
Light network management series

WEB Network Management Operation Guid

Ver 1.0.1

Tech Soppot: support@sodola-network.com

Declare

Copyright, all rights reserved

The copyright of this manual belongs to our company. Without the written permission of our company, no unit or individual may extract or copy part or all of the contents of this book without authorization, and may not disseminate it in any form.

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. The system uses a new software and hardware platform to provide a comprehensive security protection system, simple VLAN switching, port isolation and so

on. The light network management series is easy to manage and maintain, and is an ideal convergence layer switch for office networks, campus networks, small and medium-sized enterprises, and branch offices.

[Version Update]

Ver 1.01

User experience optimization

Resolves known issues and provides faster response.

Perfect support for one-key conversion between Chinese and English.

Related functions are optimized to make management easier.

Directory

Chapter 1 Login Management Interface	6
1.1 Preparation for login	6
1.2 Login steps	7
Chapter 2 WEB Management Function	8
2.1 Interface description	8
2.2 System	9
2.2.1 System information	9
2.2.2 IP Settings	9
2.2.3 SNTP Settings	10
2.2.4 User account	11
2.2.5 Port Settings	11
2.3 POE (standard PoE family support only)	12
2.3.1 PoE Port Configuration	12
2.3.2 PoE Port Status	13
2.4 Configuration	14
2.4.1 VLAN Settings	14
2.4.2 QoS	19
2.4.3 Loop Settings	20
2.4.4 IGMP snooping	23
2.4.5 DHCP snooping	23
2.4.6 Link Aggregation	25
2.4.7 Port Mirroring	26
2.4.8 Port Isolation	28
2.4.9 Bandwidth control	30
2.4.10 Jumbo Frame	31

2.4.11 MAC Constraints	31
2.4.12 EEE	32
2.5 Safety	32
2.5.1 MAC Addr	32
2.5.2 Broadcast Storm	34
2.6 Monitoring	35
2.6.1 Port statistics	35
2.7 Tools	35
2.7.1 Firmware Upgrade	35
2.7.2 Configuration backup	36
2.7.3 Reset	36
2.7.4 Save	37
2.7.5 Timed restart	37
2.7.6 Manual restart	38
2.7.7 Log Out	38

Chapter 1 Login Management Interface

1.1 Preparation for login

1. The switch is powered on and started normally, and any interface is connected to the 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 the function switch series is supported);
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 shall be installed on the management computer;
4. The IP address of the network card connecting the management computer and the switch must be in the same network segment as the management IP address of the switch. It should be 192.168. 0. * (* is any integer between 2 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 into the switch (function switch series only).

1.2 Login steps

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 user name and password in the pop-up login window. The default user name and password are admin.

The image shows a login window with a light blue background. It contains two text input fields: 'Username' and 'Password'. Below these fields are two radio buttons for language selection: '中文' (Chinese) and 'English'. The 'English' radio button is selected. At the bottom center is a 'Login' button.

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

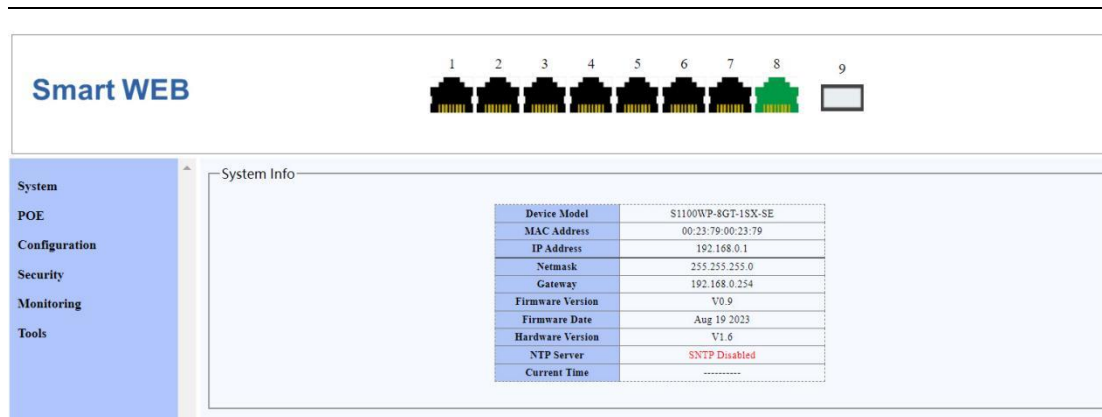


Figure 1.2 Switch System Page

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 in the connected state, and uncolored indicates that the port is in the unconnected state.
- 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.

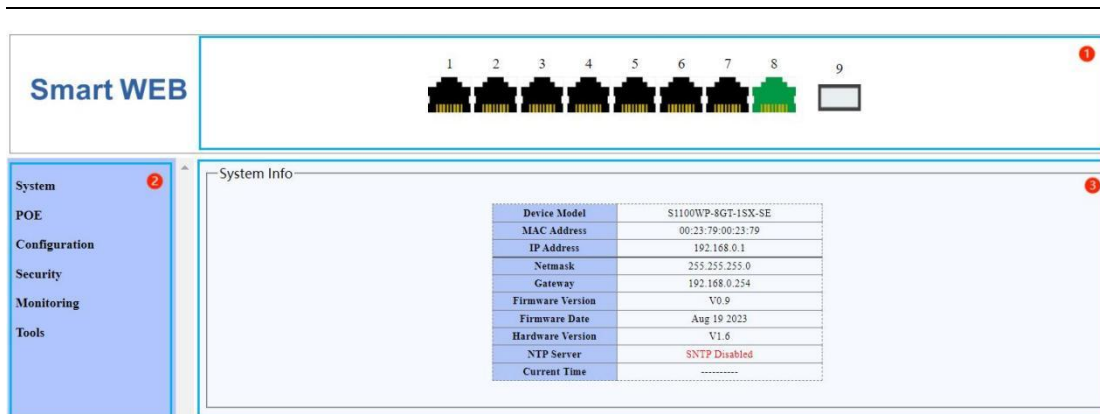


Figure 2.1 Interface Description

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 hardware version information.

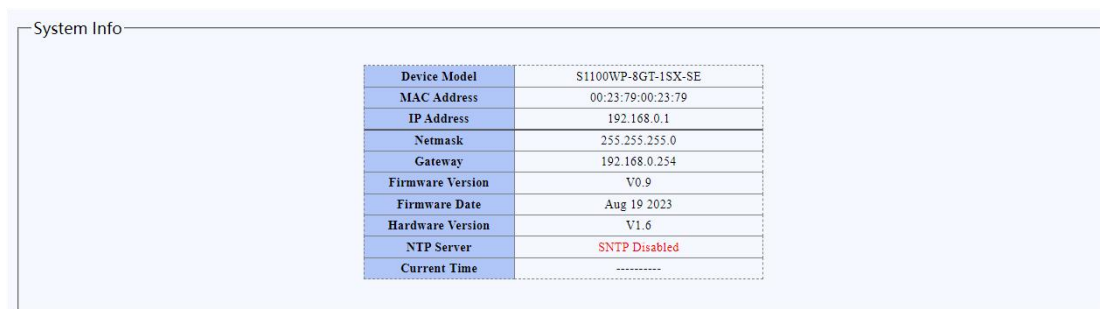


Figure 2.2.1 System Information Page

2.2.2 IP Settings

Display and set the management IP address of the switch.

When the IP mode is "static IP", you can manually configure the IP address, subnet mask, and gateway information.

When the IP mode is "DHCP", the switch will automatically obtain the IP information through the DHCP server in the network.

DHCP Setting	Disable
IP Address	192.168.0.1
Netmask	255.255.255.0
Gateway	192.168.0.254

Apply

Figure 2.2.2 IP Settings Page



When switching the IP mode, it is necessary to log in the switch again; After modifying the management IP application, it is necessary to log in with a new IP address and ensure that the network segment of the management computer matches it.

2. 2. 3 SNTP Settings

Simple Network Time Protocol, adapted from NTP, is mainly used to synchronize computer clocks in the Internet.

In this interface, the corresponding time service area can be added to synchronize the time of the time switch and the time server. The specific situation can be viewed in the system configuration.

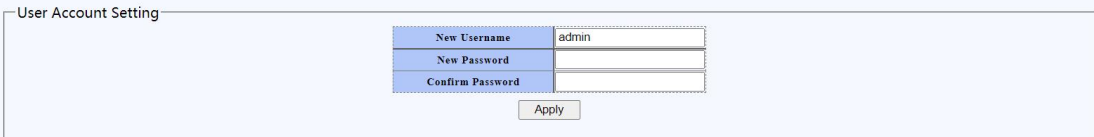
SNTP Setting	Disable
Time Server IP	182.92.12.11
Time Server IP(Backup)	185.209.85.222
Time Zone(Ex: 8 or -3)	8

Apply

Figure 2.2.3 SNTP Setting Page

2. 2. 4 User account

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



The screenshot shows a web interface titled "User Account Setting". It contains a table with three rows: "New Username" with the value "admin", "New Password", and "Confirm Password". Below the table is an "Apply" button.

New Username	admin
New Password	
Confirm Password	

Apply

Figure 2.2.4 User Account Page

2. 2. 5 Port Settings

On the port setting page, the user sets and displays the port status, including the following contents:

Port: select the port to be set

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

Rate/Duplex: All interfaces default to the "auto" state, that is, adaptive mode. It can 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 select "Automatic" mode;

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

Port Setting

Port	State	Speed/Duplex	Flow Control
Port 1			
Port 2			
Port 3			
Port 4	Enable	Auto	Off
Port 5			
Port 6			
Port 7			
Port 8			

Apply

Port	State	Speed/Duplex	Flow Control
Port 9	Enable	Auto	Off

Apply

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

Figure 2.2.5 Port Settings Page

2.3 POE (standard PoE family support only)

2.3.1 PoE Port Configuration

Port: select the port to be set for PoE (only the network port supporting PoE)

PoE management status: Open by default, and the port PoE can be closed.

PoE protocol type: the corresponding power supply protocol can be selected according to the actual situation.

AF: 802.3 AF (POE) maximum power 15.4 W

ATs: 802.3 ATs (POE +) maximum power 30 W

Hi: Hi-PoE supports a maximum power of 60W (Note: unconventional functions are only supported by individual series, see the specifications for detail)

s)

BT: 802.3 BT (POE + +) Max. Power 90W (Note: Unconventional functions are only supported by individual series, see specifications for details)

PoEDog: After this port is opened, the port will be POE restarted when the data of the port is lost for more than 3 minutes.

PoE Port Configuration

Total PoE Power(W) 120

Port	PoE Admin Status	PoE Protocol Type	PoEDog
Port 1			
Port 2			
Port 3			
Port 4	Enable	BT	Disable
Port 5			
Port 6			
Port 7			
Port 8			

Apply

Port	PoE Admin Status	PoE PSE Type	PoE Dog
Port 1	Enable	BT	Disable
Port 2	Enable	AT	Disable
Port 3	Enable	AT	Disable
Port 4	Enable	AT	Disable
Port 5	Enable	AT	Disable
Port 6	Enable	AT	Disable
Port 7	Enable	AT	Disable
Port 8	Enable	AT	Disable

Figure 2.3.1 PoE Port Configuration

2.3.2 PoE Port Status

This page is used to display the PoE port status, and select to restart the corresponding PoE port according to the actual situation.

PoE Port Status

Consumption (W) 0.0 Power Usage (%) 0

Port	Admin Status	PSE Type	PoEDog	Operation	Class	Power(W)	Voltage(V)	Current(mA)	Reset
Port 1	Enable	BT	Disable	Off	-	-	-	-	Reset
Port 2	Enable	AT	Disable	Off	-	-	-	-	Reset
Port 3	Enable	AT	Disable	Off	-	-	-	-	Reset
Port 4	Enable	AT	Disable	Off	-	-	-	-	Reset
Port 5	Enable	AT	Disable	Off	-	-	-	-	Reset
Port 6	Enable	AT	Disable	Off	-	-	-	-	Reset
Port 7	Enable	AT	Disable	Off	-	-	-	-	Reset
Port 8	Enable	AT	Disable	Off	-	-	-	-	Reset

Figure 2.3.2 PoE Port Status

2.4 Configuration

2.4.1 VLAN Settings

2.4.1.1 802.1Q VLAN

Static VLANs are used to set 802.1 Q VLAN properties for a switch port.

VLAN : Identifier used to distinguish different VLANs. Terminals between different VLANs cannot communicate directly.

VLAN name: The name or description of the corresponding VLAN, which is usually used to distinguish different VLANs intuitively.

Without label: for the port marked as having no label, when the data frame goes out of the port, if it is a frame with VLAN label, the label will be removed and then sent out. If there is no label, the data frame will be sent directly. Data frames entering the port are internally tagged with the VLAN of the port. Commonly use for access terminal equipment.

Tag Label: The port identified as a label carries the VLAN label when the data frame is sent to the port. Therefore, the peer device must be able to identify 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 managed switch.

Non-member: When the port is checked, it means that the current port is not a member port of this VLAN.

Add/Modify VLAN

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

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

Click "Add/Modify" button below.

Delete a VLAN

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

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

802.1Q VLAN

VLAN	[1-4094]									VLAN Name
Port	Select All	1	2	3	4	5	6	7	8	9
Untagged	All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Tagged	All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Not Member	All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add / Modify

VLAN	VLAN Name	Member Ports	Tagged Ports	Untagged Ports	Delete
1		1-9		1-9	<input type="checkbox"/>

Delete Select All

Figure 2.4.1.1 802.1 Q VLAN Page

2.4.1.2 802.1Q VID

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 the port with the PVID. The default PVID for all ports is 1.

Receive frame format

All: The designated port processes the received frame regardless of whether it is 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.

Only with label: The designated port only receives labeled data frames. G

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.

Only unlabeled: The designated 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.

VLAN Port Setting

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

Apply

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

Figure 2.4.1.2-1 802.1 Q VLD Page

For example, as shown in the 2.4.1.2 -2, the superior device has been configured with VLANs 10, 20, and 30, and the corresponding VLAN is allowed to pass through the port connected to the switch. The three terminals connected to port 1, 2 and 3 of this machine are respectively planned to VLAN 10, 20 and 30.

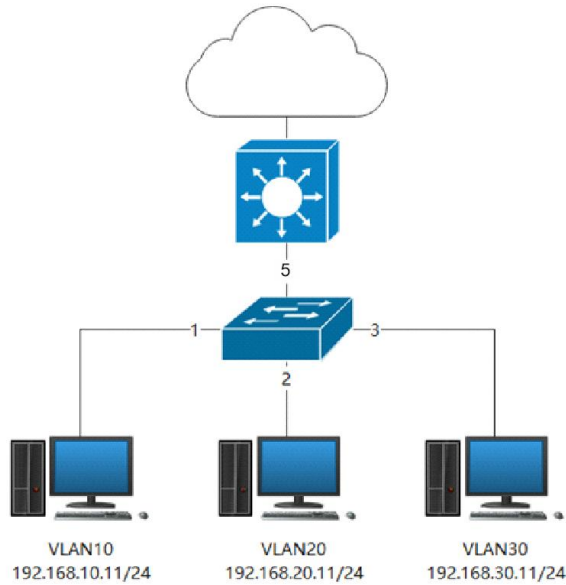


Figure 2.4.1.2-2

Start by adding the appropriate VLAN and port settings on the Static VLAN N page. Take VLAN 10 as an example, fill in VLAN ID 10, select No Label under port 1, select Label under port 5, and click Add. When all VLANs have been added, you should see Figure 2.4. 1.2-3.

802.1Q VLAN

VLAN	(1-4094)									VLAN Name	
Port	Select All	1	2	3	4	5	6	7	8	9	
Untagged	All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Tagged	All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Not Member	All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Add / Modify

VLAN	VLAN Name	Member Ports	Tagged Ports	Untagged Ports	Delete
1		1-9	-	1-9	<input type="checkbox"/>
10	10	1,5	5	1	<input type="checkbox"/>
20	20	2,5	5	2	<input type="checkbox"/>
30	30	3,5	5	3	<input type="checkbox"/>

Delete Select All

Figure 2.4.1.2-3

Then enter the "VLAN Port Settings" page, select port 1, fill in PVID 10, and click Apply. Set port 2 and port 3 respectively according to this method, and set PVID to 20 and 30 respectively, as shown in Figure 2.4. 1.2 -4.

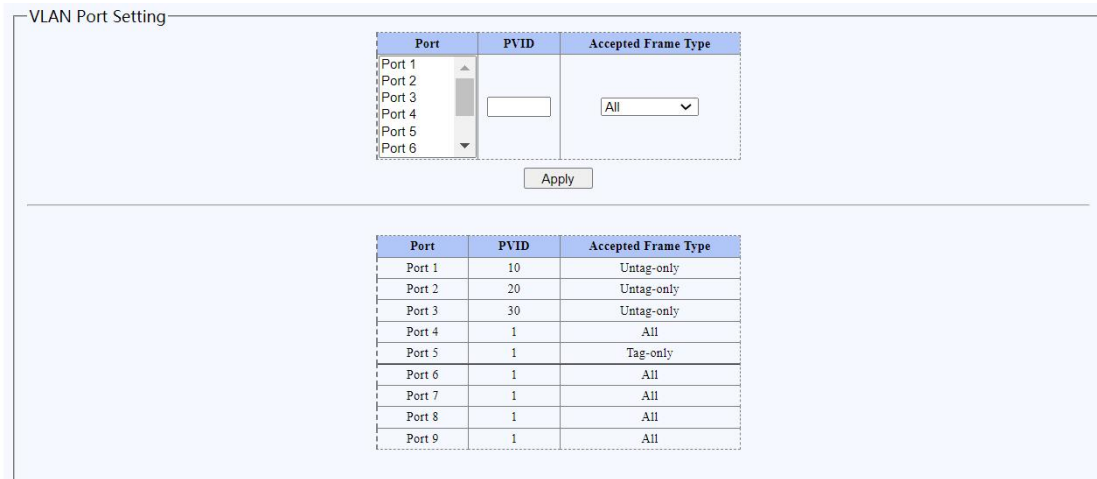


Figure 2.4.1.2-4

For example, as shown in the figure 2.4, 1.2 -5. When multiple broadband need to be accessed, but the number of available physical interfaces of the router is insufficient, it is necessary to expand the Wan port through the switch (this function needs to be supported by the router function).

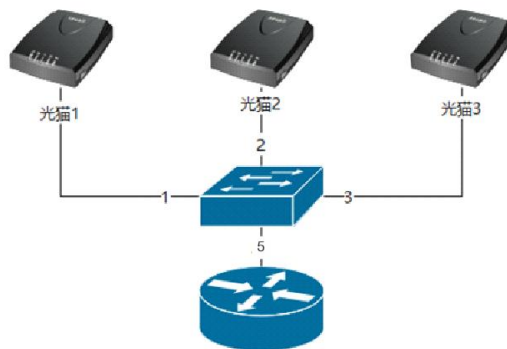


Figure 2.4.1.2-5

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 subint

erface or related Wan port configuration in the router.

2.4.2 QoS

2.4.2.1 Port to queue

The port queue selection page configures the corresponding queue (queue range 1-8) for the switch port.

Port	Queue
Port 1	1
Port 2	1
Port 3	1
Port 4	1
Port 5	1
Port 6	1
Port 7	1
Port 8	1
Port 9	1

Figure 2.4.2.1 Port to Queue Page

2.4.2.2 Queue weight

Configure the weight priority of the set queue (the range is 0-15)

Queue	Weight
1	Strict priority
2	Strict priority
3	Strict priority
4	Strict priority
5	Strict priority
6	Strict priority
7	Strict priority
8	Strict priority

Figure 2.4.2.2 Queue Weight Page

2. 4. 3 Loop Settings

2. 4. 3. 1 Loop protocol

Loop protocol settings are divided into three main categories, namely, enable loop detection, loop avoidance, and spanning tree.

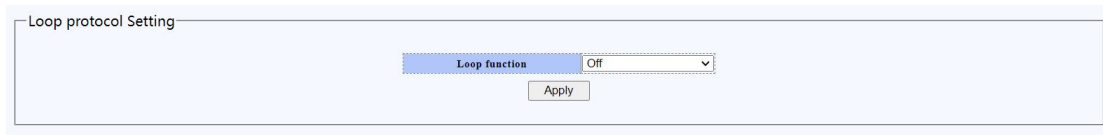


Figure 2.4.3.1-1 Loop Detection Page

Loop detection: After this function is enabled, it can detect whether there is a loop in the link, and the corresponding loop port indicator will flash at the same time. (Such as the 1-2 loop in Figure 2.4.3.1-3)

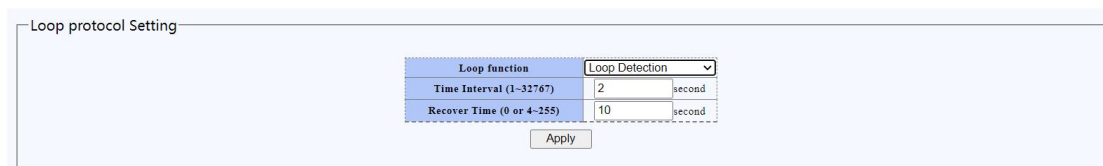


Figure 2.4.3.1-2 Open Loop Detection

Loop avoidance: When this feature is enabled, the switch will block the corresponding looped port when there is a loop on the link.

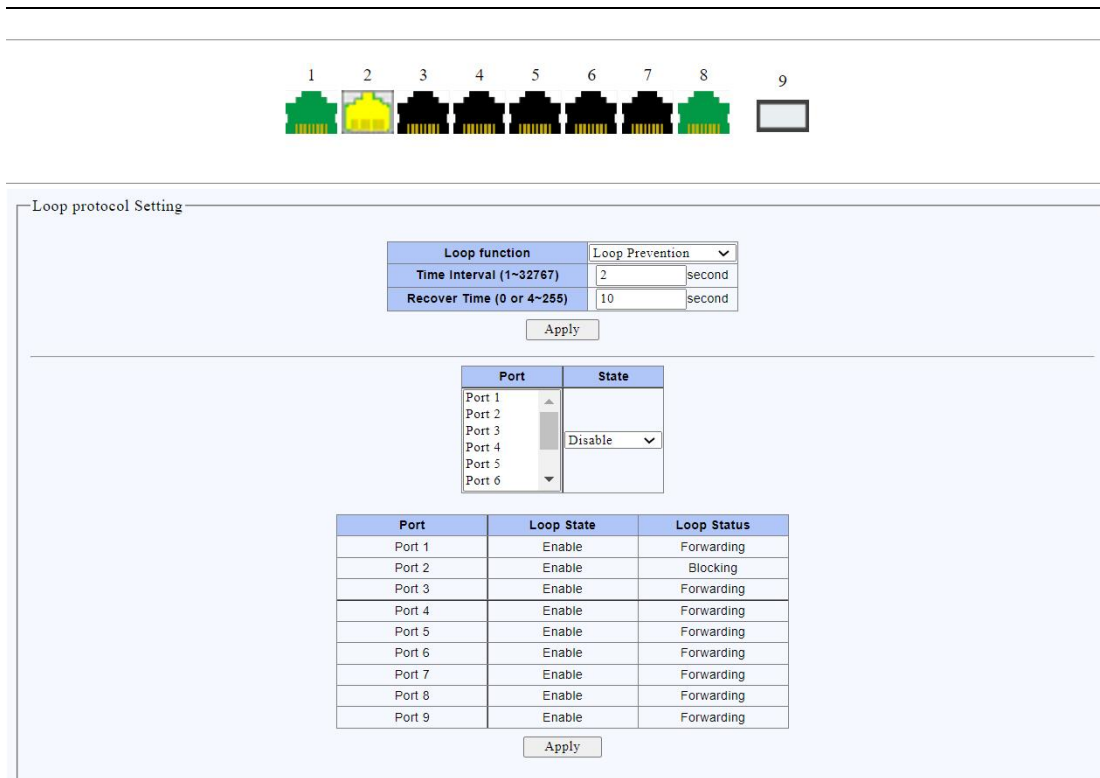


Figure 2.4.3.1-3 Loop Avoidance

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



Figure 2.4.3.1-4 Spanning Tree

2. 4. 3. 2 STP 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, RSTP/STP protocol, priority and other related configurations can be configured according to the actual environment.

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



Spanning Tree Setting

Spanning Tree Status	Disable	
Force Version	RSTP	▼
Priority	32768	▼
Maximum Age	20	(6-40 Sec)
Hello Time	2	(1-10 Sec)
Forward Delay	15	(4-30 Sec)
Root Priority	32768	
Root MAC Address	00:23:79:00:23:79	
Root Path Cost	0	
Root Port	-	
Root Maximum Age	20 Sec	
Root Hello Time	2 Sec	
Root Forward Delay	15 Sec	

Apply

Figure 2.4.3.2 STP Global Page

2. 4. 3. 3 STP Port

After enabling STP/RSTP, relevant ports can be configured on this page.

Path Cost, an STP metric that represents the distance between bridges.

Path Cost is the sum of the costs of all links on the path between two bridges.

Port priority: small priority, default 128, step size 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.

Spanning Tree Port Setting

Port	Path Cost	Priority	P1P	Edge
Port 1	0 (1~200000000),0=Auto	128	Auto	False
Port 2				
Port 3				
Port 4				
Port 5				
Port 6				

Apply

Port	State	Role	Path Cost		Priority	P1P		Edge	
			Config	Actual		Config	Actual	Config	Actual
Port 1	Forwarding	Disabled	Auto	2000000	128	Auto	Unknown	False	False
Port 2	Forwarding	Disabled	Auto	2000000	128	Auto	Unknown	False	False
Port 3	Forwarding	Disabled	Auto	2000000	128	Auto	Unknown	False	False
Port 4	Forwarding	Disabled	Auto	2000000	128	Auto	Unknown	False	False
Port 5	Forwarding	Disabled	Auto	2000000	128	Auto	Unknown	False	False
Port 6	Forwarding	Disabled	Auto	2000000	128	Auto	Unknown	False	False
Port 7	Forwarding	Disabled	Auto	2000000	128	Auto	Unknown	False	False
Port 8	Forwarding	Disabled	Auto	20000	128	Auto	Unknown	False	False
Port 9	Forwarding	Disabled	Auto	2000000	128	Auto	Unknown	False	False

Figure 2.4.3.3 STP Ports Page

2. 4. 4 IGMP snooping

Turn on/off the IGMP enable setting.

IGMP Snooping is a multicast constraint mechanism. Switches use it to dynamically register multicast groups. Switches running IGMP Snooping manage and control multicast groups by snooping and analyzing IGMP messages exchanged between hosts and multicast routers, which can effectively inhibit the diffusion of multicast data in the network.

IGMP Enable Setting

Enable

Apply

Dump IGMP entry

IP Address	Port	VLAN ID

Figure 2.4.4 IGMP Settings Page

2. 4. 5 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.

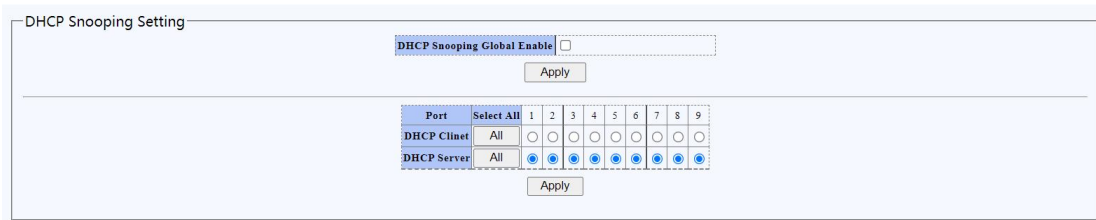


Figure 2.4.5-1 DHCP Snooping Page

For example, as shown in Figure 2.4.5-2, port 5 of the switch is connected to a router as a legal DHCP server to allocate an IP address to an intranet terminal, and port 4 is connected to an illegal DHCP server.

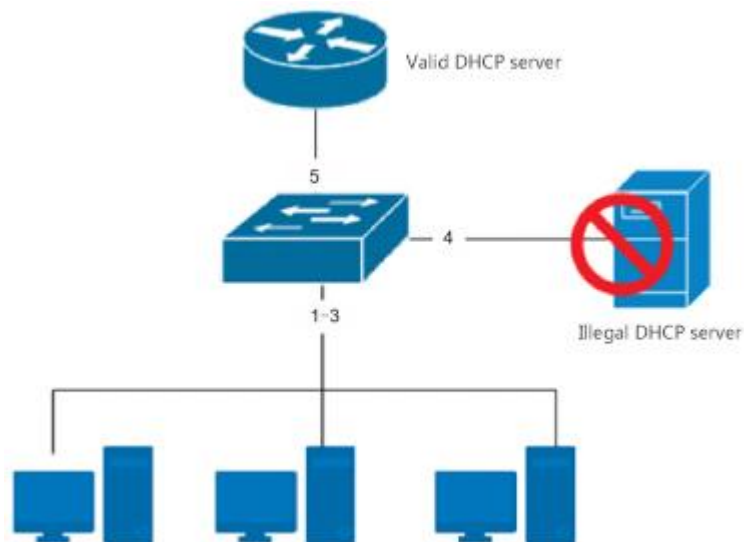


Figure 2.4.5-2

As shown in figure 2.4.5-3. Select port 1-3 as DHCP Client and port 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 prevent DHCP servers other than 4-5 from providing illegal address allocation services.

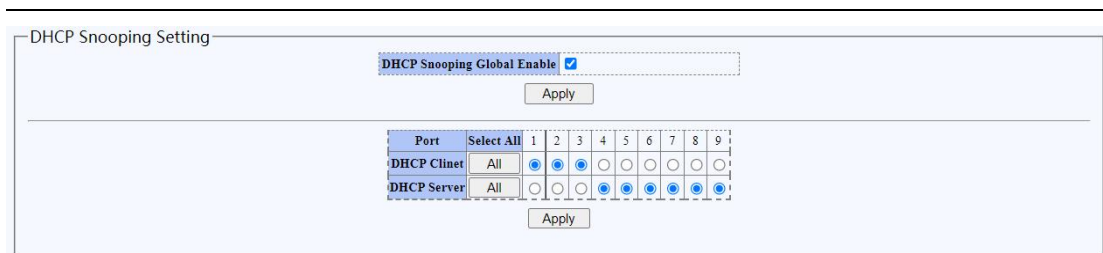


Figure 2.4.5-3

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 the port selected as the DHCP Client obtains the address through the DHCP service for normal communication, if the switch is restarted, the binding relationship will be invalid and the communication cannot be performed. The device needs to obtain the address through the DHCP again for normal communication.

2. 4. 6 Link Aggregation

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

The switch supports 2 aggregation groups, and each aggregation group can 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.

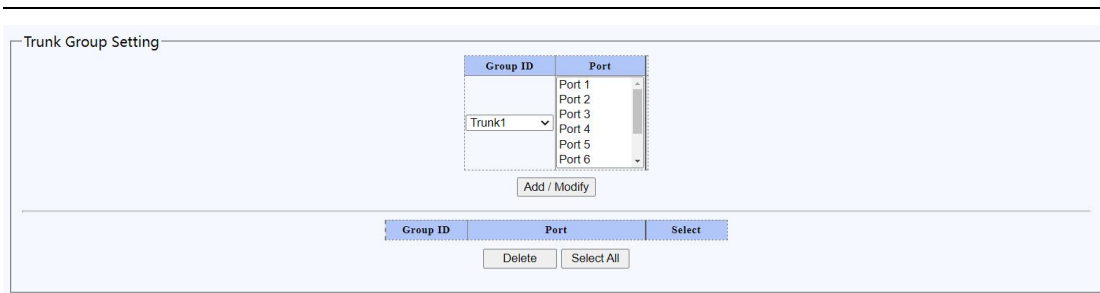


Figure 2.4.6 Link Aggregation Page



The corresponding port of the peer device needs to be configured accordingly, otherwise it may cause aggregation failure or loop problems due to the closure of the port by the spanning tree protocol.

2.4.7 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:

- (1) Ingress mirroring: Only the traffic entering from this port is mirrored.
- (2) Exit mirroring: Only the traffic from the port is mirrored.
- (3) Bidirectional mirroring: supports the mirroring of the bidirectional traffic received and sent by the port.

Mirror port: The target port of the port mirror. 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. The data packet in the specified direction of the mirrored port will be copied to the mirroring port.

Port Mirroring Setting

Mirror Direction	Mirroring Port	Mirrored Port List
Rx	Port 1	Port 1

Apply

Mirror Direction	Mirroring Port	Mirrored Port List
Rx	1	2

Delete

Figure 2.4.7-1 Port Mirror Page

For example, as shown in 2.4.7-2, the computer installed by the administrator 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 packet capture.

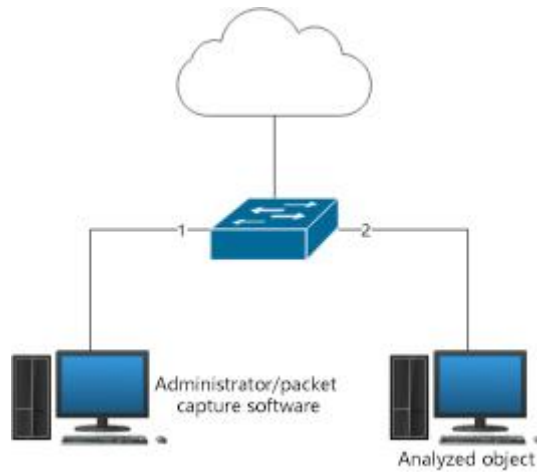


Figure 2.4.7-2

As shown in Figure 2.4.7-3, the direction is RX (the message sent by the device connected to the switch is received by the switch port), the mirror port is 1, and the mirrored port is 2.

Port Mirroring Setting

Mirror Direction	Mirroring Port	Mirrored Port List
Rx	Port 1	Port 1

Apply

Mirror Direction	Mirroring Port	Mirrored Port List
Rx	1	2

Delete

Figure 2.4.7-3

2.4.8 Port Isolation

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

Port: Set the object port.

Port isolation list: set the port allowed to forward

Port Isolation Setting

Port	Port Isolation List
Port 1	Port 1
Port 2	Port 2
Port 3	Port 3
Port 4	Port 4
Port 5	Port 5
Port 6	Port 6

Apply

Port	Port Isolation List
Port 1	1-9
Port 2	1-9
Port 3	1-9
Port 4	1-9
Port 5	1-9
Port 6	1-9
Port 7	1-9
Port 8	1-9
Port 9	1-9

Figure 2.4.8-1 Port Isolation Page

For example, as shown in Figure 2.4. 8-2, the five ports of the switch are connected 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.

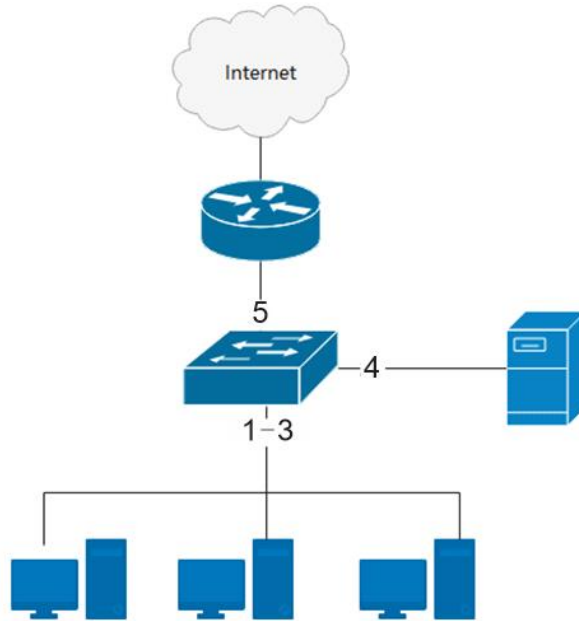


Figure 2.4.8-2

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 2.4.8-3:

Port Isolation Setting

Port	Port Isolation List
Port 1	Port 1
Port 2	Port 2
Port 3	Port 3
Port 4	Port 4
Port 5	Port 5
Port 6	Port 6

Apply

Port	Port Isolation List
Port 1	5
Port 2	5
Port 3	5
Port 4	1-9
Port 5	1-9
Port 6	1-9
Port 7	1-9
Port 8	1-9
Port 9	1-9

Figure 2.4.8-3



Isolation cannot be set on 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 communication with the superior device.

2.4.9 Bandwidth control

The bandwidth control function can limit the maximum rate of a specified port and direction, with a minimum control granularity of 16 Kbps.

Port: Set the object port.

Type: inlet or outlet

Status: The bandwidth control function of the object port is turned off or on.

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

Bandwidth Control Setting

Port	Type	State	Rate(Kbit/sec)
Port 1			
Port 2			
Port 3			
Port 4	Ingress	Disable	Unlimited (0-2500000, multiple of 16)
Port 5			
Port 6			

Apply

Port	Type	State	Rate(Kbit/sec)
Port 9	Ingress	Disable	Unlimited (0-10000000, multiple of 16)

Apply

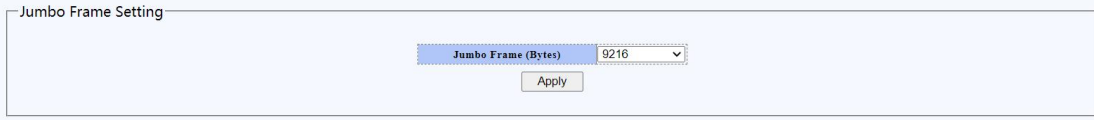
Port	Ingress Rate (Kbit/sec)	Egress Rate (Kbit/sec)
Port 1	Unlimited	Unlimited
Port 2	Unlimited	Unlimited
Port 3	Unlimited	Unlimited
Port 4	Unlimited	Unlimited
Port 5	Unlimited	Unlimited
Port 6	Unlimited	Unlimited
Port 7	Unlimited	Unlimited
Port 8	Unlimited	Unlimited
Port 9	Unlimited	Unlimited

Figure 2.4.9 Broadband Control Page

2. 4. 10 Jumbo Frame

Jumbo frames are Ethernet frames whose payload exceeds the IEEE 802.3 standard limit of 1500 bytes.

The minimum setting value of this series of switches is 1522 bytes, and the maximum is 16383 bytes.



Jumbo Frame Setting

Jumbo Frame (Bytes) 9216

Apply

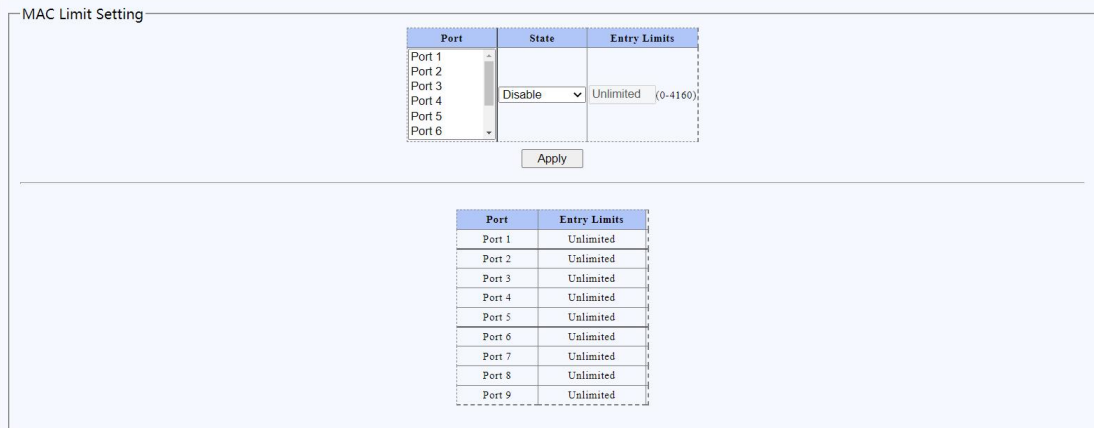
Figure 2.4.10 Jumbo Frame Page

2. 4. 11 MAC Constraints

Port: Select the port to be set

Status: off or on

Limited number: unlimited number (0-4160)



MAC Limit Setting

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

Apply

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

Figure 2.4.11 MAC Constraints Page

2.4.12 EEE

After this function is enabled, the switch will automatically turn off part of the idle circuit, effectively reducing power consumption and saving energy.

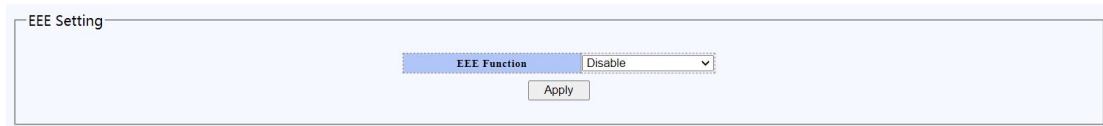


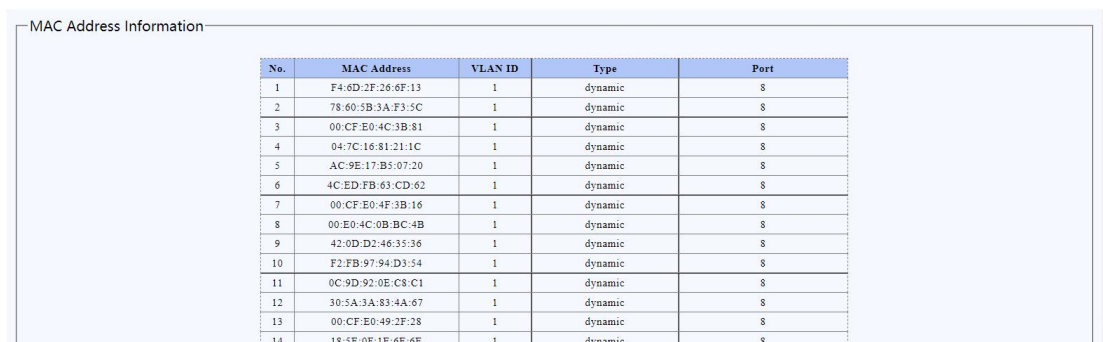
Figure 2.4.12 EEE Page

2.5 Safety

2.5.1 MAC Addr

2.5.1.1 MAC lookup

Select the MAC address and VLAN to be queried according to the actual access and query. If the MAC is queried correctly, the system will display the corresponding port. The error indicates that it is not found.



The screenshot shows a table titled "MAC Address Information". The table has five columns: No., MAC Address, VLAN ID, Type, and Port. It contains 14 rows of data.

No.	MAC Address	VLAN ID	Type	Port
1	F4:6D:2F:26:6F:13	1	dynamic	8
2	78:60:5B:3A:F3:5C	1	dynamic	8
3	00:CF:E0:4C:3B:81	1	dynamic	8
4	04:7C:16:81:21:1C	1	dynamic	8
5	AC:9E:17:B3:07:20	1	dynamic	8
6	4C:ED:FB:63:CD:62	1	dynamic	8
7	00:CF:E0:4F:3B:16	1	dynamic	8
8	00:E0:4C:0B:BC:4B	1	dynamic	8
9	42:0D:D2:46:35:36	1	dynamic	8
10	F2:FB:97:94:D3:54	1	dynamic	8
11	0C:9D:92:0E:C8:C1	1	dynamic	8
12	30:5A:3A:83:4A:67	1	dynamic	8
13	00:CF:E0:49:2F:28	1	dynamic	8
14	18:5E:0F:1E:6E:6E	1	dynamic	8

Figure 2.5.1.1 MAC Lookup Page

2.5.1.2 Static MAC

The static MAC function can be set to bind 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.

Static MAC Setting

MAC Address	VLAN ID	Port
94:E1:AC:C5:E9:E0	1 (1~4094)	Port 1 Port 2 Port 3 Port 4 Port 5 Port 6

Add

No.	MAC Address	VLAN ID	Port	Select
1	94:E1:AC:C5:E9:E0	1	3	<input type="checkbox"/>

Delete

Figure 2.5.1.2-1 Static MAC Page

For example, as shown in Figure 2.5.1.2-2, 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	<input type="checkbox"/>

Figure 2.5.1.2-2

2.5.2 Broadcast Storm

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

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

Port: acting port (multiple choices are allowed).

Status: The packet control function of this type on the specified port is enabled or disabled.

Speed: Maximum upper limit speed (unit: PPS, i.e., packets per second)

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

Storm Control Setting

Storm Type	Port	State	Rate (kbps)
Broadcast	Port 1 Port 2 Port 3 Port 4 Port 5 Port 6	Off	(1-2500000)(kbps)

Apply

Storm Type	Port	State	Rate (kbps)
Broadcast	Port 9	Off	(1-10000000)(kbps)

Apply

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

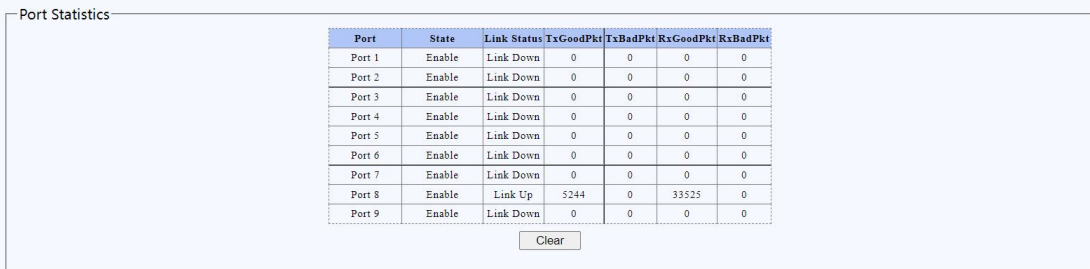
Figure 2.5.2 Broadcast Storm Page

2.6 Monitoring

2.6.1 Port statistics

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

Click the "Clear" button to clear the statistical information.



Port	State	Link Status	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt
Port 1	Enable	Link Down	0	0	0	0
Port 2	Enable	Link Down	0	0	0	0
Port 3	Enable	Link Down	0	0	0	0
Port 4	Enable	Link Down	0	0	0	0
Port 5	Enable	Link Down	0	0	0	0
Port 6	Enable	Link Down	0	0	0	0
Port 7	Enable	Link Down	0	0	0	0
Port 8	Enable	Link Up	5244	0	33525	0
Port 9	Enable	Link Down	0	0	0	0

Clear

Figure 2.6.1 Port Statistics Page

2.7 Tools

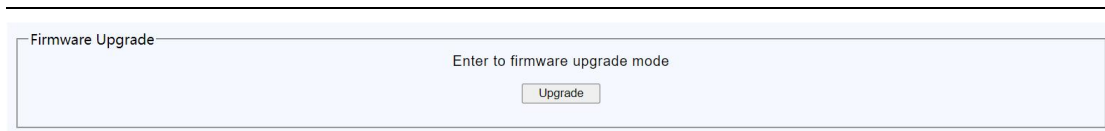
2.7.1 Firmware Upgrade

The Firmware Update page contains configuration export, import, and firmware upgrade functions.

Export configuration: Export the configuration on the switch for configuration backup.

Import configuration: Import the backup configuration into the switch for configuration recovery.

Firmware upgrade: update the switch system software, and click to enter firmware upgrade.



After entering the post-upgrade tool, you can select the corresponding file to upgrade, or restart and exit the page.

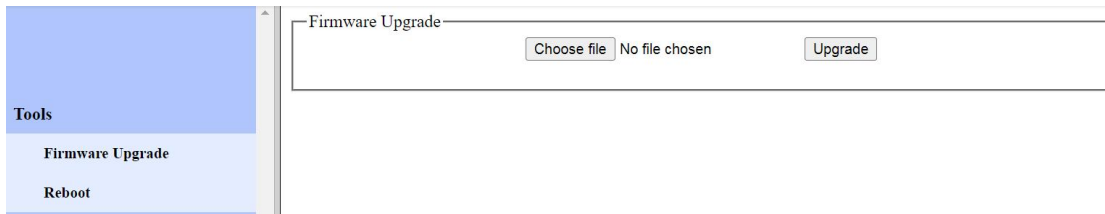


Figure 2.7.1 Firmware Upgrade Page

2. 7. 2 Configuration backup

Backup configuration: export the configuration on the switch for configuration backup.

Restore configuration: import the backup configuration into the switch to restore the configuration. When restoring, select the configuration to be restored and click Upgrade. After the upgrade is successful, restart to take effect.

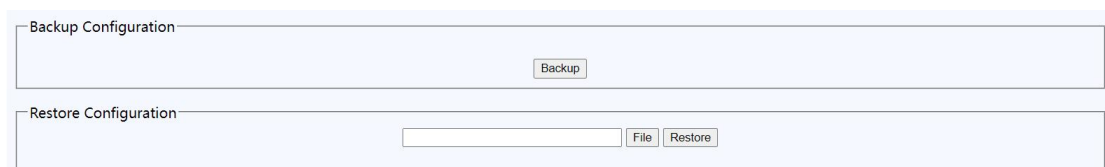


Figure 2.7.2 Configure Backup Page

2. 7. 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 the reset key of the switch for a long time until all the indicator lights flash, and then the factory settings can be restored.

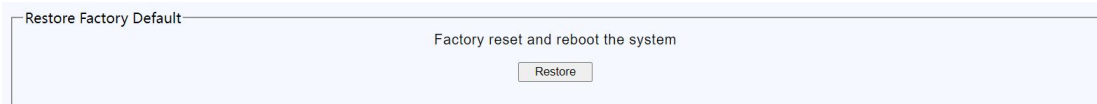


Figure 2.7.3 Reset Page

2.7.4 Save

Save the changes made in the administration page. The unsaved configuration will be lost on the next reboot.



Figure 2.7.4 Save Page

2.7.5 Timed restart

Perform timing restart configuration operation on the switch according to the requirements, select the corresponding time of each week and the corresponding time of each day, and enable the timing restart function to take effect after saving.

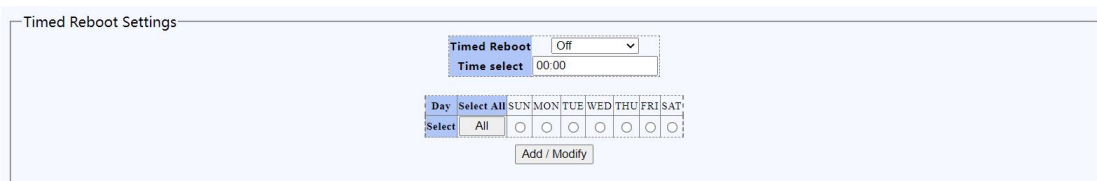


Figure 2.7.5 Timed Restart Page

2.7.6 Manual restart

Restart the switch. Click Restart to restart the switch.



Figure 2.7.6 Manual Restart Page

2.7.7 Log Out

Select the logout button and the switch will exit the current WEB interface

