

CERIO Corporation

CS-2424G-24P

**PoE CS-2000 Series - 24 Port 10/100/1000M Gigabit Web
Managed PoE+ Switch with 4 SFP Ports (400Watt Power)**



User Manual

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 radiates 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 may be required to take adequate measures.

1.	Introduction	6
1.1	Front Panel.....	6
1.2	Rear Panel Layout.....	7
2.	Software Configuration	8
2.1	Example of Segment: (Windows 7).....	8
2.2	System login username and password information.....	12
3.	System Status	13
3.1	Device Information.....	13
3.2	Port Flow Chart.....	14
3.3	Traffic Statistics.....	14
3.4	MAC Table.....	15
3.5	System Load.....	16
3.6	Network Detection.....	17
4.	Network	18
4.1	IP Address.....	18
4.2	MAC Address.....	19
4.3	DNS Settings.....	19
4.4	DHCP Protect (snooping).....	20
4.5	DHCP Option82.....	21
4.6	IGMP Snooping.....	22
4.7	Multicast VLAN.....	24
4.8	Voice VLAN.....	24
4.9	MAC VLAN.....	26
4.10	802.1x.....	26
4.11	LLDP.....	29
4.12	STP.....	29
4.13	Loop Detection.....	32
4.14	Jumbo Frame.....	33
4.15	RSTP.....	33
5.	Port Configuration	34
5.1	Port Configuration.....	34
5.2	MDIX Configuration.....	35
5.3	Port Mirroring.....	36
5.4	MAC Limit.....	36
5.5	Port Aggregation.....	37
5.6	Port-IP-MAC-Binding.....	39
5.7	Rate Limit.....	40

5.8	Storm Control	41
6.	Security	42
6.1	Port Grouping	43
6.2	Port Isolation	43
6.3	MAC filter	44
6.4	DOS Defense	45
7.	VLAN Configuration	47
7.1	802.1Q VLAN	47
7.2	VLAN Management	48
8.	ACL	48
8.1	MAC ACL	48
8.2	IP ACL	49
9.	QoS	51
9.1	Global Setting	51
9.2	Queue Weight	51
9.3	Queue Algorithm	52
9.4	Default Priority	53
9.5	Priority Mapping	53
9.6	QOS Trust	54
10.	POE Configuration	54
10.1	POE Global Settings	54
10.2	Power Priority	55
10.3	Power Supply	56
10.4	PoE Timing Reboot	57
10.5	Power Limitation	58
10.6	PoE Status	58
10.7	Device Manager	59
11.	System Setting	60
11.1	Quick Settings	60
11.2	Web Management	61
11.3	Administrator	61
11.4	System Config	62
11.5	Firmware Upgrade	63
11.6	System Time	63
11.7	Reboot	64
12.	System Log	66
12.1	Event Log	66



Cerio Corporation

www.cerio.com.tw

12.2 Alarm Log	66
12.3 Security Log	67
12.4 Network Log	67
Specifications	69

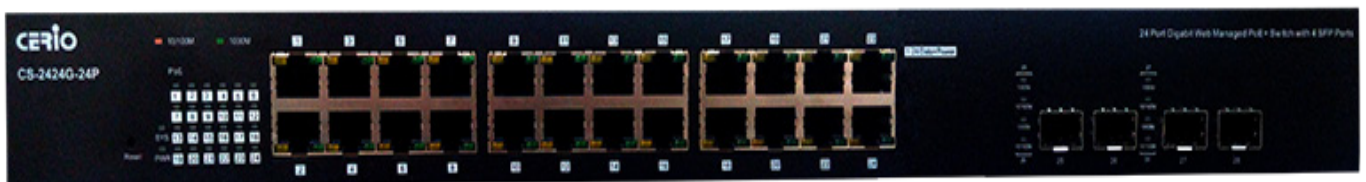
1. Introduction

CERIO CS-2000 Series Model: **CS-2424G-24P** is a powerful high-performance 24 port Gigabit PoE switch, **supporting 4 SFP** uplink ports, and is compliant with POE+ **IEEE 802.3at and 802.3af** standards. This layer 2 Web Management switch includes a 400watt internal power supply, providing a 350watt PoE power budget, and supports Remote on/off control of PoE power ports. CS-2424G-24P layer 2 functions include Spanning Tree and Rapid Spanning Tree Protocol, IEEE802.1Q Tag/Port Based VLAN functions, IEEE802.1p-based/Port-based QoS bandwidth control, IGMP Snooping, Link Aggregation Control Protocol (LACP), and much more. This device can solve the limitation of the power outlet locations and offer the system relocation convenience

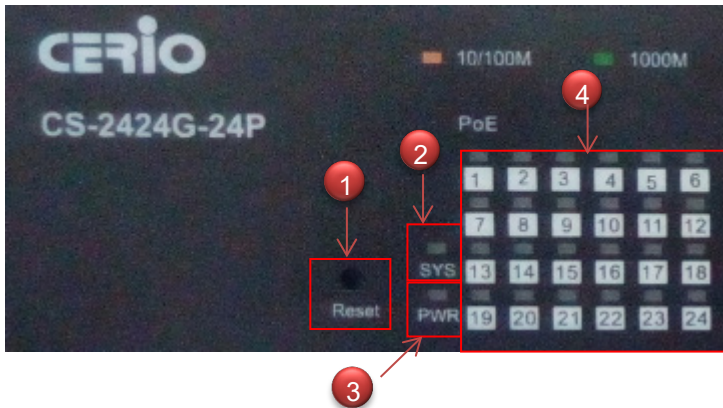
CERIO's **CS-2424G-24P** PoE+ Switch is designed for office deployment and can be upgraded to 1U" chassis for server room installation. CS-2424G-24P is ideal for micro-segmenting large network into smaller networks, connecting subnets for improved performance, and enabling the bandwidth demanded for multimedia and imaging applications. Administrators using CS-2424G-24P can meet the increasing management requirements when deploying **Wireless AP or VoIP phone or IP Camera**. Cerio's web-managed switches offer convenient configuration which ultimately provides premium performance, easy installation, and is sure to meet the increasing demands of growing networks.

1.1 Front Panel

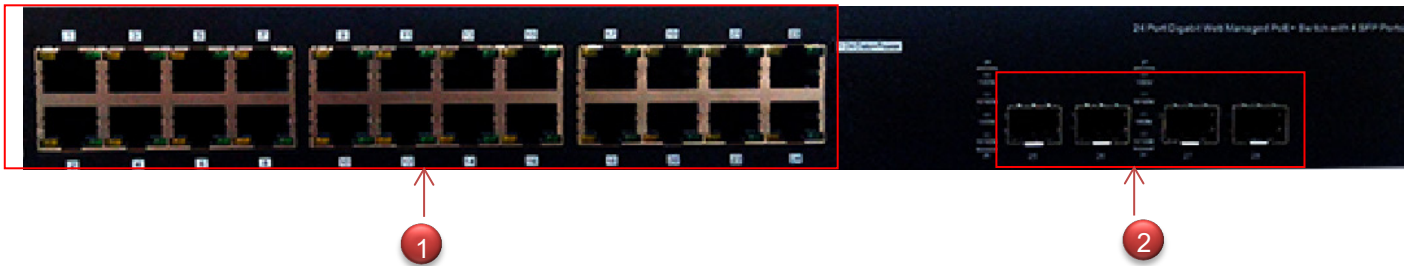
Status LED lights for 24 Port 10/100/1000Mbps with 4 SFP Port



Status Explanation

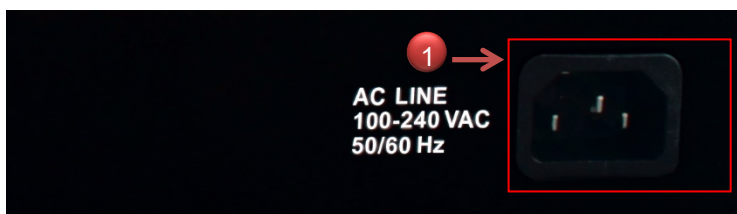


- 1) Hardware Reset button, press and hold for approximately 10 seconds. Once all the LED lights begin to flash, release the button to reset to default
- 2) System operational LED light
- 3) Power LED light.
- 4) 24 Port PoE LED status light.



- 1) 24 10/100/1000Mbps Ethernet Ports, 10/100Mbps is Orange and 1000Mbps is Green lights
- 2) 4 Fiber Ports

1.2 Rear Panel Layout



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

2. Software Configuration

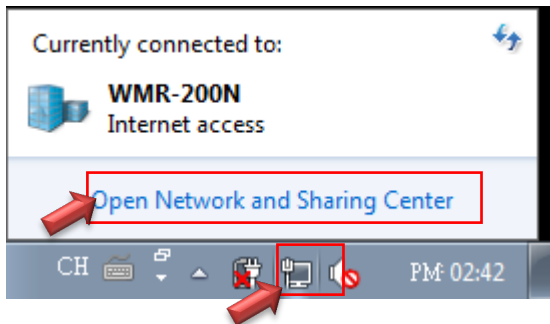
CS-2424G-24P supports web-based configuration. Upon the completion of hardware installation, **CS-2424G-24P** can be configured through a PC/NB by using its web browser such as Internet Explorer 6.0 or later.

Set the IP segment of the administrator's computer to be in the same range as **CS-2424G-24P** for accessing the system. Do not duplicate the IP Address used here with IP Address of **CS-2424G-24P** or any other device within the network. **Please refer to the following steps**

2.1 Example of Segment: (Windows 7)

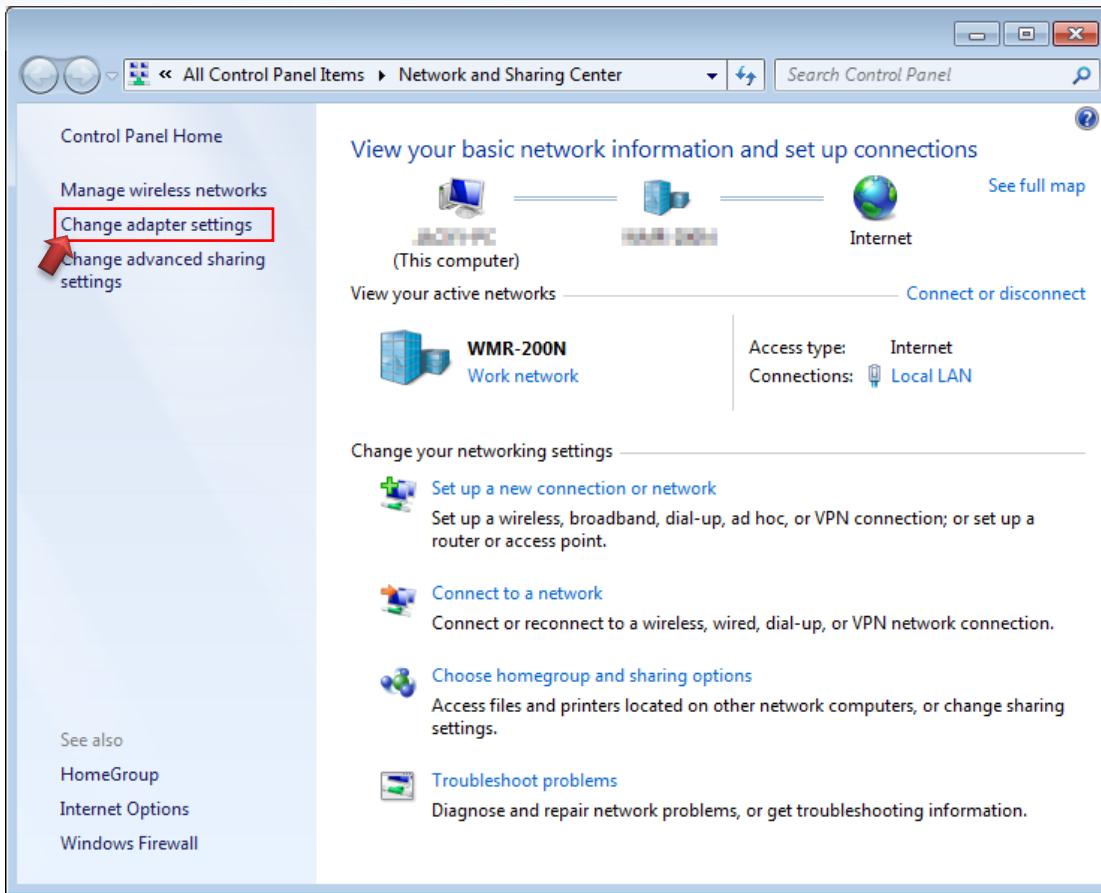
Step 1 :

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



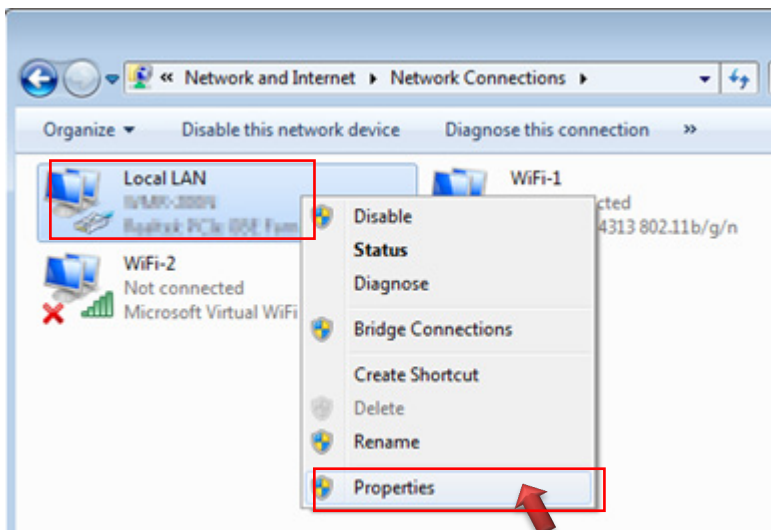
Step 2 :

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



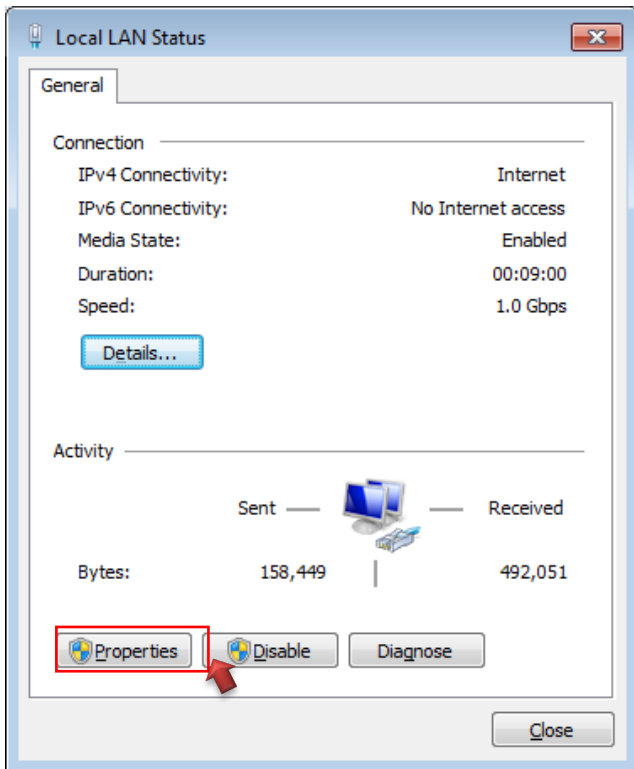
Step 3 :

In “Change adapter setting” Page, right click on Local LAN then select “Properties”



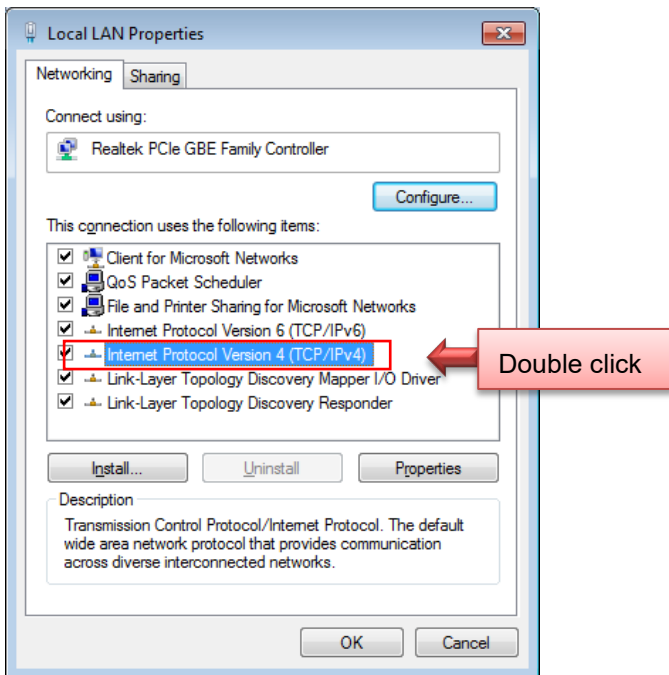
Step 4 :

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



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



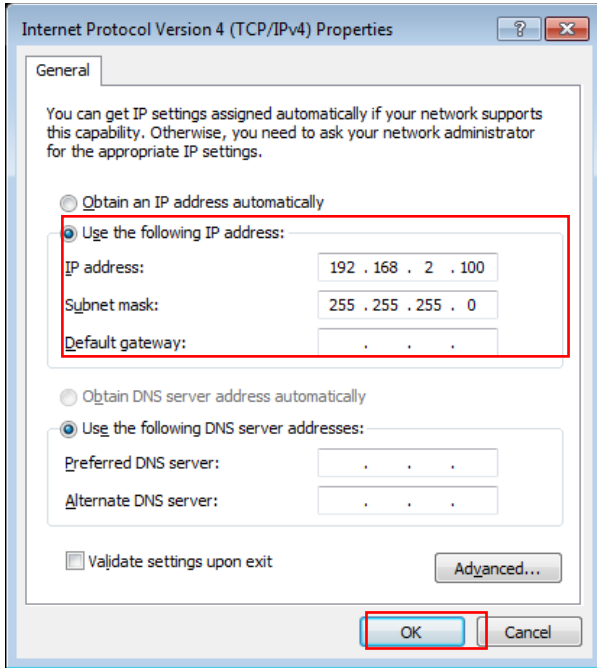
Step 6 :

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

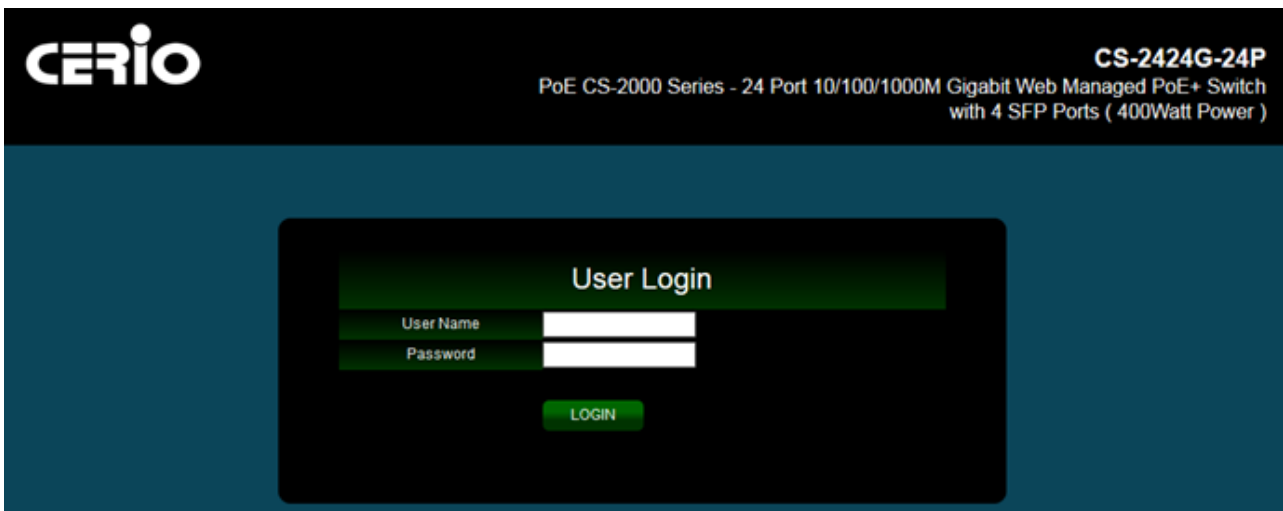
And Click **“OK”** to complete fixing the computer IP settings



Step 7 :

Open Web Browser

Without a valid certificate, users may encounter the following problem in IE7 when they try to access system's WMI (<https://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

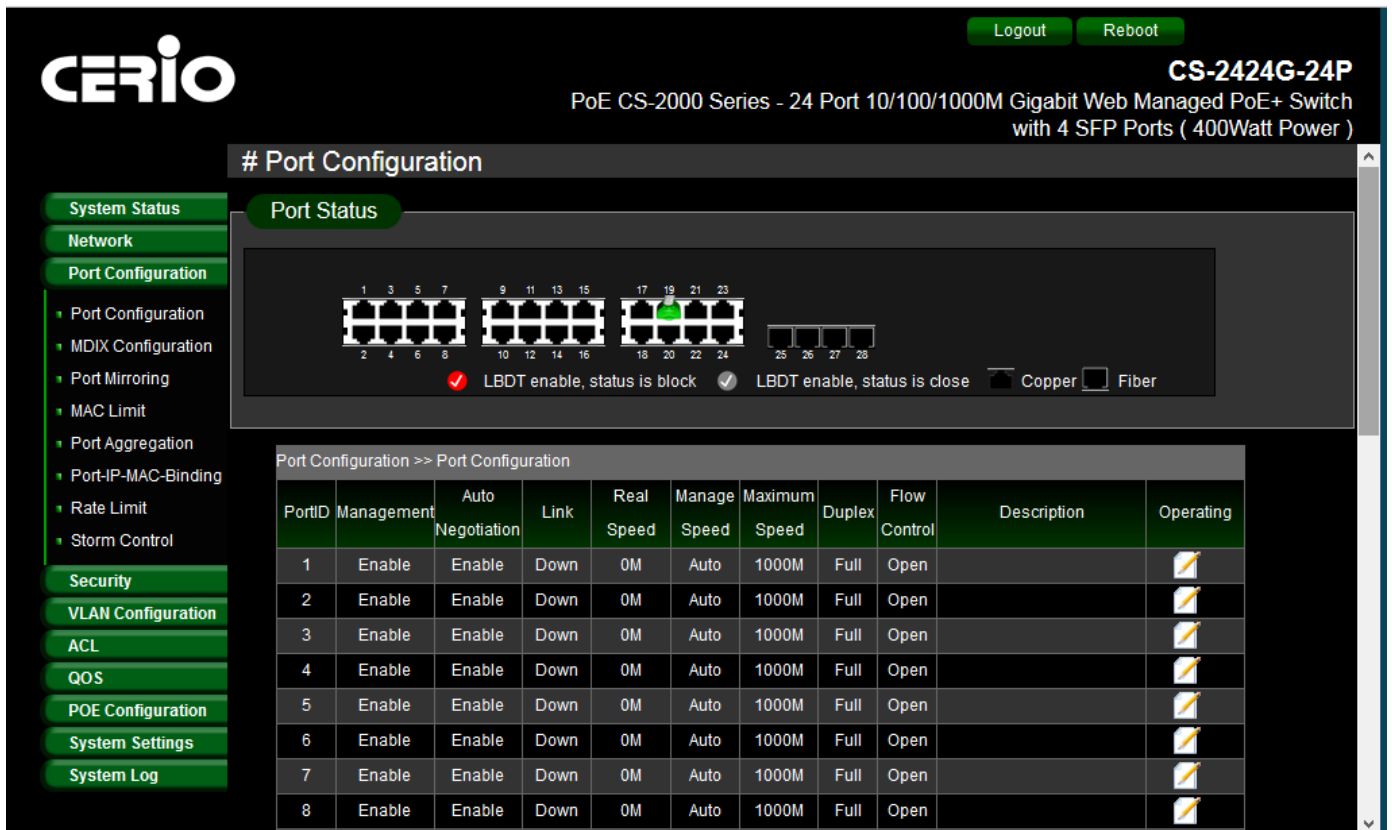
The CS-2424G-24P web switch default IP is 192.168.2.200

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 shows up. Select one of the configurations by clicking the icon.



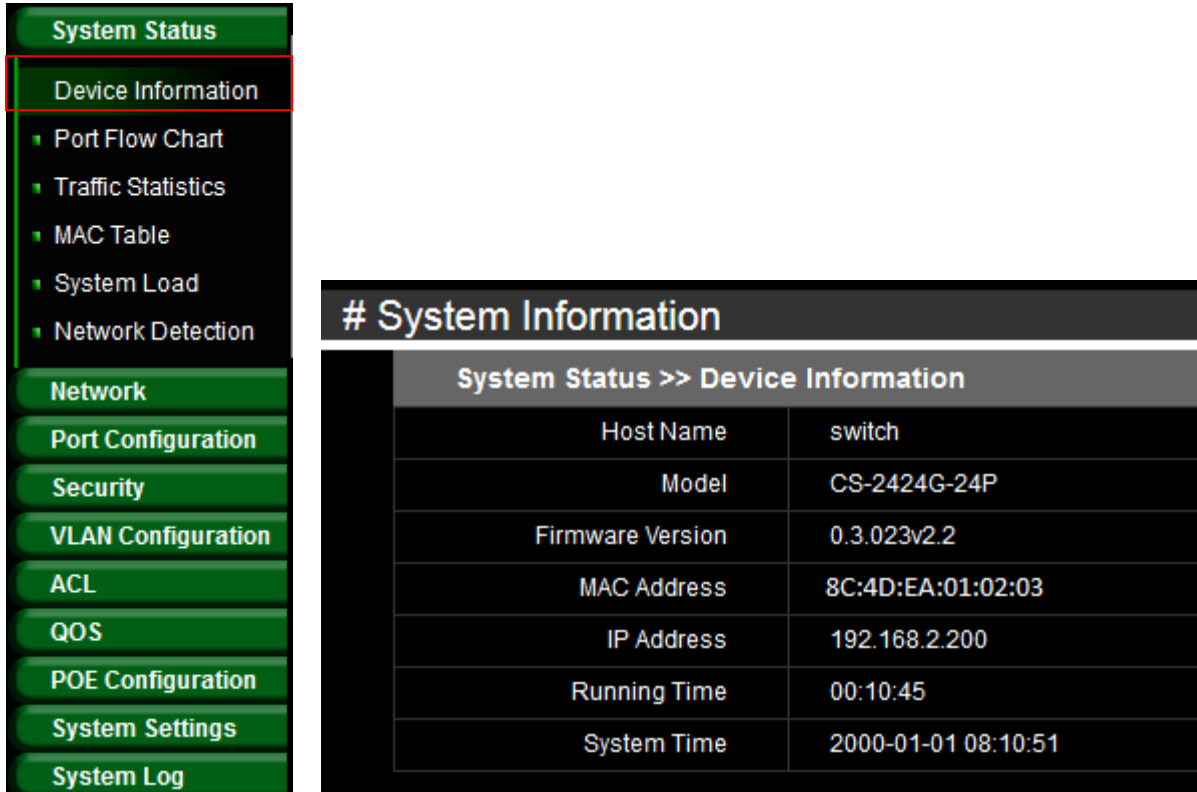
The screenshot shows the CERIO web management interface for a CS-2424G-24P switch. The page title is "# Port Configuration". On the left, there is a navigation menu with options like System Status, Network, Port Configuration, Security, VLAN Configuration, ACL, QOS, POE Configuration, System Settings, and System Log. The main content area shows a "Port Status" section with a visual representation of the switch ports (1-28) and a table of port configuration details.

PortID	Management	Auto Negotiation	Link	Real Speed	Manage Speed	Maximum Speed	Duplex	Flow Control	Description	Operating
1	Enable	Enable	Down	0M	Auto	1000M	Full	Open		
2	Enable	Enable	Down	0M	Auto	1000M	Full	Open		
3	Enable	Enable	Down	0M	Auto	1000M	Full	Open		
4	Enable	Enable	Down	0M	Auto	1000M	Full	Open		
5	Enable	Enable	Down	0M	Auto	1000M	Full	Open		
6	Enable	Enable	Down	0M	Auto	1000M	Full	Open		
7	Enable	Enable	Down	0M	Auto	1000M	Full	Open		
8	Enable	Enable	Down	0M	Auto	1000M	Full	Open		

3. System Status

3.1 Device Information

This administrator can check device system information in the “Device Information” tab



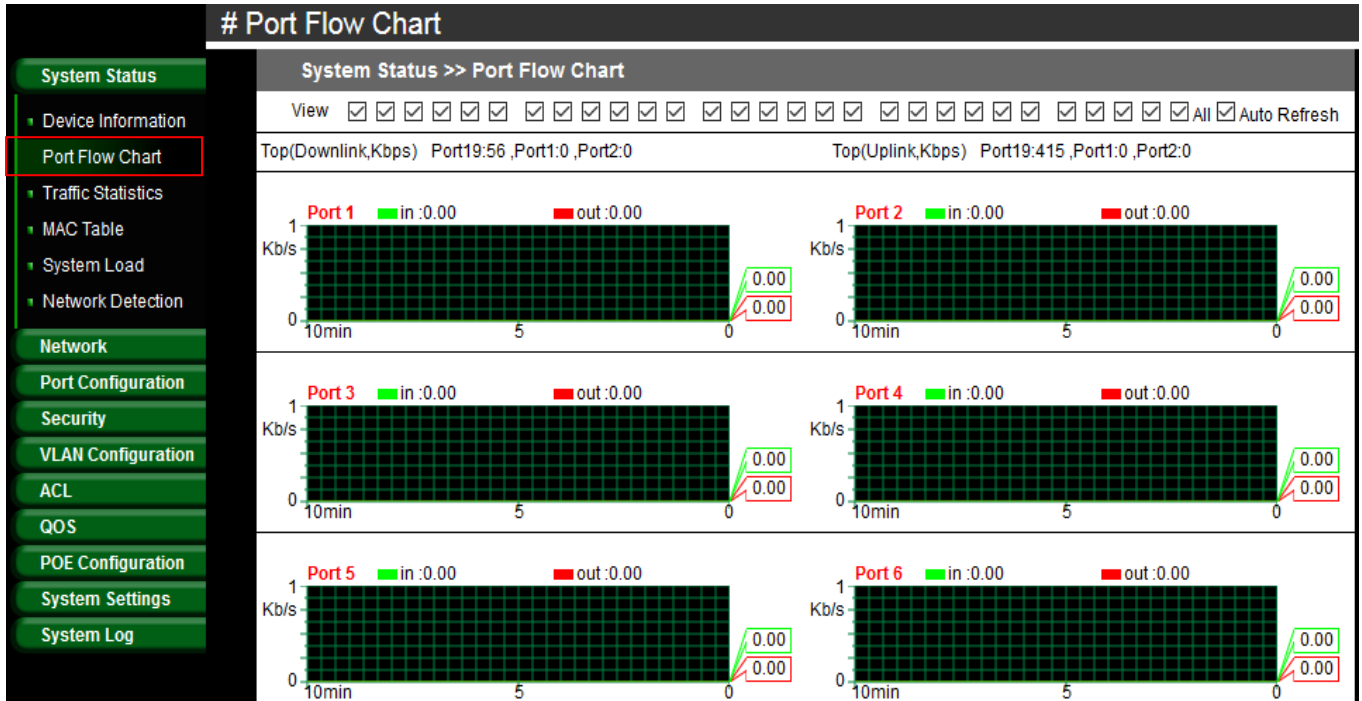
The screenshot shows a sidebar menu on the left with the following items: System Status (highlighted), Device Information (highlighted), Port Flow Chart, Traffic Statistics, MAC Table, System Load, Network Detection, Network, Port Configuration, Security, VLAN Configuration, ACL, QOS, POE Configuration, System Settings, and System Log. The main content area displays the "# System Information" tab, which contains a table titled "System Status >> Device Information".

System Status >> Device Information	
Host Name	switch
Model	CS-2424G-24P
Firmware Version	0.3.023v2.2
MAC Address	8C:4D:EA:01:02:03
IP Address	192.168.2.200
Running Time	00:10:45
System Time	2000-01-01 08:10:51

- **Host Name:** Display host name of the device.
- **Model:** Display switch model name.
- **Firmware Version:** Display system firmware version.
- **MAC Address:** Display MAC address for the device.
- **IP Address:** Display system login IP address.
- **Running Time:** Display system working time.
- **System Time:** Display system time.

3.2 Port Flow Chart

Administrator can monitor ports through graphical flow charts.



➤ **View:** Administrator can select all or one port to monitor.

3.3 Traffic Statistics

Administrator can check the cumulative flow of each port.

# Traffic Statistics					
System Status >> Traffic Statistics					
<input checked="" type="checkbox"/> Auto Refresh					
Port	In/Out Cumulative Flow	In/Out Unicast Packet	In/Out Multicast Packet	In/Out Broadcast Packet	Operating
1	0.00 B / 0.00 B	0 / 0	0 / 0	0 / 0	Reset
2	1.08 MB / 5.76 MB	2333 / 4648	98 / 310	15 / 247	Reset
3	0.00 B / 0.00 B	0 / 0	0 / 0	0 / 0	Reset
4	0.00 B / 0.00 B	0 / 0	0 / 0	0 / 0	Reset
5	0.00 B / 0.00 B	0 / 0	0 / 0	0 / 0	Reset
6	0.00 B / 0.00 B	0 / 0	0 / 0	0 / 0	Reset
7	0.00 B / 0.00 B	0 / 0	0 / 0	0 / 0	Reset
8	0.00 B / 0.00 B	0 / 0	0 / 0	0 / 0	Reset
9	0.00 B / 0.00 B	0 / 0	0 / 0	0 / 0	Reset
10	0.00 B / 0.00 B	0 / 0	0 / 0	0 / 0	Reset
11	0.00 B / 0.00 B	0 / 0	0 / 0	0 / 0	Reset
12	0.00 B / 0.00 B	0 / 0	0 / 0	0 / 0	Reset
13	0.00 B / 0.00 B	0 / 0	0 / 0	0 / 0	Reset

3.4 MAC Table

The MAC Table page can monitor device MAC information based on the connected port. Administrators can set individual ports to static or dynamic MAC addresses. If dynamic MAC Address is selected, administrators can then set dynamic aging time.

- **Forwarding List:** Display MAC address of the devices.
 - **Status:** Administrator can click the status button to change from static to dynamic MAC address.
- **Set Static MAC:** When using a port for a fixed device (e.g. server), administrators can set static MAC address of the port.

- **MAC Address:** Administrator can set the MAC address of the device.
- **VLAN:** Administrator can select for the device network VLAN ID.

- **Port:** Select linked port for the device.

➤ **Dynamic Address settings:** Administrator can set aging Time for Dynamic MAC address.

Forwarding List		Set Static MAC	Dynamic Address Settings
Aging Time	<input type="text"/>	Value Range: 10 - 630	
<input type="button" value="Save"/>			
Information Name		Information Value	
Aging Time		300	

- **Aging Time:** Administrator can set a time for aging time. (Range 10~630 min)

3.5 System Load

System Load function to display the usage status of the memory and the CPU/ Memory of switch via the data graph. If the CPU or Memory usage rate increases sharply, please check to see if you network is secure from hackers or unknown users.

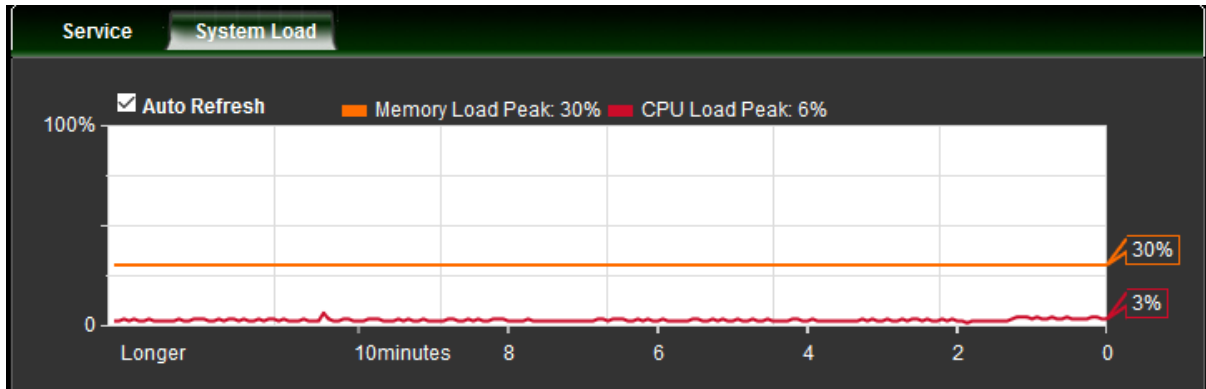
The System Load function is designed with a SNMP Trap function. Administrators can set CPU or Memory Threshold to monitor Switch usage amount. If CPU or Memory Thresholds are surpassed, the system will use SNMP Trap to notify the system administrator.

System Status	Service		System Load	
	<ul style="list-style-type: none"> Device Information Port Flow Chart Traffic Statistics MAC Table System Load Network Detection 	Service	<input type="radio"/> Enable	<input type="radio"/> Disable
	CPU Threshold	<input type="text" value="50%"/>	<input type="text" value="50%"/>	
	Memory Threshold	<input type="text" value="50%"/>	<input type="text" value="50%"/>	
<input type="button" value="Save"/>				
Network				
Port Configuration				

- **Service:** Administrator can select Enable or disable for the service.
- **CPU/Memory Threshold:** Administrator can set CPU or Memory Threshold for the usage warning.

System Load

The Page can display the usage status of the memory and the CPU/ Memory of switch via the data graph.



3.6 Network Detection

Administrators can diagnose network connectivity via the PING or TRACERT

PING		TRACERT	
* Detection Address	<input type="text"/>		
Detection Packets	1 ▾		
<input type="button" value="Detection"/>			

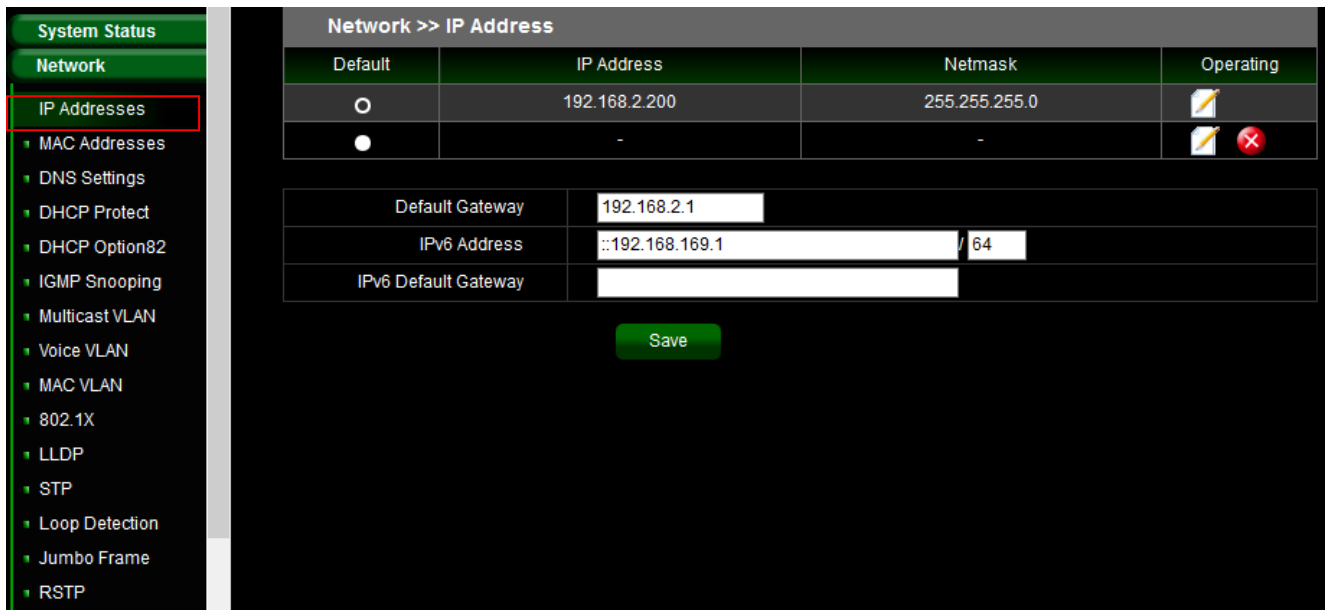
PING		TRACERT	
* Detection Address	<input type="text"/>		
View	First one hop ▾		
<input type="button" value="Detection"/>			

- **Detection Address:** Enter detection IP address.
- **Detection Packets:** Select ping packets frequency.
- **View:** Check device to destination will through hoe many gateway.

4. Network

4.1 IP Address

Administrator can set IP address for the system. The IP address support IPv4 & IPv6 protocol, if switch device must want to internet, administrator can set gateway IP address in the page.



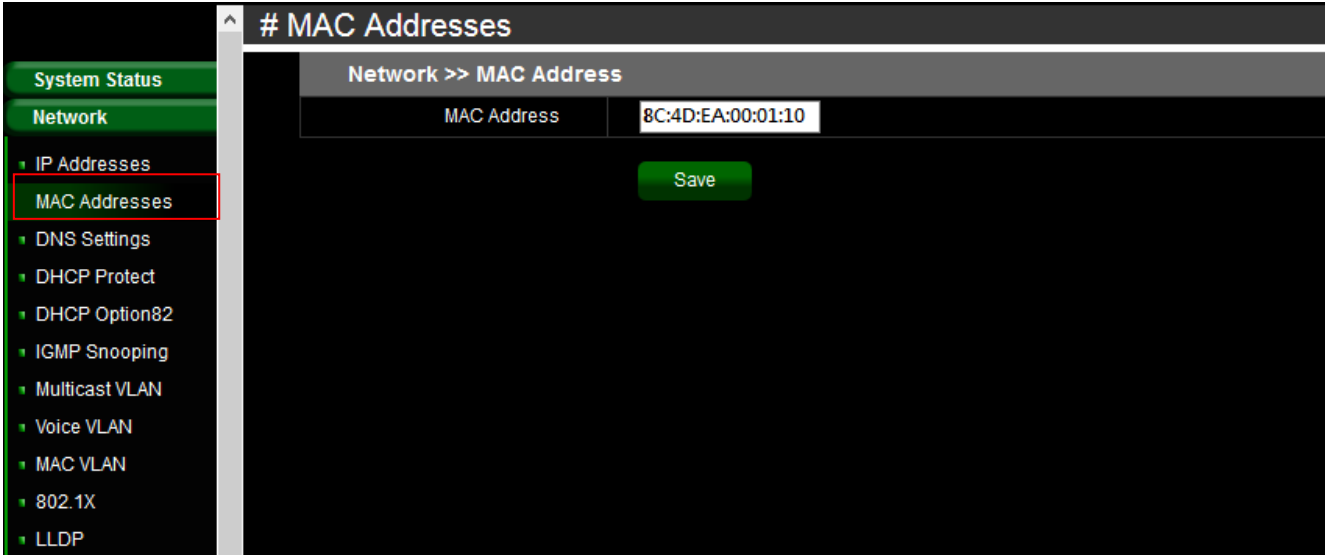
Default	IP Address	Netmask	Operating
<input type="radio"/>	192.168.2.200	255.255.255.0	
<input checked="" type="radio"/>	-	-	

Default Gateway	<input type="text" value="192.168.2.1"/>
IPv6 Address	<input type="text" value="::192.168.169.1"/> / 64
IPv6 Default Gateway	<input type="text"/>

- **List of the Default:** Administrator can select default used IP address.
- **List of the IP address:** Display system IP address.
- **List of the Netmask:** Display Netmask.
- **List of the Operating:** Administrator can click edit to modify system IP address or delete system IP address.
- **Default Gateway:** Administrator can set network gateway.
- **IPv6 Address:** Administrator can set IPv6 address.
- **IPv6 default gateway:** Administrator can set network gateway for IPv6 address.

4.2 MAC Address

Administrator can view and modify the MAC address in the system.



MAC Addresses

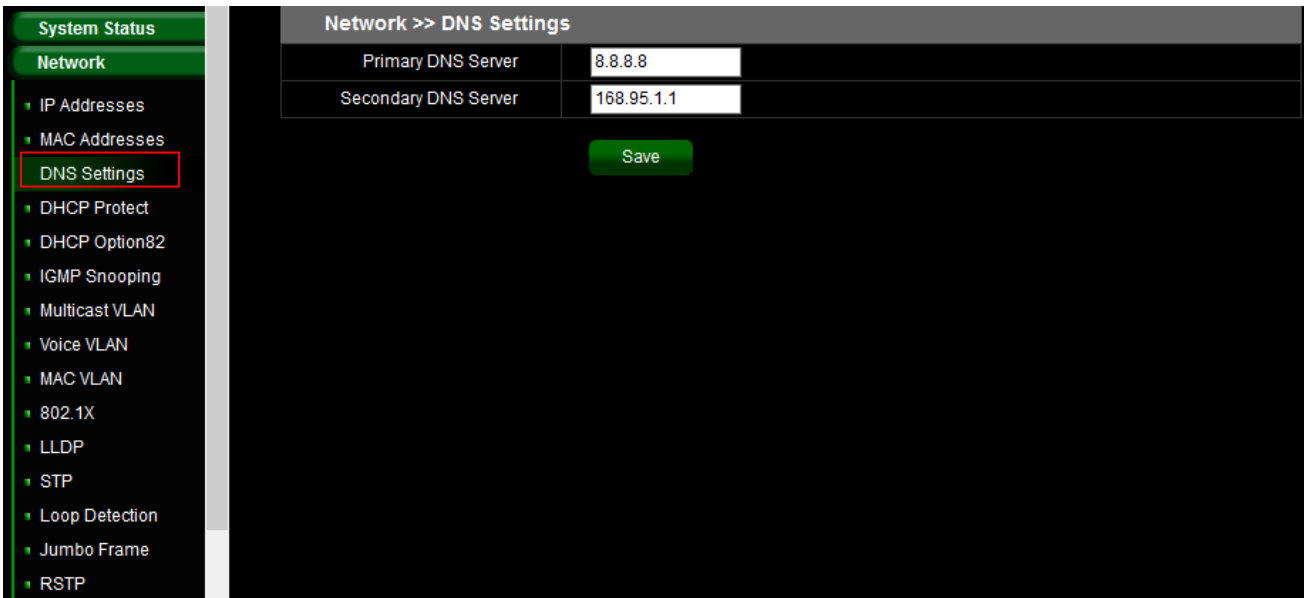
Network >> MAC Address

MAC Address	8C:4D:EA:00:01:10
-------------	-------------------

Save

4.3 DNS Settings

Administrator can set IP Address for the DNS Server.



Network >> DNS Settings

Primary DNS Server	8.8.8.8
Secondary DNS Server	168.95.1.1

Save

- Primary DNS Server: Enter IP address for Primary DNS Server.
- Secondary DNS server: Enter IP address for Secondary DNS server.

4.4 DHCP Protect (snooping)

Administrator can set Dynamic Host Configuration Protocol (DHCP) snooping, preventing interference from other DHCP server.

- Service: Administrator can select Enable or Disable for the DHCP Protect function.
- IP Version: Administrator must select IP protocol of the Version 4 or 6.

Status	Port	Trust Port(s)	Server IP	Server MAC	Remarks	Operating
	8	Trust	-	-	DHCP ...	
	1	Distrust	192.168.2.1	8C:4D:EA:01:95:D6	test ...	

- **Status:** Display the service is on/off.
- **Port:** Display the service used Port.
- **Trust Ports:** Display the service link Port is set trust or Distrust.
- **Service IP / MAC:** If port is set to Distrust, administrator must set IP / MAC address for the DHCP Server.
- **Remarks:** Administrator can set description in the remarks field.
- **Operating:** Administrator can click button to create, modify, or delete the service.

Edit
✕

Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Port	Port8 ▾	
Trust Port(s)	<input type="radio"/> Trust <input checked="" type="radio"/> Distrust	
* DHCP Server IP	<input type="text"/>	[Get MAC]
* DHCP Server MAC	<input type="text"/>	
Remarks	<input type="text" value="DHCP Server"/>	

OK
Cancel

4.5 DHCP Option82

The DHCP Relay Agent Information Option passes along port and agent information to a central DHCP server. It is useful in statistical analysis, as well as, indicating where an assigned IP address physically connects to the network. It may also be used to make DHCP decisions based on where the request is coming from or even which user is making the request.

- System Status
- Network
- IP Addresses
- MAC Addresses
- DNS Settings
- DHCP Protect
- DHCP Option82
- IGMP Snooping
- Multicast VLAN
- Voice VLAN
- MAC VLAN
- 802.1X
- LLDP
- STP
- Loop Detection
- Jumbo Frame
- RSTP

Network >> DHCP Snooping Option82

Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Trust Port(s)	1-24	✎

Save

Network >> DHCP Host Information

To Client Port	To Server Port	Client IP	Server IP	Client MAC	VLAN	Host Name	Lease Time(s)
10	24	192.168.2.21	192.168.2.1	8C:4D:EA:02:C6:ED	1	HP_242_G1-PC	86400

total 1 Page Size 15 ▾ Page No. 1 / 1 First Previous Next Last Goto 1 ▾

- **Status:** Administrator can select Enable or Disable the function.
- **Trist Ports:** Administrator can select Ports for the Trust port.

Edit
✕

Trust Port(s)	<input checked="" type="checkbox"/> 1	<input checked="" type="checkbox"/> 2	<input checked="" type="checkbox"/> 3	<input checked="" type="checkbox"/> 4	<input checked="" type="checkbox"/> 5	<input checked="" type="checkbox"/> 6
	<input checked="" type="checkbox"/> 7	<input checked="" type="checkbox"/> 8	<input checked="" type="checkbox"/> 9	<input checked="" type="checkbox"/> 10	<input checked="" type="checkbox"/> 11	<input checked="" type="checkbox"/> 12
	<input checked="" type="checkbox"/> 13	<input checked="" type="checkbox"/> 14	<input checked="" type="checkbox"/> 15	<input checked="" type="checkbox"/> 16	<input checked="" type="checkbox"/> 17	<input checked="" type="checkbox"/> 18
	<input checked="" type="checkbox"/> 19	<input checked="" type="checkbox"/> 20	<input checked="" type="checkbox"/> 21	<input checked="" type="checkbox"/> 22	<input checked="" type="checkbox"/> 23	<input checked="" type="checkbox"/> 24
	<input type="checkbox"/> 25	<input type="checkbox"/> 26	<input type="checkbox"/> 27	<input type="checkbox"/> 28		

OK
Cancel

➤ **DHCP Host Information:**

Network >> DHCP Host Information							
To Client Port	To Server Port	Client IP	Server IP	Client MAC	VLAN	Host Name	Lease Time(s)
10	24	192.168.2.21	192.168.2.1	8C:4D:EA:...	1	...-PC	86400

total 1
Page Size 15
Page No. 1 / 1
First Previous Next Last
Goto 1

- **To Client Port:** Display port number of the client send request.
- **To Server Port:** Display port number for the DHCP server response.
- **Client IP:** Display IP address for client.
- **Server IP:** Display IP address for DHCP Server.
- **Client MAC:** Display MAC address for client.
- **VLAN:** Display VLAN ID for client.
- **Host Name:** Display client device name.
- **Lease Time:** Display IP address use lease Time.

4.6 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. The IGMP snooping support v2 & v3, administrator can forward or drop Unknown Multicast.

The screenshot displays the 'Basic Configuration' and 'Multicast Table' sections of the Cerio interface. The 'IGMP Snooping' configuration includes:

- IGMP Snooping:** Enable Disable
- version:** V2 V3
- Unknown Multicast:** Forward Drop
- Router Port:** -
- Port Fast Leave:** -

The 'IGMP Snooping >> Querier' section includes:

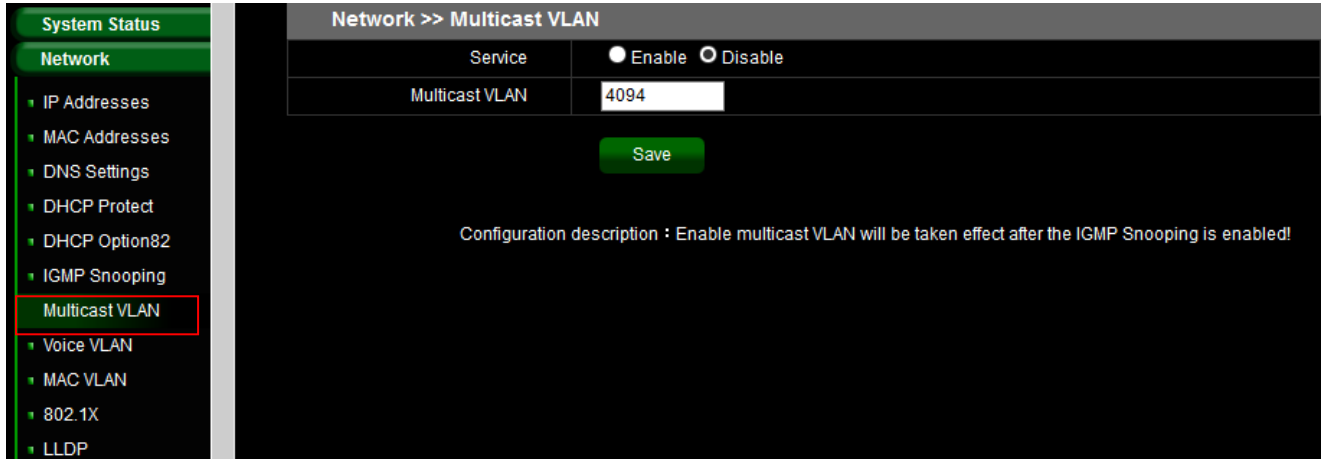
- Status Operation:** Enable Disable
- Query Interval:** 60 S

- **IGMP Snooping:** Administrator can select enable or disable for the service.
- **Version:** Administrator can select v2 or v3 for the IGMP version.
- **Unknown Multicast:** Administrator can forward or drop Unknown Multicast.
- **Router Port:** Set router port.
- **Port Fast Leave:** In Port Fast Leave mode, when the switch receives IGMP leave packets, the switch will close the multicast stream immediate without any further action. In fast leave mode, the switch will further generate a group specific query packet to all the receivers. This feature could prevent the traffic being cut if some receivers still want to receive the multicast stream.
- **Status Operation:** Administrator can enable or disable the service.
- **Query Interval:** This switch query can send packets to the corresponding port, administrator can set query Interval.

This close-up view shows the 'IGMP Snooping >> Querier' configuration area. It features a 'Status Operation' section with radio buttons for 'Enable' (selected) and 'Disable'. Below it is a 'Query Interval' field containing the value '60' followed by an 'S' for seconds. A green 'Save' button is positioned at the bottom of the configuration area.

4.7 Multicast VLAN

In multicast VLAN networks, subscribers to a multicast group can exist in VLAN. Administrator can set multicast VLAN ID, multicast VLAN by its VLAN ID in the range of 1 to 4094.



Network >> Multicast VLAN	
Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Multicast VLAN	4094

Save

Configuration description : Enable multicast VLAN will be taken effect after the IGMP Snooping is enabled!

- **Service:** Administrator can select enable or disable the Service
- **Multicast VLAN:** Administrator can set VLAN ID in the range of 1 to 4094.

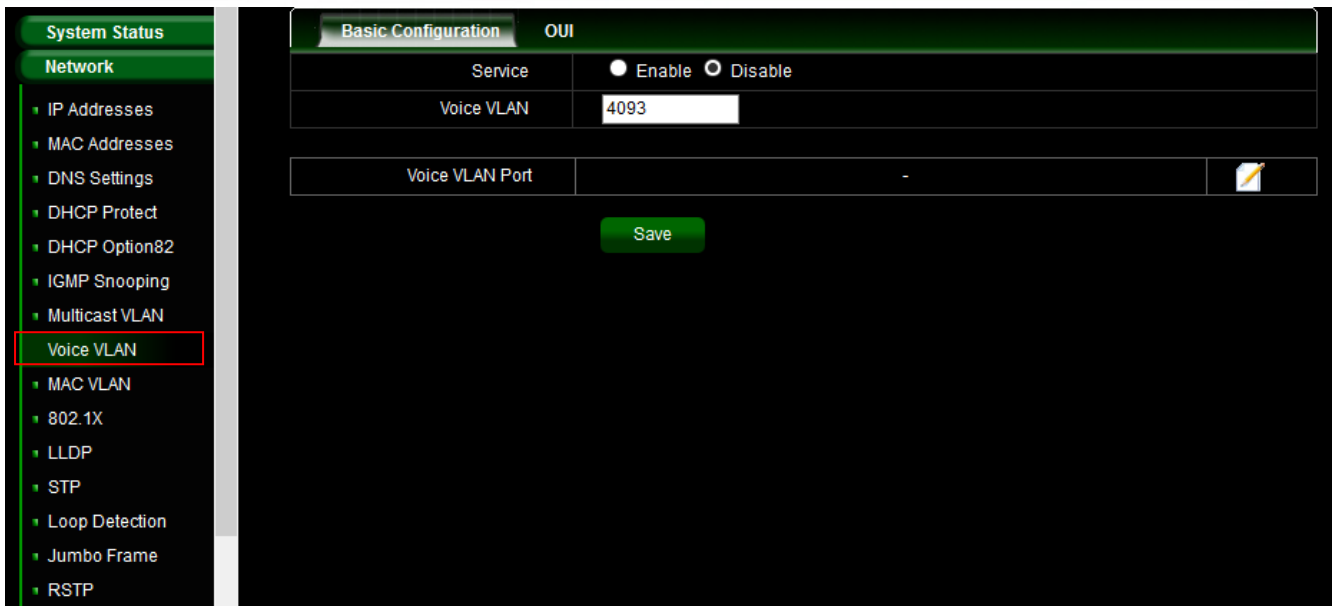


Notice

Configuration description : Enable multicast VLAN will be taken effect after the IGMP Snooping is enabled!

4.8 Voice VLAN

Voice VLAN allows you to enhance VoIP service by configuring ports to carry IP Voice traffic from IP phones on a specific VLAN. VoIP traffic has a preconfigured OUI prefix in the source MAC address. Administrator can set VLAN ID in the range of 1 to 4094.



- **Service:** Administrator can select enable or disable the Service
- **Voice VLAN:** Administrator can set VLAN ID in the range of 1 to 4094.
- **Voice VLAN Port:** Administrator can select ports for the voice VLAN.

OUI

Organizationally Unique Identifiers (OUI) is the first three bytes of a MAC Address, while the last three bytes contain a unique station ID. Administrator can add a specific manufacturer with the OUI. Once the OUI is added, all traffic received on voice VLAN ports from the specific IP phone with a listed OUI is forwarded on the voice VLAN. Unlike the telephony OUI mode that detects voice devices based on telephony OUI, Auto Voice VLAN mode depends on auto smart port to dynamically add the ports to the voice VLAN. The default has set 5 companies for the voice phone.

Basic Configuration		OUI	
Number	OUI	Company	Operating
1	00:03:6B:00:00:00	Cisco phone	
2	00:0F:E2:00:00:00	H3C Aolynk phone	
3	00:D0:1E:00:00:00	Pingtel phone	
4	00:E0:75:00:00:00	Polycom phone	
5	00:E0:BB:00:00:00	3Com phone	

4.9 MAC VLAN

A MAC VLAN takes a single Network interface and creates multiple virtual ones with different MAC addresses (many to one).

System Status

Network

- IP Addresses
- MAC Addresses
- DNS Settings
- DHCP Protect
- DHCP Option82
- IGMP Snooping
- Multicast VLAN
- Voice VLAN
- MAC VLAN**
- 802.1X
- LLDP
- STP
- Loop Detection
- Jumbo Frame
- RSTP

Network >> MAC VLAN

MAC VLAN Enable Disable

SMAC	SMAC Mask	VLAN	Operating
8C:4D:EA:04:03:02	11:22:33:44:55:66	1	
8C:4D:EA:04:03:02	00:11:22:33:44:55	1	
8C:4D:EA:04:03:02	66:55:44:33:22:11	1	
8C:4D:EA:04:03:02	00:00:00:00:00:11	1	
01:02:03:04:05:06	11:11:11:11:11:11	1	

Save The configuration has been modified, please save in time

➤ **MAC VLAN:** Administrator can enable or disable the service.



Administrator can click button to create MAC VLAN.

4.10 802.1x

When client uses a RJ-45 link to switch port, the switch port will request 802.1x authentication of the client. If authentication fails, the switch port will stop using packet flow.

802.1X Configuration Server Configuration User Info

Service: Enable Disable

Auth Method:

802.1X Port Configuration							
Port	Status	Port Mode	Control Mode	Max Users	Period Re-auth	Broadcast	Operating
1	Enable	Port-Based	Auto	256	Enable	Disable	
2	Disable	MAC-Based	Auto	256	Enable	Disable	
3	Disable	MAC-Based	Auto	256	Enable	Disable	
4	Disable	MAC-Based	Auto	256	Enable	Disable	
5	Disable	MAC-Based	Auto	256	Enable	Disable	
6	Disable	MAC-Based	Auto	256	Enable	Disable	
7	Disable	MAC-Based	Auto	256	Enable	Disable	
8	Disable	MAC-Based	Auto	256	Enable	Disable	

802.1x Configuration

- Service: Administrator can enable or disable the 802.1x authentication service.
- Auth Method: Administrator can select authentication method for 802.1x.

Administrator can click button in the Operating list to modify authentication function.

Edit

Port	<input type="text" value="1"/>
Status	<input type="text" value="Enable"/>
Port Mode	<input type="text" value="Port-Based"/>
Control Mode	<input type="text" value="Auto"/>
Max Users	<input type="text" value="256"/>
Period Re-auth	<input type="text" value="Enable"/>
Broadcast	<input type="text" value="Disable"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

- **Port:** Display Port number.
- **Status:** Administrator can select enable or disable the service.
- **Port Mode:** Administrator can select used Port/MAC-Based type.
- Max Users: Administrator can set 1-256.
- Period Re-auth: Administrator can select enable or disable for the Period Re-auth.
- Broadcast: Administrator can select enable or disable the broadcast mode.

Server Configuration

802.1X Configuration	Server Configuration	User Info		
Auth Key	<input type="text" value=""/>	The characters length of auth key can't be greater than 32!		
Num Of Retry	<input type="text" value="3"/>			
<input type="button" value="Save"/>				
The Primary(Backup) Server				
Name	IP Address	Port Number	Status	Operating
Primary Server	192.168.	1812	Active	
Backup Server	0.0.0.0	1812	Active	
Advanced Configuration: <input type="button" value="v"/>				

- **Auth Key:** Enter RADIUS Server Key.
- **Num Of Retry:** Enter re-check frequency.
- **Primary Server:** Administrator can set RADIUS Server information for Primary.
- **Backup Server:** Administrator can set RADIUS Server information for Backup.

User Info: Administrator can monitor user authentication information.

802.1X Configuration	Server Configuration	User Info	
Port	Status	Sum Of Users	Operating
1	Enable	0	<input type="button" value="View Details"/>
2	Disable	0	<input type="button" value="View Details"/>
3	Disable	0	<input type="button" value="View Details"/>
4	Disable	0	<input type="button" value="View Details"/>
5	Disable	0	<input type="button" value="View Details"/>
6	Disable	0	<input type="button" value="View Details"/>
7	Disable	0	<input type="button" value="View Details"/>
8	Disable	0	<input type="button" value="View Details"/>
9	Disable	0	<input type="button" value="View Details"/>
10	Disable	0	<input type="button" value="View Details"/>

4.11 LLDP

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, principally wired Ethernet.

LLDP information is sent by devices from each of their interfaces at a fixed interval, in the form of an Ethernet frame. Each frame contains one LLDP Data Unit (LLDPDU). Each LLDPDU is a sequence of type-length-value (TLV) structures.

Port	Port Status	Operating
1	Disable	
2	Disable	
3	Disable	
4	Disable	

- **LLDPDU Send Interval:** Set LLDPDU Send Interval(value range 5-32760) for LLDP
- **TTL Multiplier:** Set TTL Multiplier (value range 2-10) for LLDP.
- **LLDPDU Send Delay:** Set LLDPDU Send Delay (value range 1-8192) for LLDP.
- **Port Initialize Delay Time:** Set Port Initialize Delay Time (value range 1-10) for LLDP.

4.12 STP

The Spanning Tree Protocol (STP) is a network protocol that builds a logical loop-free topology for Ethernet networks. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. Spanning tree also allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling or disabling of these backup links.










System Status	STP Configuration	STP Port Configuration	STP Port Information
Network	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
IP Addresses	Bridge Priority	32768	
MAC Addresses	HelloTime	2	
DNS Settings	Forward Delay	15	
DHCP Protect	Max Age	20	
DHCP Option82	Save		
IGMP Snooping	Configuration description: Max Age value is not less than 2 times (Hello Time + 1), namely: $2 * (\text{Hello Time} + 1) \leq \text{Max Age}$ Max Age is not greater than 2 times(Forward Delay + 1), namely: $\text{Max Age} \leq 2 * (\text{Forward Delay} - 1)$		
Multicast VLAN			
Voice VLAN			
MAC VLAN			
802.1X			
LLDP			
STP			
Loop Detection			
Jumbo Frame			
RSTP			

- **Service:** Administrator can select enable or disable the STP service.
- **Bridge Priority:** The default Bridge Priority (Switch Priority) value of 32,768. Bridge Priority (Switch Priority) value decides which Switch can become Root Bridge (Root Switch).
- **HelloTime: Set HelloTime** (value range 1-10) for STP.
- **Forward Delay:** Set Forward Delay (value range 4-30) for STP.
- **Max Age:** Set Max Age (value range 6-40) for STP.



Max Age value is not less than 2 times (Hello Time + 1), namely: $2 * (\text{Hello Time} + 1) \leq \text{Max Age}$
 Max Age is not greater than 2 times(Forward Delay + 1), namely: $\text{Max Age} \leq 2 * (\text{Forward Delay} - 1)$

STP Port Configuration

STP Configuration		STP Port Configuration		STP Port Information	
Port	Status	Priority	Path Cost	Loopback Protect	Operating
1	Disable	128	100	Disable	
2	Disable	128	100	Disable	
3	Disable	128	100	Disable	
4	Disable	128	100	Disable	
5	Disable	128	100	Disable	
6	Disable	128	100	Disable	
7	Disable	128	100	Disable	
8	Disable	128	100	Disable	
9	Disable	128	100	Disable	
10	Disable	128	100	Disable	
11	Disable	128	100	Disable	
12	Disable	128	100	Disable	
13	Disable	128	100	Disable	

Administrator can click Operating list button to set STP service.

Edit
✕

Port	<input type="text" value="1"/>
Status	<input type="text" value="Disable"/> ▾
Priority	<input type="text" value="128"/> ▾
Path Cost	<input type="text" value="100"/>
Loopback Protect	<input type="text" value="Disable"/> ▾
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

STP Port Information

Display STP information for all Port

STP Configuration	STP Port Configuration	STP Port Information	
Port	Status	Destination Root MAC	Destination Bridge MAC
1	Disabled	00:00:00:00:00:00	00:00:00:00:00:00
2	Disabled	00:00:00:00:00:00	00:00:00:00:00:00
3	Disabled	00:00:00:00:00:00	00:00:00:00:00:00
4	Disabled	00:00:00:00:00:00	00:00:00:00:00:00
5	Disabled	00:00:00:00:00:00	00:00:00:00:00:00
6	Disabled	00:00:00:00:00:00	00:00:00:00:00:00
7	Disabled	00:00:00:00:00:00	00:00:00:00:00:00
8	Disabled	00:00:00:00:00:00	00:00:00:00:00:00
9	Disabled	00:00:00:00:00:00	00:00:00:00:00:00
10	Disabled	00:00:00:00:00:00	00:00:00:00:00:00
11	Disabled	00:00:00:00:00:00	00:00:00:00:00:00

4.13 Loop Detection

Loop detection can be used in an MCT topology to detect Layer 2 loops that occur due to misconfigurations, for example, on the client side when MCT links are not configured as trunk links on the MCT-unaware client. Administrator can click Operating list button to set Action for Port shutdown or Port Blocking.

System Status

Network

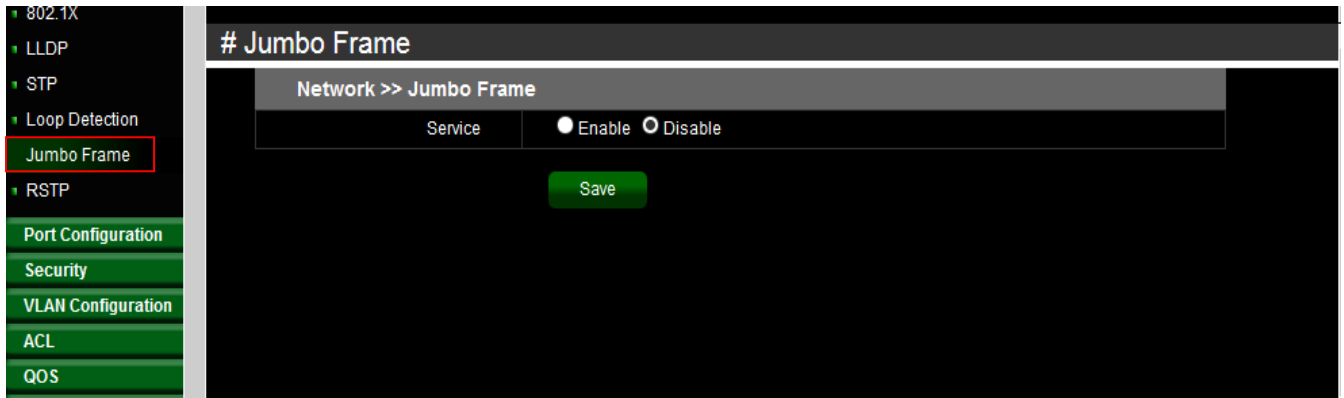
- IP Addresses
- MAC Addresses
- DNS Settings
- DHCP Protect
- DHCP Option82
- IGMP Snooping
- Multicast VLAN
- Voice VLAN
- MAC VLAN
- 802.1X
- LLDP
- STP
- Loop Detection
- Jumbo Frame
- RSTP

Save

Loop Detection >> Port Settings				
Port	Loop Status	Action	Status	Operating
1	Disable	Port Shutdown	-	
2	Disable	Port Shutdown	-	
3	Disable	Port Shutdown	-	
4	Disable	Port Shutdown	-	
5	Disable	Port Shutdown	-	
6	Disable	Port Shutdown	-	
7	Disable	Port Shutdown	-	
8	Disable	Port Shutdown	-	
9	Disable	Port Shutdown	-	
10	Disable	Port Shutdown	-	
11	Disable	Port Shutdown	-	
12	Disable	Port Shutdown	-	

4.14 Jumbo Frame

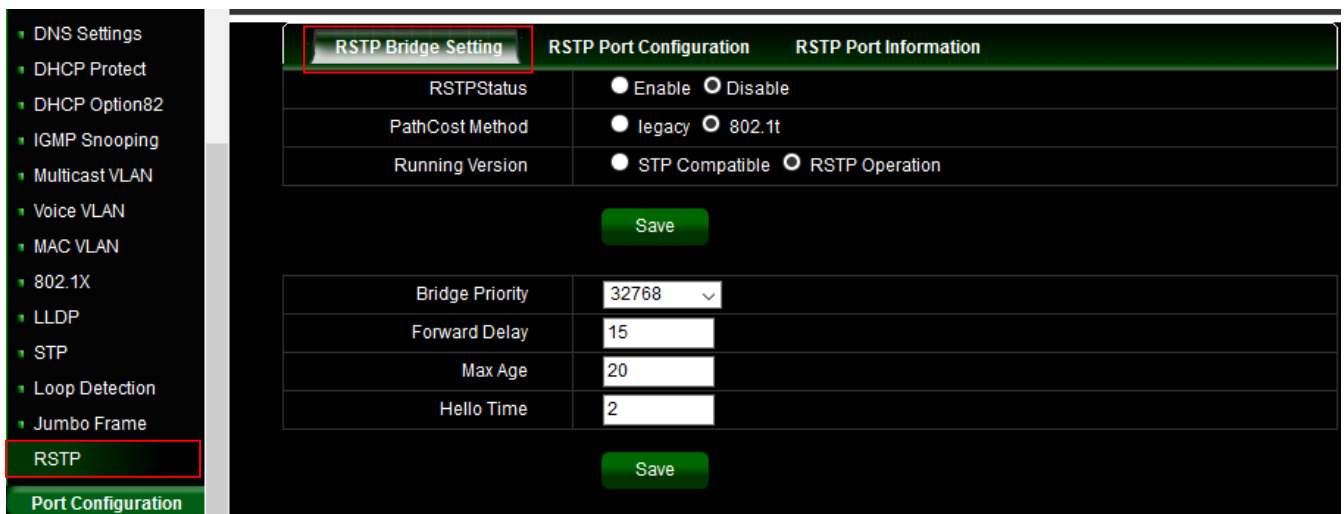
A jumbo frame is an Ethernet frame with a payload greater than the standard maximum transmission unit (MTU) of 1,500 bytes. Jumbo frames are used on local area networks that support at least 1 Gbps and can be as large as 9,000 bytes. Administrator can select enable or disable the service.



The screenshot shows the configuration page for Jumbo Frame. On the left is a navigation menu with items like 802.1X, LLDP, STP, Loop Detection, Jumbo Frame (highlighted), RSTP, Port Configuration, Security, VLAN Configuration, ACL, and QOS. The main content area is titled '# Jumbo Frame' and contains a sub-header 'Network >> Jumbo Frame'. Below this is a table with one row: 'Service' with radio buttons for 'Enable' (selected) and 'Disable'. A green 'Save' button is located below the table.

4.15 RSTP

Rapid Spanning Tree Protocol (RSTP; IEEE 802.1w) can be seen as an evolution of the 802.1D standard more than a revolution. The 802.1D terminology remains primarily the same. Most parameters have been left unchanged so users familiar with 802.1D can rapidly configure the new protocol comfortably.



The screenshot shows the configuration page for RSTP Bridge Setting. On the left is a navigation menu with items like DNS Settings, DHCP Protect, DHCP Option82, IGMP Snooping, Multicast VLAN, Voice VLAN, MAC VLAN, 802.1X, LLDP, STP, Loop Detection, Jumbo Frame, RSTP (highlighted), and Port Configuration. The main content area has three tabs: 'RSTP Bridge Setting' (highlighted), 'RSTP Port Configuration', and 'RSTP Port Information'. Under the 'RSTP Bridge Setting' tab, there is a table with three rows: 'RSTPStatus' with radio buttons for 'Enable' (selected) and 'Disable'; 'PathCost Method' with radio buttons for 'Legacy' (selected) and '802.1t'; and 'Running Version' with radio buttons for 'STP Compatible' (selected) and 'RSTP Operation'. A green 'Save' button is below the table. Below this table is another table with four rows: 'Bridge Priority' with a dropdown menu showing '32768'; 'Forward Delay' with a text input field containing '15'; 'Max Age' with a text input field containing '20'; and 'Hello Time' with a text input field containing '2'. A second green 'Save' button is at the bottom of this section.

4.16 SNMP

Using SNMP, you can monitor network performance, audit network usage, detect network faults or inappropriate access, and in some cases configure remote devices. SNMP is designed to be deployed on the largest possible number of network devices, to have minimal impact on the managed nodes, to have minimal transport requirements, and to continue working when most other network applications fail.

This system support v1 / v2 / v3 and Trap for the SNMP. Administrator can choose version of the SNMP function.

Set	Community	User	Trap
SNMP			<input type="radio"/> Enable <input type="radio"/> Disable
SNMP Trap			<input type="radio"/> Enable <input type="radio"/> Disable
Local Engine ID		8000000001020304	
Contact Info		contact@mail.com	
Physical Location Information		location.where	
SNMP Version			<input type="checkbox"/> v1 <input type="checkbox"/> v2c <input checked="" type="checkbox"/> v3

5. Port Configuration

5.1 Port Configuration

System Status
Network
Port Configuration

Port Configuration
MDIX Configuration
Port Mirroring
MAC Limit
Port Aggregation
Port-IP-MAC-Binding
Rate Limit
Storm Control

Security
VLAN Configuration
ACL
QOS

Port Status

Port Configuration >> Port Configuration

PortID	Management	Auto Negotiation	Link	Real Speed	Manage Speed	Maximum Speed	Duplex	Flow Control	Description	Operating
1	Enable	Enable	Down	0M	Auto	1000M	Full	Open		
2	Enable	Enable	Down	0M	Auto	1000M	Full	Open		
3	Enable	Enable	Down	0M	Auto	1000M	Full	Open		
4	Enable	Enable	Down	0M	Auto	1000M	Full	Open		

Administrator can click Operating list button to modify port Operation.

Edit

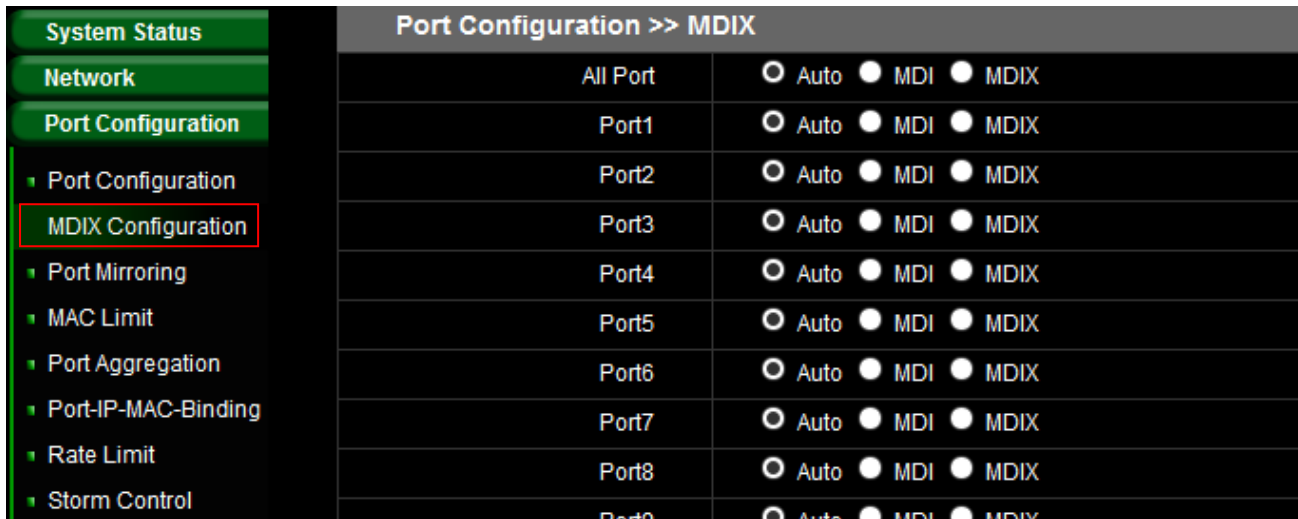
Port	1
Status	Enable
Auto Negotiation	Enable
Link	Down
Manage Speed	1000M
Maximum Speed	1000
Duplex	Full
Flow Control	Open
Description	

OK **Cancel**

5.2 MDIX Configuration

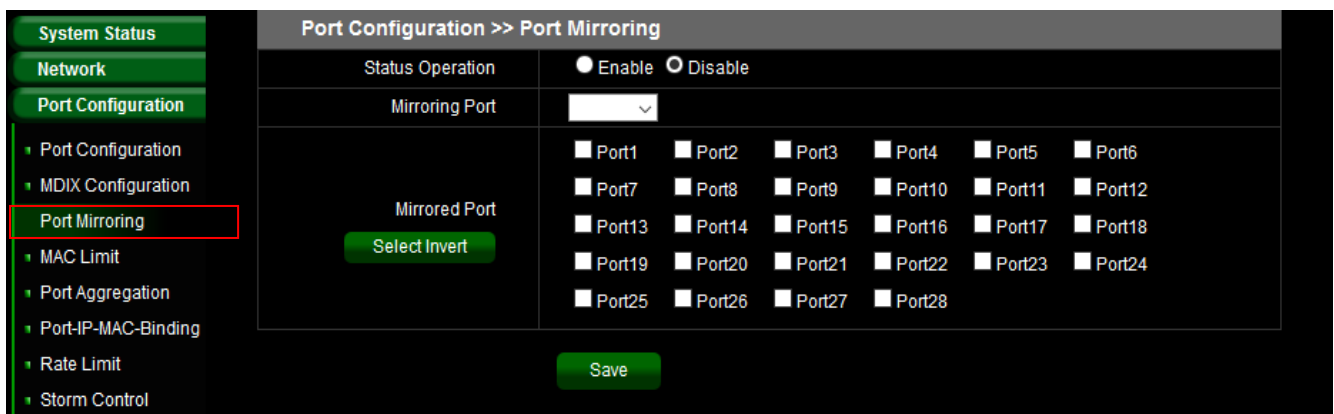
A medium dependent interface (MDI) describes the interface (both physical and electrical) in a computer network from a physical layer implementation to the physical medium used to

carry the transmission. Ethernet over twisted pair also defines a medium dependent interface crossover (MDI-X) interface. Auto MDI-X ports on newer network interfaces detect if the connection would require a crossover, and automatically chooses the MDI or MDI-X configuration to properly match the other end of the link.



5.3 Port Mirroring

Port mirroring function can mirror Rx/Tx traffic, Packet can mirror to Destination port and for analysis.



- **Status Operation:** Administrator can select enable or disable the function.
- **Mirroring Port:** Administrator can select a mirroring Port.
- **Mirrored Port:** Administrator can select plurality for mirrored port.

5.4 MAC Limit

MAC limiting protects against flooding of the Ethernet switching table (also known as the MAC forwarding table or Layer 2 forwarding table). MAC limiting sets a limit on the number of MAC

addresses that can be learned on a single Layer 2 access interface or on all the Layer 2 access interfaces on the switch, or on a specific VLAN.

# MAC Limit				
Port Configuration >> MAC Limit				
Port	Status	MAC Maximum	Operating	
1	Disable	100		
2	Disable	100		
3	Disable	100		
4	Disable	100		
5	Disable	100		
6	Disable	100		
7	Disable	100		
8	Disable	100		
9	Disable	100		
10	Disable	100		
11	Disable	100		

Administrator can click Operating list button to set MAC Limit.

Edit
✕

Port	<input style="width: 80%;" type="text" value="1"/>
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
MAC Maximum	<input style="width: 80%;" type="text" value="100"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

5.5 Port Aggregation

Port Aggregation is also referred to as link aggregation, teaming port, and port trunking for 802.3ad (LACP, Link Aggregation Control Protocol), The Port Aggregation 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.

Basic Configuration

Administrator can set Source IP/MAC or Destination IP/ MAC for the policy. The LACP service can select enable or disable and also set Aggregation group.

LACP Priority

Administrator configures the LACP system priority on each switch running LACP. LACP uses the system priority with the switch MAC address to form the system ID and also during negotiation with other switches.

The function with the lower system priority value determines which links between LACP partner devices are active and which are in standby for each LACP group. The device on the controlling end of the link uses port priorities to determine which ports are bundled into the aggregated bundle and which ports are put in standby mode. Port priorities on the other device (the non-controlling end of the link) are ignored. In priority comparisons, numerically lower values have higher priority. Therefore, the system with the numerically lower value (higher priority value) for LACP system priority becomes the controlling system. If both devices have the same LACP system priority (for example, they are both configured with the default setting of 128), the device MAC address determines which switch is in control.

Basic Configuration			LACP Priority	LACP Port Information	
System Priority		32768			
LACP Priority >> Port Priority					
Port	Priority			Operating	
1	128				
2	128				
3	128				
4	128				
5	128				
6	128				
7	128				

LACP Information

Basic Configuration		LACP Priority	LACP Port Information			Status Information	Operate Key	Operating
Aggregation Interface	Port	LACP Status	Port Priority	Port Status	Opposite Port			

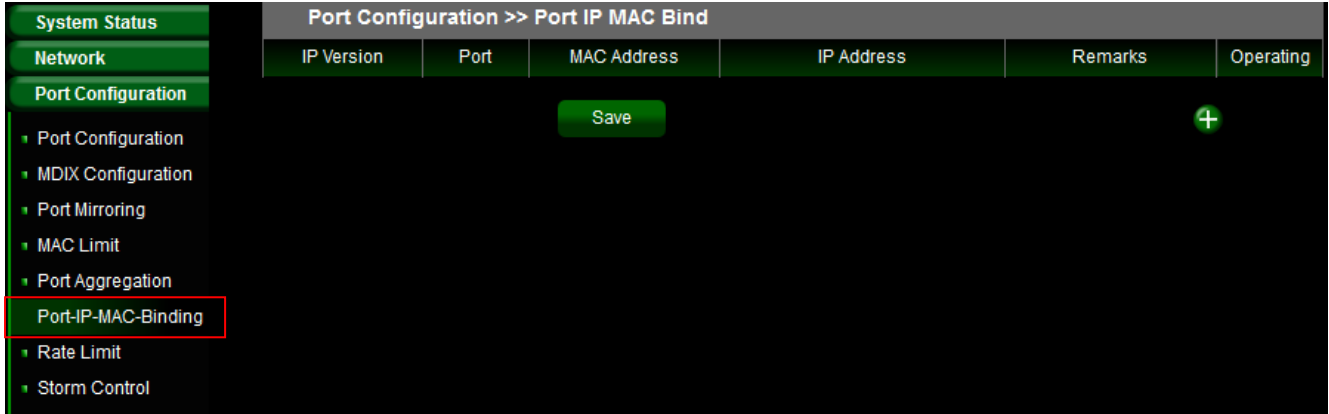
Tips: Click view details to show information and Status information: will show A~H

- A: LACP Activity
- B: LACP Timeout
- C: Aggregation
- D: synchronization
- E: Collecting
- F: Distributing
- G: Defaulted
- H: Expired

5.6 Port-IP-MAC-Binding

Port-IP-MAC-Binding is a powerful, integrated authentication function that ensures the correctness of MAC address, IP address, and connected port for devices connected to the

network. It monitors the information among the ARP, DHCP or IPv4/v6 ARP ND packets to make sure they are all from legal sources help to quarantine illegal device or hackers intend to fake the IP or MAC address on legal devices at the edge of network.



Add	
IP Version	<input type="radio"/> IPv4 <input type="radio"/> IPv6
Port	Port1
* IP Address	<input type="text"/>
* MAC Address	<input type="text"/>
Remarks	<input type="text"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

- **IP Version:** The function support IPv4/v6, administrator can select IP address by v4/v6
- **Port:** Administrator can select Port number for client.
- **IP Address:** Enter IP address for Client
- **MAC Address:** Enter MAC Address for client.
- **Remark:** Enter the information in the remark.

5.7 Rate Limit

The rate limiting function can be configured to limit of Ingress/Egress traffic on a particular

interface.

Administrator can click button in Operating list.

System Status	Port Configuration >> Port Limit			
Network	Port	Ingress(KB)	Egress(KB)	Operating
Port Configuration	1	0	0	
• Port Configuration	2	0	0	
• MDIX Configuration	3	0	0	
• Port Mirroring	4	0	0	
• MAC Limit	5	0	0	
• Port Aggregation	6	0	0	
• Port-IP-MAC-Binding	7	0	0	
Rate Limit	8	0	0	
• Storm Control	9	0	0	

Edit

Port	<input type="text" value="1"/>
Ingress	<input type="text"/> KB
Egress	<input type="text"/> KB
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

5.8 Storm Control

Traffic storm control (also called traffic suppression) allows you to monitor the levels of the

incoming broadcast, multicast, and unicast traffic over a 1-second interval. During this interval, the traffic level, which is a percentage of the total available bandwidth of the port, is compared with the traffic storm control level that you configured. When the ingress traffic reaches the traffic storm control level that is configured on the port, traffic storm control drops the traffic until the interval ends.

A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Administrator can use the traffic storm control feature to prevent disruptions on Layer 2 ports by a broadcast, multicast, or unicast traffic storm on physical interfaces.

Administrator can click button to set storm control in the Operating list.

System Status		Port Configuration >> Storm Control				
Network		Port	Unknown Unicast(KBPS)	Multicast (KBPS)	Broadcasting(KBPS)	Operating
Port Configuration		1	0	0	0	
Port Configuration		2	0	0	0	
MDIX Configuration		3	0	0	0	
Port Mirroring		4	0	0	0	
MAC Limit		5	0	0	0	
Port Aggregation		6	0	0	0	
Port-IP-MAC-Binding		7	0	0	0	
Rate Limit		8	0	0	0	
Storm Control		9	0	0	0	

Edit ✕

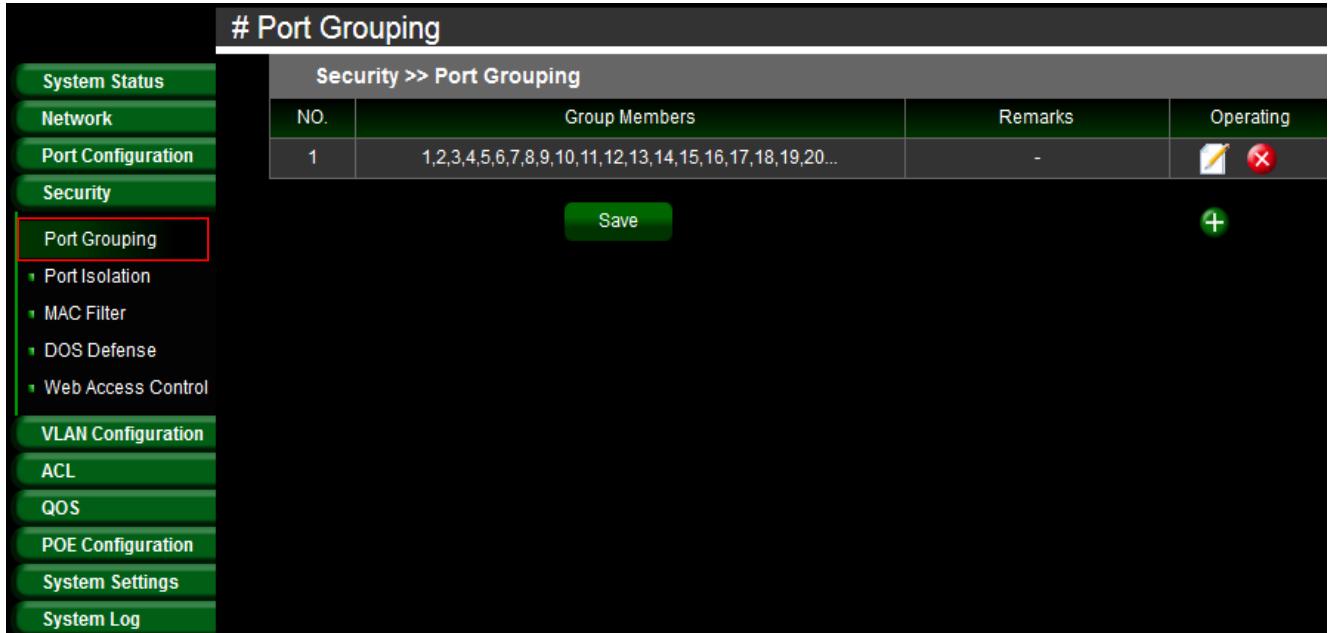
Port	<input type="text" value="1"/>
Unknown Unicast	<input type="text"/> KB
Multicast	<input type="text"/> KB
Broadcasting	<input type="text"/> KB
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

6. Security

6.1 Port Grouping

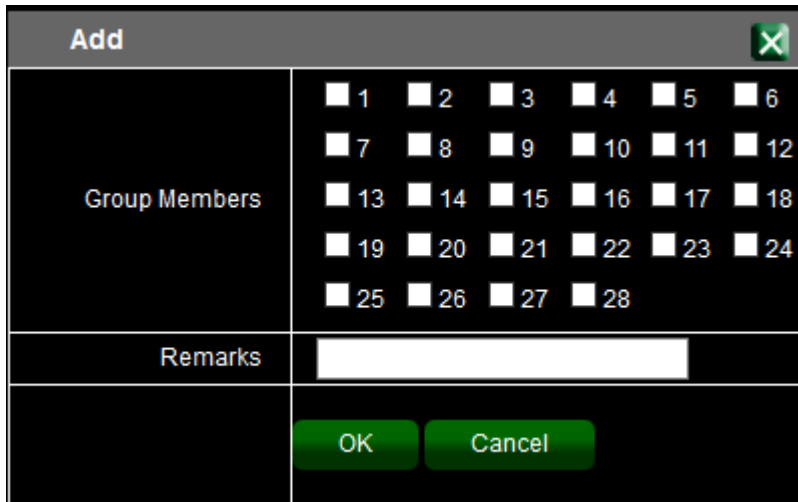
Administrator can create own grouping of devices and ports to efficiently update and manage devices.

Administrator can click button to modify or create Port Grouping in the Operating list.



# Port Grouping			
Security >> Port Grouping			
NO.	Group Members	Remarks	Operating
1	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20...	-	

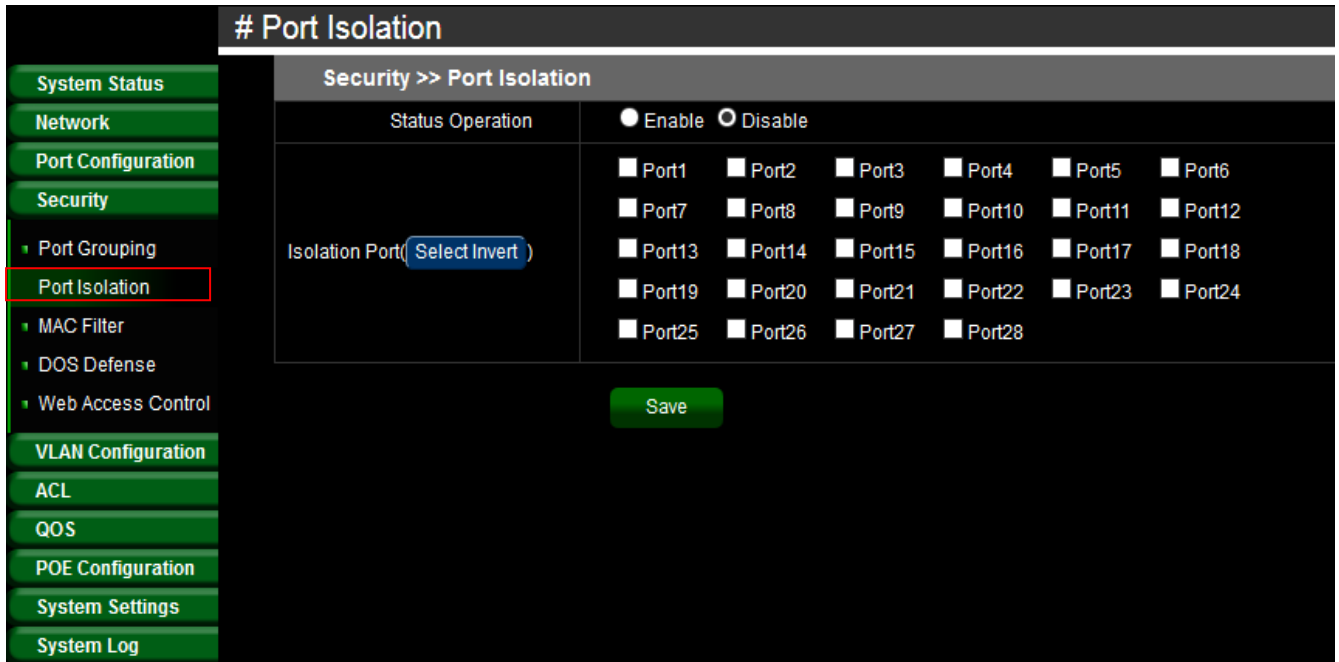
Save +



Add ✕	
Group Members	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6
	<input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12
	<input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18
	<input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24
	<input type="checkbox"/> 25 <input type="checkbox"/> 26 <input type="checkbox"/> 27 <input type="checkbox"/> 28
Remarks	<input type="text"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

6.2 Port Isolation

When administrators use the port isolation feature, the selected ports will no longer be able to communicate with each other.



6.3 MAC filter

MAC Filtering refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network. MAC addresses are uniquely assigned to each card, so using MAC filtering on the list will deny network access to specific devices the use for the blacklists. Administrator can enter source MAC address.

MAC Filter

System Status
Network
Port Configuration
Security
 Port Grouping
 Port Isolation
 MAC Filter
 DOS Defense
 Web Access Control
VLAN Configuration
ACL
QOS
POE Configuration
System Settings
System Log

Security >> MAC Filter

Number	SMAC	Operating

Save +

6.4 DOS Defense

The Switch function support DoS(denial-of-service) defense. Denial-of-service (DoS) is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. Administrator can click button to enable the security in Operating list.

DOS Defense

System Status
Network
Port Configuration
Security
 Port Grouping
 Port Isolation
 MAC Filter
 DOS Defense
 Web Access Control
VLAN Configuration
ACL
QOS
POE Configuration
System Settings
System Log

Security >> DOS Attack Defense

Service Enable Disable

Save

DOS Attack Defense >> Port Set

Port	Status	Operating
1	Disable	
2	Disable	
3	Disable	
4	Disable	
5	Disable	
6	Disable	
7	Disable	

Edit ✕	
Port	1
Status	Disable ▾
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

6.5 Web Access Control

Administrator can set source IP address in list. When this function is enabled, the source IP address can be used to login to the management page of the switch. Other IP addresses can no longer be used to login.

Web Access Control

- System Status
- Network
- Port Configuration
- Security
 - Port Grouping
 - Port Isolation
 - MAC Filter
 - DOS Defense
 - Web Access Control
- VLAN Configuration
- ACL
- QOS
- POE Configuration
- System Settings
- System Log

Security >> Web Access Control

Service
 Enable Disable

Number	SIP	Operating
		+

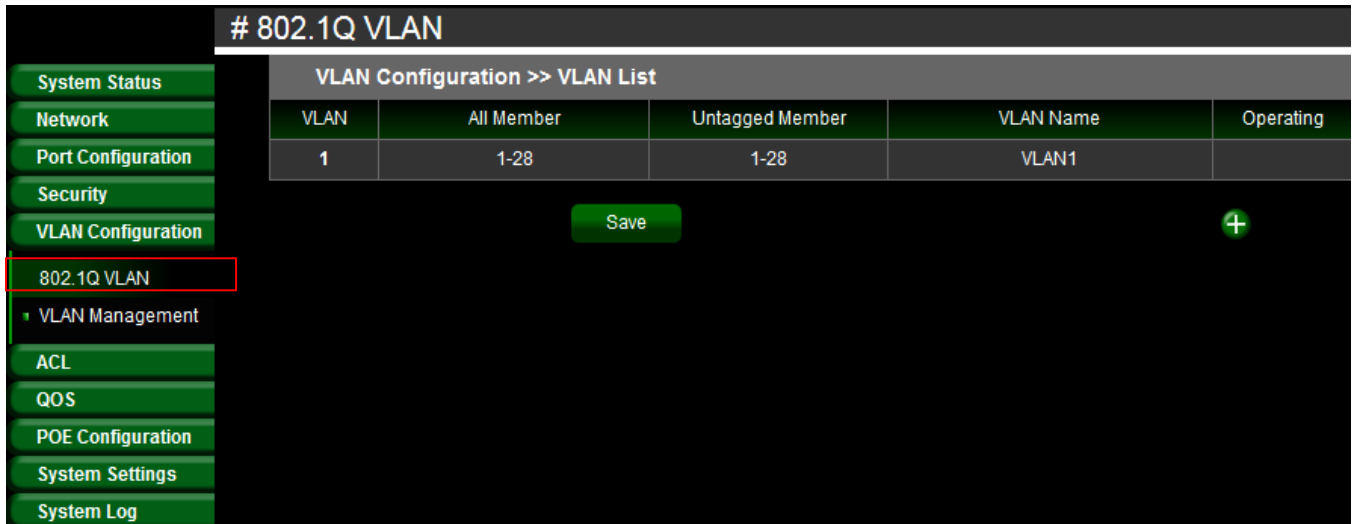
Configuration description: You must keep a source IP data after the service is enabled

Add ✕	
Number	1
SIP	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

7.VLAN Configuration

7.1 802.1Q VLAN

The VLAN function can set Tag Based VLAN.

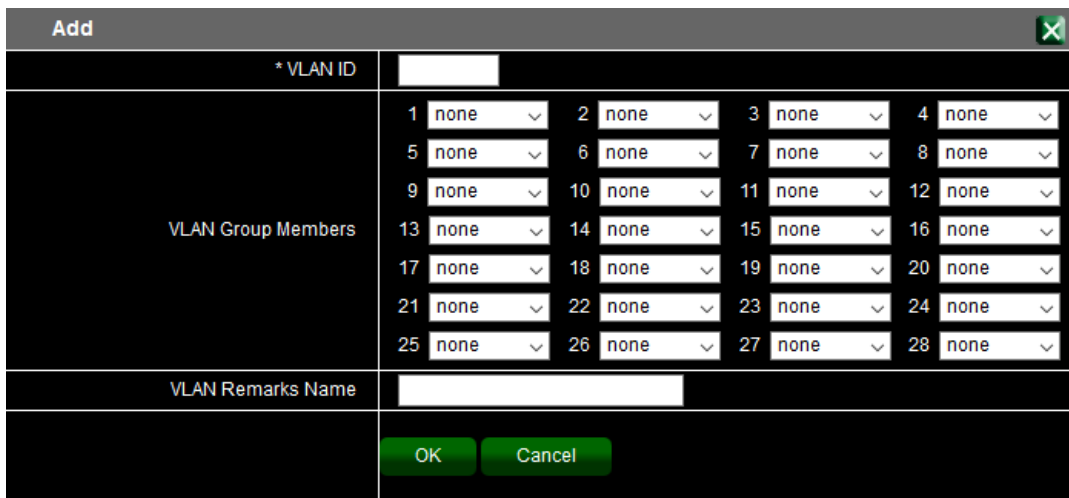


802.1Q VLAN

VLAN Configuration >> VLAN List

VLAN	All Member	Untagged Member	VLAN Name	Operating
1	1-28	1-28	VLAN1	

Save +



Add

* VLAN ID

VLAN Group Members

1	none	2	none	3	none	4	none
5	none	6	none	7	none	8	none
9	none	10	none	11	none	12	none
13	none	14	none	15	none	16	none
17	none	18	none	19	none	20	none
21	none	22	none	23	none	24	none
25	none	26	none	27	none	28	none

VLAN Remarks Name

OK Cancel

- **None:** No changes to egress packets.
- **Tagged:** Insert port's tag for egress packets.
- **UnTagged:** Remove tag ID.

7.2 VLAN Management

The Page administrator can set PVID protocol.

Vlan Management

- System Status
- Network
- Port Configuration
- Security
- VLAN Configuration
- 802.1Q VLAN
- VLAN Management
- ACL
- QOS
- POE Configuration
- System Settings
- System Log

VLAN >> VLAN Management

Management VLAN

VLAN Configuration >> PVID

Port	Pvid	Operating
1	1	
2	1	
3	1	
4	1	
5	1	
6	1	
7	1	

Edit ✕

Port	<input style="width: 80%;" type="text" value="1"/>
Pvid	<input style="width: 80%;" type="text" value="1"/>

8. ACL

8.1 MAC ACL

ACL is Access Control List, MAC ACLs are Layer 2 ACLs. Administrator can configure the Source/Destination MAC address and MAC mask rules to Permit or deny for the packet.

MAC ACL

- System Status
- Network
- Port Configuration
- Security
- VLAN Configuration
- ACL
- MAC ACL
- IP ACL
- QOS
- POE Configuration
- System Settings
- System Log

ACL >> MAC ACL

Name	Privilege	DMAC	DMAC Mask	SMAC	SMAC Mask	Operating
Save						+

Add	
Name	<input type="text"/>
Privilege	<input type="radio"/> Permit <input type="radio"/> Deny
DMAC	<input type="text"/>
DMAC Mask	<input type="text"/>
SMAC	<input type="text"/>
SMAC Mask	<input type="text"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

8.2 IP ACL

Administrator can configure the Source IP address and IP mask rules to Permit or deny for the packet.

MAC ACL

	ACL >> MAC ACL						
	Name	Privilege	DMAC	DMAC Mask	SMAC	SMAC Mask	Operating
<div style="background-color: #333; color: white; padding: 2px; margin-bottom: 2px;">System Status</div> <div style="background-color: #333; color: white; padding: 2px; margin-bottom: 2px;">Network</div> <div style="background-color: #333; color: white; padding: 2px; margin-bottom: 2px;">Port Configuration</div> <div style="background-color: #333; color: white; padding: 2px; margin-bottom: 2px;">Security</div> <div style="background-color: #333; color: white; padding: 2px; margin-bottom: 2px;">VLAN Configuration</div> <div style="background-color: #333; color: white; padding: 2px; margin-bottom: 2px;">ACL</div> <div style="background-color: #333; color: white; padding: 2px; margin-bottom: 2px;"> <ul style="list-style-type: none"> MAC ACL <li style="border: 1px solid red;">IP ACL </div> <div style="background-color: #333; color: white; padding: 2px; margin-bottom: 2px;">QOS</div> <div style="background-color: #333; color: white; padding: 2px; margin-bottom: 2px;">POE Configuration</div> <div style="background-color: #333; color: white; padding: 2px; margin-bottom: 2px;">System Settings</div> <div style="background-color: #333; color: white; padding: 2px;">System Log</div>	<div style="background-color: #333; color: white; padding: 5px; display: flex; justify-content: space-between; align-items: center;"> Save + </div>						

Add	
Name	<input type="text"/>
Privilege	<input type="radio"/> Permit <input type="radio"/> Deny
SIP	<input type="text"/>
SIP Mask	<input type="text"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

- **Name** : Administrator can enter the rule name.
- **Privilege** : Administrator can select Permit or Deny for the rule.
- **SIP**: If administrator want to deny an IP address, administrator can setting source IP address for deny.
- **SIP Mask** : Administrator must to enter source IP Mask. example: block a IP address, the Mask enter 0.0.0.0

Basic Configuration		Expert Configuration			Operating
Name	Privilege	SIP	SIP Mask		
Danny	Deny	192.168.2.20	0.0.0.0		

Expert Configuration

If want to set protocol details of the ACL, administrator can click "Expert Configuration" to set detail functions.

Basic Configuration		Expert Configuration					Operating
Name	Privilege	SIP	SIP Mask	DIP	DIP Mask	Protocol	
Danny	Deny	192.168.2.20	0.0.0.0	192.168.2.200	0.0.0.0	ICMP	

Example: If want to block ping protocol for source to destination, administrator can refer to the following example.

Edit

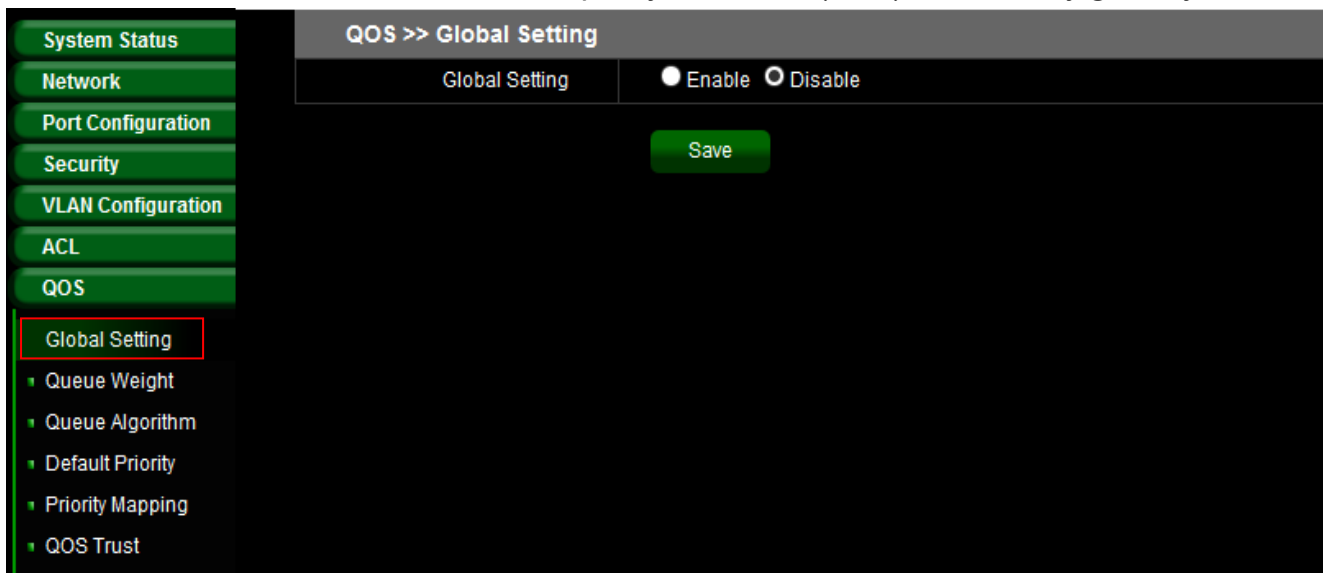
*Name	<input type="text" value="Danny"/>
*Privilege	<input type="radio"/> Permit <input checked="" type="radio"/> Deny
*SIP	<input type="text" value="192.168.2.20"/>
*SIP Mask	<input type="text" value="0.0.0.0"/>
*DIP	<input type="text" value="192.168.2.200"/>
*DIP Mask	<input type="text" value="0.0.0.0"/>
Protocol(Optional)	<input type="text" value="ICMP"/>
*Type	<input type="text" value="8"/>
*Code	<input type="text" value="0"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

9. 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.

9.1 Global Setting

Administrator can enable or disable the quality of service (QoS) functionality globally.



9.2 Queue Weight

Administrator can input the queue weight of the Q0~Q7. The weight values of "Queue Weight" can be customized and their default values are 1:2:4:8:16:32:64:127 respectively.



System Status		QOS >> Queue Weight																			
Network	Port Configuration	Security	VLAN Configuration	ACL	QOS	Global Setting	Queue Weight	Queue Algorithm	Default Priority	Priority Mapping	QOS Trust	Port ID	Queue 0	Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7	Operating
												1	1	2	4	8	16	32	64	127	
												2	1	2	4	8	16	32	64	127	
												3	1	2	4	8	16	32	64	127	
												4	1	2	4	8	16	32	64	127	
												5	1	2	4	8	16	32	64	127	
												6	1	2	4	8	16	32	64	127	
												7	1	2	4	8	16	32	64	127	
												8	1	2	4	8	16	32	64	127	
												9	1	2	4	8	16	32	64	127	
												10	1	2	4	8	16	32	64	127	
												11	1	2	4	8	16	32	64	127	

Edit	
Port	1
Queue 0	1
Queue 1	2
Queue 2	4
Queue 3	8
Queue 4	16
Queue 5	32
Queue 6	64
Queue 7	127
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

9.3 Queue Algorithm

System Status	QOS >> Queue Algorithm		
	Port	Queue Algorithm	Operating
Network	1	WFQ	
Port Configuration	2	WFQ	
Security	3	WFQ	
VLAN Configuration	4	WFQ	
ACL	5	WFQ	
QOS	6	WFQ	
Global Setting	7	WFQ	
Queue Weight	8	WFQ	
Queue Algorithm	9	WFQ	
Default Priority	10	WFQ	
Priority Mapping			
QOS Trust			

Edit	
Port	1
Queue Algorithm	<input type="text" value="WFQ"/> <ul style="list-style-type: none"> WFQ WRR WRR+SP <input type="button" value="Cancel"/>

- **WFQ:** Each Queue can set a weight by QoS. The QoS function will be based on weights to allocate bandwidth to ensure basic.

- **WRR:** Weight Round Robin Scheduling is like waiting in line, Packets in all the queues are sent in order based on the weight value for each queue.
- **WRR+SP:** Weight Round Robin + Strict Priority, Queues in SP are scheduled strictly based on SP function while the queues inside WRR follow the WRR mode.

9.4 Default Priority

Administrator can set default priority of the Queue Weight.

System Status	QOS >> Default Priority		
	Port	Default Priority	Operating
Network	1	0	
Port Configuration	2	0	
Security	3	0	
VLAN Configuration	4	0	
ACL	5	0	
QOS	6	0	
Global Setting	7	0	
Queue Weight	8	0	
Queue Algorithm	9	0	
Default Priority	10	0	
Priority Mapping	11	0	
QOS Trust			

9.5 Priority Mapping

This switch implements two priority modes based on port, on COS and on DSCP. The port priorities are labeled as CoS0~7.

System Status	COS DSCP		Operating
	COS	Inner Priority	
Network	0	0	
Port Configuration	1	1	
Security	2	2	
VLAN Configuration	3	3	
ACL	4	4	
QOS	5	5	
Global Setting	6	6	
Queue Weight	7	7	
Queue Algorithm			
Default Priority			
Priority Mapping			
QOS Trust			

Edit	
COS	<input type="text" value="0"/>
Inner Priority	<input type="text" value="0"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

- **CoS:** Class of Service is data frame in the level 2. When the port priority is specified, the data will be classified into the egress queue based on the CoS value of the ingress port and the mapping relation between the CoS in cos mapping.
-

9.6 QoS Trust

Administrator can select QoS trust mode.

System Status	QOS >> QOS Trust			
	Port	QOS Trust Mode		
Network	1	<input type="radio"/> COS Only	<input type="radio"/> DSCP Prior To The COS	<input type="radio"/> DSCP Only <input type="radio"/> Distrust
Port Configuration	2	<input type="radio"/> COS Only	<input type="radio"/> DSCP Prior To The COS	<input type="radio"/> DSCP Only <input type="radio"/> Distrust
Security	3	<input type="radio"/> COS Only	<input type="radio"/> DSCP Prior To The COS	<input type="radio"/> DSCP Only <input type="radio"/> Distrust
VLAN Configuration	4	<input type="radio"/> COS Only	<input type="radio"/> DSCP Prior To The COS	<input type="radio"/> DSCP Only <input type="radio"/> Distrust
ACL	5	<input type="radio"/> COS Only	<input type="radio"/> DSCP Prior To The COS	<input type="radio"/> DSCP Only <input type="radio"/> Distrust
QOS	6	<input type="radio"/> COS Only	<input type="radio"/> DSCP Prior To The COS	<input type="radio"/> DSCP Only <input type="radio"/> Distrust
Global Setting	7	<input type="radio"/> COS Only	<input type="radio"/> DSCP Prior To The COS	<input type="radio"/> DSCP Only <input type="radio"/> Distrust
Queue Weight	8	<input type="radio"/> COS Only	<input type="radio"/> DSCP Prior To The COS	<input type="radio"/> DSCP Only <input type="radio"/> Distrust
Queue Algorithm	9	<input type="radio"/> COS Only	<input type="radio"/> DSCP Prior To The COS	<input type="radio"/> DSCP Only <input type="radio"/> Distrust
Default Priority	10	<input type="radio"/> COS Only	<input type="radio"/> DSCP Prior To The COS	<input type="radio"/> DSCP Only <input type="radio"/> Distrust
Priority Mapping	11	<input type="radio"/> COS Only	<input type="radio"/> DSCP Prior To The COS	<input type="radio"/> DSCP Only <input type="radio"/> Distrust
QOS Trust				

10. POE Configuration

10.1 POE Global Settings

This page will display PoE status and administrator can set Total Power, Power Guard Band, Temperature Protection, Output Voltage Range and The ratio of system power supply.

PoE Global Settings

- System Status
- Network
- Port Configuration
- Security
- VLAN Configuration
- ACL
- QOS
- POE Configuration
- POEGlobal Settings
 - Power Priority
 - Power Supply
 - POE Timing Reboot
 - Power Limitation
 - POE Status
 - Device Manage
- System Settings
- System Log

POE Configuration >> POE Global Settings

PSE Total Power	350	W	
Power Guard Band	30	W	
Temperature Protection	85	°C	
Output Voltage Range	Min Voltage 44	V	Max Voltage 57 V
Power supply management	<input type="radio"/> Auto <input checked="" type="radio"/> Manual		
Power Manage Mode	<input type="radio"/> Dynamic <input checked="" type="radio"/> Static Notice: Under dynamic, max current of single port <= 600mA		

PSE Total Power	350 W
Temperature Protection	85 °C
Power Guard Band	30 W
Min Voltage	44 V
Max Voltage	57 V
Power supply management	Auto
Power Manage Mode	Dynamic
PSE1	45 °C whether or not over temperature : normal temperature
PSE2	47 °C whether or not over temperature : normal temperature

- **PSE Total Power:** Administrator can set PSE total Power total limit.
- **Power Guard Band:** The power guard band can provide protection when there is a sudden spike in the consumed power of PDs that could potentially impact other PoE enabled ports.
- **Temperature Protection:** Administrator can setting between 60 and 85 Temperature. If the system temperature higher than the set temperature, the system will appear warning messenger and through SNMP to notice manager.
- **Output Voltage Range:** Administrator can set Output Voltage Range.
- **Power supply management:** Administrator can select use Auto or manual.
- **Power Manage Mode:** Administrator can select dynamic or Static for one port PoE output power.

10.2 Power Priority

The PoE priority default is priority 3, administrator can set priority 1-3 for the Critical/High/Low. If the function setting prioritizes the power allocation to the ports that present a PD power demand. This system will remove power from one or more lower-priority ports to meet the power demand on other, higher-priority ports.

# PoE Power Priority		
System Status	POE Configuration >> Power Priority	
Network	Power Supply port	<input type="radio"/> Critical <input checked="" type="radio"/> High <input type="radio"/> Low
Port Configuration	Port1	<input type="radio"/> Critical <input checked="" type="radio"/> High <input type="radio"/> Low
Security	Port2	<input type="radio"/> Critical <input checked="" type="radio"/> High <input type="radio"/> Low
VLAN Configuration	Port3	<input type="radio"/> Critical <input checked="" type="radio"/> High <input type="radio"/> Low
ACL	Port4	<input type="radio"/> Critical <input checked="" type="radio"/> High <input type="radio"/> Low
QOS	Port5	<input type="radio"/> Critical <input checked="" type="radio"/> High <input type="radio"/> Low
POE Configuration	Port6	<input type="radio"/> Critical <input checked="" type="radio"/> High <input type="radio"/> Low
POEGlobal Settings	Port7	<input type="radio"/> Critical <input checked="" type="radio"/> High <input type="radio"/> Low
Power Priority	Port8	<input type="radio"/> Critical <input checked="" type="radio"/> High <input type="radio"/> Low
Power Supply	Port9	<input type="radio"/> Critical <input checked="" type="radio"/> High <input type="radio"/> Low
POE Timing Reboot	Port10	<input type="radio"/> Critical <input checked="" type="radio"/> High <input type="radio"/> Low
Power Limitation	Port11	<input type="radio"/> Critical <input checked="" type="radio"/> High <input type="radio"/> Low
POE Status	Port12	<input type="radio"/> Critical <input checked="" type="radio"/> High <input type="radio"/> Low
Device Manage	Port13	<input type="radio"/> Critical <input checked="" type="radio"/> High <input type="radio"/> Low

10.3 Power Supply

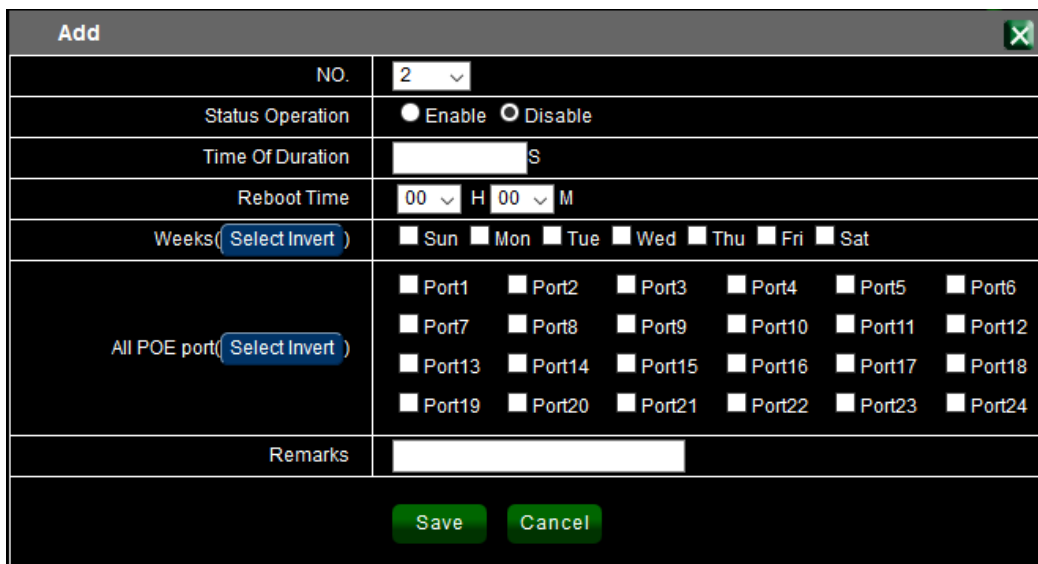
In the Power Supply function, administrator can manually control PoE Power on / off by port

# Power Supply		
System Status	POE Configuration >> Power Supply	
Network	All POE port	<input type="radio"/> Turn on the power <input checked="" type="radio"/> Turn off the power
Port Configuration	Port1	<input type="radio"/> Turn on the power <input checked="" type="radio"/> Turn off the power
Security	Port2	<input type="radio"/> Turn on the power <input checked="" type="radio"/> Turn off the power
VLAN Configuration	Port3	<input type="radio"/> Turn on the power <input checked="" type="radio"/> Turn off the power
ACL	Port4	<input type="radio"/> Turn on the power <input checked="" type="radio"/> Turn off the power
QOS	Port5	<input type="radio"/> Turn on the power <input checked="" type="radio"/> Turn off the power
POE Configuration	Port6	<input type="radio"/> Turn on the power <input checked="" type="radio"/> Turn off the power
POEGlobal Settings	Port7	<input type="radio"/> Turn on the power <input checked="" type="radio"/> Turn off the power
Power Priority	Port8	<input type="radio"/> Turn on the power <input checked="" type="radio"/> Turn off the power
Power Supply	Port9	<input type="radio"/> Turn on the power <input checked="" type="radio"/> Turn off the power
POE Timing Reboot	Port10	<input type="radio"/> Turn on the power <input checked="" type="radio"/> Turn off the power
Power Limitation	Port11	<input type="radio"/> Turn on the power <input checked="" type="radio"/> Turn off the power
POE Status	Port12	<input type="radio"/> Turn on the power <input checked="" type="radio"/> Turn off the power
Device Manage	Port13	<input type="radio"/> Turn on the power <input checked="" type="radio"/> Turn off the power
System Settings	Port14	<input type="radio"/> Turn on the power <input checked="" type="radio"/> Turn off the power
System Log	Port15	<input type="radio"/> Turn on the power <input checked="" type="radio"/> Turn off the power

10.4 PoE Timing Reboot

Administrator can control PoE output power on/off by schedule in the page.

Please click “PoE Timing Reboot” and click  button to create new schedule.

- **No.:** Administrator can select number 1-24 for identifiable item.
- **Status Operation:** Administrator can select Enable or Disable the schedule.
- **Time Of Duration:** After the system auto disable PoE, administrator can set waiting 10-1000 second to restart PoE.
- **Reboot Time/Weeks:** Administrator can set PoE disable in the schedule time.
- **Select Ports:** Administrator can select ports for the PoE reboot.

10.5 Power Limitation

If “Power Manage Mode” is set to “Static” in the POE Global setting page, the Power limitation function will be able to set output power for single PoE ports

Please click “PoE Configuration” → “Power Limitation” to set single PoE Max output Power.

# Power Limitation			
POE Configuration >> POE Power Limitation			
	Port	Max Power(mW)	Operating
System Status	All POE port	-	
Network	1	15000	
Port Configuration	2	15000	
Security	3	15000	
VLAN Configuration	4	15000	
ACL	5	15000	
QOS	6	15000	
POE Configuration	7	15000	
POE Global Settings	8	15000	
Power Priority	9	15000	
Power Supply	10	15000	
POE Timing Reboot	11	15000	
Power Limitation	12	15000	
POE Status	13	15000	
Device Manage	14	15000	
System Settings			
System Log			

10.6 PoE Status

Administrators can monitor all PoE usage (total watts) and powered information of each port.

PoE status include **PoE on/off status**, **Used voltage status**, **Used current (mA) status**, **Used power(mW) status** for single port and Total Power (Watts) status.

Please click “PoE Configuration” → “PoE Status” to monitor all PoE status.

# POE Status					
POE Configuration >> POE Status					
<input type="checkbox"/> Auto Refresh					
Port	Power Status	Voltage(V)	Current(mA)	Power(mW)	
1	Turned on	0	0	0	
2	Turned on	54.7	97	5305	
3	Turned on	0	0	0	
4	Turned on	0	0	0	
5	Turned on	0	0	0	
6	Turned on	0	0	0	
7	Turned on	0	0	0	
8	Turned on	0	0	0	
9	Turned on	0	0	0	
10	Turned on	0	0	0	
11	Turned on	0	0	0	
12	Turned on	0	0	0	
13	Turned on	0	0	0	



V * mA = mW
mW * 0.001 = W

10.7 Device Manager

Administrators can set a minimum PoE power output. The PoE output for each port cannot fall below the set minimum PoE wattage.

Please click “PoE Configuration” → “Device Manage” to set minimum manager

# Device Manage			
POE Configuration >> Device Manage			
Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Minimum equipment	1 W		
<input type="button" value="Save"/>			
POE Configuration >> Equipment Port Management			
Port	Switch	Status	Operating
1	Disable	-	
2	Enable	-	
3	Disable	-	
4	Disable	-	
5	Disable	-	
6	Disable	-	
7	Disable	-	
8	Disable	-	

Edit	
Port	1
Port Switch	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Administrator can select enable or disable for the service.

11. System Setting

11.1 Quick Settings

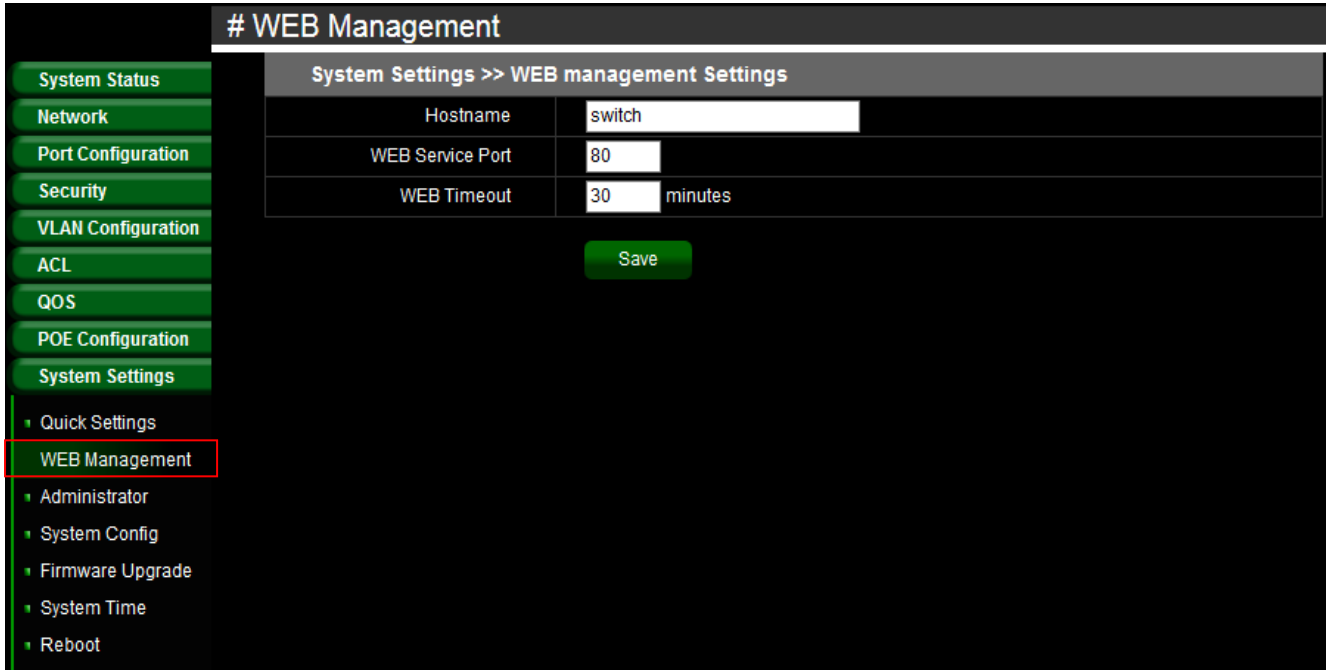
This function allows administrator to quickly make setting changes to hostname, IP address, Netmask, DNS and gateway.

# Quick Settings													
System Status	<div style="background-color: #003366; color: white; padding: 5px;">System Settings >> Quick Settings</div> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Hostname</td> <td>switch</td> </tr> <tr> <td>IP Address</td> <td>192.168.2.200</td> </tr> <tr> <td>Netmask</td> <td>255.255.255.0</td> </tr> <tr> <td>Default Gateway</td> <td>192.168.2.1</td> </tr> <tr> <td>Primary DNS Server</td> <td>8.8.8.8</td> </tr> <tr> <td>Secondary DNS Server</td> <td>168.95.1.1</td> </tr> </table> <div style="text-align: center; margin-top: 10px;"> <input type="button" value="Save"/> </div>	Hostname	switch	IP Address	192.168.2.200	Netmask	255.255.255.0	Default Gateway	192.168.2.1	Primary DNS Server	8.8.8.8	Secondary DNS Server	168.95.1.1
Hostname		switch											
IP Address		192.168.2.200											
Netmask		255.255.255.0											
Default Gateway		192.168.2.1											
Primary DNS Server		8.8.8.8											
Secondary DNS Server		168.95.1.1											
Network													
Port Configuration													
Security													
VLAN Configuration													
ACL													
QOS													
POE Configuration													
System Settings													
Quick Settings													
WEB Management													
Administrator													
System Config													
Firmware Upgrade													
System Time													
Reboot													

- **Host Name:** Administrator can set system name for the switch.
- **IP Address/Netmask:** Administrator can set IP address and Netmask for the switch
- **Default Gateway:** Administrator can set gateway IP address.
- **DNS:** Specify DNS server IP address can be able to resolve the domain name.

11.2 Web Management

The page administrator can change login service and login timeout time.

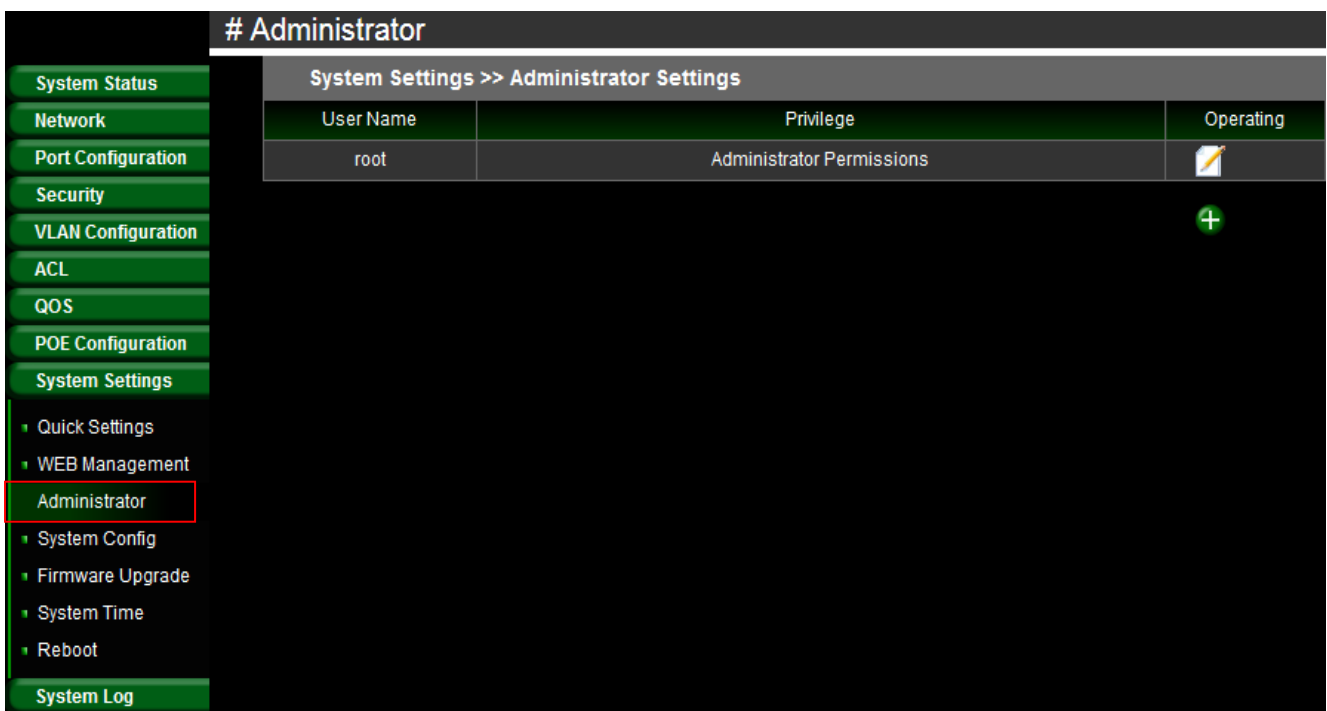


System Settings >> WEB management Settings	
Hostname	switch
WEB Service Port	80
WEB Timeout	30 minutes

Save

11.3 Administrator

Administrator can change login password or create new account / password for the system login, the account can be set to Ordinary or Administrator Permissions.



System Settings >> Administrator Settings		
User Name	Privilege	Operating
root	Administrator Permissions	[icon]

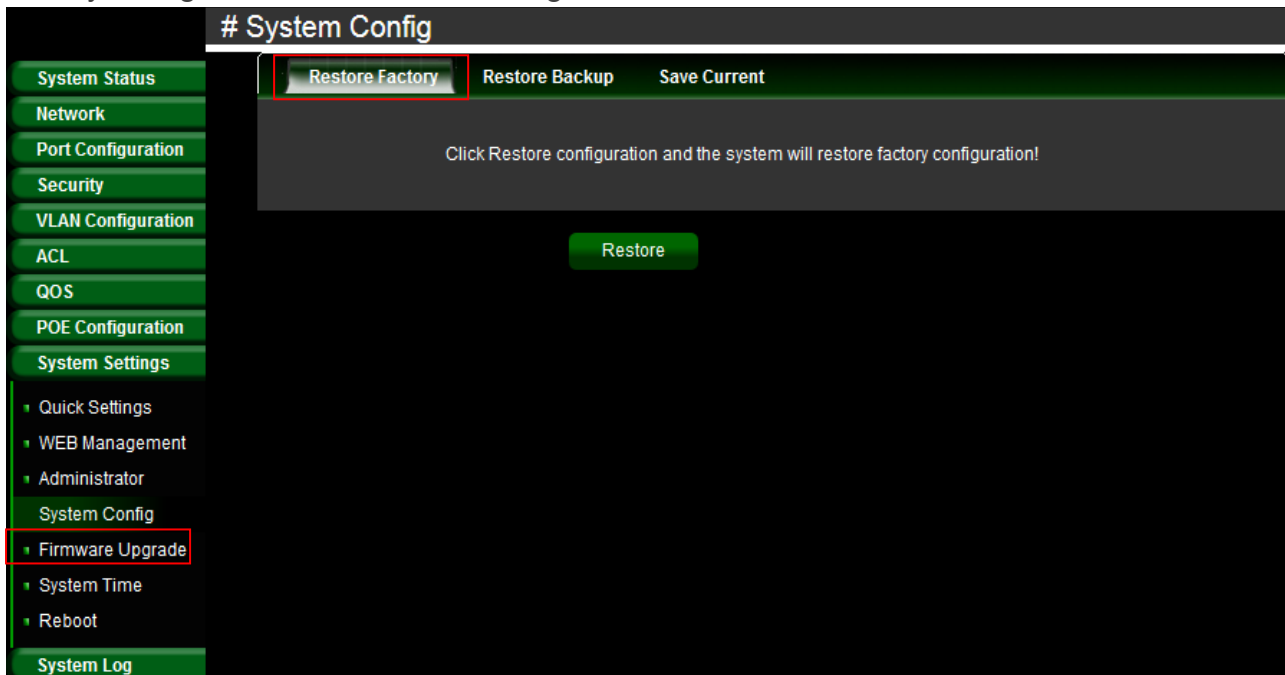
+

11.4 System Config

This function can restore the system to default settings, and also backup or restore the device using preconfigured profile settings.

Restore Factory:

Administrator can click the **"Restore"** button to reset back to default settings. This will restore factory configuration and all user configurations will be deleted.



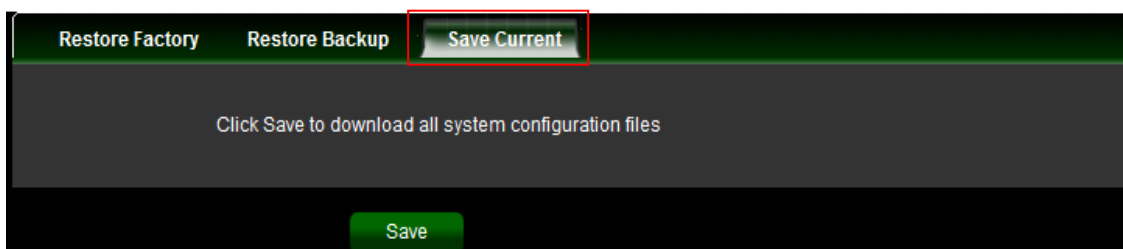
Restore Backup:

Administrator can click **"Browse"** to choose saved system configuration file.



Save Current:

Administrator can click **"Save"** button to download all system configuration files.



11.5 Firmware Upgrade

Firmware is the main software image that system needs to respond to requests and to manage real time operations. Firmware upgrades are sometimes required to include new features or bugs fix. It takes around 2 minutes to upgrade due to complexity of firmware. To upgrade system firmware, click Browse button to locate the new firmware, and then click Upgrade button to upgrade.

Firmware Upgrade

System Settings >> Firmware Upgrade

Current Version	0.3.023v2.2
* Upgrade File	Browse

[Start to upgrade](#)

- System Status
- Network
- Port Configuration
- Security
- VLAN Configuration
- ACL
- QOS
- POE Configuration
- System Settings
 - Quick Settings
 - WEB Management
 - Administrator
 - System Config
 - Firmware Upgrade**
 - System Time
 - Reboot
- System Log

11.6 System Time

System time can be configured via this page. Administrator can select Manual or Synchronization to update the system time. If select Synchronization mode, administrator can click “system time zone” to set time zone and go to “network time” function set a time server.

System Time

System Time	System Time Zone	Network Time
Update Mode	<input type="radio"/> Synchronization Time <input checked="" type="radio"/> Manually Set	
Computer Time	2016-09-09 14:03:23	
System Time	2016-09-09 14:03:33	

Synchronization

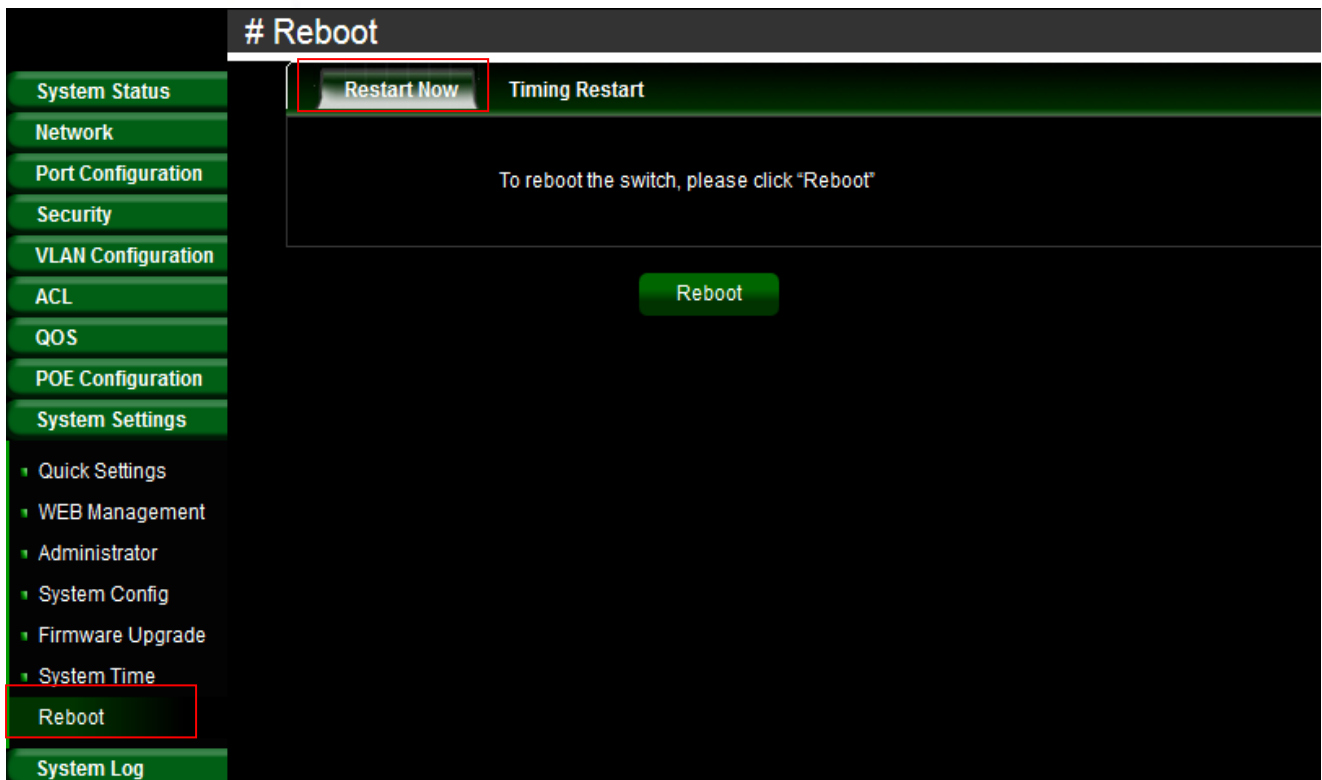
- System Status
- Network
- Port Configuration
- Security
- VLAN Configuration
- ACL
- QOS
- POE Configuration
- System Settings
 - Quick Settings
 - WEB Management
 - Administrator
 - System Config
 - Firmware Upgrade
 - System Time**
 - Reboot
- System Log

System Time	System Time Zone	Network Time																																										
Update Mode	<input type="radio"/> Synchronization Time <input type="radio"/> Manually Set																																											
* Time	2016-06-20 15:38:45																																											
System Time	<div style="border: 1px solid black; padding: 5px;"> <div style="display: flex; justify-content: space-between;"> 2016 JUN </div> <table border="1" style="width: 100%; text-align: center;"> <thead> <tr> <th>Sun</th><th>Mon</th><th>Tue</th><th>Wed</th><th>Thu</th><th>Fri</th><th>Sat</th> </tr> </thead> <tbody> <tr> <td></td><td></td><td></td><td>1</td><td>2</td><td>3</td><td>4</td> </tr> <tr> <td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td> </tr> <tr> <td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td> </tr> <tr> <td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td> </tr> <tr> <td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td></td><td></td> </tr> </tbody> </table> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> 15 38 45 </div> </div>		Sun	Mon	Tue	Wed	Thu	Fri	Sat				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30		
Sun	Mon	Tue	Wed	Thu	Fri	Sat																																						
			1	2	3	4																																						
5	6	7	8	9	10	11																																						
12	13	14	15	16	17	18																																						
19	20	21	22	23	24	25																																						
26	27	28	29	30																																								
<input type="button" value="OK"/> <input type="button" value="Close"/>																																												

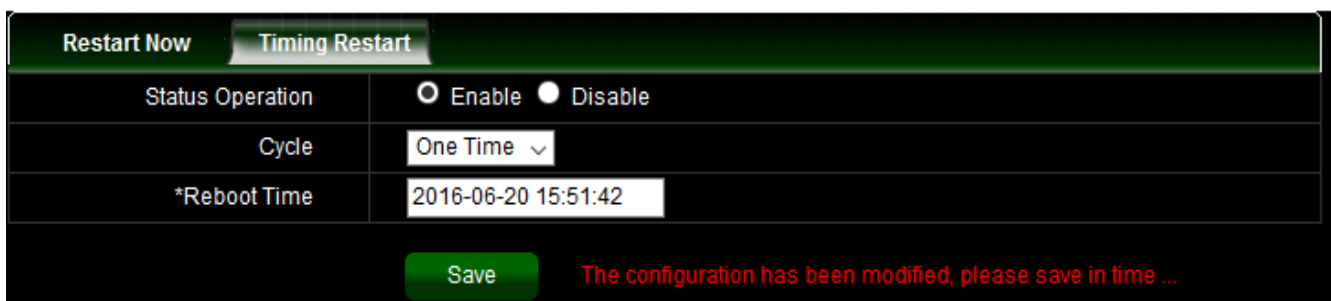
11.7 Reboot

This function allows administrator to reboot system or click “Timing Restart” function set auto reboot for the time schedule.

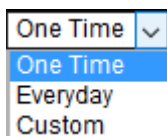
Click **Reboot** button to proceed and take around one minute to complete.



Timing Restart



- **Status Operation:** Administrator can choose Enable or Disable for the service.
- **Cycle:** Administrator can choose auto reboot by One Time or Every day or Custom.



- **One Time:** Administrator can specify a time to reboot system.
- **Everyday:** Administrator can set every day to reboot system.
- **Custom:** Administrator can set auto reboot by time schedule.

12. System Log

12.1 Event Log

The Event log displays system events when system is up and running. Also, it becomes very useful as a troubleshooting tool when issues are experienced in system.

# System Log			
System Status	System Log >> Event Log		
Network	Time	Level	Message
Port Configuration	2016-09-09 13:28:54	Warning	HTTP:Administrator root login from 192.168.2.20.Result:Accepted.
Security	2016-09-09 11:19:42	Warning	HTTP:Administrator root login from 192.168.2.20.Result:Accepted.
VLAN Configuration	2016-09-09 11:05:29	Info	HTTP:The administrator root at 192.168.2.20 updated 'WEB management' configuration.
ACL	2016-09-09 10:46:46	Warning	HTTP:Administrator root login from 192.168.2.20.Result:Accepted.
QOS	2016-09-09 10:08:50	Info	HTTP:The administrator root at 192.168.2.20 updated 'WEB management' configuration.
POE Configuration	2016-09-09 09:41:14	Info	HTTP:The administrator root at 192.168.2.20 updated 'WEB management' configuration.
System Settings	2016-09-09 09:41:04	Info	HTTP:The administrator root at 192.168.2.20 updated 'WEB management' configuration.
System Log	2016-09-09 09:40:42	Info	HTTP:The administrator root at 192.168.2.20 updated 'WEB management' configuration.
Event Log	2016-09-09 09:40:16	Info	HTTP:The administrator root at 192.168.2.20 updated 'WEB management' configuration.
Alarm Log	2016-09-09 09:07:43	Warning	HTTP:Administrator root login from 192.168.2.20.Result:Accepted.
Security Log	2016-09-08 18:08:41	Info	HTTP:The administrator root at 192.168.2.20 updated POE configuration.
Network Log	2016-09-08 18:08:00	Info	HTTP:The administrator root at 192.168.2.20 updated POE configuration.
Protocol Log	2016-09-08 18:07:49	Info	HTTP:The administrator root at 192.168.2.20 updated POE configuration.

12.2 Alarm Log

When system is up and running, the Alarm Log page can display system Alarm information.

# System Log			
System Status	System Log >> Alarm Log		
Network	Time	Level	Message
Port Configuration	2016-09-09 11:57:14	Notice	Port 2 disconnected.
Security	2016-09-09 11:56:23	Notice	Port 2 connected. Mode: 100Mbps Full-duplex.
VLAN Configuration	2016-09-09 11:56:22	Notice	Port 2 disconnected.
ACL	2016-09-09 11:56:18	Notice	Port 2 connected. Mode: 100Mbps Full-duplex.
QOS	2016-09-09 11:56:16	Notice	Port 2 disconnected.
POE Configuration	2016-09-09 11:56:02	Notice	Port 2 connected. Mode: 100Mbps Full-duplex.
System Settings	2016-09-09 11:55:58	Notice	Port 2 disconnected.
System Log	2016-09-09 11:53:05	Notice	Port 2 connected. Mode: 100Mbps Full-duplex.
Event Log	2016-09-09 11:53:03	Notice	Port 2 disconnected.
Alarm Log	2016-09-09 11:52:59	Notice	Port 2 connected. Mode: 100Mbps Full-duplex.
Security Log	2016-09-09 11:52:57	Notice	Port 2 disconnected.
Network Log	2016-09-09 11:52:43	Notice	Port 2 connected. Mode: 100Mbps Full-duplex.
Protocol Log	2016-09-09 11:52:39	Notice	Port 2 disconnected.
	2016-09-09 11:51:51	Notice	Port 2 connected. Mode: 100Mbps Full-duplex.
	2016-09-09 11:51:49	Notice	Port 2 disconnected.

Level: All total 119 Page Size 15 Page No. 1 / 8 First | Next | Prev | Last Goto 1

12.3 Security Log

When system is up and running, the security Log page can display system security information.

The screenshot shows the 'System Log' page with the 'Security Log' sub-page selected. The left sidebar contains a menu with 'Security Log' highlighted. The main content area displays a table with columns for 'Time', 'Level', and 'Message'. Above the table, there are controls for 'Level' (set to 'All'), 'total 0', 'Page Size' (set to '15'), 'Page No. 1/1', and navigation links 'First | Next | Prev | Last'. Below these controls are buttons for 'Refresh', 'Clear', and 'Export'.

12.4 Network Log

When system is up and running, the Network Log page can display system Network information.

The screenshot shows the 'System Log' page with the 'Network Log' sub-page selected. The left sidebar contains a menu with 'Network Log' highlighted. The main content area displays a table with columns for 'Time', 'Level', and 'Message'. Above the table, there are controls for 'Level' (set to 'All'), 'total 0', 'Page Size' (set to '15'), 'Page No. 1/1', and navigation links 'First | Next | Prev | Last'. Below these controls are buttons for 'Refresh', 'Clear', and 'Export'.

12.5 Protocol Log

When system is up and running, the Protocol Log page can display Protocol information.

System Log

System Log >> Protocol Log

Time	Level	Message
------	-------	---------

Level: All total 0 Page Size 15 Page No. 1 / 1 First | Next | Prev | Last Goto 1

Refresh Clear Export

- Event Log
- Alarm Log
- Security Log
- Network Log
- Protocol Log**

Specifications

Standards & Hardware Specifications

Standards Conformance	<p>IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX, IEEE 802.3ab 1000Base-T, IEEE 802.3z 1000Base-SX/LX IEEE 802.3x Flow Control IEEE 802.1p QoS IEEE 802.1Q VLAN Tag IEEE 802.3ad Link Aggregation IEEE 802.3af Power over Ethernet (15.4 Watt PoE+) IEEE 802.3at Power over Ethernet Plus (30 Watt PoE+) 24 ports RJ-45 connectors for 10/100/1000 BASE-T and PSE/ PoE function</p>
Port Configuration	<p>4 SFP Uplink Ports</p>
Hardware Reset	<p>Reset Button for returning to original factory settings</p>
Media Access Protocol	<p>CSMA / CD</p>
Network Media	<p>10BASE –T: UTP Cat. 3 or up, 100BASE-TX: UTP Cat. 5 or up, 1000BASE-T: UTP Cat. 5 or up</p>
Transmission Method	<p>Store and Forward</p>
MAC Address Table	<p>8K</p>
Built-in Buffer	<p>4Mb</p>
Data Transfer Rate	<p>10/100Mbps (Half-duplex), 20/200Mbps (Full-duplex) 1000Mbps (Half-duplex), 2000Mbps (Full-Duplex)</p>
Auto MDI/MDIX	<p>Yes</p>
LED Indicators	<p>Per Port: Link Status*24 Per Port: Activity Status*24 Per Port: (PoE) : Status *24 SFP Port: Connection Status * 8 Per Unit: (PWR)r *1 Per Unit: (SYS) *1</p>
Internal Bus Speed	<p>56Gbps</p>

Switch Specifications

Link Aggregation	IEEE802.3ad LACP Link Aggregation Supported
Port Mirror	Supported
Quality of Service (QoS)	Supports IEEE 802.1p QoS, Port-based QoS
Bandwidth Control	Supported
Spanning Tree(STP)	Supported
Rapid Spanning Tree(RSTP)	Supported
IGMP Snooping	v1, v2, v3
MAC Filter	Supported
DHCP Snooping	Supported
VLAN	IEEE802.1Q Tagging VLAN , Port-Based ,Tag based VLAN
SNMP	Supports SNMP v1/v2c

Environmental & Mechanical Characteristics

PoE Power Budget	54V/6.7A for 350 Watt (shared) for all PoE ports
Power Consumption	12V/3A for 26.5 Watt (max. with no PoE Device connected)
Power Type	Power cord: Internal Power supply
Power Requirement	AC 100~240VAC, 50-60Hz Auto-sensing
Operating Temperature	0° to 40° C
Storage Temperature	-40° to 70° C
Operating Humidity	10% to 90% non-condensing
Storage Humidity	10% to 90% non-condensing
Dimension (W x D x H)	441 x 310 x 44 mm
Weight	4.18kg
Certification	FCC, CE, RoHS-compliant