

## Reyee Series Implementation Cookbook (V1.5)

**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	V1.0 Initial publication	Nick Chen
2020.11	V1.1 Fix a typo.	Nick Chen
2020.11	V1.2 Add EST310	Henry Huang
2021.3	V1.3 Add EW1200 series and EG authentication, app control	Henry Huang
2021.6	V1.4 Add PPPoE Server	Henry Huang
2021.7	V1.5 Add WIO, Load Balancing, IPTV, OUI-based and SSID-based Whitelist/Blacklist	Henry Huang

---

## Contents

1 Preface .....	3
2 Product Introduction.....	5
2.1 Cloud-managed Access Points .....	5
2.2 Reyee Switch .....	6
2.3 Easy Gate Series Router.....	7
2.4 EST310 Bridge .....	7
3 Daily Maintenance .....	7
3.1 Device Login .....	7
3.2 Change Password .....	9
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 VPN.....	19
5.3 Smart Flow Control.....	27
5.4 Port Mapping.....	28
5.5 Authentication.....	32
5.6 Behavior .....	36
5.7 PPPoE Server .....	37
5.8 WIO .....	44
5.8 Load Balancing.....	48
5.9 IPTV .....	51
6 Reyee NBS Series Switch Configuration .....	53
6.1 VLAN Setting.....	53
6.2 Access Control List (ACL) .....	55
6.3 Port Isolation .....	59
6.4 DHCP Snooping.....	61

---



6.5 Link Aggregation .....	63
6.6 Storm Control .....	65
7 Reyee ES Series Switch Configuration.....	68
7.1 VLAN Setting.....	68
7.2 Port Isolation .....	71
7.3 DHCP Snooping.....	72
7.4 Speed Rate Limit.....	74
7.5 Storm Control .....	76
8 Reyee AP Configuration .....	78
8.1 Wi-Fi Setting.....	78
8.2 Multiple SSID setting.....	79
8.3 AP Group .....	80
8.4 Blacklist/Whitelist.....	82
8.5 Turn on/off LED indicator .....	86
9 EST Series Configuration .....	87
9.1 Basic Setting .....	87
9.2 Devices status monitor .....	91
9.3 LAN setting.....	95
9.4 Wireless Setting .....	96
9.5 System Setting .....	101
9.6 PTMP setting.....	107
10 EW Series Configuration.....	112
10.1 Basic Setting .....	112
10.2 Blacklist/Whitelist.....	121
10.3 DDNS.....	122
10.4 MESH.....	124
11 FAQ .....	127

## 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 Easy Gate 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.

## 2.4 EST310 Bridge

5GHz wireless bridge, including 2 devices for the recorder-end and camera-end, paired by default without requiring any configuration, 1 100M LAN port, up to 867Mbps throughput, built-in directional antenna, support one-to-many bridging, EWeb/ Ruijie Cloud app management, 12VDC and 24VDC non-standard PoE, wall-mounted/ pole-mounted installation

# 3 Daily Maintenance

## 3.1 Device Login

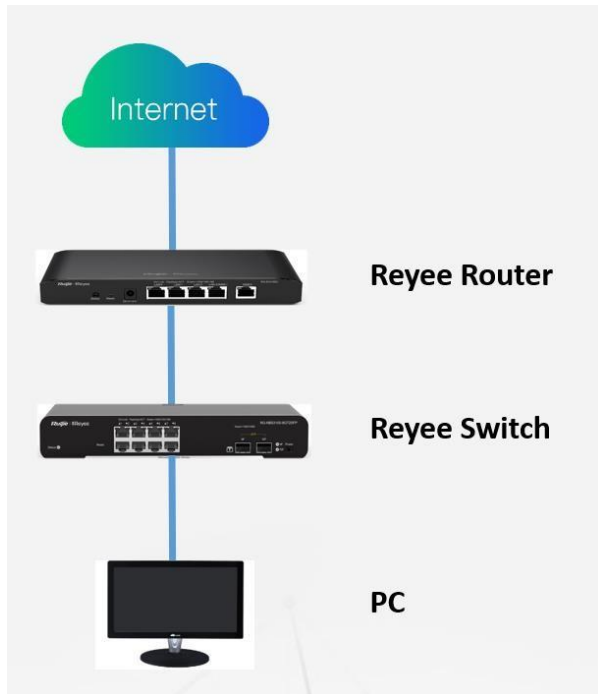
eWeb is a Web-based network management system that manages or configures devices. You can access eWeb via browsers such as Google Chrome.

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.

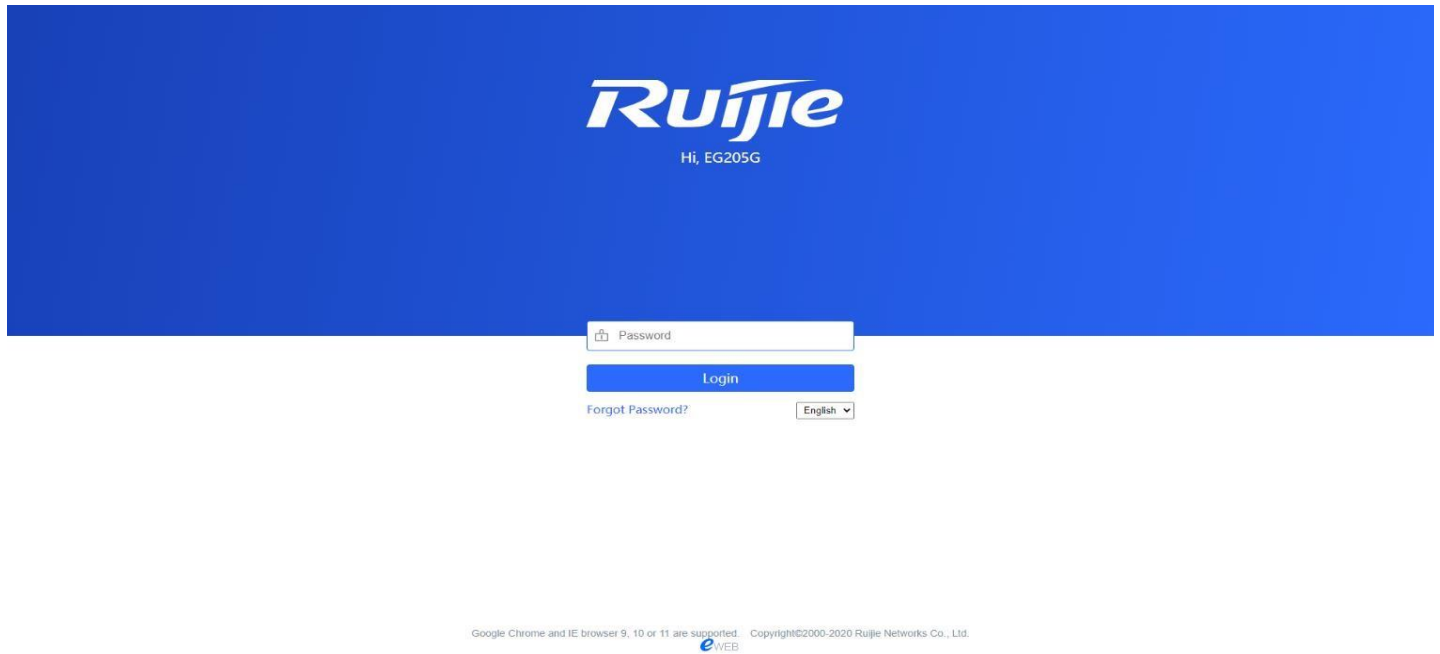
---



- 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.

For the EST, you may use 10.44.77.254 to access the device.

The default login password for all Reyee devices is **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.

---

- Overview
- Online Clients
- Gateway
- Wireless
- Switches
- Network
- Time
- Password
- Scheduled Reboot
- Reboot & Reset

### Device Password

Change the device password. Please log in again with the new password later.

\* Old Password

\* New Password

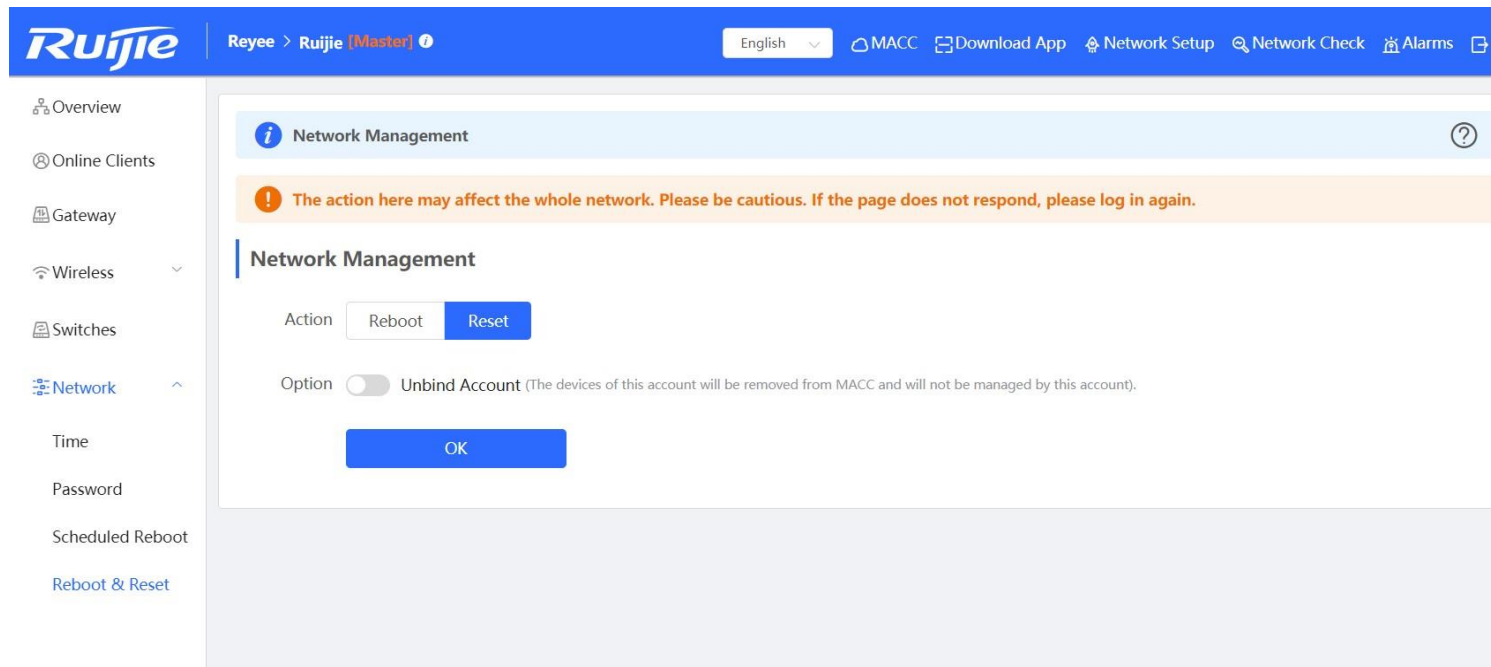
\* Confirm Password

Save

### 3.3 Factory Reset

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

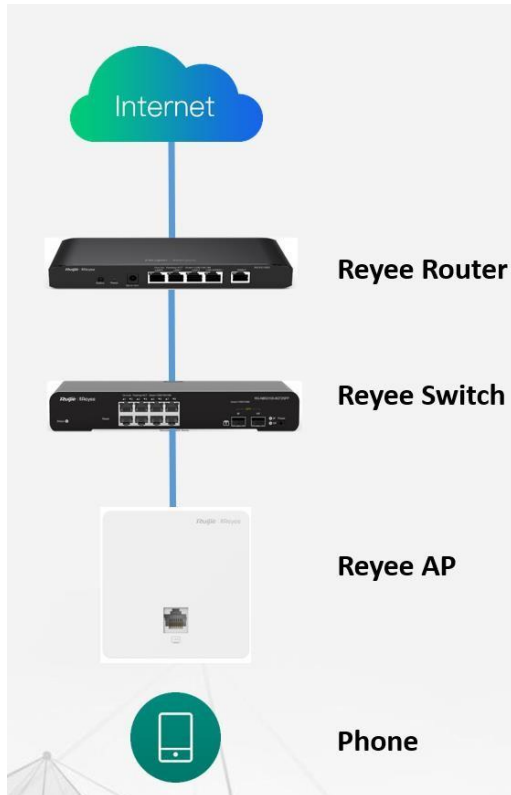
Option 2: Login to the eWeb of the device reset all device in the network.



## 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**

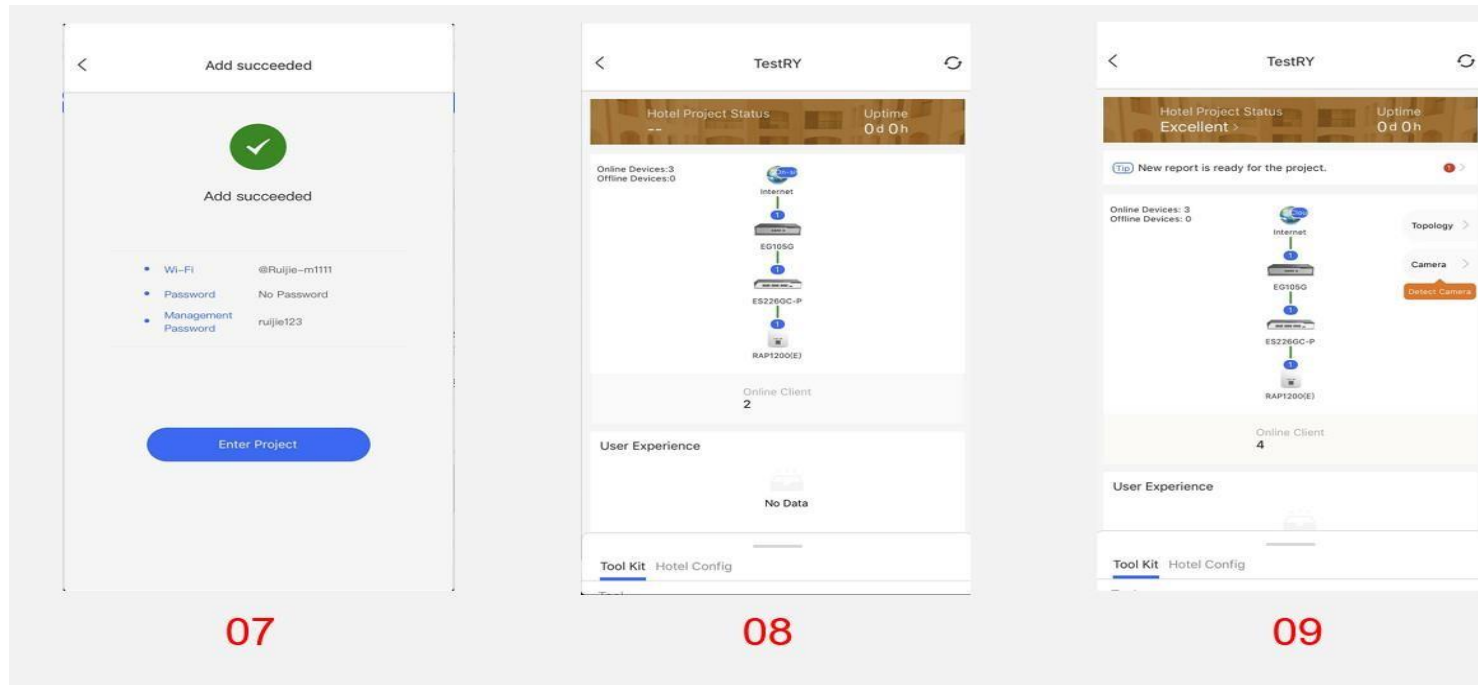
**02**

**03**

**04**

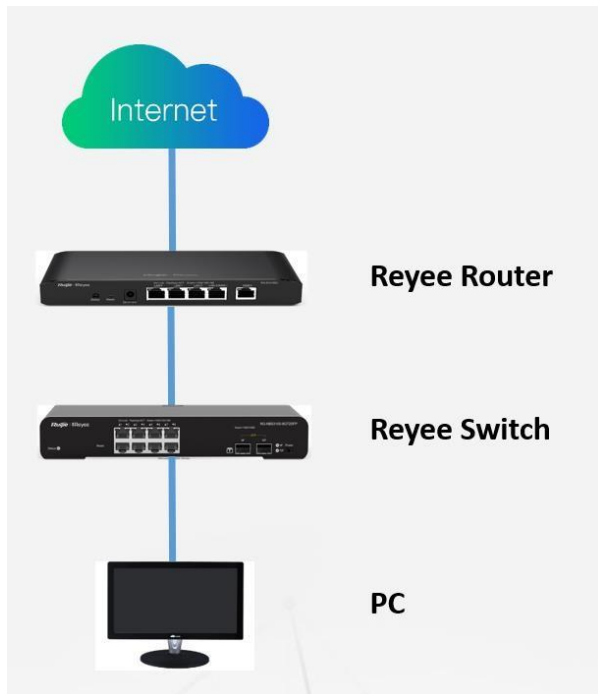
**05**

**06**



## 4.2 Quick provisioning via Reyee EWeb

### Network Topology



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

**Total Devices: 2.**  
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)

Internet — Gateway (1) — Switches (1 / 1) — APs (0 / 0)

**My Network**

New Device (2 devices)

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)B11P30,Release(07181202)
Switch RG-ES226GC-P	G1NW12E000307	192.168.110.223	00:D0:F8:20:99:99	ESW_1.0(1)B1P2,Release(07181013)

Rediscover Start Setup

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

**Create Network**

\* Network Name: Reyee

\* Password: [Masked]

IP Assignment:  PPPoE  DHCP  Static IP Address

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

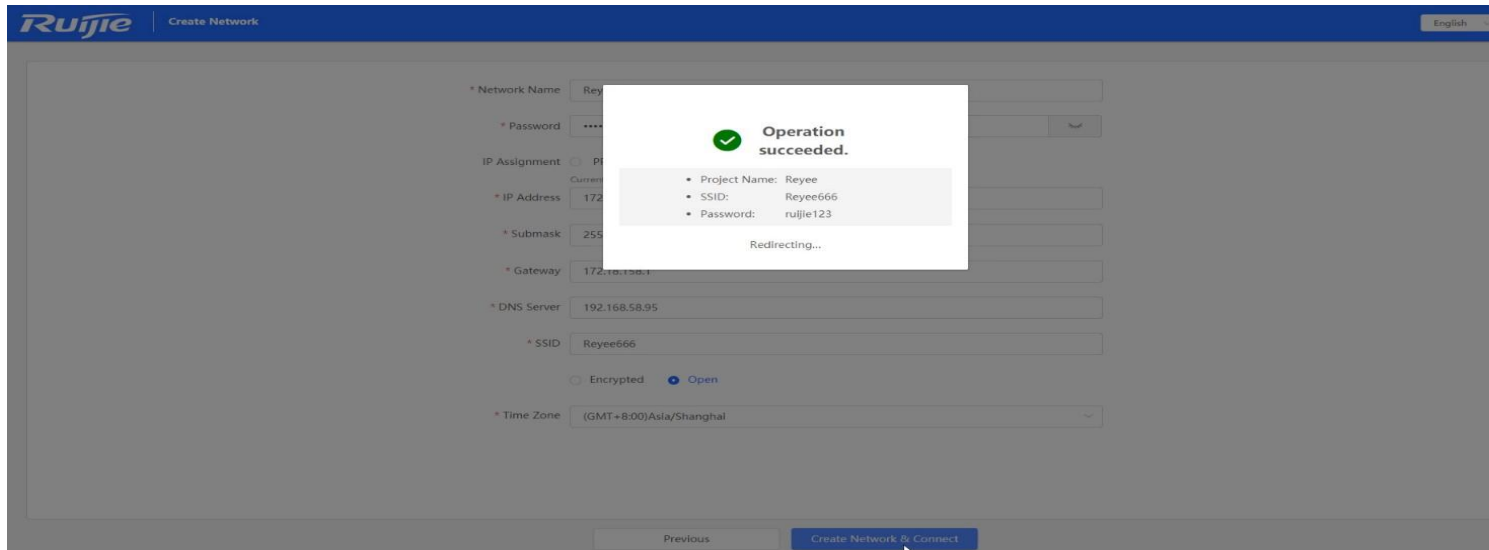
\* SSID: Reyee666

Encrypted  Open

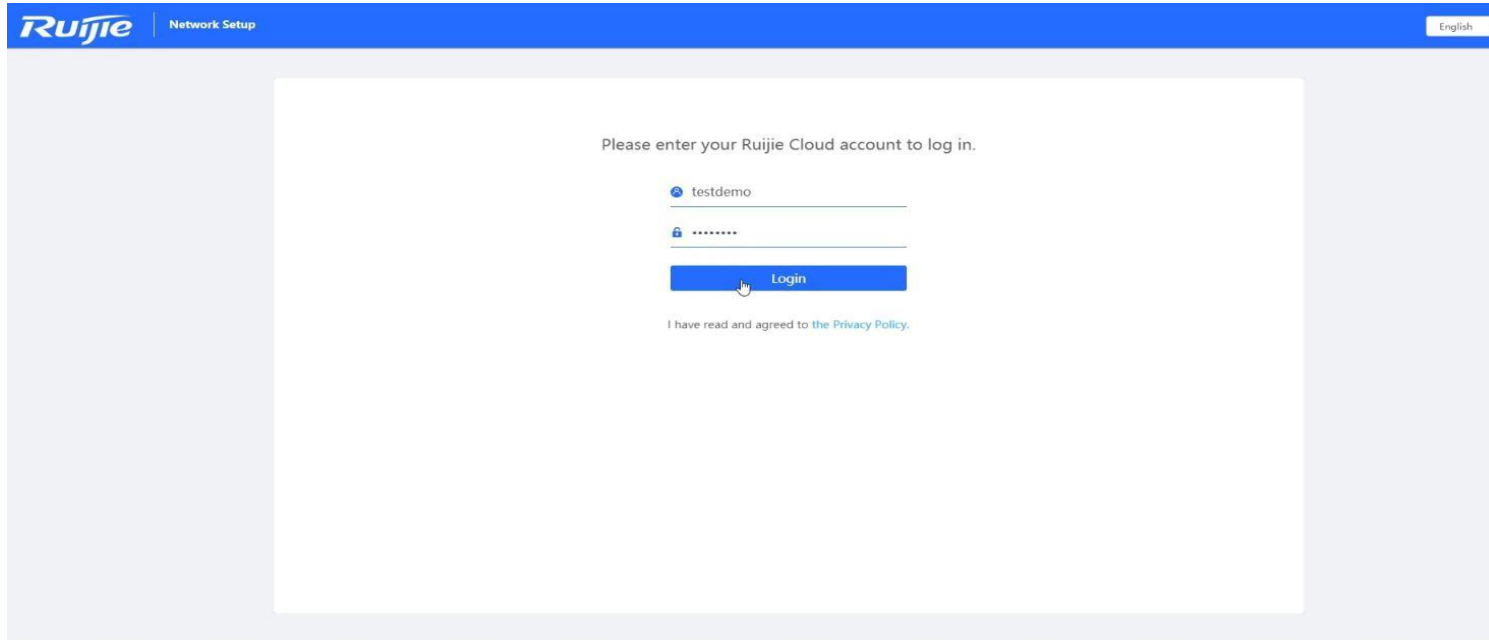
\* Time Zone: (GMT+8:00)Asia/Shanghai

Previous Create Network & Connect

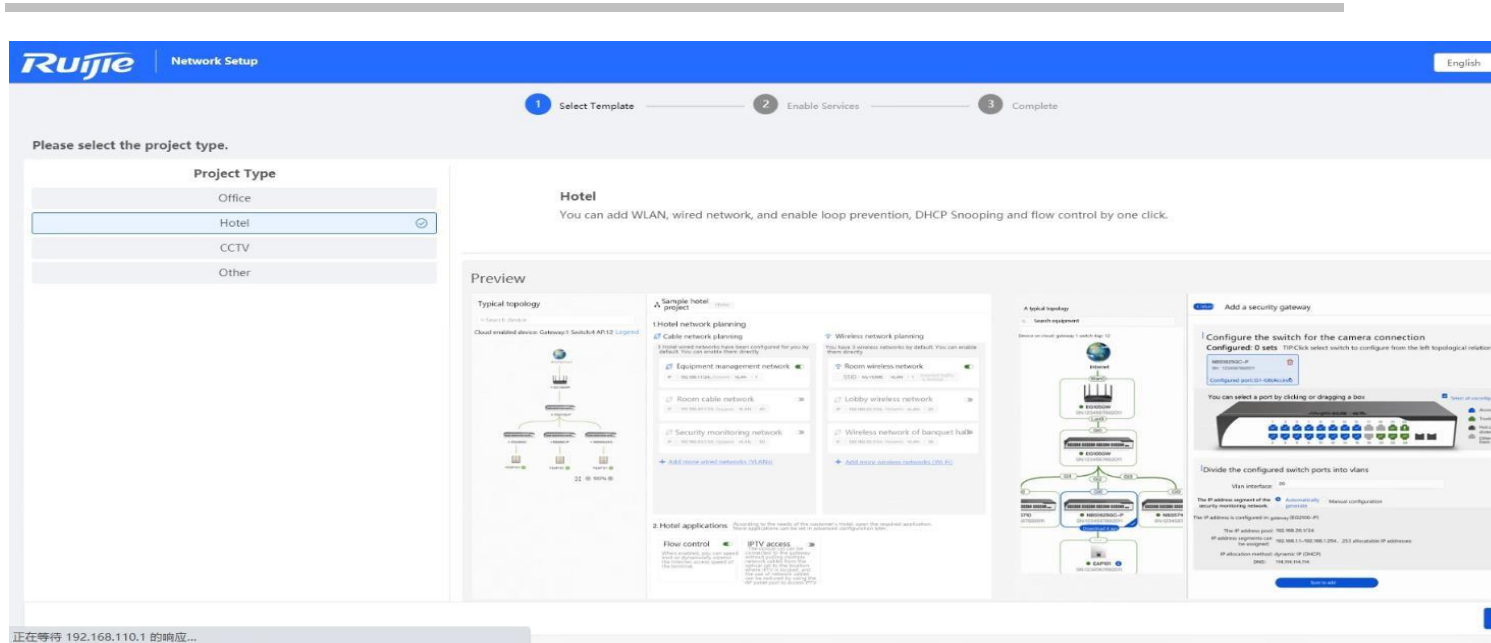
## Reyee Series Implementation Cookbook



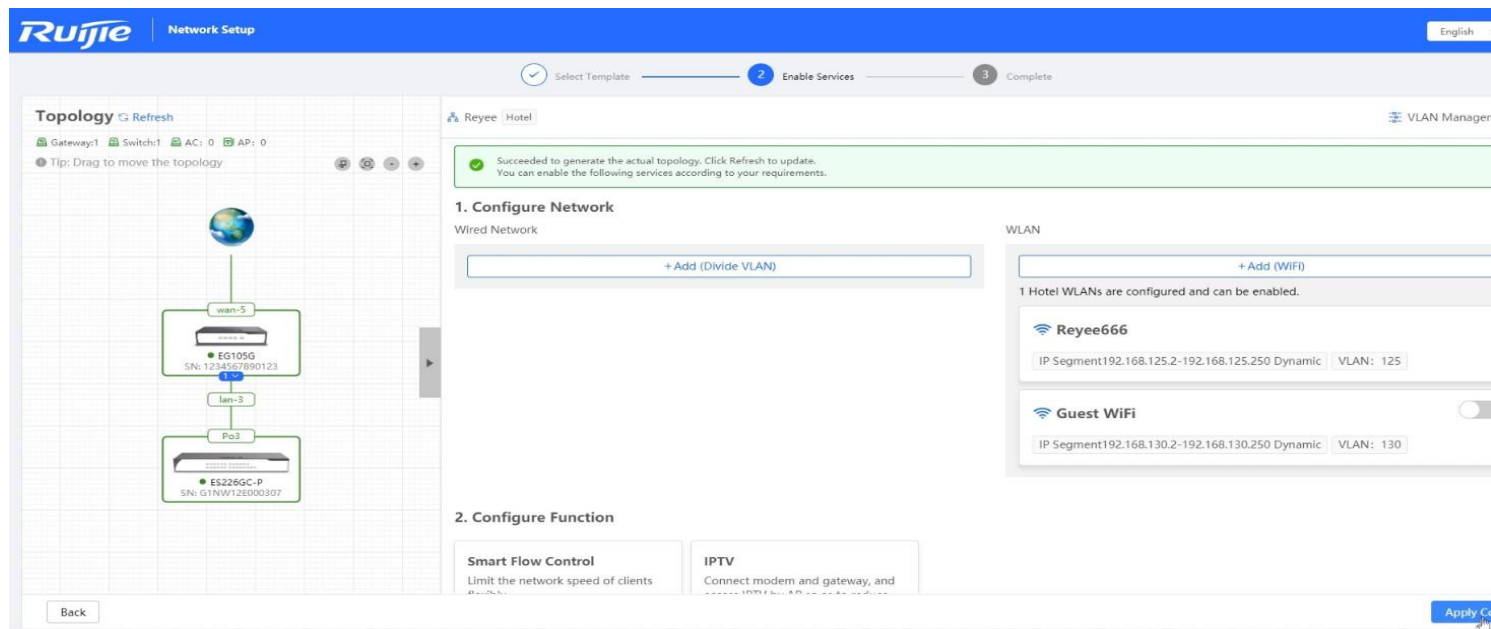
Step 3: Login to your Ruijie Cloud Account.



Step 4: Select the project type.



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



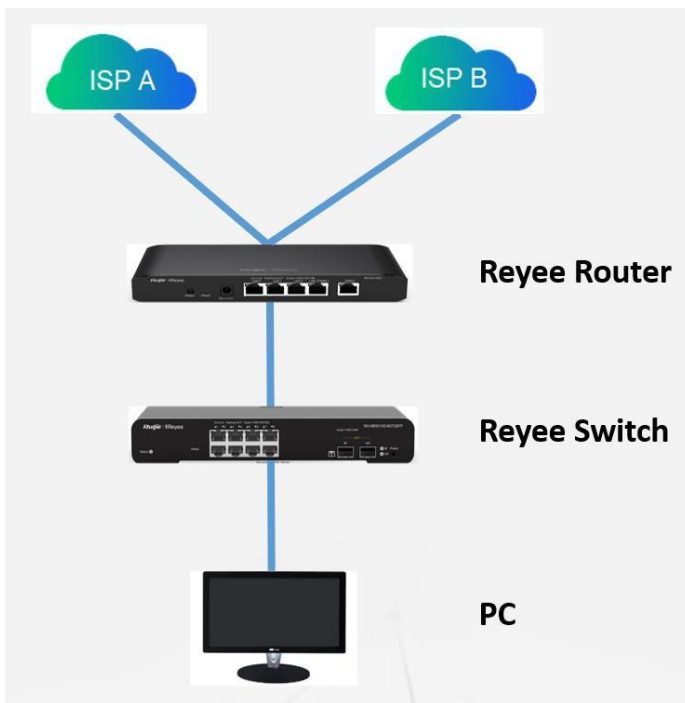
The screenshot displays the Ruijie Network Setup web interface. At the top, the Ruijie logo and 'Network Setup' are visible. A progress bar shows three steps: 'Select Template' (checked), 'Enable Services' (checked), and 'Complete' (checked). The main area is divided into a 'Topology' section on the left and a 'Network Config' section on the right. The 'Topology' section shows a network diagram with a WAN interface connected to a switch (EG105G) and a Po3 interface connected to another switch (ES226GC-P). The 'Network Config' section shows the configuration for 'Reyee666', including IP Segment (192.168.125.2-192.168.125.250 Dynamic) and VLAN (125). A large white text overlay reads 'Initial Setup Completed!'. A small dialog box in the center says 'Apply succeeded' with an 'OK' button. The background is dimmed, and the Ruijie logo is visible in the bottom right corner.

## 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

---

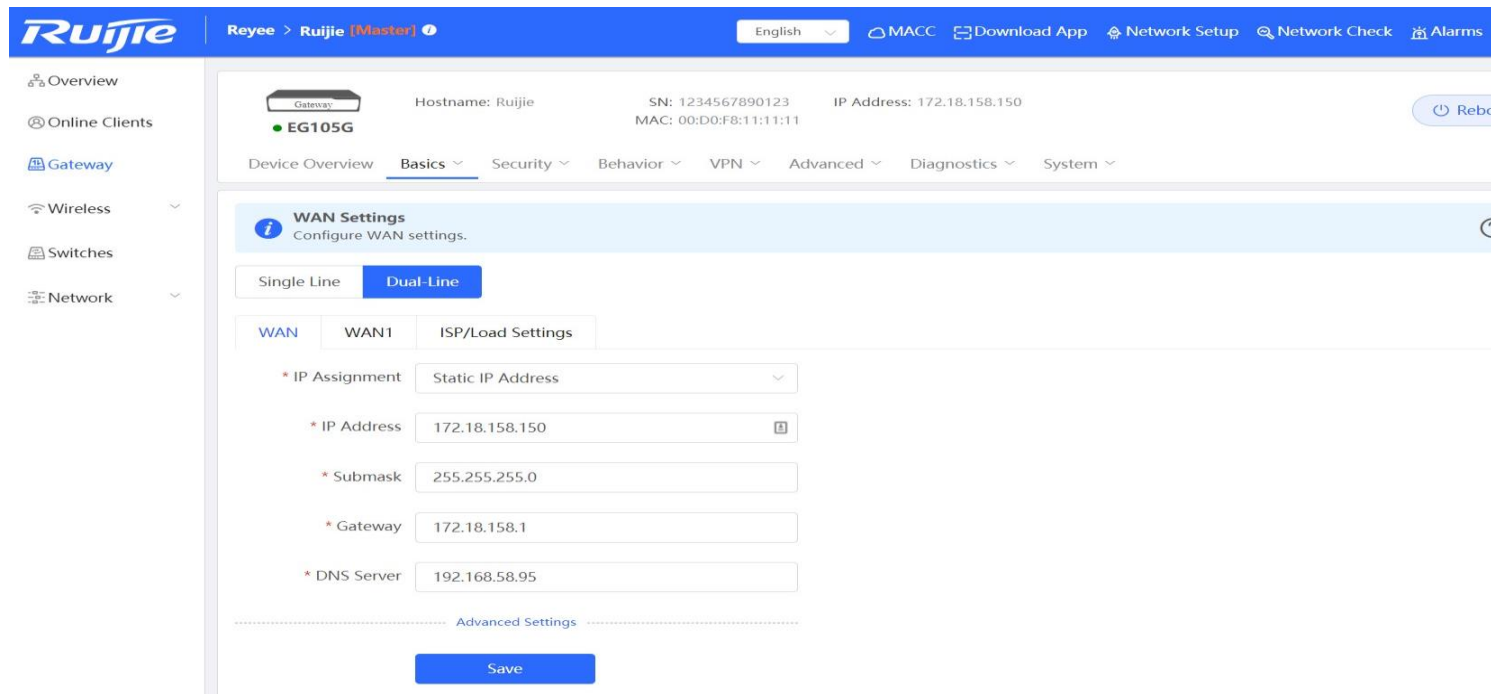
The screenshot shows the Ruijie management interface for a Gateway device. The top navigation bar includes the Ruijie logo, the device name 'Reyee > Ruijie [Master]', and utility links like 'English', 'MACC', 'Download App', 'Network Setup', 'Network Check', and 'Alarms'. A left sidebar contains menu items: 'Overview', 'Online Clients', 'Gateway' (highlighted with a red box), 'Wireless', 'Switches', and 'Network'. The main content area displays device information: Hostname: Ruijie, SN: 1234567890123, IP Address: 172.18.158.150, and MAC: 00:D0:F8:11:11:11. Below this is a tabbed interface with 'Device Overview', 'Basics' (selected), 'Security', 'Behavior', 'VPN', 'Advanced', 'Diagnostics', and 'System'. Under the 'Basics' tab, there is a 'WAN Settings' section with a sub-tab 'WAN' (highlighted with a red box). The 'WAN Settings' section has two modes: 'Single Line' (selected) and 'Dual-Line'. The configuration fields are as follows:

Field	Value
* IP Assignment	Static IP Address
* IP Address	172.18.158.150
* Submask	255.255.255.0
* Gateway	172.18.158.1
* DNS Server	192.168.58.95

Below the fields is an 'Advanced Settings' section, which is currently collapsed. A blue 'Save' button is located at the bottom of the configuration area.

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', and 'Alarms' 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: Gateway EG105G, Hostname: Ruijie, SN: 1234567890123, IP Address: 172.18.158.150, and MAC: 00:D0:F8:11:11:11. 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 sub-tabs for Single Line and Dual-Line (selected). Under Dual-Line, 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 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). Below the instructions are four input fields: '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 located at the bottom of the configuration area.

Step 4: Save the configuration

The screenshot displays the configuration page for a Ruijie Gateway (EG105G). The top navigation bar includes 'Device Overview', 'Basics', 'Security', 'Behavior', 'VPN', 'Advanced', 'Diagnostics', and 'System'. The 'Basics' tab is active, showing 'WAN Settings' with a sub-tab for 'ISP/Load Settings'. The 'Dual-Line' mode is selected. Under 'Load Balancing Settings', a blue information box states: 'Traffic will be routed based on ISP settings preferentially. The remaining traffic will be managed according to load mode.' It lists two modes: 1. Balanced mode (60% WAN, 40% WAN1) and 2. Primary & secondary mode. The configuration fields are: Load Mode (Balanced), Balancing Policy (Based on Link), \* WAN Weight (100), and \* WAN1 Weight (100). A red box highlights the 'Save' button.

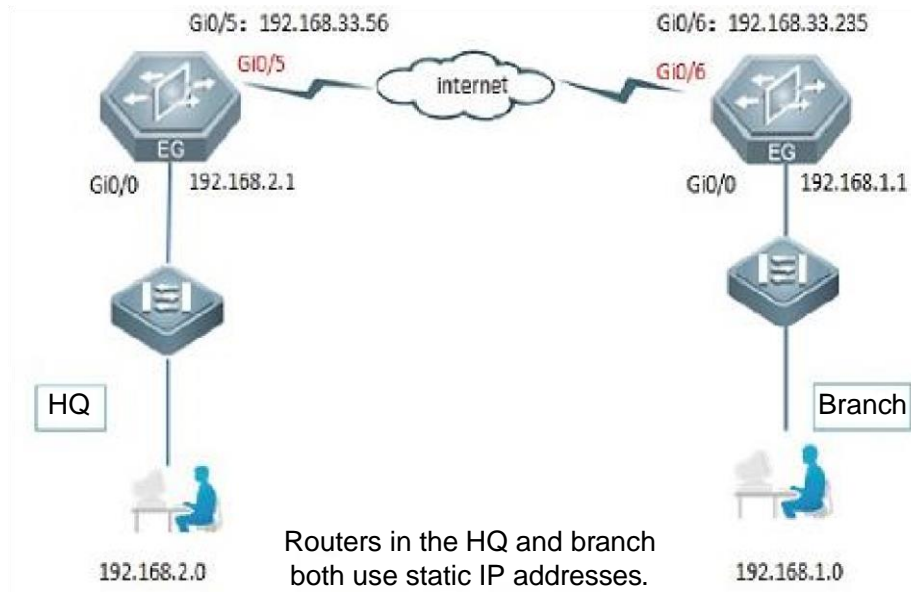
## 5.2 VPN

### 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.

---

The screenshot shows the Ruijie management interface for a Gateway device. The left sidebar has 'Gateway' highlighted. The main content area shows the 'VPN' configuration page, with 'IPSec' selected. Below this, there is an 'IPSec Security Policy' section with a note and tip. At the bottom, there is a 'Policy List' table with columns for Policy Type, Policy Name, Peer Gateway, Local Subnet, Peer Subnet, Status, and Action. The table currently shows 'No Data'. A '+ Add' button is visible in the top right of the Policy List section.

Reyee > Ruijie [Master] English MACC Download App Network Setup Network Check Alarms

Overview  
Online Clients  
**Gateway**  
Wireless  
Switches  
Network

Gateway  
EG105G  
Hostname: Ruijie  
SN: 1234567890123  
IP Address: 172.18.158.150  
MAC: 00:D0:F8:11:11:11

Device Overview Basics Security Behavior **VPN** Advanced Diagnostics System

IPSec Security Policy IPSec Connection Status **IPSec**

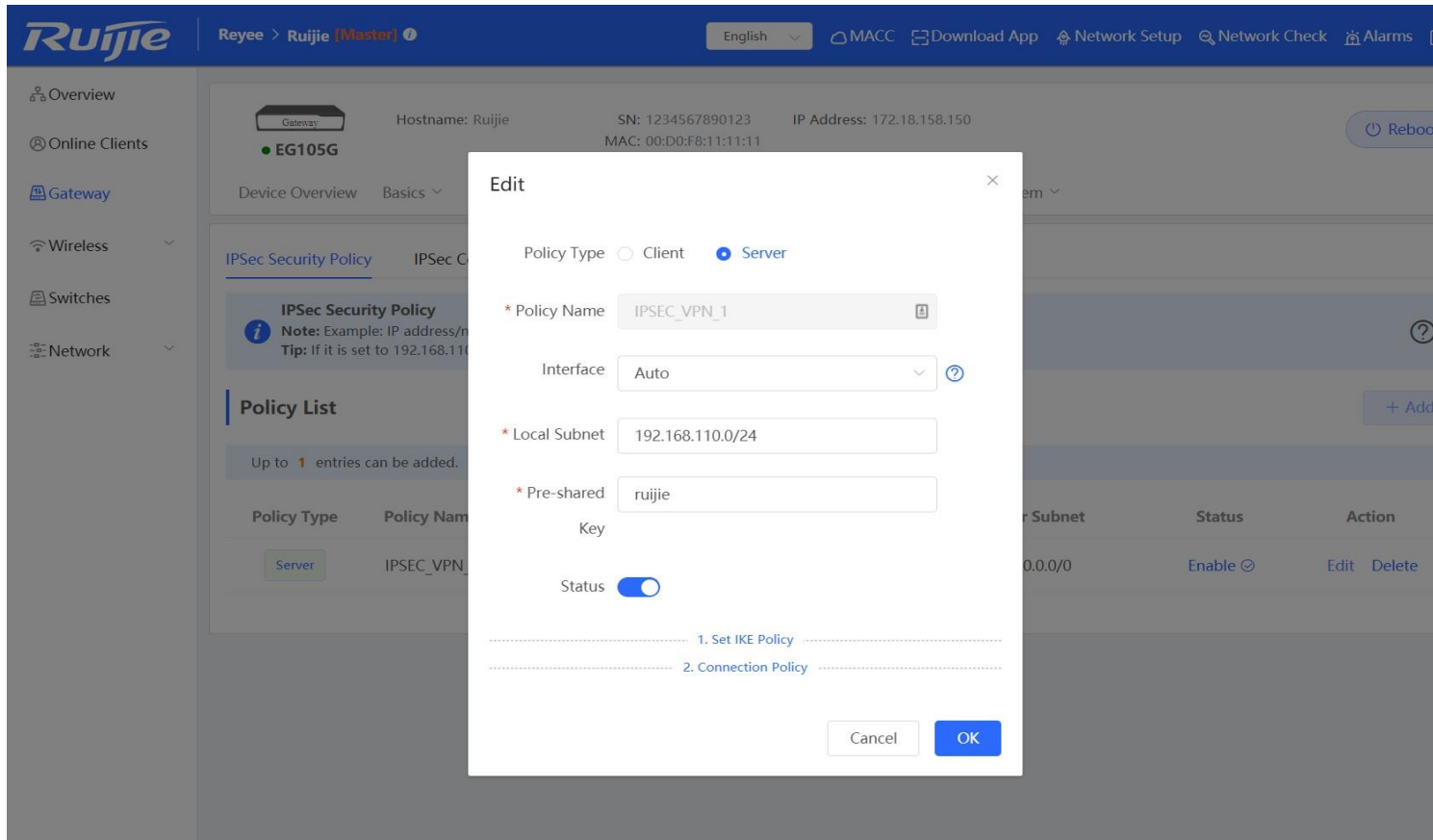
**IPSec Security Policy**  
**Note:** Example: IP address/number of subnet mask bits.  
**Tip:** If it is set to 192.168.110.x/24, the address range is from 192.168.110.1 to 192.168.110.254.

**Policy List** + Add

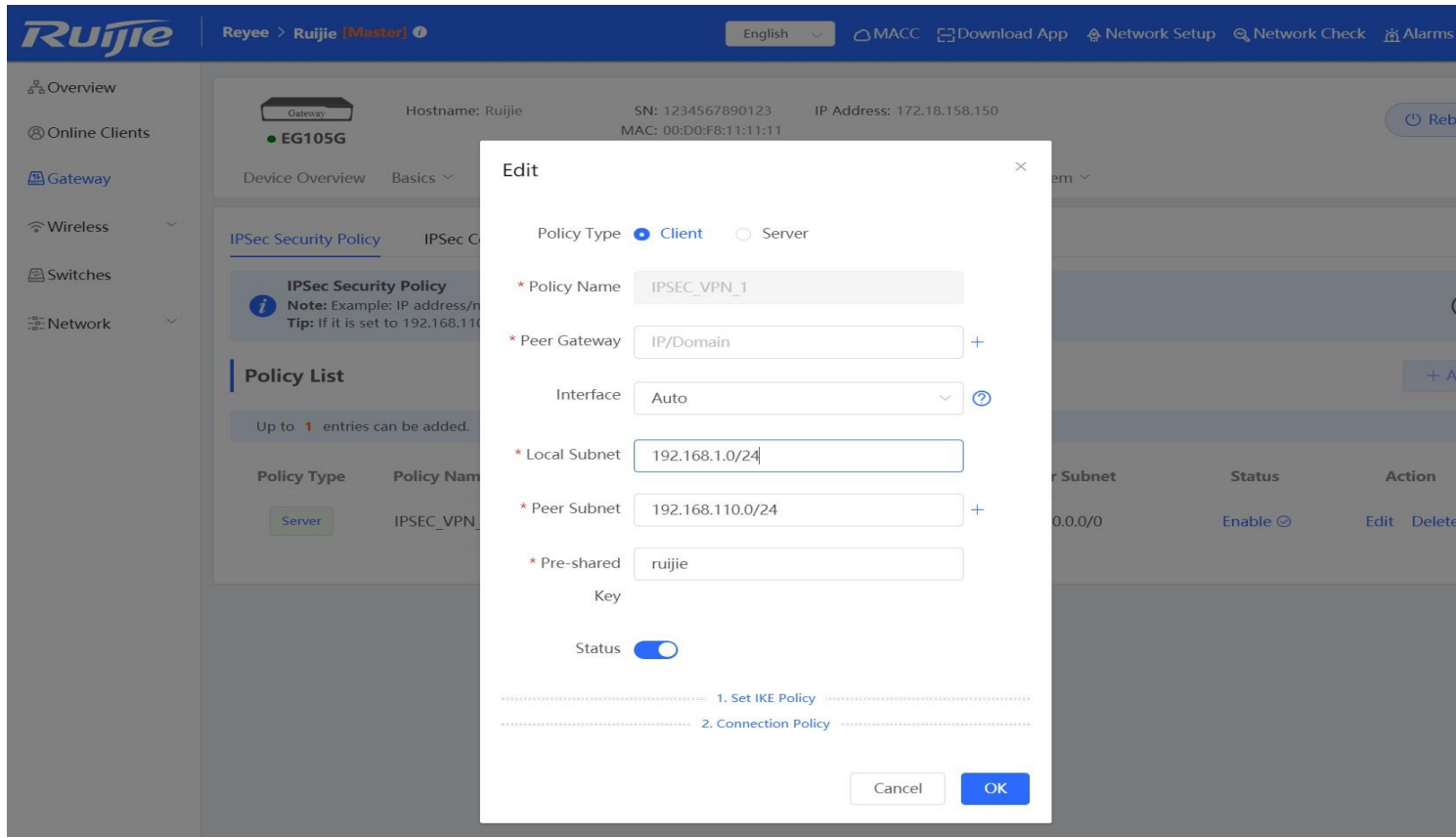
Up to 1 entries can be added.

Policy Type	Policy Name	Peer Gateway	Local Subnet	Peer Subnet	Status	Action
No Data						

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)



## L2TP/PPTP VPN

L2TP/PPTP support server and client,

L2TP Settings Tunnel List

**L2TP Settings**

L2TP Enable

L2TP Type  L2TP Server  L2TP Client

\* Local Address

\* IP Range  ?

\* DNS Server

IPSec Security  ▾

\* PPP Hello Interval  Sec

Save

**VPN Clients**

VPN Client List

+ Add Delete

Up to 30 entries can be added.

	Username	Service Type	Network Mode	Peer Subnet	Status	Action
<input type="checkbox"/>	123456	L2TP	Router to Router	192.168.1.0/24	Enable	Edit Delete



Overview Basics Security Behavior VPN Advanced

PPTP Settings Tunnel List

**PPTP Settings**

Enable PPTP

PPTP Type  PPTP Server  PPTP Client

\* Local Address

\* IP Range  ?

\* DNS Server

\* PPP Hello Interval  seconds

Save

Overview Basics Security Behavior VPN Advanced Diagnostics System

PPTP Settings Tunnel List

**Tunnel List**

	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action
<input type="checkbox"/>	123456	Client	pptp	100.1.1.2	172.26.4.207	100.1.1.1	114.114.114.114	Delete

With the PPTP/L2TP VPN Client, the branch clients no longer need to create a tunnel with the VPN server separately, and can communicate with HQ by connecting to EG

**L2TP Settings**

L2TP Enable

L2TP Type  L2TP Server  L2TP Client

\* Username

\* Password

Interface

Tunnel IP  Dynamic  Static

\* Server Address

\* Peer Subnet

IPSec Security

Work Mode  NAT  Router

\* PPP Hello Interval  Sec

**Tunnel List**

<input type="checkbox"/>	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action
<input type="checkbox"/>	123456	Client	l2tp	200.1.1.2	172.26.4.207	200.1.1.1	114.114.114.114	Delete

**PPTP Settings**

PPTP Enable

PPTP Type  PPTP Server  PPTP Client

\* Username

\* Password

Interface

Tunnel IP  Dynamic  Static

\* Server Address

\* Peer Subnet

Work Mode  NAT  Router

\* PPP Hello Interval  Sec

**Save**

Overview Basics Security Behavior VPN Advanced Diagnostics System

**Tunnel List**

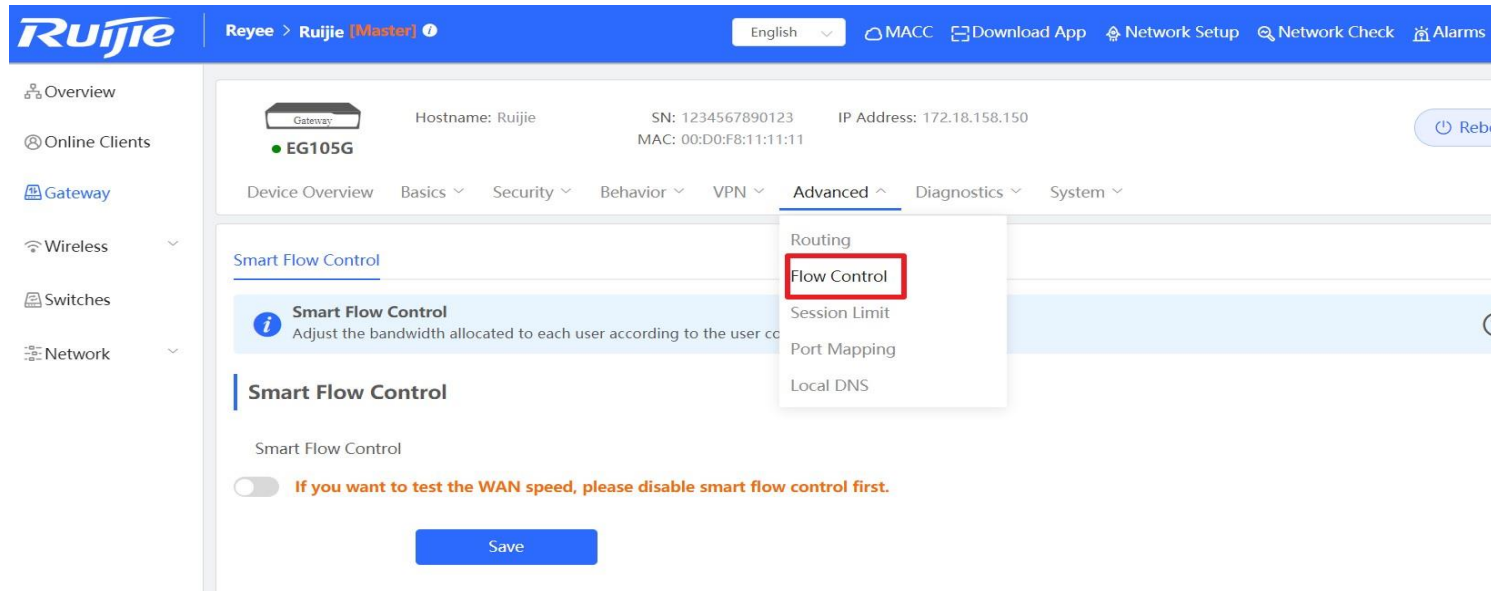
<input type="checkbox"/>	Username	Server/Client	Tunnel Name	Virtual Local IP	Access Server IP	Peer Virtual IP	DNS	Action
<input type="checkbox"/>	123456	Client	pptp	100.1.1.2	172.26.4.207	100.1.1.1	114.114.114.114	Delete

### 5.3 Smart Flow Control

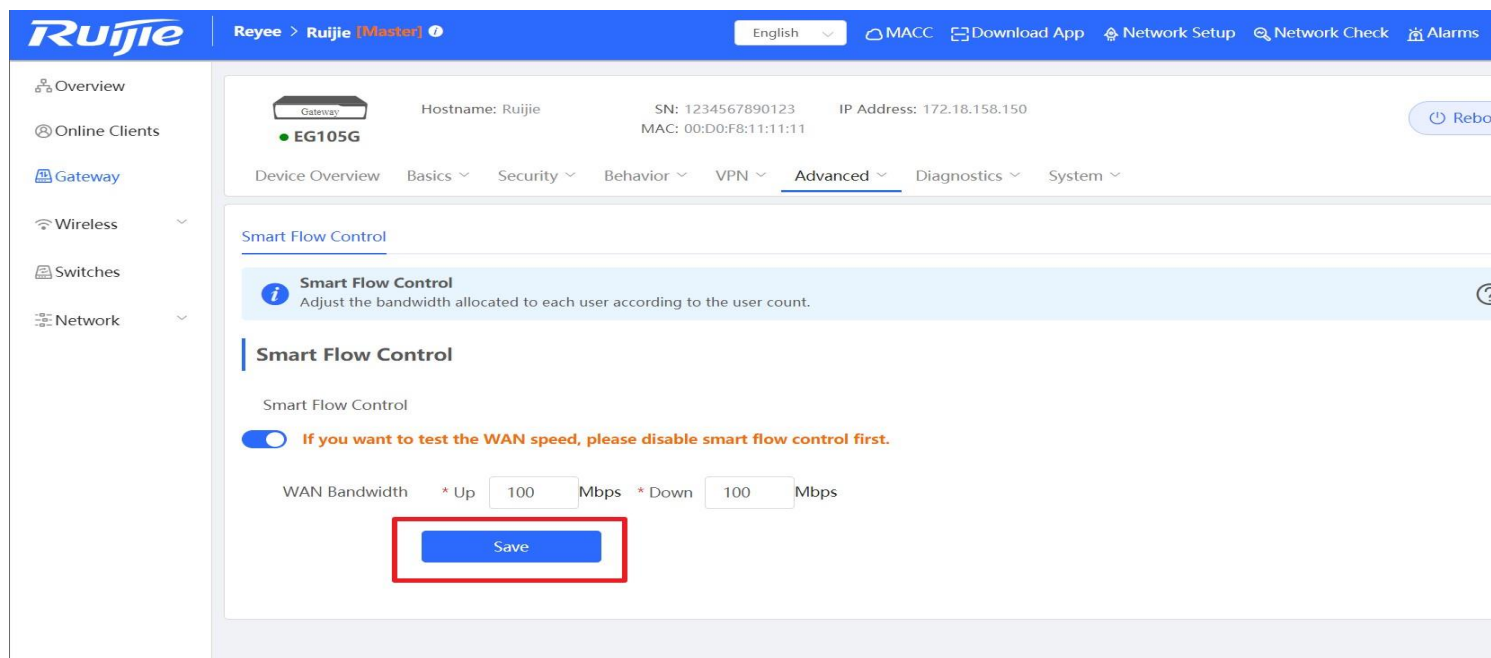
Reyee Smart Flow Control is a feature used to avoid congestion by optimizing user traffic. The working principle is shown as below: when the total user traffic is low than the maximum WAN bandwidth, the rate limit policy will not be applied, every user will get the required bandwidth; However, when the 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

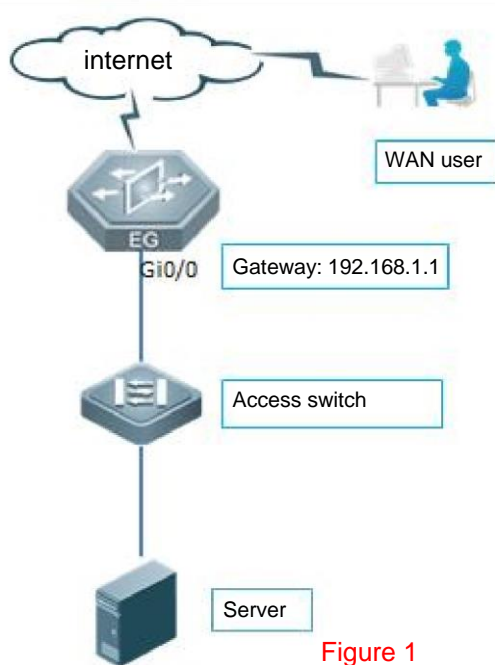


Figure 1

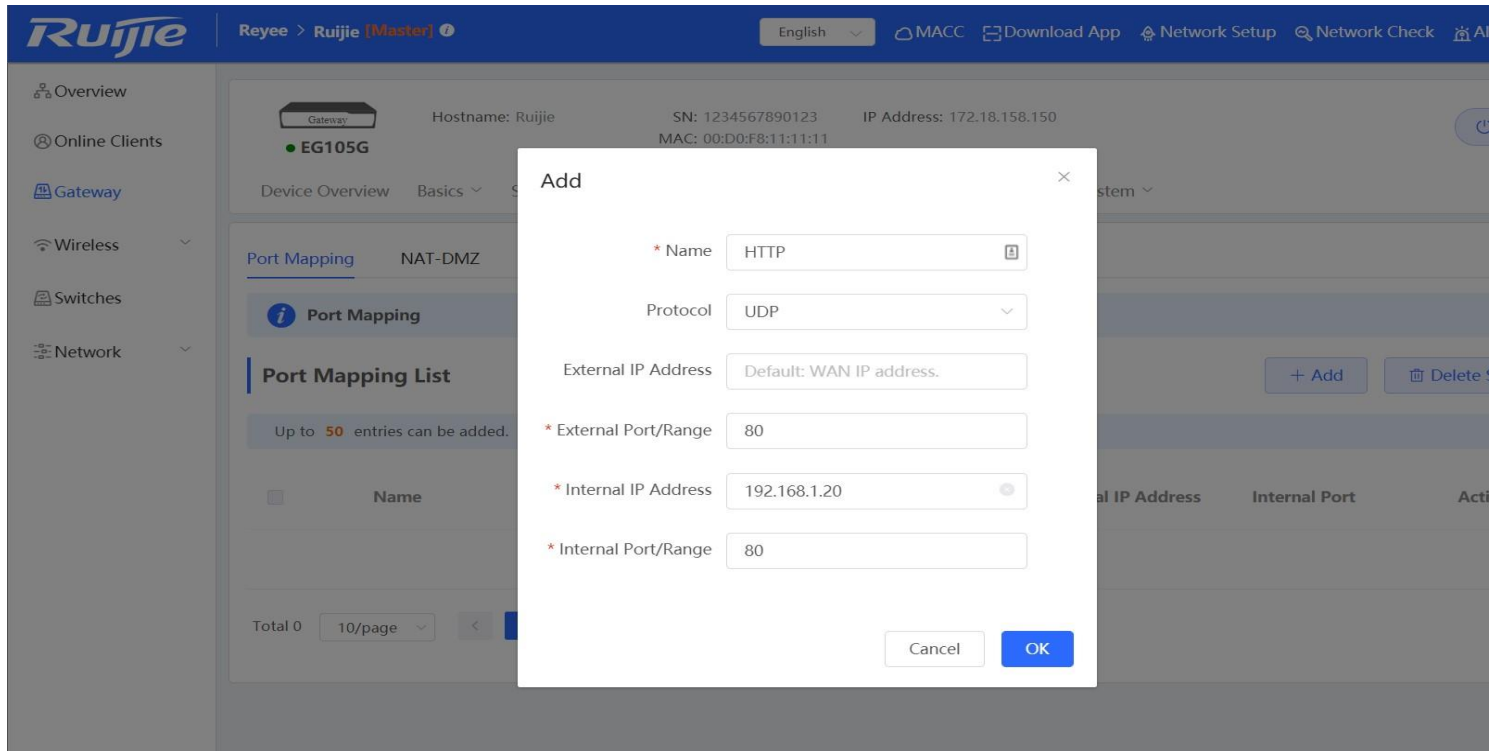
### Configuration Steps

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

---

The screenshot shows the Ruijie Gateway configuration interface. The top navigation bar includes the Ruijie logo, the device name 'Reyee > Ruijie [Master]', and utility links like 'English', 'MACC', 'Download App', 'Network Setup', 'Network Check', and 'Alarm'. The left sidebar contains navigation options: Overview, Online Clients, Gateway, Wireless, Switches, and Network. The main content area displays device information for 'EG105G' (Hostname: Ruijie, SN: 1234567890123, IP Address: 172.18.158.150, MAC: 00:D0:F8:11:11:11). Below this is a menu with 'Advanced' selected, which has opened a dropdown menu with 'Port Mapping' highlighted in a red box. The 'Port Mapping List' section shows a table with columns: Name, Protocol, External IP Address, External Port, Internal IP Address, Internal Port, and Action. The table is currently empty, displaying 'No Data'. At the bottom, there is a pagination control showing 'Total 0', '10/page', and 'Go to page 1'.

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.

## 5.5 Authentication

### Cloud Auth

Configure the Cloud authentication on cloud and sync to EG. Then need to check the configuration on EG Eweb.

| Cloud Portal Auth Only supported on P50 and higher versions

#### Note

1. The Voucher/Account portal authentication on gateway does not support speed limit and flow quota limit that defined on profile.
2. The Voucher/Account portal authentication on gateway does not support flow usage display.
3. Only One-click/Voucher/Account/SMS authentications are supported on the gateway (Facebook auth is not supported).

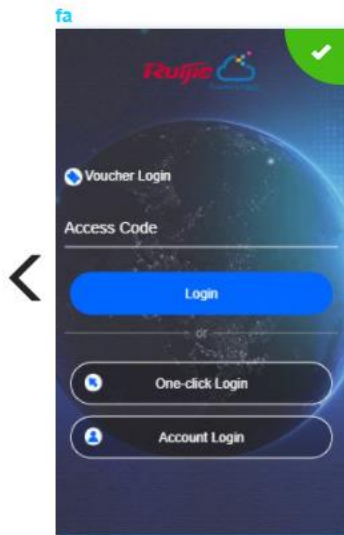
Auth  After you enable Cloud Portal Auth, it will be synced to the Reyee EG automatically.

Portal Escape

Auth IP/Range  +

Seamless Online

Please select a portal [or add a new portal.](#)





- Overview
- Online Clients
- Router
- Wireless
- Switches
- Network

Router Hostname: Ruijie SN: H1MQ8W8006802 IP Address: 172.26.7.55 MAC: 00:74:9C:DF:8F:1B

Overview Basics Security Behavior VPN **Advanced** Diagnostics System

WeChat/SMS/One-Click Auth Account Auth Authorized Auth QR Code Auth Whitelist Online Users

**WeChat/SMS/One-Click Auth**

Connect WiFi via WeChat: Please configure connecting WiFi via WeChat on WeChat public account platform and Ruijie Cloud first. [View](#)

SMS Authentication: Please configure SMS authentication on Ruijie Cloud first. [View](#)

If the IP address of the EAP device is in the authentication IP range, please choose **Whitelist** to add the EAP MAC address to the MAC address whitelist.

Authentication

\* Server Type

\* Auth Server URL

Client Escape  Enable

\* IP/IP Range  Add

Save

## EG local authentication

EG local account auth, add the account on EG Eweb and up to 200 accounts can be added.

- Overview
- Online Clients
- Router
- Wireless
- Switches
- Network

Router Hostname: Ruijie SN: H1MQ8W8006802 IP Address: 172.26.7.55 MAC: 00:74:9C:DF:8F:1B

Overview Basics Security Behavior VPN **Advanced** Diagnostics System

WeChat/SMS/One-Click Auth **Account Auth** Authorized Auth QR Code Auth Whitelist Online Users

**Account Auth**

1. Enable account authentication and create an account.  
2. A user logs in with the account created in step 1 and will be allowed to access the Internet.  
**Make sure that the device can access the Internet. Otherwise, the Portal page may not pop up on the terminal.**  
If the IP address of the EAP device is in the authentication IP range, please choose **Whitelist** to add the EAP MAC address to the MAC address whitelist.

Account Auth

Accounts 1

\* Auth IP/IP Range  Add

Save

**Account Settings**

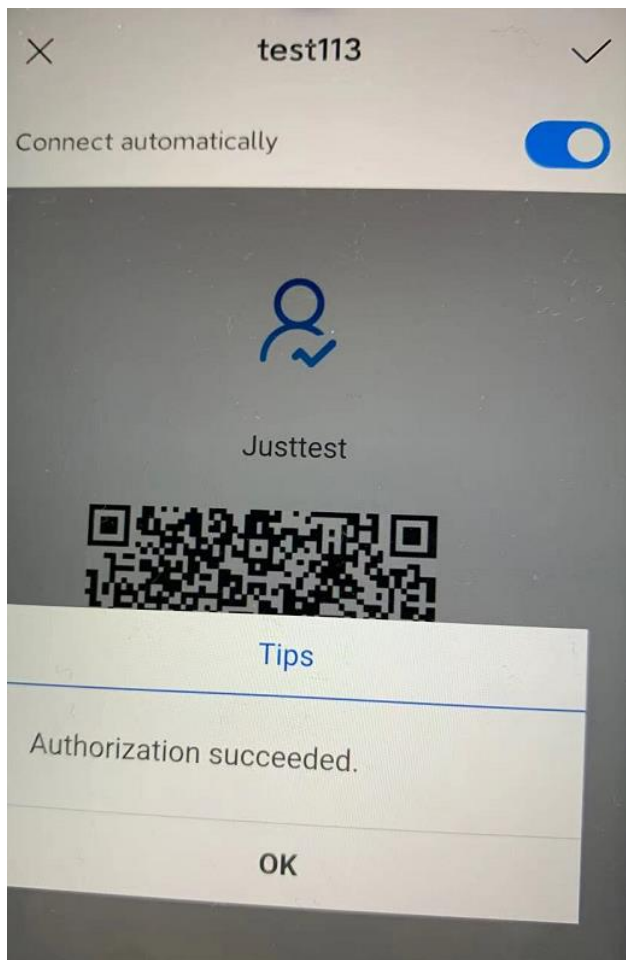
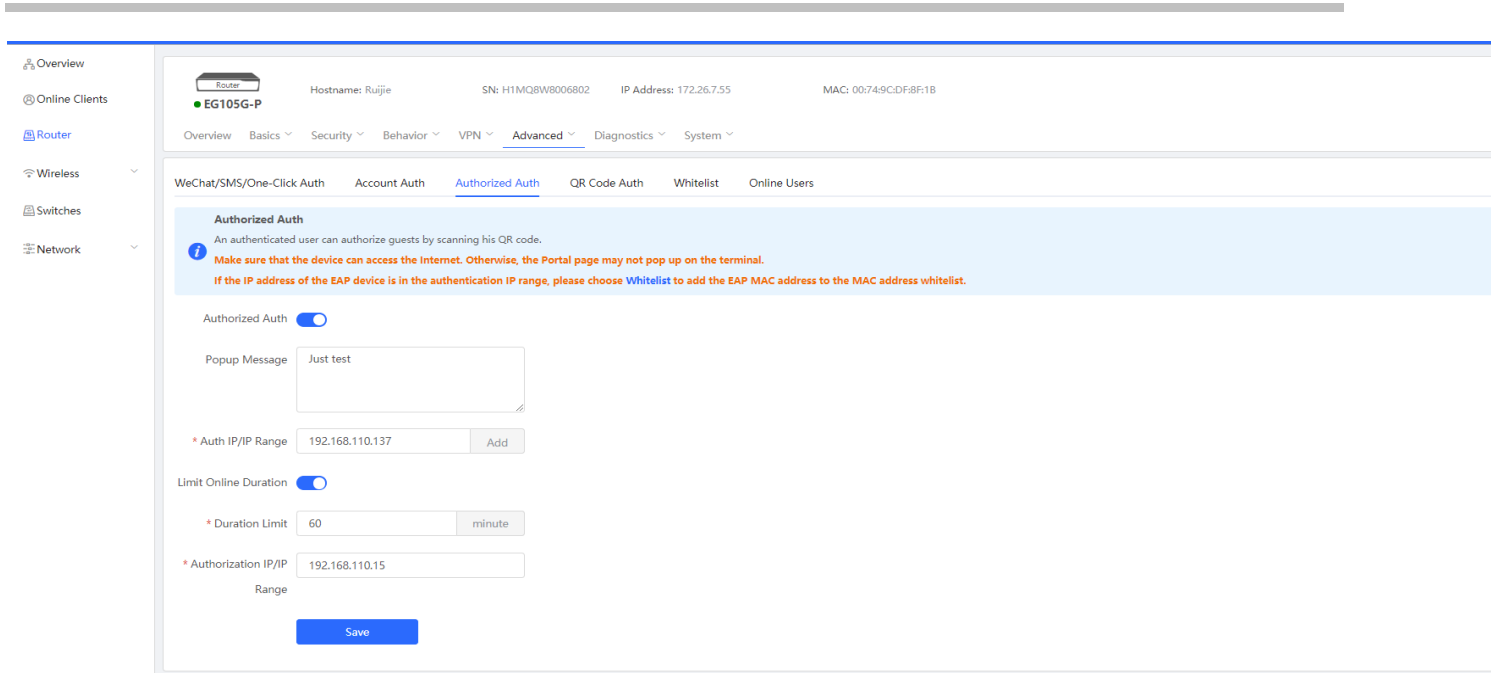
Up to **200** accounts can be added.

<input type="checkbox"/>	Username	Password	MAC	Action
<input type="checkbox"/>	test123	test123		<a href="#">Edit</a> <a href="#">Delete</a>

< 1 > 10/page

## Authorized auth

There are 2 type clients, some are auth clients, some are authorization clients. When auth clients connect to EG, will pop-up the portal page with a QR code, need the authorization clients to scan the QR code to authorize.



### Whitelist of authentication

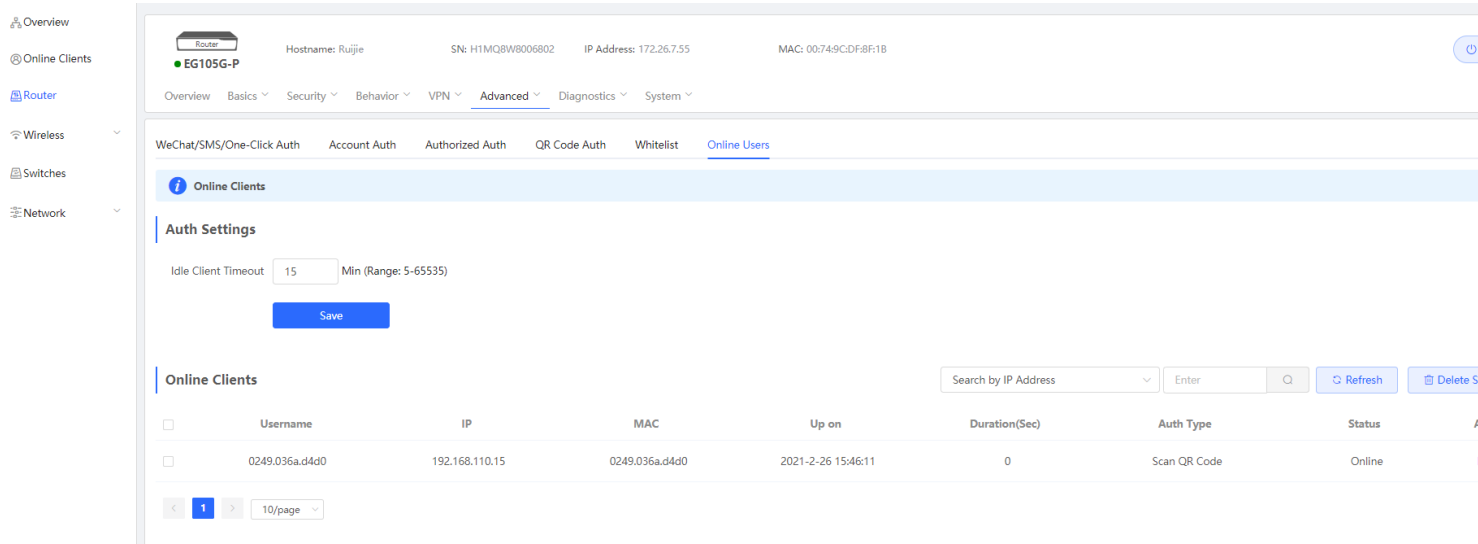
## Whitelist support user whitelist, IP whitelist, URL whitelist, MAC whitelist and MAC blacklist.

The screenshot displays the configuration page for a Ruijie EG105G-P router. The interface includes a left-hand navigation menu with options like Overview, Online Clients, Router, Wireless, Switches, and Network. The main content area is titled 'Whitelist' and contains several sections:

- User Whitelist:** A section with a header 'User Whitelist' and a sub-header 'Up to 50 entries can be added.' It features a table with columns for 'IP/IP Range' and 'Action'. The table is currently empty, showing 'No Data'. Navigation controls include a page number '1' and a dropdown for '10/page'.
- IP Whitelist:** A section with a header 'IP Whitelist' and a sub-header 'Up to 50 entries can be added.' It features a table with columns for 'IP/IP Range' and 'Action'. The table is currently empty, showing 'No Data'. Navigation controls include a page number '1' and a dropdown for '10/page'.
- URL Whitelist:** A section with a header 'URL Whitelist' and a sub-header 'Up to 100 entries can be added.' It features a table with columns for 'URL' and 'Action'. The table is currently empty, showing 'No Data'. Navigation controls include a page number '1' and a dropdown for '10/page'.
- MAC Whitelist:** A section with a header 'MAC Whitelist' and a sub-header 'Up to 250 entries can be added.' It features a table with columns for 'MAC' and 'Action'. The table is currently empty, showing 'No Data'. Navigation controls include a page number '1' and a dropdown for '10/page'.
- MAC Blacklist:** A section with a header 'MAC Blacklist' and a sub-header 'Up to 250 entries can be added.' It features a table with columns for 'MAC' and 'Action'. The table is currently empty, showing 'No Data'. Navigation controls include a page number '1' and a dropdown for '10/page'.

### Online users list

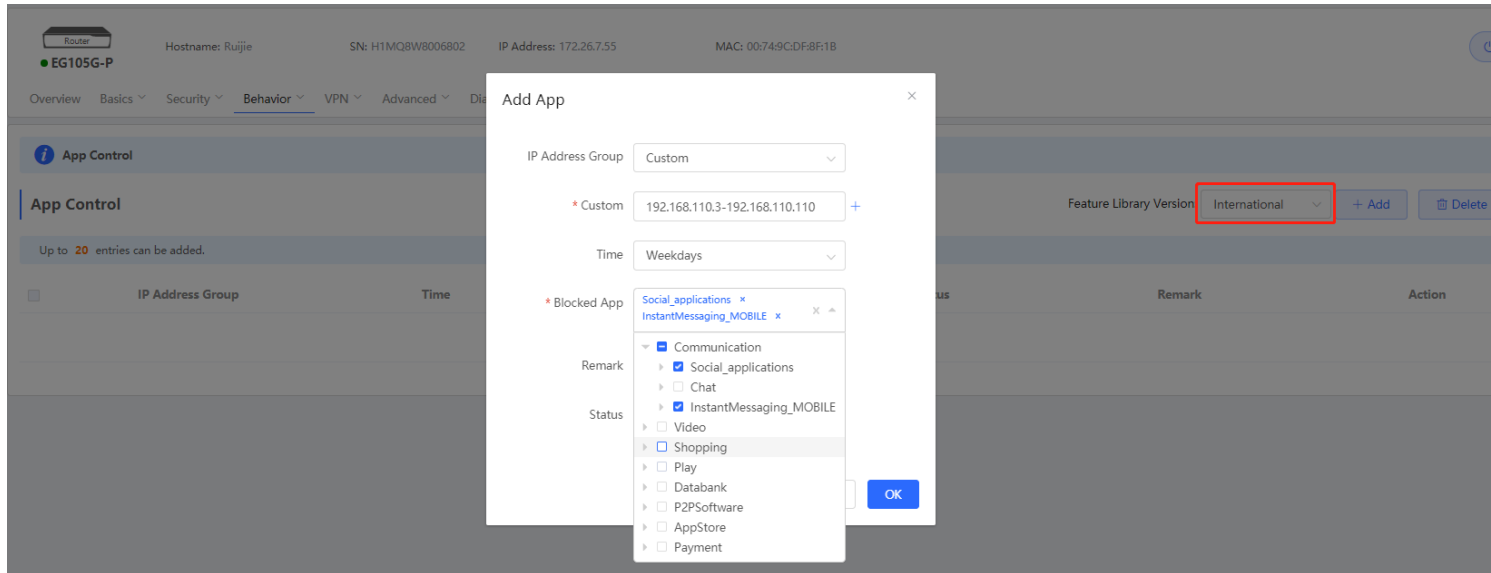
Online users show the user list, “Delete” can kill off the auth user.



## 5.6 Behavior

### APP control

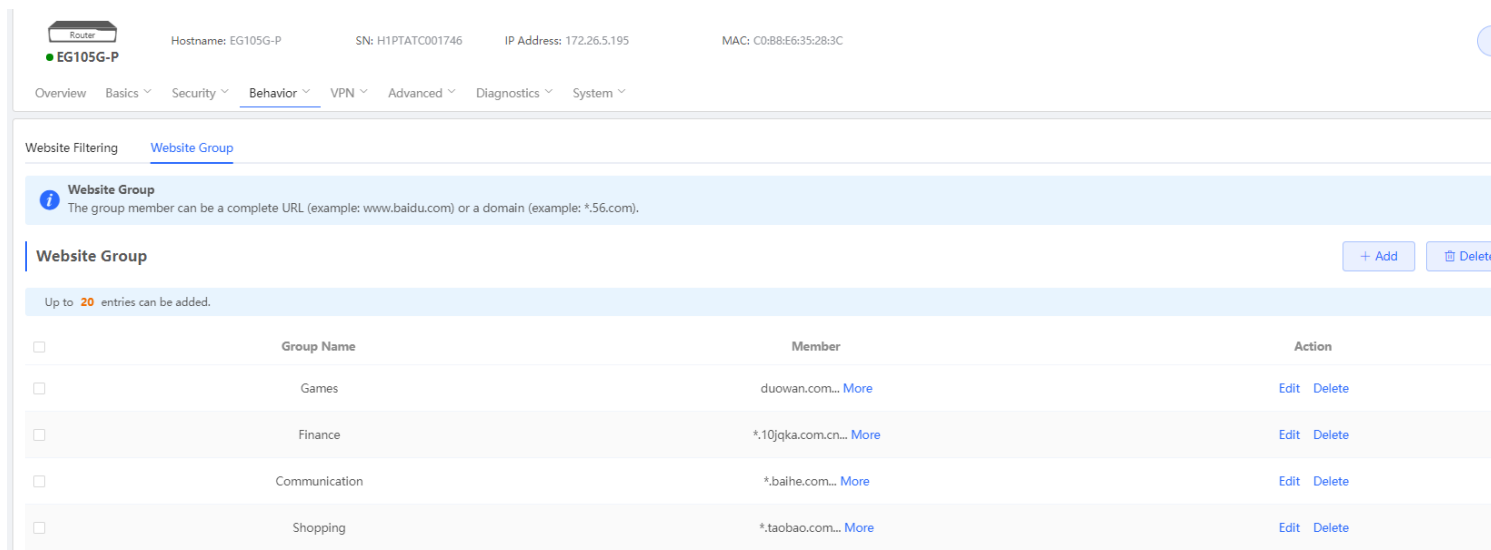
Switch the feature library to international version, choose the blocked applications. Support blocked the applications with IP address group and Time



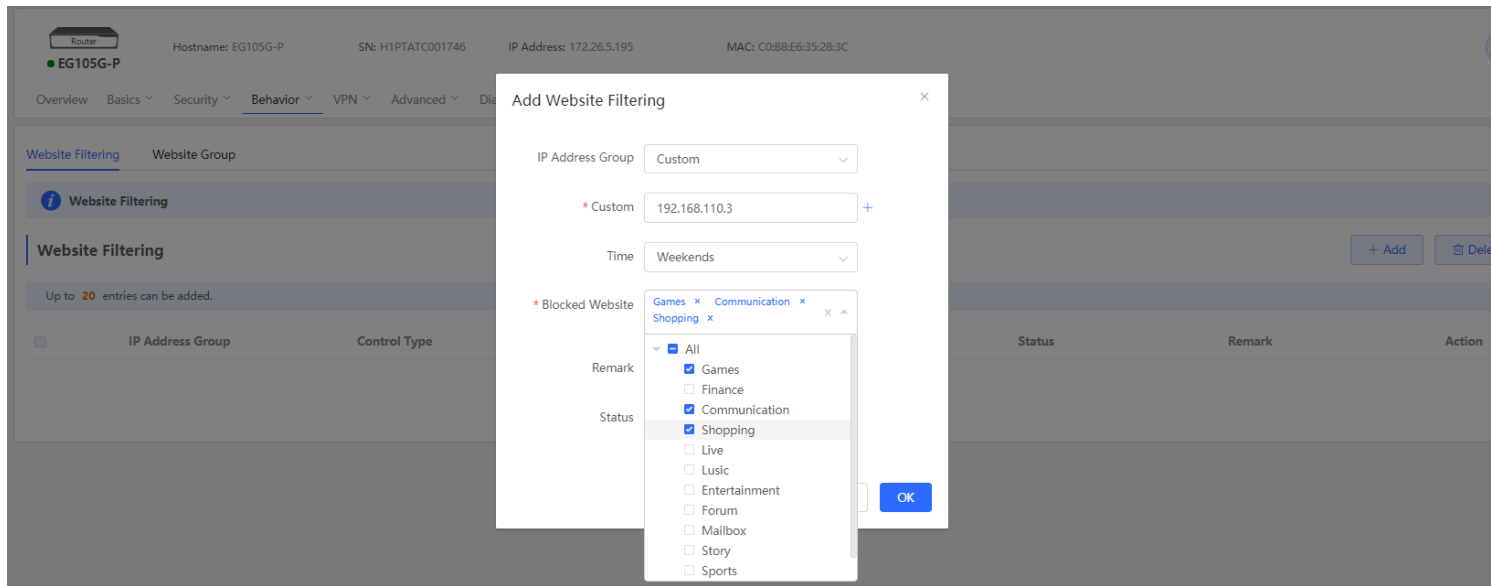
### Website Management

**Step1** Set the website group, the group member can be a complete URL or a domain.

Example: \*.ruijienetworks.com



**Step2** Set the website filtering, choose the blocked website group. Support blocked the applications with IP address group and Time



## 5.7 PPPoE Server

### Configuration Steps:

Step 1: Choose **Router** → **Advanced** → **PPPoE server**

Overview

Online Clients

Router

Wireless

Switches

Network

The screenshot shows the configuration page for a Ruijie EG105G-P router. The top section displays the router's hostname as 'Ruijie', SN as 'H1PT/...', IP Address as '192.168.1.5', and MAC as 'C0:8E:3E:8E:3E:8E'. Below this is a navigation menu with tabs for Overview, Basics, Security, Behavior, VPN, Advanced (selected), Diagnostics, and System. Under the 'Advanced' tab, there are sub-tabs for Global Settings (selected), Account Settings, Account Management, Exceptional IP Address, and Online Clients. The 'Global Settings' section contains an information icon and three warning messages: 1. MAC binding and MAC filtering are not valid for PPPoE clients. 2. The IP address of the PPPoE server cannot overlap with any interface IP range. 3. The authentication function is not valid for PPPoE clients.

Step 2: **Advanced** → **Global Settings**, enable the PPPoE Server, configure the Local address and IP Range, base on the scenario, choose the VLAN.

Overview

Online Clients

Router

Wireless

Switches

Network

Overview

Basics

Security

Behavior

VPN

Advanced

Diagnostics

System

Global Settings

Account Settings

Account Management

Exceptional IP Address

Online C

### Global Settings



- 1. MAC binding and MAC filtering are not valid for PPPoE clients.
- 2. The IP address of the PPPoE server cannot overlap with any interface IP range.
- 3. The authentication function is not valid for PPPoE clients.

PPPoE Server  Enable  Disable

Mandatory PPPoE Dialup  Enable  Disable

\* Local Address

\* IP Range

VLAN

Primary DNS Server

Secondary DNS Server

\* Unanswered LCP  Range: 1-60  
Packet Limit

Auth Mode  PAP  CHAP  
 MSCHAP  MSCHAP2

« Collapse

Global Settings

Account Settings

Account Management

Exceptional IP Address

Online Client

Global Settings



- 1. MAC binding and MAC filtering are not valid for PPPoE clients.
- 2. The IP address of the PPPoE server cannot overlap with any interface IP range.
- 3. The authentication function is not valid for PPPoE clients.

PPPoE Server  Enable  Disable

Mandatory PPPoE Dialup  Enable  Disable

\* Local Address

\* IP Range

VLAN

Primary DNS Server

Secondary DNS Server

\* Unanswered LCP

Range: 1-60

Packet Limit

Auth Mode  PAP  CHAP

MSCHAP  MSCHAP2

Step 3: **Advanced** → **Account Settings**, create the PPPoE account



---

Overview Basics Security Behavior VPN **Advanced** Diagnostics System

Global Settings **Account Settings** Account Management Exceptional IP Address Online Clients

**Account Settings**  
The account management is not in effect. Enable smart flow control

**Account List** + Add Del

Up to 35 entries can be added. Clients 1

<input type="checkbox"/>	Username	Password	Expire Date	Status	Account Management	Remark	Action
<input type="checkbox"/>	test123	test123	2021-06-26	Enable	-		Edit Del

Step 4: Access to the PPPoE client and configure the PPPoE configuration



## WAN Settings

Configure WAN settings.

Single Line

Dual-Line

\* Internet

PPPoE



\* Username

test123

\* Password

.....



[Forgot Account? Obtain Account from Old Device](#)

IP Address 10.44.66.100

Subnet Mask 255.255.255.255

Gateway 10.44.66.99

DNS Server 8.8.8.8

---



Configure WAN settings.

Single Line

Dual-Line

\* Internet

\* Username

\* Password

[Forgot Account? Obtain Account from Old Device](#)

IP Address 10.44.66.101

Subnet Mask 255.255.255.255

Gateway 10.44.66.99

DNS Server 8.8.8.8

Advanced Settings

\* MTU  Range: 576-1492.

\* MAC

802.1Q Tag

\* VLAN ID

\* Default Preference  A smaller value indicates a higher preference

Step 5: PPPoE Server → Online Clients, check the PPPoE status



# Reyee Series Implementation Cookbook

The screenshot shows the Ruijie Cloud management interface. The top navigation bar includes the Ruijie logo, 'Rcycc', and the current user 'Cloud\_Auth\_Test > Ruijie (Master)'. The right side of the bar contains links for 'English', 'Ruijie Cloud', 'Download App', 'Network Setup', 'Network Check', and 'Alarms'. The left sidebar lists various network management options: Overview, Online Clients, Router, Wireless (expanded), APs, Wi-Fi, Clients, Blacklist/Whitelist, Radio Frequency, LAN Ports, LED, Network Optimization (selected), Switches, and Network. The main content area is titled 'Network Optimization' and 'Optimization Record'. It features a progress bar with four stages: Start (checked), Scanning, Optimizing, and Finish (checked). Below the progress bar, there is a 'Description' and 'Notes' section. The 'Notes' section contains three numbered instructions: 1. During network optimization, the APs will switch channels, forcing the clients to go offline. The process will last for a while, subject to the quantity of devices. It is recommended you enable network optimization. 2. If dynamic channel allocation is running in the backend, network optimization will fail. Please try again later. 3. The configuration cannot be rolled back once optimization starts. There is a checkbox 'I have read the notes.' and a 'Network Optimization' button.

**Start**

Description:  
This feature will optimize the self-organizing network to maximize the WLAN performance. Please make sure that all APs have been online.

Notes:  
1. During network optimization, the APs will switch channels, forcing the clients to go offline. The process will last for a while, subject to the quantity of devices. It is recommended you enable network optimization.  
2. If dynamic channel allocation is running in the backend, network optimization will fail. Please try again later.  
3. The configuration cannot be rolled back once optimization starts.

I have read the notes.

Network Optimization

**Scheduled Optimization**

**Scheduled Optimization**  
Optimize the network performance at a scheduled time for a better user experience.

Scheduled

Optimization

Save

## Step 3: Start the optimization, about 2 mins

The screenshot shows the Ruijie Cloud management interface during the 'Scanning' phase. The top navigation bar and left sidebar are identical to the previous screenshot. The main content area shows the progress bar with 'Start' (checked), 'Scanning' (active), 'Optimizing', and 'Finish' (checked). A circular progress indicator shows 10% completion. The 'Scanning' section includes the start time '2021-07-13 17:41:53' and an 'Expected Time: 2 minute'. Below this, there are three informational notes: 1. Radio interference includes WLAN and non-WLAN interference. 2. WLAN interference mainly comes from 802.11 WLAN devices, including TP-LINK home routers and some public WLAN devices. It is recommended to negotiate with the device owner for provisioning and planning. 3. Non-WLAN interference mainly comes from non-WLAN devices working on 2.4Ghz or 5Ghz band, including microwave oven, Bluetooth and microwave therapy apparatus. The devices will occupy the air interface and generate interference, affecting user experience. 4. It is recommended to disable power-saving for PC clients to maintain the WLAN connection even in the sleep mode, saving re-association or re-authentication. 5. Set the roaming sensitivity level to High to ensure that clients will roam smoothly. 6. As for iOS-based clients, it is recommended to update to the latest version. Otherwise, the authentication page may pop up slowly and the Wi-Fi icon may light up slowly.

**Scanning**

Start: 2021-07-13 17:41:53  
Expected Time: 2 minute

10%

Radio interference includes WLAN and non-WLAN interference.  
WLAN interference mainly comes from 802.11 WLAN devices, including TP-LINK home routers and some public WLAN devices. It is recommended to negotiate with the device owner for provisioning and planning.  
Non-WLAN interference mainly comes from non-WLAN devices working on 2.4Ghz or 5Ghz band, including microwave oven, Bluetooth and microwave therapy apparatus. The devices will occupy the air interface and generate interference, affecting user experience.  
It is recommended to disable power-saving for PC clients to maintain the WLAN connection even in the sleep mode, saving re-association or re-authentication.  
Set the roaming sensitivity level to High to ensure that clients will roam smoothly.  
As for iOS-based clients, it is recommended to update to the latest version. Otherwise, the authentication page may pop up slowly and the Wi-Fi icon may light up slowly.

**Scheduled Optimization**

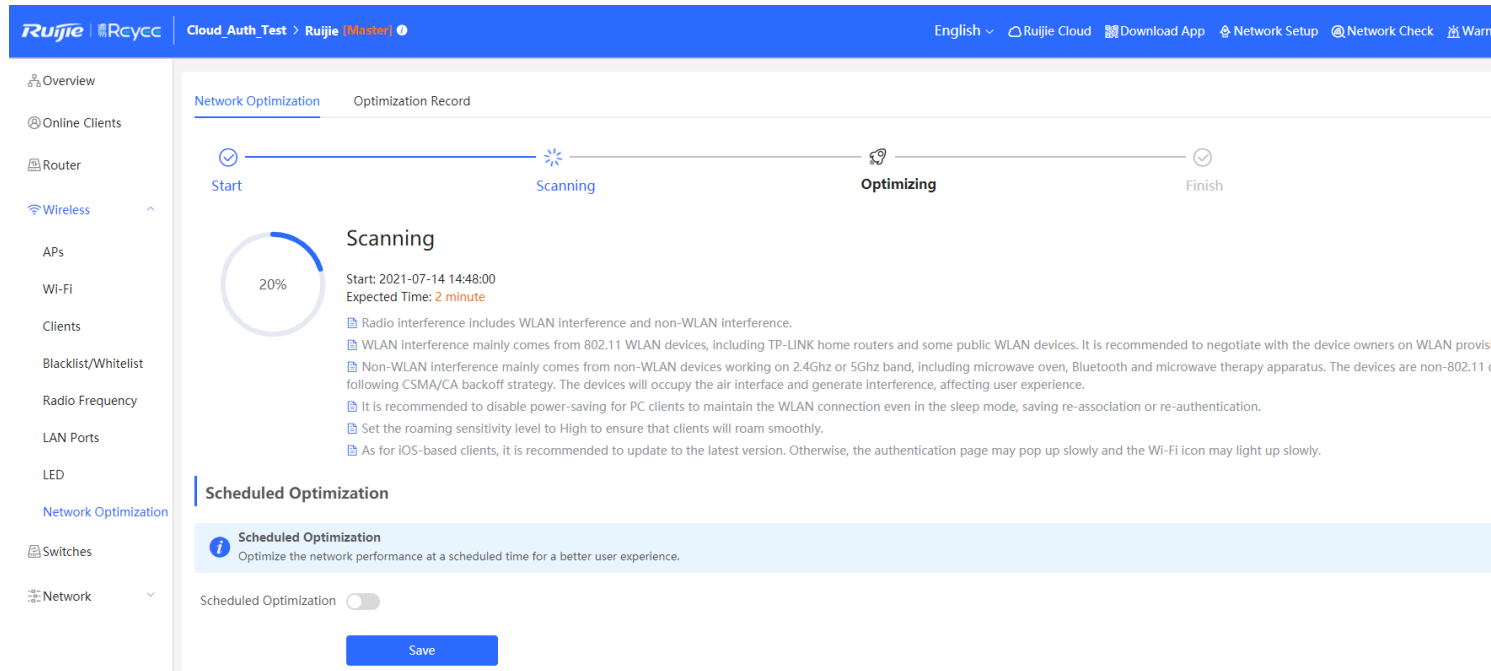
**Scheduled Optimization**  
Optimize the network performance at a scheduled time for a better user experience.

Scheduled

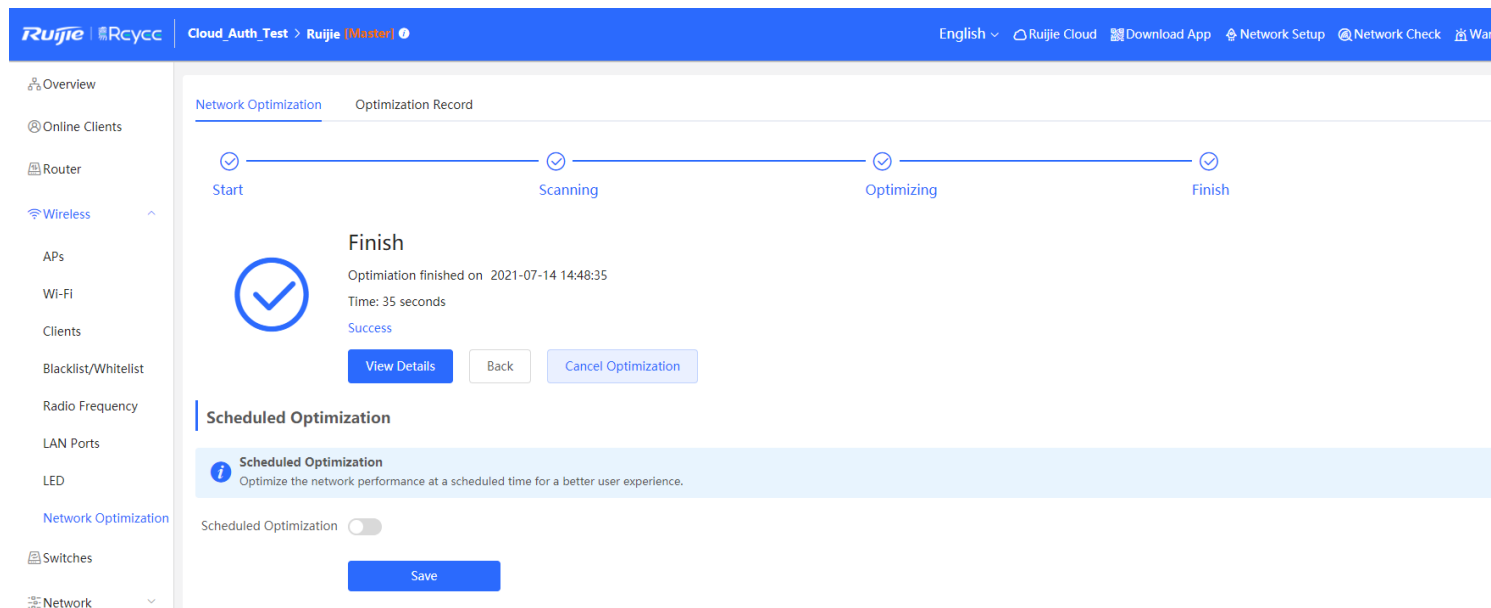
Optimization

Save

## Step 4: APs will scan the WLAN interference and submit to EG

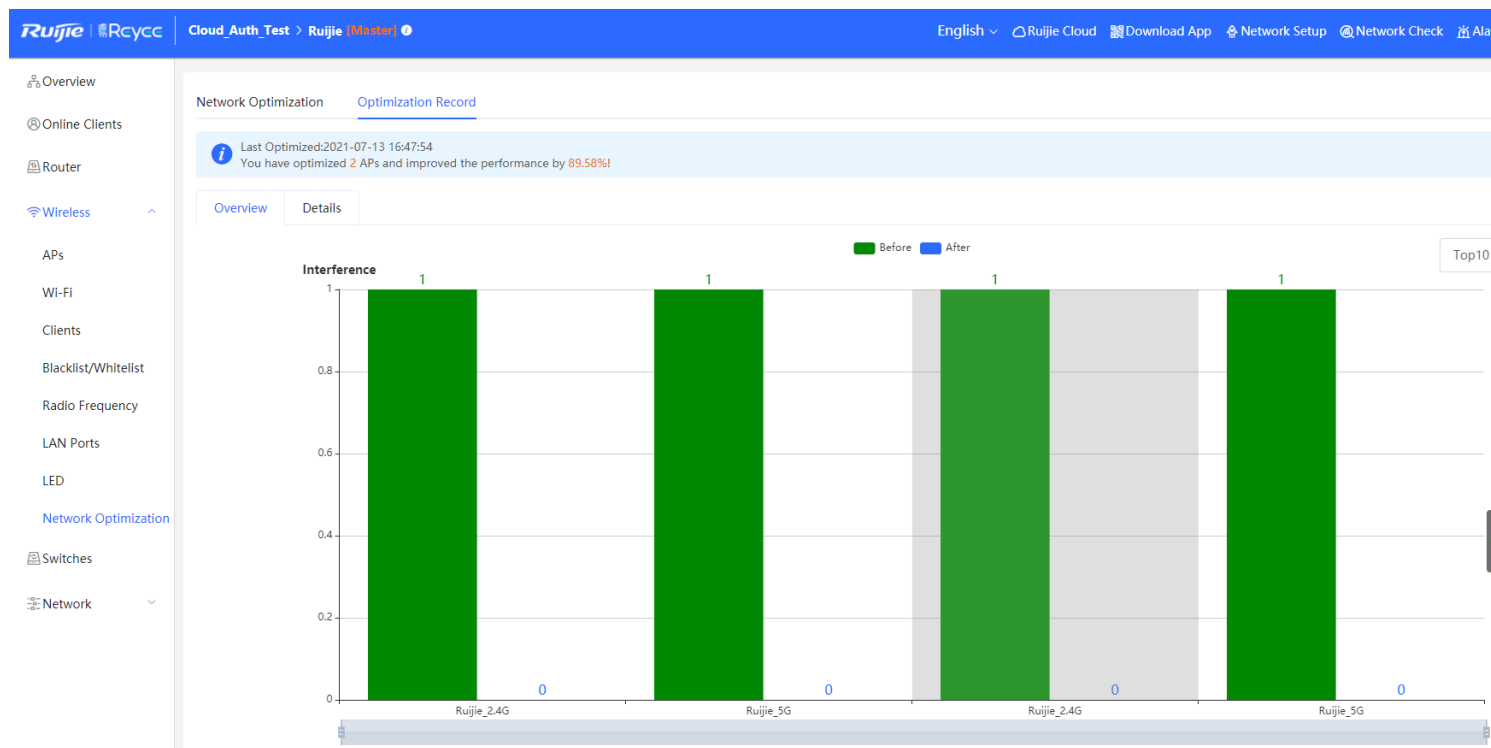


Step 5: When optimization finish, will show the optimization result



Step 6: Click "View Details", will show with overview and details. Overview, show the interference for all APs

# Reyee Series Implementation Cookbook



**Network Optimization - Optimization Record**

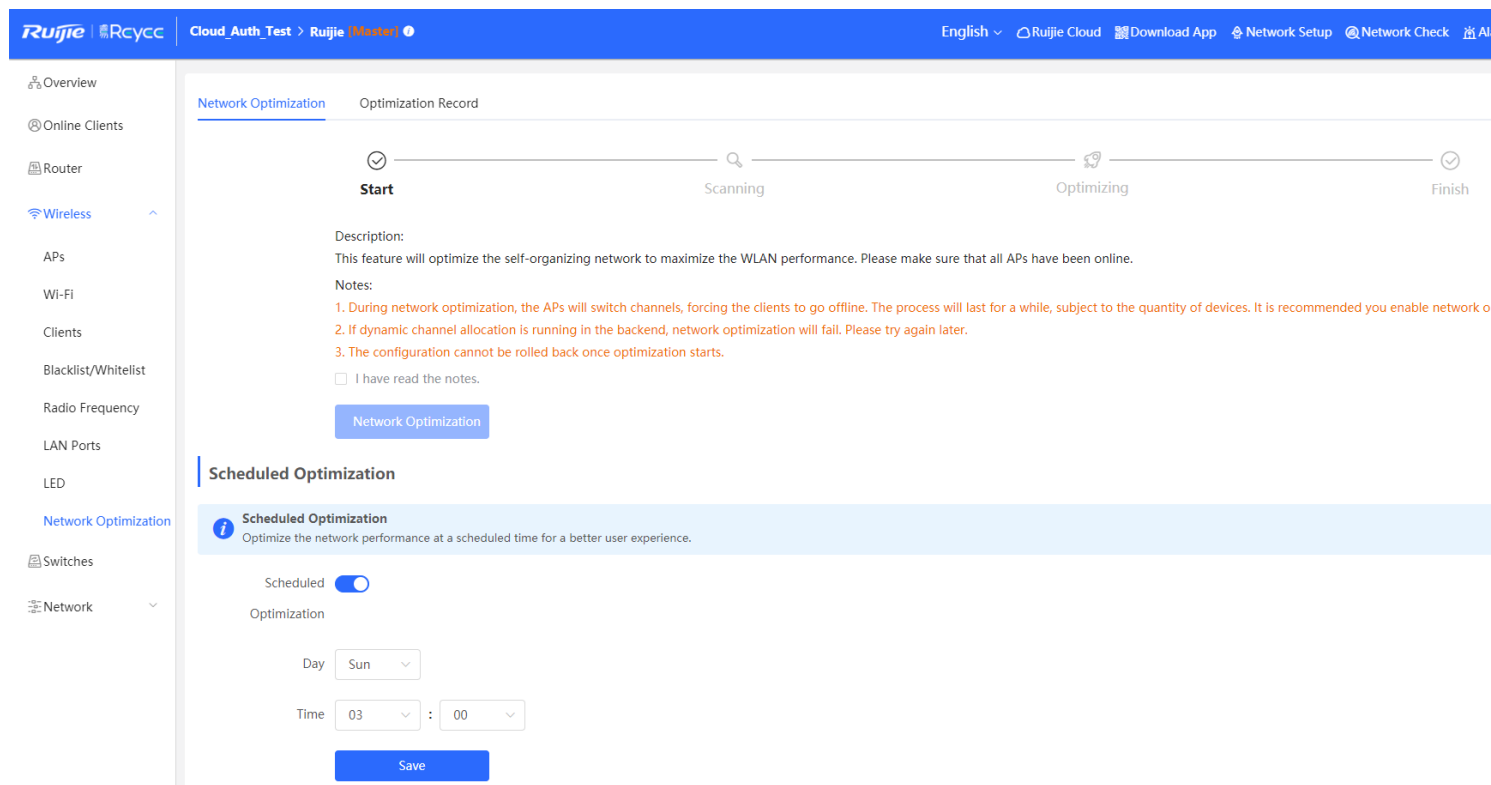
Last Optimized: 2021-07-13 16:47:54  
You have optimized 2 APs and improved the performance by 89.58%!

Overview Details

Hostname	Band	SN	Channel (Before/After)	Channel Width (Before/After)	Transmit Power (Before/After)	Sensitivity (Before/After)	Co-channel interference		Adjacent-channel	
							CCI (Before/After)	ACI (Before/After)		
Ruijie	2.4G	G1QH16Q05197B	1/11	40	100	0/90	1/0	0		
Ruijie	5G	G1QH16Q05197B	149/36	80	100	0/90	1/0	0		
Ruijie	2.4G	G1QH26P01384A	1	40	100	0/80	1/0	0		
Ruijie	5G	G1QH26P01384A	149	80	100	0/68	1/0	0		

Page 1 of 10

## Support scheduled Optimization



## Limitation

- 1) When there are only RAP2200(F), RAP1200(F) and no EG in the network, WIO is not supported (no EG and only 100M AP projects cannot be used WIO)
- 2) When there is no EG in the networking, WIO can only be used for networking with less than 50 APs (without EG, projects with less than 50 Gigabit APs networking can complete)
- 3) WIO can be used when there is EG

## Support Models

**Gateway:** EG105G, EG105G-P, EG105GW, EG210G-P, EG105G-V2

**RAP:** RAP2200(E), RAP2200(F), RAP1200(F), RAP1200(P)

## 5.8 Load Balancing

### Principle

- 1) The AP reports the number of STAs/traffic information to EG
- 2) EG judges whether to continue to allow access based on the reported information:

Comprehensively consider the balance of the entire network, and make balance decisions based on the set start threshold and traffic difference

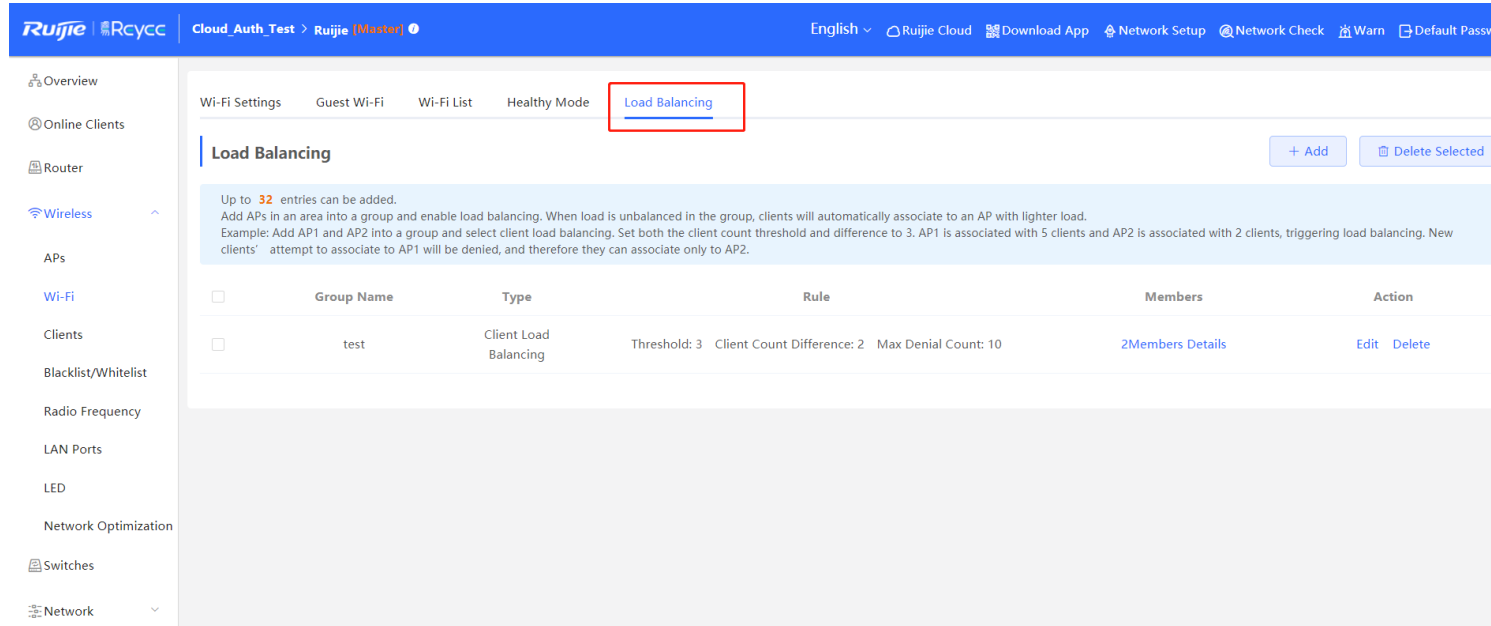
- 3) The AP adjusts whether to allow terminal access according to the status by the EG:



Respond to the information that the terminals reach the upper limit in the disallowed state (auth response message with **Status code 17**), and guide the terminal to associate with other APs

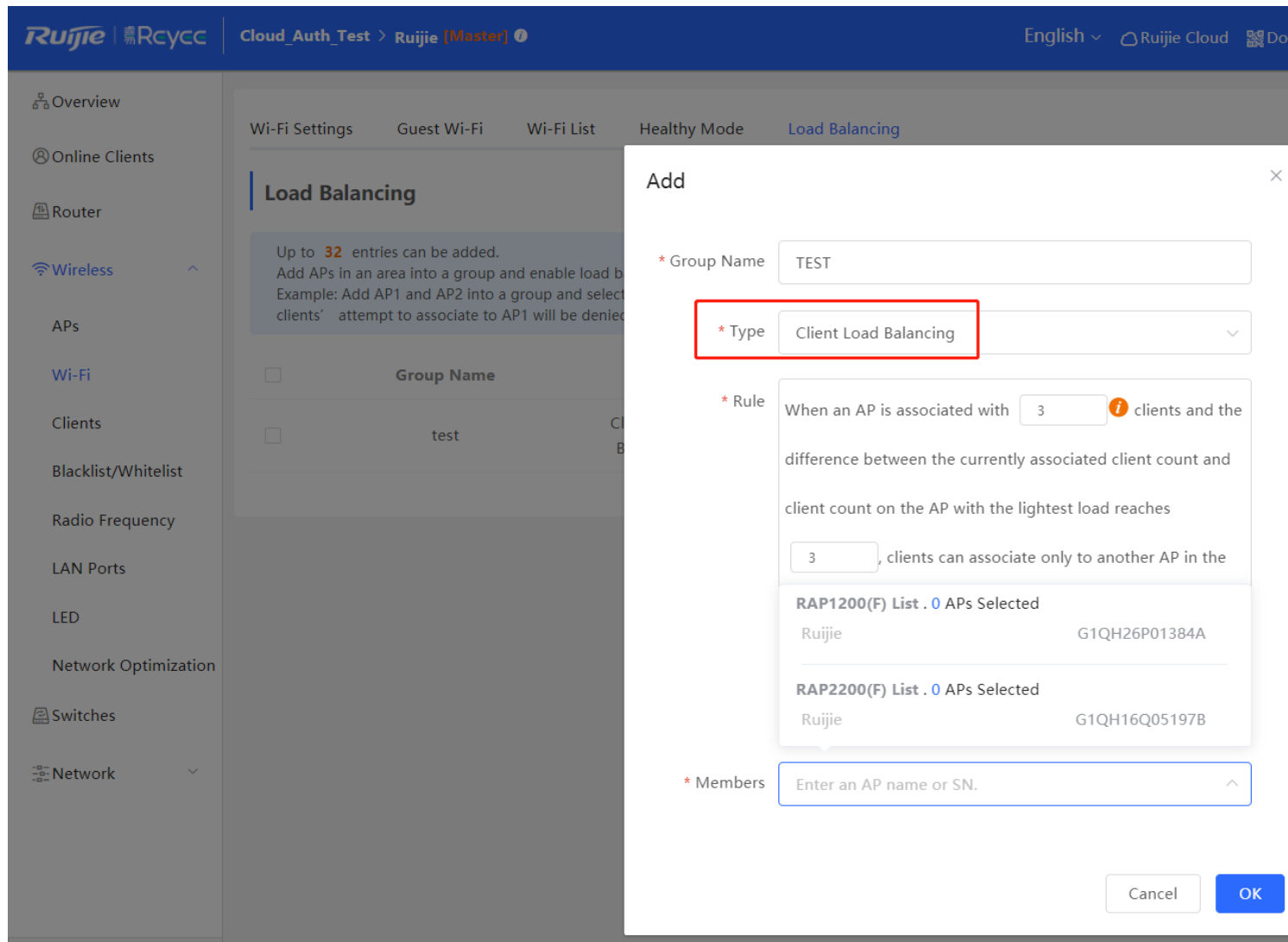
**Configuration Steps:**

**Step 1: Wireless → Wi-Fi → Load Balancing**



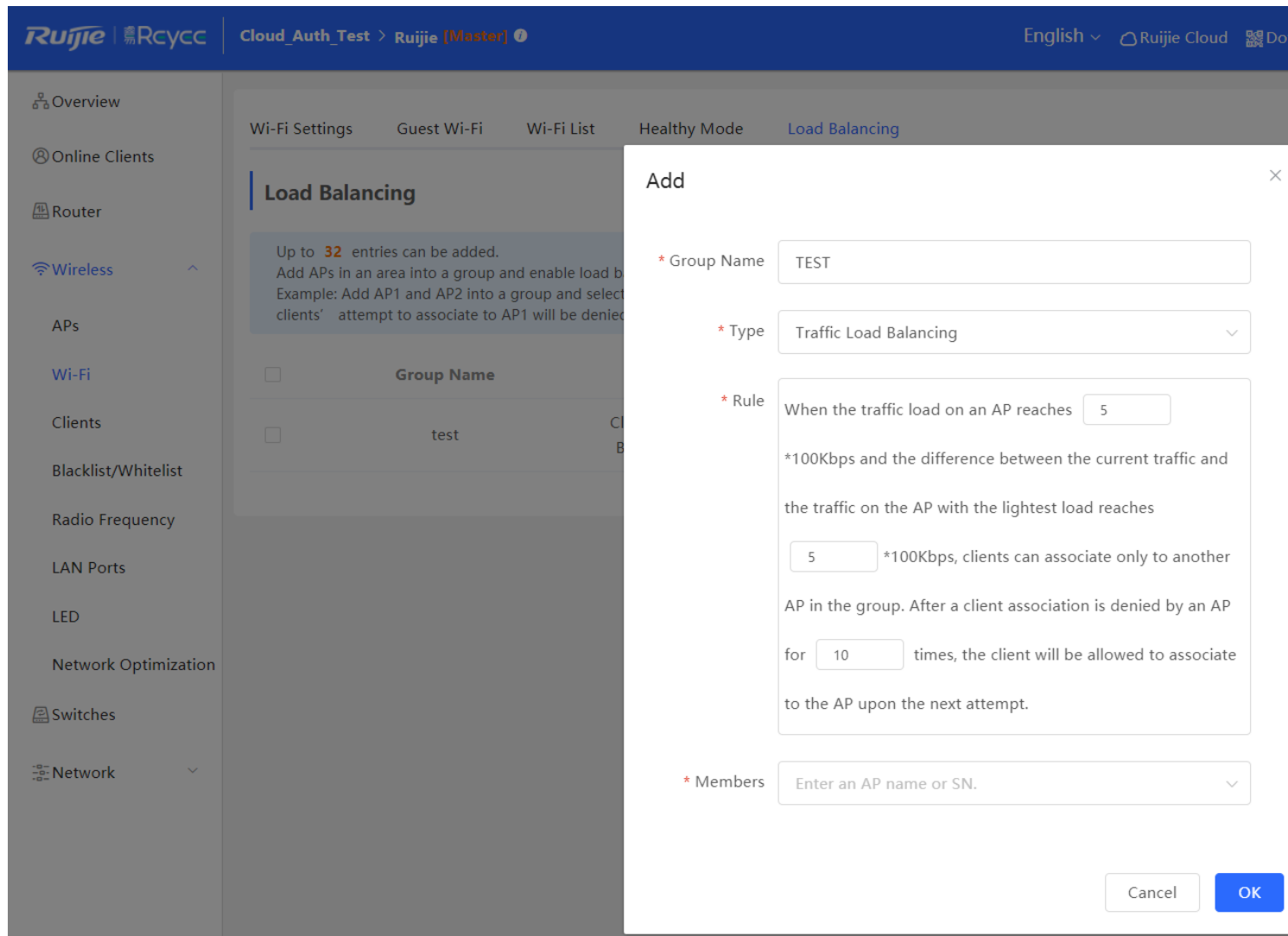
**Step 2: Based-Clients.**

Set both the client count threshold and difference to 3. AP1 is associated with 5 clients and AP2 is associated with 2 clients, triggering load balancing. New clients' attempt to associate to AP1 will be denied, and therefore they can associate only to AP2.



**Step 3: Based-traffic.**

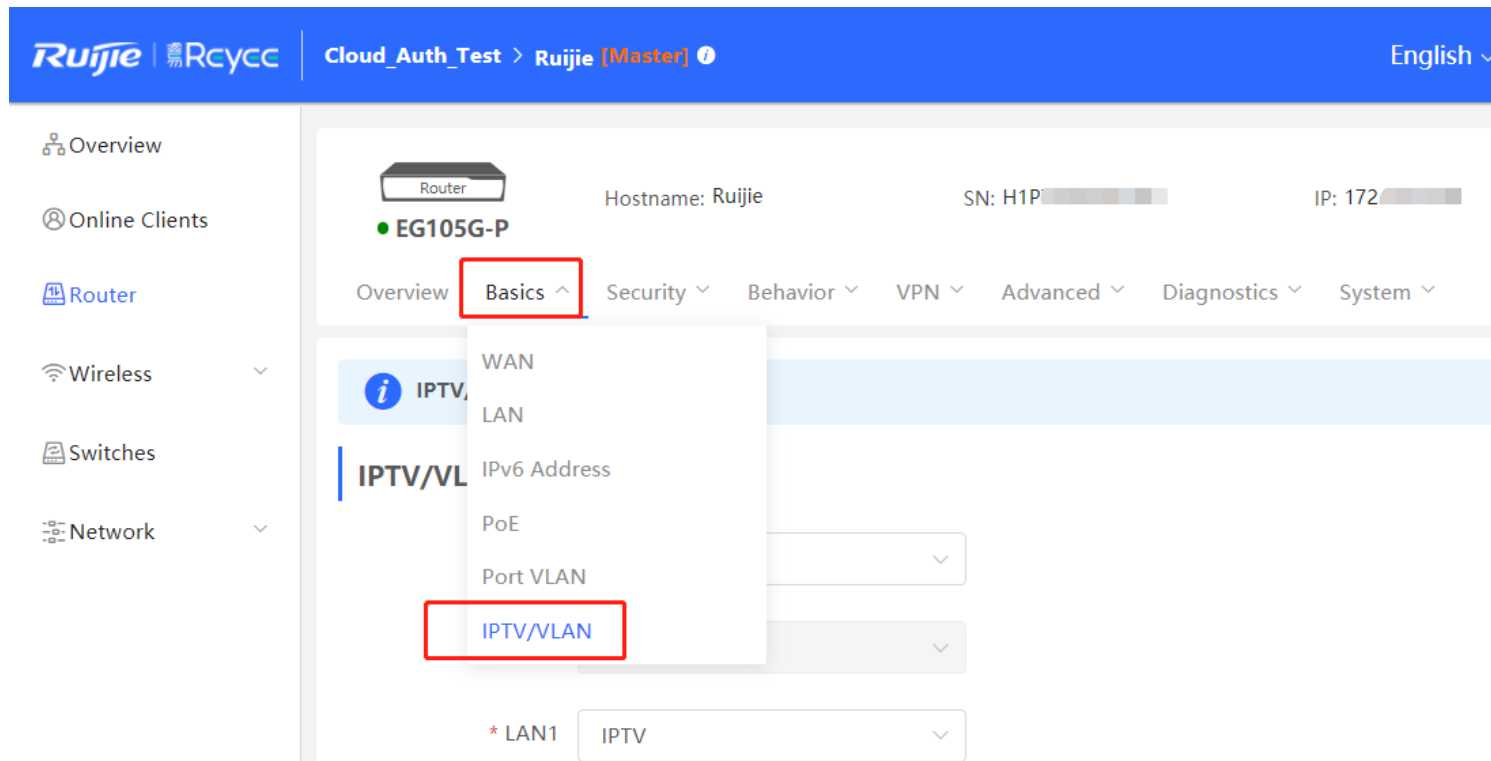
When the traffic load on an AP reaches 5\*100Kbps and the difference between the current traffic and the traffic on the AP with the lightest load reaches 5\*100Kbps, clients can associate only to another AP in the group. After a client association is denied by an AP for 10 times, the client will be allowed to associate to the AP upon the next attempt.



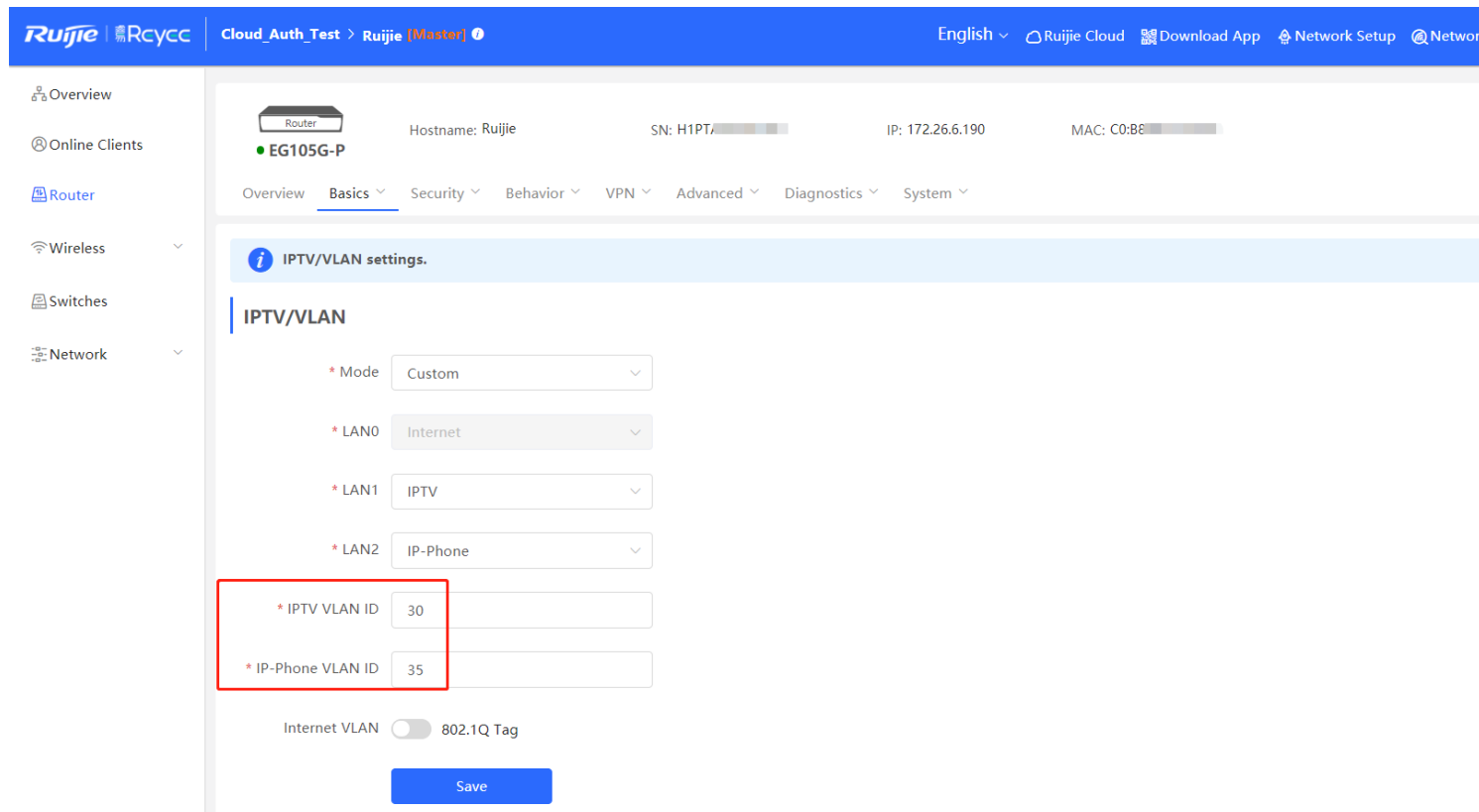
## 5.9 IPTV

### Configuration Steps:

Step 1: **Router** → **Basics** → **IPTV/VLAN**



**Step 2: Configure the IPTV VLAN ID and IP-Phone VLAN ID**



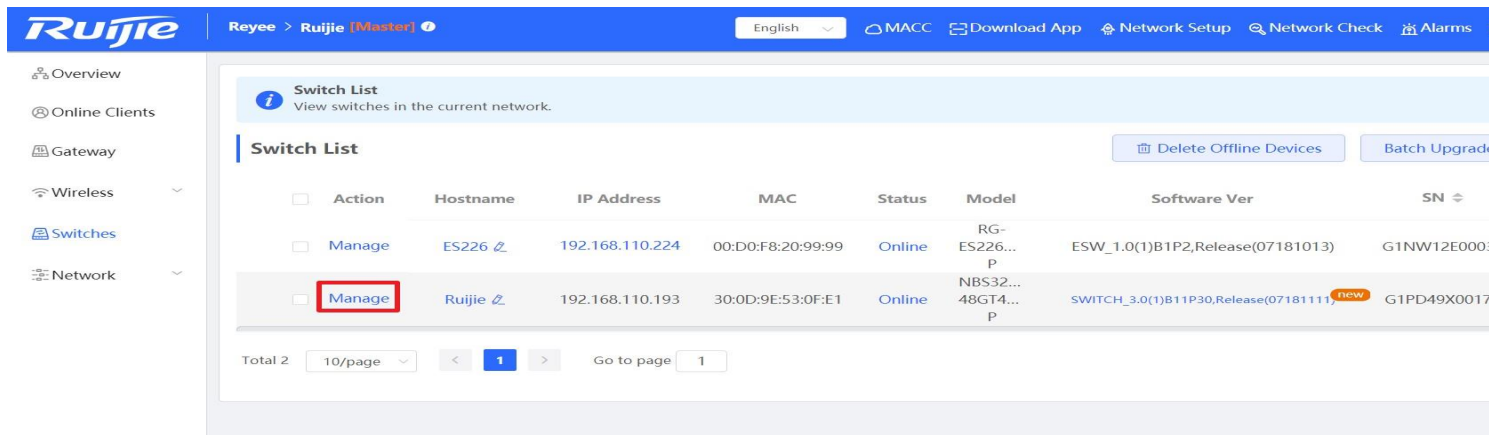
## 6 Reyee NBS Series Switch Configuration

### 6.1 VLAN Setting

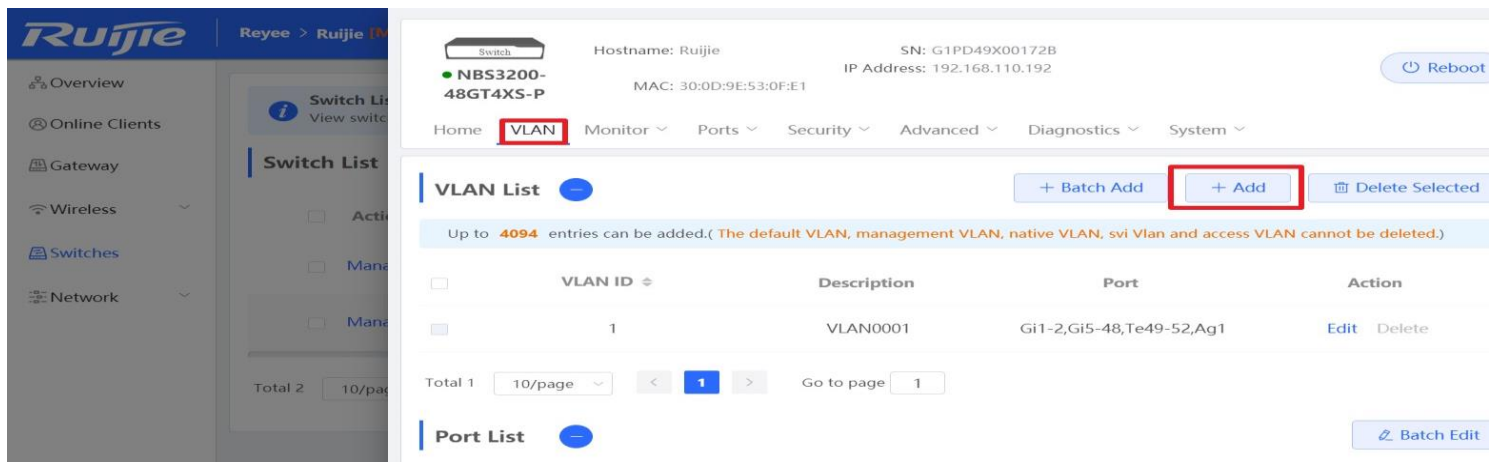
A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer. VLANs work by applying tags to network frames and handling these tags in networking systems – creating the appearance and functionality of network traffic that is physically on 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.

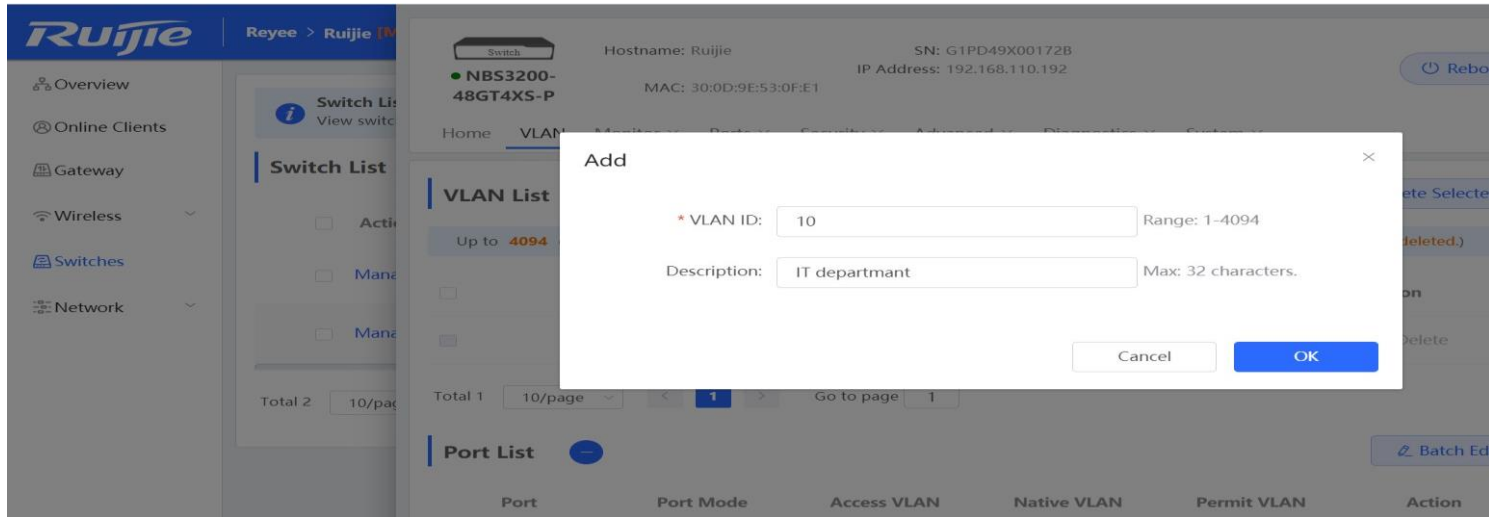
**Configuration Steps:**

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

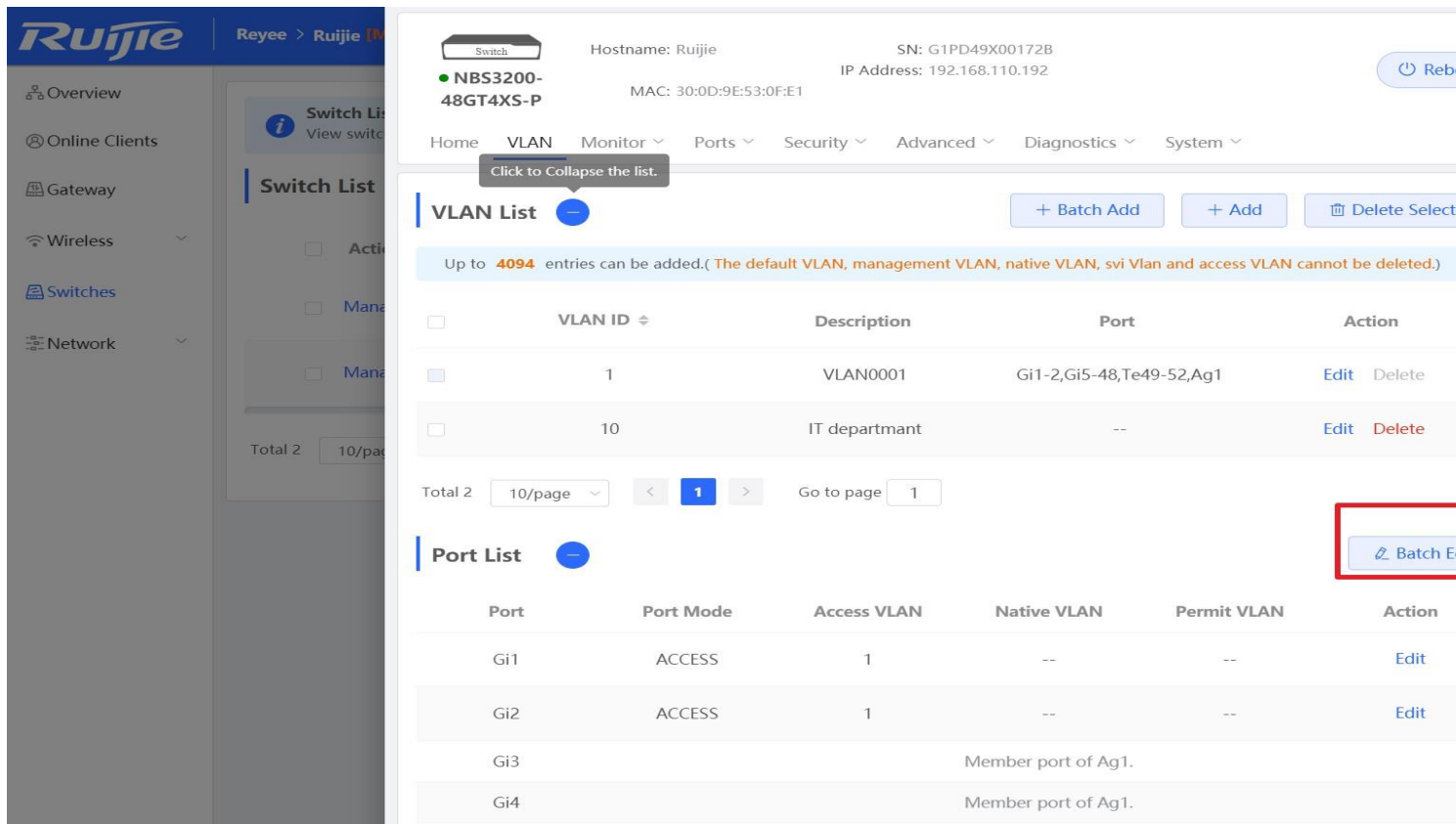


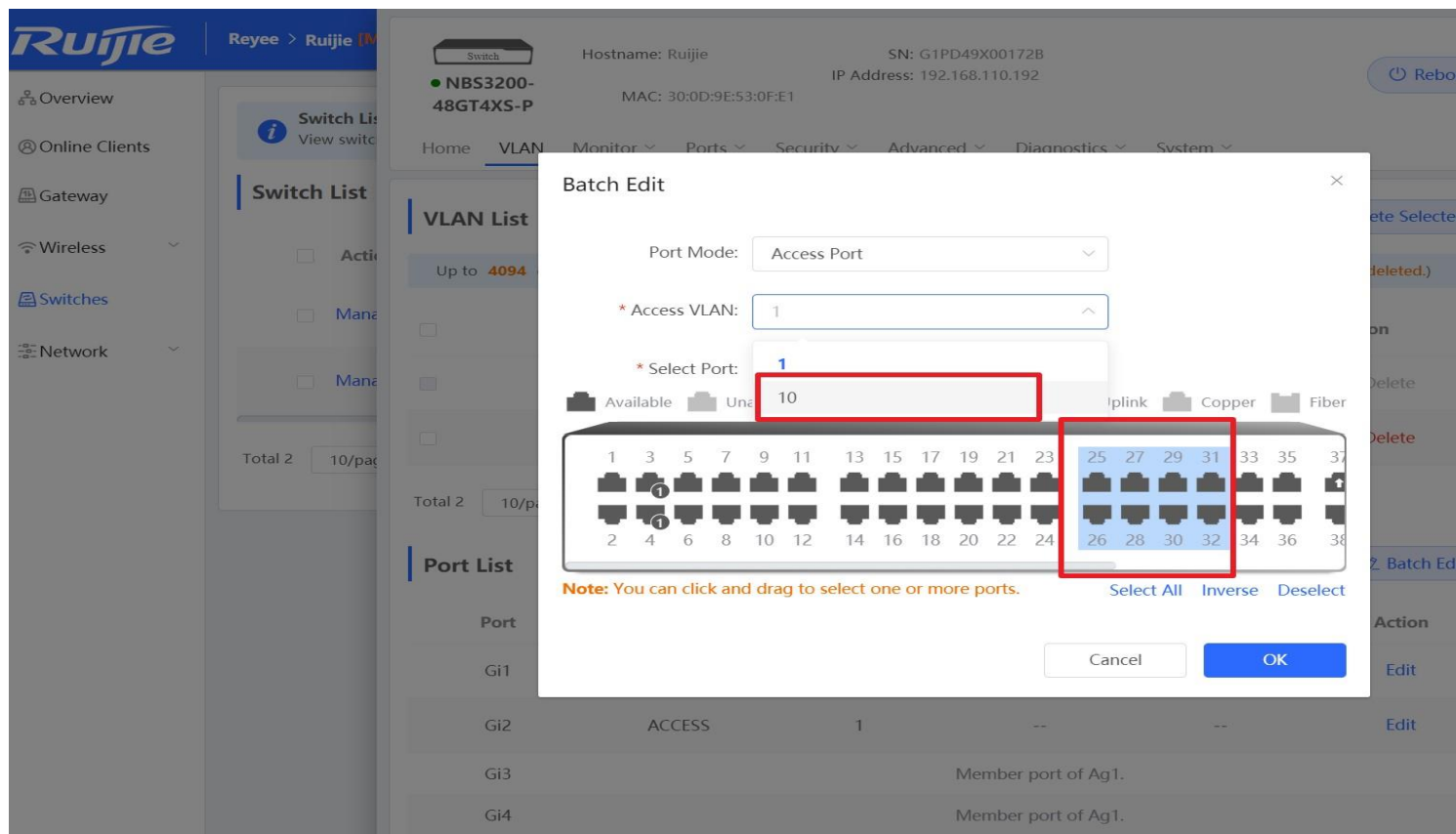
Step 2: Choose **VLAN** and Add a new VLAN





Step 3: Assign the new VLAN to ports.



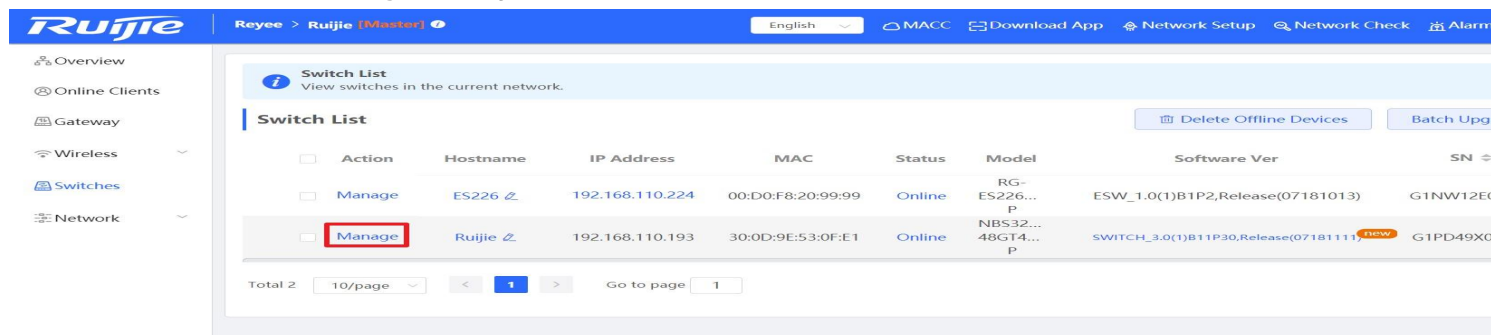


## 6.2 Access Control List (ACL)

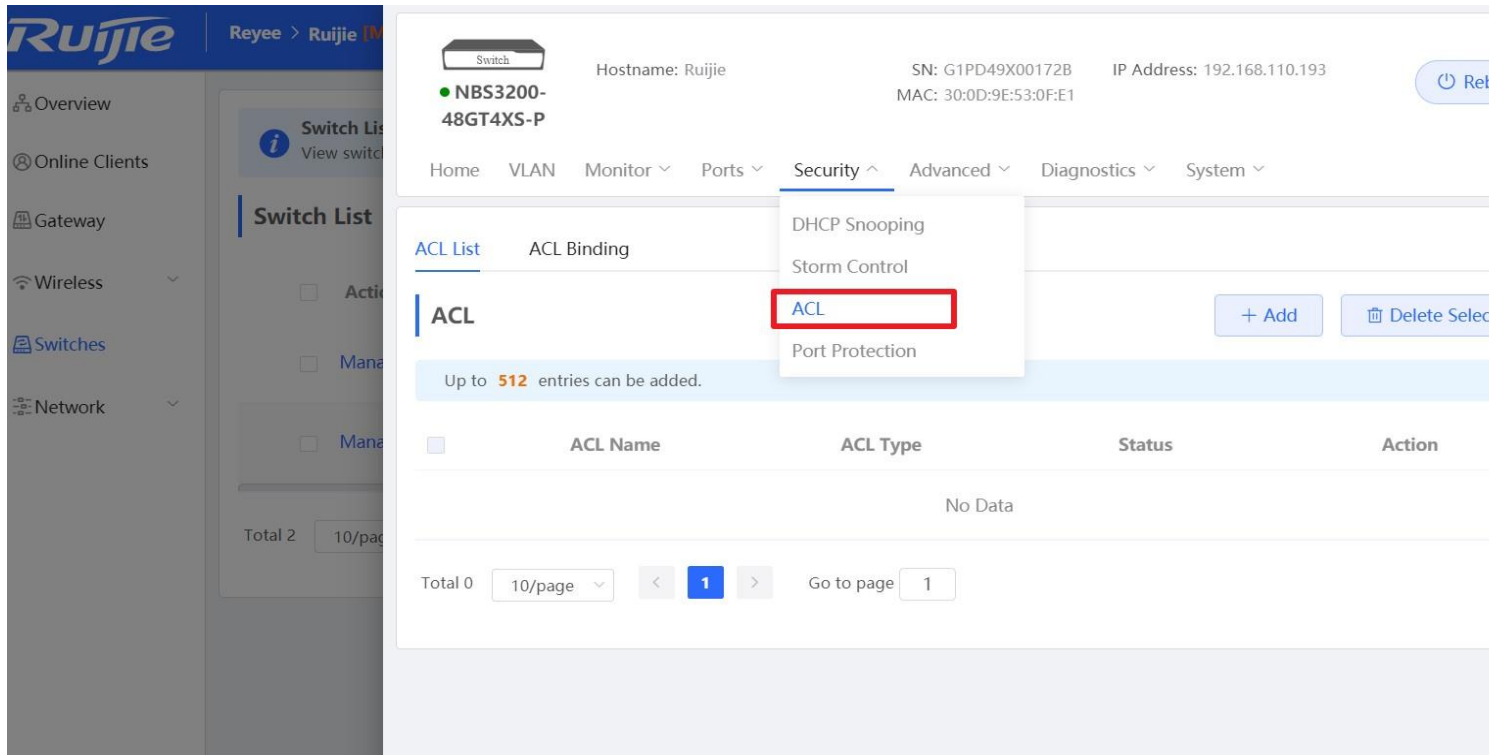
An access control list (ACL) is also referred to as firewall or packet filter in some documents. The ACL controls (permits or discards) data packets on a network device interface by defining ACEs (Access Control Entries).

### Configuration Steps:

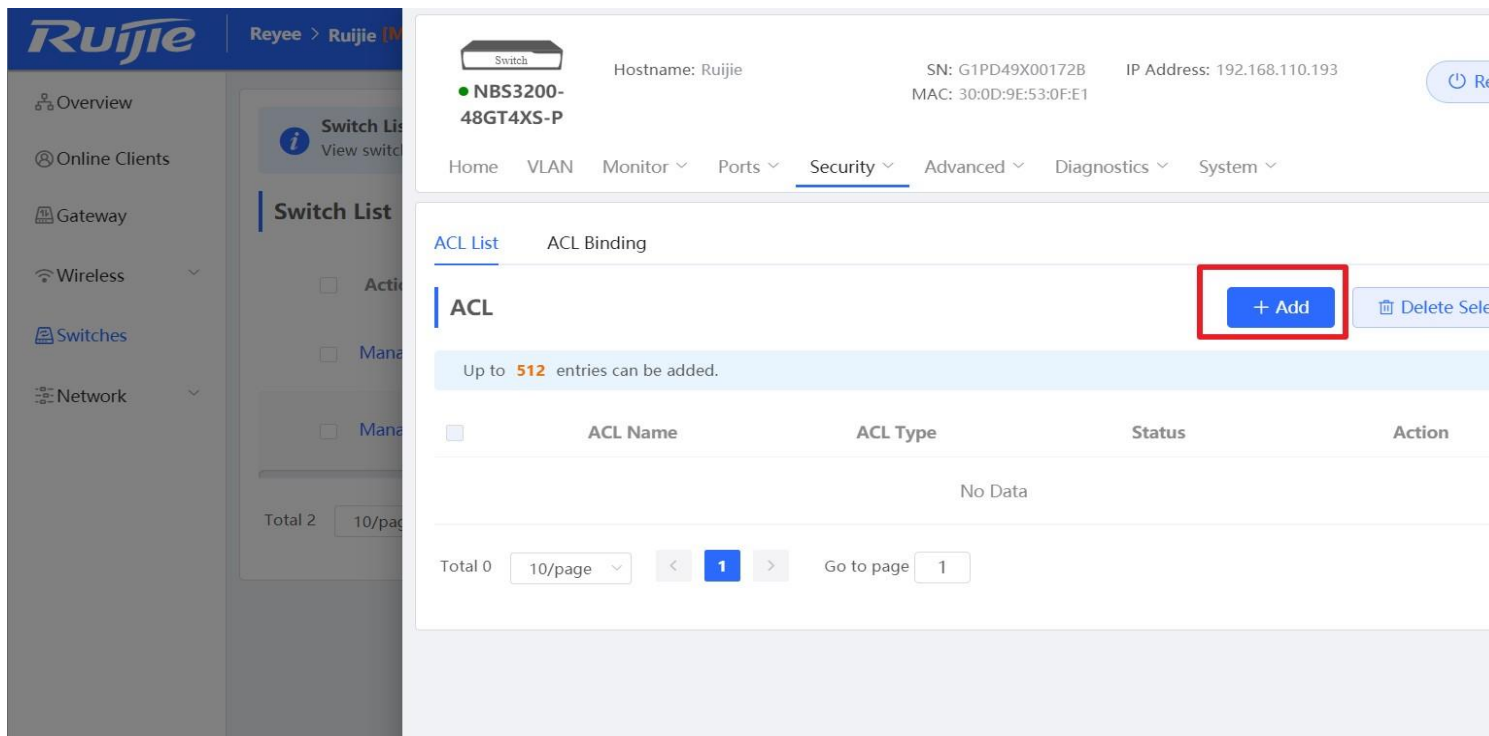
Step 1: Choose **Switches** → **Manage** to configure the switch



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

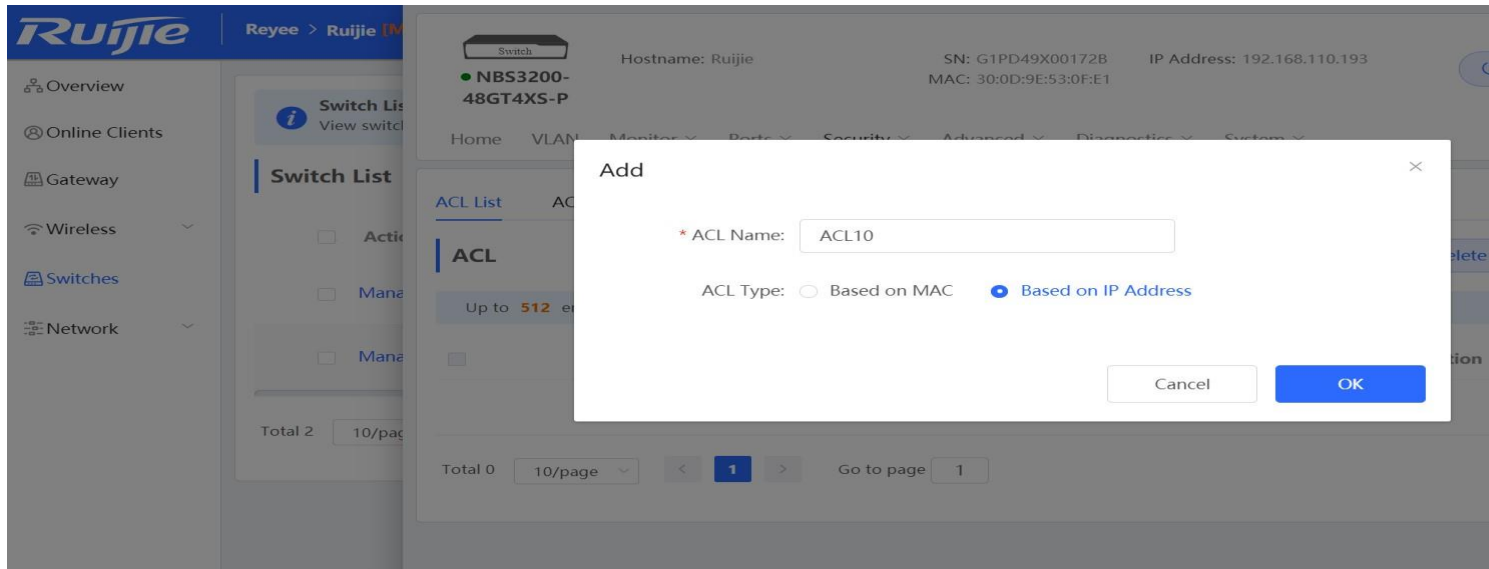


Step 3: Click the "Add" button to add an ACL

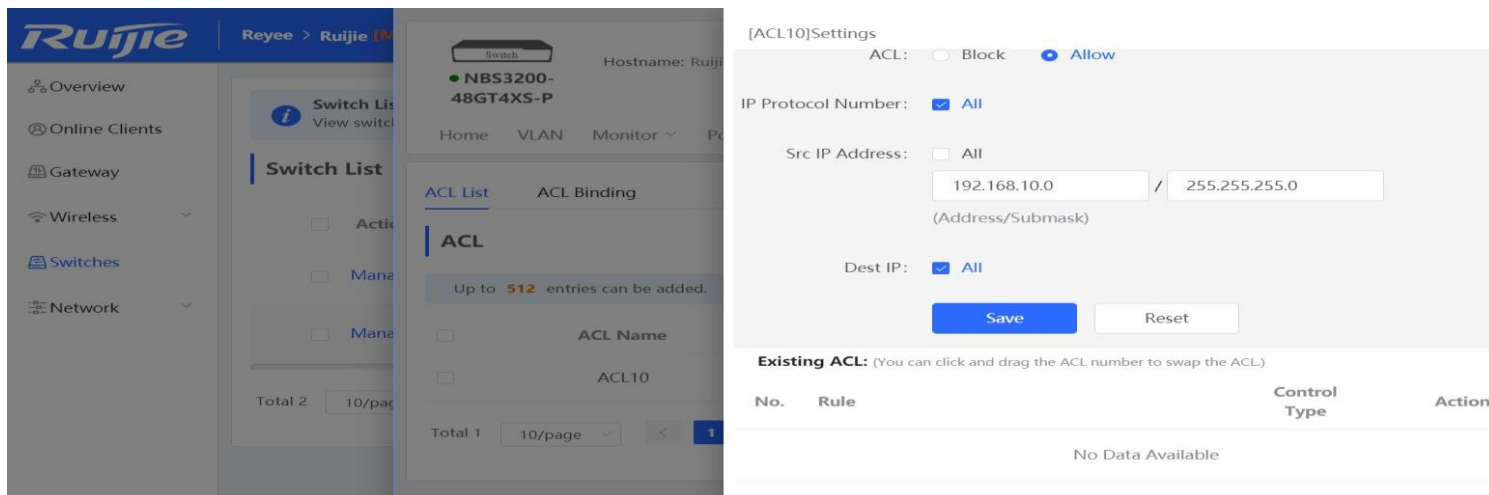
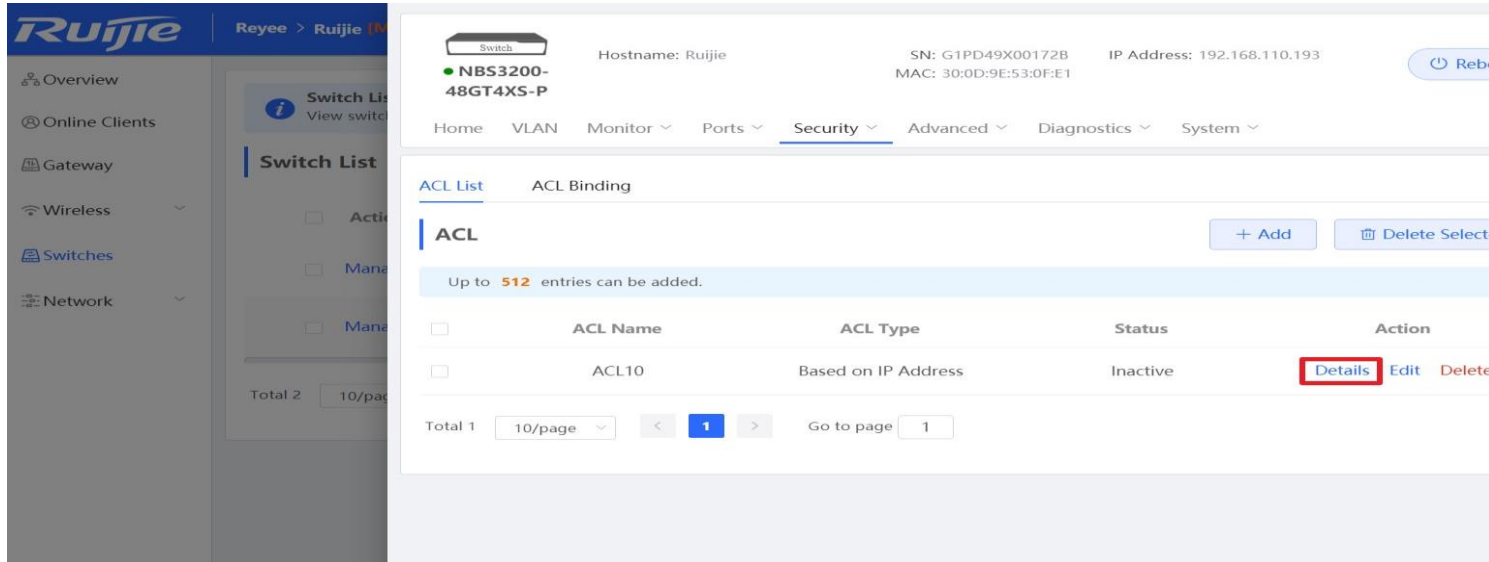


Step 4: Fill in the ACL name and type to create an ACL





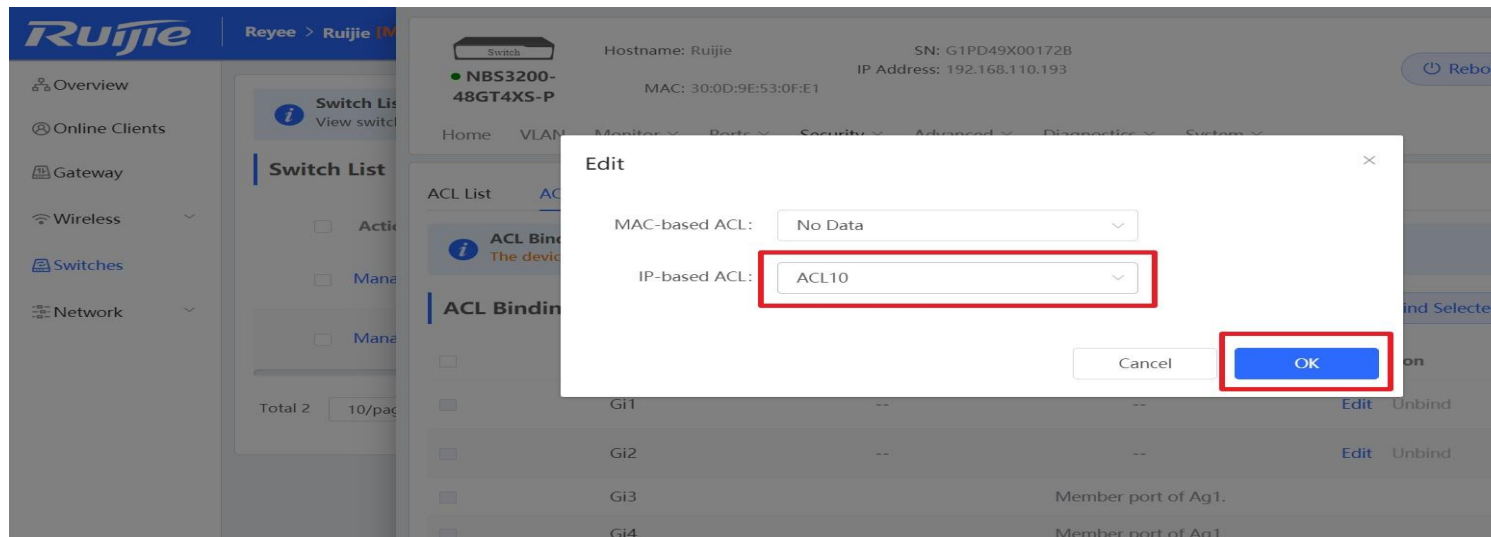
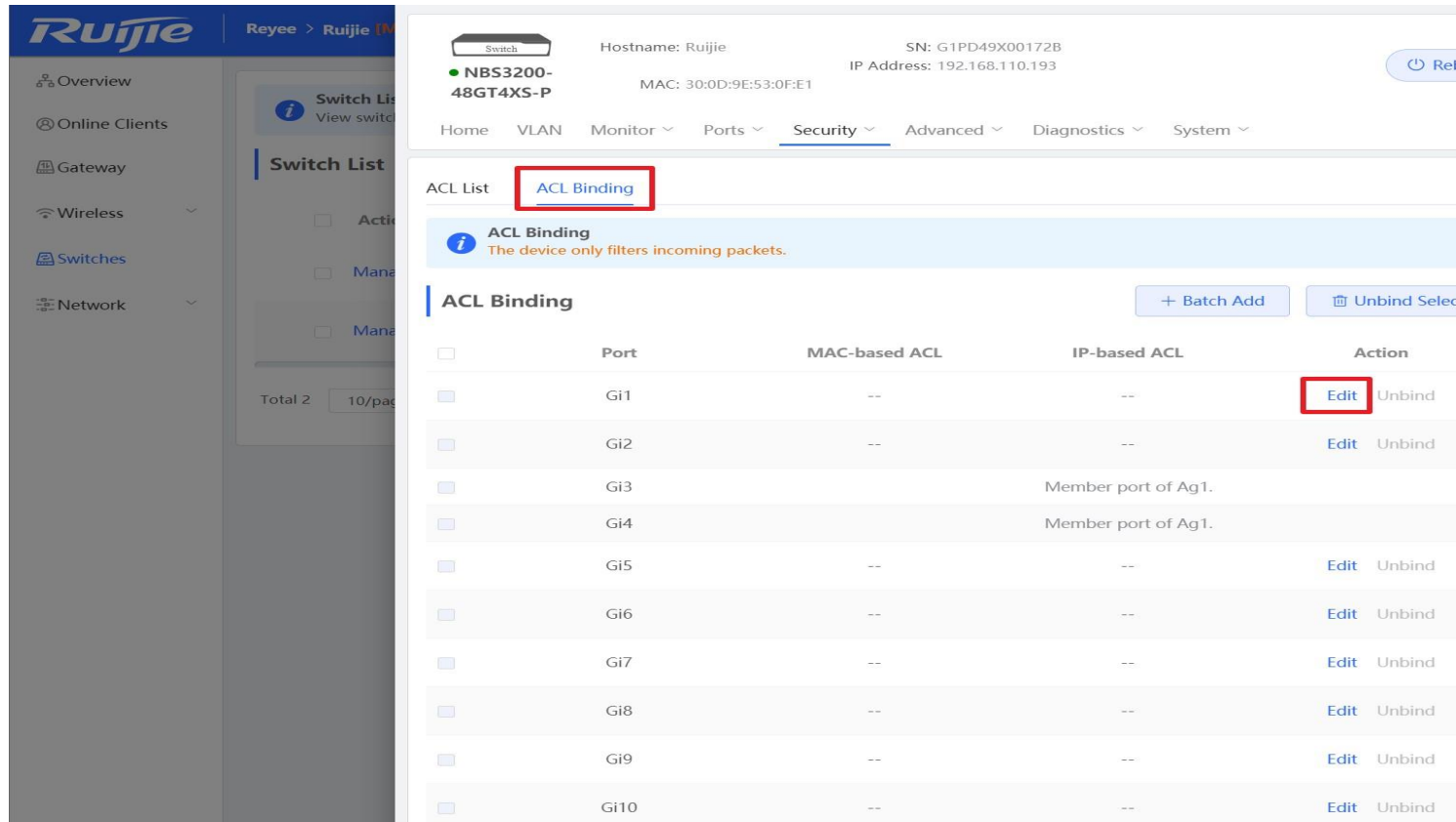
Step 4: Click "Details" to configure the ACL rule.



The screenshot shows the Ruijie web management interface. On the left is a navigation menu with items like Overview, Online Clients, Gateway, Wireless, Switches, and Network. The main content area is divided into several panels. The top panel shows a switch configuration for 'NBS3200-48GT4XS-P'. Below that is an 'ACL List' panel with a table containing one entry: 'ACL10'. To the right is the '[ACL10]Settings' panel, which includes options for ACL Name (ACL10), ACL Action (Allow selected), and checkboxes for IP Protocol Number, Src IP Address, and Dest IP, all set to 'All'. Below the settings are 'Save' and 'Reset' buttons. At the bottom right is an 'Existing ACL' table with one rule.

No.	Rule	Control Type	Action
1	[Src IP Address] 192.168.10.0/255.255.255.0 [Dest IP] All [IP Protocol Number] All	Allow	Edit Swap

Step 5: Bind the ACL to the interface.

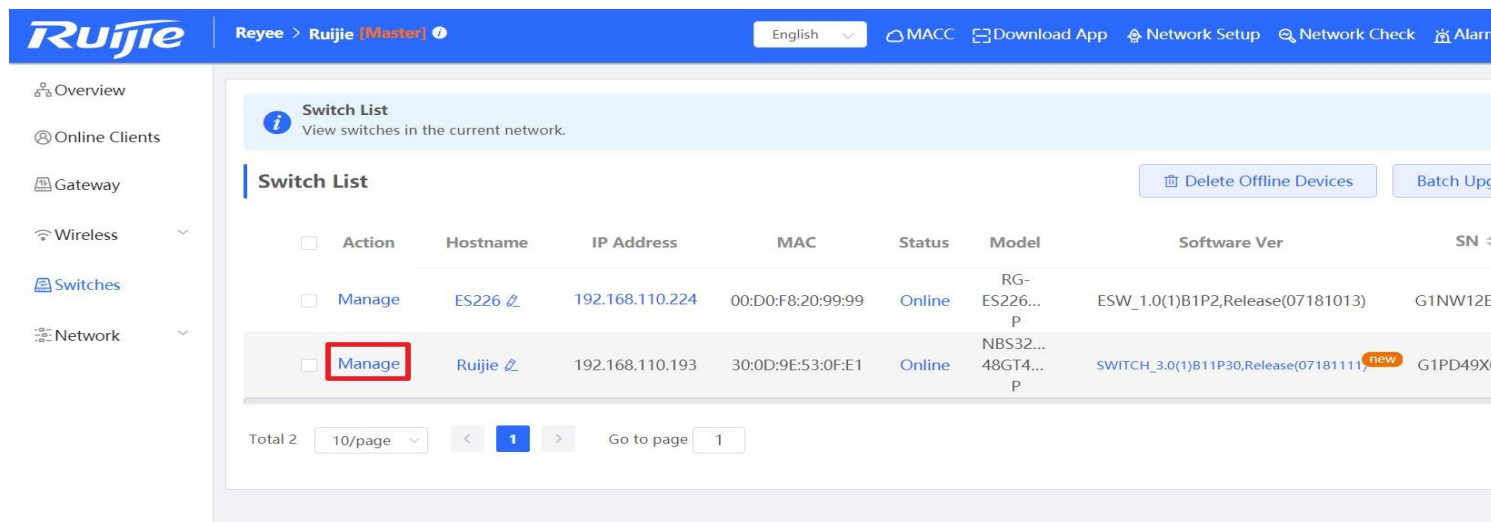


## 6.3 Port Isolation

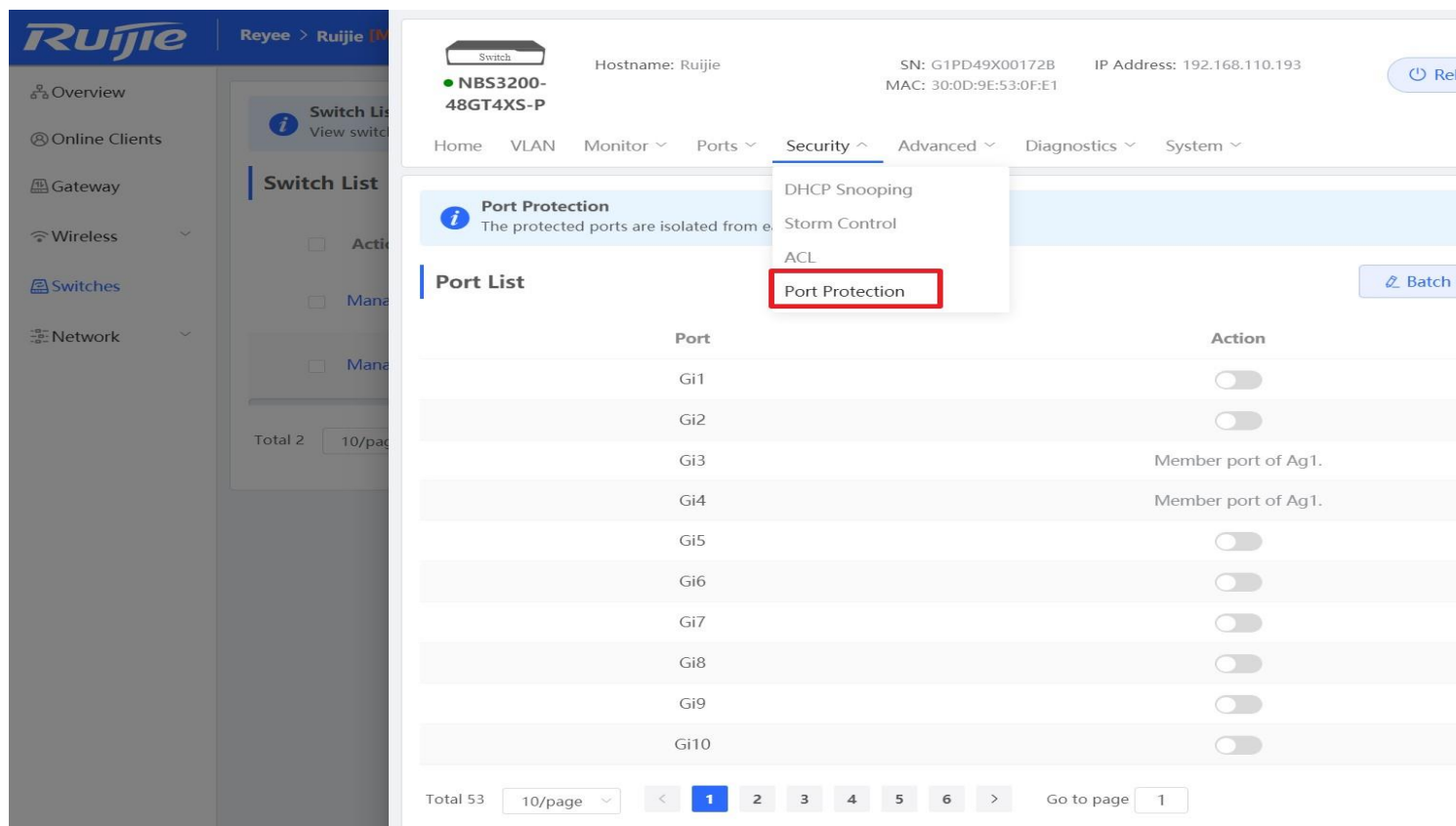
Port isolation implements layer-2 isolation of packets. After port isolation is enabled (which is disabled by default), data cannot be forwarded between isolated ports.

### Configuration Step:

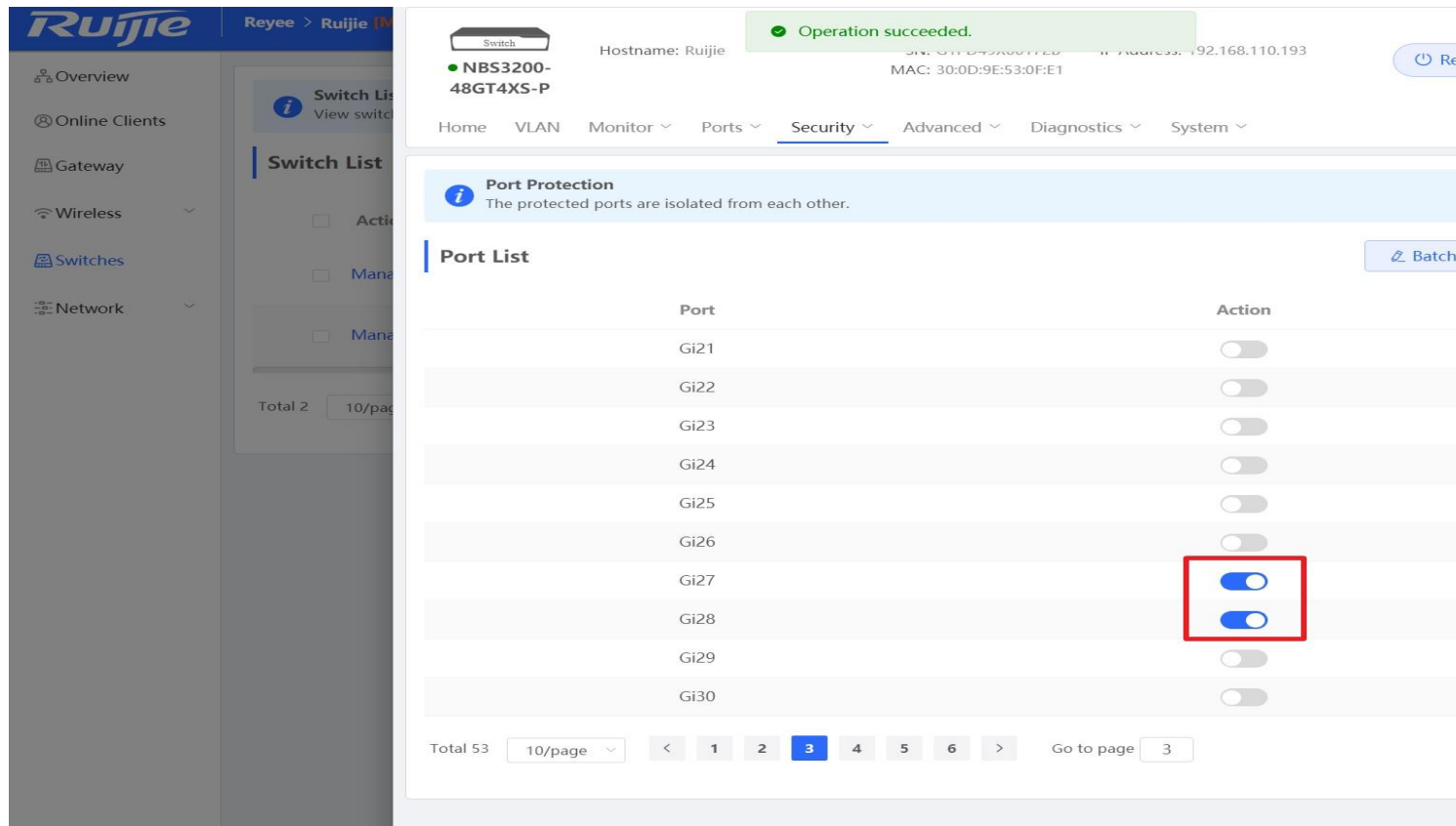
Step 1: Choose **Switches** → **Manage** to configure the switch



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



Step 3: Enable the Port Isolation on Ports.



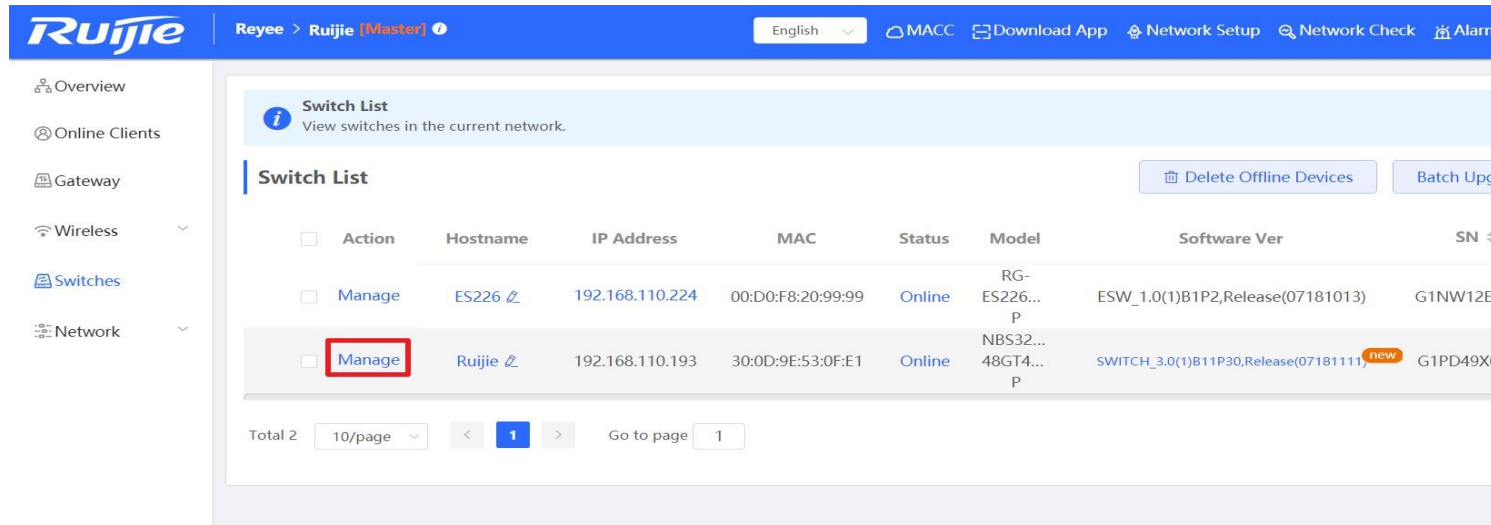
## 6.4 DHCP Snooping

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.

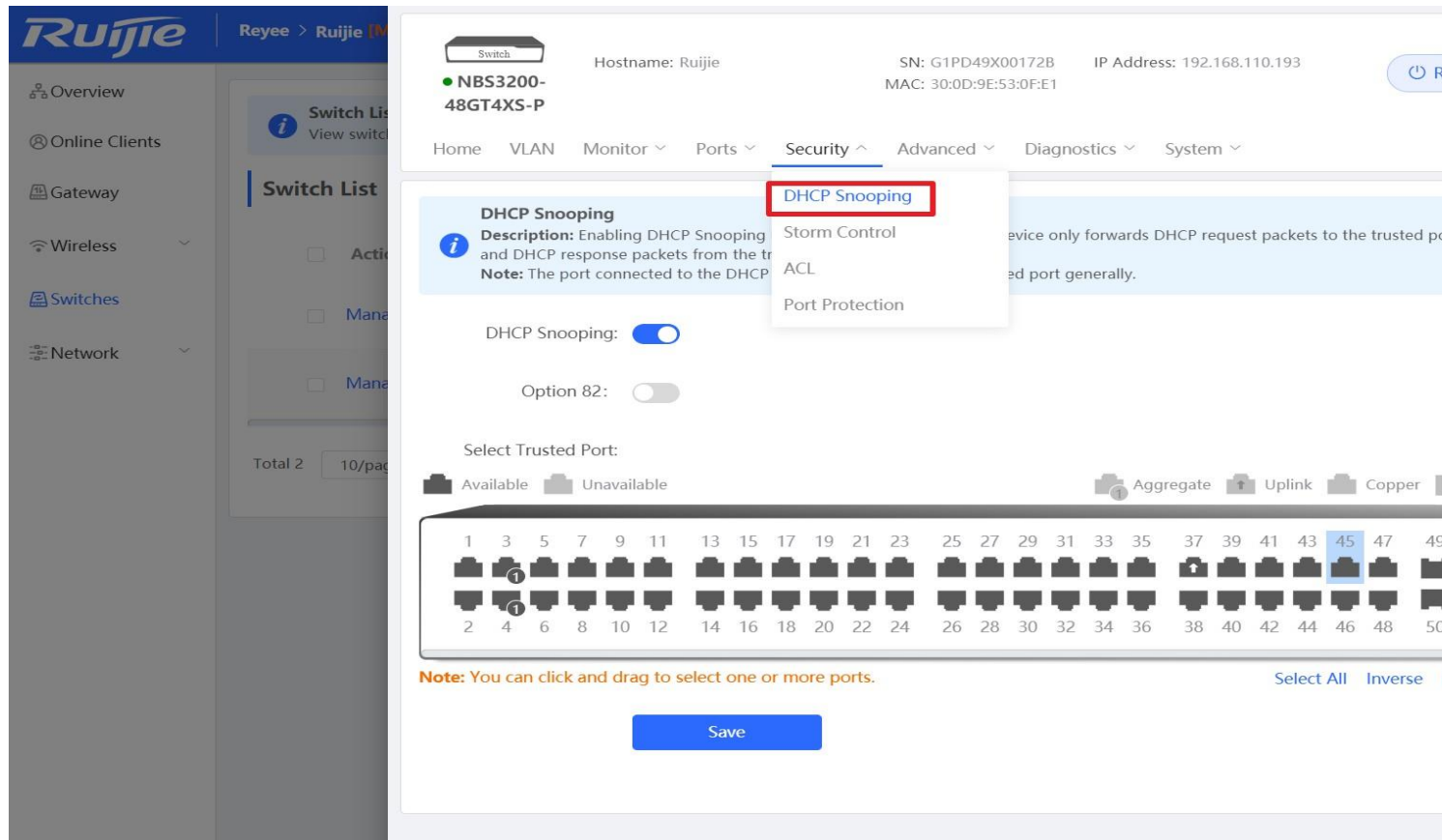
Enabling DHCP Snooping helps filter DHCP packets. Only forwards DHCP request packets to the trusted port and DHCP response packets from the trusted port. The port connected to the DHCP server is configured as the trusted port generally

### Configuration Steps

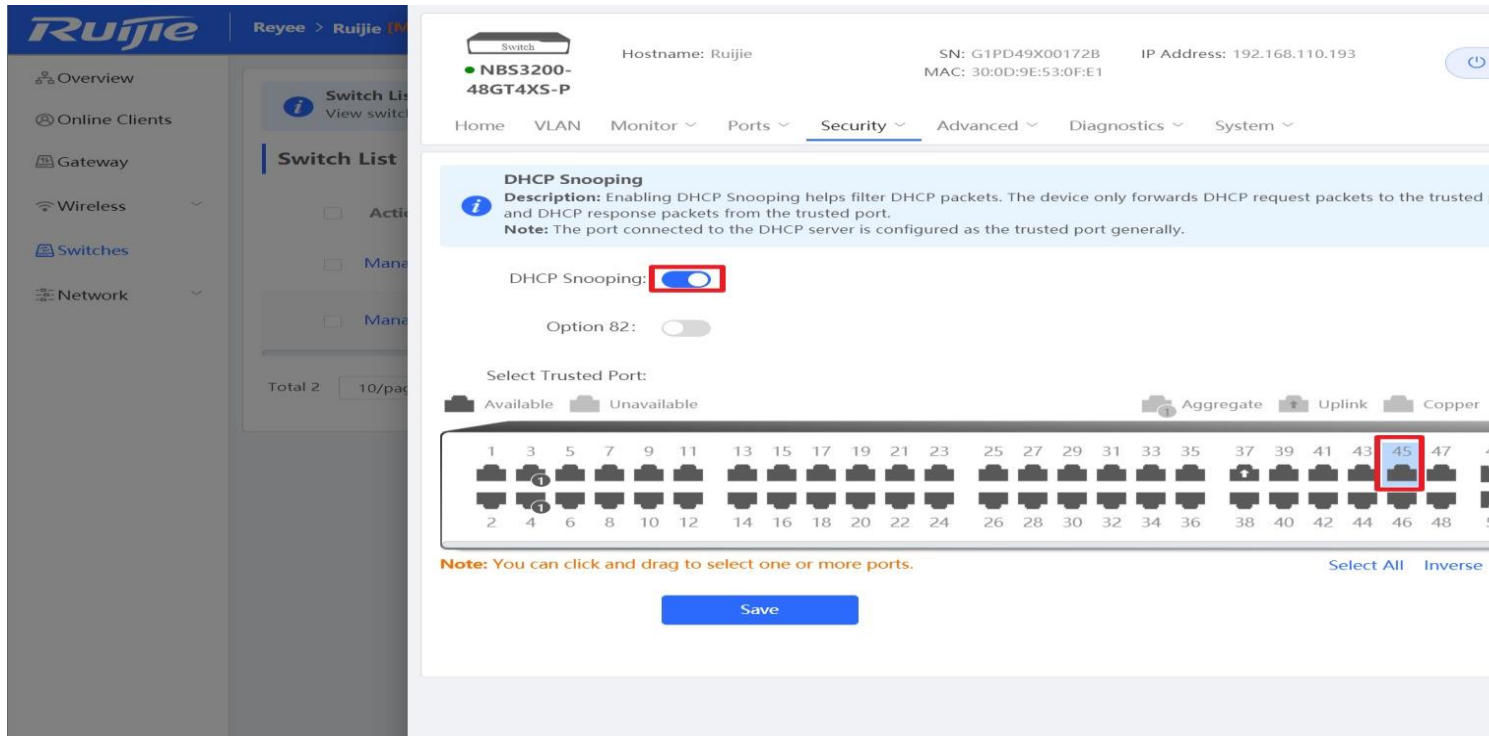
Step 1: Choose **Switches** → **Manage** to configure the switch



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

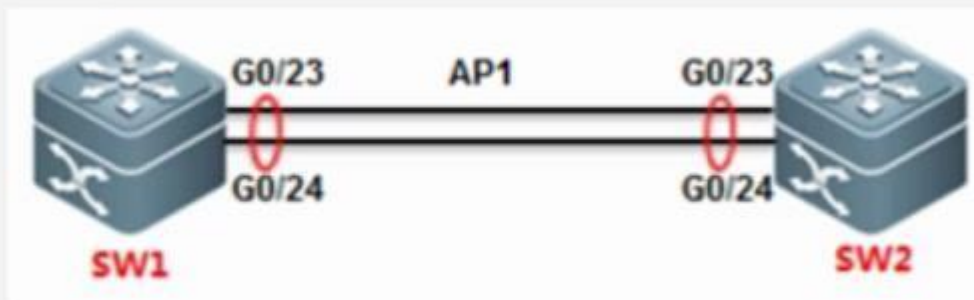


Step 3: Enable the DHCP and select the trusted port (the port connect to a DHCP server)



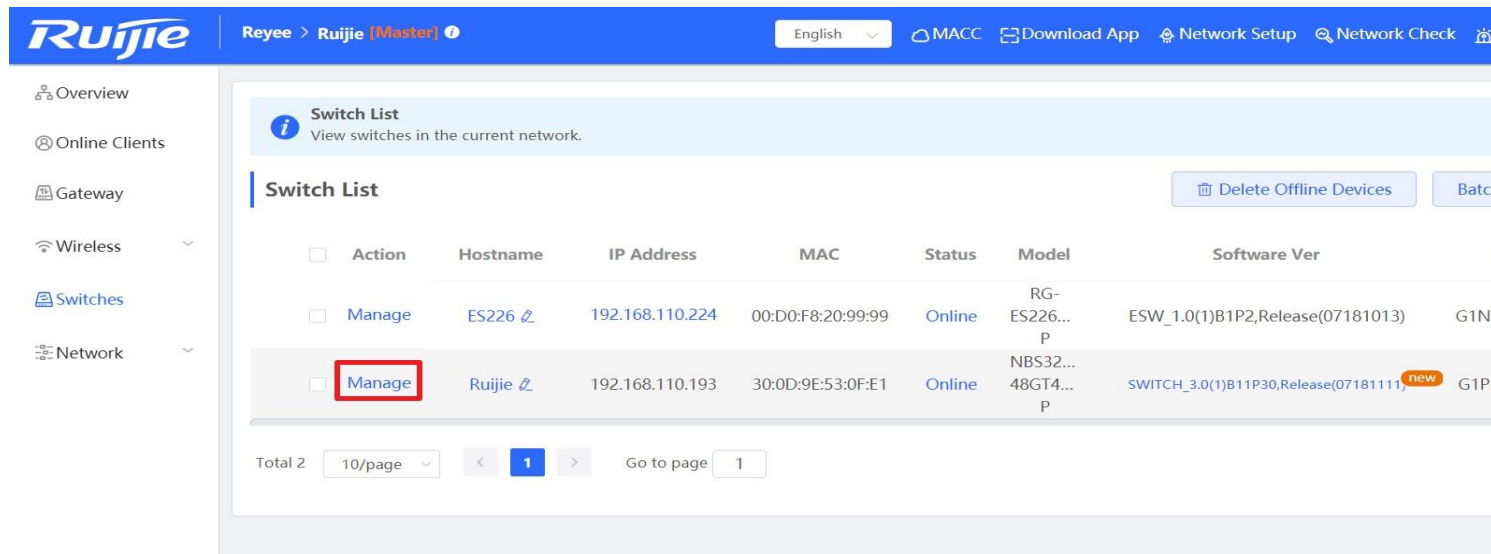
## 6.5 Link Aggregation

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.

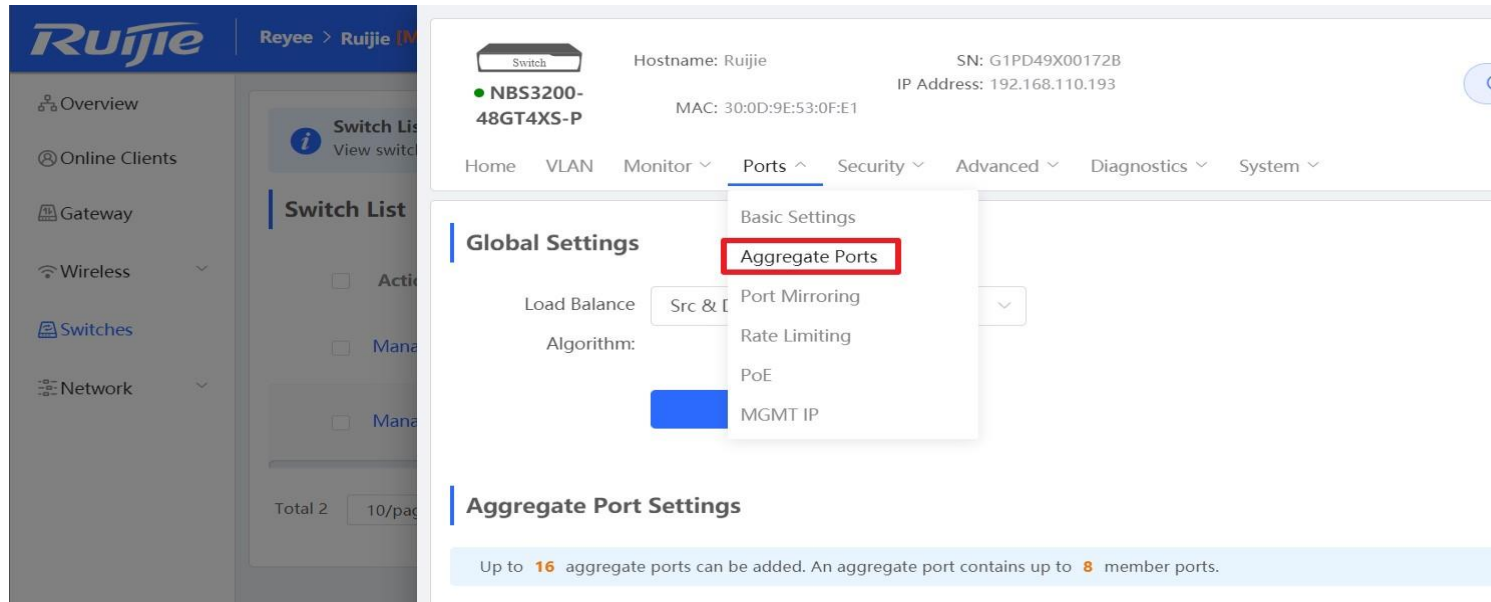


### Configuration Steps

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

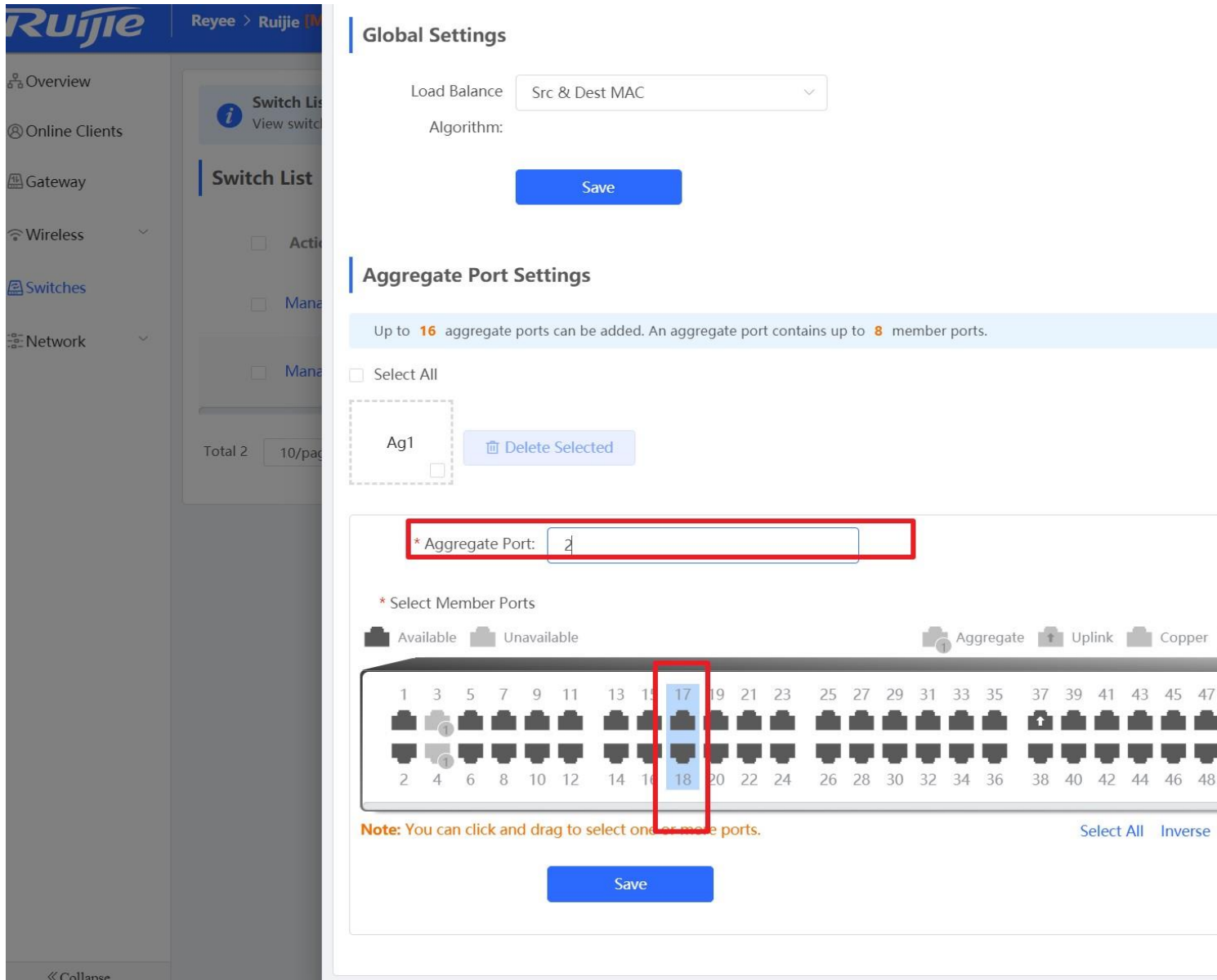


Step 2: Choose **Ports** → **Aggregate Ports** to configure the link aggregation



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





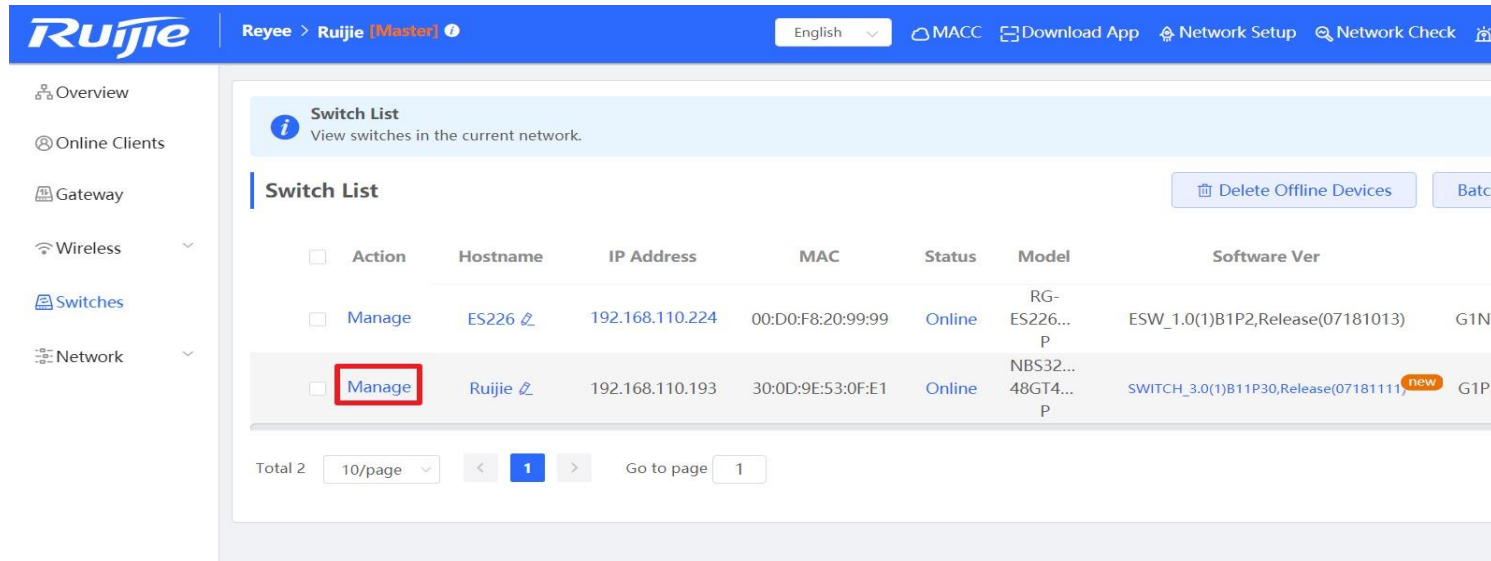
## 6.6 Storm Control

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.

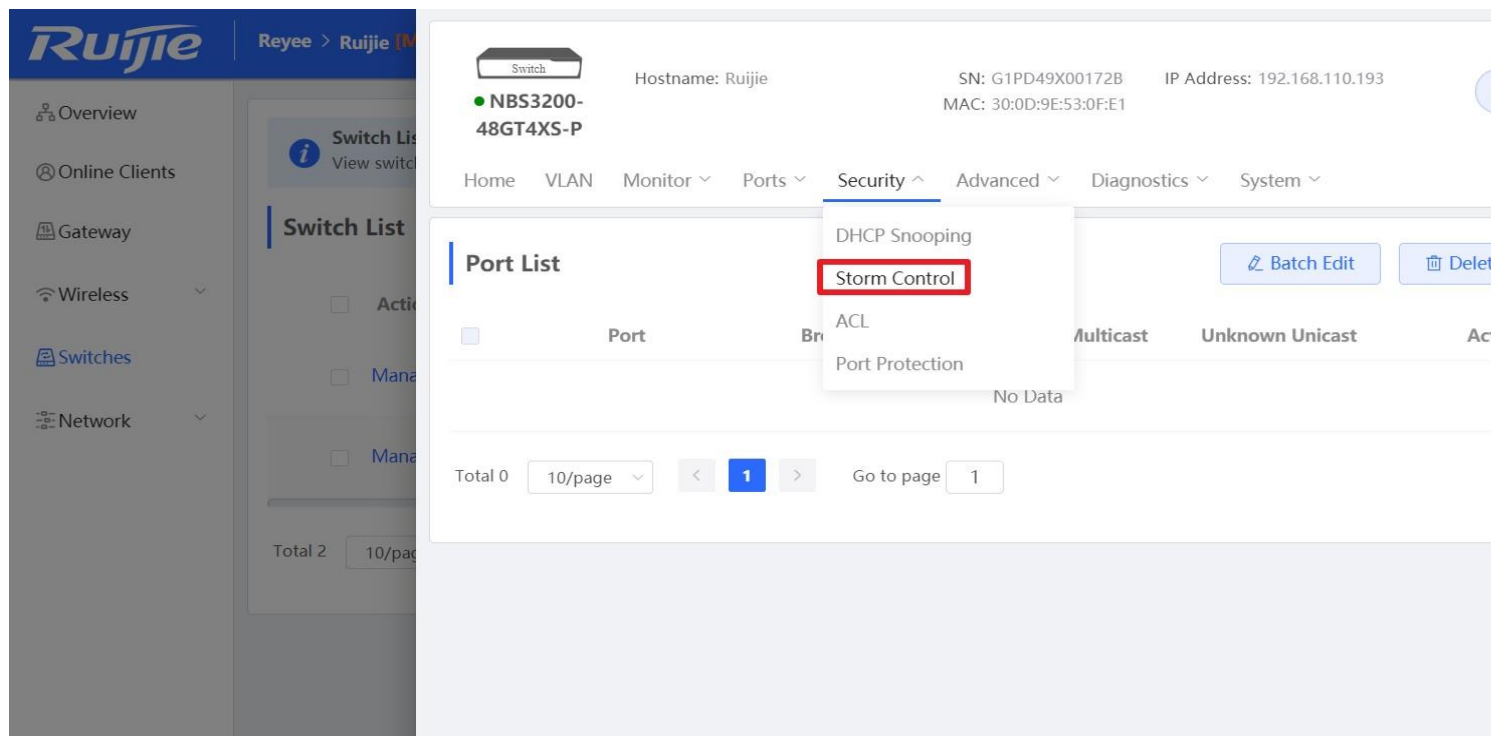
Users can perform storm control separately for the broadcast, multicast, and unknown unicast data flows. When the rate of broadcast, multicast, or unknown unicast packets received by the device port exceeds the specified rate, the number of packets allowed per second, or the number of kilobits allowed 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

The screenshot shows the Ruijie management interface for a switch. The main window displays the switch details: Hostname: Ruijie, SN: G1PD49X00172B, IP Address: 192.168.110.193, and MAC: 30:0D:9E:53:0F:E1. The model is NBS3200-48GT4XS-P. A 'Batch Edit' dialog box is open, allowing configuration by traffic volume. The dialog includes fields for Broadcast (10000), Unknown Multicast (1000), and Unknown Unicast (1000), all with a kbps range of 16-1000000. Below these fields, there are filters for port status (Available, Unavailable) and type (Aggregate, Uplink, Copper, Fiber). A grid of 48 ports is shown, with port 15 selected. A note at the bottom states: 'Note: You can click and drag to select one or more ports.' The dialog has 'Cancel' and 'OK' buttons.

**Batch Edit**

Config Type:  By Packet Count  By Traffic Volume

Broadcast:  kbps Range: 16-1000000

Unknown Multicast:  kbps Range: 16-1000000

Unknown Unicast:  kbps Range: 16-1000000

\* Select Port:

Available  Unavailable  Aggregate  Uplink  Copper  Fiber

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38

Note: You can click and drag to select one or more ports. [Select All](#) [Inverse](#) [Deselect](#)

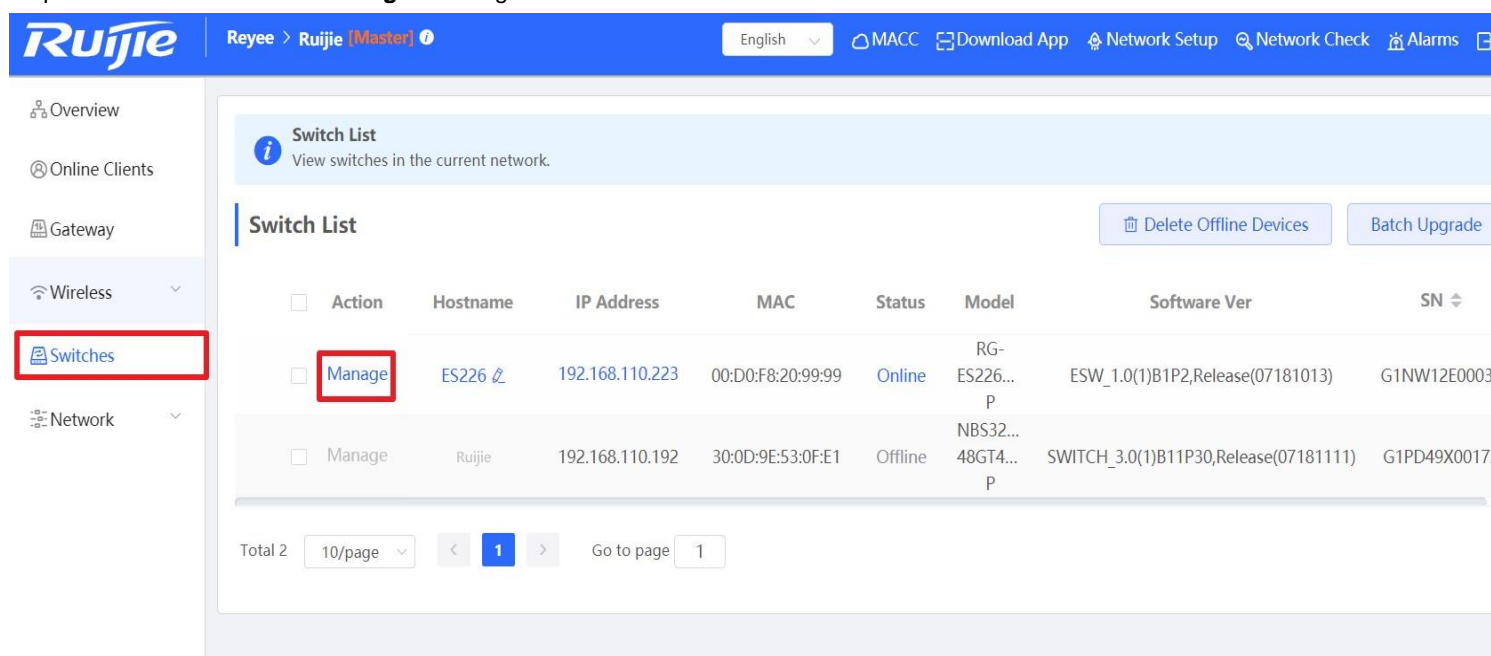
## 7 Reyee ES Series Switch Configuration

### 7.1 VLAN Setting

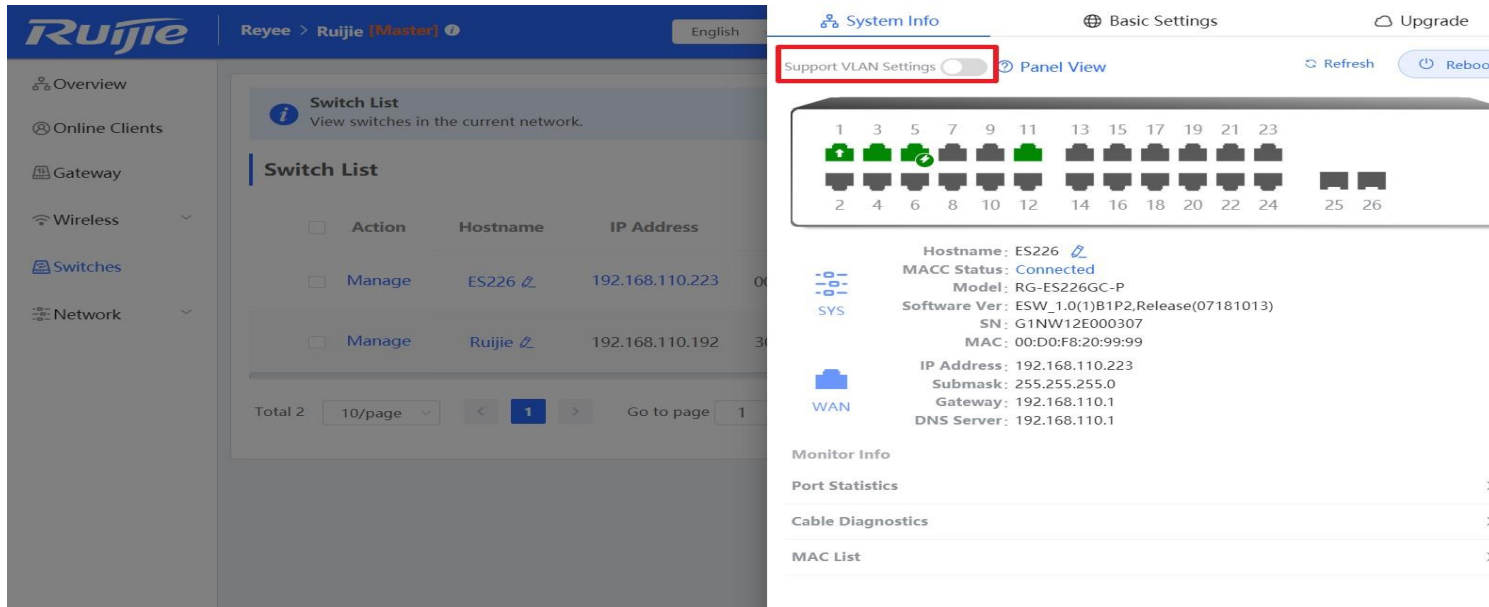
A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer. VLANs work by applying tags to network frames and handling these tags in networking systems – creating the appearance and functionality of network traffic that is physically on 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:

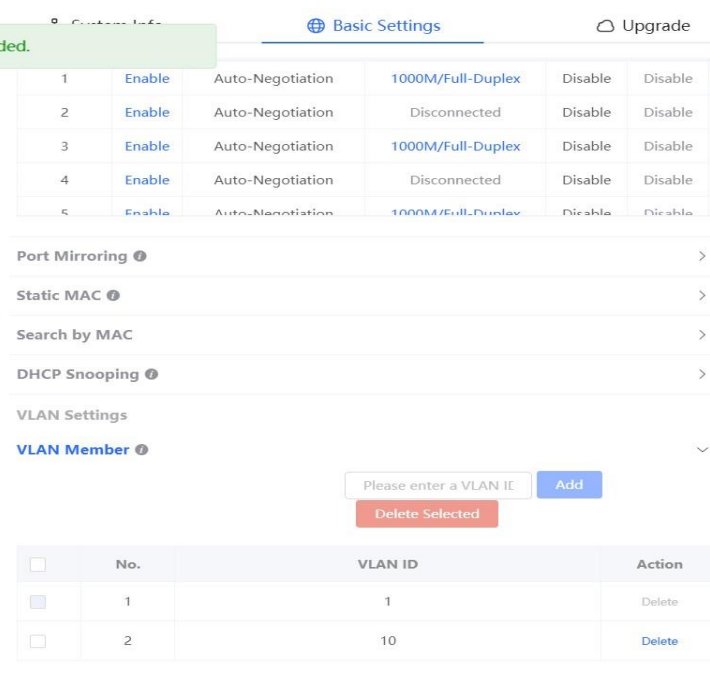
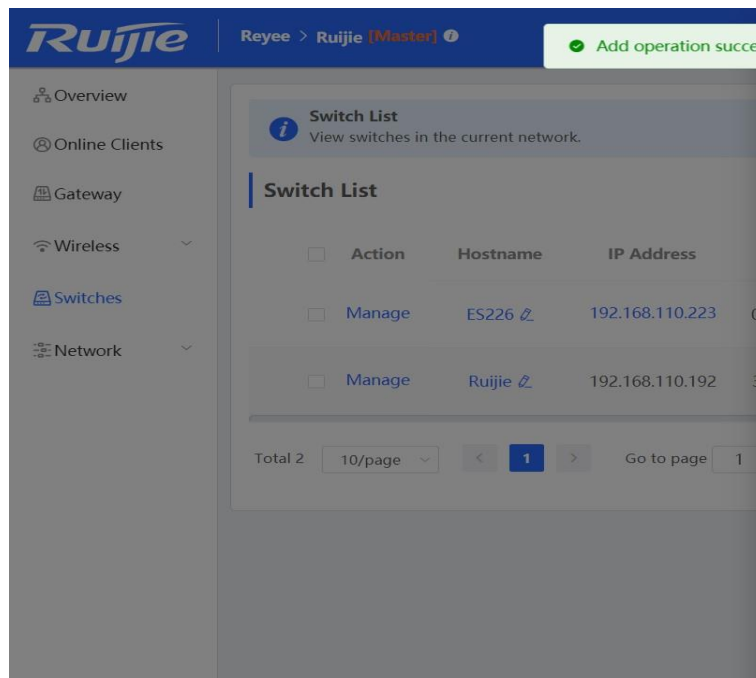
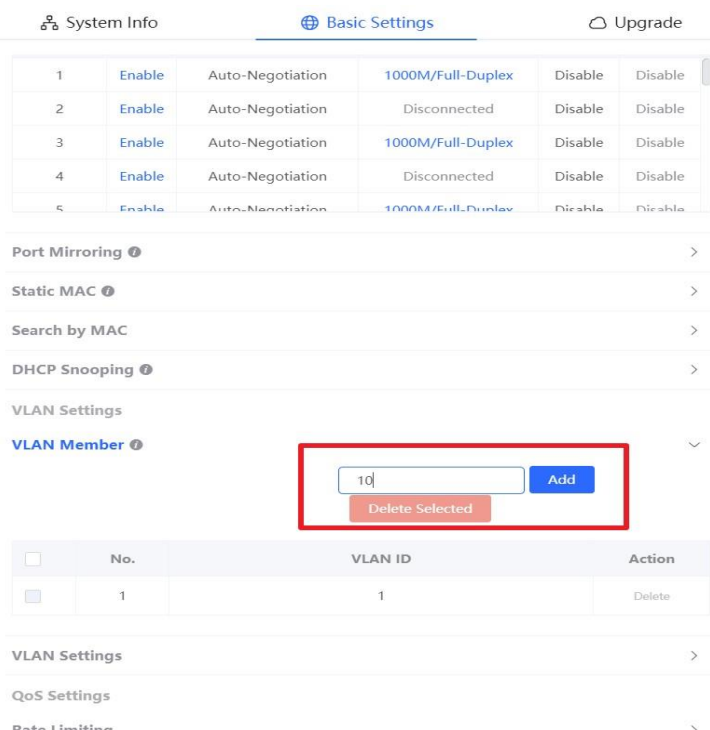
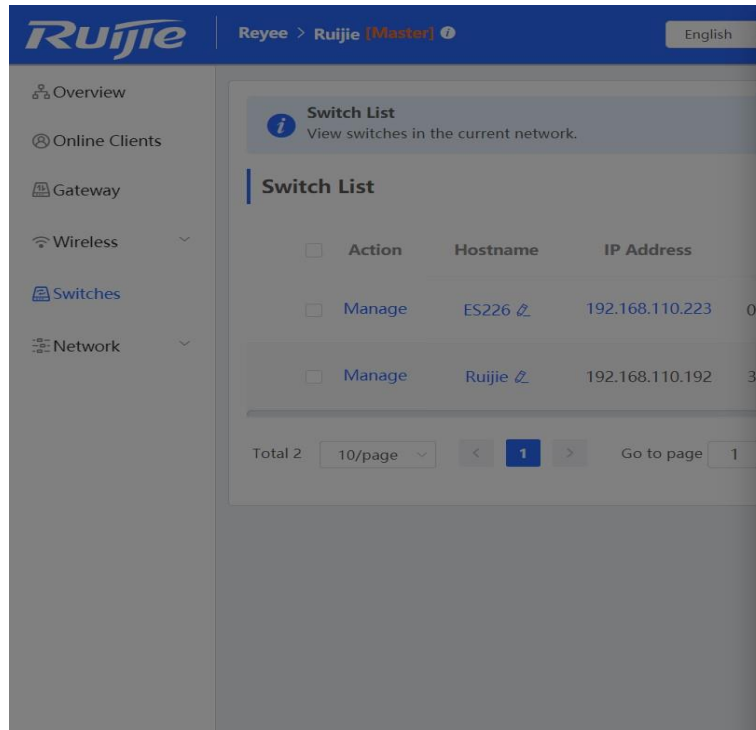
Step 1: Choose **Switches** → **Manage** to configure the switch



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



Step 3: Add a VLAN member



Step 3: Assign the new VLAN member to ports.

The screenshot displays the Ruijie management interface. On the left, the 'Switch List' table shows two switches:

Action	Hostname	IP Address
Manage	ES226	192.168.110.223
Manage	Ruijie	192.168.110.192

The right panel shows the 'VLAN Settings' configuration for a switch. The 'Port' field is set to Port 18, 19, 21, and 20. The 'Native' field is set to VLAN 10. The 'Type' is set to Access. Below the form is a table summarizing the configuration:

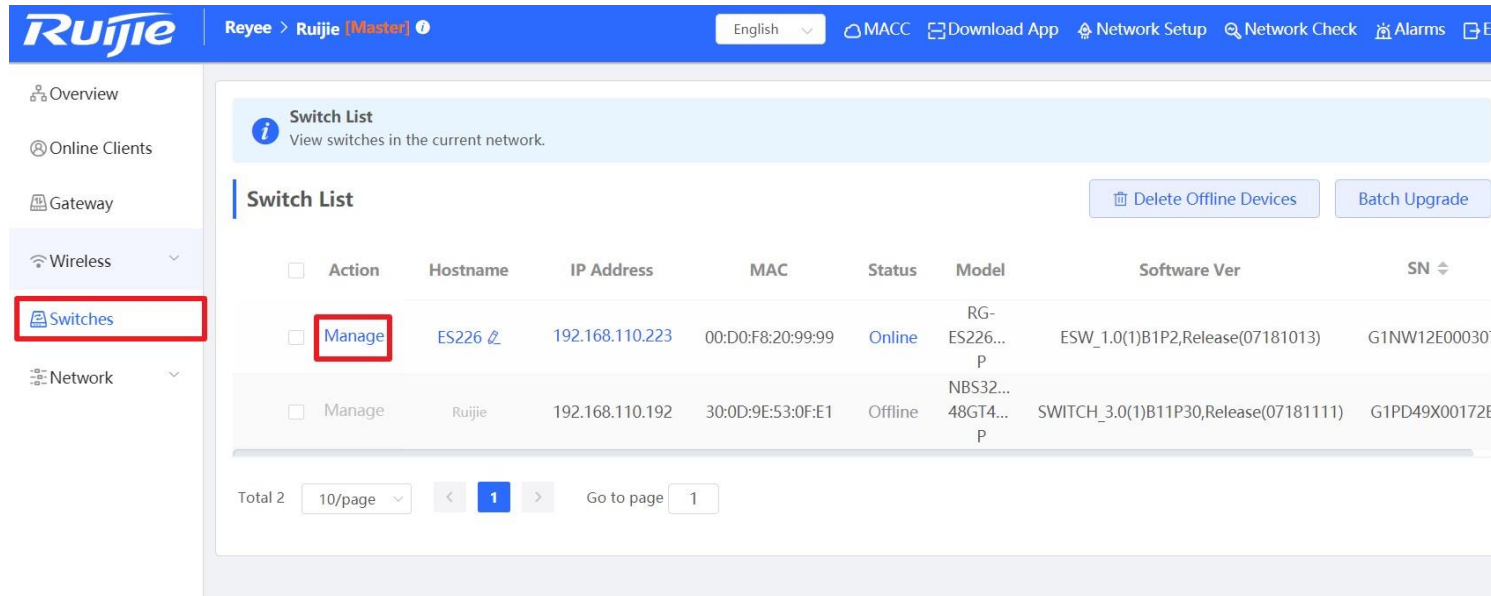
Port	VLAN Type	Permit VLAN	Native Vlan
1	Access	1	1
2	Access	1	1
3	Access	1	1
4	Access	1	1
5	Access	1	1

## 7.2 Port Isolation

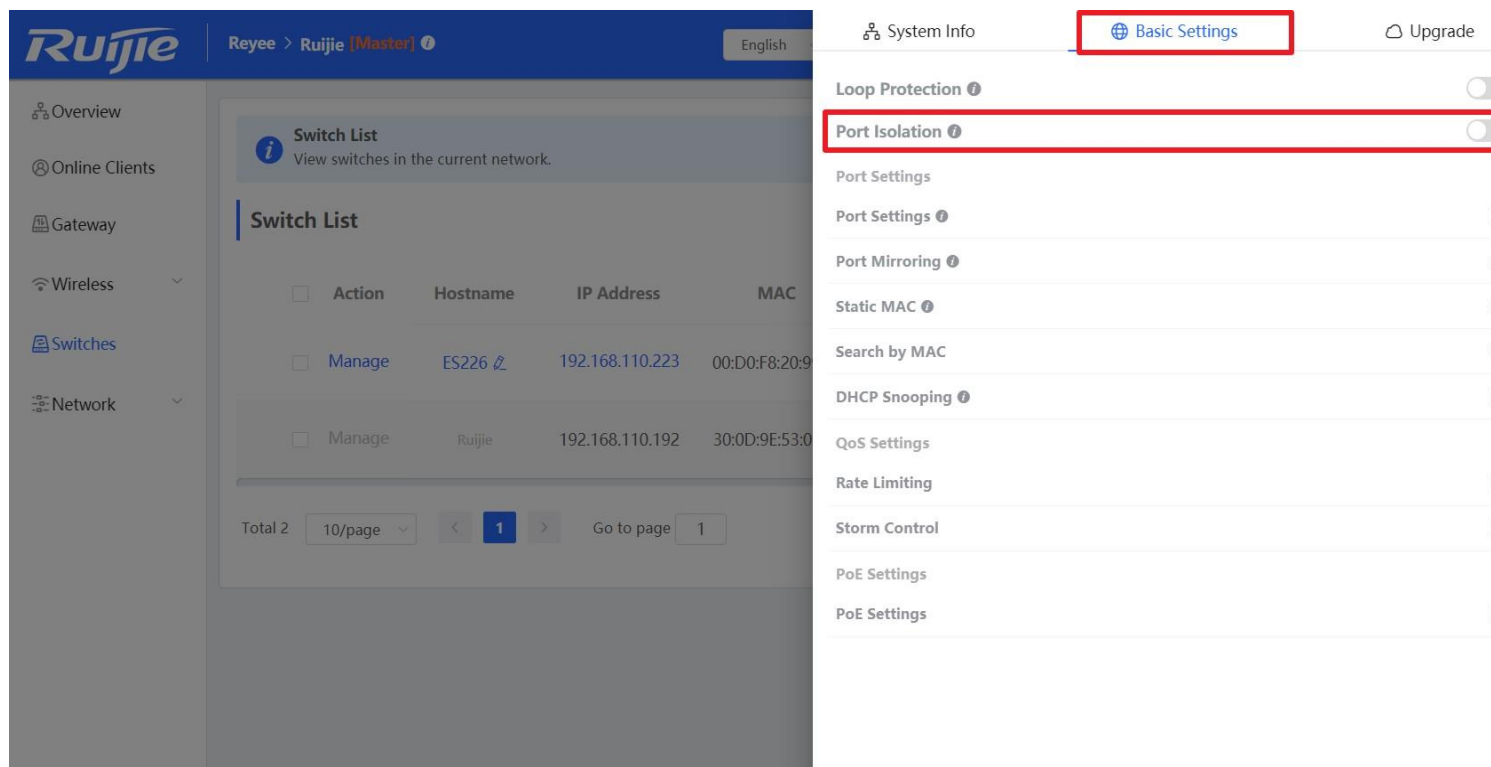
Port isolation implements layer-2 isolation of packets. After port isolation is enabled (which is disabled by default), data can be forwarded only between uplink ports and downlink ports, and **downlink ports cannot forward packets to each other**.

### 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,

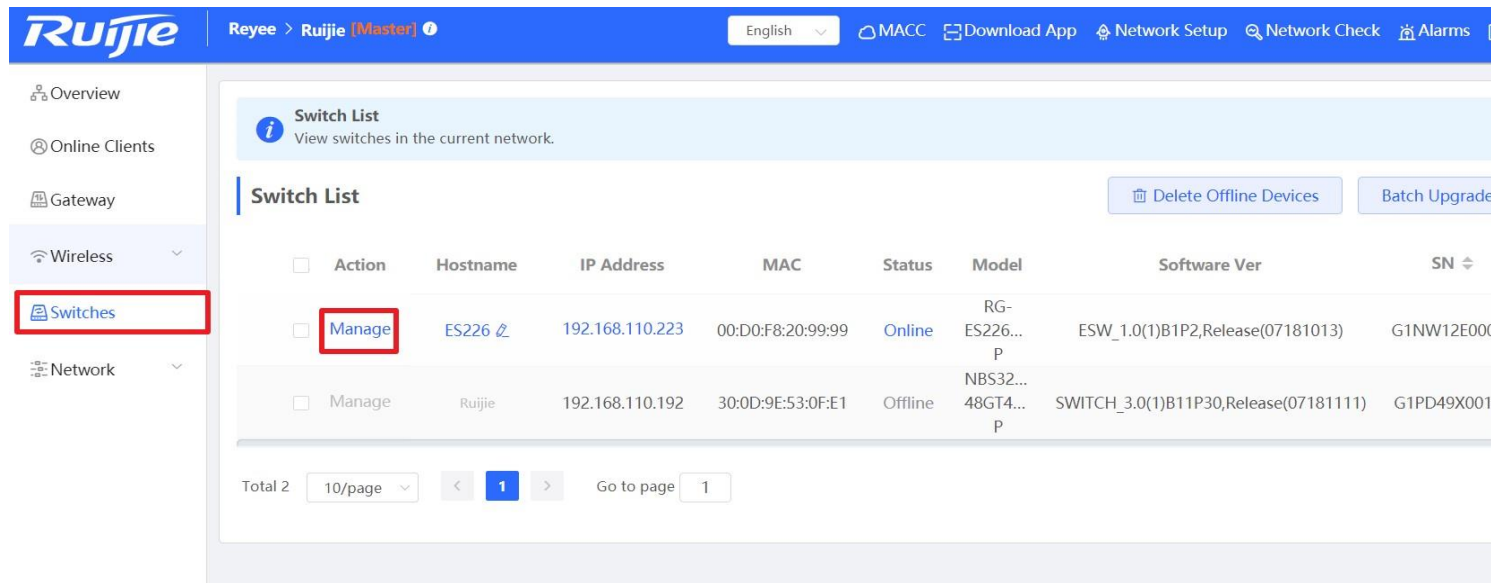


making network application more complex. In dynamic DHCP binding mode, the device records how legal users obtain IP addresses during the course of DHCP Snooping for security purpose.

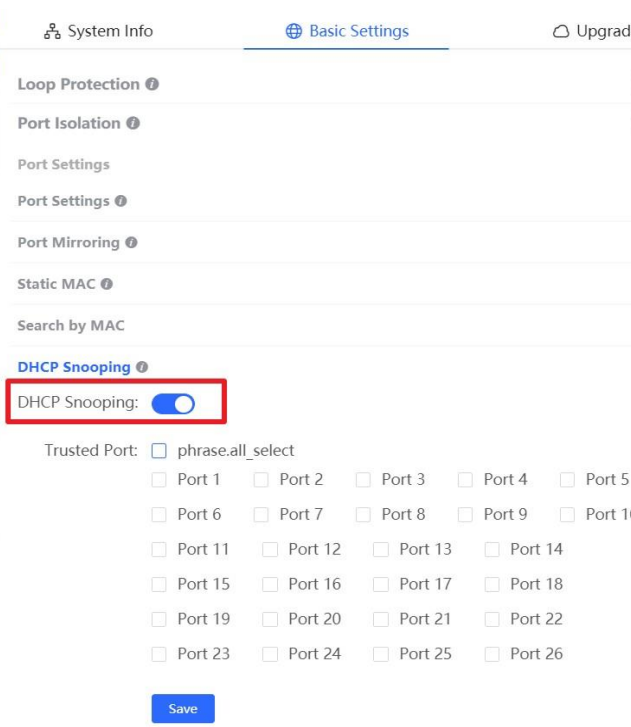
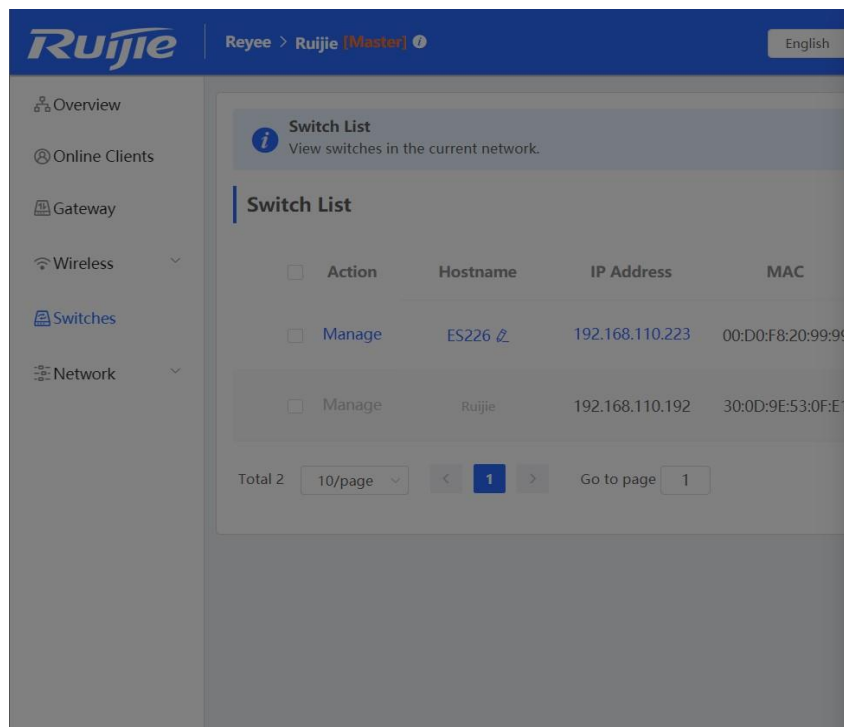
Enabling DHCP Snooping helps filter DHCP packets. Only forwards DHCP request packets to the trusted port and DHCP response packets from the trusted port. The port connected to the DHCP server is configured as the trusted port generally

### Configuration Steps

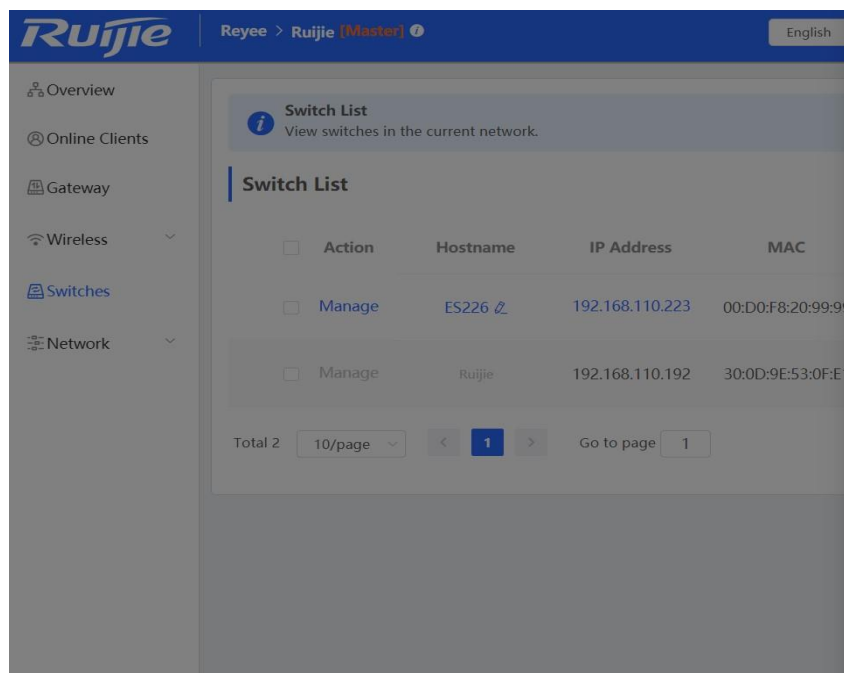
Step 1: Choose **Switches** → **Manage** to configure the switch



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



Step 3: Select the trusted port and save the configuration

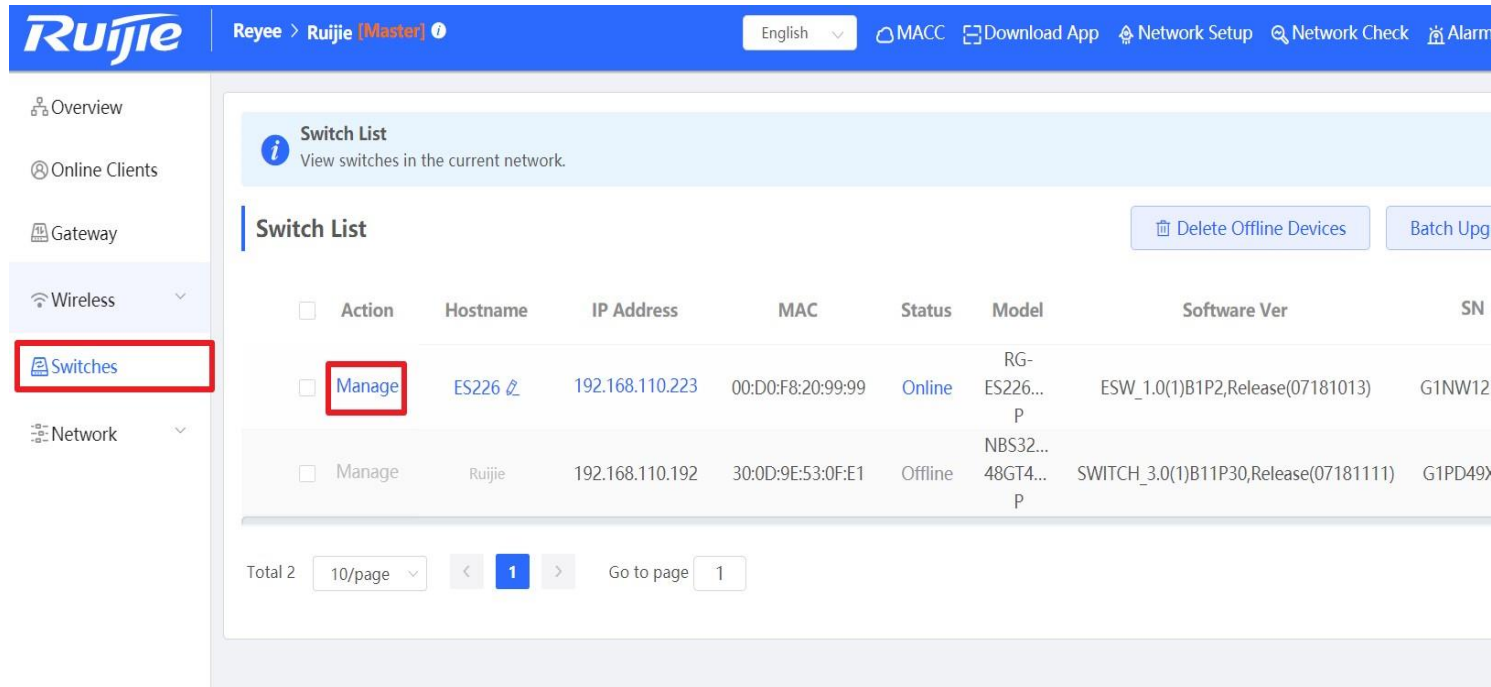


## 7.4 Speed Rate Limit

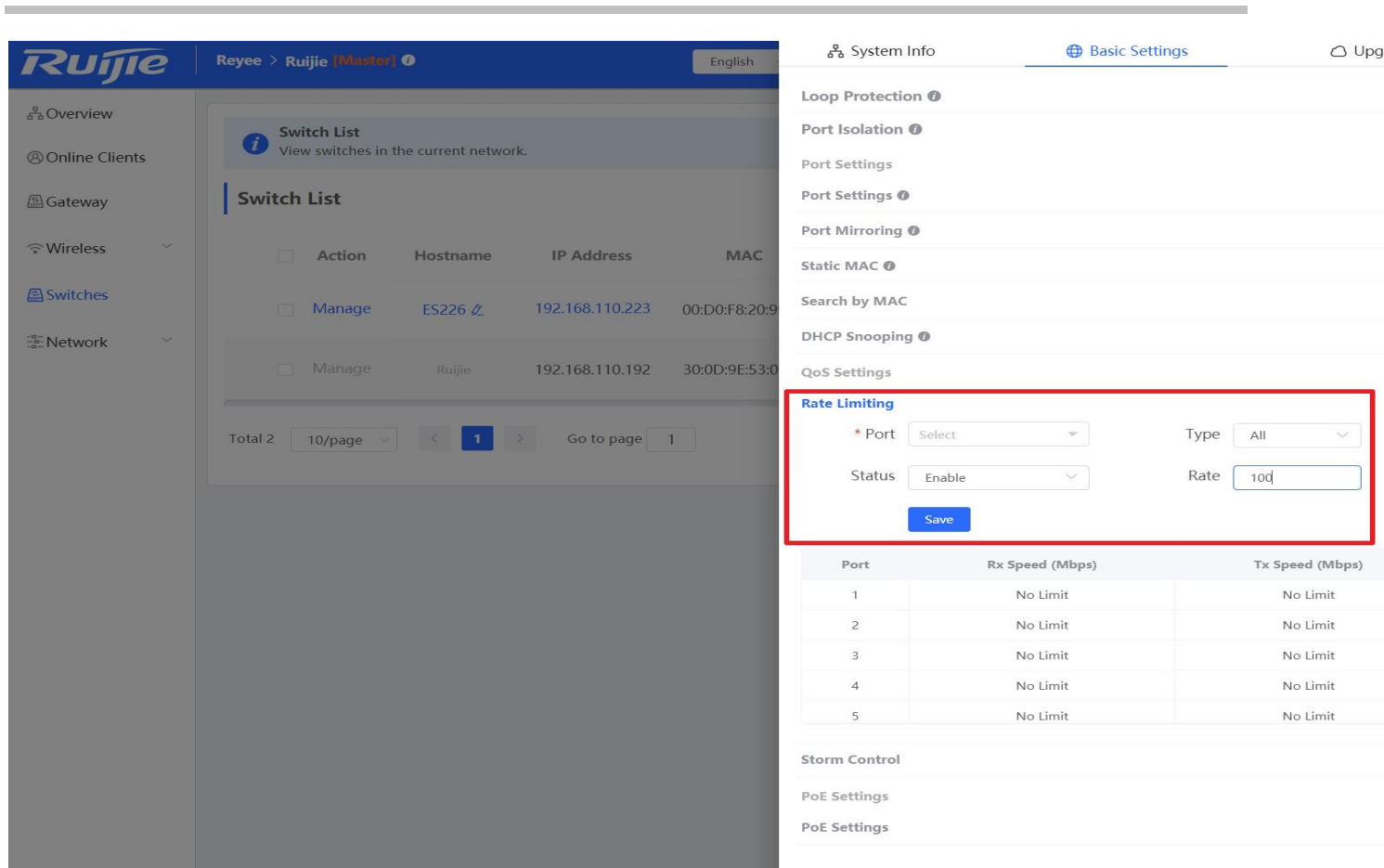
Rate limiting feature is used to limit the transmit speed rate on a specific port.

**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

**Switch List**  
View switches in the current network.

Buttons: Delete Offline Devices, Batch Upgrade

Action	Hostname	IP Address	MAC	Status	Model	Software Ver	SN
<input type="checkbox"/> Manage	ES226	192.168.110.223	00:D0:F8:20:99:99	Online	RG-ES226...P	ESW_1.0(1)B1P2,Release(07181013)	G1NW12E000...
<input type="checkbox"/> Manage	Ruijie	192.168.110.192	30:0D:9E:53:0F:E1	Offline	NBS32...48GT4...P	SWITCH_3.0(1)B11P30,Release(07181111)	G1PD49X0017...

Total 2 | 10/page | 1 | Go to page 1

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

**Basic Settings**

Direction: In

\* Dest Port: Select

Save

Src Port	Direction	Dest Port	Action
No Data			

Static MAC

Search by MAC

DHCP Snooping

QoS Settings

Rate Limiting

**Storm Control**

\* Port: Port 1 x Type: Broadcast

Status: Enable Rate: 10

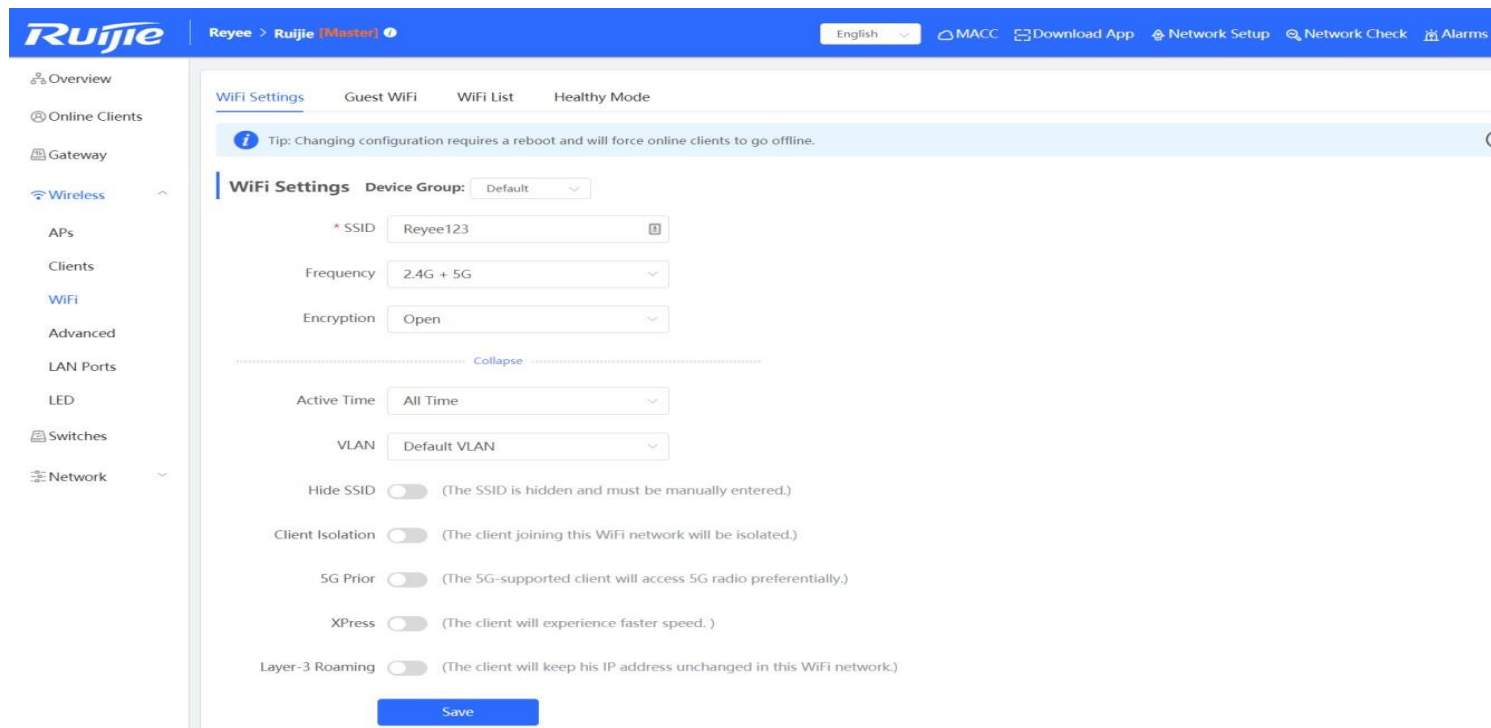
Save

Port	Broadcast (Mbit/sec)	Unknown Unicast (Mbit/sec)	Unknown Multicast (Mbit/sec)
1	Disable	Disable	Disable
2	Disable	Disable	Disable
3	Disable	Disable	Disable
4	Disable	Disable	Disable

## 8 Reyee AP Configuration

### 8.1 Wi-Fi Setting

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



**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.

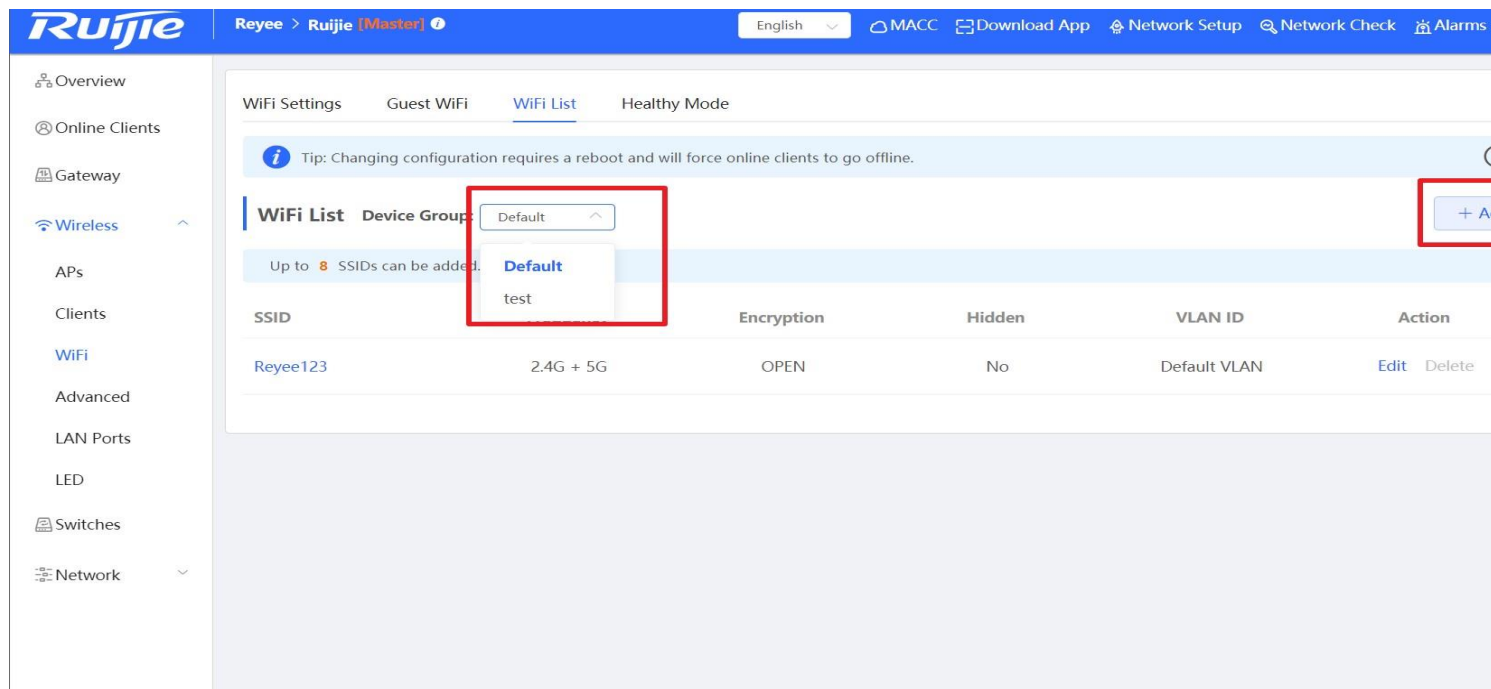
### Configuration Steps:

Step 1: Choose **Wireless** → **WiFi** → **WiFi List**

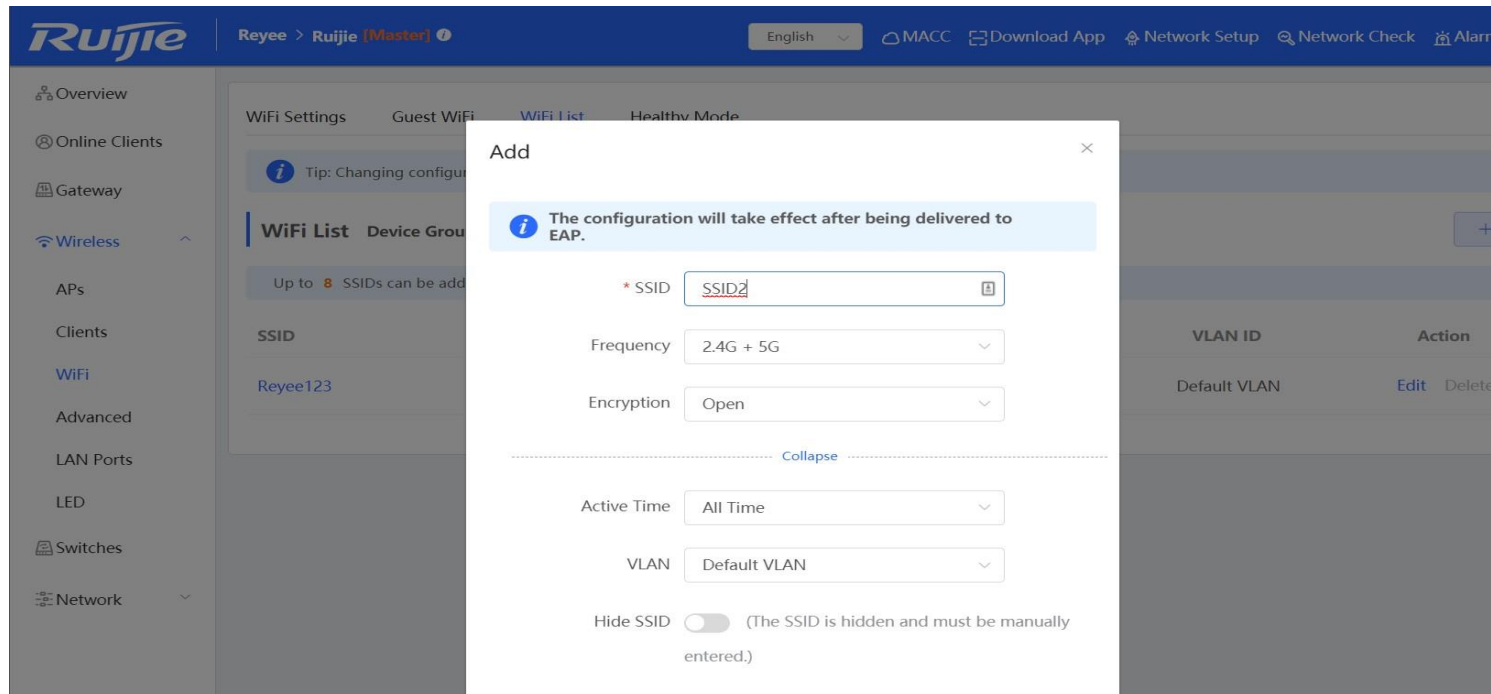
The screenshot shows the Ruijie network management interface. The top navigation bar includes the Ruijie logo, the user 'Reyee > Ruijie [Master]', and various utility links like 'English', 'MACC', 'Download App', 'Network Setup', 'Network Check', and 'Alarms'. On the left sidebar, the 'Wireless' menu is expanded, and 'WiFi' is highlighted with a red box. The main content area shows the 'WiFi List' configuration page, with 'WiFi List' also highlighted in the top navigation tabs. A tip message states: 'Tip: Changing configuration requires a reboot and will force online clients to go offline.' Below this, there is a 'WiFi List' section with a 'Device Group' dropdown set to 'Default' and a '+ Add' button. A message indicates 'Up to 8 SSIDs can be added.' A table lists the current SSID configuration:

SSID	Frequency	Encryption	Hidden	VLAN ID	Action
Reyee123	2.4G + 5G	OPEN	No	Default VLAN	Edit Delete

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



Step 3: Fill in the SSID name WiFi related settings



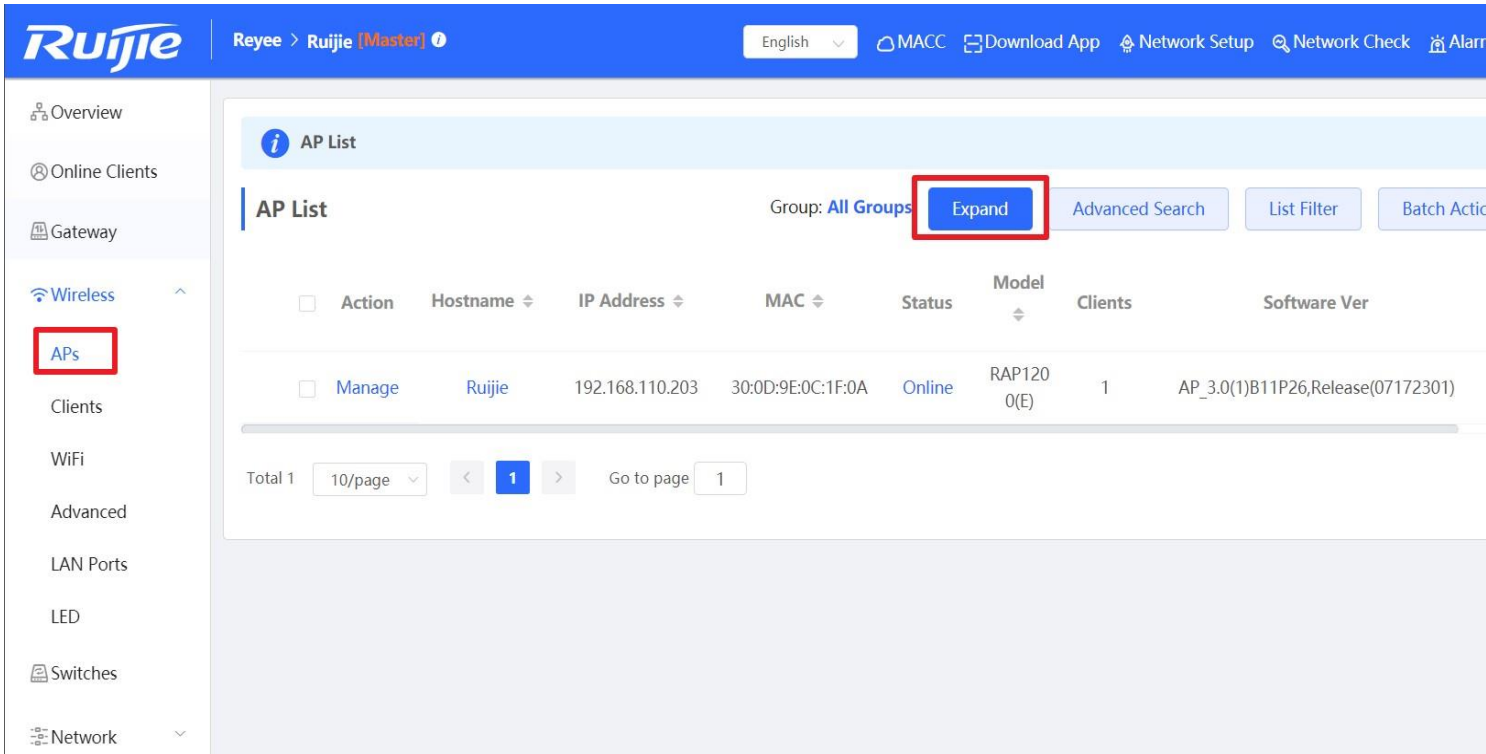
## 8.3 AP Group

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

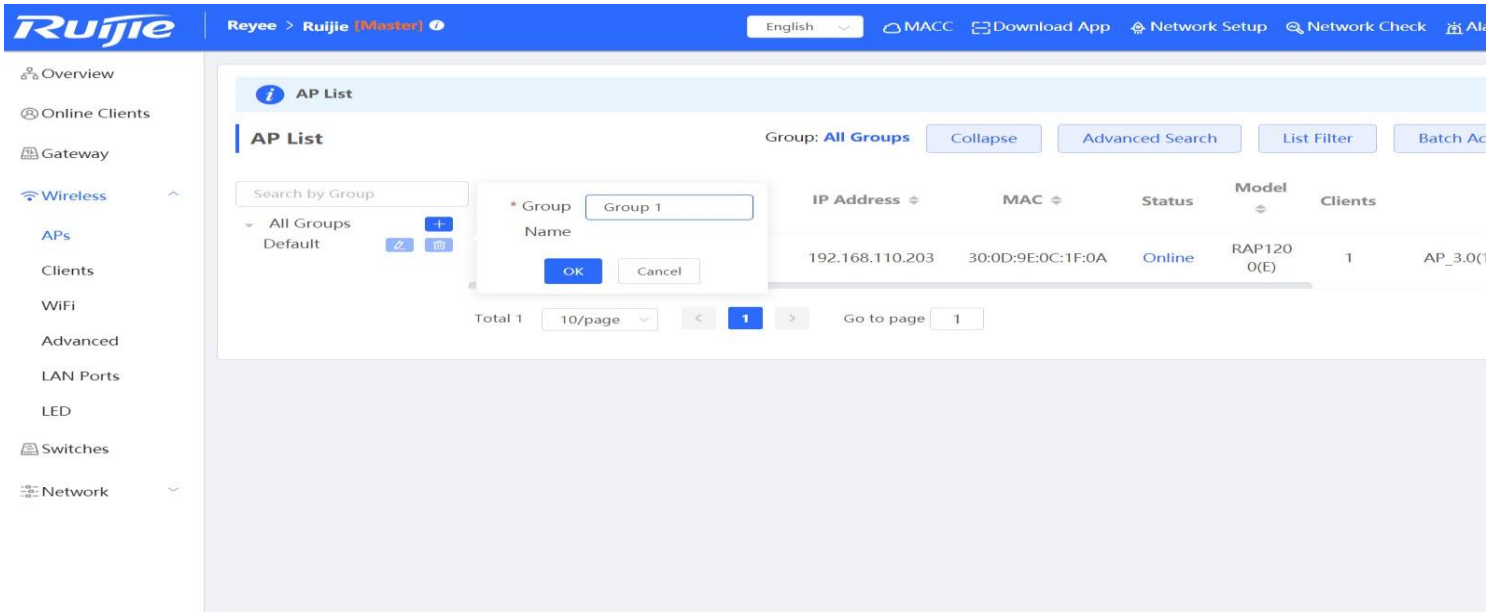
### Configuration Steps



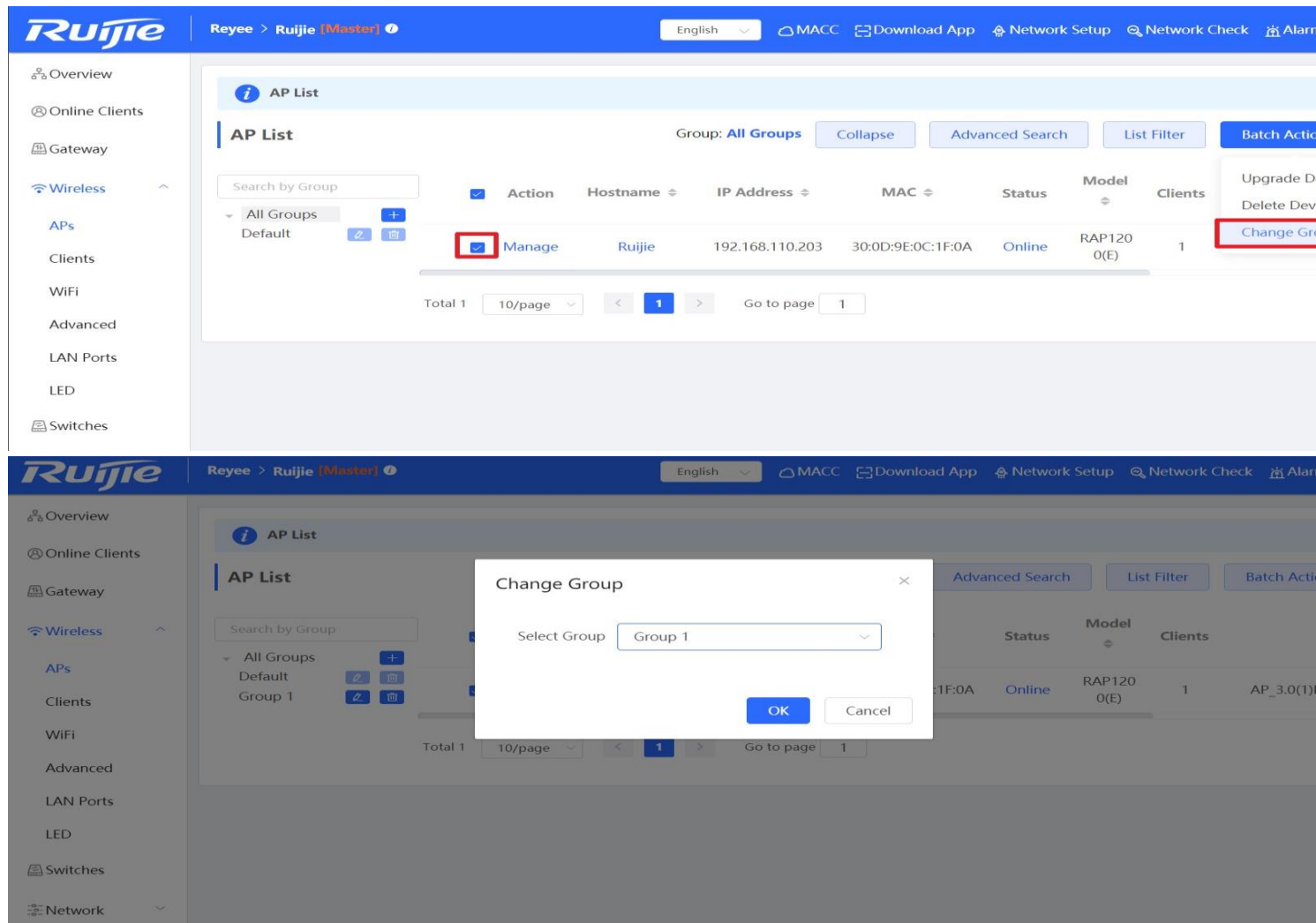
Step 1: Choose **Wireless** → **AP** and click the **“Expand”** button



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



Step 3: Move the AP to the new group



## 8.4 Blacklist/Whitelist

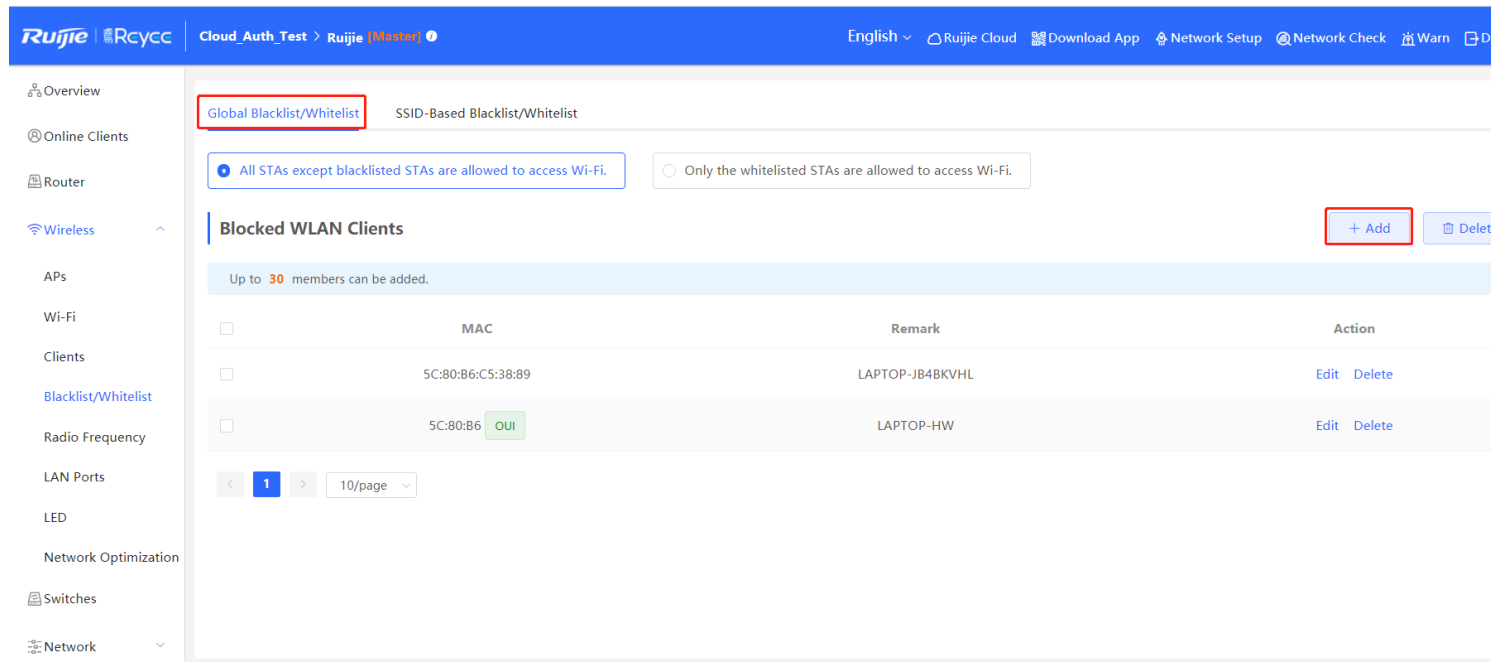
The Blacklist/Whitelist module allows you to configure client blacklist and whitelist.

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

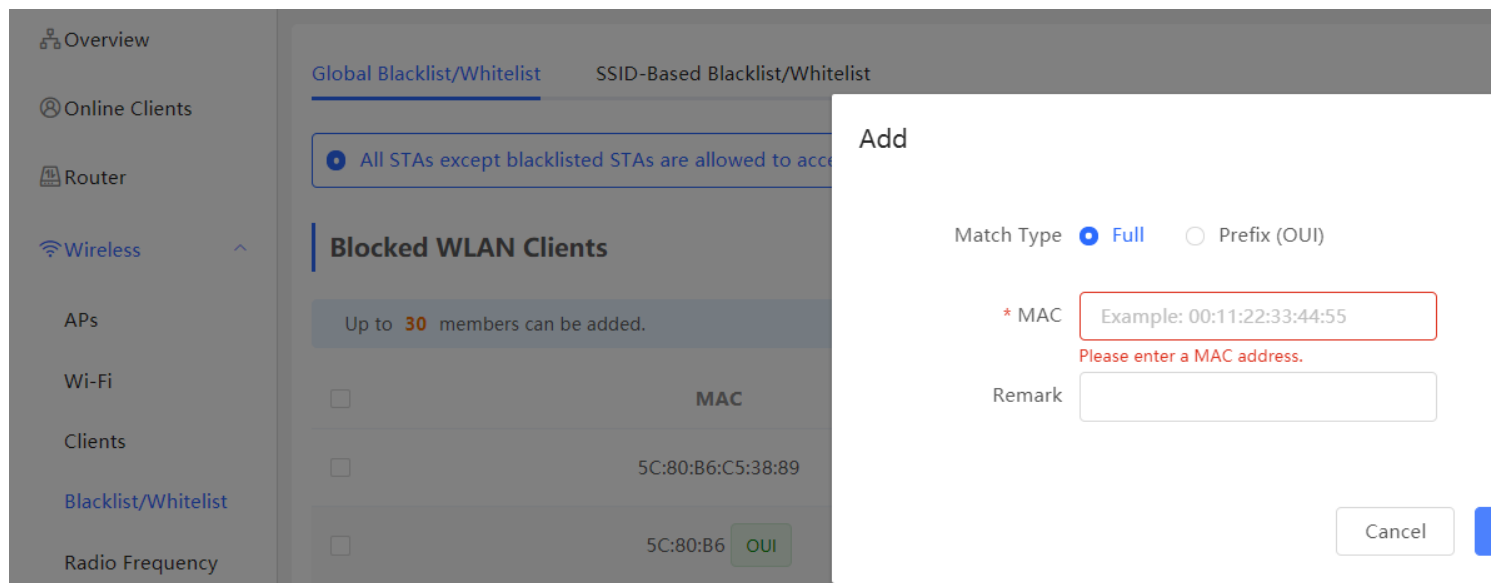
**Whitelist:** only the devices in the whitelist are allowed to access the network

### Configuration Steps

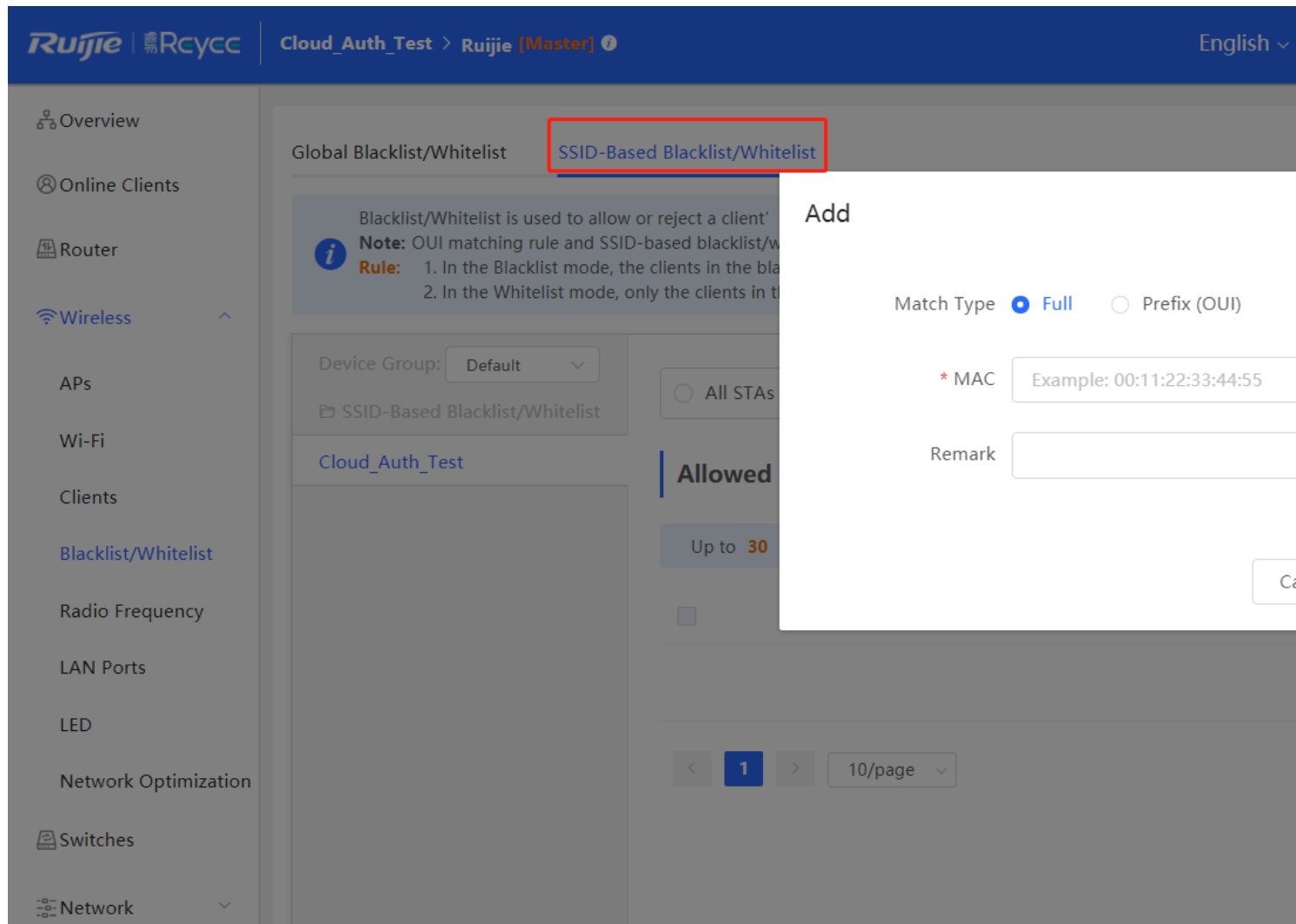
Step 1: Choose **Wireless** → **Blacklist/Whitelist** → **Global**



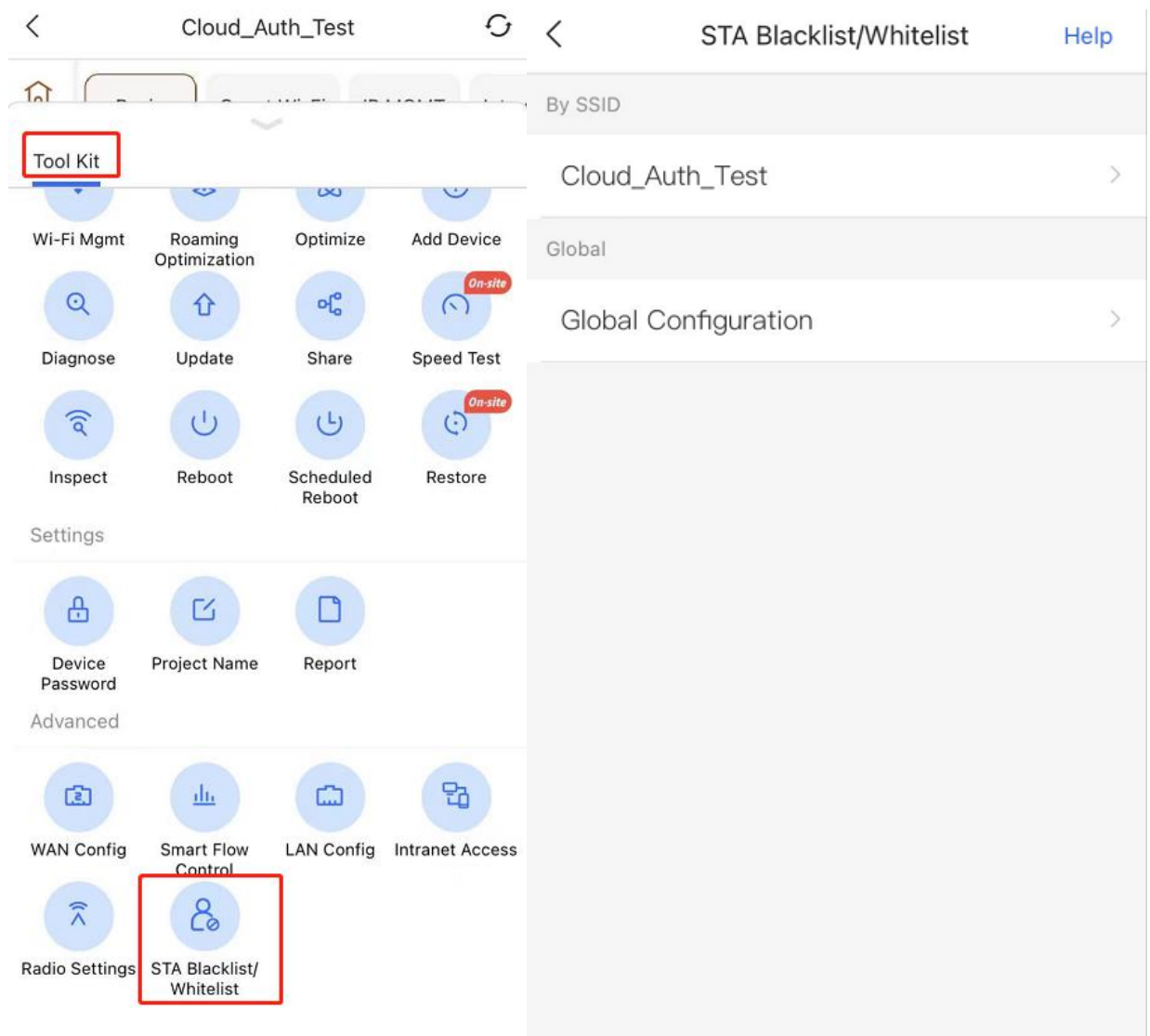
Support full match and OUI match

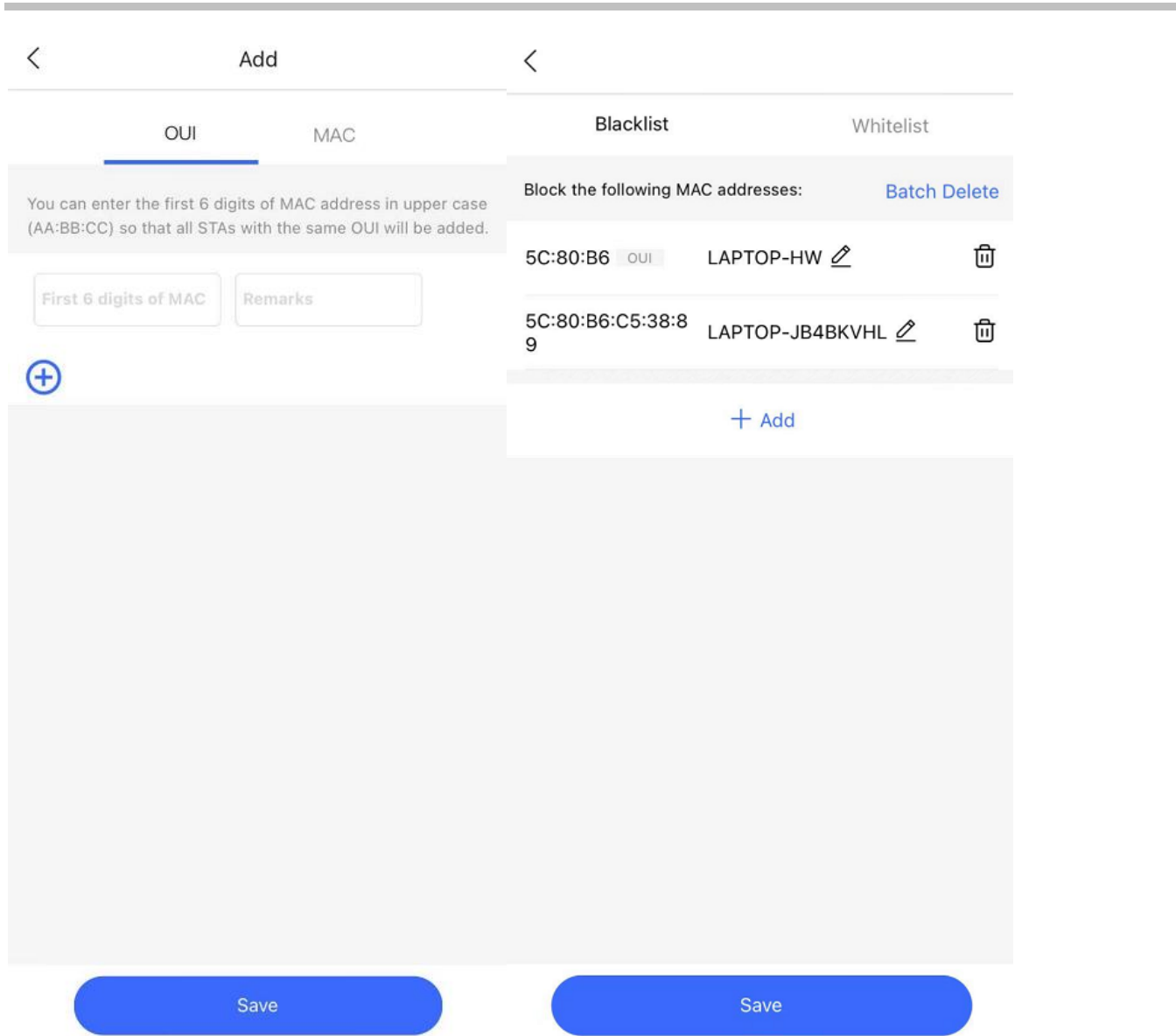


Step 2: Choose **Wireless** → **Blacklist/Whitelist** → **SSID-based**



Step 3 : Support to configure with Ruijie Cloud APP



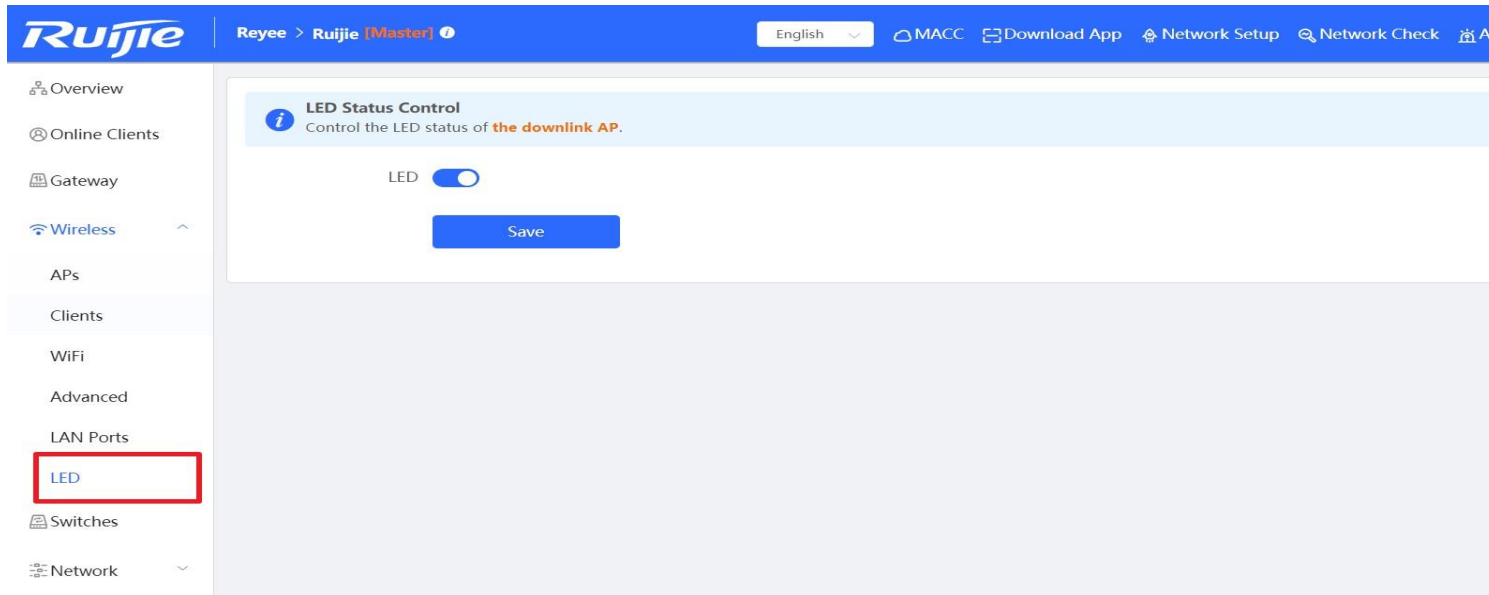


## 8.5 Turn on/off LED indicator

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.

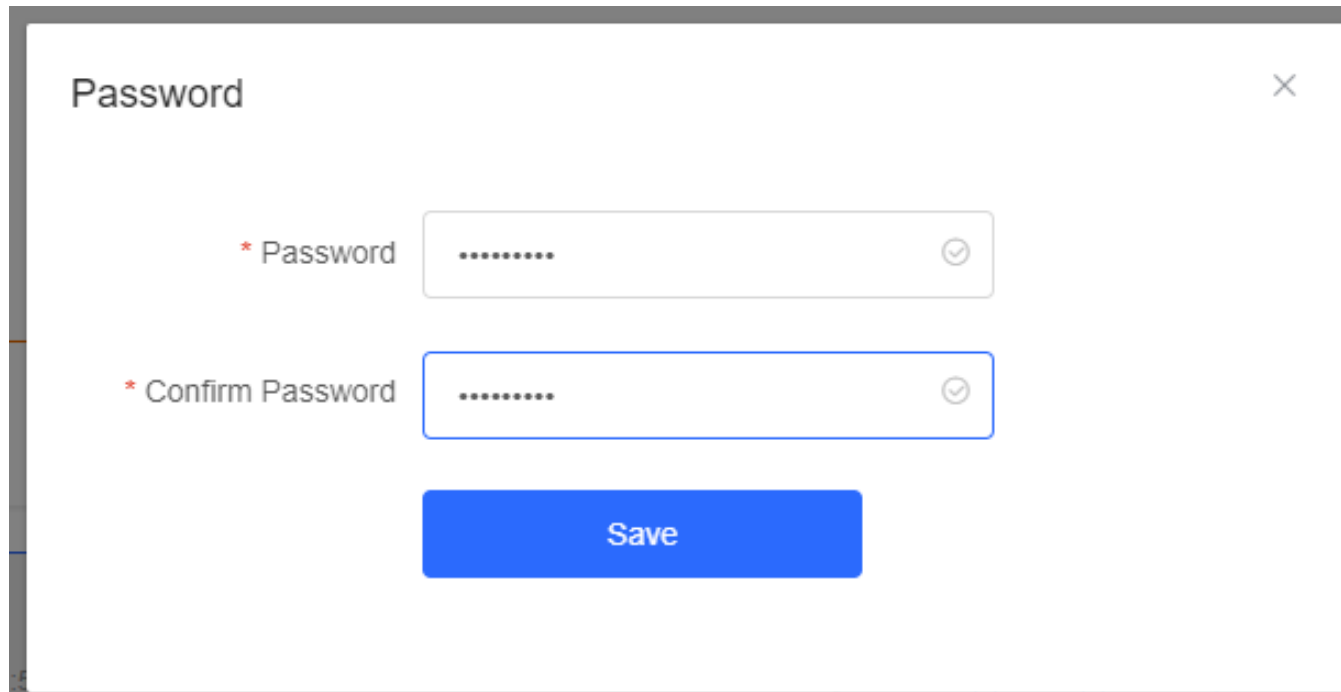
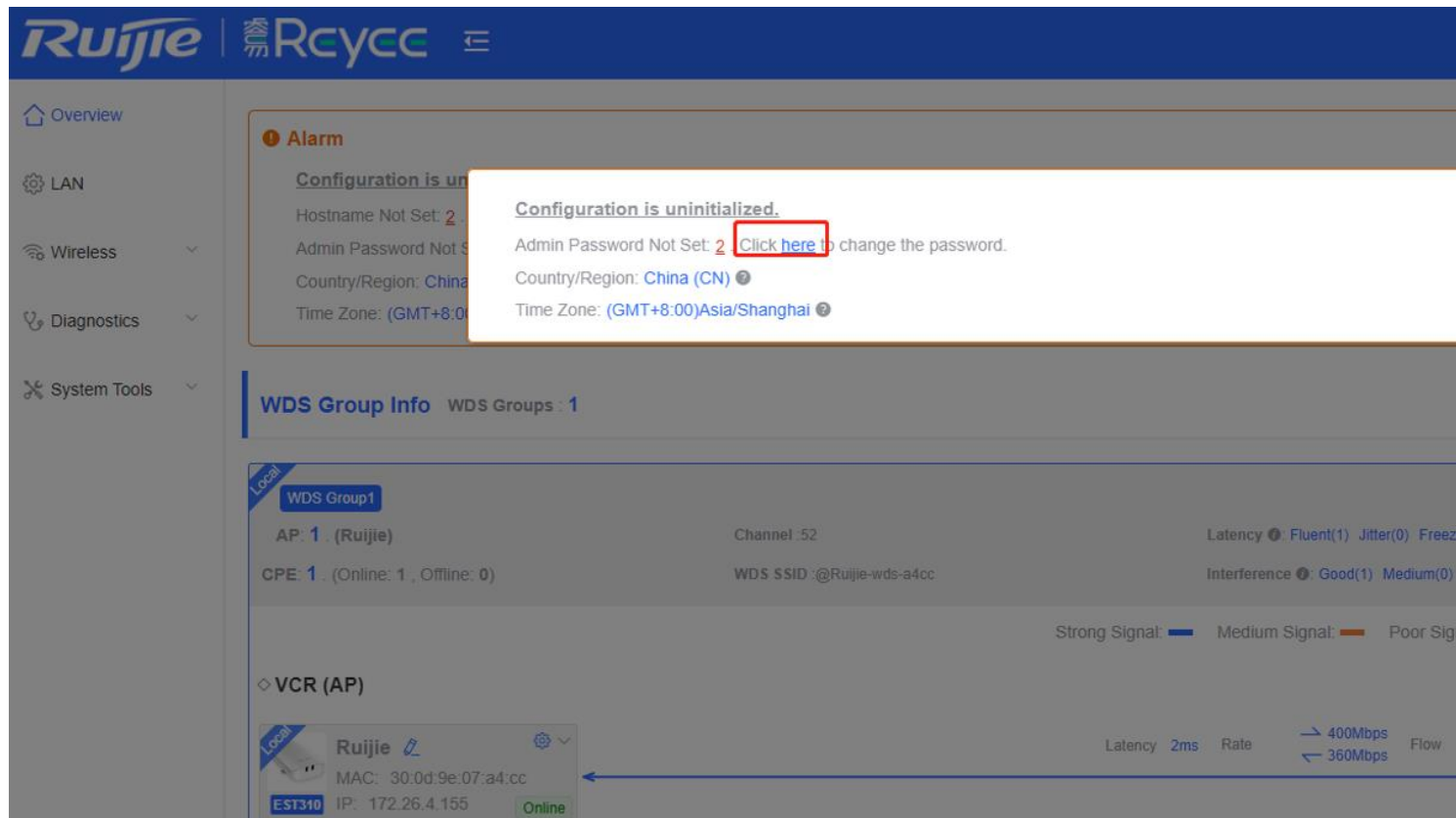


## 9 EST Series Configuration

### 9.1 Basic Setting

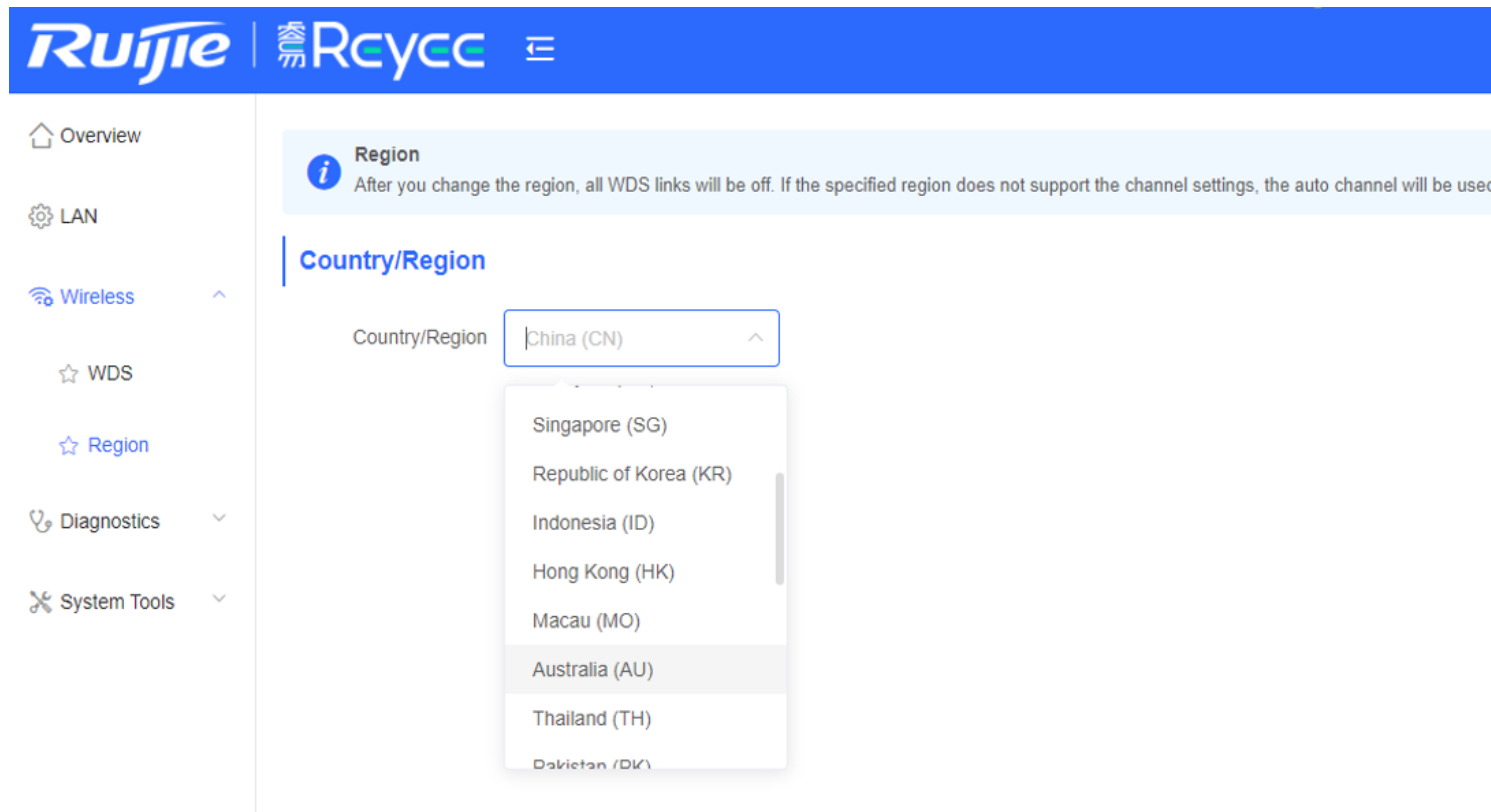
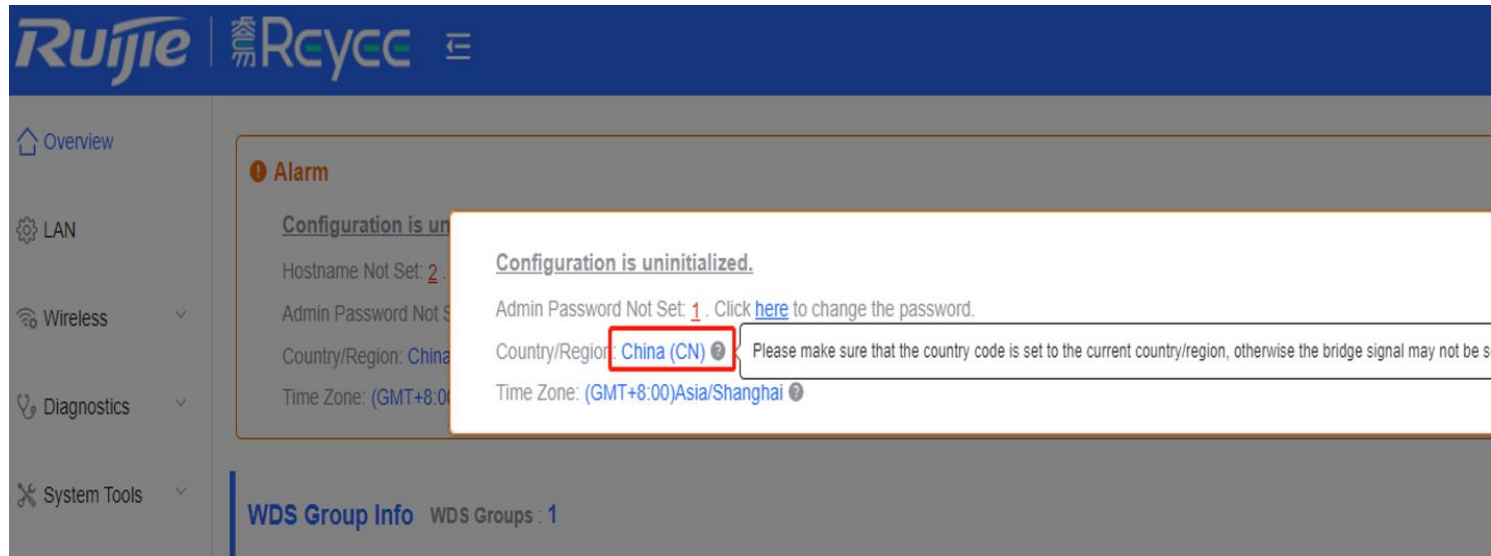
The devices are paired by default and can be used without requiring any configurations.

Change the Admin password



Change the country code. Note: After you change the region, all WDS links will be off. If the specified region does not support the channel settings, the auto channel will be used instead.











Change the Time Zone and NTP server

 Overview

 LAN

 Wireless 


 Diagnostics 


 System Tools 

### Alarm

Configuration is uninitialized.

Hostname Not Set: 2 

Country/Region: China (CN) 

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

**WDS Group Info** WDS Groups : 1

The screenshot shows the Ruijie RCYCC web interface. The top navigation bar includes the Ruijie and RCYCC logos. A left sidebar contains menu items: Overview, LAN, Wireless, Diagnostics, System Tools, Time (highlighted), Management, Update, and Reboot. The main content area is titled 'Time' and contains an information icon and a warning: 'Configure and view time (The device has no RTC module. The time settings will not be saved upon reboot)'. Below this, the 'Current Time' is displayed as '2020-11-17 15:04:16' with an 'Edit' button. The 'Time Zone' is set to '(GMT+8:00)Asia/Shanghai'. Under 'NTP Server', there is an 'Add' button and a list of servers: '0.cn.pool.ntp.org', '1.cn.pool.ntp.org', 'cn.pool.ntp.org', 'pool.ntp.org', 'asia.pool.ntp.org', 'europe.pool.ntp.org', and 'rdate.darkorb.net'. Each server entry has a 'Delete' button. A 'Save' button is located at the bottom of the configuration area.

## 9.2 Devices status monitor

The status of EST310 is shown on overview, including channel, WDS SSID, latency, bandwidth, interference, RSSI, link signal, Rate, Flow and online status.

**Alarm**  
Configuration is uninitialized.  
Hostname Not Set: 2  
Country/Region: China (CN)  
Time Zone: (GMT+8:00)Asia/Shanghai

**WDS Group Info** WDS Groups : 1

WDS Group1  
AP: 1 (Ruijie) Channel: 52 Latency: Fluent(1) Jitter(0) Freeze(0) Bandwidth: Good(1) Medium(0) Poor(0)  
CPE: 1 (Online: 1, Offline: 0) WDS SSID: @Ruijie-wds-a4cc Interference: Good(1) Medium(0) Poor(0) RSSI: Good(1) Medium(0) Poor(0)

Strong Signal: — Medium Signal: — Poor Signal: —

**VCR (AP)**  
Ruijie  
MAC: 30.0d.9e.07:a4.cc  
EST310 IP: 172.26.4.155 Online

**Camera (CPE)**  
Ruijie  
MAC: 30.0d.9e.07:a9.88  
EST310 IP: 172.26.4.157 Online

Show more details for the EST310

**Alarm**  
Configuration is uninitialized.  
Hostname Not Set: 2  
Country/Region: China (CN)  
Time Zone: (GMT+8:00)Asia/Shanghai

**WDS Group Info** WDS Groups : 1

Hostname	MAC	Latency
Ruijie	30.0d.9e.07:a9.88	2ms

Device: Group 1 / CPE / Ruijie (Select a device)

Setup: LAN WDS Reboot

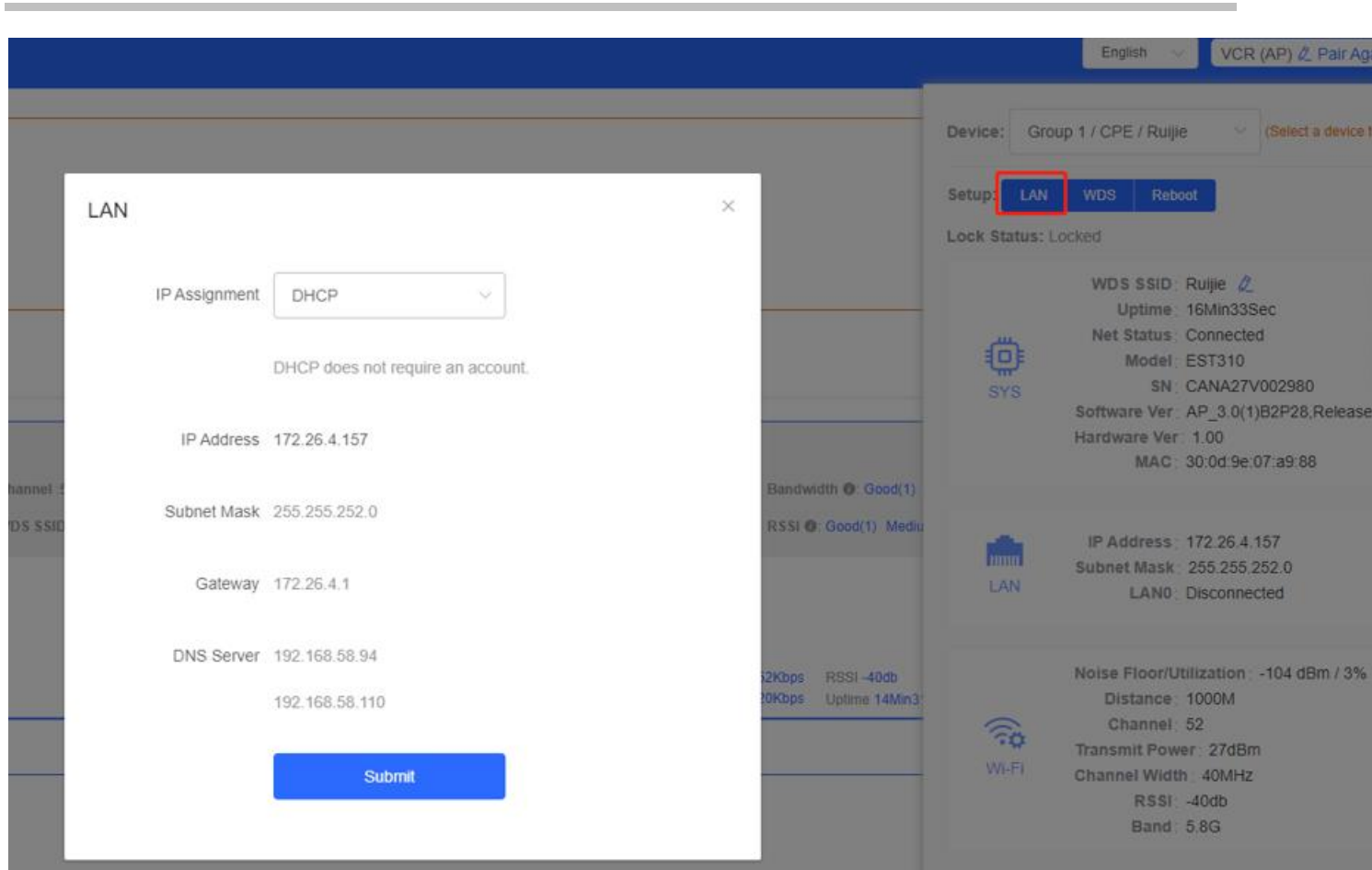
Lock Status: Locked

**SYS**  
WDS SSID: Ruijie  
Uptime: 16Min04Sec  
Net Status: Connected  
Model: EST310  
SN: CANA27V002980  
Software Ver: AP\_3.0(1)B2P28\_Release  
Hardware Ver: 1.00  
MAC: 30.0d.9e.07:a9.88

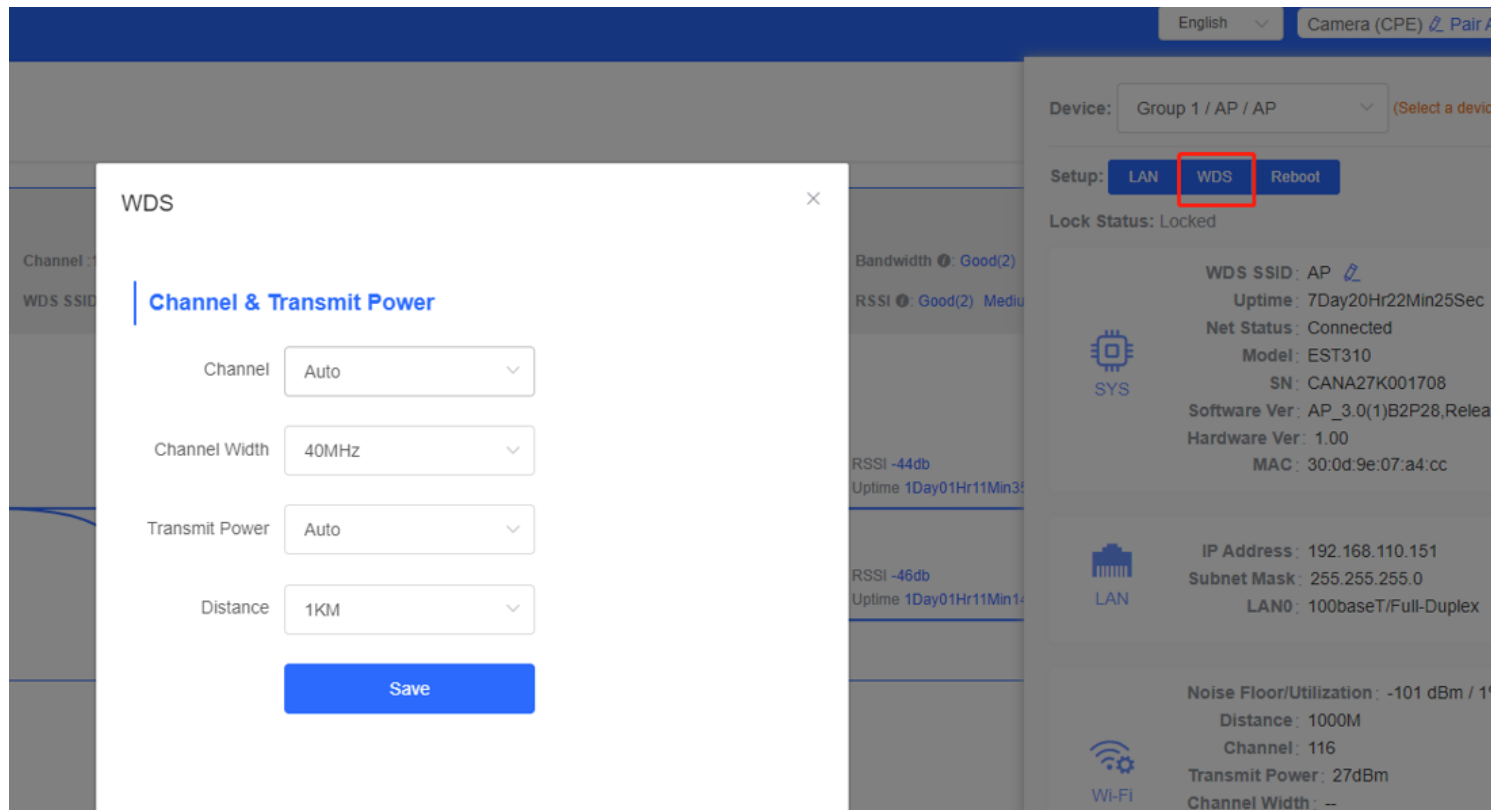
**LAN**  
IP Address: 172.26.4.157  
Subnet Mask: 255.255.252.0  
LAN0: Disconnected

**Wi-Fi**  
Noise Floor/Utilization: -104 dBm /  
Distance: 1000M  
Channel: 52  
Transmit Power: 27dBm  
Channel Width: 40MHz  
RSSI: -41db  
Band: 5.8G

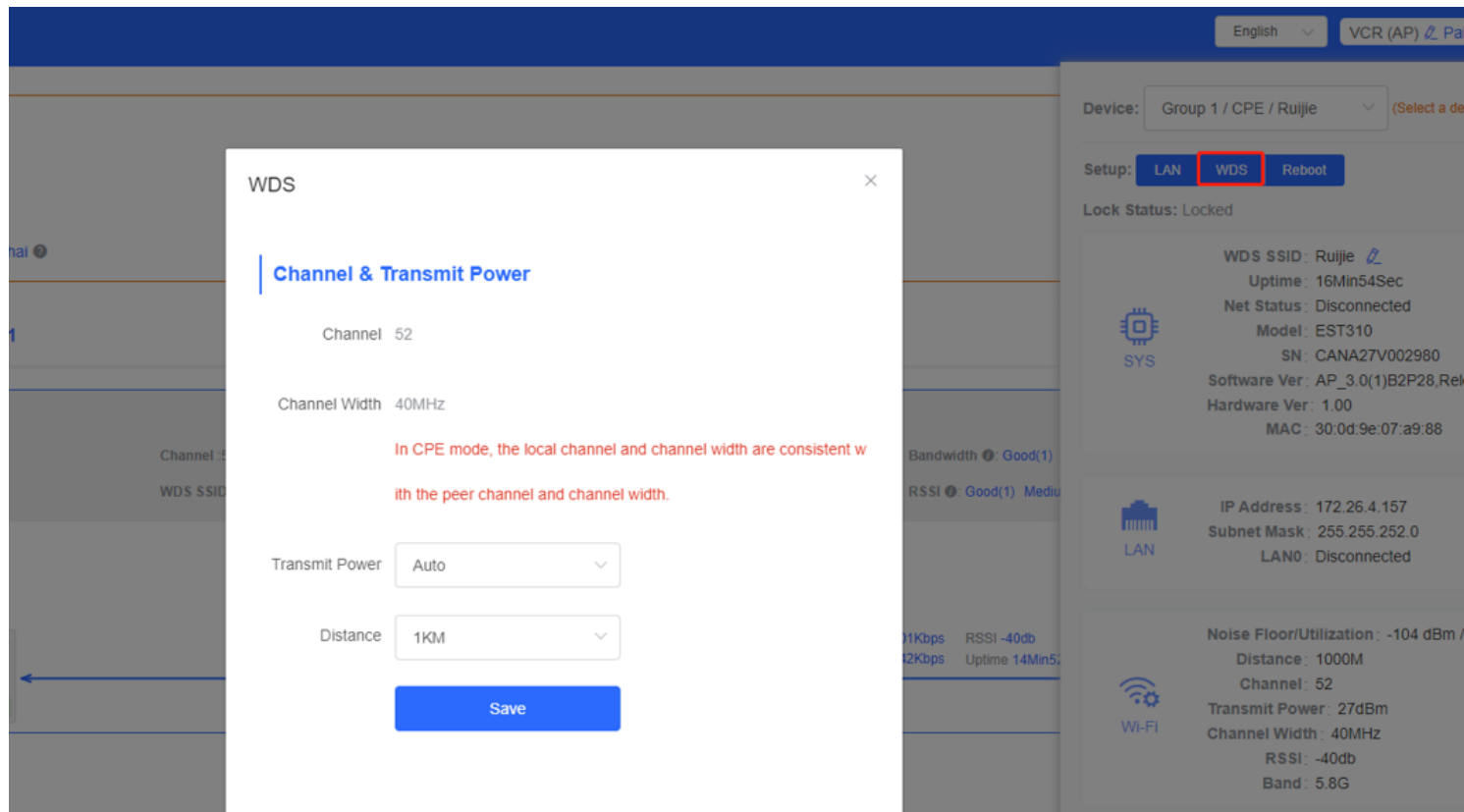
Click the LAN to edit the LAN configuration

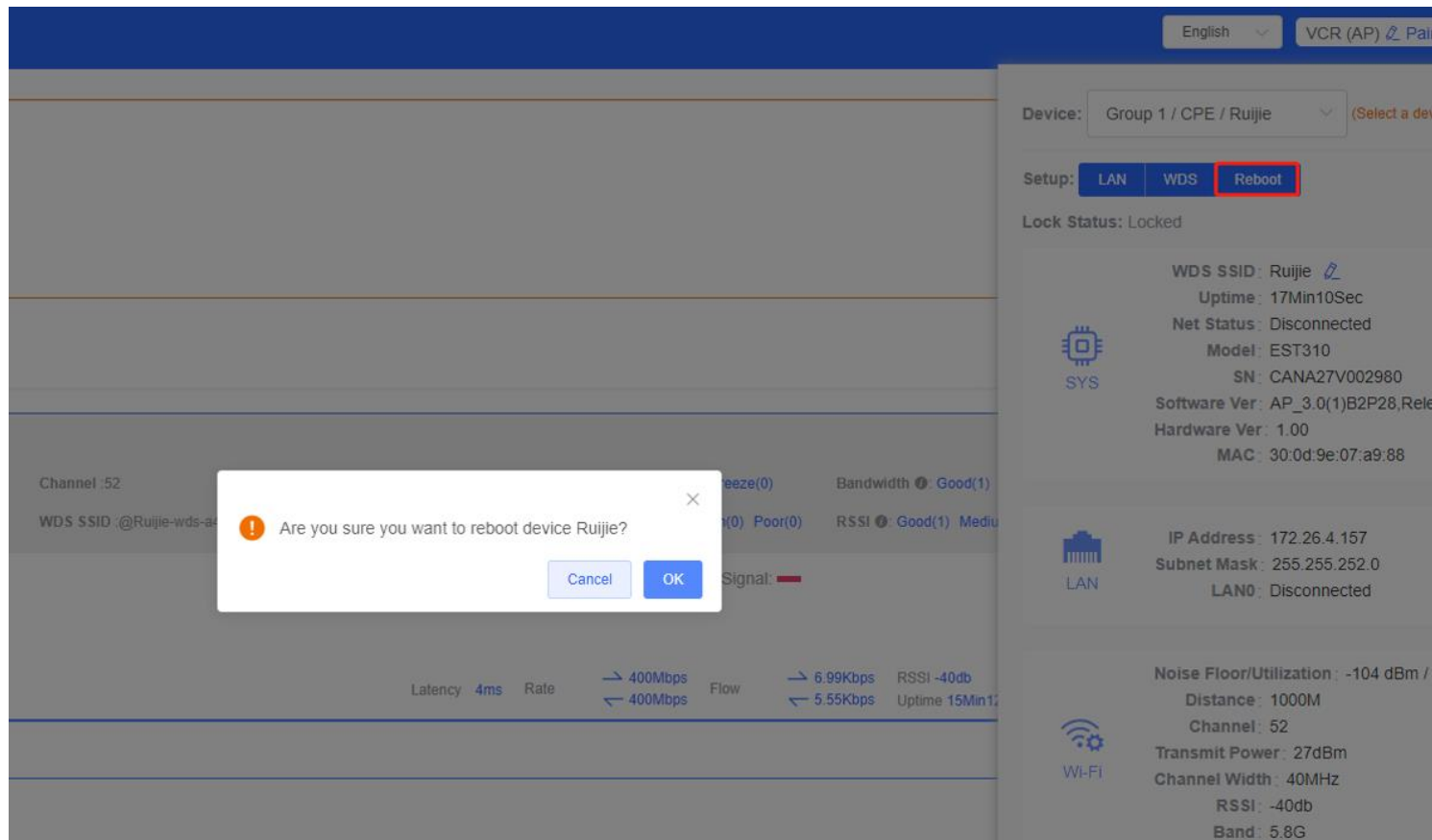


Click the AP's WDS to edit the WDS configuration



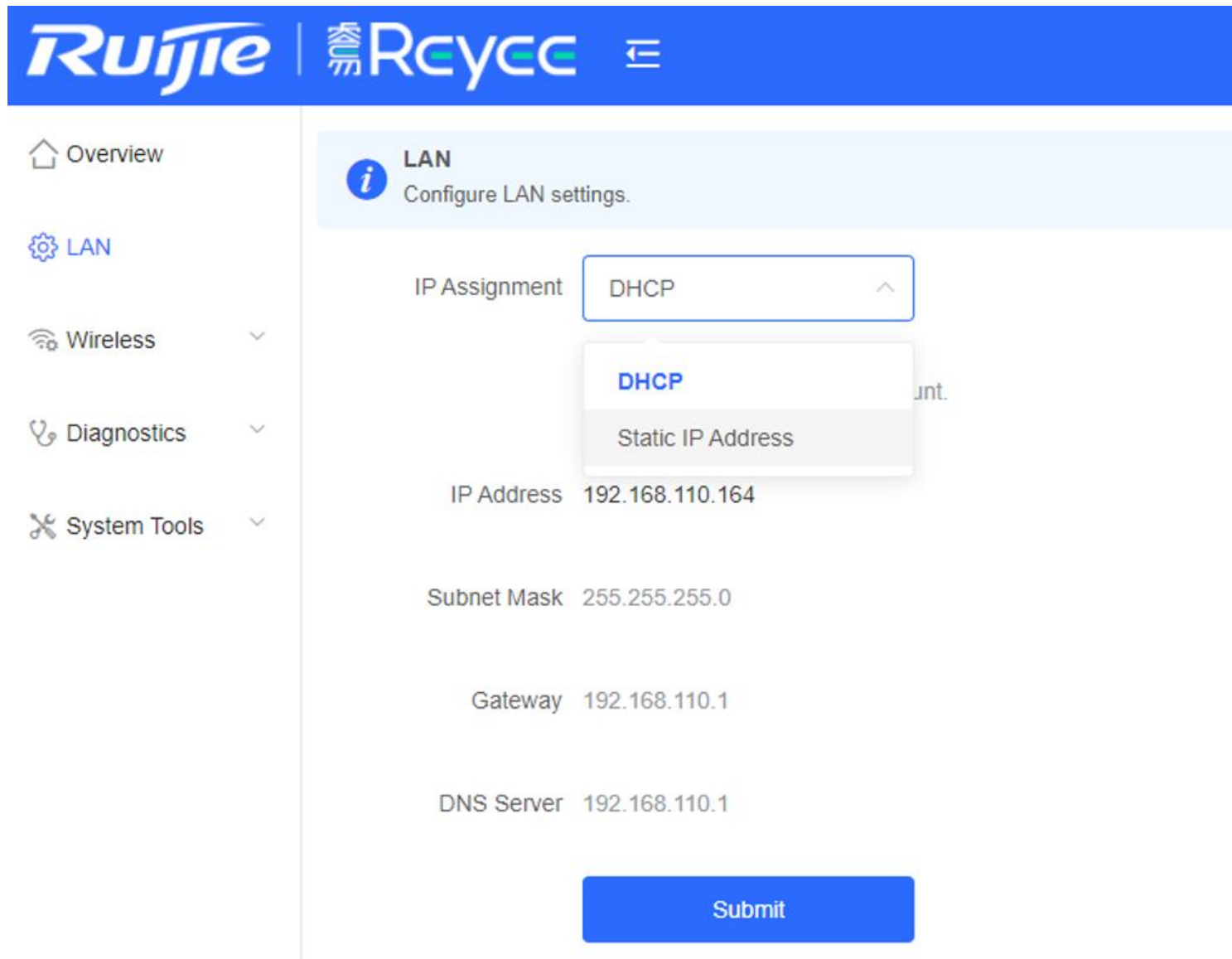
For the CPE, only show the WDS configuration and can't edit





### 9.3 LAN setting

Change LAN settings, support DHCP and Static IP Address, default is DHCP

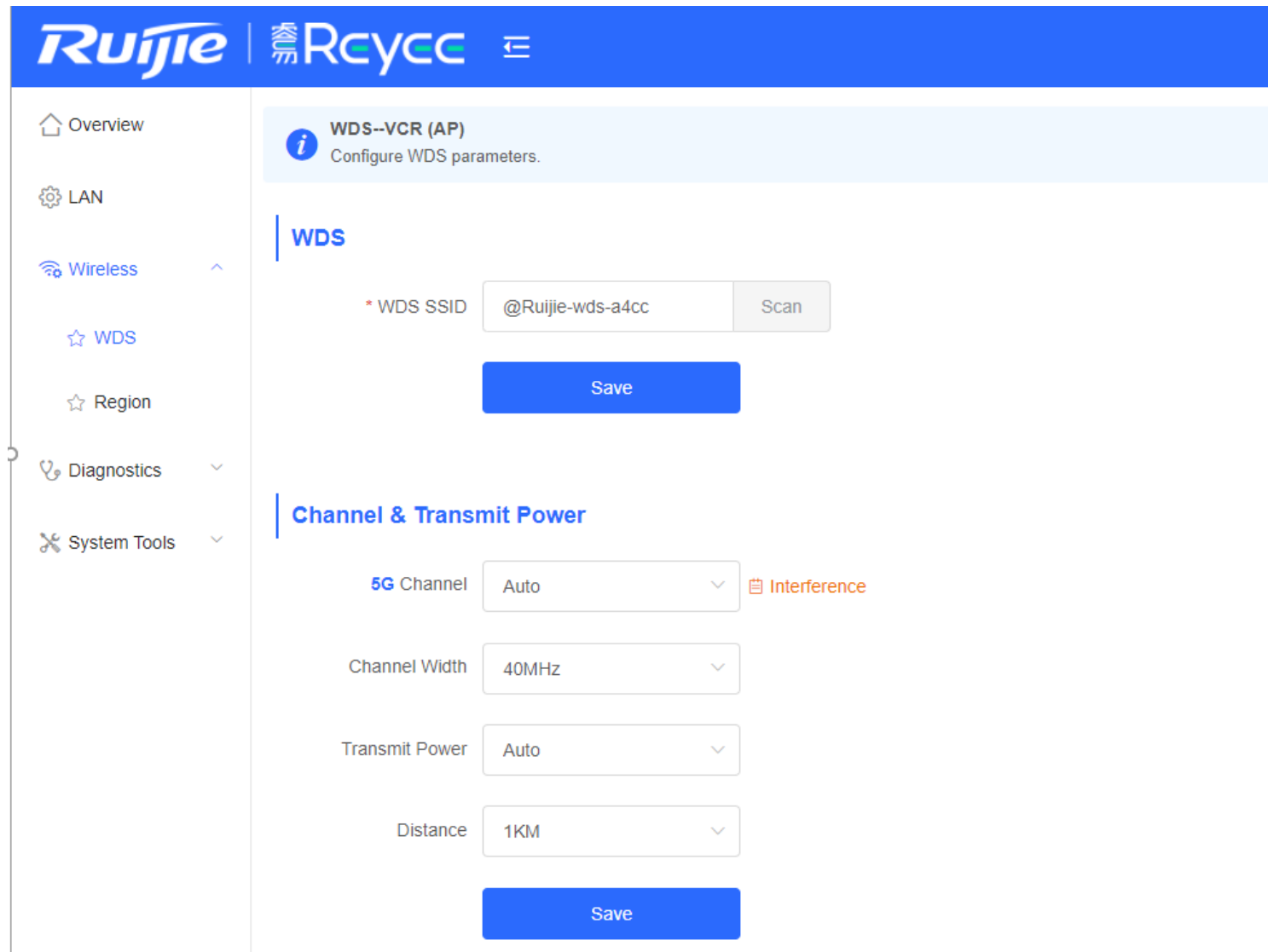


The screenshot shows the Ruijie RCYCC web interface for LAN configuration. The top navigation bar includes the Ruijie and RCYCC logos. A left sidebar contains menu items: Overview, LAN (selected), Wireless, Diagnostics, and System Tools. The main content area is titled 'LAN' with a sub-header 'Configure LAN settings.' Below this, there are several configuration fields: 'IP Assignment' is a dropdown menu currently showing 'DHCP' with a dropdown arrow; a dropdown menu is open below it, showing 'DHCP' (highlighted) and 'Static IP Address'; 'IP Address' is set to '192.168.110.164'; 'Subnet Mask' is '255.255.255.0'; 'Gateway' is '192.168.110.1'; and 'DNS Server' is '192.168.110.1'. A blue 'Submit' button is located at the bottom right of the configuration area.

## 9.4 Wireless Setting

WDS SSID configuration, only support change the SSID and the default encryption mode is WPA/WPA2-PSK





The screenshot shows the Ruijie Reyee management interface. The top navigation bar includes the Ruijie and Reyee logos. A left sidebar contains menu items: Overview, LAN, Wireless, WDS, Region, Diagnostics, and System Tools. The main content area is titled 'WDS--VCR (AP)' with a sub-header 'Configure WDS parameters.' Below this, there are two sections: 'WDS' and 'Channel & Transmit Power'. The 'WDS' section has a 'WDS SSID' field containing '@Ruijie-wds-a4cc' and a 'Scan' button. A blue 'Save' button is positioned below. The 'Channel & Transmit Power' section contains four dropdown menus: '5G Channel' (set to 'Auto'), 'Channel Width' (set to '40MHz'), 'Transmit Power' (set to 'Auto'), and 'Distance' (set to '1KM'). An 'Interference' button is located to the right of the '5G Channel' dropdown. A blue 'Save' button is at the bottom of this section.

Choose **Channel & Transmit Power** → **5G Channel**, change the channel

Click the interference, will show the analysis of 5G channel and click to select a channel you want

**WDS--VCR (AP)**  
Configure WDS parameters.

**WDS**

\* WDS SSID: @Ruijie-wds-a4cc [Scan] [Save]

**Channel & Transmit Power**

5G Channel: 56 (5.28Ghz) [Interference]

Channel Width: 40MHz

Transmit Power: Auto

Distance: 1KM

[Save]

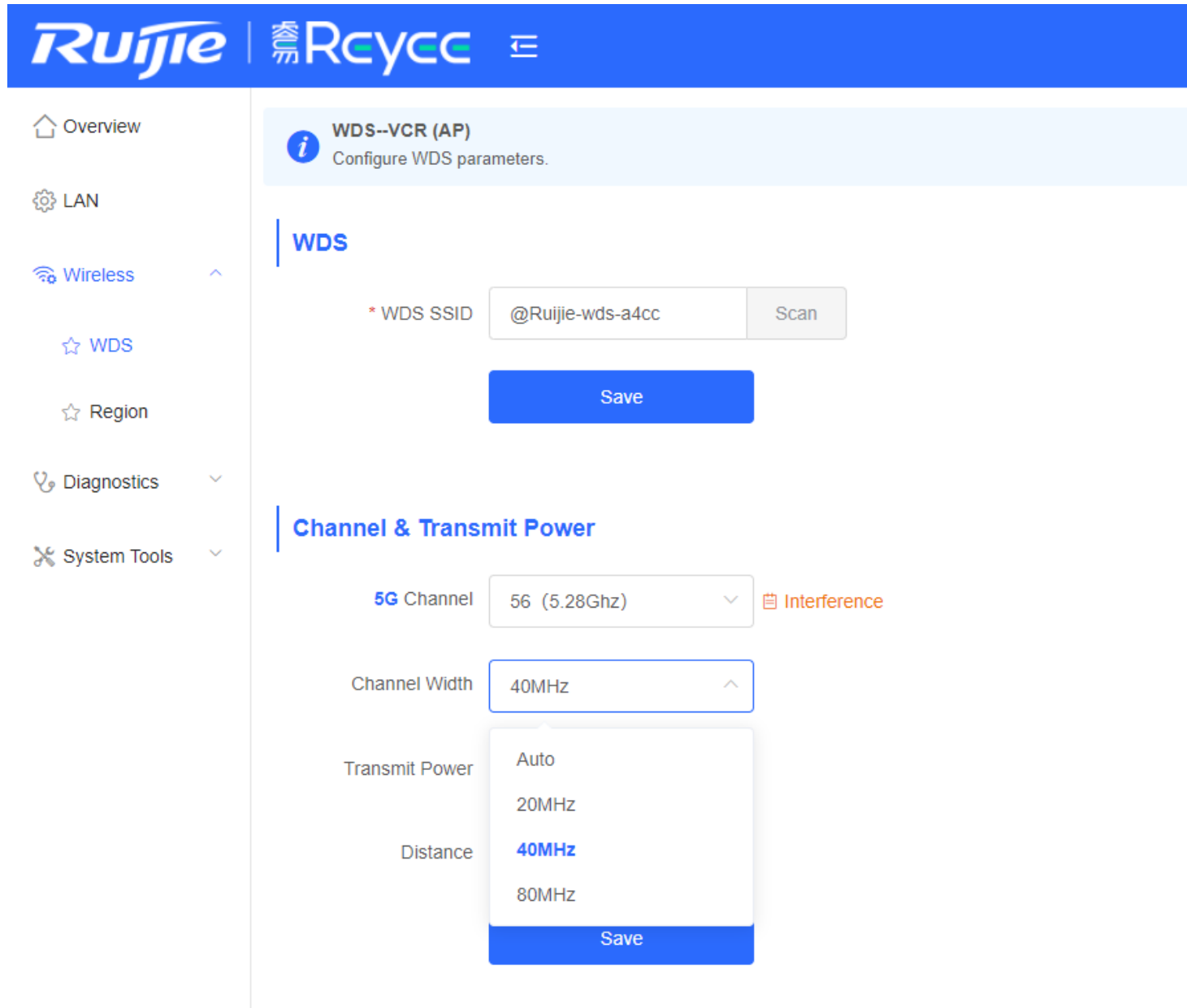
**Analysis (Current Channel: 56)** [Refresh]

RFI Strength

Channel	RFI Count
36	6
40	5
44	4
48	2
52	1
56	2
60	0
64	1
149	8
153	4
157	16
161	3

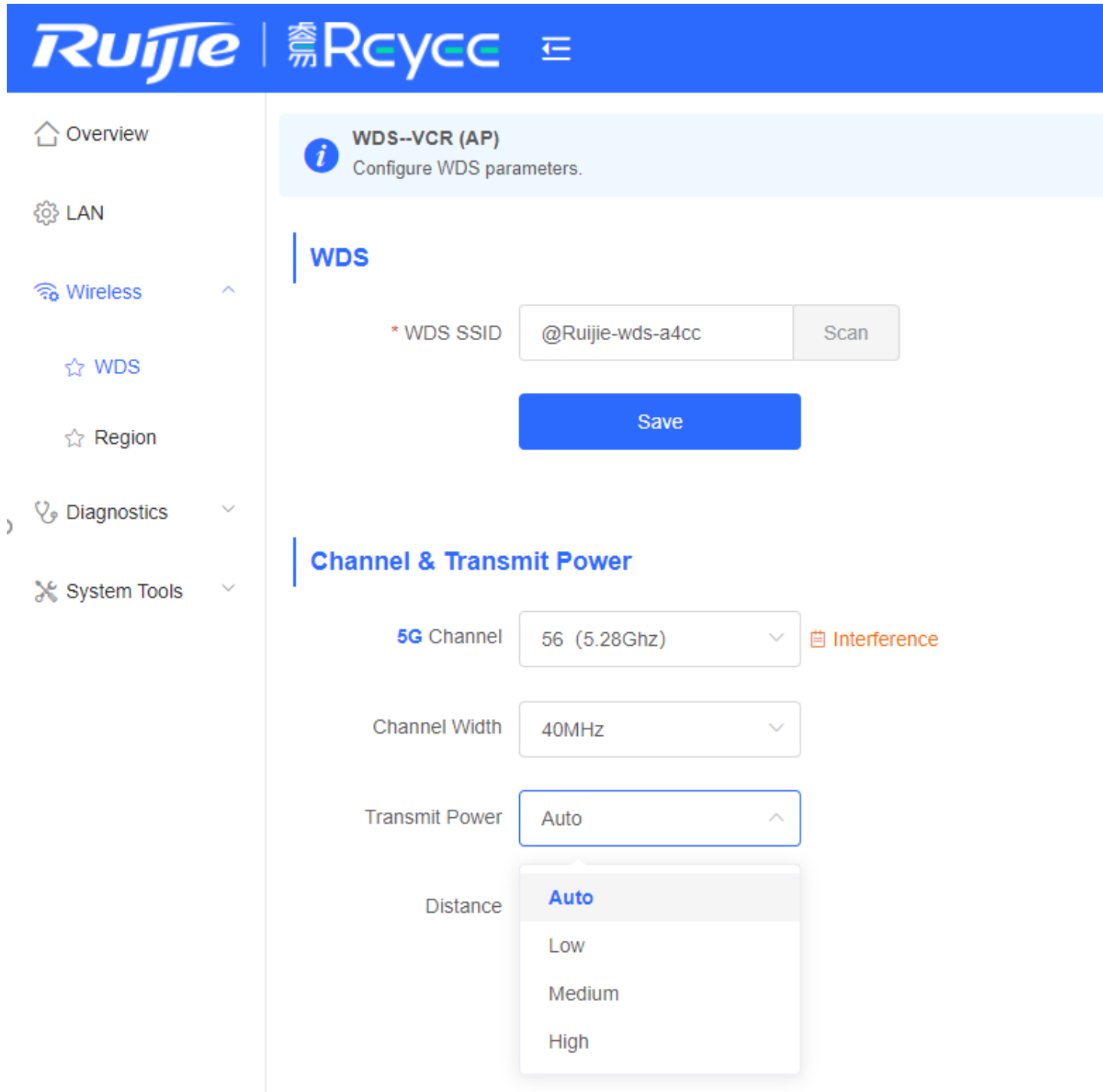
Tip : Click to select a channel.

Choose **Channel & Transmit Power** → **Channel Width**, change the band width  
Default is 40MHz, EST310 LAN only support 100M, so 40MHz is enough



The screenshot shows the Ruijie RCYCC web interface. The top navigation bar is blue with the Ruijie and RCYCC logos. A left sidebar contains menu items: Overview, LAN, Wireless, WDS, Region, Diagnostics, and System Tools. The main content area is titled 'WDS--VCR (AP)' and includes a sub-section 'WDS' with a 'WDS SSID' field set to '@Ruijie-wds-a4cc' and a 'Scan' button. Below this is a 'Save' button. The 'Channel & Transmit Power' section features a '5G Channel' dropdown set to '56 (5.28Ghz)' with an 'Interference' icon, a 'Channel Width' dropdown set to '40MHz', and a 'Transmit Power' dropdown menu open, showing options: 'Auto', '20MHz', '40MHz' (highlighted), and '80MHz'. A 'Save' button is at the bottom of the dropdown.

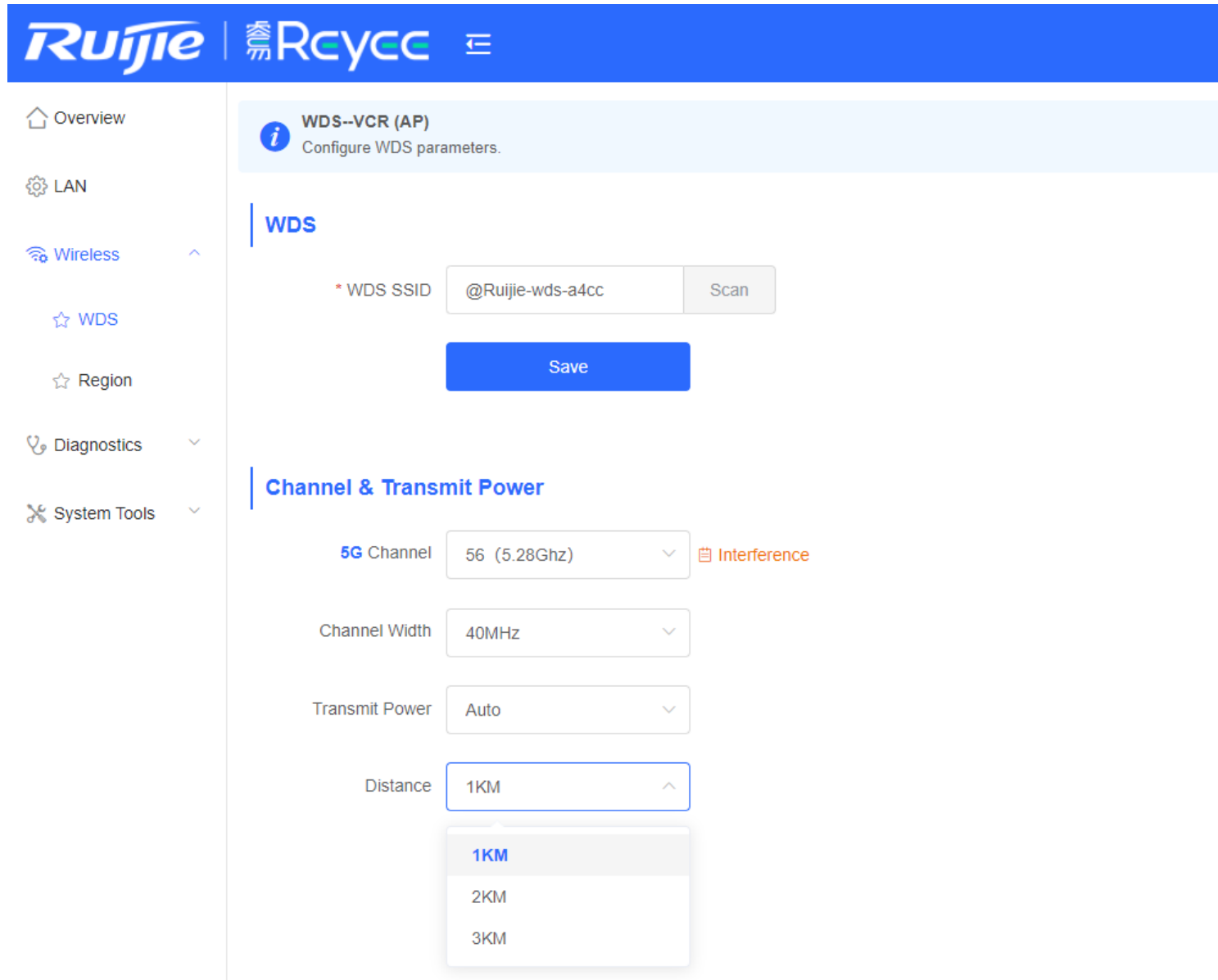
Choose **Channel & Transmit Power** → **Transmit Power**, change the power



The screenshot shows the Ruijie management interface. At the top, there is a blue header with the 'Ruijie' logo and 'Reyee' branding. A left sidebar contains navigation options: Overview, LAN, Wireless, WDS (highlighted with a star), Region, Diagnostics, and System Tools. The main content area is titled 'WDS--VCR (AP)' with a sub-header 'Configure WDS parameters.' Below this, the 'WDS' section features a 'WDS SSID' field containing '@Ruijie-wds-a4cc' and a 'Scan' button. A blue 'Save' button is positioned below the SSID field. The 'Channel & Transmit Power' section includes three dropdown menus: '5G Channel' set to '56 (5.28Ghz)', 'Channel Width' set to '40MHz', and 'Transmit Power' set to 'Auto'. An orange 'Interference' icon is visible next to the 5G Channel dropdown. A 'Distance' dropdown menu is open, showing options: 'Auto' (highlighted), 'Low', 'Medium', and 'High'.

Choose **Channel & Transmit Power** → **Distance**, change the distance

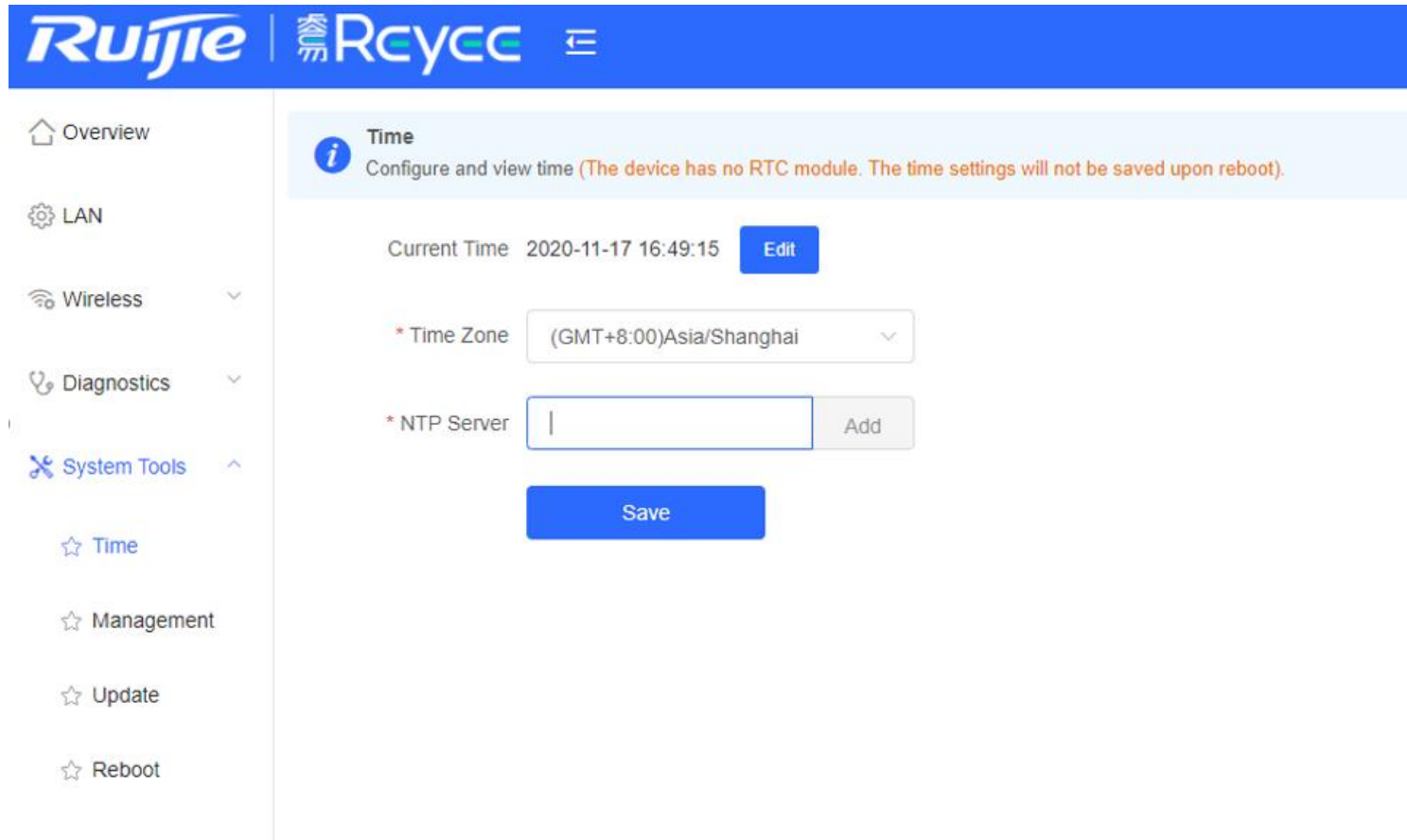
Note: The distance does not refer to the actual physical distance. For example, if there are obstructions at a distance of 1KM, the performance requirements can be met by increasing the distance to 2KM



The screenshot shows the Ruijie RCYCC web interface for configuring WDS parameters. The left sidebar contains navigation options: Overview, LAN, Wireless, WDS (selected), Region, Diagnostics, and System Tools. The main content area is titled 'WDS--VCR (AP)' and includes a 'Configure WDS parameters.' instruction. Under the 'WDS' section, there is a field for '\* WDS SSID' with the value '@Ruijie-wds-a4cc' and a 'Scan' button. A blue 'Save' button is positioned below. The 'Channel & Transmit Power' section includes dropdown menus for '5G Channel' (56 (5.28Ghz)), 'Channel Width' (40MHz), and 'Transmit Power' (Auto). An 'Interference' icon is visible next to the 5G Channel dropdown. The 'Distance' dropdown is currently open, showing options for 1KM, 2KM, and 3KM.

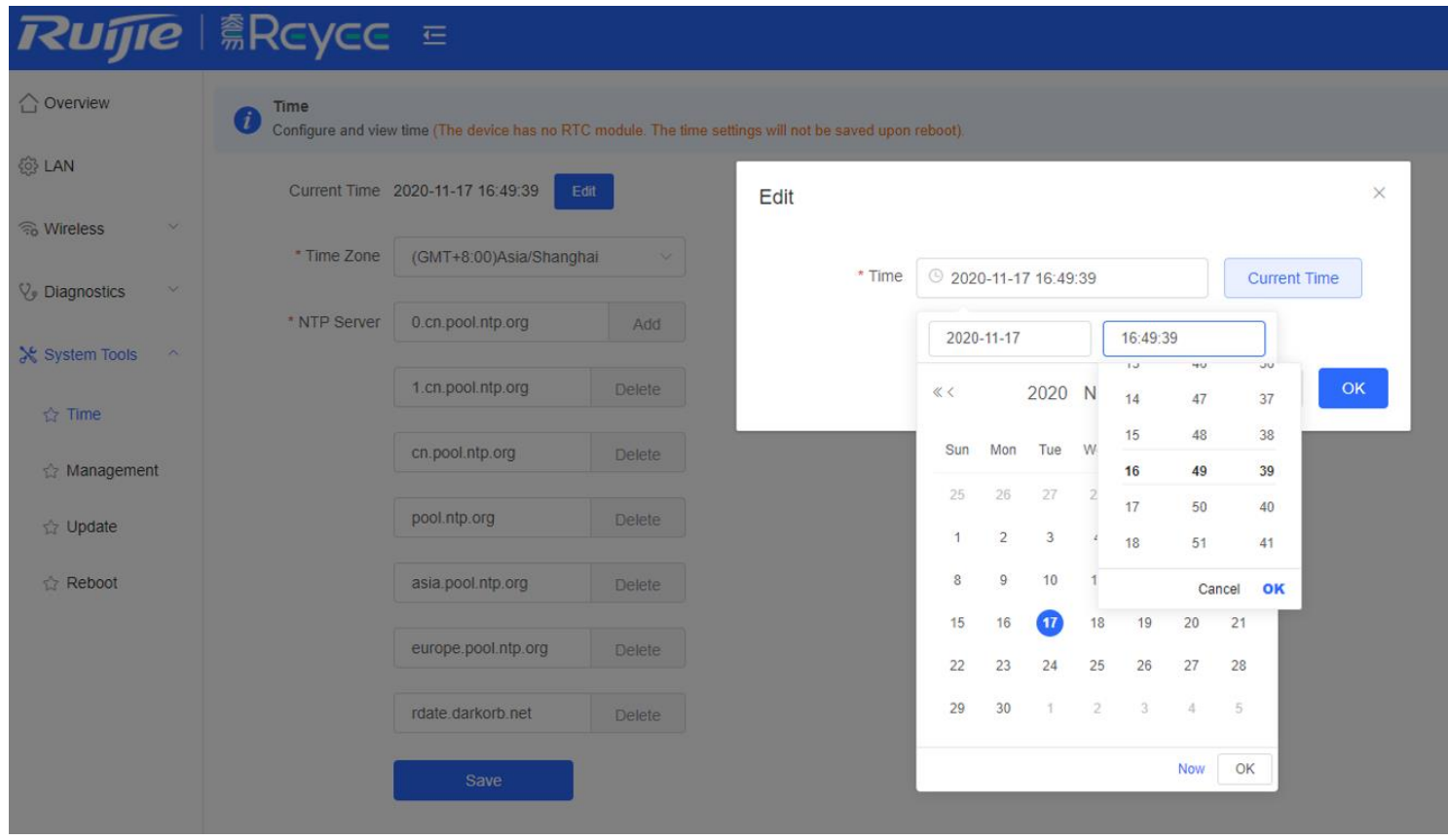
## 9.5 System Setting

Choose System Tools → Time, change the time and NTP server



The screenshot shows the Ruijie Rcycc web interface. The top navigation bar includes the Ruijie and Rcycc logos. On the left, a sidebar menu lists: Overview, LAN, Wireless, Diagnostics, System Tools, Time (selected), Management, Update, and Reboot. The main content area is titled "Time" and contains the following elements:

- Information icon and title: **Time**
- Sub-header: Configure and view time (The device has no RTC module. The time settings will not be saved upon reboot).
- Current Time: 2020-11-17 16:49:15 with an **Edit** button.
- Time Zone: A dropdown menu showing (GMT+8:00)Asia/Shanghai.
- NTP Server: A text input field with an **Add** button.
- A large **Save** button at the bottom.



This screenshot shows the same Ruijie Rcycc interface as above, but with an "Edit" dialog box open. The background is dimmed. The dialog box contains:

- Title: **Edit**
- \* Time: A text input field containing "2020-11-17 16:49:39" and a **Current Time** button.
- A date and time picker showing "2020-11-17" and "16:49:39".
- A calendar view for November 2020, with the 17th highlighted.
- Buttons for **OK**, **Cancel**, and **Now**.

In the background, the Time configuration page is visible with the following changes:

- Current Time: 2020-11-17 16:49:39
- \* NTP Server: A list of servers with **Delete** buttons:
  - 0.cn.pool.ntp.org
  - 1.cn.pool.ntp.org
  - cn.pool.ntp.org
  - pool.ntp.org
  - asia.pool.ntp.org
  - europa.pool.ntp.org
  - rdate.darkorb.net
- A **Save** button at the bottom.

Choose System Tools → Management, support backup and import setup, reset the device and set the session timeout













The screenshot displays the Ruijie RCYCC web management interface. The top navigation bar is blue with the Ruijie and RCYCC logos. A left sidebar contains menu items: Overview, LAN, Wireless, Diagnostics, System Tools (highlighted), Time, Management, Update, and Reboot. The main content area has three tabs: Backup & Import (active), Reset, and Session Timeout. Under the active tab, there is an information message: "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 setup. The device will be rebooted automatically later." Below this, the "Backup Setup" section includes a "Backup Setup" label and a blue "Backup" button. The "Import Setup" section features a "File Path" label, a text input field with the placeholder "Please select a file.", a blue "Browse" button, and a light blue "Import" button.

The screenshot shows the Ruijie Rcycc web interface. The top navigation bar is blue with the Ruijie logo and Rcycc logo. The left sidebar contains navigation items: Overview, LAN, Wireless, Diagnostics, System Tools, Time, Management, Update, and Reboot. The main content area has tabs for Backup & Import, Reset, and Session Timeout. The Session Timeout tab is active, showing a configuration section with an information icon and the text "Session Timeout". Below this, there is a field for "\* Session Timeout" with the value "3600" and the unit "Sec". A blue "Save" button is positioned below the field.


Choose **System Tools** → **Upgrade**, support online upgrade, local upgrade and update all the devices in the network

The screenshot shows the Ruijie Rcycc web interface. The top navigation bar is blue with the Ruijie logo and Rcycc logo. The left sidebar contains navigation items: Overview, LAN, Wireless, Diagnostics, System Tools, Time, Management, Update, and Reboot. The main content area has tabs for Online Update, Local Update, and Update All Devices. The Online Update tab is active, showing a configuration section with an information icon and the text "Online Update". Below this, there is a message: "Online update 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 update." and "Current Version AP\_3.0(1)B2P28\_Release(07210111) (Your version is the latest.)".



-  Overview
-  LAN
-  Wireless 
-  Diagnostics 
-  System Tools 
-  Time
-  Management
-  Update
-  Reboot

Online Update   Local Update   Update All Devices

 **Local Update**  
Please do not refresh the page or close the browser.

Model EST310

Version AP\_3.0(1)B2P28,Release(07210111) 1.00

Keep Setup  (If the target version is much later than the current version, it is recommended not to keep the setup)

Update File

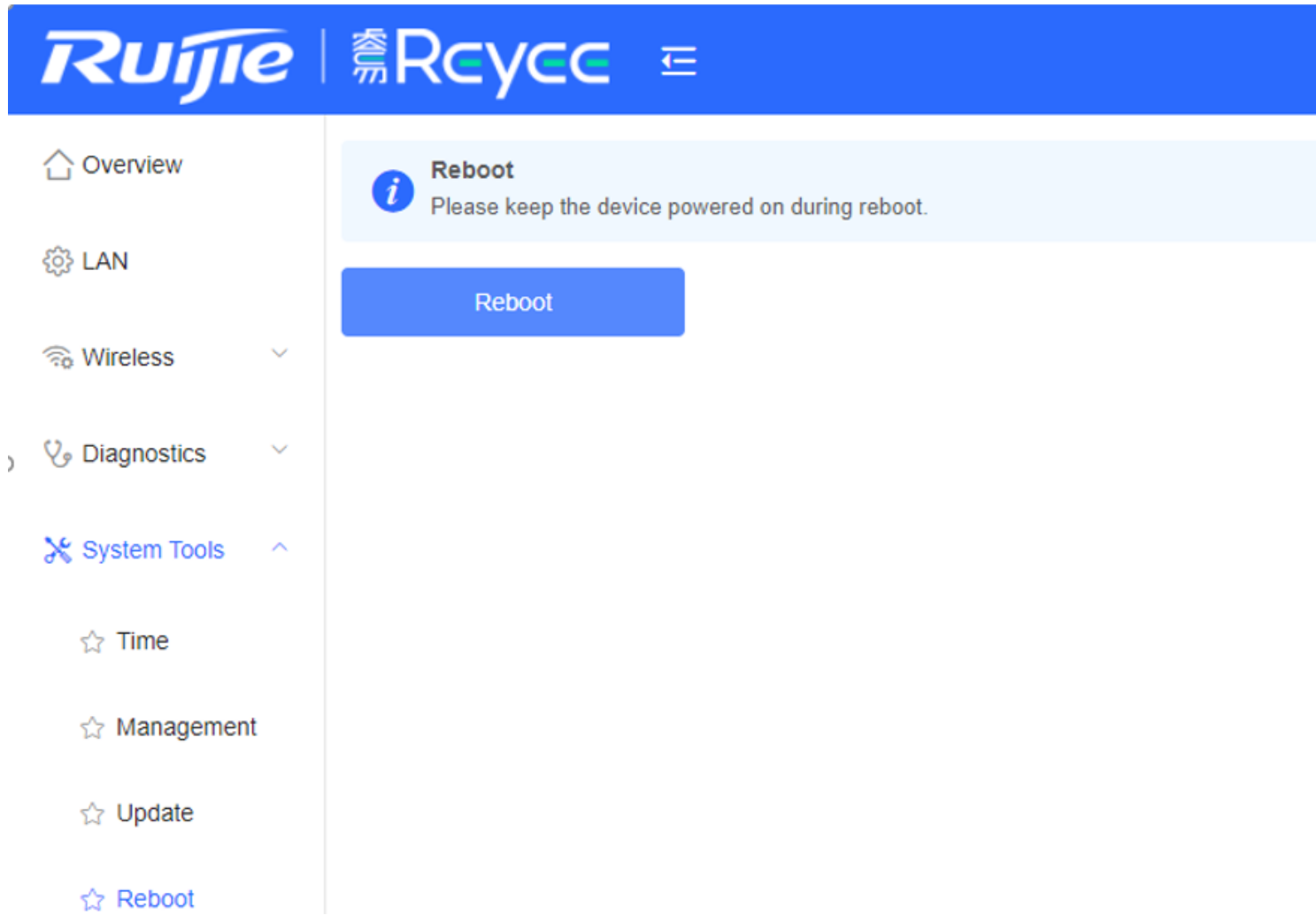
Select

Browse

Upload

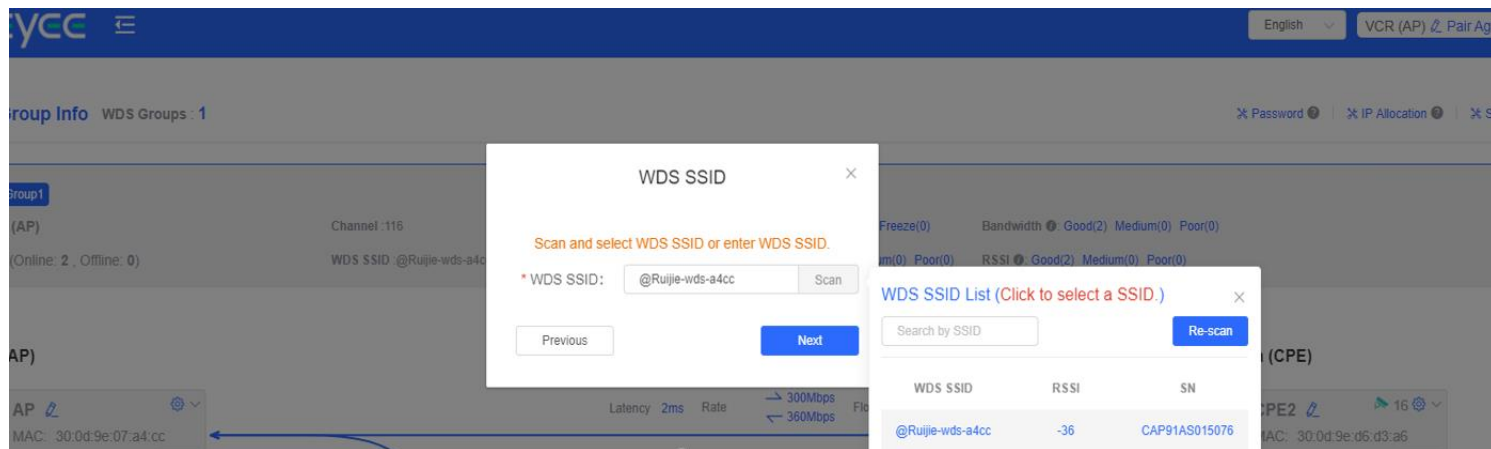
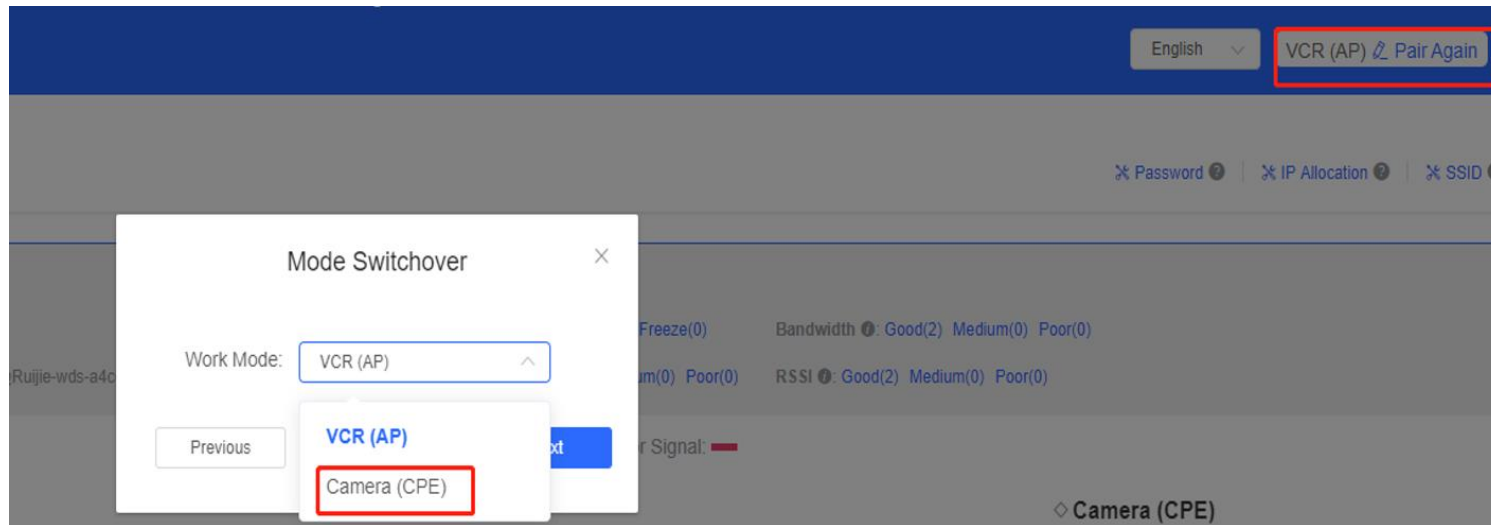
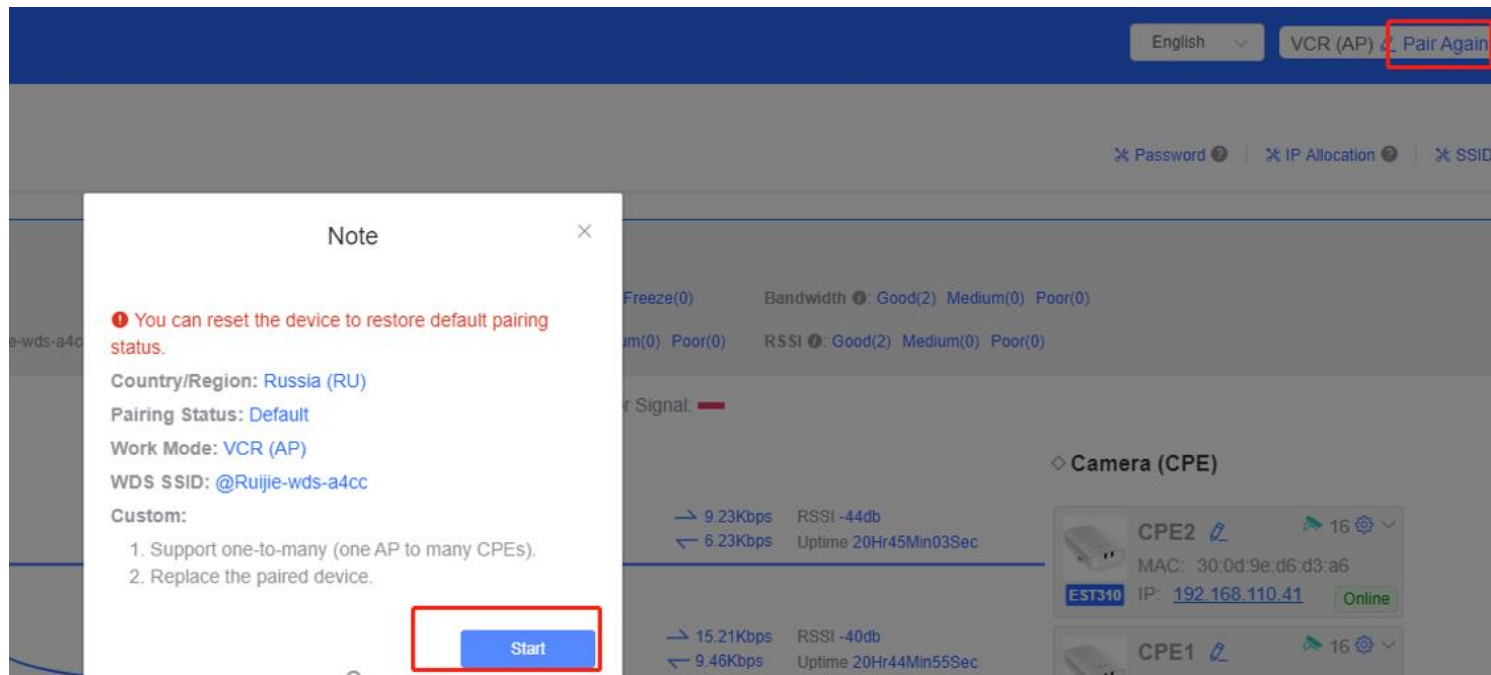
The screenshot shows the Ruijie RCYCC web interface. The top navigation bar is blue with the Ruijie logo and RCYCC text. A left sidebar contains navigation items: Overview, LAN, Wireless, Diagnostics, System Tools, Time, Management, Update, and Reboot. The main content area has three tabs: Online Update, Local Update, and Update All Devices. The 'Update All Devices' tab is active and displays a notification: 'Update All Devices' with the instruction 'Update all devices in the network. Please do not refresh the page or close the browser.' Below the notification, the device model is listed as 'EST310' and the version as 'AP\_3.0(1)B2P28,Release(07210111) 1.00'. There is a 'Keep Setup' checkbox which is checked and labeled '(Uneditable)'. At the bottom, there is an 'Update File' section with a 'Select' button, a 'Browse' button, and an 'Upload' button.

Choose **System Tools** → **Reboot** to reboot the device



## 9.6 PTMP setting

Access to the device, if the device mode is AP, need to switch to CPE mode



Access to the device, if the mode is CPE, no need to switch mode

Alarm

Configuration is uninitialized.

Hostname Not Set: 1

Admin Password Not Set: 1. Click [here](#) to change the password.

Country/Region: China (CN)

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

WDS Group Info WDS Groups : 1

Password IP Allocation

Local

WDS Group1

AP: 0 (-)

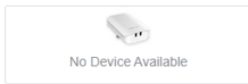
Channel --

CPE: 1 (Online: 0, Offline: 1)

WDS SSID --

Strong Signal: Medium Signal: Poor Signal:

VCR (AP)



Camera (CPE)

Local Ruijie  
MAC: 30:0d:9e:d6:d3:a6  
EST310 IP: 10.44.77.254 Offline



Choose **Wireless** → **WDS**, scan the SSID list and select a SSID, click **Save**

**WDS--Camera (CPE)**  
Configure WDS parameters.

**WDS**

\* WDS SSID

WDS SSID List (Click to select a SSID.)

WDS SSID	RSSI	SN
@Ruijie-wds-a4cc	-37	CANA27K001708

**Channel & Transmit Power**

5G Channel

Channel Width

In CPE mode, the local channel and channel

Transmit Power

Distance

**WDS--Camera (CPE)**  
Configure WDS parameters.

**WDS**

\* WDS SSID: @Ruijie-wds-a4cc [Scan]

[Save]

**Channel & Transmit Power**

5G Channel: Auto [Interference]

Channel Width: 40MHz

In CPE mode, the local channel and channel width are consistent.

Transmit Power: Auto

Distance: 1KM

[Save]

**Tip**

The network service will be unavailable for a while. Do you want to continue?

[Cancel] [OK]

PTMP success and show the actual topo on the overview

**Alarm**

Configuration is uninitialized.

Hostname Not Set: 3

Country/Region: China (CN)

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

**WDS Group Info** WDS Groups : 1

Local

**WDS Group1**

AP: 1 (Ruijie) Channel: 52 Latency: Fluent(2) Jitter(0) Freeze(0) Bandwidth: Good(2) Medium(0) Poor(0)

CPE: 2 (Online: 2, Offline: 0) WDS SSID: @Ruijie-wds-a4cc Interference: Good(2) Medium(0) Poor(0) RSSI: Good(2) Medium(0) Poor(0)

Strong Signal: [Blue] Medium Signal: [Orange] Poor Signal: [Red]

**VCR (AP)**

Ruijie  
MAC: 30:0d:9e:07:a4:cc  
EST310 IP: 10.44.77.254 Online

Latency: 2ms Rate: 400Mbps/400Mbps Flow: 11.77Kbps/7.62Kbps RSSI: -39db Uptime: 49Min31Sec

**Camera (CPE)**

Ruijie  
MAC: 30:0d:9e:d6:d3:a6  
EST310 IP: 10.44.77.254 Online

Ruijie  
MAC: 30:0d:9e:07:a9:88  
EST310 IP: 10.44.77.254 Online

Latency: 4ms Rate: 400Mbps/400Mbps Flow: 12.58Kbps/8.05Kbps RSSI: -43db Uptime: 03Hr12Min18Sec

**Alarm**  
Configuration is uninitialized.  
Hostname Not Set: 3  
Country/Region: China (CN)  
Time Zone: (GMT+8:00)Asia/Shanghai

**WDS Group Info** WDS Groups : 1

**WDS Group1**  
AP: 1 (Ruijie) Channel: 52 Latency: Fluent(2) Jitter(0) Freeze(0) Bandwidth: Good(2) Medium(0) Poor(0)  
CPE: 2 (Online: 2, Offline: 0) WDS SSID: @Ruijie-wds-a4cc Interference: Good(2) Medium(0) Poor(0) RSSI: Good(2) Medium(0) Poor(0)

**VCR (AP)**

- Ruijie (EST310) IP: 10.44.77.254 LAN
- WDS
- Reboot

**Camera Count Supported by Current WDS Link**

Camera Type	Count
100W Pixels (Data Rate: 3M)	16
130W Pixels (Data Rate: 5M)	10
200W Pixels (Data Rate: 6M)	8
300W Pixels (Data Rate: 10M)	5

**Camera**

- Ruijie (EST310) IP: 10.44.77.254 Online
- Ruijie (EST310) IP: 10.44.77.254 Online

Latency 2ms Rate → 400Mbps ← 400Mbps Flow → 11.77Kbps ← 7.62Kbps RSSI -39db Uptime 49Min31Sec

Latency 4ms Rate → 400Mbps ← 400Mbps Flow → 12.58Kbps ← 8.05Kbps RSSI -43db Uptime 03Hr12Min18Sec

## 10 EW Series Configuration

### 10.1 Basic Setting

are paired by default and can be used without requiring any configurations.

Quick setup, login to Reyee EWeb (<http://192.168.110.1>) via wired or wireless.





## Welcome to Use Reyee Router

I have read and agreed to [Software License Agreement](#)

Auto upgrade the device when a new version appears

Configure

The default configuration of WAN is DHCP.

---

Internet: DHCP Recommended 

PPPoE **DHCP** Static IP Repeater



You have gained access to the Internet.  
Account is no required.

IP Address  
192.168.1.20

Subnet Mask  
255.255.255.0

Gateway  
192.168.1.1

DNS Server  
8.8.8.8

Previous

Next

Set the WiFi settings, management password, country code and time zone.

**Ruijie** | **Rcycc** **Wizard**

---

### WiFi Settings

Dual-Band Single SSID

\* SSID (2.4G) Large Coverage & Slow Rate

\* SSID (5G) Small Coverage & Fast Rate

\* Wi-Fi Password

**Management Password (Please remember the password.)**

Same as Wi-Fi Password

\* Management Password

**Country/Region/Time Zone**

\* Country/Region

Apply the configuration to device and finish the quick setup.

✦ Applying configuration...17 Sec

SSID (2.4G): @Ruijie-s49FD

SSID (5G): @Ruijie-s49FD\_5G

Wi-Fi Password: \*\*\*\*\* 🔒

+ Add Router



Scan the QR code to download App.

- Simple configuration
- Convenient management
- Smart diagnostics

✦ Finish

### WAN setting

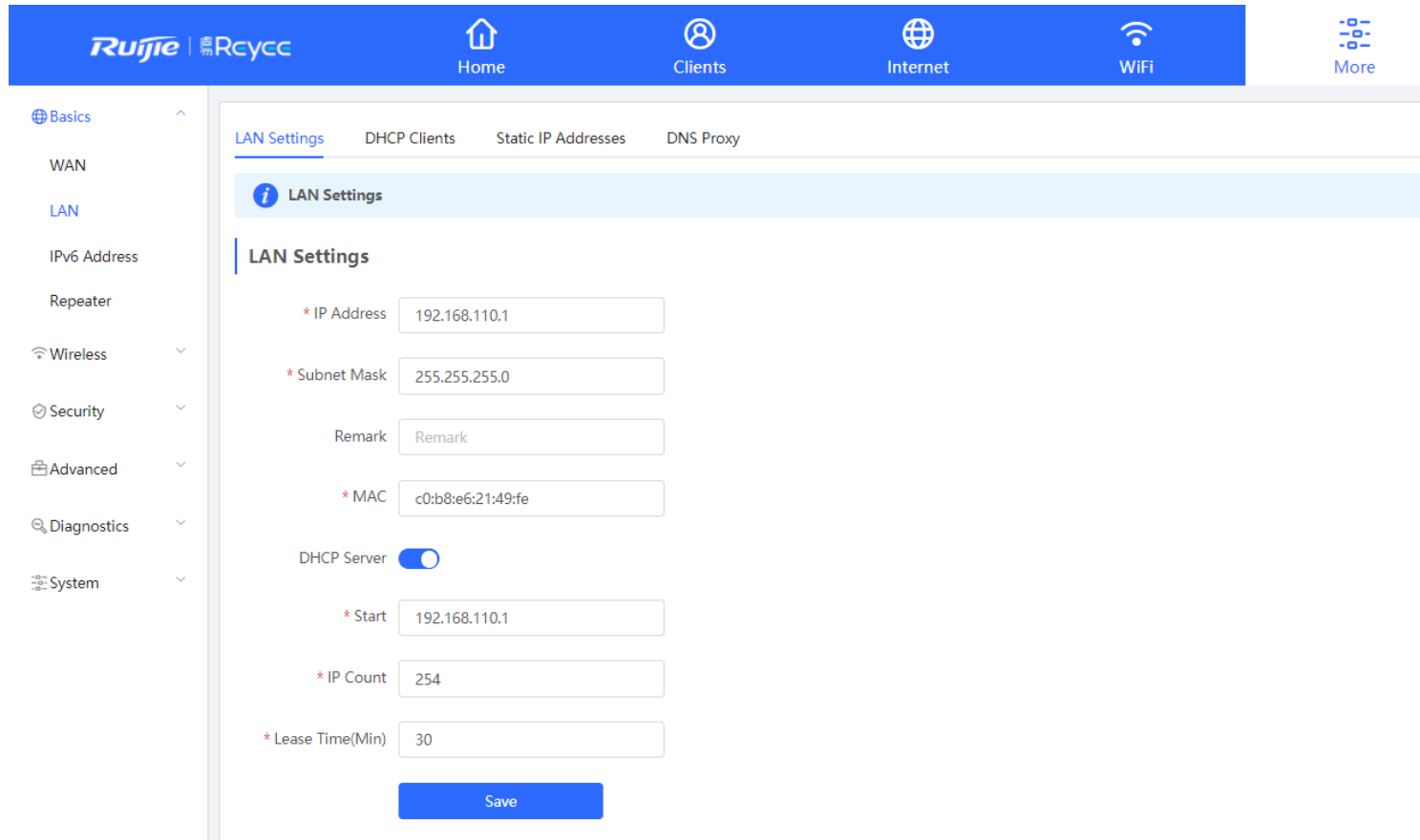
Support DHCP, PPPoE and static IP. Advanced settings including MTU, MAC and 802.1Q tag.

---

The screenshot displays the WAN Settings configuration page in the Ruijie Rcycc web interface. The left sidebar contains navigation options: Basics, WAN, LAN, IPv6 Address, Repeater, Wireless, Security, Advanced, Diagnostics, and System. The main content area is titled 'WAN Settings' and includes an information icon and the instruction 'Configure WAN settings.' The configuration is divided into two sections: Basic Settings and Advanced Settings. In the Basic Settings section, the 'Internet' dropdown is set to 'DHCP', and a note states 'No username or password is required for DHCP clients.' Below this, the IP Address is 192.168.1.20, Subnet Mask is 255.255.255.0, Gateway is 192.168.1.1, and DNS Server is 8.8.8.8. The Advanced Settings section, separated by a dashed line, includes: \* MTU set to 1500 (with a range of 576-1500), \* MAC set to c0:b8:e6:21:49:fd, 802.1Q Tag checked, and \* VLAN ID set to 300. A blue 'Save' button is located at the bottom of the configuration area.

LAN settings

Default IP of LAN is 192.168.100.1 with DHCP server.

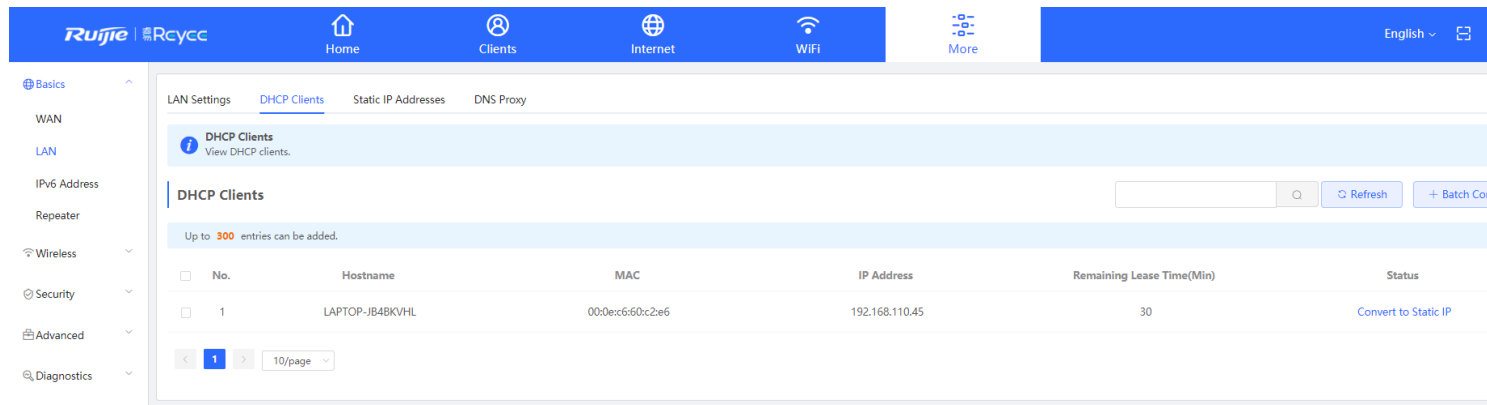


The screenshot shows the Ruijie Rcycc web interface. The top navigation bar includes Home, Clients, Internet, WiFi, and More. The left sidebar lists various configuration categories: Basics, WAN, LAN, IPv6 Address, Repeater, Wireless, Security, Advanced, Diagnostics, and System. The main content area is titled 'LAN Settings' and contains the following fields:

- \* IP Address: 192.168.110.1
- \* Subnet Mask: 255.255.255.0
- Remark: Remark
- \* MAC: c0:b8:e6:21:49:fe
- DHCP Server:
- \* Start: 192.168.110.1
- \* IP Count: 254
- \* Lease Time(Min): 30

A 'Save' button is located at the bottom of the form.

Convert the DHCP clients to static IP on DHCP clients.

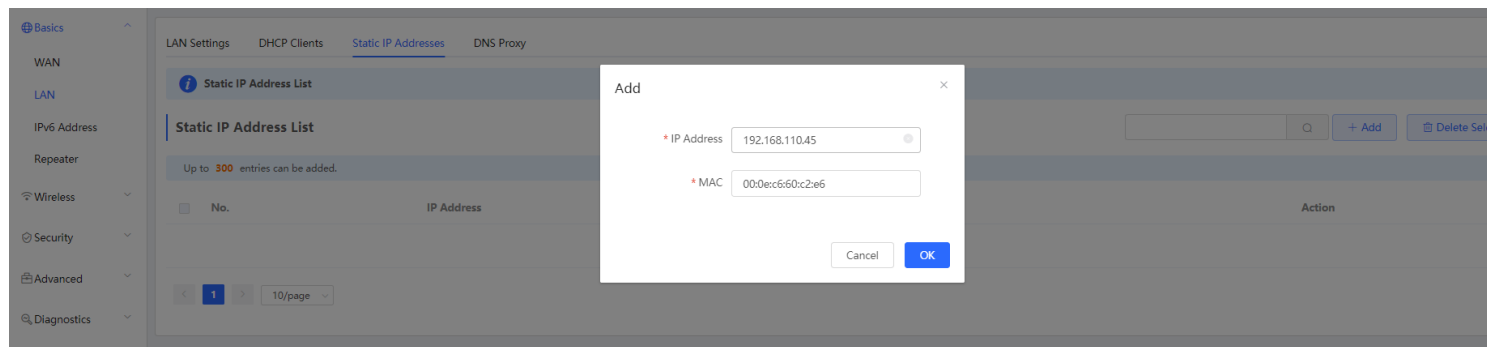


The screenshot shows the 'DHCP Clients' page in the Ruijie Rcycc interface. It features a table with the following columns: No., Hostname, MAC, IP Address, Remaining Lease Time(Min), and Status. The table contains one entry:

No.	Hostname	MAC	IP Address	Remaining Lease Time(Min)	Status
1	LAPTOP-JB4BKVHL	00:0e:c6:60:c2:e6	192.168.110.45	30	<a href="#">Convert to Static IP</a>

Below the table, there is a pagination control showing '1' of 10 entries per page. The page also includes search, refresh, and batch conversion buttons.

Add the static IP address, up to 300 entries can be added.



The screenshot shows the 'Static IP Address List' page in the Ruijie Rcycc interface. An 'Add' dialog box is open, allowing the user to add a new static IP address. The dialog contains the following fields:

- \* IP Address: 192.168.110.45
- \* MAC: 00:0e:c6:60:c2:e6

The dialog has 'Cancel' and 'OK' buttons at the bottom.

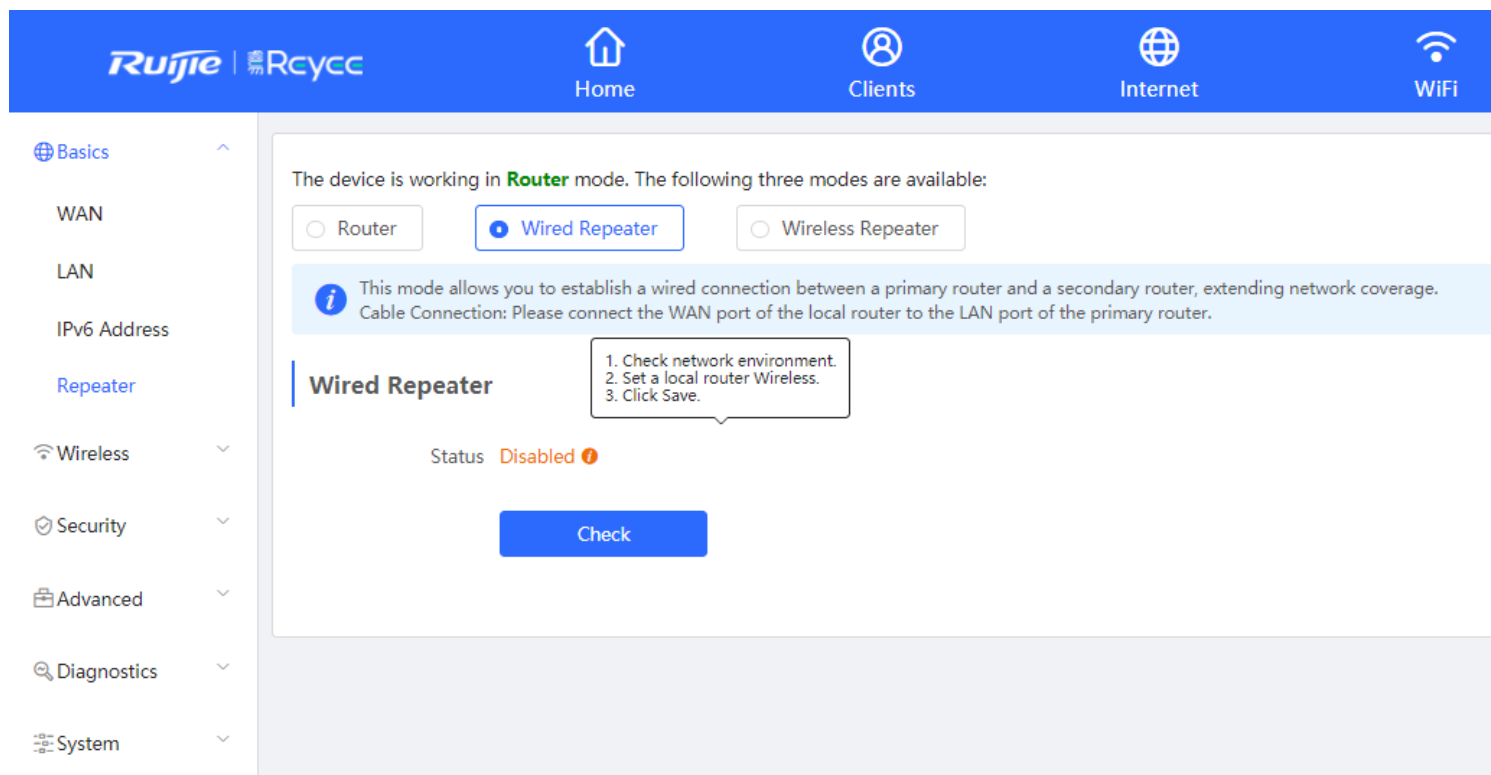
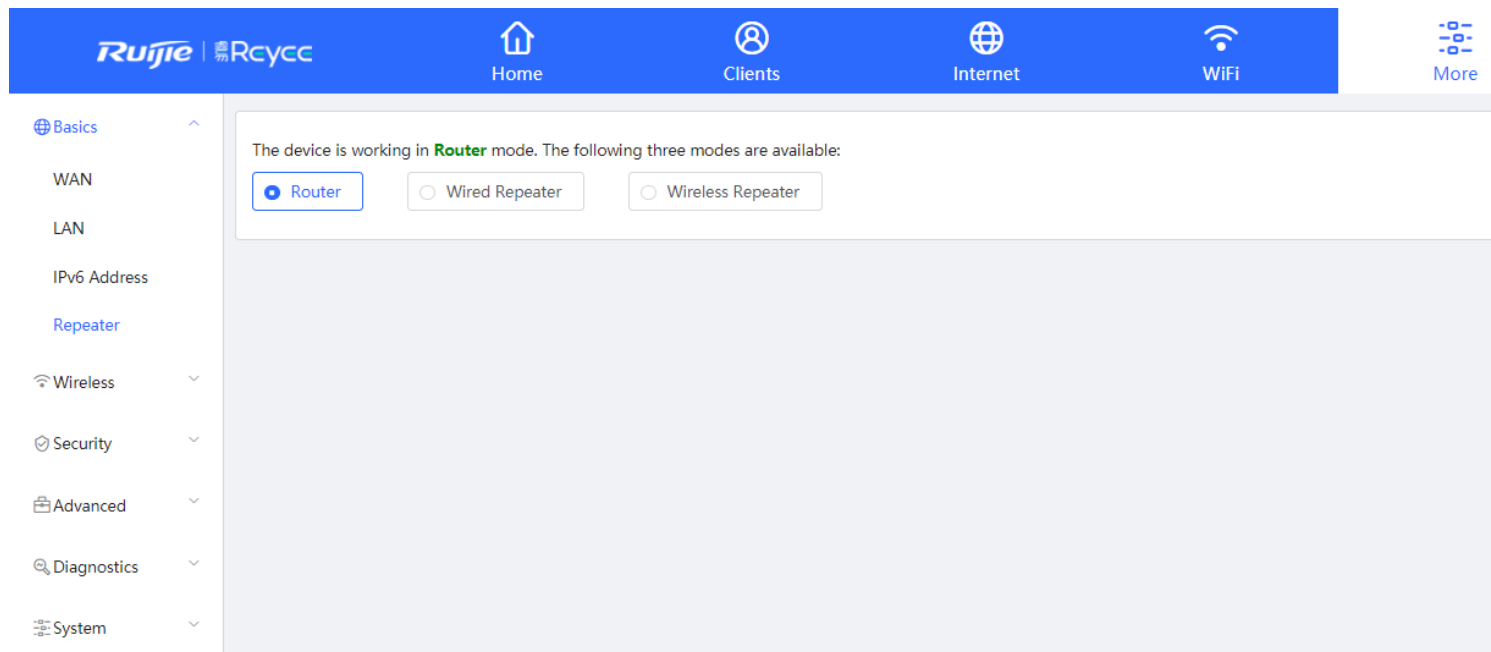
### Repeater settings

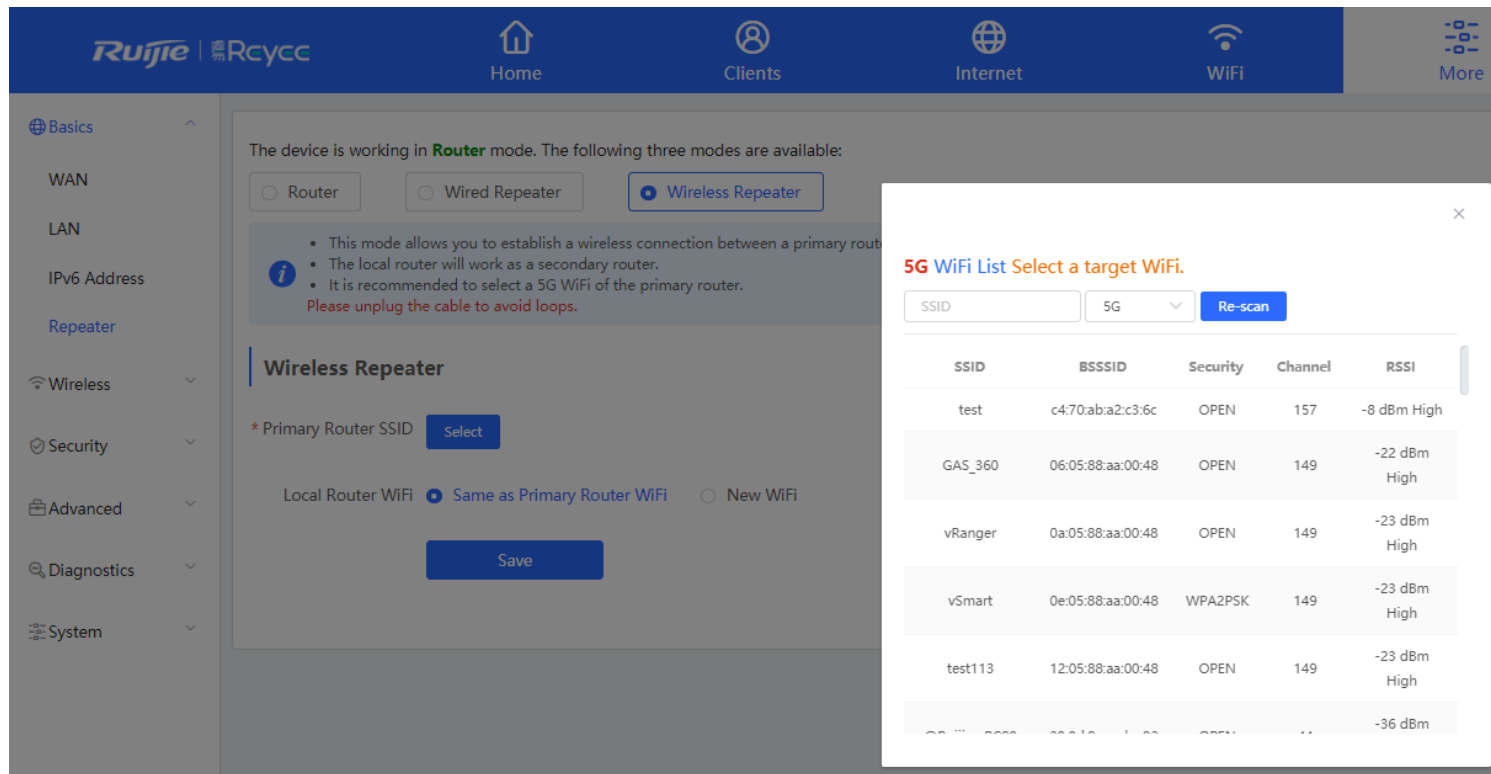
EW support 2 mode, Router, Wired repeater and Wireless repeater.

Router: The default mode of EW, support Reyee Mesh.

Wired repeater: Allows you to establish a wired connection between a primary router and a secondary router, extending network coverage.

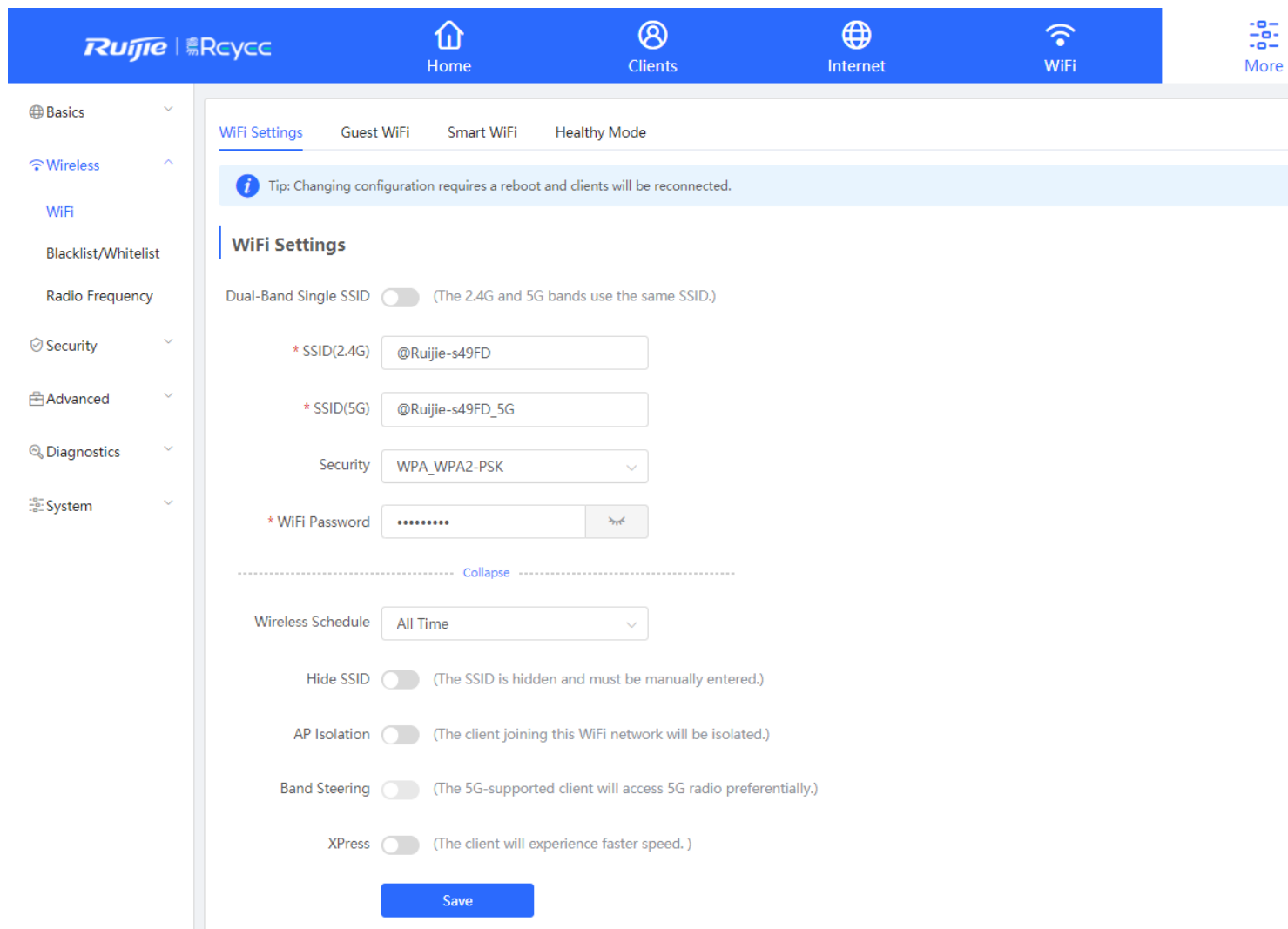
Wireless repeater: Allows you to establish a wireless connection between a primary router and a secondary router, extending network coverage. It is recommended to select a 5G WiFi of the primary router.





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





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

**Dual-band Single SSID:** Choose the radio which the following setting will be applied to. Both 2.4GHz and 5GHz radio will be applied by default.

**Security:** Choose the encryption mode.

**Wireless schedule:** Choose the time period that the Wi-Fi signal will be broadcasted.

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

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

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

**Xpress:** The client will experience faster speed.

## 10.2 Blacklist/Whitelist

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

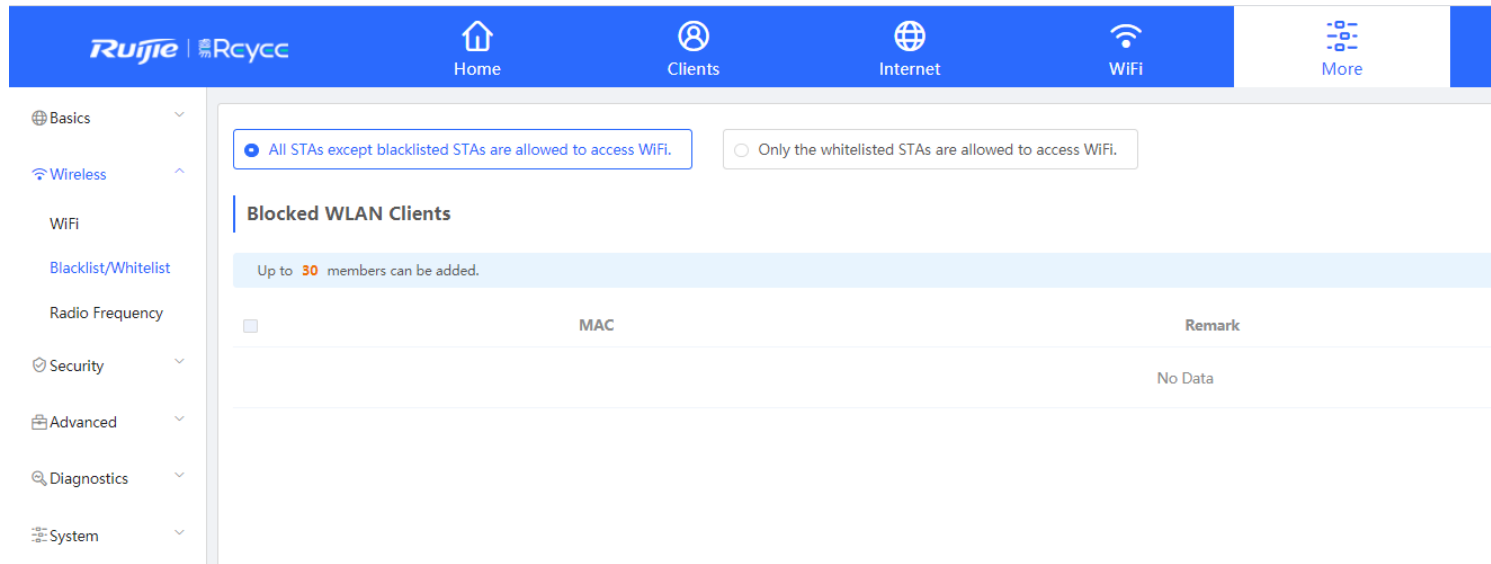
**Blacklist:** All STAs except blacklisted STAs are allowed to access Wi-Fi.

**Whitelist:** Only the whitelisted STAs are allowed to access WiFi.

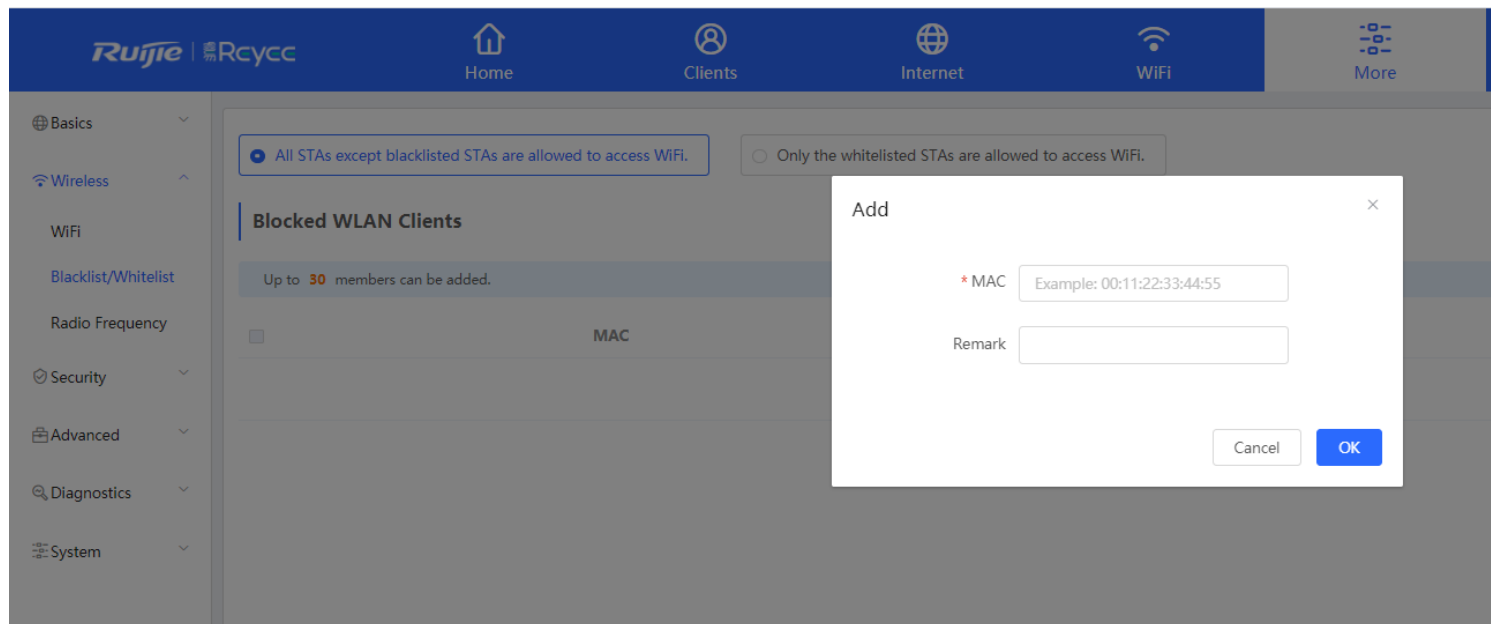
The blacklist and whitelist take effect based on the whole network based or SSID based blacklist/whitelist are not supported.

### Configuration Steps

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



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



## 10.3 DDNS

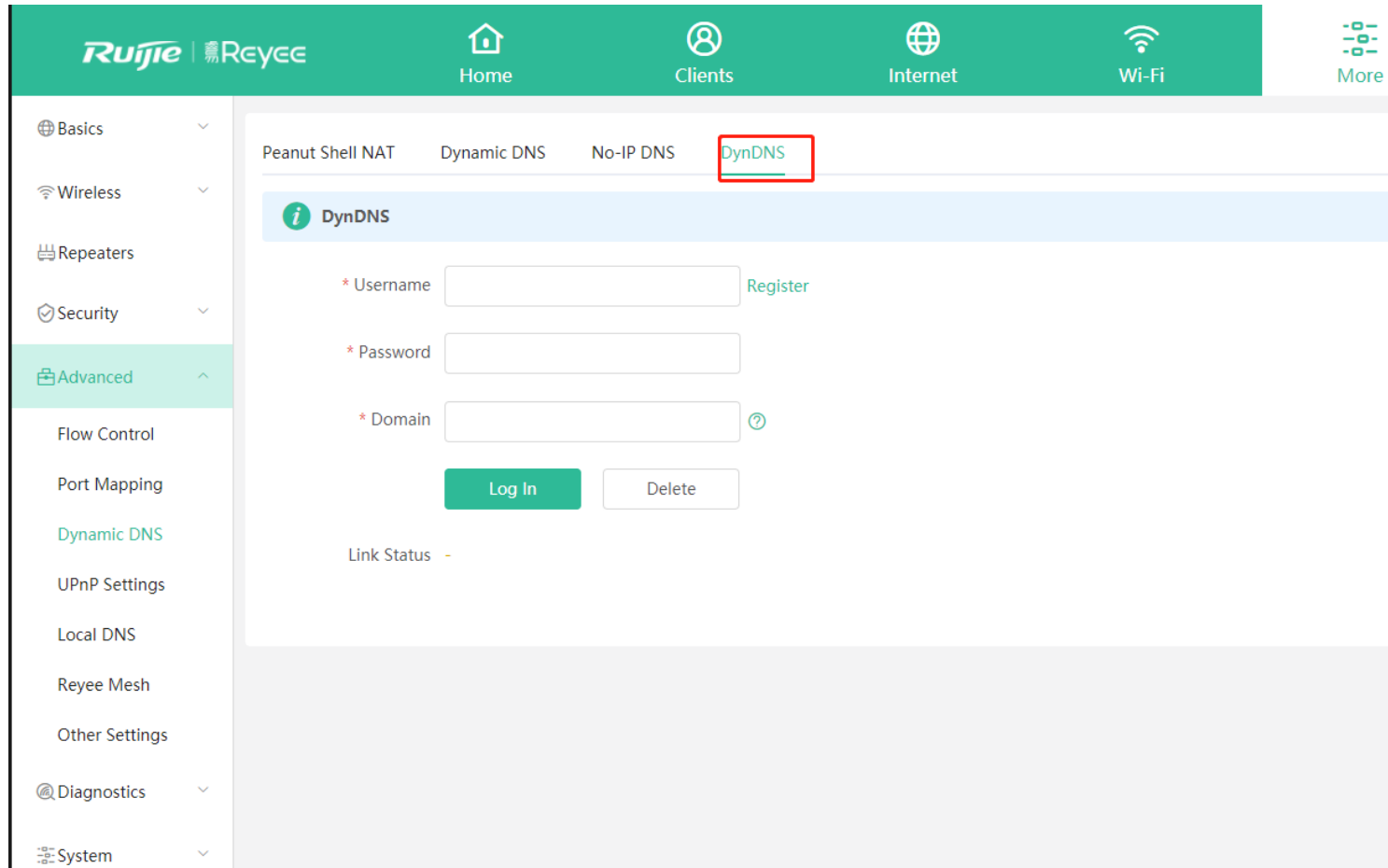
Step 1: Register the account on <https://www.noip.com/sign-up> and set the domain

The screenshot shows the Ruijie Reyee web management interface. At the top, there is a navigation bar with icons for Home, Clients, Internet, Wi-Fi, and More. On the left, a sidebar menu lists various settings categories: Basics, Wireless, Repeaters, Security, Advanced (highlighted), Flow Control, Port Mapping, Dynamic DNS, UPnP Settings, Local DNS, Reyee Mesh, Other Settings, Diagnostics, and System. The main content area is titled 'No-IP DNS' and includes sub-tabs for Peanut Shell NAT, Dynamic DNS, No-IP DNS (selected), and DynDNS. The 'No-IP DNS' section contains a form with the following fields: a required 'Username' field with a 'Register' link, a required 'Password' field, and a 'Domain' field with a help icon. Below the form are 'Log In' and 'Delete' buttons. At the bottom of the form, there are labels for 'Link Status' and 'Domain', both followed by a hyphen, indicating they are currently inactive or empty.

Step 2: Input the username, password and domain

Step 3: Check the link status

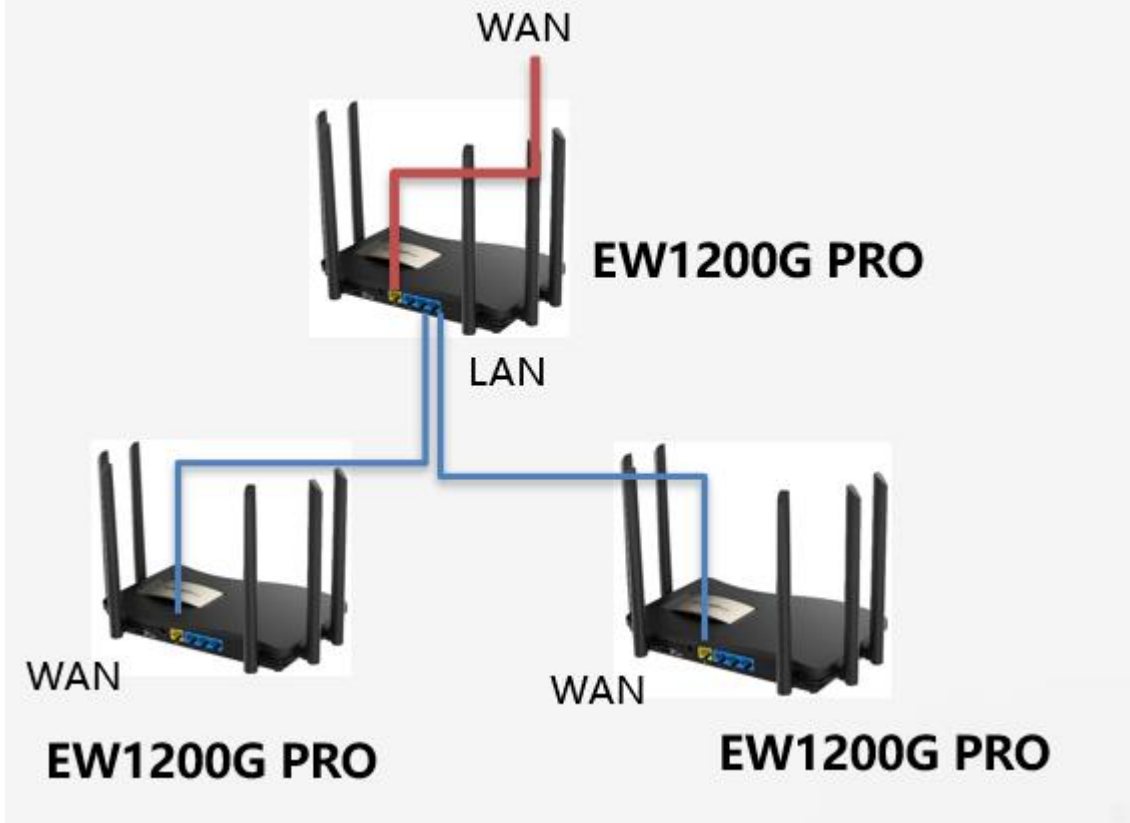
Step 4: Support dynDns



## 10.4 MESH

### Wired MESH

Topology:



Configuration steps:

By default, EW1200G-Pro is enabled with Mesh. When the WAN port of EW1200G-Pro is connected, it will automatically identify whether the uplink is an EW1200G-Pro LAN port. If it is, the EW1200G-Pro will automatically change from route mode to mesh mode.

If the topology is connected, the network will be automatically connected after the connection is completed, and all the device indicators will turn on (about 5 minutes)

**Wireless MESH**

---

### Topology:



1) Master must meet two conditions:

- ① Finish the quick setup
- ② The WAN port is connected and the interface indicator is on.

2) Slave must meet two conditions:

- ① Slave is the factory state;
- ② Slave is within 3 meters from the master and is unobstructed (ensure the signal strength is above -35)

3) Both the master and slave are powered on

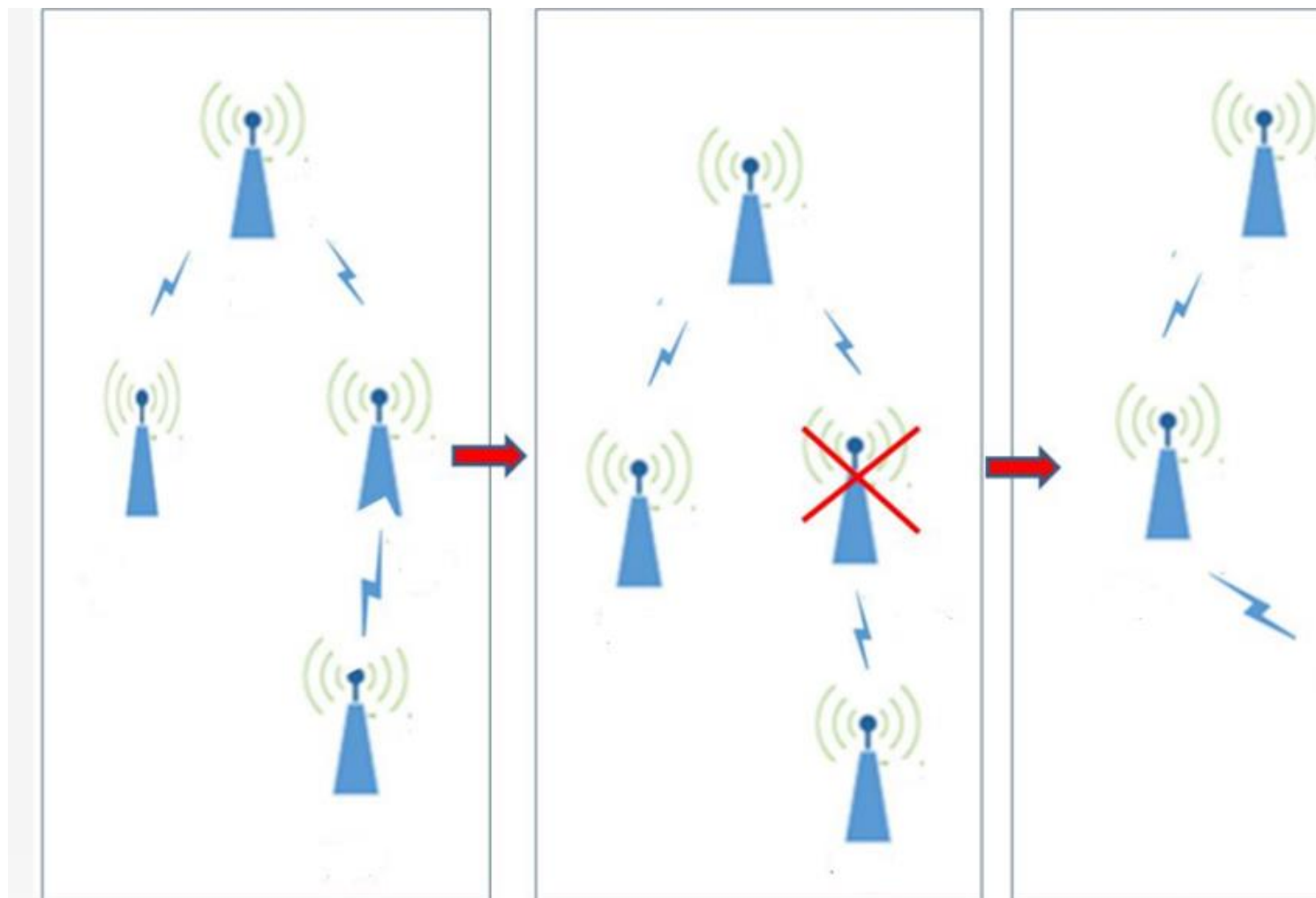
Press the reset button of the master, and the indicator light will flash quickly

After 1-3S, the slave indicator will start to flash quickly. After the indicator lights of the slave and slave are always on again, the wireless mesh is successful.

Then take the slave to the place where you need to use it and wait for the indicator light to stay on.

### Self-recovery

---



## 11 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

9-57

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.

---



