Ruijie Reyee RG-NBS Series Switches

ReyeeOS 1.84

Web-based Configuration Guide

Document Version: V1.0
Date: 2022.06.16

Copyright

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

- The official website of Ruijie Reyee: https://www.ruijienetworks.com/products/reyee

Conventions

1. GUI Symbols

Interface symbol	Description	Example
Boldface	1. Button names 2. Window names, tab name, field name and menu items 3. Link	1. Click **OK**. 2. Select **Config Wizard**. 3. Click the **Download File** link.
>	Multi-level menus items	Select **System** > **Time**.

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

This manual introduces the product model, port type and CLI for your reference. In case of any discrepancy or inconsistency between the manual and the actual version, the actual version prevails.

Contents

Preface I

1 Overview 1

2 Configuration Guide 2

2.1 Configuration Preparations 2

2.1.1 Connecting to the Device 2

2.1.2 Configuration Environment Requirements 2

2.2 Opening the Eweb Management Page 3

2.3 Quick Setup 4

2.4 Introduction to the Eweb GUI 5

2.4.1 Eweb GUI in Self-Organizing Network Mode 5

2.4.2 Eweb GUI in Standalone Mode 6

2.4.3 Switching the Work Mode 7

2.4.4 Top Navigation Bar 8

2.4.5 Menu Navigation Area 10

3 Eweb Configuration (Standalone Mode) 12

3.1 Home Page 12

3.2 VLAN 14

3.2.1 VLAN List 14

3.2.2 Port List 17

3.3 Monitor 19

3.3.1 Port Info 19

3.3.2 Clients 20

3.4 Port Management 27

3.4.1 Overview 27

3.4.2 Interface Type 27

3.4.3 Port Settings 29

3.4.4 Aggregate Ports 33

3.4.5 Port Mirroring 37

3.4.6 Rate Limiting 40

3.4.7 MGMT IP 42

3.4.8 Out-of-Band IP 43

3.5 L2 Multicast 44

3.5.1 Overview 44

3.5.2 Global Settings 45

3.5.3 IGMP Snooping 46

3.5.4 MVR 48

3.5.5 Multicast Group 51

3.5.6 IGMP Filter 52

3.5.7 Querier 54

3.6 L3 Management 56

3.6.1 L3 Interfaces 56

3.6.2 DHCP Clients 59

3.6.3 Static IP Addresses 60

3.6.4 DHCP Option 61

3.6.5 Static Routing 62

3.6.6 ARP List 63

3.7 Security 65

3.7.1 DHCP Snooping........65

3.7.2 Storm Control........66

3.7.3 ACL........67

3.7.4 Port Protection........70

3.7.5 IP-MAC Binding........71

3.7.6 IP Source Guard........73

3.7.7 Anti-ARP Spoofing........76

3.8 Advanced........77

3.8.1 STP........78

3.8.2 LLDP........81

3.8.3 RLDP........85

3.8.4 Local DNS........87

3.8.5 Voice VLAN........87

3.9 Diagnostics........91

3.9.1 Info Center........91

3.9.2 Network Tools........92

3.9.3 Fault Collection........94

3.9.4 Cable Diagnostics........95

3.9.5 System Logs........95

3.9.6 Alerts........96

3.10 System........98

3.10.1 System Time........98

3.10.2 Login........99

3.10.3 Setup........100

3.10.4 Upgrade 102

3.10.5 Scheduled Reboot 103

3.10.6 Reboot...103

4 FAQs...105

4.1 Failure to Log In to the Eweb Management System 105

4.2 Password Lost and Restoration of Factory Settings 105

4.3 IP Subnet Mask..106

1 Overview

This document describes how to use the Eweb management system. You can use the Eweb management system to manage switches.

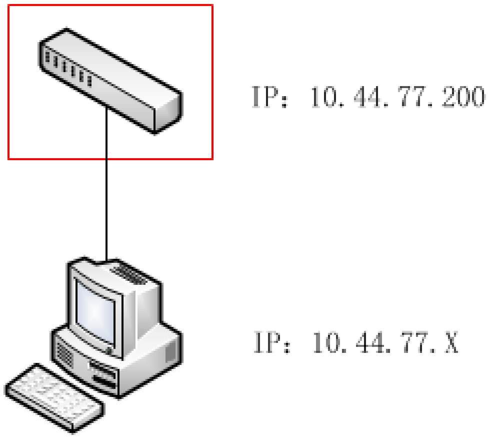
You can access the Eweb management system through a browser (such as Google Chrome) to manage switches.

2 Configuration Guide

2.1 Configuration Preparations

2.1.1 Connecting to the Device

As shown in the figure below, you can connect a PC to the switch through a network cable and access the Eweb management system of the switch to manage and configure the switch.



Note

The device enclosed in the red rectangle in the figure above is the accessed switch. Configure one IP address that is in the same network segment as the switch IP address for the management computer so that the PC can ping through the switch. Then, you can access the Eweb management system of the switch.

2.1.2 Configuration Environment Requirements

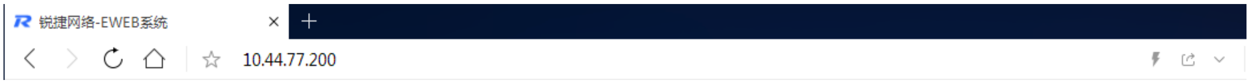
Client requirements:

- You can log in to the Eweb management page through the Web browser to manage the device. Clients refer to PCs or other mobile terminals such as laptops.
- Google Chrome, Firefox, IE9.0, IE10.0, IE11.0, and some Chromium-based browsers (such as 360 Extreme Explorer) are supported. Exceptions such as garble characters or format error may occur if an unsupported browser is used. If you are using IE6, IE7, or IE8, upgrade it to IE10 or IE11 or use a more standard browser such as Google Chrome or Firefox.

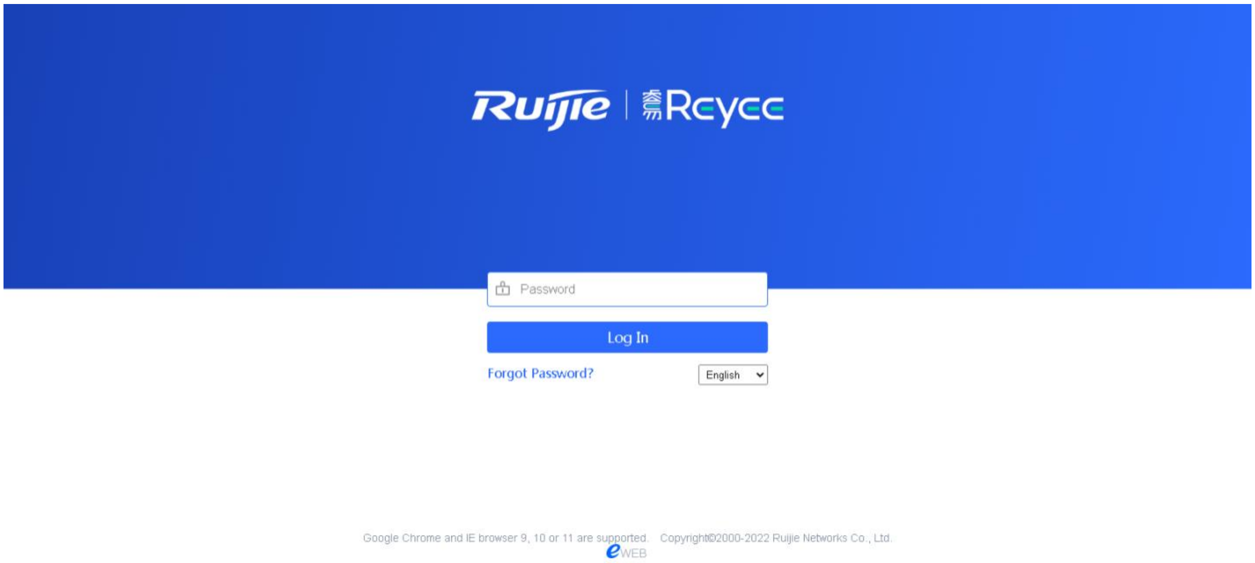
- 1024 x 768 or a higher resolution is recommended. If other resolutions are used, the page fonts and formats may not be aligned, the GUI is less artistic, or other exceptions may occur.

2.2 Opening the Eweb Management Page

Enter the IP address (10.44.77.200 by default) of the switch in the address bar of the browser. The IP address of your PC must be in the same network segment as that of the switch.



Enter the password and click **Log In** to access the management homepage of the device. If you forget the password, click **Forgot Password** and follow prompts on the page to restore factory settings.



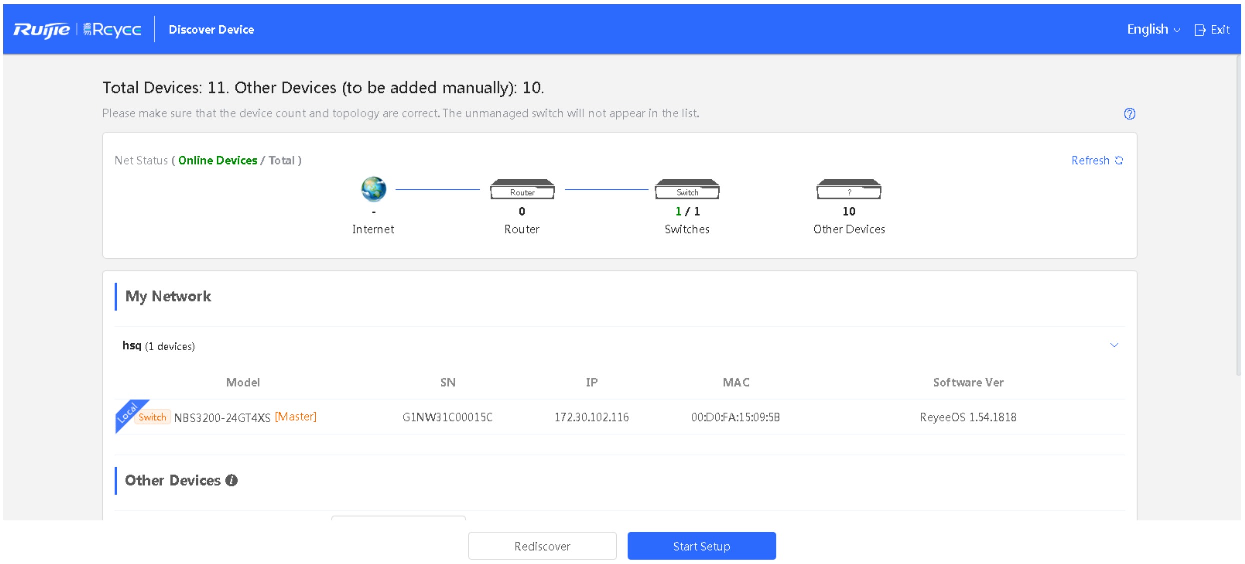
Google Chrome and IE browser 9, 10 or 11 are supported. Copyright©2000-2022 Ruijie Networks Co., Ltd.

Note

1. The default management IP address (Eweb management IP address) of the device is 10.44.77.200.
2. If a static IP address is configured for a PC or the PC dynamically obtains a new IP address, you can access the Eweb management system of the device by using the new IP address.
3. No password is configured for the Eweb management system by default. You can directly log in to the device to configure and manage the device.
4. You are strongly advised to set a management password after logging in to the Eweb management system. After setting a password, you need to enter the password to log in to the Eweb management system.

2.3 Quick Setup

You need to quickly configure the device (configure the network name, management password, and management IP address of the device) when logging in to the Eweb management system for the first time (for initial configuration). If you have set the password, skip this step.



Discover Device

Total Devices: 11. Other Devices (to be added manually): 10.

Please make sure that the device count and topology are correct. The unmanaged switch will not appear in the list.

Net Status (Online Devices / Total)

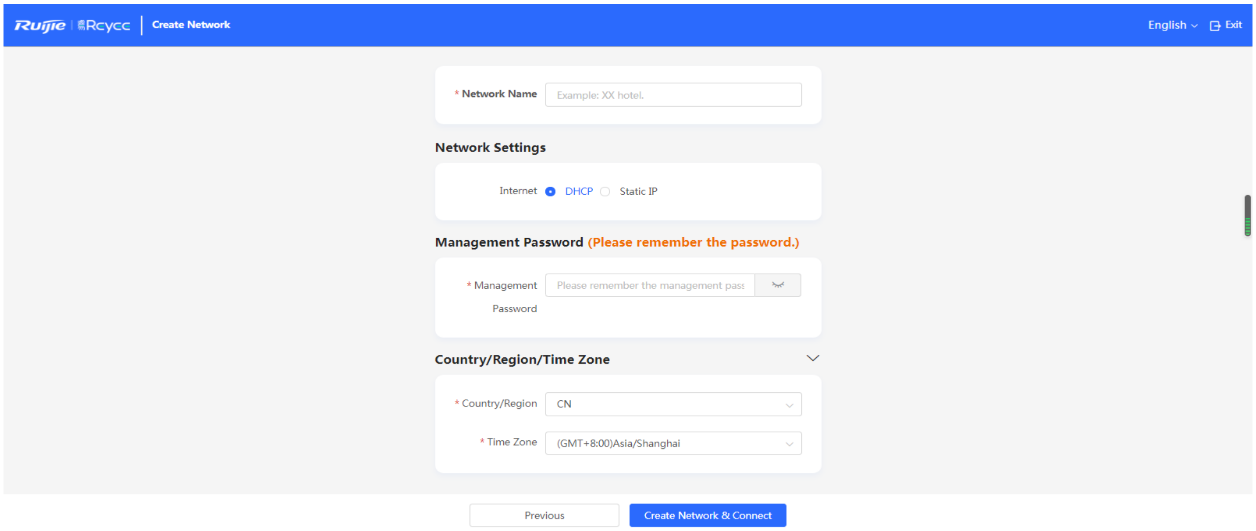
My Network

hsq (1 devices)

Model	SN	IP	MAC	Software Ver
Local Switch NBS3200-24GT4XS [Master]	G1NW31C00015C	172.30.102.116	00:D0:FA:15:09:5B	ReyeeOS 1.54.1818

Other Devices

Confirm the device on the network and click **Start Setup**.



Create Network

* Network Name: Example: XX hotel.

Network Settings

Internet ● DHCP ○ Static IP

Management Password (Please remember the password.)

* Management Password: Please remember the management pass

Country/Region/Time Zone

* Country/Region: CN

* Time Zone: (GMT+8:00)Asia/Shanghai

Network Name identifies the network where the device is located (you need to enter the network name upon initial use).

Management Password indicates the password for logging in to the Eweb management system of the device. (Keep the password confidential. If you forget the password, see 4.2 Password Lost and Restoration of Factory Settings).

Internet allows you to configure the network access mode for the device, and can be set to **DHCP** (the Dynamic Host Configuration Protocol (DHCP) server allocates IP addresses) or **Static IP** (you need to manually enter a specified IP address, subnet mask, gateway IP address, and Domain Name System (DNS) address).

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

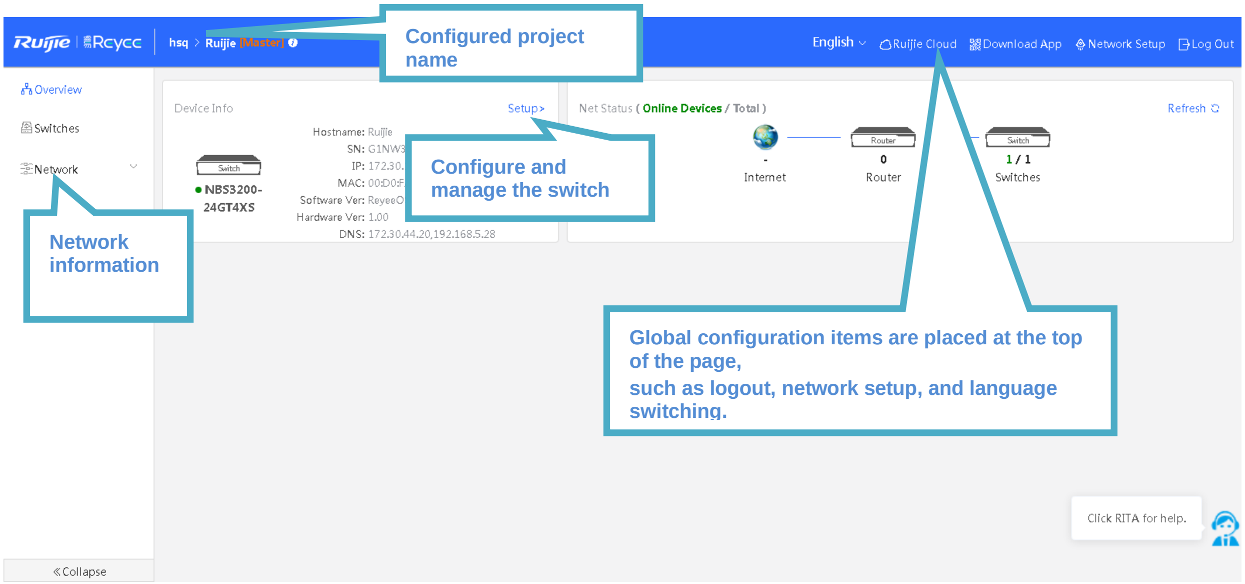
Click **Exit** in the upper right corner and follow prompts to perform operations. Then, the device can skip quick setup to go to the Eweb management system.

2.4 Introduction to the Eweb GUI

The device supports two work modes: **Standalone** and **Self-Organizing Network**. It works in **Self-Organizing Network** mode by default. The system presents different menu items based on the work mode.

2.4.1 Eweb GUI in Self-Organizing Network Mode

In self-organizing network mode, you can configure and manage the logged in device and configure and maintenance other devices on the network.



Configured project name

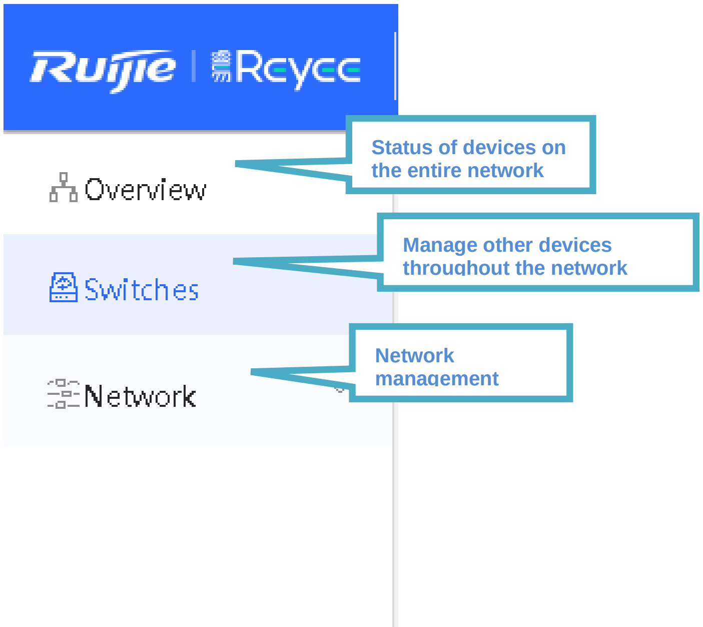
Configure and manage the switch

Network information

Global configuration items are placed at the top of the page,
such as logout, network setup, and language switching.

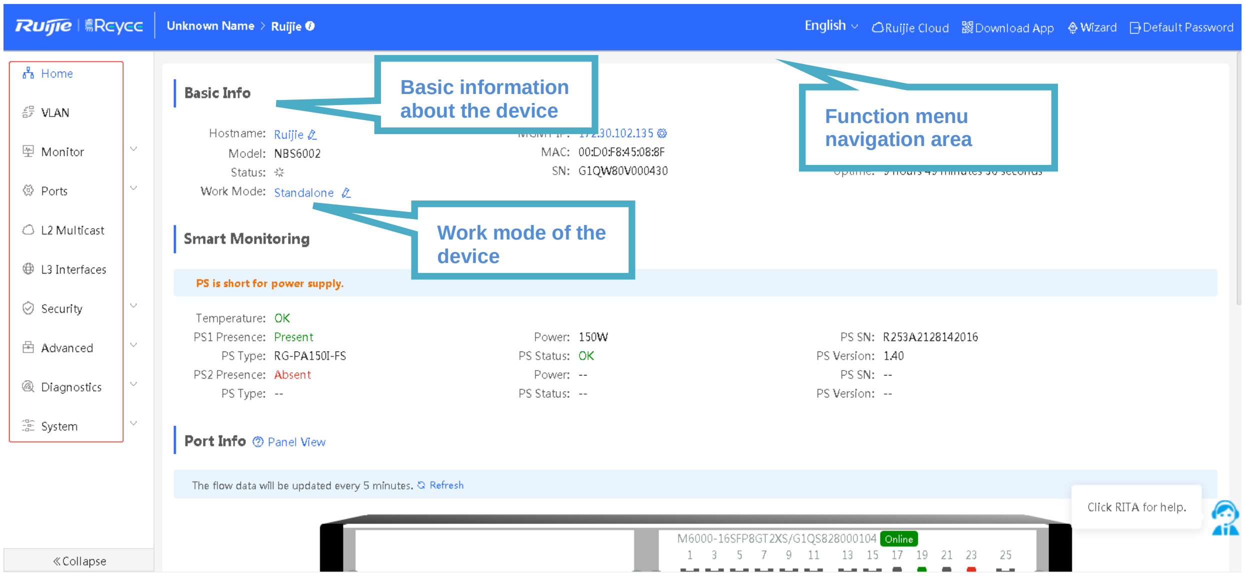
1. Network Information Area

In self-organizing network mode, the network information area is displayed in the left part of the Eweb homepage. The area displays the bridging status of devices on the entire network and allows you to modify network configurations. You can also quickly modify the configuration of a device.


Ruijie | Reyee
Overview
Switches
Network
Status of devices on the entire network
Manage other devices throughout the network
Network management

2. Switch Configuration

In self-organizing network mode, select the current logged in device from **Overview** and click **Setup** to go to the switch configuration page.



Basic Info

Hostname: Ruijie
Model: NBS6002
Status:
Work Mode: Standalone
MGMT IP: 172.30.102.135
MAC: 00:D0:F8:45:08:8F
SN: G1QW80V000430

Smart Monitoring

PS is short for power supply.

Temperature: OK
PS1 Presence: Present
PS Type: RG-PA150I-FS
PS2 Presence: Absent
PS Type: --

Power: 150W
PS Status: OK
Power: --
PS Status: --

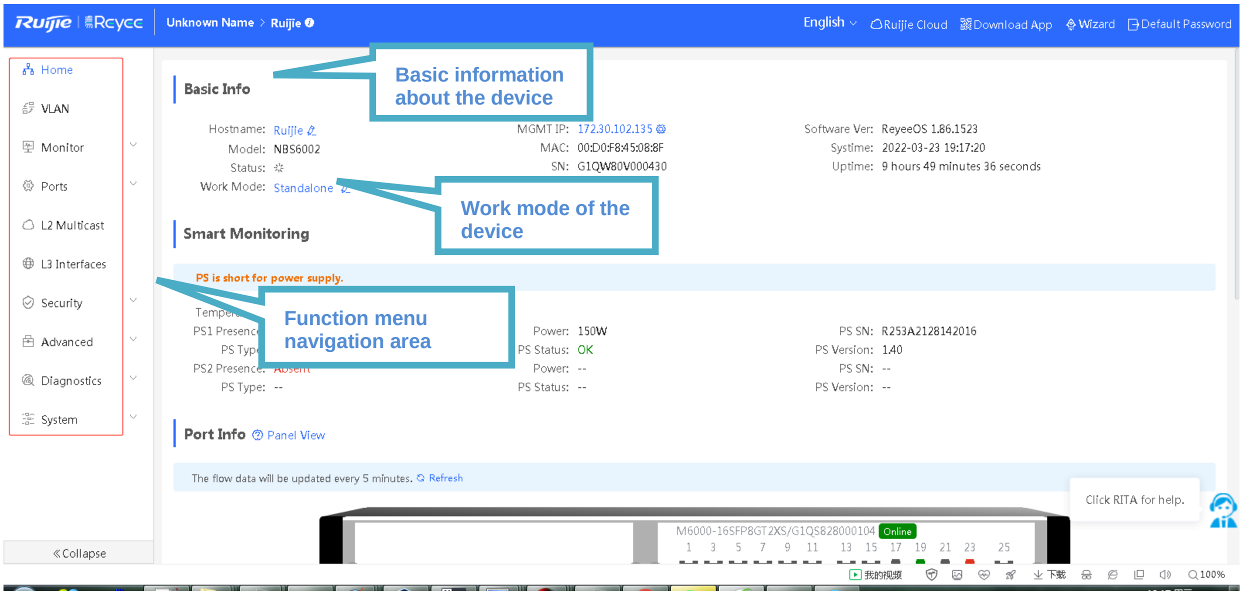
PS SN: R253A2128142016
PS Version: 1.40
PS SN: --
PS Version: --

Port Info Panel View

The flow data will be updated every 5 minutes. Refresh

2.4.2 Eweb GUI in Standalone Mode

In standalone mode, you can configure and manage only the current logged in device.



Basic information about the device

Work mode of the device

Function menu navigation area

Basic Info

Hostname: Ruijie
Model: NBS6002
Status:
Work Mode: Standalone
MGMT IP: 172.30.102.135
MAC: 00:D0:F8:45:08:8F
SN: G1QW80V000430
Software Ver: ReyeeOS 1.86.1523
Systime: 2022-03-23 19:17:20
Uptime: 9 hours 49 minutes 36 seconds

Smart Monitoring

PS is short for power supply.

Tempe
PS1 Presenc
PS Typ
PS2 Presence: Absent
PS Type: --
Power: 150W
PS Status: OK
Power: --
PS Status: --
PS SN: R253A2128142016
PS Version: 1.40
PS SN: --
PS Version: --

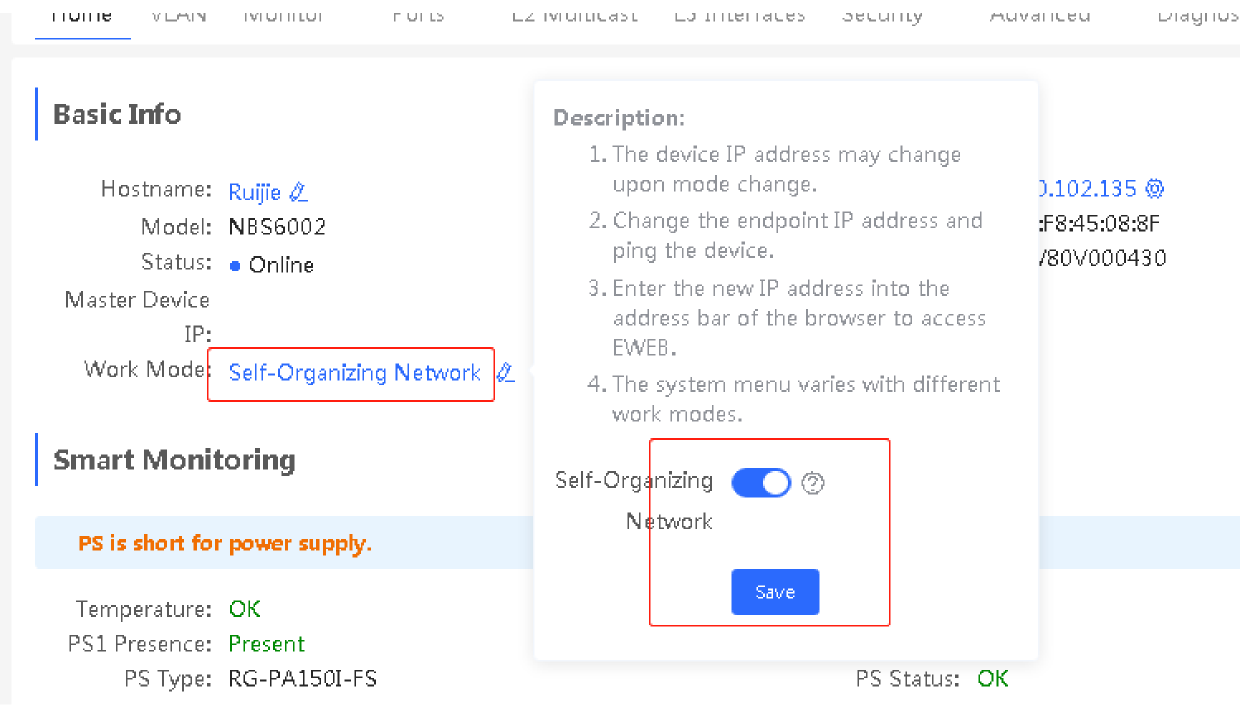
Port Info

The flow data will be updated every 5 minutes.

2.4.3 Switching the Work Mode

The device supports two work modes: **Standalone** and **Self-Organizing Network**. It works in **Self-Organizing Network** mode by default.

1. In self-organizing networking mode, click **Overview** and select **Setup** to go to the switch configuration page (ignore this step in standalone mode).
2. Click **Home** and click the work mode in **Basic Info**, select whether to enable the self-organizing network mode and click **Save** to switch the work mode of the device.



Basic Info

Hostname: Ruijie

Model: NBS6002

Status: ● Online

Master Device IP:

Work Mode: Self-Organizing Network

0.102.135

:F8:45:08:8F

/80V000430

Smart Monitoring

PS is short for power supply.

Temperature: OK

PS1 Presence: Present

PS Type: RG-PA150I-FS

PS Status: OK

Description:

1. The device IP address may change upon mode change.
2. Change the endpoint IP address and ping the device.
3. Enter the new IP address into the address bar of the browser to access EWEB.
4. The system menu varies with different work modes.

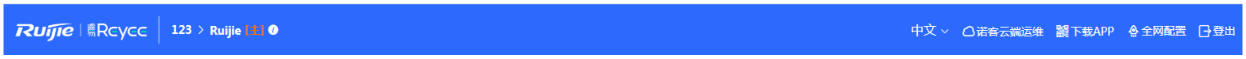
Self-Organizing Network

Caution

1. The browser refreshes the page after the device switches the work mode.

2. After the mode is switched, the IP address of the device may change. You need to change the client address to ensure that the client can ping through the device. Then, enter the new address in the browser to access the Eweb management system.

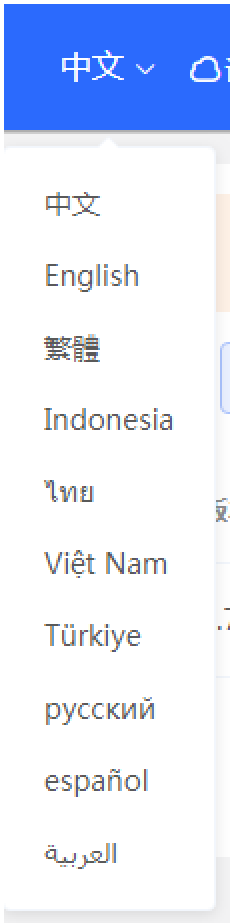
2.4.4 Top Navigation Bar



The top navigation bar successively displays the manufacturer logo, network name, and device name on the left, and device shortcuts (including **Language**, **Ruijie Cloud**, **Download App**, **Wizard**, **Log Out**) on the right.

1. Language Switching

Click **English** and select the required language to switch the display language of Eweb. Currently, multiple languages are supported.



2. Ruijie Cloud

Move the cursor over **Ruijie Cloud**. The Web link of Ruijie Cloud and the QR code of the management mini program pop up below.

3. Download App

Move the cursor over **Download App**. The QR code for downloading the app is displayed below. You can scan the QR code to download the app for mobile configuration.

4. Network Setup

Move the cursor over **Wizard** to redirect to the network configuration page, which shows other switches in the same network segment as the switch. You can add other switches to your project network for centralized management.

5. Exit

Click **Exit** to log out of the system. If you are using a public computer, you are advised to log out in time after completing operations.

Note

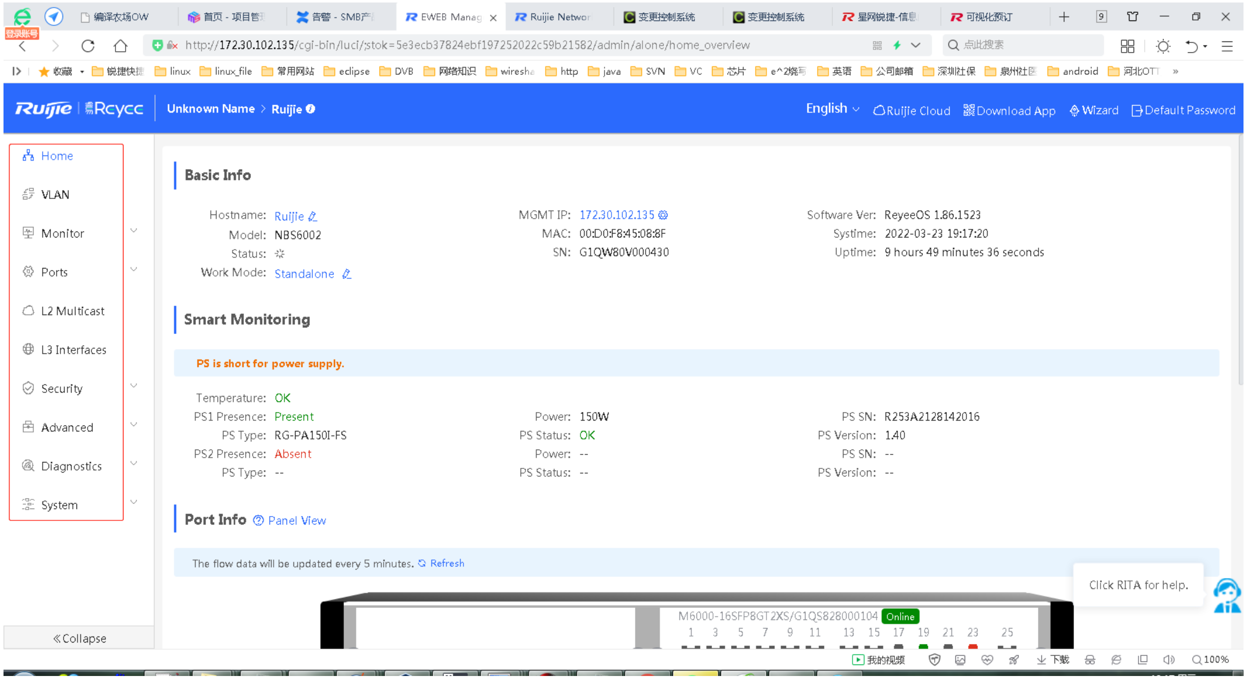
If a user does not log out, the user can still access the Eweb management system without authentication within the Web session timeout duration (1 hour by default). After the current session times out, the user needs to re-log in. For details about how to set the Web session timeout duration, see 3.10.2 Login.

2.4.5 Menu Navigation Area

The Eweb management page provides the function menu navigation area, which is located in the left part of Eweb in standalone mode and on the switch configuration page in self-organizing network mode. This area lists all functions of the switch. Click a menu item to open the detailed setup page.

The menu is organized in two levels. When you click a menu item that contains level-2 menu items, the level-2 menu items will be displayed. For example, clicking **Monitor** will expand the **Port Flow** and **Clients** submenu items.

Standalone mode:



Basic Info

Hostname: Ruijie
Model: NBS6002
Status:
Work Mode: Standalone
MGMT IP: 172.30.102.135
MAC: 00:D0:F8:45:08:8F
SN: G1QW80V000430
Software Ver: ReyeeOS 1.86.1523
Systime: 2022-03-23 19:17:20
Uptime: 9 hours 49 minutes 36 seconds

Smart Monitoring

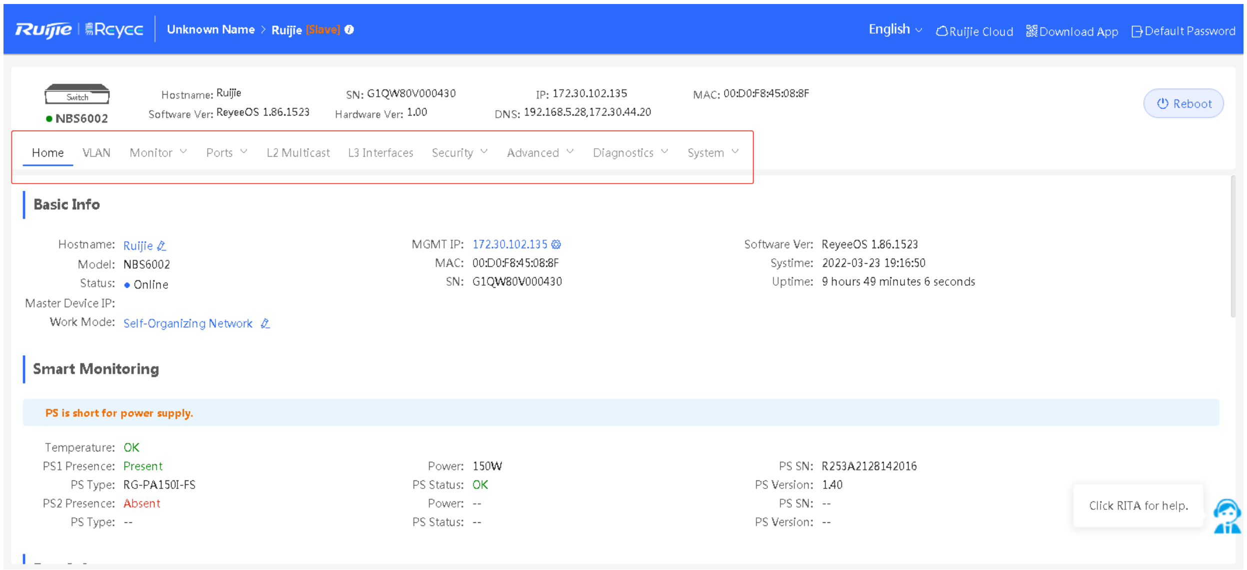
PS is short for power supply.

Temperature: OK
PS1 Presence: Present
PS Type: RG-PA150I-FS
PS2 Presence: Absent
PS Type: --
Power: 150W
PS Status: OK
Power: --
PS Status: --
PS SN: R253A2128142016
PS Version: 1.40
PS SN: --
PS Version: --

Port Info Panel View

The flow data will be updated every 5 minutes. Refresh

Self-organizing mode:



Hostname: Ruijie
Software Ver: ReyeeOS 1.86.1523
SN: G1QW80V000430
Hardware Ver: 1.00
IP: 172.30.102.135
DNS: 192.168.5.28,172.30.44.20
MAC: 00:D0:F8:45:08:8F

Basic Info

Hostname: Ruijie
Model: NBS6002
Status: ● Online
Master Device IP:
Work Mode: Self-Organizing Network

MGMT IP: 172.30.102.135
MAC: 00:D0:F8:45:08:8F
SN: G1QW80V000430

Software Ver: ReyeeOS 1.86.1523
Systime: 2022-03-23 19:16:50
Uptime: 9 hours 49 minutes 6 seconds

Smart Monitoring

PS is short for power supply.

Temperature: OK
PS1 Presence: Present
PS Type: RG-PA150I-FS
PS2 Presence: Absent
PS Type: --

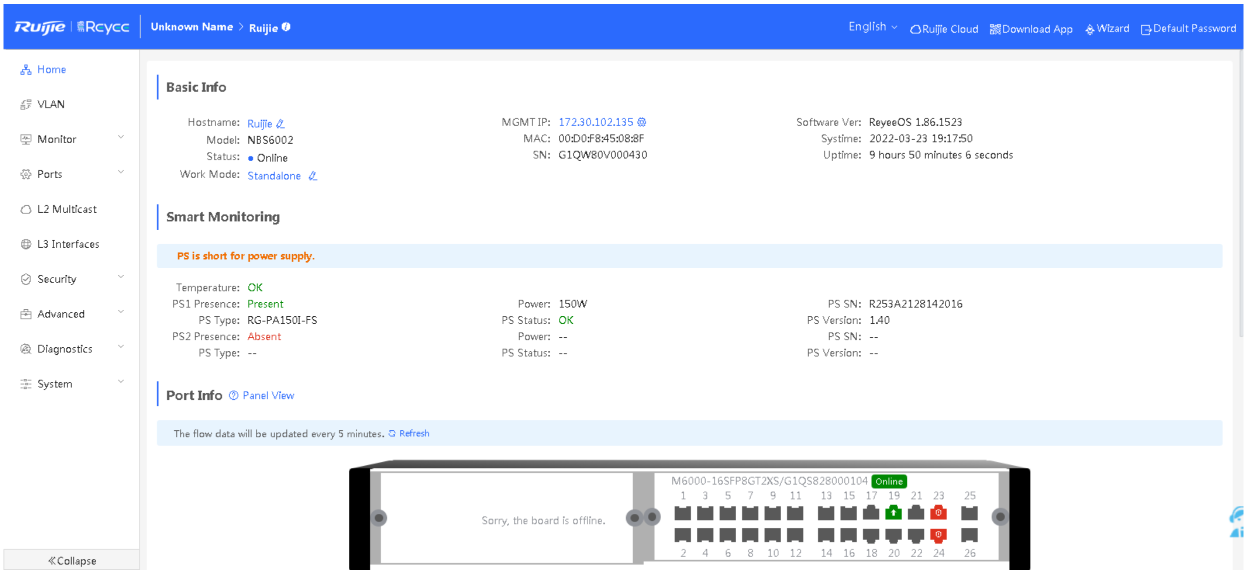
Power: 150W
PS Status: OK
Power: --
PS Status: --

PS SN: R253A2128142016
PS Version: 1.40
PS SN: --
PS Version: --

3 Eweb Configuration (Standalone Mode)

3.1 Home Page

The **Home** page displays basic information about the device and details about switch ports. See the figure below.



Basic Info

Hostname: Ruijie
Model: NBS6002
Status: Online
Work Mode: Standalone
MGMT IP: 172.30.102.135
MAC: 00:D0:F8:45:08:8F
SN: G1QW80V000430
Software Ver: ReyeeOS 1.86.1523
Systime: 2022-03-23 19:17:50
Uptime: 9 hours 50 minutes 6 seconds

Smart Monitoring

PS is short for power supply.

Temperature: OK
PS1 Presence: Present
PS Type: RG-PA150I-FS
Power: 150W
PS Status: OK
PS SN: R253A2128142016
PS Version: 1.40
PS2 Presence: Absent
PS Type: --
Power: --
PS Status: --
PS SN: --
PS Version: --

Port Info

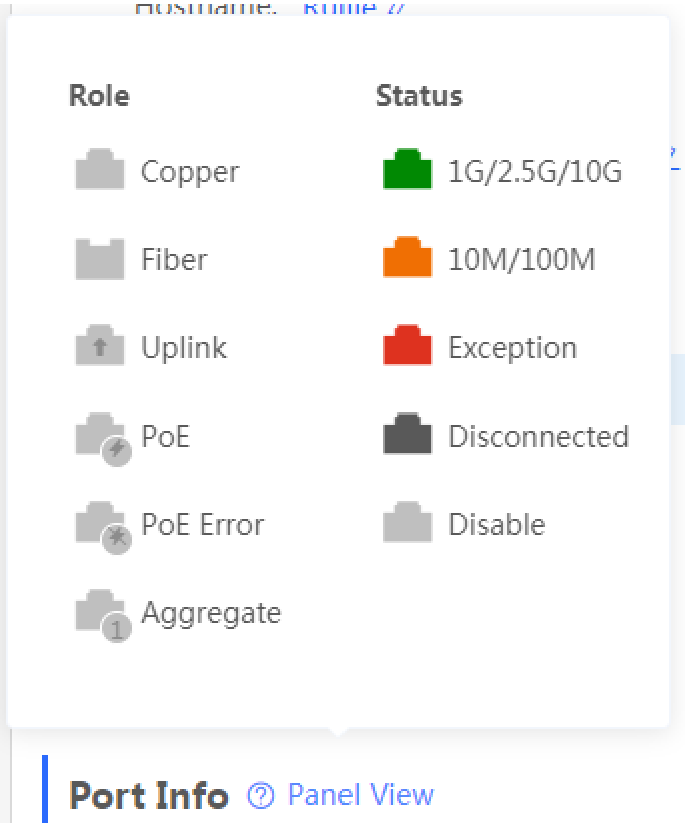
The flow data will be updated every 5 minutes.

Sorry, the board is offline.

In the **Basic Info** area, you can configure the device name and device management IP address, switch the work mode of the device (see 2.4.3 Switching the Work Mode).

The **Smart Monitoring** area displays the current hardware operating status of the device, such as the device temperature and power supply status (only some devices support this function).

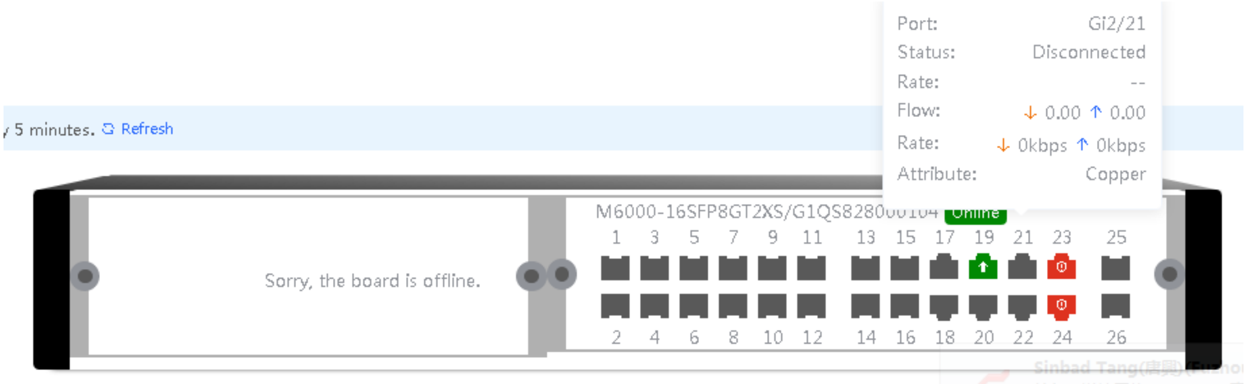
The **Port Info** area displays details about all ports on the switch. Click **Panel View** to display the icon color and type corresponding to each port status.



Role	Status
Copper	🟩 1G/2.5G/10G
Fiber	🟧 10M/100M
Uplink	🟥 Exception
PoE	■ Disconnected
PoE Error	Disable
Aggregate	

Port Info ⓘ Panel View

Move the cursor over the icon of a port (for example, Gi1/23) on the port panel. More information about the port is displayed, including the port ID, port status, port rate, uplink and downlink traffic, transmission rate, and optical/electrical attribute of the port.



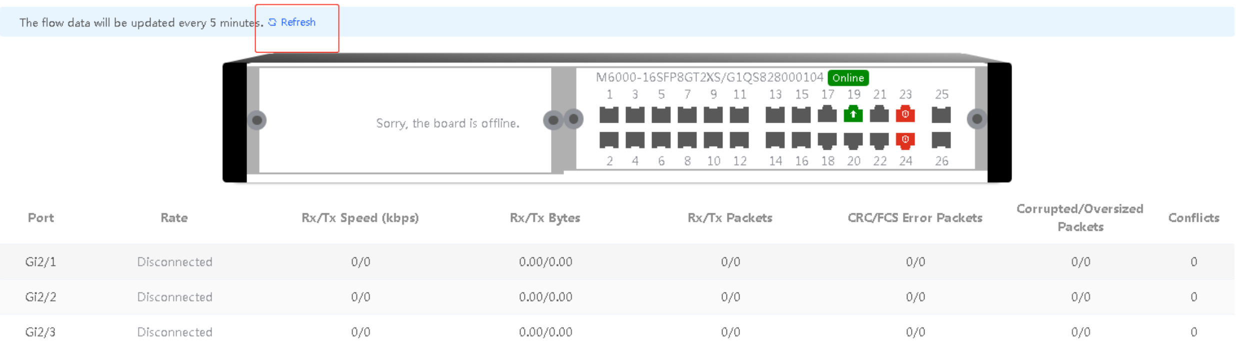
5 minutes. Refresh

Port:	Gi2/21
Status:	Disconnected
Rate:	--
Flow:	↓ 0.00 ↑ 0.00
Rate:	↓ 0kbps ↑ 0kbps
Attribute:	Copper

Sorry, the board is offline.

M6000-16SFP8GT2XS/G1QS828000104 Online

Traffic data is automatically updated every five minutes. You can click **Refresh** above the port panel to obtain the latest port traffic and status information.



The flow data will be updated every 5 minutes. Refresh

Port	Rate	Rx/Tx Speed (kbps)	Rx/Tx Bytes	Rx/Tx Packets	CRC/FCS Error Packets	Corrupted/Oversized Packets	Conflicts
Gi2/1	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
Gi2/2	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
Gi2/3	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0

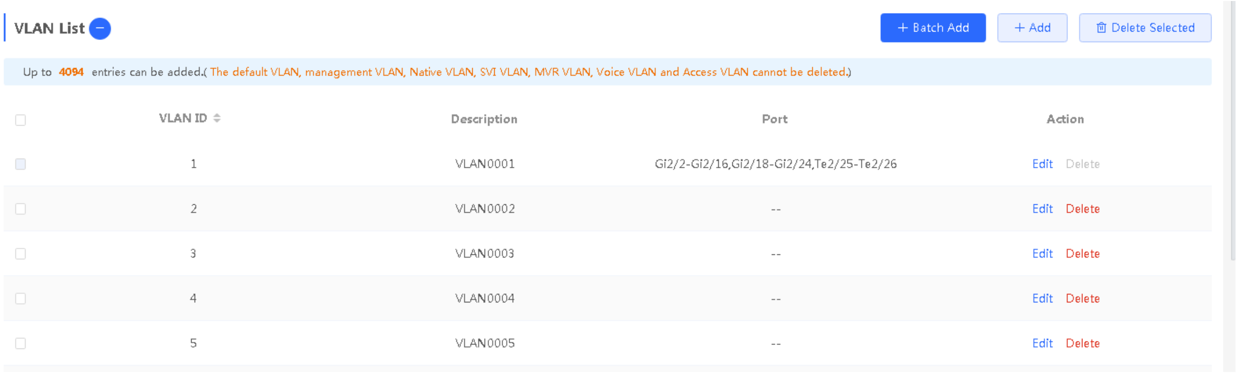
3.2 VLAN

A virtual local area network (VLAN) is a logical network created on a physical network. A VLAN has the same properties as a normal physical network except that it is not limited by its physical location. Each VLAN has an independent broadcast domain. Different VLANs are L2-isolated. L2 unicast, broadcast, and multicast frames are forwarded and spread within one VLAN and will not be transmitted to other VLANs.

When a port is defined as a member of a VLAN, all clients connected to the port are a part of the VLAN. A network supports multiple VLANs. VLANs can make L3 communication with each other through L3 devices or L3 interfaces.

In the Eweb management system, the VLAN module includes **VLAN List** (creating, deleting, and editing VLANs) and **Port List** (binding VLANs to ports).

3.2.1 VLAN List



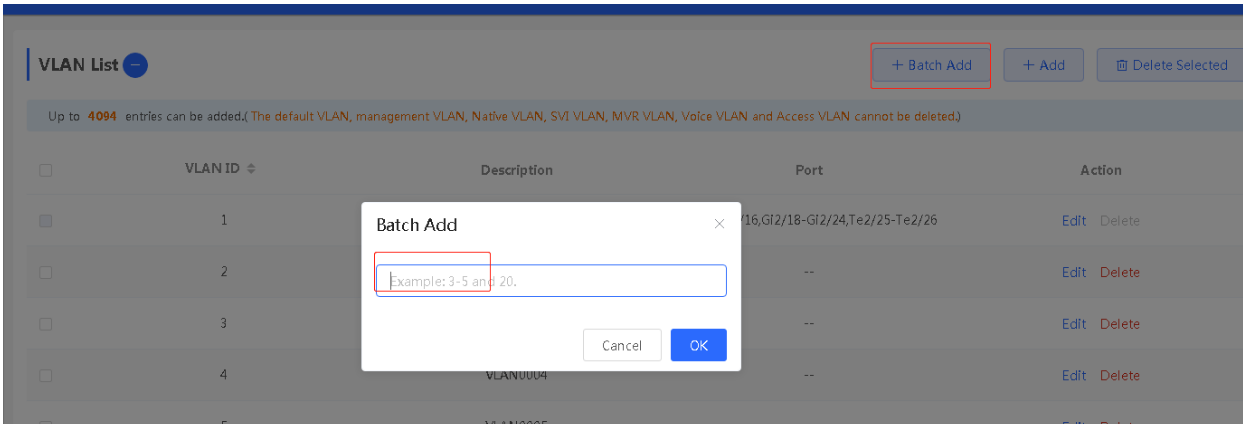
VLAN List

Up to 4094 entries can be added.(The default VLAN, management VLAN, Native VLAN, SVI VLAN, MVR VLAN, Voice VLAN and Access VLAN cannot be deleted.)

□	VLAN ID	Description	Port	Action
□	1	VLAN0001	Gi2/2-Gi2/16,Gi2/18-Gi2/24,Te2/25-Te2/26	Edit Delete
□	2	VLAN0002	--	Edit Delete
□	3	VLAN0003	--	Edit Delete
□	4	VLAN0004	--	Edit Delete
□	5	VLAN0005	--	Edit Delete

➢ **Adding a VLAN**

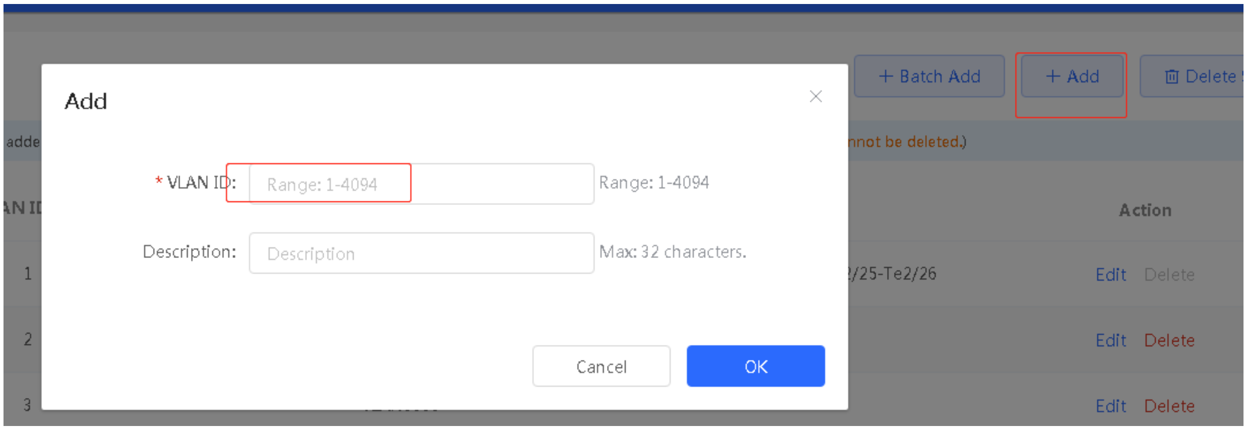
Method 1: Click **Batch Add**. In the displayed dialog box, enter a single VLAN ID or a VLAN ID range (separate multiple VLAN ID ranges with commas (,)), and click **OK**. After a VLAN is added successfully, it is displayed in **VLAN List**.



Up to 4094 entries can be added.(The default VLAN, management VLAN, Native VLAN, SVI VLAN, MVR VLAN, Voice VLAN and Access VLAN cannot be deleted.)

VLAN ID	Description	Port	Action
1		/16,Gi2/18-Gi2/24,Te2/25-Te2/26	Edit Delete
2		--	Edit Delete
3		--	Edit Delete
4	VLAN0004	--	Edit Delete

Method 2: Click **Add**. In the displayed dialog box, enter the VLAN ID (required) and VLAN description and click **OK**. After a VLAN is added successfully, it is displayed in **VLAN List**.

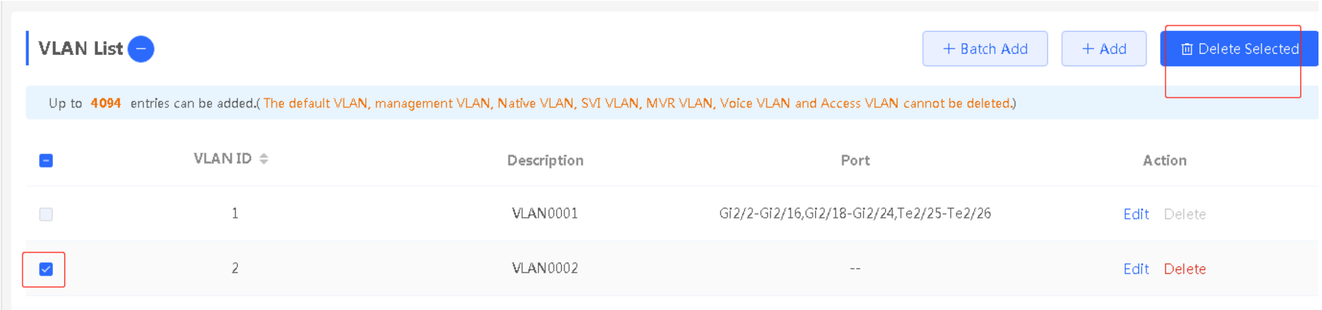


* VLAN ID: Range: 1-4094 Range: 1-4094

Description: Description Max: 32 characters.

Deleting a VLAN

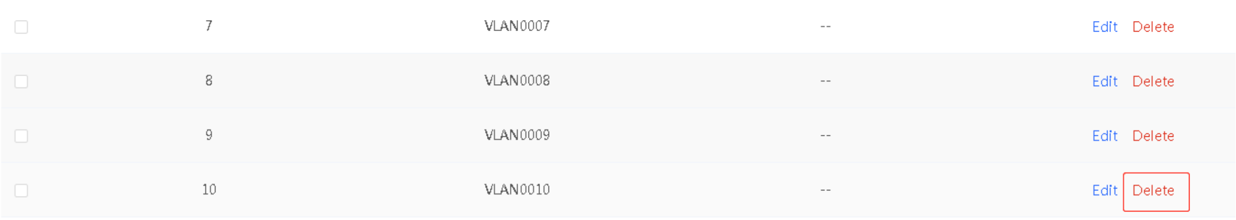
Method 1: In **VLAN List**, select multiple records and click **Delete Selected** to delete multiple VLAN records.



Up to 4094 entries can be added.(The default VLAN, management VLAN, Native VLAN, SVI VLAN, MVR VLAN, Voice VLAN and Access VLAN cannot be deleted.)

	VLAN ID	Description	Port	Action
□	1	VLAN0001	Gi2/2-Gi2/16,Gi2/18-Gi2/24,Te2/25-Te2/26	Edit Delete
☑	2	VLAN0002	--	Edit Delete

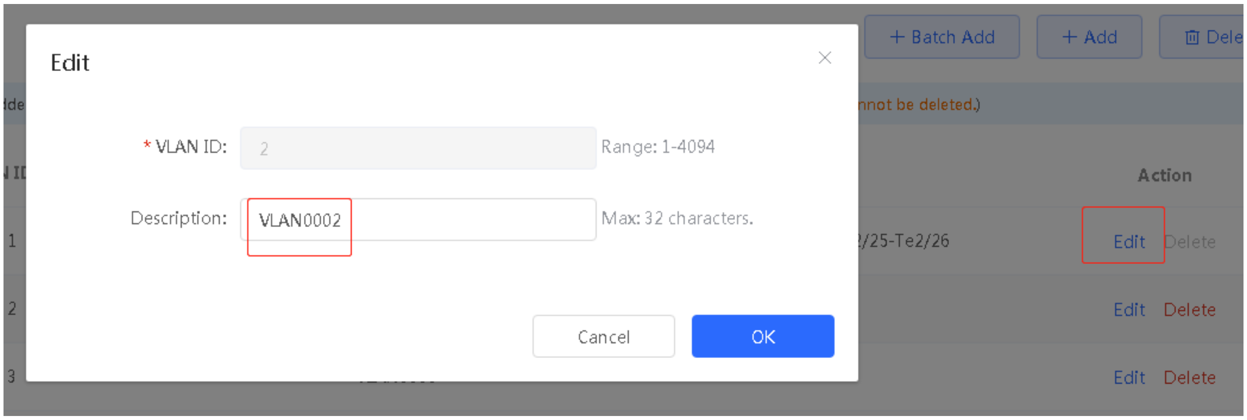
Method 2: In **VLAN List**, click **Delete** in the last **Action** column. In the displayed dialog box, click **OK**. The prompt "Delete operation succeeded." is displayed, indicating deletion completion.



□	7	VLAN0007	--	Edit Delete
□	8	VLAN0008	--	Edit Delete
□	9	VLAN0009	--	Edit Delete
□	10	VLAN0010	--	Edit Delete

➢ Editing a VLAN

In **VLAN List**, click **Edit** in the last **Action** column. In the displayed dialog box, you can modify the VLAN description and click **OK**. The prompt "Edit operation succeeded." is displayed, indicating editing completion.



Edit

* VLAN ID: 2 Range: 1-4094

Description: VLAN0002 Max: 32 characters.

Note

1. The range of a VLAN ID is from 1 to 4094.
2. The default VLAN (VLAN 1), management VLAN, native VLAN, and access VLAN cannot be deleted. For these VLANs, the **Delete** button is unavailable.
3. You can separate multiple VLANs to be added in batches with commas (,), and separate the start and end VLAN IDs of a VLAN range with a hyphen (-).
4. If no VLAN description is configured when the VLAN is added, the system automatically creates a VLAN description in the specified format, for example, VLAN000XX. The VLAN descriptions of different VLANs must be unique.
5. If there are too many VLANs, it may take a longer time to load the VLAN list page.
6. If the device supports L3 functions, VLANs, routed ports, and L3 aggregate ports (L3APs) share limited hardware resources. If resources are insufficient for VLAN creation, a message indicating resource insufficiency for VLAN creation will be displayed.

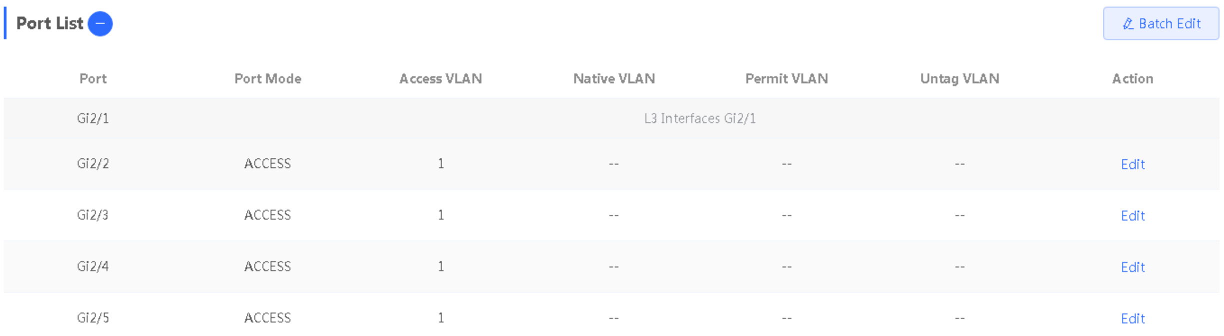
3.2.2 Port List

You can configure the VLAN member type for a port to determine the type of frames that are allowed to pass through the port and the number of VLANs, to which the port can belong. For details about VLAN member types, see Table **3-1 VLAN Types**.

Table 3-1 VLAN Types

Port Type	Description
Access port	One access port can belong to only one VLAN and allow only frames from this VLAN to pass through. This VLAN is called an access VLAN.
Trunk port (IEEE 802.1Q)	One trunk port supports one native VLAN and several allowed VLANs. Native VLAN frames forwarded by a trunk port do not carry tags while allowed VLAN frames forwarded by the trunk port carry tags. A trunk port belongs to all VLANs of the device by default, and can forward frames of all VLANs. You can set the allowed VLAN list (allowed VLANs) to limit VLAN frames that can be forwarded.

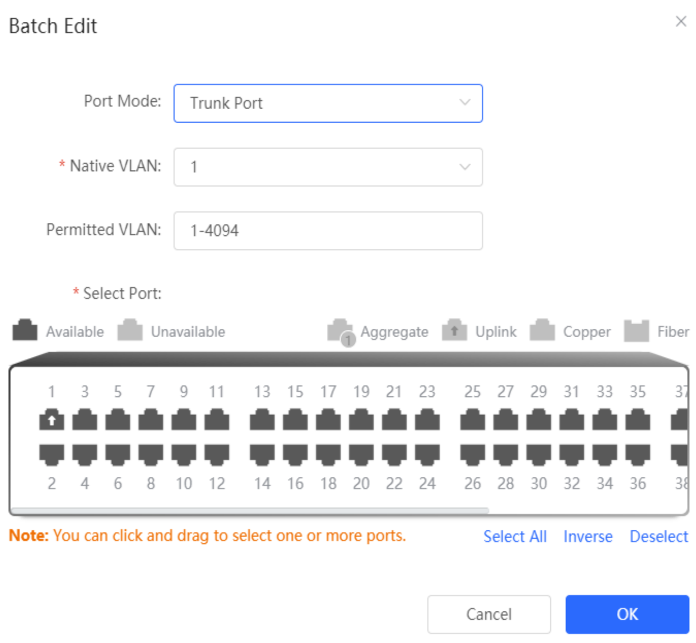
Mapping between ports and VLANs (you can configure ports in batches or configure a single port):



Port	Port Mode	Access VLAN	Native VLAN	Permit VLAN	Untag VLAN	Action
Gi2/1	L3 Interfaces Gi2/1					
Gi2/2	ACCESS	1	--	--	--	Edit
Gi2/3	ACCESS	1	--	--	--	Edit
Gi2/4	ACCESS	1	--	--	--	Edit
Gi2/5	ACCESS	1	--	--	--	Edit

➢ **Setting and Editing a Port VLAN**

Method 1: Click **Batch Edit**. A dialog box as shown in the figure below pops up. Select the port to be configured and set the port mode. If the port is configured to work in access mode, configure an access VLAN. If the port is configured to work in trunk mode, configure the native VLAN and allowed VLANs. Click **OK**.



Batch Edit

Port Mode: Trunk Port

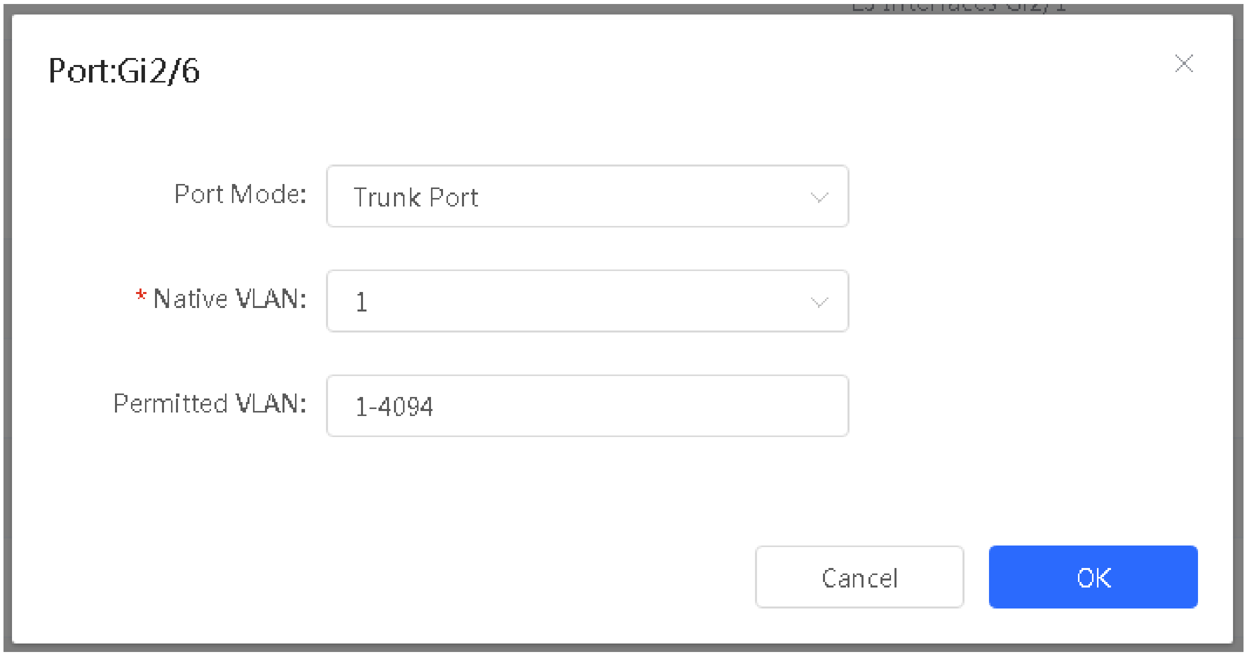
* Native VLAN: 1

Permitted VLAN: 1-4094

* Select Port:

Note: You can click and drag to select one or more ports.

Method 2: In **Port List**, click **Edit** in the last Action column of a specified port, configure the port mode and corresponding VLAN, and click **OK**.



Port:Gi2/6

Port Mode: Trunk Port

* Native VLAN: 1

Permitted VLAN: 1-4094

Note

1. VLANs supported by the product comply with the IEEE 802.1Q standard. The device supports a maximum of 4094 VLANs (VLAN IDs 1–4094). VLAN 1 is the default VLAN and cannot be deleted.

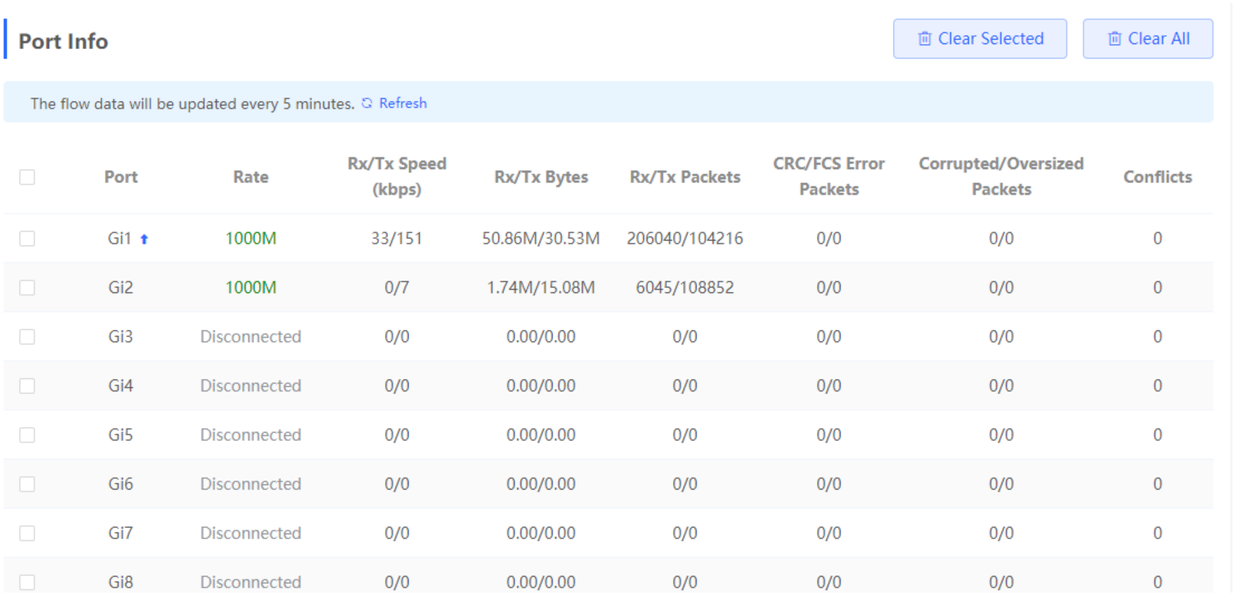
2. The range of an allowed VLAN is from 1 to 4094.

3. When hardware resources are insufficient, the system displays a VLAN creation failure message.
4. Improper configuration of VLANs on a port (especially uplink port) may cause the failure to log in to the Eweb management system. Therefore, exercise caution when configuring VLANs.

3.3 Monitor

3.3.1 Port Info

The **Port Info** page displays traffic data and other data of device ports.



Port Info

The flow data will be updated every 5 minutes. Refresh

□	Port	Rate	Rx/Tx Speed (kbps)	Rx/Tx Bytes	Rx/Tx Packets	CRC/FCS Error Packets	Corrupted/Oversized Packets	Conflicts
□	Gi1 ↑	1000M	33/151	50.86M/30.53M	206040/104216	0/0	0/0	0
□	Gi2	1000M	0/7	1.74M/15.08M	6045/108852	0/0	0/0	0
□	Gi3	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
□	Gi4	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
□	Gi5	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
□	Gi6	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
□	Gi7	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
□	Gi8	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0

Select a port and click **Clear Selected**, or click **Clear All** to clear statistics such as current port traffic and start statistics collection again.

Note

1. Data in the **Rate** column is updated every five seconds. Other traffic statistics are updated every five minutes.
2. Aggregate ports can be configured. Traffic of an aggregate port is the sum of traffic of all member ports.

3.3.2 Clients

1. Overview

The MAC address table records the MAC addresses, interface IDs, and VLAN IDs of the devices connected to the switch.

When forwarding a packet, the device searches for the output port in the MAC address table based on the destination MAC address and VLAN ID of the packet. After finding the output port based on the MAC address, the device forwards the packet in unicast, multicast, or broadcast mode.

Note

This section only involves the management of dynamic and static addresses and filtered addresses. For the management of multicast addresses, see 3.5.3 IGMP Snooping.

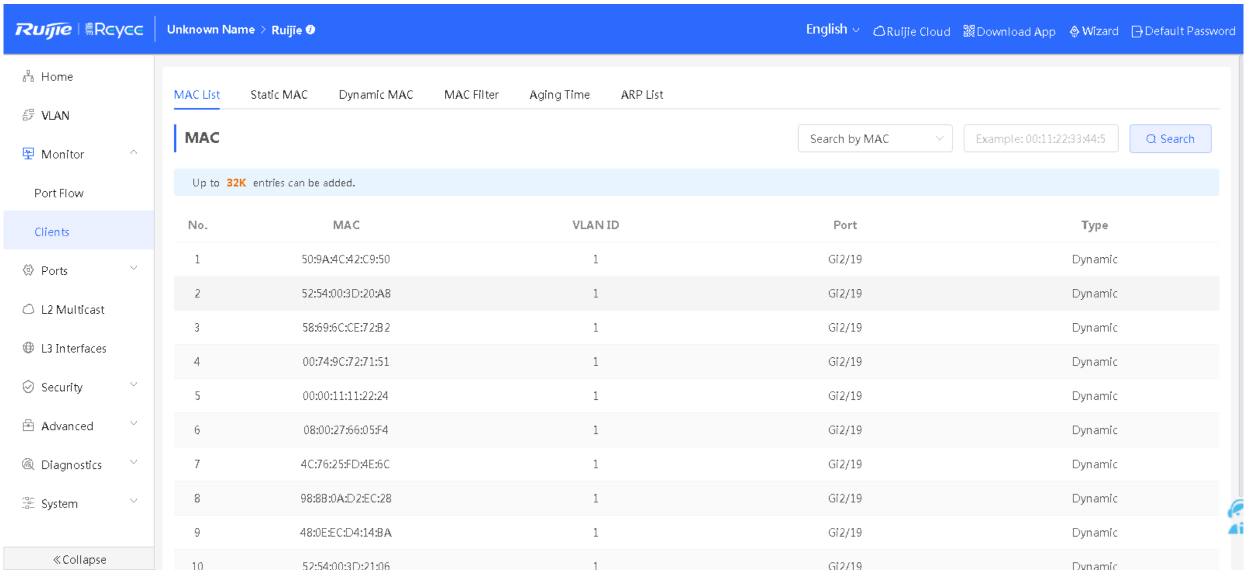
Table 3-2 Application Scenarios of MAC Addresses

Function	Application Scenario
Dynamic address learning	Packets are forwarded in unicast mode through dynamic address learning.
MAC address change notification	MAC address adding and deletion notifications are used to monitor changes of users connected to the network device.

Client management includes **MAC List**, **Static MAC**, **Dynamic MAC**, **MAC Filter**, **Aging Time**, and **ARP List**.

2. MAC List

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



MAC

Search by MAC

Example: 00:11:22:33:44:5

Up to 32K entries can be added.

No.	MAC	VLAN ID	Port	Type
1	50:9A:4C:42:C9:50	1	Gi2/19	Dynamic
2	52:54:00:3D:20:A8	1	Gi2/19	Dynamic
3	58:69:6C:CE:72:B2	1	Gi2/19	Dynamic
4	00:74:9C:72:71:51	1	Gi2/19	Dynamic
5	00:00:11:11:22:24	1	Gi2/19	Dynamic
6	08:00:27:66:05:F4	1	Gi2/19	Dynamic
7	4C:76:25:FD:4E:6C	1	Gi2/19	Dynamic
8	98:8B:0A:D2:EC:28	1	Gi2/19	Dynamic
9	48:0E:EC:D4:14:BA	1	Gi2/19	Dynamic
10	52:54:00:3D:21:06	1	Gi2/19	Dynamic

- **Search**

Select the search type (by MAC address, by VLAN, or by port), enter the search string, and click **Search**. Then, the list displays MAC address entries that meet search criteria.

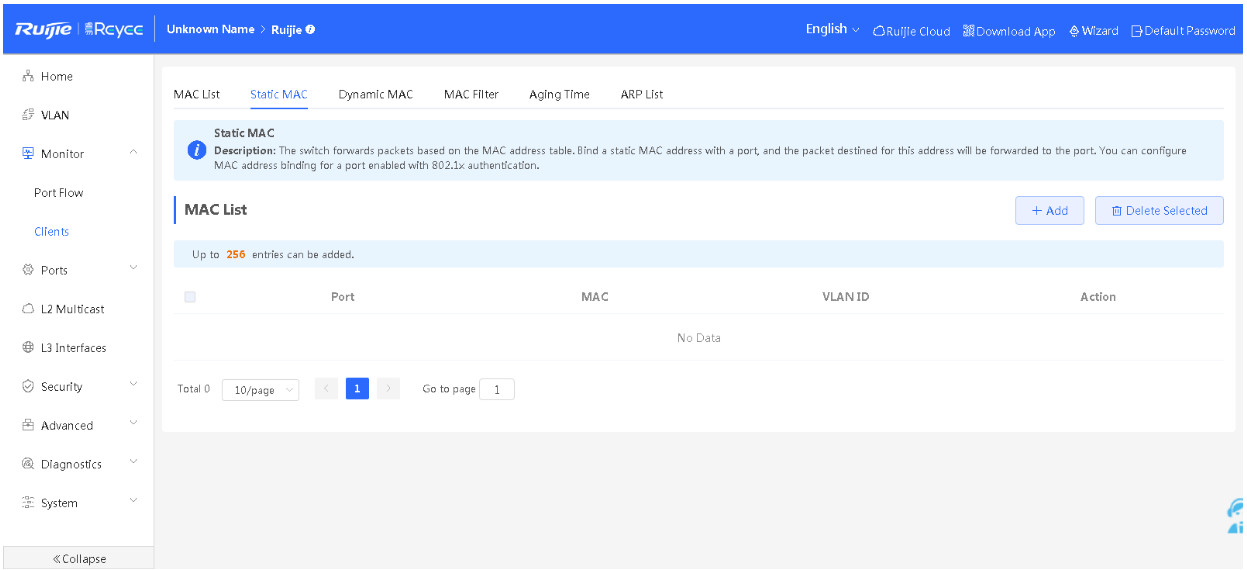
Note

1. The MAC address entry capacity varies with the device, for example, the MAC address entry capacity of the device shown in the figure above is 32K.
2. The search function supports fuzzy search.

3. Static MAC

The switch forwards data according to the MAC address table. You can manually bind the MAC address of a downlink network device connected to a port of the device with the port of the device to set a static MAC address. After a static address is configured, when the device receives a packet destined to this address from the VLAN, it forwards the packet to the specified port. If IEEE 802.1x authentication is enabled on the port, you can configure MAC address binding to implement authentication exemption.

You can check and manually configure the mappings between MAC addresses of network devices and ports.



Static MAC

Description: 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.

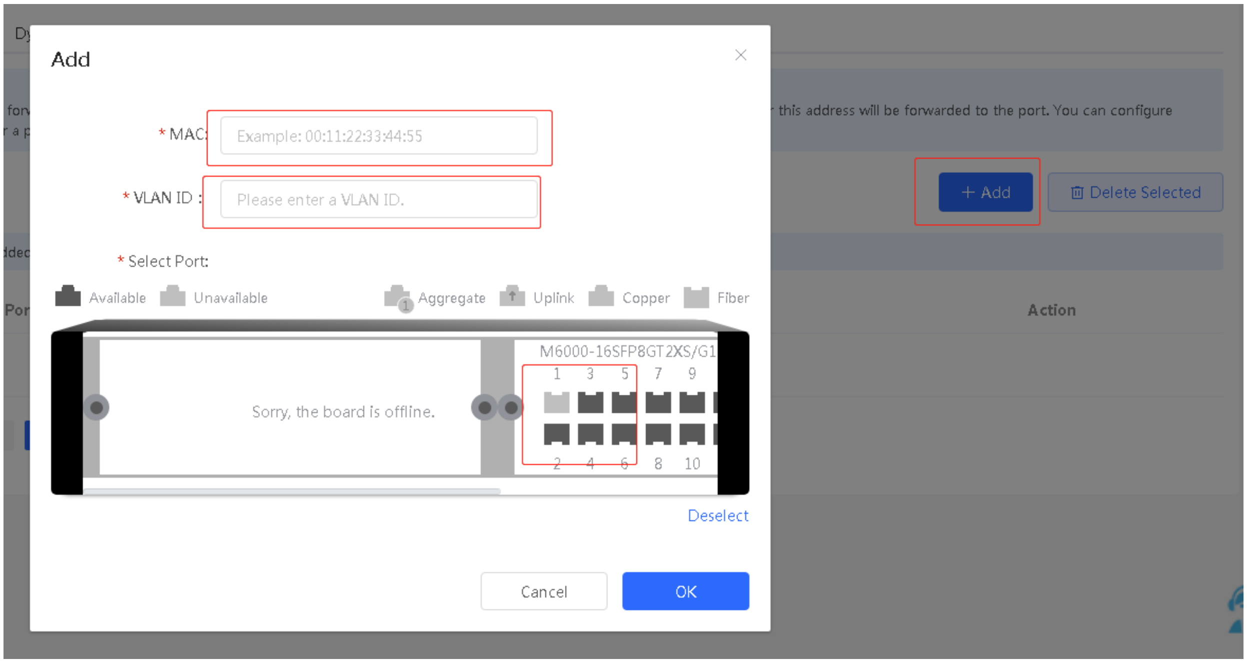
MAC List

Up to 256 entries can be added.

	Port	MAC	VLAN ID	Action
No Data				

➢ Adding a Static Address

Click **Add**. In the displayed dialog box, enter the MAC address and VLAN ID, select the port for packet forwarding, and click **OK**. If the static address is added successfully, the message "Add operation succeeded" is displayed and the list is updated.


Add
* MAC: Example: 00:11:22:33:44:55
* VLAN ID : Please enter a VLAN ID.
* Select Port:
Available
Unavailable
Aggregate
Uplink
Copper
Fiber
M6000-16SFP8GT2XS/G1
1 3 5 7 9
2 4 6 8 10
Sorry, the board is offline.
Deselect
Cancel
OK
+ Add
Delete Selected
this address will be forwarded to the port. You can configure
Action

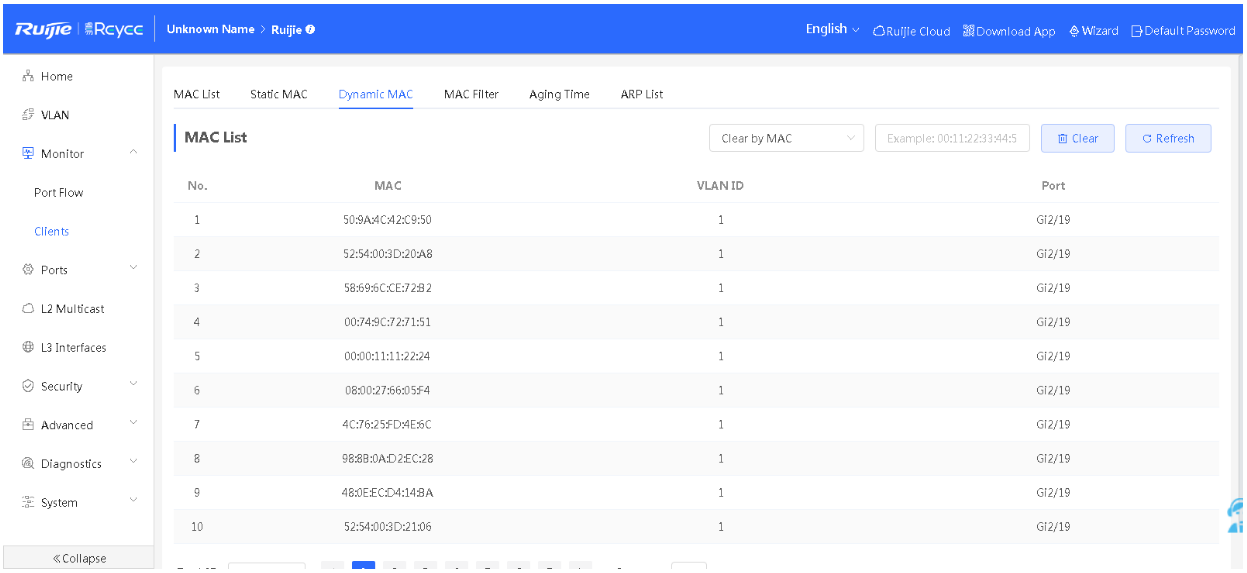
➢ Deleting a Static Address

Method 1: In **MAC List**, select the MAC address entry to be deleted and click **Delete Selected**. In the confirmation dialog box, click **OK**. A deletion success message is displayed and the list is updated.

Method 2: In **MAC List**, click **Delete** in the last **Action** column. The prompt "Are you sure you want to delete the entry?" is displayed. Click **OK** to complete the deletion.

4. Dynamic MAC

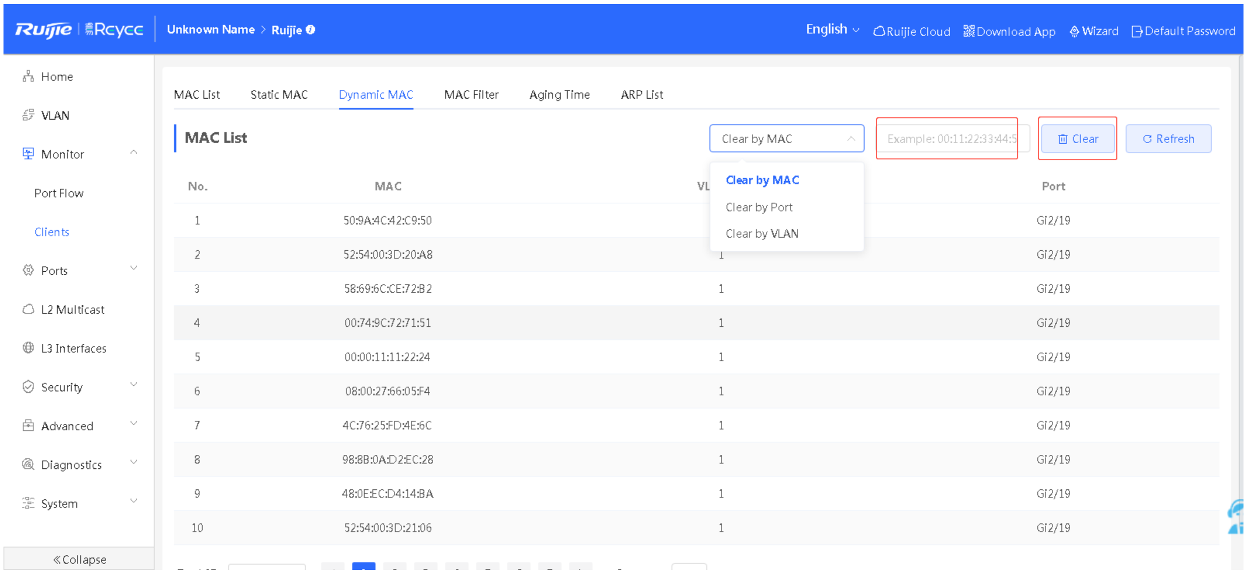
The **Dynamic MAC** page displays dynamic MAC addresses learned by the device.



No.	MAC	VLAN ID	Port
1	50:9A:4C:42:C9:50	1	Gi2/19
2	52:54:00:3D:20:A8	1	Gi2/19
3	58:69:6C:CE:72:B2	1	Gi2/19
4	00:74:9C:72:71:51	1	Gi2/19
5	00:00:11:11:22:24	1	Gi2/19
6	08:00:27:66:05:F4	1	Gi2/19
7	4C:76:25:FD:4E:6C	1	Gi2/19
8	98:8B:0A:D2:EC:28	1	Gi2/19
9	48:0E:EC:D4:14:BA	1	Gi2/19
10	52:54:00:3D:21:06	1	Gi2/19

➢ Clear

Select the clear type (by MAC address, by VLAN, or by port), enter a string for matching the dynamic MAC address entry, and click **Clear**. The device will clear MAC address entries that meet the conditions.



No.	MAC	VL	Port
1	50:9A:4C:42:C9:50		Gi2/19
2	52:54:00:3D:20:A8	1	Gi2/19
3	58:69:6C:CE:72:B2	1	Gi2/19
4	00:74:9C:72:71:51	1	Gi2/19
5	00:00:11:11:22:24	1	Gi2/19
6	08:00:27:66:05:F4	1	Gi2/19
7	4C:76:25:FD:4E:6C	1	Gi2/19
8	98:8B:0A:D2:EC:28	1	Gi2/19
9	48:0E:EC:D4:14:BA	1	Gi2/19
10	52:54:00:3D:21:06	1	Gi2/19

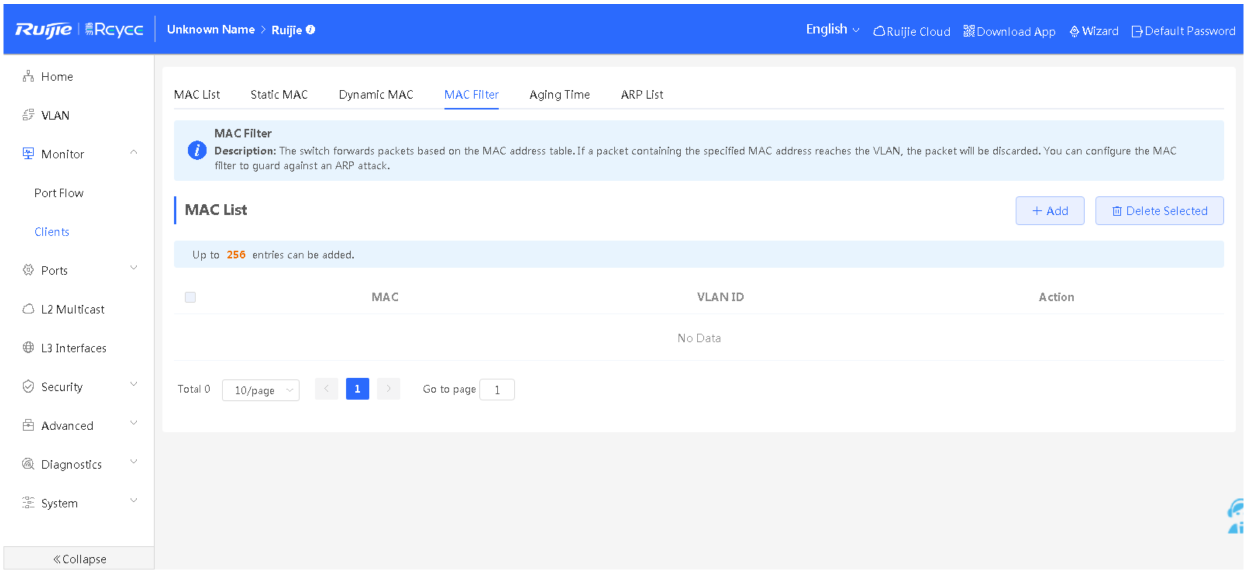
➢ Refresh

Click **Refresh** to obtain the latest dynamic MAC address entries.

5. MAC Filter

The switch forwards data according to the MAC address table. When receiving a packet with its source address or destination address being the configured filtered MAC address in the configured VLAN, the switch discards the packet.

You can manually configure the binding between the MAC address of a connected network device and the VLAN of the device to filter out the packets that match the binding. For example, if a user initiates ARP attacks, the MAC address of the user can be configured as a filtered address to prevent attacks.



MAC Filter

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

MAC List

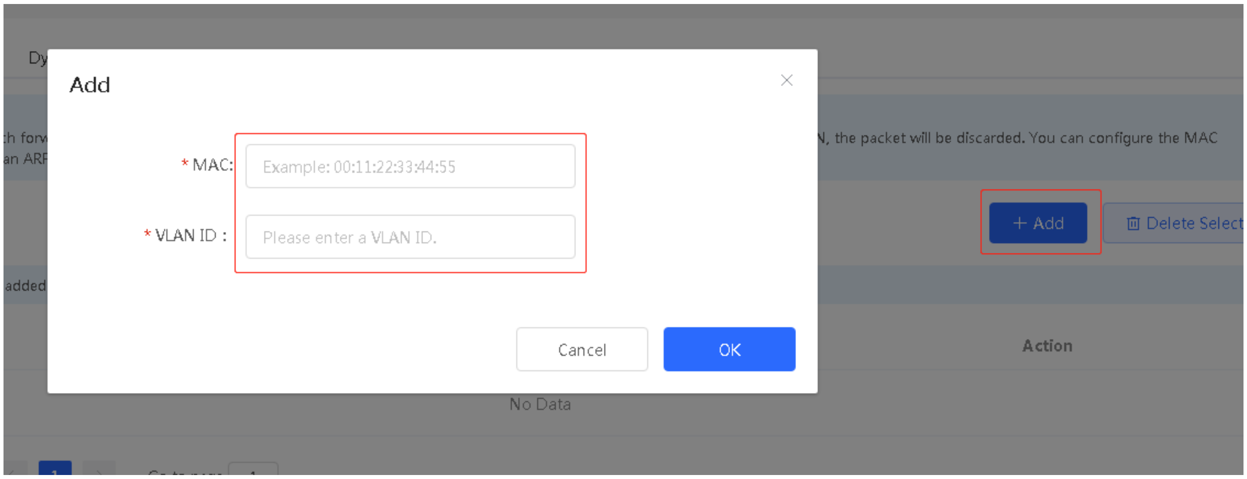
Up to 256 entries can be added.

□	MAC	VLAN ID	Action
		No Data	

Total 0 10/page 1 Go to page 1

➢ Adding a Filtered Address

Click **Add**. In the displayed dialog box, enter a MAC address and VLAN, and click **OK**.


Add
* MAC:
Example: 00:11:22:33:44:55
* VLAN ID :
Please enter a VLAN ID.
Cancel
OK
N, the packet will be discarded. You can configure the MAC
+ Add
Delete Select
Action
No Data

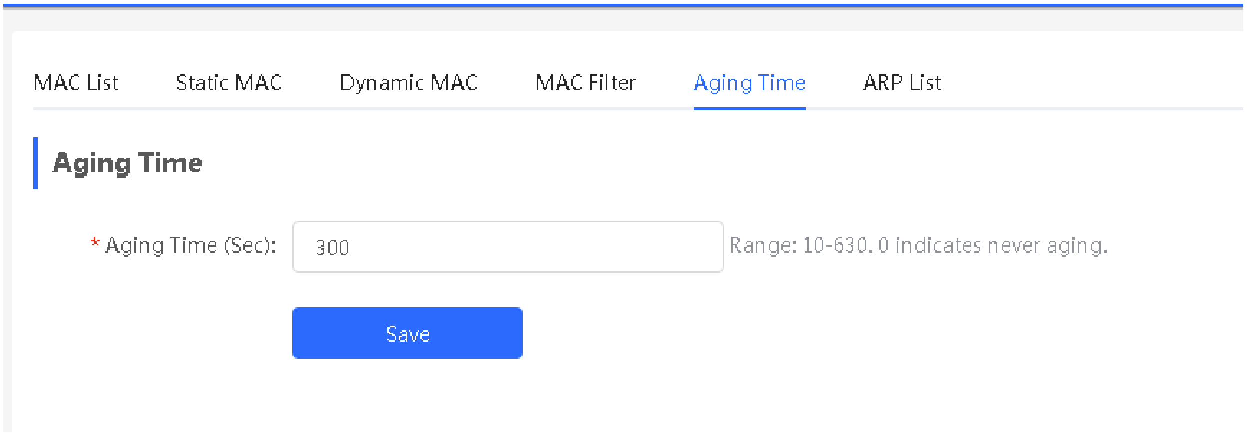
- **Deleting a Filtered Address**

Method 1: In **MAC List**, select the MAC address entry to be deleted and click **Delete Selected**. In the confirmation dialog box, click **OK**.

Method 2: In **MAC List**, click **Delete** in the last **Action** column. In the displayed dialog box, click **OK**.

6. Aging Time

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



* Aging Time (Sec): 300 Range: 10-630. 0 indicates never aging.

- **Configuring Aging Time**

Enter valid aging time and click **Save**. The message "Operation succeeded" is displayed, indicating that the aging time of MAC address entries of the device is successfully modified.

Note

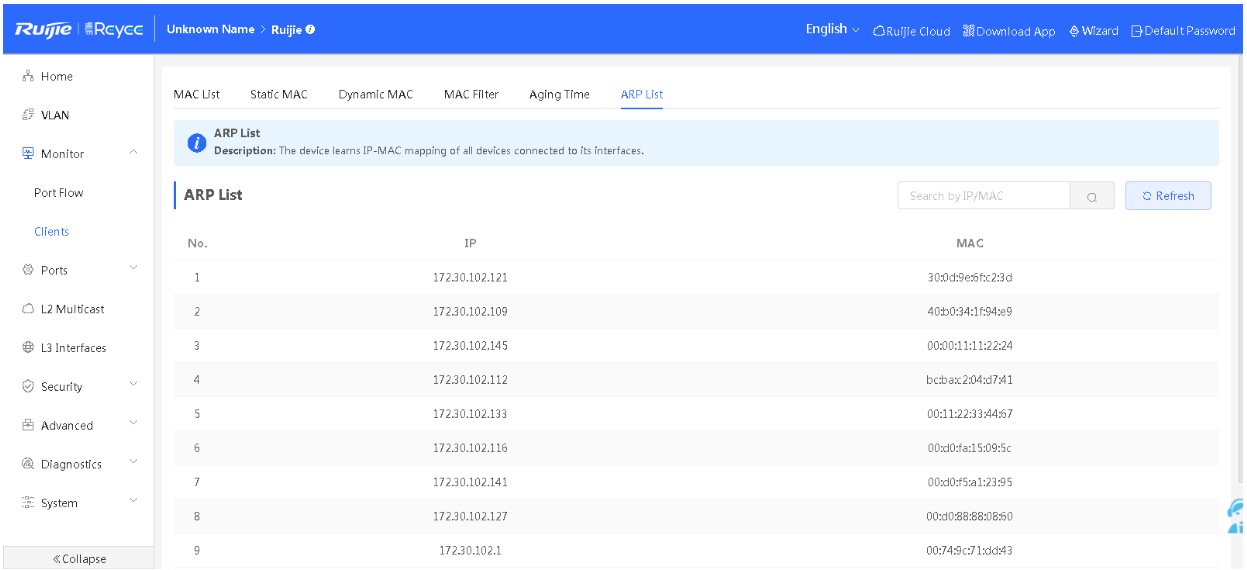
The aging time ranges from 10 to 630, in seconds. The value **0** indicates no aging.

7. ARP List

When two IP-based devices need to communicate with each other, the sender must know the IP address and MAC address of the peer. With MAC addresses, an IP-based device can encapsulate link-layer frames and then send data frames to the physical network. The process of obtaining MAC addresses based on IP addresses is called address resolution.

The Address Resolution Protocol (ARP) is used to resolve IP addresses into MAC addresses. ARP can obtain the MAC Address associated with an IP address. ARP stores the mappings between IP addresses and MAC addresses in the ARP cache of the device. By default, the IP and ARP protocols on the Ethernet use the Ethernet II frame structure to encapsulate frames.

The device learns the IP and MAC addresses of the network devices connected to ports of the device and generates ARP entries. The **ARP List** page displays ARP entries learned by the device.



ARP List

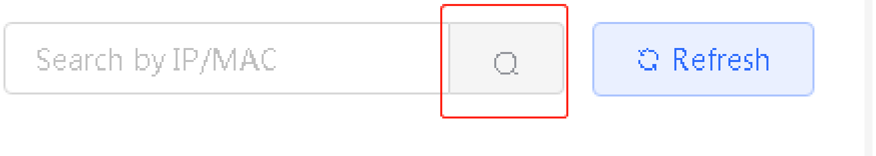
Description: The device learns IP-MAC mapping of all devices connected to its interfaces.

ARP List

No.	IP	MAC
1	172.30.102.121	30:0d:9e:6f:c2:3d
2	172.30.102.109	40:b0:34:1f:94:e9
3	172.30.102.145	00:00:11:11:22:24
4	172.30.102.112	bc:ba:c2:04:d7:41
5	172.30.102.133	00:11:22:33:44:67
6	172.30.102.116	00:d0:fa:15:09:5c
7	172.30.102.141	00:d0:f5:a1:23:95
8	172.30.102.127	00:d0:88:88:08:60
9	172.30.102.1	00:74:9c:71:dd:43

➢ **Search**

The ARP list allows you search for specified ARP entries by IP or MAC address.



- **Refresh**

Click **Refresh** to obtain the latest ARP entries.

3.4 Port Management

3.4.1 Overview

Interfaces are important components for data exchange on network devices. The device supports physical interfaces and logical interfaces. Physical interfaces are physical hardware interfaces on the device, such as 100M Ethernet interfaces and GE interfaces. Although a logical interface does not have a physical hardware interface, it can be associated with or independent of a physical interface, such as the loopback interface and tunnel interfaces. For network protocols, physical and logical interfaces provide the same processing.

The **Ports** module allows you to configure basic settings for ports, and configure link aggregation, switched port analyzer (SPAN), port rate limiting, management IP address, and chassis management IP address (for devices providing the MGMT port), and power over Ethernet (PoE) (for devices supporting the PoE function).

3.4.2 Interface Type

Table 3-3 Description of Interface Types

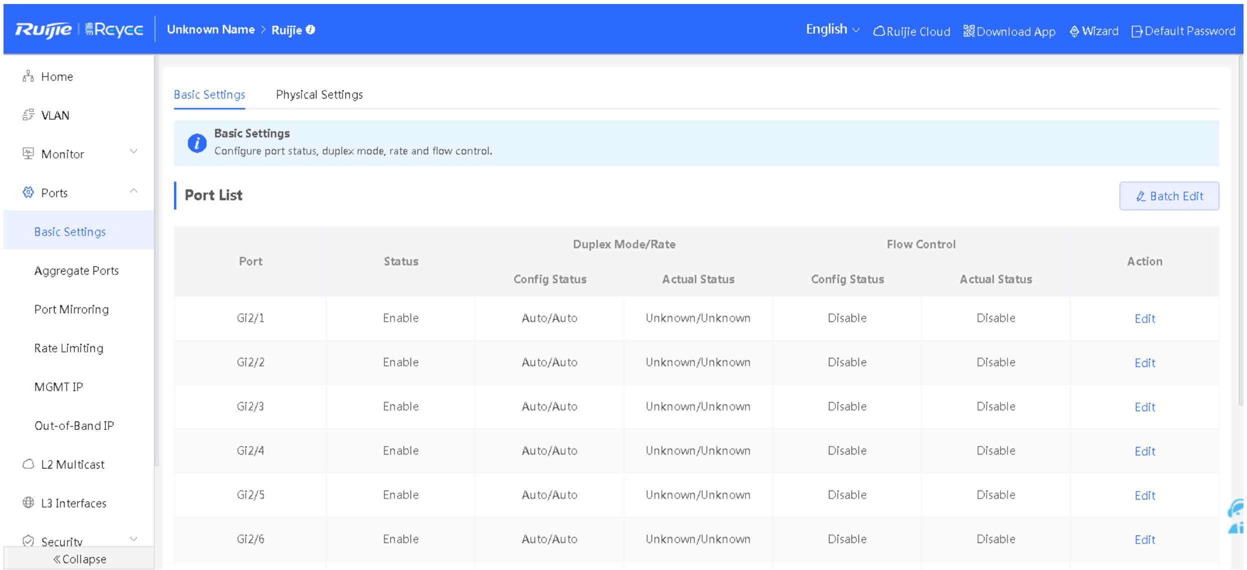
Interface Type	Description	Remarks
Switch port	A switch port consists of a single physical port on the device and provides only the L2 switching function. Switch ports are used to manage physical interfaces and their associated L2 protocols.	Described in this section
L2 aggregate port	An aggregate port is a combination of multiple physical member ports. Several physical links can be bound together to form a simple logical link, which is called an aggregate port. For L2 switching, an aggregate port is like a high-bandwidth switch port. It can combine the bandwidths of multiple ports to expand link bandwidth. In addition, for frames sent through an L2 aggregate port, load balancing is performed on member ports of the L2 aggregate port. If one member link of the aggregate port fails, the L2 aggregate port automatically transfers traffic on this link to other available member links, improving connection reliability.	Described in this section
SVI	A switch virtual interface (SVI) serves as the management interface of the device. Administrators can manage the device through this interface. You can also create an SVI as a gateway interface, which is equivalent to the virtual interface of each VLAN and can be used for inter-VLAN routing on L3 devices.	For details, see 3.6 L3 Management.
Routed port	On L3 devices, you can configure a single physical port as a routed port and use it as the gateway interface of L3 switching. A routed port is not associated with a particular VLAN but acts as an access port. Routed ports do not support the L2 switching function.	For details, see 3.6 L3 Management.

Interface Type	Description	Remarks
L3 aggregate port	An L3 aggregate port is a logical aggregate port group composed of multiple physical member ports, just like an L2 aggregate port. The ports to be aggregated must be L3 interfaces of the same type. An aggregate port serves as the gateway interface of L3 switching. It treats multiple physical links in the same aggregate group as one logical link. It is an important way to expand link bandwidth. In addition, frames sent through an L3 aggregate port can also be load-balanced among member ports of the L3 aggregate port. If one member link of the aggregate port fails, the L3 aggregate port automatically transfers traffic on this link to other available member links, improving connection reliability. L3 aggregate ports do not support the L2 switching function.	For details, see 3.6 L3 Management.

3.4.3 Port Settings

Port settings include the port enabling status, duplex mode, flow control configuration, physical settings of ports, and other basic configuration. You can adjust the interface rate, duplex mode, flow control mode, and auto-negotiation factor mode.

1. Basic Settings



Basic Settings
Configure port status, duplex mode, rate and flow control.

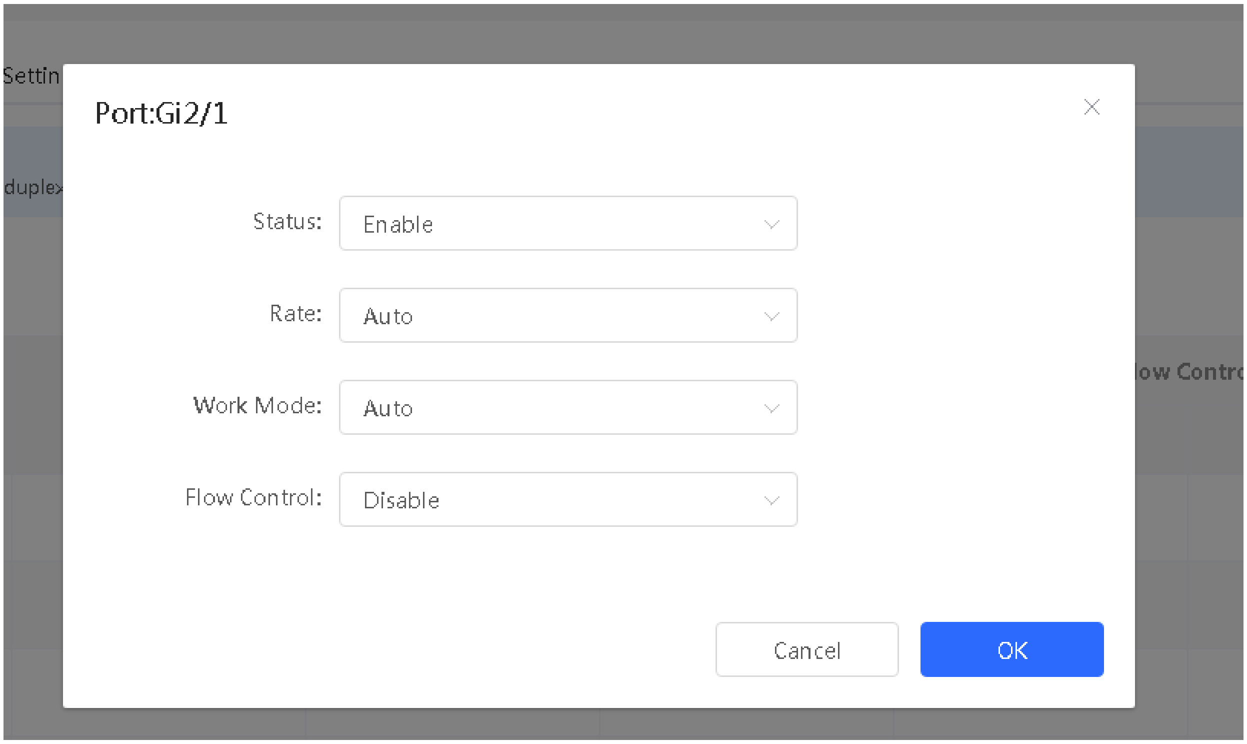
Port List

Port	Status	Duplex Mode/Rate		Flow Control		Action
		Config Status	Actual Status	Config Status	Actual Status	
Gi2/1	Enable	Auto/Auto	Unknown/Unknown	Disable	Disable	Edit
Gi2/2	Enable	Auto/Auto	Unknown/Unknown	Disable	Disable	Edit
Gi2/3	Enable	Auto/Auto	Unknown/Unknown	Disable	Disable	Edit
Gi2/4	Enable	Auto/Auto	Unknown/Unknown	Disable	Disable	Edit
Gi2/5	Enable	Auto/Auto	Unknown/Unknown	Disable	Disable	Edit
Gi2/6	Enable	Auto/Auto	Unknown/Unknown	Disable	Disable	Edit

➢ Editing a Port

Method 1: Click **Batch Edit**. In the displayed dialog box, select the port to be configured, configure the port status, rate, and mode, and click **OK** to deliver the configuration.

Method 2: In **Port List**, select an item and click **Edit** in the **Action** column. In the displayed dialog box, configure the port status, rate, and mode, and click **OK**.


Port:Gi2/1

Status: Enable

Rate: Auto

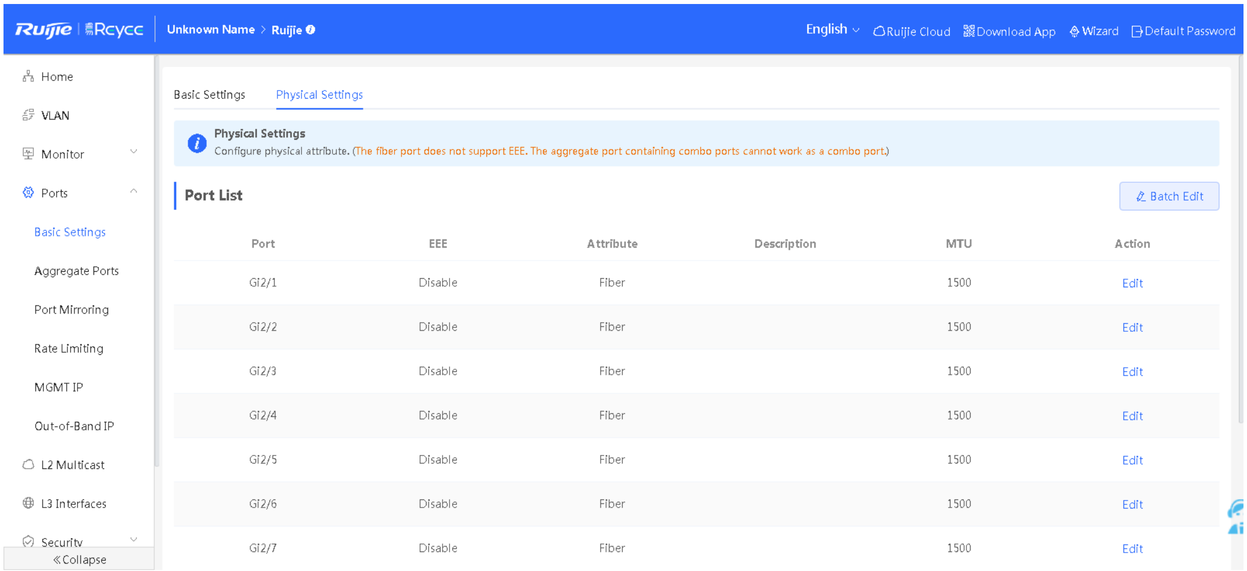
Work Mode: Auto

Flow Control: Disable

Note

1. The rate of a GE port can be set to 1000M, 100M, or auto. The rate of a 10G port can be set to 10G, 1000M, or auto.
2. In batch configuration, optional configuration items are a common collection of selected ports (that is, attributes supported the selected ports).

2. Physical Settings



Physical Settings

Configure physical attribute. (The fiber port does not support EEE. The aggregate port containing combo ports cannot work as a combo port.)

Port List

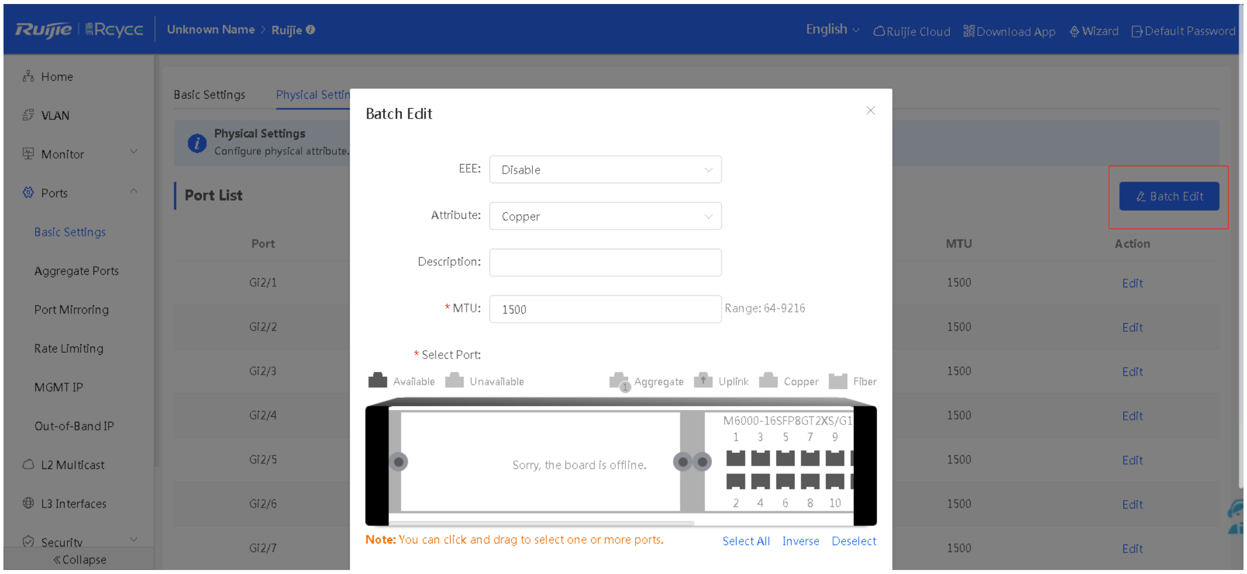
Port	EEE	Attribute	Description	MTU	Action
Gi2/1	Disable	Fiber		1500	Edit
Gi2/2	Disable	Fiber		1500	Edit
Gi2/3	Disable	Fiber		1500	Edit
Gi2/4	Disable	Fiber		1500	Edit
Gi2/5	Disable	Fiber		1500	Edit
Gi2/6	Disable	Fiber		1500	Edit
Gi2/7	Disable	Fiber		1500	Edit

➢ Setting Physical Information About a Port

Table 3-4 Description of Physical Configuration Parameters

Parameter	Description	Default Value
EEE	It is short for energy-efficient Ethernet, which is based on the standard IEEE 802.3az protocol. When no data is being transmitted, the low power idle (LPI) signal is sent through the MAC address to enable the PHY to enter the low power consumption mode. Value: Disable/Enable	Disable
Attribute	The port attribute indicates whether the port is a copper port or an SFP port. Coper port: copper mode (cannot be changed) SFP port: fiber mode (cannot be changed) Only SFP combo ports support mode change.	Depending on the port attribute
Description	You can add a description to label the functions of a port.	NA
MTU	The maximum transmission unit (MTU) is used to notify the peer of the acceptable maximum size of a data service unit. It indicates the size of the payload acceptable to the sender.	1500

Method 1: Click **Batch Edit**. In the displayed dialog box, select the port to be configured, configure the EEE switch, port mode, enter the port description and MTU size, and click **OK**.



Batch Edit

EEE: Disable

Attribute: Copper

Description:

* MTU: 1500 Range: 64-9216

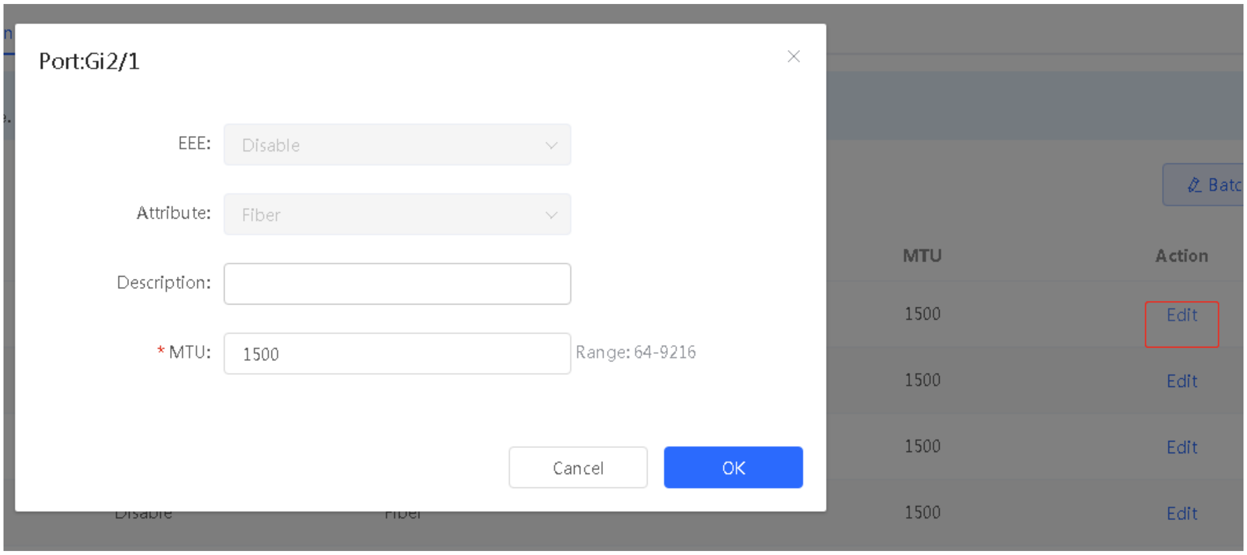
* Select Port:

Sorry, the board is offline.

Note: You can click and drag to select one or more ports.

Port	MTU	Action
Gi2/1	1500	Edit
Gi2/2	1500	Edit
Gi2/3	1500	Edit
Gi2/4	1500	Edit
Gi2/5	1500	Edit
Gi2/6	1500	Edit
Gi2/7	1500	Edit

Method 2: Click **Edit** in the **Action** column of the list. In the displayed configuration box, configure the EEE switch, port mode, enter the port description and MTU size, and click **OK**.



Port:Gi2/1

EEE: Disable

Attribute: Fiber

Description:

* MTU: 1500 Range: 64-9216

MTU	Action
1500	Edit
1500	Edit
1500	Edit
1500	Edit

Note

1. Different ports support different attributes and configuration items.

2. Only the SFP combo ports support port mode switching.
3. SFP ports do not support EEE configuration.
4. Copper ports and SFP ports cannot be both configured during batch configuration.

3.4.4 Aggregate Ports

1. Overview

An aggregate port (AP) is a logical link formed by binding multiple physical links. It is used to expand link bandwidth, thereby improving connection reliability.

The AP function supports load balancing and therefore, evenly distributes traffic to member links. The AP implements link backup. When a member link of an AP is disconnected, the system automatically distributes traffic of this link to other available member links. Broadcast or multicast packets received by one member link of an AP are not forwarded to other member links.

- If a single interface that connects two devices supports the maximum rate of 1000 Mbps (assume that interfaces of both devices support the rate of 1000 Mbps), when the service traffic on the link exceeds 1000 Mbps, the excess traffic will be discarded. Link aggregation can solve this problem. For example, use *n* network cables to connect the two devices and bind the interfaces together. In this way, the interfaces are logically bound to support the maximum traffic of 1000 Mbps × *n*.
- If two devices are connected through a single cable, when the link between the two interfaces is disconnected, services carried on this link are interrupted. After multiple interconnected interfaces are bound, as long as there is one link available, services carried on these interfaces will not be interrupted.

2. Working Principle

➢ **Static AP Mode**

In static AP mode, you can manually add a physical interface to an aggregate port. An aggregate port in static AP mode is called a static aggregate port and the member ports are called member ports of the static aggregate port. Static AP can be easily implemented. You can aggregate multiple physical links by running commands to add specified physical interfaces to an AP. Once a member interface is added to an AP, it can send and receive data and balance traffic in the AP.

➢ **Load Balancing**

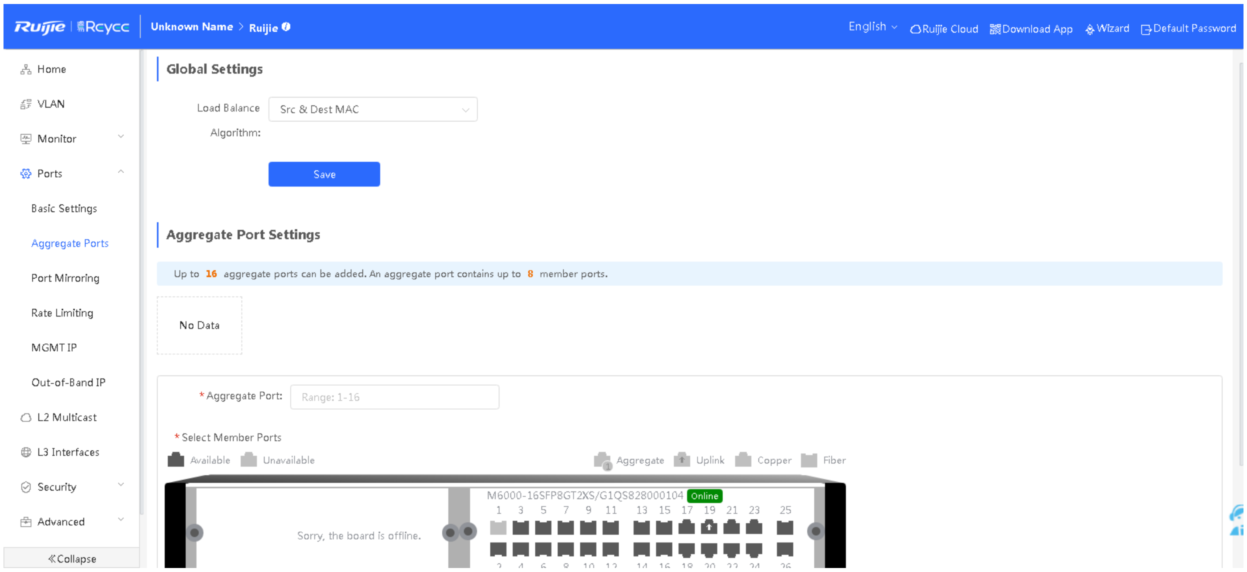
An AP, based on packet characteristics such as the source MAC address, destination MAC address, source IP address, destination IP address, L4 source port ID, and L4 destination port ID of packets received by an inbound interface, differentiates packet flows according to one or several combined algorithms. It sends the same packet flow through the same member link, and evenly distributes different packet flows among member links. For example, in load balancing mode based on source MAC addresses, packets are distributed to different member links of an AP based on their source MAC addresses. Packets with different source MAC addresses are distributed to different member links; packets with a same source MAC address are forwarded along a same member link.

Currently, the AP supports the traffic balancing modes based on the following:

- Source MAC address or destination MAC address
- Source MAC address + destination MAC address
- Source IP address or destination IP address
- Source IP address + destination IP address
- Source port
- L4 source port or L4 destination port
- L4 source port + L4 destination port

3. Configuration Steps

You can configure static APs and global load balancing algorithms for the APs.



Global Settings

Load Balance Algorithm: Src & Dest MAC

Aggregate Port Settings

Up to 16 aggregate ports can be added. An aggregate port contains up to 8 member ports.

No Data

* Aggregate Port: Range: 1-16

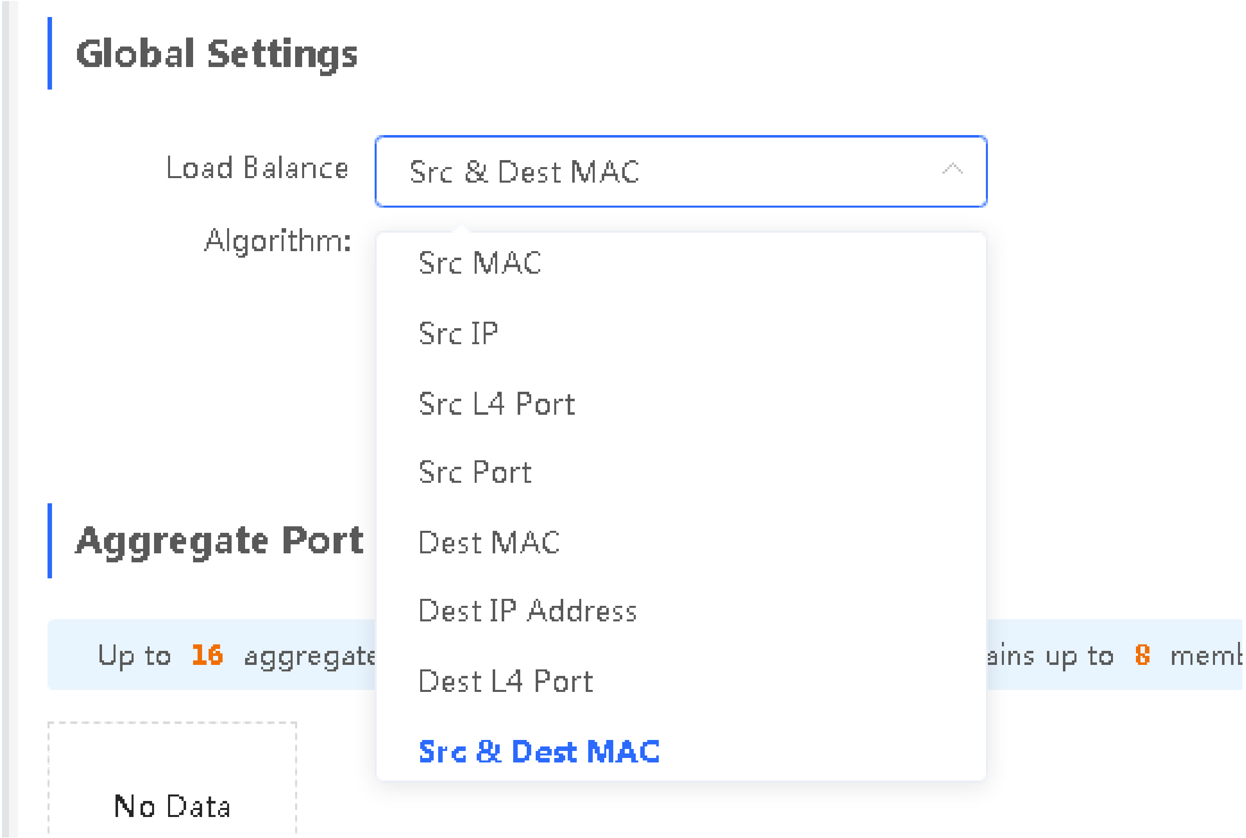
* Select Member Ports

Sorry, the board is offline.

M6000-16SFP8GT2XS/G1QS828000104 Online

- **Global Settings**

Select **Load Balance Algorithm** and click **Save**.

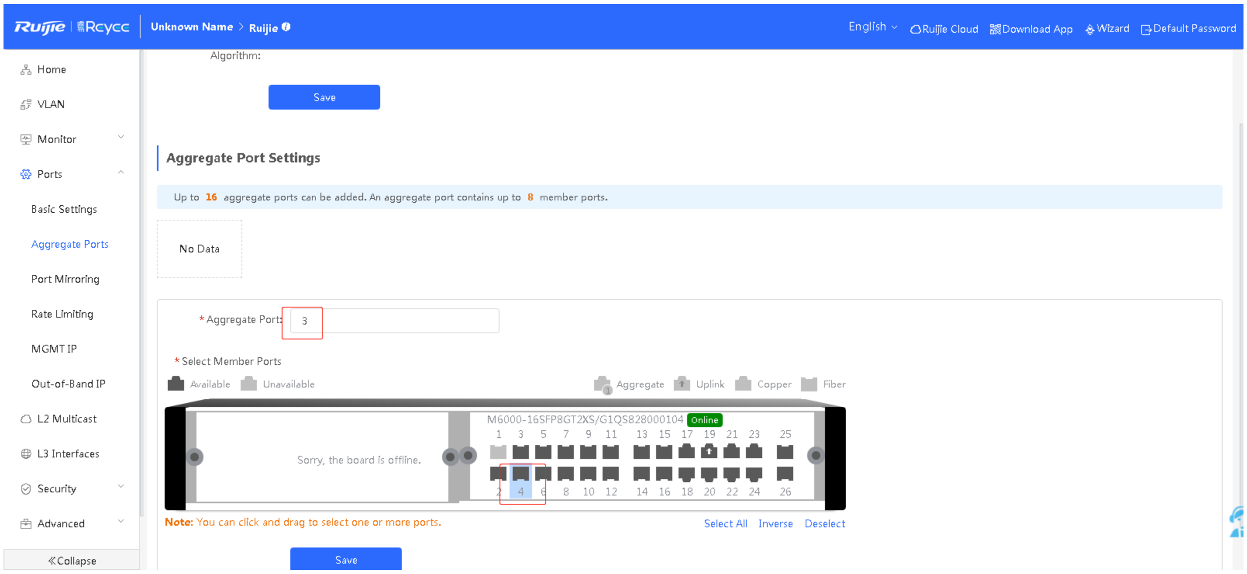


Global Settings

Load Balance Algorithm: Src & Dest MAC

- **Adding an Aggregate Port**

Enter an aggregate port ID, select member ports (ports that have been added to an aggregate port cannot be selected), and click **Save**. The port panel displays a successfully added aggregate port.



Algorithm:

Aggregate Port Settings

Up to 16 aggregate ports can be added. An aggregate port contains up to 8 member ports.

No Data

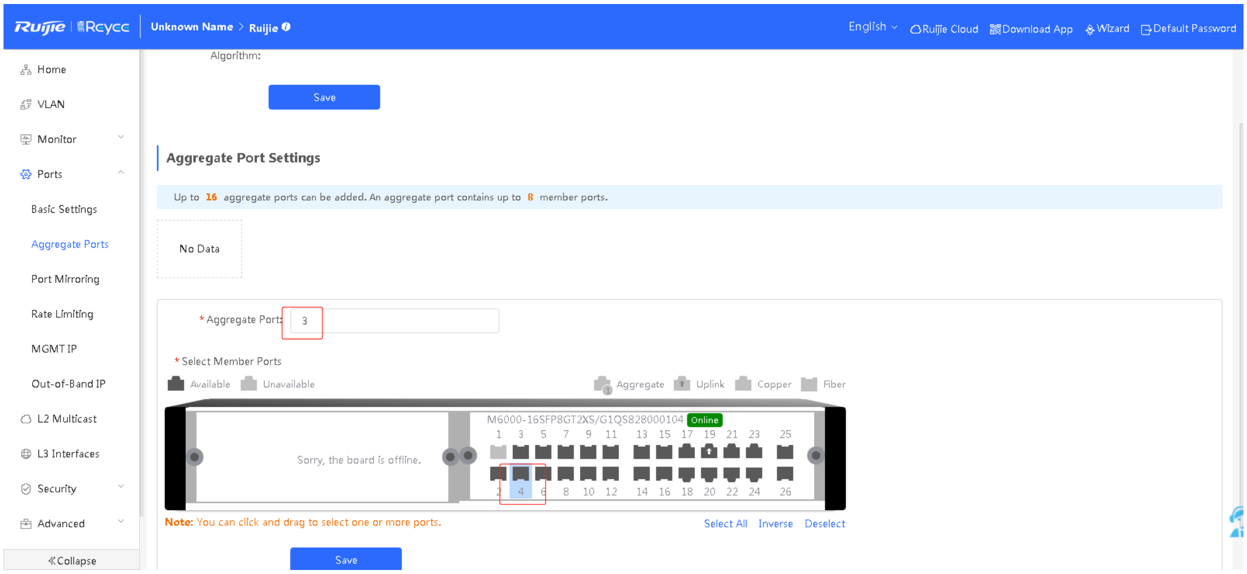
* Aggregate Port: 3

* Select Member Ports

Note: You can click and drag to select one or more ports.

➢ Editing an Aggregate Port

Click an added aggregate port. Member ports of the aggregate port will become selected. Click a port to deselect it, and then click **Save**.



Algorithm:

Aggregate Port Settings

Up to 16 aggregate ports can be added. An aggregate port contains up to 8 member ports.

No Data

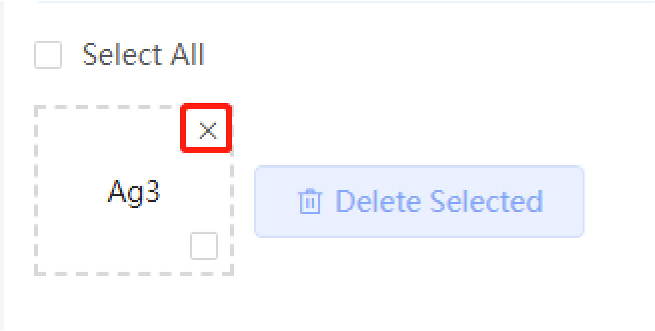
* Aggregate Port: 3

* Select Member Ports

Note: You can click and drag to select one or more ports.

➢ Deleting an Aggregation Port

Move the cursor over a created aggregate port and click × . A message is displayed, asking you whether to delete the aggregate port. Click **OK** to delete the created aggregate port. The corresponding ports become available on the port panel.



Note

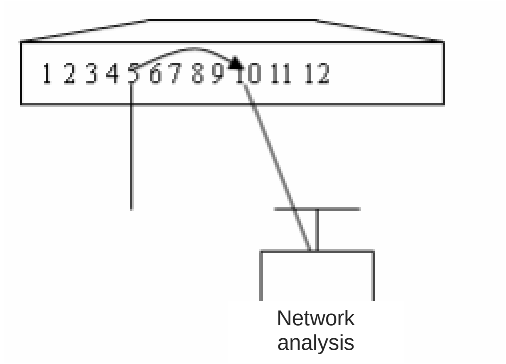
1. A port that has been added to an aggregate port cannot be added to another one.
2. After an aggregate port is deleted, its member ports are restored to the default settings and are disabled.
3. An aggregate port contains a maximum of eight member ports.
4. Copper ports and SFP ports cannot be both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

3.4.5 Port Mirroring

1. Overview

The switched port analyzer (SPAN) function replicates packets from a specified port to another port on the switch that is connected to a network monitoring device for network monitoring and troubleshooting.

Using SPAN, you can monitor all packets that enter and exit source ports. For example, as shown in the figure below, all packets on port 5 are mapped to port 10. The network analyzer connected to port 10 can receive all packets passing through port 5 even though it is not directly connected to port 5.



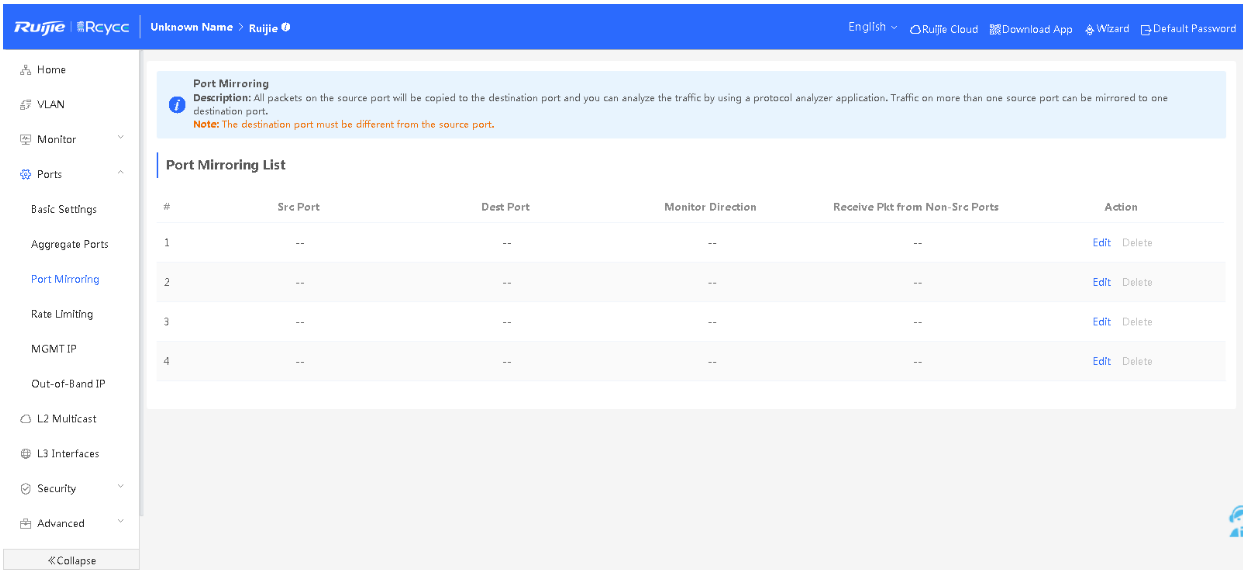
The SPAN function is mainly used to monitor network information and troubleshoot network faults in network monitoring and troubleshooting scenarios.

Table 3-5 Typical Applications of SPAN

Application Type	Description	Remarks
One-to-many mirroring	Multiple users need to monitor data on the same port.	Described in this section
RSPAN basic application	Packets from the source device need to be mirrored to the destination device for monitoring.	Described in this section

2. Configuration Steps

Configure SPAN. A maximum of four SPAN entries can be configured.



Port Mirroring
Description: All packets on the source port will be copied to the destination port and you can analyze the traffic by using a protocol analyzer application. Traffic on more than one source port can be mirrored to one destination port.
Note: The destination port must be different from the source port.

Port Mirroring List

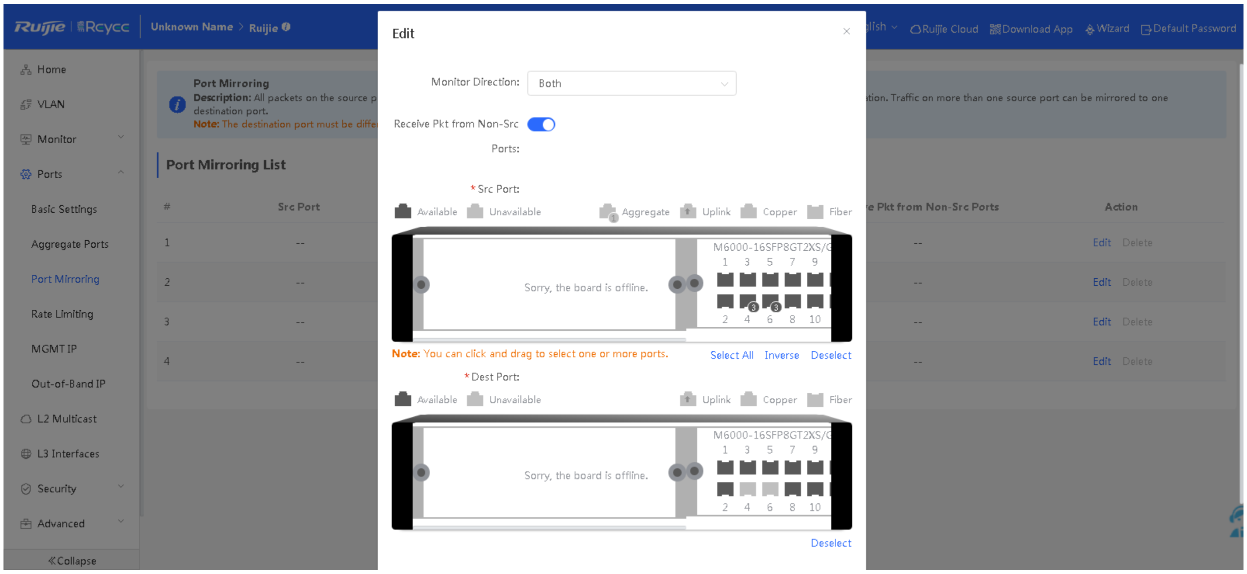
#	Src Port	Dest Port	Monitor Direction	Receive Pkt from Non-Src Ports	Action
1	--	--	--	--	Edit Delete
2	--	--	--	--	Edit Delete
3	--	--	--	--	Edit Delete
4	--	--	--	--	Edit Delete

Table 3-6 SPAN Parameters

Parameter	Description	Default Value
Src Port	A source port is also called a monitored port. During a SPAN session, data flows on the source port are monitored for network analysis or troubleshooting.	N/A
Dest Port	A SPAN session has a destination port (also called a monitoring port) for receiving copies of packets from a source port.	N/A
Monitor Direction	It specifies the type of packets (data flow direction) to be monitored by a source port. The value can be all packets, incoming packets, or outgoing packets.	All packets
Receive Pkt from Non-Src Port	It is applied to the destination port and indicates whether a destination port forwards other packets while monitoring packets. Enable: monitor packets + forward packets Disable: monitor packets only	Enable

➢ Configuring an SPAN Entry

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



Port Mirroring

Description: All packets on the source p… …tion. Traffic on more than one source port can be mirrored to one destination port.

Note: The destination port must be diffe…

Edit

Monitor Direction: Both

Receive Pkt from Non-Src Ports: on

* Src Port:

Sorry, the board is offline.

Note: You can click and drag to select one or more ports.

* Dest Port:

Sorry, the board is offline.

➢ Deleting an SPAN Entry

Click **Delete** in the list. In the displayed confirmation box, click **OK** to delete the SPAN entry.

Caution

1. You can select multiple source traffic monitoring ports but only one destination port. Moreover, the source traffic monitoring ports cannot contain the destination port.
2. An aggregate port cannot be used as the destination port.
3. A maximum of four SPAN entries can be configured. SPAN cannot be configured for ports that have been used for SPAN.

3.4.6 Rate Limiting

The **Rate Limiting** module allows you to configure traffic limits for ports, including rate limits for inbound and outbound direction of ports.

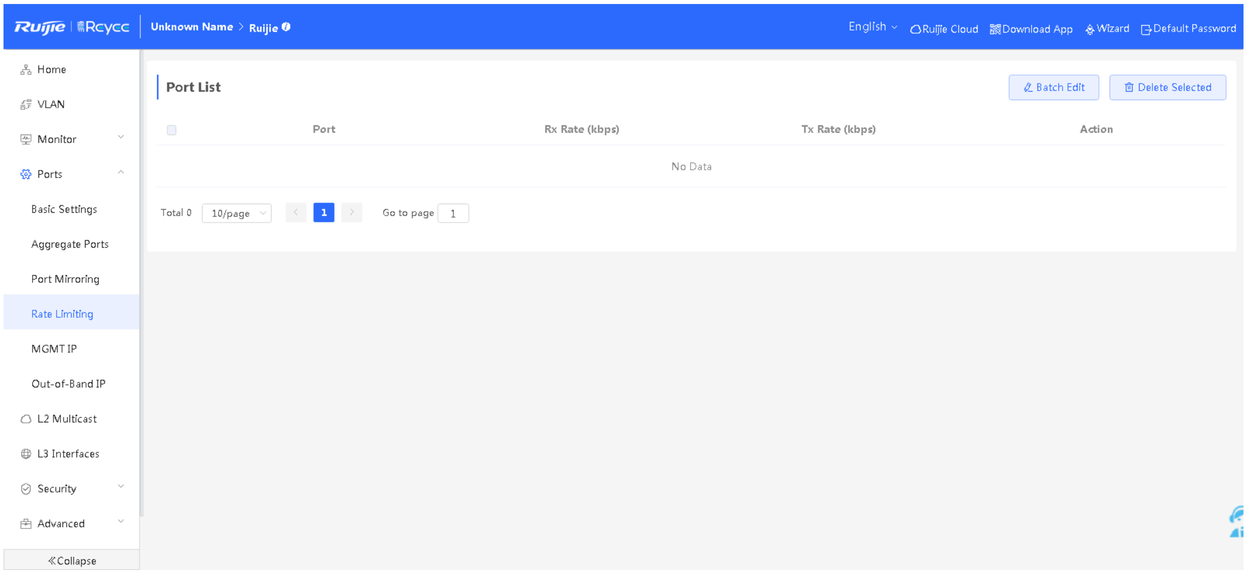
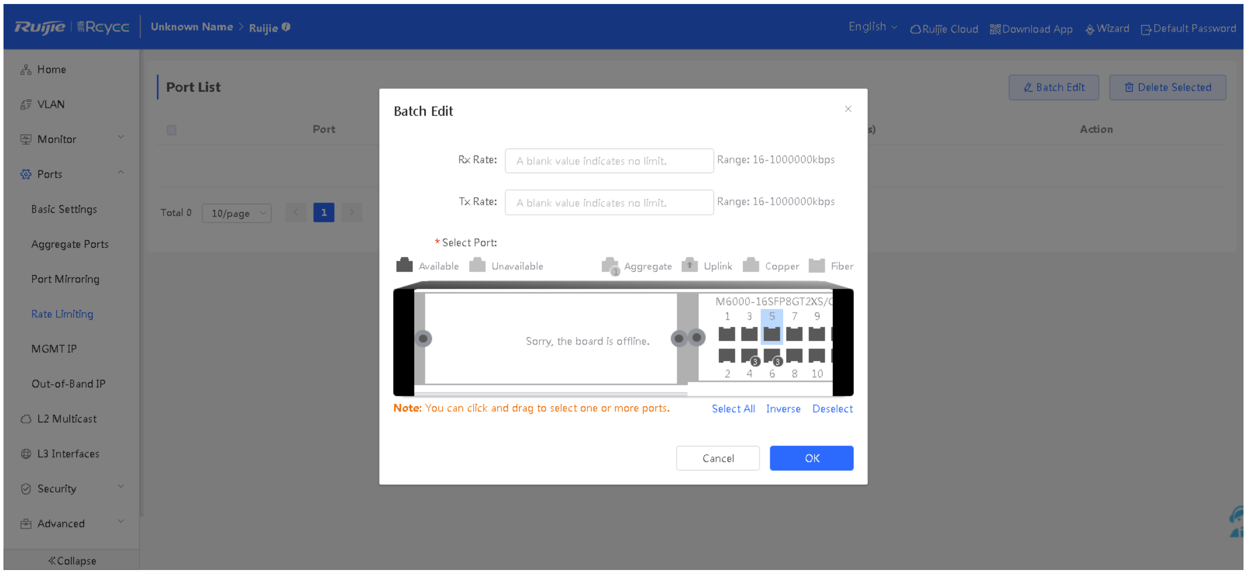


Table 3-7 Rate Limit Parameters of Ports

Parameter	Description	Default Value
Ingress rate	Rate, at which packets are sent from a port to a switch.	Not limited
Egress rate	Rate, at which packets are sent out of a switch through a port.	Not limited

➢ Adding Rate Limits for a Port

Click **Batch Edit**. In the displayed dialog box, select a port, configure at least the ingress rate or egress rate, and click **OK**. The added rate limits of the port will be displayed in the port rate limit list.



Batch Edit

Rx Rate: A blank value indicates no limit. Range: 16-1000000kbps

Tx Rate: A blank value indicates no limit. Range: 16-1000000kbps

* Select Port:

Sorry, the board is offline.

Note: You can click and drag to select one or more ports.

➢ Changing Rate Limits of a Single Port

In **Port List**, click **Edit**. In the displayed dialog box, set the ingress rate and egress rate and click **OK**. After the configuration succeeds, the rate limits are updated in the port list.

➢ Deleting Rate Limits of a Port

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

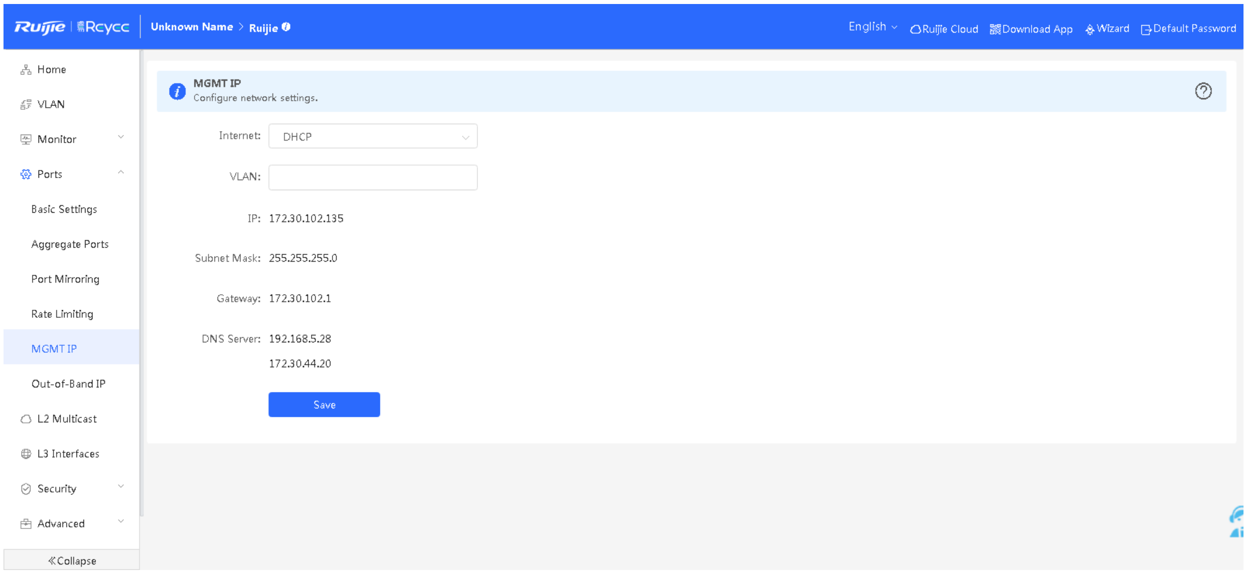
Method 2: In **Port List**, click **Delete**. In the confirmation dialog box, click **OK** to delete the data record.

Note

1. When configuring rate limits for a port, you must configure at least the ingress rate or egress rate.
2. When the ingress rate or egress rate is not set, the port rate is not limited.

3.4.7 MGMT IP

The **MGMT IP** page allows you to configure the management IP address for the device.



MGMT IP
Configure network settings.

Internet: DHCP

VLAN:

IP: 172.30.102.135

Subnet Mask: 255.255.255.0

Gateway: 172.30.102.1

DNS Server: 192.168.5.28
172.30.44.20

Save

The device can be networked in two modes:

DHCP: Uses a temporary IP address dynamically assigned by the upstream DHCP server for Internet access.

Static IP: Uses a static IP address for Internet access.

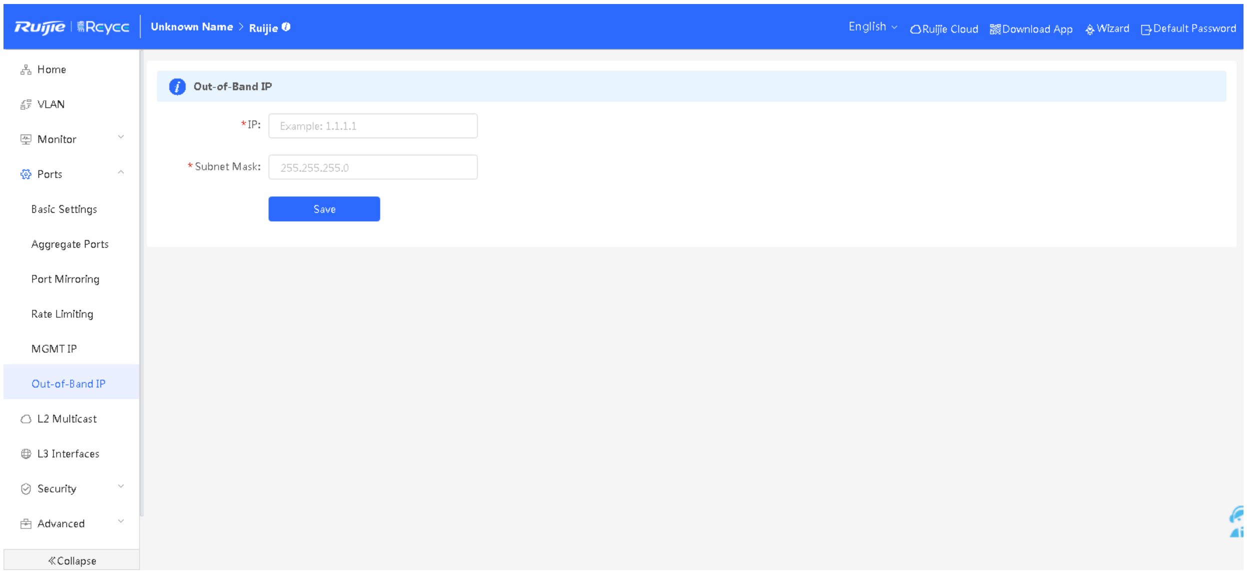
If you select DHCP, the device obtains parameters from the DHCP server. If static IP is selected, you need to enter the management VLAN, IP address, subnet mask, default gateway IP address, and DNS server. Click **Save**. A setting success message is displayed.

Note

1. If the management VLAN is null or not specified, VLAN 1 takes effect by default.
2. The management VLAN must be selected from existing VLANs. If no VLAN is created, go to the VLAN list to add a VLAN (for details, see 3.2.1 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.

3.4.8 Out-of-Band IP

The management IP address of the chassis is the IP address of the MGMT port. Only the NBS6002, NBS7003, and NBS7006 switch series support this IP address.



Out-of-Band IP

*IP: Example: 1.1.1.1

*Subnet Mask: 255.255.255.0

Note

No IP address is configured for the MGMT port by default. Currently, only a static IP address can be configured for the MGMT port but DHCP is not supported.

3.5 L2 Multicast

3.5.1 Overview

The Internet Group Management Protocol (IGMP) snooping is an IP multicast snooping mechanism running on a VLAN to manage and control the forwarding of IP multicast traffic within the VLAN. It implements the L2 multicast function.

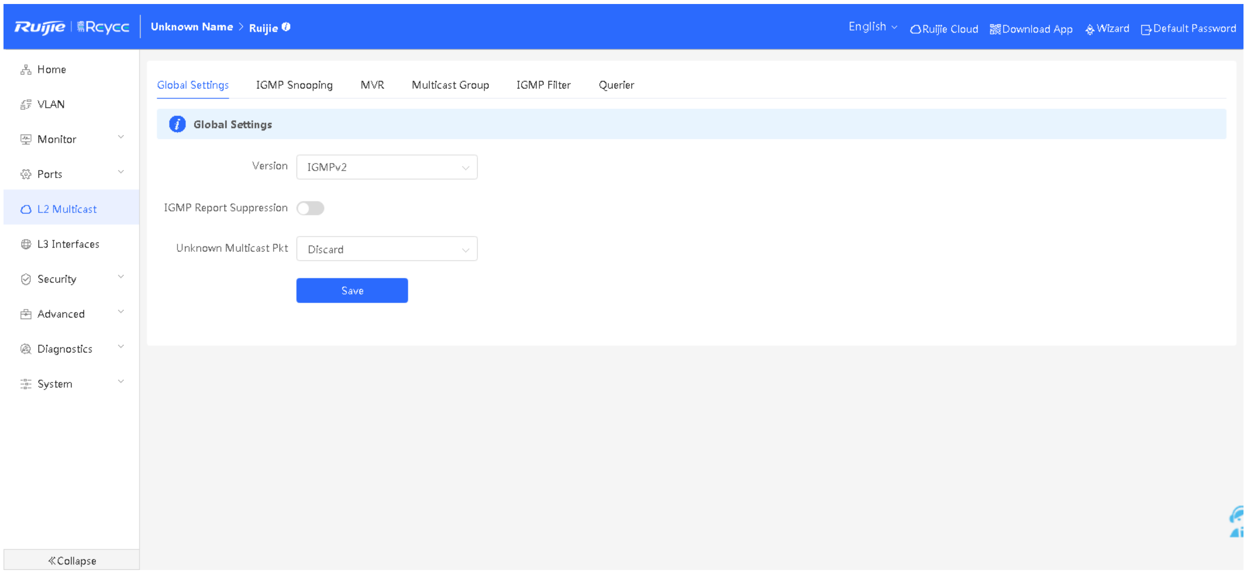
Table 3-8 Application of L2 Multicasting

Application Type	Description
L2 multicast control	L2 multicast packets are accurately forwarded to avoid L2 flooding of multicast packets.
Public multicast service (multicast VLAN)	Users of multiple VLANs share multicast streams of the same VLAN.
Chargeable channels and preview	The address range of multicast groups demanded by users is controlled and multicast groups that cannot be demanded can be previewed.

Currently, the **L2 Multicast** module allows you to configure global settings, IGMP snooping, MVR, multicast group, IGMP filter, querier, and other functions.

3.5.2 Global Settings

The **Global Settings** page allows you to specify the IGMP protocol version, whether to enable report packet suppression, and the behavior for processing unknown multicast packets.



Global Settings

Version IGMPv2

IGMP Report Suppression

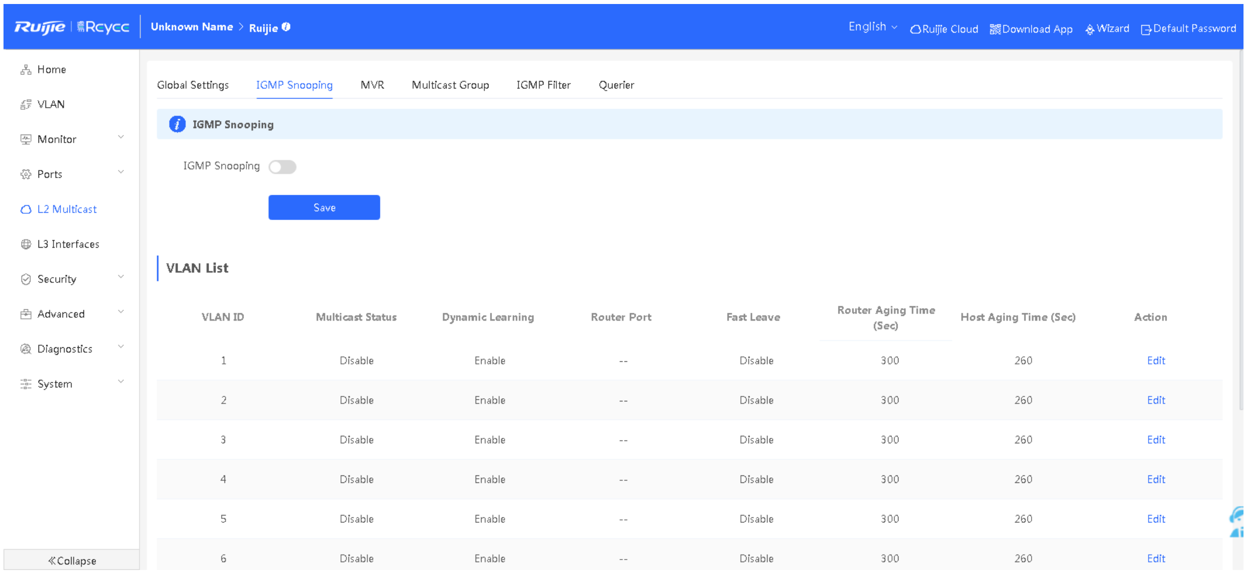
Unknown Multicast Pkt Discard

Table 3-9 Parameters on the Global Settings Page

Parameter	Description	Default Value
Version	It specifies the highest version of IGMP packets that can be processed by the L2 multicast function.	IGMPv2
IGMP Report Suppression	After this function is enabled, the switch forwards only one report packet to the multicast router if multiple downlink clients connected to the switch simultaneously send the report packet to demand the same multicast group.	Disable
Unknown Multicast Pkt	It specifies the method of processing unknown multicast packets when both global and VLAN multicast functions are enabled. The value can be **Discard** or **Flood**.	Discard

3.5.3 IGMP Snooping

IGMP snooping has one entry for each VLAN. Therefore, the number of IGMP snooping entries is the same as that of VLANs.



IGMP Snooping

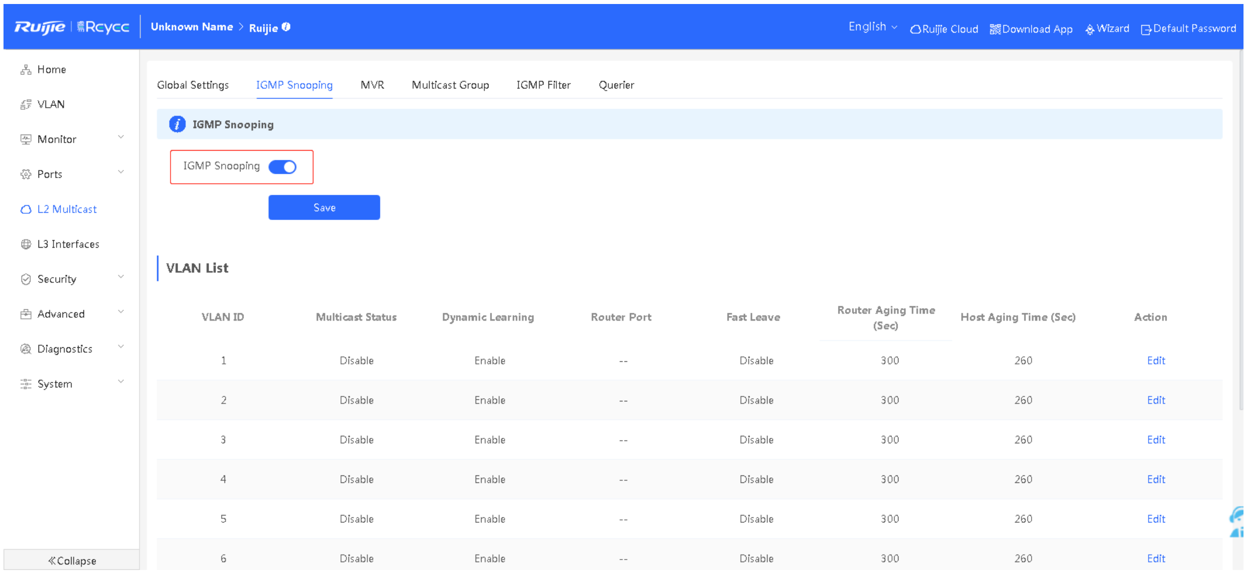
IGMP Snooping ○

VLAN List

VLAN ID	Multicast Status	Dynamic Learning	Router Port	Fast Leave	Router Aging Time (Sec)	Host Aging Time (Sec)	Action
1	Disable	Enable	--	Disable	300	260	Edit
2	Disable	Enable	--	Disable	300	260	Edit
3	Disable	Enable	--	Disable	300	260	Edit
4	Disable	Enable	--	Disable	300	260	Edit
5	Disable	Enable	--	Disable	300	260	Edit
6	Disable	Enable	--	Disable	300	260	Edit

➢ **Enabling IGMP Snooping**

Click **IGMP Snooping** to enable it and click **Save** for the configuration to take effect.



IGMP Snooping

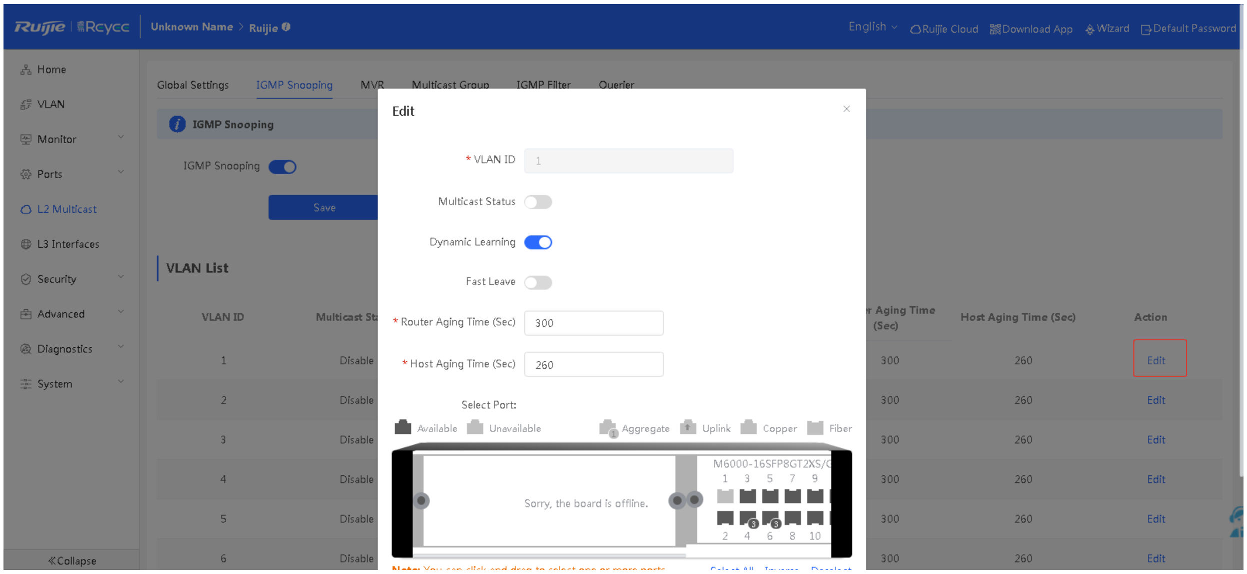
IGMP Snooping: enabled

VLAN List

VLAN ID	Multicast Status	Dynamic Learning	Router Port	Fast Leave	Router Aging Time (Sec)	Host Aging Time (Sec)	Action
1	Disable	Enable	--	Disable	300	260	Edit
2	Disable	Enable	--	Disable	300	260	Edit
3	Disable	Enable	--	Disable	300	260	Edit
4	Disable	Enable	--	Disable	300	260	Edit
5	Disable	Enable	--	Disable	300	260	Edit
6	Disable	Enable	--	Disable	300	260	Edit

➢ Editing a VLAN Entry

Click **Edit**. In the displayed dialog box, enable/disable the multicast function, dynamic learning function, and fast leave function, configure routed ports, and set the connected port aging time and member port aging time, and click **OK**.



Edit

* VLAN ID: 1

Multicast Status: disabled

Dynamic Learning: enabled

Fast Leave: disabled

* Router Aging Time (Sec): 300

* Host Aging Time (Sec): 260

Select Port:

Table 3-10 VLAN Configuration Parameters of IGMP Snooping

Parameter	Description	Default Value
Multicast Status	Whether to enable or disable the VLAN multicast function. The multicast function of a VLAN takes effect only when both the global IGMP snooping and VLAN multicast functions are enabled.	Disable
Dynamic Learning	Whether to enable or disable the dynamic learning function of the multicast router port.	Enable
Router Port	List of current multicast router ports, including dynamically learned and statically configured ports.	NA
Fast Leave	After this function is enabled, a port is immediately deleted from a multicast group without waiting for aging timeout after it receives the leave packet. This function is usually enabled on the access switch directly connected to a client.	Disable
Router Aging Time (Sec)	Aging time of dynamically learned multicast router ports, in seconds.	300 seconds
Host Aging Time (Sec)	Aging time of dynamically learned member ports of a multicast group, in seconds.	260 seconds
Select Port	Static multicast router port.	NA

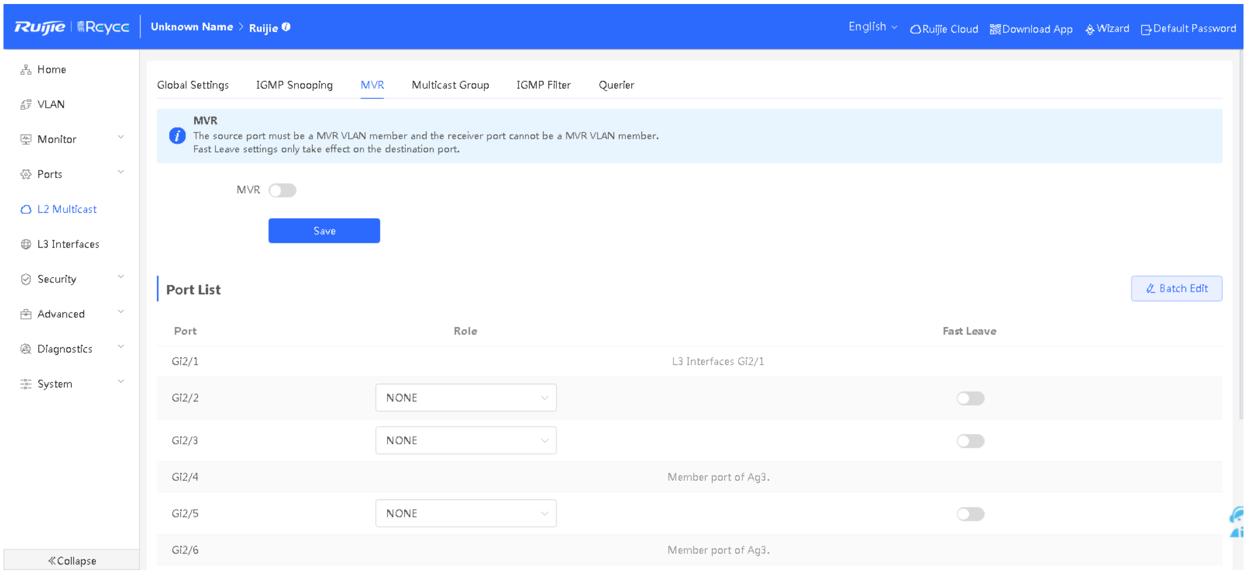
Note

1. The aging time of multicast router ports is in the range of 30–3600 seconds.
2. The aging time of the member interfaces is in the range of 30–65535 seconds.

3.5.4 MVR

IGMP snooping can forward multicast traffic only in the same VLAN. If multicast traffic needs to be forwarded to different VLANs, the multicast source must send multicast traffic to different VLANs. In order to save upstream bandwidth and reduce the burden of multicast sources, multicast VLAN register (MVR) comes into being.

MVR can copy multicast traffic received from an MVR VLAN to different VLANs and forward the traffic.



MVR
The source port must be a MVR VLAN member and the receiver port cannot be a MVR VLAN member.
Fast Leave settings only take effect on the destination port.

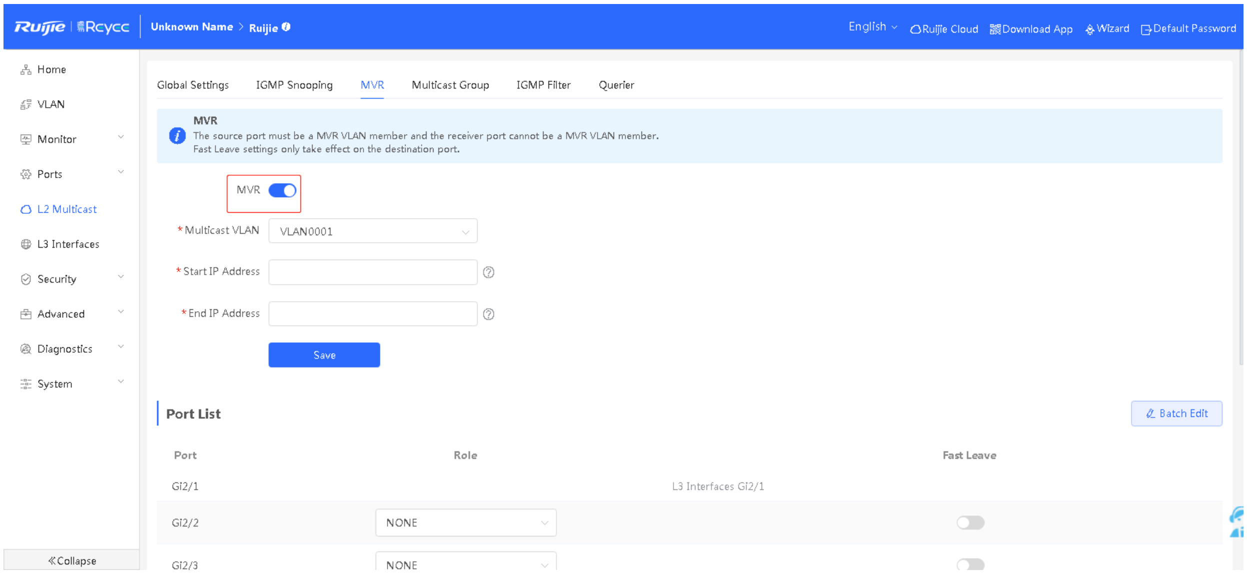
MVR: off

Port List

Port	Role	Fast Leave
Gi2/1	L3 Interfaces Gi2/1	
Gi2/2	NONE	off
Gi2/3	NONE	off
Gi2/4	Member port of Ag3.	
Gi2/5	NONE	off
Gi2/6	Member port of Ag3.	

➢ Configuring MVR

After the MVR function is enabled, you need to select the multicast VLAN and set the multicast start address and multicast end address. Click **Save**.



MVR
The source port must be a MVR VLAN member and the receiver port cannot be a MVR VLAN member.
Fast Leave settings only take effect on the destination port.

MVR: on
*Multicast VLAN: VLAN0001
*Start IP Address:
*End IP Address:

Port List

Port	Role	Fast Leave
Gi2/1	L3 Interfaces Gi2/1	
Gi2/2	NONE	off
Gi2/3	NONE	off

Table 3-11 Global MVR Configuration Parameters

Parameter	Description	Default Value
MVR	Enables/Disables MVR globally.	Disable
Multicast VLAN	VLAN of a multicast source, that is, the VLAN before conversion.	1
Start IP Address	Learned or configured start multicast IP address of an MRV multicast group.	NA
End IP Address	Learned or configured end multicast IP address of an MRV multicast group.	NA

➢ **Configuring Ports**

You can set the port role to **NONE**, **RECEIVER**, or **SOURCE**. You can also set whether to enable the fast leave function for a port.

Table 3-12 MVR Configuration Parameters of a Port

Parameter	Description	Default Value
Role	**NONE**: Indicates that the MRV function is disabled. **SOURCE**: Indicates the source port that receives multicast data streams. **RECEIVER**: Indicates the receiver port connected to a client.	NONE
Fast Leave	Configures the fast leave function for a port. After the function is enabled, if the port receives the leave packet, it is directly deleted from the multicast group.	Disable

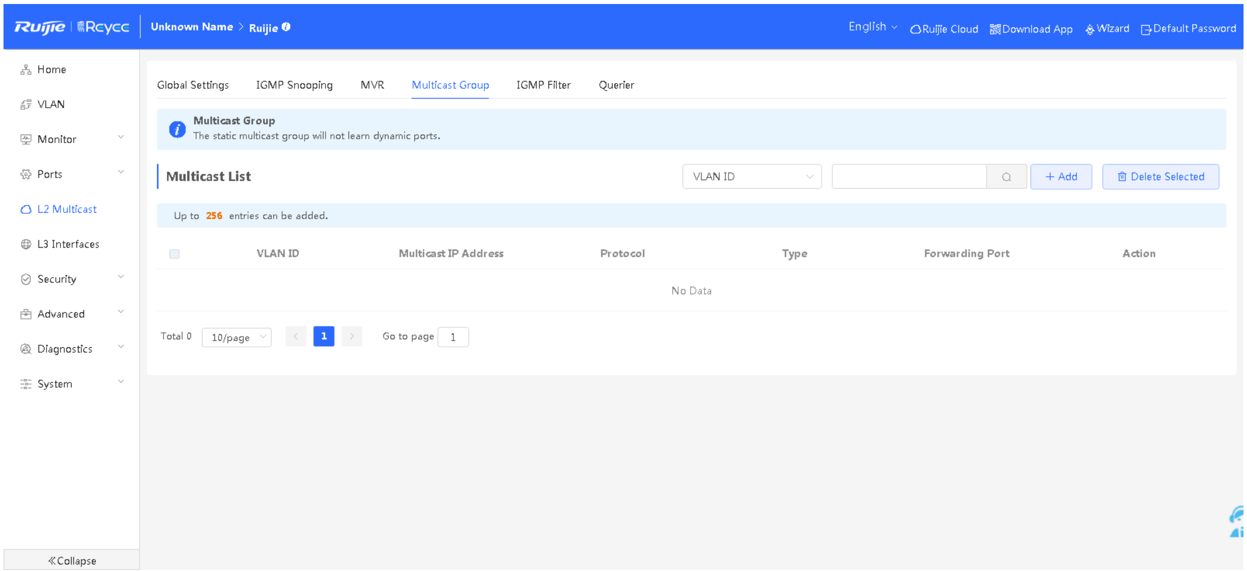
Note

1. If a source port or a receiver port is configured, the source port must belong to the MVR VLAN and the receiver port must not belong to the MVR VLAN.
2. The fast leave function takes effect only on the receiver port.

3.5.5 Multicast Group

A multicast group consists of the destination ports, to which multicast packets are to be sent. Multicast packets are sent to all ports in the multicast group.

You can view the configured multicast list on the current page. Click **Add** to create a multicast group.



Multicast Group
The static multicast group will not learn dynamic ports.

Multicast List

Up to 256 entries can be added.

□	VLAN ID	Multicast IP Address	Protocol	Type	Forwarding Port	Action
No Data						

Total 0

Table 3-13 Multicast Group Configuration Parameters

Parameter	Description	Default Value
VLAN ID	VLAN, to which received multicast traffic belongs	NA
Multicast IP Address	On-demand multicast IP address	NA
Protocol	If the VLAN ID is a multicast VLAN and the multicast address is within the multicast IP address range of the MVR, the protocol is MVR. In other cases, the protocol is IGMP snooping.	NA
Type	Multicast group generation mode, which can be statically configured or dynamically learned	NA
Forwarding Port	List of ports that forward multicast traffic	NA

➢ **Searching for a Multicast Group**

Select the search type (by VLAN ID or by multicast address), enter the search string, and click 🔍. Multicast address entries that meet search criteria will be displayed in the list.

- **Changing a Multicast Port**

In **Multicast List**, click **Edit**. In the displayed dialog box, select a port and click **OK**. After the configuration succeeds, the port in the multicast entry is updated.

- **Deleting a Multicast Address**

Method 1: In **Multicast List**, select the multicast entry to be deleted and click **Delete Selected**. In the displayed confirmation box, click **OK**. A deletion success message is displayed and data in the list will be updated.

Method 2: In **Multicast List**, click **Delete** in the last **Action** column. In the displayed dialog box, click **OK** to complete deletion.

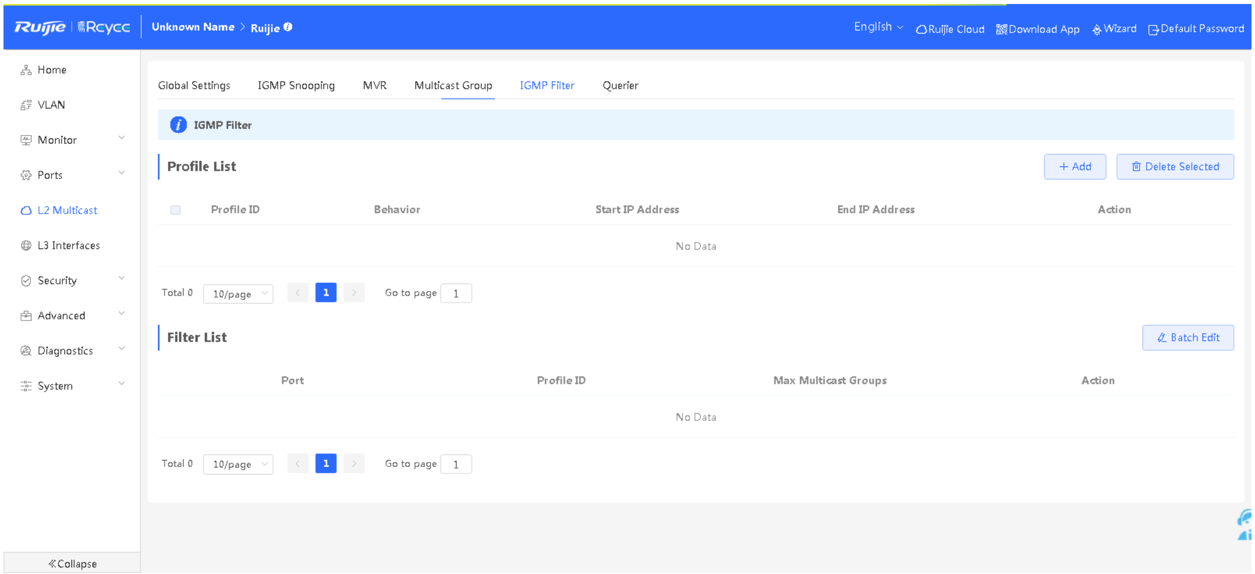
Note

A maximum of 256 multicast addresses can be configured.

3.5.6 IGMP Filter

A profile is used to define the range of multicast group addresses that can be or cannot be demanded by users. Other function modules can cite the profile to define the multicast group address range.

When configuring a port filter, you can cite a profile to define the range of multicast group addresses that can be or cannot be demanded by users on a port.



IGMP Filter

Profile List

Profile ID	Behavior	Start IP Address	End IP Address	Action
No Data				

Filter List

Port	Profile ID	Max Multicast Groups	Action
No Data			

➢ Creating a Profile

Click **Add**. In the displayed dialog box, enter the profile ID, action, and multicast address range.

Table 3-14 Profile Configuration Parameters

Parameter	Description	Default Value
Profile ID	Profile ID	NA
Behavior	**Deny**: Forbids learning multicast IP addresses in a specified range. **Permit**: Only allows learning multicast IP addresses in a specified range.	NA
Start IP Address	Start multicast IP address	NA
End IP Address	End multicast IP address	NA

➢ Configuring a Port Filter

Click **Edit**. In the displayed dialog box, select profile ID and enter the maximum number of multicast groups allowed by a port.

Table 3-15 Port Filter Configuration Parameters

Parameter	Description	Default Value
Profile ID	Profile that takes effect on a port. If it is not set, no profile rule is bound to the port.	NA
Max Multicast Groups	Maximum number of multicast groups that a port can join.	256

Note

VLAN filters are not supported.

3.5.7 Querier

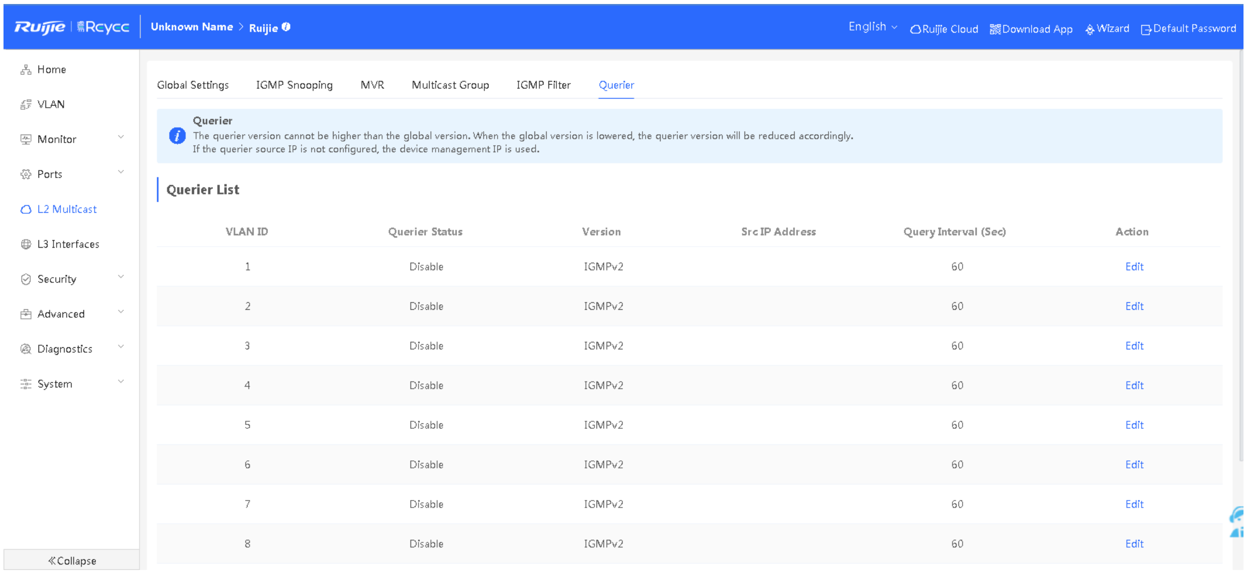
1. Overview

On a network with L3 multicast devices, an L3 multicast device serves as the IGMP querier. L2 multicast devices only need to listen to IGMP packets to establish and maintain forwarding entries and implement L2 multicasting.

On a network without L3 multicast devices, no L3 multicast device serves as an IGMP querier. To enable an L2 multicast device to listen to IGMP packets, you must configure the IGMP querier function on the L2 multicast device. The L2 multicast device need to serve as an IGMP querier and monitor IGMP packets so as to establish and maintain forwarding table entries and implement L2 multicasting.

2. Configuration Steps

One querier is set for each VLAN. The number of queriers is the same as that of device VLANs.



Querier
The querier version cannot be higher than the global version. When the global version is lowered, the querier version will be reduced accordingly.
If the querier source IP is not configured, the device management IP is used.

Querier List

VLAN ID	Querier Status	Version	Src IP Address	Query Interval (Sec)	Action
1	Disable	IGMPv2		60	Edit
2	Disable	IGMPv2		60	Edit
3	Disable	IGMPv2		60	Edit
4	Disable	IGMPv2		60	Edit
5	Disable	IGMPv2		60	Edit
6	Disable	IGMPv2		60	Edit
7	Disable	IGMPv2		60	Edit
8	Disable	IGMPv2		60	Edit

➢ Setting a Querier

In **Querier List**, click **Edit** in the last **Action** column. In the displayed dialog box, select whether to enable the querier, set the querier version, querier source IP address, and packet query interval, and click **OK**.

Table 3-16 Querier Configuration Parameters

Parameter	Description	Default Value
Querier Status	Whether to enable or disable the VLAN querier function.	Disable
Version	IGMP version of query packets sent by the querier. It can be set to IGMPv2 or IGMPv3.	IGMPv2
Src IP Address	Source IP address carried in query packets sent by the querier.	NA
Query Interval (Sec)	Interval for sending query packets, in seconds.	60 seconds

Note

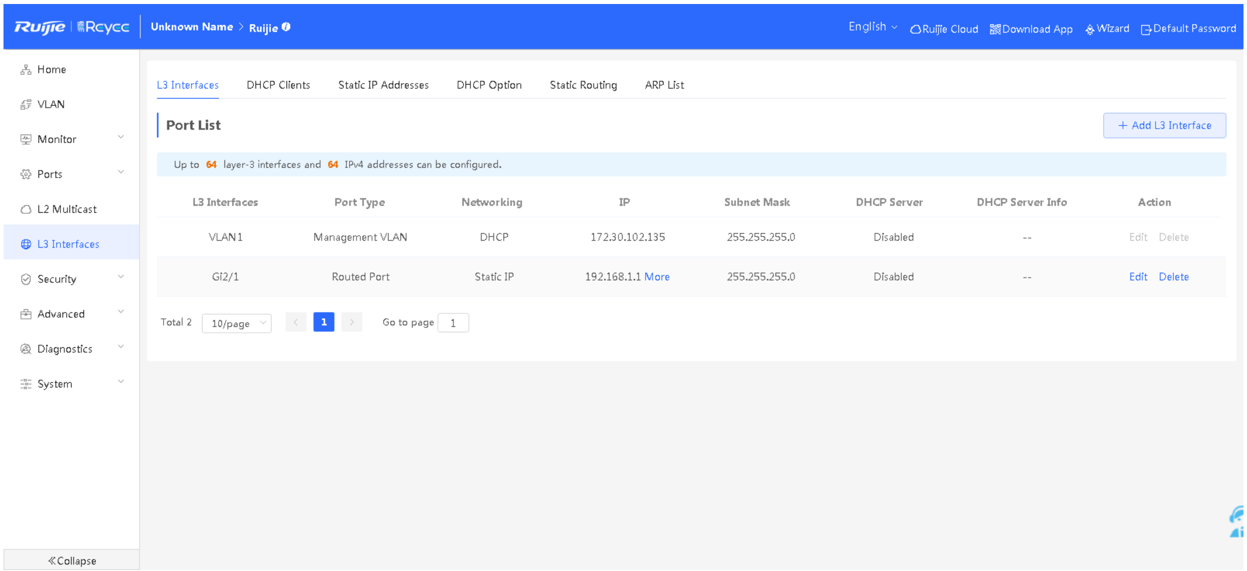
1. The querier version cannot be higher than the global IGMP version. When the global IGMP version is lowered, the querier version is lowered accordingly.
2. If no querier source IP is configured, the device management IP is used as the source IP address of the querier.
3. The value range of the query interval is from 30 to 18000, in seconds.

3.6 L3 Management

L3 management allows you configure L3 interfaces, address pools, DHCP relay, client list, static address allocation, DHCP options, static routing, and ARP list.

3.6.1 L3 Interfaces

The port list displays various types of L3 interfaces on the device, including SVIs, routed ports, and L3 aggregate ports.



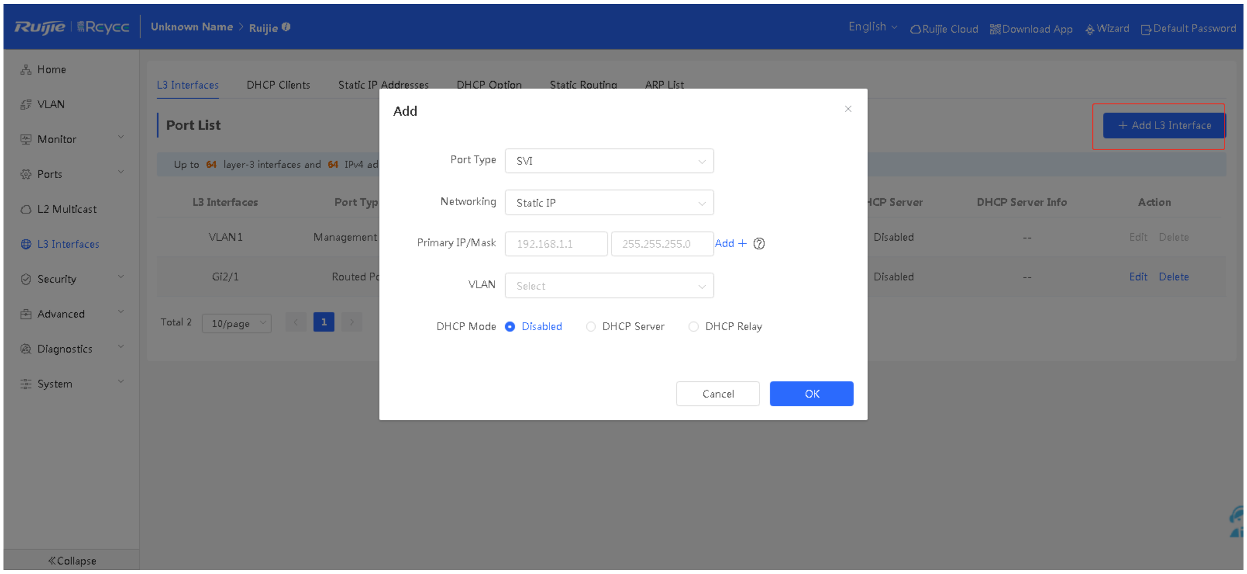
Port List

Up to 64 layer-3 interfaces and 64 IPv4 addresses can be configured.

L3 Interfaces	Port Type	Networking	IP	Subnet Mask	DHCP Server	DHCP Server Info	Action
VLAN1	Management VLAN	DHCP	172.30.102.135	255.255.255.0	Disabled	--	Edit Delete
Gi2/1	Routed Port	Static IP	192.168.1.1 More	255.255.255.0	Disabled	--	Edit Delete

➢ **Setting an L3 Interface**

Click **Add L3 Interface**. In the displayed dialog box, set the type of an L3 interface to be created and configure attributes for the L3 interface.



L3 Interfaces	Port Typ	HCP Server	DHCP Server Info	Action
VLAN1	Management	Disabled	--	Edit Delete
Gi2/1	Routed Pc	Disabled	--	Edit Delete

Add

Port Type: SVI

Networking: Static IP

Primary IP/Mask: 192.168.1.1 255.255.255.0 Add +

VLAN: Select

DHCP Mode: ● Disabled ○ DHCP Server ○ DHCP Relay

Cancel OK

Table 3-17 Configuration Parameters of an L3 Interface

Parameter	Description
Port Type	Specifies the type of a created L3 interface. It can be an SVI, routed port, or L3 aggregate port.
Networking	Specifies DHCP or static mode for a port to obtain the IP address.
VLAN	Specifies the VLAN, to which an SVI belongs.
IP/Mask	When **Networking** is set to **Static IP**, you need to manually enter the IP address and subnet mask.
Select Port	Select the device port to be configured.
Aggregate	Specifies the aggregate port ID, for example, Ag1, when an L3 aggregate port is created.
DHCP Mode	Select whether to enable the DHCP service on the L3 interface. **Disabled**: Indicates that the DHCP service is disabled. No IP address can be assigned to clients connected to the interface. **DHCP Server**: Indicates that the device functions as the DHCP server to assign IP addresses to downlink devices connected to the interface. You need to set the start IP address of an address pool, number of IP addresses that can be assigned, and address lease. **DHCP Relay**: Indicates that the device serves as a DHCP relay, obtains IP addresses from an external server, and assigns the IP addresses to downlink devices. The interface IP address and DHCP server IP address need to be configured. The interface IP address must be in the same network segment as the address pool of the DHCP server.

➢ **Editing an L3 Interface**

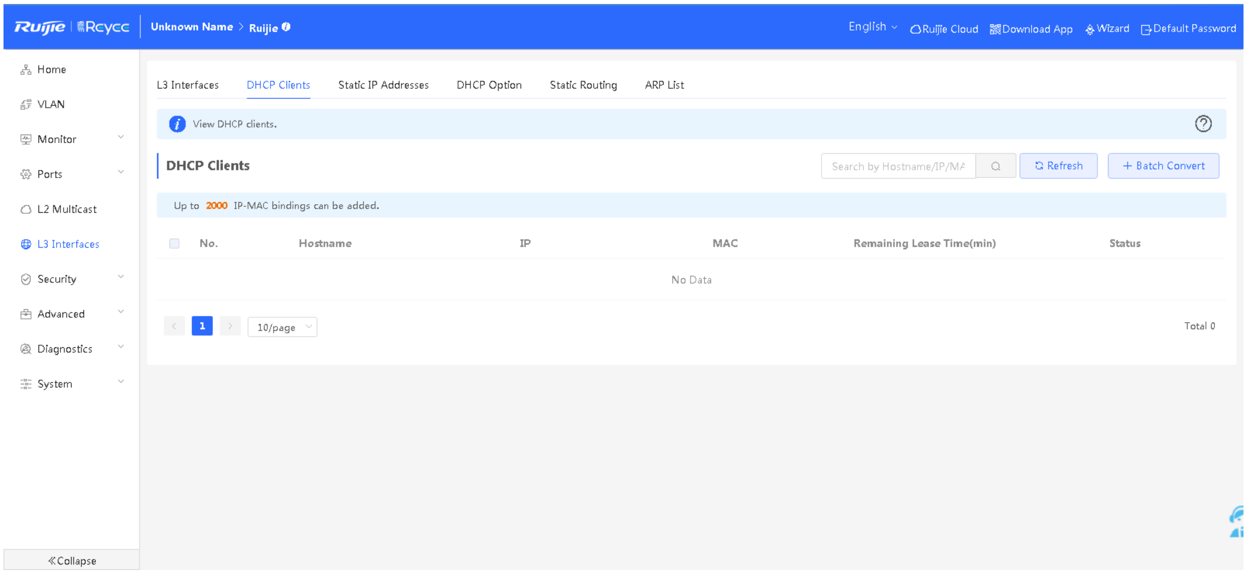
Click **Edit**. In the displayed dialog box, modify the attributes of an L3 interface and click **OK**.

Note

1. VLAN 1 is the default SVI of the device. It can be neither modified or deleted.
2. The management VLAN is only displayed (cannot be modified) on the **L3 Interfaces** page. You can modify it on the **MGMT IP** page. For details, see 3.4.7 MGMT IP.
3. The DHCP relay and DHCP server functions of an L3 interface are mutually exclusive and cannot be configured at the same time.
4. Member ports of an L3 interface must be routed ports.

3.6.2 DHCP Clients

The client port list displays IP addresses assigned to downlink devices connected to an L3 interface after the DHCP server function is enabled on the L3 interface.



View DHCP clients.

DHCP Clients

Up to 2000 IP-MAC bindings can be added.

□	No.	Hostname	IP	MAC	Remaining Lease Time(min)	Status
			No Data			

Total 0

➢ **Search**

Select the search type (by MAC address, by IP address, or by host name), enter the search string (fuzzy search is supported), and click 🔍. Entries that meet the search criteria are displayed in the list.

➢ **Adding a Static Entry**

Add the learned IP and MAC entries to the static address assignment list to assign static IP addresses to hosts with fixed MAC addresses.

Method 1: In **DHCP Clients**, select an entry to be converted and click **Batch Convert**. In the confirmation box, click **OK**. A deletion success message is displayed and the static entry data in the list is updated.

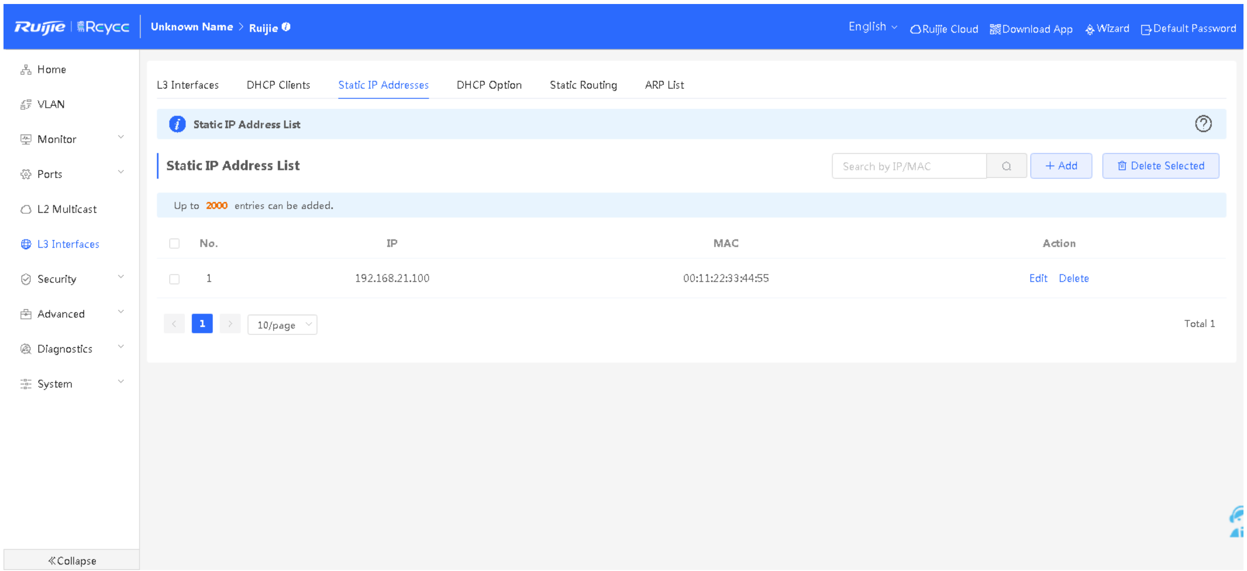
Method 2: In **DHCP Clients**, click **Convert to Static IP** in the last **Action** column to convert a dynamic entry into a static entry.

Note

The DHCP client list allows you to configure a maximum of 2000 static address entries. The actual maximum number of static address entries supported by a device is subject to the product specifications.

3.6.3 Static IP Addresses

The static IP address list displays client entries, in which DHCP addresses in the client list are converted into static addresses, as well as manually added static entries.



Static IP Address List

Up to 2000 entries can be added.

□	No.	IP	MAC	Action
□	1	192.168.21.100	00:11:22:33:44:55	Edit Delete

Total 1

➢ **Search**

Select the search type (by MAC address or by IP address), enter the search string (fuzzy search is supported), and click 🔍. Static address entries that meet the search criteria are displayed in the list.

➢ **Adding a Static Address**

Click **Add**. In the displayed dialog box, enter a MAC address and an IP address, and click **OK**. An adding success message is displayed and the list is updated.

➢ **Deleting a Static Address**

Method 1: In **Static IP Address List**, select a static entry to be deleted and click **Delete Selected**. In the confirmation box, click **OK**. A deletion success message is displayed and the list is updated.

Method 2: In **Static IP Address List**, click **Delete** in the last **Action** column, and click **OK** to delete the IP address.

➢ **Editing a Static Address**

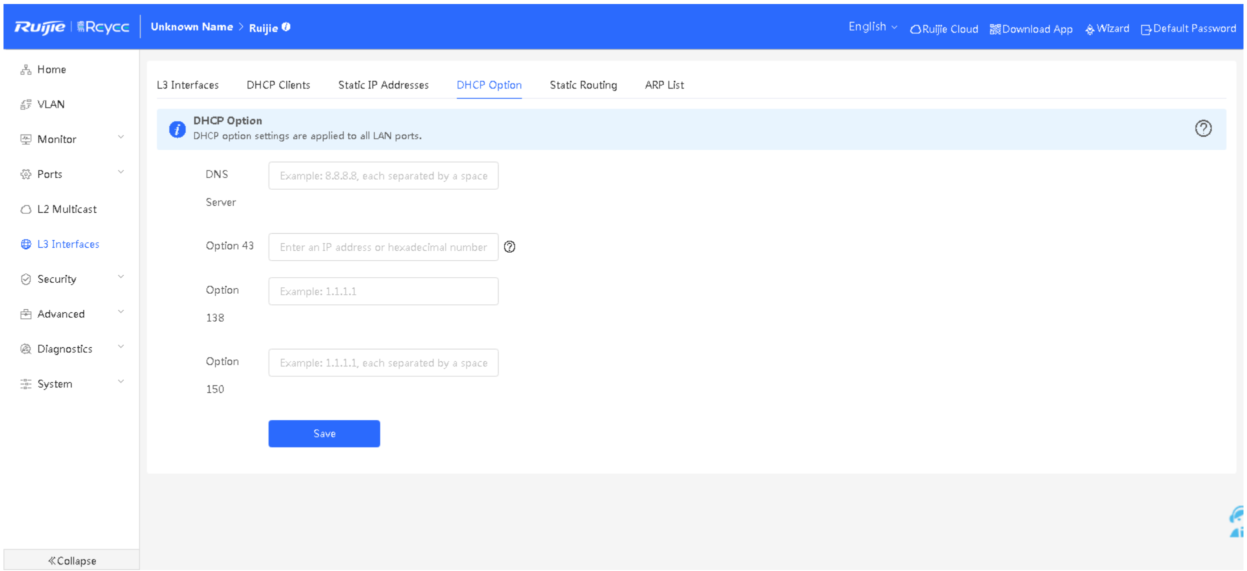
In **Static IP Address List**, click **Edit** in the **Action** column. In the displayed dialog box, modify the IP address and MAC address of the entry. Click **OK**. A configuration success message is displayed and the list is updated.

Note

A maximum of 2000 static address entries can be configured. The actual maximum number of static address entries that can be configured on a device is subject to the product specifications.

3.6.4 DHCP Option

The **DHCP Option** page allows you to configure settings to be delivered to downlink devices connected to an L3 interface when the L3 interface serves as the DHCP server. The configuration items are optional.



DHCP Option
DHCP option settings are applied to all LAN ports.

DNS Server: Example: 8.8.8.8, each separated by a space

Option 43: Enter an IP address or hexadecimal number

Option 138: Example: 1.1.1.1

Option 150: Example: 1.1.1.1, each separated by a space

Table 3-18 Settings of the DHCP Server Option

Parameter	Description	Remarks
DNS Server	DNS server address provided by an ISP. It does not need to be modified unless in special cases.	It takes effect globally.
Option 43	When an AC is connected to an AP through an L3 network, the AP cannot discover the AC in broadcast mode. Therefore, you need to configure Option 43 to be carried in DHCP response packets on the DHCP server to discover the AC.	It takes effect globally.
Option 138	In DHCP, option 138 is used to configure the DNS.	It takes effect globally.

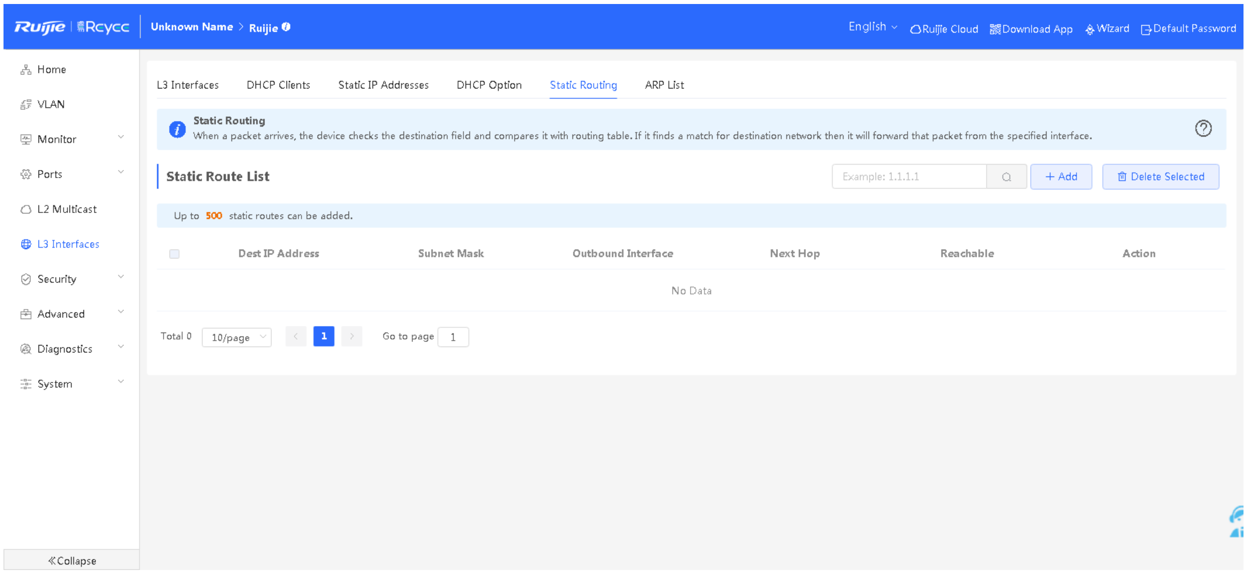
Parameter	Description	Remarks
Option 150	Address option of the TFTP server. Enter the IP address of the TFTP server to specify the TFTP server address assigned to the client.	It takes effect globally. Multiple TFTP server addresses can be configured.

Note

DHCP options are optional configuration when the device functions as an L3 DHCP server. The configuration takes effect globally and does not need to be configured by default. If no DNS server address is specified, the DNS address assigned to a downlink port is the gateway IP address.

3.6.5 Static Routing

When a packet matches a static route, the packet is forwarded in specified forwarding mode.



Static Routing

When a packet arrives, the device checks the destination field and compares it with routing table. If it finds a match for destination network then it will forward that packet from the specified interface.

Static Route List

Up to 500 static routes can be added.

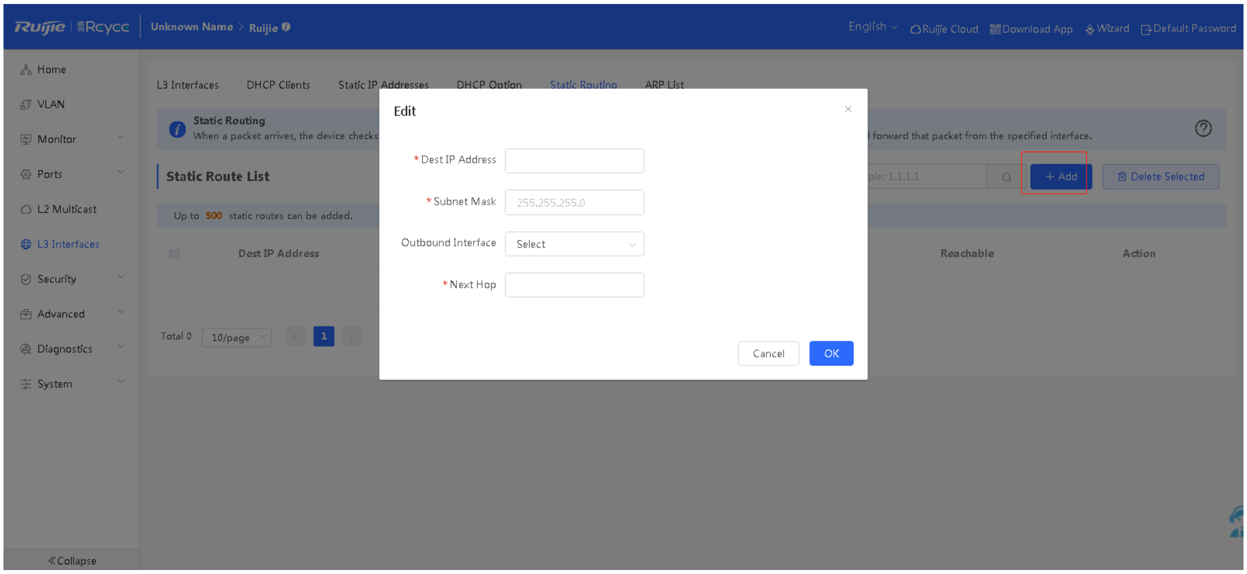
□	Dest IP Address	Subnet Mask	Outbound Interface	Next Hop	Reachable	Action
No Data						

- **Search**

Enter the IP address to be searched and click 🔍. Static route entries that meet the search criteria are displayed in the list.

- **Adding a Static Route**

Click **Add**. In the displayed dialog box, enter the destination IP address, subnet mask, next hop, select the outbound interface, and click **OK**.



Static Routing

When a packet arrives, the device checks … forward that packet from the specified interface.

Up to 500 static routes can be added.

*Dest IP Address

*Subnet Mask 255.255.255.0

Outbound Interface Select

*Next Hop

➢ Deleting a Static Route

Method 1: In **Static Route List**, select a static route entry to be deleted and click **Delete Selected**. In the confirmation box, click **OK**. A deletion success message is displayed and the list is updated.

Method 2: In **Static Route List**, click **Delete** in the last **Action** column and click **OK** in the confirmation box to delete the static route.

➢ Editing a Static Route

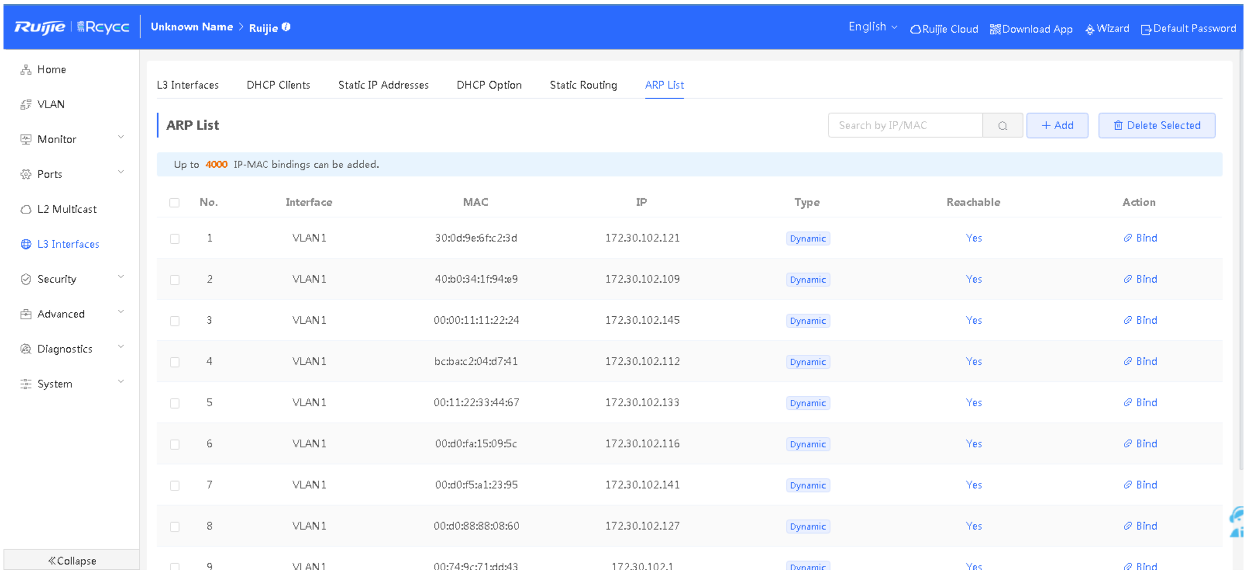
In **Static Route List**, click **Edit** in the **Action** column. In the displayed dialog box, modify the IP address, subnet mask, and next hop, select the outbound interface, and click **OK**.

Note

A maximum of 500 static route entries can be added. The actual number of static route entries supported by the device is subject to the product specifications.

3.6.6 ARP List

The device learns the IP and MAC addresses of the network devices connected to ports of the device and generates ARP entries. The **ARP List** page displays ARP entries learned by the device.



ARP List

Up to 4000 IP-MAC bindings can be added.

□	No.	Interface	MAC	IP	Type	Reachable	Action
□	1	VLAN1	30:0d:9e:6f:c2:3d	172.30.102.121	Dynamic	Yes	Bind
□	2	VLAN1	40:b0:34:1f:94:e9	172.30.102.109	Dynamic	Yes	Bind
□	3	VLAN1	00:00:11:11:22:24	172.30.102.145	Dynamic	Yes	Bind
□	4	VLAN1	bc:ba:c2:04:d7:41	172.30.102.112	Dynamic	Yes	Bind
□	5	VLAN1	00:11:22:33:44:67	172.30.102.133	Dynamic	Yes	Bind
□	6	VLAN1	00:d0:fa:15:09:5c	172.30.102.116	Dynamic	Yes	Bind
□	7	VLAN1	00:d0:f5:a1:23:95	172.30.102.141	Dynamic	Yes	Bind
□	8	VLAN1	00:d0:88:88:08:60	172.30.102.127	Dynamic	Yes	Bind
□	9	VLAN1	00:74:9c:71:dd:43	172.30.102.1	Dynamic	Yes	Bind

➢ Search

Select the search type (by MAC address or by IP address), enter the search string, and click 🔍. ARP entries that meet search criteria are displayed.

➢ Adding an ARP Entry

Method 1: Click **Add**. In the displayed dialog box, enter an IP address and a MAC address, and click **OK**.

Method 2: Click **Bind** for a dynamic ARP entry. The dynamic ARP entry is converted into a static ARP entry.

➢ Deleting an ARP Entry

Method 1: In **ARP List**, select an ARP entry to be deleted and click **Delete Selected**. In the confirmation dialog box, click **OK**. A deletion success message is displayed and the list data is updated.

Method 2: In **ARP List**, click **Delete** in the last **Action** column. The prompt "Are you sure you want to delete the entry?" is displayed. Click **OK** to complete the deletion.

➢ Editing an ARP Entry

In **ARP List**, static ARP entries can be modified. Click **Edit** in the **Action** column. In the displayed dialog box, modify the IP address and MAC address of the entry. Click **OK**. A configuration success message is displayed and the list is updated.

Note

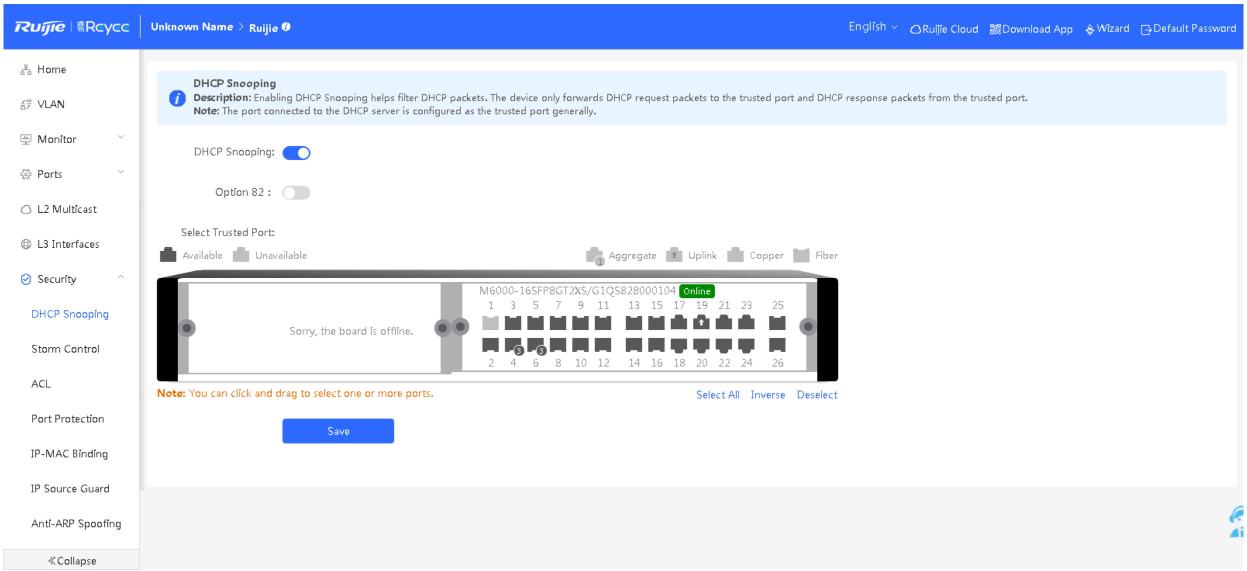
The ARP list supports a maximum of 4000 ARP entries. The actual maximum number of ARP entries that can be configured on a device is subject to the product specifications.

3.7 Security

The **Security** module allows you to configure **DHCP Snooping**, **Storm Control**, **ACL**, **Port Protection**, **IP-MAC Binding**, **IP Source Guard**, and **Anti-ARP Spoofing**.

3.7.1 DHCP Snooping

DHCP snooping snoops DHCP packets exchanged between clients and servers to record and monitor the IP addresses of users. It also filters out invalid DHCP packets, including request packets from clients and response packets from servers. DHCP snooping records generated user data entries to serve security applications such as IP Source Guard.



DHCP Snooping

Description: Enabling DHCP Snooping helps filter DHCP packets. The device only forwards DHCP request packets to the trusted port and DHCP response packets from the trusted port.

Note: The port connected to the DHCP server is configured as the trusted port generally.

DHCP Snooping: ●

Option 82 : ○

Select Trusted Port:

Sorry, the board is offline.

Note: You can click and drag to select one or more ports.

➢ **Enabling/Disabling DHCP Snooping**

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

Note

1. Generally, the port connected to the DHCP server is configured as a trusted port.

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.

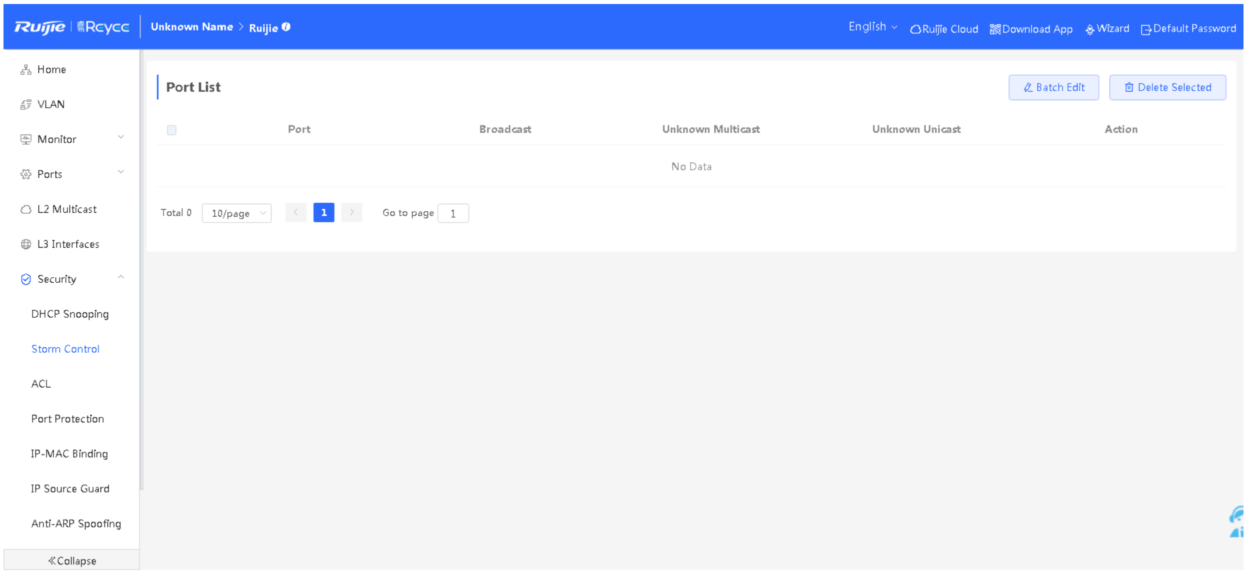
3.7.2 Storm Control

1. Overview

When there are excessive broadcast, multicast, or unknown unicast data flows in the LANs, the network speed decreases and the packet transmission timeout probability 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 bandwidth, the number of packets allowed per second, or the number of kilobits allowed per second, the device transmits packets only at the specified bandwidth, 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.

2. Configuration Steps



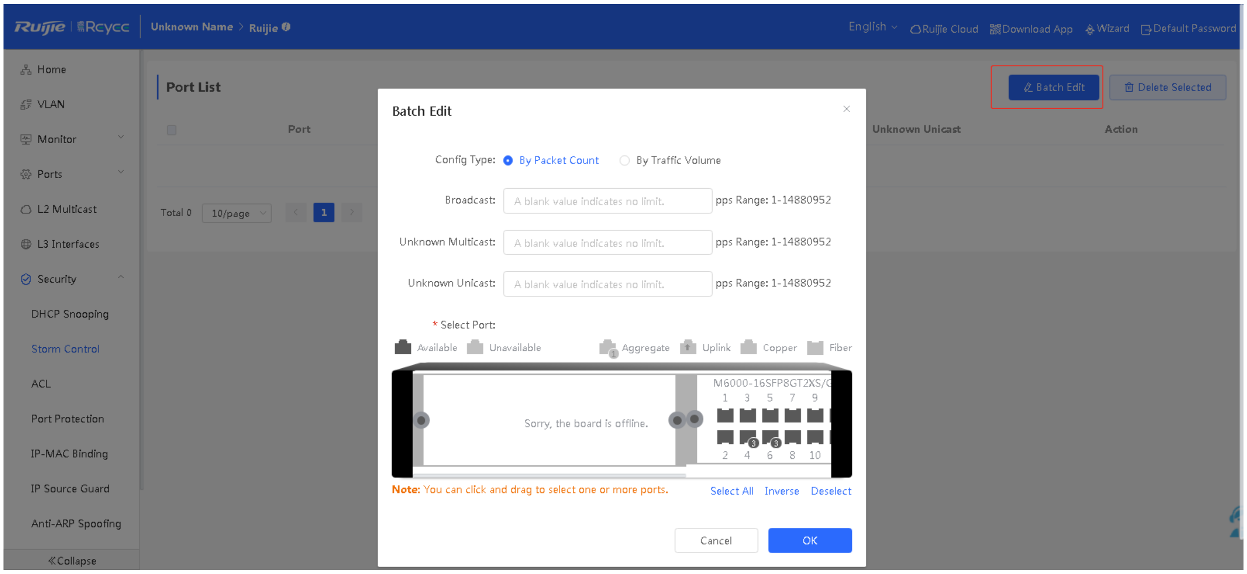
Port List

□	Port	Broadcast	Unknown Multicast	Unknown Unicast	Action
			No Data		

Total 0 10/page < 1 > Go to page 1

➢ **Adding Storm Control for a Port**

Click **Batch Edit**. In the displayed dialog box, set the configuration type, select ports, enter the broadcast, unknown unicast, and unknown multicast rate limits, and click **OK**. The configured storm control record is displayed in the storm control list.



Batch Edit

Config Type: ● By Packet Count ○ By Traffic Volume

Broadcast: A blank value indicates no limit. pps Range: 1-14880952

Unknown Multicast: A blank value indicates no limit. pps Range: 1-14880952

Unknown Unicast: A blank value indicates no limit. pps Range: 1-14880952

* Select Port:

Sorry, the board is offline.

Note: You can click and drag to select one or more ports.

Select All Inverse Deselect

Cancel OK

➢ **Editing Storm Control of a Single Port**

In **Port List**, click **Edit**. In the displayed dialog box, set the configuration type, enter the broadcast, unknown unicast, and unknown multicast rate limits, and click **OK**.

➢ **Delete Storm Control of a Port**

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

Method 2: In **Port List**, click **Delete**. In the confirmation dialog box, click **OK** to delete the data record.

Note

When the broadcast, unknown unicast, and unknown multicast rate limits are empty, the port rate is not limited.

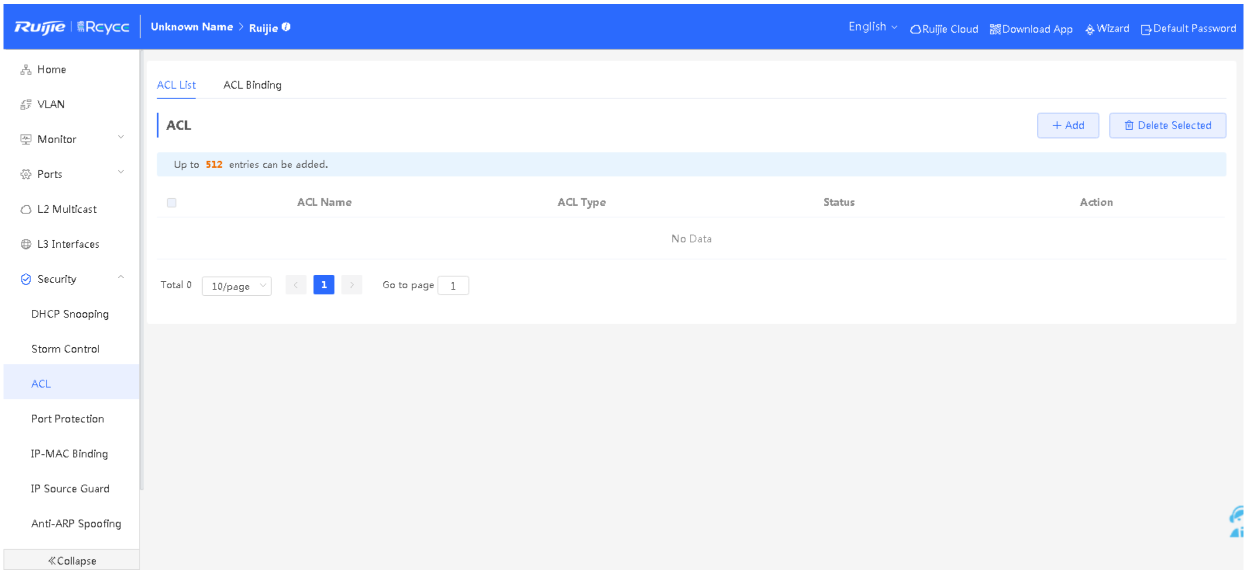
3.7.3 ACL

1. Overview

An access control list (ACL) is commonly referred to as packet filter in some documents. An ACL defines a series of permit or deny rules and applies these rules to device interfaces to control packets sent to and from the interfaces, so as to enhance security of the network device.

You can add ACLs based on MAC addresses or IP addresses and bind ACLs to ports.

2. ACL List

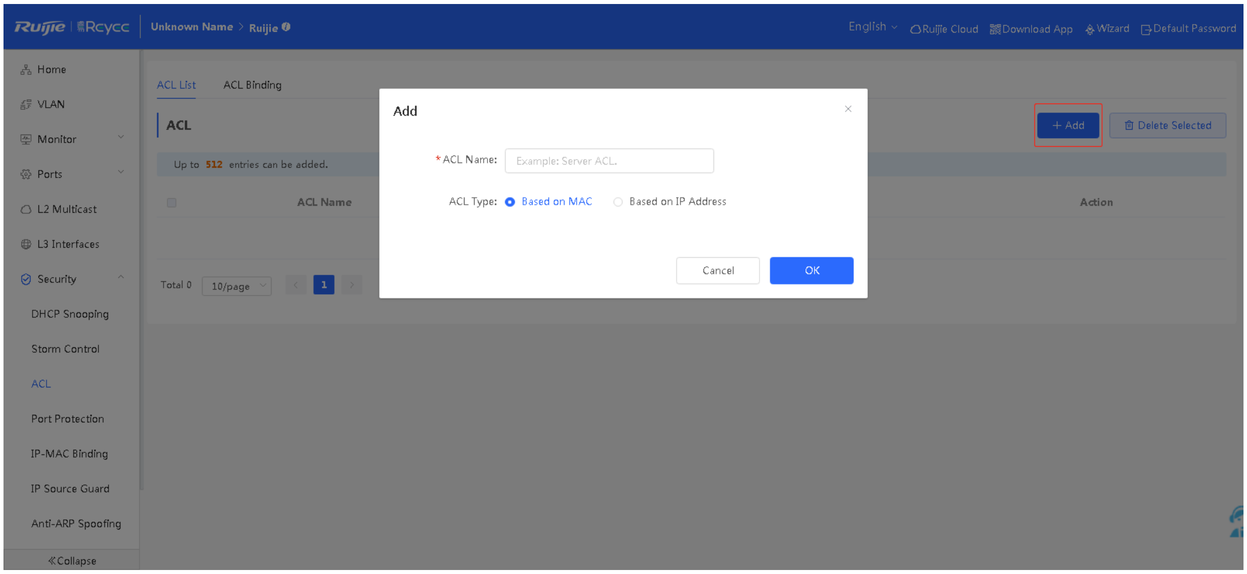


Up to 512 entries can be added.

□	ACL Name	ACL Type	Status	Action
No Data				

➢ Adding an ACL

Click **Add**. In the displayed dialog box, set the ACL control type, enter an ACL name, and click **OK** to create an ACL.



* ACL Name: Example: Server ACL.

ACL Type: ● Based on MAC ○ Based on IP Address

➢ Deleting an ACL

Select the **ACL** check box and click **Delete Selected** or click **Delete** in the **Action** column. In the confirmation box, click **OK** to Delete the ACL.

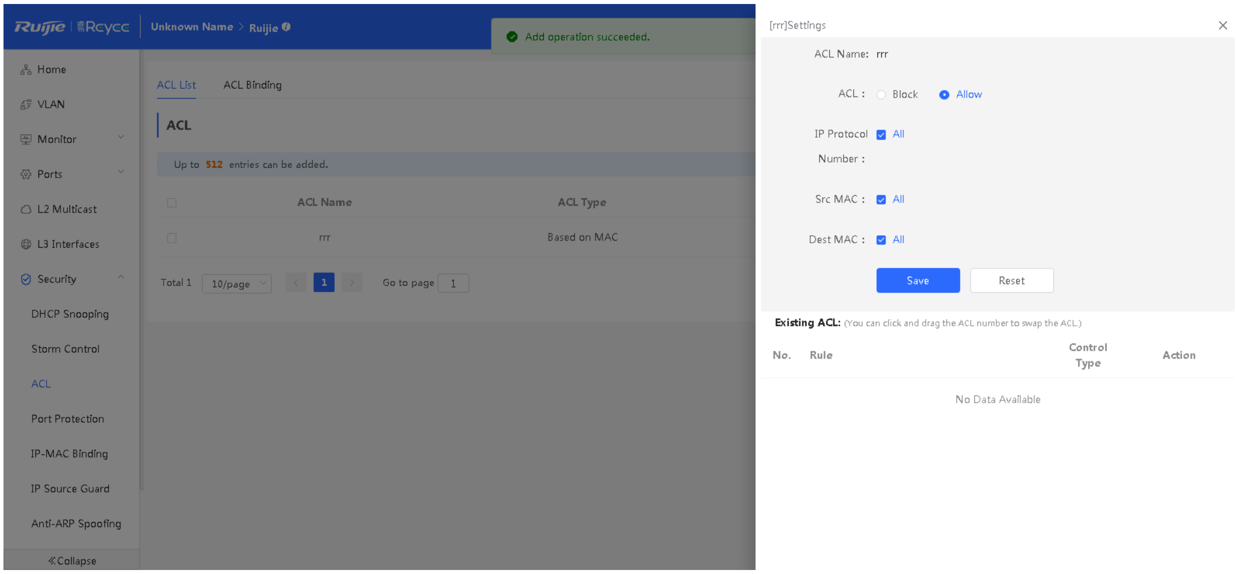
➢ Editing an ACL

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

➢ Editing ACL Rules

An access control entry (ACE) is a statement that contains the permit or deny action and a filtering rule. The sequence of an ACE in an ACL determines the matching priority of the ACE in the ACL. When processing packets, the network device matches packets with ACEs based on the ACE sequence numbers.

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



Add operation succeeded.

Up to 512 entries can be added.

□	ACL Name	ACL Type
□	rrr	Based on MAC

Total 1 10/page < 1 > Go to page 1

[rrr]Settings

ACL Name: rrr

ACL : ○ Block ● Allow

IP Protocol Number : ☑ All

Src MAC : ☑ All

Dest MAC : ☑ All

Existing ACL: (You can click and drag the ACL number to swap the ACL.)

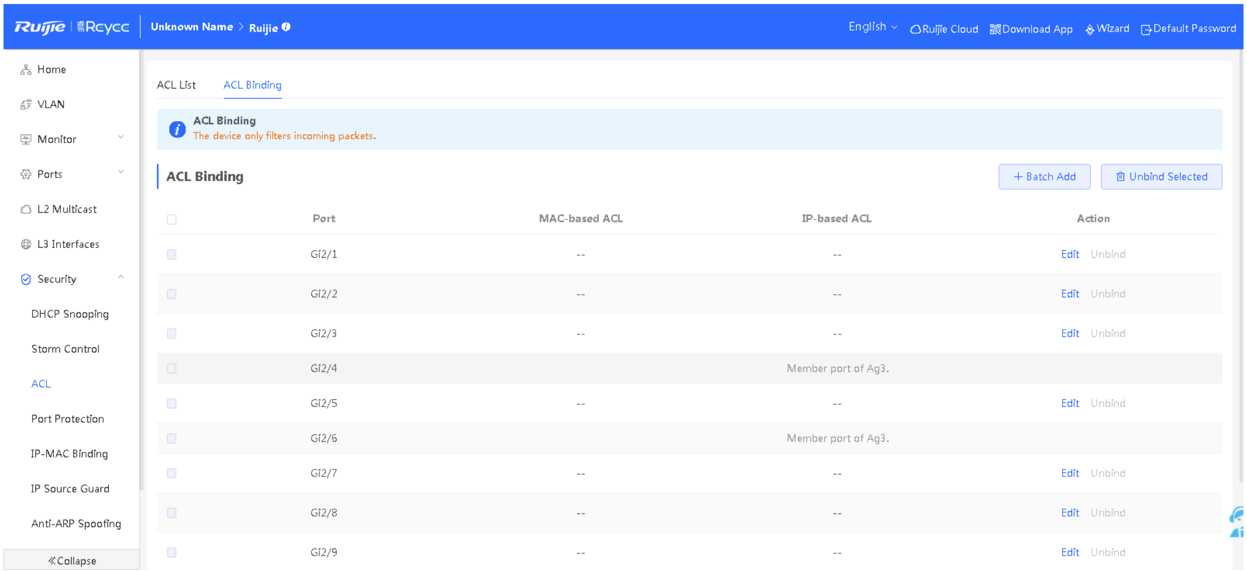
No.	Rule	Control Type	Action

No Data Available

Note

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.
4. There is one default ACE that denies all packets hidden at the end of an ACL.
5. Currently, ACLs can be applied only in the inbound direction of ports, that is, to filter incoming packets.

3. ACL Binding



ACL Binding

The device only filters incoming packets.

ACL Binding

□	Port	MAC-based ACL	IP-based ACL	Action
□	Gi2/1	--	--	Edit Unbind
□	Gi2/2	--	--	Edit Unbind
□	Gi2/3	--	--	Edit Unbind
□	Gi2/4		Member port of Ag3.	
□	Gi2/5	--	--	Edit Unbind
□	Gi2/6		Member port of Ag3.	
□	Gi2/7	--	--	Edit Unbind
□	Gi2/8	--	--	Edit Unbind
□	Gi2/9	--	--	Edit Unbind

➢ Binding an ACL

Click **Batch Add**. In the displayed dialog box, select the desired MAC ACL and IP ACL and ports, and click **OK** to bind the ACLs to the ports.

➢ Unbinding an ACL

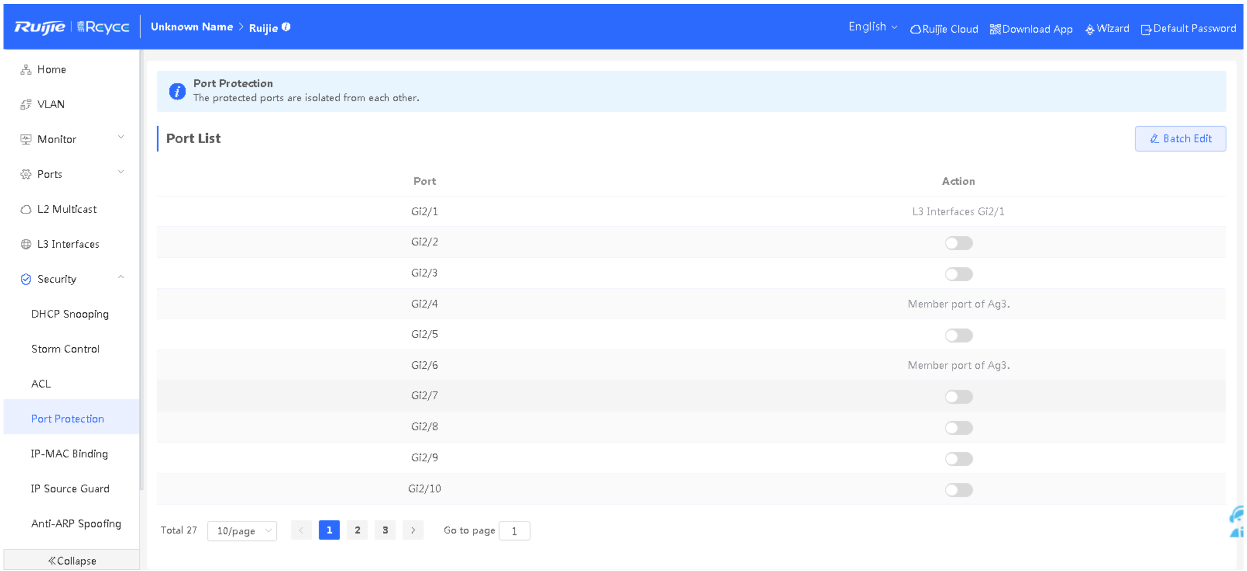
Select the **ACL Binding** check box and click **Unbind Selected** or click **Unbind** in the **Action** column. In the confirmation box, click **OK** to unbind the ACL from the port.

Note

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

3.7.4 Port Protection

When port protection is enabled, users on different ports are L2-isolated and users on protected ports cannot communicate with each other.



Port Protection

The protected ports are isolated from each other.

Port List

Port	Action
Gi2/1	L3 Interfaces Gi2/1
Gi2/2	○
Gi2/3	○
Gi2/4	Member port of Ag3.
Gi2/5	○
Gi2/6	Member port of Ag3.
Gi2/7	○
Gi2/8	○
Gi2/9	○
Gi2/10	○

Total 27 10/page < 1 2 3 > Go to page 1

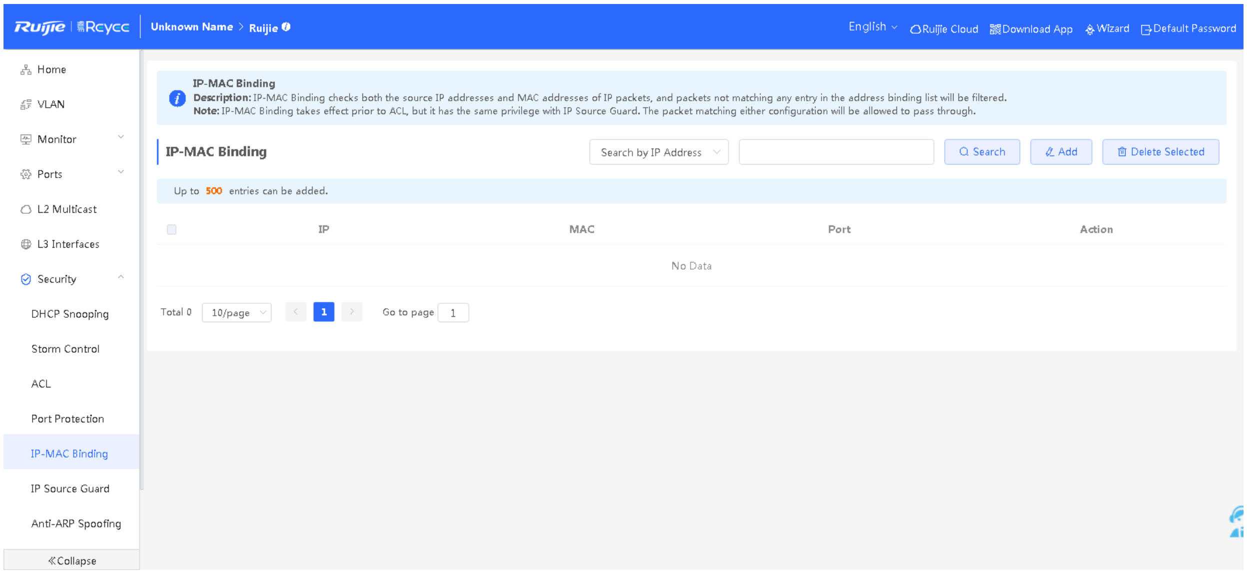
➢ **Setting Port Protection**

Method 1: Click **Batch Edit**. In the displayed dialog box, enable port protection and select the port, on which port protection needs to take effect.

Method 2: In **Port List**, click the button in **Action** column. In the confirmation box, click **OK** to configure port protection.

3.7.5 IP-MAC Binding

After IP-MAC binding is configured on a port, the device checks whether the source IP addresses and source MAC addresses of IP packets are those configured for the device, and filters out IP packets not matching the binding to strictly control the validity of input sources.



IP-MAC Binding

Description: IP-MAC Binding checks both the source IP addresses and MAC addresses of IP packets, and packets not matching any entry in the address binding list will be filtered.

Note: IP-MAC Binding takes effect prior to ACL, but it has the same privilege with IP Source Guard. The packet matching either configuration will be allowed to pass through.

IP-MAC Binding

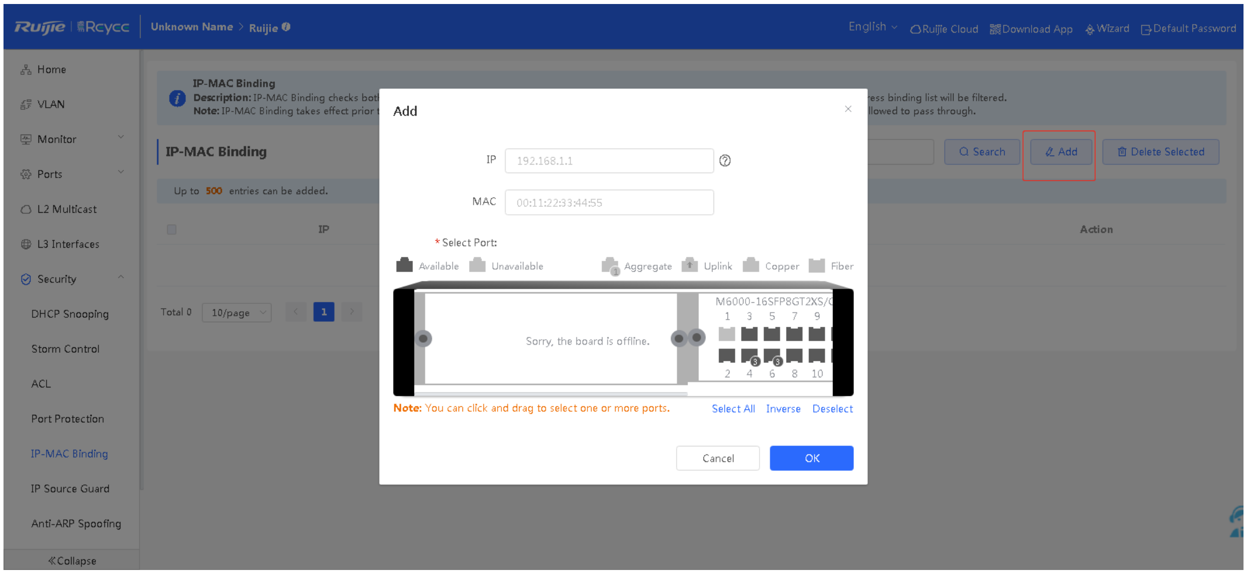
Up to 500 entries can be added.

Search

Select the search type (by MAC address, by IP address, or by port), enter the search string, and click **Search**. Entries that meet the search criteria are displayed in the list.

Adding an IP-MAC Binding Entry

Click **Add**. In the displayed dialog box, enter a MAC address and an IP address, select a port, and click **OK**.



Sorry, the board is offline.

Note: You can click and drag to select one or more ports.

Delete an IP-MAC Binding Entry

Method 1: In **IP-MAC Binding**, select a static entry to be deleted and click **Delete Selected**. In the confirmation dialog box, click **OK**. A deletion success message is displayed and the list is updated.

Method 2: In **IP-MAC Binding**, click **Delete** in the last **Action** column. The prompt "Are you sure you want to delete the entry?" is displayed. Click **OK** to complete the deletion.

➢ **Edit an IP-MAC Binding Entry**

In **IP-MAC Binding**, click **Edit** in the last **Action** column. In the displayed dialog box, modify the IP address, MAC address, and port of the entry. Click **OK**. A configuration success message is displayed and the list is updated.

⚠ **Caution**

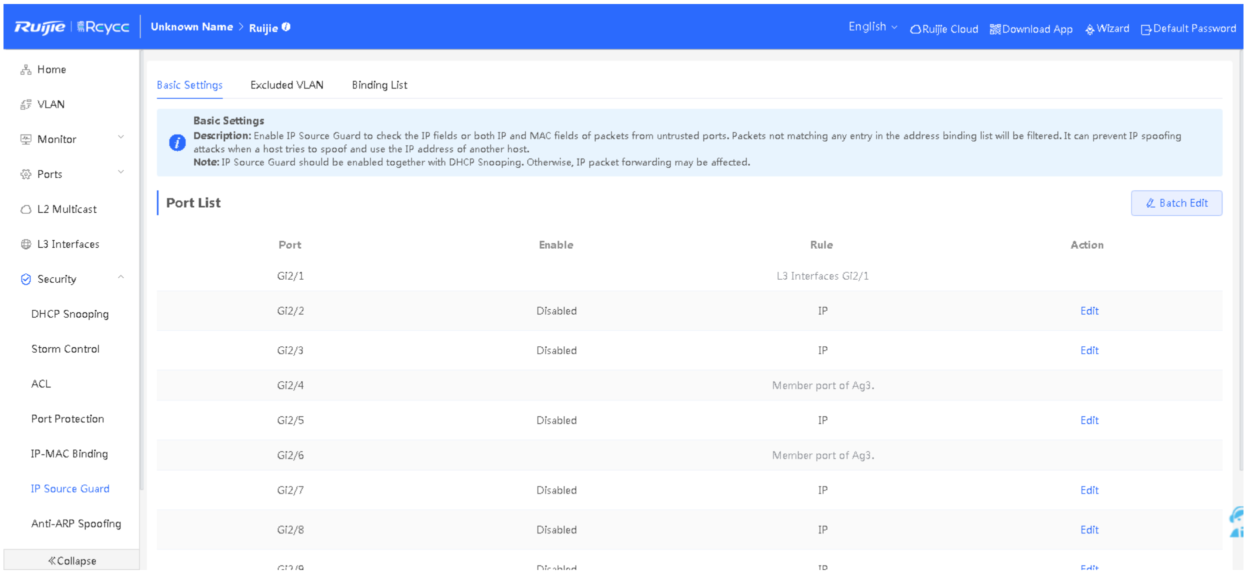
1. IP-MAC binding is prior to ACL and has the same priority as IP Source Guard. Packets are allowed to pass through as long as they meet one of the function configurations.
2. A maximum of 500 IP-MAC binding entries can be configured.

3.7.6 IP Source Guard

The **IP Source Guard** module allows you to configure ports and excluded VLANs, and view the binding list.

1. Basic Settings

After the IP Source Guard function is enabled, the device checks IP packets from DHCP non-trusted ports. You can configure the device to check only the IP field or IP+MAC field to filter out IP packets not matching the binding list. It can prevent users from setting private IP addresses and forging IP packets.



Basic Settings

Description: Enable IP Source Guard to check the IP fields or both IP and MAC fields of packets from untrusted ports. Packets not matching any entry in the address binding list will be filtered. It can prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

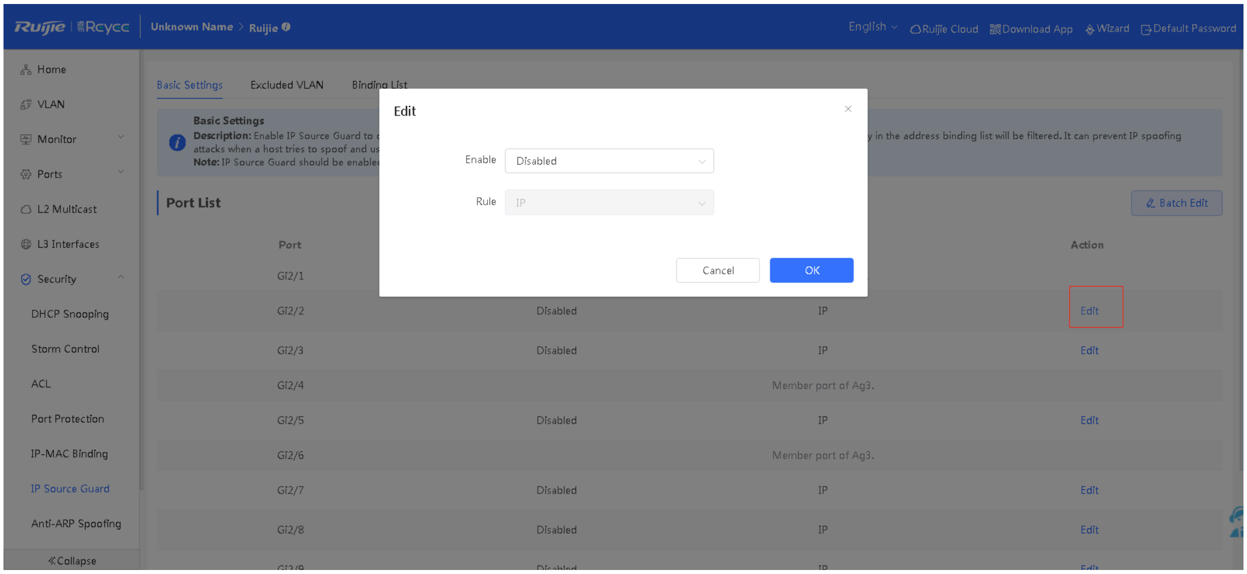
Note: IP Source Guard should be enabled together with DHCP Snooping. Otherwise, IP packet forwarding may be affected.

Port List

Port	Enable	Rule	Action
Gi2/1		L3 Interfaces Gi2/1	
Gi2/2	Disabled	IP	Edit
Gi2/3	Disabled	IP	Edit
Gi2/4		Member port of Ag3.	
Gi2/5	Disabled	IP	Edit
Gi2/6		Member port of Ag3.	
Gi2/7	Disabled	IP	Edit
Gi2/8	Disabled	IP	Edit
Gi2/9	Disabled	IP	Edit

➢ **Enabling IP Source Guard**

In **Port List**, click **Edit** in the **Action** column. In the displayed dialog box, configure whether to enable the IP Source Guard function on the port, set a matching rule (matching only IP addresses or both IP and MAC addresses), and click **OK**. A configuration success message is displayed and the port list is updated.



Basic Settings
Description: Enable IP Source Guard to c… y in the address binding list will be filtered. It can prevent IP spoofing attacks when a host tries to spoof and us…
Note: IP Source Guard should be enable…

Edit

Enable: Disabled

Rule: IP

Port List

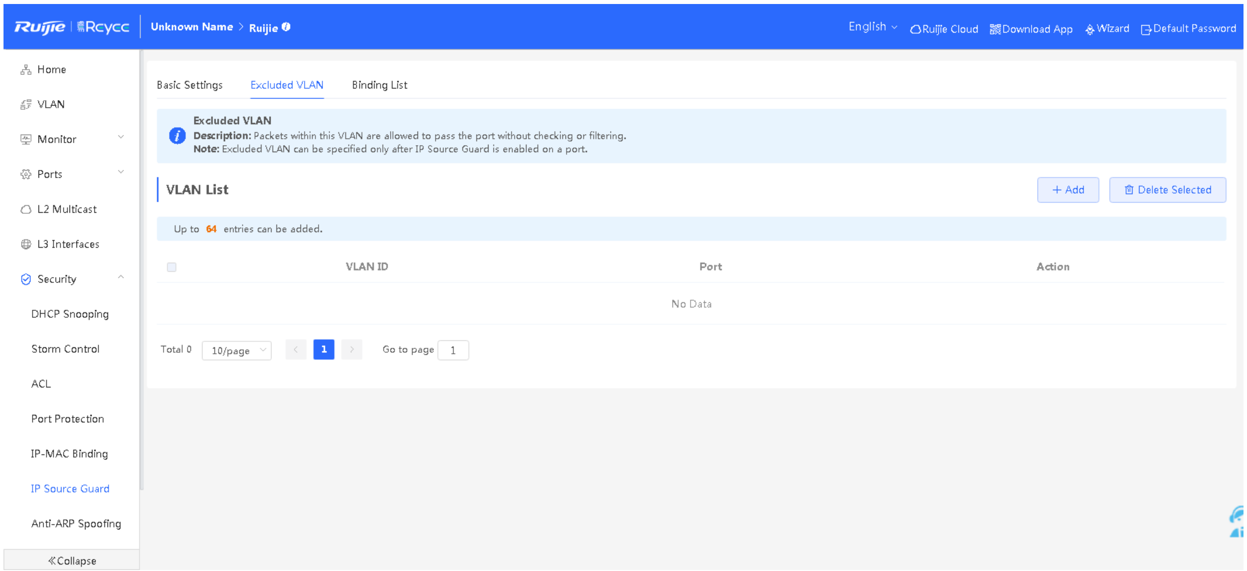
Port			Action
Gi2/1			
Gi2/2	Disabled	IP	Edit
Gi2/3	Disabled	IP	Edit
Gi2/4		Member port of Ag3.	
Gi2/5	Disabled	IP	Edit
Gi2/6		Member port of Ag3.	
Gi2/7	Disabled	IP	Edit
Gi2/8	Disabled	IP	Edit
Gi2/9	Disabled	IP	Edit

Caution

The function is usually used in combination with DHCP snooping (see 3.7.1 DHCP Snooping). Enabling IP Source Guard separately will cause an IP packet forwarding exception. Therefore, exercise caution when configuring this function.

2. Excluded VLAN

After the IP Source Guard function is enabled on a port, you can configure an excluded VLAN so that IP packets from the VLAN are not checked or filtered.



Excluded VLAN

Description: Packets within this VLAN are allowed to pass the port without checking or filtering.

Note: Excluded VLAN can be specified only after IP Source Guard is enabled on a port.

VLAN List

Up to 64 entries can be added.

□	VLAN ID	Port	Action
	No Data		

➢ Adding an Excluded VLAN

Click **Add**. In the displayed dialog box, enter a VLAN, select a port, and click **OK**. The adding success message is displayed and the list is updated.

➢ Deleting an Excluded VLAN

Method 1: In **VLAN List**, select an excluded VLAN to be deleted and click **Delete Selected**. In the confirmation dialog box, click **OK**. A deletion success message is displayed and the list is updated.

Method 2: In **VLAN List**, click **Delete** in the last **Action** column and click **OK** to delete the VLAN.

➢ Editing an Excluded VLAN

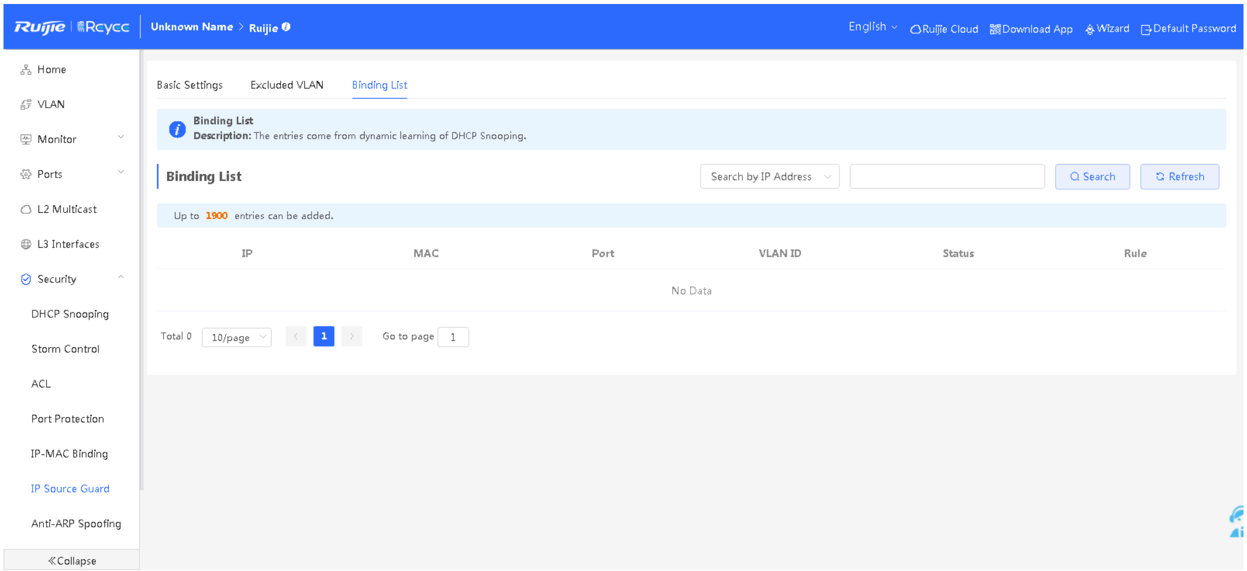
In **VLAN List**, click **Edit** in the last **Action** column. In the displayed dialog box, modify the port of the entry and click **OK**. A configuration success message is displayed and the list is updated.

Caution

1. Configure an excluded VLAN on a port, on which IP Source Guard is enabled.
2. A maximum of 64 excluded VLANs can be configured. The actual maximum number of excluded VLANs that can be configured is subject to the product specifications.

3. Binding List

Data in **Binding List** is sourced from dynamic learning results of DHCP snooping. The IP Source Guard function filters IP packets according to data in the binding list.



Binding List
Description: The entries come from dynamic learning of DHCP Snooping.

Binding List

Up to 1900 entries can be added.

IP	MAC	Port	VLAN ID	Status	Rule
No Data					

➢ Search

Select the search type (by MAC address, by IP address, by VLAN, or by port), enter the search string or select a port, and click **Search**. Entries that meet the search criteria are displayed in the list.

➢ Refresh

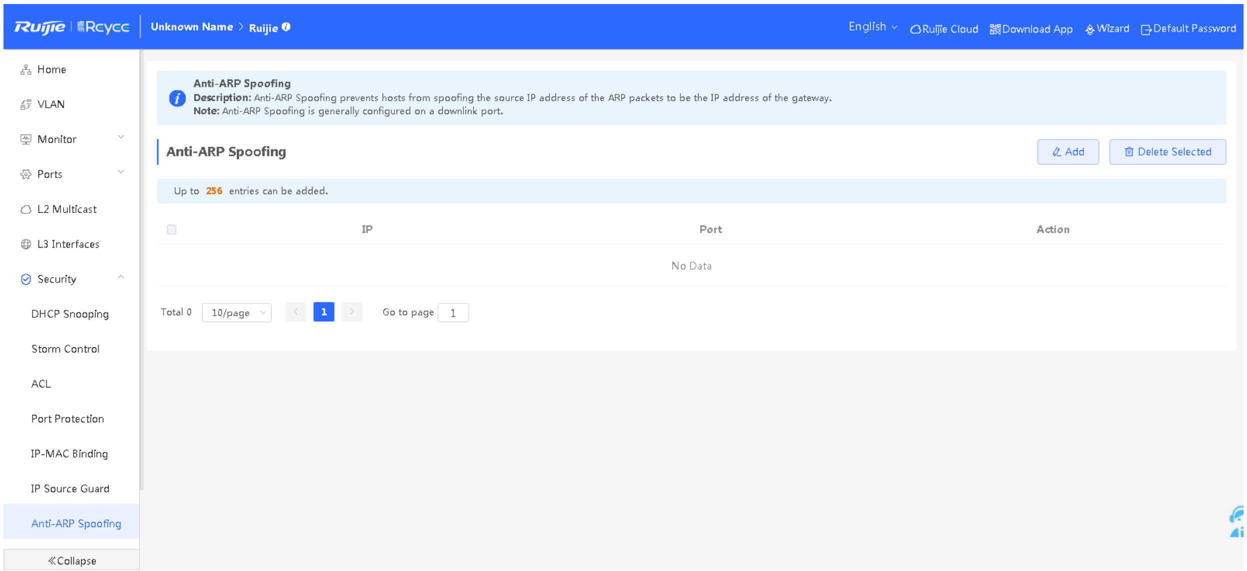
Click **Refresh** to obtain the latest DHCP snooping entries.

Note

A maximum of 1900 binding entries are supported, depending on the product specifications.

3.7.7 Anti-ARP Spoofing

After the anti-ARP spoofing function is configured, the device checks the source IP address of ARP packets on the selected port and filters out the ARP spoofing packets whose source IP addresses are the same as the configured IP address (gateway IP address) to prevent ARP spoofing on the gateway.



Anti-ARP Spoofing
Description: Anti-ARP Spoofing prevents hosts from spoofing the source IP address of the ARP packets to be the IP address of the gateway.
Note: Anti-ARP Spoofing is generally configured on a downlink port.

Anti-ARP Spoofing

Up to 256 entries can be added.

□	IP	Port	Action

No Data

➢ Adding an Anti-ARP Spoofing Entry

Click **Add**. In the displayed dialog box, enter an IP address, select a port, and click **OK**.

➢ Deleting an Anti-ARP Spoofing Entry

Method 1: In the anti-ARP spoofing list, select an entry to be deleted and click **Delete Selected**. In the confirmation dialog box, click **OK**. A deletion success message is displayed and the list is updated.

Method 2: In the anti-ARP spoofing list, click **Delete** in the last **Action** column and click **OK** to delete the entry.

➢ Editing an Anti-ARP Spoofing Entry

In the anti-ARP spoofing entry list, click **Edit** in the **Action** column. In the displayed dialog box, modify the port and IP address of the entry and click **OK**. A configuration success message is displayed and the list is updated.

Note

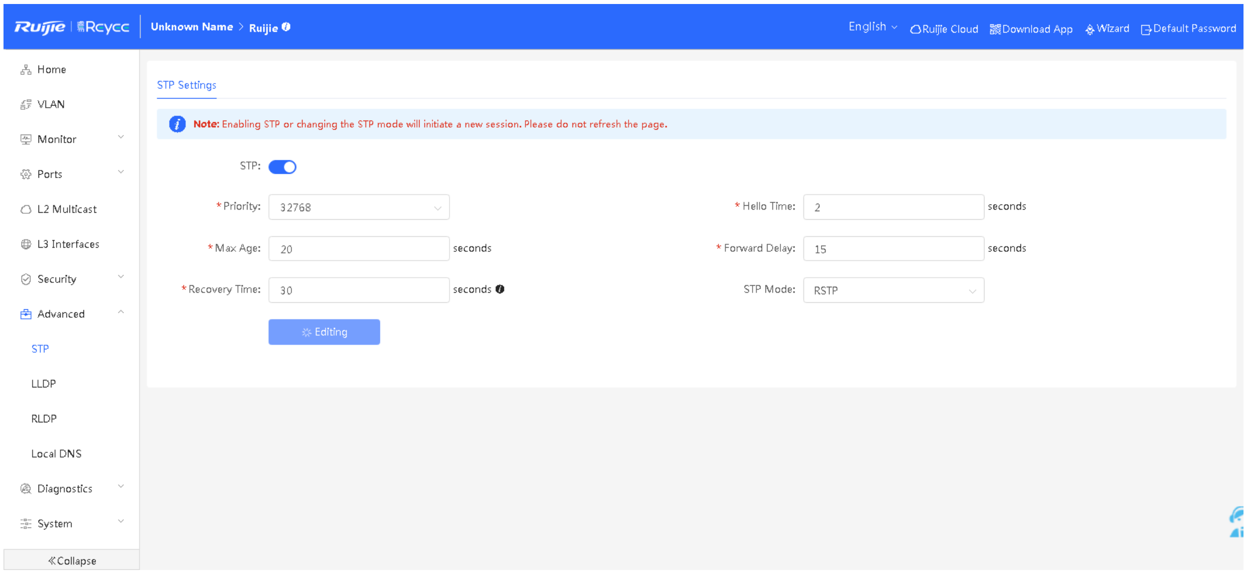
1. The anti-ARP spoofing list supports a maximum of 256 entries. The actual maximum number of supported entries is subject to the product specifications.
2. Generally, the anti-ARP spoofing function is enabled on the downlink ports of the device.

3.8 Advanced

Advanced settings include the Spanning Tree Protocol (STP), Link Layer Discovery Protocol (LLDP), Rapid Link Detection Protocol (RLDP), and local DNS settings.

3.8.1 STP

STP is an L2 management protocol that eliminates L2 loops by selectively blocking redundant links in the network. It also provides the link backup function.



Note: Enabling STP or changing the STP mode will initiate a new session. Please do not refresh the page.

STP: ●

* Priority: 32768

* Hello Time: 2 seconds

* Max Age: 20 seconds

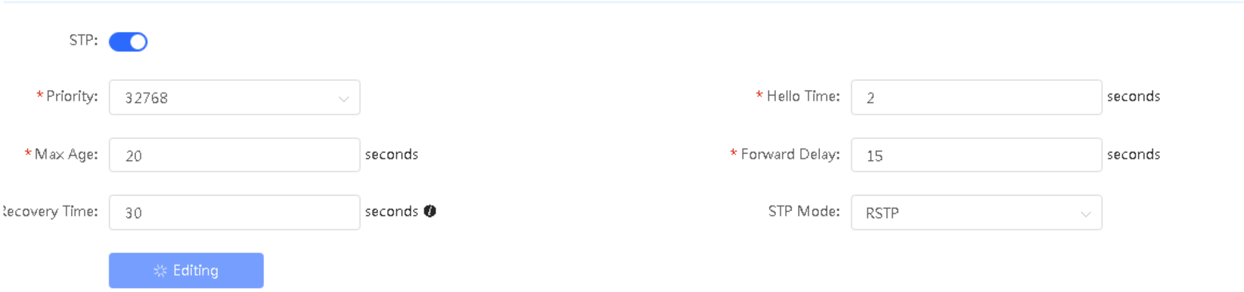
* Forward Delay: 15 seconds

* Recovery Time: 30 seconds

STP Mode: RSTP

- **Configuring STP Globally**

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



STP: ●

* Priority: 32768

* Hello Time: 2 seconds

* Max Age: 20 seconds

* Forward Delay: 15 seconds

ecovery Time: 30 seconds

STP Mode: RSTP

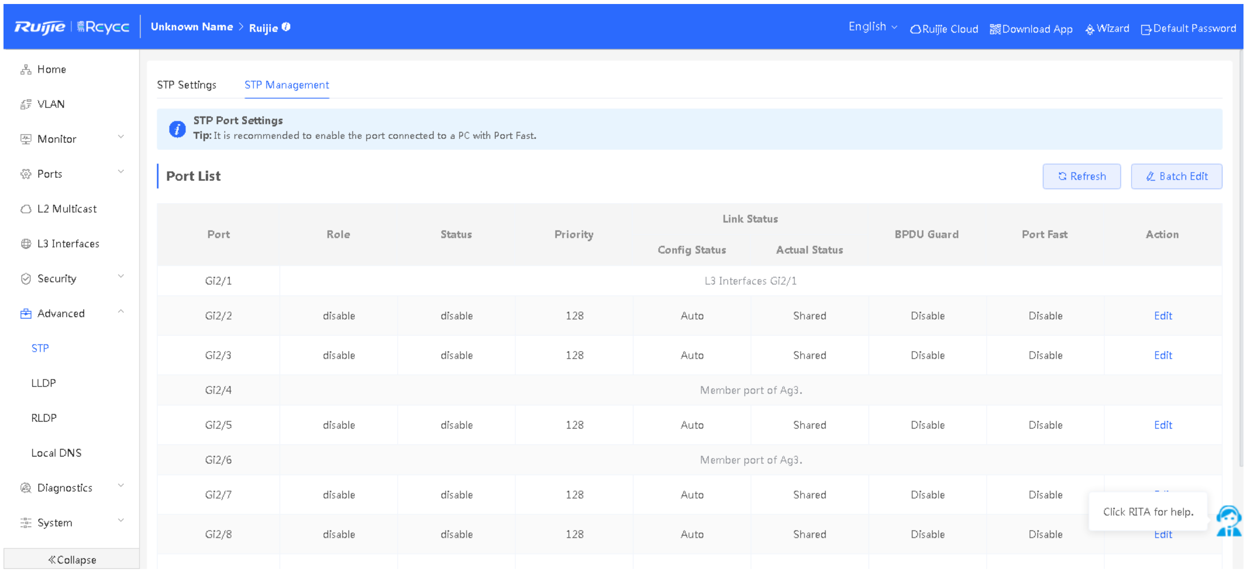
Table 3-19 STP Parameters

Parameter	Description	Default Value
STP	Whether to enable the STP function. It takes effect globally. STP attributes can be configured only after STP is enabled.	Disable
Priority	Bridge priority. The device compares the bridge priority first during root bridge selection. A smaller value indicates a higher priority.	32768

Parameter	Description	Default Value
Max Age	Entry aging time. If no new packet is received on the network, the entry will be deleted after the aging time expires.	20 seconds
Recovery Time	Network recovery time when redundant links occur on the network.	30 seconds
Hello Time	BPDU transmission interval.	2 seconds
Forward Delay	Port status change delay.	15 seconds
STP Mode	Protocol type used by redundant links. Currently, STP/RSTP is supported.	STP

- **STP Management**

Click **Batch Edit**. In the displayed dialog box, select ports and configure parameters. Alternatively, in **Port List**, click **Edit** in the **Action** column. In the displayed dialog box, configure parameters and click **OK**. Then, STP will be applied to the ports.



STP Port Settings

Tip: It is recommended to enable the port connected to a PC with Port Fast.

Port List

Port	Role	Status	Priority	Link Status		BPDU Guard	Port Fast	Action
				Config Status	Actual Status			
Gi2/1	L3 Interfaces Gi2/1							
Gi2/2	disable	disable	128	Auto	Shared	Disable	Disable	Edit
Gi2/3	disable	disable	128	Auto	Shared	Disable	Disable	Edit
Gi2/4	Member port of Ag3.							
Gi2/5	disable	disable	128	Auto	Shared	Disable	Disable	Edit
Gi2/6	Member port of Ag3.							
Gi2/7	disable	disable	128	Auto	Shared	Disable	Disable	Edit
Gi2/8	disable	disable	128	Auto	Shared	Disable	Disable	Edit

Table 3-20 STP Parameters of Ports

Parameter	Description	Default Value
Role (port role)	**Root**: A root port is located on a non-root bridge and is closest to the root switch. The root port sends data to the root bridge. It is the best path from the switch port to the root bridge. **Designated**: Designated ports are located on both non-root and root bridges. All ports on the root bridge are designated ports. For a non-root bridge, a designated port sends and receives data to and from the root switch as required. **Alternate**: An alternate port is located on a non-root bridge and is used to provide an alternate path to the root bridge, that is, an alternate port is a backup of the root port and works in blocked state in a stable topology. **Disable**: Disabled ports exist on both non-root and root bridges. They have no effect in the spanning tree.	NA
Status (port status)	**Disable**: A port in the disable state neither processes BPDU packets nor forwards other user data. The status may be caused by port initialization or port enabling and a port in this state will enter the blocking state. **Blocking**: A port in the blocking state cannot forward data packets, but can receive configuration BPDUs and send them to the CPU for processing. It cannot send configuration BPDUs or perform address learning. **Listening**: A port in the listening state does not forward data or learn addresses, but can receive and send configuration BPDUs. **Learning**: A port in the learning state cannot forward data, but starts to learn addresses, and can receive, process, and send configuration BPDUs. **Forwarding**: Once a port enters the forwarding state, it can forward any data, learn addresses, and receive, process, and send configuration BPDUs.	NA
Priority	Port priority	128
Config Status(Link Status)	Configured the link type. The options include shared, point-to-point, or auto. In auto mode, the interface type is determined based on the duplex mode. For full-duplex ports, the interface type is point-to-point, and for half-duplex ports, the interface type is shared.	Auto
Actual Status(Link Status)	Actual link type: shared or point-to-point.	Shared

Parameter	Description	Default Value
BPDU Guard	Whether to enable the BPDU guard function. After the function is enabled, if Port Fast is enabled on a port or the port is automatically identified as an edge port but the port receives BPDUs, the port will be disabled and enters the error-disabled state. This indicates that an unauthorized user may add a network device to the network, resulting in network topology change.	Disable
Port Fast	Whether to enable the Port Fast function. After Port Fast is enabled on a port, the port will neither receive nor send BPDUs. In this case, the host directly connected to the port cannot receive BPDUs. If a port, on which Port Fast is disabled exits the Port Fast state because it receives BPDUs, the BPDU filter feature is automatically disabled.	Disable

Note

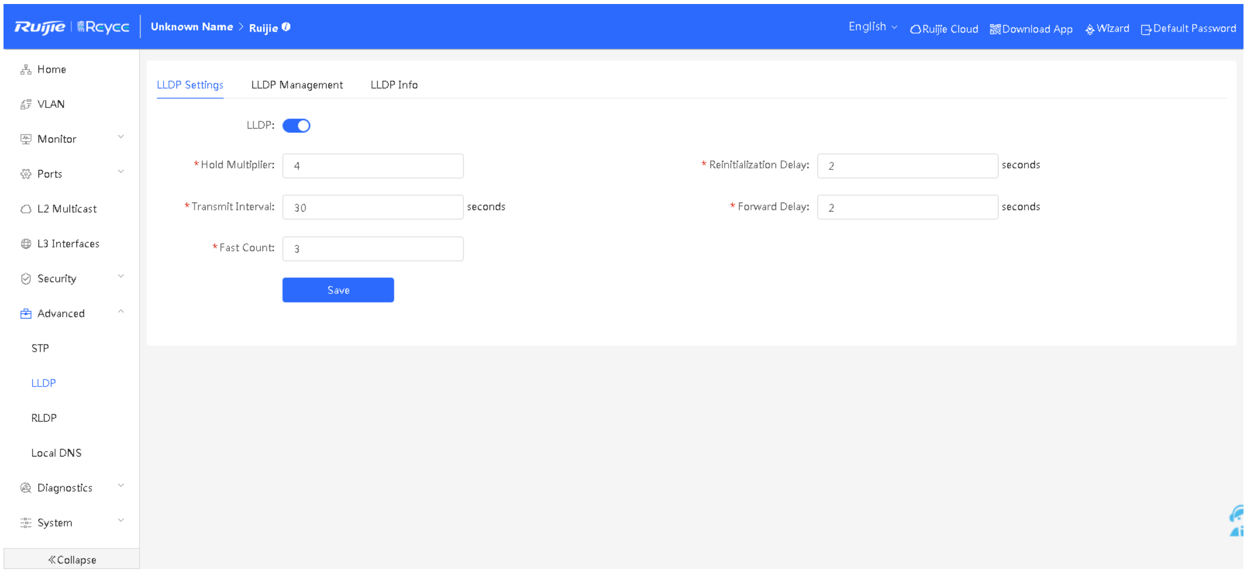
1. Enabling the STP or changing the STP mode will initiate a new session. Do not refresh the page during the configuration.
2. It is recommended to enable Port Fast on the port connected to a PC.
3. A port switches to the forwarding state more than 30 seconds after STP is enabled. Therefore, transient disconnection occurs (no packets are forwarded).

3.8.2 LLDP

1. Overview

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.

2. LLDP Settings



LLDP: ●

*Hold Multiplier: 4

*Transmit Interval: 30 seconds

*Fast Count: 3

*Reinitialization Delay: 2 seconds

*Forward Delay: 2 seconds

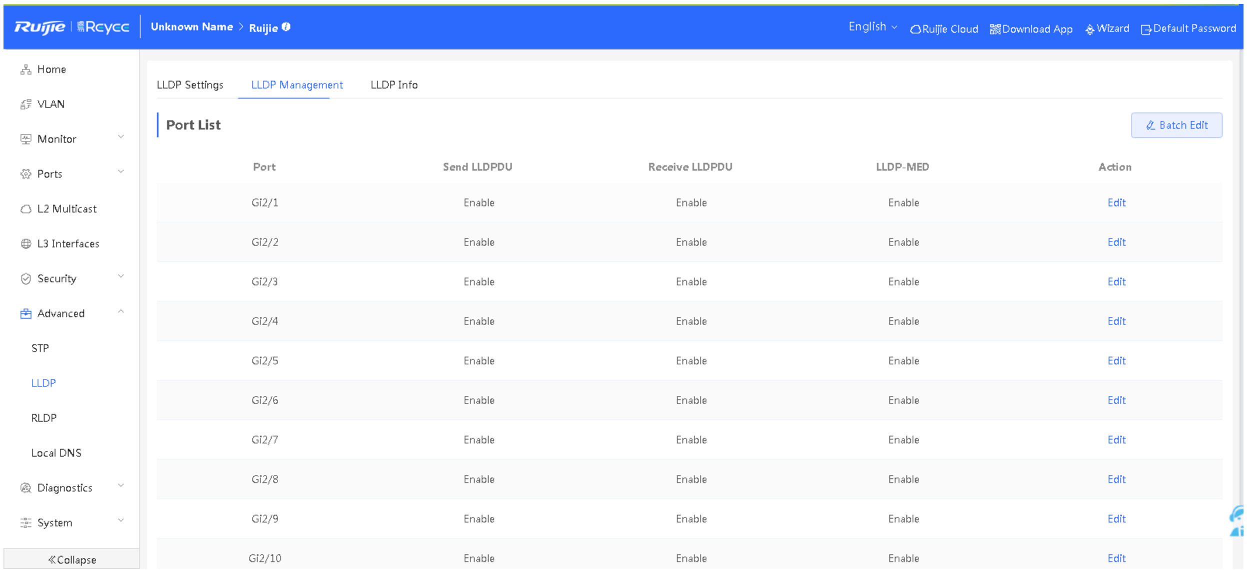
Table 3-21 LLDP Parameters

Parameter	Description	Default Value
LLDP	Whether to enable the LLDP function	Enable
Hold Multiplier	TTL multiplier of LLDP	4
Transmit Interval	Transmission interval of LLDP packets, in seconds	30 seconds
Fast Count	Number of sent packets	3
Reinitialization Delay	Port initialization delay, in seconds	2 seconds
Forward Delay	Delay for sending LLDP packets, in seconds	2 seconds

➢ Configuring LLDP

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

3. LLDP Management

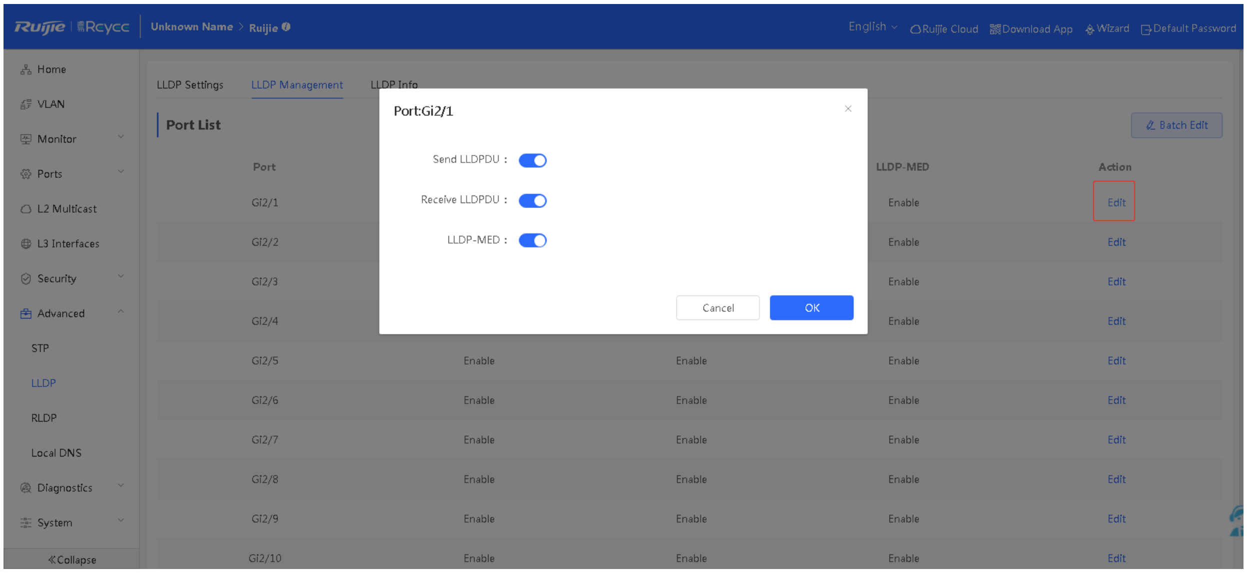


Port List

Port	Send LLDPDU	Receive LLDPDU	LLDP-MED	Action
Gi2/1	Enable	Enable	Enable	Edit
Gi2/2	Enable	Enable	Enable	Edit
Gi2/3	Enable	Enable	Enable	Edit
Gi2/4	Enable	Enable	Enable	Edit
Gi2/5	Enable	Enable	Enable	Edit
Gi2/6	Enable	Enable	Enable	Edit
Gi2/7	Enable	Enable	Enable	Edit
Gi2/8	Enable	Enable	Enable	Edit
Gi2/9	Enable	Enable	Enable	Edit
Gi2/10	Enable	Enable	Enable	Edit

➢ Applying LLDP to a Port

Click **Batch Edit**. In the displayed dialog box, select a port and configure parameters. Alternatively, in **Port List**, click **Edit** in the **Action** column. In the displayed dialog box, configure whether to enable the LLDP MED function on the port, whether the port can receive or send LLDPDUs, and click **OK**. Then, LLDP will be applied to the port.



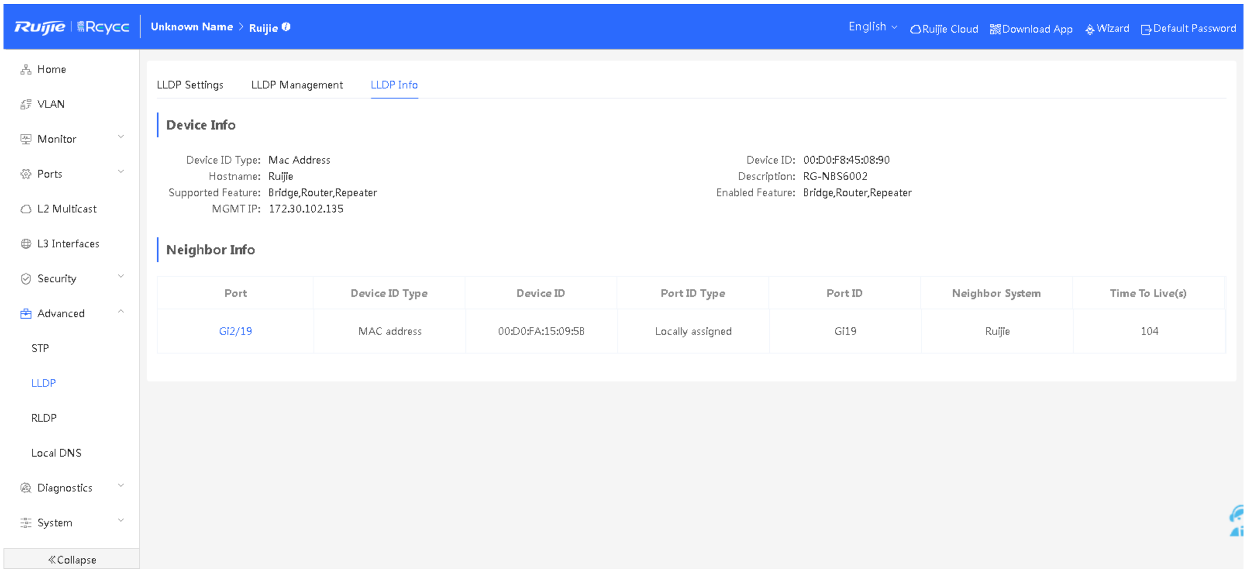
Port:Gi2/1

Send LLDPDU : ●

Receive LLDPDU : ●

LLDP-MED : ●

4. LLDP Info



Device Info

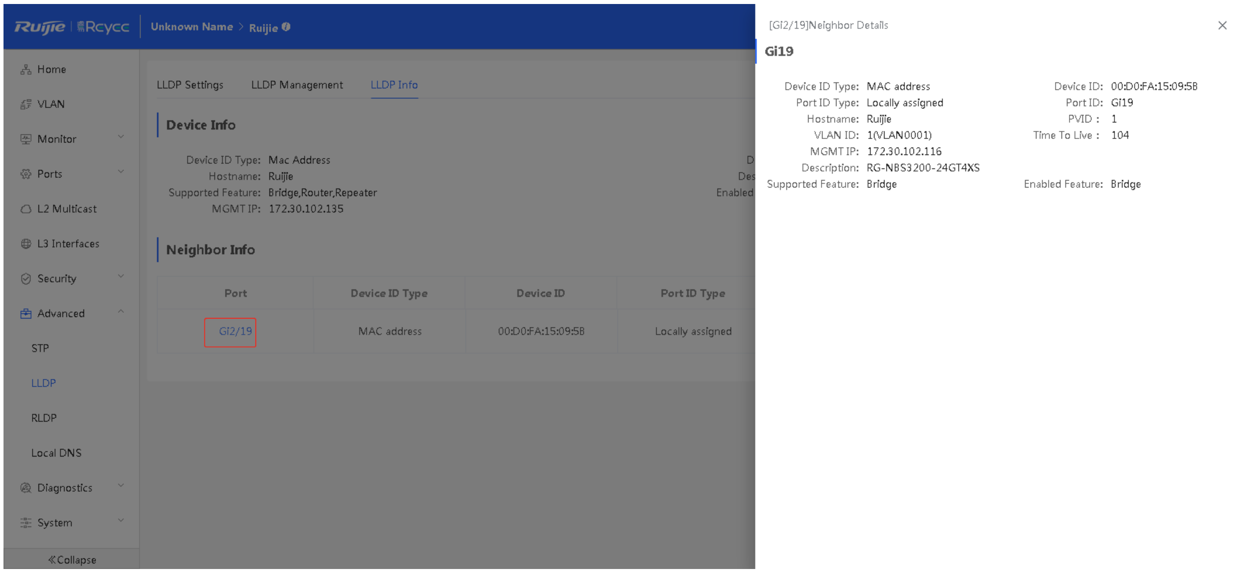
Device ID Type: Mac Address
Hostname: Ruijie
Supported Feature: Bridge,Router,Repeater
MGMT IP: 172.30.102.135
Device ID: 00:D0:F8:45:08:90
Description: RG-NBS6002
Enabled Feature: Bridge,Router,Repeater

Neighbor Info

Port	Device ID Type	Device ID	Port ID Type	Port ID	Neighbor System	Time To Live(s)
Gi2/19	MAC address	00:D0:FA:15:09:58	Locally assigned	Gi19	Ruijie	104

➢ LLDP Device Info

Device Info displays information about the current device and the neighbor information of each port. You can click a port name to display details about neighbors of the port.



[Gi2/19]Neighbor Details

Gi19

Device ID Type: MAC address
Port ID Type: Locally assigned
Hostname: Ruijie
VLAN ID: 1(VLAN0001)
MGMT IP: 172.30.102.116
Description: RG-NBS3200-24GT4XS
Supported Feature: Bridge
Device ID: 00:D0:FA:15:09:58
Port ID: Gi19
PVID : 1
Time To Live : 104
Enabled Feature: Bridge

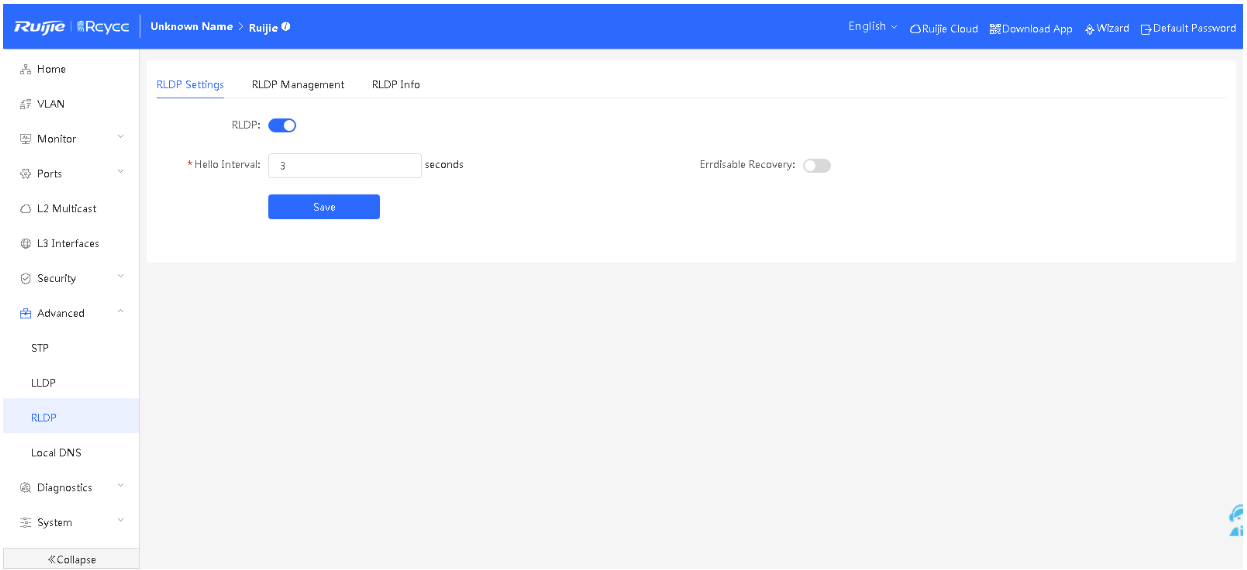
Note

1. LLDP can be used to display the topological connection status, for example, information about the switch devices, 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 switch devices are directly connected in the network topology.

3.8.3 RLDP

RLDP allows users to quickly detect link faults on Ethernet devices, including loop faults. Link faults include unidirectional link faults and bidirectional link faults.

1. RLDP Settings



RLDP: ●

* Hello Interval: 3 seconds

Errdisable Recovery: ○

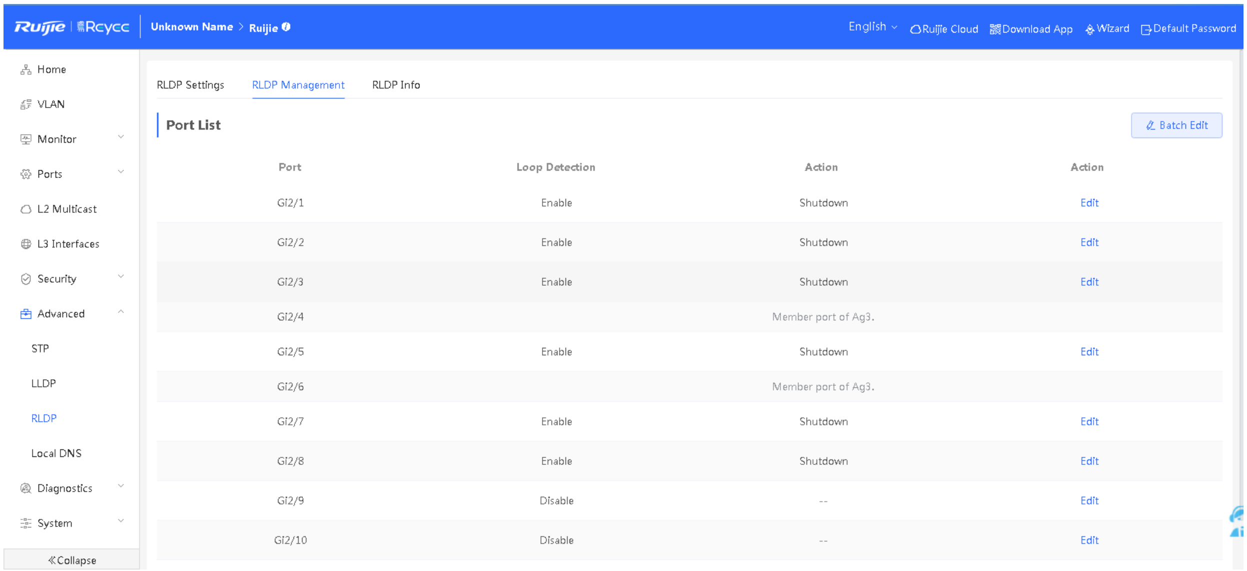
Table 3-22 RLDP Parameters of Ports

Parameter	Description	Default Value
RLDP	Whether to enable the RLDP function	Disable
Hello Interval	Interval for RLDP to send detection packets, in seconds	3 seconds
Errdisable Recovery	After it is enabled, a port automatically recovers after a loop occurs.	Disable
Errdisable Recovery Interval	Automatic recovery time after a loop occurs on a port, in seconds	30 seconds

➢ **Configuring RLDP**

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

2. RLDP Management



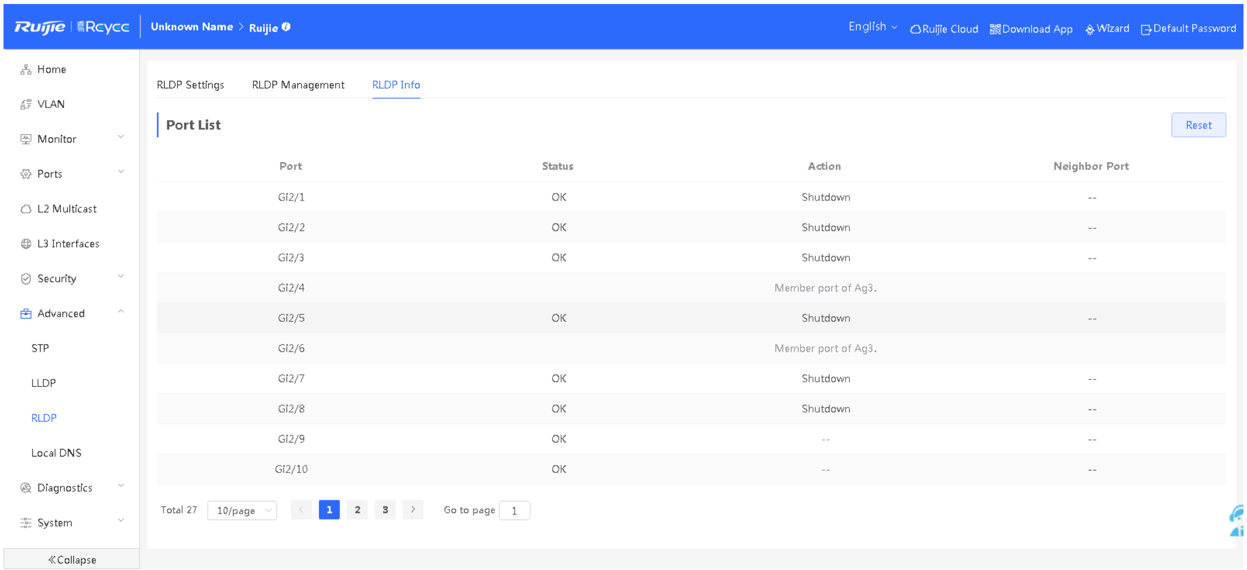
Port List

Port	Loop Detection	Action	Action
Gi2/1	Enable	Shutdown	Edit
Gi2/2	Enable	Shutdown	Edit
Gi2/3	Enable	Shutdown	Edit
Gi2/4		Member port of Ag3.	
Gi2/5	Enable	Shutdown	Edit
Gi2/6		Member port of Ag3.	
Gi2/7	Enable	Shutdown	Edit
Gi2/8	Enable	Shutdown	Edit
Gi2/9	Disable	--	Edit
Gi2/10	Disable	--	Edit

➢ Applying RLDP to a Port

Click **Batch Edit**. In the displayed dialog box, select a port. Alternatively, in **Port List**, click **Edit** in the **Action** column. In the displayed dialog box, configure whether to enable loop detection on the port and the processing mode after a link fault is detected (including warning block shutdown), and click **OK**. Then, RLDP is applied to the port.

3. RLDP Info



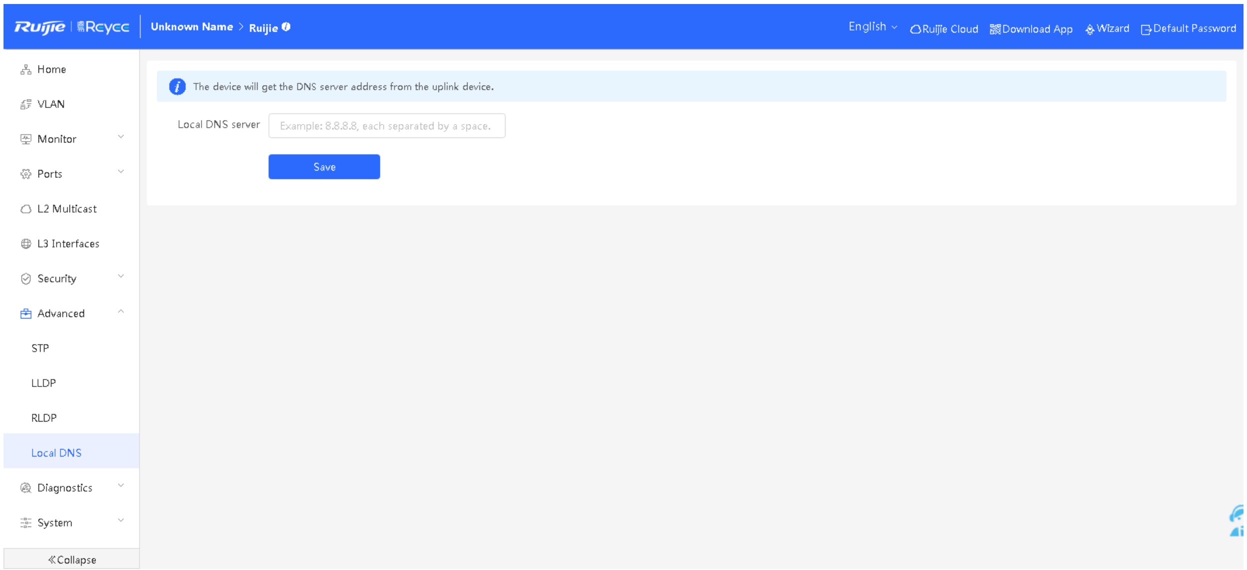
Port List

Port	Status	Action	Neighbor Port
Gi2/1	OK	Shutdown	--
Gi2/2	OK	Shutdown	--
Gi2/3	OK	Shutdown	--
Gi2/4		Member port of Ag3.	
Gi2/5	OK	Shutdown	--
Gi2/6		Member port of Ag3.	
Gi2/7	OK	Shutdown	--
Gi2/8	OK	Shutdown	--
Gi2/9	OK	--	--
Gi2/10	OK	--	--

Total 27 10/page < 1 2 3 > Go to page 1

RLDP Info displays the RLDP processing information of ports on the current device and the status of each port. You can click **Reset** to restore the RLDP status triggered by a port to the normal state.

3.8.4 Local DNS



The device will get the DNS server address from the uplink device.

Local DNS server: Example: 8.8.8.8, each separated by a space.

➢ Configuring DNS

Enter the IP address of the DNS server and click **Save**.

Note

1. The local DNS server configuration is not mandatory. The device obtains the DNS server address from the connected uplink device by default.
2. After configuration, packets first use the DNS of the management IP address for parsing and then use this DNS.

3.8.5 Voice VLAN

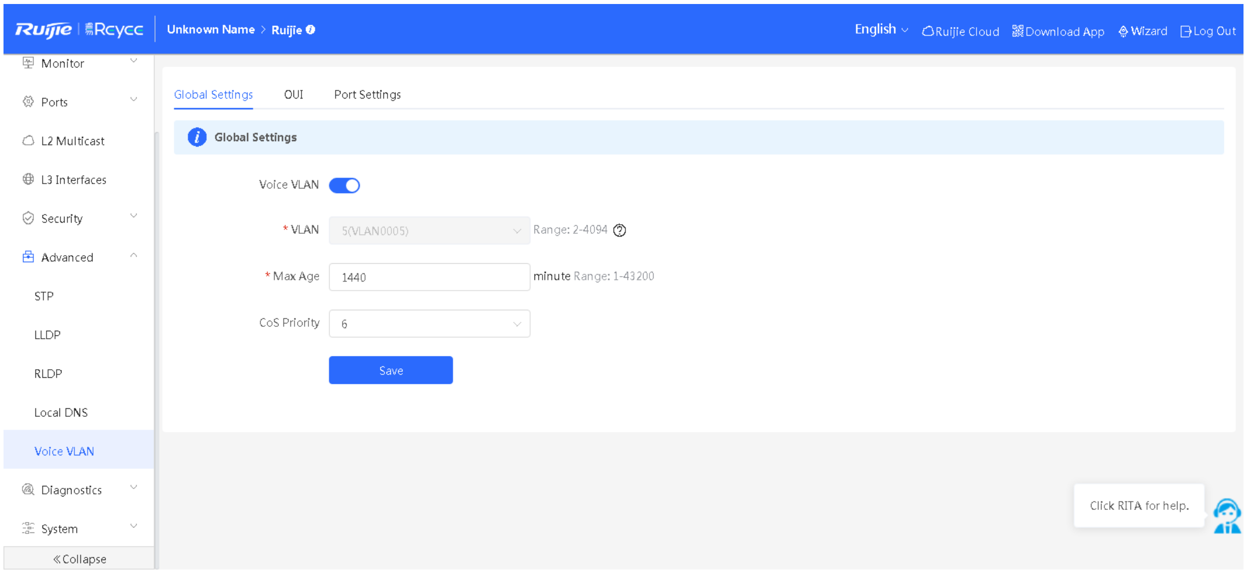
Note

The voice VLAN function is supported by NBS3100, NBS3200, and NBS5000.

1. Overview

The voice VLAN is specially classified for voice data flows. By creating a voice VLAN and adding ports connected to voice devices to the voice VLAN, you can have voice data transmitted in the voice VLAN and configure the quality of service (QoS) for voice streams, to improve the transmission priority of voice traffic and ensure the call quality.

2. Global Settings



Global Settings

Voice VLAN: enabled

* VLAN: 5(VLAN0005) Range: 2-4094

* Max Age: 1440 minute Range: 1-43200

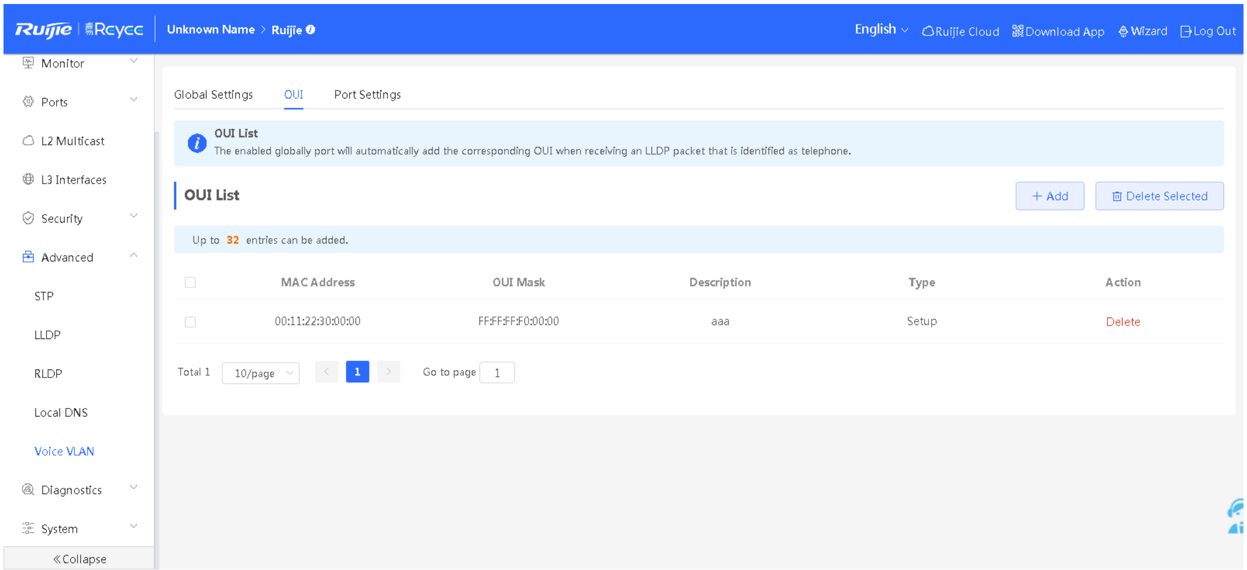
CoS Priority: 6

➢ Configuring Voice VLAN Globally

Enable the voice VLAN function, configure parameters, and click **Save** to configure the voice VLAN globally.

3. OUI

The source MAC address of a voice packet contains the organizationally unique identifier (OUI) of the voice device manufacturer. After the voice VLAN OUI is configured, the device compares the voice VLAN OUI with the source MAC address in a received packet to identify voice data packets, and sends them to the voice VLAN for transmission.



OUI List

The enabled globally port will automatically add the corresponding OUI when receiving an LLDP packet that is identified as telephone.

OUI List

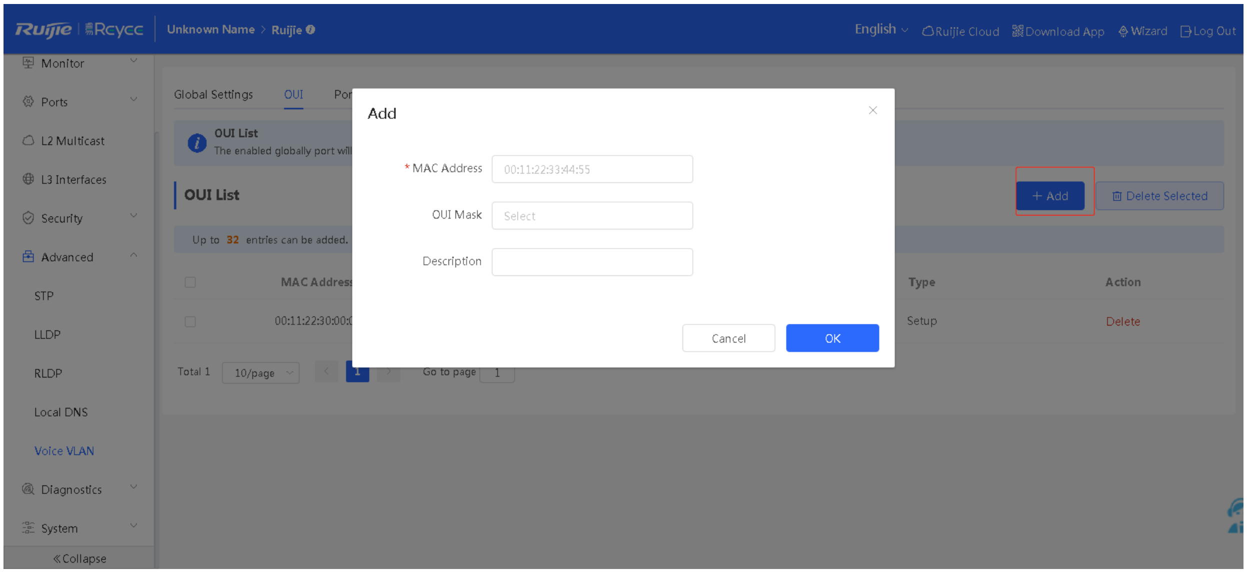
Up to 32 entries can be added.

□	MAC Address	OUI Mask	Description	Type	Action
□	00:11:22:30:00:00	FF:FF:FF:F0:00:00	aaa	Setup	Delete

Total 1 10/page < 1 > Go to page 1

➢ Adding an OUI

Click **Add**. In the displayed dialog box, enter an MAC address, select the mask of the MAC address, and click **OK** to add an OUI entry.



➢ Deleting an OUI

Select a check box on the left and click **Delete Selected** or click **Delete** in the **Action** column. In the confirmation box, click **OK** to delete the OUI entry.

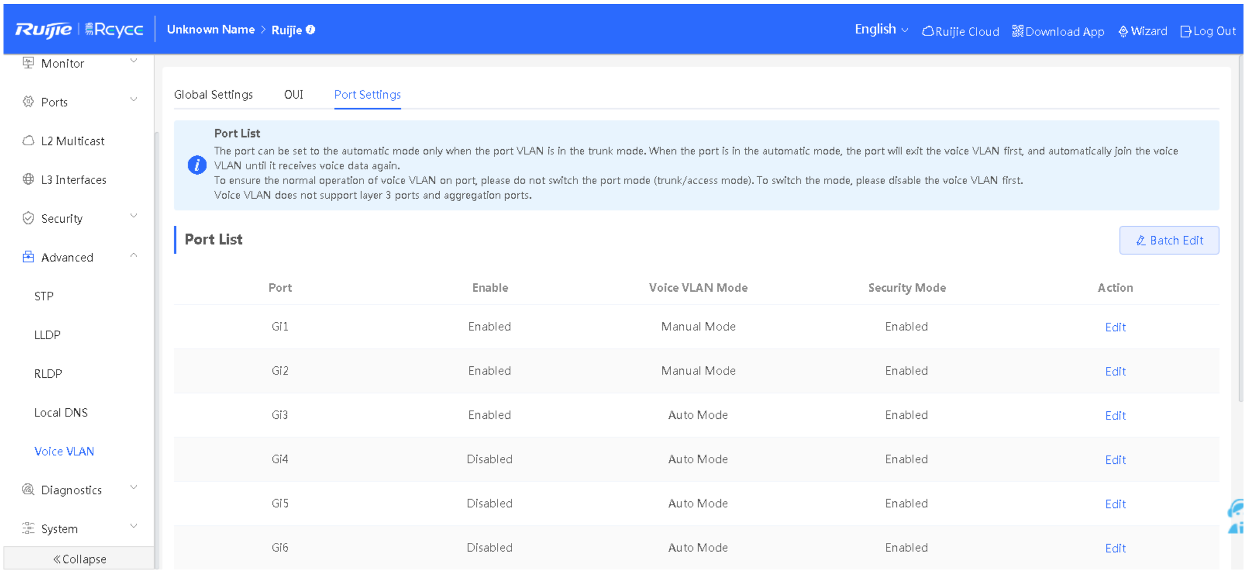
➢ Editing an OUI

Click **Edit** in the **Action** column of the list. In the displayed dialog box, modify the OUI description click **OK** to modify the OUI.

Note

After the voice VLAN function is enabled on a port, the device can capture LLDP packets sent by IP phones, identify the device capability fields in the packets, and identify the devices with the capability of Telephone as voice devices. After that, the device extracts the source MAC address of a protocol packet and processes it as the MAC address of the voice device. In this way, the OUI can be added automatically.

4. Port Settings



Port List

The port can be set to the automatic mode only when the port VLAN is in the trunk mode. When the port is in the automatic mode, the port will exit the voice VLAN first, and automatically join the voice VLAN until it receives voice data again.

To ensure the normal operation of voice VLAN on port, please do not switch the port mode (trunk/access mode). To switch the mode, please disable the voice VLAN first.

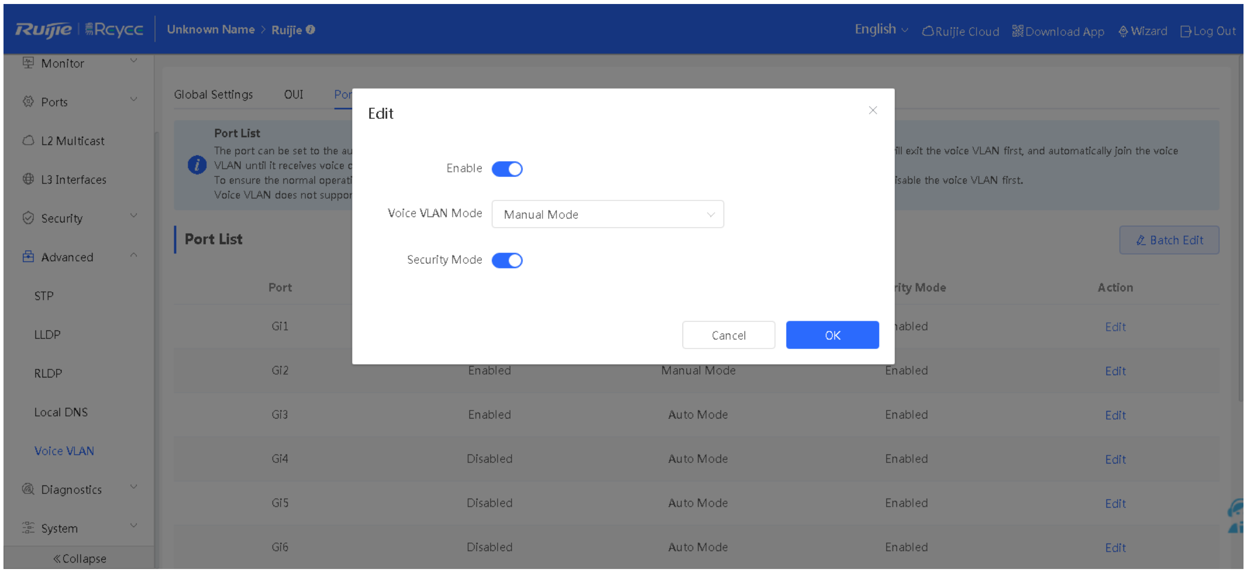
Voice VLAN does not support layer 3 ports and aggregation ports.

Port List

Port	Enable	Voice VLAN Mode	Security Mode	Action
Gi1	Enabled	Manual Mode	Enabled	Edit
Gi2	Enabled	Manual Mode	Enabled	Edit
Gi3	Enabled	Auto Mode	Enabled	Edit
Gi4	Disabled	Auto Mode	Enabled	Edit
Gi5	Disabled	Auto Mode	Enabled	Edit
Gi6	Disabled	Auto Mode	Enabled	Edit

➢ Enabling the Voice VLAN Function on a Port

Click **Edit** on the right of a port or click **Batch Edit**. In the displayed dialog box, select whether to enable the voice VLAN function on the port, voice VLAN mode to be applied, and whether to enable the security mode. Click **OK** to change the port settings.



Enable: ●
Voice VLAN Mode: Manual Mode
Security Mode: ●

Auto Mode: In this mode, the device checks whether the permit VLANs of a port contain the voice VLAN after the voice VLAN function is enabled on the port. If yes, the device deletes the voice VLAN from the permit VLANs of the port until the port receives a voice packet containing a specified OUI. Then, the device automatically adds the voice VLAN to the port's permit VLANs. If the port does not receive a voice packet containing the specified OUI within the global aging time, the device removes the Voice VLAN from the permit VLANs of the port.

Manual Mode: If the permit VLANs of a port contains the voice VLAN, voice packets can be transmitted in the voice VLAN.

Security Mode: When the security mode is enabled, the voice VLAN is allowed to transmit only voice streams. The device checks the source MAC addresses of packets. If the source MAC address of a packet is within the range of the voice VLAN OUI entries, the packet can be transmitted in the voice VLAN. Otherwise, the packet is discarded. When the security mode is disabled, the source MAC addresses of packets are not checked and all packets can be transmitted in the voice VLAN.

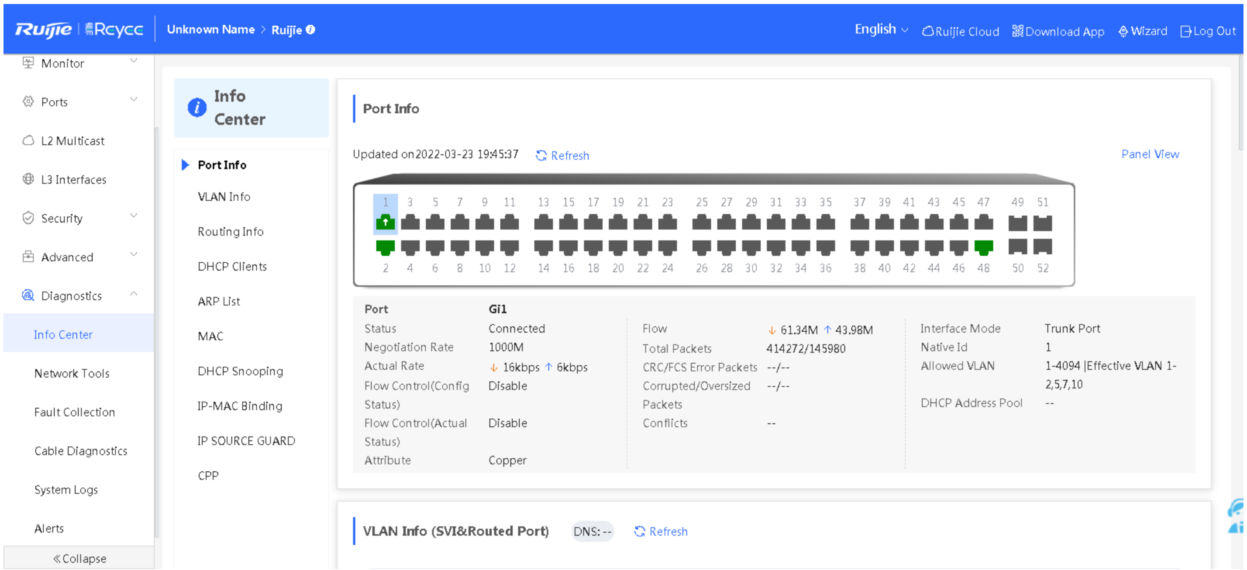
Note

1. The auto mode can be configured only when the VLAN of a port works in trunk mode. If auto mode is configured for a port, the port exits the voice VLAN first and is automatically added to the voice VLAN only after receiving voice data.
2. After the voice VLAN function is enabled on a port, do not switch the L2 mode (trunk or access mode) of the port to ensure normal operation of the function. If you need to switch the L2 mode of the port, disable the voice VLAN function on the port first.
3. The voice VLAN function is unavailable on L3 ports or aggregate ports.

3.9 Diagnostics

3.9.1 Info Center

In **Info Center**, you can view port traffic, VLAN information, routing information, client list, ARP list, MAC address, DHCP snooping status, IP-MAC binding status, IP Source Guard status, and CPP status of the device and relevant configurations.



Port Info

Updated on2022-03-23 19:45:37

Port	Gi1				
Status	Connected	Flow	↓ 61.34M ↑ 43.98M	Interface Mode	Trunk Port
Negotiation Rate	1000M	Total Packets	414272/145980	Native Id	1
Actual Rate	↓ 16kbps ↑ 6kbps	CRC/FCS Error Packets	--/--	Allowed VLAN	1-4094 |Effective VLAN 1-2,5,7,10
Flow Control(Config Status)	Disable	Corrupted/Oversized Packets	--/--	DHCP Address Pool	--
Flow Control(Actual Status)	Disable	Conflicts	--		
Attribute	Copper				

VLAN Info (SVI&Routed Port) DNS: --

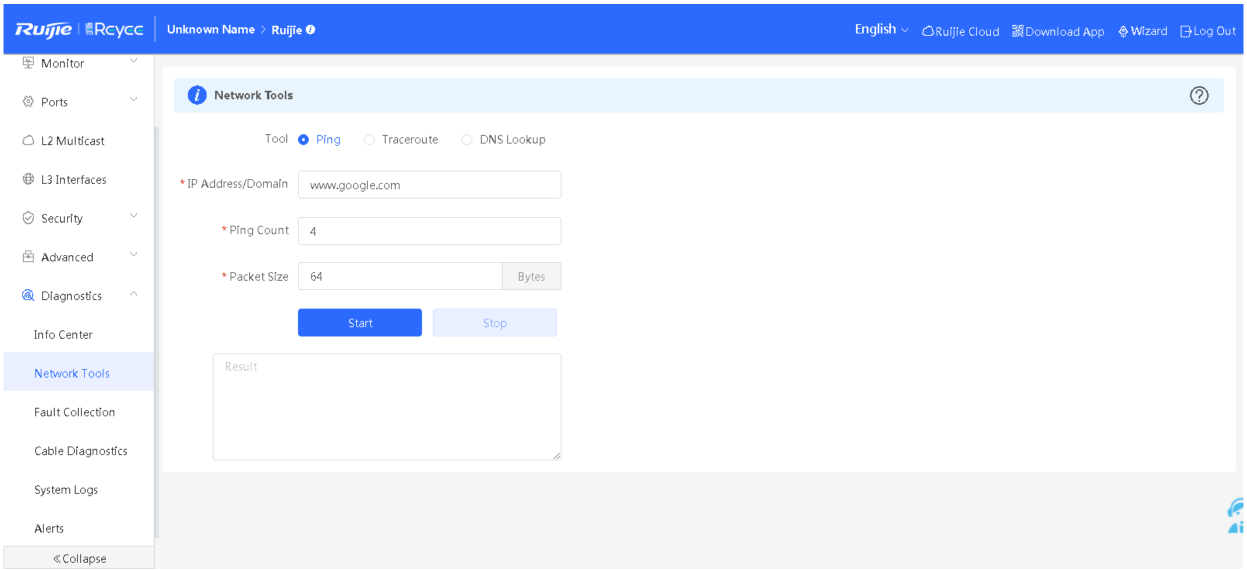
3.9.2 Network Tools

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

1. Ping

The ping command is used to detect the network connectivity.

Select **Ping** as the diagnosis mode, enter the destination IP address or website address, configure the ping count and packet size, and click **Start** to test the network connectivity between the device and the IP address or website. If "Ping failed" is displayed, the device is not reachable to the IP address or website.



Tool ● Ping ○ Traceroute ○ DNS Lookup

*IP Address/Domain: www.google.com

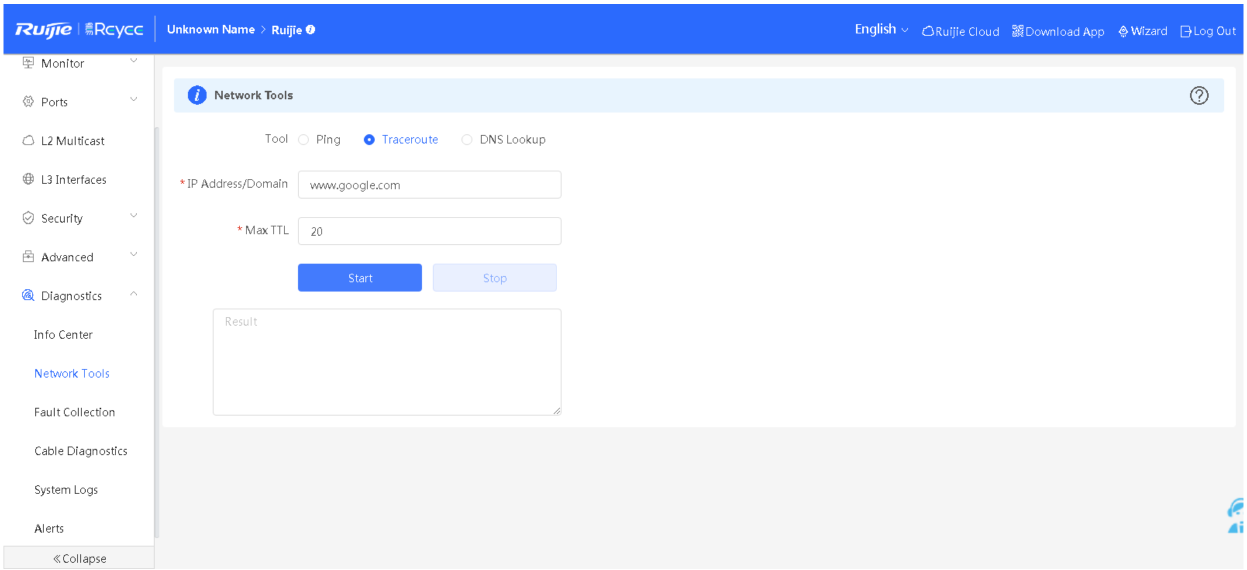
*Ping Count: 4

*Packet Size: 64 Bytes

2. Traceroute

The traceroute function is used to identify the network path from one device to another. On a simple network, the network path may pass through only one routing node or none at all. On a complex network, packets may pass through dozens of routing nodes before reaching their destination. The traceroute function can be used to judge the transmission path of data packets during communication.

Detection page and result of "Traceroute":



Tool ○ Ping ● Traceroute ○ DNS Lookup

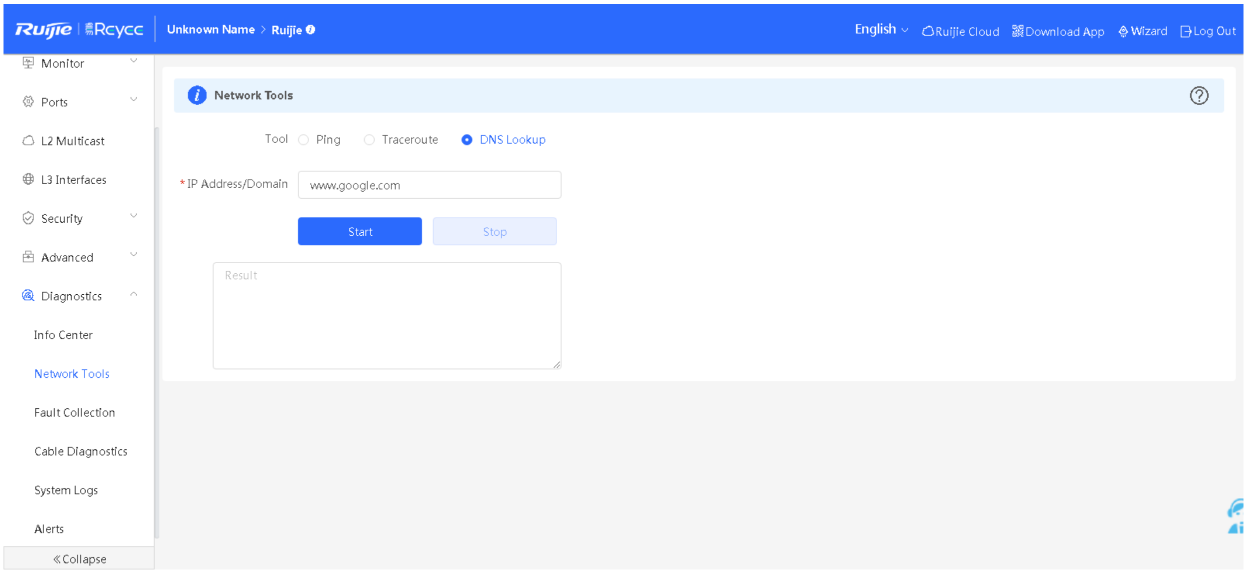
*IP Address/Domain: www.google.com

*Max TTL: 20

3. DNS Lookup

The DNS lookup function is used to query DNS records, check whether domain name resolution is normal, and diagnose network faults. If you can ping through the IP address of the Internet from your web page but the browser cannot open the web page, you can use the DNS lookup function to check whether domain name resolution is normal.

Detection page and result of "DNS lookup":

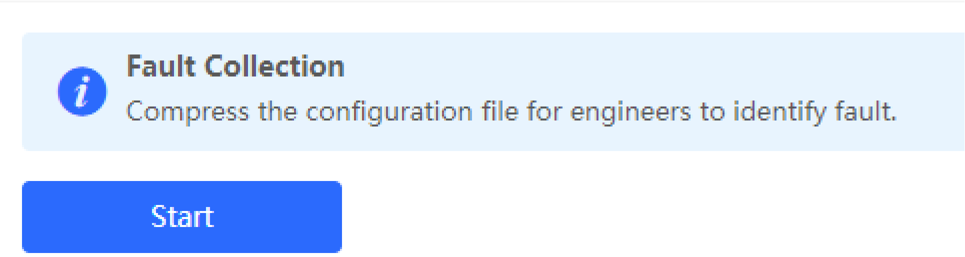


Tool ○ Ping ○ Traceroute ● DNS Lookup

*IP Address/Domain: www.google.com

3.9.3 Fault Collection

When an unknown fault occurs on the device, you can run the one-click fault collection command on this page to collect fault information. Click **Start** to package the device configuration file as a compressed file. After downloading it to the local PC, you can send it to R&D engineers to locate faults.

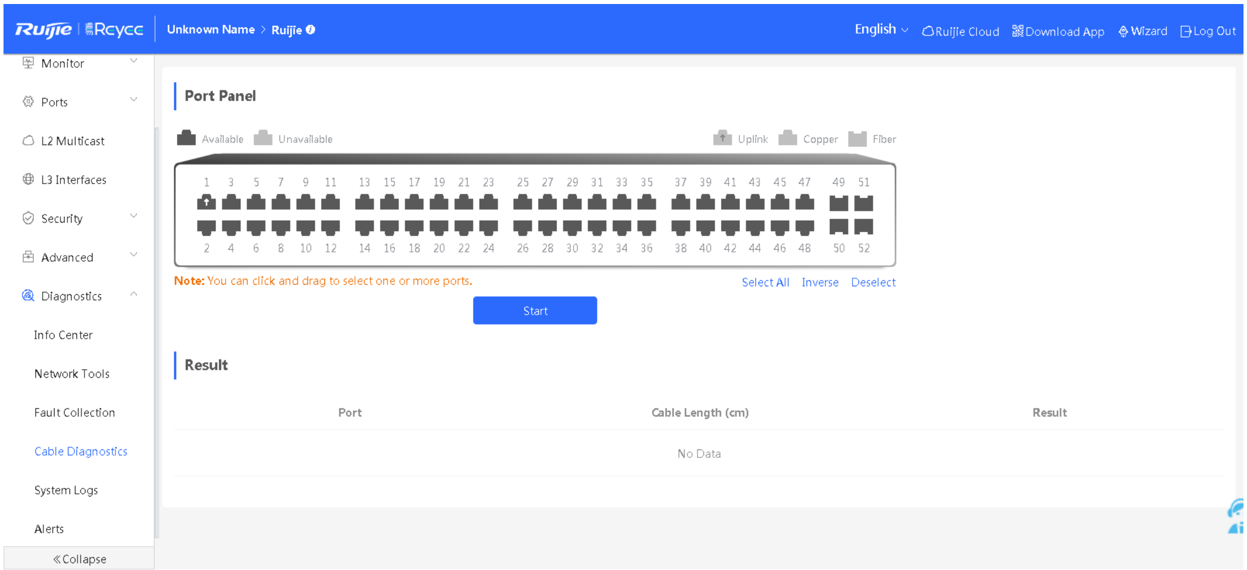

Fault Collection

Compress the configuration file for engineers to identify fault.

3.9.4 Cable Diagnostics

The cable diagnostics function can detect the approximate length of a cable connected to a port and whether the cable is faulty.

Select the port to be detected on the port panel and click **Start**. The detection results will be displayed below.



Note: You can click and drag to select one or more ports.

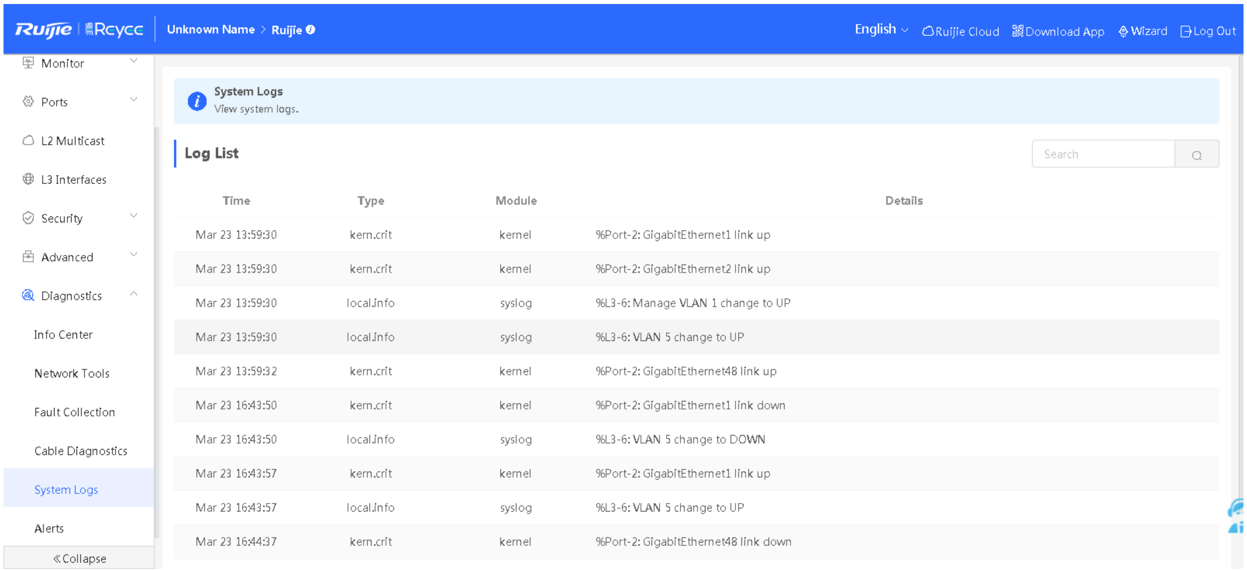
Port	Cable Length (cm)	Result
	No Data	

⚠ **Caution**

If a detected port contains an uplink port, the network may be intermittently disconnected. Therefore, exercise caution when performing this operation.

3.9.5 System Logs

System logs record device operations, operation time, and operation modules. System logs are used by administrators to monitor the running status of the device, analyze network status, and locate faults. You can search for specified logs by fault type, faulty module, and keyword in fault information.



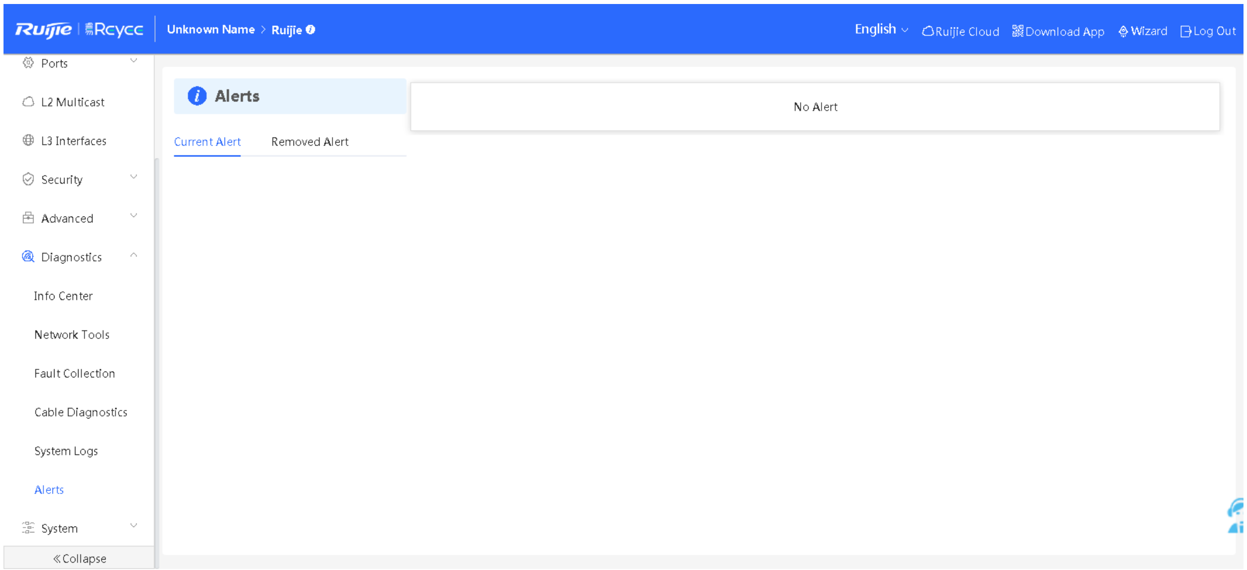
System Logs
View system logs.

Log List

Time	Type	Module	Details
Mar 23 13:59:30	kern.crit	kernel	%Port-2: GigabitEthernet1 link up
Mar 23 13:59:30	kern.crit	kernel	%Port-2: GigabitEthernet2 link up
Mar 23 13:59:30	local.info	syslog	%L3-6: Manage VLAN 1 change to UP
Mar 23 13:59:30	local.info	syslog	%L3-6: VLAN 5 change to UP
Mar 23 13:59:32	kern.crit	kernel	%Port-2: GigabitEthernet48 link up
Mar 23 16:43:50	kern.crit	kernel	%Port-2: GigabitEthernet1 link down
Mar 23 16:43:50	local.info	syslog	%L3-6: VLAN 5 change to DOWN
Mar 23 16:43:57	kern.crit	kernel	%Port-2: GigabitEthernet1 link up
Mar 23 16:43:57	local.info	syslog	%L3-6: VLAN 5 change to UP
Mar 23 16:44:37	kern.crit	kernel	%Port-2: GigabitEthernet48 link down

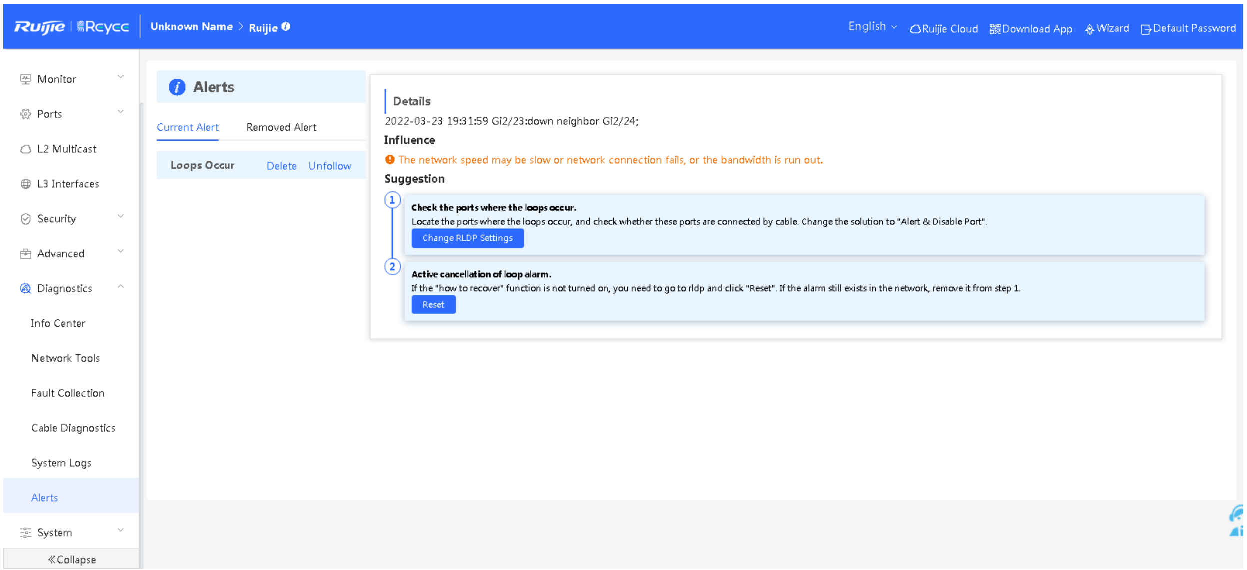
3.9.6 Alerts

The Alerts page displays possible problems on the network environment and device. On the **Current Alert** page, you can check fault alarms and delete or unfollow alarms.



No Alert

You can view the alarm occurrence time, port, alarm impact, and handling suggestions, and rectify device faults according to handling suggestions.



Details

2022-03-23 19:31:59 Gi2/23:down neighbor Gi2/24;

Influence

The network speed may be slow or network connection fails, or the bandwidth is run out.

Suggestion

1. **Check the ports where the loops occur.**
   Locate the ports where the loops occur, and check whether these ports are connected by cable. Change the solution to "Alert & Disable Port".
   Change RLDP Settings
2. **Active cancellation of loop alarm.**
   If the "how to recover" function is not turned on, you need to go to rldp and click "Reset". If the alarm still exists in the network, remove it from step 1.
   Reset

You can click **Unfollow** in the operation column for an alarm to unfollow this type of alarm. The system will no longer display this type of alarm. To enable the notification function of a type of alarm, follow the alarm type on the **Removed Alert** page.

Table 3-23 Alarm Types

Alarm Type	Description	Applicable Products
Addresses in the DHCP address pool are to be exhausted.	This alarm is generated when the device functions as a DHCP server and the number of allocated IP addresses exceeds the maximum number of addresses that can be allocated.	It is applicable only to devices that support L3 functions. Products that do not support L3 functions such as S1930, NBS3100, and NBS3200, do not support this type of alarm.
The IP address of the local device conflicts with that of another device.	The IP address of the local device conflicts with that of another client on the LAN.	N/A
An IP address conflict occurs on downlink devices connected to the device.	Among the devices connected to the current device on the LAN, an IP address conflict occurs on one or more devices.	N/A

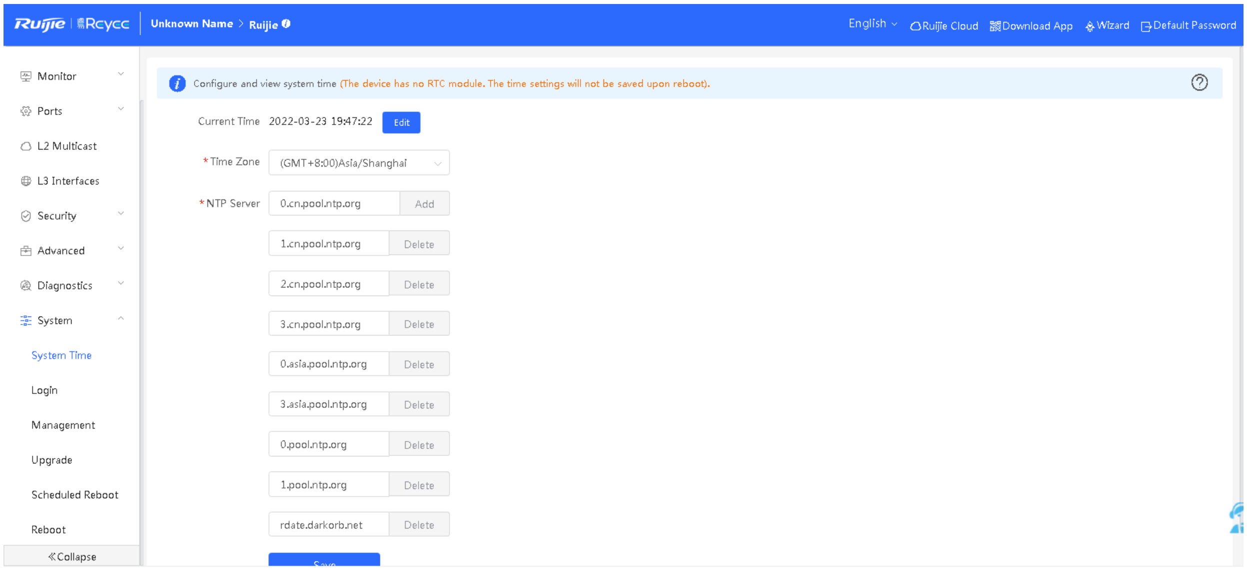
Alarm Type	Description	Applicable Products
The MAC address table is full of entries.	The number of L2 MAC address entries exceeds the hardware capacity of the product.	N/A
The ARP table is full of ARP entries.	The number of ARP entries on the large network exceeds the ARP capacity of the device.	N/A
The PoE process is not running.	The PoE service of the device fails and no power can be supplied.	It is applicable only to NBS products that support the PoE function. (The device models are marked with "-P".)
The total PoE power is overloaded.	The total PoE power of the device is overloaded, and PD cannot be powered properly.	It is applicable only to NBS products that support the PoE function. (The device models are marked with "-P".)
The device has a loop alarm.	A network loop occurs on the LAN.	N/A

3.10 System

3.10.1 System Time

The **System Time** page allows you to view and set the system time. On this page, you can change the system time and configure the system time zone and NTP server.

If the current time is incorrect, check and select the local time zone. If the time zone is correct but time is still incorrect, click **Edit** to manually set the time. The device allows you to configure the Network Time Protocol (NTP) server to synchronize time from the network. By default, multiple servers serve as the backup of each other. You can add or delete local servers as required.



Configure and view system time (The device has no RTC module. The time settings will not be saved upon reboot).

Current Time 2022-03-23 19:47:22

*Time Zone (GMT+8:00)Asia/Shanghai

*NTP Server 0.cn.pool.ntp.org

1.cn.pool.ntp.org

2.cn.pool.ntp.org

3.cn.pool.ntp.org

0.asia.pool.ntp.org

3.asia.pool.ntp.org

0.pool.ntp.org

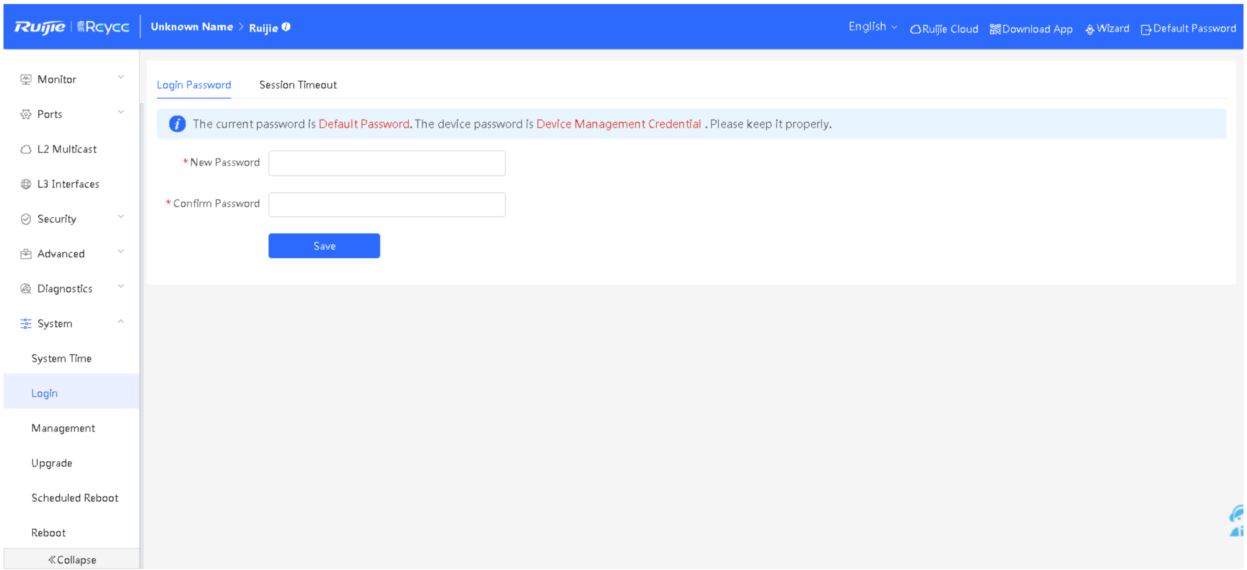
1.pool.ntp.org

rdate.darkorb.net

3.10.2 Login

1. Login Password

You can change the login password of the device. Enter the old device password and the new device password and click **Save**. After changing the device password, you need to log in to the Eweb management system again.



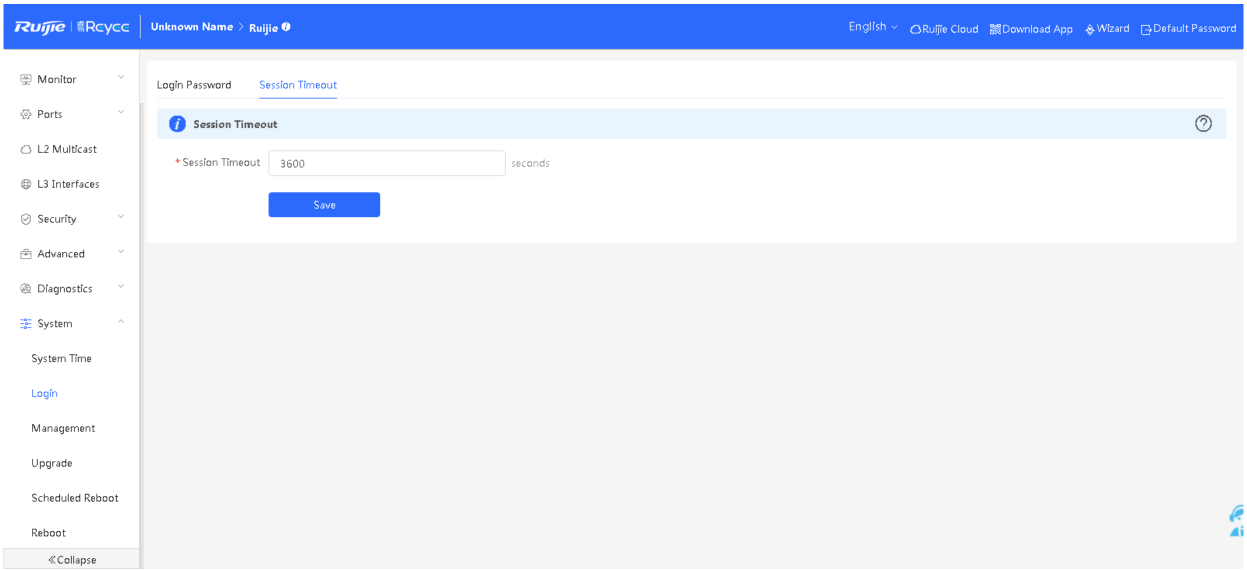
The current password is Default Password. The device password is Device Management Credential . Please keep it properly.

*New Password

*Confirm Password

2. Session Timeout

If you do not log out after login, the Eweb management system allows you to continue the access without authentication on the current browser within one hour by default. After one hour, the Eweb management system automatically refreshes the page and you need to relog in before continuing your operations. You can change the session timeout duration.



* Session Timeout 3600 seconds

Note

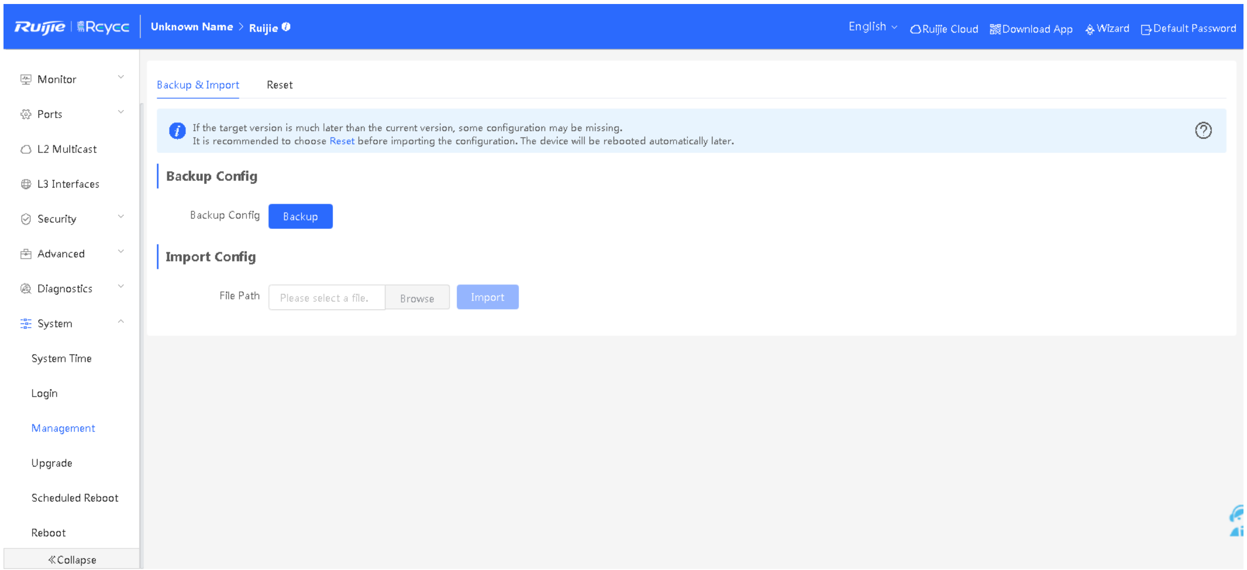
The default timeout duration for Web access is 1 hour (3600 seconds). To ensure device security, you are advised to log out of the Eweb management system in time after completing configuration.

3.10.3 Setup

1. Backup & Import

Backup Config: After the switch is configured, you can export the configuration file. Click **Backup** to generate the backup configuration and download it locally.

Import Config: An exported backup file can be imported after the device is restored to factory settings. Click **Browse**, select a backup configuration file locally, and click **Import** to import the configuration. Then, the device will restart.



If the target version is much later than the current version, some configuration may be missing.
It is recommended to choose Reset before importing the configuration. The device will be rebooted automatically later.

Backup Config

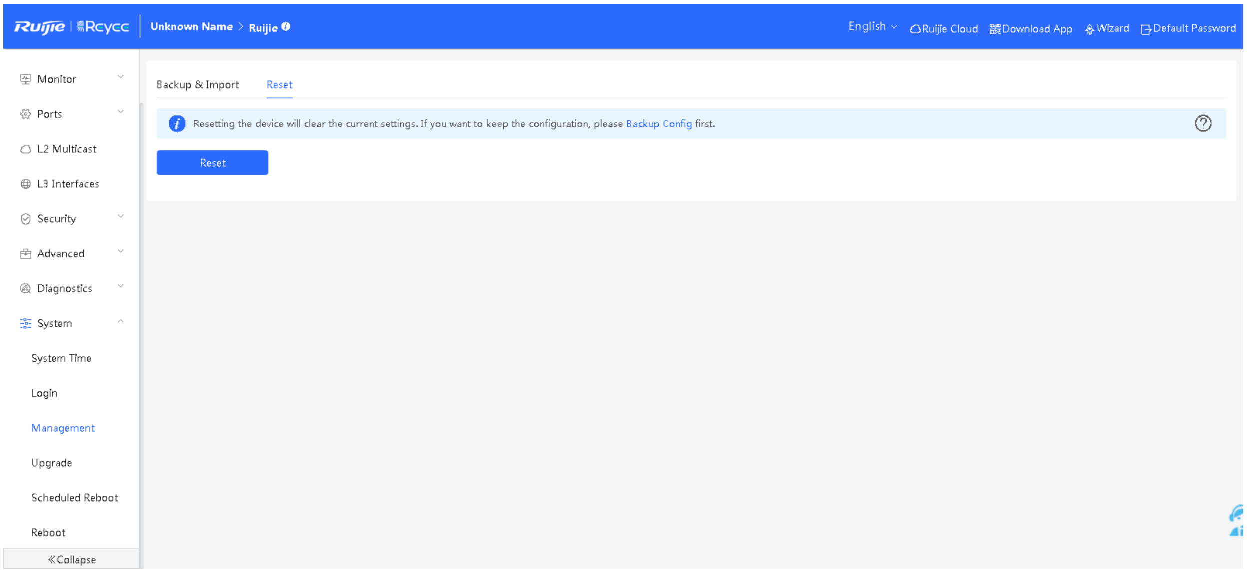
Backup Config: Backup

Import Config

File Path: Please select a file.

2. Reset

Click **Reset** to restore factory settings.



Resetting the device will clear the current settings. If you want to keep the configuration, please Backup Config first.

Caution

1. 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 client is connected to the device by referring to 2.1 Configuration Preparations.

2. After the device is restored to factory settings, all user configurations will be deleted and you need to reconfigure the device. The cloud device will be cleared and needs to be added again. Therefore, exercise caution when performing this operation.

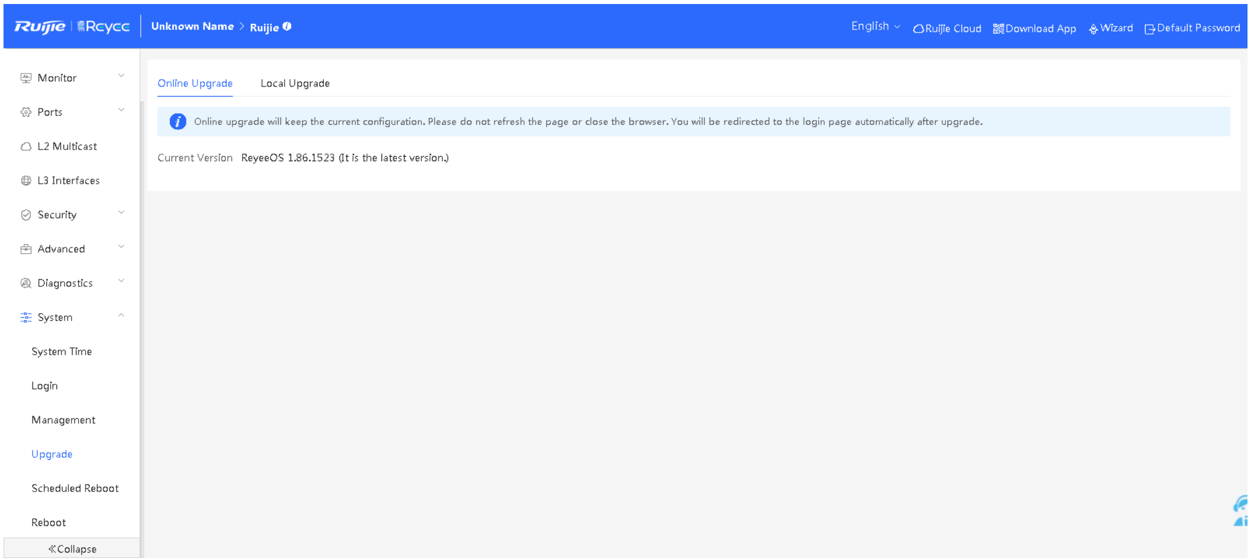
Click **OK** to restore all default values. This function is recommended when the network configuration is incorrect or the network environment is changed. If you fail to access the Eweb management system, check whether the client is connected to the device by referring to Configuration Preparations.

3.10.4 Upgrade

1. Online Upgrade

When detecting an available online upgrade version, the device displays information about the available upgrade version. Click **Upgrade**. The device downloads the upgrade package from the network and upgrades the current version. The upgrade operation retains configuration information of the current device. If the device cannot access the external network, you can download the upgrade package to the local device and import the upgrade version on the local upgrade page.

If there is no available upgrade package on the network, a page as shown in the figure below is displayed.

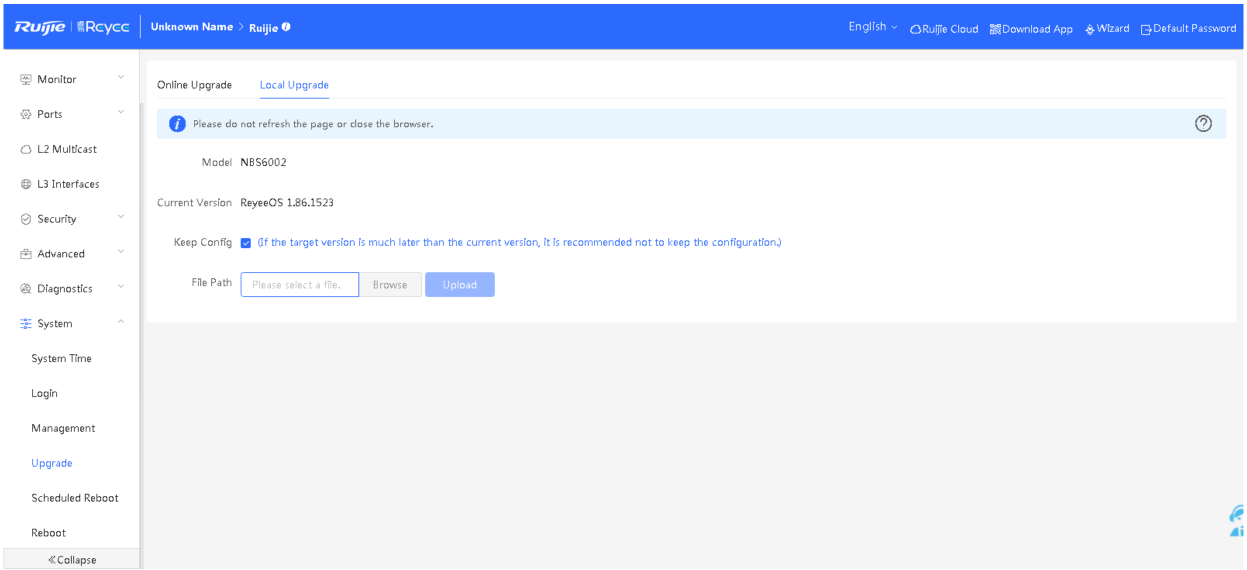


Online upgrade will keep the current configuration. Please do not refresh the page or close the browser. You will be redirected to the login page automatically after upgrade.

Current Version ReyeeOS 1.86.1523 (It is the latest version.)

2. Local Upgrade

Select a system upgrade package from the local path, and click **Upload**. The device is upgraded to the version specified in the upgrade package. The upgrade package is in the format of xxxx.tar.gz.



Please do not refresh the page or close the browser.

Model NBS6002

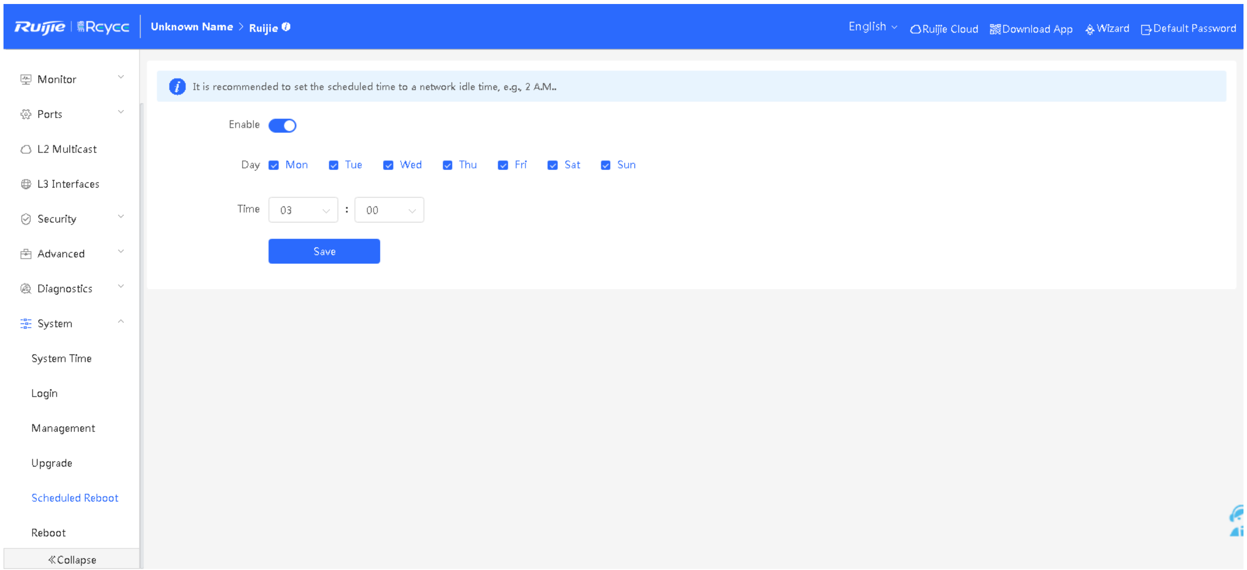
Current Version ReyeeOS 1.86.1523

Keep Config ☑ (If the target version is much later than the current version, it is recommended not to keep the configuration.)

File Path Please select a file.

3.10.5 Scheduled Reboot

Click **Enable**, and select the date and time of scheduled reboot every week. Click **Save**. When the system time matches the scheduled reboot time, the device will restart. Off-peak hours are recommended for the reboot.



It is recommended to set the scheduled time to a network idle time, e.g., 2 A.M..

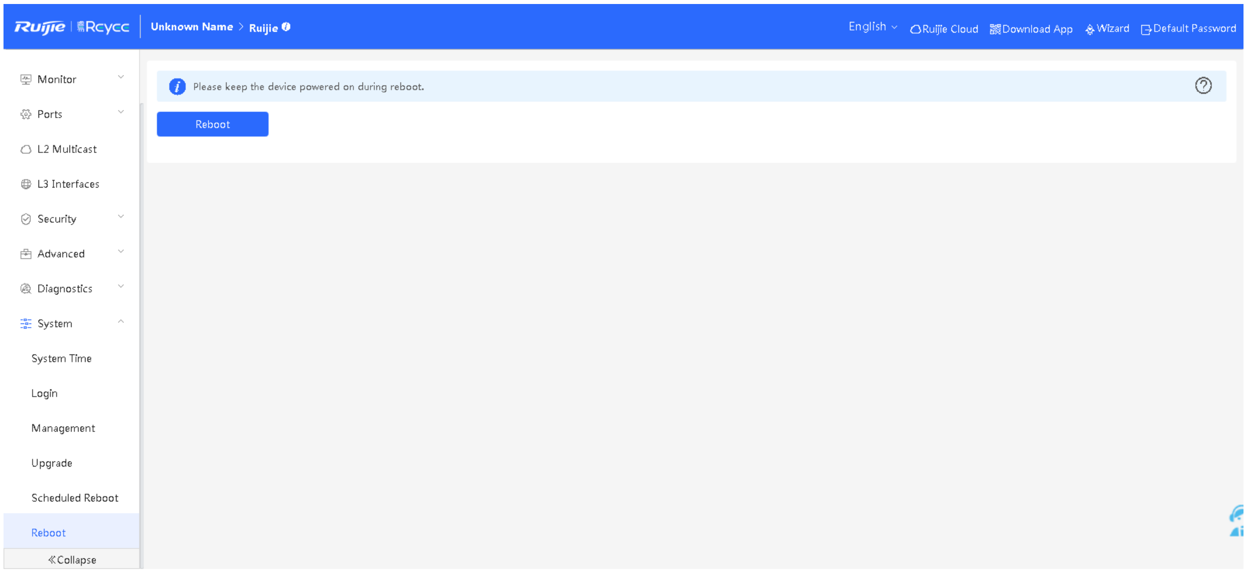
Enable ●

Day ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun

Time 03 : 00

3.10.6 Reboot

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



Please keep the device powered on during reboot.

Click **Reboot** and then click **OK**. The device will restart. After restart, you need to relog in to the Eweb management system.

Do not refresh the page or close the browser during the reboot. After the device is successfully rebooted and the Web service becomes available, the device automatically jumps to the login page of the Eweb management system.

4 FAQs

4.1 Failure to Log In to the Eweb Management System

- **What can I do when I failed to log in to the Eweb management system?**

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 setup page, you are advised to configure a static IP address for the PC. The IP address of the PC should be set to 10.44.77.*X* (*X* is an integer between 2 and 254), and the subnet mask is 255.255.255.0.

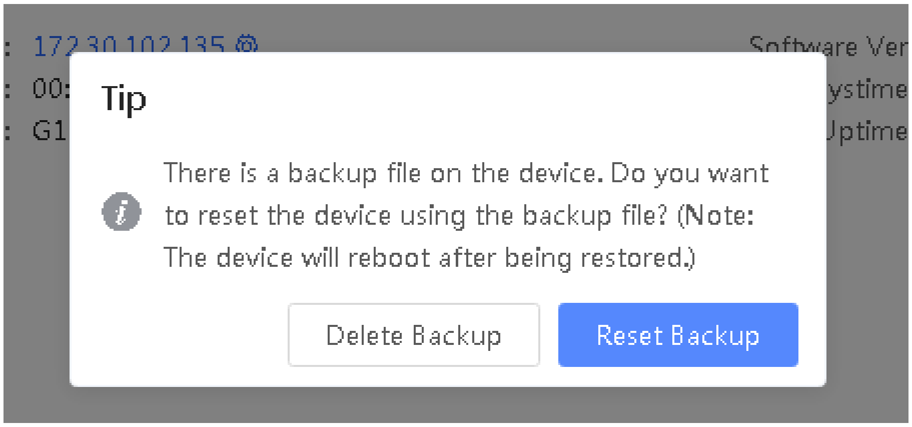
(3) Run the ping command to check the connectivity between the PC and the device.

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

4.2 Password Lost and Restoration of Factory Settings

- **What can I do when I forget the device username and password? How can I restore factory settings?**

When you forget the username and password, press the **Reset** button on the device as follows to restore the password: Power on the device, hold down the **Reset** button for more than 5 seconds, release the button after the system indicator blinks. After the device is started, log in to the Eweb management system, as shown in the figure below. Follow prompts to determine whether to restore factory settings or restore the default password.



Tip

There is a backup file on the device. Do you want to reset the device using the backup file? (Note: The device will reboot after being restored.)

Select **Reset Backup** to restore the default password.

Select **Delete Backup** to restore factory settings, that is, passwords and configurations will be deleted.

After restoration, the default management address is http://10.44.77.200.

4.3 IP Subnet Mask

- **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).