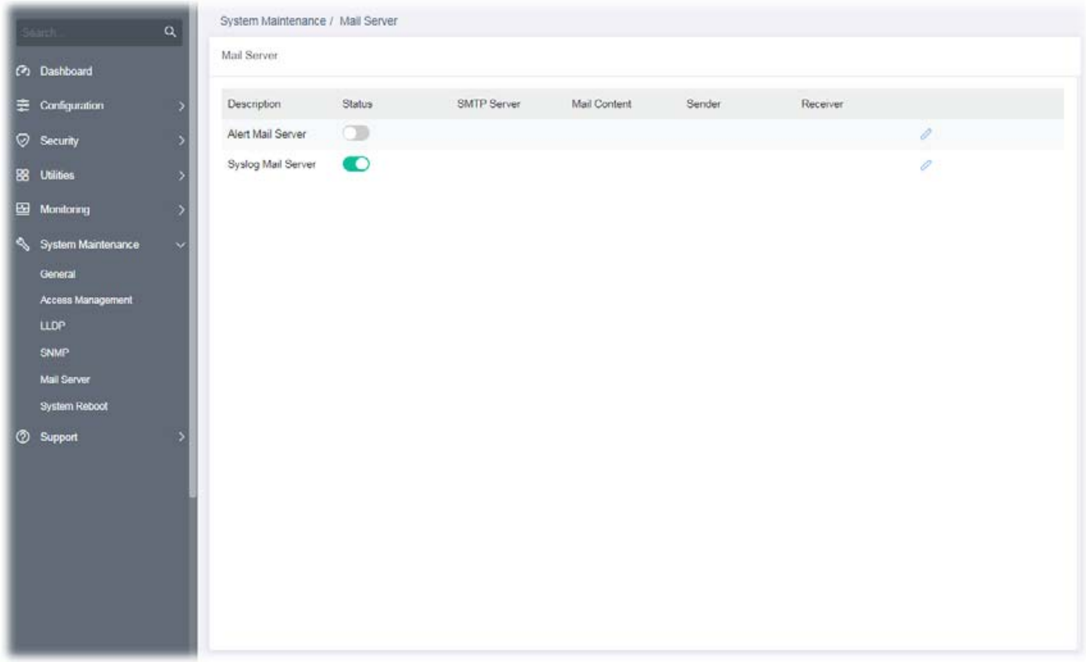
Item	Description
Add Notification Server	
Server Type	Choose IPv4/IPv6/Hostname to specify IP address or the hostname of the SNMP trap recipients. ● **Hostname** ● **IPv4** ● **IPv6**
Server Address	Specify SNMP notification version (SNMPv1/v2/v3).
Server Port	Specify a port number for the server.
SNMP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

	Specify SNMP security level for SNMP notification packet. It is available when SNMPv3 is selected. ● **No Security** – No authentication. ● **Authentication** – Authentication without encryption will be performed for packets. ● **Authentication and Privacy** – Authentication with encryption will be performed for packets.

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

VI-5 Mail Server

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



System Maintenance / Mail Server

Mail Server

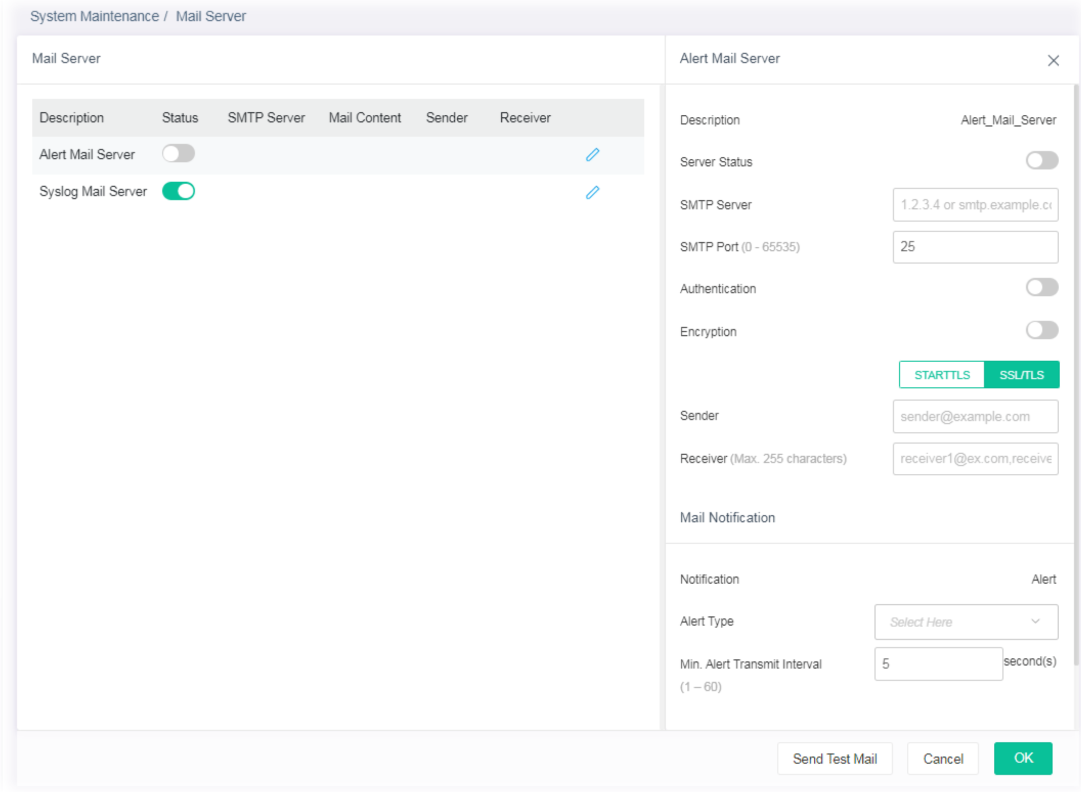
Description	Status	SMTP Server	Mail Content	Sender	Receiver	
Alert Mail Server	○					✎
Syslog Mail Server	●					✎

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. ● - means “Enable”. ○ - means “Disable”.
SMTP Server	Displays the IP address / host of the SMTP server.
Mail Content	Displays the condition(s) for VigorSwitch system to send a mail out.
Sender	Displays the email address sending the alert/syslog mail.
Receiver	Displays the email address receiving the alert/syslog mail.
✎	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.



System Maintenance / Mail Server

Mail Server

Description	Status	SMTP Server	Mail Content	Sender	Receiver	
Alert Mail Server	○					✎
Syslog Mail Server	●					✎

Alert Mail Server

Description: Alert_Mail_Server

Server Status: ○

SMTP Server: 1.2.3.4 or smtp.example.c

SMTP Port (0 - 65535): 25

Authentication: ○

Encryption: ○

STARTTLS | SSL/TLS

Sender: sender@example.com

Receiver (Max. 255 characters): receiver1@ex.com,receive

Mail Notification

Notification: Alert

Alert Type: Select Here

Min. Alert Transmit Interval (1 – 60): 5 second(s)

Available settings are explained as follows:

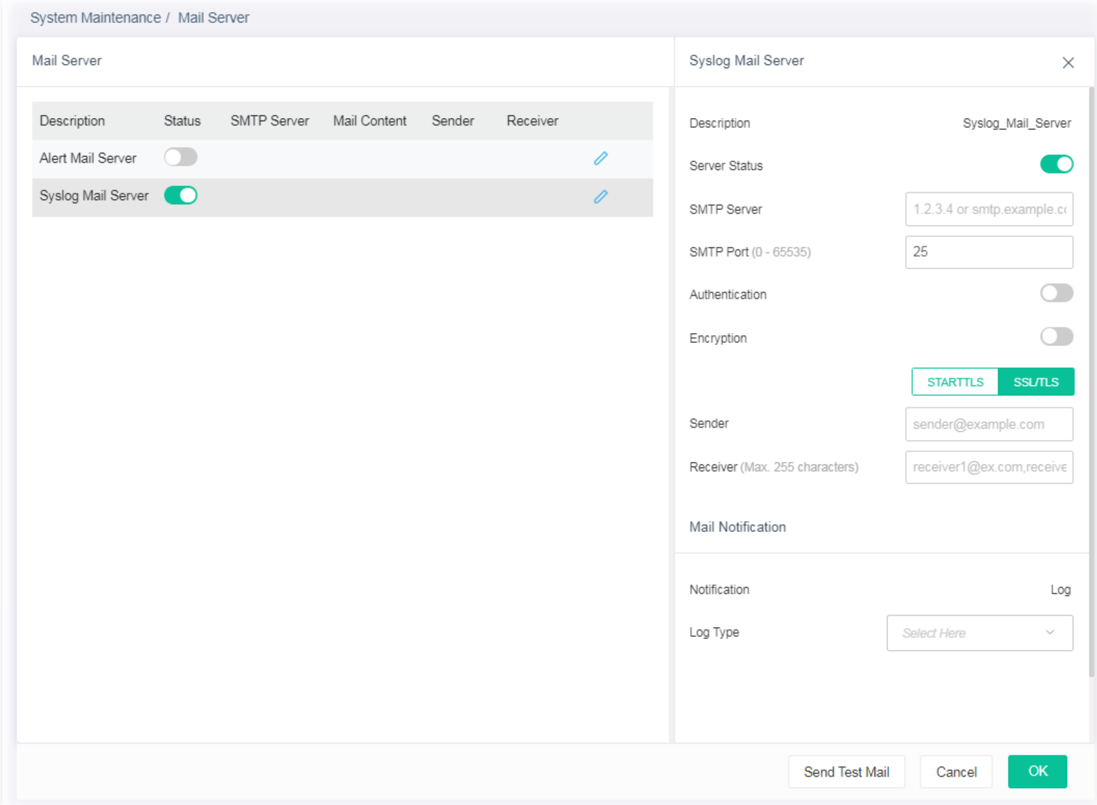
Item	Description
Alert Mail Server	
Description	Displays the name (Alert or Syslog) of the mail server.
Server Status	Click the toggle to enable / disable the mail server. ● - means “Enable”. ○ - means “Disable”.
SMTP Server	Enter IP address or URL of the SMTP server.
SMTP Port	Enter the port number for the SMTP server.
Authentication	Click the toggle to enable / disable this function. ● **User Name** - Enter a user name for authentication. ● **Password** - Enter a password for authentication.
Encryption	Click the toggle to enable / disable this function. After enabling Authentication, choose one of the encryption servers for data encryption. ● **STARTTLS -** The mail will be encrypted with StartTLS. ● **SSL/TLS -** The mail will be encrypted with SSL/TLS.
Sender	Enter the email address which will send the alert mail out.
Receiver	Enter the email address which will receive the alert mail.
Mail Notification	

Alert Type	Specify the condition(s) for VigorSwitch system to send an alert out. ● Port Link Status ● Port Link Speed ● System Restarted ● PoE Warning Status IP Conflict
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.



System Maintenance / Mail Server

Mail Server

Description	Status	SMTP Server	Mail Content	Sender	Receiver	
Alert Mail Server	○					✎
Syslog Mail Server	●					✎

Syslog Mail Server

Description: Syslog_Mail_Server

Server Status: ●

SMTP Server: 1.2.3.4 or smtp.example.c

SMTP Port (0 - 65535): 25

Authentication: ○

Encryption: ○

STARTTLS | SSL/TLS

Sender: sender@example.com

Receiver (Max. 255 characters): receiver1@ex.com,receive

Mail Notification

Notification: Log

Log Type: Select Here

Available settings are explained as follows:

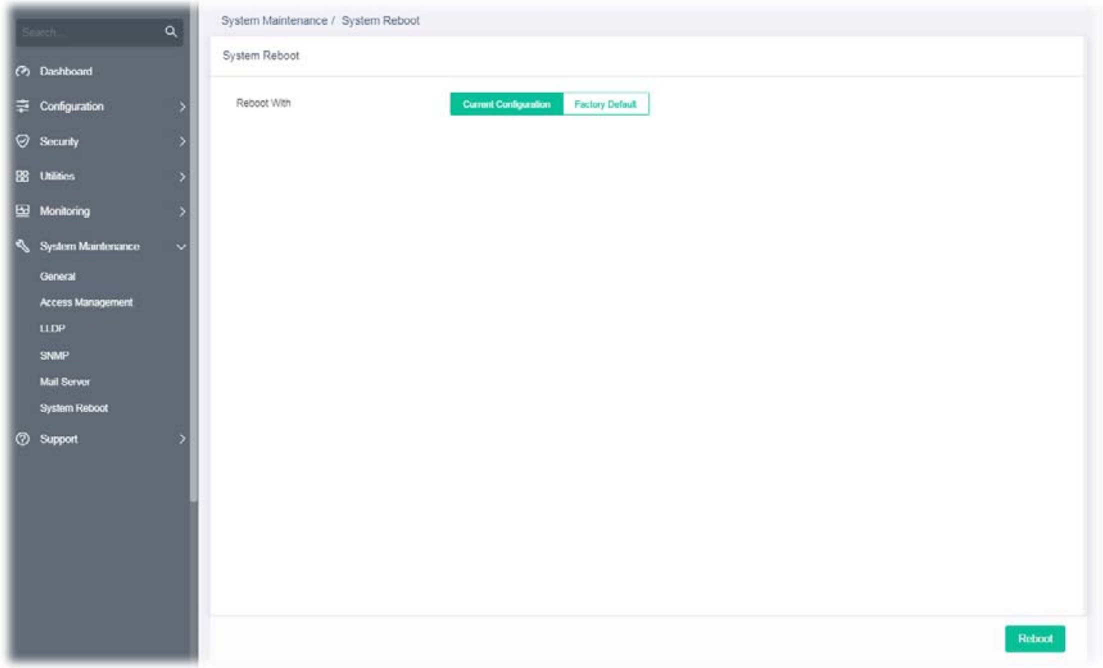
Item	Description
Alert Mail Server	
Description	Displays the name (Alert or Syslog) of the mail server.
Server Status	Click the toggle to enable / disable this function. ● - means “Enable”. ○ - means “Disable”.
SMTP Server	Enter IP address or URL of the SMTP server.

SMTP Port	Enter the port number for the SMTP server.
Authentication	Click the toggle to enable / disable this function. ● **User Name** - Enter a user name for authentication. ● **Password** - Enter a password for authentication.
Encryption	Click the toggle to enable / disable this function. After enabling Authentication, choose one of the encryption servers for data encryption. ● **STARTTLS -** The mail will be encrypted with StartTLS. ● **SSL/TLS -** The mail will be encrypted with SSL/TLS.
Sender	Enter the email address which will send the syslog mail out.
Receiver	Enter the email address which will receive the syslog mail.
Mail Notification	
Log Type	Vigor system will send the e-mail related to the selected feature(e.g., AAA, ACL) to the recipient.
Send Test Mail	After clicking this button, VigorSwitch system will send a test mail to the recipient.

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

VI-6 System Reboot

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



Available settings are explained as follows:

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

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.

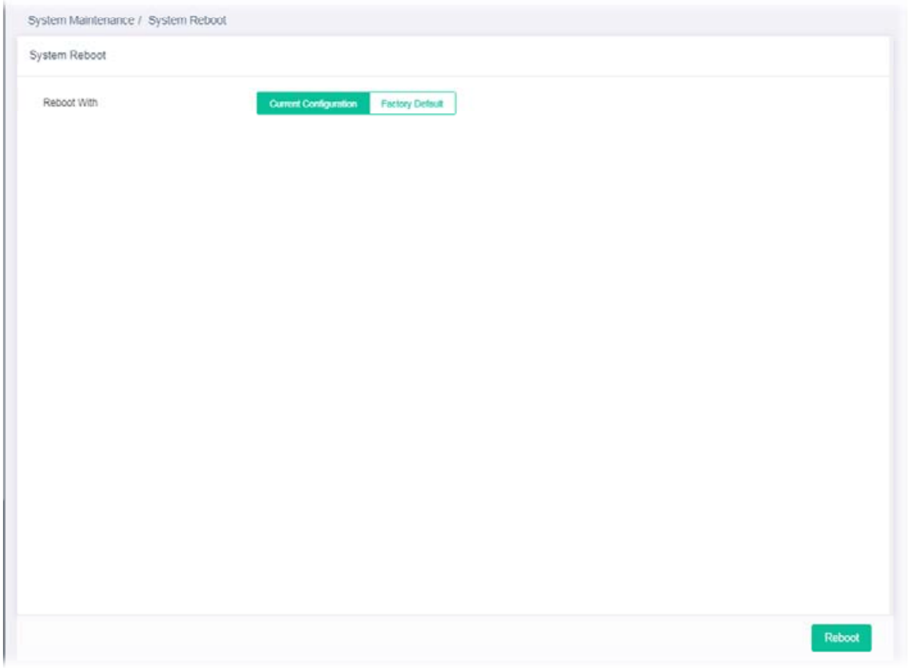
Warning:

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.



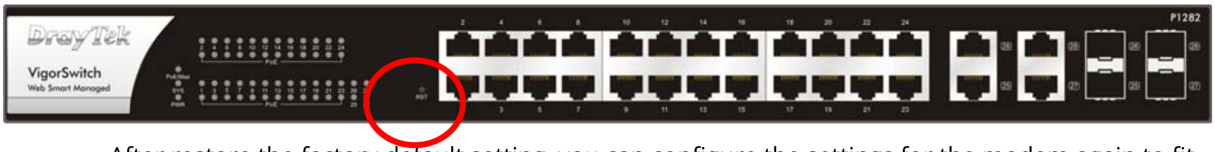
System Maintenance / System Reboot

System Reboot

Reboot With [✓ Current Configuration] Factory Default

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

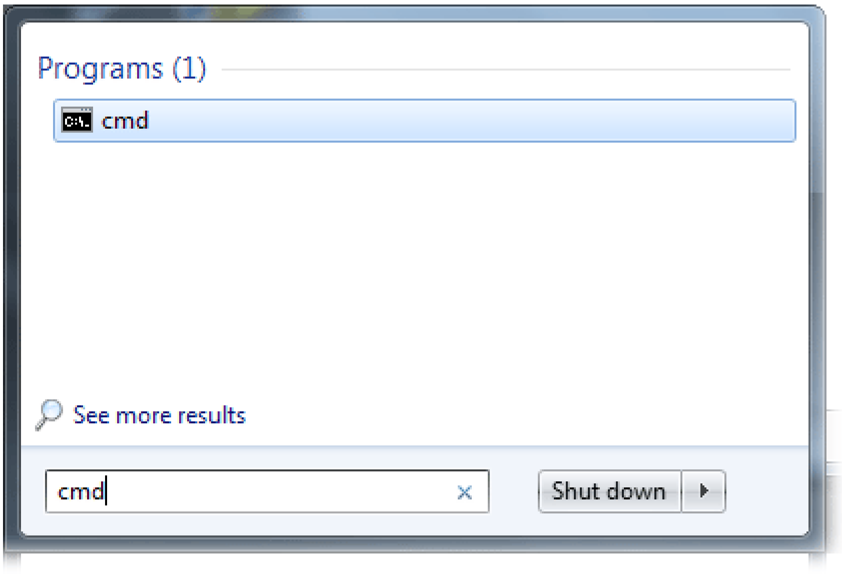
A-1 Accessing Telnet of Vigor Switch

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

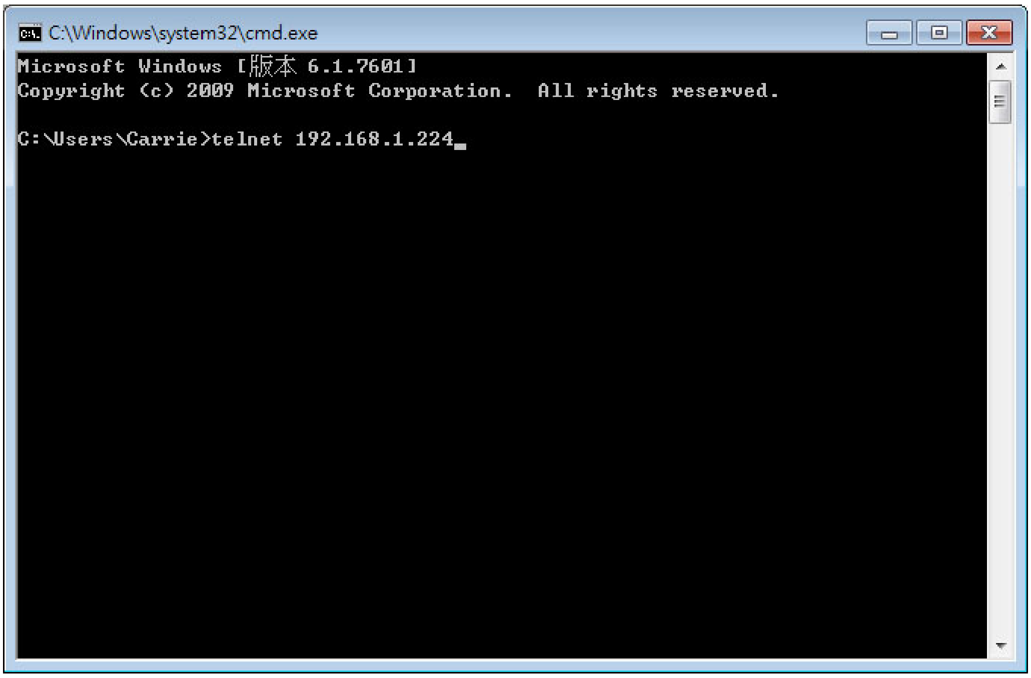
Note:

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.

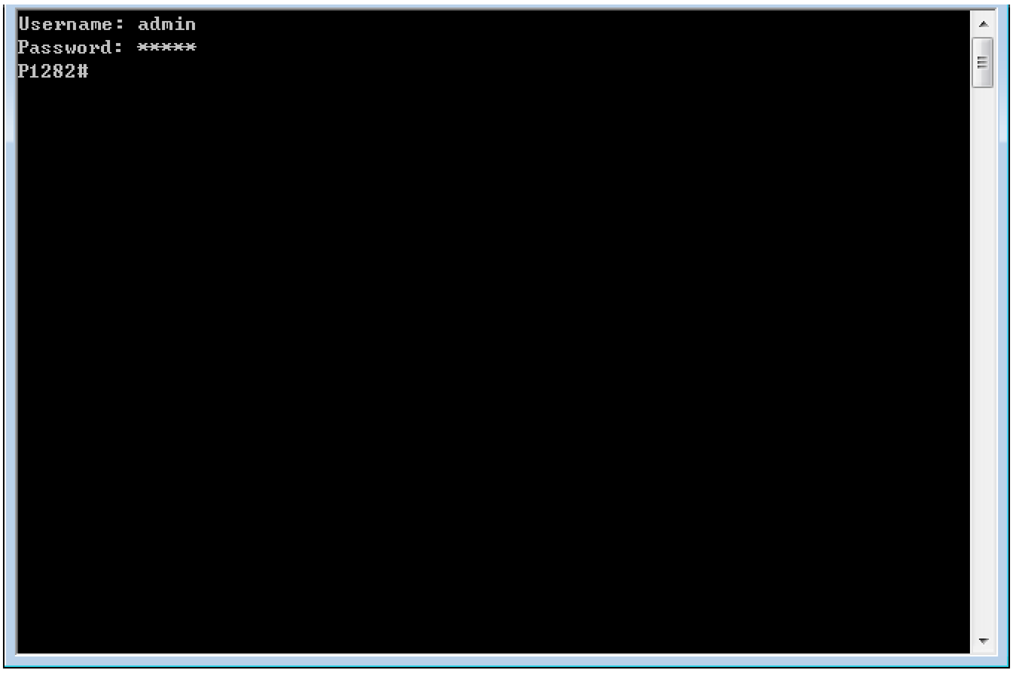


```
Microsoft Windows [版本 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Carrie>telnet 192.168.1.224_
```

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

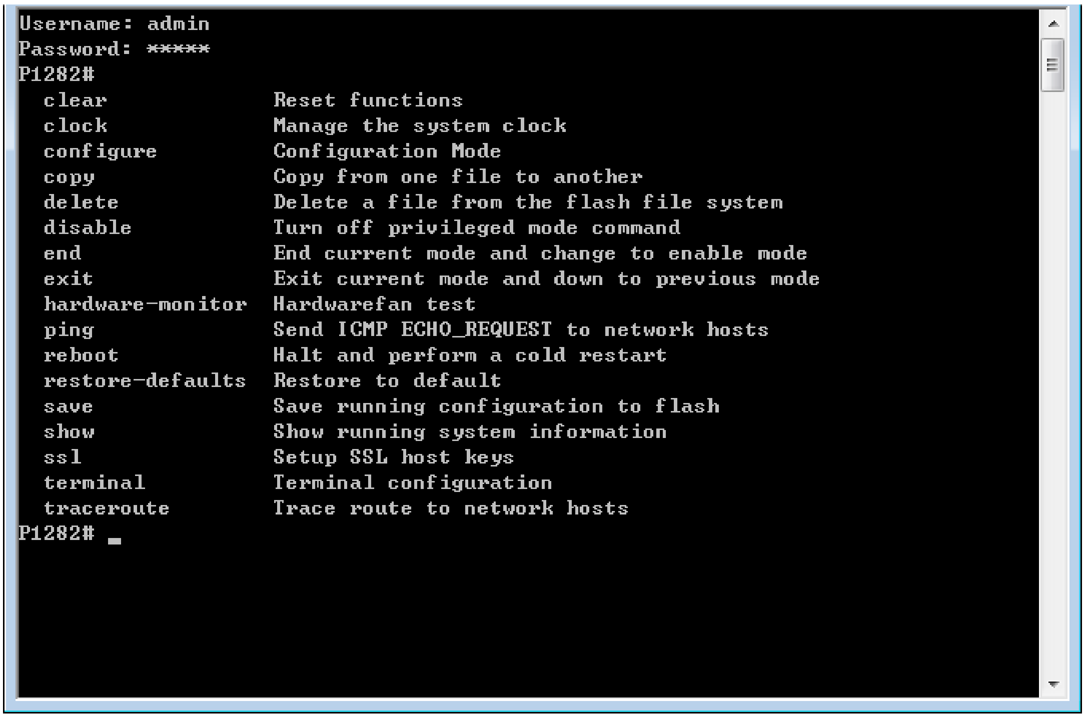
Next, enter admin/admin for Account/Password.



```
Username: admin
Password: *****
P1282#
```

A-2 Available Commands

Enter ? to get a list of available commands.



```
Username: admin
Password: *****
P1282#
  clear             Reset functions
  clock             Manage the system clock
  configure         Configuration Mode
  copy              Copy from one file to another
  delete            Delete a file from the flash file system
  disable           Turn off privileged mode command
  end               End current mode and change to enable mode
  exit              Exit current mode and down to previous mode
  hardware-monitor  Hardwarefan test
  ping              Send ICMP ECHO_REQUEST to network hosts
  reboot            Halt and perform a cold restart
  restore-defaults  Restore to default
  save              Save running configuration to flash
  show              Show running system information
  ssl               Setup SSL host keys
  terminal          Terminal configuration
  traceroute        Trace route to network hosts
P1282# _
```

The available commands contain – clear, clock, configure, copy, delete, disable, end, exit, hardware-monitor, ping, reboot, restore-defaults, save, show, ssl, terminal, and traceroute. 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). Related Syntax: ● # clear arp ● # clear arp <A.B.C.D>

Example

```
P1282# clear arp 192.168.1.224
P1282#
```

Telnet Command: clear interfaces

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

Syntax Items

clear interfaces GigabitEthernet

clear interfaces LAG

Description

Syntax Items	Description
clear interfaces GigabitEthernet	Specify a LAN interface for clearing statistics counters on that port. <1-28> - Enter the number (1 to 28) of LAN port. Related Syntax: ● # clear interfaces gigabitEthernet <1-24> counters
clear interfaces LAG	Specify a LAG interface for clearing statistics counters on that port. <1-8> - Enter the number (1 to 8) of LAG interface (IEEE 802.3 Link Aggregation Interface). Related Syntax: ● # clear interfaces LAG <1-8> counters

Example

```
P1282# clear interfaces gigabitethernet 3 counters
P1282# clear interfaces
P1282# clear interfaces lag 2 counters
P1282#
```

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 igmp

Description

Syntax Items	Description
clear ip igmp	snooping groups dynamic - Clear dynamic snooping groups of IGMP server. snooping groups static - Clear static snooping groups of IGMP server. snooping statistics - Clear snooping statistics for IGMP server.

	Related Syntax: ● # clear ip igmp snooping groups dynamic ● # clear ip igmp snooping groups static ● # clear ip igmp snooping statistics

Example

```
P1282# clear ip igmp snooping groups dynamic
P1282#
```

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. snooping groups static - Clear static snooping groups of MLD. Related Syntax: ● # clear ipv6 mld snooping groups dynamic ● # clear ipv6 mld snooping groups static ● # clear ipv6 mld snooping statistics

Example

```
P1282# clear ipv6
P1282# clear ipv6 mld snooping groups dynamic
P1282# clear ipv6 mld snooping groups dynamic?
   <cr>
P1282# clear ipv6 mld snooping groups static
P1282#
```

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). Related Syntax: ● # clear lacp <1-8> counters

clear lacp counters	Clear LACP configuration for all LAG interfaces. Related Syntax: ● # clear lacp counters

Example

```
P1282# clear lacp 1 counters
No interfaces configured in the channel group
P1282#
```

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. Related Syntax: ● # clear line ssh
clear line telnet	Clear SSH Telnet configuration for line connection. Related Syntax: ● # clear line telnet

Example

```
P1282# clear line ssh
P1282# 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. Related Syntax: ● # clear lldp global statistics
clear lldp interfaces	Specify a LAN / LAG interface for clearing LLDP information. <1-28> - Enter the number (1 to 28) of LAN port. <1-8> - Enter the number (1 to 8) of LAG interface (IEEE 802.3 Link Aggregation Interface).

	Related Syntax: ● # clear lldp interfaces GigabitEthernet <1-28> statistics ● # clear lldp interfaces LAG <1-8> statistics

Example

```
P1282# clear lldp global statistics
P1282#
P1282# clear lldp interfaces LAG 1 statistics
P1282# clear lldp interfaces gigabitethernet 1 statistics
P1282#
```

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. Related Syntax: ● # clear logging buffered
clear logging file	Clear the log stored in flash. Related Syntax: ● # clear logging file

Example

```
P1282# clear logging buffered
P1282# clear logging file
P1282#
```

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	<1-28> - Enter the number (1 to 28) of LAN port. <1-8>- Enter the number (1 to 8) of LAG interface (IEEE 802.3 Link Aggregation Interface). <1-4094> - Specify a VLAN ID by entering its number. Related Syntax: ● # clear mac adderss-table dynamic interfaces

	GigabitEthernet <1-28> ● # clear mac adderss-table dynamic interfaces LAG <1-8> ● # clear mac adderss-table dynamic vlan <1-4094>

Example

```
P1282# clear mac address-table dynamic vlan 2038
P1282# clear mac address-table dynamic interfaces gigabitethernet 3
P1282#
```

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. <1-28>- Enter the number (1 to 28) of LAN port. <1-8>- Enter the number (1 to 8) of LAG interface (IEEE 802.3 Link Aggregation Interface). Related Syntax: ● # clear spanning-tree interfaces GigabitEthernet <1-28> statistics ● # clear spanning-tree interfaces LAG <1-8> statistics

Example

```
P1282# clear spanning-tree interfaces GigabitEthernet
   <1-28>    GigabitEthernet device number
P1282# clear spanning-tree interfaces gigabitethernet 3 statistics
P1282# clear spanning-tree interfaces LAG 1 statistics
P1282#
```

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:

	<HH:MM:SS> - Hour, minute, second (e.g., 08:10:30). <Jan> - January. <feb> - February <mar> - March <apr> - April <may> - May <jun> - June <jul> - July <aug> - August <sep> - September <oct> - October <nov> - November <dec> - December <1-31> - Date 1 to 31. <2000-2035> - Year of 2000 to 2035. Related Syntax: ● # clock set HH:MM:SS jan/feb/mar/apr/may/jun/jul/aug/sep/oct/nov/dec <1-31> <2000-2035>

Example

```
P1282# 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:

clock, custom, dos, do, dray_surveillence, enable, end, errdisable, exit, hostname, http, interface, ip, ipv6, jumbo-frame, lacp, lag, line, lldp, logging, logmail, loop-protection, mac, mailalert, management-vlan, mirror, no, openvpn, poe, qos, schedule, snmp, sntp, spanning-tree, start-up, storm-control, surveillance-vlan, system, tr069, 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

```
P1282# configure
P1282(config)#
P1282(config)# exit
P1282#
```

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. "local" means to use static time. It is the default setting. Related Syntax: ● <config># clock source local
clock source sntp	Configure an external time source for the system clock. "sntp" means to use SNTP time. Related Syntax: ● <config># clock source sntp
clock summer-time	Configure the system to automatically switch to summer time (daylight saving time). 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) <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. <1-31> means date 1 to 31. <2000-2037> - means year of 2000 to 2035. <HH:MM> - means hours and minutes. recurring - Summer time should start and end on the corresponding specified days every year. <1-1440>- Set the number of minutes to add during the summer time. The default number is 60. eu - The summer time is based on the European Union rules. (Start point – last Sunday in March, End point – last Sunday in October) usa - The summer time is based on the United States rules. (Start point – second Sunday in March, End point – first Sunday in November) first - The first week of the month. last - The last week of the month. <sun/mon/tue/wed/thu/fri/sat> - Indicate Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday. <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. <first/last>- Specify the first week or the last week of the month. <1-5> - Specify the number of the week in the month. 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. Related Syntax: ● <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> ● <config># clock summer-time ACRONYM recurring eu <1-1440> ● <config># clock summer-time ACRONYM recurring usa <1-1440> ● <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> ● <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> ● <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. 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) <-12-13> – Specify the hour offset (from -12 to +13) of time zone. minutes <0-59> – Specify the minute difference from UTC. Related Syntax: ● <config># clock timezone ACRONYM <-12-13> minutes <0-59>

Example

```
P1282# configure
P1282(config)# clock source sntp
P1282(config)# exit
P1282# show clock detail
2019-01-05 06:51:23 UTC+8
Time source is sntp
Time zone:
Acronym is
Offset is UTC+8
P1282# configure
P1282(config)# clock summer-time tw date jan 30 2019 23:30 feb 1 2019 20:50
P1282(config)# exit
P1282# 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.
P1282# configure
P1282(config)# clock summer-time ACRONYM recurring eu 1200
P1282(config)# clock summer-time ACRONYM recurring first mon jan 10:10 first sun feb 10:10
1000
P1282(config)# exit
P1282# 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. Related Syntax: ● <config># custom enable

Example

```
P1282# configure
P1282(config)# custom enable
P1282(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. Related Syntax: ● <config># dos daeqsa-deny
dos icmp-frag-pkts-deny	Drop the fragmented ICMP packets. Related Syntax: ● <config># dos icmp-frag-pkts-deny
dos icmp-ping-max-length	Set the maximum packet size for ICMPv4/ICMPv6 ping operation. <0-65535> - Specify a packet number. Related Syntax: ● <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. Related Syntax: ● <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.

	Related Syntax: ● <config># dos icmpv6-ping-max-check
dos ipv6-min-frag-size-check	Check minimum size of IPv6 fragments. Related Syntax: ● <config># dos ipv6-min-frag-size-check
dos ipv6-min-frag-size-length <0-65535>	Set the minimum packet size of IPv6 fragmented packets. <0-65535> - Specify a packet number. Related Syntax: ● <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. Related Syntax: ● <config># dos land-deny
dos nullscan-deny	Drop the packets if attacked by NULL Scan. Related Syntax: ● <config># dos nullscan-deny
dos pod-deny	Drop the packets if attacked by Ping of Death. Related Syntax: ● <config># dos pod-deny
dos smurf-deny	Drop the packets if encountered Smurf attack. Related Syntax: ● <config># dos smurf-deny
dos smurf-netmask	Set the smurf attack size. <0-32> - Enter a number as smurf attacks size. Related Syntax: ● <config># dos smurf-netmask <0-32>
dos syn-sportl1024-deny	Drop SYN packets with sport less than 1024. Related Syntax: ● <config># dos syn-sportl1024-deny
dos synfin-deny	Drop the packets with SYN and FIN bits set. Related Syntax: ● <config># dos synfin-deny
dos synrst-deny	Drop the packets with SYNC and RST bits set. Related Syntax: ● <config># dos synrst-deny
dos tcp-frag-off-min-check	Drop the TCP fragmented packet with offset equals to the minimum packet size. Related Syntax: ● <config># dos tcp-frag-off-min-check
dos tcpblat-deny	Drop the packets if the source TCP port equals to destination TCP port. Related Syntax: ● <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. Related Syntax: ● <config># dos tcphdr-min-check
dos tcphdr-min-length	Set the minimum size of TCP header. <0-65535> - Specify a packet number. Related Syntax: ● <config># dos tcphdr-min-length <0-65535>
dos udpblat-deny	Drop the packets if the source UDP port equals to destination UDP port. Related Syntax: ● <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: ● <config># dos xma-deny

Example

```
P1282# configure
P1282(config)#
P1282(config)# dos icmp-ping-max-length 25252
P1282(config)# dos icmpv4-ping-max-check
P1282(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. Related Syntax: (for example) ● <config># do show info

Example

```
P1282(config)# do show info
System Name          : P1282
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
P1282(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. WORD <36-36> - Enter the UUID string of the IP camera or IP-based device. Related Syntax: ● <config># dray_surveillence add device uuid WORD <36-36> ● <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. Related Syntax: ● <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. password WORD<1-32>> - Enter a string as the default password. encptpwd WORD <1-128> - Enter a string as the encrypted key. WORD <36-36> - Enter the UUID string of the IP camera or the IP-based device. ip <A.B.C.D> - Enter the IP address of the IP camera or the

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

Example

```
P1282# configure
P1282(config)#
P1282(config)# dray_surveillence
P1282(config)#
P1282(config)# dray_surveillence add device uuid 53d7762a-c52b-4bb9-8000-305501e0f35f
P1282(config)#
```

Telnet Command: enable

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

Syntax Items

enable password

enable secret

Description

Syntax Items	Description
enable password	Edit the password for each privilege level for activating authentication. <1-15> - Enter a number for specifying a privilege level. Default value is 15. Related Syntax: ● <config># enable password <1-15>
enable secret	<PASSWORD> - Enter a new string as the encrypted password. Related Syntax: ● <config># enable secret PASSWORD ● <config># enable secret encrypted PASSWORD

Example

```
P1282# configure
P1282(config)# enable secret encrypted testtest
P1282(config)# exit
P1282# show running-config
P1282# ...
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

```
P1282# configure
P1282(config)#end
P1282#
```

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. Related Syntax: ● <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. <30-86400> - The default value is 300 seconds. Related Syntax: ● <config># errdisable recovery interval <30-86400>

Example

```
P1282# configure
P1282(config)#
P1282(config)# errdisable recovery interval 600
P1282(config)#
```

Telnet Command: exit

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

Syntax Items

exit

Example

```
P1282# configure
P1282(config)#
P1282(config)# exit
P1282#
```

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. Related Syntax: <config># hostname WORD

Example

```
P1282# configure
P1282(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:

```
P1282# configure
P1282(config)#
P1282(config)# interface GigabitEthernet 3
```

```
P1282(config-if)#
```

Or

```
P1282# configure
P1282(config)#
P1282(config)# interface range LAG 3
P1282(config-if-range)#
```

Syntax Items

interface GigabitEthernet

interface VLAN

interface LAG

interface range

Description

Syntax Items	Description
interface GigabitEthernet	<1-28> - Specify the number of Ethernet LAN port. Related Syntax: ● <config># interface GigabitEthernet <1-28>
Interface vlan	<1-4094> - Specify the number of VLAN ID. Related Syntax: ● <config># interface vlan <1-4094>
interface LAG	<1-8> - Specify the number of LAG interface. Related Syntax: ● <config># interface LAG <1-8>
Interface range	Specify an interface ranges for configuring detailed settings. Related Syntax: ● <config># interface range GigabitEthernet <1-28> ● <config># interface range LAG <1-8>

Example

```
P1282# configure
P1282(config)# interface LAG 1
P1282(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># back-pressure

<config-if># custom

<config-if># description

<config-if># device-check

<config-if># dos

<config-if># do

<config-if># dray_surveillence

```
<config-if># duplex
<config-if># eee
<config-if># end
<config-if># exit
<config-if># flowcontrol
<config-if># ip
<config-if># ipv6
<config-if># lacp
<config-if># lag
<config-if># lldp
<config-if># loop-protection
<config-if># mac
<config-if># no
<config-if># poe
<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># vlan
<config-if># voice-vlan
```

Description

Syntax Items	**Description**
back-pressure	Enable back-pressure for the specified interface (Ethernet port/LAG port). Related Syntax: ● <config-if># back-pressure
custom	<enable> - Enable the custom module configuration for the specified interface (Ethernet port/LAG port). Related Syntax: ● <config-if># custom enable
description	Write a description for the specified interface (Ethernet port/LAG port). <WORD> - Enter a description (up to 32 characters). Related Syntax: ● <config-if># description <WORD>
device-check	Perform a device check the specified interface (Ethernet port/LAG port). ip-address<A.B.C.D> - Enter the IP address of the device. interval <120/15/30/60>– Check the device interval by entering

	the time value. Unit is second. retry <1/3/5> - Enter the retry time during a checking period. failure-action <nothing/powercycle/poweroff> – Set the power cycle. alert <disable/enable> - Enable or disable the alert function. <STRING> - Enter multiple IP addresses separated by ",". Related Syntax: ● <config-if># device-check ip-address <A.D.C.D> interval <120/15/30/60> retry <1/3/5> failure-action <nothing/powercycle/poweroff> ● <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> ● <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).
do	Run execution commands in current mode.
dray_surveillence	Use this command to set the ONVIF throughput alert threshold. <16-1000000> - Specify a number as the alert threshold for egress /ingress throughput. Related Syntax: ● <config-if>#dray_surveillence set threshold alert egress <16-1000000> ● <config-if>#dray_surveillence set threshold alert ingress <16-1000000>
duplex	Apply the duplex configuration to the specified interface (Ethernet port/LAG port). <Auto> – Auto duplex configuration. <Full>– Force full duplex operation. <Half> – Force half-duplex operation. Related Syntax: ● <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). <Auto> – Enable AUTO flow-control configuration. <Off> – Disable the force flow-control. <On> – Enable the force flow-control. Related Syntax: ● <config-if># flowcontrol <auto/off/on>

ip	Apply IP configuration to the specified interface (Ethernet port/LAG port). acl <NAME> - Specify an ACL for packets. Enter the name of the ACL. bind-ip <A.B.C.D> - Enter an IP address for binding with the port type. conflict prevention bind-ip <A.B.C.D> - Enter the IP address for the binding. conflict prevention port-type DHCP-Client – Set DHCP Client as the port type. conflict prevention port-type DHCP-Server –Set DHCP Server as the port type. conflict prevention port-type Multiple-Hosts – Set Multiple-Hosts as the port type. conflict prevention port-type Multiple-Hosts has-server – Use this string if there is a DHCP server in this port. conflict prevention port-type Static-Binding –Set Static-Binding as the port type. igmp filter <1-128> - Use it to bind a profile for a port. Specify a profile ID. igmp max-groups <0-256> - Use it to limit port learning max group number (0-256). igmp max-groups action <deny/replace> - Use it to set the action (deny or replace) when the number of groups reach the limitation. source binding max-entry <1-50> - Set the maximum dynamic binding entry number. source binding max-entry no-limit - No limit to binding entry. source verify mac-and-ip – Use it to enable IP source guard function. Related Syntax: ● <config-if># ip acl <NAME> ● <config-if># ip conflict prevention bind-ip <A.B.C.D> ● <config-if># ip conflict prevention port-type DHCP-Client ● <config-if># ip conflict prevention port-type DHCP-Client has-server ● <config-if># ip conflict prevention port-type DHCP-Server ● <config-if># ip conflict prevention port-type DHCP-Server has-server ● <config-if># ip conflict prevention port-type Multiple-Hosts ● <config-if># ip conflict prevention port-type Multiple-Hosts has-server ● <config-if># ip conflict prevention port-type Static-Binding ● <config-if># ip conflict prevention port-type Static-Binding has-server ● <config-if># ip igmp filter <1-128> ● <config-if># ip igmp max-groups <0-256> ● <config-if># ip igmp max-groups action <deny/replace> ● <config-if># ip source binding max-entry <1-50>

	● <config-if># ip source binding max-entry no-limit ● <config-if># ip source verify mac-and-ip
ipv6	Apply IPv6 configuration to the specified interface (Ethernet port/LAG port). acl <NAME> - Specify the ACL name for packets mld <filter> – Set IPv6 filter for MLD configuration. mld max-groups – Specify the number for maximum group. <0-256> - MLD snooping group number. action <deny /replace> – Define the action to be performed when excessing the maximum group. Related Syntax: ● <config-if># ipv6 acl <NAME> ● <config-if># ipv6 mld filter ● <config-if># ipv6 mld max-groups <0-256> ● <config-if># ipv6 mld max-groups action <deny / replace>
lacp	Apply LACP Configuration to the specified interface (Ethernet port/LAG port). <1-65535> - Set a number for IEEE 802.3 link aggregation port priority. <long/short> – Set long or short timeout value. Related Syntax: ● <config-if># lacp port-priority <1-65535> ● <config-if># lacp timeout <long/short>
lag	Apply Link Aggregation Group Configuration the specified interface (Ethernet port/LAG port). <1-8> - Specify LAG number. Related Syntax: ● <config-if># lag <1-8>
loop-protection	Record the log, shutdown the port or follow the global loop-protection settings for each port. Related Syntax: ● <config-if># loop-protection action all ● <config-if># loop-protection action global ● <config-if># loop-protection action log ● <config-if># loop-protection action shutdown
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. med network-policy add / remove - Configure the LLDP MED network policy table. Add /remove a network policy entry that can be bind to ports. med tlv-select - Configure LLDP MED TLVs selection. Available optional TLVs are network-policy, location, inventory and poe-pse. tlv-select - Select LLDP TLVs to send.

	<civic-address> - The location is specified as civic address. <ADDR> - Range from 6 to 160 hexadecimal bytes. <Coordinate> - The location is specified as coordinates. <ADDR> - 16 hexadecimal bytes exactly. <ecs-elin> - The location is specified as ECS ELIN. <ADDR> - 10 to 25 hexadecimal bytes. <IDX_LIST> - Range from 1 to 32. <TLV> - LLDP optional TLV, pick from: port-desc, sys-name, sys-desc, sys-cap, mac-phy, lag, max-frame-size, management-addr. pvid <disable/enable> - Enable or disable the TX optional-TLV 802.1 PVID. vlan-name <add/remove> <2-4094> - Add/remove a selected VLAN. Enter the VLAN ID number. <rx> - Enable LLDP reception on interface. <tx> - Enable LLDP transmission on interface. Related Syntax: ● <config-if># lldp med location <civic-address/coordinate/ecs-elin> <ADDR> ● <config-if># lldp med network-policy add <IDX_LIST> ● <config-if># lldp med network-policy remove <IDX_LIST> ● <config-if># lldp med tlv-select <network-policy/location/inventory/poe-pse> <network-policy/location/inventory/poe-pse> <network-policy/location/inventory/poe-pse> ● <config-if># lldp tlv-select <TLV/pvid/vlan-name> ● <config-if># lldp tlv-select pvid <disable/enable> ● <config-if># lldp tlv-select vlan-name <add/remove> <2-4094> ● <config-if># lldp <rx/tx>
mac	Specify an access control list for packets. Before configuring, you have to create an ACL based on MAC address. For example, <config># mac acl CA_ACL <config-mac-acl># <NAME> - Enter a name for ACL. Related Syntax: ● <config-if># mac acl <NAME>
no	Negate command. Such command can disable current setting of command executed and return to the factory setting of that command. Example: <config-if> # no mvr The operation will make mvr setting is default. Continue? [yes/no]:yes <config-if> # Related Syntax:

	● <config-if># no <command>
poe	Enable or disable the PoE port.
power	Configure the inline power for the PoE device. inline auto - Turn on the PoE device discovery protocol and apply the power to the devcie. inline never - Turn off the PoE device power. power-limit <15.4w/30w/MW> - Set the power limit for the PoE device. priority <1-3/critical/high/low> - Set the priority of power application for the PoE device. schedule-index - Specify the index number (1 to 15) of the schedule profile. Related Syntax: ● <config-if># power inline auto ● <config-if># power inline never ● <config-if># power power-limit <15.4w/30w/MW> ● <config-if># power priority <1-3/critical/high/low> ● <config-if># power schedule-index <1-15>
protected	Configure an interface to be a protected port. Related Syntax: ● <config-if>#protected
qos	cos - Configure the default CoS value for an Ethernet port. <0-7> - Specify a CoS value for the selected interface. Default value is 0. remark - Configure remarking state of each port. 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. <cos> - Enable cos remarking. <dscp> - Enable DSCP remarking. <cos-dscp> - Enable cos and DSCP remarking. <precedence> - Enable IP precedence remarking. Related Syntax: ● <config-if>#qos cos <0-7> ● <config-if>#qos remark <cos/dscp/precedence> ● <config-if>#qos trust <cos/cos-dscp/ dscp/precedence>
rate-limit	It is effective for Ethernet port only. egress - Configure the egress port shaper. ingress - Configure the ingress port shaper. egress queue – Configure queue for egress port shaper. <0-1000000> - Enter a number as the average traffic rate in Kbps. It must be a multiple of 16. <16-1000000> - Enter a number as the average traffic rate in Kbps. It must be a multiple of 16. <1-8> - Specify a number as queue ID. Related Syntax:

	● <config-if># rate-limit egress <0-1000000> ● <config-if># rate-limit egress queue <1-8> <16-1000000> ● <config-if># rate-limit ingress <16-1000000>
shutdown	Disable the selected interface. Example: (config)# interface gigabitethernet 3 (config-if)# shutdown (config-if)# exit (config)# exit # show interface Gigabitethernet 3 GigabitEthernet3 is down Related Syntax: ● <config-if># shutdown
spanning-tree	Configure spanning-tree settings. bpdu-filter - Set the BPDU-Filter for specified port. bpdu-guard - Set the BPDU-Guard for specified port. edge - Set the edge-port for specified port. cost - Change an interface’s spanning tree path cost. link-type - Specify a link type for spanning tree protocol use. mcheck - Set the mcheck for specified port to migrate. mst - Set spanning-tree parameters of instance. port-priority- Set the priority for specified instance. <0-200000000> - Specify a value of internal path cost (0 means Auto). <point-to-point> - The selected port will be treated as point-to-point. <shared> - The selected port will be treated as shared. <0-15> - Specify an instance ID. <0-240> - Specify a priority number for the selected port. Related Syntax: ● <config-if># spanning-tree <bpdu-filter /bpdu-guard/ edge> ● <config-if># spanning-tree cost <0-200000000> ● <config-if># spanning-tree link-type <point-to-point/shared> ● <config-if>#spanning-tree mcheck ● <config-if>#spanning-tree mst <0-15> cost <0-200000000> ● <config-if># spanning-tree port-priority <0-240>
speed	Configure speed operation. <10/100/1000> - Force 10/100/1000 Mbps operation. <auto> - Enable Auto speed configuration. Related Syntax: ● <config-if># speed<10/100/1000> ● <config-if># speed auto
storm-control	action - Select an action for storm control after exceeding the threshold.

	broadcast level - Enable the storm control type of broadcast for the selected port. unknown-multicast level - Enable the storm control type of unknown-multicast for the selected port. unknown-unicast level- Enable the storm control type of unknown-unicast for the selected port. <drop> - Drop packets after exceeding storm control threshold. <shutdown> - Disable the port after exceeding storm control threshold. <1-1000000> - Specify the rate value. Related Syntax: ● <config-if># storm-control action <drop/shutdown> ● <config-if># storm-control broadcast level <1-1000000> ● <config-if># storm-control unknown-multicast level <1-1000000> ● <config-if># storm-control unknown-unicast level <1-1000000>
surveillance-vlan	cos - Set surveillance VLAN configuration. mode - Set surveillance member port join mode. <all> - QoS attributes are applied to all packets that are classified to the Surveillance VLAN. <src> - QoS attributes are applied only on packets from IP phones. <auto> - Make surveillance member port join voice VLAN automatically. <manual> - The administrator manually makes surveillance member port join voice VLAN. Related Syntax: ● <config-if># surveillance-vlan cos <all/src> ● <config-if># surveillance-vlan mode <auto/manual>
switchport	Set switching mode characteristics. access vlan –Use it to set a native VLAN on the interface. default-vlan tagged – Use it to make the selected port interface to become the default VLAN tagged member. forbidden default-vlan – Use it to forbid the defult-vlan on the interface. forbidden vlan - Use it to forbid a vlan on the interface. hybrid acceptable-frame-type – Use it to choose which type of frame will be accepted. hybrid allowed – Use it to allow a VALN set on the interface. hybrid ingress-filtering – Use it to enable VLAN ingress filter. hybrid pvid – Use it to set PVID of the interface. mode access - Use it to configure the selected port as the role of access. Only untagged frames will be accepted. mode hybrid - Use it to configure the selected port as the role of hybrid. Support all functions defined in IEEE 802.1Q specification.

	mode trunk uplink – Use it to configure the selected port as the role of trunk. It can recognize double tagging on the interface. trunk allowed – Use it to allow a VALN on the interface. trunk native – Use it to set a native VLAN on the interface. tunnel vlan – Use it to set a Dot1q tunnel VLAN on the interface. vlan tpid – Use it to set TPID on the interface. <1-4094> - Specify a VLAN ID. <add/remove> - Add or remove the allowed VLAN list. <all/tagged-only/untagged-only> - Specify an option for accepting all frames, only tagged frames or only untagged frames. <1-4094/all> - Specify a VLAN ID or all VLAN IDs. < 0x8100 / 0x88A8 / 0x9100 / 0x9200> - Specify one tag-protocol-id. Related Syntax: ● <config-if># switchport access vlan <1-4094> ● <config-if># switchport default-vlan tagged ● <config-if># switchport forbidden default-vlan ● <config-if># switchport forbidden vlan <add/remove> <1-4094> ● <config-if># switchport hybrid acceptable-frame-type <all/tagged-only/untagged-only> ● <config-if># switchport hybrid allowed vlan add <1-4094> ● <config-if># switchport hybrid allowed vlan add <1-4094> <tagged/ untagged> ● <config-if># switchport hybrid allowed vlan remove <1-4094> ● <config-if># switchport hybrid ingress-filtering ● <config-if># switchport hybrid pvid <1-4094> ● <config-if># switchport mode <access/hybrid> ● <config-if># switchport mode trunk uplink ● <config-if># switchport trunk allowed vlan <add /remove> <1-4094/all> ● <config-if># switchport trunk native <1-4094> ● <config-if># switchport tunnel vlan <1-4094> ● <config-if># switchport vlan tpid < 0x8100/0x88A8 / 0x9100 / 0x9200>
vlan	mac-vlan group - Set a MAC-based VLAN configuration. protocol-vlan group - Set a protocol-based VLAN configuration. <1-2147483647> - Specify a group ID to map. <1-4094> - Specify a VLAN ID. Related Syntax: ● <config-if># vlan mac-vlan group <1-2147483647> vlan <1-4094> ● <config-if># vlan protocol-vlan group<1-2147483647> vlan <1-4094>

voice-vlan	cos - Set voice VLAN configuration as COS mode. mode - Set voice member port join mode. <all> - QoS attributes are applied on all packets that are classified to the Voice VLAN. <src> - QoS attributes are applied only on packets from IP phones. <auto> - Make voice member port join voice VLAN automatically. <manual> - The administrator manually makes voice member port join voice VLAN. Related Syntax: ● <config-if># voice-vlan cos <all/src> ● <config-if># voice-vlan mode <auto/manual>

Example

```
P1282# configure
P1282(config)# interface LAG 1
P1282(config-if)# speed 100
P1282(config-if)# backpressure
P1282(config-if)# lldp med location ecs-elin 112233445566778899AA
P1282(config-if)# vlan mac-vlan group 35 vlan 1000
P1282(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 conflict

ip default-gateway

ip dhcp

ip dns

ip forcedhttps

ip http

ip https

ip igmp

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. To configure detailed settings, enter the name of ACL to access

	into next level. <config>#ip acl <NAME> Then, available sub-command includes: <config-ip-acl>#deny <config-ip-acl>#do <config-ip-acl>#end <config-ip-acl>#exit <config-ip-acl>#permit <config-ip-acl>#sequence <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. <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. dscp <0-63> - Set the DSCP filtering by specifying a value for DSCP. precedence <0-7> - Set the cos value and the cos mask for a packet. shutdown – Disable the Ethernet interface. any – Any IP address (as source or destination). Related Syntax: ● <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> ● <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 ● <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> ● <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 ● <config-ip-acl >#deny <0-255> any <A.B.C.D>/<A.B.C.D> dscp <0-63> ● <config-ip-acl >#deny <0-255> any <A.B.C.D>/<A.B.C.D> dscp <0-63> shutdown ● <config-ip-acl >#deny <0-255> any <A.B.C.D>/<A.B.C.D> precedence <0-7> ● <config-ip-acl >#deny <0-255> any <A.B.C.D>/<A.B.C.D> precedence <0-7> shutdown ● <config-ip-acl >#deny <0-255> any any dscp <0-7> ● <config-ip-acl >#deny <0-255> any any dscp <0-7> shutdown ● <config-ip-acl >#deny <0-255> any any precedence <0-7> ● <config-ip-acl >#deny <0-255> any any precedence <0-7> shutdown
	Use the “do” command to run execution command in current mode.

	<SEQUENCE> - Related Syntax: ● <config-ip-acl>#do <SEQUENCE>
	Use the "end" command to finish current mode. Any changes in current mode will be saved. Related Syntax: ● <config-ip-acl>#end
	Use the "exit" command to close the current CLI session or return to the previous mode without saving the settings. Related Syntax: ● <config-ip-acl>#exit
	Use the "no sequence" command to delete any entry in management ACL. <1-2147483647>- Specify an index number of the ACL. Related Syntax: ● <config-ip-acl>#no sequence <1-2147483647>
	Use the "sequence" command to deny or permit the ACL. <1-2147483647> - Enter the sequence of ACL entry. The sequence represents the priority of the ACE in the ACL. Related Syntax: ● <config-ip-acl >#sequence <1-2147483647> deny ● <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. 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. mask <A.B.C.D> - Specify the netmask of the IP address. Related Syntax: ● <config>#ip address <A.B.C.D> ● <config>#ip address <A.B.C.D> mask <A.B.C.D>
ip conflict	Use this command to do IP conflict prevention. lag - Enable/disable the function. <A.B.C.D> - Specify the IPv4 addresses. <1-28> - Specify a physical port. <1-8> - Specify a LAG port. Related Syntax: ● <config>#ip conflict detection ● <config>#ip conflict lag ● <config>#ip conflict prevention ● <config>#ip conflict prevention clear ● <config>#ip conflict prevention server-ip <A.B.C.D> interface GigabitEthernet <1-28> ● <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. address <A.B.C.D> - Specify the IPv4 addresses. Related Syntax: ● <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. Related Syntax: ● <config>#ip dhcp
ip dns	Use this command to modify DNS server configuration. <A.B.C.D> - Specify the IP address as primary DNS server. <A.B.C.D> <A.B.C.D> - Sepcify two IP addresses as primary and secondary DNS server. <X:X:XX:X:X> - Specify the MAC address as primary DNS server. <X:X:XX:X:X><X:X::X:X> - Specify two MAC addresses as primary and secondary DNS server. lookup – Enable the IP domain naming system lookup. Related Syntax: ● <config>#ip dns <A.B.C.D> ● <config>#ip dns <A.B.C.D> <A.B.C.D> ● <config>#ip dns <X:X:XX:X:X> ● <config>#ip dns <X:X:XX:X:X><X:X::X:X> ● <config>#ip dns lookup
ip forcedhttps	Use this command to enable the function of forced HTTPS configuration. Related Syntax: ● <config>#ip forcedhttps
ip http	Use this command to enable the function of HTTP configuration. Session-timeout – Set the session timeout. <0-86400> - Set the timeout value. 0 means no timeout. Related Syntax: ● <config>#ip http session-timeout <0-86400>
ip https	Use this command to enable the function of HTTPS configuration. session-timeout – Set the session timeout. <0-86400> - Set the timeout value. 0 means no timeout. tls version <tls1.2/tls1.3> - Set the TLS version. Related Syntax: ● <config>#ip https session-timeout <0-86400> ● <config>#ip https tls version <tls1.2/tls1.3>
ip igmp	Use this command to set IGMP profile and enable IGMP snooping function. Profile – Set IGMP profile. <1-128> - Enter the index number of IGMP profile to access

	into next phase for configuring detailed settings. <A.B.C.D><A.B.C.D> - Specify the source and destination IPv4 addresses action <deny/permit> - Specify the rule (deny/permit) for the IGMP profile. snooping forward-method <dip/mac> - Set the forward method. snooping report-suppression - Set the IGMP v1 or v2 report suppression. snooping unknown-multicast action drop /flood/router-port- Set unknown multicast. The packets will be dropped, flood, or forwarded to the router ports. snooping version <2/3> - Set the IGMP snooping operation version. snooping vlan <VLAN-LIST>- Set a VLAN ID (1 to 4094) for the IGMP VLAN configuration. forbidden-port GigabitEthernt <1 to 28> / LAG <1 to 8> - Specify an interface for the IPv4 forbidden port configuration. immediate-leave - Enable the IGMP snooping immediate-leave function. last-member-query-count <1-7>- Set a value as the Last Member Query Count. last-member-query-interval <1-25> - Set the time interval. querier - Enable the querier for the IGMP VLAN configuration. querier <2/3> - Set the querier version (Version 2 or Version 3). query-interval <30-18000> - Set the time interval for the query. response-time <5-20> - Set the response time. robustness-variable <1-7> - Set the robustness variable. router learn pim-dvmrp - Enable the IGMP snooping router port learn by PIM, DVMRP and IGMP messages. static-group <A.B.C.D> - Specify the IPv4 multicast address. interfaces GigabitEthernt <1 to 28>/ LAG <1 to 8> - Specify an interface. static-port GigabitEthernt <1 to 28>/LAG <1 to 8> - Set the static port for an interface. static-router-port GigabitEthernt <1 to 28>/LAG <1 to 8> - Set the static router port for an interface. Related Syntax: ● <config>#ip igmp profile <1-128> ● <config-igmp-profile># do ● <config-igmp-profile># end ● <config-igmp-profile># exit ● <config-igmp-profile># profile range ip <A.B.C.D><A.B.C.D> ● <config-igmp-profile># profile range ip <A.B.C.D><A.B.C.D> action <deny/permit> ● <config-igmp-profile># profile range ip <A.B.C.D> action <deny/permit> ● <config-igmp-profile># show

	● <config>#ip igmp snooping ● <config>#ip igmp snooping forward-method <dip/mac> ● <config>#ip igmp snooping report-suppression ● <config>#ip igmp snooping unknown-multicast action <drop / flood / router-port> ● <config>#ip igmp snooping version <2/3> ● <config>#ip igmp snooping vlan <VLAN-LIST> forbidden-port GigabitEthernt <1 to 28> ● <config>#ip igmp snooping vlan <VLAN-LIST> forbidden-port LAG <1 to 8> ● <config>#ip igmp snooping vlan <VLAN-LIST> forbidden-router-port GigabitEthernt <1 to 28> ● <config>#ip igmp snooping vlan <VLAN-LIST> forbidden-router-port LAG <1 to 8> ● <config>#ip igmp snooping vlan <VLAN-LIST> immediate-leave ● <config>#ip igmp snooping vlan <VLAN-LIST> last-member-query-count <1-7> ● <config>#ip igmp snooping vlan <VLAN-LIST> last-member-query-interval <1-25> ● <config>#ip igmp snooping vlan <VLAN-LIST> querier ● <config>#ip igmp snooping vlan <VLAN-LIST> querier <2/3> ● <config>#ip igmp snooping vlan <VLAN-LIST> query-interval <30-18000> ● <config>#ip igmp snooping vlan <VLAN-LIST> response-time <5-20> ● <config>#ip igmp snooping vlan <VLAN-LIST> robustness-variable <1-7> ● <config>#ip igmp snooping vlan <VLAN-LIST> router learn pim-dvmrp ● <config>#ip igmp snooping vlan <VLAN-LIST> static-group <A.B.C.D> interfaces GigabitEthernt <1 to 28> ● <config>#ip igmp snooping vlan <VLAN-LIST> static-group <A.B.C.D> interfaces LAG <1 to 8> ● <config>#ip igmp snooping vlan <VLAN-LIST> static-port GigabitEthernt <1 to 28> ● <config>#ip igmp snooping vlan <VLAN-LIST> static-port LAG <1 to 8> ● <config>#ip igmp snooping vlan <VLAN-LIST> static-router-port GigabitEthernt <1 to 28> ● <config>#ip igmp snooping vlan <VLAN-LIST> static-router-port LAG <1 to 8>
ip source	Use this command to create a static IP source binding entry. <A:B:C:D:E:F> - Enter the MAC address for the binding entry. vlan <1-4094> - Specify the VLAN ID number. <A.B.C.D><A.B.C.D> - Specify the source and destination IPv4 addresses. <1-28> - Specify a physical port. <1-8> - Specify a LAG port.

	Related Syntax: ● <config>#ip source binding <A:B:C:D:E:F> vlan <1-4094> <A.B.C.D> <A.B.C.D> interface GigabitEthernet <1-28> ● <config>#ip source binding <A:B:C:D:E:F> vlan <1-4094> <A.B.C.D> <A.B.C.D> interface LAG <1-8> ● <config>#ip source binding vlan <1-4094> <A.B.C.D> <A.B.C.D> interface GigabitEthernet <1-28> ● <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. <all/v1/v2> - Select the key files for SSH connection. Related Syntax: ● <config>#ip ssh <all/v1/v2>
ip telnet	Use this command to enable telnet service. Related Syntax: ● <config>#ip telnet

Example

```
P1282# configure
P1282(config)# ip acl market_1
P1282(config-ip-acl)#
P1282(config-ip-acl)# deny 20 192.168.2.55/255.255.255.0 192.168.2.85/255.255.255.0
P1282(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. To configure detailed settings, enter the name of ACL to access into next level. <config>#ipv6 acl <NAME> Then, available sub-command includes: <config-ipv6-acl>#deny <config-ipv6-acl>#do

	<config-ipv6-acl>#end <config-ipv6-acl>#exit <config-ipv6-acl>#no <config-ipv6-acl>#permit <config-ipv6-acl>#sequence <config-ipv6-acl>#show
	Use the “deny” command to create deny rules for the IPv4 access list. <0-255/icmp/ipv6/tcp /udp > - Specify the IP protocol number or enter the name of the protocol. <0-255/any> - Specify ICMPv6 number. <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> - Specify the source/destination IPv6 addresses and subnet masks. dscp <0-63> - Set the DSCP filtering by specifying a value for DSCP. precedence <0-7> - Set the cos value and the cos mask for a packet. shutdown – Disable the Ethernet interface. any – Any IP address (as source or destination). <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. 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). <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. Related Syntax: ● <config-ipv6-acl >#deny <0-255> <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> ● <config-ipv6-acl >#deny <0-255> <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> dscp <0-63> ● <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> ● <config-ipv6-acl >#deny <0-255> <X:X::X:X>/<0-128>

	<X:X::X:X>/<0-128> precedence <0-7> shutdown ● <config-ipv6-acl >#deny <0-255> <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> shutdown ● <config-ipv6-acl >#deny <0-255> <X:X::X:X>/<0-128> any dscp <0-63> ● <config-ipv6-acl >#deny <0-255> <X:X::X:X>/<0-128> any dscp <0-63> shutdown ● <config-ipv6-acl >#deny <0-255> <X:X::X:X>/<0-128> any precedence <0-7> ● <config-ipv6-acl >#deny <0-255> <X:X::X:X>/<0-128> any precedence <0-7>shutdown ● <config-ipv6-acl >#deny <0-255> <X:X::X:X>/<0-128> any shutdown ● <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> ● <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 ● <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> ● <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 ● <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 ● <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> ● <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 ● <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> ● <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 ● <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 ● <config-ipv6-acl >#deny ipv6 <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> ● <config-ipv6-acl >#deny ipv6 <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> dscp <0-63> ● <config-ipv6-acl >#deny ipv6 <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> dscp <0-63> shutdown ● <config-ipv6-acl >#deny ipv6 <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> precedence <0-7> ● <config-ipv6-acl >#deny ipv6 <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> precedence <0-7> shutdown ● <config-ipv6-acl >#deny ipv6 <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> shutdown ● <config-ipv6-acl >#deny ipv6 <X:X::X:X>/<0-128> any dscp <0-63> ● <config-ipv6-acl >#deny ipv6 <X:X::X:X>/<0-128> any dscp <0-63> shutdown ● <config-ipv6-acl >#deny ipv6 <X:X::X:X>/<0-128> any precedence <0-7> ● <config-ipv6-acl >#deny ipv6 <X:X::X:X>/<0-128> any precedence <0-7>shutdown ● <config-ipv6-acl >#deny ipv6 <X:X::X:X>/<0-128> any shutdown ● <config-ipv6-acl >#deny ipv6 any <X:X::X:X>/<0-128> ● <config-ipv6-acl >#deny ipv6 any <X:X::X:X>/<0-128> dscp <0-63> ● <config-ipv6-acl >#deny ipv6 any <X:X::X:X>/<0-128> dscp <0-63> shutdown ● <config-ipv6-acl >#deny ipv6 any <X:X::X:X>/<0-128> precedence <0-7> ● <config-ipv6-acl >#deny ipv6 any <X:X::X:X>/<0-128> precedence <0-7> shutdown ● <config-ipv6-acl >#deny ipv6 any <X:X::X:X>/<0-128>

shutdown

- <config-ipv6-acl >#deny ipv6 any any
- <config-ipv6-acl >#deny ipv6 any any dscp <0-63>
- <config-ipv6-acl >#deny ipv6 any any dscp <0-63> shutdown
- <config-ipv6-acl >#deny ipv6 any any precedence <0-7>
- <config-ipv6-acl >#deny ipv6 any any precedence <0-7> shutdown
- <config-ipv6-acl >#deny ipv6 any any shutdown
- <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>
- <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>
- <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
- <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 >#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 ● <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> ● <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 ● <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 ● <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> ● <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 ● <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 ● <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> ● <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> ● <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 ● <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> ● <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 ● <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. <SEQUENCE> - Related Syntax: ● <config-ipv6-acl>#do <SEQUENCE>
	Use the “end” command to finish current mode. Any changes in current mode will be saved.

	Related Syntax: ● <config-ipv6-acl>#end
	Use the “exit” command to close the current CLI session or return to the previous mode without saving the settings. Related Syntax: ● <config-ipv6-acl>#exit
	Use the “no sequence” command to delete any entry in management ACL. <1-2147483647>- Specify an index number of the ACL. Related Syntax: ● <config-ip-acl>#no sequence <1-2147483647>
	Use the “permit” command to create permit rules which bypass the packets meet the rule. <0-255/icmp/ipv6/tcp /udp > - Specify the IP protocol number or enter the name of the protocol. <0-255/any> - Specify ICMPv6 number. <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> - Specify the source/destination IPv6 addresses and subnet masks. dscp <0-63> - Set the DSCP filtering by specifying a value for DSCP. precedence <0-7> - Set the cos value and the cos mask for a packet. shutdown – Disable the Ethernet interface. any – Any IP address (as source or destination). <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. 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). <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. Related Syntax: ● <config-ipv6-acl >#permit <0-255> <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> ● <config-ipv6-acl ># permit <0-255> <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> dscp <0-63>

	● <config-ipv6-acl ># permit <0-255> <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> dscp <0-63> shutdown ● <config-ipv6-acl ># permit <0-255> <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> precedence <0-7> ● <config-ipv6-acl ># permit <0-255> <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> precedence <0-7> shutdown ● <config-ipv6-acl ># permit <0-255> <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> shutdown ● <config-ipv6-acl ># permit <0-255> <X:X::X:X>/<0-128> any dscp <0-63> ● <config-ipv6-acl ># permit <0-255> <X:X::X:X>/<0-128> any dscp <0-63> shutdown ● <config-ipv6-acl ># permit <0-255> <X:X::X:X>/<0-128> any precedence <0-7> ● <config-ipv6-acl ># permit <0-255> <X:X::X:X>/<0-128> any precedence <0-7>shutdown ● <config-ipv6-acl ># permit <0-255> <X:X::X:X>/<0-128> any shutdown ● <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> ● <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 ● <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> ● <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 ● <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 ● <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>

	● <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 ● <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> ● <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 ● <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 ● <config-ipv6-acl ># permit ipv6 <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> ● <config-ipv6-acl ># permit ipv6 <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> dscp <0-63> ● <config-ipv6-acl ># permit ipv6 <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> dscp <0-63> shutdown ● <config-ipv6-acl ># permit ipv6 <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> precedence <0-7> ● <config-ipv6-acl ># permit ipv6 <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> precedence <0-7> shutdown ● <config-ipv6-acl ># permit ipv6 <X:X::X:X>/<0-128> <X:X::X:X>/<0-128> shutdown ● <config-ipv6-acl ># permit ipv6 <X:X::X:X>/<0-128> any dscp <0-63> ● <config-ipv6-acl ># permit ipv6 <X:X::X:X>/<0-128> any dscp <0-63> shutdown ● <config-ipv6-acl ># permit ipv6 <X:X::X:X>/<0-128> any precedence <0-7> ● <config-ipv6-acl ># permit ipv6 <X:X::X:X>/<0-128> any precedence <0-7>shutdown ● <config-ipv6-acl ># permit ipv6 <X:X::X:X>/<0-128> any shutdown ● <config-ipv6-acl ># permit ipv6 any <X:X::X:X>/<0-128> ● <config-ipv6-acl ># permit ipv6 any <X:X::X:X>/<0-128> dscp <0-63> ● <config-ipv6-acl ># permit ipv6 any <X:X::X:X>/<0-128> dscp <0-63> shutdown ● <config-ipv6-acl ># permit ipv6 any <X:X::X:X>/<0-128>

	precedence <0-7> ● <config-ipv6-acl ># permit ipv6 any <X:X::X:X>/<0-128> precedence <0-7> shutdown ● <config-ipv6-acl ># permit ipv6 any <X:X::X:X>/<0-128> shutdown ● <config-ipv6-acl ># permit ipv6 any any ● <config-ipv6-acl ># permit ipv6 any any dscp <0-63> ● <config-ipv6-acl ># permit ipv6 any any dscp <0-63> shutdown ● <config-ipv6-acl ># permit ipv6 any any precedence <0-7> ● <config-ipv6-acl ># permit ipv6 any any precedence <0-7> shutdown ● <config-ipv6-acl ># permit ipv6 any any shutdown ● <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> ● <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> ● <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 ● <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 ● <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> ● <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 ● <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 ● <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> ● <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 ● <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 ● <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> ● <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> ● <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 ● <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> ● <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 ● <config-ipv6-acl ># permit udp <X:X::X:X>/<0-128> <0-65535> any
	Use the “sequence” command to deny or permit the ACL. <1-2147483647> - Enter the sequence of ACL entry. The sequence represents the priority of the ACE in the ACL.

	Related Syntax: ● <config-ipv6-acl >#sequence <1-2147483647> deny ● <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. 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. prefix <0-128> - Specify the prefix length of the IPv6 address. Related Syntax: ● <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. default-address <X:X::X:X> - Specify the IPv6 addresses of the gateway. Related Syntax: ● <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. Related Syntax: ● <config>#ipv6 dhcp
ipv6 mld	Use this command to set MLD configuration. profile <1-128> - Use it to enter profile configuration. snooping – Use it to enable MLD snooping function. forward-method <dip/mac> - Specify a method to forward the packets. report-suppression – Use it to enable MLD snooping report-suppression function. unknown-multicast action <drop/flood/router-port> - Use it to set unknown multicast action. version <1/2> – Use it to change MLD support version. vlan <1-4094> - Use it to enable MLD on VLAN. Specify a VLAN ID for configuration. forbidden-port GigabitEthernet <1-28> - Specify a physical port. forbidden-port LAG <1-8> - Specify a LAG port. forbidden-router-port GigabitEthernet <1-24> - 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. immediate-leave – Use it to enable fastleave function. 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. last-member-query-interval <1-25> - Use it to set interval between each query packet. Specify the last member query

interval. Default is 1.

query-interval <30-18000> - Use it to set interval between each query. Specify the query interval. Default is 125.

response-time <5-20> - Use it to set response time. Specify a time value. Default is 10.

robustness-variable <1-7> - Specify a robustness-variable value. Default is 2.

router learn pim-dvmrp – Use it to enable learning router port by rouing protocol packets (DVMRP).

static-group <X:X::X:X> interfaces gigabitethernet <1-28> - Use it to add a static group. Specify a physical port.

static-group <X:X::X:X> interfaces LAG <1-8> - Use it to add a static group. Specify a LAG port.

static-port gigabitethernet <1-28>- Use it to add static forwarding port. Specify a physical port.

static-port LAG <1-8>- Use it to add static forwarding port. Specify a LAG port.

static-router-port GigabitEthernet <1-28> - Use it to add static router port. All query packets wil forward to the specified port. Specify a physical port.

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.

Related Syntax:

- <config>#ipv6 mld profile <1-128>
    - <config-mld-profile># do
    - <config-mld-profile># end
    - <config-mld-profile># exit
    - <config-mld-profile># profile range ipv6 <X:X::X:X> action <deny/permit>
    - <config-mld-profile># profile range ipv6 <X:X::X:X> <X:X::X:X>
    - <config-mld-profile># profile range ipv6 <X:X::X:X> <X:X::X:X> action <deny/permit>
    - <config-mld-profile># show
- <config>#ipv6 mld snooping
- <config>#ipv6 mld snooping forward-method <dip/mac>
- <config>#ipv6 mld snooping report-suppression
- <config>#ipv6 mld snooping unknown-multicast action <drop/flood/router-port>
- <config>#ipv6 mld snooping version <1/2>
- <config>#ipv6 mld snooping vlan <1-4094>
- <config>#ipv6 mld snooping vlan <1-4094> forbidden-port GigabitEthernet <1-28>
- <config>#ipv6 mld snooping vlan <1-4094> forbidden-port LAG <1-8>
- <config>#ipv6 mld snooping vlan <1-4094> forbidden-router-port GigabitEthernet <1-28>
- <config>#ipv6 mld snooping vlan <1-4094>

	forbidden-router-port LAG <1-8> ● <config>#ipv6 mld snooping vlan <1-4094> immediate-leave ● <config>#ipv6 mld snooping vlan <1-4094> last-member-query-count <1-7> ● <config>#ipv6 mld snooping vlan <1-4094> last-member-query-interval <1-25> ● <config>#ipv6 mld snooping vlan <1-4094> query-interval <30-18000> ● <config>#ipv6 mld snooping vlan <1-4094> response-time <5-20> ● <config>#ipv6 mld snooping vlan <1-4094> robustness-variable <1-7> ● <config>#ipv6 mld snooping vlan <1-4094> router learn pim-dvmrp ● <config>#ipv6 mld snooping vlan <1-4094> static-group <X:X::X:X> interfaces gigabitethernet <1-28> ● <config>#ipv6 mld snooping vlan <1-4094> static-group <X:X::X:X> interfaces LAG <1-8> ● <config>#ipv6 mld snooping vlan <1-4094> static-port gigabitethernet <1-28> ● <config>#ipv6 mld snooping vlan <1-4094> static-port LAG <1-8> ● <config>#ipv6 mld snooping vlan <1-4094> static-router-port GigabitEthernet <1-28> ● <config>#ipv6 mld snooping vlan <1-4094> static-router-port LAG <1-8>

Example

```
P1282# configure
P1282(config)#
P1282(config)# ipv6 mld snooping vlan 33
P1282(config)# ipv6 acl CA_v6
P1282(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. Set the maximum frame size. <1518-10000> - The default value is 1522. Related Syntax: ● <config># jumbo-frame

	● <config># jumbo-frame <1518-10000>

Example

```
P1282# configure
P1282(config)#
P1282(config)# jumbo-frame 8000
P1282(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. <1-65535> - Specify the system priority value. Related Syntax: ● <config># lacp ● <config># lacp system-priority <1-65535>

Example

```
P1282# configure
P1282(config)#
P1282(config)# lacp system-priority 1000
P1282(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. Related Syntax: ● <config># lag load-balance src-dst-mac

	● <config># lag load-balance src-dst-mac-ip

Example

```
P1282# configure
P1282(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. To configure detailed settings, access into next level. <config>#line <console/ssh/telnet> console - Select the console line to configure. Then, available sub-commands are: <config-line>#do <config-line>#exec-timeout <config-line>#exit <config-line>#lhistory <config-line>#no <config-line>#password-thresh <config-line>#silent-time
	Select SSH line to configure. Then, available sub-commands are: <config-line>#do <config-line>#end <config-line>#exec-timeout <config-line>#exit <config-line>#password-thresh <config-line>#silent-time
	telnet - Select telnet line to configure. Then, available sub-commands are: <config-line>#do <config-line>#end <config-line>#exec-timeout <config-line>#exit <config-line>#password-thresh <config-line>#silent-time
#do	Use the “do” command to run execution command in current

	mode. <SEQUENCE> - Related Syntax: ● <config-line>#do <SEQUENCE>
#exec-timeout	Use the “exec-timeout” to set the session timeout configuration. <0-65535> - Enter the number. Related Syntax: ● <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. Related Syntax: ● <config-line>#exit
#history	Use the “history” command to specify the index number of history. <1-256> - Enter a number. Related Syntax: ● <config-line>#history <1-256>
#no	Use the “no” command to negate line command. Related Syntax: ● <config-line>#no enable ● <config-line>#no history ● <config-line>#no login
#password-thresh	Use the “password-thresh” command to set the login password intrusion threshold. <0-120> - Set a number of allowed password attempts. 0 means no threshold. Related Syntax: ● <config-line>#password-thresh <0-120>
#silent-time	Use the “silent-time” command to set fail silent time. <0-65535> - Set the time to disable the console response. Related Syntax: ● <config-line>#silent-time <0-65535>

Example

```
P1282# configure
P1282(config)#
P1282(config)# line telnet
P1282(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. <2-10> - Set the LLDP hold time multiplier. Related Syntax: ● <config># lldp holdtime-multiplier <2-10>
lldp lldpdu	bridging - The LLDP packets will be bridging when LLDP is disabled. filtering - The LLDP packets will be filtered and deleted when LLDP is disabled. flooding - The LLDP packets will be flooded and forwarded to all interfaces when LLDP is disabled. Related Syntax: ● <config># lldp lldpdu bridging ● <config># lldp lldpdu filtering ● <config># lldp lldpdu flooding
lldp reinit-delay	Set the LLDP re-initial delay to avoid LLDP generating too many PDU. <1-10> - Specify a number for LLDP server to initialize. Related Syntax: ● <config># lldp reinit-delay <1-10>
lldp tx-delay	Set the delay time between the successful LLDP frame transmissions. <1-8191> - Enter the number of delay time. Note that both tx-interval and tx-delay will affect the LLDP PDU TX time. Related Syntax: ● <config># lldp tx-delay <1-8191>
lldp tx-interval	Set the LLDP TX interval. <5-32767> - Enter the interval in unit of second. Related Syntax: ● <config># lldp tx-interval <5-32767>

Example

```
P1282# configure
P1282(config)#
P1282(config)# lldp holdtime-multiplier 5
```

```
P1282(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. <0-7> - Specify the logging level by entering a number (from EMEGR-DEBUG). Related Syntax: ● <config># logging console ● <config># logging console severity <0-7>
logging file	Store the log message in the flash. <0-7> - Specify the logging level by entering a number (from EMEGR-DEBUG). Related Syntax: ● <config># logging file severity <0-7>
logging host	Define the logging server. host <A.B.C.D> - Enter an IP address of the remote (or local) server. facility <local0-local7> - Specify the facility parameter for the syslog message. port <1-65535> - Enter a number for the remote server. Default is 514. severity <0-7> - Specify the logging level by entering a number (from EMEGR-DEBUG). <HOSTNAME> - Define a name as the host. Related Syntax: ● <config>#logging host <A.B.C.D> facility <local0-local7> ● <config>#logging host <A.B.C.D> port <1-65535> ● <config>#logging host <A.B.C.D> port <1-65535> facility <local0-local7> ● <config>#logging host <A.B.C.D> port <1-65535> severity <0-7> facility <local0-local7> ● <config>#logging host <A.B.C.D> severity <0-7> facility <local0-local7>

	● <config>#logging host <HOSTNAME> facility <local0-local7> ● <config>#logging host <HOSTNAME> port <1-65535> ● <config>#logging host <HOSTNAME> port <1-65535> facility <local0-local7> ● <config>#logging host <HOSTNAME> port <1-65535> severity <0-7> facility <local0-local7> ● <config>#logging host <HOSTNAME> severity <0-7> facility <local0-local7> ● <config>#logging host <X:X::X:X> facility <local0-local7> ● <config>#logging host <X:X::X:X> port <1-65535> ● <config>#logging host <X:X::X:X> port <1-65535> facility <local0-local7> ● <config>#logging host <X:X::X:X> port <1-65535> severity <0-7> facility <local0-local7>

Example

```
P1282# configure
P1282(config)#
P1282(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. Related Syntax: ● <config># logmail active <disable/enable>
logmail auth	<disable/enable> - Enable or disable the function of SMTP server authentication. Related Syntax: ● <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. Related Syntax: ● <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. <PASSWORD> - Enter the password for SMTP server encrypt authentication. Related Syntax: ● <config># logmail encpassword <PASSWORD>
logmail encry	<disable/ssltls/starttls> - Specify the encryption type for mail alert. Related Syntax: ● <config># logmail encry <disable/ ssltls/starttls>
logmail password	<PASSWORD> - Enter the password for SMTP server authentication. Related Syntax: ● <config># logmail password <PASSWORD>
logmail port	<0-65535>- Enter a port number. Related Syntax: ● <config># logmail port <0-65535>
logmail receiver	Specify an address for receiving the alart mail. <ADDRESS> - Enter the email address of the receiver. Related Syntax: ● <config># logmail receiver <ADDRESS>
logmail sender	Specify an address which sends out the alert mail. <ADDRESS> - Enter the email address of the sender. Related Syntax: ● <config># logmail
logmail server	Set the IP address of the server. <ADDRESS> - Enter the IP address of the SMTP server. Related Syntax: ● <config># logmail server <ADDRESS>
logmail username	<NAEM> - Enter the username authenticated by STMP server. Related Syntax: ● <config># logmail username <NAME>

Example

```
P1282# configure
P1282(config)#
P1282(config)# logmail receiver carrie_ni@draytek.com
P1282(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. <all/log/shutdown> - Specify one action to be executed. Related Syntax: ● <config># loop-protection action <all/log/shutdown>
loop-protection periodicTime	Send the loop protection packets to the network hosts. <1-3> - Enter the number of the packet. Related Syntax: ● <config># Related Syntax: ● <config># loop-protection periodicTime <1-3>
loop-protection state	<enable/disable> - Enable or disable the function of loop protection. Related Syntax: ● <config># loop-protection state <enable/disable>

Example

```
P1282# configure
P1282(config)#
P1282(config)# loop-protection state enable
P1282(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). To configure detailed settings, enter the name of ACL to access

	into next level. <config>#mac acl <NAME> Then, available sub-commands are: <config-mac-acl>#deny <config-mac-acl>#do <config-mac-acl>#end <config-mac-acl>#exit <config-mac-acl>#permit <config-mac-acl>#sequence
	Use the “deny” command to add deny rules for the MAC access list: <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. cos <0-7><0-7> - Set the cos value and the cos mask for a packet. <0x0600-0xFFFF> - Set the EtherType of the packet. Shutdown – Disable the Ethernet interface. vlan <1-4094> - Specify the VLAN ID of the packet. any – Any MAC address. Related Syntax: ● <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> ● <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> ● <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 ● <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 ● <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> ● <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 ● <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 ● <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> ● <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> ● <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 ● <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 ● <config-mac-acl >#deny any any cos <0-7><0-7>

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

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

	● <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 ● <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 ● <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> ● <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 ● <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 ● <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> ● <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> ● <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 ● <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 ● <config-mac-acl >#sequence <1-2147483647>deny any any cos <0-7><0-7> ● <config-mac-acl >#sequence <1-2147483647>deny any any cos <0-7><0-7> ethtype <0x0600-0xFFFF> ● <config-mac-acl >#sequence <1-2147483647>deny any any cos <0-7><0-7> ethtype <0x0600-0xFFFF> shutdown ● <config-mac-acl >#sequence <1-2147483647>deny any any cos <0-7><0-7> shutdown ● <config-mac-acl >#sequence <1-2147483647>deny any any ethtype <0x0600-0xFFFF> ● <config-mac-acl >#sequence <1-2147483647>deny any any ethtype <0x0600-0xFFFF> shutdown ● <config-mac-acl >#sequence <1-2147483647>deny any any shutdown ● <config-mac-acl >#sequence <1-2147483647>deny any any vlan <1-4094> ● <config-mac-acl >#sequence <1-2147483647>deny any any vlan <1-4094> cos <0-7><0-7> ● <config-mac-acl >#sequence <1-2147483647>deny any any vlan <1-4094> cos <0-7><0-7> ethtype <0x0600-0xFFFF> ● <config-mac-acl >#sequence <1-2147483647>deny any any vlan <1-4094> cos <0-7><0-7> ethtype <0x0600-0xFFFF> shutdown ● <config-mac-acl >#sequence <1-2147483647>deny any any

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

	any vlan <1-4094> cos <0-7><0-7> ● <config-mac-acl >#sequence <1-2147483647>permit any any vlan <1-4094> cos <0-7><0-7> ethtype <0x0600-0xFFFF> ● <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. address-table static - Add a static address to the MAC address table to drop the packets with the specified source or destination MAC address. <10-630> - Unit is second. Default is 300. static <A:B:C:D:E:F> - Enter the MAC address. vlan <1-4094> - Specify the VLAN ID of the packet. gigabitEthernet <1-24> - Specify a physical port. LAG <1-8> - Specify a LAG port. Related Syntax: ● <config># mac address-table aging-time <10-630> ● <config># mac address-table static <A:B:C:D:E:F> vlan <1-4094> drop ● <config># mac address-table static <A:B:C:D:E:F> vlan <1-4094> interfaces 10GigabitEthernet <1-4> ● <config># mac address-table static <A:B:C:D:E:F> vlan <1-4094> interfaces GigabitEthernet <1-24> ● <config># mac address-table static <A:B:C:D:E:F> vlan <1-4094> interfaces LAG <1-8>

Example

```
P1282# configure
P1282(config)# mac acl test_CA
P1282(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
P1282(config-mac-acl)# deny any 00:50:00:7f:12:11/00:00:00:00:10:20 cos 5 6 ethtype 0x0600
P1282(config-mac-acl)# deny any
P1282(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. Related Syntax: ● <config># mailalert active <disable/enable>
mailalert auth	<disable/enable> - Enable or disable the function of SMTP server authentication. Related Syntax: ● <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. Related Syntax: ● <config># mailalert devicecheck <disable/enable>
mailalert encpassword	<PASSWORD> - Set a encryption authentication password for the mail alert. Related Syntax: ● <config># mailalert encpassword <PASSWORD>
mailalert encry	Specify the encryption type for mail alert. <disable/ssltls/starttls> - Related Syntax: ● <config># mailalert encry <disable/ ssltls/starttls>
mailalert hwmon	Send a mail alert when hardware monitor error. <disable/enable> - Enable or disable the function. Related Syntax: ● <config># mailalert hwmon <disable/enable>
mailalert interval	Set the transmission interval for the mail alert. <1-60> - Unit is second. Related Syntax: ● <config># mailalert interval <1-60>
mailalert ipconflict	<disable/enable> - Enable or disable the function of sending a mail alert if encountering the IP conflict. Related Syntax:

	● <config># mailalert ipconflict <disable/enable>
mailalert password	<PASSWORD> - Enter the password for SMTP server authentication. Related Syntax: ● <config># mailalert password <PASSWORD>
mailalert poestatus	<disable/enable> - Enable or disable the function of sending a mail alert when PoE status is changed. Related Syntax: ● <config># mailalert poestatus <disable/enable>
mailalert port	<0-65535>- Enter a port number. Related Syntax: ● <config># mailalert port <0-65535>
mailalert portlink	<disable/enable> - Enable or disable the function of sending an alert when the port lnik status changes. Related Syntax: ● <config># mailalert portlink <disable/enable>
mailalert portspeed	<disable/enable> - Enable or disable the function of sending an alert when the port link speed changes. Related Syntax: ● <config># mailalert portspeed <disable/enable>
mailalert receiver	Specify an address for receiving the alart mail. <ADDRESS> - Enter the email address of the receiver. Related Syntax: ● <config># mailalert receiver <ADDRESS>
mailalert sender	Specify an address which sends out the alert mail. <ADDRESS> - Enter the email address of the sender. Related Syntax: ● <config># mailalert sender <ADDRESS>
mailalert server	Set the IP address of the server. <ADDRESS> - Enter the IP address of the SMTP server. Related Syntax: ● <config># mailalert server <ADDRESS>
mailalert sysrestart	<disable/enable> -Enable or disable the function of sending a mail alert when the system restarts. Related Syntax: ● <config># mailalert sysrestart <disable/enable>
mailalert throughputcheck	<disable/enable> - Enable or disable the function of sending a mail alert when reaching the throughput threshold. Related Syntax: ● <config># mailalert throughputcheck <disable/enable>
mailalert username	<NAEM> - Enter the username authenticated by STMP server. Related Syntax: ● <config># mailalert username <NAME>

Example

```
P1282# configure
P1282(config)#
P1282(config)# mailalert receiver carrie_ni@draytek.com
```

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

Example

```
P1282# configure
P1282(config)#
P1282(config)# management-vlan vlan 200
VLAN 200: VLAN does not exist
P1282(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 interface of a port mirror session. <1-4> - Specify the mirror session ID number. GigabitEthernet <1-28> - Specify a physical port as the SPAN destination. LAG <1-8> - Specify a LAG port. allow-ingress – Enable the ingress traffic forwarding. <both/rx/tx> - Specify the mirror direction, TX only, RX only or TX and RX. Related Syntax: ● <config># mirror session <1-4> destination interface GigabitEthernet <1-28> allow-ingress ● <config># mirror session <1-4> source interfaces GigabitEthernet <1-28> <both/rx/tx> ● <config># mirror session <1-4> source interfaces LAG <1-8><both/rx/tx>

Example

```
P1282# configure
P1282(config)#
P1282(config)# mirror session 3 destination interface GigabitEthernet 3 allow
P1282(config)#
P1282(config)# mirror session 3 source interfaces LAG 3 both
P1282(config)#
```

Telnet Command: no

Use this command to disable specific command.

Syntax Items

no <command>

Example

```
P1282# configure
P1282(config)#
P1282(config)# no port-security
P1282(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. Related Syntax: ● <config># openvpn filename <NAME>

Example

```
P1282# configure
G1282(config)#openvpn enable
killall: openvpn: no process killed
P1282(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. manual - VigorSwitch will supply actual power demand for the PoE device and reserved PD class power for the PoE device. none - VigorSwitch does not supply any power for the PoE device. Related Syntax: ● <config># poe mode auto ● <config># poe mode manual ● <config># poe mode none
poe schedule	Specify a schedule for PoE device. global-enable - Enable the global setting. index <1-24> - Specify the index number of the schedule profiles. Related Syntax: ● <config># poe schedule global-enable ● <config># poe schedule index <1-24>

Example

```
P1282# configure
P1282(config)#
P1282(config)# poe
```

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. Related Syntax: ● <config># qos
qos map	map cos-queue - Set the CoS to queue map. map dscp-queue - Set the DSCP to queue map. map precedence-queue - Set the IP Precedence to queue map.

	map queue-cos - Modify the queue to CoS map. map queue-dscp - Modify the queue to DSCP map. map queue-precedence - Modify the queue to IP precedence map. <1-8> - Specify the queue number for the following CoS values mapped. <1-8> - Specify the queue number to which the DSCP value shall correspond. <1-8> - Specify the queue number to which the IP precedence value shall correspond. <0-7> - Enter the cos value to which the queue ID shall correspond. <0-7> - Enter the DSCP value to which the queue ID shall correspond. <0-7> - Enter the IP precedence value to which the queue ID shall correspond. Related Syntax: ● <config># qos map cos-queue SEQUENCE to <1-8> ● <config># qos map dscp-queue SEQUENCE to <1-8> ● <config># qos map precedence-queue SEQUENCE to <1-8> ● <config># qos map queue-cos SEQUENCE to <0-7> ● <config># qos map queue-dscp SEQUENCE to <0-7> ● <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. <0-8> - Specify the queue number. <weight1-weight8> <1-127> - Specify a number (1~127) representing queue weight value. Related Syntax: ● <config># qos queue strict-priority-num <0-8> ● <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. Related Syntax: ● <config># qos trust <cos/cos-dscp/ dscp/ip-precedence>

Example

```
P1282# configure
P1282(config)#
P1282(config)# qos map cos-queue SEQUENCE to 3
P1282(config)#
```

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. <1-15> - Enter a number to select a schedule profile. <DESCRIPTION> - Give a brief description for such profile. cycle-days - The action applied with the schedule will take place every few days. monthly-date - The action applied with the schedule will take place in specified day within a month. once - The action applied with the schedule will take place for one time. weekdays - The action applied with the schedule will take place on a certain day within a week. <1-31> - Enter a number to make action repeat. <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. <sun /mon /tue /wed / thu / fri / sat> - Represent Sunday, Monday, Tuesday, Wednesday, Thursday, Friday and Saturday. <1-31> - Enter a number as the start date within a month. <2000-2035> - Enter the number as the year of start date. <HH:MM> - Enter the hours and the miniutes. <on/off> - Enable (on) or disable (off) the action applied with such profile. Related Syntax: ● <config># schedule index <1-15> description <DESCRIPTION> ● <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> ● <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> ● <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> ● <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

```
P1282# configure
P1282(config)#
P1282(config)# schedule index 1 how-often cycle-days 3 start-date jan 1 2019 start-time 08:01 duraton 17:30 action on
P1282(config)# schedule index 2 how-often weekdays sun start-date may 11 2019 start-time 02:10 duration 12:10 action on
P1282(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. Available parameters for SNMP community: <NAME> after community - Enter a string (maximum length: 20 characters) as community name. <NAME> after group - Enter a string (maximum length: 30 characters) as access group. ro - Set the community as read only. rw - Set the community as read and write. Related Syntax: ● <config># snmp community <NAME> group <NAME> ● <config># snmp community <NAME> ro ● <config># snmp community <NAME> rw ● <config># snmp community <NAME> view <NAME> ro ● <config># snmp community <NAME> view <NAME> rw
snmp engineid	snmp engineid - Set the remote host for SNMP engine. default - Reset to default setting of engine ID for SNMP server. <ENGINEID> - Such number must be 10 ~ 64 hexadecimal. <A.B.C.D> - Enter the IP address of the remote SNMP server. <HOSTNAME> - Enter the host name of the remote SNMP server. <X:X::X:X> - Enter the IPv6 address for remote SNMP server. Related Syntax: ● <config># snmp engineid <ENGINEID>

	● <config># snmp engineid default ● <config># snmp engineid remote <A.B.C.D> <ENGINEID> ● <config># snmp engineid remote <HOSTNAME> <ENGINEID> ● <config># snmp engineid remote <X:X::X:X><ENGINEID>
snmp group	snmp group - Set the SNMP group. <NAME> - Specify the name of SNMP group. version <1/2c/3> - Specify the version of SNMP service. <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. read-view <NAME> - Set the view name to enable agent configuration. notify-view <NAME> - Set the view name to send only trap included in SNMP view for notification. write-view <NAME> - Set the view name to enable viewing. Related Syntax: ● <config># snmp group <NAME> version <1/2c/3> <auth/noauth/priv> read-view <NAME> ● <config># snmp group <NAME> version <1/2c/3> <auth/noauth/priv> read-view <NAME> notify-view <NAME> ● <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. <A.B.C.D> - Enter the IPv4/IPv6 address or host name of the receipt. version <1/2c/3> - Specify the version of SNMP service. <NAME> - Set the community name sent with the notification. udp-port <1-65535> - Set the UDP port number. timeout <1-300> - Set the timeout of V2c informs. retries <1-255> - Enter the retry counter of V2c informs. Related Syntax: Set a host to receive SNMP notifications. ● <config># snmp host <A.B.C.D> <NAME> retries <1-255> ● <config># snmp host <A.B.C.D> <NAME> timeout <1-300> retries <1-255> ● <config># snmp host <A.B.C.D> <NAME> udp-port <1-65535> retries <1-255> ● <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. ● <config># snmp host <A.B.C.D> informs <NAME> retries

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

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

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

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

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

Example

```
P1282# configure
P1282(config)#
P1282(config)# snmp engineid remote 192.168.2.38 00036D001188
P1282(config)# snmp engineid remote 00:50::16:88 00036D002288
P1282(config)# snmp host 192.168.2.89 CAR_community udp-port 1500 timeout 200
P1282(config)# snmp host 192.168.2.88 informs version 2c CAR_community udp-port 3000
timeout 180 retries 35
P1282(config)# snmp host 192.168.2.88 traps version 2c CAR_traps udp-port 6500 timeout 60
```

```
retries 2
P1282(config)# snmp host 192.168.2.88 version 2c CAR_version udp-port 3000 timeout 60
retries 2
P1282(config)# snmp host HOSTNAME CAR_host udp-port 3000 timeout 60 retries
P1282(config)# snmp host HOSTNAME informs HA_informs udp-port 3000 timeout 60 retries 2
P1282(config)# snmp host HOSTNAME version 2c HT_verstion udp-port 3000 timeout 60 retries
2
P1282(config)# snmp user CA_user_1 CA_group_1 auth md5 CA12345678 priv PR12345678
P1282(config)# snmp view CAR_community subtree 10 oid-mask 9 viewtype included
P1282(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. <HOSTNAME> - Enter the IP address or hostname of SNTP server. <1-65535> - Specify the port number for the SNTP server. Related Syntax: ● <config># sntp host <HOSTNAME> ● <config># sntp host <HOSTNAME>> port <1-65535>

Example

```
P1282# configure
P1282(config)#
P1282(config)# sntp host KEY1245 port 3000
P1282(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. Related Syntax: ● <config># spanning-tree
spanning-tree bpdu	Filter/flood the BPDU packets. <filtering> - Packets will be filtered when STP is disabled on specified interface. <flooding> - Packets will be flooded to all interfaces with STP disabled and flooding mode. Related Syntax: ● <config># spanning-tree bpdu<filtering/flooding>
spanning-tree forward-delay	Set the STP forward delay time. <4-30> - Default value is 15 (seconds). Related Syntax: ● <config># spanning-tree forward-delay <4-30>
spanning-tree hello-time	Set the hello time interval to broadcast the message to other bridges. <1-10> - Default value is 2 (seconds). Related Syntax: ● <config># spanning-tree hello-time <1-10>
spanning-tree maximum-age	Set the time interval for VigorSwitch to wait without receiving the configuration message. <6-40> - Default value is 20 (seconds). Related Syntax: ● <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). Related Syntax: ● <config># spanning-tree mode <mstp/rstp/stp>
spanning-tree pathcost	Set the path-cost method for spanning tree. <long/short> - Long means the path cost ranging from 1 to 200000000; short means the path cost ranging from 1 to 65535. Related Syntax: ● <config># spanning-tree pathcost method <long/short>
spanning-tree priority	Set the priority for the specified instance ID. <0-61440> - The number must be multiple of 4096. Related Syntax: ● <config># spanning-tree priority <0-61440>
spanning-tree tx-hold-count	Set the maximum number of packets transmission per second. <1-10> - Valid range is from 1 to 10. Related Syntax:

	● <config># spanning-tree tx-hold-count <1-10>

Example

```
P1282# configure
P1282(config)#
P1282(config)# spanning-tree forward-delay 20
P1282(config)#
P1282(config)# spanning-tree maximum-age 38
P1282(config)#
P1282(config)# spanning-tree tx-hold-count 3
P1282(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: ● <config># start-up icp enable

Example

```
P1282# configure
P1282(config)#
P1282(config)# start-up icp enable
P1282(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. Related Syntax: ● <config># storm-control ifg exclude
storm-control ifg include	Include the preamble and IFG (inter frame gap) into the calculating.

	Related Syntax: ● <config># storm-control ifg include
storm-control unit bps	Change the unit of calculating method for storm-control. bps – Calculate the storm control rate by octet-based. Related Syntax: ● <config># storm-control unit bps
storm-control unit pps	Change the unit of calculating method for storm-control. pps – Calculate the storm control rate by packet-based. Related Syntax: ● <config># storm-control unit pps

Example

```
P1282# configure
P1282(config)#
P1282(config)# storm-control ifg exclude
P1282(config)#
P1282(config)# storm-control unit bps
P1282(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. Related Syntax: ● <config># surveillance-vlan
surveillance-vlan aging-time	Set the aging time for surveillance VLAN. <30-65536> - Enter a value as aging time. Related Syntax: ● <config># surveillance-vlan aging-time <30-65536>
surveillance-vlan cos	Set the class of service (0~7) for surveillance VLAN. <0-7>- Enter a number. Related Syntax: ● <config># surveillance-vlan cos <0-7> remark
surveillance-vlan oui-table	Enable OUI surveillance VLAN configuration for specified interface. <A:B:C> - Enter the OUI address (e.g., 00:50:12).

	<DESCRIPTION> - Enter a string to briefly explain the surveillance VLAN. Related Syntax: ● <config># surveillance-vlan oui-table <A:B:C> <DESCRIPTION>
surveillance-vlan vlan	Specify a VLAN profile as surveillance VLAN. <2-4094> - Specify the surveillance VLAN ID. Related Syntax: ● <config># surveillance-vlan vlan <2-4094>

Example

```
P1282# configure
P1282(config)#
P1282(config)#
P1282(config)# surveillance-vlan aging-time 60
P1282(config)#
P1282(config)# surveillance-vlan oui-table 00:50:12 fortestonly
P1282(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). Related Syntax: ● <config># system contact <CONTACT>
system location	<LOCATION> - Specify the location of the host. Related Syntax: ● <config># system location <LOCATION>
system name	<NAME> - Change the name of the system. The default name is “P1282”. Related Syntax: ● <config># system name <NAME>

Example

```
P1282# configure
P1282(config)#
P1282(config)# system contact callMIS
P1282(config)#
P1282(config)# system location DrayTek
```

```
P1282(config)# system name UPDATEFRIM
UPDATEFRIM(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. Related Syntax: ● <config># tr069 acsPwd<PASSWORD>
tr069 acsUsername	<NAME> - Enter the username used for registering to VigorACS server. Related Syntax: ● <config># tr069 acsUsername<NAME>
tr069 acsurl	<ADDRESS> - Enter the URL for VigorACS server. Related Syntax: ● <config># tr069 acsurl <ADDRESS>
tr069 cpeEnable	<disable/enable> - Enter Enable for VigorACS controlling such CPE through the Internet. Related Syntax: ● <config># tr069 cpeEnable <disable/enable>
tr069 cpePwd	<PASSWORD> - Enter the password that VigorACS server can

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

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

Example

```
P1282# configure
P1282(config)#
P1282(config)# tr069 stunaddr 192.168.3.99
P1282(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. secret - Set a user account with unencrypted password. secret encrypted - Set a user account with encrypted password. <WORD> - Enter the name (0~32 characters) of the local user profile. <admin/ user> - Specify the privilege level to be admin (privilege 15) / user (privilege 1). <PASSWORD> - Enter a string as the password for the local user. Related Syntax: ● <config># username <WORD> privilege <admin/user> secret <PASSWORD> ● <config># username <WORD> secret <PASSWORD>

	● <config># username <WORD> secret encrypted <PASSWORD>

Example

```
P1282# configure
P1282(config)#
P1282(config)# username carrie_1 privilege admin secret md123456
P1282(config)#
P1282(config)# username carrie_1 secret encrypted ca123456
Old password: ********
P1282(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:

```
P1282# configure
P1282(config)#
P1282(config)# vlan 3
P1282(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. <vlan-list> - The available range is 1 to 4094. <config># vlan 33 <config-vlan># Then, available sub-commands are: <config-vlan>#do <config-vlan>#end <config-vlan>#exit <config-vlan>#name
	Use the “do” command to run execution command in current mode. <SEQUENCE> - Related Syntax: ● <config-vlan>#do <SEQUENCE>
	Use the “end” command to finish current mode. Any changes in current mode will be saved. Related Syntax: ● <config-vlan>#end

	Use the “exit” command to close the current CLI session or return to the previous mode without saving the settings. Related Syntax: ● <config-macl>#exit
	Use the “name” command to add a VLAN profile. <string> - Enter the name of the VLAN profile. Related Syntax: ● <config-vlan>#name <string>
vlan mac-vlan group	Create a MAC-vlan group. <1-2147483647> - Specify a group ID. <A:B:C:D:E:F> - Enter the MAC address to be mapped. <9-48> - Enter a number representing the subnet mask. Related Syntax: ● <config># vlan mac-vlan group <1-2147483647> <A:B:C:D:E:F> mask <9-48>

Example

```
P1282# configure
P1282(config)# vlan 3
P1282(config-vlan)#
P1282(config-vlan)# name vlan_friends
P1282(config-vlan)#
…
P1282(config)# vlan mac-vlan group 33 00:50:17:22:12:ff mask 10
P1282(config)# vlan group 1 frame-type ethernet_ii protocol-value 0x0600
P1282(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. <30-65536> - The unit is minute. Default is 1440 (minutes). <string> - Enter the name of the VLAN profile. Related Syntax: ● <config># voice-vlan aging-time <30-65536>
voice-vlan cos	Set the voice VLAN cos value and remark function. Specify the class of service for voice VLAN.

	<0-7> - CoS value. Default is 6. Remark is disabled. remark – L2 user priority is remarked with the CoS value. Related Syntax: ● <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. <A:B:C> - Enter the OUI address. <DESCRIPTION> - Enter a brief description for the specified MAC address to the voice VLAN OUI table. Related Syntax: ● <config># voice-vlan cos <0-7> remark
voice-vlan vlan	Set the VLAN identifier of the voice VLAN. <2-4094> - Enter the number of VLAN ID. Related Syntax: ● <config># voice-vlan vlan <2-4094>

Example

```
P1282# configure
P1282(config)# voice-vlan aging-time 1000
P1282(config)#
P1282(config)# voice-vlan oui-table 22:30:ff test_01
P1282(config)#
P1282(config)# voice-vlan oui-table 00:01:E2 STAMP
P1282(config)# exit
P1282# 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
P1282#
```

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. Related Syntax: ● <config># webhook active <enable/disable>
webhook host	Specify the destination (URL, domain name, IP address) to receive the data transferred by VigorSwitch. ip <ADDRESS> - Enter the IP address of the destination. path <PATH> - Enter the path string (part of the composition of the URL) of the destination. port <number> - Enter a port number (1-65535). service <http/https> - Specify the protocol (http or https) of the destination. 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. Related Syntax: ● <config># webhook host ip <ADDRESS> ● <config># webhook host path <PATH> ● <config># webhook host port <number> ● <config># webhook host service <http/https> ● <config># webhook host url <domain name>
webhook interval	<1-60> - Set the transmission interval (unit is minute). Related Syntax: ● <config># webhook interval <1-60>
webhook keep	setings <enable/disable> - Enable or disable the function of keep webhook settings. Related Syntax: ● <config># webhook keep setings <enable/disable>

Example

```
P1282# configure
P1282(config)# webhook host service https
P1282(config)# webhook host url www.demo.com
```

```
P1282(config)# webhook host path Draytek/demo
P1282(config)# webhook host port 443
P1282(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: ● # copy flash:// flash:// ● # copy flash:// tftp://
copy startup-config	running-config - Copy the startup configuration file to the running configuration. tftp://- Copy the startup configuration file to remote TFTP server with a filename. <IP address> - Enter the IP address of TFTP sever. <filename> - Create a name to save the configuration file. Related Syntax: ● # copy startup-config tftp://
copy tftp://	running-config - Get the running configuration from specified TFTP server. startup-config - Get the startup configuration from specified TFTP server. Related Syntax: ● # copy tftp:// flash:// ● # copy tftp:// startup-config ● # copy tftp:// tftp://

Example

```
P1282# copy startup-config tftp://172.16.3.8/test_da.cfg
Uploading file. Please wait...
Save configuration done.
P1282#
```

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. Related Syntax: ● # delete flash://startup-config
delete startup-config	Restore the factory default settings of VigorSwitch. Related Syntax: ● # delete startup-config

Example

```
P1282# delet 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. Related Syntax: ● # disable <1-14>

Example

```
P1282# disable ?
<1-14>    Privilege level
<cr>
P1282# disable 3
P1282#
<1-14>    Privilege level
<cr>
P1282# disable 3
P1282#
```

A-2-7 End Configuration

Use this command to end current mode.

Syntax Items

end

Example

```
P1282(config)# interface GigabitEthernet 3
P1282(config-if)# end
P1282#
```

A-2-8 Exit Configuration

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

Syntax Items

exit

Example

```
P1282(config)# interface GigabitEthernet 3
P1282(config-if)# exit
P1282(config)#
```

A-2-9 Hardware-Monitor Configuration

Use this command to execute the hardware fan test.

Syntax Items

hardware-monitor fan-test

Example

```
P1282# hardware-monitor fan-test
P1282#
```

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. <1-999999999> - Specify the number of repetitions of ping operation.

	Related Syntax: ● # ping <HOSTNAME> ● # ping <HOSTNAME> count <1-999999999>

Example

```
P1282# 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
P1282#
```

A-2-11 Reboot Configuration

Use this command to perform a cold restart of VigorSwitch.

Syntax Items

reboot

Example

```
P1282# reboot
P1282#
```

A-2-12 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	<1-28> - Enter the number (1 to 28) of LAN port. <1-8> - Enter the number of LAG port. Related Syntax: ● # restore-defaults ● # restore-defaults interfaces GigabitEthernet <1-28> ● # restore-defaults interfaces LAG <1-8>

Example

```
P1282# restore-defaults interfaces gigabitethernet 3
Interface gi3: restore factory defaults.
P1282#
```

```
P1282# restore-default
System: restore factory defaults. Do you want to reboot now? (y/n)y
```

A-2-13 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

```
P1282# save
Success
P1282#
```

A-2-14 Show Configuration

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

Syntax Items

show <command>

Example

```
P1282# show acl utilization
Type: sys                                   usage: 256
Type: IPSG                                  usage: 128
Type: Auth                                  usage: 128
P1282#
P1282#
P1282# 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
P1282# 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
P1282#
```

A-2-15 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

```
P1282# 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
P1282#
```

A-2-16 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. Related Syntax: ● # terminal length <0-24>

Example

```
P1282# terminal length 15
P1282# show running-config
……
```

A-2-17 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. Related Syntax: ● # traceroute <HOSTNAME>

Example

```
P1282# 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
P1282#
```