Ruijie XS-S1960-H Series Switches

Web-Based Configuration Guide, Release 11.4(1)B12P17

Copyright Statement

Exemption Statement

Preface

Thank you for using our products.

Audience

This manual is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Obtaining Technical Assistance

- Ruijie Networks Website: https://www.ruijienetworks.com/
- Technical Support Website: https://ruijienetworks.com/support
- Case Portal: http://caseportal.ruijienetworks.com
- Community: http://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijienetworks.com
- Skype: service_rj@ruijienetworks.com

Related Documents

Documents	Description
Command Reference	Describes the related configuration commands, including command modes, parameter descriptions, usage guides, and related examples.
Hardware Installation and Reference Guide	Describes the functional and physical features and provides the device installation steps, hardware troubleshooting, module technical specifications, and specifications and usage guidelines for cables and connectors.

Conventions

This manual uses the following conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Symbols

Means reader take note. Notes contain helpful suggestions or references.

Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

1 Web-based Configuration

1.1 Overview

Users access the Web management system (eWeb) of switches through a browser (for example Google Chrome) to manage the switches.

The eWeb consists of the Web server and Web client. The Web server is integrated into the switch and is used to receive and process requests from the client (reading Web files or executing commands), and return the processing results to the client. The Web client is usually a Web browser, such as Google Chrome.

This document applies only to XS-S19-H series switches.

1.2 Typical Application

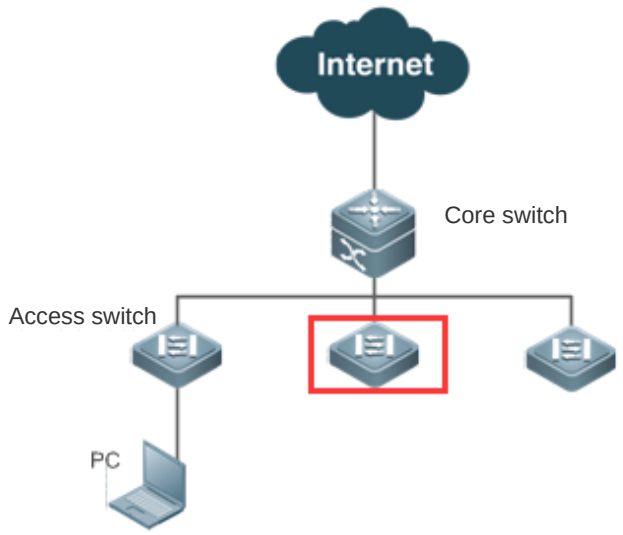
Typical Application	Description
Managing Devices via eWeb	After switches are configured, you can access the eWeb through a browser.

1.2.1 Managing Devices via eWeb

Scenario

As shown in Figure 1, you can access the eWeb of an access or aggregation switch through a browser to manage and configure the switch.

Figure 1



Remarks	The device enclosed in the red rectangle in the preceding figure is the accessed switch. If the switch can be pinged successfully from the PC, you can access the eWeb of the switch.

Deployment

Configuration Environment Requirements

Client requirements:

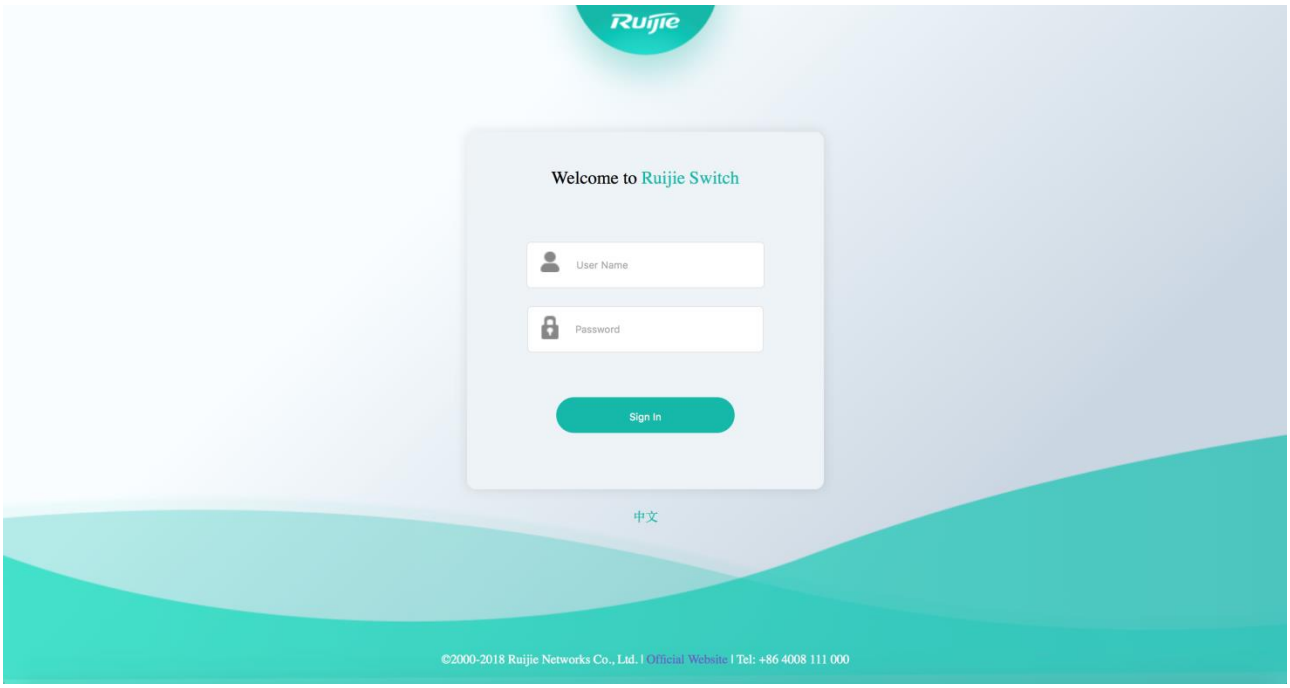
- The administrator can log in to the eWeb from the browser of the Web client to manage switches. Clients refer to PCs or other mobile terminals such as laptops.
- Browser: Google Chrome (recommended), Firefox, and Safari are supported. Exceptions such as garbles or format errors may occur if an unsupported browser is used.
- Resolution: It is recommended to set the resolution to 1024 x 768, 1280 x 1024, 1440 x 960, or 1920 x 1080. If other resolutions are used, the page fonts and formats may not be aligned and the UI is not artistic, or other exceptions may occur.

Web configuration and command line interface (CLI) configuration can be performed at the same time. After CLI configuration is complete, enter the write command to save the configuration. If a web page is opened, refresh the page to ensure synchronization between web and CLI configurations.

Logging In to the eWeb

Enter the switch's management IP address (http://192.168.1.200 by default) in the address bar of a browser and press **Enter** to open the login page. You can select Chinese or English on the login page.

Figure 2 Login Page



Specify the username and password and click **Sign In**. The following table describes the default username and password.

Default Username/Password	Permission Description
admin/admin	Super administrator with all permissions

After authentication is successful, the eWeb home page is displayed, as shown in Figure 3.

Figure 3 eWeb Home Page

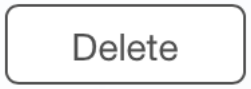
For details about eWeb pages, see section 1.3 "eWeb".

1.3 eWeb

Basic Concepts

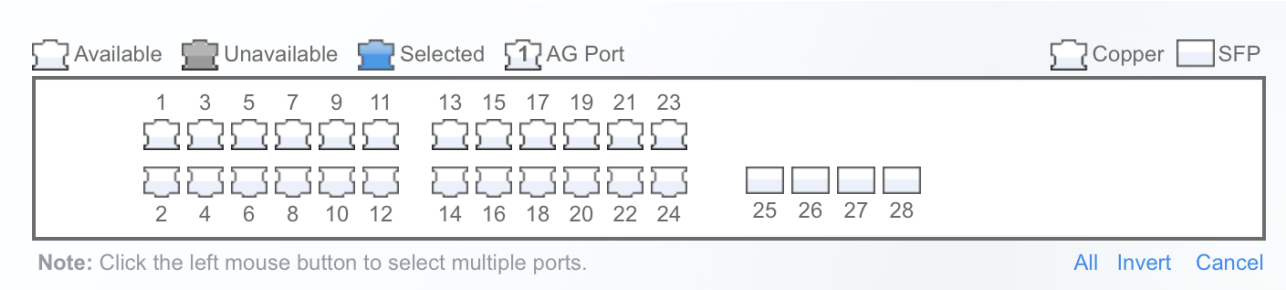
Icons and Buttons on Graphical User Interfaces (GUIs)

Icon/Key	Description
	Edit. After you click the icon, you can edit the selected record.
	Delete
	Function enabling/disabling icon
	Available port. After you click or select the icon for a port, the port status is changed to **Selected**.

	Unavailable port
	Selected port
	AG Port. The digit in the port indicates the aggregation port number.
	Trunk port, displayed on the panel of the VLAN settings page
	Save button, for submitting and saving input information
	For adding settings
	For deleting settings
	Panel port batch processing buttons, in the lower right corner of the panel Note: These buttons are available only on panels where multiple ports can be selected.
*	Mandatory item. If an input box carries this symbol, the item is mandatory.

System Operations

- Port panel



- Port panel operation

Click the port icon on the panel or drag the mouse to select multiple ports to change the port status from **Available** to **Selected**. Then, set selected ports, for example, add port description, port mirroring, and port rate limit.

Feature

The following table describes feature configurations of the first-level and second-level menus in the left navigation tree of the eWeb.

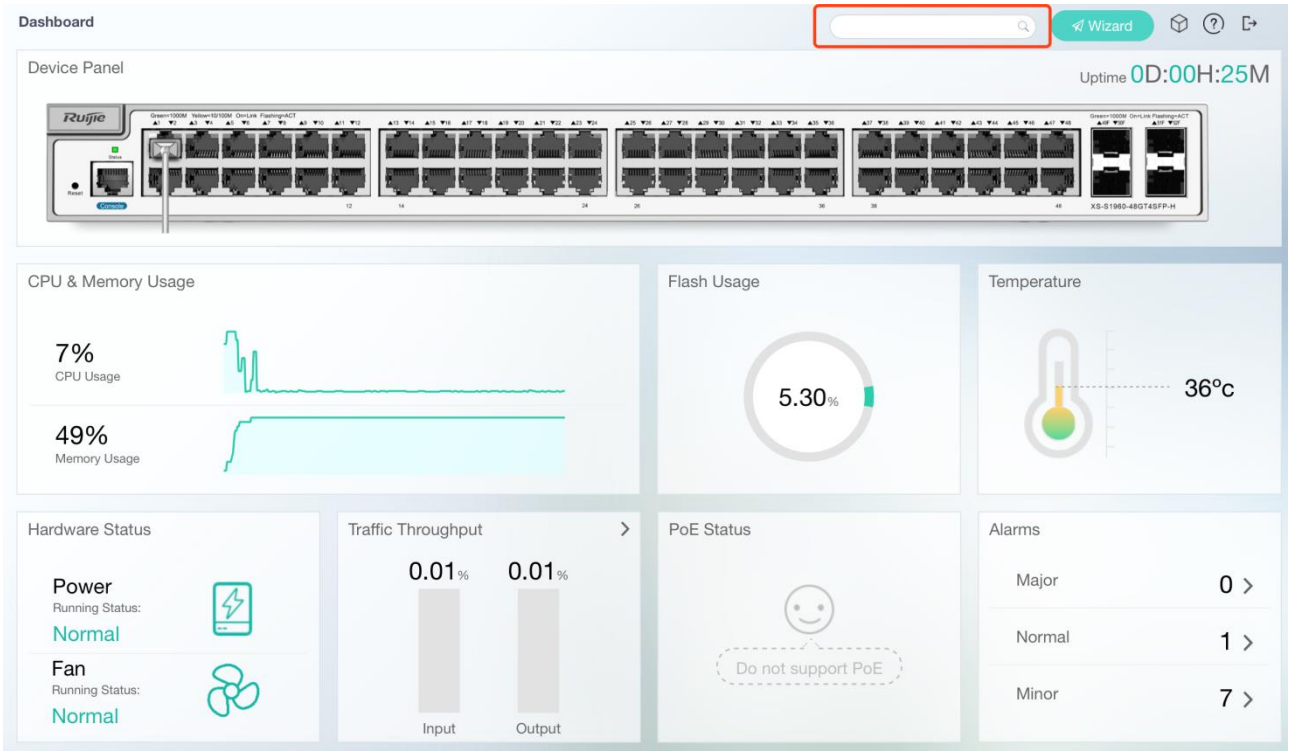
Feature	Description
Search	Allows keyword-based global searches, to enter the configuration page of a function quickly.
Help	Provides five technical service modes, including Skype, email, and official website.
Language	Supports switching between Chinese and English.
Wizard	Supports simple configuration through the configuration wizard.

Dashboard	Displays port information and overall device running status.
Port	Sets basic port information, port aggregation, port mirroring, port rate limit, and storm suppression.
VLAN	Sets virtual local area networks (VLANs), trunk ports, and IP addresses.
Diagnosis	Performs the ping, traceroute, or cable detection operations.
MAC Address	Sets the static and filtering addresses.
Routing	Sets routes.
ARP Entry	Sets Address Resolution Protocol (ARP) entries.
DHCP Server	Allocates Dynamic Host Configuration Protocol (DHCP) and static addresses, and sets the client list.
DHCP Relay	Sets the DHCP relay.
ACL & QoS	Sets the time range, access control list (ACL), ACL application, classification, policy, and stream.
STP & RLDP	Sets the global basic information of Spanning Tree Protocol (STP), STP ports, and RLDP.
NFPP	Displays content related to NFPP guard.
Port Protection	Sets port protection.
Port Security	Sets basic port security information and security binding.
IP Source Guard	Sets ports and user binding.
Anti ARP Spoofing	Sets gateway ARP spoofing, ARP check, and dynamic ARP inspection (DAI).
IGMP Snooping	Sets Internet Group Management Protocol (IGMP) snooping.
DHCP Snooping	Sets DHCP snooping.
PoE	Sets global power over Ethernet (PoE) and content related to port PoE.
DNS	Sets static domain name server (DNS).
Service	Sets Web, Telnet, Secure Shell (SSH), and Simple Network Management Protocol (SNMP) services.
System Log	Sets the log server and queries system logs.
Time & NTP	Sets the system time, Network Time Protocol (NTP) key, and NTP server.
System Restart	Restarts the device.
Restore to Default	Restores to the factory settings.
Backup	Backs up the current configurations.
System Upgrade	Performs local upgrade and web package online upgrade.

1.3.1 Search

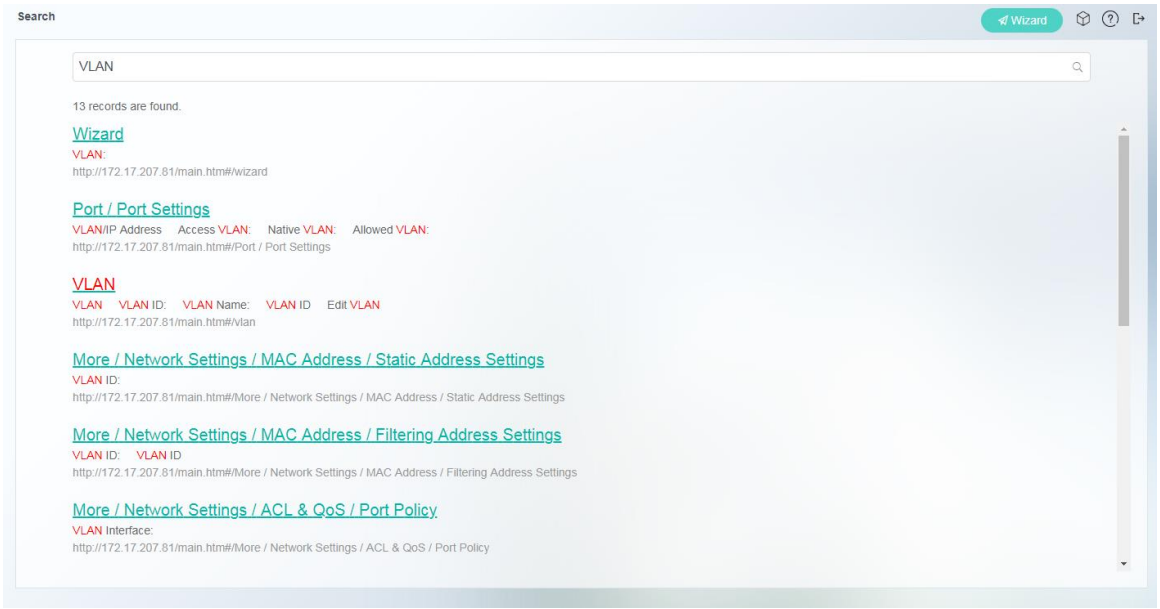
The Search box is always displayed in the upper right corner of the eWeb home page, as shown in Figure 4.

Figure 4 Search Box



Enter the keyword to be searched in the Search box and press **Enter** or click the search icon. The search results are displayed, as shown in Figure 5.

Figure 5 Search Results



Click a title or link in the search results to enter the configuration page of the corresponding function.

1.3.2 Help

The Help icon is always displayed in the upper right corner of the eWeb home page, and five technical service modes are provided. After you click the Help icon, the following five technical service modes are displayed:

1. Live Chat (with the Skype icon)

After you click **Live Chat**, the online Skype chat window is displayed.

2. Mail-to (with the Mail-to icon)

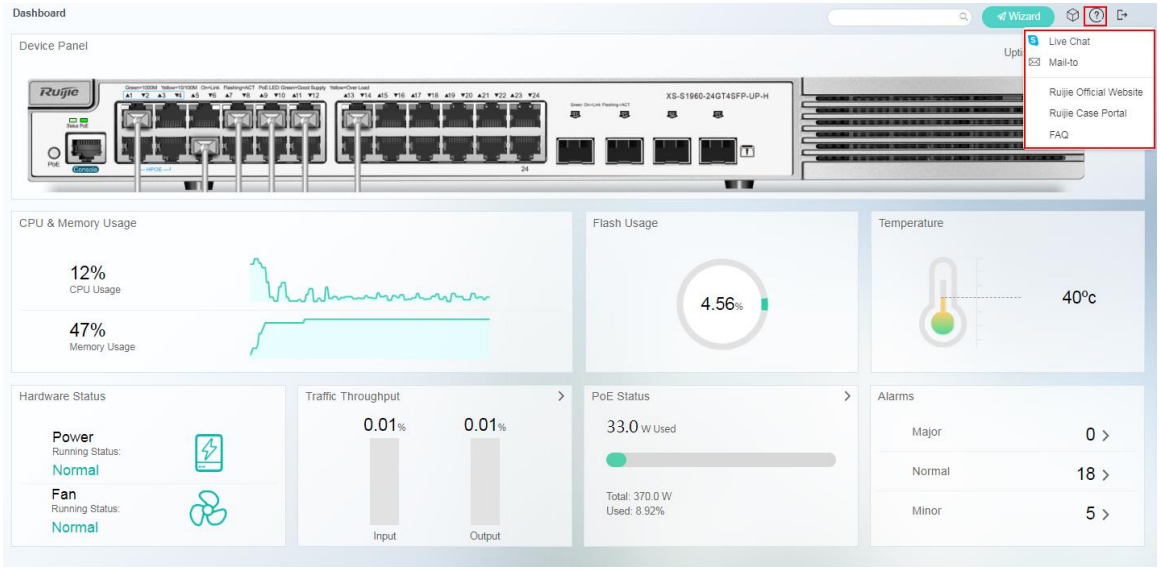
After you click **Mail-to**, the Mail-to window of the eWeb is displayed.

3. Ruijie Official Website (http://ruijienetworks.com/)

4. Ruijie Case Portal (http://caseportal.ruijienetworks.com)

5. FAQ (http:// community.ruijienetworks.com)

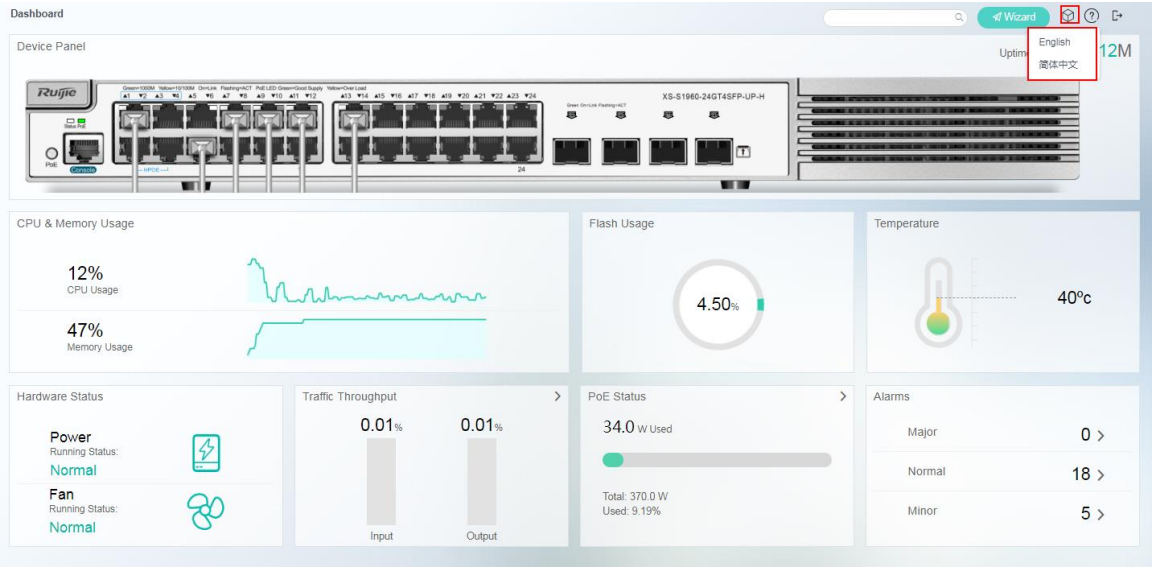
Figure 6 Help



1.3.3 Language

The Language icon is always displayed in the upper right corner of the eWeb home page. Switching between Chinese and English is supported. You can select either language on the eWeb home page or the login page.

Figure 7 Language



1.3.4 Wizard

The Wizard icon is always displayed in the upper right corner of the eWeb home page. When you use the eWeb for the first time, a welcome page is displayed. Click **Yes** and configure **Password**, **Management IP**, **Device Location**, **Remote Control**, and **Cloud Management** in sequence on the **Config Wizard** page. The **Complete** page displays configured information. Finally, click **Finish**.

Figure 8 Welcome

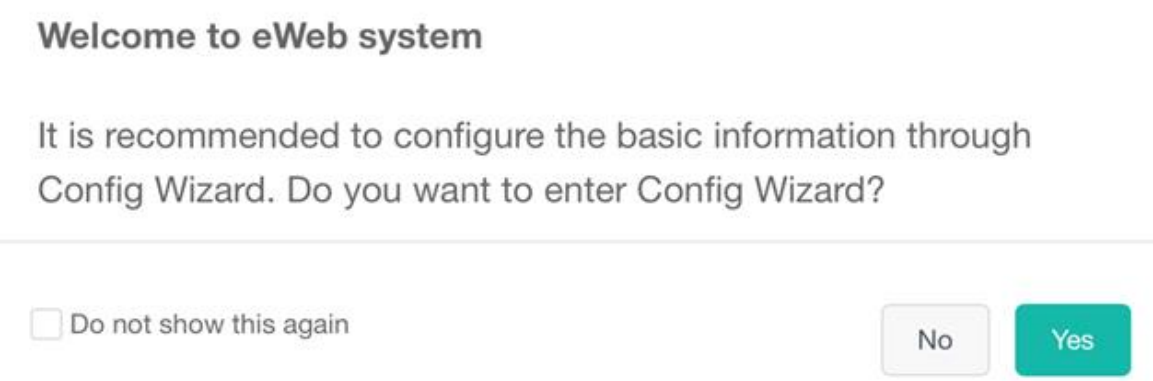


Figure 9 Password

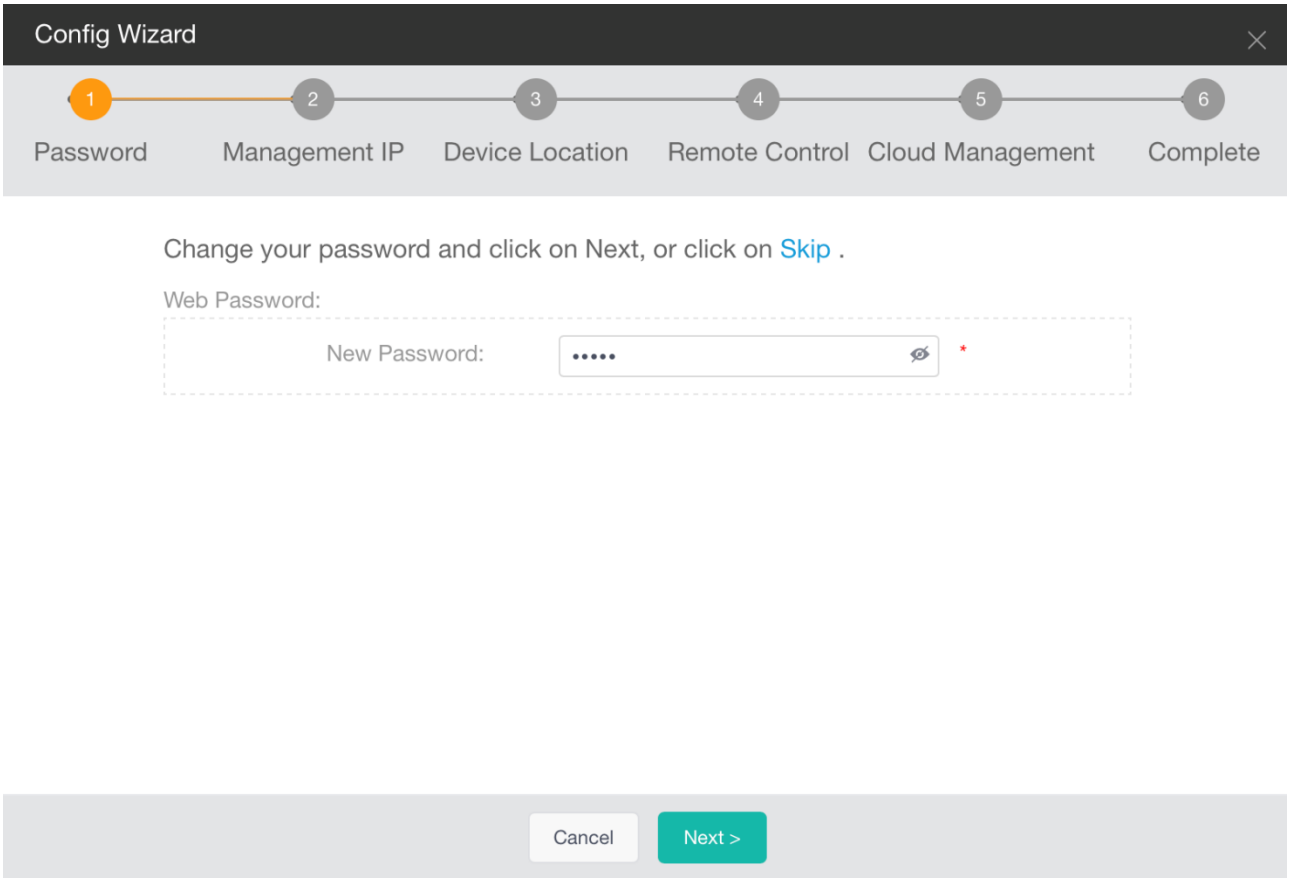
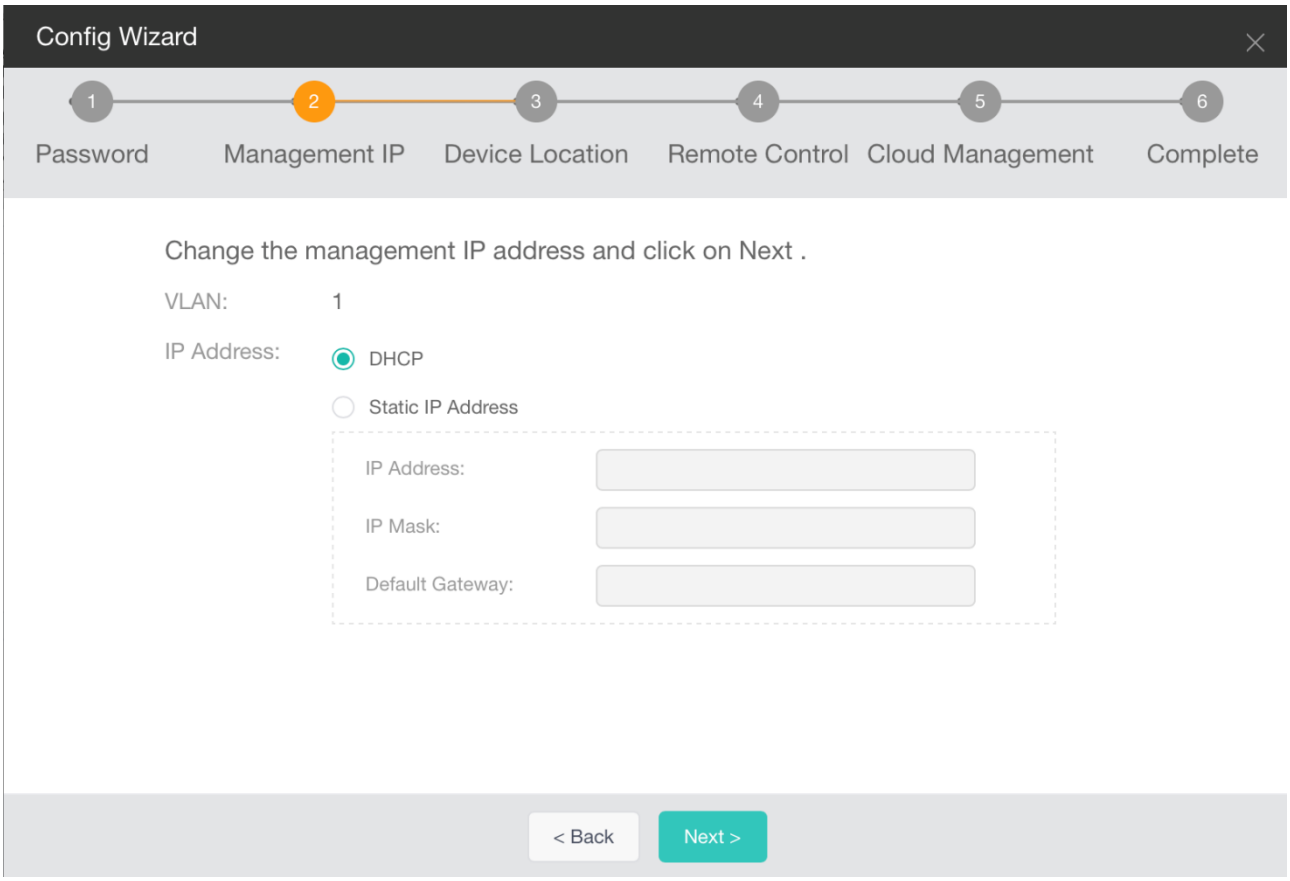


Figure 10 Management IP



You can select **DHCP** for **IP Address** to obtain a dynamic IP address or configure a static management IP address.

After you change **Static IP Address** to **DHCP** and click **Next**, the following information is displayed, prompting you to log in to the device over a serial port to obtain the new IP address. After you click **OK**, the **Device Location** page is displayed.

Figure 11 Prompt

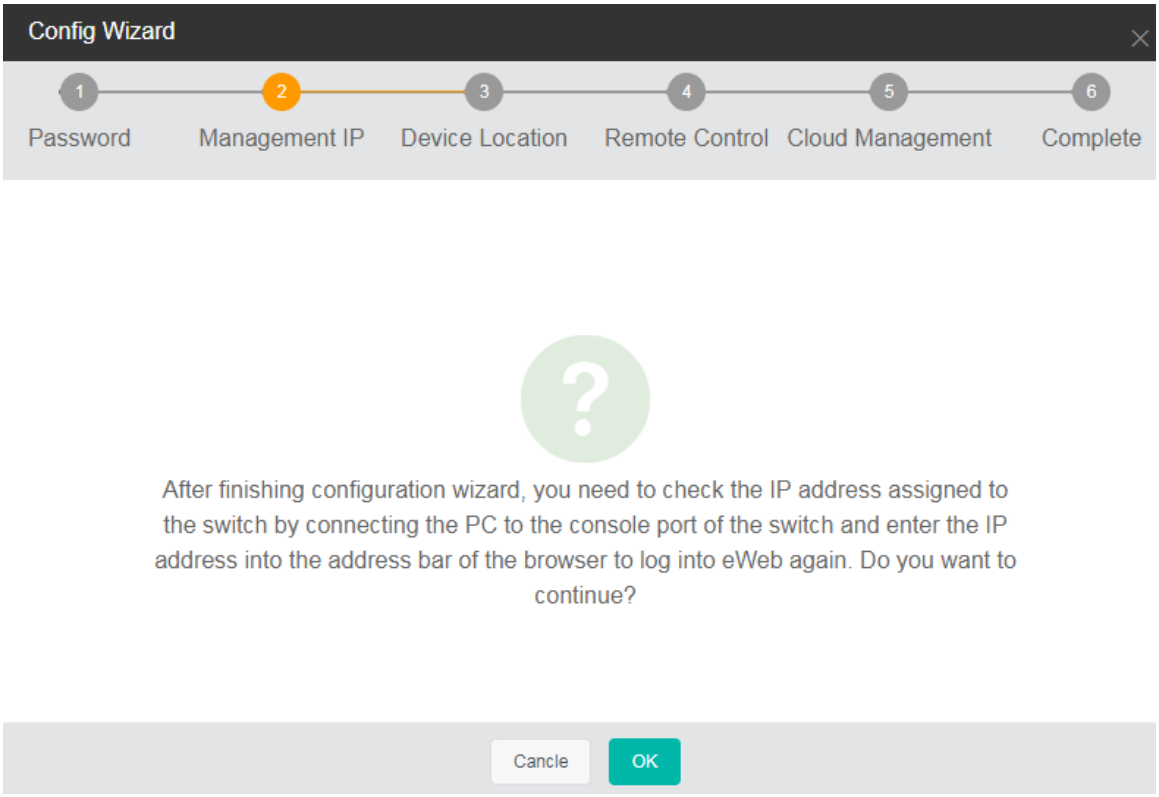


Figure 12 Device Location

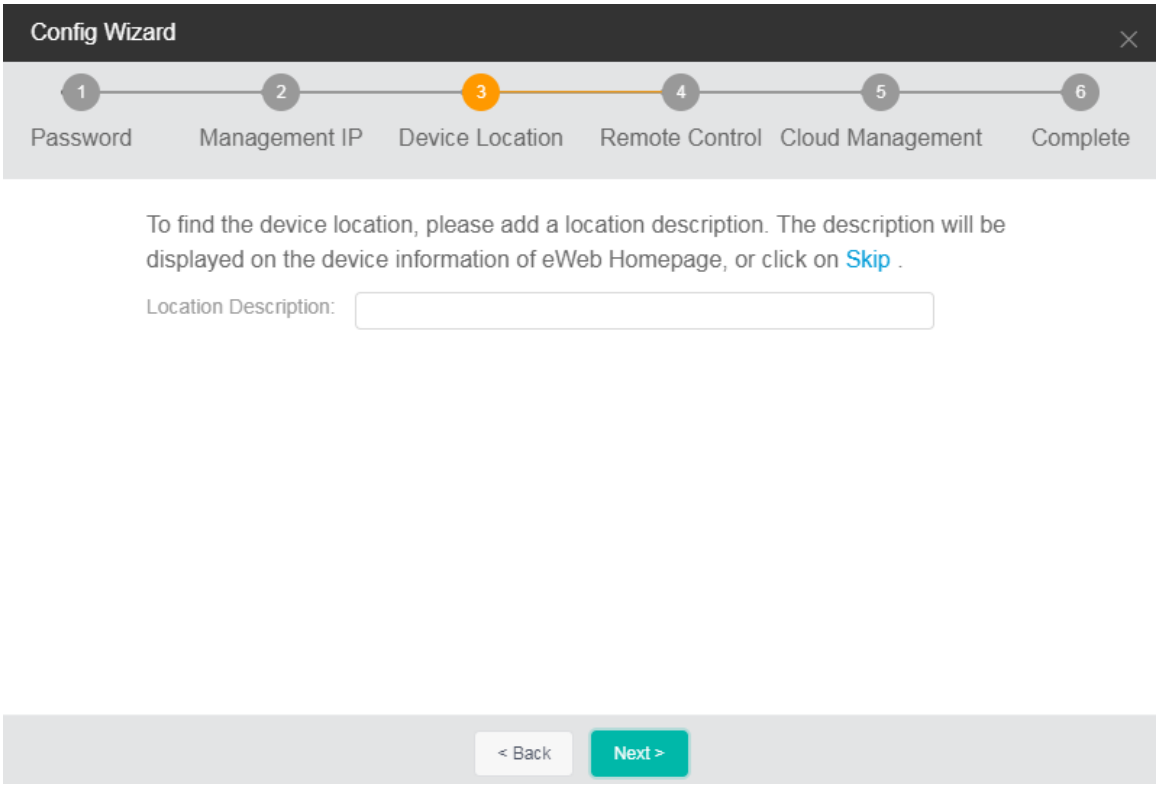
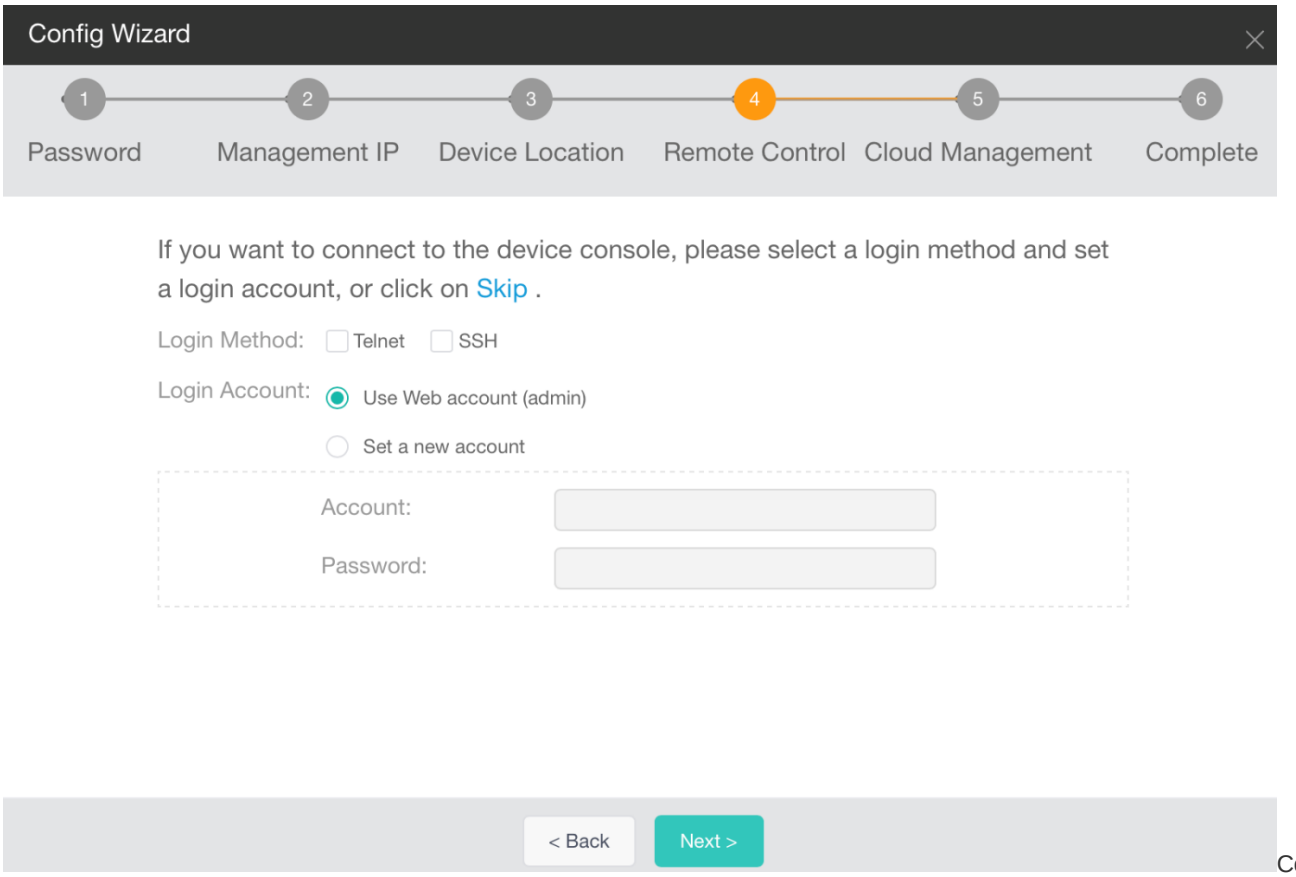
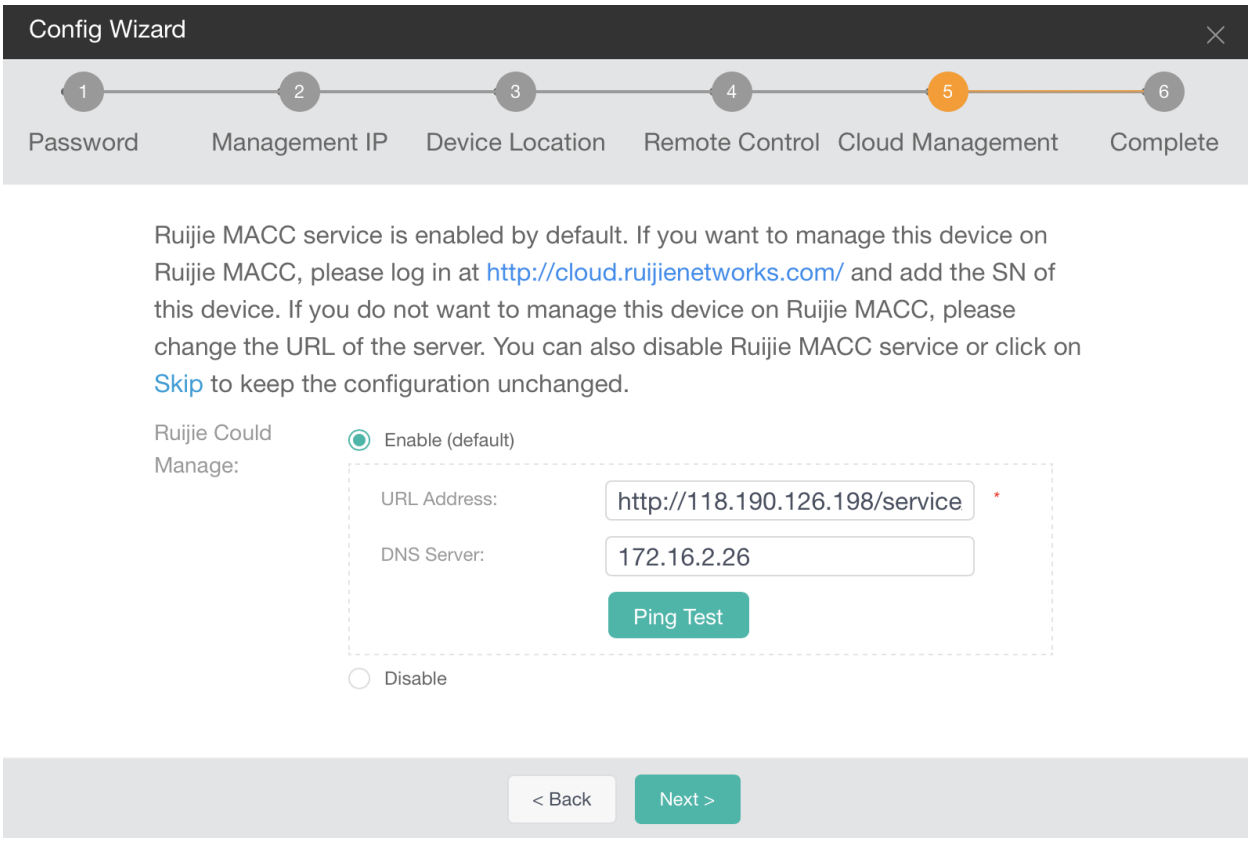


Figure 13 Remote Control



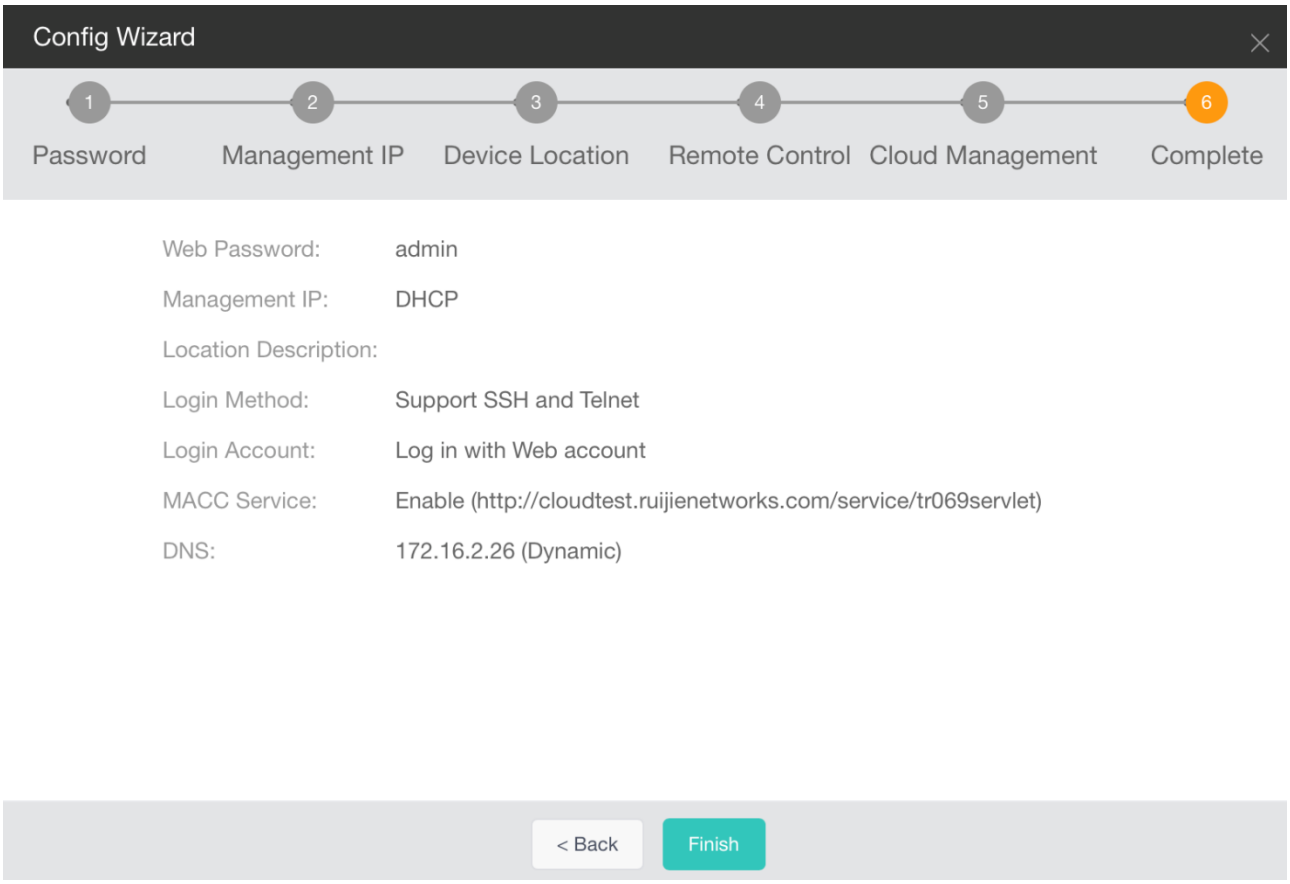
Configure the Telnet and SSH services and the service passwords.

Figure 14 Cloud Management



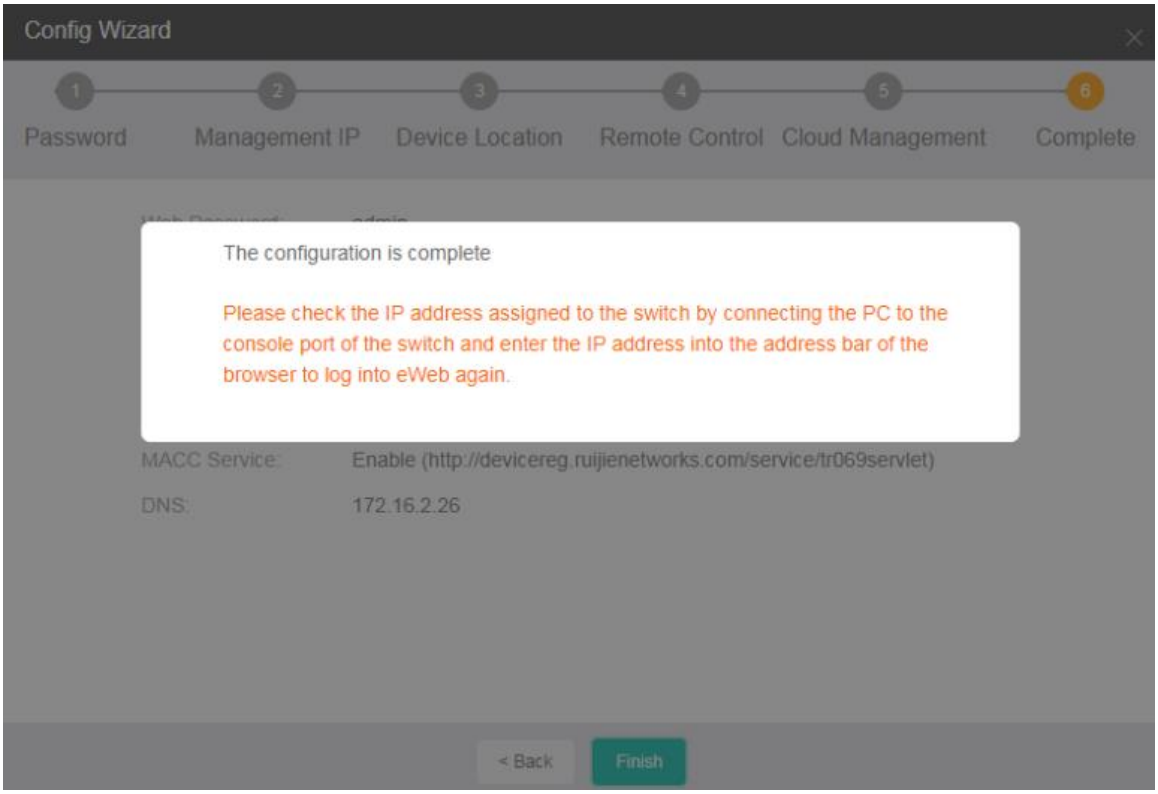
By default, Ruijie MACC is configured. You can change **URL Address** and **DNS Server** as required and click **Ping Test** to check whether the device can connect to the cloud management system.

Figure 15 Complete



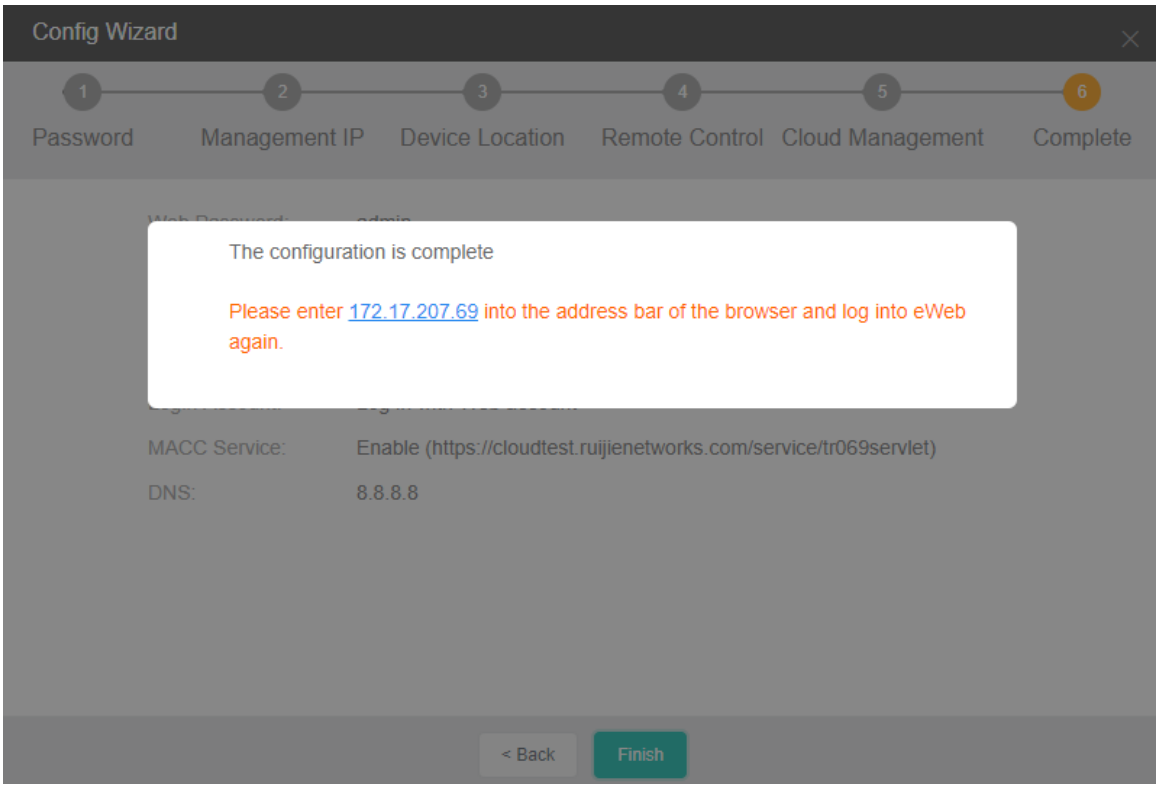
Configured information is displayed. You can click **Finish** to deliver the configurations. When the management IP mode and IP address are not changed, the **Config Wizard** page disappears. When **Static IP Address** is changed to **DHCP**, the following information is displayed, prompting you to log in to the device through a serial port and view the new IP address.

Figure 16



When **DHCP** is changed to **Static IP Address**, the following information is displayed. Click the specified static IP address to switch to the new IP address.

Figure 17



1.3.5 Dashboard

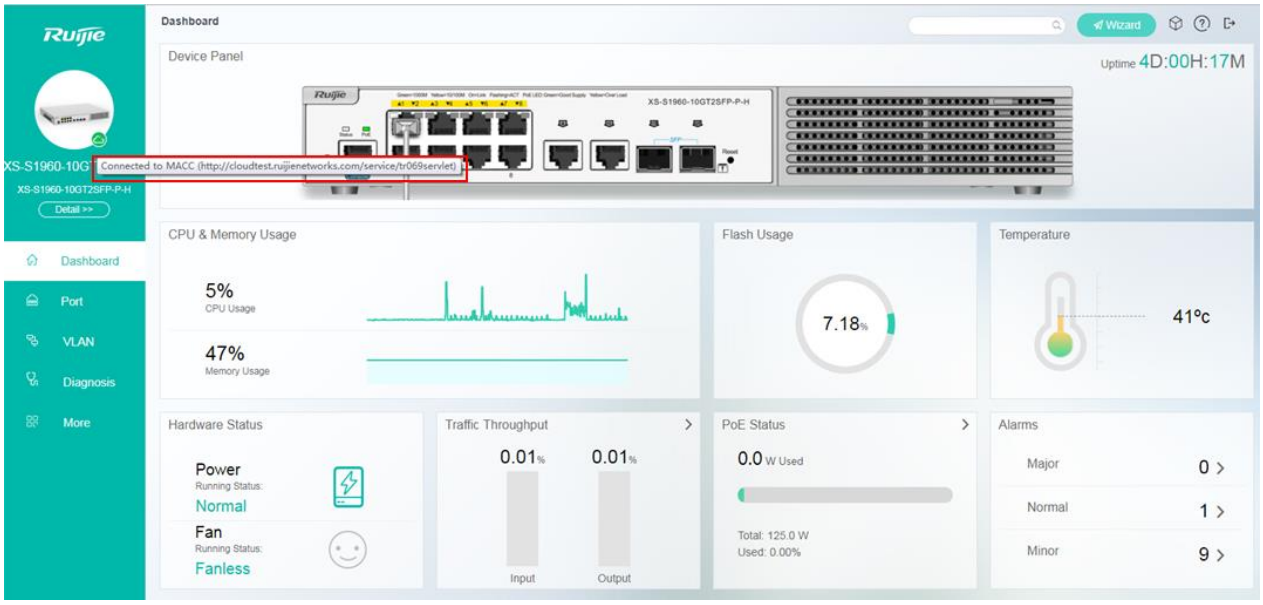
The eWeb home page displays basic device information, port status, CPU and memory usage changes, flash usage, temperature, power, fan, PoE status, device throughput, basic port information and statistics, and alarm information.

Figure 18 shows the eWeb home page.

Figure 18 eWeb Home Page

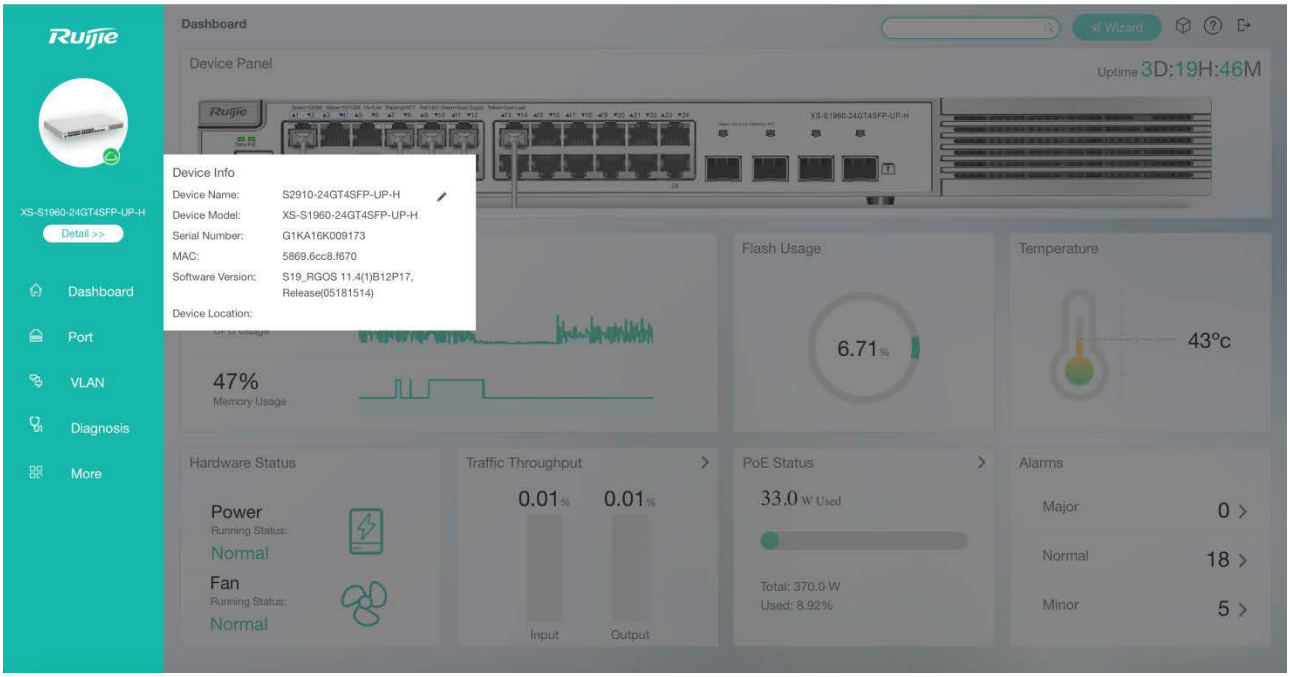
Point to the cloud icon in the lower right corner of the switch picture in the left navigation tree to check whether the switch is connected to the configured cloud.

Figure 19 Cloud Status



Point to **Detail** to view basic device information.

Figure 20 Basic Device Information

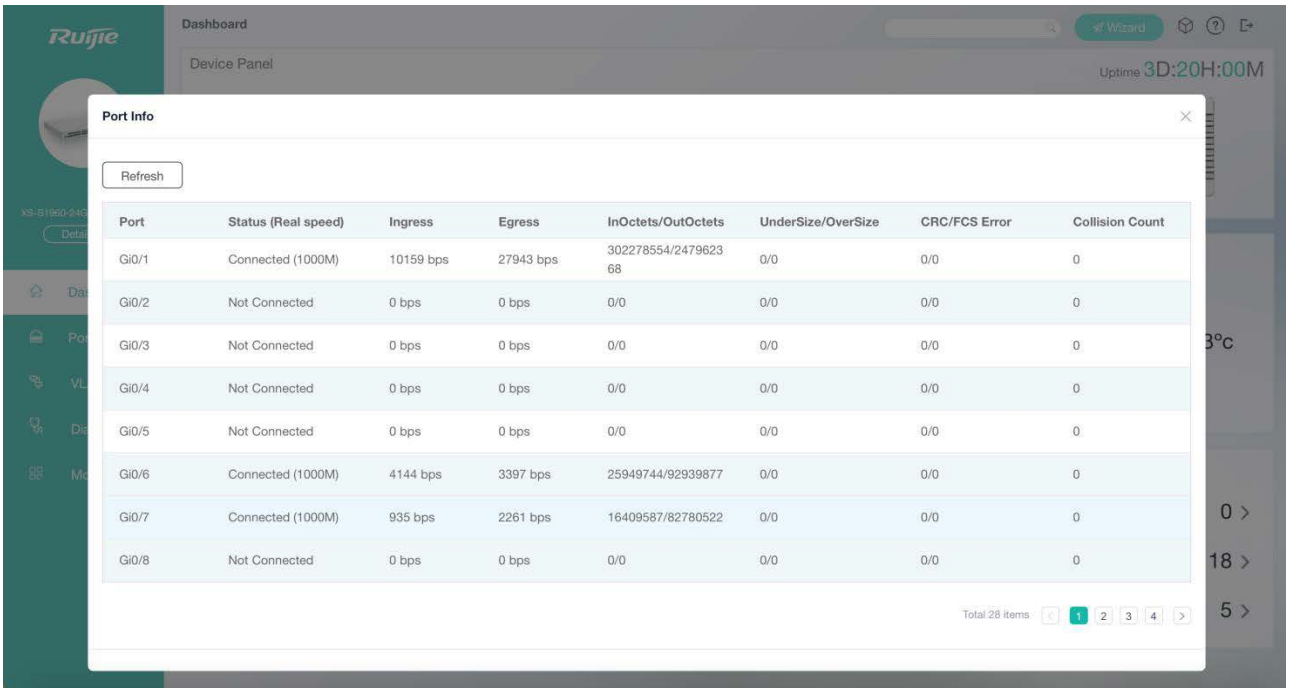


Device Panel: displays the online statuses of ports. When you point to an online port, detailed information about the port can be displayed. You can click the PoE icon on the left of the panel to switch between the switching and PoE modes.

Figure 21 Port Details

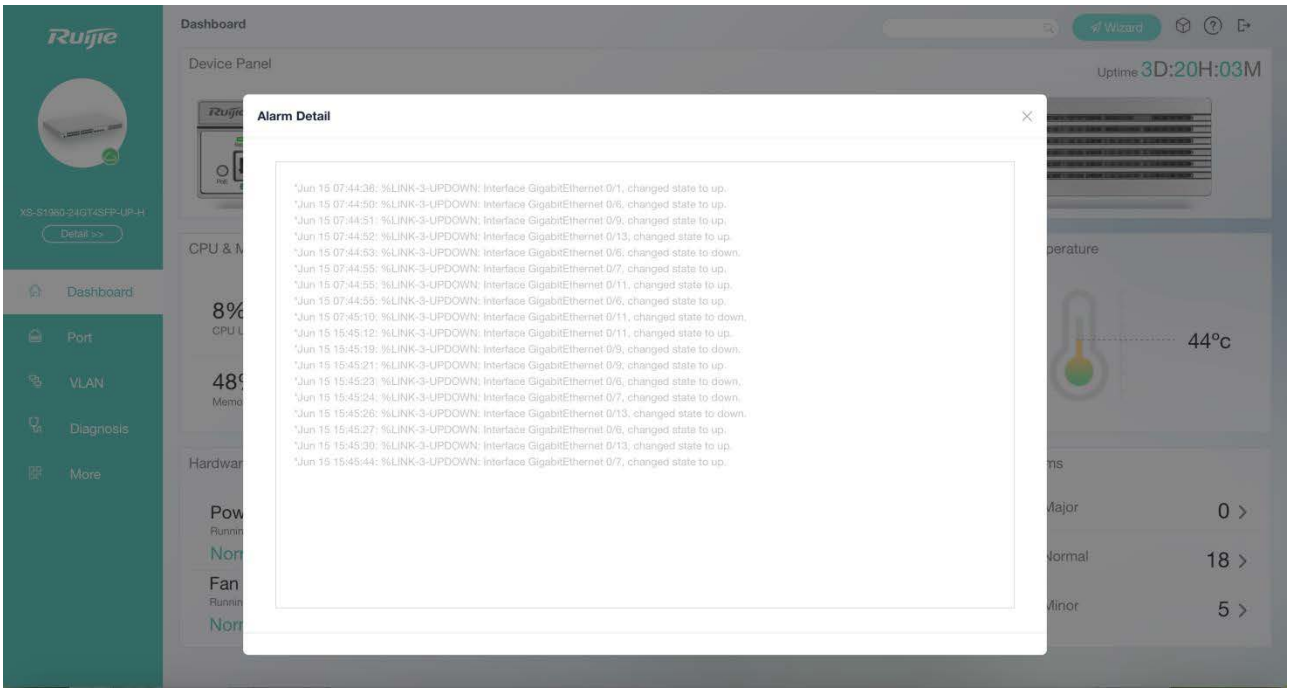
You can click **>** in the **Traffic Throughput** area to view the port status and data traffic statistics.

Figure 22 Port Traffic Statistics



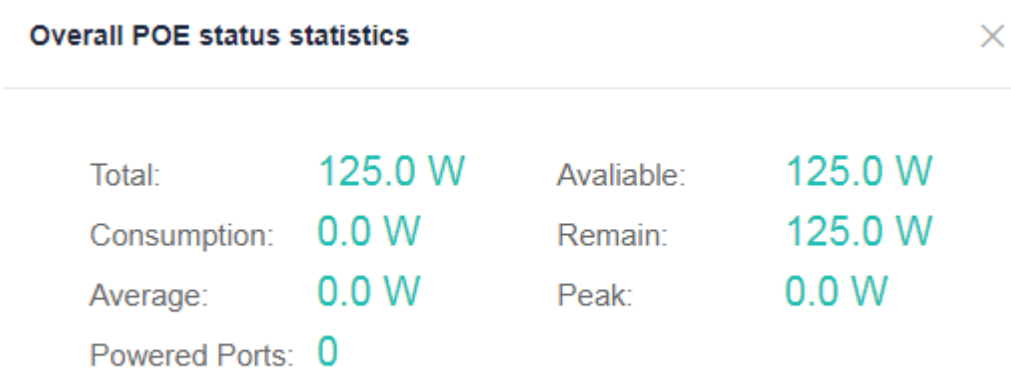
You can click **>** of different severities in the **Alarms** area to view detailed information about the corresponding alarm severities.

Figure 23 Alarm Detail



Click **>** in the **PoE Status** area to view PoE details.

Figure 24 PoE Details

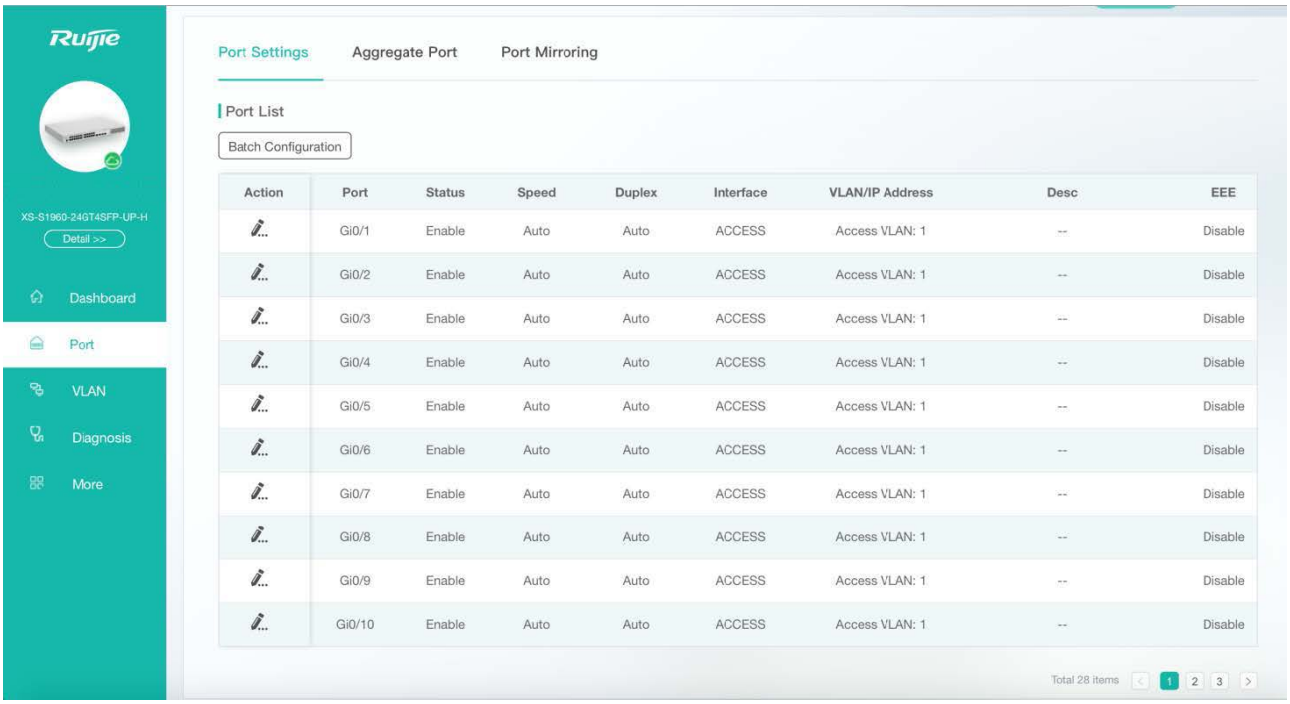


1.3.6 Port

On the **Port** page, you can set basic port information, aggregation ports, and port mirroring.

Port Settings

Figure 25 Port Settings

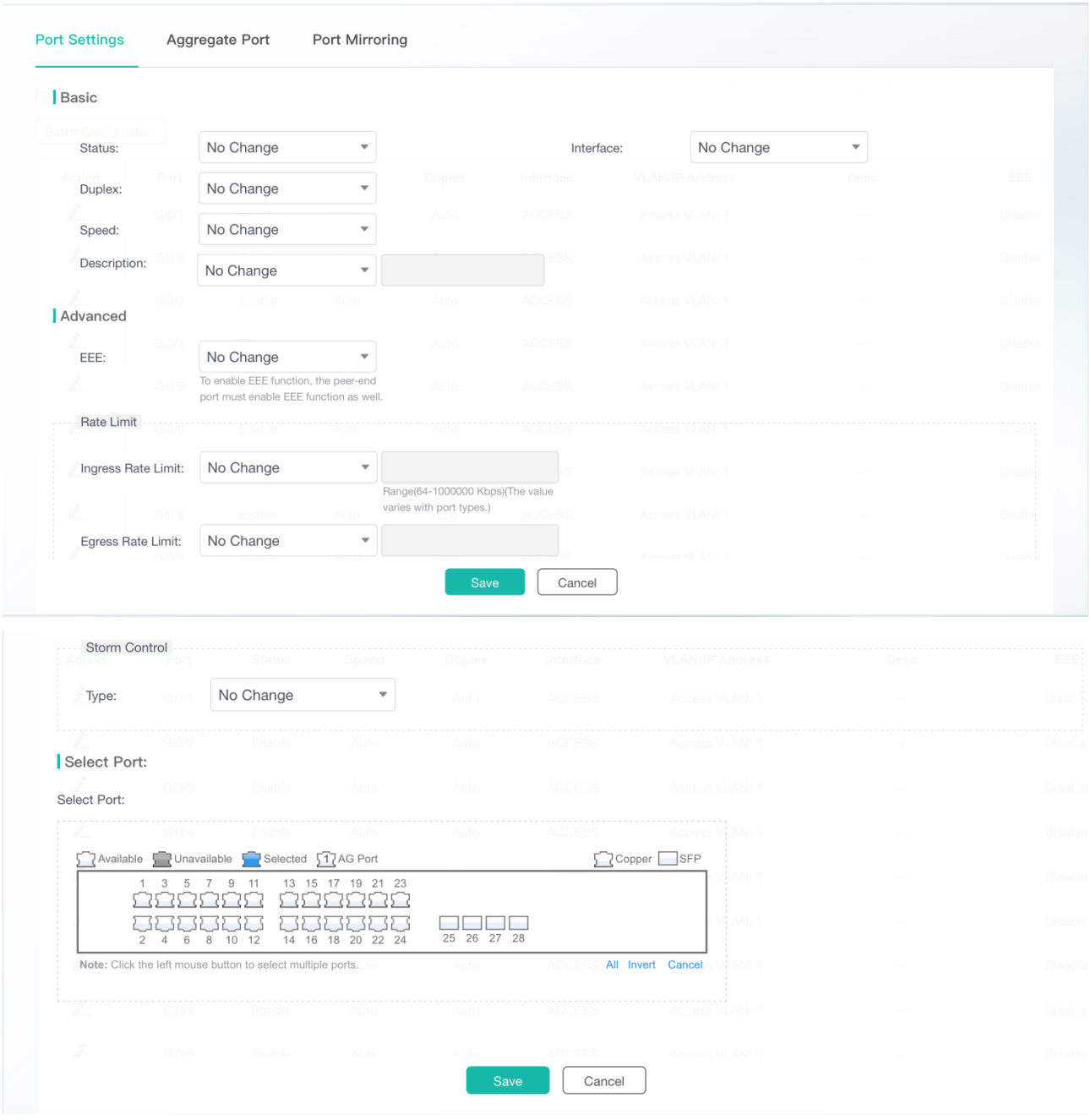


- Batch Configuration

Click **Batch Configuration**. The **Batch Configuration** page is displayed. You can scroll down to view configurable items.

Specify **Status**, **Speed**, **Duplex**, **Rate Limit**, and **Storm Control**. **No Change** indicates that the original configuration is retained. Select the required port and click **Save** to complete configuration. During batch settings, you can specify **No Change** to implement batch settings of one or more items.

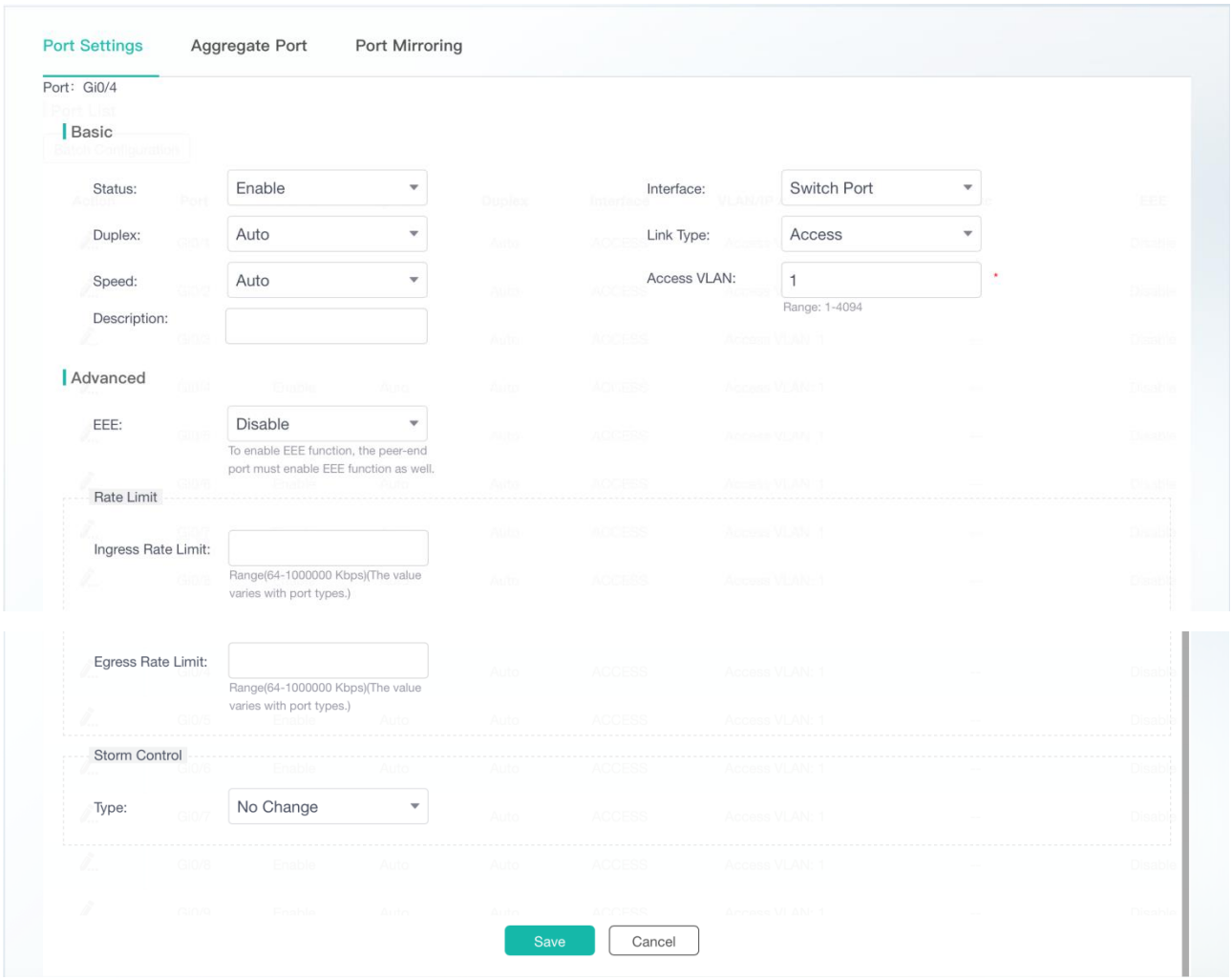
Figure 26 Batch Configuration



- Editing Ports

Click the Edit icon of a port in the **Action** column of **Port List**. The port configuration information is displayed. After you edit the information, click **Save**. After "Configuration succeeded!" is displayed, the editing operation is complete. The port status, duplex mode, speed mode, port type, rate limit, and storm suppression can be configured. You can edit not only physical ports but also aggregation ports and member ports of an aggregation port.

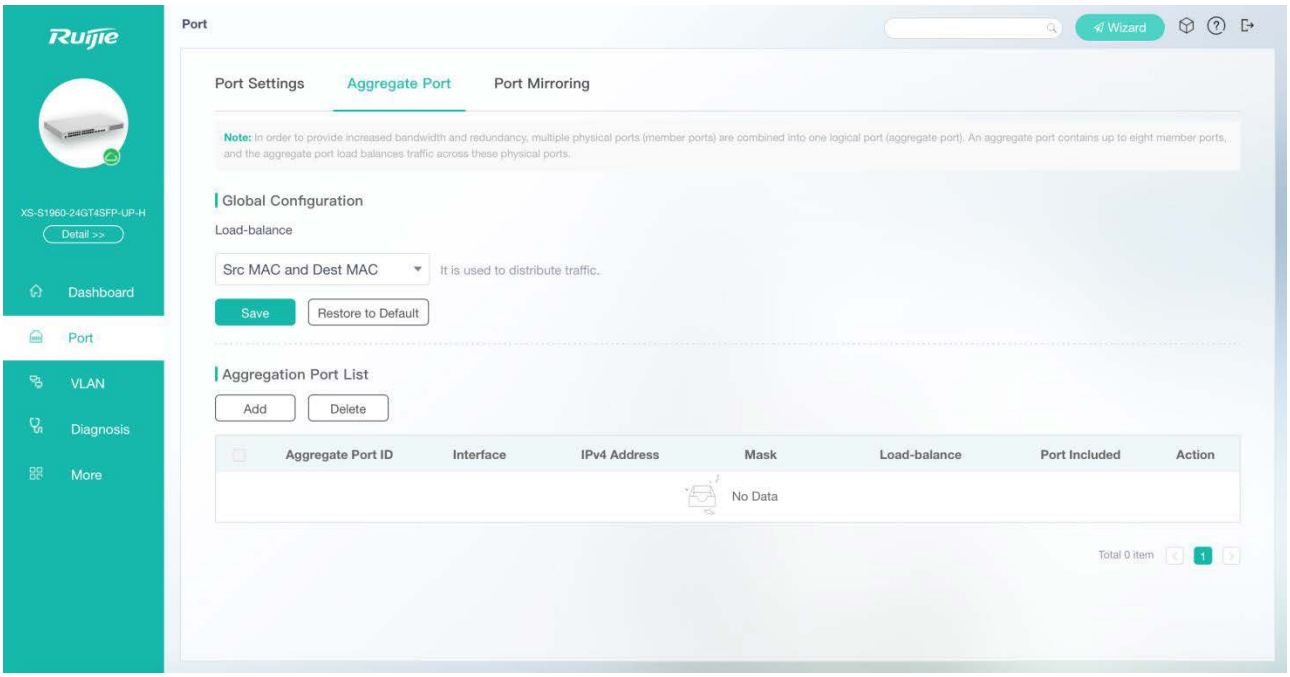
Figure 27 Editing Ports



Aggregate Port

Figure 28 shows the **Aggregate Port** page.

Figure 28 Aggregate Port



- Adding Aggregation Ports

Click **Add**. The **Add** page is displayed. Enter the aggregation port number, select the port type, traffic balance algorithm, and member ports, and click **Save**. After "Add operation succeeded!" is displayed, an aggregation port is successfully added. The successfully added aggregation port is displayed in **Aggregation Port List**.

Figure 29 Add

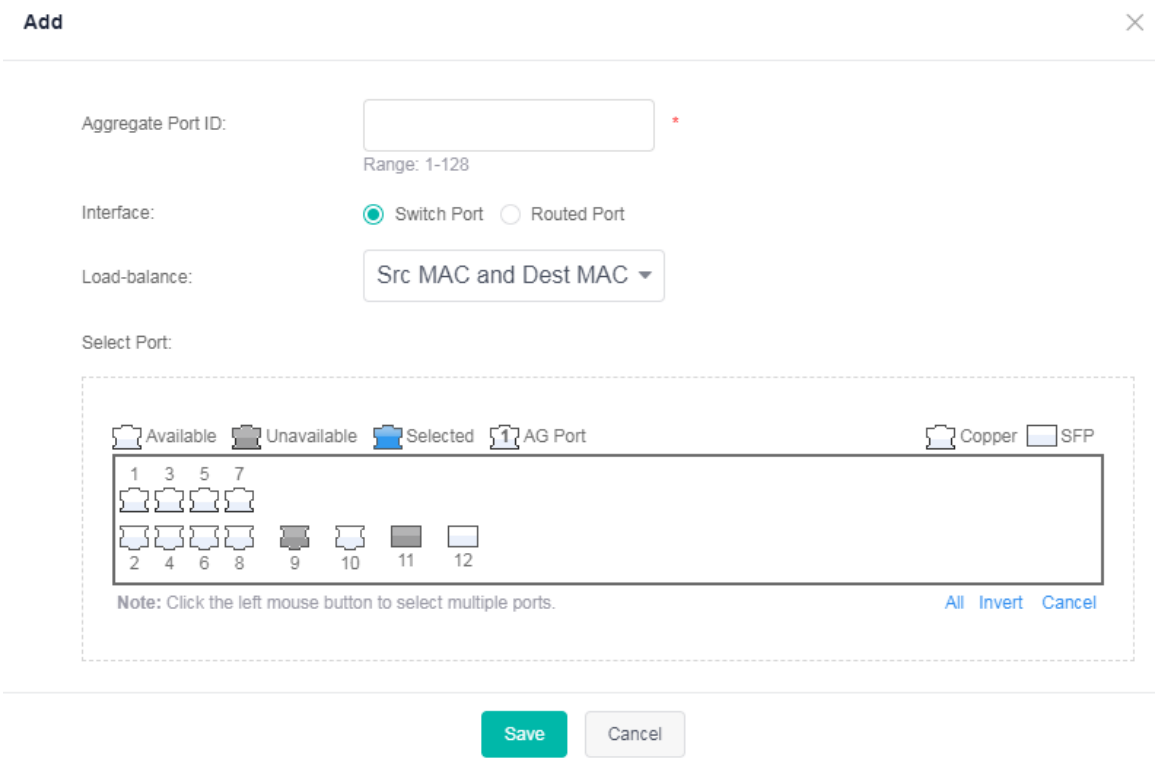
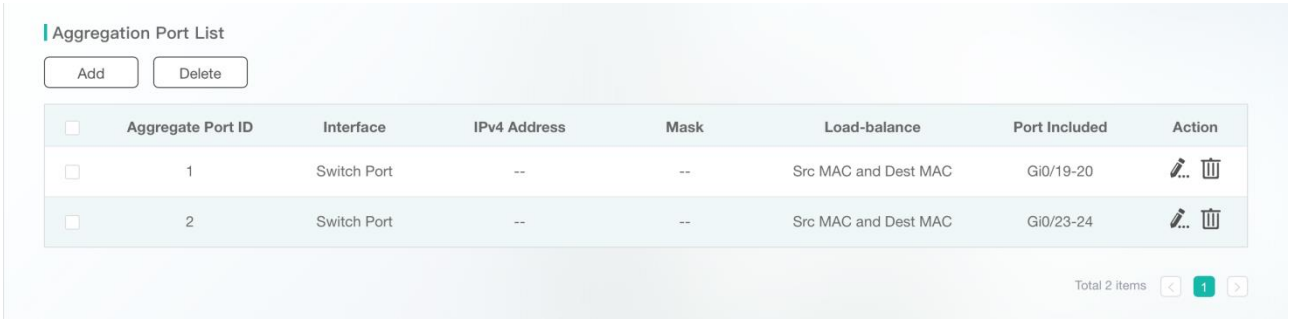


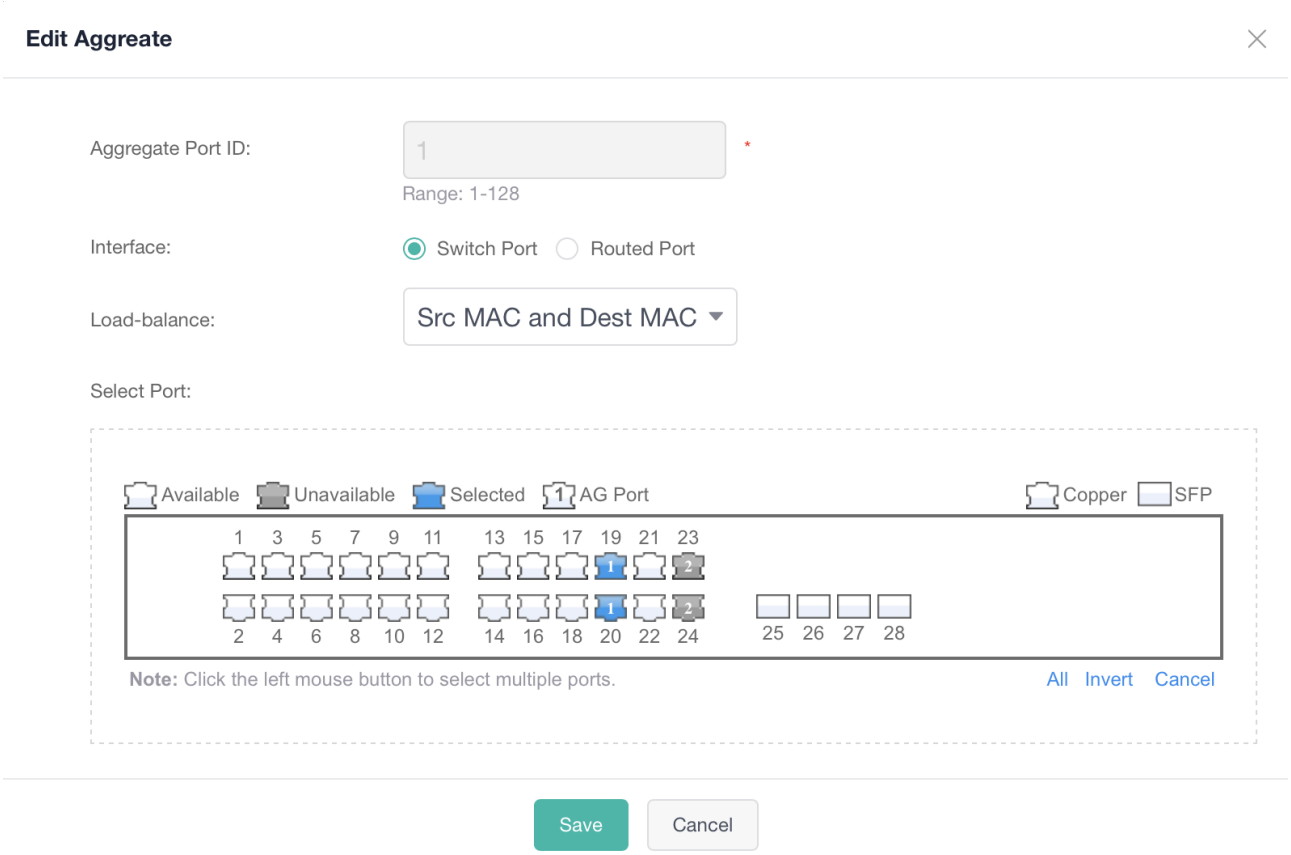
Figure 30 Aggregation Port List



- Editing Aggregation Ports

Click the edit icon of a port in the **Action** column of **Aggregation Port List**. The **Edit Aggregate** page is displayed. Modify the port type, traffic balance algorithm, or member port, and click **Save**. After "Edit operation succeeded!" is displayed, an aggregation port is successfully edited.

Figure 31 Edit Aggregate



- Deleting Aggregation Ports

Click the delete icon of a port in the **Action** column of **Aggregation Port List**. The deletion confirmation dialog box is displayed. After you click **OK**, the aggregation port is deleted. The deleted aggregation port is no longer displayed in **Aggregation Port List**.

- Batch Deleting Aggregation Ports

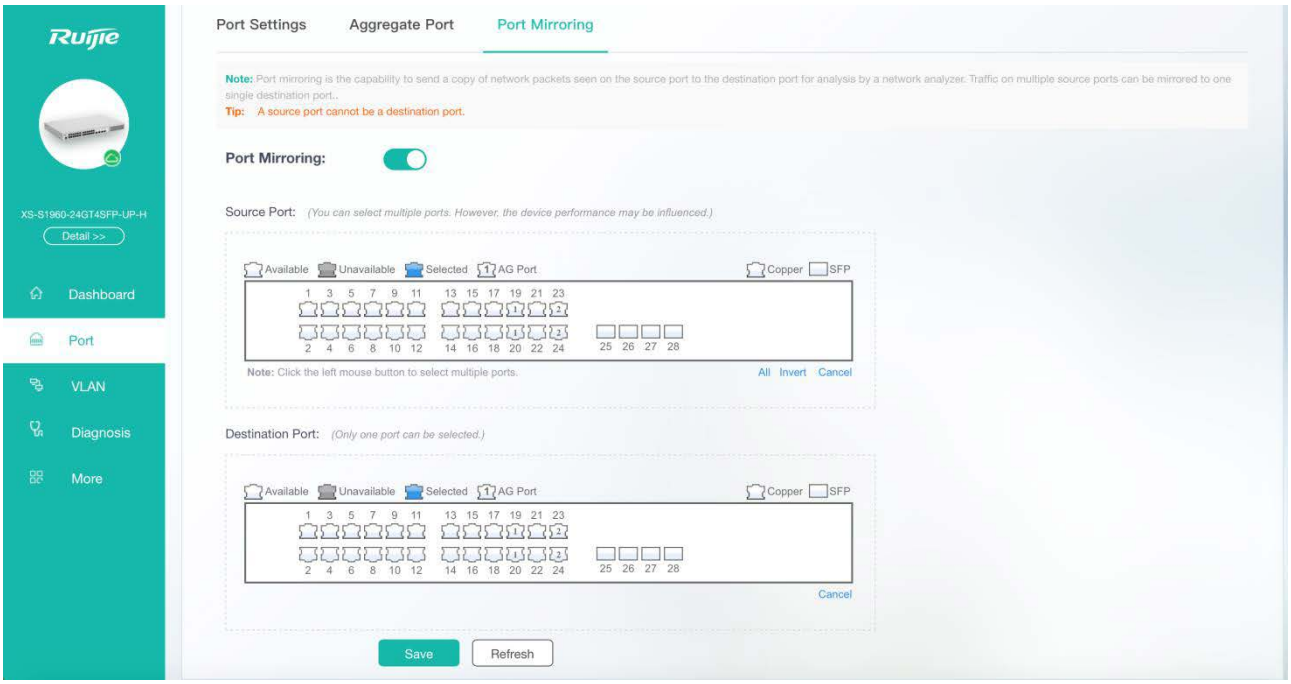
Select the aggregation ports to be deleted in **Aggregation Port List** and click **Delete**. The deletion confirmation dialog box is displayed. After you click **OK**, the aggregation ports are deleted. The deleted aggregation ports are no longer displayed in **Aggregation Port List**.

Ports with the ARP check function, anti-gateway ARP spoofing, or the MAC VLAN function enabled and ports monitored in port mirroring cannot be added to an aggregation port, and these ports are **Unavailable** on the panel. When you point to **Unavailable** of a port, a message "This port is enabled with…" is displayed indicating that these functions are enabled for the port and the port cannot be selected.

Port Mirroring

Figure 32 shows the **Port Mirroring** page.

Figure 32 Port Mirroring



Only one mirrored port can be set on the eWeb. Enable **Port Mirroring**, specify **Source Port** and **Destination Port**, and click **Save**. Port mirroring is successfully configured after "Save operation succeeded!" is displayed.

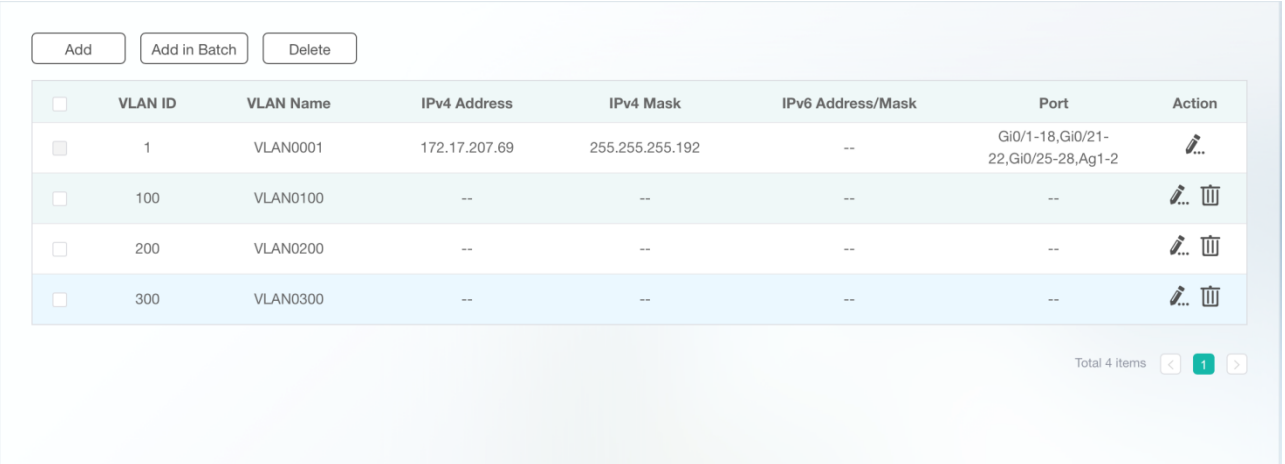
The panel displays the current port mirroring status, and both the source and destination ports are in the editable state. If you expect to abandon a modification to port information, click **Refresh** to restore the panel to the current port mirroring configuration status.

A member port of an aggregation port cannot function as a source or destination port, and the source and destination ports cannot be the same port.

1.3.7 VLAN

Figure 33 shows the **VLAN** page.

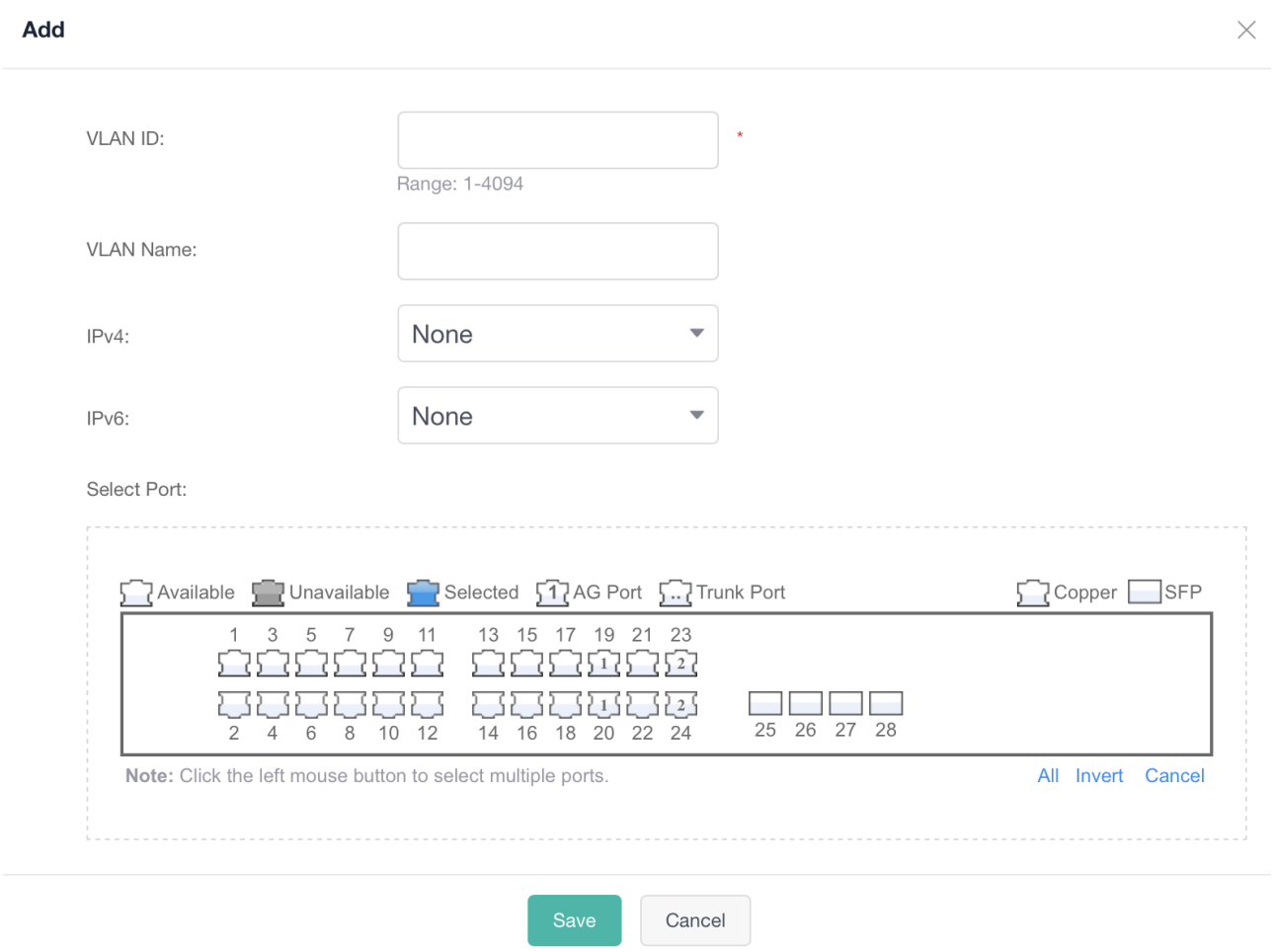
Figure 33 VLAN



- Adding VLANs

Click **Add**. The **Add** page is displayed. Specify **VLAN ID** and other information (optional) and click **Save**. After "Add operation succeeded!" is displayed, the added VLAN is displayed in **VLAN List**. If the selected port is an access port on the switch, the access VLAN of the port is changed to the configured VLAN. If the selected port is a trunk port on the switch, the configured VLAN is added to **Allowed VLAN**.

Figure 34 Add



- Editing VLANs

Click the edit icon of a VLAN in the **Action** column of **VLAN List**. The VLAN information is displayed. Edit the information, and click **Save**. After "Edit operation succeeded!" is displayed, the editing operation is complete. Information of the VLAN in **VLAN List** is updated.

- Deleting VLANs

1. Select multiple records in **VLAN List** and click **Delete** to batch delete the data records.

2. Click the edit icon of a VLAN in the **Action** column of **VLAN List**. In the displayed deletion confirmation dialog box, click **OK**. After "Delete operation succeeded!" is displayed, the deletion is complete.

VLAN1 is the default management VLAN. It can only be modified and cannot be deleted. When modifying the IP address of VLAN1, ensure that the new IP address is reachable. After the modification is successful, the login page is displayed and you need to log in to the eWeb again. If switching to the login page fails and a message indicating that the web page cannot be found is displayed, the specified IP address may be unreachable. Check the network connection.

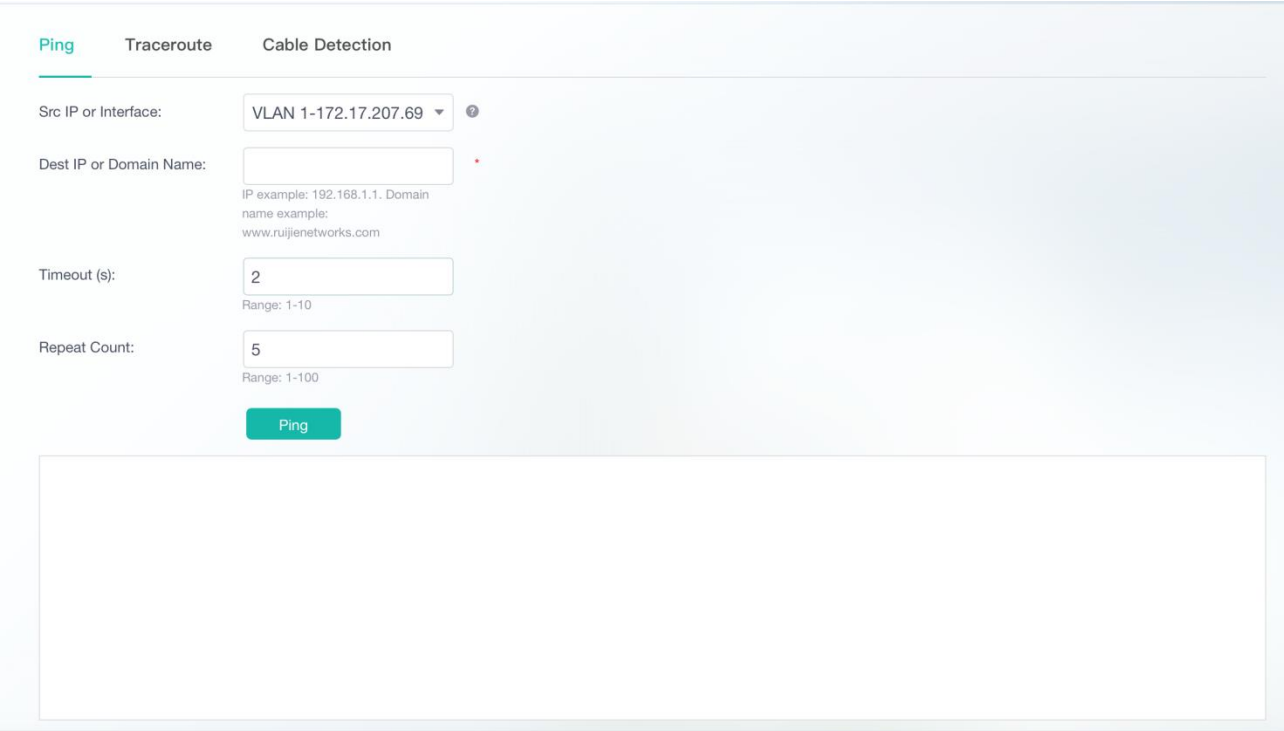
1.3.8 Diagnosis

The **Diagnosis** page consists of three parts: **Ping**, **Traceroute**, and **Cable Detection**.

Ping

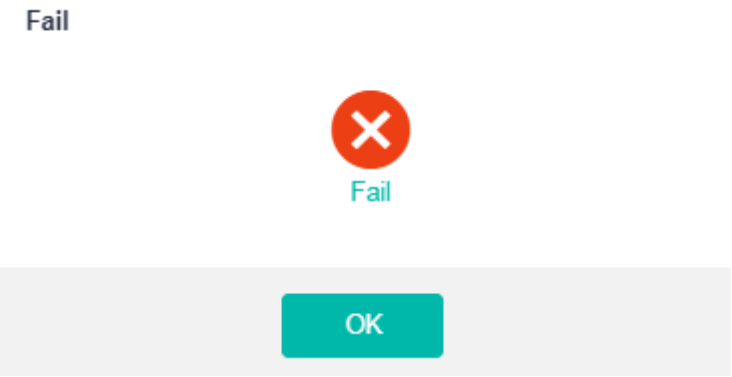
Figure 35 shows the **Ping** page.

Figure 35 Ping



Specify **Src IP or Interface**, enter **Dest IP or Domain Name** and click **Ping**. The detection result is displayed in the text box. If no detection result is returned for more than 5 minutes, the **Fail** dialog box is displayed.

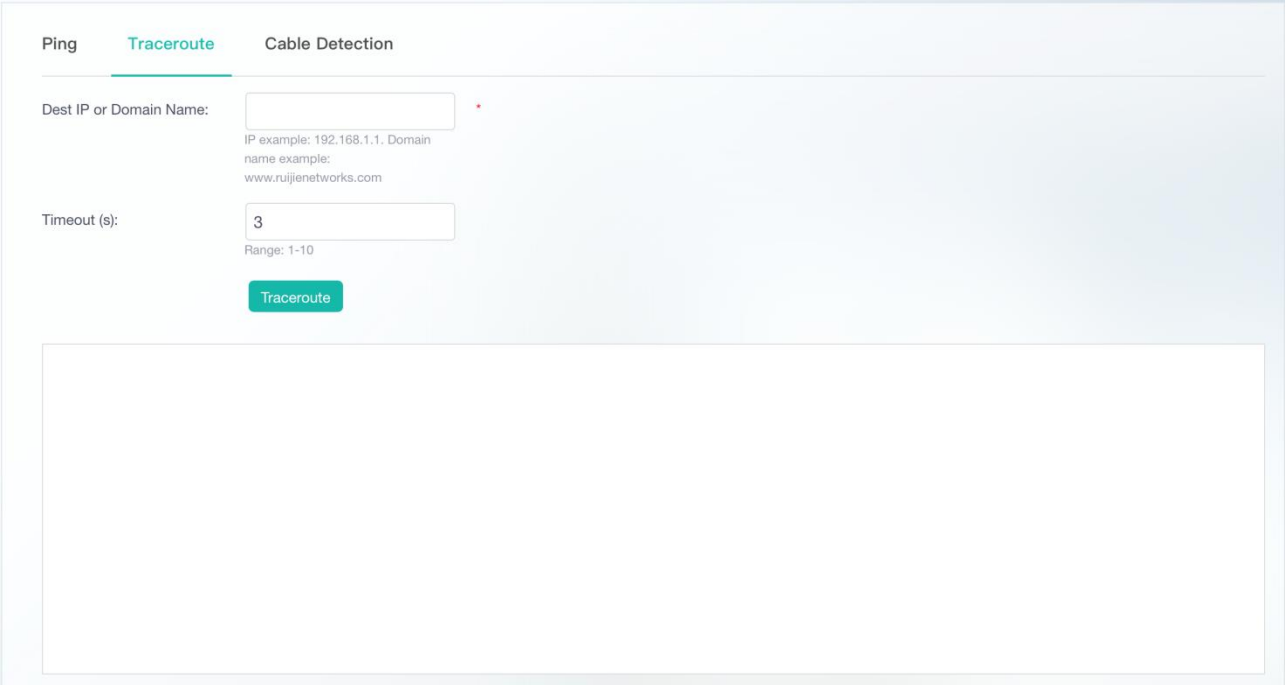
Figure 36 Fail



Traceroute

Figure 37 shows the **Traceroute** page.

Figure 37 Traceroute

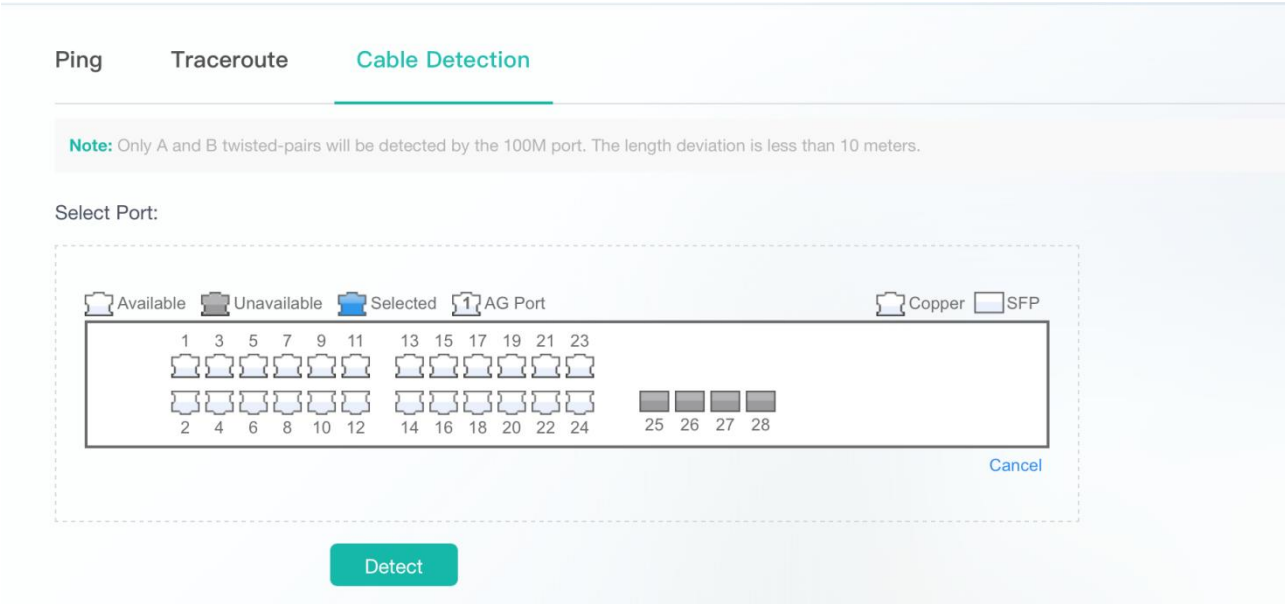


Specify **Dest IP or Domain Name** and other information and click **Traceroute**. The detection result is displayed in the text box later. If no detection result is returned for more than 5 minutes, the **Fail** dialog box same as that in Figure 36 is displayed.

Cable Detection

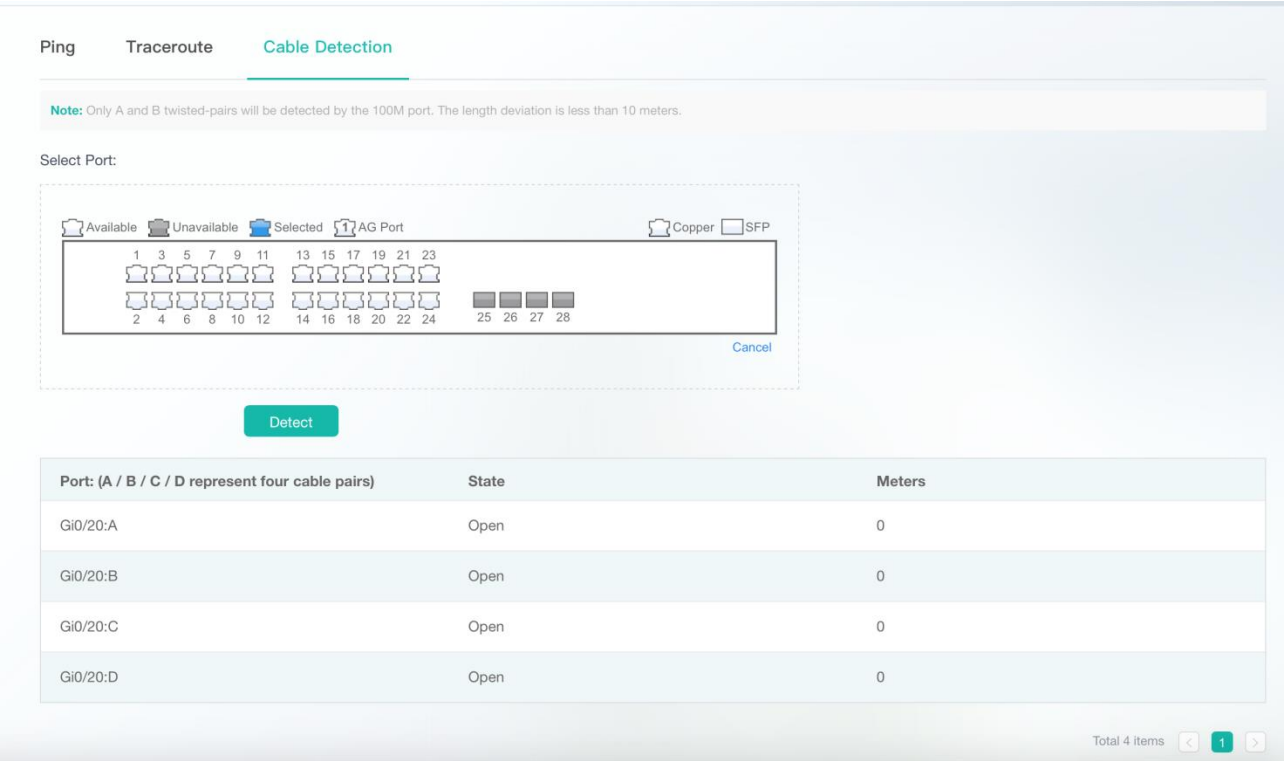
Figure 38 shows the **Cable Detection** page.

Figure 38 Cable Detection



Select an available port on the panel and click **Detect**. After the detection confirmation dialog box is displayed, click **OK**. The detection result is displayed in the table below **Detect** later.

Figure 39 Cable Detection Result



1.3.9 Network Settings

The first-level menu **More** includes three second-level menus: **Network Settings**, **Security Settings**, and **System Settings**.

This section mainly introduces **Network Settings**.

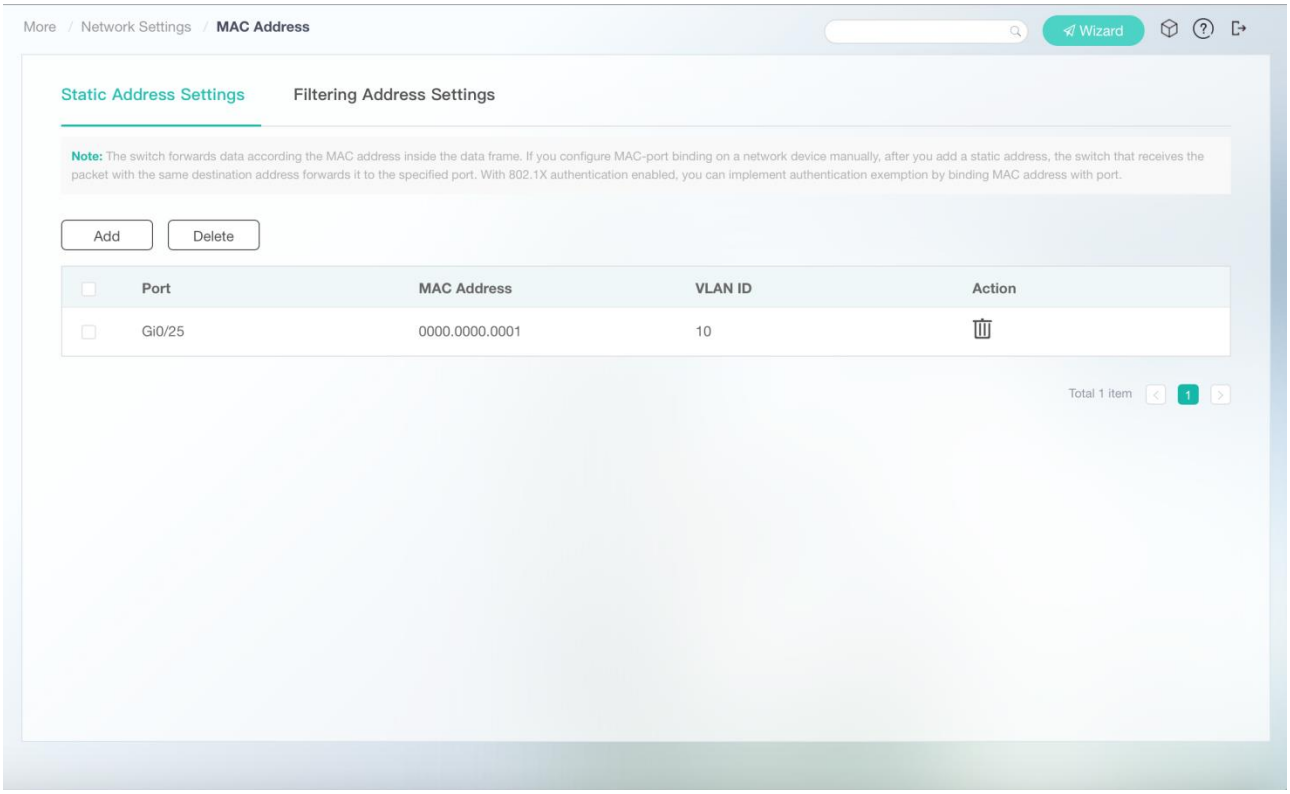
1.3.9.1 MAC Address

The **MAC Address** page consists of two parts: **Static Address Settings** and **Filtering Address Settings**.

↘ Static Address Settings

Figure 40 shows the **Static Address Settings** page.

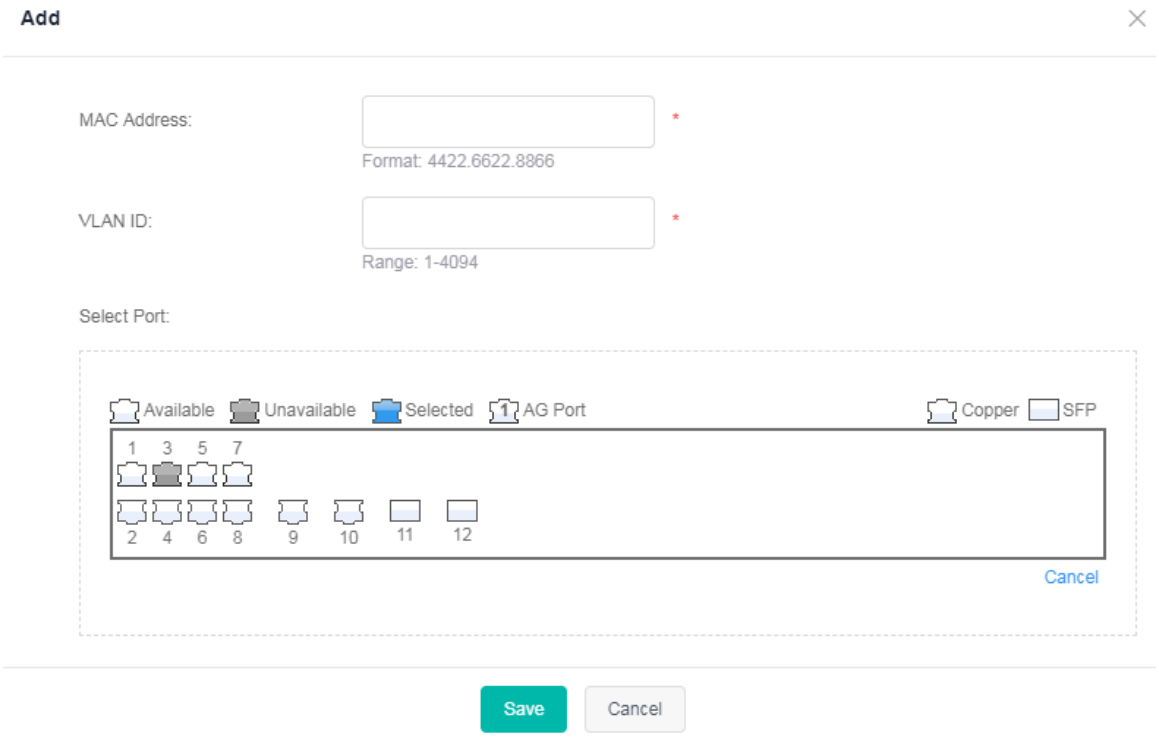
Figure 40 Static Address Settings



- Adding Static Addresses

Click **Add**. The **Add** page is displayed. Specify **MAC Address**, **VLAN ID**, and **Port** and click **Save** to set a static address. After "Add operation succeeded!" is displayed, the newly added address is displayed in the static address list.

Figure 41 Add



- Deleting Static Addresses

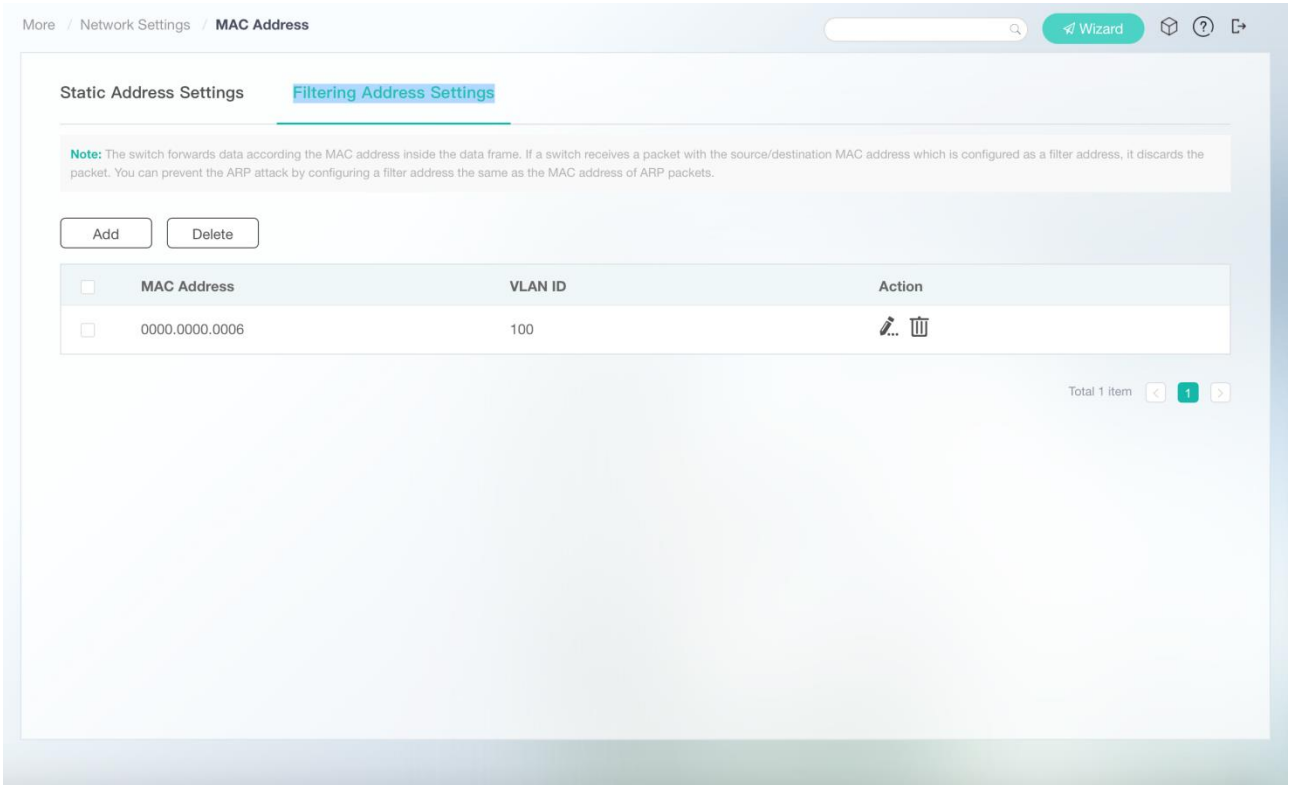
1. Click the delete icon of a static address in the **Action** column of the MAC address list. In the displayed deletion confirmation dialog box, click **OK**. After "Delete operation succeeded!" is displayed, the deletion is complete. The deleted static address is no longer displayed in the MAC address list.

2. Select multiple records in the MAC address list and click **Delete** to batch delete the data records.

Filtering Address Settings

Figure 42 shows the **Filtering Address Settings** page.

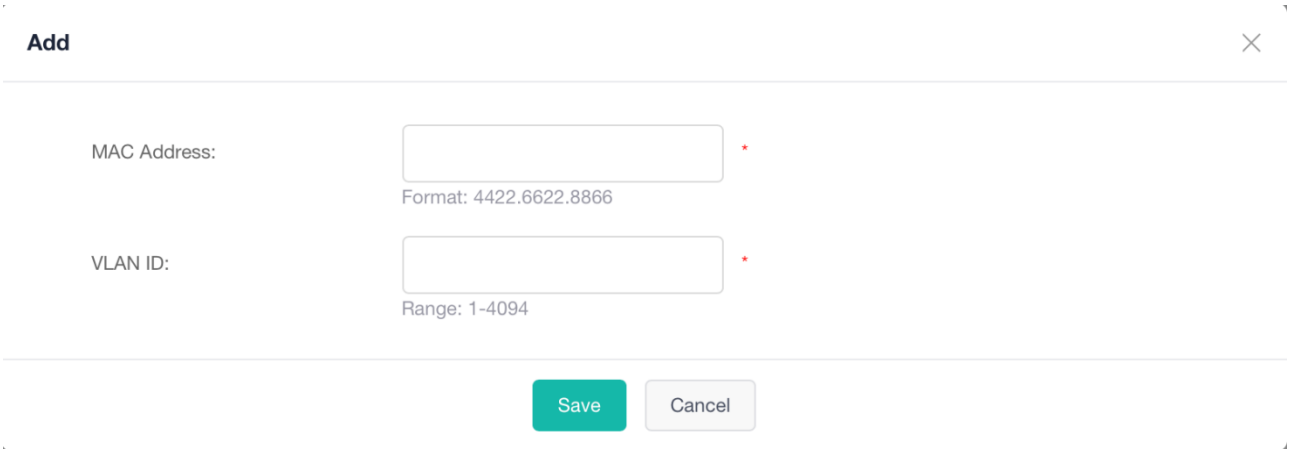
Figure 42 Filtering Address Settings



- Adding Filtering Addresses

Click **Add**. The **Add** page is displayed. Specify **MAC Address** and **VLAN ID** and click **OK** to set a filtering address. After "Add operation succeeded!" is displayed, the filtering address is displayed in the filtering address list.

Figure 43 Add



- Editing Filtering Addresses

Click the edit icon of a filtering address in the **Action** column of the filtering address list. The filtering address information is displayed. After you edit the information, click **Save**. After "Edit operation succeeded!" is displayed, the editing operation is complete.

- Deleting Filtering Addresses

1. Click the delete icon of a filtering address in the **Action** column of the filtering address list**.** In the displayed deletion confirmation dialog box, click **OK**. After "Delete operation succeeded!" is displayed, the deletion is complete. The deleted filtering address is no longer displayed in the filtering address list.

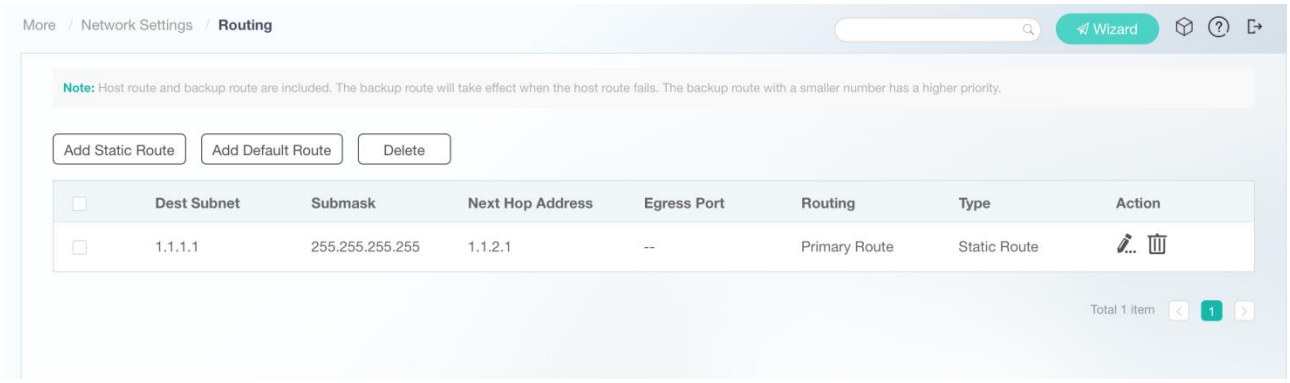
2. Select multiple records in the filtering address list and click **Delete** to batch delete the data records.

1.3.9.2 Routing

The **Routing** page enables you to manage routes.

Figure 44 shows the **Routing** page.

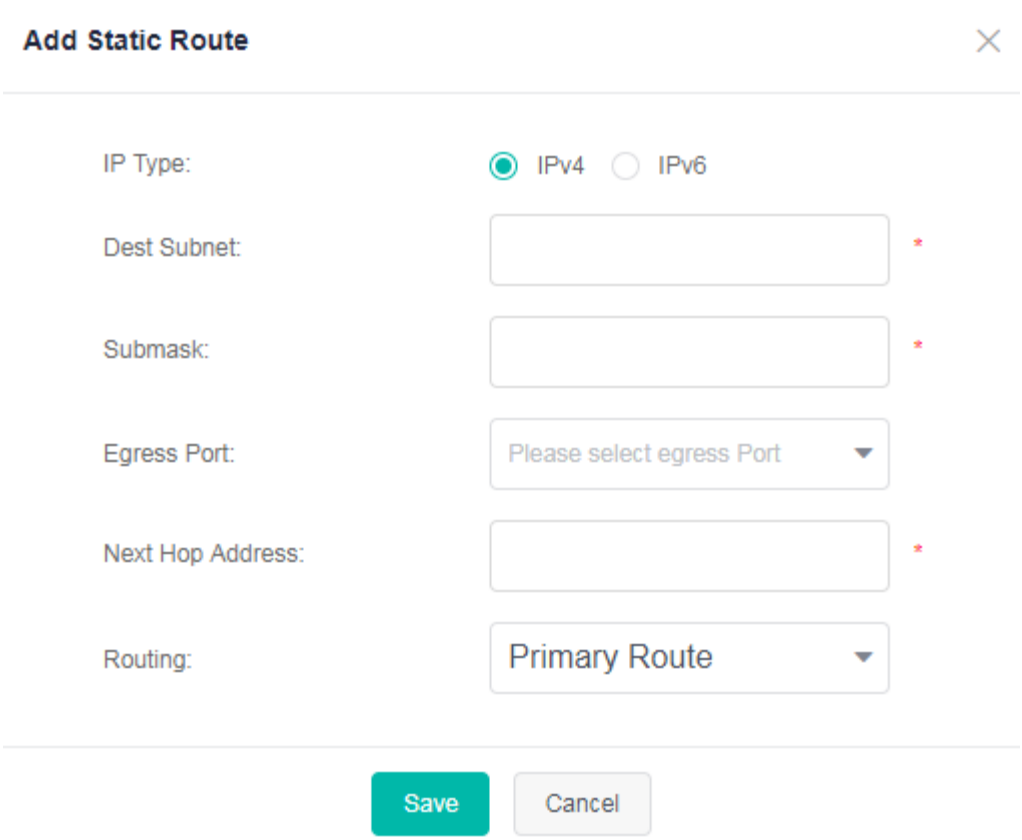
Figure 44 Routing



- Adding Static Routes

Click **Add Static Route**. The **Add Static Route** page is displayed. Specify mandatory parameters **IP Type**, **Dest Subnet**, **Submask**, and **Next Hop Address**, and click **Save**. After "Add operation succeeded!" is displayed, the added route is displayed in **Route List**.

Figure 45 Add Static Route



- Editing Routes

Click the edit icon of a route in the **Action** column of the route list. The route information is displayed. After you edit the information, click **Save**. After "Edit operation succeeded!" is displayed, the editing operation is complete.

- Deleting Routes

1. Select multiple records in the route list and click **Delete** to batch delete the data records.

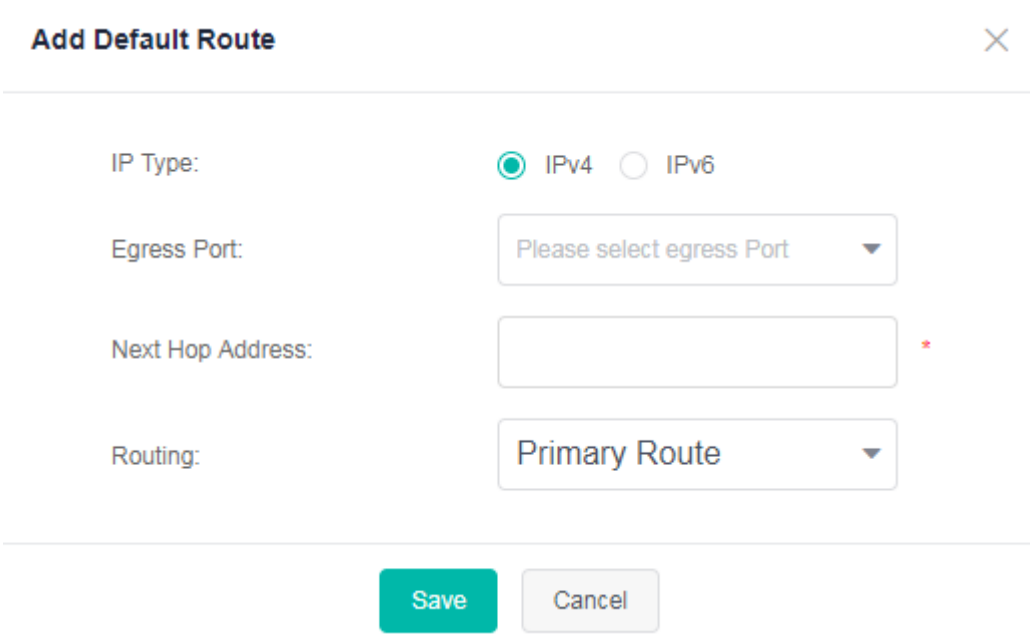
2. Click the delete icon of a route in the **Action** column of the route list. In the displayed deletion confirmation dialog box, click **OK**. After "Delete operation succeeded!" is displayed, the deletion is complete. The deleted route is no longer displayed in the route list.

- Add Default Route

Click **Add Default Route**. The **Add Default Route** page is displayed. Specify mandatory parameters **IP Type** and **Next Hop Address**, and click **Save**. After "Add operation succeeded!" is displayed, the added default route is displayed in the route list.

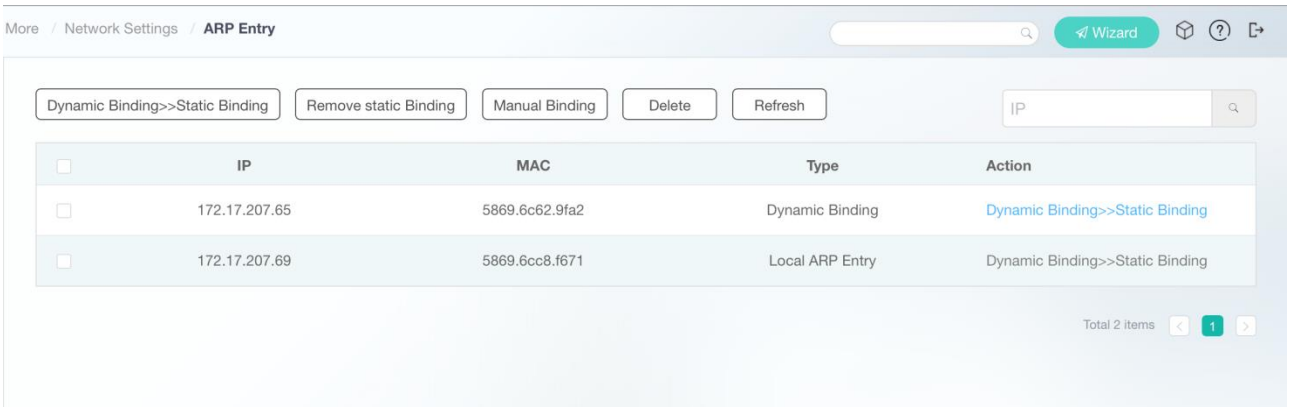
Routes are classified into active and standby routes. When a primary route becomes invalid, a backup route takes over services. Backup routes are selected based on their priorities. The priority of backup route 1 is higher than that of backup route 2.

Figure 46 Add Default Route



1.3.9.3 ARP Entry

Figure 47 ARP Entry



- Dynamic Binding>>Static Binding

1. Select multiple dynamic data records in the ARP entry list and batch set them as static binding records.

2. Click **Dynamic Binding>>Static Binding** in the **Action** column of the ARP entry list. After "Operation succeeded!" is displayed, static binding is successful.

- Remove Static Binding

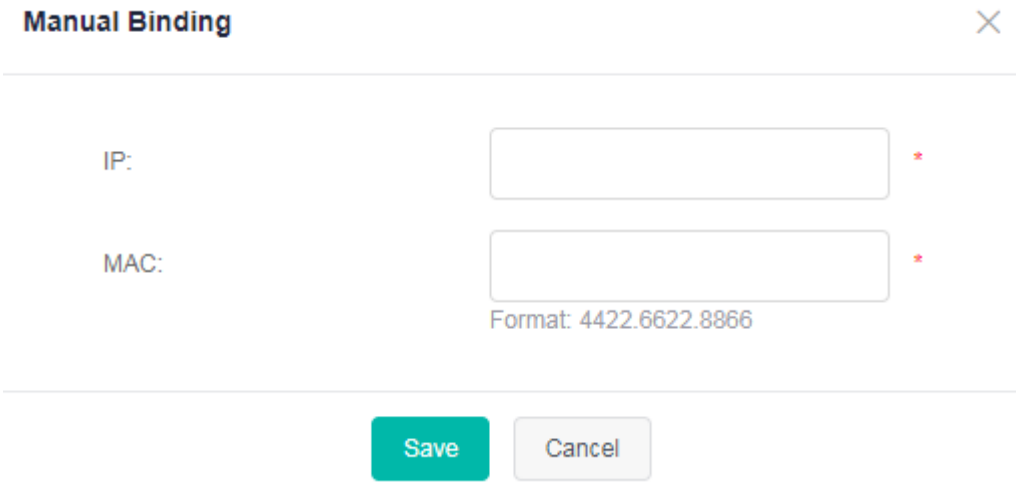
1. Select multiple static binding data records in the ARP entry list and click **Remove static Binding**.

2. Click **Remove static Binding** in the **Action** column of the ARP entry list. After "Operation succeeded!" is displayed, static binding is removed.

- Manual Binding

Click **Manual Binding**. The **Manual Binding** page is displayed. Specify mandatory parameters **IP** and **MAC address**, and click **Save**. After "Operation succeeded!" is displayed, the manual binding record is displayed in the ARP entry list.

Figure 48 Manual Binding



- Delete

Select multiple dynamic or static binding data records in the ARP entry list to batch delete the data records.

- Refresh

Click **Refresh** to update the current ARP entry list.

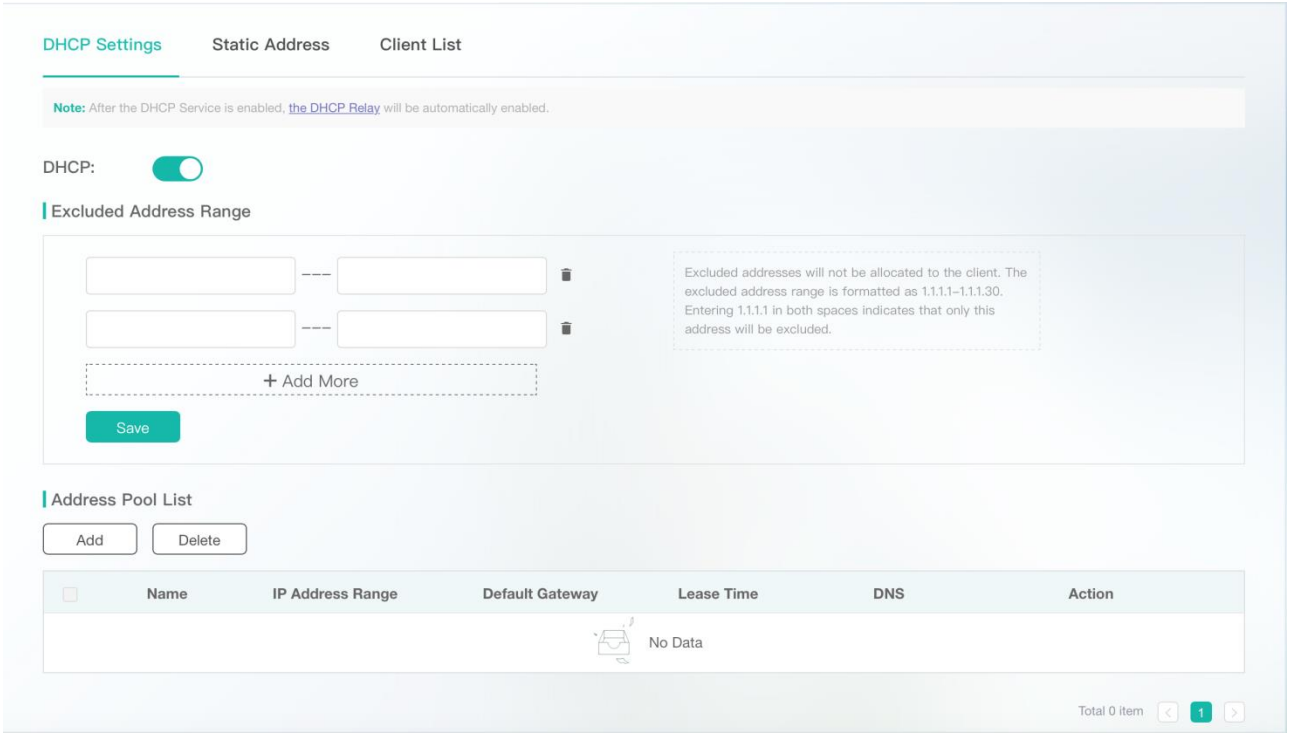
1.3.9.4 DHCP Server

The **DHCP Server** page consists of three parts: **DHCP Settings**, **Static Address**, and **Client List**.

DHCP Settings

Figure 49 shows the **DHCP Settings** page.

Figure 49 DHCP Settings



- Enabling DHCP

Enable the DHCP function. After "Enable operation succeeded!" is displayed, the global DHCP function is enabled.

- Configuring Excluded Addresses

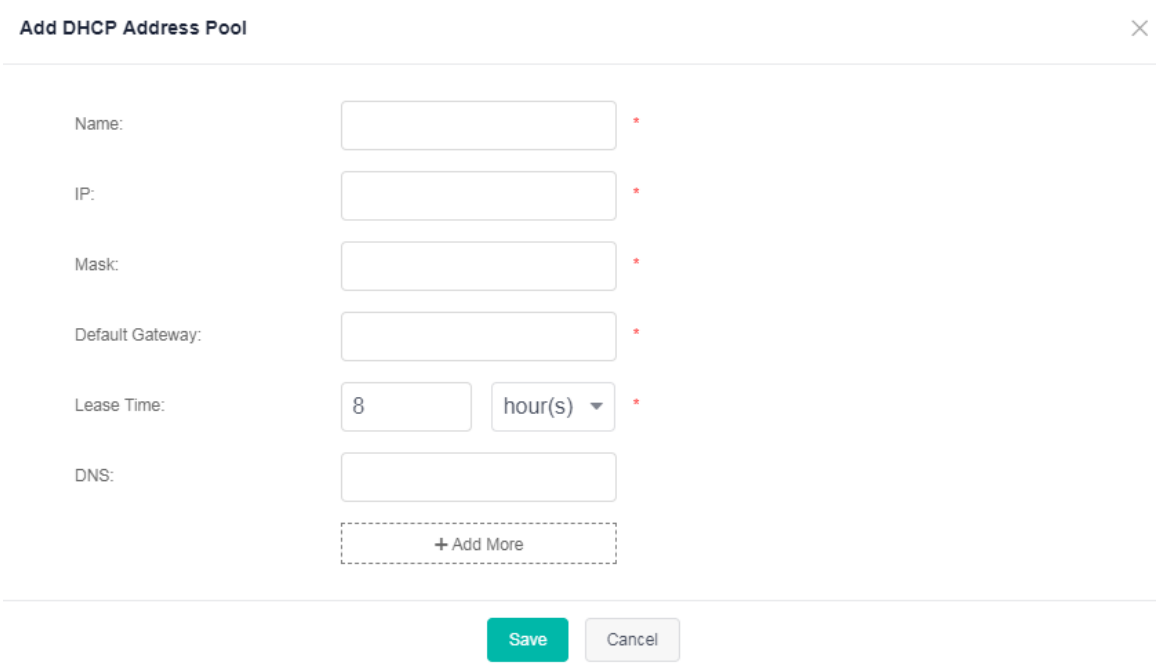
Excluded addresses are not allocated to the clients.

You can add or delete excluded addresses in **Excluded Address Range**.

- Adding DHCP Address Pools

In **Address Pool List**, click **Add**. The **Add DHCP Address Pool** page is displayed. Specify mandatory parameters **Name**, **IP**, **Mask**, **Default Gateway**, and **Lease Time**, and click **Save**. After "Add operation succeeded!" is displayed, the added DCHP address pool is displayed in **Address Pool List**.

Figure 50 Add DHCP Address Pool



- Editing DHCP Address Pools

Click the edit icon of an address pool in the **Action** column of **Address Pool List**. The DHCP address pool information is displayed. After you edit the information, click **Save**. After "Edit operation succeeded!" is displayed, the editing operation is complete.

- Deleting DHCP Address Pools

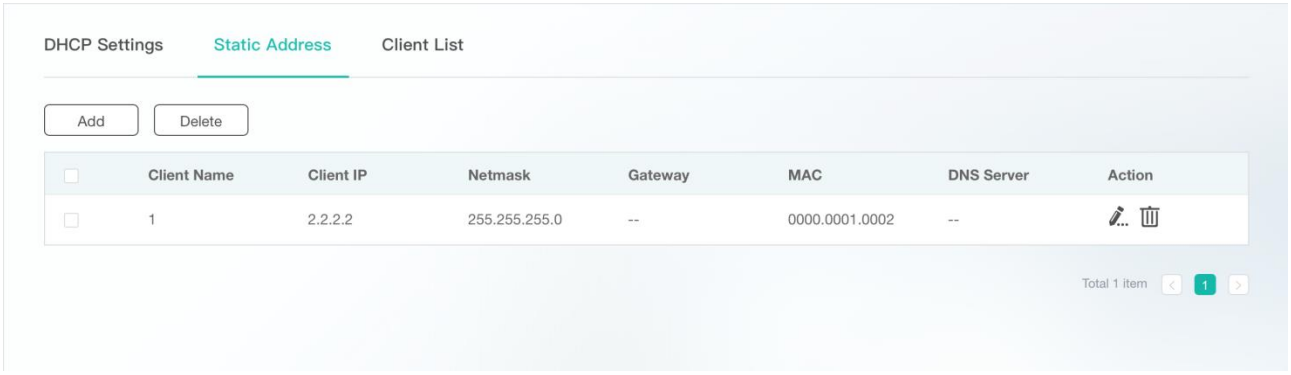
1. Select multiple records in **Address Pool List** and click **Delete** to batch delete the data records.

2. Click the delete icon of an address pool in the **Action** column of **Address Pool List**. In the displayed deletion confirmation dialog box, click **OK**. After "Delete operation succeeded!" is displayed, the deletion is complete. The deleted DHCP address pool is no longer displayed in **Address Pool List**.

Static Address

Figure 51 shows the **Static Address** page.

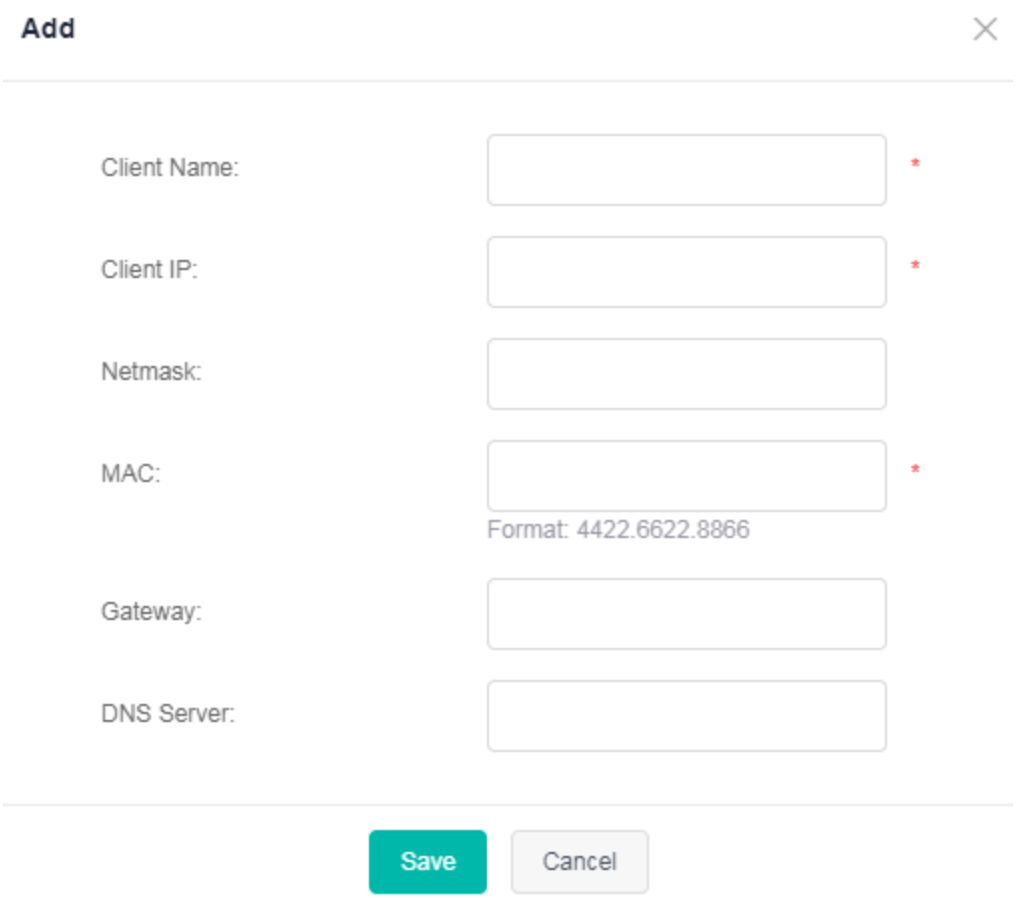
Figure 51 Static Address



- Adding Static Addresses

Click **Add**. The **Add** page is displayed. Specify mandatory parameters **Client Name**, **Client IP**, **Netmask**, and **MAC**, and click **Save**. After "Add operation succeeded!" is displayed, the added static address is displayed in the static address list.

Figure 52 Add



- Editing Static Addresses

Click the edit icon of a static address in the **Action** column of the static address list. The static address information is displayed. After you edit the information, click **Save**. After "Edit operation succeeded!" is displayed, the editing operation is complete.

- Deleting Static Addresses

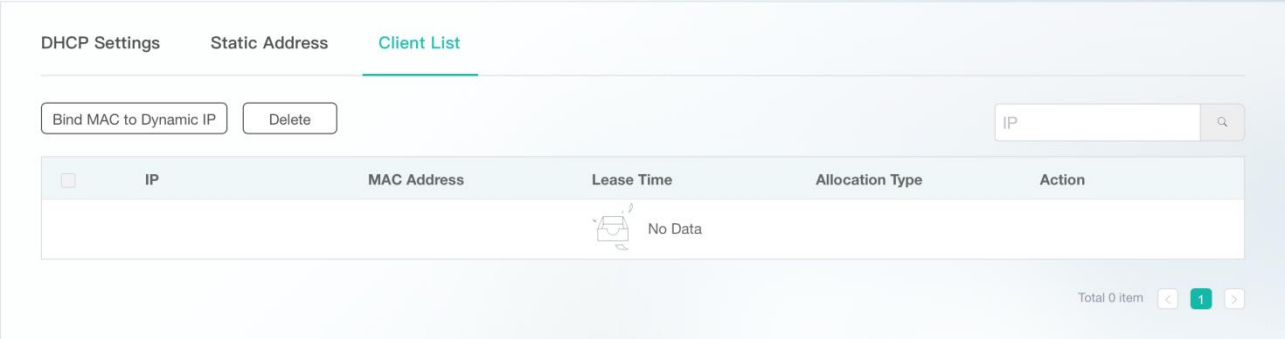
1. Select multiple records in the static address list and click **Delete** to batch delete the data records.

2. Click the delete icon of a static address in the **Action** column of the static address list. In the displayed deletion confirmation dialog box, click **OK**. After "Delete operation succeeded!" is displayed, the deletion is complete. The deleted static address is no longer displayed in the static address list.

Client List

Figure 53 shows the **Client List** page.

Figure 53 Client List



- IP Address-based Searches

  Enter an IP address in the search box and click the search icon to query the IP address.

- Bind MAC to Dynamic IP

  Select multiple records in **Client List** and click **Bind MAC to Dynamic IP** to bind MAC addresses to dynamic IP addresses.

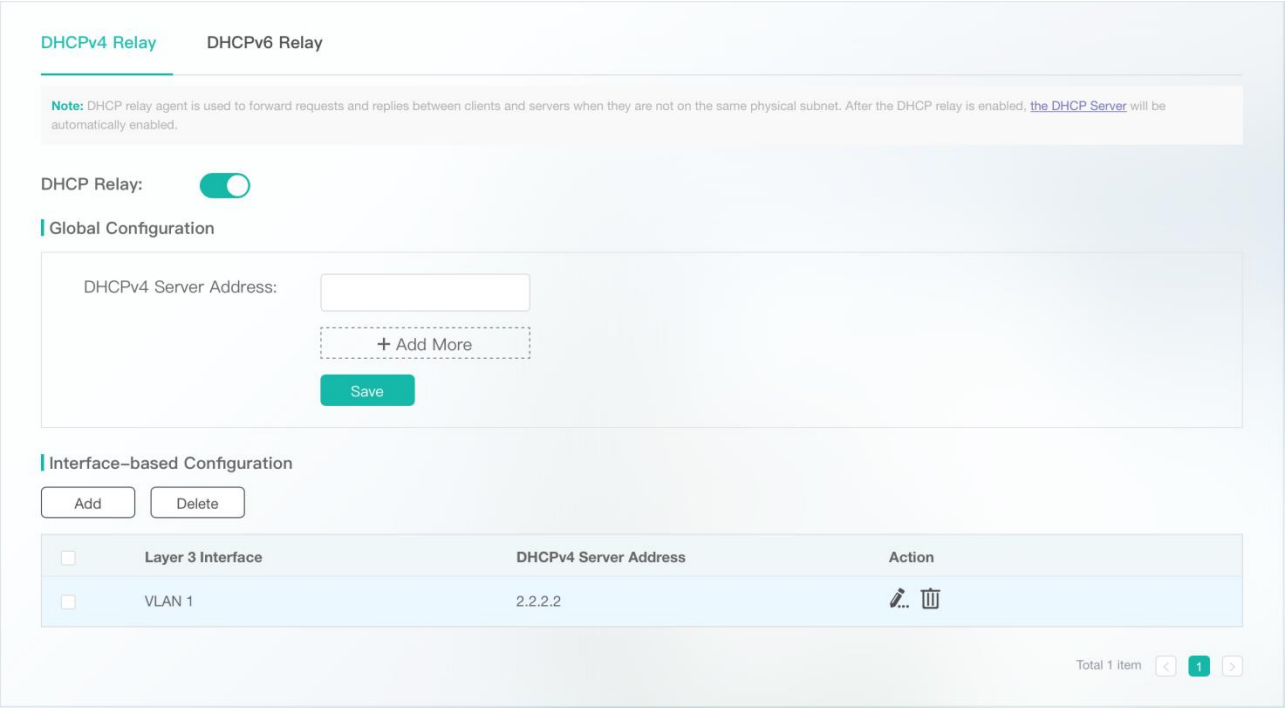
1.3.9.5 DHCP Relay

The **DHCP Relay** page consists of two parts: **DHCPv4 Relay** and **DHCPv6 Relay**.

DHCPv4 Relay

Figure 54 shows the **DCHPv4 Relay** page.

Figure 54 DCHPv4 Relay



- Enabling DHCP Relay

Enable the DHCP Relay function. After "Enable operation succeeded!" is displayed, the global DHCP function and DHCP Relay function are enabled.

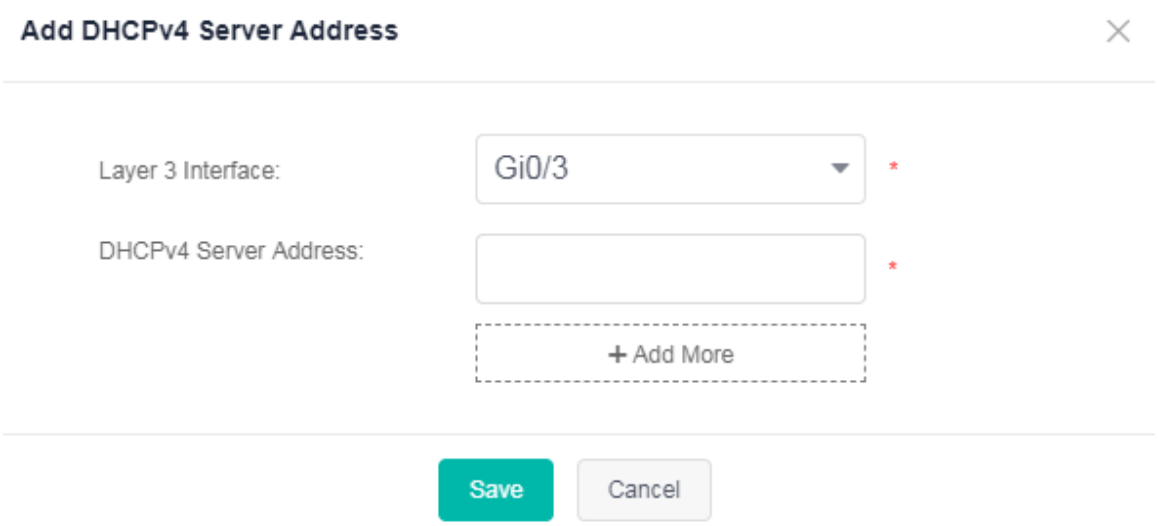
- Global Configuration

Multiple global DHCPv4 server addresses can be added. Content related to the DHCPv4 relay is not displayed when the DHCP Relay function is disabled and is displayed when DHCP Relay function is enabled.

- Interface-based Configuration

1. Click **Add**. The **Add** page is displayed. Specify **Layer 3 Interface** and **DHCPv4 Server Address**, and click **Save**. After "Add operation succeeded!" is displayed, the added DCHPv4 server address is displayed in **Interface-based Configuration List**.

Figure 55 Add DCHPv4 Server Address



2. Click the edit icon of a DHCPv4 server address in the **Action** column of **Interface-based Configuration List**. The DHCPv4 server address information is displayed. After you edit the information, click **Save**. After "Edit operation succeeded!" is displayed, the editing operation is complete.

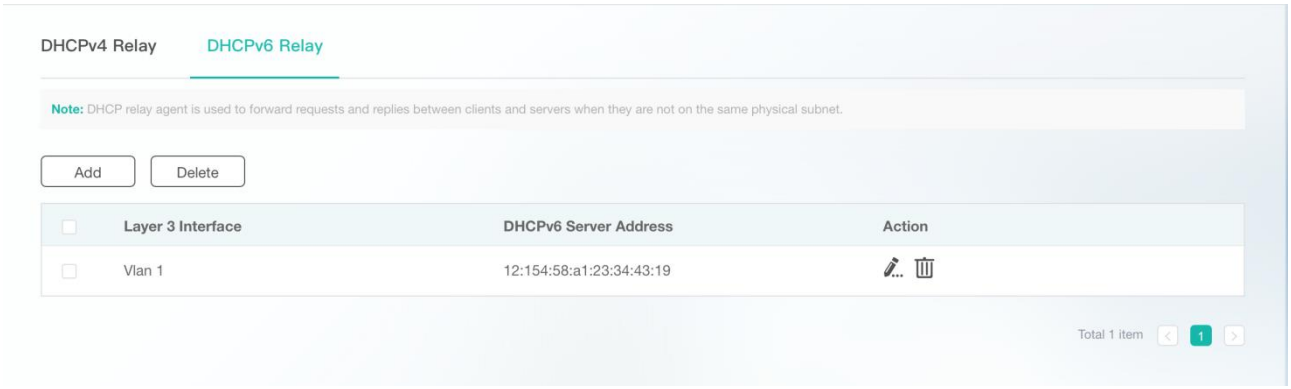
3. Select multiple records in **Interface-based Configuration List** and click **Delete** to batch delete the data records.

4. Click the delete icon of a DHCPv4 server address in the **Action** column of **Interface-based Configuration List**. In the displayed deletion confirmation dialog box, click **OK**. After "Delete operation succeeded!" is displayed, the deletion is complete. The deleted DHCPv4 server address is no longer displayed in **Interface-based Configuration List**.

DHCPv6 Relay

Figure 56 shows the **DCHPv6 Relay** page.

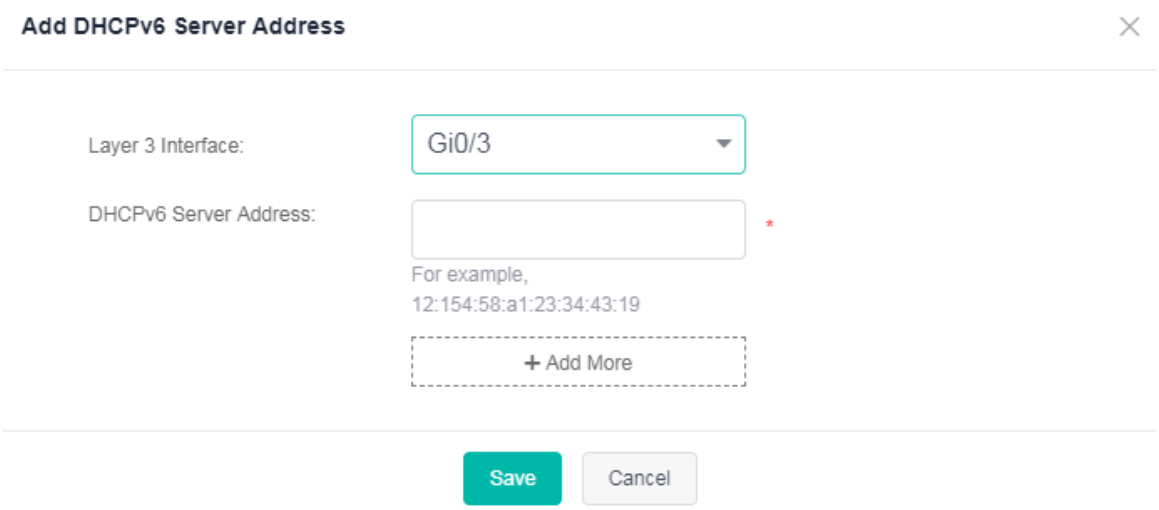
Figure 56 DCHPv6 Relay



- Adding DHCPv6 Server Addresses

Click **Add**. The **Add DHCPv6 Server Address** page is displayed. Specify **Layer 3 Interface** and **DHCPv6 Server Address**, and click **Save**. After "Add operation succeeded!" is displayed, the added DHCPv6 server address is displayed in **DHCPv6 Relay List**.

Figure 57 Add DCHPv6 Server Address



- Editing DHCPv6 Server Addresses

Click the edit icon of a DHCPv6 server address in the **Action** column of **DHCPv6 Relay List**. The DHCPv6 server address information is displayed. After you edit the information, click **Save**. After "Edit operation succeeded!" is displayed, the editing operation is complete.

- Deleting DHCPv6 Server Addresses

1. Select multiple records in **DHCPv6 Relay List** and click **Delete** to batch delete the data records.

2. Click the delete icon of a DHCPv6 server address in the **Action** column of **DHCPv6 Relay List**. In the displayed deletion confirmation dialog box, click **OK**. After "Delete operation succeeded!" is displayed, the deletion is complete. The deleted DHCPv6 server address is no longer displayed in **DHCPv6 Relay List**.

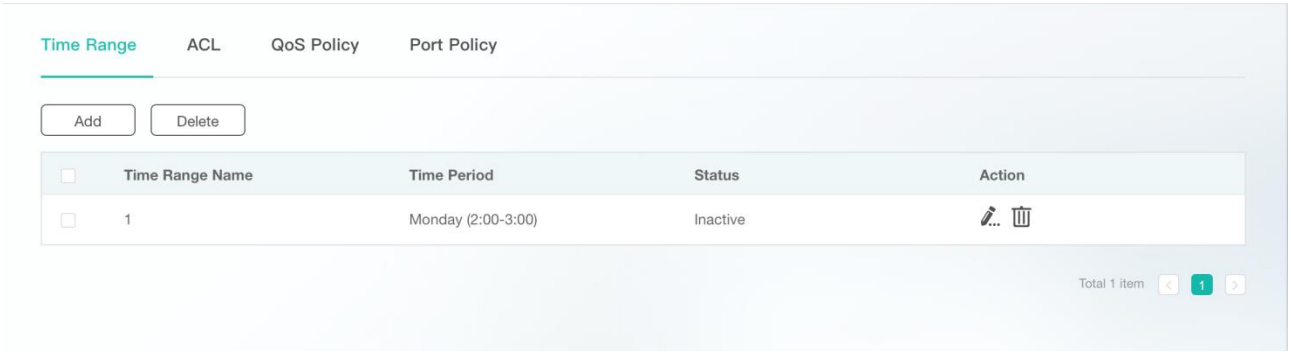
1.3.9.6 ACL & QoS

The **ACL & QoS** page consists of the four parts: **Time Range**, **ACL**, **QoS Policy**, and **Port Policy**.

Time Range

Figure 58 shows the **Time Range** page.

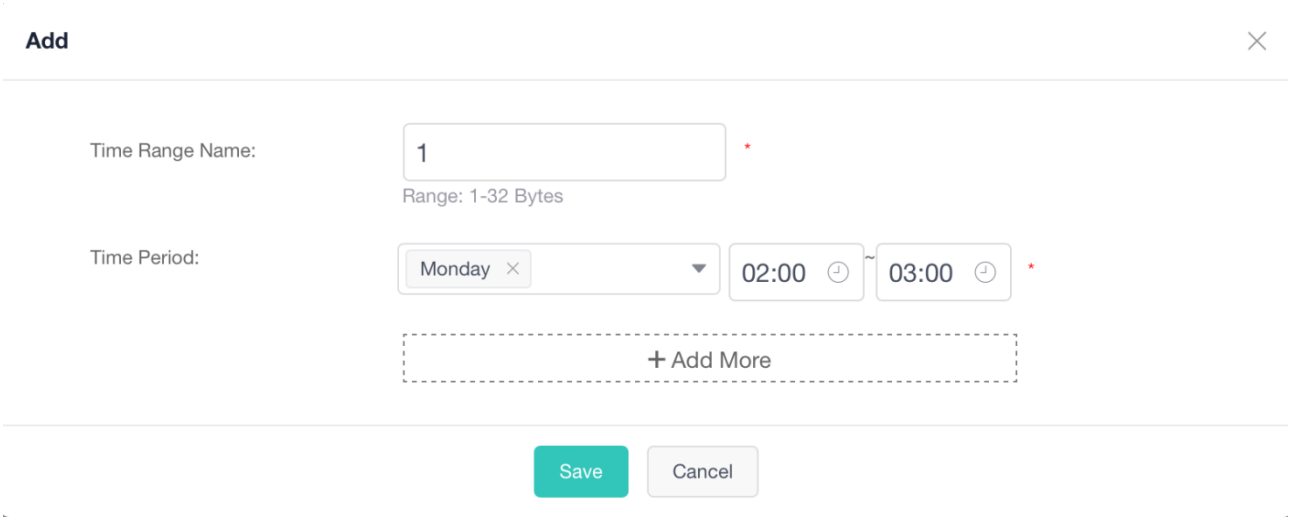
Figure 58 Time Range



- Adding Time Ranges

Click **Add**. The **Add** page is displayed. Specify **Time Range Name** and **Time Period**, and click **Save**. After "Add operation succeeded!" is displayed, the added time range is displayed in **Time Range List**.

Figure 59 Add



- Editing Time Ranges

Click the edit icon of a time range in the **Action** column of **Time Range List**. The time range information is displayed. After you edit the information, click **Save**. After "Edit operation succeeded!" is displayed, the editing operation is complete.

- Deleting Time Ranges

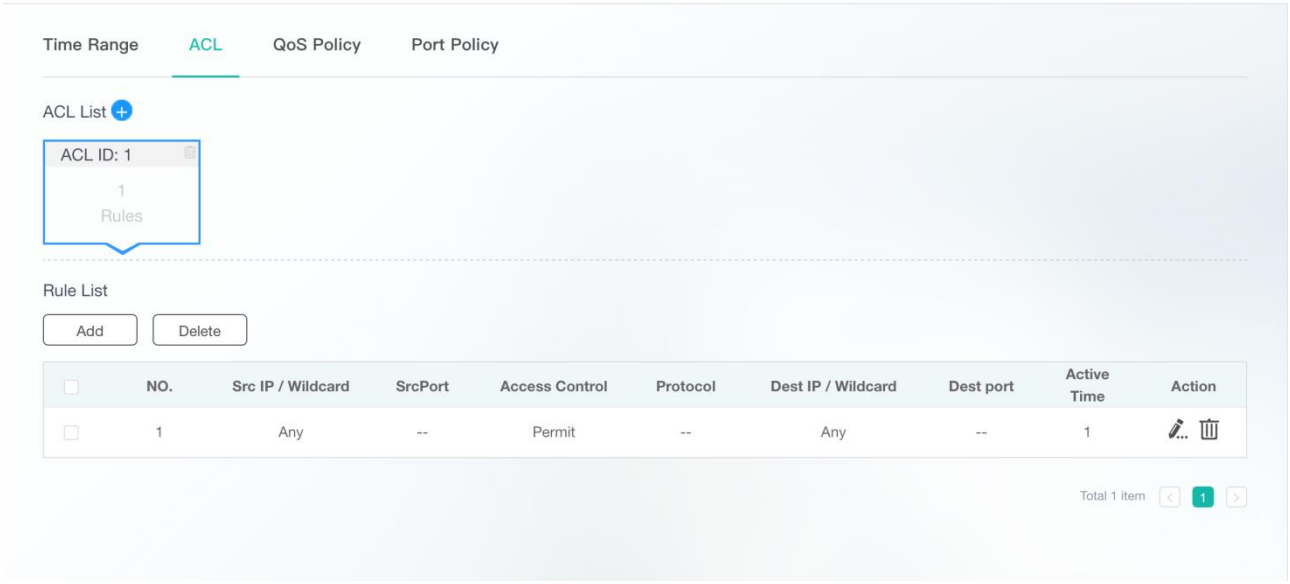
1. Select multiple records in **Time Range List** and click **Delete** to batch delete the data records.

2. Click the delete icon of a time range in the **Action** column of **Time Range List**. In the displayed deletion confirmation dialog box, click **OK**. After "Delete operation succeeded!" is displayed, the deletion is complete. The deleted time range is no longer displayed in **Time Range List**.

ACL

Figure 60 shows the **ACL** page.

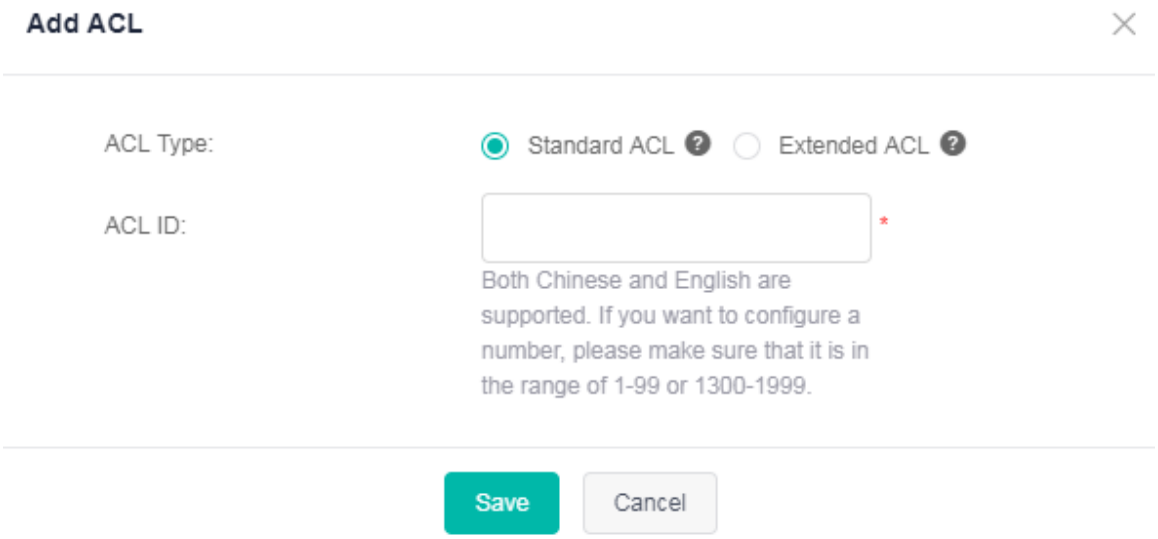
Figure 60 ACL



- Adding ACLs

Click the **+** icon on the right of **ACL List**. The **Add ACL** page is displayed. Specify **ACL Type** and **ACL ID**, and click **Save**. After "Add operation succeeded!" is displayed, the added ACL is displayed in **ACL List**.

Figure 61 Add ACL



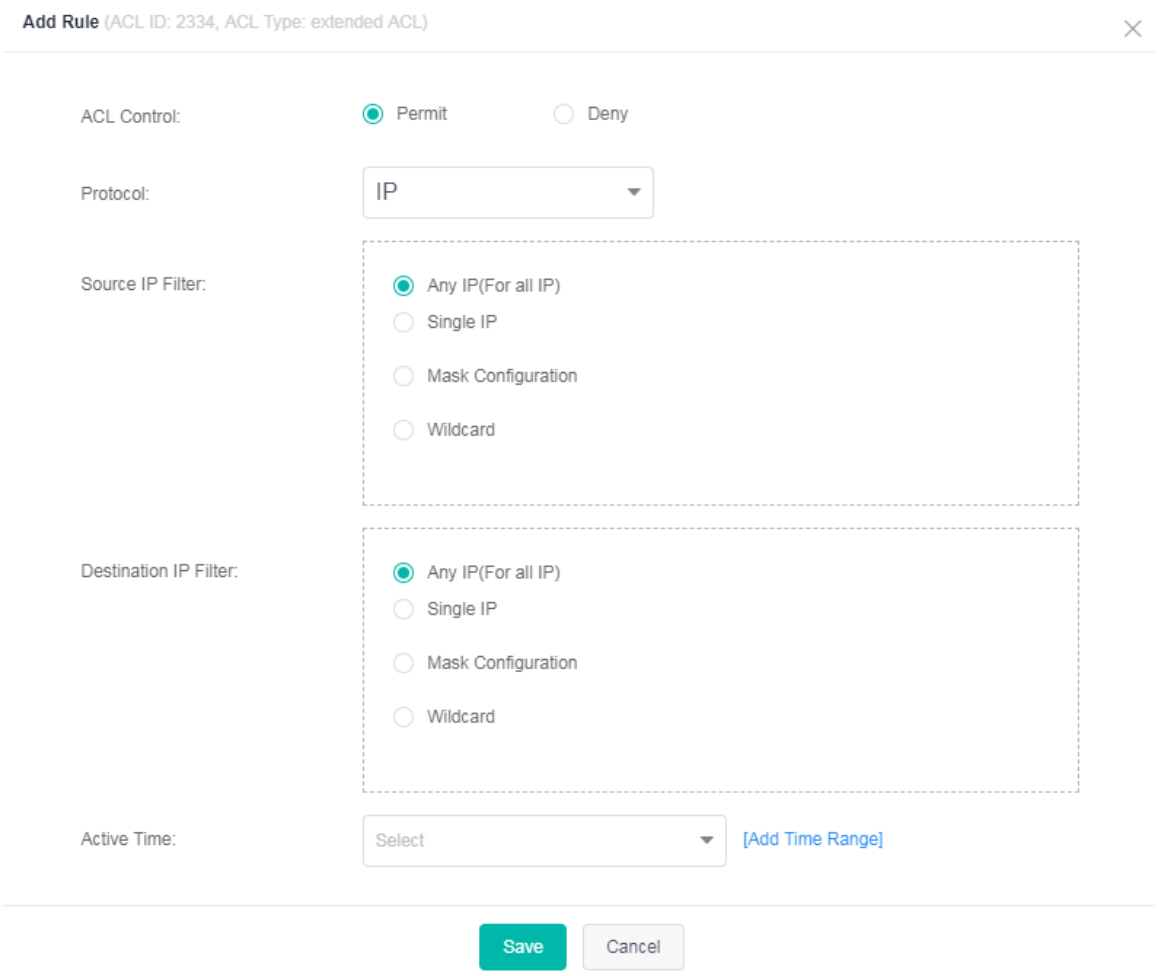
- Deleting ACLs

Click the delete icon on the right of **ACL ID**. After the deletion confirmation dialog box is displayed, click **OK**. After "Delete operation succeeded!" is displayed, the deletion is complete.

- Adding ACL Rules

Click **Add** in **Rule List**. The **Add Rule** page is displayed. Specify **ACL Control**, **Protocol**, **IP**, and **Active Time**, and click **Save**. After "Add operation succeeded!" is displayed, the added ACL rule is displayed in **Rule List**.

Figure 62 Add Rule



- Editing ACL Rules

Click the edit icon of an ACL rule in the **Action** column of **Rule List**. The ACL rule information is displayed. After you edit the information, click **Save**. After "Edit operation succeeded!" is displayed, the editing operation is complete.

- Deleting ACL Rules

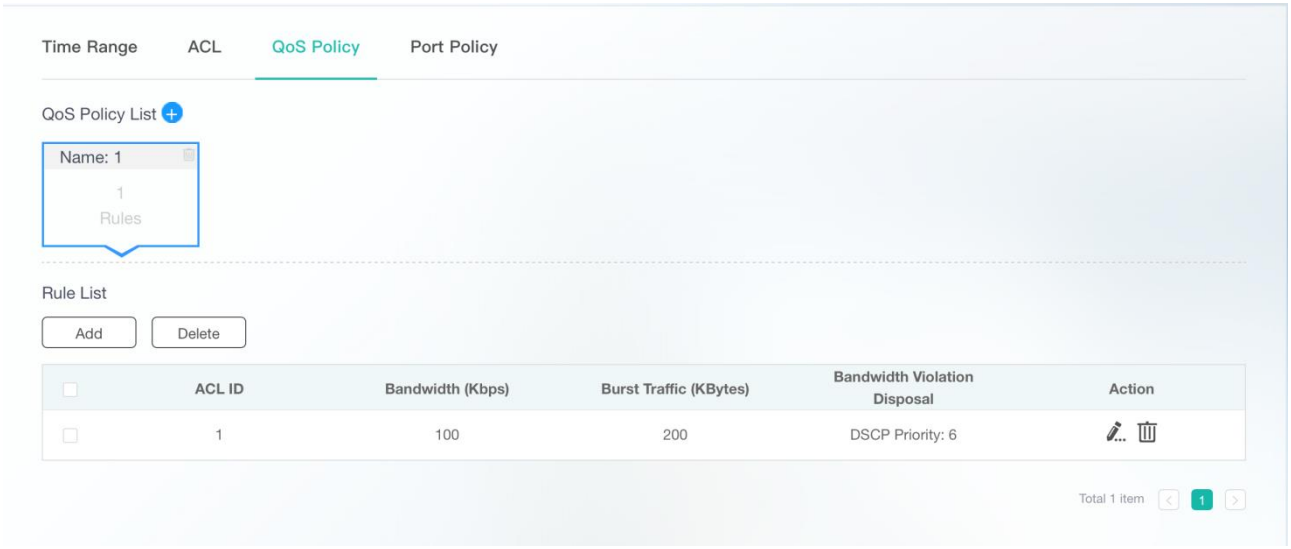
1. Select multiple records in **Rule List** and click **Delete** to batch delete the data records.

2. Click the delete icon of an ACL rule in the **Action** column of **Rule List**. In the displayed deletion confirmation dialog box, click **OK**. After "Delete operation succeeded!" is displayed, the deletion is complete. The deleted ACL rule is no longer displayed in **Rule List**.

QoS Policy

Figure 63 shows the **QoS Policy** page.

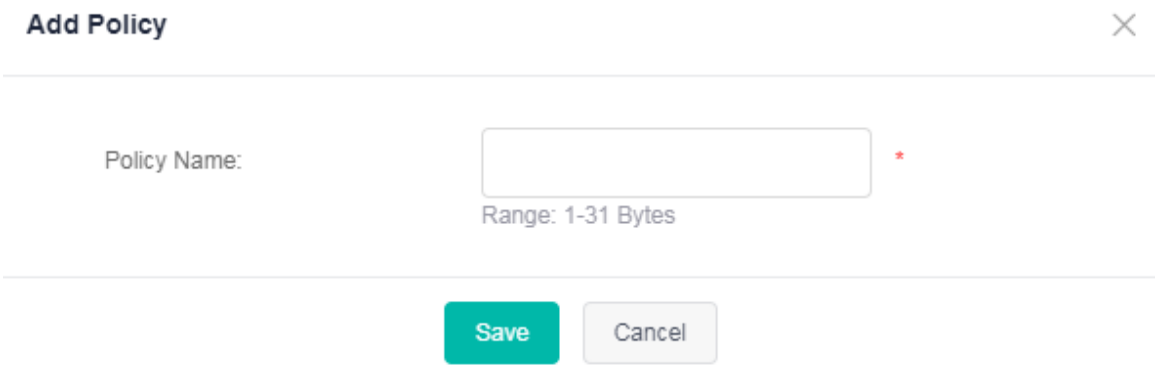
Figure 63 QoS Policy



- Adding QoS Policies

Click the **+** icon on the right of **QoS Policy List**. The **Add Policy** page is displayed. Specify **Policy Name**, and click **Save**. After "Add operation succeeded!" is displayed, the added QoS policy is displayed in **QoS Policy List**.

Figure 64 Add Policy



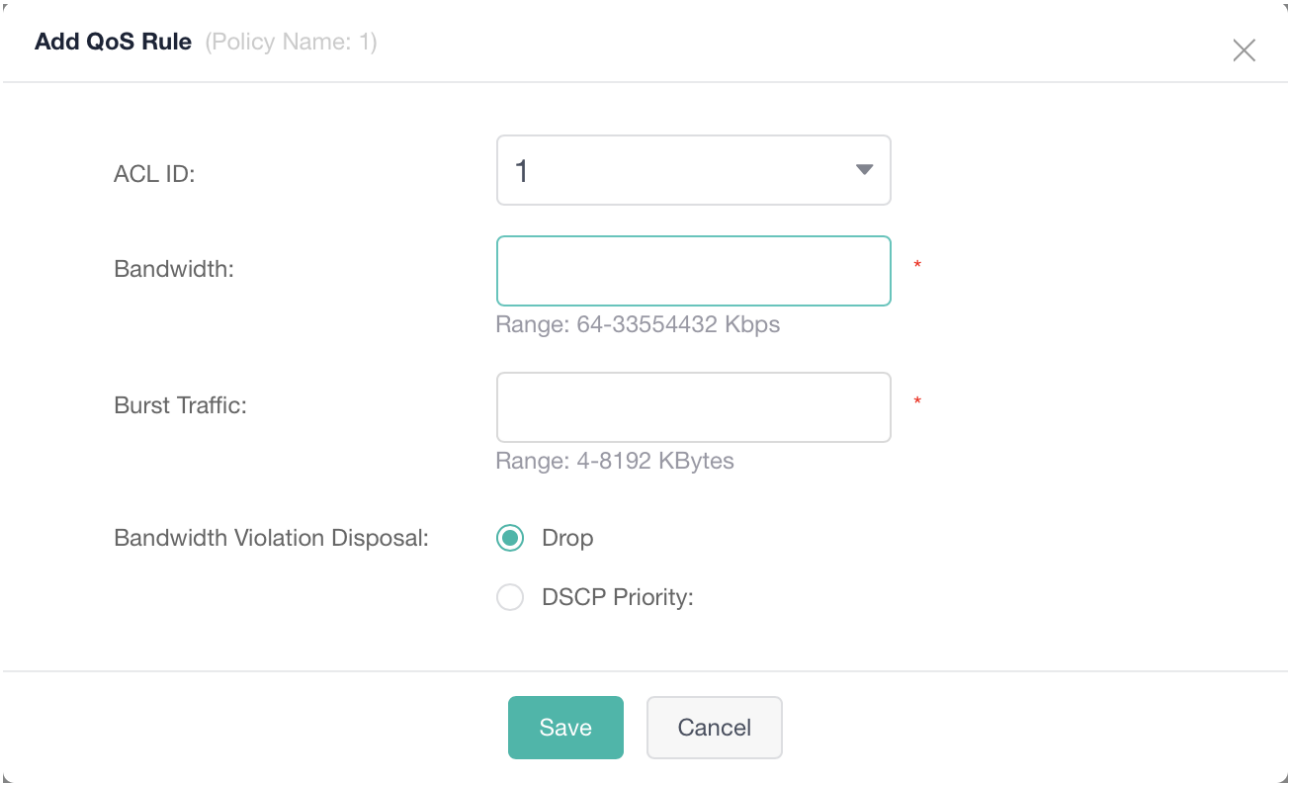
- Deleting QoS Policies

Click the delete icon on the right of **Name** of an existing QoS policy. After the deletion confirmation dialog box is displayed, click **OK**. After "Delete operation succeeded!" is displayed, the deletion is complete.

- Adding QoS Rules

Click **Add** in **Rule List**. The **Add QoS Rule** page is displayed. Specify **ACL ID**, **Bandwidth**, **Burst Traffic**, and **Bandwidth Violation Disposal**, and click **Save**. After "Add operation succeeded!" is displayed, the added QoS rule is displayed in **Rule List**.

Figure 65 Add QoS Rule



- Editing QoS Rules

Click the edit icon of a QoS rule in the **Action** column of **Rule List**. The QoS rule information is displayed. After you edit the information, click **Save**. After "Edit operation succeeded!" is displayed, the editing operation is complete.

- Deleting QoS Rules

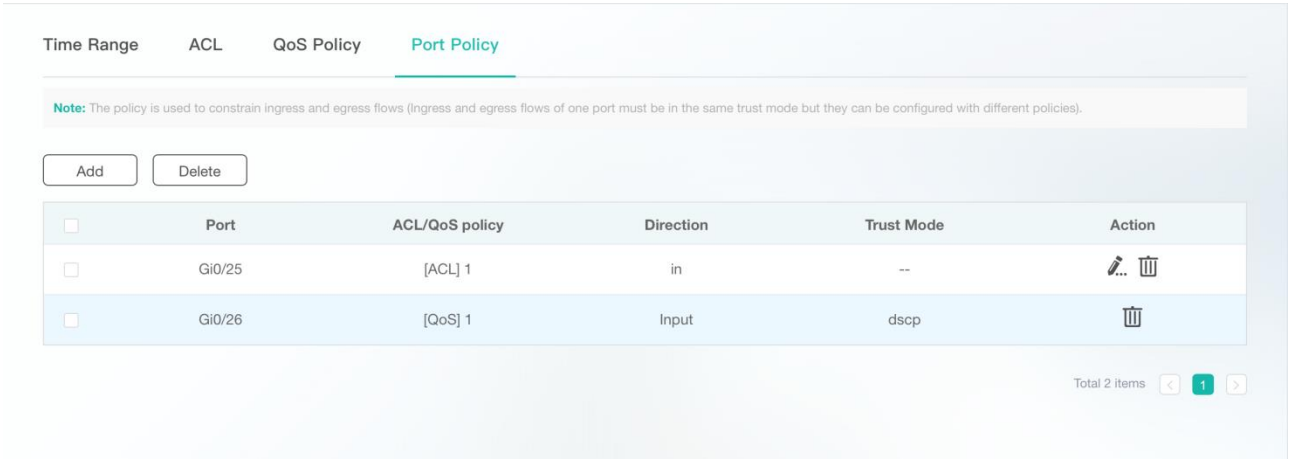
1. Select multiple records in **Rule List** and click **Delete** to batch delete the data records.

2. Click the delete icon of a QoS rule in the **Action** column of **Rule List**. In the displayed deletion confirmation dialog box, click **OK**. After "Delete operation succeeded!" is displayed, the deletion is complete. The deleted QoS rule is no longer displayed in **Rule List**.

Port Policy

Figure 66 shows the **Port Policy** page.

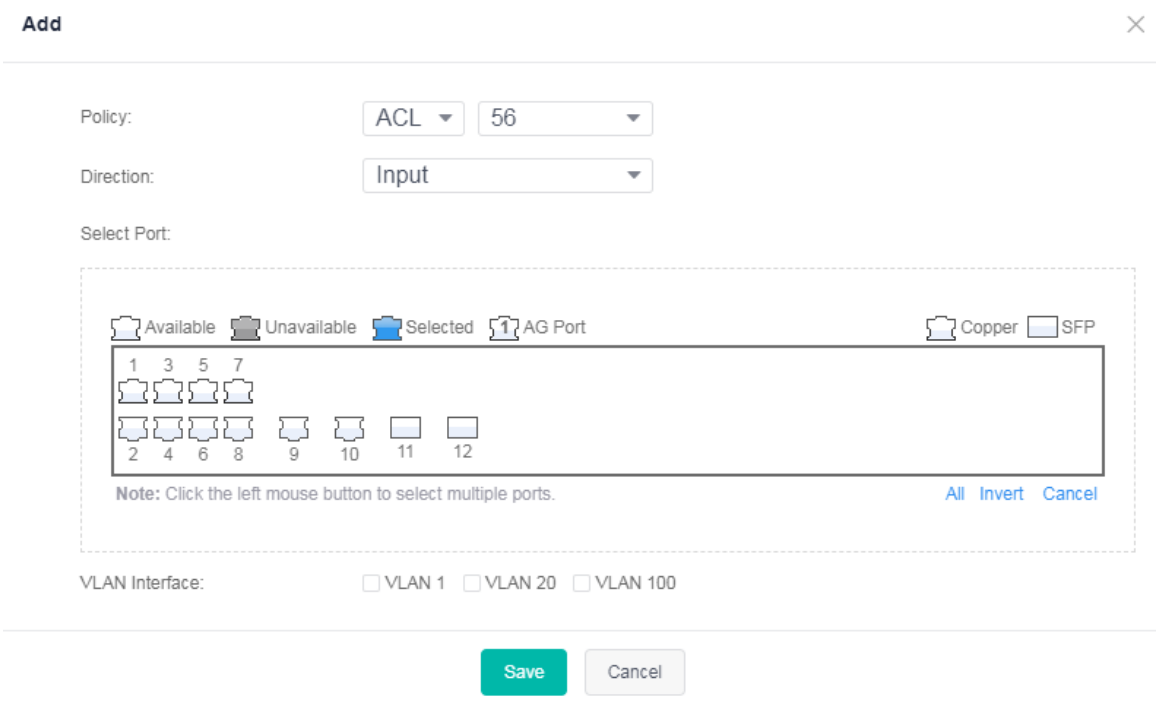
Figure 66 Port Policy



- Adding Port Policies

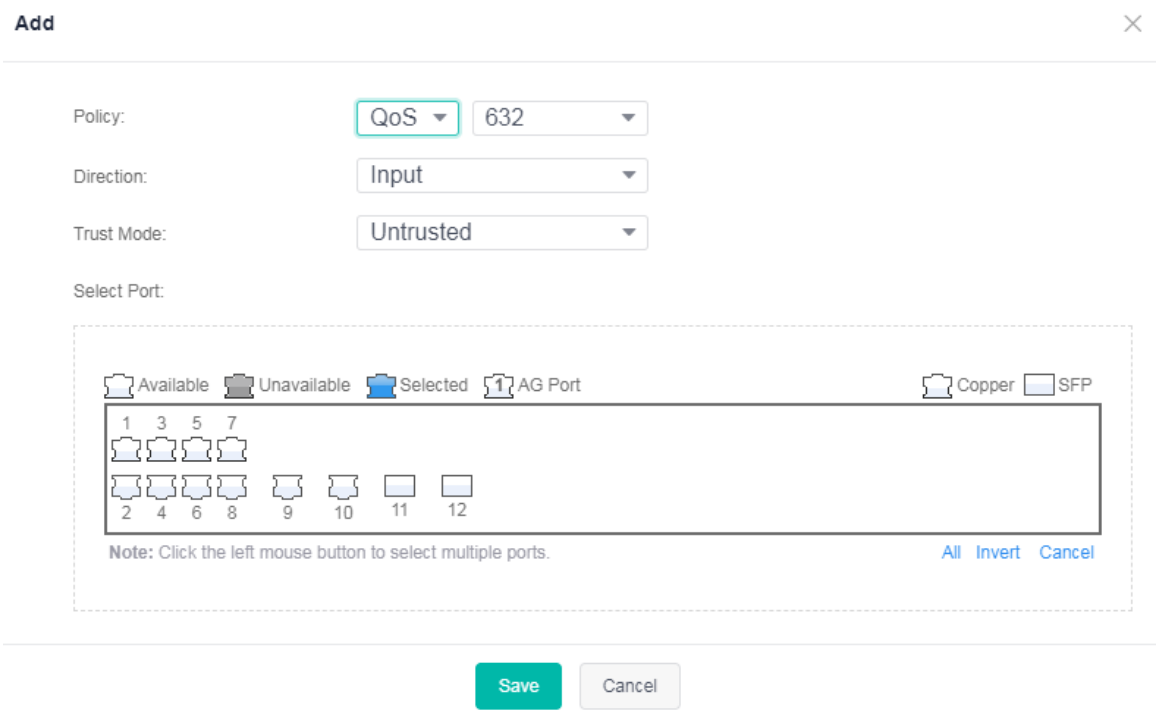
1. Click **Add**. The **Add** page is displayed. If **ACL** is selected for **Policy**, specify **Direction**, **Port** and **VLAN Interface** (optional), and click **Save**. After "Add operation succeeded!" is displayed, the added port policy is displayed in **Port Policy**.

Figure 67 Adding Port Policy Based ACL



2. Click **Add**. The **Add** page is displayed. If **QoS** is selected for **Policy**, specify **Direction**, **Trust Mode**, and **Port**, and click **Save**. After "Add operation succeeded!" is displayed, the added port policy is displayed in **Port Policy**.

Figure 68 Adding Port Policy Based QoS



- Editing Port Policies

Only ACL-based port policies can be edited.

Click the edit icon of a port policy in the **Action** column of **Port Policy List**. The port policy information is displayed. After you edit the information, click **Save**. After "Edit operation succeeded!" is displayed, the editing operation is complete.

- Deleting Port Policies

1. Select multiple records in **Port Policy List** and click **Delete** to batch delete the data records.

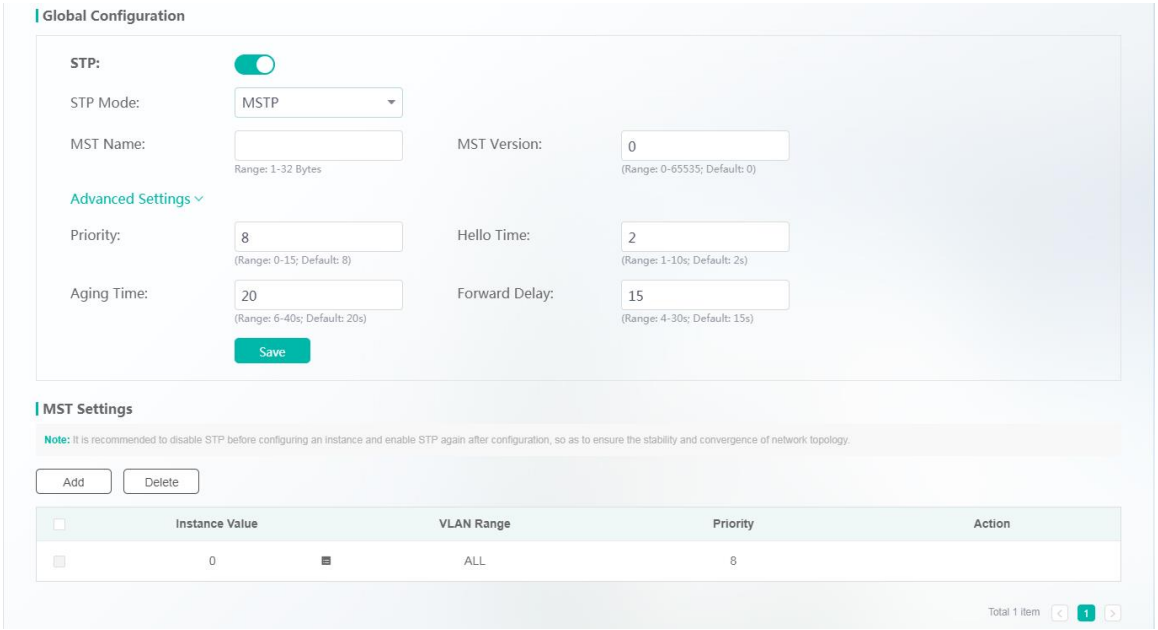
2. Click the delete icon of a port policy in the **Action** column of **Port Policy List**. In the displayed deletion confirmation dialog box, click **OK**. After "Delete operation succeeded!" is displayed, the deletion is complete. The deleted port policy is no longer displayed in **Port Policy**.

1.3.9.7 STP & RLDP

The **STP & RLDP** page consists of three parts: **Global Configuration**, **STP Port Settings**, and **RLDP**.

Global Configuration

Figure 69 Global Configuration

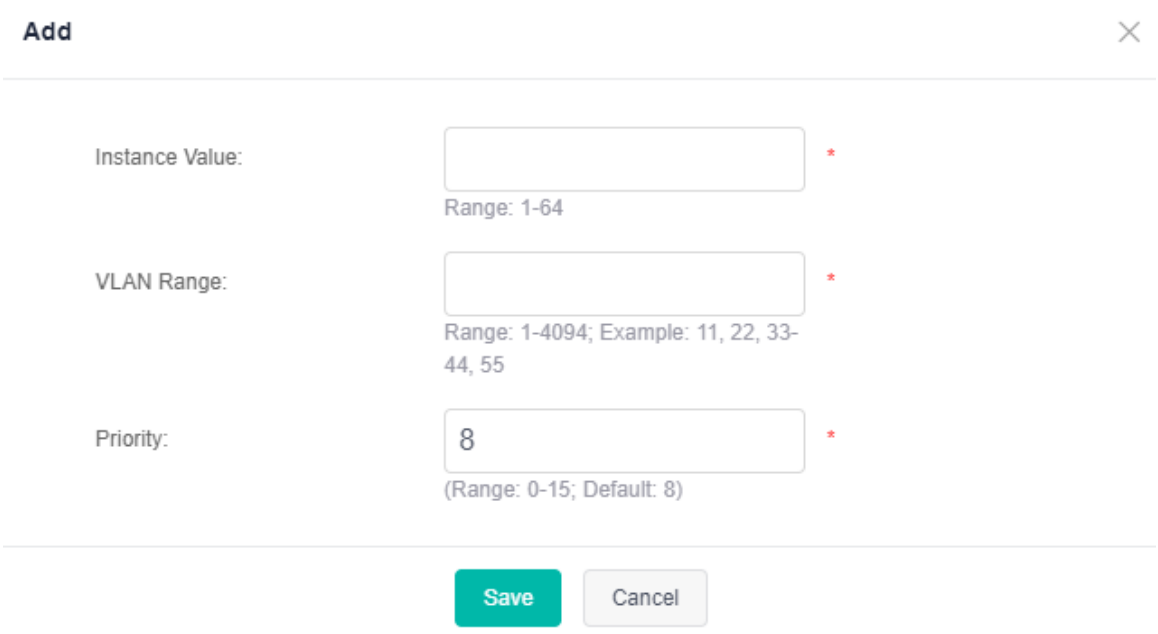


You can configure global STP parameters. When **MSTP** is selected for **STP Mode**, you can perform MST settings.

- Adding Instances

Click **Add** in **MST Settings**. The **Add** page is displayed.

Figure 70 Add



Specify **Instance Value**, **VLAN Range**, and **Priority**, and click **Save**. After "Add operation succeeded!" is displayed, the instance configuration information is displayed in **Instance List**.

- Editing Instances

Click the edit icon of an instance in the **Action** column of **Instance List**. The instance information is displayed. After you edit the information, click **Save**. After "Edit operation succeeded!" is displayed, the editing operation is complete.

- Deleting Instances

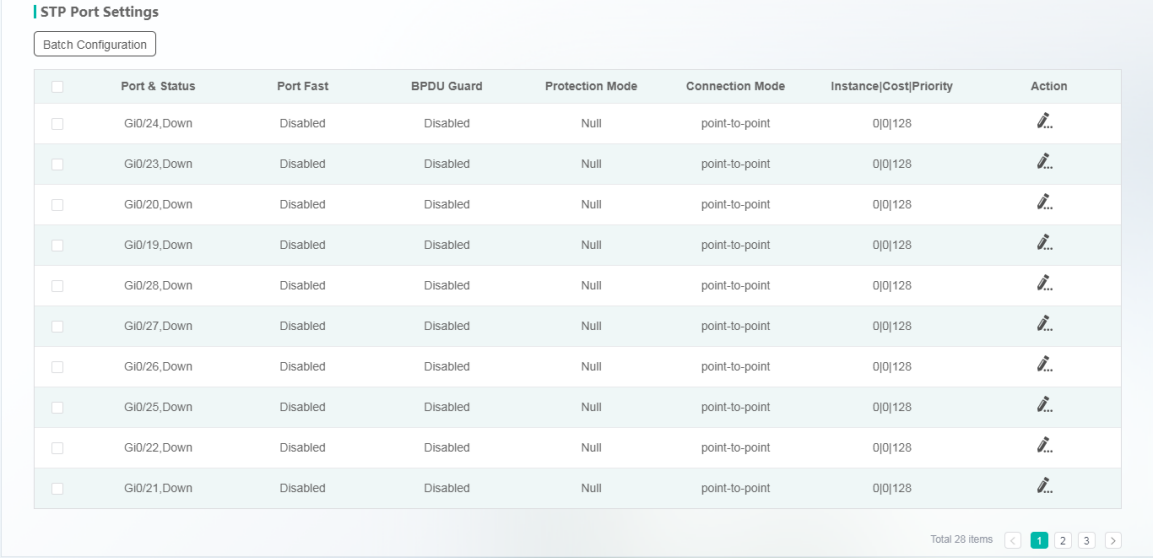
1. Select multiple records in **Instance List** and click **Delete** to batch delete the data records.

2. Click the delete icon of an instance in the **Action** column of **Instance List**. In the displayed deletion confirmation dialog box, click **OK**. After "Delete operation succeeded!" is displayed, the deletion is complete.

Instance 0 is the default instance and cannot be edited or deleted.

STP Port Settings

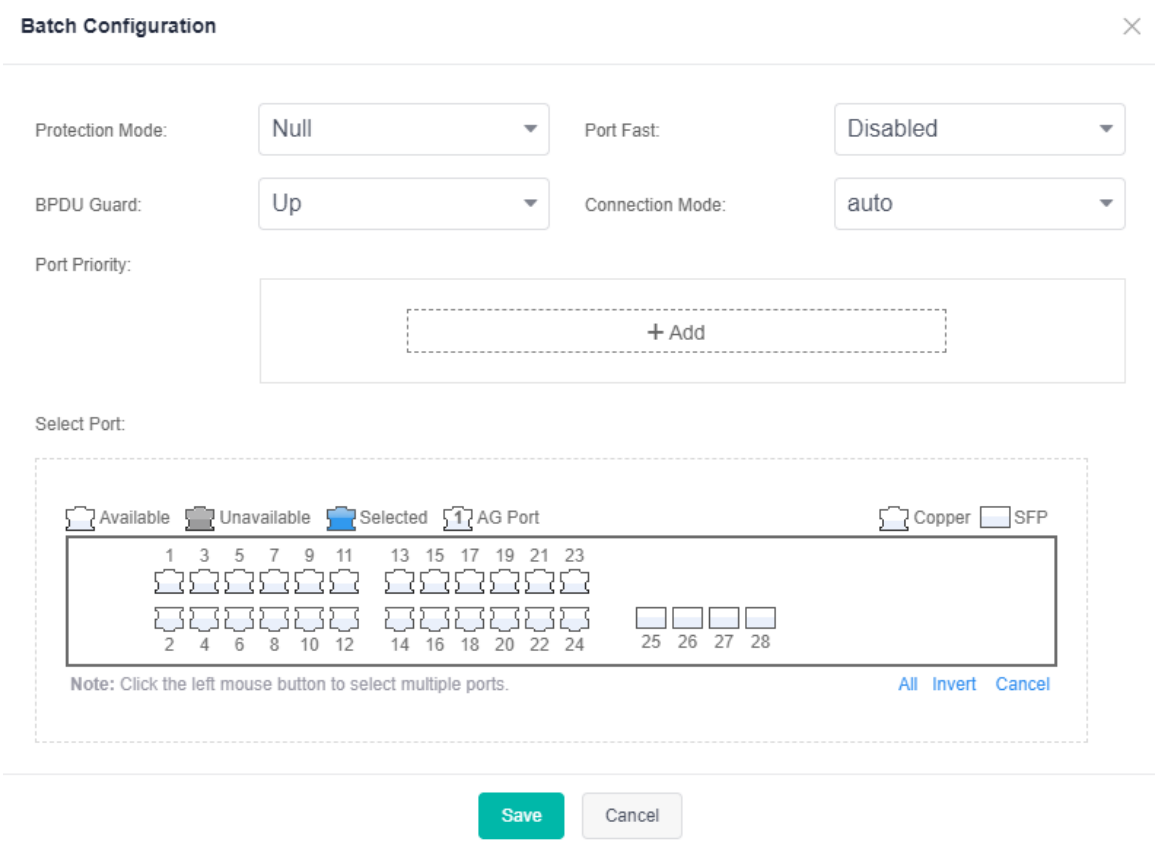
Figure 71 STP Port Settings



- Batch Configuration

Click **Batch Configuration**. The **Batch Configuration** page is displayed. Specify **Protection Mode**, **Port Fast**, **BPDU Guard**, **Connection Mode**, and **Port Priority** and select ports for batch configuration.

Figure 72 Batch Configuration

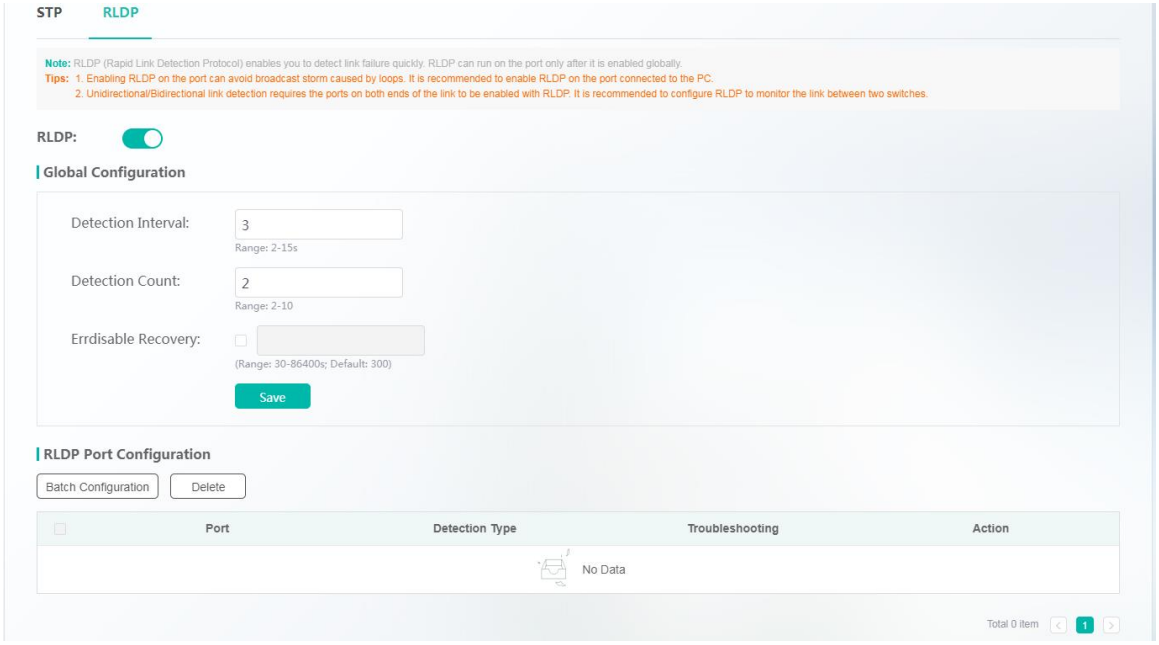


- Editing Settings

Click the edit icon of an STP port in the **Action** column of **STP Port Settings**. The port information is displayed. After you edit the information, click **Save**. After "Edit operation succeeded!" is displayed, the editing operation is complete.

RLDP

Figure 73 RLDP



1. Global Configuration

Enable the RLDP function. After "Enable operation succeeded!" is displayed, the global RLDP function is enabled. Disable the RLDP function. After "Disable operation succeeded!" is displayed, the global RLDP function is disabled.

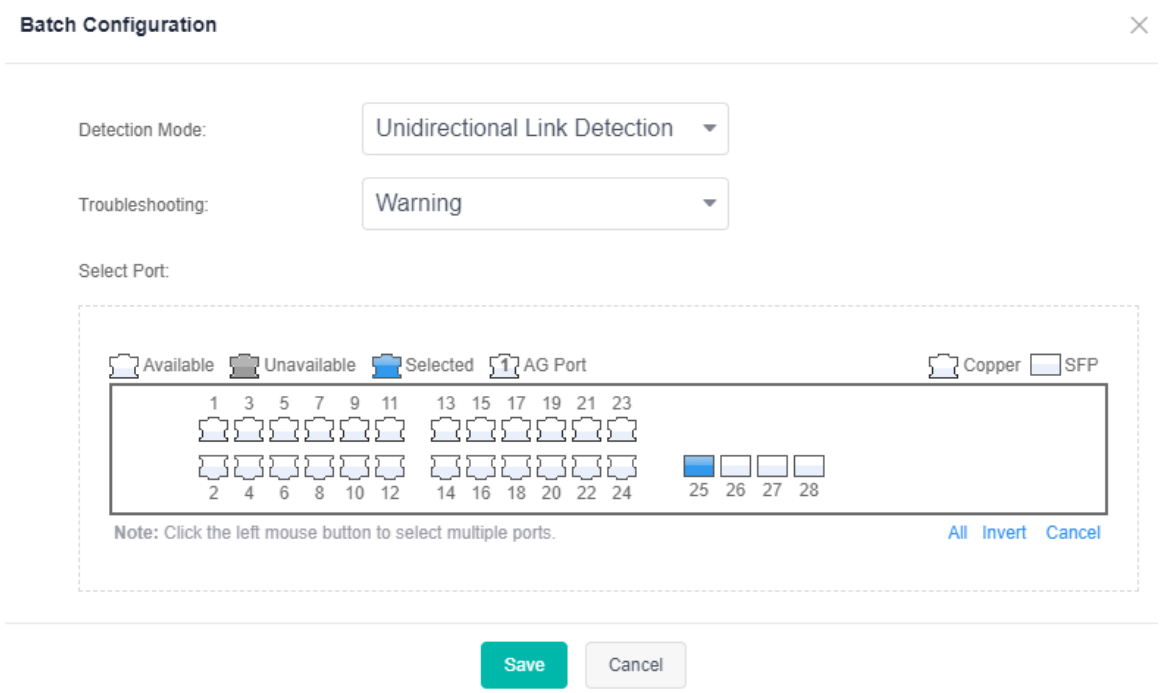
When the RLDP function is enabled, edit **Detection Interval**, **Detection Count**, and **Errdisable Recovery**, and click **Save**. After "Save operation succeeded!" is displayed, the configuration is complete.

2. RLDP Port Configuration

- Batch Configuration

Click **Batch Configuration**. The **Batch Configuration** page is displayed. Specify **Detection Mode**, **Troubleshooting**, and **Port**, and click **Save**. After "Add operation succeeded!" is displayed, selected ports can be configured in batches, and the configuration information is displayed in **RLDP Port Configuration**.

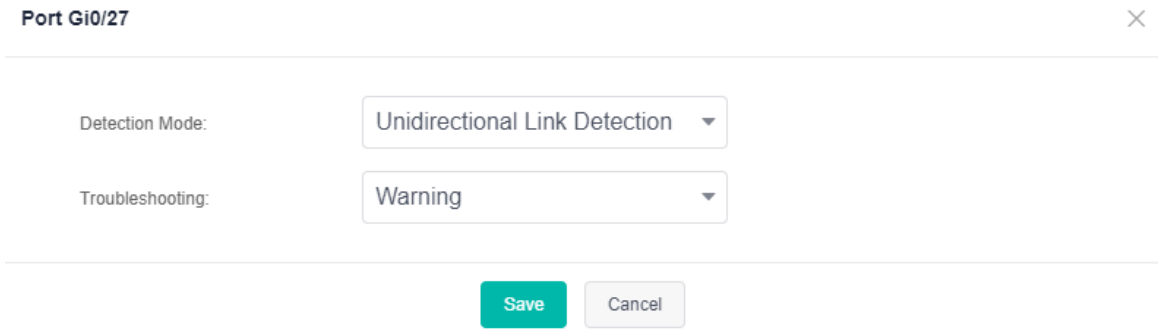
Figure 74 Batch Configuration



3. Editing RLDP Port Settings

Click the edit icon of an RLDP port in the **Action** column of **RLDP Port Configuration**. The RLDP port information is displayed. After you edit the information, click **Save**. After "Edit operation succeeded!" is displayed, the editing operation is complete.

Figure 75 RLDP Port List



4. Deleting RLDP Port Settings

1. Select multiple records in **RLDP Port Configuration** and click **Delete** to batch delete the data records.

2. Click the edit icon of an RLDP port in the **Action** column of **RLDP Port Configuration**. In the displayed deletion confirmation dialog box, click **OK**. After "Delete operation succeeded!" is displayed, the deletion is complete.

1.3.10 Security Settings

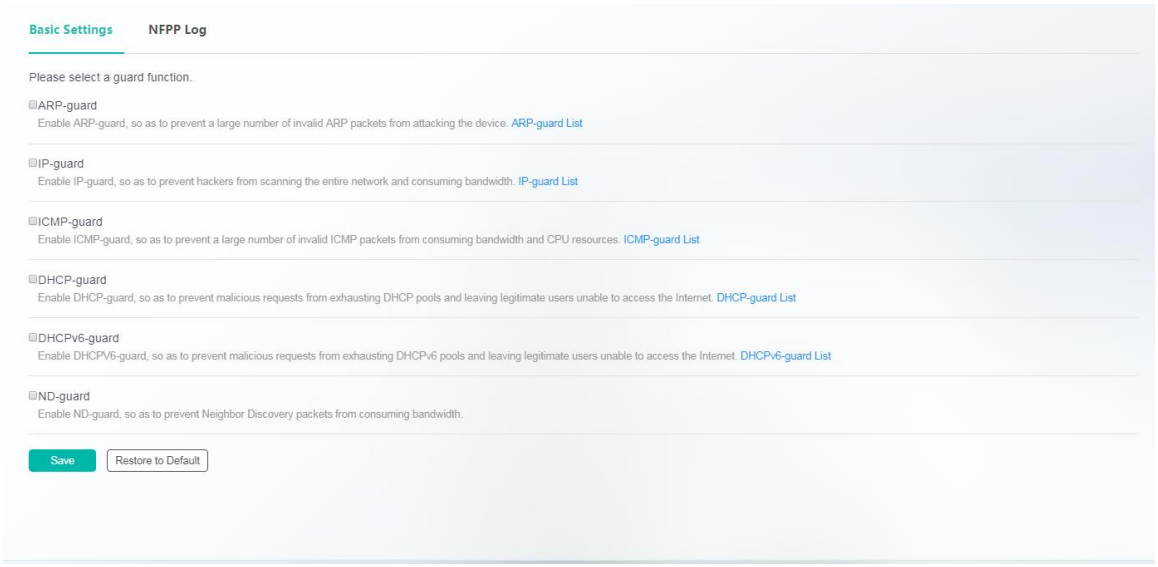
The first-level menu **More** includes three second-level menus: **Network Settings**, **Security Settings**, and **System Settings**.

This section mainly describes **Security Settings**.

1.3.10.1 NFPP

Basic Settings

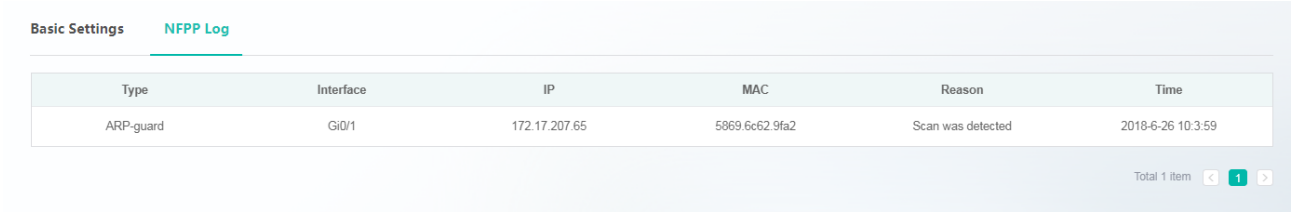
Figure 76 Basic Settings



Different guard functions can be enabled or disabled. When a guard function is disabled, the disablement confirmation dialog box is displayed. Click **OK** and **Save**. After "Save operation succeeded!" is displayed, the configuration is complete. To restore the default settings, click **Restore to Default**.

NFPP Log

Figure 77 NFPP Log

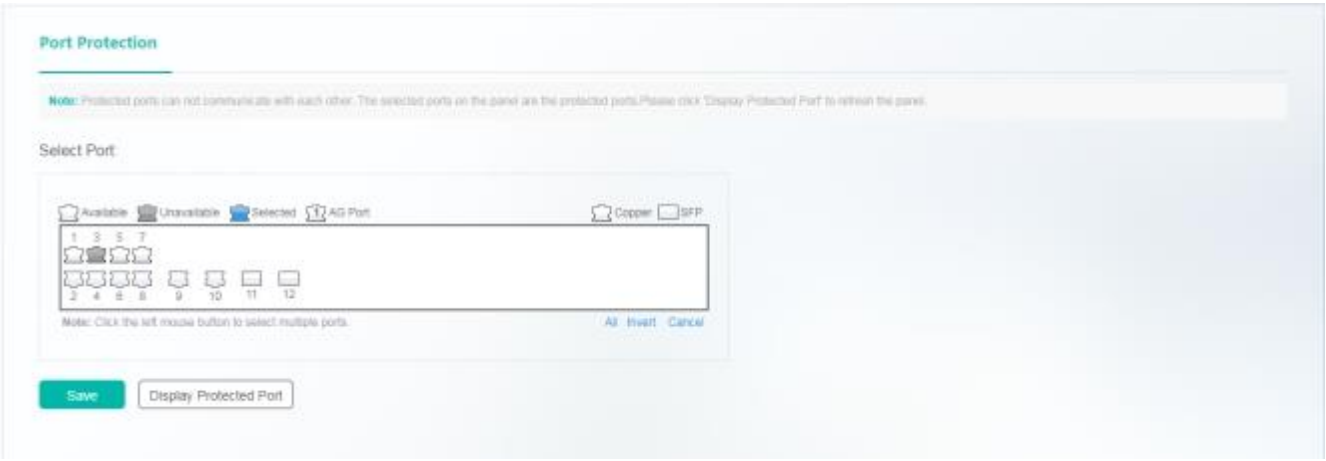


After NFPP guard functions are enabled and a device is attacked, the corresponding attack record is displayed in logs.

1.3.10.2 Port Protection

Figure 78 shows the **Port Protection** page.

Figure 78 Port Protection

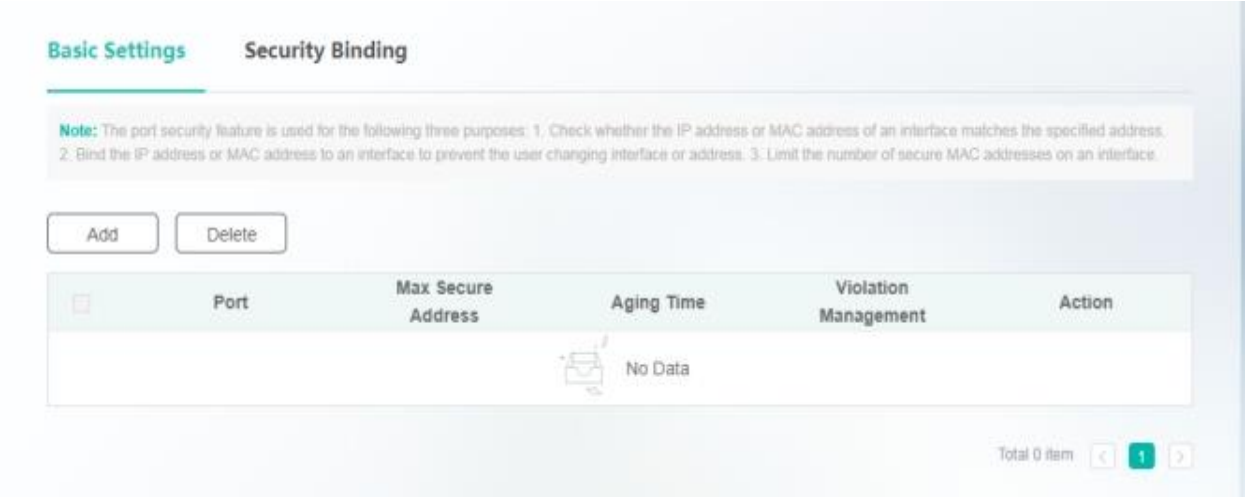


Select a port on the panel and click **Save** to set a port as a protection port. After the confirmation dialog box is displayed, click **OK**. After "Save operation succeeded!" is displayed, the configuration is complete.

1.3.10.3 Port Security

Basic Settings

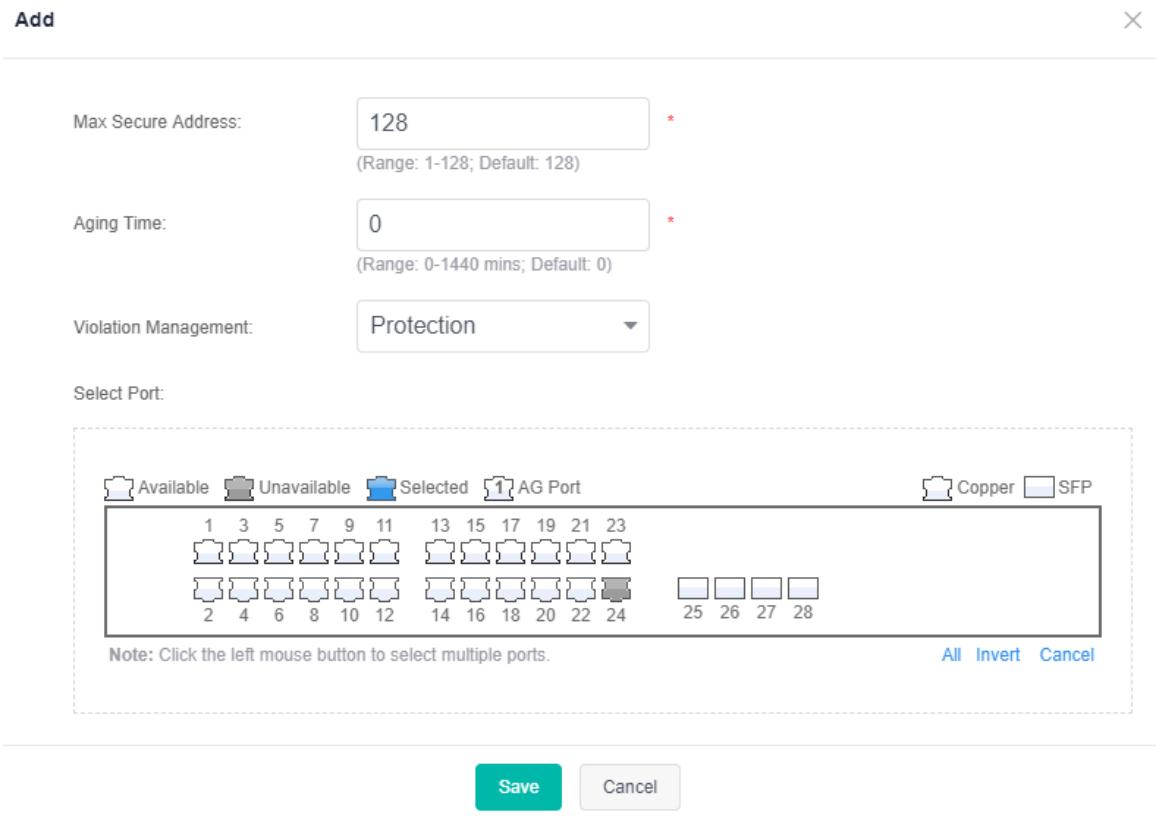
Figure 79 Basic Settings



- Adding Security Ports

Click **Add**, specify **Max Secure Address**, **Aging Time**, and **Violation Management**, select a port, and click **Save**. After "Add operation succeeded!" is displayed, the added port is displayed in the security port list.

Figure 80 Add



- Editing Security Ports

Click the edit icon of a security port in the **Action** column of the security port list. The security port information is displayed. After you edit the information, click **Save**. After "Edit operation succeeded!" is displayed, the editing operation is complete.

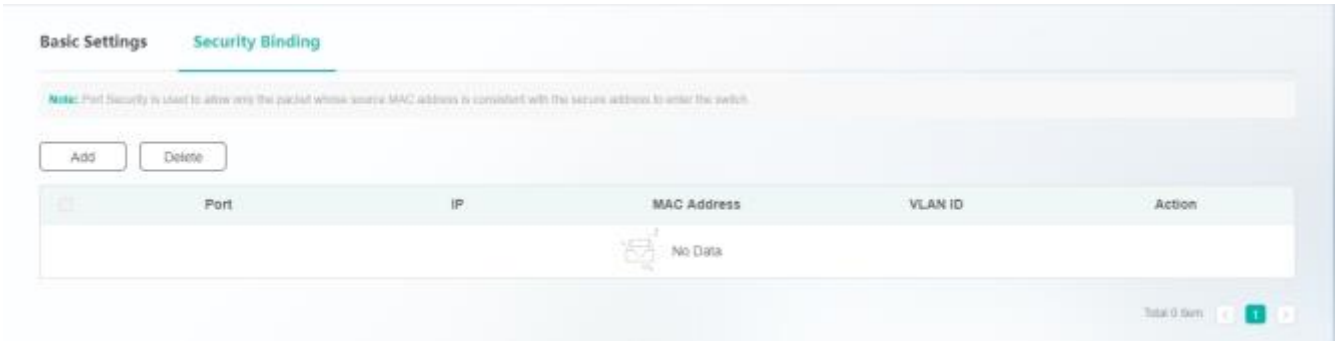
- Deleting Security Ports

1. Select multiple records in the security port list and click **Delete** to batch delete the data records.

2. Click the delete icon of a security port in the **Action** column of the security port list. In the displayed deletion confirmation dialog box, click **OK**. After "Delete operation succeeded!" is displayed, the deletion is complete.

Security Binding

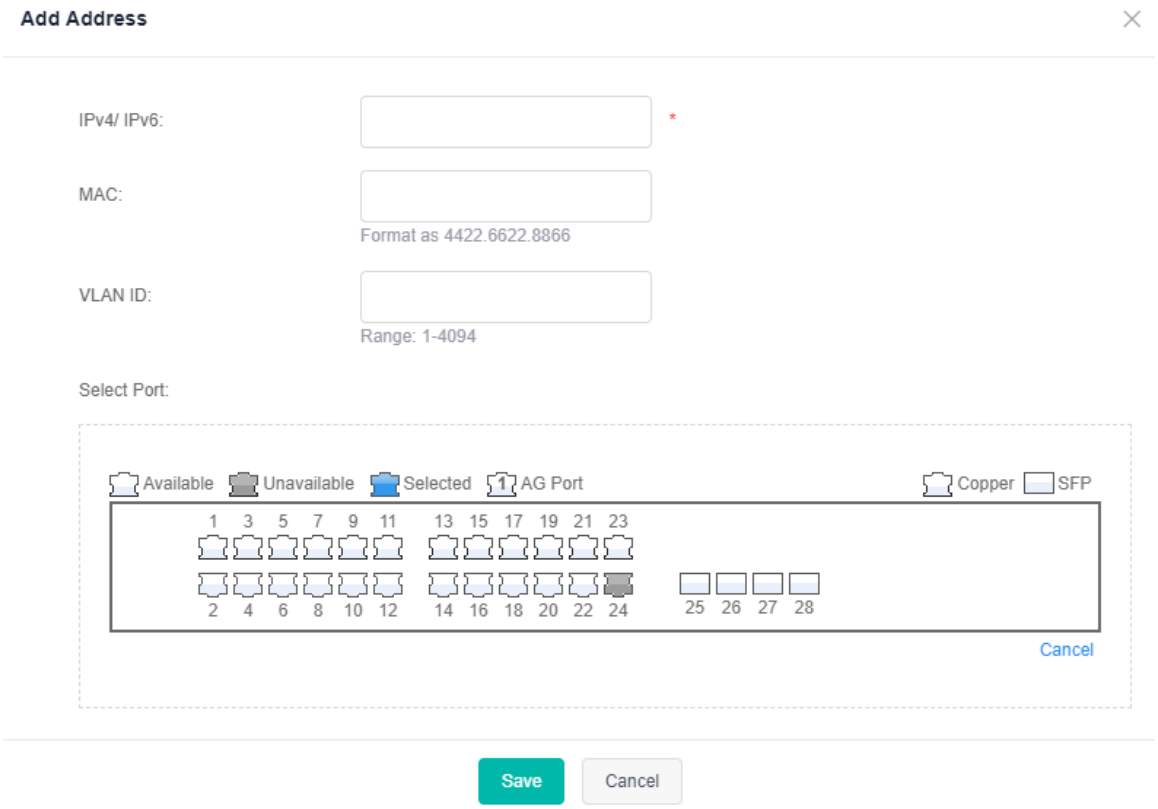
Figure 81 Security Binding



- Adding Addresses

Click **Add**. The **Add Address** page is displayed. Specify **IPv4/IPv6**, **MAC**, and **VLAN ID**, select a port, and click **Save**. After "Add operation succeeded!" is displayed, the added address is displayed in the security binding address list.

Figure 82 Add Address



- Editing Security Binding Addresses

Click the edit icon of a security binding address in the **Action** column of the security binding address list. The binding information is displayed. After you edit the information, click **Save**. After "Edit operation succeeded!" is displayed, the editing operation is complete.

- Deleting Security Binding Addresses

1. Select multiple records in the security binding address list and click **Delete** to batch delete the data records.

2. Click the delete icon of a security binding address in the **Action** column of the security binding address list. In the displayed deletion confirmation dialog box, click **Save**. After "Delete operation succeeded!" is displayed, the deletion is complete.

1.3.10.4 IP Source Guard

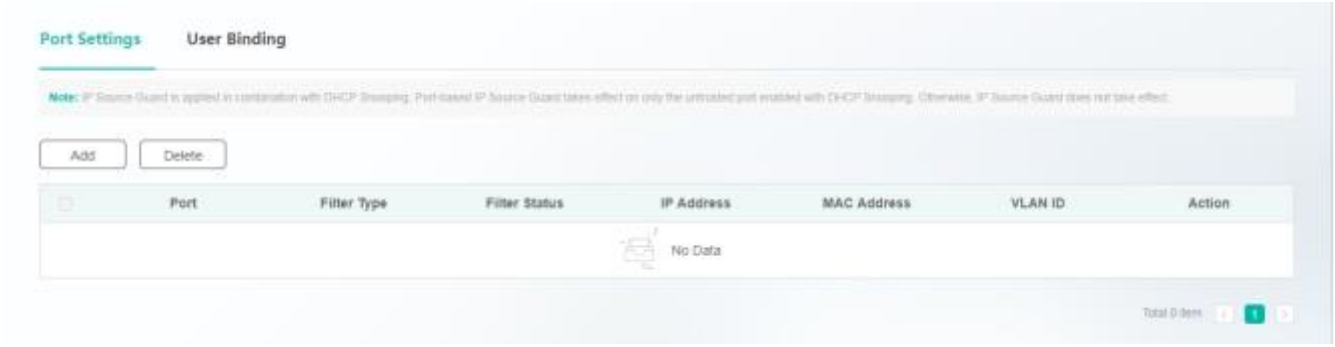
The **IP Source Guard** page consists of two parts: **Port Settings** and **User Binding**.

IP Source Guard prevents users from setting IP addresses by themselves or changing the source IP address. Users need to obtain IP addresses in dynamic DHCP mode. Otherwise, network connection fails.

After the **IP Source Guard** function is enabled for a port, the port filters all non-DHCP IP packets. After the static IP address bound by the user is configured, the port allows IP packets from the statically bound IP address.

Port Settings

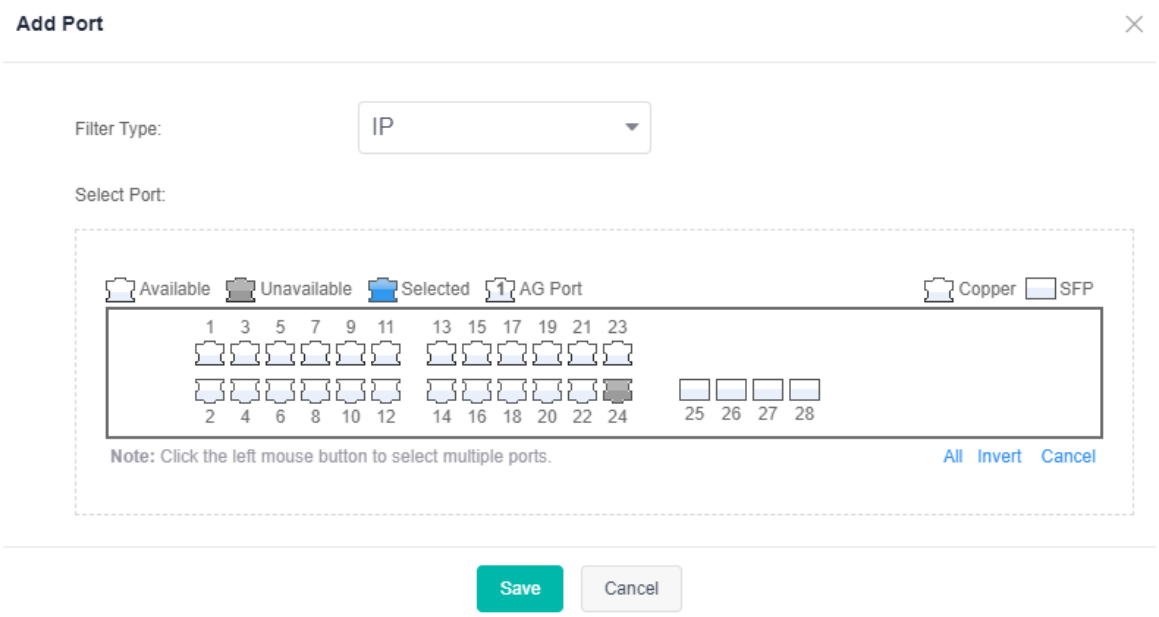
Figure 83 Port Settings



- Adding Ports

Click **Add**. The **Add Port** page is displayed. Specify **Filter Type**, select a port, and click **Save**. After "Add operation succeeded!" is displayed, the added port is displayed in the IP source guard port list.

Figure 84 Add Port



- Deleting Ports

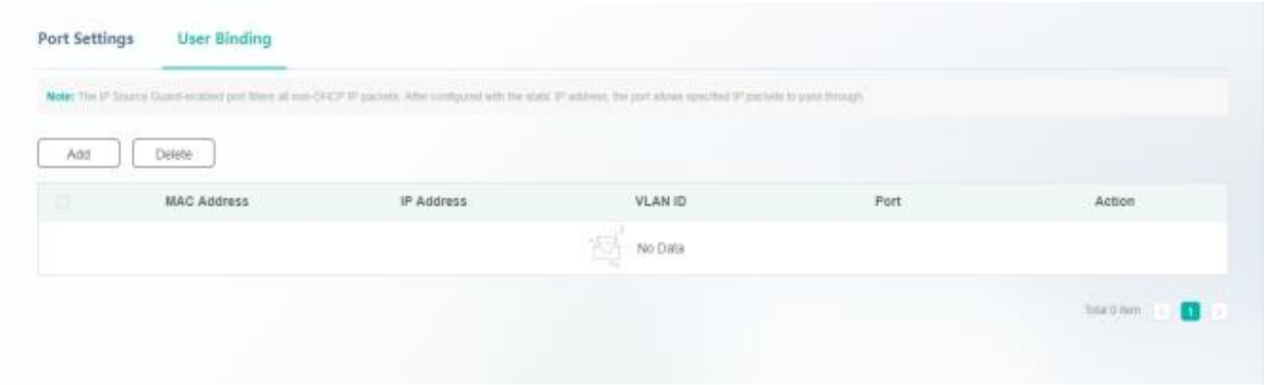
1. Select multiple records in the IP source guard port list and click **Delete** to batch delete the data records.

2. Click the delete icon of a port in the **Action** column of the IP source guard port list. In the displayed deletion confirmation dialog box, click **OK**. After "Delete operation succeeded!" is displayed, the deletion is complete.

User binding ports are also displayed in the IP source guard port list, but they cannot be edited or deleted.

User Binding

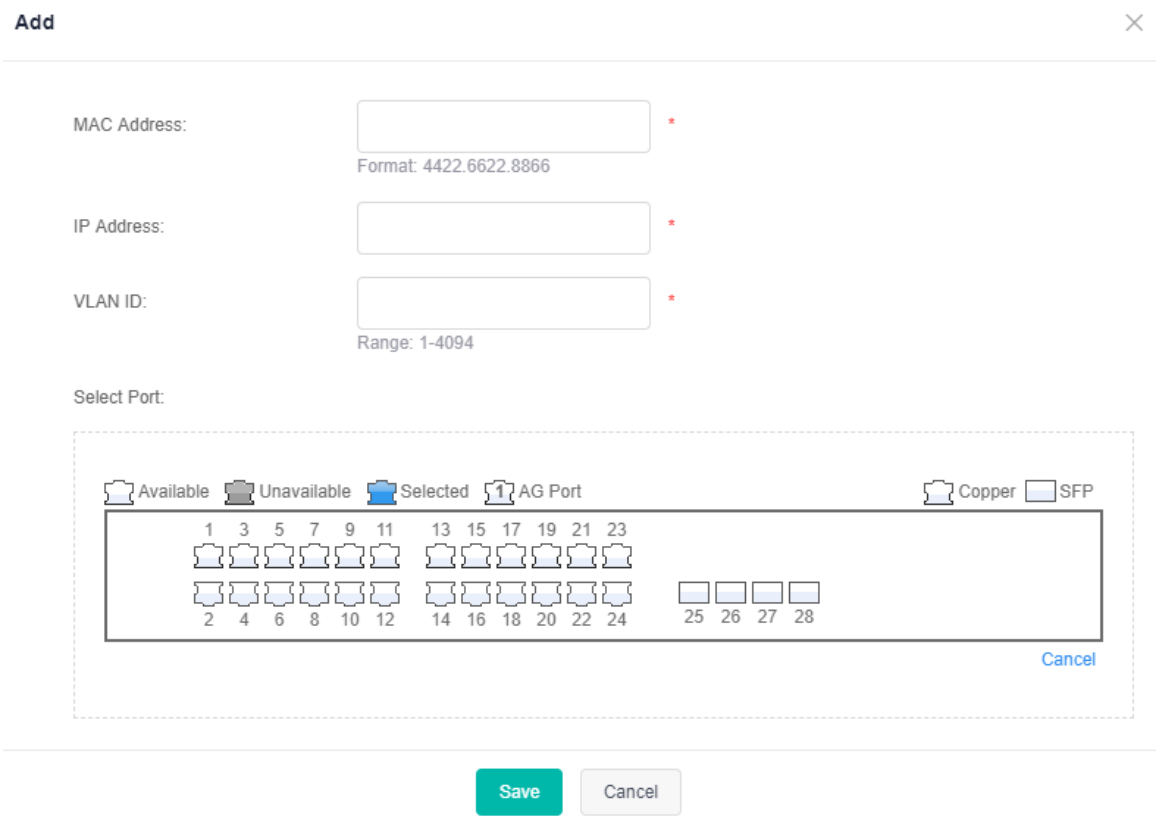
Figure 85 User Binding



- Adding User Bindings

Click **Add**. The **Add** page is displayed. Specify **MAC Address**, **IP Address**, and **VLAN ID**, select a port, and click **Save**. After "Add operation succeeded!" is displayed, the user binding port is displayed in the user binding port list and IP source guard port list.

Figure 86 Add



- Editing User Bindings

Click the edit icon of a user binding port in the **Action** column of the user binding port list. The user binding information is displayed. After you edit the information, click **Save**. After "Edit operation succeeded!" is displayed, the editing operation is complete.

- Deleting User Bindings

1. Select multiple records in the user binding port list and click **Delete** to batch delete the data records.

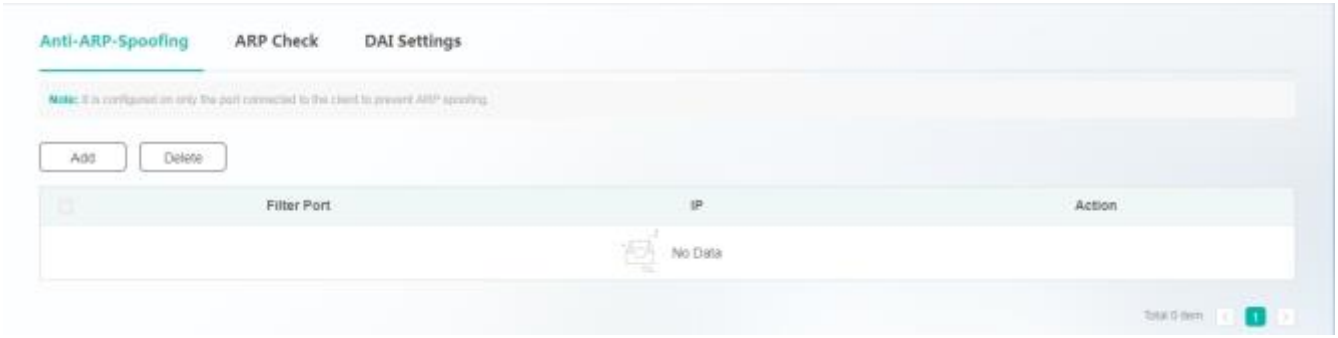
2. Click the delete icon of a user binding port in the **Action** column of the user binding port list. In the displayed deletion confirmation dialog box, click **OK**. After "Delete operation succeeded!" is displayed, the deletion is complete.

1.3.10.5 Anti ARP Spoofing

The **Anti ARP Spoofing** page consists of three parts: **Anti-ARP-Spoofing**, **ARP Check**, and **DAI Settings**.

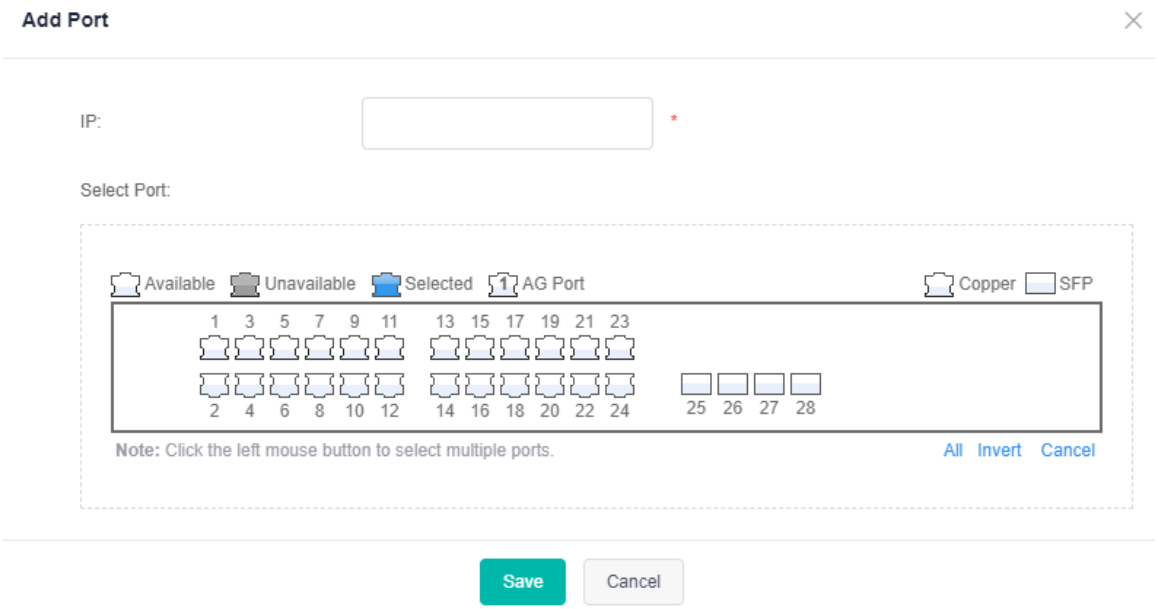
↘ Anti-ARP-Spoofing

Figure 87 Anti-ARP-Spoofing



- Adding Filtering Ports

Click **Add**. The **Add Port** page is displayed. Specify **IP**, select a port, and click **Save**. After "Add operation succeeded!" is displayed, the added port is displayed in the filtering port list.



- Editing Filtering Ports

Click the edit icon of a port in the **Action** column of the filtering port list. The filtering port information is displayed. After you edit the information, click **Save**. After "Edit operation succeeded!" is displayed, the editing operation is complete.

- Deleting Filtering Ports

1. Select multiple records in the filtering port list and click **Delete** to batch delete the data records.

2. Click the delete icon of a filtering port in the **Action** column of the filtering port list. In the displayed deletion confirmation dialog box, click **OK**. After "Delete operation succeeded!" is displayed, the deletion is complete.

ARP Check

Figure 88 ARP Check

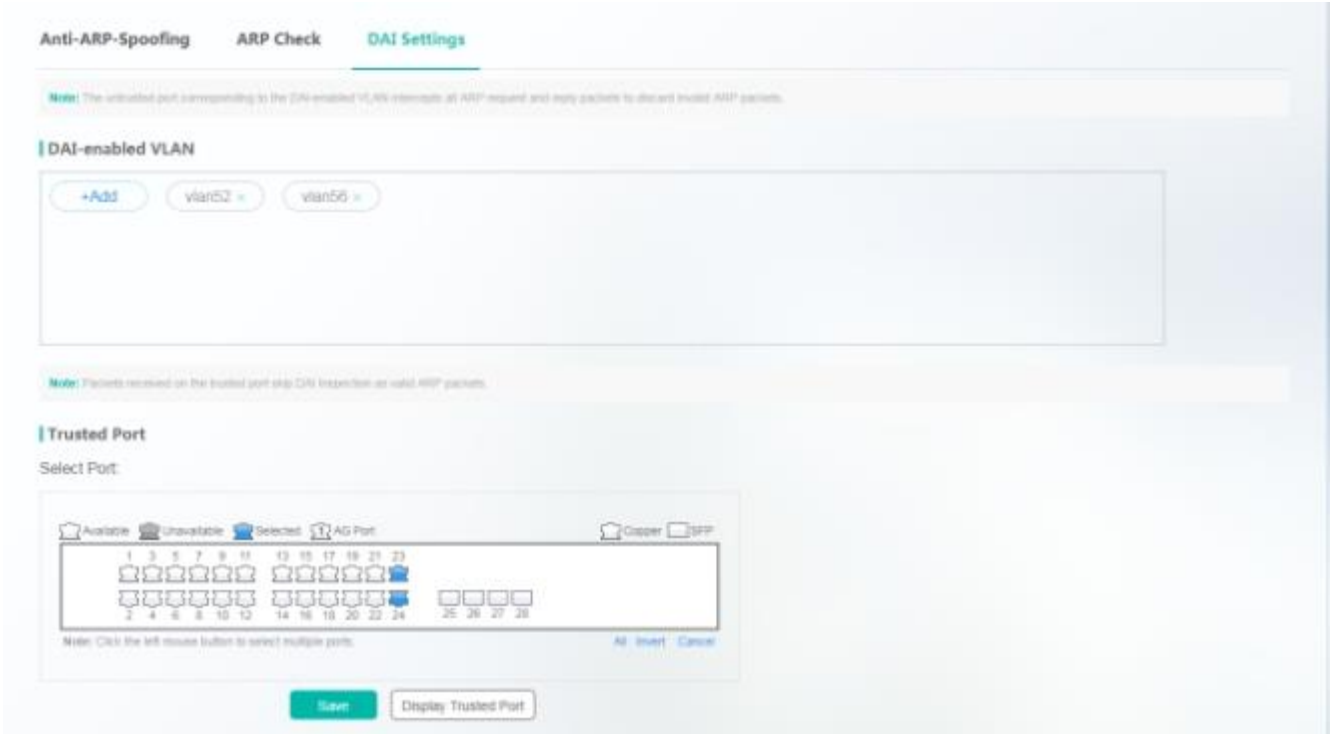
Select a port on the panel and click **Save**. After "Save operation succeeded!" is displayed, the ARP check function is enabled.

The panel displays ports with the ARP check function enabled and the ports are in the editable state. If you expect to abandon a modification to port information, click **Display ARP Check Port** to restore the panel to the current ARP check configuration status.

The ARP check function cannot be enabled for DHCP snooping trusted ports.

DAI Settings

Figure 89 DAI Settings



1. DAI-enabled VLANs

Click **+Add**, specify **VLAN**, and click ✓. After the confirmation dialog box is displayed, click **OK**. After "Add operation succeeded!" is displayed, the addition is complete.

2. Trusted Ports

Select a port on the panel and click **Save**. After "Save operation succeeded!" is displayed, the DAI trust function is enabled.

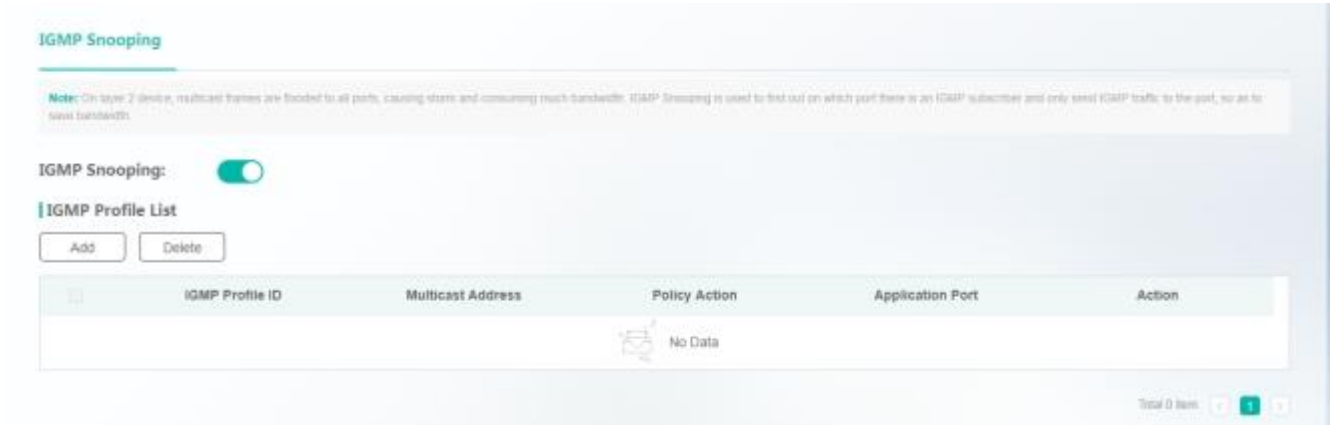
The panel displays ports with the DAI trusted port function enabled, and the ports are in the editable state. If you expect to abandon a modification to port information, click **Display Trusted Port** to restore the panel to the current DAI trusted port configuration status.

The ARP check function cannot be enabled for DHCP snooping trusted ports.

1.3.10.6 IGMP Snooping

Figure 90 shows the **IGMP Snooping** page.

Figure 90 IGMP Snooping



- Enabling/Disabling IGMP Snooping

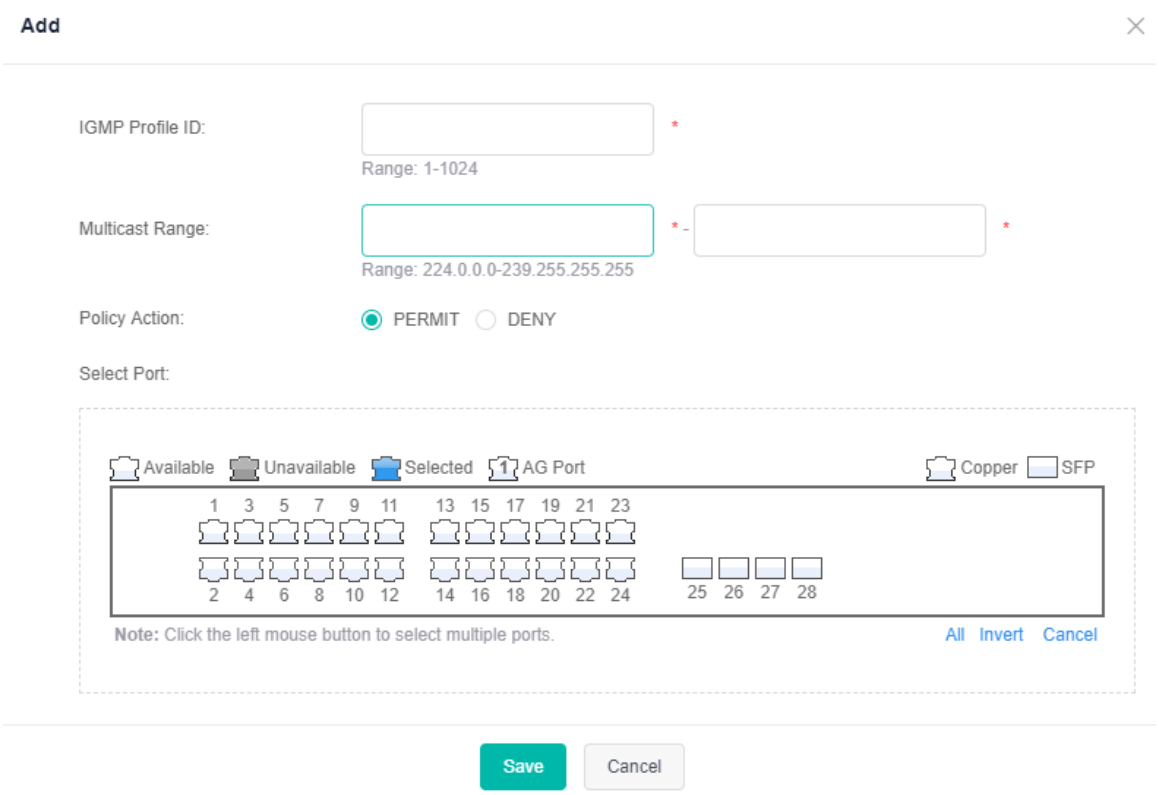
Enable the IGMP Snooping function. After "Enable operation succeeded!" is displayed, **IGMP Profile List** is displayed.

Disable the IGMP Snooping function. After the confirmation dialog box is displayed, click **OK**. After "Disable operation succeeded!" is displayed, IGMP Snooping is disabled.

- Adding IGMP Profiles

Click **Add**. The **Add** page is displayed. Specify **IGMP Profile ID**, **Multicast Range**, **Policy Action**, and other information (optional), and click **Save**. After "Add operation succeeded!" is displayed, the added IGMP profile is displayed in **IGMP Profile List**.

Figure 91 Add



- Editing IGMP Profiles

Click the edit icon of an IGMP profile in the **Action** column of **IGMP Profile List**. The IGMP profile information is displayed. After you edit the information, click **Save**. After "Edit operation succeeded!" is displayed, the editing operation is complete.

- Deleting IGMP Profiles

1. Select multiple records in **IGMP Profile List** and click **Delete** to batch delete the data records.

2. Click the delete icon of an IGMP profile in the **Action** column of **IGMP Profile List**. In the displayed deletion confirmation dialog box, click **OK**. After "Delete operation succeeded!" is displayed, the deletion is complete.

1.3.10.7 DHCP Snooping

Figure 92 shows the **DHCP Snooping** page.

Figure 92 DHCP Snooping

Ports connected to the DHCP server need to be set as DHCP trusted ports. The DHCP server works improperly over non-trusted ports. Selected ports on the panel are DHCP trusted ports. You can select ports on the panel and click **Save**. After "Save operation succeeded!" is displayed, the configuration is complete.

The panel displays ports with the DHCP trusted port function enabled, and the ports are in the editable state. If you expect to abandon a modification to port information, click **Display Trusted Port** to restore the panel to the current DHCP trusted port configuration status.

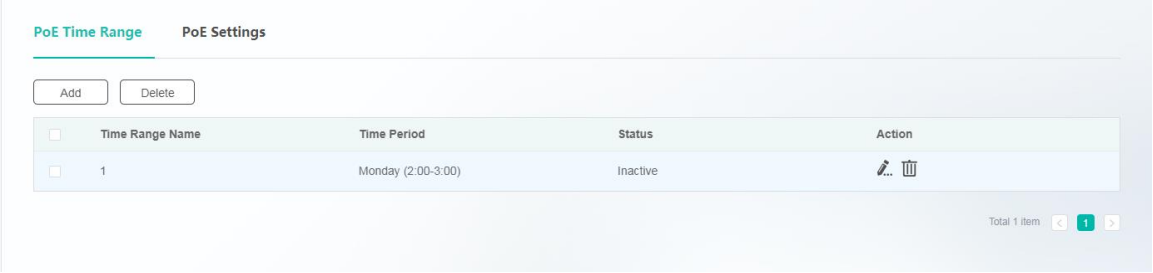
1.3.11 System Settings

1.3.11.1 PoE

The **PoE** page consists of two parts: **PoE Time Range** and **PoE Settings**. The **PoE** page is available only for devices that support the PoE function.

PoE Time Range

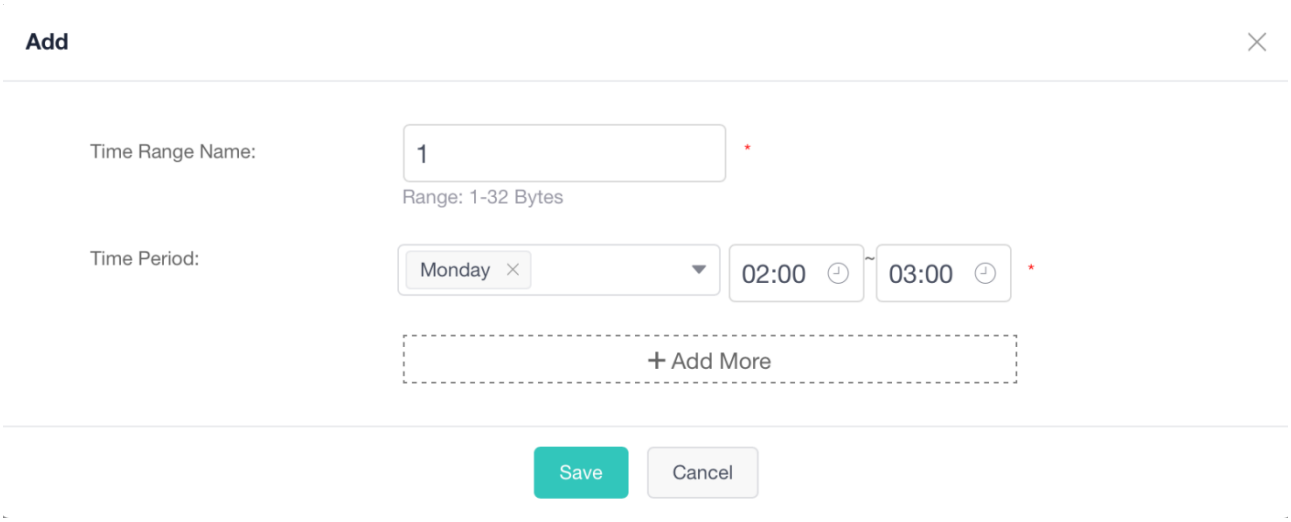
Figure 93 PoE Time Range



- Adding Time Ranges

Click **Add**. The **Add** page is displayed. Specify **Time Range Name** and **Time Period**, and click **Save**. After "Add operation succeeded!" is displayed, the added time range is displayed in **Time Range List**.

Figure 94 Add



- Editing Time Ranges

Click the edit icon of a time range in the **Action** column of **Time Range List**. The time range information is displayed. After you edit the information, click **Save**. After "Edit operation succeeded!" is displayed, the editing operation is complete.

- Deleting Time Ranges

1. Select multiple records in **Time Range List** and click **Delete** to batch delete the data records.

2. Click the delete icon of a time range in the **Action** column of **Time Range List**. In the displayed deletion confirmation dialog box, click **OK**. After "Delete operation succeeded!" is displayed, the deletion is complete. The deleted time range is no longer displayed in **Time Range List**.

PoE Settings

The **PoE Settings** page consists of two parts: **Global Configuration** and **Port Settings**.

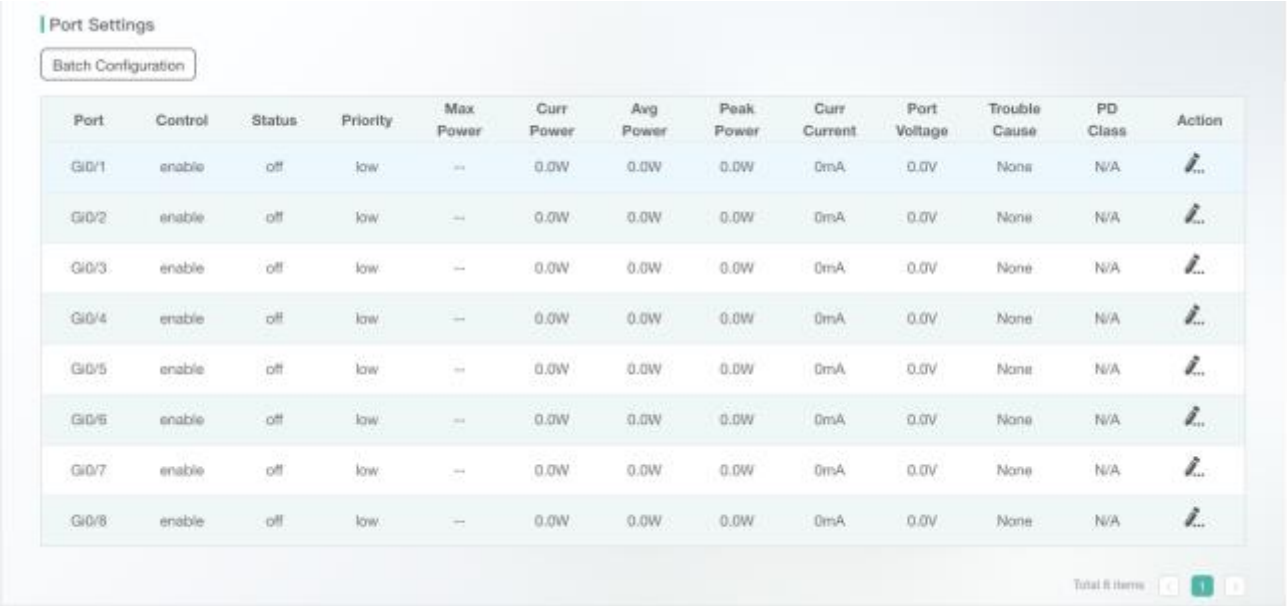
Global Configuration

Figure 95 Global Configuration

Set **Alarm Notification Threshold** and **Not Interrupt PoE During Reboot**, and click **Save**. After "Save operation succeeded!" is displayed, the configuration is complete.

Port Settings

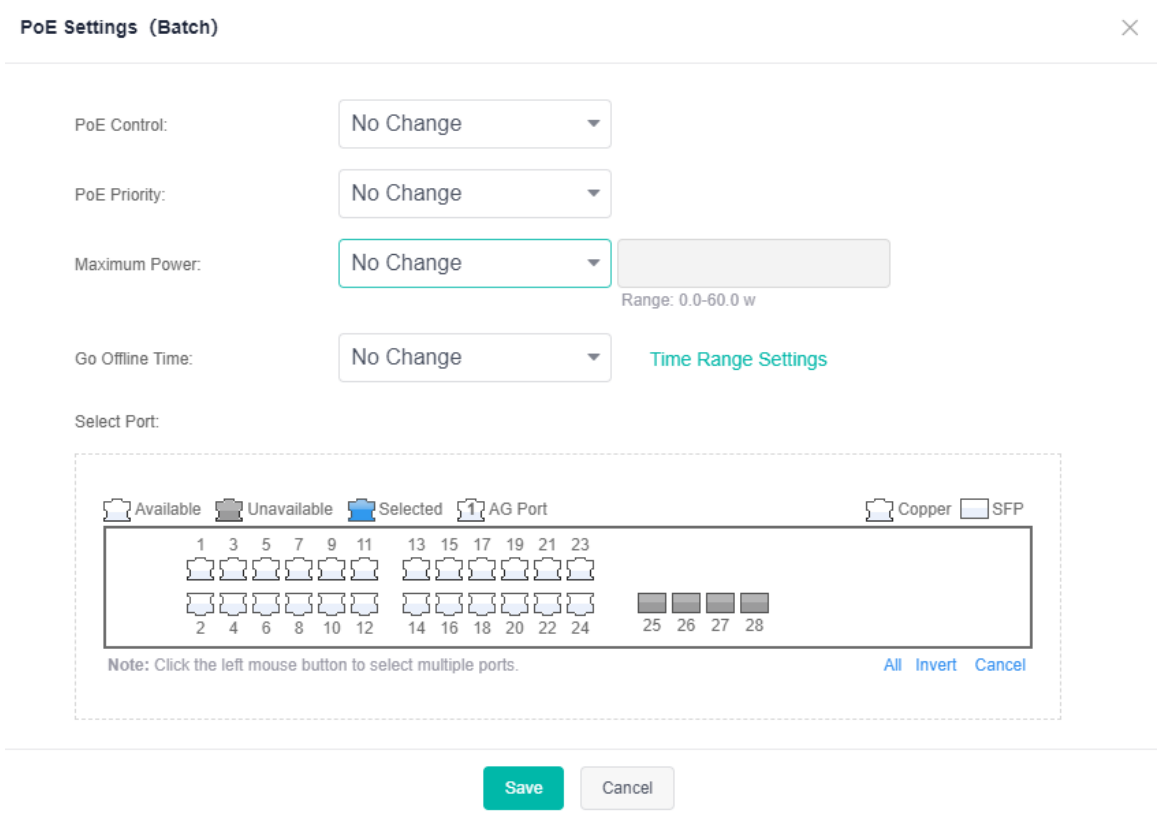
Figure 96 Port Settings



- Batch Configuration

Click **Batch Configuration**. The **Batch Configuration** page is displayed. Select required ports, specify **PoE Control**, **PoE Priority**, **Maximum Power**, and **Go Offline Time**, and click **Save**. After "Save operation succeeded!" is displayed, the configuration is complete.

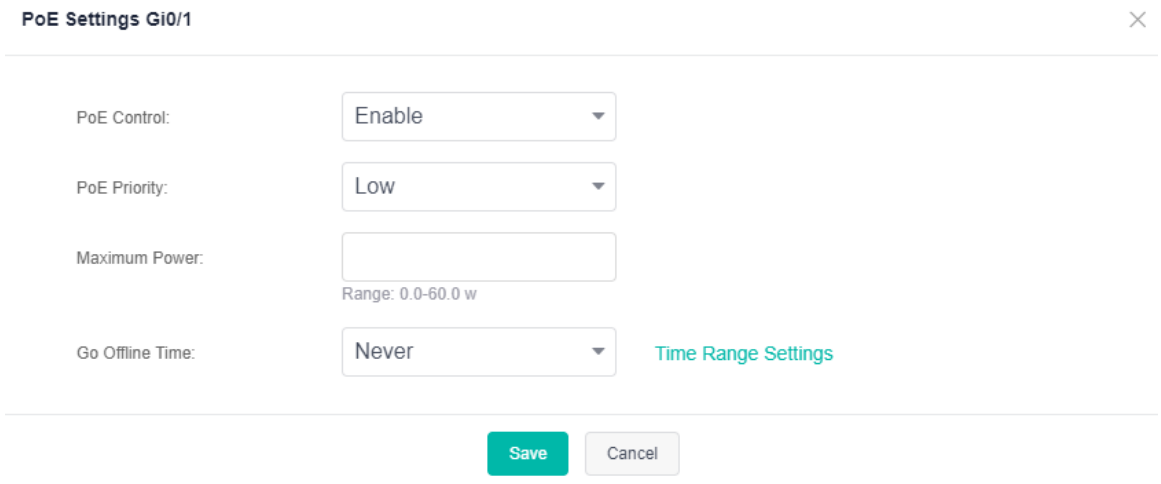
Figure 97 Batch Configuration



- Editing Ports

Click the edit icon of a port in the **Action** column of **Port List**. The port information is displayed. After you edit the information, click **Save**. After "Edit operation succeeded!" is displayed, the editing operation is complete.

Figure 98 PoE Settings



1.3.11.2 DNS

Figure 99 shows the **DNS** page.

Figure 99 DNS

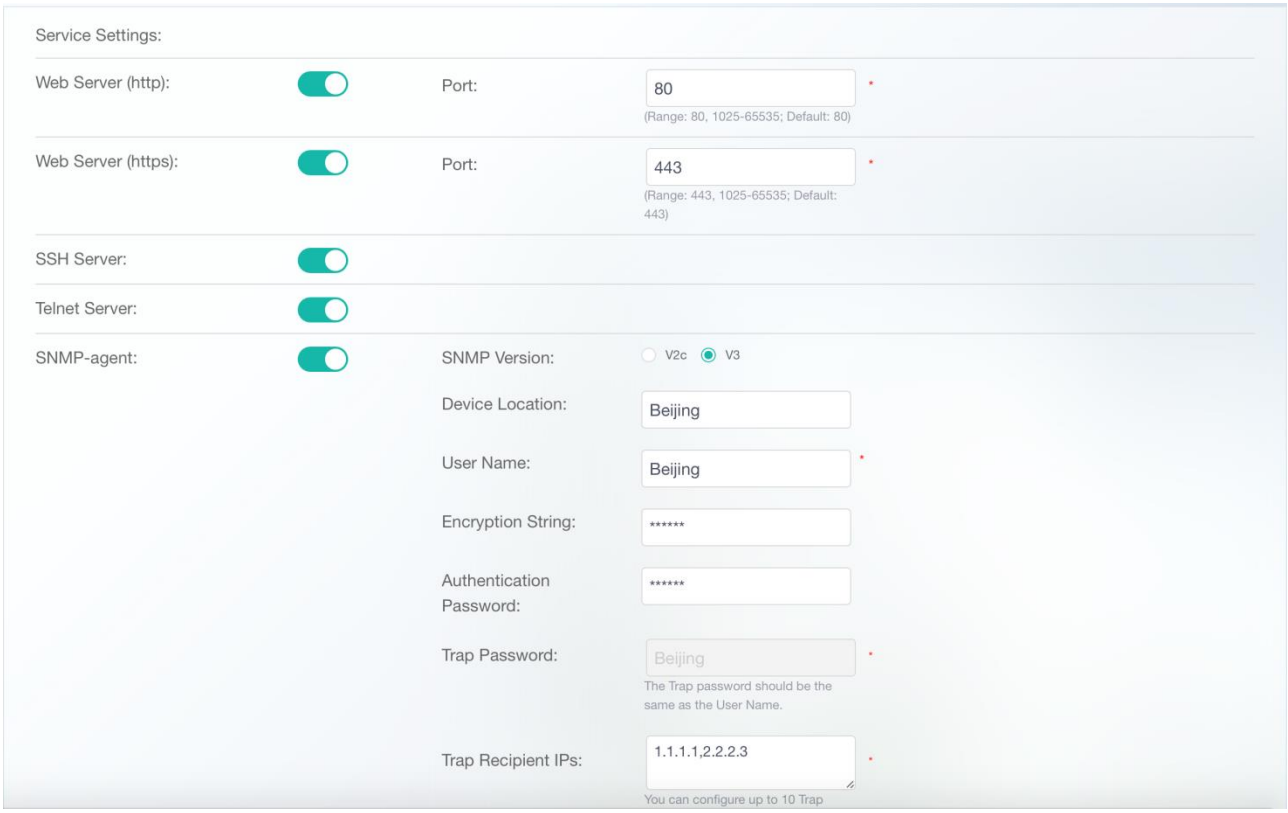
Enable the DNS function, specify **DNS Server**, and click **Save**. After "Save operation succeeded!" is displayed, the configuration is complete. A maximum of six DNS records can be configured.

1.3.11.3 Service

Five services, including **Web Server (http)**, **Web Server (https)**, **SSH Server**, **Telnet Server**, and **SNMP-agent** can be configured on the **Service** page.

Figure 100 shows the **Service** page.

Figure 100 Service



Set the service statuses. In the **SNMP-agent** area, set mandatory parameters **SNMP Version**, **User Name** (v3), **SNMP Password** (v2), **Trap Password**, and **Trap Recipient IPs**, and click **Save**. After "Save operation succeeded!" is displayed, the configuration is complete.

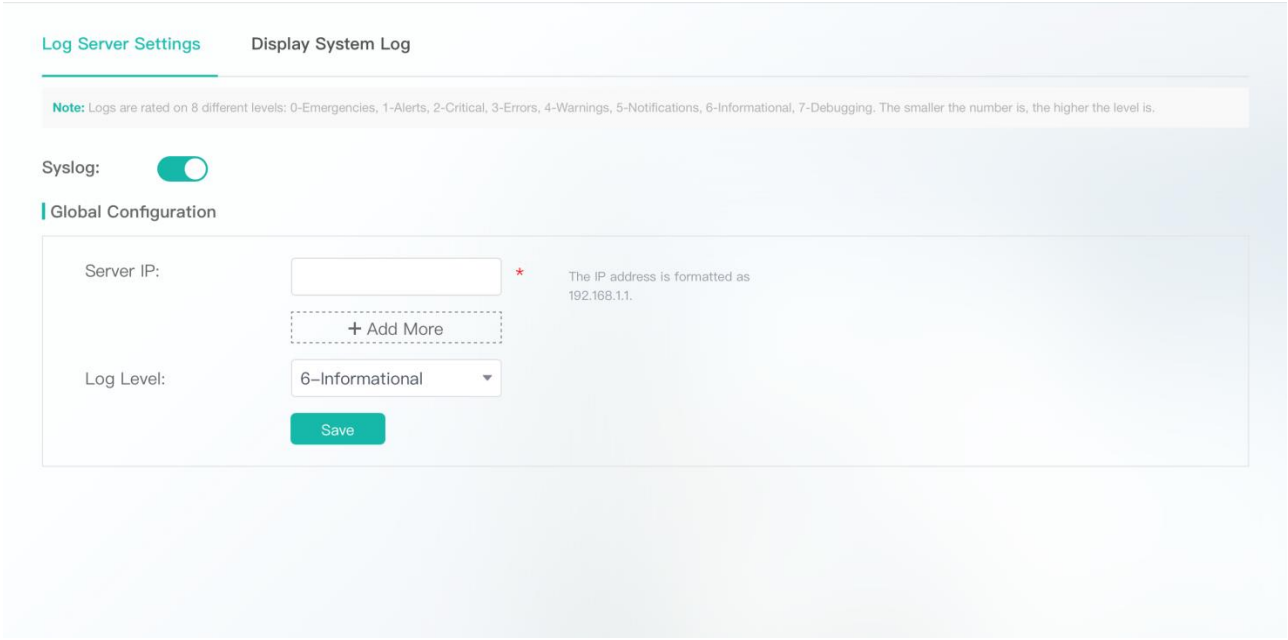
1.3.11.4 System Log

The **System Log** page consists of two parts: **Log Server Settings** and **Display System Log**.

Log Server Settings

Figure 101 shows the **Log Server Settings** page.

Figure 101 Log Server Settings



1. Enable the Syslog function. After "Enable operation succeeded!" is displayed, the Syslog function is enabled. Disable the Syslog function. After "Disable operation succeeded!" is displayed, the Syslog function is disabled.

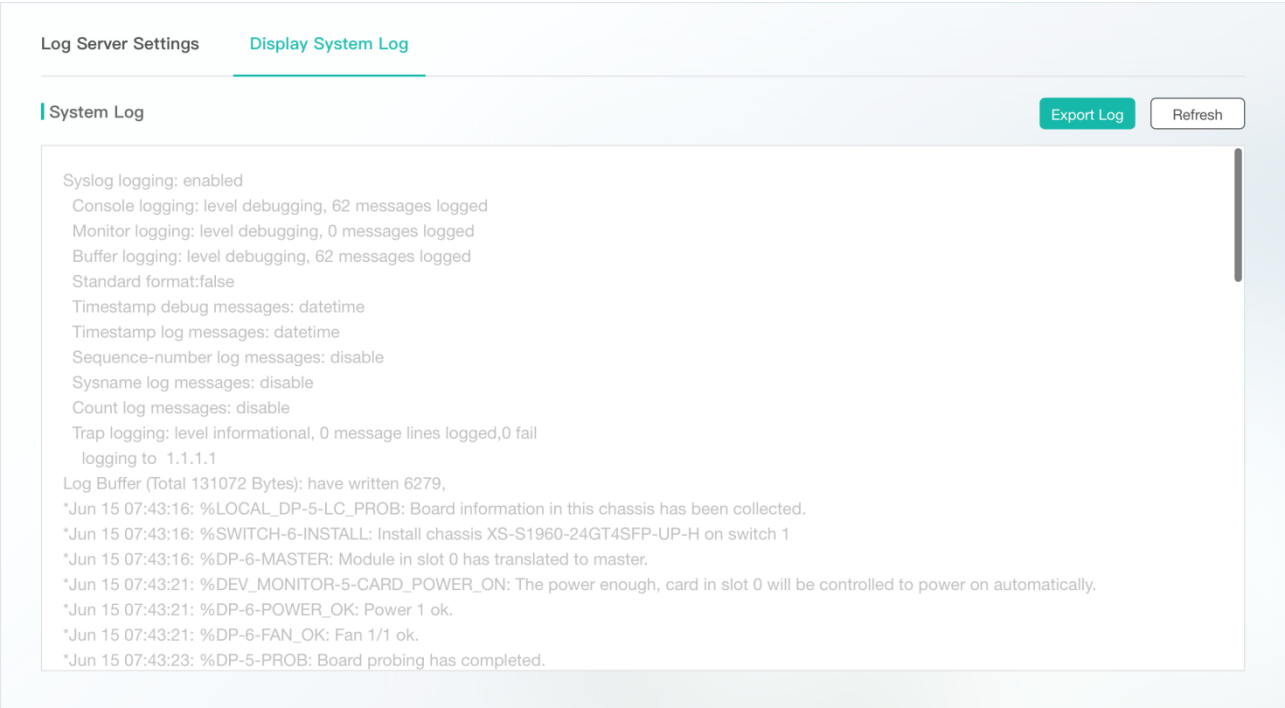
2. Set the system log server IP address and log level parameters, and click **Save**. After "Save operation succeeded!" is displayed, the setting is complete. The device sends logs to the corresponding server.

A maximum of five system log servers can be configured.

Display System Log

Figure 102 shows the **Display System Log** page.

Figure 102 Display System Log



The text box displays current log information. You can click **Export Log** to export log information and click **Refresh** to refresh the log information.

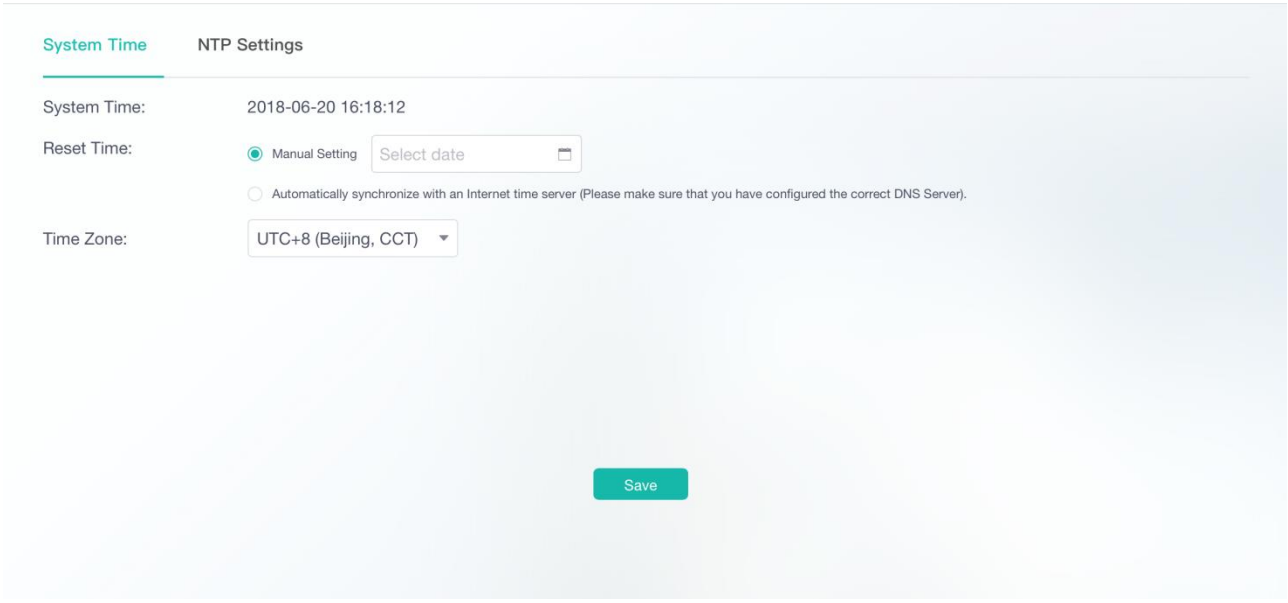
1.3.11.5 Time & NTP

The **Time & NTP** page consists of two parts: **System Time** and **NTP Settings**.

System Time

Figure 103 shows the **System Time** page.

Figure 103 System Time



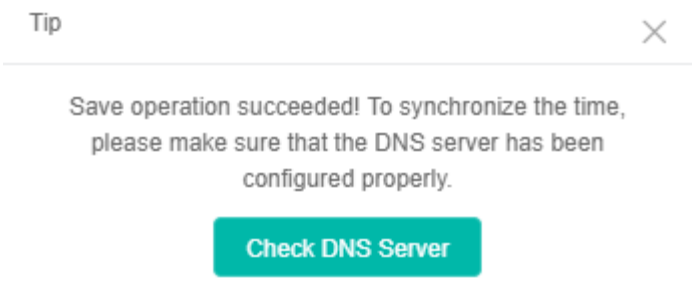
The **System Time** page displays the current system time. You can manually set the system time.

Alternatively, you can select **Automatically synchronize with an Internet time server** and set **Time Zone** to set the time.

Select either mode and click **Save**. After "Save operation succeeded!" is displayed, the configuration is complete.

Click **Configure DNS Server** on the **Tip** page to switch to the DNS configuration page.

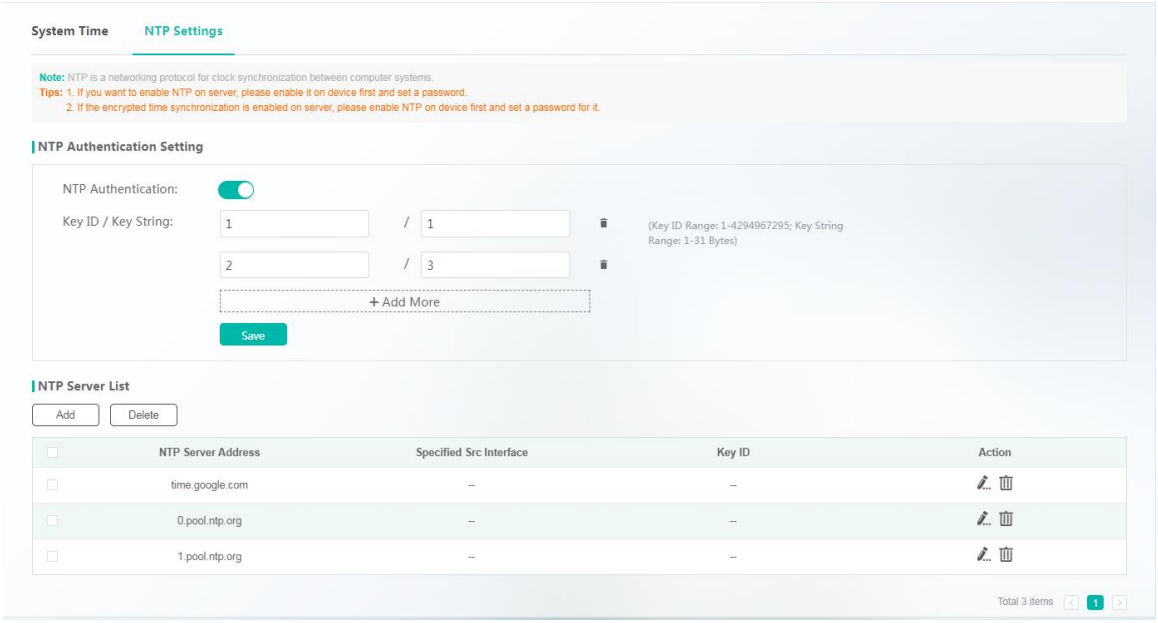
Figure 104 Tip



NTP Settings

Figure 105 shows the **NTP Settings** page.

Figure 105 NTP Settings



- Adding NTP Authentication Entries

Enable the NTP Authentication function, specify **Key ID/Key String**, and click **Save**. After "Save operation succeeded!" is displayed, the specified **Key ID/Key String** is displayed in the **Key ID/Key String** area.

- Editing NTP Authentication Entries

Click **Add more** to add new NTP authentication configurations or directly modify existing configurations. After you edit the information, click **Save**. After "Save operation succeeded!" is displayed, the editing operation is successful.

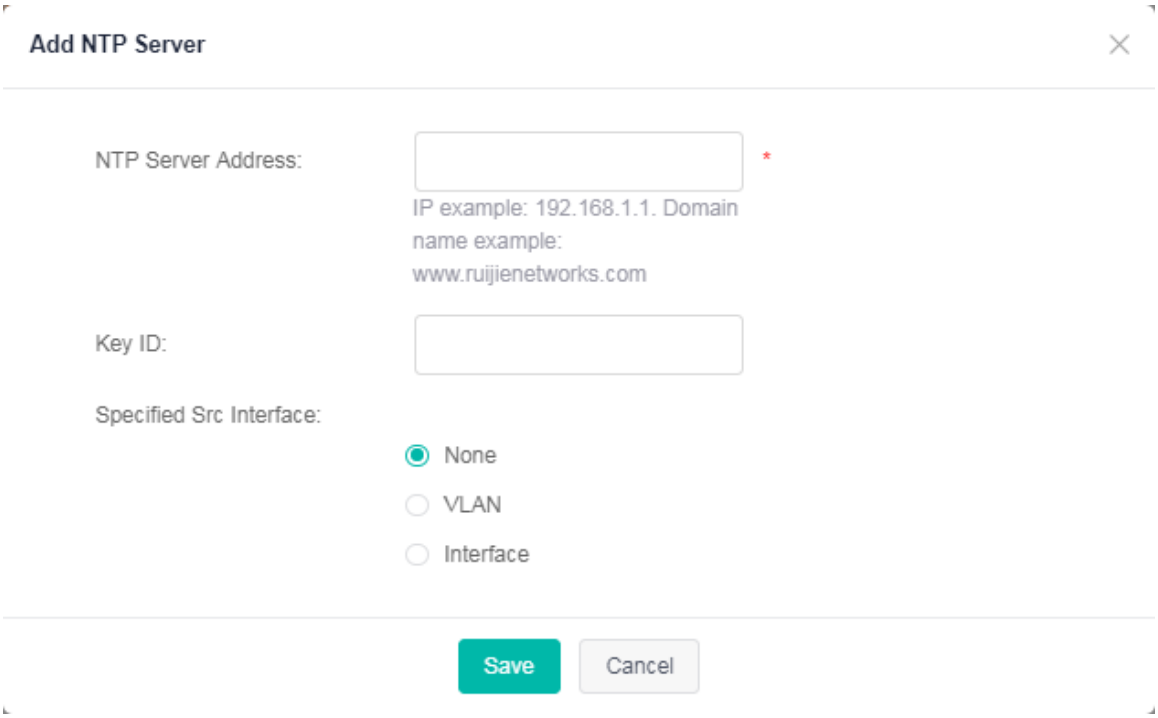
- Deleting NTP Authentication Entries

Select the delete icon behind **Key ID/Key String**, and click **Save**. After "Save operation succeeded!" is displayed, the deletion is successful. The deleted NTP authentication configuration is no longer displayed in the list.

- Adding NTP Servers

Click **Add**. The **Add NTP Server** page is displayed. Specify **NTP Server Address** and **Key ID** (existed), and click **Save**. After "Add operation succeeded!" is displayed, the added NTP server is displayed in **NTP Server List**.

Figure 106 Add NTP Server



- Editing NTP Servers

Click the edit icon of an NTP server in the **Action** column of **NTP Server List**. The NTP server information is displayed. After you edit the information, click **Save**. After "Edit operation succeeded!" is displayed, the editing operation is complete.

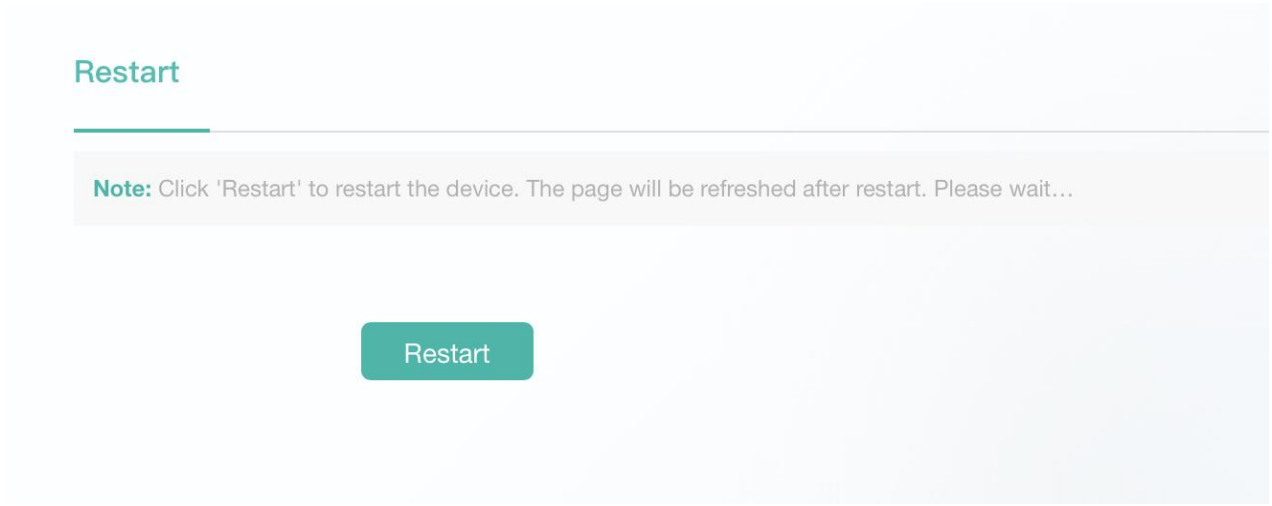
- Deleting Time Ranges

1. Select multiple records in **NTP Server List** and click **Delete** to batch delete the data records.

2. Click the delete icon of an NTP server in the **Action** column of **NTP Server List**. In the displayed deletion confirmation dialog box, click **OK**. After "Delete operation succeeded!" is displayed, the deletion is complete. The deleted NTP server is no longer displayed in **NTP Server List**.

1.3.11.6 System Restart

Figure 107 Restart



Click **Restart**. A restart confirmation dialog box is displayed. After you click **OK**, the device restarts. The restart process takes a few minutes. Please wait. The login page will be displayed after the device is restarted.

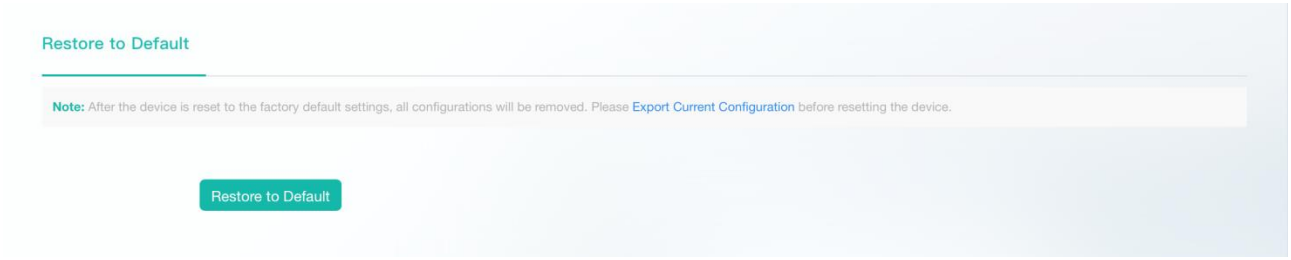
1.3.11.7 Restore to Default

1. Click **Export Current Configuration** in **Note** to export current configurations.

2. Click **Restore to Default** to clear the configurations and restore the factory settings.

Figure 108 shows the **Restore to Default** page.

Figure 108 Restore to Default



1.3.11.8 Backup

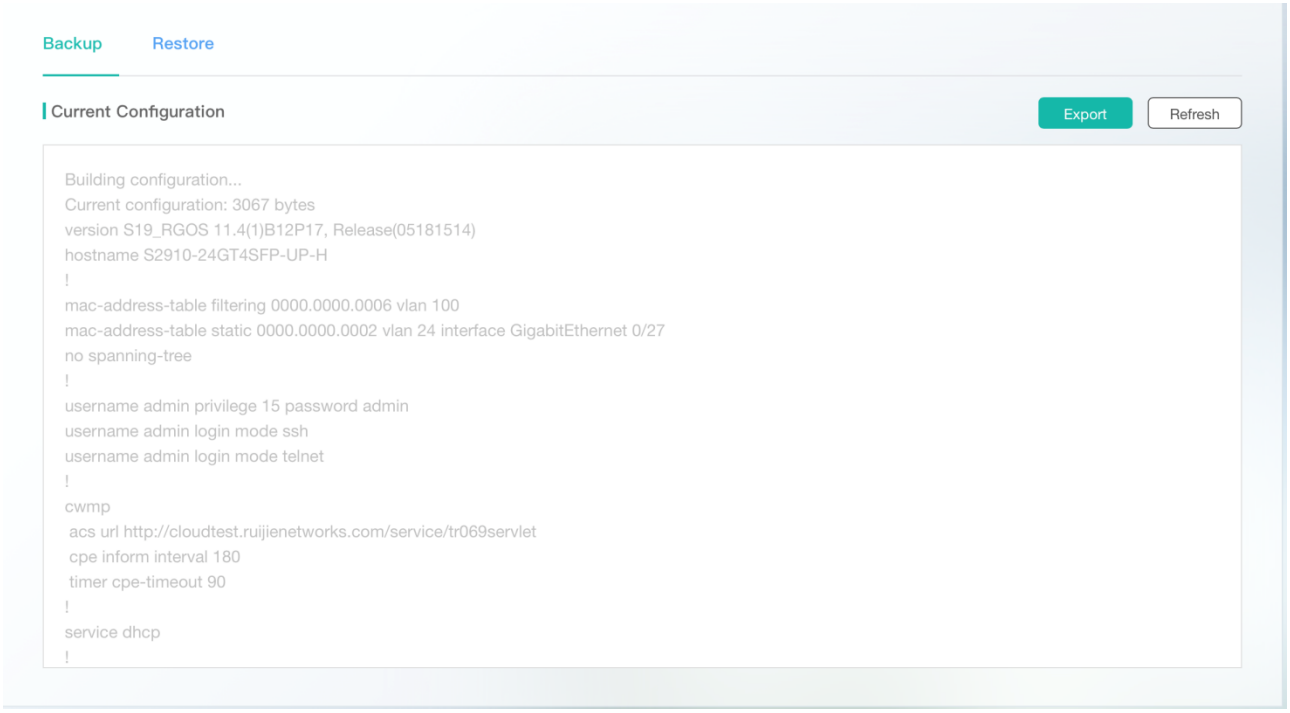
- Backup

1. Click **Export** to export the current configurations.

2. Click **Refresh** to refresh the current configurations.

Figure 109 shows the **Backup** page.

Figure 109 Backup



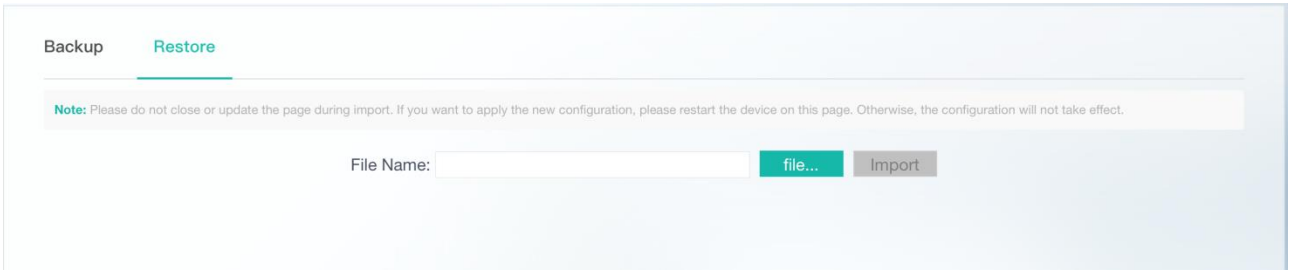
- Restore

After the configurations are imported, the device needs to be restarted for the configurations to take effect.

Click **file** and select the **config.txt** file. Click **Import** to import the configurations. After a restart confirmation dialog box is displayed, click **OK** to restart the device. After the device is restarted, the login page will be displayed.

Figure 110 shows the **Restore** page.

Figure 110 Restore

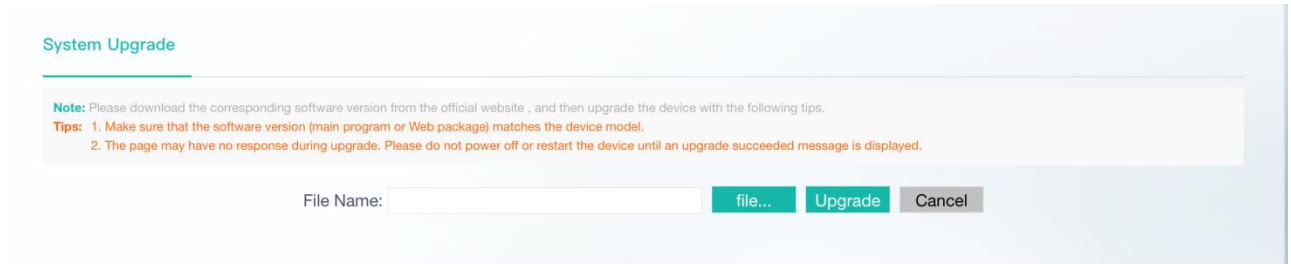


1.3.11.9 System Upgrade

The **System Upgrade** page consists of two parts: main program upgrade and Web package online upgrade.

Figure 111 shows the **System Upgrade** page.

Figure 111 System Upgrade

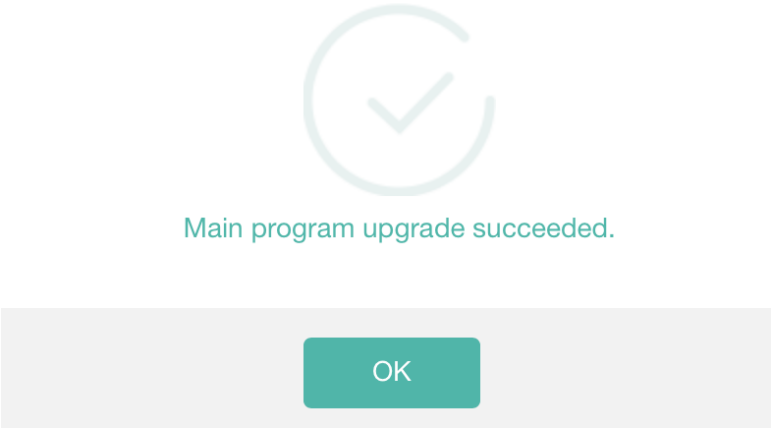


1.

Main program upgrade

Click **file**, select a locally saved bin file, and click **Upgrade** to upgrade the main program. After the main program is successfully upgraded, the login page is displayed.

Figure 112 Successful Main Program Upgrade



2. Web package online upgrade

Click **file**, select a locally saved UPD file, and click **Upgrade** to upgrade the web package. After the web package is successfully upgraded, refresh the page for the new eWeb system to take effect.

Figure 113 Successful Web Package Upgrade