

## Reyee Series Implementation Cookbook (V1.0)

Redefine your easy network



## Copyright Statement

Ruijie Networks©2013

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



**Red-Giant 锐捷**<sup>®</sup>, **锐捷**<sup>®</sup> are registered trademarks of Ruijie Networks. Counterfeit is strictly prohibited.

## Exemption Statement

This document is provided "as is". The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

# 1 Preface

## Audience

Network Engineers

Network Administrator

## Obtain Technical Assistance

Ruijie Networks Websites: <https://www.ruijienetworks.com>

Ruijie Service Portal: <https://caseportal.ruijienetworks.com>

Welcome to report error and give advice in any Ruijie manual to Ruijie Service Portal

## Revision History

Date	Change contents	Reviser
2020.8	Initial publication V1.0	Ruijie GTAC

# Contents

1 Preface .....	3
2 Product Introduction.....	5
2.1 Cloud-managed Access Points .....	5
2.2 Reyee Switch.....	5
2.3 EasyGate Series Router .....	6
3 Daily Maintenance .....	7
3.1 Device Login .....	7
3.2 Change Password.....	8
3.3 Factory Reset.....	7
4 Quick Provisioning.....	8
4.1 Quick provisioning via Ruijie Cloud APP.....	8
4.2 Quick provisioning via Reyee EWeb.....	10
5 Reyee EG Series Router Configuration .....	15
5.1 WAN Load balance .....	15
5.2 IPsec VPN .....	19
5.3 Smart Flow Control.....	22
5.4 Port Mapping .....	23
6 Reyee NBS Series Switch Configuration .....	26
6.1 VLAN Setting .....	26
6.2 Access Control List (ACL).....	29
6.3 Port Isolation.....	35
6.4 DHCP Snooping.....	37
6.5 Link Aggregation .....	39
6.6 Storm Control.....	41
7 Reyee ES Series Switch Configuration.....	44
7.1 VLAN Setting .....	44
7.2 Port Isolation.....	47
7.3 DHCP Snooping.....	48
7.4 Speed Rate Limit.....	50
7.5 Storm Control.....	51
8 Reyee AP Configuration .....	53
8.1 Wi-Fi Setting .....	53
8.2 Multiple SSID setting .....	54
8.3 AP Group.....	55
8.4 Blacklist/Whitelist .....	57
8.5 Turn on/off LED indicator .....	58
9 FAQ .....	59

---

## 2 Product Introduction

### 2.1 Cloud-managed Access Points

Reyee cloud-managed access point is a high performance for indoor/outdoor/wall scenarios. Compliant with 802.11ac wave2 Wi-Fi protocol, cloud-managed series access points support MU-MIMO dual stream technology.

The industrial product design makes the product is simple to install and maintenance.

Cloud-managed access points support self-organizing network.

#### **Provide better performance based on Dual-band Wi-Fi**

Supports 2.4GHz and 5GHz dual-band communication, providing access rate of 400Mbps at 2.4GHz, 867Mbps at 5GHz and up to 1267Mbps per AP. It can provide 5GHz frequency band with less interference, wider channel, and faster speed for the terminals, allowing the users to enjoy excellent wireless experience.

#### **Seamless Layer 3 Roaming**

The device supports Layer 3 roaming for the complex Layer 3 network. When users move across the Layer 3 networks, seamless roaming can be achieved without service interruption.

#### **Support Self-organizing networking feature**

Self-organizing networking feature, which breaks through the product limitations and realizes auto-discovery, auto-networking and auto-configuration between routers, switches, and wireless APs without the need for controllers or Internet access. With the mobile app, users can quickly complete the device deployment and configuration, remote management, operation and maintenance of the entire network, which greatly reduces the investment of equipment cost, labor cost and time cost in the process of wireless network construction.

### 2.2 Reyee Switch

Reyee switches are designed to offer reliable and professional choices to businesses of all sizes. Unmanaged switches are well suited for businesses requiring no management or monitoring of their LAN, smart/L2 switches provide a cost-effective solution for small and medium-sized businesses, and L3 managed switches provide a scalable and stable solution for large organizations, campus networks and ISP networks.

#### **Ruijie Cloud App/ Ruijie Cloud Platform Remote Management**

The Reyee managed switches not only support web interface management, but also support life time free Ruijie Cloud App and Ruijie Cloud platform remote management. Users can view the network status, modify the configuration, and troubleshooting at home. In addition, the PoE port can be restarted remotely to restart the faulty PoE camera. With the mobile

---

app, users can quickly complete the device deployment and configuration, remote management, operation and maintenance of the entire network, such as NVR/ Camera recognition, configure VLAN, real time monitoring, real time alarm, and reboot remotely , which greatly reduces the investment of equipment cost, labor cost and time cost in the process of wireless network construction.

#### **Self-Organizing Networking Feature**

Self-organizing networking feature, which breaks through the product limitations and realizes auto-discovery, auto-networking and auto-configuration between routers, switches, and wireless APs without the need for controllers or Internet access.

#### **Full-Power PoE Supporting PoE Cameras at Maximum Capacity**

Ruijie Reyee smart surveillance switches support full-power PoE output, powering PoE network cameras for all PoE ports simultaneously. Whether it is day or night, the infrared light of the camera is on or off, it can ensure that all PoE network cameras are powered.

## **2.3 EasyGate Series Router**

Ruijie Reyee RG-EG series Router is a cloud managed router designed for villas and smart home, restaurant, small offices, homestay hotel. it is affordable, small and easy to use, but at the same time comes with 500M-600M bandwidth and supporting up to 200 terminals.

RG-EG series can perform per-port VLAN configuration to achieve port isolation, and integrate with smart flow control to achieve comprehensive network planning and perform local and remote network diagnosis.

---

## 3 Daily Maintenance

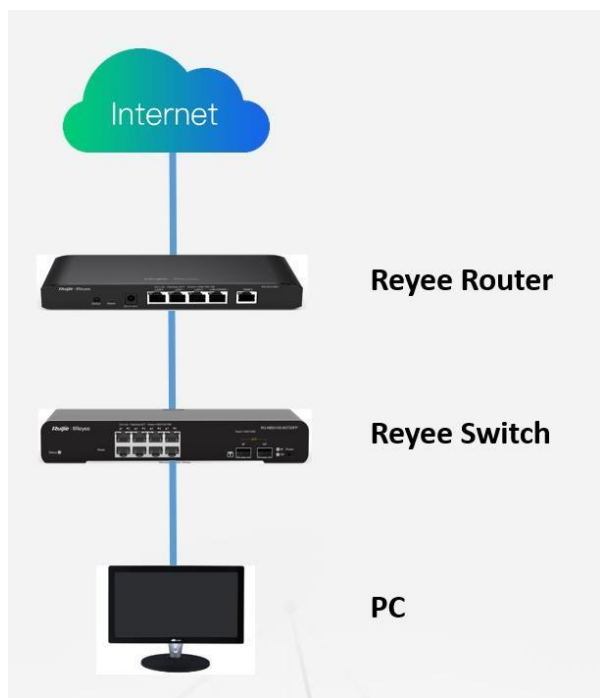
### 3.1 Device Login

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

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

#### Network Topology

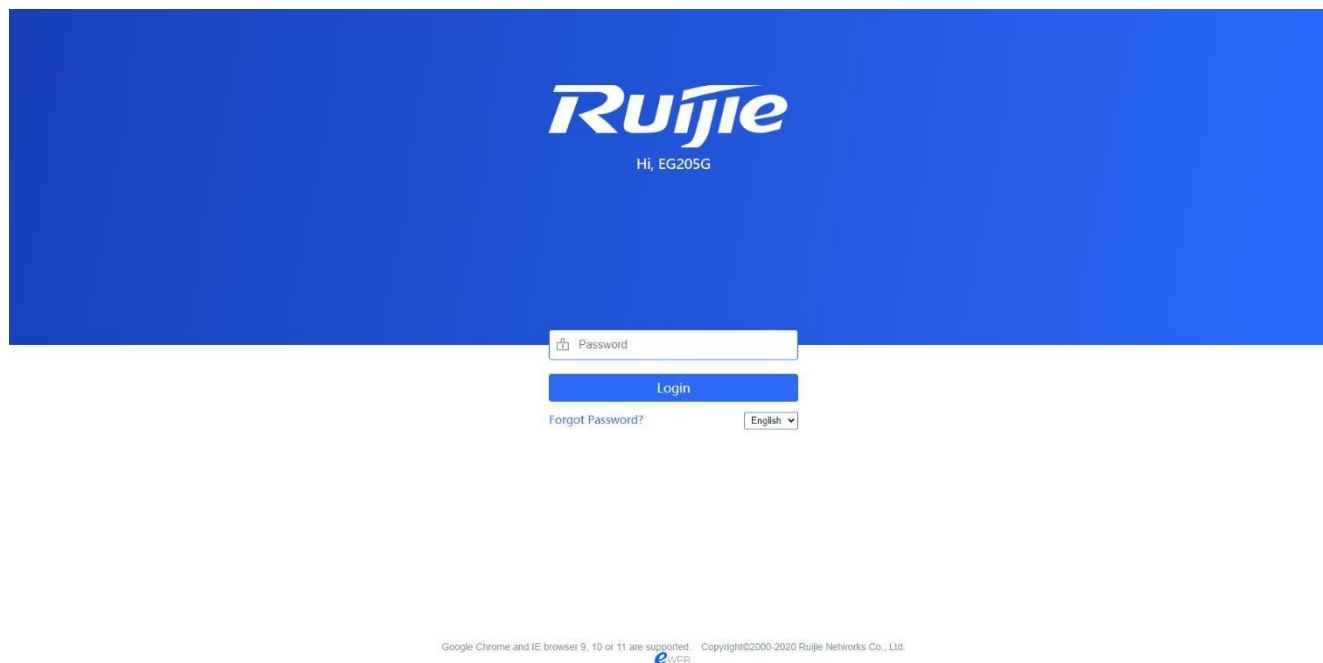
As shown in the figure below, you can access the eWeb management system of an access or aggregation switch via a PC browser to manage and configure the device.



- 1) Set PC's IP assignment mode to **Obtain an IP address automatically**.
- 2) Visit <http://192.168.110.1> by Chrome browser.
- 3) Enter the password on the login page and click "Login".

Default Password: **admin**

---



For the Reyee EG device, you may use either **192.168.110.1** or **10.44.77.254** to access the device.

For the Reyee switches, you may use **10.44.77.200** to access the device.

For the Reyee AP, you may use either **192.168.120.1** or **10.44.77.254** to access the device.

The default login password for all Reyee devices are **admin**.

You may visit <https://10.44.77.253> to login to the master device of Reyee network.

## 3.2 Change Password

Login to the master device and choose **Network** → **Password** to change the device password.

---

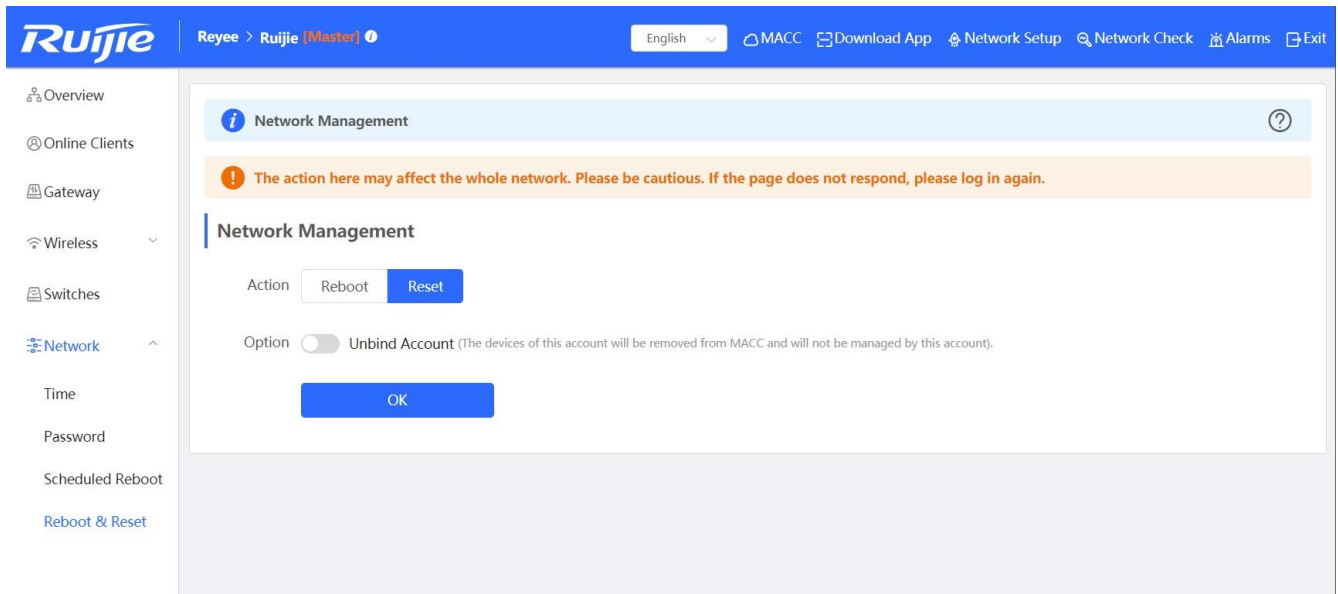


The screenshot displays the Ruijie web management interface. At the top, the Ruijie logo is on the left, and navigation links for 'Reyee > Ruijie [Master]', 'English', 'MACC', 'Download App', 'Network Setup', 'Network Check', 'Alarms', and 'Exit' are on the right. A left-hand navigation menu includes 'Overview', 'Online Clients', 'Gateway', 'Wireless', 'Switches', 'Network', 'Time', 'Password', 'Scheduled Reboot', and 'Reboot & Reset'. The main content area is titled 'Device Password' and contains an information icon, the text 'Change the device password. Please log in again with the new password later.', and a help icon. Below this are three password input fields: '\* Old Password', '\* New Password', and '\* Confirm Password', each with a password strength indicator. A blue 'Save' button is positioned below the fields.

### 3.3 Factory Reset

Option 1: Press the “Reset” button on the device for more than 5 seconds to factory reset the device.

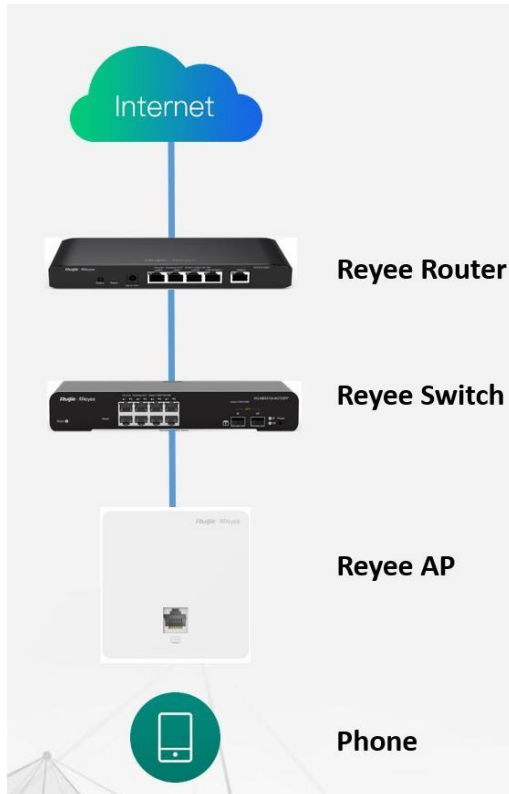
Option 2: Login to the eWeb of the device reset all device in the network.



## 4 Quick Provisioning

### 4.1 Quick provisioning via Ruijie Cloud APP

#### Network Topology



1) If your mobile phone does not have the Ruijie Cloud App installed, please search “Ruijie Cloud” on App Store and install it on your mobile phone. Below is an example of searching “Ruijie Cloud” on Google Play Store. Tap INSTALL to install the App directly.

2) Ruijie Cloud App provides a quick start to Create Network and Add Device. You can follow the steps below to finish provisioning.

**Step1:** Connect to the Wi-Fi with Reyee AP.

**Step2:** Choose the SSID of “@Ruijie\_mXXXX”.

**Step3:** Check all the devices are detected.

**Step4:** Add the project name and password.

**Step5:** Finish the WAN configuration.

**Step6:** Add the wireless configuration.

**Step7:** Finish all the configuration.

**Step8:** Devices all online in Ruijie Cloud.

**01**

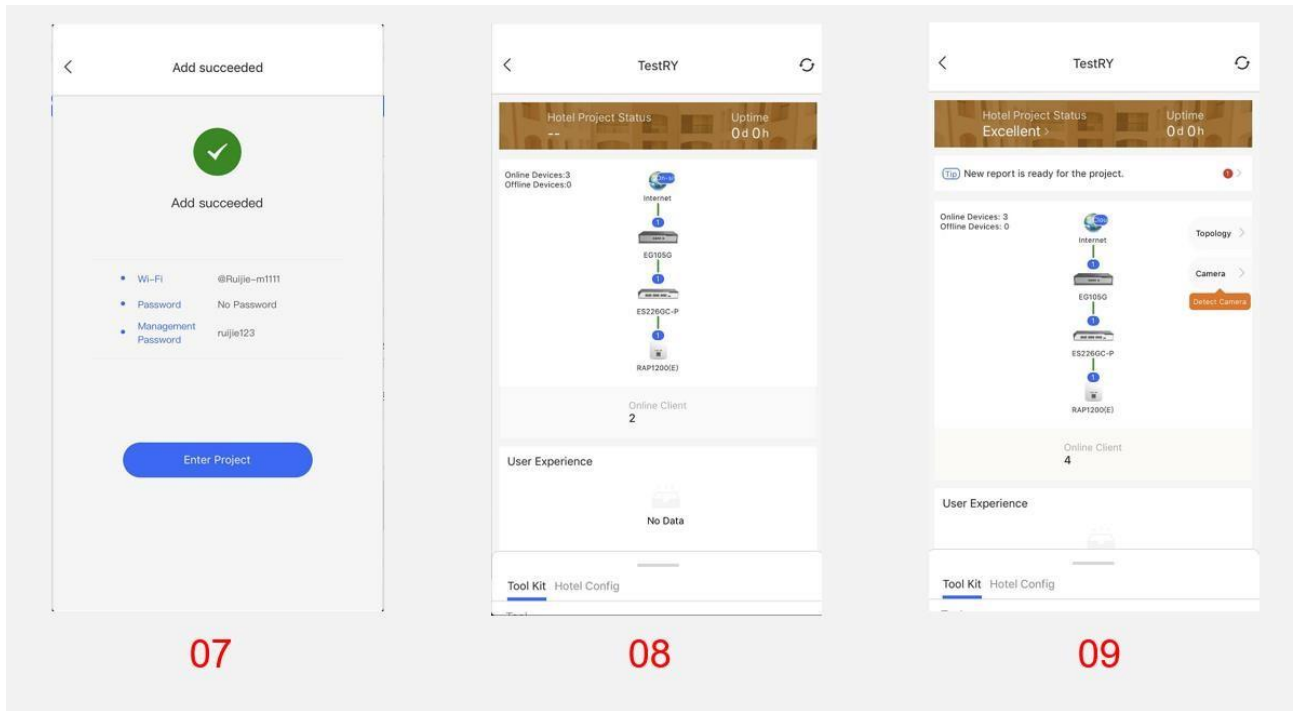
**02**

**03**

**04**

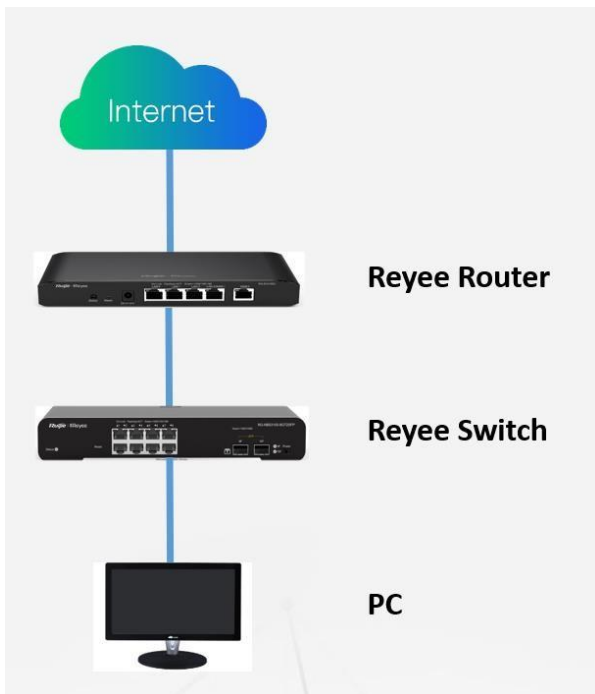
**05**

**06**



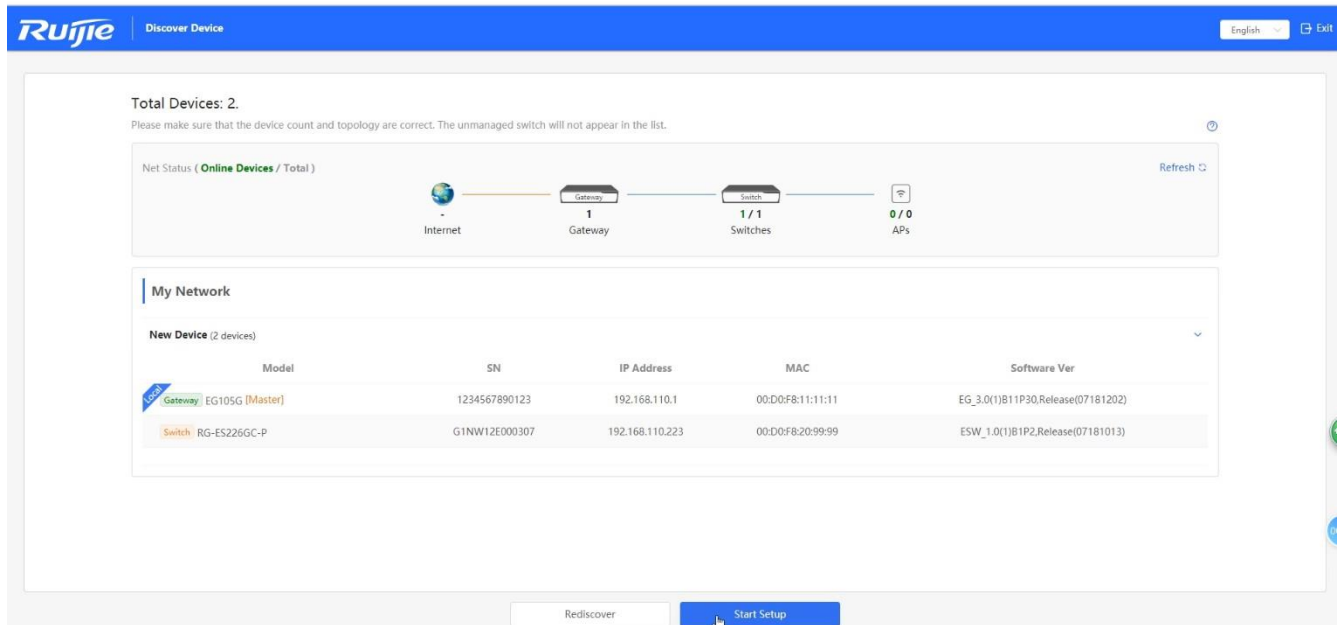
## 4.2 Quick provisioning via Reyee EWeb

### Network Topology



## Reyee Series Implementation Cookbook

Step 1: Login to Reyee EWeb (<http://192.168.110.1>), the local devices will be discovered automatically.

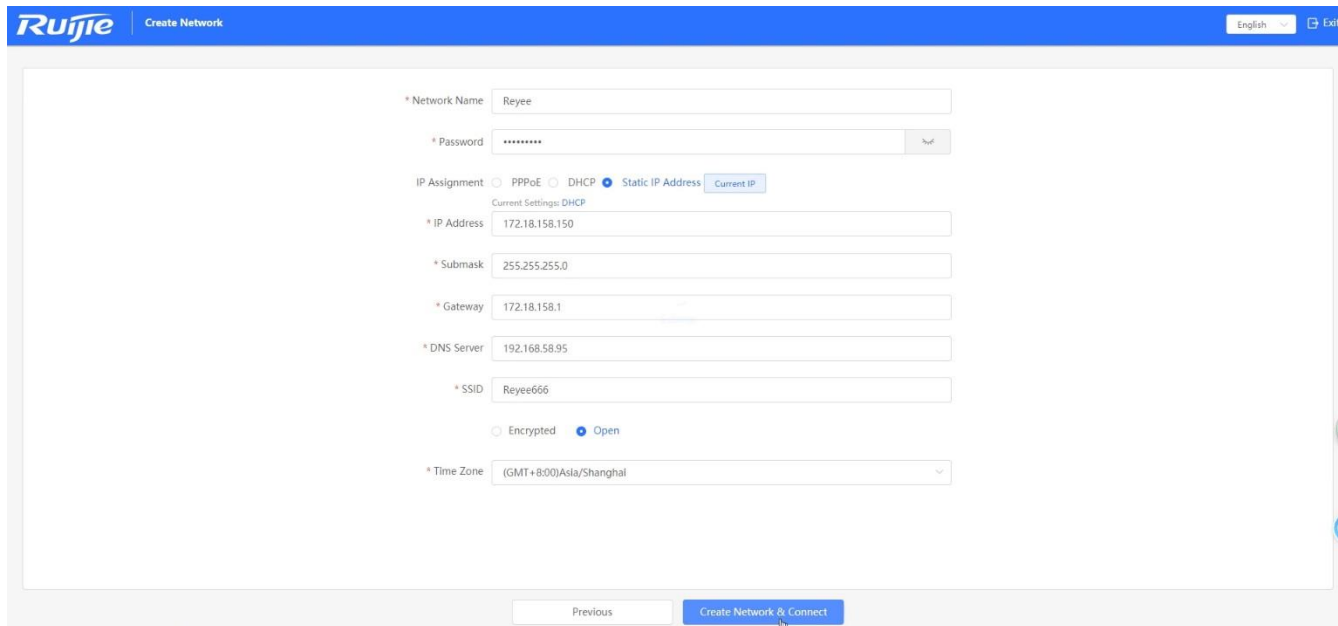


The screenshot shows the 'Discover Device' interface in the Ruijie EWeb. At the top, it says 'Total Devices: 2.' and provides a net status diagram: Internet -> Gateway (1) -> Switches (1/1) -> APs (0/0). Below this is a table titled 'New Device (2 devices)' with the following data:

Model	SN	IP Address	MAC	Software Ver
Gateway EG105G (Master)	1234567890123	192.168.110.1	00:D0:F8:11:11:11	EG_3.0(1)B1P30,Release(07181202)
Switch RG-ES226GC-P	G1NW12E000307	192.168.110.223	00:D0:F8:20:99:99	ESW_1.0(1)B1P2,Release(07181013)

At the bottom, there are 'Rediscover' and 'Start Setup' buttons.

Step 2: Create a network based on the actually scenario (PPPoE/DHCP/Static IP Address).

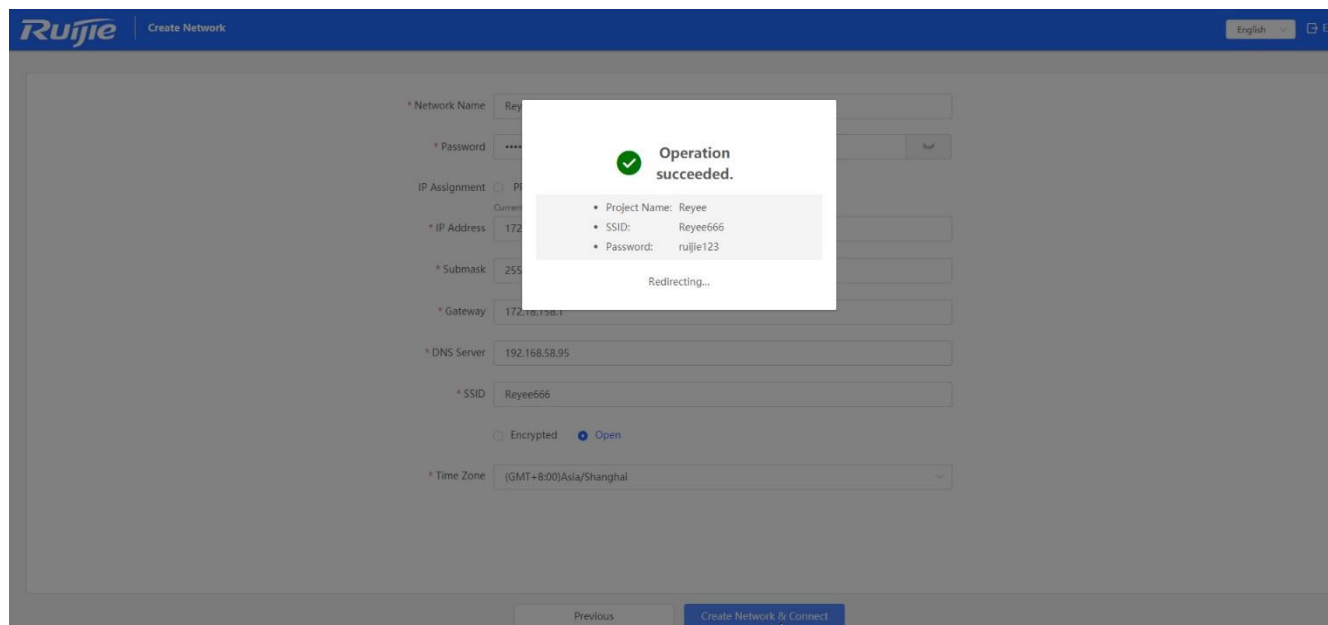


The screenshot shows the 'Create Network' interface. The configuration is as follows:

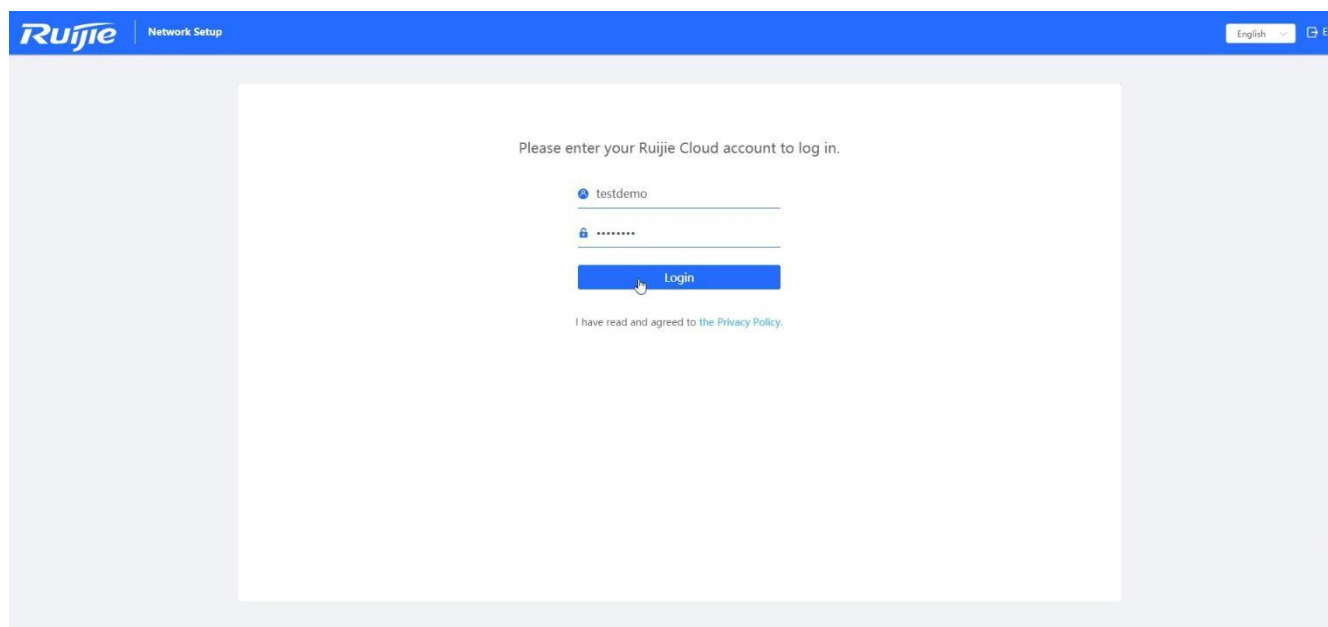
- Network Name: Reyee
- Password: [Redacted]
- IP Assignment:  Static IP Address (Current IP)
- Current Settings: DHCP
- IP Address: 172.18.158.150
- Submask: 255.255.255.0
- Gateway: 172.18.158.1
- DNS Server: 192.168.58.95
- SSID: Reyee666
- Encryption:  Open
- Time Zone: (GMT+8:00)Asia/Shanghai

At the bottom, there are 'Previous' and 'Create Network & Connect' buttons.

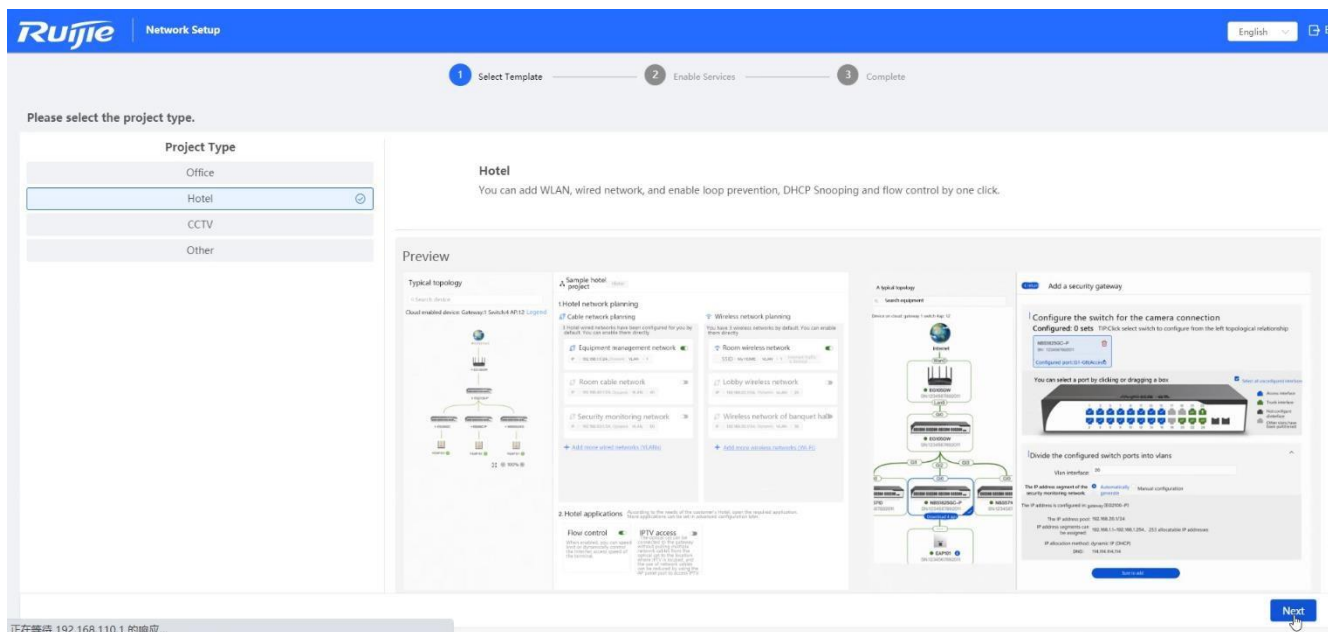
## Reyee Series Implementation Cookbook



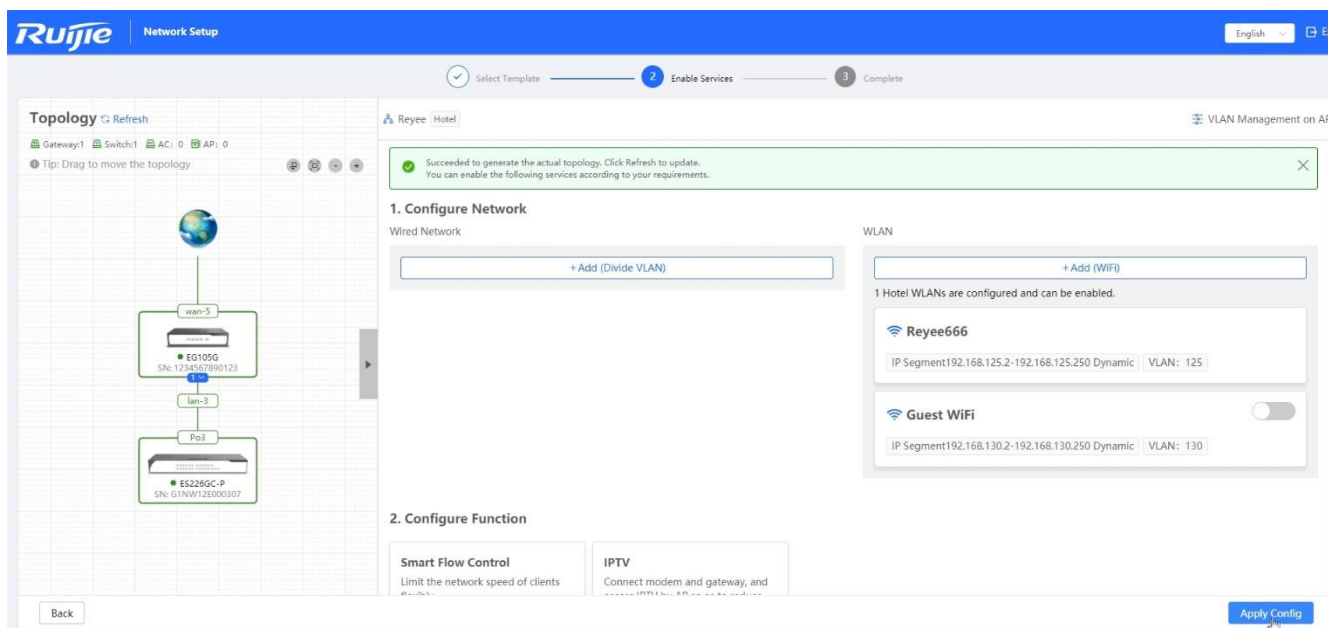
Step 3: Login to your Ruijie Cloud Account.



Step 4: Select the project type.



Step 5: Enable the services as you need and apply the config.





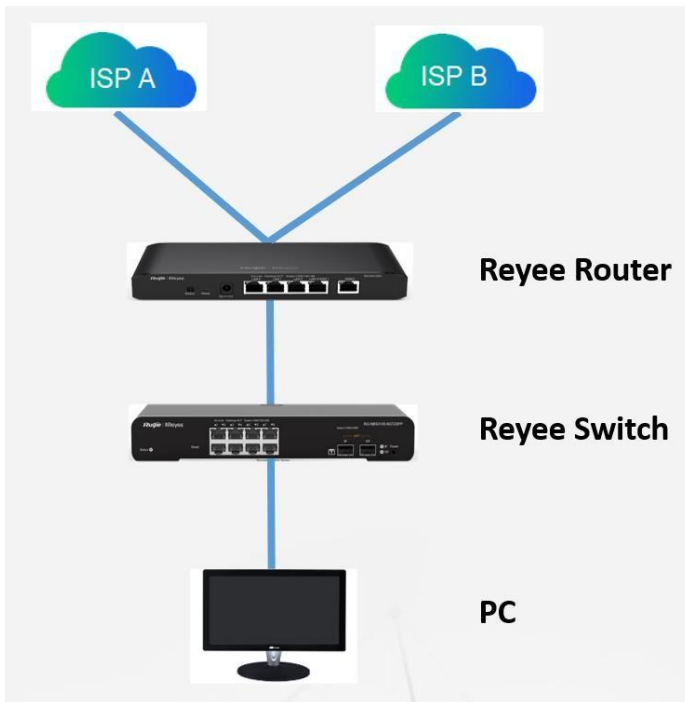
The screenshot displays the Ruijie Network Setup web interface. At the top, the 'Ruijie Network Setup' header is visible, along with a language dropdown set to 'English' and an 'Exit' button. Below the header, a progress bar shows three steps: 'Select Template' (checked), 'Enable Services' (checked), and 'Complete' (checked). The main content area is divided into two panels. The left panel, titled 'Topology', shows a network diagram with a central switch labeled 'lan-3' (ES226GC-P) connected to a gateway labeled 'wan-5' (EG105G) and a Po3 switch (ES226GC-P). The right panel, titled 'Network Config', shows the configuration for 'WLAN' under the 'Reyee666' profile. It lists 'IP Segment' as '192.168.125.2-192.168.125.250 Dynamic' and 'VLAN' as '125'. Below this, there are two configuration entries for 'ES105G' and 'ES226GC-P' with their respective SNs. A modal dialog box is centered on the screen with the text 'Initial Setup Completed!' and an 'Apply succeeded' message with an 'OK' button. At the bottom right, there is a 'Ruijie Cloud' button.

## 5 Reyee EG Series Router Configuration

### 5.1 WAN Load balance

The load balancing function distributes the data to multiple WAN interfaces to avoid the traffic congestion and provide redundancy.

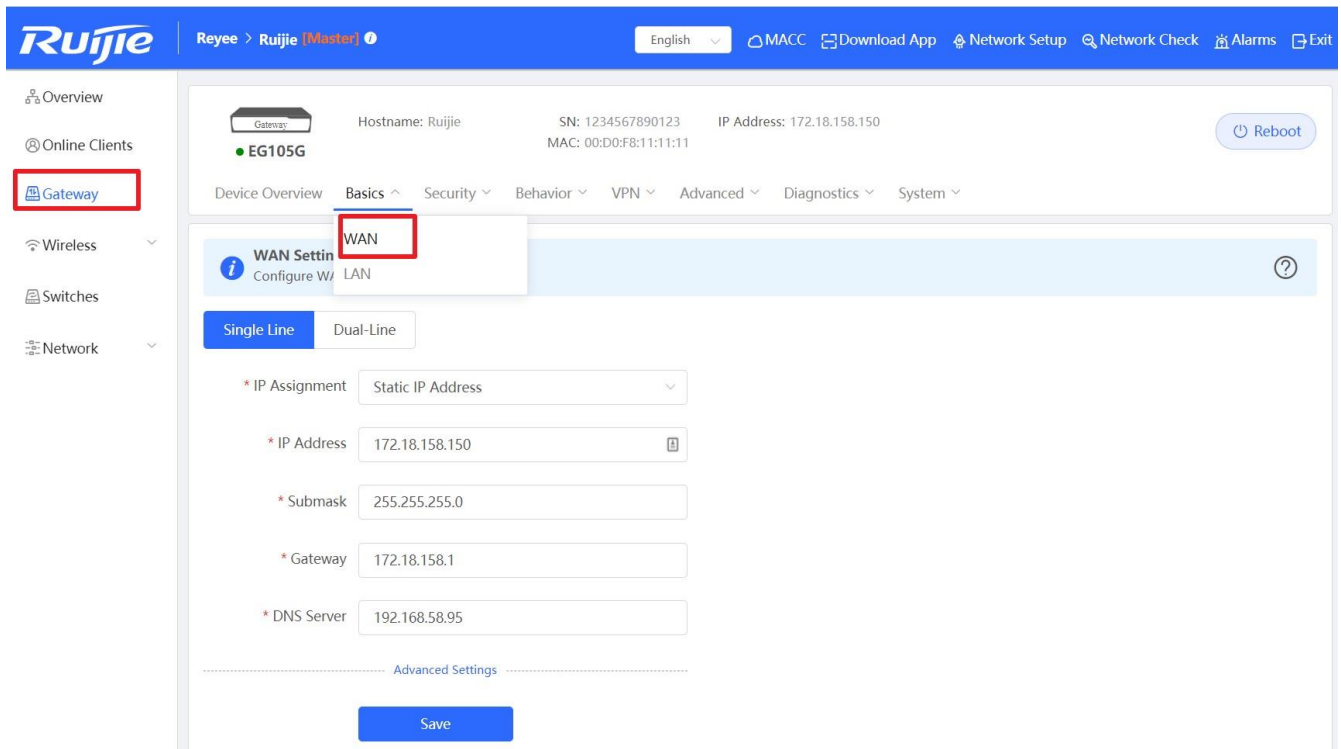
#### Network Topology



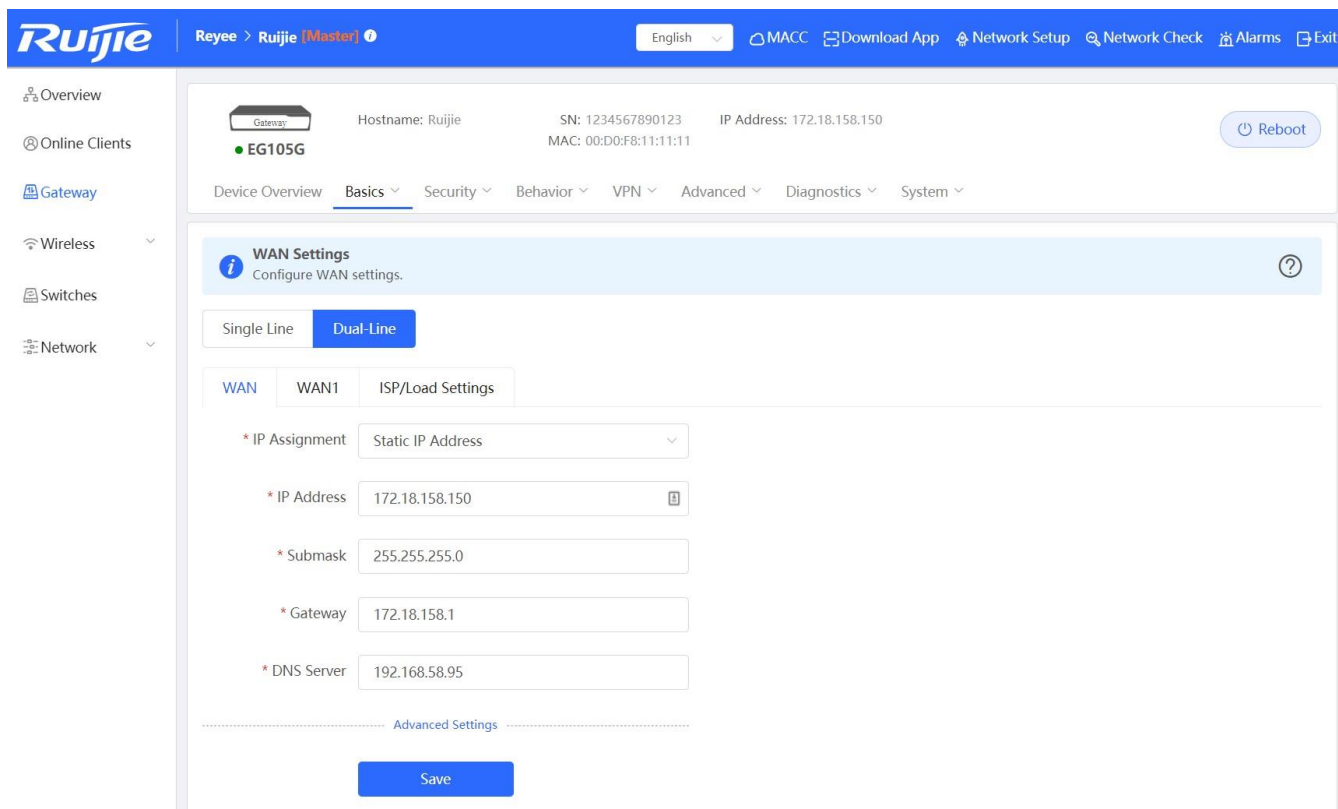
#### Configuration Steps

---

Step 1: Choose **Gateway** → **Basics** → **WAN**



Step 2: Configure the WAN interface accordingly



Step 3: Choose **ISP/Load Settings**, and configure the load mode and interface weight

1. **Balanced mode:** The traffic will be spread across multiple links according to the weight of each WAN port. For example, if WAN and WAN1 weight are set to 3 and 2 respectively, 60% of the total traffic will be routed over WAN and 40% over WAN1.
2. **Primary & secondary mode:** All traffic is routed over the primary interface. Once the primary interface fails, traffic will be switched over to the secondary interface. If there are multiple primary and secondary interfaces, please configure their weight (See balanced mode).

The screenshot shows the Ruijie Gateway configuration interface. At the top, the Ruijie logo is on the left, and navigation links for 'Reyee > Ruijie (Master)', 'English', 'MACC', 'Download App', 'Network Setup', 'Network Check', 'Alarms', and 'Exit' are on the right. A left sidebar contains menu items: Overview, Online Clients, Gateway, Wireless, Switches, and Network. The main content area displays device information for 'EG105G' (Gateway) with Hostname: Ruijie, SN: 1234567890123, IP Address: 172.18.158.150, and MAC: 00:D0:F8:11:11:11. A 'Reboot' button is present. Below this is a navigation bar with tabs: Device Overview, Basics (selected), Security, Behavior, VPN, Advanced, Diagnostics, and System. The 'WAN Settings' section is active, with a sub-tab for 'Dual-Line'. Underneath, there are tabs for WAN, WAN1, and ISP/Load Settings. The 'Load Balancing Settings' section contains a blue information box with the text: 'Traffic will be routed based on ISP settings preferentially. The remaining traffic will be managed according to load mode.' Below this, two numbered instructions describe 'Balanced mode' and 'Primary & secondary mode'. Configuration fields include 'Load Mode' (set to 'Balanced'), 'Balancing Policy' (set to 'Based on Link'), '\* WAN Weight' (set to '100'), and '\* WAN1 Weight' (set to '100'). A 'Save' button is at the bottom.

Step 4: Save the configuration

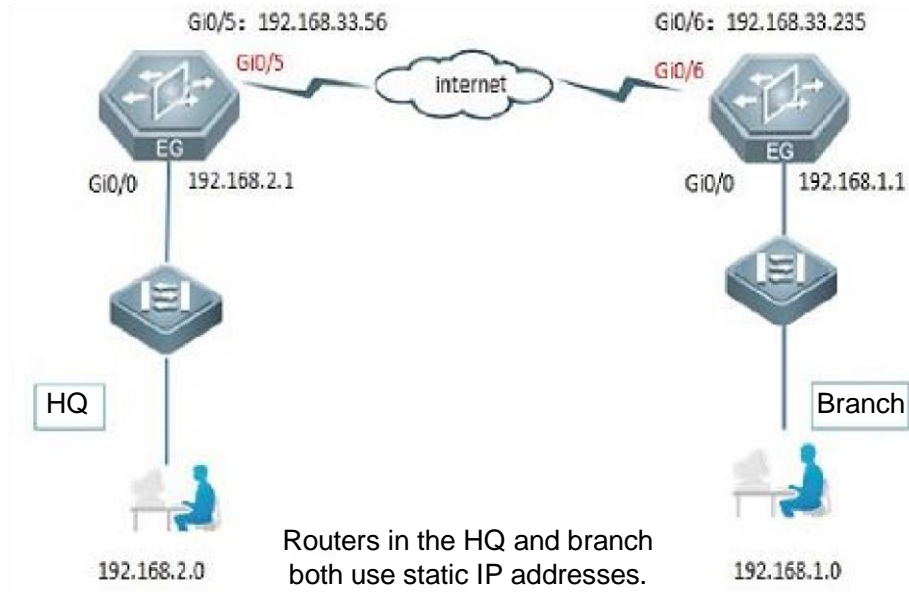
The screenshot displays the configuration page for a Ruijie Gateway (EG105G). The top navigation bar includes 'Overview', 'Online Clients', 'Gateway', 'Wireless', 'Switches', and 'Network'. The main content area is titled 'WAN Settings' and includes a 'Reboot' button. Below this, there are tabs for 'Single Line' and 'Dual-Line', with 'Dual-Line' selected. Underneath, there are tabs for 'WAN', 'WAN1', and 'ISP/Load Settings', with 'ISP/Load Settings' selected. The 'Load Balancing Settings' section contains a blue information box with the following text: 'Traffic will be routed based on ISP settings preferentially. The remaining traffic will be managed according to load mode.' Below this, there are two numbered instructions: 1. 'Balanced mode: The traffic will be spread across multiple links according to the weight of each WAN port. For example, if WAN and WAN1 weight are set to 3 and 2 respectively, 60% of the total traffic will be routed over WAN and 40% over WAN1.' 2. 'Primary & secondary mode: All traffic is routed over the primary interface. Once the primary interface fails, traffic will be switched over to the secondary interface. If there are multiple primary and secondary interfaces, please configure their weight (See balanced mode).' The configuration fields are: 'Load Mode' set to 'Balanced', 'Balancing Policy' set to 'Based on Link', '\* WAN Weight' set to '100', and '\* WAN1 Weight' set to '100'. A red box highlights the 'Save' button at the bottom of the configuration area.

## 5.2 IPsec VPN

### Networking Requirements

The HQ and branch routers use static IP addresses. The HQ router needs to verify the IP address of the branch router.

### Network Topology



### Configuration Key Points

1. Configure router A in the HQ as the IPsec server.
2. Configure router B in the branch as the IPsec client.
3. Keep parameter settings at both ends consistent. The parameter settings in this case are as follows:

Authentication mode: pre-shared key, with the key set to **ruijie**.

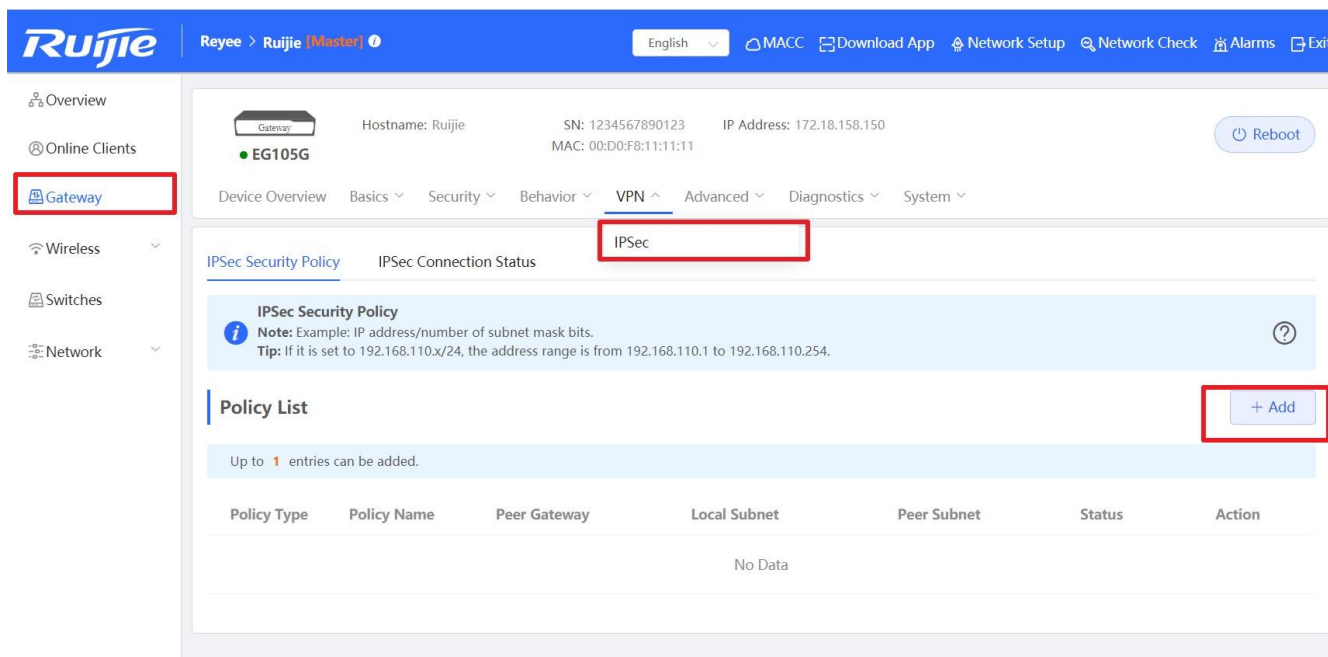
IKE algorithm: 3DES-MD5, DH2

IPsec negotiation scheme: ESP(3DES-MD5)

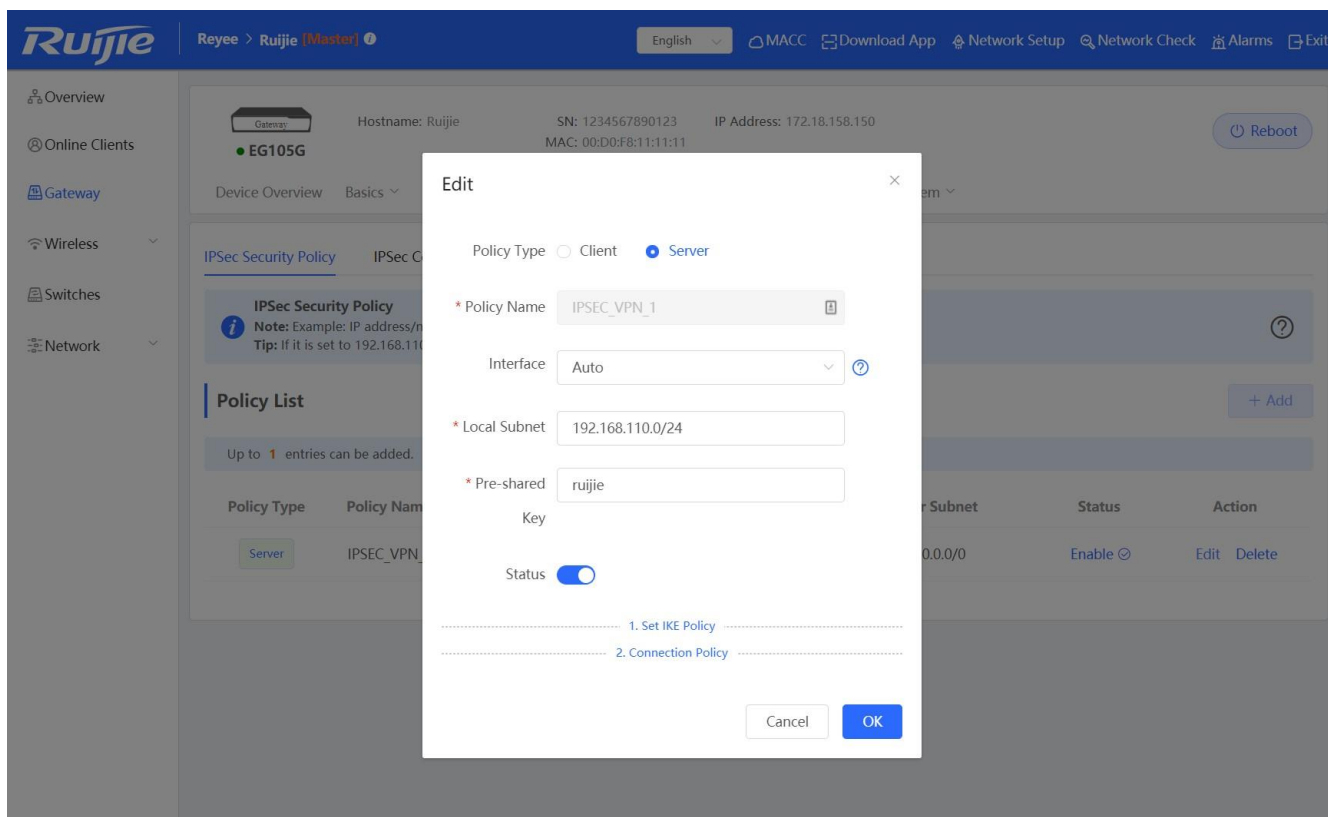
### Configuration Steps

Step 1: Configure the HQ router. Choose **Gateway** → **VPN** → **IPSec** → **Add** to add a policy.

---

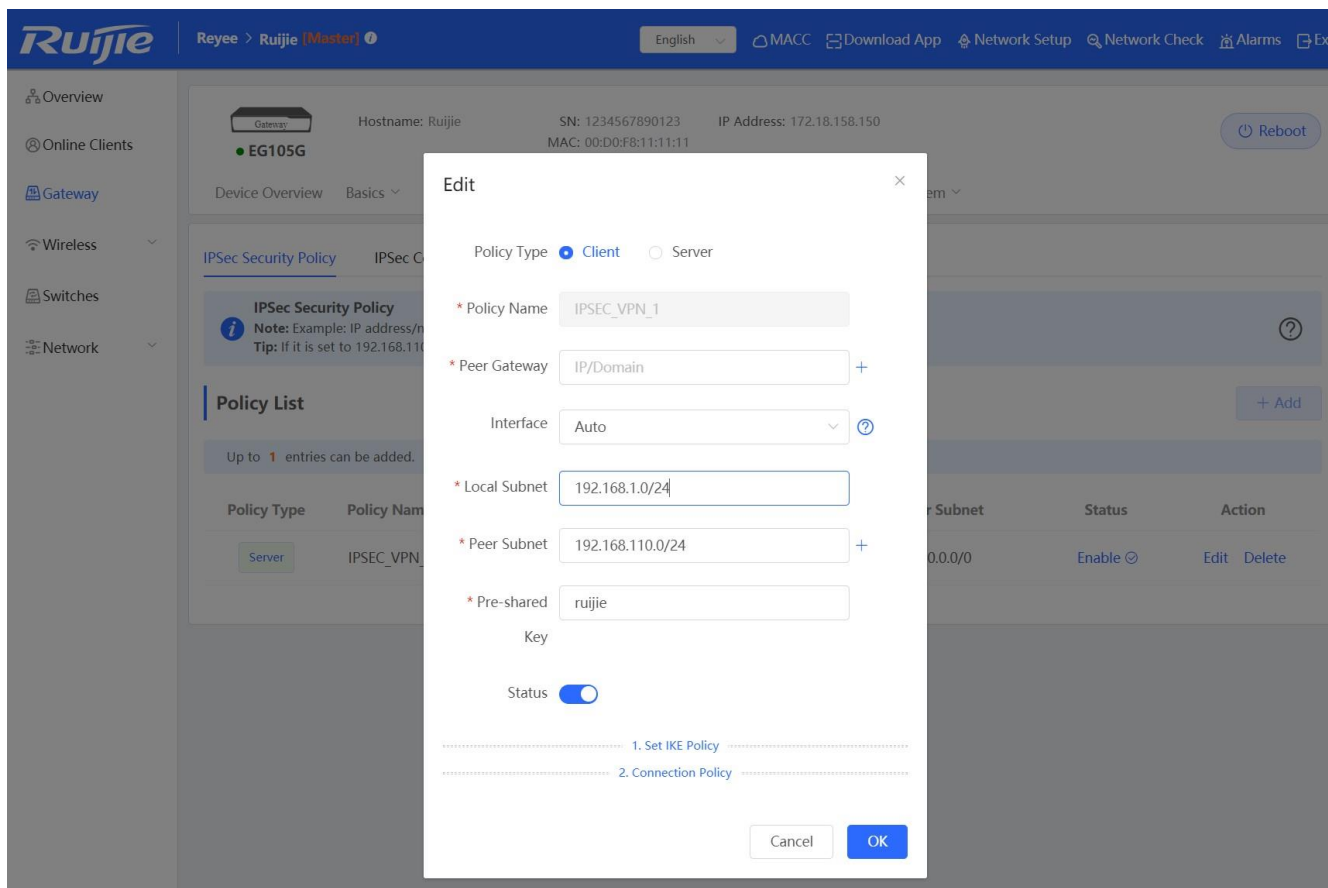


Step 2: Configure the server site’s subnet and pre-shared key. For building VPN with other Reyee EG series routers, you may keep the default setting of “Set IKE Policy” and “Connection Policy”; For other devices, the parameters need to be configured accordingly.



Step 3: Configure the branch router. Fill in the **Peer Gateway** (HQ’s public IP address or domain), **Local Subnet**, **Peer Subnet** and **Pre-shared Key** (need to be the same as HQ’s key)



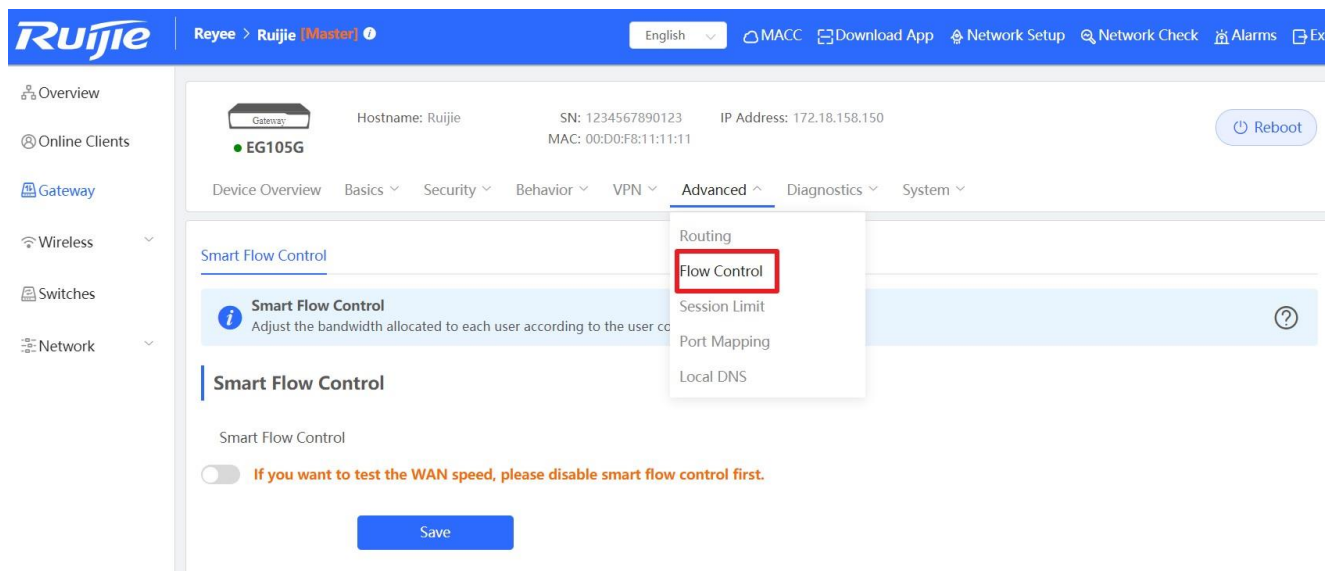


### 5.3 Smart Flow Control

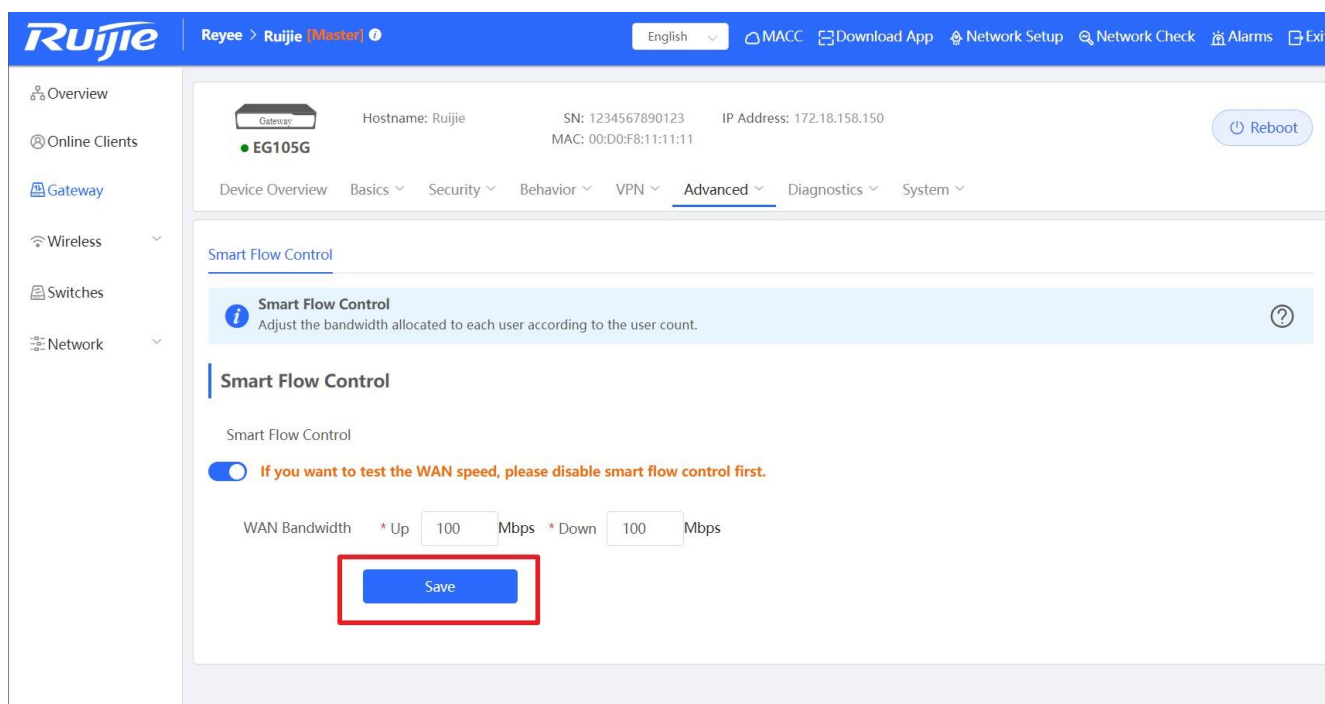
Reyee Smart Flow Control is a feature used to avoid congestion by optimizing user traffic. The working principle is shown as below: when the total user traffic is low than the maximum WAN bandwidth, the rate limit policy will not be applied, every user will get the required bandwidth; However, when the total user traffic exceeds the maximum WAN bandwidth, the user-based rate limit will take effect. The total WAN bandwidth will be equally allocated to every user. For example, If there are 10 users in the network, the total user traffic is 200Mbps and WAN bandwidth is 100Mbps, every user will get 10Mbps bandwidth after enabling the smart flow control feature.

#### Configuration Steps

Step 1: Choose **Gateway** → **Advanced** → **Flow Control** and enable the feature.



Step 2: Fill in the WAN bandwidth and Save the configuration.



## 5.4 Port Mapping

### Application Scenario

A customer deploys a server on the LAN and enables the HTTP or other services. The server address is a private address. WAN users can neither access this address directly nor use services provided by the server. In this case, you can enable the port mapping function to allow WAN users to access the LAN server.

For example, the server address is 192.168.1.20 and HTTP is enabled. As the server address is a private address, WAN users cannot directly access the HTTP service provided by the server. In this case, you can map the server address and server ports to a public network address on the EG device so that WAN users can access the HTTP service provided by the server.

### Networking Requirements

1. The WAN line is a single 10 Mbps fixed line. The address is 122.133.2.22, subnet mask is 255.255.255.0, and DNS address is 218.85.157.99.
2. There is a remote desktop server on the LAN. The IP address of the server is 192.168.1.20. If the LAN server needs to be accessed from the WAN, port mapping is required to map the interfaces of the LAN server to the public network. **Network**

### Topology

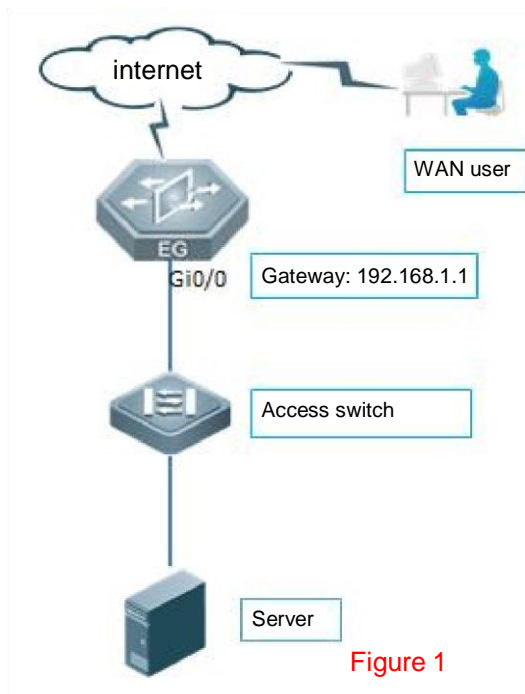
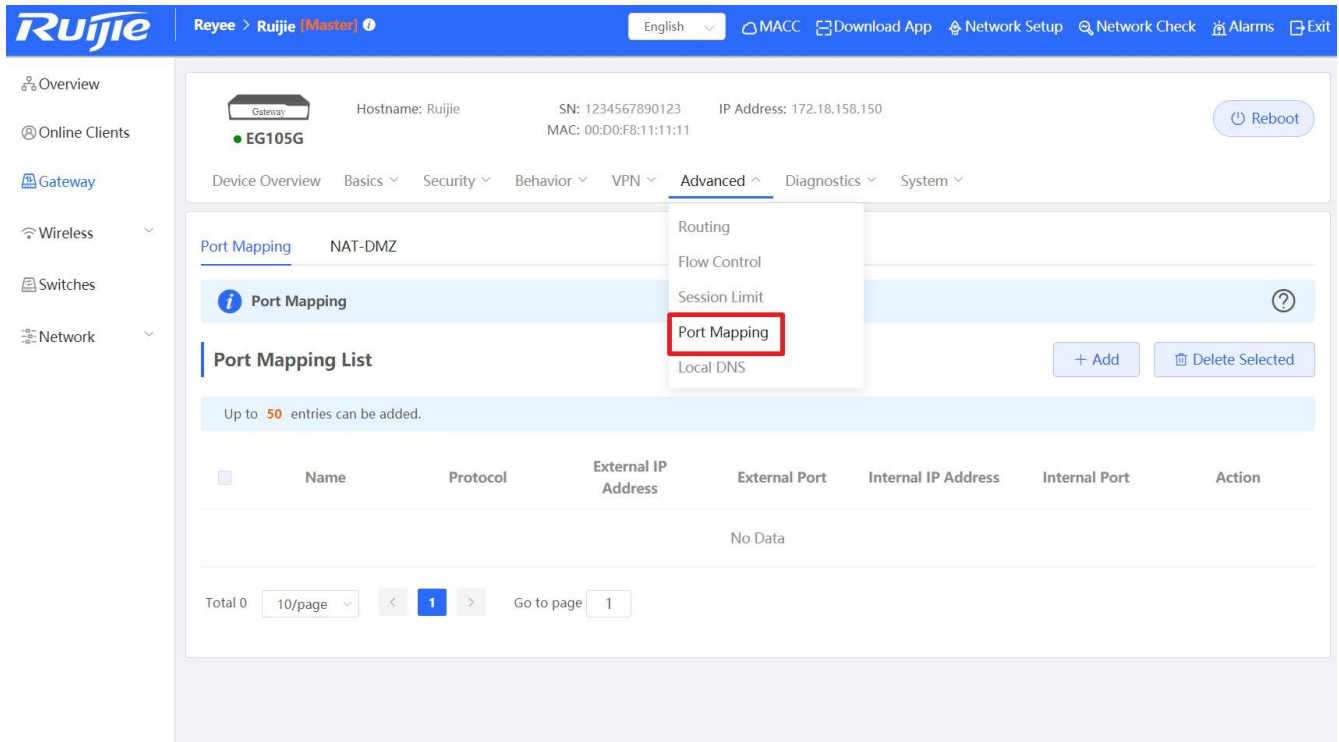


Figure 1

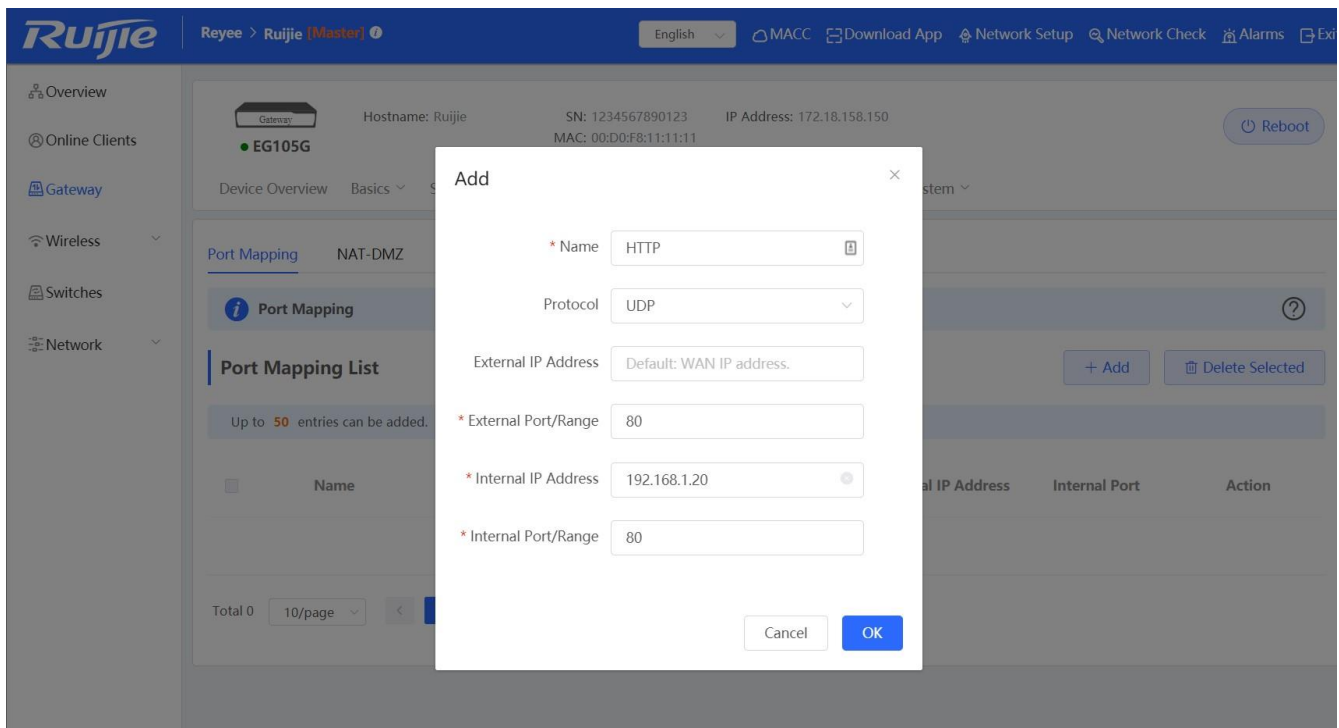
### Configuration Steps

Step 1: Choose **Gateway** → **Advanced** → **Port Mapping**

---



Step 2: Add a new Policy



**Internal IP Address:** Indicates the IP address of the server.

**Internal Port/Range:** Indicates the port for the server that is to provide external services.

**External IP:** Indicates the IP address of a WAN port.

**External Port/Range:** Indicates the target WAN service port of port mapping.

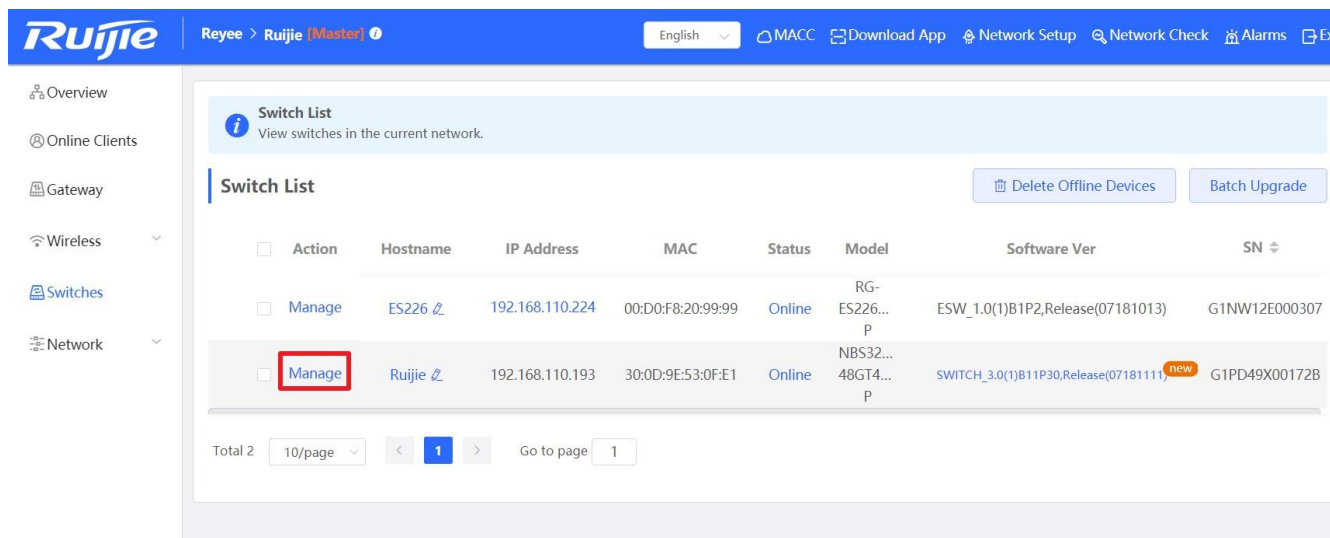
## 6 Reyee NBS Series Switch Configuration

### 6.1 VLAN Setting

A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer. VLANs work by applying tags to network frames and handling these tags in networking systems – creating the appearance and functionality of network traffic that is physically on a single network but acts as if it is split between separate networks. In this way, VLANs can keep network applications separate despite being connected to the same physical network, and without requiring multiple sets of cabling and networking devices to be deployed.

#### Configuration Steps:

Step 1: Choose **Switches** → **Manage** to configure the switch



Step 2: Choose **VLAN** and Add a new VLAN

The image shows two screenshots of the Ruijie management interface. The top screenshot displays the 'VLAN List' page for a switch with Hostname 'Ruijie'. The 'VLAN' menu item is highlighted with a red box. The '+ Add' button is also highlighted with a red box. Below the buttons, a table lists the existing VLANs:

VLAN ID	Description	Port	Action
1	VLAN0001	Gi1-2,Gi5-48,Te49-52,Ag1	Edit Delete

The bottom screenshot shows the same interface with an 'Add' dialog box open. The dialog contains the following fields:

- \* VLAN ID: 10 (Range: 1-4094)
- Description: IT departmant (Max: 32 characters)

Buttons for 'Cancel' and 'OK' are visible at the bottom of the dialog.

Step 3: Assign the new VLAN to ports.

The screenshot displays the Ruijie Reyeer web management interface for a switch. The top navigation bar includes 'Home', 'VLAN', 'Monitor', 'Ports', 'Security', 'Advanced', 'Diagnostics', and 'System'. The 'VLAN List' section is active, showing a table with columns for VLAN ID, Description, Port, and Action. Two VLANs are listed: VLAN 1 (VLAN0001) and VLAN 10 (IT department). A 'Batch Edit' button is highlighted with a red box. Below the VLAN list is the 'Port List' section, which shows a table with columns for Port, Port Mode, Access VLAN, Native VLAN, Permit VLAN, and Action. Ports Gi1 and Gi2 are in ACCESS mode and assigned to VLAN 1. Ports Gi3 and Gi4 are listed as member ports of Ag1.

Switch Hostname: Ruijie SN: G1PD49X00172B  
NBS3200-48GT4XS-P MAC: 30:0D:9E:53:0F:E1 IP Address: 192.168.110.192

Click to Collapse the list.

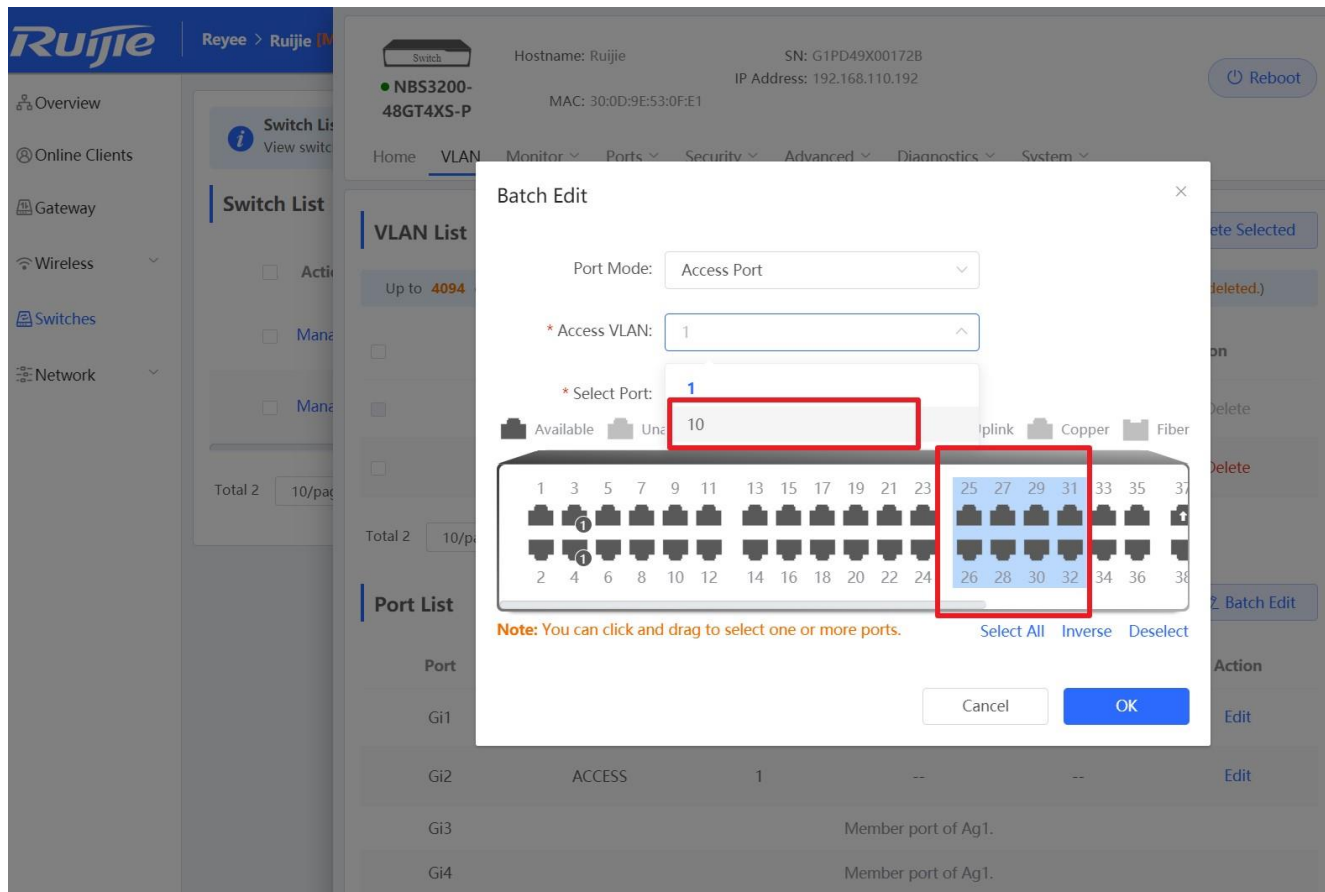
Up to 4094 entries can be added.( The default VLAN, management VLAN, native VLAN, svi Vlan and access VLAN cannot be deleted.)

VLAN ID	Description	Port	Action
1	VLAN0001	Gi1-2,Gi5-48,Te49-52,Ag1	Edit Delete
10	IT department	--	Edit Delete

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

Batch Edit

Port	Port Mode	Access VLAN	Native VLAN	Permit VLAN	Action
Gi1	ACCESS	1	--	--	Edit
Gi2	ACCESS	1	--	--	Edit
Gi3			Member port of Ag1.		
Gi4			Member port of Ag1.		



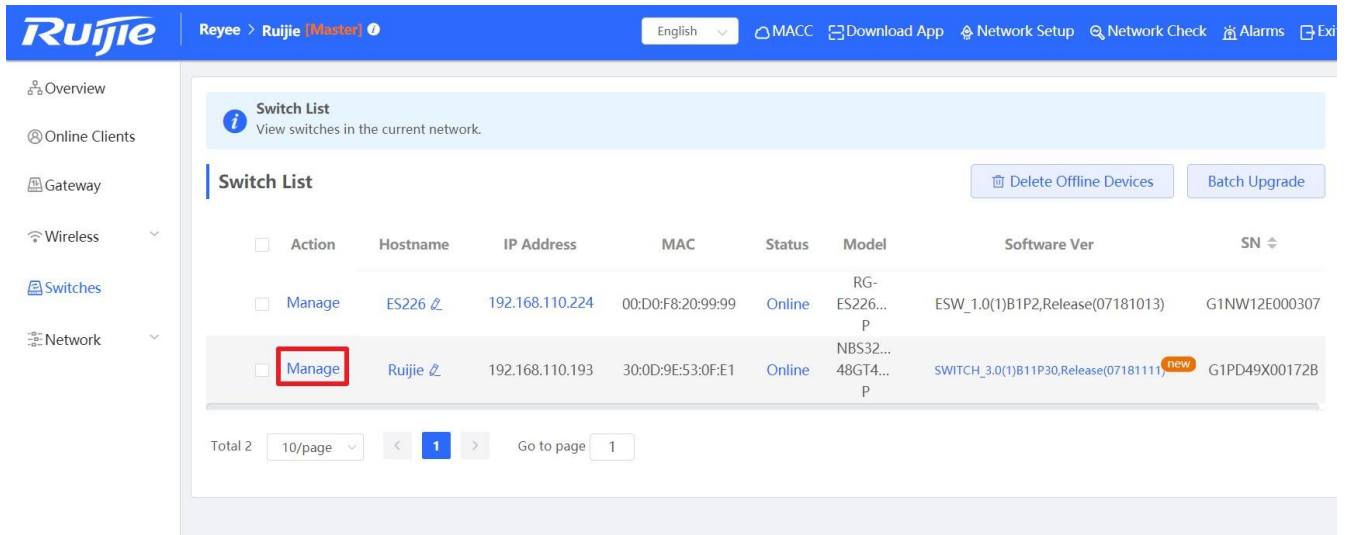
## 6.2 Access Control List (ACL)

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

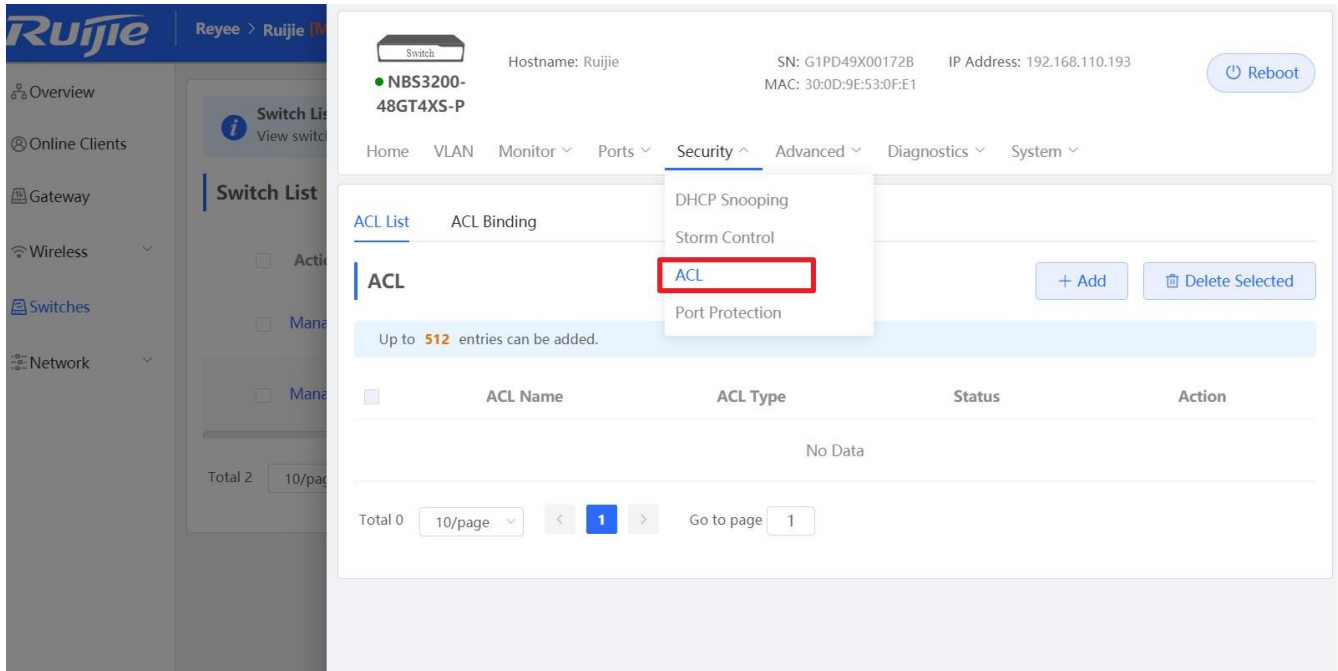
### Configuration Steps:

Step 1: Choose **Switches** → **Manage** to configure the switch

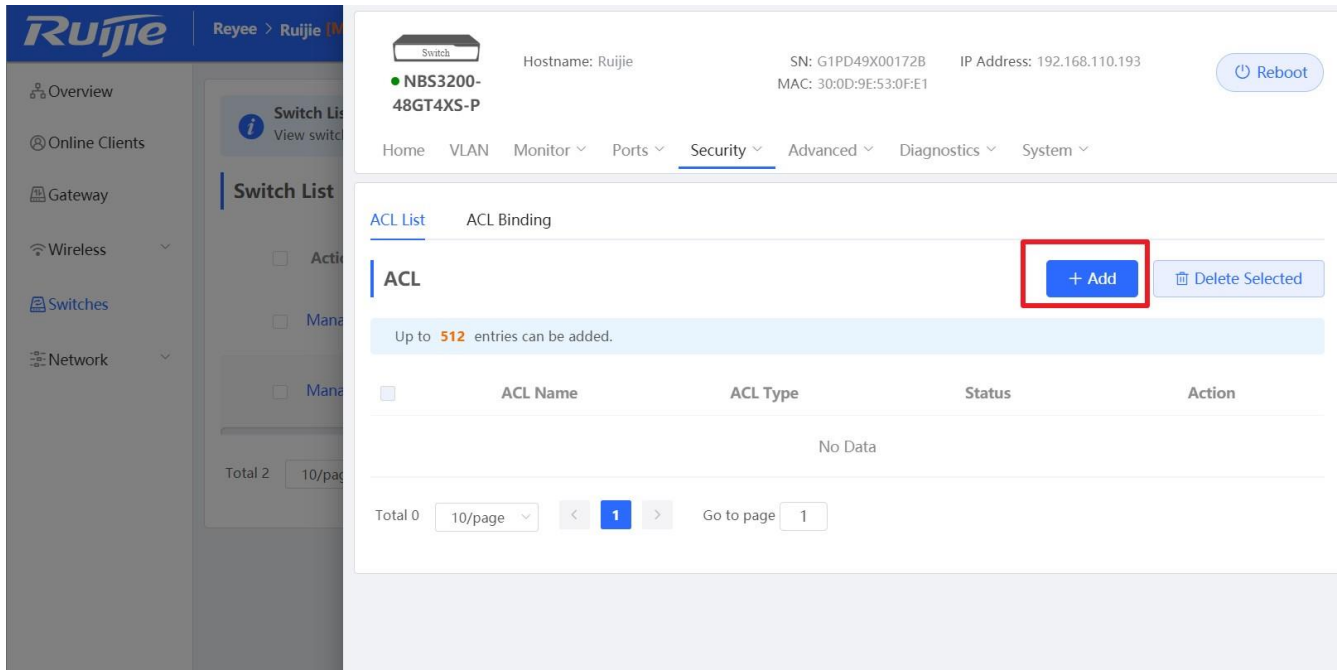




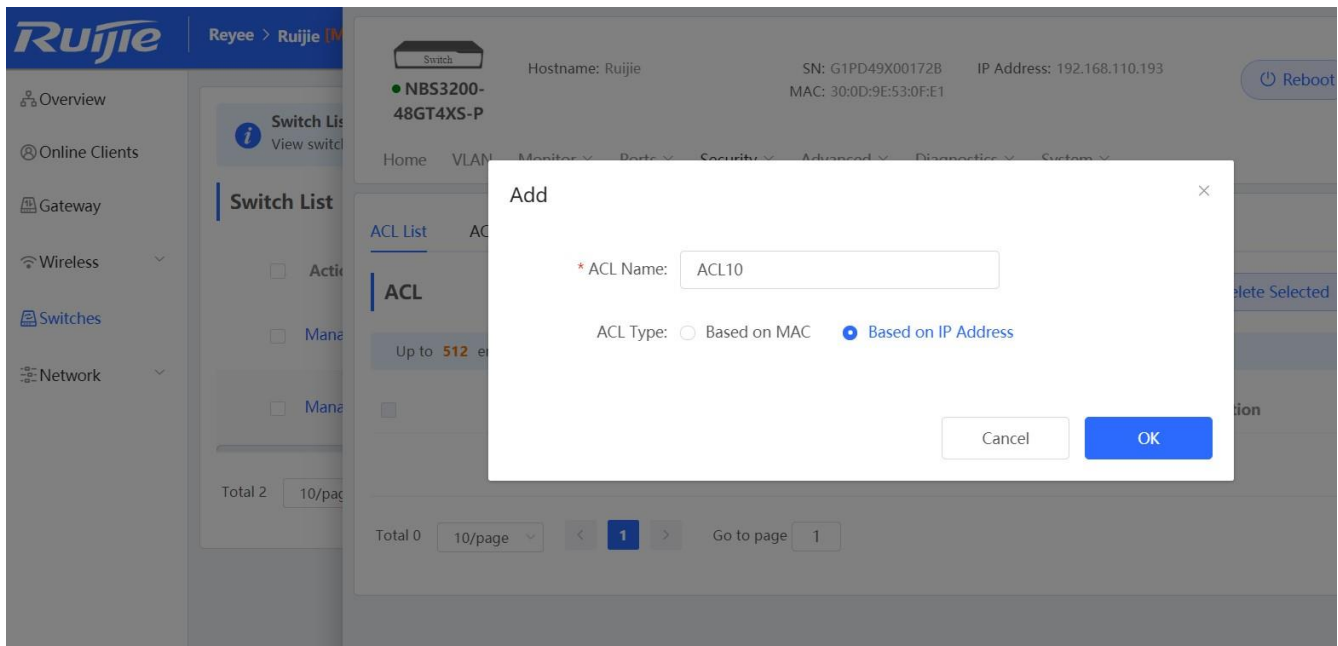
Step 2: Choose **Security** → **ACL** to enter the ACL management page



Step 3: Click the **Add** button to add an ACL



Step 4: Fill in the ACL name and type to create an ACL



Step 4: Click "Details" to configure the ACL rule.

Hostname: Ruijie SN: G1PD49X00172B IP Address: 192.168.110.193  
 MAC: 30:0D:9E:53:0F:E1

Home VLAN Monitor Ports **Security** Advanced Diagnostics System

ACL List ACL Binding

ACL

Up to 512 entries can be added.

ACL Name	ACL Type	Status	Action
ACL10	Based on IP Address	Inactive	<a href="#">Details</a> <a href="#">Edit</a> <a href="#">Delete</a>

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

[ACL10]Settings

ACL:  Block  Allow

IP Protocol Number:  All

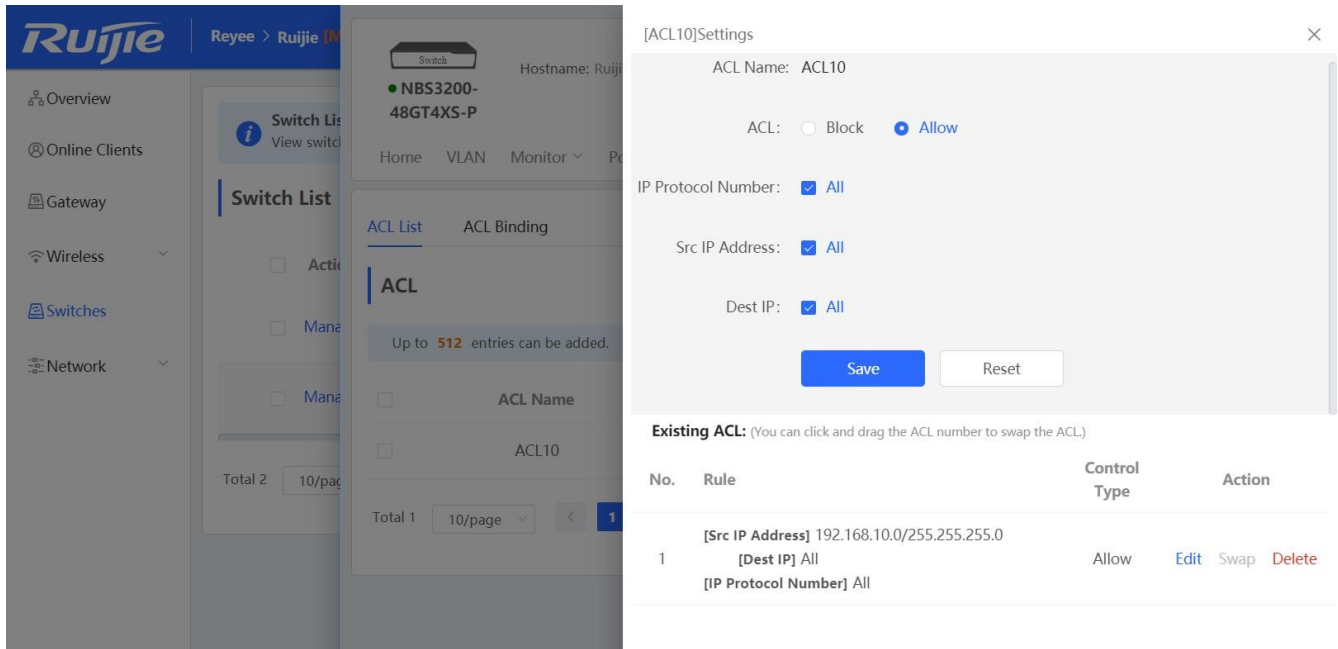
Src IP Address:  All  
 192.168.10.0 / 255.255.255.0  
 (Address/Submask)

Dest IP:  All

Save Reset

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

No.	Rule	Control Type	Action
No Data Available			



Step 5: Bind the ACL to the interface.

The screenshot shows the Ruijie web management interface for a switch. The top navigation bar includes 'Home', 'VLAN', 'Monitor', 'Ports', 'Security', 'Advanced', 'Diagnostics', and 'System'. The 'Security' menu is expanded, and 'ACL Binding' is selected. A red box highlights the 'ACL Binding' link in the navigation menu. Below the navigation, there is a section for 'ACL Binding' with a '+ Batch Add' and 'Unbind Selected' button. A table lists the binding configuration for various ports (Gi1 to Gi10). The 'Action' column for Gi1 has a red box around the 'Edit' link.

Port	MAC-based ACL	IP-based ACL	Action
Gi1	--	--	<b>Edit</b> Unbind
Gi2	--	--	Edit Unbind
Gi3		Member port of Ag1.	
Gi4		Member port of Ag1.	
Gi5	--	--	Edit Unbind
Gi6	--	--	Edit Unbind
Gi7	--	--	Edit Unbind
Gi8	--	--	Edit Unbind
Gi9	--	--	Edit Unbind
Gi10	--	--	Edit Unbind

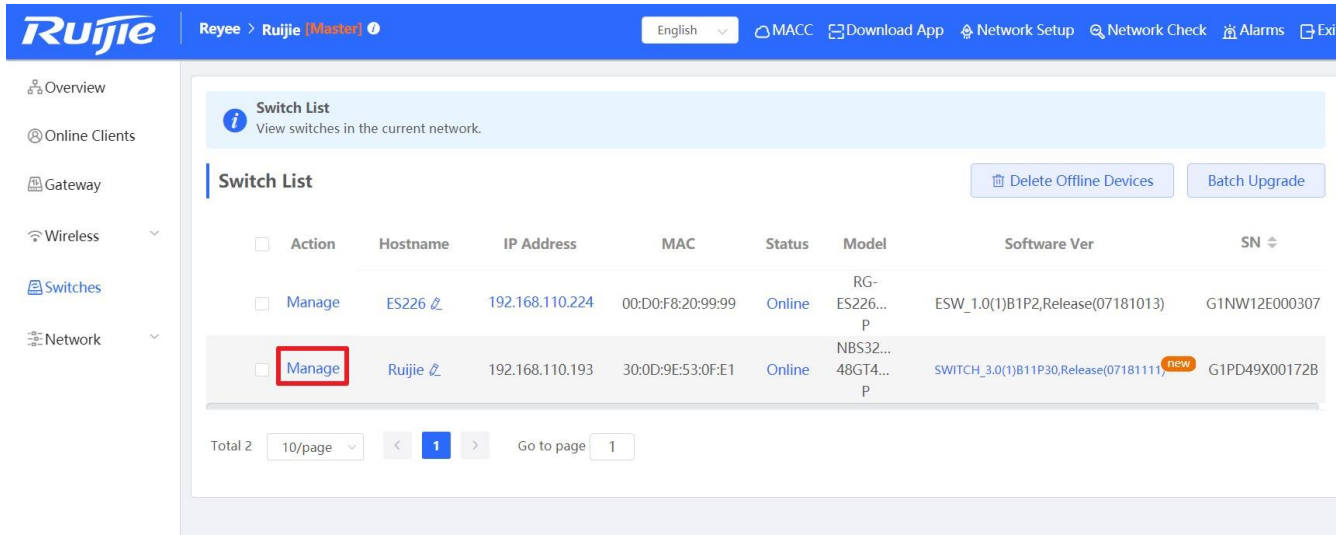
The screenshot shows the 'Edit' dialog box in the Ruijie web management interface. The dialog has a title bar 'Edit' and a close button 'X'. It contains two dropdown menus: 'MAC-based ACL' with 'No Data' selected, and 'IP-based ACL' with 'ACL10' selected. A red box highlights the 'IP-based ACL' dropdown. At the bottom right, there are 'Cancel' and 'OK' buttons, with the 'OK' button also highlighted by a red box.

## 6.3 Port Isolation

Port isolation implements layer-2 isolation of packets. After port isolation is enabled (which is disabled by default), data cannot be forwarded between isolated ports.

### Configuration Step:

Step 1: Choose **Switches** → **Manage** to configure the switch

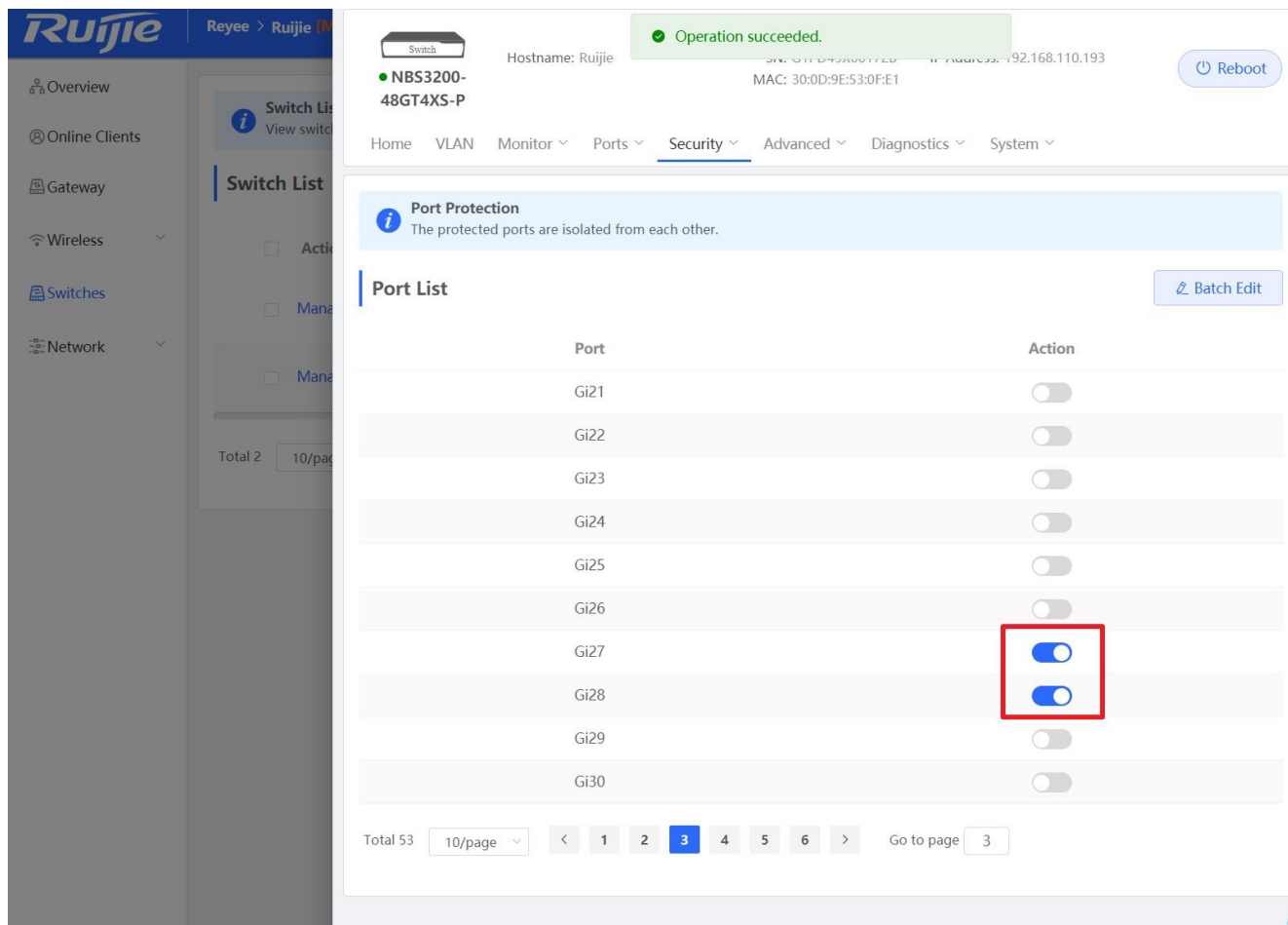


Step 2: Choose **Security** → **Port Protection** to configure the port isolation

The screenshot shows the Ruijie management interface for a switch. The top navigation bar includes 'Home', 'VLAN', 'Monitor', 'Ports', 'Security', 'Advanced', 'Diagnostics', and 'System'. The 'Security' menu is expanded, showing options for 'DHCP Snooping', 'Storm Control', 'ACL', and 'Port Protection', with 'Port Protection' highlighted in a red box. Below the navigation, the 'Port Protection' section is active, displaying a 'Port List' table. The table has two columns: 'Port' and 'Action'. The 'Action' column contains toggle switches for each port, with Gi3 and Gi4 showing 'Member port of Ag1.' and others showing a simple toggle. A 'Batch Edit' button is located to the right of the table. At the bottom, there is a pagination control showing 'Total 53', '10/page', and page numbers 1 through 6, with 'Go to page 1'.

Port	Action
Gi1	<input type="checkbox"/>
Gi2	<input type="checkbox"/>
Gi3	Member port of Ag1.
Gi4	Member port of Ag1.
Gi5	<input type="checkbox"/>
Gi6	<input type="checkbox"/>
Gi7	<input type="checkbox"/>
Gi8	<input type="checkbox"/>
Gi9	<input type="checkbox"/>
Gi10	<input type="checkbox"/>

Step 3: Enable the Port Isolation on Ports.



## 6.4 DHCP Snooping

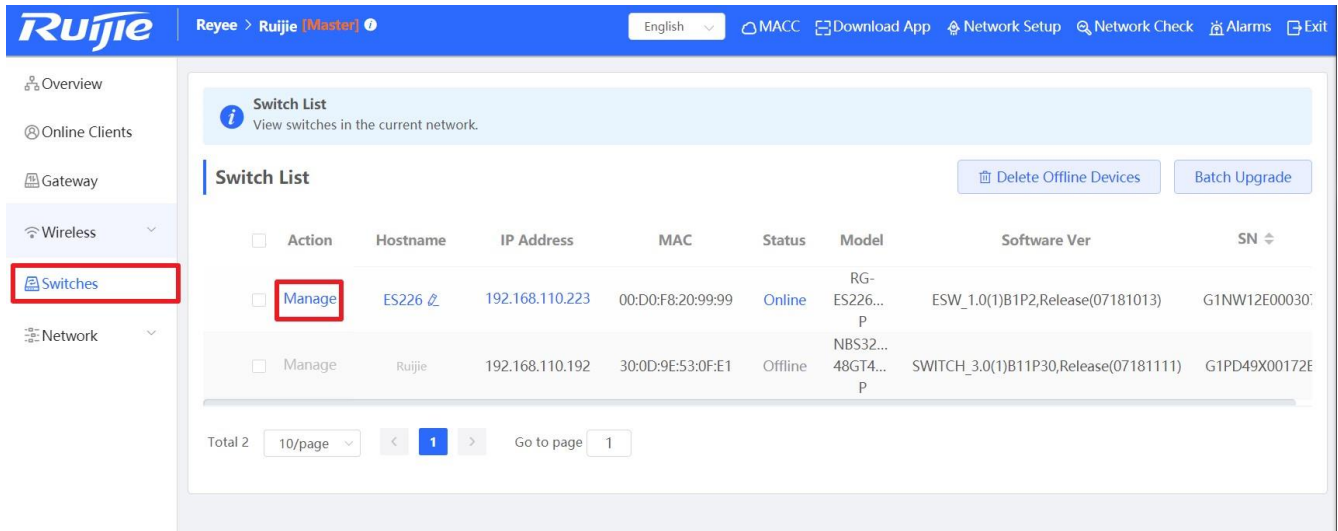
In the DHCP-enabled network, the general problem facing administrator is that some users use private IP addresses rather than dynamically obtaining IP addresses. As a result, some users using dynamic IP addresses cannot access the network, making network application more complex. In dynamic DHCP binding mode, the device records how legal users obtain IP addresses during the course of DHCP Snooping for security purpose.

Enabling DHCP Snooping helps filter DHCP packets. Only forwards DHCP request packets to the trusted port and DHCP response packets from the trusted port. The port connected to the DHCP server is configured as the trusted port generally

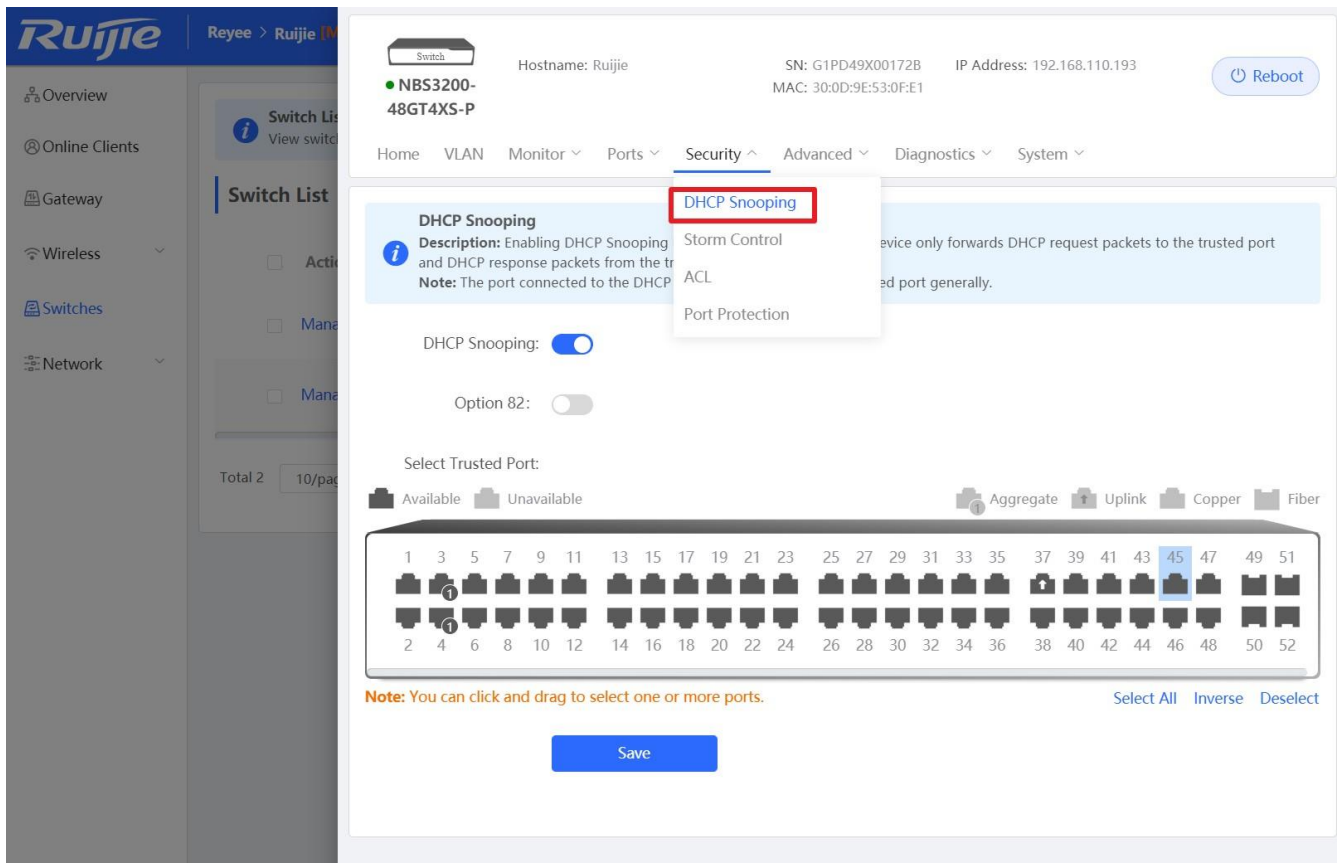
### Configuration Steps

Step 1: Choose **Switches** → **Manage** to configure the switch





Step 2: Choose **Security** → **DHCP Snooping** to configure the DHCP snooping

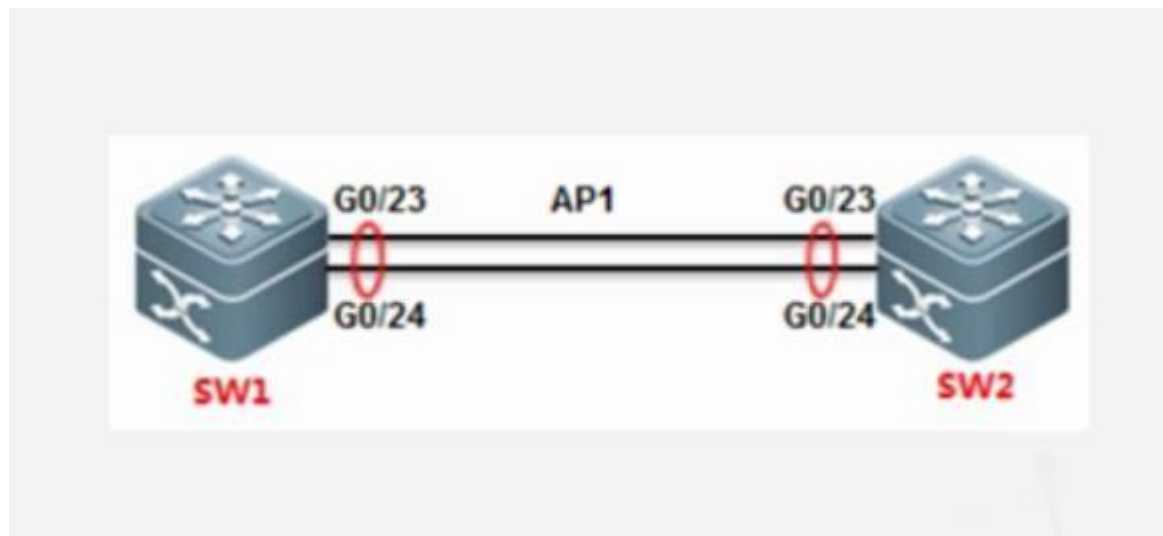


Step 3: Enable the DHCP and select the trusted port (the port connect to a DHCP server )

The screenshot shows the Ruijie web management interface for a switch. The switch model is NBS3200-48GT4XS-P. The configuration page is for the Security tab, specifically the DHCP Snooping section. The DHCP Snooping feature is enabled, indicated by a blue toggle switch. Below it, the Option 82 feature is disabled. A section titled 'Select Trusted Port' shows a grid of 48 ports. Port 45 is highlighted with a red box, indicating it is selected as a trusted port. The interface also includes a 'Save' button at the bottom.

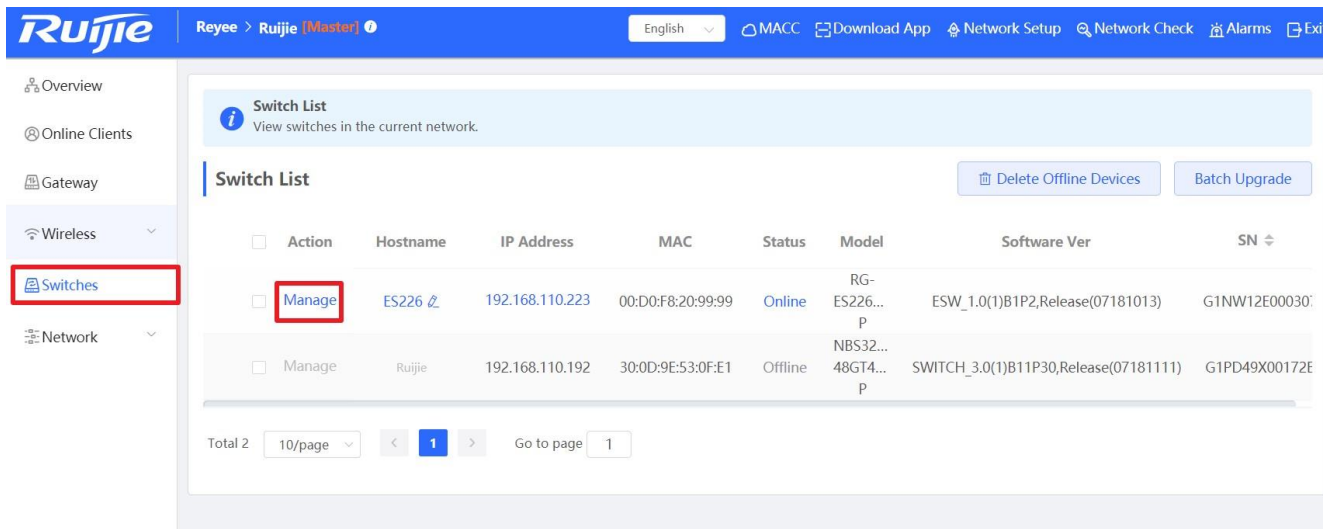
## 6.5 Link Aggregation

Link aggregation is a technology to combine multiple network connections in parallel in order to increase throughput and provide redundancy in case one of the links should fail.

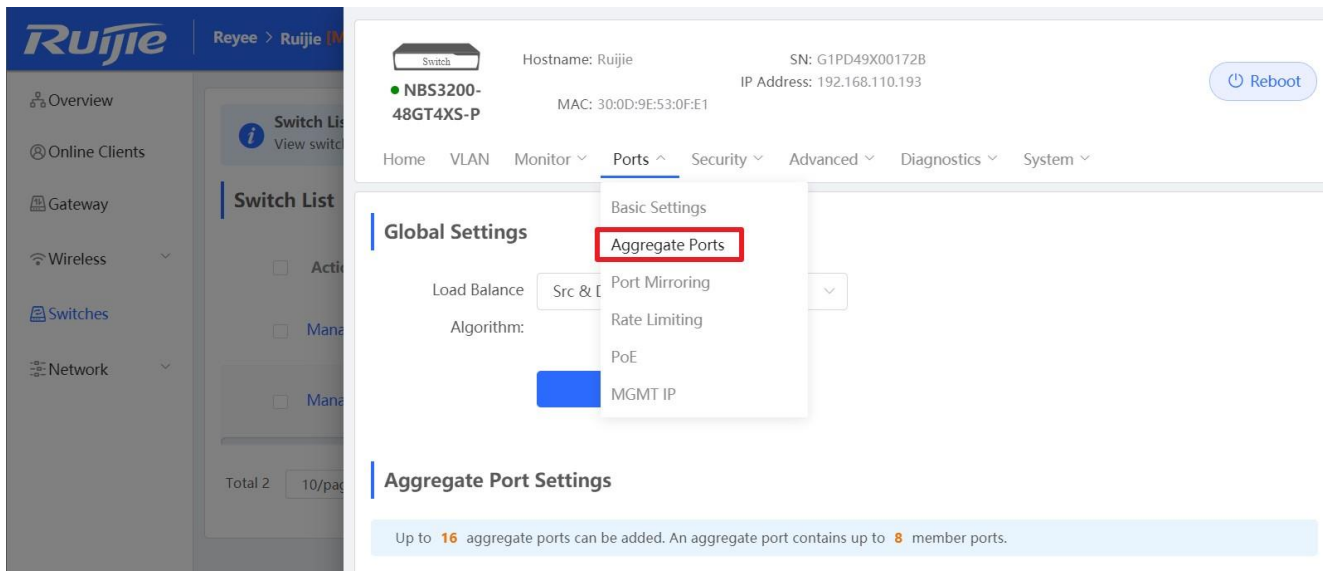


### Configuration Steps

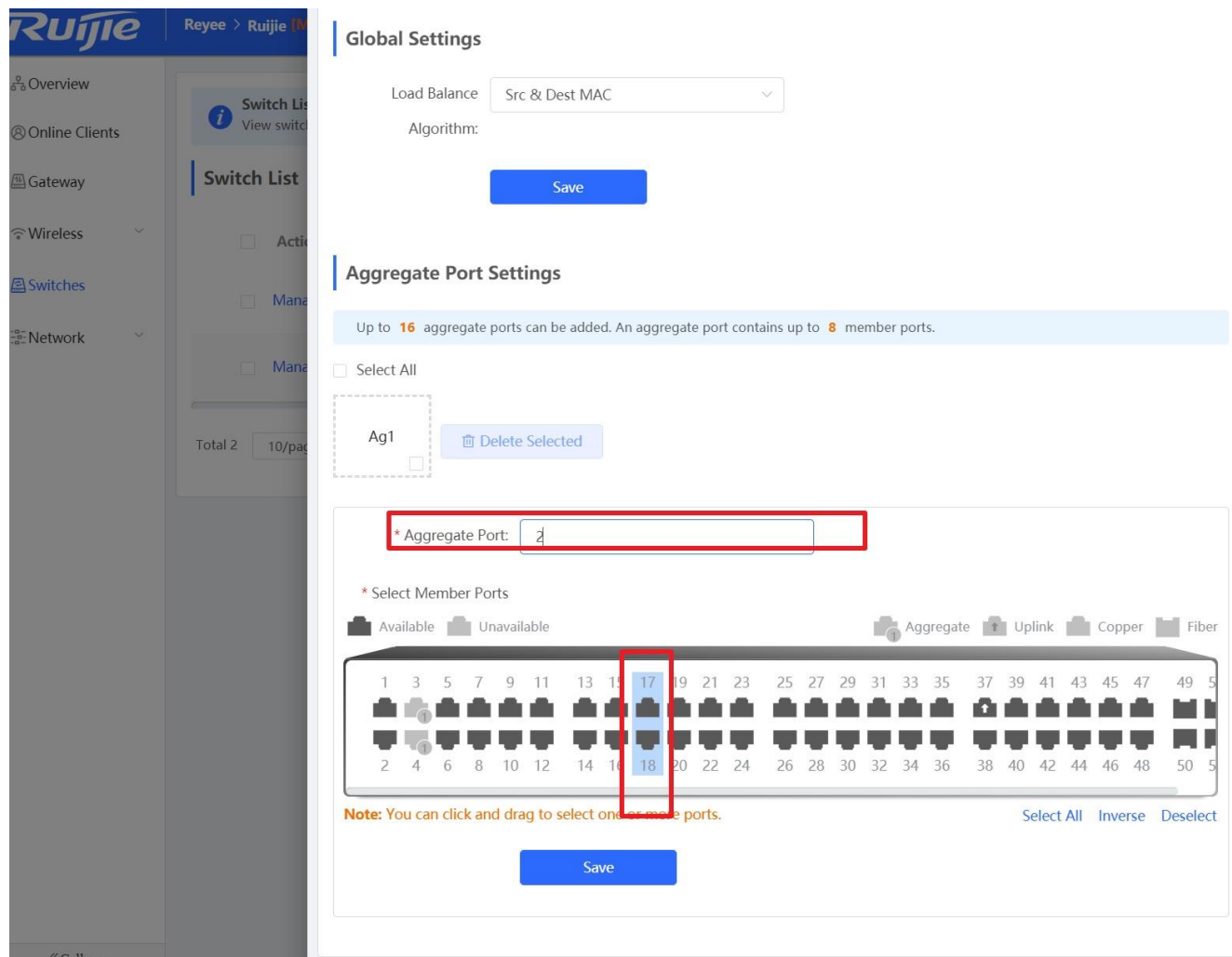
Step 1: Choose **Switches** → **Manage** to configure the switch



Step 2: Choose **Ports** → **Aggregate Ports** to configure the link aggregation



Step 3: Fill in the aggregate port number and select the port member.



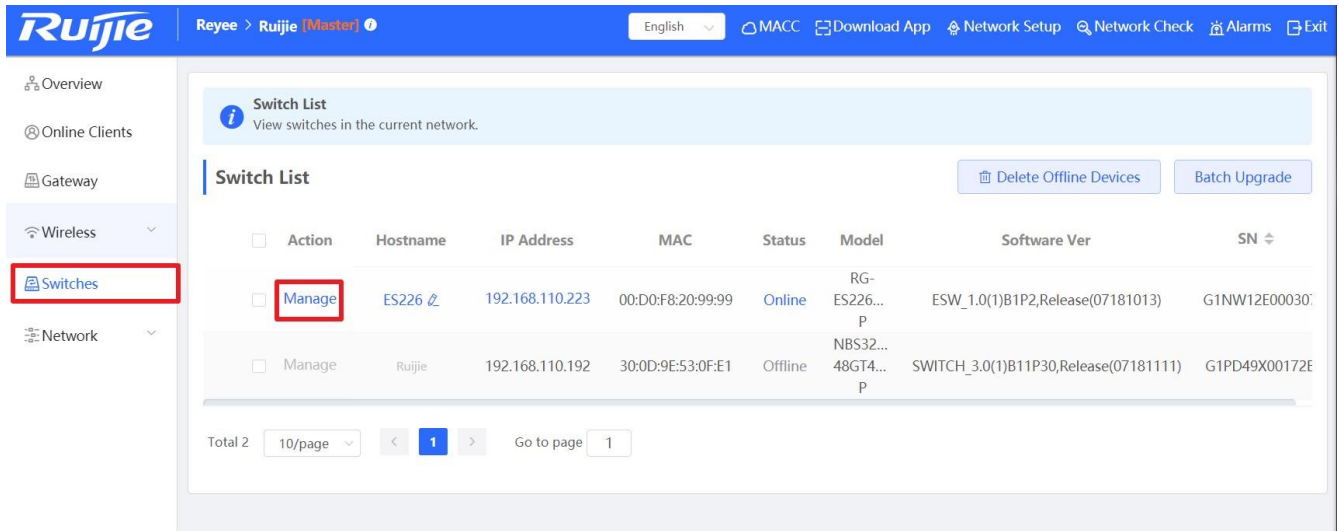
## 6.6 Storm Control

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

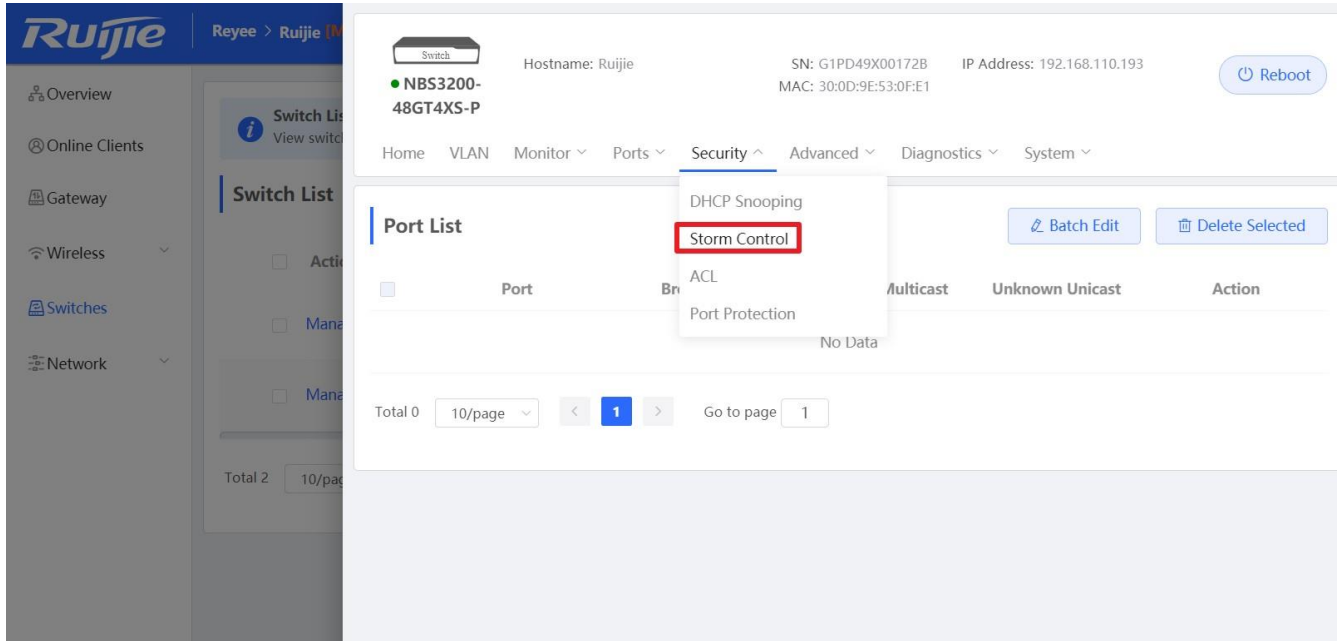
Users can perform storm control separately for the broadcast, multicast, and unknown unicast data flows. When the rate of broadcast, multicast, or unknown unicast packets received by the device port exceeds the specified rate, the number of packets allowed per second, or the number of kilobits allowed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

### Configuration Steps

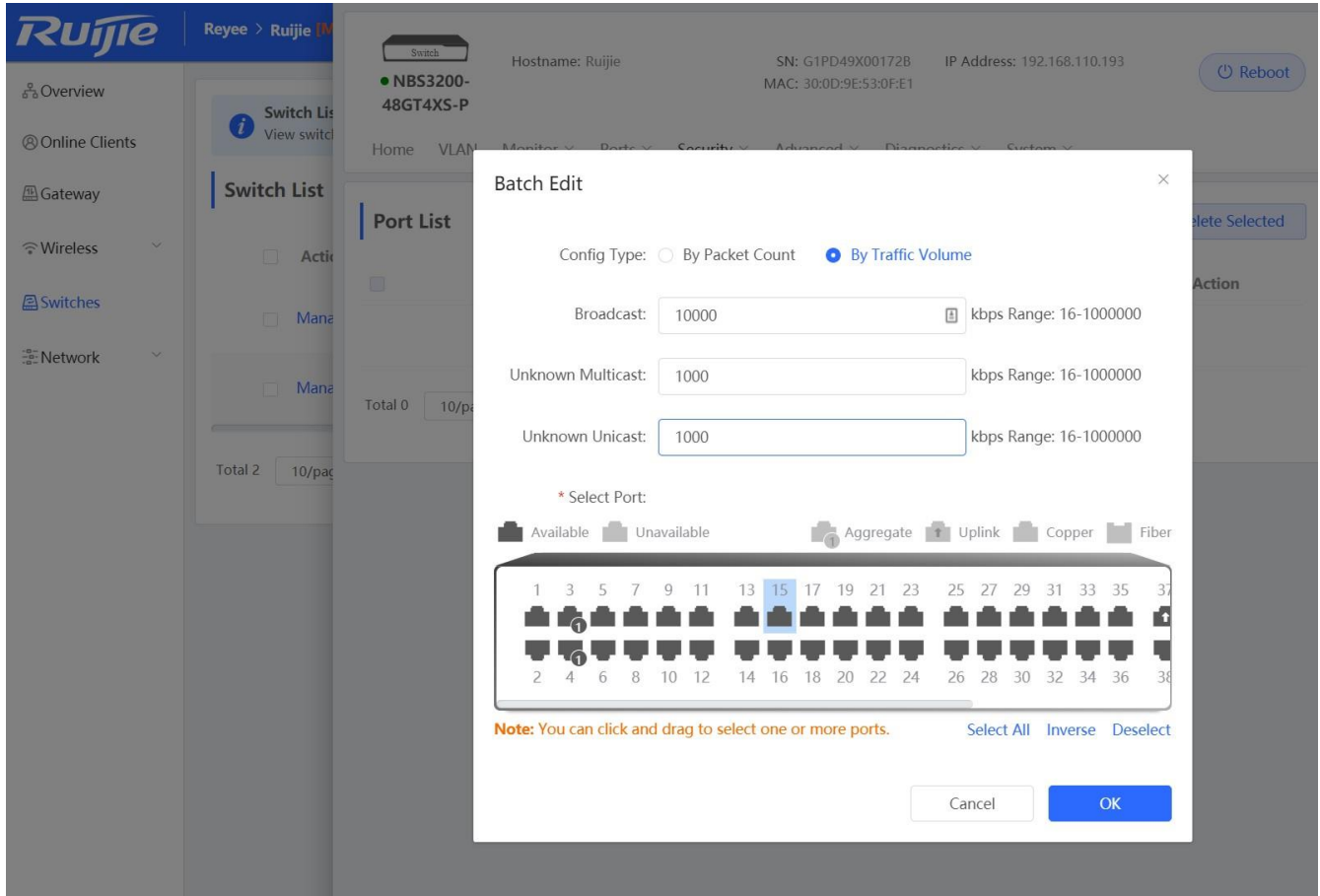
Step 1: Choose **Switches** → **Manage** to configure the switch



Step 2: Choose **Security** → **Storm Control**, and click **Batch Edit**



Step 3: Fill in the threshold value and select the port



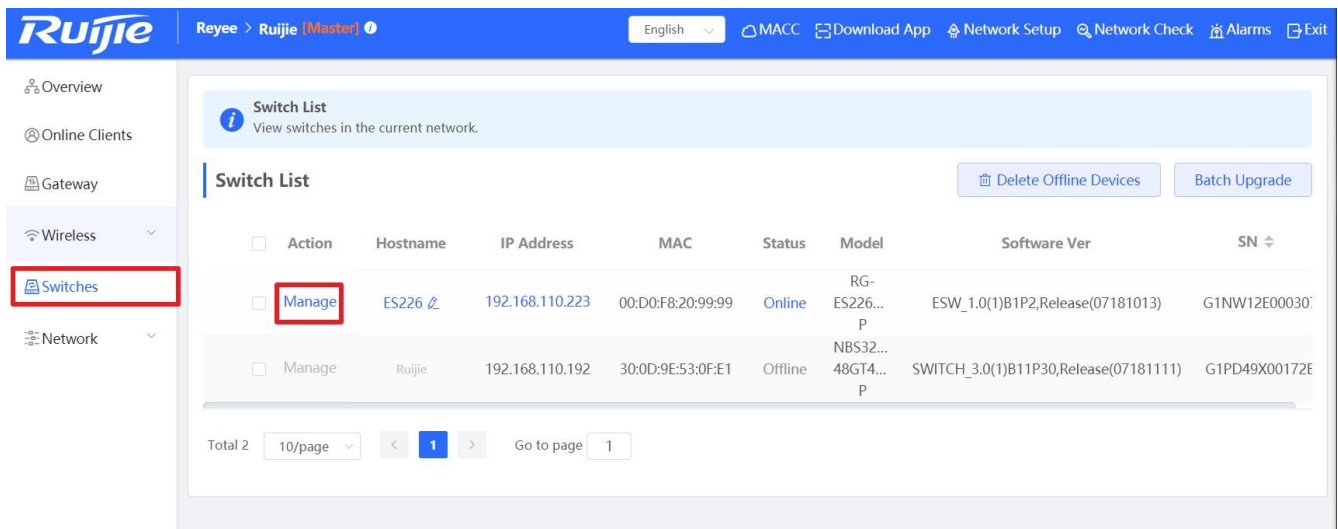
# 7 Reyee ES Series Switch Configuration

## 7.1 VLAN Setting

A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer. VLANs work by applying tags to network frames and handling these tags in networking systems – creating the appearance and functionality of network traffic that is physically on a single network but acts as if it is split between separate networks. In this way, VLANs can keep network applications separate despite being connected to the same physical network, and without requiring multiple sets of cabling and networking devices to be deployed.

### Configuration Steps:

Step 1: Choose **Switches** → **Manage** to configure the switch



Step 2: Enable the VLAN settings (disabled by default)

The screenshot displays the Ruijie network management interface. On the left is a navigation sidebar with options like Overview, Online Clients, Gateway, Wireless, Switches, and Network. The main content area is titled 'Switch List' and shows a table of switches. A 'Support VLAN Settings' toggle is highlighted with a red box. To the right, a 'System Info' panel provides details for a specific switch (ES226), including its MAC status, model, software version, SN, MAC, IP address, submask, gateway, and DNS server. Below this are links for Monitor Info, Port Statistics, Cable Diagnostics, and MAC List.

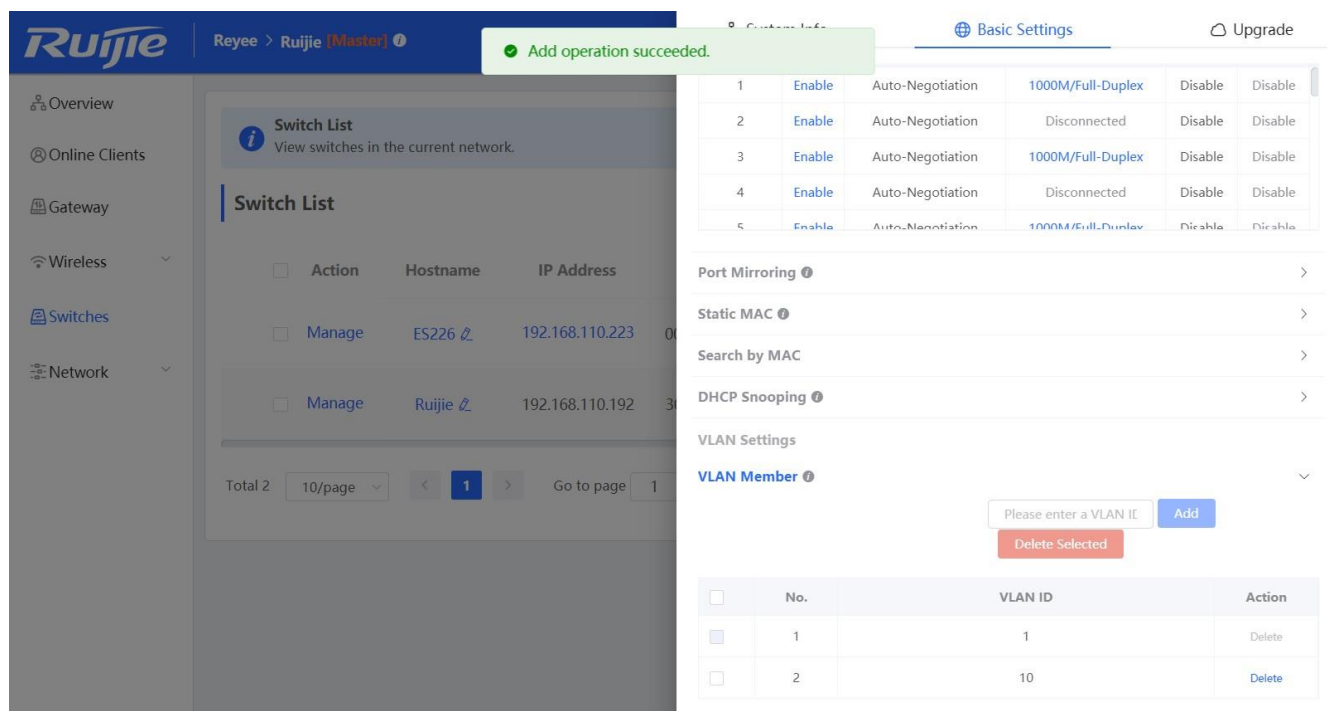
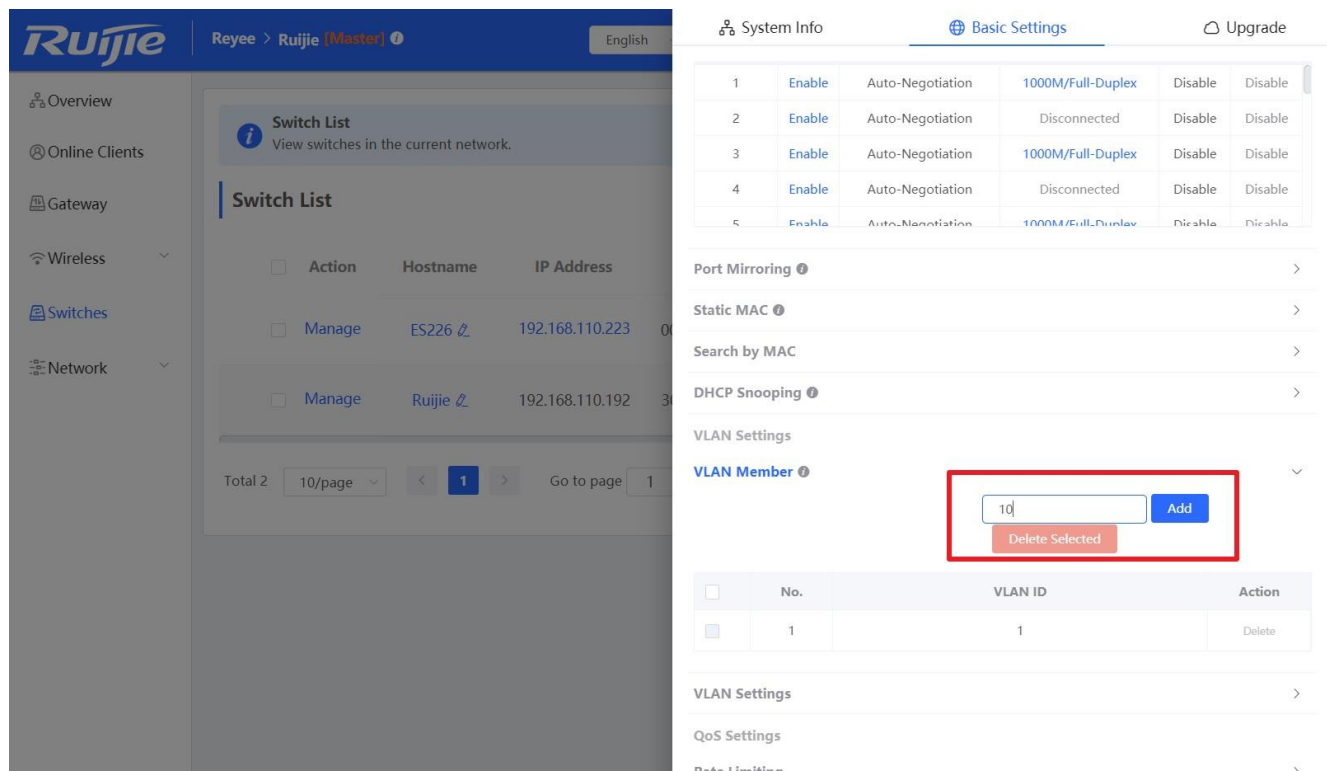
Action	Hostname	IP Address
<input type="checkbox"/> Manage	ES226	192.168.110.223
<input type="checkbox"/> Manage	Ruijie	192.168.110.192

System Info for ES226:

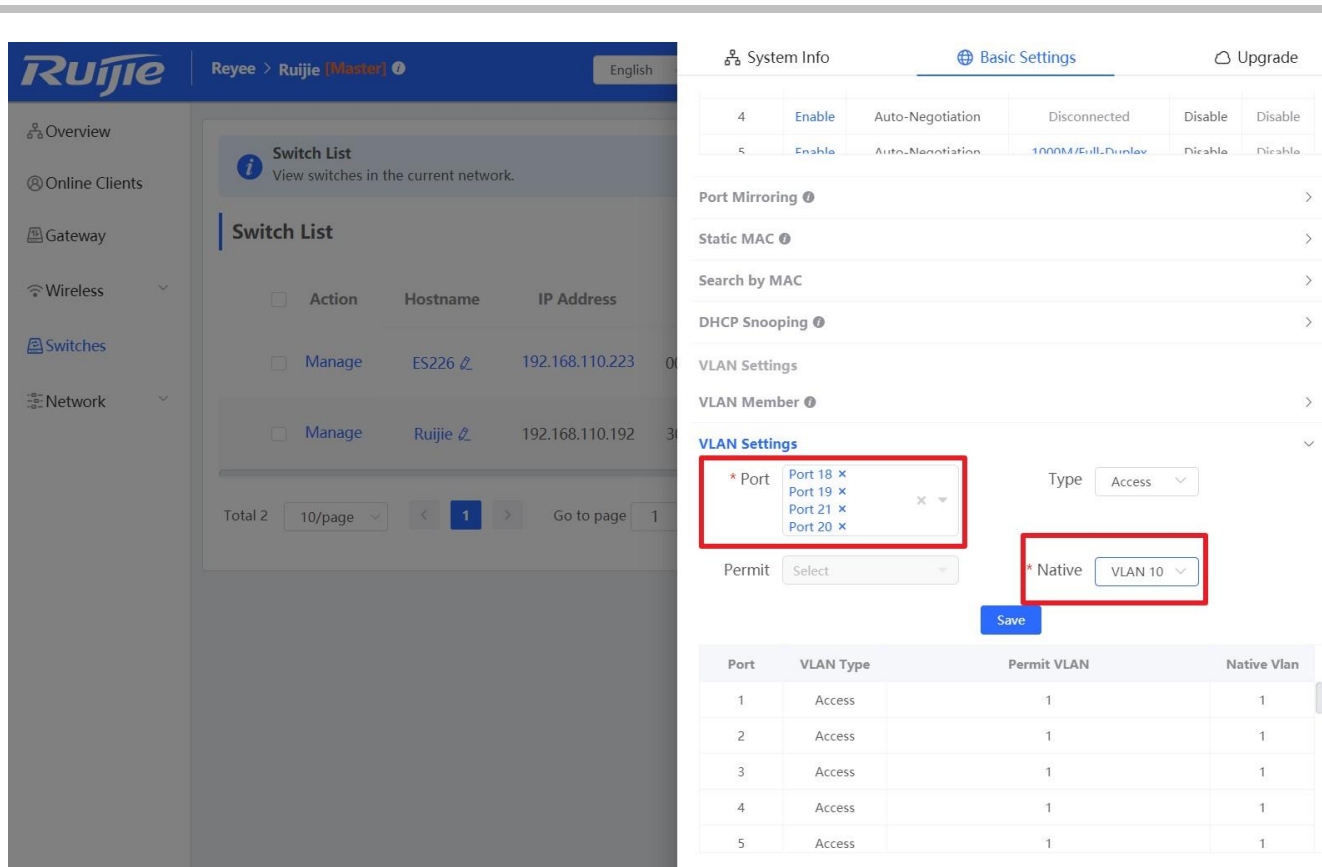
- MACC Status: Connected
- Model: RG-ES226GC-P
- Software Ver: ESW\_1.0(1)B1P2,Release(07181013)
- SN: G1NW12E000307
- MAC: 00:D0:F8:20:99:99
- IP Address: 192.168.110.223
- Submask: 255.255.255.0
- Gateway: 192.168.110.1
- DNS Server: 192.168.110.1

Step 3: Add a VLAN member





Step 3: Assign the new VLAN member to ports.

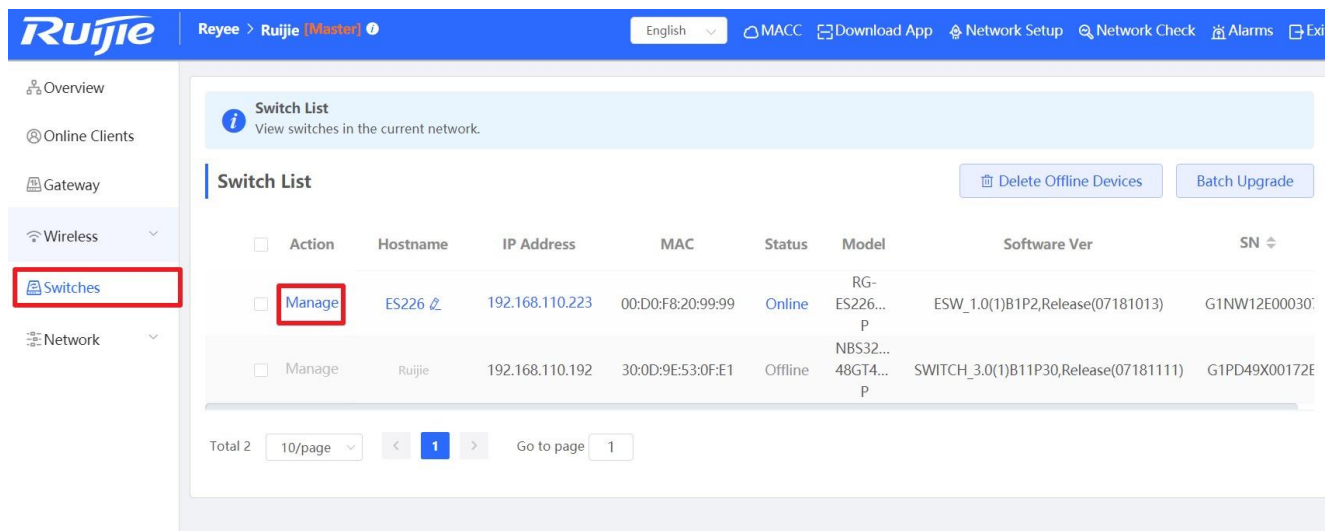


## 7.2 Port Isolation

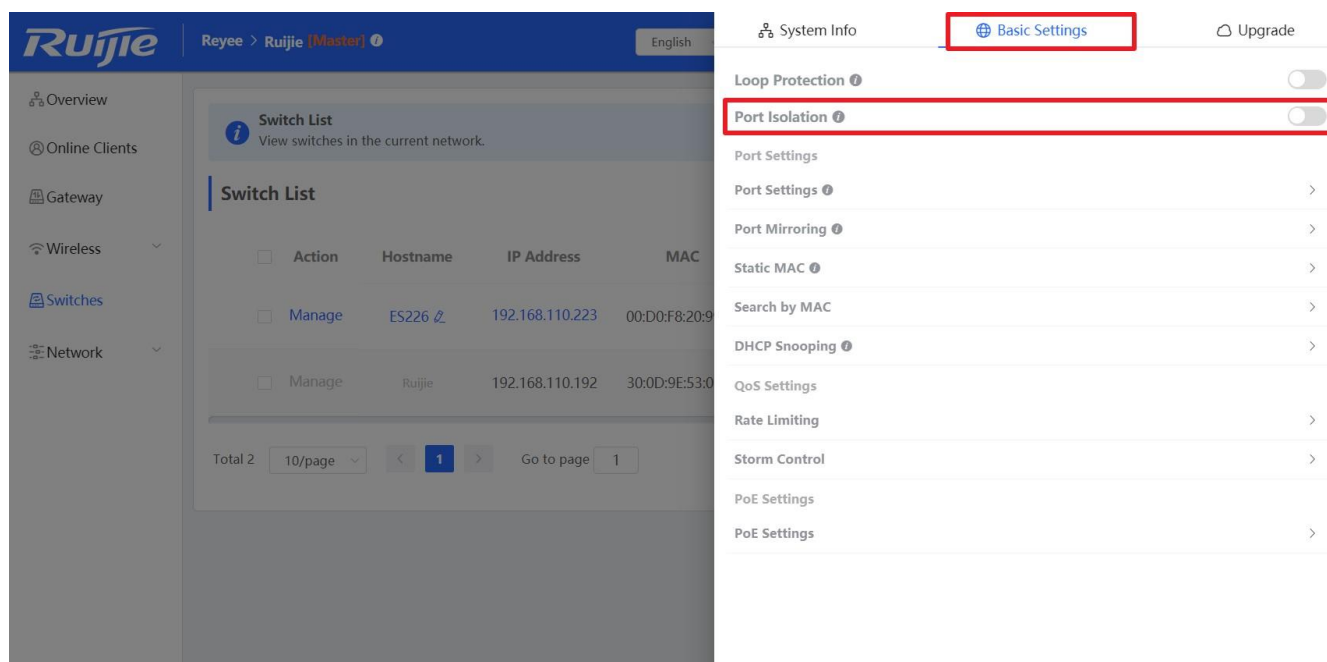
Port isolation implements layer-2 isolation of packets. After port isolation is enabled (which is disabled by default), data can be forwarded only between uplink ports and downlink ports, and **downlink ports cannot forward packets to each other**.

### Configuration Steps

Step 1: Choose **Switches** → **Manage** to configure the switch



Step 2: Choose **Basic Settings** → **Port Isolation** to enable the Port Isolation



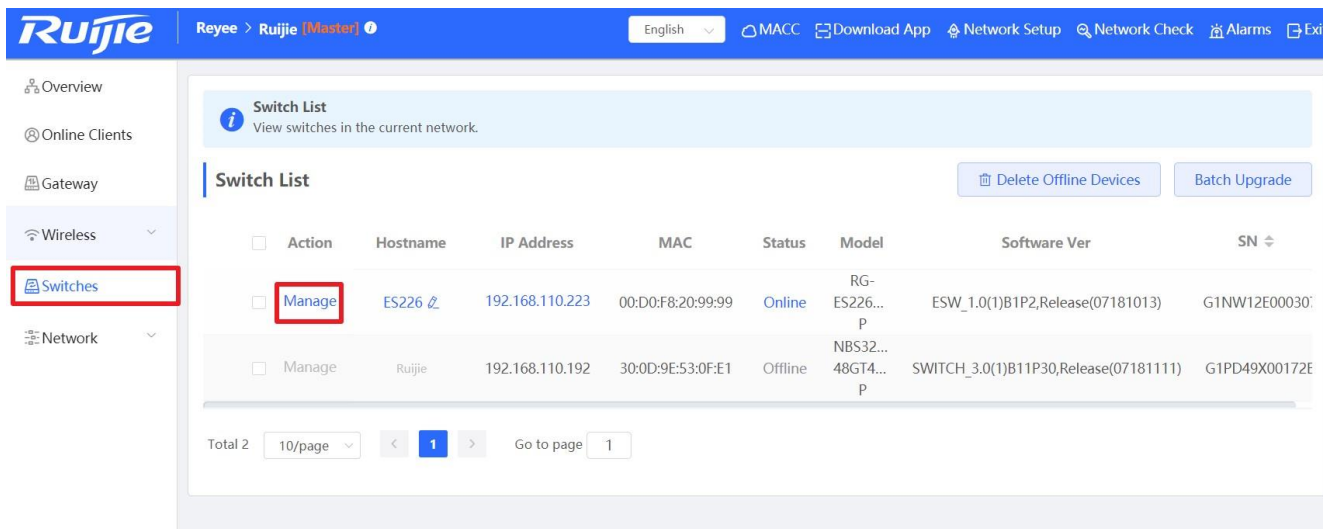
## 7.3 DHCP Snooping

In the DHCP-enabled network, the general problem facing administrator is that some users use private IP addresses rather than dynamically obtaining IP addresses. As a result, some users using dynamic IP addresses cannot access the network, making network application more complex. In dynamic DHCP binding mode, the device records how legal users obtain IP addresses during the course of DHCP Snooping for security purpose.

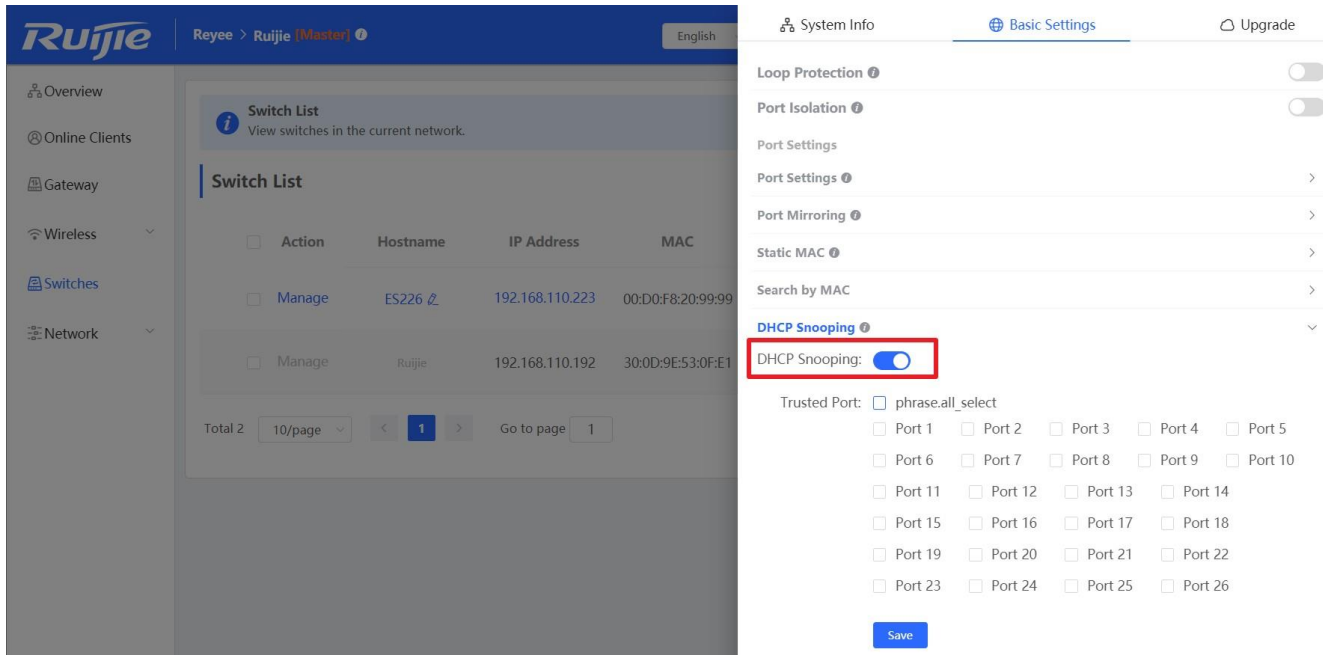
Enabling DHCP Snooping helps filter DHCP packets. Only forwards DHCP request packets to the trusted port and DHCP response packets from the trusted port. The port connected to the DHCP server is configured as the trusted port generally

### Configuration Steps

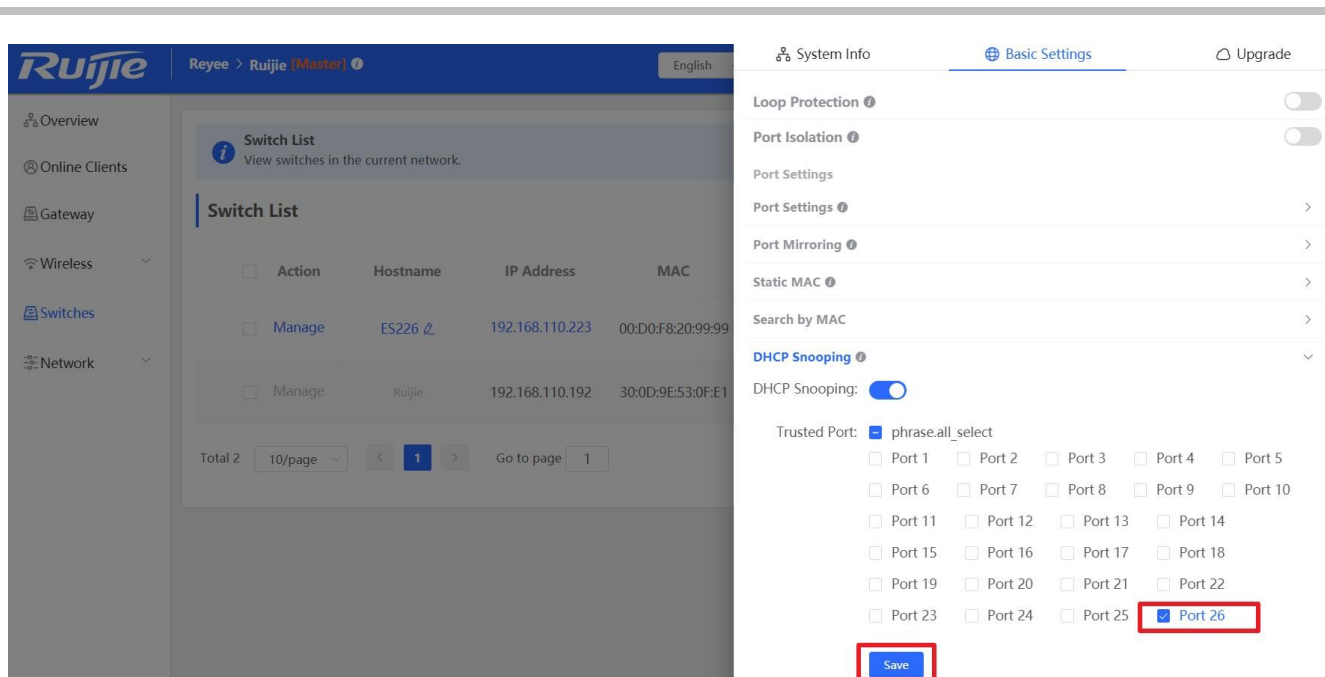
Step 1: Choose **Switches** → **Manage** to configure the switch



Step 2: Choose **Basic Settings** → **DHCP Snooping**, and enable the setting.



Step 3: Select the trusted port and save the configuration

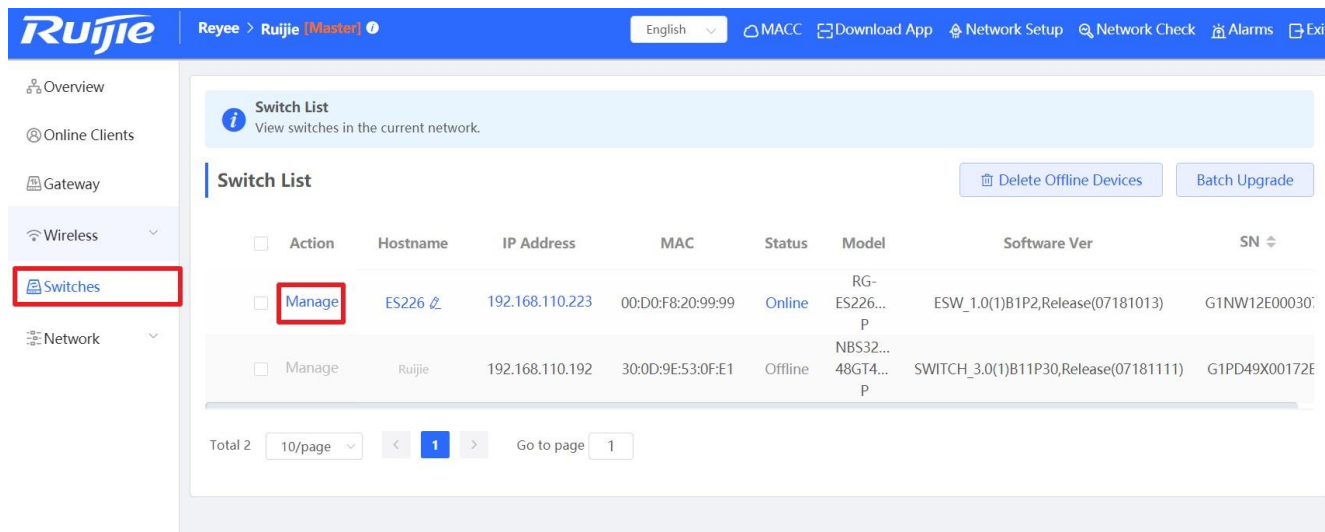


## 7.4 Speed Rate Limit

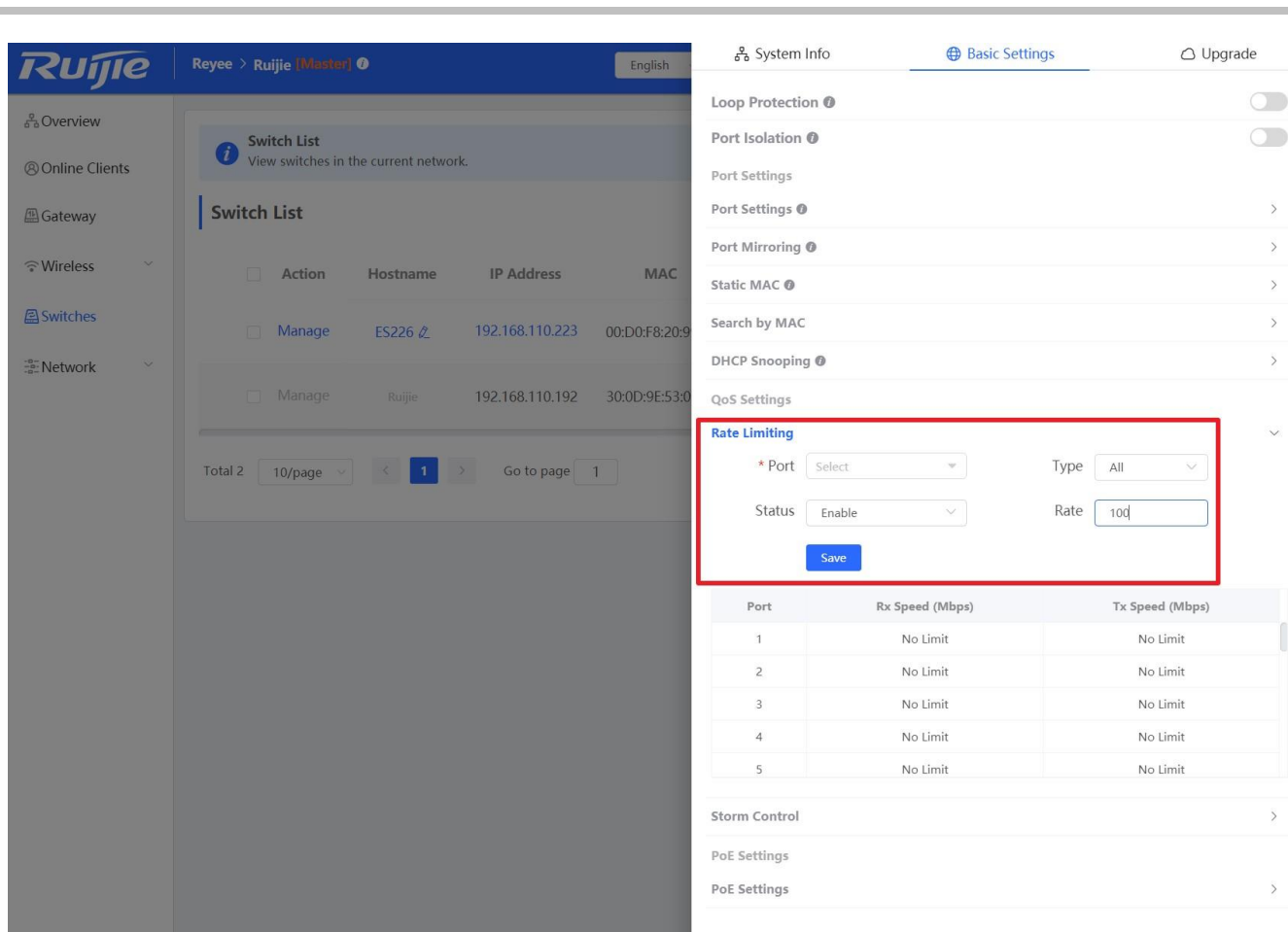
Rate limiting feature is used to limit the transmit speed rate on a specific port.

### Configuration Steps:

Step 1: Choose **Switches** → **Manage** to configure the switch



Step 2: Choose **Basic Settings** → **Rate Limiting**, and fill in the Port, Type, Status and Rate information.



## 7.5 Storm Control

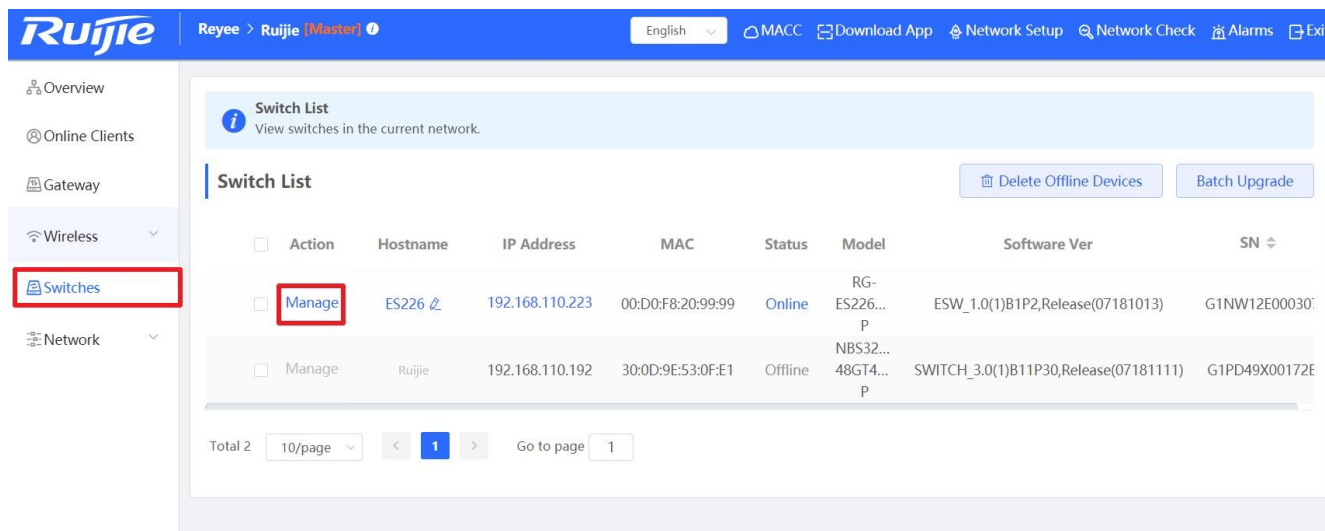
When there are excessive broadcast, multicast or unknown unicast data flows in the LANs, the network speed decreases and packet transmission timeout greatly increases. This is called LAN storm, which may be caused by topology protocol execution errors or incorrect network configuration.

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

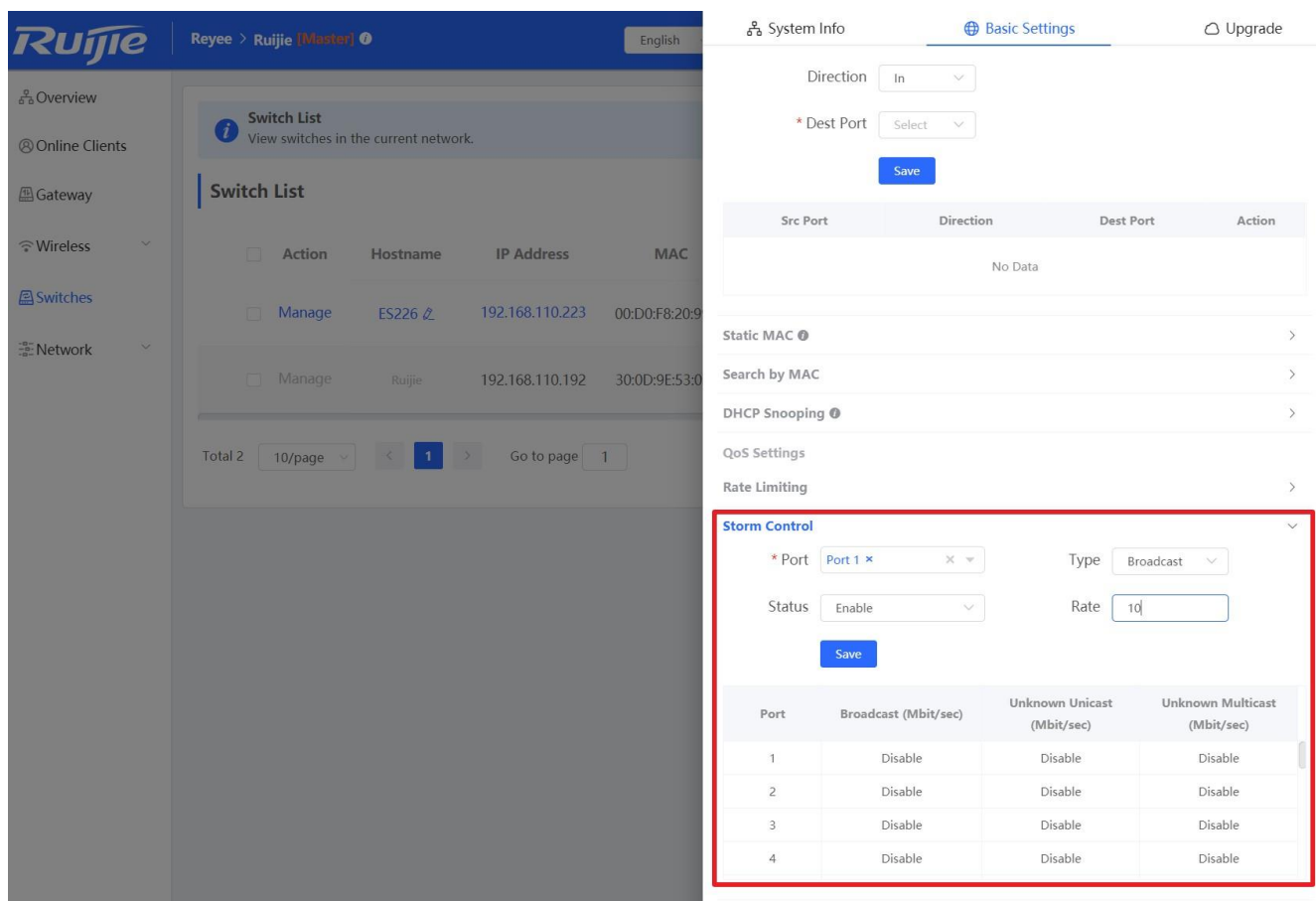
### Configuration Steps:

Step 1: Choose **Switches** → **Manage** to configure the switch

# Reyee Series Implementation Cookbook



Step 2: Choose **Basic Settings** → **Rate Limiting**, and fill in the Port, Type, Status and Rate information.



## 8 Reyee AP Configuration

### 8.1 Wi-Fi Setting

The Wi-Fi Settings module allows you to configure the Wi-Fi parameters.

The screenshot displays the Ruijie AP configuration interface. The top navigation bar shows 'Ruijie > Ruijie (Master)' and various utility links like 'English', 'MACC', 'Download App', 'Network Setup', 'Network Check', 'Alarms', and 'Exit'. The left sidebar lists navigation options: Overview, Online Clients, Gateway, Wireless, APs, Clients, WiFi, Advanced, LAN Ports, LED, Switches, and Network. The main content area is titled 'WiFi Settings' and includes a 'Device Group' dropdown set to 'Default'. A tip message states: 'Tip: Changing configuration requires a reboot and will force online clients to go offline.' The configuration fields are: SSID (Reyee123), Frequency (2.4G + 5G), Encryption (Open), Active Time (All Time), and VLAN (Default VLAN). Below these are several toggle switches: Hide SSID (off), Client Isolation (off), 5G Prior (off), Xpress (off), and Layer-3 Roaming (off). A 'Save' button is located at the bottom of the configuration area.

**Device Group:** Choose the AP group, the following setting will only be applied to the chosen group.

**SSID:** The Wi-Fi name which the APs broadcasted.

**Frequency:** Choose the radio which the following setting will be applied to. Both 2.4GHz and 5GHz radio will be applied by default.

**Encryption:** Choose the encryption mode.

**Active Time:** Choose the time period that the Wi-Fi signal will be broadcasted.

**VLAN:** The VLAN number that the WiFi will be associated with.

**Hide SSID:** The SSID is hidden and must be manually entered.

**Client Isolation:** The client joining this Wi-Fi network will be isolated, which means the clients cannot be accessed by each other.

**5G Prior:** The 5G-supported client will access 5G radio preferentially.

**Xpress:** The QoS setting will be automatically applied to optimize the game experience.

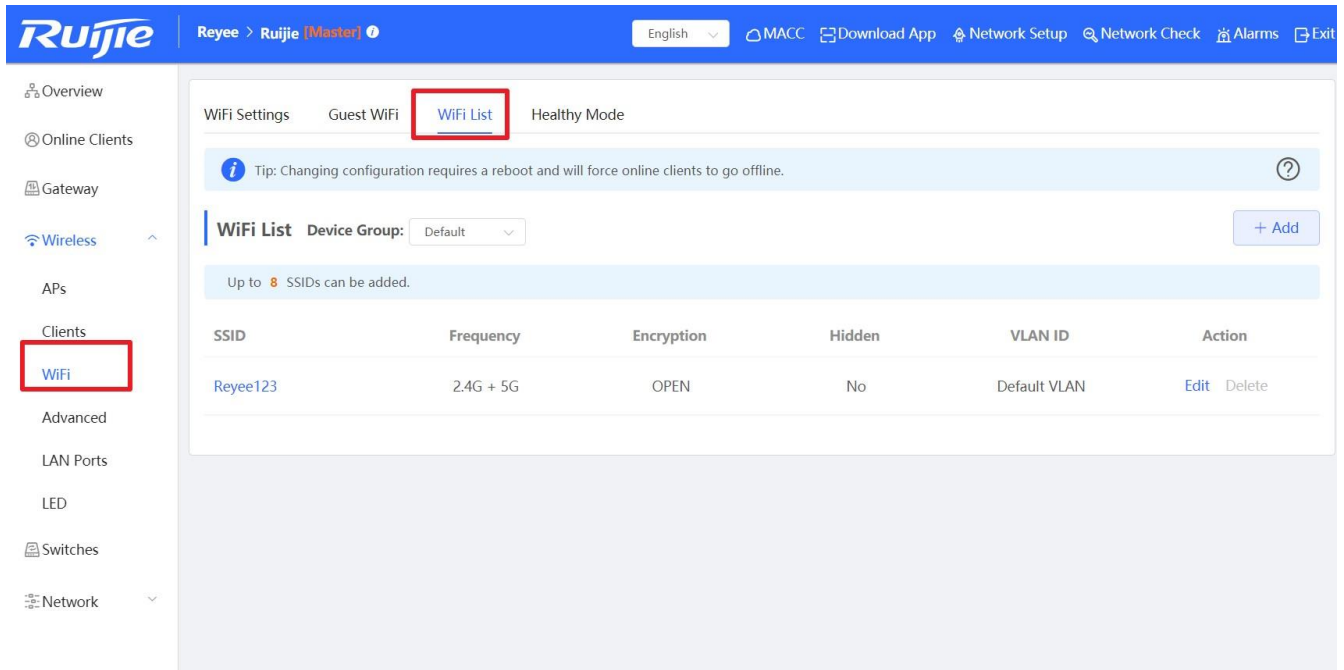


## 8.2 Multiple SSID setting

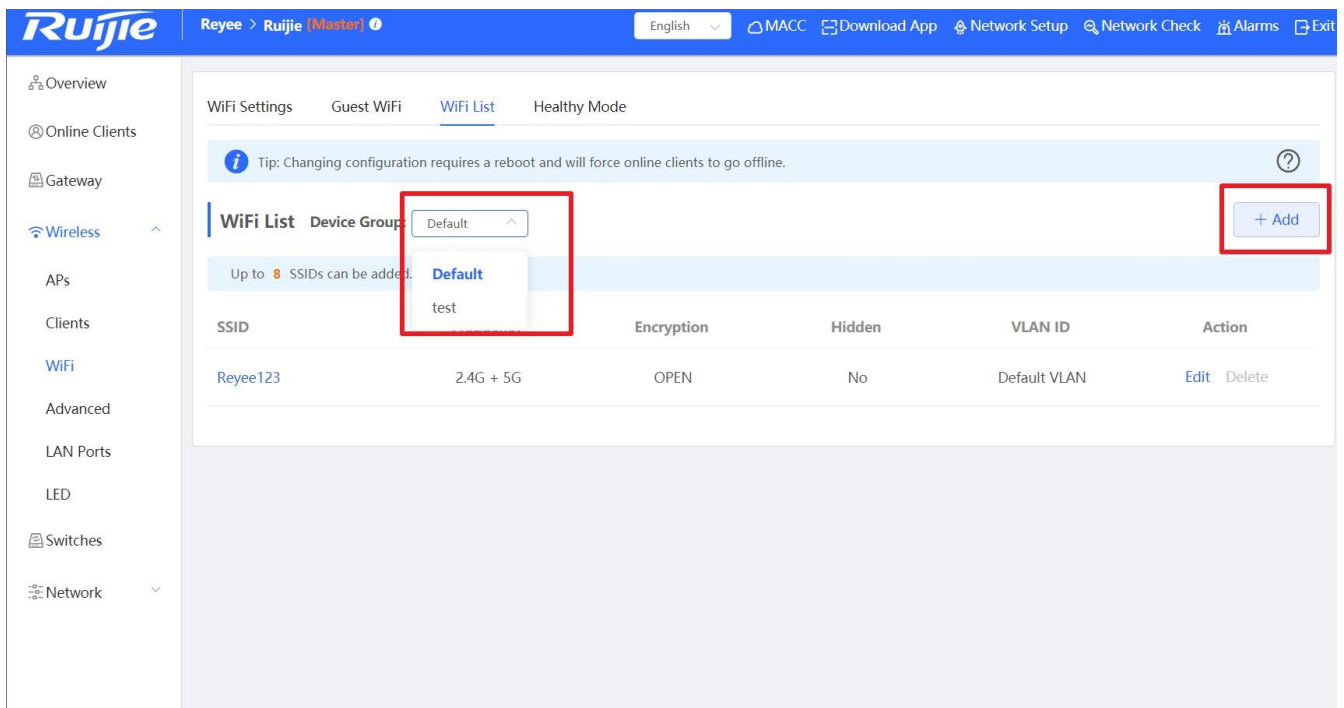
In some scenario, multiple SSIDs are needed in the network.

### Configuration Steps:

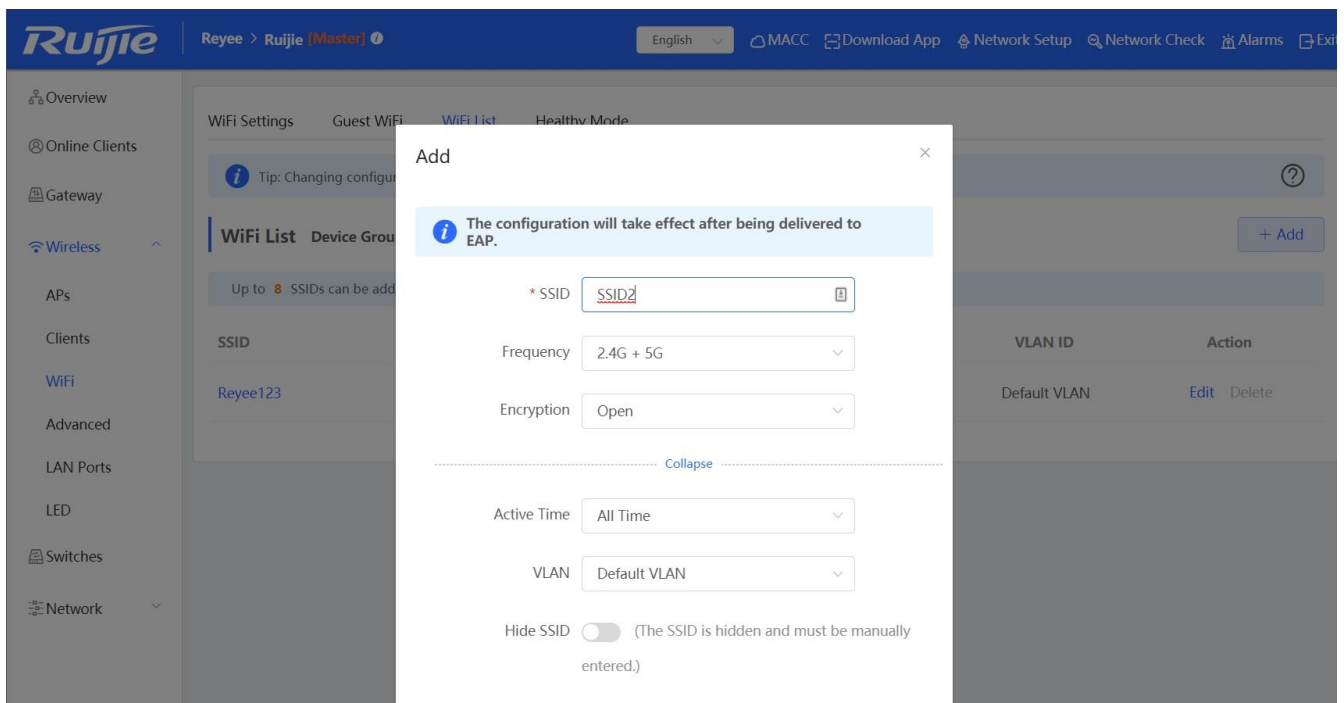
Step1: Choose **Wireless** → **WiFi** → **WiFi List**



Step 2: Choose a **Device Group** and click the “**Add**” button



Step 3: Fill in the SSID name WiFi related settings

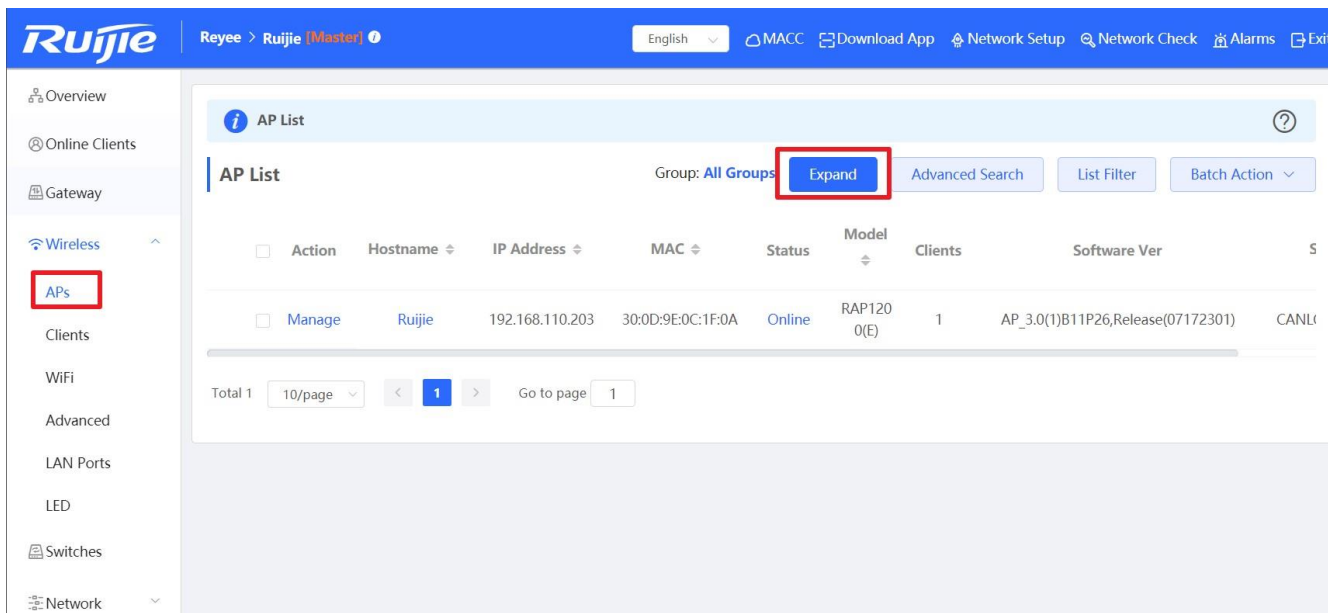


## 8.3 AP Group

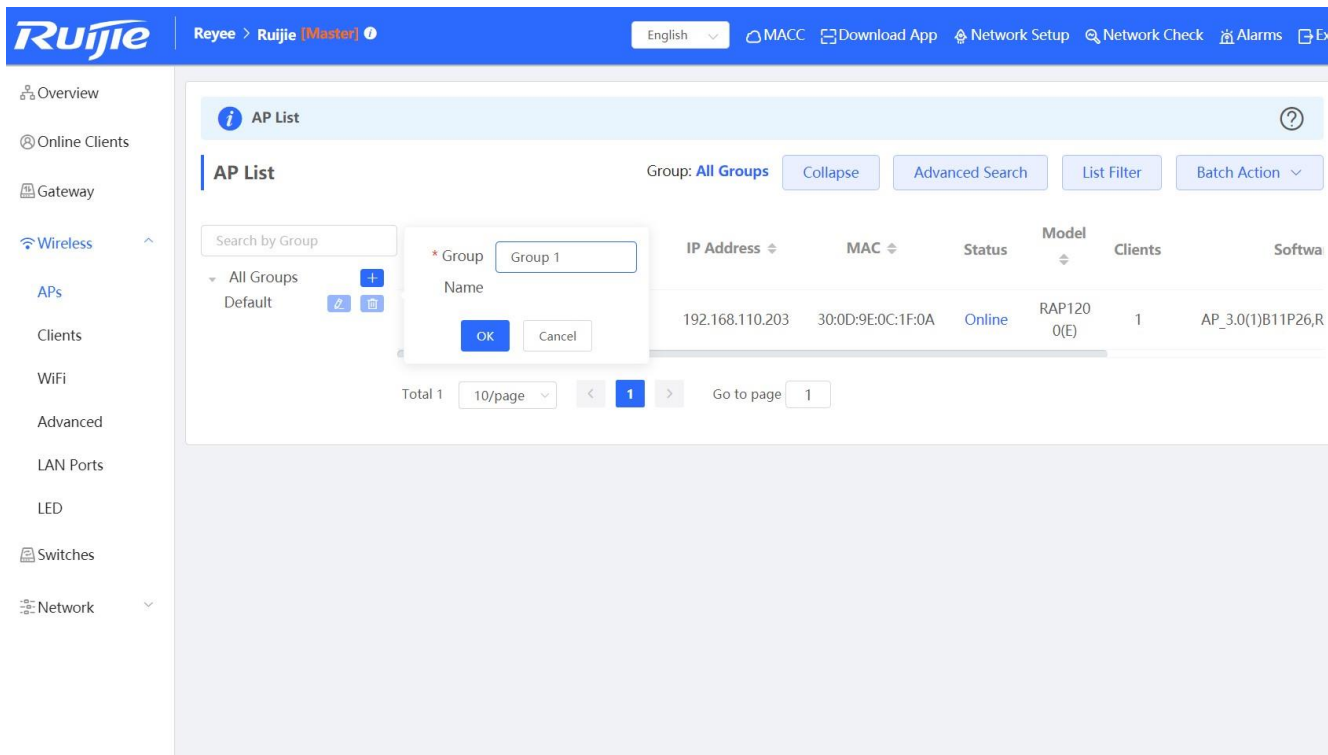
Reyee APs can be divided into different AP groups with different WiFi settings

### Configuration Steps

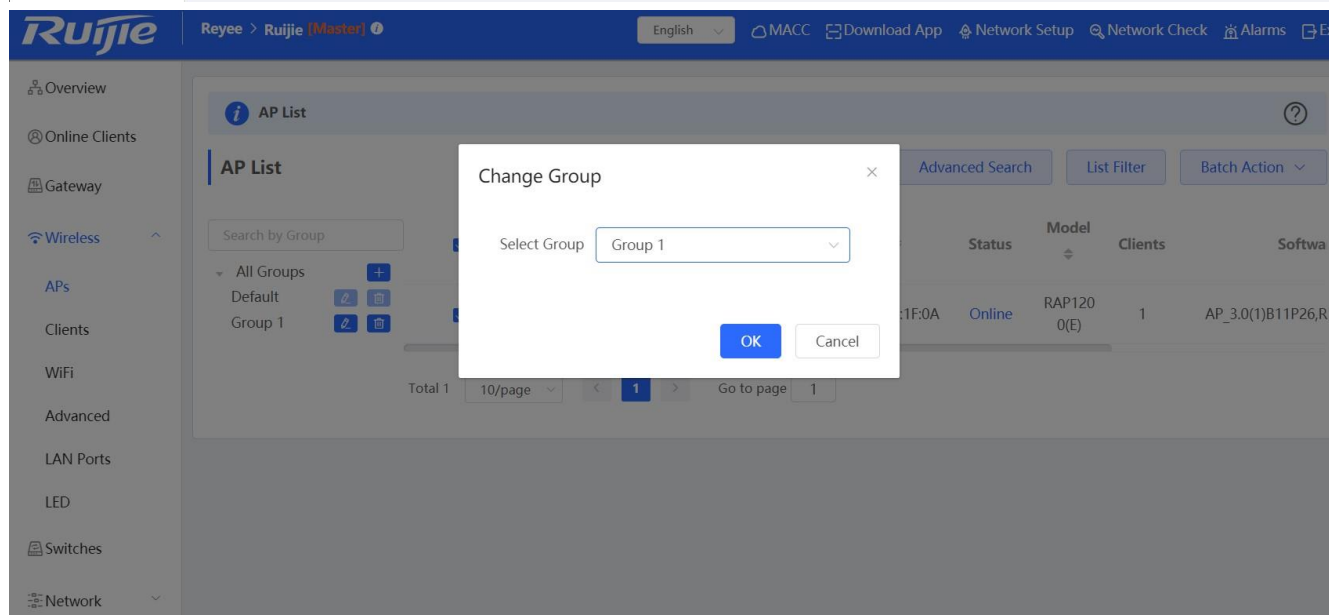
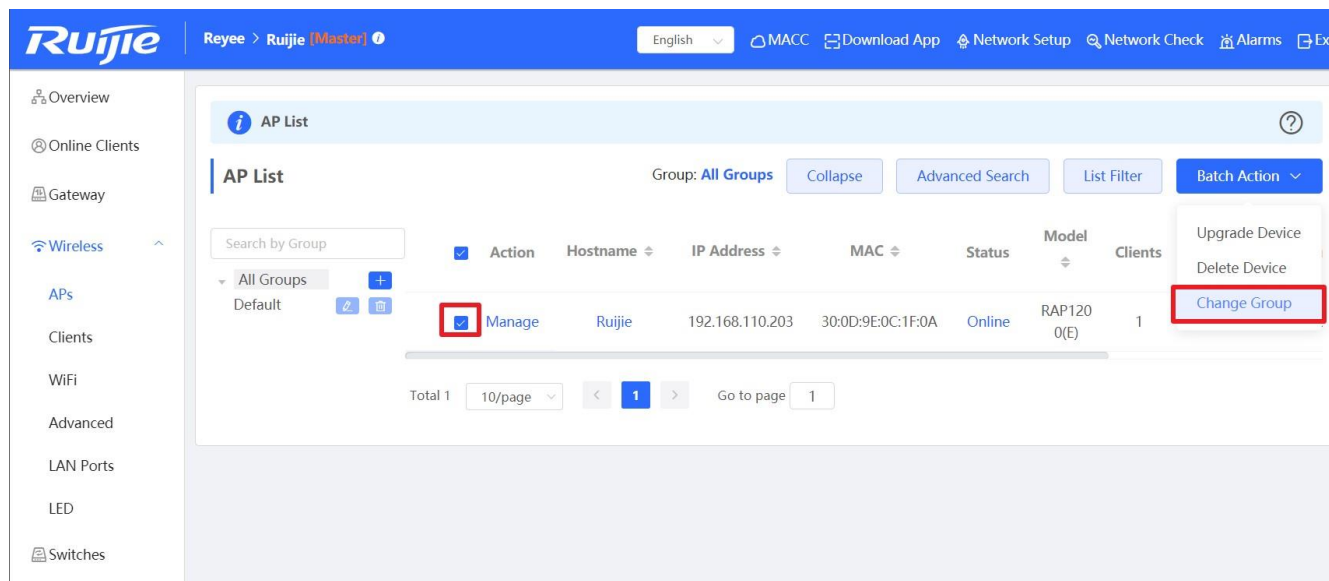
Step 1: Choose **Wireless** → **AP** and click the **“Expand”** button



Step 2: Click the **“+”** button to add an AP group



Step 3: Move the AP to the new group



## 8.4 Blacklist/Whitelist

The Blacklist/Whitelist module allows you to configure client blacklist and whitelist.

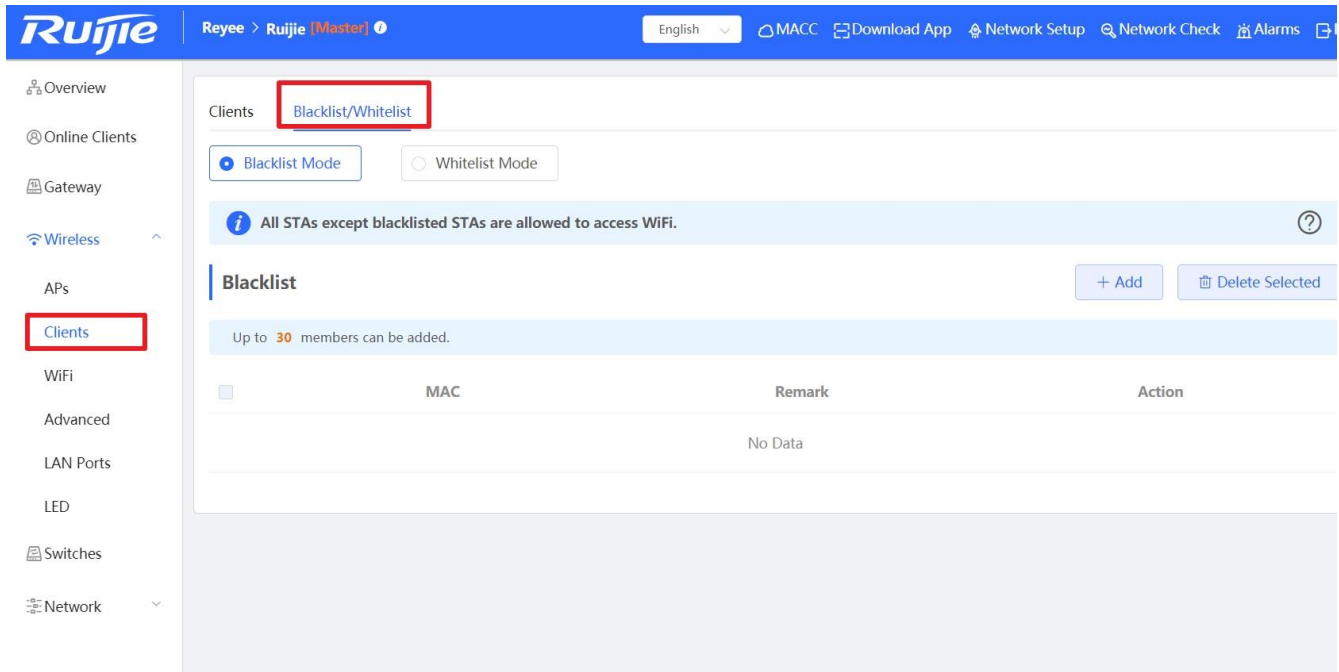
**Blacklist:** the devices are added into blacklist will not be able to access the network

**Whitelist:** only the devices in the whitelist are allowed to access the network

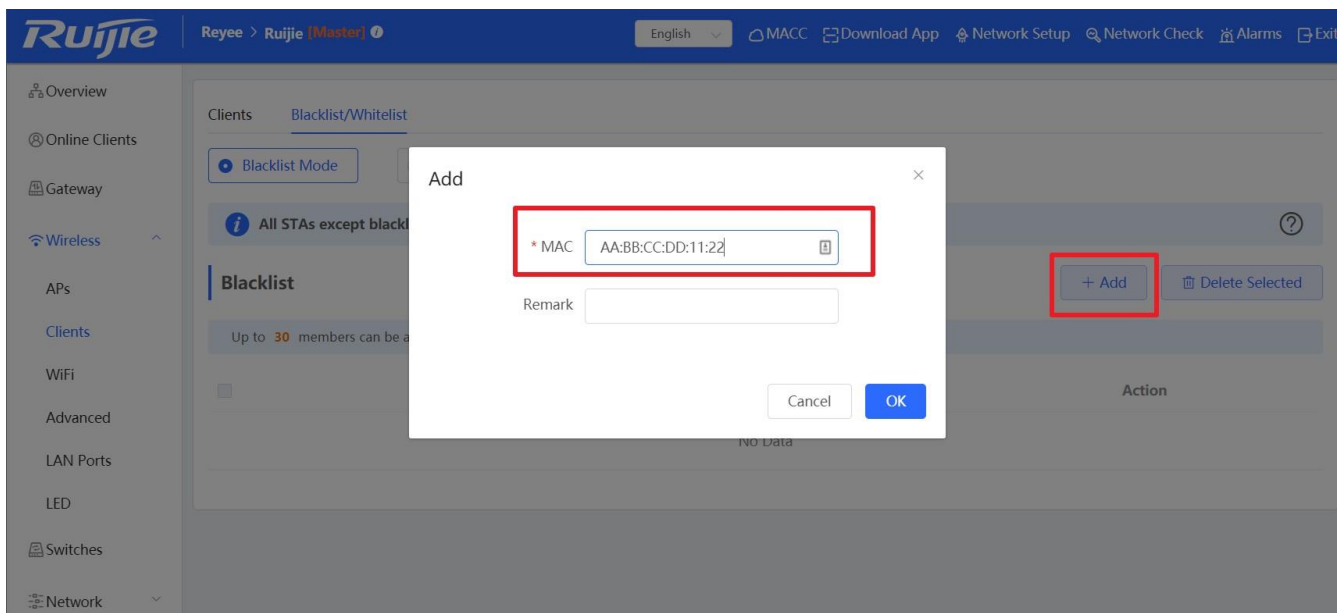
The blacklist and whitelist take effect based on the whole network based or SSID based blacklist/whitelist are not supported.

### Configuration Steps

Step 1: Choose **Wireless** → **Clients** → **Blacklist/Whitelist**



Step 2: Click the “Add” button to add the client’s MAC address

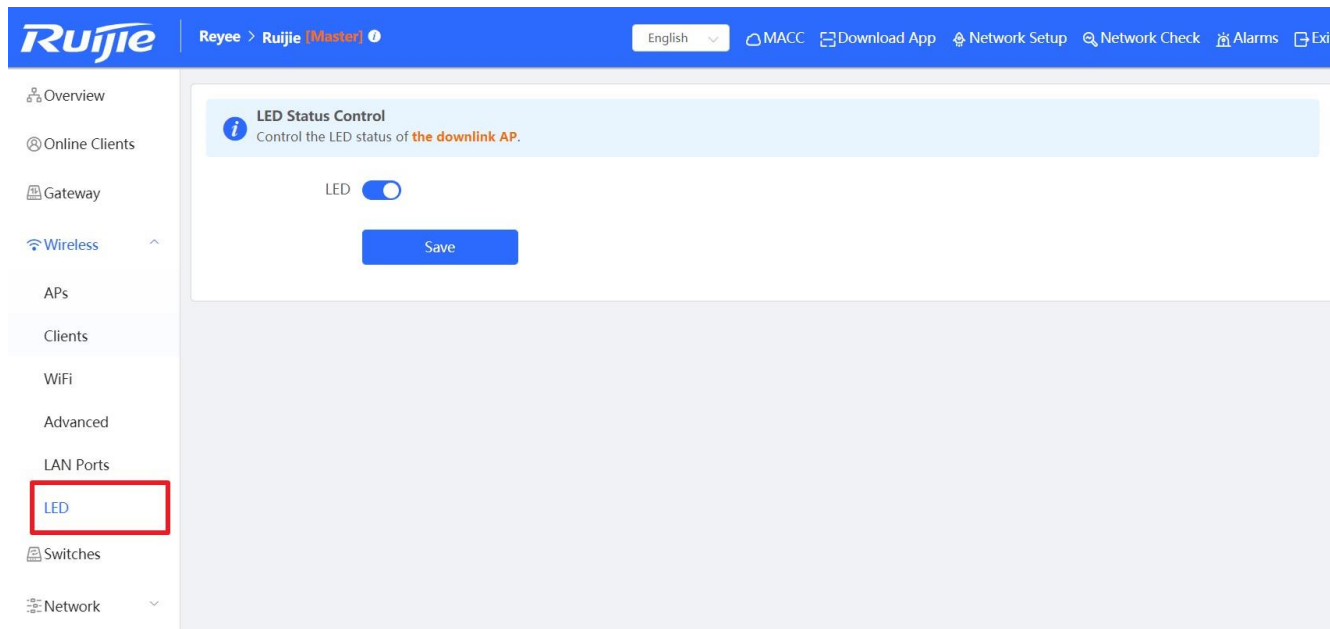


## 8.5 Turn on/off LED indicator

The LED indicators on APs could be turned on/off according to the actual requirement.

### Configuration Steps:

Choose **Wireless** → **LED**, and turn on/off the **LED** setting.



## 9 FAQ

**1. Does Reyee Device support Telnet or SSH login?**

No. Reyee device only support web management.

**2. What is the default IP address of the Reyee switch?**

10.44.77.200.

**3. What is the IP address of the master device on the self-organizing network?**

10.44.77.253

**4. What is the device priority of the self-organizing network master selection? EG > AP > Switch**

**5. What is the difference between the default SSID @Ruijie-s and @Ruijie-m?**

@Ruijie-m is generated after successful network self-organization, while @Ruijie-s is generated on a standalone device.

**6. Does the self-organizing network support to be formed between Reyee series devices and other Ruijie devices (Running RGOS)?**

No. Self-organizing network can only be formed between Reyee Series devices.

**7. I failed to log into the eWeb management system. What can I do?**

Perform the following steps:

- (1) Check that the network cable is properly connected to the LAN port of the device and the corresponding LED indicator blinks or is steady on.
- (2) Before accessing the configuration GUI, set the IP assignment mode to Obtain an IP address automatically (recommended), so that the server with DHCP enabled can automatically assign an IP address to the PC. To designate a static IP address to the PC, set the IP address of the PC in the same network segment as the IP address of the management interface. For example, if the default IP address of the management interface is 192.168.110.1 and the

subnet mask is 255.255.255.0, set the IP address of the PC to 192.168.110.X (X is any integer ranging from 2 to 254), and the subnet mask is 255.255.255.0.

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

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

**8. What can I do if I forget my username and password? How to restore the factory settings?**

To restore the factory settings, power on the device, and press and hold the Reset button for 5s or more, and release the Reset button after the system LED indicator blinks. The device automatically restores the factory settings and restarts. The original configuration will be lost after the factory settings are restored. After the restoration, the default management address is <http://10.44.77.254>. You can set the username and password upon first login.

---

