Full-Gigabit 2-Fiber 24-Copper Web-Managed PoE Switch

Light network management series

WEB Network Management Operation Guide

Model: KL-024G-SFP

Smart Solutions

www.kline.knowledgline.com

Ver 1.0.1

Declare

Foreword

This manual mainly describes the WEB platform page of the light network management Ethernet switch. The user can manage the switch through the WEB page. This manual only gives a brief introduction to the operation of each WEB page. Please refer to the User Manual for the introduction of each function.

The preamble contains the following：

- Audience Object
- Product Introduction

Audience Object

- Network Planner
- On-site technical support and maintenance personnel
- Network administrator responsible for network configuration and maintenance

Product Introduction

The light network management Ethernet switch is independently designed and developed by our company. It is a web management Ethernet switch specially designed for building a high-security and high-performance network. T

he system uses a new software and hardware platform to provide a comp rehensive security protection system, simple VLAN switching, port isolation an d so on. The light network management series is easy to manage and maintai n, and is an ideal convergence layer switch for office networks, campus netwo rks, small and medium-sized enterprises, and branch offices.

[Version Update]

Ver 1.0.1

User experience optimization

Resolves known issues and provides faster response.

Related functions are optimized to make management easier.

Directory

Chapter 1 Login Management Interface

1.1 Logon preparation

1. The switch is normally powered on and started, and any interface is connected with a computer network port for login management;
2. Make sure that the function switch on the front panel of the switch is in the "WEB" position (only support the function switch series);
3. At least IE 8.0 or above, the latest version of FireFox, Chrome and Safari browsers or one of the above core browser software should be installed on the management computer;
4. The IP address of the network card connecting the management computer and the switch should be in the same network segment as the management IP address of the switch. It should be 192.168. 0. * (* is any integer between 3 and 254) when it is set for the first time. The subnet mask is 255.255. 255.0.

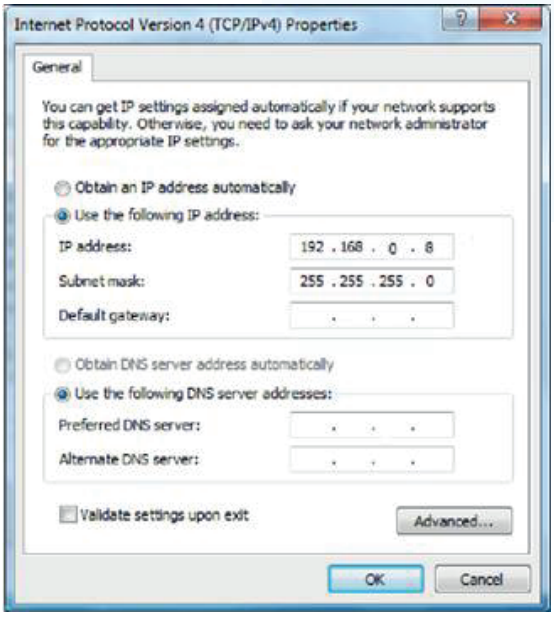


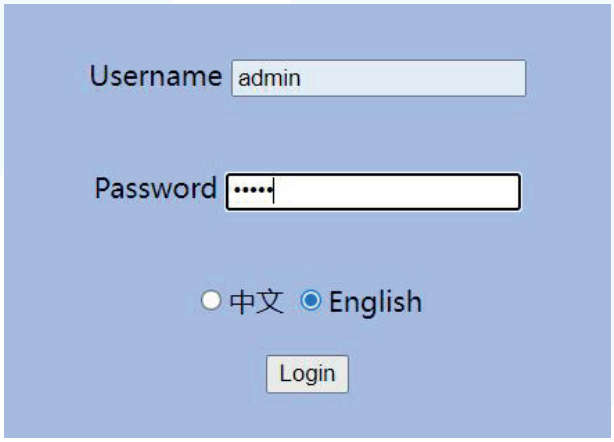
Figure 1. 1

Verify that the function switch is in the WEB position when logging in to the switch (function switch series only).

1.2 Login step

1. Open the browser and enter the management address of the switch in the address bar (the default address is the http://192.168.0.1) to log in to the management interface of the switch.

2. Enter the switch management username and password in the pop-up login window. The default username and password are admin.



3. After a successful login, the switching system information page is displayed.

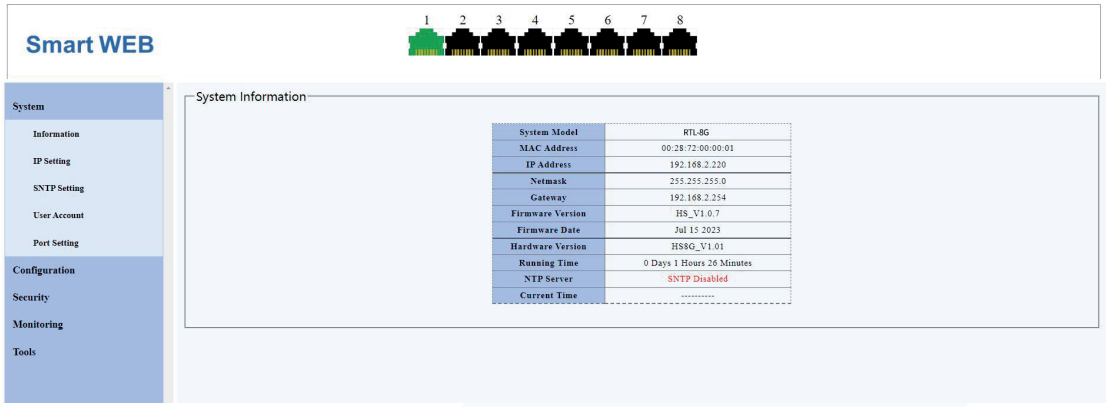


Figure 1.2 Switching System Page

Chapter 2 WEB Management Function

2.1 Interface description

① **Interface Status:** Displays the working status of the port. Green indicates that the port is connected. Uncolored indicates that the port is not connected.

② **Function navigation tree:** You can quickly switch to the corresponding function page through function navigation.

③ **Function details:** information display and configuration details of the currently selected function.

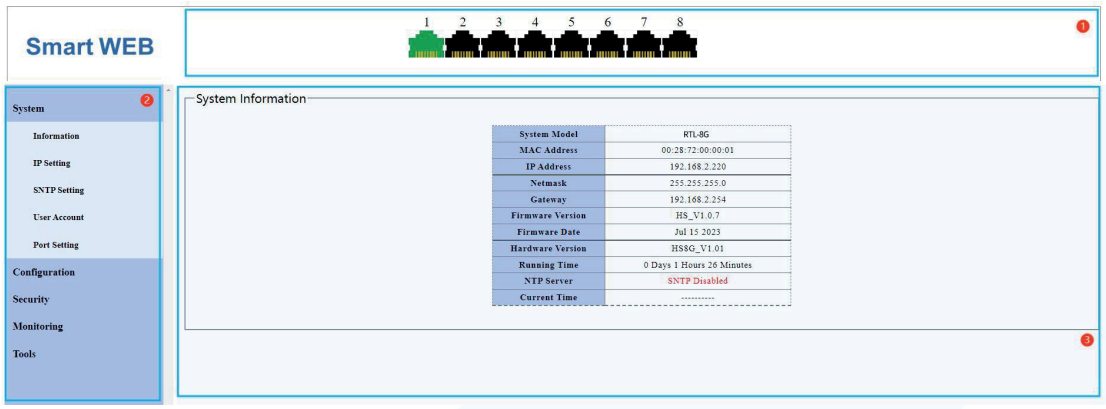


Figure 2.1 Interface description

2.2 system

2.2.1 System Information

The system information page displays the basic information of the switch system, including device model, MAC address, IP information, firmware and h ardware version information.

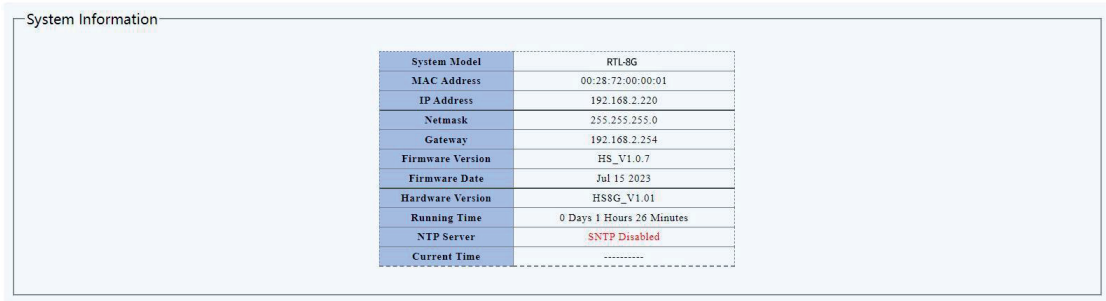


Figure 2.2.1 System Information Page

2.2.2 IP Settings

Displays and sets the management IP address of the switch.

When the IP mode is Static IP, you can manually configure the IP addres s, subnet mask, and gateway information.

When the IP mode is DHCP, the switch automatically obtains IP informati on from a DHCP server in the network.

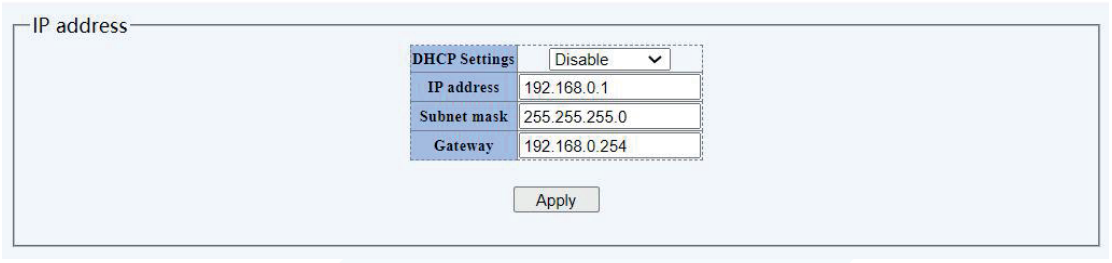


Figure 2.2.2 IP Settings Page

When switching the IP mode, you need to log in the switch again;

After modifying the management IP application, you need to use the ne w IP address to log in and ensure that the network segment of the man agement computer matches it.

2.2.3 SNTP Settings

Simple Network Time Protocol, adapted from NTP, is primarily used to sy nchronize computer clocks across the Internet

In this interface, you can add the corresponding time service area to sync hronize the time between the time switch and the time server. The details can be viewed in the system configuration.

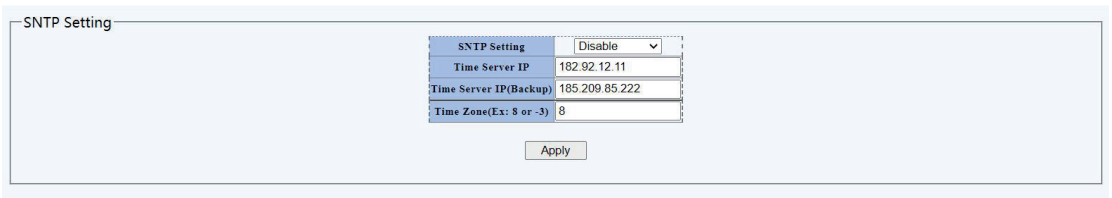


Figure 2.2.3 SNTP Setting Page

2. 2. 4 User Settings

On the User Settings page, you can modify the user name and password of the switch management account. If a new user name is set on this page, th e original user name will be invalid. The password length is required to be bet ween 8 and 16 digits.

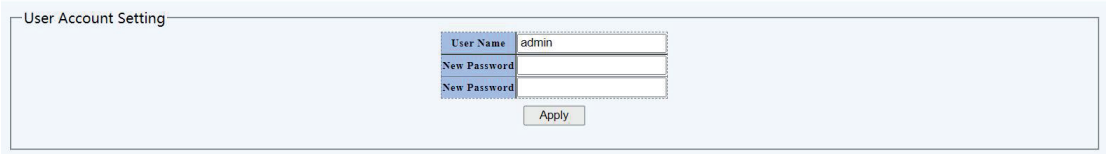


Figure 2.2.4 User Settings Page

2. 2. 5 Port Settings

The Port Settings page allows the user to set and display the port status, including the following:

Status: "Open" and "Close" status. If set to "Close", the port is manually closed and communication is not possible;

Speed/Duplex: All interfaces default to Auto, which is adaptive mode. It c an be manually configured as "full-duplex/half-duplex mode", and the speed of 10 M, 100 M and 1000 M can be selected. It is generally recommended to sel ect "Automatic" mode;

Flow control: When the flow control is on and the port is blocked, the swi tch will send a "PASUSE" frame to the information officer to inform the informa tion source to pause for a period of time before sending the information.

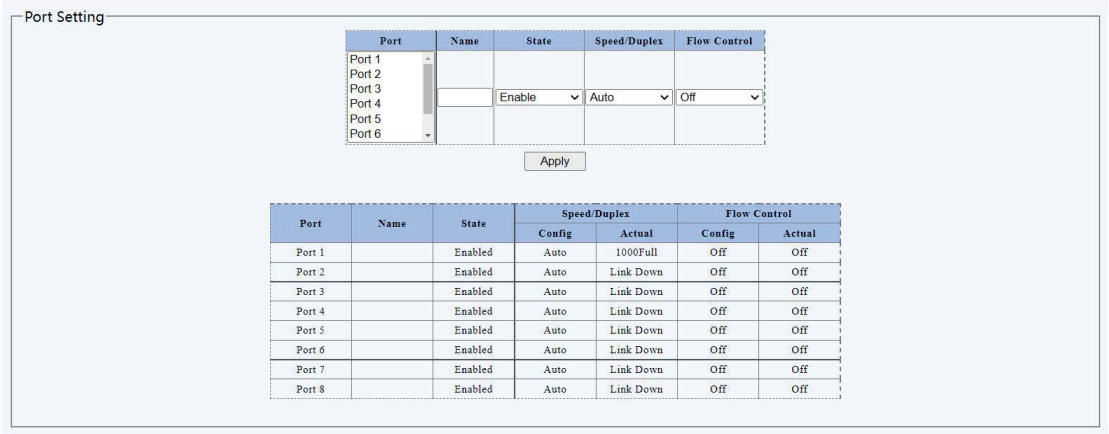


Figure 2.2.5 Port Settings Page

2. 3 configurations

2. 3. 1 VLAN Settings

2. 3. 1. 1 Static VLAN

Static VLANs are used to set the 802.1Q VLAN properties for a switch po rt.

VLAN ID: Identifier used to distinguish different VLANs. Terminals in diffe rent VLANs cannot communicate directly.

VLAN name: a name or description of the corresponding VLAN, usually used to visually distinguish different VLANs.

No tag: The port is marked as having no tag. When the data frame goes out of the port, if it is a frame with a VLAN tag, the tag will be removed and the n sent out. If it is a data frame without a tag, it will be sent out directly. Data fra mes entering the port are internally tagged with the VLAN ID of the port. Com monly use for access terminal equipment.

Label: The port identified as a label carries the VLAN ID label when the d

ata frame is sent to the port. Therefore, the peer device must be able to identif y the VLAN label, otherwise it cannot identify the data normally. Typically used to connect to the TRUNK, HYBRID, or VLAN-capable router ports of a manag ed switch.

No member: when the port is checked, it means that the current port is n ot a member port of this VLAN.

Add/Modify VLAN

Fill in the VLAN ID and VLAN name to be added (optional);

Select the corresponding option under the port name according to the tag and tag attributes required by the port (click the "VLAN" button of the corresp onding option to set all ports to the corresponding attributes);

Click the "Add/Modify" button below.

Delete VLAN

Check the delete selection box behind the corresponding VLAN ID in the VLAN list below, and click "Delete" to delete the corresponding VLAN;

VLAN 1 is the default VLAN and cannot be deleted. Click Select All to sel ect all VLANs except VLAN 1.

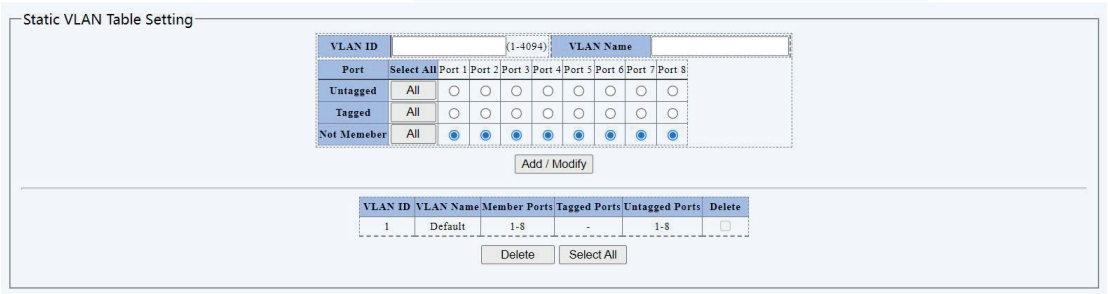


Figure 2.3.1.1 Static VLAN pack

2. 3. 1. 2 VLAN Settings

The VLAN Port Settings page is used to set the PVID of the port (based on the VLAN ID of the port) and the frame format that the port receives.

PVID: All ports have one and only one PVID. When an untagged data frame enters a switch port, the switch internally tags the data frame from that port with the PVID. The default PVID for all ports is 1.

Receiving frame format

All: The designated port processes received frames regardless of whether they are tagged or not. For untagged frames, the PVID is tagged with the VLAN tag for further processing. For the tagged frame, if the port belongs to the member of the corresponding VLAN ID, the next step is processed, and if the port does not belong to the member, the frame is discarded.

Labeled Only: Specifies that the port only receives labeled data frames. Generic client devices do not support VLAN tagging, so the port to which the client is connected may not communicate when this option is selected.

Unlabeled Only: Specifies that the port only receives unlabeled data frames. If the interface of the peer device is multi-VLAN communication (such as the TRUNK interface of the switch and the router configured with VLAN-based subinterfaces), only PVID can communicate.

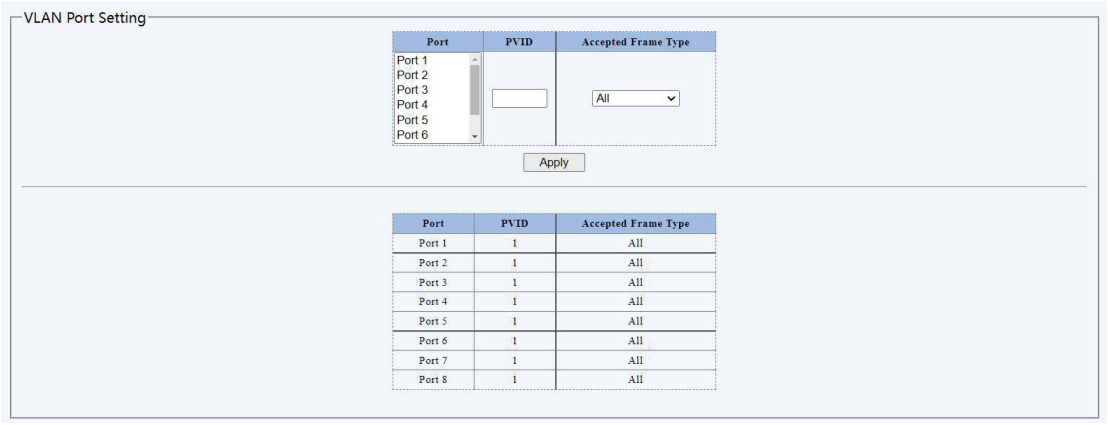


Figure 2.3.1.2-1 VLAN Setting Page

For example, as shown in the 2.3, 1.2 -2, the superior device has been co nfigured with VLANs 10, 20, and 30, and the corresponding VLAN is allowed t o pass through the port connected to the switch. The three terminals connecte d to port 1, 2 and 3 of this machine are respectively planned to VLAN 10, 20 a nd 30.

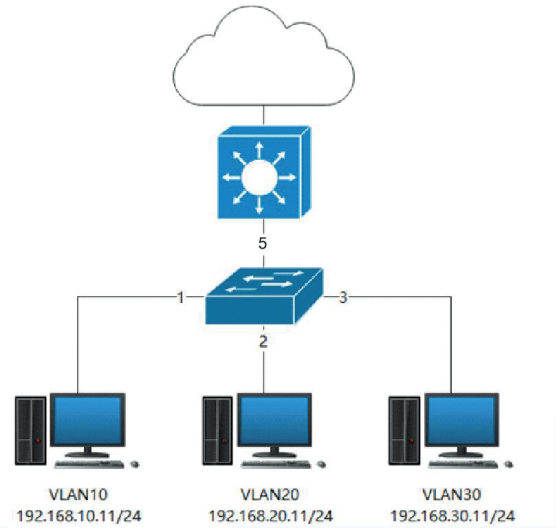


Figure 2. 3. 1. 2–2

Start by adding the appropriate VLAN and port settings on the Static VLA N page. Take VLAN 10 as an example, fill in VLAN ID 10, select No Label und er port 1, select Label under port 5, and click Add. When all VLANs have been added, you should see Figure 2.3. 1.2-3.

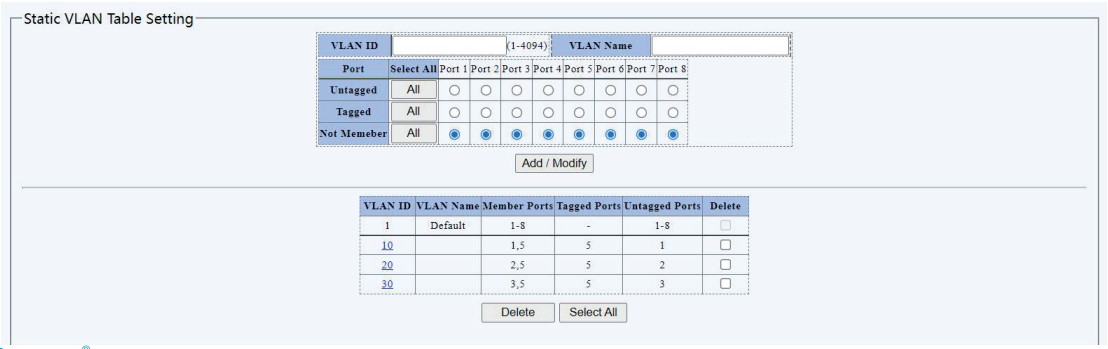


Figure 2. 3. 1. 2−3

Then enter the "VLAN Port Settings" page, select port 1, fill in PVID 10, a nd click Apply. Set port 2 and port 3 respectively according to this method, an d set PVID to 20 and 30 respectively, as shown in Figure 2.3. 1.2 -4.

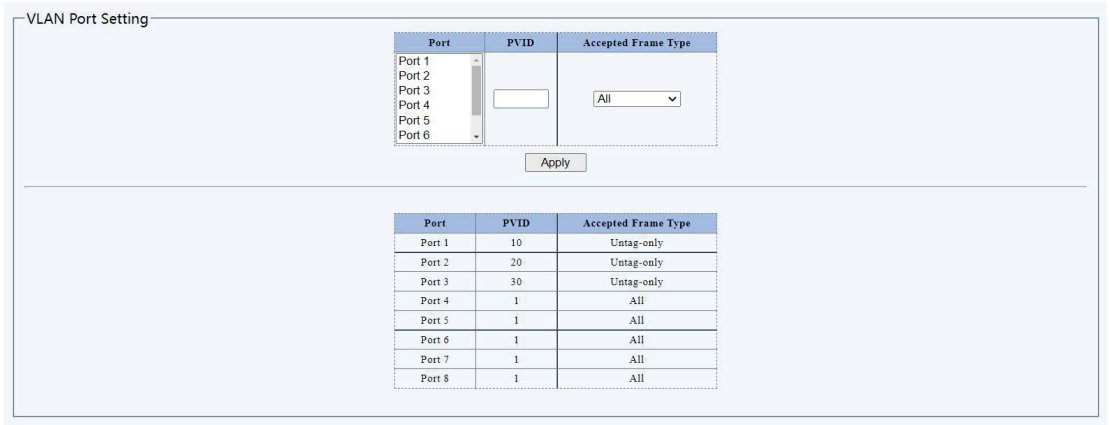


Figure 2. 3. 1. 2−4

For example, as shown in the figure 2.3.1.2-5. When multiple broadbands need to be accessed, but the number of available physical interfaces of the ro uter is insufficient, it is necessary to expand the Wan port through the switch (t his function needs to be supported by the router function).

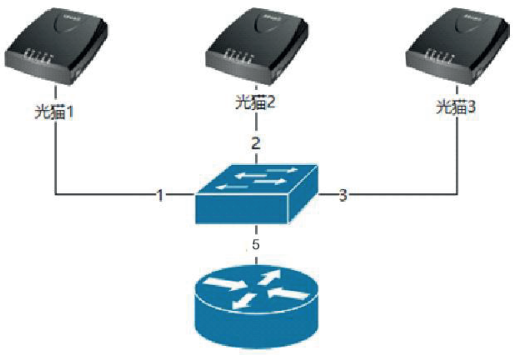


Figure 2.3.1.2-5

The relevant settings of the switch are the same as the previous example, but the difference is that 5 ports are connected to the router, and 1-3 ports are connected to the corresponding operator access equipment respectively. After that, use the corresponding VLAN ID to configure the corresponding subinterface or related Wan port configuration in the router.

2.3.2 QoS

2.3.2.1 Priority Choice

The priority selection page sets different types of priorities for packets for warded through the switch. The higher the value, the higher the priority.

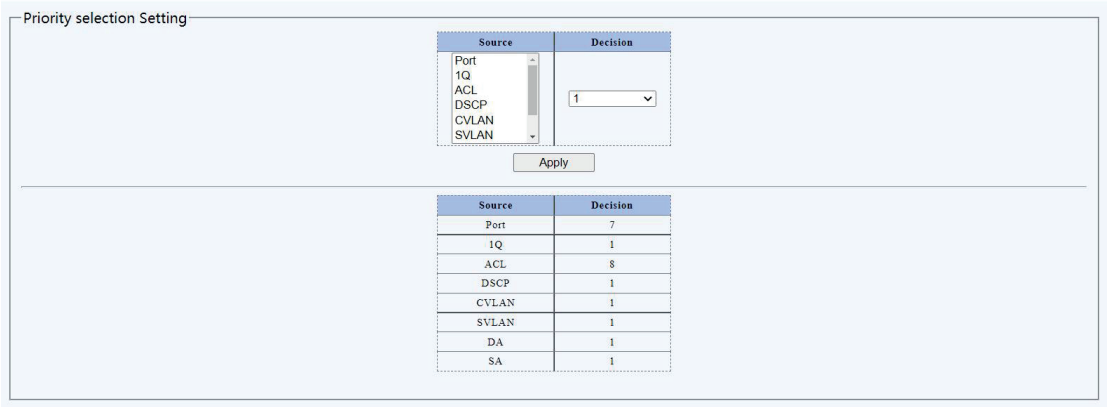


Figure 2.3.2.1 Priority Selection Page

2.3.2.2 DSCP remapping

Sets the DSCP value in IP packets entering the switch port and determines the output queue for the packet based on the user-configured DSCP value and priority. Select the DSCP value to be set and the level priority value to det

ermine the output queue of the data packet.

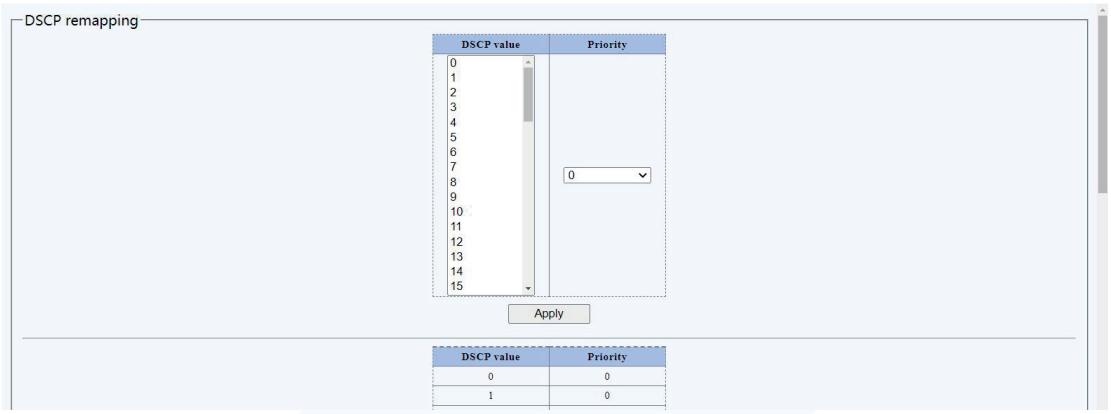


Figure 2.3.2.2 DSCP remapping page

2. 3. 2. 3 Priority to Queue

The queue priority page is used to sort the priority of the data packet que ue output by the switch and determine the output queue of the data packet. T he higher the priority value is, the higher the priority is. The data in this queue is forwarded first.

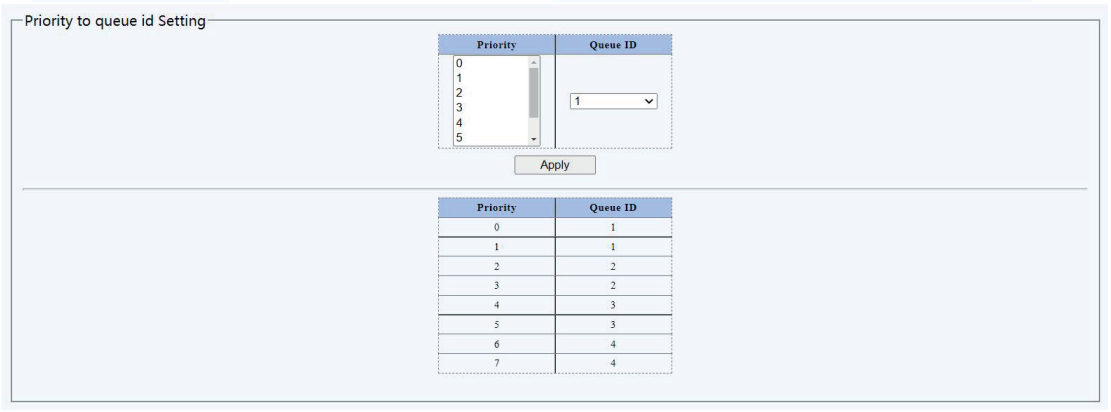


Figure 2.3.2.3 Priority to Queue Page

2. 3. 2. 4 Port priority

The port priority page is used to arrange the priority of the data packets tr ansmitted by the switch port. The higher the value, the higher the priority.

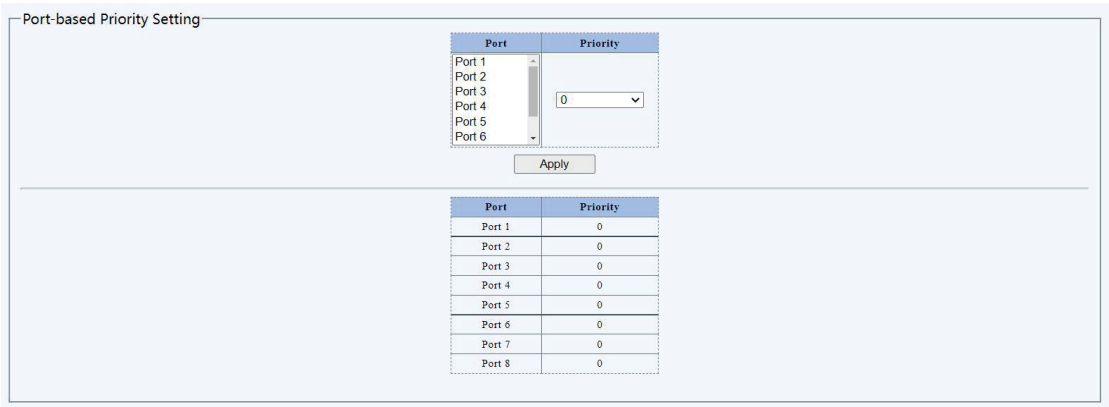


Figure 2.3.2.4 Port Priority Page

2. 3. 2. 5 Queue weight

The queue scheduling page can select the scheduling strategy and the c orresponding priority in the queue priority to define the weight value. (Weight v alue min 1 Max 15).

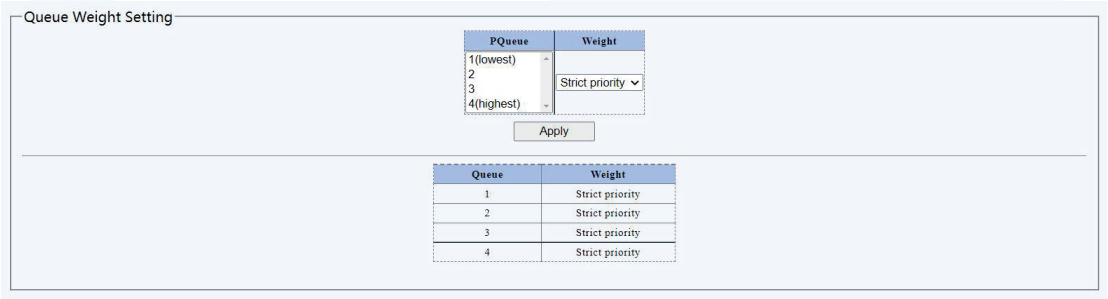


Figure 2.3.2.5 Queue Weight Page

2. 3. 3 DHCP Snooping

Through the DHCP Snooping function, IP address confusion caused by manual configuration of IP addresses by illegal DHCP servers and clients can be eliminated.

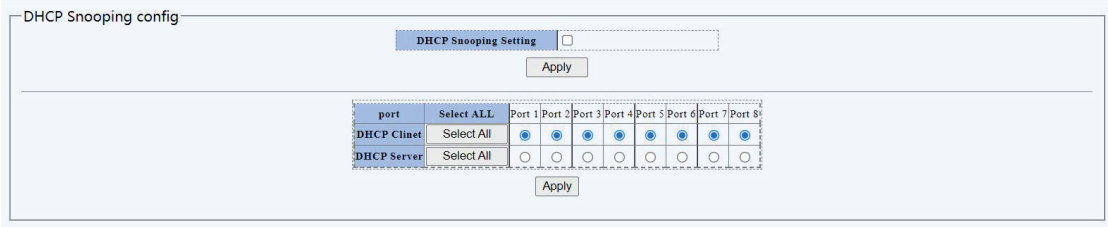


Figure 2.3.3-1 DHCP Snooping Page

For example, as shown in Figure 2.3.3-2, port 5 of the switch is connecte d to a router as a legal DHCP server to allocate an IP address to an intranet t erminal, and port 4 is connected to an illegal DHCP server.

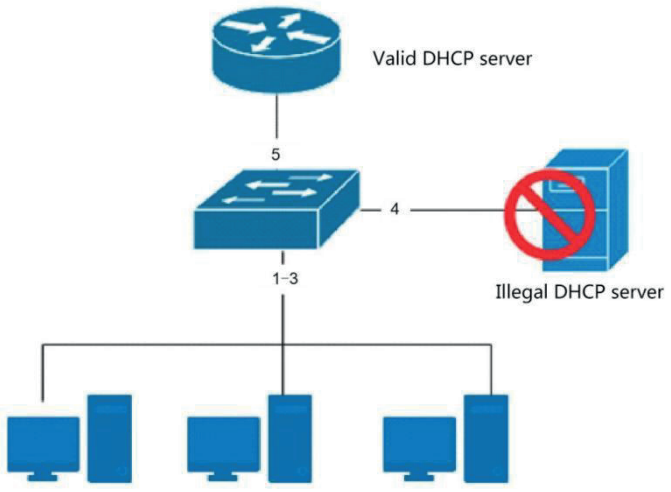


Figure2. 3. 3−2

As shown in the figure below, select ports 1-3 as DHCP Client and ports 4-5 as DHCP Server. Through the above configuration, the switch will discard the DHCP OFFER messages sent by interfaces other than 4-5, so as to preve

nt DHCP servers other than 4-5 from providing illegal address allocation servi ces.

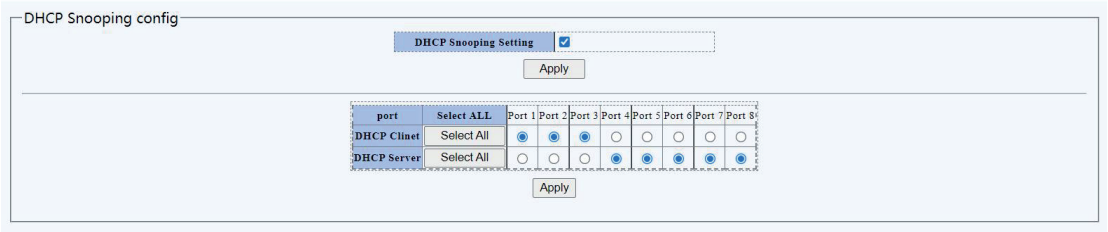


Figure2. 3. 3−3

At the same time, non-DHCP IP addresses obtained on the port selected as the DHCP Client will not be able to communicate.

After the DHCP Snooping function is configured, when the device on th e port selected as the DHCP Client obtains the address through the DH CP service for normal communication, if the switch is restarted, the binding rel ationship will be invalid and the communication cannot be performed, and the device needs to obtain the address through the DHCP again for normal comm unication.

2. 3. 4 IGMP Settings

After the IGMP setting is enabled, the multicast packet is only forwarded t o the corresponding member port, and the data packet of the multicast group i s not forwarded to the non-member port, and the unknown multicast packet is discarded.

When the IGMP function is not enabled, the multicast packet will be broa

dcast and forwarded to all ports.

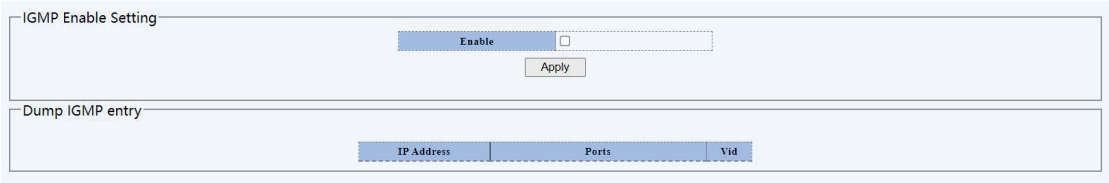


Figure 2.3.4 IGMP Settings Page

2. 3. 5 Link Aggregation

Port aggregation is mainly used to bind two or more physical links into on e logical link between switches to achieve bandwidth increase, load balancing, link redundancy, and other functions.

The switch supports 2 aggregation group, and each aggregation group ca n support up to 4 ports.

When adding ports, you can press and hold the mouse to select multiple consecutive ports. When selecting non-consecutive ports, you can press and hold the "Ctrl" key to select multiple ports or deselect the corresponding ports.

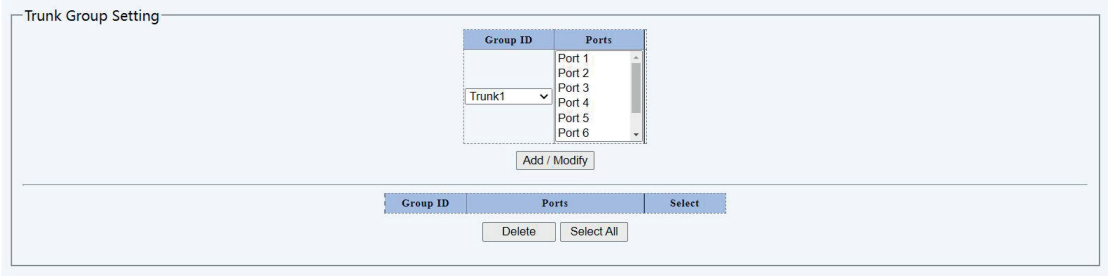


Figure 2.3.5 Link Aggregation Page

e to the closure of the port by the spanning tree protocol.

2. 3. 6 Loop Protection

Loop prevention settings are mainly divided into three categories: loop pr evention, loop detection, and spanning tree.

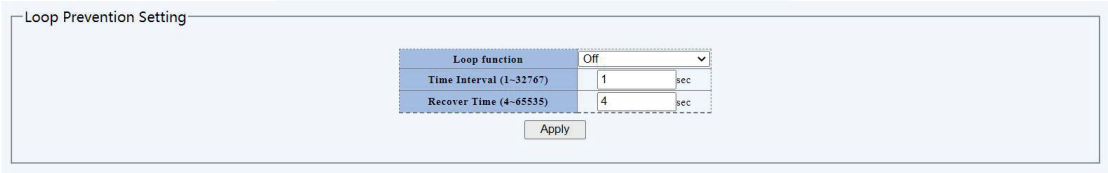


Figure 2.3.6-1 Loop Protection Page

Loop prevention: After this function is enabled, when the link has a loop, t he switch will block the corresponding loop port.

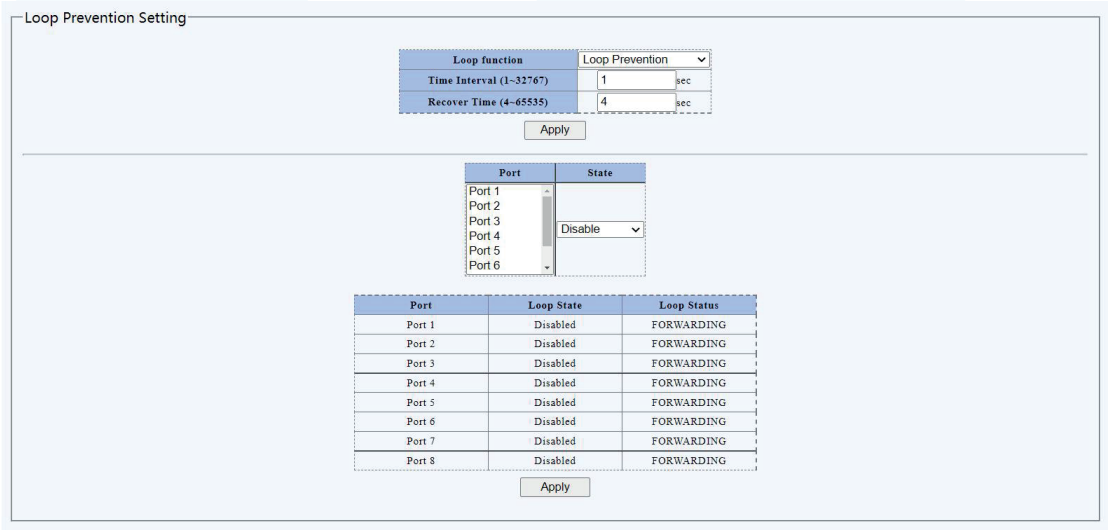


Figure 2.3.6-2 Loop Prevention Page

Loop detection: After this function is enabled, it can detect whether there i s a loop in the link, and the loop indicator will start flashing.

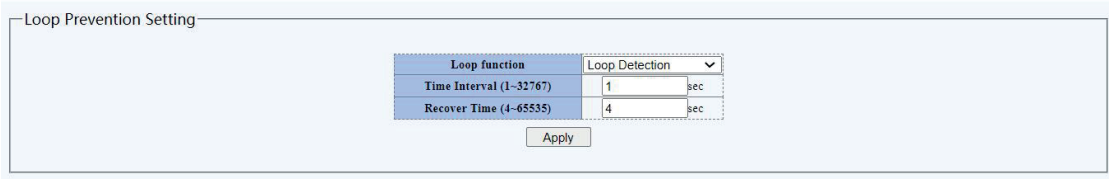


Figure 2.3.6-3 Loop Detection

Spanning Tree: Enable this function to directly open the RSTP global.

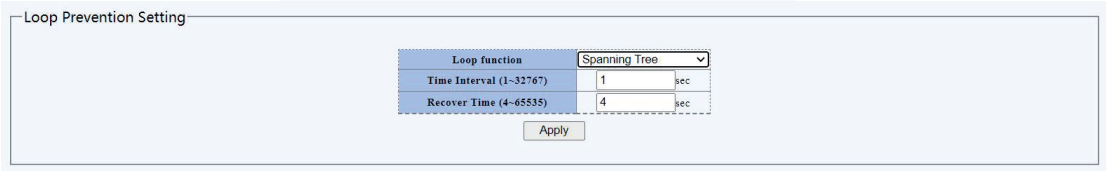


Figure2.3.6-4 Spanning tree

2. 3. 7 RSTP Global

RSTP: (rapid spanning Tree Protocol) Rapid Spanning Tree Protocol is turned on in Loop Protection. This protocol can converge the network more quickly when the network structure changes, and is used as a backup of the designated port.

STP: Spanning Tree Protocol. The protocol can be applied to the loop network to achieve path redundancy through a certain algorithm, and at the same time, the loop network is pruned into a loop-free tree network, so as to avoid the proliferation and infinite circulation of messages in the loop network.

After opening this page, you can configure the RSTP/STP protocol and priority according to the actual environment.

Spanning tree priority: small priority, default 32768, step length 4096, value range 0 ~ 61440.

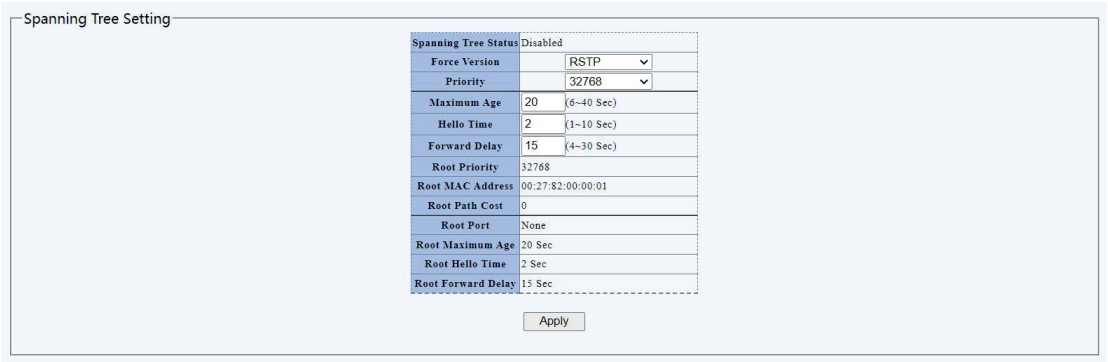


Figure 2.3.7 RSTP Global Page

2. 3. 8 RSTP port

After RSTP is enabled, relevant ports can be configured on this page

Path Cost, an STP metric used to represent the distance between bridges. Path Cost is the sum of all link costs along the path between two bridges.

Port priority: small priority, default 128, step 16, value range 0 ~ 240.

Point-to-point: It means that the sender transmits data to the device directly connected to it, and this device transmits data to the next device directly connected to it at an appropriate time, and the data is transmitted to the receiving end through one directly connected device.

In RSTP, when a non-edge designated port moves from blocking to forwarding, the handshake with the downstream bridge must ensure that the link is a point-to-point link.

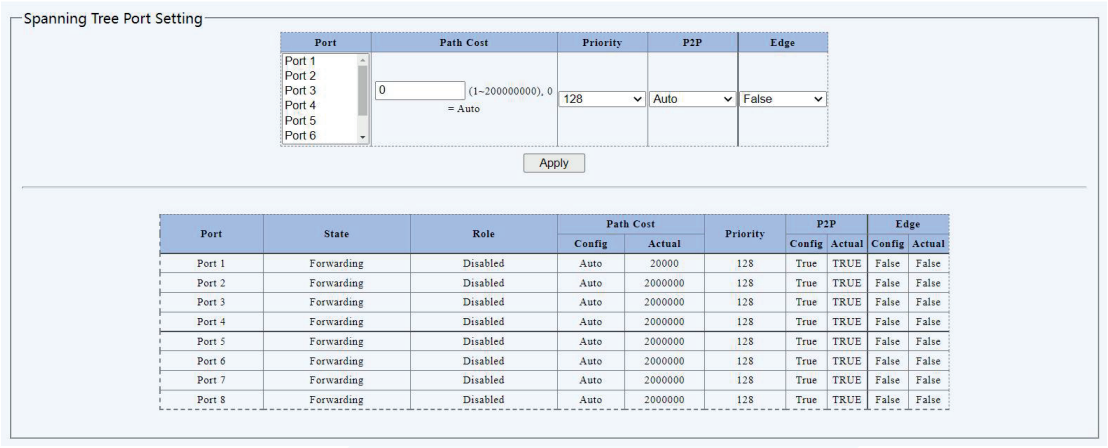


Figure 2.3.8 RSTP Ports Page

2. 3. 9 Port mirroring

The port mirror function can be set to copy the data of the specified direction of the port to the mirror port. Up to 4 sets of port mirroring can be set.

Mirror direction:

Ingress mirroring: Mirrors only the traffic coming in from that port.

Egress mirroring: Only the traffic originating from this port is mirrored.

Bidirectional mirroring: supports the mirroring of bidirectional traffic to and from the port.

Mirror Port: The port to which the port is mirrored. The mirrored data will be sent to this port. For example, in a packet capture application, this interface is used to connect to a computer running packet capture software.

Mirrored Port: The data source port of the port mirroring function. Packets in the specified direction of the mirrored port will be copied to the mirroring port.

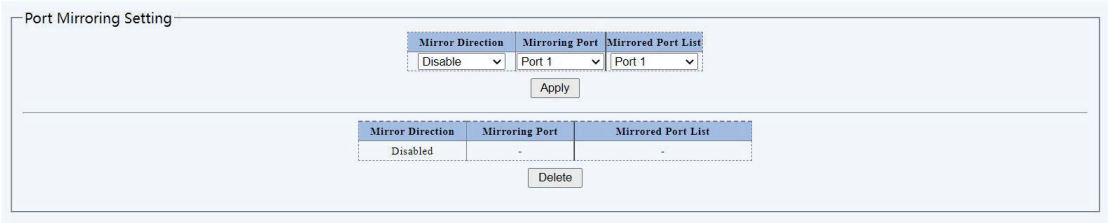


Figure 2.3.9-1 Port Mirroring Page

For example, as shown in 2.3.9-2, the computer installed by the administr ator with packet capture software is connected to port 1 of the switch, and the data sent by the computer connected to port 2 needs to be analyzed by packe t capture.

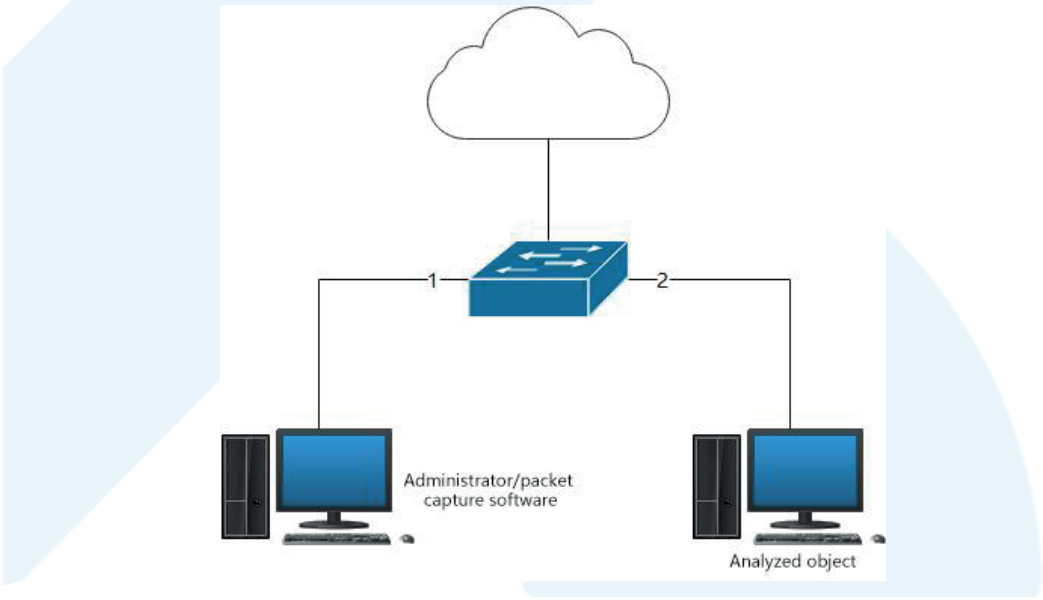


Figure 2. 3. 9−2

As shown in Figure 2.3.9-3, the direction is RX (the message sent by the device connected to the switch is received by the switch port), the monitoring port is 1, and the mirrored port is 2.

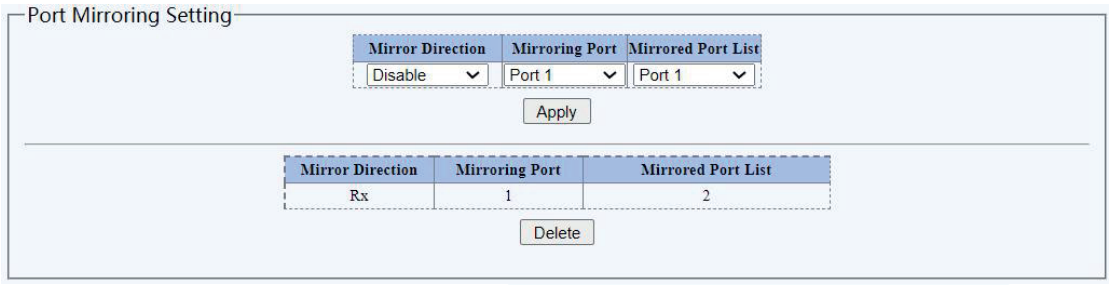


Figure 2. 3. 9-3

2. 3. 10 Port Isolation

The port isolation function can realize the two-layer data isolation betwee n different ports, and can not communicate with each other. By default, all port s are not isolated from each other.

Port: The object port to set.

Allow Forwarding Ports: Ports that are allowed to communicate with the object port, that is, ports that are not isolated from the object port mirror. Exce pt for the allowed forwarding port, the other ports cannot communicate with th e object port.

When adding ports, you can hold down the mouse and drag to select mul tiple consecutive ports. When selecting non-consecutive ports, you can hold d own the "Ctrl" key to select multiple ports or deselect the corresponding ports.

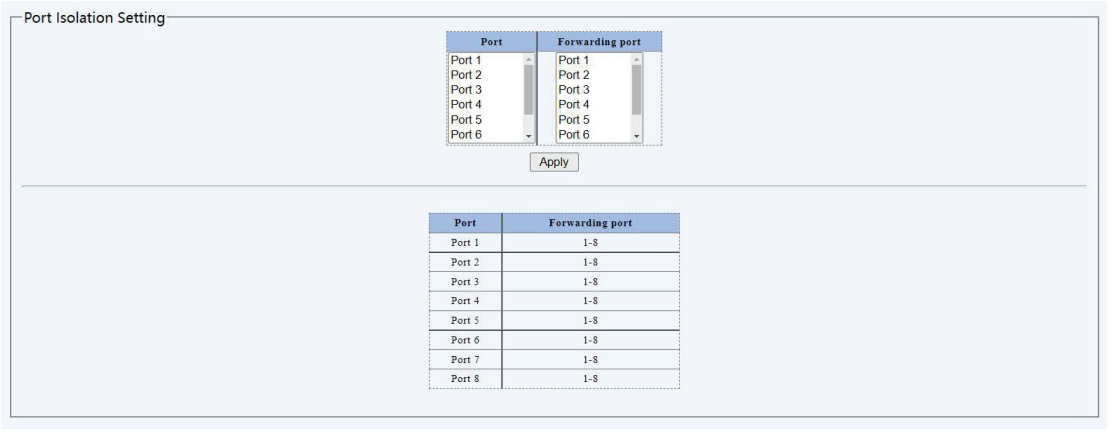


Figure 2.3.10-1 Port Isolation Page

For example, as shown in Figure 2.3. 10-2, the five ports of the switch are con nected to the Internet through the router, and the five ports are connected to a server. It is required that all terminals on ports 1-3 cannot communicate with each other, but they are allowed to access the Internet and the server.

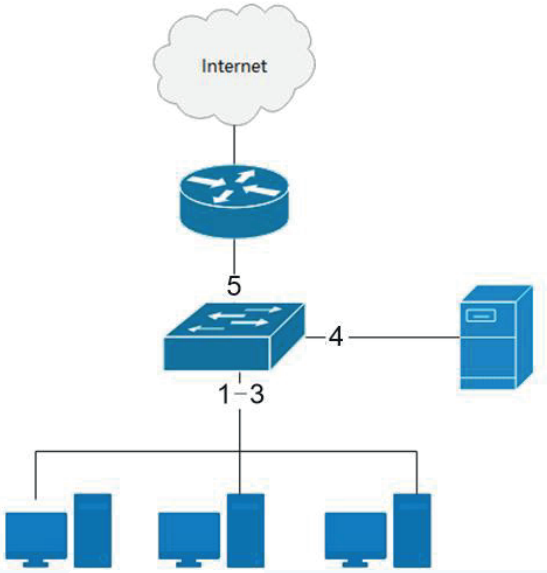


Figure2. 3. 10-2

Select ports 1-3 in the port column, select ports 4 and 5 in the allowed for warding port column, and click Apply. As shown in Figure 2.3.10-3:

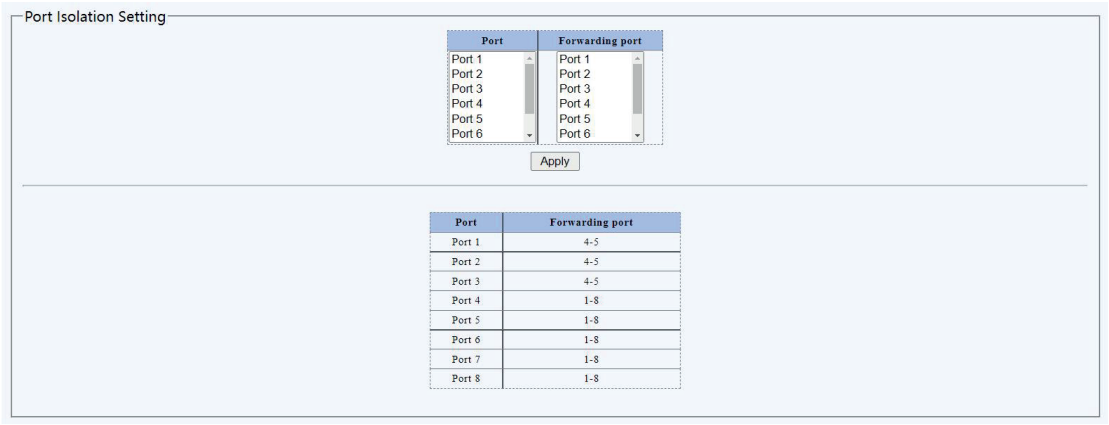


Figure2. 3. 10−3

Isolation cannot be set for all upstream ports.

In general, it is necessary to ensure that the uplink port is located in the allowed forwarding port of all object ports to ensure normal communicati on with the superior device.

2. 3. 11 Bandwidth Control

Bandwidth control limits the maximum rate for a specified port and directi on, with a minimum control granularity of 16Kbps.

Port: The object port to set.

Type: inlet or outlet

Status: Enable or disable the bandwidth control function of the object por t.

Rate: The maximum rate of throttling. The rate value must be an integer multiple of 16.

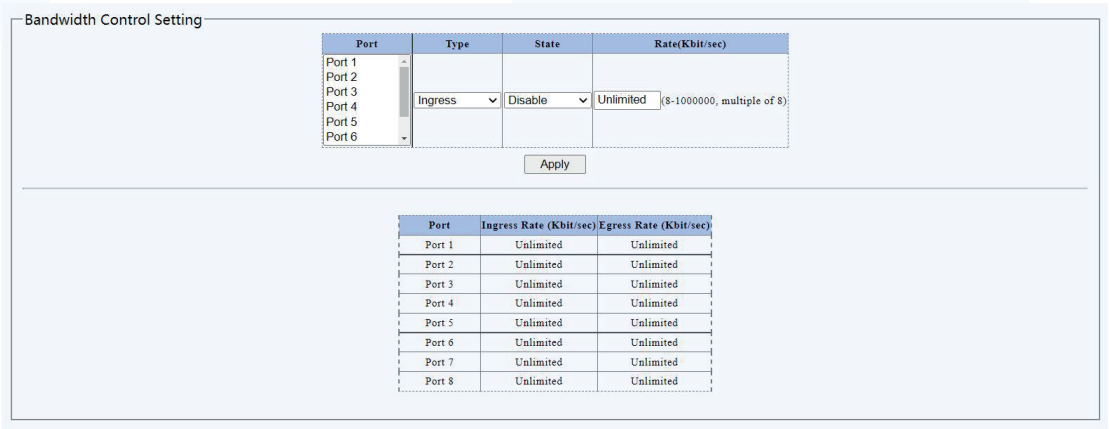


Figure 2.3.11 Broadband Control Page

2. 3. 12 Jumbo frame

Jumbo frames are Ethernet frames with payloads that exceed the 1500-byte limit of the IEEE 802.3 standard.

The minimum setting value of this series of switches is 1522 bytes, and the maximum is 9216 bytes.

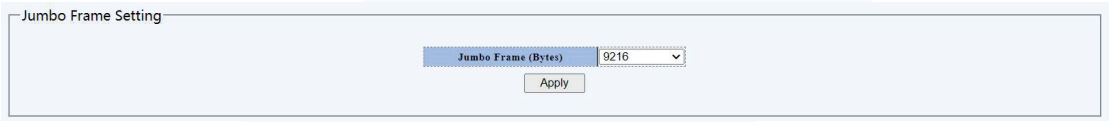


Figure 2.3.12 Jumbo Frame Page

2. 3. 13 MAC constraint

Learn the overflow action mode: Flooding. The switch forwards frames coming in from a certain interface through other non-receiving interfaces. Flooding is a point-to-multipoint operation (flooding is flooding within a VLAN, and there is isolation between VLANs).

Discard, where the switch discards a frame received from an interface without forwarding it

Effective after application

MAC constraint setting, select the corresponding port and open it, set the limit range (0-2112) as required, and it will take effect after application and saving.

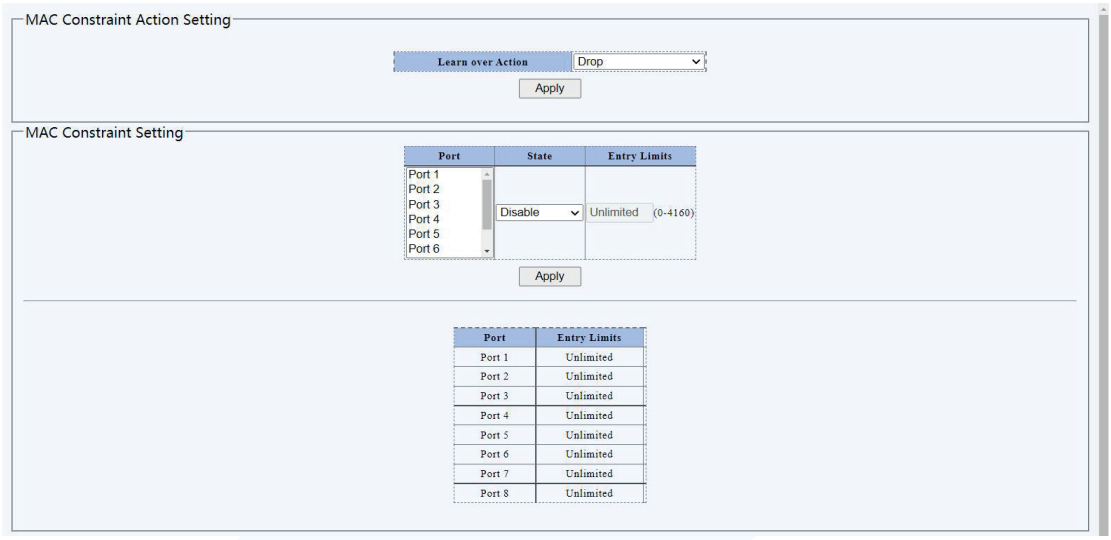


Figure 2.3.13 MAC Constraints Page

2. 3. 14 Green Ethernet

The port enters an inactive mode and saves power while keeping the port management state open. Click Open and Apply to take effect.

Figure 2.3.14 Green Ethernet Page

2. 3. 15 EEE

When this function is turned on, the switch will automatically turn off some idle circuits, effectively reducing power consumption and saving energy.

Figure 2.3.15 EEE Page

2.4 safe

2.4.1 MAC Addr

2.4.1.1 MAC table

This page shows the access MAC information under the port.

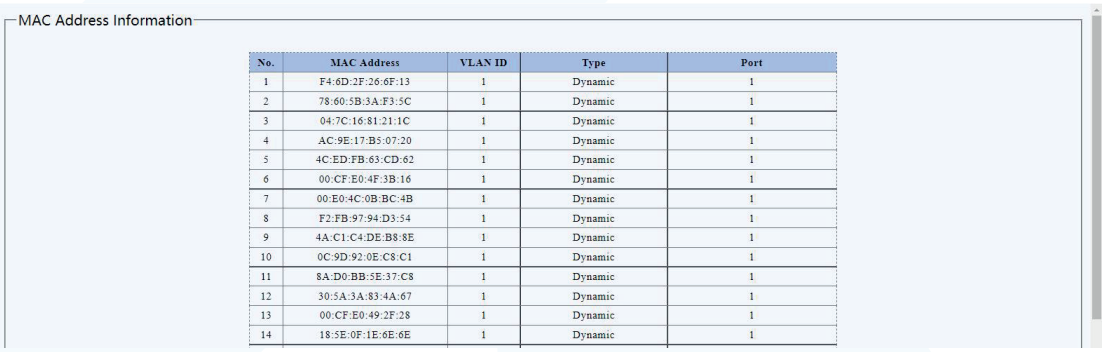


Figure 2.4.1.1 MAC Table Page

2.4.1.2 MAC lookup

Select the MAC address to be queried and the VLAN according to the act ual access and query. If the queried MAC is correct, the system will display th e corresponding port. An error indicates that it was not found.

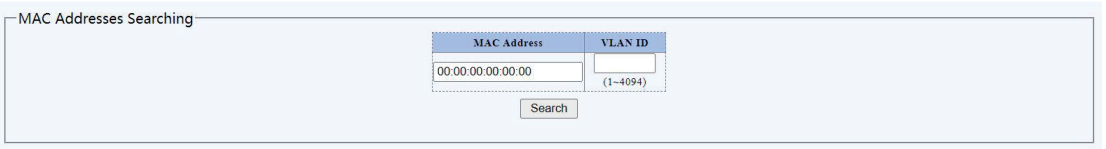


Figure 2.4.1.2 MAC Lookup Page

2. 4. 1. 3 Static MAC

The static MAC function can be set to bind or block the specified MAC on the specified port and VLAN.

MAC address: controlled MAC address object.

VLAN ID: The VLAN ID of the role (integer between 1-4094).

Port: The active port (when not selected, it is effective for all ports).

Source MAC blocking: controlled mode. If it is checked, the MAC address will be blocked. If it is not checked, the MAC address will be bound.

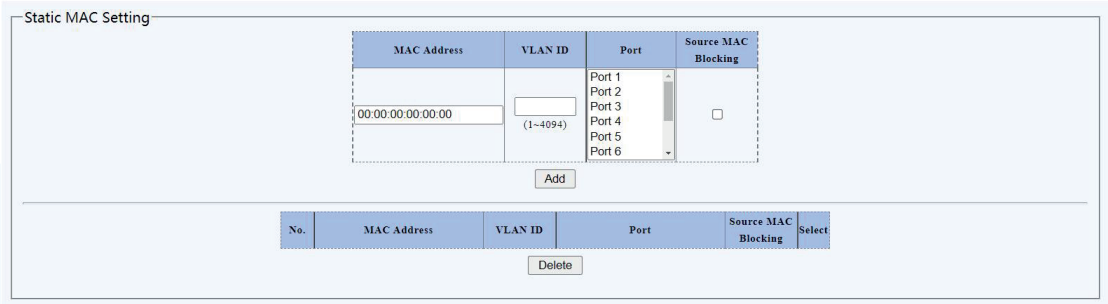


Figure2.4.1.3-1 Static MAC page

For example, as shown in Figure 2.4. 1.3-2, the configuration example binds the MAC address 94: E1: AC: C5: e9: E0 to port 3 and VLAN 1. At this point, the device will not be able to communicate if it is connected to another port or VLAN.

No.	MAC Address	VLAN ID	Port	Select
1	94:E1:AC:C5:E9:E0	1	3	☐

Figure2.4.1.3-2

2. 4. 2 Broadcast Storm

The storm control function can limit the packet rate of broadcast, multi-dia l, unknown unicast and unknown multicast types of the specified port.

Storm type: controlled data packet type, including broadcast, multicast, u nknown unicast and unknown multicast.

Port: acting port (multiple choices are allowed).

Status: Specifies whether the type of packet control on the port is on or o ff.

Speed: Maximum speed (in PPS, packets per second)

Select the corresponding port to select the type and speed to be suppres sed. After the state is opened, click Apply to take effect.

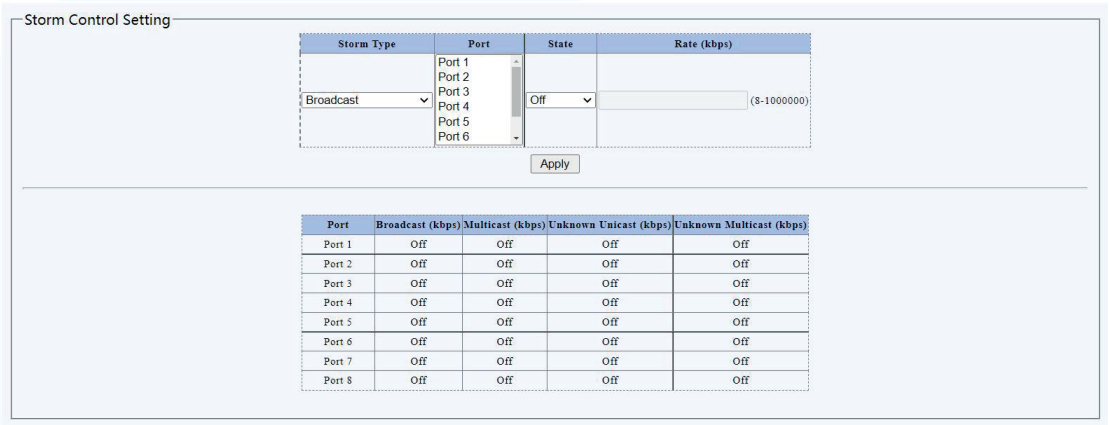


Figure 2.4.2 Broadcast Storm Page

2.5 Monitor

2.5.1 Port Statistics

Port statistics status shows the management status, link status, and statis tics of sent and received packets of the port.

Click the "Clear" button to clear the statistics.

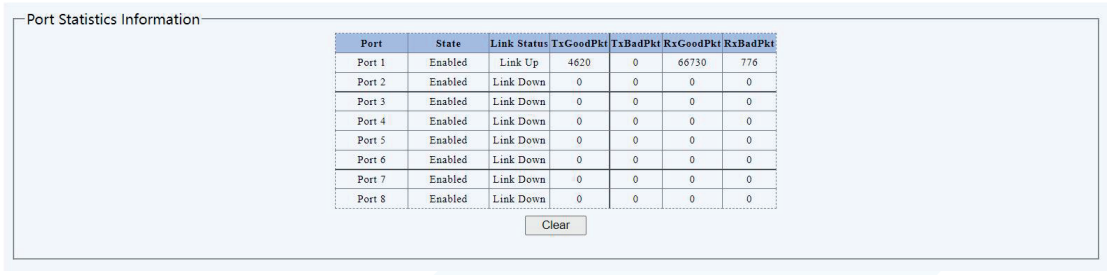


Figure 2.5.1 Port Statistics Page

2.5.2 Cable Diagnostics

Select the corresponding port to test the cable, and click Apply to take eff ect.

Figure 2.5.2 Cable Diagnostics Page

2.6 tool

2.6.1 Firmware upgrade

Select the required files and upgrade them.

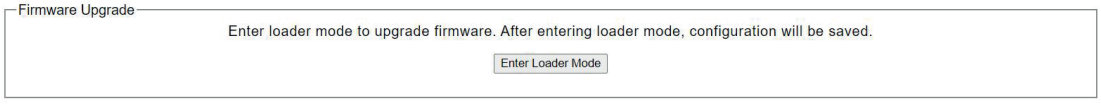


Figure 2.6.1 Firmware Upgrade Page

2.6.2 Configure Backup

Back up the current configuration file of the switch. Click Backup to generate a backup configuration file.

Restore the backup configuration file, select the configuration to be restored, and click Upgrade. After the upgrade is successful, restart to take effect.

Figure 2.6.2 Configuration Backup Page

2.6.3 Reset

Restore the switch to the factory default setting state, and click "Restore factory default" to restart the switch to take effect.

When the web management interface cannot be restored due to configuration errors or other reasons, press and hold the reset key of the switch until all the indicators flash to restore the factory settings.

Figure 2.6.3 Reset Page

2.6.4 save

Save the changes made in the management page. The unsaved configur ation will be lost on the next reboot.

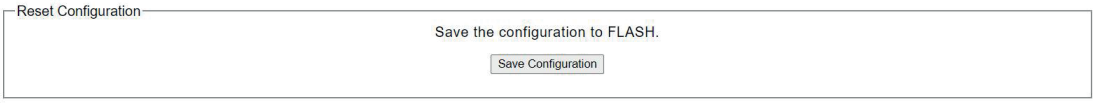


Figure 2.6.4 Save Page

2.6.5 Timed restart

Perform scheduled restart configuration operation on the switch as requir ed, select the corresponding time of each week and the corresponding hour of each day, and enable the scheduled restart function to take effect after saving .

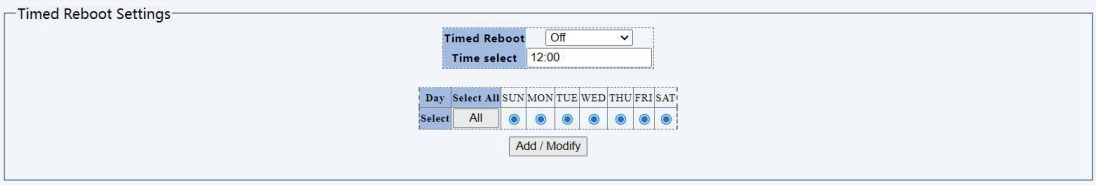


Figure 2.6.5 Timed Restart Page

2.6.6 Manual Restart

Restart the switch. Click Restart to restart the switch.

Figure 2.6.6 Manual Restart Page

2.6.7 Logout

Select the logout button to exit the current WEB interface.

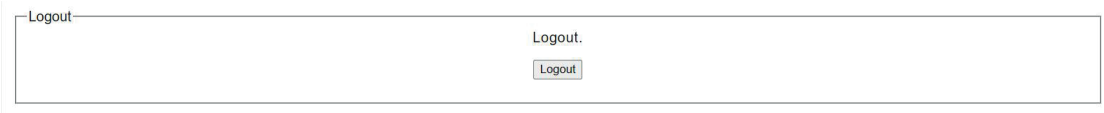


Figure 2.6.7 Logoff Page