Network Switch Software Manual

Web User Interface

Table of Contents

Chapter 1 Introduction to the Manual

This manual details the configuration method of the functions of the switch software. Please read this manual carefully before the operation。

1.1. Target readers

The target readers of this manual are those who understand or use the functions of this Web light network management software.

1.2. Manual agreement

Show the Web interface and software functions.

Use- -> symbols to express the entry order of the menu, the first-level function menu- -> two-level function menu- -> three-level function menu, among which, some functions have no two-level and three-level function menu.

The <> sharp brackets that appear in the text indicate the button name, such as <app>, <app ply>.

Special icons used in this manual are described as follows:

Explain	Description of the operation content, make the necessary supplement and explanation.
⚠ Notice	Remind the precautions in the operation, improper operation may lead to data loss or equipment damage.

Chapter 2 Introduction to Web light network management functions

2.1. Functional profile

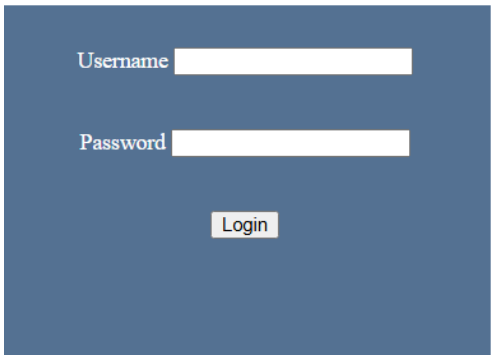
Our newly developed Web light network management switch function software, support a variety of models. Provide VLAN, QoS, RSTP, SNMP, POE control, link aggregation and other functions.

Home page	Support Logo, interface panel, system information display
System	IP address setting, port settings, and user account
POE	POE power port control
Configure	VLAN
	QOS
	IGMP
	Link aggregation
	Ring road protection
	RSTP
	Port mirror image
	Port isolation
	bandwidth control
	Giant frame
	MAC restrain
	Green Ethernet
	EEE
	SNNP
Security	MAC address
	broadcast storm
Monitor	Port statistics
Tools	Firmware upgrade
	Configure backup
	Feset
	Save
	Reboot

Chapter 3 Log in to the web interface

3.1. Login

1. The switch has been started normally, and any port has been connected to the management PC.
2. Management PC has installed at least one of the following browser: IE 8.0 or above, the latest version of Chrome, 360 browser.
3. The IP address of the management PC has been set to the same network segment as the switch port, namely 192.168.1.X (any integer from 2 to 254), and the subnet mask is 255.255.255.0.
4. In order to ensure a better experience of the display effect of the Web interface, it is recommended to adjust the resolution of the display to 1,2,80,800 or more pixels.
5. Open the browser and enter the switch default management address in the address bar http: / / 192.168.1.200 in the switch Web management interface.
6. The switch login page is shown in the figure below. Enter the user name and password of the switch management account, and the factory default value is admin



Left navigation bar, this is the neutral software. The Logo is not shown. The upper right is the model interface panel. The lower right is the basic information of the system.

Chapter 4 System

4.1. System information

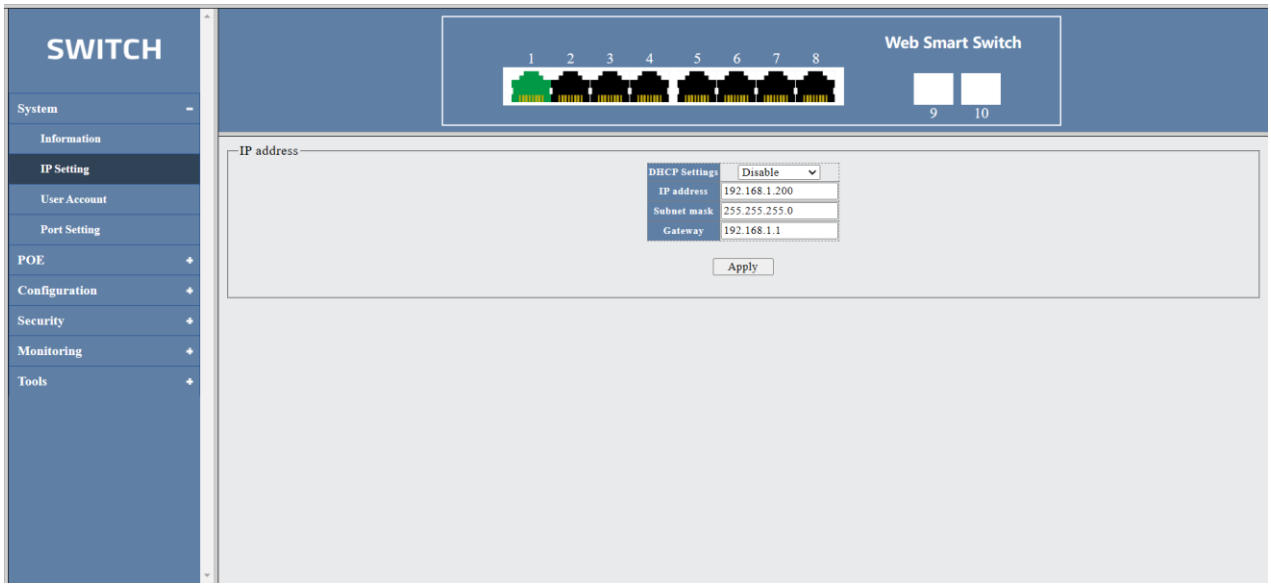
You can view the device system information and set the device model. In the navigation bar, click: System- -> System Information

explain:

Device model	Display device model
MAC address	Displays the M and the C address of the device
IP address	Displays the Device Management TP address
subnet mask	Displays the device subnet mask
gateway	Displays the device's default gateway
Key version	Displays the software version
Firmware date	Displays the software version date
Hardware version	Displays the device hardware version

4.2. IP setting

Each device in the network has an IP address through which you can login the management interface. Click on the navigation bar: System- -> IP Settings



explain:

DHCP setting Select the DHCP feature on or off.

Disable: IP address, subnet mask and default gateway manually.

Enable: Select Enable, Exchange opportunities gets network parameters from the DHCP server.

IP Address sets the IP address of the device. The Subnet mask sets the subnet mask of the device.

Default gateway sets the default gateway address of the device.

Click <Apply> System management IP, subnet mask, and gateway will be modified to the set point。

4.3. User Account

You can modify the user name and password used during login. Click on the navigation bar: System- -> User account

explain:

User name sets the user name of the login switch. The user name cannot be longer than 16 characters and can only use numbers, English letters and underscores.

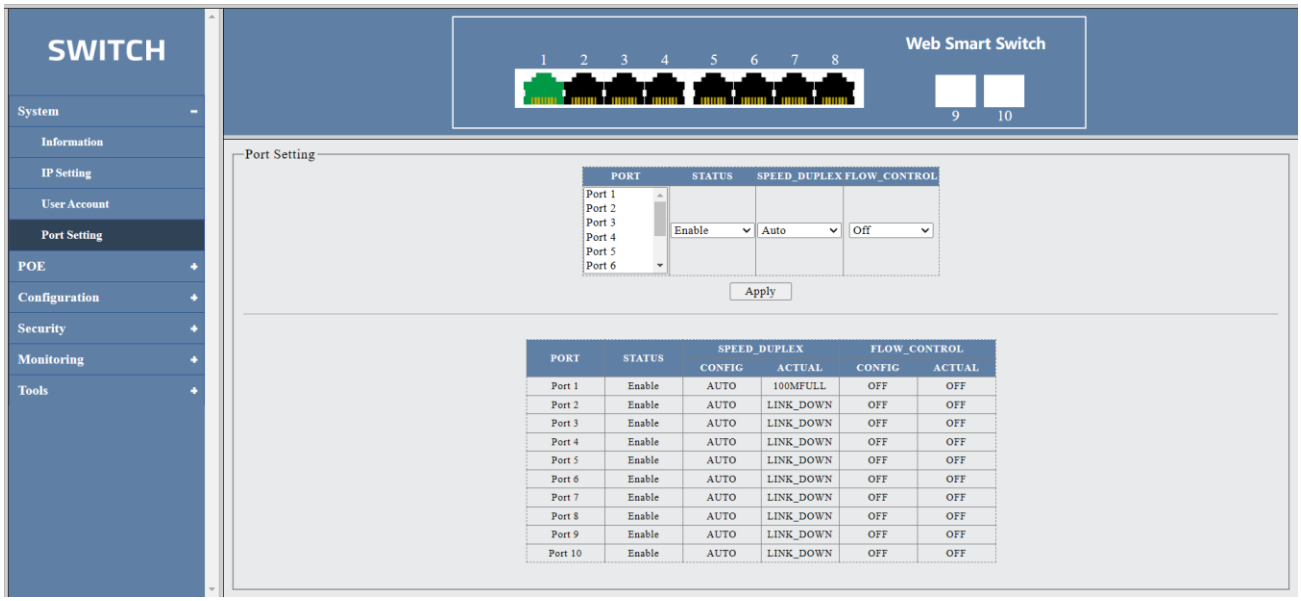
The new password will reset the password for the login switch. The new password cannot be longer than 16 characters and can only use numbers, English letters and underscores.

Consure the password is the same.

Note: Please refresh the page again after changing the password.

4.4. Port Setting

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



explain:

The Name sets the port alias.

The port is open and closed. If the port is opened, the port can forward messages normally.

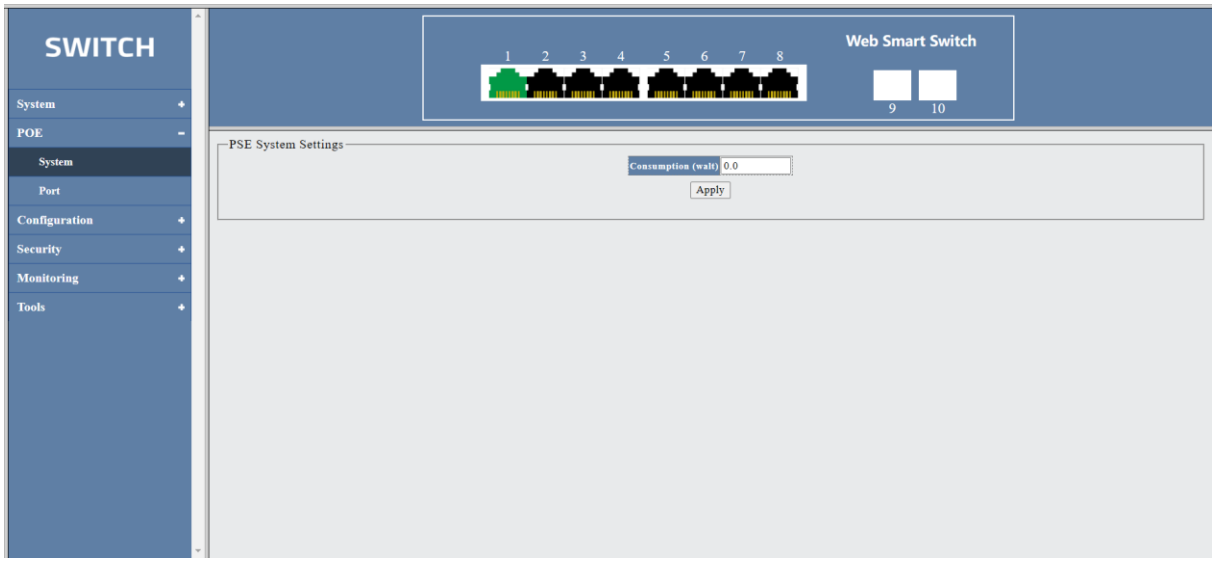
Speed / duplex is optional 10M / Half, 10M / Full, 100M / Half, 100M / Full, automatic. When the mode selection is automatic, the rate and the duplex will be determined by negotiation

Stream control function, open and close, open the flow control function, can control and adjust the forwarding rate of each port packet to avoid congestion. After changing the Settings, click the port setting to refresh the display status. Note: the flow control function will actually be opened in semi-duplex mode

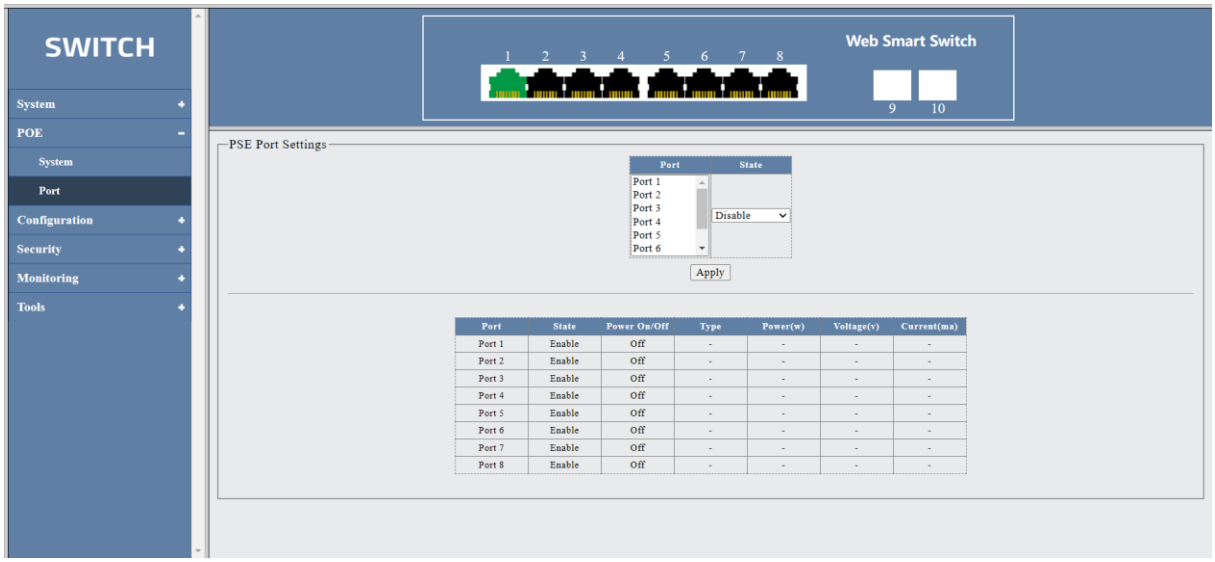
Chapter 5 POE

5.1. POE

Displays the total power consumed by the POE port. Click on the navigation bar: the POE- -> system



You can set the PSE port status here (only for devices that support POE power supply function) and click on the navigation bar: POE- -> port



explain:

Ports can select multiple ports

The state can supply power normally in the open state.

Power supply on / off displays the current working status

Power display port output power

The voltage displays the PSE port supply voltage

Current shows the PSE port supply current

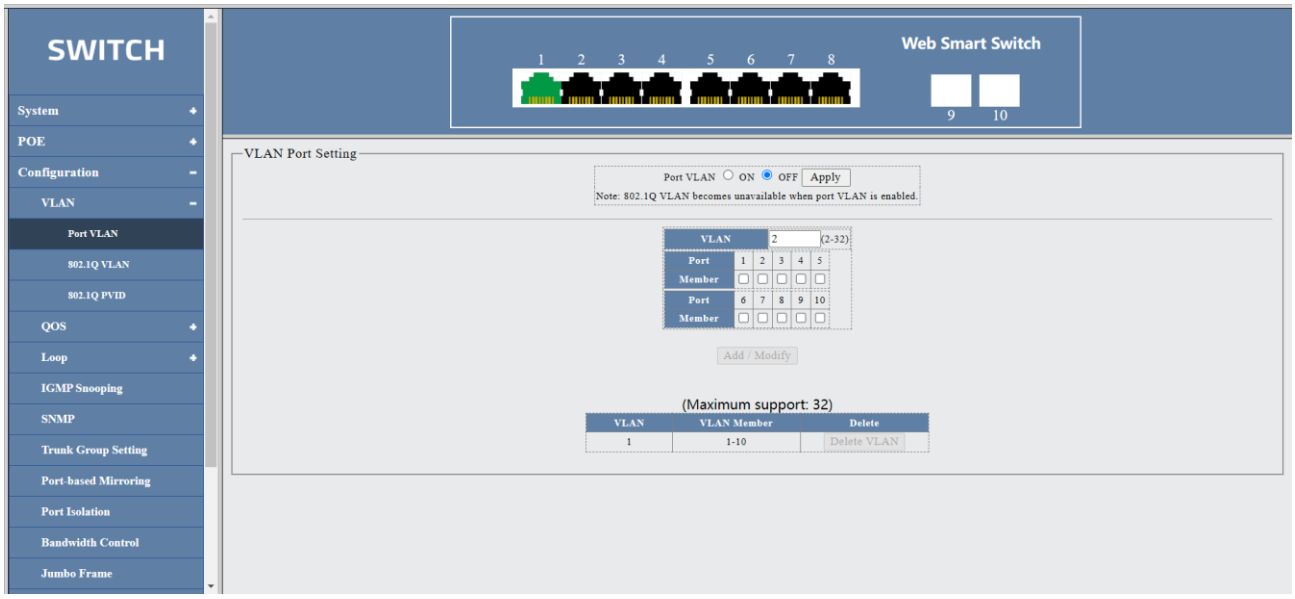
Chapter 6 Configuration

6.1. VLAN

6.1.1. Port VLAN

VLAN (Virtual Local Area Network, virtual LAN) is a communication technology that logically divides a physical LAN into multiple broadcast fields. By defining the extended fields on the LAN data frame, this technology divides the physical network logically, so as to limit the forwarding range of the LAN data frame and narrow the broadcast domain. VLAN technology is mainly used in network equipment such as switches, routers and switches.

Click on the navigation bar: Configure- -> Port VLAN



The VLAN is distinguished by the VLAN ID, and all the Untagged packets reaching the port are labeled with the Tag of the port PVID.

explain:

Need to set the VLAN ID before setting the port VID

The static VLAN set VLAN ID, range 1-4094.

If the Untagged port is Untagged port, the output data frame without tag information. If the Tagged port is the Tagged port, the output data frame with tag information.

When no member port is selected, that port is not a member port of the VLAN.

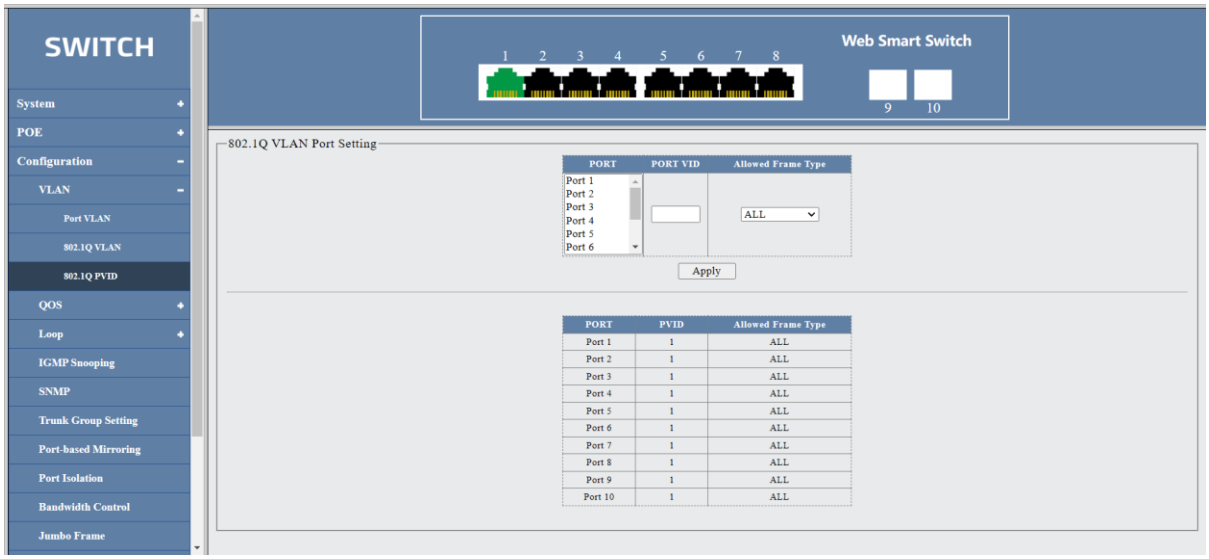
Note: Before deleting the VLAN, set the VID of the VLAN to be 1 before deleting the VLAN.

6.1.2. 802.1Q VLAN

Click on the navigation bar: Configure- -> 502.1Q VLAN

6.1.3. 802.1Q VID

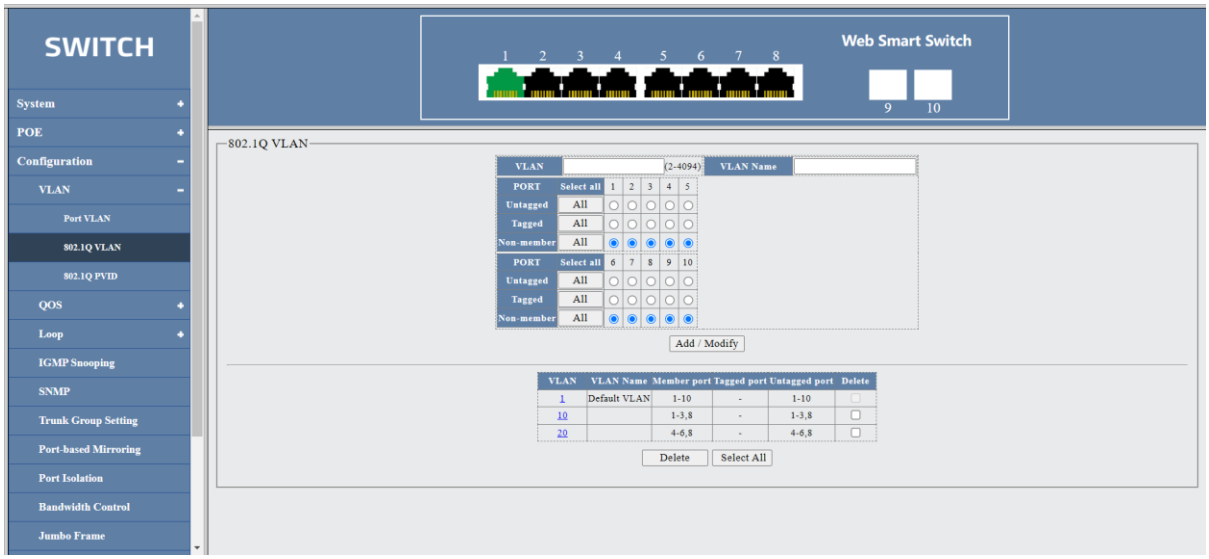
Click on the navigation bar: Configure- -> 802.1Q VID



6.1.4. Examples

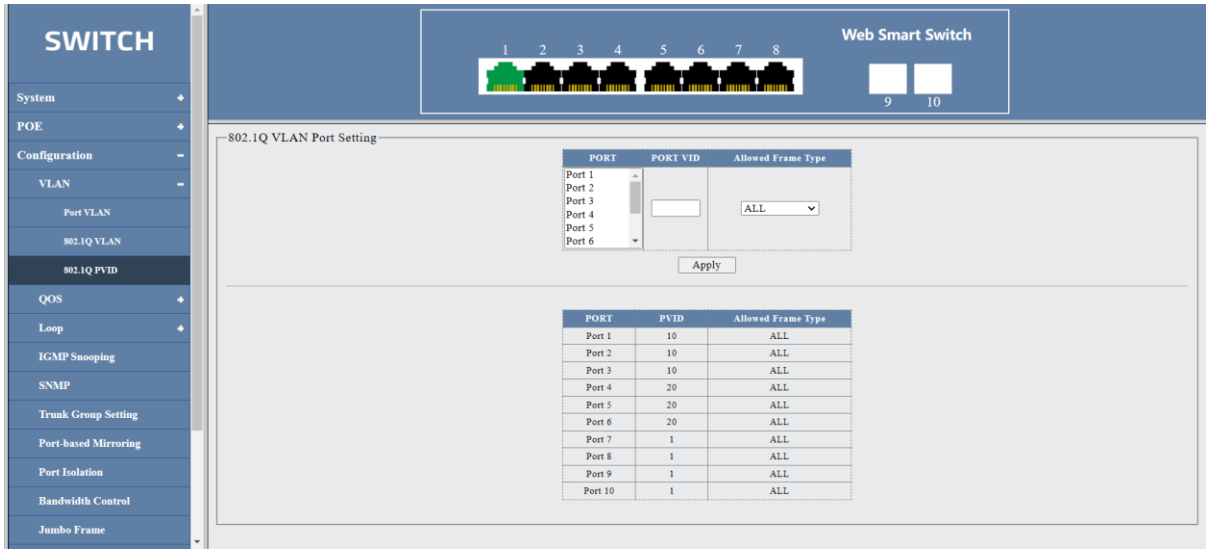
Click on the navigation bar: Configure- -> 502.1Q VLAN

Set switches 1,2,3, and port set bit VLAN10,4,5, and 6, Port 8 add VLAN10 and VLAN20 as upper ports, respectively. Also the VLAN1 contains all of the ports. So that the VLAN10, VLAN20 port packets can be forwarded to port 8. As shown in the figure below



After setting the VLAN table, you also need to set the port VID. Click on the navigation bar: Configure- -> 502.1Q VID

Set port VID of ports 1,2,3, to 10, port 4,5,6,7, to 20, and VID of port 8 to default 1. This way, the 8-port data can be forwarded to all the ports. The results are shown in the following figures



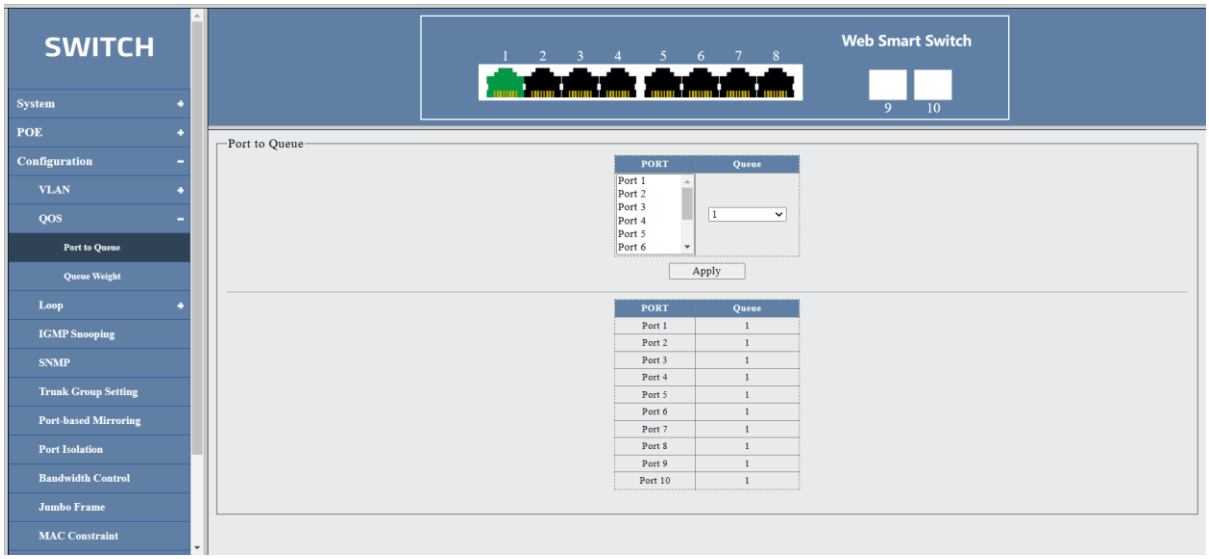
6.2. QoS

The QoS (Quality of Service) function is used to optimize the network performance and provide a better network service experience. The switch is based on the port, 802.1P, and DSCP priority mode.

6.2.4. Port to queue

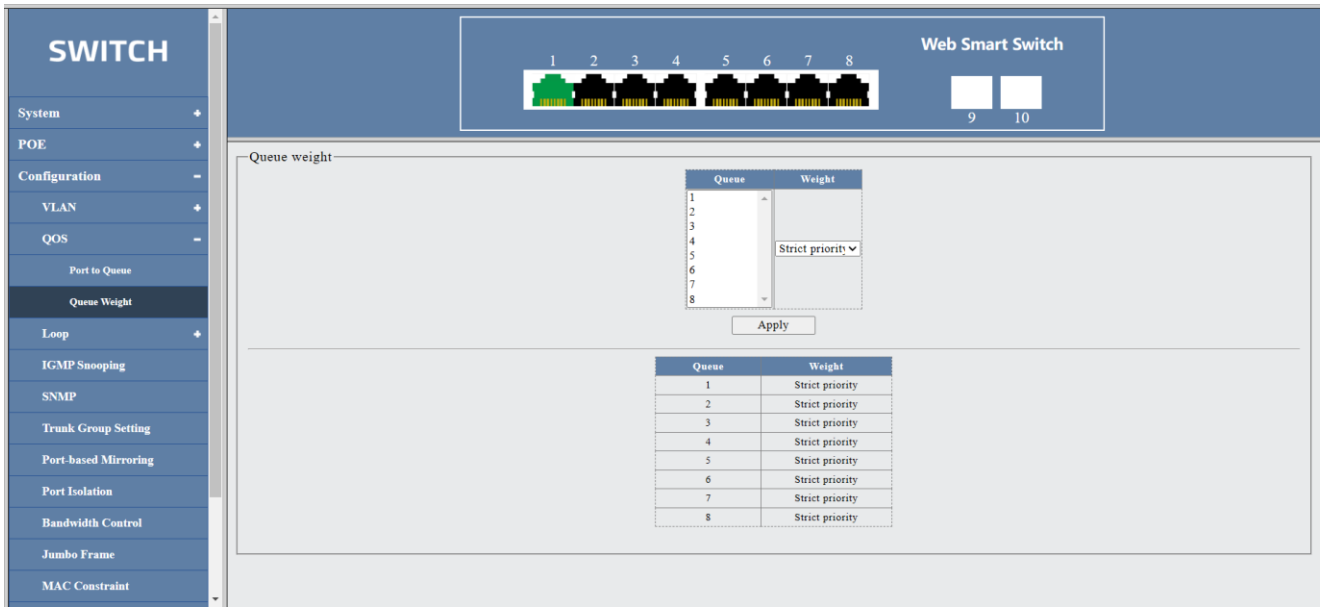
These packages are mapped to 8 different queues based on the entry ports.

Click on the navigation bar: Configure- -> QOS- -> Port to the queue



6.2.5. Queue weight

Set the queue weights so that different queues get different scheduling priorities. Click on the navigation bar: Configure- -> QOS- -> Queue Weight

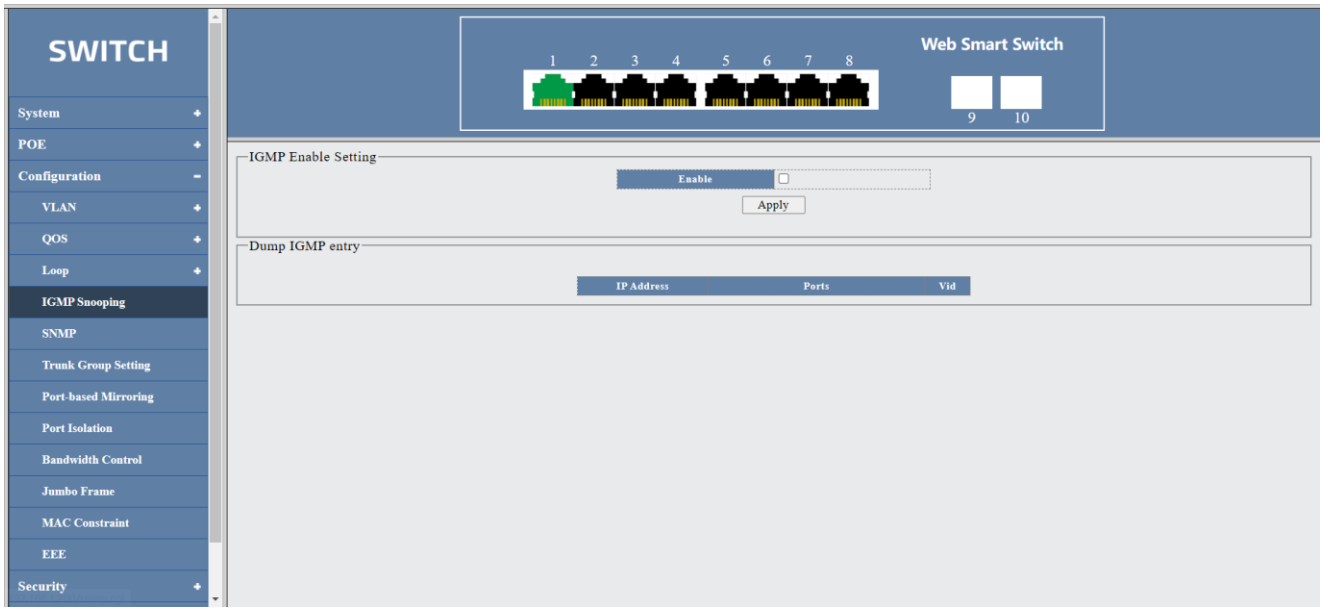


6.3. IGMP intercept

IGMP (Internet Group Management Protocol Snooping) is a multicast constraint mechanism running on second II devices used to manage and control multicast groups. Add the switch port to the group by configuring the multicast VLAN

Broadcast VLAN makes users in different VLAN share one multicast VLAN receive multicast data, and the multicast stream is only transmitted within one multicast VLAN, thus saving bandwidth. And because of the multicast VLAN with the users. The VLAN is completely isolated, with both security and bandwidth guaranteed.

Click on the navigation bar: Configure- -> IGMP Listen



explain:

IGMP, enabling settings to select to enable or disable IGMP listening.

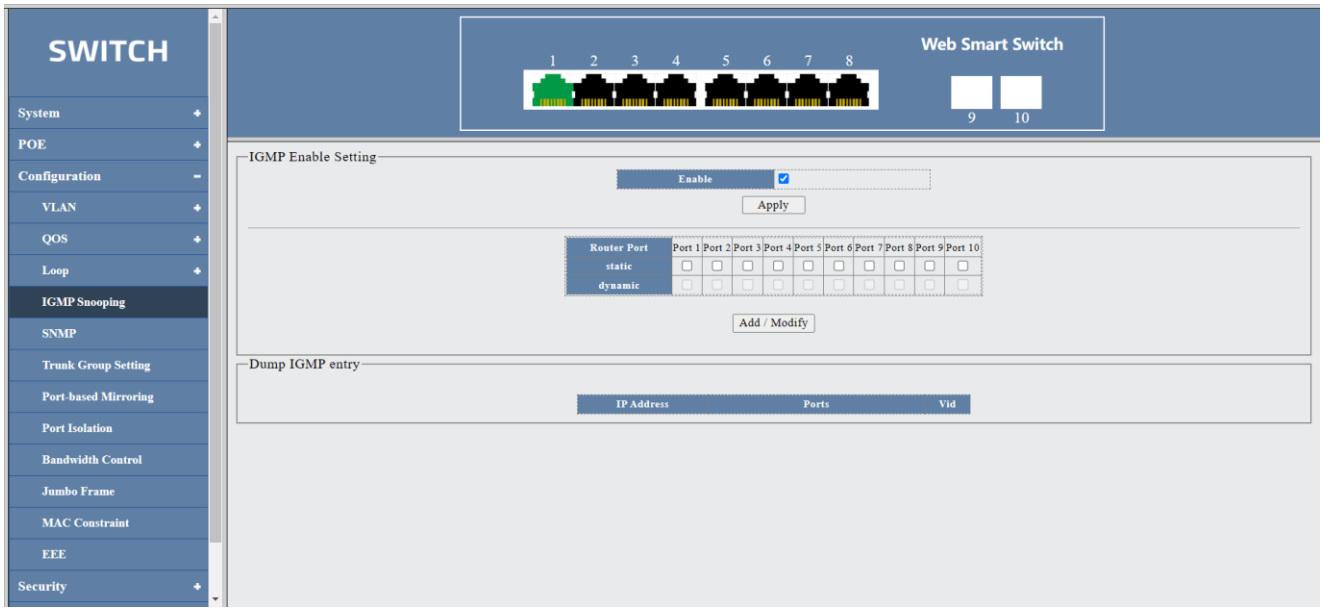
IP address View the multicast IP address

Port View the list of multicast group ports

VID view the multicast group corresponding to VLAN ID

6.3.1. Examples

Check, and then click the app to open the IGMP listening function



explain:

IP address

multicast IP

Port multicast

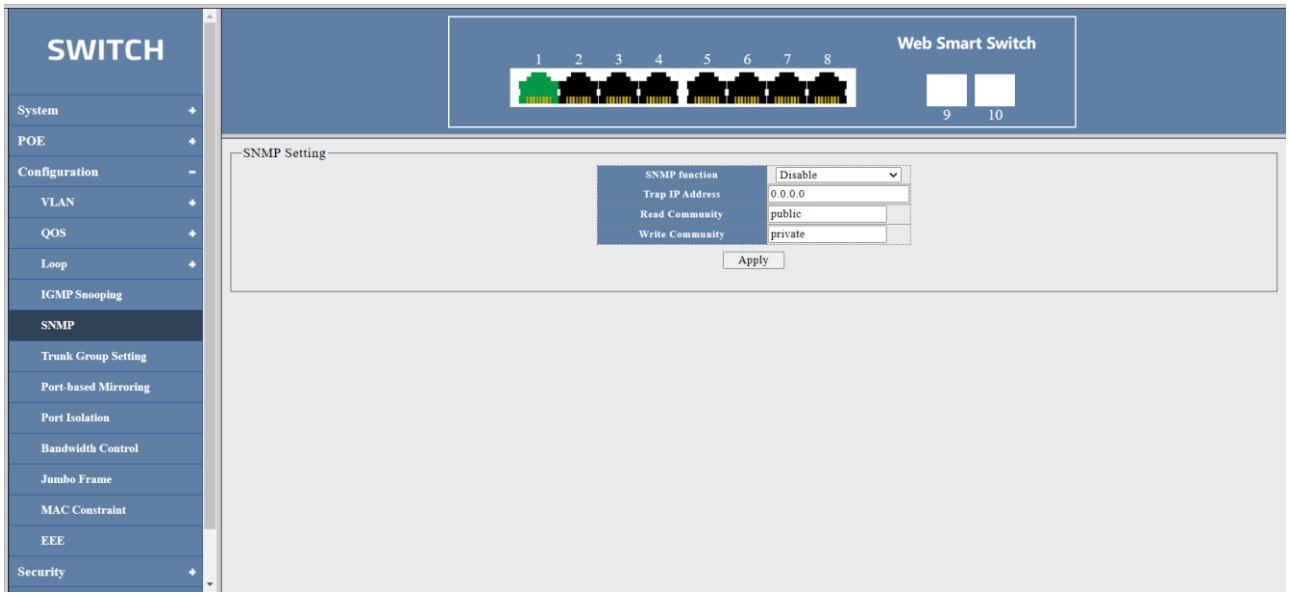
port

VID VLAN ID

6.14.SNMP

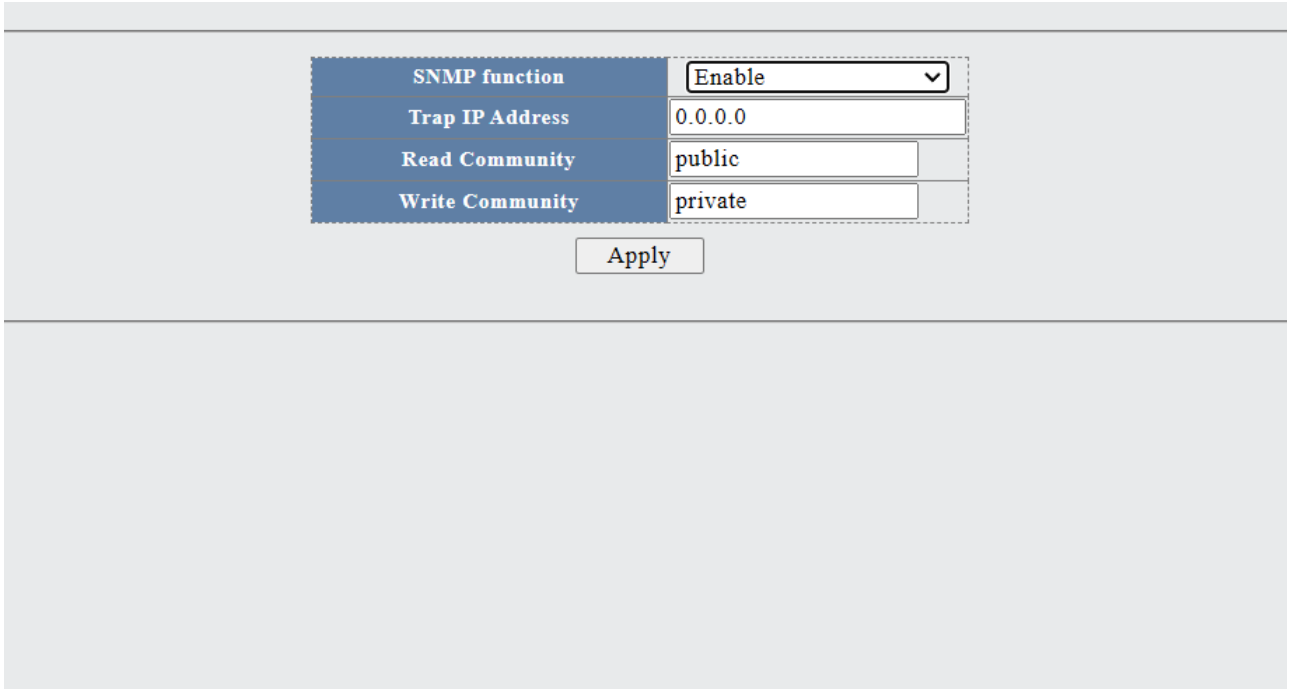
SNMP is the standard network management protocol widely used in TCP / IP networks. This protocol can support the network management system to monitor for any devices connected to the network to attract management attention. The basic components of SNMP include network management system NMS (Network Management System), agent process (Agent), managed object (Managed Object) and management information database MIB (Management Information Base)

Click on the navigation bar: Configure- -> SNMP

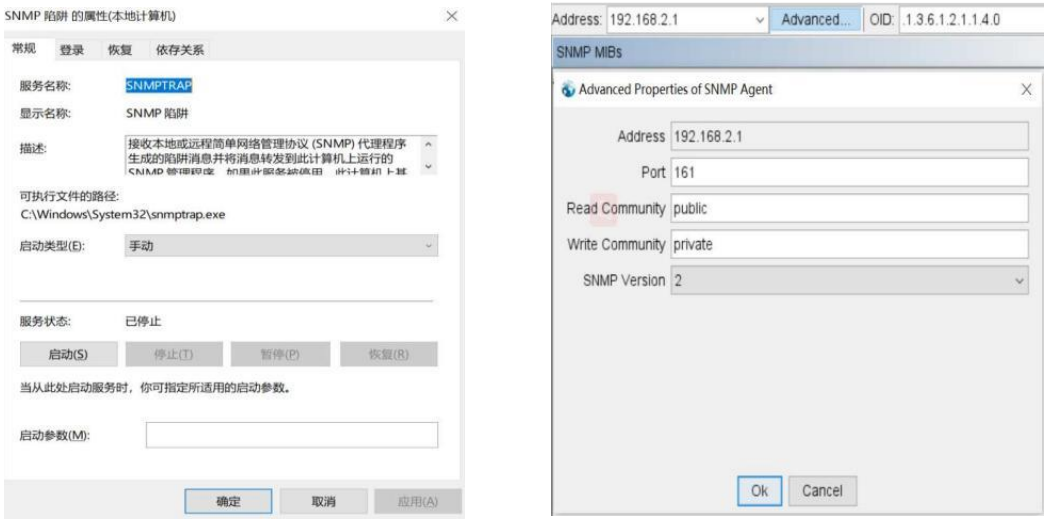


6.14.1. Examples

1. Turn on the SNMP function

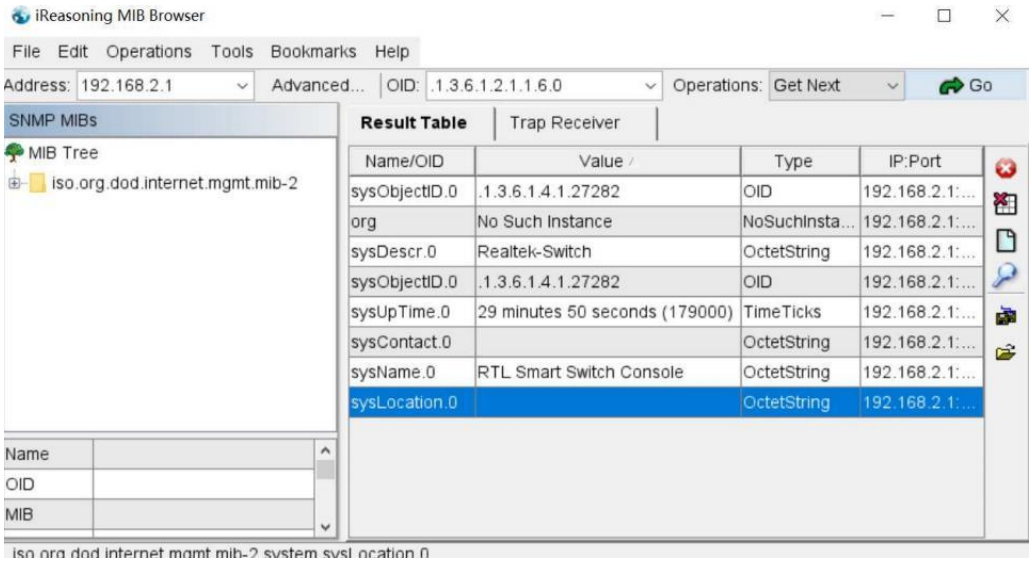


2. Turn off the SNMP service of the 162 port

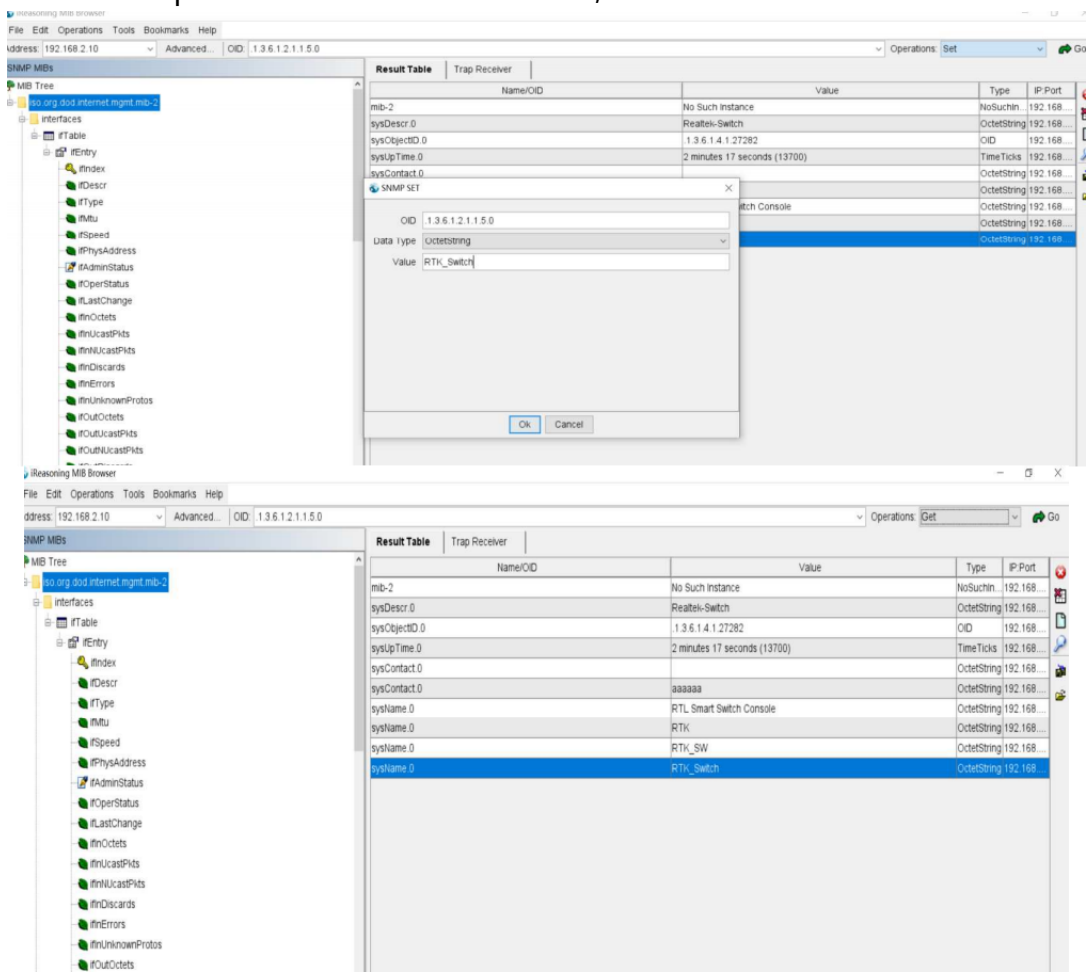


Close the management host SNMP service and the MID Browser settings

3. Open the IReasoning MIB Browser software setting as shown in the right figure above.
4. Click Get Next-> GO in MIB Browser to show the results shown in the following below

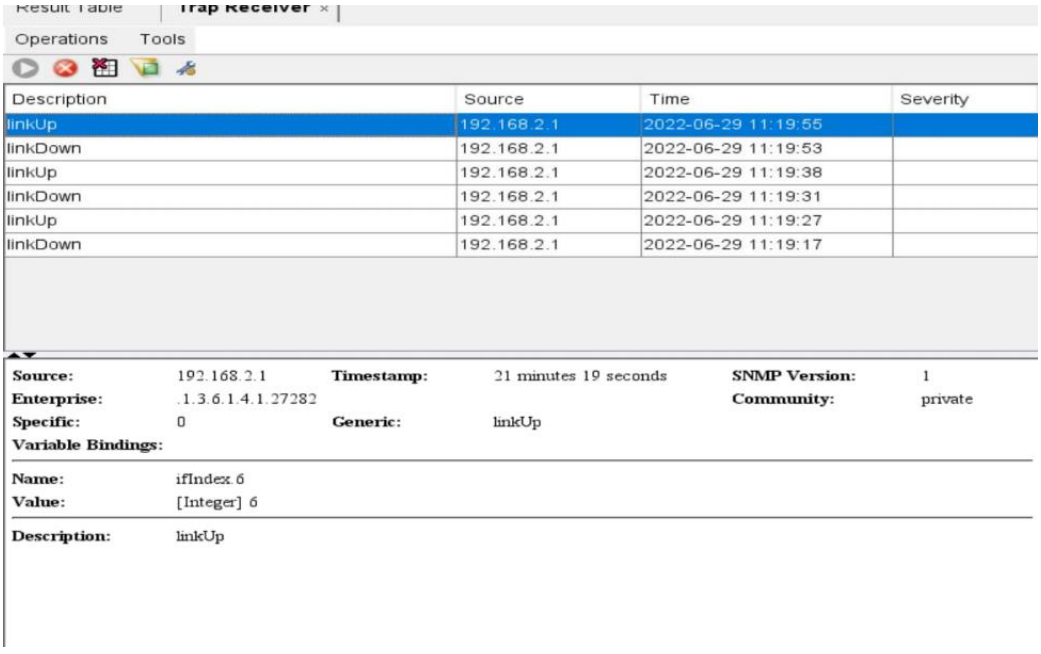


5. After MIB Browser Operations selection of set-> GO, the Get results are shown as follows.



SNMP Trap Set

6. Set the IP address of the management PC to the Trap IP address of the switch configuration, and receive the switch port status change information in the MIB Browser Tools selection Trap Receiver

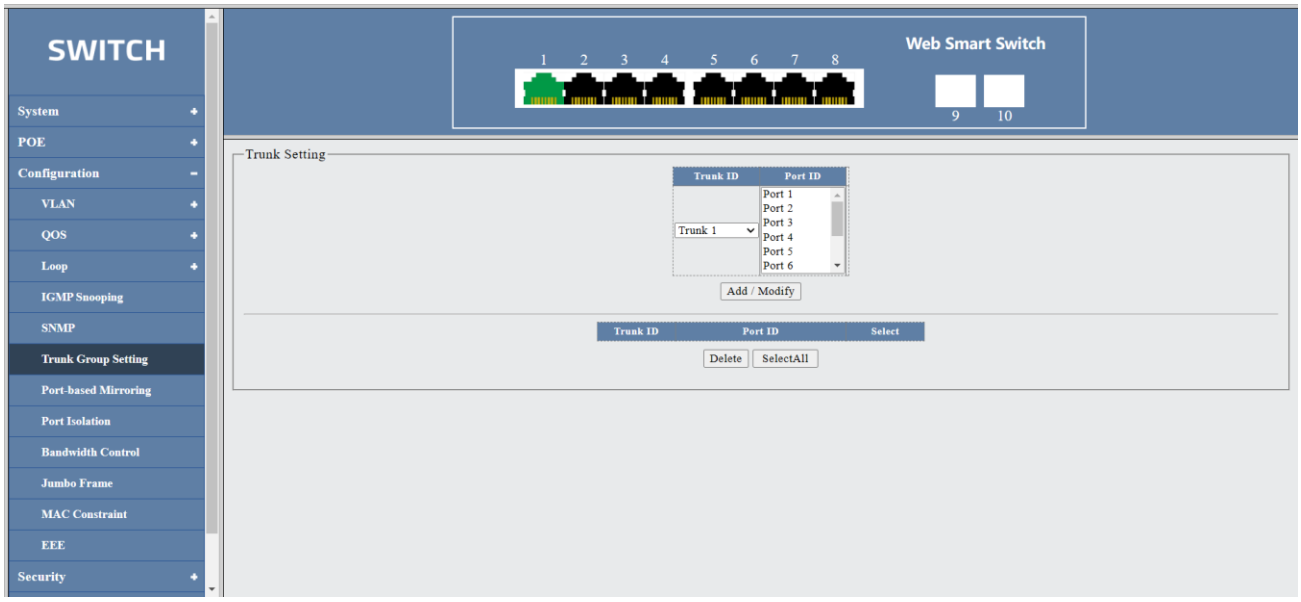


Trap Receiver

6.4. Link aggregation

Link convergence is a way to bundle a set of physical interfaces together as a logical interface to increase bandwidth and reliability. The port configuration is convergence. With the following requirements, it can be achieved by configuration link aggregation: when the reliability of the connection between two switch devices through one link does not meet the requirements.

Click on the navigation bar: Configure- -> trunk group setting



For example, add 1-4 ports to aggregate group 1, and 5-8 ports to aggregate group 2

Explain:

Group ID converges on the group ID.

The ports belong to the physical port of the aggregation group

Member ports that belong to the same cluster group must have a consistent configuration.

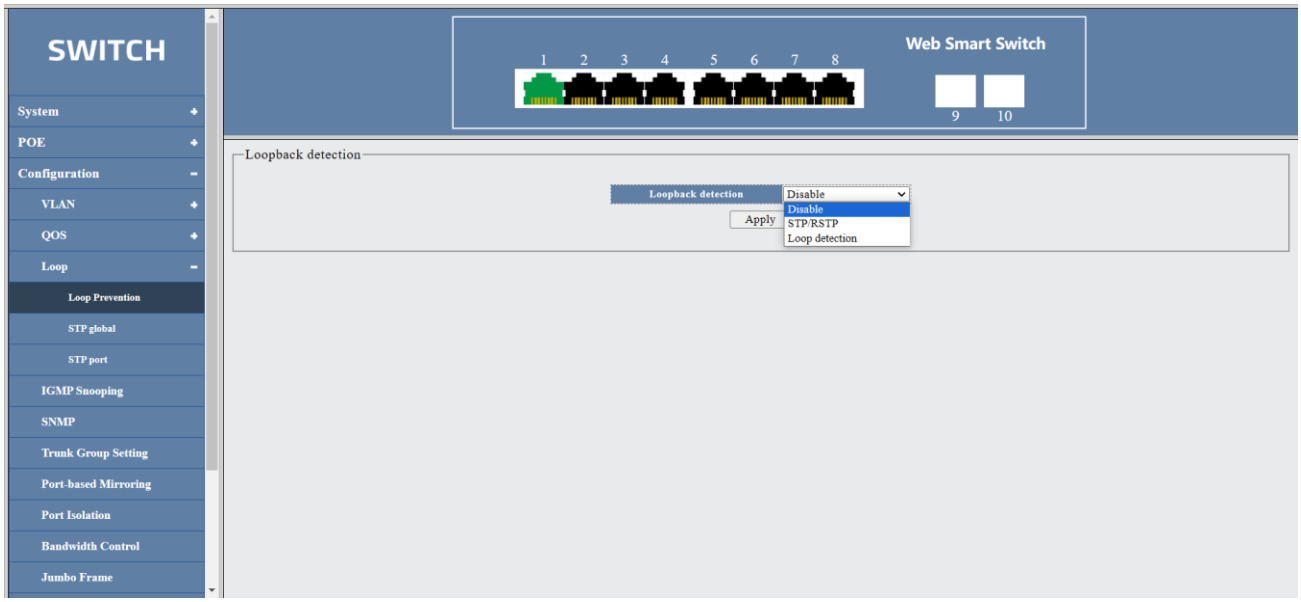
Note: trunk 1 supports 1~4 ports, trunk 2 supports 5~8 ports, and trunk3 (10 port switch) supports 9~10 ports

6.5. Ring road agreement

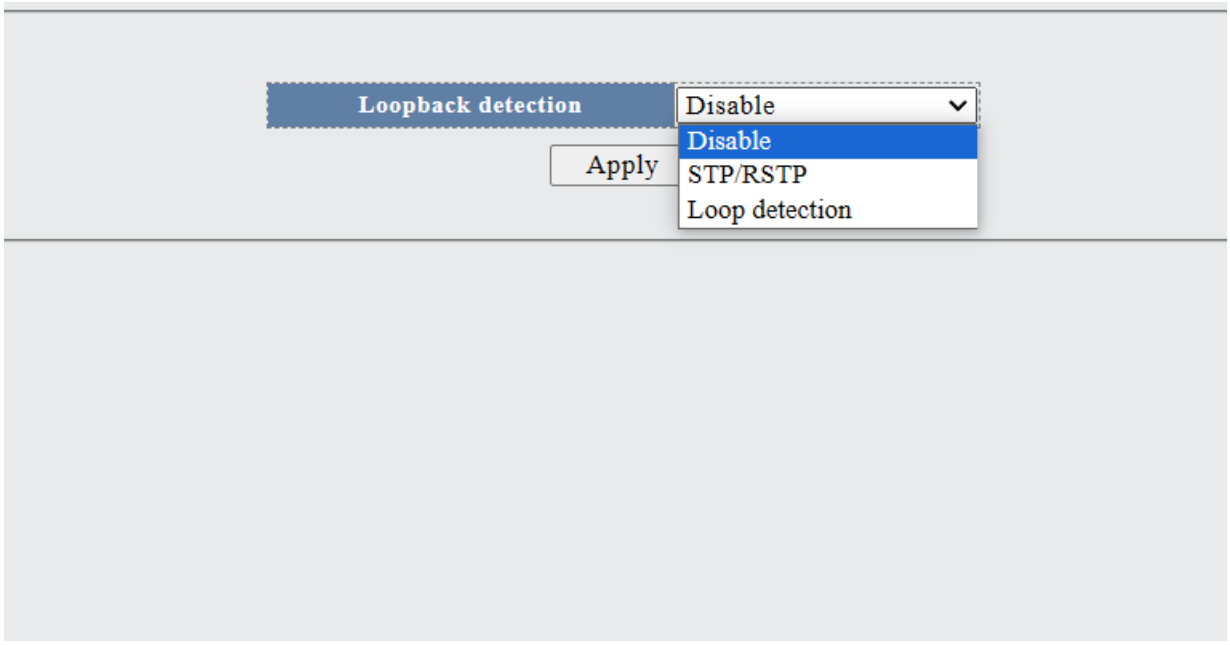
6.5.1 loop detection

Loop is the topological structure of the ring formed by the network of the switch. The loop will cause the Intranet broadcast storm, which will consume a large amount of CPU and line bandwidth of the switch, and can even cause equipment crash and network paralysis in serious cases.

Click the navigation bar: Configure-> Loop protocol- -> Loop protection



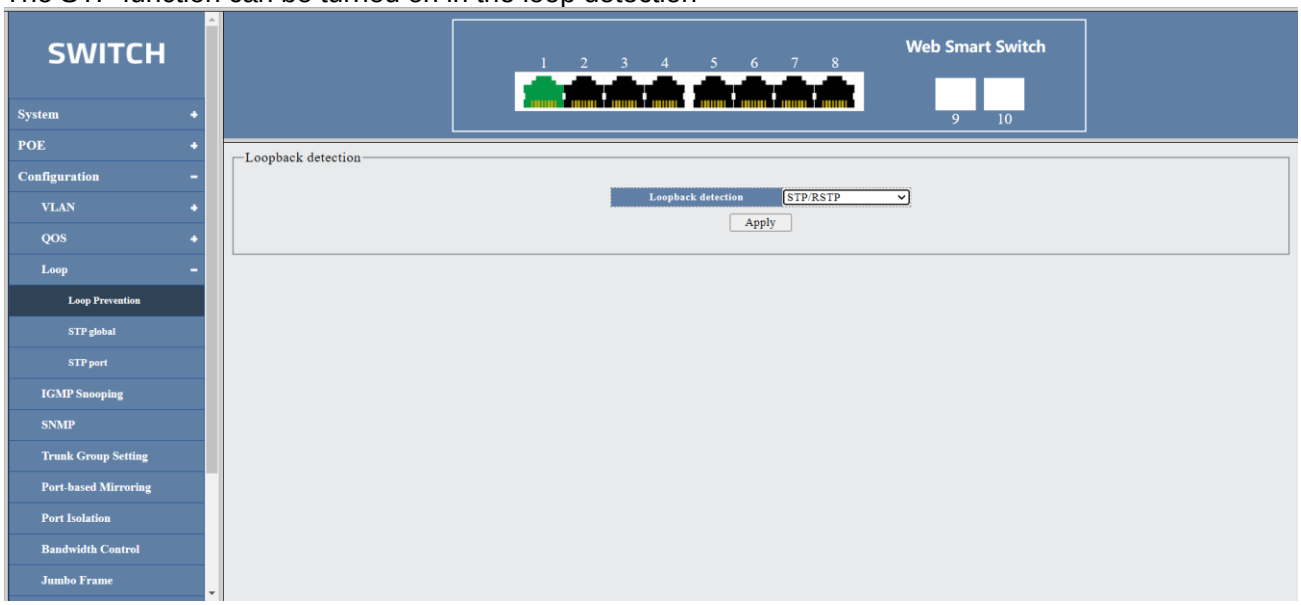
Detection status is default off, select STP / RSTP and normal loop detection



Default closed

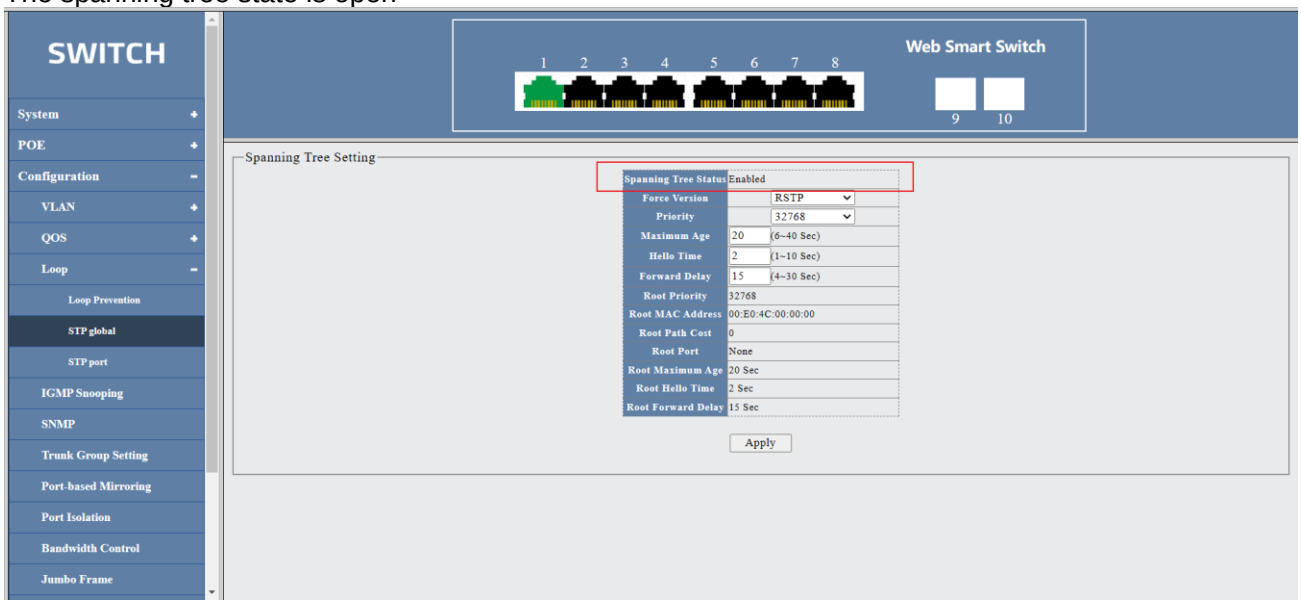
6.5.2 STP overall situation

The STP function can be turned on in the loop detection



6.5.3 STP port

The spanning tree state is open

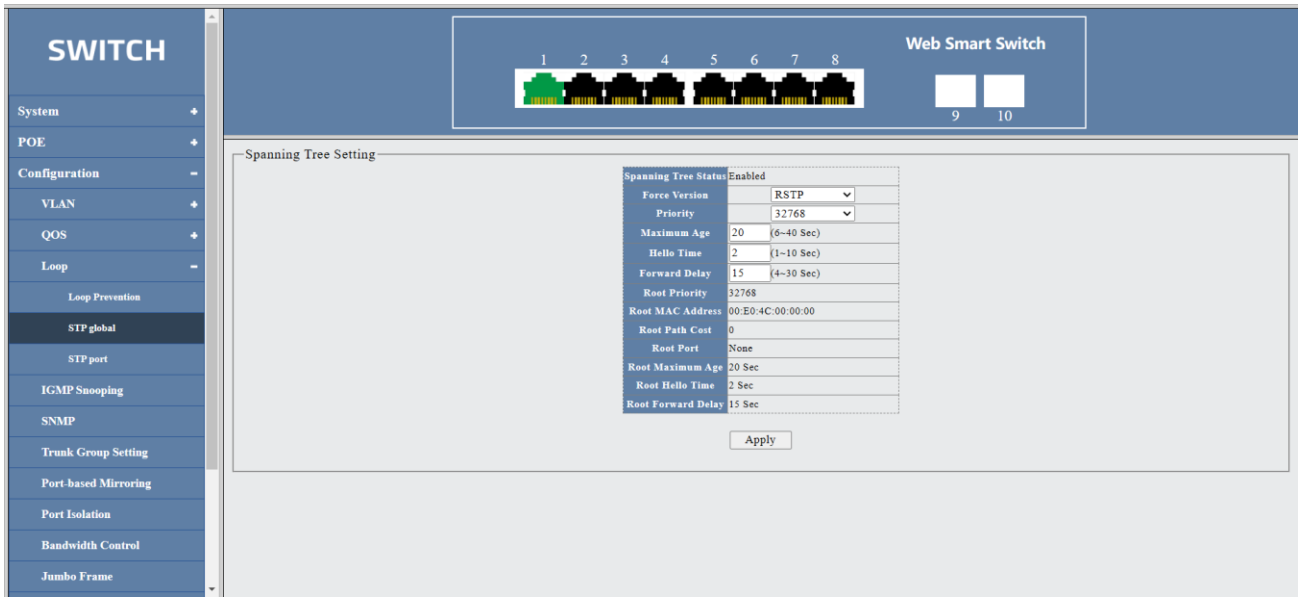


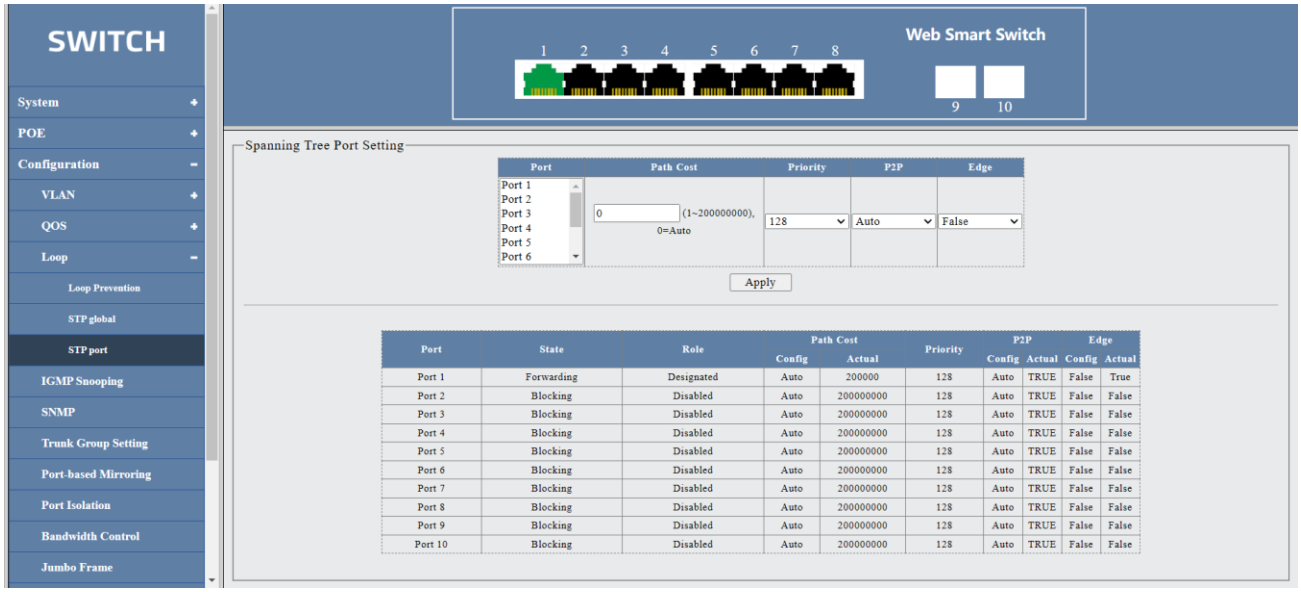
6.6. Spanning tree

In an Ethernet switching network, redundant links are usually used to conduct link backup and improve network reliability. However, using redundant links will generate loops on the switching network, causing faults such as broadcast storm and unstable MAC address table, resulting in poor user communication quality and even communication interruption. To solve the loop problem in switching network, the generative tree protocol STP (Spanning Tree Protocol) is proposed.

Like the development process of many protocols, the spanning tree protocol is constantly updated with the development of the network, from the STP defined in the original I EEE 802.1D to the rapid spanning tree protocol RSTP (Rapid Spanning Tree Protocol) defined in IEEE 802.1W, to the multi-spanning tree protocol MSTP defined in the latest IEEE 802.1S.

Click on the navigation bar: Configure- -> Loop protocol- -> STP Global





Root bridge: first compare the priority of the switch, the switch with a small priority as the root bridge switch; if the priority is the same, select the small MAC address as the root bridge switch.

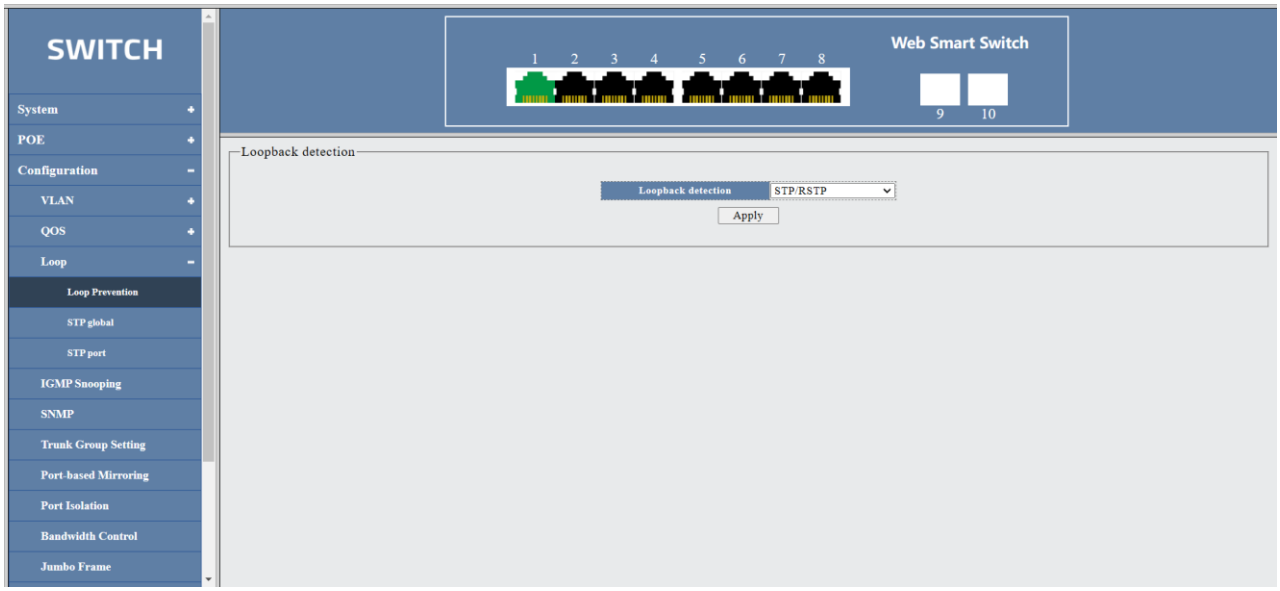
Root port: elect a root port on each non-root bridge switch, first compare the overhead value of the link where the switch port reaches the root bridge (the smaller, the better); if the overhead value is the same, compare the bridge ID (priority-> MAC address); if two links exist, select the port where the uplink switch port number is small to become the root port.

Designated port: Select a specified port on each link (the interface of the root bridge is the specified port). Comparing the root port of the switch on the link to the root port reaches the root port, the smaller side becomes the root port, and the smaller port becomes the specified port.

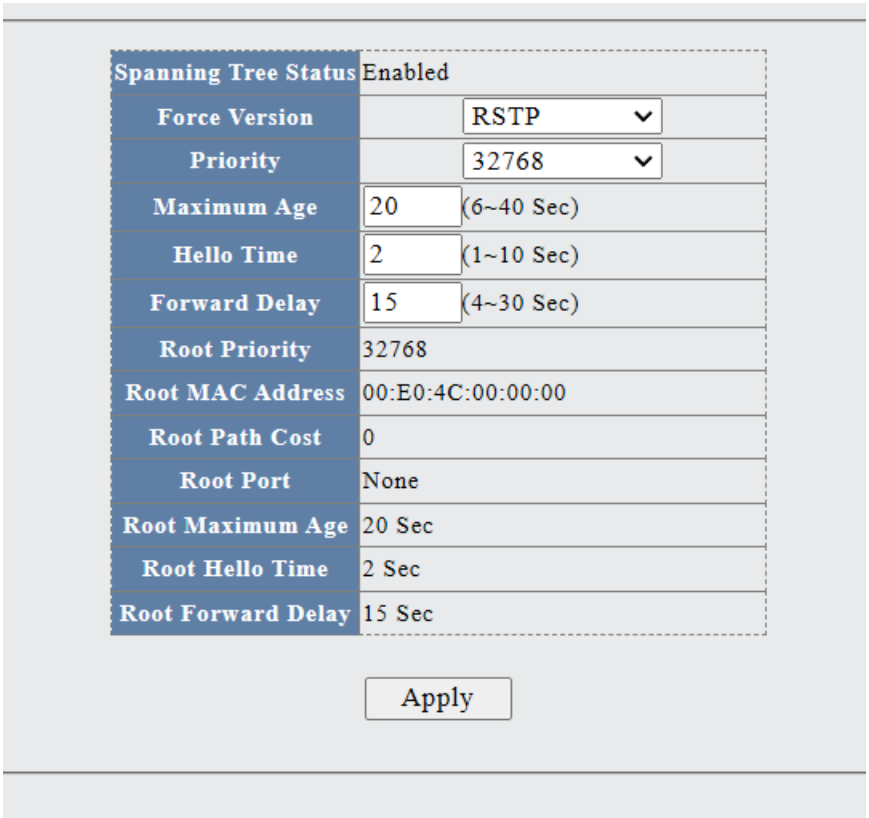
Blocking port: After passing the above election, the port on the link is not elected as a blocked port

6.6.1. Examples

1. Click the navigation bar: Configure- -> loop protocol- -> loop detection, and open the generating tree function



2. Click the navigation bar: Configure- -> Loop protocol- - -> STP Global Set switch priority.



3. Click the navigation bar: Configure- -> Loop Protocol- -> STP port Set path overhead.

Port	State	Role	Path Cost		Priority	P2P		Edge	
			Config	Actual		Config	Actual	Config	Actual
Port 1	Forwarding	Designated	Auto	200000	128	Auto	TRUE	False	True
Port 2	Blocking	Disabled	Auto	200000000	128	Auto	TRUE	False	False
Port 3	Blocking	Disabled	Auto	200000000	128	Auto	TRUE	False	False
Port 4	Blocking	Disabled	Auto	200000000	128	Auto	TRUE	False	False
Port 5	Blocking	Disabled	Auto	200000000	128	Auto	TRUE	False	False
Port 6	Blocking	Disabled	Auto	200000000	128	Auto	TRUE	False	False
Port 7	Blocking	Disabled	Auto	200000000	128	Auto	TRUE	False	False
Port 8	Blocking	Disabled	Auto	200000000	128	Auto	TRUE	False	False
Port 9	Blocking	Disabled	Auto	200000000	128	Auto	TRUE	False	False
Port 10	Blocking	Disabled	Auto	200000000	128	Auto	TRUE	False	False

6.7. Port mirror

Port mirroring is a copy of the packet of the specified port of the switch to the destination port; the copied port is called the source port and the replicated port is called the destination port. The target port will be connected to the data detection device, and the user will analyze the messages received by the target port for network monitoring and troubleshooting

Click on the navigation bar: Configure- -> Port based mirroring

explain:

Data flow direction of the mirror port (in, out, both)

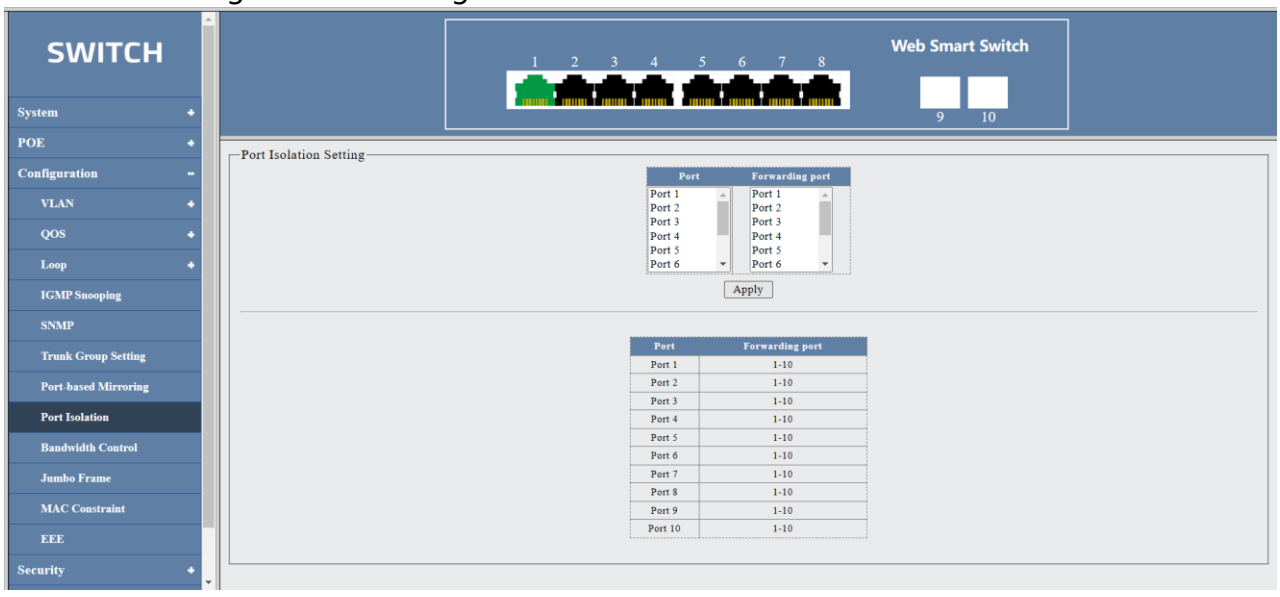
6.7.1. Example

Port 1 connects the device with IP address 192.168.137.10, port 5 to 192.168.137.251 devices, port 8 to the management host, set port 8 to the monitored port and port 1 to the monitored port. Use the Wireshark scratch package in the managed host. It can be found to grasp the ping package in Wireshark as shown in Fig

No.	Time	Source	Destination	VLAN tag	DSCP	Protocol	Length	Info
55…	381.3611…	192.168.137.10	192.168.137.251		CS0	ICMP	74	Echo (ping) reply id=0x0
55…	381.3611…	192.168.137.10	192.168.137.251		CS0	ICMP	74	Echo (ping) reply id=0x0
55…	381.3648…	192.168.137.10	192.168.137.251		CS0	ICMP	74	Echo (ping) reply id=0x0
55…	381.3648…	192.168.137.10	192.168.137.251		CS0	ICMP	74	Echo (ping) reply id=0x0
55…	382.0126…	192.168.137.251	192.168.137.10		CS0	ICMP	74	Echo (ping) request id=0x0
55…	382.0127…	192.168.137.1	192.168.137.251		CS0	ICMP	102	Redirect (Redir
55…	382.0127…	192.168.137.251	192.168.137.10		CS0	ICMP	74	Echo (ping) request id=0x0
55…	382.0128…	192.168.137.251	192.168.137.10		CS0	ICMP	74	Echo (ping) request id=0x0
55…	382.0128…	192.168.137.251	192.168.137.10		CS0	ICMP	74	Echo (ping) request id=0x0
55…	382.0130…	192.168.137.251	192.168.137.10		CS0	ICMP	74	Echo (ping) request id=0x0
55…	382.0130…	192.168.137.251	192.168.137.10		CS0	ICMP	74	Echo (ping) request id=0x0

6.8. Port isolation

Click on the navigation bar: Configure- -> Port isolation



Explain:

Port source port

Port isolation Reforwarding ports

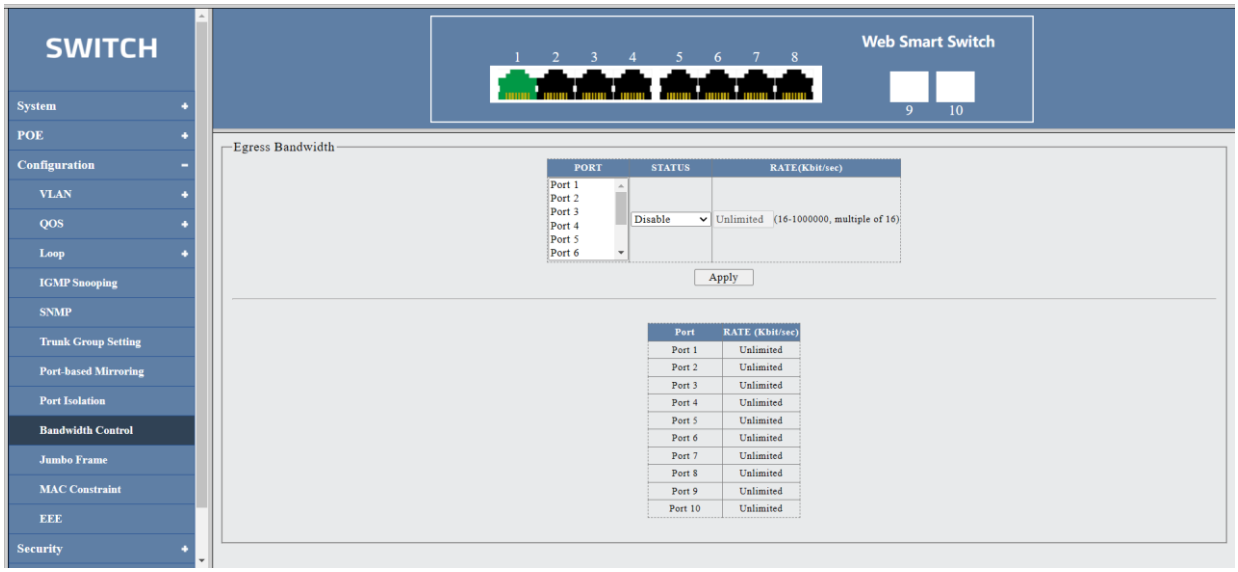
Configure forwarding ports for the source port, which receives packets that cannot be forwarded to ports not in the forwarding port.

6.9. bandwidth control

Configuring port bandwidth is limiting the rate at which the physical interface receives data outward or inward.

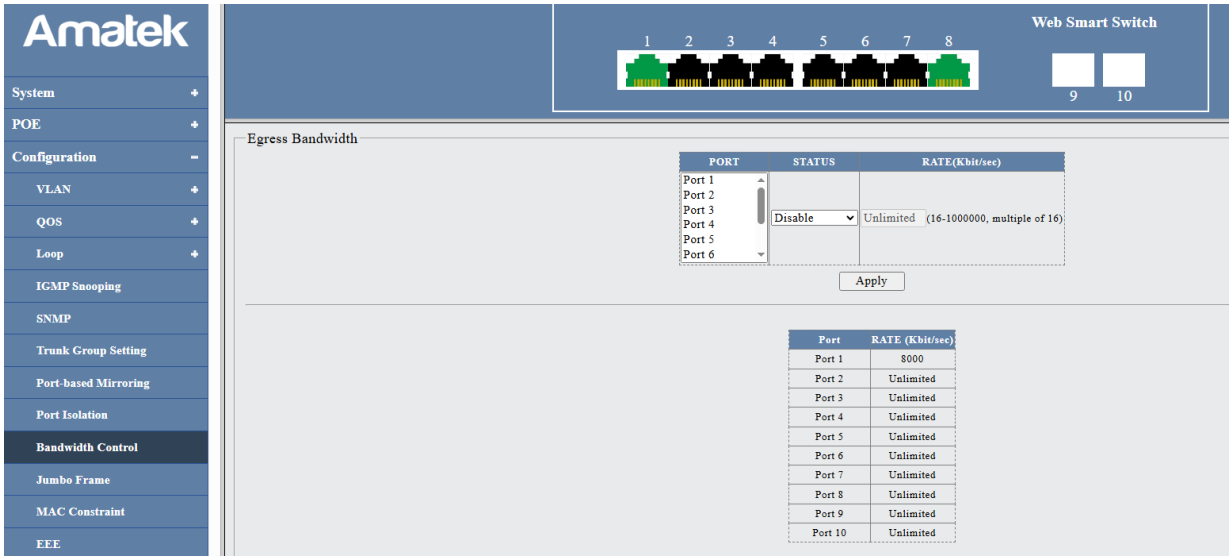
Before the flow is sent from the interface, configure the speed limit in the outgoing direction of the interface to control all the outgoing message flow. Before the traffic is received from the interface, the speed limit is configured in the incoming direction of the interface to control all the incoming packet traffic.

Click on the navigation bar: Configure- -> Bandwidth control



6.9.1. Example

Limit the port 1 entrance and exit rate to 8000kbps, setting the figure below.

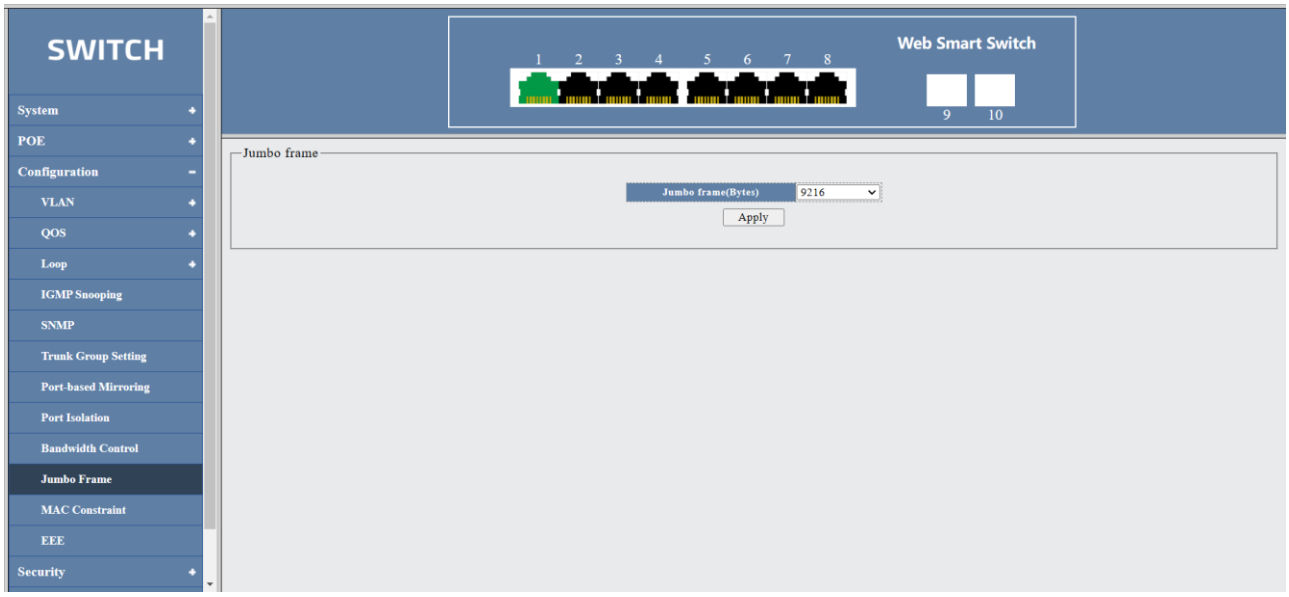


Download the file on the port 1 connection PC, open the Task Manager and click on Ethernet to display the receiving rate

6.10.Jumbo frame

Configure the maximum message length that the system can forward

Click on the navigation bar: Configure- ->Jumbo frame



6.10.1. E xample

。After opening the giant frame, set the PC network card to open the giant frame, set the ping packet data 8000, no subcontract. Command ping-f 192.168.2.210-l 8000-t to catch giant frames at a PC with IP 192.168.2.210.


```
14… 171.5954…  192.168.2.210   192.168.2.100   CS0 ICMP    642 Echo (ping) reply    id=0x00
14… 172.6010…  192.168.2.100   192.168.2.210   CS0 ICMP   8042 Echo (ping) request  id=0x00
```

6.11.MAC constraint

The system supports the port Mac learning restriction function. Systematically learns the source MAC in the user message, when the learned MAC reaches the limit threshold. If the source MAC of the user message already exists in the MAC table, the user message will continue to forward; if the source MAC of the message does not exist in the MAC table, the system will process the message according to the MAC restrictions. For example, if the action is discarded, then the user message will be discarded at the entry port.

Click on the navigation bar: Configure- -> Mac constraint

6.12. EEE

Energy-saving Ethernet (EEE) supports operation in low-power idle mode. The system at both ends of the link can disable some functions when the link utilization is low, thus saving power consumption. It is recommended to close.

Click on the navigation bar: Configure- -> EEE

Chapter 7 Safety

7.1. MAC address

7.1.1. MAC search

Click on the navigation bar: Security- -> MAC Address- -> MAC search

7.1.2. Static MAC

CClick on the navigation bar: Security- -> MAC Address- -> Static MAC

7.2. Broadcast storm

Broadcast storm refers to the number of broadcast frames on the network due to the continuous forwarding, which affects the normal network communication and seriously reduces the network performance. Broadcast storms can take up considerable network bandwidth, causing normal packets to fail. When the broadcast data fills the network and cannot process and occupies a lot of network bandwidth, resulting in normal business can not operate, this causes a broadcast storm, causing local or entire local network paralysis:

Click the navigation bar: security- -> storm control

Explain:

Storm type broadcast, multicast, unknown unicast, unknown multicast

Port selection port, multiple optional

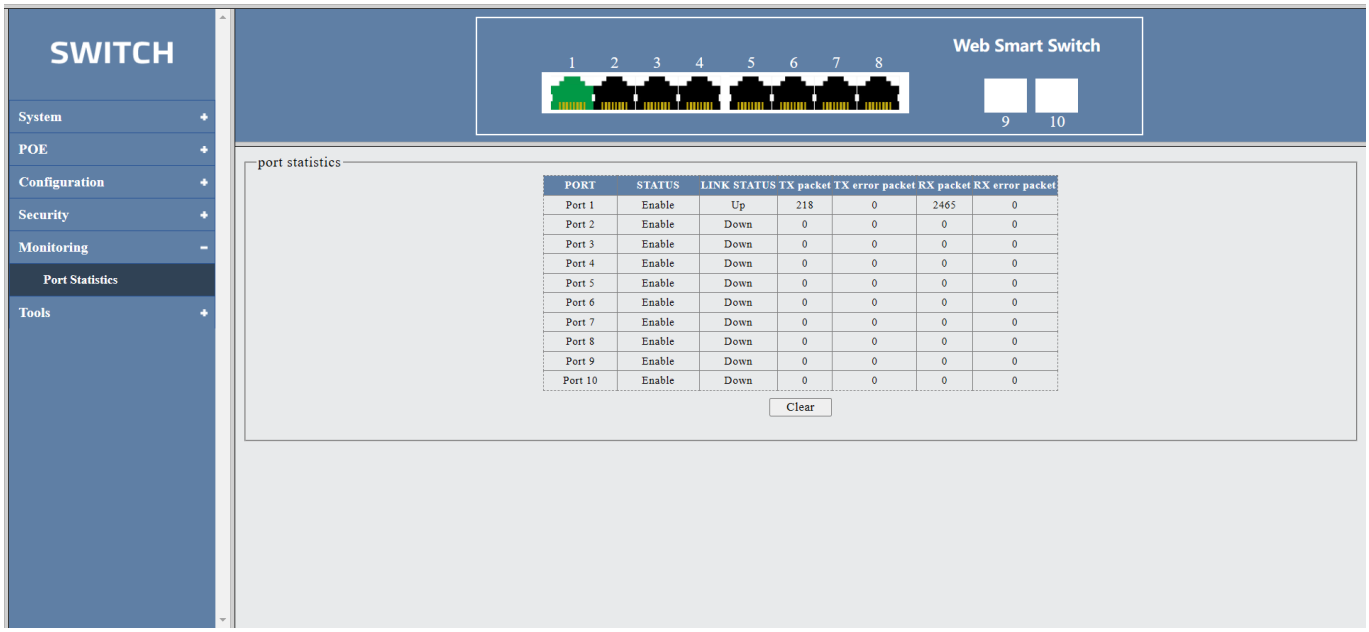
The State turns on or off the Broadcast Storm suppression function

Speed setting of the port broadcast, multicast package, unknown unicast, unknown multicast bandwidth.

Chapter 8 Monitoring

8.1. Port statistics

Port statistics display the traffic information of each port, convenient to monitor traffic and analyze network abnormalities. Click on the navigation bar: Monitor- -> Port Statistics



Explain:

port

port number

state

The ports status is displayed to forwards packets normally

accepting state

The port has the current LINK status

Send the correct package number

Display the correct number of contract ports

Send error package number

Displays the number of port errors

Receive the correct package number

Displays the number of correct packets received by the port

Receive the number of error packages

Displays the number of port-received error packets

Chapter 9 Tools

9.1. Firmware upgrade

You can upgrade the software of the switch here. Click on the navigation bar: Tool- -> Firmware Upgrade

Click the <Select File> button to load the latest firmware file. Click <Upgrade> again to start upgrading, and click <OK> in the pop-up window.

notice :

During the firmware upgrade process, please do not power off the device, keep the power supply stable, and do not refresh the page. Upgrading the firmware may lose the currently unsaved configuration information, please save the configuration before you upgrade.

Click the navigation bar: tool- -> Restart to restart the switch

9.2. Configure backup

You can save the current configuration information here and recommend back up the current configuration information before modifying the configuration and upgrading the software.

Click the navigation bar: Tools- -> Configure Backups

Configure Backup: Click <Backup> to download the current configuration file locally through the browser.

Configuration Recovery: Click <Select File> Select the configuration file and click Upgrade. Then restart the switch into effect.

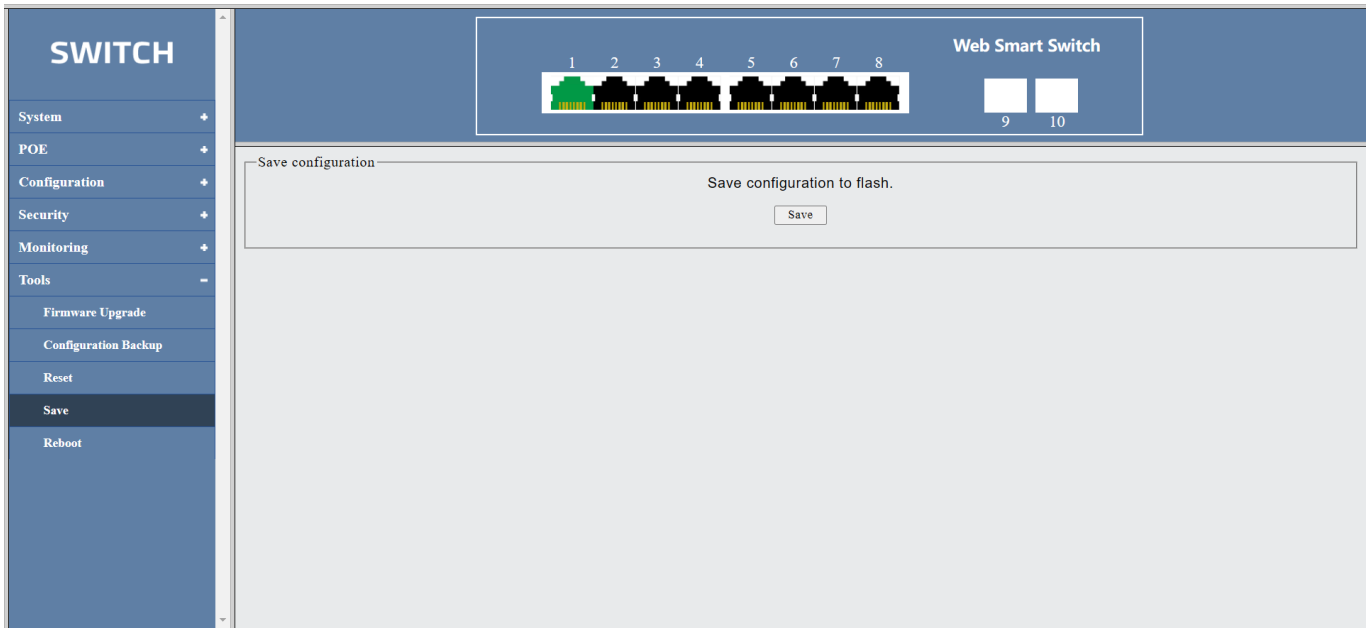
9.3. Reset

In addition to the hardware restore factory setting switch, you can also restore the default settings on the Web. Click the navigation bar: tool- -> Reset

Click the <Restore Default Settings> button to restore all settings defaults. The current configuration information will be lost. It is recommended to back up the configuration before restoring the defaults. The default management IP address is 192.168.1.200, and the account name and password are both admin.

9.4. Save configuration

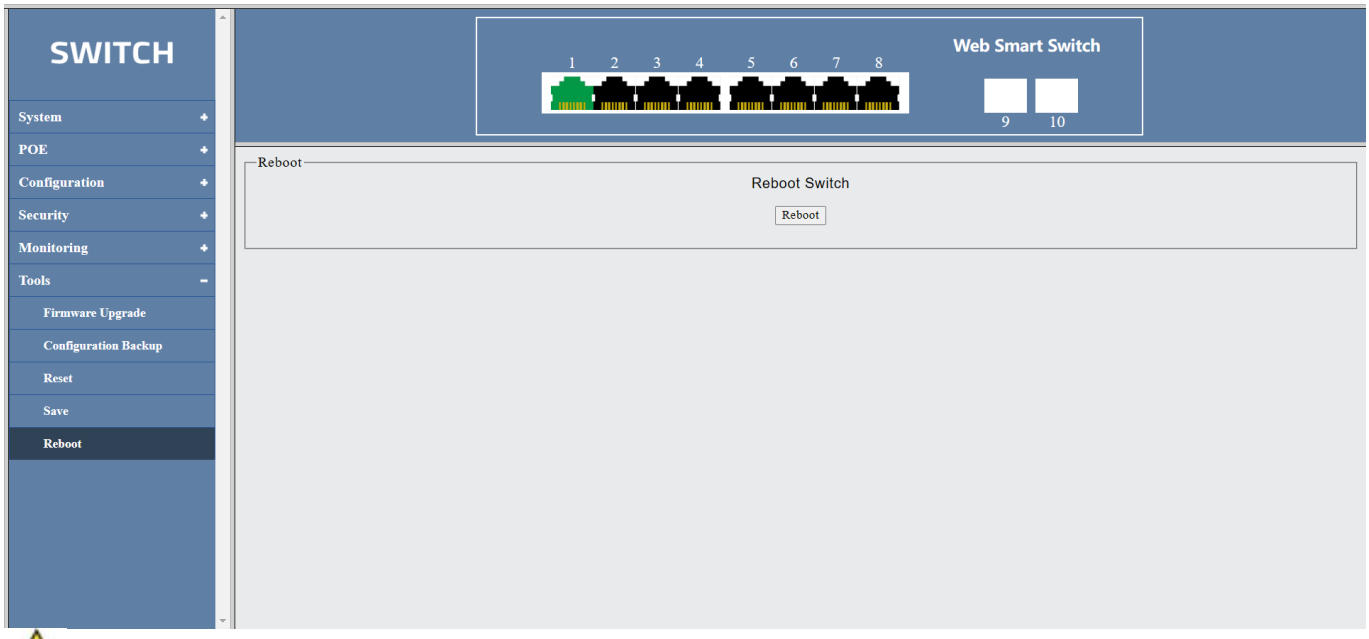
Click on the navigation bar: Tool- -> Save



It is recommended that after modifying the settings, save the settings to FLASH. Otherwise the settings for power off or restart modification will be lost.

9.5. Reboot

After clicking restart, the switch will restart. Before restart, it is recommended to save the configuration to prevent the currently modified configuration from being lost. Click on the navigation bar: tool- -> to restart



notice :

Please do not turn off the power during the restart process to ensure the power stability during the restart process and avoid forced power failure.