

# CERIO Corporation

## CS-2424G

**24 Port 10/100/1000M Gigabit Web Managed Switch with 4**

**SFP Ports**



## User's 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	Feature .....	6
1.2	Package Contents .....	8
1.3	Front Panel.....	8
1.4	Rear Panel Layout.....	9
2.	Software Configuration .....	10
2.1	Example of Segment: (Windows 7).....	10
2.2	System login username and password information.....	14
3.	System Status.....	15
3.1	Device Information.....	15
3.2	Port Flow Chart.....	16
3.3	Traffic Statistics.....	16
3.4	MAC Table .....	17
3.5	System Load.....	18
3.6	Network Detection.....	19
4.	Network .....	20
4.1	IP Address .....	20
4.2	MAC Address.....	21
4.3	DNS Settings.....	21
4.4	DHCP Protect (snooping).....	22
4.5	DHCP Option82 .....	23
4.6	IGMP Snooping .....	24
4.7	Multicast VLAN.....	26
4.8	Voice VLAN .....	26
4.9	MAC VLAN.....	28
4.10	802.1x.....	28
4.11	LLDP .....	31
4.12	STP .....	32
4.13	Loop Detection.....	34
4.14	Jumbo Frame.....	35
4.15	RSTP .....	35
4.16	SNMP .....	36
5.	Port Configuration .....	37
5.1	Port Configuration.....	37
5.2	MDIX Configuration.....	38
5.3	Port Mirroring .....	38

5.4	MAC Limit .....	39
5.5	Port Aggregation .....	40
5.6	Port-IP-MAC-Binding .....	42
5.7	Rate Limit.....	43
5.8	Storm Control .....	44
6.	Security .....	45
6.1	Port Grouping.....	45
6.2	Port Isolation .....	46
6.3	MAC filter.....	46
6.4	DOS Defense .....	47
7.	VLAN Configuration .....	49
7.1	802.1Q VLAN.....	49
7.2	PVID.....	50
8.	ACL.....	50
8.1	MAC ACL.....	50
8.2	IP ACL.....	51
9.	QoS.....	53
9.1	Global Setting.....	53
9.2	Queue Weight.....	53
9.3	Queue Algorithm.....	54
9.4	Default Priority .....	55
9.5	Priority Mapping .....	55
9.6	QOS Trust.....	56
10.	System Setting .....	57
10.1	Quick Settings.....	57
10.2	Web Management.....	57
10.3	Internal No.....	58
10.4	Administrator.....	58
10.5	System Config.....	59
10.6	Firmware Upgrade.....	60
10.7	System Time .....	60
10.8	Reboot.....	62
11.	System Log.....	63
11.1	Event Log.....	63
11.2	Alarm Log.....	64
11.3	Security Log.....	64
11.4	Network Log.....	65

Specifications .....66

# 1. Introduction

CERIO CS-2000 Series Model: **CS-2424G** is a powerful high-performance 4 SFP Gigabit 24 port 10/100/1000Mbps web managed switch and supports Remote control and management through a web-based User Interface. This Layer 2 Web Managed switch supports Spanning Tree / Rapid Spanning Tree protocol, Port base IEEE802.1Q VLAN Tagging, IGMP snooping, IEEE802.1p port-based QoS, and Bandwidth control / Loop Detection. CS-2424G's high performance gigabit design provides reliable performance and allows for easy management of auto-negotiation speeds.

The CERIO CS-2000 Series **CS-2424G** Web Managed Switch is ideal for minimizing network downtime, connecting subnets for improved performance, and enabling the bandwidth demanded for multimedia and imaging applications. **CS-2424G** effectively reduces operational costs by allowing network administrators to remotely access and monitor their network, ultimately eliminating the need for constant on-site maintenance staff. **CS-2424G's** layer 2 web managed design also increases network security by providing enhanced network control through port management and visible MAC table addresses/clients. This device's high feature and high performance design, paired with an easy to use web interface, effectively improves both network management and efficiency for medium and large sized applications

## 1.1 Feature

- Complying with IEEE 802.3 10Base-T, IEEE 802.3u 100Base-TX, IEEE 802.3ab 1000Base-T, IEEE 802.3z 1000Base-SX/LX, IEEE 802.3az EEE
- 24port 10/100/1000Mbps TX Auto-Negotiation Ethernet Switch ,
- Supports 4 Gigabit SFP uplink ports and MiniGBic1000Base-SX/LX
- Full/Half-Duplex capability on each TX port , Auto-learning networking configurations
- Supports store & forward operation
- Supporting the flow control: back pressure for Half-duplex and IEEE 802.3x for Full-duplex mode
- Non-blocking & Non-head-of-line blocking full-wire speed forwarding
- Supports network interface Auto MDIX function for auto TX/RX swap
- Automatic Source MAC Address Learning and Aging
- Provides 9K Jumbo frames to improve network utilization of a large file transfers

- Supports up to 8K MAC addresses
- Up to 4Mb Packet Buffer size
- VLAN and IEEE802.1Q tag-base VLAN based on ports & VIDs; add/remove/modify tag
- IEEE802.3ad Link Aggregation LACP
- Provides IGMP v1/v2/v3 snooping function
- Supports Bandwidth Control with KB/s size control
- Supports 802.1x protocol to support CHAP, EAP mode and port/MAC based network access control
- Supports DoS (Denial of Service) Defense for enhanced network security
- Link Layer Discovery Protocol (LLDP) and LLDP-MED
- Supports DHCP Snooping function to prevent access by unauthorized hosts and DHCP servers
- Each port supports limiting the number of MAC Addresses with IP and MAC address Binding
- Supports Access Control List (ACL) for MAC and IP Address filtering
- Supports QoS Quality of Service, Port-based QoS bandwidth management, 802.1q priority Tag based with 8 priority Queues and 8 Weights
- Supports bandwidth control to set control traffic limits (inflow and outflow) for each port
- Supports Port Mirroring function
- Supports Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP)
- Supports proxy DNS Server and NTP network time synchronization function
- Supports Event Log, Alarm Log, Security Log, Network Log, and Protocol Log
- Supports web-based HTTP web management user interface and supports SNMP v1/v2c
- Supports GUI display for monitoring network data status by port, traffic analysis by port, and device CPU and Memory loading for convenient administrative network analysis and management

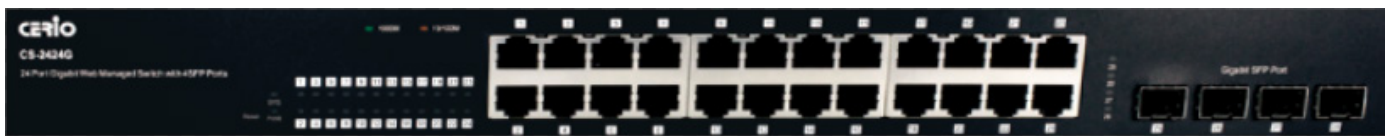
## 1.2 Package Contents

Before you start to install this switch, please verify your package contains the following items:

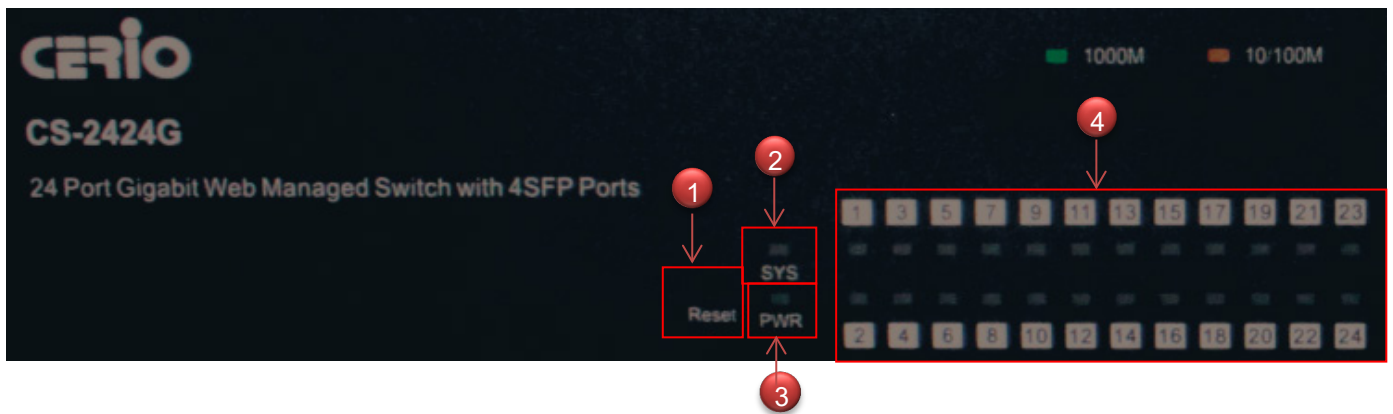
<b>CS-2424G Main Unit</b>	<b>x1</b>
<b>D Manual</b>	<b>x1</b>
<b>Power Cord</b>	<b>x1</b>
<b>19" Mount Brackets</b>	<b>x1</b>
<b>Warranty Card</b>	<b>x1</b>

## 1.3 Front Panel

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

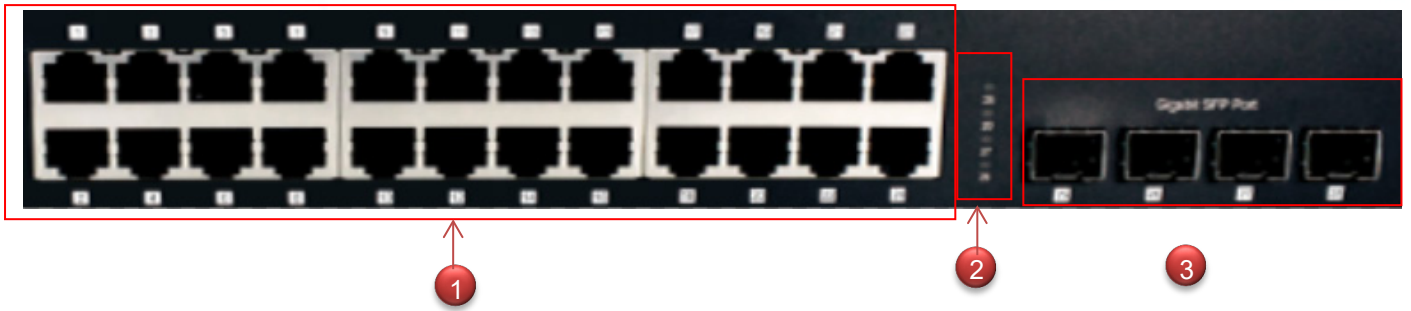


### Status Explanation



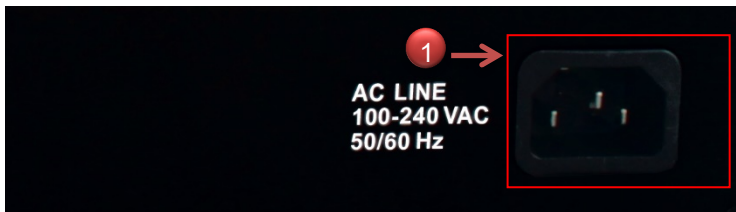
- 1) Hardware Reset button, press and hold for approximately 10 seconds. Once all the LED lights begin to flash, release the button to reset to default
- 2) System operational LED light
- 3) Power LED light.
- 4) 24 10/100/1000Mbps Port Link/ACT LED status light.





- 1) 24 10/100/1000Mbps Ethernet Ports
- 2) 4 SFP LED Status lights
- 3) 4 Fiber Ports

## 1.4 Rear Panel Layout



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

## 2. Software Configuration

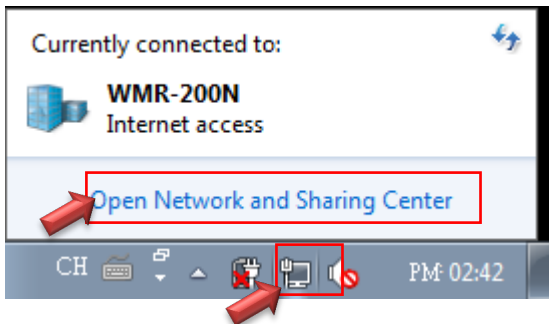
**CS-2424G** supports web-based configuration. Upon the completion of hardware installation, **CS-2424G** can be configured through a PC/NB by using its web browser such as Internet Explorer 6.0 or later.

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

### 2.1 Example of Segment: (Windows 7)

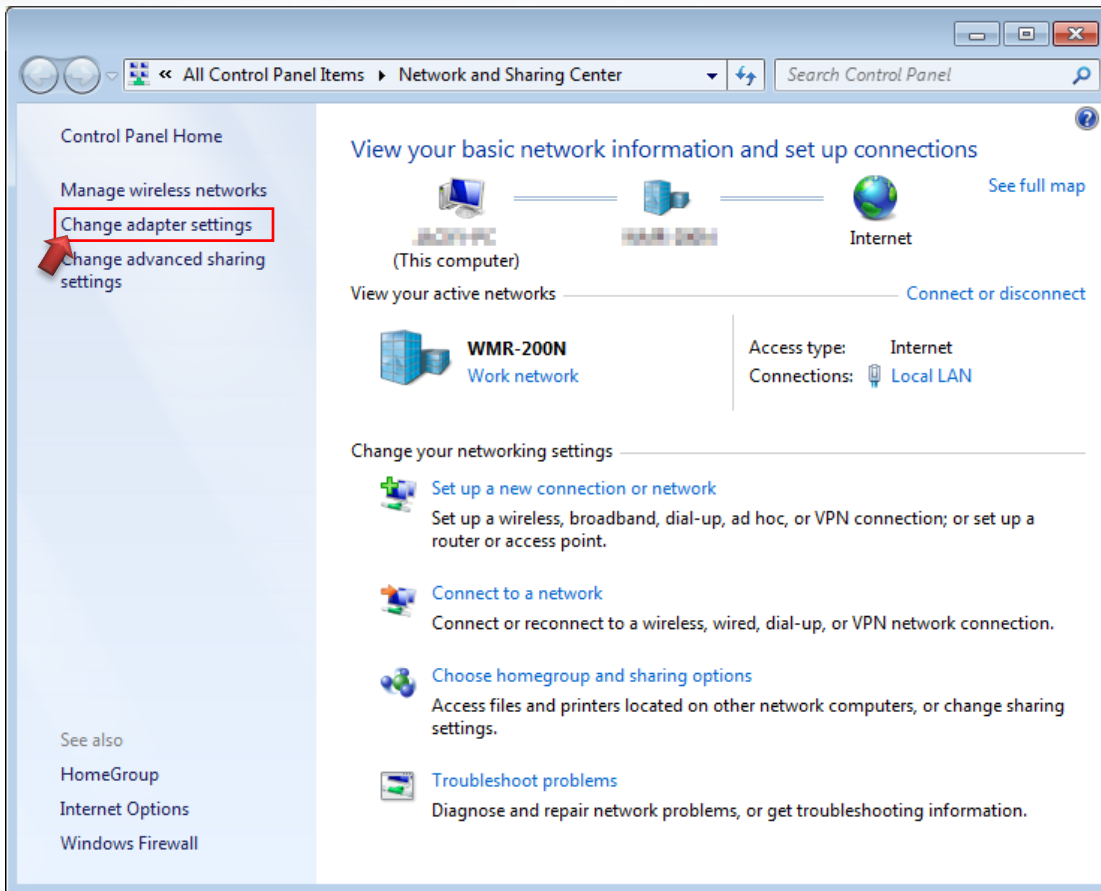
#### Step 1 :

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



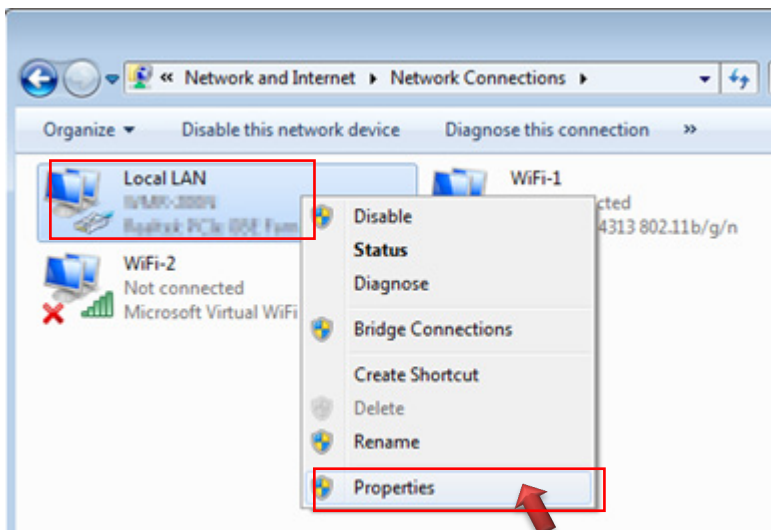
#### Step 2 :

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



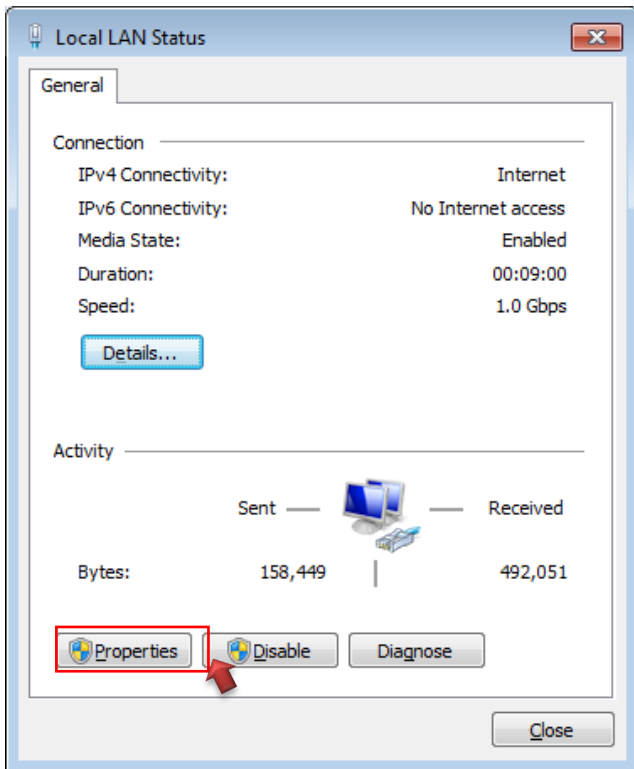
**Step 3 :**

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



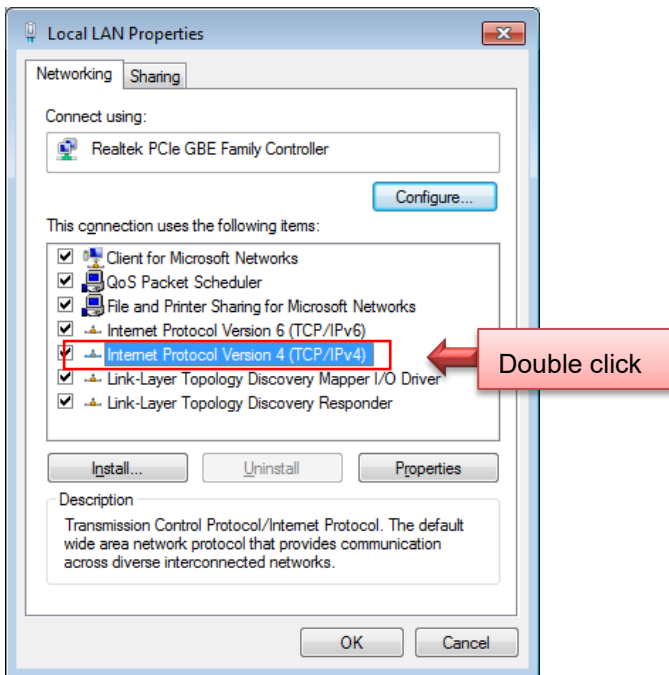
**Step 4 :**

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



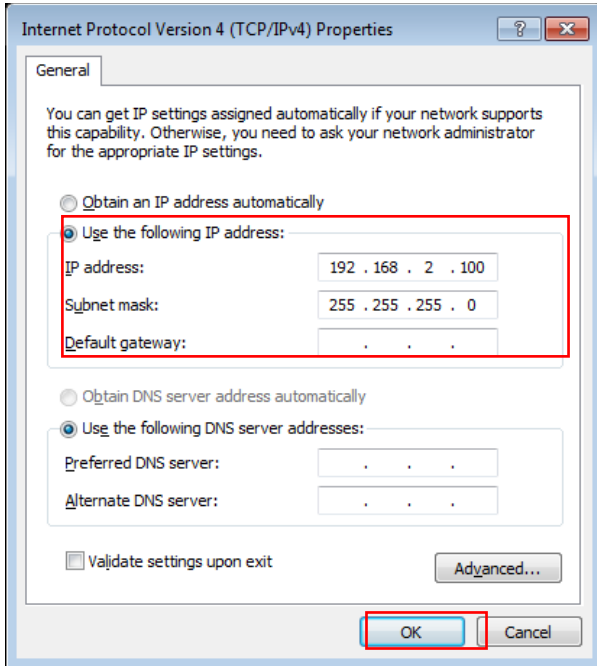
**Step 6 :**

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

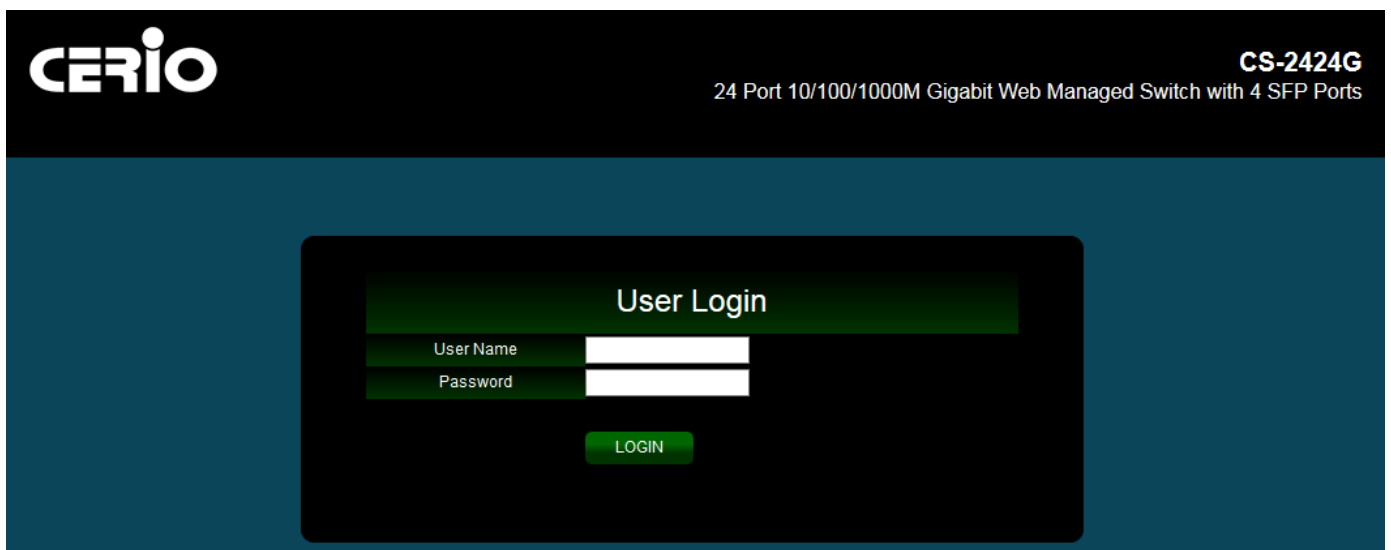
And Click **“OK”** to complete fixing the computer IP settings



**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

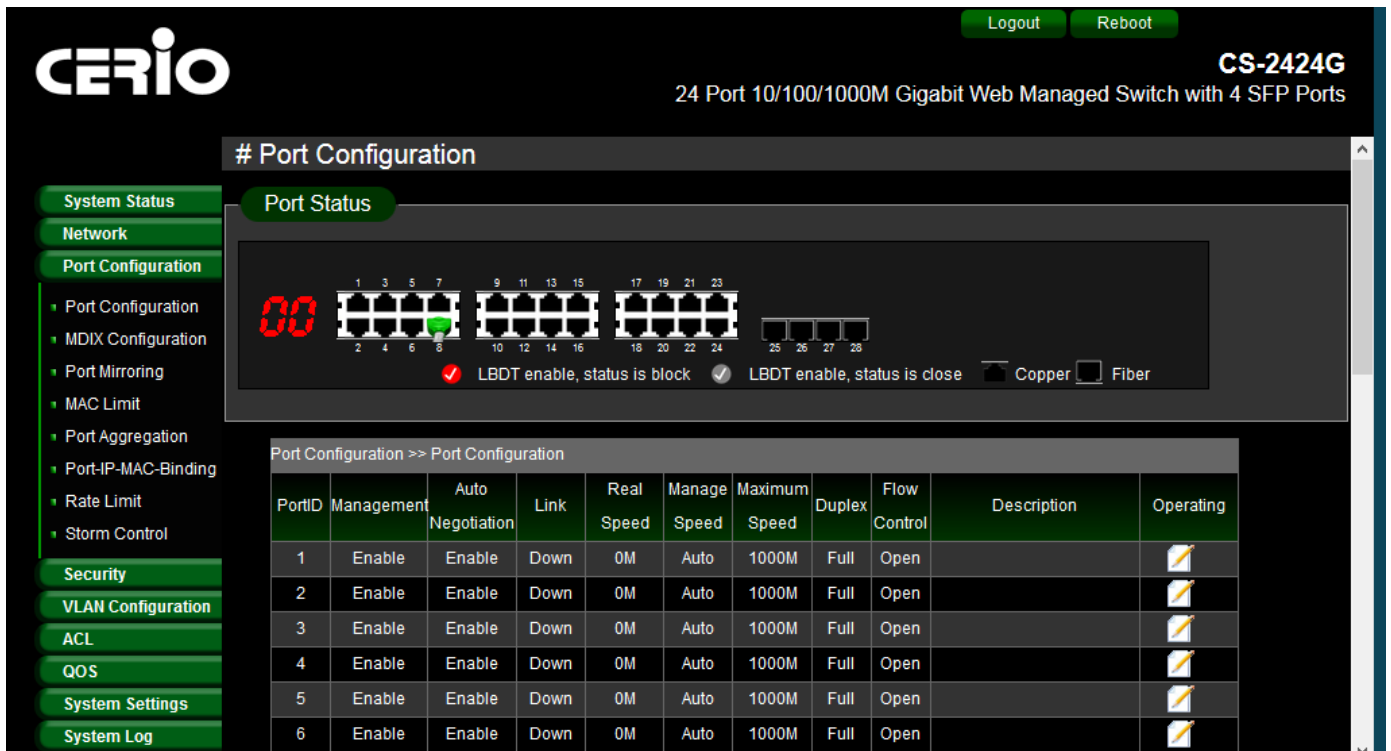
The **CS-2424G** web switch default IP is 192.168.2.200







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

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

<b>Management Account</b>	Root Account
<b>Username</b>	root
<b>Password</b>	default

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

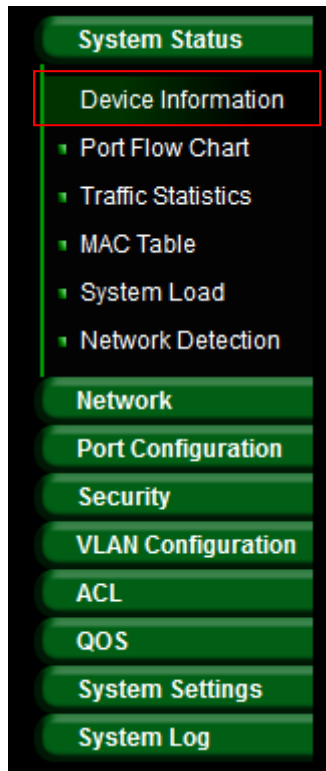


PortID	Management	Auto Negotiation	Link	Real Speed	Manage Speed	Maximum Speed	Duplex	Flow Control	Description	Operating
1	Enable	Enable	Down	0M	Auto	1000M	Full	Open		
2	Enable	Enable	Down	0M	Auto	1000M	Full	Open		
3	Enable	Enable	Down	0M	Auto	1000M	Full	Open		
4	Enable	Enable	Down	0M	Auto	1000M	Full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

## 3. System Status

### 3.1 Device Information

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

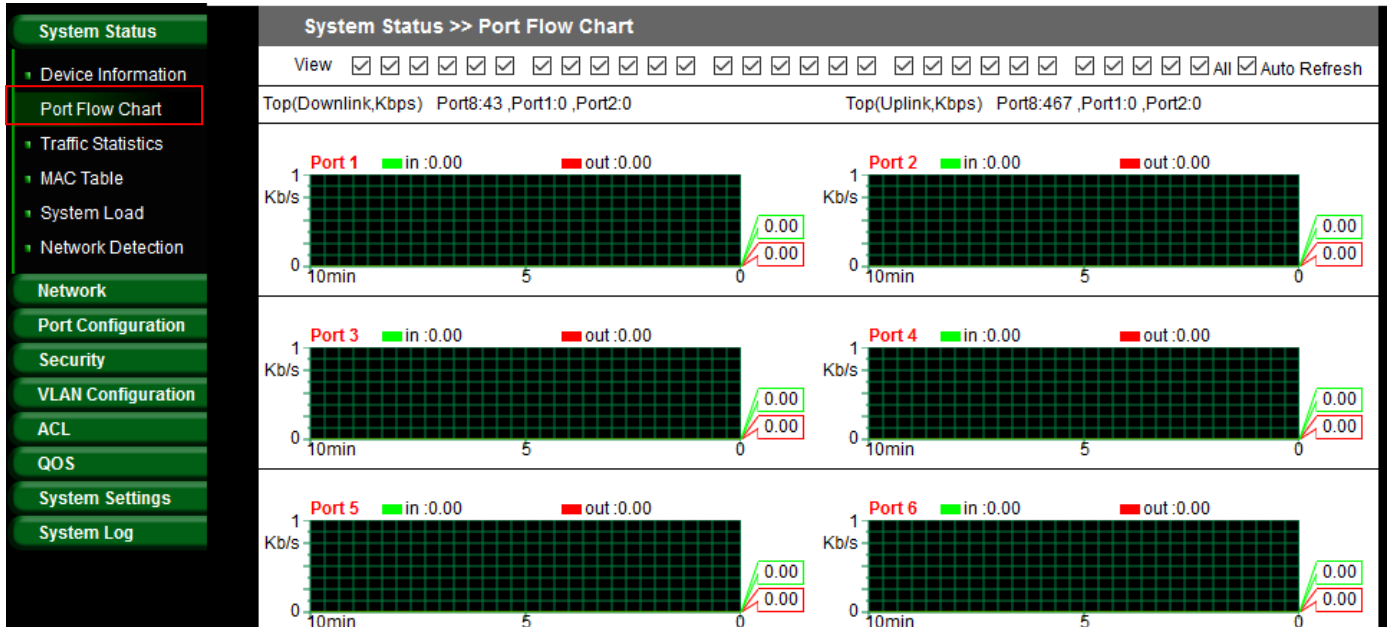


System Status >> Device Information	
Host Name	CERIO_Switch
Model	CS-2424G
Firmware Version	0.3.023u6
MAC Address	8C:4D:EA:04:11:11
IP Address	192.168.2.200
Running Time	00:12:08
System Time	2016-06-02 09:17:26

- **Host Name:** Display host name for 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.

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	0.00 B / 0.00 B	0 / 0	0 / 0	0 / 0	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	688.99 KB / 6.27 MB	4175 / 6064	616 / 4	234 / 2	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



### 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.

The screenshot shows the 'MAC Table' page in a web interface. On the left is a sidebar with menu items: System Status, Device Information, Port Flow Chart, Traffic Statistics, MAC Table (highlighted with a red box), System Load, Network Detection, Network, Port Configuration, Security, VLAN Configuration, ACL, QOS, System Settings, and System Log. The main content area has tabs for 'Forwarding List', 'Set Static MAC', and 'Dynamic Address Settings'. Below the tabs is a table with the following data:

Port	MAC Address	VLAN ID	Status
8	8C:4D:EA:02:C6:ED	1	Dynamic

Below the table, there are pagination controls: 'total 1', 'Page Size 15', 'Page No. 1 / 1', and navigation buttons 'First', 'Previous', 'Next', 'Last', 'Goto 1'.

- **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.

The screenshot shows the 'Set Static MAC' configuration window. It has tabs for 'Forwarding List', 'Set Static MAC' (highlighted with a red box), and 'Dynamic Address Settings'. Below the tabs is a table with the following data:

Number	MAC Address	VLAN ID	Port	Operating
1	8C:4D:EA:02:C6:ED	1	8	

Below the table is an 'Edit' dialog box with the following fields:

MAC Address	8C:4D:EA:02:C6:ED
VLAN	1
Port	Port8

At the bottom of the dialog are 'Save' and 'Cancel' buttons.

- **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.

The screenshot shows a web interface with three tabs: 'Forwarding List', 'Set Static MAC', and 'Dynamic Address Settings'. The 'Dynamic Address Settings' tab is active. It contains a form with a label 'Aging Time' and a text input field containing the value '500'. To the right of the input field, it says 'Value Range: 10 - 630'. Below the input field is a green 'Save' button.

- **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.

The screenshot shows a web interface with a sidebar on the left containing menu items: 'System Status', 'Device Information', 'Port Flow Chart', 'Traffic Statistics', 'MAC Table', 'System Load' (highlighted with a red box), 'Network Detection', 'Network', and 'Port Configuration'. The main content area has two tabs: 'Service' and 'System Load'. The 'System Load' tab is active and contains a table with the following data:

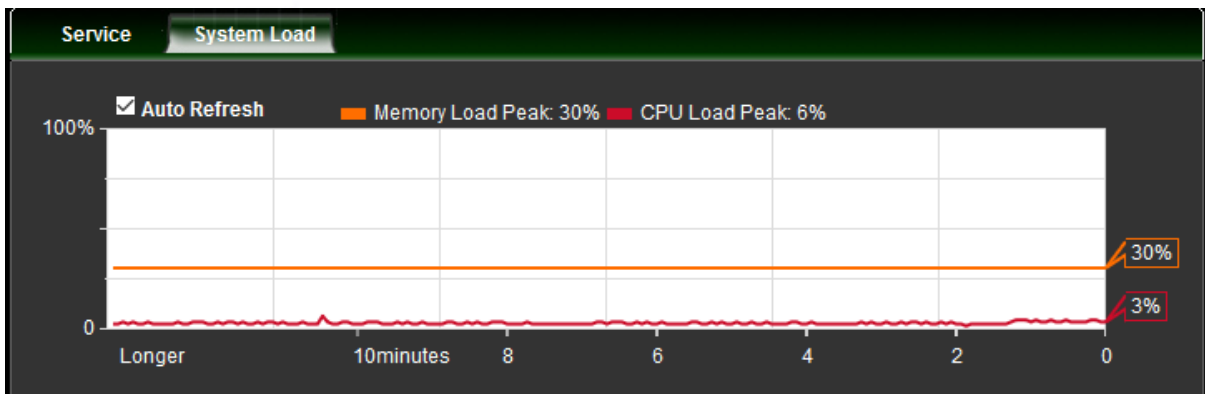
Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
CPU Threshold	50% ▾
Memory Threshold	50% ▾

Below the table is a green 'Save' button.

- **Service:** Administrator can select Enable or disable for the service.
- **CUP/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="v"/>
<input type="button" value="Detection"/>	

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

**Network >> IP Address**

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

Default Gateway	<input type="text" value="192.168.2.1"/>
IPv6 Address	<input type="text" value="::192.168.169.1"/> / <input type="text" value="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 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	DHCP Server
<input type="button" value="OK"/> <input type="button" value="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  Enable  Disable

Trust Port(s) 1-24

**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 Trist 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

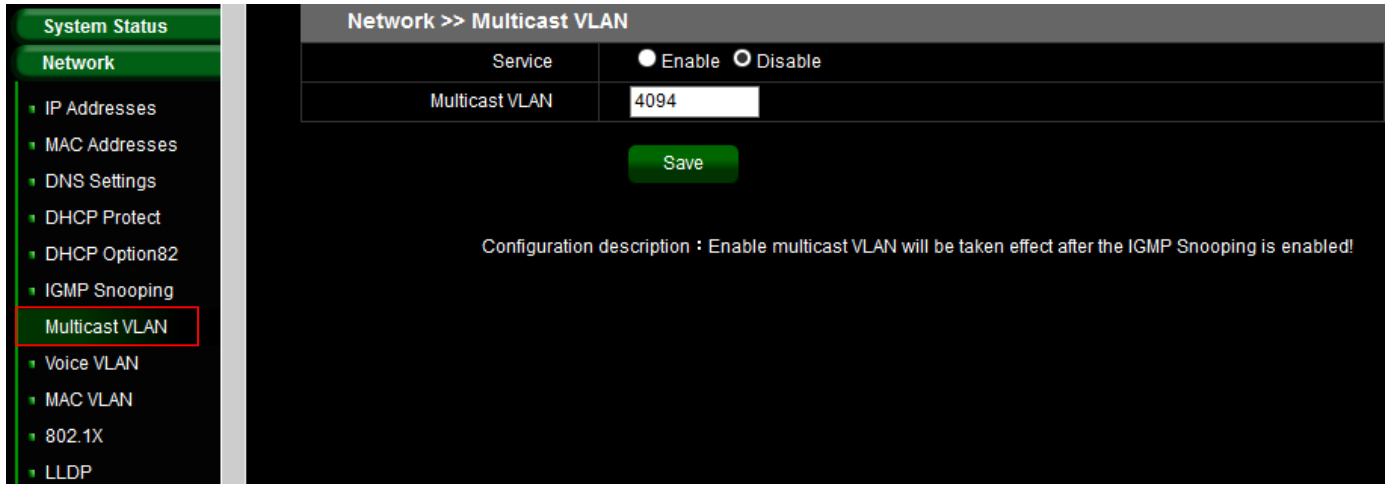
IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast 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.



- **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 immediate 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.

## 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.



**System Status**

**Network**

- IP Addresses
- MAC Addresses
- DNS Settings
- DHCP Protect
- DHCP Option82
- IGMP Snooping
- Multicast VLAN**
- Voice VLAN
- MAC VLAN
- 802.1X
- LLDP

**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!

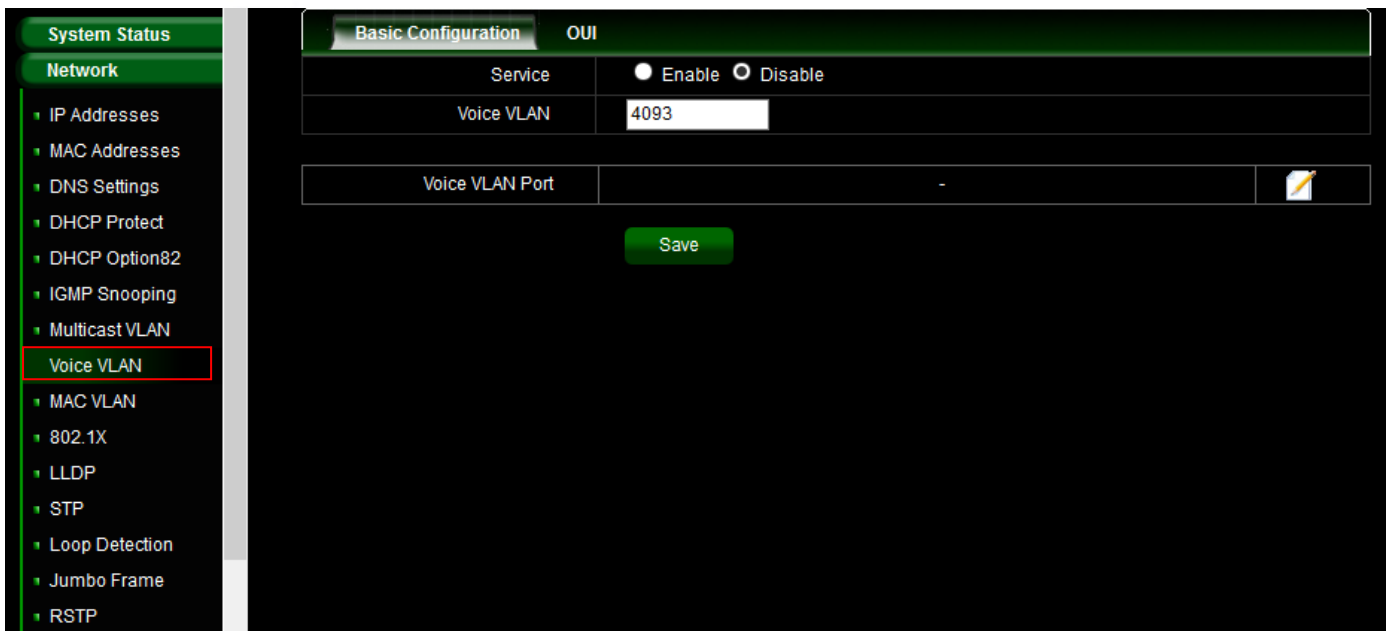
- **Service:** Administrator can select enable or disable the Service
- **Multicast VLAN:** Administrator can set VLAN ID in the range of 1 to 4094.



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	

Save +

## 4.9 MAC VLAN

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

The screenshot shows the 'Network >> MAC VLAN' configuration page. At the top, there is a toggle for 'MAC VLAN' with 'Enable' selected. Below this is a table with the following data:

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	

Below the table, there is a green 'Save' button and a red message: 'The configuration has been modified, please save in time'. A green '+' button is also visible in the bottom right corner of the main area.

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



Administrator can click button to create MAC VLAN.

## 4.10 802.1x

When client used 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 for 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"/>

- **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="XXXXXXXXXX"/>	The characters length of auth key can't be greater than 32!
Num Of Retry	<input type="text" value="3"/>	

### 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:

- **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.

The screenshot displays the LLDP configuration page. On the left is a navigation menu with 'LLDP' highlighted. The main content area is divided into two sections: 'LLDP Set' and 'LLDP Port Neighbor Info'.

**LLDP Set**

Service:  Enable  Disable

LLDPDU Send Interval:

TTL Multiplier:

LLDPDU Send Delay:

Port Initialize Delay Time:

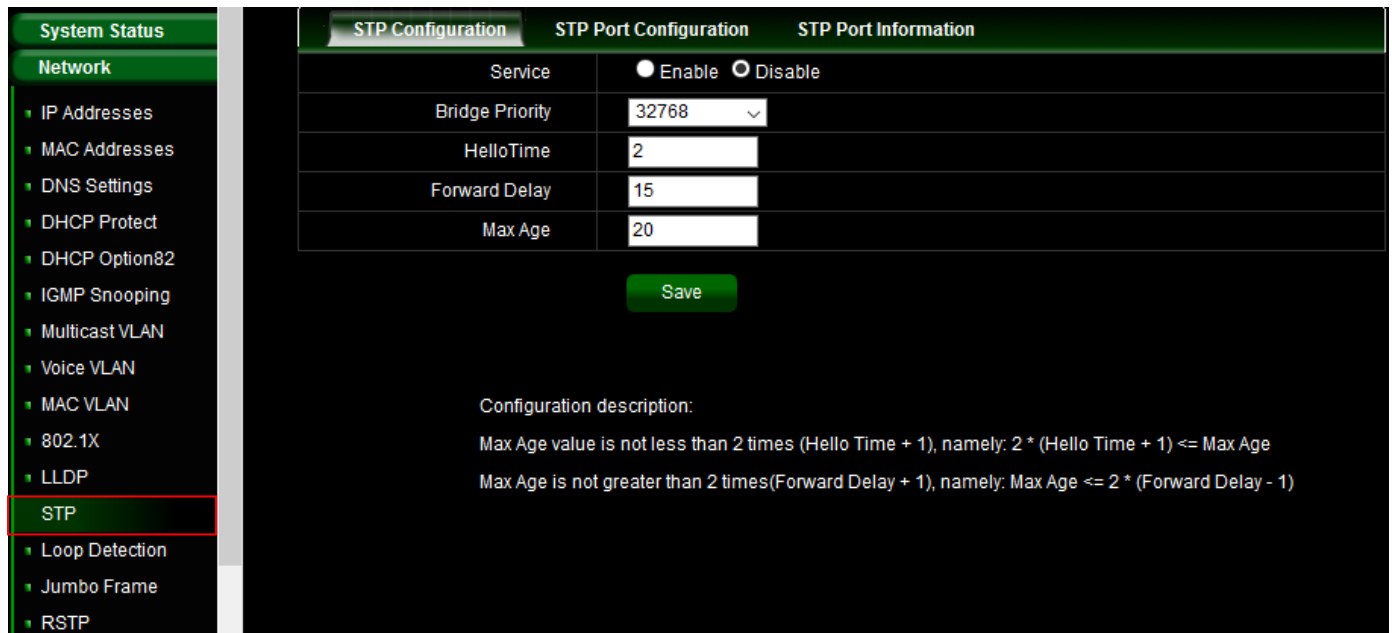
**LLDP Port Neighbor Info**

Network >> LLDP Port Set			
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.



The screenshot shows the STP Configuration page in the Cerio web interface. The left sidebar lists various network settings, with 'STP' selected. The main content area has three tabs: 'STP Configuration', 'STP Port Configuration', and 'STP Port Information'. The 'STP Configuration' tab is active, showing a table with the following settings:

Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Bridge Priority	32768
HelloTime	2
Forward Delay	15
Max Age	20

Below the table is a 'Save' button. Underneath, there is a 'Configuration description:' section with the following text:

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:  $\text{Max Age} \leq 2 * (\text{Forward Delay} - 1)$

- **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**

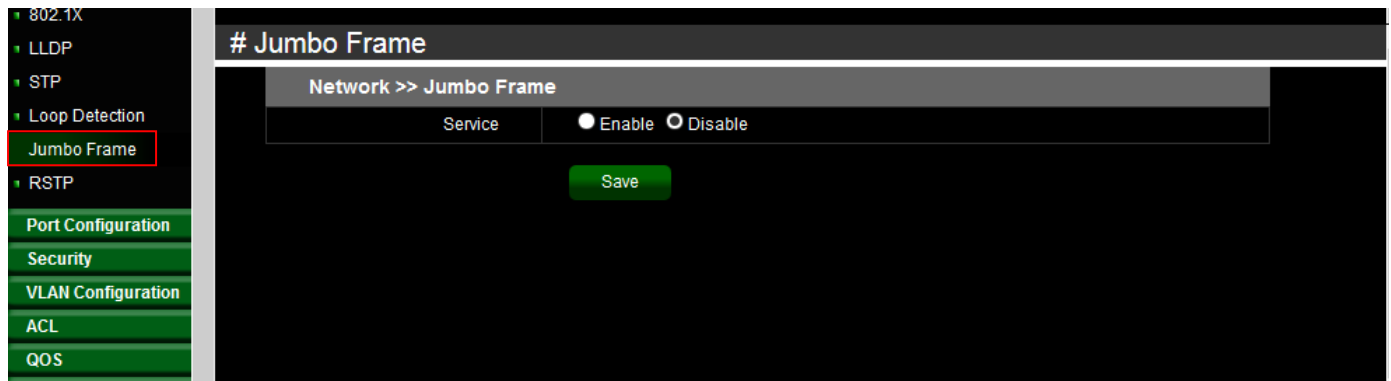
- IP Addresses
- MAC Addresses
- DNS Settings
- DHCP Protect
- DHCP Option82
- IGMP Snooping
- Multicast VLAN
- Voice VLAN
- MAC VLAN
- 802.1X
- LLDP
- STP
- Loop Detection
- Jumbo Frame
- RSTP

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	-	

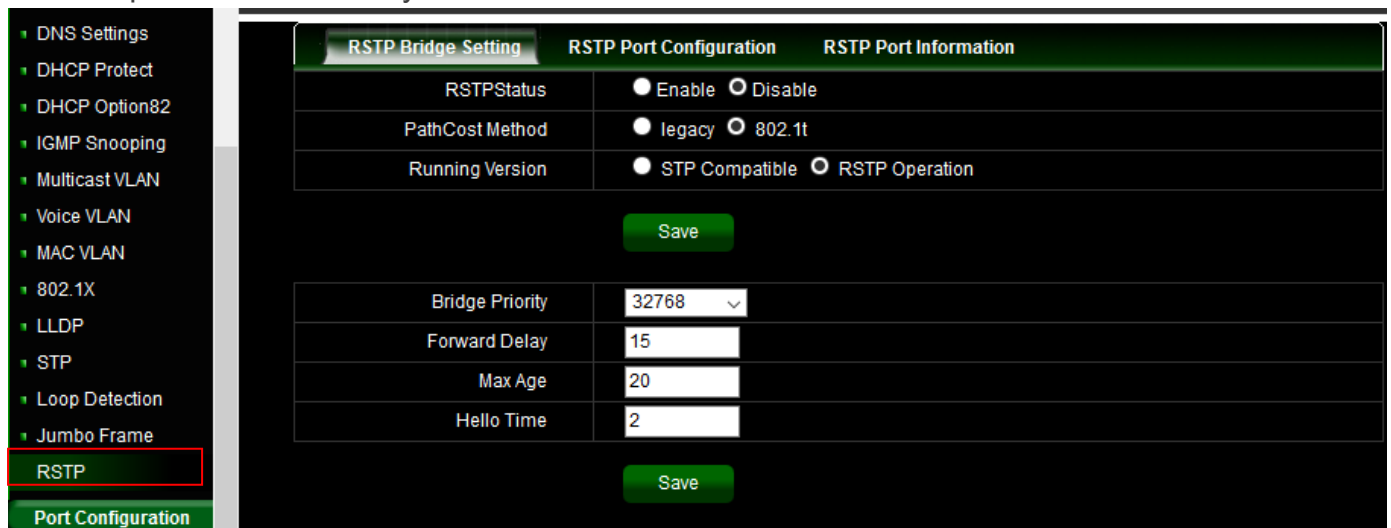
## 4.14 Jumbo Frame

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.



## 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.



## 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.

# SNMP Settings

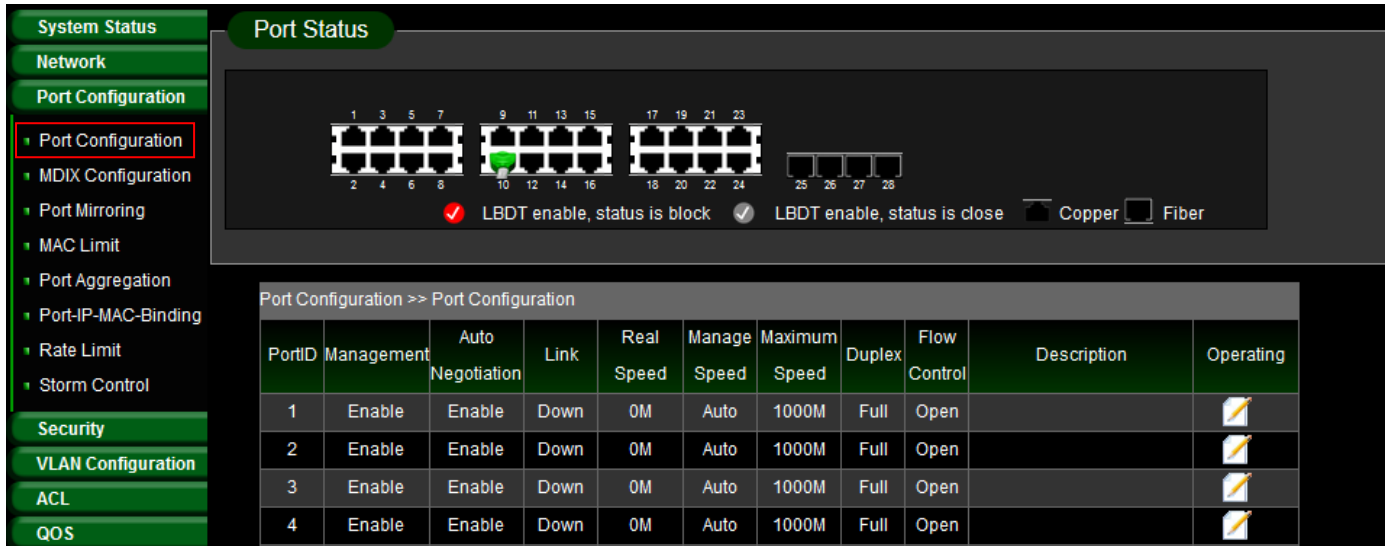
Set	Community	User	Trap
SNMP			<input type="radio"/> Enable <input type="radio"/> Disable
SNMP Trap			<input type="radio"/> Enable <input type="radio"/> Disable
Local Engine ID		8000000001020304	
Contact Info		contact@mail.com	
Physical Location Information		location.where	
SNMP Version			<input type="checkbox"/>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

Save

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

## 5. Port Configuration

### 5.1 Port Configuration



Port Status

1 3 5 7 9 11 13 15 17 19 21 23  
2 4 6 8 10 12 14 16 18 20 22 24 25 26 27 28

LBDT enable, status is block  LBDT enable, status is close  Copper  Fiber

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		

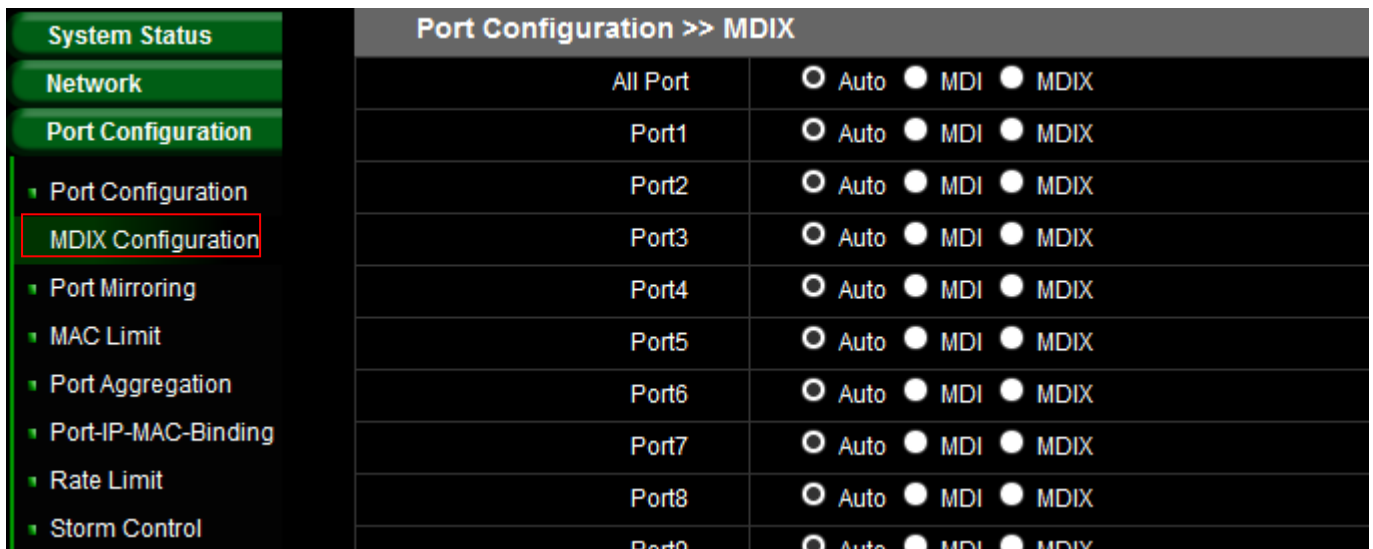
Administrator can click Operating list button to modify port Operation.

**Edit**

Port	<input type="text" value="1"/>
Status	<input type="text" value="Enable"/>
Auto Negotiation	<input type="text" value="Enable"/>
Link	<input type="text" value="Down"/>
Manage Speed	<input type="text" value="1000M"/>
Maximum Speed	<input type="text" value="1000"/>
Duplex	<input type="text" value="Full"/>
Flow Control	<input type="text" value="Open"/>
Description	<input type="text"/>
<input type="button" value="OK"/> <input type="button" value="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.

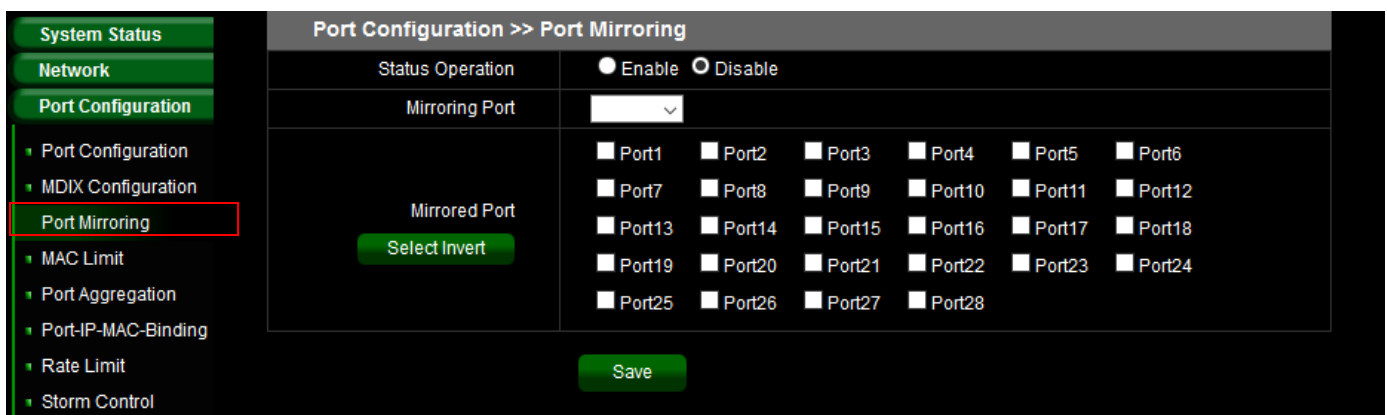


The screenshot shows the 'Port Configuration >> MDIX' page. On the left is a navigation menu with 'MDIX Configuration' highlighted. The main area is a table with columns for 'All Port' and three radio button options: 'Auto', 'MDI', and 'MDIX'. The 'MDI' option is selected for all ports from Port1 to Port9.

Port	Auto	MDI	MDIX
All Port	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port1	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port3	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port4	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port5	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port6	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port7	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port8	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port9	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

## 5.3 Port Mirroring

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































The screenshot shows the 'Port Configuration >> Port Mirroring' page. The 'Status Operation' is set to 'Enable'. The 'Mirroring Port' is set to a dropdown menu. The 'Mirrored Port' section contains a grid of checkboxes for ports 1 through 28. A 'Select Invert' button is located below the grid. A 'Save' button is at the bottom.

- **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.

System Status		Port Configuration >> MAC Limit			
Network		Port	Status	MAC Maximum	Operating
Port Configuration		1	Disable	100	 
<ul style="list-style-type: none"> <li>▸ Port Configuration</li> <li>▸ MDIX Configuration</li> <li>▸ Port Mirroring</li> <li style="border: 1px solid red;">▸ MAC Limit</li> <li>▸ Port Aggregation</li> <li>▸ Port-IP-MAC-Binding</li> <li>▸ Rate Limit</li> <li>▸ Storm Control</li> </ul>		2	Disable	100	 
Security		3	Disable	100	 
VLAN Configuration		4	Disable	100	 
ACL		5	Disable	100	 
QOS		6	Disable	100	 
System Settings		7	Disable	100	 
System Log		8	Disable	100	 
		9	Disable	100	 
		10	Disable	100	 
		11	Disable	100	 
		12	Disable	100	 
		13	Disable	100	 
		14	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"/>
<div style="display: flex; justify-content: center; gap: 20px;"> <span style="background-color: #333; color: white; padding: 5px 15px; border-radius: 3px;">Save</span> <span style="background-color: #333; color: white; padding: 5px 15px; border-radius: 3px;">Cancel</span> </div>	

## 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.

The screenshot displays the configuration page for Port Aggregation. On the left is a navigation menu with categories: System Status, Network, Port Configuration (with sub-items: Port Configuration, MDIX Configuration, Port Mirroring, MAC Limit, Port Aggregation, Port-IP-MAC-Binding, Rate Limit, Storm Control), Security, VLAN Configuration, ACL, QOS, System Settings, and System Log. The main content area has three tabs: Basic Configuration, LACP Priority, and LACP Port Information. Under 'Basic Configuration', there is a 'Policy' field and radio buttons for SIP, DIP, SIP + DIP, SMAC, DMAC, and SMAC + DMAC. Below this is a 'Save' button. The next section is 'Port Aggregation >> LACP', featuring a 'Status' field with 'Enable' and 'Disable' radio buttons, and another 'Save' button. The final section is 'Port Aggregation >> Aggregation Group', which contains a table with columns: Aggregation Interface, Link Type, Port Members, Remarks, and Operating. Below the table are a 'Save' button and a '+' icon.

### 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.

This close-up shows the 'Basic Configuration' tab. It includes a 'Policy' input field, radio buttons for SIP, DIP, SIP + DIP, SMAC, DMAC, and SMAC + DMAC, and a 'Save' button.

This close-up shows the 'Port Aggregation >> LACP' section with 'Status' (Enable/Disable) and a 'Save' button. Below it is the 'Port Aggregation >> Aggregation Group' section, showing a table with columns: Aggregation Interface, Link Type, Port Members, Remarks, and Operating. It also includes a 'Save' button and a '+' icon.



### 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

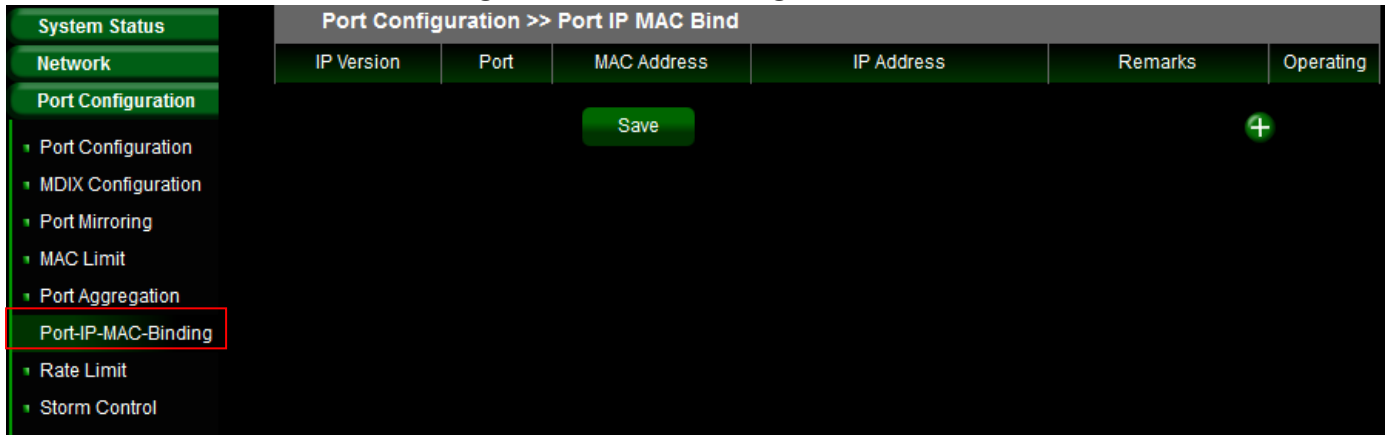
Basic Configuration		LACP Priority	LACP Port Information					
Aggregation Interface	Port	LACP Status	Port Priority	Port Status	Opposite Port	Status Information	Operate Key	Operating

**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	
<ul style="list-style-type: none"> <li>▸ Port Configuration</li> <li>▸ MDIX Configuration</li> <li>▸ Port Mirroring</li> <li>▸ MAC Limit</li> <li>▸ Port Aggregation</li> <li>▸ Port-IP-MAC-Binding</li> <li>▸ Rate Limit</li> <li style="border: 1px solid red;">▸ Storm Control</li> </ul>		2	0	0	0	
		3	0	0	0	
		4	0	0	0	
		5	0	0	0	
		6	0	0	0	
		7	0	0	0	
		8	0	0	0	
		9	0	0	0	

**Edit**
✕

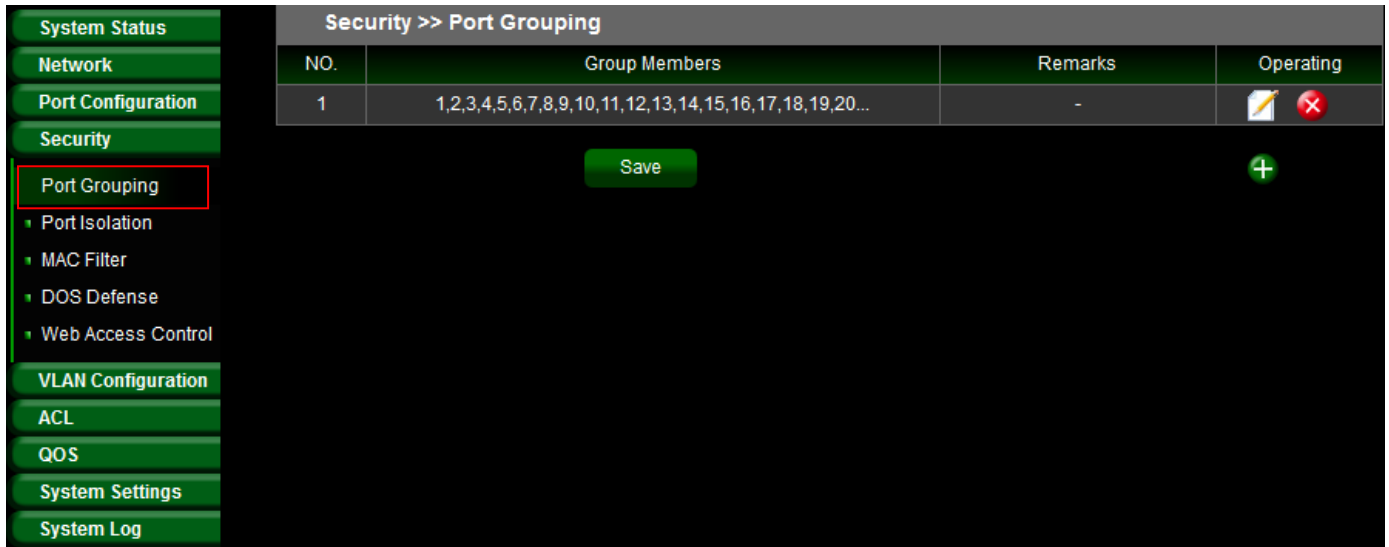
Port	<input type="text" value="1"/>
Unknown Unicast	<input type="text"/> KB
Multicast	<input type="text"/> KB
Broadcasting	<input type="text"/> KB
<div style="display: flex; justify-content: center; gap: 20px;"> <span style="background-color: #333; color: white; padding: 5px 15px; border-radius: 3px;">OK</span> <span style="background-color: #333; color: white; padding: 5px 15px; border-radius: 3px;">Cancel</span> </div>	

## 6. Security

### 6.1 Port Grouping

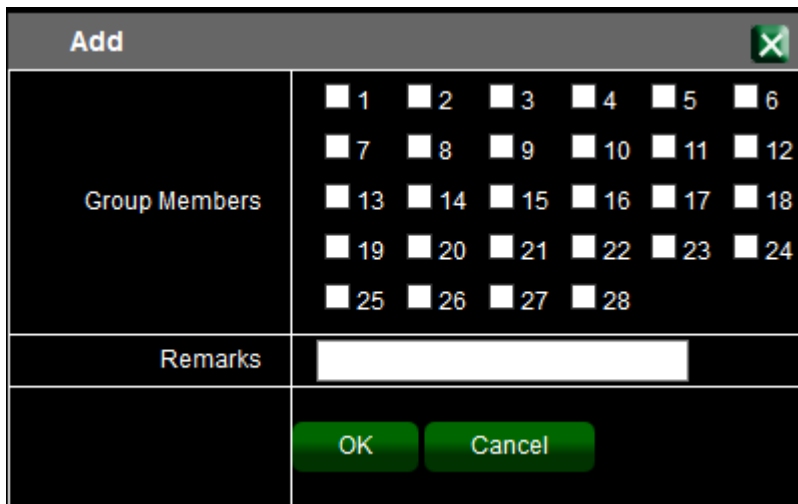
Administrator can create own grouping of devices and ports to efficiently update and manage devices.

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



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...	-	

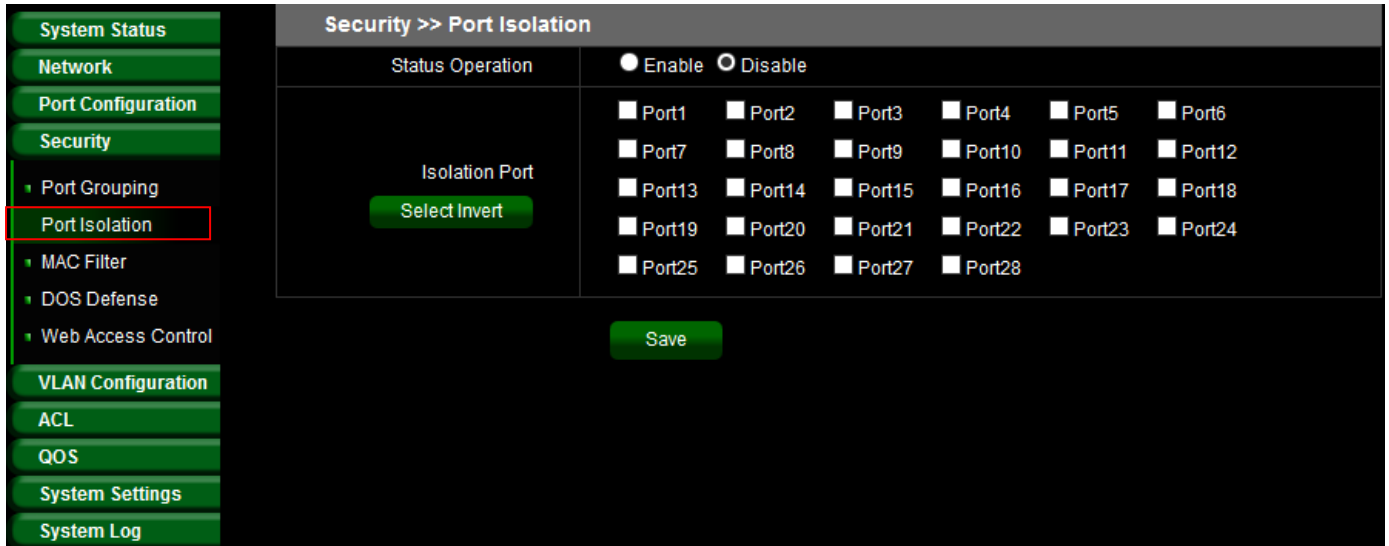
**Save** **+**



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"/>	

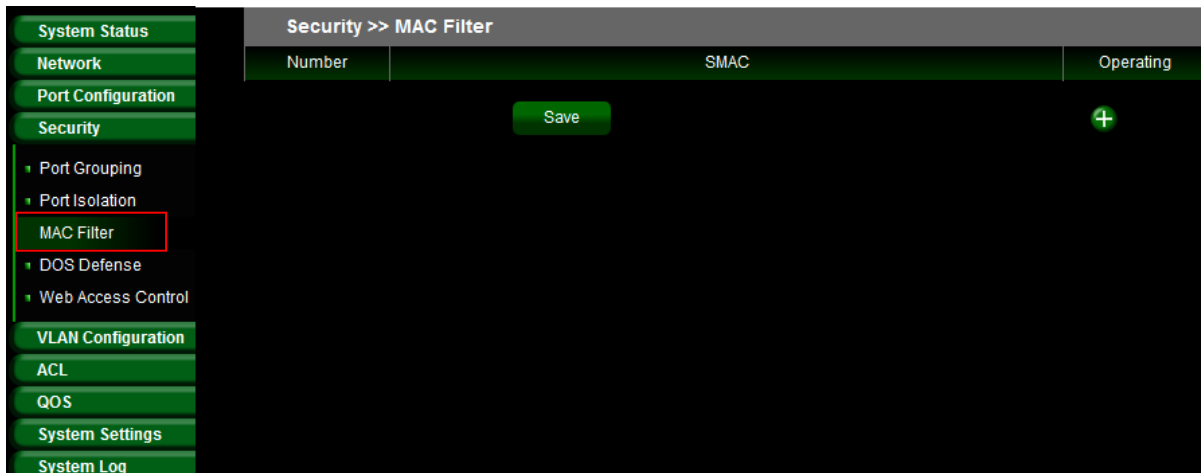
## 6.2 Port Isolation

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.



## 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.

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

Security >> DOS Attack Defense

Service  Enable  Disable

DOS Attack Defense >> Port Set

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

Edit
✕

Port	<input type="text" value="1"/>
Status	<input type="text" value="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.

**System Status**

**Network**

**Port Configuration**

**Security**

- Port Grouping
- Port Isolation
- MAC Filter
- DOS Defense
- Web Access Control

**VLAN Configuration**

ACL

QOS

System Settings

System Log

**Security >> Web Access Control**

Service  Enable  Disable

Number	SIP	Operating
		+

Save

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

**Add** [Close]

Number	1
SIP	

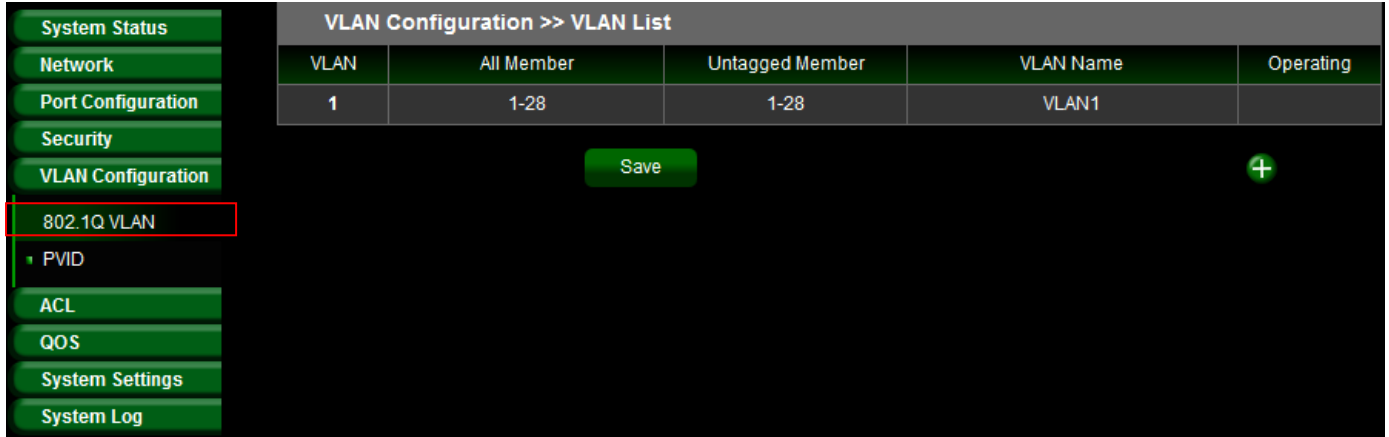
OK Cancel



# 7.VLAN Configuration

## 7.1 802.1Q VLAN

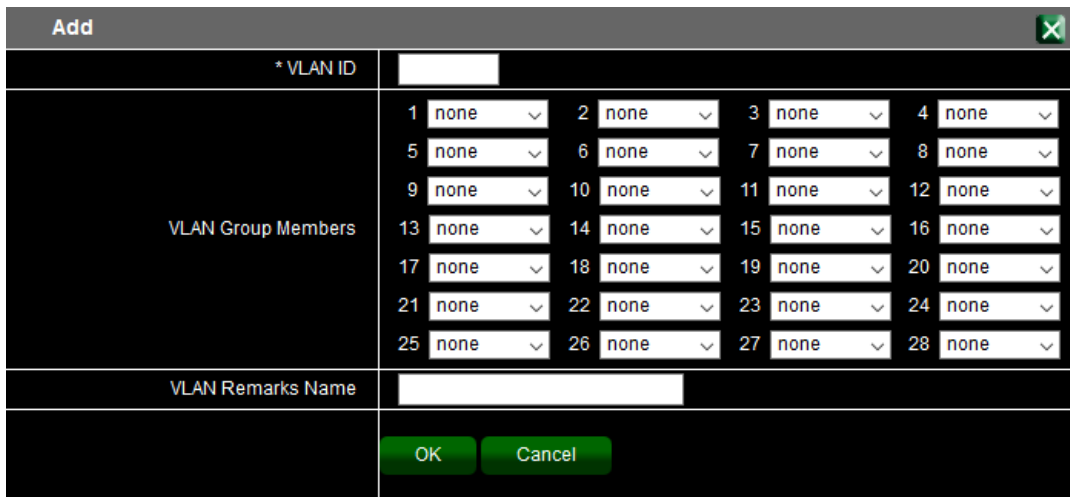
The VLAN function can set Tag Based VLAN.



VLAN Configuration >> VLAN List				
VLAN	All Member	Untagged Member	VLAN Name	Operating
1	1-28	1-28	VLAN1	

Buttons: Save, +

Navigation menu: System Status, Network, Port Configuration, Security, VLAN Configuration (802.1Q VLAN highlighted), PVID, ACL, QOS, System Settings, System Log



**Add** [Close]

\* VLAN ID:

VLAN Group Members	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
	none	none	none	none	none	none	none	none	none	none	none	none	none	none	none	none	none	none	none	none	none	none	none	none	none	none	none	none

VLAN Remarks Name:

Buttons: OK, Cancel

- **None:** No change any egress packets.
- **Tag:** Insert port's tag for egress packets.
- **UnTagged:** Remove tag ID.

## 7.2 PVID

The Page administrator can set PVID protocol.

System Status		VLAN Configuration >> PVID		
Network	Port	Pvid	Operating	
Port Configuration	1	1		
Security	2	1		
VLAN Configuration	3	1		
802.1Q VLAN	4	1		
<b>PVID</b>	5	1		
ACL	6	1		
QOS	7	1		
System Settings	8	1		
System Log	9	1		

**Edit** ✕

Port	<input type="text" value="1"/>
Pvid	<input 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.

System Status		ACL >> MAC ACL						
Network	Name	Privilege	DMAC	DMAC Mask	SMAC	SMAC Mask	Operating	
Port Configuration	<input type="button" value="Save"/>							
Security								
VLAN Configuration								
ACL								
<b>MAC ACL</b>								
IP ACL								
QOS								
System Settings								
System Log								

Add <span style="float: right;">✕</span>	
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.

	Basic Configuration	Expert Configuration			
	Name	Privilege	SIP	SIP Mask	Operating
	<input type="button" value="Save"/>				<input type="button" value="+"/>
System Status					
Network					
Port Configuration					
Security					
VLAN Configuration					
ACL					
MAC ACL					
<b>IP ACL</b>					
QOS					
System Settings					
System Log					

Add <span style="float: right;">✕</span>	
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 detail protocol of the ACL, administrator can click "Expert Configuration" to set detail function.

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 the following example.

**Edit**
✕

<b>*Name</b>	<input type="text" value="Danny"/>
<b>*Privilege</b>	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
<b>*SIP</b>	<input type="text" value="192.168.2.20"/>
<b>*SIP Mask</b>	<input type="text" value="0.0.0.0"/>
<b>*DIP</b>	<input type="text" value="192.168.2.200"/>
<b>*DIP Mask</b>	<input type="text" value="0.0.0.0"/>
<b>Protocol(Optional)</b>	<input type="text" value="ICMP"/> ▾
<b>*Type</b>	<input type="text" value="8"/>
<b>*Code</b>	<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									
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		
1	WFQ			
2	WFQ			
3	WFQ			
4	WFQ			
5	WFQ			
6	WFQ			
7	WFQ			
8	WFQ			
9	WFQ			
10	WFQ			

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

- **WFQ:** Each Queue can set the 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 <span style="float: right;">✕</span>	
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.

	QOS >> QOS Trust			
	Port	QOS Trust Mode		
	1	<input type="radio"/> COS Only	<input type="radio"/> DSCP Prior To The COS	<input type="radio"/> DSCP Only <input type="radio"/> Distrust
	2	<input type="radio"/> COS Only	<input type="radio"/> DSCP Prior To The COS	<input type="radio"/> DSCP Only <input type="radio"/> Distrust
	3	<input type="radio"/> COS Only	<input type="radio"/> DSCP Prior To The COS	<input type="radio"/> DSCP Only <input type="radio"/> Distrust
	4	<input type="radio"/> COS Only	<input type="radio"/> DSCP Prior To The COS	<input type="radio"/> DSCP Only <input type="radio"/> Distrust
	5	<input type="radio"/> COS Only	<input type="radio"/> DSCP Prior To The COS	<input type="radio"/> DSCP Only <input type="radio"/> Distrust
	6	<input type="radio"/> COS Only	<input type="radio"/> DSCP Prior To The COS	<input type="radio"/> DSCP Only <input type="radio"/> Distrust
	7	<input type="radio"/> COS Only	<input type="radio"/> DSCP Prior To The COS	<input type="radio"/> DSCP Only <input type="radio"/> Distrust
	8	<input type="radio"/> COS Only	<input type="radio"/> DSCP Prior To The COS	<input type="radio"/> DSCP Only <input type="radio"/> Distrust
	9	<input type="radio"/> COS Only	<input type="radio"/> DSCP Prior To The COS	<input type="radio"/> DSCP Only <input type="radio"/> Distrust
	10	<input type="radio"/> COS Only	<input type="radio"/> DSCP Prior To The COS	<input type="radio"/> DSCP Only <input type="radio"/> Distrust
	11	<input type="radio"/> COS Only	<input type="radio"/> DSCP Prior To The COS	<input type="radio"/> DSCP Only <input type="radio"/> Distrust



## 10. System Setting

### 10.1 Quick Settings

The function administrator can quick set switch for the hostname, IP address, DNS and gateway.

System Settings >> Quick Settings	
Hostname	<input type="text" value="switch"/>
IP Address	<input type="text" value="192.168.169.1"/>
Netmask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.2.1"/>
Primary DNS Server	<input type="text" value="0.0.0.0"/>
Secondary DNS Server	<input type="text" value="0.0.0.0"/>

- System Status
- Network
- Port Configuration
- Security
- VLAN Configuration
- ACL
- QOS
- System Settings
- Quick Settings
- WEB Management
- Internal No.
- Administrator
- System Config
- Firmware Upgrade
- System Time
- Reboot

### 10.2 Web Management

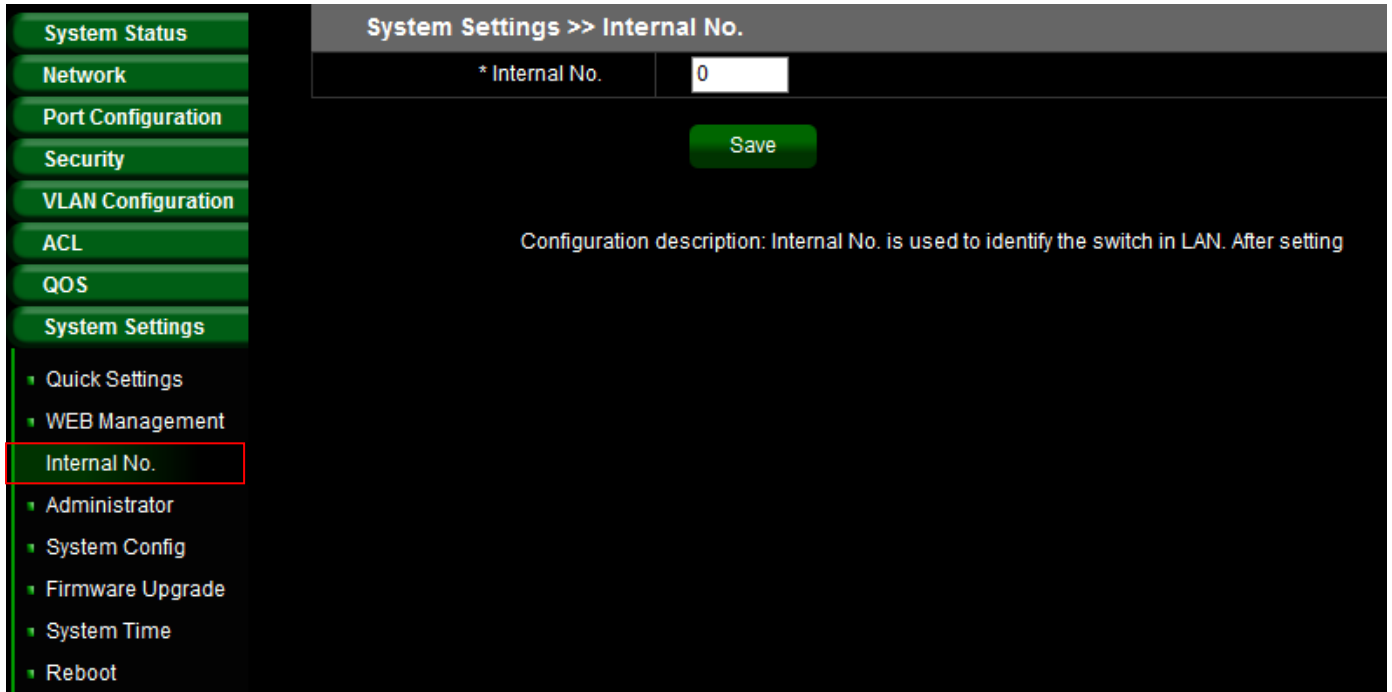
The page administrator can change login service and login timeout.

System Settings >> WEB management Settings	
Hostname	<input type="text" value="switch"/>
WEB Service Port	<input type="text" value="80"/>
WEB Timeout	<input type="text" value="30"/> minutes

- System Status
- Network
- Port Configuration
- Security
- VLAN Configuration
- ACL
- QOS
- System Settings
- Quick Settings
- WEB Management
- Internal No.
- Administrator
- System Config
- Firmware Upgrade
- System Time
- Reboot

### 10.3 Internal No.

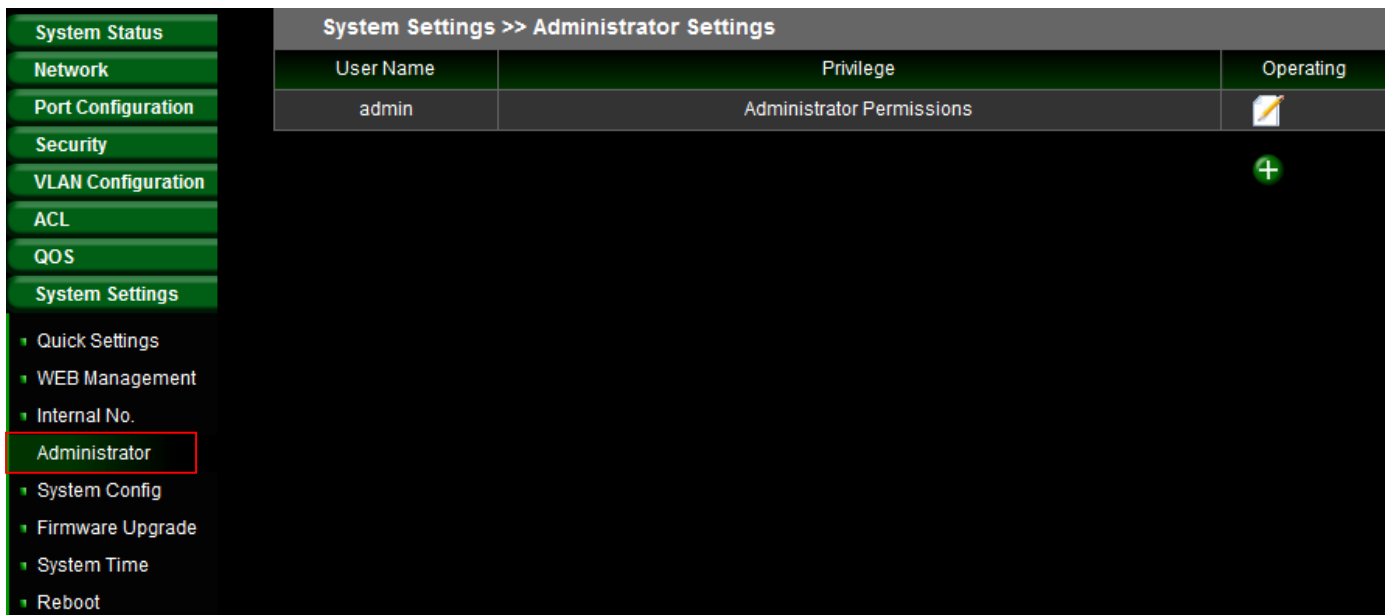
The feature is used to identify the switch in LAN. Administrator can set a number in switch.




The screenshot shows the 'System Settings >> Internal No.' configuration page. On the left is a navigation menu with 'Internal No.' highlighted. The main content area has a title bar 'System Settings >> Internal No.', a form field for '\* Internal No.' with the value '0', and a 'Save' button. Below the form is a configuration description: 'Configuration description: Internal No. is used to identify the switch in LAN. After setting'.

### 10.4 Administrator

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



The screenshot shows the 'System Settings >> Administrator Settings' configuration page. On the left is a navigation menu with 'Administrator' highlighted. The main content area has a title bar 'System Settings >> Administrator Settings' and a table with the following data:

User Name	Privilege	Operating
admin	Administrator Permissions	

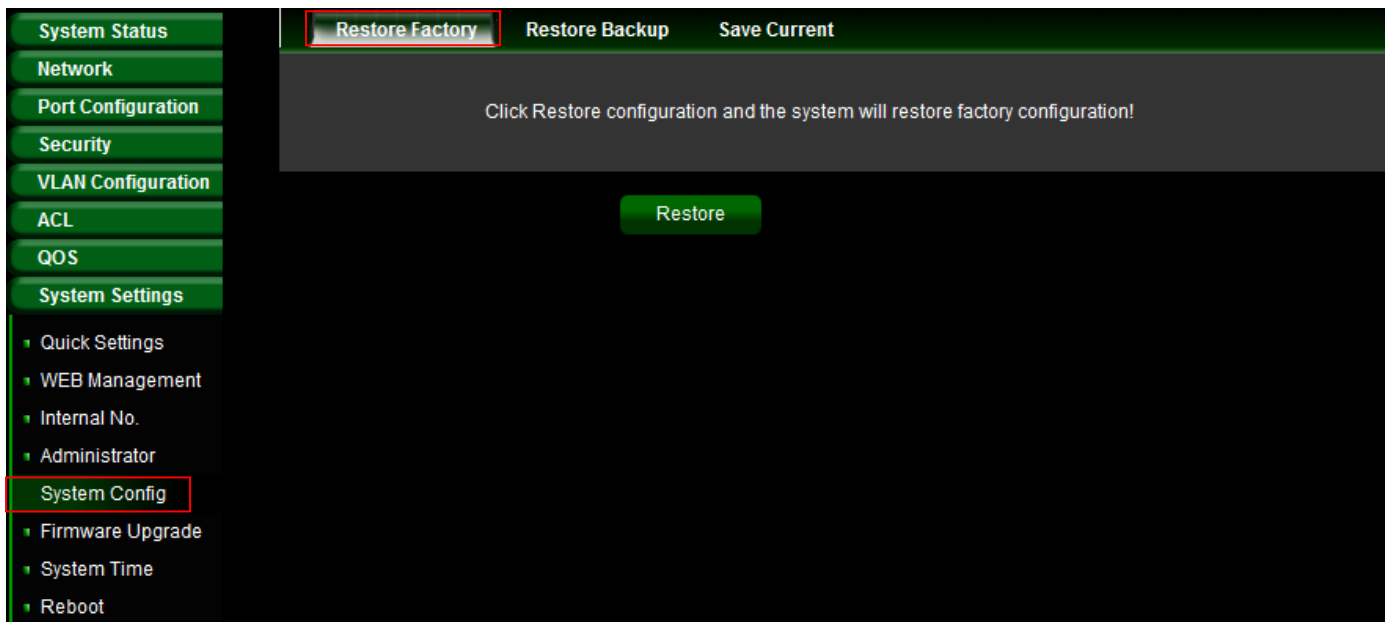
Below the table is a green plus sign icon.

## 10.5 System Config

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

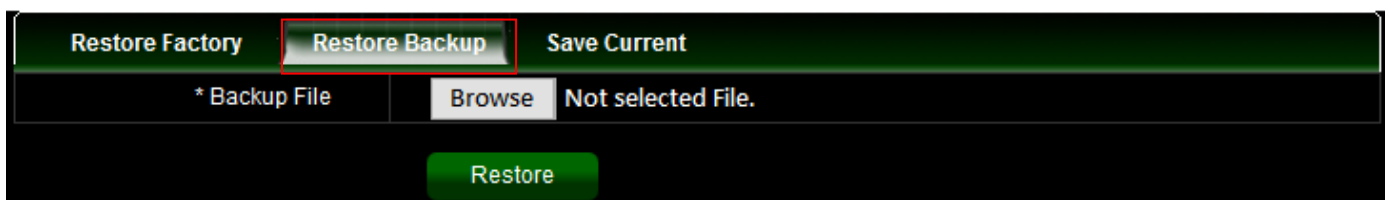
### Restore Factory:

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



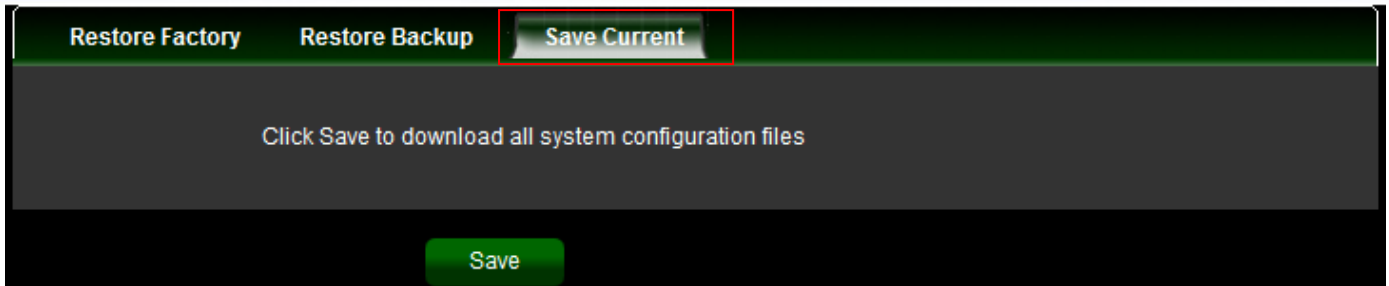
### Restore Backup:

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



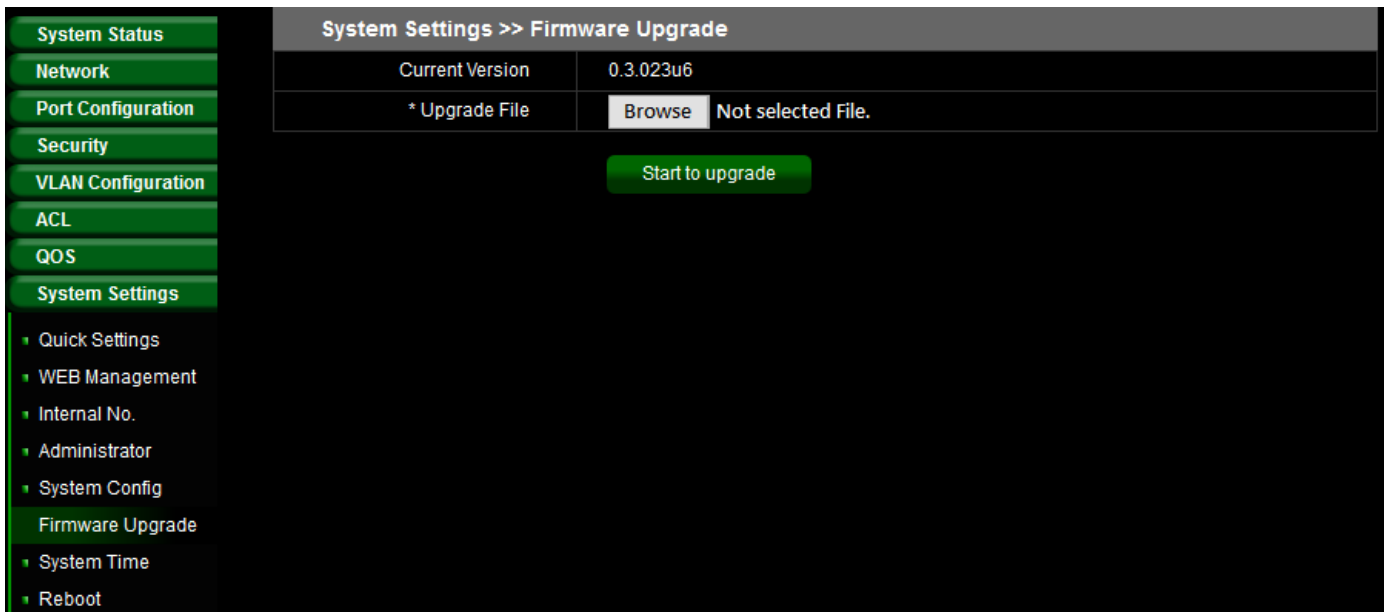
### Save Current:

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



## 10.6 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.



## 10.7 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.

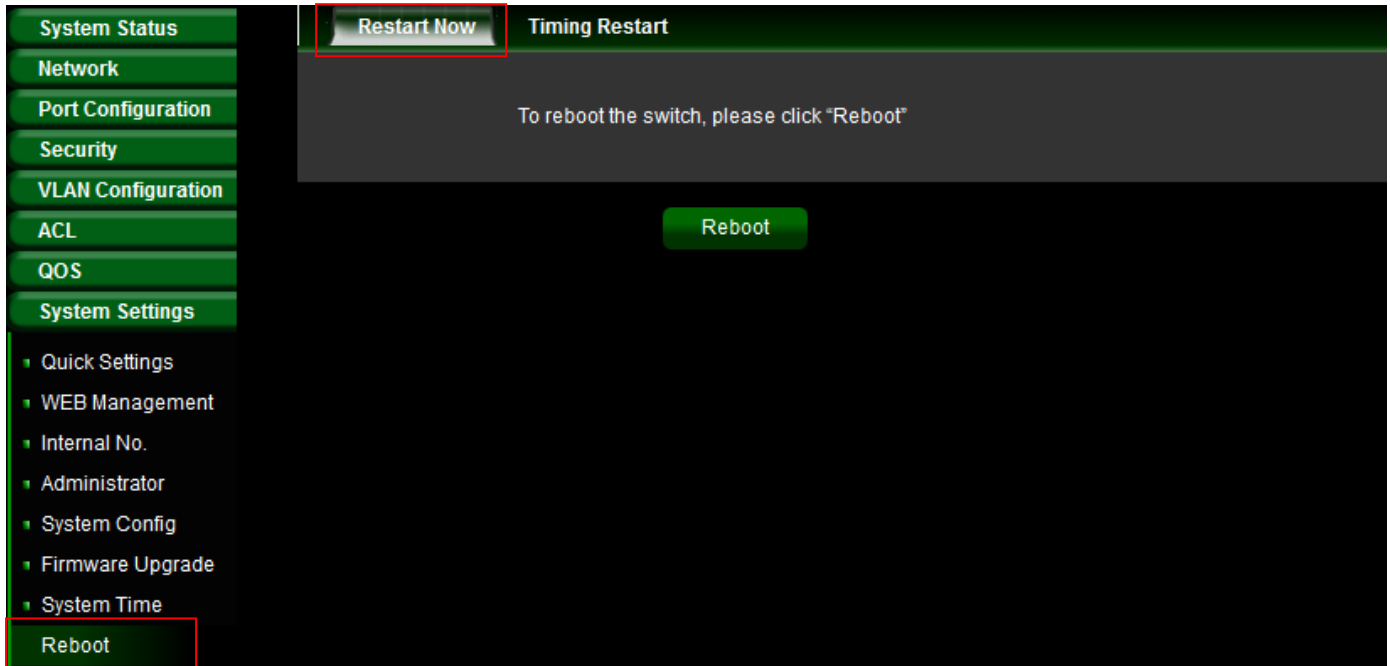
System Status	System Time	System Time Zone	Network Time
Network	Update Mode	<input type="radio"/> Synchronization Time <input checked="" type="radio"/> Manually Set	
Port Configuration	Computer Time	2016-06-20 14:49:56	
Security	System Time	2016-06-20 15:04:09	
VLAN Configuration	<input type="button" value="Synchronization"/>		
ACL			
QOS			
System Settings			
<ul style="list-style-type: none"> <li>▪ Quick Settings</li> <li>▪ WEB Management</li> <li>▪ Internal No.</li> <li>▪ Administrator</li> <li>▪ System Config</li> <li>▪ Firmware Upgrade</li> <li style="border: 1px solid red;">▪ System Time</li> <li>▪ Reboot</li> </ul>			

System Time	System Time Zone	Network Time																																										
Update Mode	<input type="radio"/> Synchronization Time <input checked="" 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; align-items: center;"> <span>2016</span> <span>JUN</span> </div> <table border="1" style="width: 100%; text-align: center; border-collapse: collapse;"> <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 style="background-color: #e0f0ff;">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; align-items: center; margin-top: 5px;"> <span>15</span> <span>:</span> <span>38</span> <span>:</span> <span>45</span> </div> <div style="display: flex; justify-content: center; margin-top: 5px;"> <input type="button" value="OK"/> <input type="button" value="Close"/> </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																																								

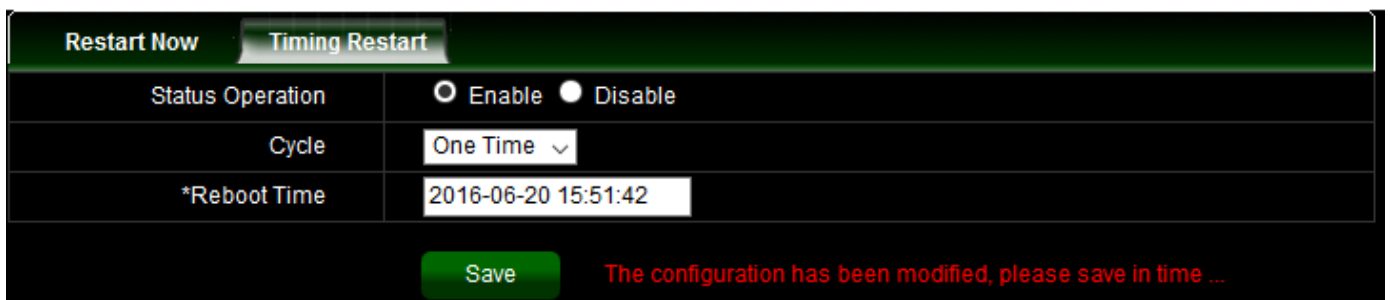
## 10.8 Reboot

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

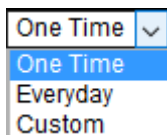
Click **Reboot** button to proceed and take around one minute to complete.



### 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.

# 11. System Log

## 11.1 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 Status
- Network
- Port Configuration
- Security
- VLAN Configuration
- ACL
- QOS
- System Settings
- System Log
- Event Log
- Alarm Log
- Security Log
- Network Log
- Protocol Log

System Log >> Event Log			
Time	Level	Message	
2016-06-20 16:09:41	Warning	HTTP:Administrator admin login from 192.168.2.22.Result:Accepted.	
2016-06-20 15:38:37	Warning	HTTP:Administrator admin login from 192.168.2.22.Result:Accepted.	
2016-06-20 14:52:58	Warning	HTTP:Administrator admin login from 192.168.2.22.Result:Accepted.	
2016-06-20 14:22:27	Warning	HTTP:Administrator admin login from 192.168.2.22.Result:Accepted.	
2016-06-20 13:32:10	Warning	HTTP:Administrator admin login from 192.168.2.22.Result:Accepted.	
2016-06-20 13:28:59	Warning	HTTP:Administrator admin login from 192.168.2.22.Result:Accepted.	
2016-06-15 17:48:16	Warning	HTTP:Administrator admin login from 192.168.2.20.Result:Accepted.	
2016-06-15 17:48:08	Warning	HTTP:Administrator admin login from 192.168.2.20.Result:Denied.	
2016-06-15 14:42:39	Warning	HTTP:Administrator admin login from 192.168.2.20.Result:Accepted.	
2016-06-14 14:43:16	Info	HTTP:The administrator admin at 192.168.2.20 updated 'Port-based VLAN' configuration.	
2016-06-14 14:15:27	Info	HTTP:The administrator admin at 192.168.2.20 updated 'Port-based VLAN' configuration.	
2016-06-14 14:15:16	Info	HTTP:The administrator admin at 192.168.2.20 updated 'Port-based VLAN' configuration.	
2016-06-14 14:15:00	Info	HTTP:The administrator admin at 192.168.2.20 updated 'Port-based VLAN' configuration.	
2016-06-14 14:14:48	Info	HTTP:The administrator admin at 192.168.2.20 updated 'Port-based VLAN' configuration.	
2016-06-14 14:14:35	Info	HTTP:The administrator admin at 192.168.2.20 updated 'Port-based VLAN' configuration.	

Level: All total 79 Page Size 15 Page No. 1/6 [First](#) | [Next](#) | [Prev](#) | [Last](#) Goto 1

Refresh
Clear
Export

## 11.2 Alarm Log

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

System Log >> Alarm Log		
Time	Level	Message
2016-06-20 15:38:30	Notice	Port 2 connected. Mode: 1000Mbps Full-duplex.
2016-06-20 15:21:54	Notice	Port 2 disconnected.
2016-06-20 14:22:17	Notice	Port 2 connected. Mode: 1000Mbps Full-duplex.
2016-06-20 13:55:28	Notice	Port 2 disconnected.
2016-06-20 13:27:20	Notice	Port 2 connected. Mode: 1000Mbps Full-duplex.
2016-06-20 09:15:29	Notice	Port 12 connected. Mode: 1000Mbps Full-duplex.
2016-06-17 08:56:27	Notice	Port 12 connected. Mode: 1000Mbps Full-duplex.
2016-06-16 15:52:22	Notice	Port 2 disconnected.
2016-06-16 15:50:50	Notice	Port 2 connected. Mode: 100Mbps Full-duplex.
2016-06-16 15:50:49	Notice	Port 2 disconnected.
2016-06-16 15:50:41	Notice	Port 2 connected. Mode: 100Mbps Full-duplex.
2016-06-16 15:50:40	Notice	Port 2 disconnected.

## 11.3 Security Log

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

System Log >> Security Log		
Time	Level	Message
Level: <input type="text" value="All"/> total 0 Page Size: <input type="text" value="15"/> Page No. 1 / 1 First   Next   Prev   Last Goto <input type="text" value="1"/>		
<input type="button" value="Refresh"/> <input type="button" value="Clear"/> <input type="button" value="Export"/>		



## 11.4 Network Log

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

The screenshot shows the 'System Log >> Network Log' page. On the left is a navigation menu with 'System Log' expanded to show 'Network Log' selected. The main content area has a table header with columns 'Time', 'Level', and 'Message'. Below the header, 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'. There are also 'Goto 1' and buttons for 'Refresh', 'Clear', and 'Export'.

## 11.5 Protocol Log

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

The screenshot shows the 'System Log >> Protocol Log' page. On the left is a navigation menu with 'System Log' expanded to show 'Protocol Log' selected. The main content area has a table header with columns 'Time', 'Level', and 'Message'. Below the header, 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'. There are also 'Goto 1' and buttons for 'Refresh', 'Clear', and 'Export'.

## Specifications

### Standards & Hardware Specifications

	IEEE 802.3 10Base-T
	IEEE 802.3u 100Base-TX,
	IEEE 802.3ab 1000Base-T,
	IEEE 802.3z 1000Base-SX/LX
<b>Standards Conformance</b>	IEE 802.3x Flow Control
	IEEE 802.1p QoS
	IEEE 802.3az EEE
	IEEE 802.1Q VLAN Tag
	IEEE 802.3ad Link Aggregation
<b>Port Configuration</b>	24 ports RJ-45 connectors for 10/100/1000 BASE-TX
	4 SFP Gigabit uplink ports
<b>Media Access Protocol</b>	CSMA / CD
<b>Network Media</b>	10BASE -T: UTP Cat. 3 or up,
	100BASE-TX: UTP Cat. 5 or up,
	1000BASE-T: UTP Cat. 5 or up
<b>Transmission Method</b>	Store and Forward
<b>MAC Address Table</b>	8K
<b>Built-in Buffer</b>	4Mb
<b>Data Transfer Rate</b>	10/100Mbps (Half-duplex), 20/200Mbps (Full-duplex)
	1000Mbps ( Half-duplex), 2000Mbps (Full-Duplex)
<b>Jumbo Frames</b>	9k Jumbo Frames Support
<b>Auto MDI/MDIX</b>	Yes
	Per Port:(Link / ACT): Status*24,
<b>LED Indicators</b>	Per Unit: Power*1,
	Per Unit: System*1,
	Per Unit: SFP Port Status*4
<b>Internal Bus Speed</b>	56Gbps
<b>Switch Specifications</b>	
<b>Link Aggregation</b>	IEEE802.3ad LACP Link Aggregation Supported
<b>Port Mirroring</b>	Supported

<b>Quality of Service (QoS)</b>	Supports IEEE 802.1p QoS, Port-based QoS
<b>Bandwidth Control</b>	Supported
<b>Spanning</b>	Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP)
<b>IGMP Snooping</b>	v1, v2, v3
<b>MAC Filtering</b>	Supported
<b>DHCP Snooping</b>	Supported
<b>VLAN</b>	IEEE802.1Q Tagging VLAN , Port-Based ,Tag based VLAN
<b>SNMP</b>	Supports SNMP v1/v2c

### **Environmental & Mechanical Characteristics**

<b>Power Consumption</b>	18Watt
<b>Power Type</b>	Power cord: Internal Power supply
<b>Power Requirement</b>	AC 100~240VAC, 50-60Hz Auto-sensing
<b>Operating Temperature</b>	0° to 50° C
<b>Storage Temperature</b>	-40° to 70° C
<b>Operating Humidity</b>	10% to 90% non-condensing
<b>Storage Humidity</b>	10% to 90% non-condensing
<b>Dimension ( W x D x H )</b>	441 x 200 x 44 mm
<b>Weight</b>	2.45Kg
<b>Certification</b>	FCC, CE, RoHS-compliant