



Dahua 10/100/1000 Mbps Industrial Managed PoE Switch Web Config Manual

V1.0.0

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:

The number one reason systems get "hacked" is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

2. Update Firmware

As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

"Nice to have" recommendations to improve your network security

1. Change Passwords Regularly

Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

2. Change Default HTTP and TCP Ports:

- Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.
- These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

3. Enable HTTPS/SSL:

Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

4. Enable IP Filter:

Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

5. Change ONVIF Password:

On older IP Camera firmware, the ONVIF password does not change when you change the system's credentials. You will need to either update the camera's firmware to the latest revision or manually change the ONVIF password.

6. Forward Only Ports You Need:

- Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.
- You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

7. Disable Auto-Login on SmartPSS:

Those using SmartPSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

8. Use a Different Username and Password for SmartPSS:

In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system.

9. Limit Features of Guest Accounts:

If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

10. UPnP:

- UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors.

- If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real applications.

11. SNMP:

Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

12. Multicast:

Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

13. Check the Log:

If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

14. Physically Lock Down the Device:

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.

15. Connect IP Cameras to the PoE Ports on the Back of an NVR:

Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.

16. Isolate NVR and IP Camera Network

The network your NVR and IP camera resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.

Foreword

General






This Web Config Manual (hereinafter referred to as "the Manual") introduces operations on web interface of Dahua Gigabit Industrial Managed PoE Switch. The Ethernet Switch supports web access. You can visit the switch on web browser, and configure and manage the switch.

Models

DH-PFS4207-4GT-DP

Safety Instructions

The following categorized signal words with defined meaning might appear in the Manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
 TIPS	Provides methods to help you solve a problem or save you time.
 NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

No.	Version	Revision Content	Release Time
1	V1.0.0	First Release	February, 2019

Privacy Protection Notice

As the device user or data controller, you might collect personal data of other such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to:

providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

About the Manual

- The Manual is for reference only. If there is inconsistency between the Manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the Manual.
- The Manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the Manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the Manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the Manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

The Manual helps you to use our product properly. To avoid danger and property damage, read the Manual carefully before using the product, and we highly recommend you to keep it well for future reference.

Operating Requirements

- Do not expose the device directly to the sunlight, and keep it away from heat.
- Do not install the device in the damp environment, and avoid dust and soot.
- Make sure the device is in horizontal installation, and install the device on solid and flat surface to avoid falling down.
- Avoid liquid spattering on the device. Do not place object full of liquid on the device to avoid liquid flowing into the device.
- Install the device in the well-ventilated environment. Do not block the air vent of the device.
- Use the device at rated input and output voltage.
- Do not disassemble the device without professional instruction.
- Transport, use, and store the device in allowed ranges of humidity and temperature.

Power Supply Requirements

- Use the battery properly to avoid fire, explosion, and other dangers.
- Replace the battery with battery of the same type.
- Use locally recommended power cord in the limit of rated specifications.
- Use the standard power adapter. We will assume no responsibility for any problems caused by nonstandard power adapter.
- The power supply shall meet the SELV requirement. Use the power supply that conforms to Limited Power Source, according to IEC60950-1. Refer to the device label.
- Adopt GND protection for I-type device.
- The coupler is the disconnecting apparatus. Keep it at the angle for easy to operate.

Table of Contents

Cybersecurity Recommendations	I
Foreword	III
Important Safeguards and Warnings	V
1 Login the Switch	7
2 Quick Settings	9
2.1 System Info	9
2.2 Local	10
2.3 vLAN.....	10
2.4 Aggregation	11
2.4.1 Static Aggregation Configuration	12
2.4.2 Dynamic Aggregation Configuration	12
2.5 IP and routes.....	13
3 Advanced Settings	16
3.1 Common Configuration	16
3.1.1 System Configuration	16
3.1.2 Port configuration.....	22
3.1.3 VLAN Configuration	23
3.1.4 Aggregation.....	25
3.1.5 MAC Table	27
3.1.6 Spanning Tree	31
3.2 Seldom-used Configuration	34
3.2.1 ERPS	34
3.2.2 ACL	42
3.2.3 Loop Protection.....	45
3.2.4 Security	45
3.2.5 IGMP Snooping	50
3.2.6 QoS.....	52
3.2.7 SNMP.....	61
3.2.8 DHCP Server	65
3.2.9 LLDP	67
3.2.10 Serial Config	错误!未定义书签。
3.2.11 PoE	70
4 Maintenance	74
4.1 System Reboot.....	74
4.2 Restore Default	74
4.3 Config Manage.....	74
4.3.1 Export Config file	74
4.3.2 Upload Config file.	75
4.4 Software Update	75
4.5 Mirror	75
4.6 Ping	77

1 Login the Switch

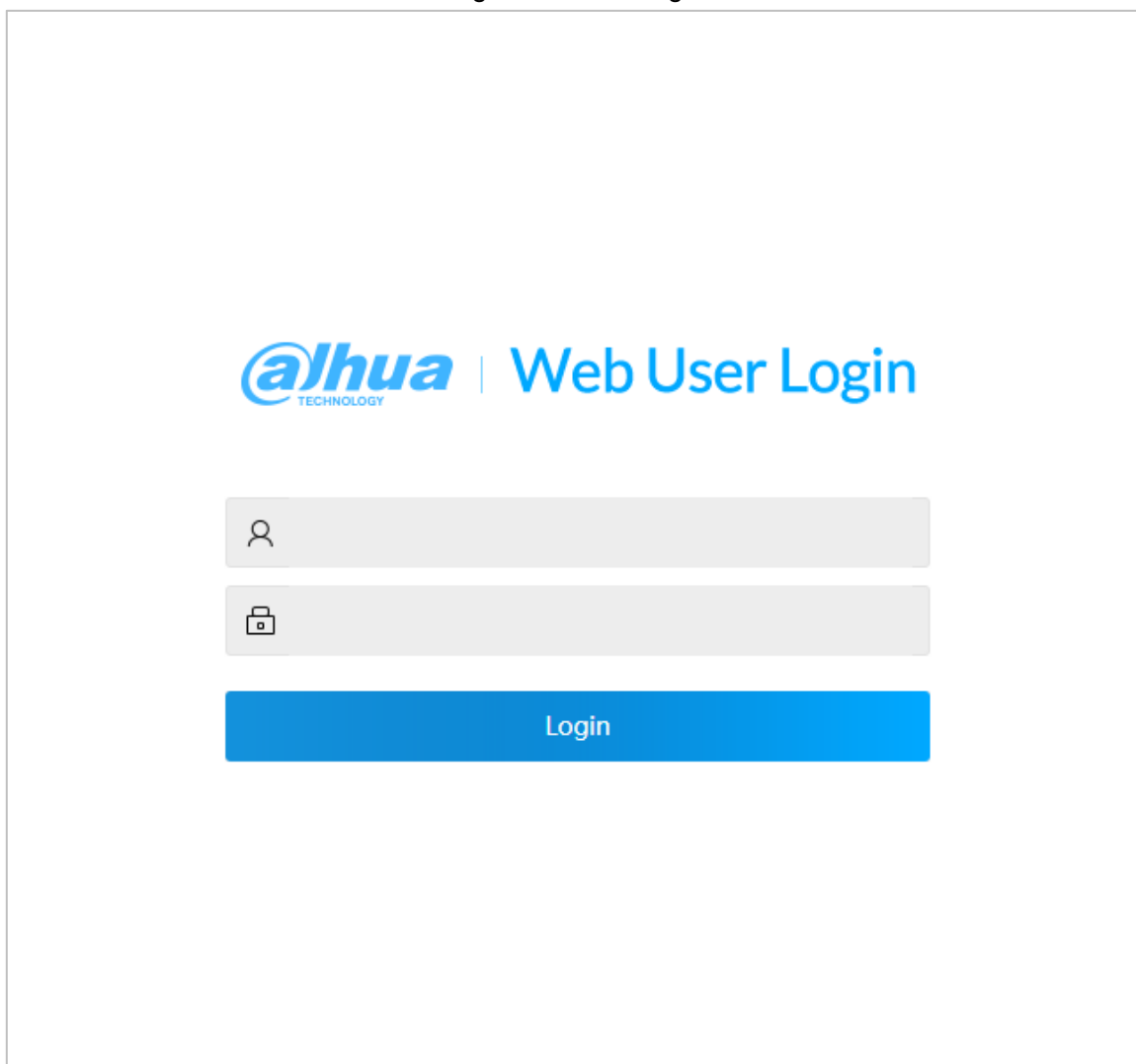
Before login, make sure:

- You already configure the IP address of the switch. The IP address of VLAN 1 is 192.168.1.110 by default.
- The PC with web browser is connected to the network, and the PC can ping the switch successfully.

Step 1 Enter the IP address of the switch in the address bar of the web browser. The IP address is 192.168.1.110 by default, and press Enter.

The Login interface is displayed. See Figure 1-1.

Figure 1-1 Web login



The screenshot shows the web login page for a Dahua switch. At the top, there is the Dahua logo (a stylized 'd' in a circle) followed by the text 'Web User Login'. Below this, there are two input fields. The first field has a person icon on the left, indicating it is for the username. The second field has a lock icon on the left, indicating it is for the password. Below these fields is a prominent blue button with the word 'Login' in white text.

Step 2 Enter user name and password. The user name and the password are admin by default.

Step 3 Click **Login**.

The **Quick Setting** interface is displayed.



Modify the password after first login. The new password can be set from 8 characters through 32 characters and contains at least two types from number, letter, and special characters (excluding "", "", ", ":", and "&").

2 Quick Settings

On the interface, you can view the system information, and set the device parameters, VLAN, aggregation, IP and route.

2.1 System Info

You can view the name, type, serial number, and software version of the device, and port status and port information.

After logging in the system, the **System Info** is displayed. See Figure 2-1. On the switch, if the port shows green, it means the port is connected successfully. And if the port shows gray, it means the port is not connected or the connection fails. See Table 2-1.

Figure 2-1 System information


The screenshot shows the Aihua switch management interface. At the top, there are navigation tabs: Quick Setting, Advanced, and Maintain. The System Info section displays the following details:

- Device Name: SWITCH
- Device Type: DH-IS5500-5GT2GF-DPWR
- Serial Number: 0000000000000001
- Software Version: 1.001.0000000.0.6.R
- IP Address: [Redacted]

Below the System Info is a table showing port information:

Port	Port Type	Link	Flow Control	Speed/Duplex	VLAN	POE	Receive Usage	Send Usage	Media Type
1	Access	Down	Off	Down	1	0W	0%	0%	Copper
2	Access	Down	Off	Down	1	0W	0%	0%	Copper
3	Access	Down	Off	Down	2	0W	0%	0%	Copper
4	Access	Down	Off	Down	3	0W	0%	0%	Copper
5	Access	Up	Off	1G Full	1	0W	0.1%	0%	Copper
6	Access	Down	Off	Down	5	0W	0%	0%	Fiber
7	Access	Down	Off	Down	6	0W	0%	0%	Fiber

Table 2-1 Port information

Paramater	Description
Port	Show all ports of the switch.  This switch contains 7 ports. Port quantity might vary depending on the model you purchased, and the actual product shall preveil.
Port Type	Three types: Access , Hybrid , and Trunk .
Link	Two link states: Up and Down . Up indicates the port is connected successfully, and Down indicates the port is not connected or the connection fails.
Flow Control	Show the flow control state.

Parameter	Description
Speed/Duplex	<ul style="list-style-type: none"> • Online: It shows the port rate and the duplex mode. • Offline : It shows Down.
VLAN	The port VLAN. It is VLAN 1 by default.
POE	Show the power consumption of POE. Only 1~4 ports support.
Receive Usage	The current receive speed is divided by the average speed in a certain period (5 minutes usually).
Send Usage	The current send speed is divided by the average speed in a certain period (5 minutes usually).
Media Type	Two media types: Copper and Fiber . Copper indicates RJ-45 port, and Fiber indicates fiber port.

2.2 Local

You can set the system name, IP address, and subnet mask.

Step 1 Click **Local** on the **Quick setting** interface.

The **Local** interface is displayed. See Figure 2-2.

Figure 2-2 Local

Step 2 Set the system name, IP address, and mask length.

Step 3 Click **OK**.

2.3 VLAN

Add the port to the VLAN, and configure the VLAN. By default, the port belongs to VLAN1.

Step 1 Click **VLAN** on the **Quick Setting** interface.

The **VLAN** interface is displayed. See Figure 2-3.

Figure 2-3 VLAN

Port	Mode	Port VLAN	Allowed VLANs
1	Access	1	1
2	Access	1	1
3	Access	1	1
4	Access	1	1
5	Access	1	1
6	Access	1	1
7	Access	1	1

Step 2 Configure the port VLAN parameters. See Table 2-2.

Table 2-2 Port VLAN configuration parameter

Parameter	Description
Port	Show all ports of the switch.
Mode	Three Mode: Access , Hybrid , and Trunk . <ul style="list-style-type: none"> ● Access: When the port connects to terminal devices (such as PC and IPC), select Access. ● Trunk: When the port connects to switch, select Trunk. ● Hybrid: Not often used.
Port VLAN	Add the port to a VLAN. By default, the port belongs to VLAN1, and the range is 1~4094.
Allowed VLANs	Set the allowed VLAN. When the mode is Trunk , you can set it.

Step 3 Click **OK**.

2.4 Aggregation

Add the port to the aggregation. There are two types of aggregations: For the details, see "3.1.4 Aggregation."

Click **Aggregation** on **Quick Setting** interface, and the **Aggregation** interface is displayed. See Figure 2-4.

Figure 2-4 Aggregation

Aggregation		Mode	1	2	3	4	5	6	7
Status			■	■	■	■	■	■	■
Receive Usage			0%	0%	0%	0%	0.1%	0%	0%
Send Usage			0%	0%	0%	0%	0%	0%	0%
Group			●	●	●	●	●	●	●
Group1	Disabled		●	●	●	●	●	●	●
Group2	Disabled		●	●	●	●	●	●	●
Group3	Disabled		●	●	●	●	●	●	●

OK Cancel

2.4.1 Static Aggregation Configuration

Example: Add port 1 and port 2 to Static Group 1.

Step 1 Select **Model** as **Static** in group 1, which indicates that the group is static aggregation.

Step 2 Select port 1 and port 2 in group 1 to add the two ports to static aggregation. See Figure 2-5.



You can configure up to 3 groups of static aggregation.

Figure 2-5 Static configuration

Aggregation		Mode	1	2	3	4	5	6	7
Status			■	■	■	■	■	■	■
Receive Usage			0%	0%	0%	0%	0.1%	0%	0%
Send Usage			0%	0%	0%	0%	0%	0%	0%
Group			●	●	●	●	●	●	●
Group1	Static		●	●	●	●	●	●	●
Group2	Disabled		●	●	●	●	●	●	●
Group3	Disabled		●	●	●	●	●	●	●

OK Cancel

Step 3 Click **OK**.

The port 1 and port 2 form a logical port.

2.4.2 Dynamic Aggregation Configuration

Example: Add port 3 and port 4 to aggregation group 2, and add port 5 and port 6 to aggregation group 3.

Step 1 Add the port members to the dynamic group.

- 1) Select **Mode** as **LACP (Passive)**, and add the port members to the aggregation group. For example, add port 3 and port 4 to aggregation group 2. See Figure 2-6.

- 2) Select **Mode** as **LACP (Passive)**, and add the port members to the aggregation group. For example, add port 5 and port 6 to aggregation group 3. See Figure 2-6.

Figure 2-6 Dynamic configuration

	Mode	1	2	3	4	5	6	7
Status		■	■	■	■	■	■	■
Receive Usage		0%	0%	0%	0%	0.1%	0%	0%
Send Usage		0%	0%	0%	0%	0%	0%	0%
Group		○	○	○	○	○	○	●
Group1	Static	●	●	○	○	○	○	○
Group2	LACP(Active)	○	○	●	●	○	○	○
Group3	LACP(Passive)	○	○	○	○	●	●	○

Step 2 Click **OK**.

2.5 IP and route

You can add the IP address of VLAN interface and IP route. For details, see "3.1.1.2 IP and route."

Step 1 Click **VLAN** on the **IP & route** interface.

The **IP & route** interface is displayed. See Figure 2-7.

Figure 2-7 IP and route

IP & Route
✕

IP Config
+ Add
Delete

	VLAN	IP Address	Mask Length	Delete
<input type="checkbox"/>	1	172.20.0.1	16	Delete

Route Config
+ Add
Delete

	Network	Mask Length	Next Hop	Delete
<input type="checkbox"/>	0.0.0.0	0	172.20.0.1	Delete

OK
Cancel

Step 2 Add the VLAN interface.

- 1) Click **Add** in the **IP Config**.
A new record is added. See Figure 2-8.

Figure 2-8 VLAN interface

IP Config
+ Add
Delete

	VLAN	IP Address	Mask Length	Delete
<input type="checkbox"/>	1	172.20.0.1	16	Delete
<input type="checkbox"/>				Delete

- 2) For the parameters, see Table 2-3.

Table 2-3 VLAN interface

Parameter	Description
VLAN	Enter VLAN number.
IP address	Set the IP address of the VLAN interface.
Mask Length	Set the mask length of the VLAN interface.

Step 3 Add the IP route.

- 1) Click **Add** in the **Route Config**.

A new record is added. See Figure 2-9.

Figure 2-9 IP route

The screenshot shows a 'Route Config' interface with two buttons: '+ Add' and 'Delete'. Below the buttons is a table with the following columns: Network, Mask Length, Next Hop, and Delete. The table contains two rows. The first row has a checkbox, the value '0.0.0.0' in the Network column, '0' in the Mask Length column, '172.12.0.1' in the Next Hop column, and a trash icon in the Delete column. The second row is highlighted with a yellow border and contains a checkbox, empty input fields for Network, Mask Length, and Next Hop, and a trash icon in the Delete column.

2) For the parameters, see Table 2-4.

Table 2-4 IP routes

Parameter	Description
Network	It is the destination of the IP packet.
Mask Length	Mask length, with the destination address, is to identify the IP address of the destination host or the route. After Logical AND between destination address and network mask, you can get the IP address of the destination host or the route.
Next Hop	The next hop IP of the route.

Step 4 Click **OK**.

3

Advanced Settings

3.1 Common Configuration

3.1.1 System Configuration

3.1.1.1 System Information

You can set the device name, IP address, mask length and DHCP enable, and view the software information, hardware information and time.



Be careful when you enable DHCP Client. After enabling DHCP Client, the IP router or DHCP server connecting to the switch will assign IP to the switch automatically and the existing IP will be invalidated, and then you cannot access the web interface.

Step 1 Select **Advanced > Common > System Config> System Info**.

The **System Info** interface is displayed. See Figure 3-1.

Figure 3-1 System information

System Info	IP&Route	Current Time	Log
System:			
Device Name:	SWITCH		
IP Address:	[REDACTED]		
Mask Length:	16		
DHCP Enable:	<input type="checkbox"/>		
Software:			
Software Version:	1.001.0000000.6.R		
Compile Date:	2018-11-29 15:25:16+08:00		
Hardware:			
Device Name:	SWITCH		
Device Type:	DH-IS5500-5GT2GF-DPWR		
IP Address:	[REDACTED]		
Mask Length:	16		
MAC Address:	[REDACTED]		
Serial Number:	0000000000000001		
Time:			
System Date:	2018-05-21 08:37:34		
System Running Time:	0 days 00:23:17		
<input type="button" value="Save"/> <input type="button" value="Refresh"/>			

Step 2 Set the device name, IP address and mask length and DHCP enable.

Step 3 Click **Save**.

3.1.1.2 IP and route

The hosts belong to different VLANs cannot communicate. Route or the layer 3 switch is needed for forwarding.

The switch supports layer 3 forwarding through VLAN interface. VLAN interface is the virtual interface of layer 3 mode, for layer 3 communication between the VLANs. It is not the physical entity on the device. Every VLAN is related to a VLAN interface, and the VLAN interface can forward packet for the VLAN. Generally, because the VLAN can isolate the broadcasting domain, every VLAN corresponds to a network segment. VLAN interface is the gateway of the network segment, and it supports layer 3 forwarding for the message based on IP address.

Step 1 Select **Advanced > Common > System Config > IP&Route**.

The **IP&Route** interface is displayed. See Figure 3-2.

Figure 3-2 IP and route

The screenshot displays the 'IP&Route' configuration page. At the top, there are tabs for 'System Info', 'IP&Route', 'Current Time', and 'Log'. Below the tabs, there are buttons for '+ Add' and 'Delete' under 'IP Setting', and an 'Auto Refresh' checkbox which is checked. The main area is divided into two columns. The left column contains a table for IP settings:

<input type="checkbox"/>	VLAN	IP Address	Mask Length	Delete	Delete IP
<input type="checkbox"/>	1	192.168.1.1	16		

The right column contains a table for interface status:

Interface	Address	Status
1	192.168.1.1	UP

Below these tables, there is a 'Route Setting' section with '+ Add' and 'Delete' buttons. It contains two tables. The left table is for route configuration:

<input type="checkbox"/>	Network	Mask Length	Next Hop	Delete
<input type="checkbox"/>	0.0.0.0	0	192.168.1.1	

The right table is for route details:

Destination	Mask Length	Protocol	Priority	Next Hop	Egress
0.0.0.0	0	Static	60	192.168.1.1	0
192.168.1.0	16	Direct	0	VLAN1	-

At the bottom left of the configuration area, there is a 'Save' button.

Step 2 Add the VLAN interface.

- 1) Click **Add** in **IP&route**.

The **Add IP** interface is displayed. See Figure 3-3.

Figure 3-3 Add IP

2) For the parameters, see Table 3-1.

Table 3-1 VLAN interface

Parameter	Description
VLAN	Enter VLAN number.
IP address	Set the IP address of the VLAN interface.
Mask Length	Set the mask length of the IP address.

3) Click **OK**.

Step 3 Add the IP route.

1) Click **Add** in the **IP Config**.

The **Add IP** interface is displayed. See Figure 3-4.

Figure 3-4 Add route

2) For the parameters, see Table 3-2.

Table 3-2 IP routes

Parameter	Description
Network	It is the destination of the IP packet.
Mask Length	Mask length, with destination address, is to identify the IP address of the destination host or the route. After Logical AND between destination address and network mask, you can get the IP address of the destination host or the route.
Next Hop	The next hop IP of the route.

3) Click **OK**.

Step 4 Click **Save**.

3.1.1.3 System time

Set the system time of switch.

Select **Advanced > Common > System Config > Current Time**.

The **Current Time** interface is displayed. See Figure 3-5.

Figure 3-5 Current time (1)

You can set the system time through the following three methods:

- Set the time manually
Set the date and time on **Current Time** interface, and then click **Save**.
- Sync time
Click **Sync PC**, and the switch time synchronizes with the local time automatically.
- Sync NTP server time
Only with NTP server configured in the network can you enable this function as following steps:

Step 1 Select the **NTP Enable** box to enable the NTP service.

Step 2 Set the IP address of the NTP server. See Figure 3-6.

Figure 3-6 Current time (2)

Step 3 Click **Save**.

The switch time automatically synchronizes with the time of server 1.

3.1.1.4 Log

You can view logs, export logs and clear logs.

Select **Advanced > Common > System Config > Log**. The System Log interface is displayed. See Figure 3-7.

Figure 3-7 Log

No.	Log Time	Log Level	Description
1	2018-03-31 03:16:59	Informational	SYS-BOOTING: Switch just made a cold boot.
2	2018-03-31 03:17:04	Informational	USERS: modify the password of user [admin]
3	2018-03-31 03:17:07	Notice	CHIP 1, PSE CHIP FOUND
4	2018-03-31 03:17:08	Notice	LINK-CHANGED: Interface GigabitEthernet 1/1, changed state to up (MEP).
5	2018-03-31 03:17:08	Notice	LINK-CHANGED: Interface GigabitEthernet 1/2, changed state to up (MEP).
6	2018-03-31 03:17:08	Notice	LINK-CHANGED: Interface GigabitEthernet 1/3, changed state to up (MEP).
7	2018-03-31 03:17:08	Notice	LINK-CHANGED: Interface GigabitEthernet 1/4, changed state to up (MEP).
8	2018-03-31 03:17:08	Notice	LINK-CHANGED: Interface GigabitEthernet 1/5, changed state to up (MEP).
9	2018-03-31 03:17:08	Notice	LINK-CHANGED: Interface GigabitEthernet 1/6, changed state to up (MEP).

- View logs.
Set the start time, end time and log level, and then click **Search** to view the details of the logs. **Log Level** includes **Error**, **Warning**, **Notice** and **Information**.
- Click **Export** to export all logs.
- Click **Clear** to clear all logs.

3.1.2 Port configuration

You can set the port parameters, including speed, full duplex and half duplex, and so on.

Step 1 Select **Advanced > Common > Port**.

The **Port Configuration** interface is displayed. See Figure 3-8.

Figure 3-8 Port configuration







Port	Link	Speed Duplex Status	Speed Duplex Setting	Flow Control Status	Flow Control Setting	Ingress Limit Enable	Ingress Limit (kbps)	Egress Limit Enable	Egress Limit (kbps)	Receive Usage	Send Usage
1	Down	Down	Auto	Off	<input checked="" type="checkbox"/>	<input type="checkbox"/>	500	<input type="checkbox"/>	500	0%	0%
2	Down	Down	Auto	Off	<input checked="" type="checkbox"/>	<input type="checkbox"/>	500	<input type="checkbox"/>	500	0%	0%
3	Down	Down	Auto	Off	<input checked="" type="checkbox"/>	<input type="checkbox"/>	500	<input type="checkbox"/>	500	0%	0%
4	Down	Down	Auto	Off	<input checked="" type="checkbox"/>	<input type="checkbox"/>	500	<input type="checkbox"/>	500	0%	0%
5	Up	1G Full	Auto	Off	<input checked="" type="checkbox"/>	<input type="checkbox"/>	500	<input type="checkbox"/>	500	0.1%	0%
6	Down	Down	Auto	Off	<input checked="" type="checkbox"/>	<input type="checkbox"/>	500	<input type="checkbox"/>	500	0%	0%
7	Down	Down	Auto	Off	<input checked="" type="checkbox"/>	<input type="checkbox"/>	500	<input type="checkbox"/>	500	0%	0%

Save Refresh

Step 2 For the parameters, see Table 3-3.

Table 3-3 Port parameter

Parameter	Description
Port	Show all ports of the switch.
Aggregation state	Green Up indicates the port is connected successfully, and Red Down indicates the port is not connected or the connection fails.
Speed Duplex Status	Down means disconnection, and the specific speed means successful connection. Full means full duplex; Half means half duplex.
Speed Duplex Setting	Set the speed and the duplex mode.

Parameter	Description
Flow Control State	Show flow control actual negotiator or enable status, including ON and OFF. <ul style="list-style-type: none"> ● ON: Negotiation succeeds. ● OFF: Negotiation fails.
Flow Control Setting	ON/OFF flow control function. <ul style="list-style-type: none"> ●  : Flow control is ON. ●  : Flow control is OFF.
Ingress Limit Enable	Enable/Disable ingress limit. <ul style="list-style-type: none"> ●  : Ingress enable is enabled. ●  : Ingress enable is disabled.
Ingress Limit (kbps)	Set the ingress limit.
Egress Limit Enable	Enable/Disable egress limit. <ul style="list-style-type: none"> ●  : Egress enable is enabled. ●  : Egress enable is disabled.
Egress Limit (kbps)	Set the egress limit.
Receive Usage	Show the acceptance usage.
Send Usage	Show the send usage.

Step 3 Click **Save**.

3.1.3 VLAN Configuration

Add the port to the VLAN, and configure the VLAN. By default, the port belongs to VLAN1.

Step 1 Select **Advanced > Common > VLAN Settings**.

The **VLAN Settings** interface is displayed. See Figure 3-9.

Figure 3-9 VLAN Settings

VLAN Settings

VLANs The allowable range is '1-4094'. Such as '2', '3,7' or '1-9'

Port	Mode	Port VLAN	Ingress Acceptance	Egress Tagging	Allowed VLANs
1	Access	1	Tagged and Untagged	Untag All	1
2	Trunk	1	Tagged and Untagged	Untag Port VLAN	1-4094
3	Hybird	1	Tagged and Untagged	Untag Port VLAN	1-4094
4	Access	1	Tagged and Untagged	Untag All	1
5	Access	1	Tagged and Untagged	Untag All	1
6	Access	1	Tagged and Untagged	Untag All	1
7	Access	1	Tagged and Untagged	Untag All	1

Step 2 Enter 1, 2 in VLANs to create VLAN 1 and VLAN 2.

Step 3 Configure the port VLAN parameters. See Table 3-4.

Table 3-4 Port VLAN configuration parameter

Parameter	Description
Port	Show all ports of the switch.
Mode	Three Mode: Access , Hybrid , and Trunk .
Port VLAN	Add the port to a VLAN. By default, the port belongs to VLAN1. The range is 1~4094.
Ingress Acceptance	Show whether data can flow into the port. Only Hybird supports the configuration (By default, all date flows into the port under other models). See the following situations: <ul style="list-style-type: none"> ● Tagged and Untagged: All data flows into the port. ● Tagged only: Only tagged data can flows into the port. ● Untagged only: Only untagged data can flow into the port.
Egress Tagging	Show whether to tag the data that will egress the port. See the following three situations: <ul style="list-style-type: none"> ● Untag Port VLAN: If the data flow tag is the same with PVID, the tag will be peeled. ● Tag All: All data will be tagged. ● Untag All: All data will not be tagged.
Allowed VLANs	Set the allowed VLAN.

Step 4 Click **Save**.

3.1.4 Aggregation

Aggregation is to form the multiple physical ports of the switch into the logical port.

The multiple links in the same group can be regarded as a logical link with the larger bandwidth. Through aggregation, the ports in the same group can share the communication flow, to make a larger bandwidth. Besides, the ports in the same group can back up reciprocally and dynamically, to enhance the link reliability.

3.1.4.1 Static Configuration

Step 1 Select **Advanced > Common > Aggregation**.

The **Aggregation** interface is displayed. See Figure 3-10.

Figure 3-10 Aggregation

Aggregation								
Aggregation Configuration <input checked="" type="checkbox"/> Source MAC Address <input type="checkbox"/> Destination MAC Address <input checked="" type="checkbox"/> IP Address <input checked="" type="checkbox"/> TCP/UDP Port								
	Mode	1	2	3	4	5	6	7
Status		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Receive Usage		0%	0%	0%	0%	0.1%	0%	0%
Send Usage		0%	0%	0%	0%	0%	0%	0%
Group		<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"/>
Group1	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group2	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group3	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Save Refresh

Step 2 Select the aggregation load balancing algorithm mode in **Aggregation Configuration**.

There are four types:

- Source MAC Address: The aggregation load balancing algorithm based on MAC address.
- Destination MAC Address: The aggregation load balancing algorithm based on destination MAC address.
- IP Address: The aggregation load balancing algorithm based on source IPv4 address and destination IPv4 address.
- TCP/UDP Port: The aggregation load balancing algorithm based on source and destination TCP/UDP port.

Step 3 Select **Mode** as **Static**, and add the port members to the dynamic aggregation group. For example, add port 1 and port 2 to aggregation group. See Figure 3-11.



At most, 3 static aggregation groups can be set at the same time.

Figure 3-11 Static configuration

Aggregation								
Aggregation Configuration <input checked="" type="checkbox"/> Source MAC Address <input type="checkbox"/> Destination MAC Address <input checked="" type="checkbox"/> IP Address <input checked="" type="checkbox"/> TCP/UDP Port								
	Mode	1	2	3	4	5	6	7
Status		■	■	■	■	■	■	■
Receive Usage		0%	0%	0%	0%	0.1%	0%	0%
Send Usage		0%	0%	0%	0%	0%	0%	0%
Group		●	●	●	●	●	●	●
Group1	Static	●	●	●	●	●	●	●
Group2	Disabled	●	●	●	●	●	●	●
Group3	Disabled	●	●	●	●	●	●	●

Save Refresh

Step 4 Click **Save**.

The port 1 and port 2 form a logical port.

3.1.4.2 LACP

LACP (Link Aggregation Control Protocol) is the protocol for link dynamic aggregation. LACP communication with another port through LACPDU (Link Aggregation Control Protocol Data Unit).

Select the port role from the drop-down list in **Mode**. There are two types:

- **Active**: The port can send LACPDU packet actively to the opposite port, and analyzes the LACP.
- **Passive**: The port can not send LACPDU packet actively. After receiving the LACP packet sent by the opposite port, the port analyzes the LACP.

Step 1 Select **Advanced > Common > Aggregation**.

The **Aggregation** interface is displayed. See Figure 3-12.

Figure 3-12 LACP (1)

Aggregation								
Aggregation Configuration <input checked="" type="checkbox"/> Source MAC Address <input type="checkbox"/> Destination MAC Address <input checked="" type="checkbox"/> IP Address <input checked="" type="checkbox"/> TCP/UDP Port								
	Mode	1	2	3	4	5	6	7
Status		■	■	■	■	■	■	■
Receive Usage		0%	0%	0%	0%	0.1%	0%	0%
Send Usage		0%	0%	0%	0%	0%	0%	0%
Group		●	●	●	●	●	●	●
Group1	Disabled	●	●	●	●	●	●	●
Group2	Disabled	●	●	●	●	●	●	●
Group3	Disabled	●	●	●	●	●	●	●

Save Refresh

Step 2 Select **Mode** as **LACP (Passive)**, and add the port member to the dynamic aggregation group. For example, add port 3 and port 4 to aggregation Group 2. See Figure 3-13.

Step 3 Select **Mode** as **LACP (Passive)**, and add the port member to the dynamic aggregation group. For example, add port 5 and port 6 to aggregation Group 3. See Figure 3-13.

Figure 3-13 LACP (2)

Aggregation								
Aggregation Configuration <input checked="" type="checkbox"/> Source MAC Address <input type="checkbox"/> Destination MAC Address <input checked="" type="checkbox"/> IP Address <input checked="" type="checkbox"/> TCP/UDP Port								
	Mode	1	2	3	4	5	6	7
Status		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Receive Usage		0%	0%	0%	0%	0.1%	0%	0%
Send Usage		0%	0%	0%	0%	0%	0%	0%
Group		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Group1	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group2	LACP(Active)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group3	LACP(Passive)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Save Refresh

Step 4 Click **Save**.

3.1.5 MAC Table

MAC (Media Access Control) Table records the relationship between the MAC address and the port, and the information including the VLAN that the port belongs to. When the device is forwarding the packet, it queries in the MAC address table for the destination MAC address of the packet. If the destination MAC address of the packet is contained in the MAC address table, the packet is forwarded through the port in the table directly. And if the destination MAC address of the packet is not contained in the MAC address table, the device adopts broadcasting to forward the packet to all the ports except the receiving port in VLAN.

3.1.5.1 Adding Static MAC Table

Step 1 Select **Advanced > Common > MAC Table > MAC Address Table**.

The **MAC Address Table** interface is displayed. See Figure 3-14.

Figure 3-14 MAC address table

MAC Address Table | Port MAC Filtering

+ Add Delete Refresh MAC Address Port Search

<input type="checkbox"/>	MAC Address	Type	VLAN	Port	Delete
<input type="checkbox"/>	00:00:00:00:00:01	Dynamic	1	5	
<input type="checkbox"/>	00:00:00:00:00:02	Dynamic	1	5	
<input type="checkbox"/>	00:00:00:00:00:03	Dynamic	1	5	
<input type="checkbox"/>	00:00:00:00:00:04	Dynamic	1	5	
<input type="checkbox"/>	00:00:00:00:00:05	Dynamic	1	5	
<input type="checkbox"/>	00:00:00:00:00:06	Dynamic	1	5	
<input type="checkbox"/>	00:00:00:00:00:07	Dynamic	1	5	
<input type="checkbox"/>	00:00:00:00:00:08	Dynamic	1	5	
<input type="checkbox"/>	00:00:00:00:00:09	Dynamic	1	5	
<input type="checkbox"/>	00:00:00:00:00:0A	Dynamic	1	5	

1 / 18

Step 2 Bind the MAC address to the port in the certain VLAN. For example, bind the MAC address 00:00:00:00:00:01 to the port 3 in VLAN 2.

1) Click **Add**.

The **Add Static MAC Address** interface is displayed.

2) Set the MAC address, port and VLAN. See Figure 3-15.

Figure 3-15 Adding static MAC table

Add Static MAC Address ✕

MAC Address
Example:00:23:AE:77:10:53

Port

Vlan

3) Click **OK**.

3.1.5.2 Port MAC Filtering

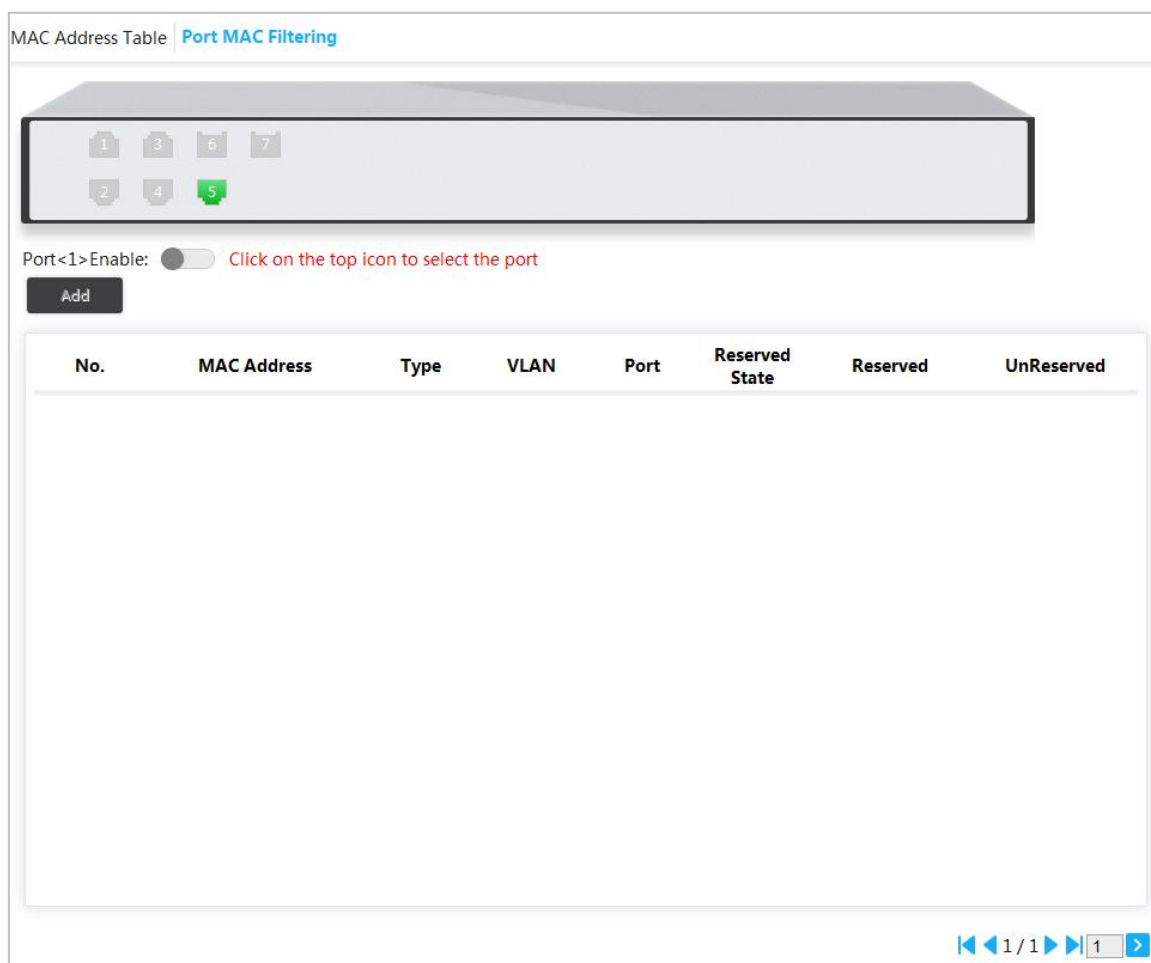
After enabling port MAC filtering, the following two MAC devices can communicate with the port.

- Devices in MAC whitelist
- The static MAC devices changing from the dynamic MAC devices

Step 1 Select **Advanced > Common > MAC Table > Port MAC Filtering**.

The **Port MAC Filtering** interface is displayed. See Figure 3-16.

Figure 3-16 Port MAC filtering




Step 2 Select the port, such as port 5.

Step 3 Click behind **Port <5> Enable** to enable the port. See Figure 3-17.

Figure 3-17 Enable port MAC filtering

MAC Address Table **Port MAC Filtering**



Port<5>Enable: Click on the top icon to select the port

Add

No.	MAC Address	Type	VLAN	Port	Reserved State	Reserved	UnReserved
1	00:00:00:00:00:00	Dynamic	1	5	UnReserved	Reserved	UnReserved
2	00:00:00:00:00:00	Dynamic	1	5	UnReserved	Reserved	UnReserved
3	00:00:00:00:00:00	Dynamic	1	5	UnReserved	Reserved	UnReserved
4	00:00:00:00:00:00	Dynamic	1	5	UnReserved	Reserved	UnReserved
5	00:00:00:00:00:00	Dynamic	1	5	UnReserved	Reserved	UnReserved
6	00:00:00:00:00:00	Dynamic	1	5	UnReserved	Reserved	UnReserved
7	00:00:00:00:00:00	Dynamic	1	5	UnReserved	Reserved	UnReserved
8	00:00:00:00:00:00	Dynamic	1	5	UnReserved	Reserved	UnReserved
9	00:00:00:00:00:00	Dynamic	1	5	UnReserved	Reserved	UnReserved
10	00:00:00:00:00:00	Dynamic	1	5	UnReserved	Reserved	UnReserved

Save

Navigation: << 1 / 17 >> 1 >

- Change dynamic MAC device to static.
 - 1) Select one record, and click **Reserved**.
 - 2) Click **Save**. The type changes from **Dynamic** to **Static**.
Static MAC devices can communicate with the port normally.
- Add MAC whitelist.
 - 1) Click **Add**.
The **Add MAC Whitelist** interface is displayed. See Figure 3-18.

Figure 3-18 Add MAC whitelist.

Add MAC Whitelist ✕

MAC Address
Example:00:23:AE:77:10:53

VLAN

- 2) Set MAC address and VLAN.
- 3) Click **OK**.

The devices in MAC whitelist can communicate with port normally.

3.1.6 Spanning Tree

The spanning tree protocol is the protocol of layer 2. It can eliminate the ring cycle of layer 2 by choosing to block the redundant links in the network, and it can back up the links.

Similar to other protocols, the spanning tree protocol is updated with the development of the network: From STP (Spanning Tree Protocol), to RSTP (Rapid Spanning Tree Protocol), and to the latest MSTP (Multiple Spanning Tree Protocol).

Step 1 Select **Advanced > Common > Spanning Tree > STP Ports Settings**.

The **STP Ports Settings** interface is displayed. See Figure 3-19.

Figure 3-19 STP ports settings

The screenshot shows the 'STP Port Settings' configuration page. At the top, there is a label 'STP Port Settings' in blue. Below it, the 'STP Mode' is set to 'Disable' in a dropdown menu. The main area contains a table with the following headers: 'Port', 'Enable Priority' (with a checkbox), 'RPC', 'State', 'Status', 'Designated Bridge', and 'Designated Port'. The table body is empty. At the bottom left, there is a blue 'Save' button.

Step 2 Select the STP mode: **STP**, **RSTP** and **MSTP**.

- **STP**: The most basic spanning tree protocol.
- **RSTP**: Improved based on STP, and realizes rapid convergence of network topology.
- **MSTP**: Remedies the defects of STP and RSTP. MSTP not only realizes rapid convergence, but also provides better load sharing mechanism for the redundant links by forwarding the flow from different VLANs through their own paths.

Step 3 Click **Save**, and the results are various according to the different modes. See Figure 3-20, Figure 3-21 and Figure 3-22.

Figure 3-20 STP

STP Port Settings

STP Mode: STP

Port	<input type="checkbox"/> Enable Priority	RPC	State	Status	Designated Bridge	Designated Port
1	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
2	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
3	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
4	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
5	<input type="checkbox"/>	128	-	Non-STP	Forwarding	-
6	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
7	<input type="checkbox"/>	128	-	Non-STP	Discarding	-

Save

Figure 3-21 RSTP

STP Mode: RSTP

Port	<input type="checkbox"/> Enable Priority	RPC	State	Status	Designated Bridge	Designated Port
1	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
2	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
3	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
4	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
5	<input type="checkbox"/>	128	-	Non-STP	Forwarding	-
6	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
7	<input type="checkbox"/>	128	-	Non-STP	Discarding	-

Save

Figure 3-22 MSTP

STP Port Settings

STP Mode: MSTP

Port	<input type="checkbox"/> Enable Priority	RPC	State	Status	Designated Bridge	Designated Port
1	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
2	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
3	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
4	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
5	<input type="checkbox"/>	128	-	Non-STP	Forwarding	-
6	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
7	<input type="checkbox"/>	128	-	Non-STP	Discarding	-

Save

Step 4 Select 3 ports at least to combine a STP/RSTP/MSTP snoop. For example: Port 1, port 2 and port 3 combine a STP snoop. See Figure 3-23.

Figure 3-23 STP snoop

STP Port Settings

STP Mode: STP

Port	<input type="checkbox"/> Enable Priority	RPC	State	Status	Designated Bridge	Designated Port
1	<input checked="" type="checkbox"/>	128	-	Non-STP	Discarding	-
2	<input checked="" type="checkbox"/>	128	-	Non-STP	Discarding	-
3	<input checked="" type="checkbox"/>	128	-	Non-STP	Discarding	-
4	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
5	<input type="checkbox"/>	128	-	Non-STP	Forwarding	-
6	<input type="checkbox"/>	128	-	Non-STP	Discarding	-
7	<input type="checkbox"/>	128	-	Non-STP	Discarding	-

Save

Step 5 Click **Save**.

The states of port 1, port 2 and port 3 will change.

3.2 Seldom-used Configuration

3.2.1 ERPS

ERPS (Ethernet Ring Protection Switching) is the loop prevention protocol standard of layer 2 defined by ITU-T, and the standard number is ITU-T G.8032/Y1344. So it is also called G.8032. It defines RAPS (Ring Auto Protection Switching) protocol packet and protection switching scheme.

ERPS supports two versions (V1 and V2). V1 was released by ITU-T in June 2008, and V2 was released by ITU-T in August 2010. V2 is compatible with V1, and adds the following functions:

1. Multi-ring networks including crossing ring.
2. Sub-ring switch RAPS packet by virtual channel or non-virtual channel.
3. Forcedly and manually switch blocks.
4. ERPS reverse switch is configurable.

3.2.1.1 MEP Configuration

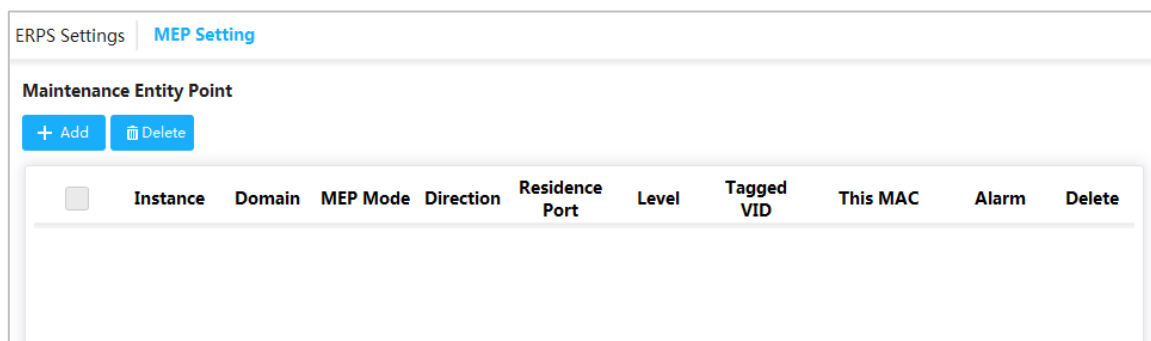
MEP (Maintenance Entity Point) is a part of ERPS.

The layer 2 device added into ERPS are called node. Add no more than 2 ports into a ERPS for each node.

Step 1 Select **Advanced > Seldom-used > ERPS > MEP Setting**.

The **MEP Setting** interface is displayed. See Figure 3-24.

Figure 3-24 MEP configuration



Step 2 Click **Add**.

The **Add** interface is displayed. See Figure 3-25.

Figure 3-25 Add

The 'Add' dialog box is titled 'Add' and has a close button (X) in the top right corner. It contains four input fields: 'Instance', 'Residence Port', 'Level', and 'Tagged VID'. At the bottom right, there are two buttons: 'OK' and 'Cancel'.

Step 3 For the parameters, see Table 3-5.

Table 3-5 MEP parameters

Parameter	Description
Instance	Enter MEP instance number, such as 1.
Residence Port	Enter the port number that MEP belongs to, such as Port 1.
Level	Maintenance level, and it is recommended to set it to be 0.
Tagged VID	Enter protocol VLAN, such as VLAN 3.

Step 4 Click **OK**.

3.2.1.2 ERPS Configuration

Step 1 Select **Advanced > Seldom-used > ERPS > ERPS Settings**.

The **ERPS Settings** interface is displayed. See Figure 3-26.

Figure 3-26 ERPS configuration

The 'ERPS Settings' interface shows a 'MEP Setting' sub-tab. Under 'Ethernet Ring Protection Switching', there are '+ Add' and 'Delete' buttons. Below is a table with the following columns: ERPSID, Port 0, Port 1, APS, SF, Ring Type, Interconnected Node, Virtual Channel, Major Ring ID, Alarm, and Delete. The table currently contains one row with a checkbox in the ERPSID column.

Step 2 Click **Add**.

The **Add ERPS** interface is displayed. See Figure 3-27.

Figure 3-27 Add ERPS

Step 3 For the parameters, see Table 3-6.

Table 3-6 ERPS parameters

Parameter	Description
ERPS ID	The ID number of ERPS.
Port 0	The two ports added into the ERPS.
Port 1	
Port 0 APS MEP	The corresponding protocol packet ERPS to ERPS port. Keep Port 0 APS MEP consistent with Port 0 SF MEP. Keep Port 1 APS MEP consistent with Port 1 SF MEP. For example: Port 0 APS MEP is 1 and Port 1 APS MEP is 2.
Port 1 APS MEP	
Port 0 SF MEP	The corresponding aggression inspection MEP to ERPS port. Keep Port 0 APS MEP consistent with Port 0 SF MEP. Keep Port 1 APS MEP consistent with Port 1 SF MEP. For example: Port 0 SF MEP is 1 and Port 1 SF MEP is 2.
Port 1 SF MEP	

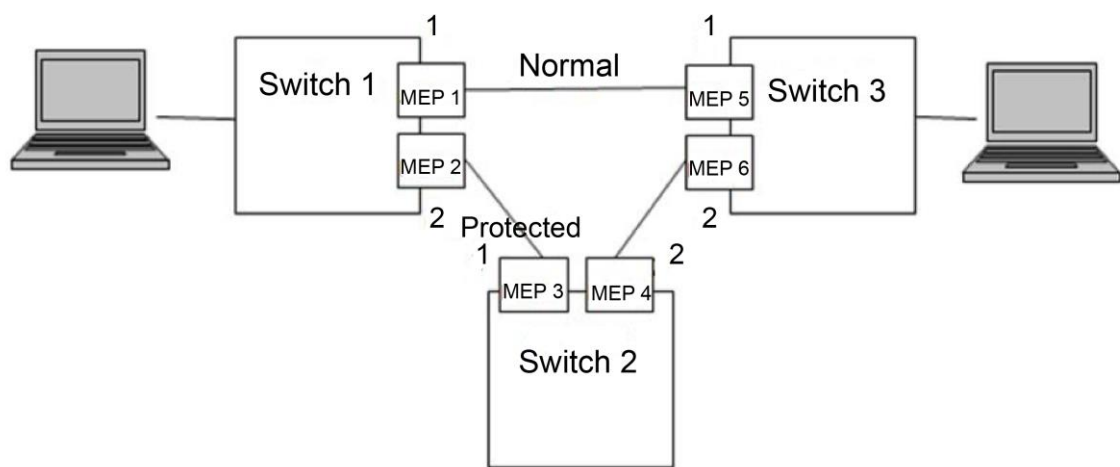
Step 4 Click **OK**.

3.2.1.3 Example: ERPS Single Ring Configuration

Networking Requirement

Three switches, port 1 and port 2 are requested to combine an ERPS. See Figure 3-28. The corresponding relationship: Switch 1: MEP 1 and MEP 2; Switch 2: MEP3 and MEP 4; Switch 3: MEP 5 and MEP 6.

Figure 3-28 ERPS single ring configuration



Configuration

Configure the ERPS with the following thoughts:

- 1) Confirm Topology, and plan protection VLAN and protocol VLAN.
- 2) Confirm RPL owner port.
- 3) Ensure to disable the mutex function of the ports.
- 4) VLAN Configuration
- 5) Create ERPS.
- 6) Create ERPS, and configure control VLAN and protection instance.
- 7) View the status.

Example

Plan protection VLAN and protocol VLAN to be 2 and 3. Set port 2 of switch 1 to be RPL owner port. Ensure to disable the mutex function of the ports, including STP function and LLDP function.

The configurations of the switch are as following:

Step 1 Configure protection VLAN and protocol VLAN are 2 and 3 separately.

- 1) Select **Advanced > Common > VLAN Settings**.
The **VLAN Settings** interface is displayed.
- 2) Set the mode of port 1 and port 2 to be **Trunk**. See Figure 3-29.
- 3) Set the port VLAN of port 1 and port 2 to be 1.
- 4) Set the allowed VLAN to be 2 and 3.
- 5) Click **Save**.

Figure 3-29 Add port 1 and port 2 into VLAN 1

VLAN Settings

VLANs The allowable range is '1-4094'. Such as '2', '3,7' or '1-9'

Port	Mode	Port VLAN	Ingress Acceptance	Egress Tagging	Allowed VLANs
1	Trunk	1	Tagged and Untagged	Untag Port VLAN	2,3
2	Trunk	1	Tagged and Untagged	Untag Port VLAN	2,3
3	Access	1	Tagged and Untagged	Untag All	1
4	Access	1	Tagged and Untagged	Untag All	1
5	Access	1	Tagged and Untagged	Untag All	1
6	Access	1	Tagged and Untagged	Untag All	1
7	Access	1	Tagged and Untagged	Untag All	1
8	Access	1	Tagged and Untagged	Untag All	1
9	Access	1	Tagged and Untagged	Untag All	1
10	Access	1	Tagged and Untagged	Untag All	1
11	Access	1	Tagged and Untagged	Untag All	1
12	Access	1	Tagged and Untagged	Untag All	1

Step 2 Create MEP1 and MEP 2

- 1) Select **Advanced > Seldom-used > ERPS > MEP Setting**.
The **MEP Setting** interface is displayed.
- 2) Click **Add**.
The **Add** interface is displayed.
- 3) Set Instance to be 1. See Figure 3-30.
- 4) Set Residence Port to be 1.
- 5) Set Level to be 0.
- 6) Set Tagged VID to be 3, that is portocal VLAN.
- 7) Click **OK**.

Figure 3-30 Add MEP

Add ✕

Instance

Residence Port

Level

Tagged VID

Add MEP2 in the same way. Set Instance to be 2, Residence port to be 2, Level to be 0 and Tagged VID to be 3.

Step 3 Click **1** and **2** separately under **Instance** to enter the configuration interface. Modify MEP ID and add peer ID. See Figure 3-31 and Figure 3-32.

Figure 3-31 Configure the peer ID of MEP 1

MEP Configuration [X]

Instance Data

Instance	Domain	MEP Mode	Direction	Residence Port	This MAC	Oper State
1	Port	MEP	ingress	1	90-02-A9-DA-67-CD	■

Instance Configuration

Level	MEP ID	Tagged VID
0	1	3

Peer MEP Configuration [Add]

<input type="checkbox"/>	Peer MEP ConfigId	Unicast Peer MAC	Delete
<input type="checkbox"/>	5	00:00:00:00:00:00	[Delete]

[Delete] [OK] [Cancel]

Figure 3-32 Configure the peer ID of MEP 2

MEP Configuration [X]

Instance Data

Instance	Domain	MEP Mode	Direction	Residence Port	This MAC	Oper State
2	Port	MEP	ingress	2	90-02-A9-DA-67-CE	■

Instance Configuration

Level	MEP ID	Tagged VID
0	1	3

Peer MEP Configuration [Add]

<input type="checkbox"/>	Peer MEP ConfigId	Unicast Peer MAC	Delete
<input type="checkbox"/>	3	00:00:00:00:00:00	[Delete]

[Delete] [OK] [Cancel]

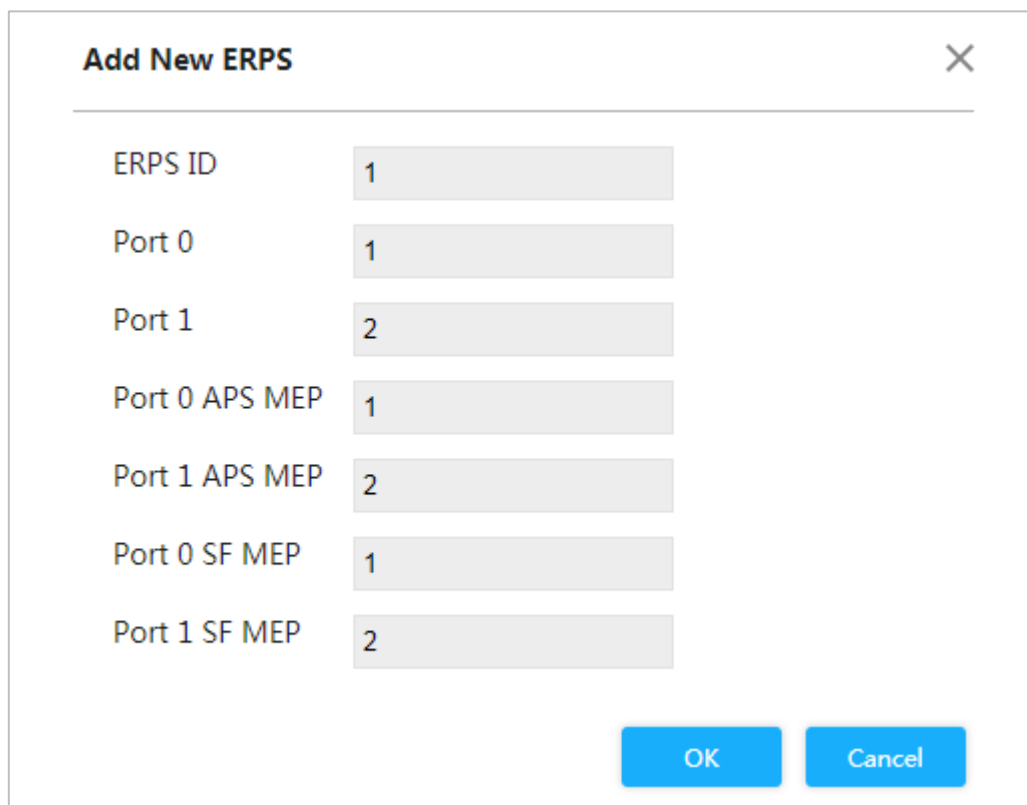
Step 4 Click **OK**.

Step 5 Create ERPS.

- 1) Select **Advanced > Seldom-used > ERPS > ERPS Setting**.
The **ERPS Setting** interface is displayed.
- 2) Click **Add**.
The **Add New ERPS** interface is displayed.
- 3) Set ERPS ID to be 1. See Figure 3-33.
- 4) Set Port 0 to be 1 and Port 1 to be 2.
- 5) Set Port 0 APS MEP to be 1 and Port 1 APS MEP to be 2.

- 6) Set Port 0 SF MEP to be 1 and Port 1 SF MEP to be 2 .
- 7) Click **OK**.

Figure 3-33 Add ERPS



ERPS ID	1
Port 0	1
Port 1	2
Port 0 APS MEP	1
Port 1 APS MEP	2
Port 0 SF MEP	1
Port 1 SF MEP	2

OK Cancel

Step 6 Click **1** under **ERPSID** to enter the configuration interface. For ERPS configuration, see Figure 3-34.

Figure 3-34 ERPS configuration

ERPS Configuration ✕

Instance Data

ERPSID	Port 0	Port 1	Port 0 APS MEP	Port 1 APS MEP	Port 0 SF MEP	Port 1 SF MEP	Ring Type
1	1	2	1	2	1	2	Major Ring

Instance Configuration

Configured	Guard Time(Ms)	WTR Time	Hold Off Time(Ms)	Version	Revertive	VLANconfig
●	500	1min	0	v2	<input checked="" type="checkbox"/>	VLANconfig

RPL Configuration

RPL Role	RPL Port	RPLClear
None	None	<input type="checkbox"/>

Instance Command

Command	CommandPort
None	None

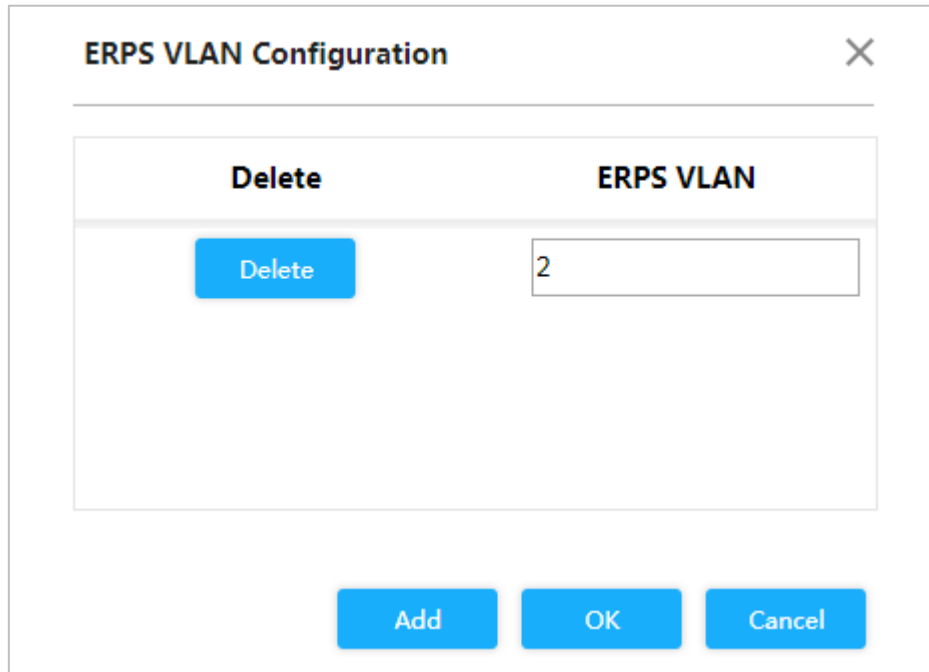
Instance State

Protection State	State Port0	State Port1	Transmit APS	Port0 ReceiveAPS	Port1 Receive APS	WTR Remaining	RPL Unblocked	No APS Received	Port0 BlockStatus	Port1 BlockStatus	FOP Alarm
Protected	OK	SF	2	0	0	0	●	●	Blocked	Unblocked	●

OK
Cancel

- 1) Click **VLANconfig**.
The **ERPS VLAN Configuration** interface is displayed.
- 2) Click **Add**.
- 3) Set ERPS VLAN to be 2. See Figure 3-35.
- 4) Click **OK**.

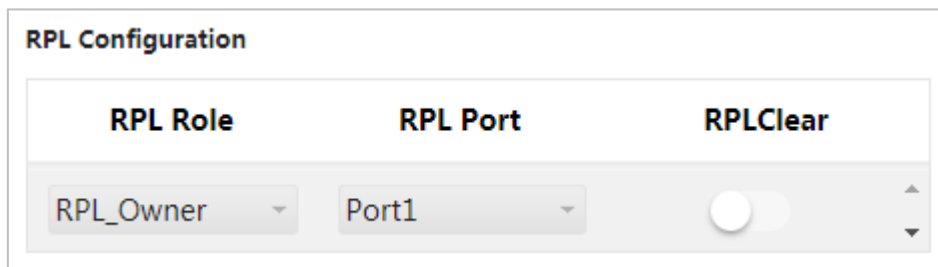
Figure 3-35 ERPS VLAN configuration



The dialog box titled "ERPS VLAN Configuration" contains a table with two columns: "Delete" and "ERPS VLAN". Under "Delete" is a blue "Delete" button. Under "ERPS VLAN" is a text input field containing the number "2". At the bottom of the dialog are three blue buttons: "Add", "OK", and "Cancel".

- 5) Set port 2 of switch 1 to be RPL owner in RPL Configuration. See Figure 3-36.

Figure 3-36 Ower port configuration



The dialog box titled "RPL Configuration" contains a table with three columns: "RPL Role", "RPL Port", and "RPLClear". Under "RPL Role" is a dropdown menu showing "RPL_Owner". Under "RPL Port" is a dropdown menu showing "Port1". Under "RPLClear" is a toggle switch that is currently turned off.

Step 7 Click **OK**.

Step 8 Configure switch 2 and switch 3 in the same way.

Step 9 View the state in **Instance State** on the **ERPS Configuration** interface.

Figure 3-37 Instance state

Instance State											
Protection State	State Port0	State Port1	Transmit APS	Port0 Receive	Port1 Receive	WTR APS Remaining	RPL Unblocked	No APS Received	Port0 BlockStatus	Port1 BlockStatus	FOP Alarm
Pending	OK	SF	2	0	0	48680	●	●	Unblocked	Blocked	●

3.2.2 ACL

ACL (Access Control List) is for flow identification. For filtering the packet, the network device needs to configure a series of matching conditions to classify the packets. The conditions can be the source address, destination address, and the port number of the packet.

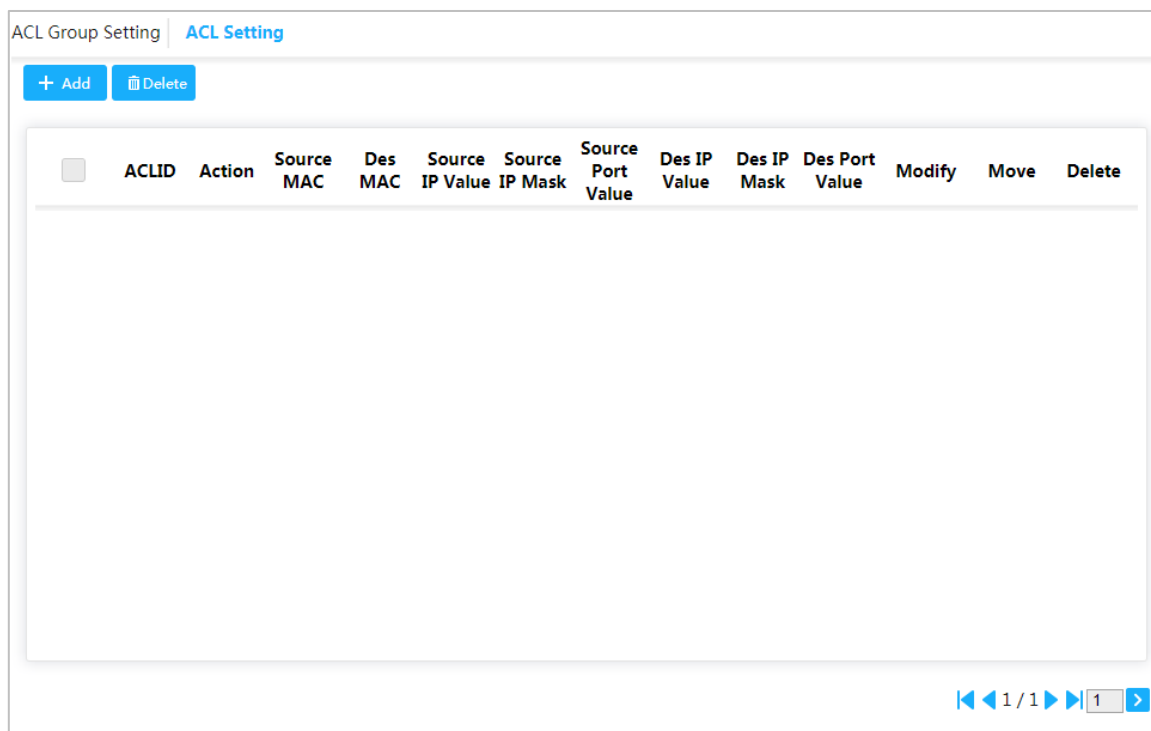
When the device port receives the packet, it can analyze the packet field according to the ACL rule of the current port. And after the specific packet is identified, the packet is allowed or forbidden to pass according to the preset rule.

3.2.2.1 ACL Configuration

Step 1 Select **Advanced > Seldom-used > ACL > ACL Setting**.

The **ACL Setting** interface is displayed. See Figure 3-38.

Figure 3-38 ACL configuration



Step 2 Click **Add**.

The **Add** interface is displayed. See Figure 3-39.

Figure 3-39 Add

Add [Close]

Mode: MAC ACL

ACL ID: [Text Input]

Action: Permit

Source MAC: any

Source MAC Address: [Text Input]
such as 00:23:AE:77:10:53

Des MAC: any

Destination MAC Address: [Text Input]

[OK] [Cancel]

Step 3 Set the ACL ID, and the range is 1~128.

Step 4 Click **OK**.

3.2.2.2 ACL Group Configuration

Step 1 Select **Advanced > Seldom-used > ACL > ACL Group Setting**.

The **ACL Group Setting** interface is displayed. See Figure 3-40.

Figure 3-40 ACL group configuration

ACL Group Setting | ACL Setting

Port	ACLID
1	[Text Input]
2	[Text Input]
3	[Text Input]
4	[Text Input]
5	[Text Input]
6	[Text Input]
7	[Text Input]
8	[Text Input]

[Save] [Refresh]

Step 2 Enter ACL ID. Ensure the ACL ID has been added during ACL configuration.

Step 3 Click **Save**.

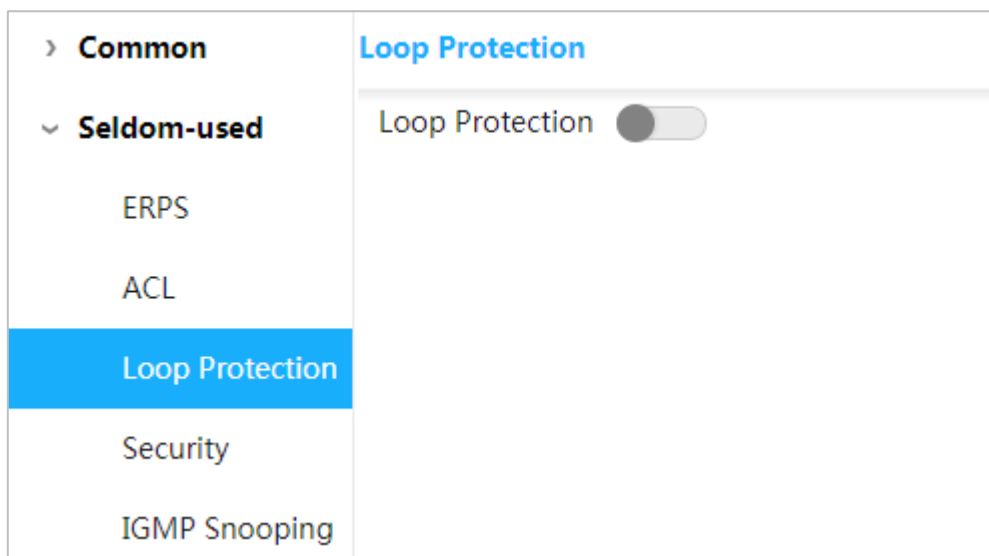
3.2.3 Loop Protection

Detect the loop among the ports. After the device has detected the loop, it will break the loop.

Step 1 Select **Advanced > Seldom-used > Loop Protection**.

The **Loop Protection** interface is displayed. See Figure 3-41.

Figure 3-41 Loop protection



Step 2 Click Loop  to enable Loop Protection

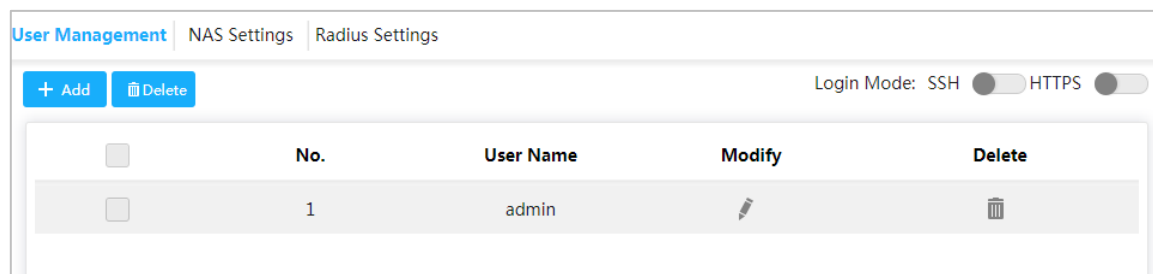
3.2.4 Security

3.2.4.1 User Management

You can add, edit, and delete the user.

Select **Advanced > Seldom-used > Security > User Management**. And the **User Management** interface is displayed. See Figure 3-42.

Figure 3-42 User management



Add user

Step 1 Click **Add**.

The **Add User** interface is displayed. See Figure 3-43.

Figure 3-43 Add user

Add User [Close]

User Name [Input Field]

Password [Input Field]

Confirm Password [Input Field]

[OK] [Cancel]

Step 2 Enter the user name, password, and confirm password. The password can be set from 8 characters through 32 characters and contains at least two types from number, letter, and special characters (excluding "", "", ";", ":" and "&"). For example, add the new user test 01.

Step 3 Click **Save**.

The new user test 01 is added. See Figure 3-44.

Figure 3-44 New user added

User Management | NAS Settings | Radius Settings


+ Add Delete Login Mode: SSH [On] HTTPS [Off]

<input type="checkbox"/>	No.	User Name	Modify	Delete
<input type="checkbox"/>	1	admin		
<input type="checkbox"/>	2	test01		

Modify and Delete User

- Click , and the **Modify User** interface is displayed. See Figure 3-45.

Figure 3-45 Modify user


- Click  to delete the user.



You can not delete the admin user.


SSH

You can enable or disable SSH function.

Click  corresponding to SSH on the upper right corner of the **User Management** interface.

HTTPS

HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer) is the HTTP channel for security target. SSL layer and TLS layer are added to HTTP. SSL and TLS are the security foundation of HTTP, so SSL/TLS are requested for encryption. HTTPS is the URI scheme, and the syntax is similar to HTTP. so SSL/TLS are requested for encryption. HTTPS is the URI scheme, and the syntax is similar to HTTP. It is used for security HTTP data transmission. Built in the web Netscape Navigator, it provides authentication and encryption communication. It is widely applied in world wide web for security sensitive communication. For example, to protect account security and use information.

Click  corresponding to HTTPS on the upper right corner of the **User Management** interface to enable HTTPS service.

3.2.4.2 NAS Configuration

NAS (Network Access Server) is a server that allows ISP to provide Internet access service.

Step 1 Select **Advanced > Seldom-used > Security > NAS Settings**.

The **NAS Settings** interface is displayed. See Figure 3-46.

Figure 3-46 NAS configuration

User Management | **NAS Settings** | Radius Settings

Mode

Reauthentication Enabled

Port	Admin State	Port State
1	<input type="text" value="Force Authorized"/>	Globally Disabled
2	<input type="text" value="Force Authorized"/>	Globally Disabled
3	<input type="text" value="Force Authorized"/>	Globally Disabled
4	<input type="text" value="Force Authorized"/>	Globally Disabled
5	<input type="text" value="Force Authorized"/>	Globally Disabled
6	<input type="text" value="Force Authorized"/>	Globally Disabled
7	<input type="text" value="Force Authorized"/>	Globally Disabled

Step 2 Select **Mode** as **Enabled** to enable mirroring function.

Step 3 Select the **Reauthentication Enable** box to enable reauthentication.

Step 4 Set **Admin State: Force Authorized, Force Unauthorized, Prot based 802.1X** or **MAC-based Auth**.

Step 5 Click **Save**.

3.2.4.3 Radius Configuration

RADIUS (Remote Authentication Dial-In User Service) is a common protocol to realize AAA (Authentication, Authorization and Accounting).

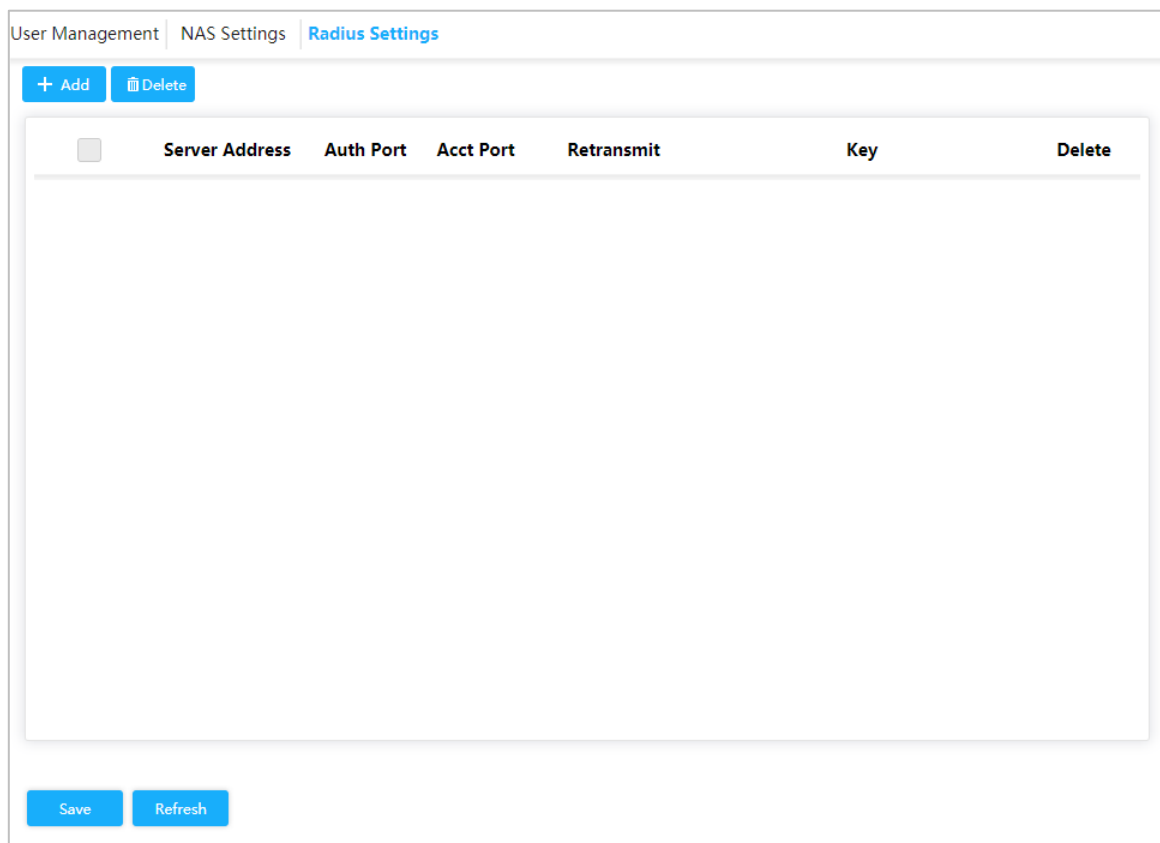
RADIUS is an information interaction protocol of distributed and C/S construction. It can protect the network from the interfere of unauthorized visits. It is used in the network that allows remote visits but requests the higher security. It defines the RADIUS packet format and the message transmission mechanism. It stipulates that using UDP as transport layer protocol to encapsulate the RADIUS packet.

At the beginning, RADIUS is the AAA protocol for the dial-up users only. With the development of the user accesses, RADIUS adapts to various access, including Ethernet access and ADSL access. It accesses server through authentication and authorization, and collects records the usage of network source through accounting.

Step 1 Select **Advanced > Seldom-used > Security > Radius Settings**.

The **Radius Settings** interface is displayed. See Figure 3-47.

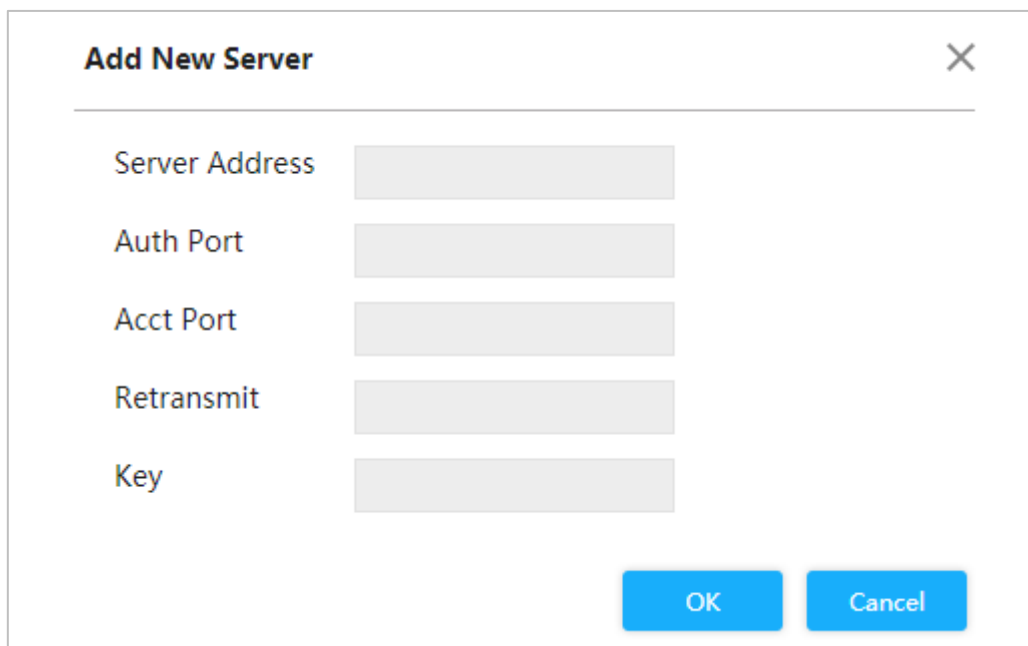
Figure 3-47 Radius configuration



Step 2 Click **Add**.

The **Add New Server** interface is displayed. See Figure 3-48.

Figure 3-48 Add new server



The image shows a dialog box titled "Add New Server" with a close button (X) in the top right corner. The dialog contains five input fields, each with a label to its left: "Server Address", "Auth Port", "Acct Port", "Retransmit", and "Key". At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

Step 3 Set the server address, auth port, acct port, retransmit and key.

Step 4 Click **OK**.

3.2.5 IGMP Snooping

IGMP Snooping (Internet Group Management Protocol Snooping) is the multicast constraint mechanism running on the device of layer 2, for managing and controlling the multicast. Through analyzing the received IGMP packet, the device of layer 2, which runs IGMP Snooping, creates the mapping between the port and the MAC multicast address, and forwards the multicast data according to the mapping.

Step 1 Select **Advanced > Seldom-used > IGMP Snooping**.

The **IGMP Snooping** interface is displayed. See Figure 3-49.

Figure 3-49 IGMP snooping

IGMP Snooping

IGMP Snooping Disable Enable

Discarding Unknown IGMP Packets Disable Enable

+ Add **- Delete**

<input type="checkbox"/>	VLAN ID	Querier Election	Querier Address	Delete

Save **Refresh**

Step 2 Select **Enable IGMP Snooping** to enable the function.

Step 3 Select **Disable** or **Enable Discarding Unknown IGMP Packets**.

Step 4 Click **Add**.

The **Add VLAN** interface is displayed. See Figure 3-50.

Figure 3-50 Add VLAN

Add VLAN ✕

VLAN ID

Querier Election

Querier Address

OK **Cancel**

Step 5 Set VLAN ID and querier address, and select the **Querier Election** box to enable the querier

Step 6 Click **OK**.

3.2.6 QoS

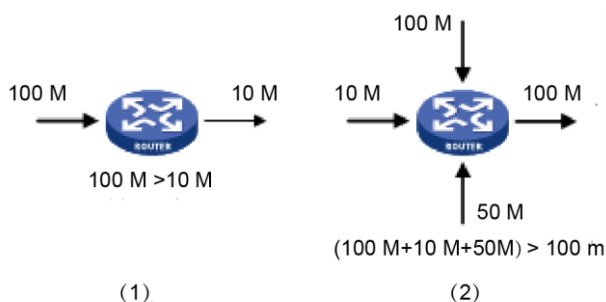
QoS (Quality of Service) is used to evaluate the capability that server meets customer's service demands. In Internet, what QoS evaluates is the service capability of network forwarding and packet.

QoS can evaluate from the different aspects according to the various services provided by the network. QoS evaluates bandwidth, delay, dithering and packet loss during packet and forwarding.

Congestion

Congestion is common in a complex Internet packet switched environment. See the following example:

Figure 3-51 Flow congestion



- 1) The packet comes in the device by the high-speed link and exits by low-speed link.
- 2) The packet comes in the device from multiple ports and exits from one port (The speed rate of multiple ports larger than that of the exit port).

If the flow arrives at linear speed, it will encounter the resource chock point, and then the congestion will generate.

Besides the aggression bandwidth, any other resource shortages (such as the shortages of distributive processing time, buffer and memory resources) will cause congestion. Additionally, the poor control of the arrived flow in a certain time, which leads to the flow exceeding the distributive network resource, is also a factor for generating congestion.

3.2.6.1 Port

Through setting Cos, the priority for packet passing egress port of switch can be decided.

If the congestion occurs at the egress port, the switch will give a CoS value to the packet after it passing the ingress port.

The larger the Cos value, the higher the priority.

Step 1 Select **Advanced > Seldom-used > QoS > Port Classification**.

The **Port Classification** interface is displayed. See Figure 3-52.

Figure 3-52 Port classification

Port Classification | Port Schedulers | Port Shapers | DSCP-Based | Storm Policer

Port	CoS	<input type="checkbox"/> DSCP
1	0	<input type="checkbox"/>
2	0	<input type="checkbox"/>
3	0	<input type="checkbox"/>
4	0	<input type="checkbox"/>
5	0	<input type="checkbox"/>
6	0	<input type="checkbox"/>
7	0	<input type="checkbox"/>

Step 2 Set CoS. For example: Set port 1 to be 1, and port 2 to be 2. See Figure 3-53.

Port 1 and port 2 are ingress ports, and port 3 is egress port. The Cos value of port 2 is large than that of port 1, so the data of port 2 will pass port 3 first.

Figure 3-53 Set Cos

Port Classification | Port Schedulers | Port Shapers | DSCP-Based | Storm Policer

Port	CoS	<input type="checkbox"/> DSCP
1	1	<input type="checkbox"/>
2	2	<input type="checkbox"/>
3	0	<input type="checkbox"/>
4	0	<input type="checkbox"/>
5	0	<input type="checkbox"/>
6	0	<input type="checkbox"/>
7	0	<input type="checkbox"/>

Step 3 Click **Save**.

3.2.6.2 Port Schedulers

The two modes of port schedulers:

- **Strict Priority.** When congestion occurs, the priority for packet passing egress port of switch depends on the Cos value in **Port Classification**.
- **2~8 Queues Weighted.** When congestion occurs, the priority for packet passing egress port of switch depends on the proportion of total rate.

Step 1 Select **Advanced > Seldom-used > QoS > Port Schedulers**.

The **Port Schedulers** interface is displayed. See Figure 3-54.

Figure 3-54 Port schedulers

Port Classification									
Port Schedulers									
Port Shapers									
DSCP-Based									
Storm Policer									
Port	Mode	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
1	Strict Priority	-	-	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-	-	-

Step 2 Click the port, such as port 1.

The **QoS Egress Port Schedulers and Shapers Port 1** interface is displayed. See Figure 3-55. The CoS of Q0 is 0., and so on.

Figure 3-55 Port configuration

QoS Egress Port Scheduler and Shapers Port 1
✕

Scheduler Mode Strict Priority

QPort	Ingress Queue Shaper				Queue Scheduler	
	<input type="checkbox"/> Enable	Rate	Unit	Rate-type	Weight	Percent
Q0	<input type="checkbox"/>	500	kbps	Line	-	-
Q1	<input type="checkbox"/>	500	kbps	Line	-	-
Q2	<input type="checkbox"/>	500	kbps	Line	-	-
Q3	<input type="checkbox"/>	500	kbps	Line	-	-
Q4	<input type="checkbox"/>	500	kbps	Line	-	-
Q5	<input type="checkbox"/>	500	kbps	Line	-	-
Q6	<input type="checkbox"/>	500	kbps	Line	-	-
Q7	<input type="checkbox"/>	500	kbps	Line	-	-

Egress Queue Shaper

<input type="checkbox"/> Enable	Rate	Unit	Rate-type
<input type="checkbox"/>	500	kbps	Line

OK
Cancel

Step 3 Select mode.

- **Strict Priority.** The priority for packet passing egress port of switch depends on the Cos value in **Port Classification**.
- **2~8 Queues Weighted.** When congestion occurs, the priority for packet passing egress port of switch depends on the proportion of total rate.

For example: select **Scheduler Mode** as **2 Queues Weighted**. The max speed limit of port 1 and port 2 is 500 kbps. When congestion occurs, 50% ingress port packet will pass the egress port. See the following for the configuration:

- 1) Select **Scheduler Mode** as **2 Queues Weighted**. See Figure 3-56.
- 2) In **Ingress Queue Shaper**, set the **Rate** of **Q0** and **Q1** to be 500 kbps, and **Rate-type** to be Line.
- 3) In **Egress Queue Shaper**, set the **Rate** to be 500 kbps, and **Rate-type** to be Line. When congestion occurs, and the speed of the two port are 400 kbps, the speed passing the egress port is 250 kbps.

Figure 3-56 Port schedulers

QoS Egress Port Scheduler and Shapers Port 1 ✕

Scheduler Mode 2 Queues Weighted

Ingress Queue Shaper					Queue Scheduler	
QPort	<input type="checkbox"/> Enable	Rate	Unit	Rate-type	Weight	Percent
Q0	<input checked="" type="checkbox"/>	500	kbps	Line	50	50%
Q1	<input checked="" type="checkbox"/>	500	kbps	Line	50	50%
Q2	<input type="checkbox"/>	500	kbps	Line		
Q3	<input type="checkbox"/>	500	kbps	Line		
Q4	<input type="checkbox"/>	500	kbps	Line		
Q5	<input type="checkbox"/>	500	kbps	Line		
Q6	<input type="checkbox"/>	500	kbps	Line		
Q7	<input type="checkbox"/>	500	kbps	Line		

Egress Queue Shaper

<input checked="" type="checkbox"/> Enable	Rate	Unit	Rate-type
<input checked="" type="checkbox"/>	500	kbps	Line

Step 4 Click **OK**.

3.2.6.3 Port Shapers

The configuration is the same for port schedulers and port shapers. The only difference is that the port schedulers interface shows the weight value and the port shapers interface shows the speed rate.

Select **Advanced > Seldom-used > QoS > Port Shapers**. The **Port Shapers** interface is displayed. See Figure 3-57.

Figure 3-57 Port shapers

Port	Q0(kbps)	Q1(kbps)	Q2(kbps)	Q3(kbps)	Q4(kbps)	Q5(kbps)	Q6(kbps)	Q7(kbps)	Port Speed(kbps)
1	500	500							500
2									
3									
4									
5									
6									
7									

3.2.6.4 DSCP-Based

Make sure that you have enabled DSCP before configuring DSCP function.

Step 1 Select **Advanced > Seldom-used > QoS > Port Classification**.

The **Port Classification** interface is displayed.

Step 2 Enable DSCP at DSCP port. Suppose port 3 is the egress port, see Figure 3-58.

Figure 3-58 Port classification

Port Classification | Port Schedulers | Port Shapers | DSCP-Based | Storm Policer

Port	CoS	<input type="checkbox"/> DSCP
1	0	<input type="checkbox"/>
2	0	<input type="checkbox"/>
3	0	<input checked="" type="checkbox"/>
4	0	<input type="checkbox"/>
5	0	<input type="checkbox"/>
6	0	<input type="checkbox"/>
7	0	<input type="checkbox"/>

Step 3 Click **Save**.

Step 4 Select **Advanced > Seldom-used > QoS > DSCP-Based**.

The **DSCP-Based** interface is displayed.

Step 5 When setting DSCP to be 4 and 8, the CoS is 2 and DPL are 2 and 1.

- 1) When DSCP are 4 and 8, select **Trust** to enable the function. See Figure 3-59.
- 2) When setting DSCP to be 4, CoS is 2 and DPL is 2.
- 3) When setting DSCP to be 8, CoS is 2 and DPL is 1.

The larger the CoS and DPL of DSCP, the higher the priority. When the CoS is the same, the larger DPL, the higher the priority. The corresponding port packet will pass the egress port first.

Figure 3-59 DSCP-Based

Port Classification | Port Schedulers | Port Shapers | **DSCP-Based** | Storm Policer

DSCP	<input type="checkbox"/> Trust	CoS
0	<input type="checkbox"/>	0
1	<input type="checkbox"/>	0
2	<input type="checkbox"/>	0
3	<input type="checkbox"/>	0
4	<input checked="" type="checkbox"/>	2
5	<input type="checkbox"/>	0
6	<input type="checkbox"/>	0
7	<input type="checkbox"/>	0
8	<input checked="" type="checkbox"/>	1
9	<input type="checkbox"/>	0

Step 6 Click **Save**.

3.2.6.5 Storm Policer

Inhibit the three packets, including unicast, multicast and broadcast.

Step 1 Select **Advanced > Seldom-used > QoS > Storm Policer**.

The **Storm Policer** interface is displayed. See Figure 3-60.

Figure 3-60 Storm policer

Port Classification | Port Schedulers | Port Shapers | DSCP-Based | **Storm Policer**

Frame Type	<input type="checkbox"/> Enable	Rate	Unit
Unicast	<input type="checkbox"/>	1	fps
Multicast	<input type="checkbox"/>	1	fps
Broadcast	<input type="checkbox"/>	1	fps

[Save](#)

Step 2 The port can receive the rate up to 1024 fps. See Figure 3-61.

- In **Unicast**, select the **Enable** box, and enter 1024 in **Rate**. It means that the port can receive the rate up to 1024 fps of unicast packet.
- In **Multicast**, select the **Enable** box, and enter 1024 in **Rate**. It means that the port can receive the rate up to 1024 fps of multicast packet.
- In **Broadcast**, select the **Enable** box, and enter 1024 in **Rate**. It means that the port can receive the rate up to 1024 fps of broadcast packet.

Figure 3-61 Storm policer configuration

Port Classification | Port Schedulers | Port Shapers | DSCP-Based | **Storm Policer**

Frame Type	<input checked="" type="checkbox"/> Enable	Rate	Unit
Unicast	<input checked="" type="checkbox"/>	1024	fps
Multicast	<input checked="" type="checkbox"/>	1024	fps
Broadcast	<input checked="" type="checkbox"/>	1024	fps

[Save](#)

Step 3 Click **Save**.

3.2.7 SNMP

SNMP (Simple Network Management Protocol) is the standard protocol for network management in Internet, and it is widely applied for management device to access and manage the managed devices. SNMP has the following features:

- It supports intelligent management for network device. By using the network management platform based on SNMP, the network administrator can query the running status and the parameters of the network device, and can set the parameter, find the error, perform fault diagnosis, and then to plan the capacity and create the report.
- SNMP supports to manage the devices of different physical features. SNMP provides only the most basic function library. It makes the management task and the physical feature and the networking technology of the managed device independent, to manage the devices from different manufacturers.

SNMP network provides two elements, NMS and Agent.


- NMS (Network Management System) is the manager in SNMP network, and it provides friendly human-machine interface to help the network administrator to finish most of the network management work.
- Agent is the managed role in SNMP network, and it receives and handles the request packet from NMS. In some emergency circumstances, for example, if the port status changes, Agent can send alarm packet to NMS proactively.

3.2.7.1 Enable SNMP Function

Step 1 Select **Advanced > Seldom-used > SNMP**.

The **SNMP** interface is displayed. See Figure 3-62.

Figure 3-62 SNMP

Step 2 Click  in **SNMP** to enable SNMP.



Every SNMP v3 agent has an engine ID as its unique identifier.

3.2.7.2 Configuring SNMP v1/v2

Example: Configure SNMP v1. The configuration of SNMP v2 is the same with that of SNMP v1.

Step 1 Select SNMP v1 in **SNMP Version**.

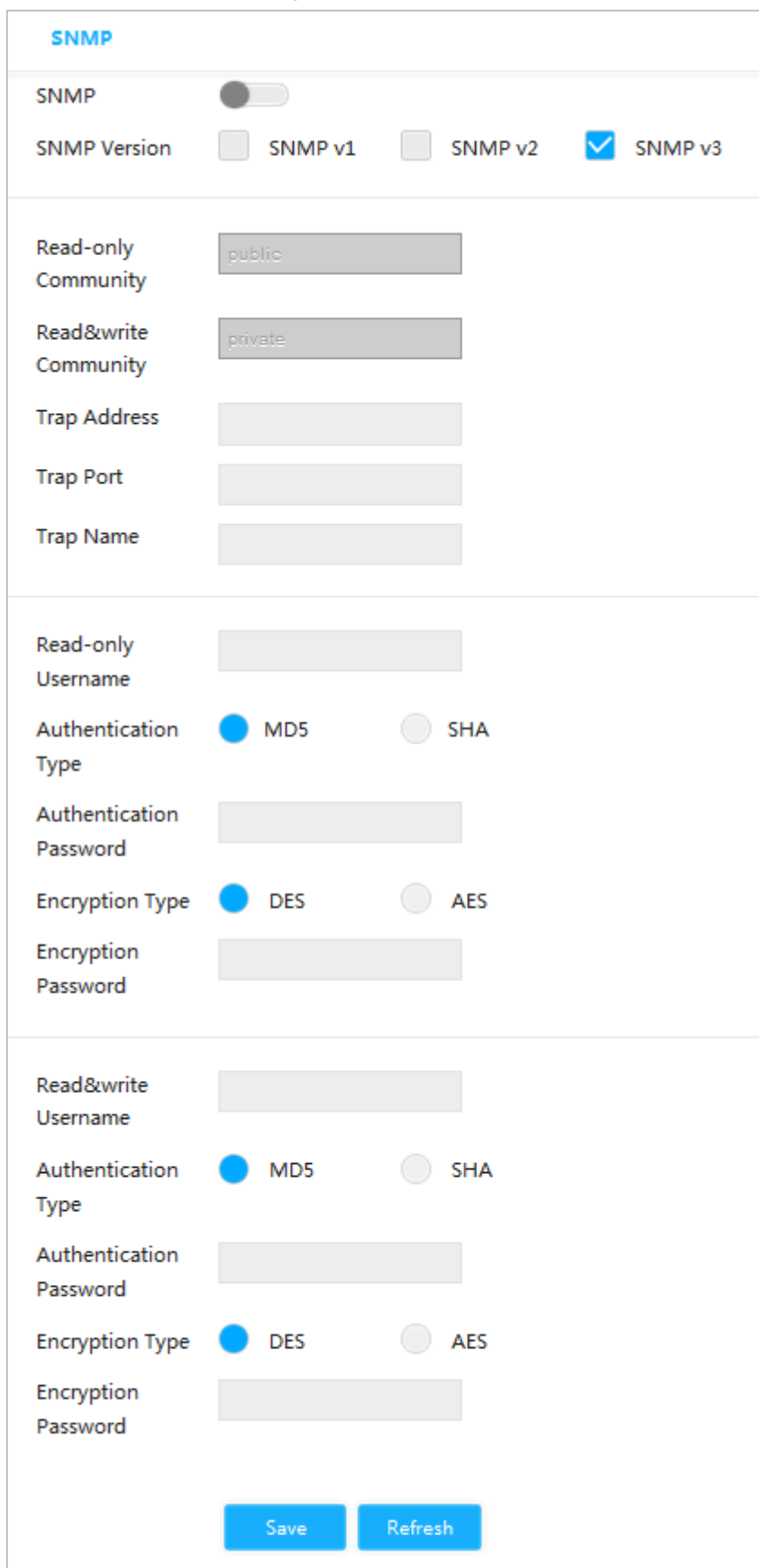
Step 2 Set the read-only community, read&write community, trap address and trap port.

Step 3 Click **Save**.

3.2.7.3 Configuring SNMP v3

Step 1 Select SNMP v3 in **SNMP Version**. See Figure 3-63.

Figure 3-63 SNMP v3



The image shows a web-based configuration interface for SNMP v3. It is divided into several sections. At the top, there is a toggle switch for 'SNMP' which is currently turned off. Below this, there are three radio buttons for 'SNMP Version': 'SNMP v1', 'SNMP v2', and 'SNMP v3'. The 'SNMP v3' option is selected with a blue checkmark. The next section contains three text input fields: 'Read-only Community' with the value 'public', 'Read&write Community' with the value 'private', and 'Trap Address'. Below these are two more text input fields: 'Trap Port' and 'Trap Name'. The following section is for the 'Read-only' user, featuring a text input for 'Read-only Username', a radio button selection for 'Authentication Type' (MD5 is selected), a text input for 'Authentication Password', a radio button selection for 'Encryption Type' (DES is selected), and a text input for 'Encryption Password'. The final section is for the 'Read&write' user, with identical fields for 'Read&write Username', 'Authentication Type' (MD5 selected), 'Authentication Password', 'Encryption Type' (DES selected), and 'Encryption Password'. At the bottom of the interface are two blue buttons: 'Save' and 'Refresh'.

Step 2 Set the trap address, trap port and trap name.

Step 3 Set the read-only username, authentication type, authentication password, encryption type and encryption password.

Step 4 Set the read&write username, authentication type, authentication password, encryption type and encryption password.

Step 5 Click **Save**.

3.2.8 DHCP Server

DHCP Server is the server for managing DHCP standard in the specific network. DHCP Server is to allocate IP address for the workstation and make sure that the IP address for every workstation is different. DHCP Server simplifies the network management task which should be done manually before.

Generally, in the following scenes, DHCP Server is adopted to allocate IP address.

- The network scale is large. The workload is too heavy if manually configured, and centralized management for network will be difficult.
- The quantity of PC is larger than the quantity of IP address in the network, and it is impossible to allocate a static IP address for every PC. For example, the user quantity that can access network at the same time is limited by ISP, and the user needs to acquire the IP address dynamically.
- Only a small number of PC need the static IP address, and most of the PC do not need the static IP address.

There are three parts of DHCP Server configuration: **VLAN Mode**, **Excluded IP** and **Pool**.

Step 1 Select **Advanced > Seldom-used > DHCP > DHCP Server**.

The **DHCP Server** interface is displayed. See Figure 3-64.

Figure 3-64 DHCP Server

DHCP Server

Global Mode

VLAN Mode

<input type="checkbox"/>	Vlan Range	Delete

Excluded IP

<input type="checkbox"/>	Excluded IP	Delete

Pool

<input type="checkbox"/>	Name	Type	IP	Subnet mask	Default Gateway	Lease Time	Delete

Step 2 Click  in **Global Mode**, to enable DHCP Server function.

Step 3 Configure DHCP mode.



Add VLAN interface first. See “3.1.1.2IP and route.”

1) Click **Add** in **Vlan Mode**.

The **Add VLAN Mode** interface is displayed. See Figure 3-65.

Figure 3-65 Add VLAN mode

2) Enter the VLAN range, such as 2-4.

3) Click **OK**.

Step 4 Configure network segment of excluded IP.



Excluded IP refers to the IP reserved for the server, which will not assign to the client.

1) Click **Add** in **Excluded IP**.

The **Add Excluded IP** interface is displayed. See Figure 3-66.

Figure 3-66 Add excluded IP

2) Enter the IP address range, such as 192.168.100.2-192.168.100.50.

3) Click **OK**.

Step 5 Add DHCP address pool.

4) Click **Add** in **Pool**.

The **Add Pool** interface is displayed. See Figure 3-67.

Figure 3-67 Add pool

5) For the parameters. See Table 3-7.

Table 3-7 Pool parameters

Parameter	Description
Pool Name	DHCP address pool name, such as vlan2_test.
Type	Two types: Network and Host . <ul style="list-style-type: none"> • Network: The network segment of an IP. • Host: A specific IP
IP	The IP address of the host or the network.
Subnet Mask	The subnet mask of the host or the network.
Lease Time	Enter the lease time of the address pool.
Gateway	Configure the default gateway of the address pool.

6) Click **OK**.

3.2.9 LLDP

LLDP (Link Layer Discovery Protocol) is a standard link layer discovery way. It can form its main capabilities, management address, device no and port no as TLV (Type Length Value), encapsulate it in LLDPDU (Link Layer Discovery Protocol Data Unit), and advertises it to its neighbour. The neighbour will keep the received information in the form of standard MIB (Management Information Base), so that the network management can query and judge the communication state of the link.

LLDP

Step 1 Select **Advanced > Seldom-used > LLDP**.

The **LLDP** interface is displayed. See Figure 3-68.

Figure 3-68 LLDP

Interface	Mode
1	Enable
2	Enable
3	Enable
4	Enable
5	Enable
6	Enable
7	Enable

Save

Step 2 Set LLDP mode.

- Select **Enable**: Both send and receive LLDP packet.
- Select **Disable**: Neither send nor receive LLDP packet.
- Select **Rx only**: Only receive LLDP packet.
- Select **Tx only**: Only send LLDP packet.

Step 3 Click **Save**.

View the LLDP Neighbor Information.

Select **Advanced > Seldom-used > LLDP > LLDP Neighbor**. The **LLDP Neighbor** interface is displayed. See Figure 3-69.

Figure 3-69 LLDP neighbor

LLDP		LLDP Neighbor			
LLDP Remote Device Summary					
Local Interface	Port ID	Port Description	System Name	System Capabilities	Management Address
GigabitEthernet 1/8	Ethernet1/0/5	Ethernet1/0/5 Interface	SW1	Bridge(+), Router(+)	192.168.1.1 (IPv4) - if-index:12 OID: 0.0

3.2.10 485 Config

Transmit the data of asynchronous serial port RS232/485 transparently through Ethernet.

Select **Advanced > Seldom-used > 485 Config**. The **485 Config** interface is displayed. See Figure 3-70.

Figure 3-70 485 config

485 Config

Serial Index:

Enable: ON OFF

Network Setting:

Protocol Type:

IP Address:

IP Port:

Timeout(s):

Serial Setting:

Serial Speed:

Data Bits:

Parity Bits:

Stop Bits:

3.2.11 PoE

PoE (Power Over Ethernet) is the function that through Ethernet RJ-45 port, the device can provide power for the external PD remotely with twisted pair. PoE function helps to centralize power supply and facilitate backup. The network terminal does not need the external power source anymore, and one network cable is enough, It conforms to the standards of IEEE 802.3af and IEEE 802.3at, adopting the power interface globally agreed. It can be applied in IP telephone, wireless AP (Access Point), portable device charger, card reader, network camera, data collection, and so on.

3.2.11.1 PoE parameters.

Configure reserved power, warning power, enable or disable PoE.

Step 1 Select **Advanced > Seldom-used > PoE > PoE Settings**.

The **PoE Settings** interface is displayed. See Figure 3-71.

Figure 3-71 PoE settings

The screenshot shows the PoE Settings interface with the following sections:

- PoE Settings:**
 - Total Power: 120 W
 - Available Power: 108 W
 - Overload: 120 W
- Power Status:**
 - Consumed: 0 W
 - Remaining: 120 W
 - Reserved: 0 W
- Port Status and Control:**

Port	Consumed	<input checked="" type="checkbox"/> Enable	PD Class	Status
1	0	<input checked="" type="checkbox"/>	-	No PD detected
2	0	<input checked="" type="checkbox"/>	-	No PD detected
3	0	<input checked="" type="checkbox"/>	-	No PD detected
4	0	<input checked="" type="checkbox"/>	-	No PD detected

At the bottom, there are **Save** and **Refresh** buttons.

Step 2 In **PoE Settings**, you can view the total power of the 4 ports, and configure available power and overload power.

Step 3 In **Power Status**, you can view consumed power, remaining power and reserved power.

Step 4 In **Port Status and Control**, select the **Enable** box to enable or disable PoE of the corresponding port.

Step 5 Click **Save**.

3.2.11.2 Green PoE

Set PoE Off time and PoE On time.

Step 1 Select **Advanced > Seldom-used > PoE > Green PoE**.

The **Green PoE** interface is displayed. See Figure 3-72.

Figure 3-72 Green PoE

PoE Settings	Green PoE	Legacy Support	PoE Event Statistics
PoE Off Time:	Monday	16 : 18 : 42	
PoE On Time:	Monday	16 : 18 : 42	
<input type="checkbox"/> Enable			
	<input type="checkbox"/>	Port	1
	<input type="checkbox"/>		2
	<input type="checkbox"/>		3
	<input type="checkbox"/>		4
<input type="button" value="Save"/>			

Step 2 Set **PoE Off Time**.

Step 3 Set **PoE On Time**.

Step 4 Select the **Enable** box.

Step 5 Click **Save**.

3.2.11.3 Legacy Support

Enable **Legacy Support** when the device power supplied does not conform to standard.

Select **Advanced > Seldom-used > PoE > Legacy Support**.

The **Legacy Support** interface is displayed. See Figure 3-73.

Figure 3-73 Legacy support

PoE Settings	Green PoE	Legacy Support	PoE Event Statistics
The port will provide power compulsorily no matter whether the connected PD device conforms to standard or not after Legacy Support is enabled. Please use it carefully!			
<input type="checkbox"/> Enable			
	<input type="checkbox"/>	Port	1
	<input type="checkbox"/>		2
	<input type="checkbox"/>		3
	<input type="checkbox"/>		4
<input type="button" value="Save"/>			

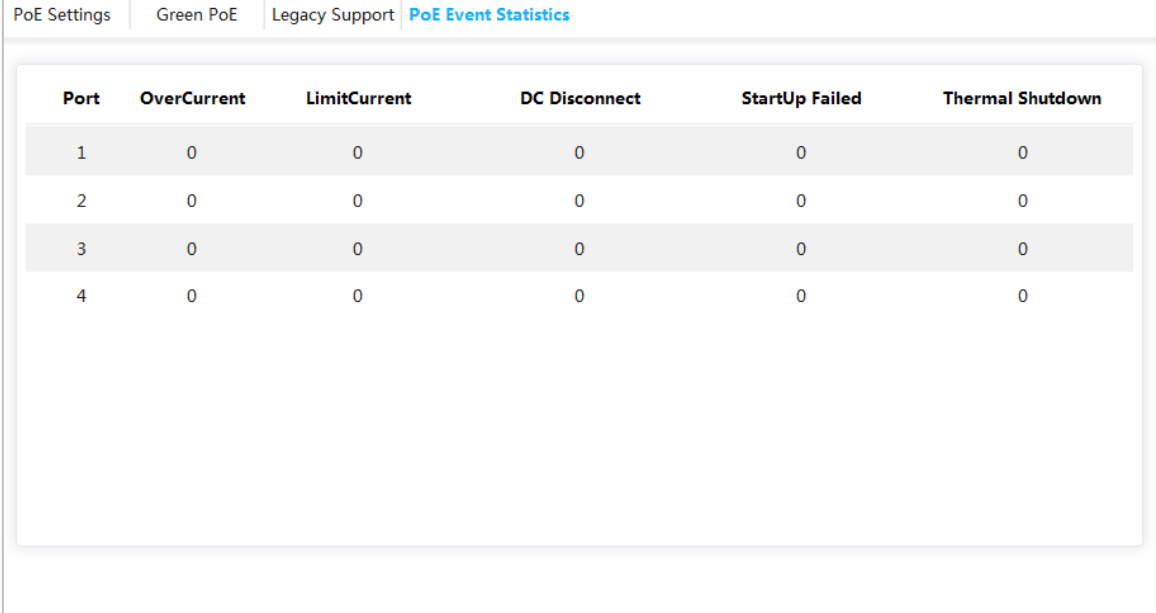
Step 6 Select the **Enable** box.

Step 7 Click **Save**.

3.2.11.4 View PoE event statistics

Select **Advanced > Seldom-used > PoE > PoE Event Statistic**. The **PoE Event Statistic** interface is displayed. See Figure 3-74.

Figure 3-74 PoE event statistic



Port	OverCurrent	LimitCurrent	DC Disconnect	StartUp Failed	Thermal Shutdown
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0

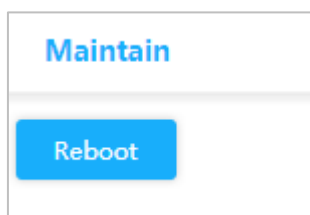
4 Maintenance

4.1 System Reboot

Step 1 Select **Maintain > Common > System Reboot**.

The **System Reboot** interface is displayed. See Figure 4-1.

Figure 4-1 System reboot



Step 2 Click **Reboot**. The confirm dialog box pops up.

Step 3 Click **Confirm**, and the device reboots.

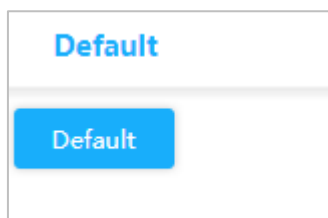
4.2 Restore Default

You can restore all the switch configuration to the factory defaults, except the VLAN IP address of the switch.

Step 1 Select **Maintain > Common > Restore Default**.

The **Restore Default** interface is displayed. See Figure 4-2.

Figure 4-2 Restore default



Step 2 Click **Default**.

All the configuration except VLAN IP address of the switch is restored to factory defaults.

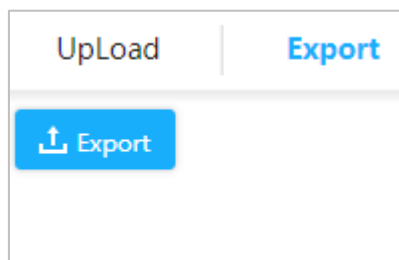
4.3 Config Manage

4.3.1 Export Config File

Step 1 Select **Maintain > Common > Config Manage > Export**.

The **Export** interface is displayed. See Figure 4-3.

Figure 4-3 Export

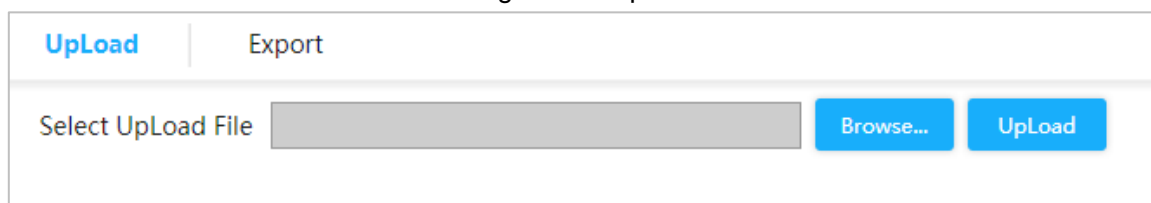


- Step 2 Click **Export**.
Export Config file.

4.3.2 Upload Config File.

- Step 1 Select **Maintain > Common > Config Manage > UpLoad**.
The **UpLoad** interface is displayed. See Figure 4-4 .

Figure 4-4 Upload



- Step 2 Click **Browse...**, and select the config file to upload.
Step 3 Click **UpLoad**.

4.4 Software Update

- Step 1 Select **Maintain > Common > Software Update**.
The **Update** interface is displayed. See Figure 4-5.

Figure 4-5 Upgrade



- Step 2 Click **Browse...**, and select the file in .mif format to upload.
Step 3 Click **UpLoad**.
The device reboots after the upgrade finished. Login the switch again, and all configuration will not be changed.

4.5 Mirror

Port mirroring is also called port monitoring. Port monitoring is the data package acquiring technology that through configuring switch, data package from one or several ports (mirroring source ports) can be copied to a specific port (mirroring destination port).The mirroring destination port connects to a PC that data package analyzing software is installed, and it can analyze the received data package for network monitoring and troubleshooting.

Step 1 Select **Maintain > Common > Mirror**.

The **Mirror** interface is displayed. See Figure 4-6.

Figure 4-6 Mirror

Mirror

Global Settings:

Mode

Port Configuration:

Port	Source	Destination
1	<input type="text" value="Disabled"/>	<input type="checkbox"/>
2	<input type="text" value="Disabled"/>	<input type="checkbox"/>
3	<input type="text" value="Disabled"/>	<input type="checkbox"/>
4	<input type="text" value="Disabled"/>	<input type="checkbox"/>
5	<input type="text" value="Disabled"/>	<input type="checkbox"/>
6	<input type="text" value="Disabled"/>	<input type="checkbox"/>
7	<input type="text" value="Disabled"/>	<input type="checkbox"/>
CPU	<input type="text" value="Disabled"/>	<input checked="" type="checkbox"/>

Step 2 In **Global Settings**, select **Enabled** in **Mode** to enable mirror.

Step 3 In **Port Configuration**, select **Source** or **Destination** according to the actual situation.

- Select the following four ways for source port.
 - ◇ Both: Enable the port as the source address of mirror.
 - ◇ Disable: Disable the port as the source address of mirror.
 - ◇ Rx only: The port only mirror receiving data, not mirror sending data.
 - ◇ Tx only: The port only mirror sending data, not mirror receiving data.
- Select the **Destination** box to set the port to be destination.

Step 4 Click **Save**.

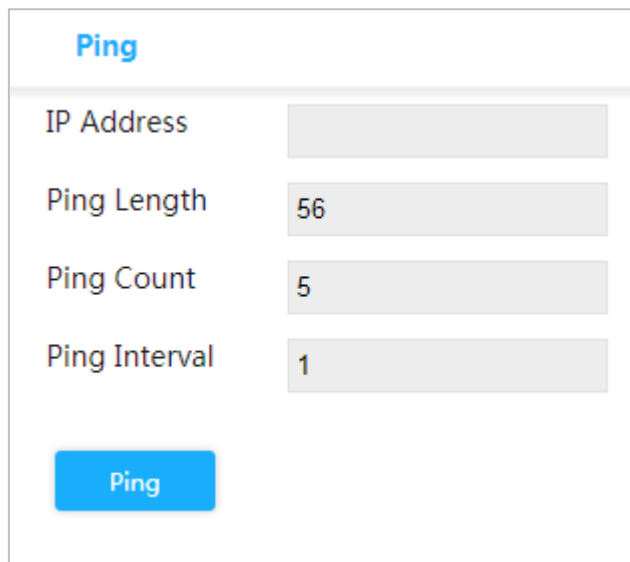
4.6 Ping

With Ping protocol, you can check whether the device with a specified IP address can be accessed, and check whether the network connection fails.

Step 1 Select **Maintain > Common > Ping**.

The **Ping** interface is displayed. See Figure 4-7.

Figure 4-7 Ping



Ping	
IP Address	<input type="text"/>
Ping Length	<input type="text" value="56"/>
Ping Count	<input type="text" value="5"/>
Ping Interval	<input type="text" value="1"/>
<input type="button" value="Ping"/>	

Step 2 Enter the IP address, and click **Ping**.

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No.1199, Bin'an Road, Binjiang District, Hangzhou, P.R. China

Postcode: 310053

Tel: +86-571-87688883

Fax: +86-571-87688815

Email: overseas@dahuatech.com

Website: www.dahuasecurity.com