Ruijie RG-CS86 Series Switches CS86_ RGOS12.6(4)B0102

Web-based Configuration Guide

Applicable products and versions:

RG-CS86 series switches: CS86-12XMG4VS-UP, CS86-24MG4VS-UP; CS86-24XMG4XS4VS-UPD; CS86-48MG4VS2QXS-UPD; CS86-20XS4VS2QXS-D

Document Version: V1.0
Date: July 23, 2026
Copyright © 2026 Ruijie Networks

Copyright

Copyright © 2026 Ruijie Networks

All rights are reserved in this document and this statement.

Without the prior written consent of Ruijie Networks, no organization or individual is permitted to reproduce, extract, back up, modify, or distribute the content of this document in any manner or form. It is also prohibited to translate the document into other languages or use any or all parts of it for commercial purposes.

 and  trademarks are owned by Ruijie Networks.

All other trademarks or registered trademarks mentioned in this document are owned by their respective owners.

Disclaimer

The products, services, or features that you purchase are subject to commercial contracts and terms. It is possible that some or all of the products, services, or features described in this document may not be available for purchase or use. Unless agreed upon otherwise in the contract, Ruijie Networks does not provide any explicit or implicit statements or warranties regarding the content of this document.

The names, links, descriptions, screenshots, and any other information regarding third-party software mentioned in this document are provided for your reference only. Ruijie Networks does not explicitly or implicitly endorse or recommend the use of any third-party software and does not make any assurances or guarantees concerning the applicability, security, or legality of such software. You should choose and use third-party software based on your business requirements and obtain proper authorization. Ruijie Networks assumes no liability for any risks or damages arising from your use of third-party software.

The content of this document is subject to constant change due to product version upgrades or other reasons. Thus, Ruijie Networks reserves the right to modify the content of the document without prior notice or prompt.

This manual serves solely as a user guide. While Ruijie Networks endeavors to ensure the accuracy and reliability of the content when compiling this manual, it does not guarantee that the content of the manual is free of errors or omissions. All information contained in this manual does not constitute any explicit or implicit warranties.

Personal Data Statement

During the operation or troubleshooting of the products, services, or features you have purchased, certain personal data of users may be collected or used. Therefore, it is essential for you to establish and implement appropriate privacy policies, in compliance with the relevant laws and regulations of the applicable countries or regions, to ensure the complete protection of users' personal data.

If Ruijie Networks is involved in this process, we will strictly adhere to the relevant laws and regulations of the applicable countries or regions and take all necessary actions to safeguard users' personal data.

When discarding, reclaiming, or reusing a device, please ensure to back up or clear any stored data to avoid data leakage. For assistance, please contact our after-sales technical support.

Preface

Intended Audience

This document is intended for:

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

Technical Support

- Ruijie Networks website: https://www.ruijie.com
- Online support center: https://www.ruijie.com/support
- Case portal: https://caseportal.ruijie.com
- Community: https://community.ruijie.com
- Email support: service_rj@ruijie.com
- Live chat: https://www.ruijie.com/rita
- Documentation feedback: doc@ruijie.com.cn

Conventions

1. Conversions

Convention	Description
Bold font	Commands, command options, and keywords are in bold font.
Italic font	Arguments for which you supply values are in *italic* font.
[ ]	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.
&<1-n>	The argument before the sign (&) can be input for consecutive 1- n times.
//	Double slashes at the beginning of a line of code indicate a comment line.

2. Signs

The signs used in this document are described as follows:

Warning

An alert that calls attention to important rules and information that if not understood or followed can result in data loss or equipment damage.

Caution

An alert that calls attention to essential information that if not understood or followed can result in function failure or performance degradation.

Note

An alert that contains additional or supplementary information that if not understood or followed will not lead to serious consequences.

Specification

An alert that contains a description of product or version support.

3. Note

The manual offers configuration information (including model, port type, and command line interface) for indicative purpose only. In case of any discrepancy or inconsistency between the manual and the actual version, the actual version prevails.

Contents

Preface..... I

1 Overview 1

2 Typical Applications 1

2.1 Managing Devices Through the eWeb Management System 1

2.1.1 Server Requirements 1

1. Non-supported Out-of-the-Box Management on eWeb 1

2.1.2 Client requirements 2

2.2 Logging In 2

2.2.1 Logging In to the Web Management System 2

2.2.2 Forgot Password 3

3 Network management 3

3.1 Main Interface 3

3.1.2 Header 4

1. Device Info 4

2. Language Switching 4

3. Remote O&M 5

4. Network Configuration 5

5. Log Out 6

3.1.3 Navigation Menu 6

3.2 Network Configuration 6

3.2.1 Discover Device 7

3.2.2 Project Settings 7

3.3 Overview 8

3.4 Device 9
3.4.2 Adding Networking Devices 9
3.4.3 Managing Networking Devices 10
3.5 System Configuration 11
3.5.1 Setting the Web Login Password 11
3.5.2 Reset 11
3.5.3 Rebooting the Device 12
2. Rebooting the Master Device 12
3. Rebooting the Devices in the Network 13
4. Rebooting Specified Devices in the Network 13
4 eWeb Management System 15
4.1 Main Interface 15
4.1.2 Header 15
1. Quick Setup 15
2. Access History 16
3. Quick Search 16
4. Operation Log 20
5. Favorites 20
6. Customer Service Center 23
7. Theme Switching 23
8. Language Switching 24
9. Changing Password 24
10. Exit 25
4.1.3 Navigation Menu 25

4.1.4 Main Operation Area 26
4.2 Quick Configuration 26
4.2.1 Layer 2 Mode 26
4.2.2 Layer 3 Mode 28
4.3 Home Page 30
4.3.1 Overview 30
4.3.2 Interfaces 30
4.3.3 CPU/Memory Usage 31
4.3.4 Temperature/Power Module/Fan 31
4.3.5 Bandwidth 32
4.4 Network 33
4.4.1 Port Config 33
1. Port Management 33
2. VLAN Management 46
3. PoE53
4.4.2 Loop Guard 56
1. STP Loop Guard 56
2. RLDP Link Detection 60
4.4.3 Route Configuration 65
1. PBR 65
2. Routing table 67
3. Static Route 68
4.4.4 Network Management Protocols 71
1. SNMP/Trap 71

2. Telnet/SSH 73
4.4.5 Advanced Configuration 74
1. DHCP Server 74
2. VSU Settings 80
3. MAC Address Table 83
4.5 Security 87
4.5.1 DHCP Snooping 87
4.5.2 ACL 88
1. ACL List 88
2. ACL Application 93
4.6 O&M 95
4.6.1 Network Diagnostic Tools 95
1. Network Detection 95
2. One-Click Collect 96
4.6.2 Device O&M 98
1. Upgrade 98
2. Restart 99
3. System Time 100
4. Log Server 100
5. DNS Server 101
6. System Character Set 101
7. Web Console 102
4.6.3 Backup and Recovery 103
1. Configuration Management 103

2. Manual Database Backup 105
3. Auto Database Backup 107
4. Restore Factory Settings 109
4.7 System 110
4.7.1 Operation Log 110
4.7.2 Licensing Procedure 111
4.7.3 Certificates and Registration 112
4.7.4 SMB SON Management 112

1 Overview

This document describes how to use the eWeb management system. You can use the eWeb management system to configure common settings for devices.

You can access the eWeb management system through a browser (such as Google Chrome) to manage switches.

2 Typical Applications

Typical Application	Description
Managing Devices Through the eWeb Management System	After switches are properly configured, you can access the eWeb management system through a browser to manage these switches.

2.1 Managing Devices Through the eWeb Management System

2.1.1 Server Requirements

1. Non-supported Out-of-the-Box Management on eWeb

Before you log in to the web system for the first time, you can connect the PC to the console port of the device and configure the device's IP address. Run the **enable service web-server all** command to enable the web service function. The configuration is as follows:

```
Hostname> enable
Web login password and enable password isn't set up, please set the password.  //
If you start up an unconfigured device, you need to set the login password and
enable password for the web system.

Please Set the password:********

Please check the password:********

Set the password success!

Hostname#
Hostname# configure
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 192.168.3.100 255.255.255.0 //
Configure the IP address for eWeb login. This IP address must be reachable from the IP address of the
PC which is used to log in to the eWeb.
```

```
Hostname(config-if-GigabitEthernet 0/1)# exit
Hostname(config)# ip route 0.0.0.0 0.0.0.0 192.168.3.1 // Configure the gateway.
Hostname(config)# enable service web-server // Enable the HTTP and HTTPS.
```

The default username is admin, and the password is the one configured during the initial device setup for the web service.

Caution

For your network security, you are advised to regularly change your login password.

2.1.2 Client requirements

(1) Client: A client refers to a PC or a mobile terminal such as a laptop. A network administrator can log in to the eWeb graphical user interface (GUI) of a switch from the client's browser to manage switches.

(2) Browser: Google Chrome is recommended. Exceptions such as garbled characters or formatting errors may occur if an unsupported browser is used. If an exception occurs due to the use of an old version of Google Chrome, you are advised to upgrade it to the latest version.

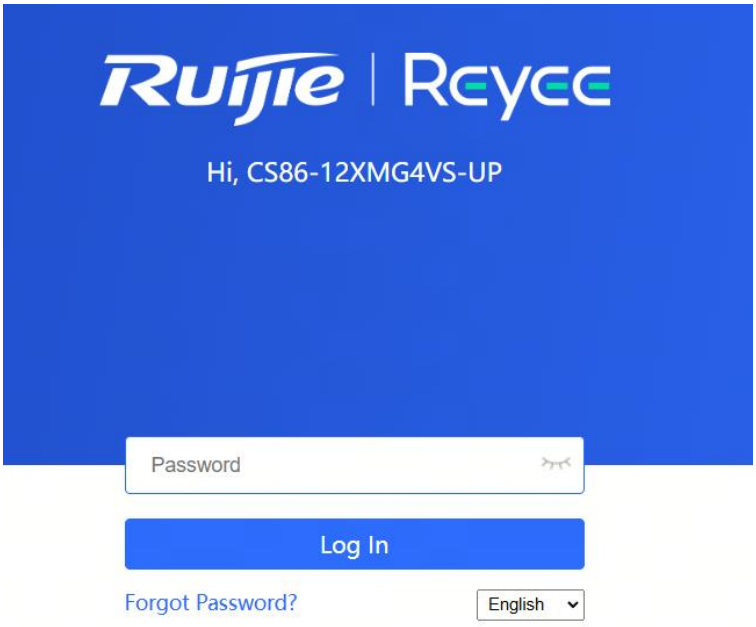
(3) Resolution: You are advised to set the resolution to 1600 x 900 or 1920 x 1080. If other resolutions are used, font and formatting issues may occur.

2.2 Logging In

2.2.1 Logging In to the Web Management System

Enter the switch IP address in your browser's address bar. Make sure that the IP address is reachable. The login page is displayed.

Figure2-1 Logging In



(1) Enter the username and password and click **Log In**. The main interface of the eWeb management system is displayed.

(2) If you need customer service assistance, contact local technical support.

(3) To prevent login through brute-force cracking, your account will be locked for 10 minutes after 5 failed attempts. You cannot log in during the locking period.

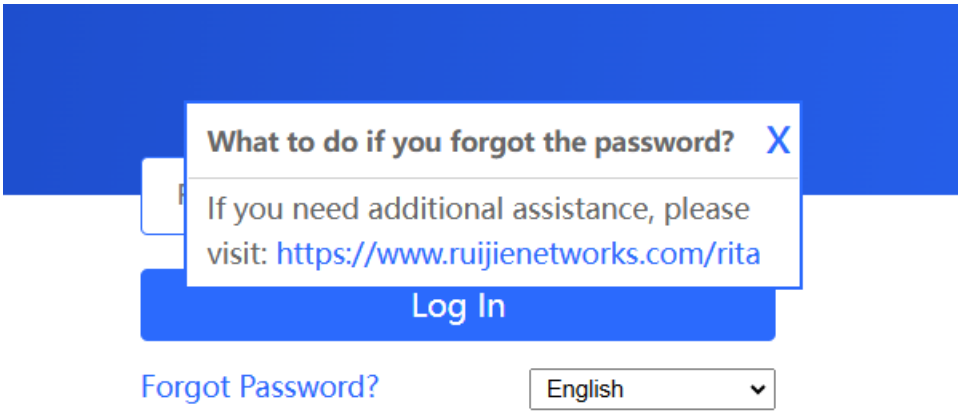
Note

To use the eWeb management system, ensure that the rg-web component has been installed on the switch and the web service has been enabled (if the web service is not enabled, run the **enable service web-server** command in config mode to enable it). Otherwise, the login page is not displayed. In most situations, the rg-web component is integrated in the rgos.bin system by default. However, if it is not installed, you can install it by installing the upgrade file mentioned in this release note of the eWeb management system.

2.2.2 Forgot Password

If you cannot remember your username or password, click **Forgot Password?**

Figure2-2 Forgot Password



If the Telnet password is known, run the **webmaster password** command. The configuration is as follows: The configuration is as follows:

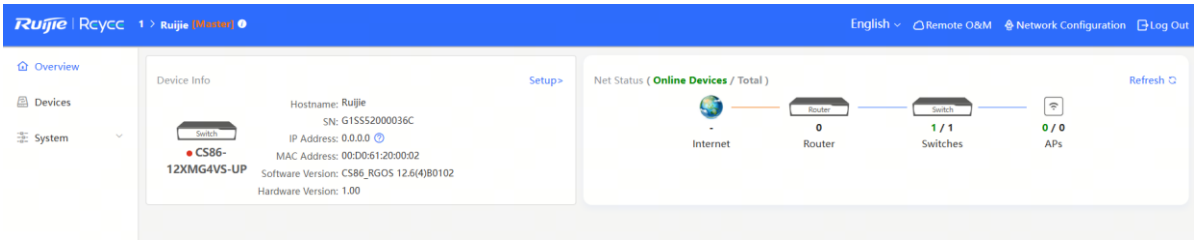
```
Hostname> enable
Hostname# configure
Hostname(config)# webmaster level 0 username admin password hostname@123
```

3 Network management

3.1 Main Interface

The main interface of the network management system is displayed.

Figure3-1 Main Interface



3.1.2 Header

This area displays links to common functions, including **Device Info**, **Change Language**, **Remote O&M**, **Network Configuration**, and **Log Out**. You can click these links to switch to specific configuration pages.

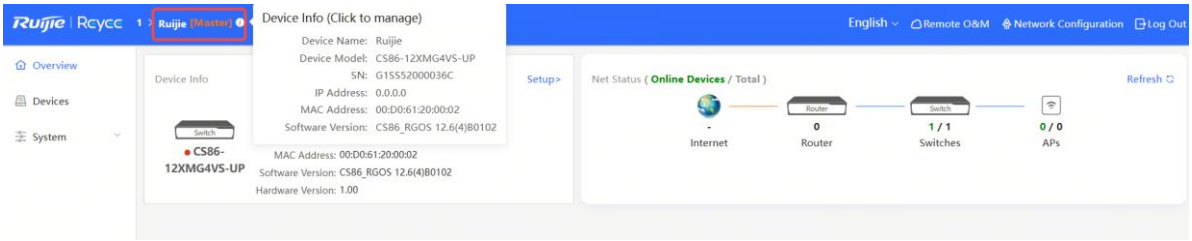
Figure3-2 Header



1. Device Info

When you move the cursor to the device name, the basic information of the online device is displayed, including the device name, device model, SN, IP address, MAC address, and software version.

Device Info

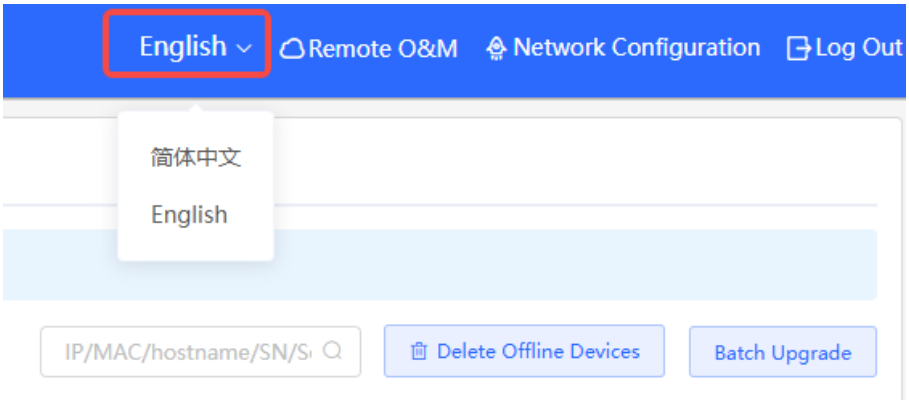


Click the device name to access the **Home** page. For details, see 4 eWeb Management System.

2. Language Switching

Click **English** in the upper right corner to switch the system language.

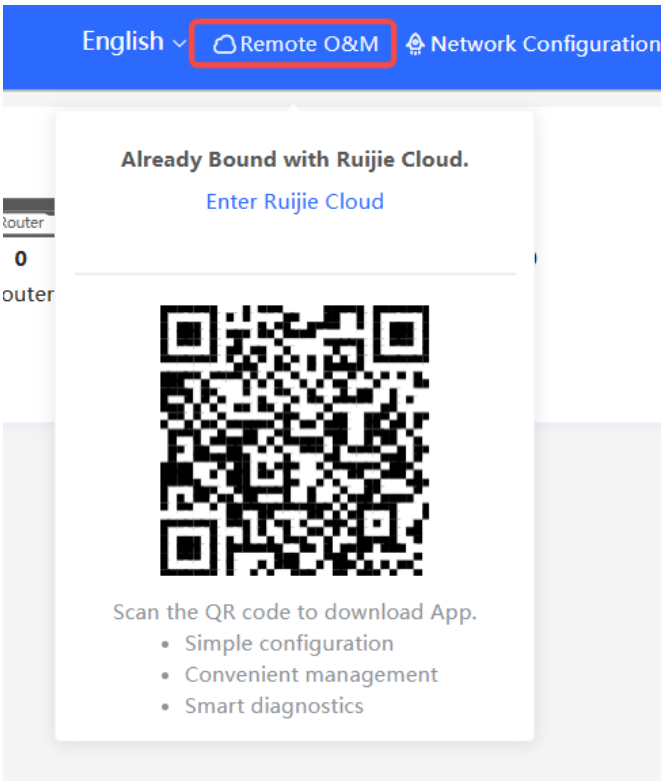
Figure3-3 Language Switching



3. Remote O&M

Click **Remote O&M** in the upper right corner to log in to the MACC for remote O&M through the URL or by scanning the QR code.

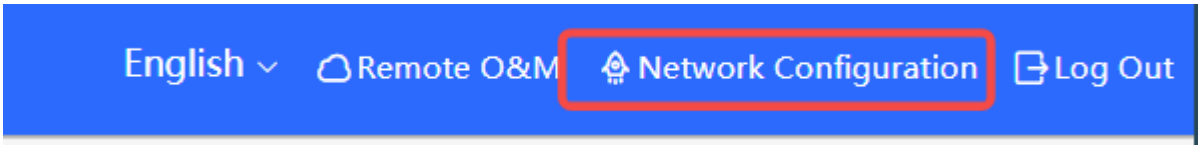
Figure3-4 Remote O&M



4. Network Configuration

Click **Network Configuration** in the upper right corner to access the network setup wizard. For details, see 3.2 Network Configuration.

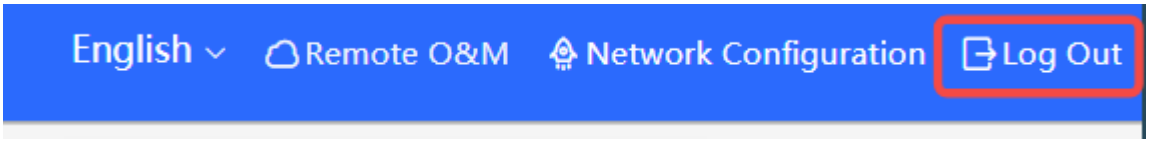
Figure3-5 Network Configuration



5. Log Out

After the network management is complete, click **Log Out** to exit the eWeb home page and return to the login page, as shown in the following figure.

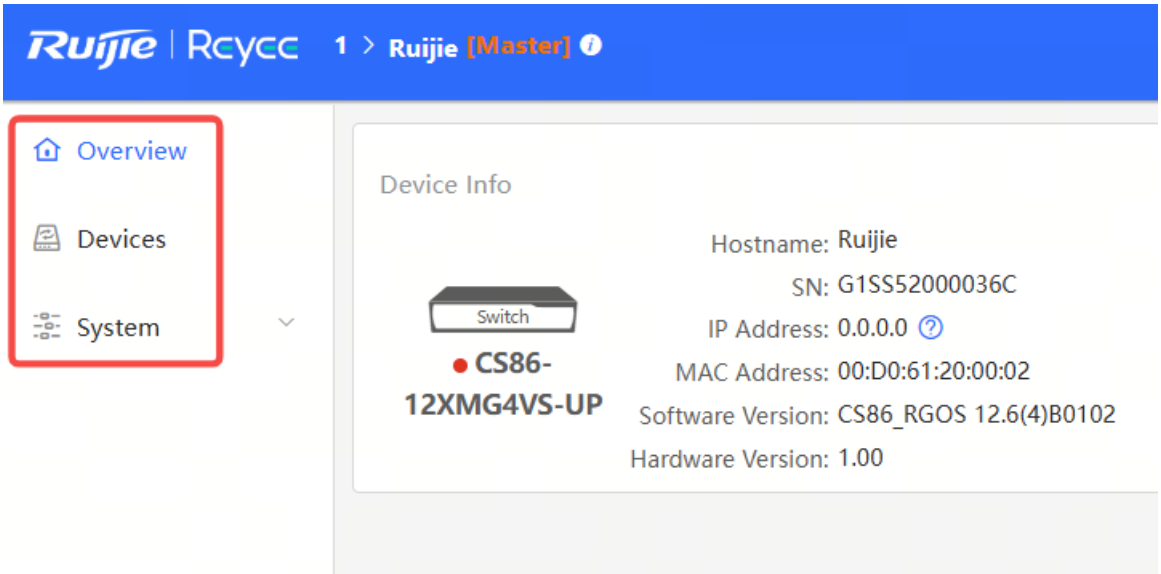
Figure3-6 Log Out



3.1.3 Navigation Menu

This area displays main tabs of the network management system.

Figure3-7 Navigation Menu



3.2 Network Configuration

Click **Network Configuration** in the upper right corner to access the **Discover Device** page.

3.2.1 Discover Device

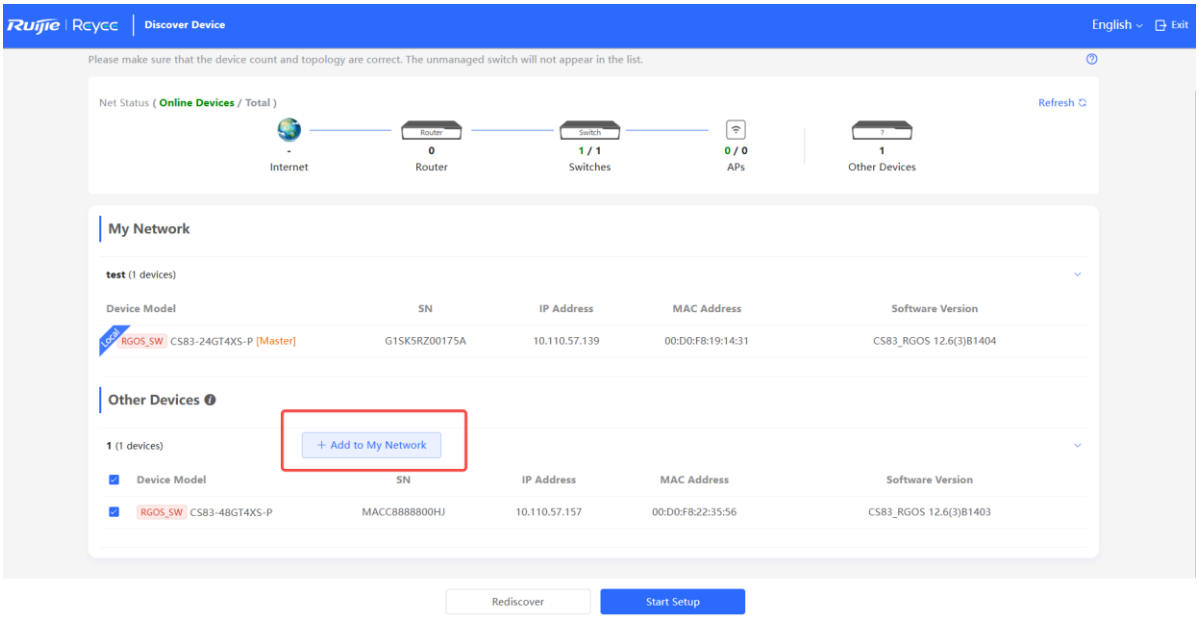
By default, users can perform batch settings and centralized management of all devices in the network. Therefore, before starting configuration, you need to check and confirm the number of online devices and network status in the network.

Note

Under normal circumstances, when multiple new devices are powered on and connected, they will be automatically interconnected into a network, and the user only needs to confirm that the number of devices is correct.

If there are other devices in the network that are not added to the current network, you can click **Add to My Network** and enter the management password of the added device to manually add the corresponding device to the network where the device is located, and then start the network-wide configuration.

Figure3-8 Discover Device



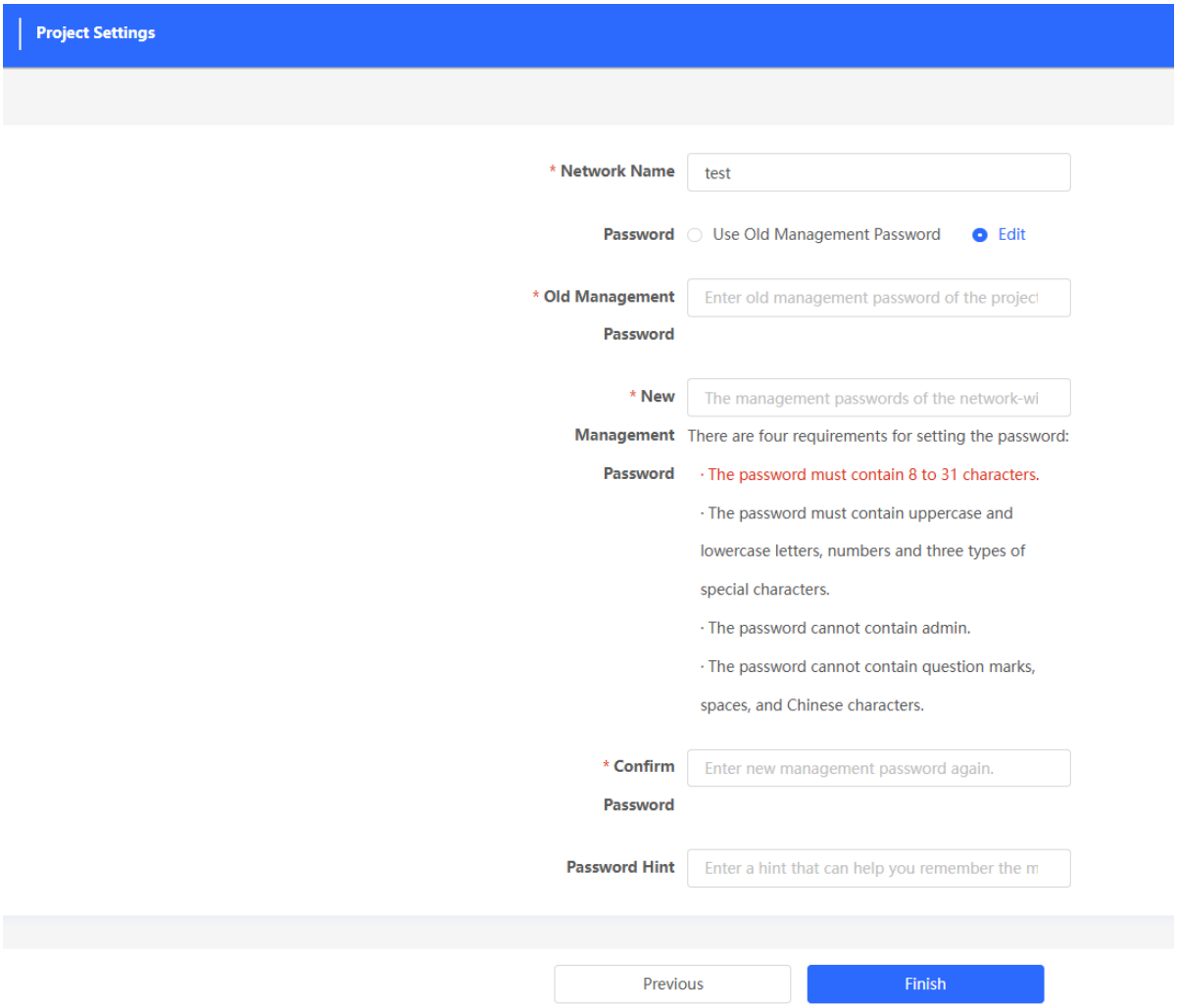
3.2.2 Project Settings

Click **Start Setup** to set the network name and management password of the device.

Network Name: Identify the network where the device is located.

Management Password: Set the password for logging in to the management page.

Figure3-9 Project Settings



Click **Finish** to deliver related configuration for initialization and detect the network. After completing the quick setup, the new device is connected to the Internet, and you can continue to bind the device to the cloud account for remote management. For specific operations, please refer to the instructions on the page to log in to the Ruijie Cloud platform for configuration.

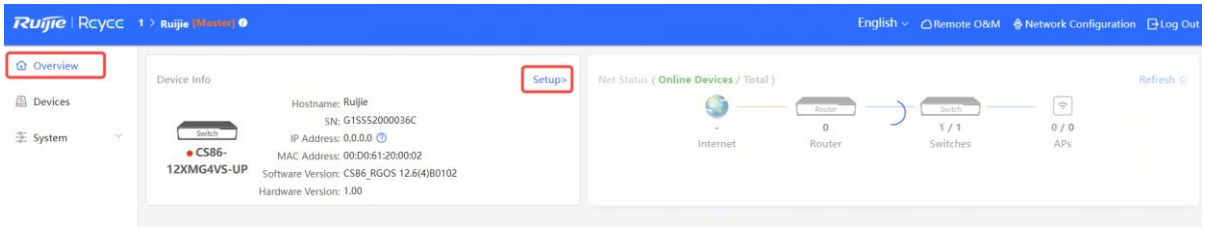
Note

After changing the management password, you need to re-visit the device management address and use the new password to log in to the device.

3.3 Overview

The **Overview** page displays the information about the online device and the status of all devices on the network. Click **Setup** to access the **Home** page.

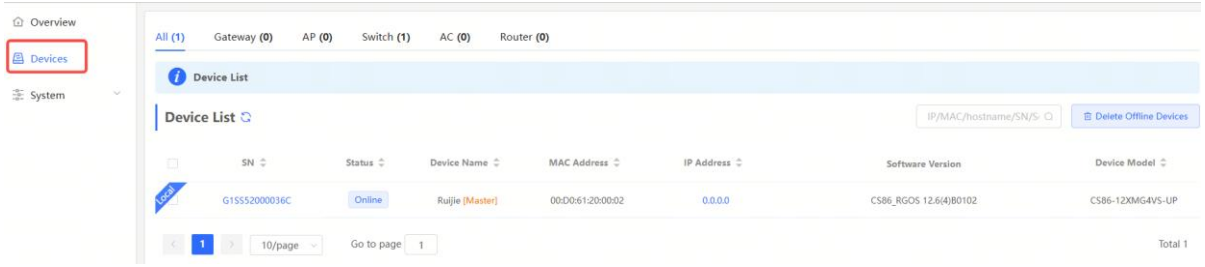
Figure3-10 Overview



3.4 Device

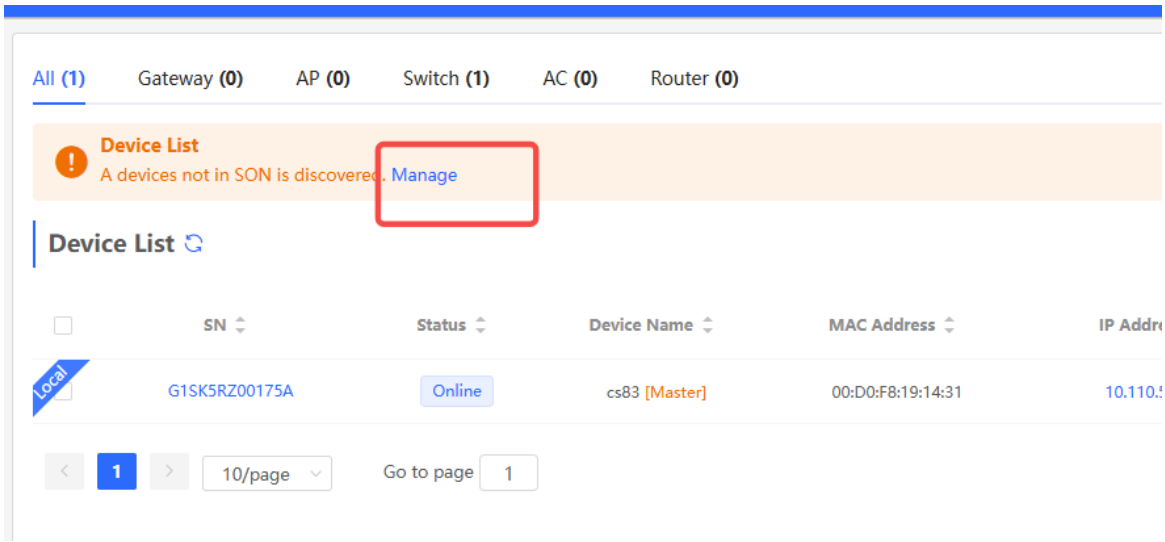
Click **Devices** in the menu bar to switch to the device list view. Then, you can view all the device information in the current networking. Users only need to log in to one device in the network to configure and manage devices in the entire network.

Figure3-11 Devices

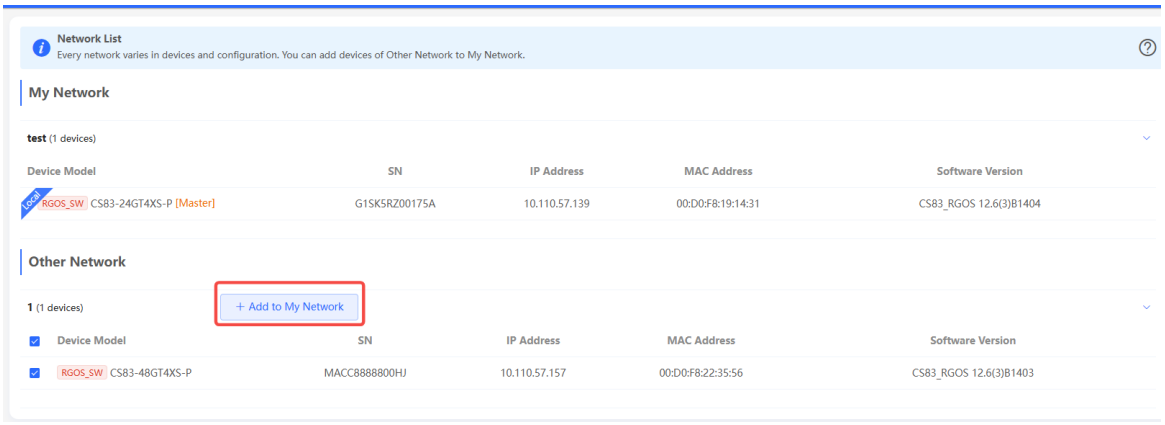


3.4.2 Adding Networking Devices

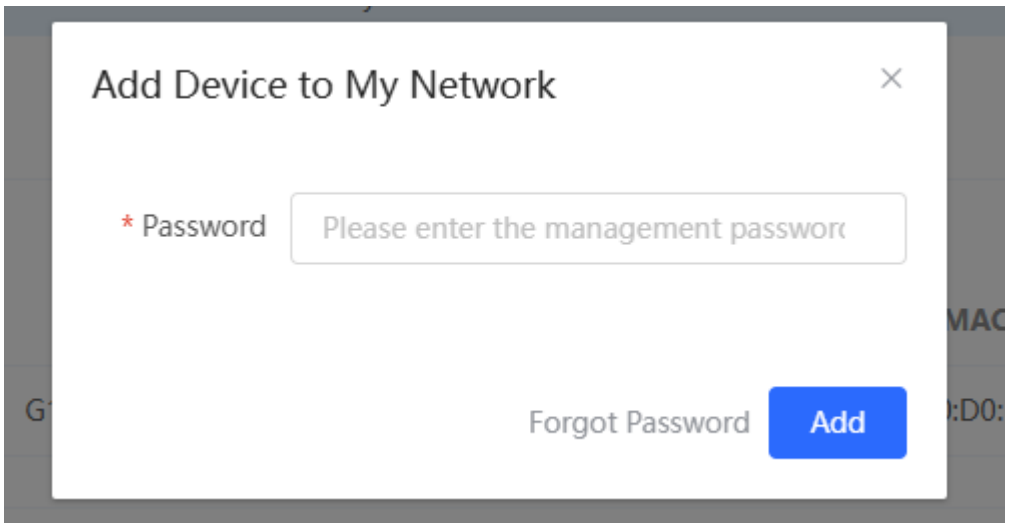
(1) When a new device connects to an existing device on the network, the system displays the message "A device not in SON is discovered." You can click **Manage** to add this device to the current network.



(2) After the system switches to the **Network List** page, click **Other Network**. In the **Other Network** section, select the device to be added to the network and click **Add to My Network**.



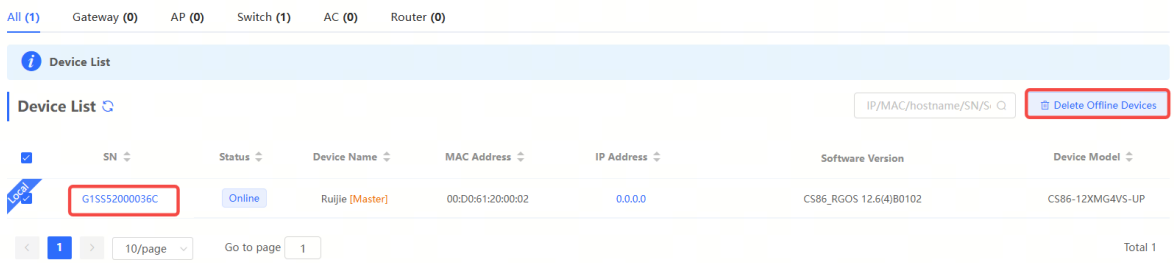
(3) You do not need to enter the password if the device to add is newly delivered from factory. If the device has a password, enter the configuring password of the device. Device addition fails if the password is incorrect.



3.4.3 Managing Networking Devices

Click the device **SN** to configure the specified device separately.

(1) Check offline devices and click **Delete Offline Devices** to remove them from the list and networking topology.



3.5 System Configuration

3.5.1 Setting the Web Login Password

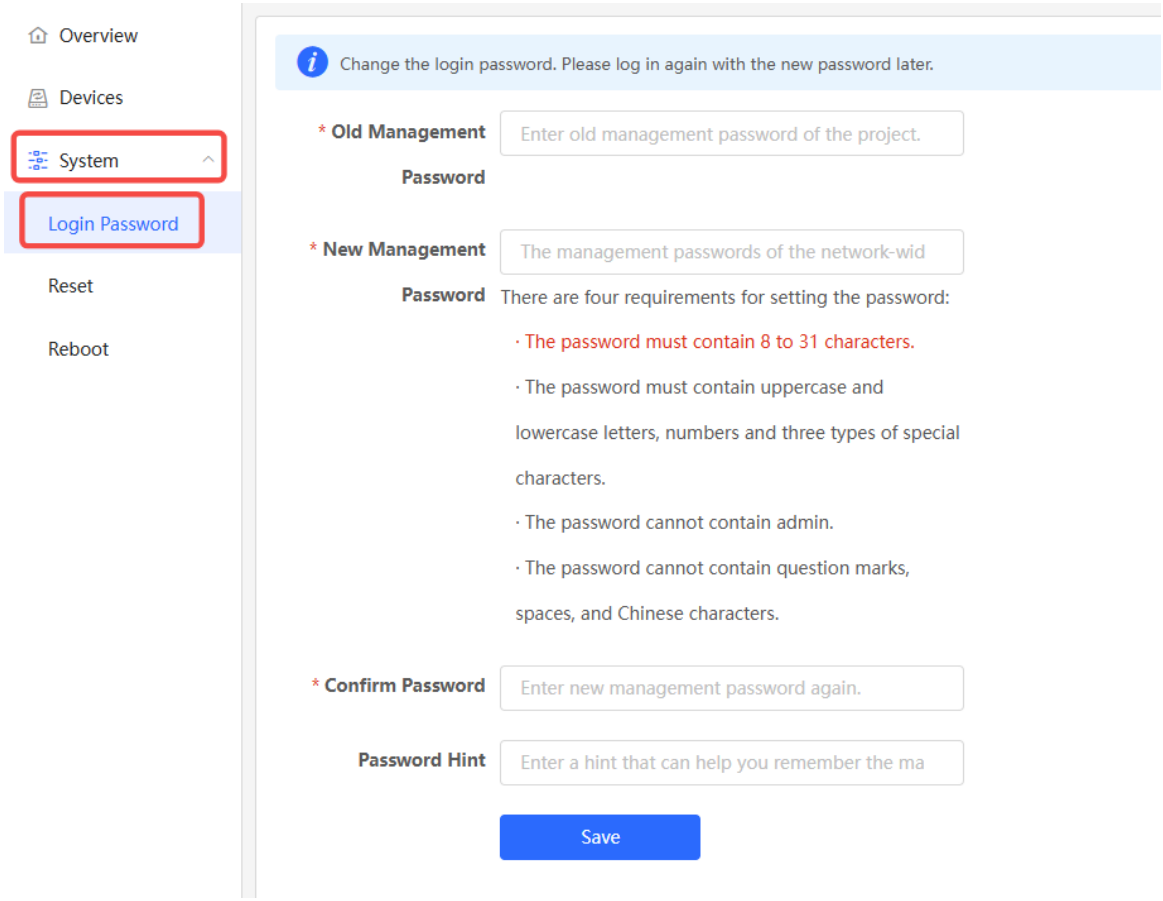
Choose **System** > **Login Password.**

Enter the old password and new password. After saving the configuration, use the new password to log in.

Caution

When self-organizing network discovery is enabled, the login password of all devices in the network will be changed synchronously.

Figure3-12 Login Password

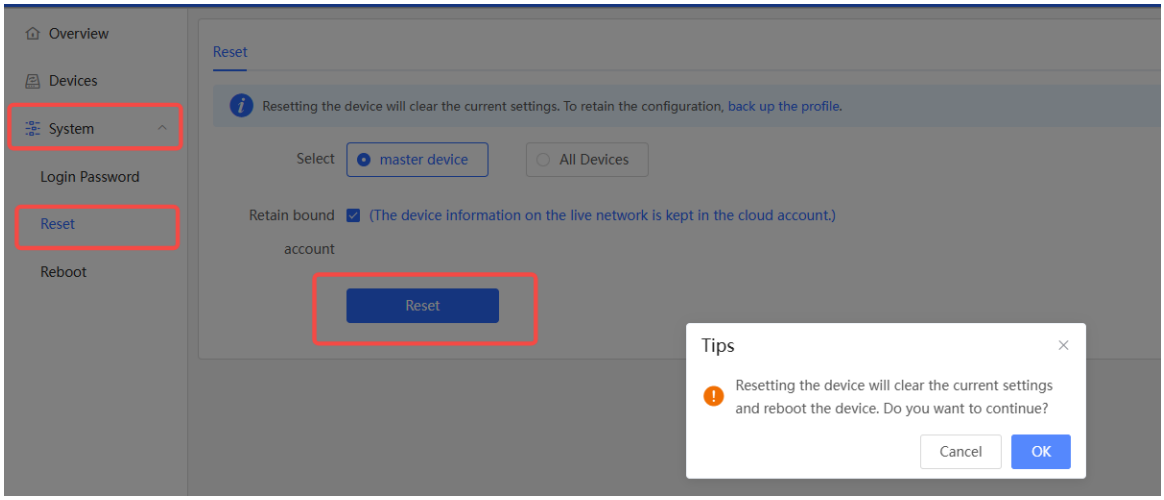


3.5.2 Reset

Choose **System** > **Reset**.

Click **Reset**, and click **OK** to restore factory settings.

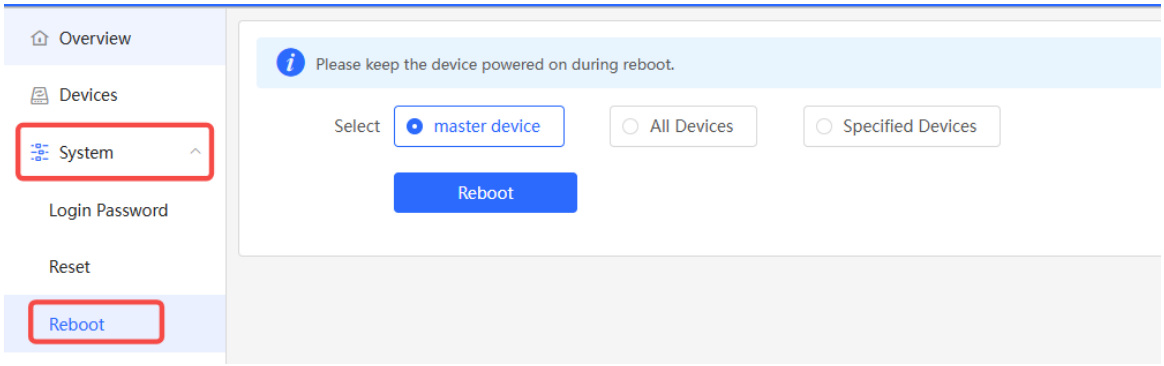
Figure3-13 Restore Factory Settings



3.5.3 Rebooting the Device

Choose **System** > **Reboot**. On the displayed page, click **Reboot** to restart the master device, all devices, or specified devices.

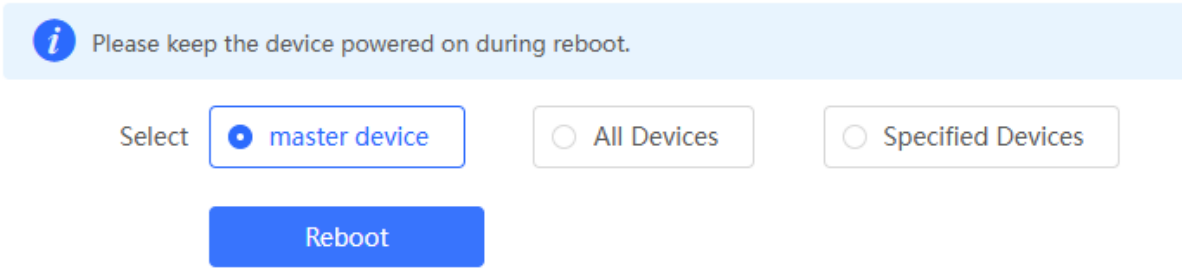
Figure3-14 Restart Device



1. Rebooting the Master Device

Select **master device** and click **Reboot**. The device will restart. Do not refresh the page or close the browser during the reboot. After the device is successfully rebooted and the Web service becomes available, the device automatically jumps to the login page.

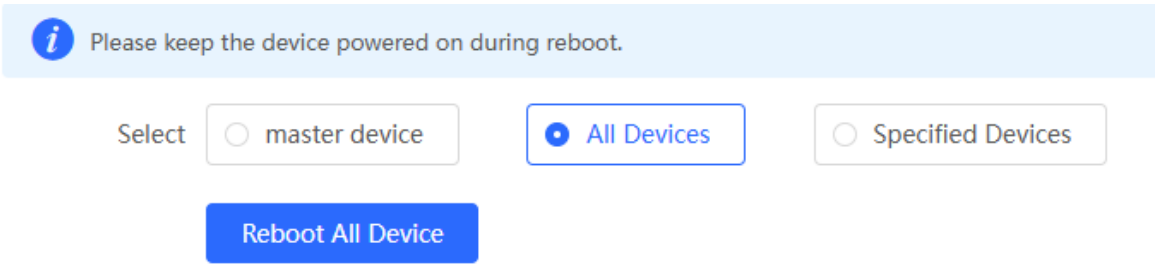
Figure3-15 Rebooting the Master Device



2. Rebooting the Devices in the Network

Select **All Devices**, and click **Reboot All Device** to reboot all devices in the current network.

Figure3-16 Rebooting the Devices in the Network



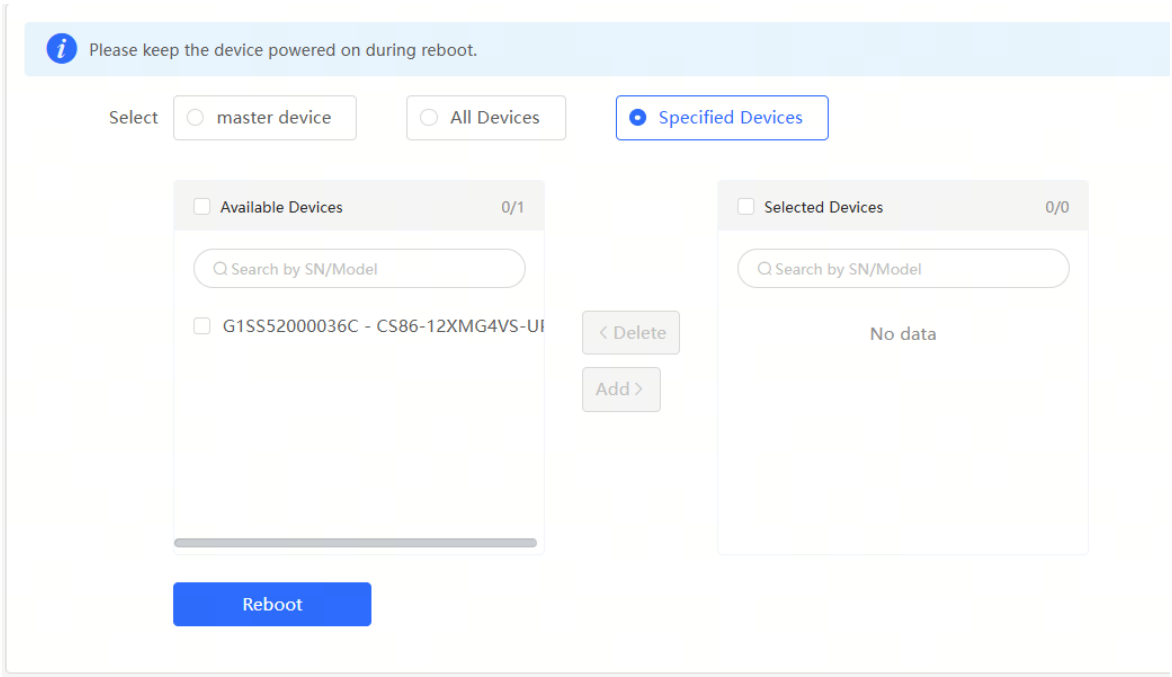
Caution

It will take some time for the network to reboot, please be patient. The network operation will affect the entire network. Therefore, exercise caution when performing this operation.

3. Rebooting Specified Devices in the Network

Click **Specified Devices**, select desired devices from the **Available Devices** list, and click **Add** to add devices to the **Selected Devices** list on the right. Click **Reboot**. Specified devices in the **Selected Devices** list will be rebooted.

Figure3-17 Restarting a Specified Device

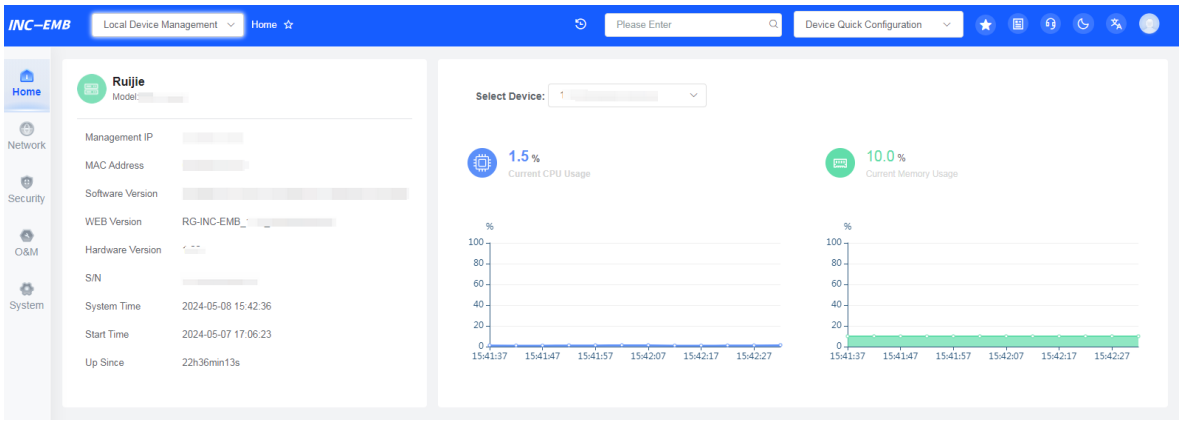


4 eWeb Management System

4.1 Main Interface

The main interface of the eWeb management system is displayed.

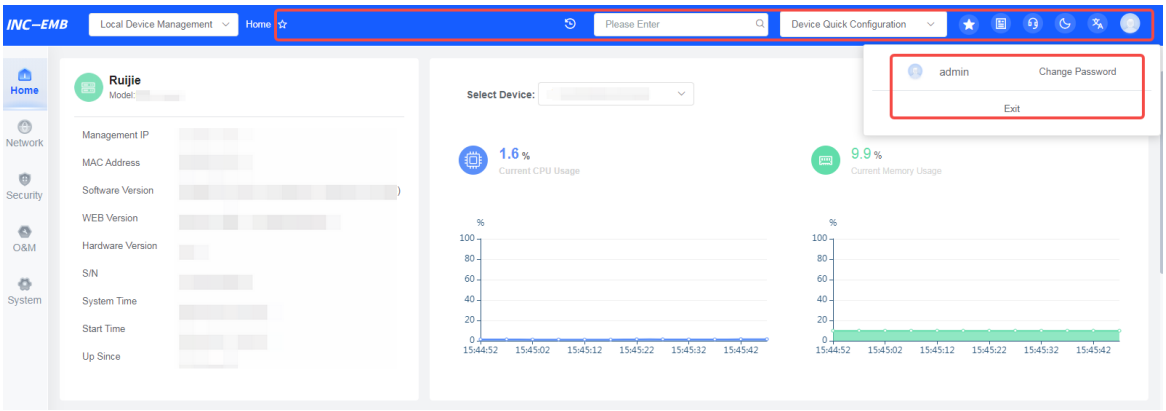
Figure4-1 Main Interface



4.1.2 Header

This area displays links to common functions, including the Favorite, Quick Search, Access History, Quick Setup, Change Language, Exit, Operation Log, Theme Switching, and Customer Service Center. You can click these links to switch to specific configuration pages.

Figure4-2 Header

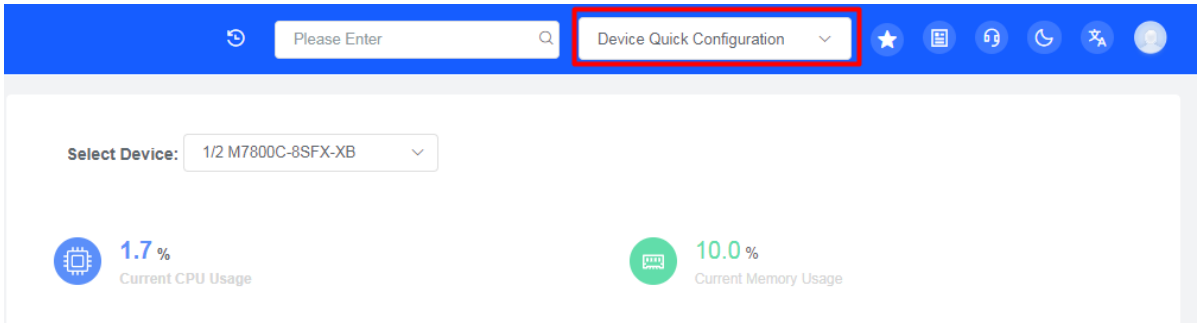


1. Quick Setup

The switch is not configured when you log in to the eWeb management system for the first time. You can use the **Quick Setup** wizard to configure common settings for the device.

Click **Device Quick Configuration** in the drop-down list box in the upper right corner to enter the **Device Quick Configuration** page, as shown in the following figure. For details, see the Quick Setup section.

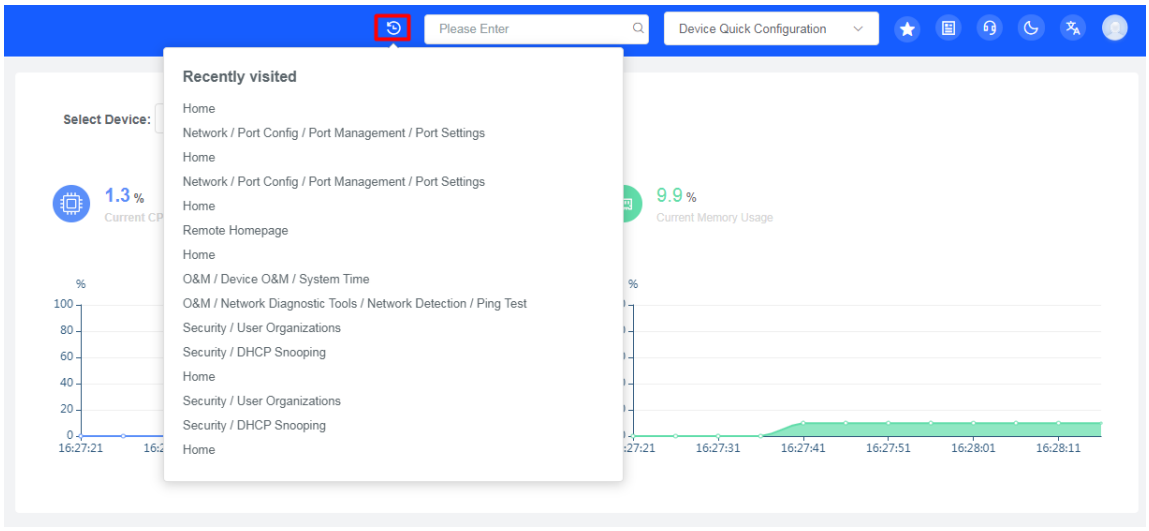
Figure4-3 Quick Setup



2. Access History

Click the **Recently visited** icon in the upper right corner to display the access history, as shown in Figure4-4. You can view the pages that you recently visited.

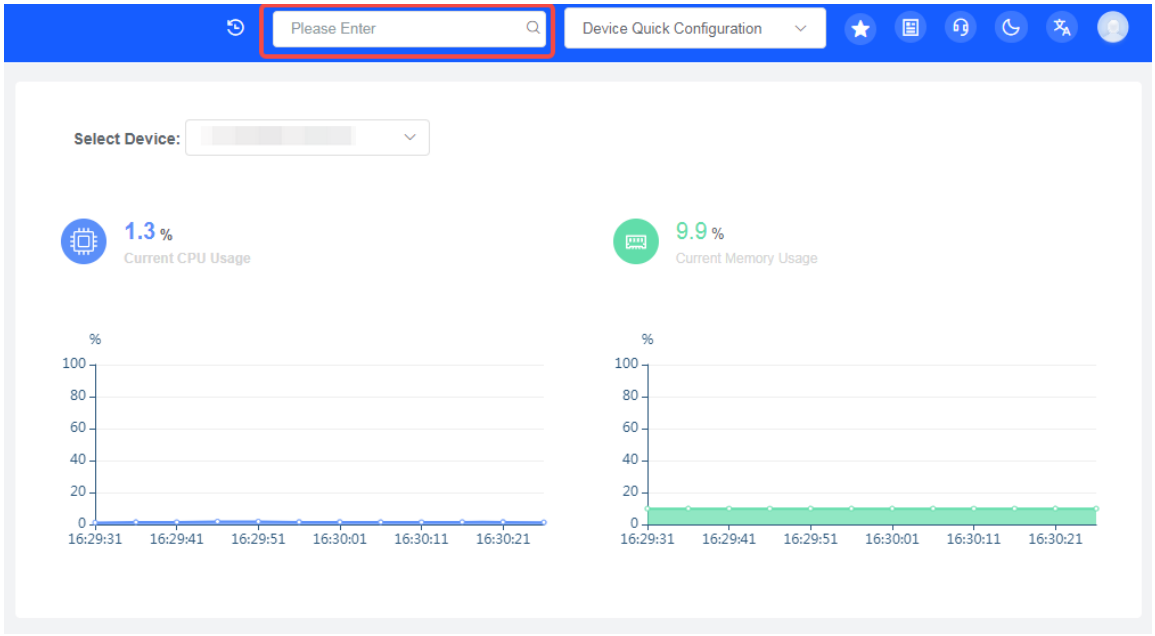
Figure4-4 Recently Visited



3. Quick Search

Click the **Quick Search** box in the upper right corner and then enter a keyword to perform a quick search, as shown in Figure4-5. You can search for items of **Control panel** and **Favorites** by entering a keyword, and view, select, and clear historical search items.

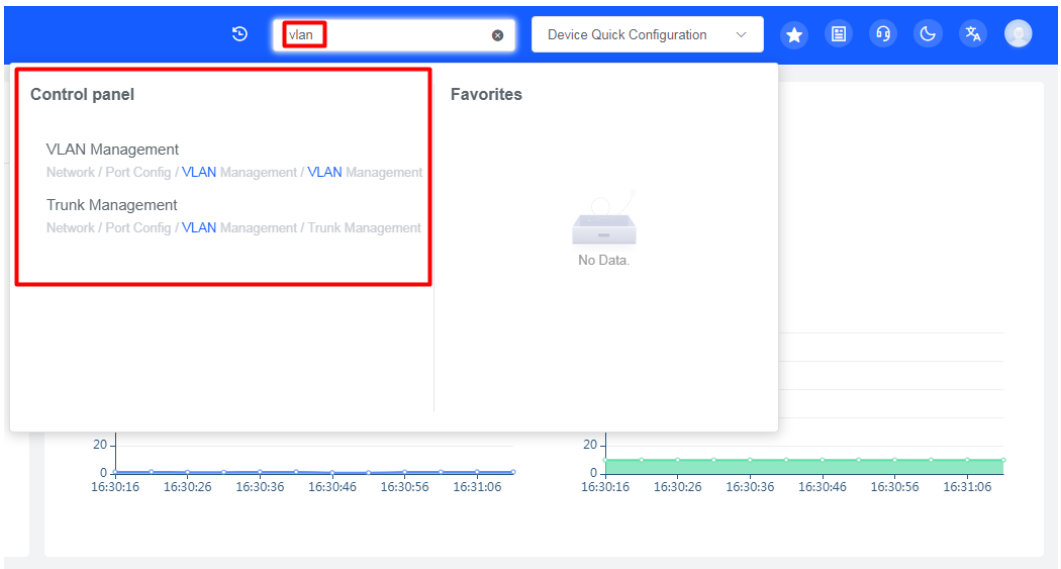
Figure4-5 Quick Search



- Searching for Items of Control Panel

  Enter a keyword in the search box to query the items of **Control panel**, as shown in Figure4-6.

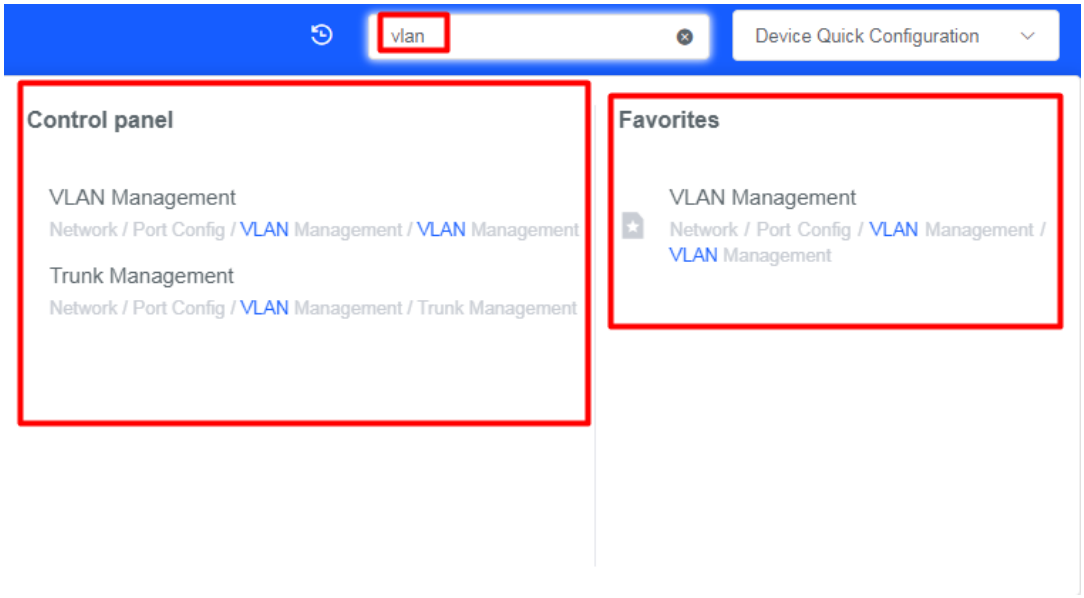
Figure4-6 Control Panel



- Searching for Favorites

  If the menu items corresponding to the keyword is added to your favorites, they are displayed in the **Favorites** area, as shown in Figure4-7.

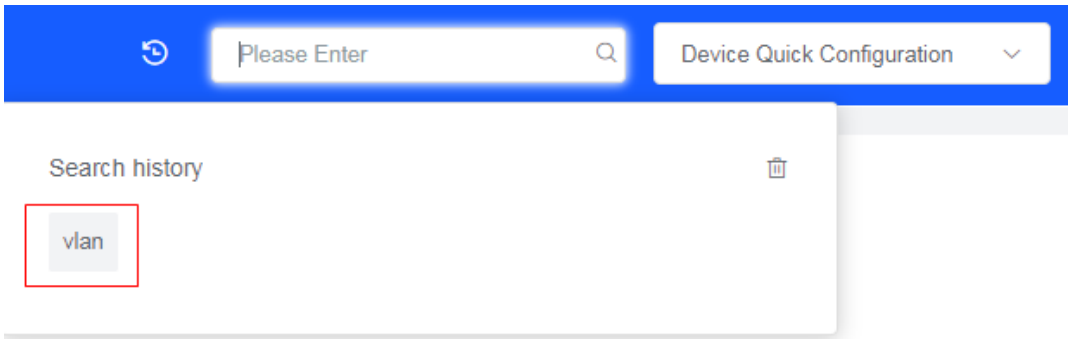
Figure4-7 Favorites



- Selecting the Search History

  In the **Search history** area, select the keyword, as shown in Figure4-8. Then, the related menu items are displayed in the **Control panel** area.

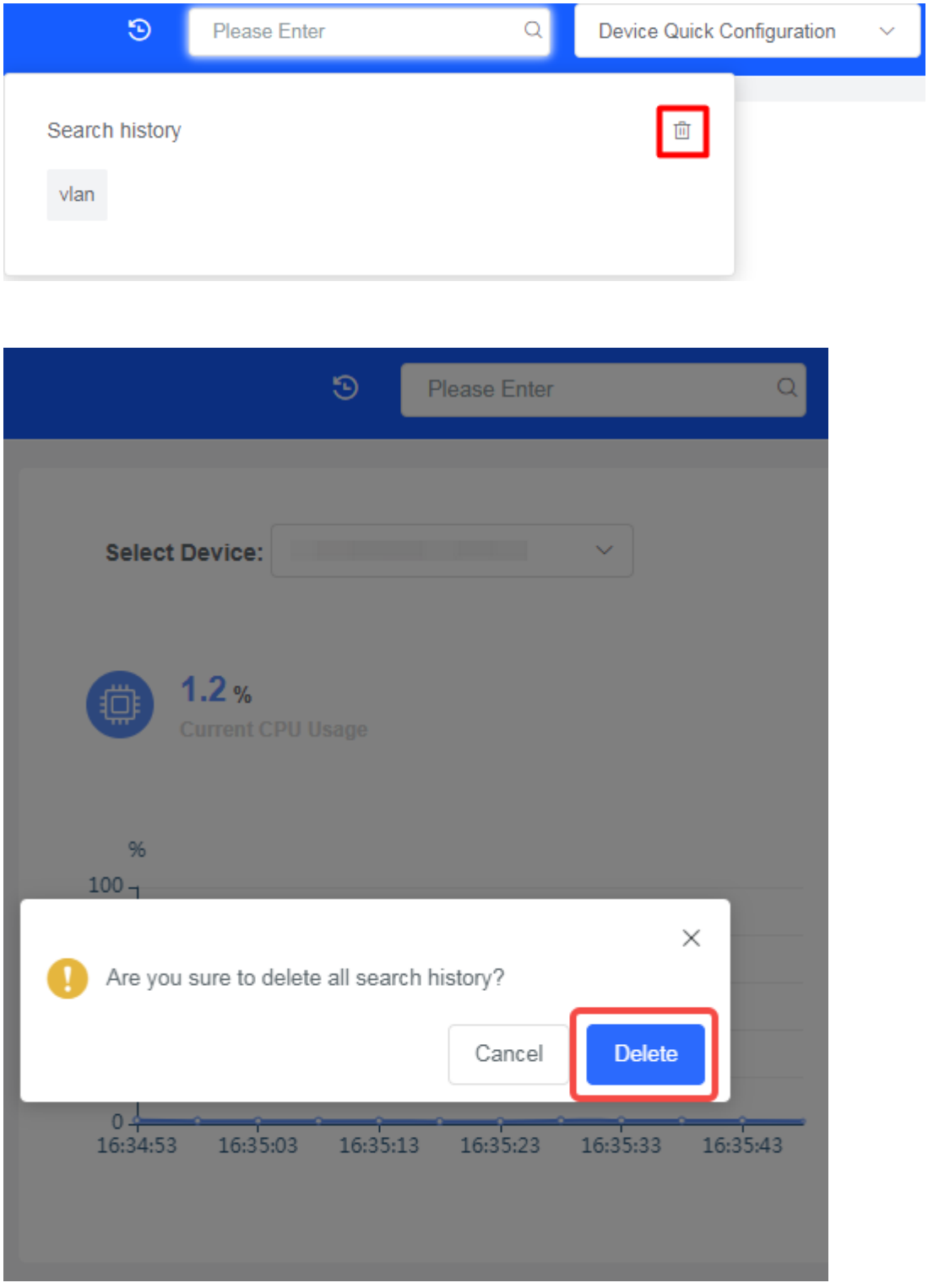
Figure4-8 Search History

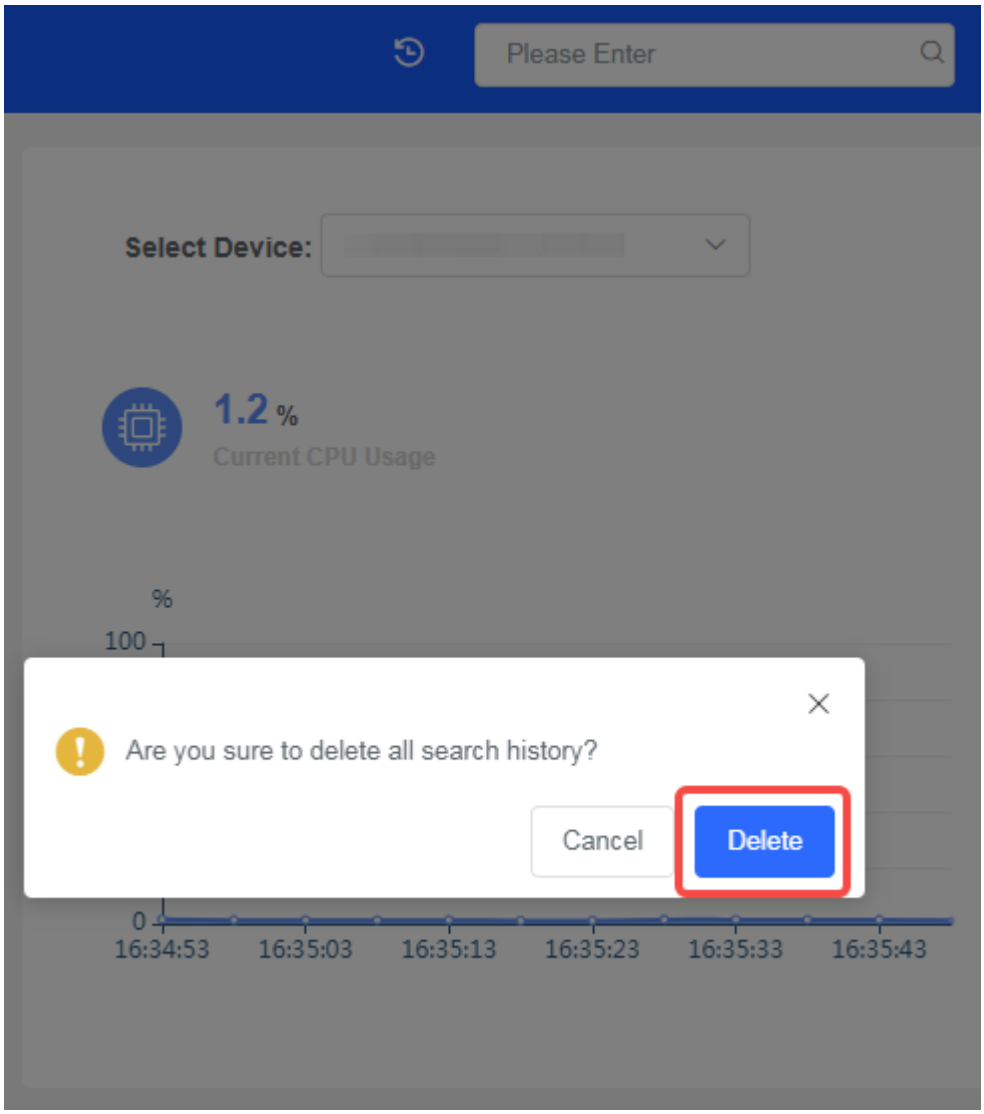


- Clearing the Search History

  As shown in Figure4-9, click the **Delete** icon in the upper right corner of the **Search history** area. In the dialog box that appears, select **Delete** to delete all search history entries.

Figure4-9 Clearing the Search History

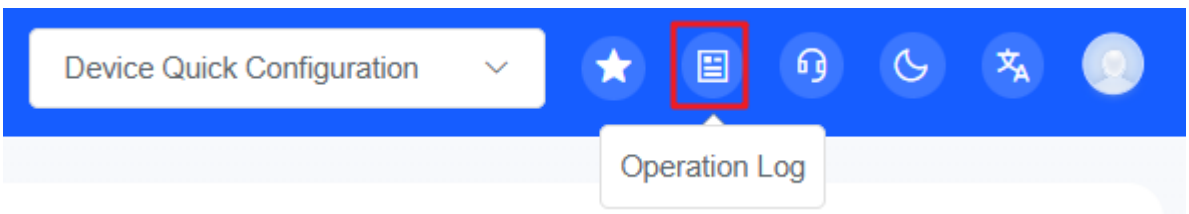




4. Operation Log

Click **Operation Log** in the upper right corner to go to the operation log page, as shown in the following figure. This page displays operation logs of the system. For details, see the Operation Log section.

Figure4-10 Operation Log

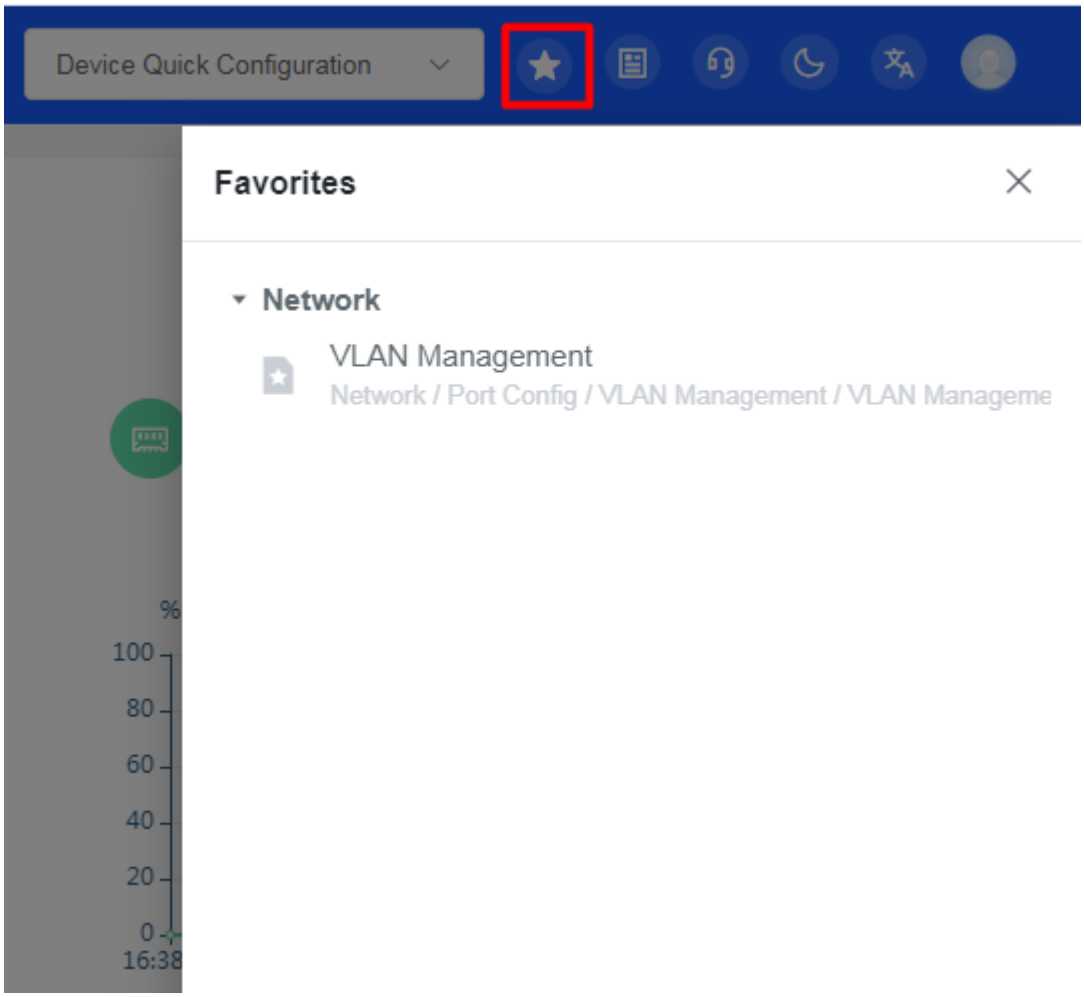


5. Favorites

- Favorites

Click the **Favorite** icon in the upper right corner to access the **Favorites** page, as shown in Figure4-11. You can query and remove favorite information on this page.

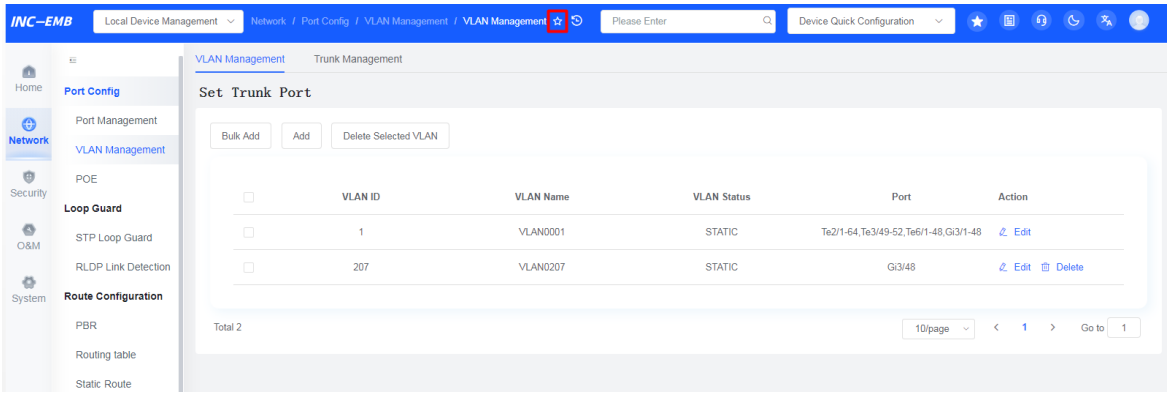
Figure4-11 Favorites



- Adding Pages to Favorites

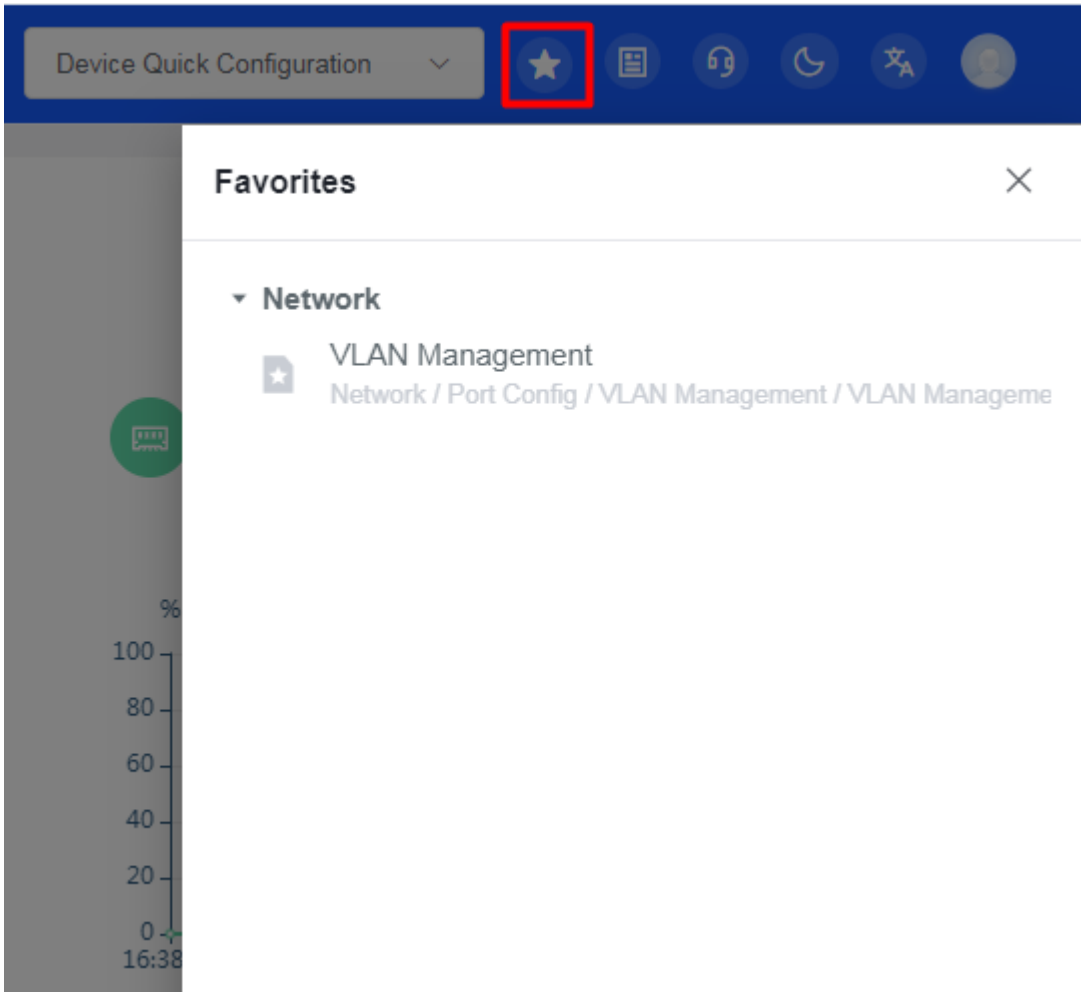
  For frequently accessed pages, add them to favorites so that you can quickly redirect to these pages next time. After you access the page of a function that you want to add to your favorites, click the **Favorites** icon in the top navigation bar, as shown in Figure4-12.

Figure4-12 Adding Pages to Favorites



Click the **Favorites** icon in the upper right corner to query favorite information, as shown in Figure4-13.

Figure4-13 Querying Favorite Information



- Canceling Favorite Pages

  For a page added to your favorites, the **Favorites** icon is highlighted. Click the highlighted **Favorites** icon to remove the page from favorites.

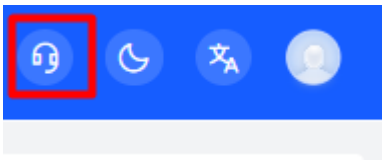
Figure4-14 Cancel Favorite Pages

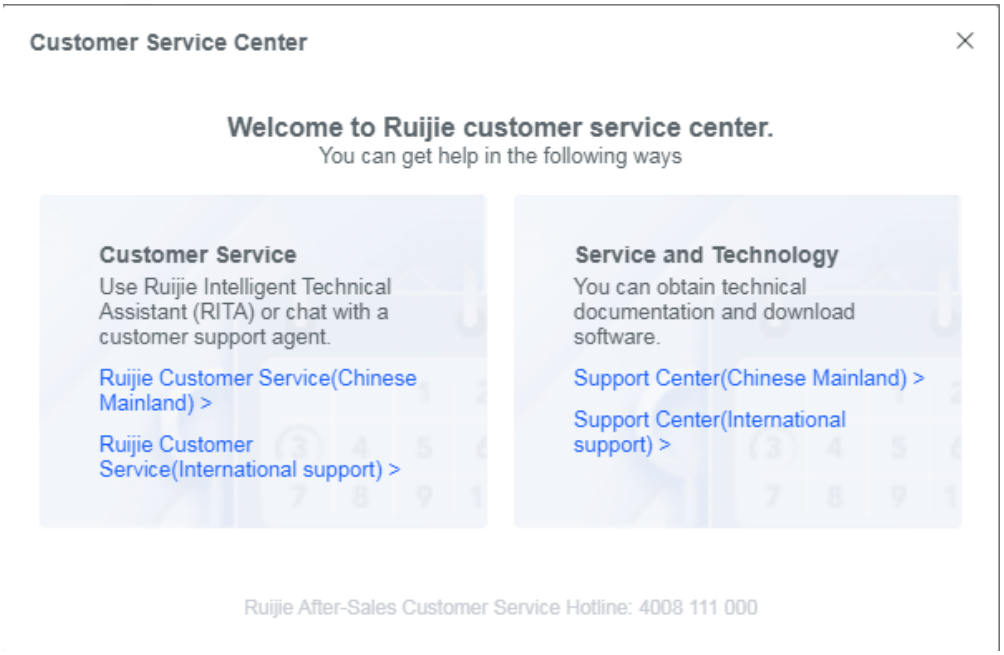


6. Customer Service Center

Click the **Customer Service** icon in the upper right corner to quickly access the customer service channels, including the **Customer Service** channel and **Service and Technology** channel, as shown in the following figure. You can click the links to obtain required services.

Figure4-15 Customer Service Center





7. Theme Switching

Click the Theme Switching icon in the upper right corner to switch the theme. The system supports two theme tones: light and dark, as shown in the following figure.

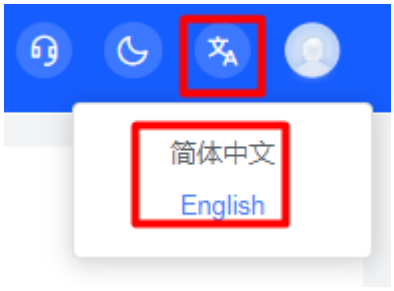
Figure4-16 Theme Switching



8. Language Switching

Click the Language Switching icon in the upper right corner to switch the system language. The system supports Chinese and English.

Figure4-17 Language Switching



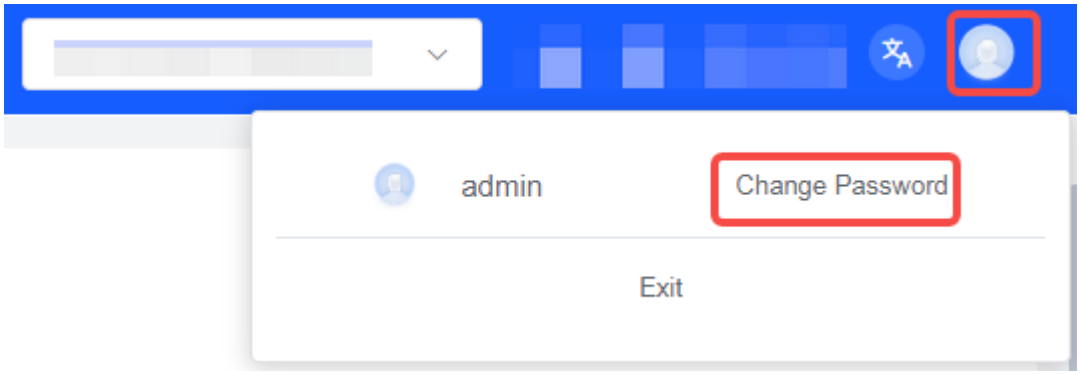
9. Changing Password

To change the password, click the Account icon in the upper right corner and click **Change Password**.

Caution

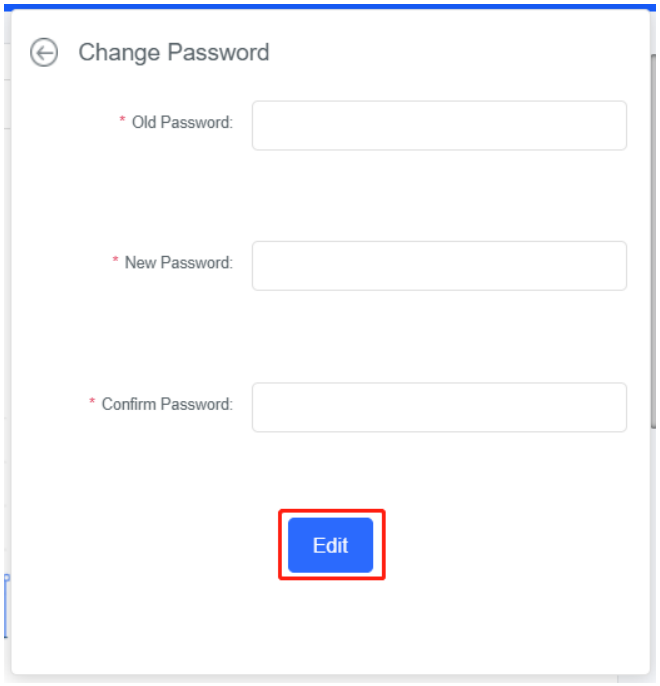
You can change the password only when you know the current password. If you forgot the password, please refer to the Forgot Password section.

Figure4-18 Change Password



Click **Change Password**. The **Change Password** window is displayed. Enter the old password and new password, and click **Edit**.

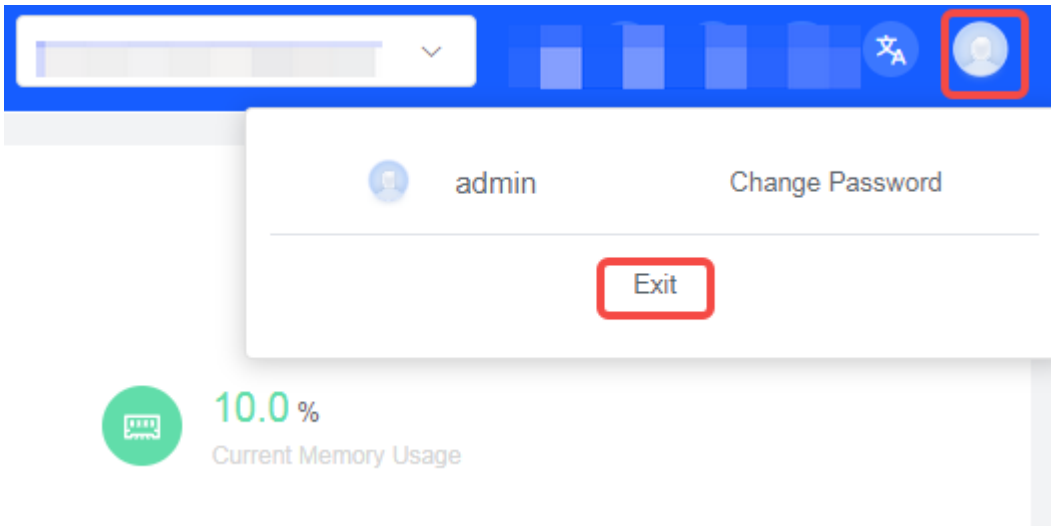
Figure4-19 Change Password



10. Exit

After the device management is complete, click **Exit** to exit the eWeb home page and return to the login page, as shown in the following figure.

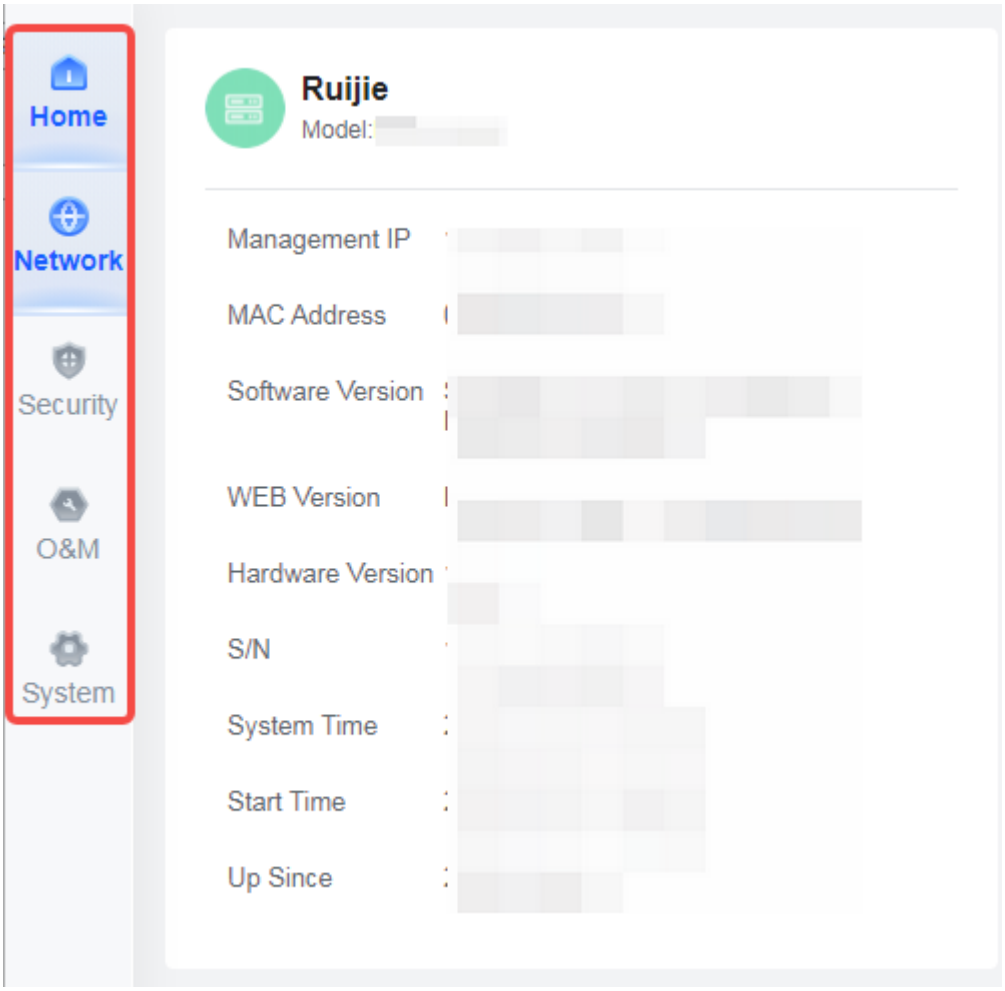
Figure4-20 Exit



4.1.3 Navigation Menu

This area displays main tabs of the eWeb management system.

Figure4-21 Navigation Menu



4.1.4 Main Operation Area

In this area, you can perform configurations on the eWeb management system. When you click the shortcut menu at the left of the page, the detailed configuration page is displayed.

4.2 Quick Configuration

The switch is not configured when you log in to the eWeb management system for the first time. To simplify the configuration, you can use the **Quick Setup** wizard to configure common settings for the switch.

Note

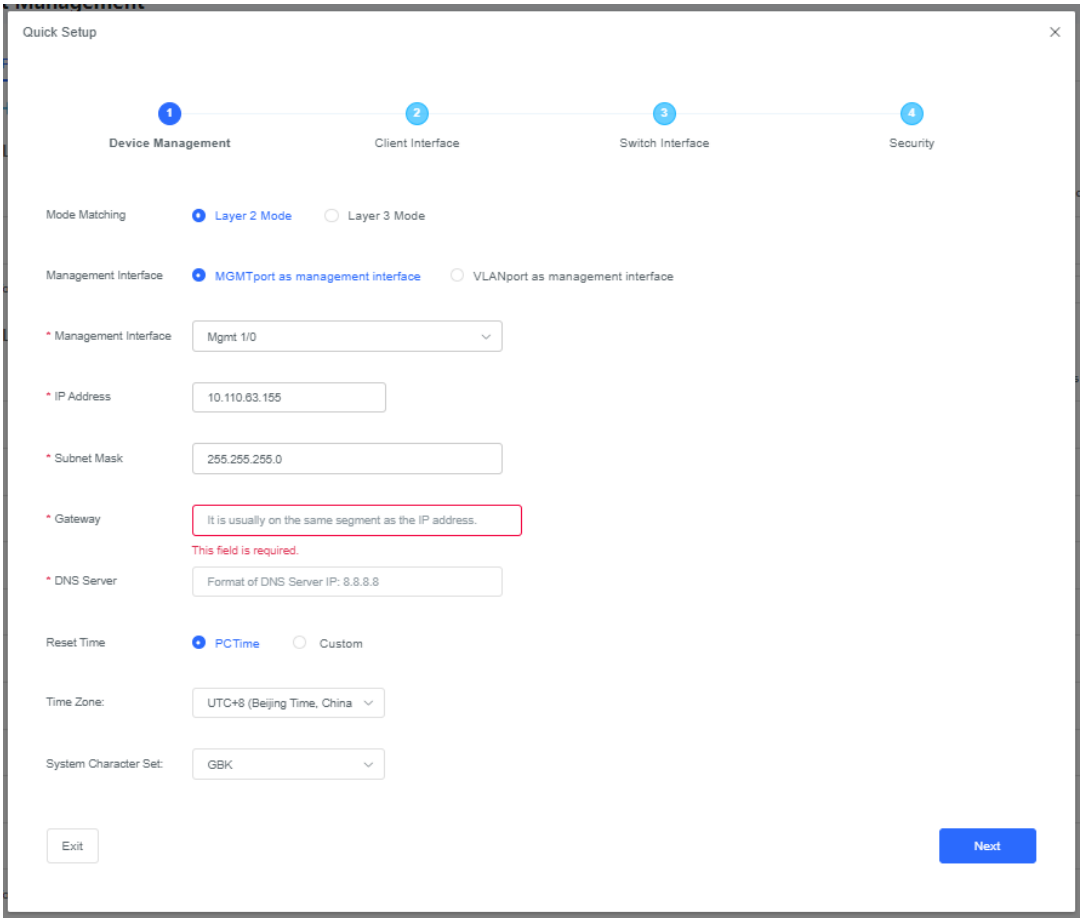
You can click **Device Quick Configuration** in the upper-right corner of the main interface of the eWeb management system to open the **Quick Setup** wizard.

4.2.1 Layer 2 Mode

There are four steps in this mode.

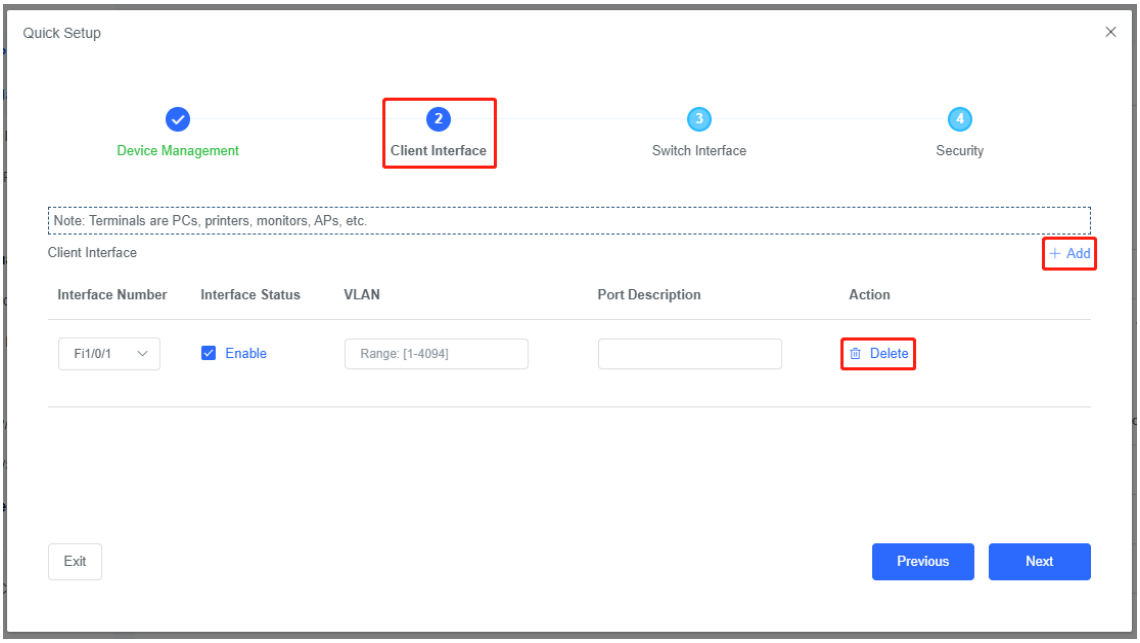
(1) Device Management

Figure4-22 Device Management



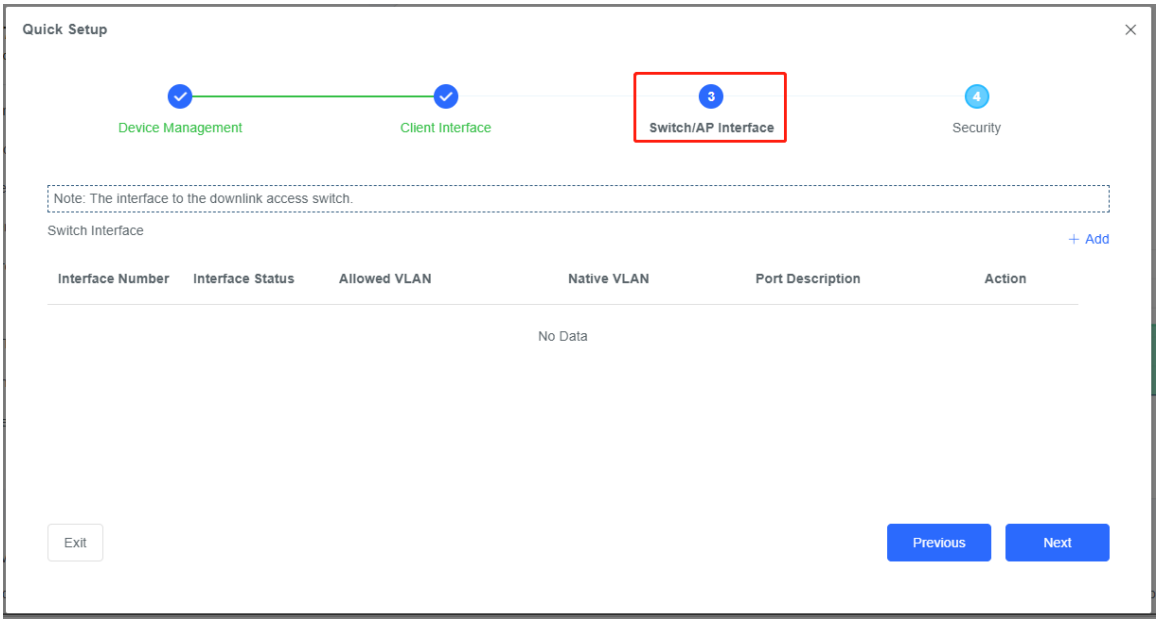
(2) Client Interface

Figure4-23 Client Interface



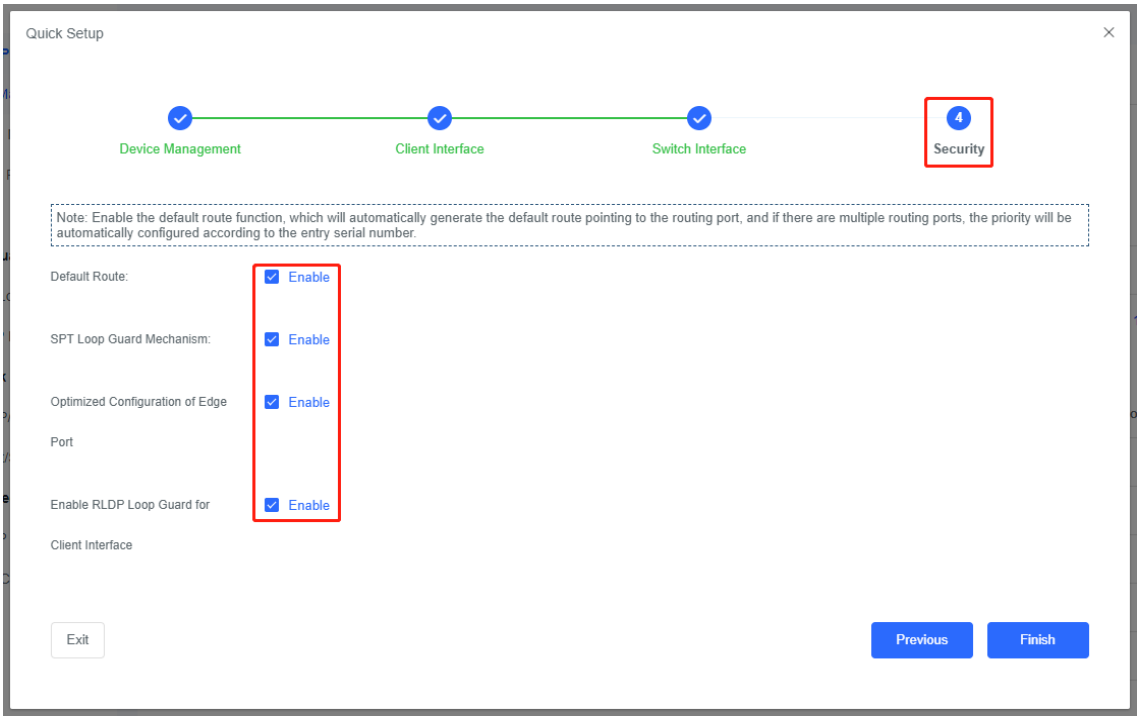
(3) Switch/AP Interface

Figure4-24 Switch/AP Interface



(4) Security

Figure4-25 Security



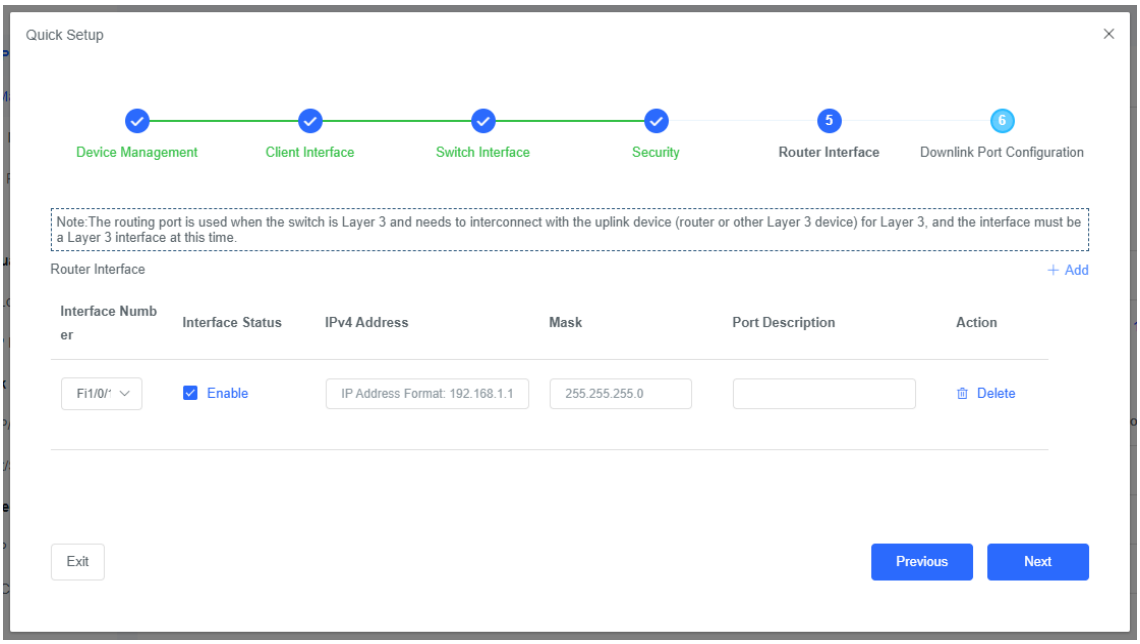
4.2.2 Layer 3 Mode

There are six steps in this mode.

The first four steps are the same as those in Layer 2 mode, so only the last two steps are described here.

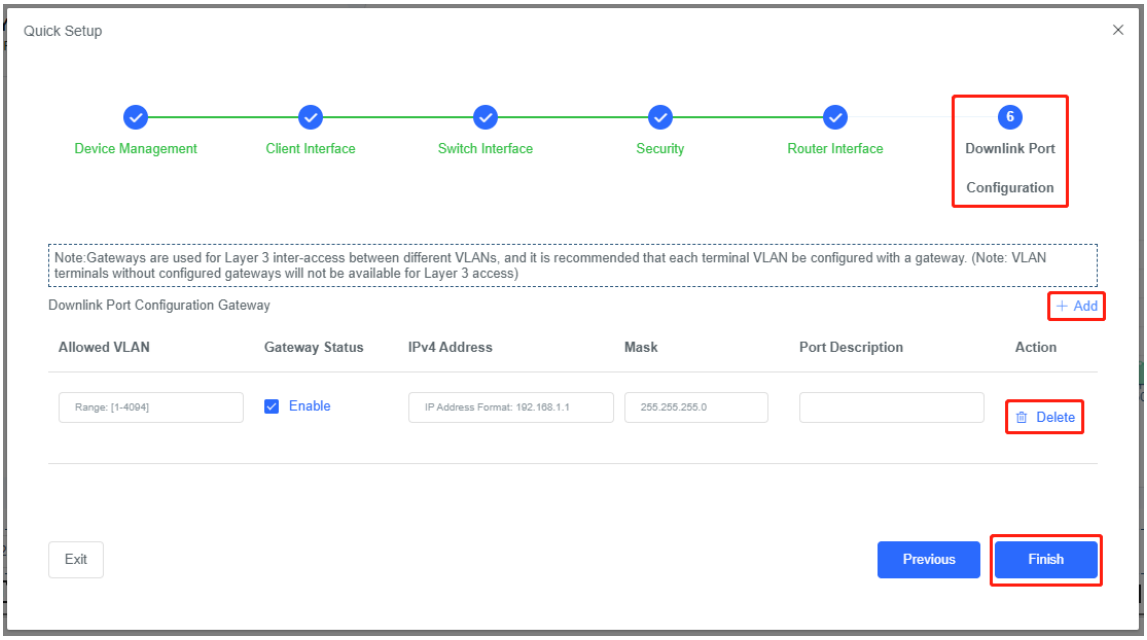
(1) Router Interface (Layer 3 Mode)

Figure4-26 Router Interface



(2) Downlink Port Configuration (Layer 3 Mode)

Figure4-27 Downlink Port Configuration



4.3 Home Page

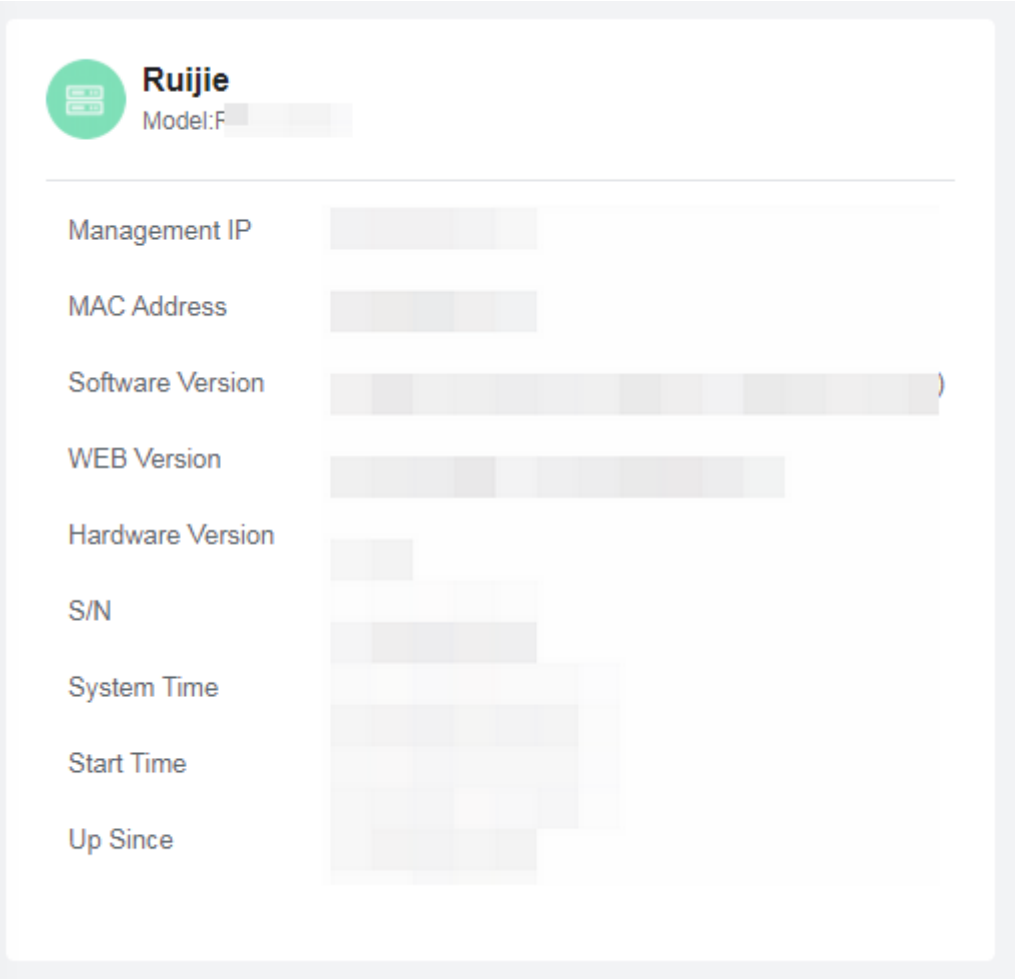
After you log in to the eWeb management system, you will be automatically redirected to the home page. Or, you can click **Home** in the navigation menu to switch to the home page.

On this page, you can view the CPU, memory usage, system version, current system time, and other information of the switch. By analyzing the trend of Top 5 interface traffic, you can identify common network problems on this page and quickly resolve these problems.

4.3.1 Overview

At the top of the home page, you can view the switch name, model, management IP address, MAC address, software version, hardware version, serial number, system time, startup time, and uptime. You can reset the system time on the **System Time** page by choosing **O&M** > **Device O&M** > **System Time**.

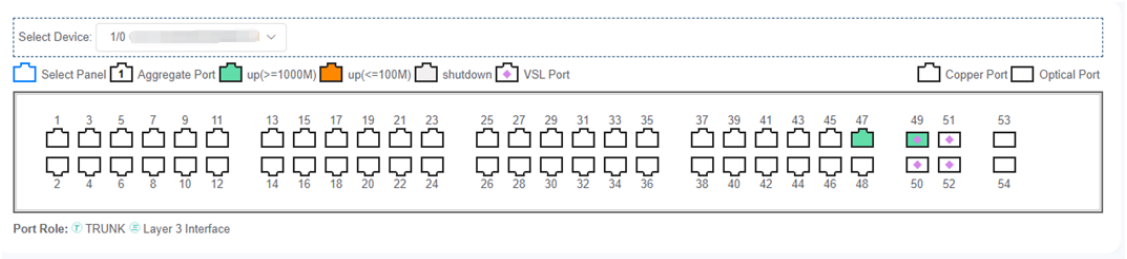
Figure4-28 Overview



4.3.2 Interfaces

In the upper part of the home page is the interface panel where interface information is displayed. The panel shows the basic interface configurations, such as interface type, state, aggregated interface, and virtual switching link (SVL) interface.

Figure4-29 Interfaces



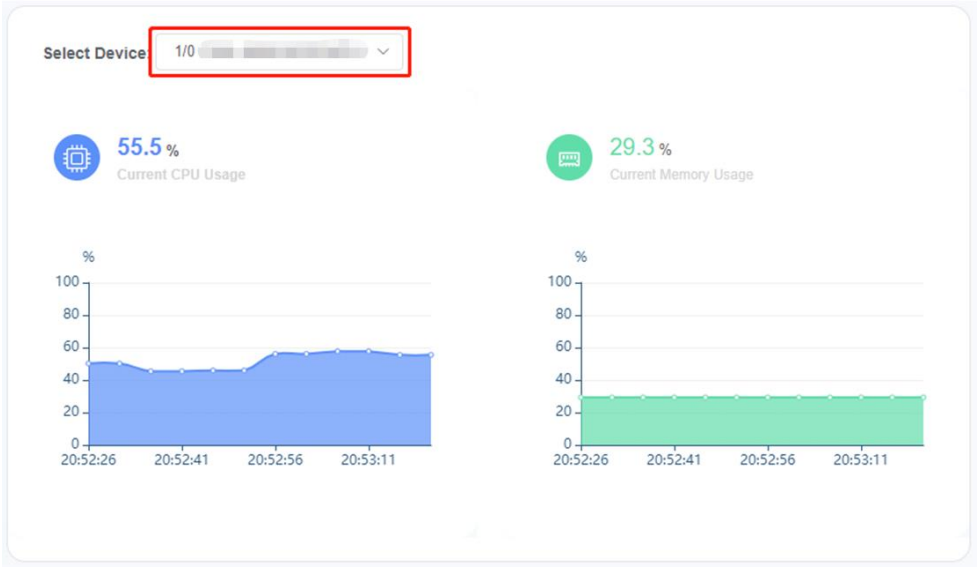
4.3.3 CPU/Memory Usage

The CPU and memory usage of the switch is displayed at the top of the home page.

(1) CPU: indicates the CPU usage of the device. It helps you learn about the device running status.

(2) Memory: indicates the memory usage of the device.

Figure4-30 CPU/Memory Usage

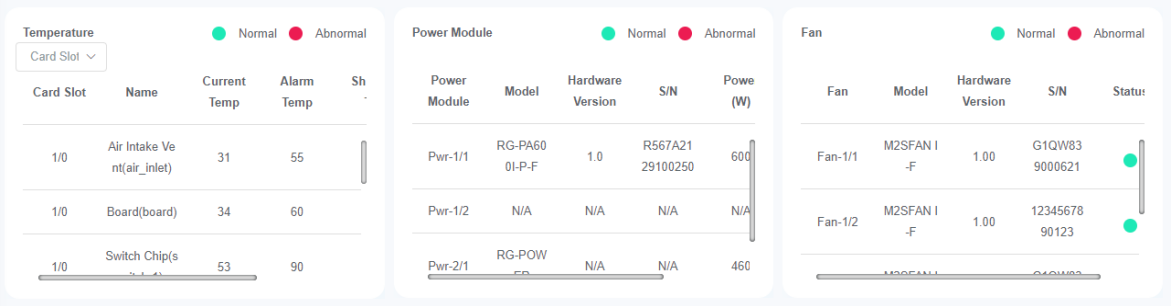


In the **Temperature** panel, you can view the temperature of a card slot by selecting a card clot from the **Card Slot** drop-down list box.

4.3.4 Temperature/Power Module/Fan

The middle part of the home page displays the temperature, power module status, fan status of the switch at different positions.

Figure4-31 Temperature/Power Module/Fan



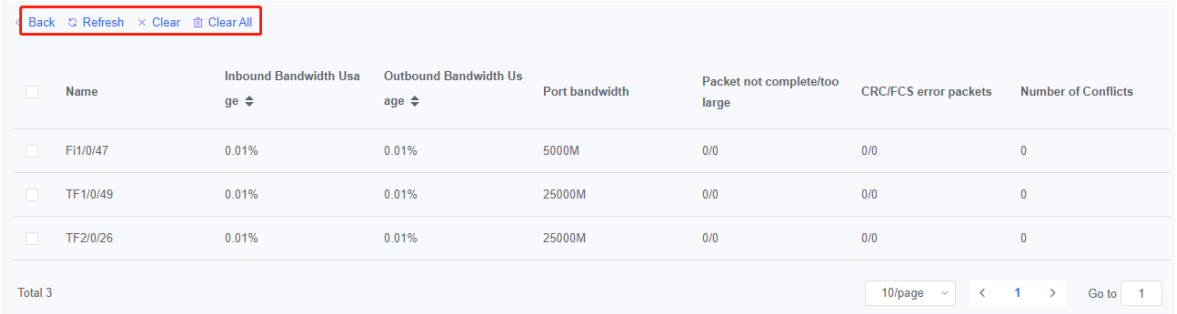
4.3.5 Bandwidth

Figure4-32 Bandwidth



You can click **More** in the **Top 5 Interface Bandwidth Usage** panel to query more details about interface bandwidth utilization.

Figure4-33 Top 5 Interface Bandwidth Usage



- Back: returns to the home page.
- Refresh: re-queries the interface bandwidth utilization.
- Clear: deletes statistics about a selected interface, such as the number of error packets and conflicting count.

- Clear All: deletes statistics about all interfaces, such as the number of error packets and conflicting count.

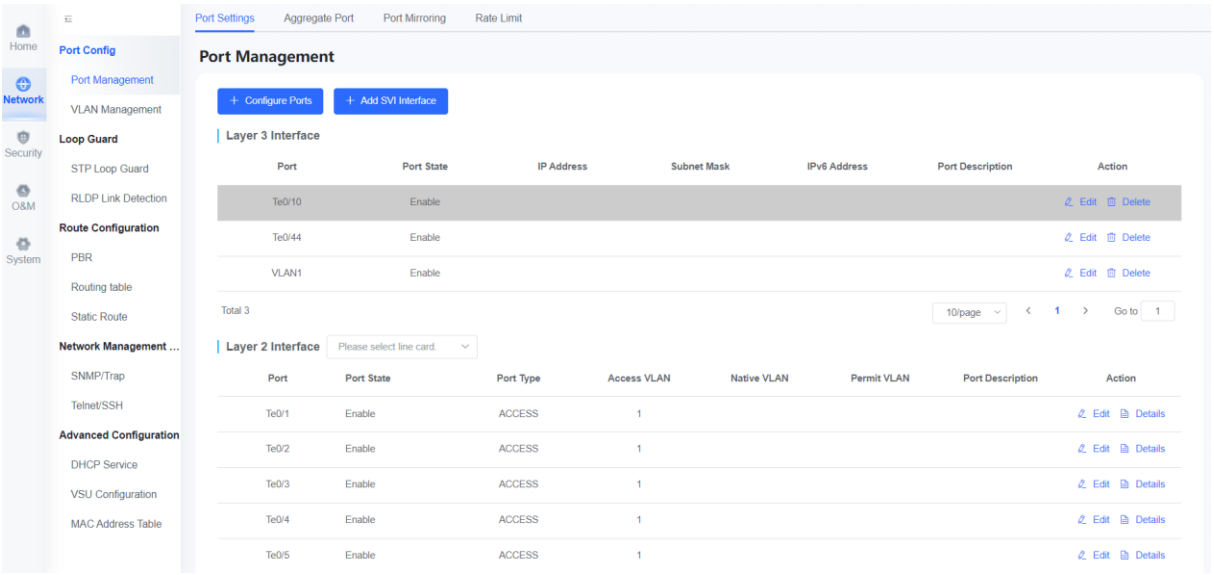
4.4 Network

4.4.1 Port Config

1. Port Management

Choose **Network** > **Port Config** > **Port Management** > **Port Configuration** to access the Port Configuration page.

Figure4-34 Port Management

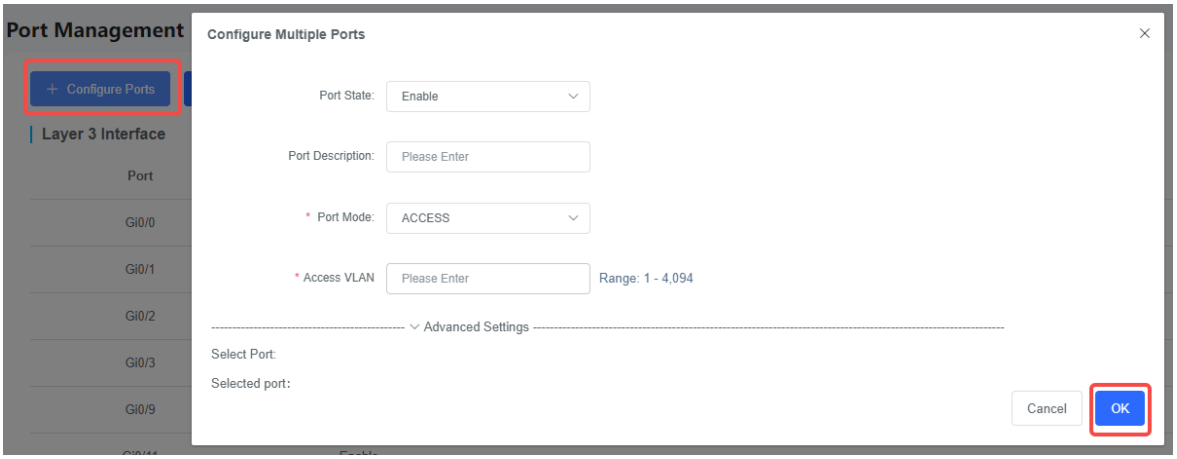


(2) Port Configuration

- Configuring multiple ports

  Click **Configure Ports** and the **Configure Multiple Ports** window is displayed. Set configuration parameters and click **OK**.

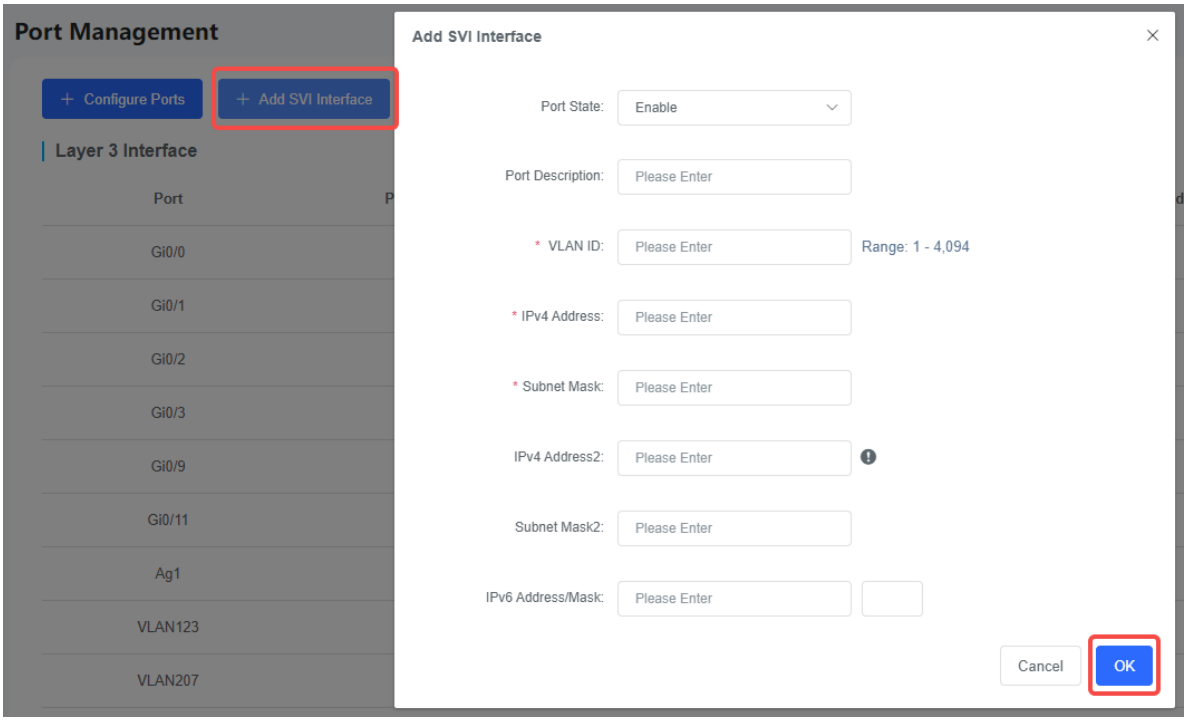
Figure4-35 Port Configuration



- Adding SVI Interface

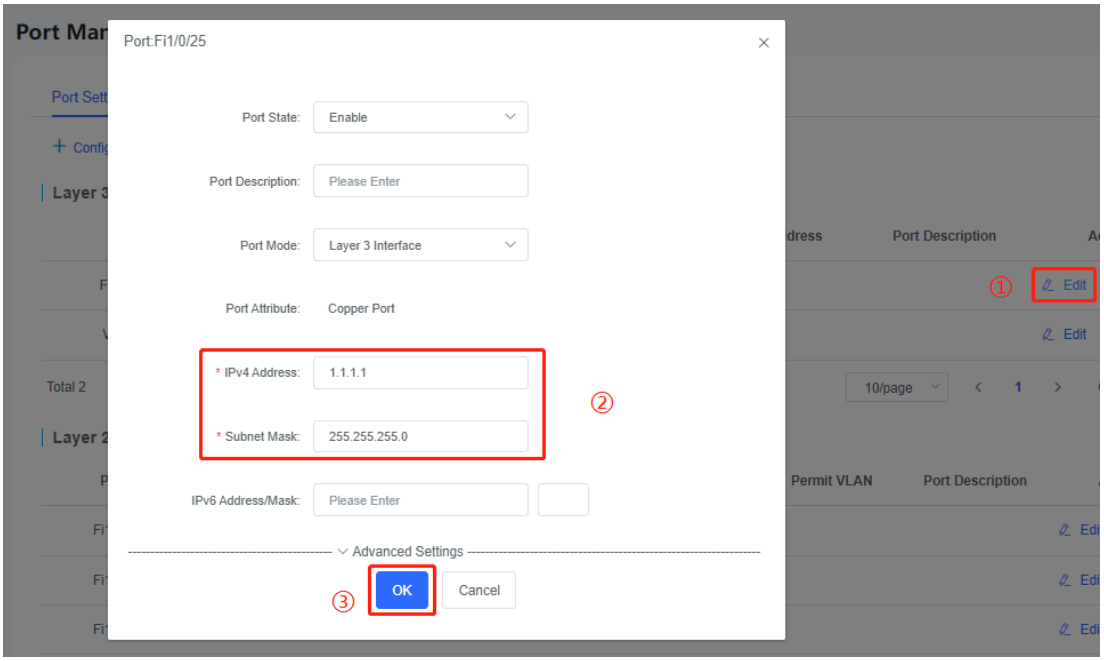
  Click **Add SVI Interface**. Set configuration parameters in the displayed window. Click **OK**. The result can be viewed in the **Layer 3 Interface** list.

Figure4-36 Adding SVI Interface



- Editing a Layer 3 interface
- Click **Edit**. Set configuration parameters in the displayed window. Click **OK**. The result can be viewed in the interface list. When the **Port Mode** is **Layer 3 Interface**, the result is displayed in the Layer 3 interface list. When the **Port Mode** is **Trunk Port** or **Access Port**, the result is displayed in the Layer 2 interface list.

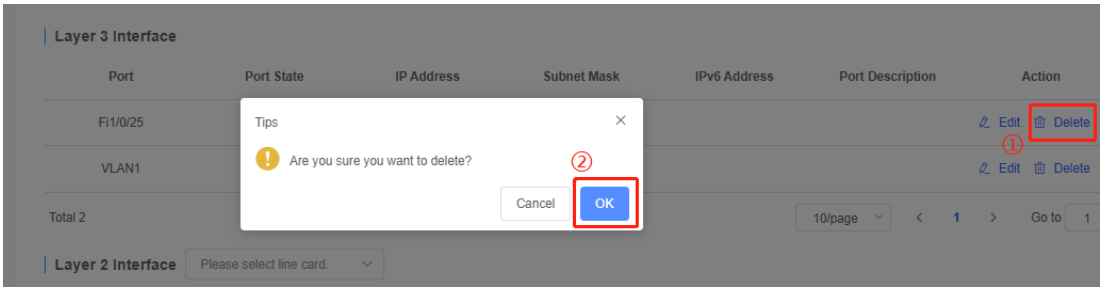
Figure4-37 Editing a Layer 3 interface



- Deleting a Layer 3 interface

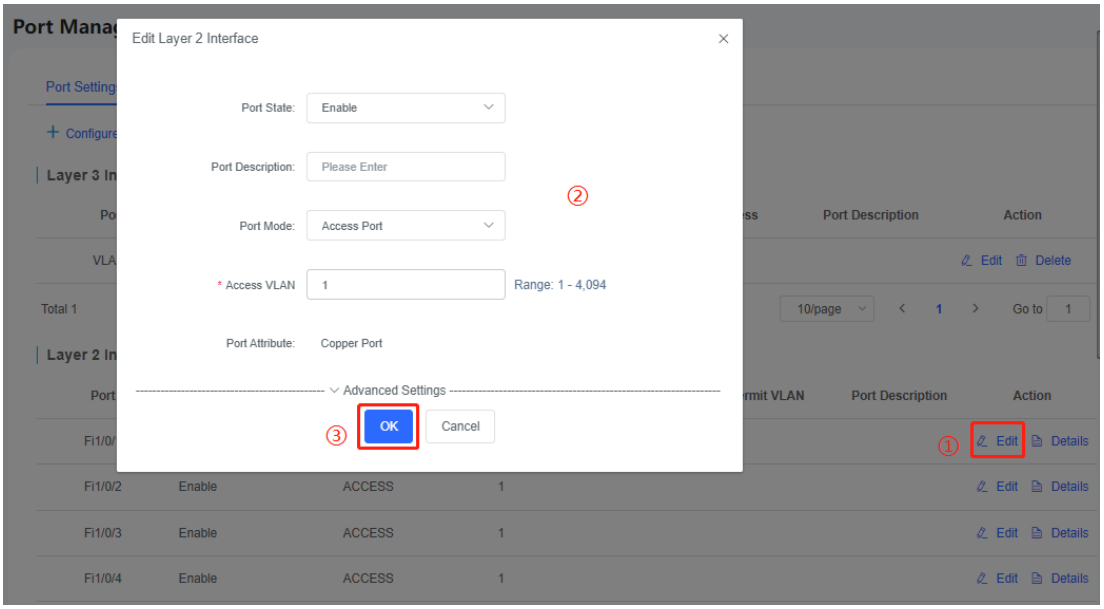
  Click **Delete**. Click **OK** in the displayed window. The selected port can be removed from in the interface list.

Figure4-38 Deleting a Layer 3 interface



- Editing a Layer 2 interface
- Click **Edit**. Set configuration parameters in the displayed window. Click **OK**. The result can be viewed in the interface list. When the port mode is a Layer 3 port, the result can be viewed in the Layer 3 port list. When the port mode is a trunk port or an access port, the result can be viewed in the Layer 2 port list.

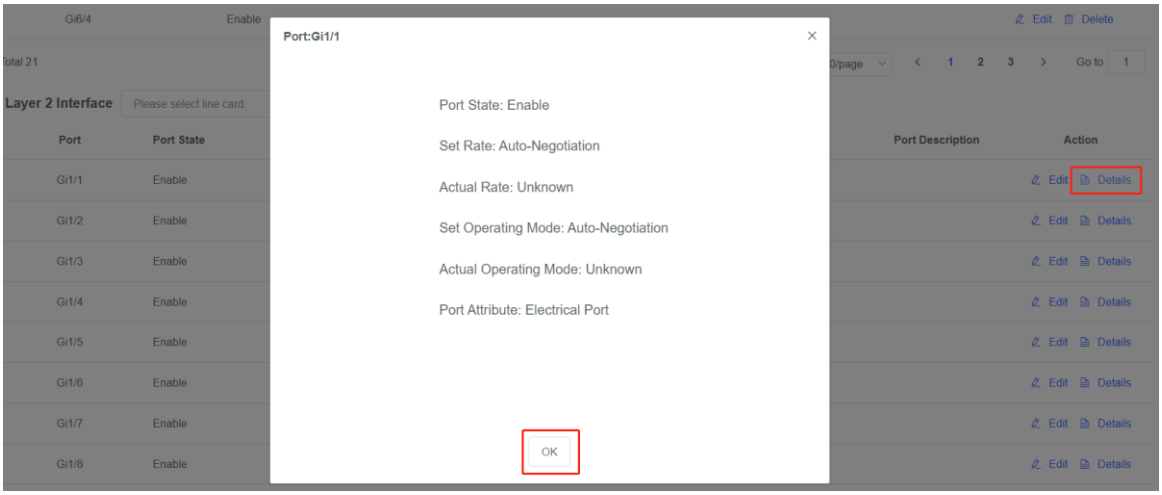
Figure4-39 Editing a Layer 2 interface



- A Layer 2 interface details

  Click **Details**. You can view detailed information about a selected port.

Figure4-40 A Layer 2 interface details



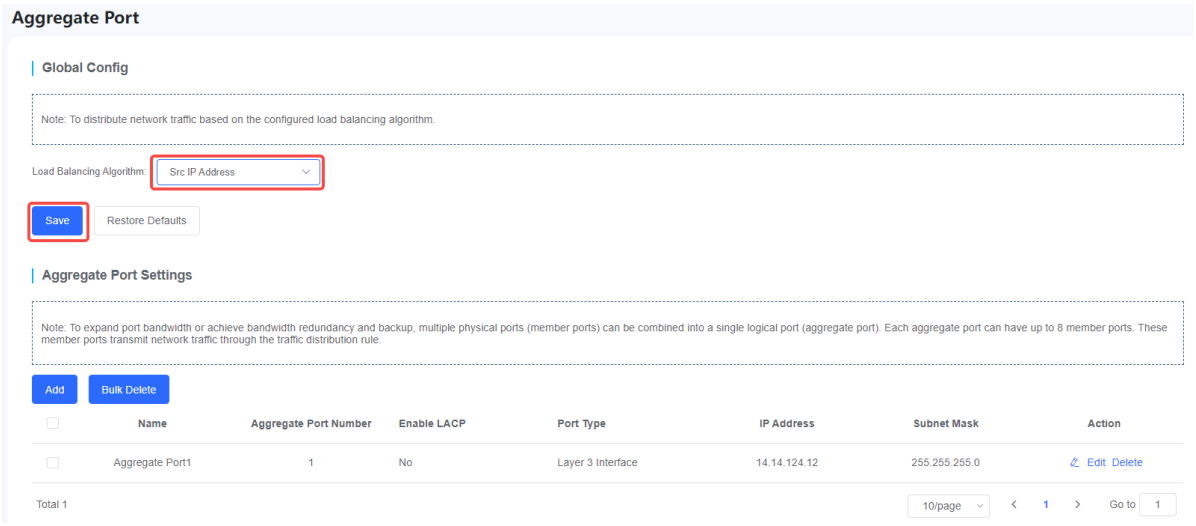
(3) Aggregate Port

To expand port bandwidth or achieve bandwidth redundancy and backup, multiple physical ports (member ports) can be combined into a single logical port (aggregate port). Each aggregate port can have up to 8 member ports. These member ports transmit network traffic through the traffic distribution rule.

- Global Config

  Select an algorithm from the **Load Balancing Algorithm** drop down list box. Click **Save**.

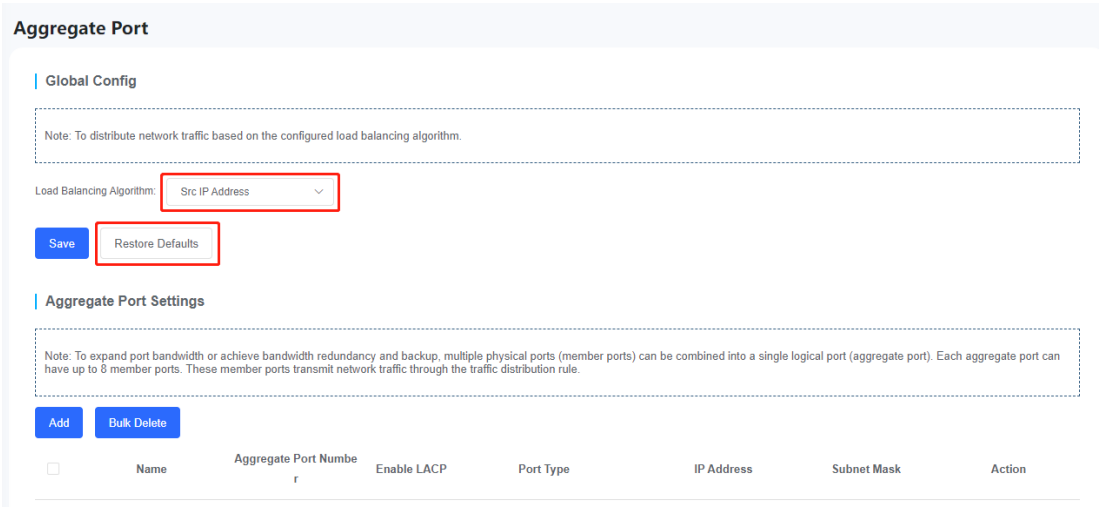
Figure4-41 Global Config



- Restoring default settings

  Click **Restoring Defaults** to restore the load balancing algorithm to the default algorithm.

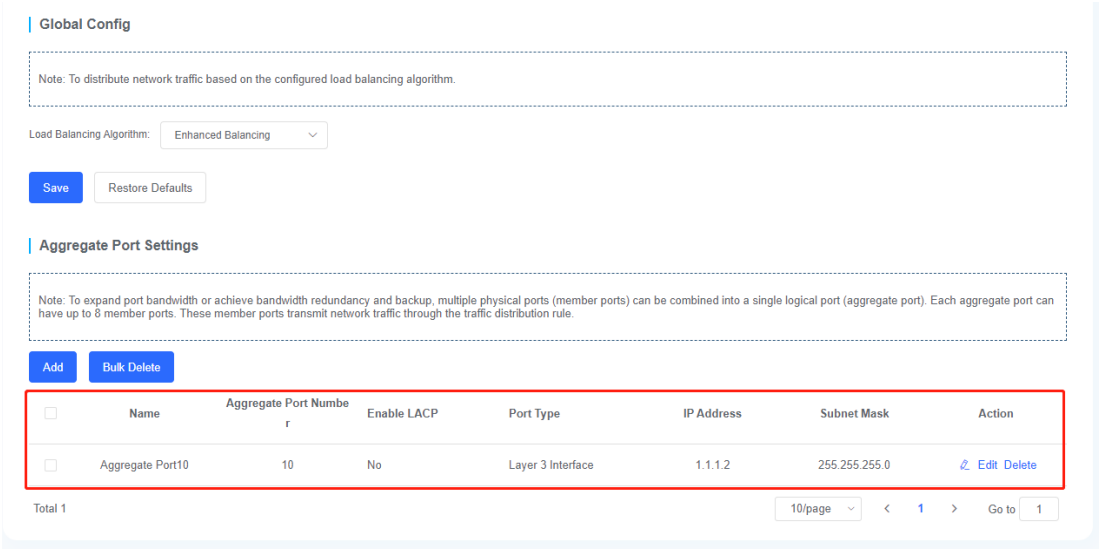
Figure4-42 Restoring default settings



- Aggregate interface

  Aggregate interface list: displays all aggregate ports and related information, including the name, port number, LACP status, port type, IP address, and subnet mask.

Figure4-43 Querying the aggregated port list



- Adding an aggregated port

  Click **Add**. Set configuration parameters in the displayed window. Click **Add**. The result can be viewed in the Aggregate Port list.

Figure4-44 Adding an aggregated port-1

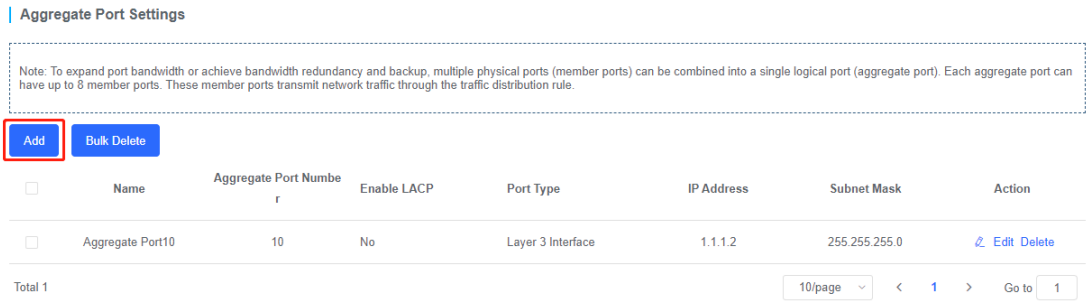
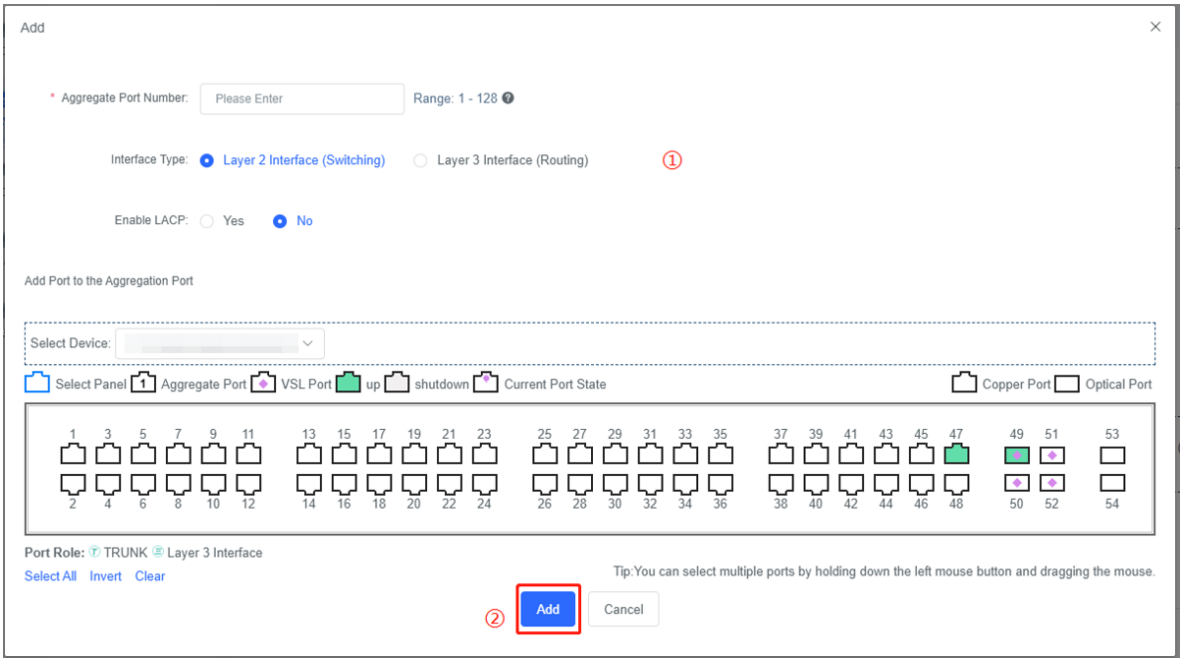
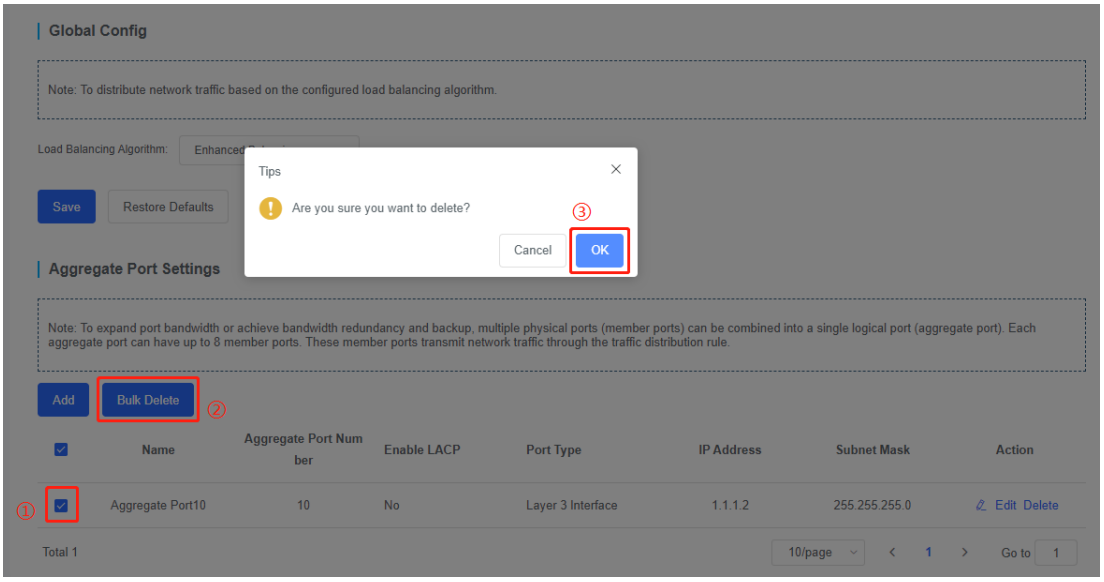


Figure4-45 Adding an aggregated port-2



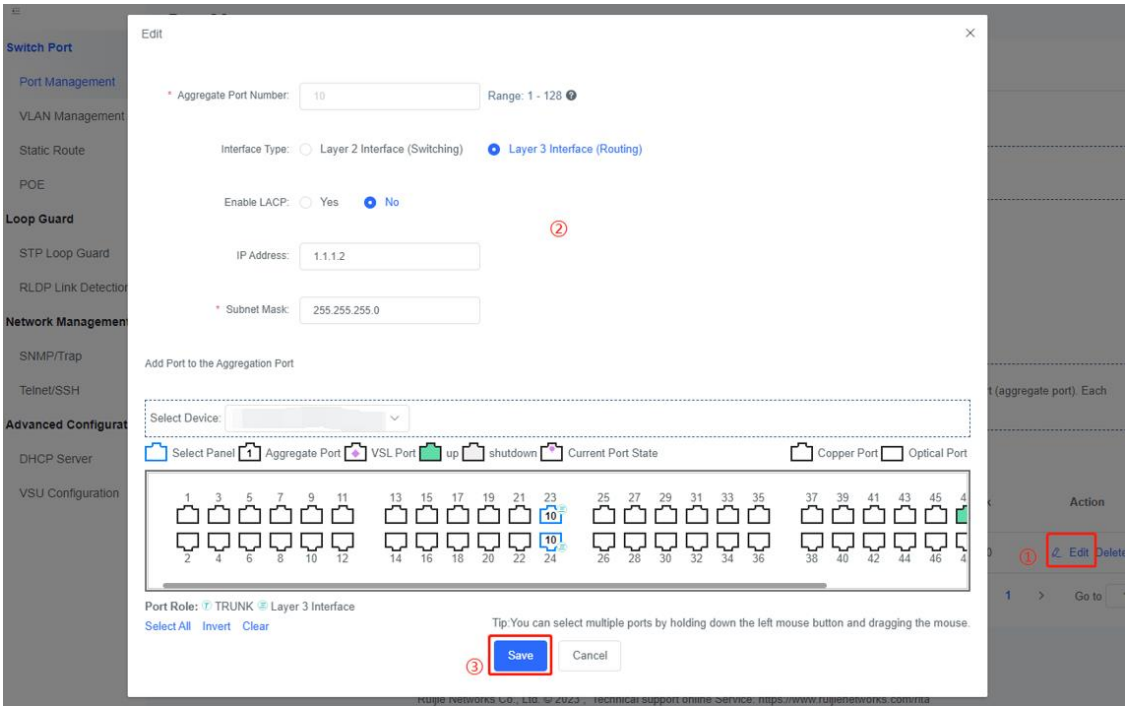
- Deleting multiple aggregated ports
  a. Click **Bulk Delete**.
  b. Click **OK** in the displayed window. The selected aggregated ports can be removed from in the Aggregate Port list

Figure4-46 Deleting multiple aggregated ports



- Editing an aggregated port
  a. Click **Edit**. Set configuration parameters in the displayed window.
  b. Click **Save**. The result can be viewed in the Aggregate Port list.

Figure4-47 Editing an aggregated port

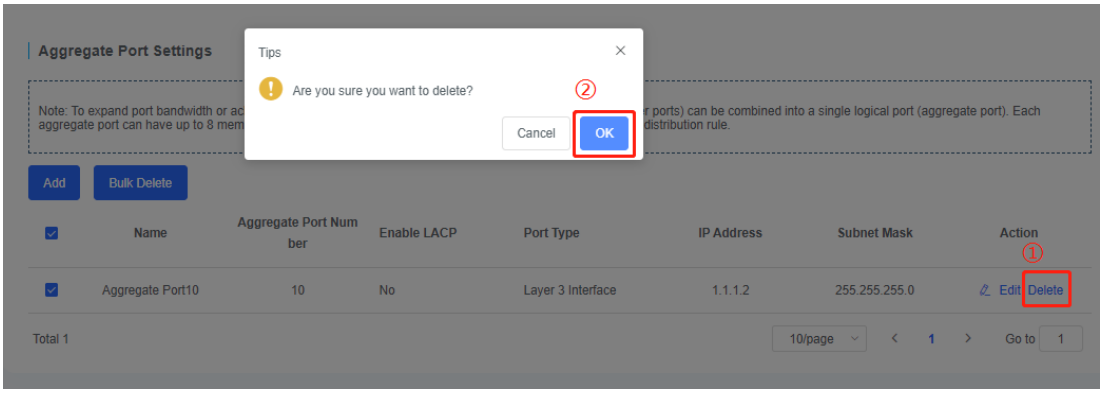


- Deleting an aggregated port

  a. Click **Delete**.

  b. Click **OK** in the displayed window. The selected port can be removed from in the Aggregate Port list

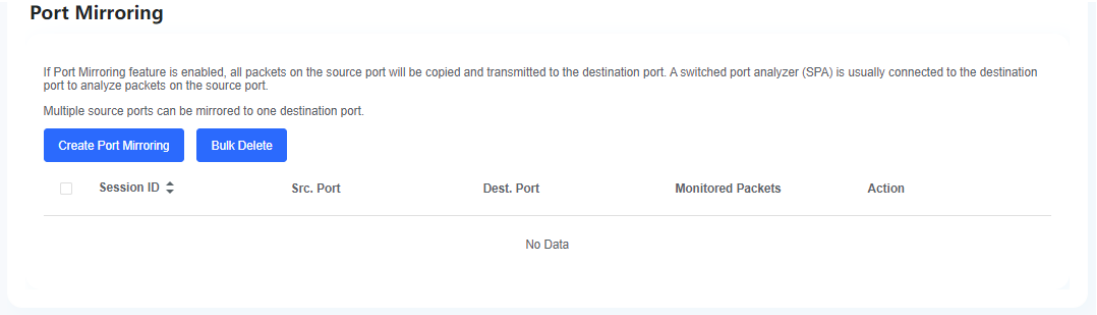
Figure4-48 Deleting an aggregated port



(4) Port Mirroring

After port mirroring is enabled on a source port, all packets on the source port are copied and forwarded to a destination port. A packet analyzer is usually connected to the destination port to analyze the packets on the source port.

Figure4-49 Port Mirroring



- Creating port mirroring

  a. Click **Create port mirroring**.

  b. Set configuration parameters in the displayed window.

  c. Click **OK**. The result can be viewed in the list.

Figure4-50 Creating port mirroring-1

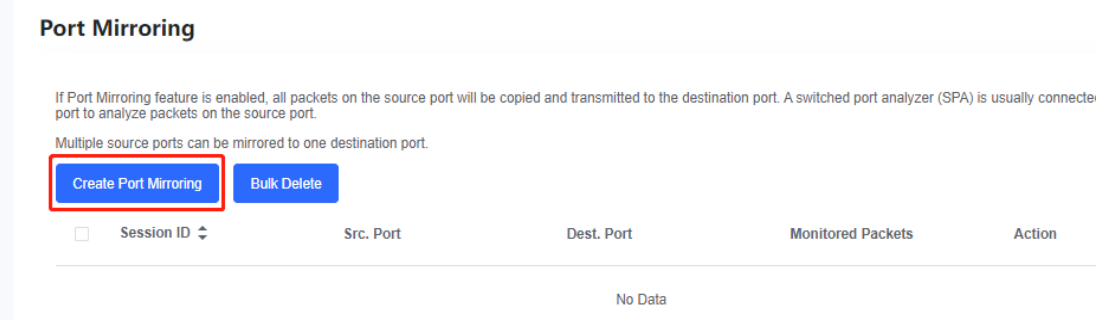
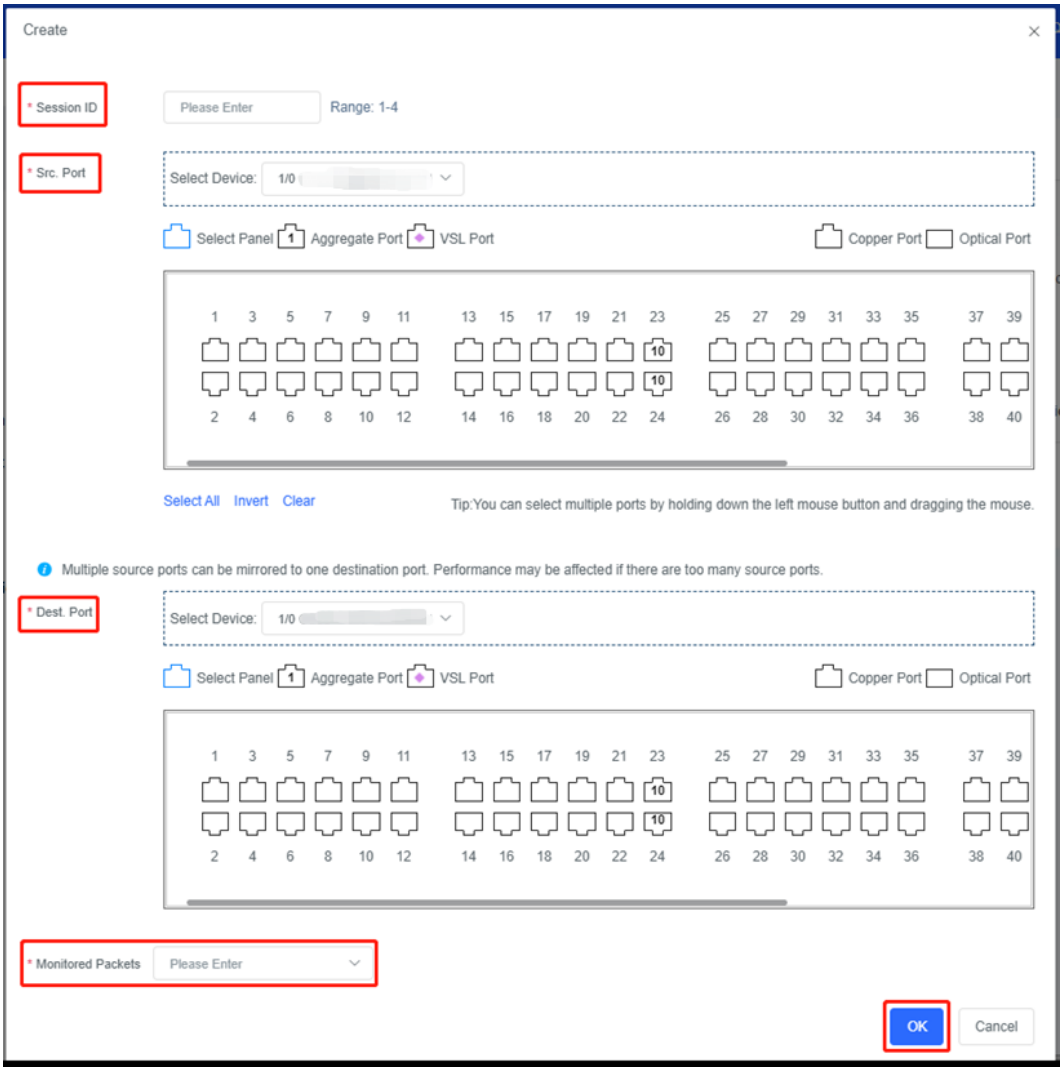


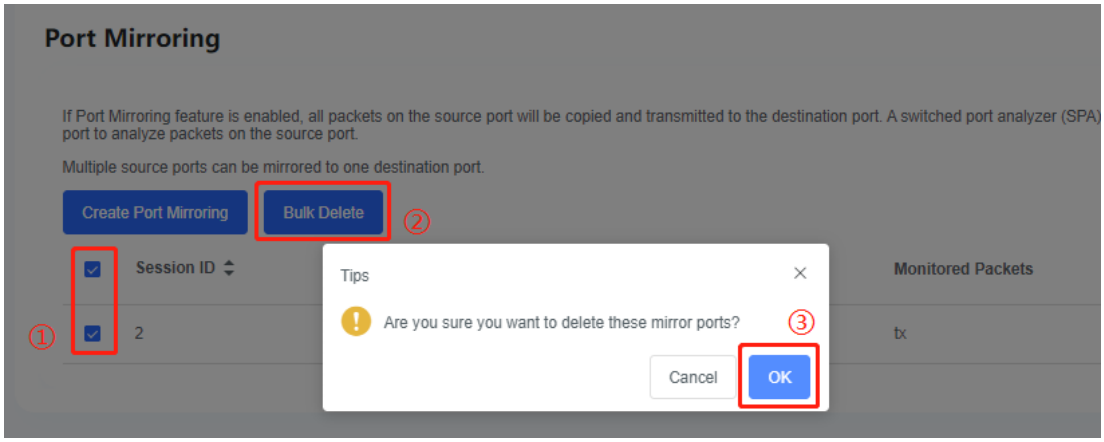
Figure4-51 Creating port mirroring-2



- Deleting multiple mirrored ports

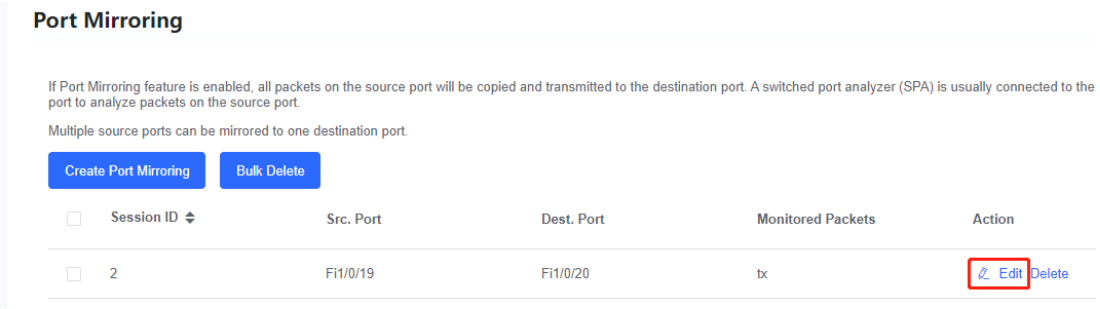
  Click **Bulk Delete**. Click **OK** in the displayed window. The mirrored ports can be deleted.

Figure4-52 Deleting multiple mirrored ports



- Editing a mirrored port

Figure4-53 Editing a mirrored port (1)

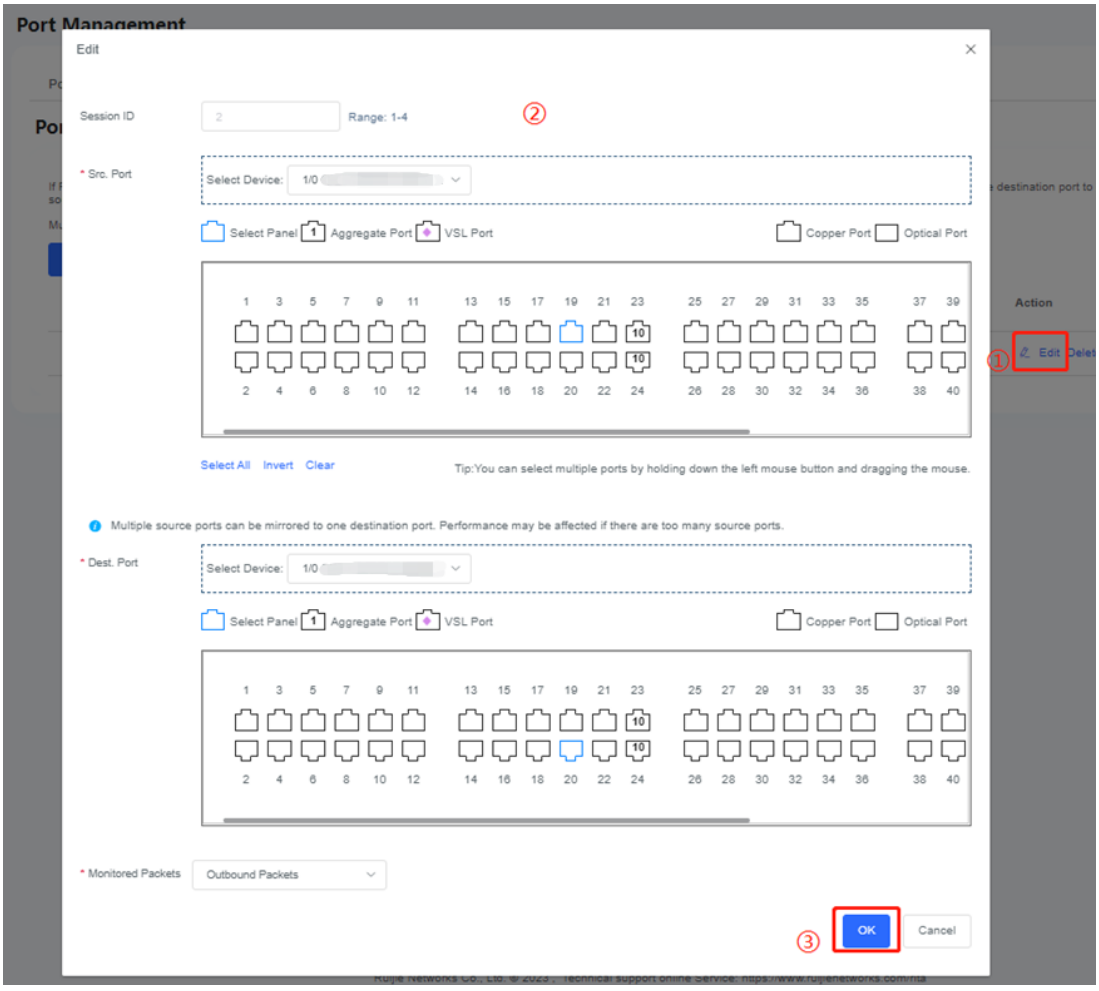


a. Click **Edit**.

b. Set configuration parameters in the displayed window.

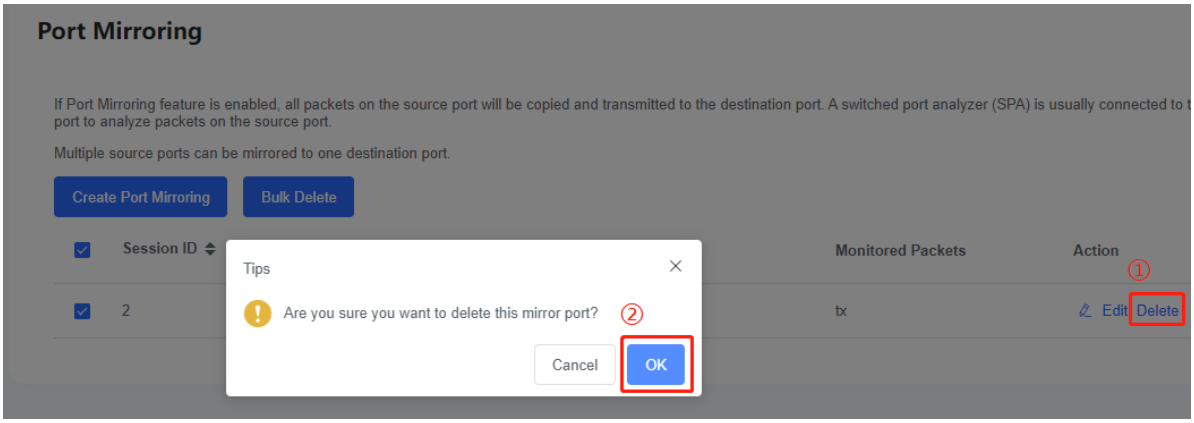
c. Click **OK**. The result can be viewed in the list.

Figure4-54 Editing a mirrored port (2)



- Deleting a mirrored port

Figure4-55 Deleting a mirrored port



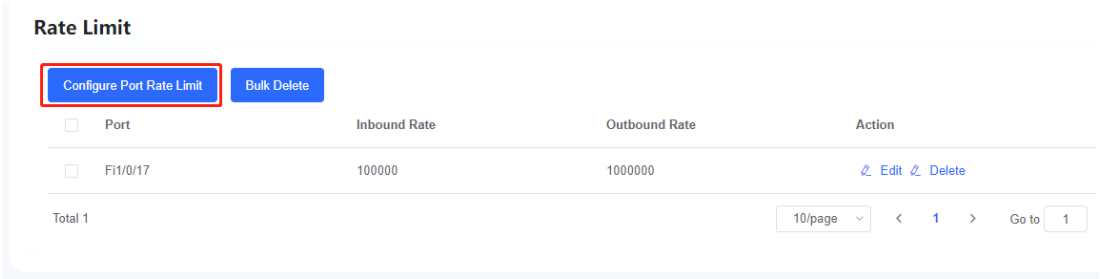
a. Click **Delete**.

b. Click **OK** in the displayed window. The mirrored ports can be deleted.

(5) Rate Limit

- Configuring port rate limiting

Figure4-56 Configuring port rate limiting (1)

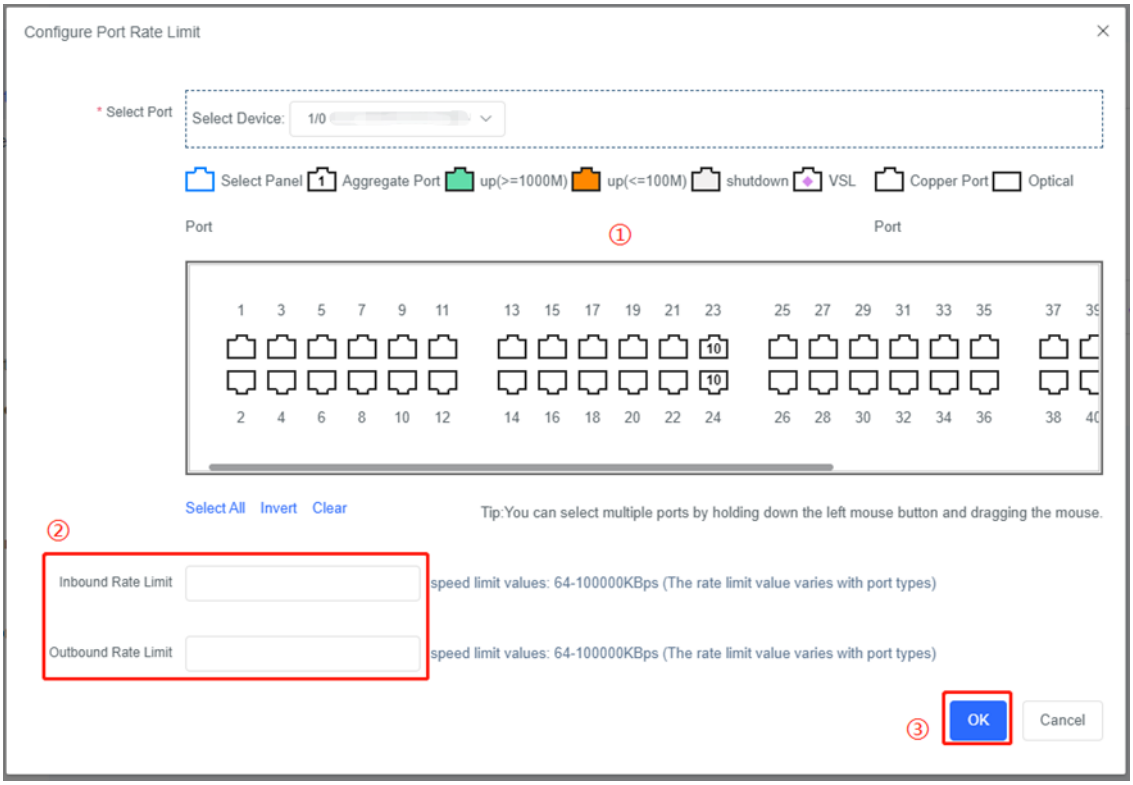


a. Click **Configure Port Rate Limit**.

b. Set configuration parameters in the displayed window.

c. Click **OK**. The result can be viewed in the list.

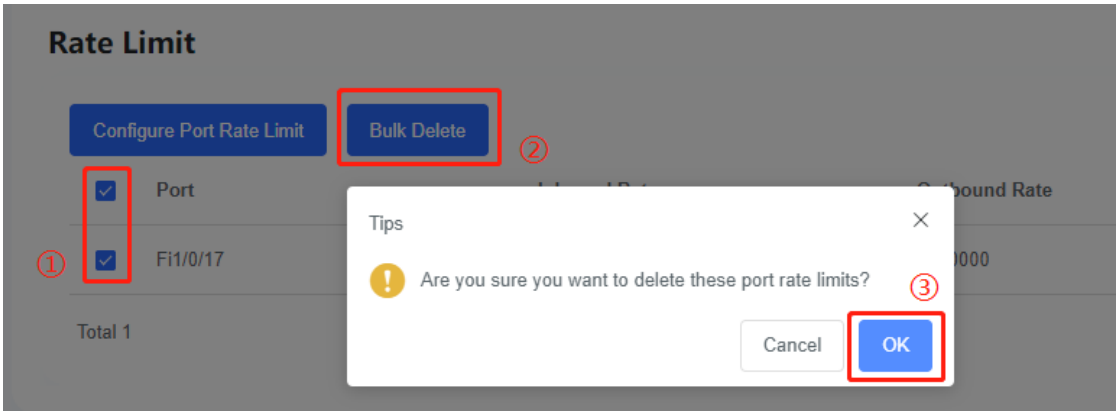
Figure4-57 Configuring port rate limiting (2)



- Deleting multiple rate limiting entries

  Click **Bulk Delete**. Click **OK** in the displayed window. The rate limiting entries can be deleted.

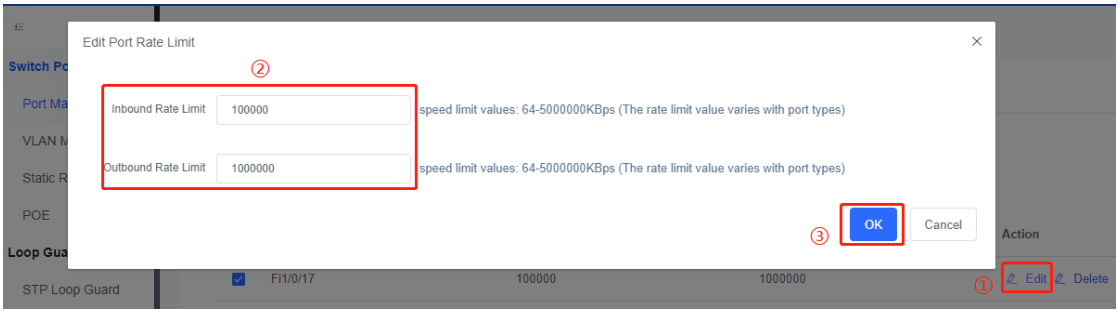
Figure4-58 Deleting multiple rate limiting entries



- Editing a port rate limiting entry

  Click **Edit**. Set configuration parameters in the displayed window. Click **OK**. The result can be viewed in the list.

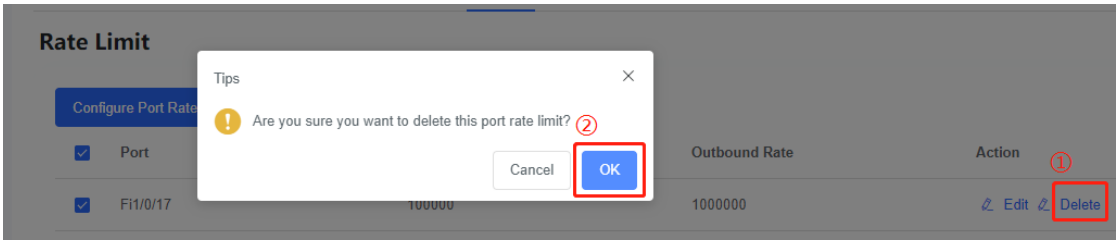
Figure4-59 Editing a port rate limiting entry



- Deleting a port rate limiting entry

  Click **Delete**. Click **OK** in the displayed window. The rate limiting entry can be deleted.

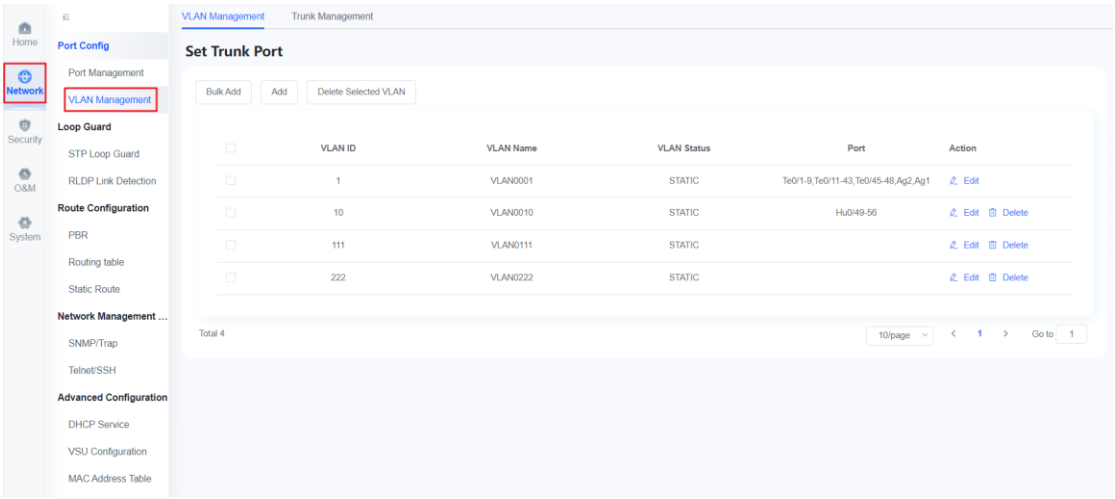
Figure4-60 Deleting a port rate limiting entry



2. VLAN Management

Choose **Network** > **Switch Port** > VLAN Management to access the VLAN Management page.

Figure4-61 VLAN Management

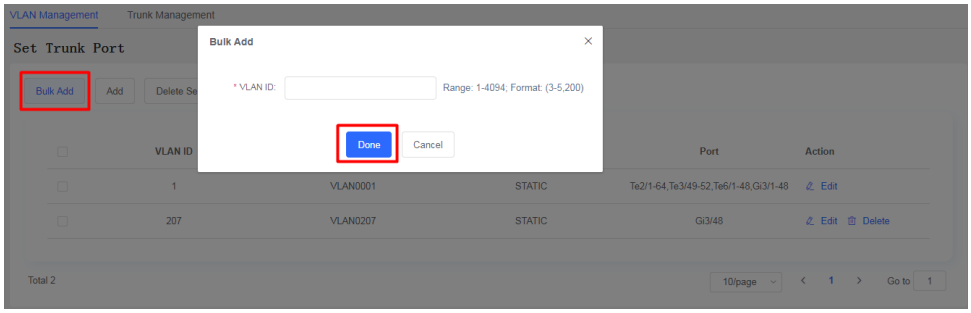


(2) VLAN Management

- VLAN Adding multiple VLANs

  To add multiple VLANs, click **Bulk Add** and the **Bulk Add** window is displayed. Enter the VLAN ID and click **Done**.

Figure4-62 VLAN Adding multiple VLANs



- Adding a single VLAN

  To add a single VLAN, click **Add** and the **Add** window is displayed. Set configuration parameters and click **Done**.

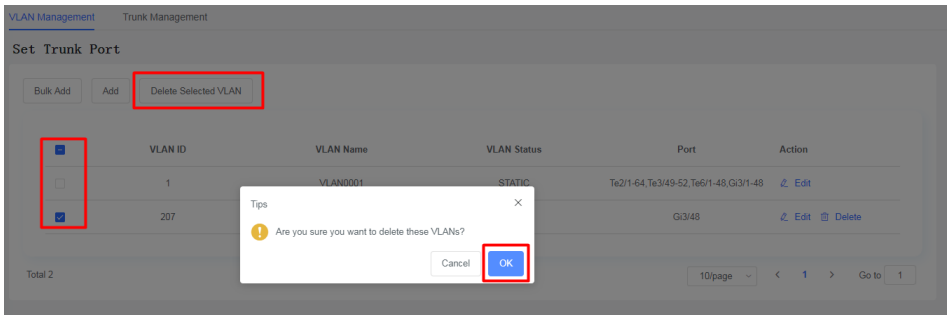
Figure4-63 Adding a single VLAN



- Deleting multiple VLANs

  To delete the selected VLANs, click black box before each VLAN to select multiple VLANs, then click **Delete Selected VLAN**. The error message is displayed. Click **OK**.

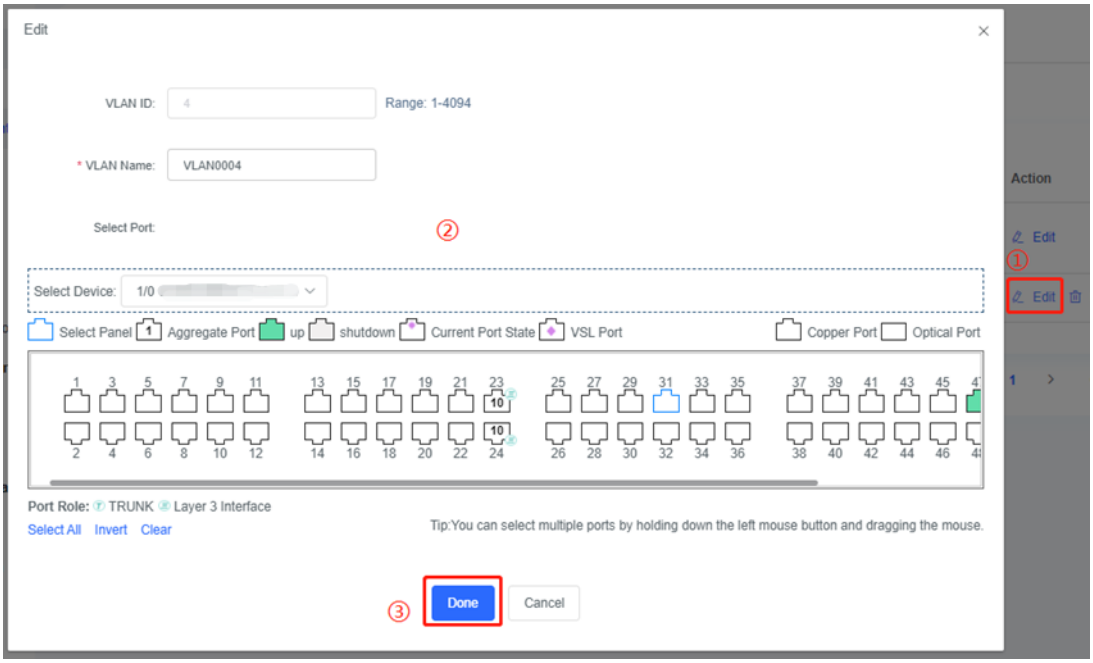
Figure4-64 Deleting multiple VLANs



- Editing a VLAN

  To edit a VLAN, click **Edit**, and the Edit window is displayed. Set configuration parameters and click **Done**.

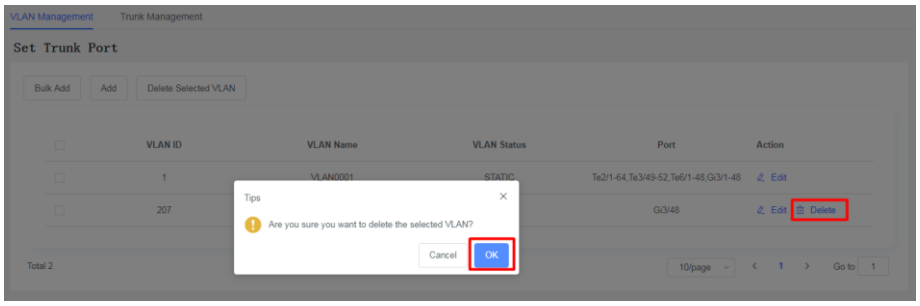
Figure4-65 Editing a VLAN



- Deleting a VLAN

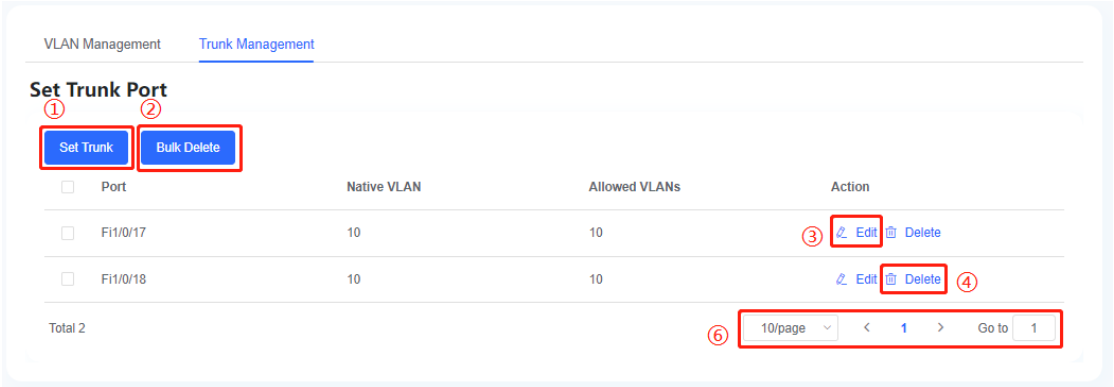
  To delete a VLAN, click **Delete**. The **Error** dialog box is displayed. Click **OK**.

Figure4-66 Deleting a VLAN



- Trunk Management

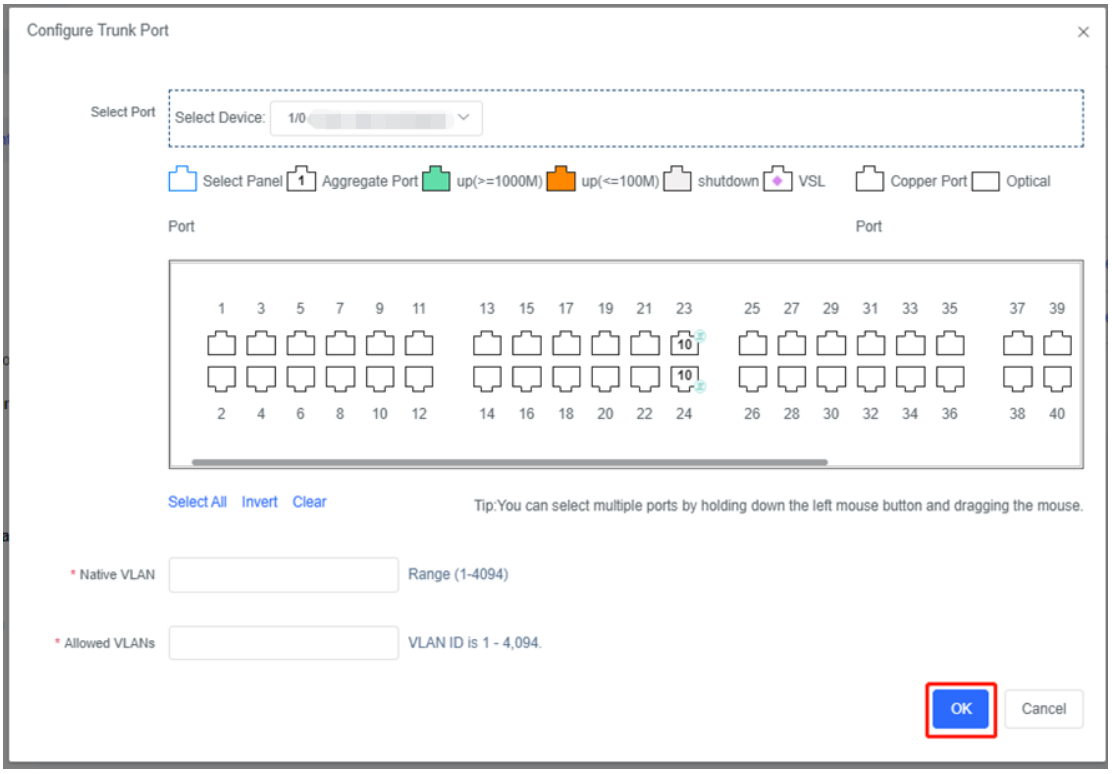
Figure4-67 Trunk Management



- Setting a Trunk port

  To set a trunk port, click **Set Trunk**. The **Configure Trunk Port** window is displayed. Set configuration parameters and click **OK**.

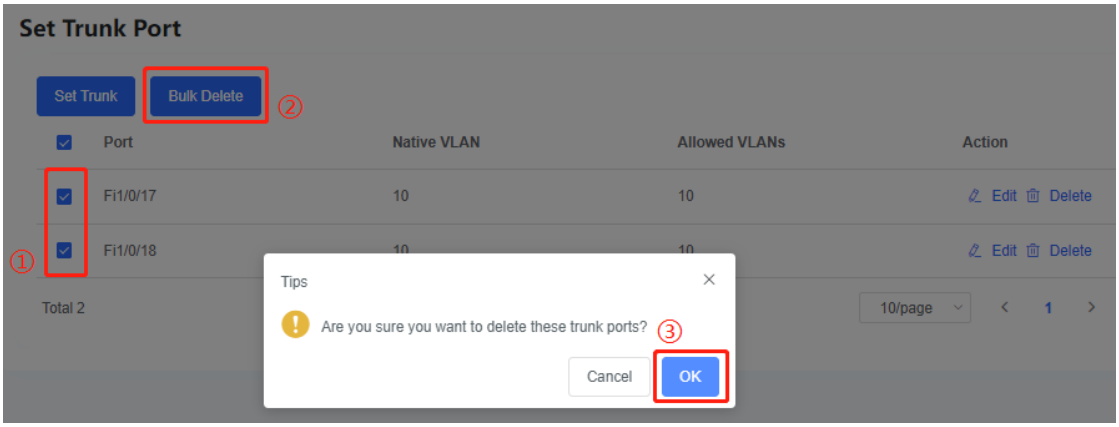
Figure4-68 Setting a Trunk port



- Deleting multiple trunk ports

  To delete multiple trunk ports, click black box next to each trunk port to select multiple trunk ports, and then click **Bulk Delete**. The **Error** dialog box is displayed. Click **OK**.

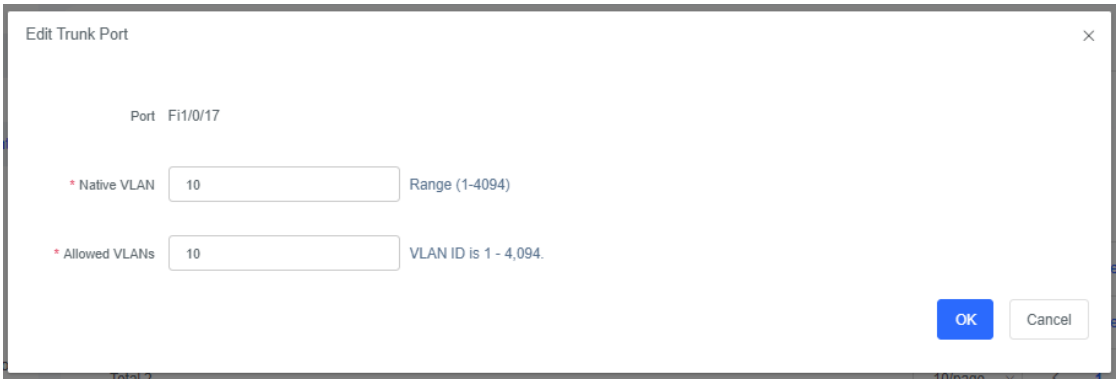
Figure4-69 Deleting multiple trunk ports



- Editing a trunk port

To edit a Trunk port, click **Edit**. The Edit Trunk Port window is displayed. Set configuration parameters and Click **OK**.

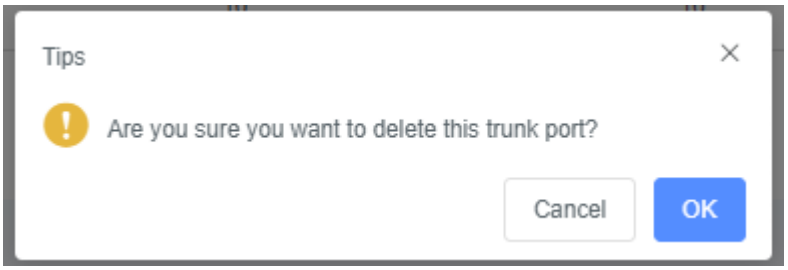
Figure4-70 Editing a trunk port



- Deleting a trunk port

  To delete a selected trunk port, Click **Delete**. The **Error** dialog box is displayed. Click **OK**.

Figure4-71 Deleting a trunk port



(3) PoE (non-remote power supply)

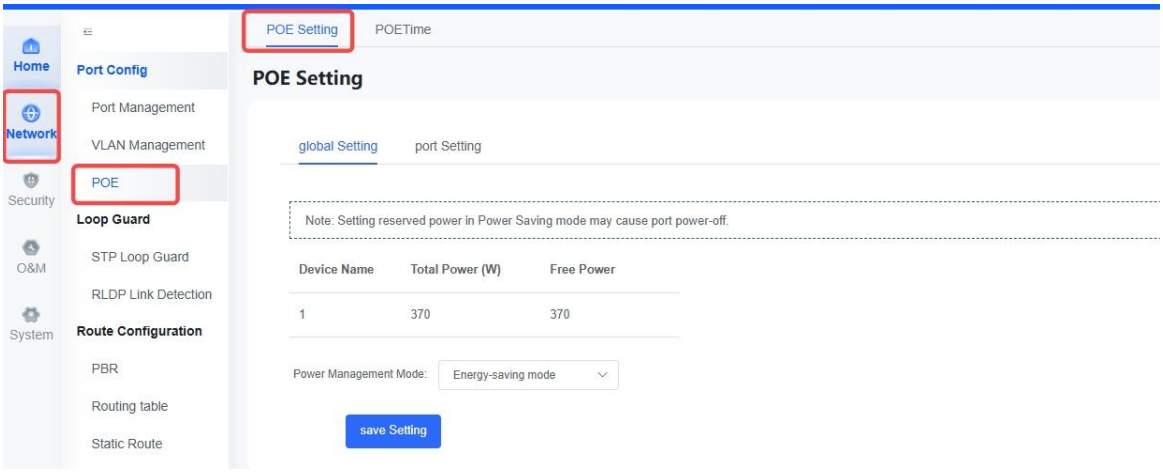
Specification

PoE is supported by only the RG-S5760C-48GT4XS-HP-X,RG-S5310-24GT4XS-P-E,and RG-S5310-48GT4XS-P-E.

(4) PoE Setting

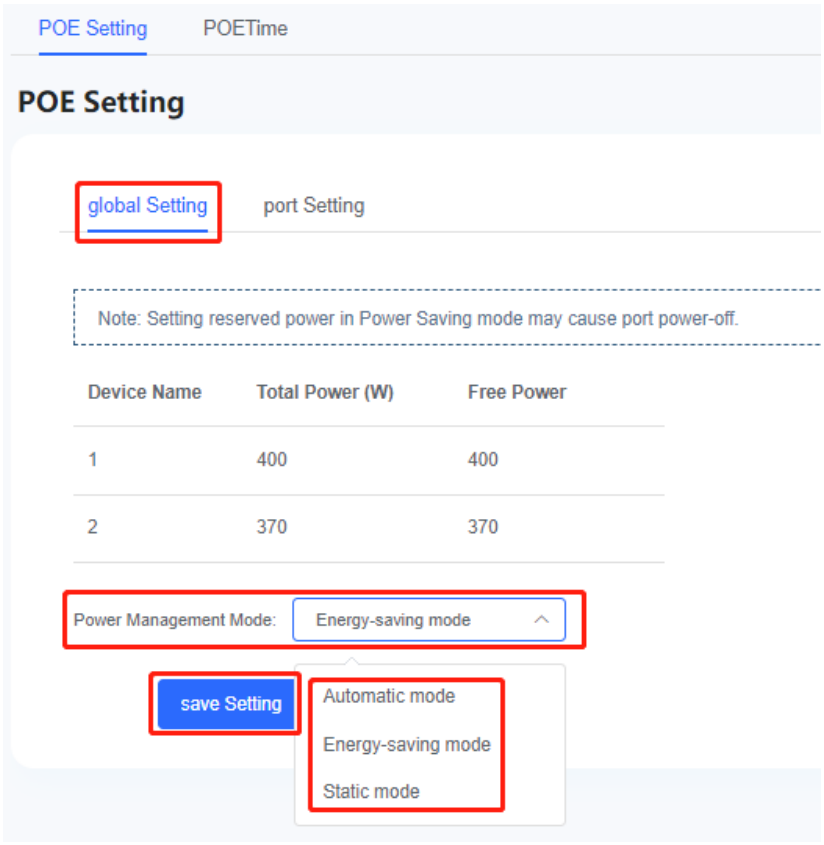
Choose **Network** > **Switch Port** > **POE** to access the **PoE Setting** page.

Figure4-72 POE Setting



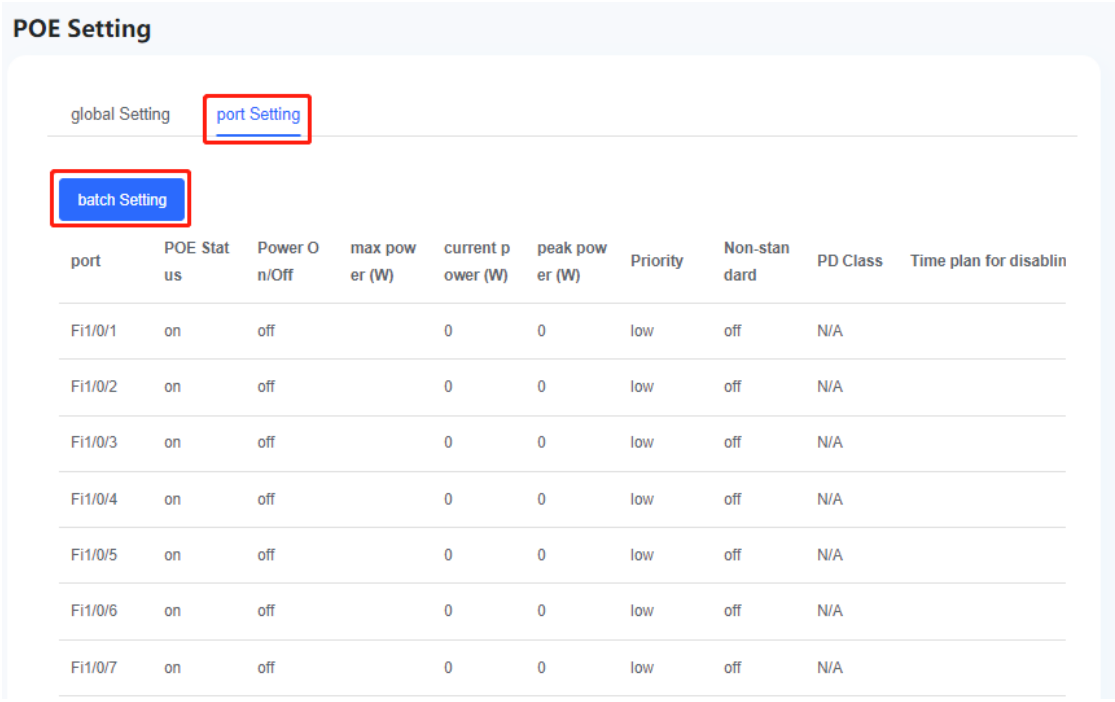
- Global Setting

Figure4-73 Global Setting



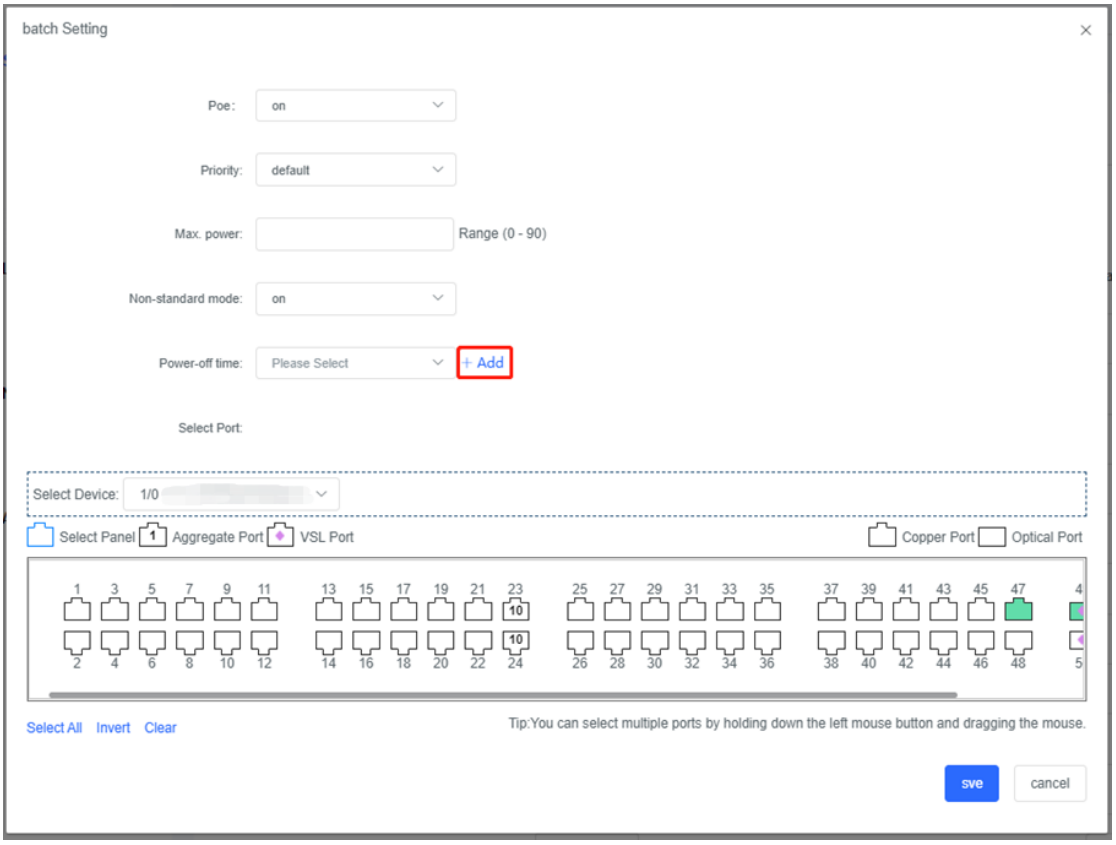
- Port Setting

Figure4-74 Port Setting



Click **batch Setting**, set configuration parameters on the **Batch Setting** page. Click **save**.

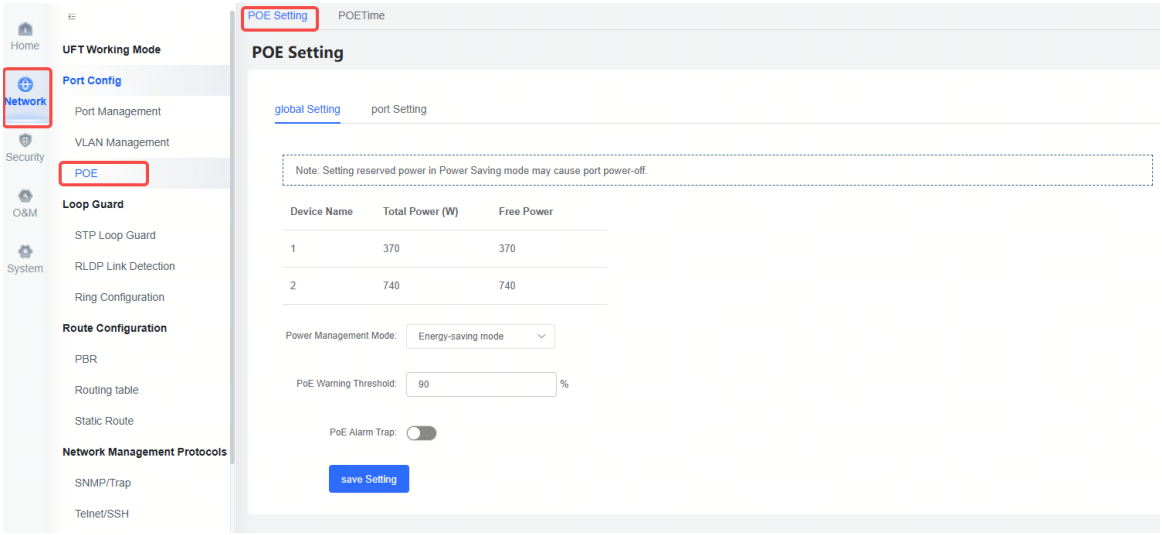
Figure4-75 Batch Setting



3. PoE

Choose **Network** > **Port Config** > **POE** to go to the **PoE Setting** page, as shown in the following figure.

Figure4-76 PoE Settings



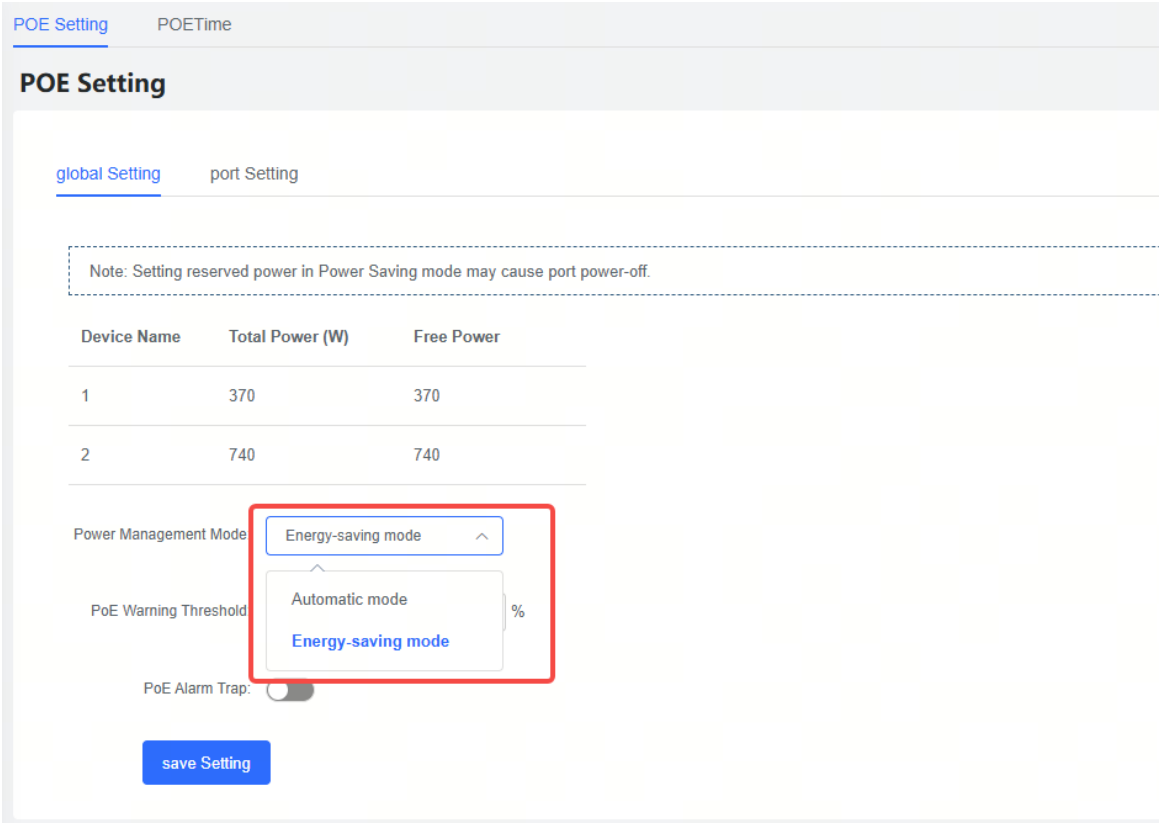
- **PoE Setting**

  PoE Setting includes **global setting** and **port setting**.

  - **global setting**

    Click the **global setting** tab to view device power information and modify the power supply management mode.

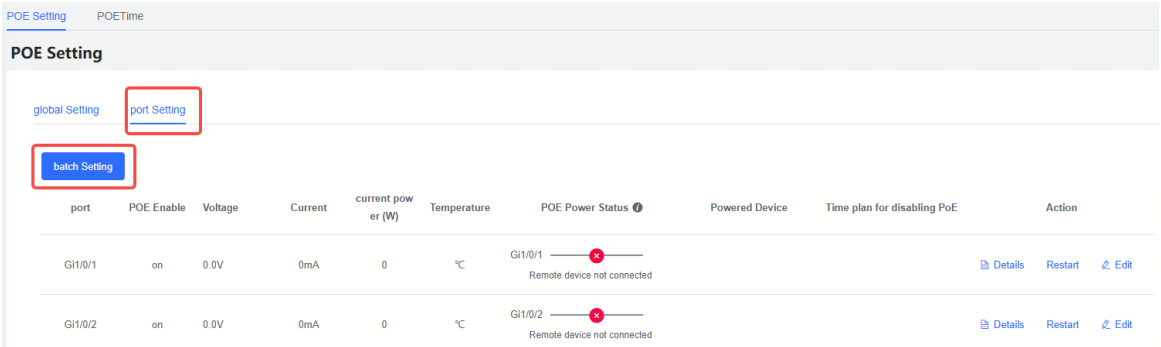
Figure4-77 global setting

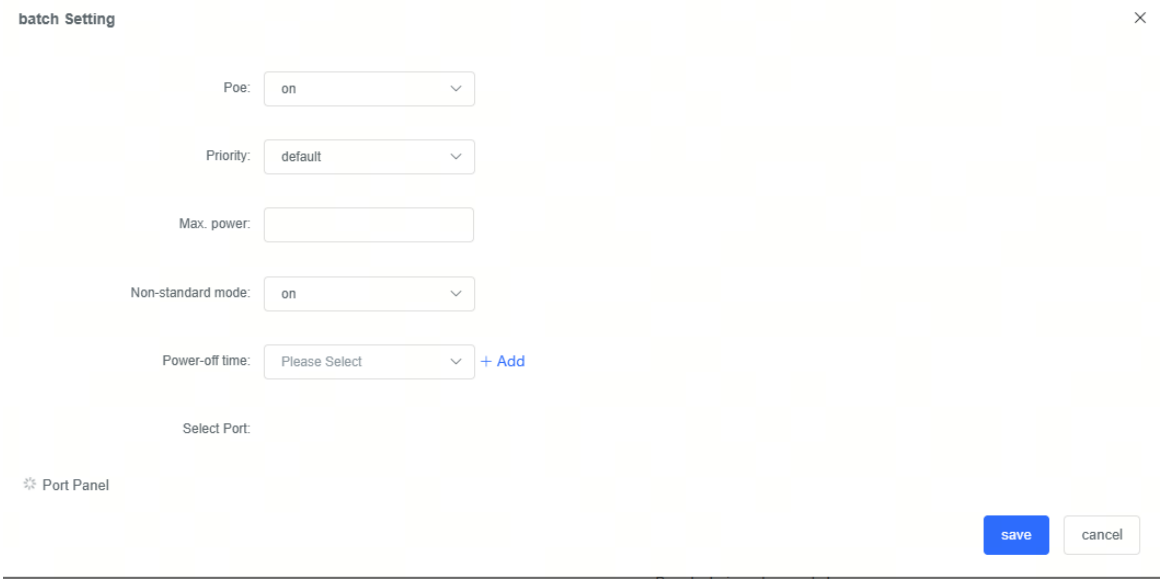


- **port setting**

  Click the **port setting** tab. On this tab page, you can click **Batch Setting** set ports in batches. In the displayed dialog box, set parameters and click **Save** to deliver the configuration.

Figure4-78 port setting

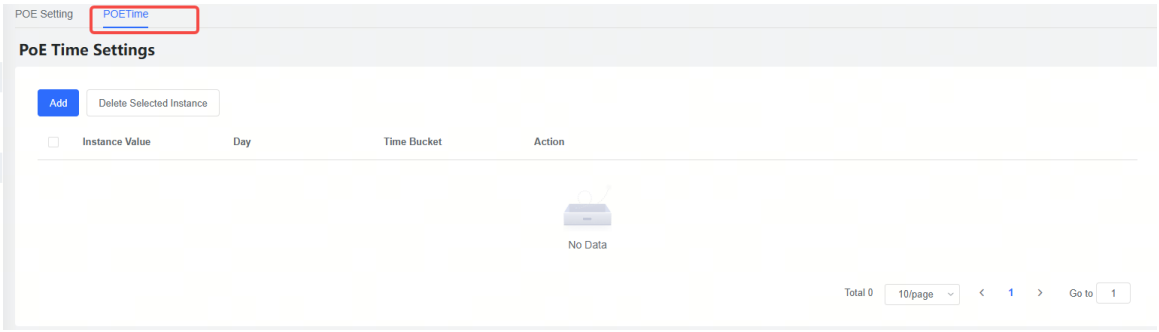




- PoE Time

  The PoE power-off time must be periodic. You can complete the PoE time settings on this tab page.

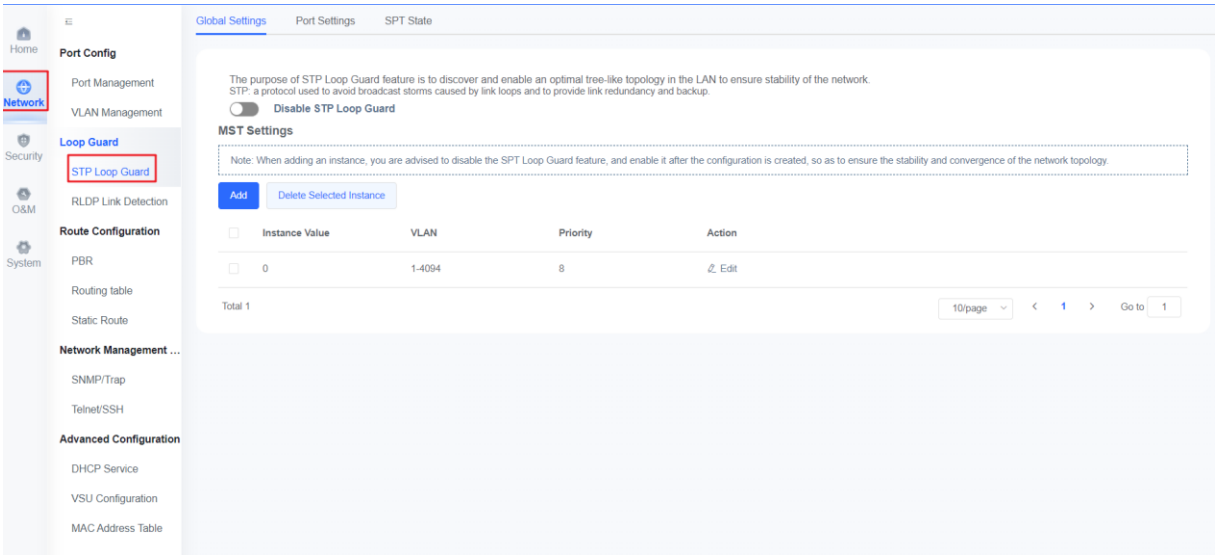
Figure4-79 PoE Time



4.4.2 Loop Guard

1. STP Loop Guard

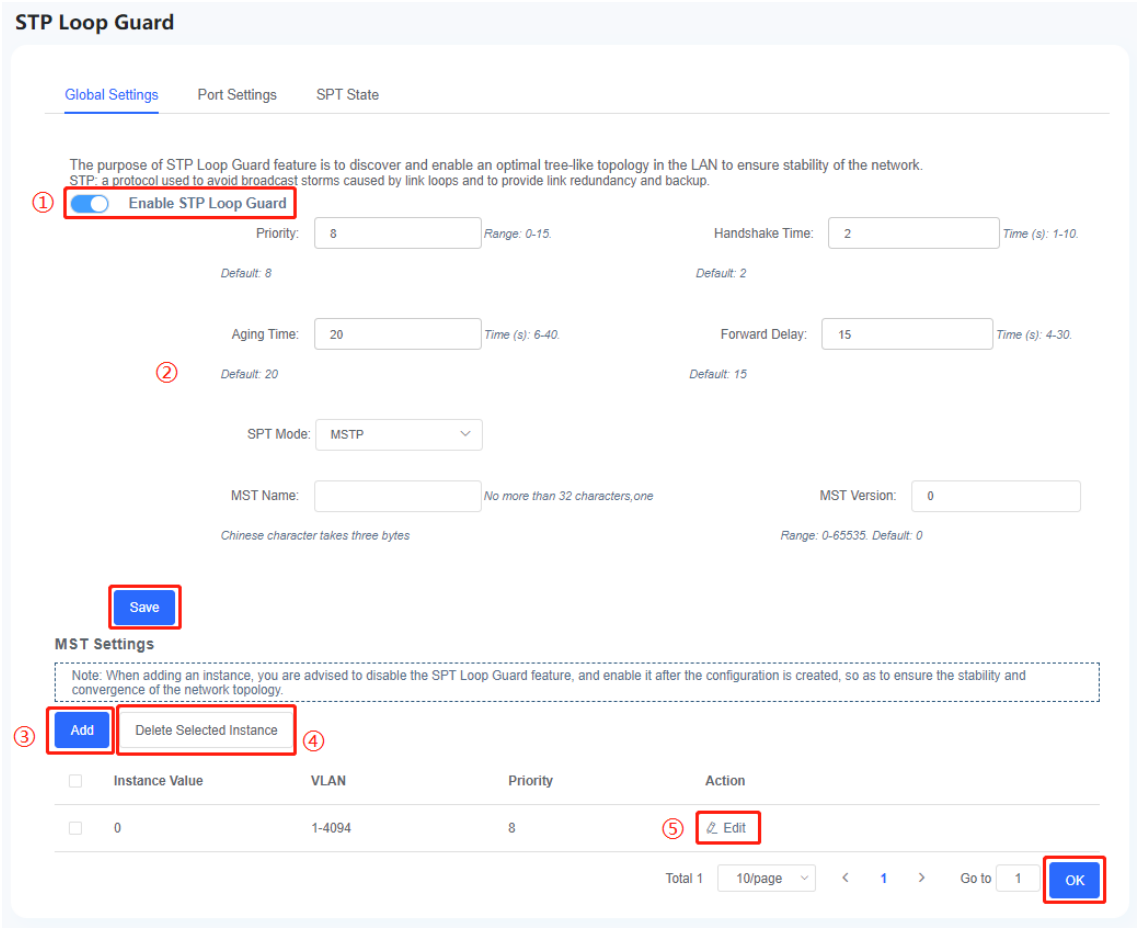
Figure4-80 STP Loop Guard



Enable or disables STP Loop Guard: Click **Enable STP Loop Guard** to enable or disable STP loop guard.

(2) Global Settings

Figure4-81 STP Loop Guard - Global Settings



a. Global Settings: Enable **STP Loop Guard** and set configuration parameters. There are three STP modes, which are STP, RSTP, and MSTP. Click **Save** to submit the global settings.

b. Add instances: Click **Add** to add instances.

c. Delete instances: Click **Delete Selected instance** to delete instances.

d. Edit instances: Click **Edit** to edit instances.

(3) Port Settings

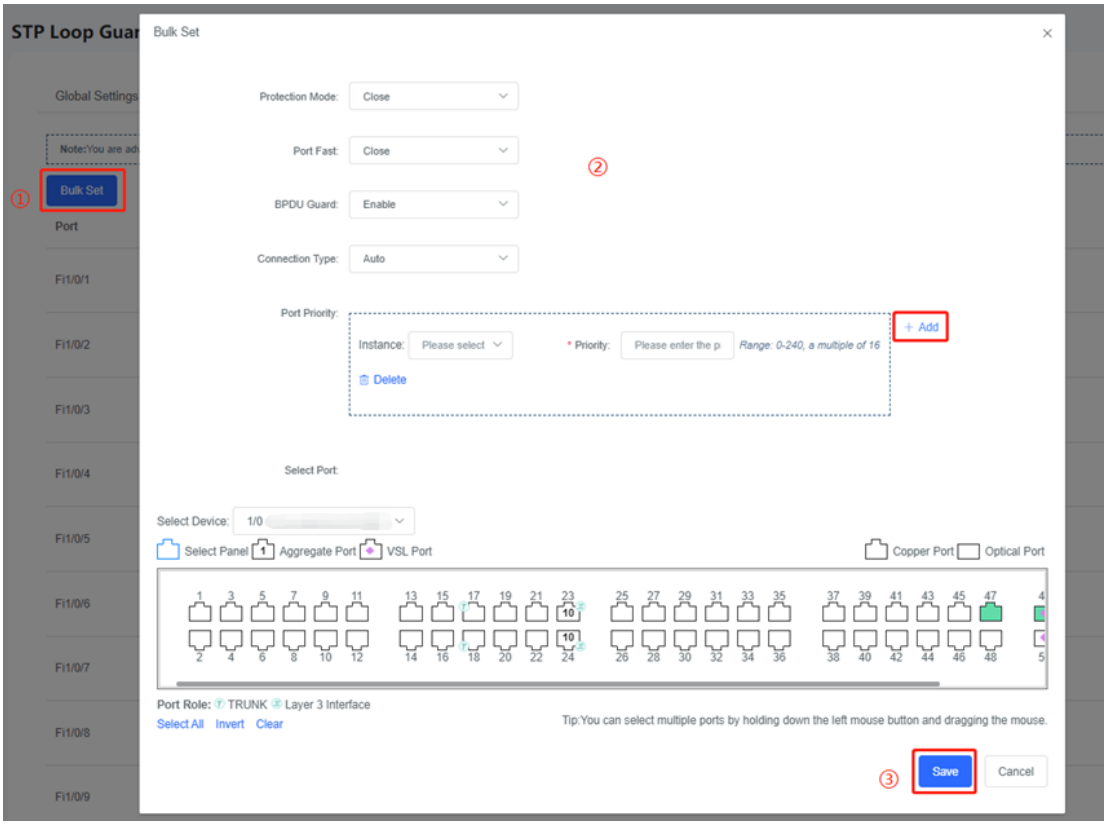
Note

You are advised to enable **Port Fast** on the port directly connected to a PC.

- Setting the STP loop guard function for multiple ports

  Click **Bulk Set**. The **Bulk Set** window is displayed. Set configuration parameters. Add or delete the port priority by clicking **Add** or **Delete**. Select multiple ports, and click **Save** to submit the configuration. Then the result will be displayed in the list.

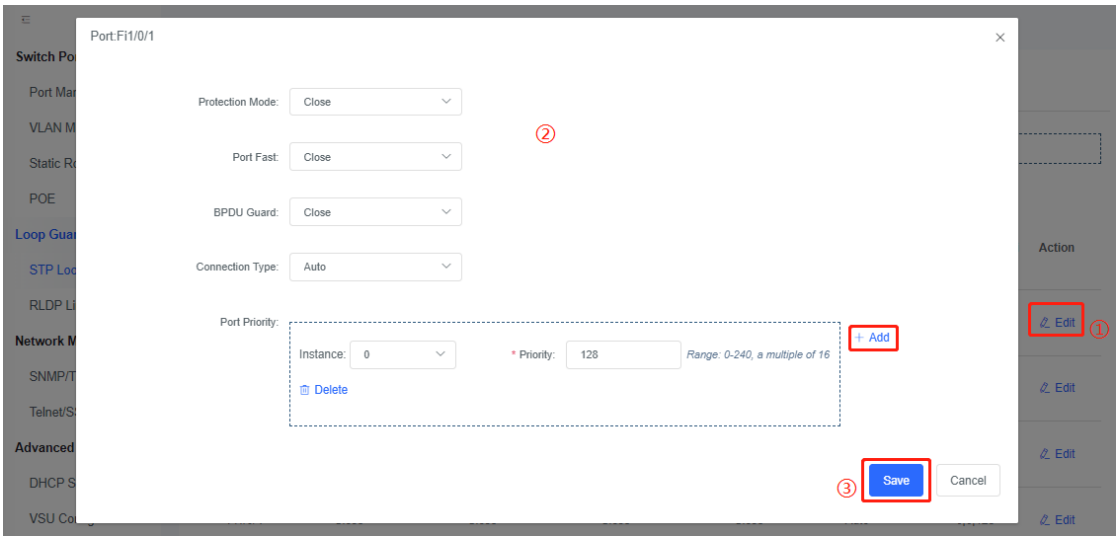
Figure4-82 STP Loop Guard - Port Settings



- Editing the STP loop guard function for a single port

  Click **Edit** in the **Action** column. A window is displayed. Set configuration parameters. Add or delete the port priority by clicking **Add** or **Delete**. Click **Save** to submit the configuration. Then the result will be displayed in the list.

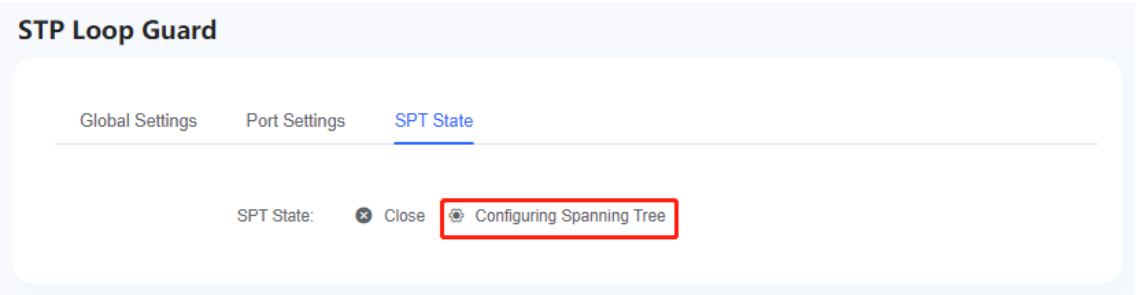
Figure4-83 Editing the STP loop guard function for a single port



(4) STP State

Click **Configuring Spanning Tree** to enable the STP loop guard function.

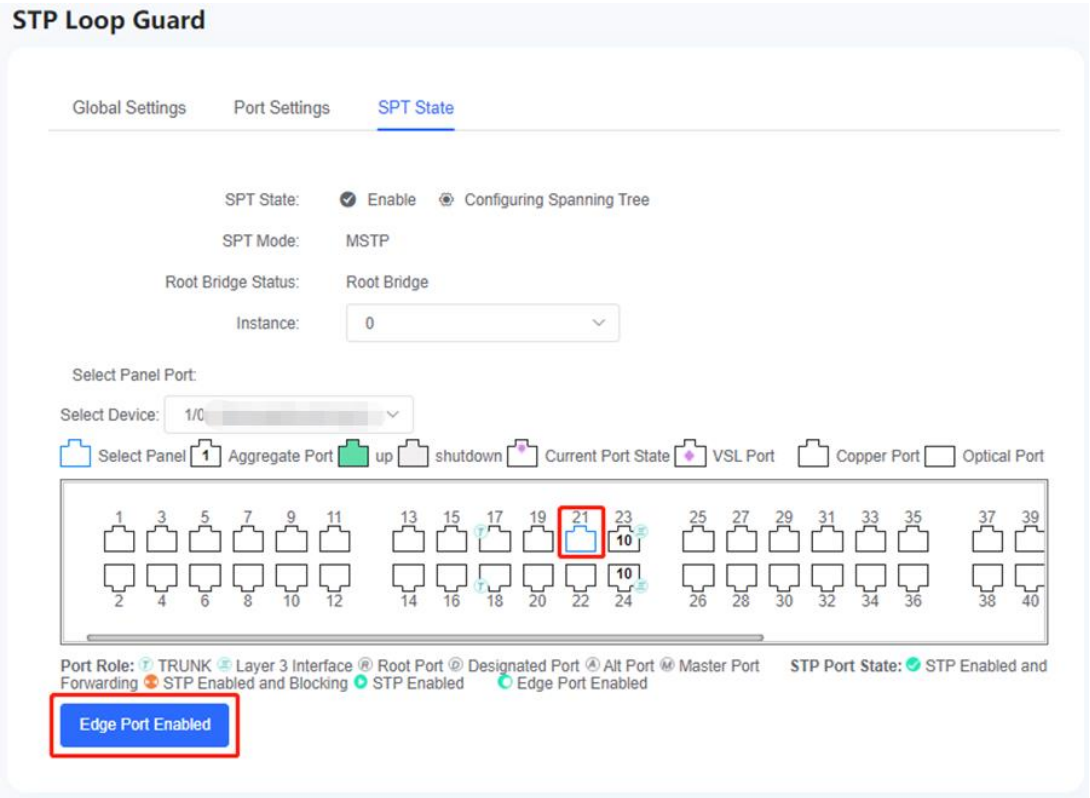
Figure4-84 STP Loop Guard - STP State



- Disable Edge Port

  Select a disabled edge port and click **Edge Port Enabled**. The icon of Port 21 is changed to enabled state.

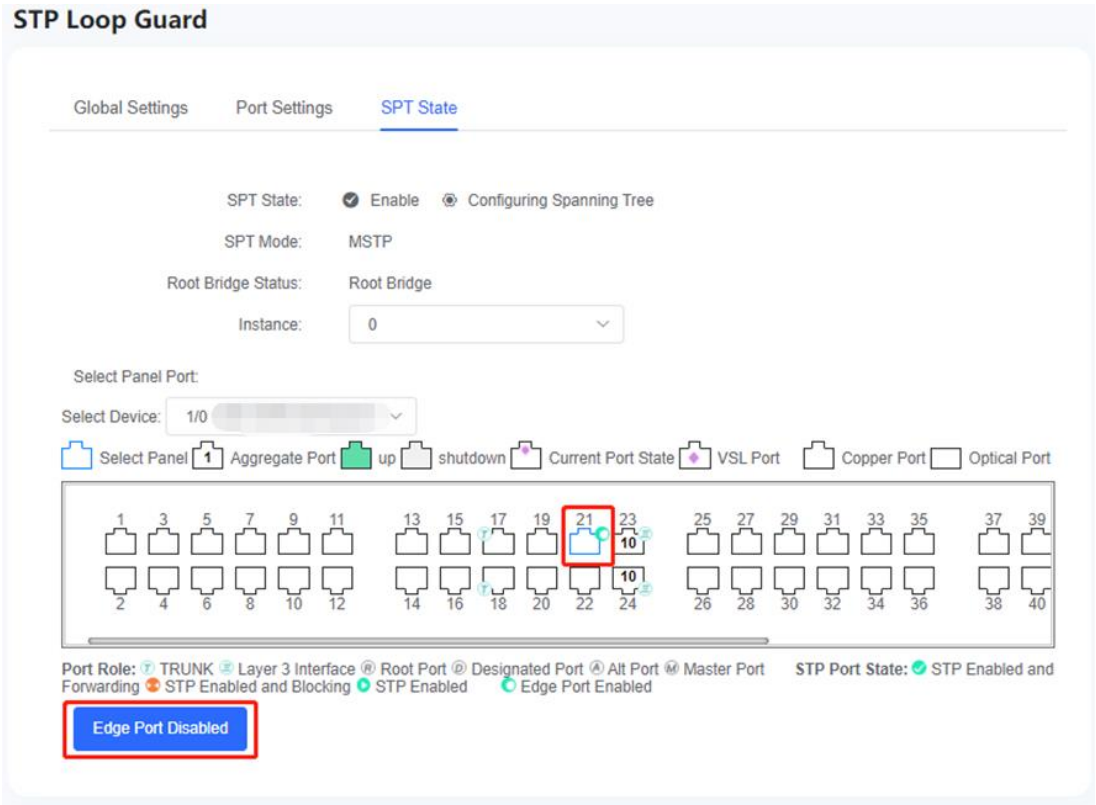
Figure4-85 Disable Edge Port



- Enable Edge Port

  Select an enabled edge port and click **Edge Port Disabled**. The icon of Port 21 is changed to disabled state.

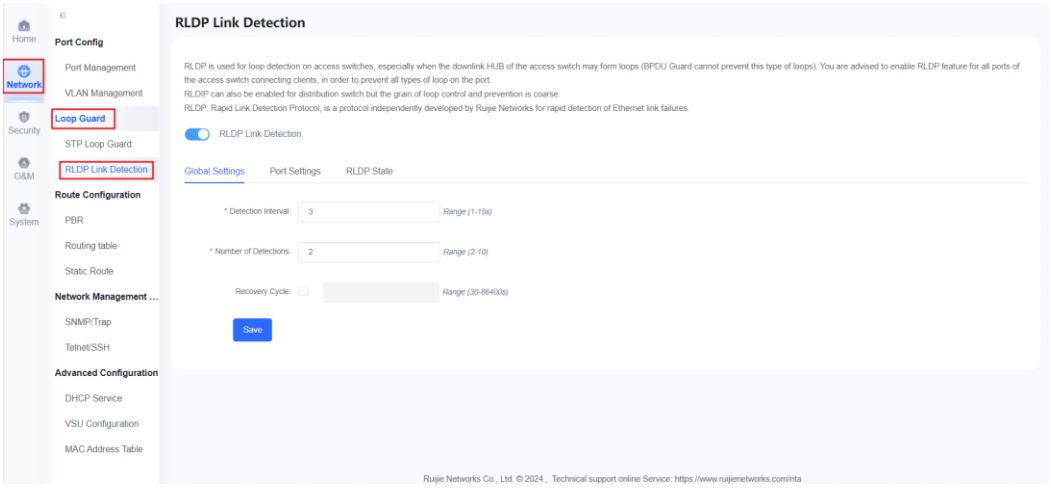
Figure4-86 Enable Edge Port



2. RLDP Link Detection

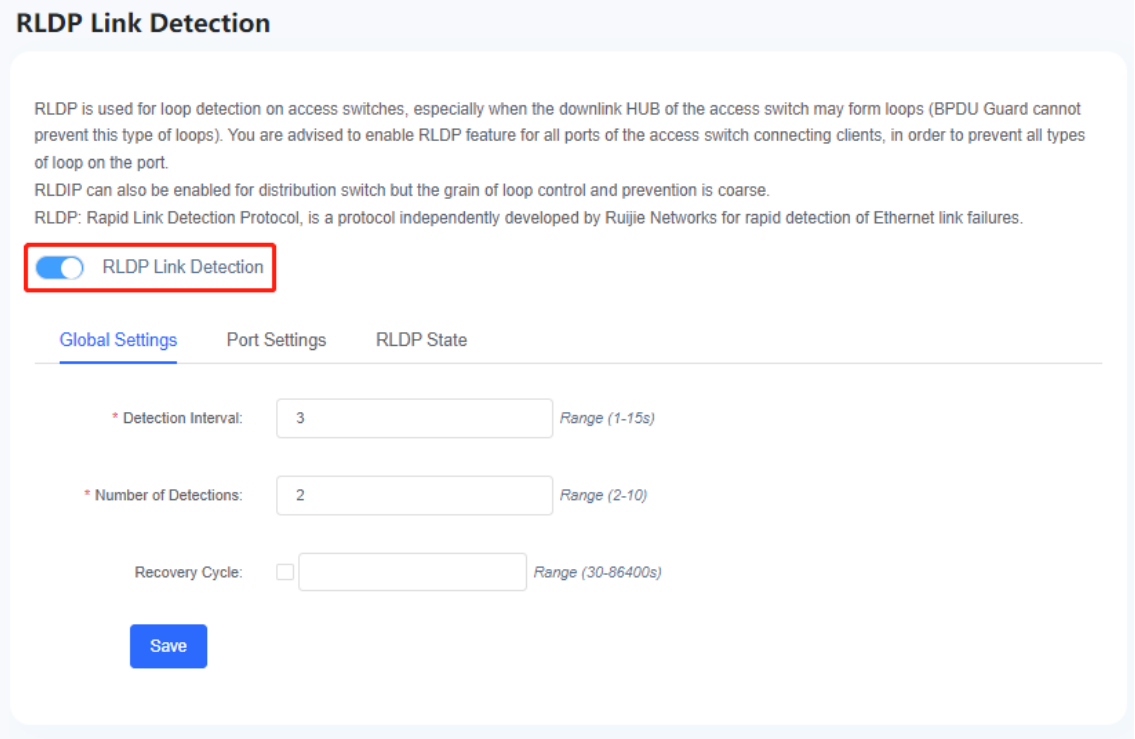
Choose **Network** > **Loop Guard** > **RLDP Link Detection** to access the **RLDP Link Detection** page.

Figure4-87 RLDP Link Detection



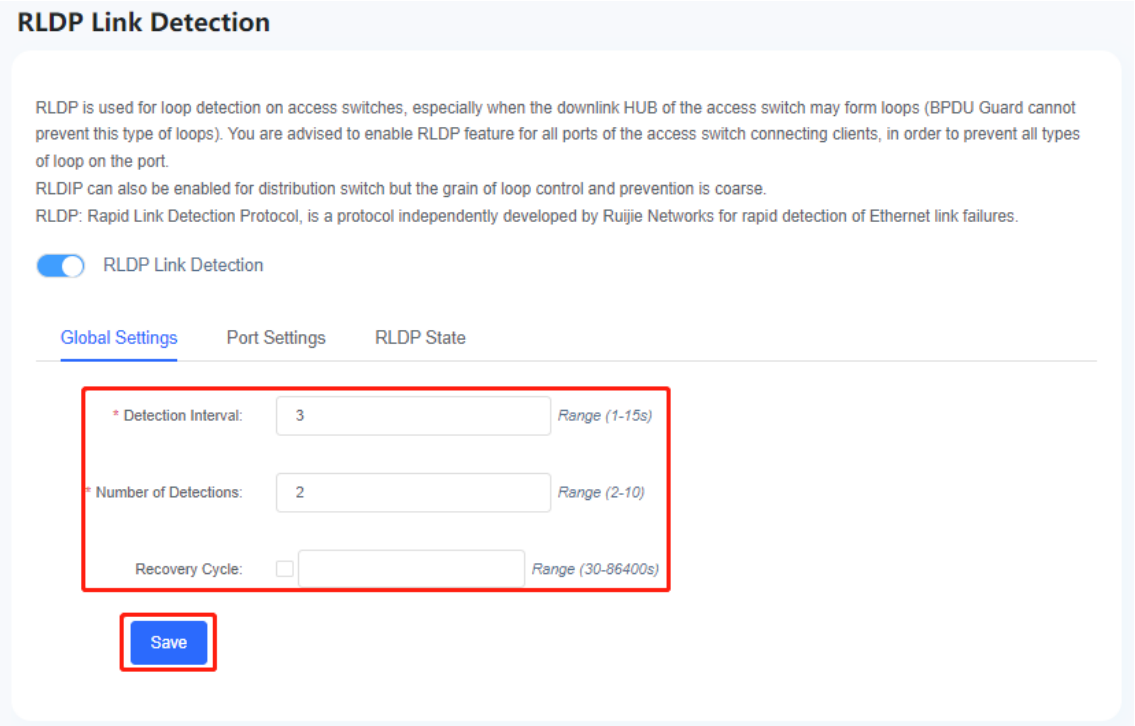
Click **RLDP Link Detection** to enable or disable RLDP.

Figure4-88 Enable/disable RLDP Link Detection



(2) Global Settings

Figure4-89 RLDP Link Detection - Global Settings



- **Save**: After you have entered the detection interval, number of detections, and restoration cycle (optional),

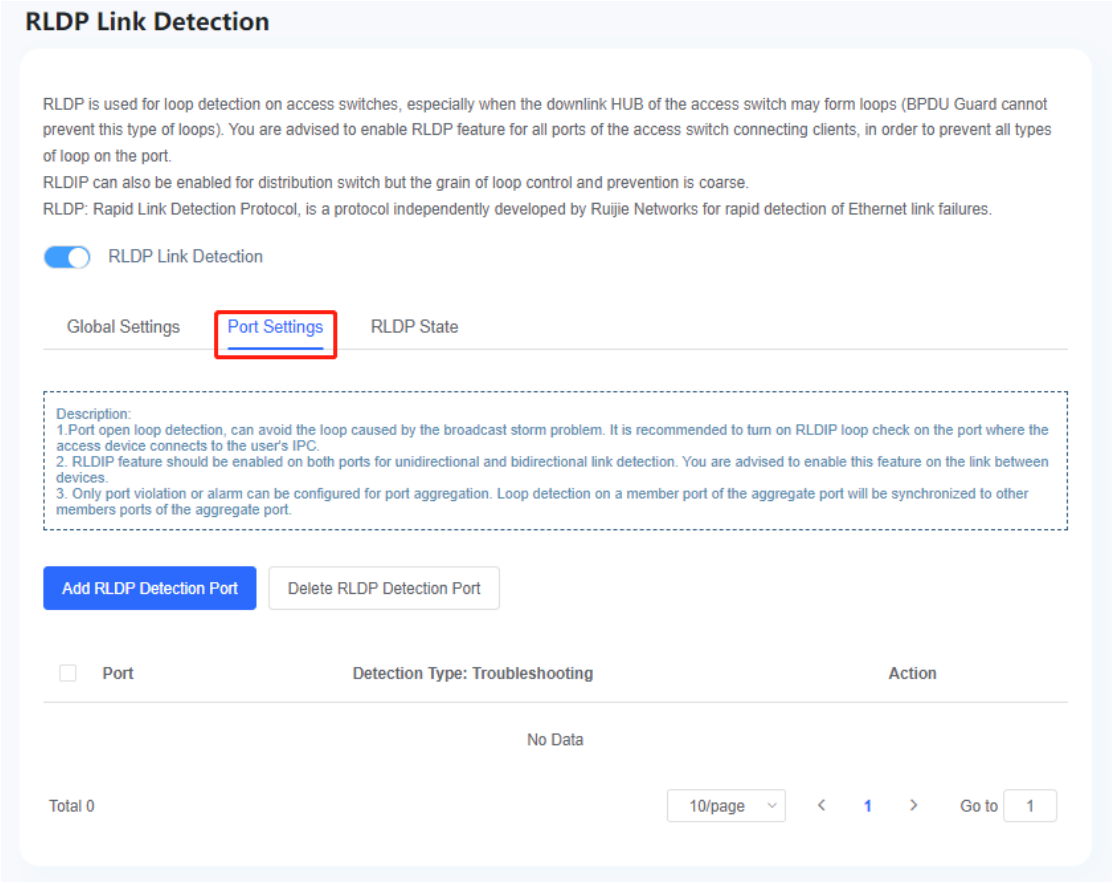
click **Save** to save the global settings.

(3) Port Settings

Note

- Port open loop detection, can avoid the loop caused by the broadcast storm problem. It is recommended to turn on RLDIP loop check on the port where the access device connects to the user's IPC.
- RLDP feature should be enabled on both ports for unidirectional and bidirectional link detection. You are advised to enable this feature on the link between devices.
- Only port violation or alarm can be configured for port aggregation. Loop detection on a member port of the aggregate port will be synchronized to other member ports of the aggregate port.

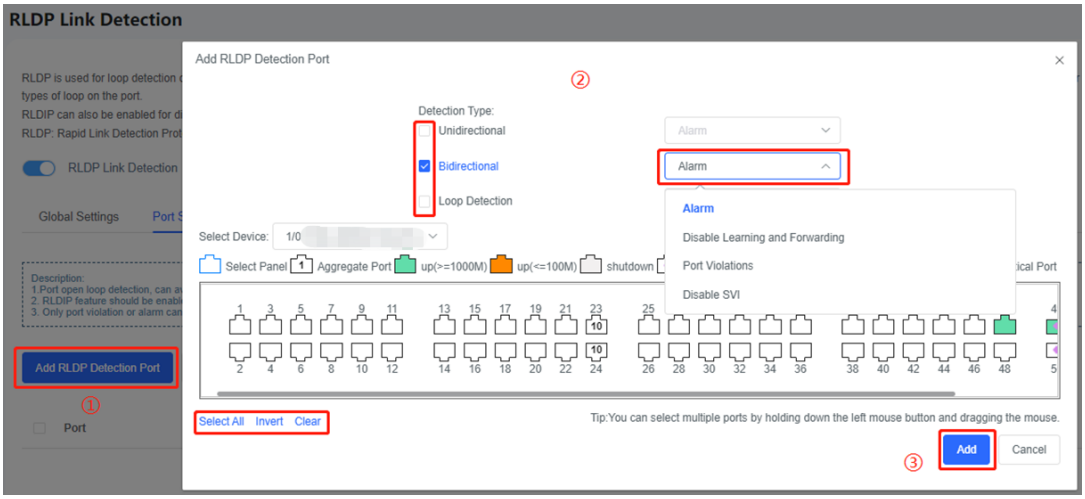
Figure4-90 RLDP Link Detection - Port Settings



- Adding an RLDP detection port

  Click **Add RLDP-enabled port**. The **Add RLDP Detection Port** window is displayed. RLDP involves unidirectional link detection, bidirectional link detection, and loop detection. You can select multiple ports one by one, or using the **Select All**, **Invert**, and **Clear** button. Click **Add** to submit the configuration. The result will be displayed in the list.

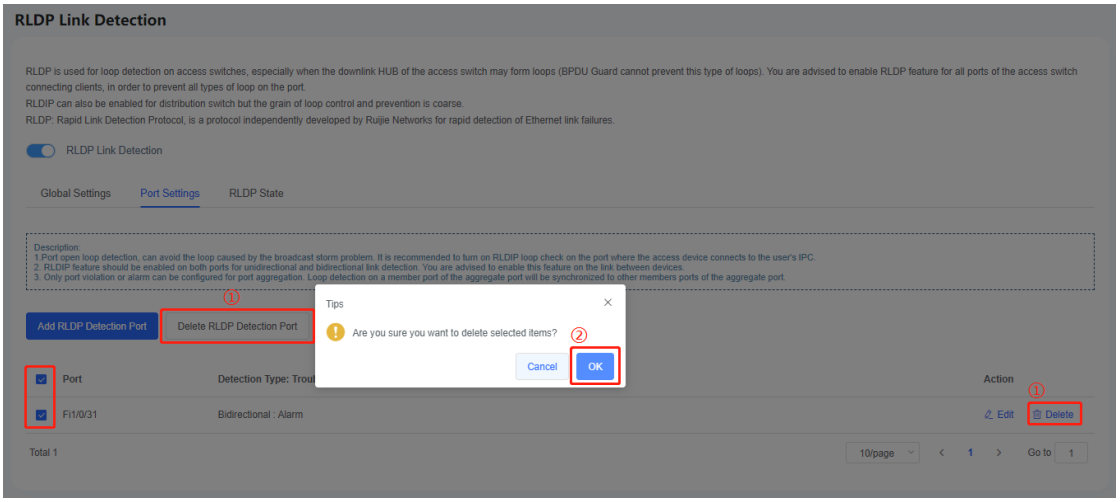
Figure4-91 Adding an RLDP detection port



- Deleting RLDP detection ports

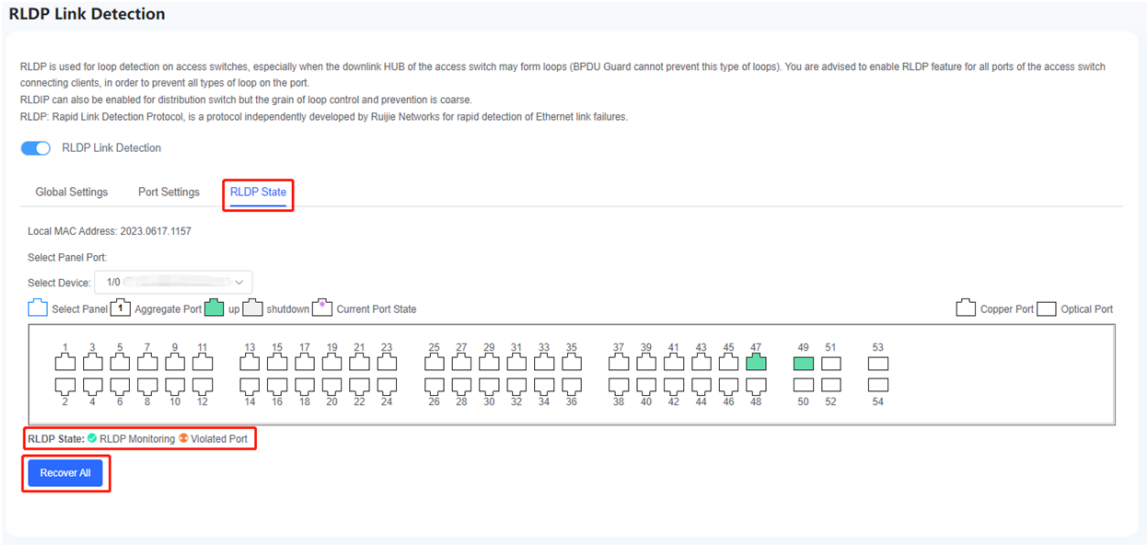
  Select one or multiple ports. Click **Delete** or **Delete RLDP Detection Port** to delete the selected ports.

Figure4-92 Deleting RLDP Detection Ports



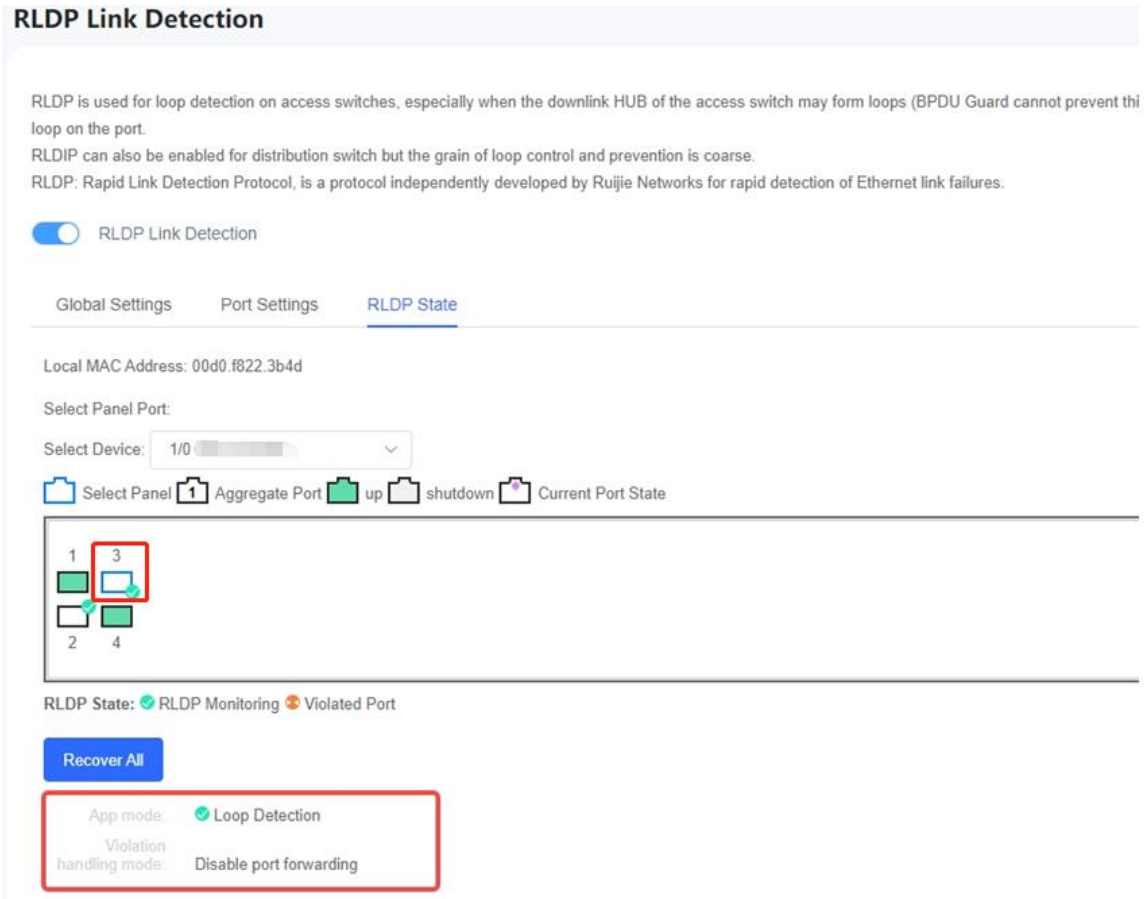
(4) RLDP State

Figure4-93 RLDP Link Detection - RLDP State



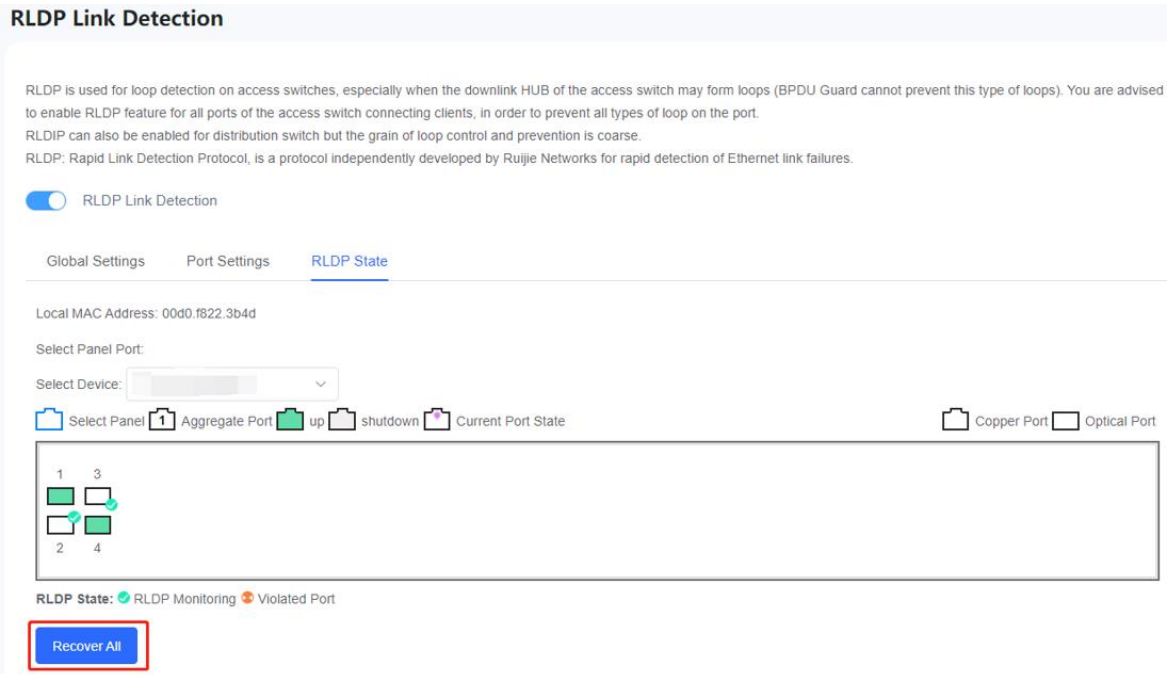
RLDP State: You can view the RLDP state of a port enabled with RLDP detection on the panel by clicking it.

Figure4-94 RLDP state of a port



Restore All: You can click **Restore All** to recover all violated ports.

Figure4-95 Restore All



4.4.3 Route Configuration

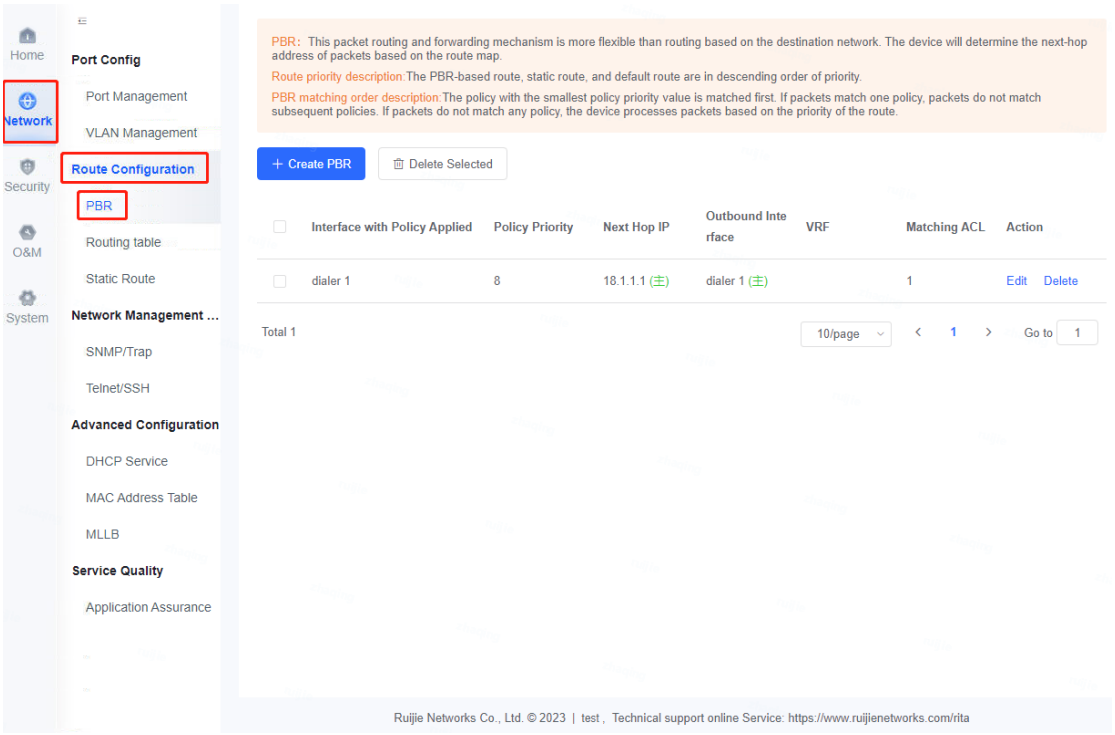
1. PBR

Route priority description: The PBR-based route, static route, and default route are in descending order of priority.

PBR matching order description: The policy with the smallest policy priority value is matched first.

Choose **Network** > **Route Configuration** > **PBR**.

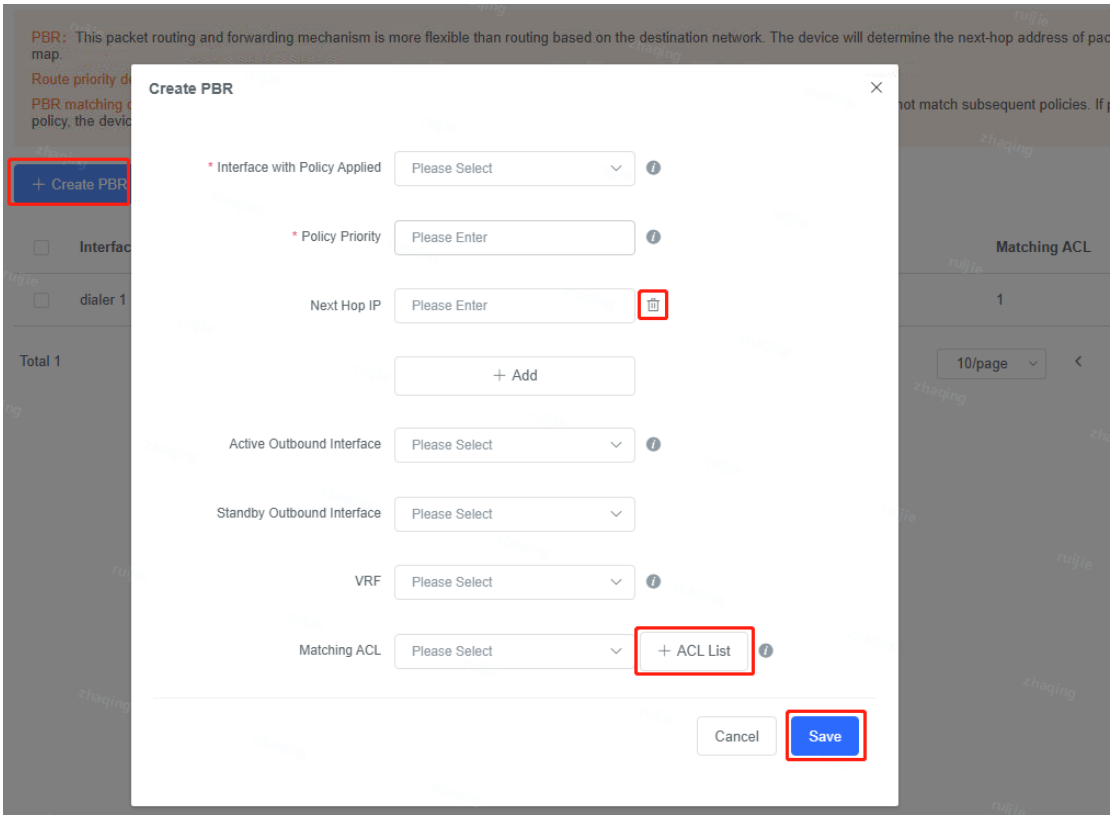
Figure4-96 PBR



(2) Creating a PBR

Click **Create PBR**. Set the configuration items in the pop-up window. Click **Save** to deliver the configuration.

Figure4-97 Creating a PBR



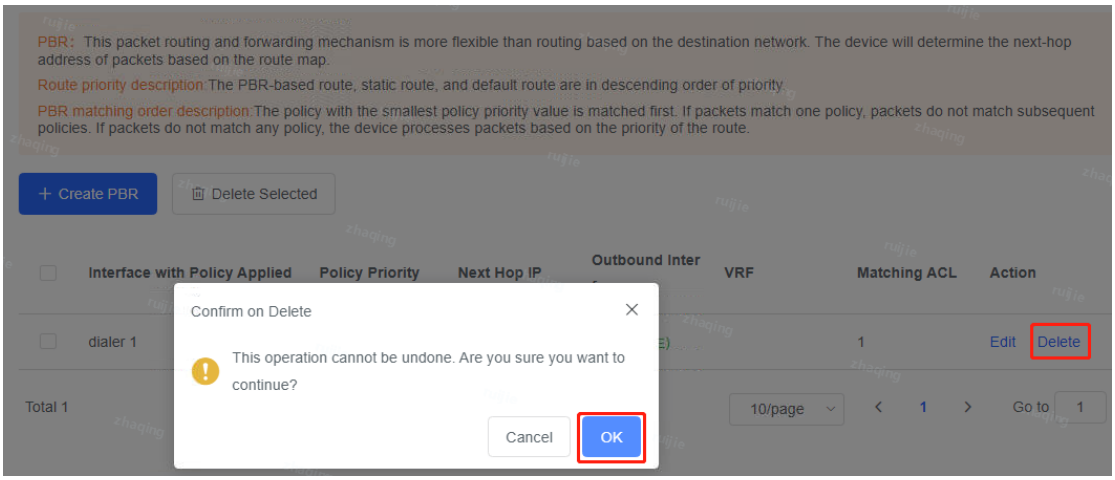
(3) Editing a PBR

Click **Edit** in the **Action** column of a PBR. Modify the configuration items in the pop-up window. Click **Save** to deliver the configuration.

(4) Deleting a PBR

You can delete one PBR or delete multiple PBRs in a batch. Select PBRs and click **Delete Selected** to delete the PBRs in a batch. Click **Delete** in the **Action** column of a PBR to delete it.

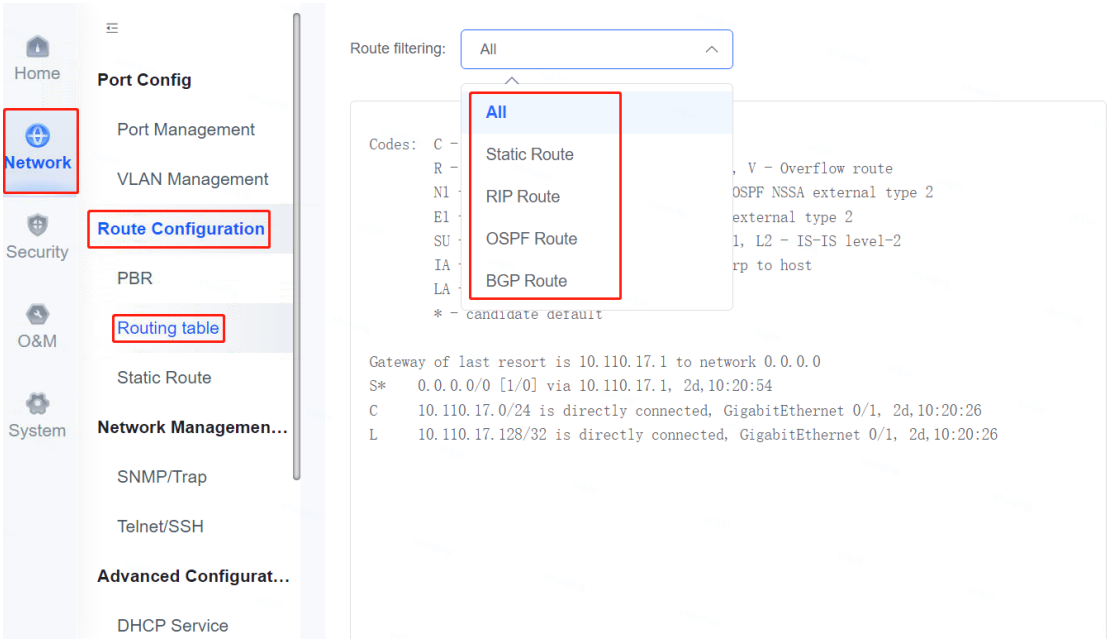
Figure4-98 Deleting a PBR



2. Routing table

Choose **Network** > **Route Configuration** > **Routing table**. You can select a route type from the **Route filtering** drop-down list to filter routes.

Figure4-99 Routing table



3. Static Route

Static Route: By adding a static route, packets destined for a specified destination network are routed along a predetermined path.

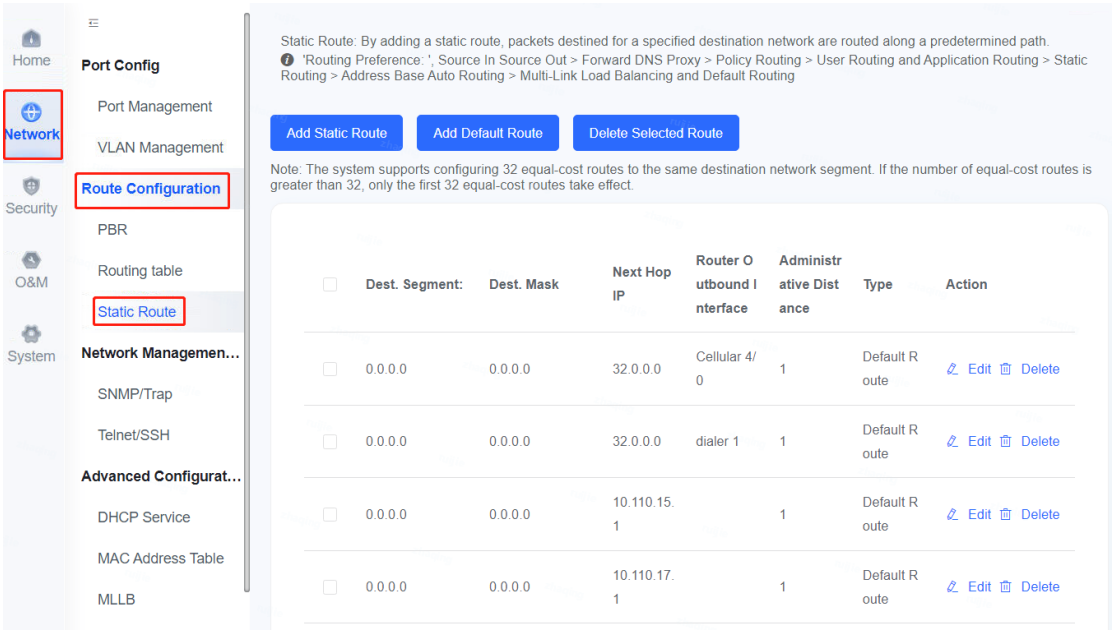
Routing Preference: Source In Source Out > Forward DNS Proxy > Policy Routing > User Routing and Application Routing > Static Routing > Address Base Auto Routing > Multi-Link Load Balancing and Default Routing

Caution

The system allows you to configure 32 equal-cost routes with the same destination network segment. If the upper limit is exceeded, the configuration only takes effect for the first 32 routes.

Choose **Network** > **Route Configuration** > **Static Route**.

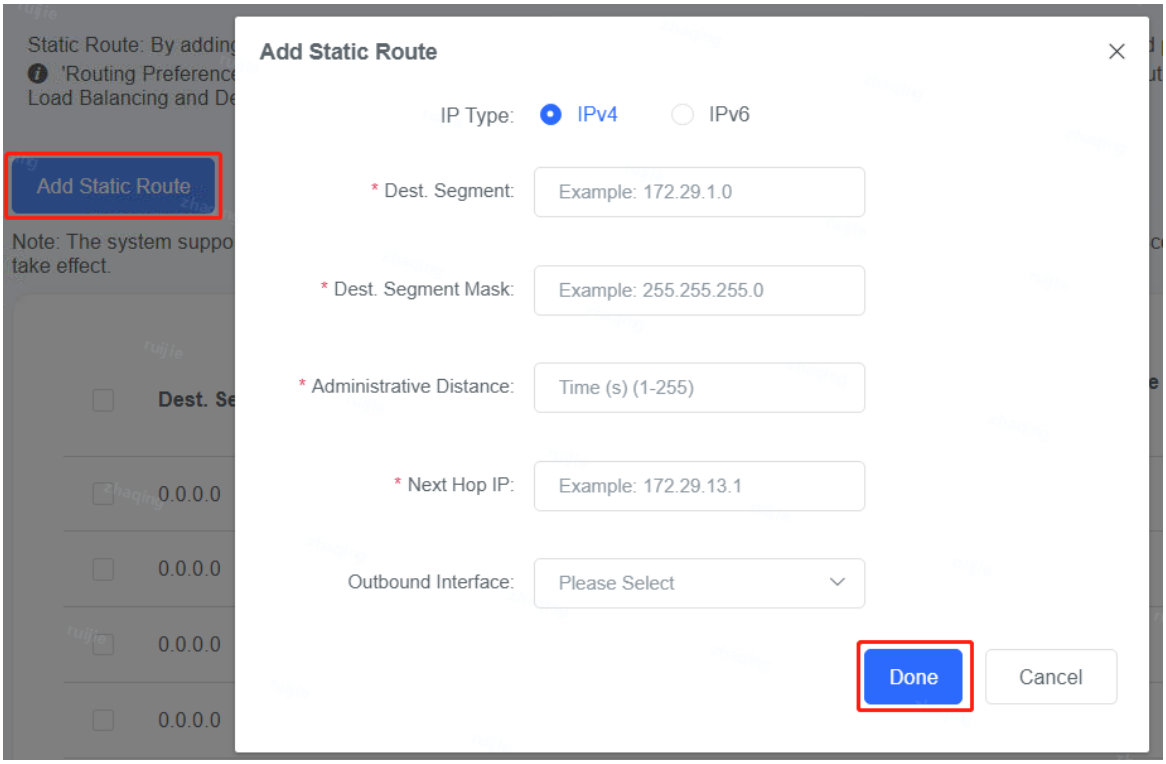
Figure4-100 Static Route



(2) Adding a Static Route

Click **Add Static Route**. In the pop-up window, set relevant parameters. After the configuration is complete, click **Done**.

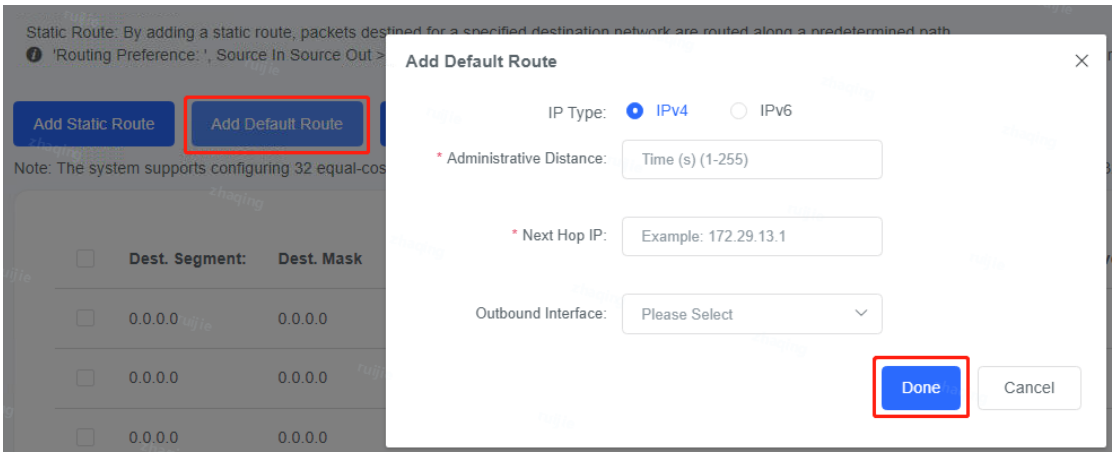
Figure4-101 Adding a Static Route



(3) Adding a Default Route

Click **Add Default Route**. In the pop-up window, set relevant parameters. After the configuration is complete, click **Done**.

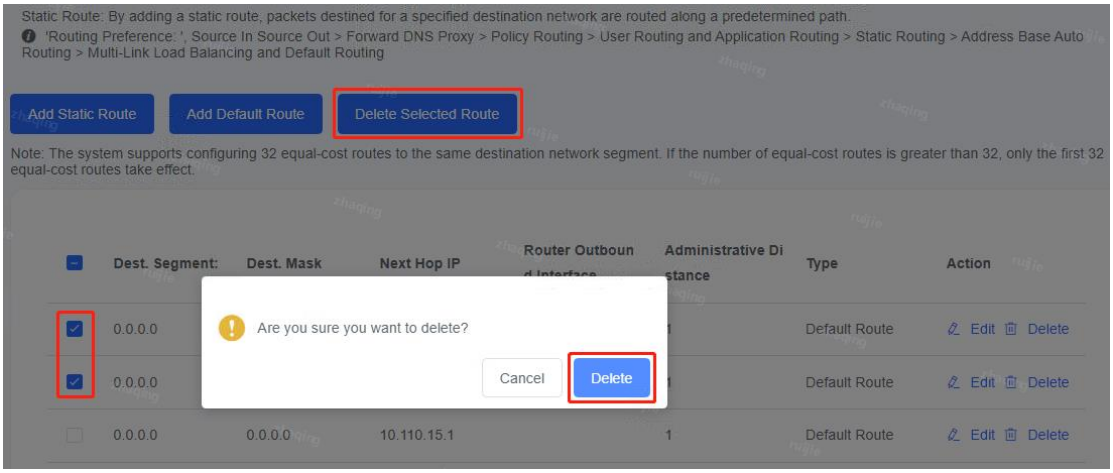
Figure4-102 Adding a Default Route



(4) Deleting Selected Routes

Select multiple routes and click **Delete Selected Route**. In the dialog box that is displayed, click **Delete**.

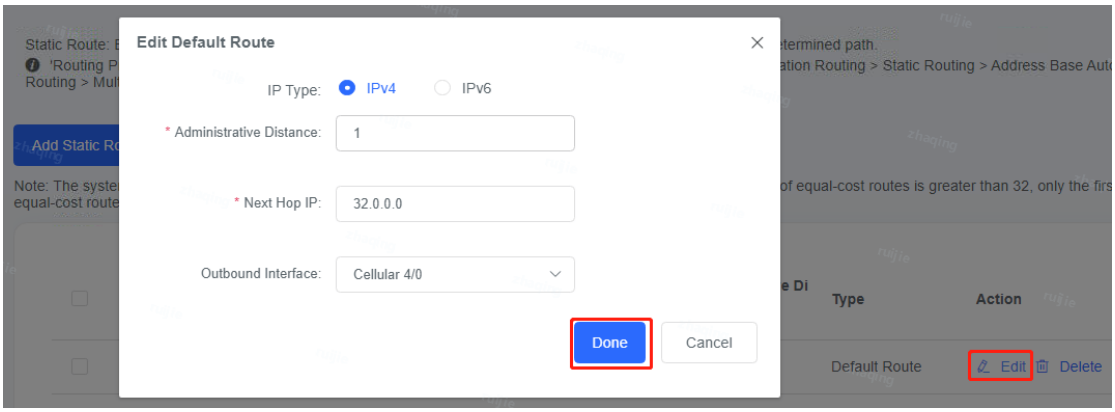
Figure4-103 Deleting Selected Routes



(5) Editing Default Route

Click **Edit** on the **Action** column of a route. In the pop-up window, set the configuration items. After the configuration is complete, click **Done**.

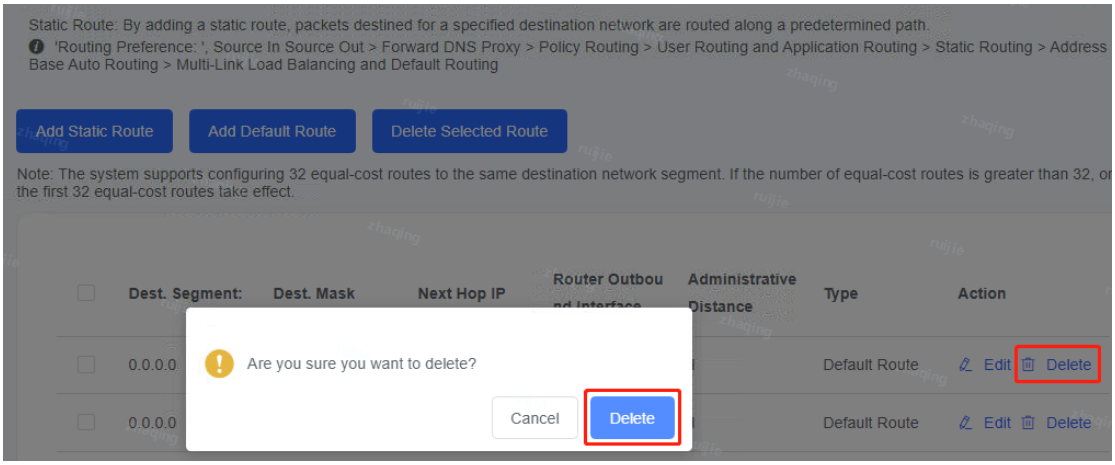
Figure4-104 Editing Default Route



(6) Deleting a route

Click **Delete** on the **Action** column. On the displayed dialog box, click **Delete**.

Figure4-105 Deleting a route



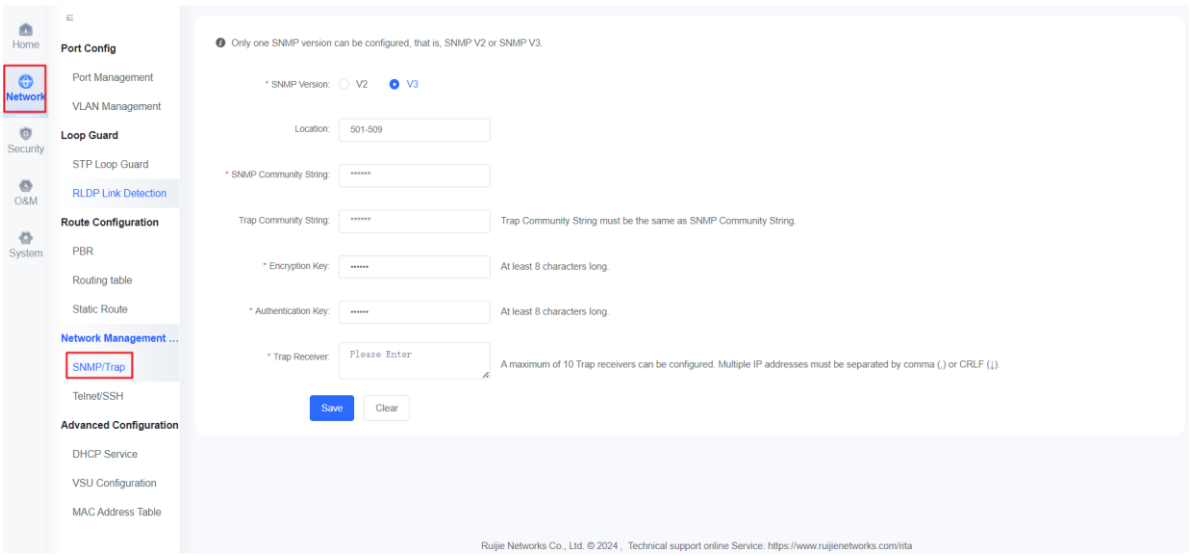
4.4.4 Network Management Protocols

1. SNMP/Trap

Choose Network > Network Management Protocols > SNMP/Trap to access the SNMP/Trap function page.

The Simple Network Management Protocol (SNMP) enables a network administrator to easily monitor and manage nodes on a network.

Figure4-106 SNMP/Trap

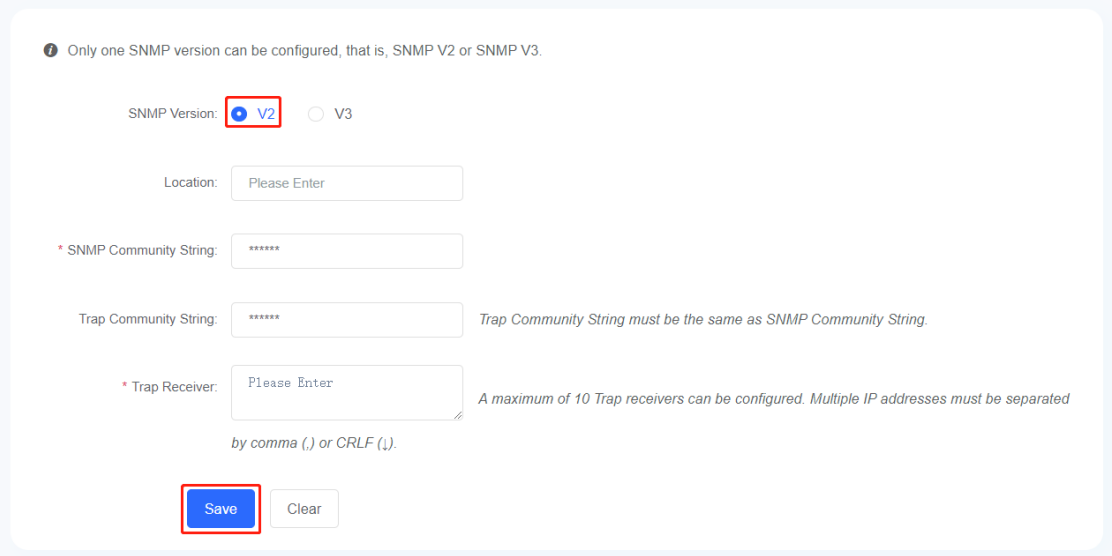


- SNMP Version: indicates the SNMP version supported by the device, which can be SNMPv2 or SNMPv3.
- Location: indicates the location of the device.
- SNMP Community String: is used by the management host to connect to a device.
- Trap Community String: is used to connect to the management host. When an alarm is generated on a device, the switch can send the alarm to the management host.
- Trap receiver: refers to the management host that receives alarms from a switch. A maximum of 10 trap

receivers can be configured.

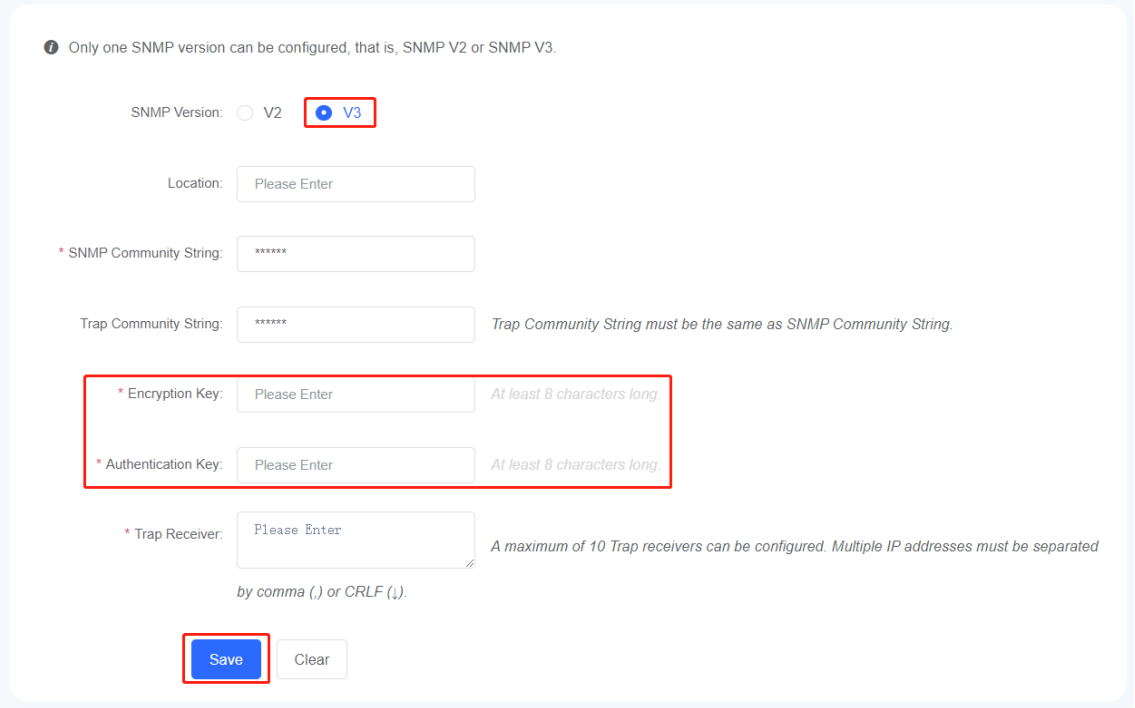
- **SNMP V2**: Select **V2**. Set configuration parameters and click **Save** to submit the configuration.

Figure4-107 SNMP V2



- **SNMP V3**: Select **V3**. Set configuration parameters and click **Save** to submit the configuration.

Figure4-108 SNMP V3

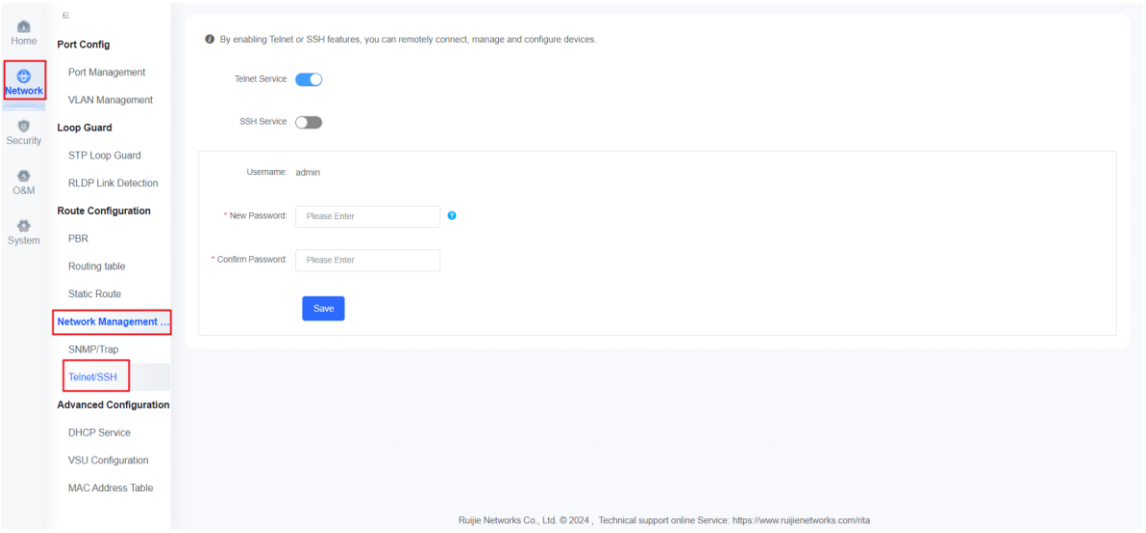


- **Clear**: Click **Clear** to clear the SNMPv2 or SNMPv3 configuration.

2. Telnet/SSH

Choose **Network** > **Network Management Protocols** > **Telnet/SSH** to access the **Telnet/SSH** function page.

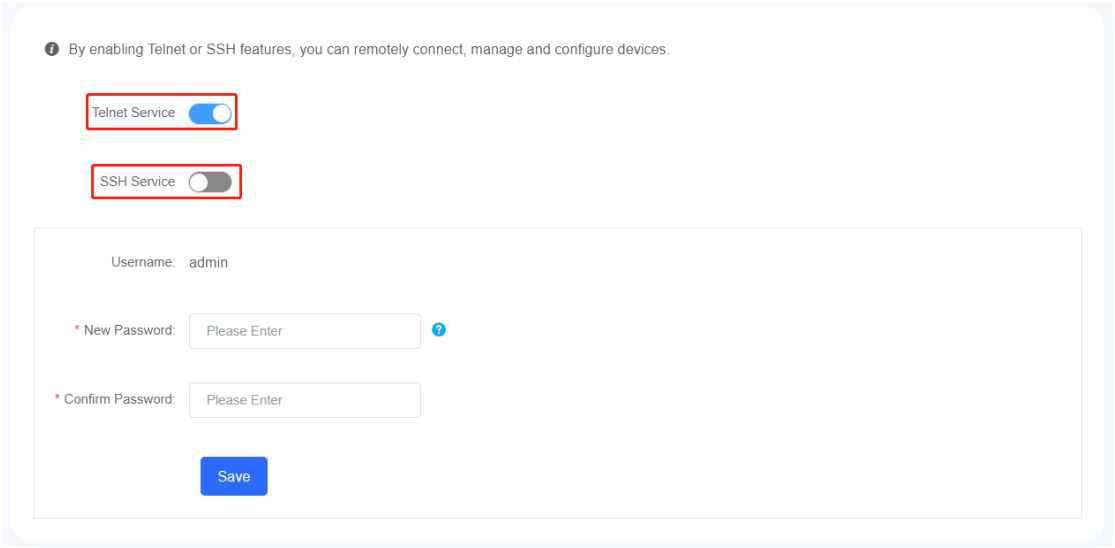
Figure4-109 Telnet/SSH



Telnet/SSH: Click **Telnet Service** to enable or disable the Telnet service, and click **SSH Service** to enable or disable the SSH service.

The default user name is **admin**. Set configuration parameters and click **Save** to submit Telnet or SSH configurations. When both the Telnet service and SSH service are disabled, you do not need to set a password.

Figure4-110 Enable/disable Telnet/SSH



When configuring a switch through Telnet, you must log in with this password.

Note

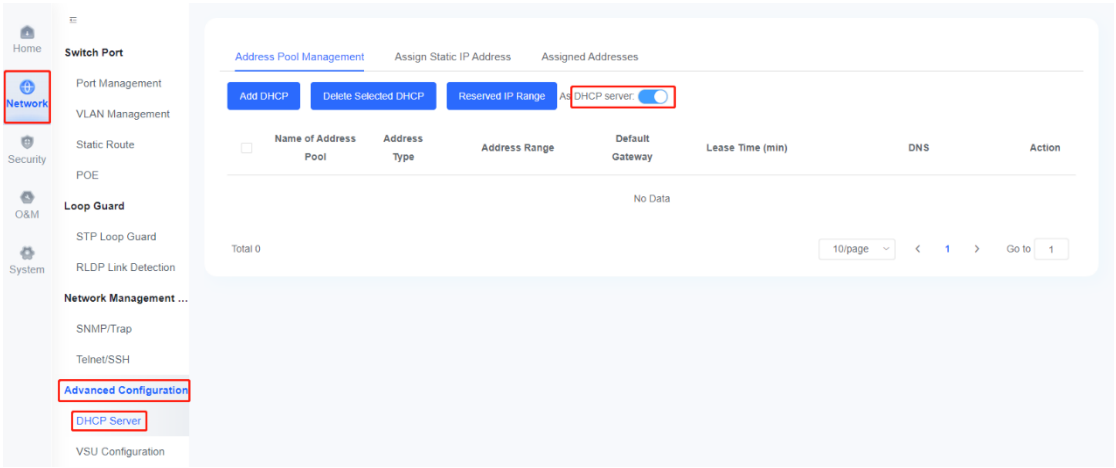
Remember the new password for login next time.

4.4.5 Advanced Configuration

1. DHCP Server

Choose **Network** > **Advanced Configuration** > **DHCP Server** to access the DHCP Server page.

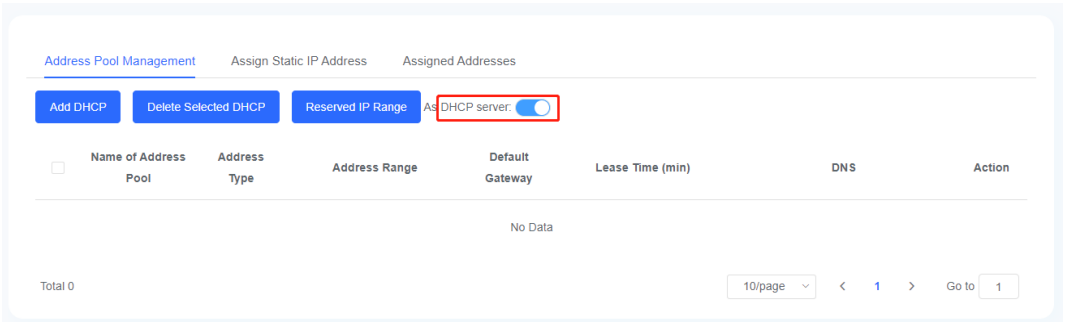
Figure4-111 DHCP Server



(2) Address Pool Management

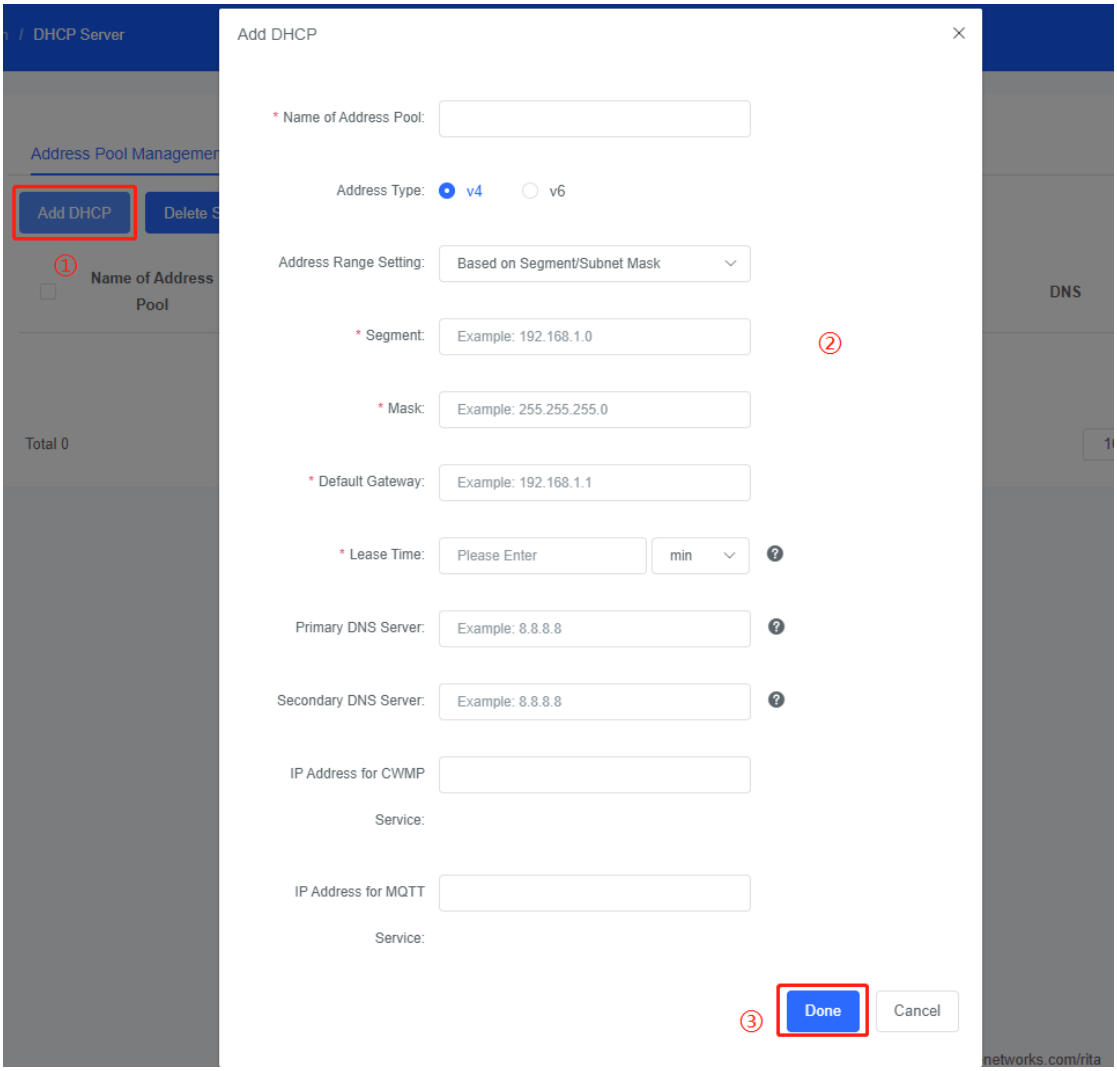
Click **As DHCP server** to enable or disable DHCP server.

Figure4-112 Address Pool Management



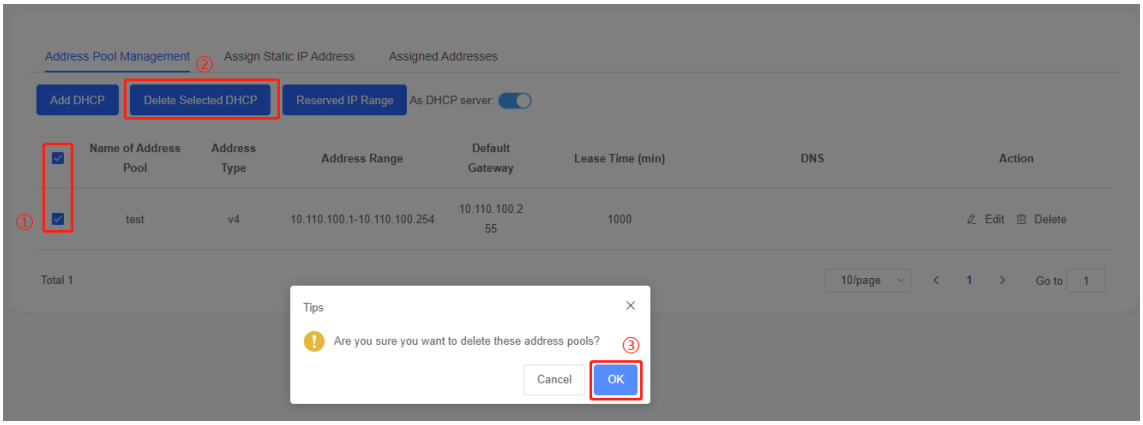
- Adding a DHCP address pool
  a. Click **Add DHCP**.
  b. Set configuration parameters in the displayed windows.
  c. Click **Done**. The result will be displayed in the list.

Figure4-113 Adding a DHCP address poo



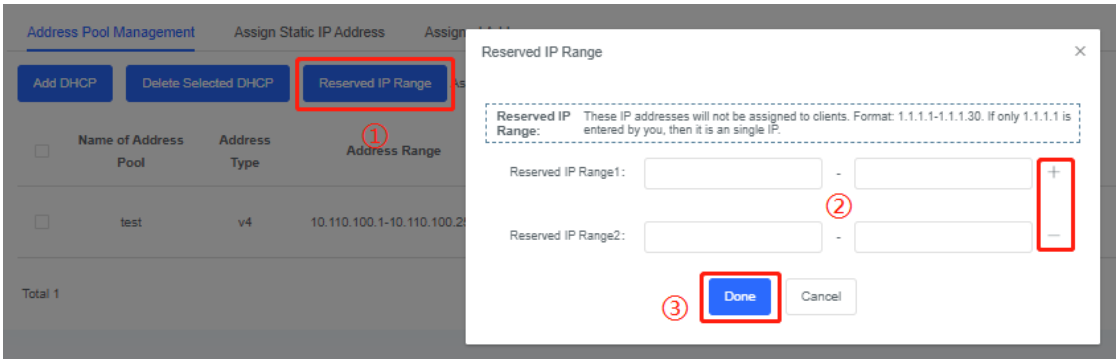
- Deleting the selected DHCP address pool
  a. Click **Delete Selected DHCP**.
  b. Click **OK**. The selected DHCP address pool is deleted.

Figure4-114 Deleting the selected DHCP address pool



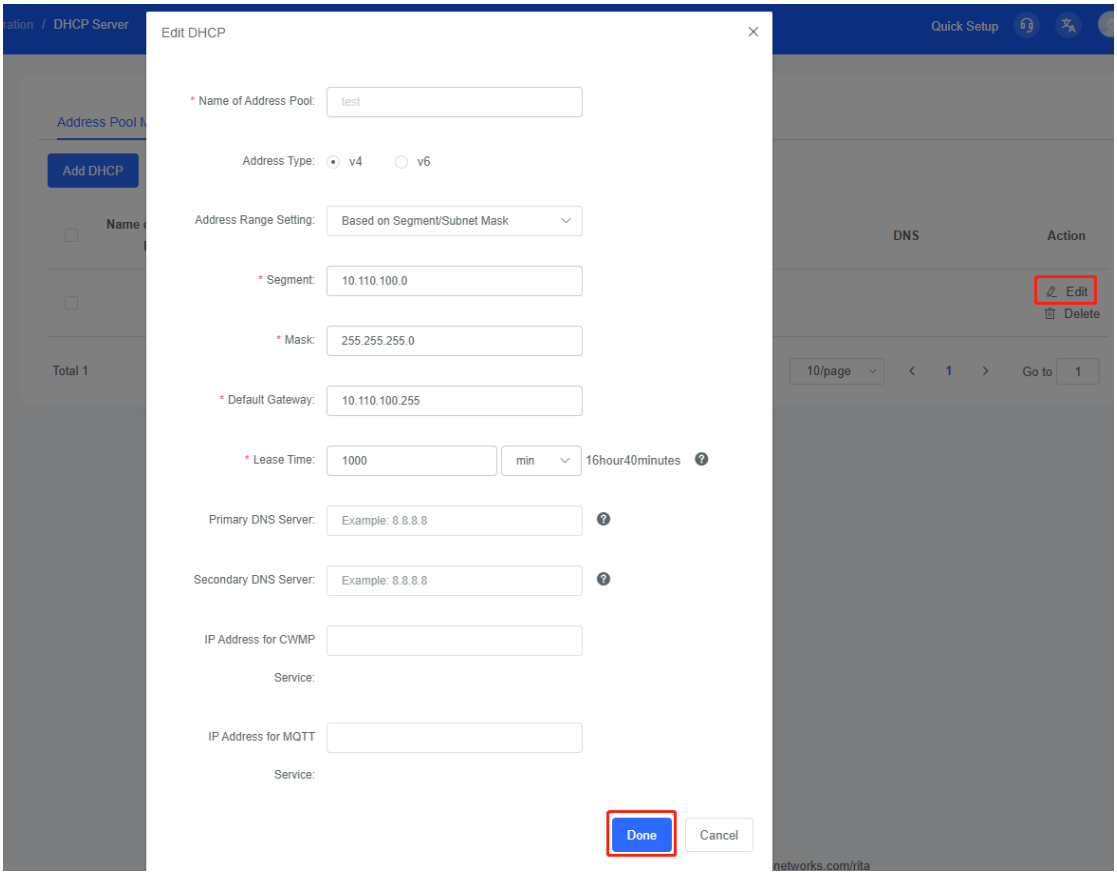
- Configuring the reserved IP range
  a. Click **Reserved IP Range**.
  b. Set configuration parameters in the displayed windows.
  c. Click **Done**. The result will be displayed on the Reserved IP Range page. The IP addresses in the configured reserved IP range will not be assigned to the clients.

Figure4-115 Configuring the reserved IP range



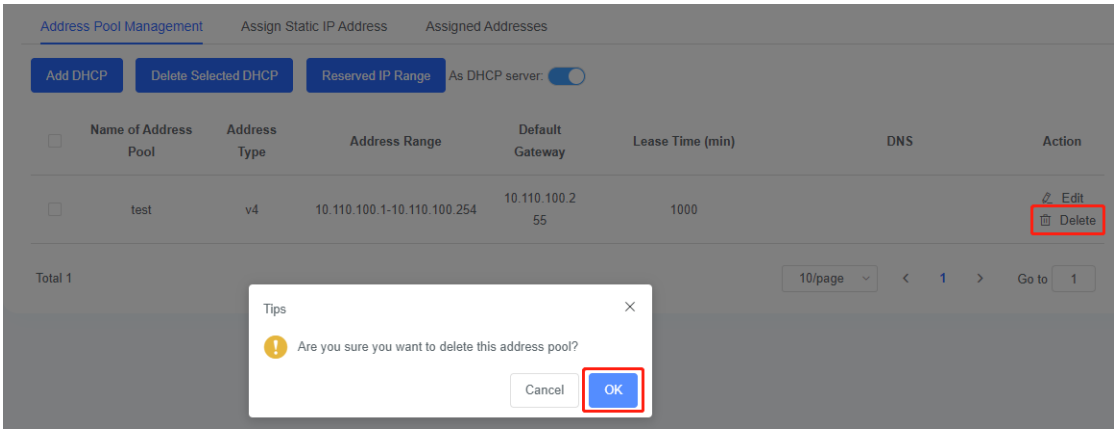
- Editing a DHCP address pool
  a. Click **Edit**.
  b. Set configuration parameters in the displayed windows.
  c. Click **Done**. The result will be displayed in the list.

Figure4-116 Editing a DHCP address pool



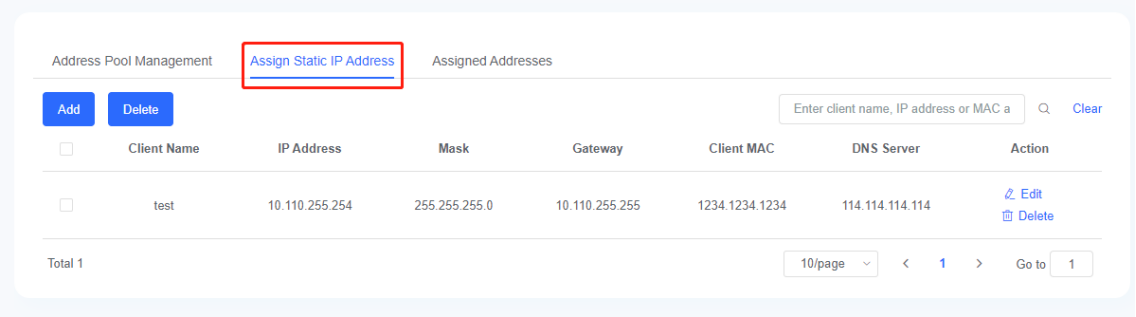
- Deleting a DHCP address pool

Figure4-117 Deleting a DHCP address pool



(3) Assign Static IP Address

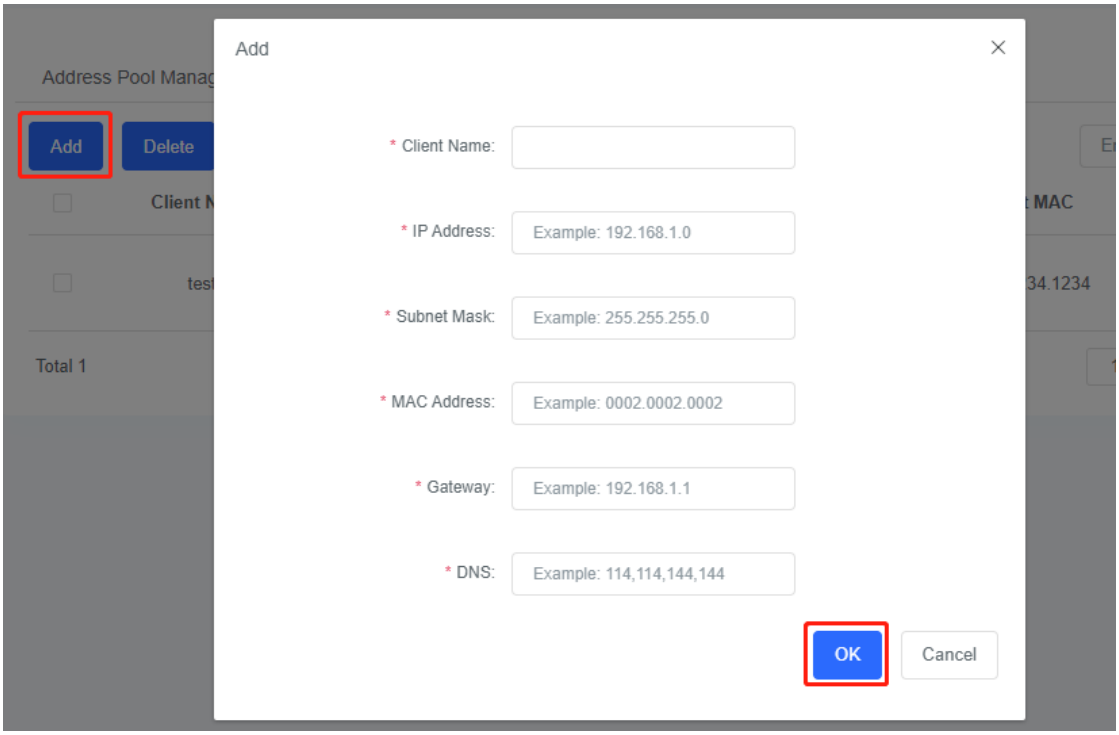
Figure4-118 Assign Static IP Address



- Adding a static IP Address

  Click **Add**. Set configuration parameters in the displayed windows. Click **OK**. The result will be displayed in the list.

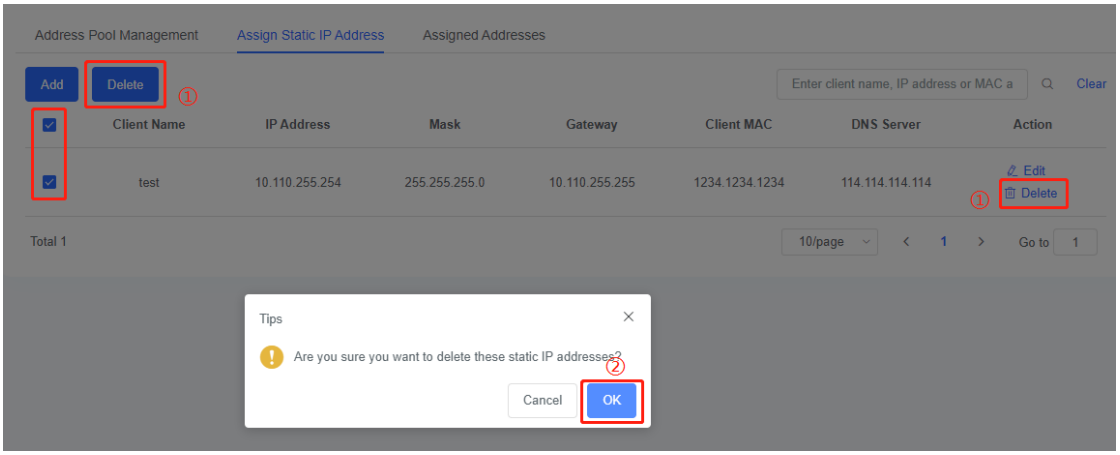
Figure4-119 Adding a static IP Address



- Deleting a static IP Address

  Click **Delete**. Click **OK** in the displayed windows. The static IP address will be deleted from the list.

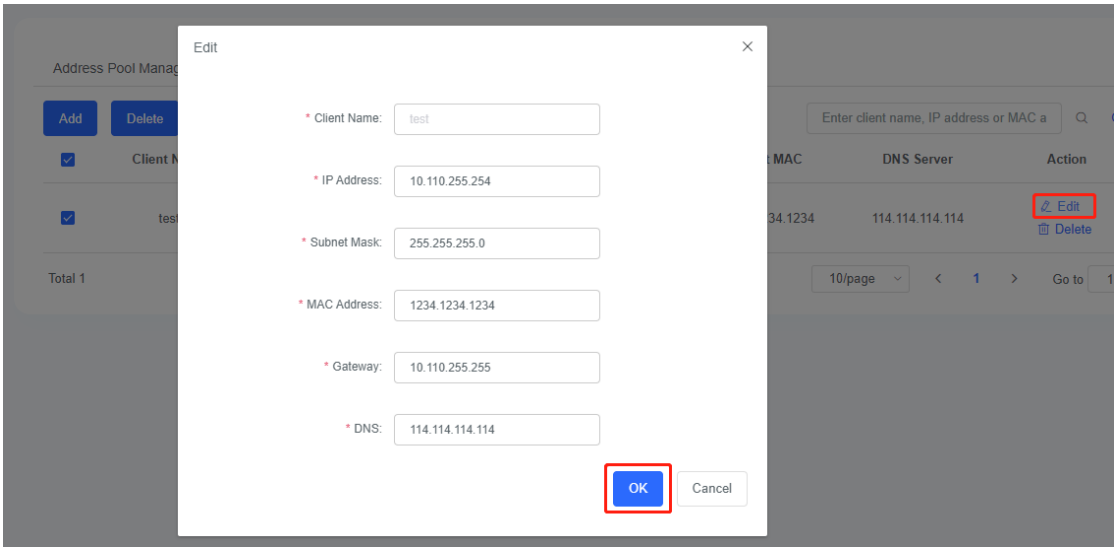
Figure4-120 Deleting a static IP Address



- Editing a static IP Address

  Click **Edit**. Set configuration parameters in the displayed windows. Click **OK**. The result will be displayed in the list.

Figure4-121 Editing a static IP Address



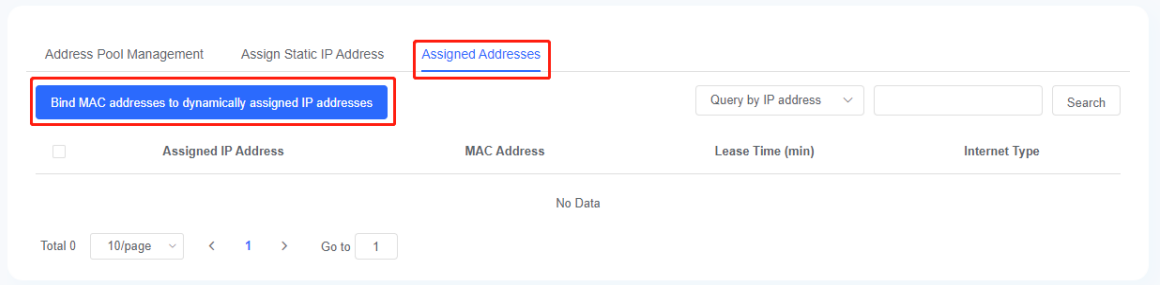
(4) Assigned Addresses

On this page, you can bind MAC addresses to dynamic IP addresses and reclaim assigned addresses.

a. Select the assigned IP addresses, and click Bind MAC addresses to dynamically assigned IP addresses.

b. On the displayed dialog box, click OK.

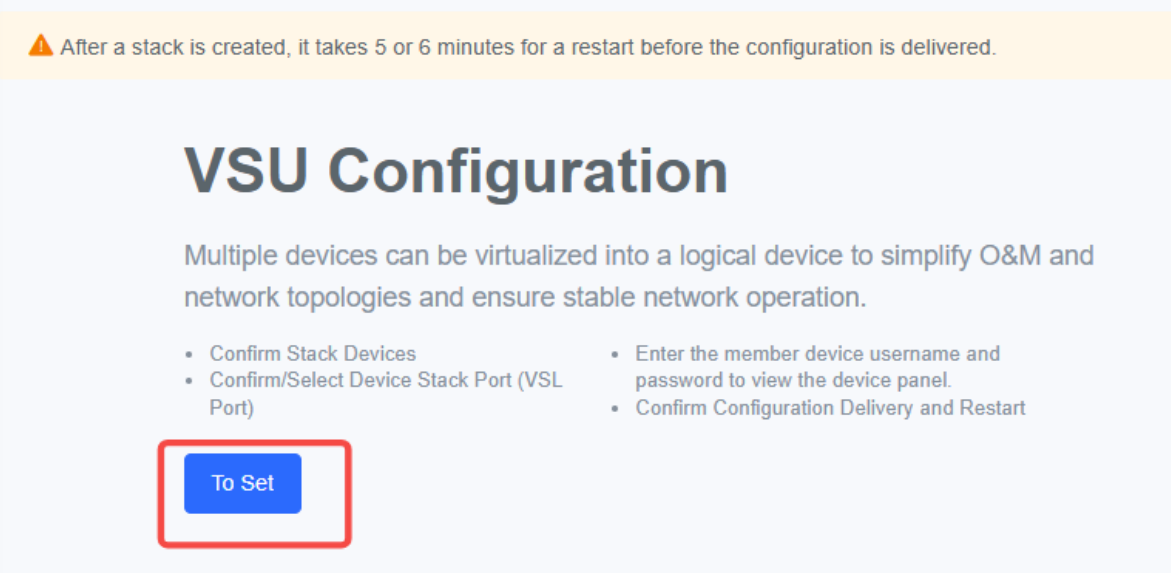
Figure4-122 Assigned Addresses



2. VSU Settings

Choose **Network** > **Advanced Configuration** > **VSU Settings** to access the **VSU Settings** page.

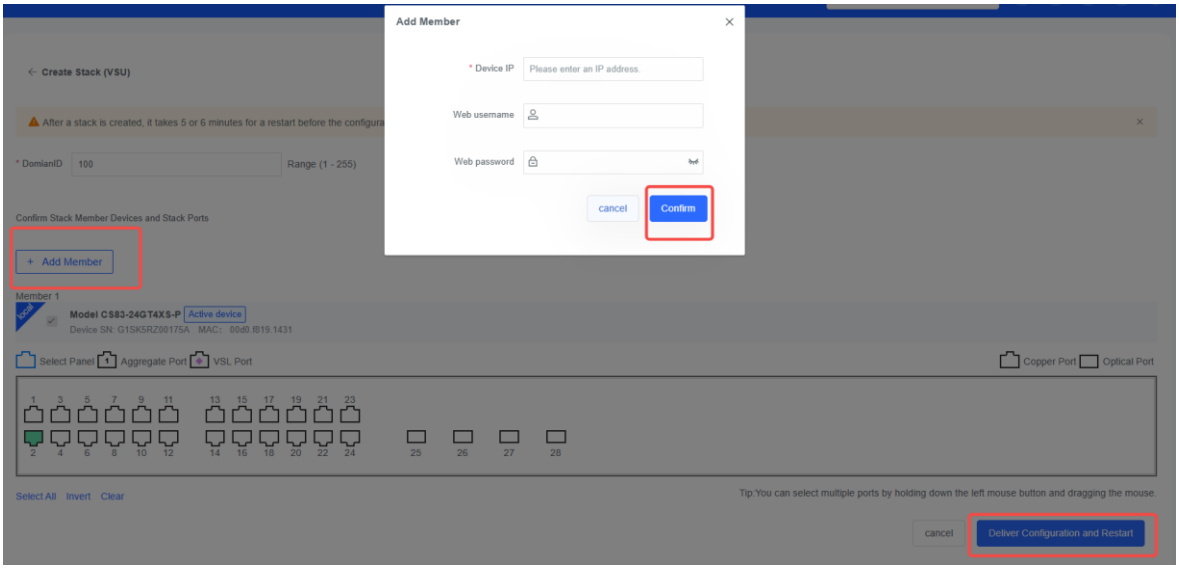
Figure4-123 VSU Settings



- VSU settings
  As shown in Figure4-123, click **To Set**. The **Create Stack (VSU)** page is displayed.

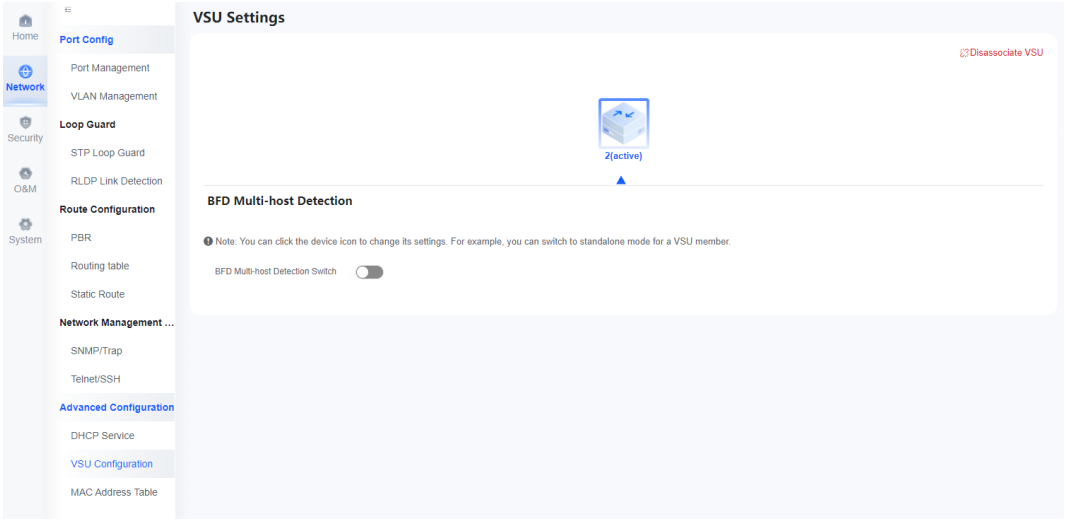
  On the **Create Stack (VSU)** page, set **DomianID** and click **Add Member**. Configure the member information and click **Confirm**. Click **Deliver Configuration and Restart**. Wait for the device to restart and enter the VSU mode.

Figure4-124 Create Stack (VSU)



[Figure4-125](#) shows the **VSU Settings** page after the device restarts and you perform the VSU configuration.

Figure4-125 VSU Settings



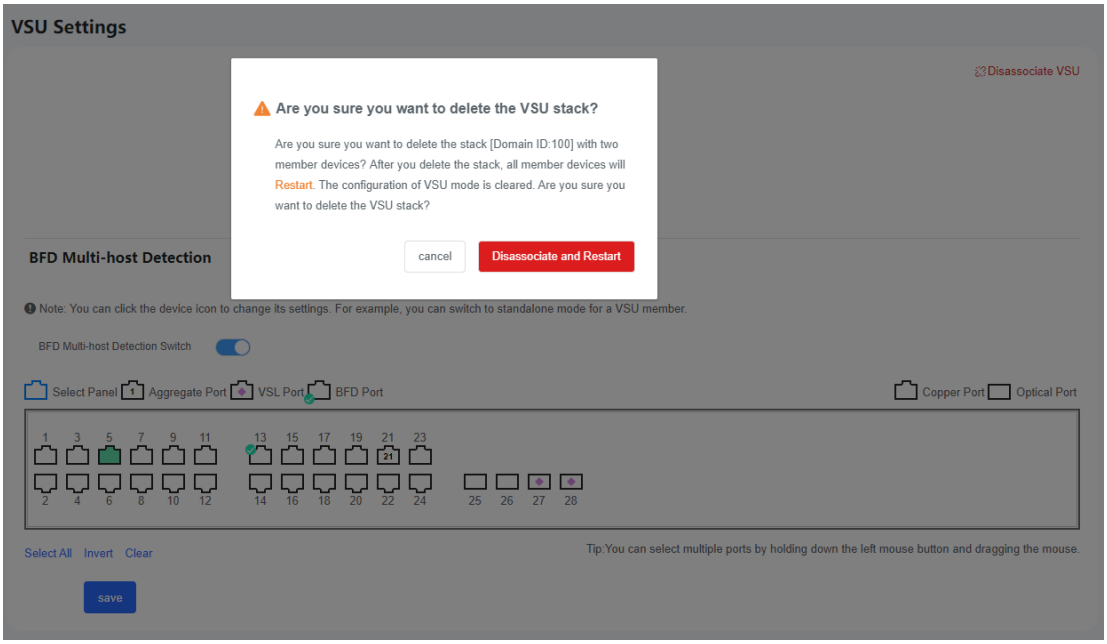
(2) Deleting a VSU Stack

Caution

After you delete the VSU stack, all member devices will restart and the configuration of VSU mode will be cleared. Please operate with caution.

Click **Disassociate** VSU. On the displayed dialog box, click **Disassociate and Restart** to delete a VSU stack.

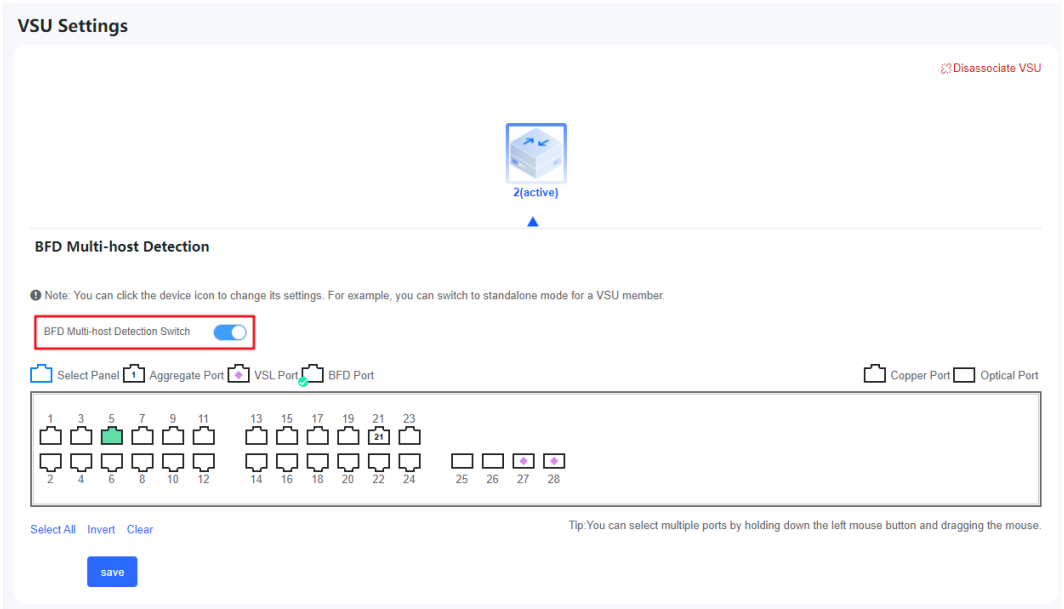
Figure4-126 Deleting a VSU Stack



(3) BFD Multi-host Detection Switch

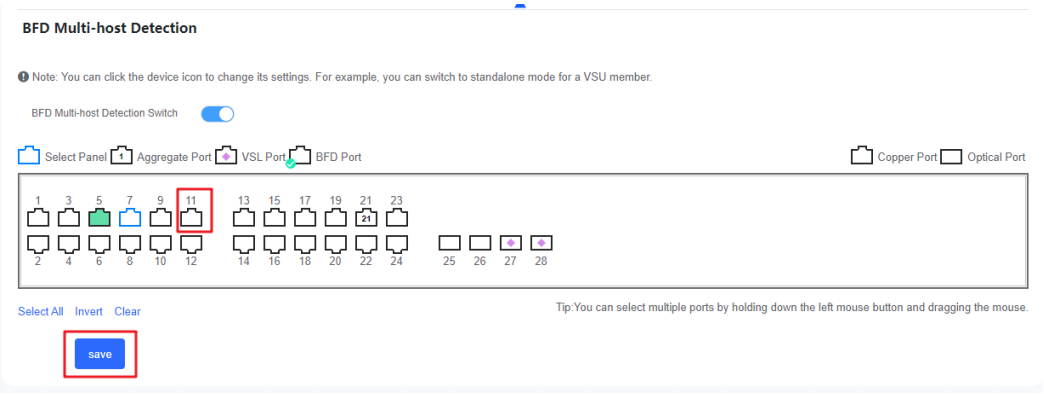
You can click **BFD Multi-host Detection Switch** to enable or disable the BFD Multi-host Detection.

Figure4-127 Enable/disable BFD Multi-host Detection Switch



Click a port on which BFD is not enabled. Click **Save** to enable BFD on the port.

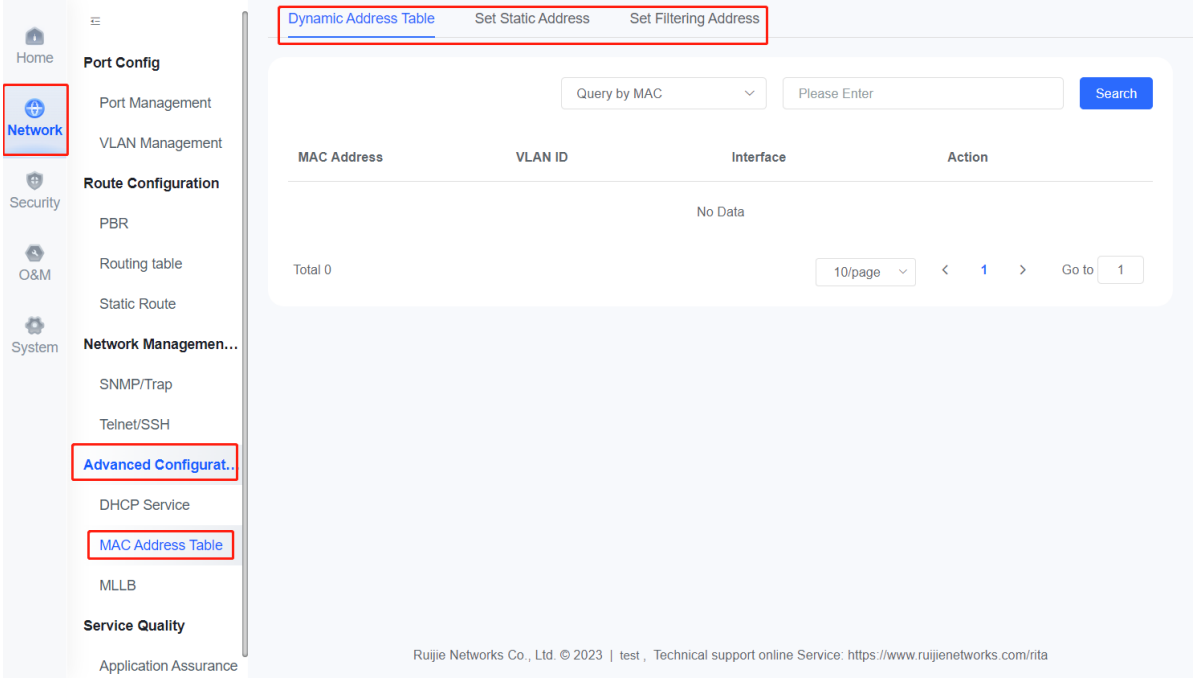
Figure4-128 Enable BFD on the port



3. MAC Address Table

Choose **Network** > **Advanced Configuration** > **MAC Address Table** to access the MAC Address Table page, as shown in the following figure. On this page, you can query dynamic address tables, set static addresses, and configure addresses to be filtered out.

Figure4-129 MAC Address Table

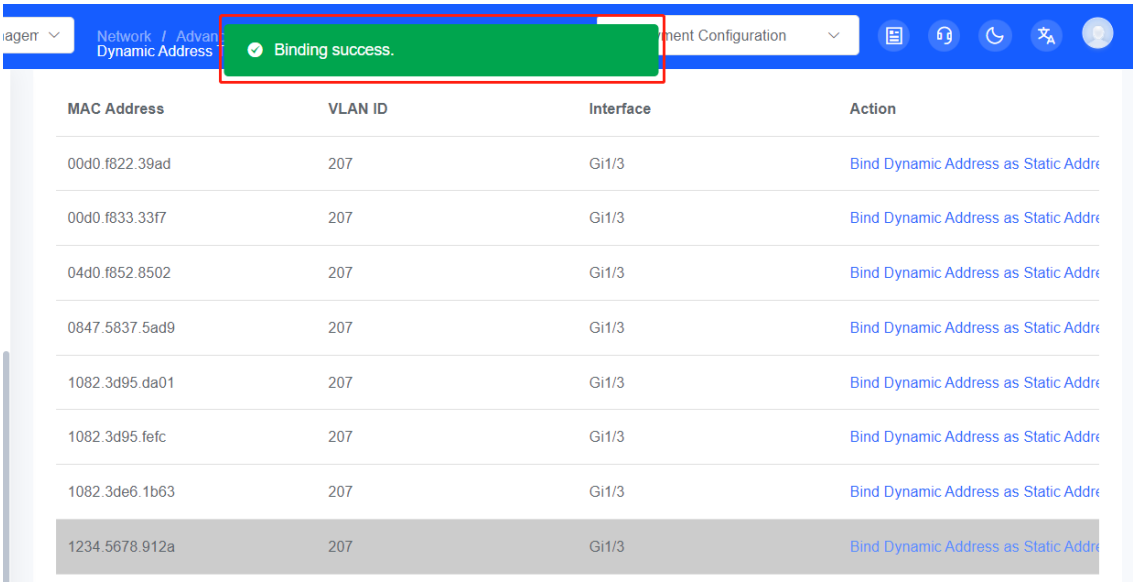


(2) Dynamic Address Table

You can bind a dynamic address as a static address and query dynamic MAC addresses on this page.

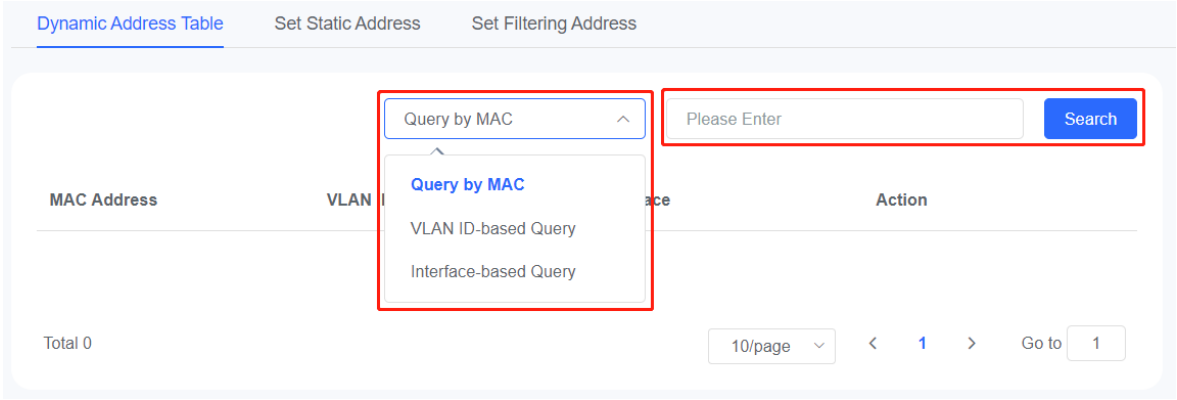
- Binding a dynamic address as a static address: Click **Bind Dynamic Address as Static Address** in the **Action** column. After the operation is successful, a message indicating binding success is displayed and the bound address is displayed in the static address list.

Figure4-130 Binding a Dynamic Address as a Static Address



- Querying dynamic MAC addresses: Click the drop-down list box on the left, and select a condition to query MAC addresses. In the search box, enter the corresponding content. Click **Search** to search for dynamic MAC addresses that meet the conditions. For example, if you select **VLAN ID-based Query**, you need to enter the VLAN ID in the search box.

Figure4-131 Querying dynamic MAC addresses



(3) Set Static Address

When the switch forwards data, it forwards packets based on the MAC address table. You need to manually bind MAC address of network devices to connected device interfaces. For example, a static address is configured. If the packet received in the VLAN carries the static address, the packet will be forwarded to the specified interface. If IEEE 802.1x authentication is enabled on an interface, you can configure MAC address binding without authentication.

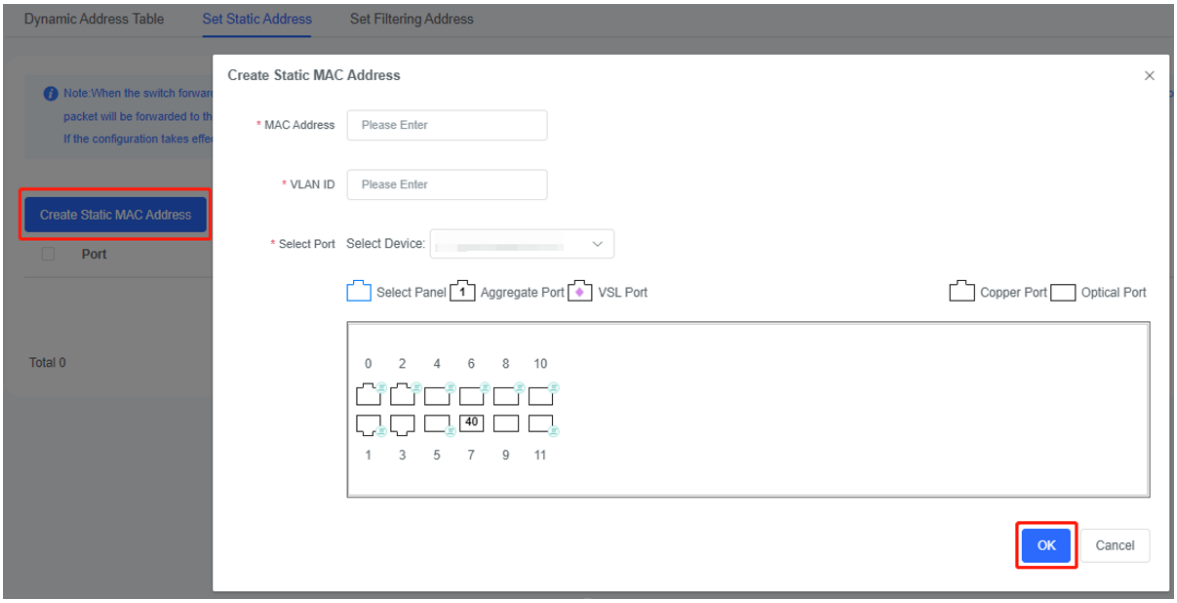
If the configuration takes effect but is not displayed properly on the page, please refresh the page.

On the **Set Static Address** page, you can create or delete static MAC addresses.

- Creating a Static Address

Click **Create Static MAC Address**. In the pop-up window, set the configuration items and click **OK** to deliver the configuration. A static MAC address is created.

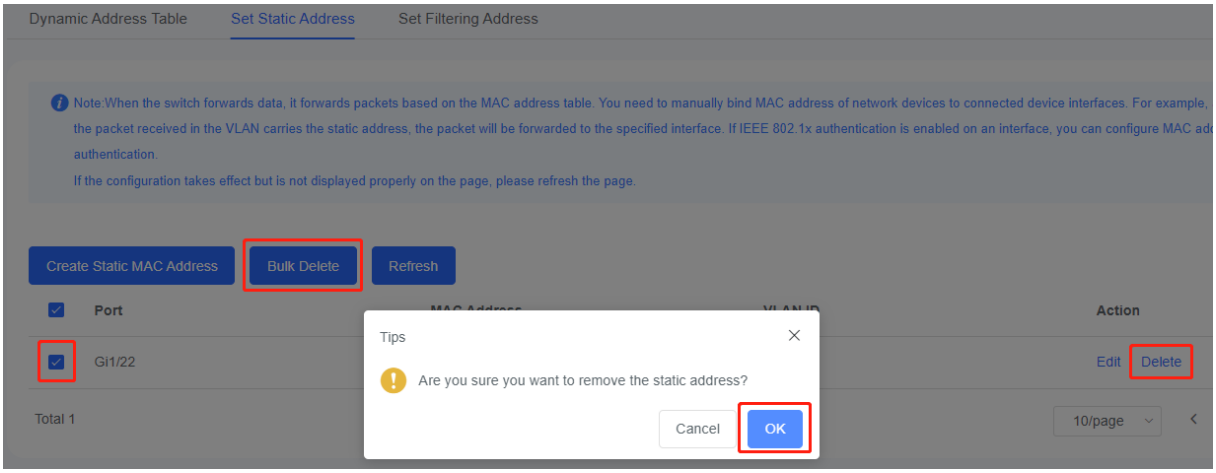
Figure4-132 Creating a Static Address



- Deleting Static Addresses

  Select one static address or multiple static addresses to be deleted, click **Delete** in the **Action** column or click **Bulk Delete**. In the displayed dialog box, click **OK**.

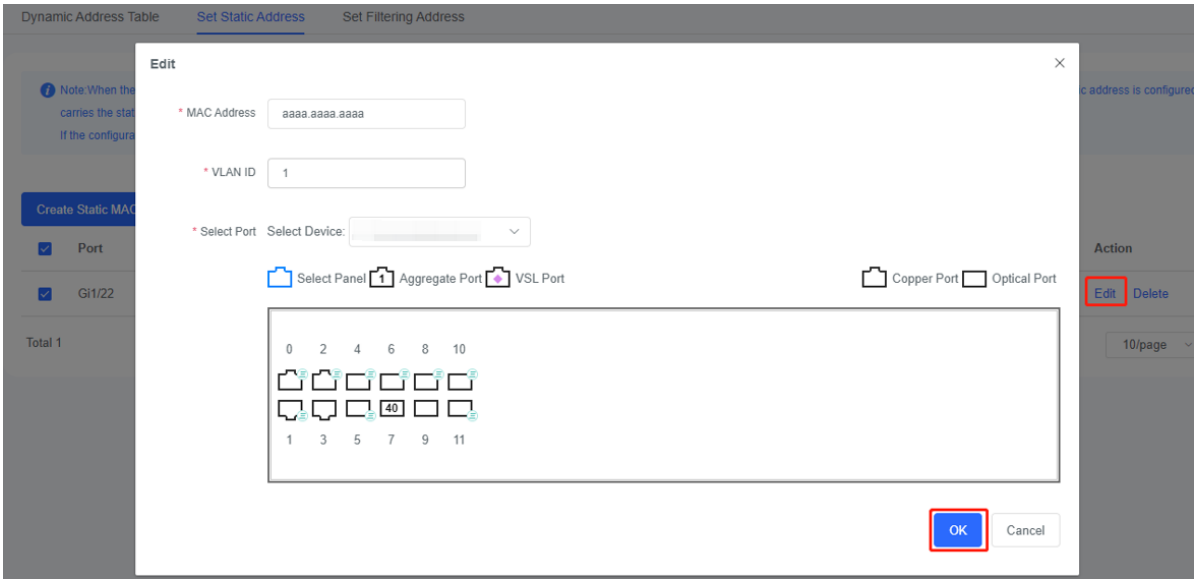
Figure4-133 Deleting Static Addresses



- Editing a Static Address

  Click **Edit** in the **Action** column. In the pop-up window, set the configuration items. Click **OK** to deliver the configuration.

Figure4-134 Editing a Static Address



(4) Set Filtering Address

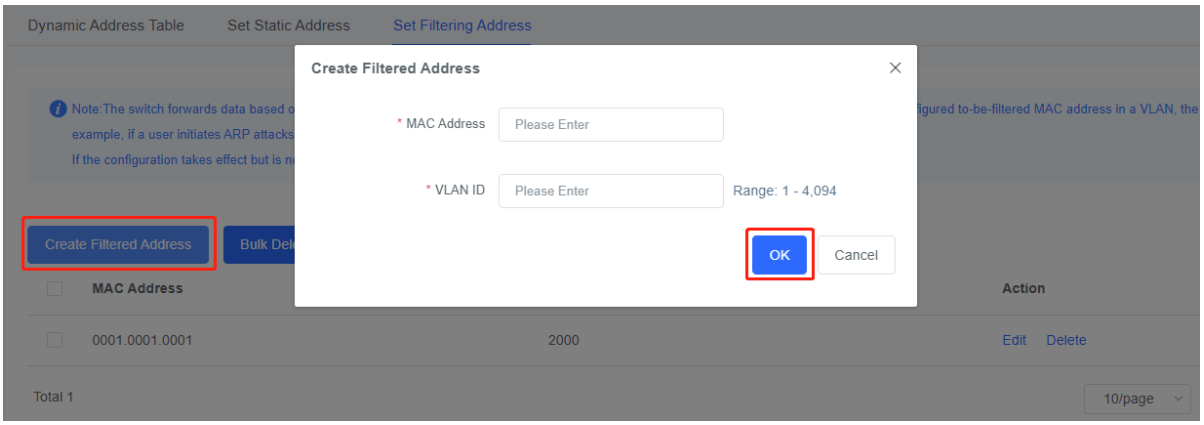
The switch forwards data based on the MAC address table. When receiving a packet with the source address or destination address of the configured to-be-filtered MAC address in a VLAN, the switch discards the packet. For example, if a user initiates ARP attacks, the MAC address of the user can be configured as a to-be-filtered address to prevent attacks.

If the configuration takes effect but is not displayed properly on the page, please refresh the page.

- Setting a MAC Address to Be Filtered Out

  Click **Create Filtered Address**. In the pop-up window, set the configuration items. Click **OK** to set a MAC address to be filtered out.

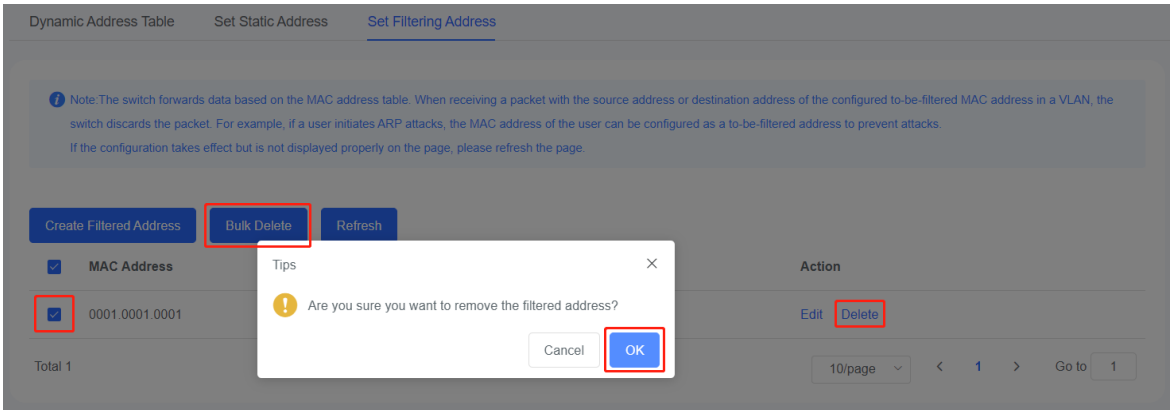
Figure4-135 Setting a MAC Address to Be Filtered Out



- Deleting MAC Addresses to Be Filtered Out

  Select one address or multiple addresses to be deleted, click **Delete** in the **Action** column or click **Bulk Delete**. In the displayed dialog box, click **OK**.

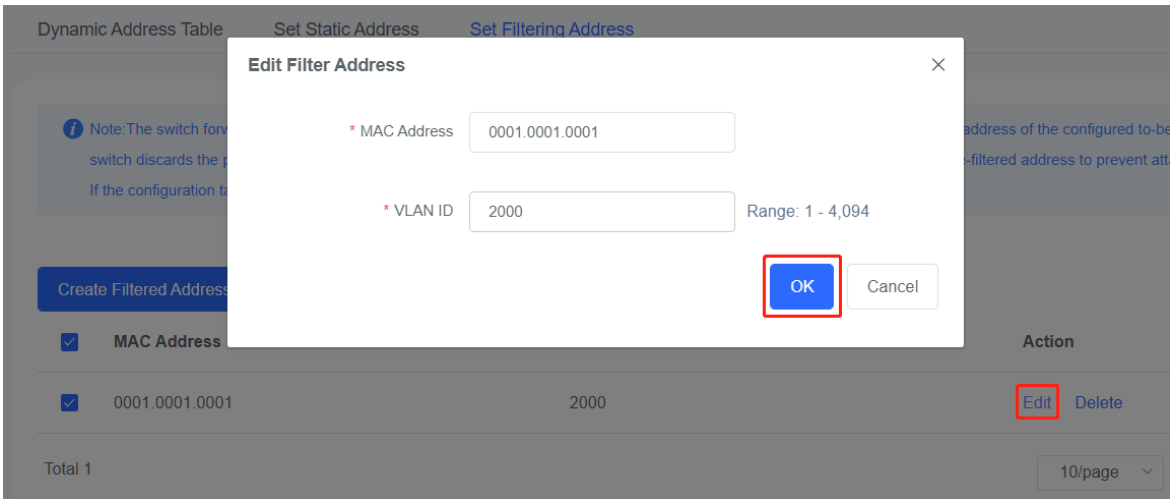
Figure4-136 Deleting MAC Addresses to Be Filtered Out



- Editing a MAC Address to Be Filtered Out

  Click **Edit** in the **Action** column. In the pop-up window, set the configuration items. Click **OK** to complete the modification.

Figure4-137 Editing a MAC Address to Be Filtered Out

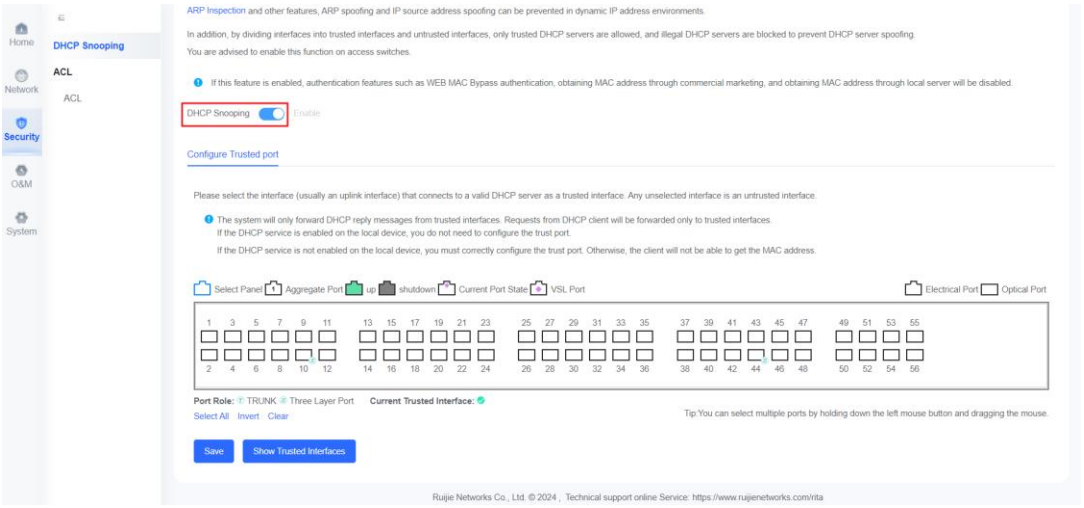


4.5 Security

4.5.1 DHCP Snooping

Choose **Security** > **DHCP Snooping** to access the **DHCP Snooping** page. Click **DHCP Snooping** to enable or disable DHCP Snooping. You can configure trusted interfaces in the page.

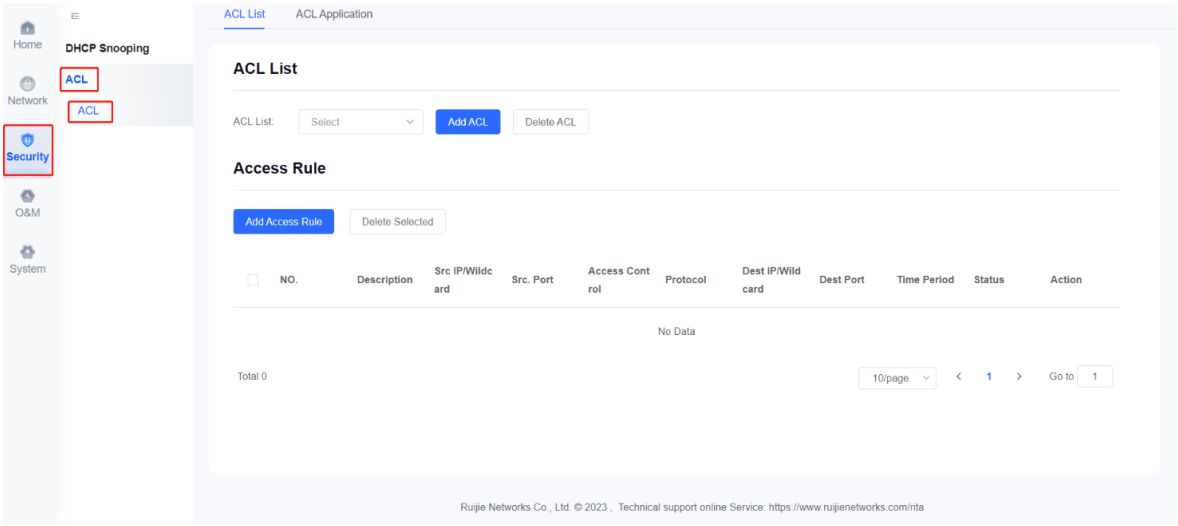
Figure4-138 DHCP Snooping



4.5.2 ACL

Choose **Security** > **ACL** to access the **ACL** page.

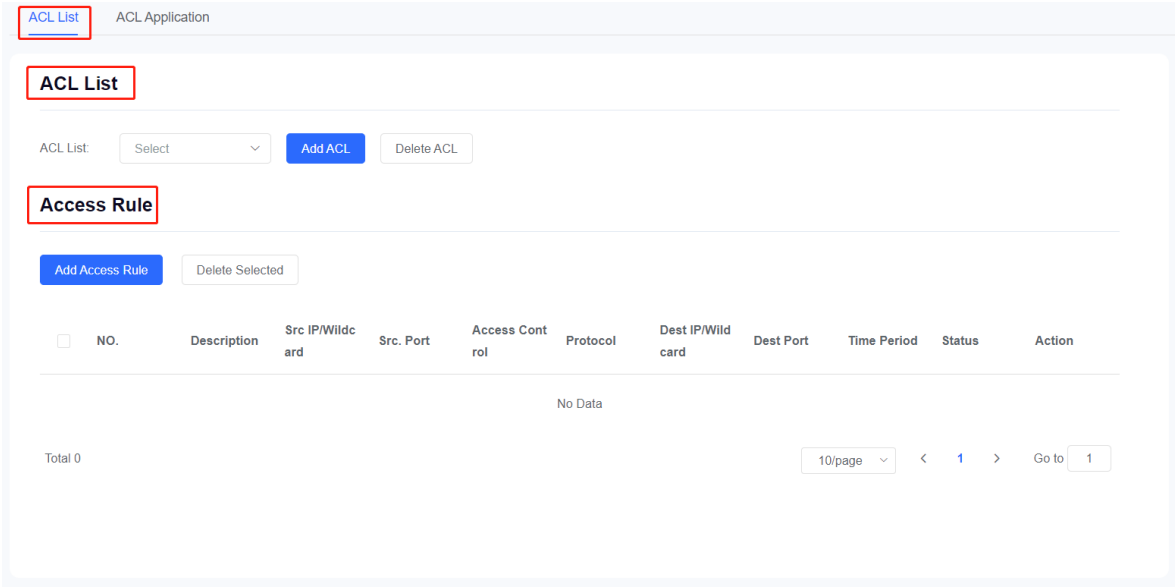
Figure4-139 ACL



1. ACL List

On this page, you can add or delete ACLs, and add, delete, or edit ACEs, as shown in the following figure.

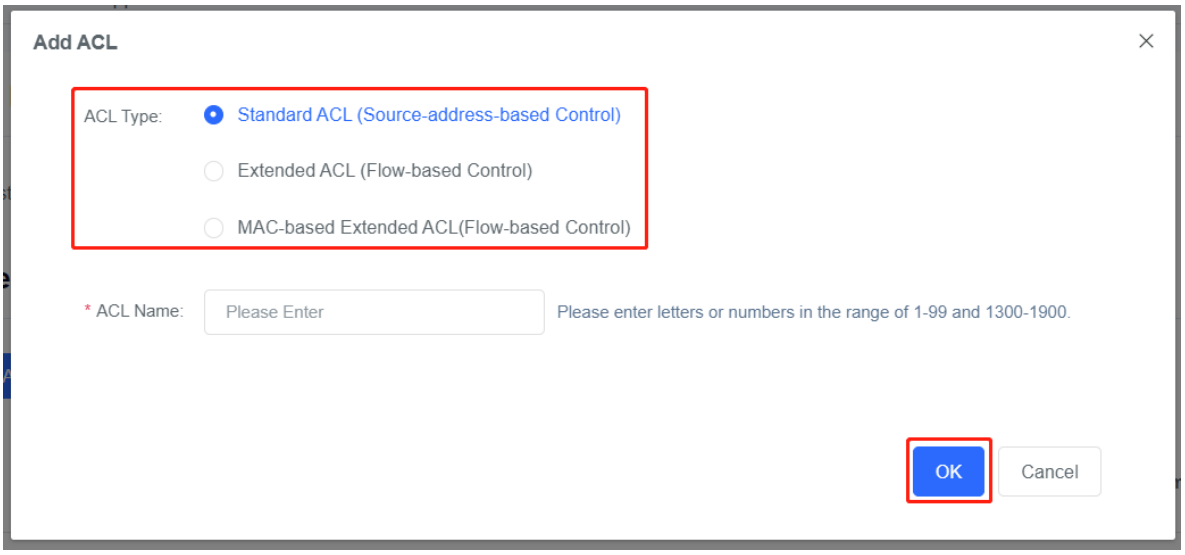
Figure4-140 ACL List



(2) Adding an ACL

Click **Add ACL**. In the pop-up window, set the configuration items. Click **OK** to add an ACE.

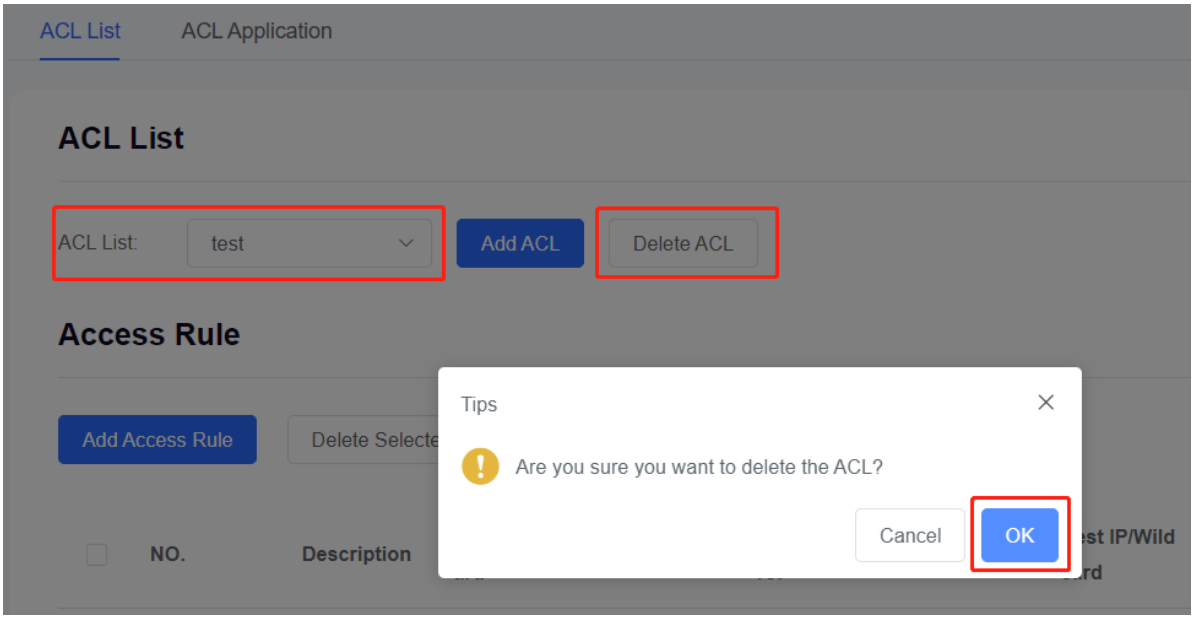
Figure4-141 Adding an ACL



(3) Deleting an ACL

Select an ACL and click **Delete ACL**. On the displayed dialog box, click **OK** to delete the ACL.

Figure4-142 Deleting an ACL



(4) Adding an ACE

Select the ACL list and click **Add Access Rule**. In the pop-up window, set the configuration items. Click **OK** to add an ACE.

Figure4-143 Adding an ACE 1

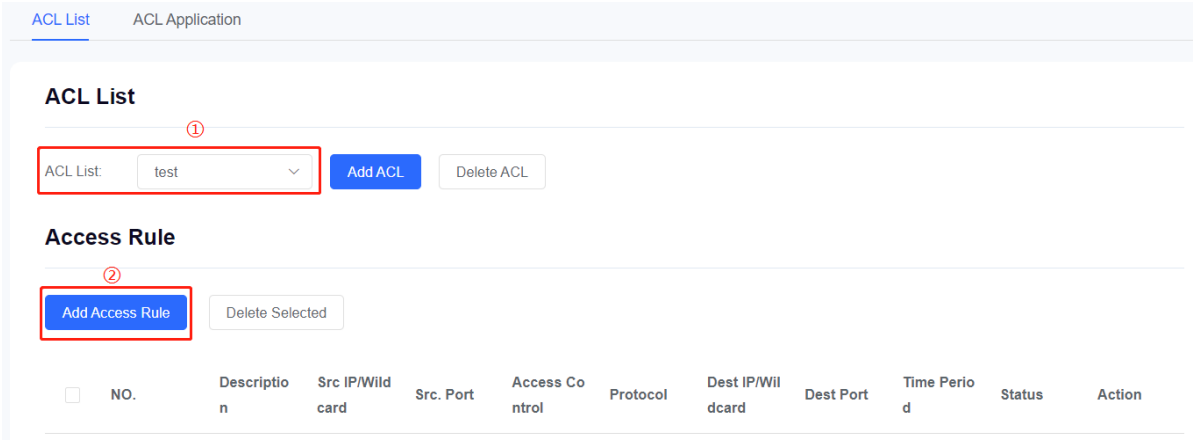
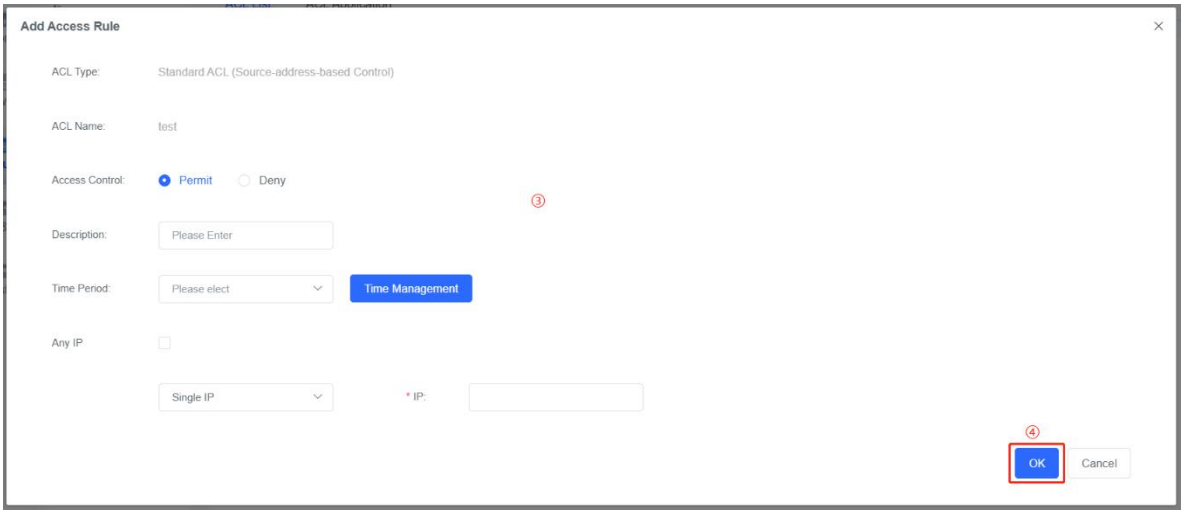


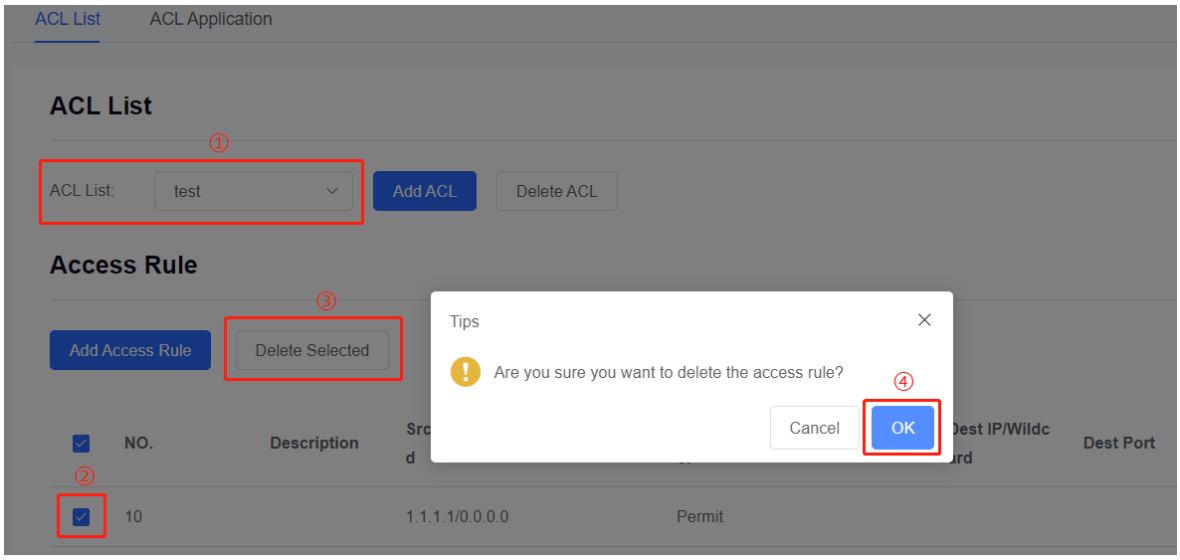
Figure4-144 Adding an ACE 2



(5) Deleting an ACE

Select the ACL and ACE in sequence. Click **Delete Selected**. In the displayed dialog box, click **OK** to delete the ACE.

Figure4-145 Deleting an ACE



- Editing an ACE

  Click **Edit** on the **Action** column. Modify the configuration items in the pop-up window. Click **OK**.

- Moving an ACE

  Click **Move** on the **Action** column. In the displayed dialog box, enter the sequence number of the ACL rule to be moved and click **Move**. After the operation is successful, a message indicating "ACE switching is successful" is displayed. The ACE rule and the selected rule are switched, as shown in the following figure.

Figure4-146 Moving an ACE

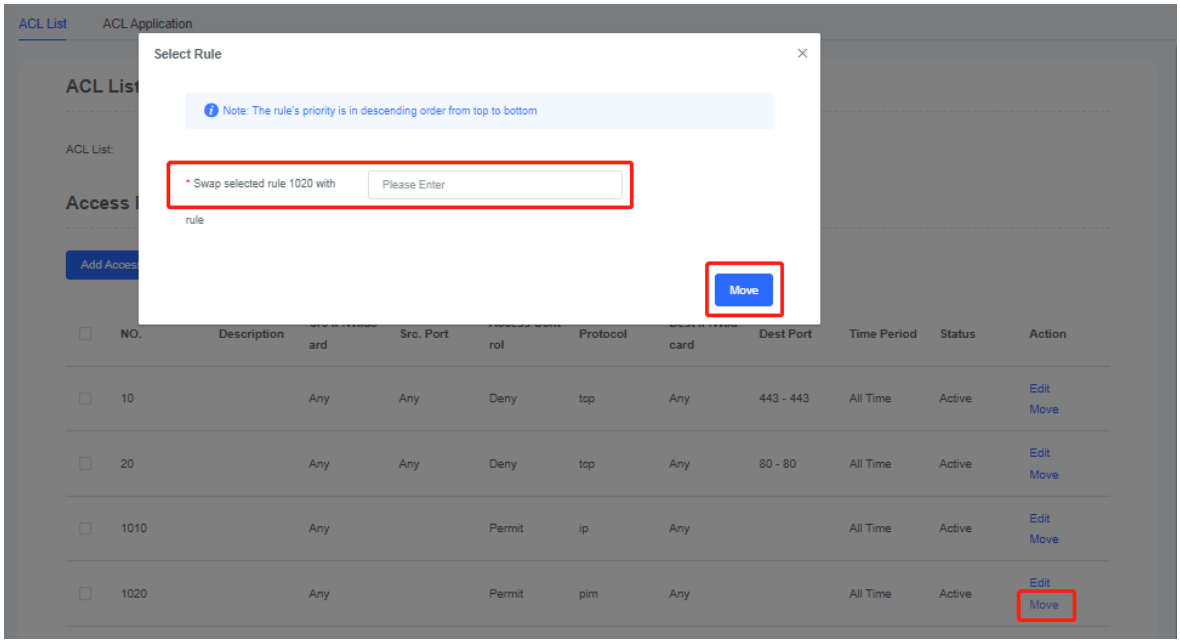


Figure4-147 ACE Rule Before Moving

NO.	Description	Src IP/Wildcard	Src. Port	Access Control	Protocol	Dest IP/Wildcard	Dest Port	Time Period	Status	Action
10		Any	Any	Deny	tcp	Any	443 - 443	All Time	Active	Edit Move
20		Any	Any	Deny	tcp	Any	80 - 80	All Time	Active	Edit Move
1010		Any		Permit	ip	Any		All Time	Active	Edit Move
1020		Any		Permit	pim	Any		All Time	Active	Edit Move
1030		Any	Any	Deny	udp	Any	Any	All Time	Active	Edit Move

Figure4-148 ACE Rule After Moving

NO.	Description	Src IP/Wildcard	Src. Port	Access Control	Protocol	Dest IP/Wildcard	Dest Port	Time Period	Status	Action
10		Any	Any	Deny	tcp	Any	443 - 443	All Time	Active	Edit Move
20		Any	Any	Deny	tcp	Any	80 - 80	All Time	Active	Edit Move
1010		Any		Permit	ip	Any		All Time	Active	Edit Move
1020		Any	Any	Deny	udp	Any	Any	All Time	Active	Edit Move
1030		Any		Permit	pim	Any		All Time	Active	Edit Move

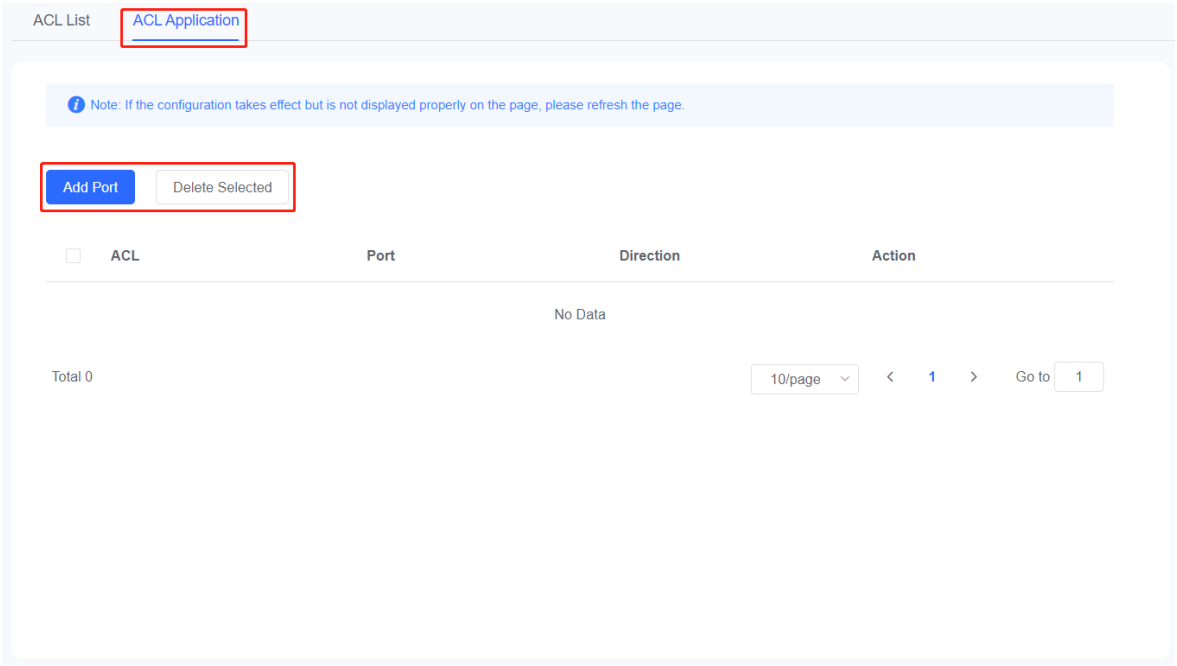
2. ACL Application

Caution

If the configuration takes effect but is not displayed properly on the page, please refresh the page.

On this page, you can add, delete, or edit application ports of an ACL, as shown in the following figure.

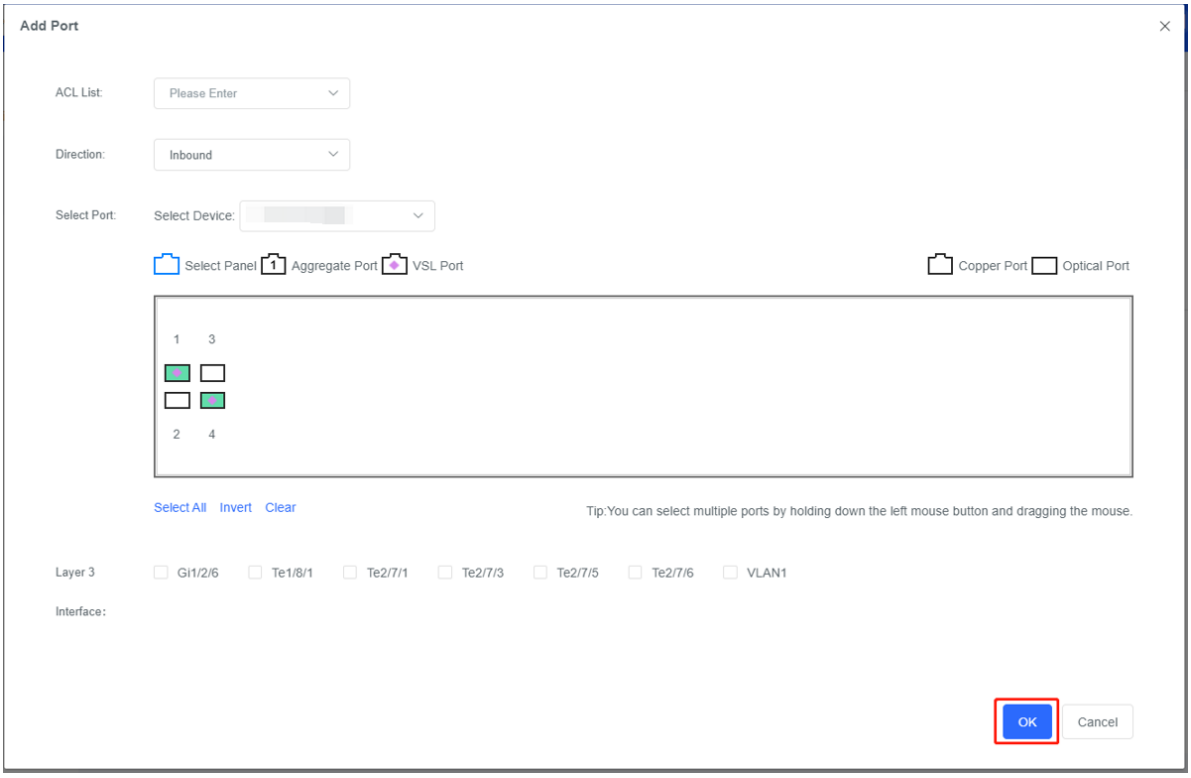
Figure4-149 ACL Application



(2) Adding an ACL Application Port

Click **Add Port**. In the pop-up window, set configuration items. Click **OK** to add an application port of an ACL.

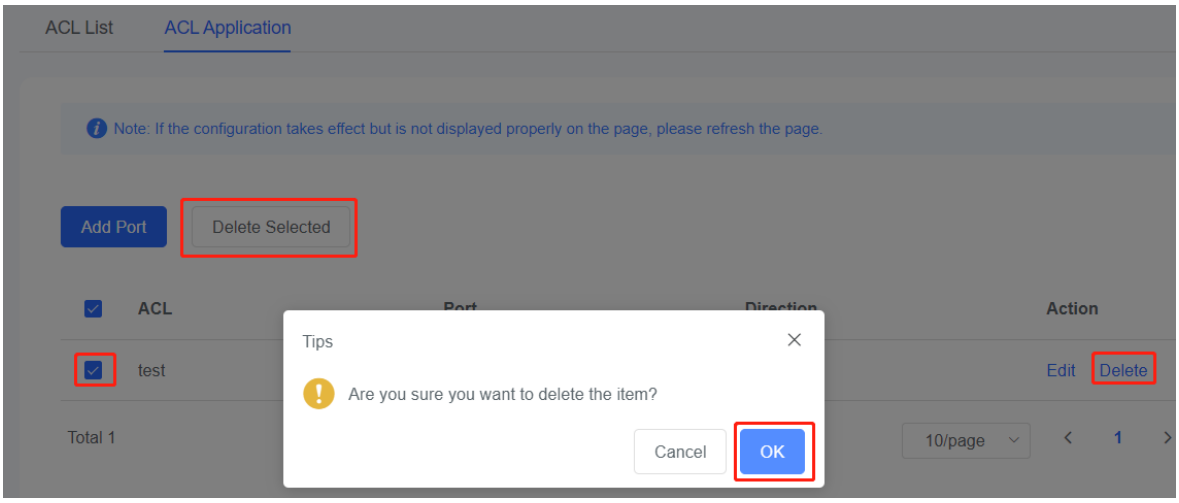
Figure4-150 Adding an ACL Application Port



(3) Deleting an Application Port

You can delete one application port or application ports in batches. Select the application port to be deleted and click **Delete** or **Delete Selected**. On the displayed dialog box, click **OK**.

Figure4-151 Deleting an Application Port



(4) Editing an Application Port

Click **Edit** on the **Action** column. Modify the configuration items in the pop-up window. Click **OK**.

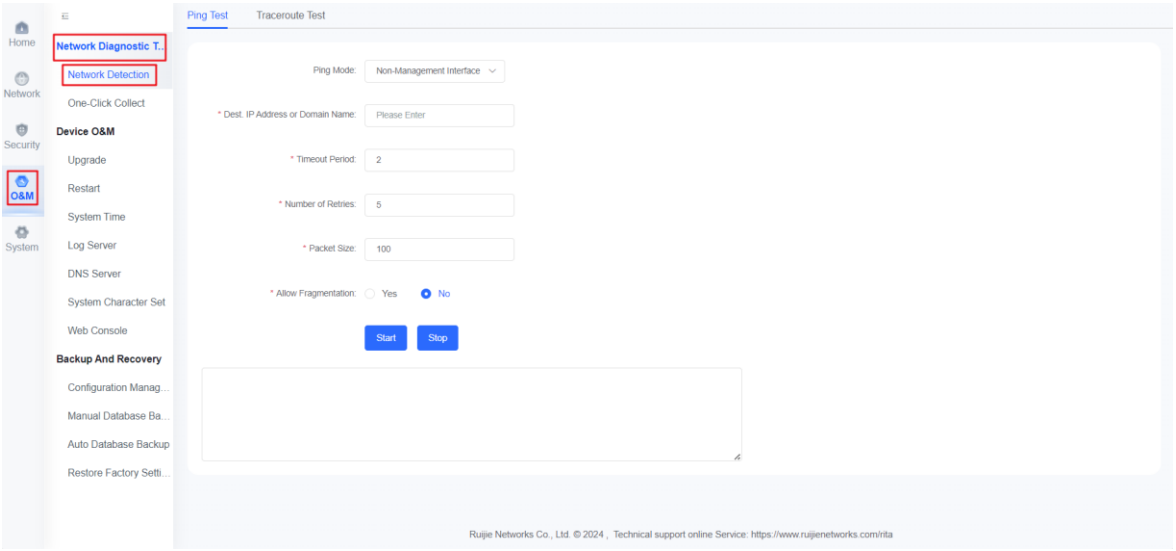
4.6 O&M

4.6.1 Network Diagnostic Tools

1. Network Detection

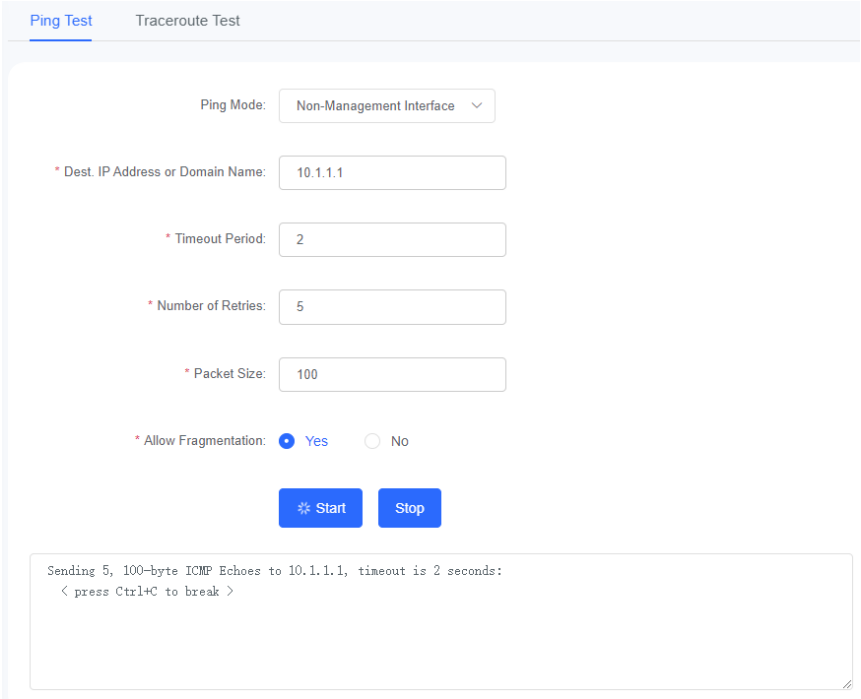
(1) Choose **O&M** > **Network Diagnostic Tools** > **Network Detection** to access the Network Detection page.

Figure4-152 Network Detection



(2) Ping Test

Figure4-153 Ping Test



- **Start**: Select **Non-Management Interface** from the **Ping Mode** drop-down list box to select the ping mode. You can select **Non-Management Interface** and **Management Interface**. Enter the destination IP address or domain name, timeout period, number of attempts, and packet size. After setting configuration parameters, click **Start** to run the ping test. After the ping test is complete, the test results will be displayed.

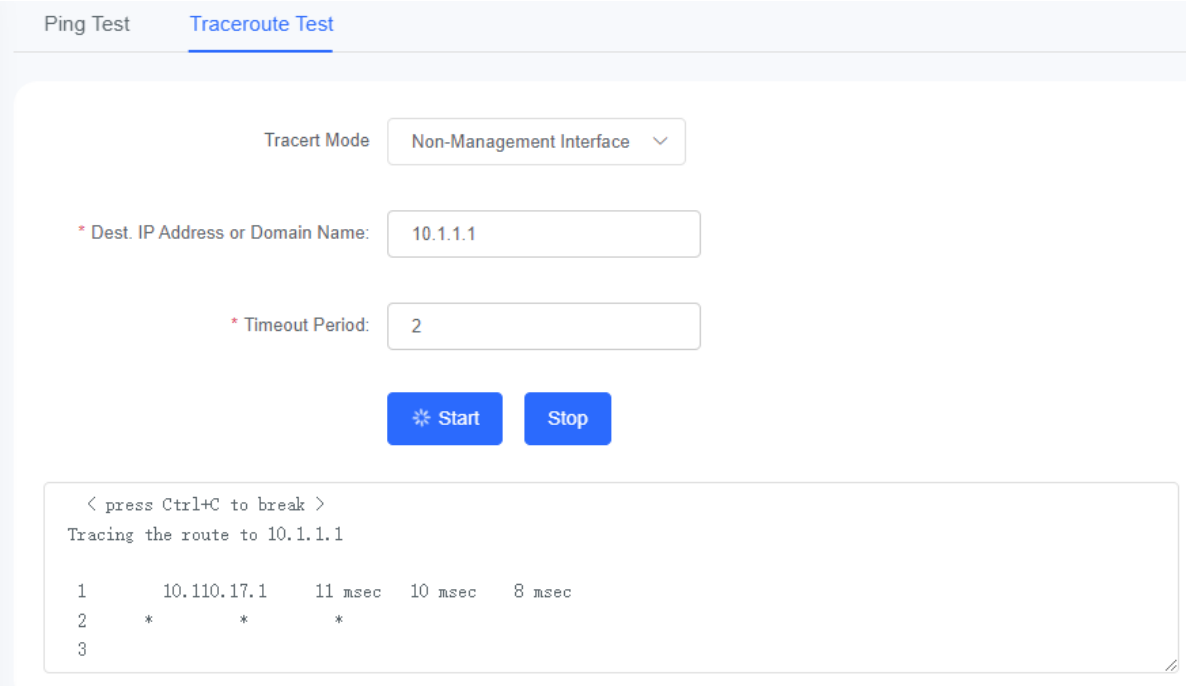
Note

The Allow Fragmentation item is displayed only when Ping Mode is set to Non-Management Interface.

- **Stop**: Click **Stop** to stop the current ping test.

(3) Trace route Test

Figure4-154 Trace route Test



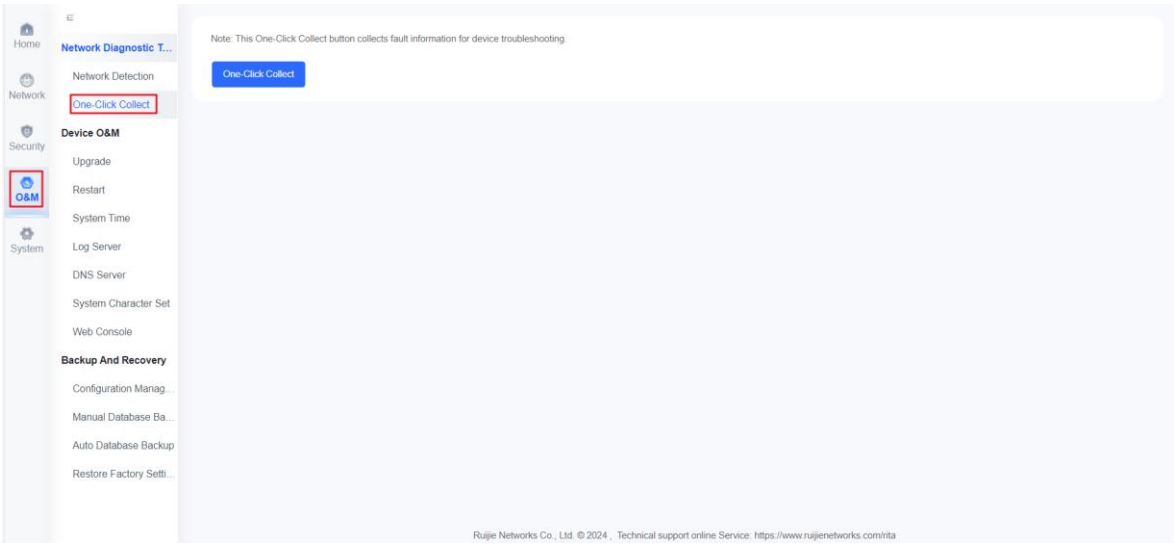
- **Start**: Select **Non-Management Interface** from the **Tracert Mode** drop-down list box to select the tracert mode. You can select **Non-Management Interface** and **Management Interface**. Enter the destination IP address or domain name and timeout period. Click **Start** to run the tracert test. After the tracert test is complete, the test results will be displayed.
- **Stop**: Click **Stop** to stop the current tracert test.

2. One-Click Collect

Choose **O&M** > **Network Diagnostic Tools** > **One-Click Collect** to access the One-Click Collect page.

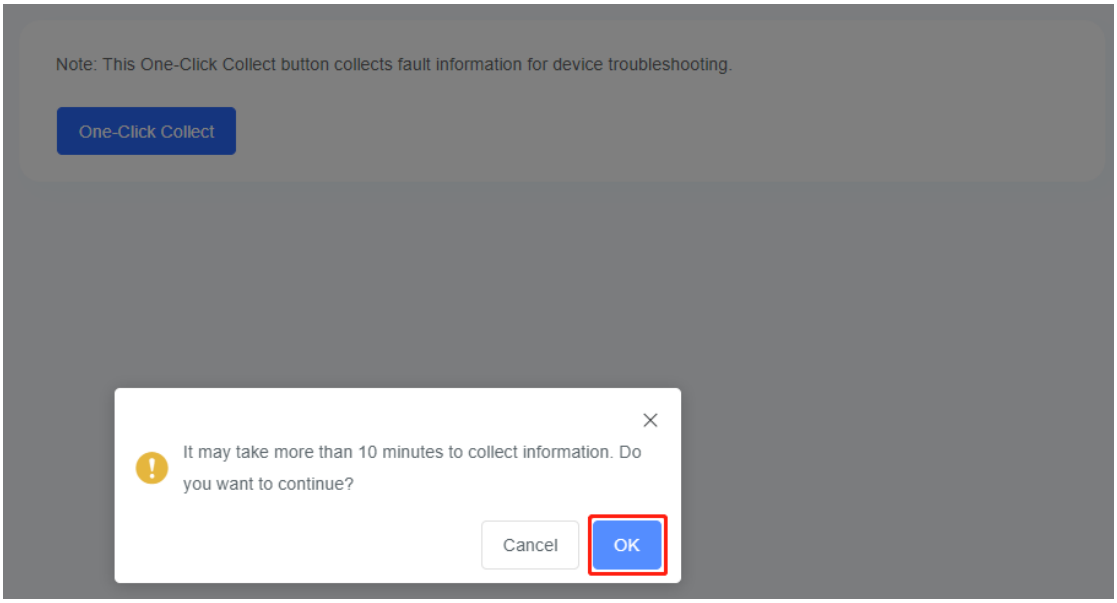
You can use the **One-Click Collect** function to collect switch fault information for troubleshooting.

Figure4-155 One-Click Collect



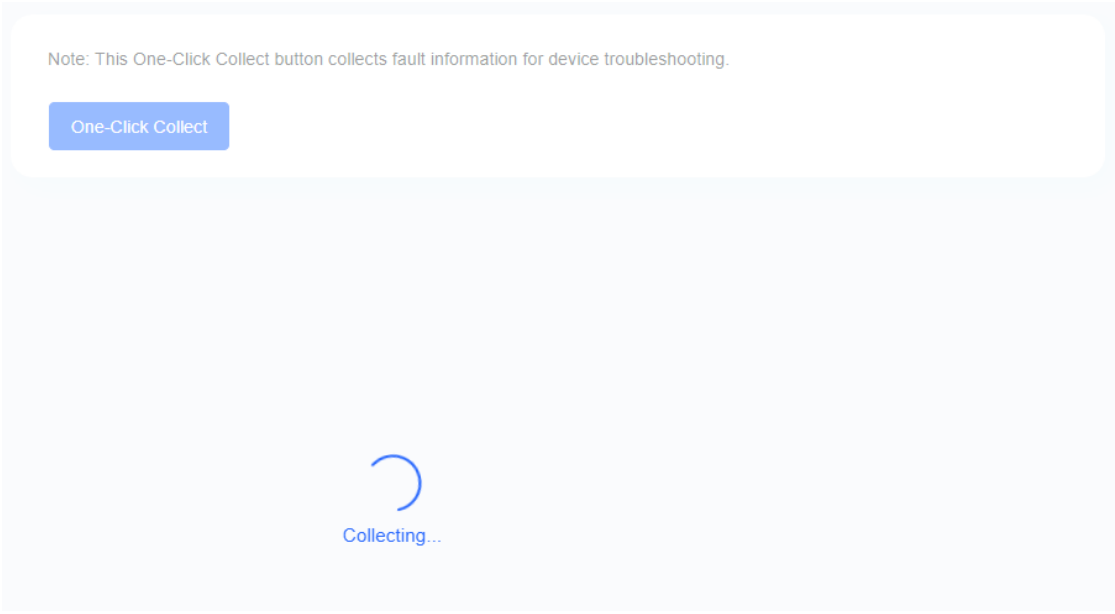
Collecting fault information may take about 10 minutes. After the collection is complete, you can download the collected fault information to a file named **tech_ vsd0_ 20210716142650.tar.gz**. Click **One-Click Collect**. The **Notice** dialog box is displayed.

Figure4-156 One-Click Collect 1



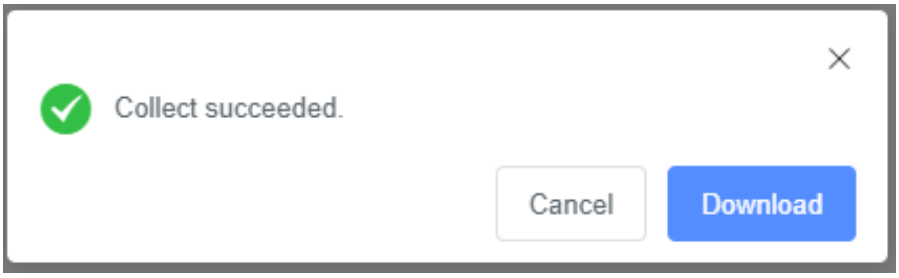
Click **OK**. The collecting process starts.

Figure4-157 One-Click Collect 2



After the collection process is complete, the **Notice** dialog box is displayed. Click **Download** to download the collected information in a **tar.gz** compressed file.

Figure4-158 One-Click Collect 3

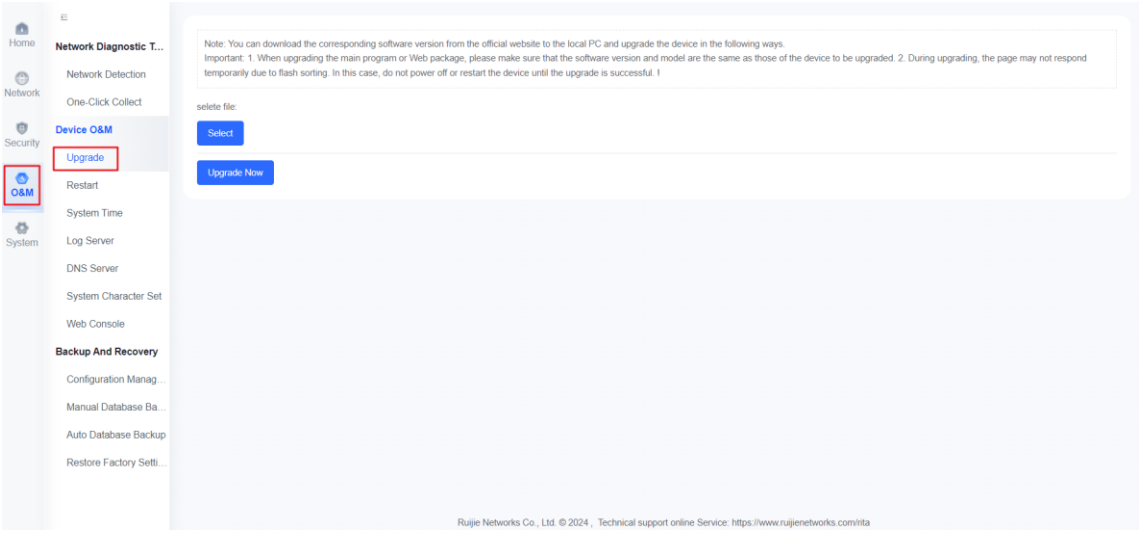


4.6.2 Device O&M

1. Upgrade

Choose **O&M** > **Device O&M** > **Upgrade** to access the Upgrade page.

Figure4-159 Upgrade



Note

You can download the required software version file from Ruijie Networks' official website to the local PC and upgrade the switch using the downloaded file.

Caution

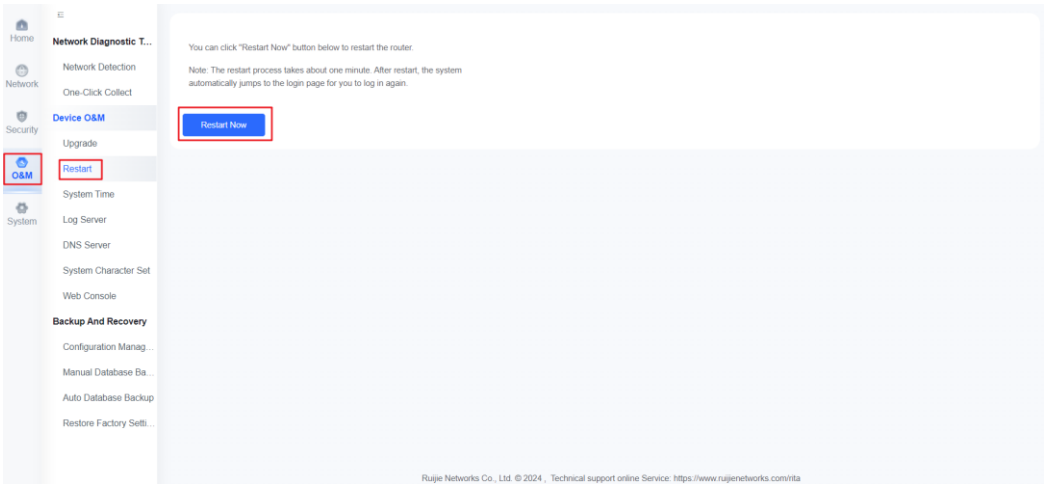
- When upgrading the main program or the web package, ensure that the version and model are the same as those of the current switch.
- During upgrading, there may be no response temporarily due to flash loading. In this case, do not power off or restart the switch until the upgrade is successful.

2. Restart

Choose **O&M** > **Device O&M** > **Restart** to access the **Restart** page.

- Click **Restart Now** to restart a switch.
- The restart process takes about 1 minute. Do not perform any operation during this period.
- After the switch is successfully restarted, the current page will be refreshed automatically.

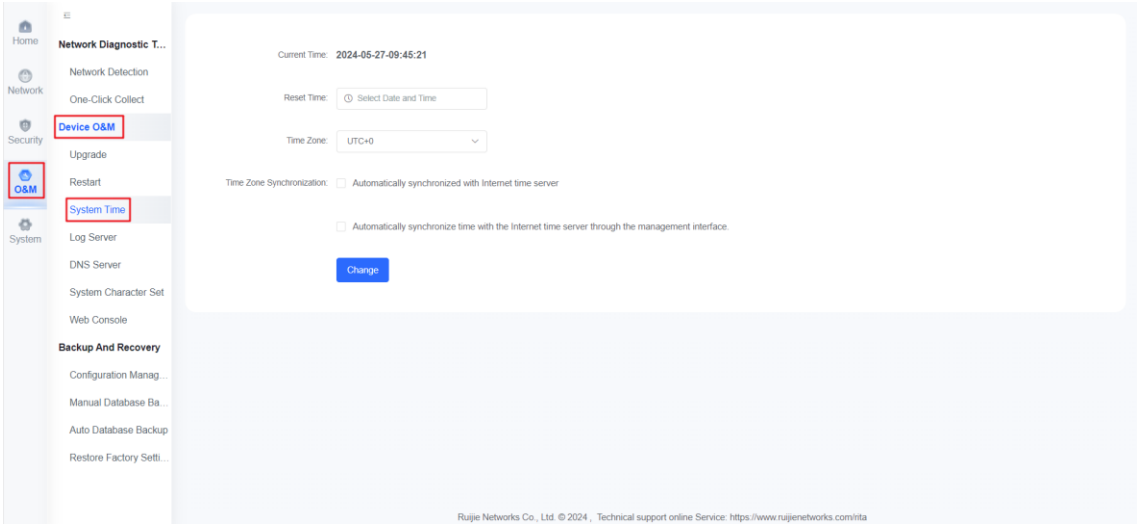
Figure4-160 Restart



3. System Time

Choose **O&M** > **Device O&M** > **System Time** to access the **System Time** page.

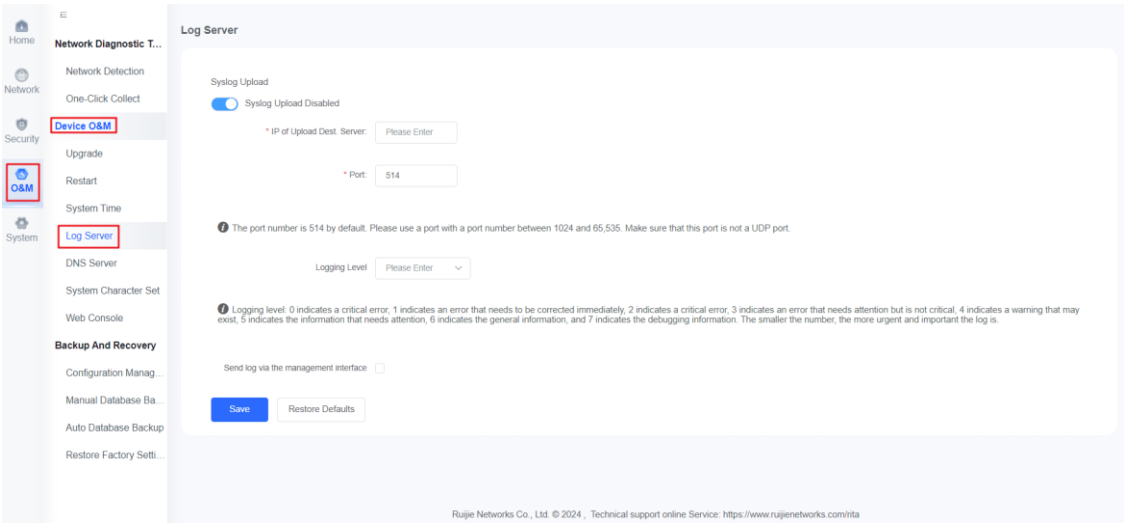
Figure4-161 System Time



4. Log Server

Choose **O&M** > **Device O&M** > **Log Server** to access the **Log Server** page. Click **Syslog Upload** to enable or disable the syslog upload function.

Figure4-162 Log Server

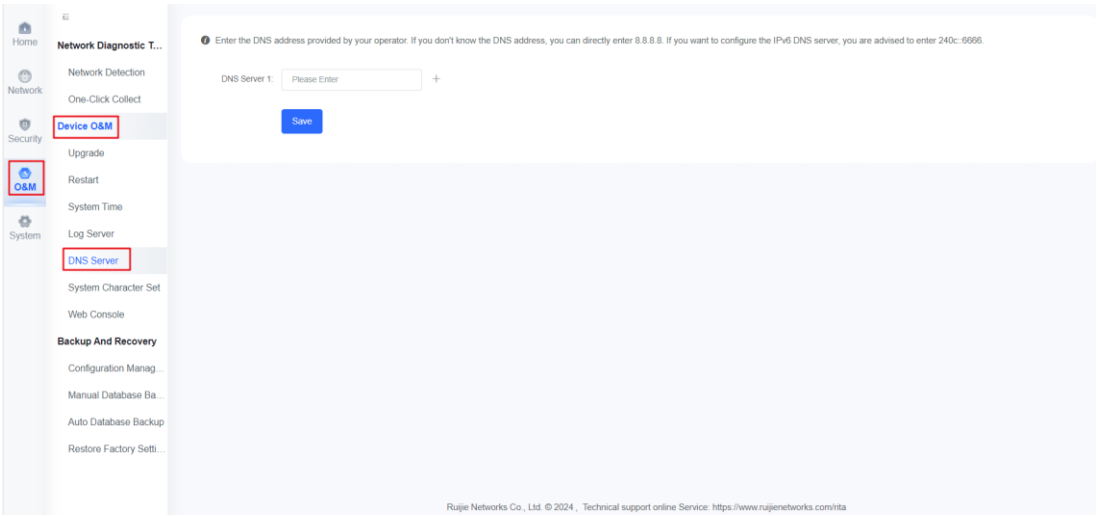


5. DNS Server

Choose **O&M** > **Device O&M** > **DNS Server** to access the **DNS Server** page.

- Click **+** to add a DNS server.
- Click **x** to delete a DNS server.
- Click **Save** to submit the configuration.

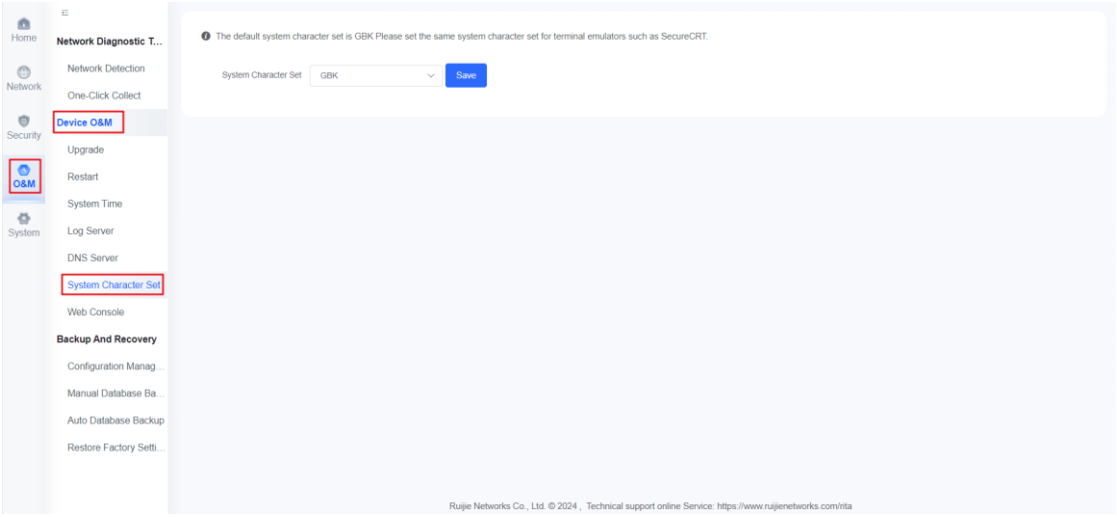
Figure4-163 DNS Server



6. System Character Set

Choose **O&M** > **Device O&M** > **System Character Set** to access the **System Character Set** page.

Figure4-164 System Character Set

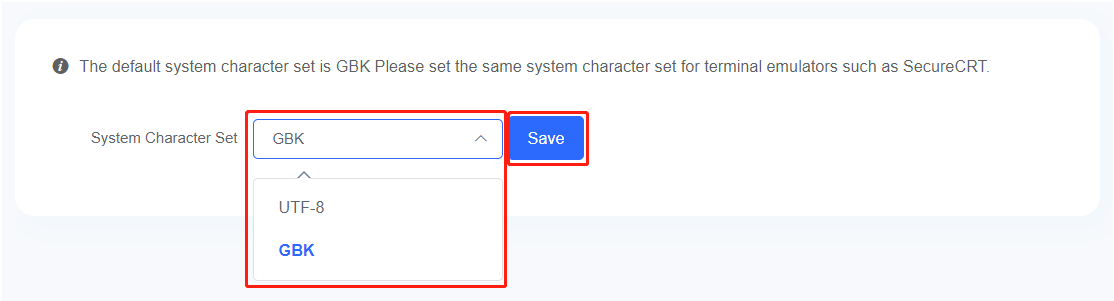


There are two options in the **System Character** Set drop-down list box, which are **UTF-8** and **GBK**. After a character set is selected, click **Save** to save the configuration.

Note

The default value is **UTF-8**.

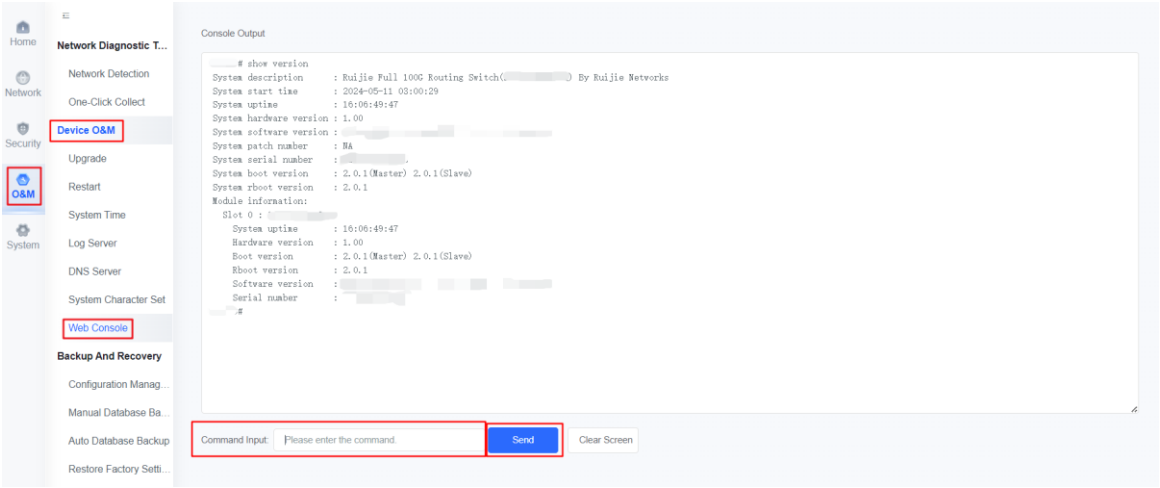
Figure4-165 Setting System Character



7. Web Console

Choose **O&M** > **Device O&M** > **Web Console** to access the **Web Console** page.

Figure4-166 Web Console



(1) Enter a command in **Command Input** box and click **Send**. The command execution result will be displayed in the console.

(2) Click **Clear Screen** to clear the output result.

4.6.3 Backup and Recovery

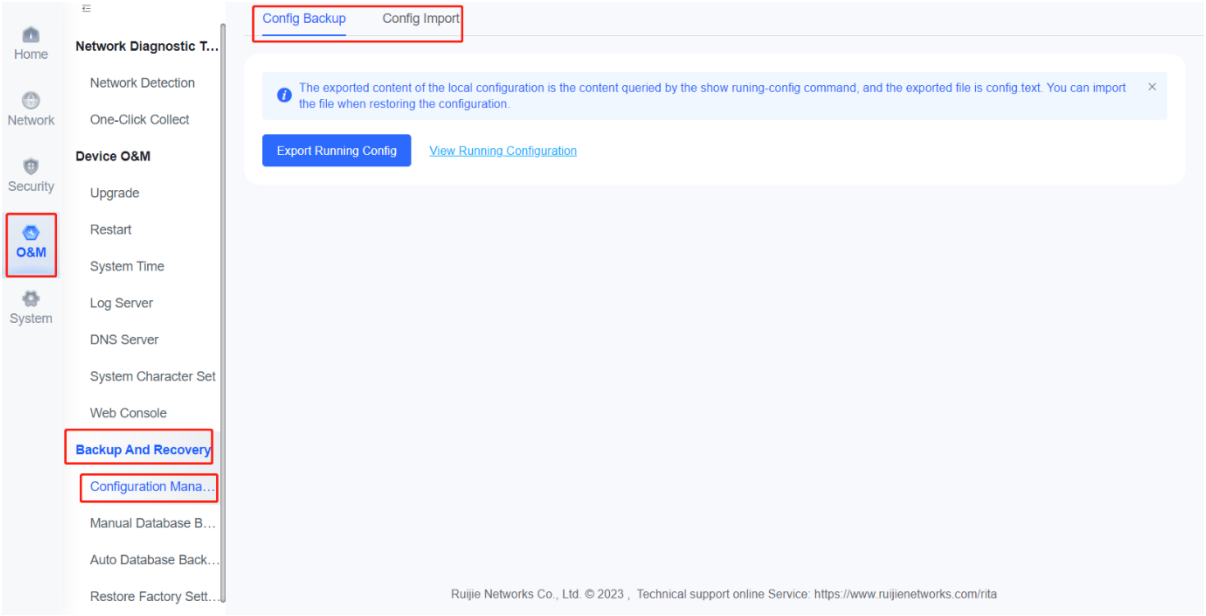
1. Configuration Management

Choose **O&M** > **Backup And Recovery** > **Configuration Management**. On this page, you can perform local configuration backup and local configuration import. The local configuration backup and import functions are used to restore local configurations and implement fast local configuration.

Caution

- The exported configuration of the local device is the local device configuration, which is the **show running-config** command output. The exported file is **config.text.** You can import this file to restore the configuration.
- You can import the **config.text** file to the device on the **Config Import** page. After the configuration file is imported, the device restarts and the configuration takes effect. Do not close or refresh the page during the import. Otherwise, the import may fail.

Figure4-167 Configuration Management



(2) Config Backup

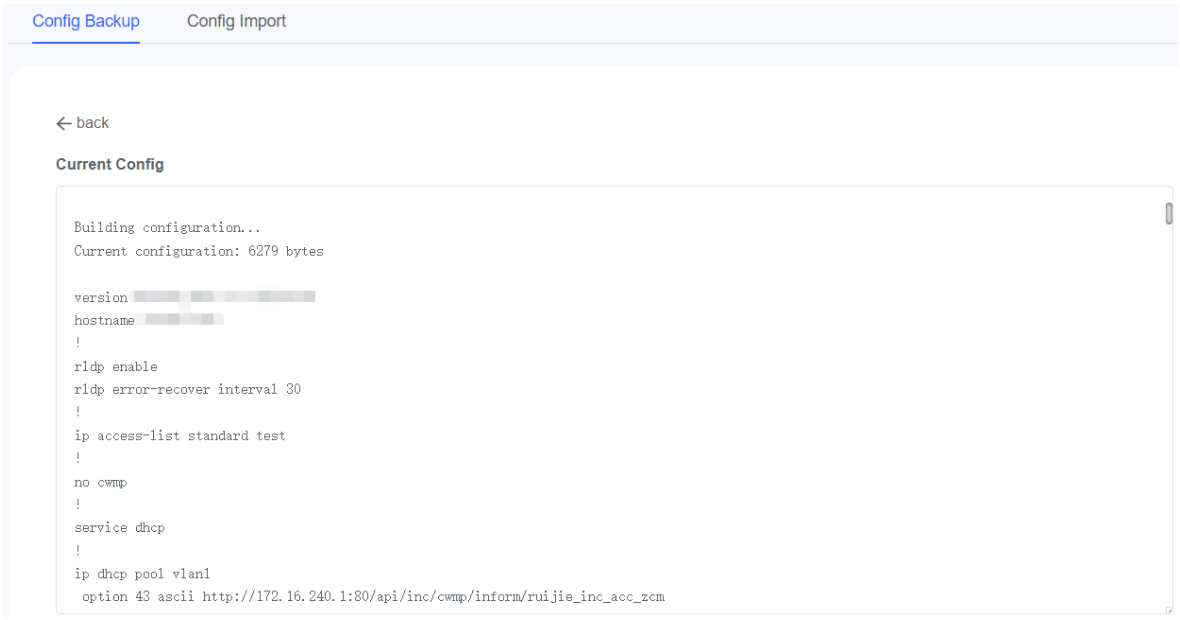
You can import or view the current configuration. The current configuration refers to **show running-config** command output.

Figure4-168 Config Backup page



- Export running configuration: Click **Export Running Config** to generate the **config.text** text file.
- View running configuration: Click **View Running Configuration** to access the current configuration page.

Figure4-169 Configuring Backup



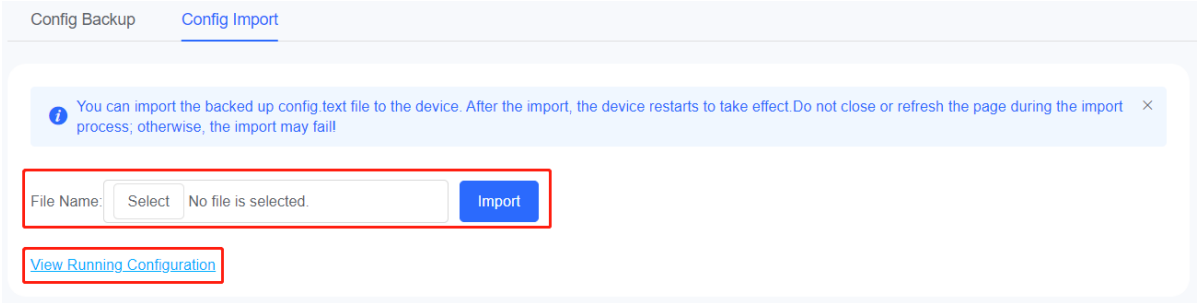
(3) Config Import

On the **Config Import** page, you can import configurations or view the current configuration. You can import an existing configuration file to the device for configuration restoration or fast configuration.

Caution

After the configuration is imported, the device restarts and the configuration takes effect. Do not close or refresh the page during the import. Otherwise, the import may fail.

Figure4-170 Configuring Import



- **Import**: click **Import**. Select the desired file and click **Import** to import the configuration file.
- **View running configuration**: Click **View Running Configuration** to access the current configuration page.

2. Manual Database Backup

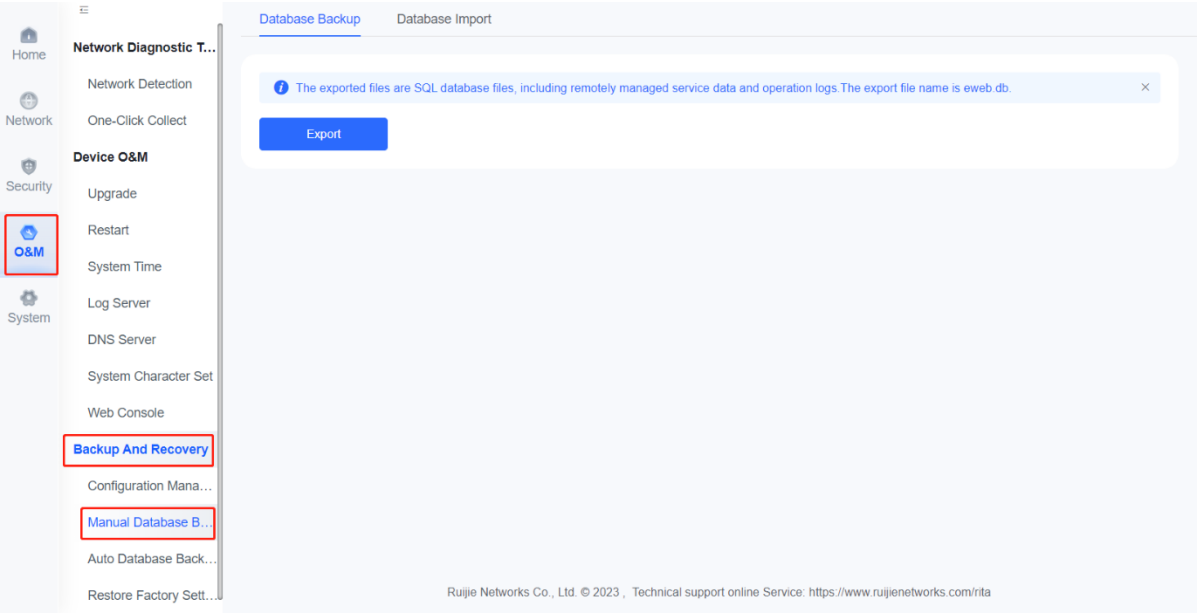
Choose **O&M** > **Backup And Recovery** > **Manual Database Backup**. On this page, you can perform database backup and database import operations. The database backup and import functions are usually used before and

after an upgrade. If the device upgrade fails, you can roll back the device to the previous version to import the data.

Caution

- The exported file is an **SQL database** file, which contains service data and operation logs for remote management. The exported file name is **eweb.db**.
- You can import the **eweb.db** file on the **Manual Database Backup** page. After the file is imported, the configuration takes effect after the web service is restarted. Do not close or refresh the page during the import. Otherwise, the import may fail.

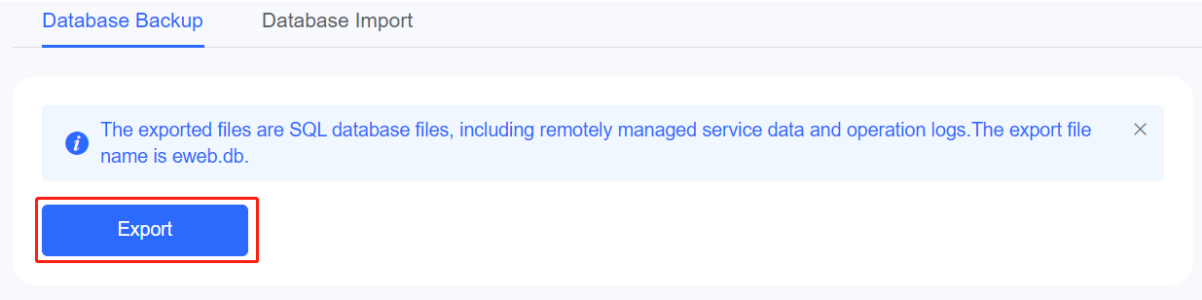
Figure4-171 Manual Database Backup



(2) Database Backup

Click **Export** to download the database file with the file name extension of **db**. The SQL database file contains service data and operation logs for remote management.

Figure4-172 Database Backup



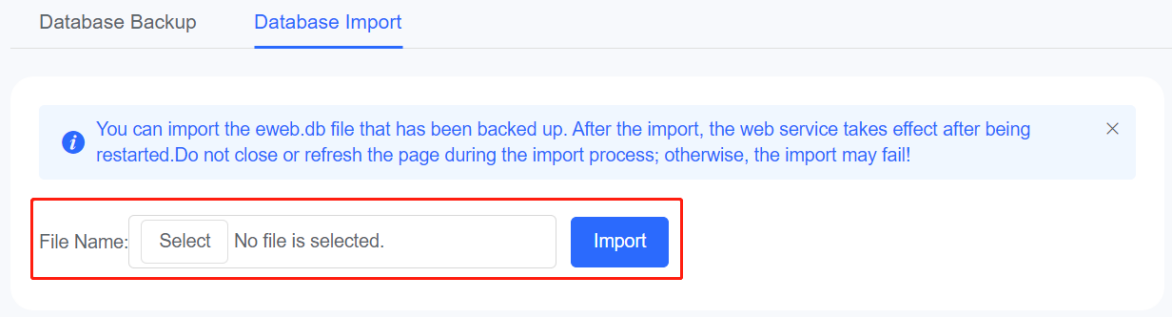
(3) Database Import

The file extension of the imported database file must be **db**.

Caution

- The imported version cannot be higher than the current database version.
- After the database file is imported, the configuration takes effect after the web service is restarted. Do not close or refresh the page during the import. Otherwise, the import may fail.

Figure4-173 Database Import



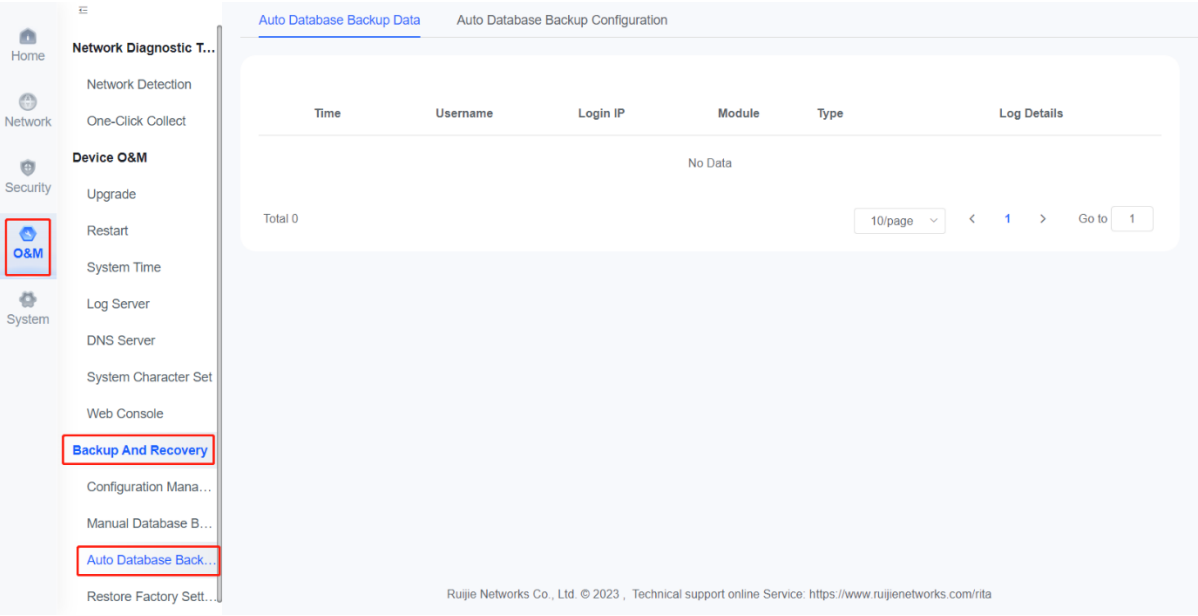
3. Auto Database Backup

Specification

This function is not supported in this version, so no configuration is required for this function.

(1) Choose **O&M** > **Backup And Recovery** > **Auto Database Backup**. You can view the automatic database backup data and enable automatic database backup configuration on this page.

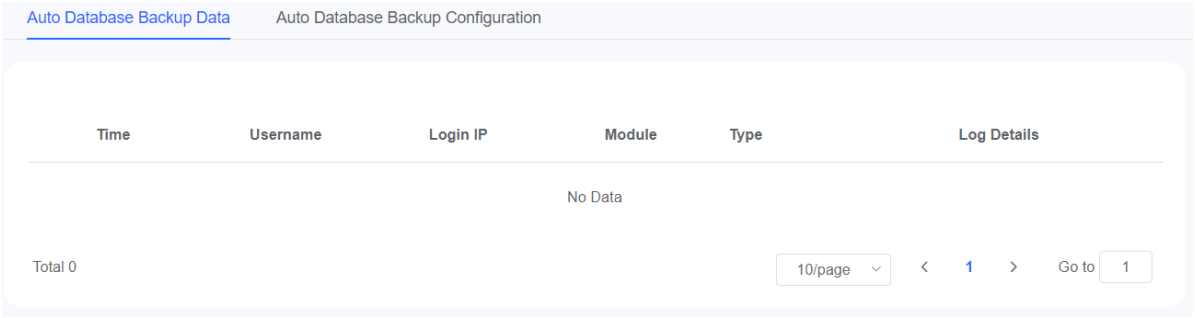
Figure4-174 Auto Database Backup



(2) Auto Database Backup Data

This page displays historical data of automatic database backup, as shown in the following figure.

Figure4-175 Auto Database Backup Data



(3) Auto Database Backup Configuration

The automatic database backup configuration function can automatically store system configuration data for disaster recovery and configuration rollback. As shown in the following figure, you can enable/disable the automatic database backup function and configure automatic database backup on this page.

a. Click **Enable** to access the **Auto Database Backup Configuration** page.

b. To enable the automatic backup function, you need to provide the SSH credential of the SFTP server, and configure the automatic backup path, frequency, and time, as shown in the following figure.

c. After the required parameters are configured, click **Save**. The automatic database backup function is enabled.

Caution

The SQL database files backed up here contain service data and operation logs for remote management.

Figure4-176 Auto Database Backup Configuration 1

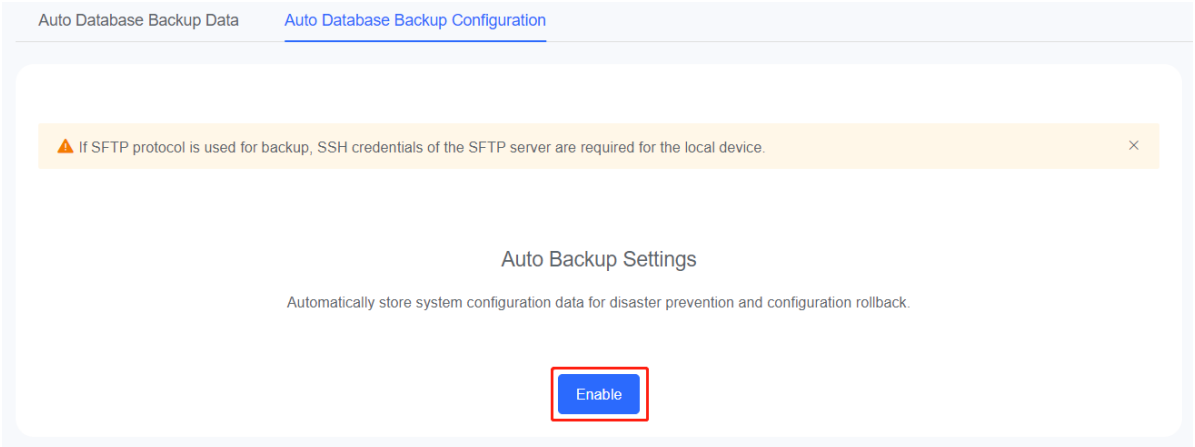
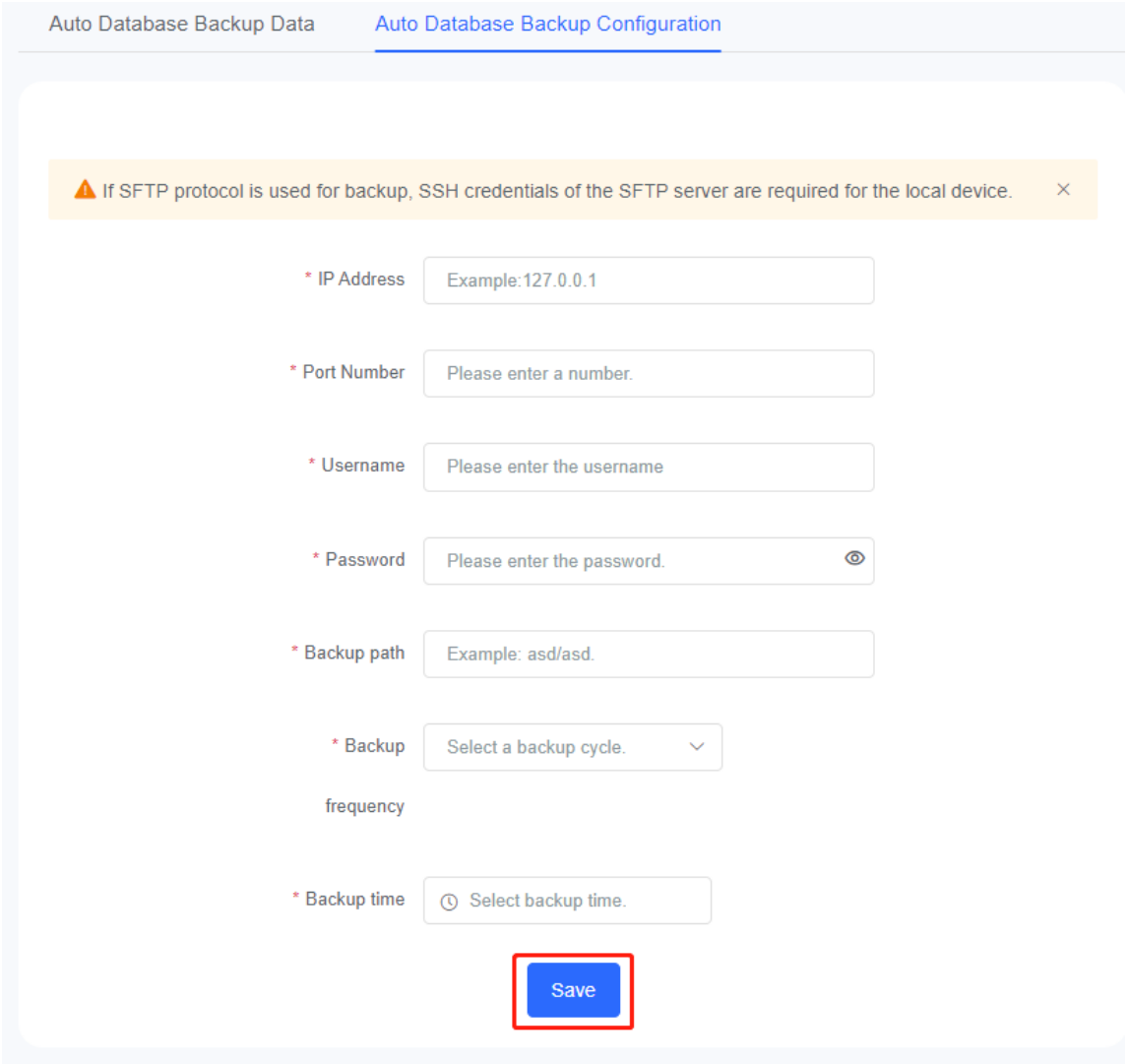


Figure4-177 Auto Database Backup Configuration 2

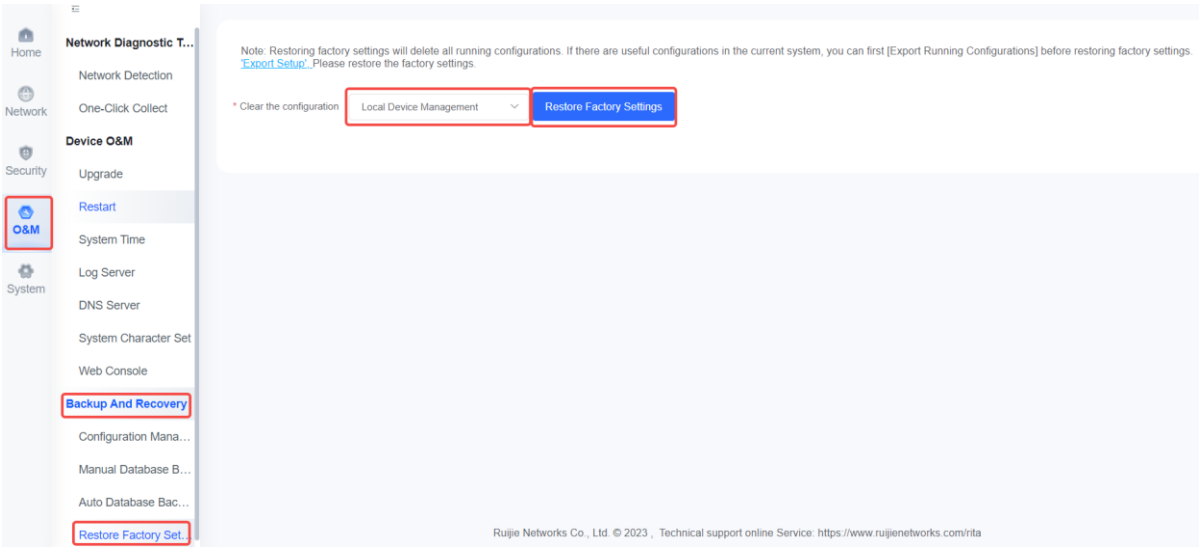


4. Restore Factory Settings

Choose **O&M** > **Device O&M** > **Restore Factory Settings** to access the **Restore Factory Settings** page.

To save the current configuration, you are advised to export the current configuration by clicking **Export Setup**.

Figure4-178 Restore Factory Settings



Caution

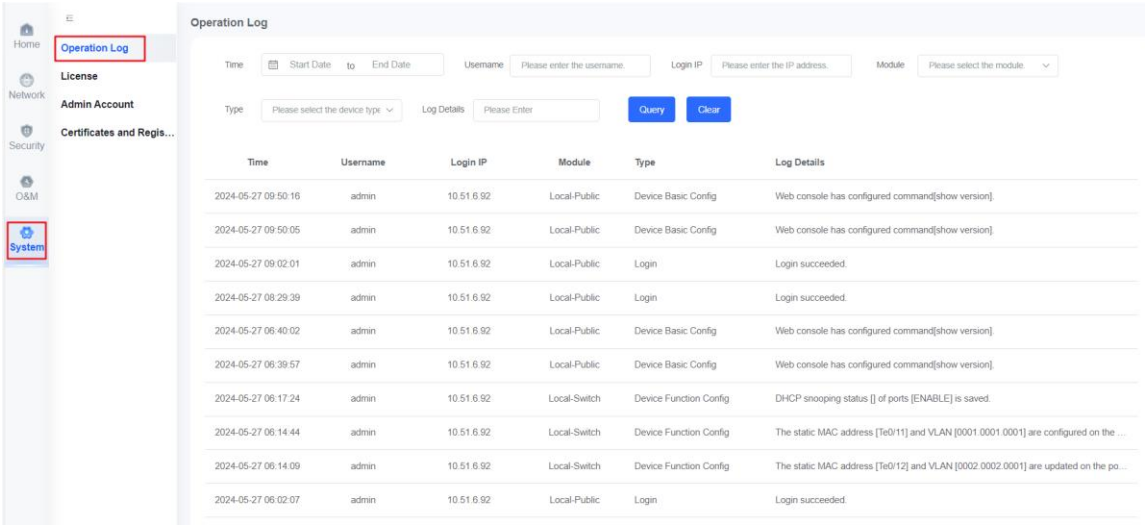
Restoring factory settings will delete all running configurations. If there are useful configurations in the current system, you can first export running configurations before restoring factory settings. Click **Export Setup** to export the running configuration before restoring the factory settings.

4.7 System

4.7.1 Operation Log

Choose **System** > **Operation Log** to access the Operation Log **page**. The operation log records users' key operations. You can query the operation log based on the search criteria.

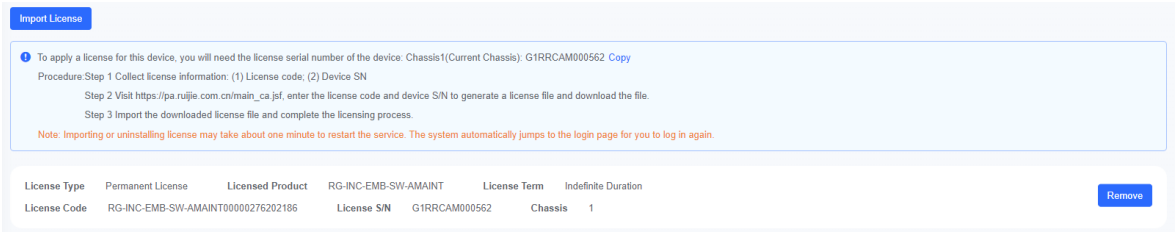
Figure4-179 Operation Log



4.7.2 Licensing Procedure

You will be given a license code after purchasing a license. You must obtain the device SN on the switch by choosing **System** > **License**.

Figure4-180 License



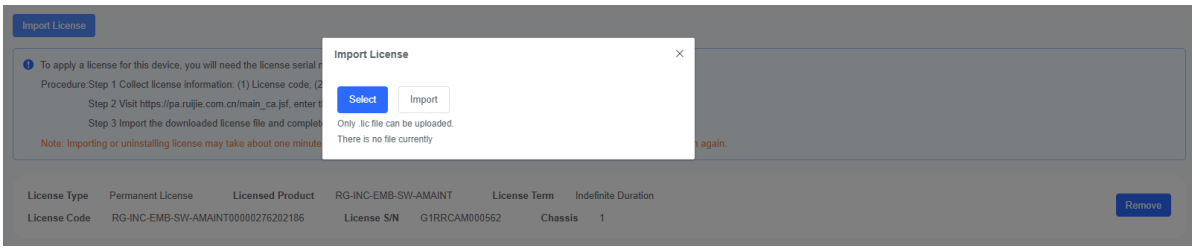
(1) Import License

a. Collect license information including License code (indicated on the license) and device SN.

b. Visit **https://pa.ruijie.com.cn/main_ca.jsf** (Ruijie Networks' PA system), and enter the license code and switch SN on the PA system to generate a license file. Enter the license SN and license code, and click **Finish** to download the license file.

c. Choose **System** > **License**, and click **Import License**. Click **Select** and select the downloaded license file with the suffix *.lic from your local PC. Click **Import**.

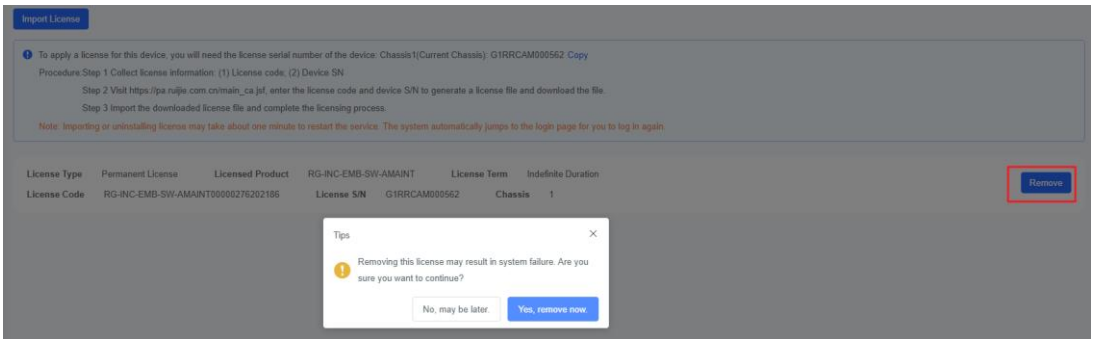
Figure4-181 Import License



(2) Uninstalling a License

You can view or remove the imported license on the **License** page in the eWeb management system. You can view or remove other licenses in addition to the INC-EMB licenses on the **License** page.

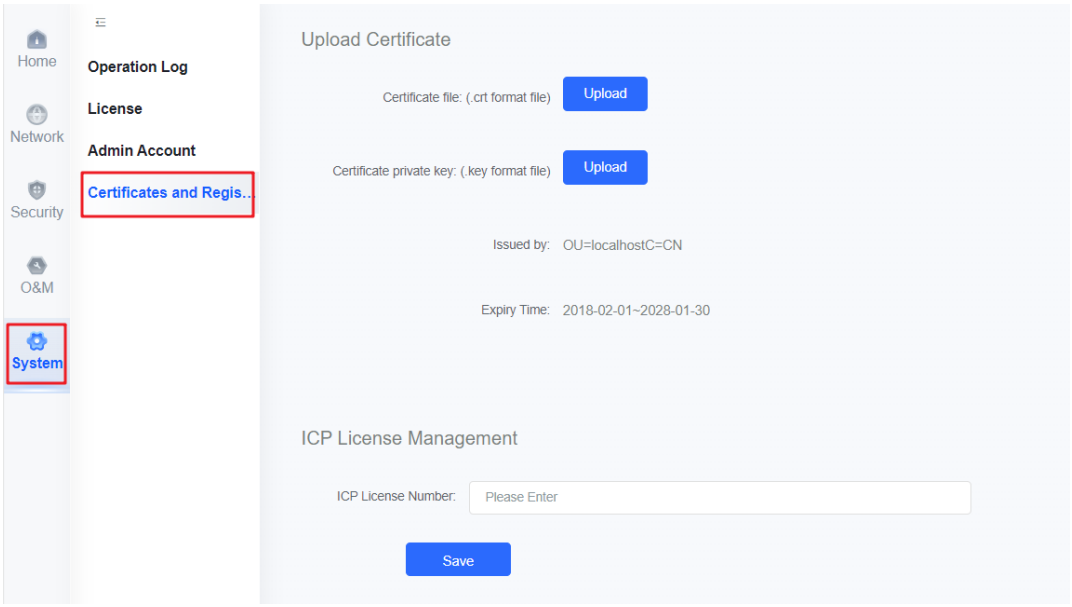
Figure4-182 Uninstalling a License



4.7.3 Certificates and Registration

Choose **System** > **Certificates and Registration** to access the **Certificates and Registration** page. You can upload certificate file and certificate private key or manage the ICP license in this page.

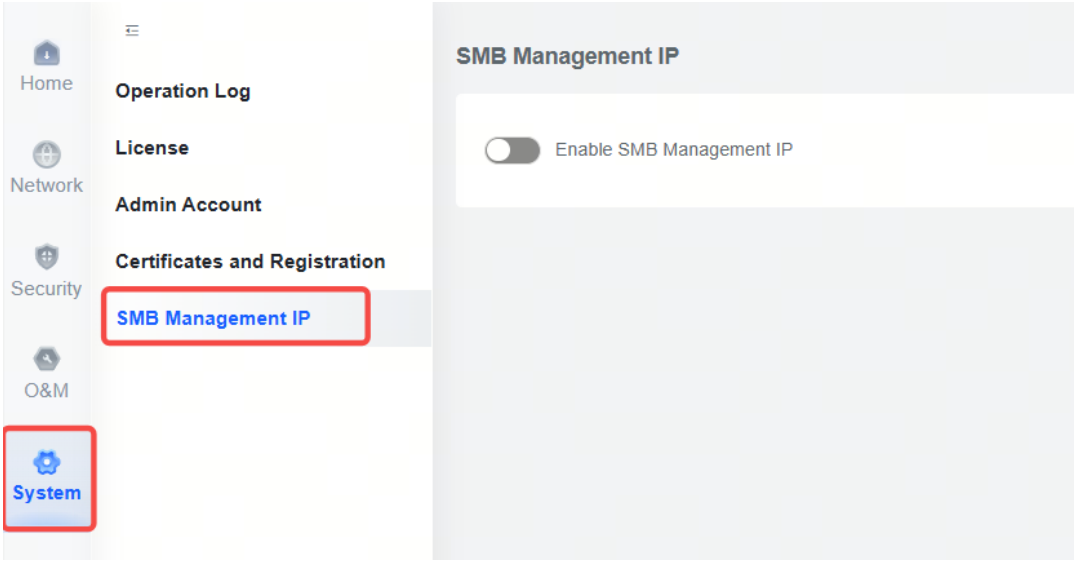
Figure4-183 Certificates and Registration



4.7.4 SMB SON Management

Choose **System** > **SMB Management IP** to access the **SMB Management IP** page.

Figure4-184 SMB Management IP



Toggle on **Enable SMB Management IP**, click **Management IP**, select an SVI in the **SVI** drop-down list box, and click **Save**. You can only select an SVI in Up state. Then SMB SON management is configured successfully.

Figure4-185 Enable SMB Management IP

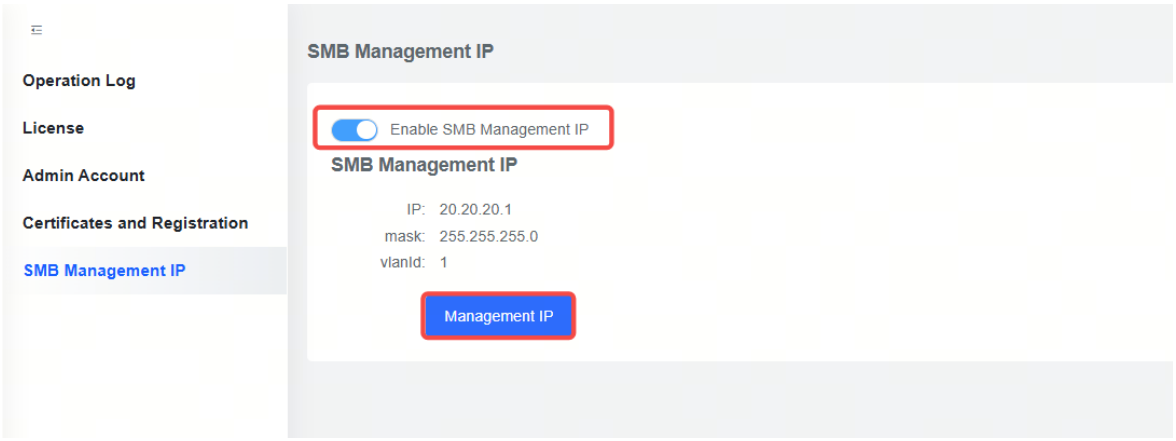


Figure4-186 Configuration Management IP

