Dahua Ethernet 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 be "the Manual") introduces operations on web interface of Ethernet Switch DH-PFS5428-24GT. The Ethernet Switch supports web access. You can visit the switch on web browser, and configure and manage the switch.

Models

DH-PFS5428-24GT

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	December, 2018

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 dissemble 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

1 Login the Switch

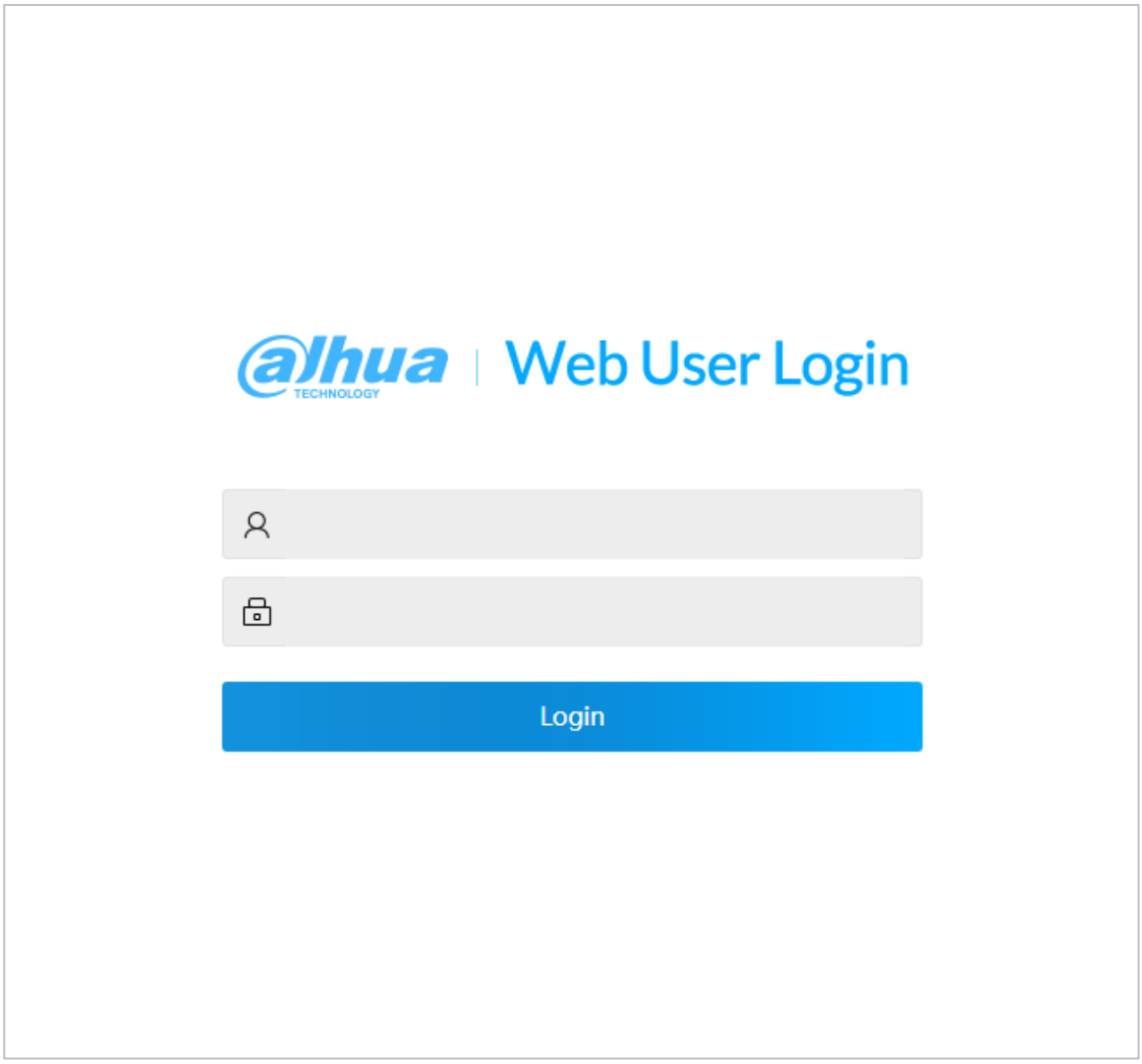
Before login, make sure:

- You have already configured 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 web login interface is displayed. See Figure 1-1.

Figure 1-1 Web login



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

Step 3 Click **Login**.

The **Quick Setting** interface is displayed.

After the first login, modify the password. 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 "&"). Modify the password in time.

2 Quick Setting

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

2.1 System Information

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

After logging in the system, the **System Info** is displayed. See Figure 2-1. If the port shows green, it means the port is connected successfully. If the port shows gray, it means the port is not connected. See Table 2-1.

Figure 2-1 Device information

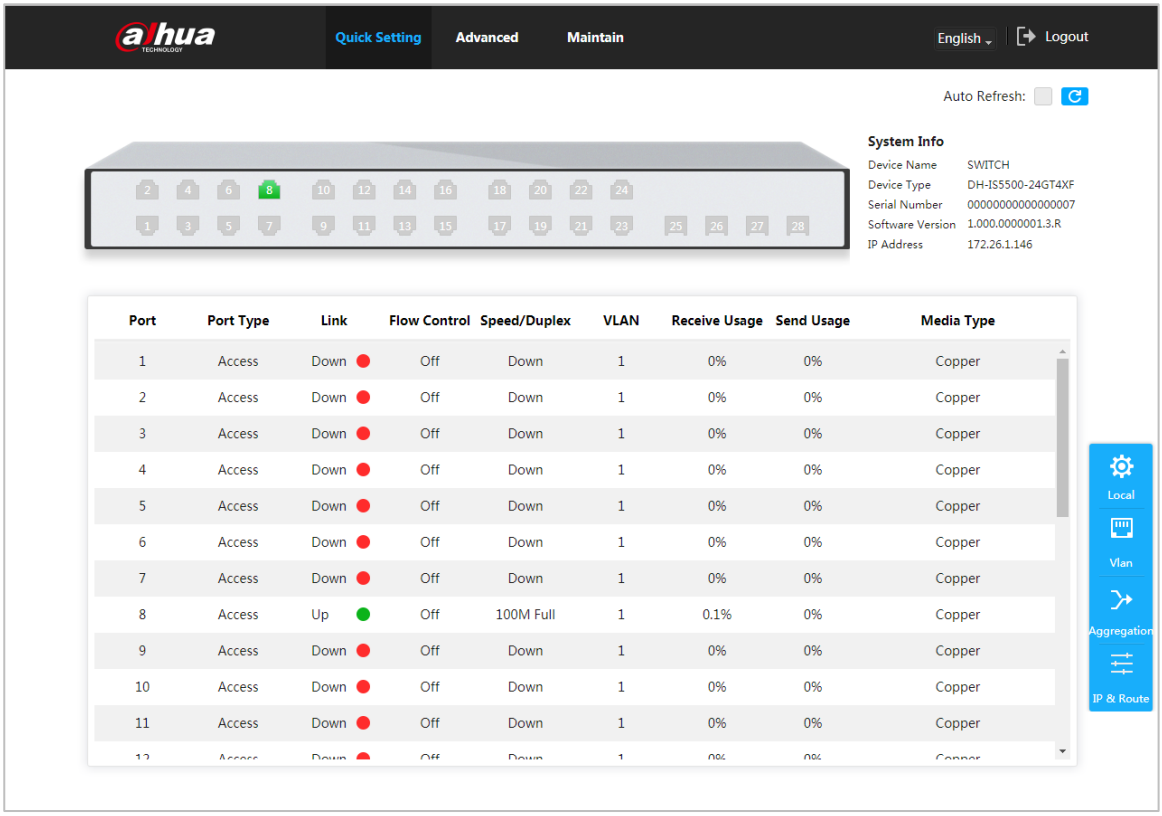


Table 2-1 Port information

Parameters	Description
Port	Show all ports of the switch. This switch has 28 ports. Port quantity might vary depending on the model you purchased, and the actual product shall prevail.
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.
Flow Control	show the flow control state.

Parameters	Description
Speed/Duplex	● Online: It shows the port rate and the duplex mode ● Offline : It shows **Down**.
VLAN	The port VLAN. It is VLAN 1 by default.
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 the RJ-45 port, and **Fiber** indicates the fiber port.

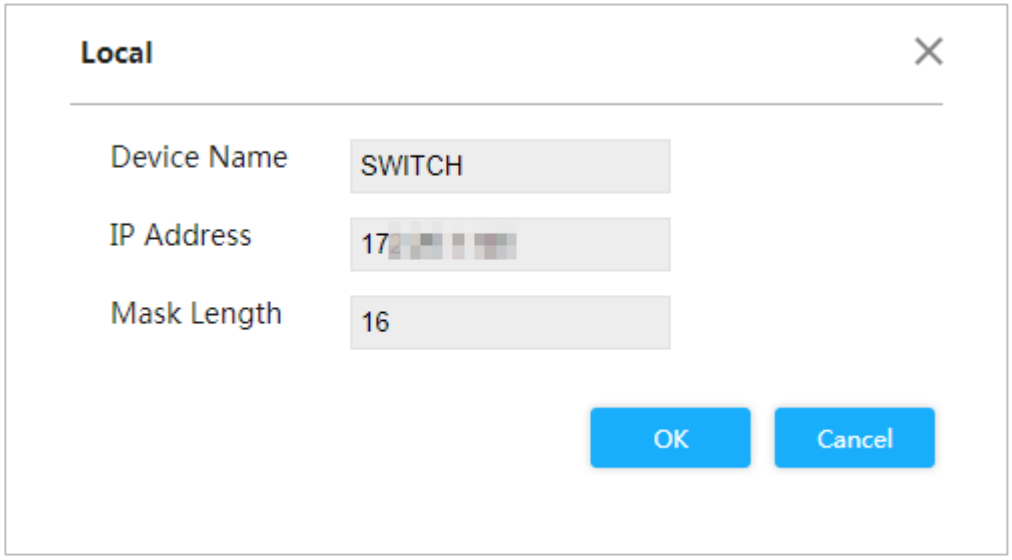
2.2 Local

You can set the device 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 device name, IP address, and mask length.

Step 3 Click **OK**.

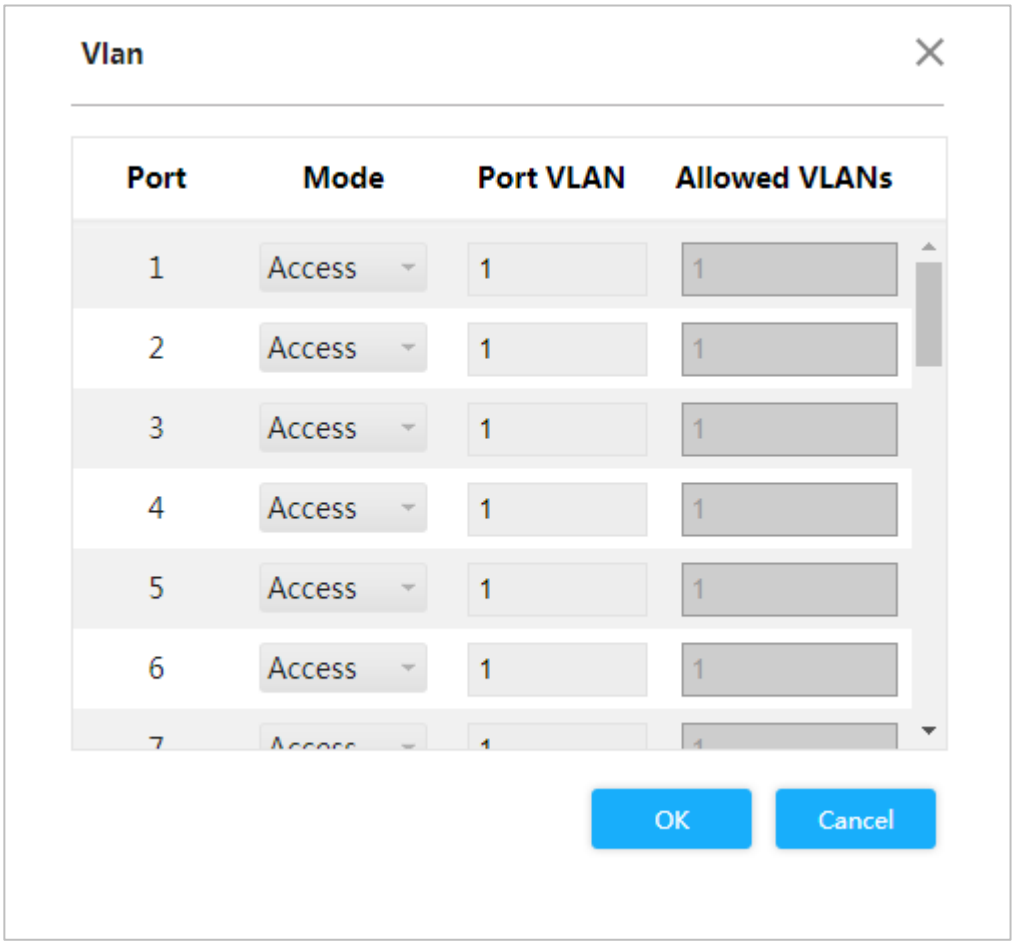
2.3 Vlan

Add the port to 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 dispalyed. See Figure 2-3.

Figure 2-3 Vlan



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

Table 2-2 VLAN parameters

Parameters	Description
Port	Show all ports of the switch.
Mode	Three modes: **Access**, **Hybrid**, and **Trunk**. ● **Access**: When the port connects to terminal devices (such as PC and IPC), select **Access**. ● **Hybrid**: Not often used. ● **Trunk**: When the port connects to switch, select **Trunk**.
Port VLAN	Add the port to a VLAN, and configure the Vlan. By default, the port belongs to Vlan1. The range is 1~4094.
Allowed VLANs	Set the allowed VLAN. When the mode is **Trunk**, you can set it.

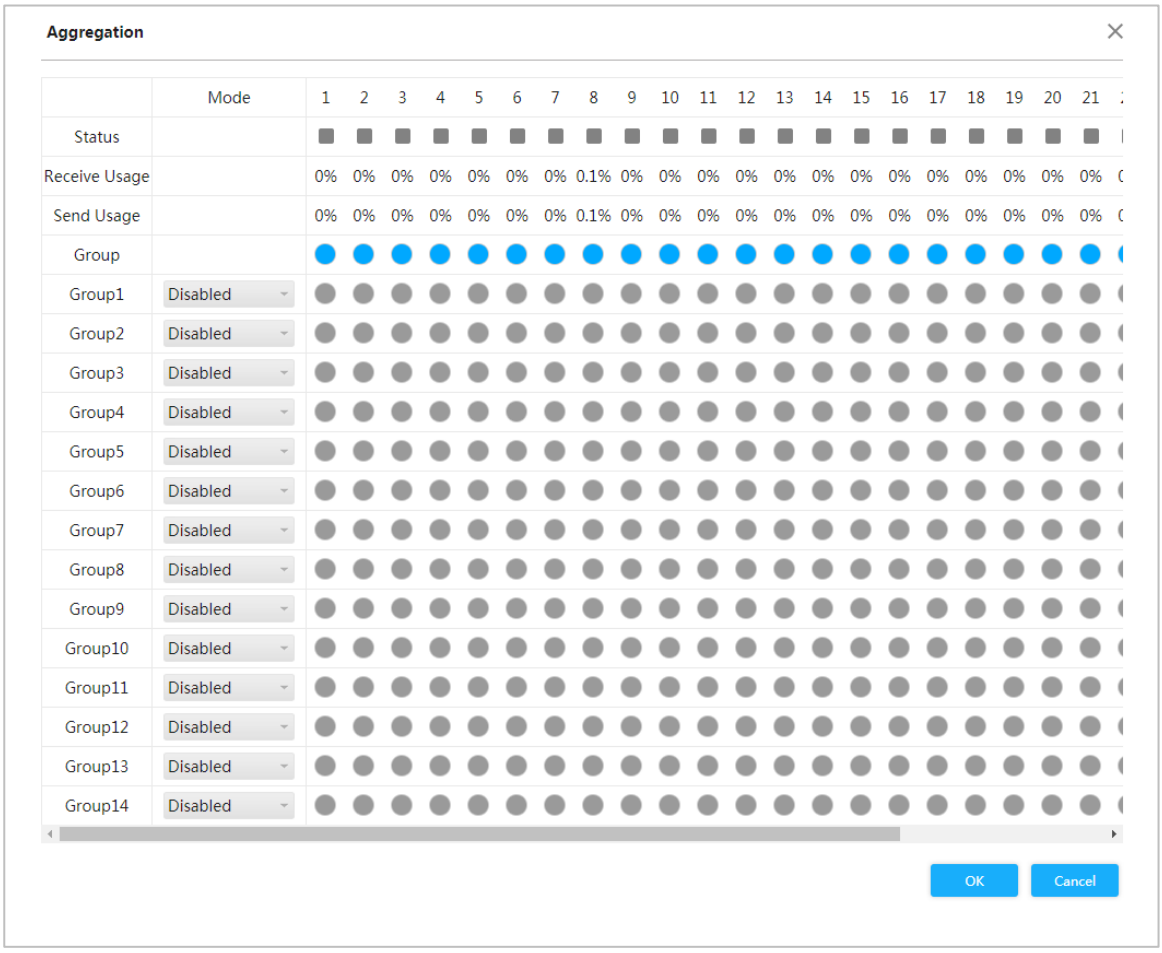
Step 3 Click **OK.**

2.4 Aggregation

Add the port to a certain aggregation. There are two types of aggregations: static aggregation and dynamic aggregation. See “3.1.4 Aggregation.”

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

Figure 2-4 Aggregation



2.4.1 Configuring Static Aggregation

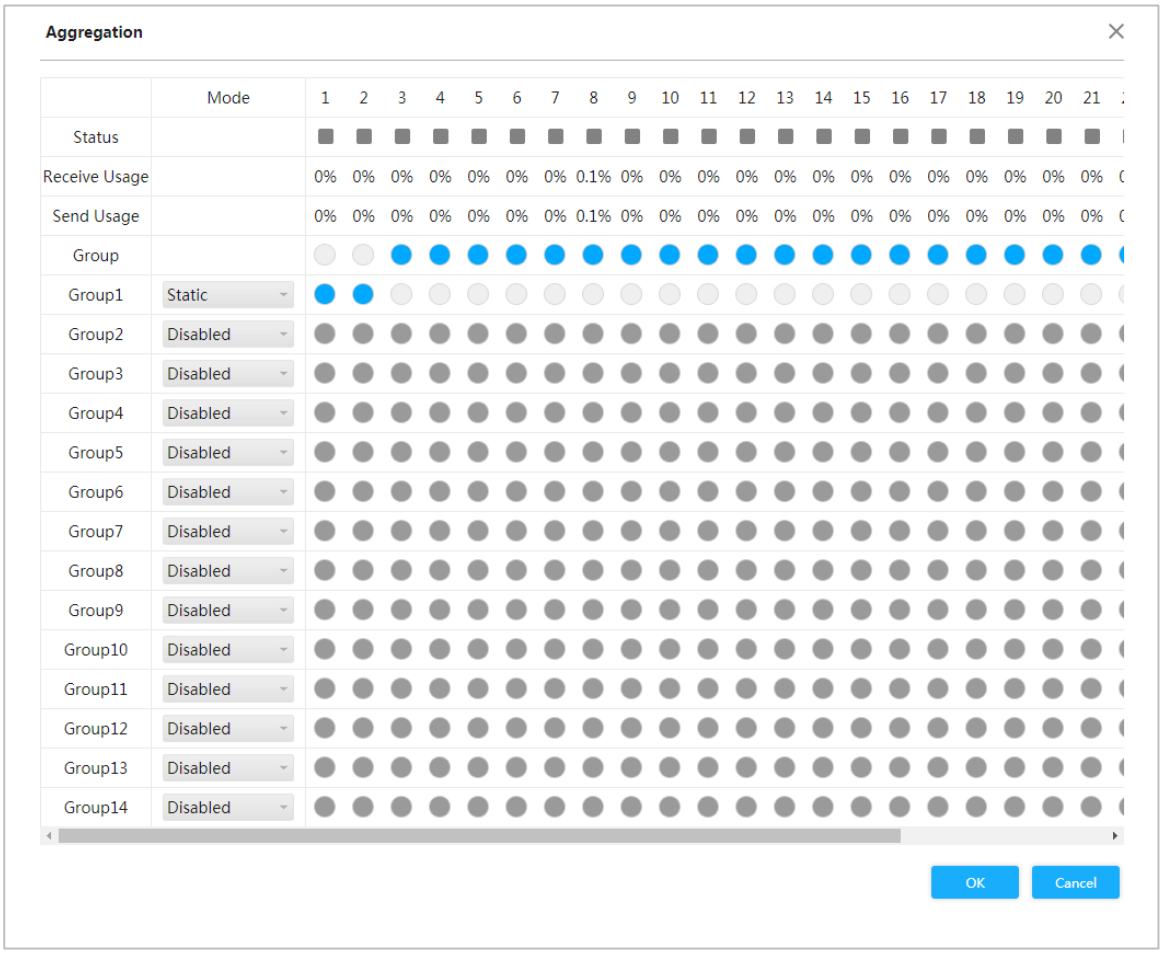
Example: Add port 1 and port 2 to static aggregation group1.

Step 1 Select **Mode** as **Static**.

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

You can set up to 14 groups of static aggregation.

Figure 2-5 Static aggregation



Step 3 Click **OK**.

Port 1 and port 2 come into being a logical port.

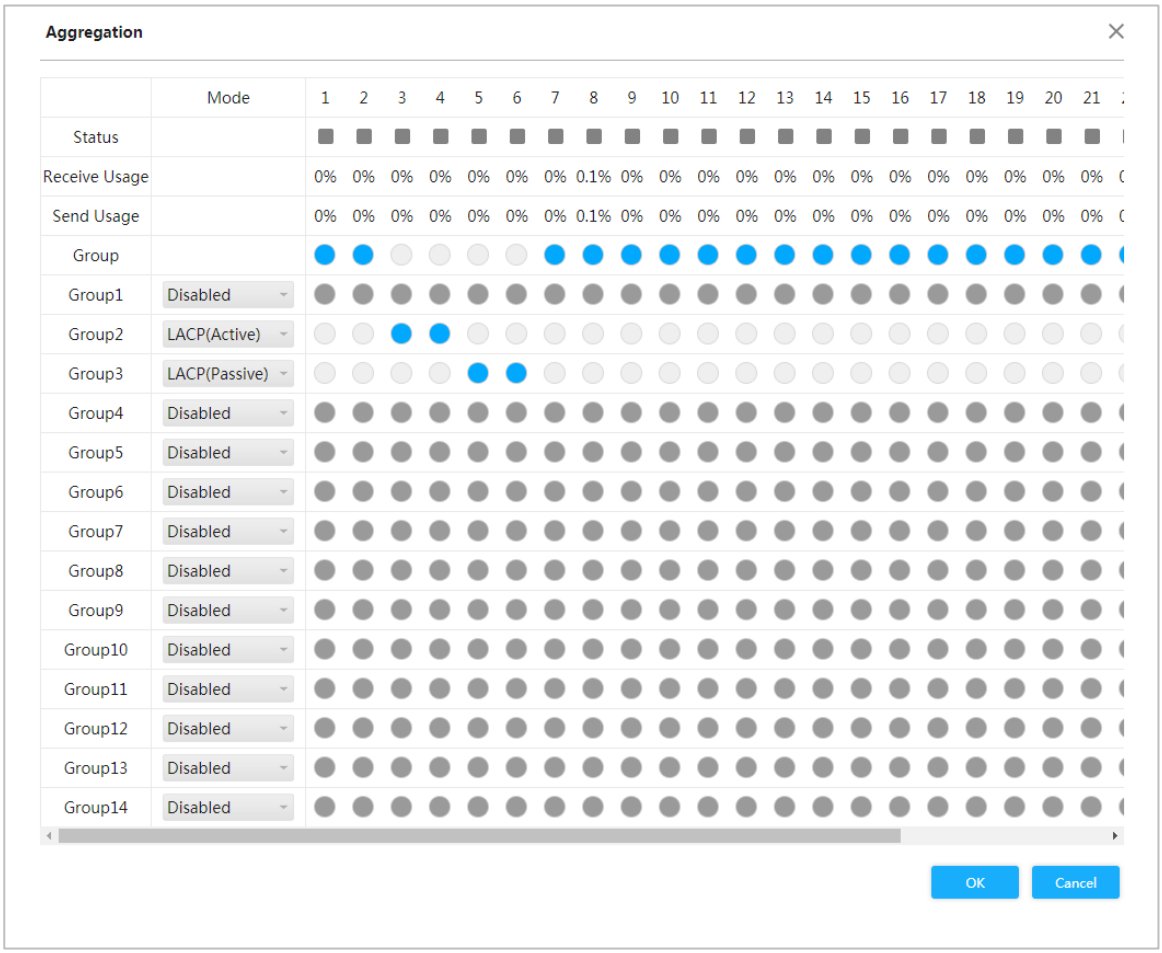
2.4.2 Configuring Dynamic Aggregation

Examples: Add port 2 and port 3 to dynamic aggregation group 2, and add port 5 and port 6 to dynamic aggregation group 3.

Step 1 Add the port member to the dynamic aggregation group.

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

Figure 2-6 Dynamic aggregation



Step 2 Click **OK**.

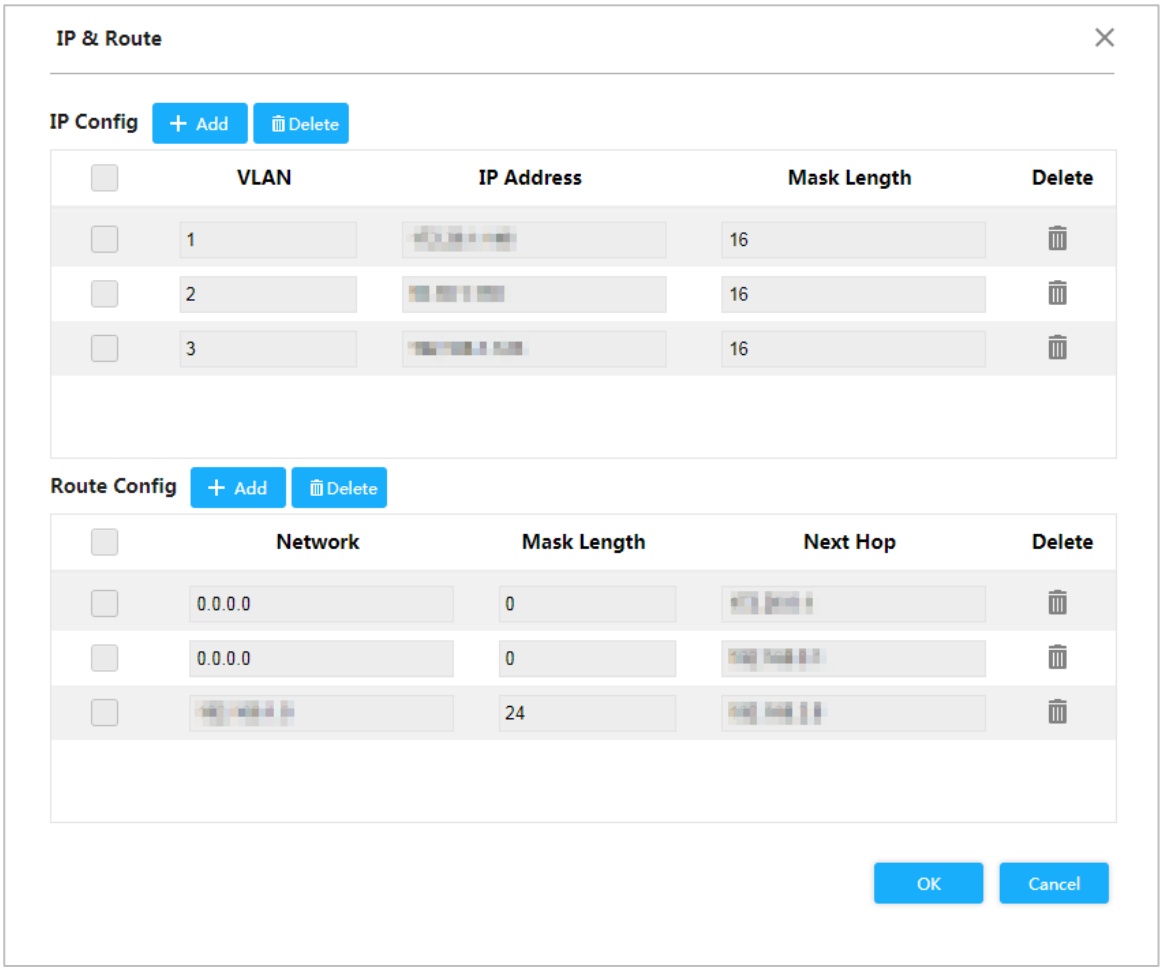
2.5 IP and Route

You can add the IP of Vlan interface and the IP route. For details, see “3.1.1.2 IP and Route.”

Step 1 Click **IP & Route** on the **Quick Setting** interface.

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

Figure 2-7 IP and Route

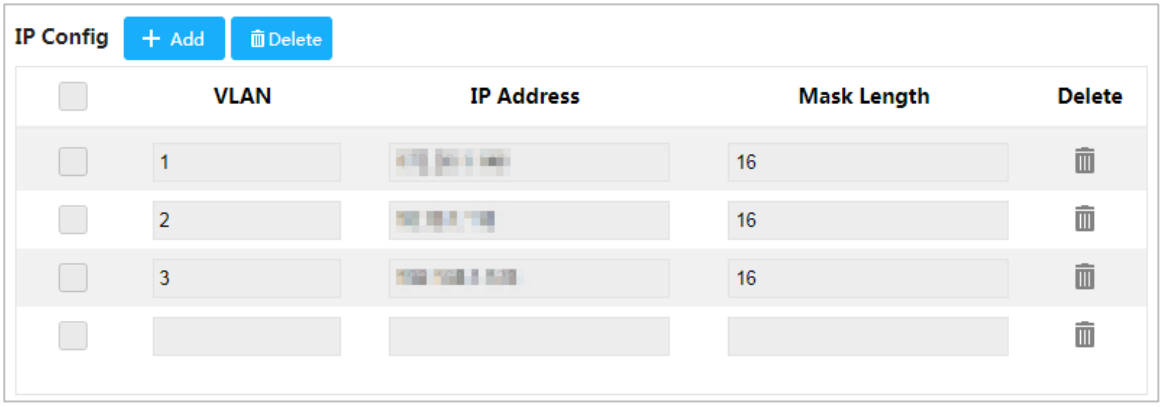


Step 2 Add Vlan interface

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

An added blank record is displayed. See Figure 2-8.

Figure 2-8 Vlan interface



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

Table 2-3 Vlan interface

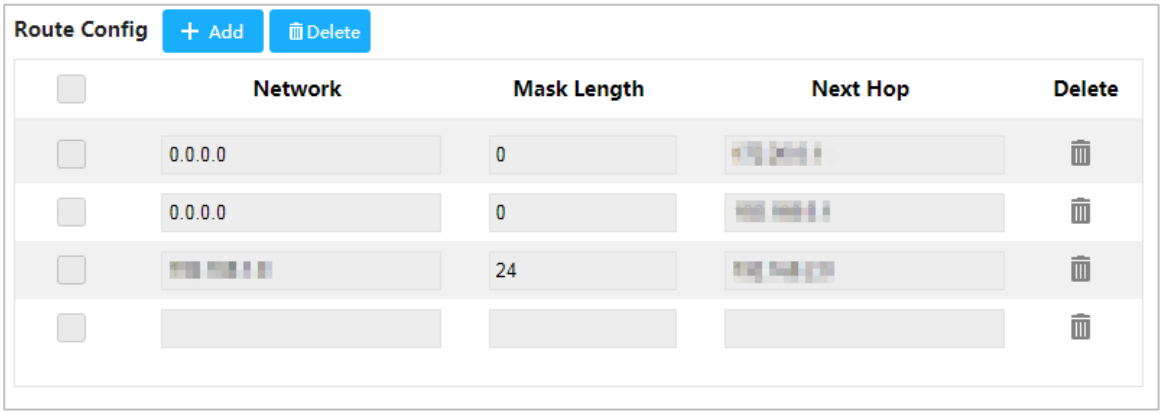
Parameters	Description
VLAN	Enter VLAN number.
IP Address	Set the IP address of the Vlan interface.
Mask Length	Set the mask length of the Vlan interface.

Step 3 Add IP route

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

A blank record is displayed. See Figure 2-9.

Figure 2-9 IP route



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

Table 2-4 IP route

Parameters	Description
Network	It is the destination of the IP packet.
Mask Length	Mask length, with destination , is to identify the IP address of the destination host or the route. After “logical AND” between destination 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 Configuration

3.1 Common Configuration

3.1.1 System Configuration

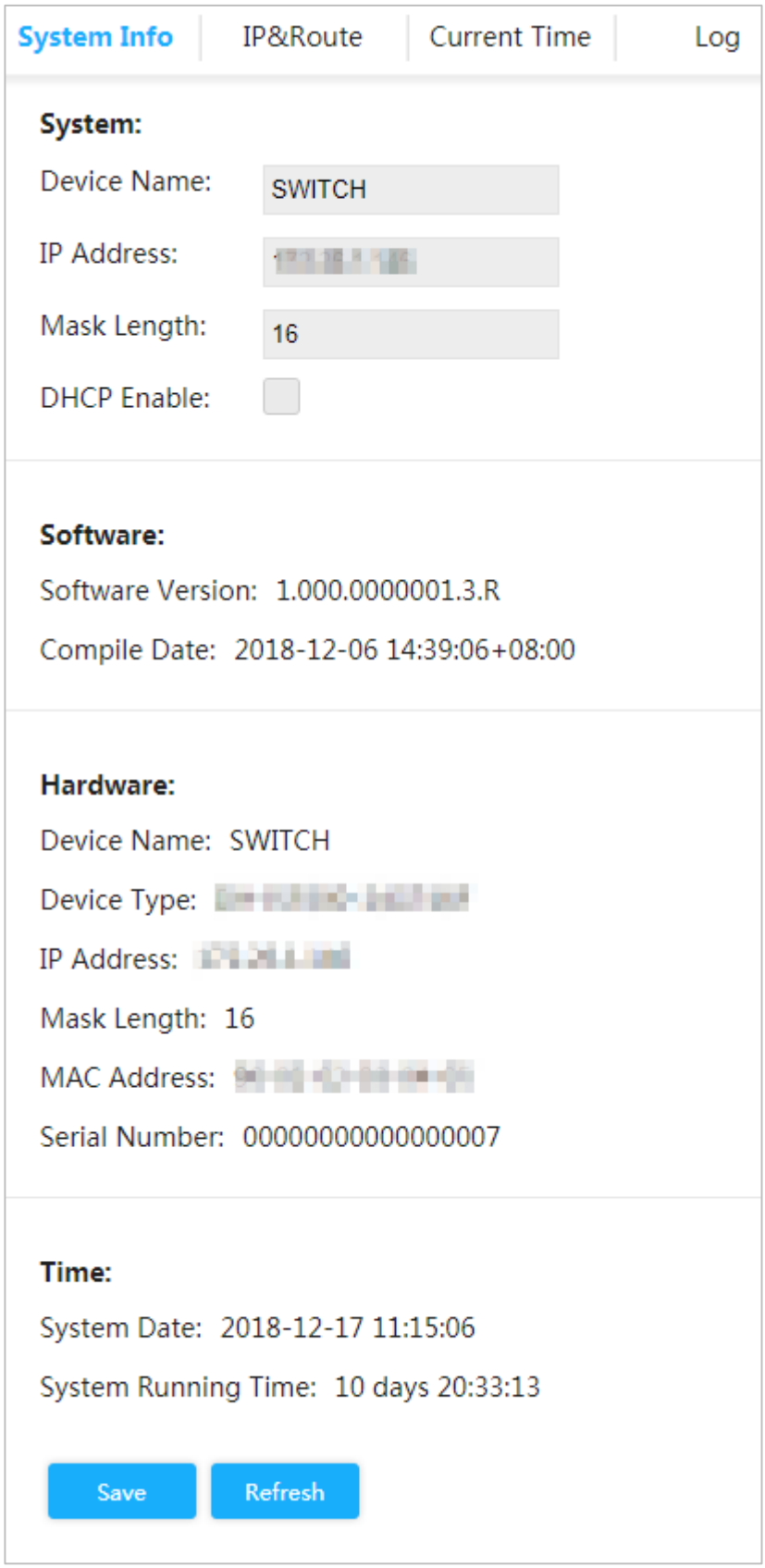
3.1.1.1 System Information

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

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

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

Figure 3-1 System information



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

Step 3 Click **Save**.

3.1.1.2 IP and Route

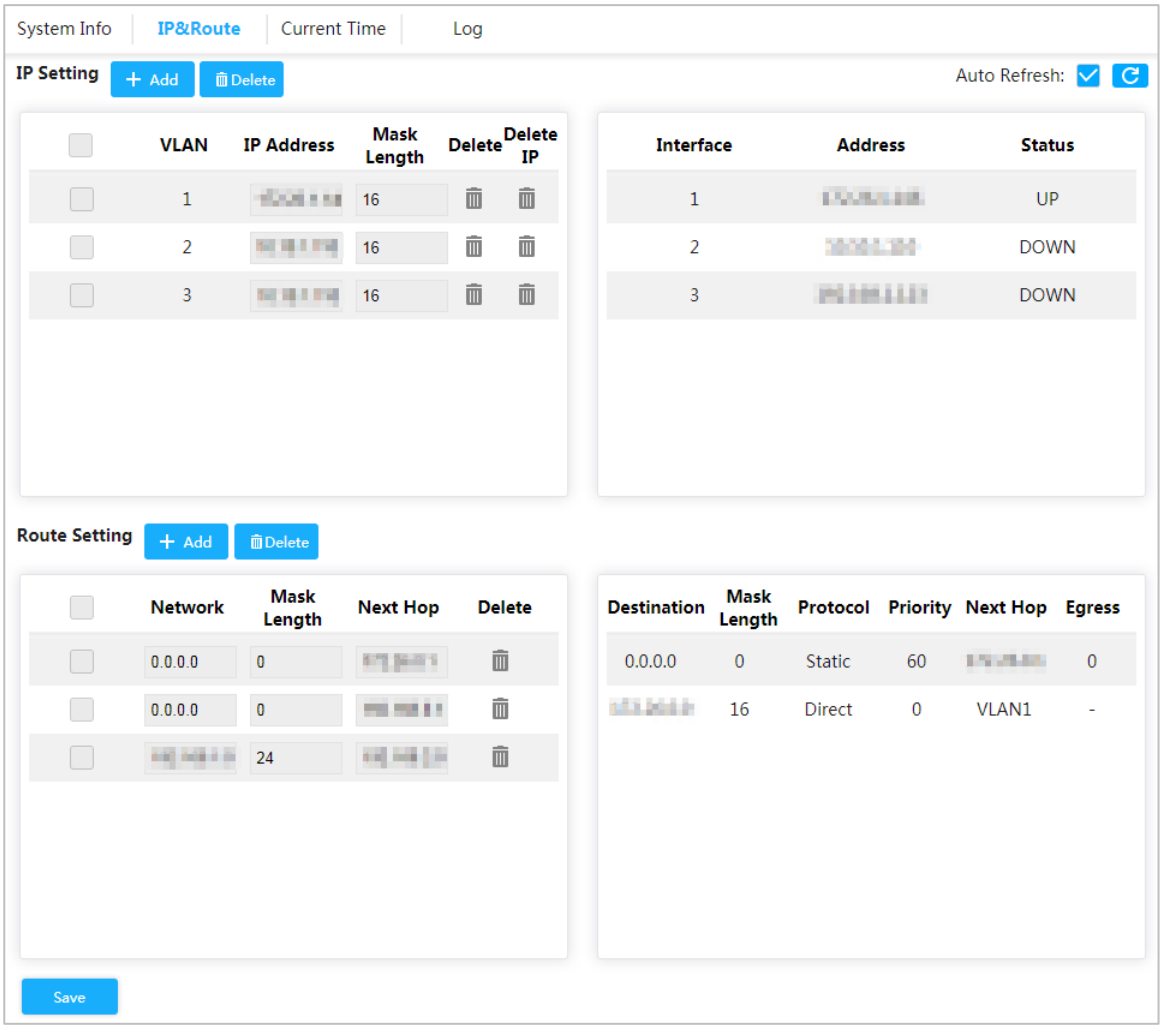
The hosts belong to different VLANs cannot communicate directly. Network devices (route or the layer 3 switch) are needed for the switching. The switch supports layer 3 switching of packet through VLAN interface.

VLAN interface is a virtual port of layer 3 mode, which is for layer 3 communication among the VLANs. It is not a physical entity on the device. Every VLAN corresponds to a VLAN interface, and the VLAN interface can switch the packet which received by the VLAN. Generally, because the VLAN can isolate the broadcasting domain, every VLAN corresponds to a network segment. As the gateway of the network segment, VLAN interface supports layer 3 switching for the packet 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

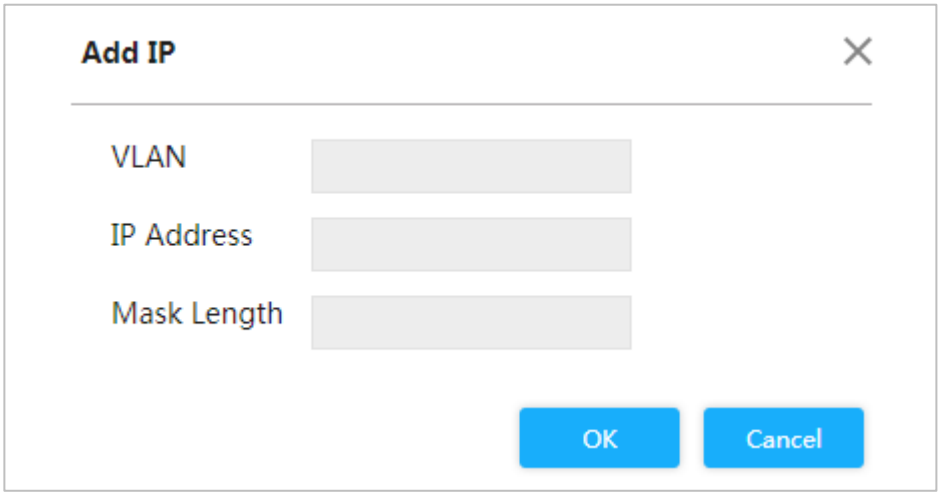


Step 2 Add Vlan interface

1) Click **Add**.

And the **Add IP** dialog bx is prompted. See Figure 3-3.

Figure 3-3 Add IP



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

Table 3-1 Vlan interface

Parameters	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.

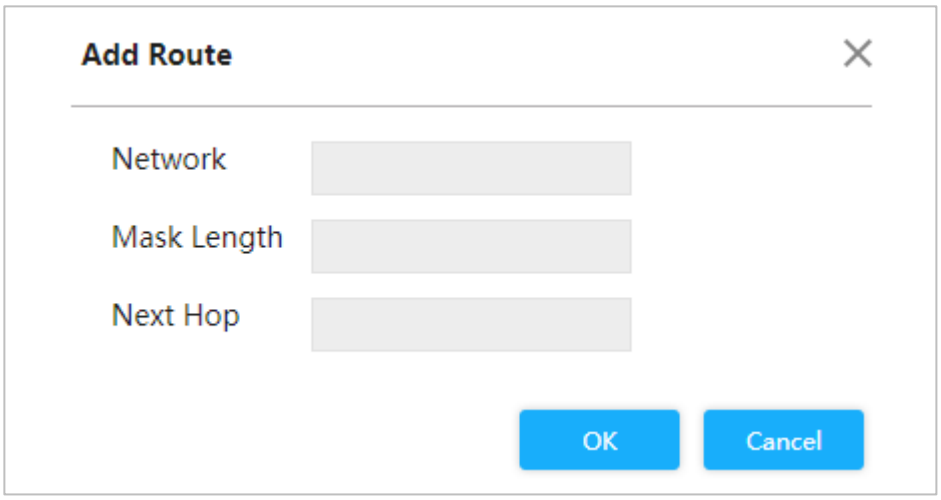
3) Click **OK**.

Step 3 Add IP route

1) Click **Add**.

And the **Add Route** dialog box is prompted. See Figure 3-4.

Figure 3-4 Add route



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

Table 3-2 IP route

Parameters	Description
Network	It is the destination of the IP packet.
Mask Length	Mask length, with destination , is to identify the IP address of the destination host or the route. After “logical AND” between destination 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**.

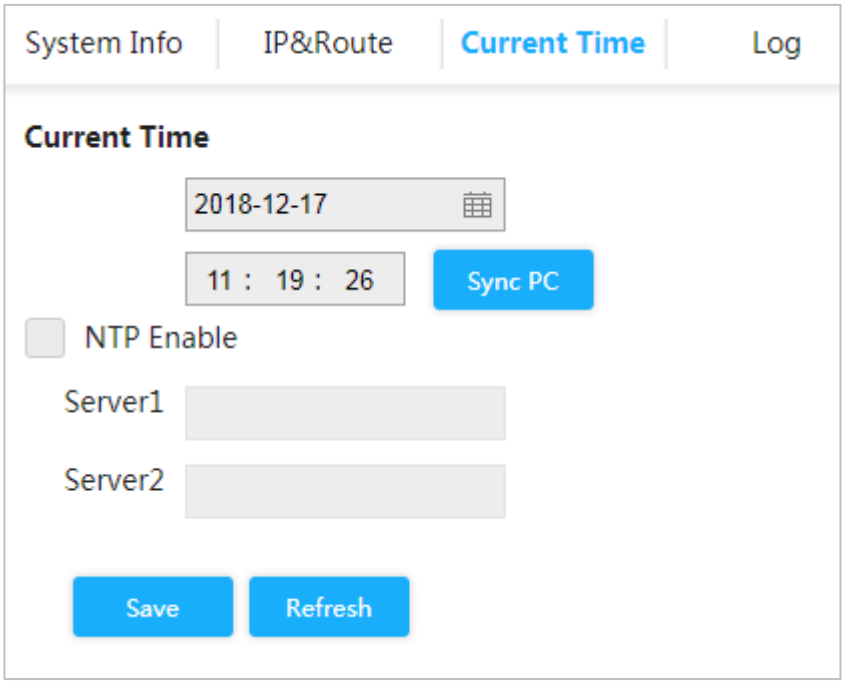
3.1.1.3 Time

You can set the time by the following three methods:

- Set the time manually.
- Sync PC time
- Sync NTP server time

Select **Advanced > Common > System Config > Current Time**. The **Current Time** interface is displayed. See Figure 3-5.

Figure 3-5 System Time (1)

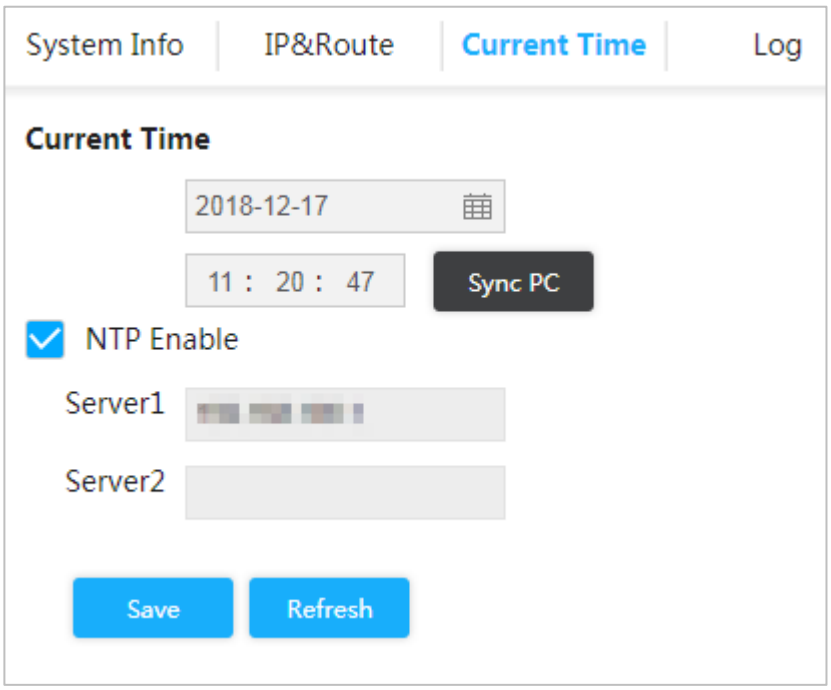


- Set the time manually
  Set the date and time on **Current Time** interface, and then click **Save**.
- Sync PC time
  Click **Sync PC**, and the switch time synchronizes with the local time automatically.
- Sync NTP server time
  Only with NTP server configured in the network can you enable this function.

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

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

Figure 3-6 System Time (2)



Step 3 Click **Save.**

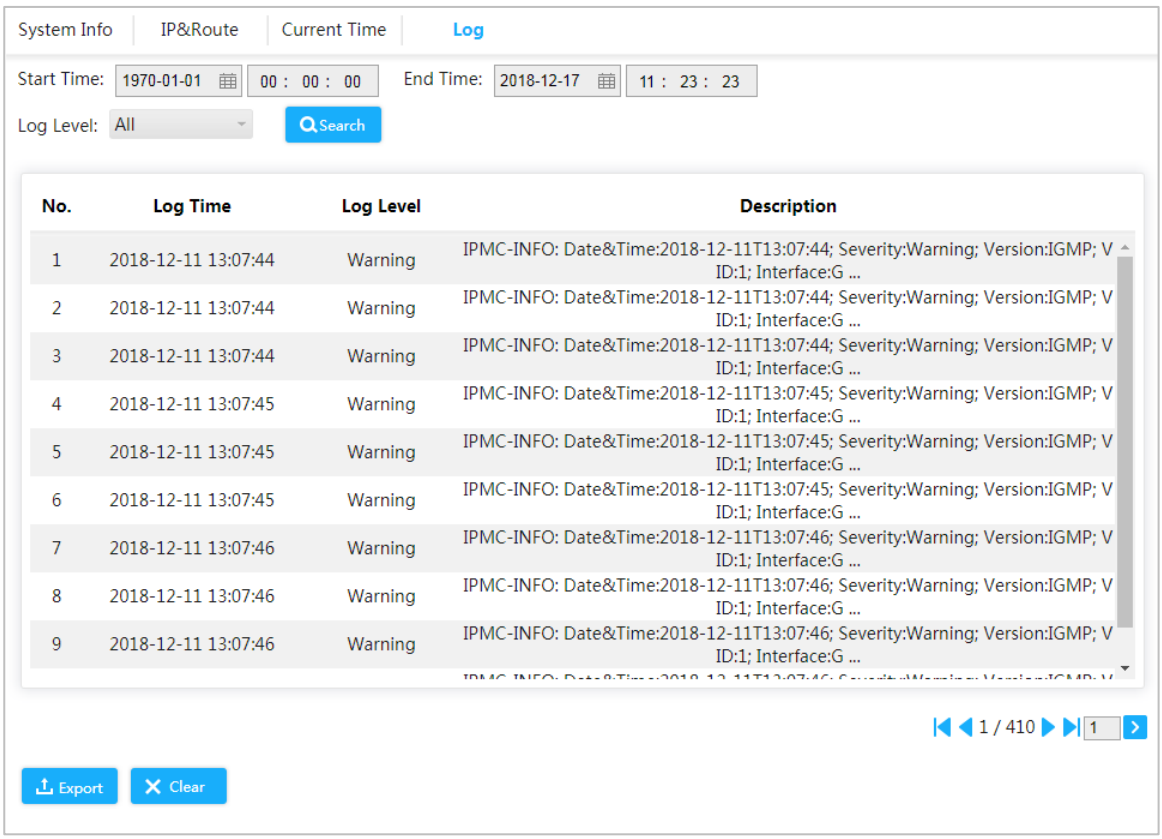
The switch time synchronizes with the server 1 automatically.

3.1.1.4 Logs

You can view logs, export logs and clear logs.

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

Figure 3-7 Log



- View the 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.

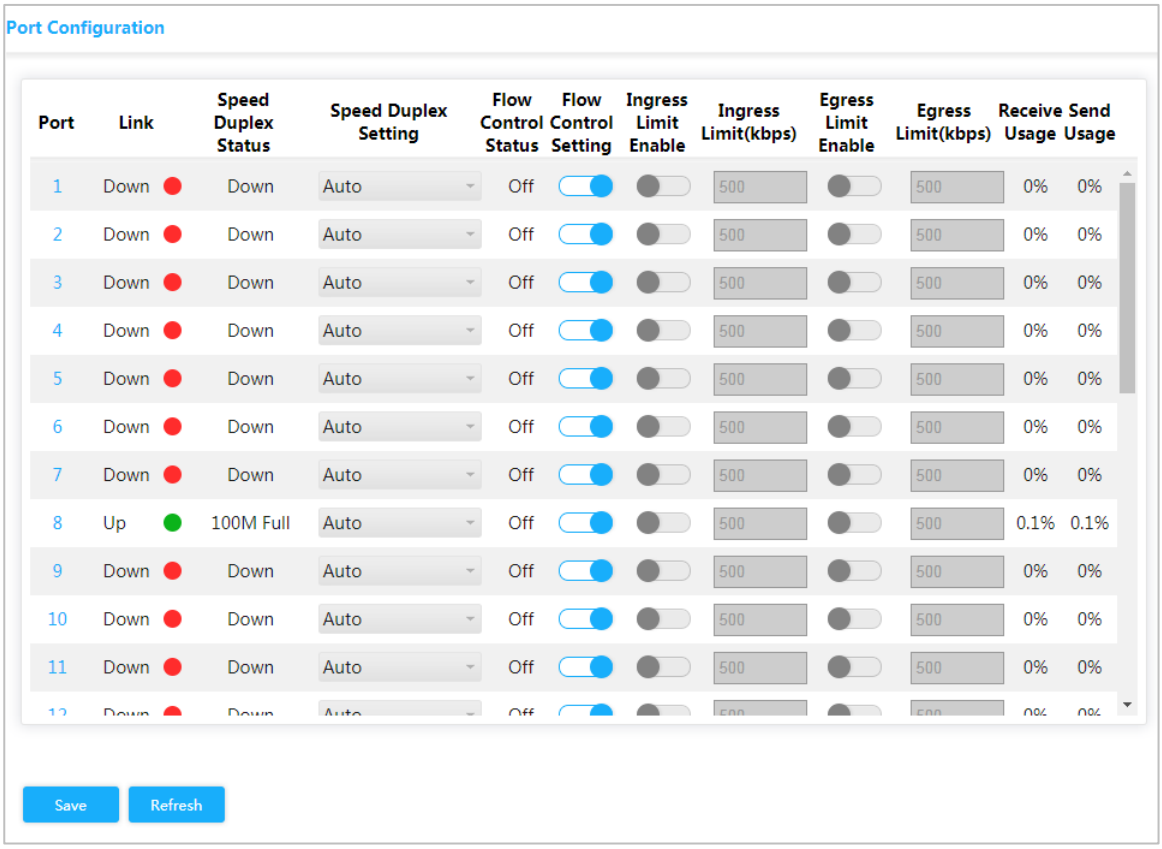
3.1.2 Port

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

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

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

Figure 3-8 Port Configuration



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

Table 3-3 Port

Parameters	Description
Port	Show all ports of the switch.
Link	Green **Up** means the connection is successful; Red **Down** means the connection is failed.
Speed duplex	**Down** means disconnection, and the specific speed means successful connection. **Full** means full duplex; **Half** means half duplex.
Speed duplex	Set the speed and duplex.
Flow control State	Show flow control actual negotiator or enable state, including ON and OFF. ON: Negotiation succeeds. OFF: Negotiation fails.
Flow cotrol configuration	ON/OFF flow control function. : Flow control is ON. : Flow control is OFF.
Ingress Limit Enable	Enable/Disable ingress limit : Ingress enable is enabled. : Ingress enable is disabled.
Ingress limit (kbps)	Set the ingress limit.

Parameters	Description
Egress Limit Enable	Enable/Disable egress limit : Egress enable is enabled. : Egress enable is disabled.
Egress limit (kbps)	I is to set the egress limit.
Receive Usage	Show the acceptance Usage.
Send Usage	Show the send usage.

Step 3 Click **Save.**

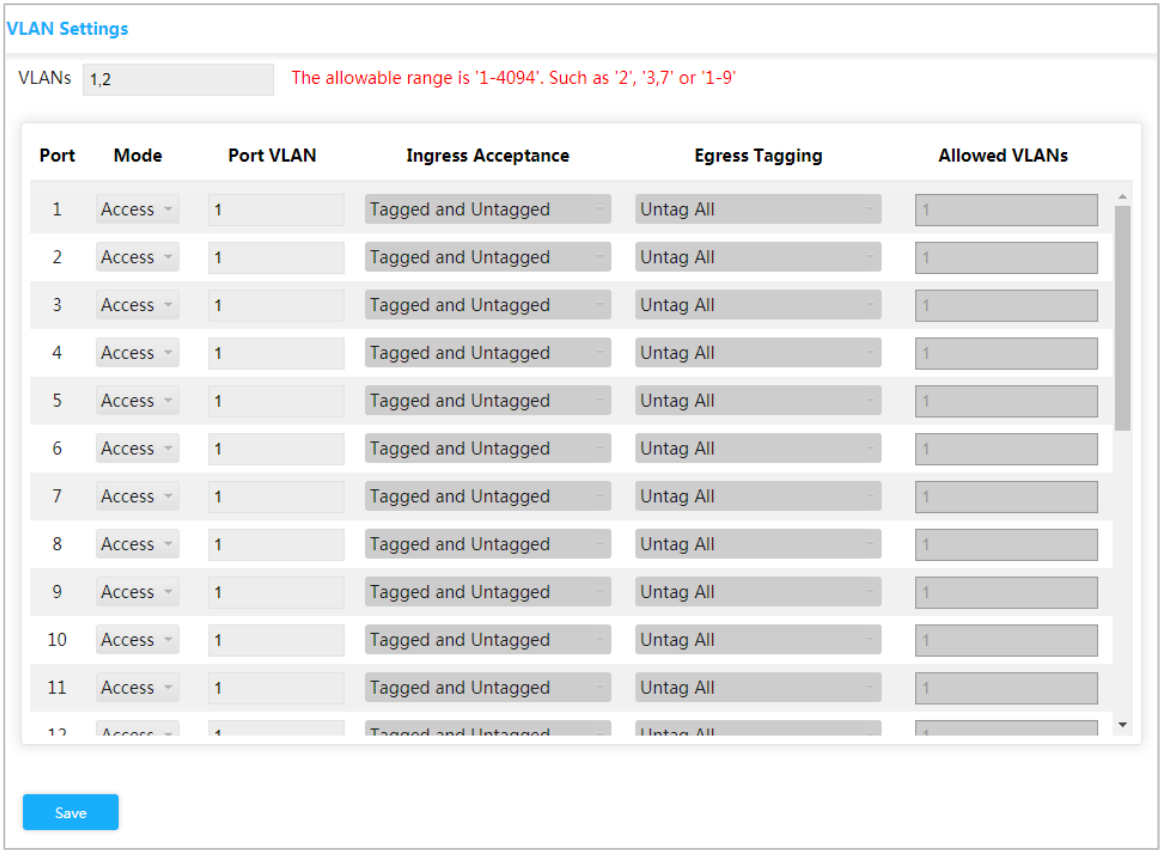
3.1.3 VLAN

Add the port to 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



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

Step 3 For the VLAN parameters, see Table 3-4.

Table 3-4 VLAN parameters

Parameters	Description
Port	Show all ports of the switch.
Mode	Three modes: **Access**, **Hybrid**, and **Trunk**.
Port VLAN	Add the port to a certain VLAN, and configure the Vlan. By default, the port belongs to Vlan1. The range is 1~4094.

Parameters	Description
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: ● **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: ● **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.

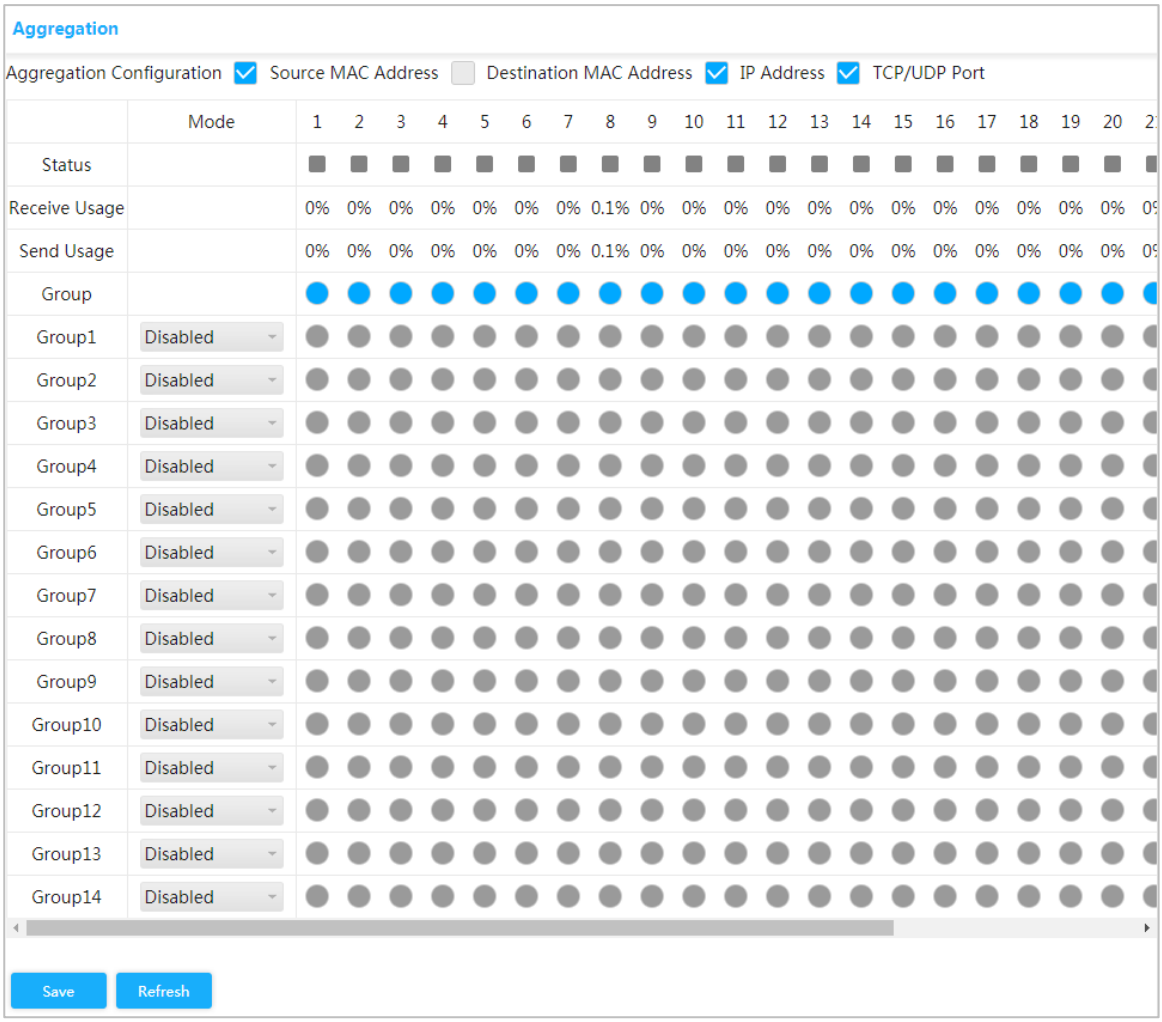
The multiple links in the same group can be regarded as a logical link with the larger bandwidth. Through aggregation, the ports in the same group can share the communication flow, to make a larger bandwidth. Besides, the ports in the same group can back up reciprocally and dynamically, to enhance the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

3.1.4.1 Static Aggregation

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

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

Figure 3-10 Aggregation



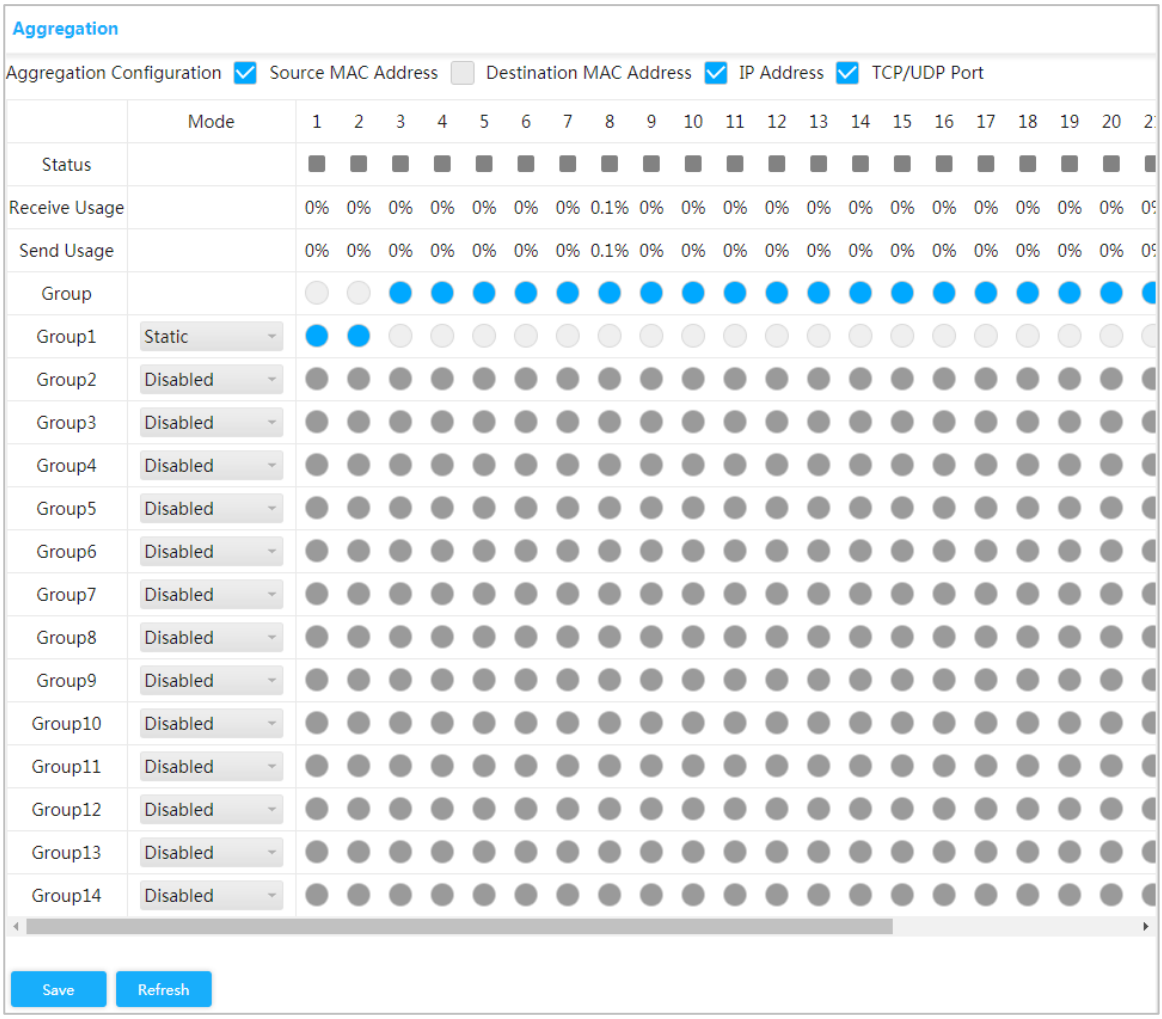
Step 2 Select the hash code contributors in **Aggregation Configuration**.There are four types:

- 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 member to the aggregation group. For example, add port 1 and port 2 to aggregation group 1. See Figure 3-11.

At most, 14 static aggregation groups can be set at the same time.

Figure 3-11 Static aggregation



Step 4 Click **Save.**

Port 1 and port 2 come into being 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).

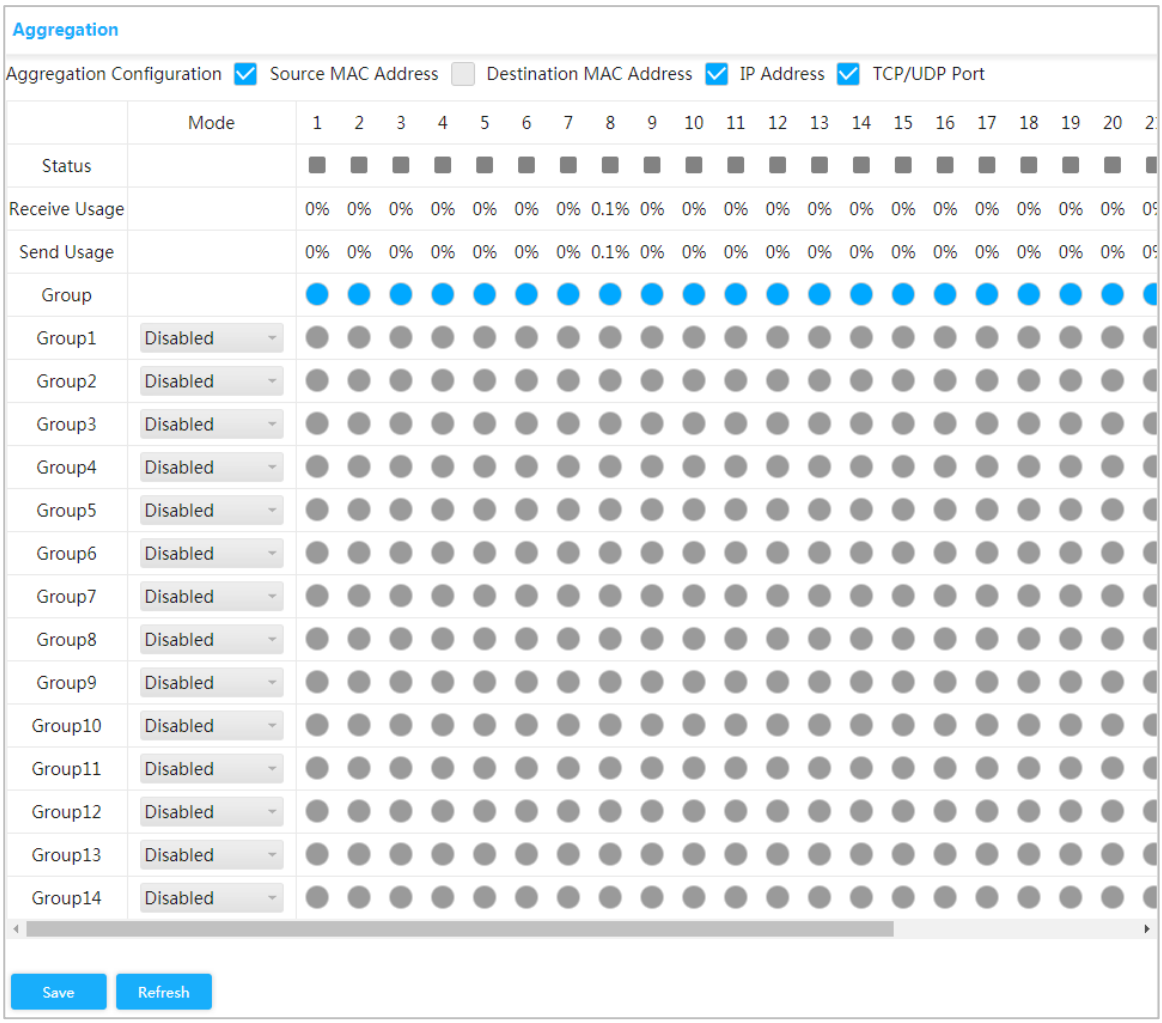
Select the role from the drop-down list.There are two types:

- **Active**: The port sends LACPDU packet actively to the opposite port, and analyzes the LACP.
- **Passive**:The port doesn't 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** is displayed.See Figure 3-12.

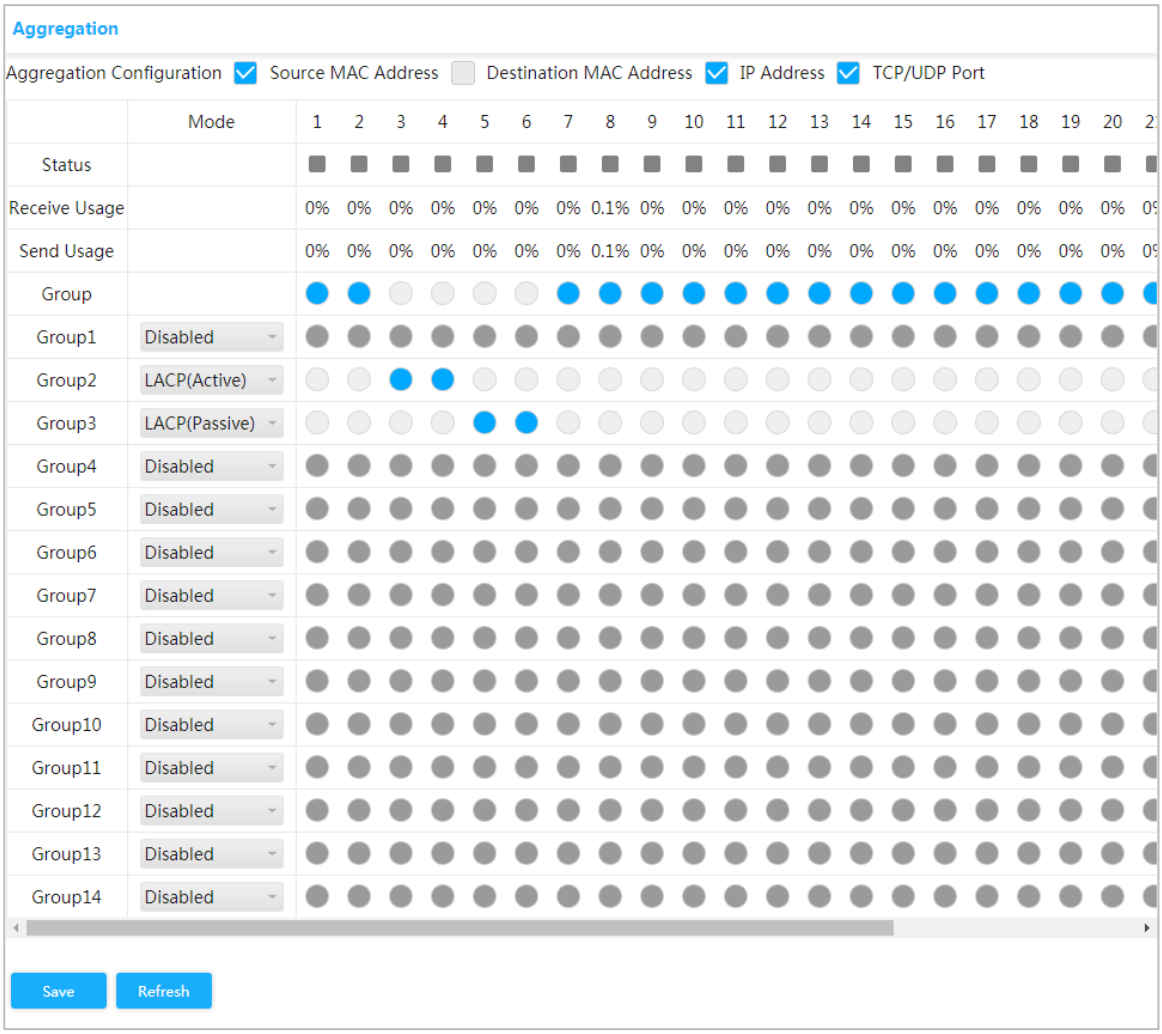
Figure 3-12 LACP (1)



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

Figure 3-13 LACP (2)



Step 4 Click **Save.**

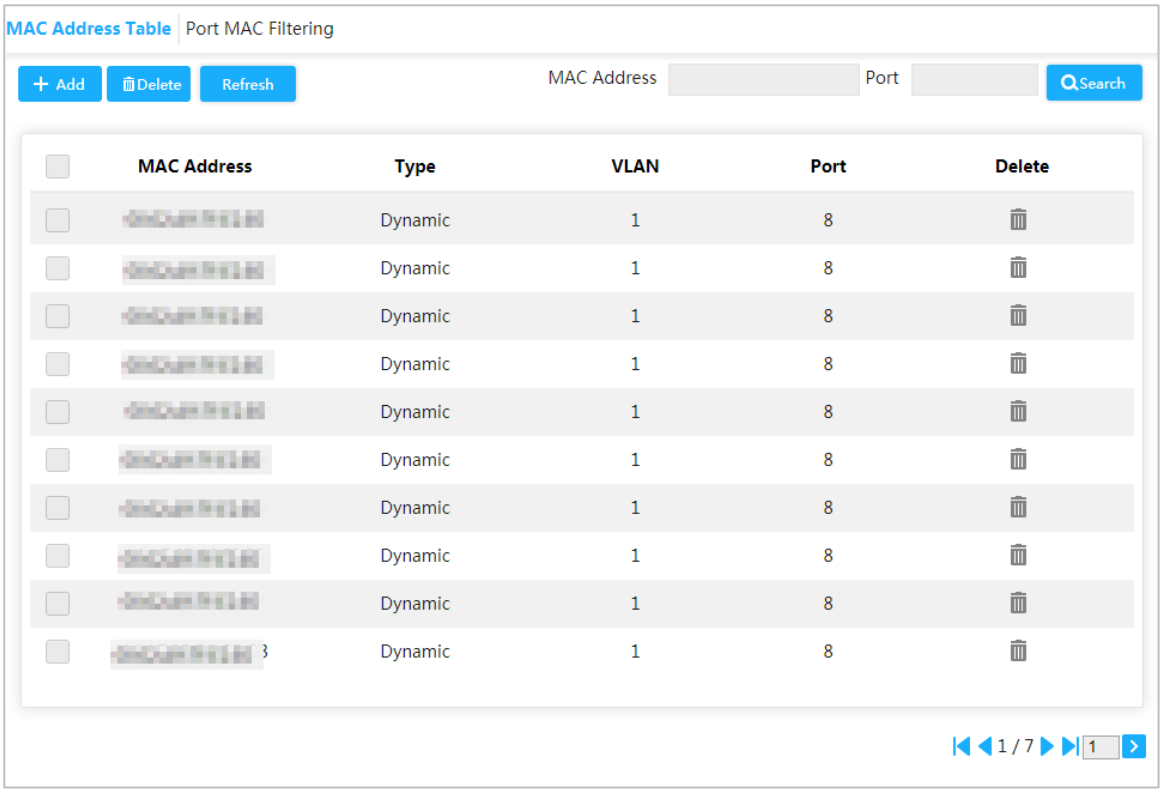
3.1.5 MAC Table

MAC (Media Access Control) table records the relationship between the MAC address and the port, and the information of the VLAN that the port belongs to. When the device is forwarding the packet, it queries 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.

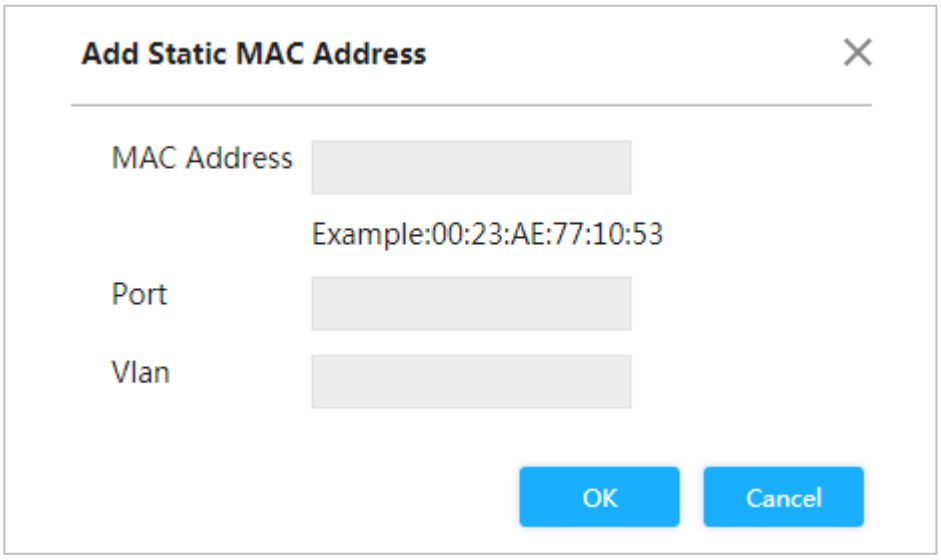
Figure 3-14 MAC address table



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 port 8 in VLAN 2.

1) Click **Add**.
   The **Add Static MAC Address** dialog box is prompted.
2) Set the MAC address, port and Vlan. See Figure 3-15.

Figure 3-15 Add static MAC address



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.

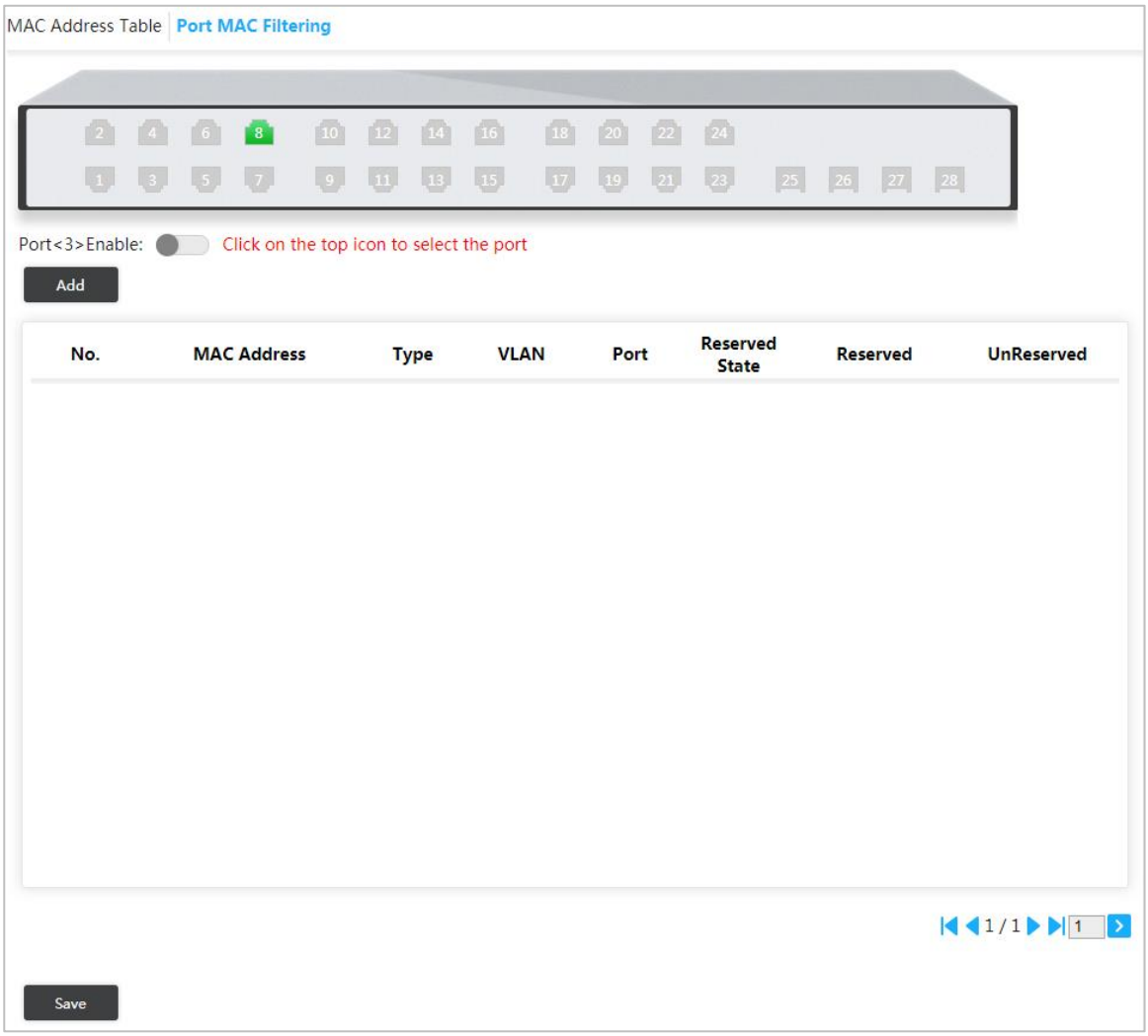
- Devices in MAC whitelist

- 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.

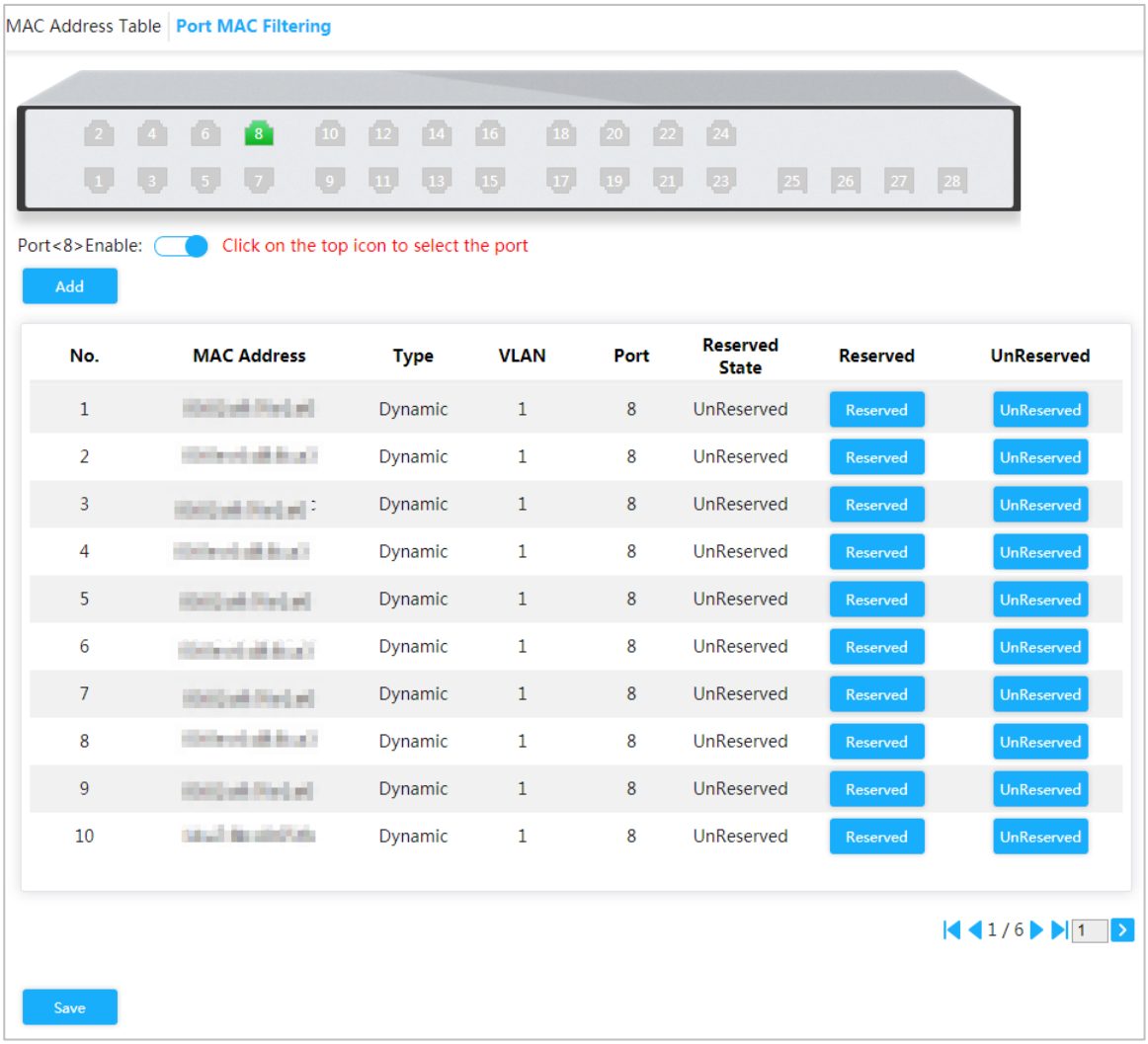
Figure 3-16 Port MAC filtering



Step 2 Select the port, For example: Port 8.

Step 3 Click  behind **Port <8> Enable** to enable the port. See Figure 3-17.

Figure 3-17 Enable port MAC filtering



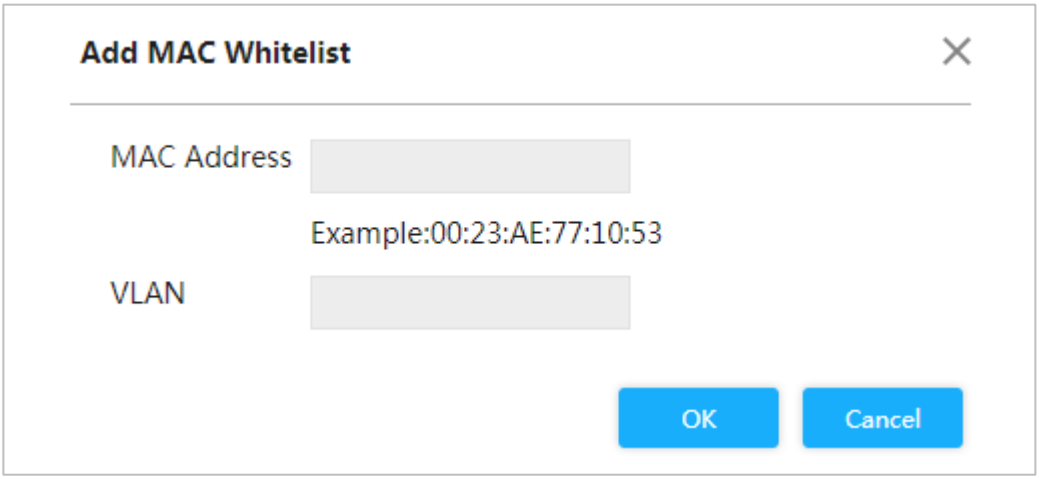
- Change Dynamic MAC device to Static.

1) 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** dialog box is prompted. See Figure 3-18.

Figure 3-18 Add MAC whitelist.



2) Set MAC address and VLAN.
3) Click **OK**.
   The devices in MAC whitelist can communicate with port normally.

3.1.6 ARP Table

ARP (Address Resolution Protocol) is the protocol to parse the IP address into Ethernet MAC address (the physical address).

In LAN, when the host or other network device needs to forward data to another host or other network device, the IP address of the target host or other network device should be known. Besides IP address, the forwarding station needs to know the physical address of the accepting station, because the IP data packet should be sent through the physical network as packaged frame. A mapping from the IP address to the physical address is needed. ARP is the protocol to realize the function.

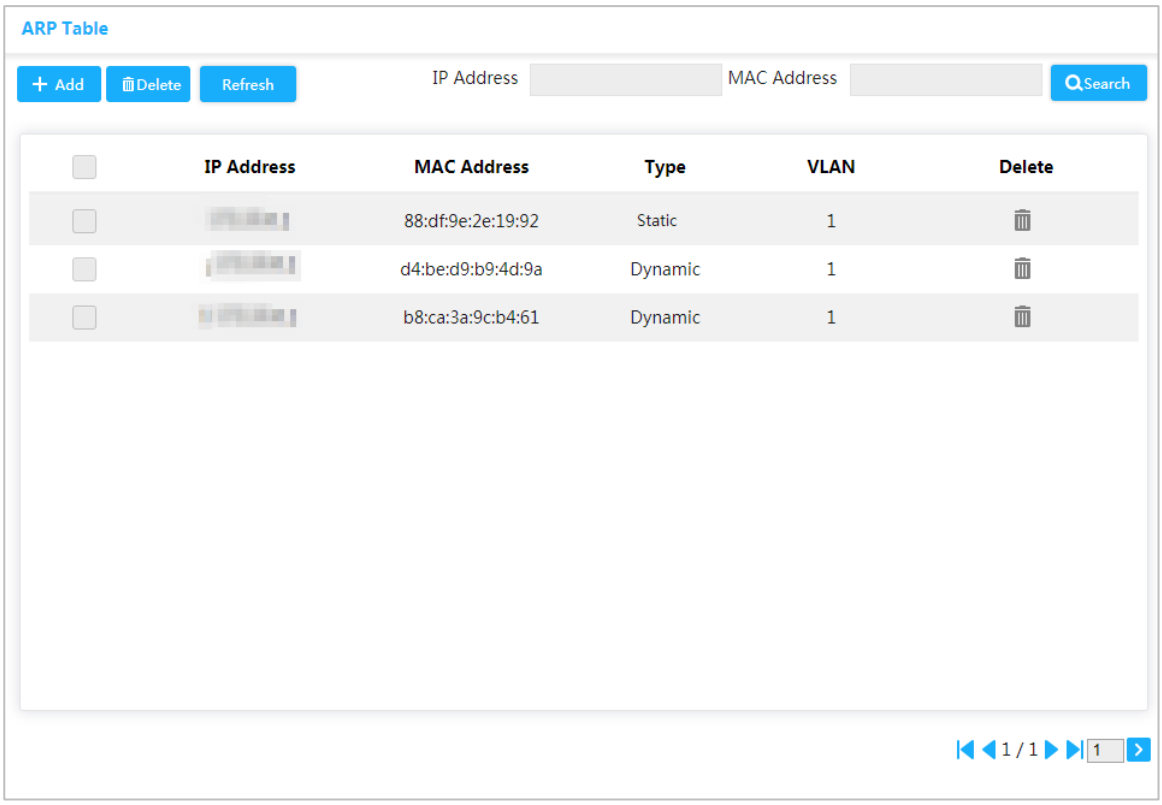
Static Table

The static ARP table is manually configured and maintained. It will not not be aged, and it will not be covered by dynamic ARP table.

Static ARP table can enhance the security performance of communication. Static ARP table can regulate that only the specific MAC address can be used in communication between network devices, and the attack packet can not modify the mapping between the IP address and the physical address of the table.Communication between the device and the pointed device is protected.

Step 1 Select **Advanced > Common > ARP Table**.
The **ARP Table** interface is displayed. See Figure 3-19. When the **Type** column shows **Static,** it is the static table.

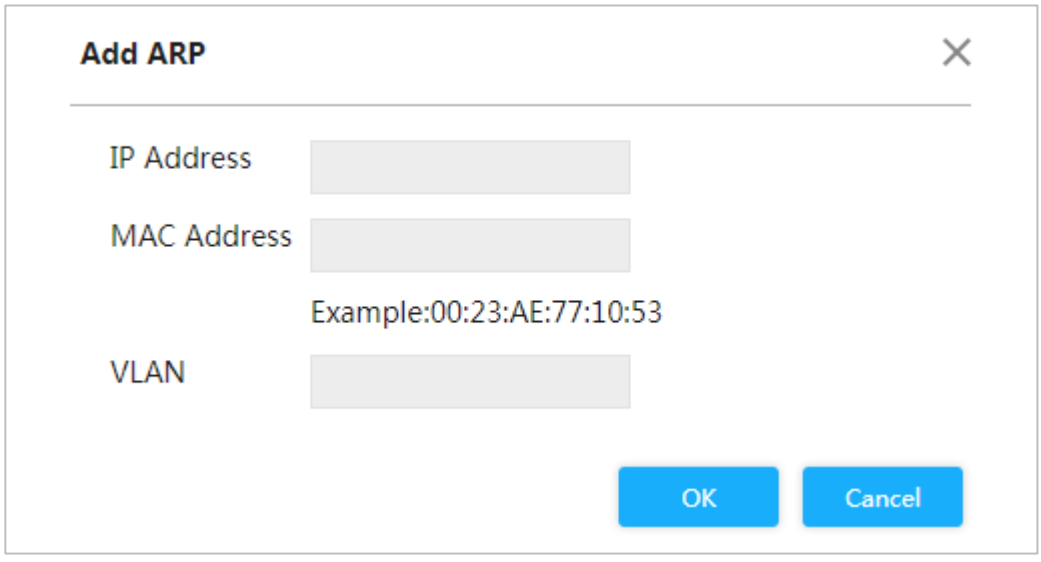
Figure 3-19 ARP table



Step 2 Click **Add**.

The **Add ARP** dialog box is prompted. See Figure 3-20.

Figure 3-20 Add ARP



Step 3 Set the IP address, MAC address and VLAN.

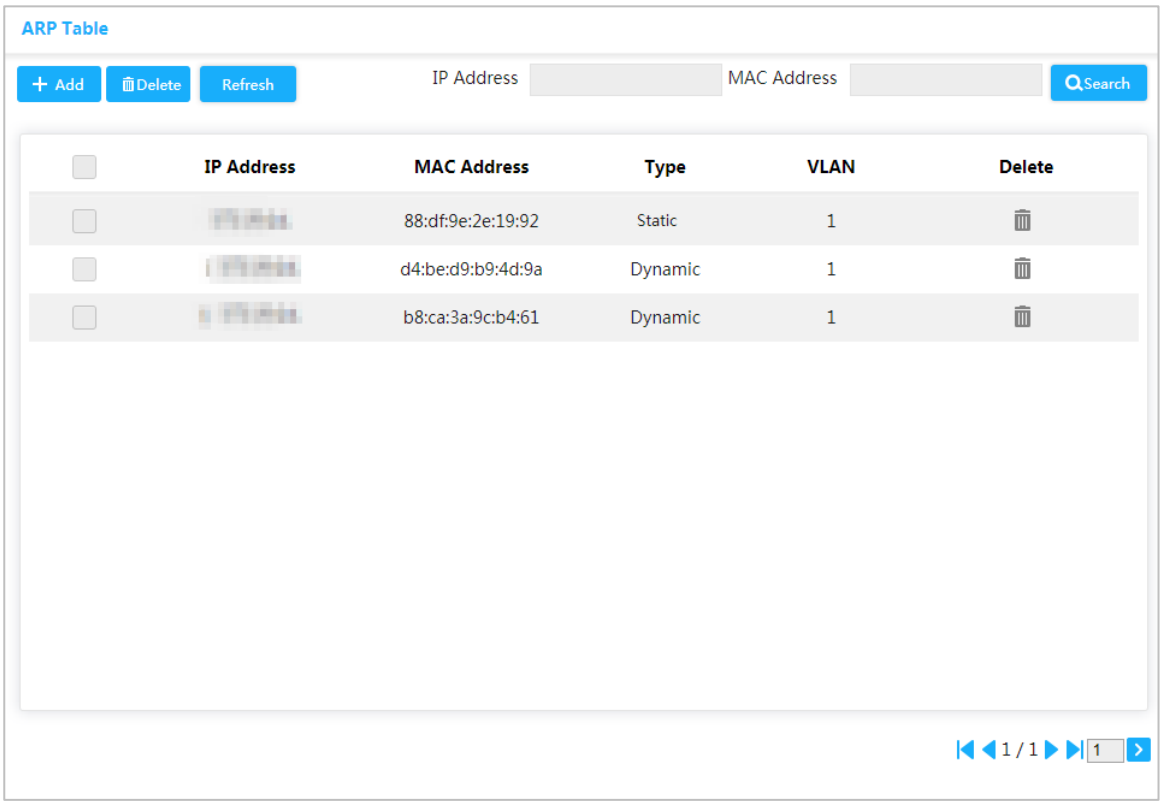
Step 4 Click **OK**.

Dynamic Table

Dynamic table is automatically created and maintained by ARP through ARP packet. It can be aged, and it can be covered by new ARP packet or static ARP table. When reaching ageing time and the port is down, the corresponding dynamic table will be deleted.

Select **Advanced > Common> ARP Table**.The **ARP Table** interface is displayed. See Figure 3-21. When the **Type** column shows **Dynamic,** it is the dynamic table.

Figure 3-21 Dynamic ARP view table



3.1.7 Spanning Tree

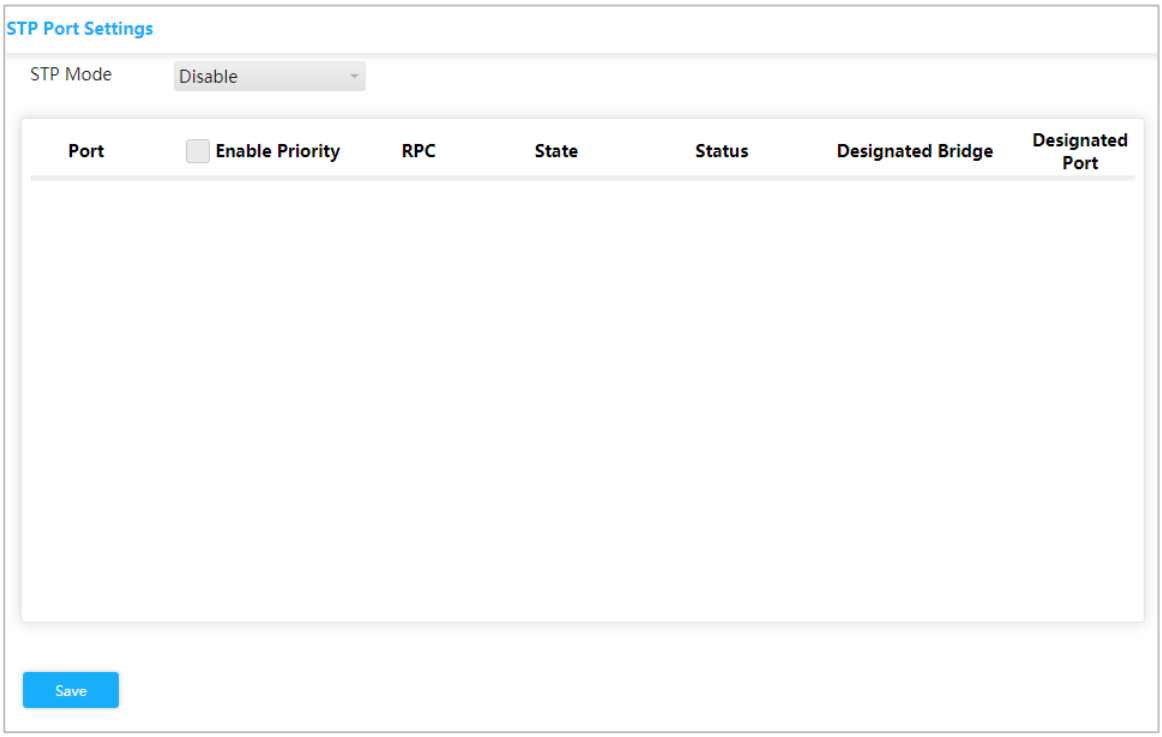
The spanning tree protocol is the protocol of layer 2. It can eliminate the ring cycle of layer 2 by choosing to block the redundant links in the network, and it can back up the links.

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 3-22.

Figure 3-22 STP ports settings



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 3-23, Figure 3-24 and Figure 3-25.

Figure 3-23 STP mode

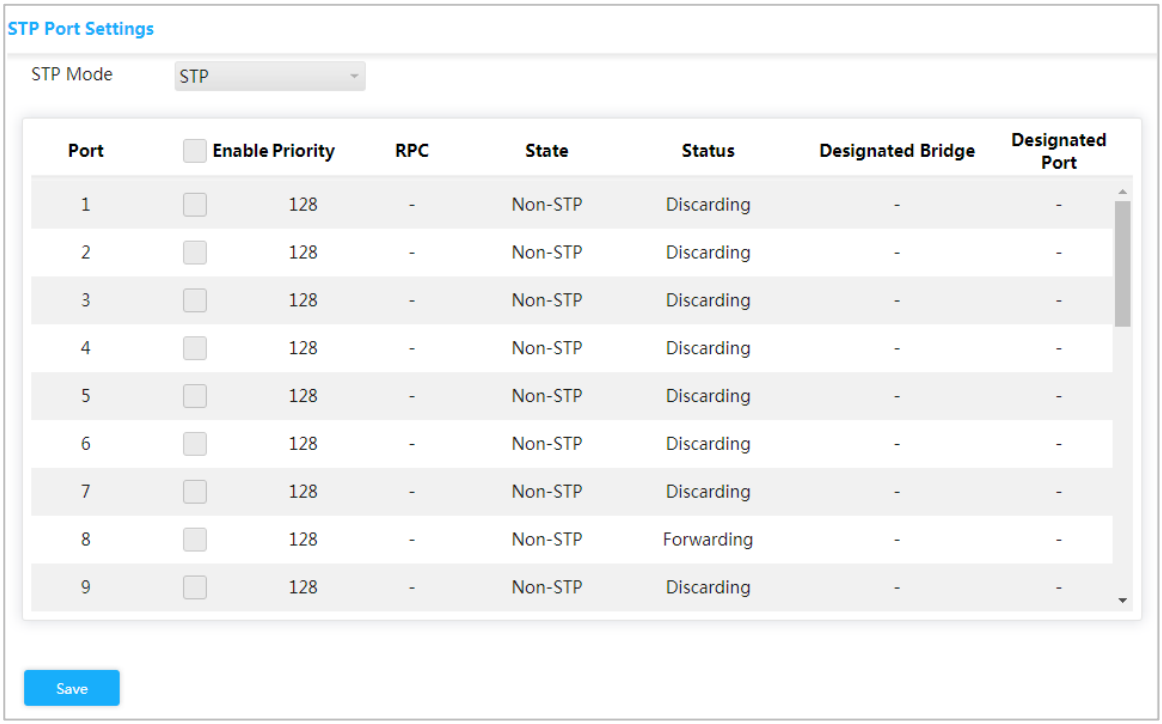


Figure 3-24 RSTP mode

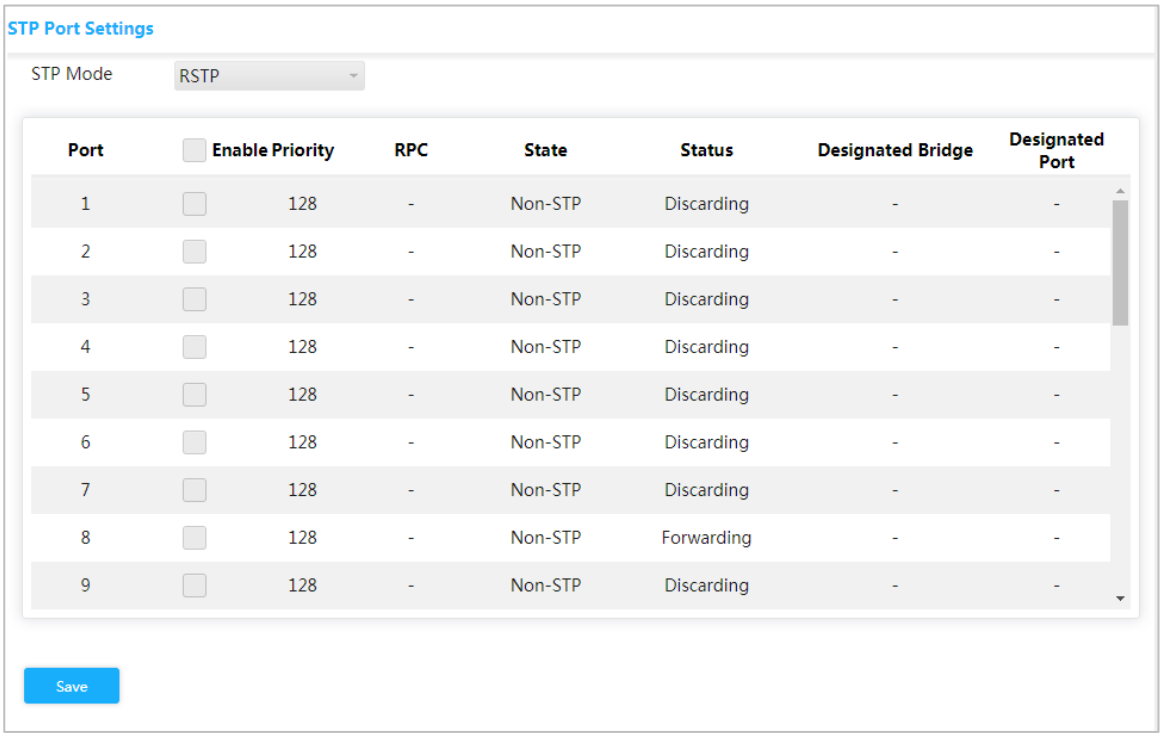
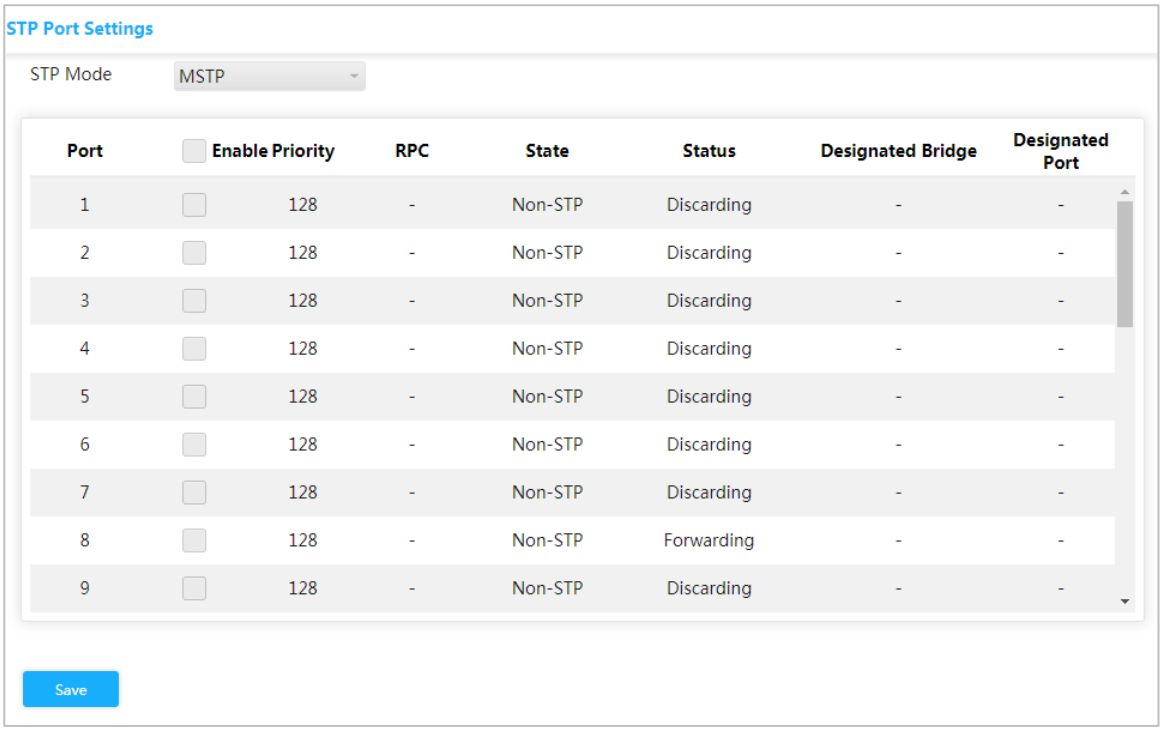
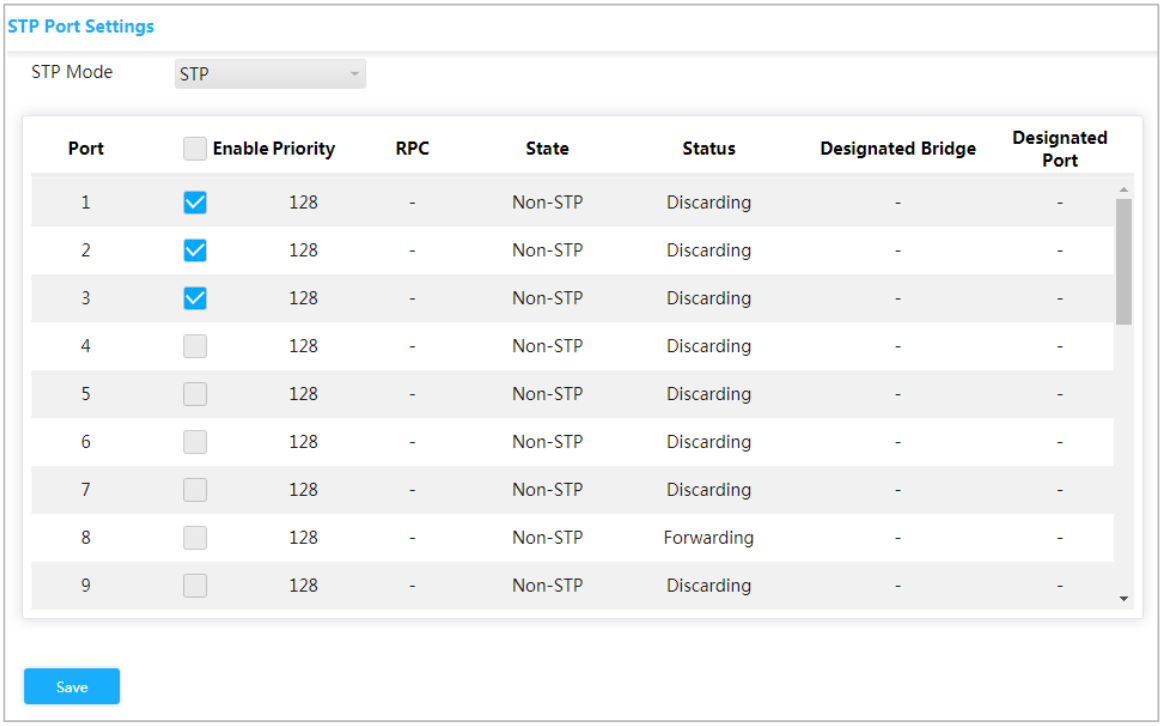


Figure 3-25 MSTP mode



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 3-26.

Figure 3-26 STP snoop



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

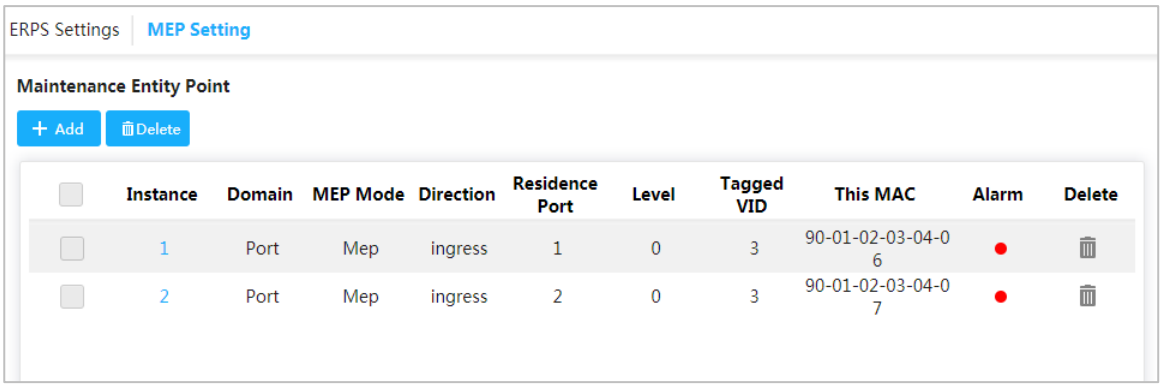
MEP (Maintenance entity group End Point) is a part of ERPS.

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 3-27.

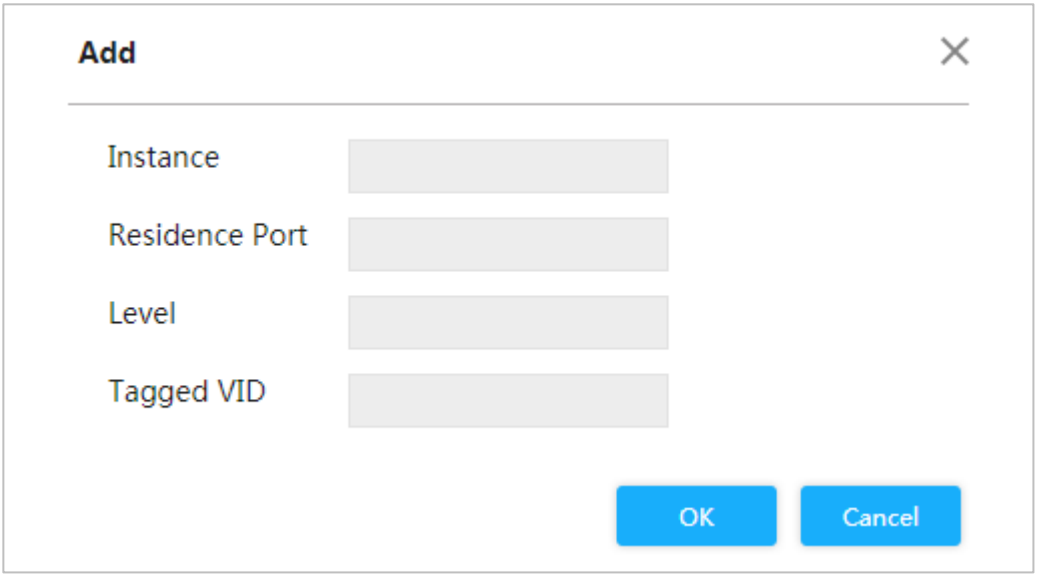
Figure 3-27 MEP Configuration



Step 2 Click **Add**.

The **Add** dialog box is prompted. See Figure 3-28.

Figure 3-28 Add



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

Table 3-5 MEP parameters

Parameters	Description
Instance	Enter MEP instance no.
Residence Port	Enter the port number that MEP belongs.
Level	Maintenance level, and it is recommended to set it to be 0.
Tagged VID	Enter protocol VLAN.

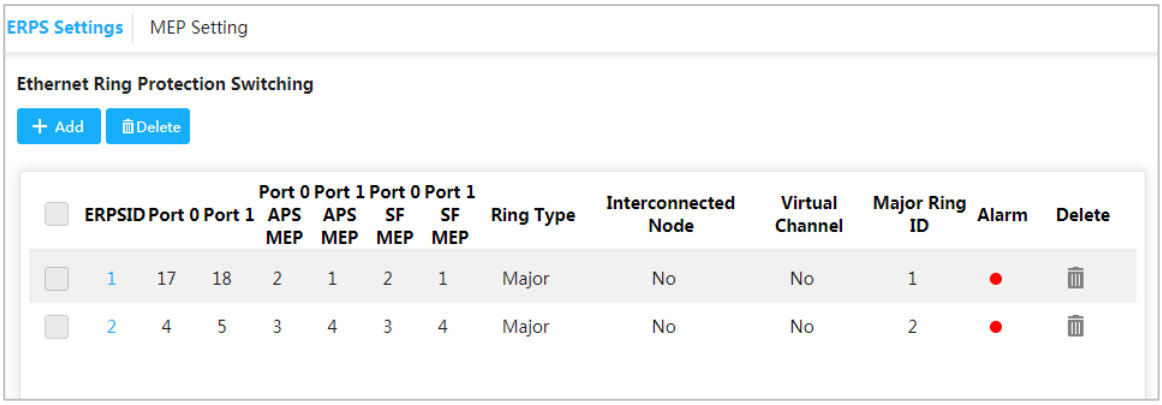
Step 4 Click **OK**.

3.2.1.2 ERPS Configuration

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

The **ERPS Setting** interface is displayed. See Figure 3-29.

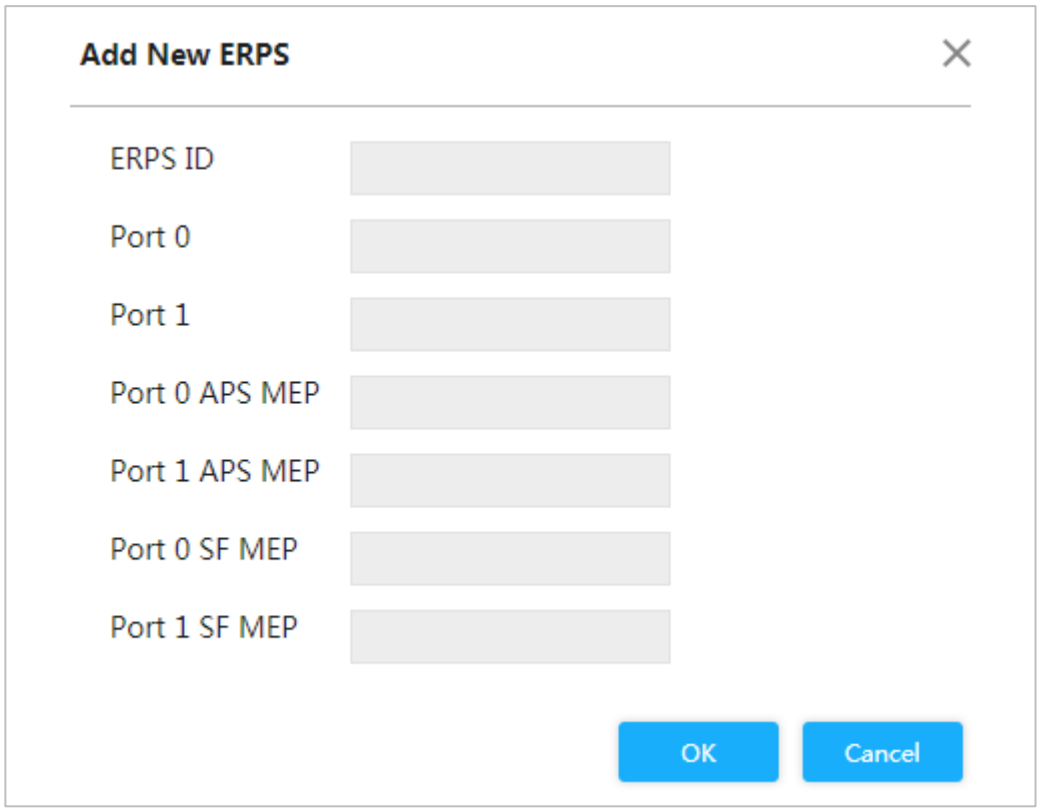
Figure 3-29 ERPS Configuration



Step 2 Click **Add**.

The **Add New ERPS** dialog box is prompted. See Figure 3-30.

Figure 3-30 Add New ERPS



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

Table 3-6 ERPS parameters

Parameters	Description
ERPS ID	The ID no of ERPS.
Port 0	The two ports added into the ERPS.
Port 1	
Port 0 APS MEP	The protocol packet ERPS corresponding to the ERPS port. Keep Port 0 APS MEP consistent with Port 0 SF MEP. Keep Port 1 APS MEP consistent with Port 1 SF MEP.
Port 1 APS MEP	
Port 0 SF MEP	Aggression Inspection MEP corresponding ERPS port. Keep Port 0 APS MEP consistent with Port 0 SF MEP. Keep Port 1 APS MEP consistent with Port 1 SF MEP.
Port 1 SF MEP	

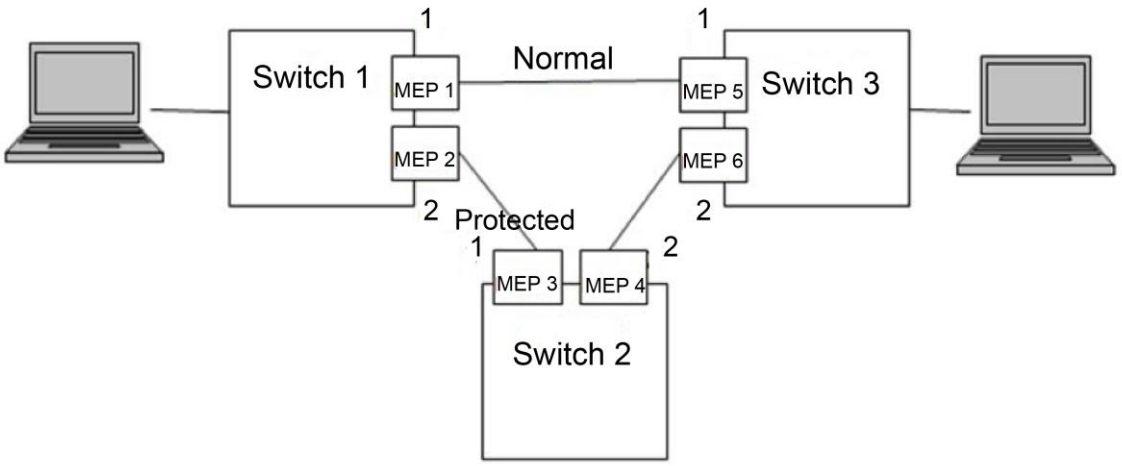
Step 4 Click **OK**.

3.2.1.3 Example: ERPS Single Ring Configuration

Networking Requirement

Three switches, and the ports are port 1 and port 2. It is requested to combine an ERPS. See Figure 3-31. The corresponding relationship: Switch 1: MEP 1 and MEP 2; Switch 2: MEP3 and MEP 4; Switch 3: MEP 5 and MEP 6.

Figure 3-31 ERPS single ring configuration



Configuration

Configure the ERPS with the following thoughts:

1) Confirm Topology, and plan protection VLAN and protocal 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 ower port. Ensure to disable the mutex function of the ports, including STP function and LLDP function.

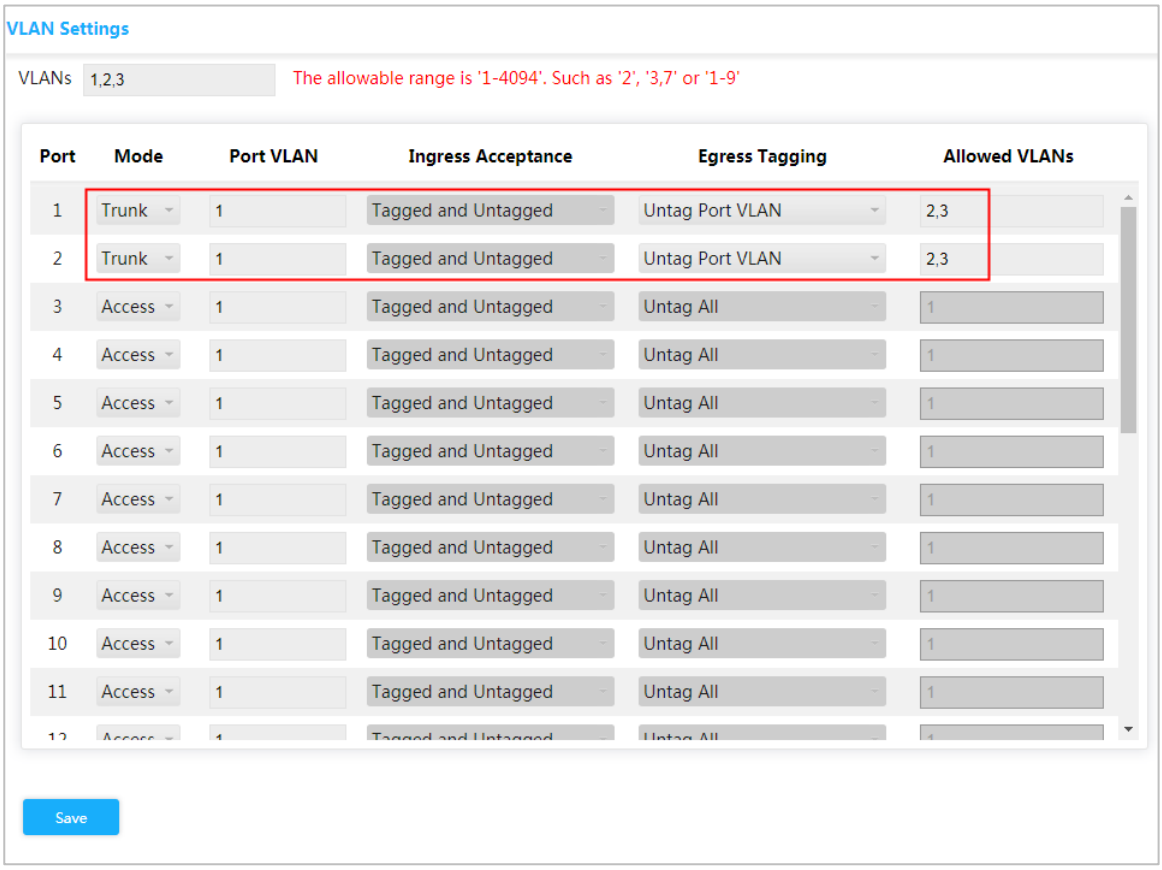
The configurations of the switch are as following：

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.See .
2) Set the mode of port 1 and port 2 to be **Trunk**. See Figure 3-32.
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.**

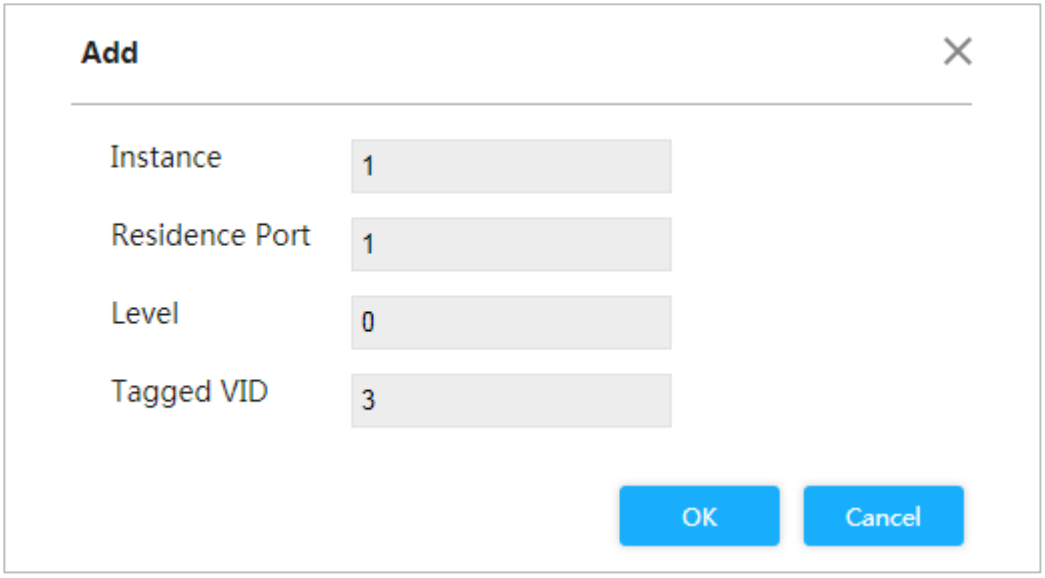
Figure 3-32 Add port 1 and port 2 into VLAN 1.



Step 2 Create MEP1 and MEP 2.

1) Select **Advanced > Seldom-used > ERPS > ERPS Setting**.
   The **ERPS Setting** interface is displayed.
2) Click **Add**.
   The **Add** dialog box is prompted.
3) Set **Instance** to be 1. See Figure 3-33.
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 3-33 Add MEP



Add MEP 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 3-34 and Figure 3-35.

Figure 3-34 Configure the peer ID of MEP 1

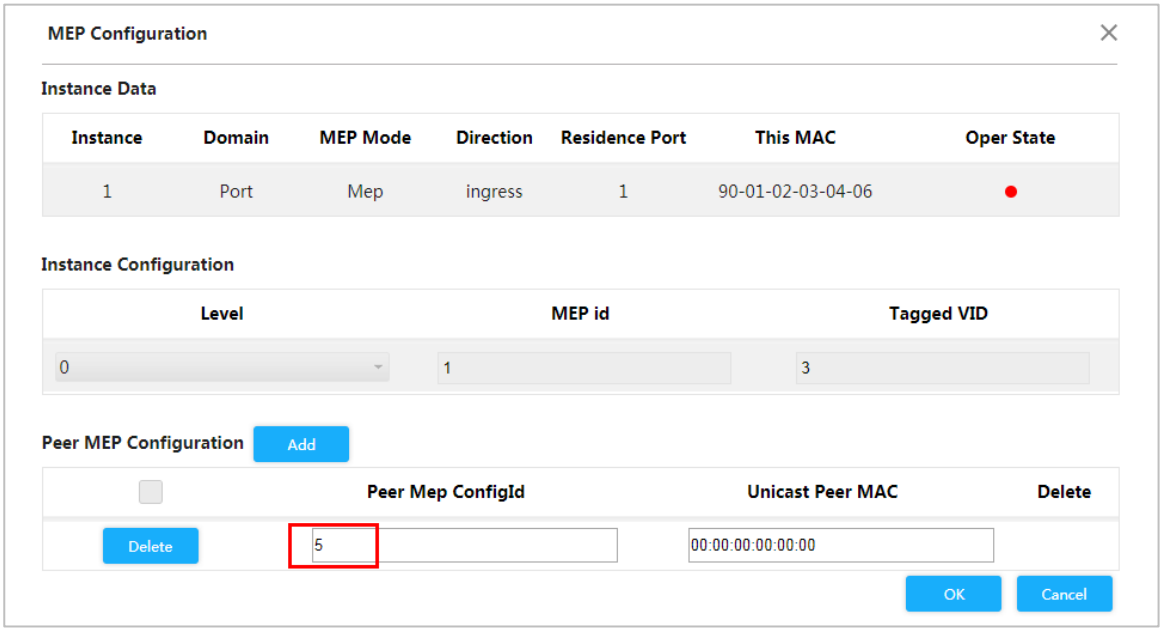
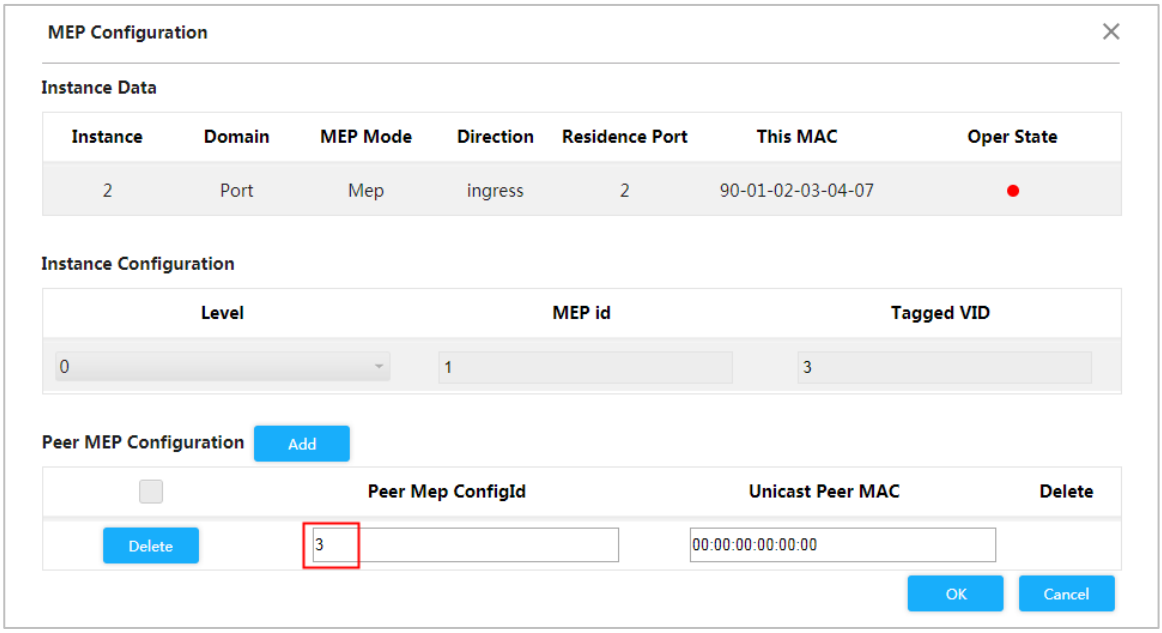


Figure 3-35 Configure the peer ID of MEP 2

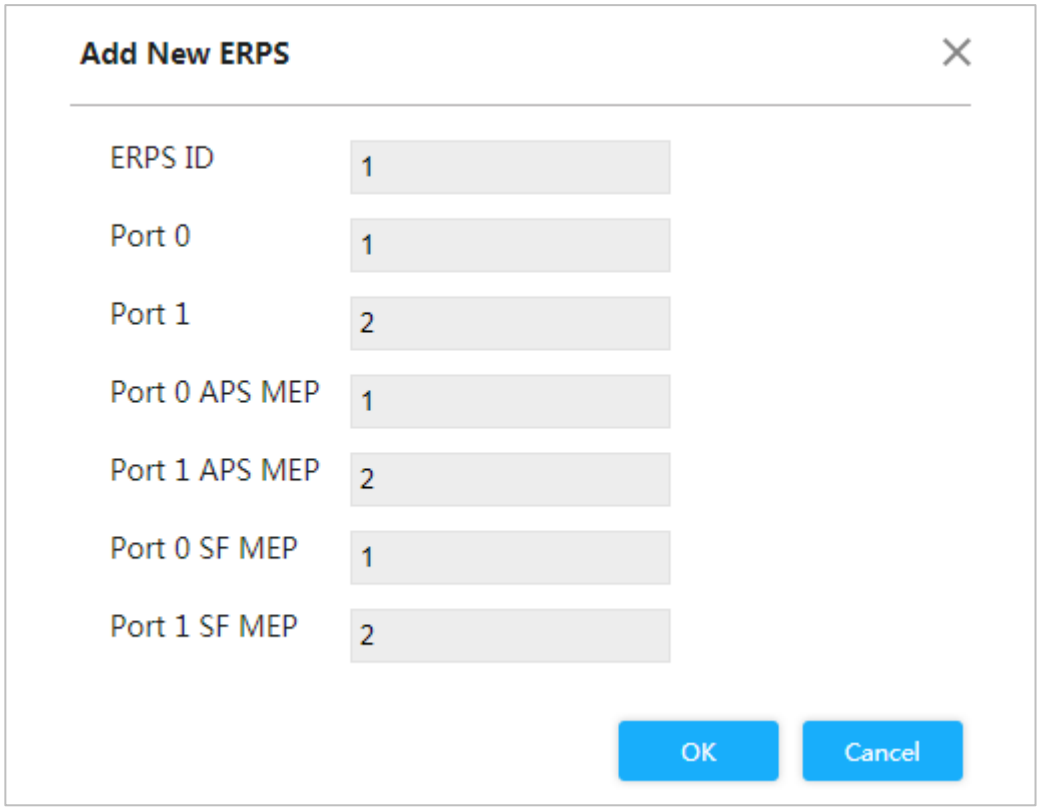


Step 4 Click **OK**.

Step 5 Create ERPS.

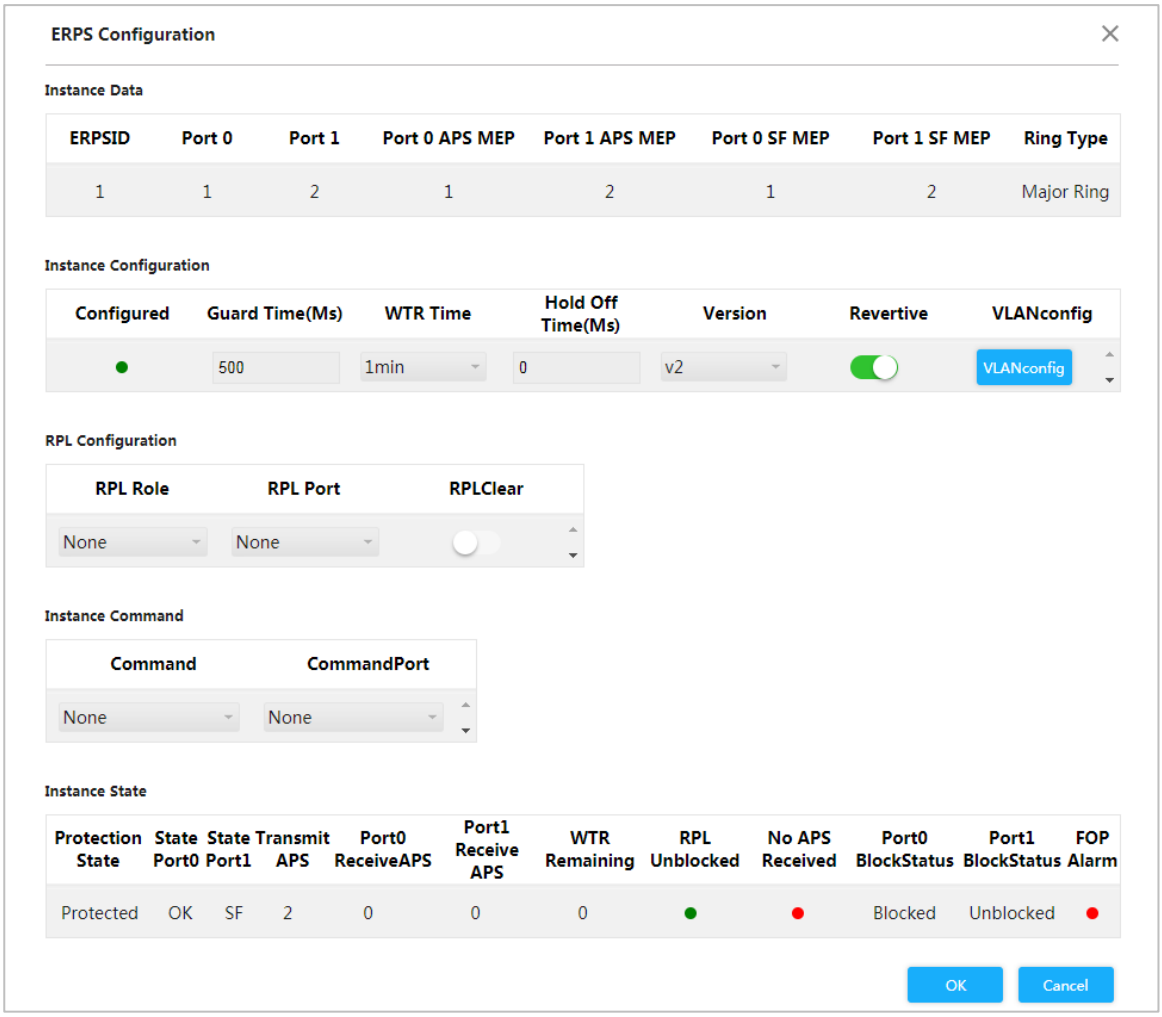
1) Select **Advanced > Seldom-used > ERPS > ERPS Setting**.
   The **ERPS Setting** interface is displayed.
2) Click **Add**.
   The **Add New ERPS** dialog box is prompted.
3) Set **ERPS ID** to be 1. See Figure 3-36.
4) Set **Port 0** to be1 and **Port 1** to be 2.
5) Set **Port0 APS MEP** to to 1 and **Port 1 APS MEP** to be 2.
6) Set **Port0 SF MEP** to be1 and **Port 1 SF MEP** to be 2 .
7) Click **OK**.

Figure 3-36 Add New ERPS



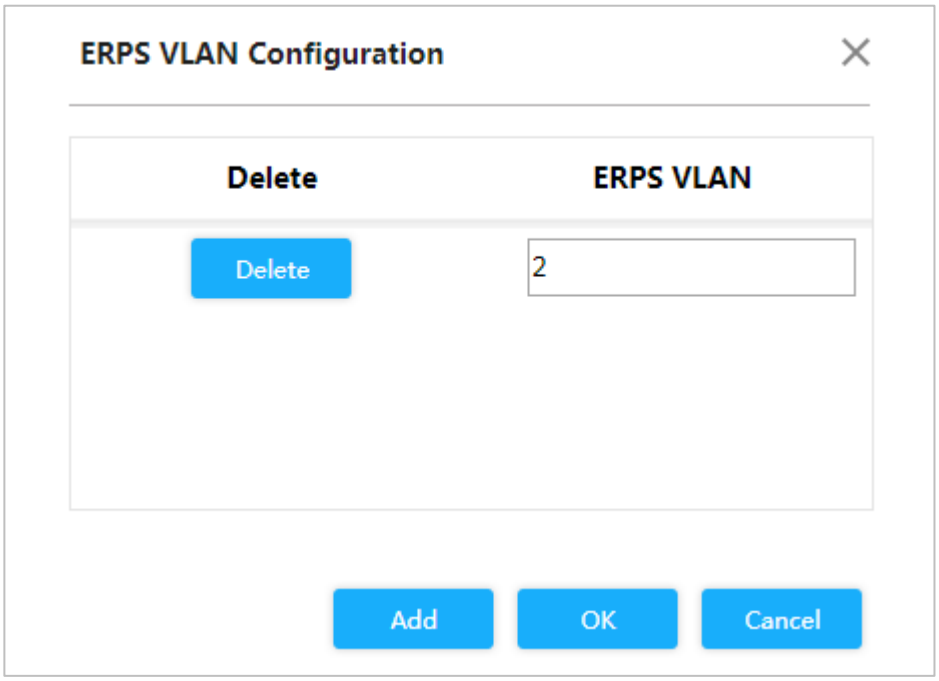
Step 6 Click **1** under **ERPSID** to enter the configuration interface. For ERPS configuration, see Figure 3-37.

Figure 3-37 ERPS Configuration



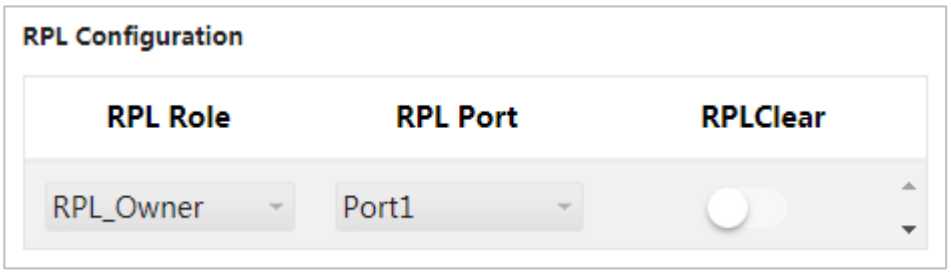
1) Click VLANconfig.
   The **ERPS VLAN Configuration** dialog is prompted.
2) Click **Add**.
3) Set **ERPS VLAN** to be 2. See Figure 3-38.
4) Click **OK**.

Figure 3-38 ERPS VLAN configuration



5) Set port 2 of switch 1 to be **RPL ower**. See Figure 3-39.

Figure 3-39 Ower port configuration

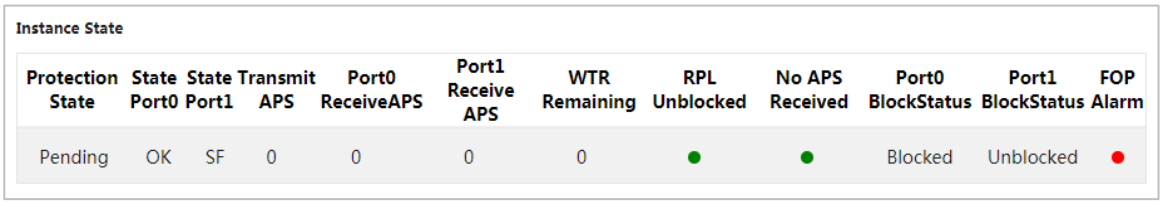


Step 7 Click **OK**.

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

Step 9 View the state on the **ERPS Configuration** interface. See Figure 3-40.

Figure 3-40 Instance State



3.2.2 ACL

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

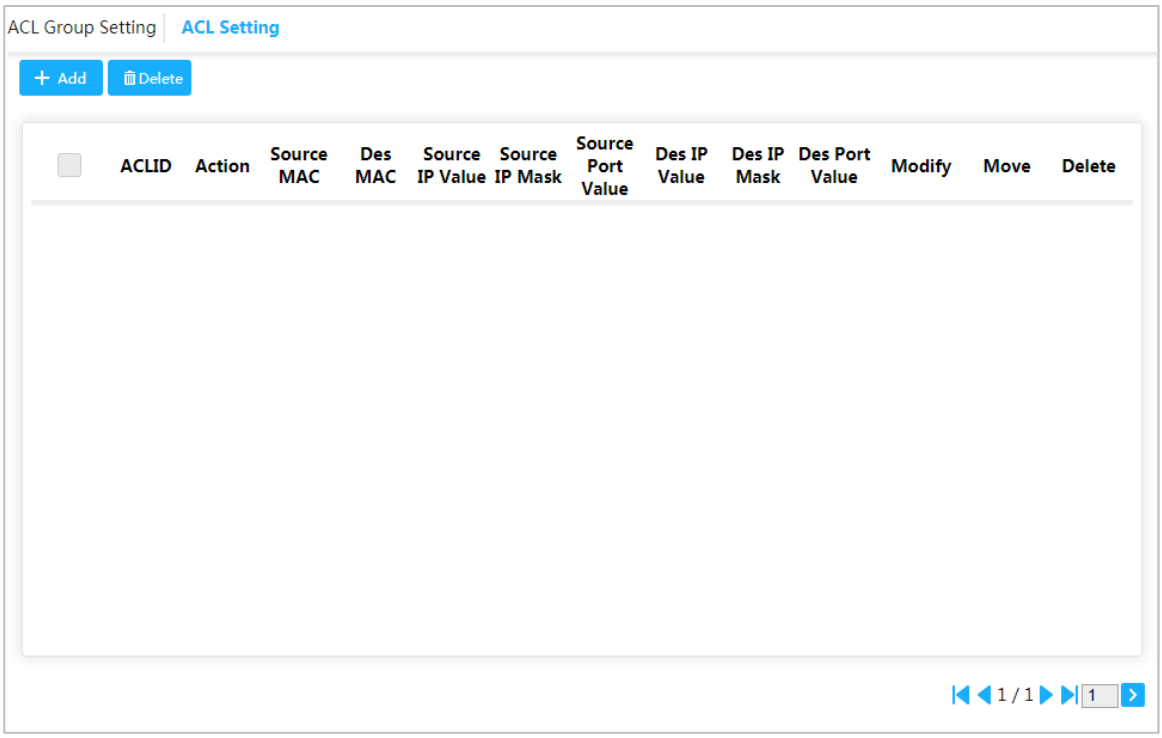
When the device port receives the packet, it can analyze the packet field according to the ACL rule of the current port. And after the specific packet is identified, the packet is allowed or forbidden to pass according to the preset rule.

3.2.2.1 ACL Configuration

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

The **ACL Setting** interface is displayed. See Figure 3-41.

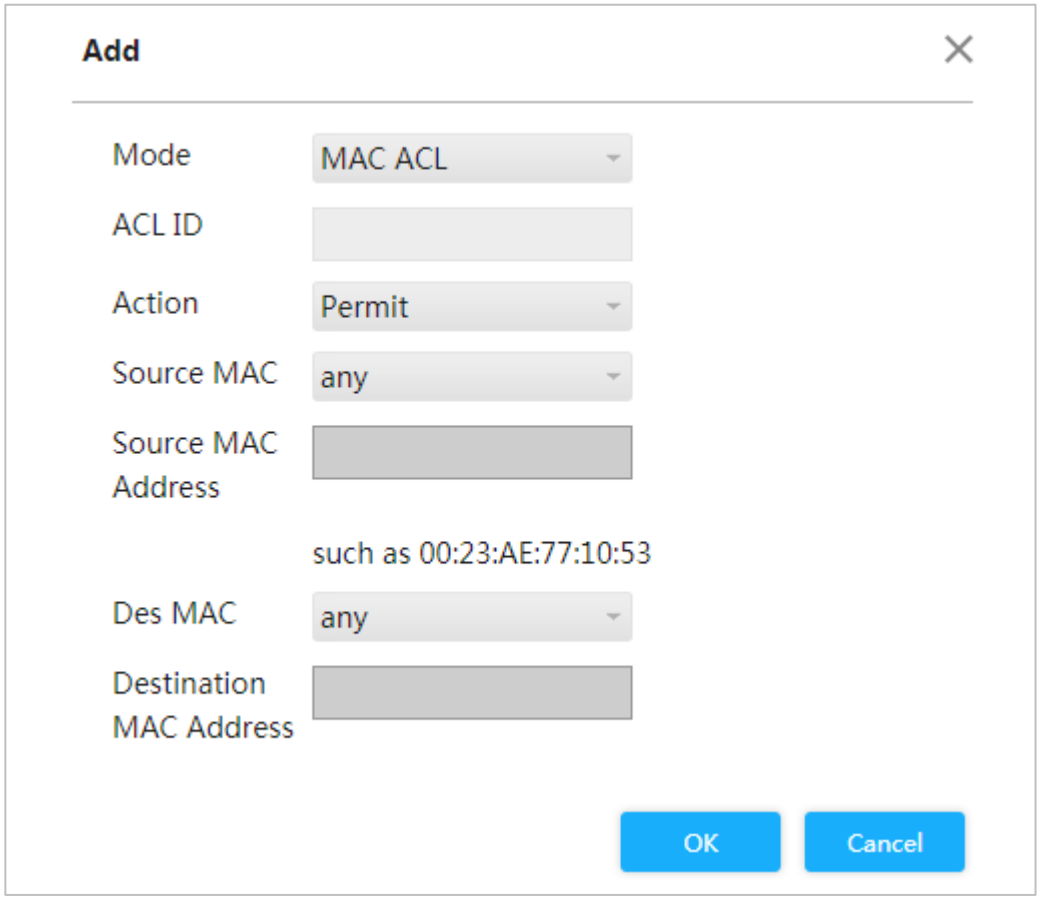
Figure 3-41 ACL Configuration



Step 2 Click **Add**.

The **Add** dialog box is prompted. See Figure 3-42.

Figure 3-42 Add



Step 3 Set the ACL ID. For example, 2.

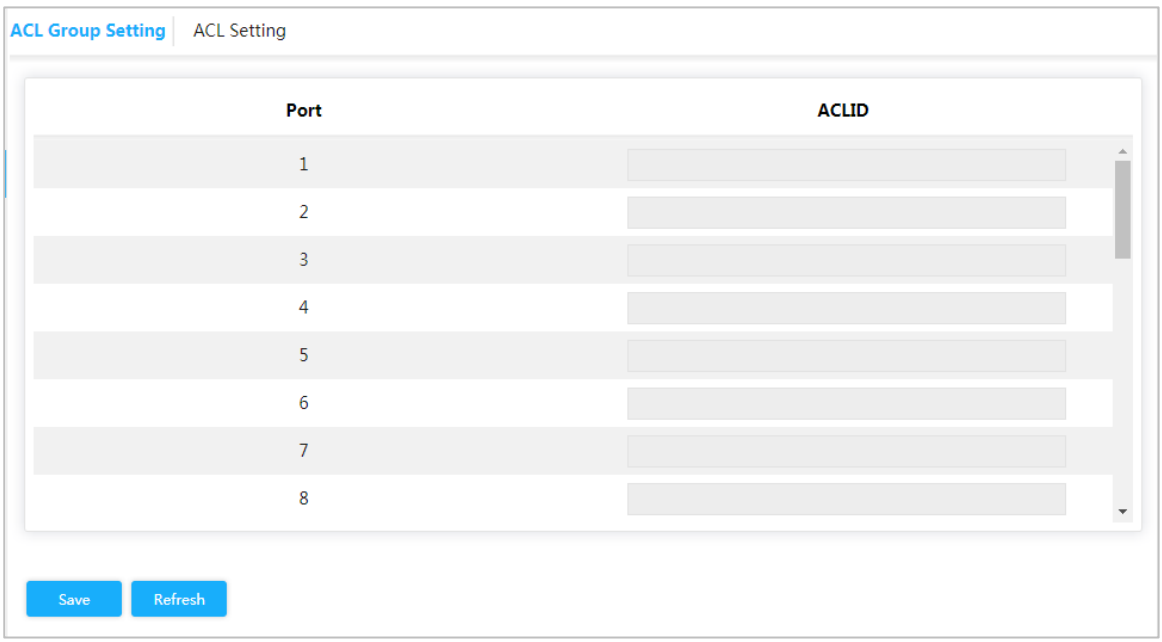
Step 4 Click **OK**.

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 3-43.

Figure 3-43 ACL Group Configuration



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

Step 3 Click **Save.**

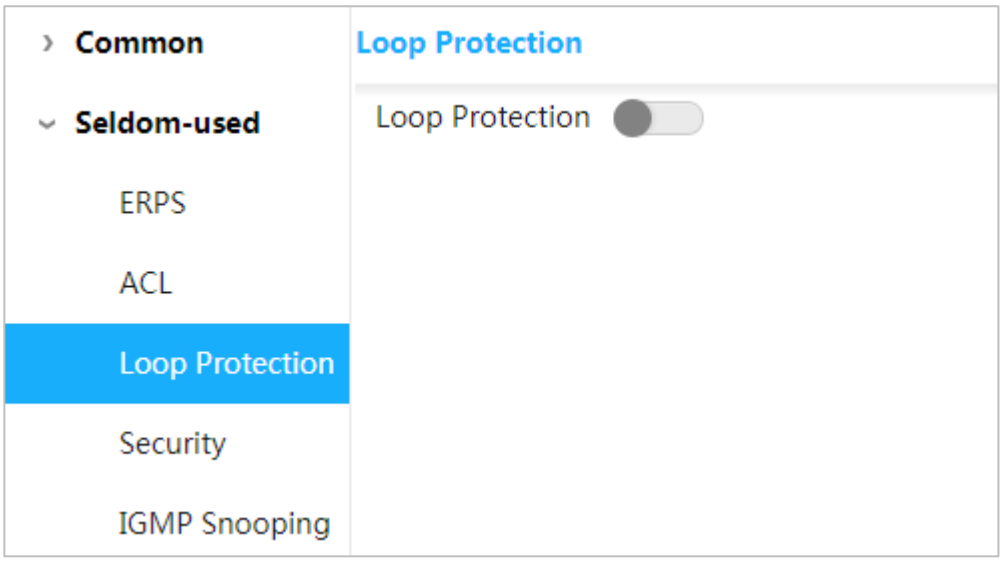
3.2.3 Loop Protection

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

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

The **Loop Protection** interface is displayed.See Figure 3-44.

Figure 3-44 Loop Protection



Step 2 Click  to enable Loop Protection.

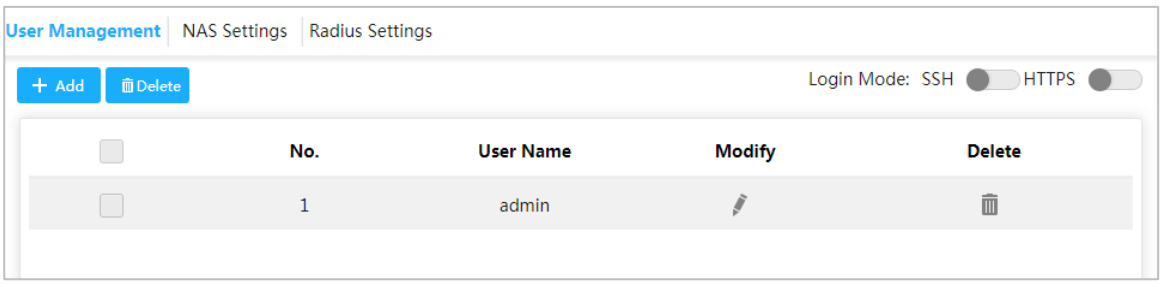
3.2.4 Security

3.2.4.1 User Management

You can add, edit, and delete user.

Select **Advanced > Seldom-used > Security > User Management**. **User Management** interface is displayed. See Figure 3-45.

Figure 3-45 User Management

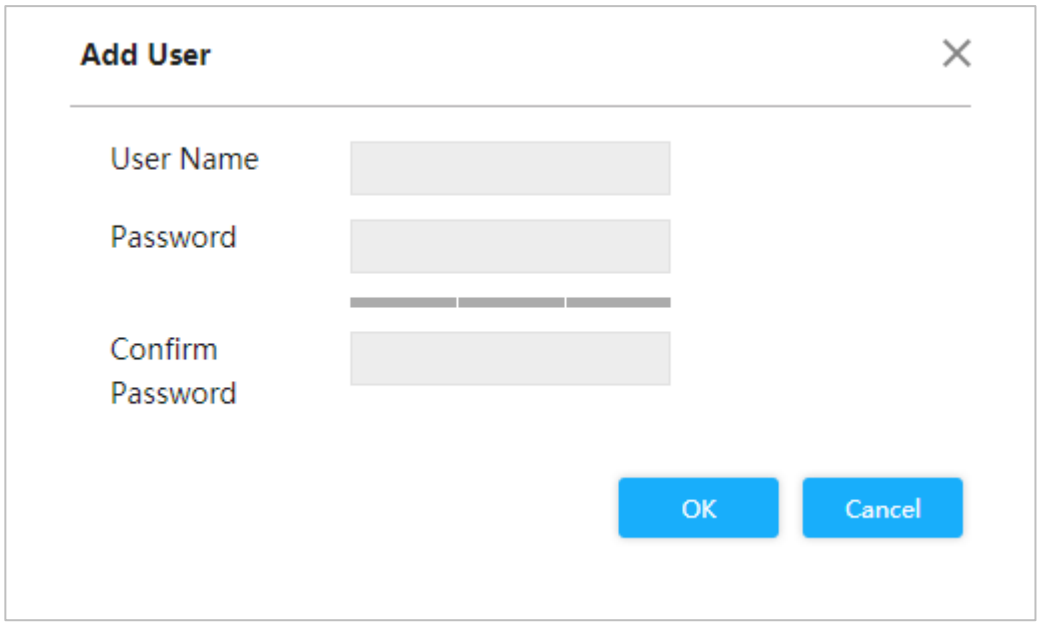


Add user

Step 1 Click **Add**.

The **Add User** interface is displayed. See Figure 3-46.

Figure 3-46 Add user

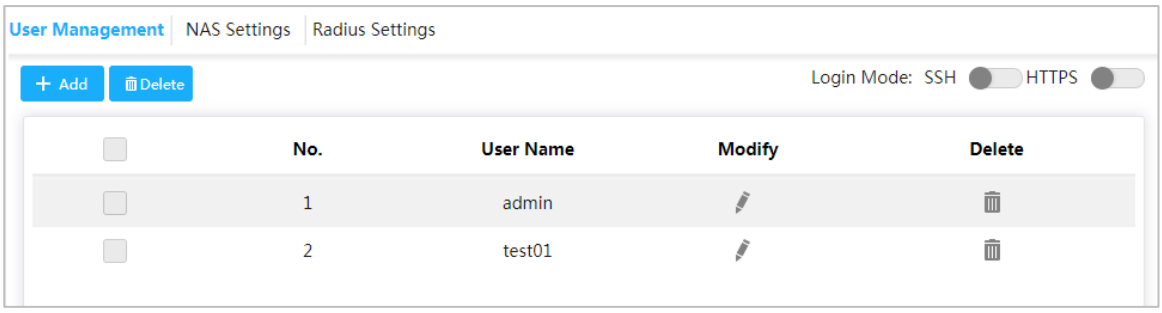


Step 2 Enter the user name, password and confirm password. The password can be set from 8 characters through 32 characters and contains at least two types from number, letter, and special characters (excluding"'", "'", ";", ":"and "&"). For example, add the new user test 01.

Step 3 Click **Save.**

The new user test 01 is added. See Figure 3-47.

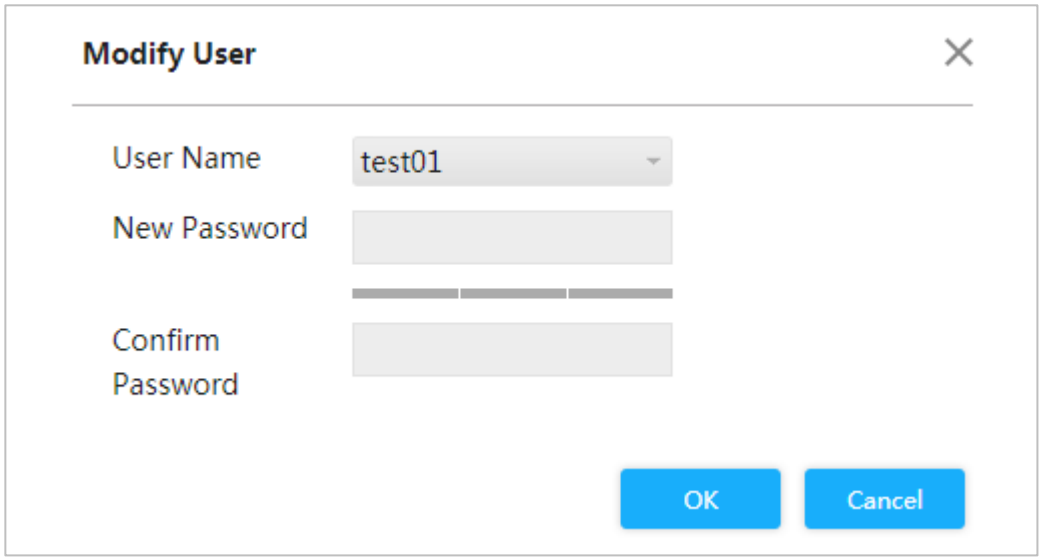
Figure 3-47 New user added



Modify and Delete User

- Click , and the **Modify User** interface is displayed. See Figure 3-48.

Figure 3-48 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 on 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. 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, it is used to protect account security and use information.

Click corresponding to HTTPS on the upper right on the **User Management** interface.

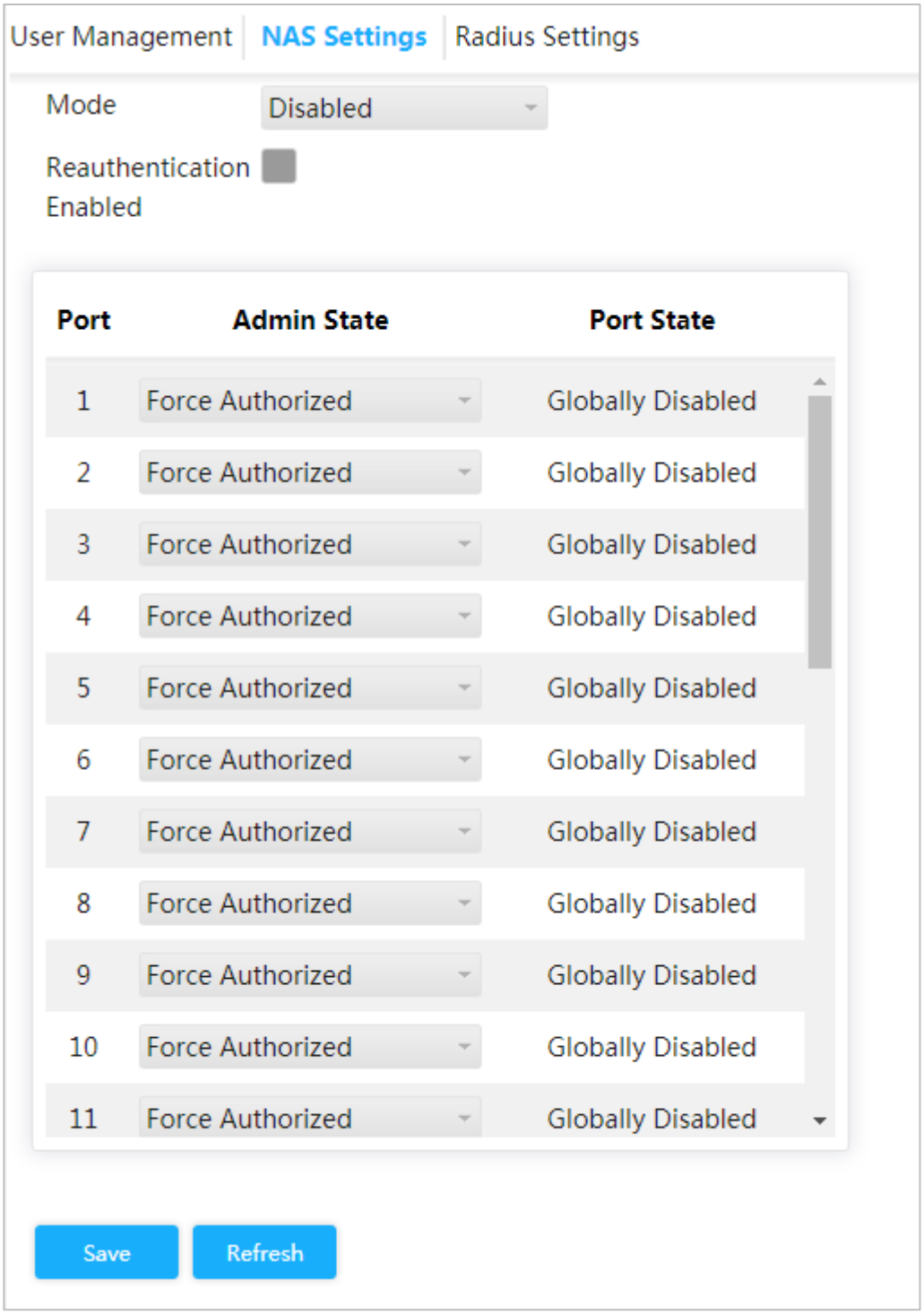
3.2.4.2 NAS Configuration

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

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

The **NAS Settings** interface is displayed.See Figure 3-49.

Figure 3-49 NAS Configuration



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

Step 3 Check the box **Reauthentication Enable** 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).

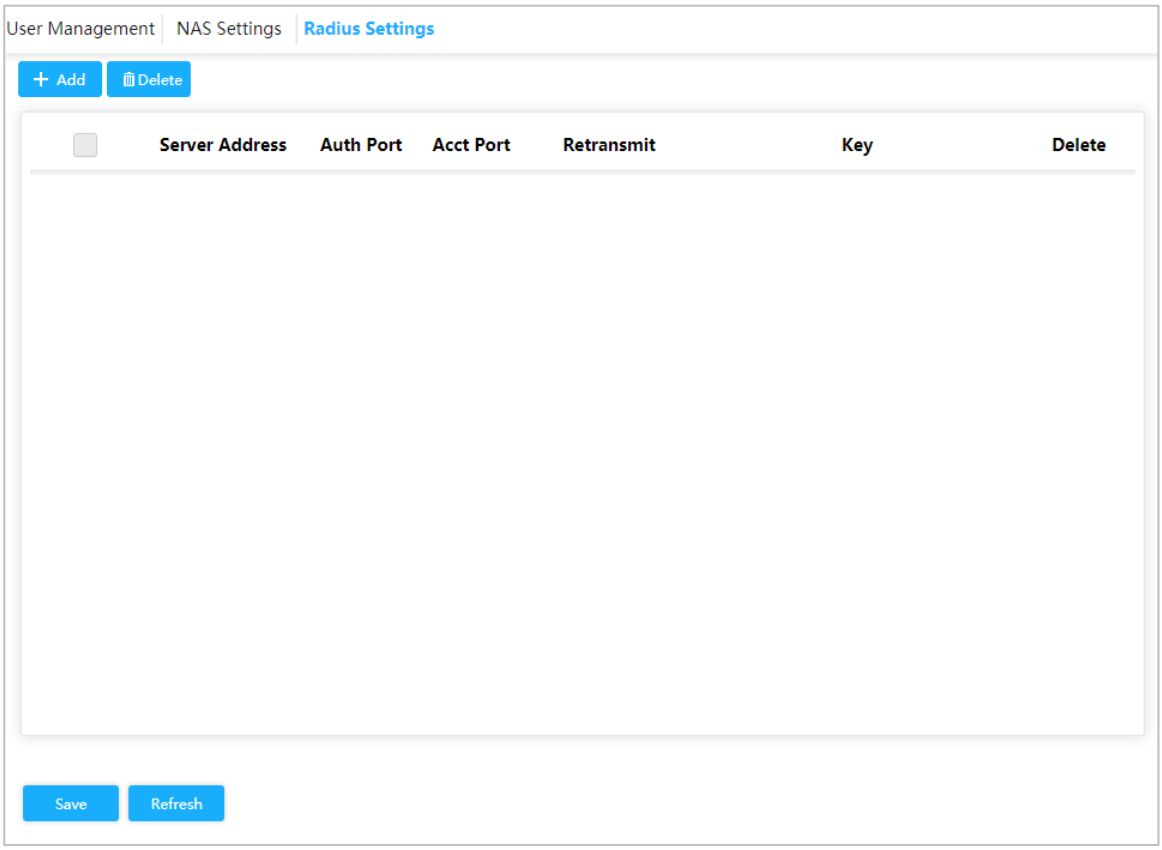
RADIUS is an information interaction protocol of distributed and C/S construction. It can protect the network from the interfere of unauthorized visits. It is used in the network that allows remote visits but requests the higher security. It defines the RADIUS packet format and the message transmission 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 3-50.

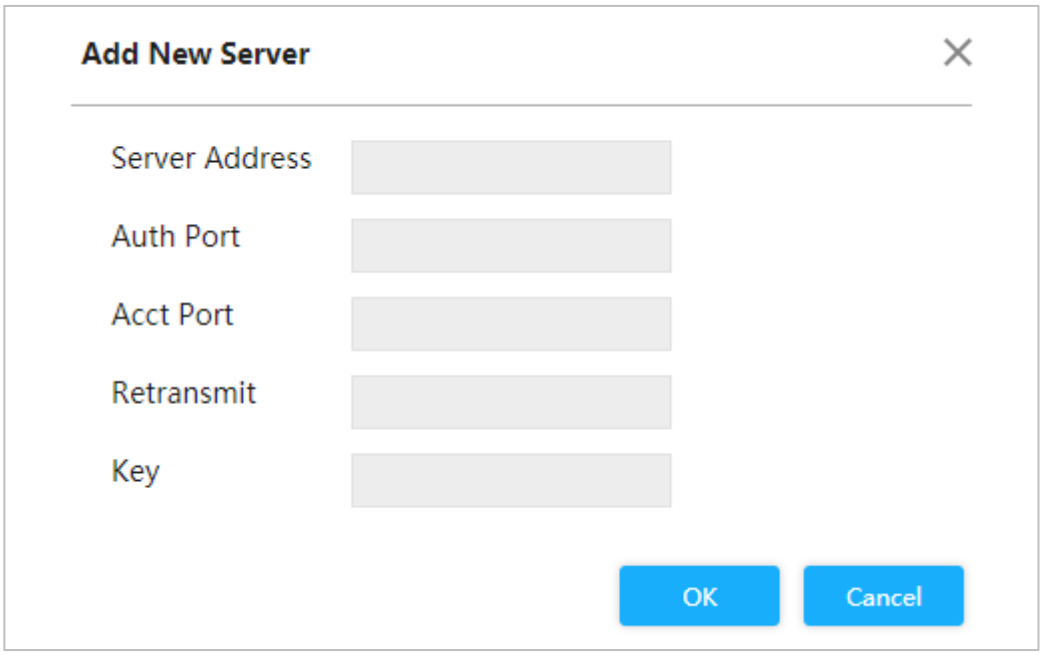
Figure 3-50 Radius configuration



Step 2 Click **Add**.

The **Add New Server** interface is displayed. See Figure 3-51.

Figure 3-51 Add new server



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

Step 4 Click **OK**.

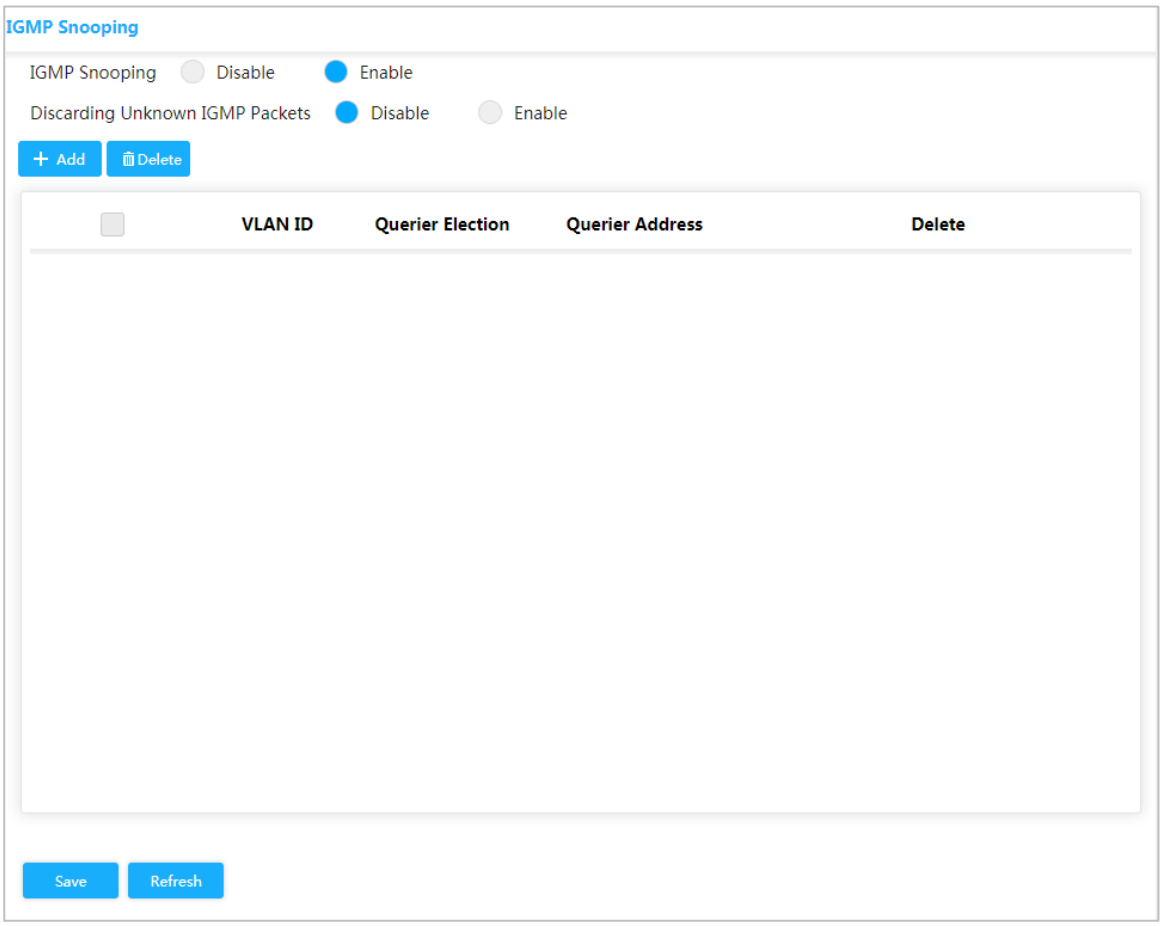
3.2.5 IGMP Snooping

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 3-52.

Figure 3-52 IGMP Snooping



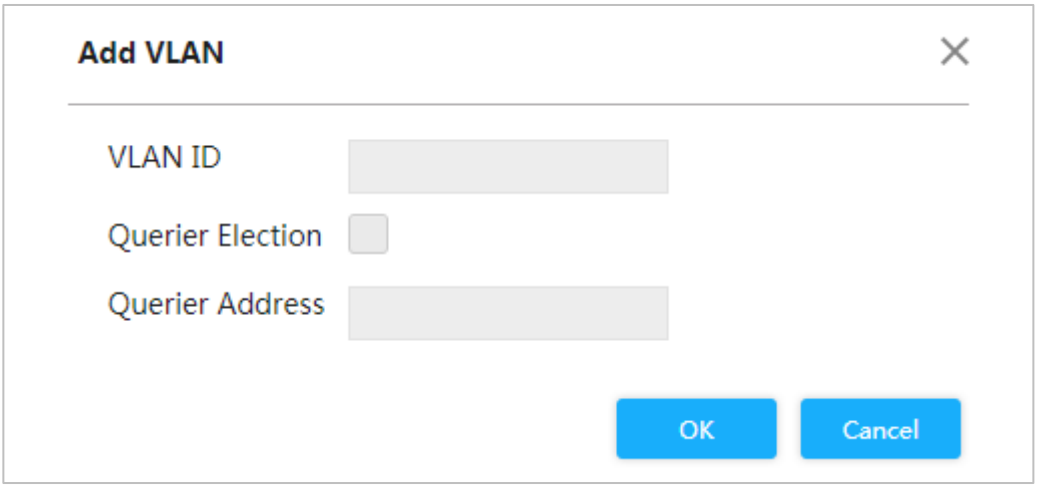
Step 2 Select **Enable IGMP Snooping** to enable the function.

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

Step 4 Click **Add**.

The **Add VLAN** dialog box is prompted. See Figure 3-53.

Figure 3-53 Add VLAN



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

Step 6 Click **OK**.

3.2.6 QoS

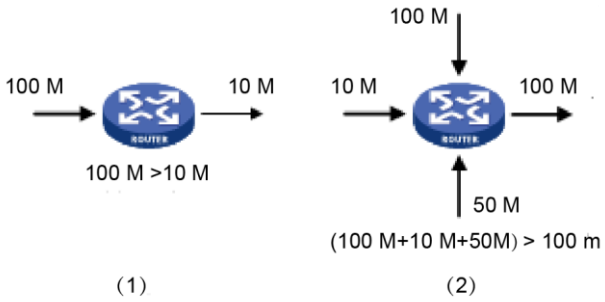
QoS (Quality of Service) is used to evaluate the capability that server meets customer's service demands. In Internet, what QoS evaluates is the service capability of network forwarding and packet.

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 3-54 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

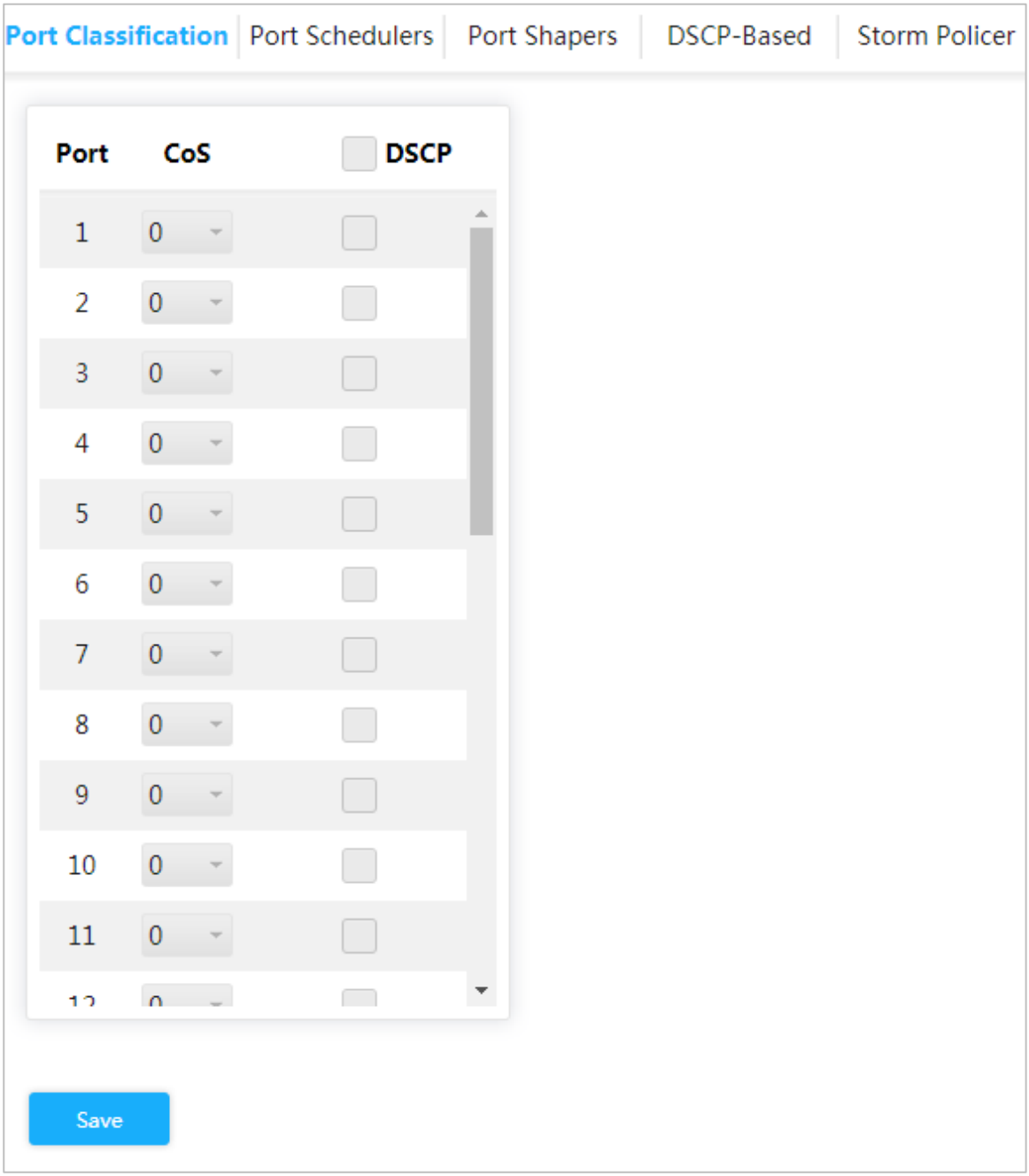
Through setting Cos, the priority for packet passing egress port of switch can be decided.

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 large the Cos value is, the higher the priority.

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

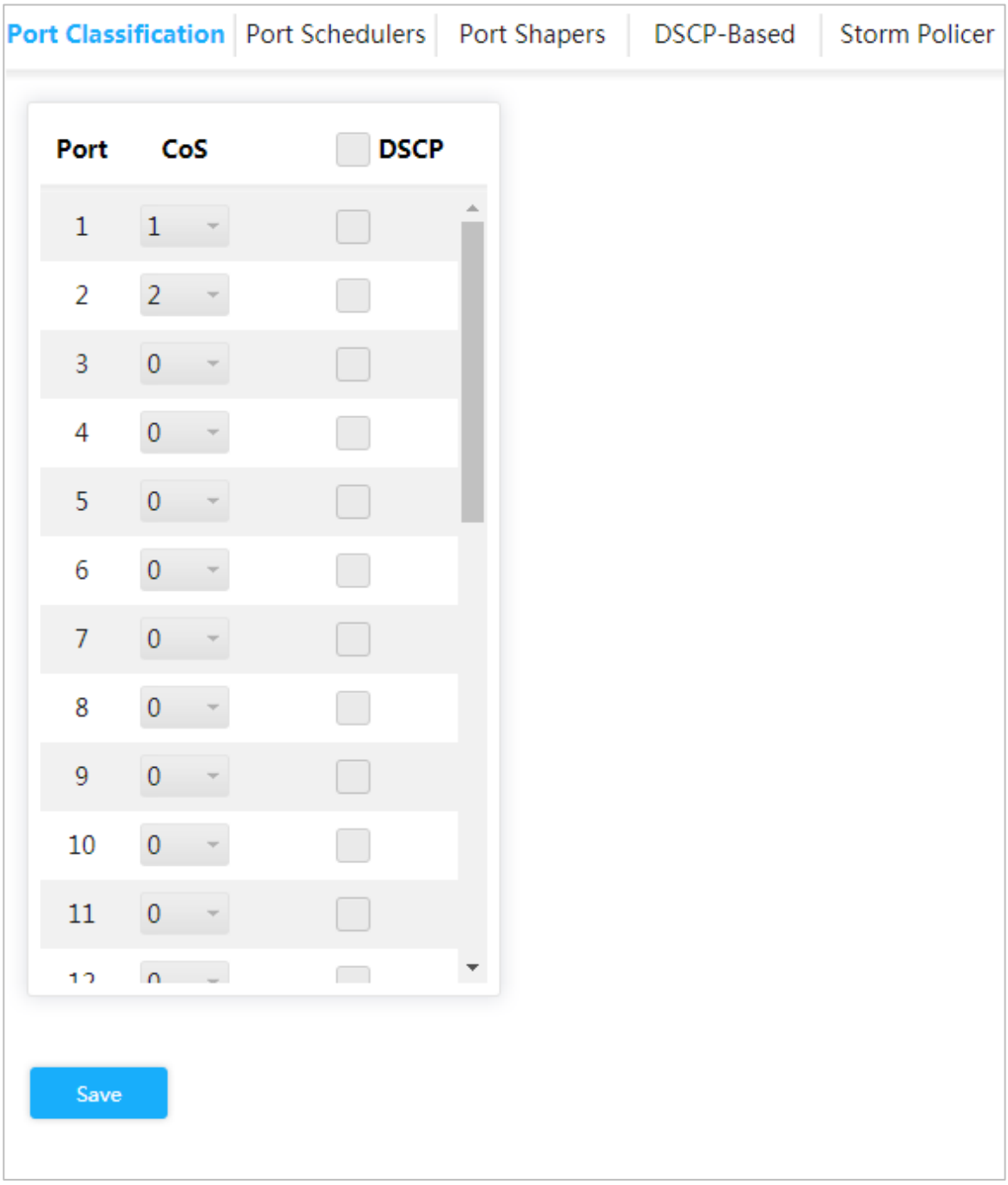
The **Port Classification** interface is displayed. See Figure 3-55.

Figure 3-55 Port classification



Step 2 Set the CoS. For example: Set port 1 to be 1, and port 2 to be 2. See Figure 3-56. 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 3-56 Set Cos



Step 3 Click **Save.**

3.2.6.2 Port Schedulers

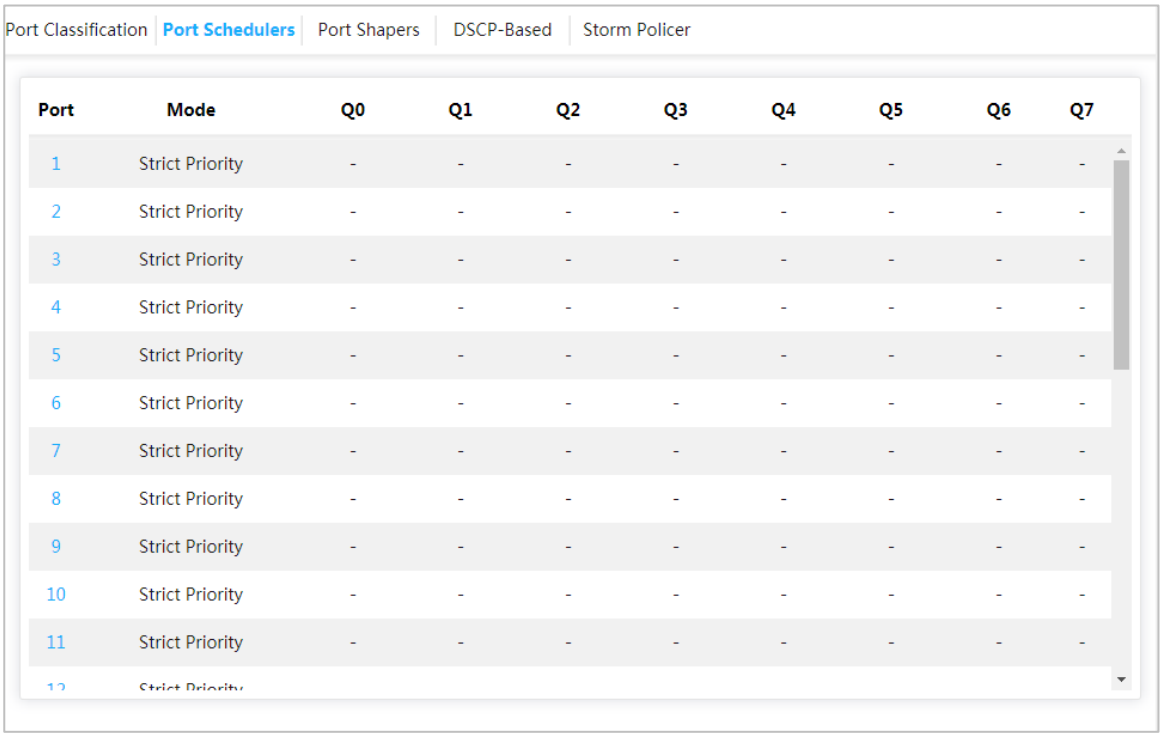
The two modes of port schedulers:

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

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

The **Port Schedulers** interface is displayed.See Figure 3-57.

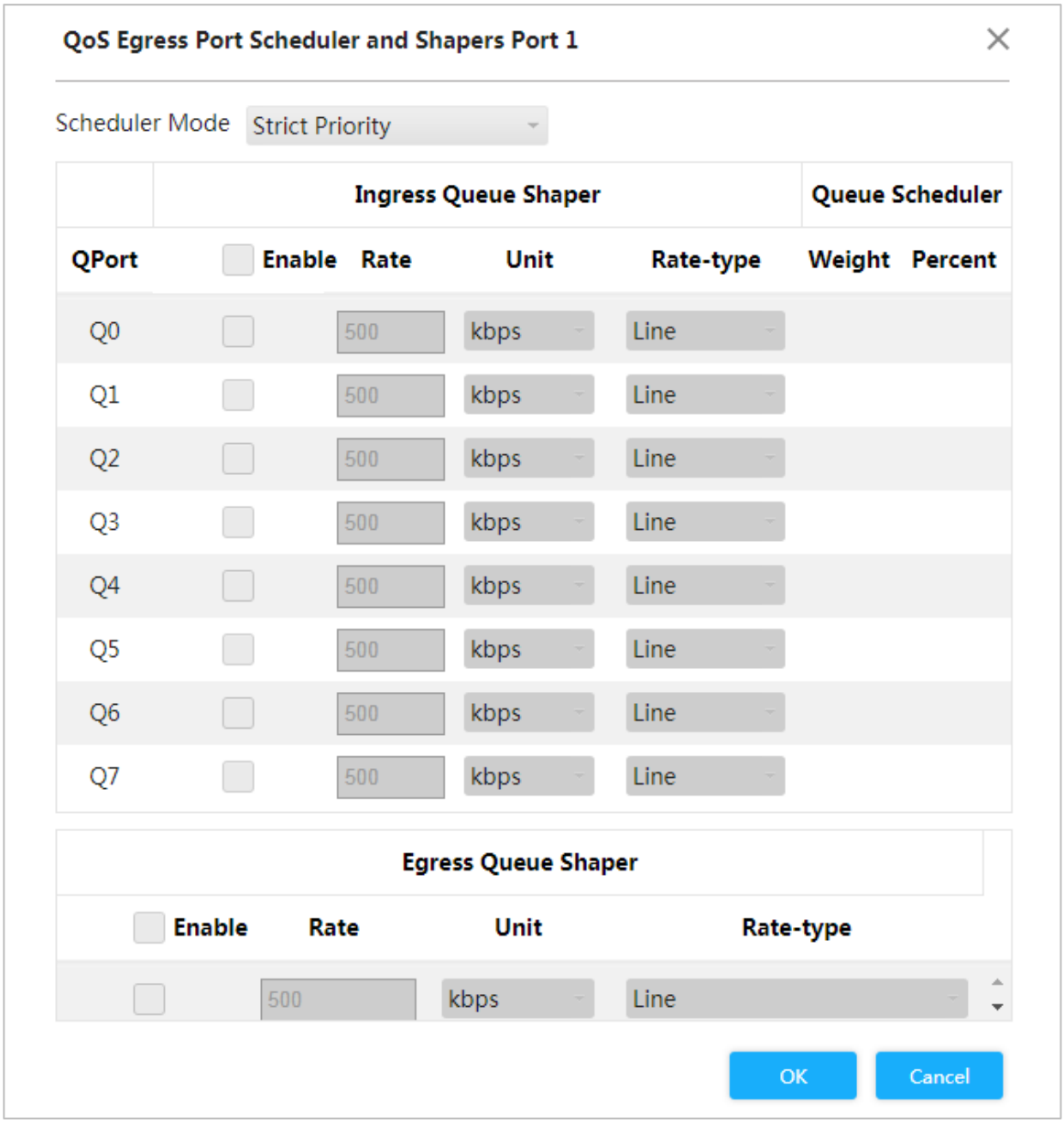
Figure 3-57 Port Schedulers



Step 2 Click the port. For example, port 1.

The **QoS Egress Port Schedulers and Sharpers Port 1** dialog box is prompted. See Figure 3-58. The CoS of Q0 is 0., and so on.

Figure 3-58 Port configuration



Step 3 Select mode.

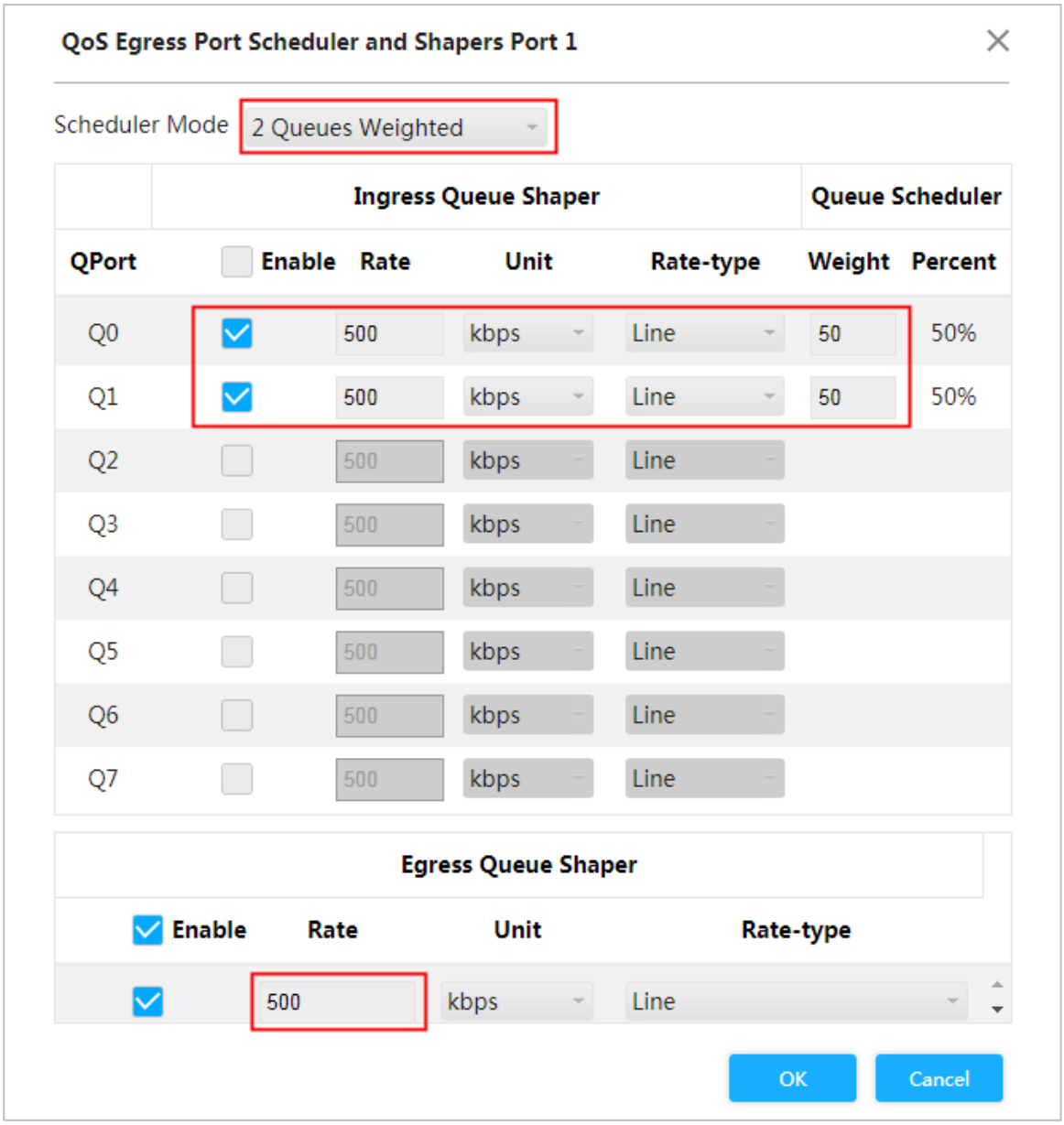
- **Strict Priority**. The priority for packet passing egress port of switch is decided according to the Cos value in **Port Classification**.
- **2~8 Queues Weighted**. When congestion occurs, the priority for packet passing egress port of switch is decided according to the proportion of total rate.

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) For example: select **Scheduler Mode** as **2 Queues Weighted**. See Figure 3-59.
2) In **Ingress Queue Shaper**, set the Rate of Q0 and Q1 to be 500 kbps, Weight to be 50, 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 3-59 Port Schedulers



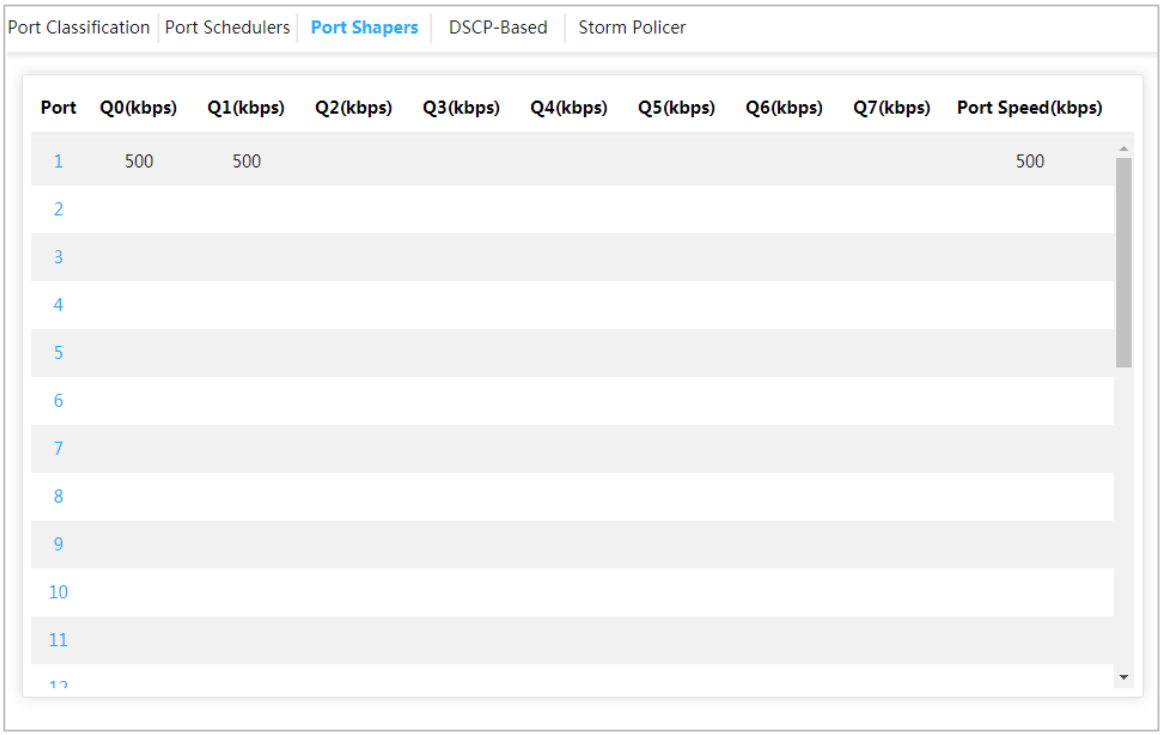
Step 4 Click **OK**.

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 3-60.

Figure 3-60 Port Shapers



3.2.6.4 DSCP-Based

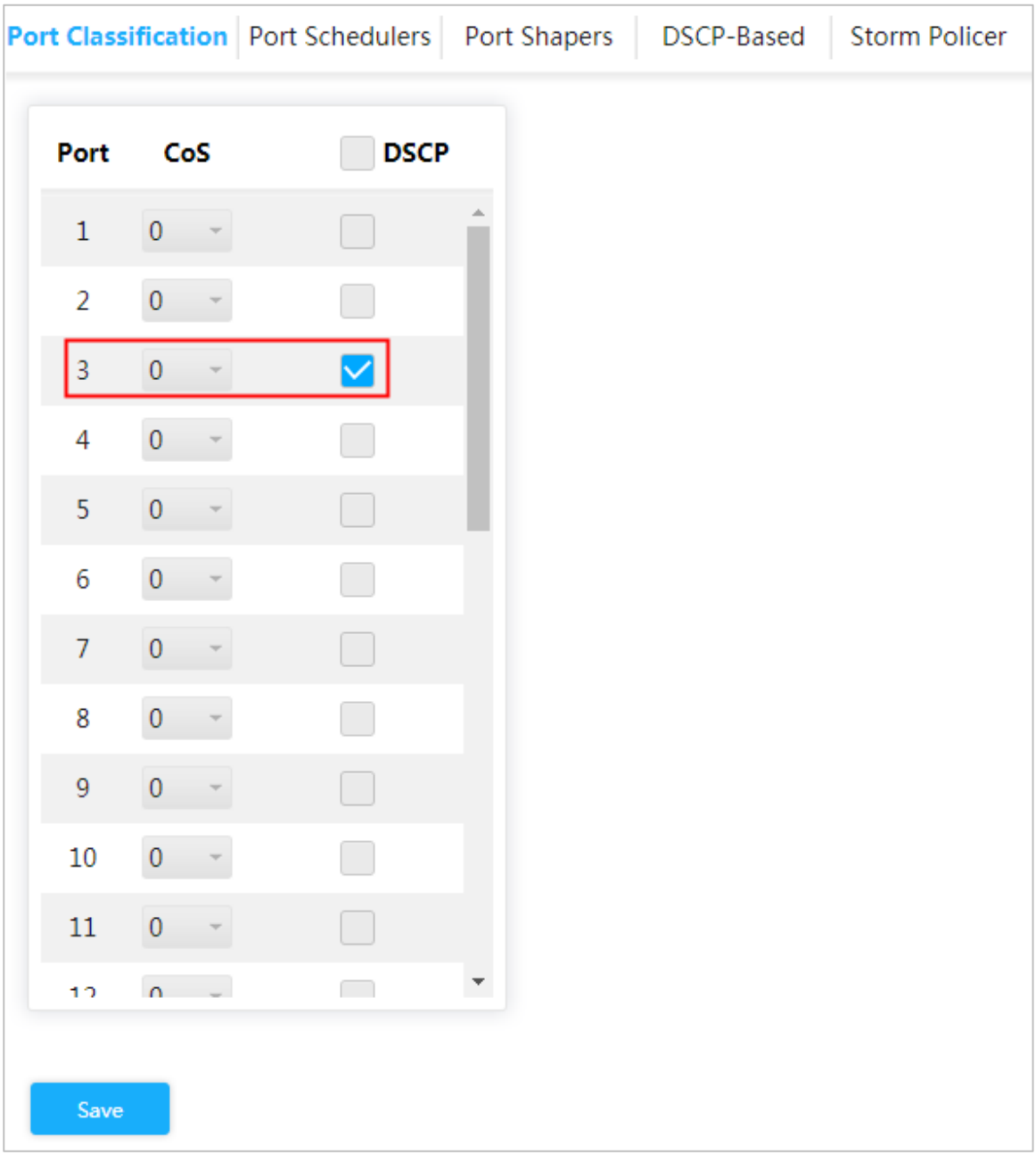
Ensure to enable DSCP before configuring DSCP-Based function.

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

The **Port Schedulers** interface is displayed.See .

Step 2 Enable DSCP at DSCP port. Suppose port 3 is the egress port, see Figure 3-61.

Figure 3-61 Port classification



Step 3 Click **Save.**

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

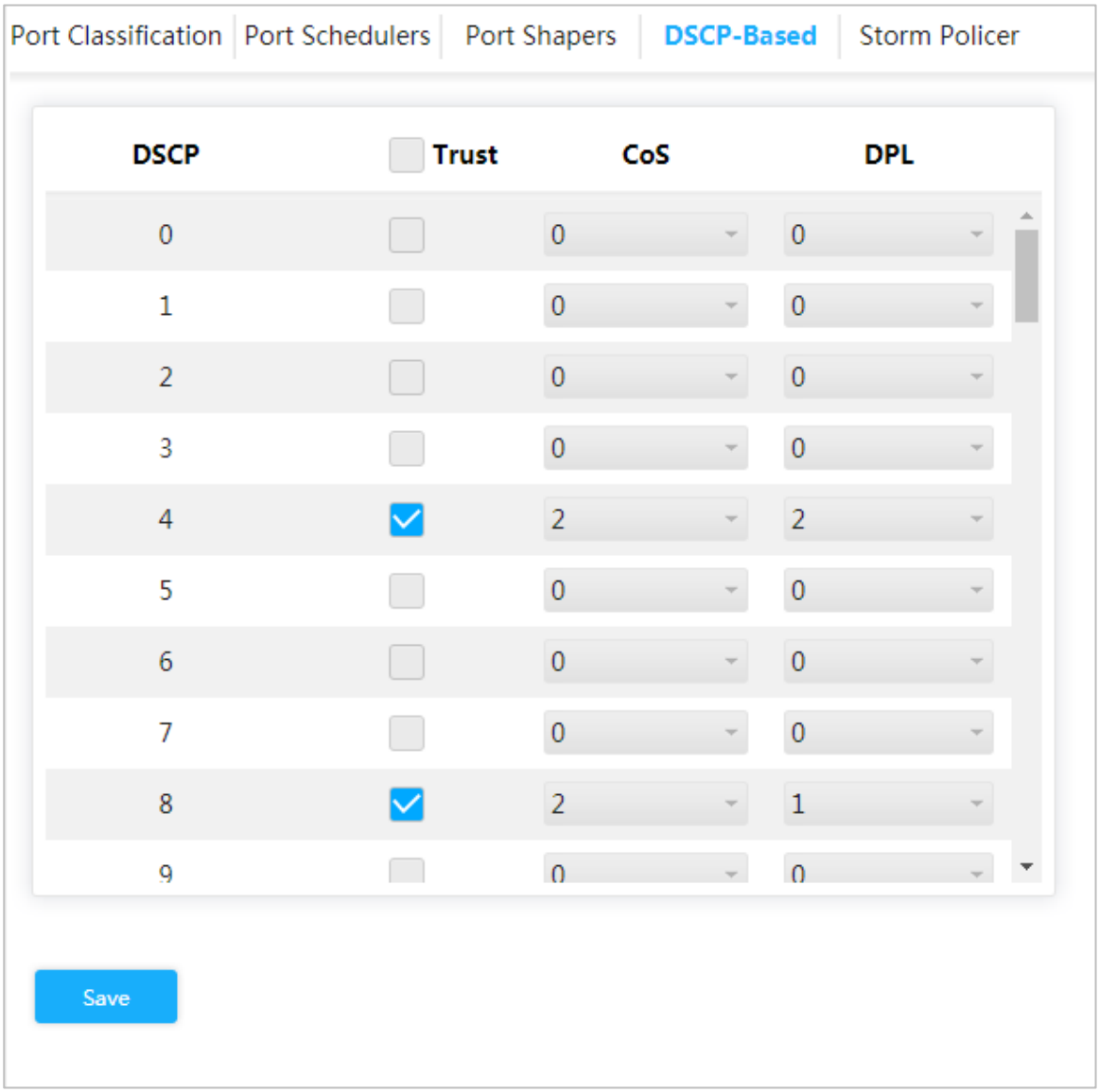
The **DSCP-Based** interface is displayed.

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 3-62.
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 is. When the CoS is the same, the larger DPL, the higher the priority is. The corresponding port packet will pass the egress port first.

Figure 3-62 DSCP-Based



Step 6 Click **Save.**

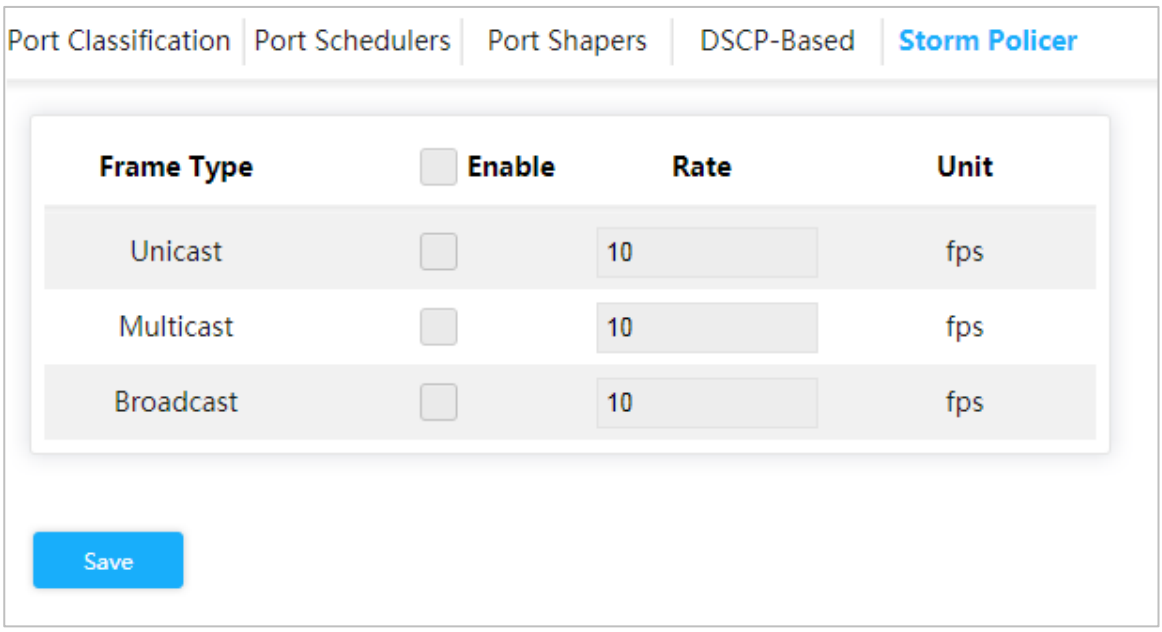
3.2.6.5 Storm Policer

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 3-63.

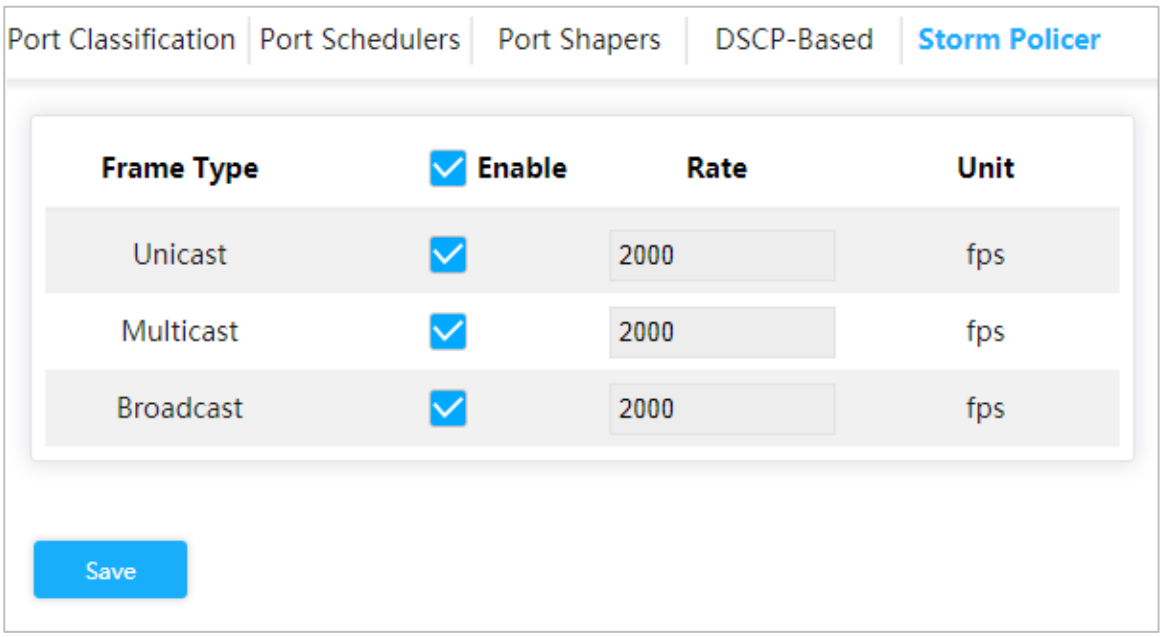
Figure 3-63 Storm Policer



Step 2 The port can receive the rate up to 2000 fps. See Figure 3-64.

- In **Unicast**, check the box **Enable**, and enter 2000 in **Rate**. It means that the port can receive the rate up to 2000 fps of unicast packet.
- In **Multicast**, check the box **Enable**, and enter 2000 in **Rate**. It means that the port can receive the rate up to 2000 fps of Multicast packet.
- In **Broadcast**, check the box **Enable**, and enter 2000 in **Rate**. It means that the port can receive the rate up to 2000 fps of broadcast packet.

Figure 3-64 Storm policer configuration



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 element, NMS and Agent.

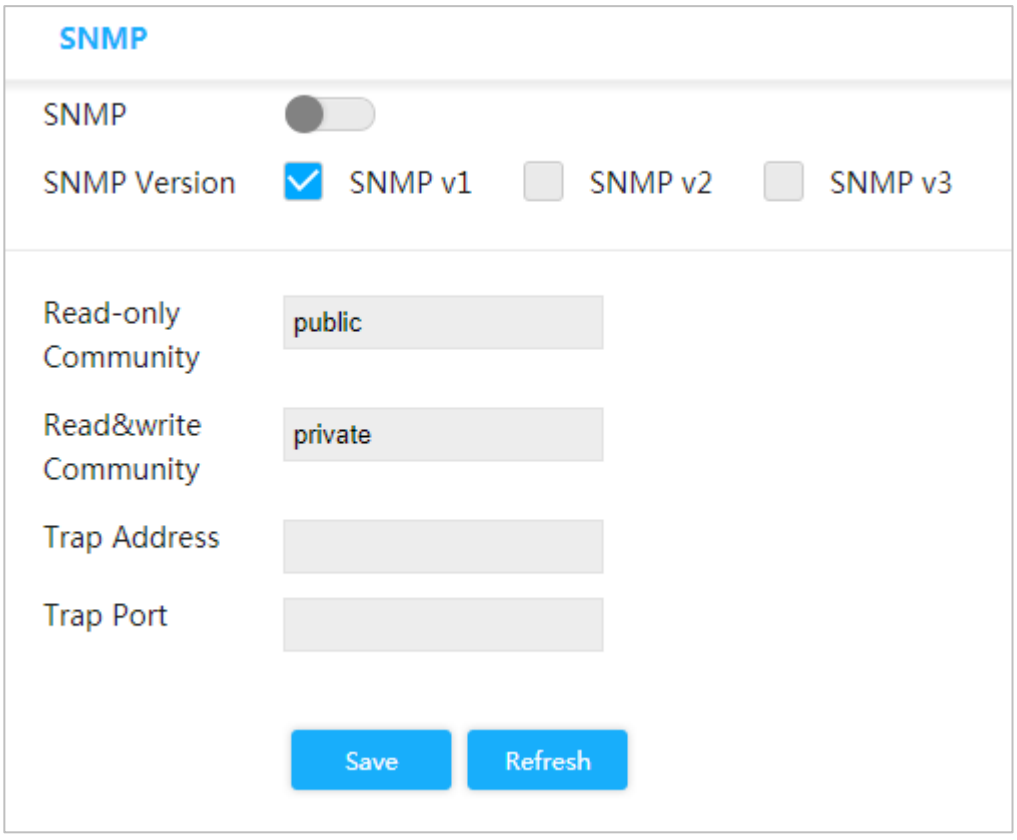
- NMS (Network Management System) is the manager in SNMP network, and it provides friendly human-machine interface, to help the network administrator to finish most of the network management work.
- Agent is the manged role in SNMP network, and it receives and handles the request packet from NMS. In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

3.2.7.1 Enable SNMP Function

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

The **SNM** interface is displayed.See Figure 3-65.

Figure 3-65 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: Configuring SNMP v1. The configuration of SNMP v2 is the same with that of SNMP v1.

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

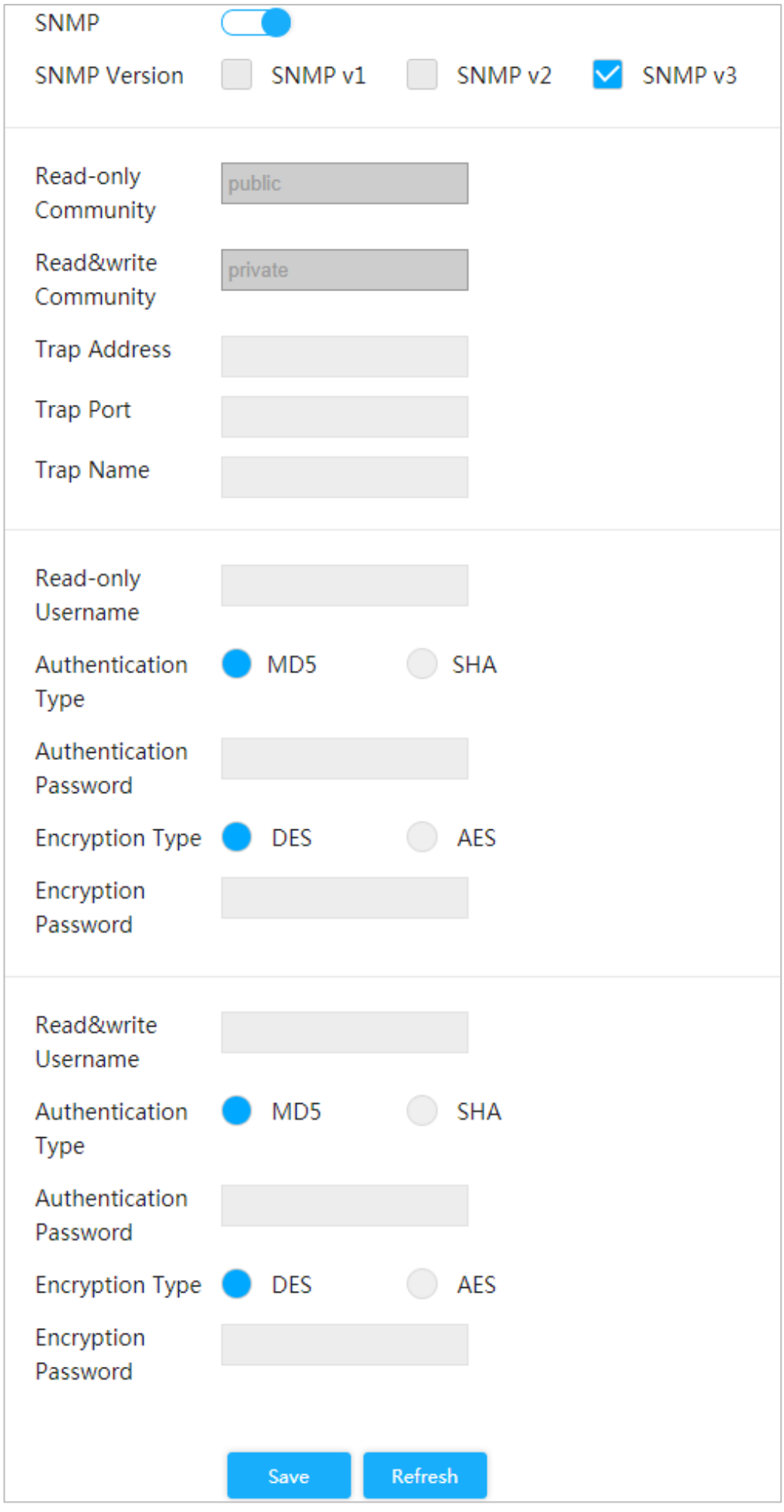
Step 2 Set **Read-only Community**, **Read&write Community**, **Trap Address** and **Trap Port.**

Step 3 Click **Save.**

3.2.7.3 Configuring SNMP v3

Step 1 Select **SNMP v3** in **SNMP Version**,. See Figure 3-66.

Figure 3-66 SNMP



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

3.2.8.1 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.

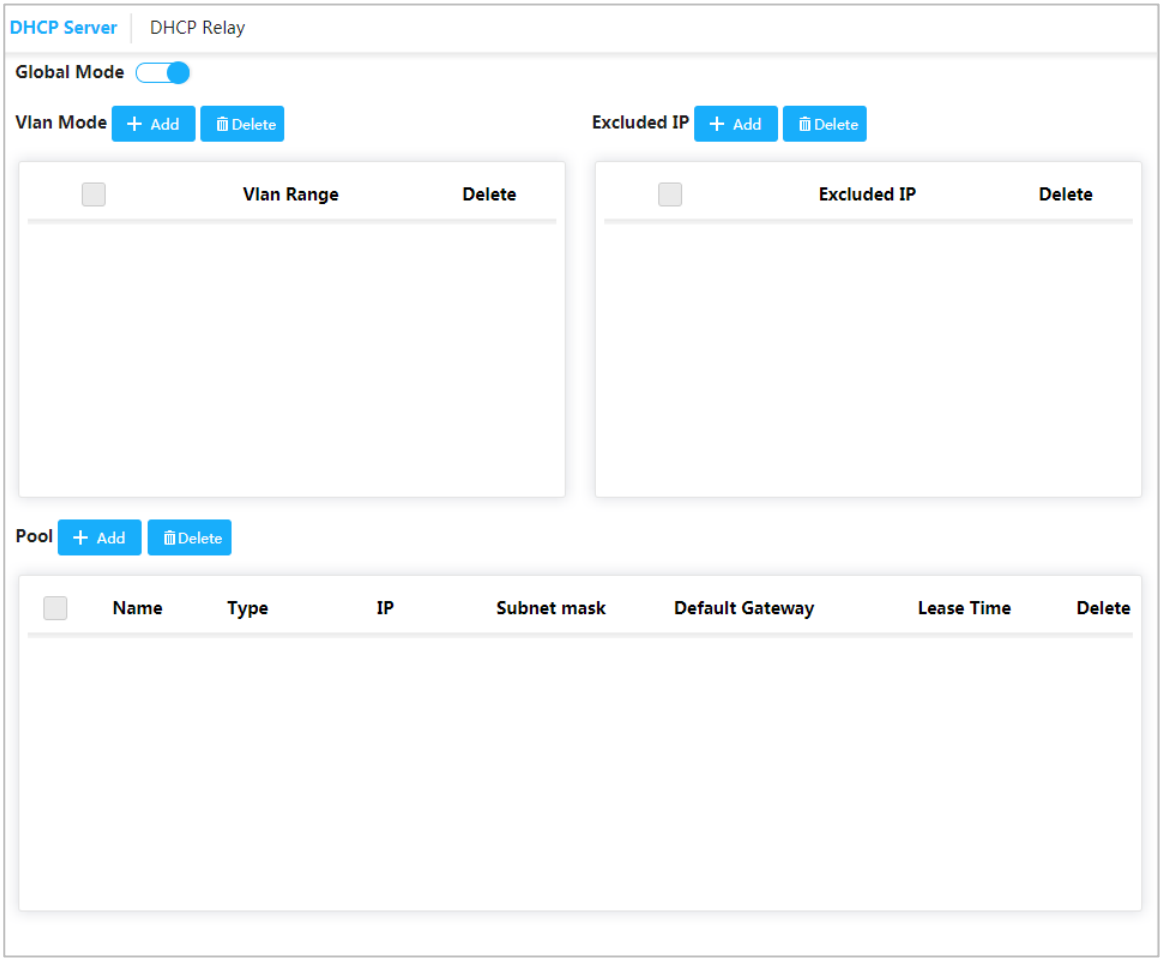
- The network scale is large.The workload is too heavy if manually configured, and centralized management for network will be difficult.
- The quantity of PC is larger than the quantity of IP address in the network, and it is impossible to allocate a static IP address for every PC. For example, the user 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 3-67.

Figure 3-67 DHCP server



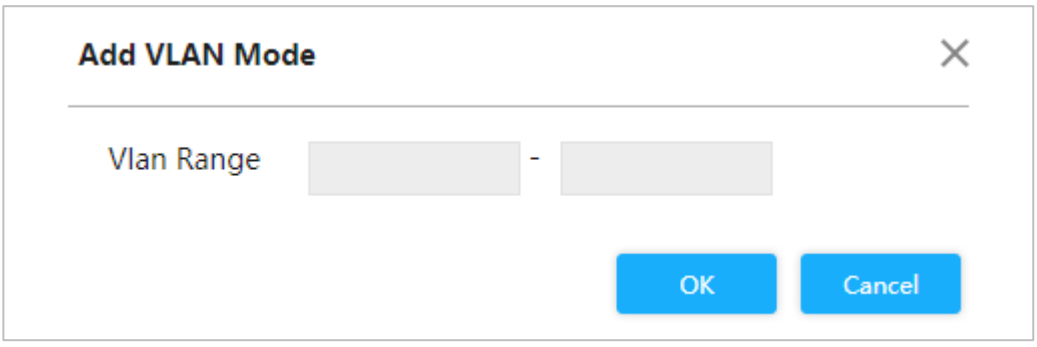
Step 2 Click  in **Global Mode**, to enable DHCP Server function.

Step 3 Configuring DHCP mode

1) Click **Add** in Vlan Mode

The **Add VLAN Mode** dialog box is prompted. See Figure 3-68.

Figure 3-68 Add VLAN Mode



2) Enter the VLAN range. For example, 2-4.

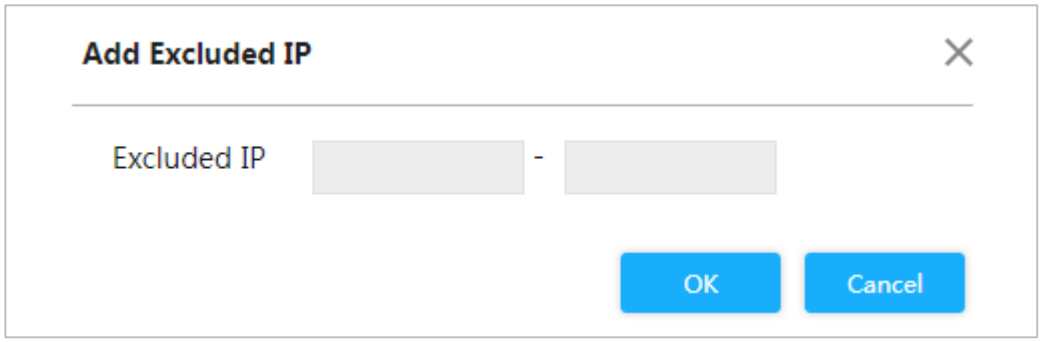
3) Click **OK**.

Step 4 Configuring network segment of IP address.

1) Click add in Excluded IP.

The **Add Excluded IP** dialog box is prompted. See Figure 3-69.

Figure 3-69 Add Excluded IP



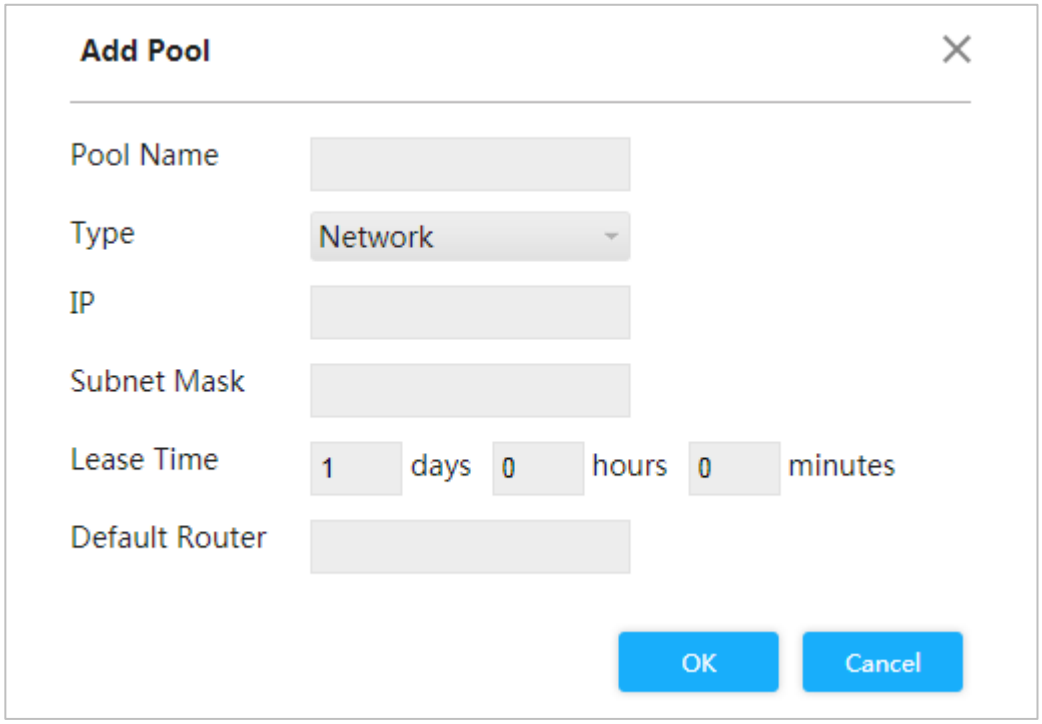
2) Enter the IP address range. For example, 192.168.100.2-192.168.100.50.
3) Click **OK**.

Step 5 Adding DHCP address pool.

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

The **Add Pool** dialog box is prompted. See Figure 3-70.

Figure 3-70 Add pool



5) For the parameters. See Table 3-7

Table 3-7 Pool parameters.

Parameters	Description
Pool Name	DHCP address pool name. For example: vlan2_test.
Type	Two types: Network and host. ● 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.
Default Router	The default gateway for configuring the address pool.

6) Click **OK**.

3.2.8.2 DHCP Relay

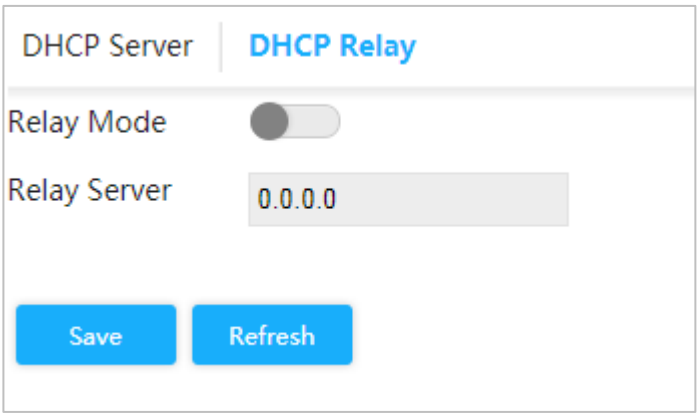
DHCP is only applicable when the client and server in the same sub network since the request packet is sent by broadcast when dynamically acquiring the IP. It is not economic to set a DHCP server in every net segment for dynamic host configuration.

The introduction of DHCP relay solves this problem: Client can get the IP address through the communication between DHCP relay and DHCP servers on the other net segments. In this way, DHCP clients in different segments can use the same DHCP server, which is economic and also convenient for centralized management.

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

The **DHCP Relay** interface is displayed.See Figure 3-71.

Figure 3-71 DHCP Relay



Step 2 Click  in **Relay Mode** to enable **DHCP Relay** function**.**

Step 3 Set the IP address of **Relay Server**

Step 4 Click **Save.**

3.2.9 LLDP

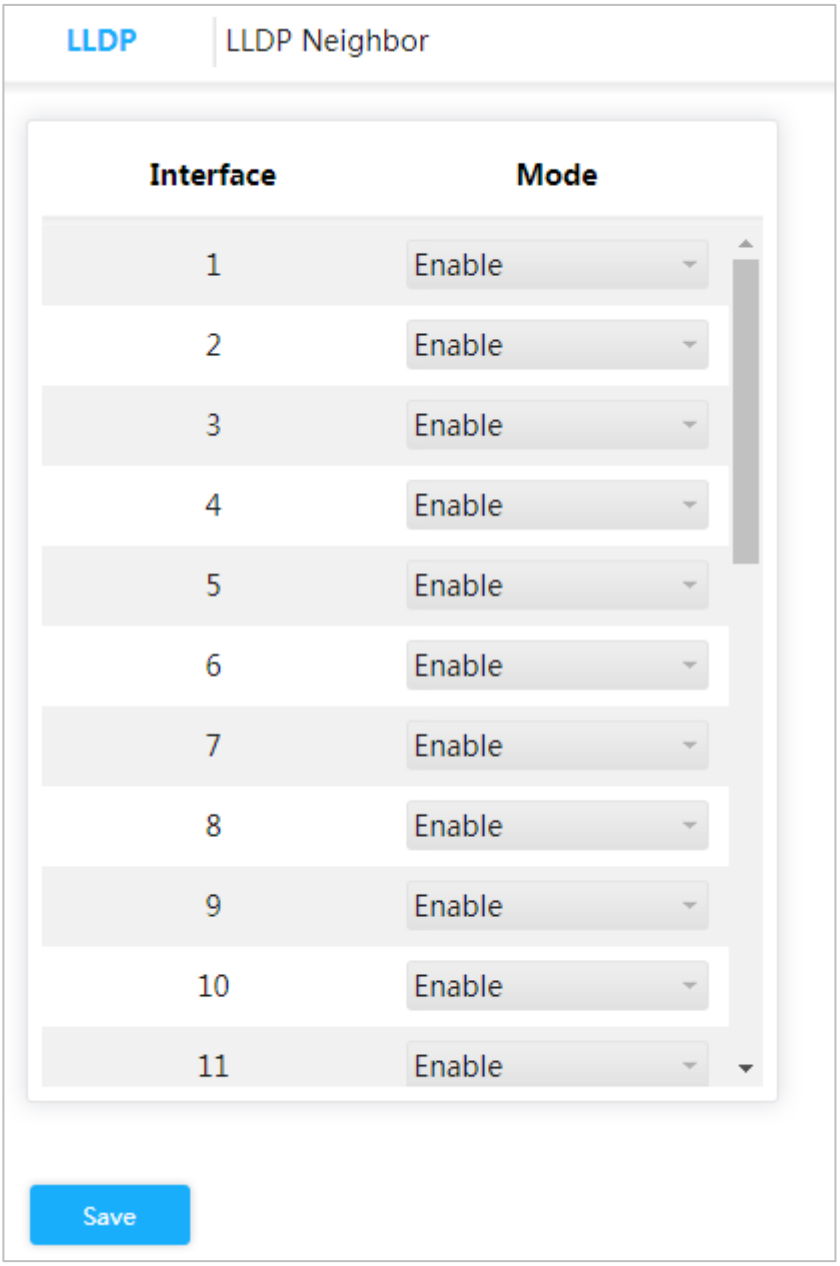
LLDP (Link Layer Discovery Protocol) is a standard link layer discovery way. It can form its main capabilities, management address, device no and port no as TLV (Type Length Value), encapsulate it in LLDPDU (Link Layer Discovery Protocol Data Unit), and advertises it to its neighour. The neighour will 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 > Configuration > LLDP**.

The **LLDP Configuration** interface is displayed. See Figure 3-72.

Figure 3-72 LLDP



Step 2 Set LLDP mode

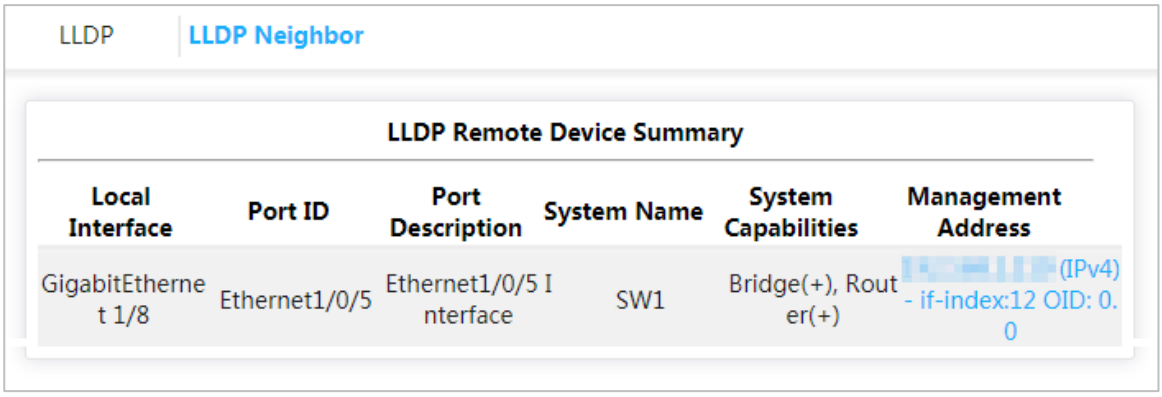
- Select **Enable**: Both send and receive LLDP packet.
- Select **Disable**:: Neither send nor receive LLDP packet.
- Select **Rx only**: Only receive LLDP packet.
- Select **Tx only**: Only send LLDP packet.

Step 3 Click **Save.**

View the LLDP Neighbor Information.

Select **Advanced > Seldom-used > DHCP > DHCP Relay > LLDP Neighbor**.The **LLDP Neighbor** interface is displayed. See Figure 3-73.

Figure 3-73 LLDP neighbor



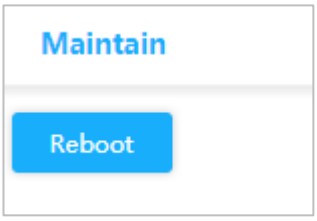
4 Maintenance

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 is prompted.

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

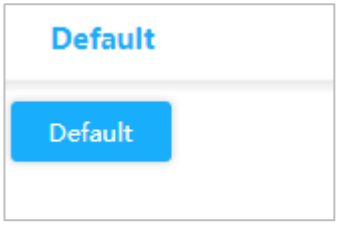
4.2 Restore Default

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

Step 1 elect **Advanced > Maintain > 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.

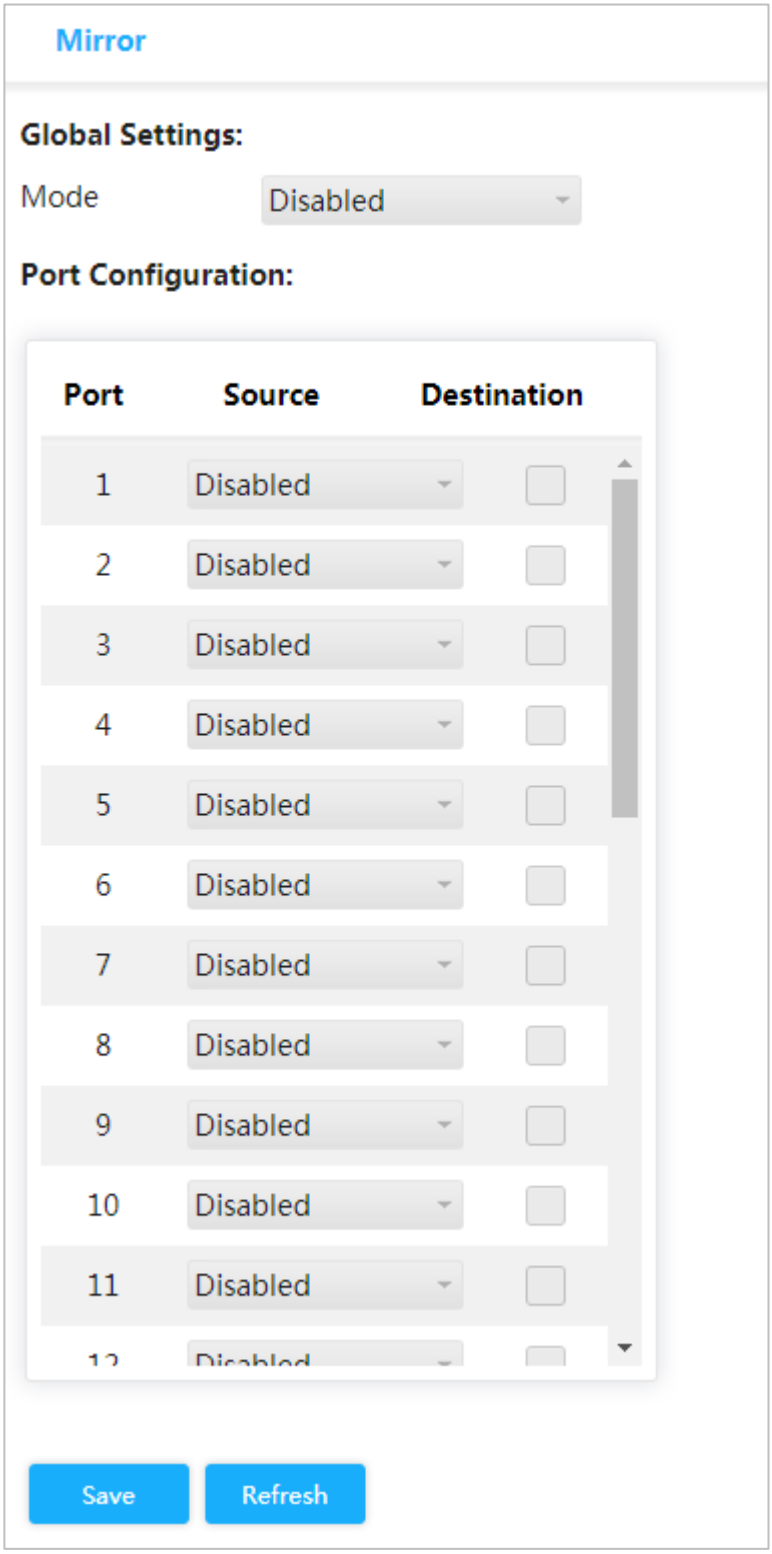
4.3 Mirror

Port mirror is also called port monitor. Port monitor 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 mirror 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 4-3.

Figure 4-3 Mirror



Step 2 In **Global Settings**, select **Enabled** for the 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.

- Check the box **Destination** to set the port to be destination.

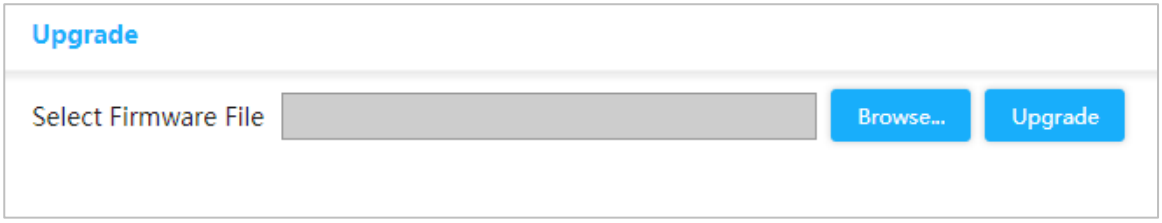
Step 4 Click **Save.**

4.4 Software Update

Step 1 Select **Maintain > Common > Software Update.**

The **Upgrade** interface is displayed.See Figure 4-4.

Figure 4-4 Upgrade



Step 2 Click **Browse...,** and select the file in .mif format.

Step 3 Click **Upgrade**.

The device reboots after the upgrade finished. Login the switch again, and all configuration will not be changed.

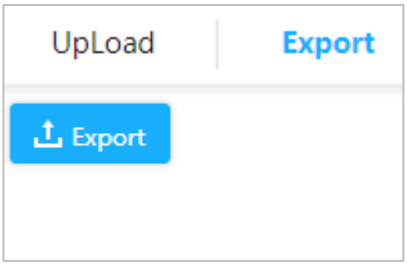
4.5 Config Manage

4.5.1 Export

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

The **Export** interface is displayed. See Figure 4-5.

Figure 4-5 Export



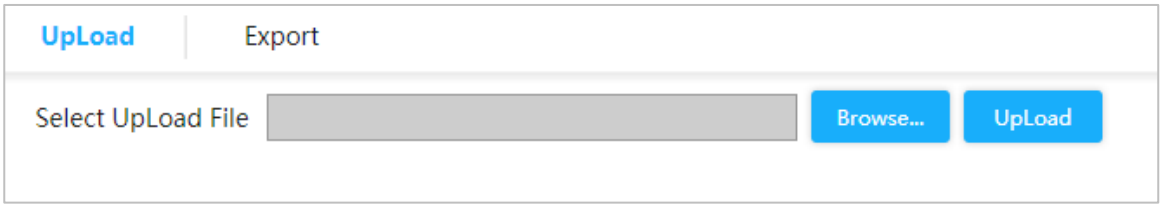
Step 2 Click **Export** to export the configuration file.

4.5.2 Upload

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

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

Figure 4-6 Upload



Step 2 Click **Broswe...**, and select the configuration file to be uploaded.

Step 3 Click **UpLoad to** upload the configuration file.

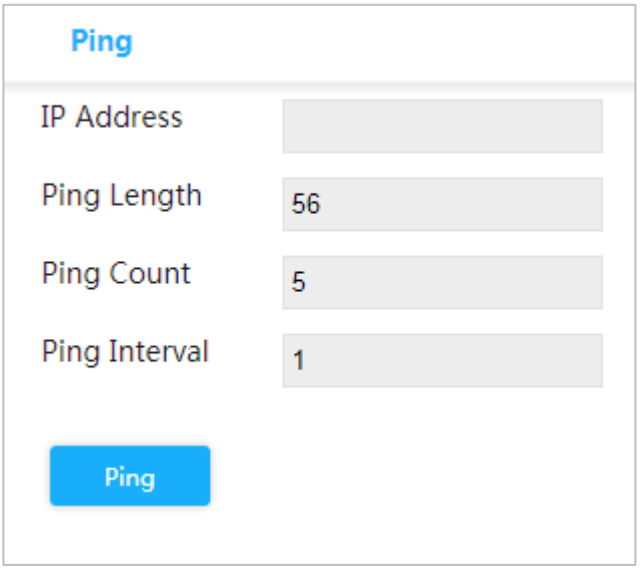
4.6 Ping

With Ping protocol, you can check whether the device with a specified IP address can be accessed, or you can check whether there is a network connection failure.

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

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

Figure 4-7 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