Ruijie RG-NBS Series Switches

Web-Based Configuration Guide

Copyright Statement

Ruijie Networks©2020

Ruijie Networks reserves all copyrights of this document. 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.

Exemption Statement

This document is provided “as is”. The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. 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

Thank you for using our products.

Audience

This manual is intended for:

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

Obtaining Technical Assistance

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

Related Documents

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

Conventions

This manual uses the following conventions:

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

1 Overview

eWeb is a Web-based network management system that manages or configures devices. You can access eWeb via browsers such as Google Chrome.

Web-based management involves the Web server and Web client. The Web server is integrated in a device, and is used to receive and process requests from the client, and return processing results to the client. The Web client usually refers to a browser, such as Google Chrome IE, or Firefox.

1.1 Conventions

In this document:

- Texts in bold are names of buttons (for example, **OK**) or other graphical user interface (GUI) elements (for example, **VLAN**).
- The eWeb management system displays different menus based on the device role, and information on the local page varies accordingly. The actual GUI prevails. The chapter eWeb Configuration describes all functions.
- The eWeb configurations vary with the device model. This document is described by using NBS5200-24SFP/8GT4XS as an example.

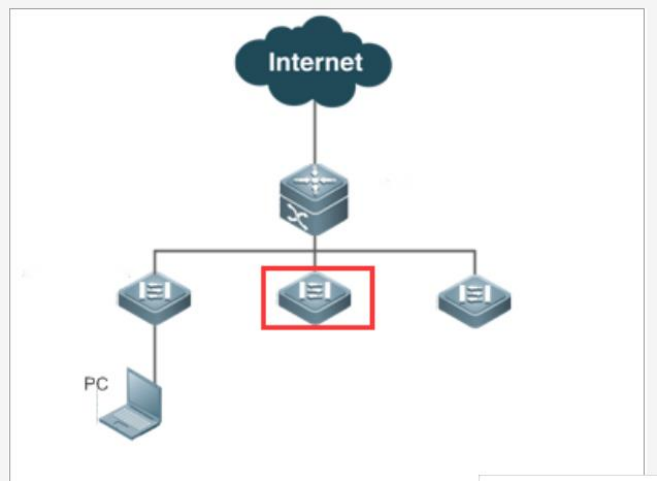
2 Configuration Guide

2.1 Configuration Preparation

2.1.1 Scenario

As shown in the figure below, you can access the eWeb management system of an access or aggregation switch via a PC browser to manage and configure the device.

Figure 2-1-1 Network Topology



Note: The device enclosed in the red frame in the preceding figure is the accessed switch. If the switch can be pinged successfully from the PC, you can access the eWeb management system deployed on the switch.

2.1.2 Deployment

Configuration Environment Requirements

Client requirements:

- An administrator can log into the eWeb management system from a Web browser to manage devices. The client refers to a PC or some other mobile endpoints such as laptops or tablets.
- Google Chrome, Firefox, IE9.0 and later versions, and some Chromium-based browsers (such as 360 Extreme Explorer) are supported. Exceptions such as garble or format error may occur if an unsupported browser is used.
- 1024 x 768 or a higher resolution is recommended. If other resolutions are used, the page fonts and formats may not be aligned and the GUI is less artistic, or other exceptions may occur.
- The device management IP address is 10.44.77.200, and the PC can be directly connected to the device for management and configuration.

- The client IP address is set in the same network segment as the device IP address, such as 10.44.77.199. The subnet mask is 255.255.255.0. The default gateway is device management address 10.44.77.1. Alternatively, you can set the IP assignment mode to **Obtain an IP address automatically**.

Server requirements:

- You can log into the eWeb management system through a LAN port or from Ruijie Cloud on an external network.
- The Web service (enabled by default) needs to be enabled on the device.
- Login authentication (enabled by default) for Web-based management needs to be configured for the device.
- A management IP address needs to be configured for the device (the IP address is automatically obtained by default).

To log into the eWeb management system, open the Google Chrome browser, and enter 10.44.77.200 in the address bar, and press **Enter**.

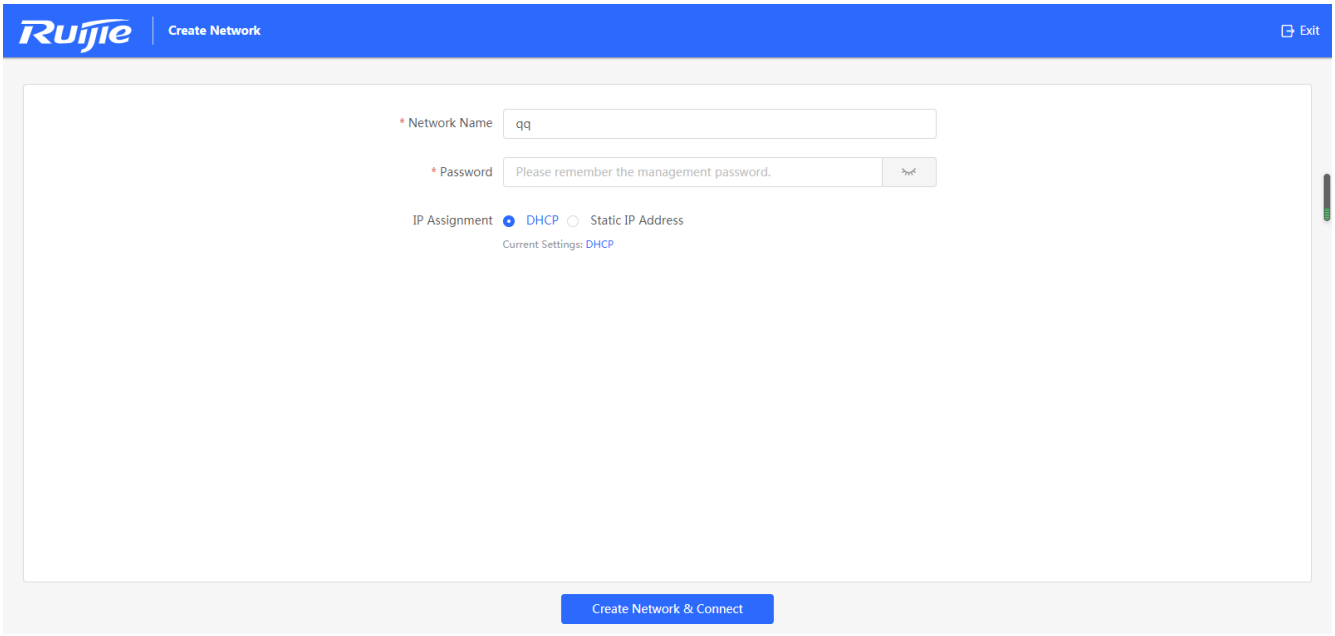
2.2 Wizard

You need to quickly configure the device (the network name, management password, and management IP address of the device) when logging into the eWeb management system for the first time (for initial configuration).

Configuration description:

- **Network Name** identifies the network where the device is located (which needs to be entered by the user upon initial use).
- **Password** indicates the login password. (Please remember the management password and keep it carefully.)
- **IP Assignment** indicates the network access mode of the device, including **DHCP** (the DHCP server allocates a dynamic IP addresses) and **Static IP Address** (the user enters a specified IP address in the required format).

Figure 2-2-1 Configuration Initialization (Wizard)



Click **Create Network & Connect** for the device to automatically deliver and initialize device configuration.

Click **Exit** in the upper right corner. A prompt is displayed and the device can skip the wizard to enter the eWeb management system of the device.

2.3 Introduction to Web GUI

Device Panel

Figure 2-3-1 Display Panel

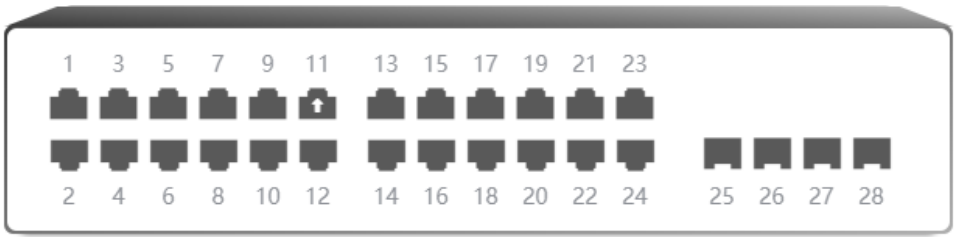
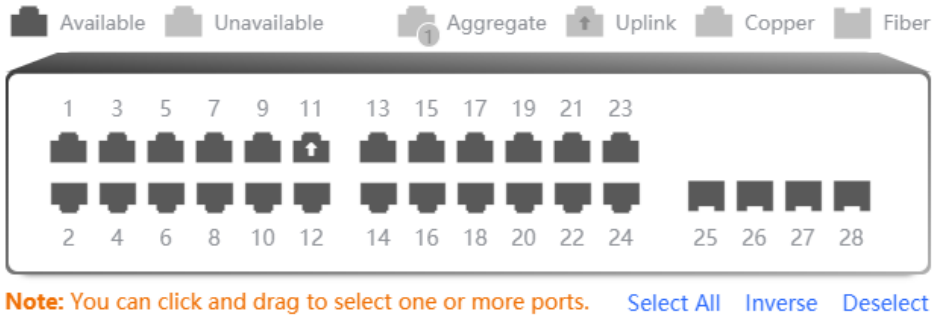


Figure 2-3-2 Edit Panel



- Panel description

The panel displays the actual port layout of the switch, including the display panel and edit panel. The display panel shows various statuses of the ports. The edit panel allows you to click and drag to select one or more ports, select all ports, inverse ports and deselect ports.

- Action

Click the port icon on the panel or drag the mouse to select multiple ports so that the ports become selected. Then, set the selected ports, for example, add the port description, port mirror, and port rate limit.

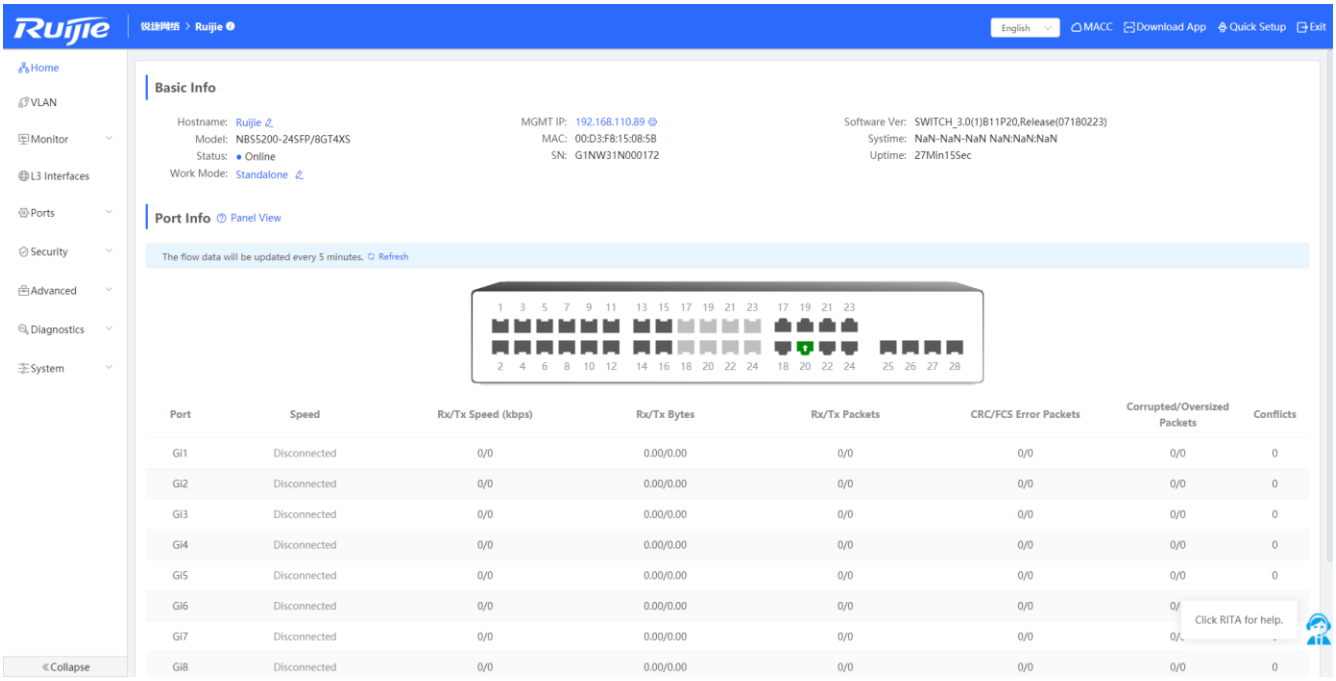
Feature

Feature	Description
Home	Displays port information and overall device information.
VLAN	Creates VLANs and sets VLANs and Trunk ports.
Port Flow	Displays and clears traffic and other information of all ports.
MAC List	Displays the MAC addresses learned by the switch, including dynamic and static MAC addresses.
Static MAC	Allows users to manually bind a MAC address to a port of the device. If 802.1x authentication is enabled on a port, a network device with its MAC address bound to the port is exempted from authentication.
Dynamic MAC	Displays the learned dynamic MAC table and allows users to manually clear the MAC table based on the conditions.
MAC Filter	Allows MAC address filtering. The switch needs to forward data according to the MAC table. When receiving a packet with a filtered MAC address, the switch discards the packet. If a user initiates ARP attacks, the MAC address of the user can be configured as an address to be filtered out, so as to prevent attacks.
Aging Time	Displays and configures the MAC aging time.
ARP List	Displays the IP-MAC mapping tables of the network devices connected to interfaces of the device.
L3 Interfaces	Configures VLAN, physical port or aggregate port as layer-3 interfaces.
Static Routing	Configures static routes.
ARP List	Displays all static and dynamic ARP entries.

Ports	Sets basic port information, link aggregation, port mirroring, port rate limit, management IP address, and PoE information.
DHCP Snooping	Sets DHCP snooping.
Storm Control	Controls storms.
ACL	Sets and applies ACLs.
Port Protection	Sets port protection to isolate ports.
STP	Configures STP global settings, STP ports and RLDP.
LLDP	Configures LLDP global settings, LLDP ports and displays neighbor information.
RLDP	Configures RLDP global settings, RLDP ports and displays RLDP information.
Network Tools	Sets Ping test, Traceroute test and DNS lookup.
Fault Collection	Packages and compresses the device configuration file, and provides the compressed file to the developer, so that the developer can decrypt and decompress the file for fault locating.
Cable Diagnostics	Displays the cable diagnostics status, and helps determine whether a cable is short-circuited, disconnected, or in other abnormal state.
System Time	Displays and sets the system time.
Login Password	Configures eWeb login password.
Session Timeout	Configures the eWeb login timeout period.
Setup	Backs up setup, imports setup, and restores defaults of device settings.
Reboot	Reboots the device and performs scheduled reboot settings.
Overview	Displays login device details and all online devices.
Switches	Displays the switch list for easy management.
Network	Enables configuration of whole system, network merging, and other operations.

System Layout

Figure 2-3-3 System Layout



2.3.1 Top Navigation Bar

The top navigation bar successively displays the manufacturer logo, network name, and device name on the left, and displays device shortcuts **Ruijie Cloud**, **Download App**, **Wizard**, and **Exit** on the right.

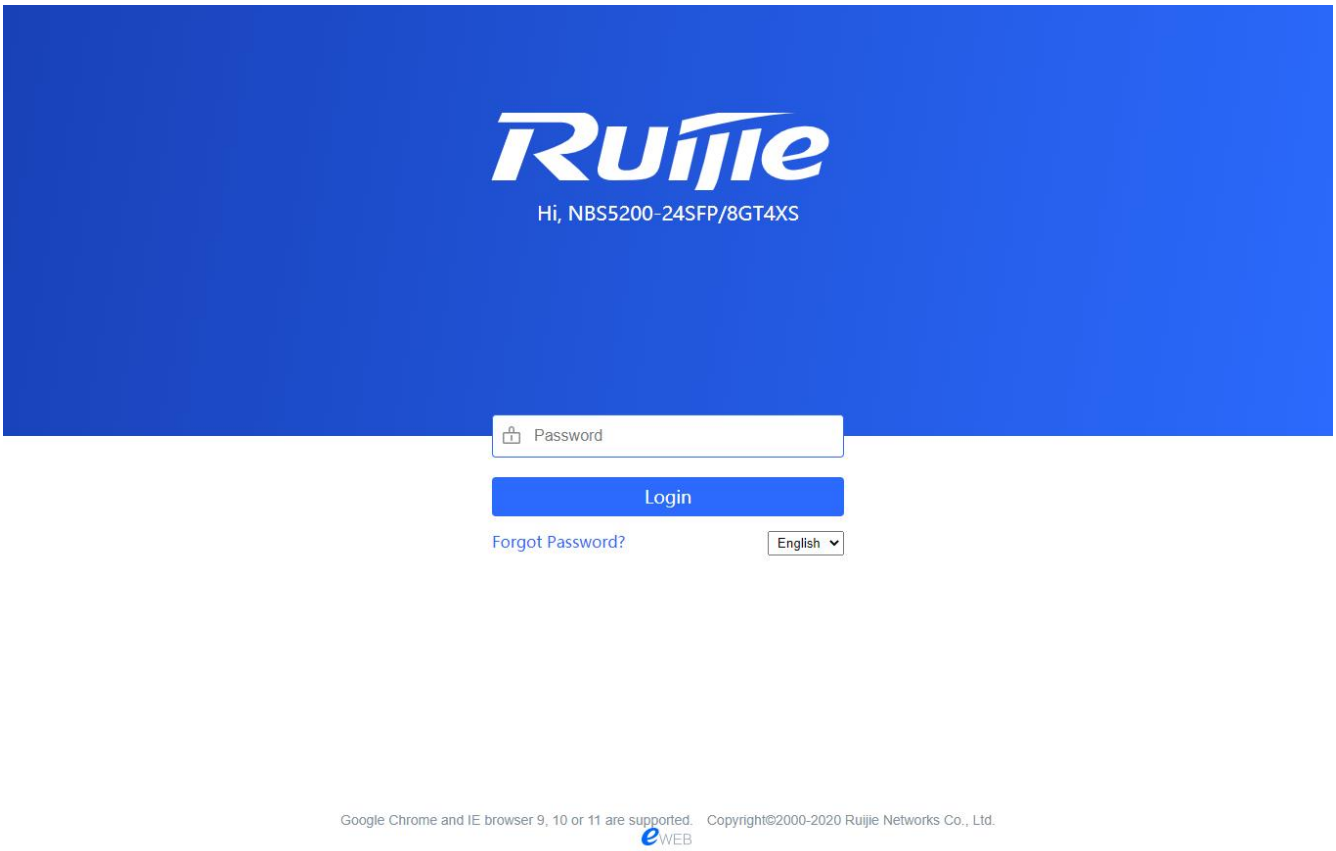
Move the mouse to the device name area to display the basic information of the login device.

Move the mouse to **Ruijie Cloud** to display the link to enter Ruijie Cloud.

Move the mouse to **Download App** to display the QR code for downloading the App. You can scan the QR code to download the App for mobile configuration.

Click **Exit** for the system to log out the current user and jump to the login page, as shown in the figure blow:

Figure 2-3-4 Login Page



Enter the correct management password of the device to reenter the configuration and management page.

2.3.2 Side Navigation Pane

The side navigation pane displays the function menu of the device (the menu items vary with the device model, and the actual functions prevail). Click a menu item to display corresponding configuration content in the main area on the right. Click **Collapse** in the lower left corner to fold the navigation pane to enlarge the main area.

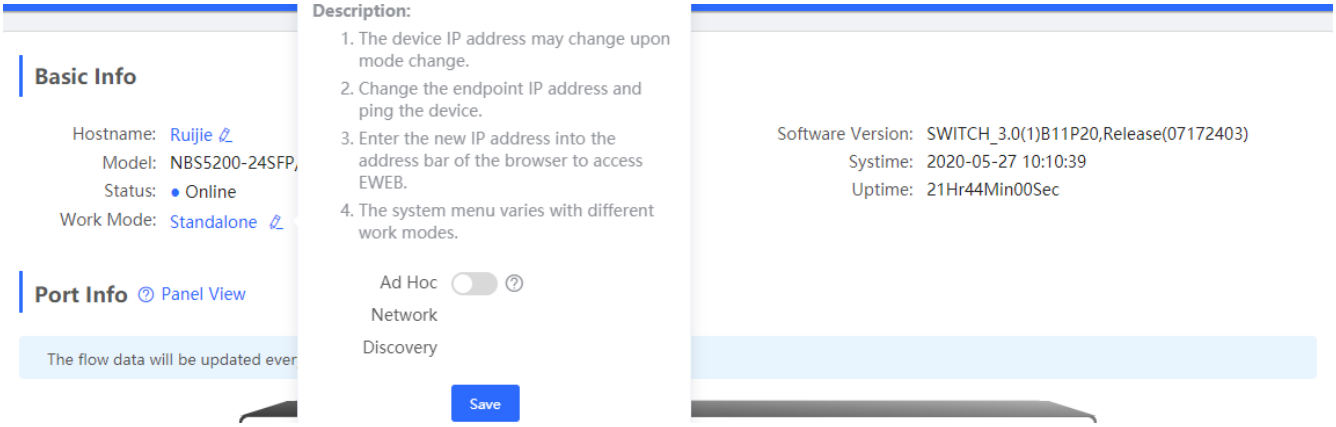
2.3.3 Main Configuration Area

The main configuration area is used to configure and display settings. The chapter eWeb Configuration describes major functions.

2.4 Work Mode

The device has two work modes: **Standalone** and **Ad Hoc Network Discovery** (default mode).

Figure 2-4-1 Mode Switching



- Mode switchover

Click in **Work Mode**, and click the **Ad Hoc Network Discovery** button on the displayed dialog box.

Tips:

1. The page will be refreshed after the work mode is switched over.
2. The system menu varies with the work mode, as shown in the figure below:

Figure 2-4-2 Ad Hoc Network Discovery Mode

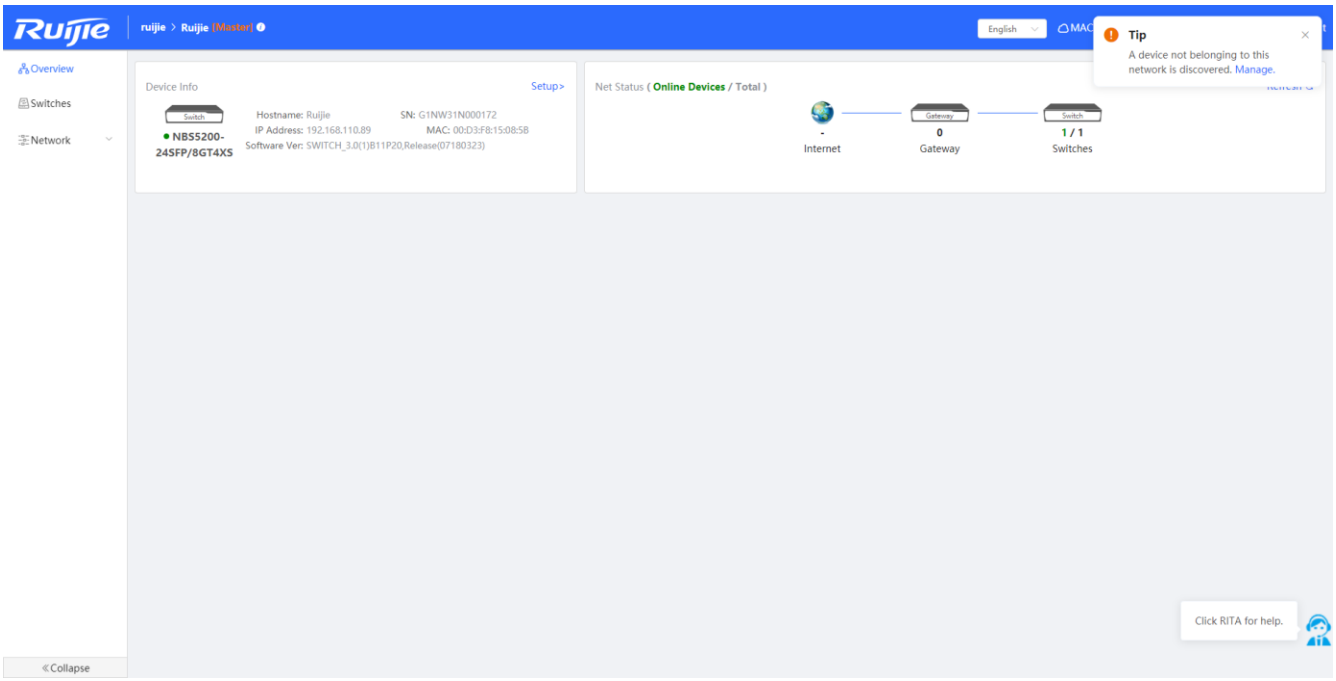
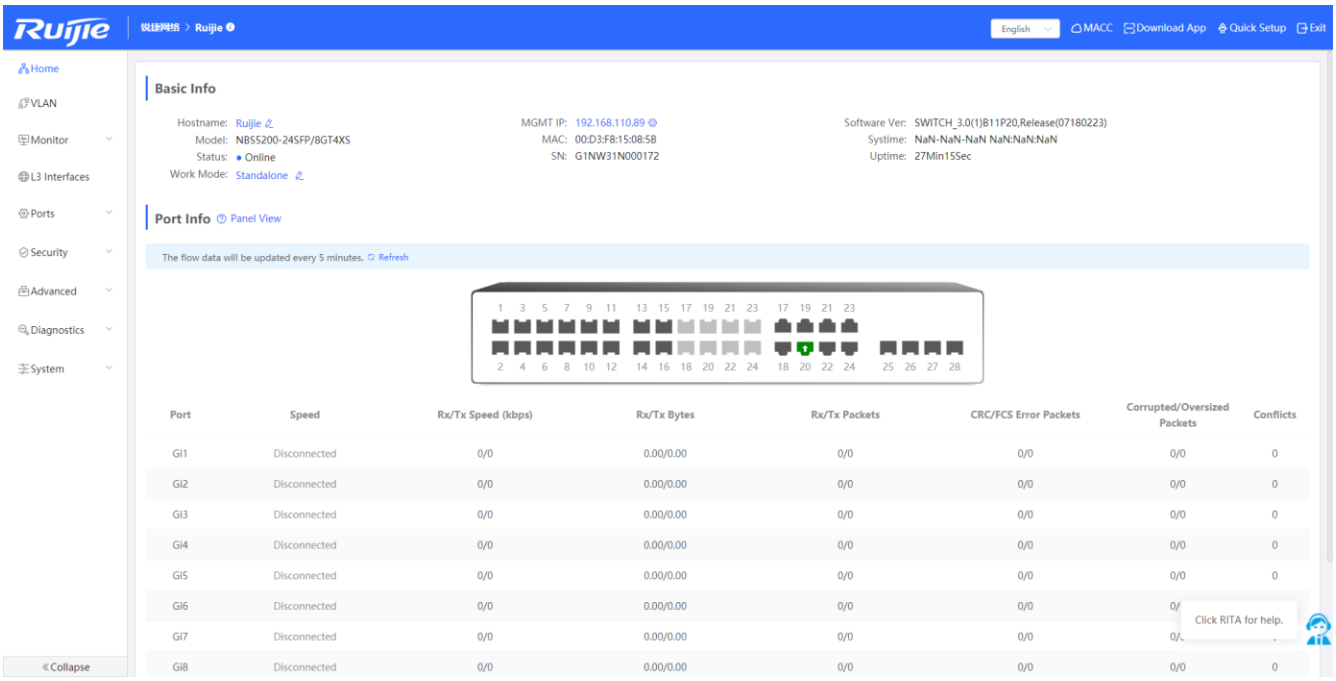


Figure 2-4-3 Standalone Mode



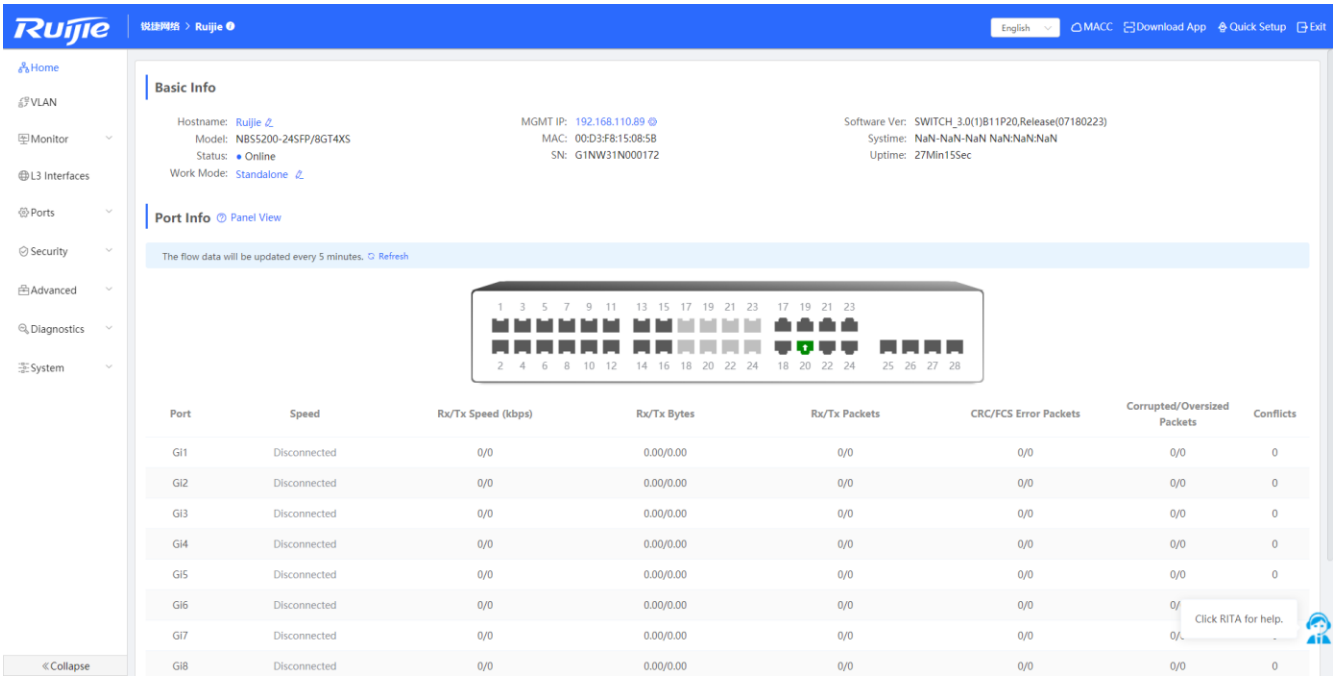
3 eWeb Configuration (Standalone Mode)

Functions are the same in different work modes. This chapter describes the Web configuration process of the switch in the standalone mode as an example.

3.1 Home

The **Home** module displays the basic information about the device and the switch ports, as shown in the figure below:

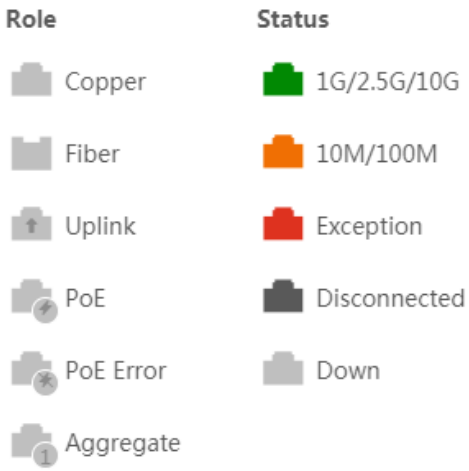
Figure 3-1-1 Home



The **Basic Info** area allows you to configure the device name and the management IP address, and switch ’over the work mode (described in the section Work Mode).

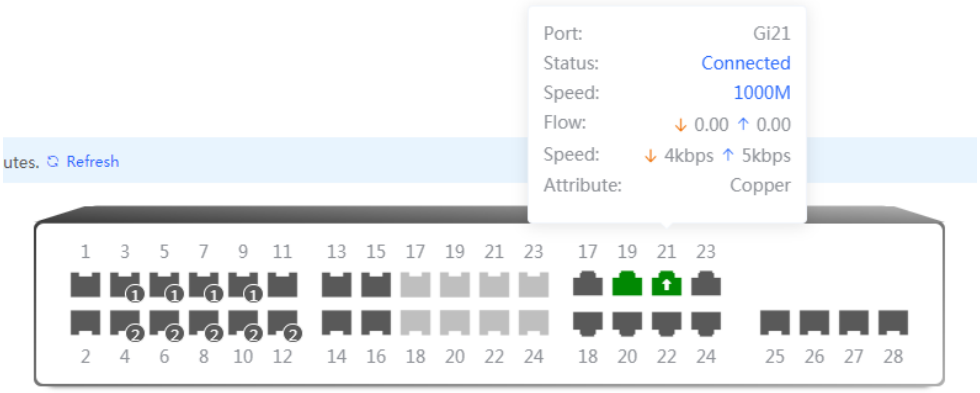
The **Port Info** area displays the details of all ports. Click **Panel View** to display the icon color and type corresponding to each port status.

Figure 3-1-2 Port Icons



Move the mouse to the port icon on the port panel to display more information, as shown in the figure below:

Figure 3-1-3 Port Panel Details

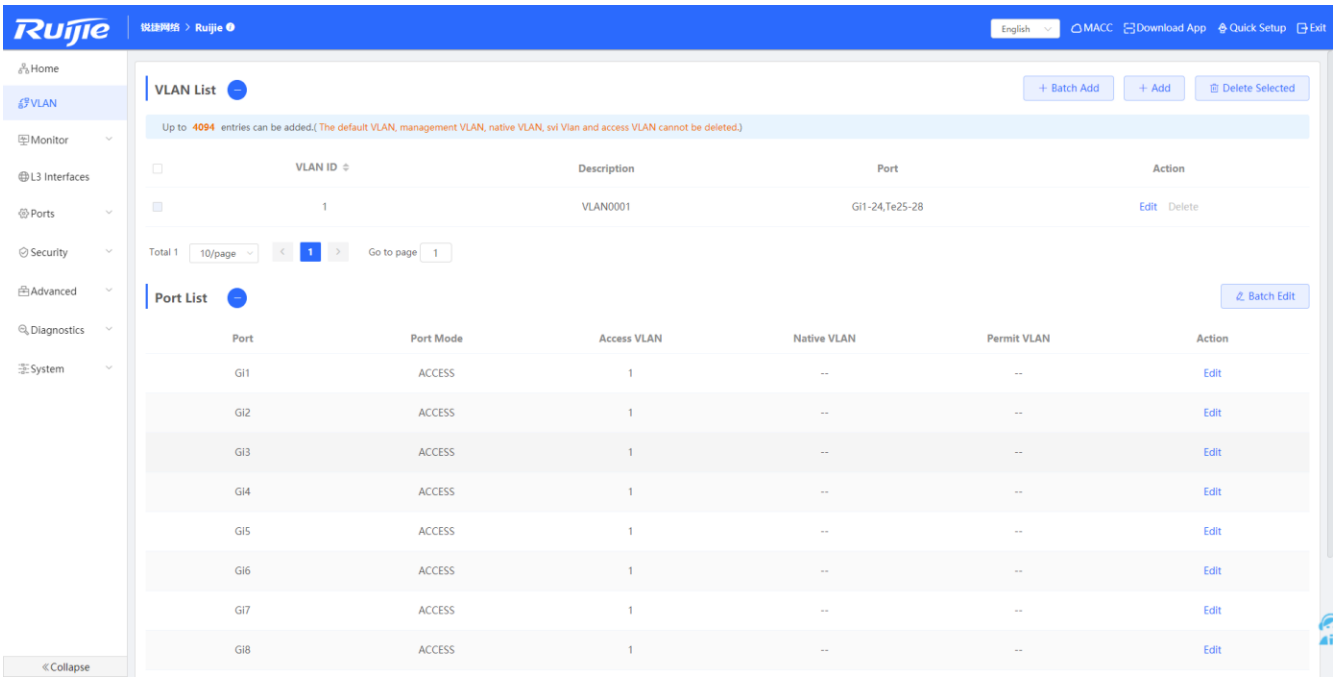


Click **Refresh** above the port panel to obtain the latest port traffic and status information.

3.2 VLAN

The **VLAN** module includes **VLAN List** and **Port List** (ports bound to VLANs).

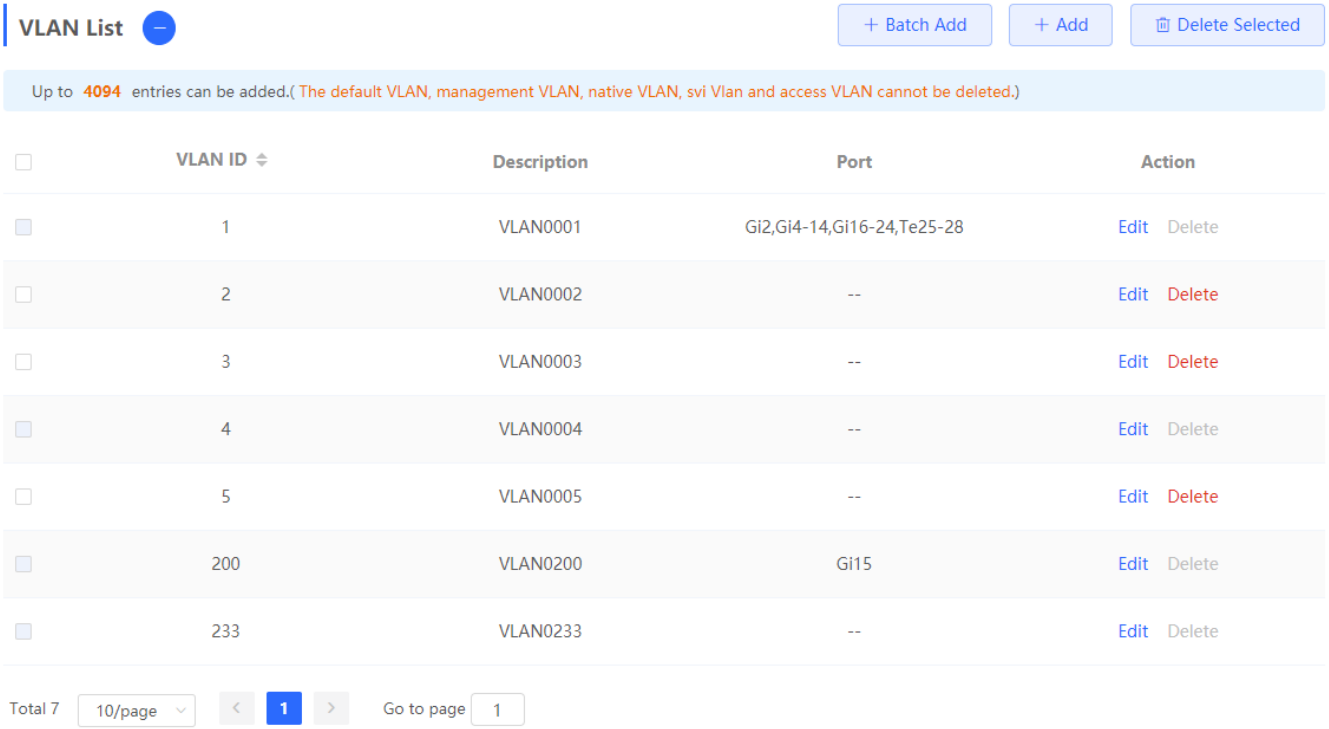
Figure 3-2-1 VLAN



Click ⊖ next to **VLAN List** or ⊕ next to **Port List** to fold or expand the list.

3.2.1 VLAN List

Figure 3-2-2 VLAN List



- Batch adding VLANs/Adding a single VLAN

1. Click **Batch Add**. In the displayed dialog box, enter VLANs or a VLAN range (separate multiple VLANs by using commas), and click **OK**. The added VLANs are displayed in **VLAN List**.
2. Click **Add**. In the displayed dialog box, enter a VLAN (mandatory) and VLAN description, and click **OK**. The added VLAN is displayed in **VLAN List**.

- Batch deleting VLANs/Deleting a single VLAN

1. Select multiple entries in **VLAN List** and click **Delete Selected**.
2. Click **Delete** in the **Action** column. The message "Are you sure you want to delete the VLAN?" is displayed. In the displayed dialog box, click **OK**. The message "Delete operation succeeded." is displayed.

- Editing a VLAN

1. Click **Edit** in the **Action** column. In the displayed dialog box, edit the VLAN description, and click **OK**. The message "Edit operation succeeded." is displayed.

Tips	1. The VLAN range is 1–4094. 2. The default VLAN (VLAN 1), management VLAN, native VLAN, and access VLAN cannot be deleted. 3. VLANs added in batches are separated by commas (","). 4. If no VLAN descriptions are configured when VLANs are added, the system creates VLAN descriptions in corresponding formats, for example, VLAN000XX. VLAN descriptions cannot be repeated. 5. The time for loading the **VLAN** page increases when there are many VLAN entries.

3.2.2 Port List

The **Port List** area allows you to configure the relationships between ports and VLANs. You can configure ports in batches or a single port.

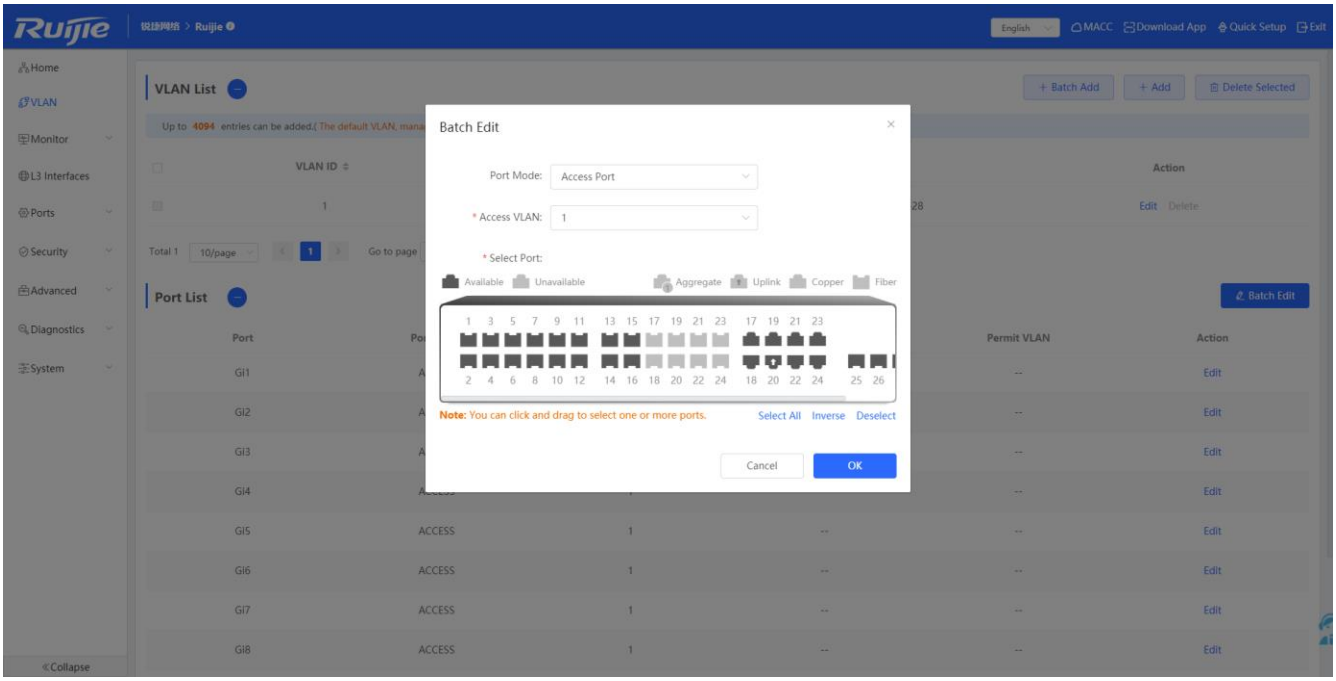
Figure 3-2-3 Port List

Port List  Batch Edit

Port	Port Mode	Access VLAN	Native VLAN	Permit VLAN	Action
Gi1			L3 Interfaces Gi1		
Gi2	ACCESS	1	--	--	Edit
Gi3			Member port of Ag1.		
Gi4	ACCESS	1	--	--	Edit
Gi5	ACCESS	1	--	--	Edit
Gi6	ACCESS	1	--	--	Edit
Gi7	ACCESS	1	--	--	Edit
Gi8	ACCESS	1	--	--	Edit
Gi9	ACCESS	1	--	--	Edit
Gi10	ACCESS	1	--	--	Edit

- Batch editing ports/Editing a single port

1. Click **Batch Edit**. In the displayed dialog box, select a port mode, select the required port, set the native VLAN or access VLAN, and click **OK**. The message "Operation succeeded." is displayed.
2. Click **Edit** in the **Action** column, configure the port mode and VLAN, and click **OK**. The message "Operation succeeded." is displayed.



Select ports on the port panel and set the port mode to **Access Port** or **Trunk Port**. In **Trunk Port** mode, configure permitted VLAN ranges (separated by commas ","), set VLAN IDs for the ports, and click **OK**. The port list and VLAN list will be updated correspondingly.

Tips:

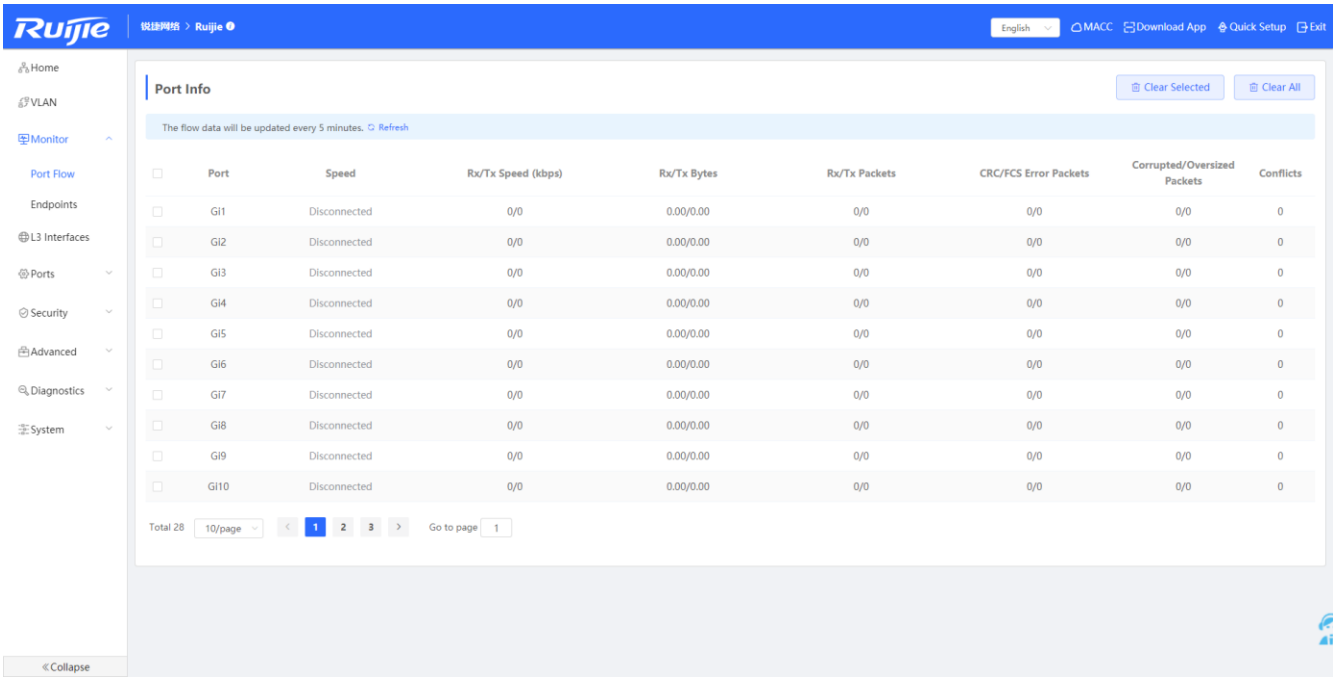
1. **In Access Port mode, if an access VLAN is configured, only packets tagged with the corresponding access VLAN ID are permitted. Untagged packets are automatically tagged with this VLAN ID**
2. **In Trunk Port mode, if a native VLAN is configured, untagged packets are automatically tagged with the corresponding native VLAN ID. Generally, the native VLAN is included in a permitted VLAN range. Otherwise, data may be blocked.**
3. **Improper configuration of port VLANs may lead to failure in accessing the eWeb management system. Exercise caution during the configuration.**

3.3 Monitor

3.3.1 Port Flow

The **Port Flow** module displays port flow data.

Figure 3-3-1 Port Flow



- Batch Clearing Data/Clearing All Data

Click **Batch Clear** or **Clear All** to clear statistics of port traffic and other data.

Tips:

1. Aggregate port flow will also be displayed. Traffic of an aggregate port is the sum of traffic of all member ports.

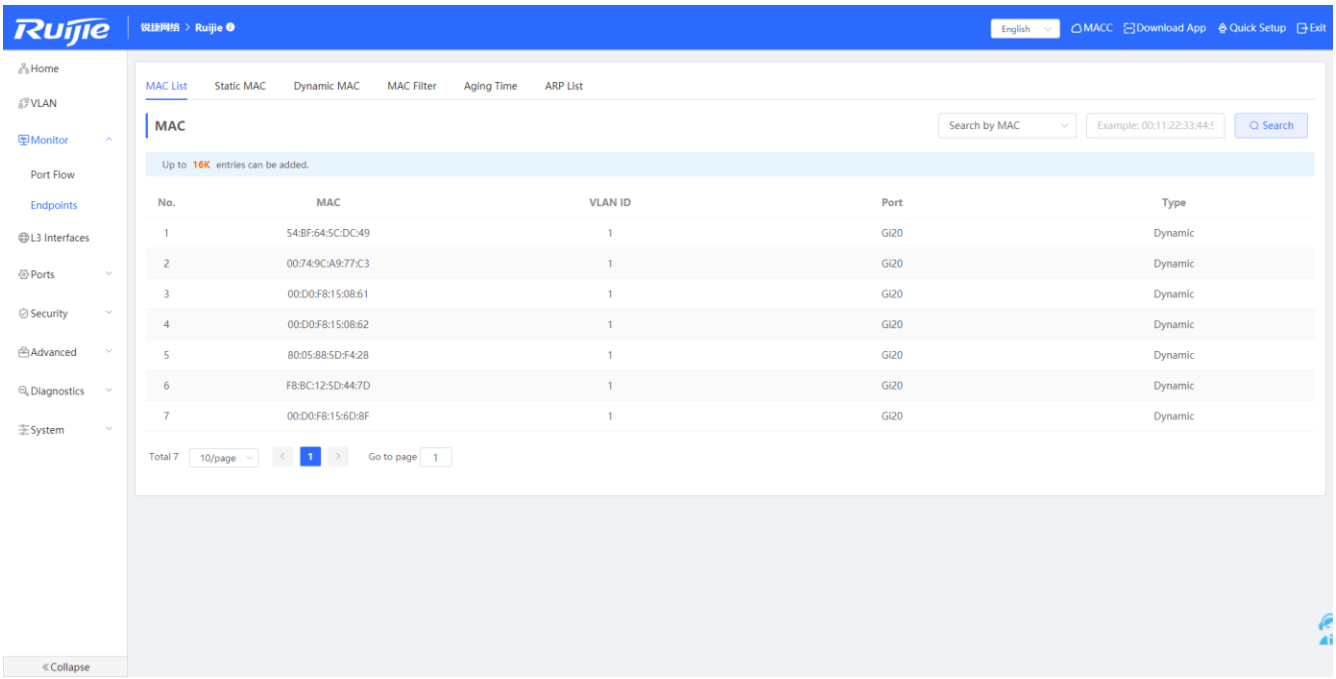
3.3.2 Endpoints

The **Endpoints** module includes **MAC List**, **Static MAC**, **Dynamic MAC**, **MAC Filter**, **Aging Time**, and **ARP List**.

3.3.2.1 MAC List

The **MAC List** page displays MAC addresses learned by the device, including dynamic and static MAC addresses.

Figure 3-3-2 MAC List



- Search

Select the search type (**Search by MAC**, **Search by VLAN**, or **Search by Port**), enter the term to be searched for, and click **Search** to filter MAC addresses that meet the search conditions.

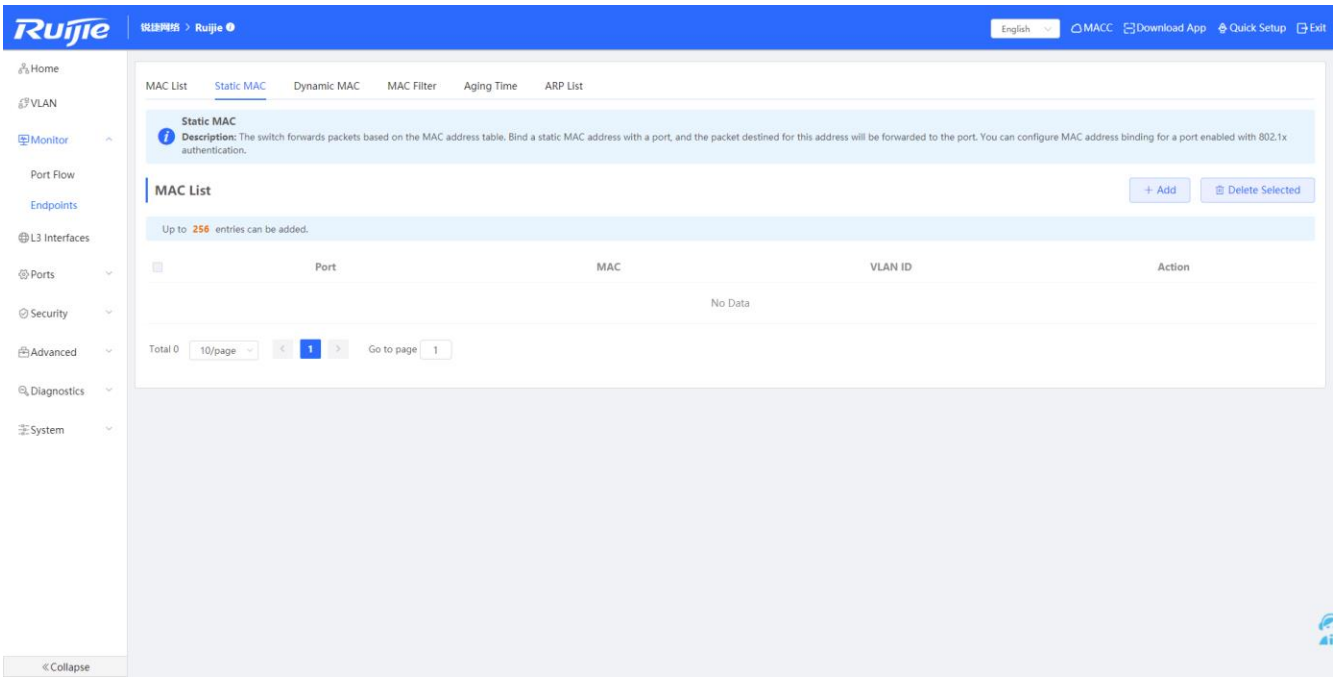
Tips:

1. The MAC address capacity varies with the device. The MAC address capacity is 16K in the figure above.

3.3.2.2 Static MAC

The **Static MAC** page displays the MAC-port binding relationship.

Figure 3-3-3 Static MAC



- Adding a static address

Click **Add**. In the displayed dialog box, enter the MAC address and VLAN, select a port, and click **OK**. The message "Add operation succeeded." is displayed, and the MAC list is updated.

- Batch deleting static MAC addresses/Deleting a single static MAC address

1. Select the target MAC address in **MAC List**, and click **Delete Selected**. In the displayed confirmation box, click **OK**. A message indicating successful deletion is displayed, and the MAC list is updated.
2. Click **Delete** in the **Action** column. The message "Are you sure you want to delete the entry?" is displayed. In the displayed confirmation box, click **OK** in the displayed dialog box. The message "Delete operation succeeded." is displayed.

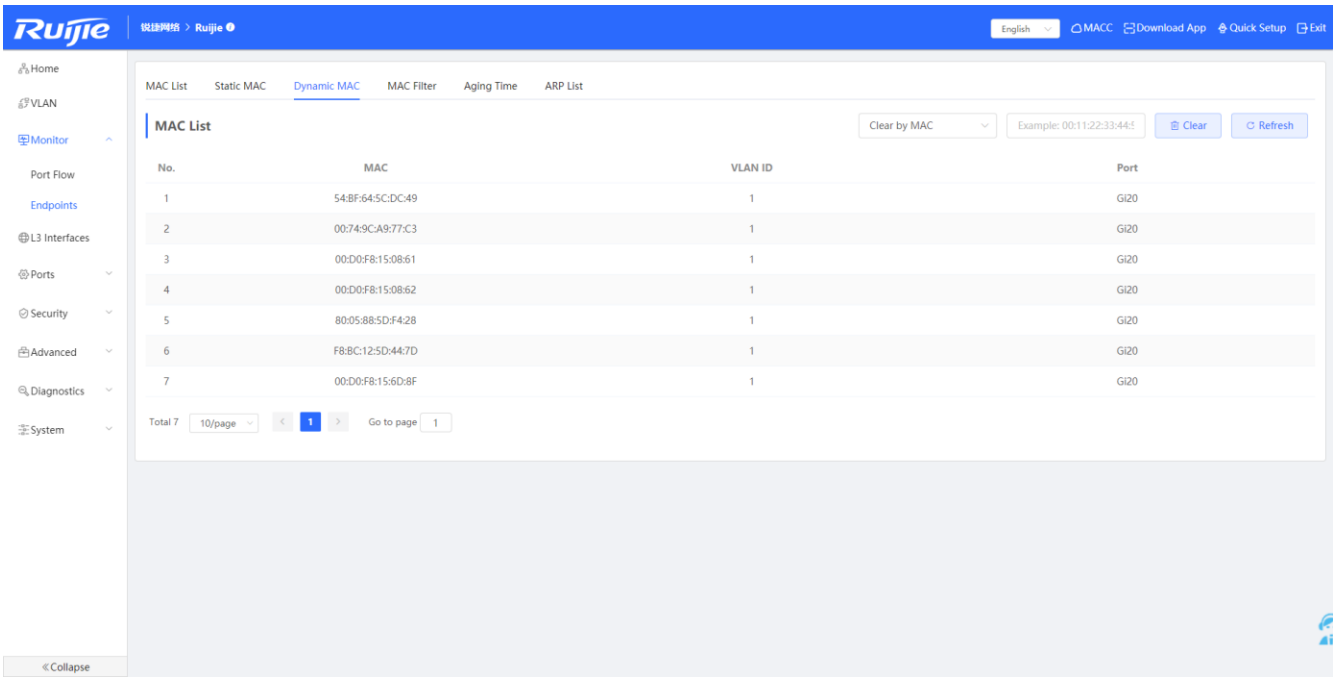
Tips:

The switch forwards packets based on the MAC address table. Bind a static MAC address with a port, and the packet destined for this address will be forwarded to the port. You can configure MAC address binding for a port enabled with 802.1x authentication.

3.3.2.3 Dynamic MAC

The **Dynamic MAC** page displays dynamic MAC addresses learned by the device.

Figure 3-3-4 Dynamic MAC



- Clear

Select the clear type (**Clear by MAC**, **Clear by Port**, or **Clear by VLAN**), enter a search term, and click **Clear** to clear MAC addresses that meet the clear conditions.

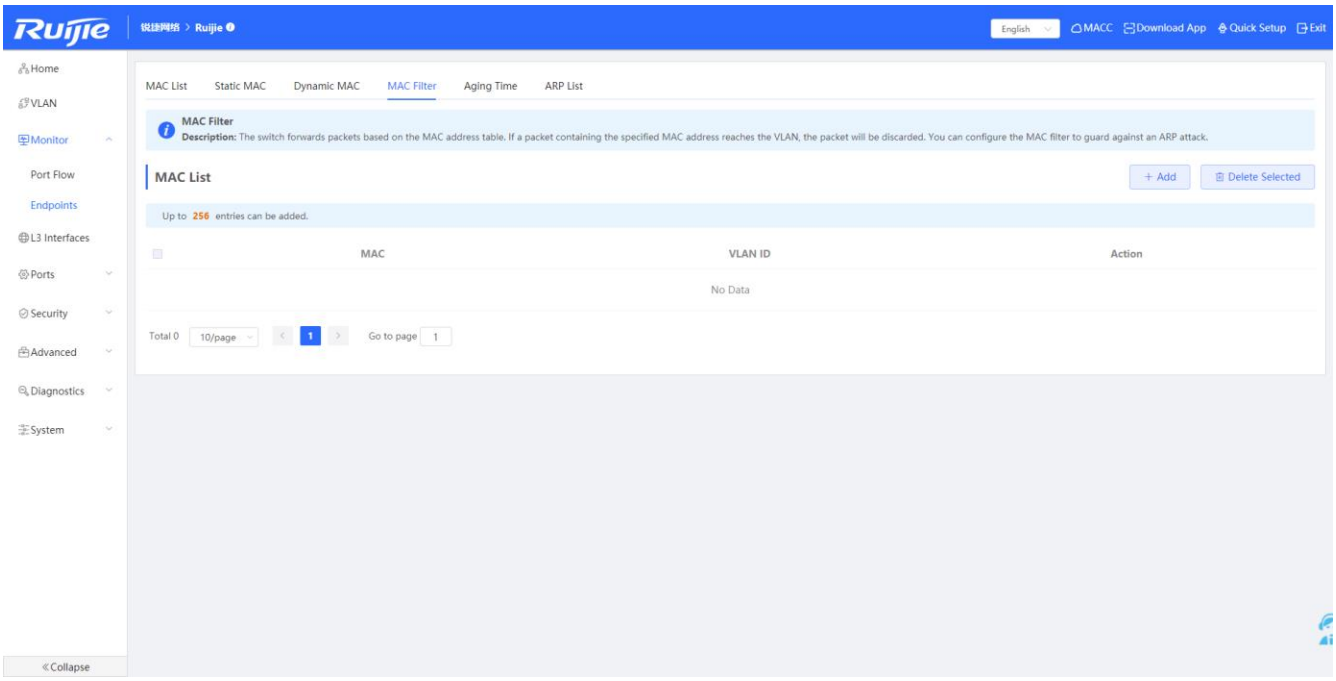
- Refresh

Click **Refresh** to display the latest dynamic MAC addresses.

3.3.2.4 MAC Filter

The **MAC Filter** page displays the MAC-port binding relationship to filter packets that meet this filter condition.

Figure 3-3-5 MAC Filter



- Adding a MAC address to be filtered

Click **Add**. In the displayed dialog box, enter the MAC address and VLAN, and click **OK**. The message "Add operation succeeded." is displayed and the MAC list is updated.

- Batch deleting MAC addresses/Deleting a single MAC address

1. Select the target MAC address, and click **Delete Selected**. In the displayed confirmation box, click **OK**. The message "Delete operation succeeded." is displayed and the MAC list is updated.
2. Click **Delete** in the **Action** column. The message "Are you sure you want to delete the entry?" is displayed. In the displayed confirmation box, click **OK** in the displayed dialog box. The message "Delete operation succeeded." is displayed.

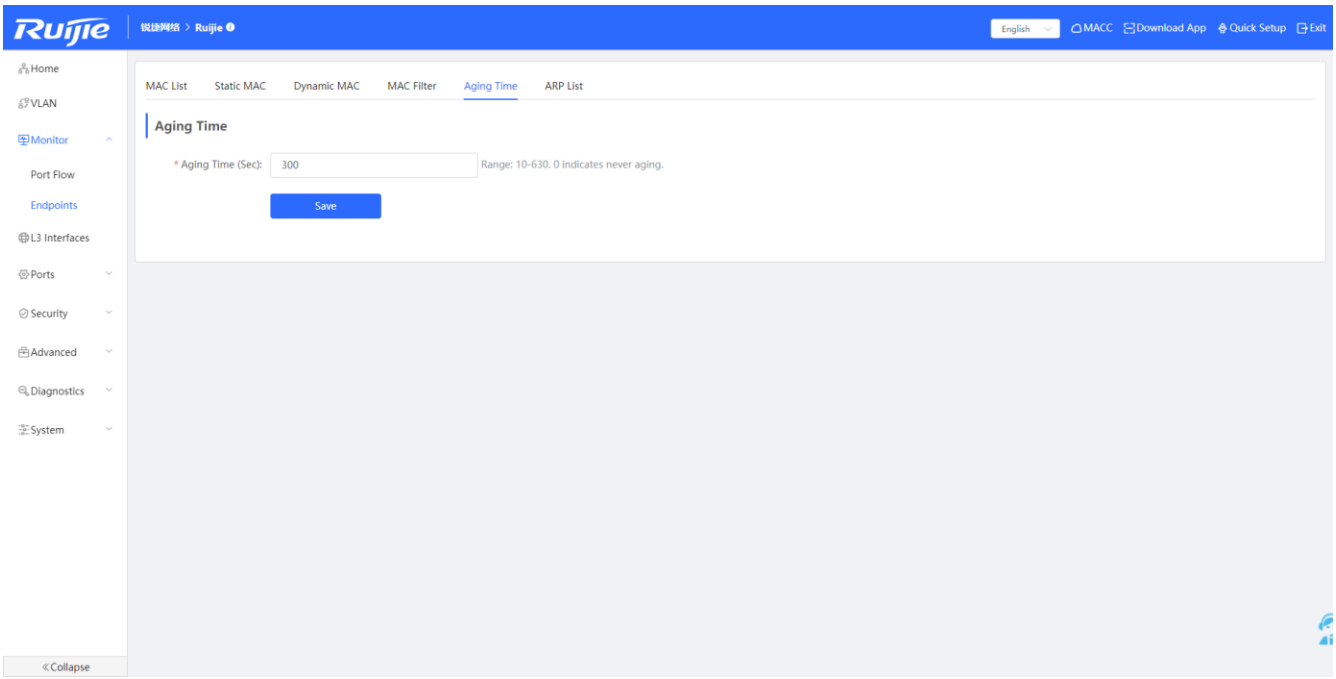
Tips:

The switch forwards packets based on the MAC address table. If a packet containing the specified MAC address reaches the VLAN, the packets will be discarded. You can configure MAC address filter to guard against an ARP attack.

3.3.2.5 Aging Time

The **Aging Time** page allows you to configure the aging time of MAC address learned by the device.

Figure 3-3-6 Aging Time



- Configuring the aging time

Enter a valid aging time, and click **Save**. The message "Operation succeeded." is displayed, indicating that the aging time of MAC addresses learned by the device is successfully configured.

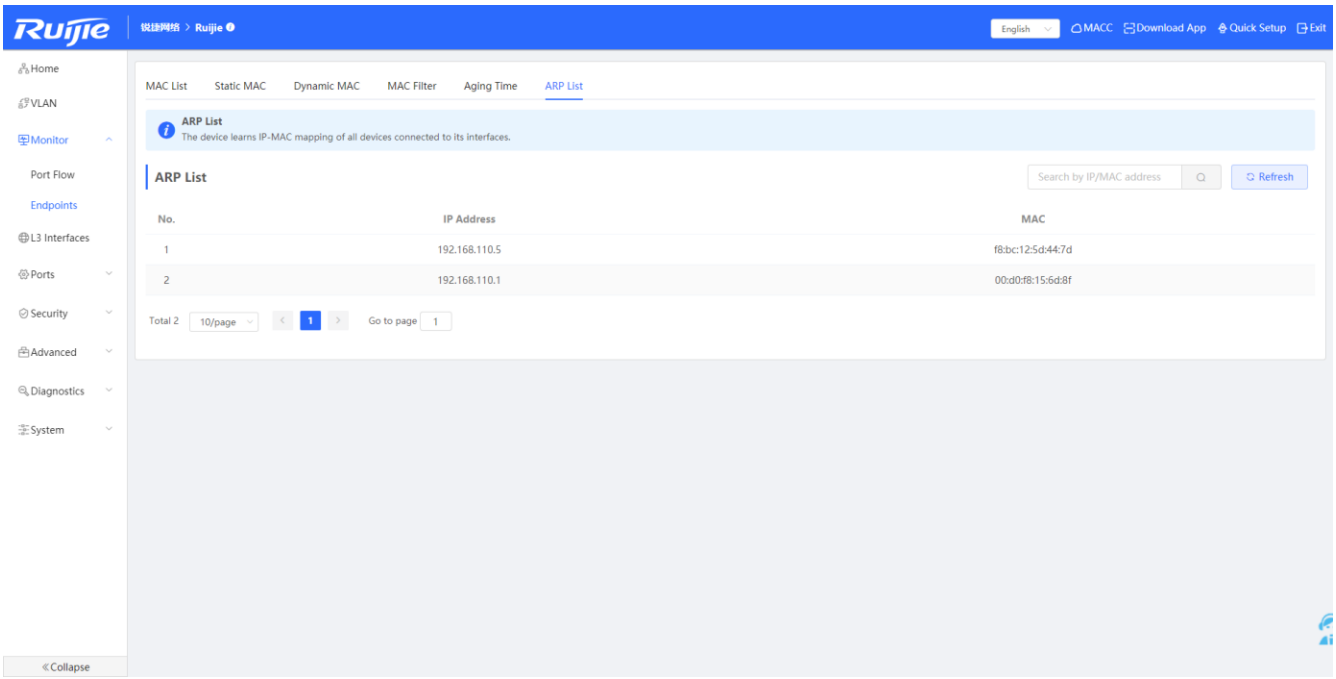
Tips:

The aging time of the device ranges from 10 to 630 seconds. The value 0 indicates that the MAC addresses do not age.

3.3.2.6 ARP List

The Address Resolution Protocol (ARP) is used to bind MAC addresses to IP addresses. If you enter an IP address, you can obtain the MAC address bound to this IP address through ARP. Once a MAC address is known, the relationship between an IP address and the MAC address is saved in the ARP cache of the device. With MAC addresses, the IP-based device can encapsulate frames at the link layer and then send the data frames to LANs. By default, IP and ARP packets on Ethernets are encapsulated in the Ethernet II type.

Figure 3-3-7 ARP List



3.4 L3 Interfaces

3.4.1 L3 Interfaces

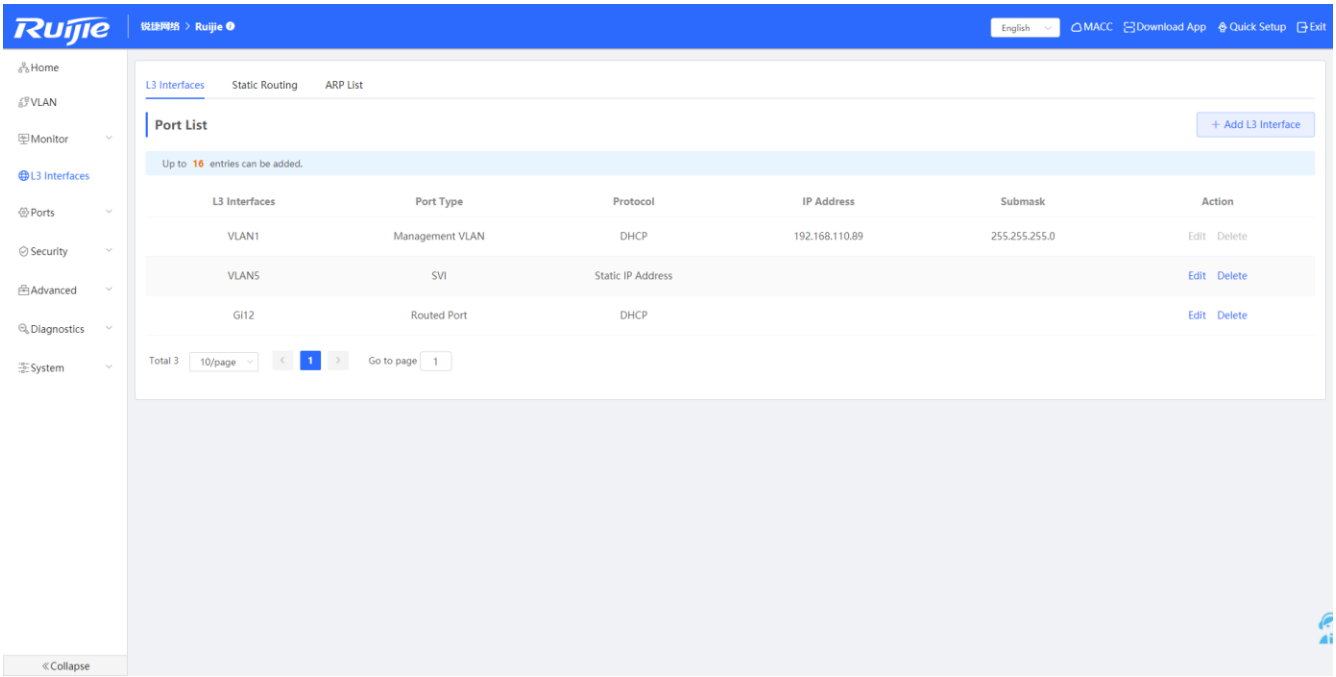
The **L3 Interfaces** module allows you to configure layer-3 interfaces.

There are three types of layer-3 interfaces available:

- Routed Port
- A physical port of a layer-3 device can be configured as a routed port. A routed port works as an access port and does not support layer-2 switching.
- L3 Aggregate Port
- A layer-3 aggregate port is a logical interface consisting of layer-3 physical interfaces of the same type. It virtualizes physical links into one link so as to increase the link rate. A layer-3 aggregate port supports load balancing among its member links. If a member link fails, traffic will be automatically switched to the other available links, which improves link reliability. A layer-3 aggregate port does not support layer-2 switching.
- SVI

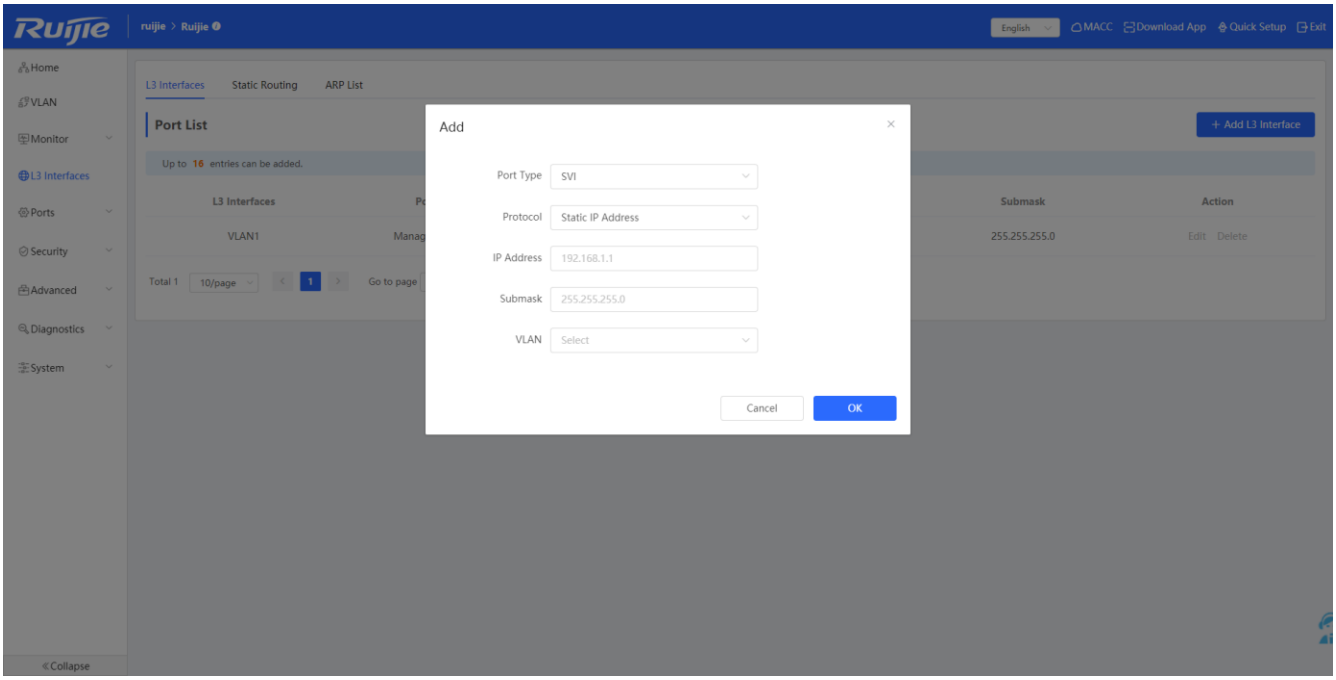
An SVI can be used as a management interface. You can also create an SVI for inter VLAN routing.

Figure 3-4-1 L3 Interfaces



3.4.1.1 Add an SVI

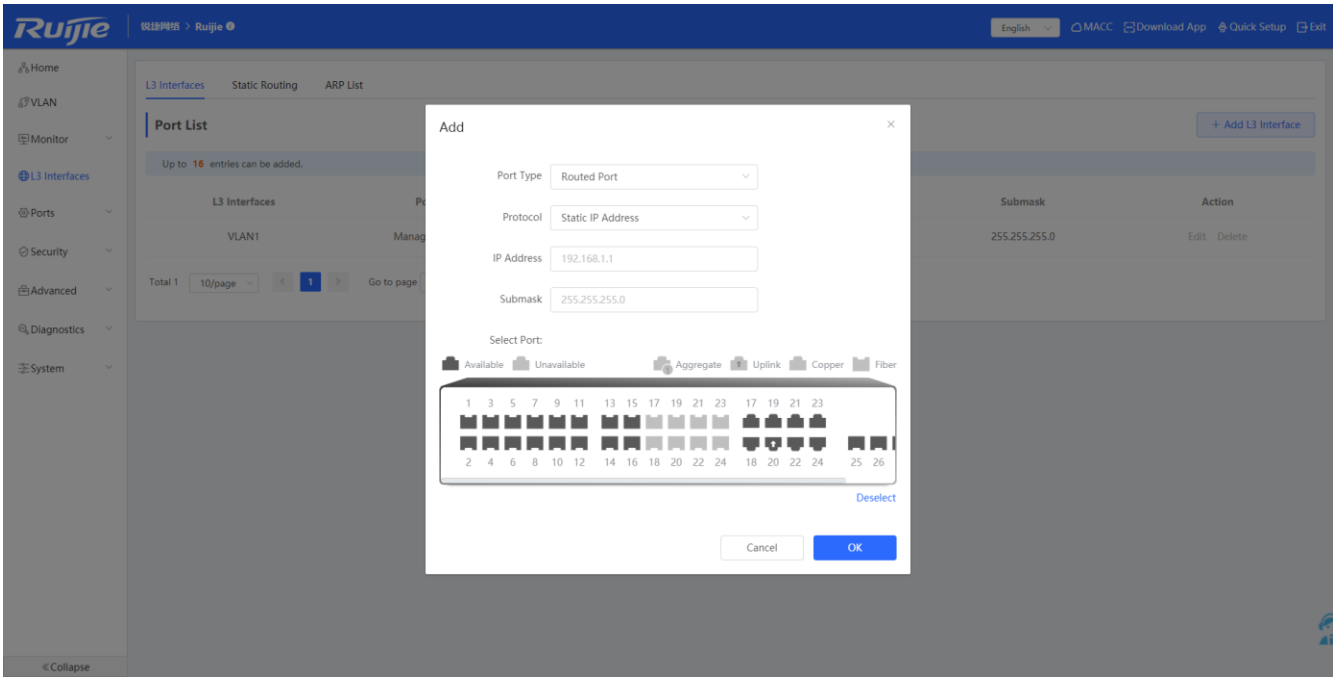
Figure 3-4-2 Adding an SVI



1. Select **SVI** from the **Port Type** dropdown list.
2. Select a protocol. If you select **Static IP Address**, you can set the IP address and the subnet mask manually (optional). If you select **DHCP**, the SVI will obtain a DHCP-assigned IP address.
3. If you want to configure an SVI for a VLAN, please make sure that the VLAN is already created.
4. Click **Save**. The message "Operation succeeded." is displayed.

3.4.1.2 Add a Routed Port

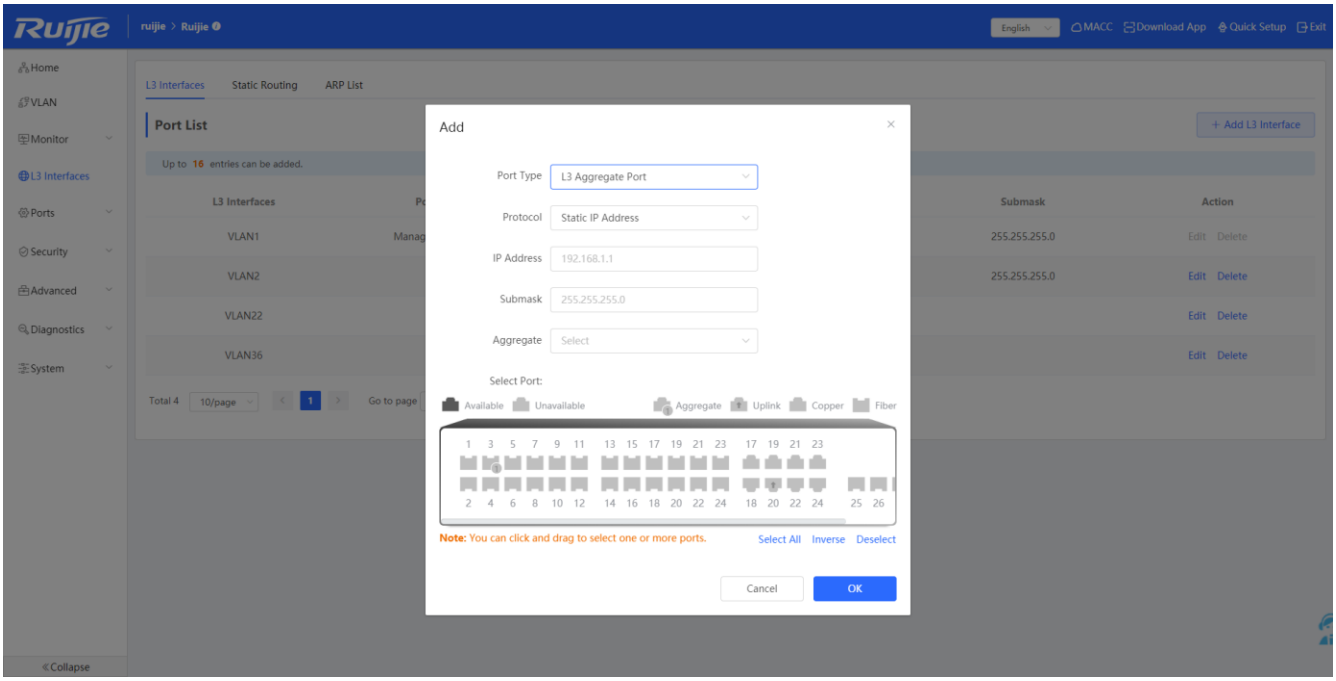
Figure 3-4-3 Adding a Routed Port



1. Select **Routed Port** from the **Port Type** dropdown list.
2. Select a protocol. If you select **Static IP Address**, you can set the IP address and the subnet mask manually (optional). If you select **DHCP**, the routed port will obtain a DHCP-assigned IP address.
3. Select a physical port from the panel.
4. Click **Save**. The message "Operation succeeded." is displayed.

3.4.1.3 Add a L3 Aggregate Port

Figure 3-4-4 Adding a L3 Aggregate Port



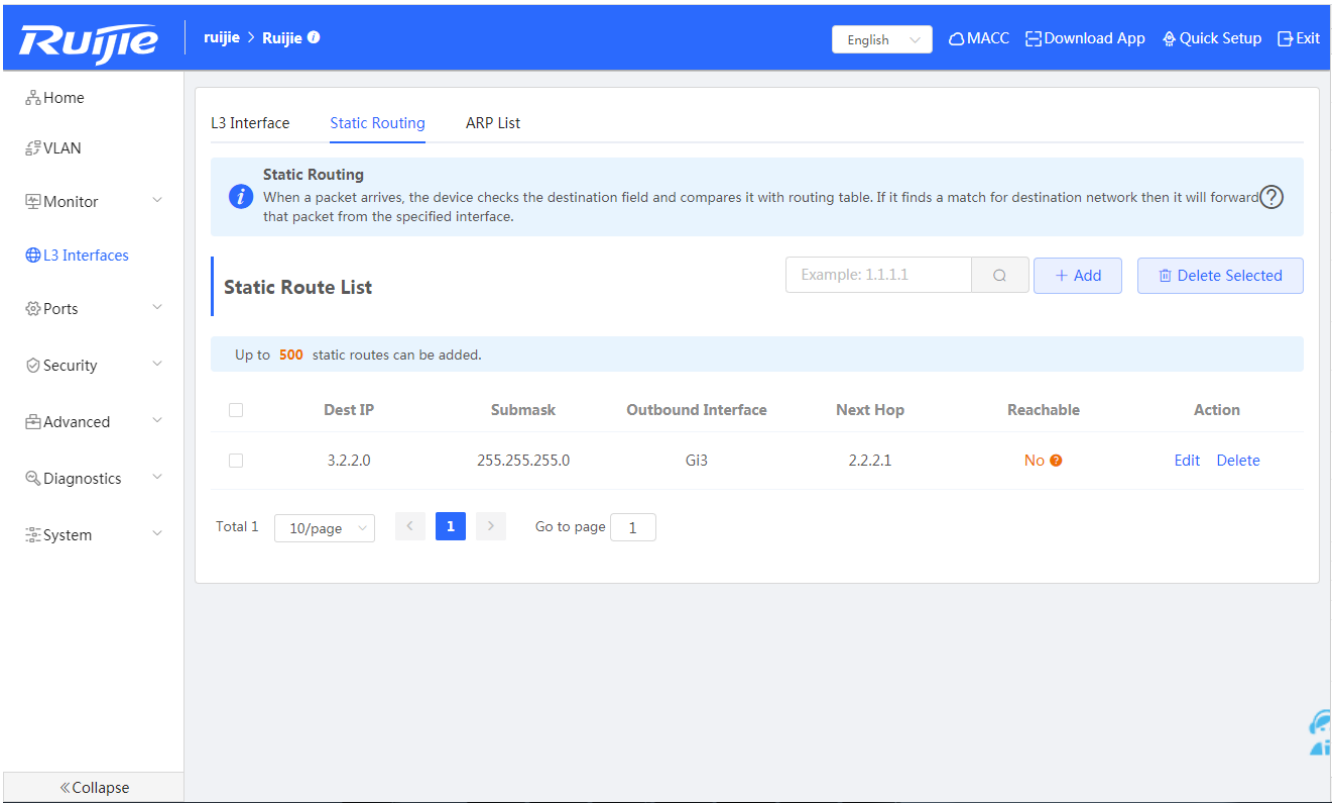
1. Select **Routed Port** from the **Port Type** dropdown list.
2. Select a protocol. If you select **Static IP Address**, you can set the IP address and the subnet mask manually (optional). If you select **DHCP**, the routed port will obtain a DHCP-assigned IP address.
3. Set an aggregate port and select its member ports from the panel. Please configure its member ports as routed ports first.
4. Click **Save**. The message "Operation succeeded." is displayed.

3.4.2 Static Routing

The **Static Routing** module allows you to add static routes.

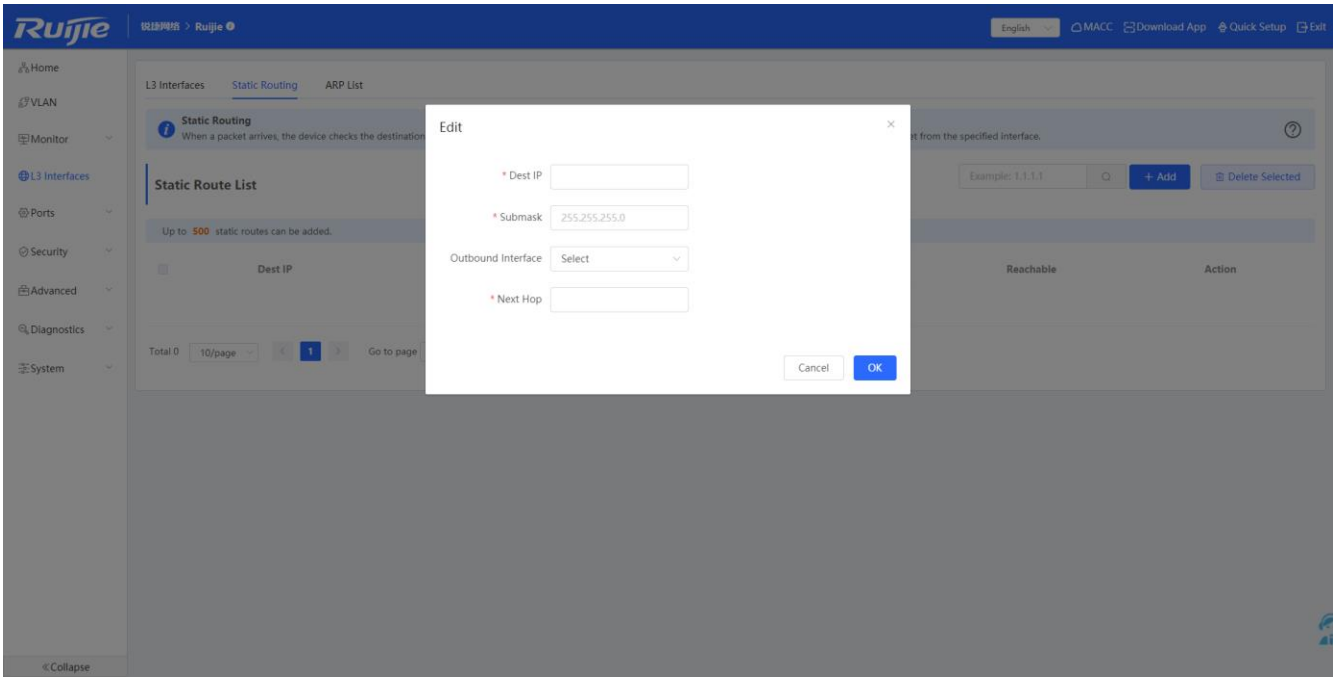
A static route is created manually and cannot accommodate changes to topological changes. Therefore, it is mainly applied to a simple network. When a network error occurs or the topology changes, the administrator needs to edit static route settings.

Figure 3-4-5 Static Routing



3.4.2.1 Add a Generic Static Route

Figure 3-4-6 Adding a Generic Static Route

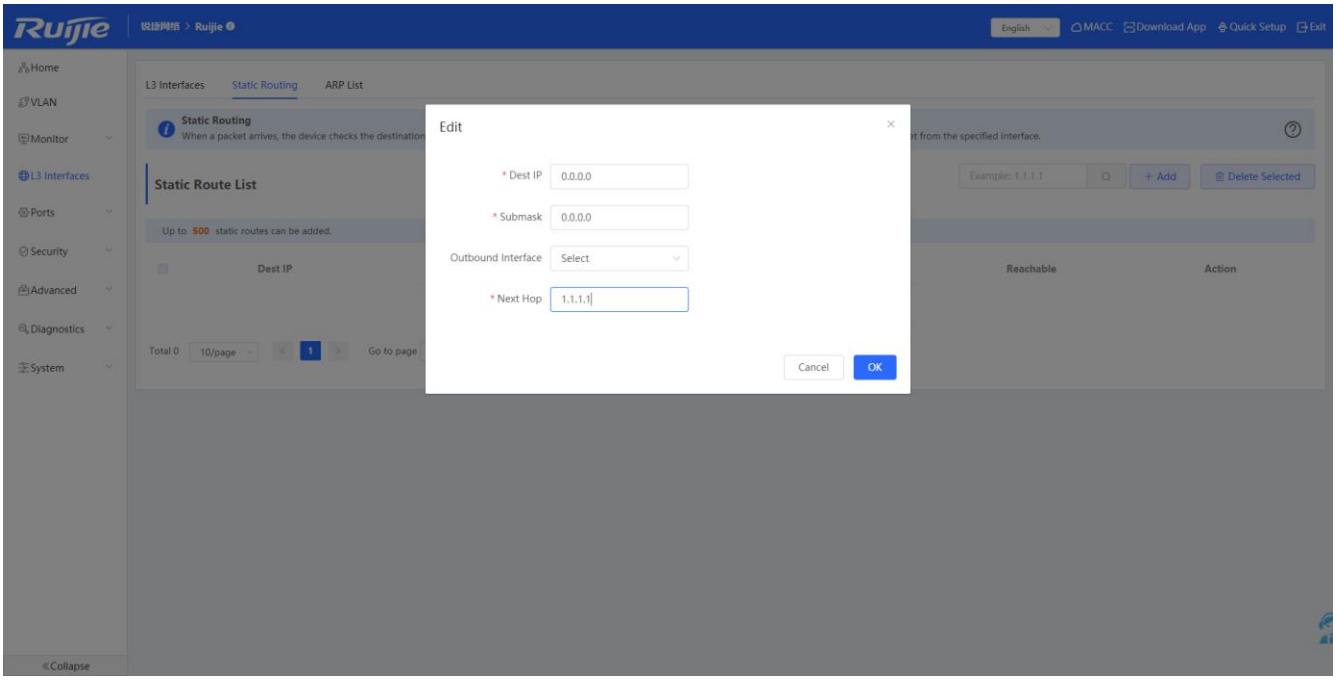


1. Specify a destination IP address and a subnet mask.
2. Select an outbound interface from the **Outbound Interface** dropdown list.
3. Set a next hop address. If the outbound interface is enabled with PPPoE, the next hop address is not required.
4. Click **Save**. The message "Operation succeeded." is displayed.

3.4.2.2 Add a Default Static Route

A default route is a route with the destination IP address set to all 0s. A manually configured default route is a default static route. If the destination address of a packet does not match any entries in the routing table, the device forwards the packet along the default route instead. The default static route can be configured on stub routers.

Figure 3-4-7 Adding a Default Static Route

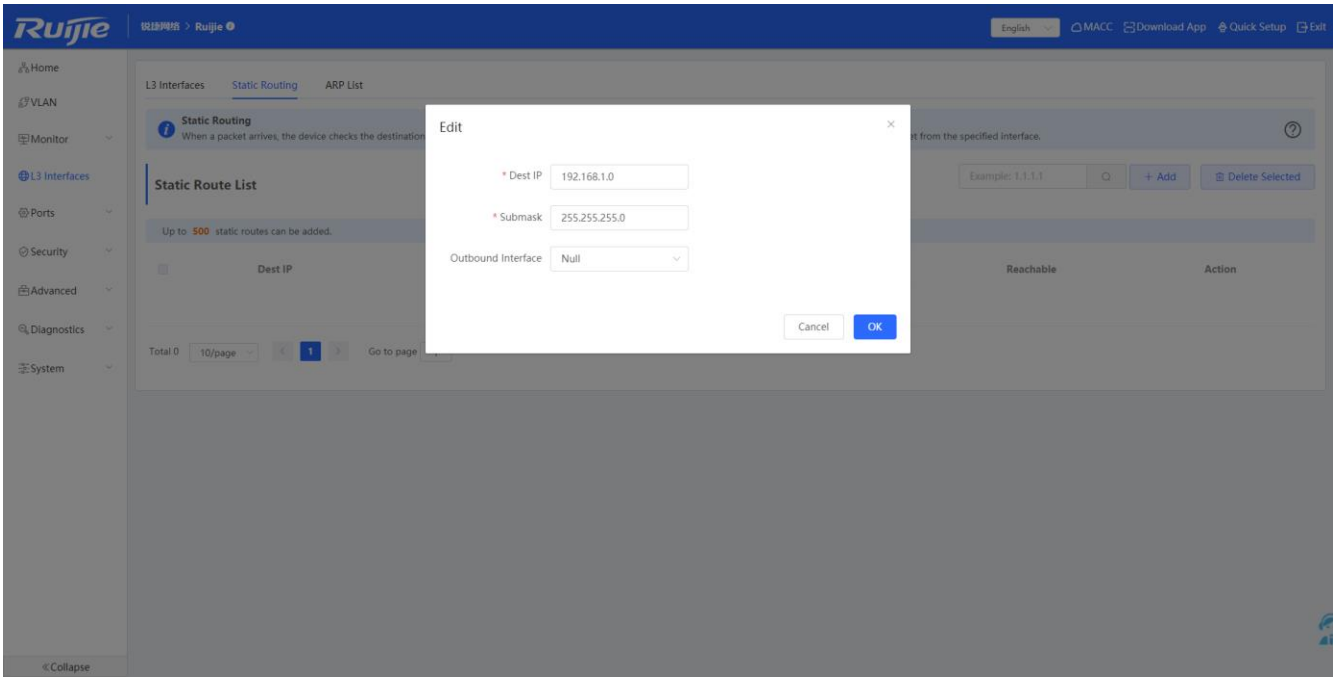


1. Set both the destination IP address and the subnet mask to all 0s.
2. Set a next hop address.
3. Click **Save**. The message "Operation succeeded." is displayed.

3.4.2.3 Add a Static Blackhole Route

Packets are routed over a blackhole route to a null interface. The null interface is a virtual interface which cannot be configured with an IP address. Therefore, the packets routed to this interface will be discarded.

Figure 3-4-8 Adding a Default Blackhole Route

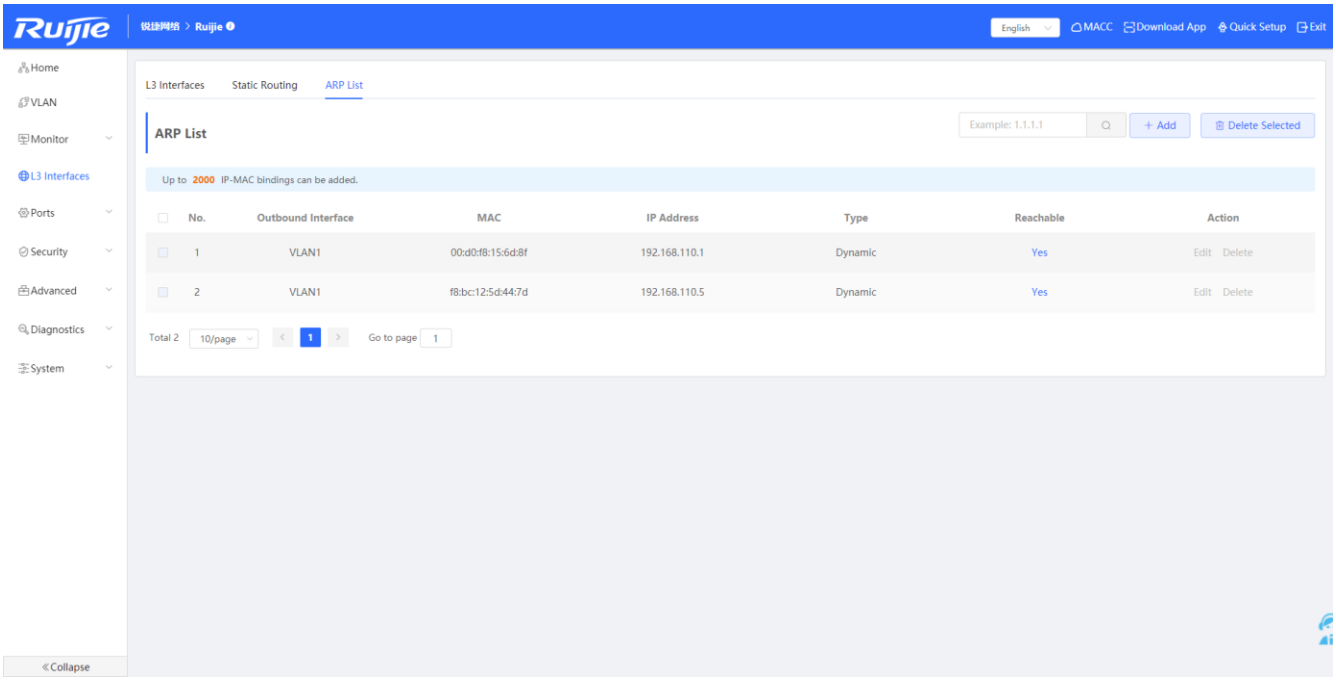


1. Specify a destination IP address and a subnet mask.
2. Select **Null** from the **Outbound Interface** dropdown list.
3. Click **Save**. The message "Operation succeeded." is displayed.

3.4.3 ARP List

The **ARP List** module displays all static and dynamic ARP entries.

Figure 3-4-9 ARP List



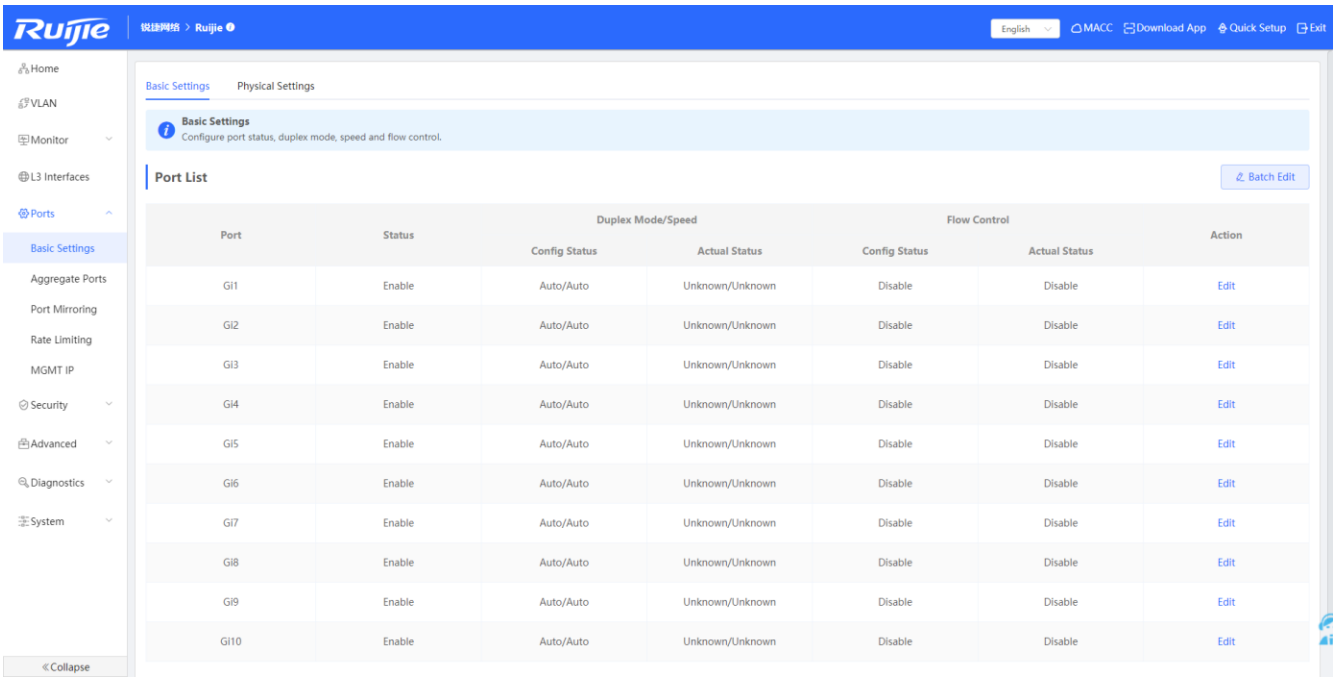
3.5 Ports

The **Ports** module allows you to set basic port information, port aggregation, port mirroring, port rate limit, management IP address, and PoE.

3.5.1 Basic Settings

The **Basic Settings** module allows you to configure the port status, duplex mode, flow control and physical settings.

Figure 3-5-1 Basic Settings



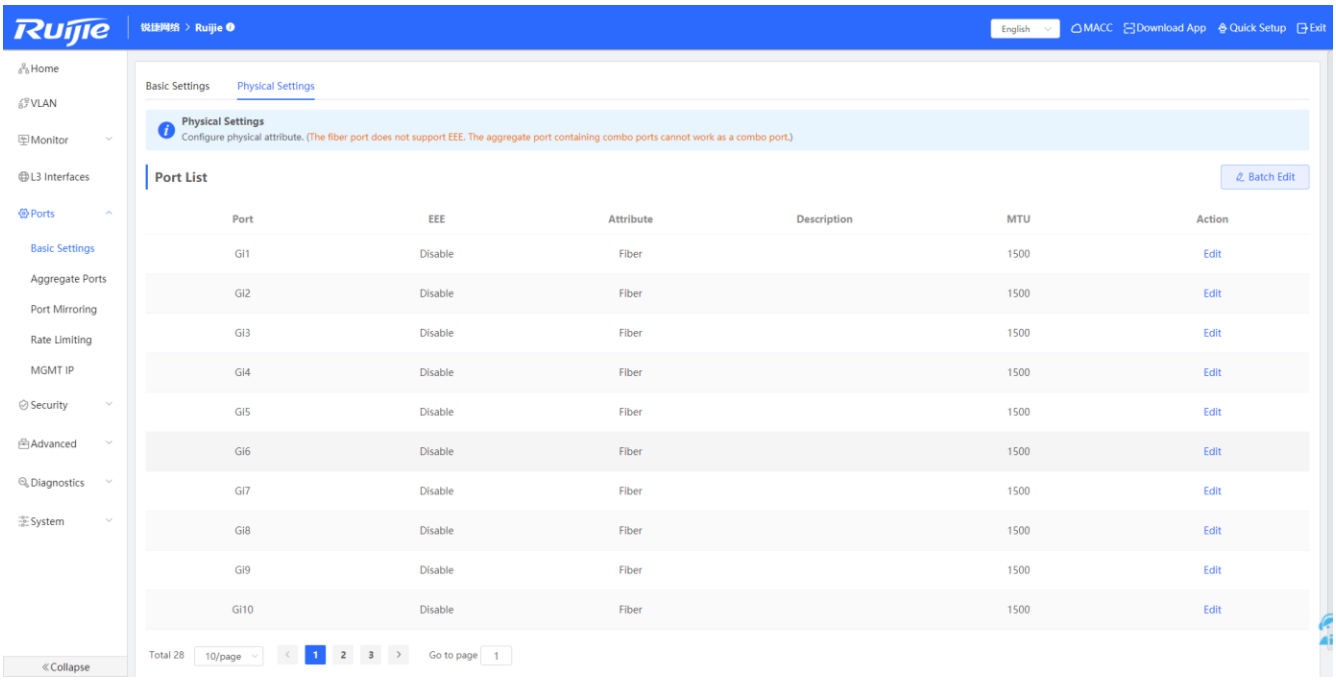
- Batch editing ports/Editing a single port

1. Click **Batch Edit**. In the displayed dialog box, select the target port, set the port status, speed, and mode, and click **OK**.
2. Click **Edit** in the **Action** column. In the displayed dialog box, select the target port, set the port status, speed, and mode, and click **OK**.

Tips:

1. Configuration items for ports with different attributes (1000M port, 10G port, and fiber port) vary.
2. During batch configuration, only the common configuration items are configurable.

Figure 3-5-2 Physical Settings



- Batch editing ports/Editing a single port

1. Click **Batch Edit**. In the displayed dialog box, select the target port, and set the EEE, port mode, and port description, MTU value, and click **OK**.
2. Click **Edit** in the **Action** column. In the displayed dialog box, set the EEE, port mode, and port description, MTU value, and click **OK**.

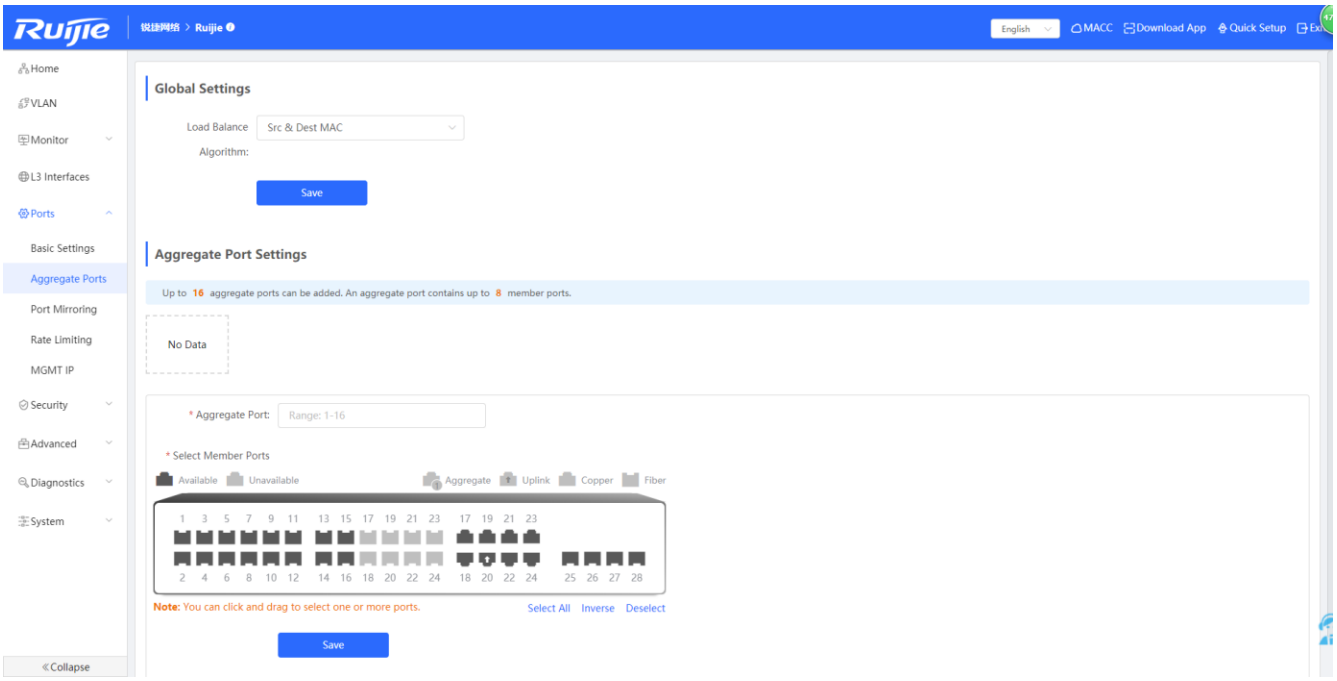
Tips:

1. Configuration items for ports with different attributes vary.
2. Only the SFP combo ports support port mode switchover.
3. Fiber ports do not support EEE configuration.
4. Copper ports and fiber ports cannot be simultaneously configured during batch configuration.

3.5.2 Aggregate Ports

The **Aggregate Ports** module includes **Global Settings** and **Aggregate Port Settings**.

Figure 3-5-3 Aggregate Ports



- Global Settings

Select a value from the **Load Balance Algorithm** drop-down list box, and click **Save**.

- Adding an aggregate port

Enter an aggregate port ID, select member ports (ports that have been added to another aggregate port cannot be selected), and click **Save**. The message "Operation succeeded." is displayed. The port panel displays the added aggregate port.

- Batch deleting aggregate ports/Deleting a single aggregate port

In the aggregate port list, click to select aggregate ports, and click **Delete Selected**. In the displayed confirmation box, click **OK**. A deleted aggregate port becomes available on the port panel.

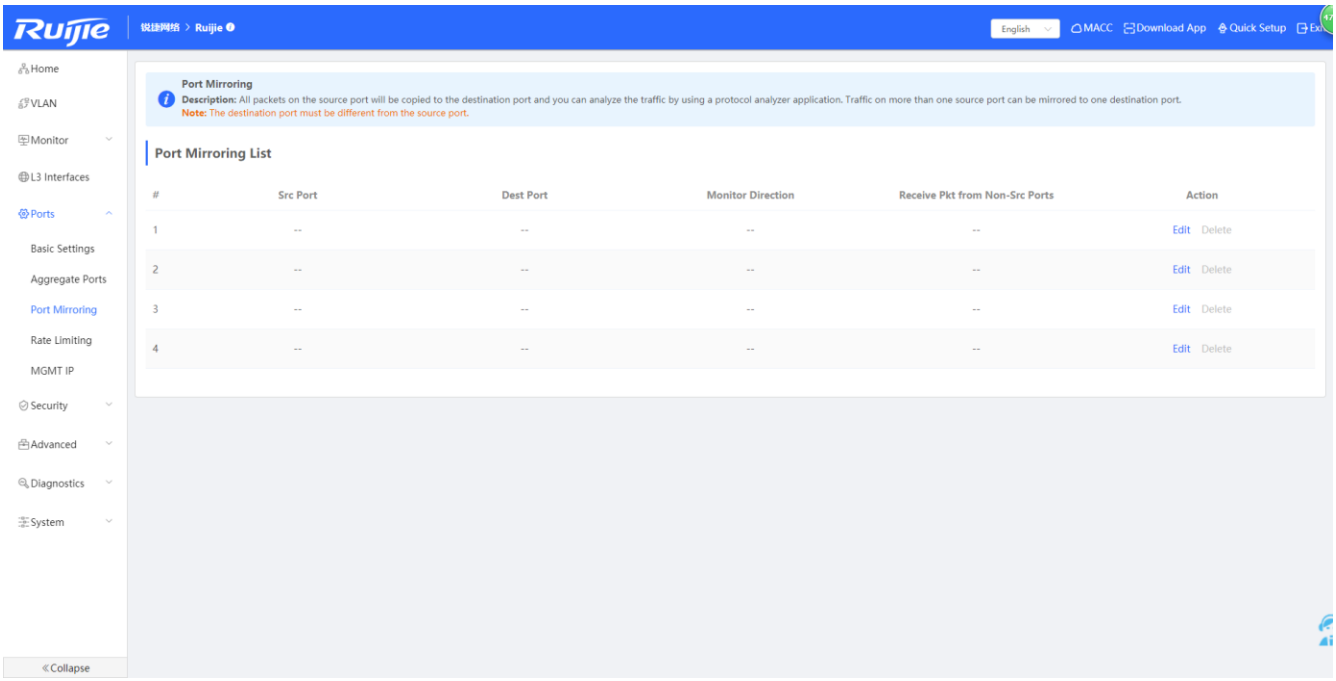
Tips:

1. A port that has been added to an aggregate port cannot be selected and added to another one.
2. After an aggregate port is deleted, its member ports are restored to the default settings and are disabled.
3. An aggregate port contains a maximum of eight member ports.

3.5.3 Port Mirroring

The **Port Mirroring** module allows you to configure port mirroring. A maximum of four port mirroring entries are supported.

Figure 3-5-4 Port Mirroring



- Editing a port mirroring entry

Click **Edit** in the **Action** column. In the displayed dialog box, set the source port, destination port, and monitoring type, and click **OK**.

- Deleting a port mirroring entry

Click **Delete** in the **Action** column. In the displayed confirmation box, click **OK**.

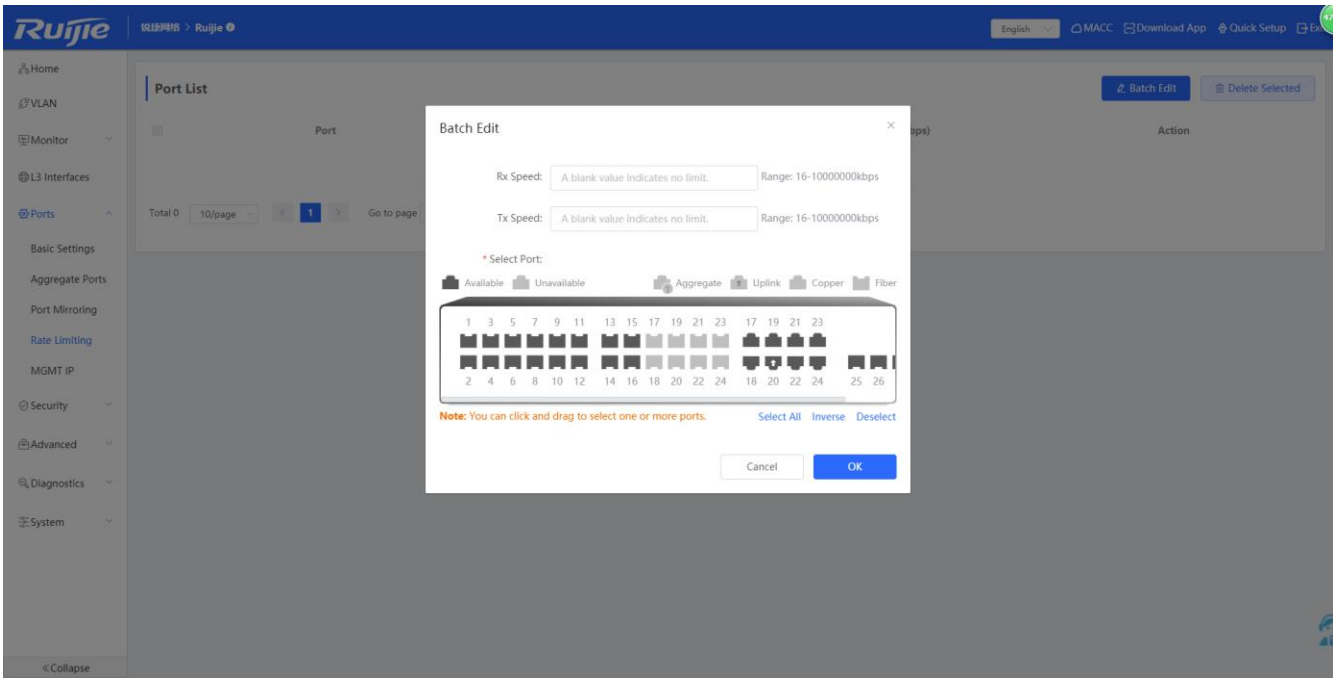
Tips:

1. You can select multiple source ports but only one destination port for port mirroring. Moreover, the source ports cannot contain the destination port and an aggregate port cannot be used as the destination port.
2. A maximum of four port mirroring entries can be configured. Port mirroring cannot be configured for ports that are already mirrored.

3.5.4 Rate Limiting

The **Rate Limiting** module allows you to configure a port rate limit.

Figure 3-5-5 Rate Limiting



- Batch editing the rate limit of ports/Editing the rate limit of a single port

1. Click **Batch Edit**. In the displayed dialog box, select ports, set the Rx speed or the Tx speed, and click **OK**. The message "Edit operation succeeded." is displayed, and the port list is updated.
2. Click **Edit** in the **Action** column. In the displayed dialog box, set the Rx speed or the Tx speed, and click **OK**. The **message** "Operation succeeded." is displayed, and the port list is updated.

- Batch deleting the rate limit of ports/Deleting the rate limit of a single port

1. Select multiple entries in **Port List** and click **Delete Selected**. In the displayed confirmation box, click **OK**.
2. Click **Delete** in the **Action** column. In the displayed confirmation box, click **OK**.

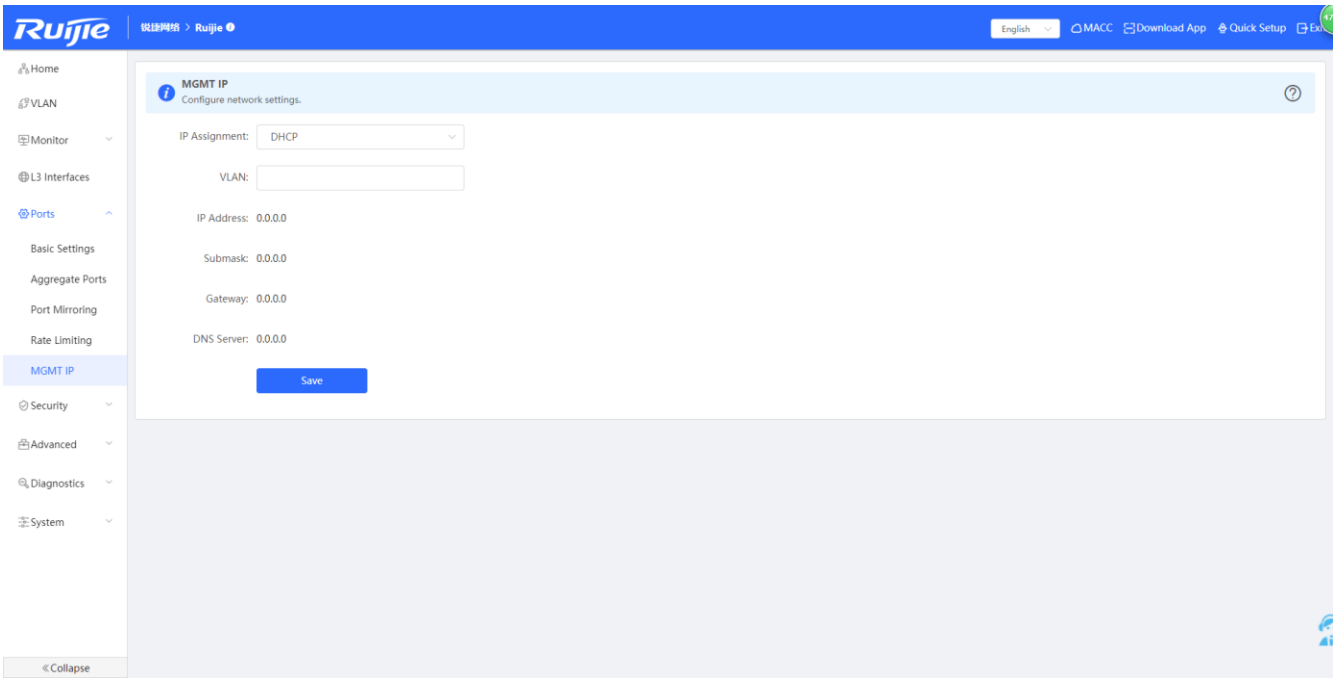
Tips:

1. You must set the Rx speed or the Tx speed.
2. When the Rx speed and the Tx speed are not set, the port rate is not limited.

3.5.5 MGMT IP

The **MGMT IP** module allows you to configure the device's management IP address.

Figure 3-5-6 MGMT IP



- Configuring an IP address

Configure the management VLAN, IP address, subnet mask, default gateway, and DNS server, and click **Submit**. A message indicating successful configuration is then displayed.

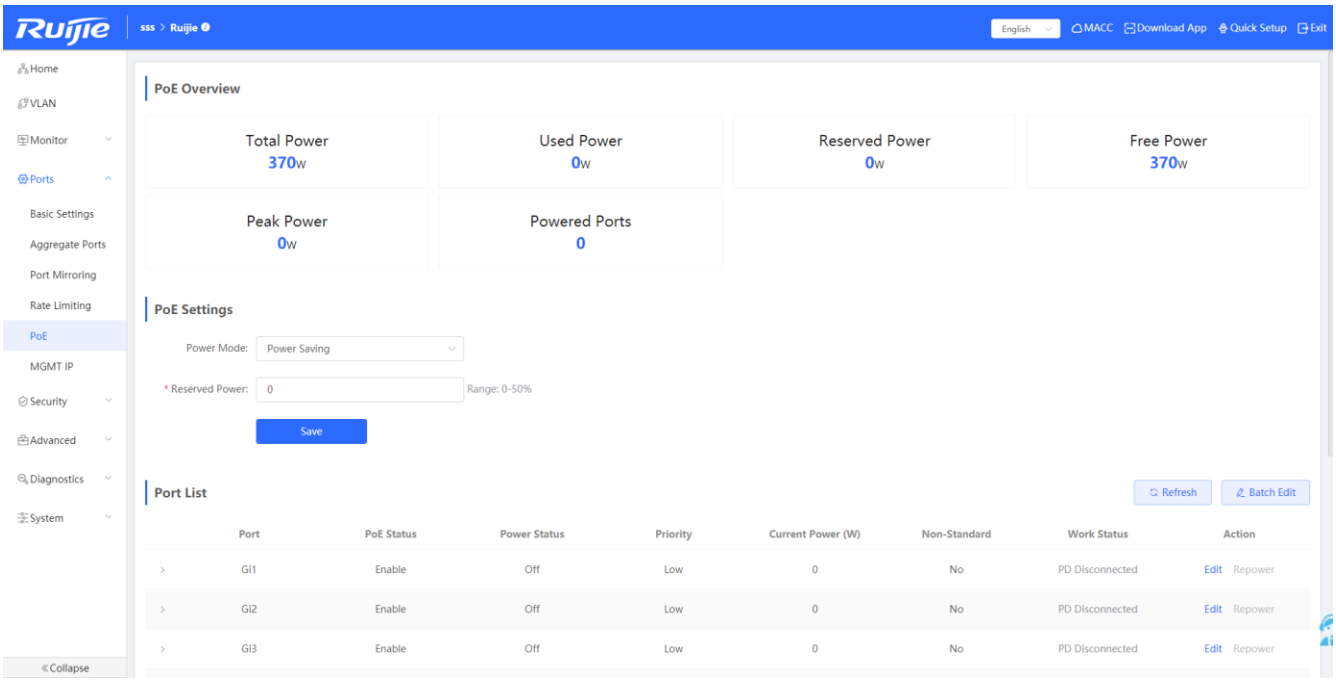
Tips:

1. VLAN 1 takes effect when the management VLAN is set to null or empty.
2. The management VLAN must be created before the configuration. To create a management VLAN, follow instructions in **VLAN List**.
3. You are advised to bind a configured management VLAN to an uplink port. Otherwise, you may fail to access the eWeb management system.

3.5.6 PoE

The **PoE** module displays the PoE overview and allows you to specify PoE settings. The **PoE** module is available only for devices that support the PoE function.

Figure 3-5-7 PoE

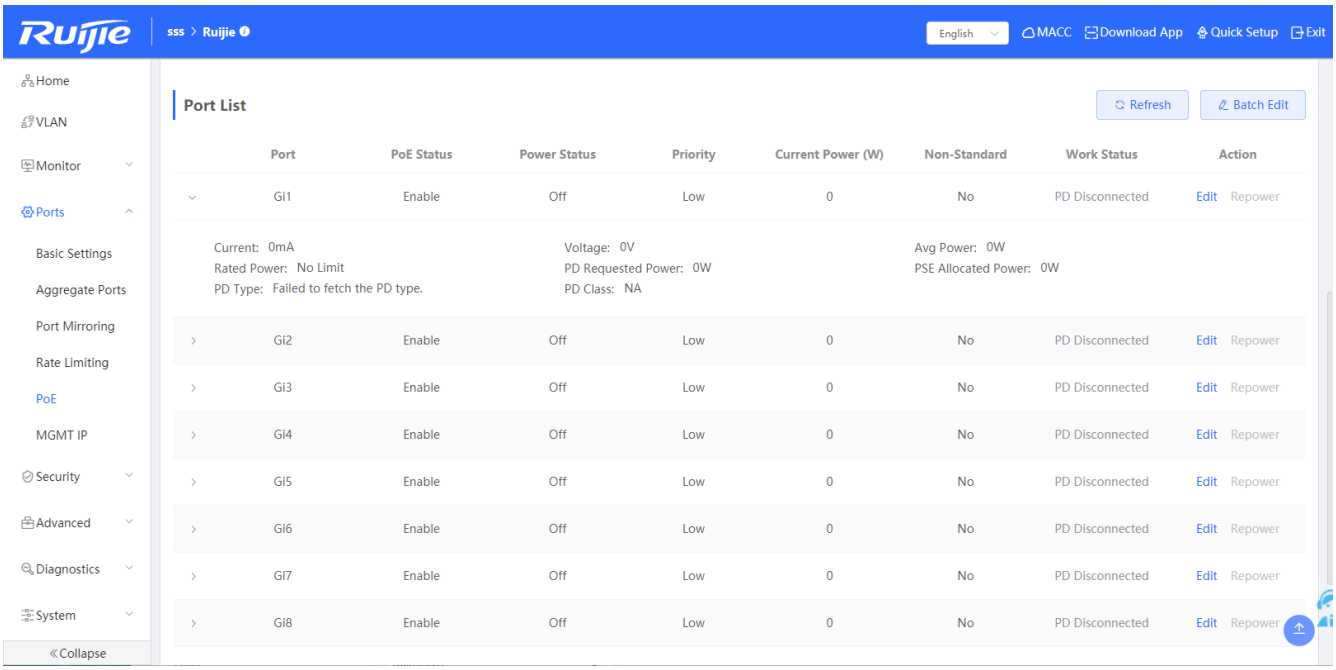


The **PoE Overview** area displays the PoE information of the entire device.

- PoE settings

Select the power mode, and click **Save**. Reserved power can be configured in power saving mode to prevent PoE flapping.

Figure 3-5-8 Configuring PoE Ports



- Batch editing PoE ports/Editing a single PoE port

Click **Edit** in the **Action** column or **Batch Edit** in **Port List**. In the displayed dialog box, set the PoE port attributes, and click **OK**.

- Displaying PoE port details

Click ˅ in **Port List** to display PoE port details.

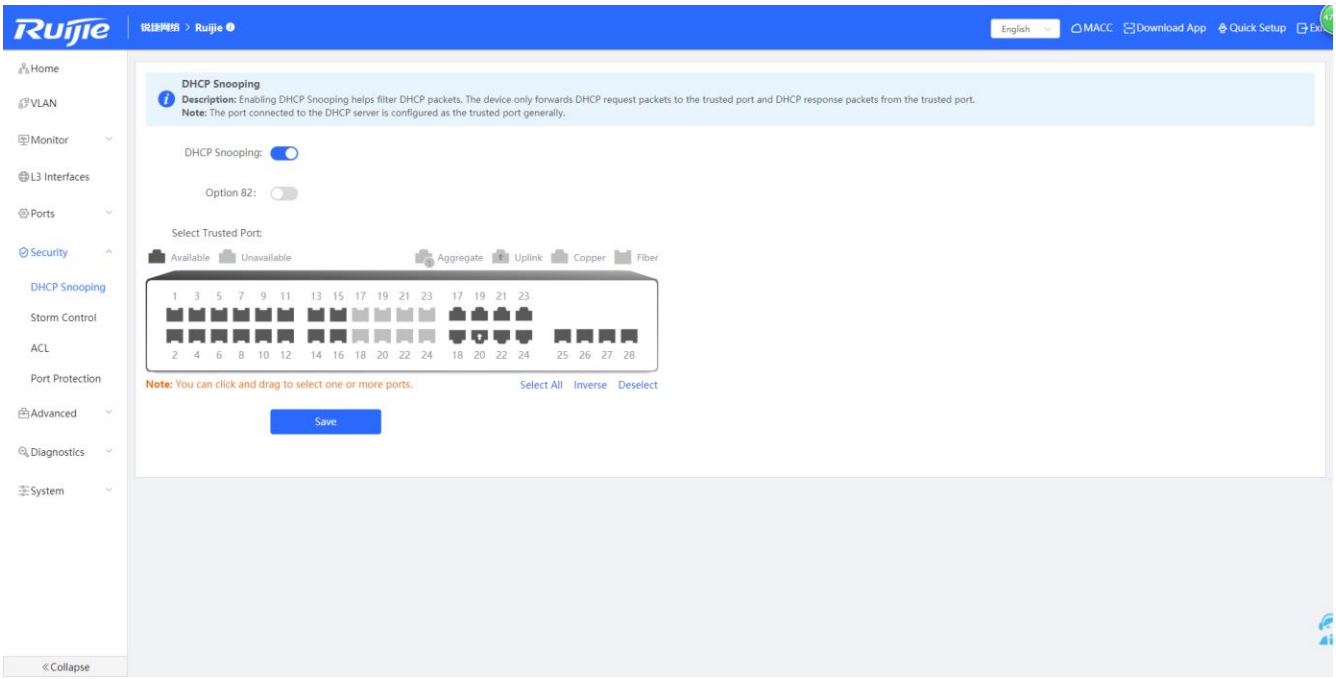
3.6 Security

The **Security** module includes **DHCP Snooping**, **Storm Control**, **ACL**, and **Port Protection**.

3.6.1 DHCP Snooping

The **DHCP Snooping** module allows snooping the DHCP packets exchanged between clients and servers to record and monitor IP addresses of users. It also allows filtering invalid DHCP packets, including request packets from clients and response packets from servers. User data based on DHCP Snooping serves security applications such as IP Source Guard.

Figure 3-6-1 DHCP Snooping



- Enabling or disabling DHCP snooping

1. Click the **DHCP Snooping** toggle to enable or disable DHCP snooping.
2. After DHCP snooping is enabled, set trusted ports, and click **Save**.

Tips:

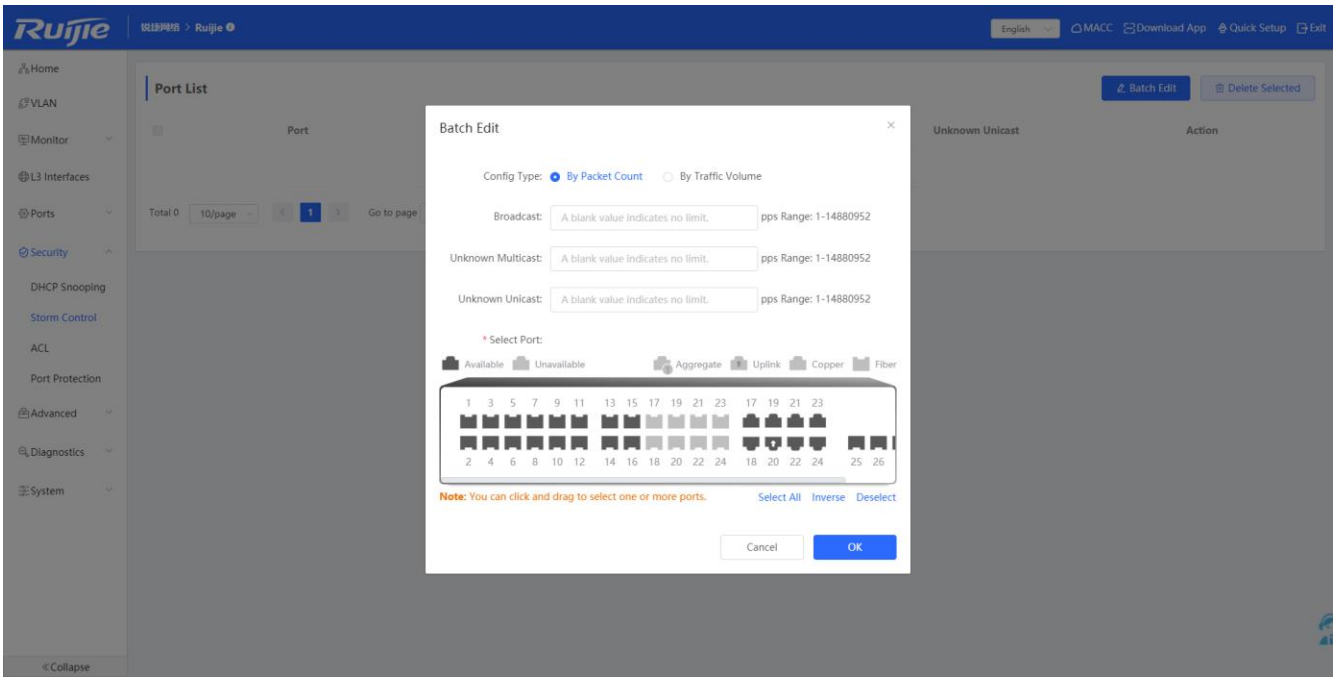
1. The port connected to the DHCP server is configured as the trusted port generally.
2. Enabling DHCP snooping can filter DHCP packets. Request packets from DHCP clients are forwarded only to trusted ports. For response packets from DHCP servers, only those from trusted ports are forwarded.

3.6.2 Storm Control

When there are excessive broadcast, multicast or unknown unicast data flows in the LANs, the network speed decreases and packet transmission timeout greatly increases. This is called LAN storm, which may be caused by topology protocol execution errors or incorrect network configuration.

Users can perform storm control separately for the broadcast, multicast, and unknown unicast data flows. When the rate of broadcast, multicast, or unknown unicast packets received by the device port exceeds the specified rate, the number of packets allowed per second, or the number of kilobits allowed per second, the device transmits packets only at the specified rate, the number of packets allowed per second, or the number of kilobits allowed per second, and discards packets beyond the rate range, until the packet rate becomes normal, thereby avoiding flooded data from entering the LAN and causing a storm.

Figure 3-6-2 Storm Control



- Batch adding ports/Adding a single port for storm control

1. Click **Batch Edit**. In the displayed dialog box, select ports, enter the broadcast, unknown unicast, and unknown multicast rate limits, and click **OK**. A message "Operation succeeded." is displayed, and the port list is updated.
2. Click **Edit** in the **Action** column of **Port List**. In the displayed dialog box, enter the broadcast, unknown unicast, and unknown multicast rate limits, and click **OK**. A message "Operation succeeded." is displayed, and the port list is updated.

- Batch deleting ports/Deleting a single port for storm control

1. Select multiple entries in **Port List** and click **Delete Selected**. In the displayed confirmation box, click **OK**.
2. Click **Delete** in the **Action** column. In the displayed confirmation box, click **OK**.

Tips:

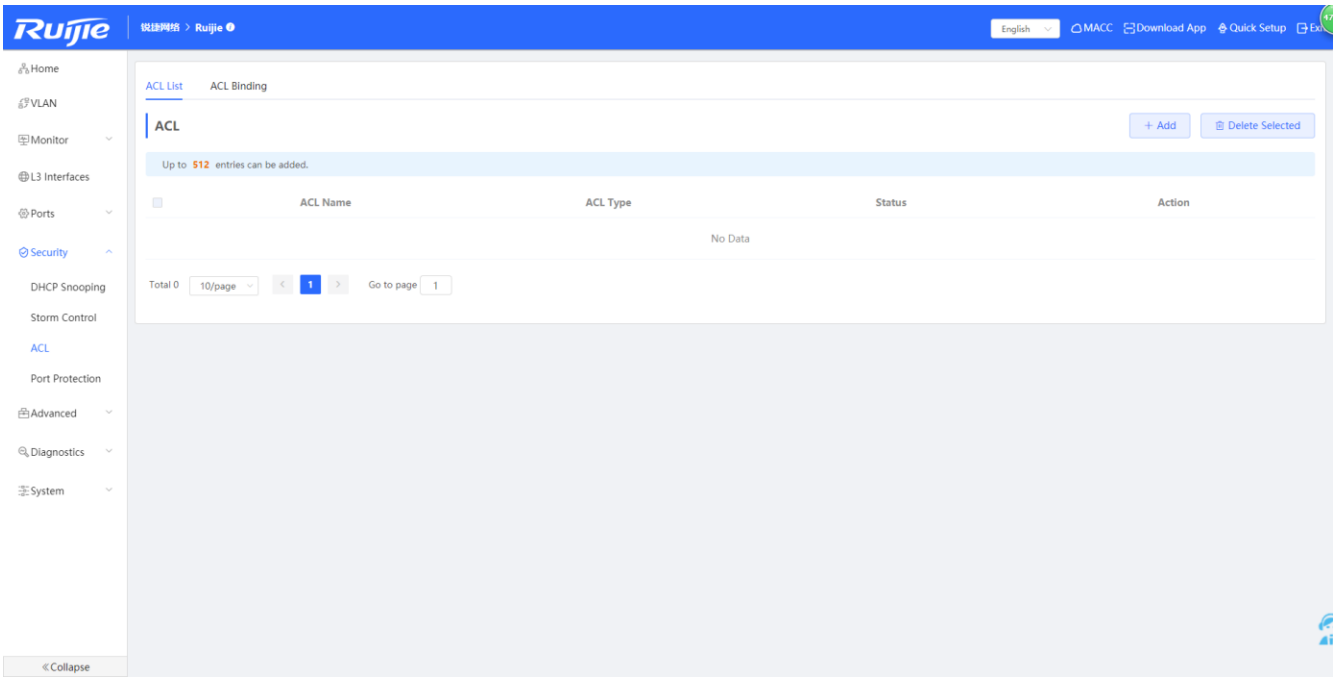
1. You must set the Rx speed or the Tx speed.
2. When the broadcast, unknown unicast, and unknown multicast rate limits are empty, the port rate is not limited.

3.6.3 ACL

An access control list (ACL) is also referred to as firewall or packet filter in some documents. The ACL controls (permits or discards) data packets on a network device interface by defining ACEs.

The **ACL** module includes **ACL List** (two types: **Based on MAC** and **Based on IP**) and **ACL Binding**.

Figure 3-6-3 ACL List



- Adding an ACL

Click **Add**. In the displayed dialog box, select the ACL type, enter the ACL name, and click **OK**.

- Batching deleting ACLs/Deleting a single ACL

Select ACLs in the ACL list, and click **Delete Selected**. Alternatively, click **Delete** in the **Action** column. In the displayed confirmation box, click **OK**.

- Editing an ACL

Click **Edit** in the **Action** column. In the displayed dialog box, edit the ACL name and click **OK**.

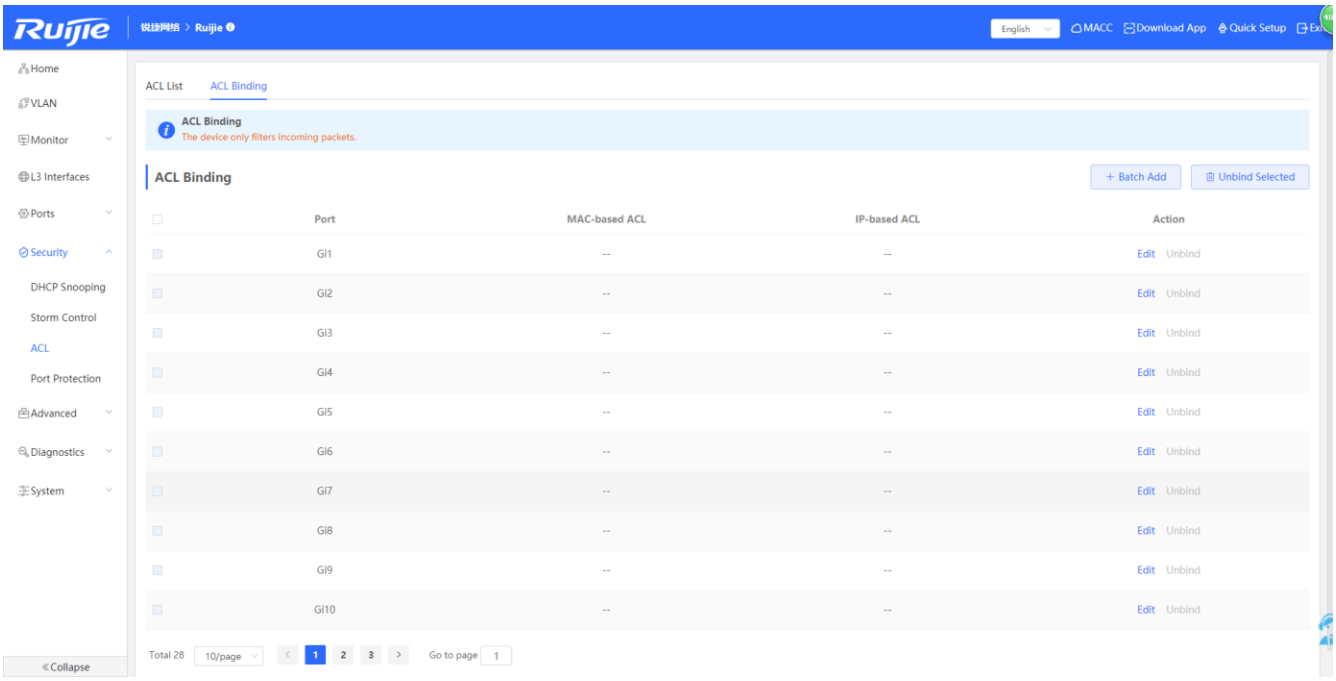
- Displaying ACL details

Click **Details** in the **Action** column. In the displayed side pane, query, add, edit, or delete ACEs.

Tips:

1. ACLs cannot have the same name. Only the name of a created ACL can be edited.
2. An ACL applied by a port cannot be edited or deleted.
3. ACE fields vary with the ACL type. ACEs can be added, edited, deleted, and moved.

Figure 3-6-4 ACL Binding



- Binding ACLs

Click **Batch Add**. In the displayed dialog box, select the target MAC-based ACL and IP-based ACL and ports, and click **OK**.

- Batch unbinding ACLs/Unbinding a single ACL

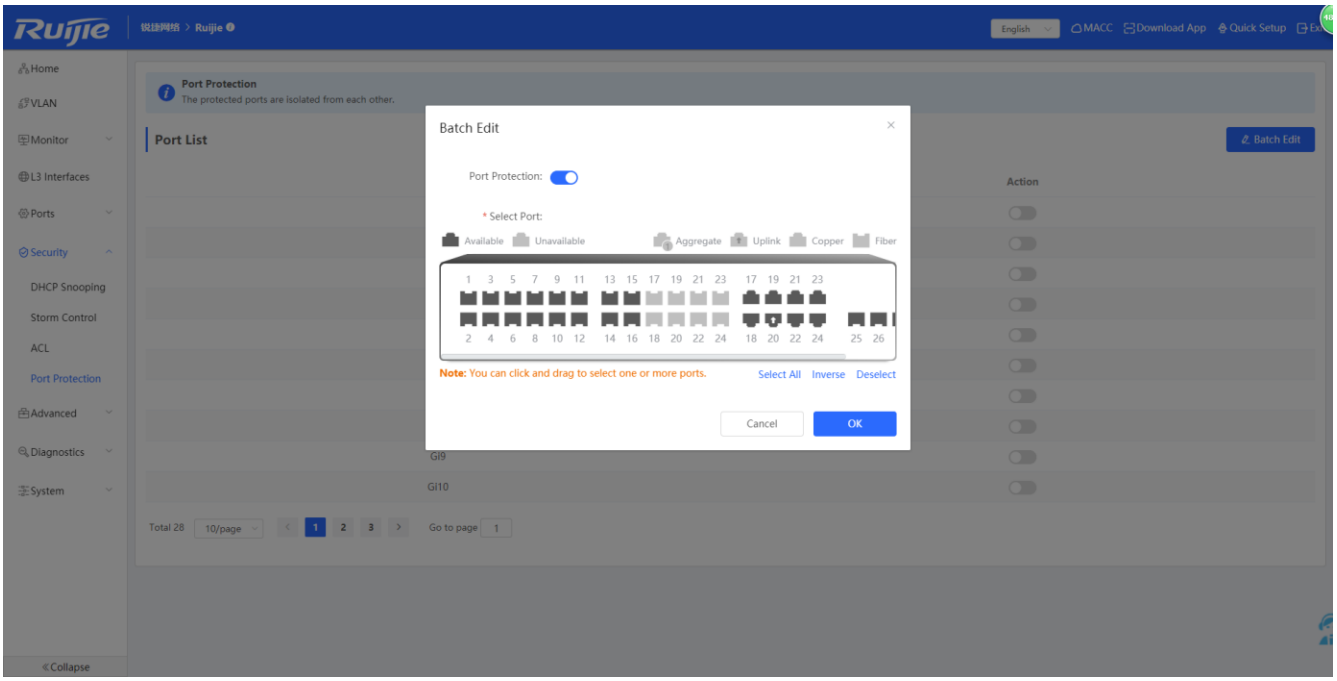
Select multiple entries in **ACL Binding**, and click **Unbind Selected**. Alternatively, click **Unbind** in the **Action** column. In the displayed confirmation box, click **OK**.

Tips: At least one ACL type needs to be selected for ACL binding.

3.6.4 Port Protection

Users on different ports are isolated at layer 2 when port protection is enabled.

Figure 3-6-5 Port Protection



- Enabling or disabling port protection

Click **Batch Edit**. In the displayed dialog box, enable or disable port protection and select ports. Alternatively, click the toggle button in the **Action** column. In the displayed confirmation box, click **OK**.

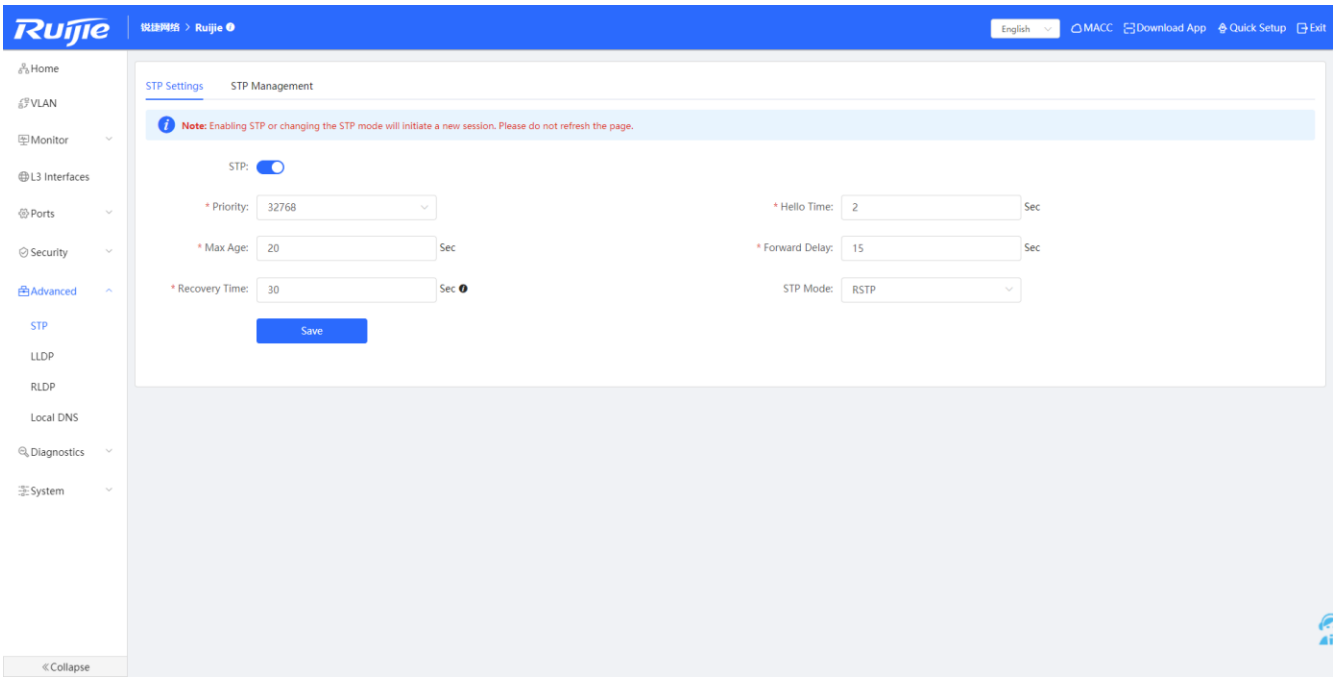
3.7 Advanced

The **Advanced** module includes **STP** and **LLDP**.

3.7.1 STP

The Spanning Tree Protocol (STP) is a layer-2 management protocol that eliminates layer-2 loops by selectively blocking redundant links in the network. It also provides the link backup function.

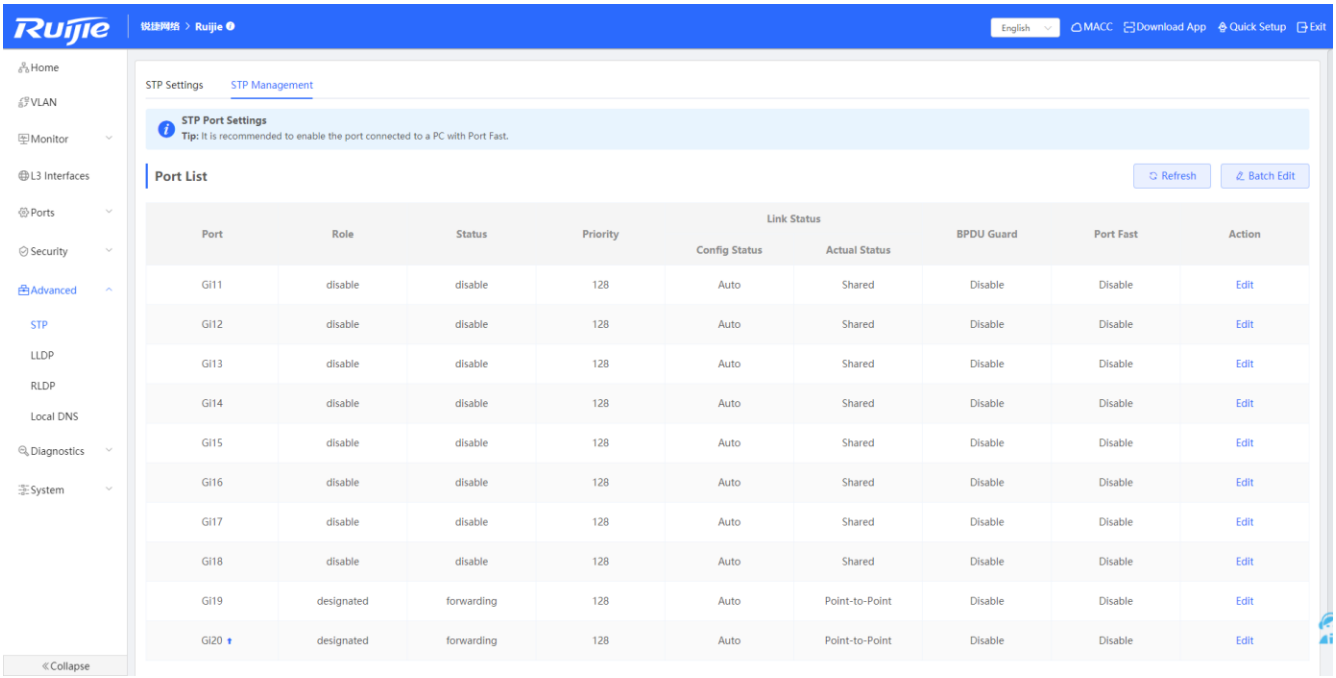
Figure 3-7-1 STP Settings



- Global STP settings

Enable STP, set global STP parameters, and click **Save**.

Figure 3-7-2 STP Management



- STP management

Click **Batch Edit**, select ports, and configure parameters. Alternatively, click **Edit** in the **Action** column, configure parameters, and click **OK**.

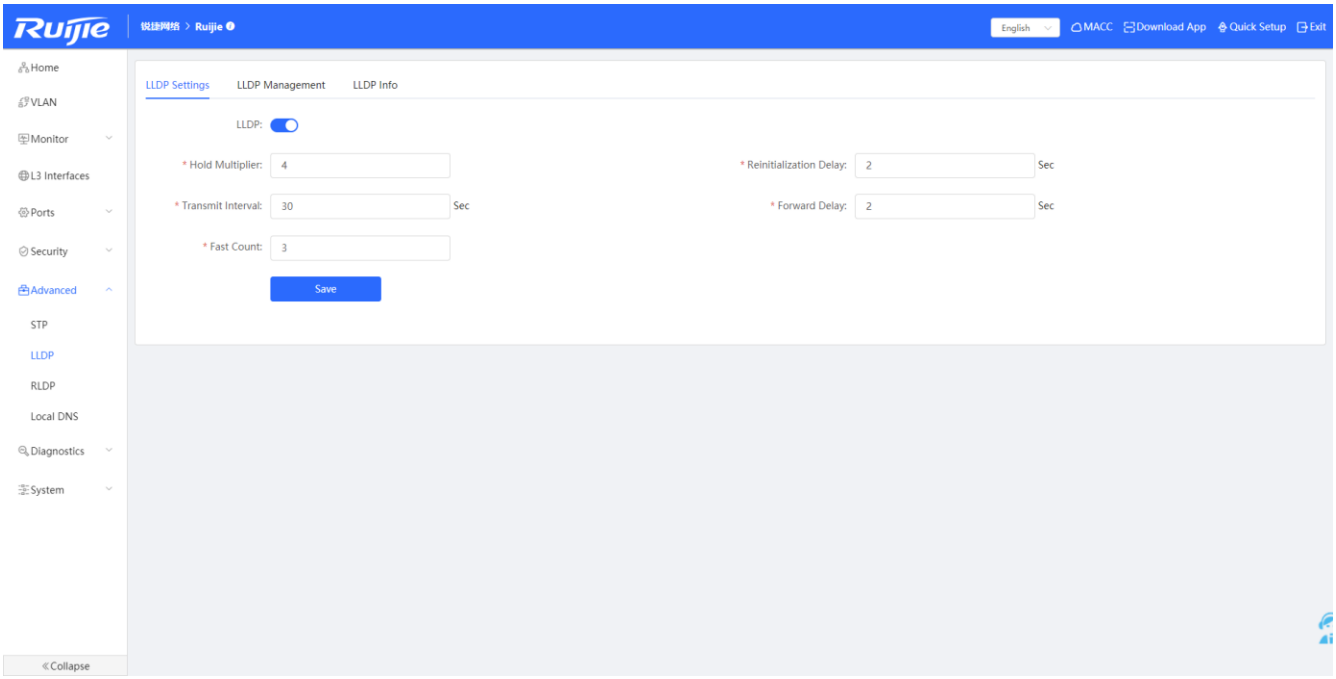
Tips:

1. Enabling the STP or changing the STP mode will initiate a new session. Do not refresh the page during the configuration.
2. It is recommended to enable Port Fast on the port connected to a PC.

3.7.2 LLDP

The Link Layer Discovery Protocol (LLDP) is defined by IEEE 802.1AB. LLDP can discover devices and detect topology changes. With LLDP, the eWeb management system can learn the topological connection status, for example, ports of the device that are connected to other devices, port rates at both ends of a link, and duplex mode matching status. An administrator can locate and troubleshoot faults quickly based on the preceding information.

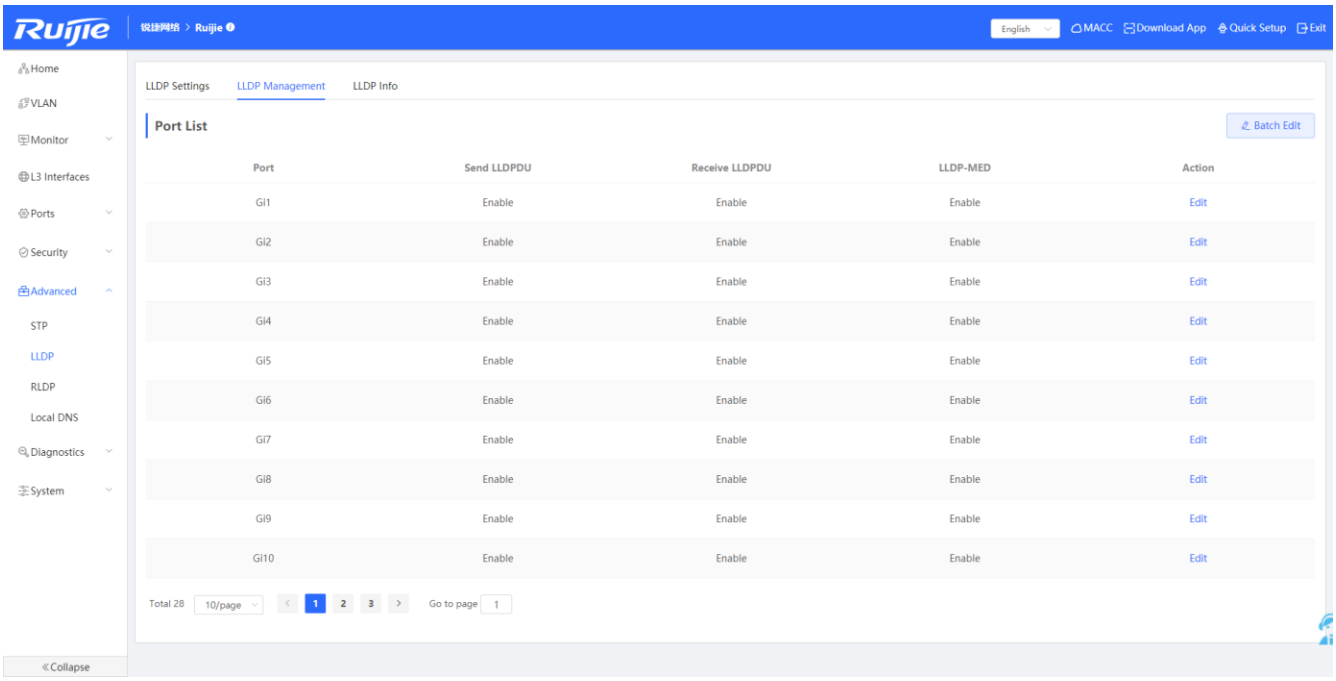
Figure 3-7-3 LLDP Settings



- LLDP settings

Enable **LLDP**, configure related parameters, and click **Save**.

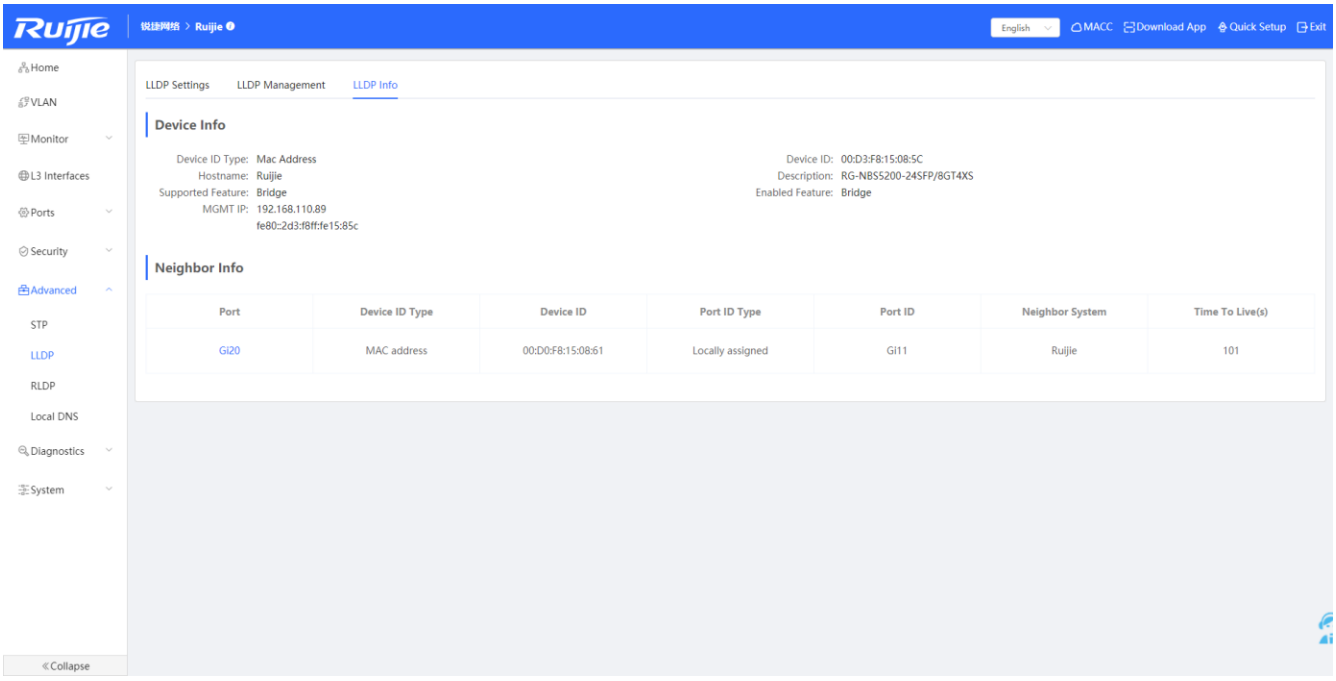
Figure 3-7-4 LLDP Management



- LLDP management

Click **Batch Edit**, select ports, and configure parameters. Alternatively, click **Edit** in the **Action** column, configure parameters, and click **OK**.

Figure 3-7-5 LLDP Info



- LLDP information

The **LLDP Info** page displays information about the current device and neighbor information of each port. Click a port name to display neighbor details of this port.

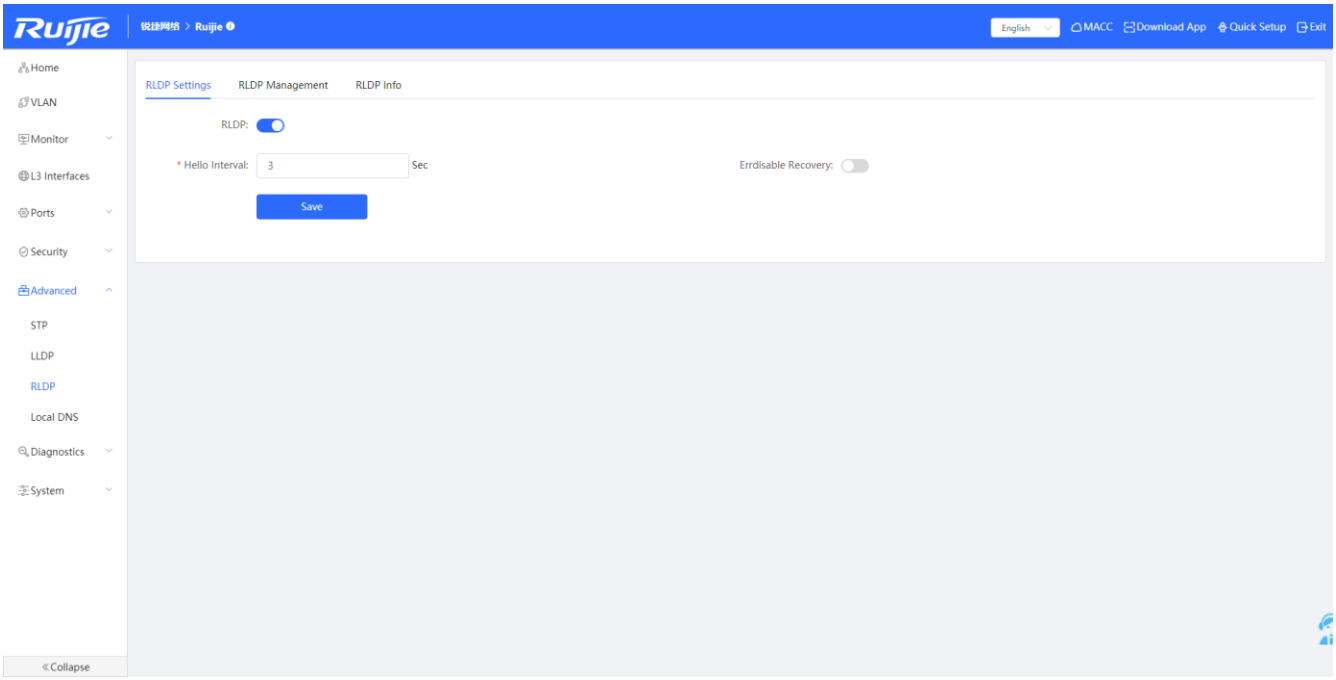
Tips:

1. LLDP can be used to display the topological connection status, for example, the numbers of switches, MED devices, and NMS devices in the network topology.
2. LLDP can be used to detect errors, for example, display incorrect configuration information if two switches are directly connected in the network topology.

3.7.3 RLDP

RLDP is used to detect to detect downlink loops. You can select an action among warning, block and shutdown to prevent forwarding loops on a layer-2 network.

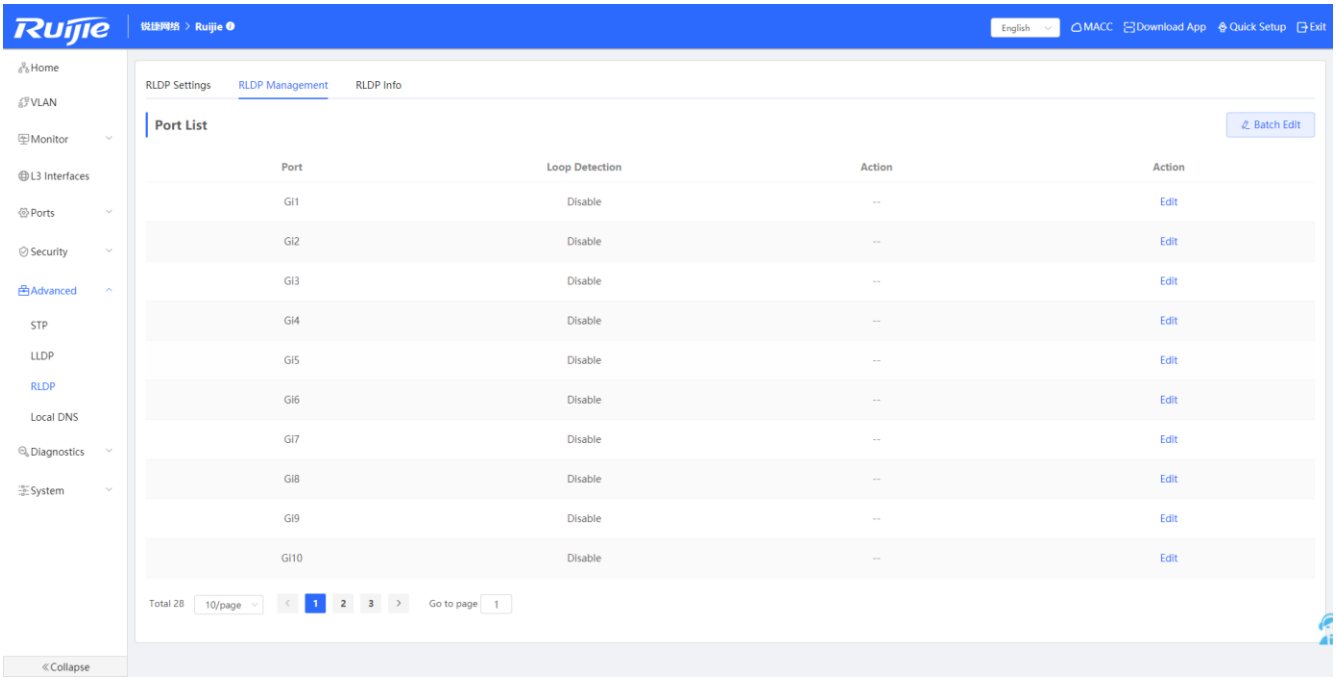
Figure 3-7-6 RLDP Settings



- RLDP settings

Enable **RLDP**, set global RLDP parameters, and click **Save**.

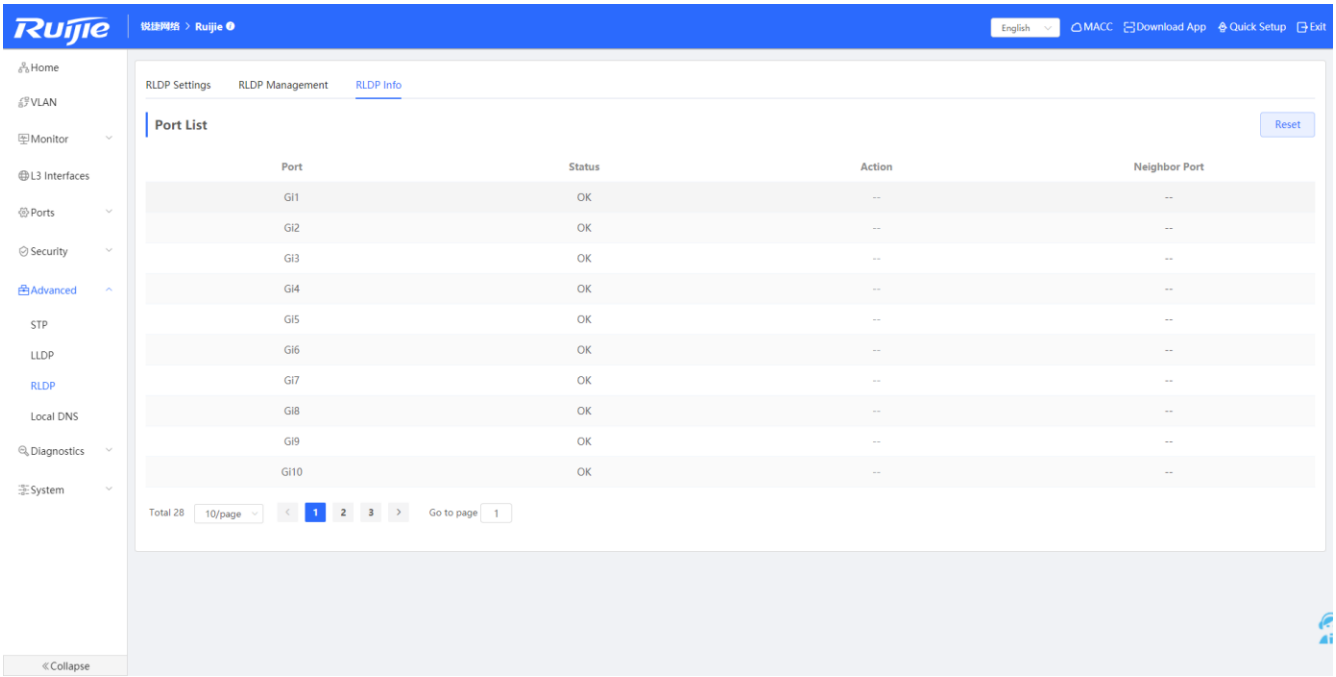
Figure 3-7-7 RLDP Management



- RLDP management

Click **Batch Edit**, select ports, and configure parameters. Alternatively, click **Edit** in the **Action** column, configure parameters, and click **OK**.

Figure 3-7-8 RLDP Information



- RLDP information

The **RLDP Info** page displays information about the current device and neighbor information of each port. Click a port name to display neighbor details of this port.

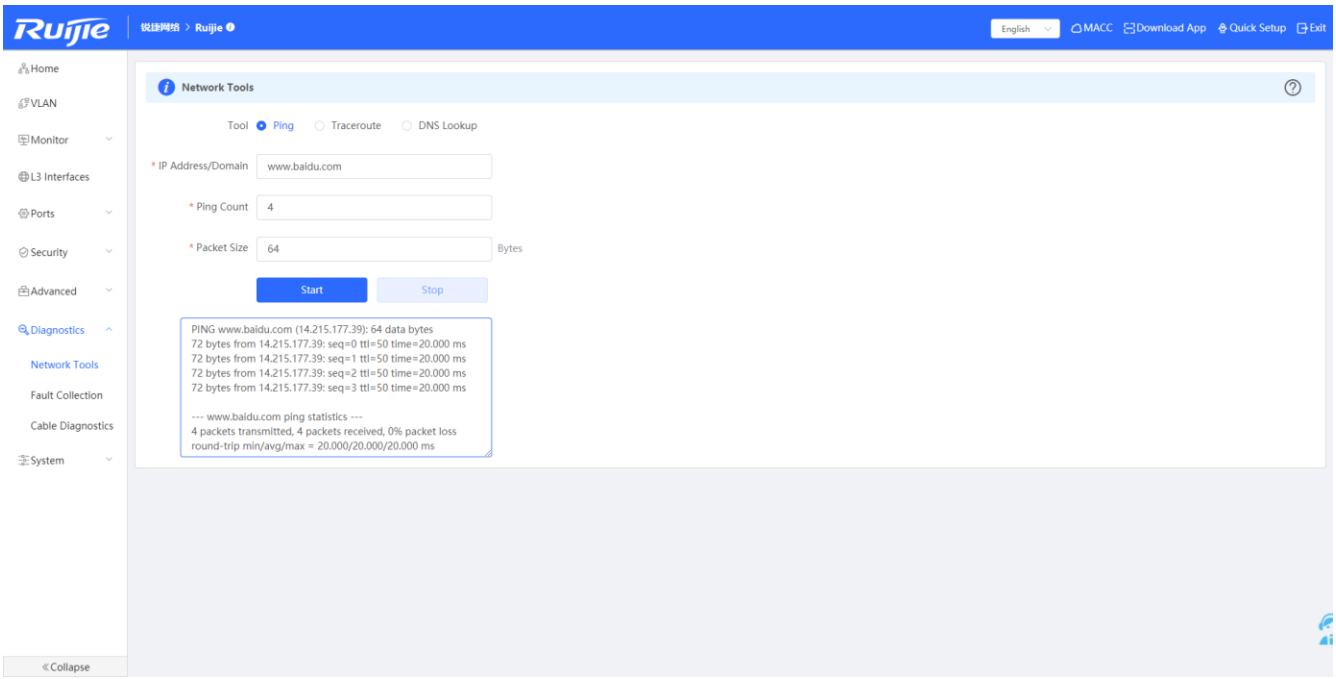
3.8 Diagnostics

3.8.1 Network Tools

The **Network Tools** module provides the following network tools to detect the network status: **Ping**, **Traceroute**, and **DNS Lookup**.

1. Ping test and result

Figure 3-8-1 Ping

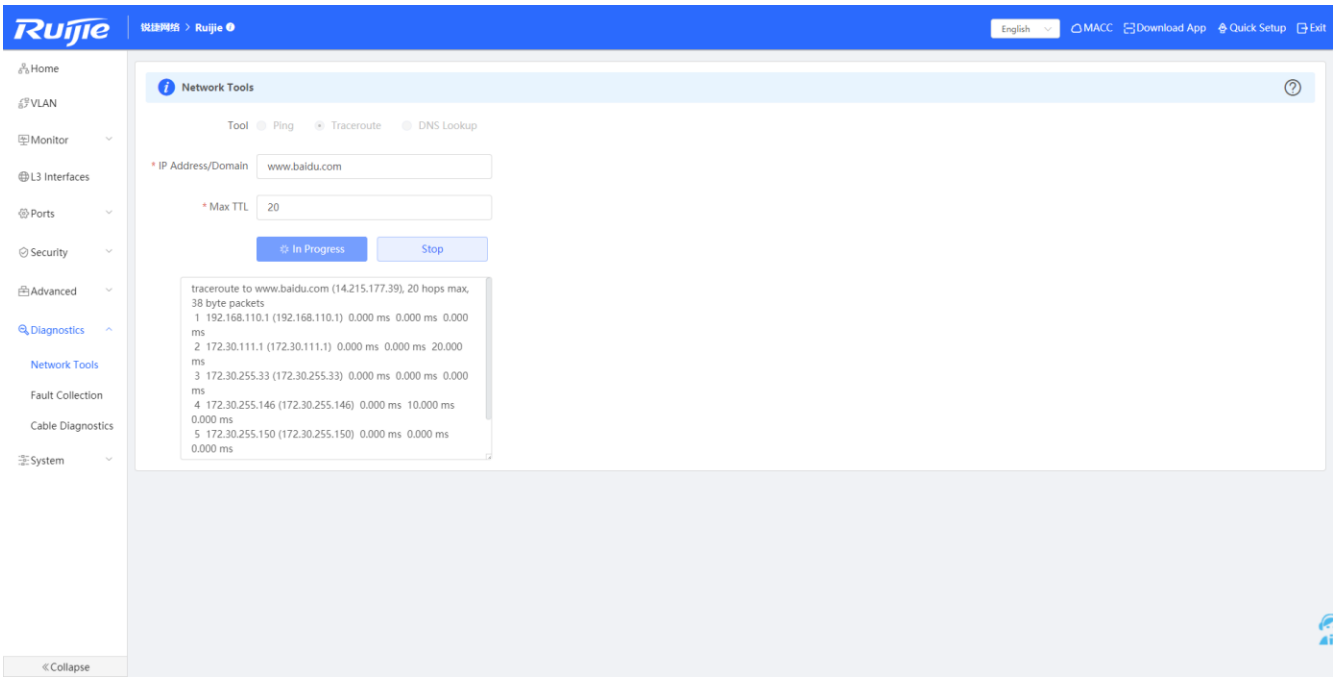


- Ping test

Enter the destination IP address and other information, and click **Start**. The test result is displayed in the text box.

2. Traceroute test and result

Figure 3-8-2 Traceroute

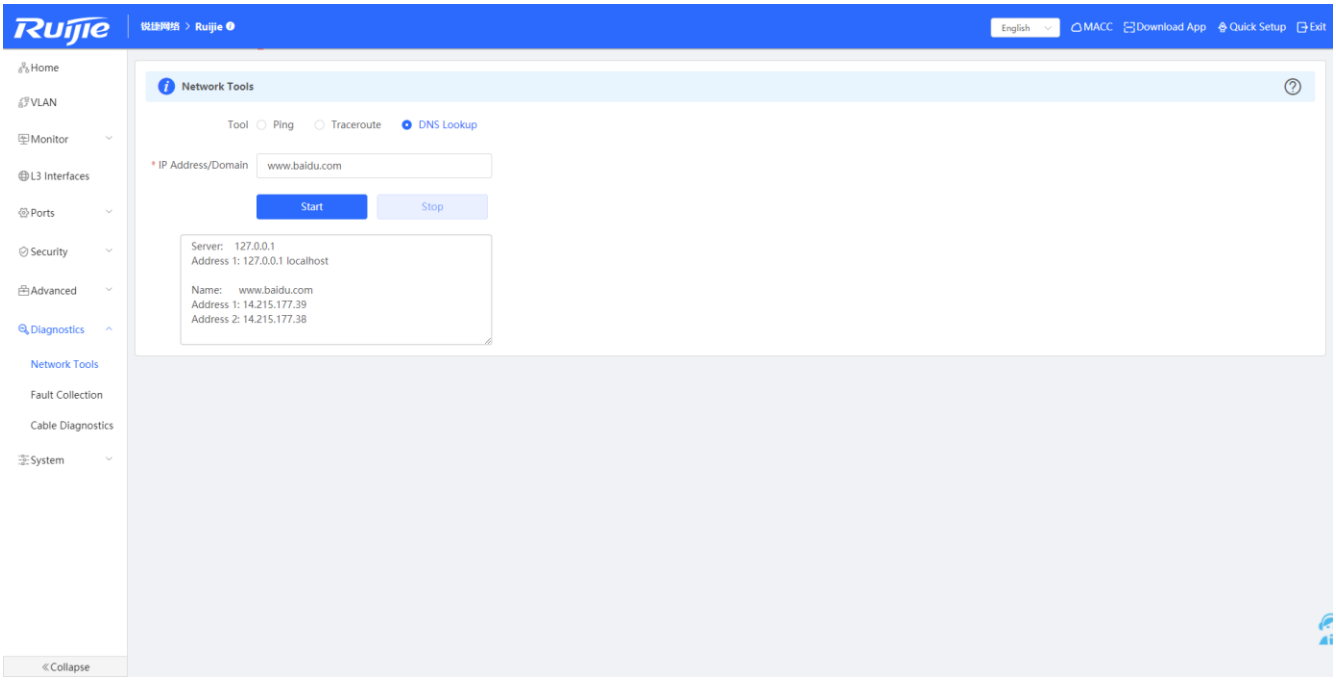


- Traceroute test

Enter the destination IP address and other information, and click **Start**. The test result is displayed in the text box.

3. DNS lookup test and result

Figure 3-8-3 DNS Lookup



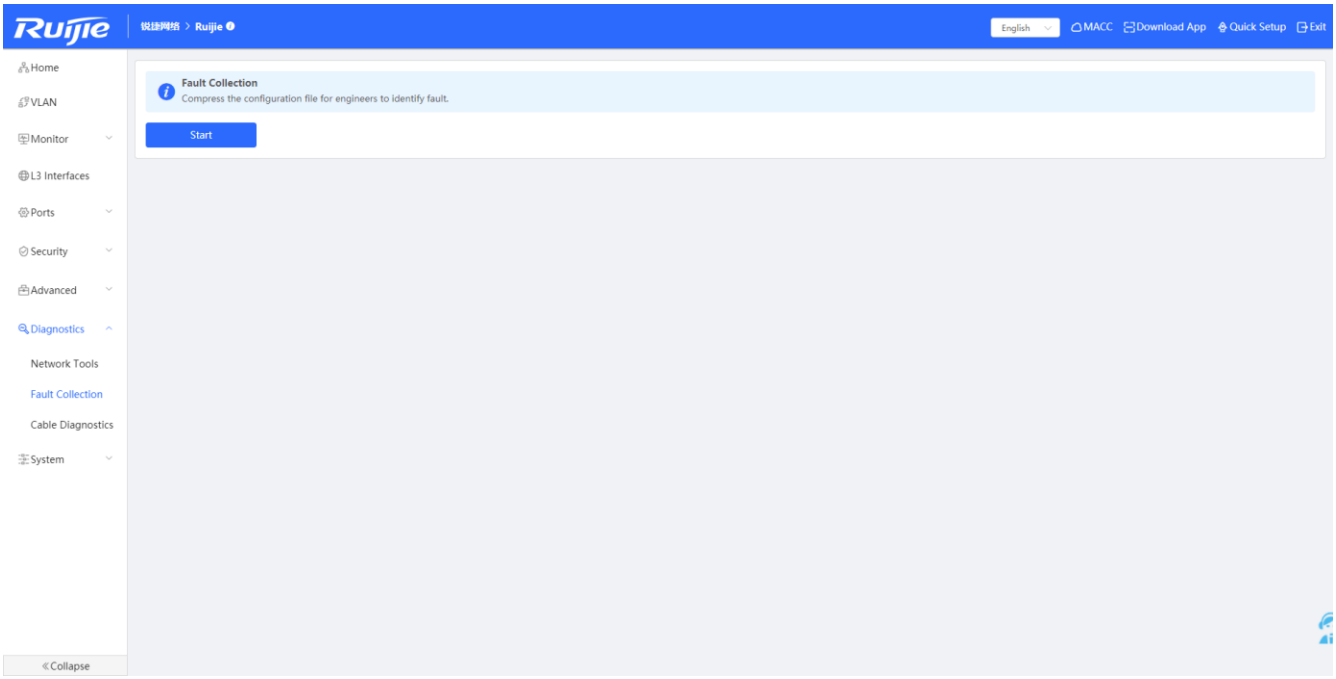
- DNS lookup test

Enter the destination IP address, and click **Start**. The test result is displayed in the text box.

3.8.2 Fault Collection

The **Fault Collection** module allows you to collect faults by one click and download the fault information to the local device.

Figure 3-8-4 Fault Collection



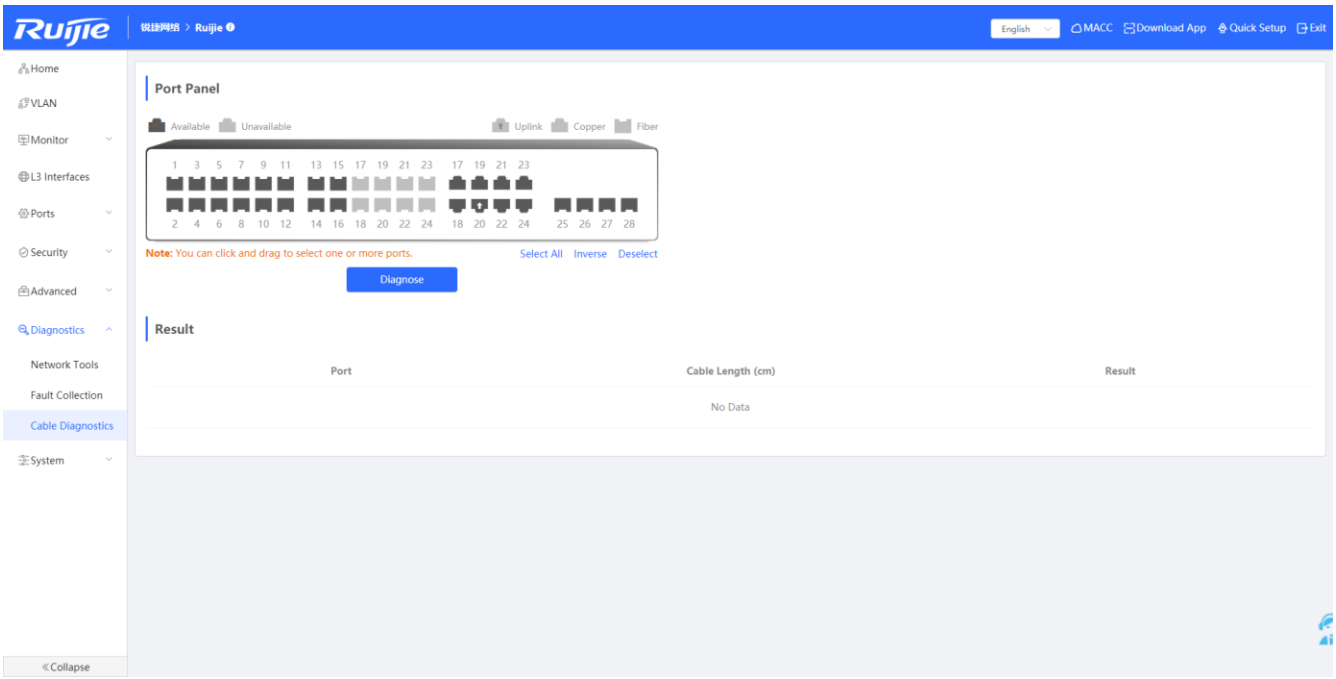
- Fault collection

Click **Start** to download the fault information.

3.8.3 Cable Diagnostics

An administrator can detect the working status of cables via the cable diagnostics command. Cable diagnostics helps determine whether a cable is short-circuited, disconnected, or in other abnormal state.

Figure 3-8-5 Cable Diagnostics



- Cable diagnostics

Select the target port on the port panel, and click **Diagnose**. The device returns the diagnostics result after a period of time and displays it in the result list.

Tips:

1. Only copper ports support cable diagnostics while fiber ports and aggregate ports do not.
2. If cable diagnostics is executed on a normally connected interface, the connection is temporarily down and will be re-established.

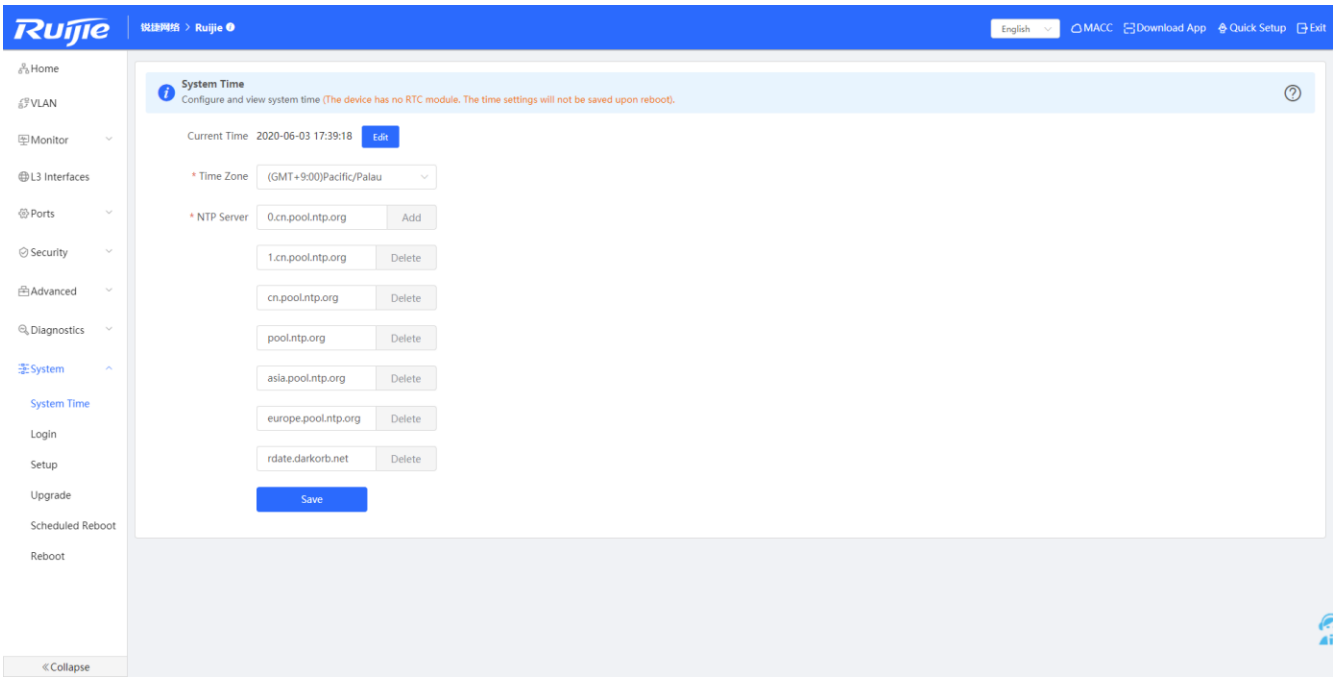
3.9 System

The **System** module allows you to perform a series of settings, including the system time, login password, upgrade, and backup and restoration.

3.9.1 System Time

The **System Time** module allows you to set the system time. The system time is synchronized with the NTP server by default.

Figure 3-9-1 System Time



- Time settings

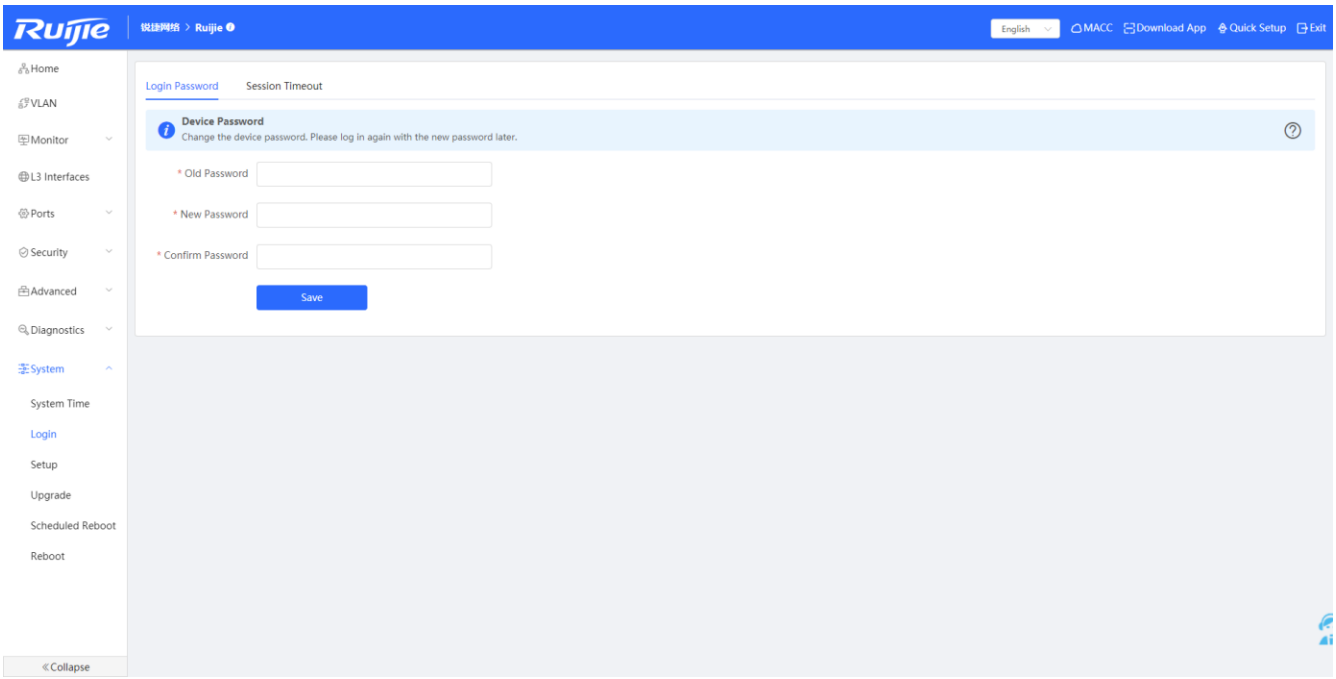
Select a time zone and set at least one NTP server, and click **Save**.

Tips:
The device has no RTC module and does not save the time after restart.

3.9.2 Login Password

The **Login Password** page allows you to set the device's login password. You need to log into the system again after changing the password.

Figure 3-9-2 Login Password



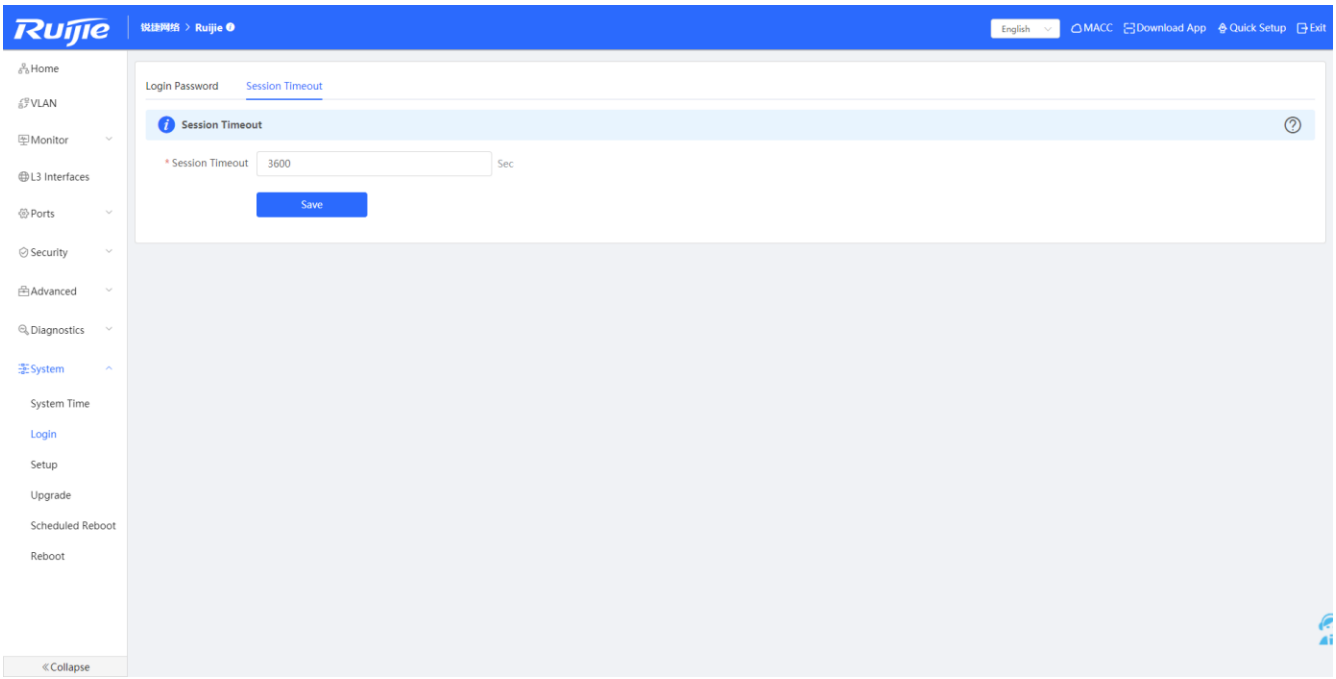
- Setting the password

Enter the old and new passwords, and click **Save**. (Please keep the login password carefully.)

3.9.3 Session Timeout

The **Session Timeout** page allows you to set the session timeout period for login to the eWeb management system.

Figure 3-9-3 Session Timeout



- Setting the session timeout period

Enter the timeout period in seconds and click **Save**.

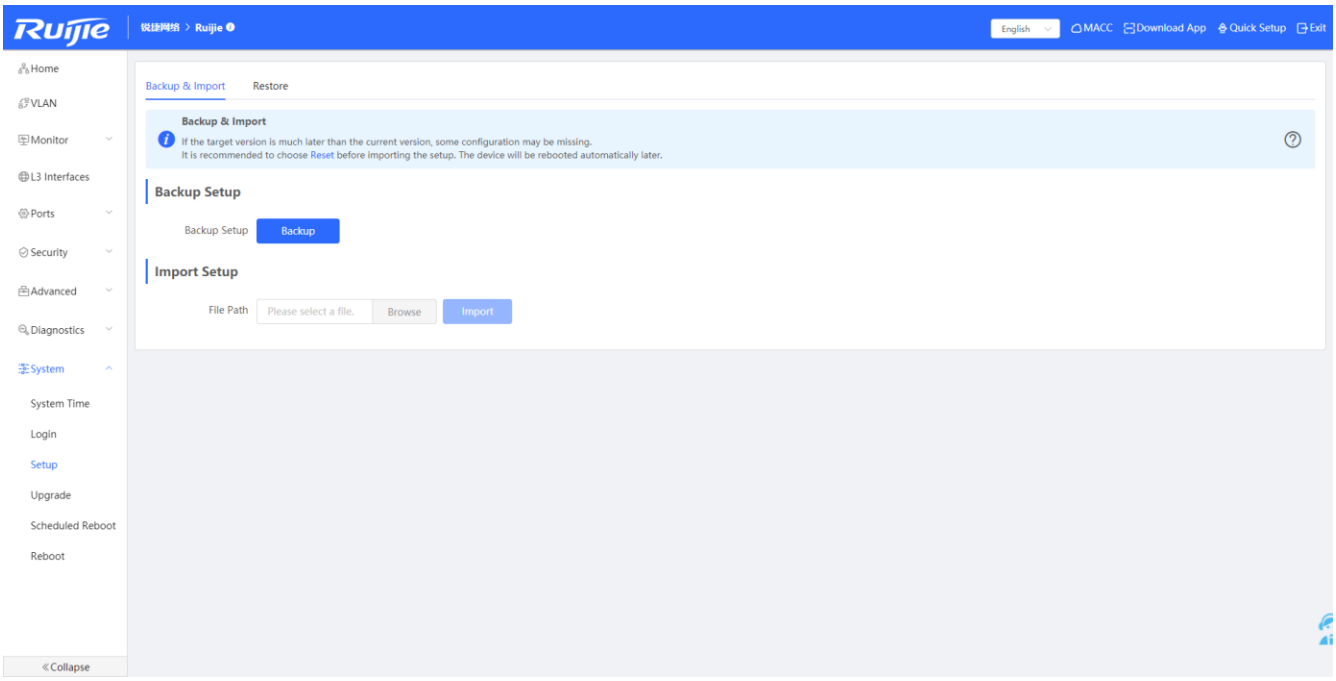
3.9.4 Setup

The **Setup** module includes **Back & Import** and **Restore**.

3.9.4.1 Backup & Import

The **Backup & Import** page allows you to import a configuration file and apply the imported settings. It also allows exporting the configuration file to generate a backup.

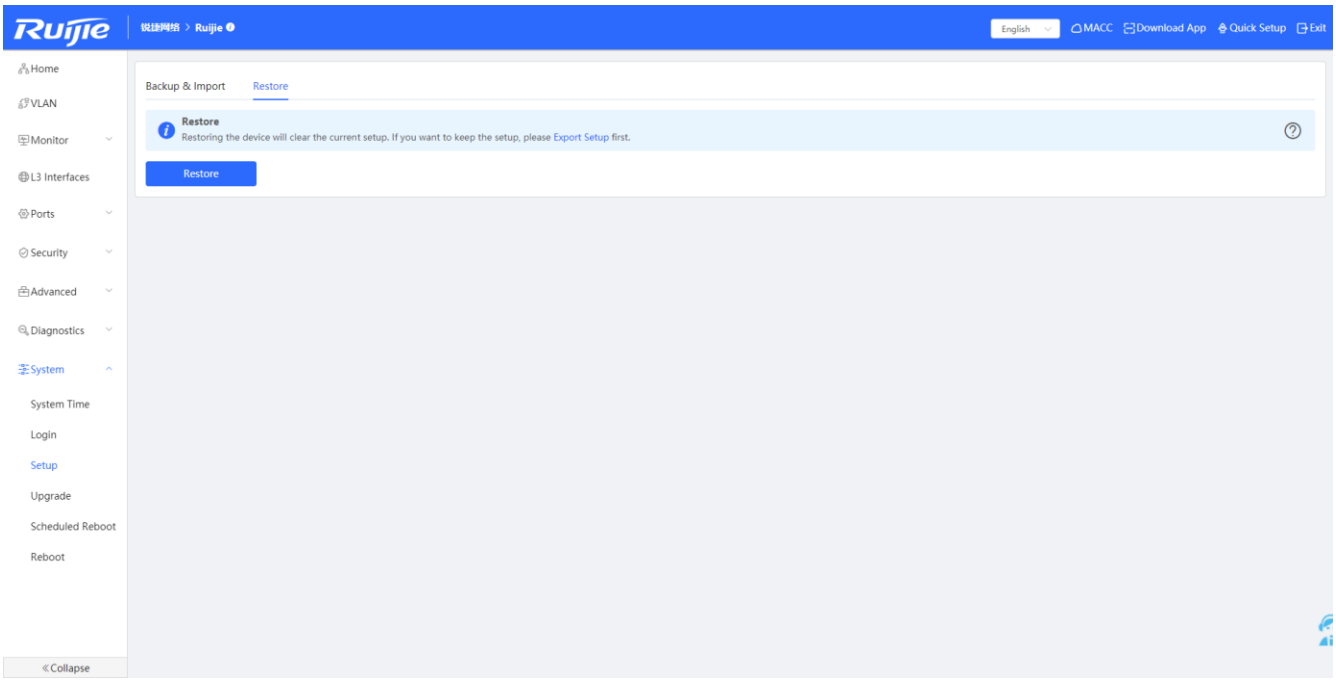
Figure 3-9-4 Backup & Import



3.9.4.2 Restore

The **Restore** page allows you to restore the device to factory settings.

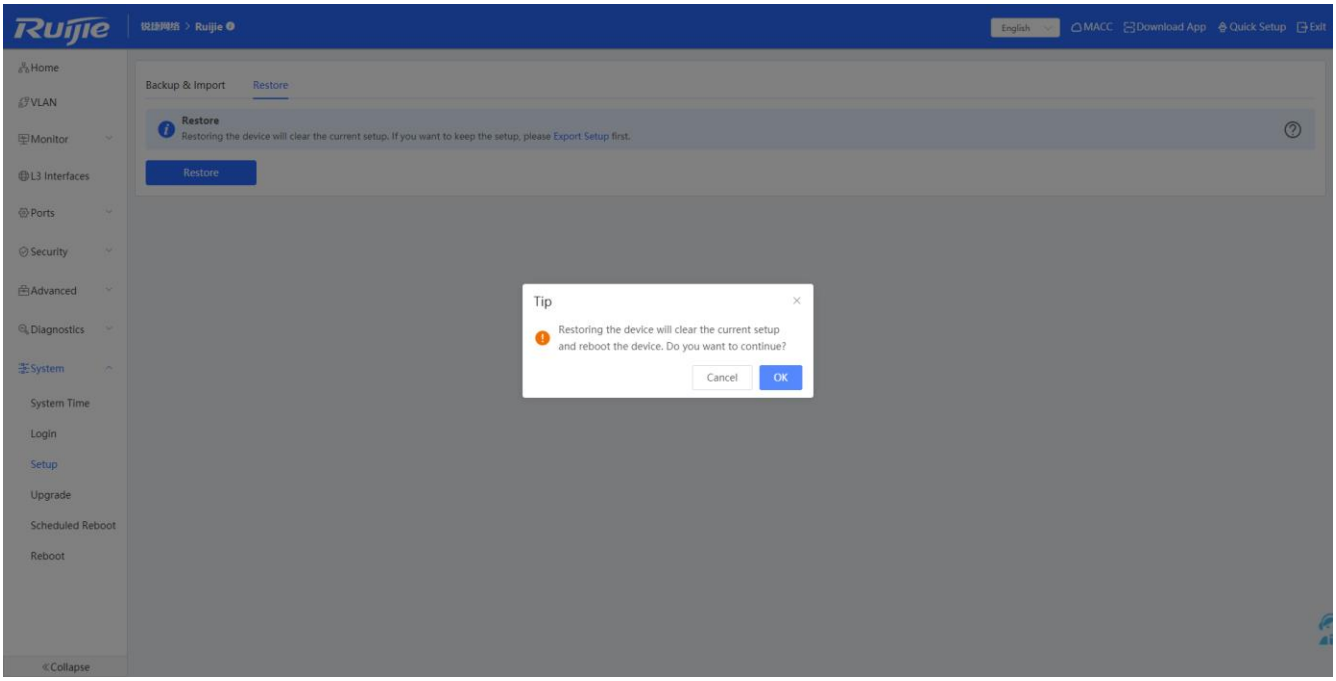
Figure 3-9-5 Restore



- Restoring factory settings

Please exercise caution if you want to restore the factory settings.

Figure 3-9-6 Confirm Restore



Click **OK** to restore all default values. This function is recommended when the network configuration is incorrect or the network environment is changed. If you fail to access the eWeb management system, check whether the endpoint is connected to the device by referring to Configuration Preparation.

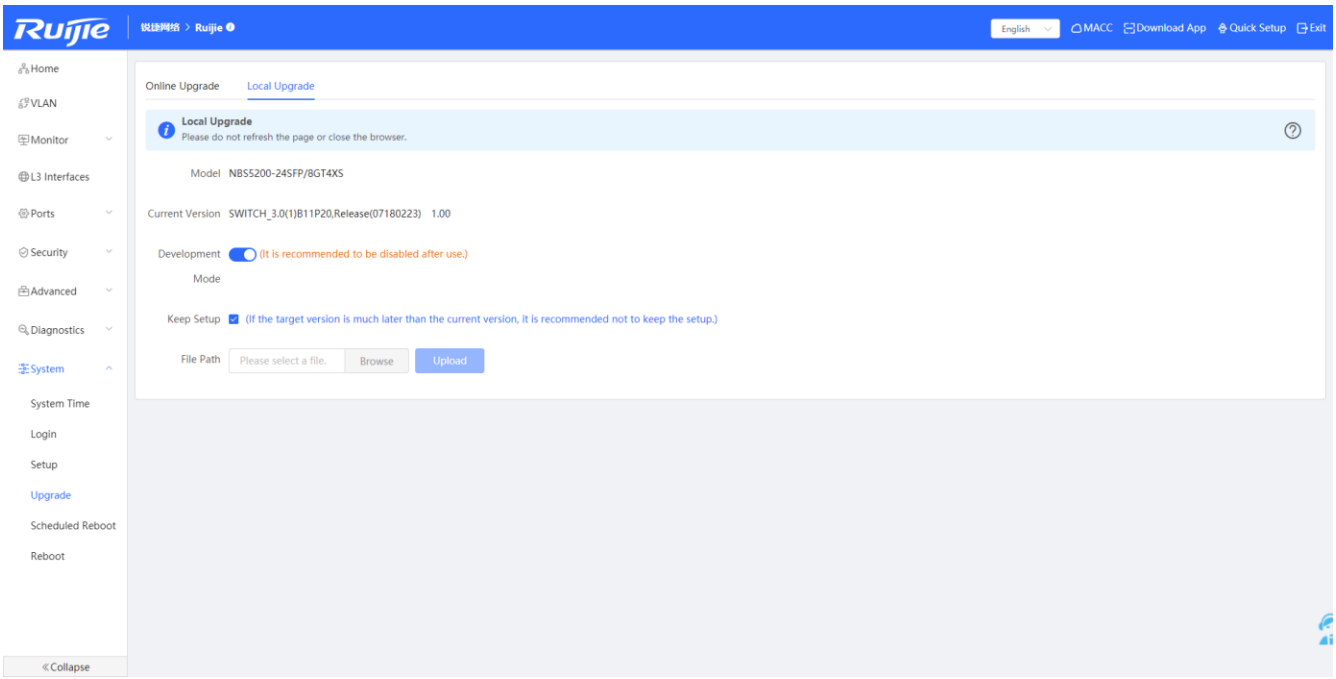
3.9.5 Upgrade

The **Upgrade** module includes **Local Upgrade** and **Online Upgrade**.

3.9.5.1 Local Upgrade

Select a system upgrade package, and click **Upload**. The device is then upgraded to the target version.

Figure 3-9-7 Local Upgrade



- Local upgrade

Click **Browse** to select an upgrade package, and click **Upload**. After uploading and checking the package, the device displays the upgrade package information and a prompt asking for upgrade confirmation. Click **OK** to start the upgrade.

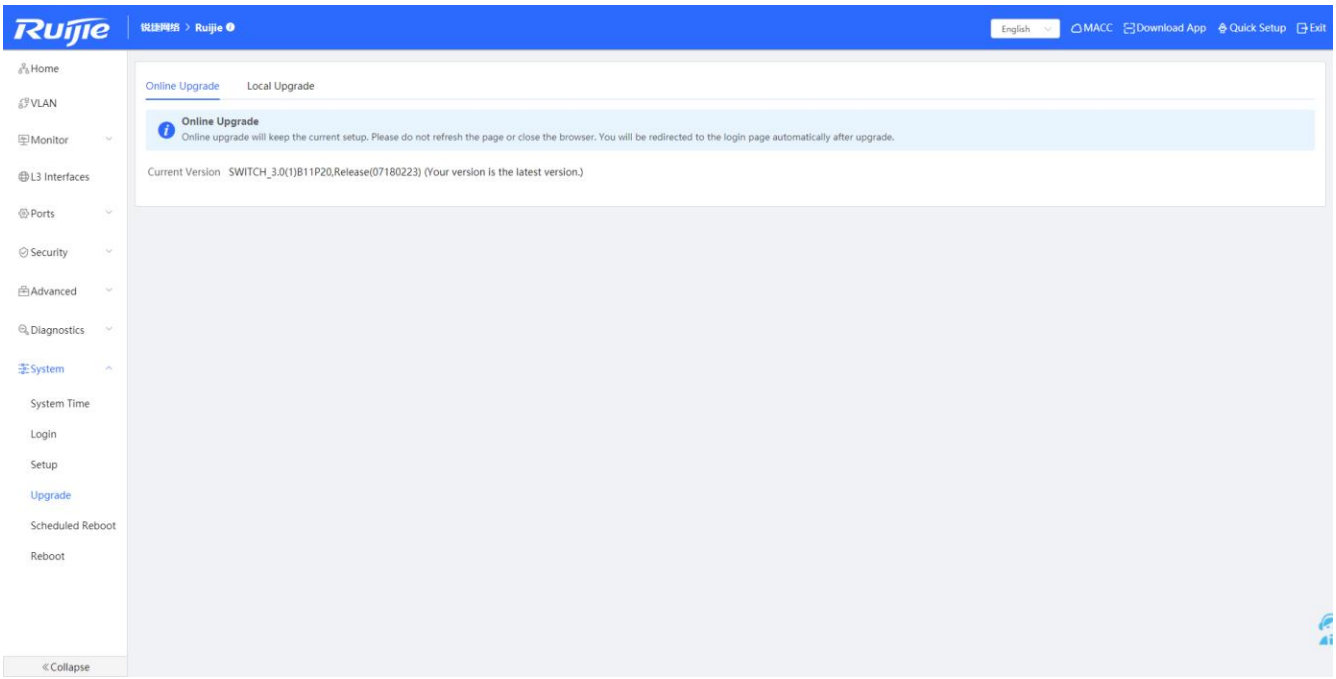
Tips:

1. If the target version is much later than the current version, it is recommended not to retain the settings (uncheck Keep Setup).
2. The upgrade takes a period of time. Do not refresh the page or close the browser during the upgrade.

3.9.5.2 Online Upgrade

The **Online Upgrade** page allows online upgrade. When detecting an available online upgrade version, the device displays information about the available upgrade version, as shown in the figure below.

Figure 3-9-8 Online Upgrade

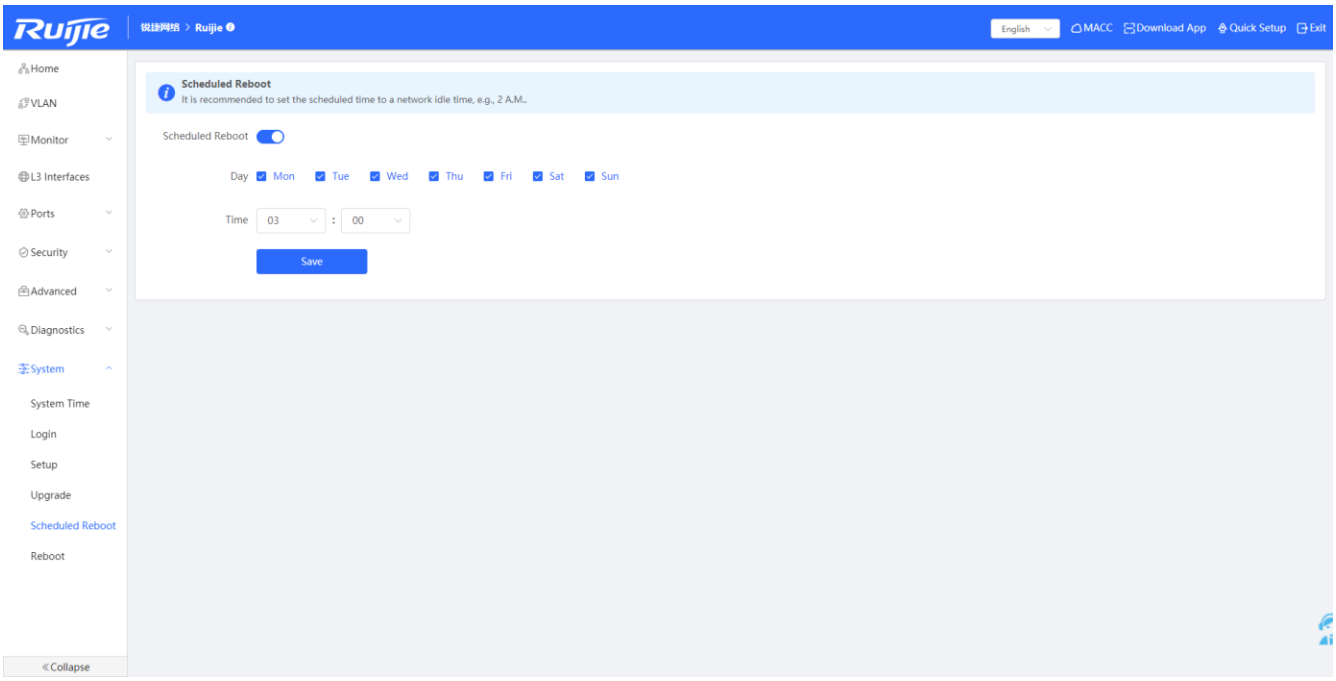


- Online upgrade

Click **Upgrade**. The device downloads the upgrade package from the network, and upgrades the current version. The upgrade operation retains configuration of the current device. Alternatively, you can select **Download File** to the local device and import the upgrade package on the Local Upgrade page. If there is no available new version, the device displays a prompt indicating that the current version is the latest.

3.9.6 Scheduled Reboot

Figure 3-9-9 Scheduled Reboot



- Scheduled reboot

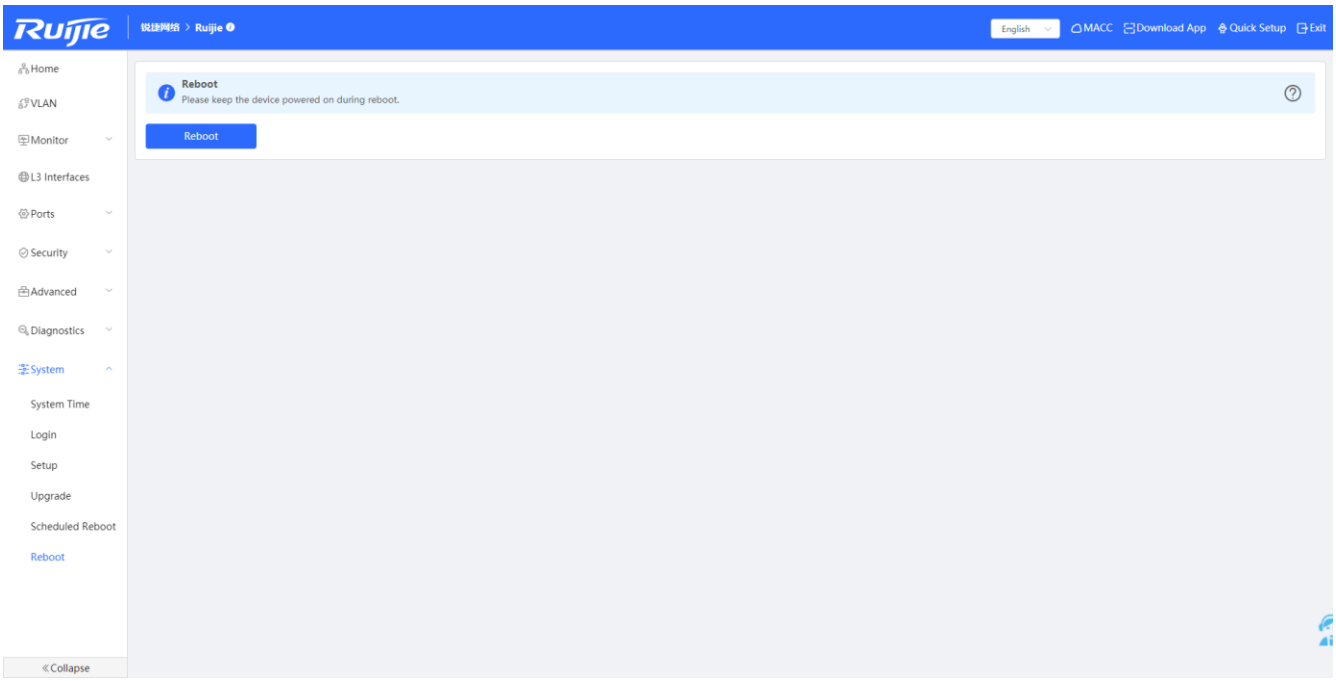
Enable **Scheduled Reboot**, set the day and time when the system needs to be rebooted, and click **Save**.

Tips: When this function is enabled, the system is rebooted at scheduled time for better experience. Off-peak hours are recommended for the reboot.

3.9.7 Reboot

The **Reboot** module provides the **Reboot** button, as shown in the figure below:

Figure 3-9-10 Reboot



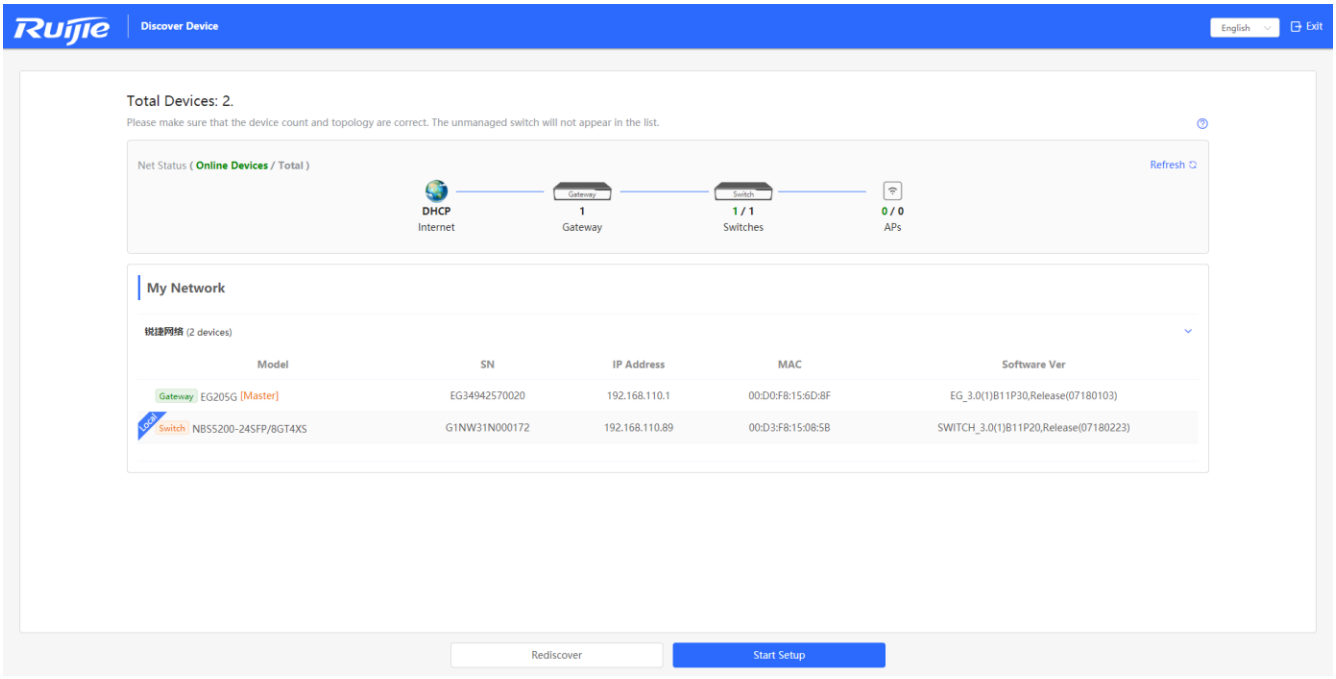
- Reboot

Click **Reboot**, and click **OK** in the confirmation box. The device is rebooted and you need to log into the eWeb management system again after the reboot. Do not refresh the page or close the browser during the reboot. After the device is successfully rebooted and the eWeb service becomes available, you will be redirected to the login page of the eWeb management system.

4 Ad Hoc Network Discovery Mode

4.1 Network Setup

Figure 4-1-1 Network Setup



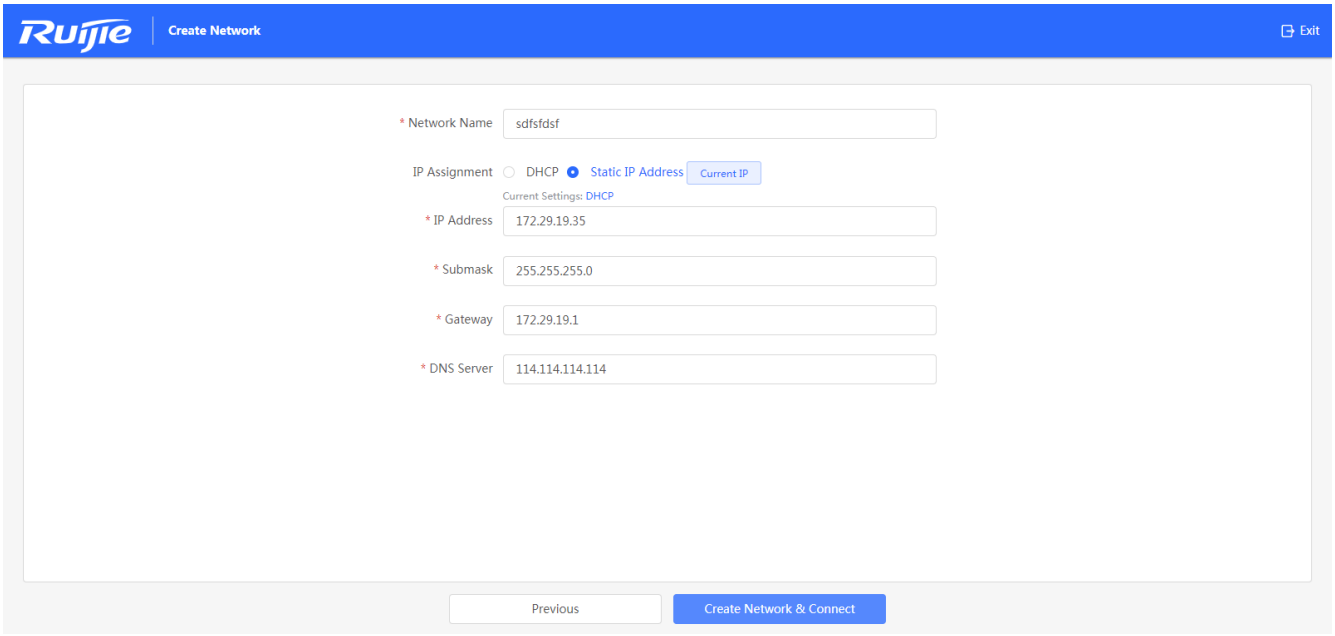
- Discovering devices

Click **Rediscover** to discover devices on the network again.

- Starting setup

Click **Start Setup**. The system jumps to the **Wizard** page, as shown in the figure below:

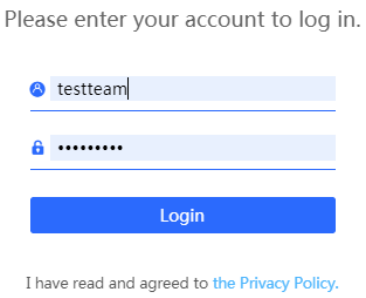
Figure 4-1-2 Wizard



- Settings

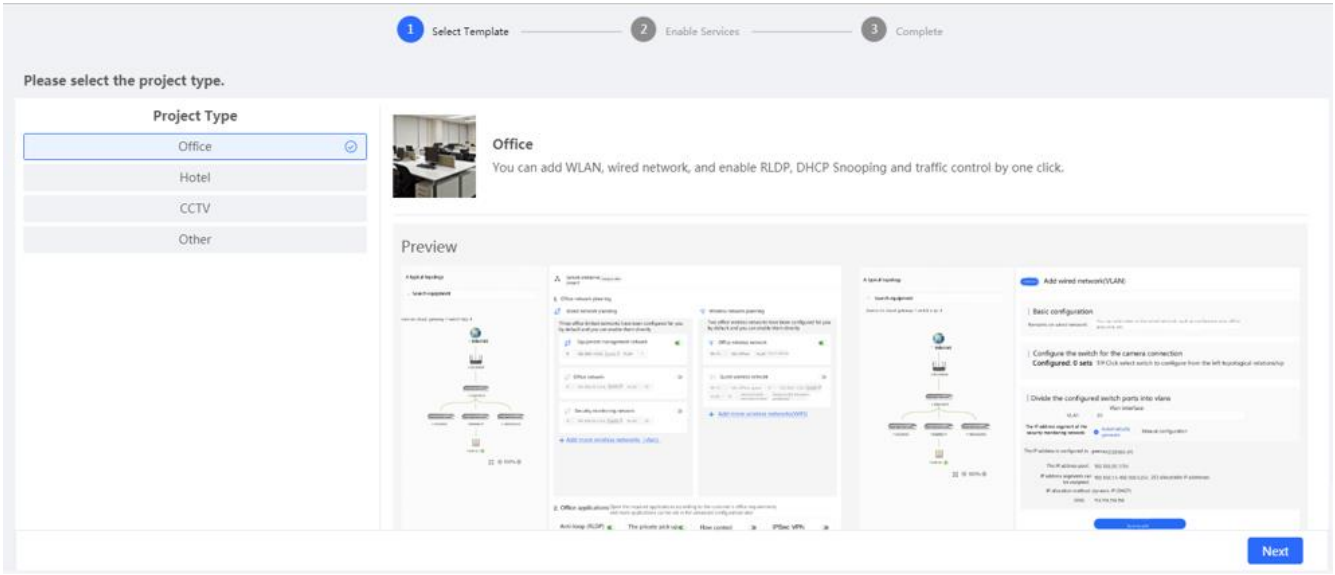
Enter the network name and management password, select the IP assignment mode, and click **Create Network & Connect**. After the network is successfully set up, the following figure is displayed:

Figure 4-1-3 Setup Completion



Enter an account, and the system will automatically jump to the Ruijie Cloud configuration page shown in the figure below:

Figure 4-1-4 Ruijie Cloud Configuration



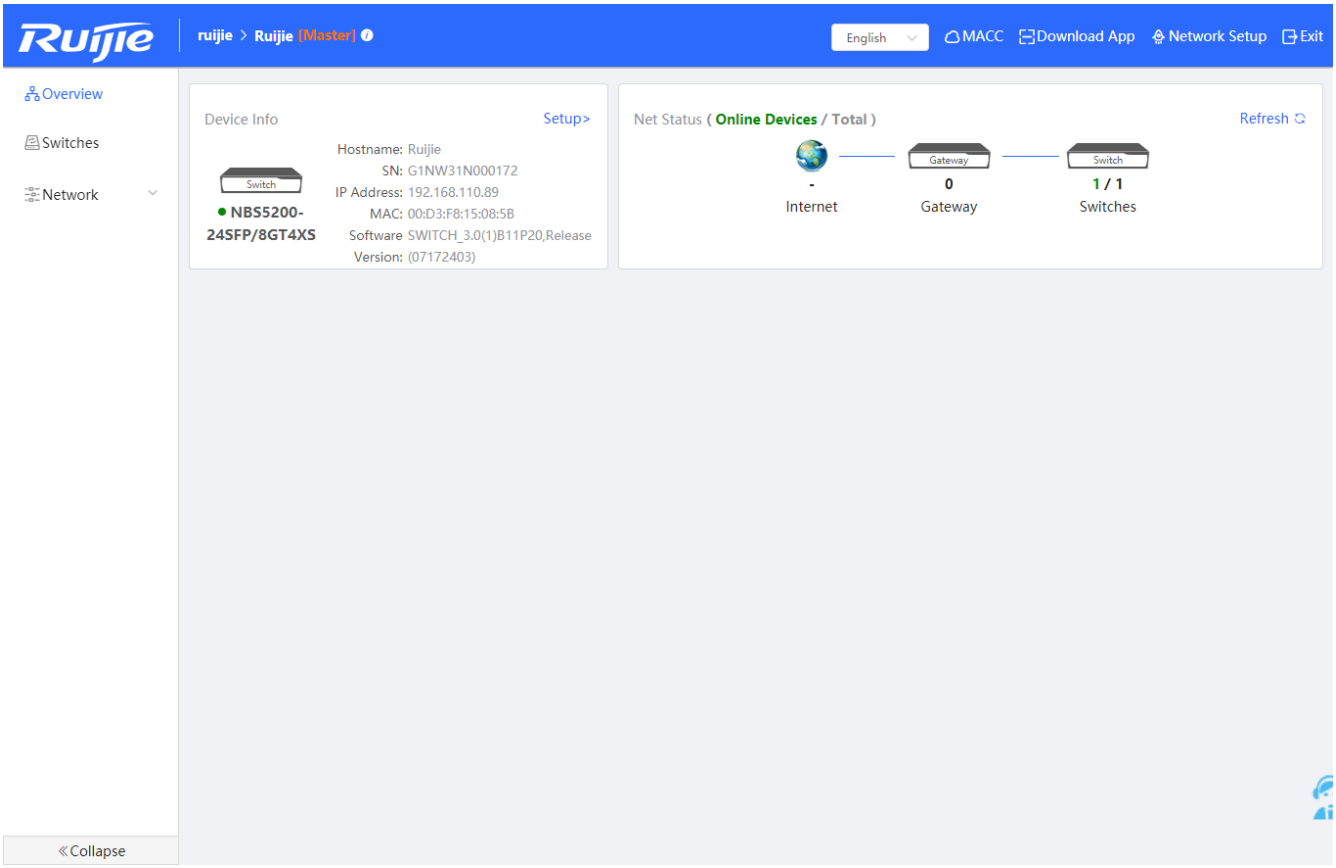
Select the project type, and click **Next**. The system jumps to the page below:

Figure 4-1-5 Topology

4.2 Overview

The **Overview** module displays online devices and basic information about the current device.

Figure 4-2-1 Overview



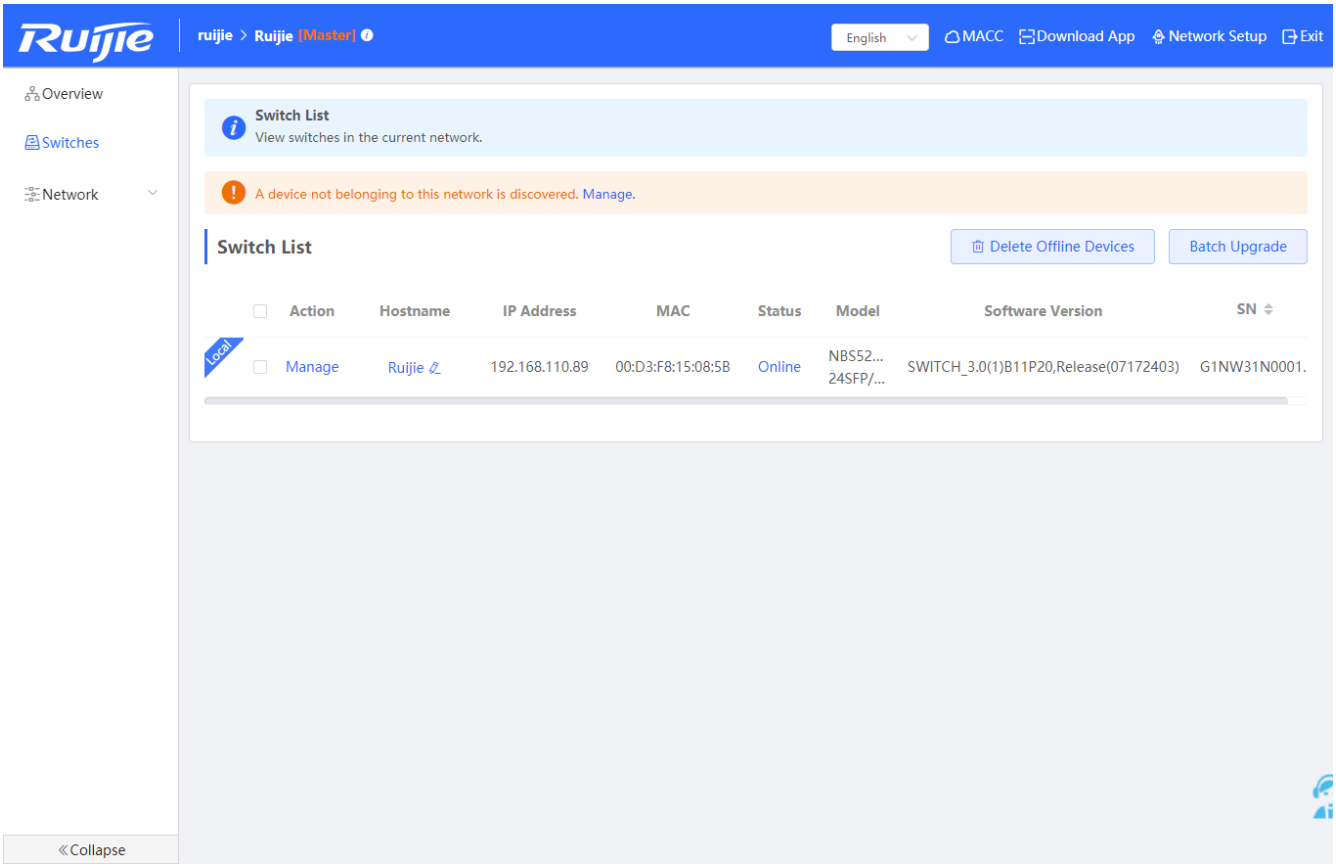
Click the device name on the top navigation bar or **Setup**. The system automatically jumps to the **Switch** module for configuration. (For details, see eWeb Configuration.)

When different devices or new devices exist on the network, a prompt is displayed in the upper right corner upon your first login to the eWeb management system. Click **Manage** to navigate to the **Network List** page to merge networks or perform other operations. For details, see Network Merging.

4.3 Switches

The **Switches** module displays a list of switches (including the NBS and ES2 series) on the same network. When there are switches on different networks, a prompt is displayed and you can click **Manage** to perform required operations.

Figure 4-3-1 Switches



- Deleting offline devices

Select devices in **Switch List**, and click **Delete Offline Devices**. In the displayed confirmation box, click **OK**.

- Upgrading devices

Select devices in **Switch List**, and click **Batch Upgrade**. In the displayed confirmation box, click **OK**.

- Configuring a device

Click **Manage** in the **Action** column. In the displayed page, configure the corresponding device.

Tips:

1. Only offline devices can be deleted.
2. Device configuration in ad hoc network discovery mode is the same as that in standalone mode.
3. The configurations of the ES2 and NBS series are different. (For configuration of the ES2 series, see the ES2 eWeb Configuration Guide.)

4.4 Network

The **Network** module includes **Time**, **Password**, **Scheduled Reboot**, and **Reboot & Reset**.

4.4.1 Time

Time setting is the same as that in **eWeb Configuration > System > System Time**.

4.4.2 Password

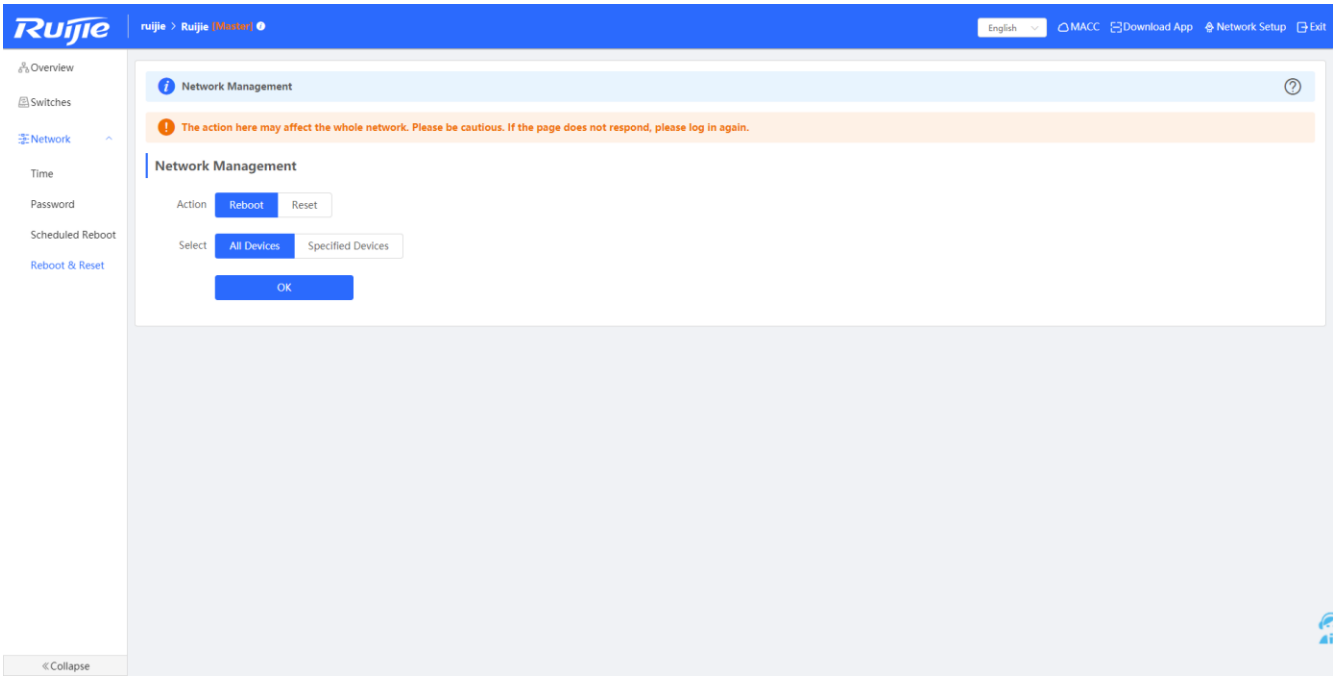
Password setting is the same as that in **eWeb Configuration > System > Login Password**.

4.4.3 Scheduled Reboot

Scheduled reboot setting is the same as that in **eWeb Configuration > System > Scheduled Reboot**.

4.4.4 Reboot & Reset

Figure 4-4-1 Reboot & Reset



- Rebooting devices

Select **Reboot** in **Action**, select **Specified Devices** and click **Add** to add devices to the **Selected Devices** area or select **All Devices**, and click **OK**.

- Resetting devices

Select **Reset** in **Action**, and click **OK**.

Tips:

1. The operations in **Reboot & Reset** may affect the whole network. If the system does not respond after configuration delivery, log into the system again.

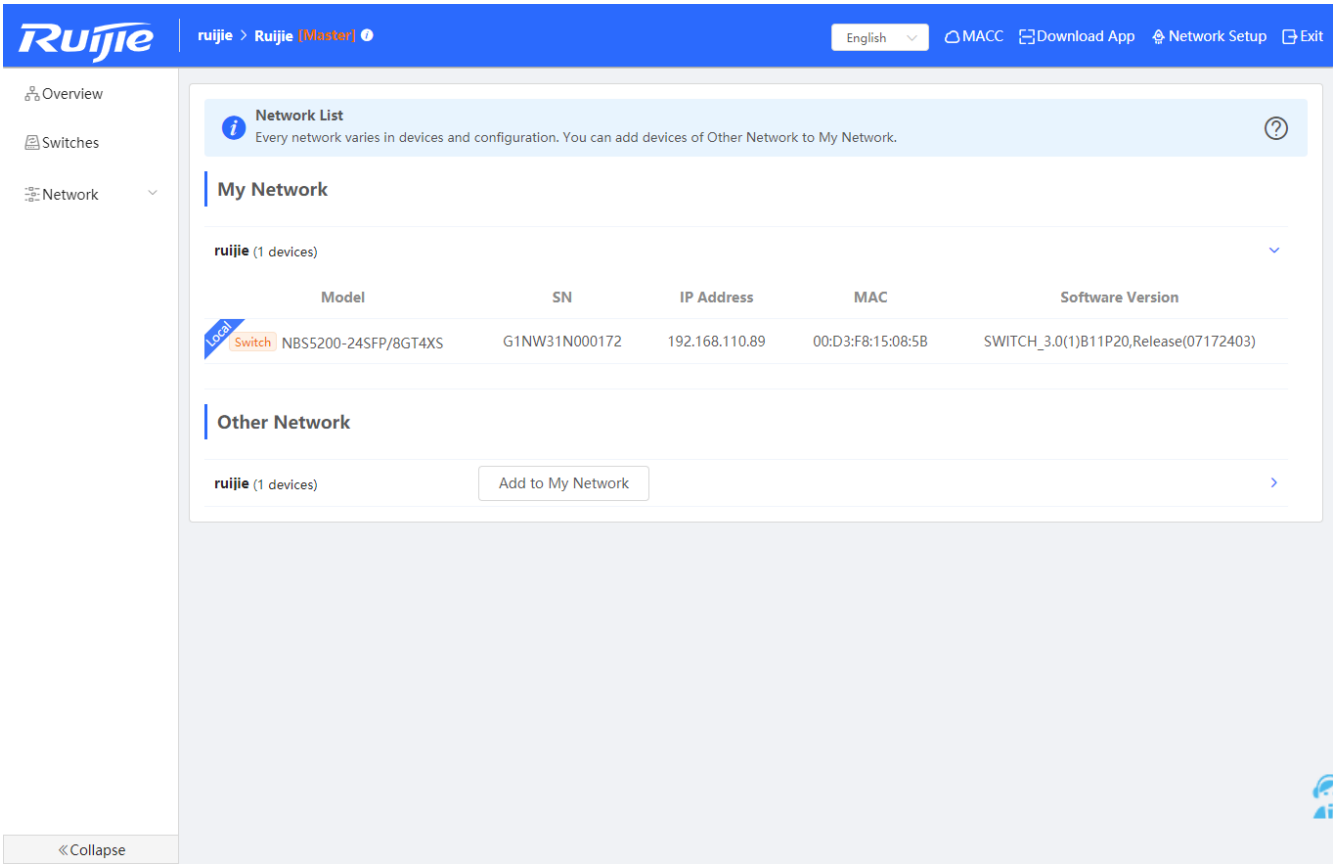
4.5 Network Merging

Every network varies in devices and configuration. You can add devices of **Other Network** to **My Network**.

When devices exist in different networks, you need to manually add these devices to the current network for network management.

The following figure shows **My Network**, **Other Network**, and a list of new devices.

Figure 4-5-1 Network Merging



- Merging networks

Select devices in different networks, and click **Add to My Network**. In the displayed dialog box, enter the management password of the current network, and click **Add**.

Tips:

1. New devices are configured with factory settings by default. No management password is needed for the merging.
2. Network merging takes a period of time.

5 FAQs

Q1: I failed to log into the eWeb management system. What can I do?

A: Perform the following steps:

(1) Check that the network cable is properly connected to the LAN port of the device and the corresponding LED indicator blinks or is steady on.

(2) Before accessing the configuration GUI, set the IP assignment mode to **Obtain an IP address automatically** (recommended), so that the server with DHCP enabled can automatically assign an IP address to the PC. To designate a static IP address to the PC, set the IP address of the PC in the same network segment as the IP address of the management interface. For example, if the default IP address of the management interface is 192.168.110.1 and the subnet mask is 255.255.255.0, set the IP address of the PC to 192.168.110.X (X is any integer ranging from 2 to 254), and the subnet mask is 255.255.255.0.

(3) Run the **ping** command to test the connectivity between the PC and the device.

(4) If the login failure persists, restore the device to factory settings.

Q2: What can I do if I forget my username and password? How to restore the factory settings?

A: To restore the factory settings, power on the device, and press and hold the **Reset** button for 5s or more, and release the **Reset** button after the system LED indicator blinks. The device automatically restores the factory settings and restarts. The original configuration will be lost after the factory settings are restored. After the restoration, the default management address is http://10.44.77.200. You can set the username and password upon first login.

Q3: The subnet mask value needs to be specified to divide the address range for certain functions. What are the common subnet mask values?

A subnet mask is a 32-bit binary address that is used to differentiate between the network address and host address. The subnet and the quantity of hosts in the subnet vary with the subnet mask.

Common subnet mask values include 8 (default subnet mask 255.0.0.0 for class A networks), 16 (default subnet mask 255.255.0.0 for class B networks), 24 (default subnet mask 255.255.255.0 for class C networks), and 32 (default subnet mask 255.255.255.255 for a single IP address).