Ruijie RG-CS83 Series Switches CS83_RGOS 12.6(3)B1403

Web-based Configuration Guide

Document Version: V1.1
Date: 2023-12-20
Copyright © 2023 Ruijie Networks

Copyright

Copyright © 2023 Ruijie Networks

All rights are reserved in this document and this statement.

Any reproduction, excerption, backup, modification, transmission, translation or commercial use of this document or any portion of this document, in any form or by any means, without the prior written consent of Ruijie Networks is prohibited.

Trademark  and  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 you purchase are subject to commercial contracts and terms. Some or all of the products, services or features described in this document may not be within the scope of your purchase or use. Unless otherwise agreed in the contract, Ruijie Networks does not make any express or implied statement or guarantee for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Ruijie Networks reserves the right to modify the content of the document without any notice or prompt.

This manual is for reference only. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Preface

Intended Audience

This document is intended for:

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

Technical Support

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

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.

1 Overview

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

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

The default username and password are both **admin**.

Before logging into the web for the first time, please use an RJ45 cable to connect the PC and the LAN port of the device, and configure the PC's IP address to be in the same network segment as the default IP address (192.168.1. x). Then, use the default IP address, username, and password to access the eWeb management system. After the first successful login, the system will prompt you to change your password.

Caution

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

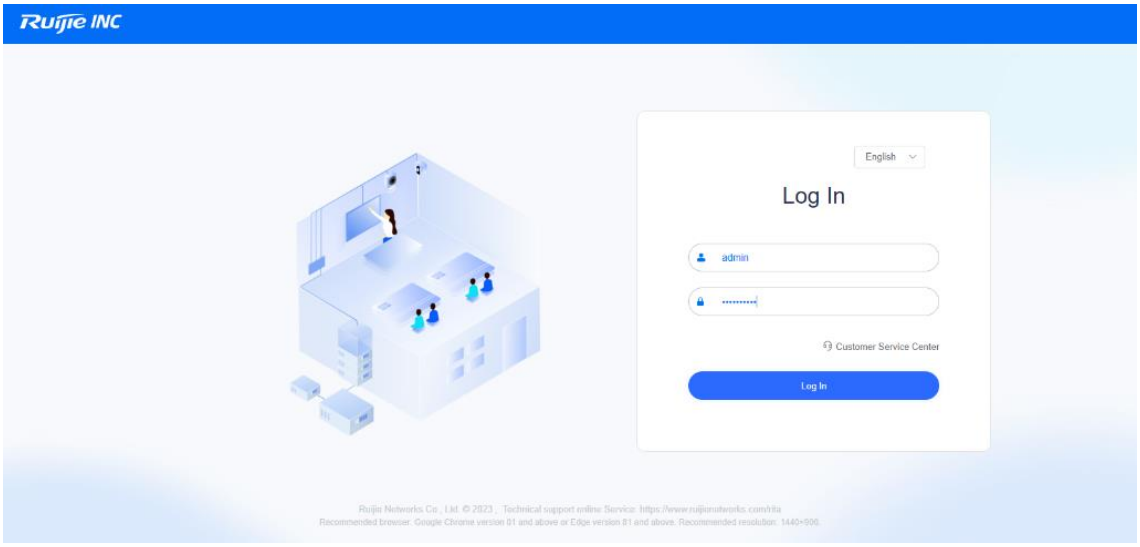
2.1.2 Client requirements

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.

3 eWeb Management System

3.1 Logging In

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



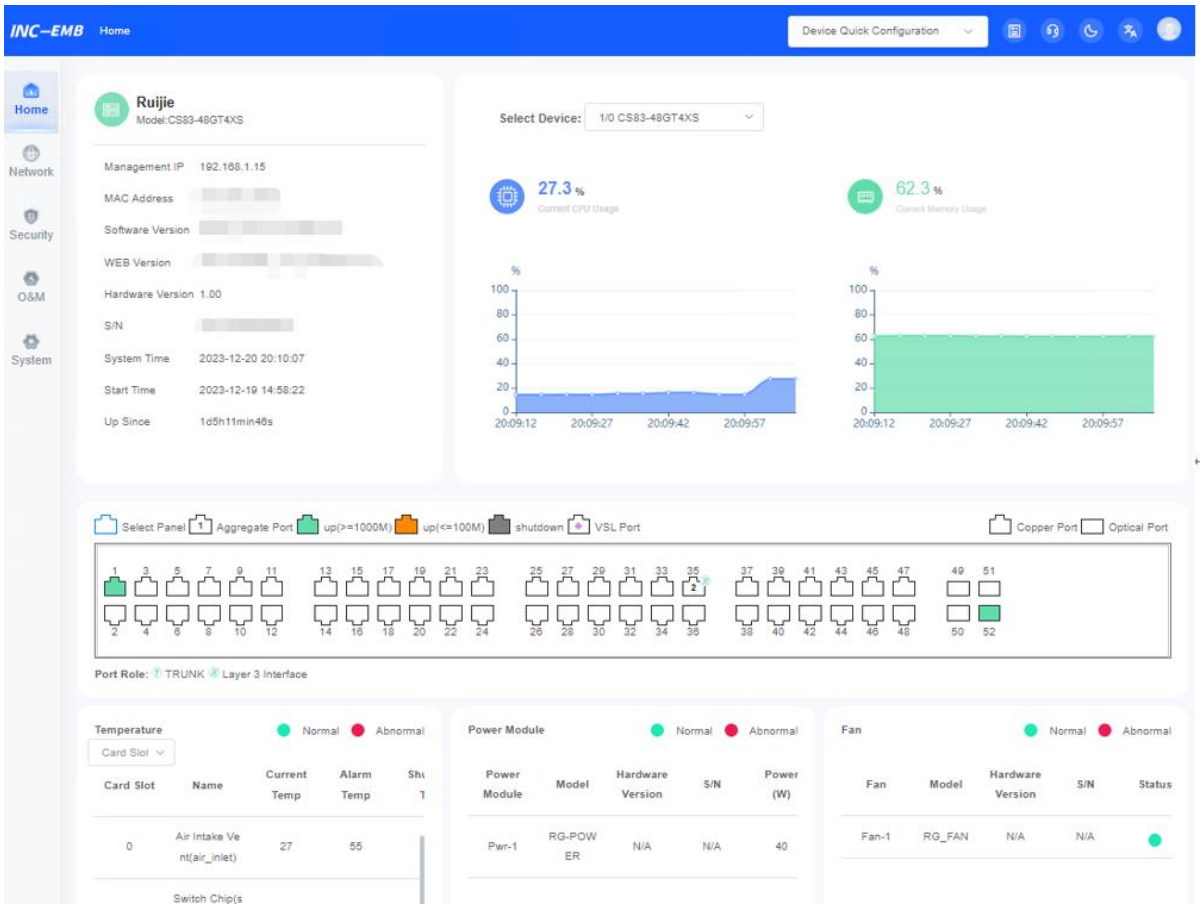
1. Enter the username and password and click **Log In**. The main interface of the eWeb management system is displayed.
2. If you cannot remember your username or password, click **Forgot Password?**
3. If you need customer service assistance, contact local technical support.
4. To prevent login through 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.

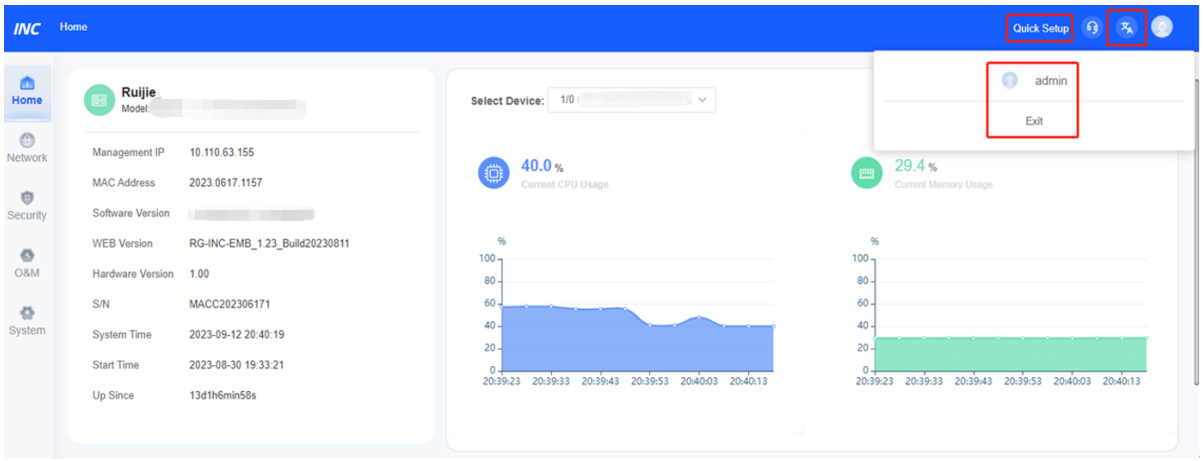
3.2 Main Interface

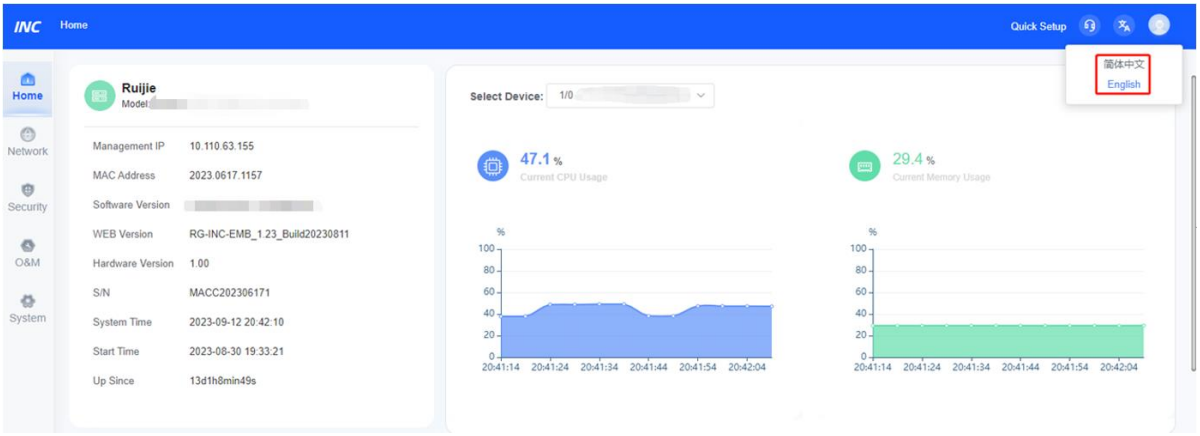
The main interface of the eWeb management system is displayed.



3.2.1 Header

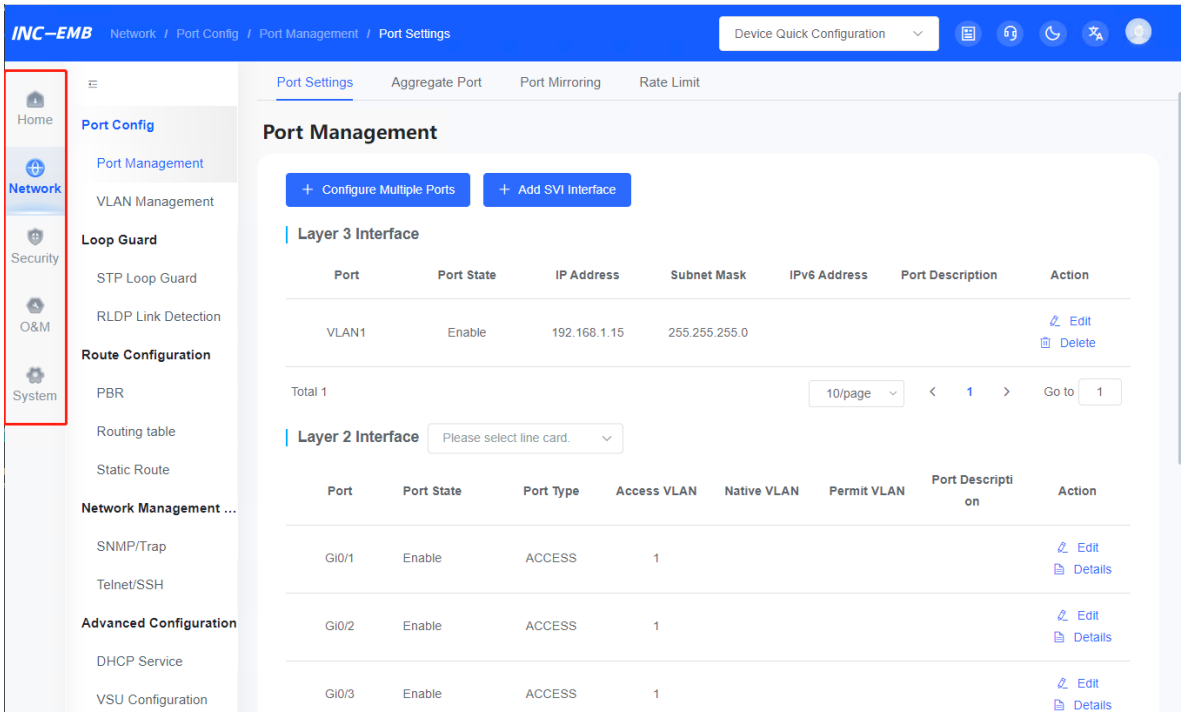
This area displays the links to common functions, including Quick Setup, change language and Exit. You can click these links to switch to specific configuration pages.





3.2.2 Navigation Menu

This area displays main tabs of the eWeb management system.



3.2.3 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.

3.3 Quick Setup

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.

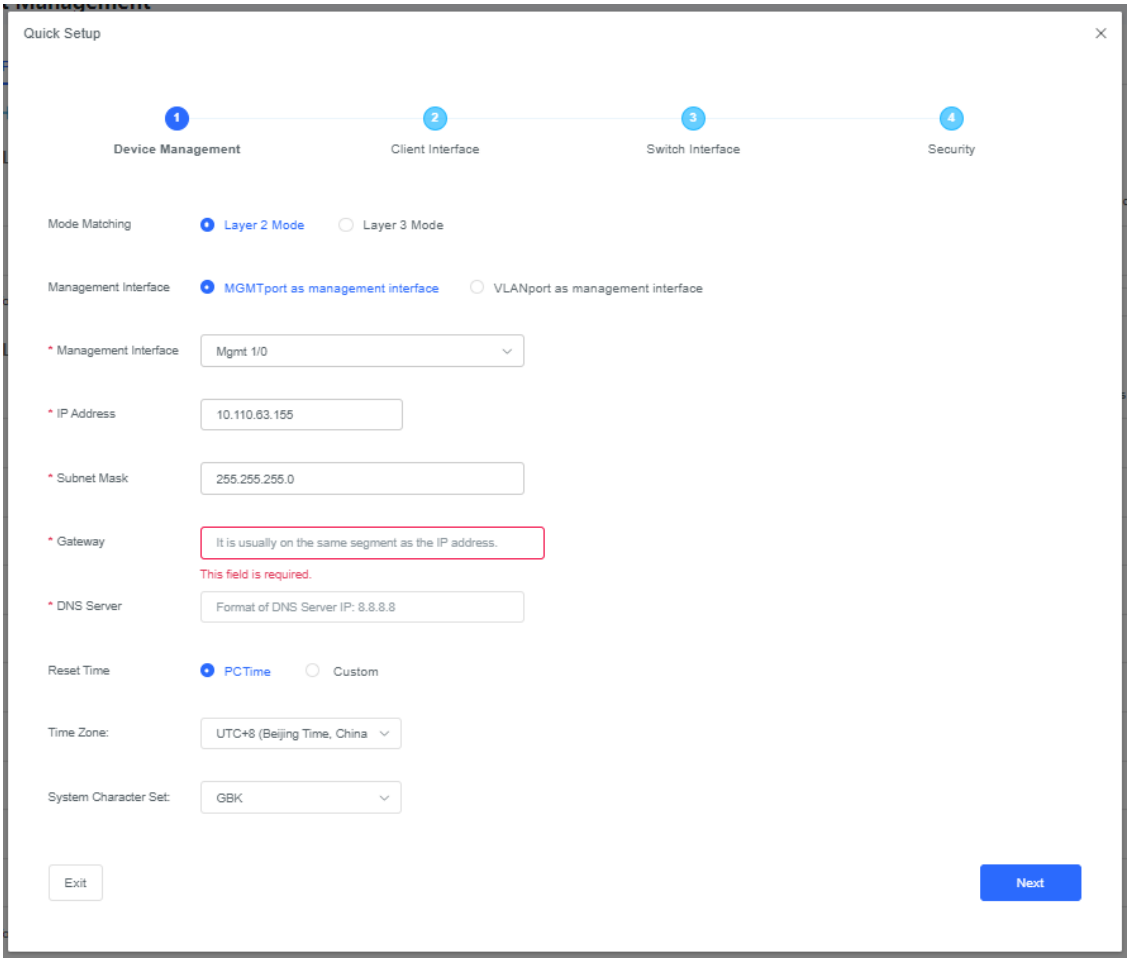
Note

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

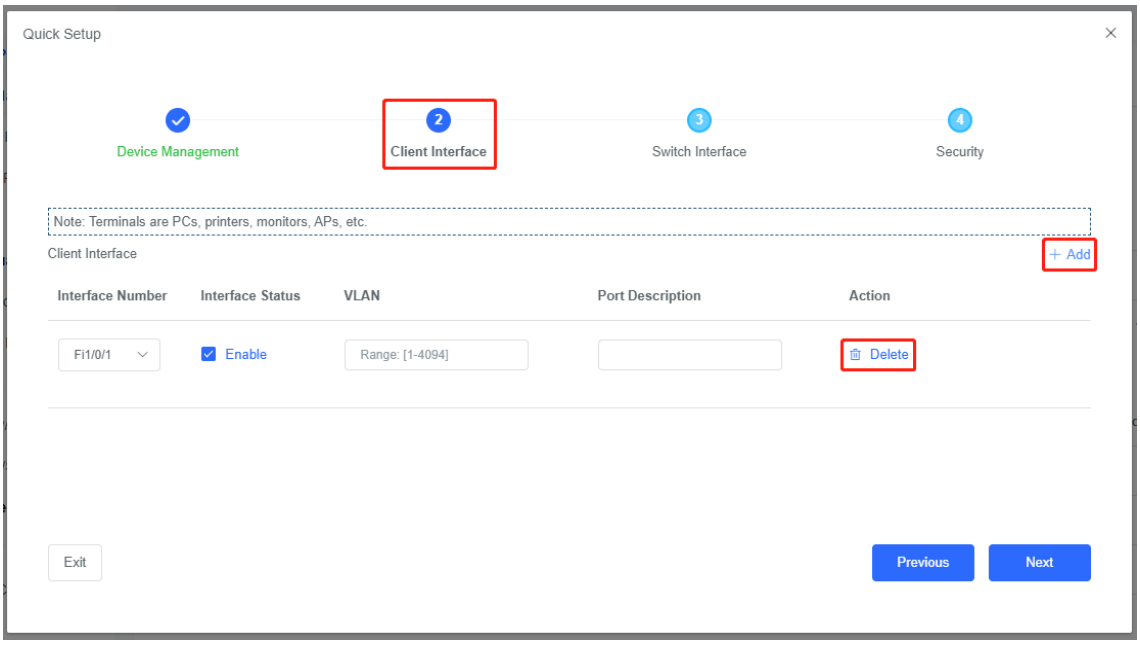
3.3.1 Layer 2 Mode

There are four steps in this mode.

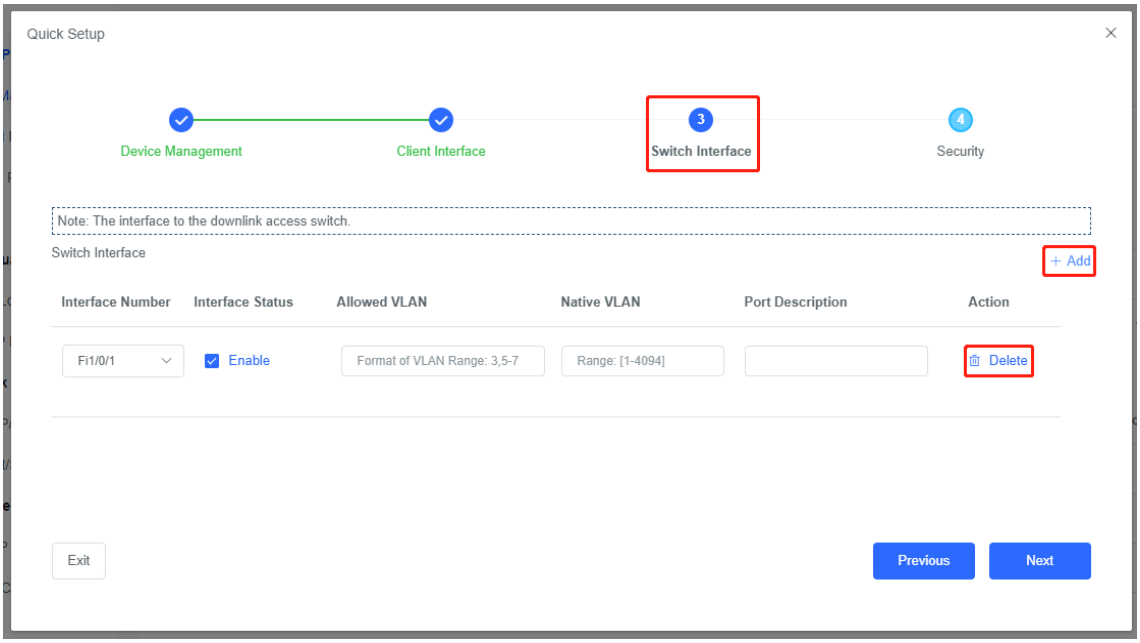
(1) Device Management



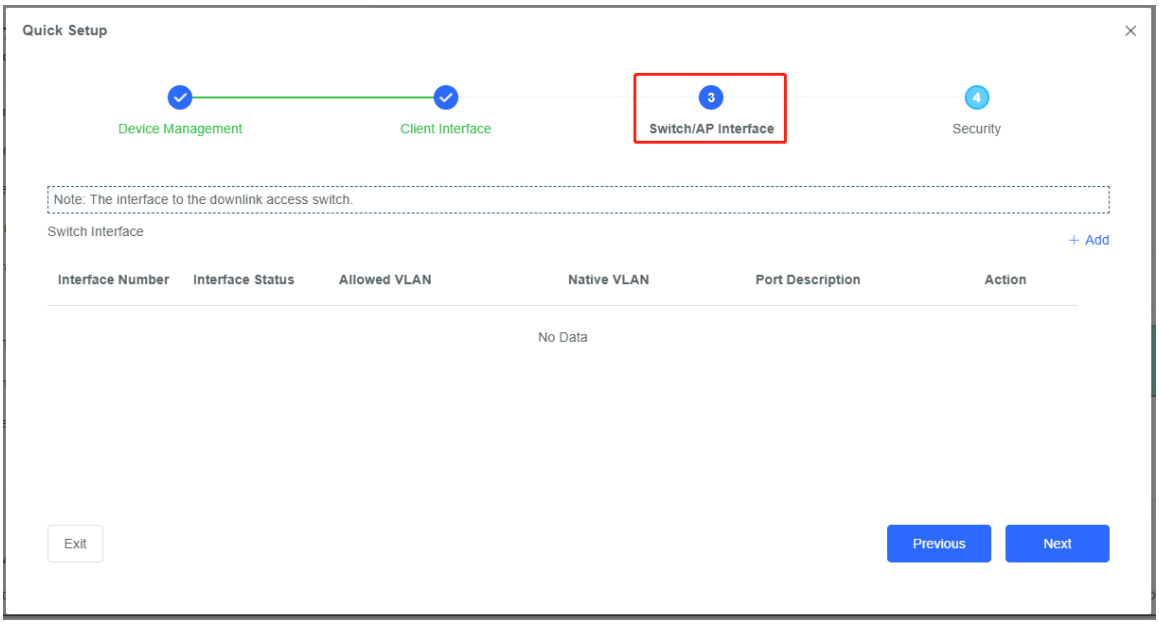
(2) Client Interface



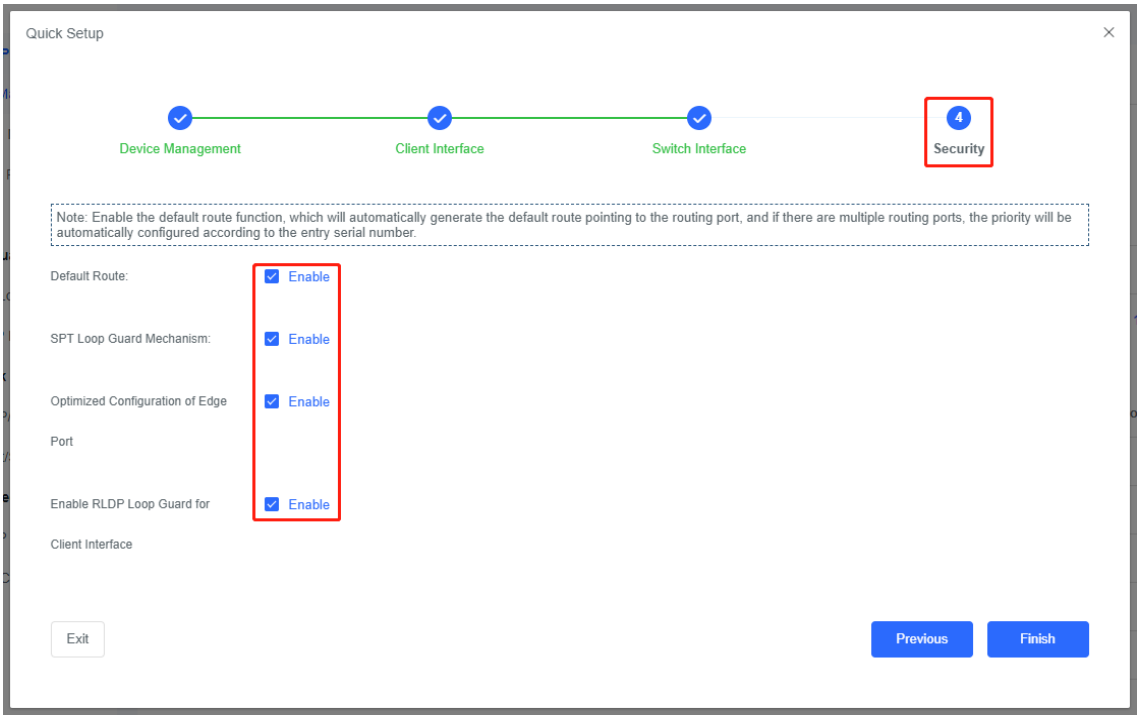
(3) Switch Interface



If the device is an integrated switch, you can configure the interface of the access point on this page.



(4) Security

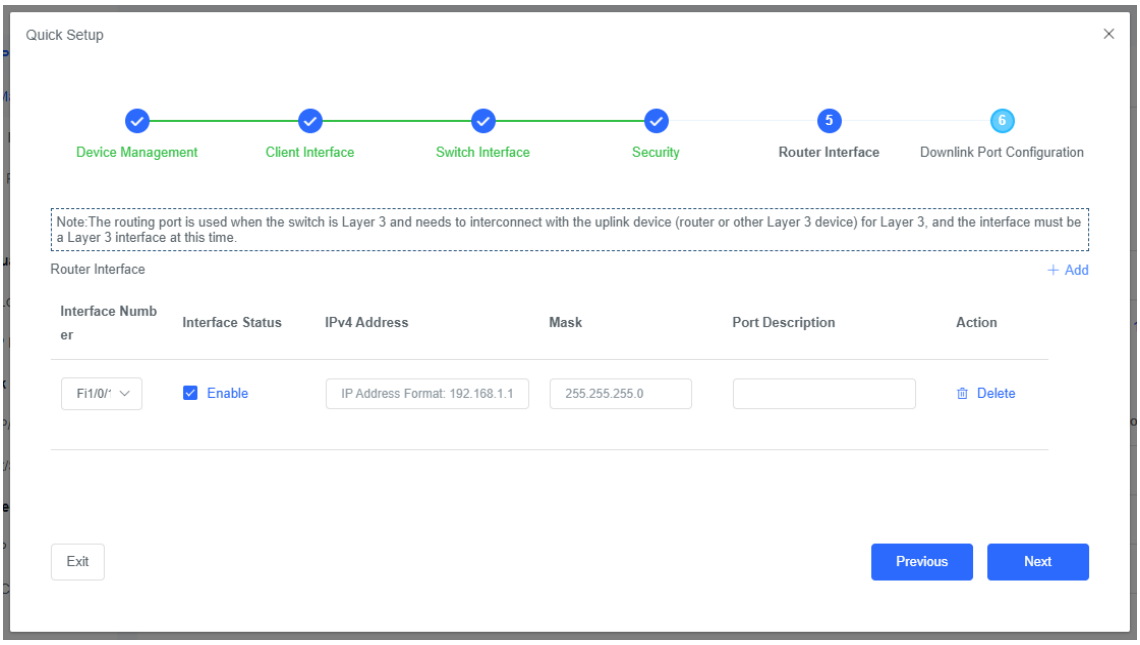


3.3.2 Layer 3 Mode

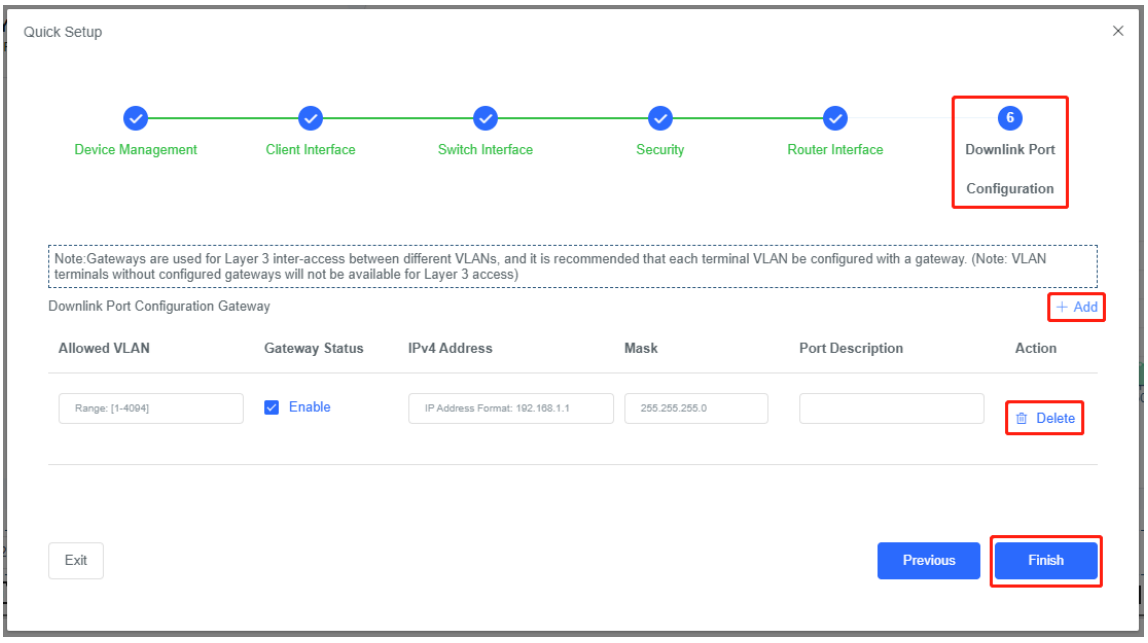
There are six steps in this mode.

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)



(2) Downlink Port Configuration (Layer 3 Mode)



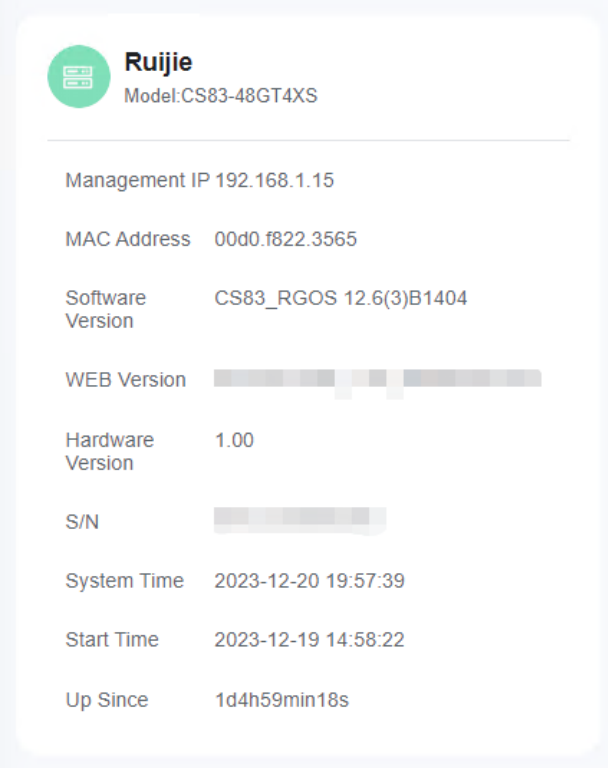
3.4 Home Page

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.

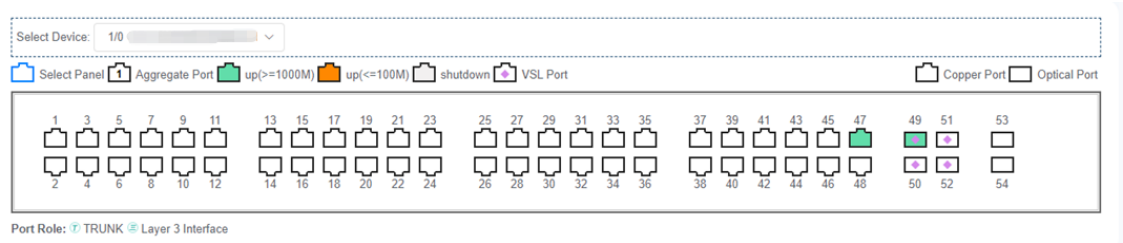
3.4.1 Switch Overview

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**.



3.4.2 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.

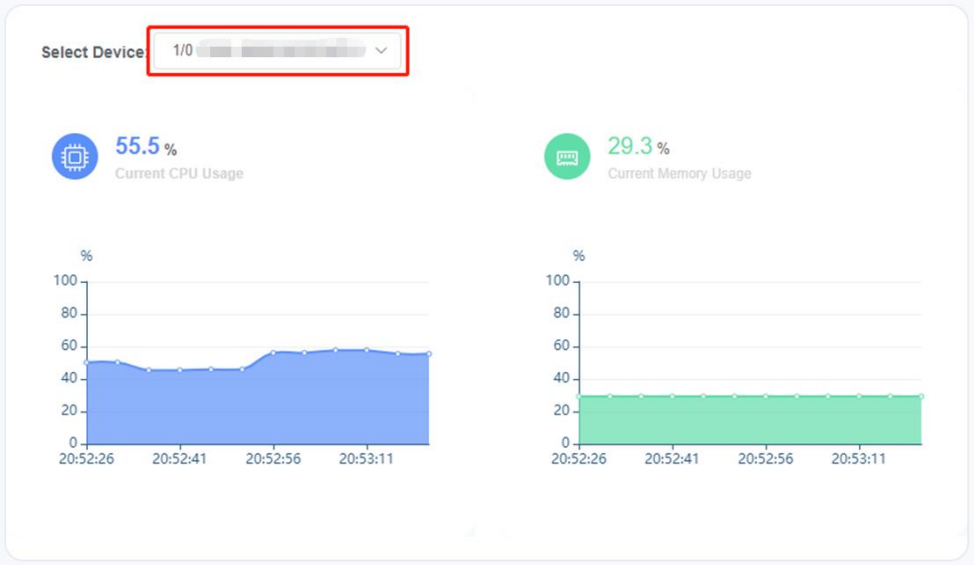


3.4.3 CPU/Memory Usage

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 switch service module.

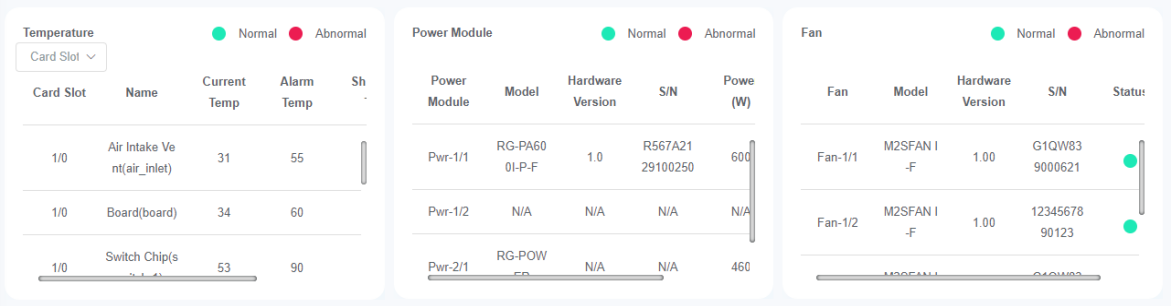
(2) Memory: indicates the memory usage of the switch service module.



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.

3.4.4 Temperature/Power Module/Fan

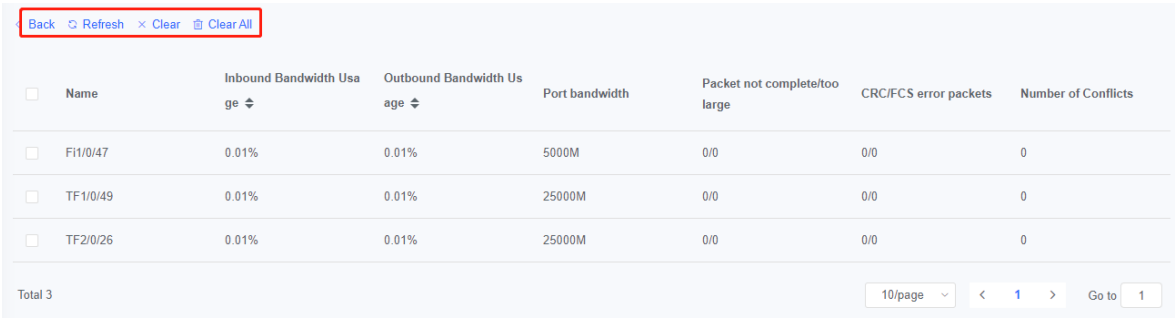
The middle part of the home page displays the temperature, power module status, fan status of the switch at different positions.



3.4.5 Bandwidth



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



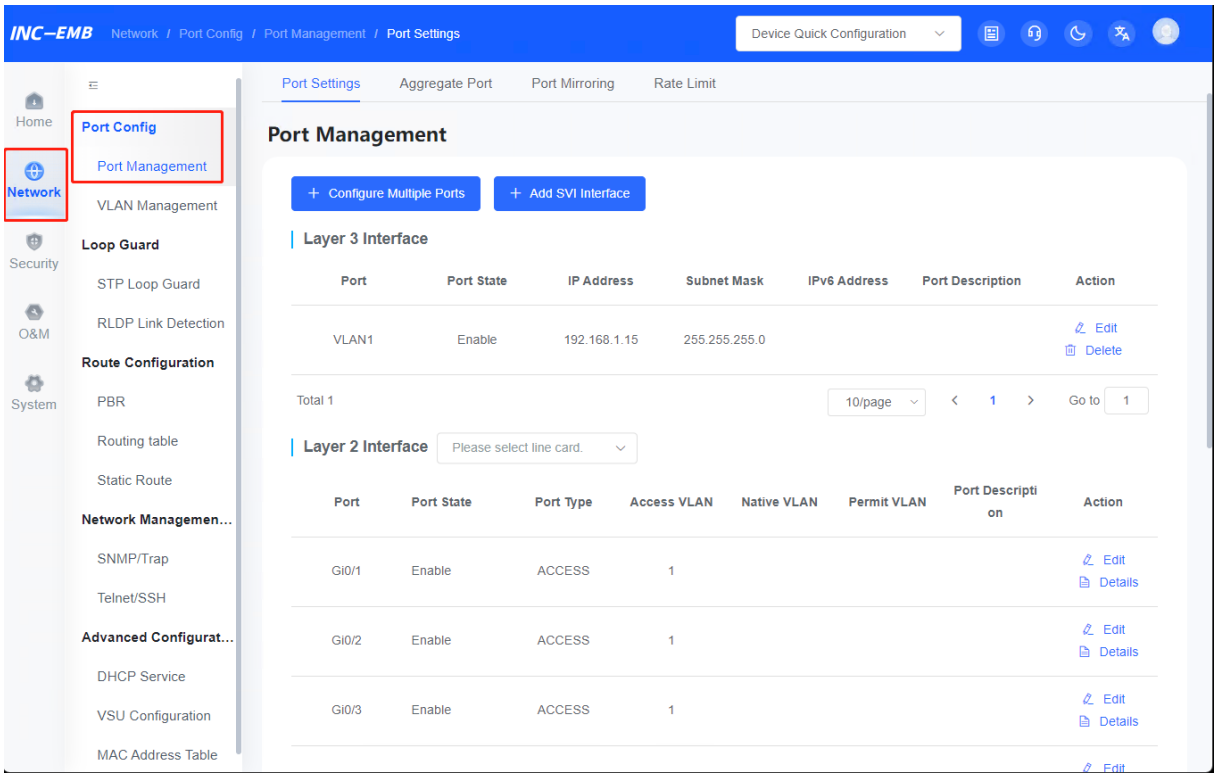
- Back: returns to the home page.
- Refresh: re-queries the interface bandwidth utilization.
- Clear: deletes statistics about a selected interface, such as the number of error packets and conflicting count.
- Clear All: deletes statistics about all interfaces, such as the number of error packets and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

3.5 Network

3.5.1 Port Config

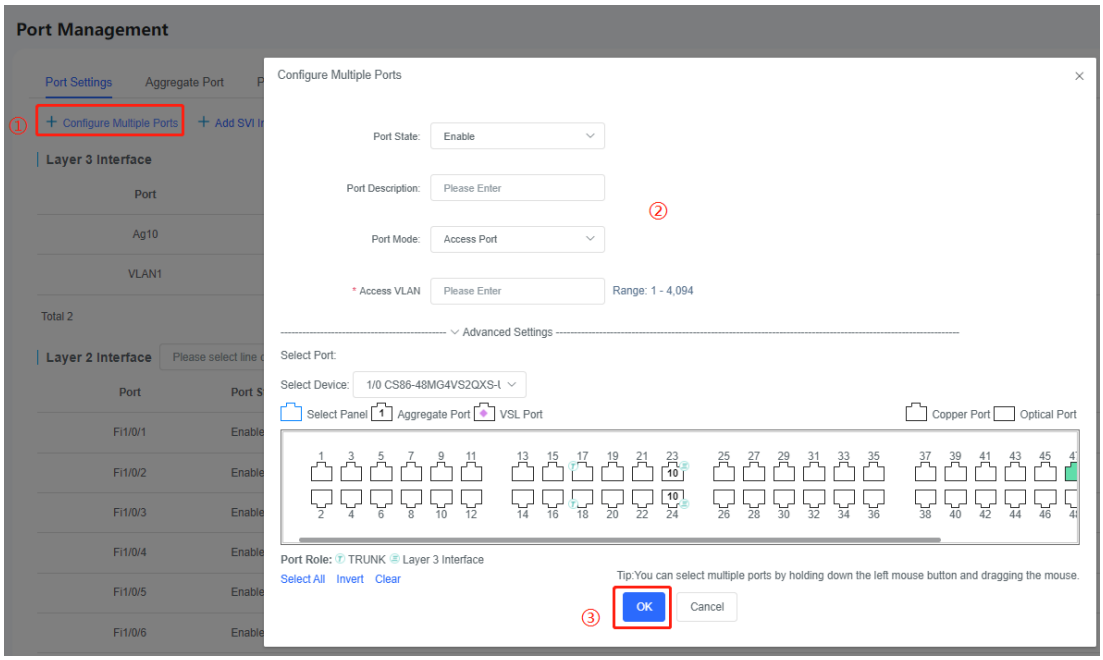
1. Port Management

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

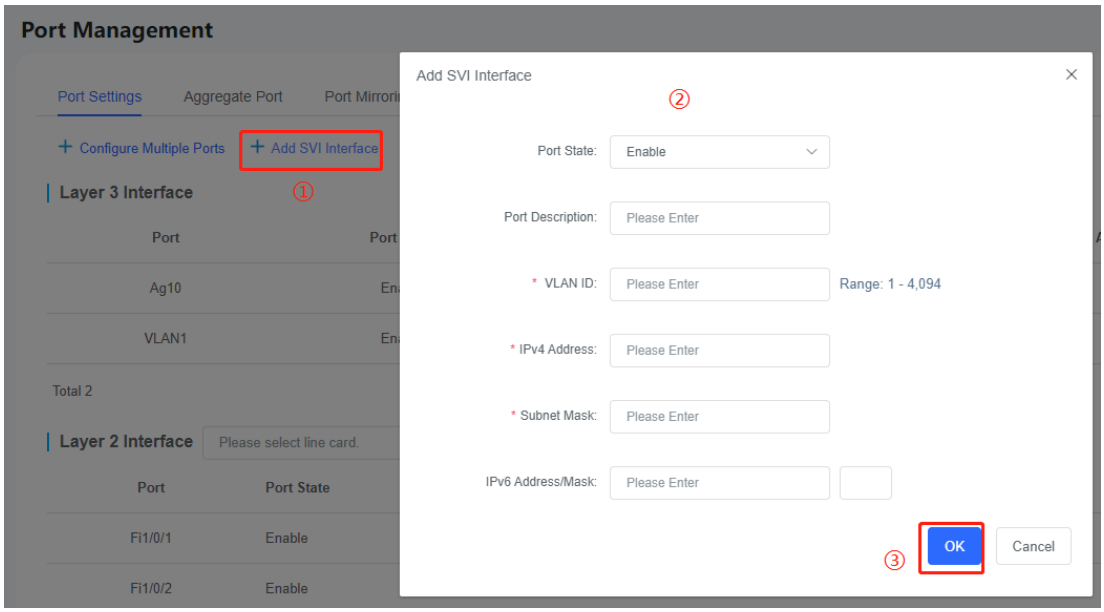


(1) Port Configuration

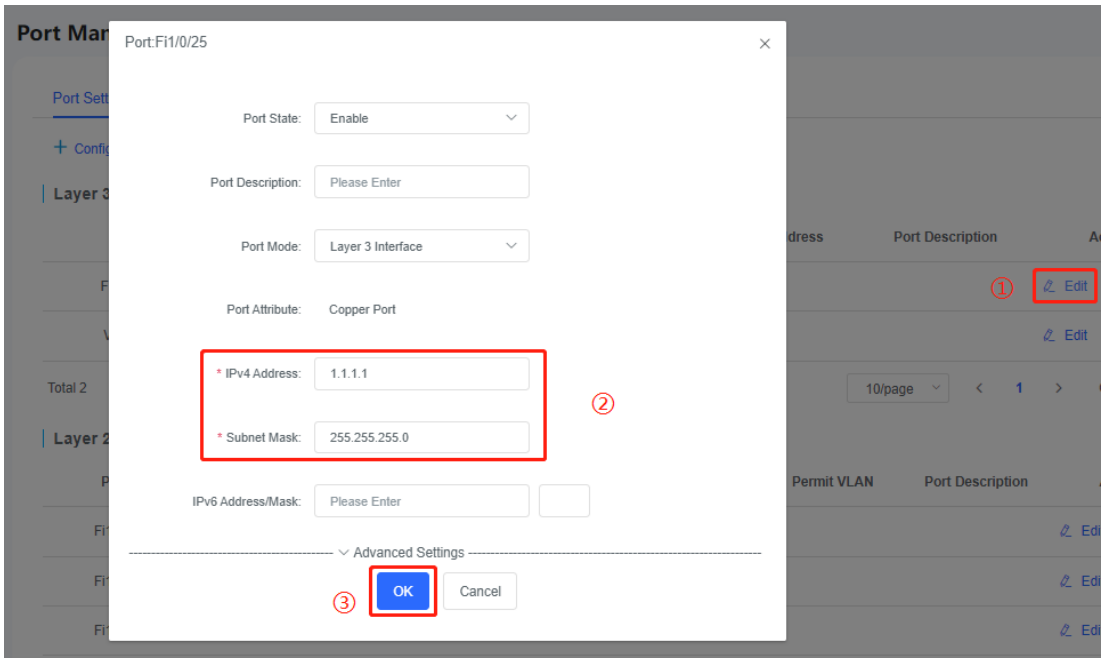
- Configuring multiple ports



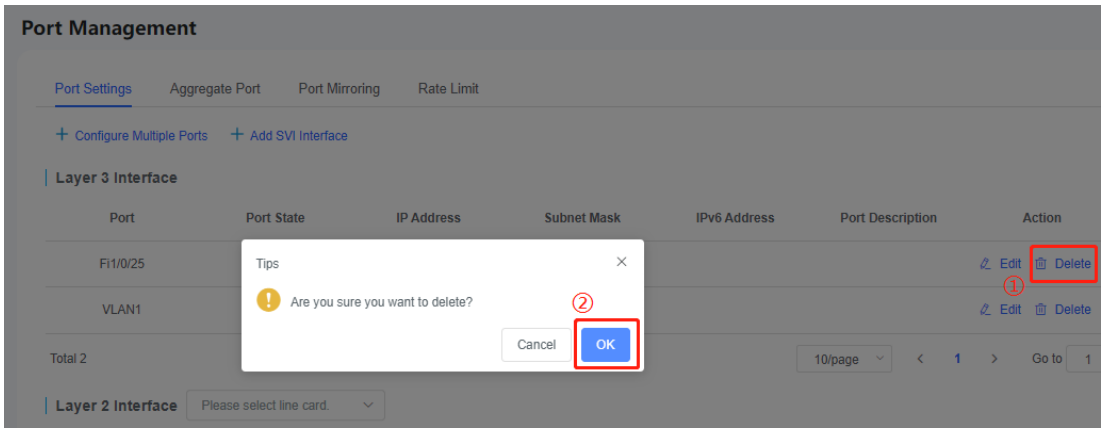
- Add SVI Interface



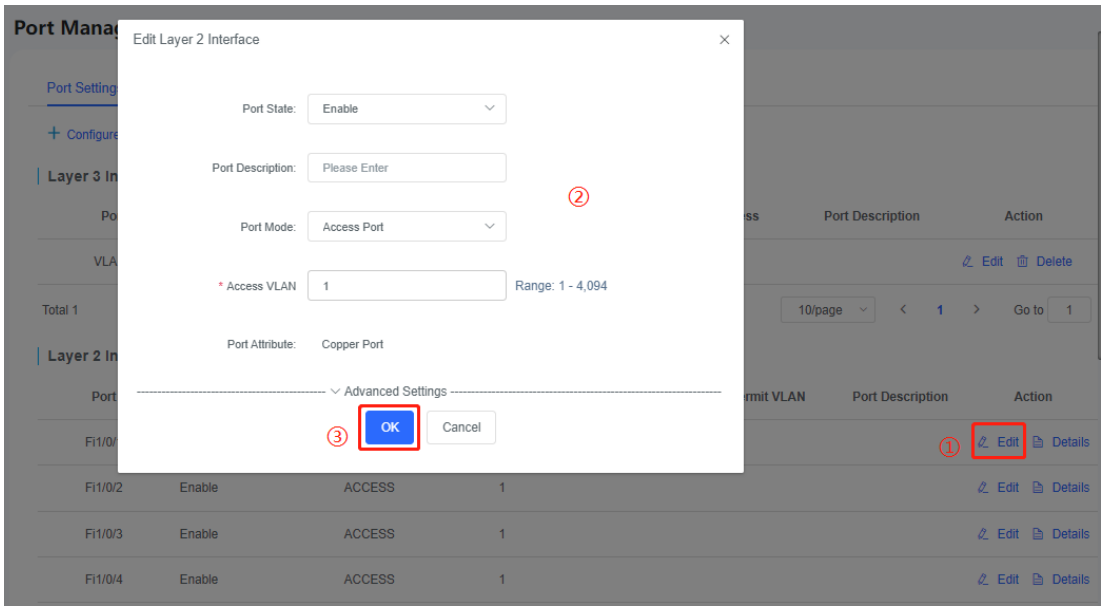
- Editing a Layer 3 interface



- Deleting a Layer 3 interface

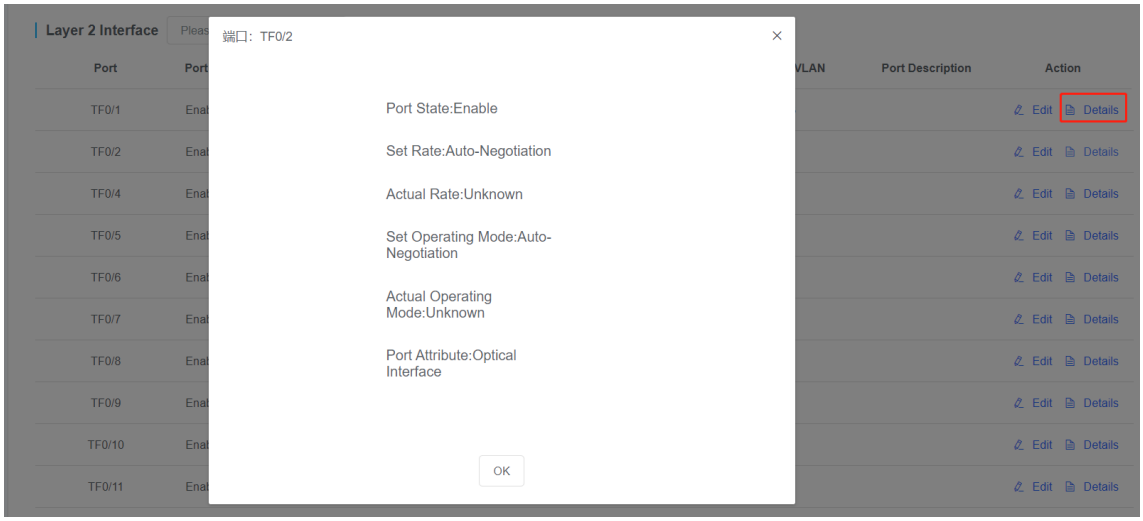


- Editing a Layer 2 interface



- A Layer 2 interface details

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



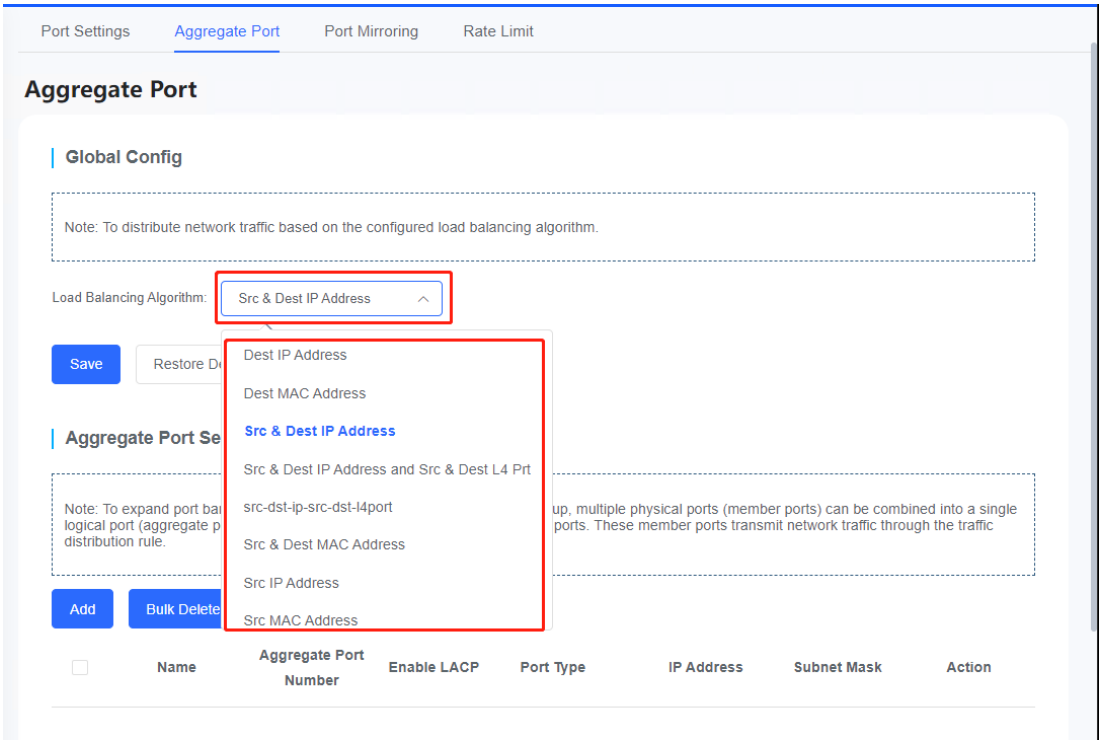
(2) Aggregate Port

Note

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.

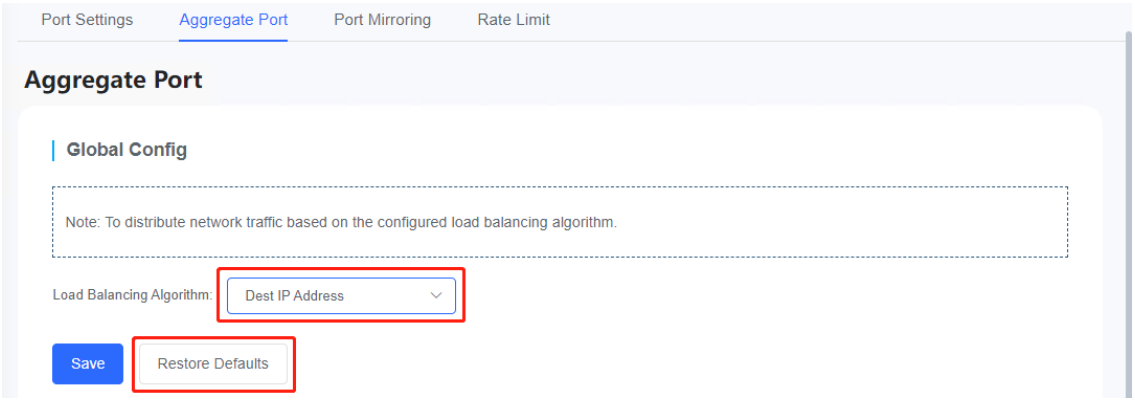
- Saving configurations

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

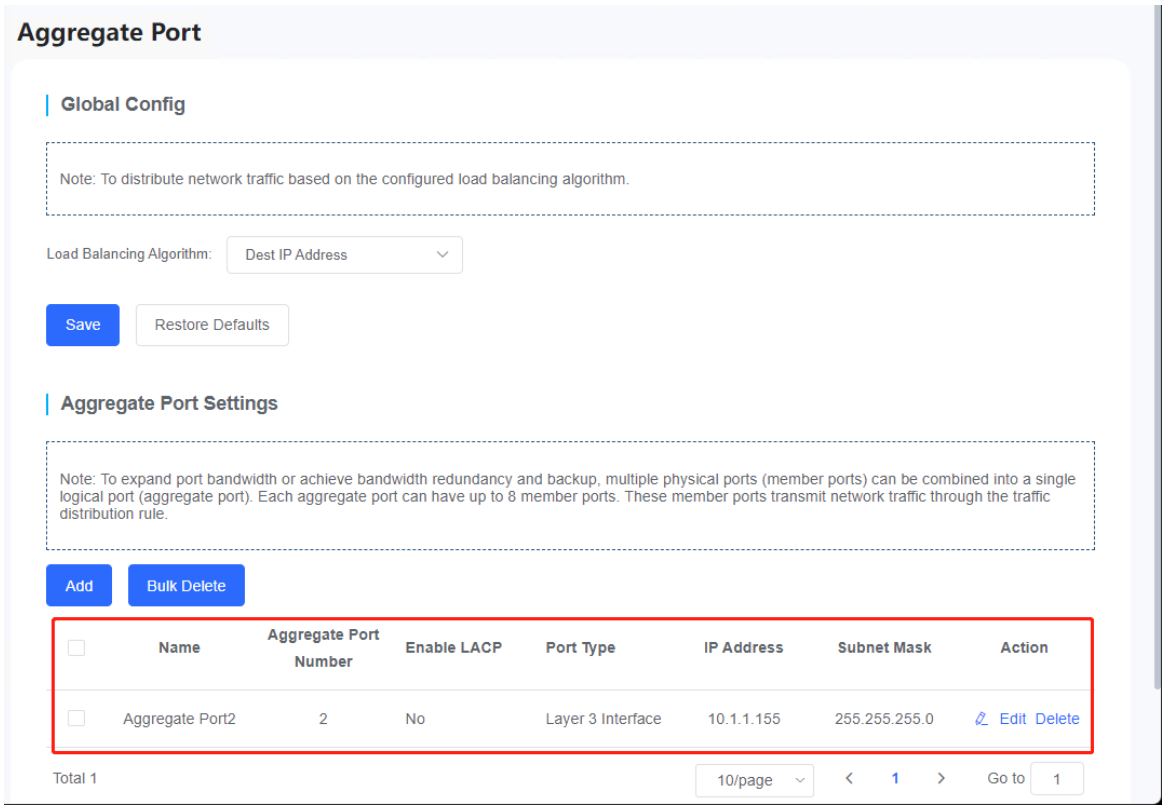


- Restoring default settings

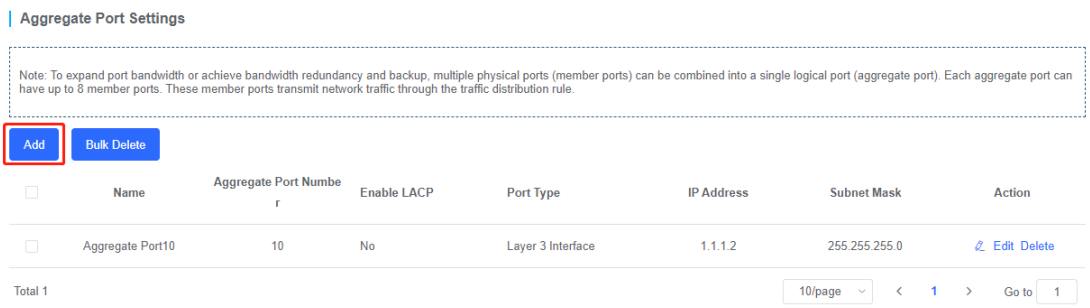
  Click **Restoring Defaults** to restore the load balacing algorithm to **Dest IP Address**.



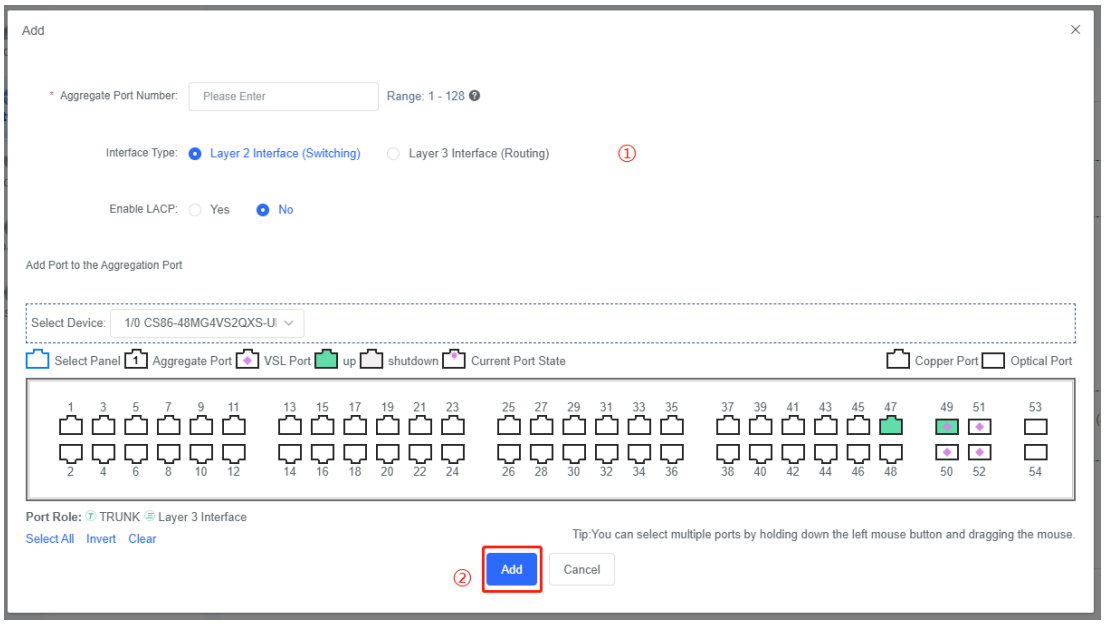
- Querying the aggregated port list



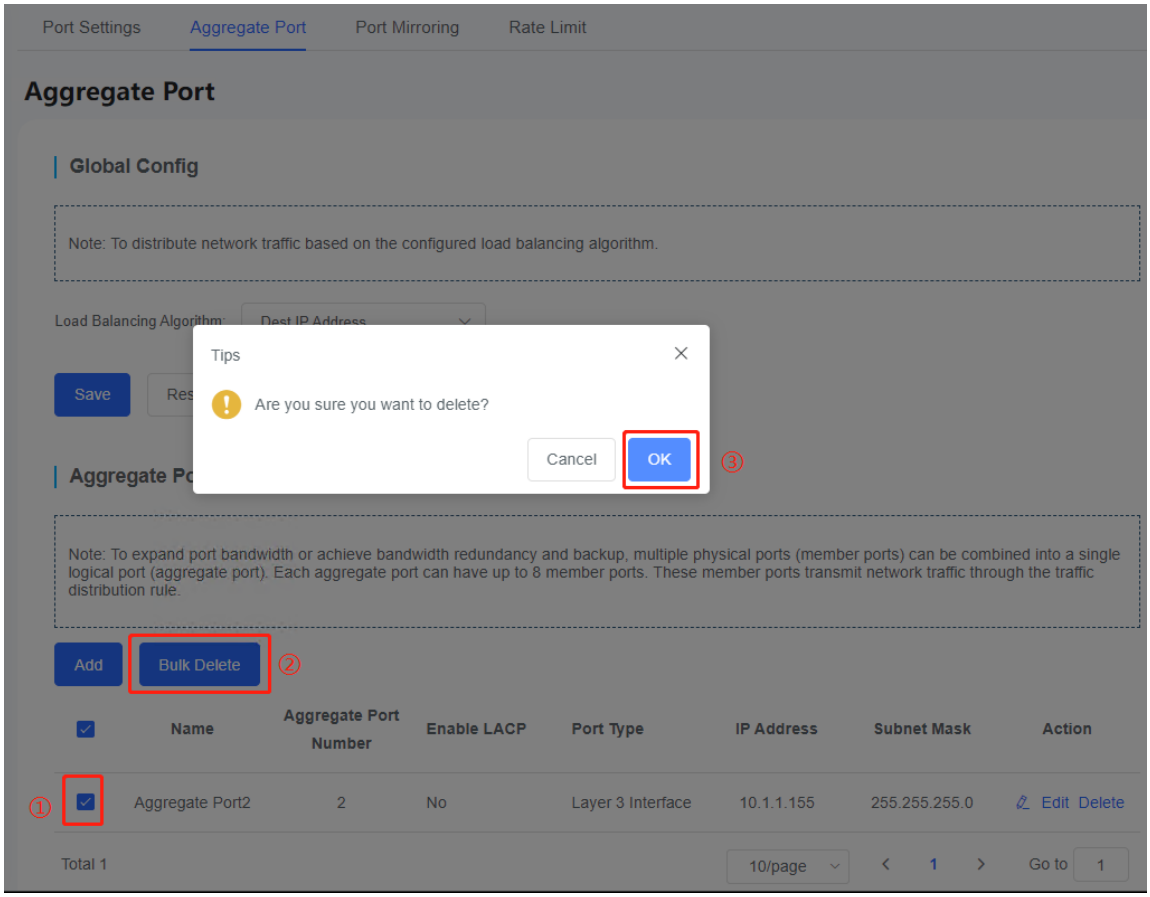
- Adding an aggregated port



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



- Deleting multiple aggregated ports

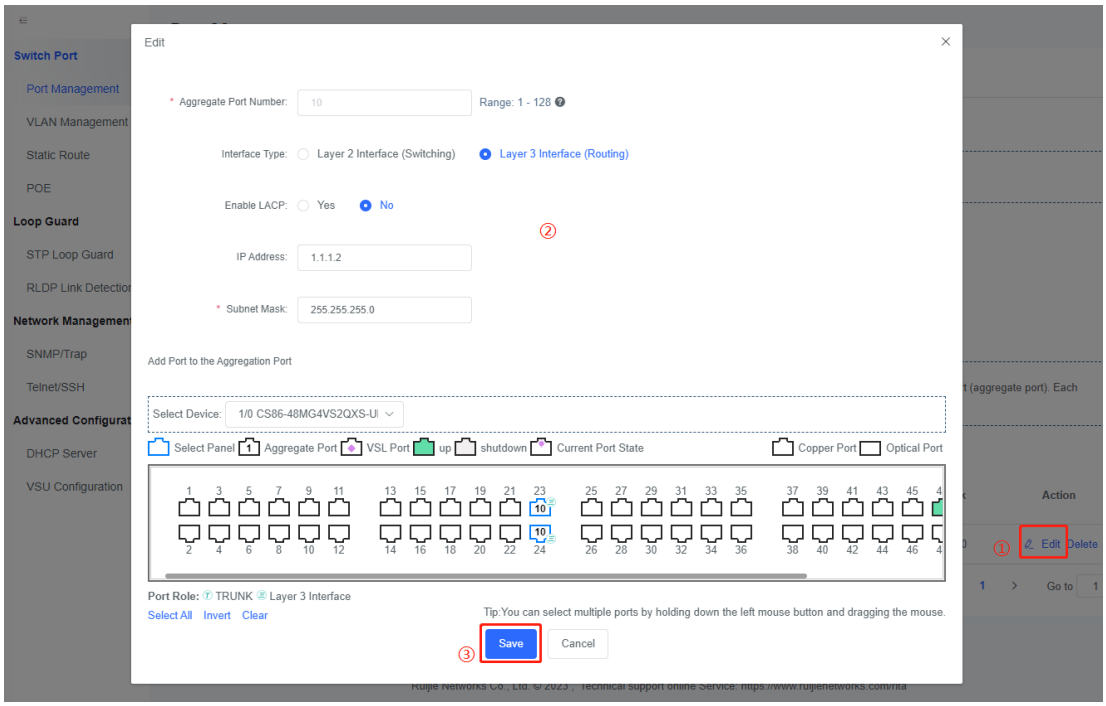


a Click Bulk Delete.

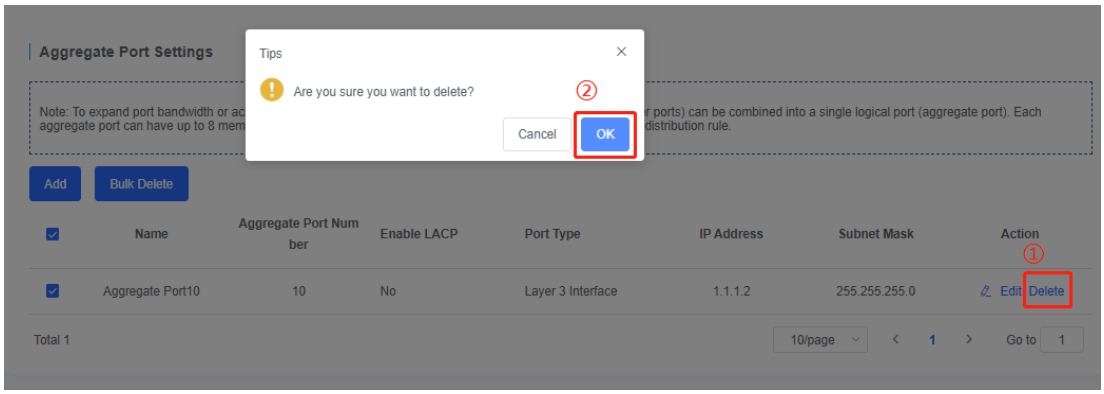
b Click OK in the displayed window. The selected aggregated ports can be removed from in the Aggregate Port list

- Editing an aggregated port

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



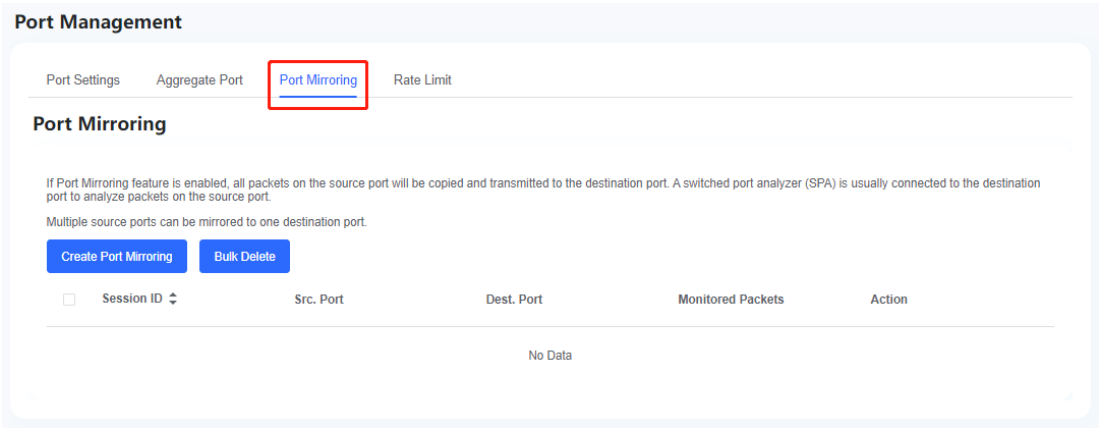
- Deleting an aggregated port



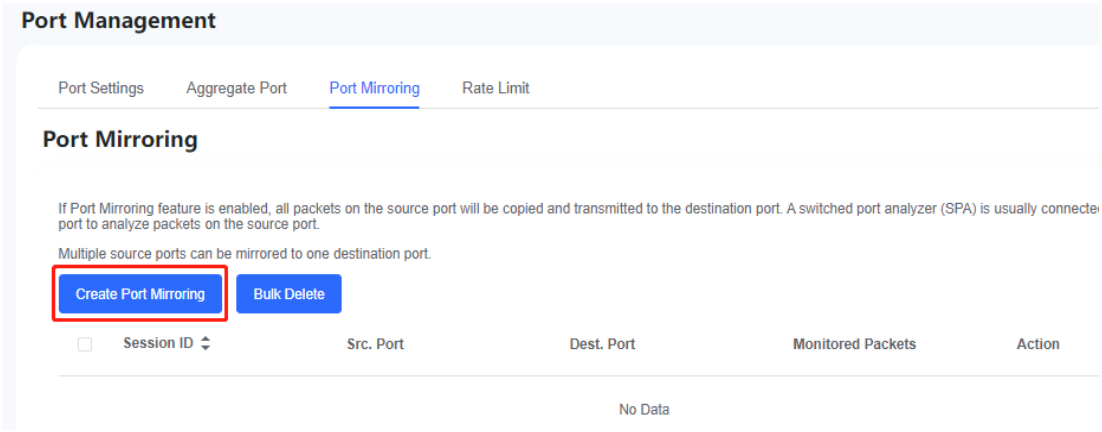
c Click **Delete**.

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

(3) Port Mirroring



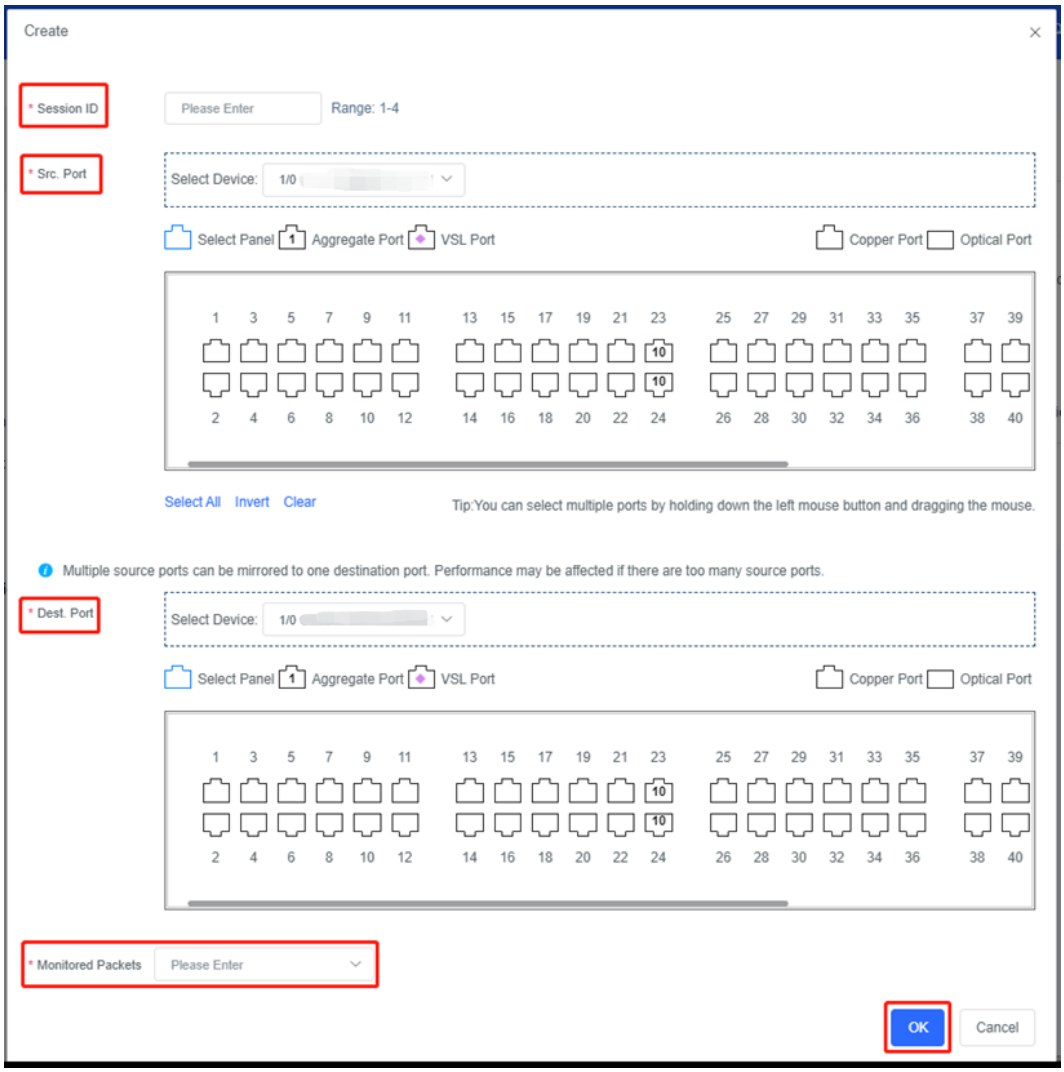
- Creating port mirroring



a Click **Create port mirroring**.

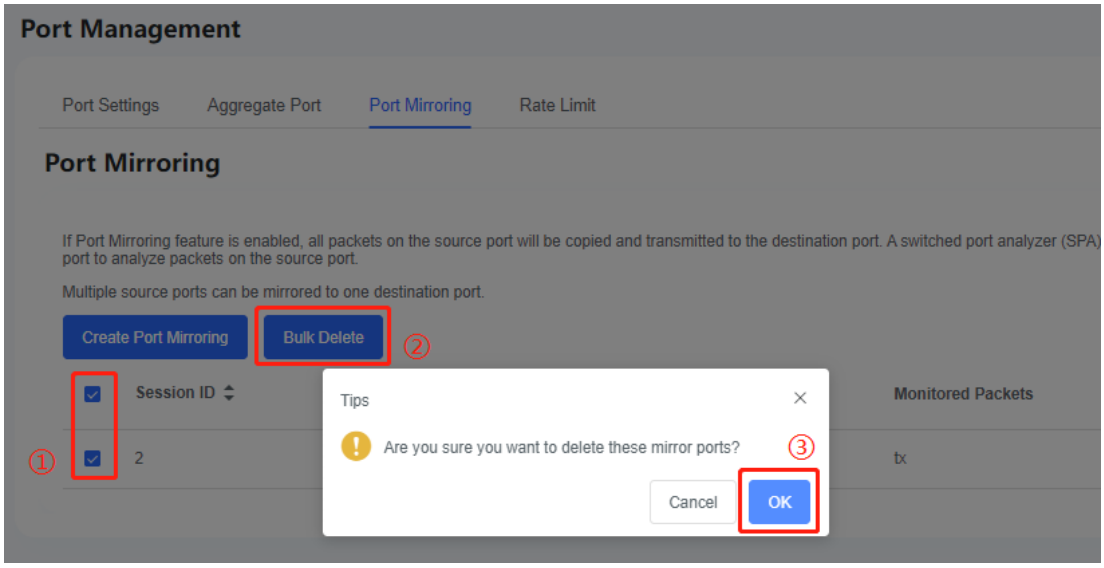
b Set configuration parameters in the displayed window.

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

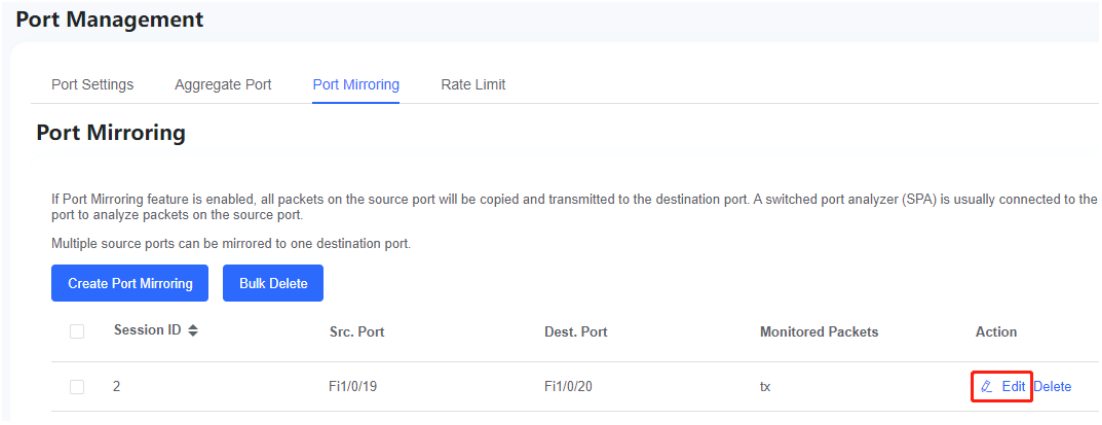


- Deleting multiple mirrored ports

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



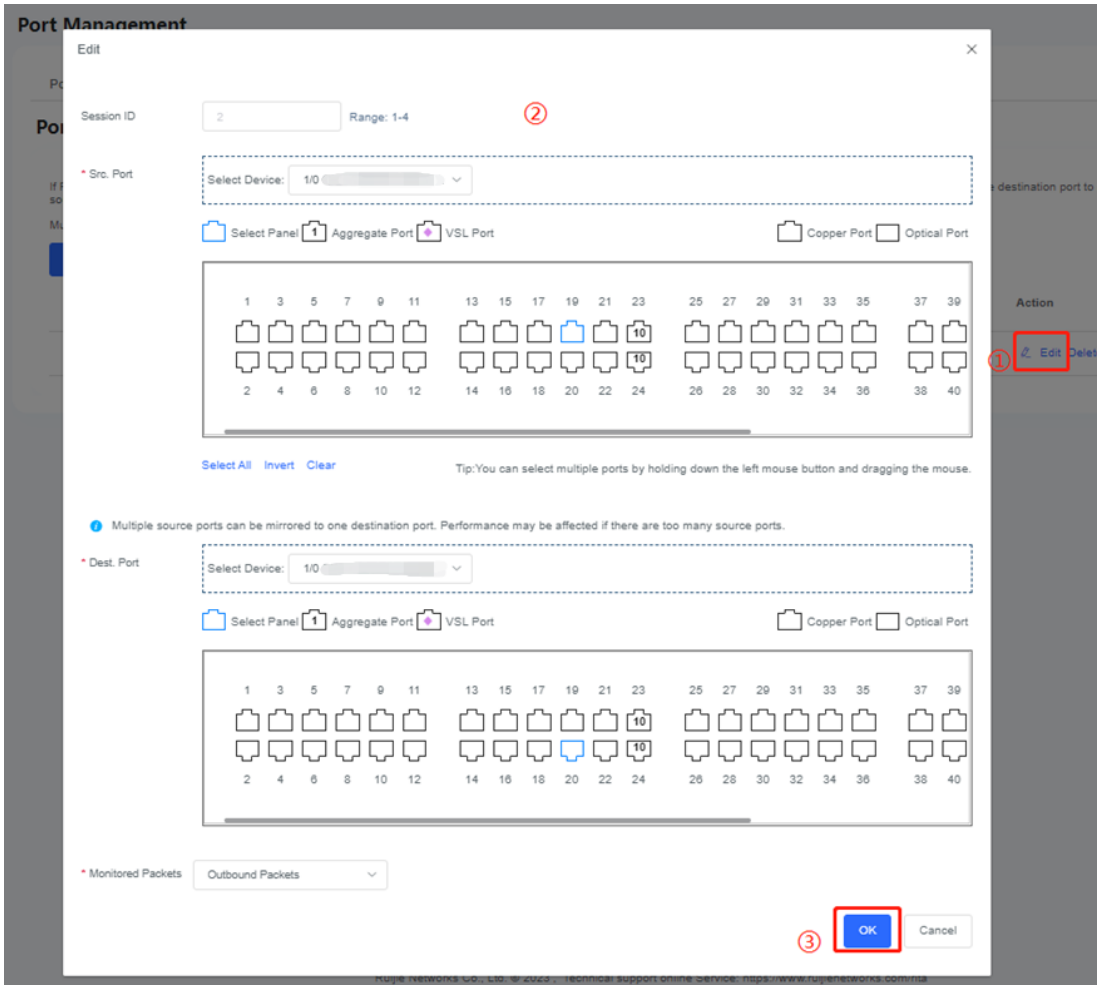
- Editing a mirrored port



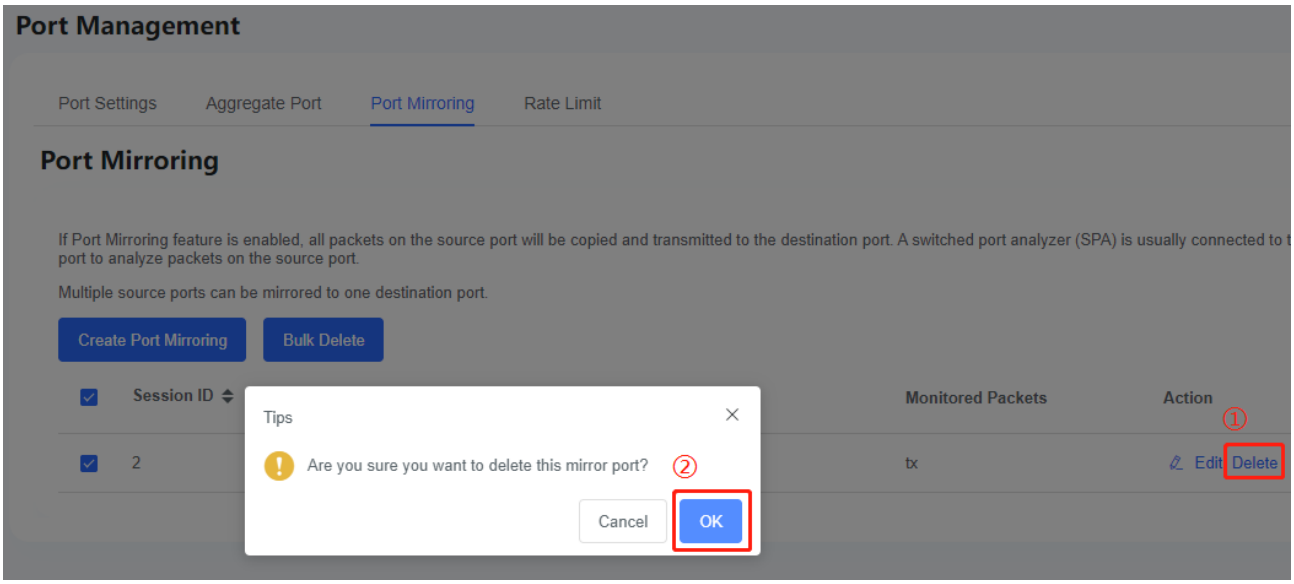
a Click **Edit**.

b Set configuration parameters in the displayed window.

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



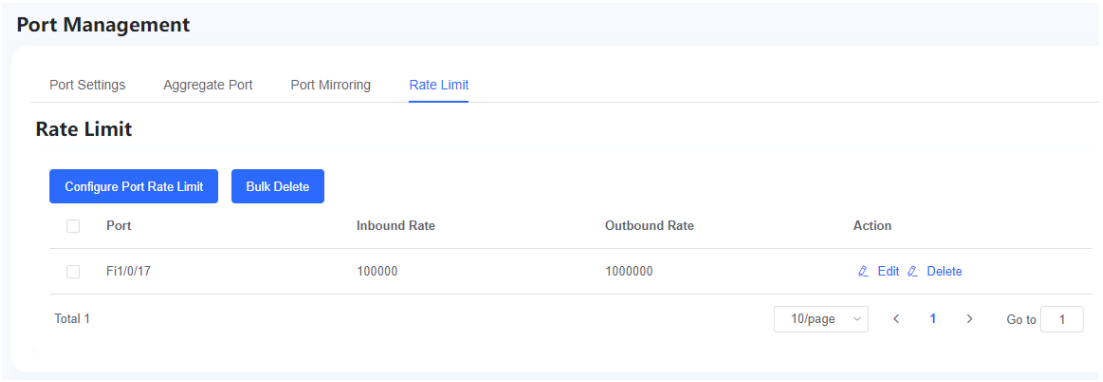
- Deleting a mirrored port



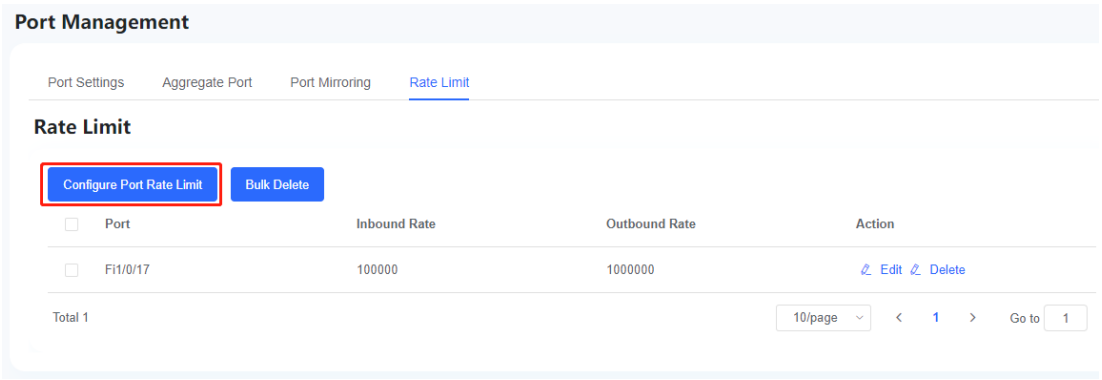
a Click **Delete**.

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

(4) Rate Limit



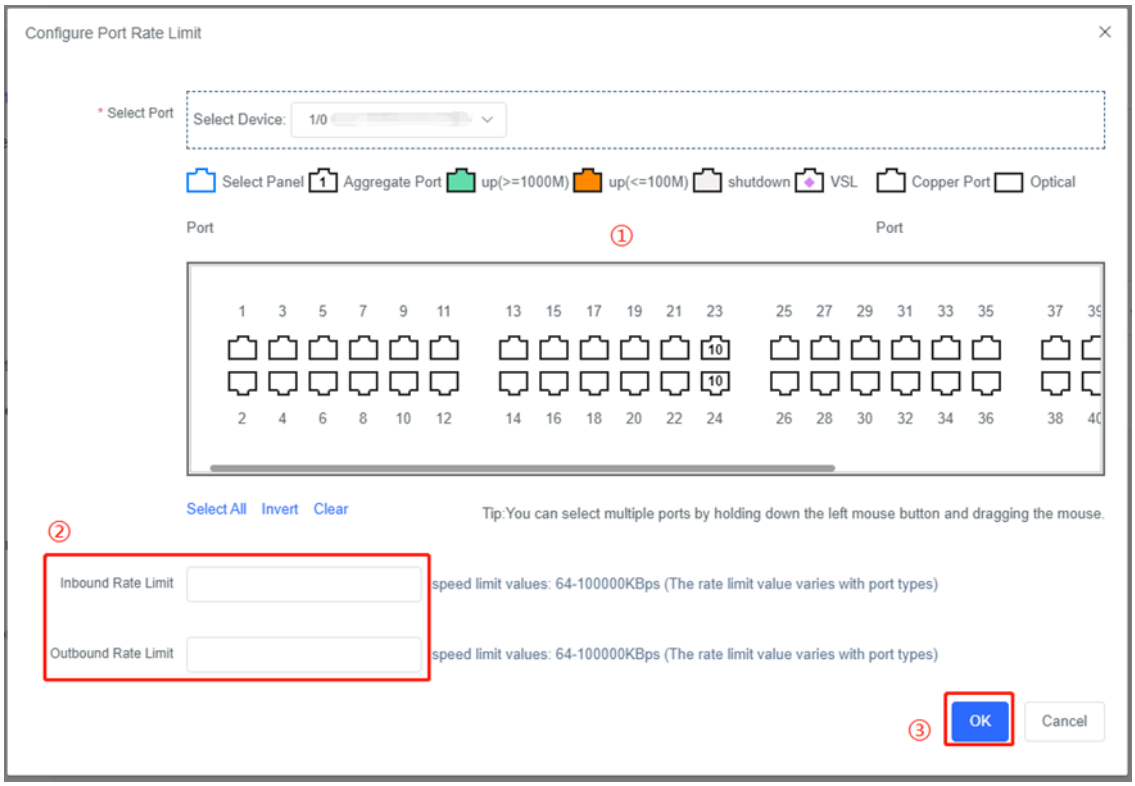
- Configuring port rate limiting



a Click **Configure Port Rate Limit**.

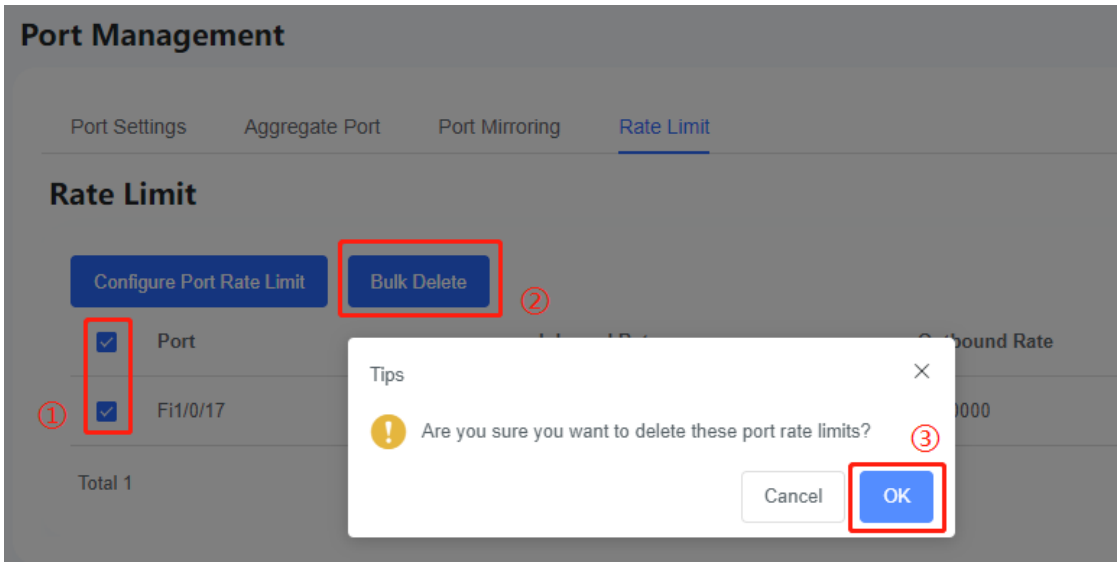
b Set configuration parameters in the displayed window.

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



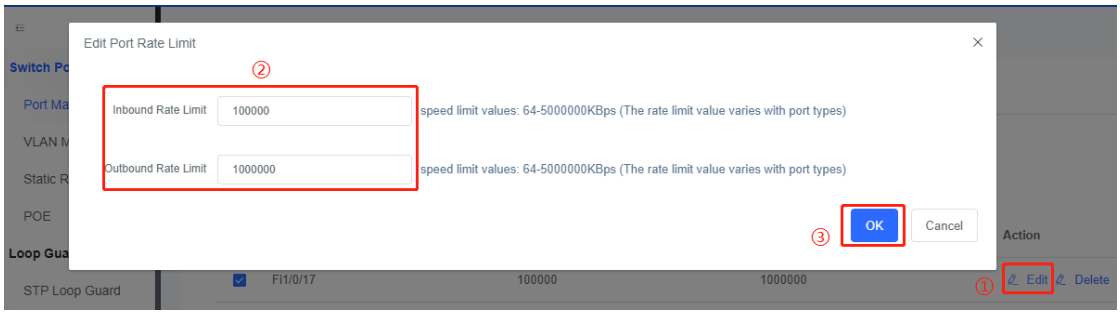
- Deleting multiple rate limiting entries

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



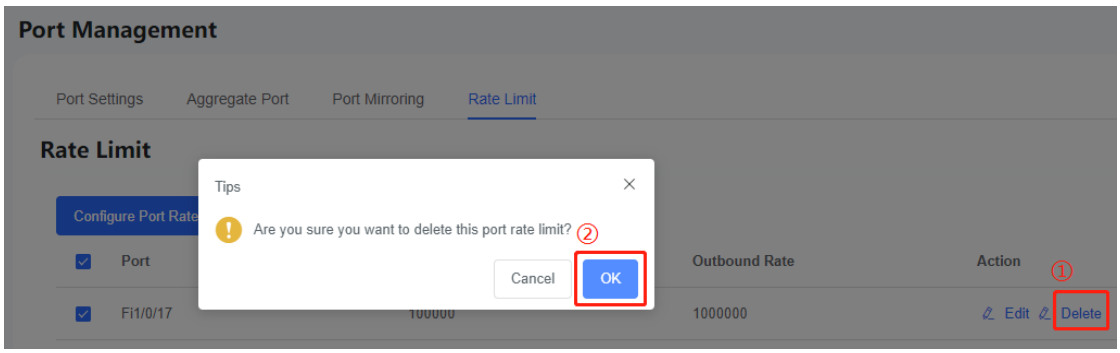
- Editing a port rate limiting entry

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



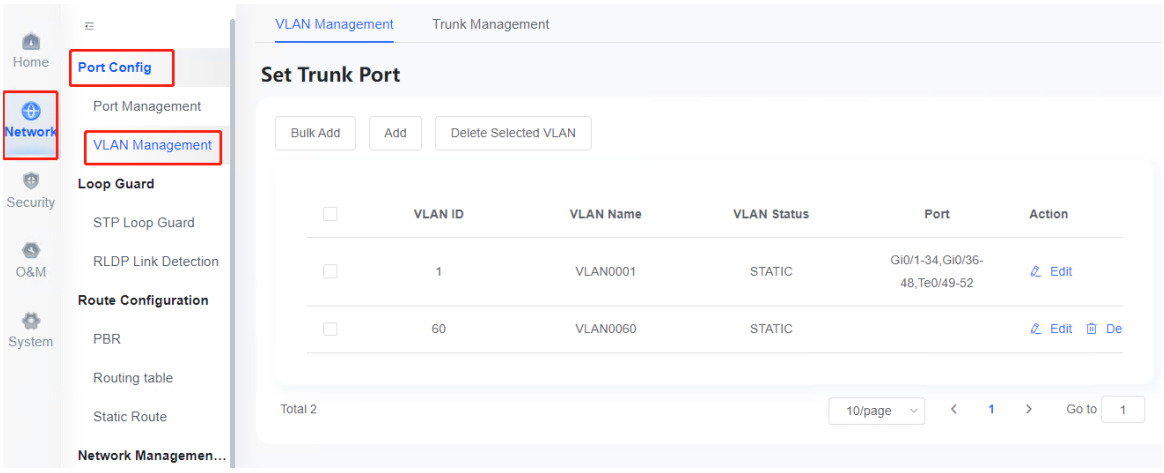
- Deleting a port rate limiting entry

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

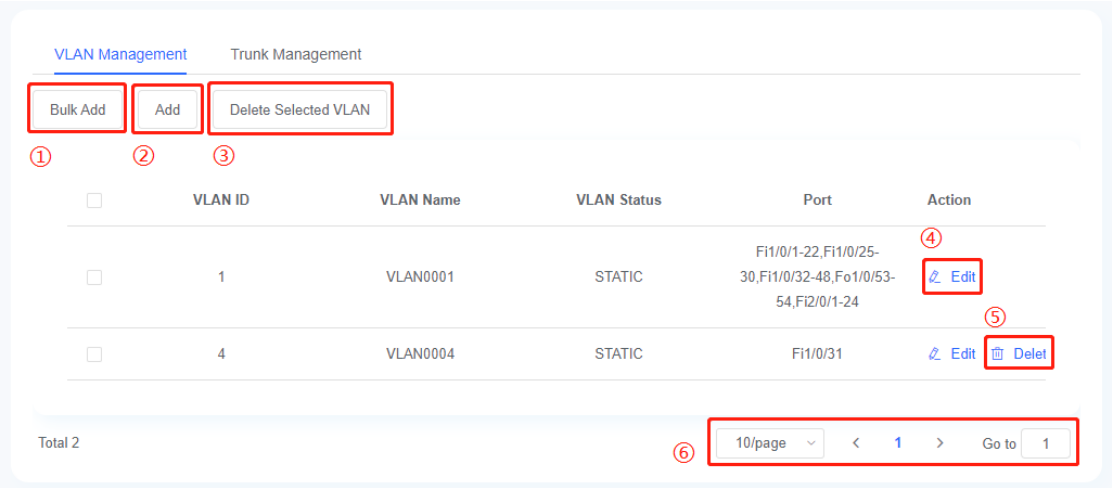


2. VLAN Management

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

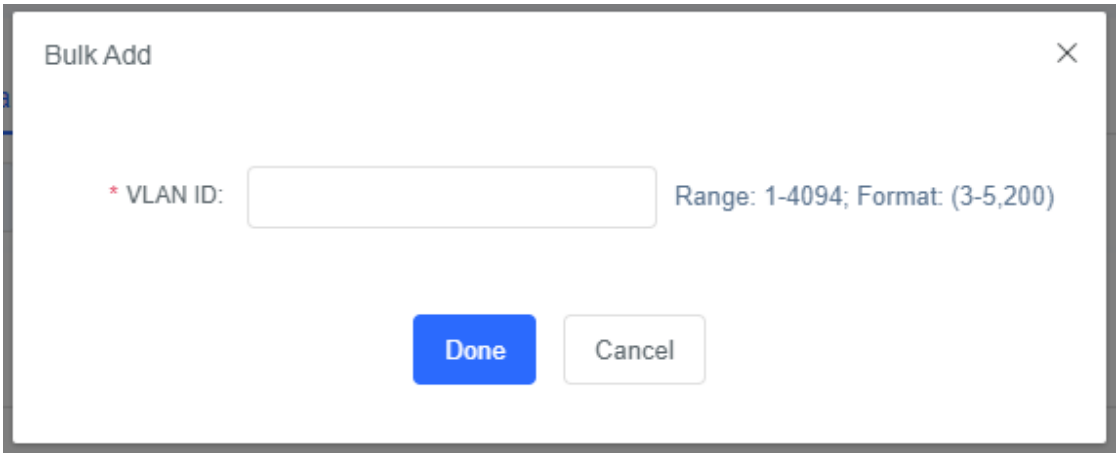


(1) VLAN Management



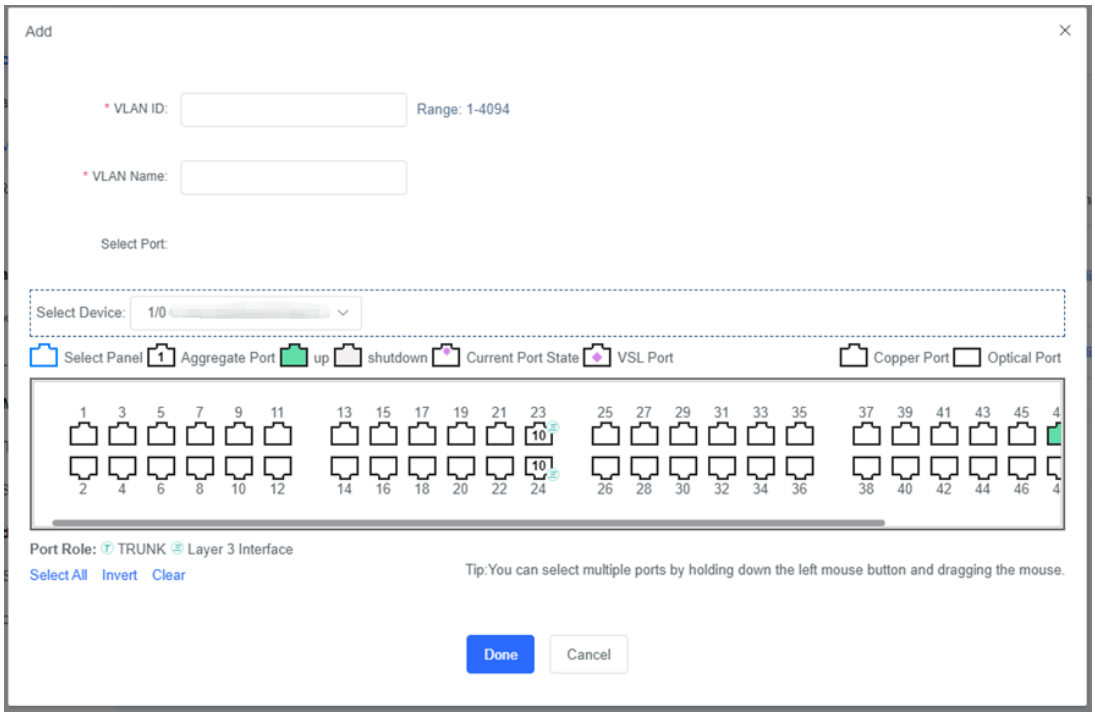
- VLAN Adding multiple VLANs

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



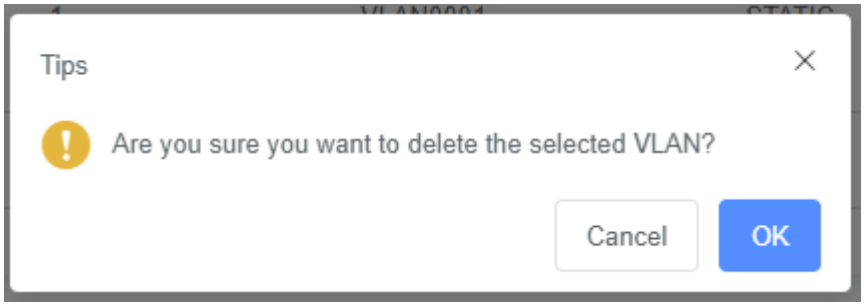
- Adding a single VLAN

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



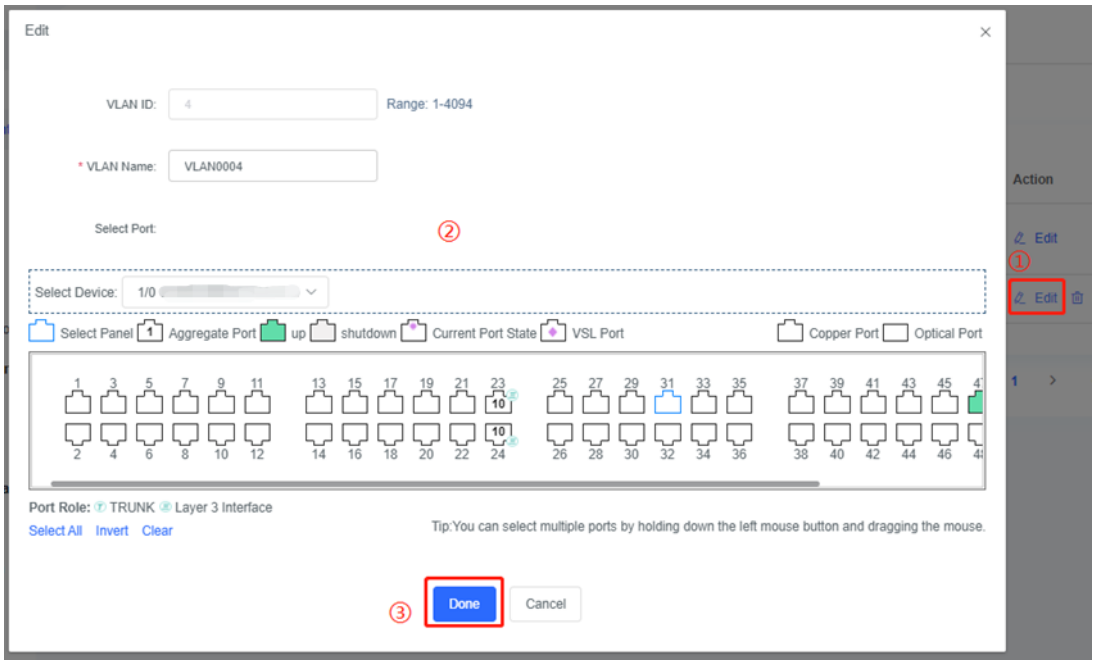
- Deleting multiple VLANs

  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**.



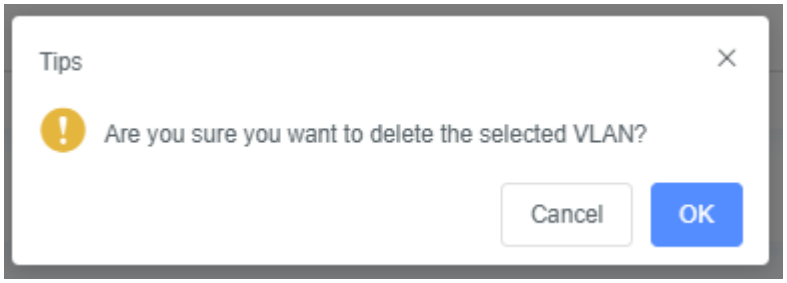
- Editing a VLAN

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

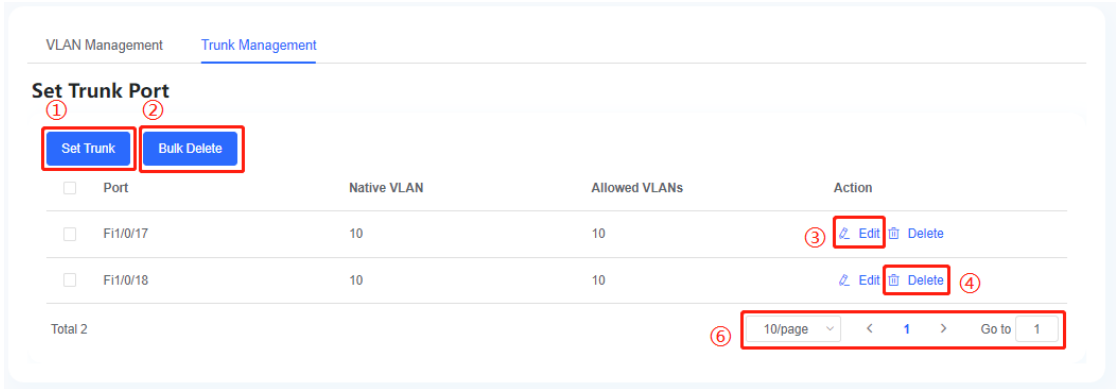


- Deleting a VLAN

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

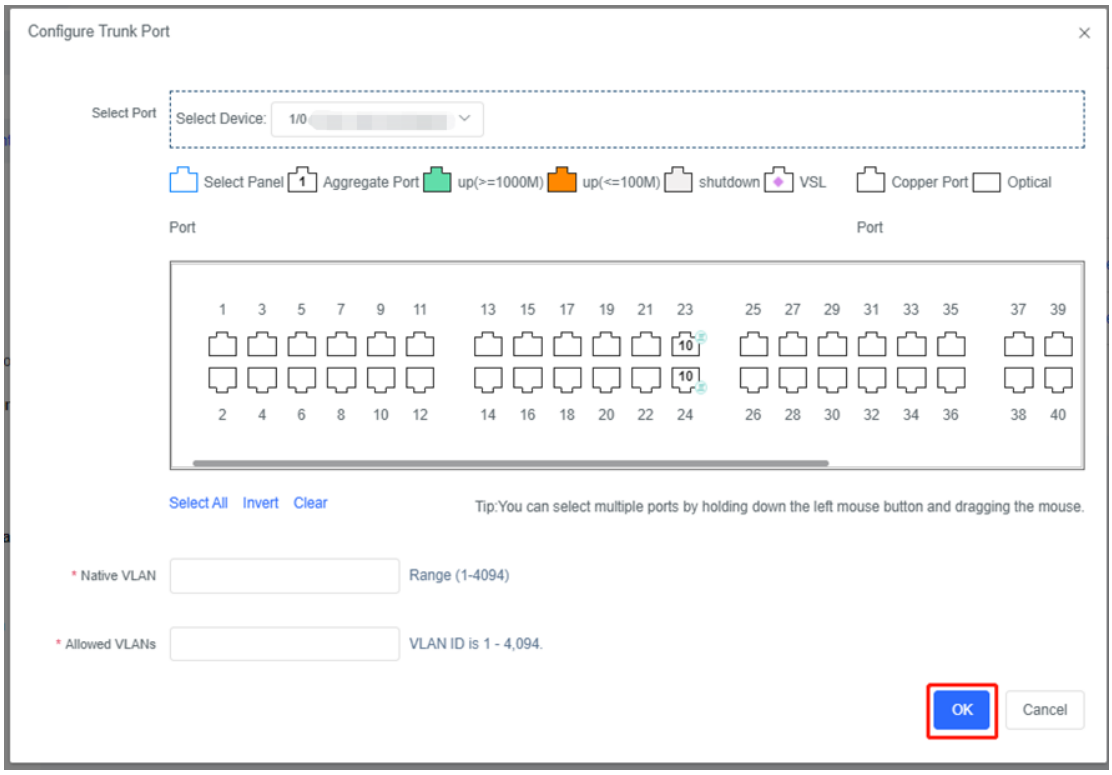


- Trunk Management



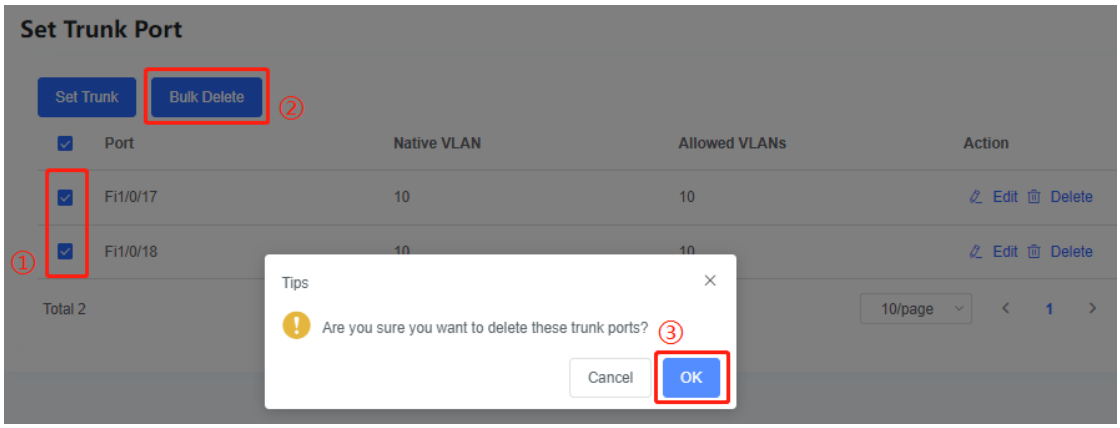
- Setting a Trunk port

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



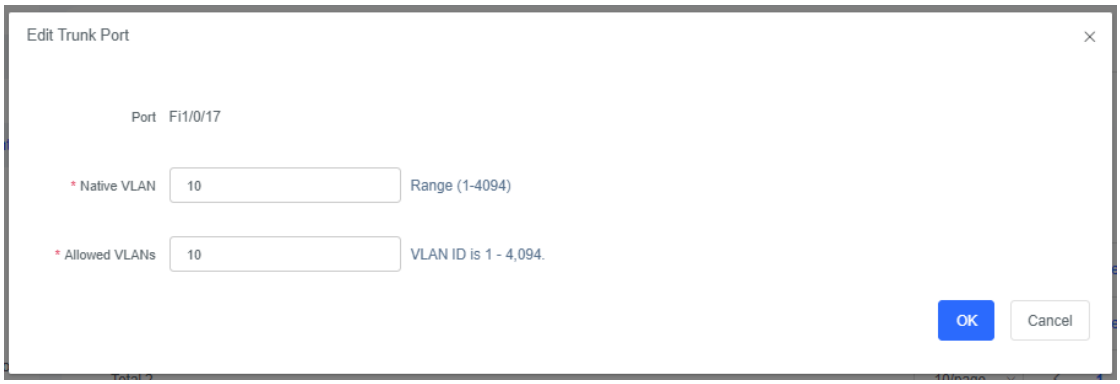
- Deleting multiple trunk ports

  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**.



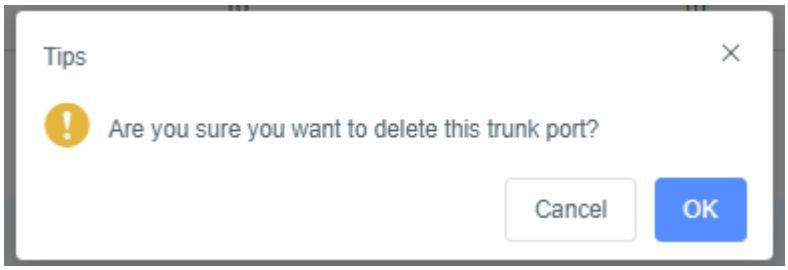
- Editing a trunk port

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



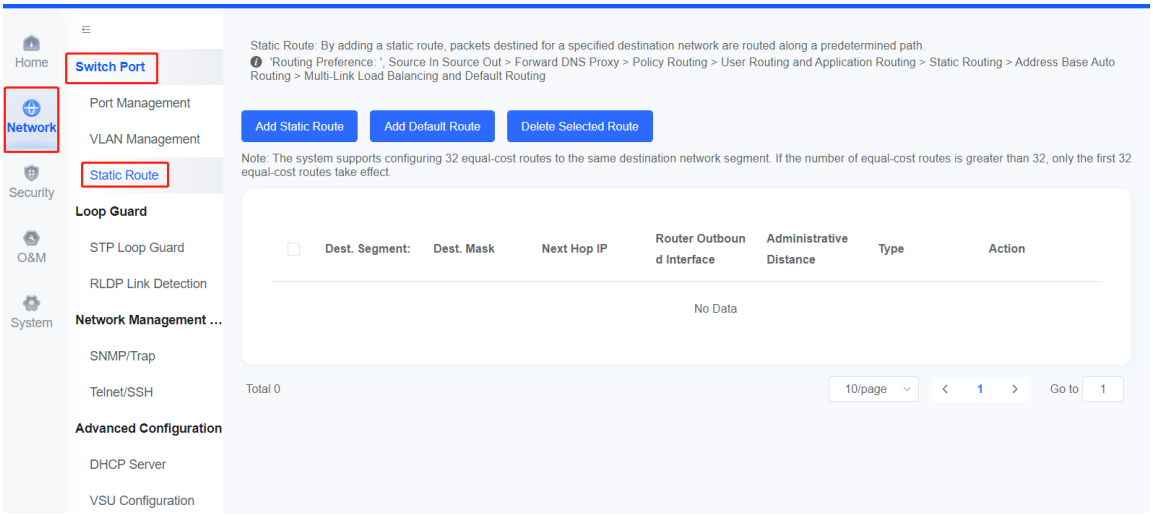
- Deleting a trunk port

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



3. Static Route

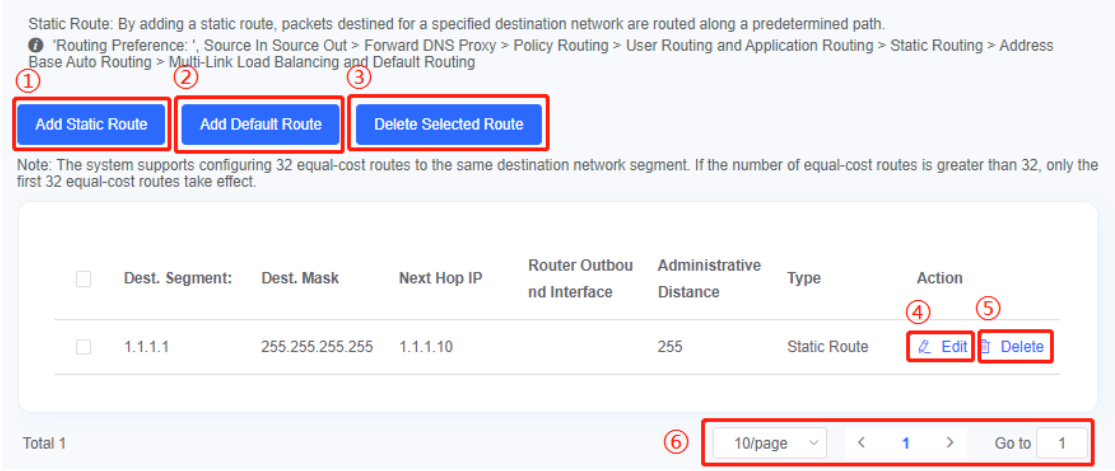
Choose **Network** > **Port Config** > **Static Route** to access the Static Route page.



Packets destined for a specified destination network are routed along a pre-determined path when a static route is configured. The routing priority is source in source out > forward DNS proxy > policy-based routing > user-defined routing and app-based routing > static route > auto routing > multi-link load balancing and default route.

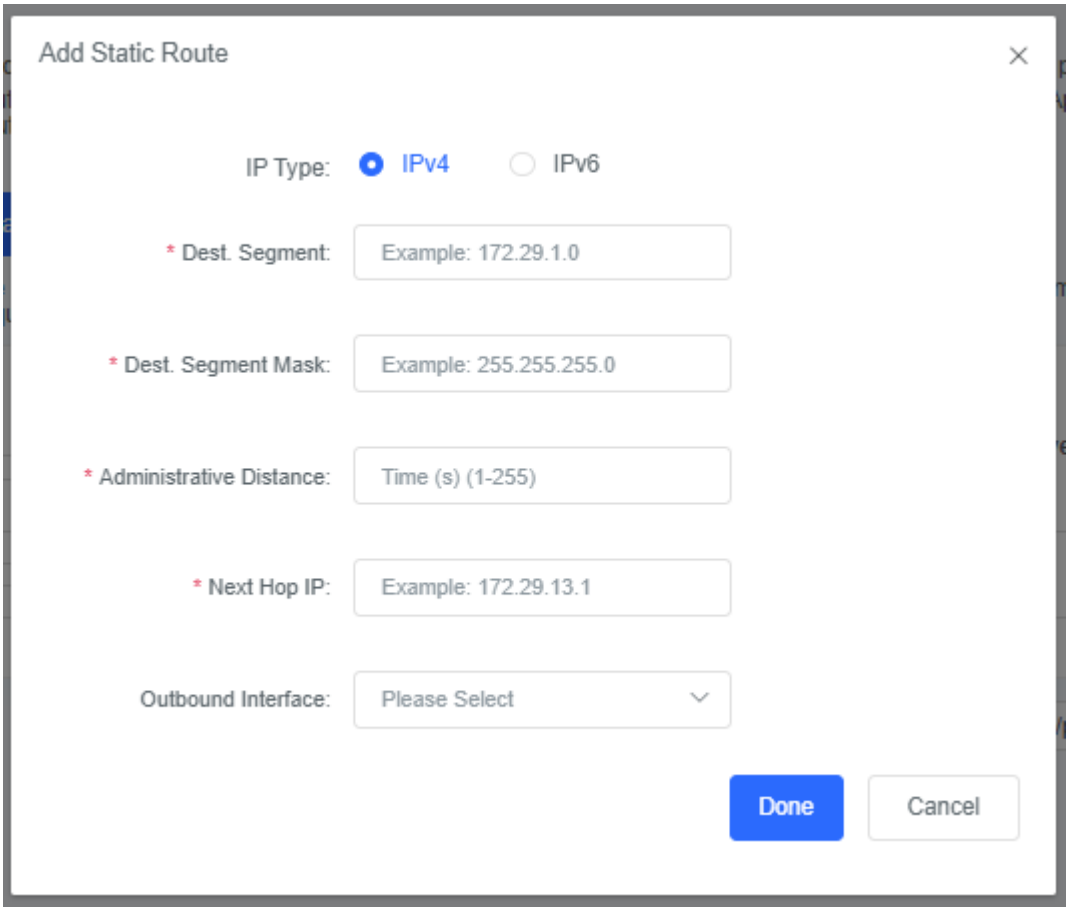
Note

The system supports up to 32 equal-cost routes to the same destination subnet. If over 32 equal-cost routes are configured, only the 32 equal-cost routes that are configured first will take effect.



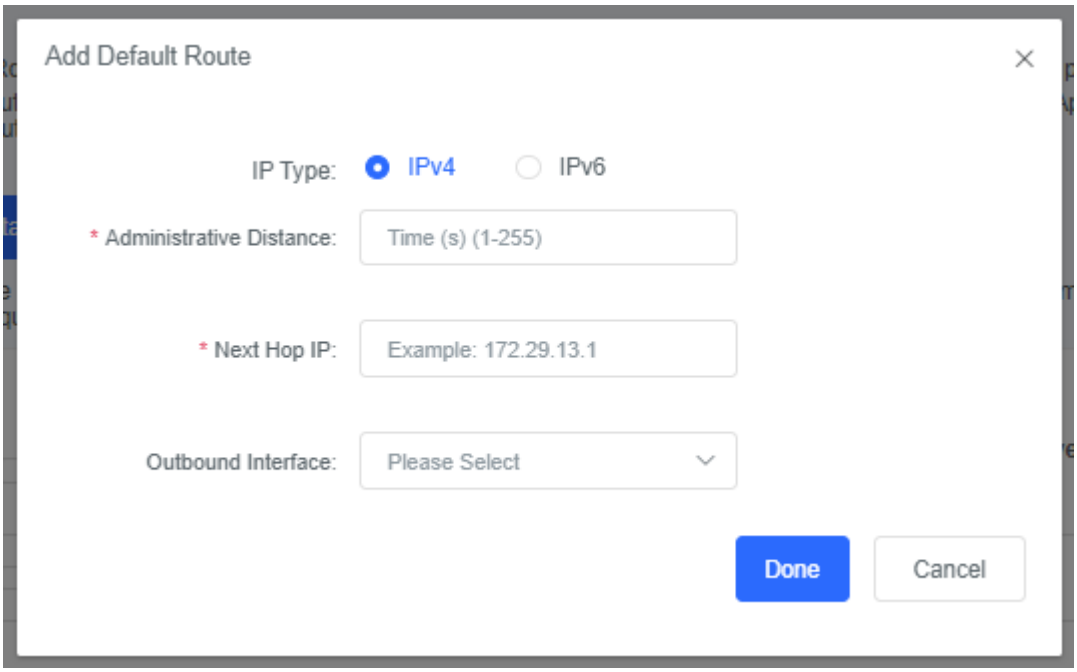
(1) Adding a static route

To add a static route, click **Add Static Route**. The **Add Static Route** window is displayed. Set configuration parameters and click **Done**.



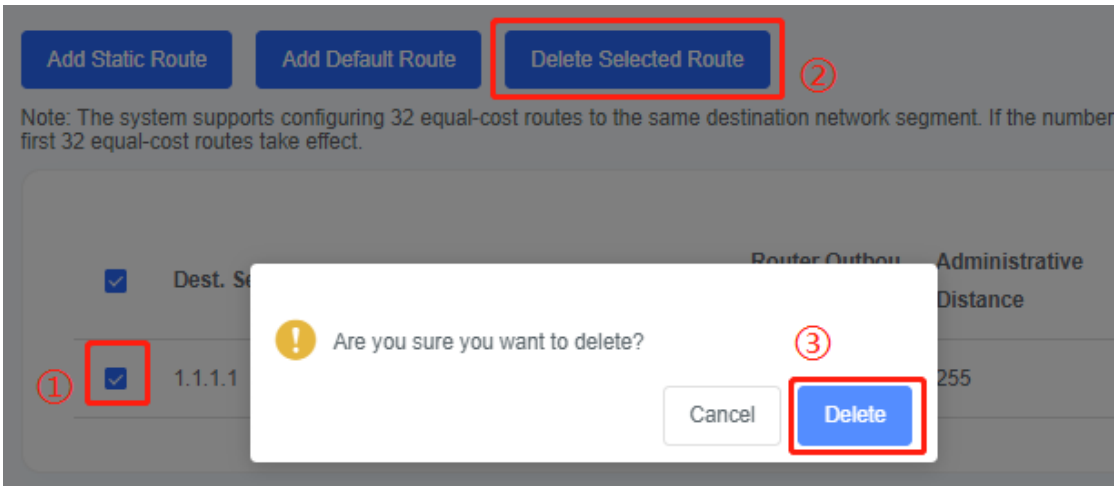
(2) Adding a default route

To add a default route, click **Add Default Route**. The **Add Default Route** window is displayed. Set configuration parameters and click **Done**.



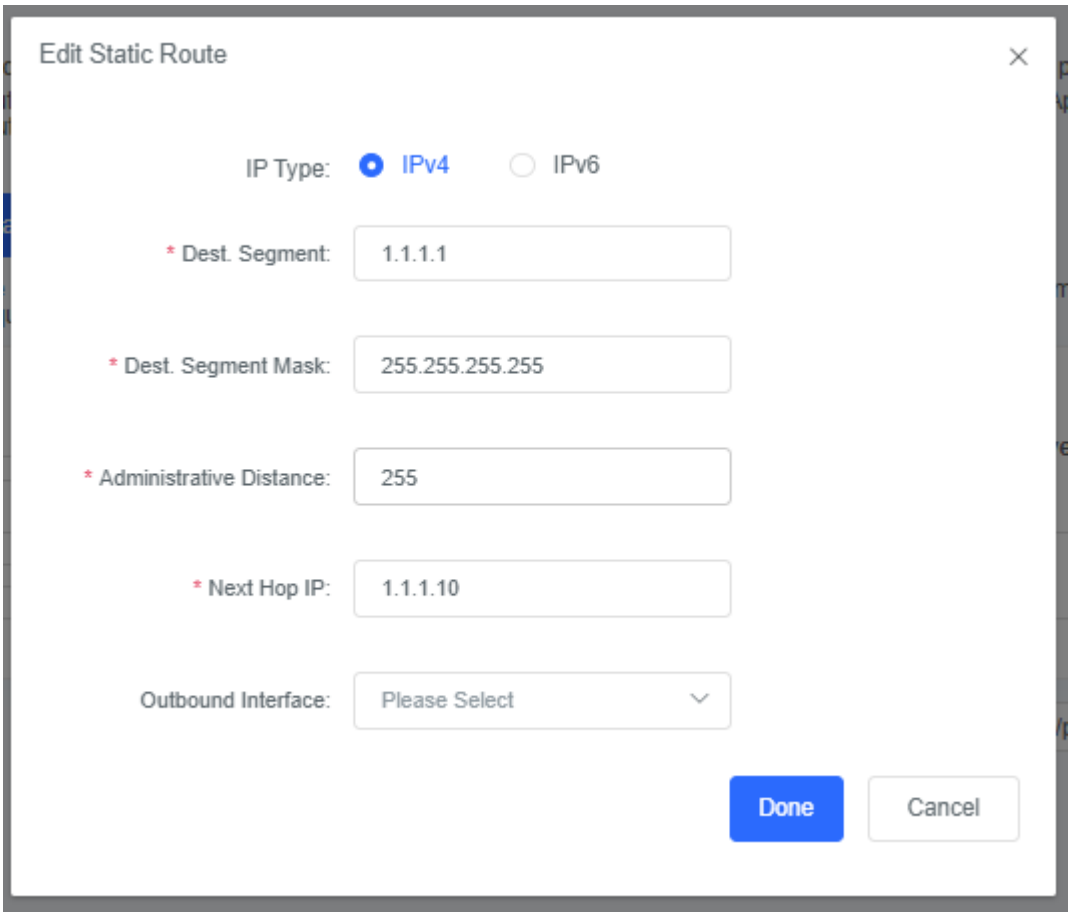
(3) Deleting the selected routes

To delete the selected routes, click black box next to each route to select multiple routes, and then click **Delete selected route**. A dialog box is displayed. Click **Delete**.



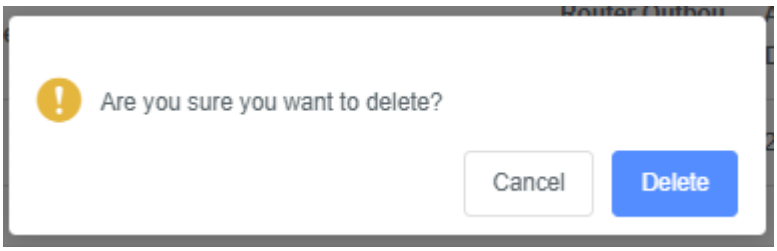
(4) Editing a static route

To edit a route, click **Edit**. The **Edit Static Route** window is displayed. Set configuration parameters and click **Done**.



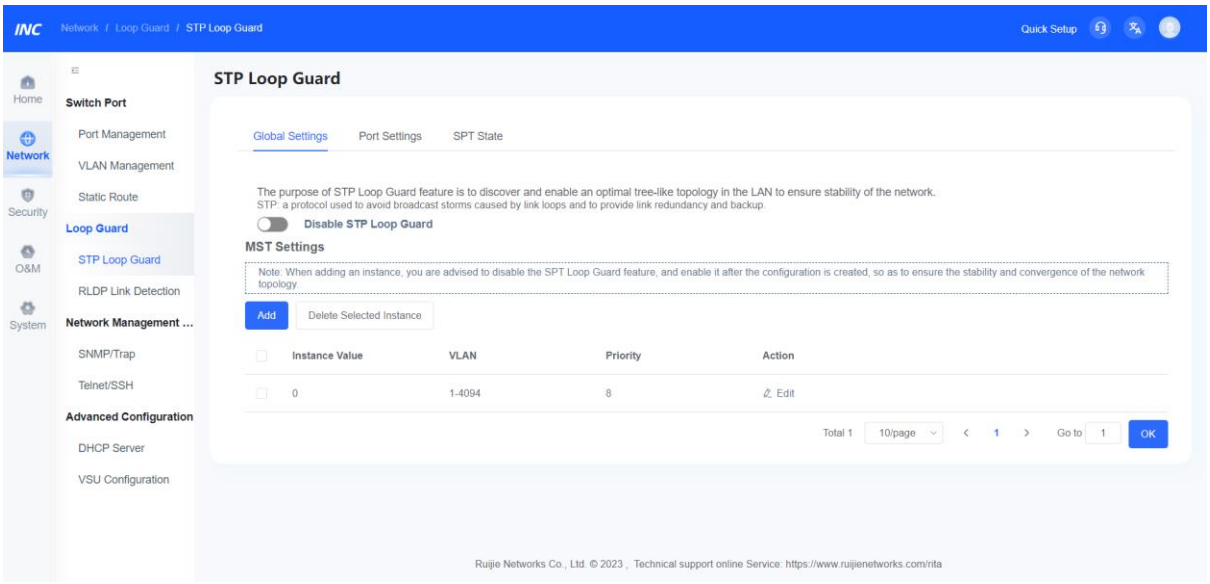
(5) Deleting a static route

To delete a static route, click **Delete**. A dialog box is displayed. Click **Delete**



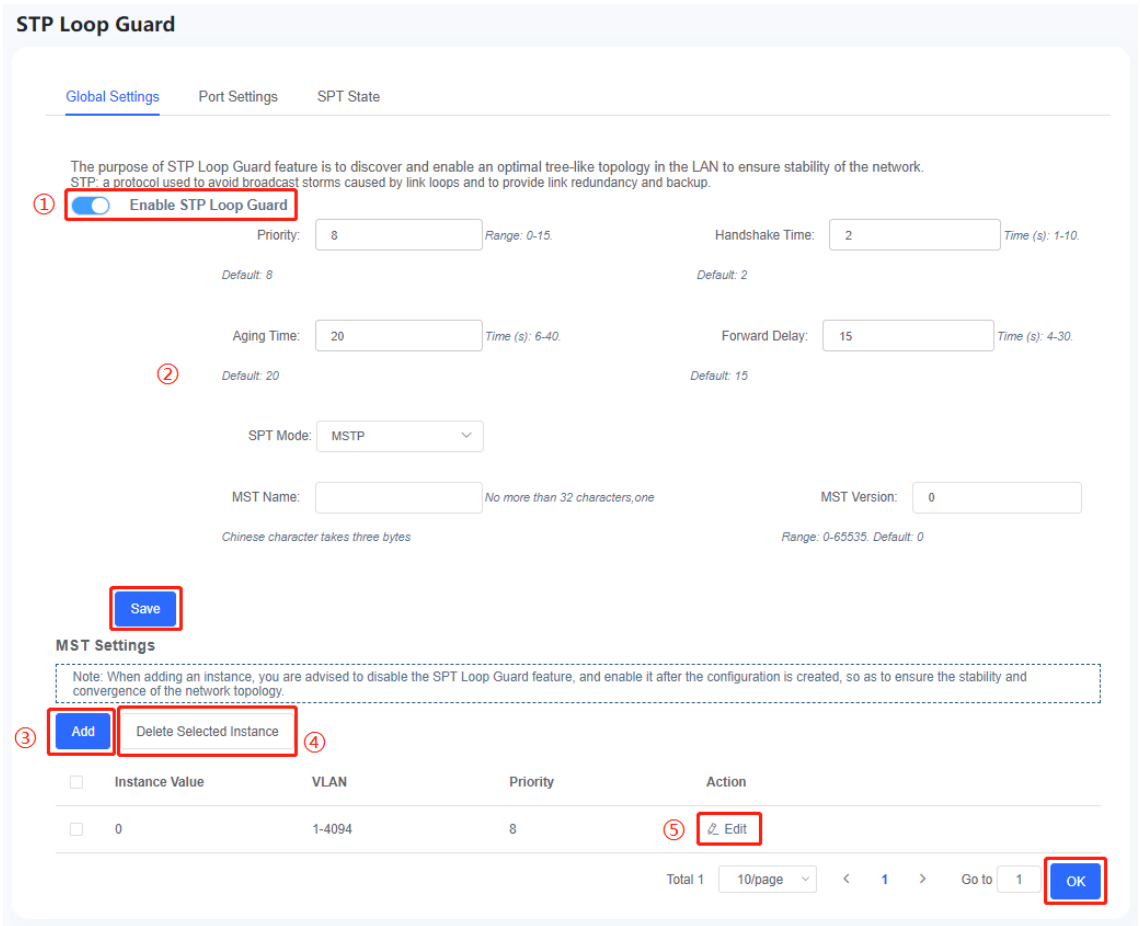
3.5.2 Loop Guard

1. STP Loop Guard



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

(1) 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 instancs: Click **Delete Selected instance** to delete instances.

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

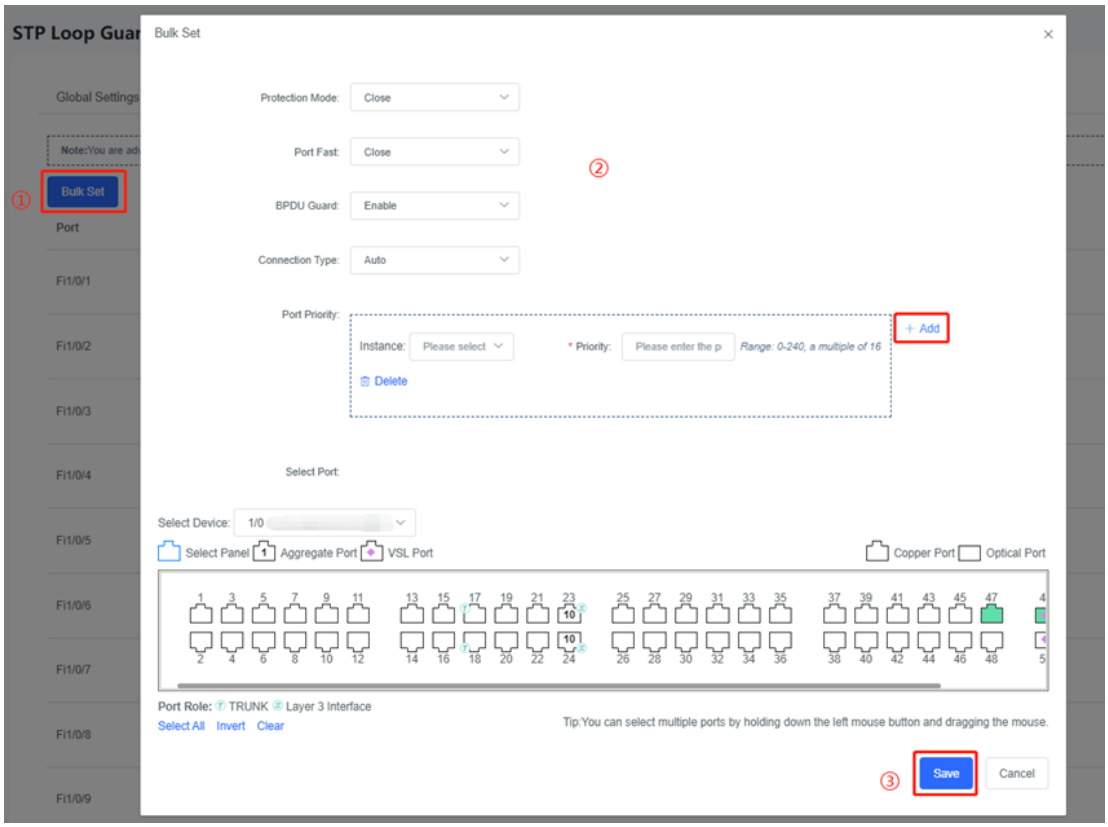
(2) Port Settings

Note

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

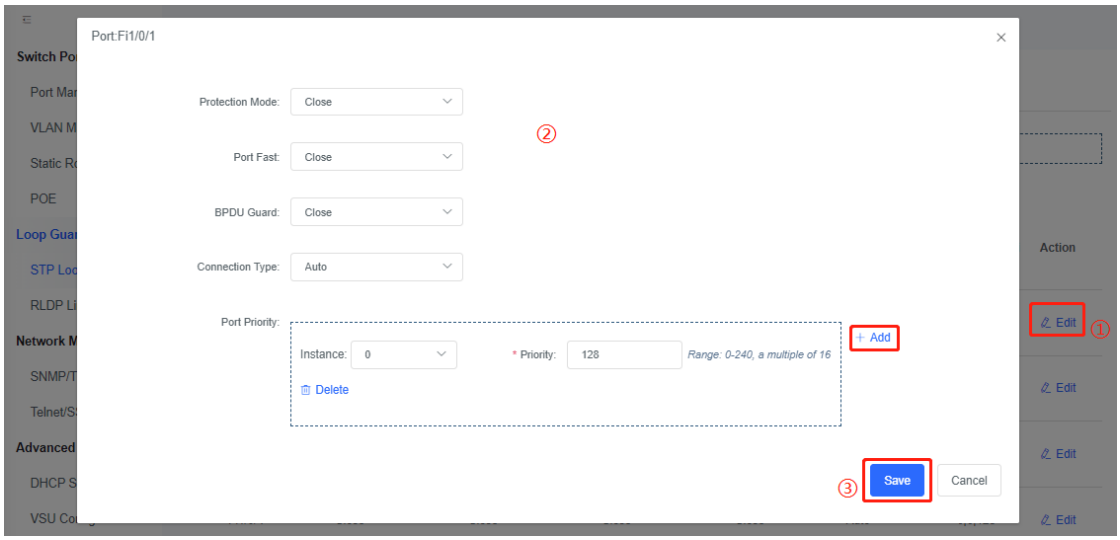
- Setting the STP loop guard function for multiple ports

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



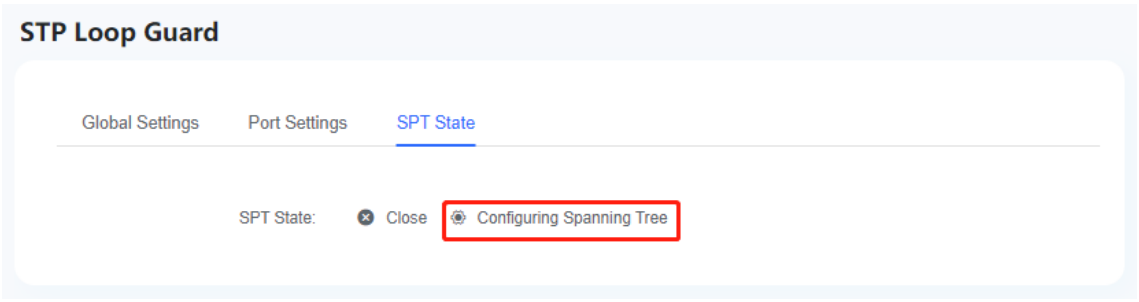
- Editing the STP loop guard function for a single port

  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.



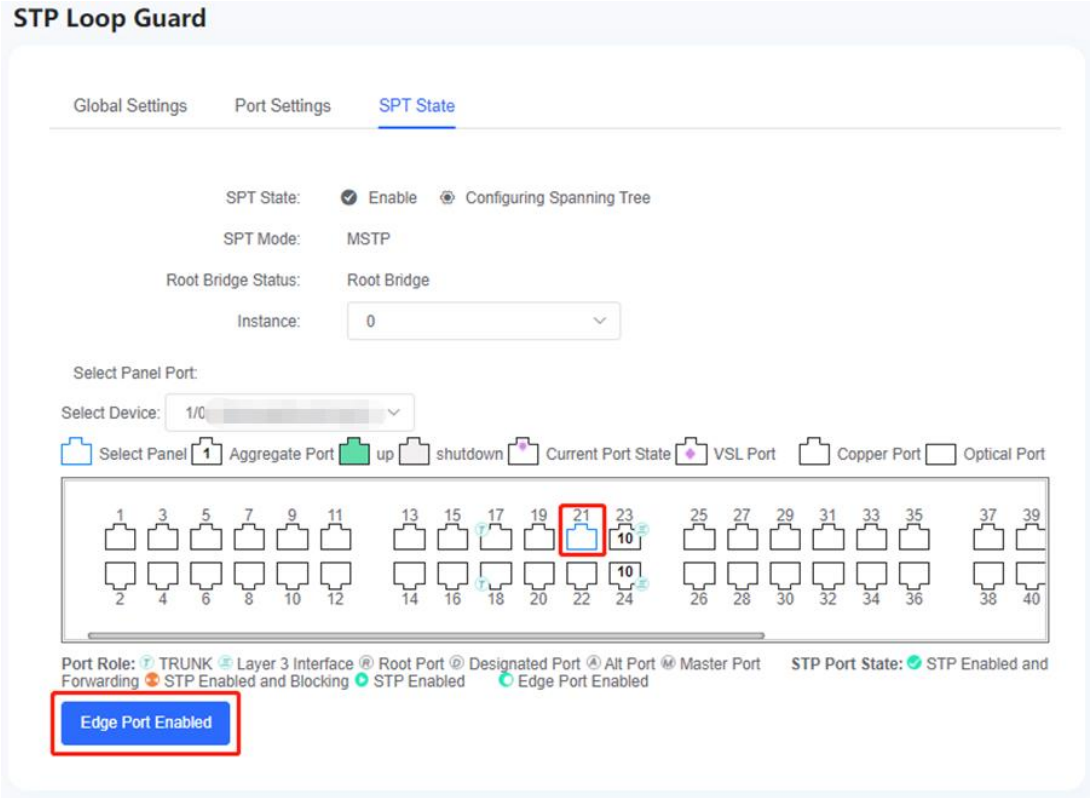
(3) STP State

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



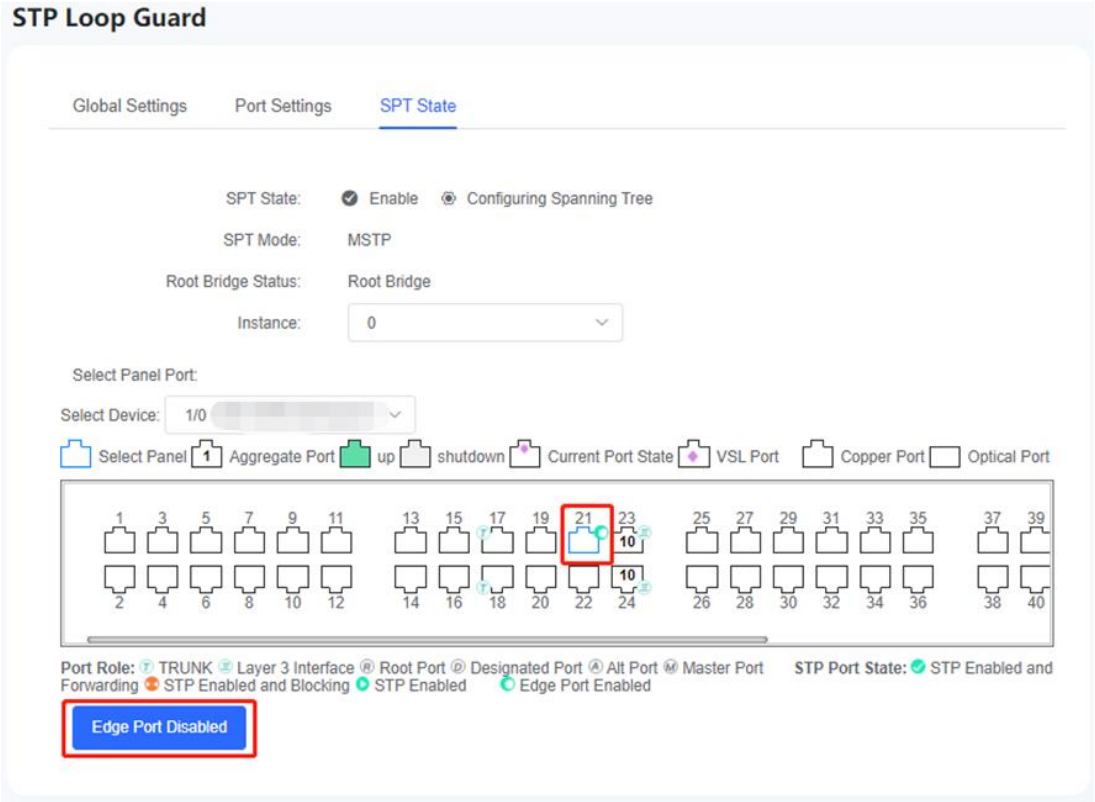
- Disable Edge Port

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



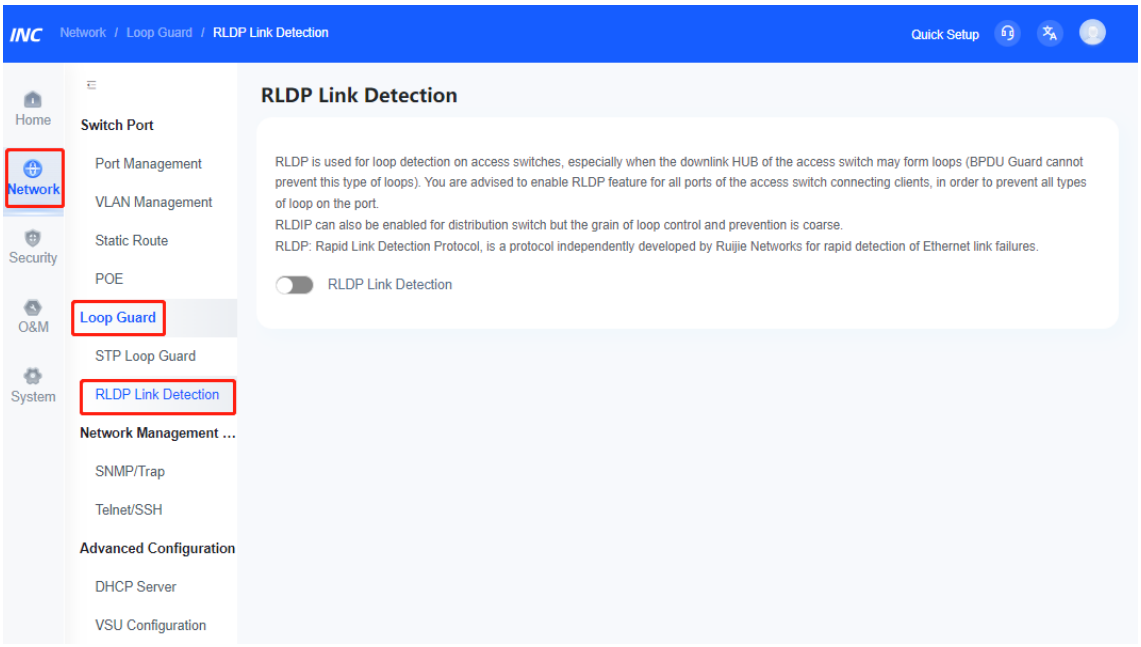
- Enable Edge Port

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

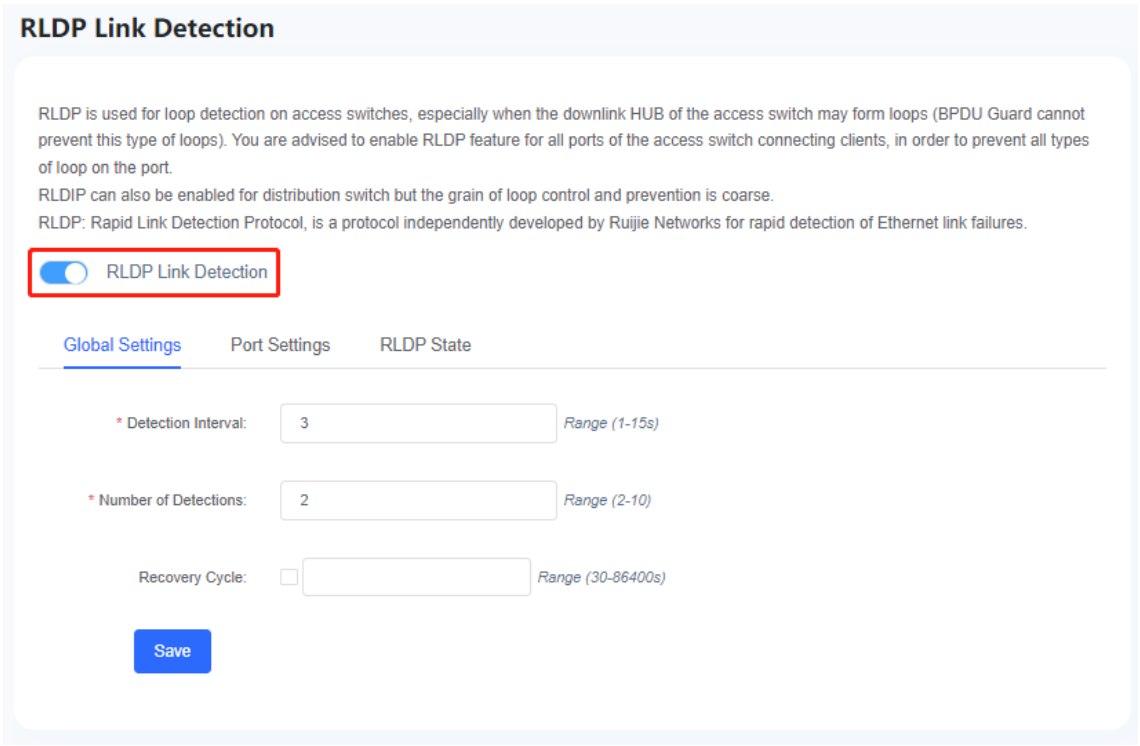


2. RLDP Link Detection

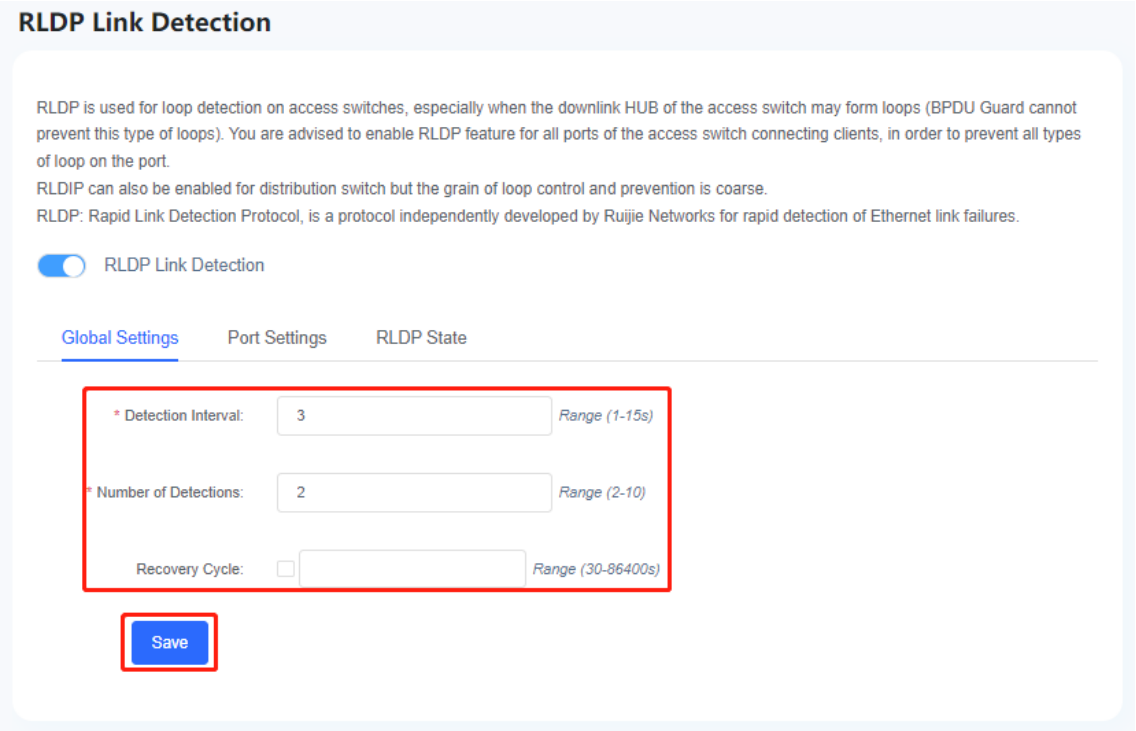
Choose **Network** > **Loop Guard** > **RLDP Link Detection** to access the **RLDP Link Detection** page.



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



(1) Global Settings

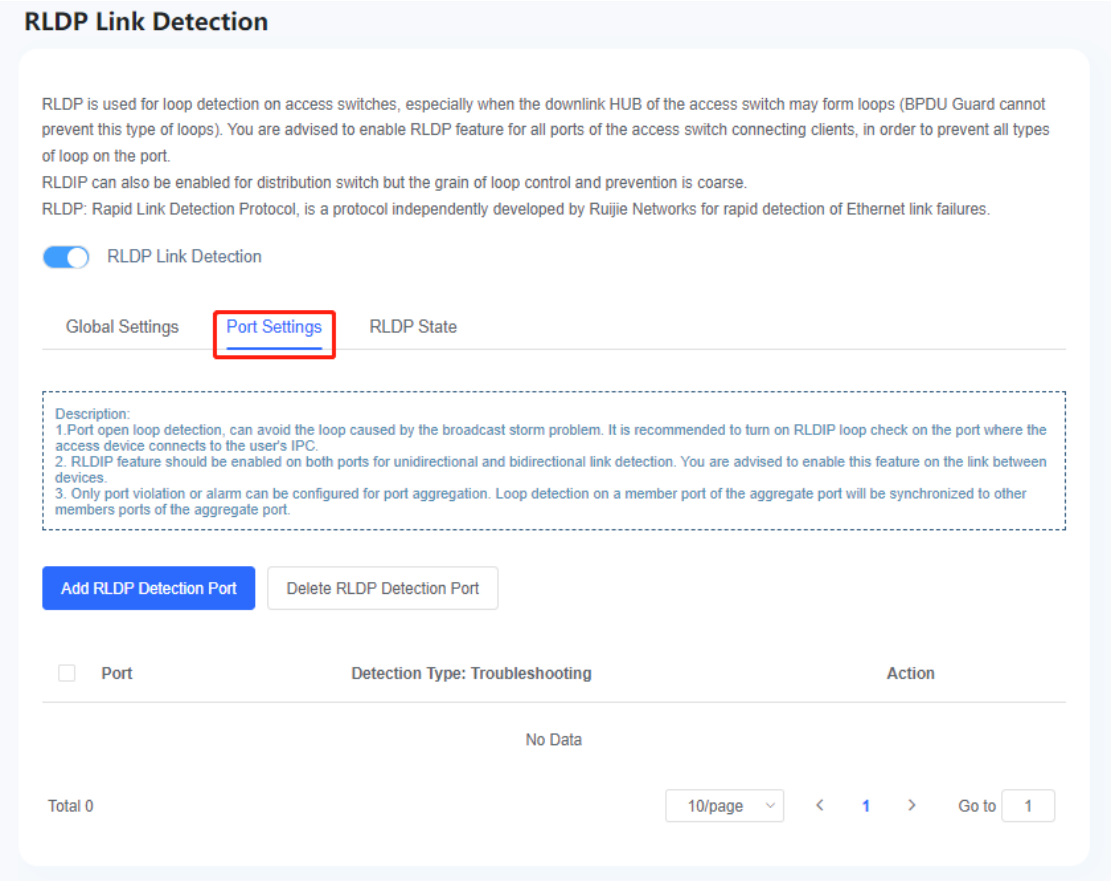


- **Save**: After you have entered the detection interval, number of detections, and restoration cycle (optional), click **Save** to save the global settings.

(2) Port Settings

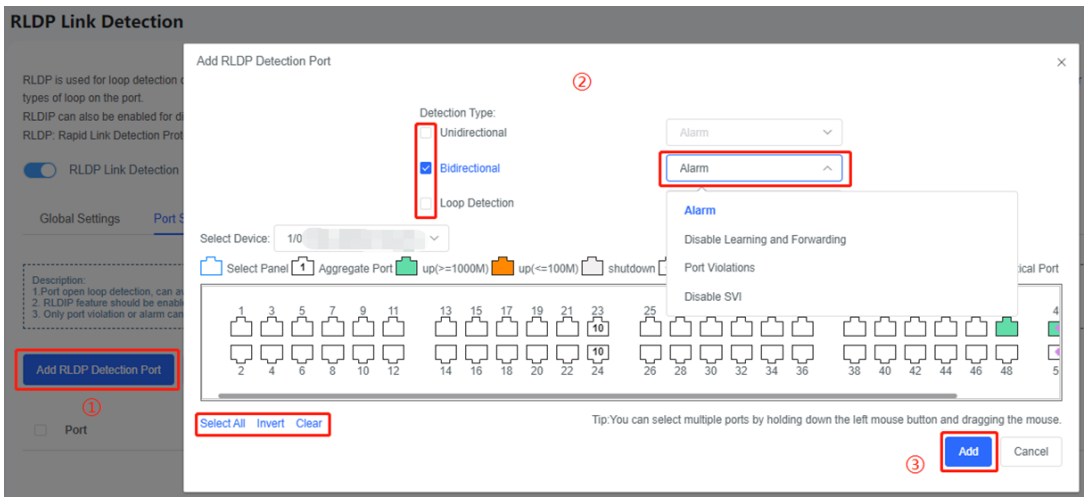
Notes

- 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 members ports of the aggregate port.



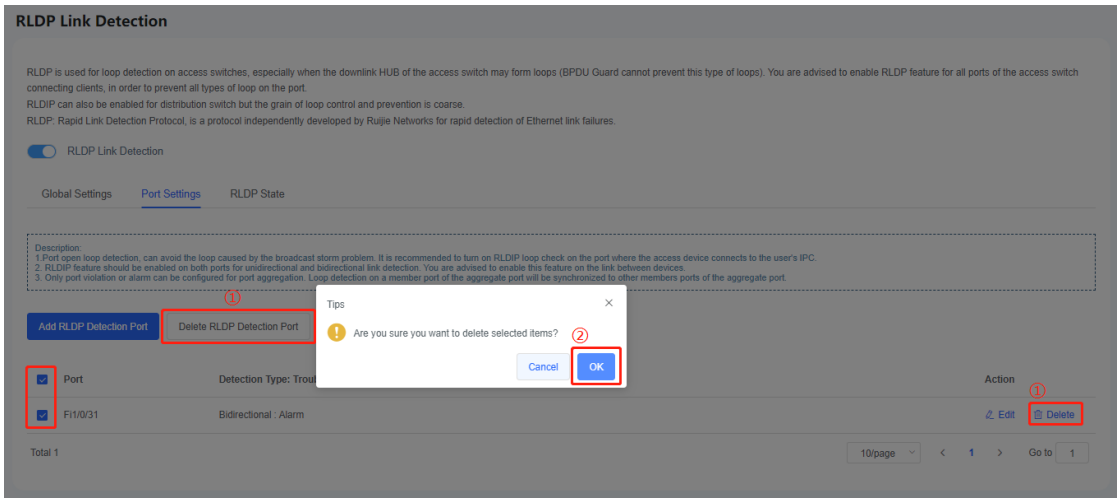
- Adding an RLDP detection port

  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.

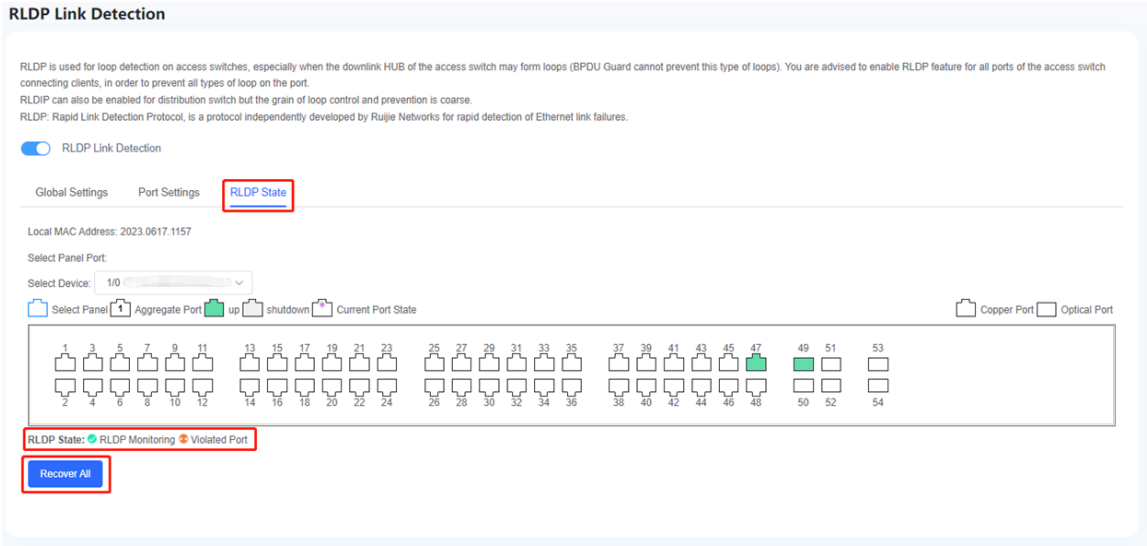


- Delecting RLDP detection ports

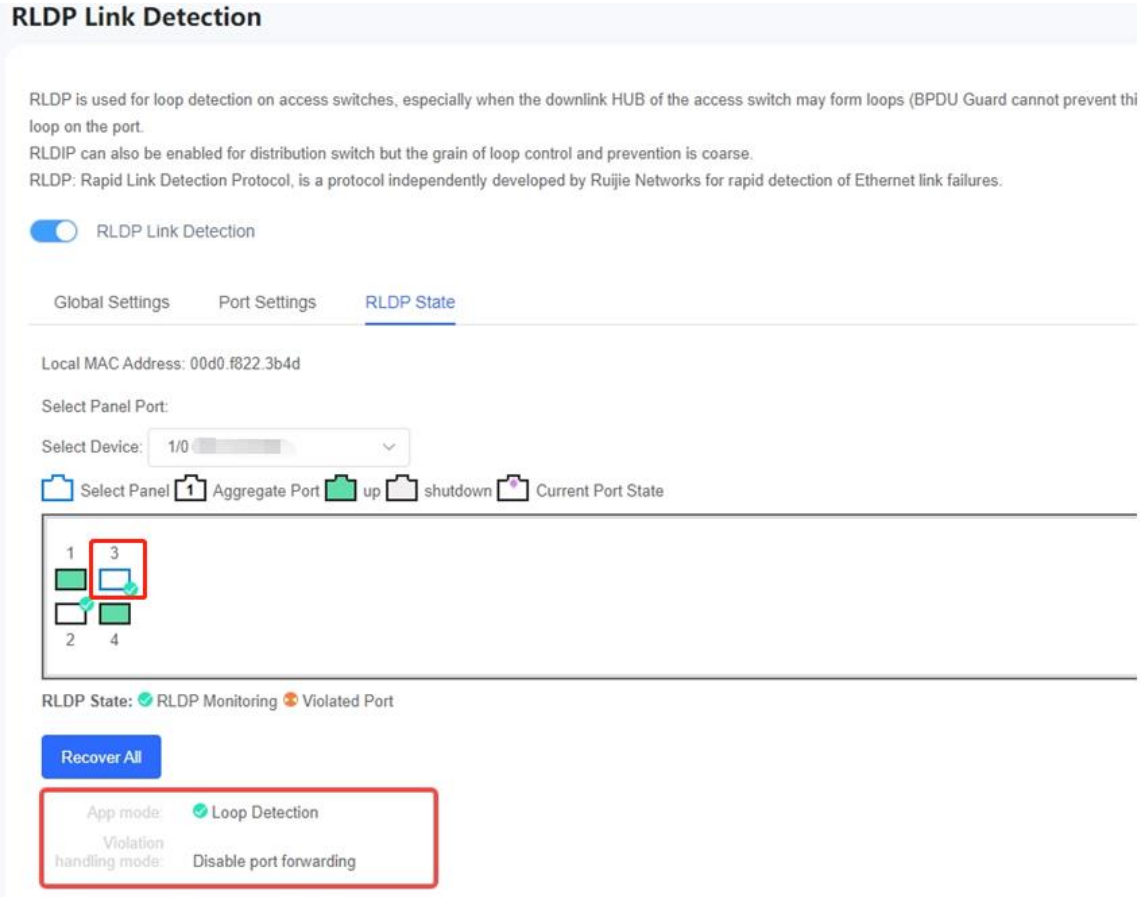
  Select one or multiple ports. Click **Delete** or **Delete RLDP Detection Port** to delete the selected ports.



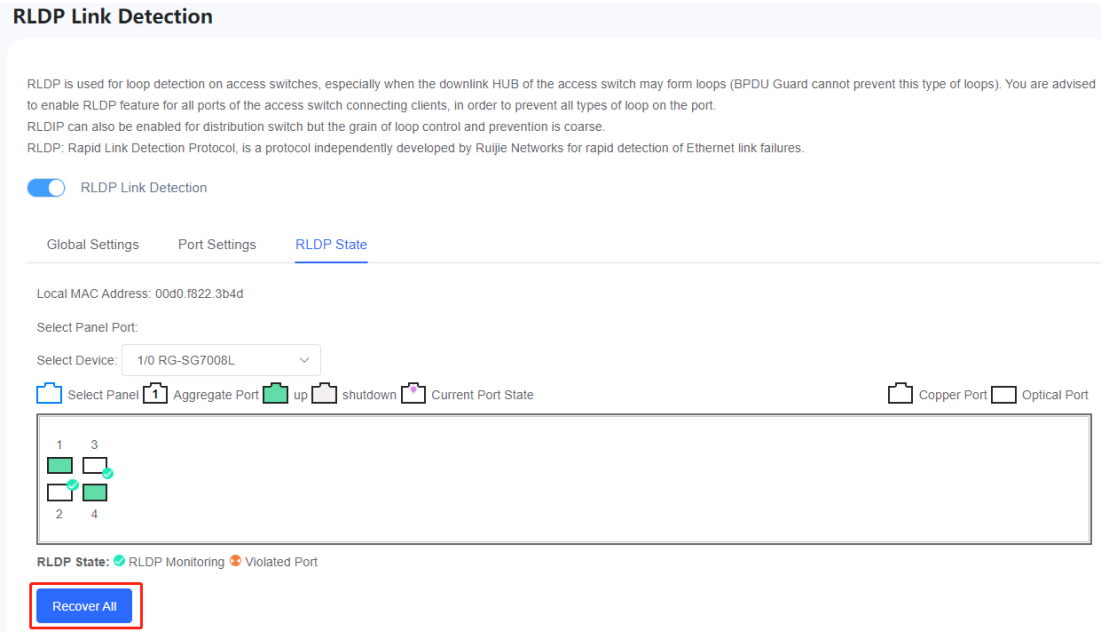
(3) RLDP State



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



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

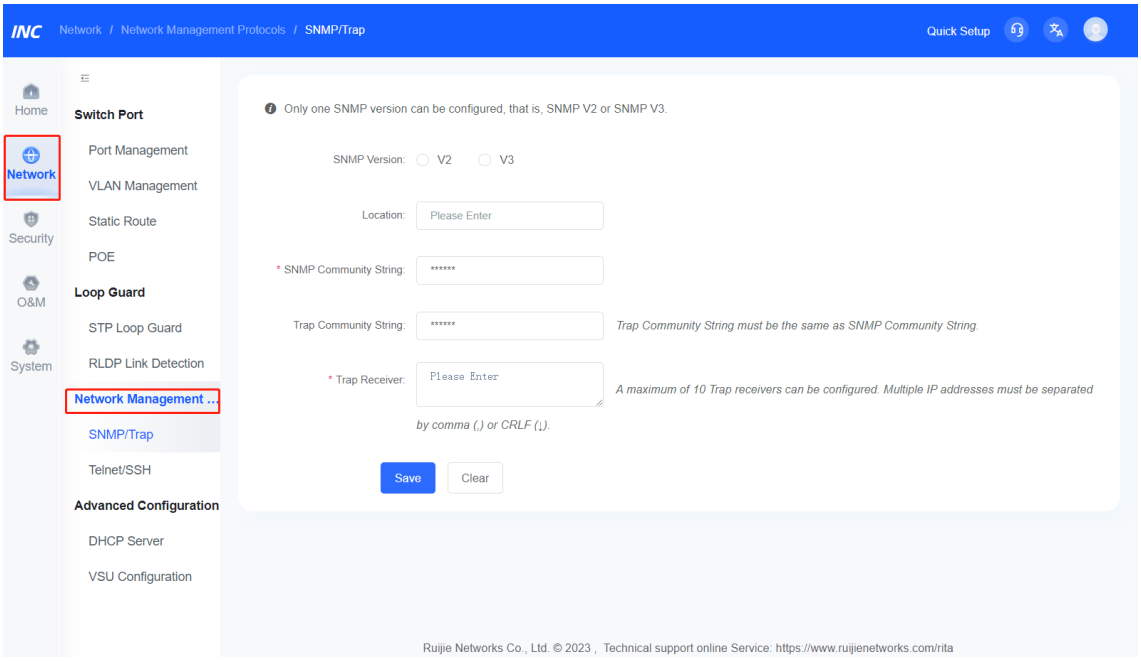


3.5.3 Network Management Protocols

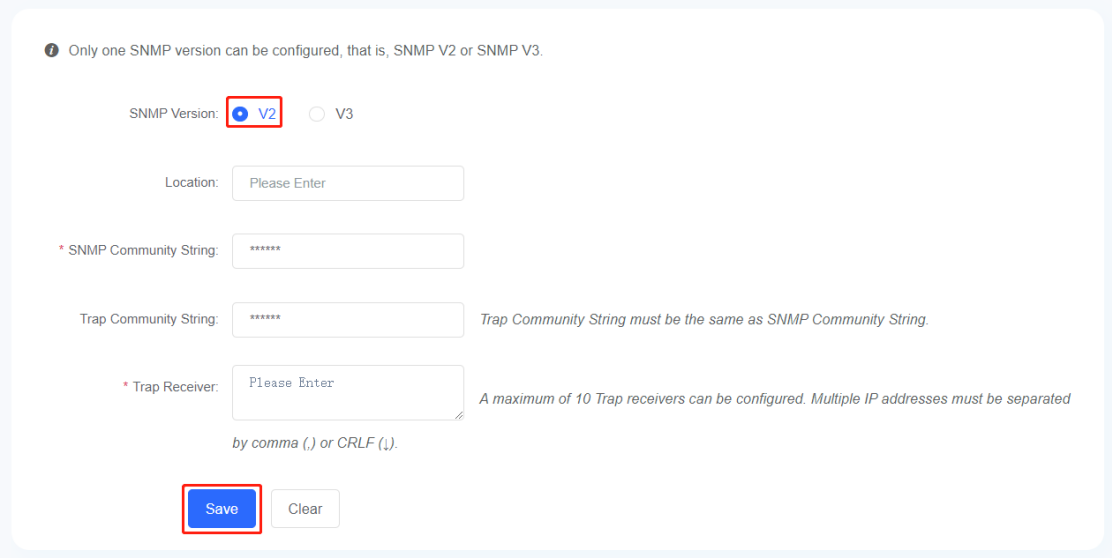
1. SNMP/TRAP

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

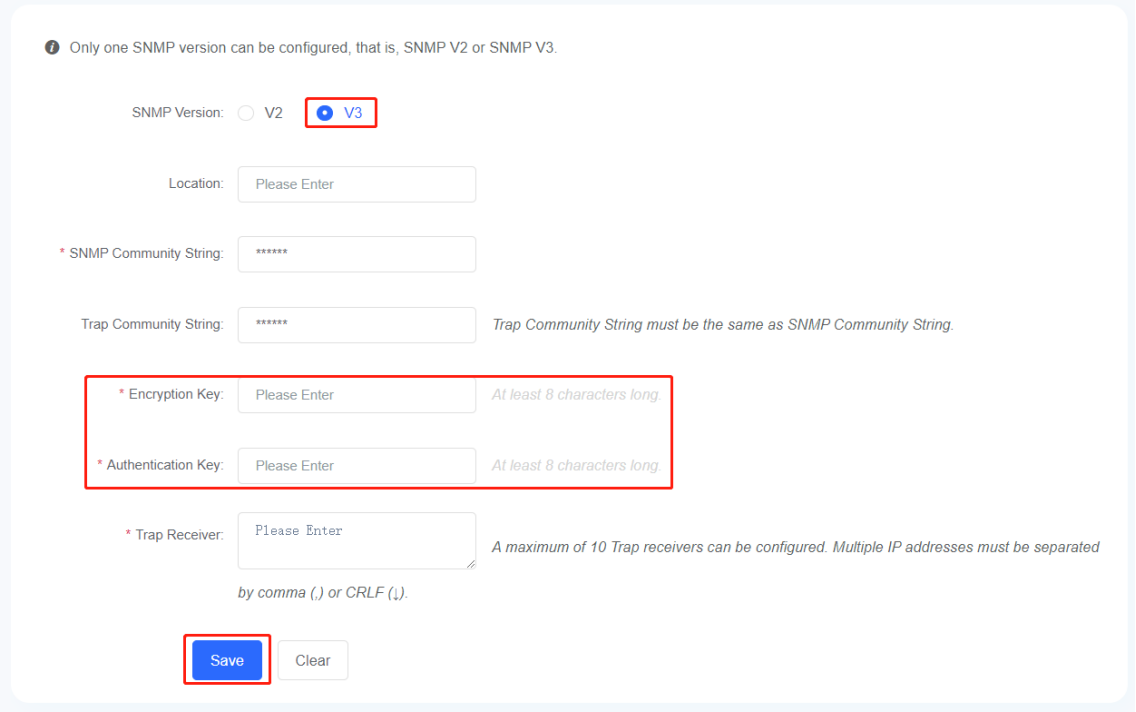
The Simple Network Management Protocol (SNMP) enables a network administrator to easily monitor and manage nodes on a network.



- SNMP Version: indicates the SNMP version supported by the switch, which can be SNMPv2 or SNMPv3.
- Location: indicates the location the switch.
- SNMP Community String: is used by the management host to connect to a switch.
- Trap Community String: is used to connect to the management host. When an alarm is generated on a switch, 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.

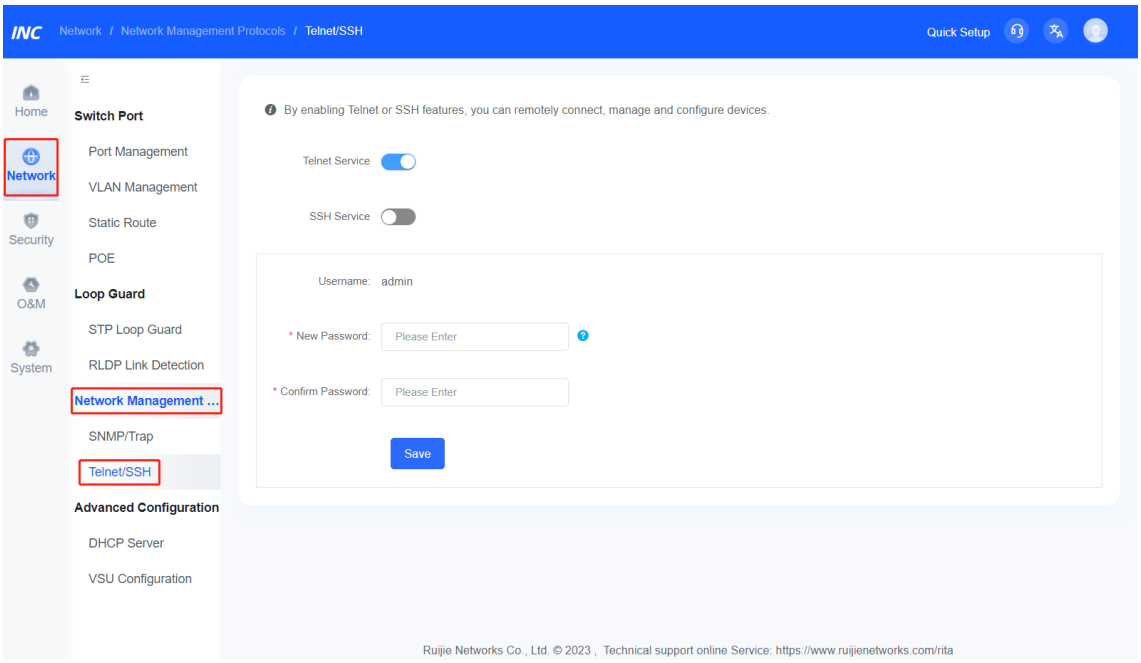


- **SNMP V2**: Select **V2**. Set configuration parameters and click **Save** to submit the configuration.
- **SNMP V3**: Select **V3**. Set configuration parameters and click **Save** to submit the configuration.
- **Clear**: Click **Clear** to clear the SNMPv2 or SNMPv3 configuration.



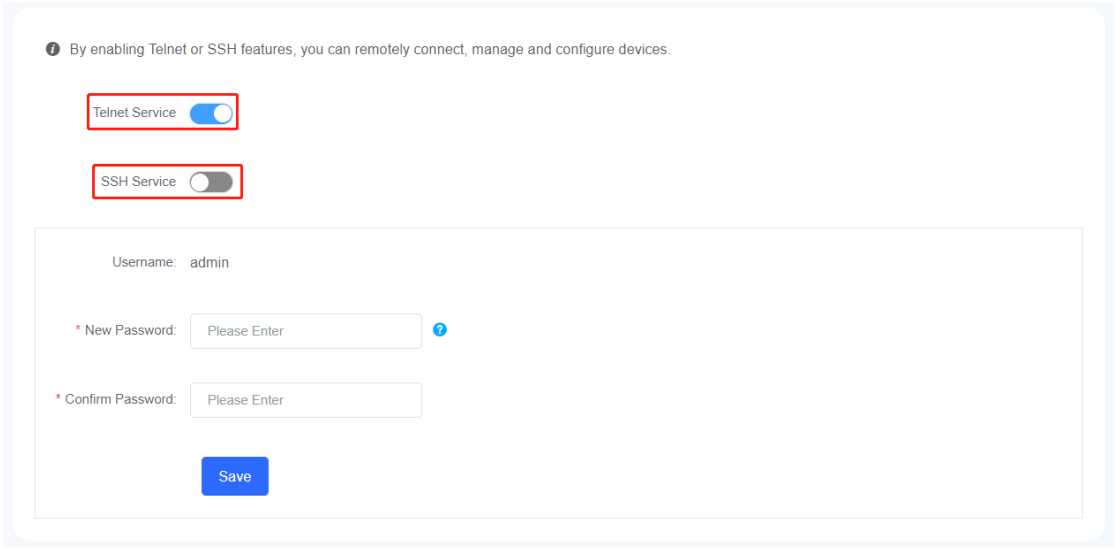
2. Telnet/SSH

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



Telnet/SSH: Click **TeInte 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.



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

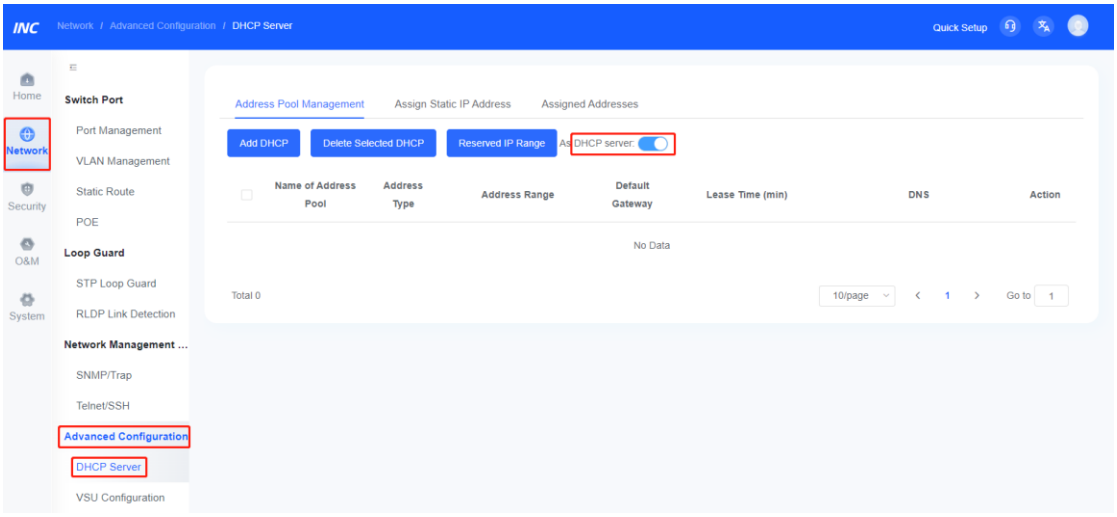
Note

Remember the new password for login next time.

3.5.4 Advanced Configuration

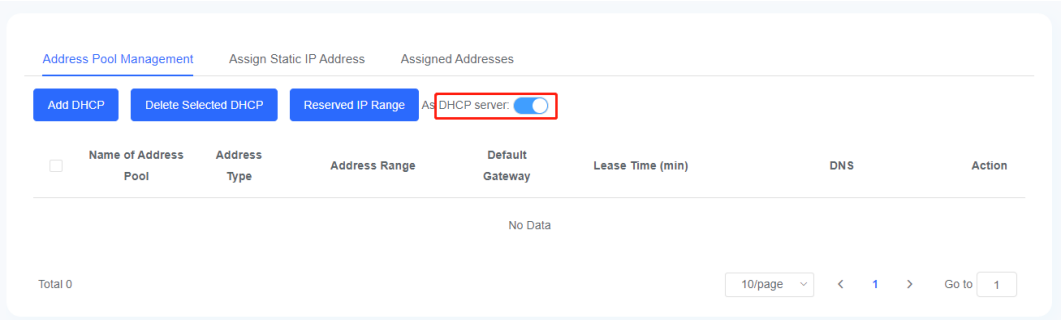
1. DHCP Server

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

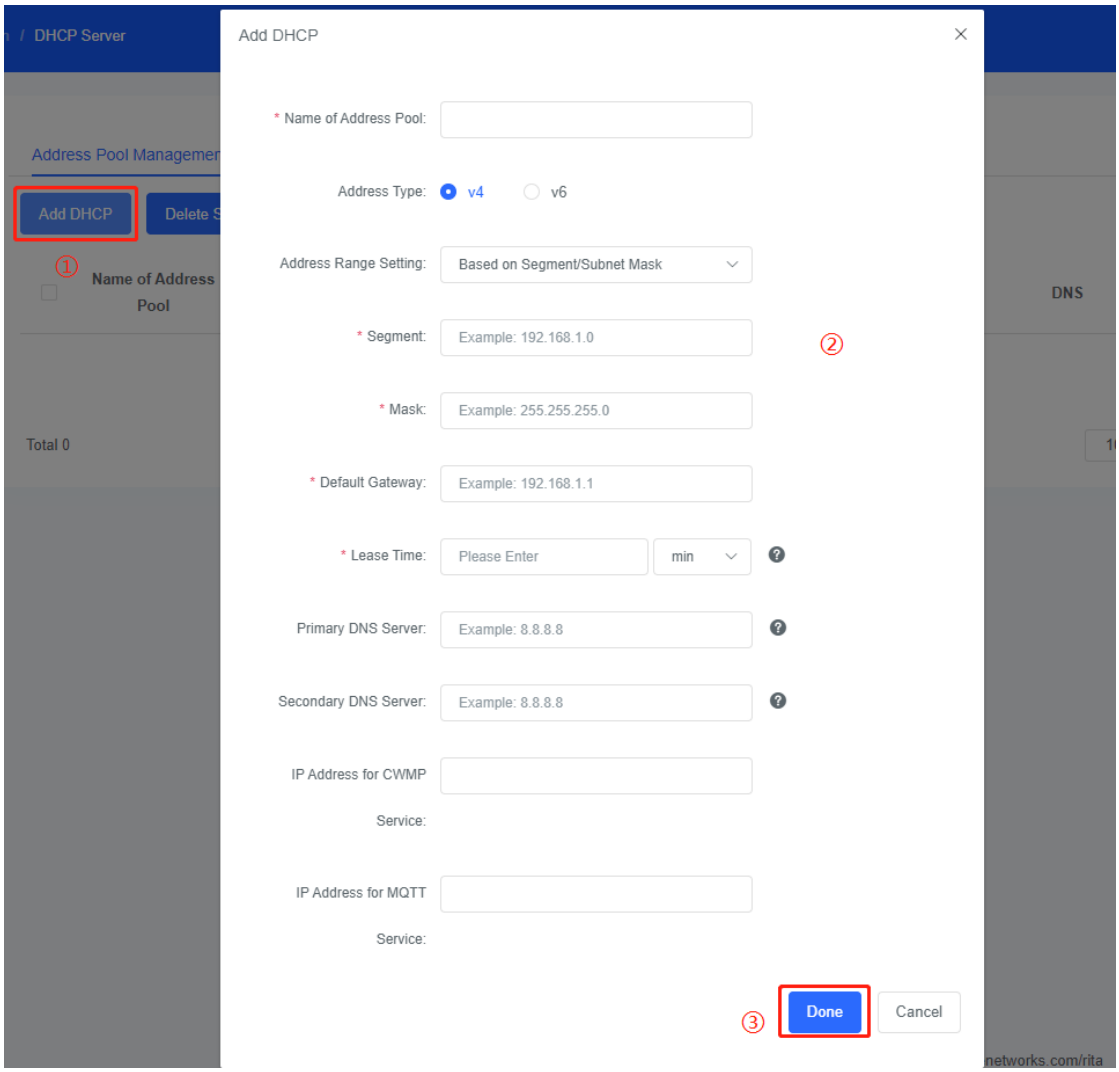


(1) Address Pool Management

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



- Adding a DHCP address pool

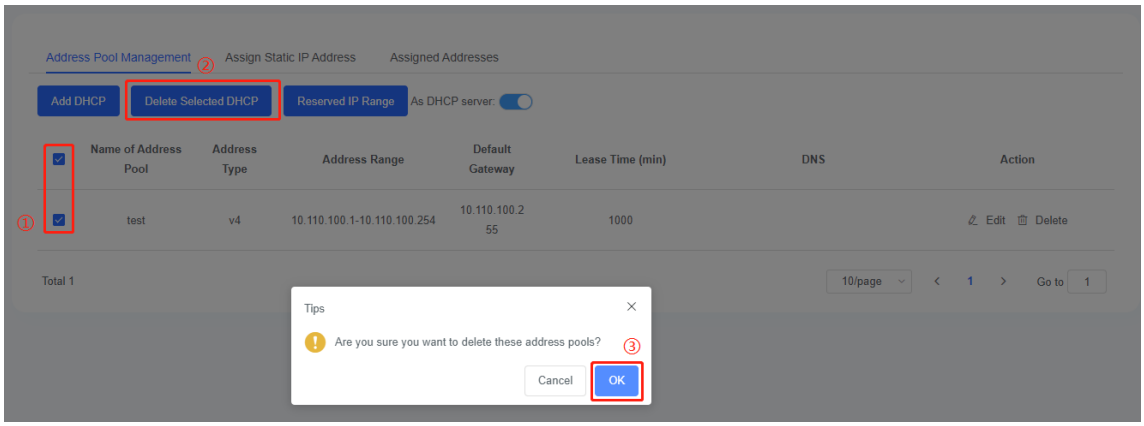


a Click **Add DHCP**.

b Set configuration parameters in the displayed windows.

c Click **Done**. The result will be displayed in the list.

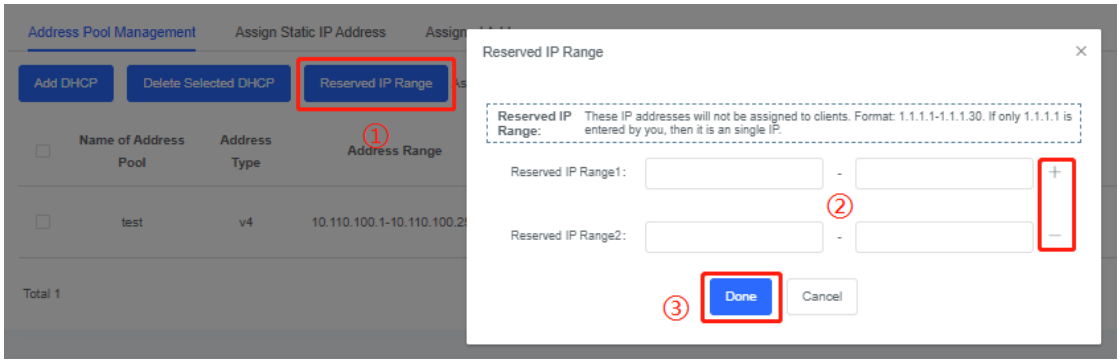
- Deleting the selected DHCP address pool



a Click **Delete Selected DHCP**.

b Click **OK**. The selected DHCP address pool is deleted.

- Configuring the reserved IP range

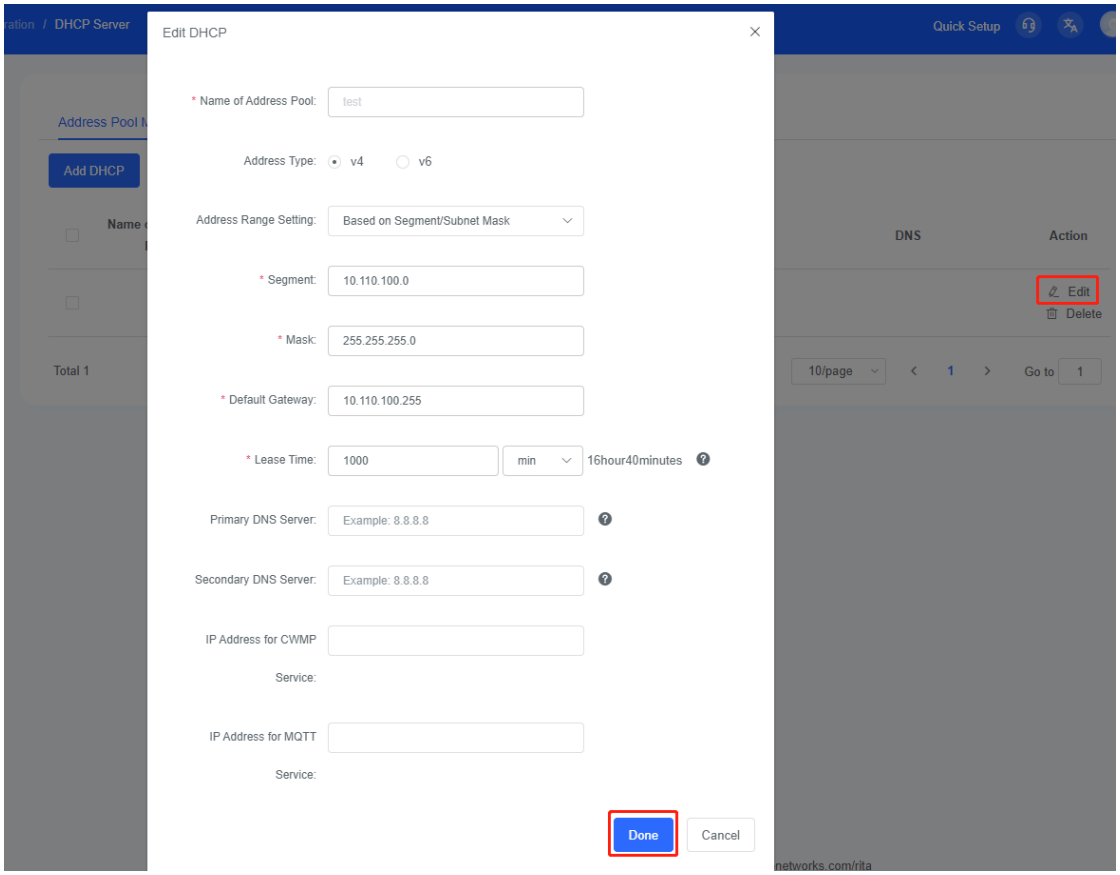


a Click **Reserved IP Range**.

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.

- Editing a DHCP address pool

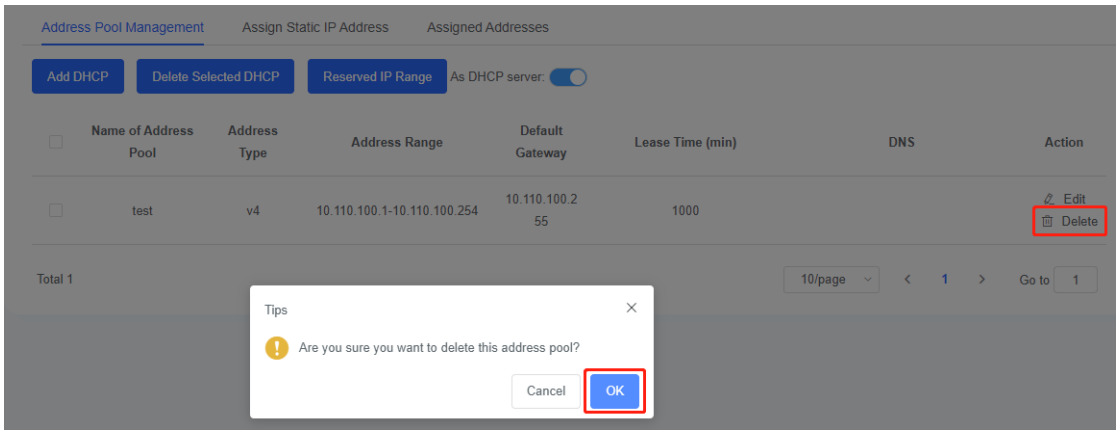


a Click Edit.

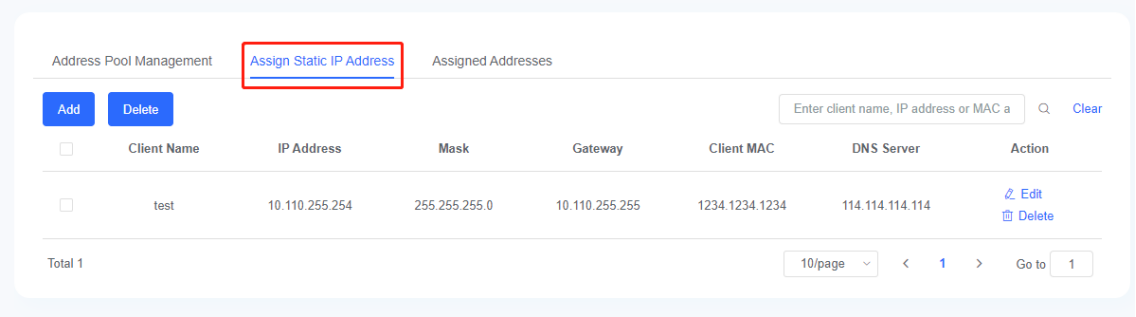
b Set configuration parameters in the displayed windows.

c Click Done. The result will be displayed in the list.

- Deleting a DHCP address pool

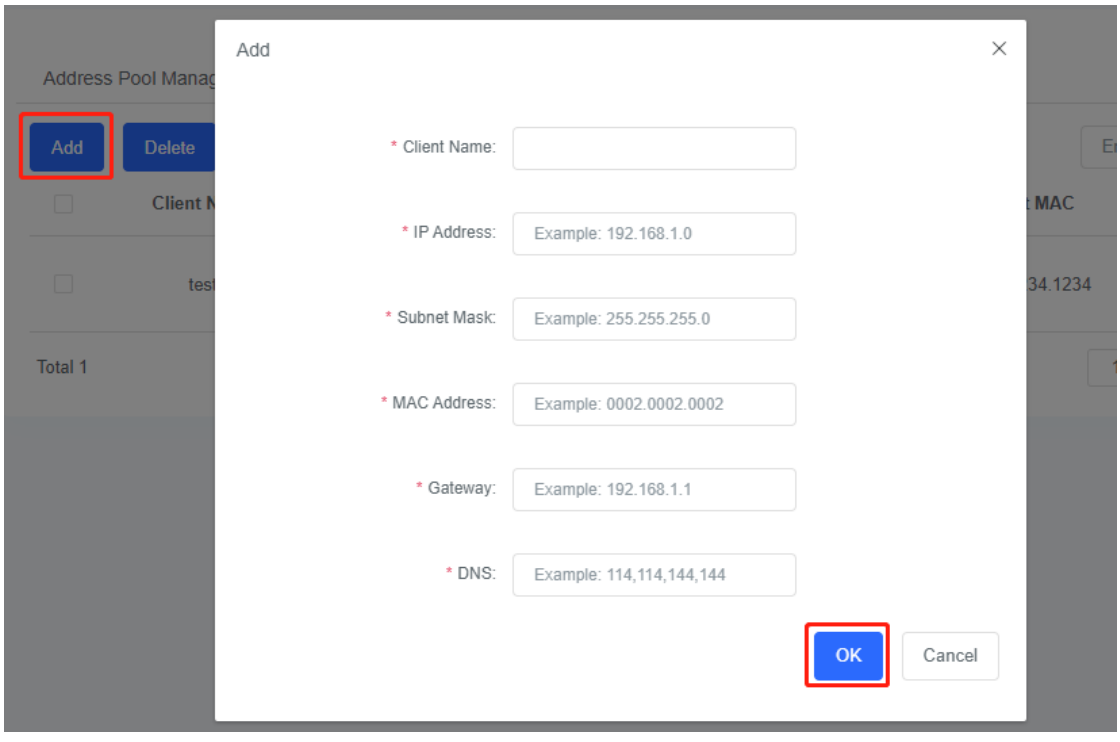


(2) Assign Static IP Address



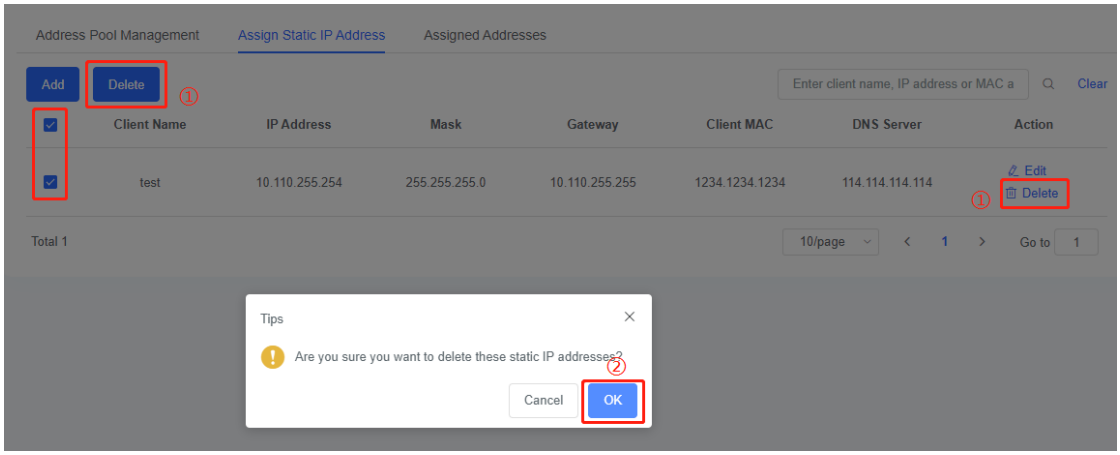
- Adding a static IP Address

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



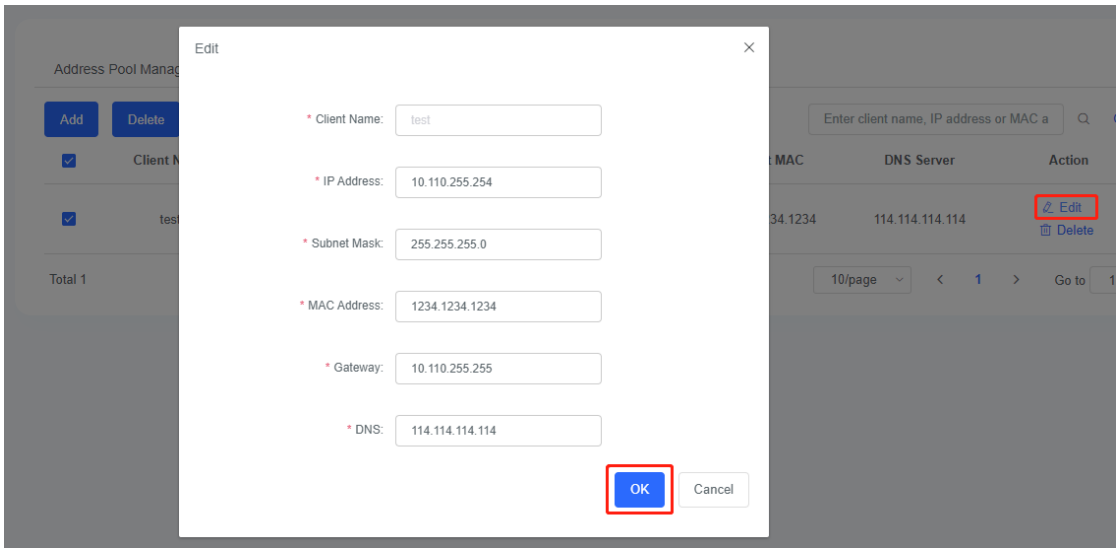
- Deleting a static IP Address

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



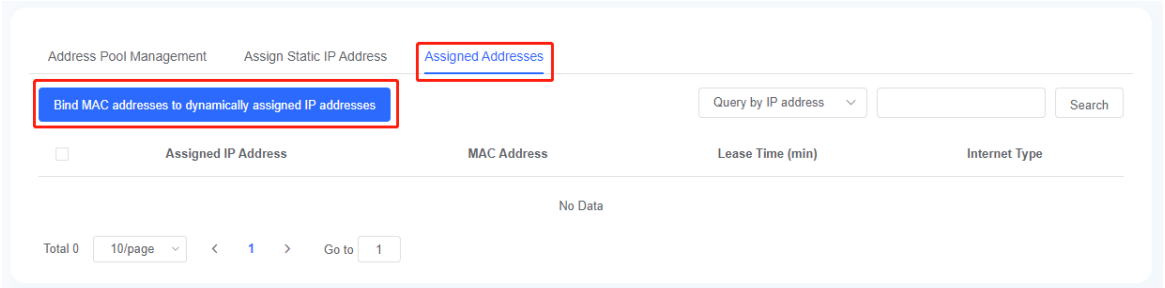
- Editing a static IP Address

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



(3) Assigned Addresses

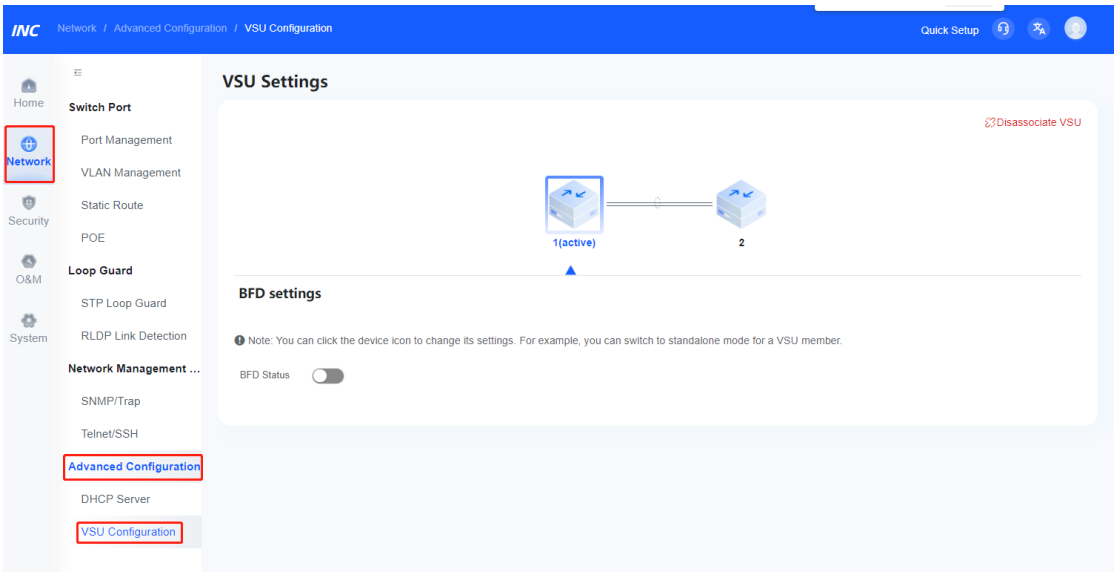
On this page, you can bind MAC addresses to dynamic IP addresses and reclaim assigned addresses.



Bind MAC addresses to dynamically assigned IP addresses: Select the assigned IP addresses, and click **Bind MAC addresses to dynamically assigned IP addresses**. On the displayed dialog box, click **OK**.

2. VSU Settings

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

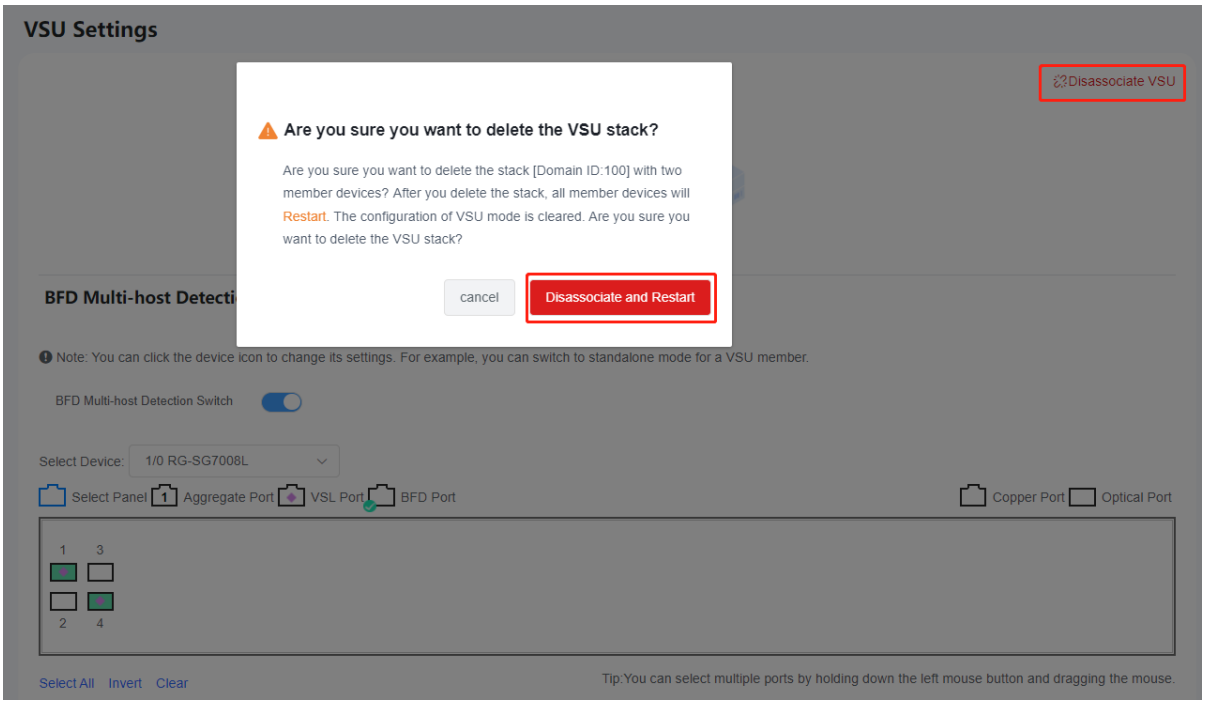


(1) Deleting a VSU Stack

Caution

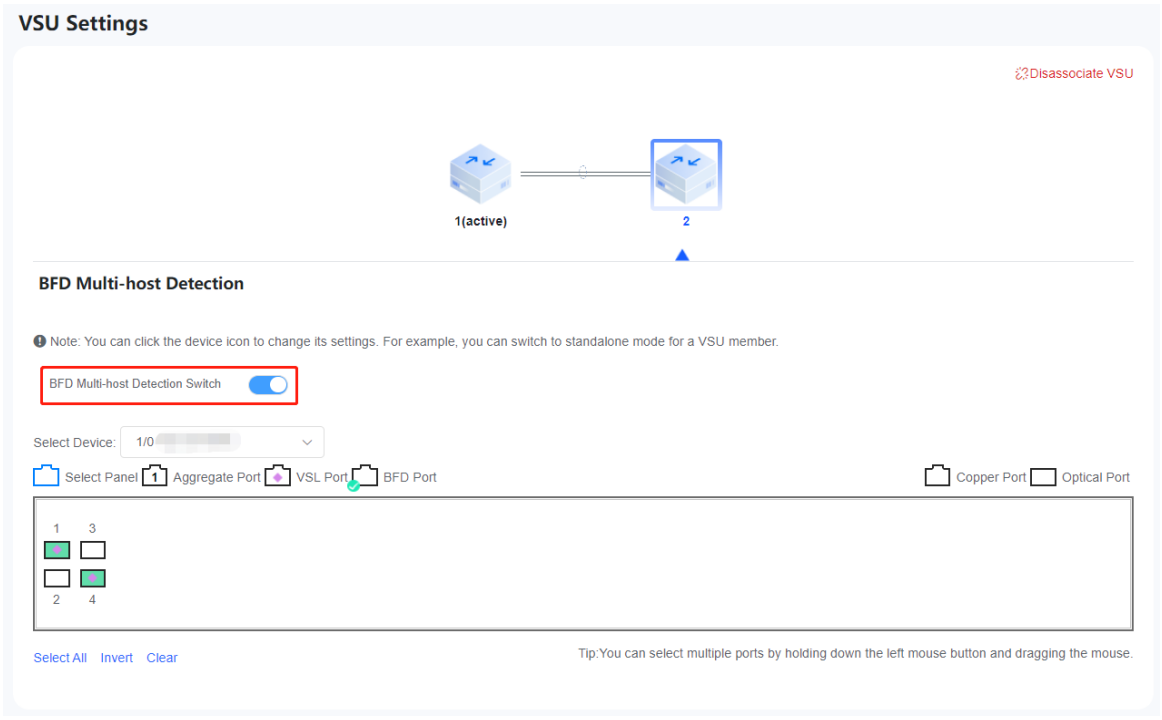
After you delete the VSU stack, all member devices will restart and the configuration of VSU mode will be cleared. Please operate with caution.

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

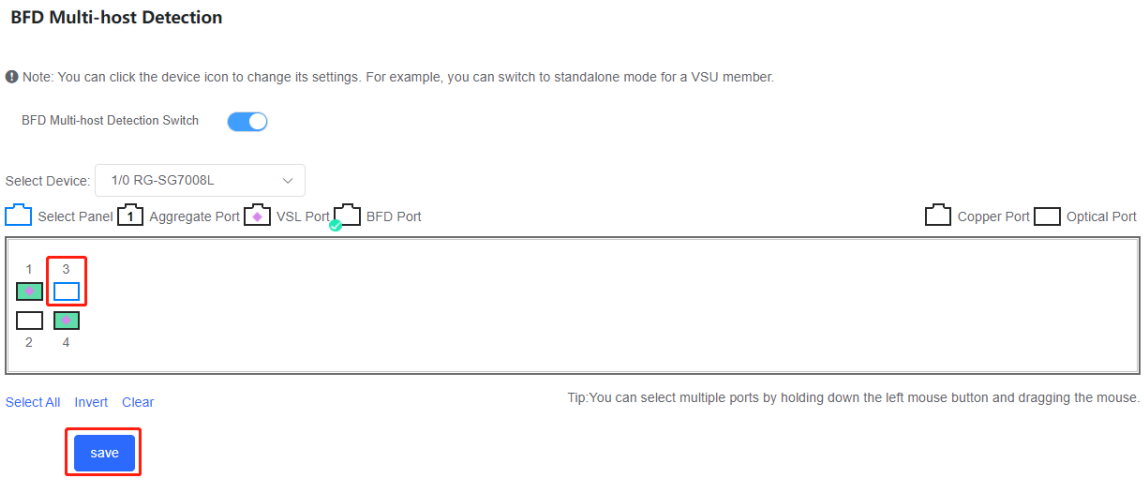


(2) BFD Multi-host Detection Switch

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



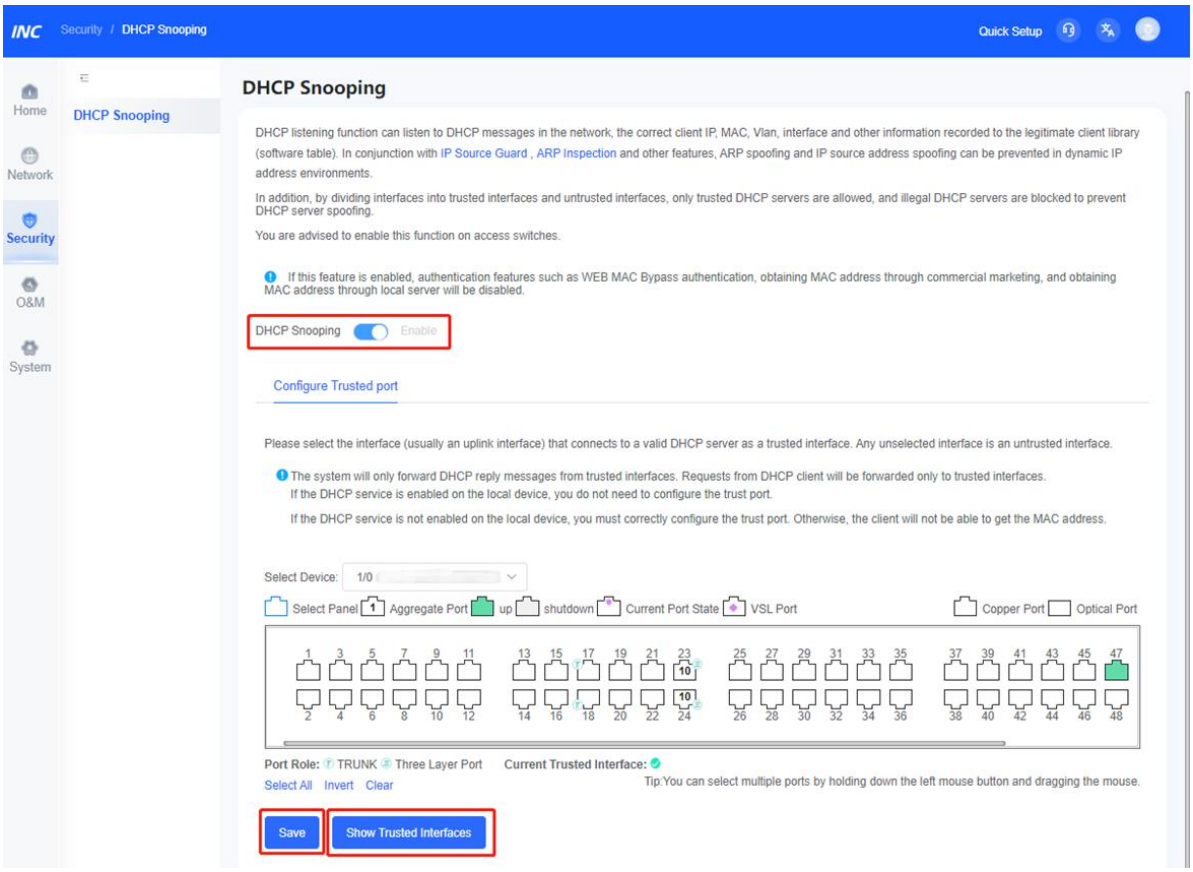
Click a port on which BFD is not enabled. Click **Save** to enable BFD on the port.



3.6 Security

3.6.1 DHCP Snooping

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



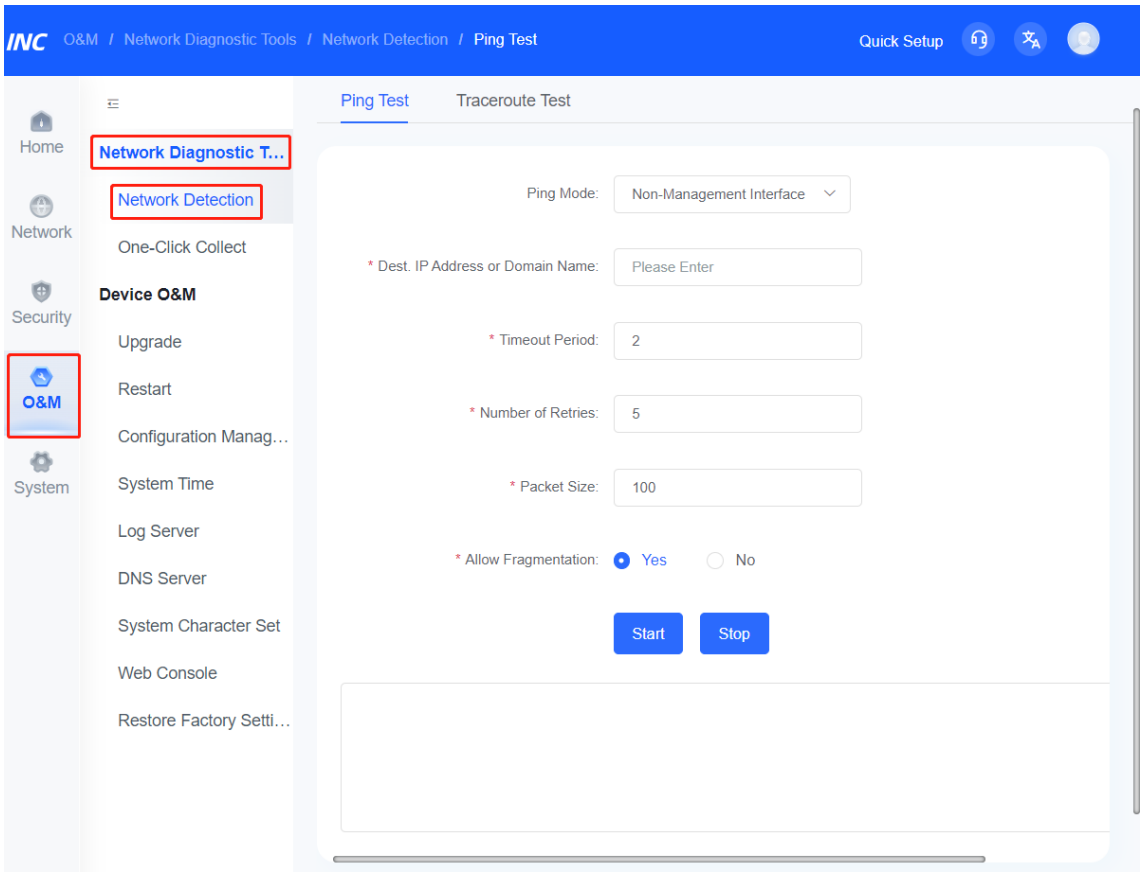
3.7 O&M

3.7.1 Network Diagnostic Tools

1. Network Detection

(1) Ping Test

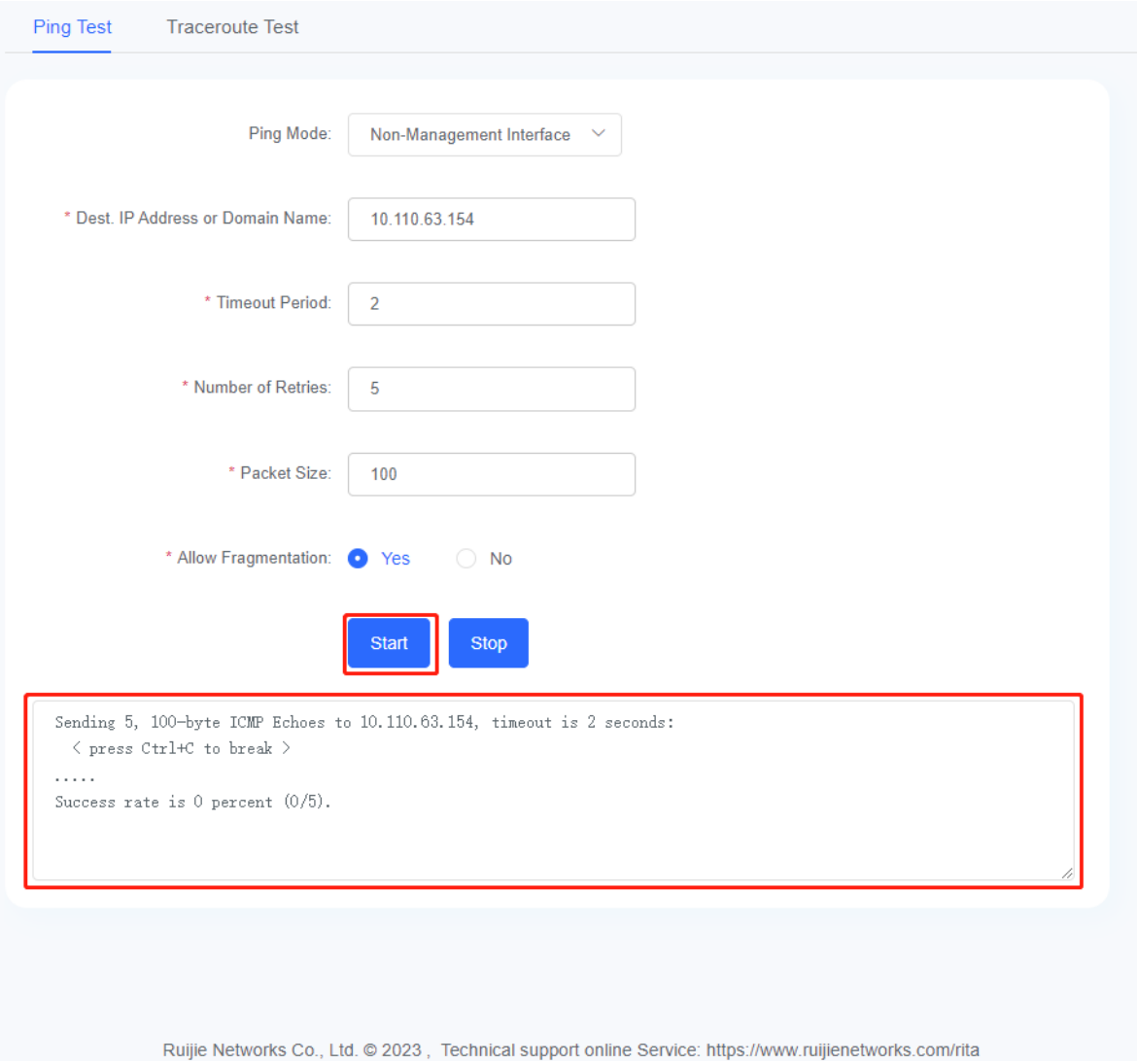
Choose **O&M** > **Network Diagnostic Tools** > **Network Detection** > **Ping Test** to access the **Ping Test** page.



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

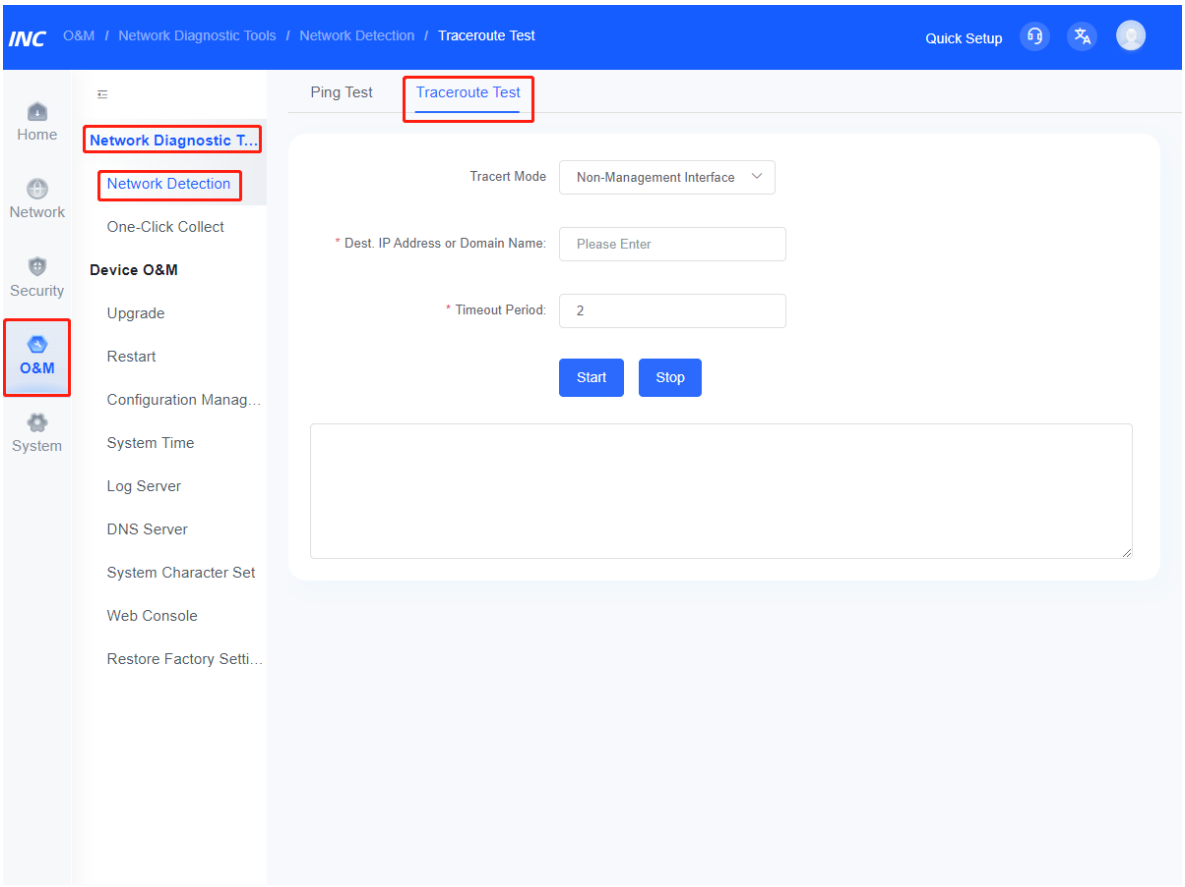
Note

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

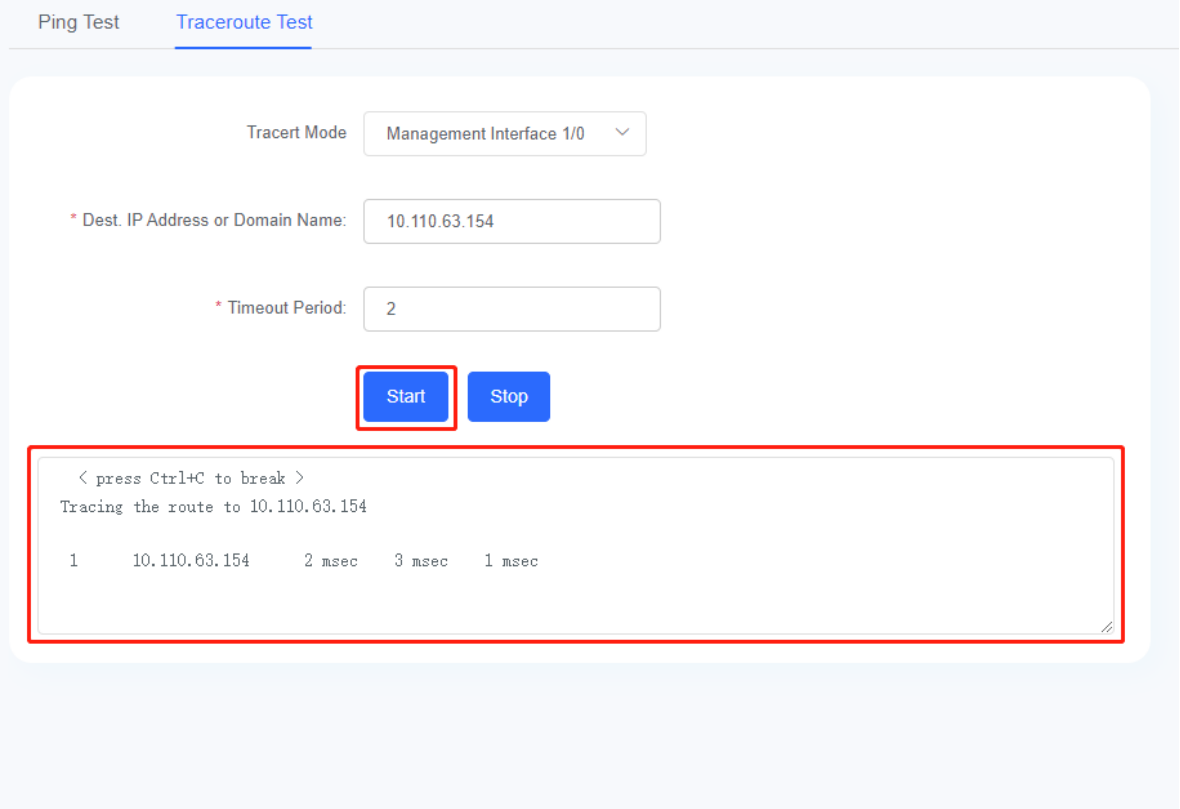


(2) Traceroute Test

Choose **O&M** > **Network Diagnostic Tools** > **Network Detection** > **Traceroute Test** to enter the **Traceroute Test** page.



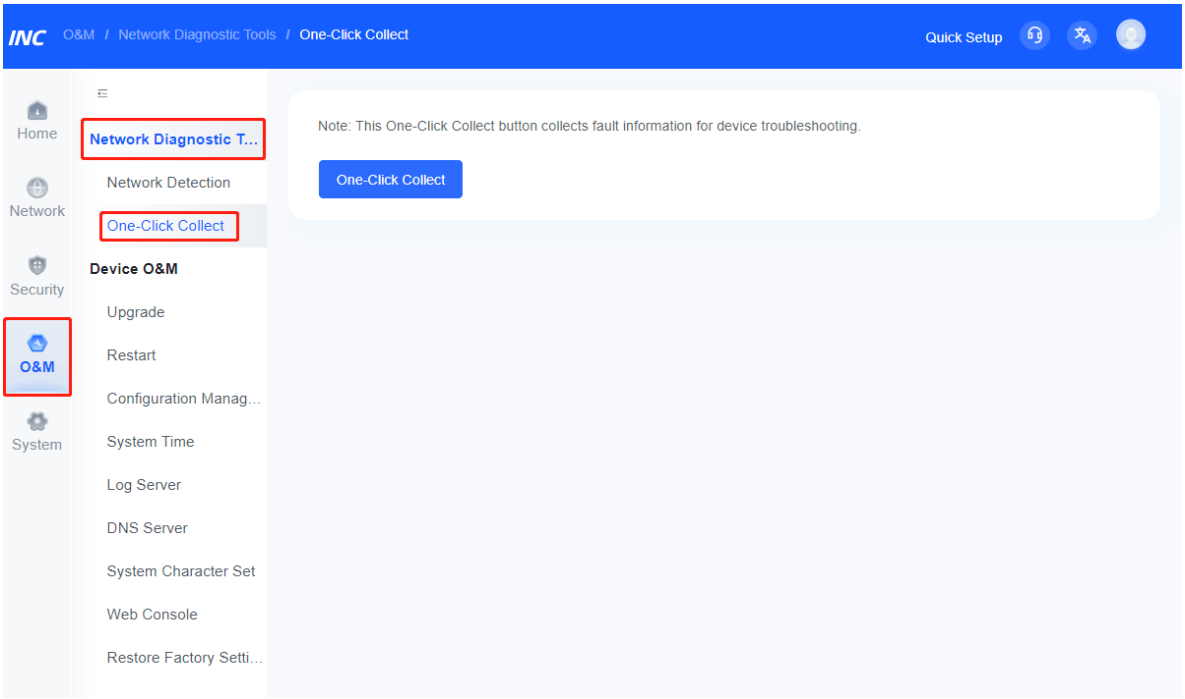
- **Start**: Select **Non-Management Interface** from the **Tracert Mode** drop-down list box to select the tracert mode. You can select **Non-Management Interface** and **Management Interface**. Enter the destination IP address or domain name and timeout period. Click **Start** to run the tracert test.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



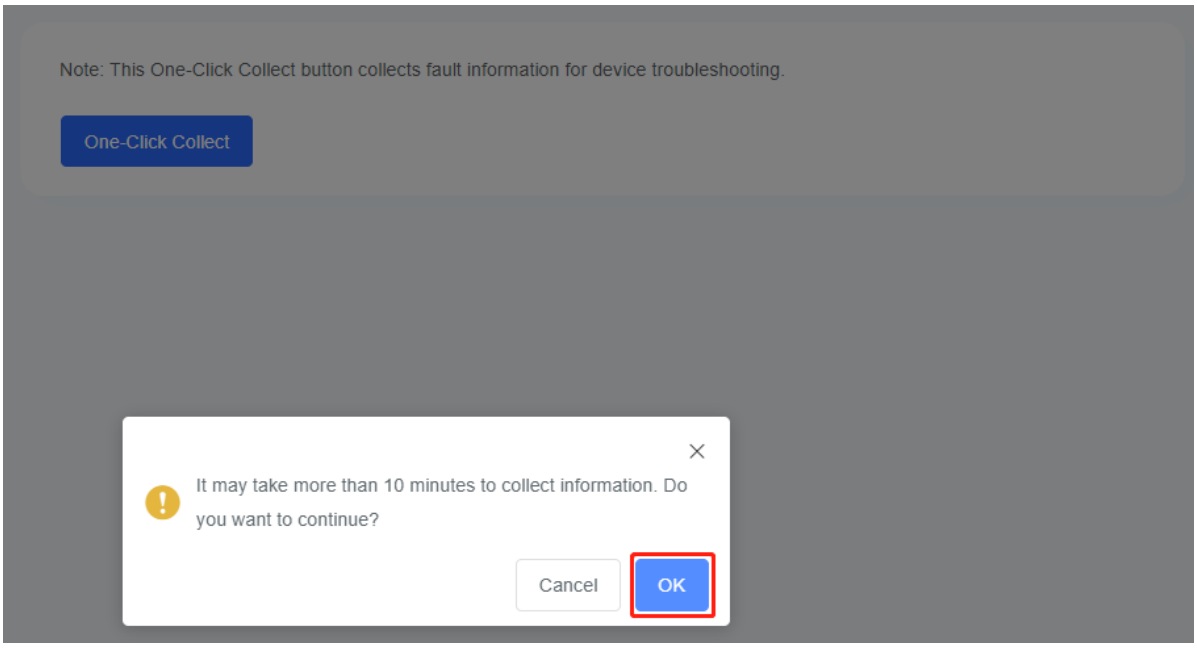
2. One-Click Collect

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

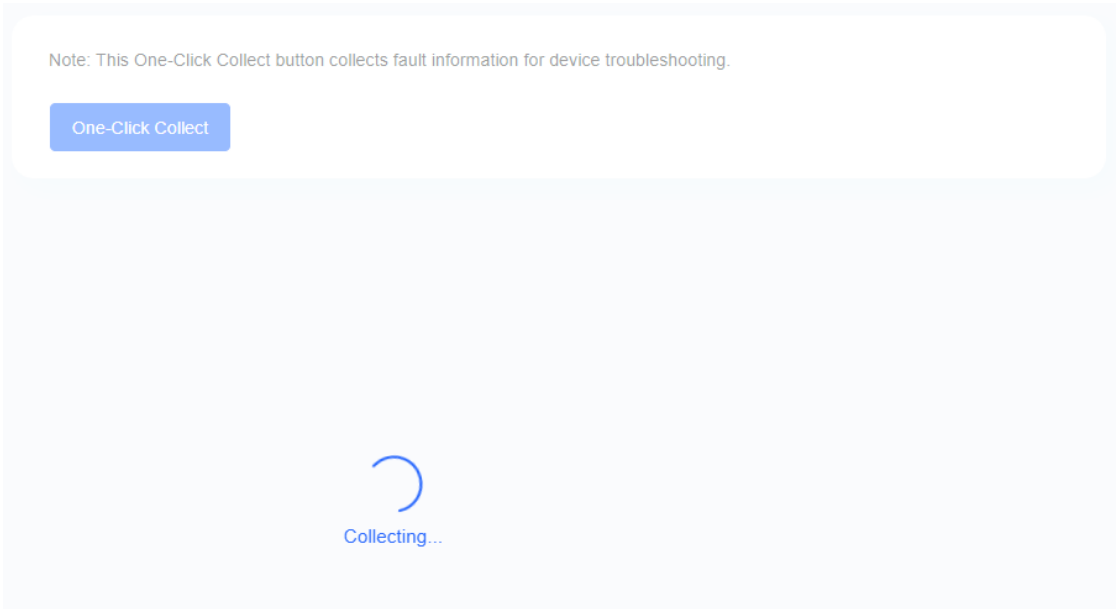
You can use the **One-Click Collect** function to collect switch fault information for troubleshooting.



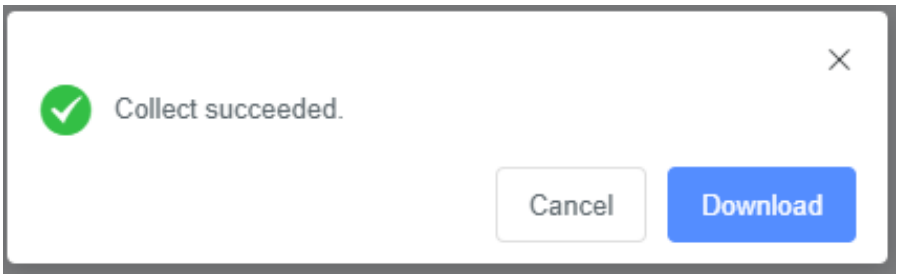
Collecting fault information may take about 10 minutes. After the collection is complete, you can download the collected fault information to a file named **tech_ vsd0_ 20210716142650.tar.gz**. Click **One-Click Collect**. The **Notice** dialog box is displayed.



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



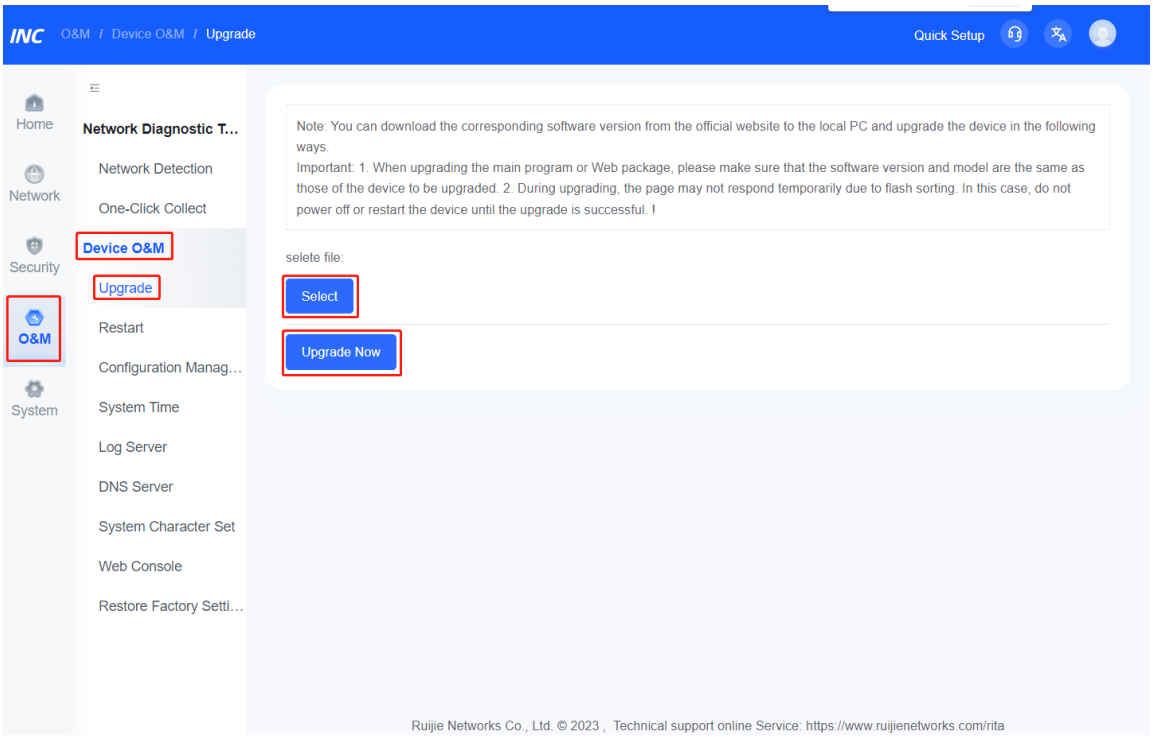
After the collection process is complete, the **Notice** dialog box is displayed. Click **Download** to download the collected information in a **tar.gz** compressed file.



3.7.2 Device O&M

1. Upgrade

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



Note

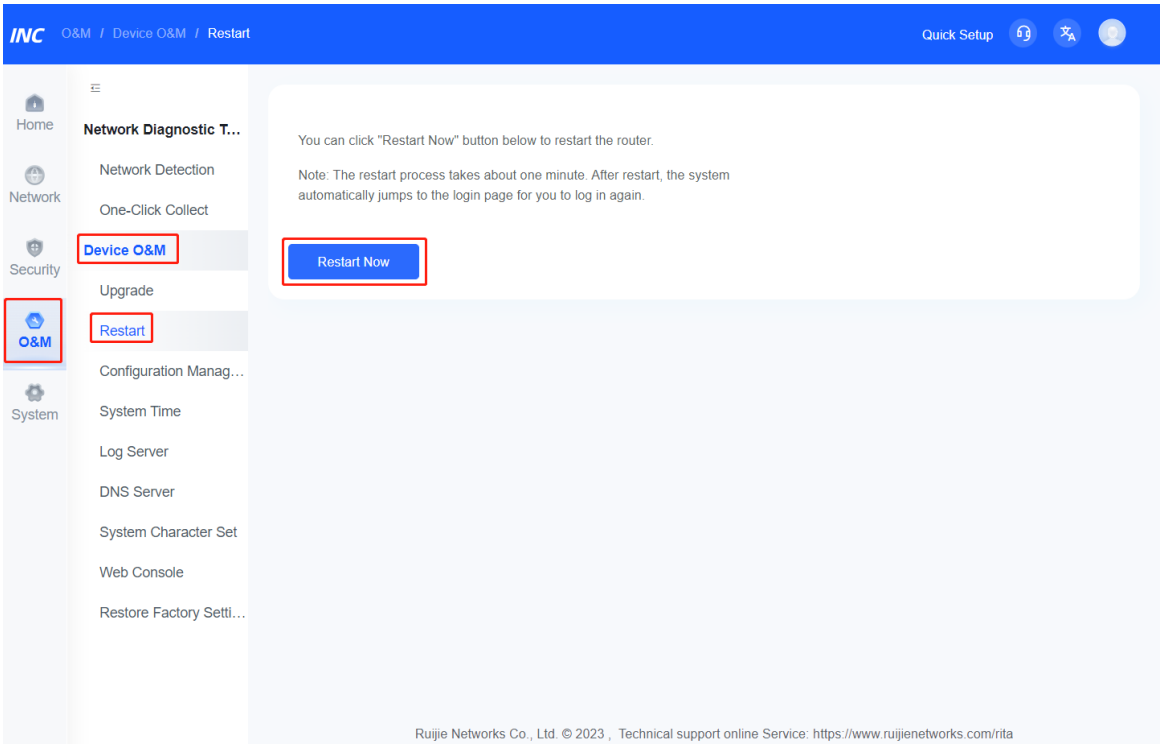
You can download the required software version file from Ruijie Networks's official website to the local PC and upgrade the switch using the downloaded file.

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.

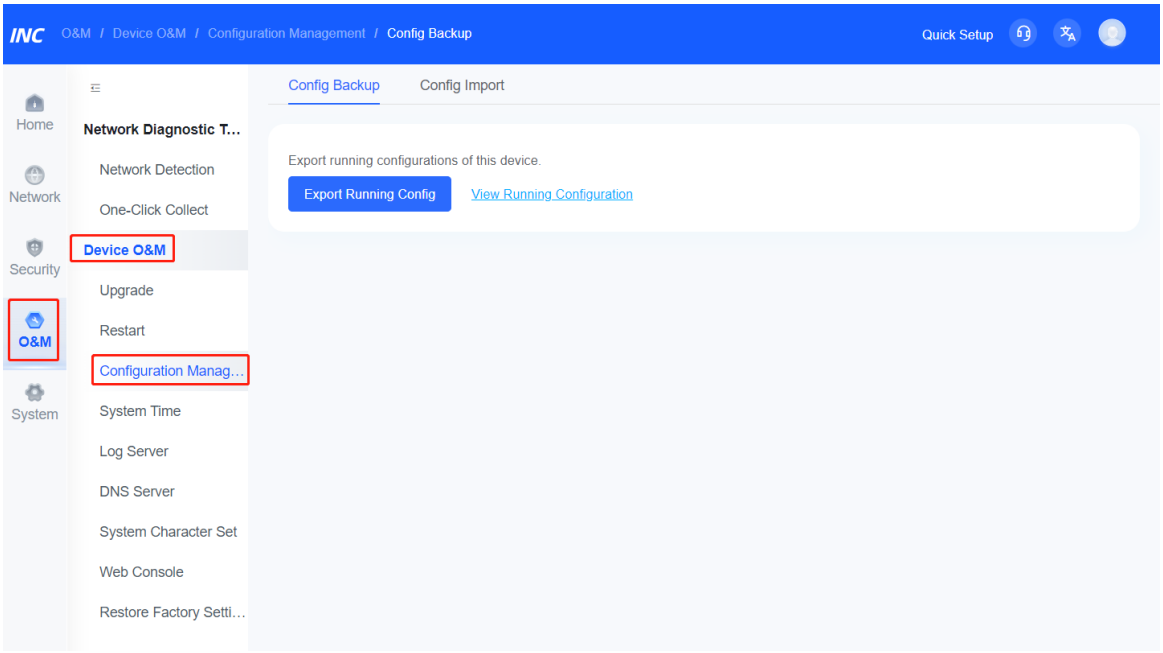
2. Restart

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.

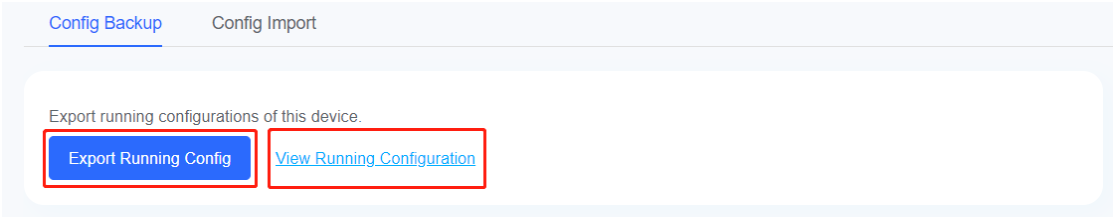


3. Configuration Management

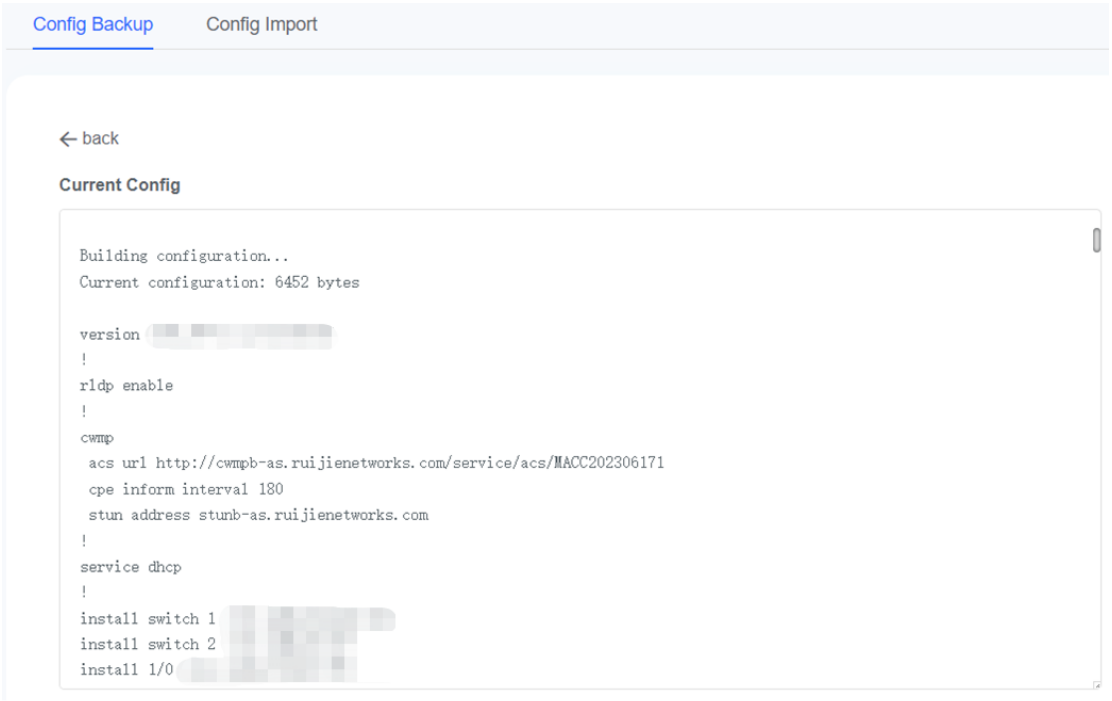
Choose **O&M** > **Device O&M** > **Configuration Management** to access the Configuration Management page.



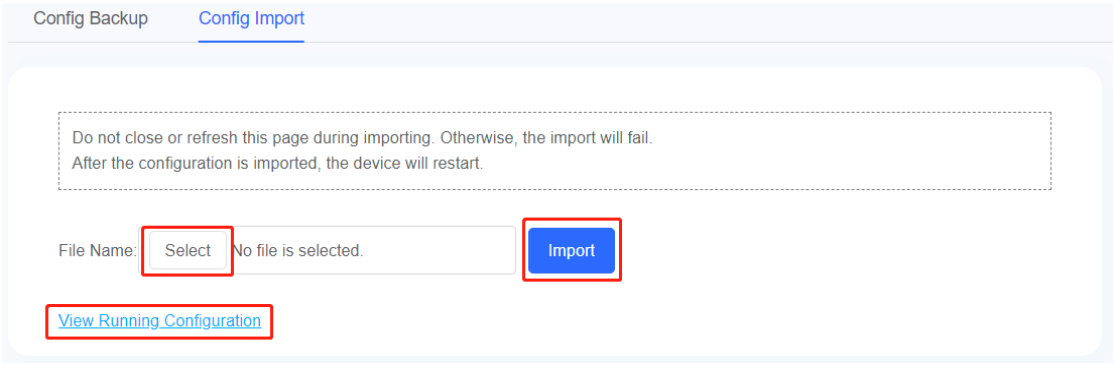
(1) Config Backup



- **Export running configuration**: You can click **Export Running Config** to generate the config.text text file.
- **View running configuration**: You can click **View running configuration** to switch to the Current Config page.

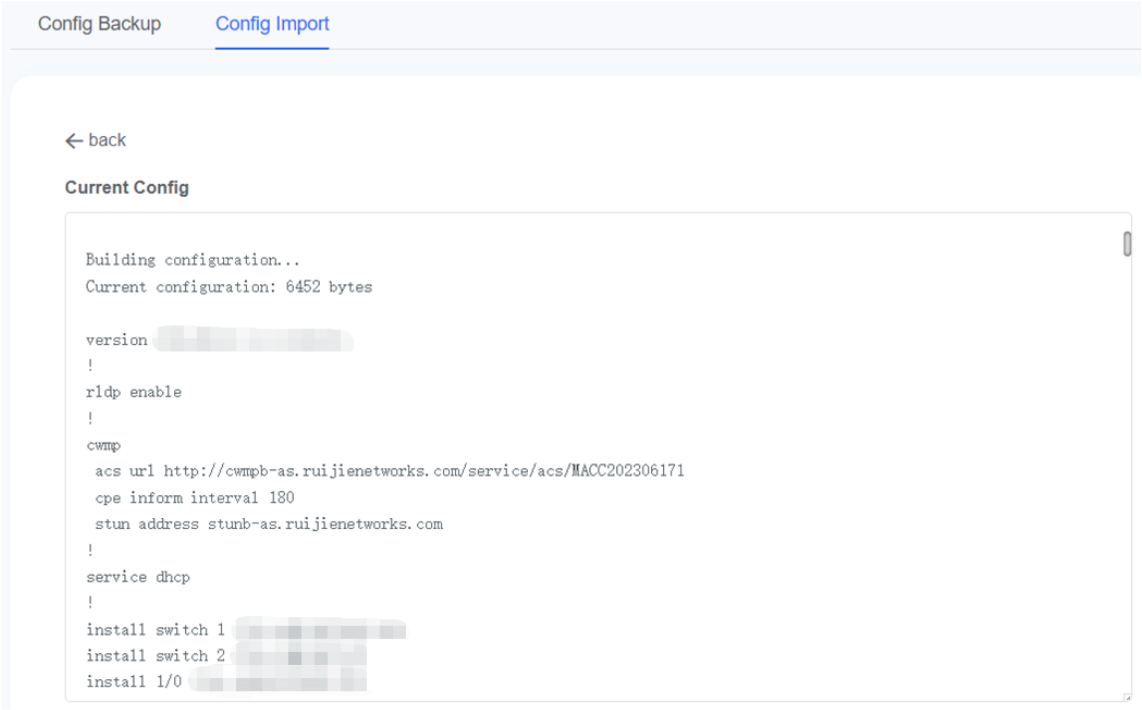


(2) Config Import



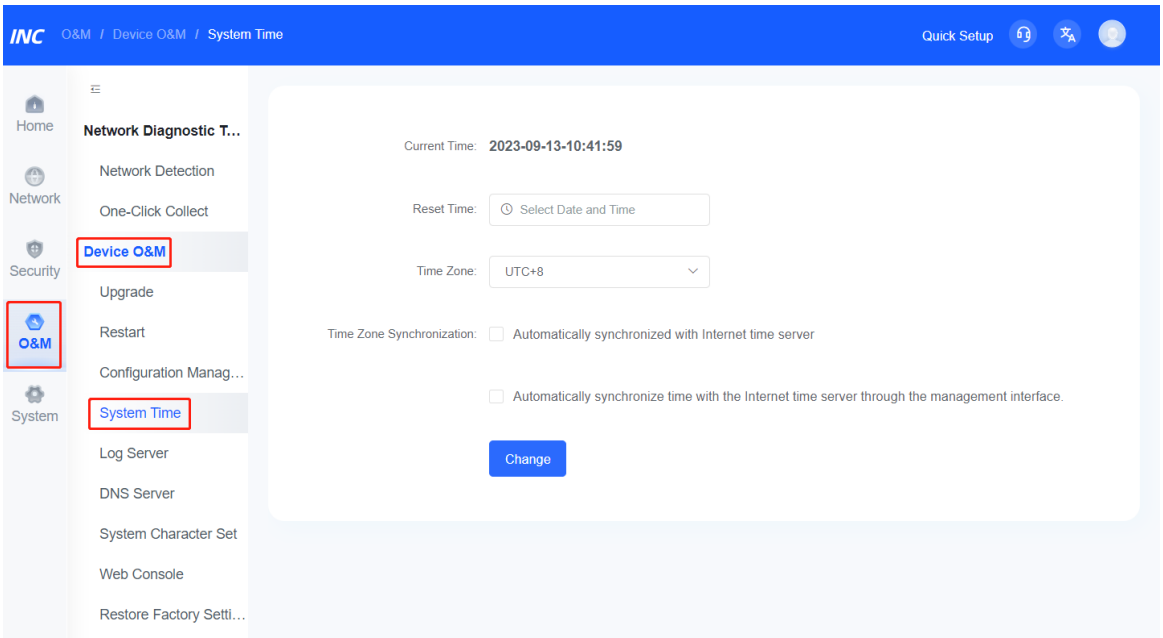
- **Import configurations**: You can click **Select** to select the configuration file to be imported, and then click **Import** to import the configuration file.

- **View running configuration**: You can click **View running configuration** to switch to the Current Config page.



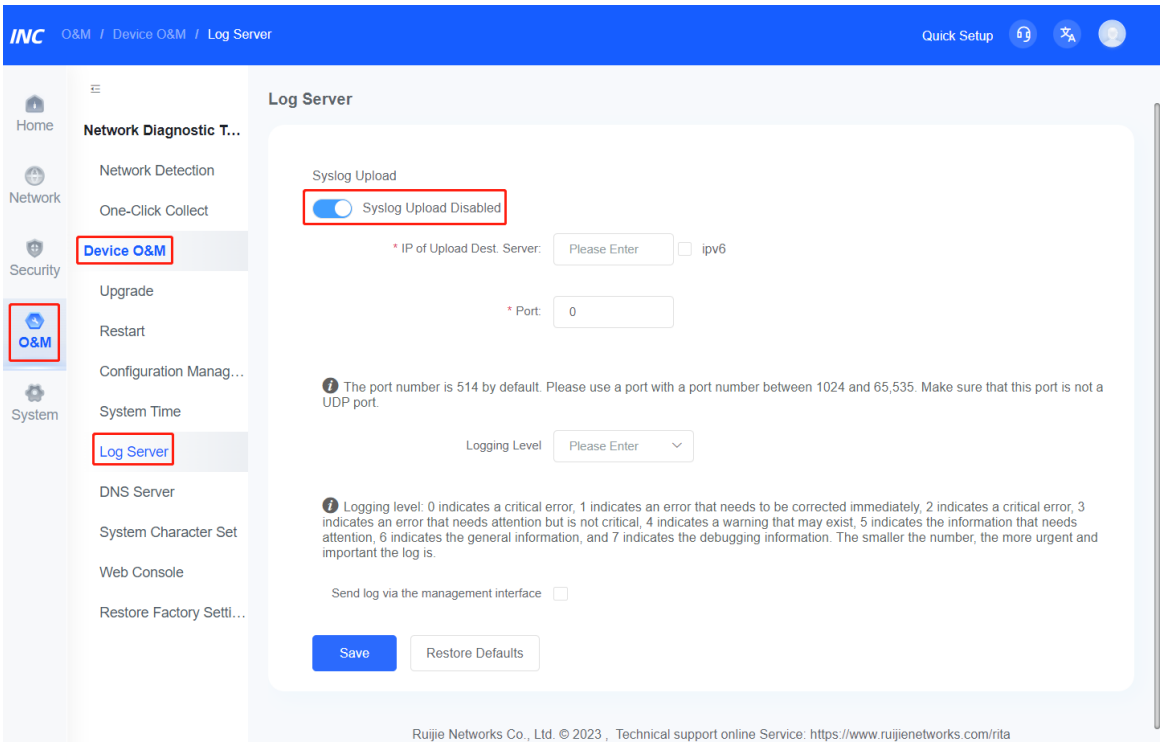
4. System Time

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



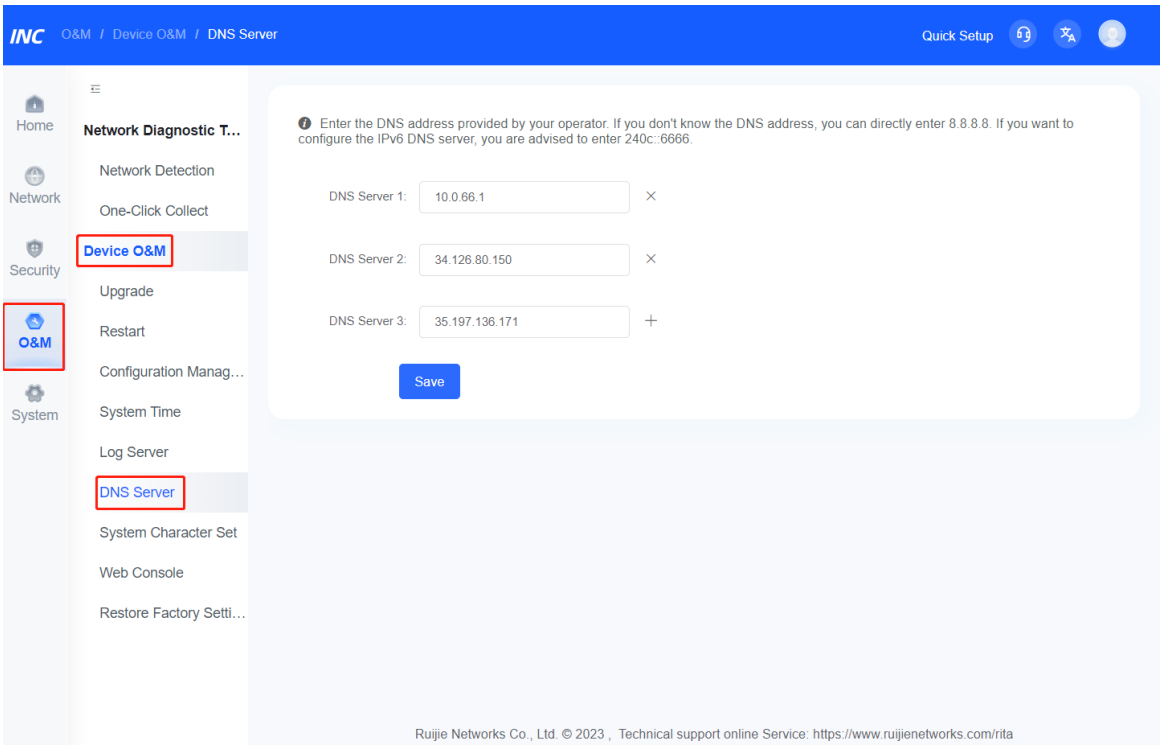
5. Log Server

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.



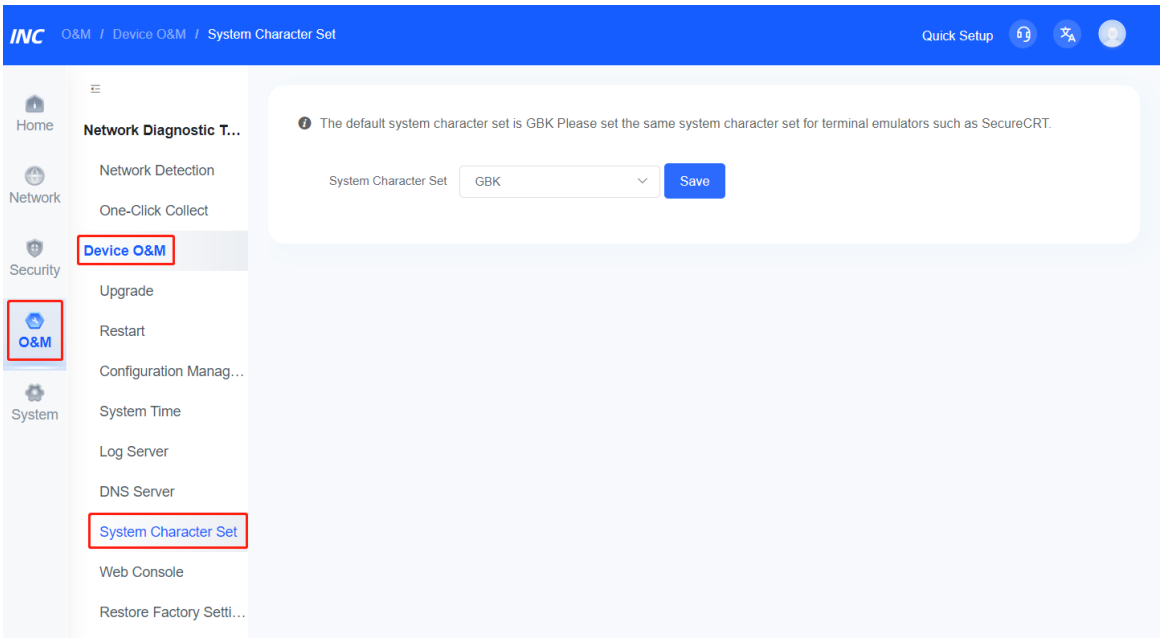
6. DNS Server

Choose **O&M** > **Device O&M** > **DNS Server** to access the **DNS Server** page. You can click **+** to add a DNS server, or click **x** to delete a DNS server, or click **Save** to submit the configuration.



7. System Character Set

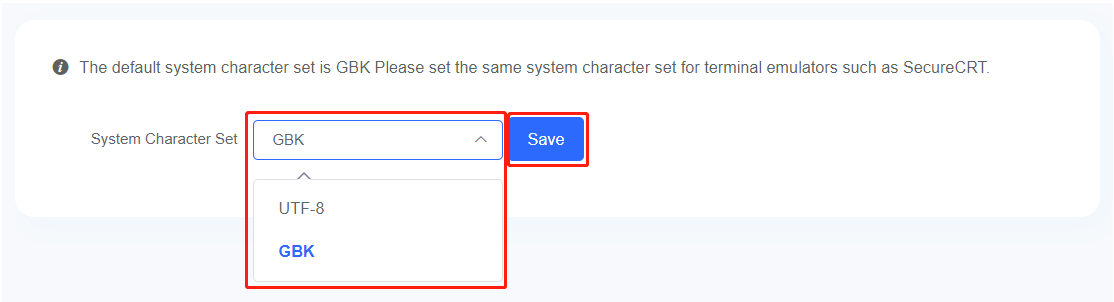
Choose **O&M** > **Device O&M** > **System Character Set** to access the **System Character Set** page.



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.

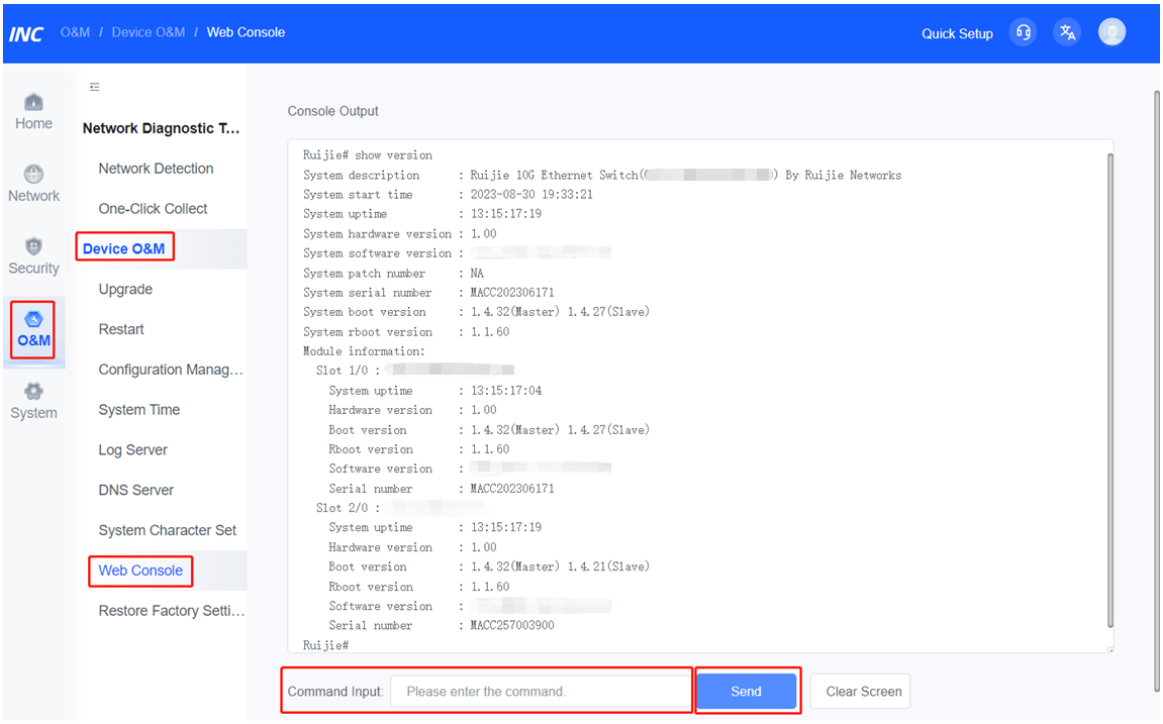
Note

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



8. Web Console

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



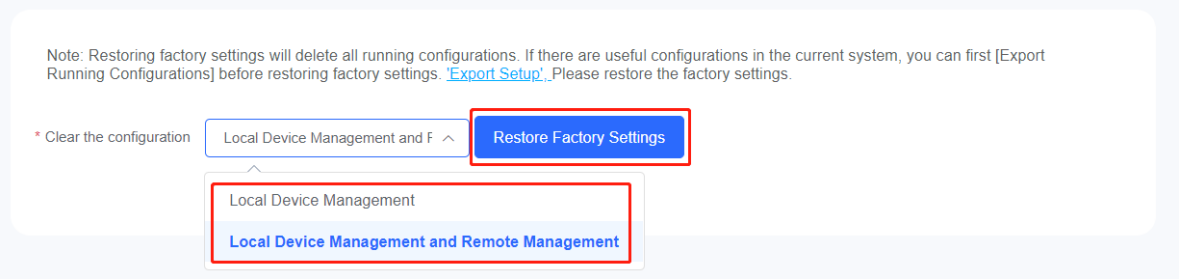
1. Enter a command in **Command Input** box and click **Send**. The command execution result will be displayed in the console.

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

9. Restore Factory Settings

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

You can select **Local Device Management** or **Local Device Management**, then click **Restore Factory Settings** to delete all the configurations of the switch, and restore the switch to factory settings. To save the current configuration, you are advised to export the current configuration by clicking **Export Setup**.



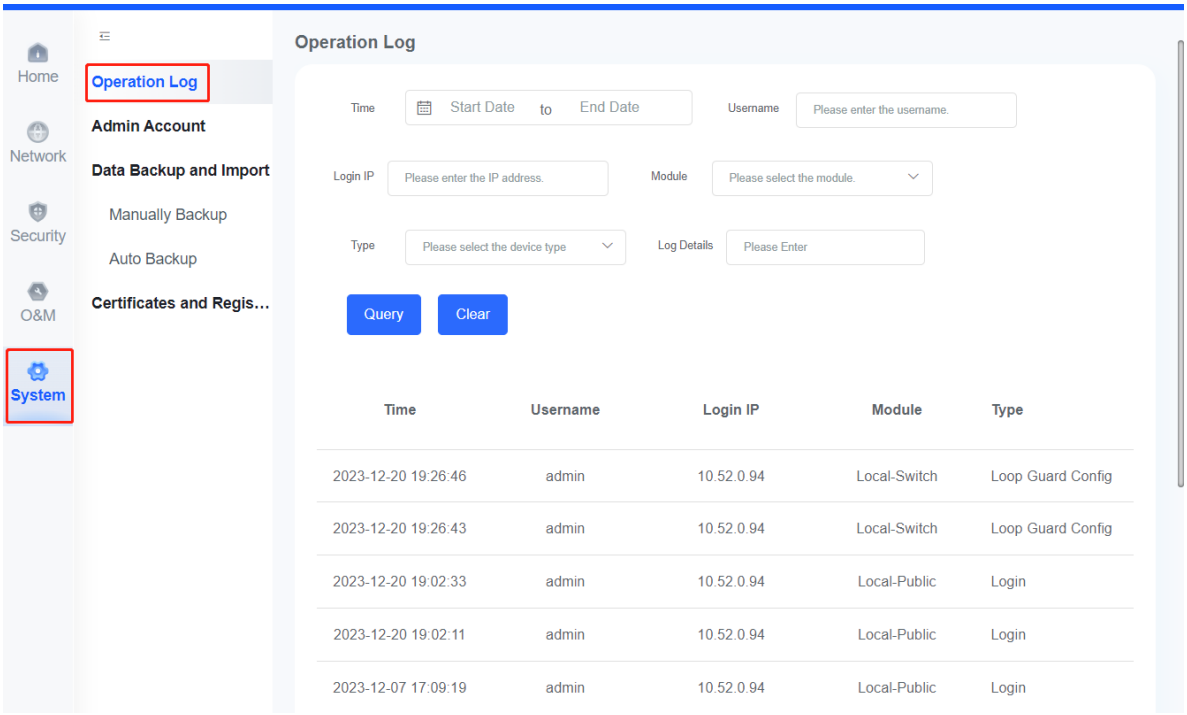
Caution

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. Please restore the factory settings.

3.8 System

3.8.1 Operation Log

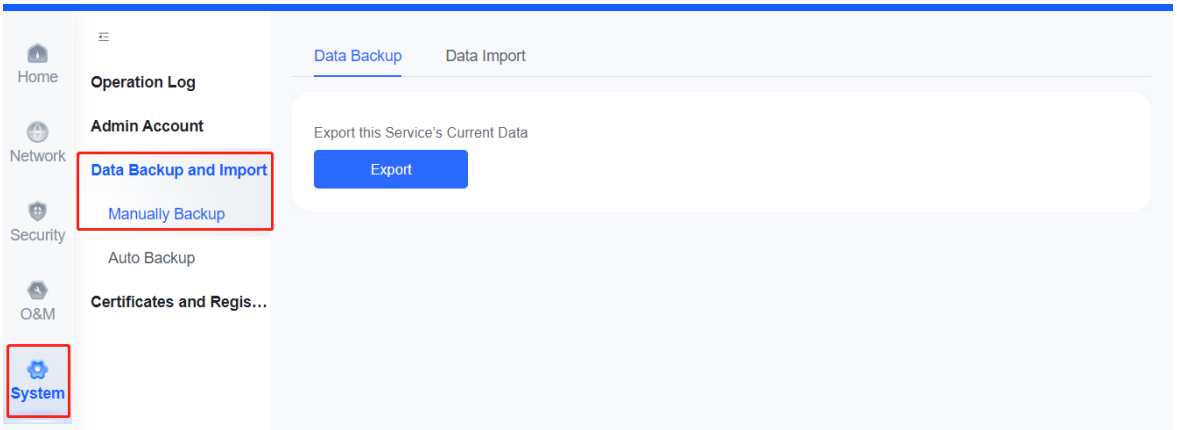
Choose **System** > **Operation Log** to access the Operation Log **page**. The operation log records users' key operations. You can query the operation log based on the search criteria.



3.8.2 Data Backup and Import

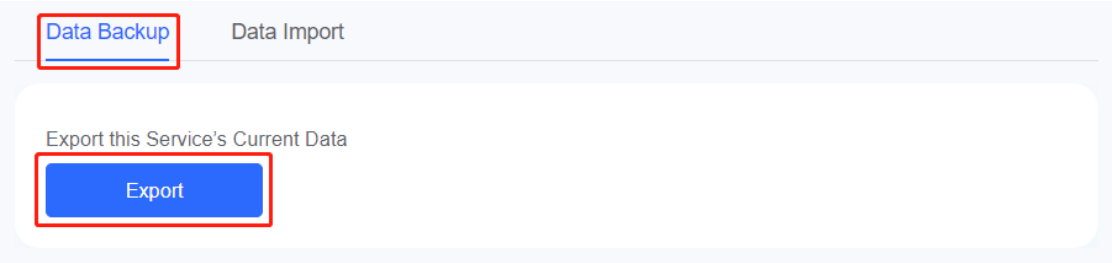
1. Manually backup

Choose **System** > **Data Backup and Import** > **Manually Backup** to access the **Manually Backup** page.



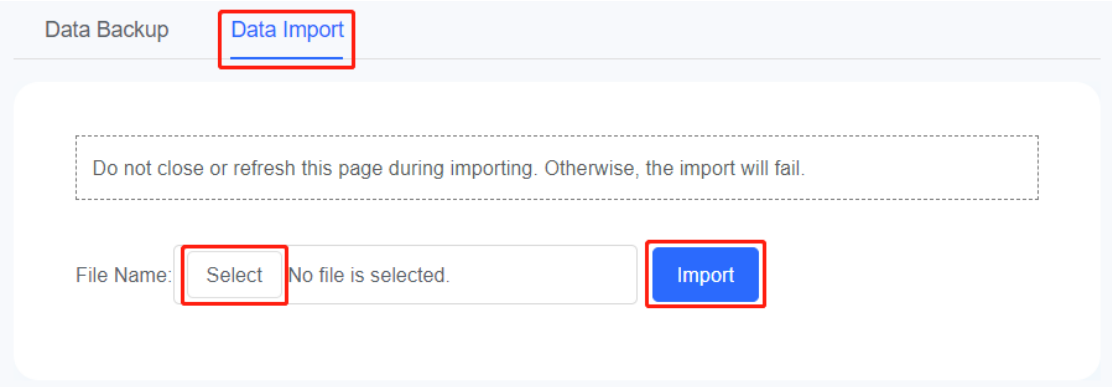
(1) Data backup

You can click **Export** to download the database file with the suffix ".db".



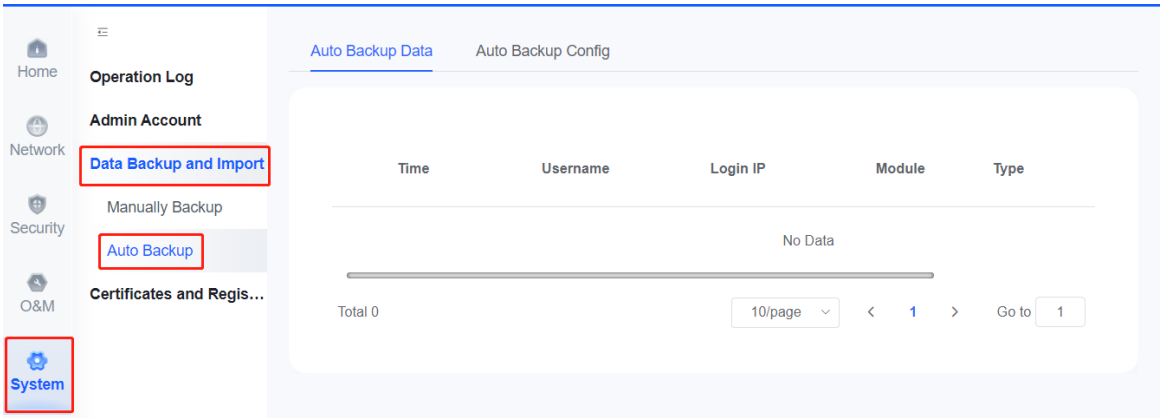
(2) Data import

The file name extension of the imported database file must be .db, and the imported file version must be the same as or earlier than the current database version.

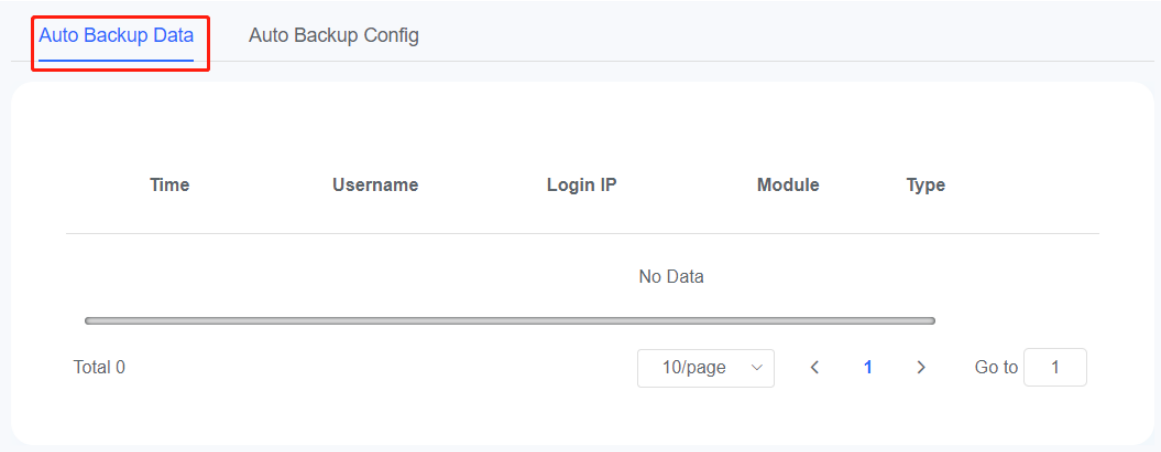


2. Auto Backup

Choose **System** > **Data Backup and Import** > **Auto Backup** to access the **Auto Backup** page.

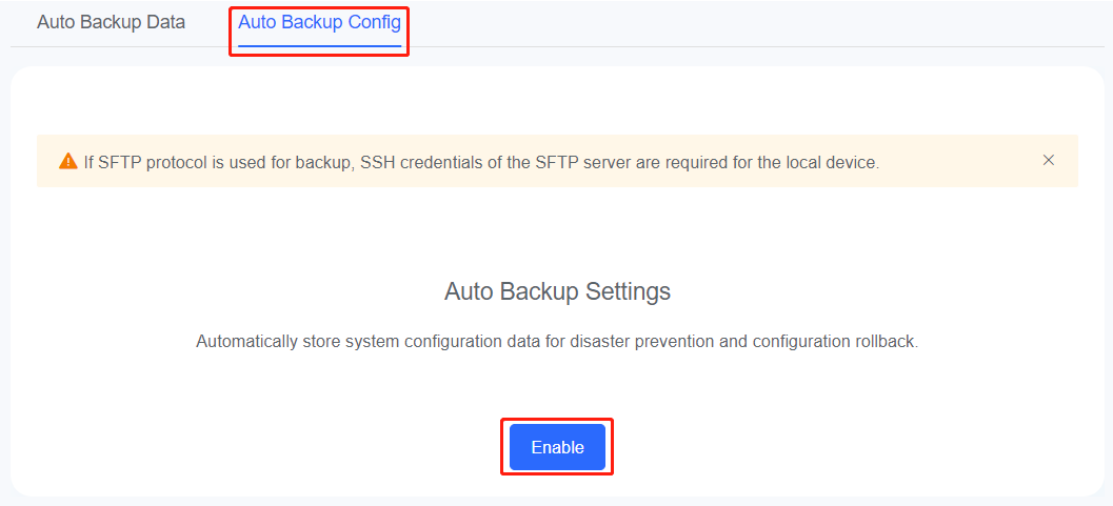


(1) Auto Backup Data



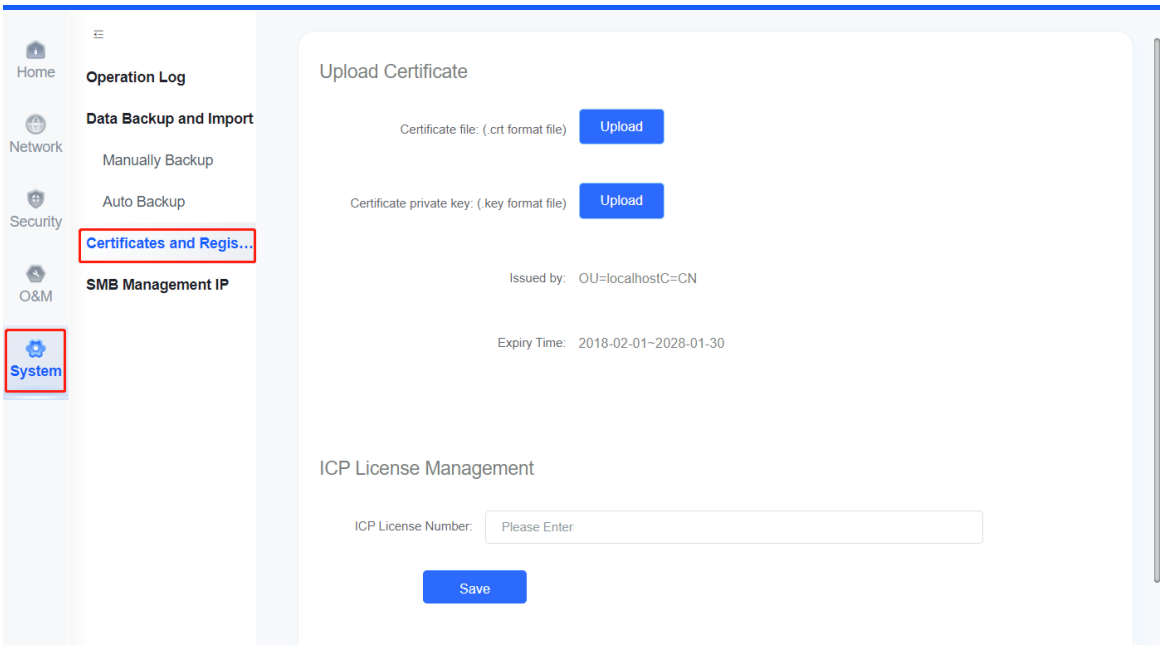
(2) Auto Backup Config

Click **Enable** to enable the auto backup function.



3.8.3 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.



3.8.4 SMB Management IP

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

