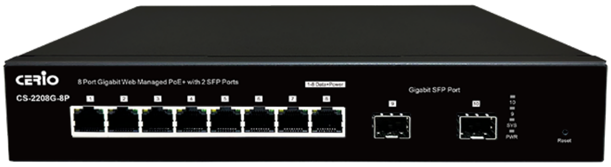
CERIO Corporation

CS-2208G-8P A3

PoE CS-2000 Series - 8 Port 10/100/1000M Gigabit Web Managed PoE+ with 2 SFP Ports



User Manual

Default IP /	Login Information
IP Address	192.168.2.200
User Name	root
Password	default

FCC Warning

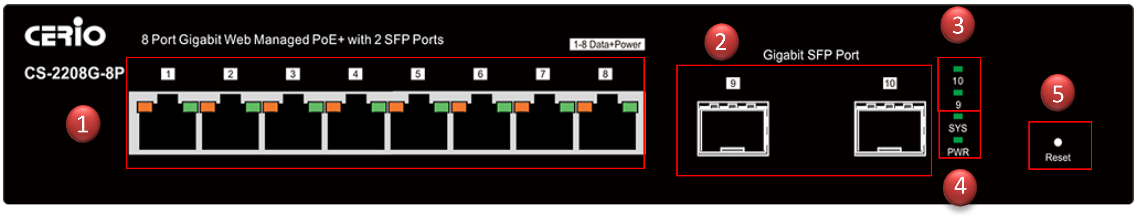
This device has been tested and found to comply with limits for a Class A digital device, pursuant to Part 2 and 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the user's manual, may cause interference in which case user will be required to correct the interference at his own expense.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user many be required to take adequate measures.

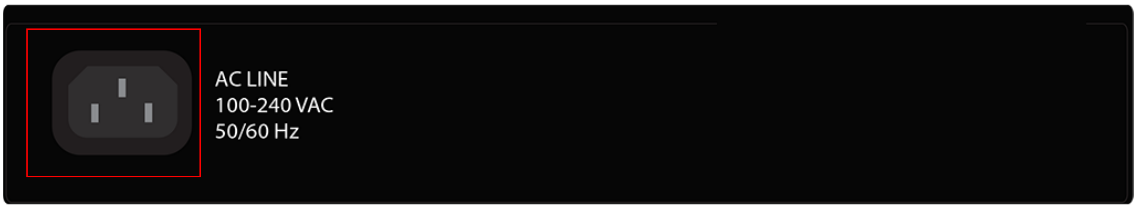
1. Introduction

1.1 Front Panel



1) 8 Gigabit Ethernet PoE Ports(RJ-45) with Ethernet PoE(left) + Ethernet Link/ACT(right) LED
2) 2 Gigabit SFP Ports.
3) 2 SFP status LED light.
4) Power and Sys standby LED light.
5) Reset to default button. (Long press the “Reset” button with a pin for 10 seconds, if the LEDs start to flash, the reset process starts.)

1.2 Rear Panel Layout



- AC input (100-240V/AC, 50-60Hz) UL Safety

LED indicators:

The LED Indicators will allow you to monitor, diagnose and help in troubleshooting any potential problem with the switch, the connection(s) or other attached devices.

RJ45 Ethernet Connector Port LED Indicator:

Each RJ45 Ethernet port has two LEDs. The left LED is yellow, The light up as long as the POE connection detection is successful., The right LED is green and lights up to indicate that a link has been established. It will flash randomly whenever there is network activity on the port

	Color	**Status**	**Description**
PWR	Green	On	Power on
		Off	Power off or fail
SYS/RUN	Green	Off	System fail or Power off
		Blinking	System boot-up and In operation
Link/ACT	Green	On	10/100/1000Mbps connected
		Blinking	Data transmitting
PoE	Orange	Orange On	PoE power output on
		Blinking	PoE power output amount not stable
	None	Off	There is no PoE power output
SFP	Green	On	100/1000FX connected
		Off	SFP not connected

2. Software Configuration

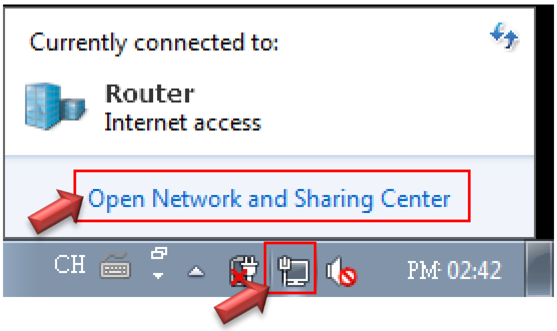
CS-2208G-8P supports web-based configuration. Upon the completion of hardware installation, The Switch can be configured through a PC/NB by using its web browser such as Internet Explorer or Microsoft Edge or Google Chrome.

Set the IP segment of the administrator's computer to be in the same range as **CS-2208G-8P** for accessing the system. Do not duplicate the IP Address used here with IP Address of **CS-2208G-8P** or any other device within the network. ***Please refer to the following steps***

2.1 Example of Segment: (Windows OS)

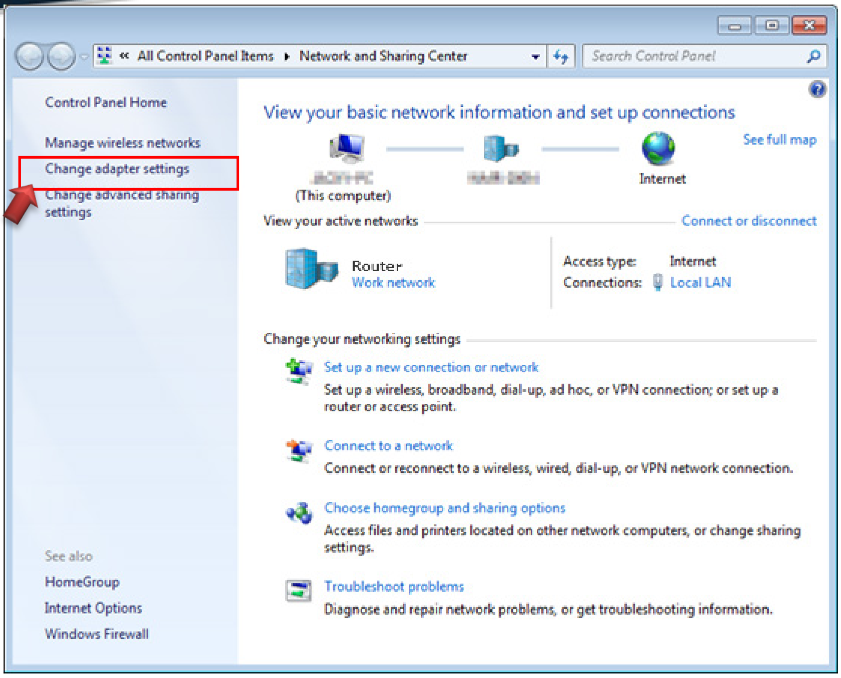
Step 1 :

Please click on the computer icon in the bottom right window, and click **“Open Network and Sharing Center”**



Step 2 :

In the Network and Sharing Center page, click on the left side of **“Change adapter setting”** button



View your basic network information and set up connections

View your active networks

Change your networking settings

Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

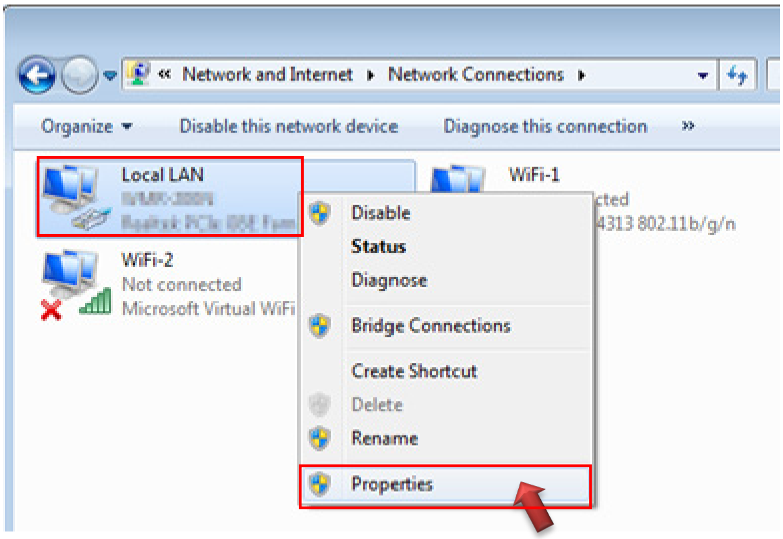
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

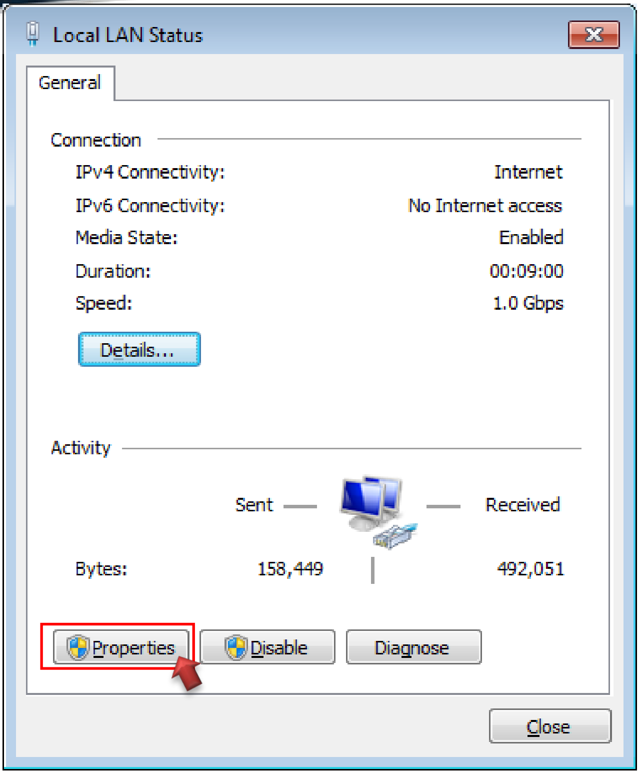
Step 3 :

In **"Change adapter setting"** Page, right click on Local LAN then select **"Properties"**



Step 4 :

In the **"Properties"** page, click the **"Properties"** button to open TCP/IP setting



Local LAN Status

General

Connection

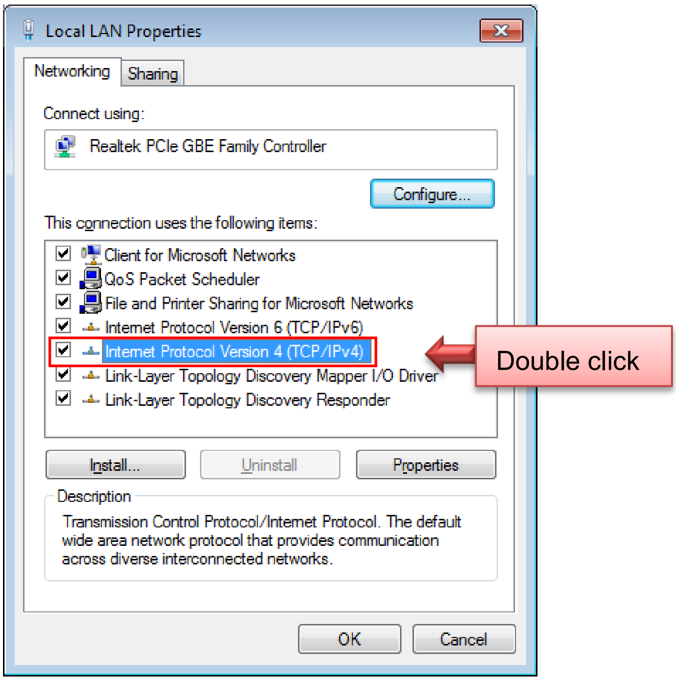
IPv4 Connectivity:	Internet
IPv6 Connectivity:	No Internet access
Media State:	Enabled
Duration:	00:09:00
Speed:	1.0 Gbps

Activity

	Sent	Received
Bytes:	158,449	492,051

Step 5 :

In Properties page for setting IP addresses, find **"Internet Protocol Version 4 (TCP/IPv4)"** and double click to open TCP/IPv4 Properties window



Local LAN Properties

Networking | Sharing

Connect using:

Realtek PCIe GBE Family Controller

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

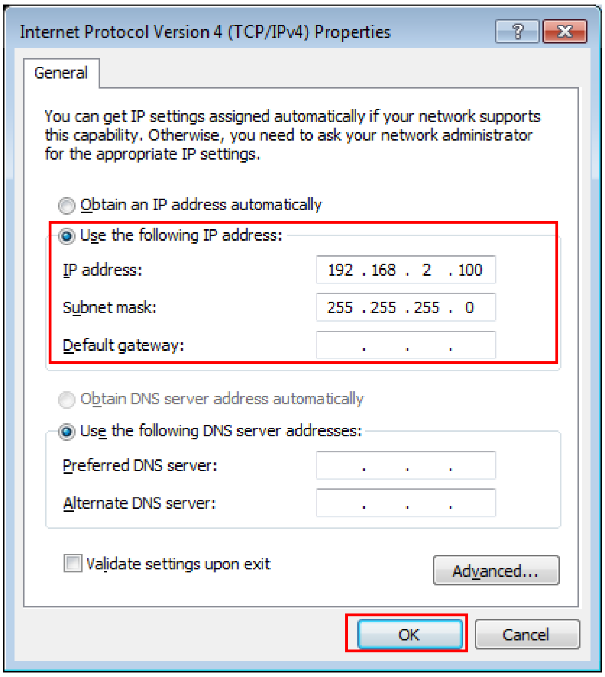
Step 6 :

Select **"Use the following IP address"**, and fix in IP Address to: 192.168.2.X

ex. The X is any number from 1 to 253

Subnet mask : 255.255.255.0

And Click **"OK"** to complete fixing the computer IP settings



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

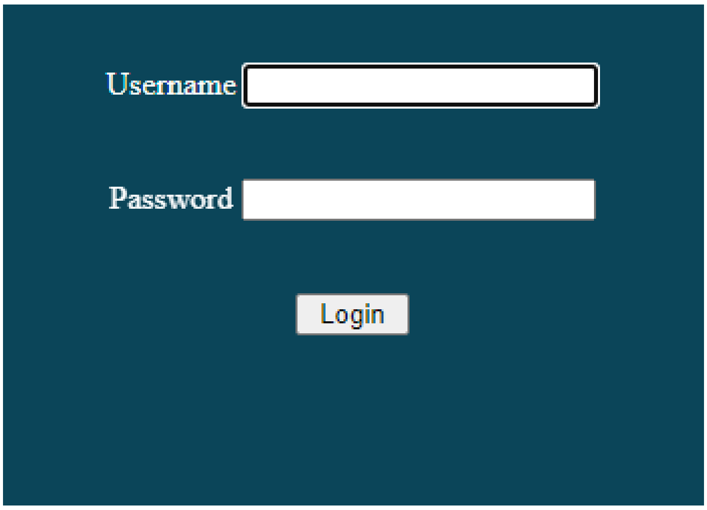
Alternate DNS server: . . .

□ Validate settings upon exit

Step 7 :

Open Web Browser

Without a valid certificate, users may encounter the following problem in IE or Microsoft Edge when they try to access system's WMI (http://192.168.2.200) . There will be a “Certificate Error”, because the browser treats system as an illegal website.



System login Overview page will appear after successful login.

2.2 System login username and password information

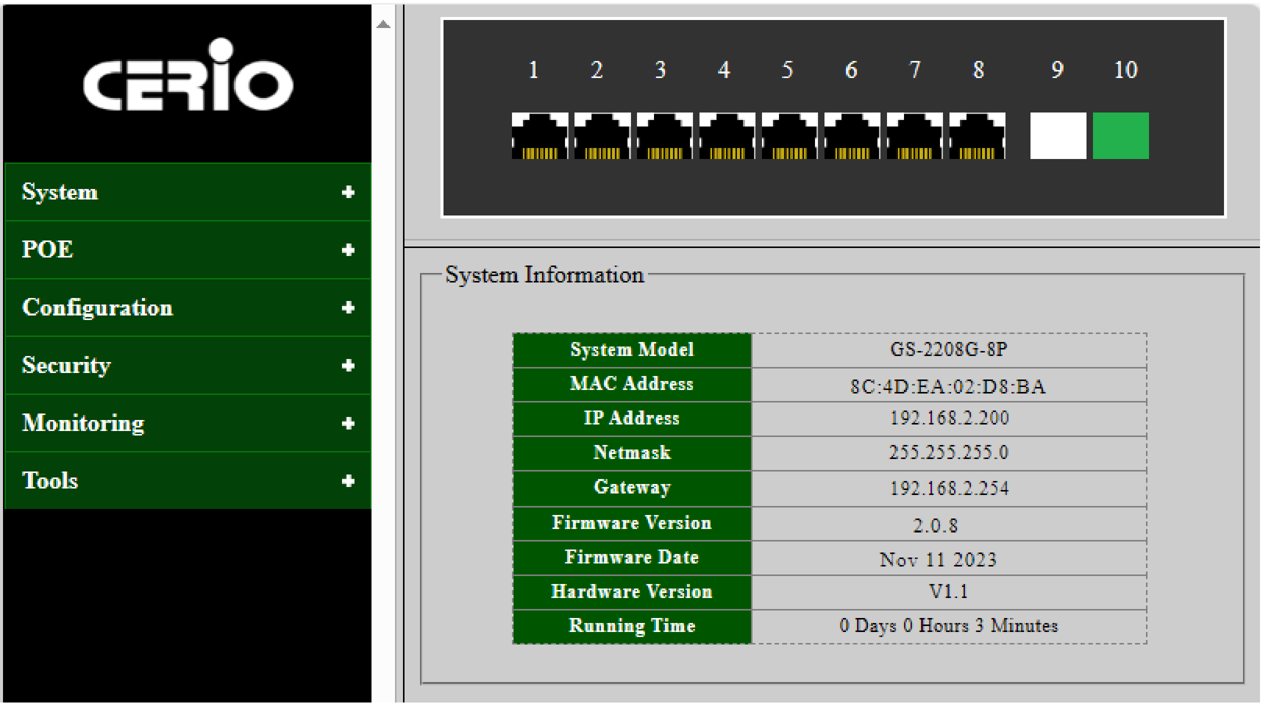
The **CS-2208G-8P** web switch default IP is 192.168.2.200

Into the management page as follows, please enter Username and password

- **Default IP Address**: 192.168.2.200
- **Default Username and Password**

Management Account	Root Account
Username	root
Password	default

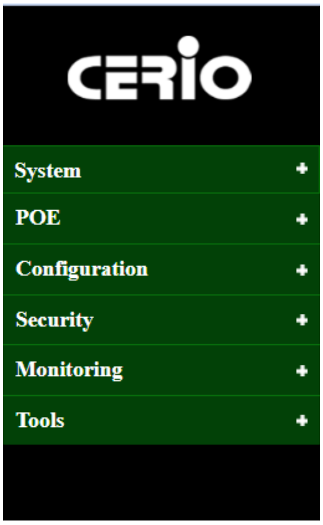
After the authentication procedure, the home page will show up. Select one of the configurations by clicking the icon.



System Information

System Model	GS-2208G-8P
MAC Address	8C:4D:EA:02:D8:BA
IP Address	192.168.2.200
Netmask	255.255.255.0
Gateway	192.168.2.254
Firmware Version	2.0.8
Firmware Date	Nov 11 2023
Hardware Version	V1.1
Running Time	0 Days 0 Hours 3 Minutes

2.3 Function Menu



The PoE smart switch software provides layer 2 rich functionality for switches in your network. This chapter describes how to use the web-based management interface (Web UI) to configure the switch’s features.

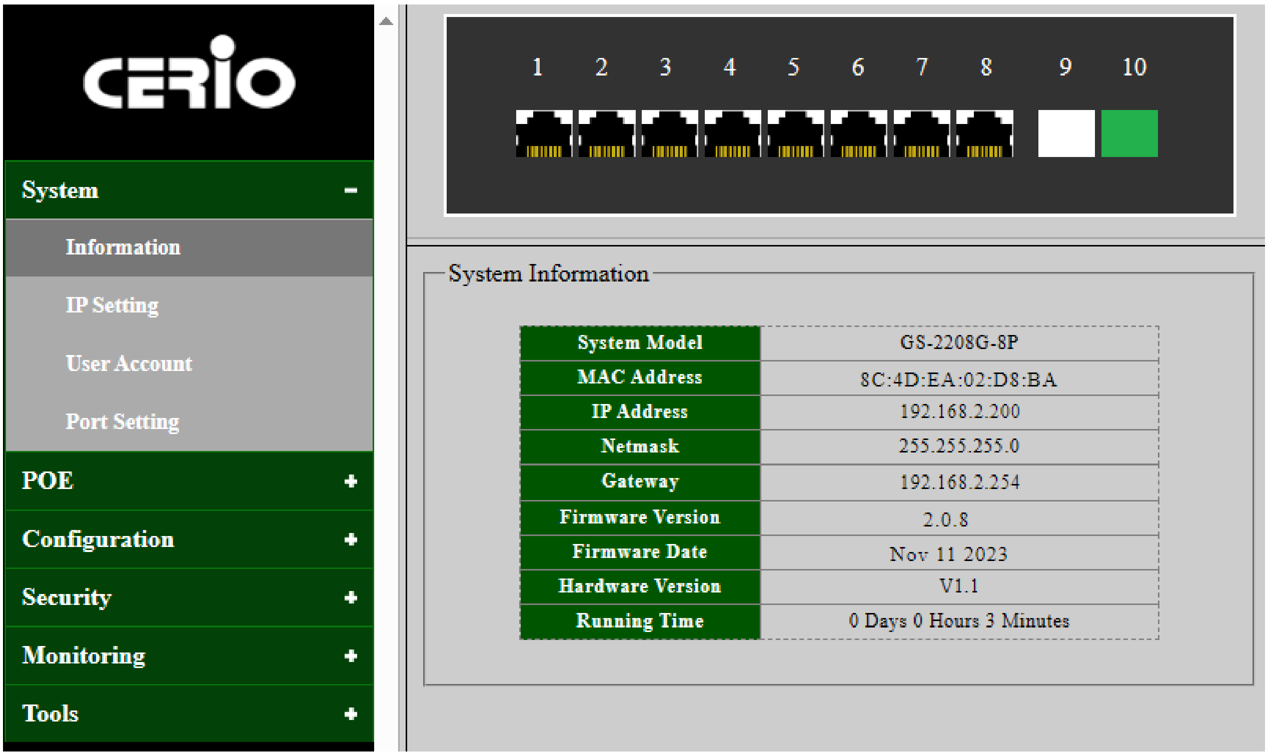
Name	Function
System	This link displays device information and ,IP address Settings, port Settings, user accounts
POE	You can configure PoE.,POE power port control
Configuration	VLAN
	QOS
	IGMP
	Link aggregation
	Loop protection
	RSTP
	Port mirroring
	Port isolation
	Bandwidth control
	Giant frame
	MAC constraints
	Green Ethernet
	EEE
	SNMP Trap

Security	MAC address
	Broadcast Storm
Monitoring	Port statistics
	Cable diagnostics
Tools	Firmware upgrade
	Configure backup
	Reset
	Save
	Restart

3. System

3.1 System Information

The page administrator can monitor switch information and modify network IP / mask. Administrator can view your device's system information here, as well as set your device model. In the navigation bar click: **System --> System Information.**



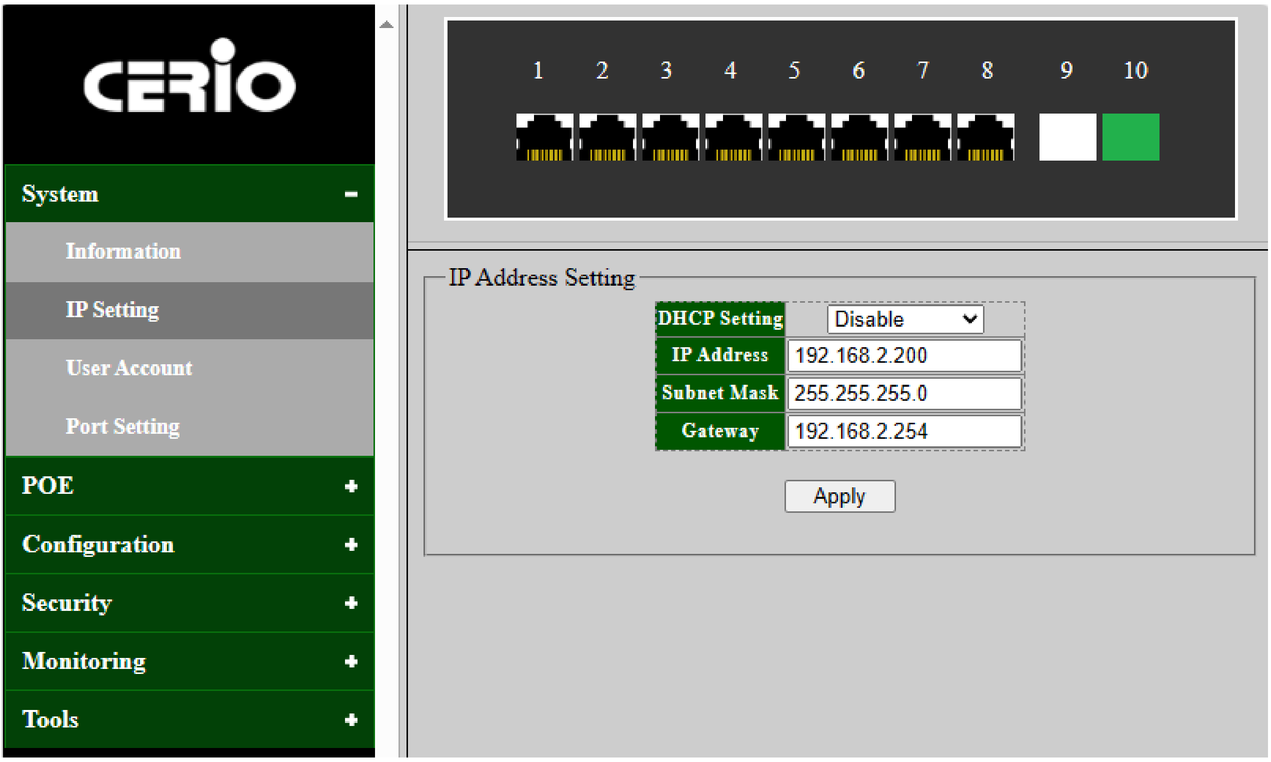
System Information

System Model	GS-2208G-8P
MAC Address	8C:4D:EA:02:D8:BA
IP Address	192.168.2.200
Netmask	255.255.255.0
Gateway	192.168.2.254
Firmware Version	2.0.8
Firmware Date	Nov 11 2023
Hardware Version	V1.1
Running Time	0 Days 0 Hours 3 Minutes

- **Device Model:** Display switch model name
- **MAC Address:** Display the system MAC Address
- **IP Address:** Display system IP address of the recent system
- **Subnet Mask:** Display network Mask
- **Gateway:** Display Gateway IP Address
- **Key version :** Display software version
- **Firmware date :** Display the software version date
- **Hardware version :** Display device hardware version
- **Run time :** Display device run time

3.2 IP Settings

This page administrator can set system IP address, Each device in the network has an IP address through which it can log into the management interface to operate the switch. Click the navigation bar: **System --> IP Settings**



IP Address Setting

DHCP Setting	Disable
IP Address	192.168.2.200
Subnet Mask	255.255.255.0
Gateway	192.168.2.254

System IP Setup

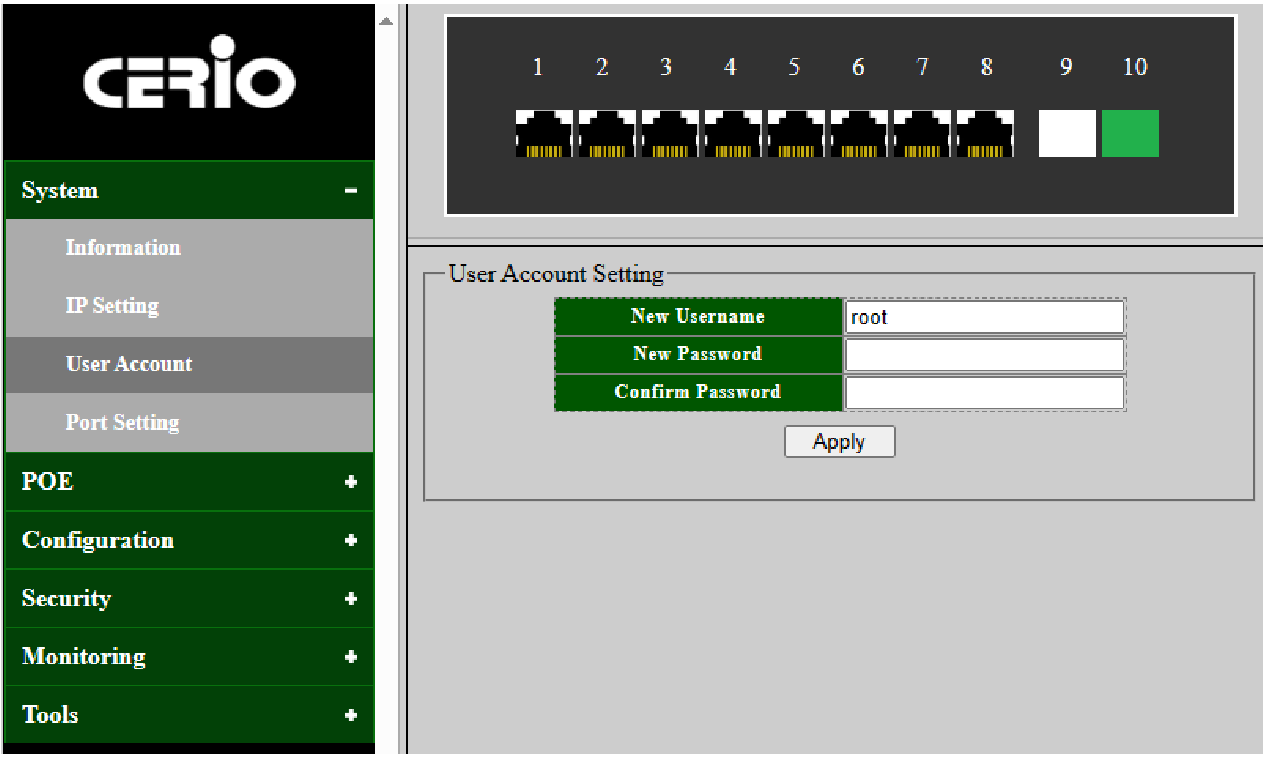
- **DHCP Settings :** DHCP Settings Choose to enable or disable the DHCP feature.
  - **Disable :** Select disable, you need to manually enter the IP address, subnet mask and default gateway.
  - **Enable :** Enable: Select Enable, the exchange will get the network parameters from the DHCP server.

- **IP Address :**
  - IP Address Sets the IP address of the device.
- **Subnet Mask :**
  - Subnet Mask Sets the subnet mask of the device.
- **Gateway :**
  - Default Gateway Sets the device's default gateway address.

Click "Apply" to save the setting. Please note that changing IP will lose the recent connection. Administrator will have to login with the newly set IP address.

3.3 User Account

This page Administrator can change the Switch login password on this page. The default login password is default.. Click the navigation bar: **System --> User Account Settings**



User Account Setting

New Username	root
New Password	
Confirm Password	

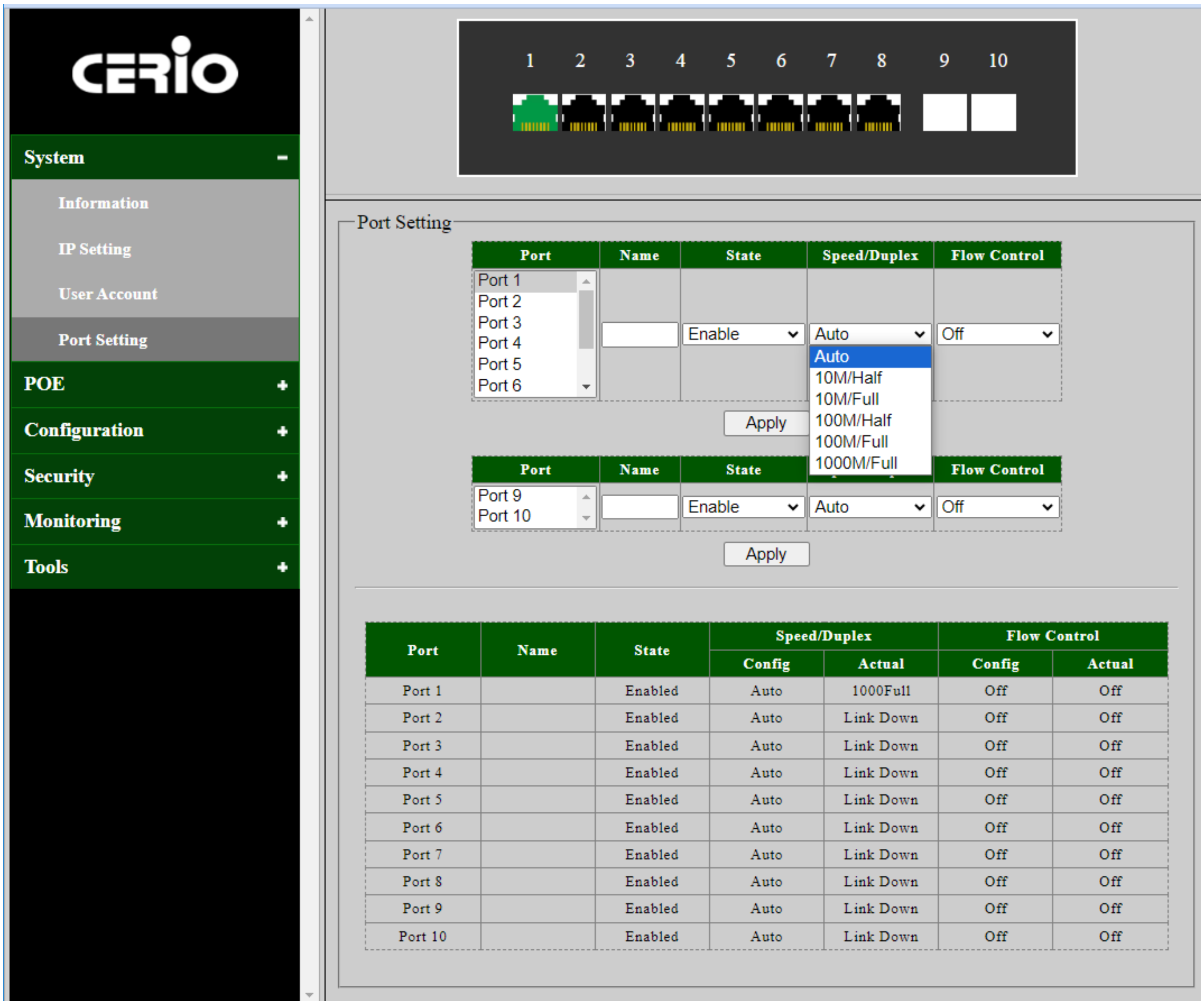
User name sets the user name to log in to the switch. The length of the user name and password cannot exceed 16 characters, and only numbers can be used. The characters used can be "a-z", "A-Z" and "0-9". Please note that when setting up, please make sure to enter the same password twice to ensure successful setting.

Administrator has to click the "Apply" button to refresh the User Account Setting.

Notice Please refresh the page again after changing the password.

3.4 Port Settings

This page administrator can set Port name, status, duplex speed, flow control can be modified here. Click on the navigation bar: **System --> Port Settings**



Port	Name	State	Speed/Duplex		Flow Control	
			Config	Actual	Config	Actual
Port 1		Enabled	Auto	1000Full	Off	Off
Port 2		Enabled	Auto	Link Down	Off	Off
Port 3		Enabled	Auto	Link Down	Off	Off
Port 4		Enabled	Auto	Link Down	Off	Off
Port 5		Enabled	Auto	Link Down	Off	Off
Port 6		Enabled	Auto	Link Down	Off	Off
Port 7		Enabled	Auto	Link Down	Off	Off
Port 8		Enabled	Auto	Link Down	Off	Off
Port 9		Enabled	Auto	Link Down	Off	Off
Port 10		Enabled	Auto	Link Down	Off	Off

- **"Ports:"** Multiple ports can be selected.
- **"Name:"** First name sets port aliases.
- **"State:"** The port is open and closed. If the port is open, the port can forward packets normally.
- **"Speed/duplex:"** Administrator can set the "**Speed**" of each "**Port**" as Auto, or **10M Half**, or **10M Full**, **or 100M Half**, or **100M Full** or **1000M Full**. When the mode is selected as auto, the rate and duplex will be determined by negotiation, Because port number **9** and **10** are of SFP ports, it is only applicable to set the **100M** or **1000M** speed of the SFP ports.

- **"Flow control:"** The flow control function is turned on and off. When the flow control function is turned on, the rate of data packet forwarding on each port can be controlled and adjusted to avoid congestion.

Administrators can hold down the "Ctrl" key and use the left mouse button to select a port, select the State, Speed/Duplex Flow Control of the selected port, and click the "Apply" button to refresh the Port Setting.

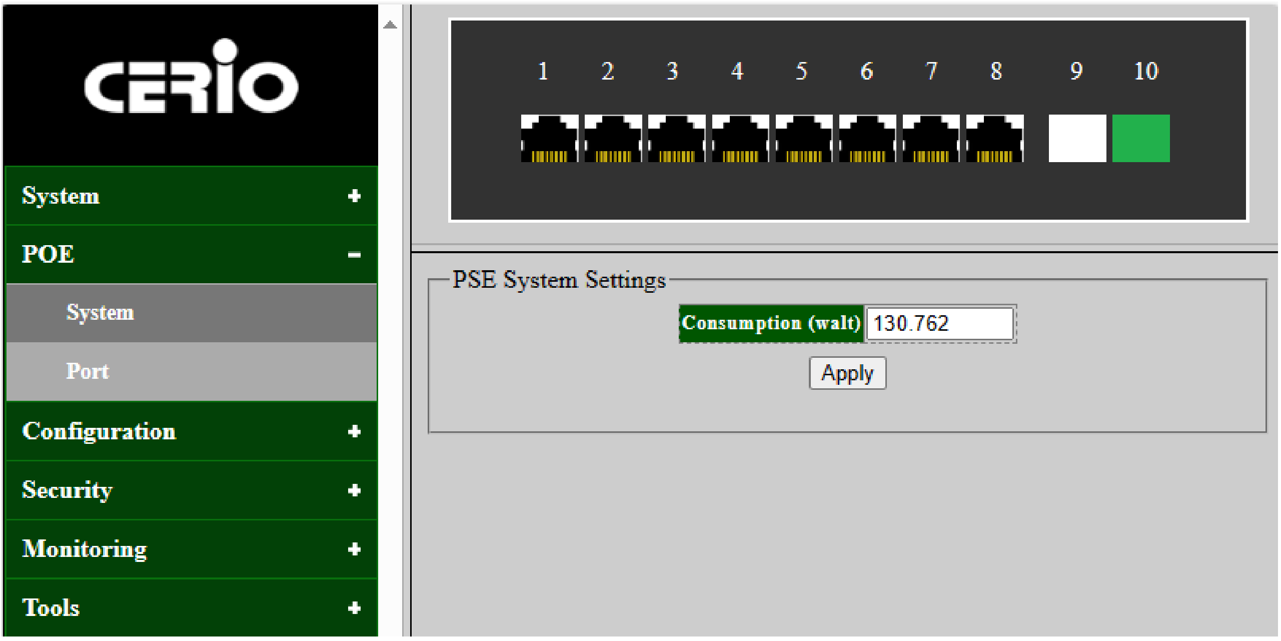
Notice After changing the Settings, click the port Settings to refresh the display status

Field	Description
Port	Displays the port number of the switch.
Name	Display custom port name.
State	Displays the actual state of the ports. • **Enabled:** Enable the port. • **Disabled:** Disable the port.
Speed/ Duplex	Current port speed configuration and link speed and duplex status. • **Config:** Displays the configuration of Speed and Duplex mode for the port. • **Actual:** Displays the actual working state of the port.
Flow Control	Current port flow control configuration and link flow control status. • **Config:** Displays the configuration of the Flow Control for the port. • **Actual:** Displays the actual working state of the port.

4. PoE

4.1 PSE System

The page shows the POE device current total power consumed by the total POE port ,
Click navigation bar : **POE --> System.**



PSE System Settings

Consumption (walt) 130.762

Apply

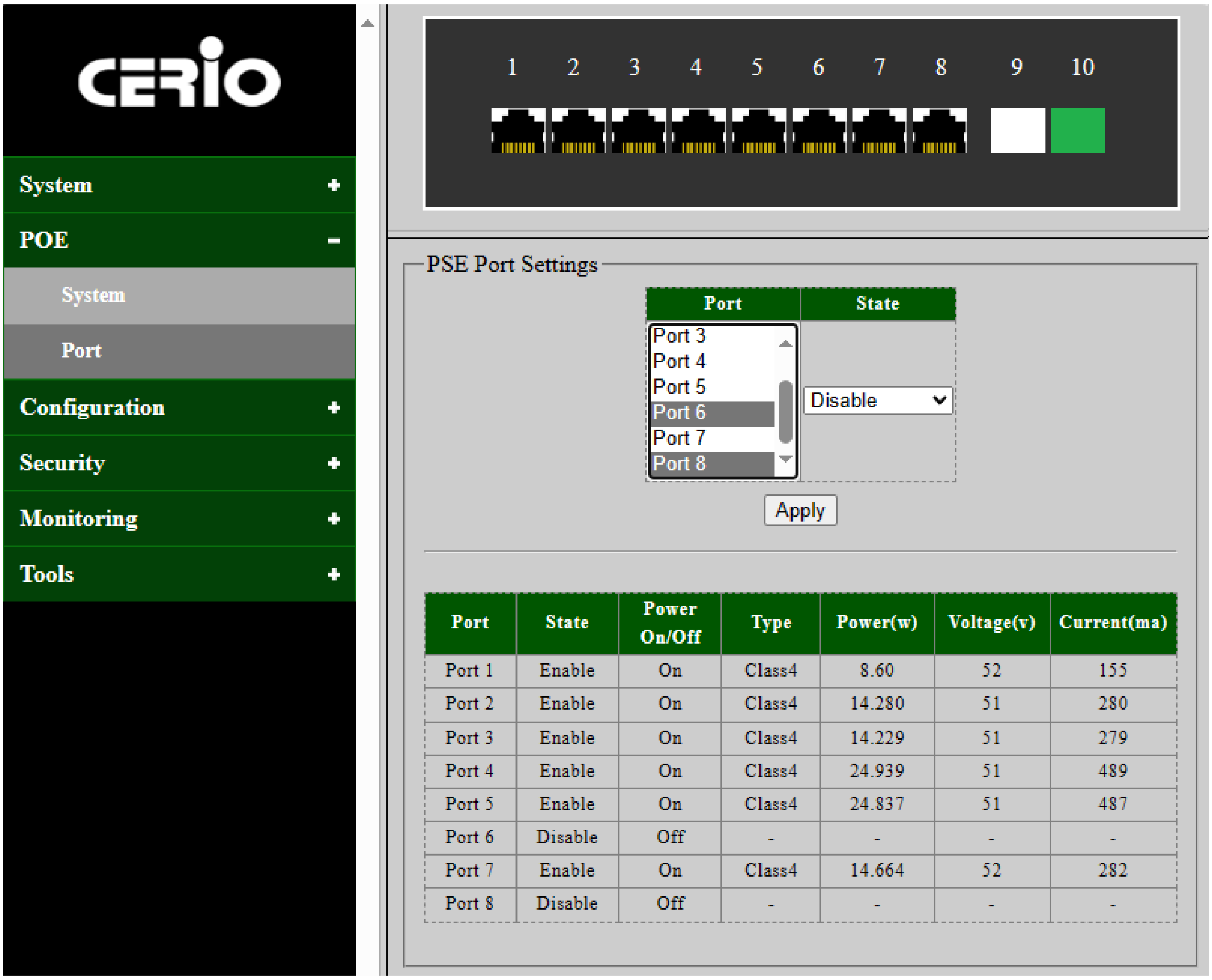
- **Consumption (Watt) :** Displays the used power in watts that the overall POE of the entire device is outputting.

Notice

This hardware specification "**POE power has a total POE output power of 130Watt (POE budget).** When used beyond the limit, it will affect the normal operating capability and stability of the machine and the service life of the product. Please do not exceed the limit..

4.2 PSE Port Setting

This page administrator can set the PoE PSE port status here ,
Click navigation bar: **POE --> Port**



PSE Port Settings

Port	State
Port 3 Port 4 Port 5 Port 6 Port 7 Port 8	Disable

Port	State	Power On/Off	Type	Power(w)	Voltage(v)	Current(ma)
Port 1	Enable	On	Class4	8.60	52	155
Port 2	Enable	On	Class4	14.280	51	280
Port 3	Enable	On	Class4	14.229	51	279
Port 4	Enable	On	Class4	24.939	51	489
Port 5	Enable	On	Class4	24.837	51	487
Port 6	Disable	Off	-	-	-	-
Port 7	Enable	On	Class4	14.664	52	282
Port 8	Disable	Off	-	-	-	-

- **"Ports:"** Multiple ports can be selected.
- **"State:"** State In the open state Administrators can control PoE usage per port through Turn On/Turn Off option by Enable or Disable.

Administrators can hold down the "Ctrl" key and use the left mouse button to select a port, select the State of the selected port, and click the "Apply" button to refresh PoE PSE Port on/off Setting.

Field	Description
Port	**Displays the port number of the switch.**
State	Displays the actual state of the POE PSE ports. • **Enabled:** Enable the port of POE PSE. • **Disabled:** Disable the port of POE PSE.

Power On/Off	Current port of POE PSE Power on/off status. • **On:** The output power supply of the POE port has been turned on. • **Off:** The output power supply of the POE port has been turned off.
Type	Display the Class Type/level used by POE, displayed Class0 / Class1 / Class2 /Class3 / Class4 ● **If your PD powered device only supports response communication in the form of 2-event classification, the “Class” level displayed in "Type" here will depend on the design communication level of your PD device , and will only be displayed as "Class 4".**
Power(w)	Displays the actual power used by each POE port (W).
Voltage(v)	Display the POE Voltage used (V).
Current(ma)	Display the POE Current used (mA).

Notice

Power over Ethernet Classification:

1-event classification – for PDs of 802.3af/at Class 0-3 (Old for POE)

The chip usually used to connect PD is the old 802.af POE communication chip. For example, the device connected to the PD is an 802.3af POE Splitter or a general low-power IPCAM.

2-event classification – for PDs of 802.3at Class 4 (New for POE+)

The chip usually used to connect to PD is new 802.at POE+ communication chip. For example, the device to connect to PD is 802.3at POE+ Splitter.

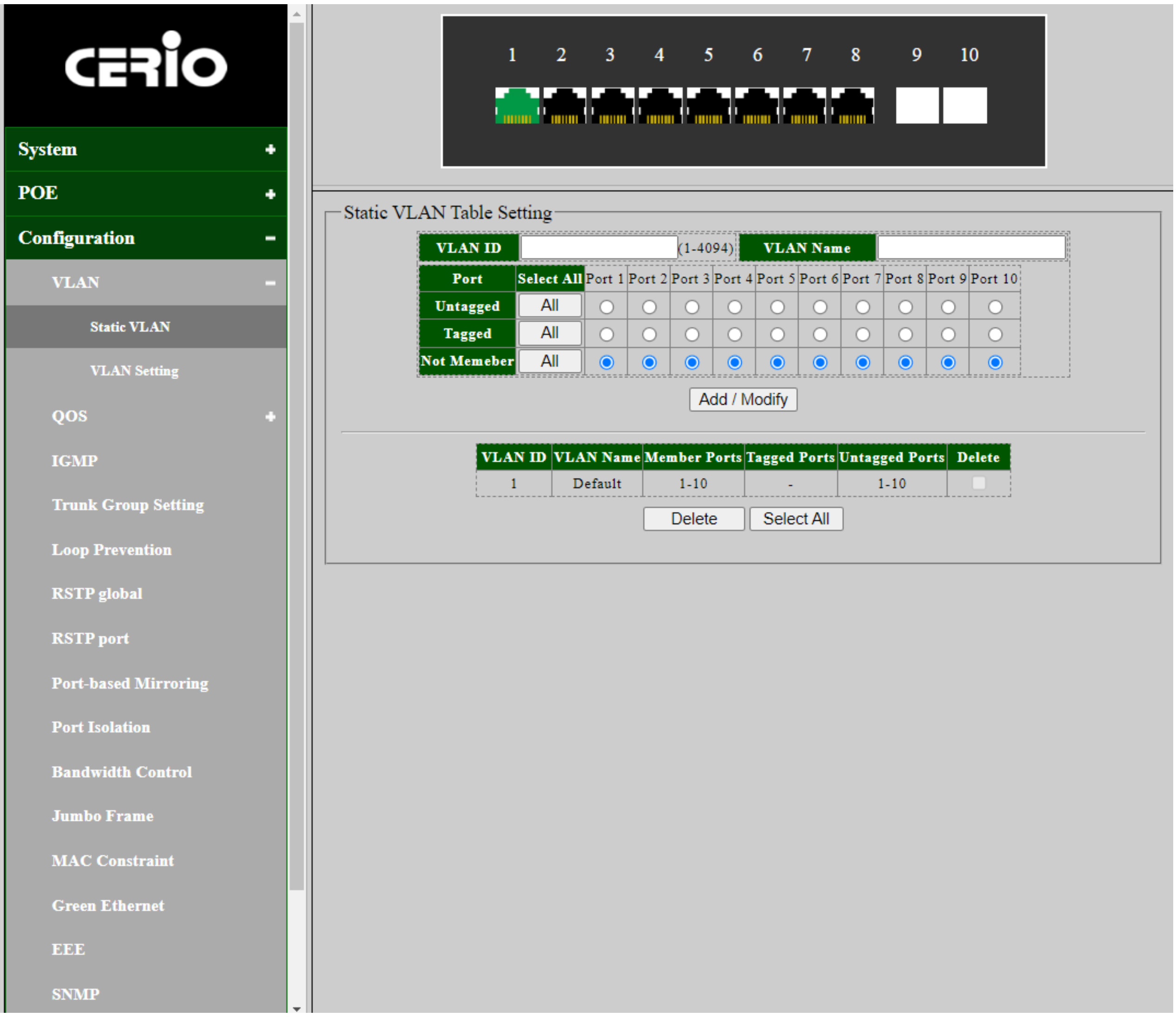
5. Configuration

5.1 VLAN

In the VLAN function, administrator can set IEEE 802.1q i.e., Tag Based VLAN settings. VLAN or virtual local area network is any broadcast of the same domain, regardless of the real physical location, that is partitioned and isolated in a computer network at the data link layer. VLAN has the same attributes as local area network, but VLAN can group the end stations together even they are not located in the same network.

5.1.1 Static VLAN (802.1Q)

Click navigation bar: **Configuration -> VLAN -> Static VLAN**



Static VLAN Table Setting

VLAN ID		(1-4094)	VLAN Name	

Port	Select All	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8	Port 9	Port 10
Untagged	All	○	○	○	○	○	○	○	○	○	○
Tagged	All	○	○	○	○	○	○	○	○	○	○
Not Memeber	All	●	●	●	●	●	●	●	●	●	●

Add / Modify

VLAN ID	VLAN Name	Member Ports	Tagged Ports	Untagged Ports	Delete
1	Default	1-10	-	1-10	□

Delete Select All

- ➢ **“VLAN ID:”** Set the port VID VLAN ID is for static VLAN, ranging from 1-4094.
- ➢ **“VLAN Name:”** Specify the VLAN Name for new created 802.1Q Static VLANs.
- ➢ **“Port:”** Displays the port number of the switch.
- ➢ **“Select All:”** Click "All" to configure all port settings. **(Helps quickly choose to set)**
- ➢ **“Untagged:”** Configure the egress rule of the traffic on the port as untagged. The switch drops the tag header before sending the packet.

- **“Tagged:”** Configure the egress rule of the traffic on the port as tagged. The switch adds the tag header before sending the packet.
- **“Not Member:”** Click All or any one port to set for not member of VLAN group.

Administrator has to click the “Add / Modify” button let users to add and modify ports, and “Delete” button let users to delete whole set of the same VLAN ID ports.

Notice

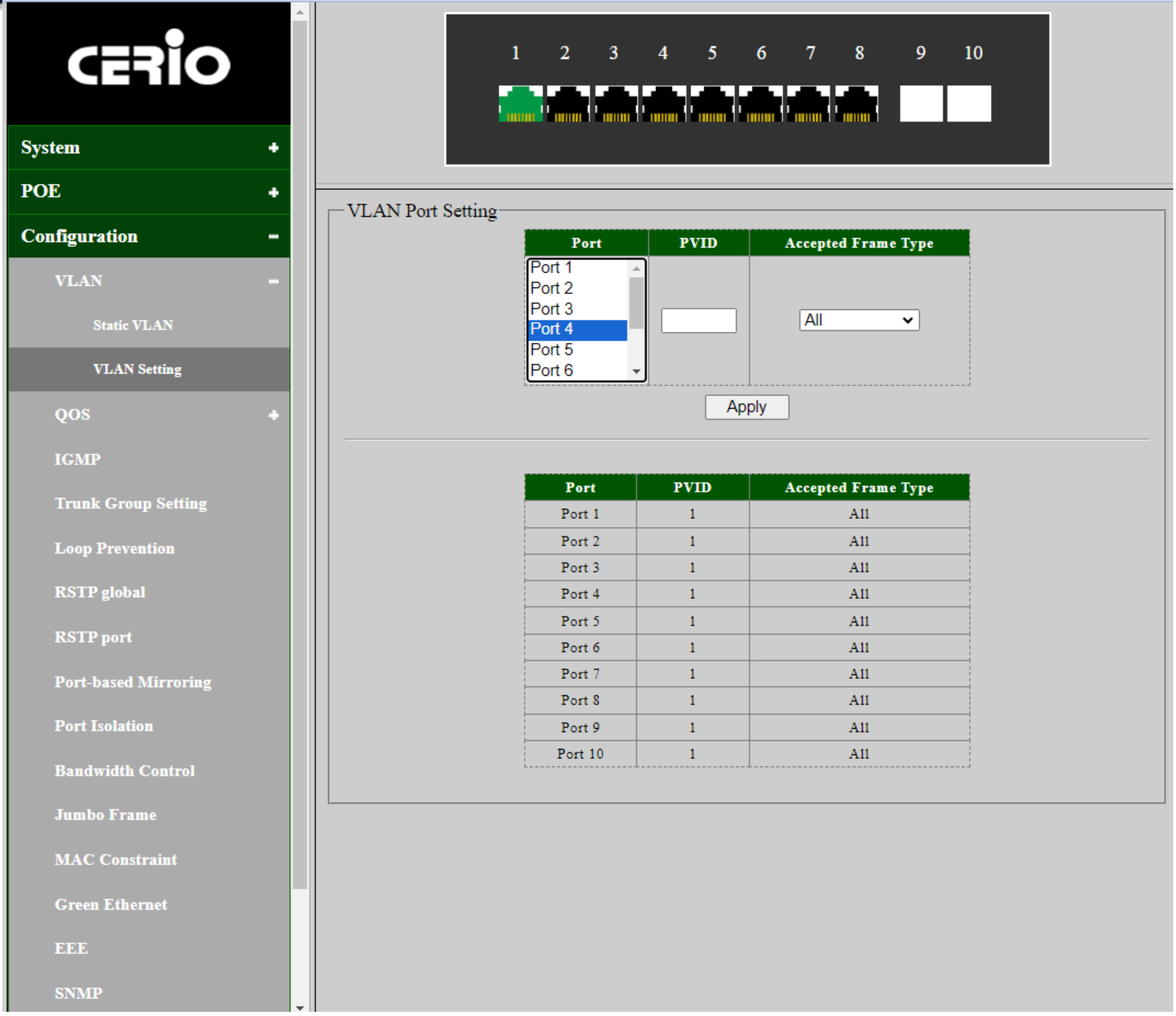
Before deleting a VLAN, you need to set the VID of the port using the VLAN back to the default value of 1. (Please make sure that in the VLAN settings, the PVID of the corresponding port to be deleted is changed back to the most basic default value) The value is "1".

Field	Description
VLAN ID	Displays the ID number of VLAN.
VLAN Name	Displays the name of VLAN.
Member Ports	Displays the port member in the VLAN.
Tagged Ports	Displays the tagged port members in the VLAN.
Untagged Ports	Displays the untagged port members in the VLAN.
Delete	Click Delete to remove some VLAN ID you selected before.
Select ALL	This helps to select all VLAN ID to be deleted at one time.

5.1.2 VLAN Setting (802.1Q)

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. If you have one unit/PC that you only want to use in VLAN2, then you set the connection port to VLAN2, and only that traffic will be send to that specific port.

Click on the navigation bar: **Configuration --> VLAN --> VLAN Settings**



VLAN Port Setting

Port	PVID	Accepted Frame Type
Port 1 Port 2 Port 3 Port 4 Port 5 Port 6		All

Port	PVID	Accepted Frame Type
Port 1	1	All
Port 2	1	All
Port 3	1	All
Port 4	1	All
Port 5	1	All
Port 6	1	All
Port 7	1	All
Port 8	1	All
Port 9	1	All
Port 10	1	All

- **"Ports:"** Multiple ports can be selected.
- **"PVID:"** Administrator can Enter a PVID number of the ports. It ranges from 1 to 4094. When adding the tag header to the received untagged packet, the switch will automatically uses this PVID value as the VLAN ID of the added tag.
- **"Accepted Frame Type:** Select the acceptable frame type for the port and the port will perform this operation before Ingress Checking.

  All : The port will accept both the tagged packets and the untagged packets.

  Tag-only: The port will accept the tagged packets only.

  Untag-only: The port will accept the untagged packets only.

Administrator has to hold "Ctrl" and the left button of the mouse to select the ports you need, and enter the PVID, select the Accepted Frame Type, "Apply" button to refresh the VLAN Port Setting.

Notice

You need to set the VLAN ID before setting the port VID VLAN ID is set for static VLAN, ranging from 1-4094.

Untagged port If Untagged port is selected, the output data frame does not have tag information. If the Tagged port is selected, the output dataframe will have tag information.

If no member port is selected, it means that the port is not a member port of VLAN.

Field	Description
Port	Displays the port number selected for configuration.
PVID	Displays the PVID number of the ports.
Accepted Frame Type	Displays the accepted frame type of the selected port.

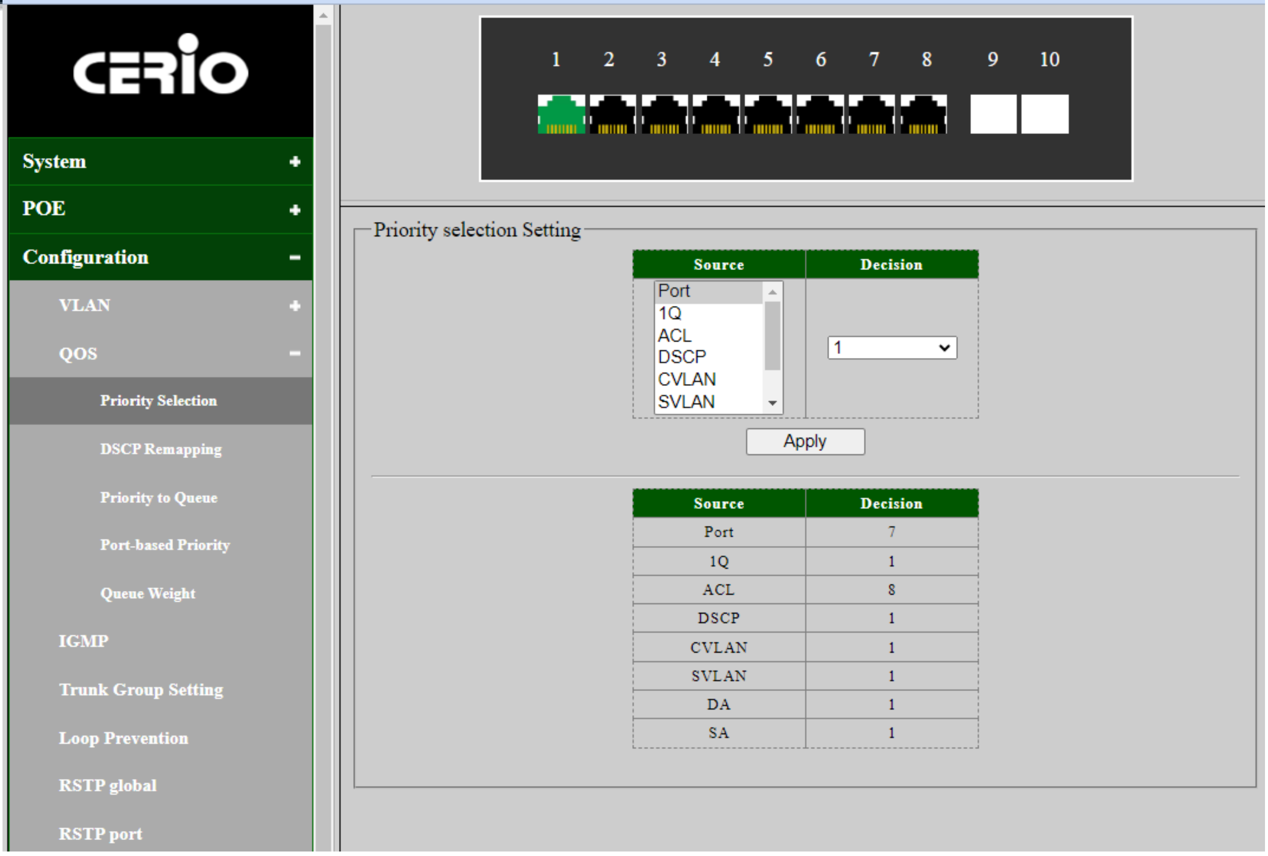
5.2 QoS

Quality of Service (QoS) prioritizes network traffic and manages available bandwidth so that the most important traffic goes first. QoS is implemented as rules or policies that prioritize packets, optionally change information in the packet header, and assign them to outbound port queues based on their priority.

5.2.1 Priority Selection

The priority selection setting page is used to configure the priority source weight. When the received packet is paired with multiple sources, the source with the highest weight will be selected to assign priority.

Click on the navigation bar: **Configuration > QOS > Priorities selection**



Priority selection Setting

Source	Decision
Port 1Q ACL DSCP CVLAN SVLAN	1

Source	Decision
Port	7
1Q	1
ACL	8
DSCP	1
CVLAN	1
SVLAN	1
DA	1
SA	1

- **"Source:"** Select and set the QoS priorities source. (Including Port, 1Q, ACL, DSCP, CVLAN, SVLAN, DA, SA)
- **"Decision:"** Priority order selection. priority (1-8) : Prioritize one child queue over other child queue. One is the highest, eight is the lowest priority. Child queue with higher priority will have chance to reach its max-limit before child with lower priority.

Administrator has to click the "Apply" button to refresh the Priority Selection Setting.

Field	Description
Source	Displays the source list.
Decision	Displays the priority order selection decision.

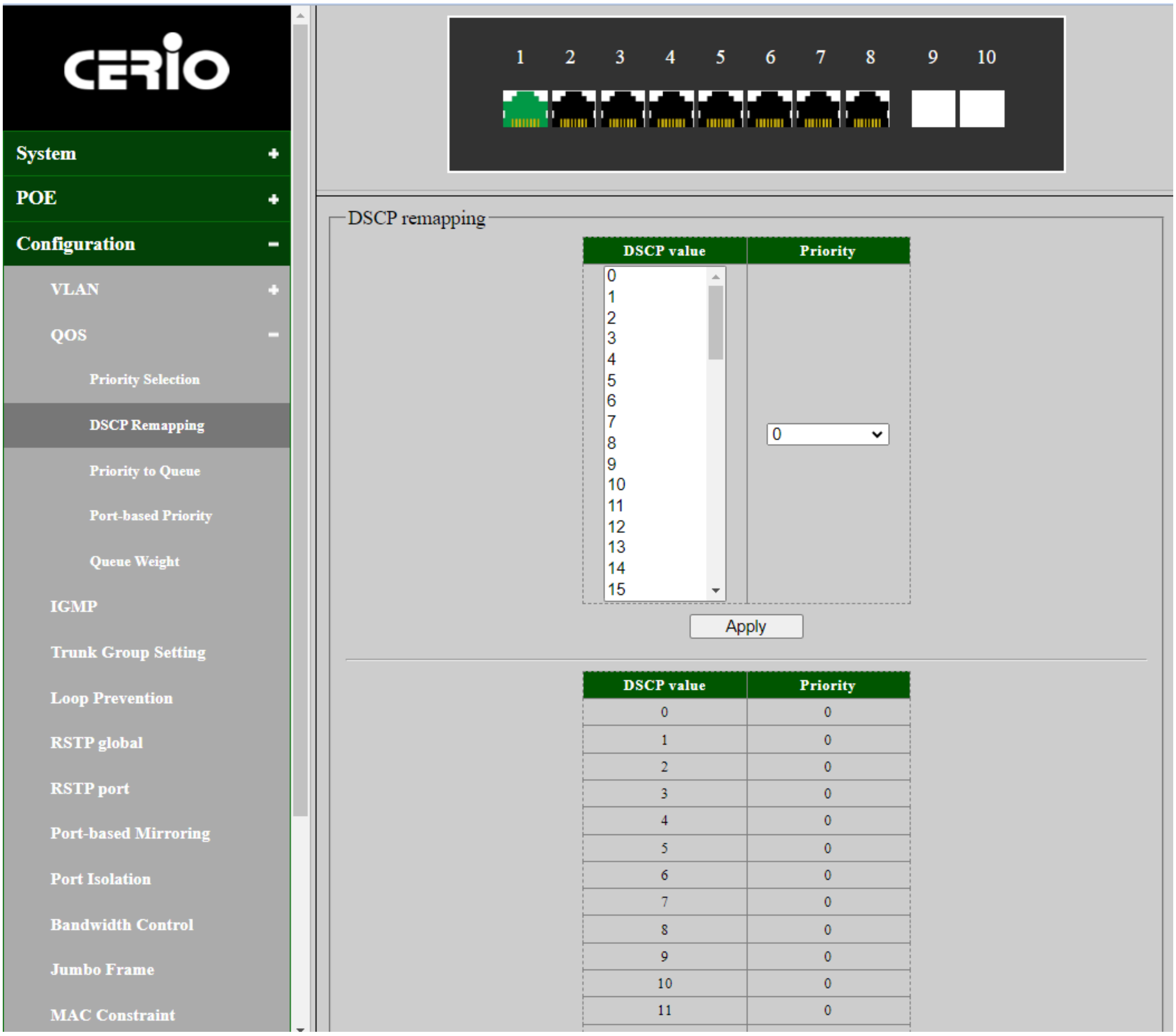
Notice

Priority selection sets the priority of the priority source, specifying the transmission queue for the frame based on the highest priority source.

5.2.2 DSCP Remapping

The DSCP remapping settings page is used to configure the internal priority mapping based on DSCP priority.This DSCP values range from 0 through 63, whereas the internal forwarding priority values range from 0 through 7. Any DSCP value within a given range is mapped to the same internal forwarding priority value. These include the CS (Class Selector), AF (Assured Forwarding) and EF (Expedited Forwarding). For example, a packet with a DSCP tag value of 1 can be assigned to the High queue.Use the Queues to DSCP page to remark DSCP value for egress traffic from each queue.

Click on the navigation bar: **Configure --> QOS --> DSCP Remapping**



DSCP remapping

DSCP value	Priority
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	0

DSCP value	Priority
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0

- **"DSCP value:"** Select and set the DSCP value of "0-63".

- **"Priority:"** Priority order selection of "0-7"level .

Administrator has to click the "Apply" button to refresh the DSCP Remapping Setting.

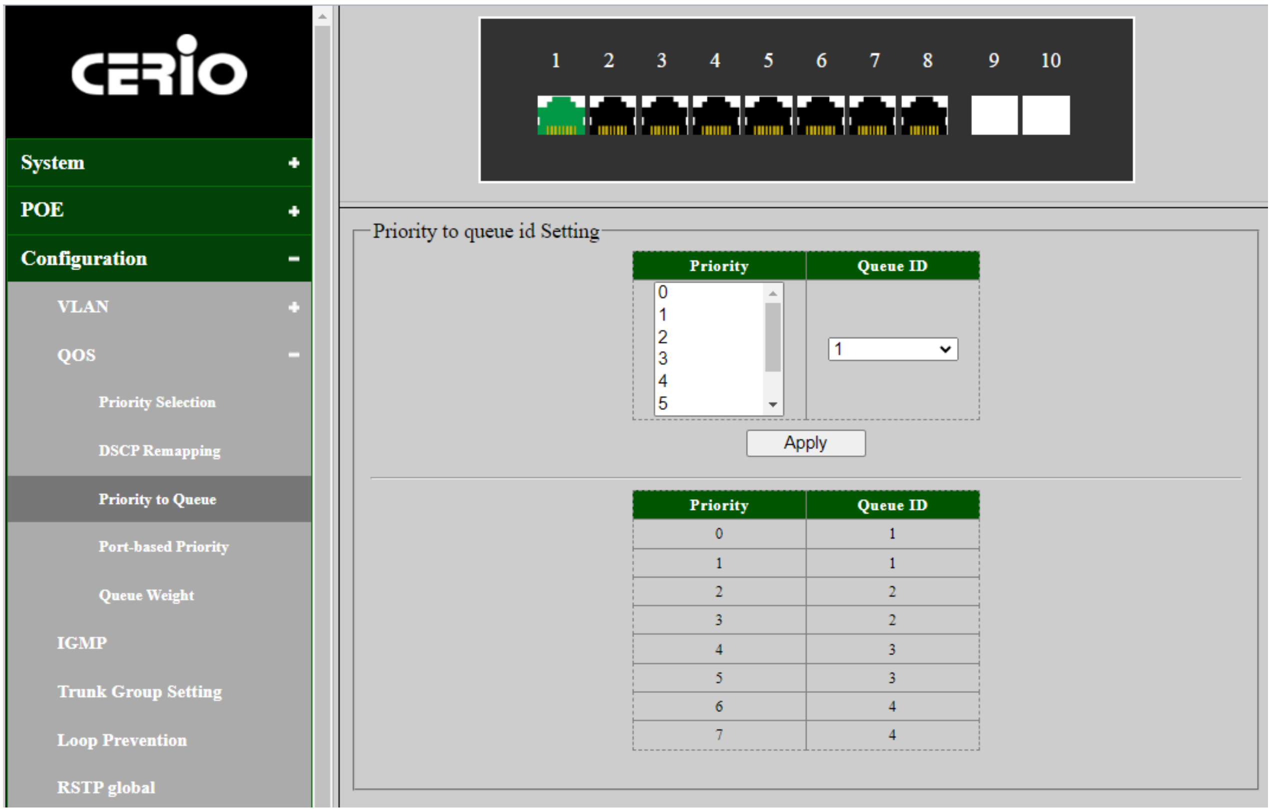
Notice Map DSCP values to internal priorities.

Field	Description
DSCP value	Displays the DSCP values.
Priority	Displays the internal forwarding priority values.

5.2.3 Priority to Queue

The priority queue ID setting page is used to configure the internal priority to queue mapping. Map different priorities to different queues (1-4 queues)

Click on the navigation bar: **Configure -> QOS -> Priority to Queue**



Priority to queue id Setting

Priority	Queue ID
0 1 2 3 4 5	1

Priority	Queue ID
0	1
1	1
2	2
3	2
4	3
5	3
6	4
7	4

The priority to queue can manually map the ingress packets of the port to four different priority queues. A higher priority transmits data with a minimum of delays. This switch allows user to select among four levels Queue ID (lowest, medium, normal, highest). Please set your priority to the corresponding Queue ID.

- **"Priority:"** Select and set the 0~7 CoS priority Queue.
- **"Queue ID:"** Priority order selection. The priorities are labeled as 1~4 and among them the bigger the value, the higher the priority.

CoS (0 to 7) 7 is highest	Description	Queue ID(1 to 4) 4 is highest priority	Description
0	Background, etc	1 (Lowest Priority)	background data
1	Best Effort, etc	2 (Normal Priority)	business-critical data, email, internet, etc
2	Excellent Effort	3 (Medium Priority)	stream multimedia, etc
3	Critical Application LVS phone SIP, etc	4 (Highest Priority)	interactive voice, video, and delay sensitive data
4	Video, etc		
5	Voice IP phone default, etc		
6	Interwork Control LVS phone RTP, etc		
7	Network Control, etc		

Administrator has to click the "Apply" button to refresh the Priority to queue id Setting.

Notice

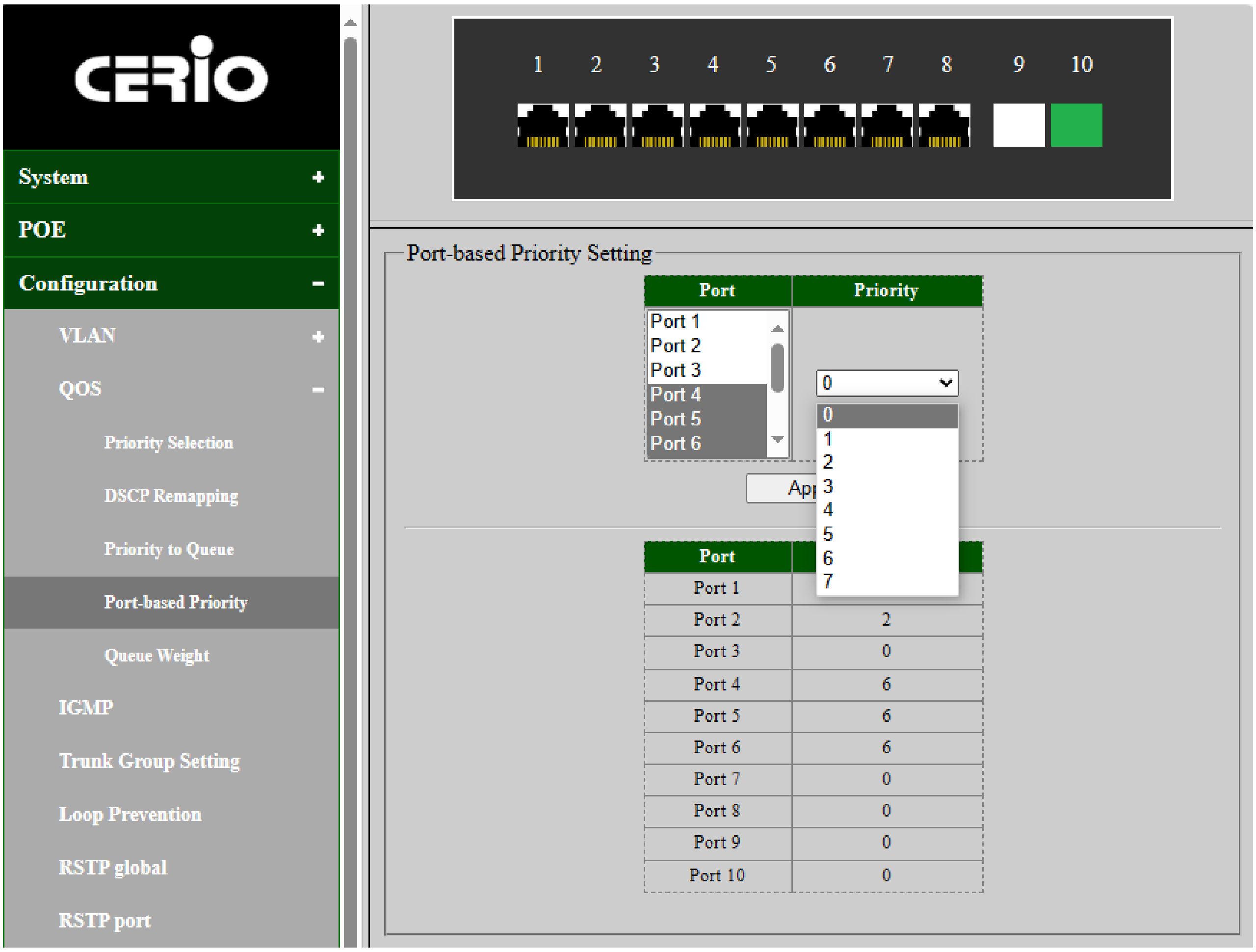
The priorities of Queue ID are labeled as 1~4 and among them the bigger the value, the higher the priority.
The priorities of Cos are labeled as 0~7 and among them the bigger the value, the higher the priority.

Field	Description
Priority	Displays the status status.
Queue ID	Displays the Queue ID status.

5.2.4 Port-based Priority

The Port-based priority QoS can manually map the ingress packets of the port to four different priority queues. A higher priority transmits data with a minimum of delays. This switch allows user to select among four levels (lowest, medium, normal, highest)
According to the IEEE 802.1p, users can define each value from 0 to 7 CoS value in 4 priority queues (0~7 CoS 8-level "priority" to 4 "Queue") : from Lowest to Normal, Medium,and Highest.

Click on the navigation bar: **Configuration -> QOS -> Port-based Priority**



Port-based Priority Setting

Port	Priority
Port 1 Port 2 Port 3 Port 4 Port 5 Port 6	0

Port	
Port 1	
Port 2	2
Port 3	0
Port 4	6
Port 5	6
Port 6	6
Port 7	0
Port 8	0
Port 9	0
Port 10	0

Port-based priority QoS allows you to assign a priority level to each of the 10 ports, Configure the priority of each port. Select the port from the left, then choose a priority level from the drop down list on the right, After selecting items 0~7 from the drop-down list of the above priority, you can use this control item to set the queuing policy for each connection port.

- **"Port:"** Select the desired port for configuration , It is multi-optional, you can choose Ten ports at most at a time, Indicate port 1 to port 10.
- **"Priority:"** Specify the priority queue the packets from the port are mapped to priorities queue, Each port has 8 priority levels—0~7 or Disable to be chosen.7 is the highest priority.

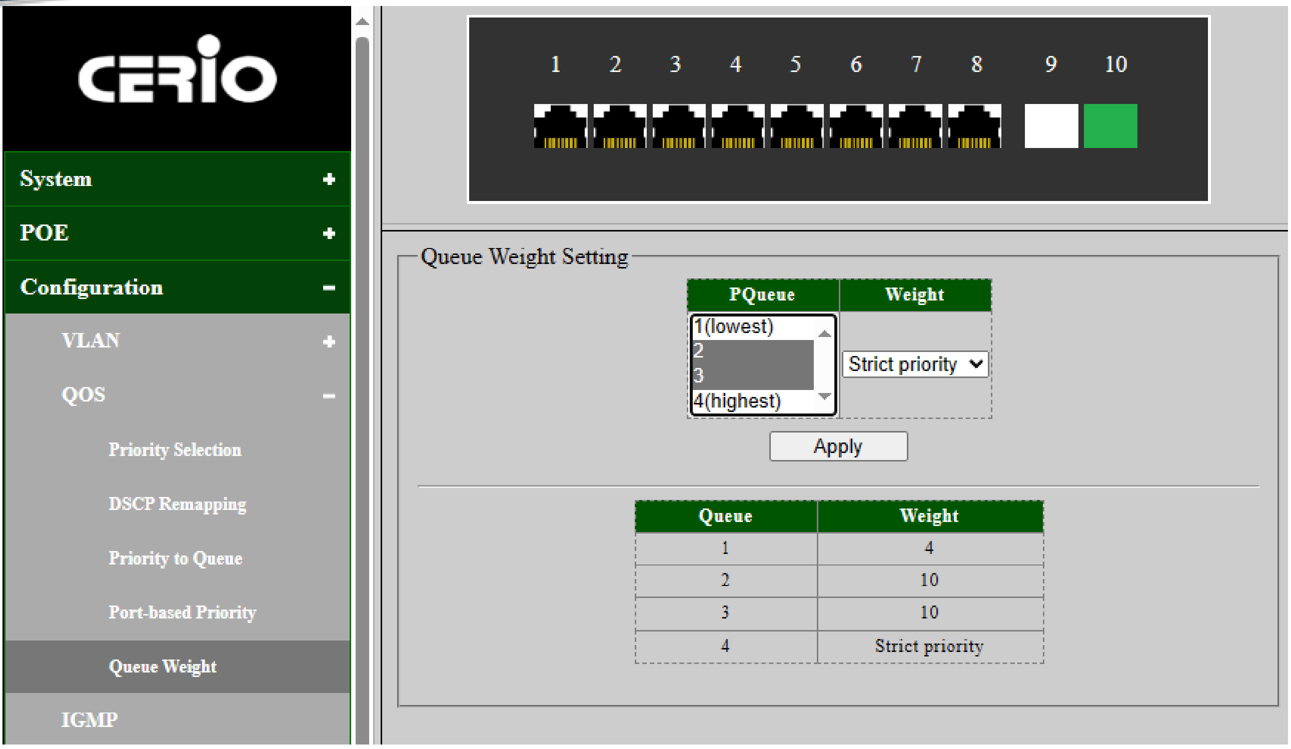
Administrator has to hold "Ctrl" and the left button of the mouse to select the ports you that you want to have a particular priority. Select the priority level and click the "Apply" button to refresh the Port-based Priority Setting

Field	Description
Port	Displays the port number of the switch.
Priority Queue	Displays the priority queue of all ports.

5.2.5 Queue Weight

The queue weight page is used to configure the weight of queue priority algorithm,
Set the queue weights so that different queues get different scheduling priorities.

Click on the navigation bar: **Configure --> QOS --> Queue Weight**



Queue Weight Setting

PQueue	Weight

1(lowest)
2
3
4(highest)
	Strict priority

Queue	Weight
1	4
2	10
3	10
4	Strict priority

- **"PQueue:" (Priority Queue)** Select the desired port for configuration, Priority Queue levels are: 1. lowest, 2. medium, 3. normal, and 4. highest.
- **"Weight:"** Administrator can select Strict Priority or Priority 1-15.

Administrator has to click the "Apply" button to refresh the Queue Weight Setting.

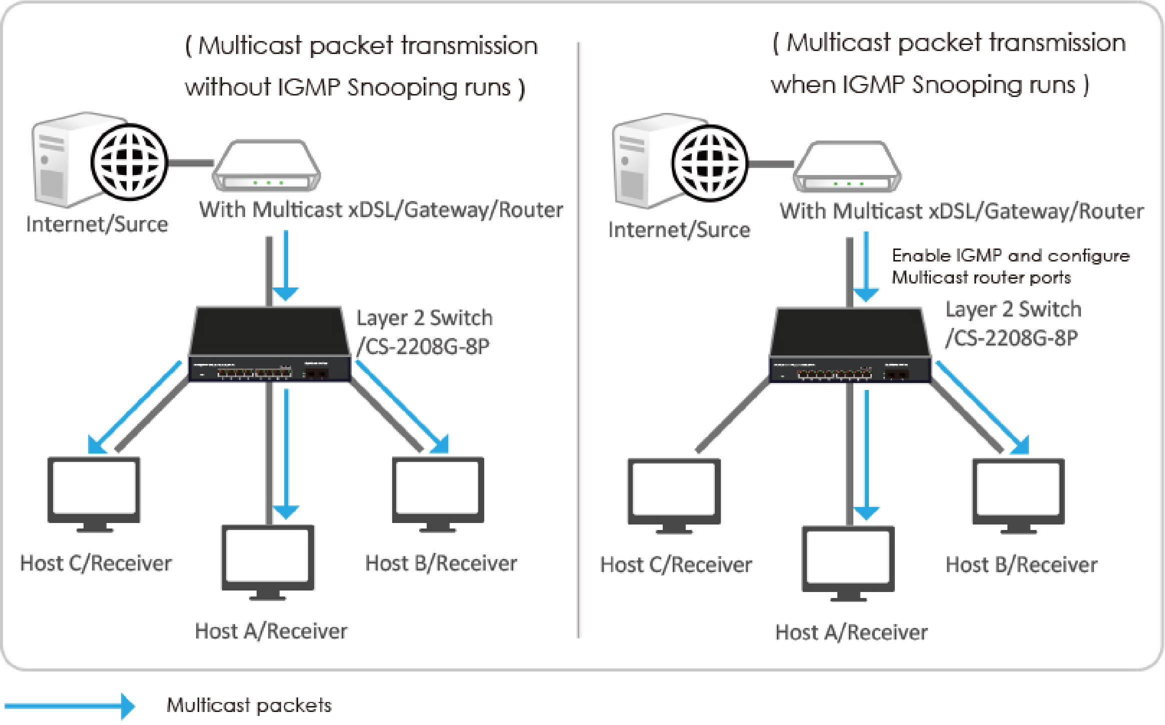
Field	Description
Queue	Displays the priority queue ID status.
Weight	Displays the weight status.

5.3 IGMP

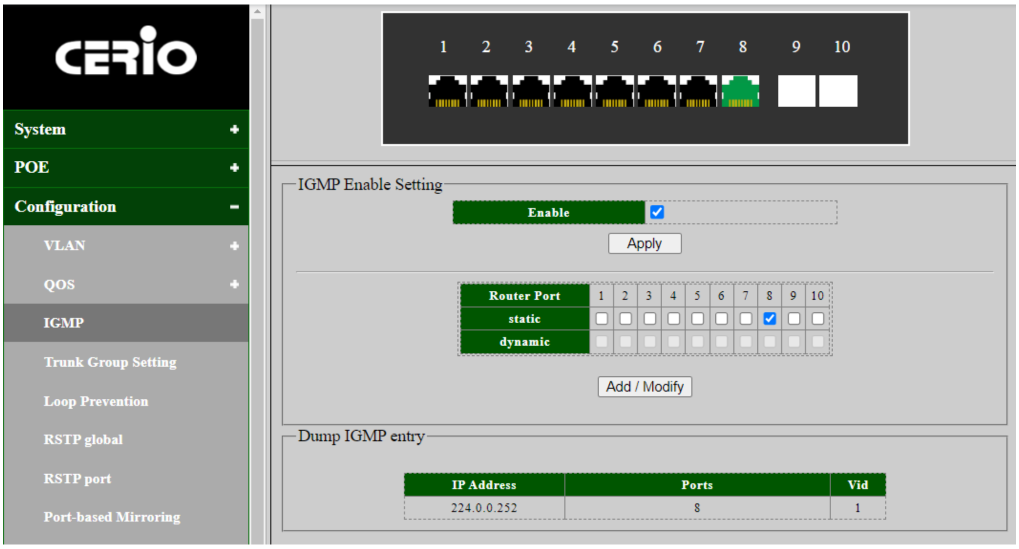
Administrators can use this section to create IGMP snooping profiles. Internet Group Management Protocol (IGMP) Snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch,This feature that allows a Layer 2 switch to "listen in" on the IGMP conversation between hosts and routers by processing the layer3 IGMP packets that are sent over a multicast network.

Host Extensions for IP Multicasting [RFC1112] specifies the extensions required of a host implementation of the Internet Protocol (IP) to support multicasting. Multicast IP traffic is traffic sent to a group of hosts. Host groups are identified by Class D IP addresses, ranging from 224.0.0.0 to 239.255.255.255. Based on IGMP query and report messages, the switch forwards traffic only to the port that requested multicast traffic.

When IGMP snooping is enabled on a switch, it analyzes all IGMP packets between hosts connected to the switch and multicast routers in the network. When the switch hears an IGMP report from a host in a given multicast group, the switch adds the host's port number to the group's multiplay list. This prevents the switch from broadcasting the traffic to all ports and possibly affecting network performance.


(Multicast packet transmission without IGMP Snooping runs)
Internet/Surce
With Multicast xDSL/Gateway/Router
Layer 2 Switch /CS-2208G-8P
Host C/Receiver
Host B/Receiver
Host A/Receiver
(Multicast packet transmission when IGMP Snooping runs)
Internet/Surce
With Multicast xDSL/Gateway/Router
Enable IGMP and configure Multicast router ports
Layer 2 Switch /CS-2208G-8P
Host C/Receiver
Host B/Receiver
Host A/Receiver
Multicast packets

Click on the navigation bar: **Configuration --> IGMP**



IGMP Enable Setting

Enable ☑

Apply

Router Port	1	2	3	4	5	6	7	8	9	10
static	□	□	□	□	□	□	□	☑	□	□
dynamic	□	□	□	□	□	□	□	□	□	□

Add / Modify

Dump IGMP entry

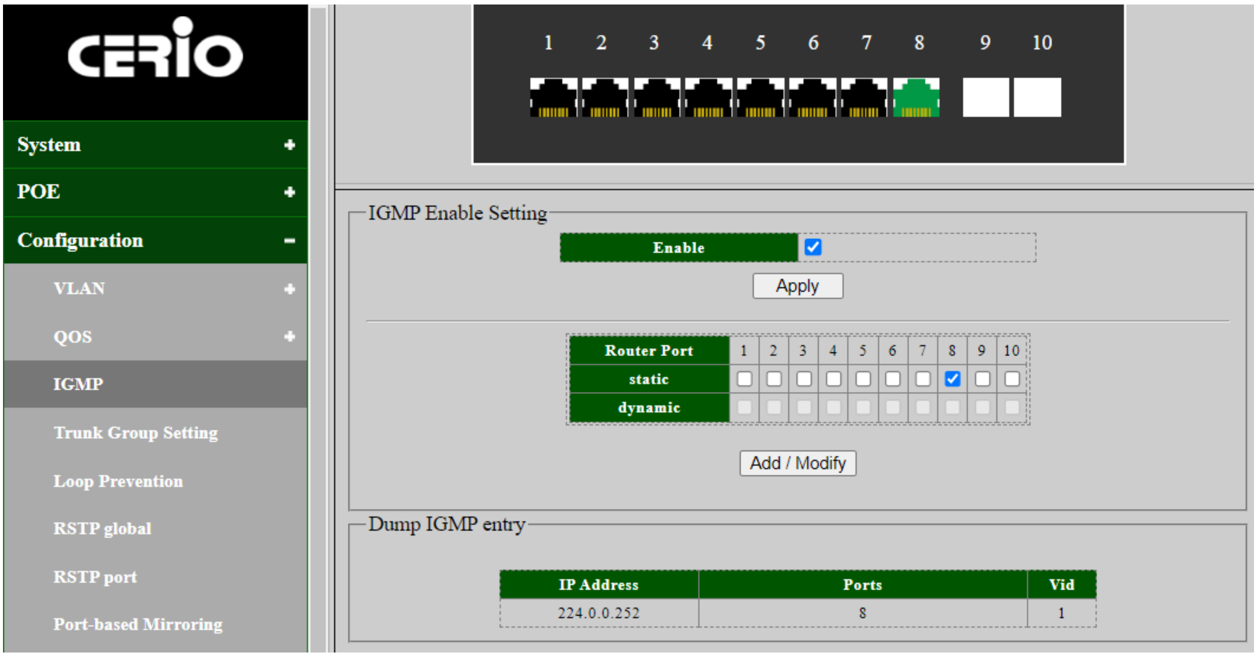
IP Address	Ports	Vid
224.0.0.252	8	1

IGMP Enable Setting :

Administrator can enable or disable IGMP Snooping on this screen, When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic.

Administrator has to click the “Apply” button to refresh the IGMP Enable Setting.

- **Add entries to the "dump IGMP entry" with the following option settings , Set if ports are connecting to the IGMP administrative routers.**



IGMP Enable Setting

Enable ☑

Apply

Router Port	1	2	3	4	5	6	7	8	9	10
static	□	□	□	□	□	□	□	☑	□	□
dynamic	□	□	□	□	□	□	□	□	□	□

Add / Modify

Dump IGMP entry

IP Address	Ports	Vid
224.0.0.252	8	1

- **“Router Port:”** Configure the router port by selecting ports.
- **“static:”** Select a static port on which to snoop,   or one of ports 1-10 ports. .
- **“dynamic:”** It is dynamically learned by IGMP snooping. After specifying and selecting IGMP Snooping static, IP multicast will be learned dynamically and automatically. (Default values are always learned).

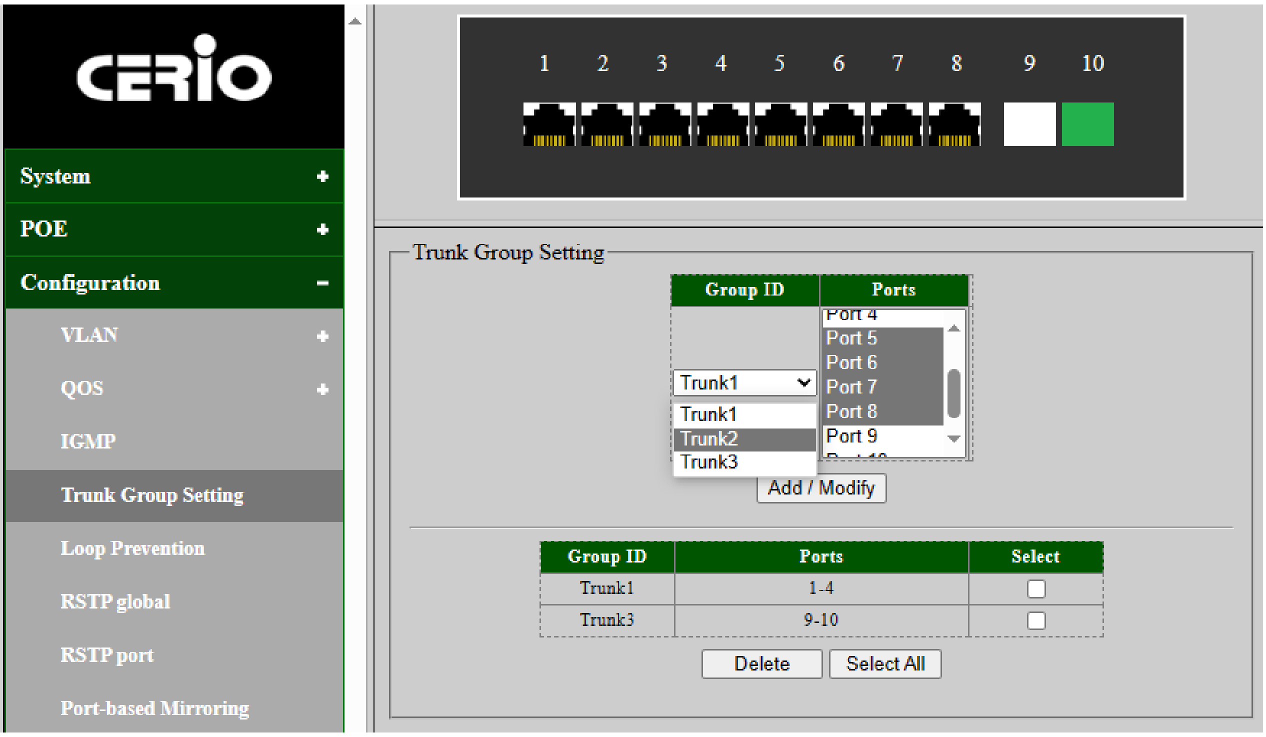
Administrator has to click the “Apply and Modify” button to refresh the “IGMP Router Port” Setting.

Field	Description
IP Address	Displays IP Address View the multicast IP address.
Ports	Displays the Ports View a list of multicast group ports.
Vid	Displays VID to view the VLAN ID corresponding to the multicast group.

5.4 Link Aggregation (Trunk Group Setting)

The function supports Link Aggregation Control Protocol.
Link Aggregation Control Protocol (LACP) can aggregate multiple Ethernet ports together to form a logical aggregation group. To upper layer entities, all the physical links in an aggregation group are a single logical link.

Click on the navigation bar: **Configuration --> Trunk Group Setting**



Group ID	Ports
Trunk1 Trunk1 Trunk2 Trunk3	Port 4 Port 5 Port 6 Port 7 Port 8 Port 9

Group ID	Ports	Select
Trunk1	1-4	□
Trunk3	9-10	□

- **"Group ID:"** Select the Trunk1 or Trunk2 or Trunk3 Group ID .
- **"Ports:"** Select ports for trunk group setting,It is multi-optional, administrator can choose Trunk1 for 1-4 ports or Trunk2 for 5-8 ports or Trunk3 for 9-10 ports or at most at a time. Click **Add/Modify,** the administrator can view the UI page following port parameters.

Notice

Total supports three group
Trunk1 and two ports from port 1 to port 4.
Trunk2 and two ports from port 5 to port 8.
Trunk3 and one ports from port 9 to port 10.

Notice

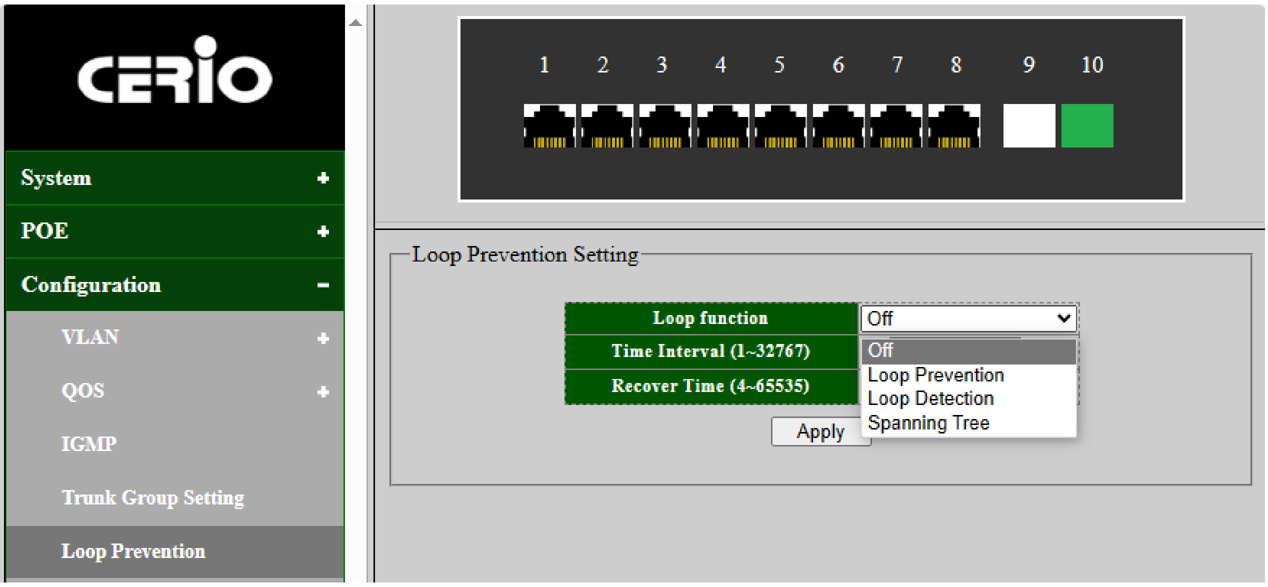
For the member ports in a trunk group, their configuration of port setting & QoS must be the same.

Field	Description
Group ID	Displays the Trunk Group as Trunk1 or Trunk2 or Trunk3.
Ports	Displays the Trunk member ports.
Select	Select and enable the Trunk Group.
Select All	Click Select All to select and enable the Trunk Group.
Delete	Click Delete to delete the Trunk Group.

5.5 Loop Prevention

The loop is the topology of the switch connected to the network to form a ring. The loop will cause a broadcast storm in the internal network, which will consume a lot of CPU and line bandwidth of the switch. In serious cases, it can even cause equipment to crash and the network to be paralyzed. The switch can detect loops using loop detection packets. The POE Switch can detect loops in your network. The loop detection feature is designed to detect loops and activate loop flash detection on the green LED to the right of RJ45 on the front panel of the switch. The loop prevention feature, on the other hand, blocks any port that has been deemed to be causing a loop automatically.

Click on the navigation bar: **Configuration - -> Loop Prevention Setting**



Loop Prevention Setting

Loop function	Off
Time Interval (1~32767)	
Recover Time (4~65535)	

Notice Loop Prevention function can be supported only if trunk Group setting disable.

- **"Loop function :"** There are four modes for you to choose:

    - **Off:** Administrator can disable loop detection or prevention or Spanning Tree function.
    - **Loop Detection:** Administrator can select used loop detection mode to detect network situation. (A loop port occurrence will be identified by the flashing of the ACT/LINK light on the RJ45 Ethernet connector), When it detects a loop, this feature does not repair the loop, but only issues a warning.
    - **Loop Prevention:** Administrator can select used loop Prevention mode to prevent network looping. When Loop Prevention function is used.
        - ✓ **Port:** Select the desired port for loop prevention configuration. It is multi-optional, administrator can choose Ten ports at most at a time.
        - ✓ **State:** Enable or Disable loop prevention for the selected port.
    - **Spanning Tree:** Administrators can select this spanning tree mode to resolve network loops. When using the spanning tree function. "RSTP global" will be automatically enabled.
- **"Time intervals :"** Administrator can set the loop time intervals for 1~32767 sec**.**
- **"Recovery Time :"** Administrator can set the loop recovery timefor 4~65535 sec**.**

Administrator has to click the "Apply" button to refresh the Loop Prevention Setting.

Administrators can choose to use spanning tree mode to resolve network loops. When using the spanning tree function. "RSTP global" will be automatically enabled

Loop Detection Enable loop detection. When it detects a loop, this feature does not repair the loop, but only issues a warning.

Loop Prevention Enable loop prevention. When it detects a loop, this feature will disable loop ports and down port LED, and the system LED will be blinking.

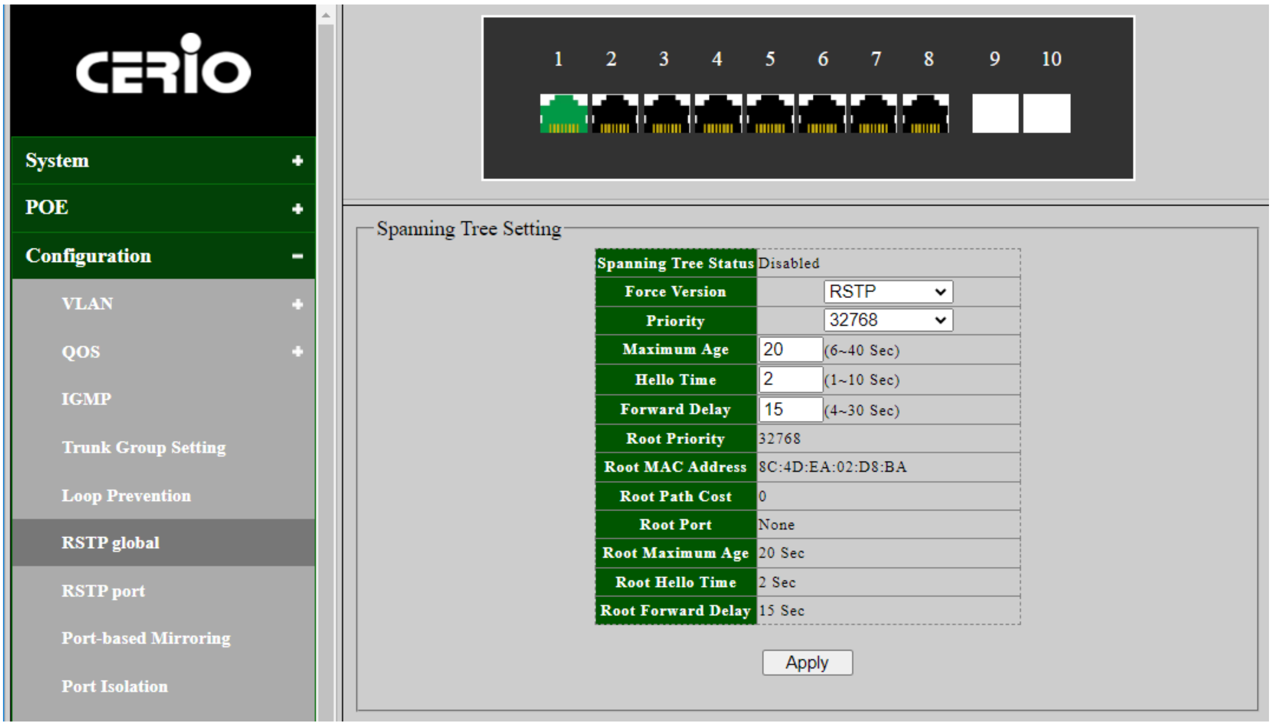
.

Notice The recovery time monitors the network loop at this time interval When the loop is found, the switch will initiate the processing mechanism, and the port will automatically return to normal after this time.

5.6 RSTP global (Rapid Spanning tree)

Spanning Tree function allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail. If Spanning Tree costs change, or if one network segment in the Spanning Tree becomes unreachable, the spanning tree algorithm reconfigures the spanning tree topology and reestablishes the link by activating the standby path. Without spanning tree in place, it is possible that both connections may be simultaneously live, which could result in an endless loop of traffic on the LAN.

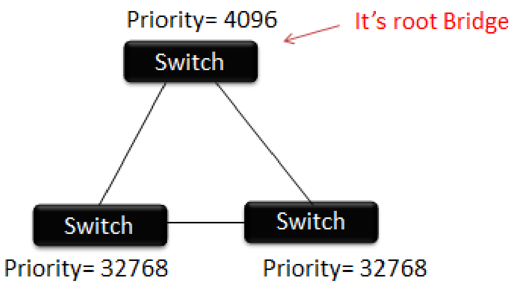
Click on the navigation bar: **Configuration --> RSTP Global (Spanning Tree Setting)**

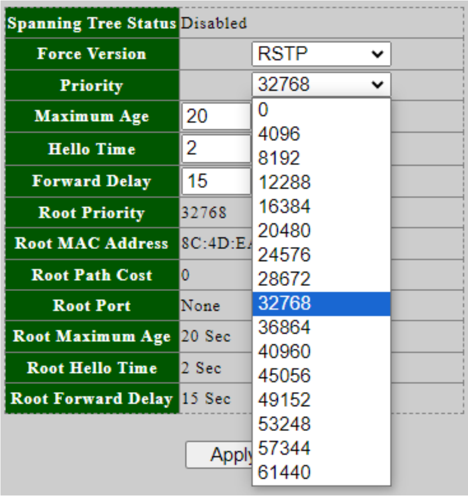


Spanning Tree Setting

Spanning Tree Status	Disabled	
Force Version	RSTP	
Priority	32768	
Maximum Age	20	(6~40 Sec)
Hello Time	2	(1~10 Sec)
Forward Delay	15	(4~30 Sec)
Root Priority	32768	
Root MAC Address	8C:4D:EA:02:D8:BA	
Root Path Cost	0	
Root Port	None	
Root Maximum Age	20 Sec	
Root Hello Time	2 Sec	
Root Forward Delay	15 Sec	

- **Spanning Tree Status :** displays enabled or disabled status. This enabled function through the Loop Prevention configuration to option.
- **"Force Version :"** The spanning tree (RSTP) version in use.
- **"Priority :"** Administrator can set bridge priority, default is 32768. The lower value (priority) is the root bridge. Specify the bridge priority. The valid range is from 0 to 61440, and the value should be the multiple of 4096. (total of 16 levels can be selected). 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.





Spanning Tree Status	Disabled
Force Version	RSTP
Priority	32768
Maximum Age	20
Hello Time	2
Forward Delay	15
Root Priority	32768
Root MAC Address	8C:4D:E
Root Path Cost	0
Root Port	None
Root Maximum Age	20 Sec
Root Hello Time	2 Sec
Root Forward Delay	15 Sec

- ➢ **"Maximum Age :"** The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. That also means the maximum life time for a BPDU frame. Number between 6-40.
- ➢ **"Hello Time :"** The hello time is the time between each bridge protocol data unit (BPDU) that is sent on a port. This time is equal to 2 seconds (sec) by default, but administrator can tune the time to be between 1 and 10 sec.
- ➢ **"Forward delay :"** The maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). Number between 4 – 30**.**

Administrator has to click the "Apply" button to refresh the RSTP global (Spanning tree)Setting.

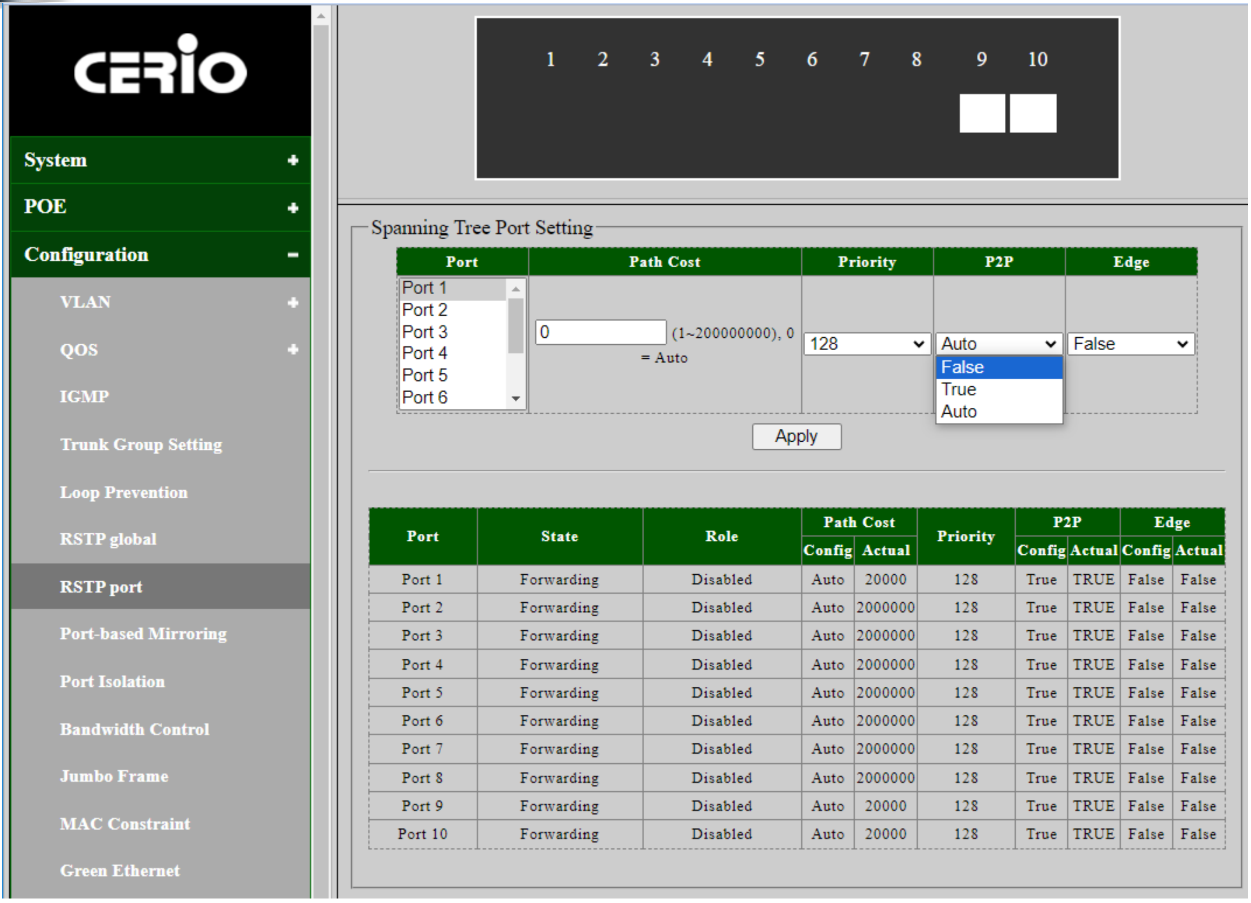
Notice

Maximum Age / Forward delay : 2*(Forward Delay-1) >= Max Age >= 2*(Hello Time+1), the time interval in seconds for a switch to wait the configuration messages, without attempting to redefine its own configuration.

5.7 RSTP Port (Rapid Spanning tree Port)

STP port summary page is used to display port STP summary information, including port, STP enable, role and status.

Click on the navigation bar: **Configuration --> RSTP Port (Spanning Tree Port Setting)**



Spanning Tree Port Setting

Port	Path Cost	Priority	P2P	Edge
Port 1 Port 2 Port 3 Port 4 Port 5 Port 6	0 (1~200000000), 0 = Auto	128	Auto False True Auto	False

Port	State	Role	Path Cost		Priority	P2P		Edge	
			Config	Actual		Config	Actual	Config	Actual
Port 1	Forwarding	Disabled	Auto	20000	128	True	TRUE	False	False
Port 2	Forwarding	Disabled	Auto	2000000	128	True	TRUE	False	False
Port 3	Forwarding	Disabled	Auto	2000000	128	True	TRUE	False	False
Port 4	Forwarding	Disabled	Auto	2000000	128	True	TRUE	False	False
Port 5	Forwarding	Disabled	Auto	2000000	128	True	TRUE	False	False
Port 6	Forwarding	Disabled	Auto	2000000	128	True	TRUE	False	False
Port 7	Forwarding	Disabled	Auto	2000000	128	True	TRUE	False	False
Port 8	Forwarding	Disabled	Auto	2000000	128	True	TRUE	False	False
Port 9	Forwarding	Disabled	Auto	20000	128	True	TRUE	False	False
Port 10	Forwarding	Disabled	Auto	20000	128	True	TRUE	False	False

- **"Port :"** Select the port to be configured.
- **"Path Cost :"** Path Cost (1-200000000) This parameter is used determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short, the maximum path cost is 65,535. Range: 1-200000000, (set 0 = Auto, default is 0).
- **"Priority :"** If the path cost for all ports on a switch is the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. Range: 0-240, default is 128.
- **"P2P :"** Specify the Point-to-Point port configuration.
  - **False:** Force to false state.
  - **True:** Force to true state.
  - **Auto:** The state is depended on the duplex setting of the port.

- **"Edge :"** Expect the port to be an edge port (linking to an end station) or a link to another STP device..

- **False:** Force to false state(as link to a bridge).
- **True:** Force to true state(as link to a host).

Administrator has to click the “Apply” button to refresh the RSTP Port (Spanning Tree Port) Setting.

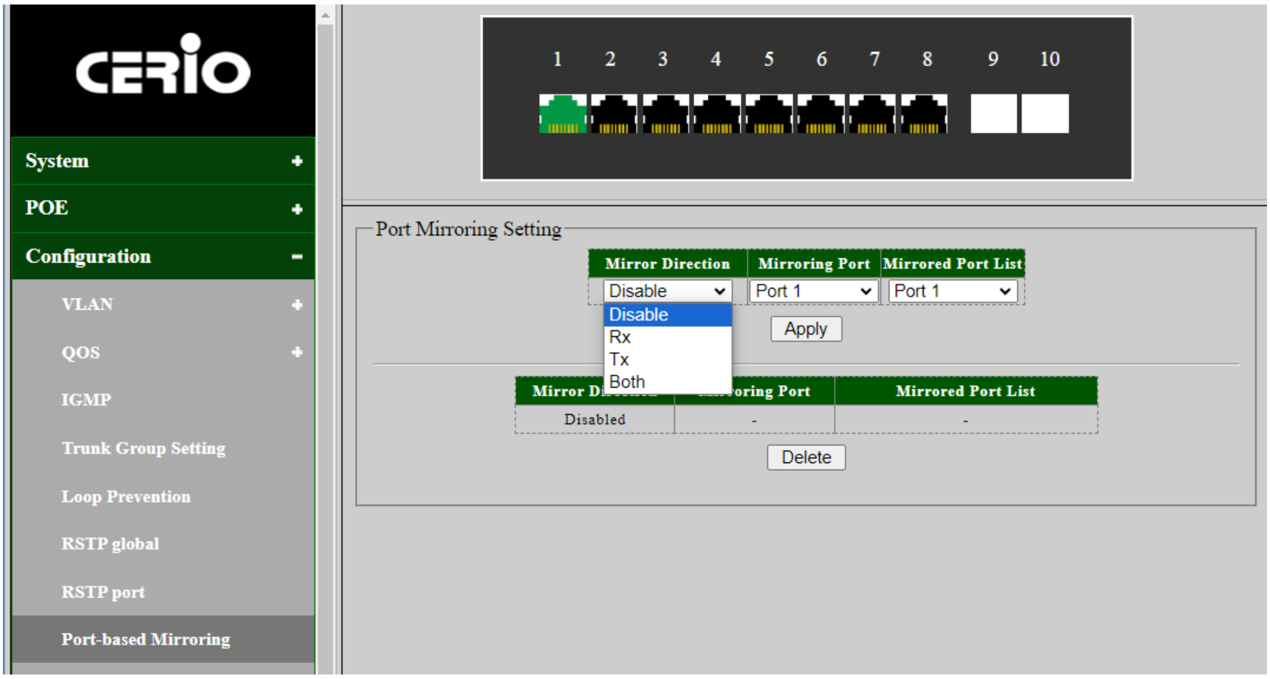
Notice	In the edge mode, the interface would be put into the Forwarding state immediately upon link up. If the edge mode is enabled for the interface and there are BPDUs received on the interface, the loop might be occurred in the short time before the STP state change.

Field	Description
Port	Specify the interface ID or the list of interface IDs.
State	The current port state on the specified port. The possible values are: “Disabled”, “Discarding”, “Learning”, and “Forwarding”.
Role	The current port role on the specified port. The possible values are: “Disabled”, “Master”, “Root”, “Designated”, “Alternative”, and “Backup”
Path Cost	STP path cost on the specified port.
Priority	STP priority on the specified port.
P2P	The operational point-to-point status on the specified port.
Edge	The operational edge port status on the specified port.

5.8 Port-based Mirroring

Port mirroring function can mirror the traffic of Ingress(Rx)/Egress(Tx) packets, and so can mirror the destination port for analyzing. Port mirroring is used on a switch to send a copy of network packets of a port or ports to a network monitoring connection on another port, is to monitor and mirror network traffic by forwarding copies of incoming and outgoing packets from one port (mirrored port) to a specific port (mirroring port).

Click on the navigation bar: **Configuration --> Port-based Mirroring**



Port Mirroring Setting

Mirror Direction	Mirroring Port	Mirrored Port List
Disable	Port 1	Port 1

Mirror Direction	Mirroring Port	Mirrored Port List
Disabled	-	-

- ➢ **“Mirror Direction :”** Select mirror direction to select as below four items to mirror selected port for forwarding packets.
  - ● **Disable:** Disable the Ingress or Egress traffic.
  - ● **Rx:** Received/Ingress traffic.
  - ● **Tx:** Transmitted/Egress traffic.
  - ● **Both:** Transmitted/Egress and received/Ingress traffic.
- ➢ **“Mirroring Port :”** Select a port as the mirroring port. Define which port will output the mirrored traffic. This is the port to which you connect your monitoring station.
- ➢ **“Mirroed Port List :”** Select a port as the mirrored port. It is multiple ports can be selected. The mirrored port to be monitored. And Define which of the Ten ports you wish to mirror the traffic for.

Administrator has to click the “Apply” button to refresh the Port-based Mirroring Setting.

Notice

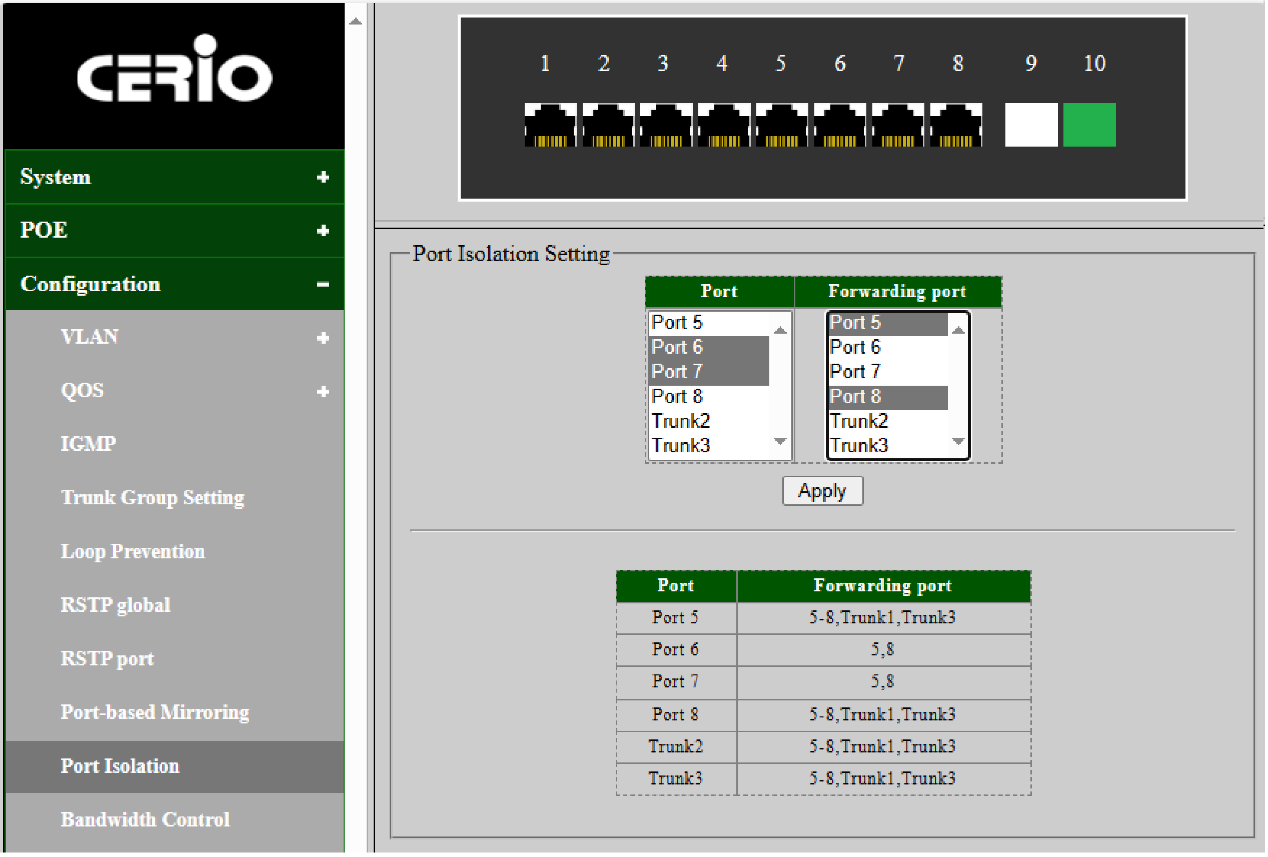
That the mirrored port cannot be the same as the mirroring port, Administrator can only create one port mirroring rule at a time, Administrator can only mirror the contents from one port to one other port, but not mirror the contents of multiple ports.

Field	Description
Mirror Direction	Display the select port mirror direction: disable/rx/tx/both four items.
Mirroring Port	Display the select mirror session port to operate monitoring status.
Mirrored Port List	Display the select mirrored port to be monitored status.
Delete	Click Delete to remove port mirror setting.

5.9 Port isolation

The port isolation setting page is used to configure and show port isolation.
By using port isolation function, administrator can achieve the goal of preventing PCs under different ports communicating with each other without configuring VLAN.
Both VLAN and port isolation are used to make part of devices independent in a space for protection, but VLAN is used to isolate broadcast, and the IP segment of users in the same VLAN is the same and share the data. If make the port isolation, they can not communicate even if they are in the same IP segment..

Click on the navigation bar: **Configuration --> Port Isolation**



Port Isolation Setting

Port	Forwarding port
Port 5 Port 6 Port 7 Port 8 Trunk2 Trunk3	Port 5 Port 6 Port 7 Port 8 Trunk2 Trunk3

Port	Forwarding port
Port 5	5-8,Trunk1,Trunk3
Port 6	5,8
Port 7	5,8
Port 8	5-8,Trunk1,Trunk3
Trunk2	5-8,Trunk1,Trunk3
Trunk3	5-8,Trunk1,Trunk3

- **"Port:"** Select the port(Source port) to be configured, It is multi-optional, you can choose Ten ports at most at a time.
- **"Forwarding Port :"** Select the port to which packets from port(source port)can be forwarded.

Administrator has to click the "Apply" button to refresh the Port isolation Setting.

Notice

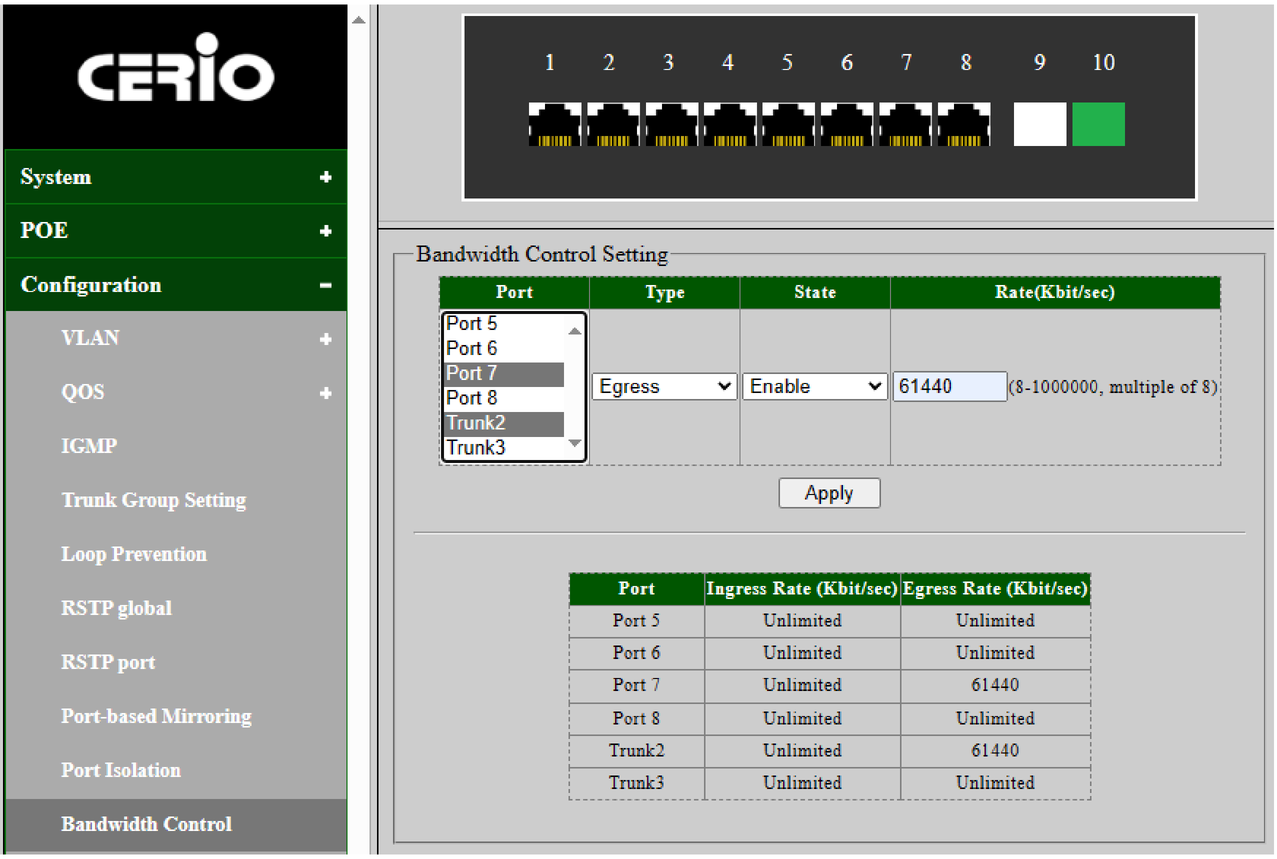
Packets received by the source port cannot be forwarded to a port that is not in the forwarding port, Since communication is two-way, if you want the host under port 1 to communicate with the host under port 2, you need to set the forwarding port list of port1 to allow port 2 and the forwarding port list of port 2 to allow at the same time. Port 1.

Field	Description
Port	Display the Port name which the port isolation.
Forwarding Port	Display the Port for packets forwarded status.

5.10 Bandwidth Control

Bandwidth control functions to control the ingress/egress traffic rate on each port via configuring the available bandwidth of each port. In this way, the network bandwidth can be reasonably distributed and utilized, To configure port bandwidth is to limit the rate at which the physical interface can send out or receive data in.
Before the traffic is sent out of the interface, the speed limit is configured on the outgoing direction of the interface to control all the outgoing packet traffic. Before the traffic is received from the interface, the speed limit is configured on the incoming direction of the interface to control all the incoming packet traffic.

Click on the navigation bar: **Configuration --> Bandwidth Control**



Bandwidth Control Setting

Port	Type	State	Rate(Kbit/sec)
Port 5 Port 6 Port 7 Port 8 Trunk2 Trunk3	Egress	Enable	61440 (8-1000000, multiple of 8)

Apply

Port	Ingress Rate (Kbit/sec)	Egress Rate (Kbit/sec)
Port 5	Unlimited	Unlimited
Port 6	Unlimited	Unlimited
Port 7	Unlimited	61440
Port 8	Unlimited	Unlimited
Trunk2	Unlimited	61440
Trunk3	Unlimited	Unlimited

- **"Port :"** Select the desired port for rate configuration. It is multi-optional, administrator can choose Ten ports at most at a time.
- **"Type :"** Select **"Ingress"** or **"Egress"** from the drop-down box.
- **"State:"** Enable or Disable bandwidth control for the selected port.
- **"Rate :"** Select the Rate for receiving packets or sending packets on the select port. administrator can choose the rate as below:

- Unlimited**:** Disable the Ingress or Egress traffic.
- Rate limit : value need to be assigned, The control Range is “8-1000000Kbps (Kbit/sec) by multiple of 8Kbps .

Administrator has to hold “Ctrl” and the left button of the mouse to select the ports , and select the type, state and rate of the selected port, click “Apply” button to refresh the bandwidth control Setting.

Notice

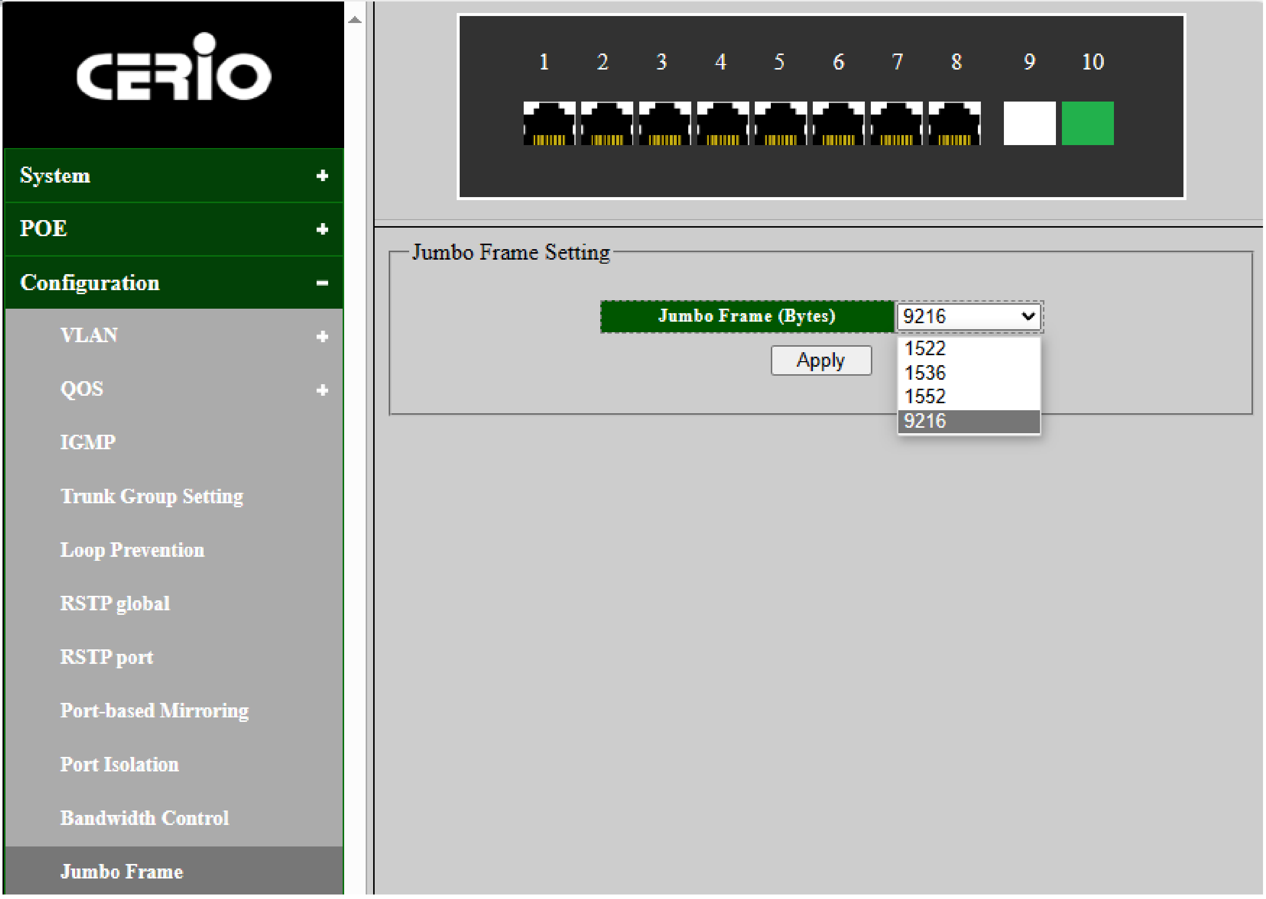
When egress bandwidth control feature is enabled for one or more ports, you are suggested to disable the flow control on each port to ensure the switch works normally.

Field	Description
Port	Displays the port number of the switch.
Ingress Rate	Displays the ingress rate of all ports.
Egress Rate	Displays the egress rate of all ports.

5.11 Jumbo Frame

The administrator can set the Jumbo Frame size and display it on this page.
Giant frame setting page, which is used to configure the maximum frame length allowed, in bytes.

Click on the navigation bar: **Configuration --> Jumbo Frame**



Jumbo Frame Setting

Jumbo Frame (Bytes): 9216

- **"Jumbo Frame :"** The maximum jumbo frame size allowed by the switch is 9216 bytes, and the default frame size is 1522 bytes, which is divided into 1522/1536/1552/9216 bytes for optional settings.

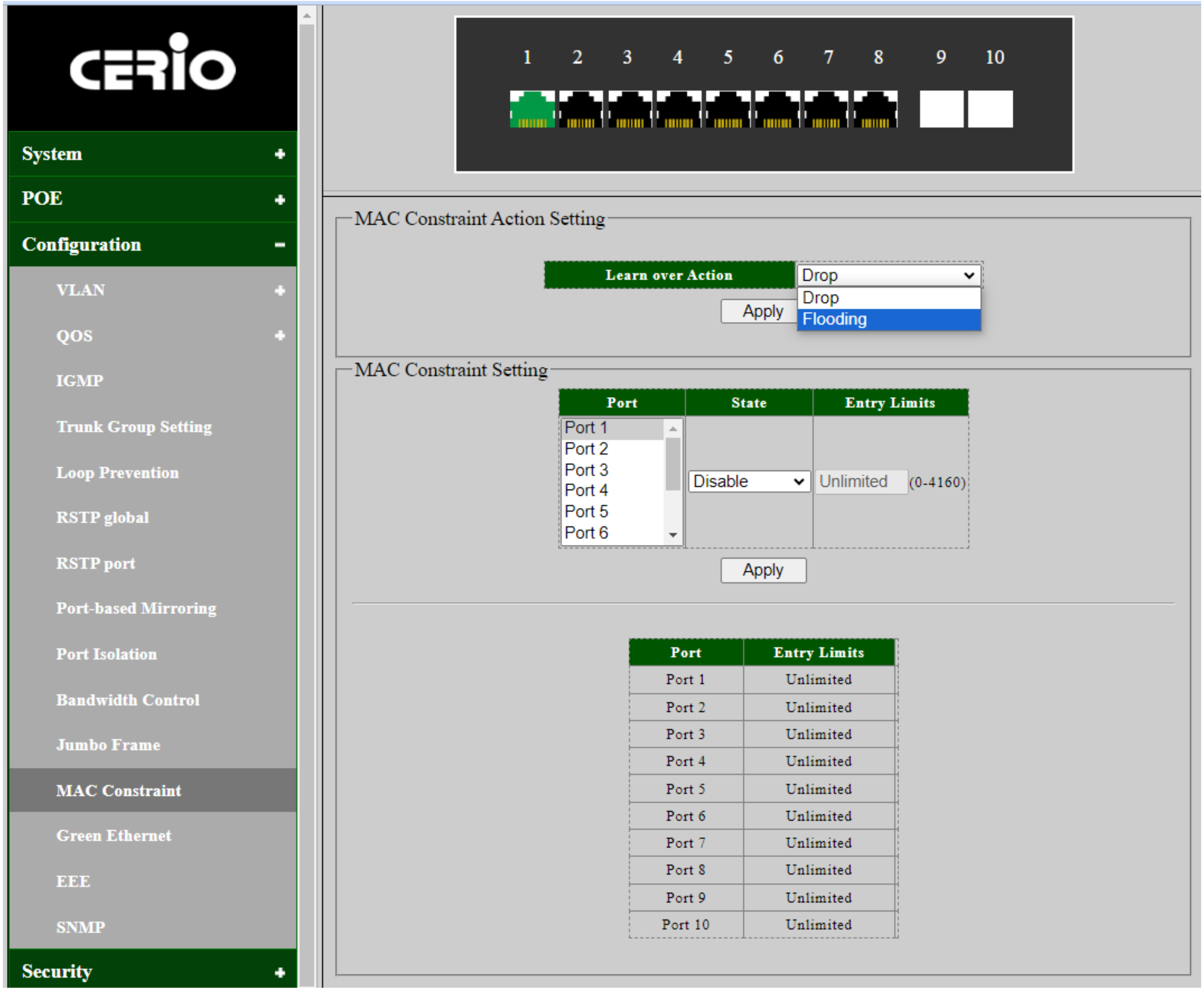
Administrator has to click the "Apply" button to refresh the Jumbo Frame Setting.

Notice When jumbo frames are required, the maximum frame size (9216) of the switch is allowed to be configured.

5.12 MAC Constraints

The MAC constraint behavior page is used to configure the number of MAC allowed to be learned by the port and the processing behavior of the MAC address learned by the port.
The system learns the source MAC of the user's packet, and when the learned MAC reaches the limit threshold. If the source MAC of the user's packet already exists in the MAC table, the user's packet will continue to be forwarded. If the source MAC of the packet does not exist in the MAC table, the system will process the packet accordingly according to the MAC restriction action. For example, if the action is drop, then the user packet will be dropped at the incoming port.

Click on the navigation bar: **Configuration --> MAC Constraints**



MAC Constraint Action Setting

Learn over Action: Drop (options: Drop, Flooding)

Apply

MAC Constraint Setting

Port	State	Entry Limits
Port 1 Port 2 Port 3 Port 4 Port 5 Port 6	Disable	Unlimited (0-4160)

Apply

Port	Entry Limits
Port 1	Unlimited
Port 2	Unlimited
Port 3	Unlimited
Port 4	Unlimited
Port 5	Unlimited
Port 6	Unlimited
Port 7	Unlimited
Port 8	Unlimited
Port 9	Unlimited
Port 10	Unlimited

MAC Constraints Action Setting:

- **"Learn over Action :"** Administrator can choose the "Learning over Action" approach of Drop or Flooding of the MAC Constraints for MAC address.

Administrator has to click the “Apply” button to refresh the MAC Constraints Action Setting.

MAC Constraints Setting:

- **“Port :”** Select the desired port for MAC Constraints configuration.
- **“State :”** Administrator can to enabled or Disable the MAC Constraints function.
- **“Entry Limits :”** Entry MAC Constraints control 0-4160 limit value on the select port. Administrator can choose the rate as below:
  - Unlimited**:** No limited to MAC Constraints for MAC address.
  - The entry limit value need to be assigned, The MAC Constraints control Range is “0-4160 MAC address .

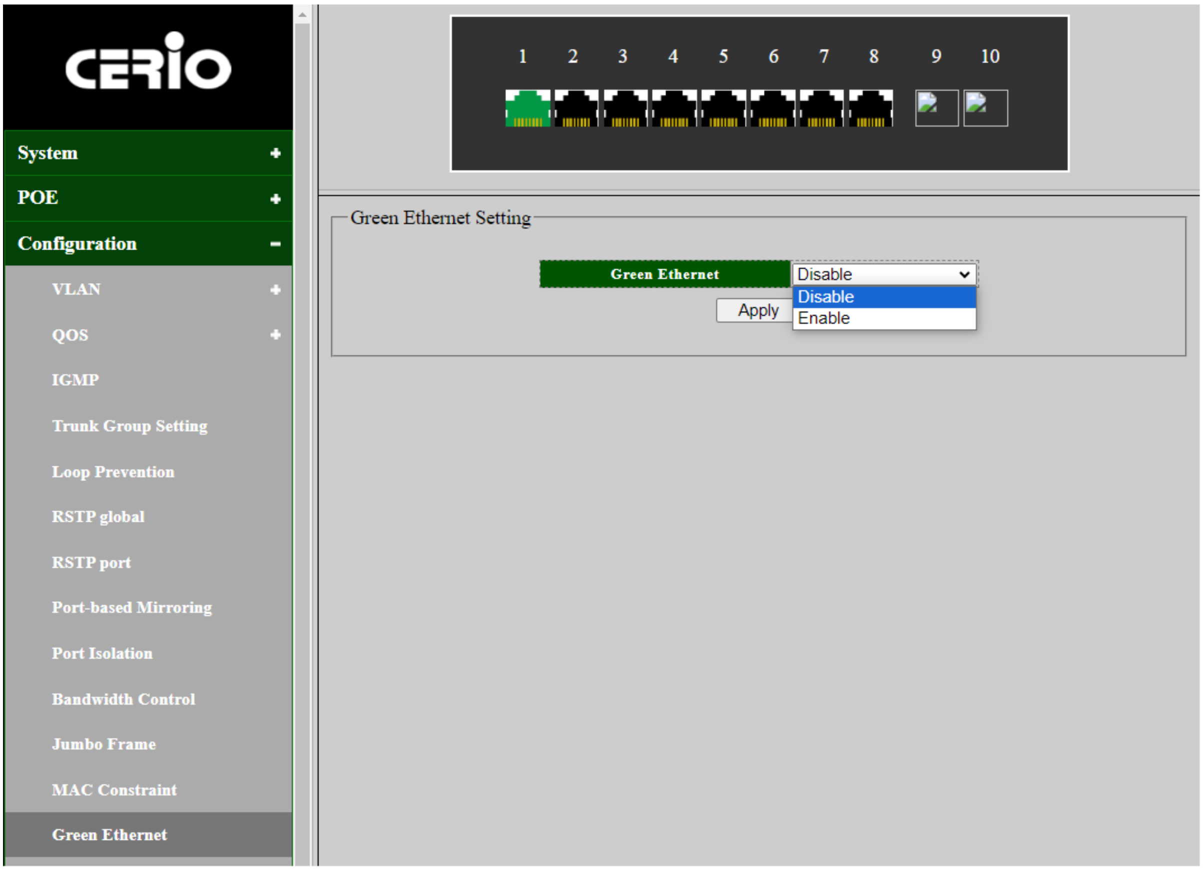
Administrator has to click the “Apply” button to refresh the MAC Constraints Setting.

Field	Description
Port	Displays the port number of the switch.
Entry Limits	Displays the Entry MAC Constraints control limit value.

5.13 Green Ethernet

Green Ethernet refers to features that are environmentally friendly and reduce the power consumption of devices. The system provides the connection and dynamic detection of the cable length, as well as the dynamic adjustment of the power required for the detected cable length. High performance and low power consumption. The link d own of the system support port saves power and greatly reduces the power consumption when the network cable is disconnected. When the input signal is detected, it wakes up from the link down power saving and enters the normal mode.

Click on the navigation bar: **Configuration --> Green Ethernet**



Green Ethernet: Disable

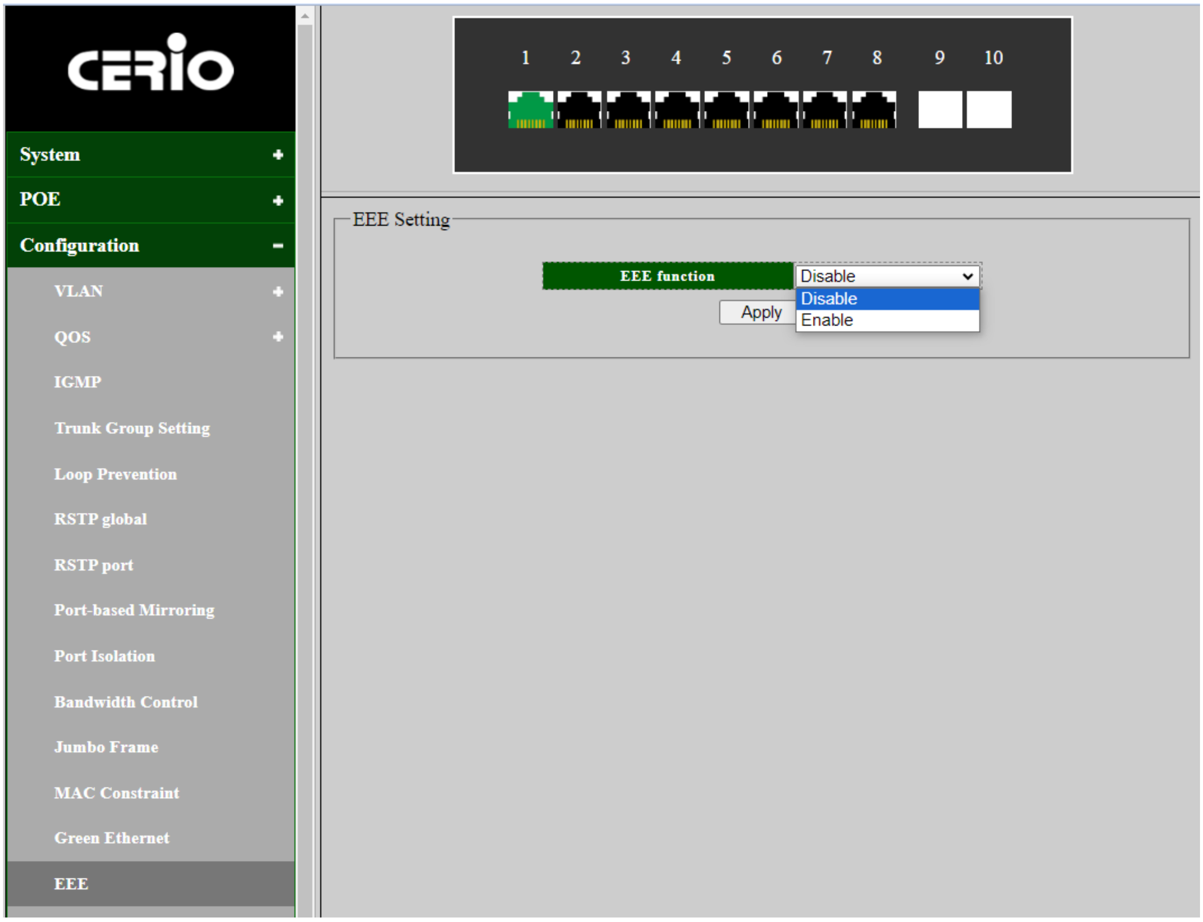
- **"Green Ethernet :"** Administrator can select to enable or disable the Green Ethernet function.

Administrator has to click the "Apply" button to refresh the Green Ethernet Setting.

5.14 EEE

Energy Efficient Ethernet (EEE) supports operating in low-power idle mode. Systems at both ends of the link can disable some functions when the link utilization is low, saving power. **Switching off is recommended.**

Click on the navigation bar: **Configuration --> EEE**



EEE Setting

EEE function: Disable

Disable
Enable

Apply

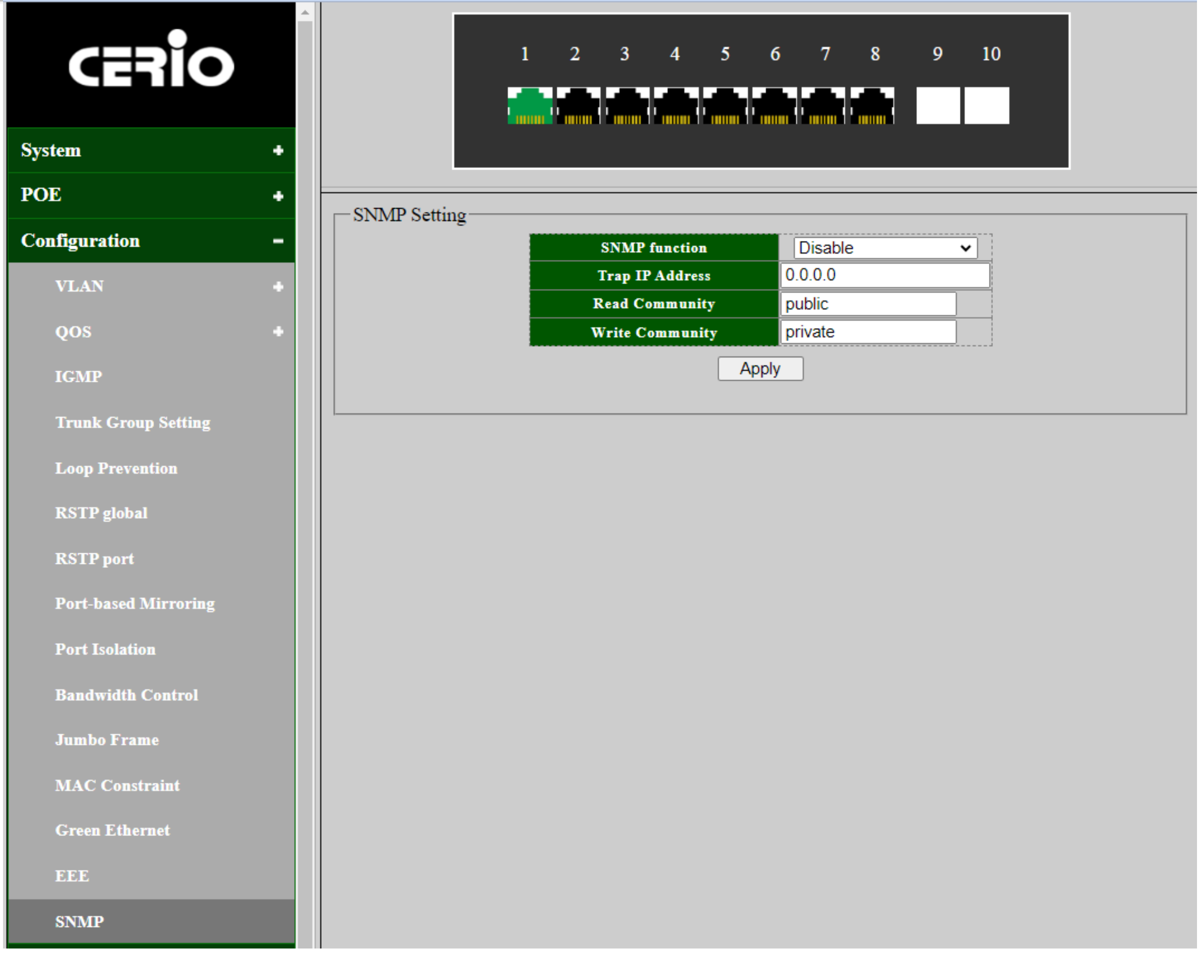
- **"EEE function :"** Administrator can select to enable or disable the EEE function.

Administrator has to click the "Apply" button to refresh the EEE Setting.

5.15 SNMP

SNMP is a standard network management protocol widely used in TCP/IP networks. The protocol can support network management systems to monitor whether there is anything that causes management concern in the equipment connected to the network. The basic components of SNMP include NMS (Network Management System), Agent (Agent), Managed Object (object) and MIB (Management Information Base).

Click on the navigation bar: **Configuration --> SNMP**



SNMP Setting

SNMP function	Disable
Trap IP Address	0.0.0.0
Read Community	public
Write Community	private

- **“SNMP function :”** Administrator can select to enable or disable the SNMP function.
- **“Trap IP Address :”** SNMP Trap Destination for IP address of the trap manager to receive notification messages from this switch. Traps indicating status changes are issued by the switch to specified trap managers. Administrator can specify trap managers so that key events are reported by this switch to your management station..
- **“Read Community :”** For Read community string that acts like a password and permits access to the SNMP database on this switch. Authorized management stations are only able to retrieve MIB objects,By “public” or “private” string to authorized .
- **“Write Community :”** For Write community string that acts like a password and permits access to the SNMP database on this switch. Authorized management stations are only able to retrieve MIB objects, By “public” or “private” string to authorized .

Administrator has to click the “Apply” button to refresh the SNMP Trap Setting.

6. Security

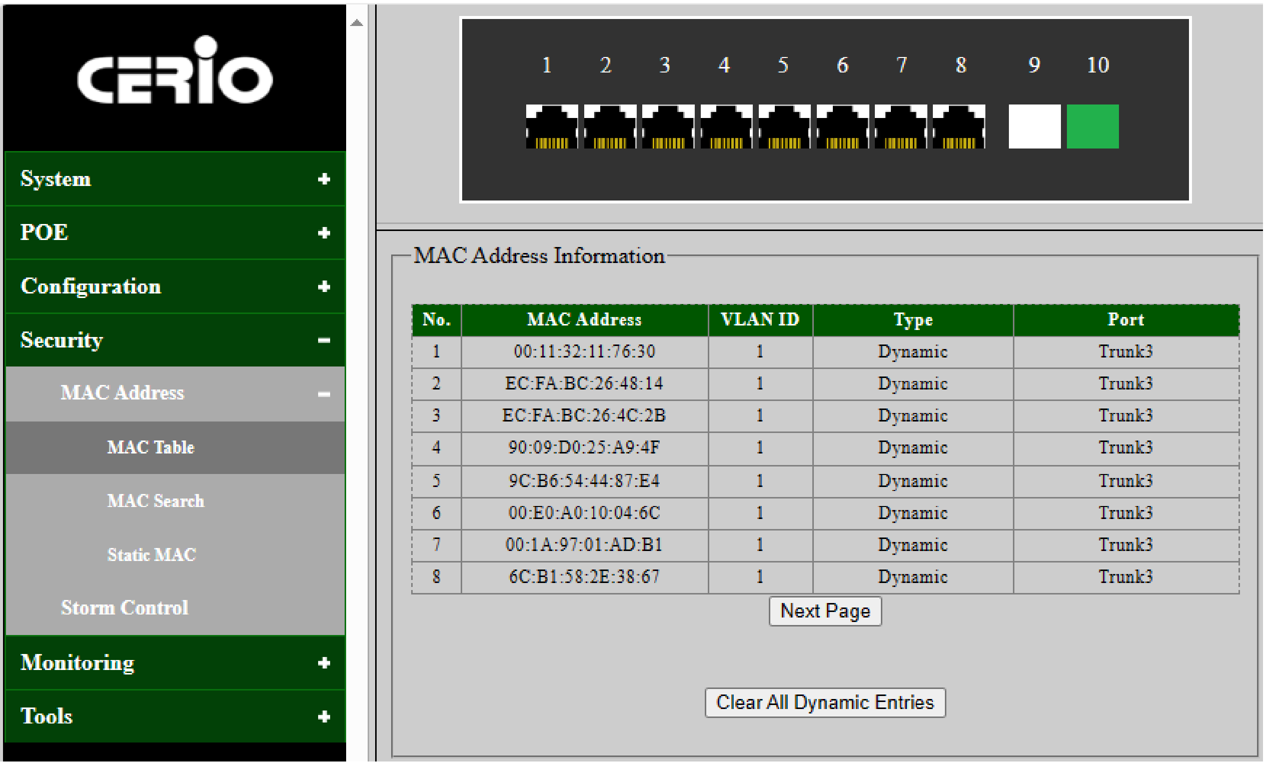
6.1 MAC Address

MAC Address in English is Media Access Control Address, literally translated as media access control address, Also known as the local area network Address (LAN Address), Ethernet Address (Ethernet Address) or Physical address (physical address), it is an address used to confirm the location of network equipment.

6.1.1 MAC Table

Use this section to configure a relationship between a MAC address, VLAN ID and switch port. The MAC address table keeps track of the Media Access Control (MAC) addresses that are associated with each port. This table allows the device to forward unicast traffic through the appropriate port. The MAC address table is sometimes called the bridge table or the forwarding database. Use the MAC Address Table page to display information about entries in the MAC address table.

Click navigation bar: **Security -> MAC Address -> MAC Table**



MAC Address Information

No.	MAC Address	VLAN ID	Type	Port
1	00:11:32:11:76:30	1	Dynamic	Trunk3
2	EC:FA:BC:26:48:14	1	Dynamic	Trunk3
3	EC:FA:BC:26:4C:2B	1	Dynamic	Trunk3
4	90:09:D0:25:A9:4F	1	Dynamic	Trunk3
5	9C:B6:54:44:87:E4	1	Dynamic	Trunk3
6	00:E0:A0:10:04:6C	1	Dynamic	Trunk3
7	00:1A:97:01:AD:B1	1	Dynamic	Trunk3
8	6C:B1:58:2E:38:67	1	Dynamic	Trunk3

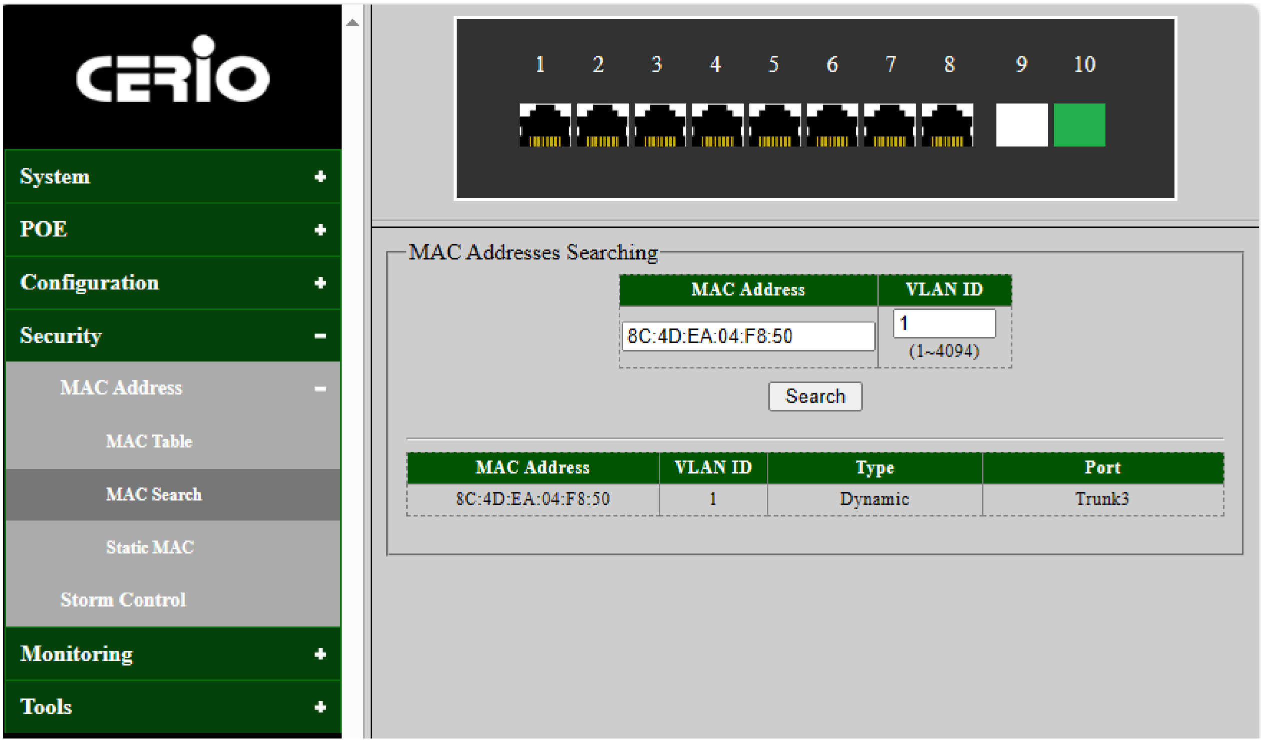
Administrator has to click the “Clear” button to refresh the MAC Table Information.

Field	Description
No	Displays the number of the list.
MAC Address	The MAC address to which packets will be statically forwarded,The format is a six-byte MAC address, with each byte separated by colons.
VLAN ID	Specify the VLAN to show or clear MAC entries. The VLAN with which the MAC address is associated. A MAC address can be associated with multiple VLANs.
Type	Specify the Type for port MAC Table. •Static: The address has been manually configured anddoes not age out •Dynamic: The address has been automatically learned by the device and can age out when it is not in use
Port	Interface or port number.

6.1.2 MAC Search

The MAC address search page is used to query the MAC address and display the VLAN ID. Administrator can set need Search MAC address in the MAC table.

Click navigation bar: **Security -> MAC Address -> MAC Search**



MAC Addresses Searching

MAC Address	VLAN ID
8C:4D:EA:04:F8:50	1 (1~4094)

Search

MAC Address	VLAN ID	Type	Port
8C:4D:EA:04:F8:50	1	Dynamic	Trunk3

- **"MAC Address : "** Enter to specify the search MAC address in the table.
- **"VLAN ID : "** Enter a VLAN ID that specifies a specific MAC address.

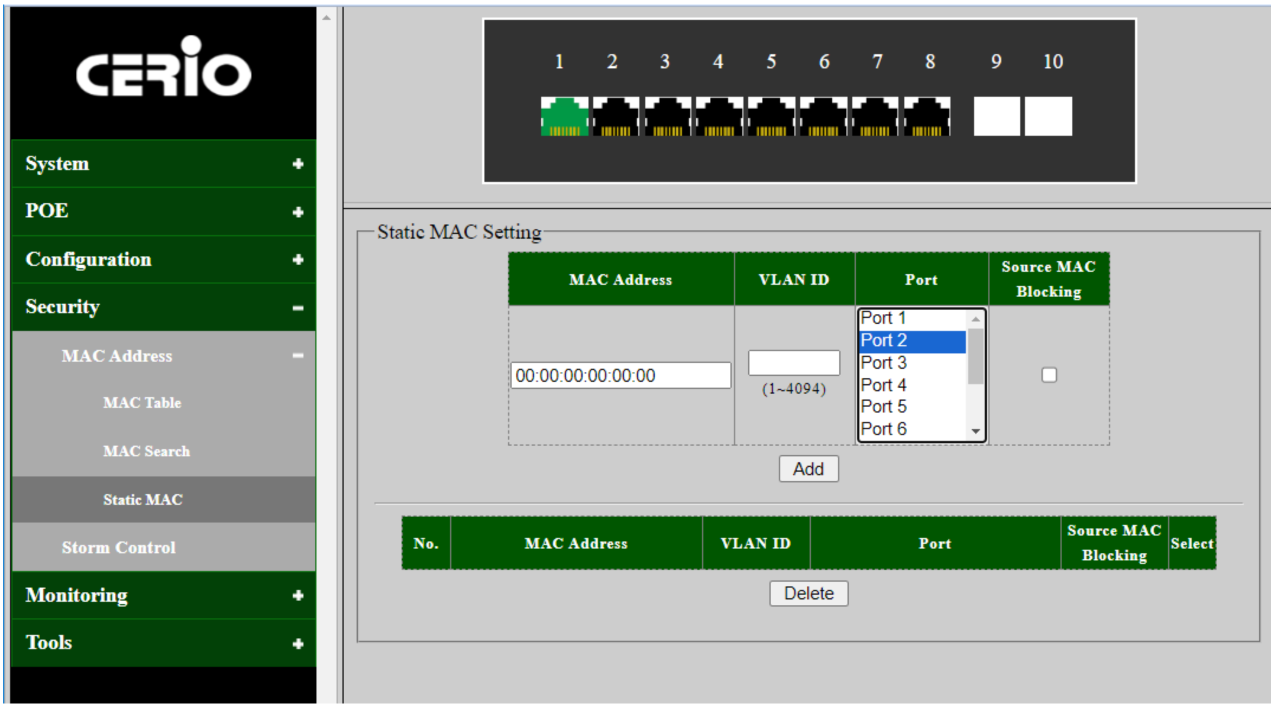
Field	Description
MAC Address	Display the search MAC address in the table.
VLAN ID	Display the VLAN ID for the specific MAC address.

Administrator has to click the "Search" button to refresh the MAC Address Searching.

6.1.3 Static MAC

The static MAC page is used to add, display and delete the static MAC address of the port. If administrator fixed an MAC address in the port then device MAC address will bind in the port, if device connection to other port will can't working only connection bind port. It also supports MAC filtering function, and administrators can also filter and block through MAC designation.

Click navigation bar: **Security -> MAC Address -> Static MAC**



Static MAC Setting

MAC Address	VLAN ID	Port	Source MAC Blocking
00:00:00:00:00:00	(1~4094)	Port 1 Port 2 Port 3 Port 4 Port 5 Port 6	□

No.	MAC Address	VLAN ID	Port	Source MAC Blocking	Select

- **"MAC Address : "** Enter to specify the static MAC address in the table. A unicast MAC address for which the switch has forwarding and/or filtering information. The format is a six-byte MAC address, with each byte separated by colons.
- **"VLAN ID : "** The VLAN to which the added static MAC belongs.
- **"Port : "** The port to which the added static MAC belongs.
- **"Source MAC Blocking : "** If this option is checked, MAC filtering function will be enable ,the message carrying this MAC is not allowed to pass.

Field	Description
MAC Address	The MAC address to which packets will be statically forwarded.
VLAN ID	Specify the VLAN to show or clear MAC entries.
Port	Interface or port number.
Source MAC Blocking (MAC filtering)	Display whether source MAC blocking is used.
Select	This helps to select static MAC list to be deleted.
Delete	Click Delete to delete the static MAC list.

Administrator has to click the "Delete" button to refresh the Static MAC Setting.

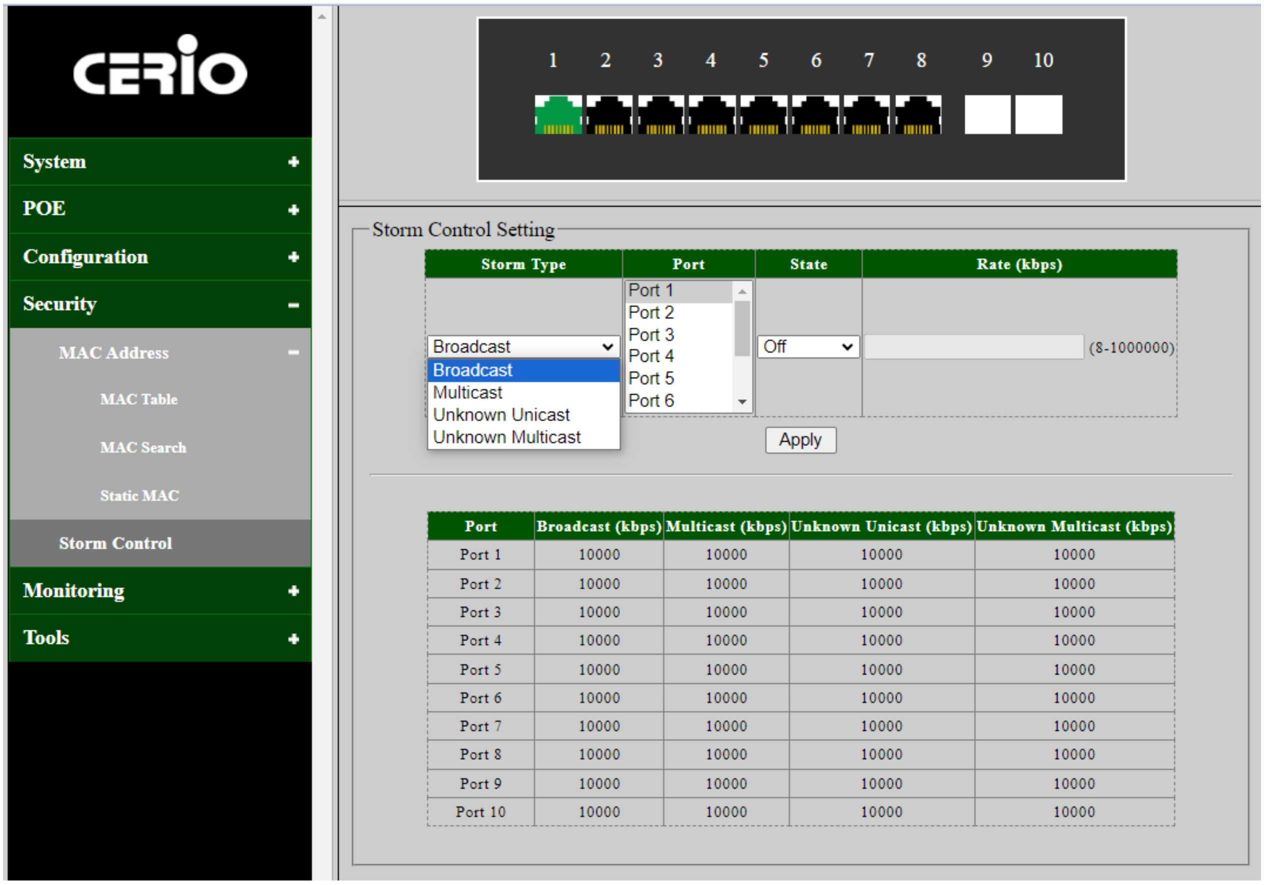
Notice

Administrator can manually bind the MAC address of a downlink network device with a port of the switch. After you add a static MAC address, when the device receives a packet destined for this address from VLAN, it forwards the packet to the specified port.

6.2 Storm Control

Broadcast storms may occur when a device on your network is malfunctioning,or if application programs are not well designed or properly configured. If thereis too much broadcast traffic on your network, performance can be severely degraded or everything can come to complete halt. Administrator can setup storm control of Broadcast / Multicast / Unicast by limiting the rates. When the rate of Broadcast / unknown Multicast or unknown Unicast frames is higher than the user-defined threshold, this function can to limit the number of frames entering the switch and to define the types of frames that are counted towards this limit. Will be the frames received beyond the threshold are discarded or the interface shuts down.

Click navigation bar: **Security -> Storm Control**



Storm Control Setting

Storm Type	Port	State	Rate (kbps)
Broadcast Broadcast Multicast Unknown Unicast Unknown Multicast	Port 1 Port 2 Port 3 Port 4 Port 5 Port 6	Off	(8-1000000)

Apply

Port	Broadcast (kbps)	Multicast (kbps)	Unknown Unicast (kbps)	Unknown Multicast (kbps)
Port 1	10000	10000	10000	10000
Port 2	10000	10000	10000	10000
Port 3	10000	10000	10000	10000
Port 4	10000	10000	10000	10000
Port 5	10000	10000	10000	10000
Port 6	10000	10000	10000	10000
Port 7	10000	10000	10000	10000
Port 8	10000	10000	10000	10000
Port 9	10000	10000	10000	10000
Port 10	10000	10000	10000	10000

- **"Storm Type :"** Select the storm type drop-down box as below:
  - **Broadcast:** If select storm control for Broadcast traffic will count Broadcast traffic towards the bandwidth threshold.
  - **Multicast:** If select storm control for unknown Multicast will count unknown

Multicast traffic towards the bandwidth threshold.

- **Unknown Unicast:** If select storm control for unknown Unicast will count unknown Unicast traffic towards the bandwidth threshold.
- **Unknown Multicast:** If select storm control for unknown Multicast will count unknown Multicast traffic towards the bandwidth threshold.

➢ **"Port :"** Select the desired port for storm control configuration. It is multi-optional, administrator can choose Ten ports at most at a time.

➢ **"State:"** Turn on or Turn off Storm control for the selected port. Set this to enable, or the values will not be saved.

➢ **"Rate :"** Select the bandwidth for receiving the specified packet on the port. The packet traffic exceeding the bandwidth will be discarded. administrator can choose the rate as below::

- Unlimited**:** When the Port status is set to "Off" and unrestricted for the Ingress or Egress traffic.
- Rate limit : value need to be assigned, The control Range is "8-1000000Kbps (Kbit/sec) by multiple of 8Kbps .

Administrator has to hold "Ctrl" and the left button of the mouse to s elect Enable from the State drop-down box to enable the setting, and then choose the rate from the checkbox "Apply" button to refresh the Storm Control Setting.

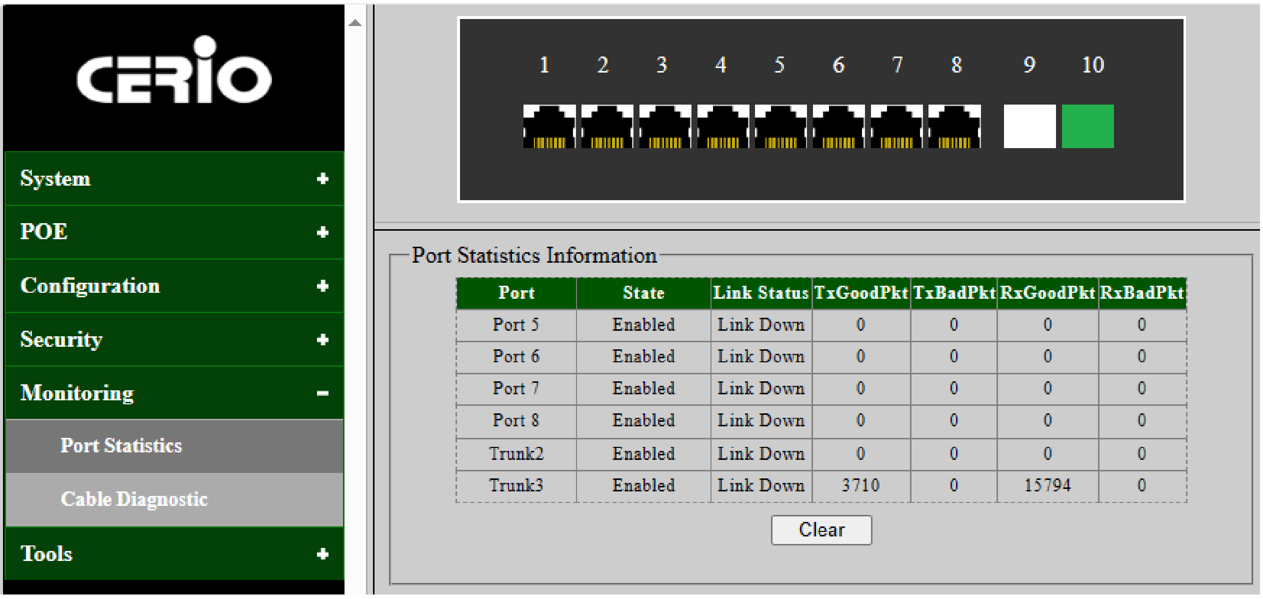
Field	Description
Port	Displays the port number of the switch.
Broadcast (Kbps)	Show the storm control for the Broadcast packets, • Displays the bandwidth threshold rate for broadcast packets.
Multicast(Kbps)	Show the storm control for the Multicast packets. • Displays the bandwidth threshold rate for Multicast packets.
Unknown Unicast(Kbps)	Show the storm control for the unknown Unicast packets. • Displays the bandwidth threshold rate for unknown Unicast packets.
Unknown Multicast(Kbps)	Show the storm control for the unknown Multicast packets. • Displays the bandwidth threshold rate for unknown Multicast packets.

7. Monitoring

7.1 Port Statistics

These pages provides statistical data about the network ports of the POE switch. The display letter includes the status of the port, the connection status, the correct data packet sent, the wrong data packet sent, the correct data packet received and the wrong data packet received.

Click navigation bar: **Monitoring -> Port Statistics**



Port Statistics Information

Port	State	Link Status	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt
Port 5	Enabled	Link Down	0	0	0	0
Port 6	Enabled	Link Down	0	0	0	0
Port 7	Enabled	Link Down	0	0	0	0
Port 8	Enabled	Link Down	0	0	0	0
Trunk2	Enabled	Link Down	0	0	0	0
Trunk3	Enabled	Link Down	3710	0	15794	0

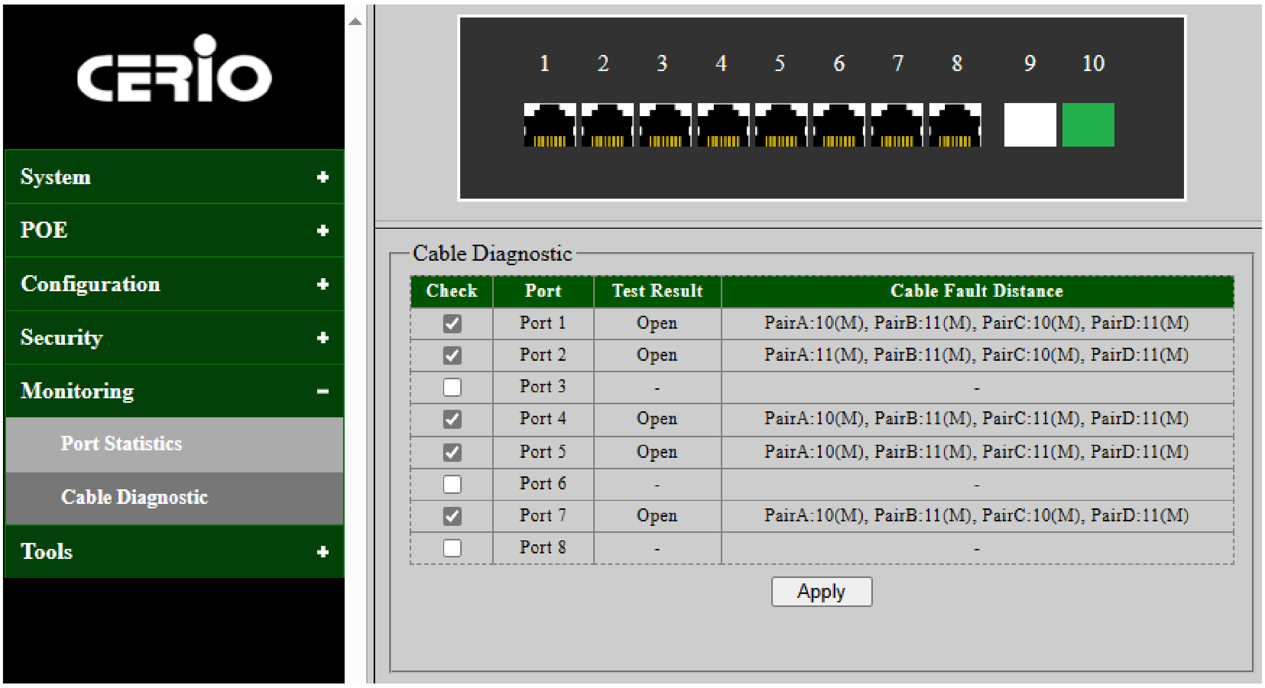
Field	Description
Port	Displays the port number of the switch.
State	Displays whether the port is enabled or disabled.
Link Status	Displays the link state of the port.
TxGoodPkt	Displays the number of good packets transmitted on the port.
TxBadPkt	Displays the number of error packets transmitted on the port.
RxGoodPkt	Displays the number of good packets received on the port.
RxBadPkt	Displays the number of error packets received on the port.

Administrator has to click the “Clear” button to refresh the Port Statistics Information.

7.2 Cable Diagnostic

Through this page, you can test all connected cables. The cable diagnosis page is used to diagnose whether the network line is normal.

Click navigation bar: **Monitoring -> Cable Diagnostic**



Cable Diagnostic

Check	Port	Test Result	Cable Fault Distance
☑	Port 1	Open	PairA:10(M), PairB:11(M), PairC:10(M), PairD:11(M)
☑	Port 2	Open	PairA:11(M), PairB:11(M), PairC:10(M), PairD:11(M)
□	Port 3	-	-
☑	Port 4	Open	PairA:10(M), PairB:11(M), PairC:11(M), PairD:11(M)
☑	Port 5	Open	PairA:10(M), PairB:11(M), PairC:11(M), PairD:11(M)
□	Port 6	-	-
☑	Port 7	Open	PairA:10(M), PairB:11(M), PairC:10(M), PairD:11(M)
□	Port 8	-	-

- **"Check:"** Click the checkbox to select the port to be diagnosed.

Field	Description
Port	Displays the port number of the switch.
Test Result Open	The cable is broken or no cable connection.
Normal	The cable connection is good.
Cable Fault Distance	Displays the distance from the port where the cable error occurred.

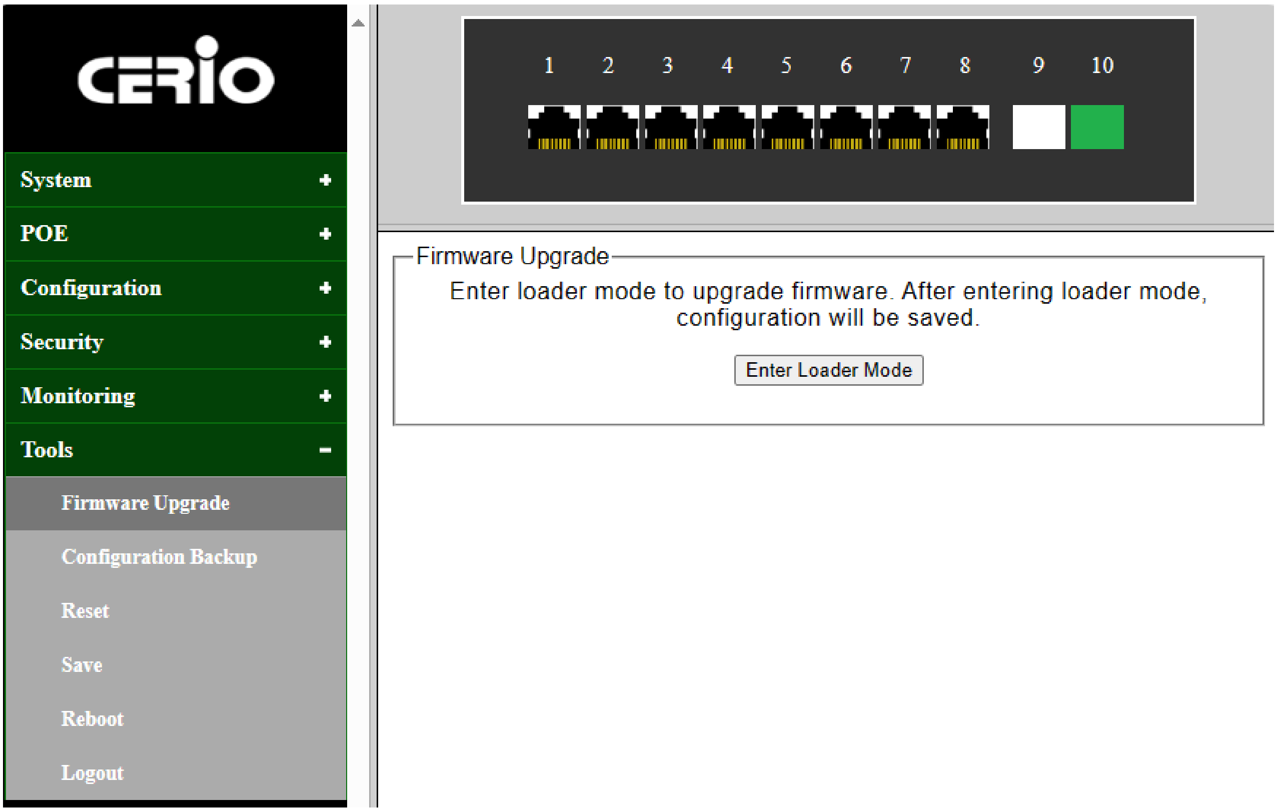
Administrator has to click the "Apply" button to refresh the Cable Diagnostic.

8. Tools

8.1 Firmware Upgrade

The firmware upgrade page is used to enter the loading mode and upgrade in the loading mode, Administrator can upgrade or backup firmware, first download a firmware upgrade file to your computer. method can choose use HTTP protocol.

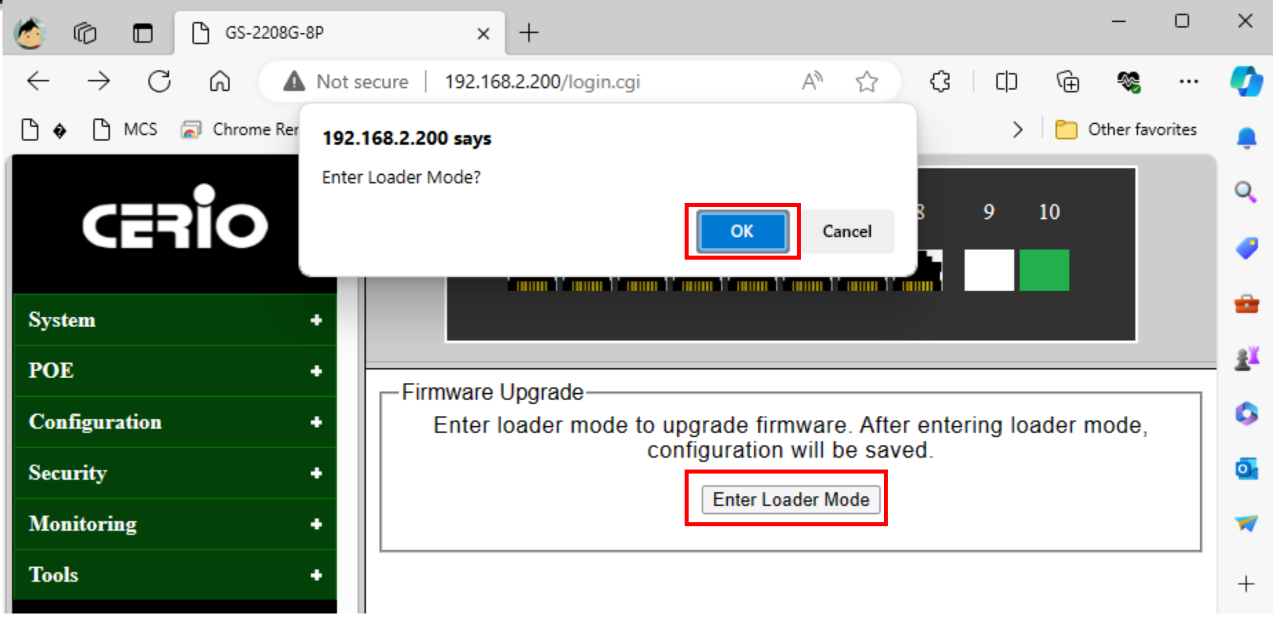
Click navigation bar: **Tools -> Firmware Upgrade**



Firmware Upgrade

Enter loader mode to upgrade firmware. After entering loader mode, configuration will be saved.

1. Administrator has to click the “Enter loader Mode” button to refresh the Firmware Upgrade Setting, then the confirm interface pops up.

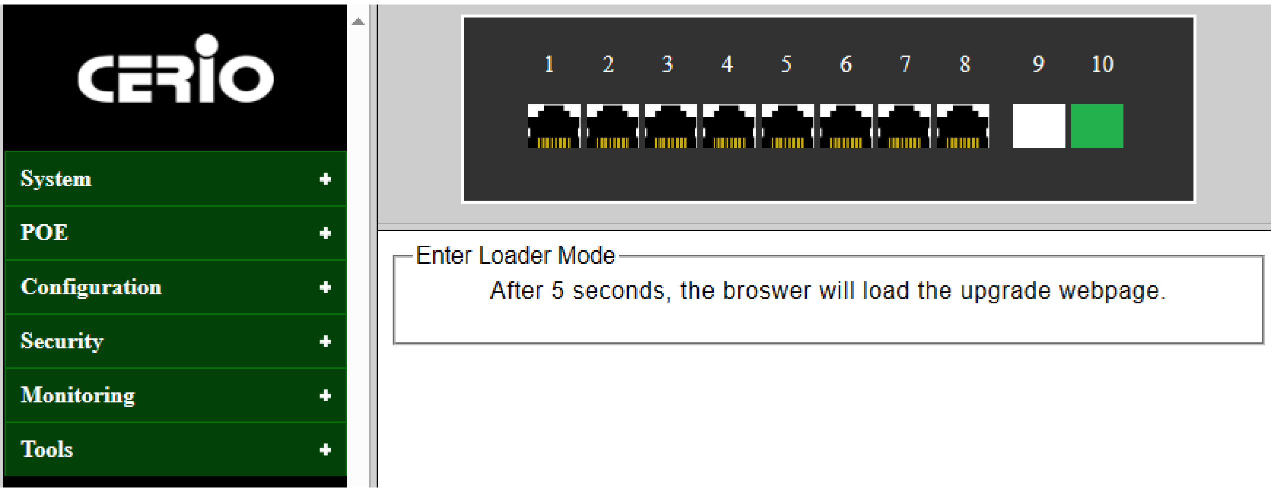


192.168.2.200 says

Enter Loader Mode?

Firmware Upgrade

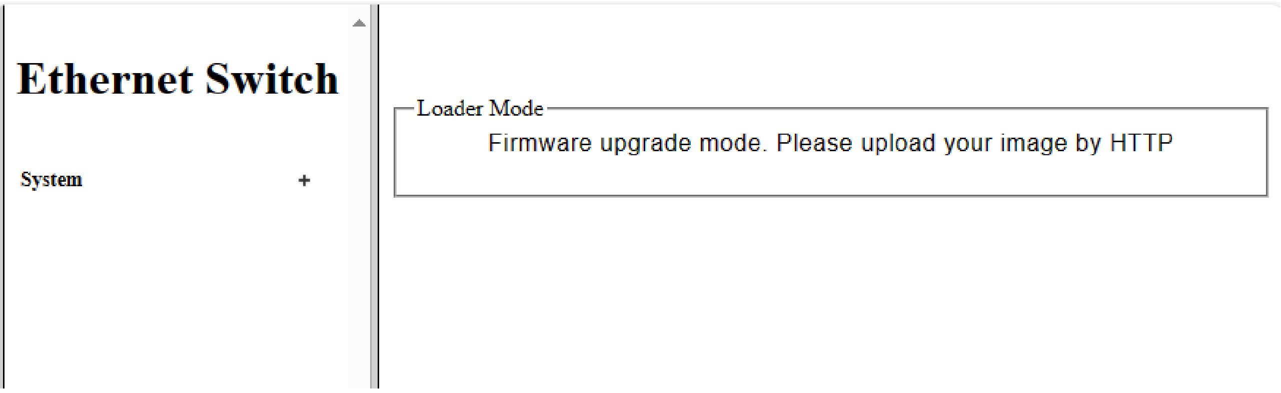
Enter loader mode to upgrade firmware. After entering loader mode, configuration will be saved.



Enter Loader Mode

After 5 seconds, the broswer will load the upgrade webpage.

2. Press OK , then the switch will save the configuration and switch to loader mode after 5 seconds. The firmware upgrade screen displays as shown below.

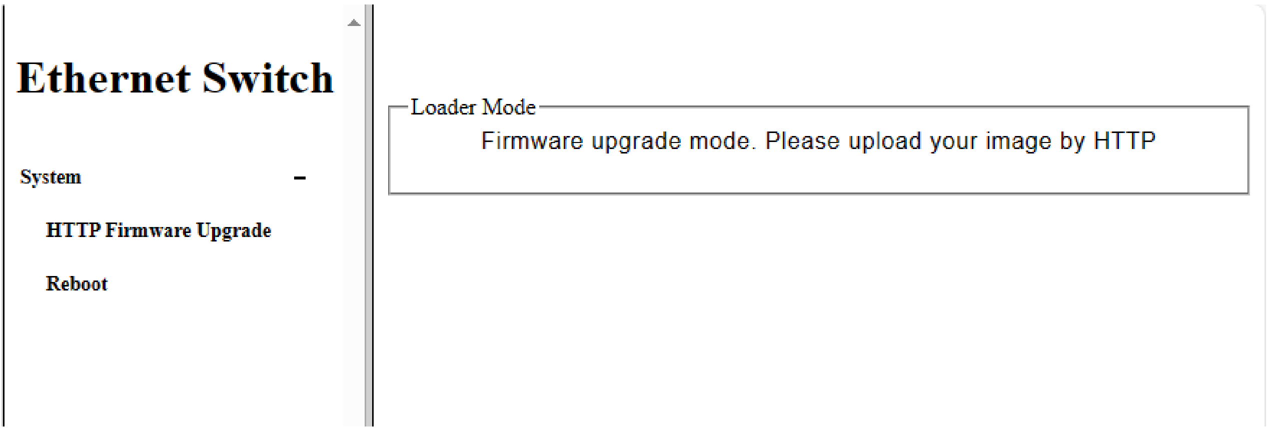


Loader Mode

Firmware upgrade mode. Please upload your image by HTTP

8.1.1 HTTP Firmware Upgrade

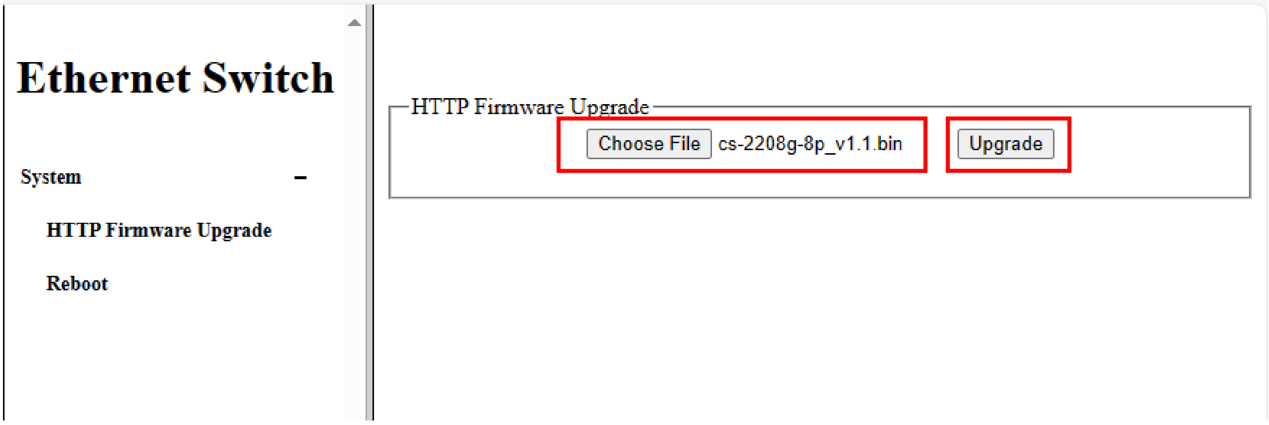
1. Select to upgrade firmware thought HTTP, click **Firmware Upgrade** < **HTTP Firmware Upgrade** to view the screen as shown below.



Loader Mode

Firmware upgrade mode. Please upload your image by HTTP

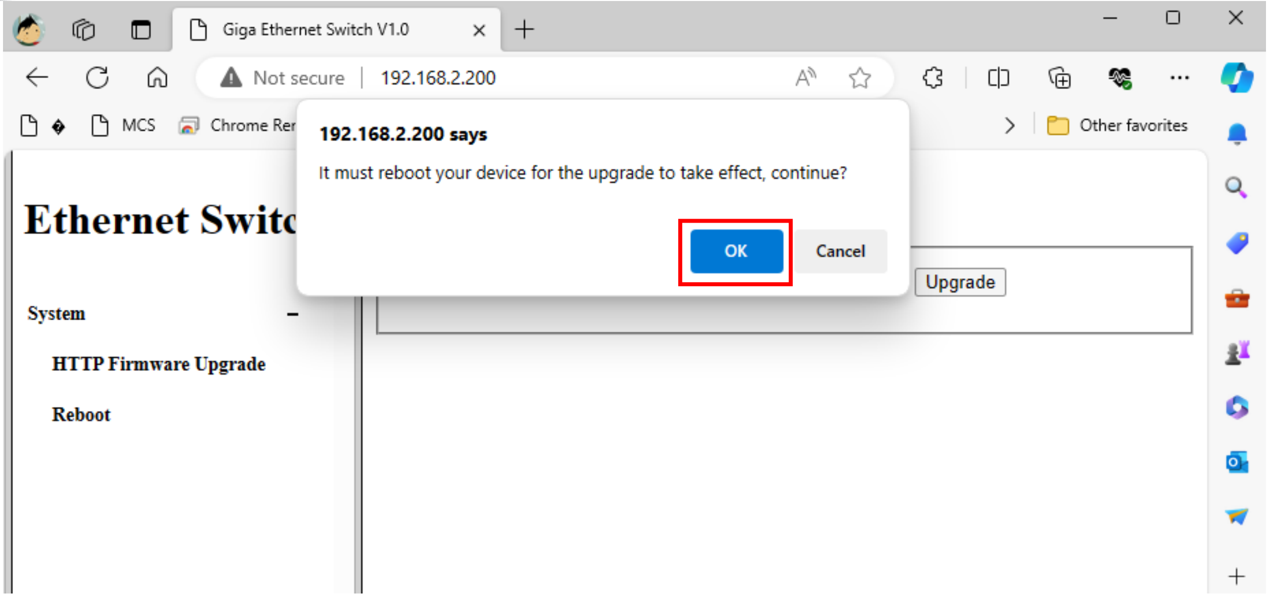
2. Click the **Browse** button to the location on your computer containing the firmware upgrade file and select the upgrade file.



HTTP Firmware Upgrade

cs-2208g-8p_v1.1.bin

3. Click **Upgrade,** then the remind interface pops up, press **OK** to operate the upgrade procedure.



192.168.2.200 says

It must reboot your device for the upgrade to take effect, continue?

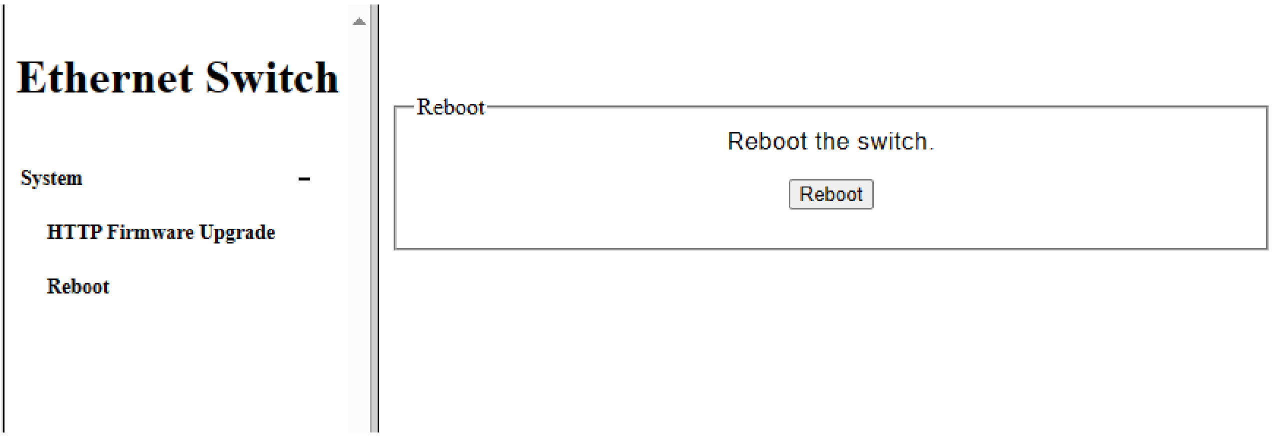
OK Cancel

4. After finishing the HTTP upgrade procedure, switch will reboot automatically.

8.1.2 Reboot

The way to leave "Loader mode" is to Select Reboot.

1. Please click "Reboot" in the menu on the left and click the "Reboot the Switch" to exit "Loader Mode" .

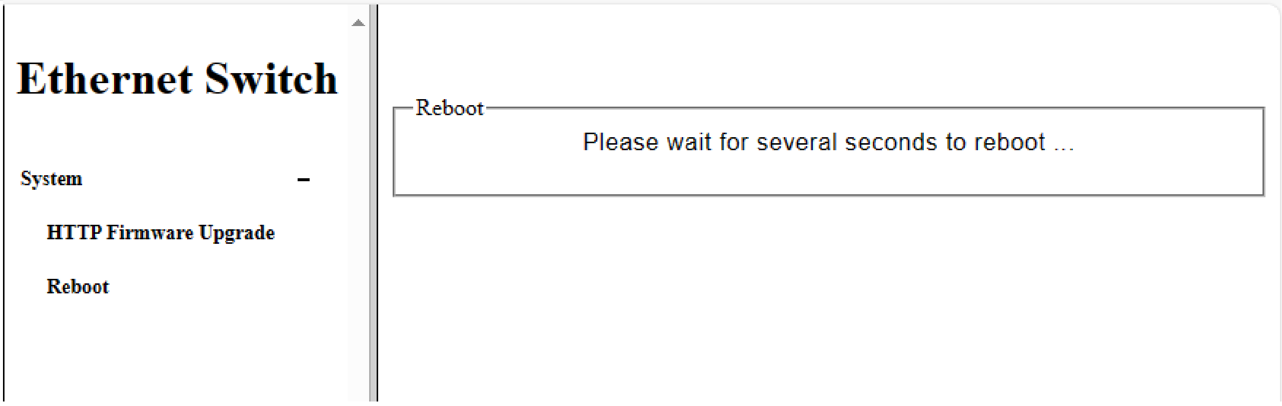


Reboot

Reboot the switch.

Reboot

2. A prompt screen will appear. Please wait for a moment and then log in to the Web UI interface again.



Reboot

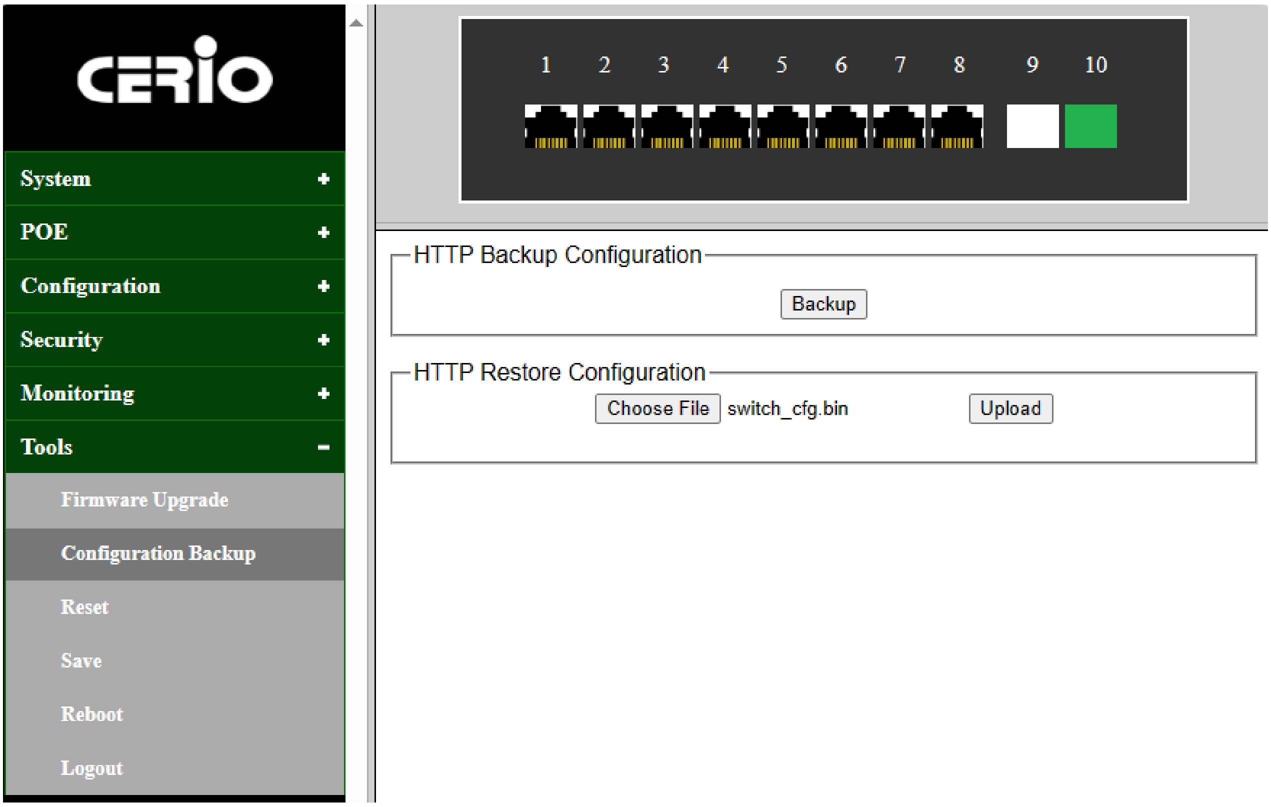
Please wait for several seconds to reboot ...

8.2 Configuration Backup

Administrator can save the current configuration information here. It is recommended to backup the current configuration information before modifying the configuration and upgrading the software.

The configuration backup page is used for configuration import and export. Click the Backup button to export the configuration to PC backup. Click the select File button to restore the configuration, select the configuration of PC backup, and then click the restore button to import the backup configuration into the device.

Click navigation bar: **Tools -> Configuration Backup**



HTTP Backup Configuration

HTTP Restore Configuration

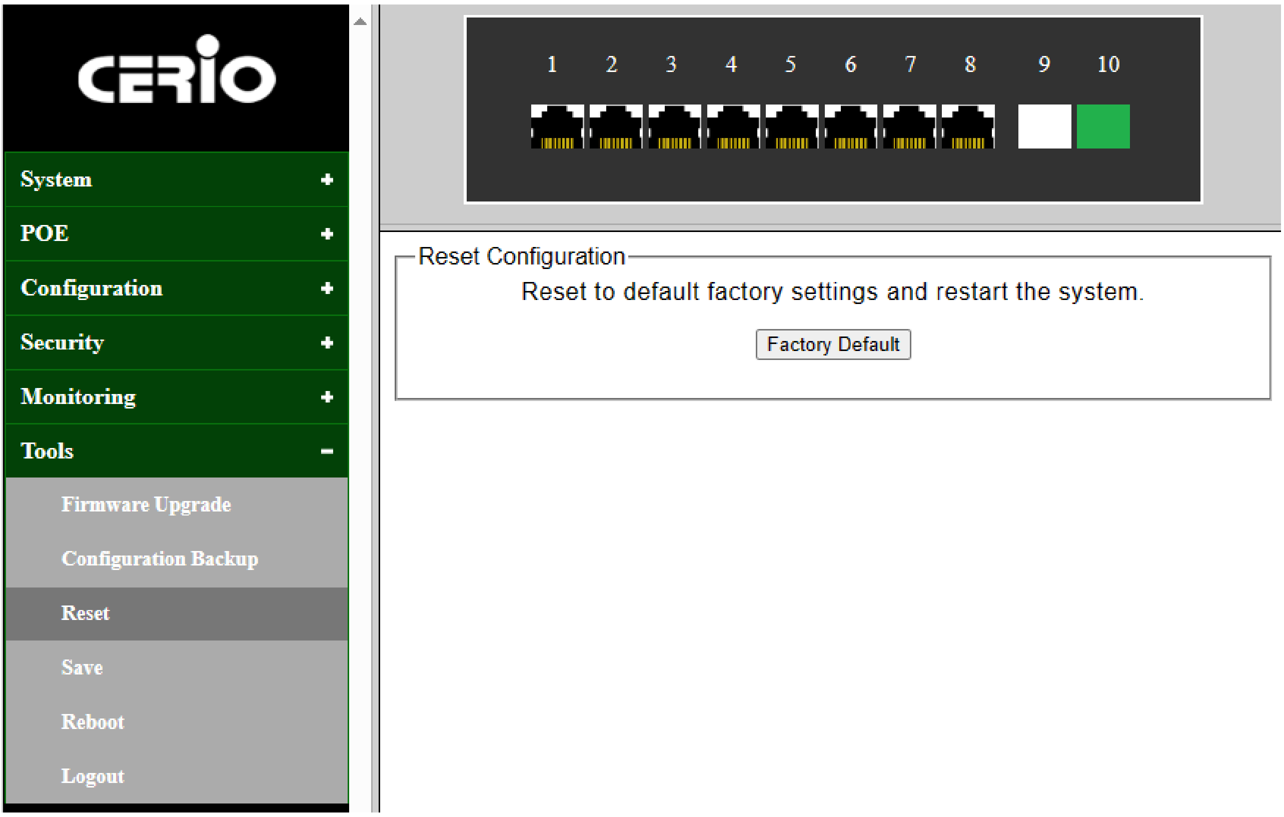
switch_cfg.bin

- **"HTTP Backup Configuration :"** Administrator has to click the Backup button to save the current configuration as a file to your computer. You are suggested to take this measure before Firmware upgrading.
- **"HTTP Restore Configuration :"** Administrator has to click the Browse button to select the backup configuration file, and then click the Restore button. It will take effect after the switch reboots.

8.3 Reset

In addition to hardware restore the factory Settings switch, you can also restore the default Settings on the Web. On this page user can reset the switch to the factory default configuration. All the settings will be cleared after the switch is reset. Follow the steps below to reset the switch back to the factory defaults.

Click navigation bar: **Tools -> Reset**



Reset Configuration

Reset to default factory settings and restart the system.

Factory Default

- **"Factory Default :"**Administrator has to click the "Factory Default" button to set Factory Default setting and the switch will restart automatically.

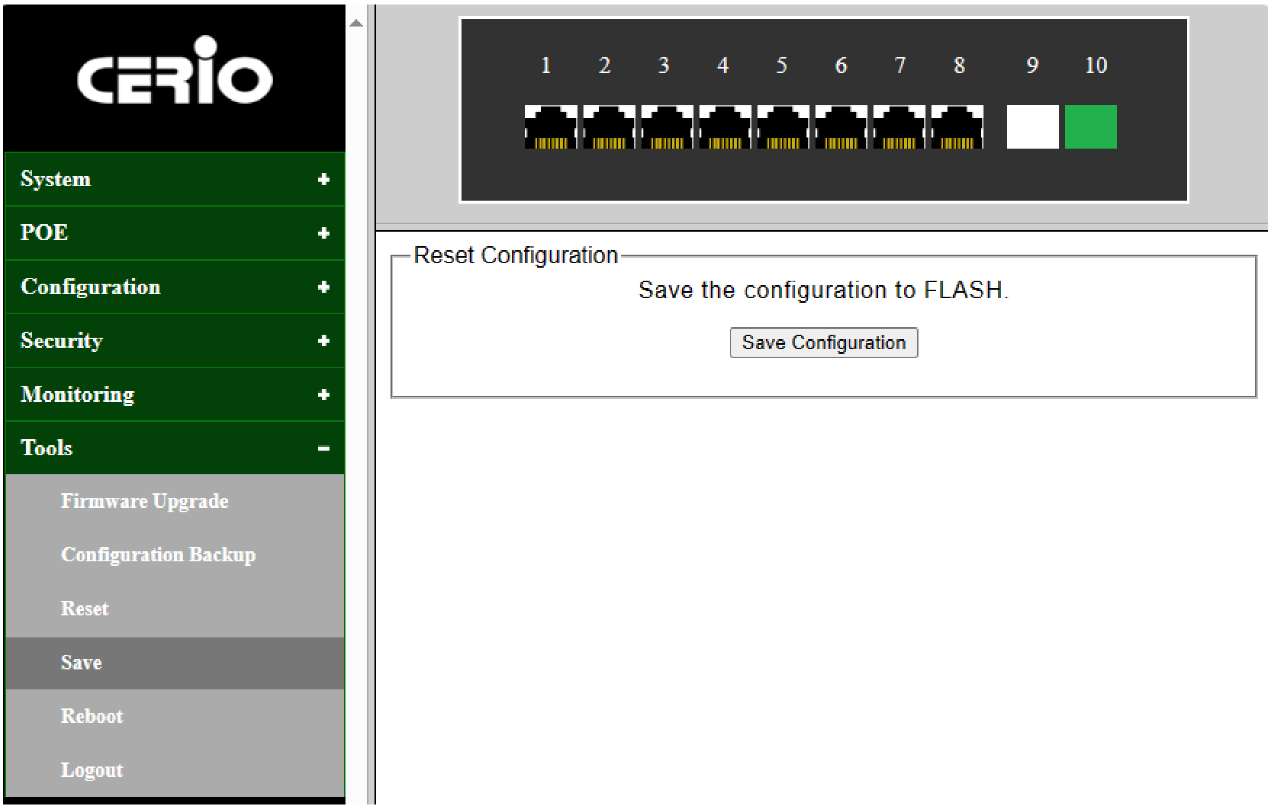
Notice

Confirming execution will restore all settings to default values. Previous configuration information will be lost. It is recommended that you back up your configuration before restoring default settings.
The default management IP address is **192.168.2.200**, the account name is **"root"**, and the password is **"default".**

8.4 Save

Save the Configuration to Hardware FLASH to prevent loss of power outage,
After clicking the save page, the system configuration will be saved immediately, and the configuration saving page will show that the configuration has been saved successfully.

Click navigation bar: **Tools -> Save**



Save the configuration to FLASH.

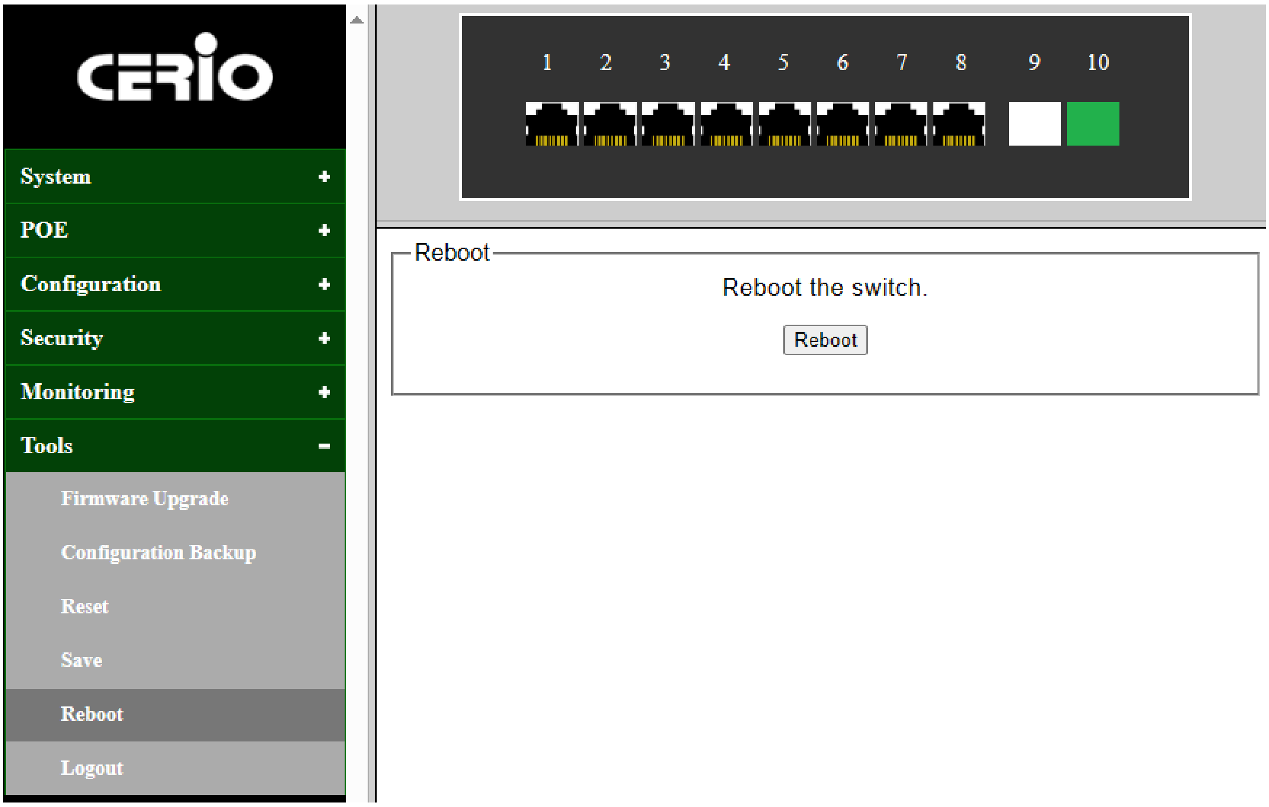
- **"Save Configuration :"** Administrator can save the current configuration easily by clicking the Config Save menu without any function button and you'll see the successful page directly..

Notice Only by clicking the "Config Save" menu can the current settings of the switch be effectively saved to the hardware FLASH, so that the settings made the next time it is started will still be valid. Otherwise, the modifie d settings may be lost after a power outage or restart..

8.5 Reboot

After clicking Restart, the switch will restart, and it is recommended to save the configuration before restarting to prevent the current modified configuration from being lost.

Click navigation bar: **Tools -> Reboot**



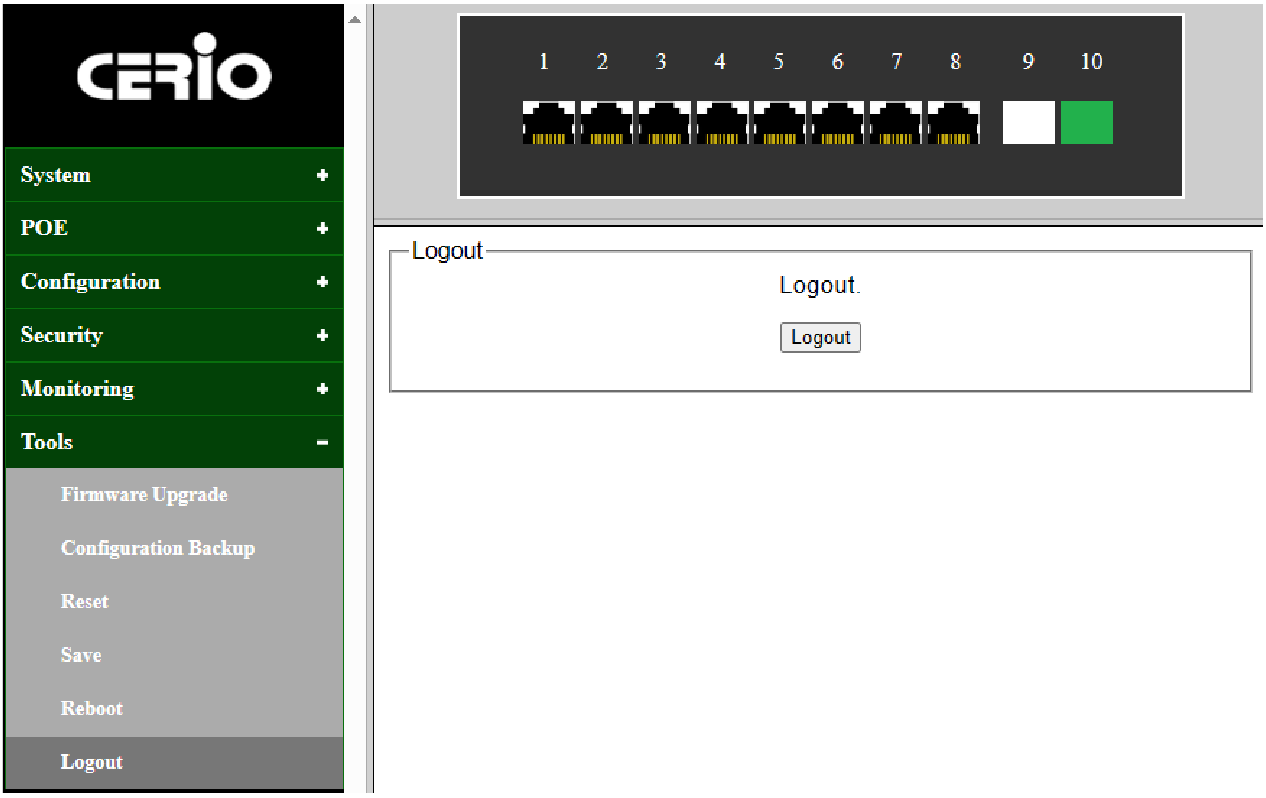
Reboot the switch.

Administrator has to click the “Reboot” button to refresh the Restart the POE Switch.

Notice Please do not turn off the power during the restart process, ensure that the power is stable during the restart process, and avoid forced power off.

8.6 Logout

Click navigation bar: **Tools -> Logout**



Administrator has to click the “Logout” button will log the administrator out of the management page.