VigorSwitch Q1100x Smart Lite Switch User's Guide

Version: 1.0

Firmware Version: V1.58.0

(For future update, please visit DrayTek web site)

Date: Nov 5, 2025

Copyrights

Trademarks

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows 10, 11 and Explorer are trademarks of Microsoft Corp.
- Apple and Mac OS are registered trademarks of Apple Inc.
- Other products may be trademarks or registered trademarks of their respective manufacturers.

Caution

Circuit devices are sensitive to static electricity, which can damage their delicate electronics. Dry weather conditions or walking across a carpeted floor may cause you to acquire a static electrical charge.

To protect your device, always:

- Touch the metal chassis of your computer to ground the static electrical charge before you pick up the circuit device.
- Pick up the device by holding it on the left and right edges only.

Warranty

We warrant to the original end user (purchaser) that the device will be free from any defects in workmanship or materials for a period of 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 routers will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents.

More update, please visit www.draytek.com.

Table of Contents

Part I Introduction

I-1 Introduction

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.

I-1-1 Key Features

Below shows key features of this device:

QoS

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

VLAN

Support 12 active VLANs and VLAN ID 1~4094.

Port Trunking

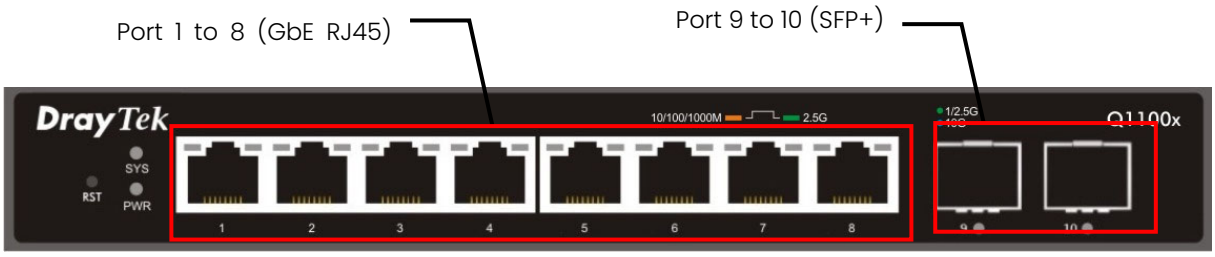
Allows one or more links to be aggregated together to form a Link Aggregation Group by the static setting.

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

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



LED	Status	Explanation
PWR/SYS	On (Green)	The switch finishes system booting and the system is ready.
	Blinking (Green)	The switch is powered on and starts system booting.
	Off	The power is off or the system is not ready / malfunctioning.
Port 1 ~ 8 (GbE RJ45)	On (Green)	The device is connected with 2.5Gbps.
	On (Amber)	The device is connected with 1G/100M/10Mbps.
	Blinking	The system is sending or receiving data through the port.
	Off	The port is disconnected or the link is failed.
Port 9 ~10 (SFP+)	On (Amber)	The device is connected with 2.5/1Gbps.
	On (Blue)	The device is connected with 10Gbps.
	Blinking	The system is sending or receiving data through the port.
	Off	The port is disconnected or the link is failed.

Interface	Description
RST	Factory reset button. Press it to reboot the system. (<5 seconds) Press it to reset the system with factory default settings. (>5 seconds)
Port 1 ~ 8 (2.5GbE RJ45)	Port 1 to Port 8 can be used for Ethernet connection.
Port 9 ~ 10 (SFP+)	Port 9 to Port 10 are used for fiber connection.

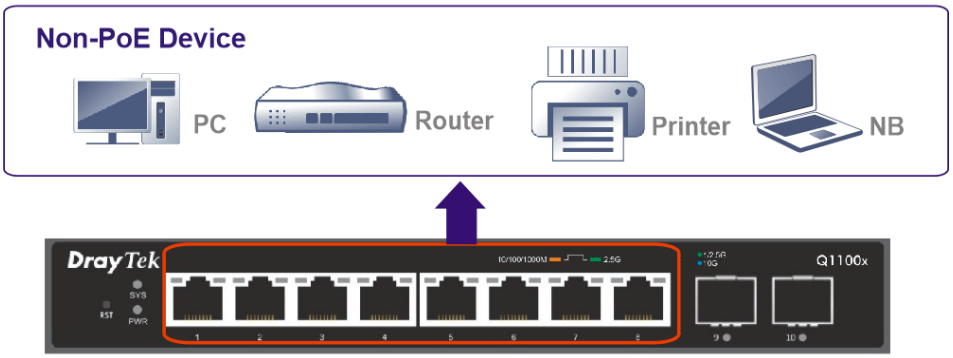
I-2 Installation

I-2-1 Network Connection

Allowance for connecting Non-PoE devices

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

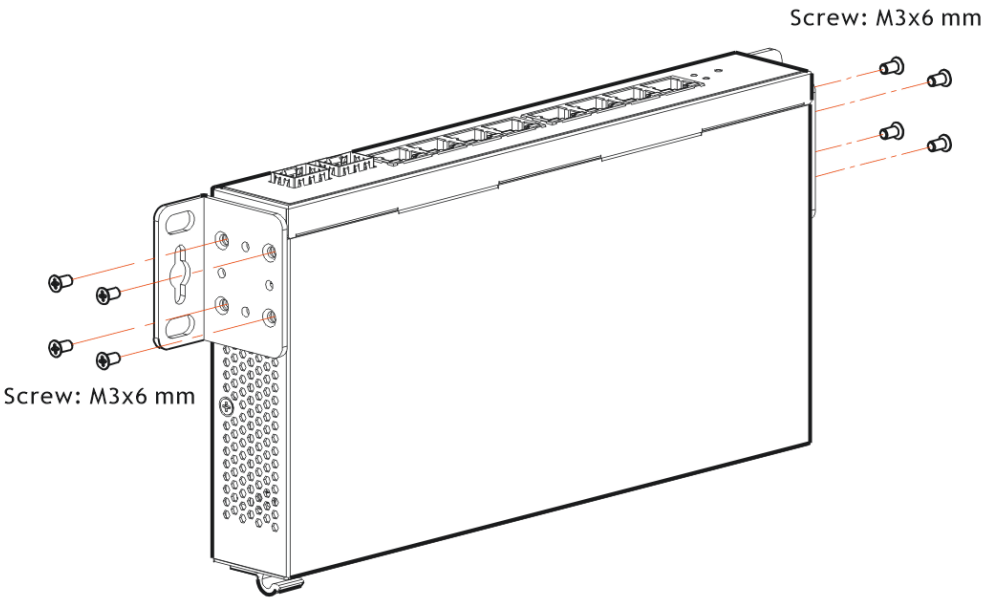
Here, we take VigorSwitch Q1100x as an example.

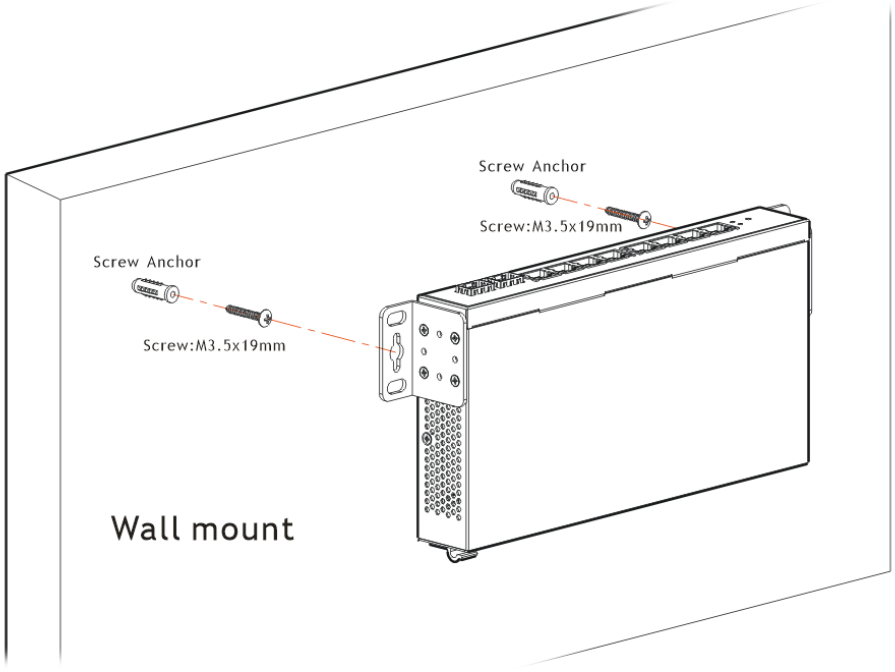


I-2-2 Wall-Mounted Installation

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

1. Attach both brackets to Vigor Switch with the fastening screws.
2. Refer to the following picture to find the recommended pairs of screw anchors and screws. Insert two anchors into the wall.
3. Lock the screws on the anchors.
4. Hang the device on the anchors





I-2-3 Typical Applications

The VigorSwitch implements 8 Gigabit Ethernet TP ports with auto MDIX and four slots for the removable module supporting comprehensive fiber types of connection, including LC and BiDi-LC SFP modules. The switch is suitable for the following applications:

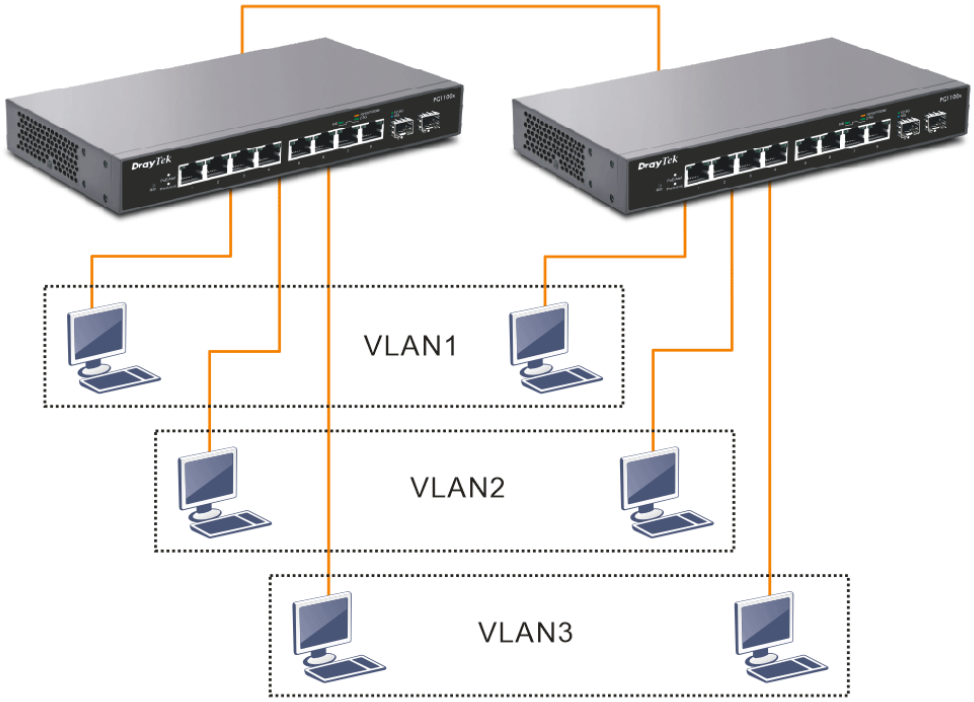
Case 1: All switch ports are in the same local area network.

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

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

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

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



Case 3: Desktop Installation

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

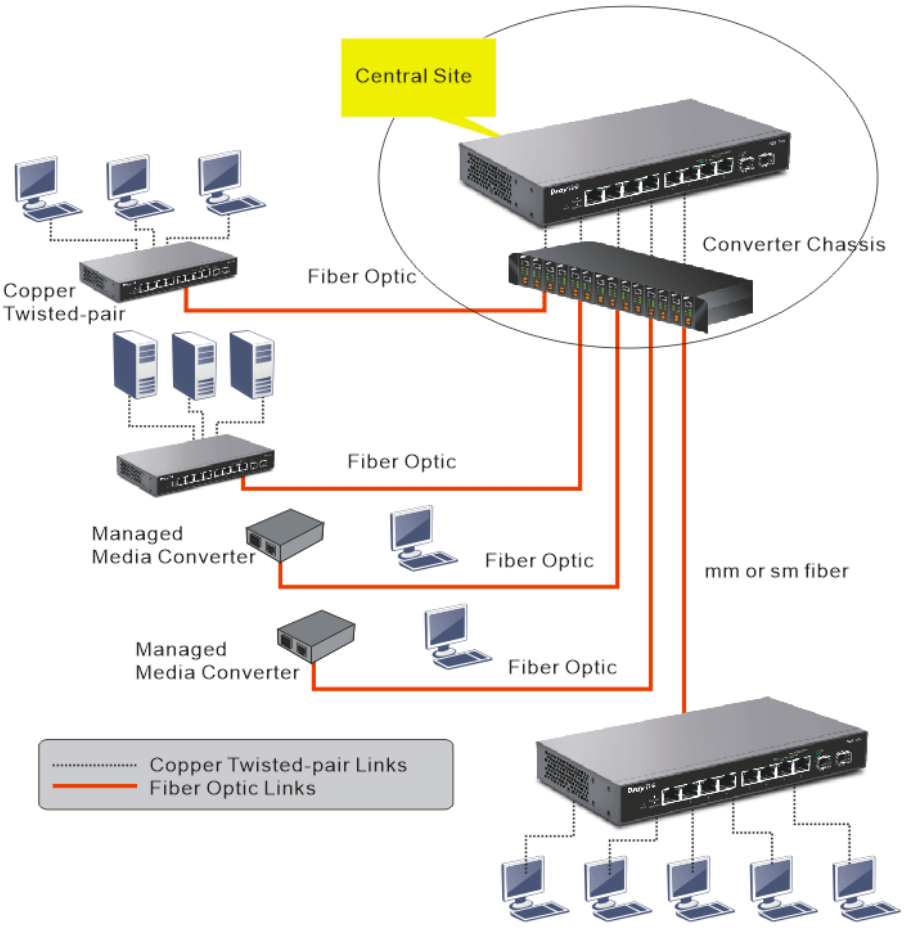
Case 4: Rack-mount Installation

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

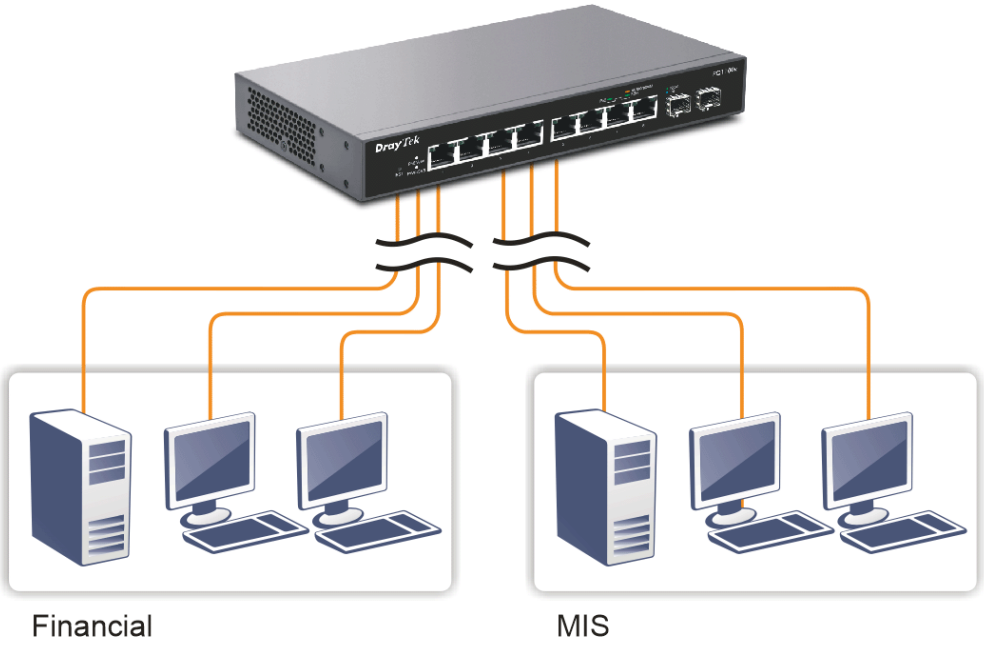
Procedures to Rack-mount the switch:

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

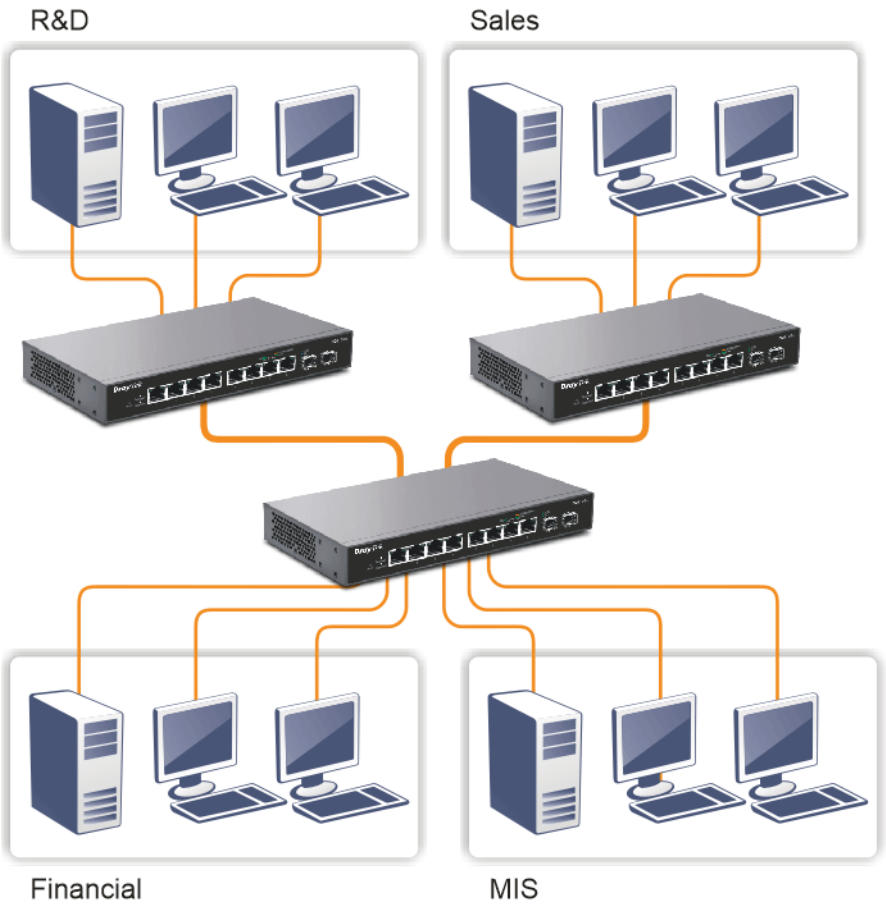
Case 5: Central Site/Remote site application is used in carrier or ISP



Case 6: Peer-to-peer application is used in two remote offices



Case 7: Office network



I-2-4 Installing Network Cables

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

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

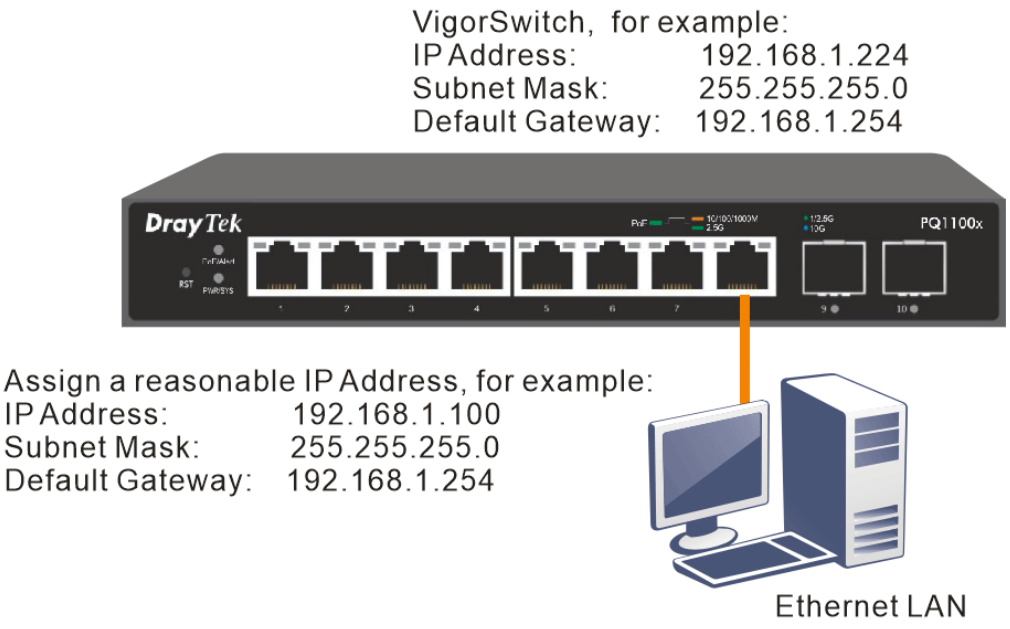
Media	Speed	Wiring
10/100/1000 Mbps copper	10 Mbps	Category 3,4,5 UTP/STP
	100Mbps	Category 5 UTP/STP
	1000 Mbps	Category 5e, 6 UTP/STP

I-2-5 Configuring the Management Agent of Switch

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

Configuring the Management Agent of VigorSwitch PQ1100x through the Ethernet Port.

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



I-2-6 Managing VigorSwitch Q1100x 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.

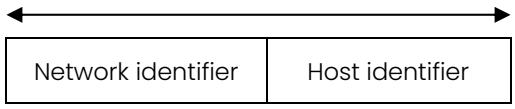
I-2-7 IP Address Assignment

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

IP address:

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

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

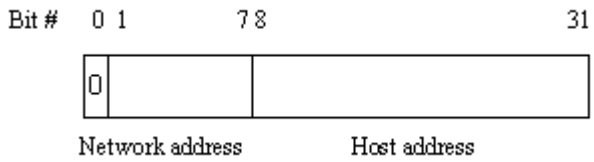


32 bits

With the classful addressing, it divides IP address into three classes, class A, class B and class C. The rest of IP addresses are for multicast and broadcast. The bit length of the network prefix is the same as that of the subnet mask and is denoted as IP address/X, for example, 192.168.1.0/24. Each class has its address range described below.

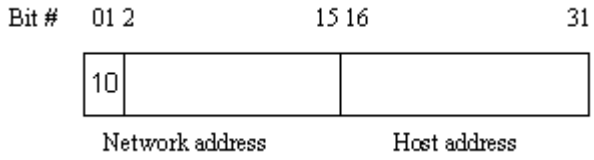
Class A:

Address is less than 126.255.255.255. There are a total of 126 networks can be defined because the address 0.0.0.0 is reserved for default route and 127.0.0.0/8 is reserved for loopback function.



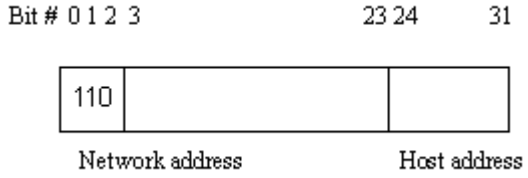
Class B:

IP address range between 128.0.0.0 and 191.255.255.255. Each class B network has a 16-bit network prefix followed 16-bit host address. There are 16,384 (2^14)/16 networks able to be defined with a maximum of 65534 (2^16 –2) hosts per network.



Class C:

IP address range between 192.0.0.0 and 223.255.255.255. Each class C network has a 24-bit network prefix followed 8-bit host address. There are 2,097,152 (2^21)/24 networks able to be defined with a maximum of 254 (2^8 –2) hosts per network.



Class D and E:

Class D is a class with first 4 MSB (Most significance bit) set to 1-1-1-0 and is used for IP Multicast. See also RFC 1112. Class E is a class with first 4 MSB set to 1-1-1-1 and is used for IP broadcast.

According to IANA (Internet Assigned Numbers Authority), there are three specific IP address blocks reserved and able to be used for extending internal network. We call it Private IP address and list below:

Class A	10.0.0.0 --- 10.255.255.255
Class B	172.16.0.0 --- 172.31.255.255
Class C	192.168.0.0 --- 192.168.255.255

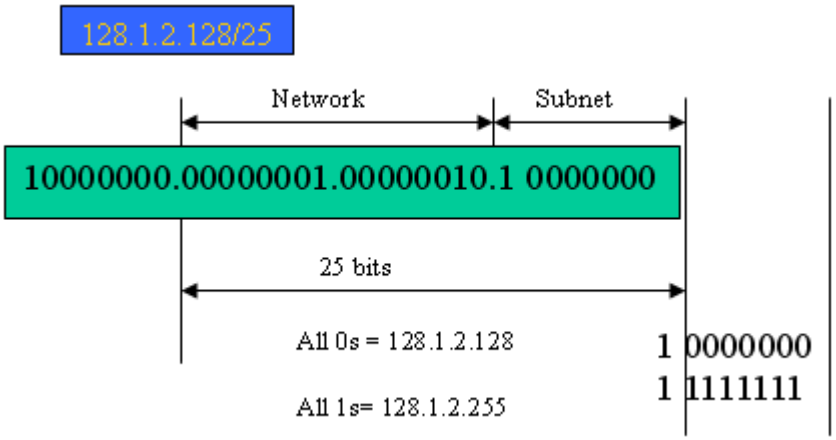
Please refer to RFC 1597 and RFC 1466 for more information.

Subnet mask:

It means the sub-division of a class-based network or a CIDR block. The subnet is used to determine how to split an IP address to the network prefix and the host address in bitwise basis. It is designed to utilize IP address more efficiently and ease to manage IP network.

For a class B network, 128.1.2.3, it may have a subnet mask 255.255.0.0 in default, in which the first two bytes is with all 1s. This means more than 60 thousands of nodes in flat IP address will be at the same network. It's too large to manage practically. Now if we divide it into smaller network by extending network prefix from 16 bits to, say 24 bits, that's using its third byte to subnet this class B network. Now it has a subnet mask 255.255.255.0, in which each bit of the first three bytes is 1. It's now clear that the first two bytes is used to identify the class B network, the third byte is used to identify the subnet within this class B network and, of course, the last byte is the host number.

Not all IP address is available in the sub-netted network. Two special addresses are reserved. They are the addresses with all zero's and all one's host number. For example, an IP address 128.1.2.128, what IP address reserved will be looked like? All 0s mean the network itself, and all 1s mean IP broadcast.



In this diagram, you can see the subnet mask with 25-bit long, 255.255.255.128, contains 126 members in the sub-netted network. Another is that the length of network prefix equals the number of the bit with 1s in that subnet mask. With this, you can easily count the number of IP addresses matched. The following table shows the result.

Prefix Length	No. of IP matched	No. of Addressable IP
/32	1	-
/31	2	-
/30	4	2
/29	8	6
/28	16	14
/27	32	30
/26	64	62
/25	128	126
/24	256	254
/23	512	510
/22	1024	1022
/21	2048	2046
/20	4096	4094
/19	8192	8190
/18	16384	16382
/17	32768	32766
/16	65536	65534

According to the scheme above, a subnet mask 255.255.255.0 will partition a network with the class C. It means there will have a maximum of 254 effective nodes existed in this sub-netted network and is considered a physical network in an autonomous network. So it owns a network IP address which may looks like 168.1.2.0.

With the subnet mask, a bigger network can be cut into small pieces of network. If we want to have more than two independent networks in a worknet, a partition to the network must be performed. In this case, subnet mask must be applied.

For different network applications, the subnet mask may look like 255.255.255.240. This means it is a small network accommodating a maximum of 15 nodes in the network.

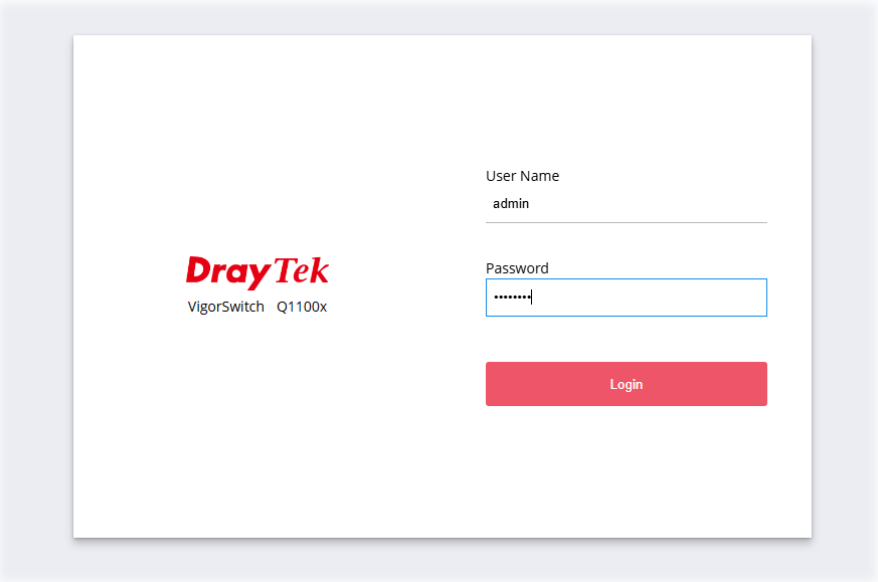
For assigning an IP address to the switch, you just have to check what the IP address of the network will be connected with the switch. Use the same network address and append your host address to it.

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

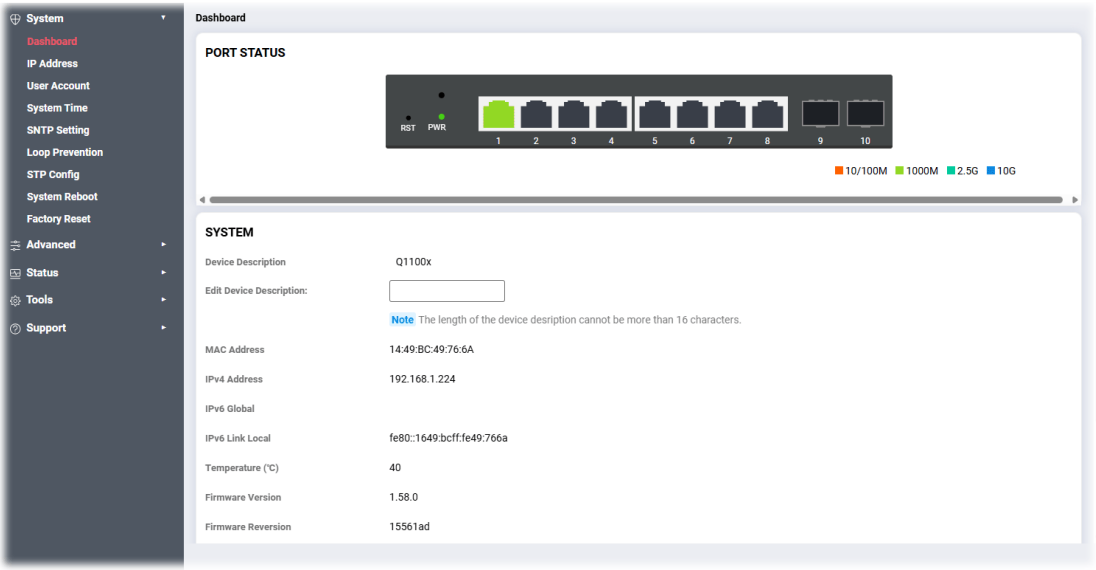
Note: The DHCP Setting is enabled in default. Therefore, if a DHCP server presented on network connected to the switch, check before accessing your switch is essential.

I-3 Accessing Web Page of VigorSwitch

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



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

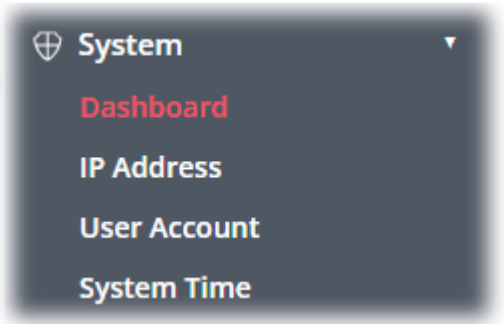


Info

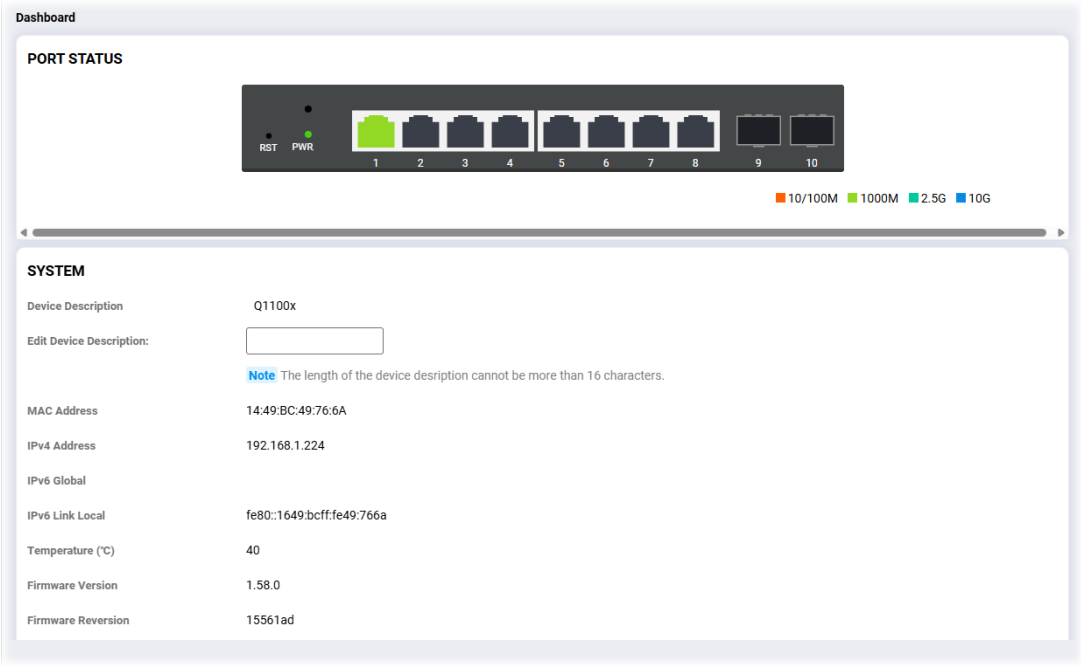
The DHCP Setting is enabled in default. Therefore, if a DHCP server presented on network connected to VigorSwitch, checking before accessing VigorSwitch is essential.

I-4 Dashboard

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



A web page with PORT STATUS and SYSTEM information will be displayed on the screen. Refer to the following figure:

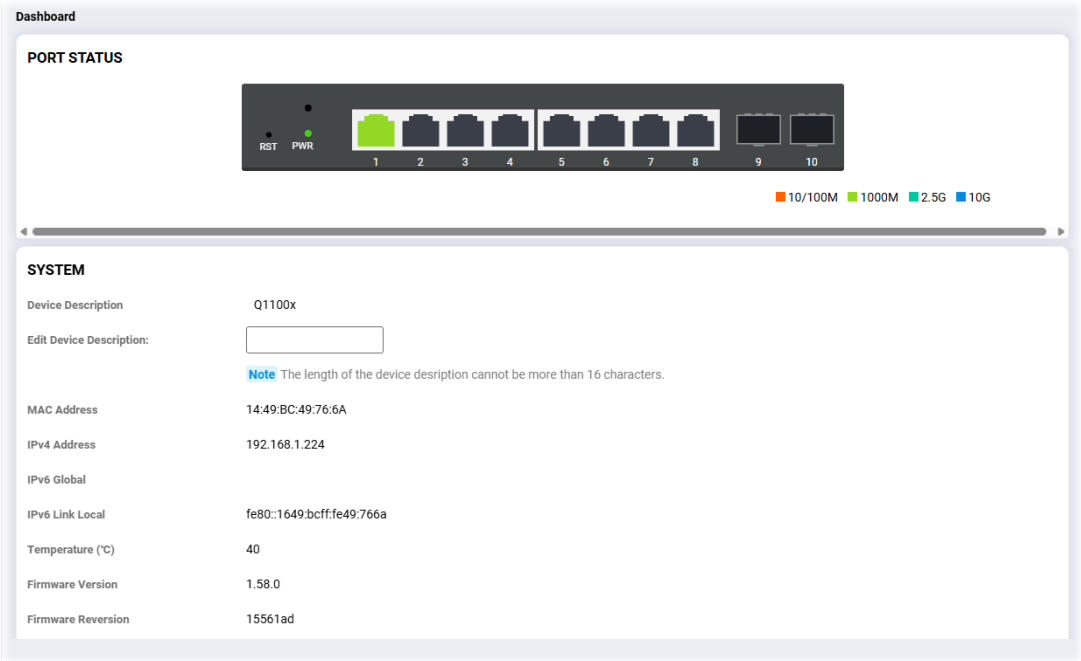


This page is left blank.

Part II System

II-1 Dashboard - System

This page displays general information (such as device name, MAC address, IP address, temperature, firmware version, system time, and uptime) for this device.



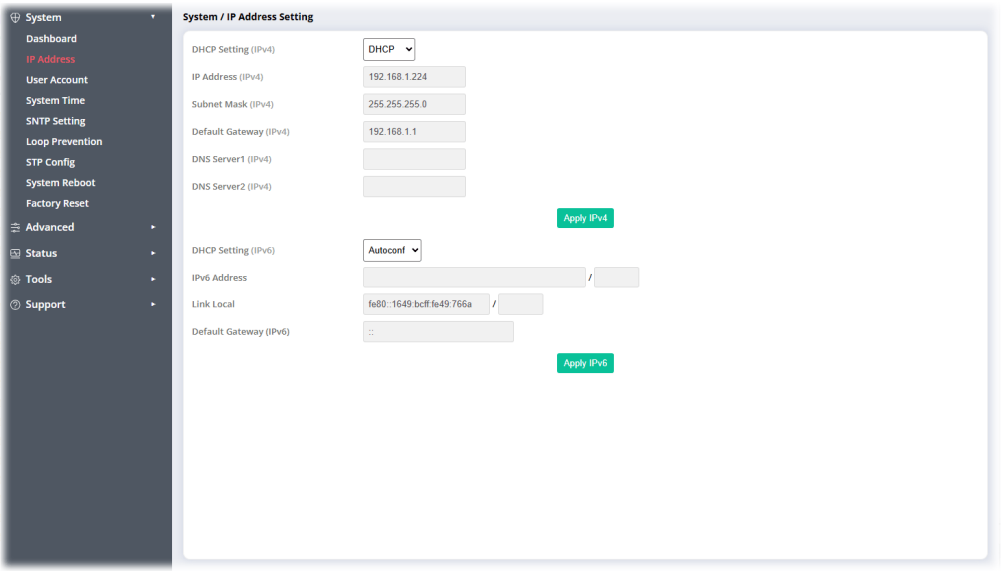
Available settings are explained as follows:

Item	Description
Edit Device Description	Enter a brief explanation (less than 16 characters) for this device.
Apply	Apply the settings to the switch.

II-2 IP Address

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 IPv6 Address (IPv4/IPv6) screen to configure the switch IPv6 address and the default gateway device. The gateway field specifies the IPv6 address of the gateway (next hop) for outgoing traffic.



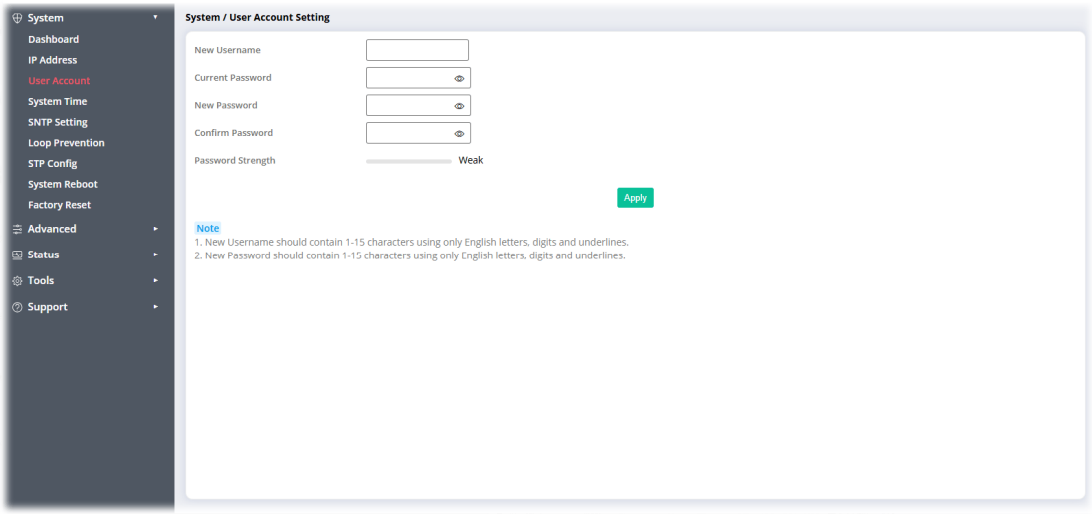
Available settings are explained as follows:

Item	Description
DHCP Setting (IPv4)	Select the mode of network connection. **Manual** - Use static IPv4 address. **DHCP** – Use DHCP provisioned IP address and Gateway if feasible.
IP Address (IPv4)	It is available when **Manual** is selected as **DHCP Setting**. 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 (IPv4)	It is available when **Manual** is selected as **DHCP Setting**. 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.
Default Gateway (IPv4)	It is available when **Manual** is selected as **DHCP Setting**. Enter the IP address of the gateway in dotted decimal notation. If static mode is enabled, enter gateway address in this field.
DNS Server 1/2 (IPv4)	It is available when **Manual** is selected as **DHCP Setting**. If static mode is enabled, enter primary DNS server / secondary DNS server address in this field.
Apply IPv4	Apply the settings to the switch.

DHCP Setting (IPv6)	**Autoconf** - Let switch automatically configure IPv6 address. **DHCP** – Select this feature if there is a DHCPv6 server on your network for assigning IPv6 Address. **Manaul** – Select this feature to enter the IPv6 address and set the default gateway(IPv6) manually.
IPv6 Address	It is available when **Manual** is selected for DHCP Setting. Enter the IPv6 address of your switch. If auto configuration mode is disabled, enter IPv6 address in this field.
Link Local	Display link local address.
Default Gateway (IPv6)	It is available when **Manual** is selected for DHCP Setting. Enter the IPv6 address of the router as your default IPv6 gateway to access IPv6 Internet or other IPv6 network.
Apply IPv6	Apply the settings to the switch.

II-3 User Account

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

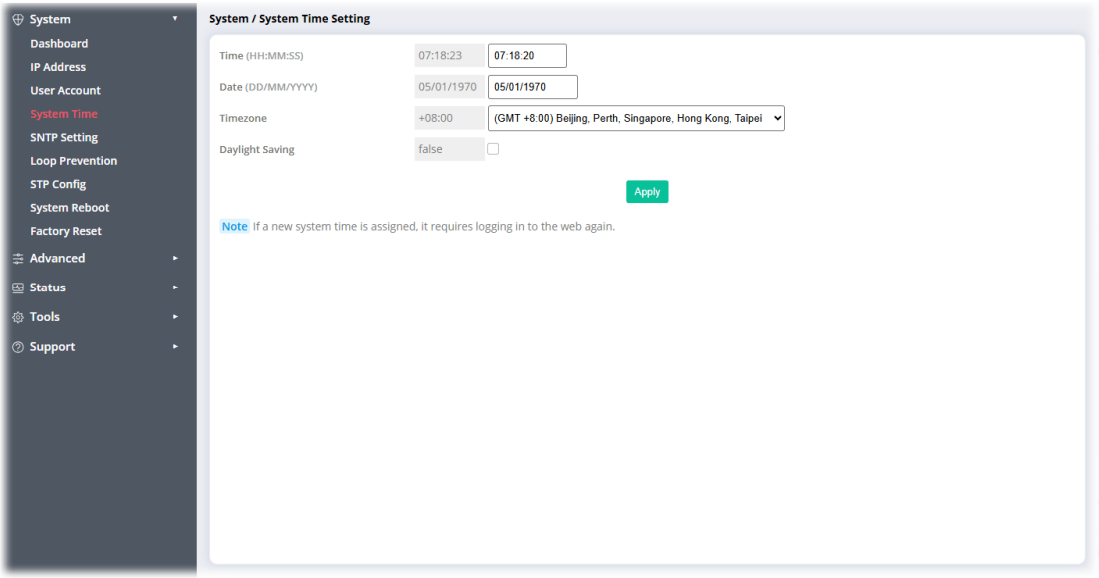


Available settings are explained as follows:

Item	Description
New Username	Enter the user name. 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.
Current Password	Enter the current password. The factory default is “admin”.
New Password	Enter the new password. The maximum length of the password is 15 characters.
Confirm Password	Enter the new password again for confirmation.
Password Strength	The system will display the strength of the password, indicated by the words “weak”, “medium” or “strong”.
Apply	Apply the settings to the switch.

II-4 System Time

This page allows users to specify the date and time for VigorSwitch.

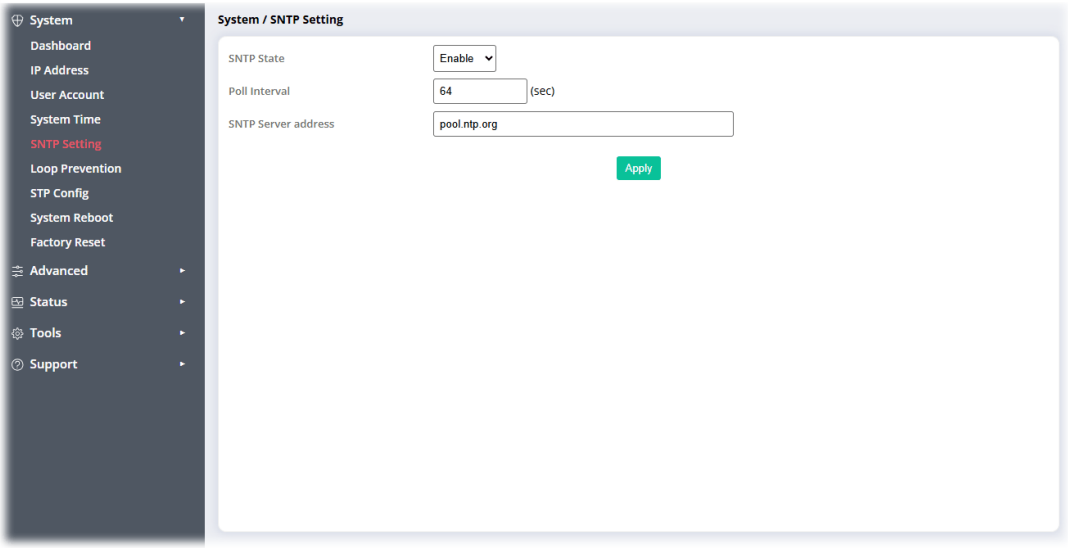


Available settings are explained as follows:

Item	Description
Time	Enter the time with the format of "HH:MM:SS".
Date	Enter the date with the format of "DD/MM/YY".
Time Zone	Select a time zone that VigorSwitch is located from the drop down list.
Daylight Saving	Check the box to enable daylight saving time.
Apply	Apply the settings to the switch.

II-5 SNTP Setting

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

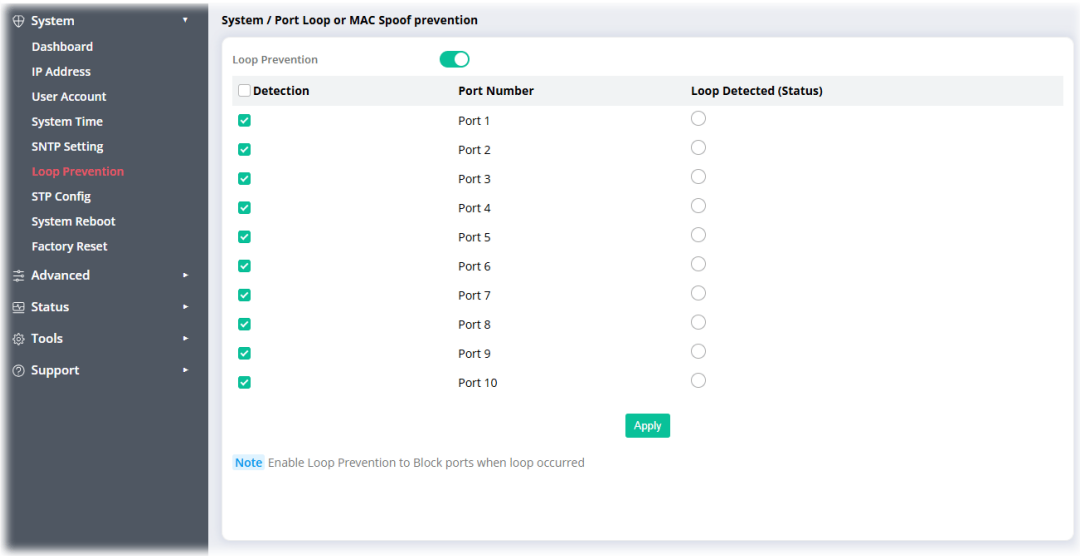


Available settings are explained as follows:

Item	Description
SNTP State	**Enable** – Click it to enable SNTP time server. **Disable** – Click to disable the time server.
Poll Interval	Set a time interval for regularly checking for changes.
SNTP Server address	Enter the web site of the time server or the IP address of the server.
Apply	Apply the settings to the switch.

II-6 Loop Prevention

Loop Prevention is a feature that enables the switch to automatically disable a LAN port when it detects a network loop. Once the loop is resolved, the LAN port will be reactivated and become operational again. To disable this feature, select "Off."

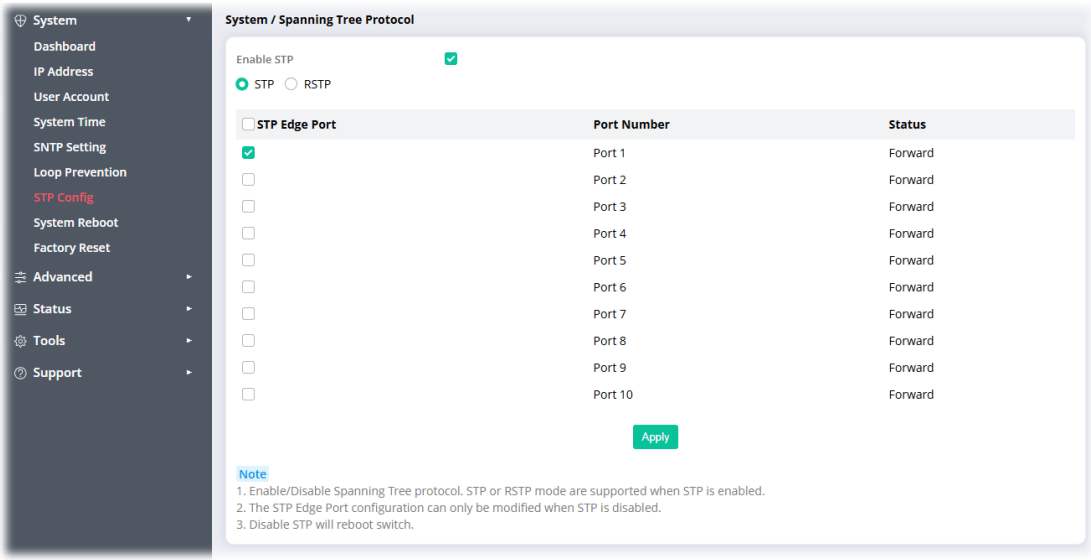


Available settings are explained as follows:

Item	Description
Detection	Check the box to enable loop prevention on the selected LAN port. By default, this box is disabled.
Port Number	Display all LAN port numbers.
Loop Detected (Status)	A red circle will appear in this field when a loop is detected.
Apply	Apply the settings to the switch.

II-7 STP Config

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

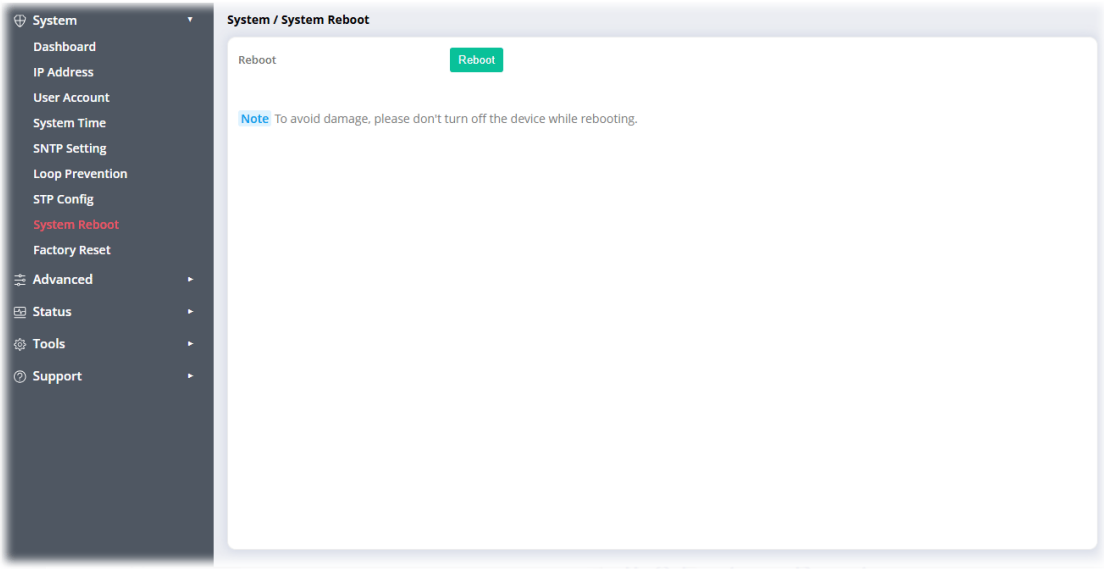


Available settings are explained as follows:

Item	Description
Enable STP	Check the box to enable the STP feature settings. ● STP - Enable the Spanning Tree (STP) operation. ● RSTP - Enable the Rapid Spanning Tree (RSTP) operation.
STP Edge Port	An optimized setting for STP, useful for edge devices. When the LAN port is connected to a non-switch device, such as a computer, printer, or server, the STP Edge Port option can be selected for that LAN port. This allows the port to enter Forwarding status, which enhances the activation speed of the LAN connection.
Port Number	Display all LAN port numbers.
Status	Display current status (Forward or Blocking) of each LAN port.
Apply	Click here to make the STP Edge Port to enter Forwarding status directly.

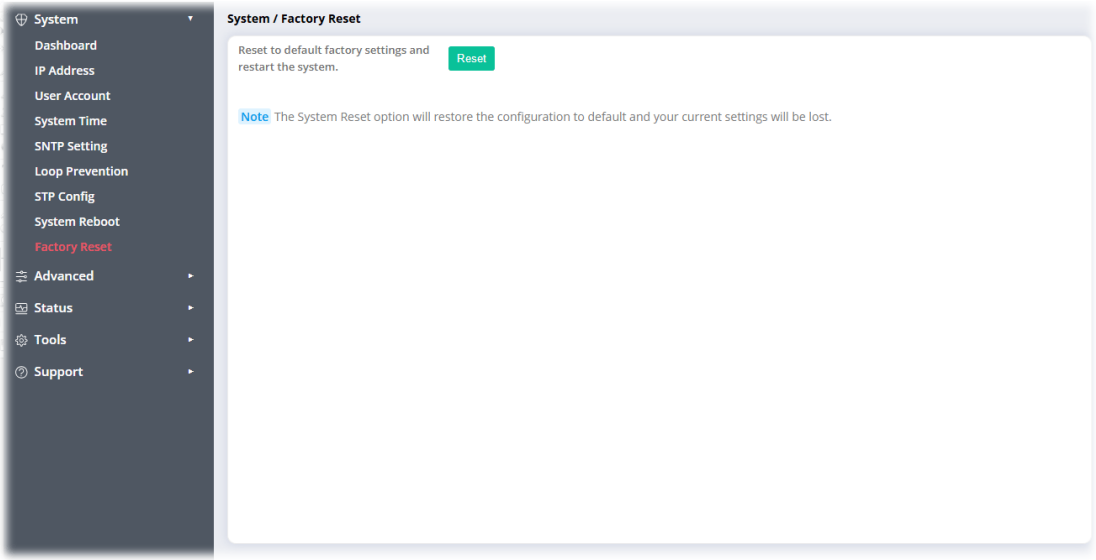
II-8 System Reboot

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



II-9 Factory Reset

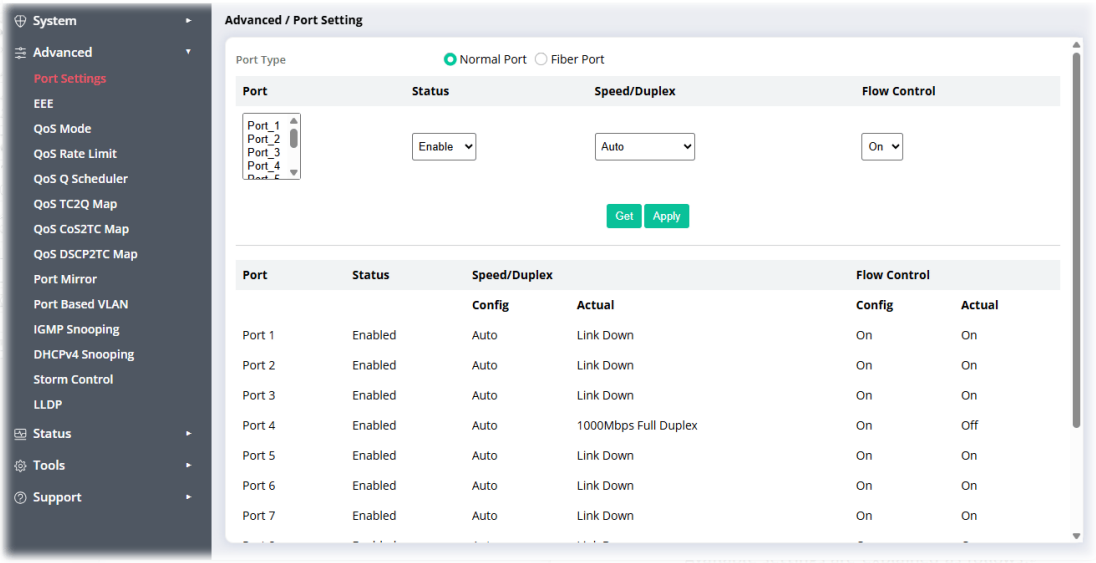
Click **Reset** to return to factory default settings for VigorSwitch.



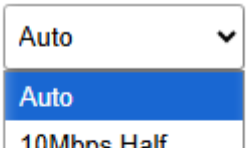
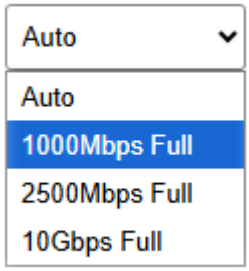
Part III Advanced

III-1 Port Setting

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



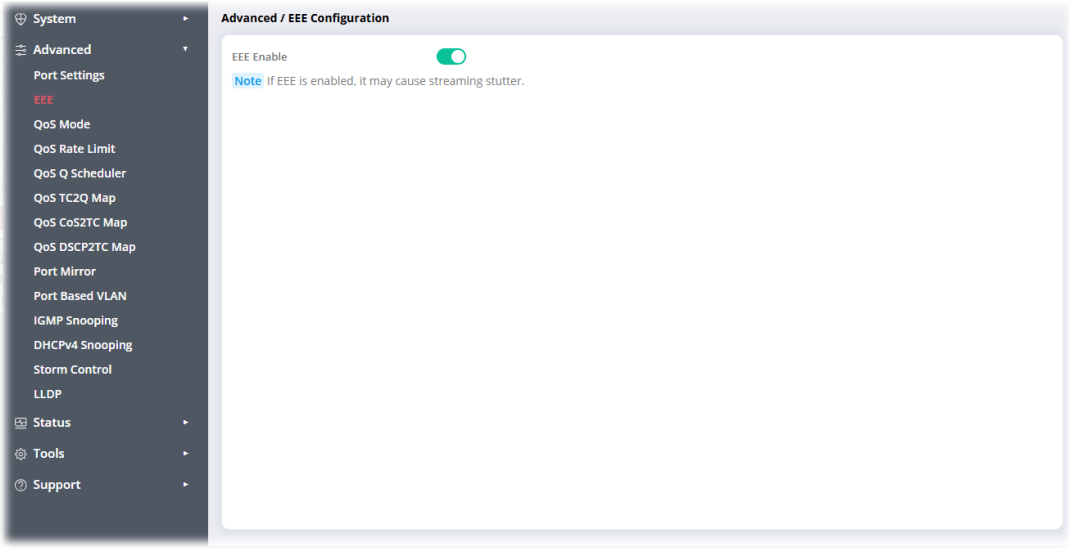
Available settings are explained as follows:

Item	Description
Port Type	**Normal Port –** Select this to display the Ethernet ports (Port_1 to Port_8). **Fiber Port –** Select this to display the fiber ports (Port_9 to Port_10).
Port	Use the drop down list to select one or more LAN port(s).
Status	**Enable –**Click it to enable the port. **Disable –** Click it to disable the port.
Speed/Duplex   	Port speed capabilities for Normal Port: ● **Auto:** Auto speed with all capabilities. ● **10Mbps Half** – 10 Mbit/s Ethernet half duplex. ● **10Mbps Full**– 10 Mbit/s Ethernet full duplex. ● **100Mbps Half**– 100 Mbit/s Fast Ethernet full duplex. ● **100Mbps Full** – 100 Mbit/s Fast Ethernet half duplex. ● **1000Mbps Full** – 1 Gbit/s Gigabit Ethernet full duplex. ● **2500Mbps Full** – 2.5 Gbit/s Gigabit Ethernet full duplex. Port speed capabilities for Fiber Port: ● **Auto:** Auto speed with all capabilities. ● **1000Mbps Full** – 1 Gbit/s Gigabit Ethernet full duplex. ● **2500Mbps Full** – 2.5 Gbit/s Gigabit Ethernet full duplex. ● **10Gbps Full** – 10 Gbit/s Gigabit Ethernet full duplex. Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the switch negotiates

	with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect. For SFP fiber module, you might need to manually configure the speed to match fiber module speed.
Flow Control	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port. The switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. On – Click it to enable such function. Off – Click it to disable such function.
Get	Refresh the page to display current settings.
Apply	Apply the settings to the switch.

III-2 EEE

Enable or disable port EEE (Energy Efficient Ethernet) function for all selected ports.

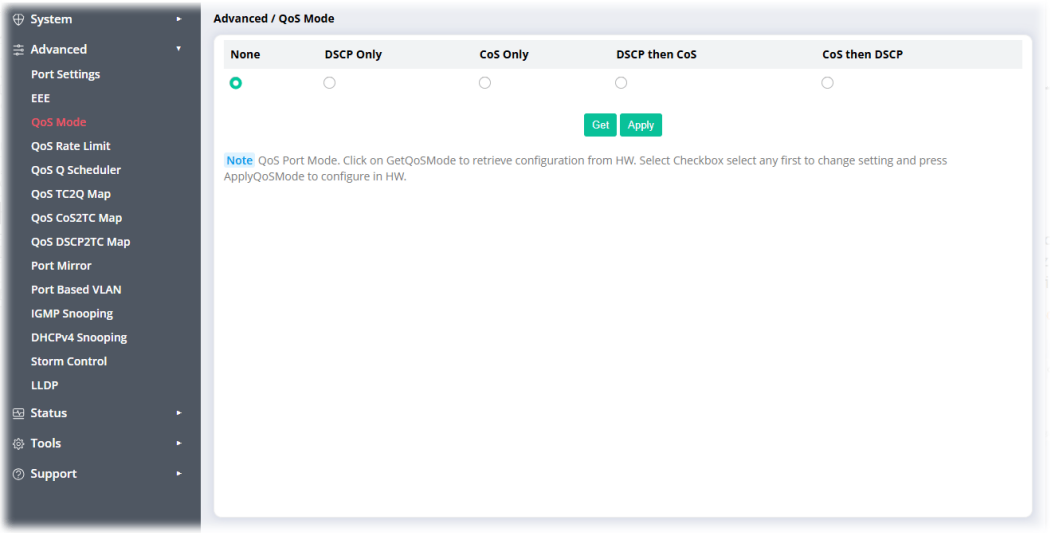


III-3 QoS Mode

The switch offers powerful QoS function.

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.

This page is to select the QoS operation mode.



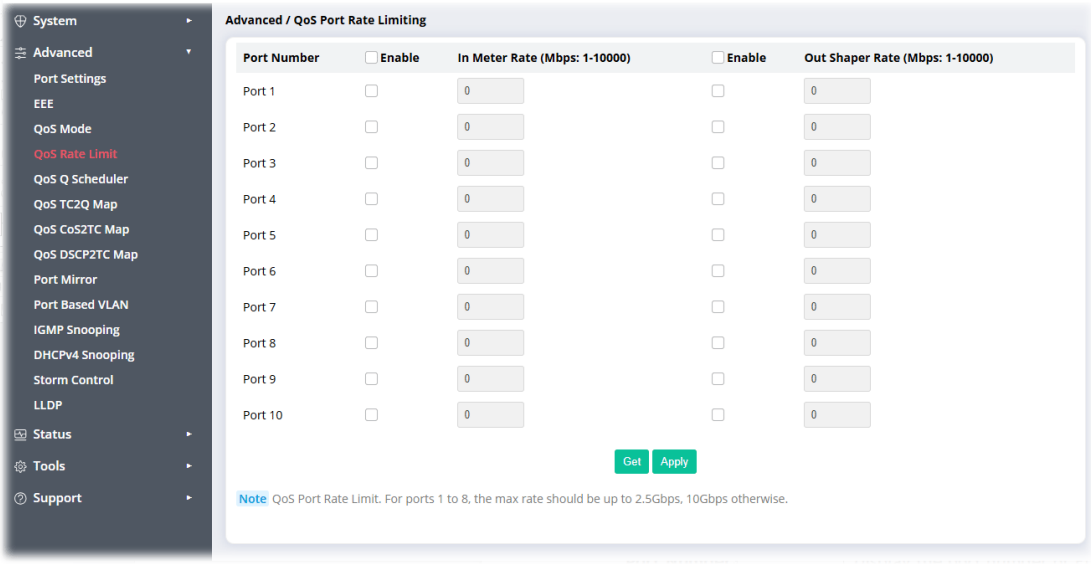
Available settings are explained as follows:

Item	Description
None	Disable this function.
DSCP Only	Select to apply the DSCP remarking only. It allows user to configure how ingress packets with DSCP tag map to QoS queues, and QoS queues to DSCP on egress packets. 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 Only	Select to apply the cos remarking only. 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. 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 then CoS	All IP traffic is mapped to queues based on the DSCP field in the IP header, and then based on the per-port default CoS value if there is no VLAN tag on the incoming packet.
CoS then DSCP	All IP traffic is mapped to queues based on the CoS field in the VLAN tag, and then based on the DSCP field in the IP header.
Get	Apply the settings to the switch without saving the change.
Apply	Apply the settings to the switch and save the change.

III-4 QoS Rate Limit

This page allows the user to configure the rate limit for QoS.

In Meter Rate and **Out Shaper Rate** settings are used to set up the limit of ingress or egress bandwidth for each port.

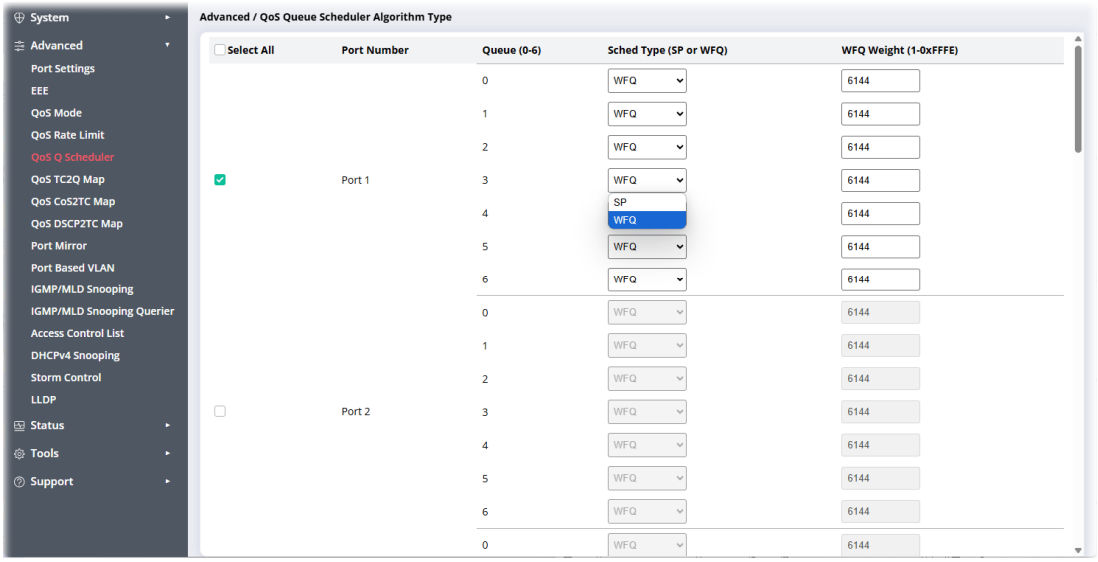


Available settings are explained as follows:

Item	Description
Port Number	Display the port number of Ethernet or Fiber ports.
Enable	Select to enable the In Meter Rate for each port.
In Meter Rate (Mbps:1-10000)	Set up the limit of ingress bandwidth for the port you choose. Incoming traffic will be discarded if the rate exceeds the value you set up in Data Rate field. Pause frames are also generated if flow control is enabled. The format of the packet limits to unicast, broadcast and multicast.
Enable	Select to enable the In Out Shaper Rate for each port.
Out Shaper Rate (Mbps:1-10000)	Set up the limit of egress bandwidth for the port you choose. Outgoing traffic will be discarded if the rate exceeds the value you set up in Data Rate field.
Get	Apply the settings to the switch without saving the change.
Apply	Apply the settings to the switch and save the change.

III-5 QoS Q Scheduler

This page offers settings for configuring QoS Queue Scheduling Type. It is used to determine the processing order for the data packets.



Available settings are explained as follows:

Item	Description
Select All	Check to select all the port numbers.
Port Number	Display the port number of Ethernet or Fiber ports.
Queue (0-6)	Display the priority number of the queue which will be effective only when SP is selected as Sched Type.
Sched Type (SP or WFQ)	Select the scheduleing type. **SP** – Strict Priority. Select this type to process the packets based on the queue priority. **WFQ** - Weighted Fair Queuing. Select this type to allocate the bandwidth for each queue fairly according to the weight value.
WFQ Weight (1-0xFFFE)	It is effective only when **WFQ** is selected as Sched Type. Set the weight for each queue of each port.
Get	Apply the settings to the switch without saving the change.
Apply	Apply the settings to the switch and save the change.

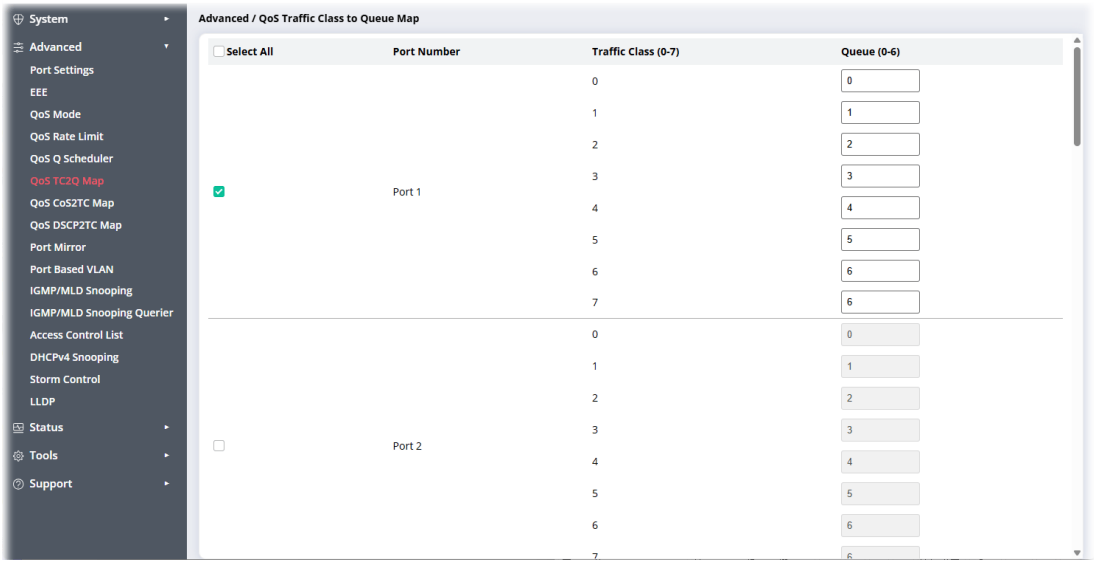
III-6 QoS TC2Q Map

There are three traffic managing methods:

- Traffic Class(TC) to Queue
- Class of Service(CoS) to Traffic Class
- Differentiated Services Code Point (DSCP) to Traffic Class (TC)

In which, CoS and DSCP are used to mark the priority of the packets via VLAN / IP header.

Therefore, it is essential to prioritize packet transmission by mapping CoS or DSCP values to different queues.



Available settings are explained as follows:

Item	Description
Select All	There are seven profiles offered for Ethernet LAN ports and Fiber ports. Click to select all profiles.
Port Number	Ports 1 to 7 are designated as network interfaces. Ports 1 through 5 support standard Ethernet LAN connections, while Ports 6 and 7 are reserved for fiber optic connectivity.
Traffic Class (0-7)	Numbers from 0 to 7 represent different priority levels. The higher the number, the higher the priority. Packets are processed and transmitted according to their priority level.
Queue (0-6)	Numbers from 0 to 6 represent the order of the packets to be processed.
Get	Apply the settings to the switch without saving the change.
Apply	Apply the settings to the switch and save the change.

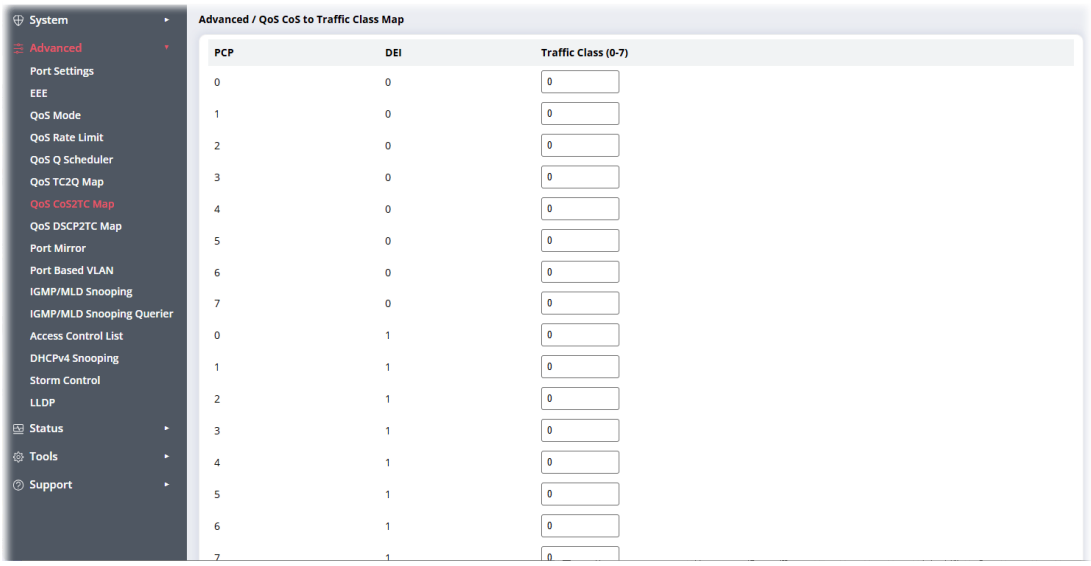
III-7 QoS CoS2TC Map

There are three traffic managing methods:

- Traffic Class(TC) to Queue
- Class of Service(CoS) to Traffic Class
- Differentiated Services Code Point (DSCP) to Traffic Class (TC)

In which, CoS and DSCP are used to mark the priority of the packets via VLAN / IP header.

This page defines the priority of packet transmission by mapping CoS values to Traffic Class (TC) values.



Available settings are explained as follows:

Item	Description
PCP	It is an abbreviation of Priority Code Point. The numbers 0 (lowest) to 7 (highest) generally represent different priority levels for various types of traffic, including general (0), video (4), voice (5), and network control (7).
DEI	It is an abbreviation of Drop Eligible Indicator. In this context, 0 indicates that the traffic is very important and should not be discarded. 1 indicates that the traffic can be discarded or removed in case of a traffic jam.
Traffic Class (0-7)	Numbers from 0 to 7 represent different priority levels. The higher the number, the higher the priority. Packets are processed and transmitted according to their priority level.
Get	Apply the settings to the switch without saving the change.
Apply	Apply the settings to the switch and save the change.

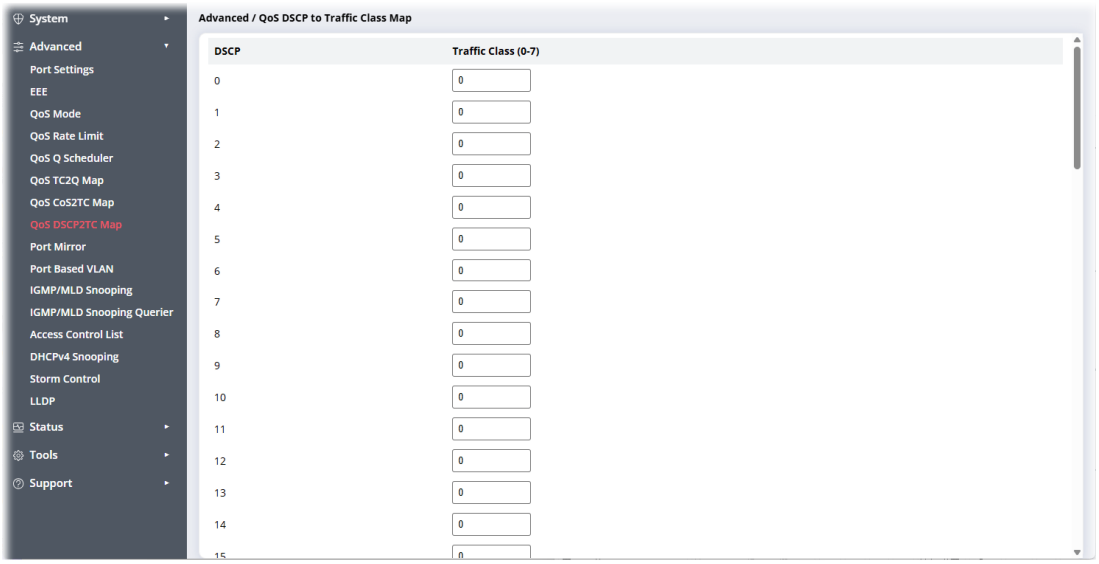
III-8 QoS DSCP2TC Map

There are three traffic managing methods:

- Traffic Class(TC) to Queue
- Class of Service(CoS) to Traffic Class
- Differentiated Services Code Point (DSCP) to Traffic Class (TC)

In which, CoS and DSCP are used to mark the priority of the packets via VLAN / IP header.

This page defines the priority of packet transmission by mapping DSCP values to Traffic Class (TC) values.

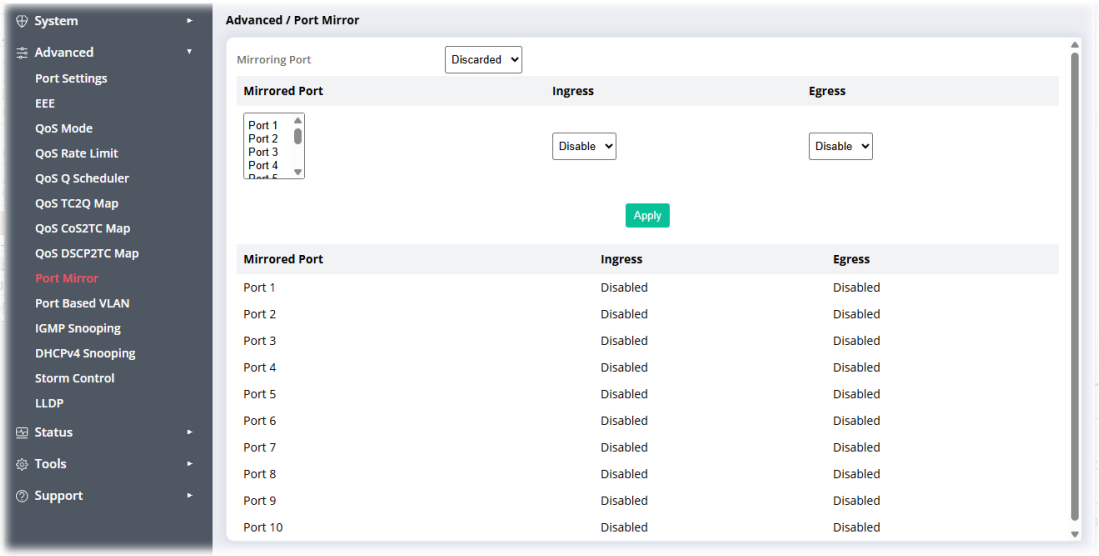


Available settings are explained as follows:

Item	Description
DSCP (0-63)	It is a marker in the header of network packets used to indicate the priority level for quality of service (QoS). 0 to 64 represents different QoS.
Traffic Class (0-7)	Numbers from 0 to 7 represent different priority levels. The higher the number, the higher the priority. Packets are processed and transmitted according to their priority level.
Get	Apply the settings to the switch without saving the change.
Apply	Apply the settings to the switch and save the change.

III-9 Port Mirror

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



Available settings are explained as follows:

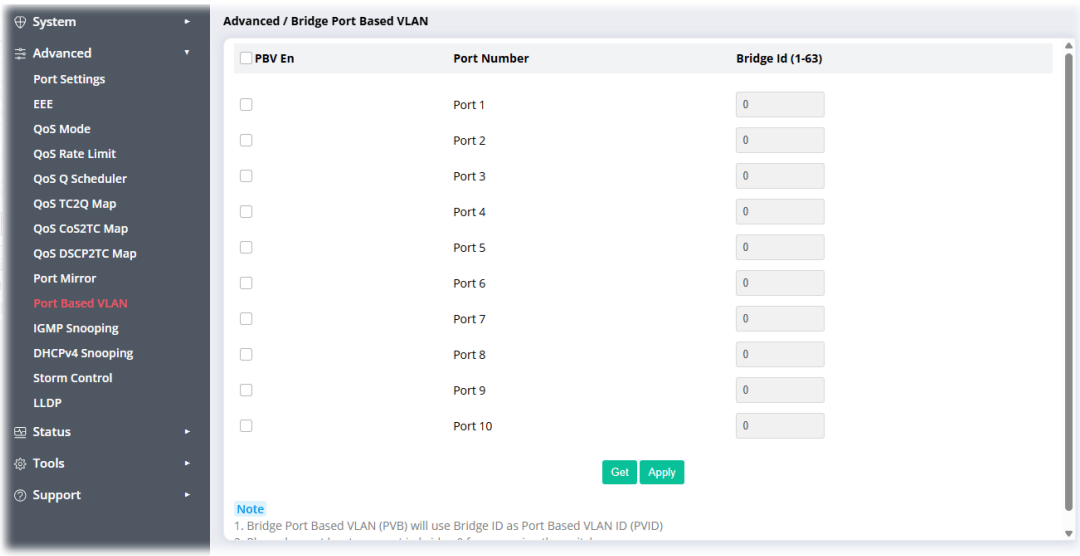
Item	Description
Mirroring Port	Discarded, Port 1 to Port 10. One and only one port is selected as the mirror port, to which traffic is to be forwarded.
Mirrored Port	Port(s) whose outbound or inbound traffic will be forwarded to the mirror port.
Ingress	Enable – If selected, the inbound traffic (receiving) will be forward to the mirror port.
Egress	Enable – If selected, the outbound traffic (transmissing) will be forward to the mirror port.
Apply	Save the settings.

III-10 Port Based VLAN

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.

Port-based VLAN is defined by port. Any packet coming in or outgoing from any one port of a port-based VLAN will be accepted.

This page allow user to configure port VLAN settings.



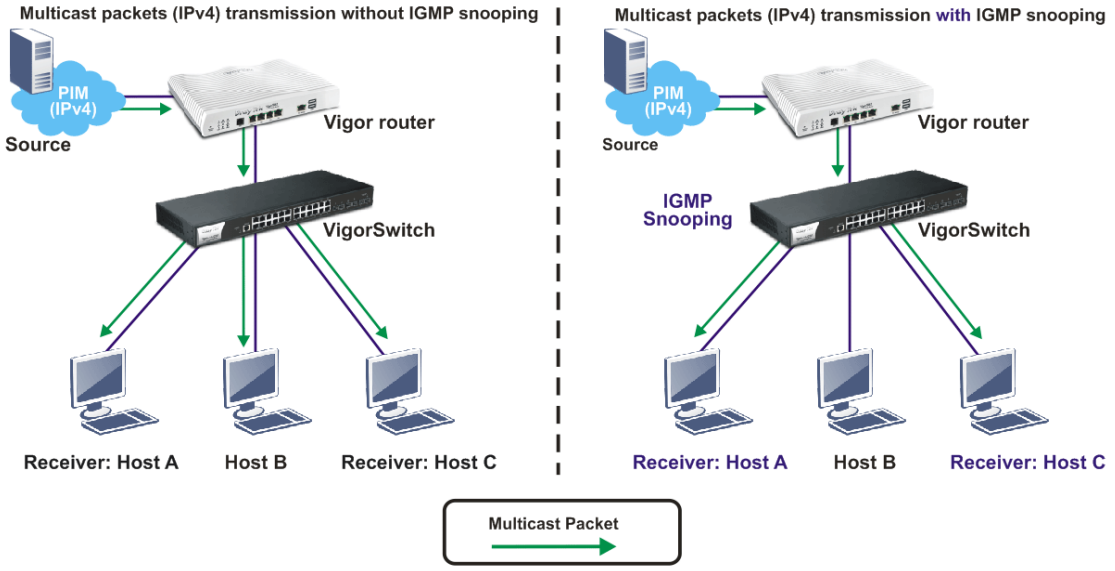
Available settings are explained as follows:

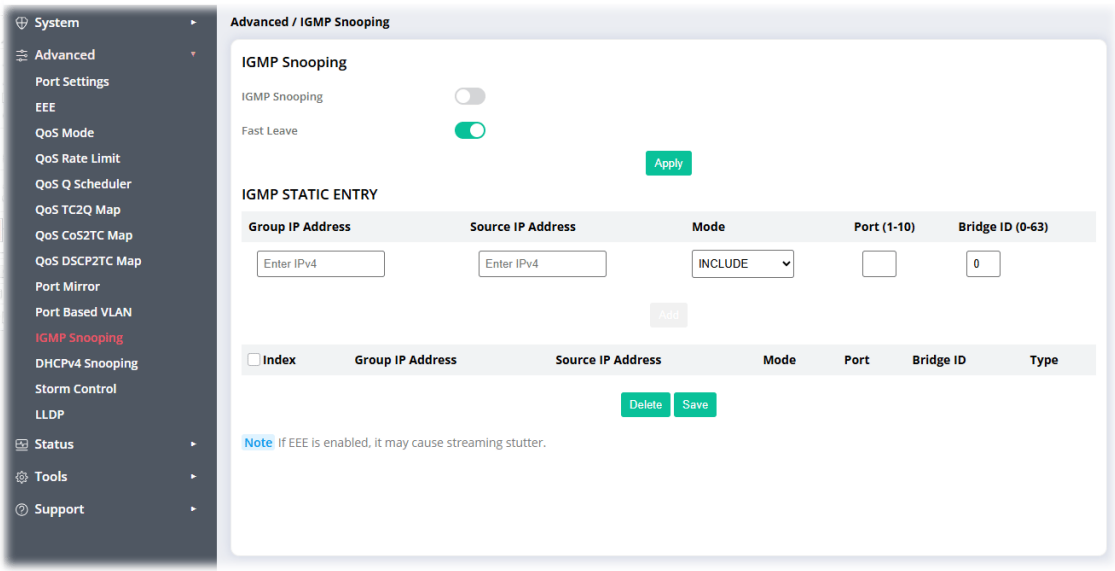
Item	Description
PBV En	Select the box to enable the port based VLAN function for each port.
Port Number	Display the interface (1 to 10).
Bridge Id (1-63)	Specify the port-based VLAN ID (1~63). Bridge Port Based VLAN (PVB) will use Bridge ID as Port Based VLAN ID (PVID). A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines.
Get	Apply the settings to the switch without saving the change.
Apply	Apply the settings to the switch and save the change.

III-11 IGMP Snooping

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.





Available settings are explained as follows:

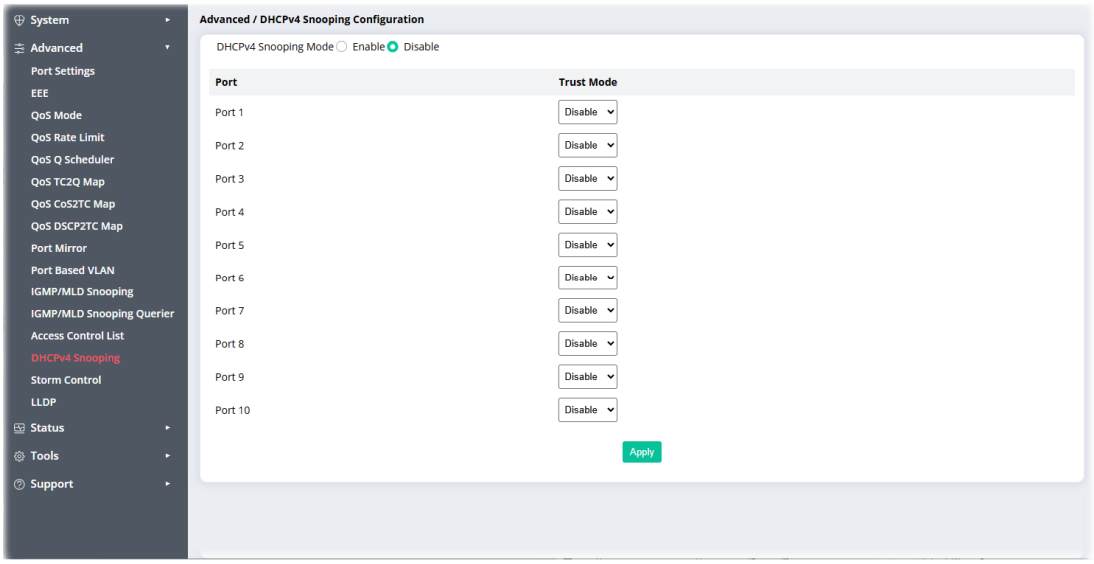
Item	Description
IGMP Snooping	
IGMP Snooping	Switch the toggle to enable/disable the IGMP Snooping function.
Fast Leave	Switch the toggle to enable/disable the IGMP Fast Leave

	function. Normally when the router receives a “leave” message from an IGMP host, it will send a last member query message to see if there are still members within the multicast group. When Fast Leave is enabled, multicast for a group is immediately terminated when the last host in that group sends a “leave” message.
Apply	Save the settings.
IGMP STATIC ENTRY	
Group IP Address	Enter the multicast groups IP addresse that are registered on this device.
Source IP Address	Enter an IP address.
Mode	INCLUDE – Only accept the packets coming from Group IP Address and Source IP Address. EXCLUDE – Accept all of the packets except Group IP Address and Source IP address. DONT CARE – Accept all of the packets.
Port (1-10)	Port ID – Select one PID number for applying the profile on Ethernet / fiber port.
Bridge ID (0-63)	Bridge ID – This number is used to identify multicast bridge logical entities. It helps to track group sources and destinations, especially in multi-VLAN environments.
Delete	Click to remove the selected entry.
Save	Save the settings.

III-12 DHCPv4 Snooping

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

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



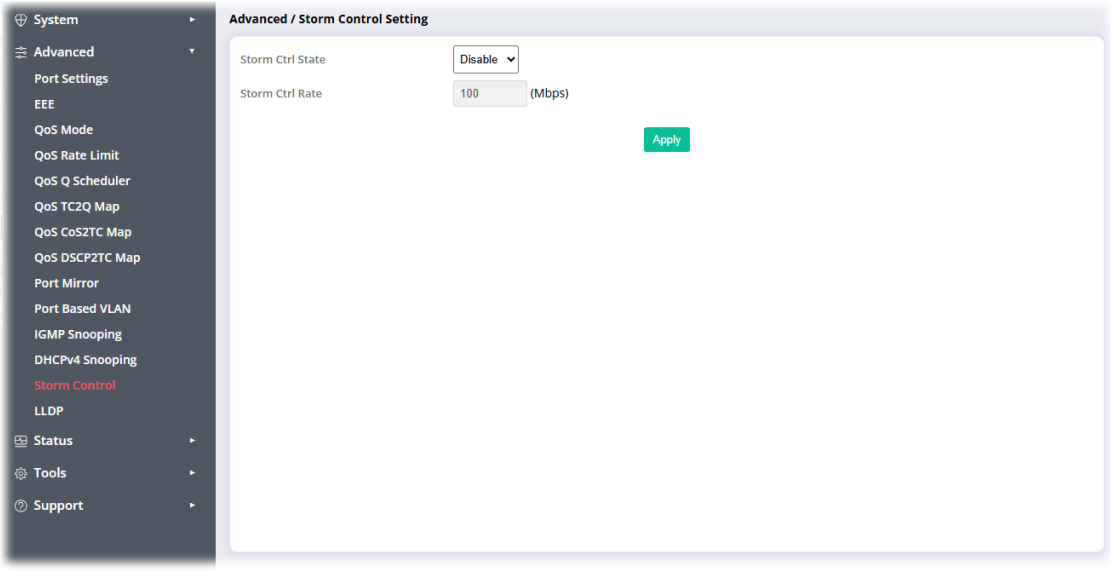
Available settings are explained as follows:

Item	Description
DHCPv4 Snooping Mode	**Enable – Click to** enable global property settings. **Disable –** Clilck to disable the settings.
Port	Display the port number.
Trust Mode	**Enable** – Select it to make the port(s) selected above as trusted interface. **Disable –** Clilck to disable the settings.
Apply	Save the settings.

III-13 Storm Control

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

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

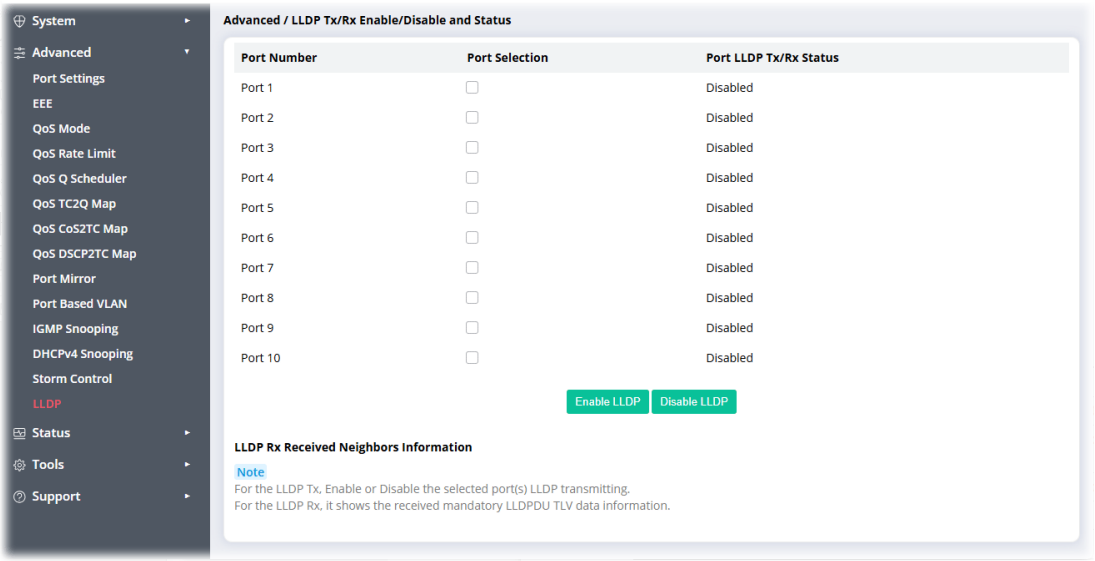


Available settings are explained as follows:

Item	Description
Storm Ctrl State	Enable / Disable the storm control function. Default is Disable.
Storm Ctrl Rate	Specify the storm control rate for packets. Value of storm control rate, Unit: Mbps (Mbits per-second). The range is from 100 to 1000000.
Apply	Save the settings.

III-14 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.



Available settings are explained as follows:

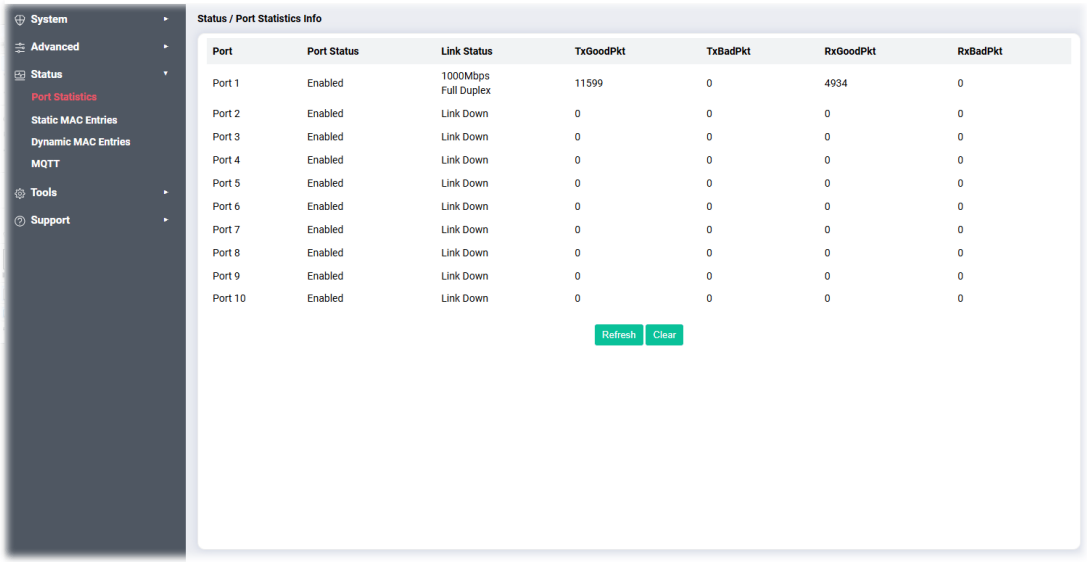
Item	Description
Port Number	Displays the number of LAN ports (1 to 10).
Port Selection	Enable (check the box) or disable (uncheck the box) the selected port(s) for LLDP transmission.
Port LLDP Tx/Rx Status	Display current status of LLDP transmission for the port.
Enable LLDP	Enable the LLDP data transmission for the selected port interface.
Disable LLDP	Disable the LLDP data transmission for the port selected.

This page is left blank.

Part IV Status

IV-1 Port Statistics

This page displays statistics for GE ports.



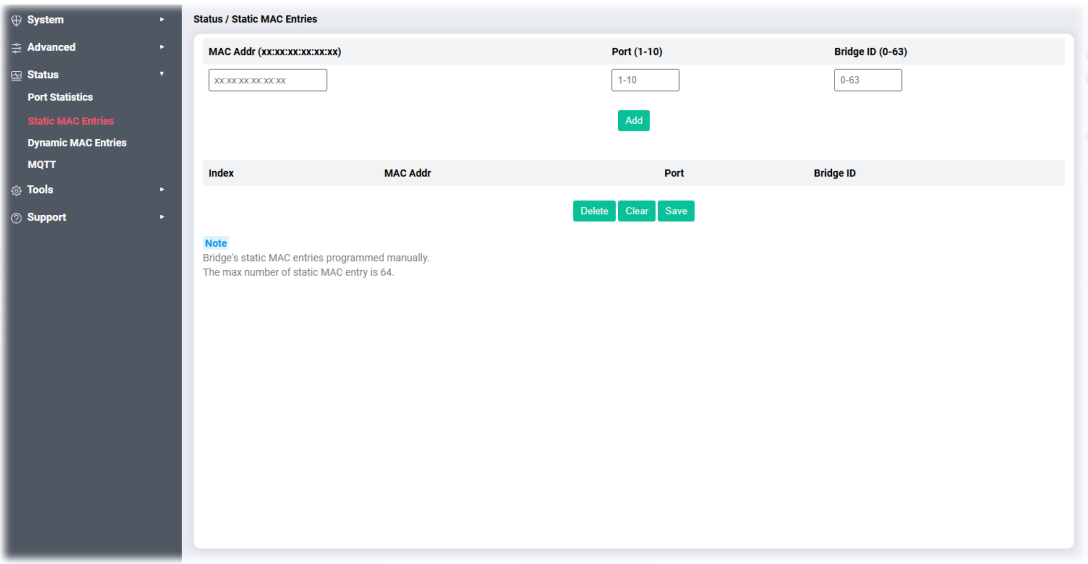
Available settings are explained as follows:

Item	Description
Refresh	Click to reload current port statistics.
Clear	Click to remove current statistics.

IV-2 Static MAC Entries

The purpose of this page is to add a static MAC entry to the MAC address table to restrict a specific device appearing only on a certain port, to prevent hacker attacks with fake MAC addresses for tampering with packet sources.

Up to 64 MAC addresses can be set and displayed on the MAC Address Table below.

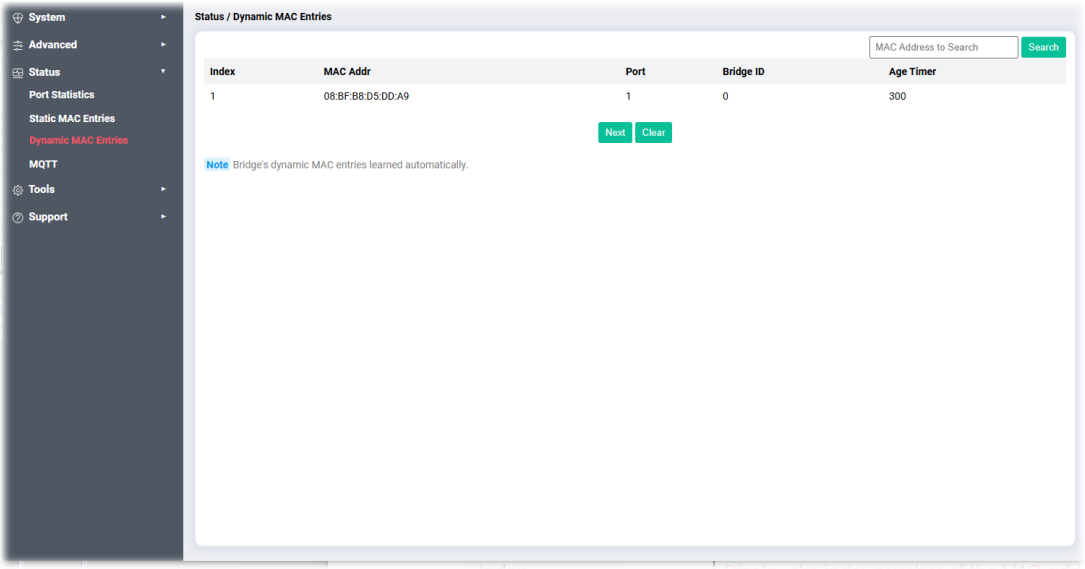


Available settings are explained as follows:

Item	Description
MAC Addr	Enter the MAC address of the device (e.g., host).
Port	Enter the port number that the device is connected to VigorSwitch.
Bridge ID	Specify the ID number of the bridge port. Devices on the bridge ports with the same bridge ID can communicate with each other.
Add	Click to add the new MAC entry and display the result on the table below.
Delete	Click to remove the selected item.
Clear	Click to remove current settings.
Save	Save the settings.

IV-3 Dynamic MAC Entries

This page displays the current dynamic entries in the MAC address table. A maximum of 50 entries will be shown per page. Click "Next" to view additional entries if more than 50 exist.



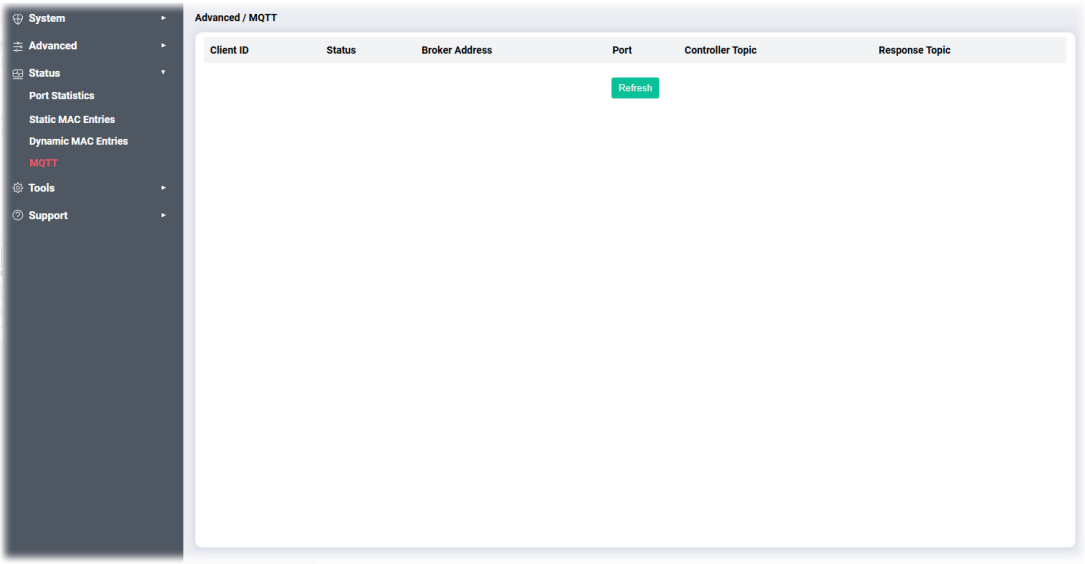
Available settings are explained as follows:

Item	Description
Index	Display the index number of the MAC address searched.
MAC Addr	Display the MAC address that will be forwarded.
Port	Display the port where the MAC address will be forwarded.
Bridge ID	Display the port-based VLAN ID (1~63). Bridge Port Based VLAN (PVB) will use Bridge ID as Port Based VLAN ID (PVID).
Age Timer	Display the Dynamic MAC address aging out value.
Next	Click to view additional entries.
Clear	Click to remove current settings.

IV-4 MQTT

MQTT stands for Message Queuing Telemetry Transport. It is a messaging protocol designed for devices with limited resources and in low-bandwidth, high-latency network environments. It is widely used in Internet of Things (IoT) applications.

This page primarily presents the status of small amounts of data.

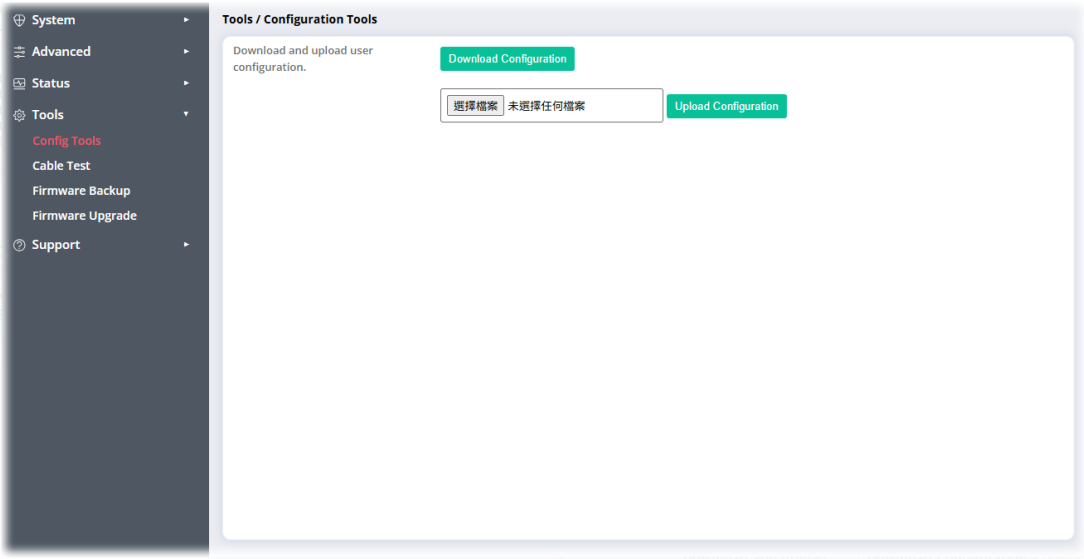


This page is left blank.

Part V Tools

V-1 Config Tools

This page allows a user to download or upload the configuration file of the switch.

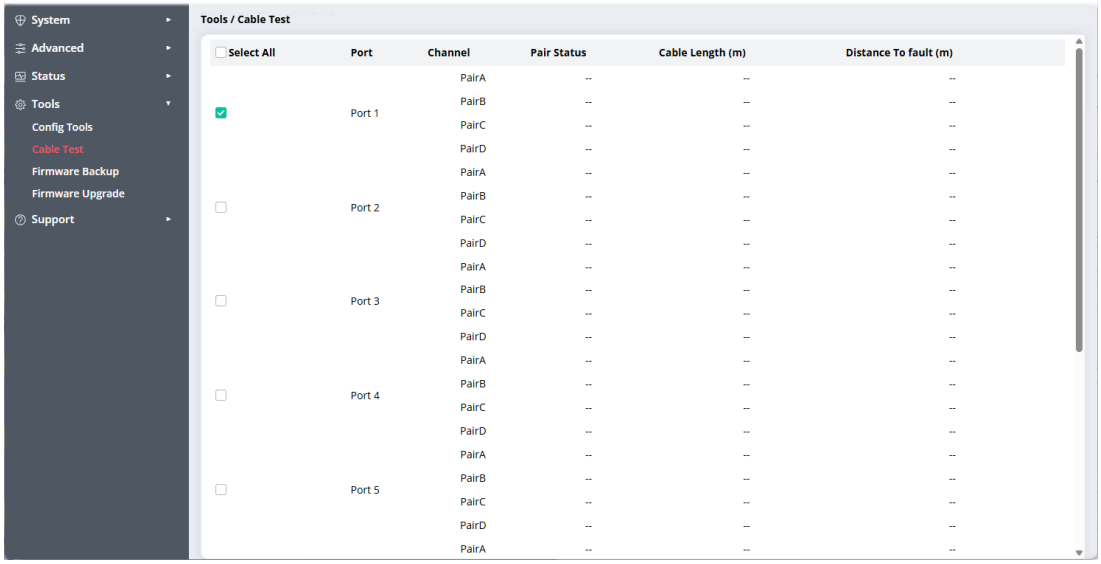


Available settings are explained as follows:

Item	Description
Download and upload user configuration	**Download Configuration** – Download the configuration and store as a file (x.cfg). **Upload Configuration** – Click this button to upload the selected configuration file onto the switch.

V-2 Cable Test

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

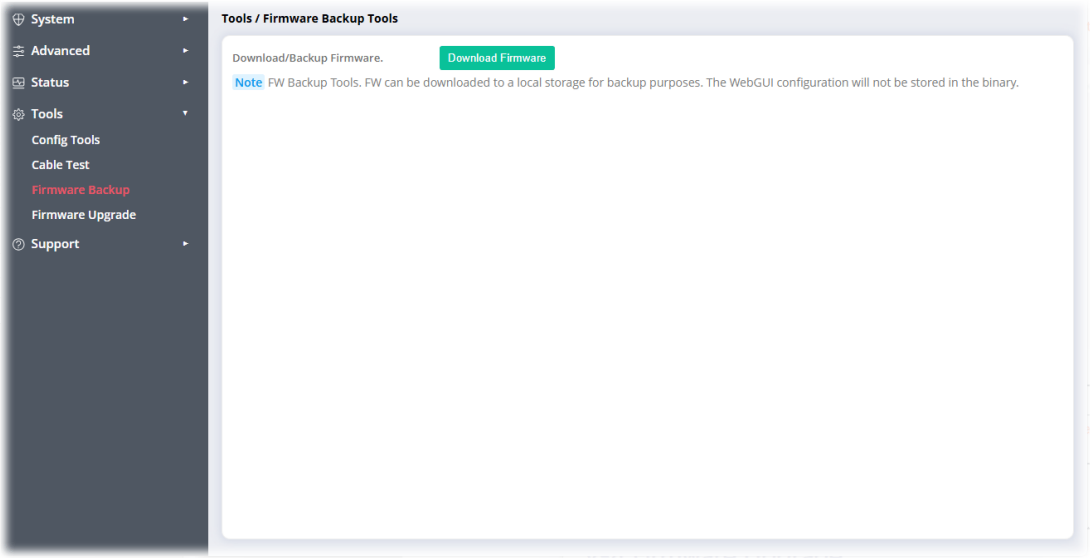


Available settings are explained as follows:

Item	Description
Start Test	Perform the copper test action. Before clicking Start Test, select the port or ports (Port1 to Port8) for performing cable diagnostics.

V-3 Firmware Backup

This page allows a user to backup the firmware image to local storage.

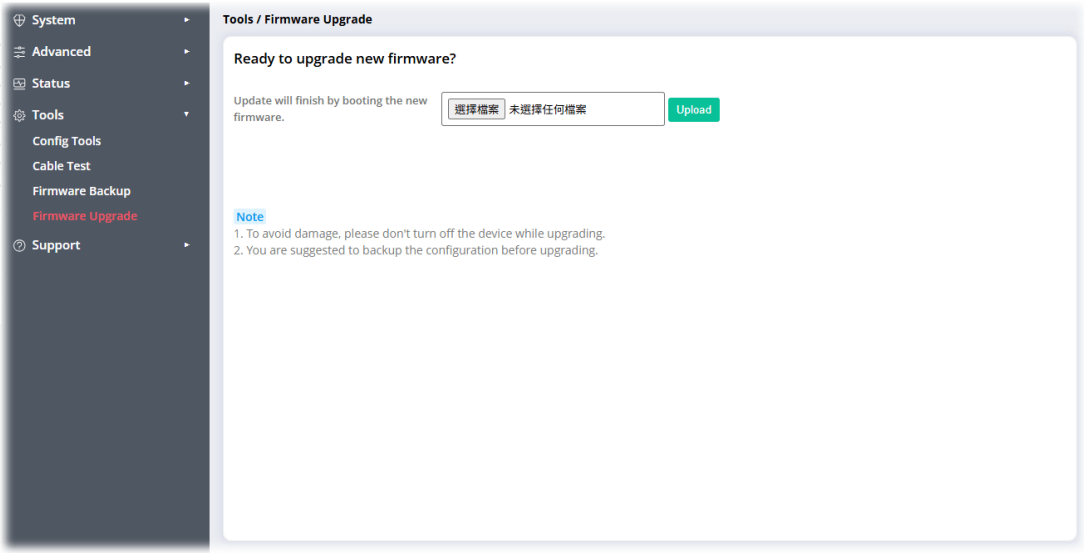


Available settings are explained as follows:

Item	Description
Download/Backup Firmware	**Download Firmware** – Click to execute the firmware backup.

V-4 Firmware Upgrade

This page allows a user to upgrade the firmware image for the switch.



Available settings are explained as follows:

Item	Description
Update will finish...	**Select** – Click to locate the new verion of the firmware stored on the host. **Upload** – Click to execute the firmware upgrade.