Reyee Series Implementation Cookbook

Cookbook

Document Version: V1.0
Date: 2022.04.29
Copyright © 2022 Ruijie Networks

Copyright

Copyright © 2022 Ruijie Networks

All rights are reserved in this document and this statement.

Without the prior written consent of Ruijie Networks, any organization or individual shall not reproduce, extract, back up, modify, or propagate the content of this document in any manner or in any form, or translate it into other languages or use some or all parts of the document for commercial purposes.

and other Ruijie networks logos are trademarks of Ruijie Networks.

All other trademarks or registered trademarks mentioned in this document are owned by their respective owners.

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms, and some or all of the products, services, or features described in this document may not be available for you to purchase or use. Except for the agreement in the contract, Ruijie Networks makes no explicit or implicit statements or warranties with respect to the content of this document.

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

This manual is designed merely as a user guide. Ruijie Networks has tried its best to ensure the accuracy and reliability of the content when compiling this manual, but it does not guarantee that the content of the manual is completely free of errors or omissions, and all the information in this manual does not constitute any explicit or implicit warranties.

Preface

Intended Audience

This document is intended for:

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

Technical Support

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

Conventions

1. GUI Symbols

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

2. Signs

This document also uses signs to indicate some important points during the operation. The meanings of these signs are as follows:

Warning

An alert that calls attention to important rules and information that if not understood or followed can result in data loss or equipment damage.

Note

An alert that calls attention to essential information that if not understood or followed can result in function failure or performance degradation.

Instruction

An alert that contains additional or supplementary information that if not understood or followed will not lead to serious consequences.

Specification

An alert that contains a description of product or version support.

3. Instruction

This manual is used to guide users to understand the product, install the product, and complete the configuration.

The example of the port type may be different from the actual situation. Please proceed with configuration according to the port type supported by the product.

The example of display information may contain the content of other product series (such as model and description). Please refer to the actual display information.

The routers and router product icons involved in this manual represent common routers and layer-3 switches running routing protocols.

Contents

1 Product Introduction

1.1 Reyee Gate Series Router

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 Router realizes the industry-leading auto-discovery and auto-networking features for gateways, switches and wireless.

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

1.1.1 Product List

Model	10/100/1000 Base-T Ethernet Port	Maximum number of clients	Recommended bandwidth	Management capacity
RG-EG105G-P	5(Support POE)	Up to 100 concurrent clients	500M asymmetric bandwidth (flow control disabled) 300M asymmetric bandwidth (flow control enabled)	In AC mode, the maximum management capacity is 300 In gateway mode, the maximum management capacity is 32
RG-EG105G-P V2	5(Support POE)	Up to 100 concurrent clients	600M asymmetric bandwidth (flow control disabled) 500M asymmetric bandwidth (flow control enabled)	In AC mode, the maximum management capacity is 300 In gateway mode, the maximum management capacity is 32
RG-EG105G	5	Up to 100 concurrent clients	500M asymmetric bandwidth (flow control	In AC mode, the maximum management

			disabled) 300M asymmetric bandwidth (flow control enabled)	capacity is 300 In gateway mode, the maximum management capacity is 32
RG-EG105G V2	5	Up to 100 concurrent clients	600M asymmetric bandwidth (flow control disabled) 500M asymmetric bandwidth (flow control enabled)	In AC mode, the maximum management capacity is 300 In gateway mode, the maximum management capacity is 32
RG-EG105GW	5	Up to 100 concurrent clients Recommended number of wireless terminals: 60	500M asymmetric bandwidth (flow control disabled) 300M asymmetric bandwidth (flow control enabled)	In gateway mode, the maximum management capacity is 32
RG-EG210G-E	10	Up to 200 concurrent clients	1Gbps asymmetric bandwidth (flow control disabled) 1Gbps asymmetric bandwidth (flow control enabled)	In AC mode, the maximum management capacity is 500 In gateway mode, the maximum management capacity is 150
RG-EG210G-P	10(Support POE)	Up to 200 concurrent clients	600M asymmetric bandwidth (flow control disabled) 500M asymmetric bandwidth (flow control enabled)	In AC mode, the maximum management capacity is 500 In gateway mode, the maximum management capacity is 150

1.1.2 LED Indicator

LED Indicator	Description
SYS	Blinking green (0.5Hz): The device has started up, but is not connected to the Ruijie Cloud. Solid green: The device has started up, and is connected to the Ruijie Cloud. Blinking green (10Hz): The device is starting up/shutting down.
Speed	Solid green: the port is connected at 10/100/1000 Mbps. Off: the port is not connected at 10/100/1000 Mbps.

1.1.3 Button

Button	Description
Reset	Press reset button until the status LED blinks green at 10Hz to restore the device to the factory default setting. The default management IP address is http://192.168.110.1.

1.2 Reyee ES Switch

Ruijie Reyee smart surveillance switches offer a variety of port options to meet the needs of video surveillance networks of different scales. Ruijie Reyee smart surveillance switches support full-power PoE output to ensure that all cameras can be powered simultaneously when connected to the switch at maximum capacity. In addition, Ruijie Real-easy Series smart surveillance switches provide simple and easy-to-use management features while offering plug and play with default factory configuration, which can quickly locate the surveillance network faults, initiate PoE port restart, perform VLAN configuration, etc. Ruijie Cloud app and Ruijie Cloud platform remote management is also supported, making the operation and maintenance of the surveillance network easier and more convenient, while reducing operation and maintenance costs.

1.2.1 Product List

RG-ES200 Series Switches

Model	10/100 Base-T Auto-sensing Ethernet Port	10/100/1000 Base-T Auto-sensing Ethernet Port	1000Base-X SFP Port	Console Port
RG-ES205GC-P	N/A	5 (Ports 1-4 support PoE+/PoE)	N/A	N/A
RG-ES209GC-P	N/A	9 (Ports 1-8 support PoE+/PoE)	N/A	N/A
RG-ES218GC-P	N/A	16 (Support PoE+/PoE)	2	N/A

RG-ES226GC-P	N/A	24 (Support PoE+/PoE)	2	N/A
RG-ES224GC	N/A	24	N/A	N/A
RG-ES216GC	N/A	16	N/A	N/A

The SPF ports cannot be downward compatible with 100Base-FX.
1000Base-T is compatible with 100Base-TX and 10Base-T in the downlink direction.

1.2.2 LED Indicator

LED	State	Meaning
System status LED	Off	The switch is not receiving power.
	Blinking green	The PoE power exceeds the power of the entire device (370 W). The new connected PD cannot be powered up due to insufficient power. The switching function is operational.
	Solid green	The switch is operational.
RJ45 port PoE status LED	Off	PoE is not enabled.
	Solid green	PoE is enabled. The port is operational.
	Blinking green	Indicates PoE overload.
1000Mbps RJ-45 port status LED	Off	The port is not connected.
	Solid green	The port is connected at 10/100/1000 Mbps.
	Blinking green	The port is receiving or transmitting traffic at 10/100/1000 Mbps.
SFP port status LED	Off	The port is not connected.
	Solid green	The port is connected at 1000 Mbps.
	Blinking green	The port is receiving or transmitting traffic at 1000 Mbps.

1.2.3 Button

Botton	Description
Port mode LED Switch-Over button	When the button is turned to the left position (Mode 1), the LED indicates the switching status of the port: when the LED is solid green, it indicates that the link is up; when the LED blinks green, data is being transmitted or received. When the button is turned to the right position (Mode 2), the LED indicates the PoE status of ports: when the LED is solid green, it indicates that the PoE-supported ports are supplying power; when the LED blinks green, the power of the ports is overloaded.

System reset button	The switch reboots after the reset button is pressed for less than 2 seconds. The switch restores the default factory settings after the reset button is pressed for more than 5 seconds (until the status LED blinks).

1.3 Reyee NBS Switch

Reyee RG-NBS3100 series of managed switches are Reyee's 4 switches tailored for SME customer applications, which can meet the different levels of network access needs of SME customers. Covering basic VLAN division and advanced security features such as ACL,etc. The model with the suffix '-P' is a model that supports PoE output, and can meet the PoE power supply requirements of wireless APs, digital cameras and other devices in various occasions.

RG-NBS3200 series switch is a new generation of high-performance, strong security and integrated multi-service layer 2 Ethernet switch launched by Reyee. This series of switches adopts an efficient hardware architecture design, providing larger entry specifications and faster Hardware processing performance, more convenient operation experience. The RG-NBS3200 series provides flexible Gigabit access to 10 Gigabit uplink ports. The entire series of switches all have 4-port 10 Gigabit optical and high-performance port uplink capabilities.

Ruijie RG-NBS5100&5200 Series Switches are the next-generation high-performance, high-security and multi-service Layer 3 Ethernet switches. Adopting an efficient hardware architecture design, this switch series provides larger MAC address table size, faster hardware processing performance, and more convenient operating experience. RG-NBS5100 series provides Gigabit access and Gigabit uplink, while RG-NBS5200 series provides Gigabit access and 10G uplink ports. Every switch of this series offers 4 fixed 10G fiber ports with high-performance uplink capability.

RG-NBS5100&5200 series switches provide comprehensive end-to-end QoS as well as flexible and rich security settings for small and medium-sized networks at an extremely high price-performance ratio to meet the needs of high-speed, secure and smart enterprise networks.

1.3.1 Product List

Model	10/100/1000 Base-T Ethernet Port	1000Base-X SFP Port	10G SFP+ Port	Console Port	Power Supply

RG-NBS3100-24GT4SFP	24	4	N/A	N/A	Single
RG-NBS3100-24GT4SFP-P	24 (Support PoE+)	4	N/A	N/A	Single
RG-NBS3100-8GT2SFP	8	2	N/A	N/A	Power adapter
RG-NBS3100-8GT2SFP-P	8 (Support PoE+)	2	N/A	N/A	Single
RG-NBS3200-24GT4XS	24	N/A	4	N/A	Single
RG-NBS3200-24SFP/8GT4XS	8 (combo)	24	4	N/A	Single
RG-NBS3200-24GT4XS-P	24 (Support PoE+)	N/A	4	N/A	Single
RG-NBS3200-48GT4XS	48	N/A	4	N/A	Single
RG-NBS3200-48GT4XS-P	48 (Support PoE+)	N/A	4	N/A	Single
RG-NBS5100-24GT4SFP	24	4	N/A	N/A	Single
RG-NBS5100-48GT4SFP	48	4	N/A	N/A	Single
RG-NBS5200-24GT4XS	24	N/A	4	N/A	Single
RG-NBS5200-24SFP/8GT4XS	8 (combo)	24	4	N/A	Single
RG-NBS5200-48GT4XS	48	N/A	4	N/A	Single

SFP port is downward compatible with 100Base-FX.

1000Base-T is downward compatible with 100Base-TX and 10Base-T.

Combo port consists of one 1000Base-X SFP port and one 10/100/1000Base-T Ethernet port. That is, only one port of them is available at a particular time.

1.3.2 LED Indicator

LED	State	Meaning
System status LED	Off	The switch is not receiving power.
	Blinking green (0.5 Hz)	The switch is running, but the alarm of insufficient PoE power prompts.
	Blinking green (10Hz)	The switch is being upgraded or initialized.
	Solid green	The switch is connected to Ruijie Cloud.
10/100/1000Base-T Ethernet port status LED	Off	The port is not connected.
	Solid green	The port is connected at 10/100/1000 Mbps.
	Blinking green	The port is receiving or transmitting traffic at 10/100/1000 Mbps.
RJ45 port PoE status LED	Off	PoE is not enabled.
	Solid green	PoE is enabled. The port is operational.
	Blinking green	The port has a PoE fault of overload.

SFP port status LED	Off	The port is not connected.
	Solid green	The port is connected.
	Blinking green	The port is receiving or transmitting traffic.
SFP+ port status LED	Off	The port is not connected.
	Solid green	The port is connected.
	Blinking green	The port is receiving or transmitting traffic.

1.3.3 Button

Botton	Description
PoE mode switch-over button	Press PoE Mode Switch-Over Button for above 3 seconds to switch the display mode between PoE mode and port rate mode.
Reset button	The switch reboots after the reset button is pressed for less than 2 seconds. The switch restores the default factory settings after the reset button is pressed for more than 5 seconds (until the status LED blinks).

1.4 Reyee Access Point

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 5GHzand 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.

1.4.1 Product List

Model	Coverage	Recommend number of clients	WLAN ID Number	SON Number	Spatial Streams
RG-RAP1200(F)	20meters	40=8(2.4G)+32(5G)	8	150	2.4G 2x2MIMO 5G 2x2MIMO
RG-RAP1200(P)	20meters	80=16(2.4G)+64(5G)	8	150	2.4G 2x2MIMO 5G 2x2MIMO
RG-RAP2200(F)	30meters	48=16(2.4G)+32(5G)	8	150	2.4G 2x2MIMO 5G 2x2MIMO
RG-RAP2200(E)	30meters	80=16(2.4G)+64(5G)	8	300	2.4G 2x2MIMO 5G 2x2MIMO
RG-RAP2260(G)	30meters	100=16(2.4G)+84(5G)	8	300	2.4G 2x2MIMO 5G 2x2MIMO
RG-RAP2260(E)	30meters	120=16(2.4G)+104(5G)	8	300	2.4G 4x4MIMO 5G 4x4MIMO
RG-EAP602	2.4G 100meters 5G 300meters	96=32(2.4G)+64(5G)	8	150	2.4G 2x2MIMO 5G 2x2MIMO
RG-RAP6260(G)	100meters	100=16(2.4G)+84(5G)	8	300	2.4G 2x2MIMO 5G 2x2MIMO

1.4.2 LED Indicator

Reyee Indoor AP(RG-RAP2200(E), RG-RAP2200(F), RG-RAP2260(E), RG-RAP2260(G)**)**

LED Indicator	State	Frequency	Meaning
LED Indicator	Off	N/A	The AP is NOT receiving power
	Blinking	0.5Hz	Normal question，but there are alarms
	Fast blinking	10Hz	Possible cases： 1、 restoring the factory settings 2、 upgrading the firmware 3、 restoring the image file 4、 initializing the device
	Solid green	NA	Normal operation

Reyee Wall AP(RG-RAP1200(F), RG-RAP1200(P)**)**

LED Indicator	State	Frequency	Meaning
LED Indicator	Off	N/A	The AP is powered off.
	Slow blinking	0.5Hz	Normal question，but there are alarms

	Fast blinking	10Hz	Possible cases: 1、 restoring the factory settings 2、 upgrading the firmware 3、 self-repairing 4、 initializing the device 5、 POE OUT is overloaded
	Solid green	NA	Normal operation

Reyee Outdoor AP(RG-EAP602, RG-RAP6260(G)**)**

LED Indicator	State	Frequency	Meaning
LED Indicator	Off	N/A	The AP is Not receiving power
	Slow blinking	0.5Hz	Normal question，but the device is not connected to Ruijie Cloud
	Fast blinking	10Hz	Possible cases: 1、 restoring the factory settings 2、 upgrading the firmware 3、 restoring the image file 4、 initializing the device
	Solid Blue	On	Normal operation

1.4.3 Button

Model	Button		Meaning
All AP	Reset	Pressed for less than 2 seconds	Restart the device
		Pressed for more than 5 seconds	Restore the factory default settings

1.5 Reyee Mesh Wi-Fi Router

Reyee EW series products are Gigabit dual-band Wi-Fi 6 wireless routers designed for use in large flat space, villas, small shops, SOHO, and other scenarios. It is designed to meet the needs of high quality next-generation Wi-Fi services. Reyee EW series products support various local and remote management platform, such as Web, Ruijie Cloud App. This wireless router also provides multiple home-care-based function, including the Parental Control Mode, Health Mode, Xpress Mode, and exclusive designed for Smart Life Kit System, meeting the needs of all household scenarios.

1.5.1 Product List

Model	Reyee Mesh	Wi-Fi Standards	Max. Wi-Fi Speed	MIMO	Recommended Users
EW300 PRO	Not Support	Wi-Fi 4 (802.11n)	2.4 GHz: 300 Mbps	2.4 GHz: 2×2	16
EW1200	Support	Wi-Fi 5 (802.11ac)	2.4 GHz: 300 Mbps 5 GHz: 867 Mbps	2.4 GHz: 2×2 5 GHz: 2×2	96
EW1200G PRO	Support	Wi-Fi 5 (802.11ac)	2.4 GHz: 400 Mbps 5 GHz: 867 Mbps	2.4 GHz: 2×2 5 GHz: 2×2	96
EW1800GX PRO	Support	Wi-Fi 6 (802.11ax)	2.4 GHz: 574 Mbps 5 GHz: 800 Mbps	2.4 GHz: 2×2 5 GHz: 2×2	192
EW3200GX PRO	Support	Wi-Fi 6 (802.11ax)	2.4 GHz: 800 Mbps 5 GHz: 2400 Mbps	2.4 GHz: 4× 5 GHz: 4×4	192

1.5.2 LED Indicator

a) EW1800GX PRO and EW3200GX PRO

LED	Status		Description
Mesh Indicator	Green	Blinking	The device is being paired
		Steady on	The device is paired and Wi-Fi signal is norm
	Orange	Steady on	The device is paired but Wi-Fi signal is weak
	Red	Steady on	The device pairing is disconnected
System Status Indicator	Blue	Steady on	The device is running normally
		Blinking	Restoring the factory settings or restart

b) EW1200G PRO

LED	Status	Description
System Status Indicator	Off	The router is not powered on
	Steady on	The router is running normally
	Fast Blinking	Restoring factory settings/Rebooting
	Slow Blinking	Reyee Mesh is being paired or repeater stops
Port Indicator	Off	The port is not connected or the cable disconnects
	Steady on	The port is connected normally
	Blinking	Data is being transmitting

c) 1.5.2.3 EW1200

LED	Status	Description
System Status Indicator	Off	The router is not powered on
	Steady on	The router is running normally
	Fast Blinking	Restoring factory settings/Rebooting
WiFi Indicator	Steady on	Reyee Mesh is sunning normally
	Slow Blinking	Reyee Mesh is being paired or repeater stops
Port Indicator	Off	The port is not connected or the cable disconnects
	Steady on	The port is connected normally.

d) EW300 PRO

LED	Status	Description
System Status Indicator	Off	The router is not powered on
	Steady on	The router is running normally
	Fast Blinking	The router is starting or power off
	Slow Blinking	The Internet cannot be accessed
	Fast Blinking Twice	The router is restoring factory settings or upgrading
	Slow Blinking Once and Fast Blinking Three Times	The firmware is faulty

1.5.3 Button

Button	Function	Operation
Reset	Pair	Press the button 1second to pair
	Reboot	Press the button for 2 seconds, and the device will be rebooted.
	Reset	Press the button for over 5 seconds until the LED starts to blink. Release the button, and the device will be reset.

1.6 Reyee Wireless Bridge

Ruijie & Reyee Series EST products are 802.11ac wireless bridge for video surveillance backhaul or remote wireless transmission in scenarios such as tower cranes, factories, scenic spots, campuses, planting bases, aquafarm breeding bases, and construction sites. Operating at 5 GHz, RG-EST350 supports two spatial streams (2x2 MIMO technology) and provides up to 867 Mbps throughput, which can fully meet the data link bandwidth requirements of various services.

EST310

EST350

1.6.1 Product List

Model	Distance (m)	RSSI (dBm)	Negotiate Speed (Mbps)	Rate (Mbps)	3Mbps 2MP Camera (Unit)	4-5Mbps 3MP Camera (Unit)	6-7Mbps 4MP Camera (Unit)
RG-EST310 V2	100	-52	400	90	16	10	7
	500	-65	400	80	16	10	7
	1000	-68	240	80	16	10	7
	2000	-75	120	40	6	4	3
RG-EST350 V2	1000	-58	400	230	50	30	20
	3000	-66	360	200	45	25	13
	5000	-70	270	150	20	12	8

1.6.2 LED Indicator

a) EST30

LED	State	Meaning
System Status	Solid green	Video recorder mode
	Fast blinking green	The system is being upgraded or reset.
	Blinking green at a frequency of 2Hz	Camera mode
LAN Port Status	Solid on	The LAN port is not receiving or transmitting data.
	Blinking	The LAN port is receiving or transmitting data.
RSSI (3 LEDs in total)	LED 1 blinks	RSSI < -69dBm
	LED 1 is solid on.	-69dBm< RSSI <-59dBm
	LED 1 and LED 2 are solid on.	RSSI > -59dBm
	LED 1, LED 2 and LED 3 are solid on.	RSSI > -49dBm
	Off	No signal

b) EST350

LED	State	Meaning
System Status	Solid green	The device is working properly.
	Fast blinking green	The system is being upgraded or reset.
	Blinking green at a frequency of 1Hz	The device is being booted.
LAN Port Status	Solid green	The LAN port is not receiving or transmitting data.
	Blinking	The LAN port is receiving or transmitting data.
RSSI (3 LEDs in total)	STR1 blinking/on	The device is bridged.
	STR1 on	RSSI > -75 dBm
	STR1 on + STR2 blinking	RSSI > -73 dBm
	STR1 on + STR2 on	RSSI > -71 dBm
	STR1 on + STR2 on + STR3 blinking	RSSI > -68 dBm
	STR1 on + STR2 on + STR3 on	RSSI > -64 dBm

1.6.3 Button

Button	Function	Operation
Reset	Reboot	Press the button for 2 seconds, and the device will be rebooted.
	Reset	Press the button for over 5 seconds until the LED starts to blink. Release the button, and the device will be reset.

2 Device Management

2.1 Logging in

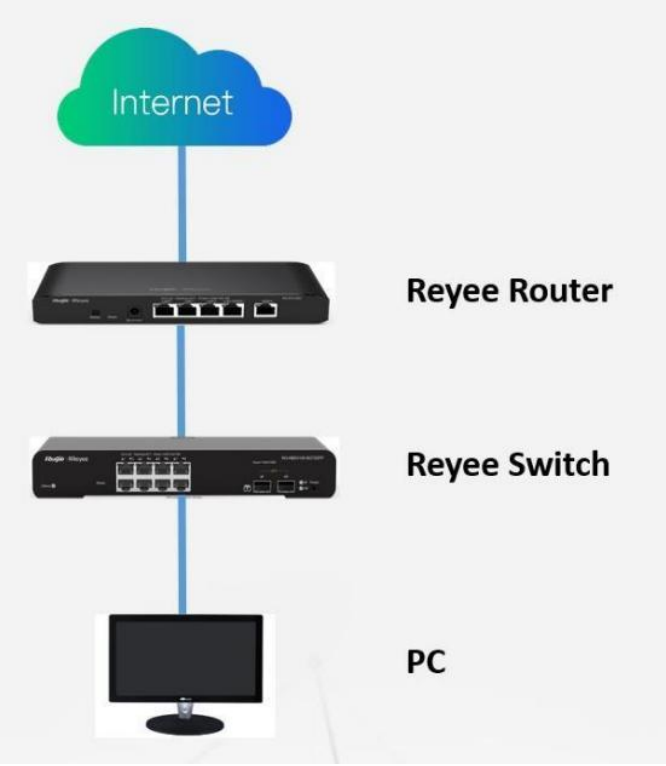
Web is a Web-based network management system used to manage or configure devices. You can access eWeb via browsers such as Google Chrome.Web-based management involves a Web server and a Web client. The Web server is integrated in a device, and is used to receive and process requests from the client, and return processing results to the client. The Web client usually refers to a browser, such as Google Chrome IE, or Firefox.

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.

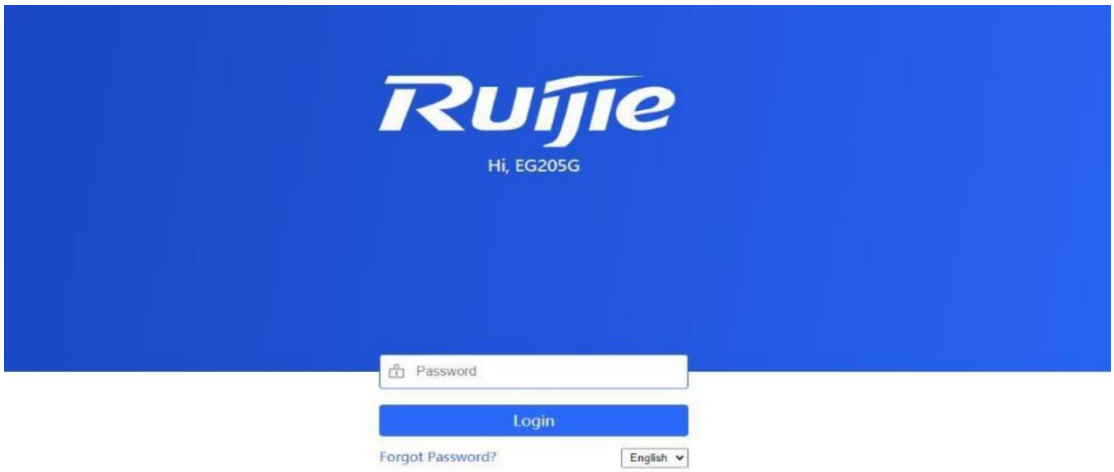
2.1.1 Case Demonstration

Network Topology

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



1. Set PC's IP assignment mode to obtain the IP address automatically.
2. Visit http://192.168.110.1 by Chrome browser.
3. Enter the password on the login page and click "Login".
4. 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.

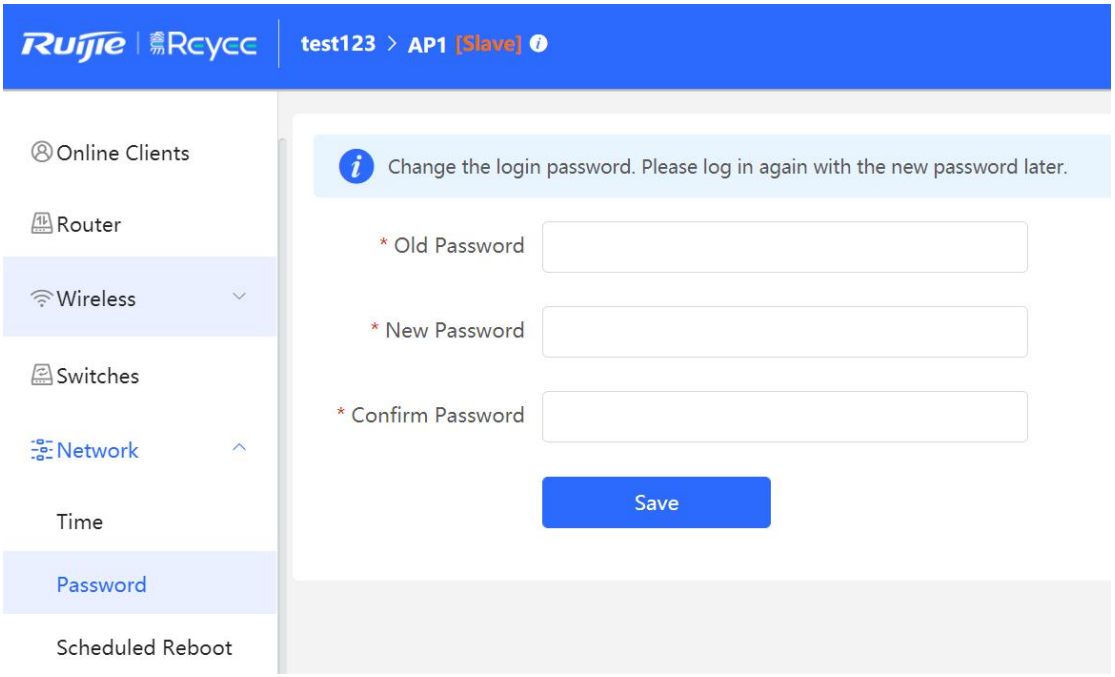
For the **Reyee AP**, you may use either 192.168.120.1 or 10.44.77.254 to access the device.

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

The default login password for all Reyee devices is admin.

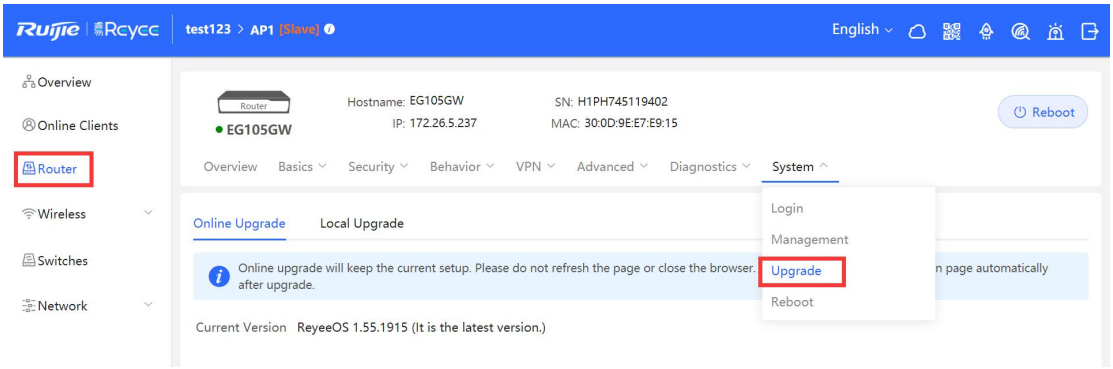
You may visit https://10.44.77.253 to login to the master device of Reyee network.

2.2 Configuring Password



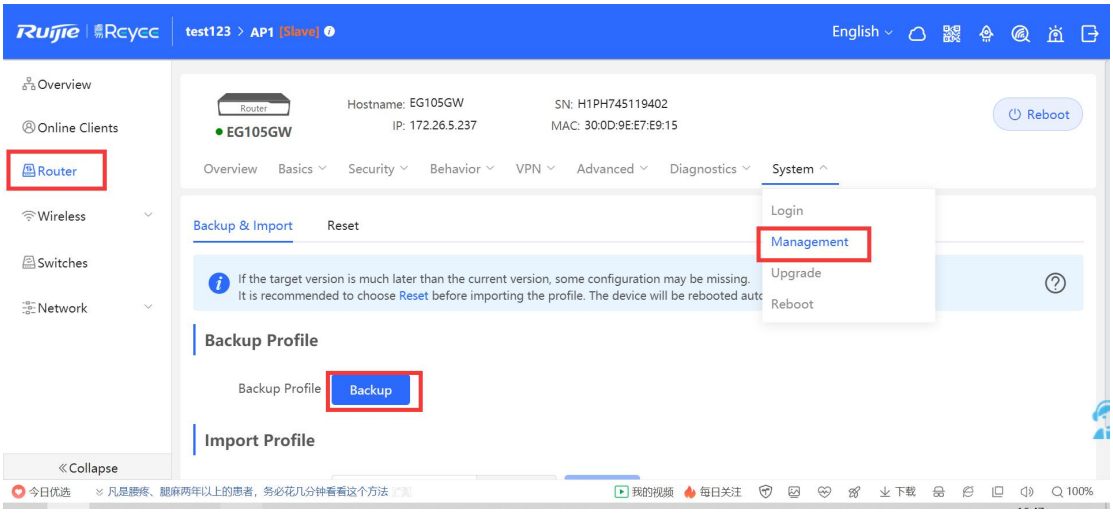
2.3 Upgrading

Login to the eWeb of the device and choose Router--System--Upgrade.

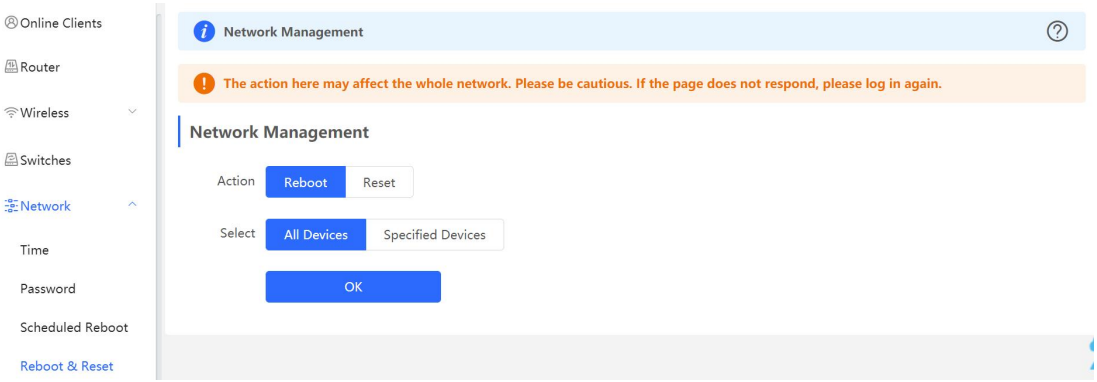


2.4 Backing up and Resetting

Login in the eWeb of the device and choose Router--System--Management.

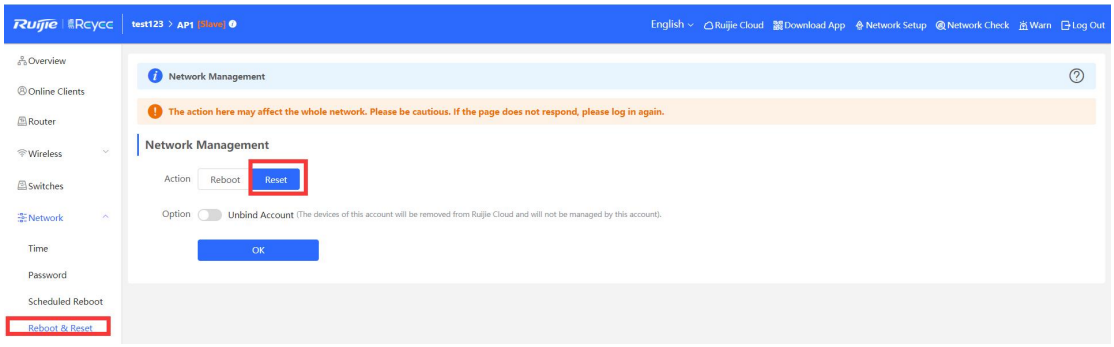


Login in the eWeb of the device and click Network--Reboot&Reset, then you can reset your devices.



2.5 Restoring Factory Settings

Login in the eWeb of the device Reset all device in the network.



3 Getting Start

3.1 Preparing for Installation

3.1.1 Safety Suggestions

To avoid personal injury and equipment damage, please carefully read the safety suggestions before you install each device. The following safety suggestions do not cover all possible dangers

3.1.1.1 Installation

a) Keep the chassis clean and free from any dust.

b) Do not place devices in a walking area.

c) Do not wear loose clothes or accessories that may be hooked or caught by devices during installation and maintenance

3.1.1.2 Movement

a) Do not frequently move devices.

b) When moving devices, note the balance and avoid hurting legs and feet or straining the back.

c) Before moving devices, turn off all power supplies and dismantle all power modules.

3.1.1.3 Electricity

a) Observe local regulations and specifications when performing electric operations. Relevant operators must be qualified.

b) Before installing the device, carefully check any potential danger in the surroundings, such as ungrounded power supply, and damp/wet ground or floor.

c) Before installing the device, find out the location of the emergency power supply switch in the room. First cut off the power supply in the case of an accident.

d) Try to avoid maintaining the switch that is powered-on alone.

e) Be sure to make a careful check before you shut down the power supply.

f) Do not place the equipment in a damp location. Do not let any liquid enter the chassis

3.1.1.4 Static Discharge Damage Prevention

To prevent damage from static electricity, pay attention to the following:

a) Proper grounding of grounding screws on the back panel of the device. Use of a three-wire single-phase socket with protective earth wire (PE) as the AC power socket.

b) Indoor dust prevention

c) Proper humidity conditions

3.1.1.5 Laser

Some devices support varying models of optical modules sold on the market which are Class I laser products. Improper use of optical modules may cause damage. Therefore, pay attention to the following when you use them:

a) When a fiber transceiver works, ensure that the port has been connected with an optical fiber or is covered with a dust cap, to keep out dust and avoid burning your eyes.

b) When the optical module is working, do not pull out the fiber cable and stare into the transceiver interface or you may hurt your eyes.

3.1.2 Installation Site Requirement

To ensure the normal working and a prolonged durable life of the equipment, the installation site must meet the following requirements

3.1.2.1 Ventilation

For installing devices, a sufficient space (at least 10 cm distances from both sides and the back plane of the cabinet) should be reserved at the ventilation openings to ensure the normal ventilation. After various cables have been connected, they should be arranged into bundles or placed on the cabling rack to avoid blocking the air inlets. It is recommended to clean the switch at regular intervals (like once every 3 months). Especially, avoid dust from blocking the screen mesh on the back of the cabinet.

3.1.2.2 Temperature and Humidity

To ensure the normal operation and prolong the service life of router, you should keep proper temperature and humidity in the equipment room.

If the equipment room has temperature and humidity that do not meet the requirements for a long time, the equipment may be damaged.

In an environment with relatively high humidity, the insulating material may have bad insulation or even leak electricity. Sometimes the materials may suffer from mechanical performance change and metallic parts may get rusted.

In an environment with relatively low humidity, however, the insulating strip may dry and shrink. Static electricity may occur easily and endanger the circuit on the equipment.

In an environment with high temperature, the equipment is subject to even greater harm, as its performance may degrade significantly and various hardware faults may occur.

3.1.2.3 Cleanness

Dust poses a severe threat to the running of the equipment. The indoor dust falling on the equipment may be adhered by the static electricity, causing bad contact of the metallic joint. Such electrostatic adherence may occur more easily when the relative humidity is low, not only affecting the useful life of the equipment, but also causing communication faults.

3.1.2.4 Grounding

A good grounding system is the basis for the stable and reliable operation of devices. It is the chief condition to prevent lightning stroke and resist interference. Please carefully check the grounding conditions on the installation site according to the grounding requirements, and perform grounding operations properly as required

1.1 Lightning Grounding

The lightning protection system of a facility is an independent system that consists of the lightning rod, download conductor and the connector to the grounding system, which usually shares the power reference ground and yellow/green safety cable ground. The lightning discharge ground is for the facility only, irrelevant to the equipment.

1.2 EM C Grounding

The grounding required for EMC design includes shielding ground, filter ground, noise and interference suppression, and level reference. All the above constitute the comprehensive grounding requirements. The resistance of earth wires should be less than 1Ω

3.1.2.5 EMI

Electro-Magnetic Interference (EMI), from either outside or inside the equipment or application system, affects the system in the conductive ways such as capacitive coupling, inductive coupling, and electromagnetic radiation.

There are two types of electromagnetic interference: radiated interference and conducted interference, depending on the type of the transmission path.

When the energy, often RF energy, from a component arrives at a sensitive component via the space, the energy is known as radiated interference. The interference source can be either a part of the interfered system or a completely electrically isolated unit. Conducted interference results from the electromagnetic wire or signal cable connection between the source and the sensitive component, along which cable the interference conducts from one unit to another. Conducted interference often affects the power supply of the equipment, but can be controlled by a filter. Radiated interference may affect any signal path in the equipment and is difficult to shield.

a) For the AC power supply system TN, single-phase three-core power socket with protective earthing conductors (PE) should be adopted to effectively filter out interference from the power grid through the filtering circuit.

b) The grounding device of the switch must not be used as the grounding device of the electrical equipment or anti-lightning grounding device. In addition, the grounding device of the switch must be deployed far away from the grounding device of the electrical equipment and anti-lightning grounding device.

c) Keep the equipment away from high-power radio transmitter, radar transmitting station, and high-frequency large-current device.

d) Measures must be taken to shield static electricity.

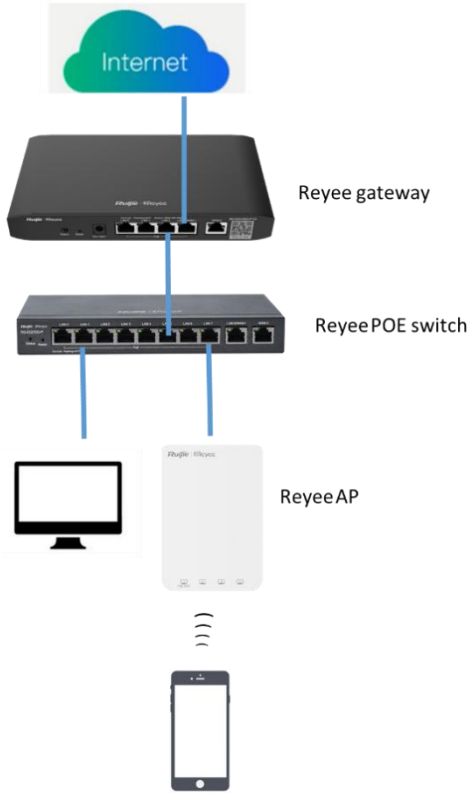
e) Interface cables should be laid inside the equipment room. Outdoor cabling is prohibited, avoiding damages to device signal interfaces caused by over-voltage or over-current of lightning

3.1.3 Network Planning

The DHCP server has two address pools on the egress gateway:

192.168.110.0/24 in VLAN 1 for devices of this network

192.168.10.0/24 in VLAN 10 for clients of this network



Following ports are used for Ruijie Cloud management. To let devices go online on Ruijie Cloud, ensure these ports are available and the data stream is permitted in this network.

Cloud	Domain name	DST.TCP	DST.UDP
Cloud-as	devicereg.ruijienetworks.com	80,443	
	ryrc.ruijienetworks.com	80,443	
	stunrc.ruijienetworks.com		3478,3479
	stunsvr-as.ruijienetworks.com		3478,3479
	cwmpsvr-as.ruijienetworks.com	80,443	
	34.87.93.12	80,443	
	firmware.ruijienetworks.com	80,443	
	cloudweb.ruijienetworks.com	80,443	
	fastonline.ruijienetworks.com	80,443	
	cloudapi.ruijienetworks.com	80,443	
	cdn.ruijienetworks.com	80,443	
	iotrc.ruijienetworks.com		7683
	iotsvr-as.ruijienetworks.com		5683
	iotlog-as.ruijienetworks.com		6683
	iotdl-as.ruijienetworks.com		8683

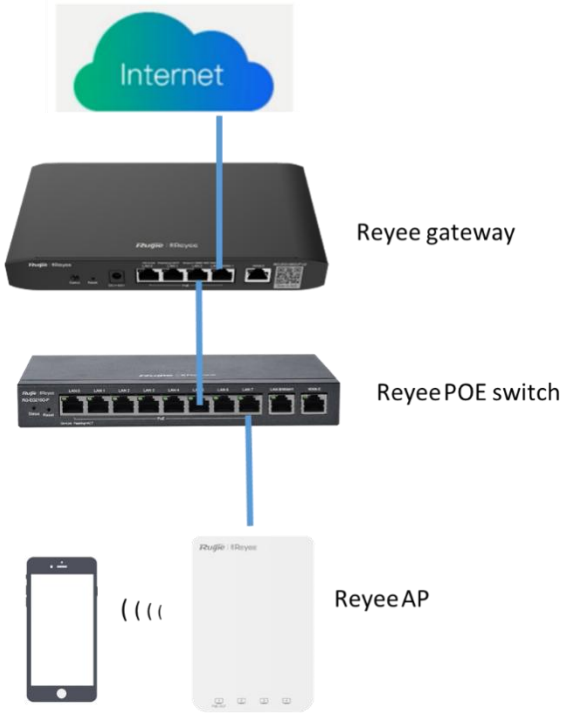
Cloud	Domain name	DST.TCP	DST.UDP
Cloud-eu	devicereg.ruijienetworks.com	80,443	
	ryrc.ruijienetworks.com	80,443	
	stunrc.ruijienetworks.com		3478,3479
	stunsvr-eu.ruijienetworks.com		3478,3479
	cwmpsvr-eu.ruijienetworks.com	80,443	
	cloudlog-eu.ruijienetworks.com	80,443	
	firmware.ruijienetworks.com	80,443	
	cloudweb.ruijienetworks.com	80,443	
	fastonline.ruijienetworks.com	80,443	
	cloudapi.ruijienetworks.com	80,443	
	cdn.ruijienetworks.com	80,443	
	iotrc.ruijienetworks.com		7683
	iotsvr-eu.ruijienetworks.com		5683
	iotlog-eu.ruijienetworks.com		6683
	iotdl-eu.ruijienetworks.com		8683

Cloud	Domain name	DST.TCP	DST.UDP
Cloud-ru	devicereg.ruijienetworks.com	80,443	
	ryrc.ruijienetworks.com	80,443	
	stunrc.ruijienetworks.com		3478,3479
	stunsvr-ru.ruijienetworks.com		3478,3479
	cwmpsvr-ru.ruijienetworks.com	80,443	
	130.193.40.202	80,443	
	firmware.ruijienetworks.com	80,443	
	cloudweb.ruijienetworks.com	80,443	
	fastonline.ruijienetworks.com	80,443	
	cloudapi.ruijienetworks.com	80,443	
	cdn.ruijienetworks.com	80,443	
	iotrc.ruijienetworks.com		7683
	iotsvr-ru.ruijienetworks.com		5683
	iotlog-ru.ruijienetworks.com		6683
	iotdl-ru.ruijienetworks.com		8683

3.2 Quick Provisioning

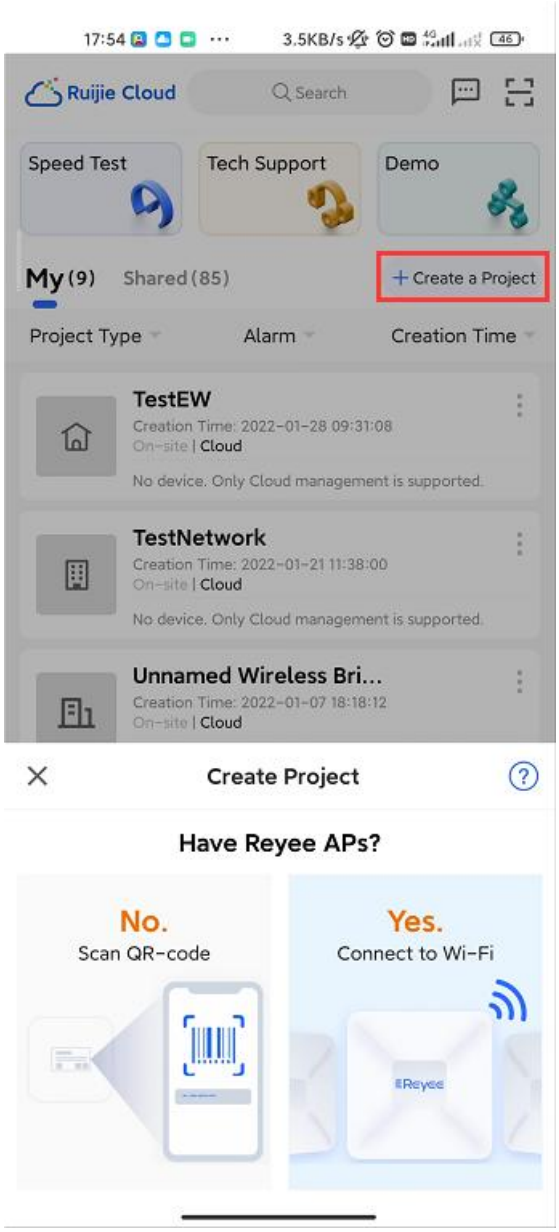
3.2.1 Quick provisioning via Ruijie Cloud APP

The network topology shown in the below picture includes the Reyee gateway, Reyee POE switch and Reyee RAP.



3.2.1.1 Create a project

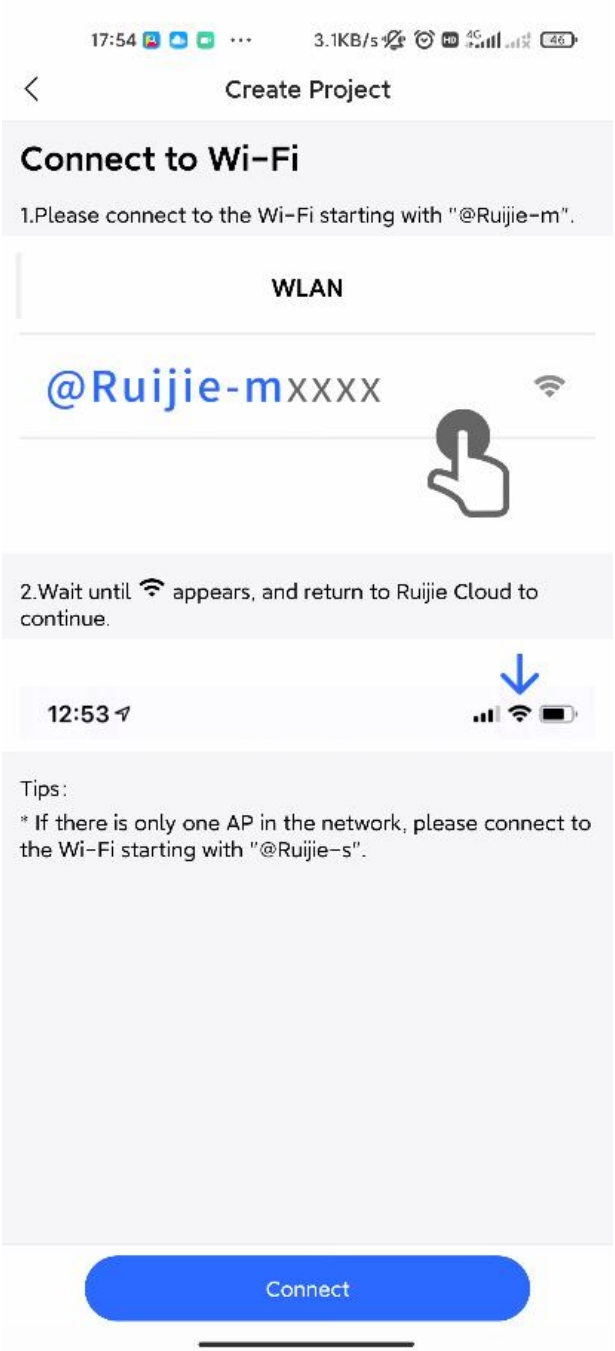
Open Ruijie Cloud App and Click **Create a Project,** then select **Connect to Wi-Fi.**



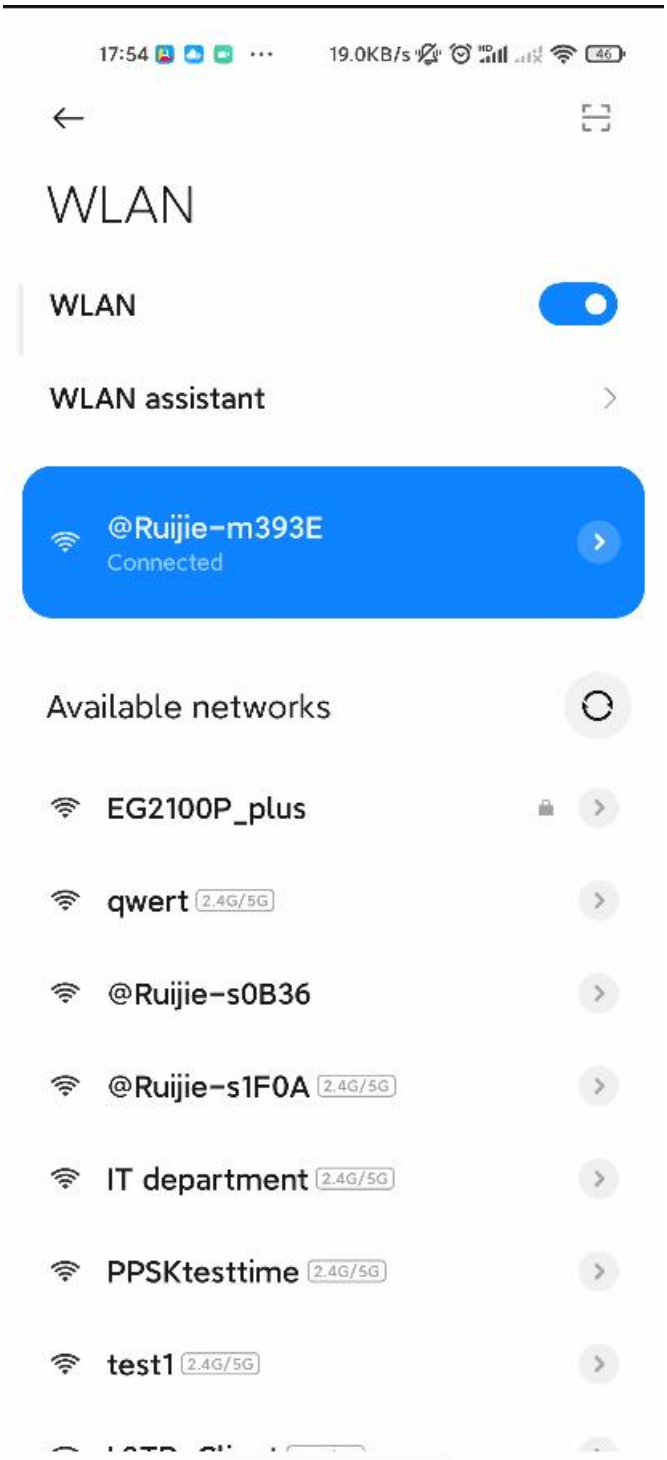
After click **Yes**, then Cloud App will prompt you to connect @Ruijie-mxxxx SSID.

Note:

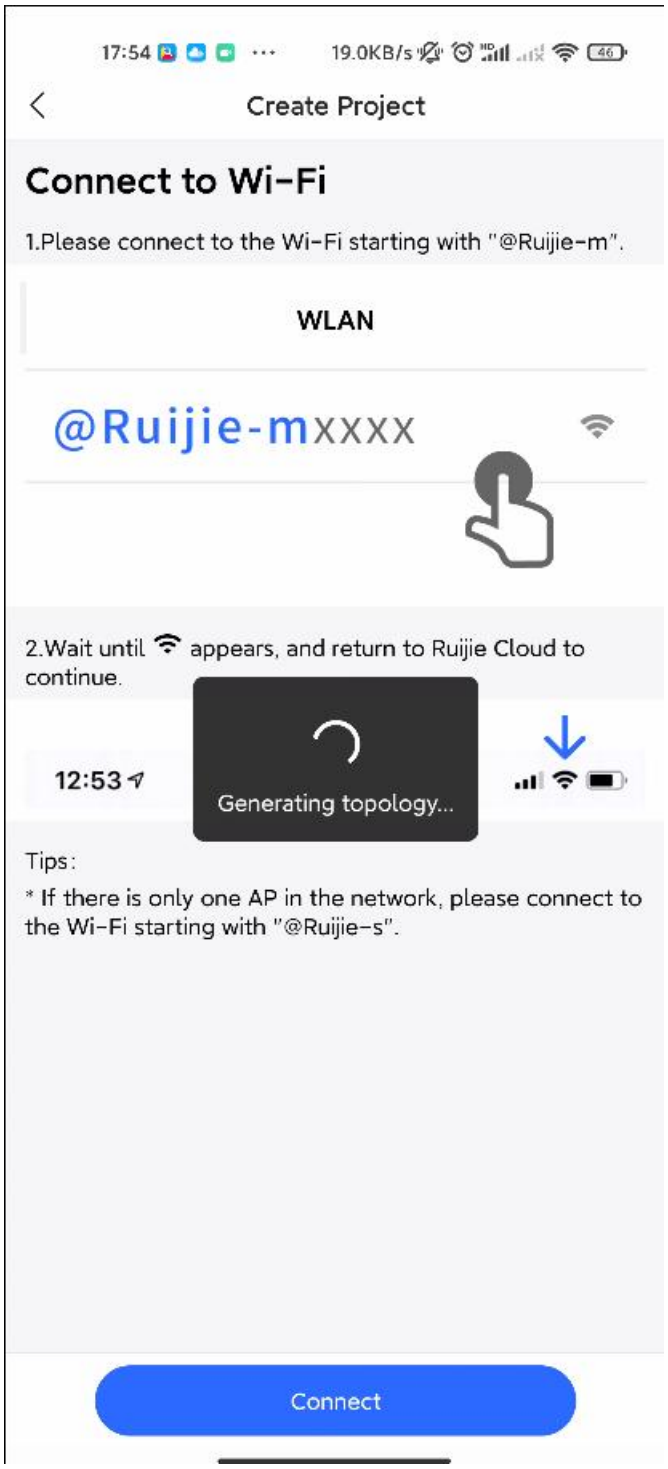
@Ruijie-mxxxx is generated after network self-organization established successfully, while @Ruijie-sxxxx is generated on a standalone device, xxxx is the last four letters of mac address of device.

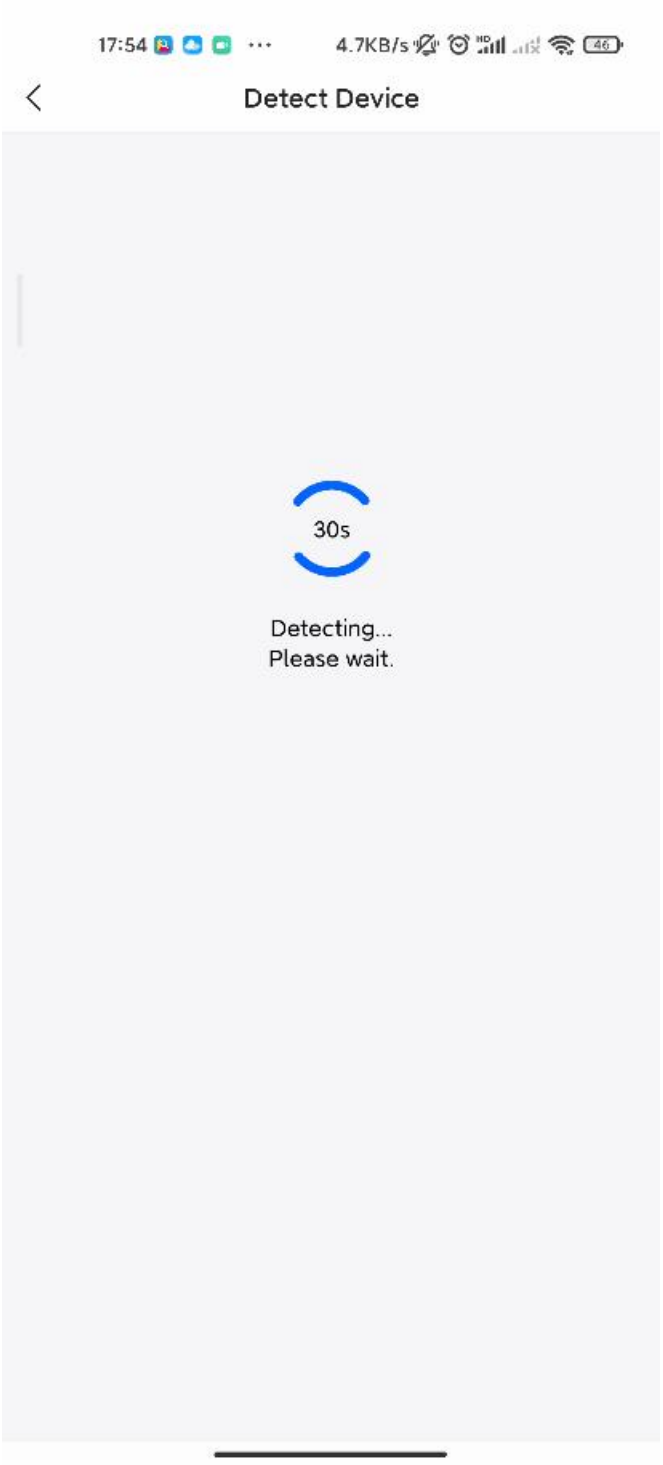


Connect the @Ruijie-mxxxx SSID on your phone.

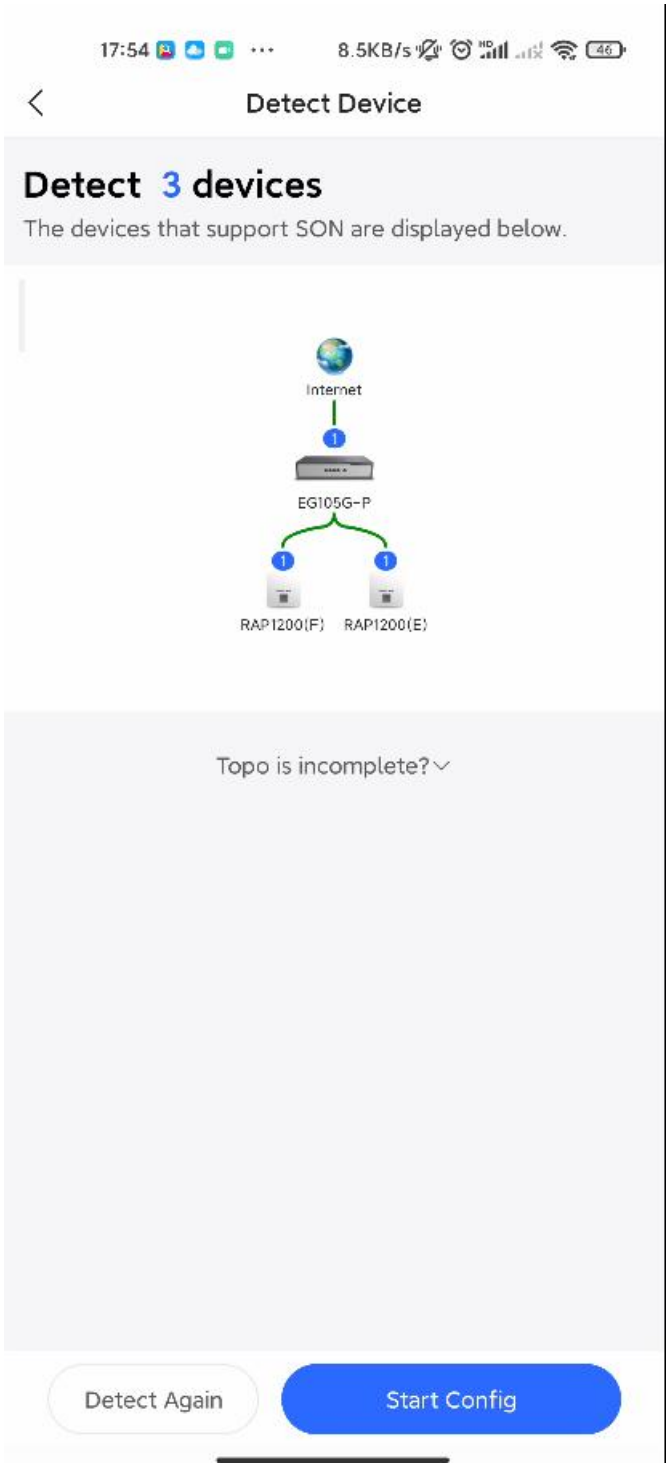


After connected the @Ruijie-mxxxx SSID, the Cloud App will prompt to generate topology and detect all devices in this SON.


17:54
19.0KB/s
Create Project
Connect to Wi-Fi
1.Please connect to the Wi-Fi starting with "@Ruijie-m".
WLAN
@Ruijie-mxxxx
2.Wait until appears, and return to Ruijie Cloud to continue.
12:53
Generating topology...
Tips:
* If there is only one AP in the network, please connect to the Wi-Fi starting with "@Ruijie-s".
Connect

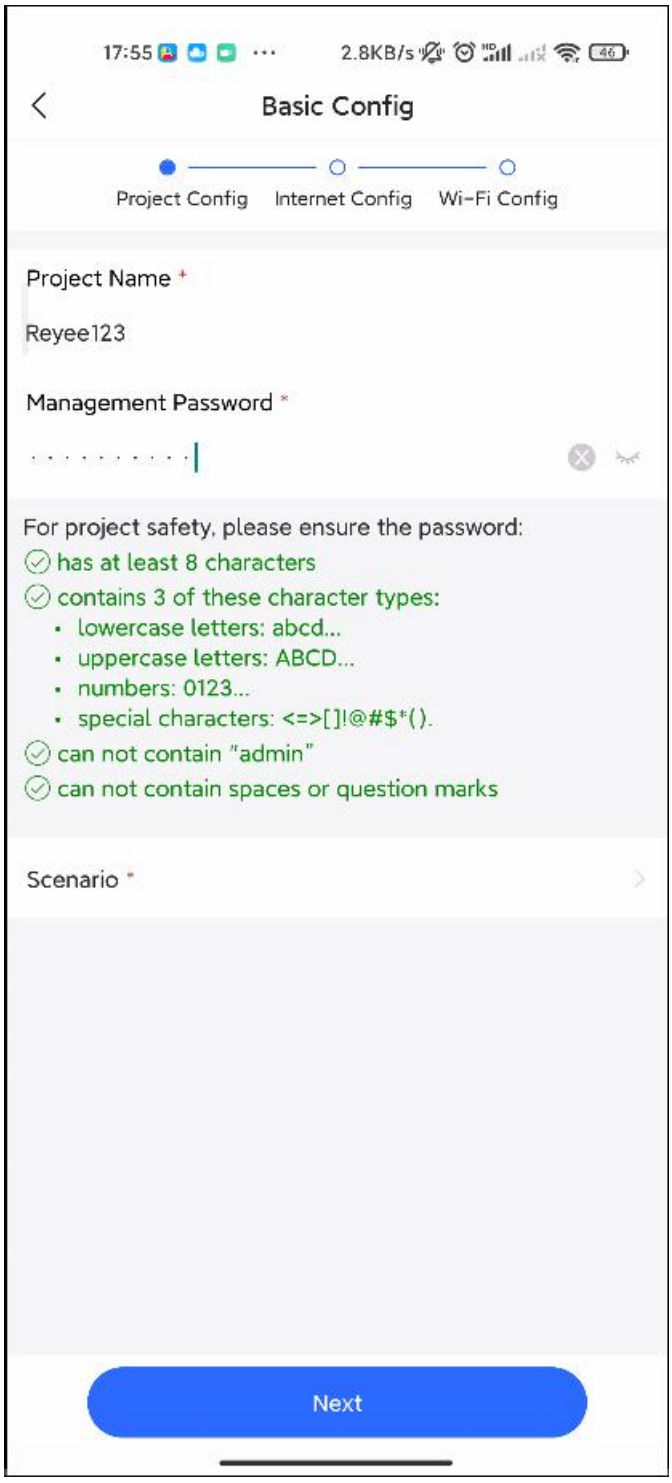


After all devices were detected, Cloud App will display them and show the topology, shown in the below picture. Click **Start Config** to perform the basic configuration of this project.

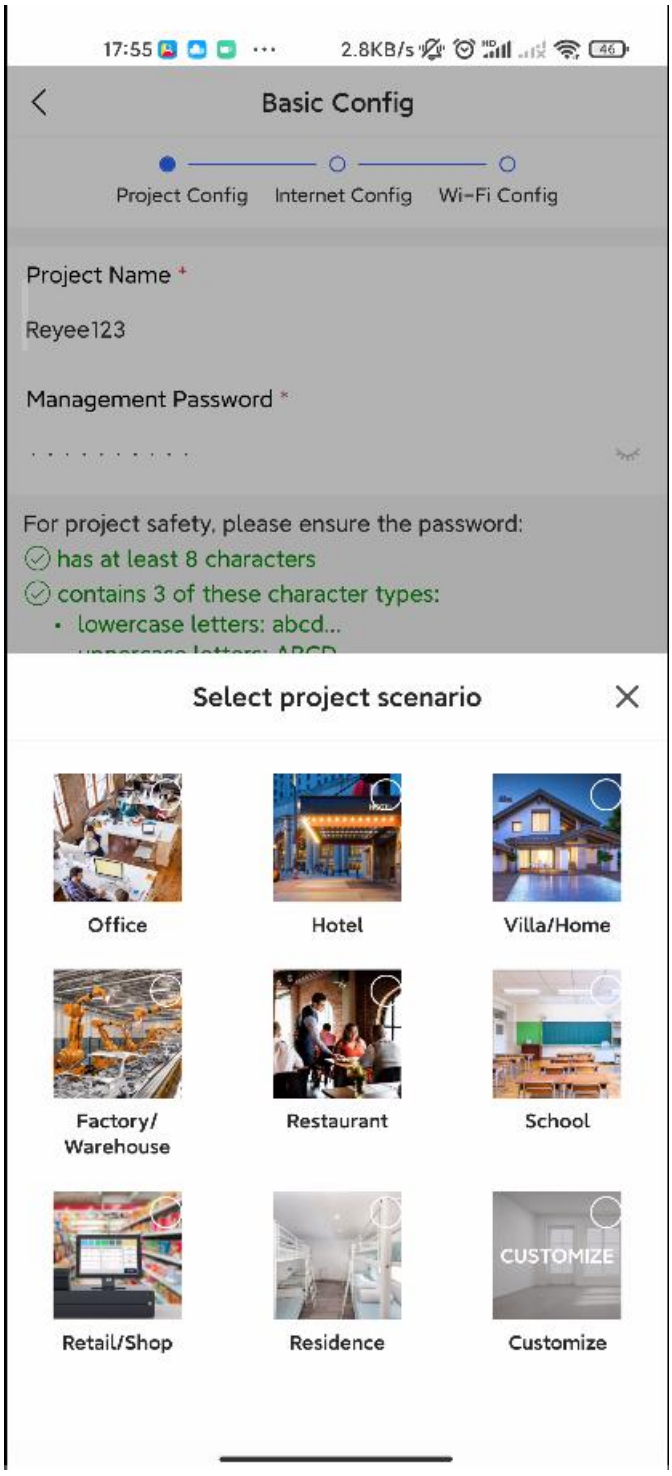


3.2.1.2 Configure the project

Input the Project Name and Management Password.

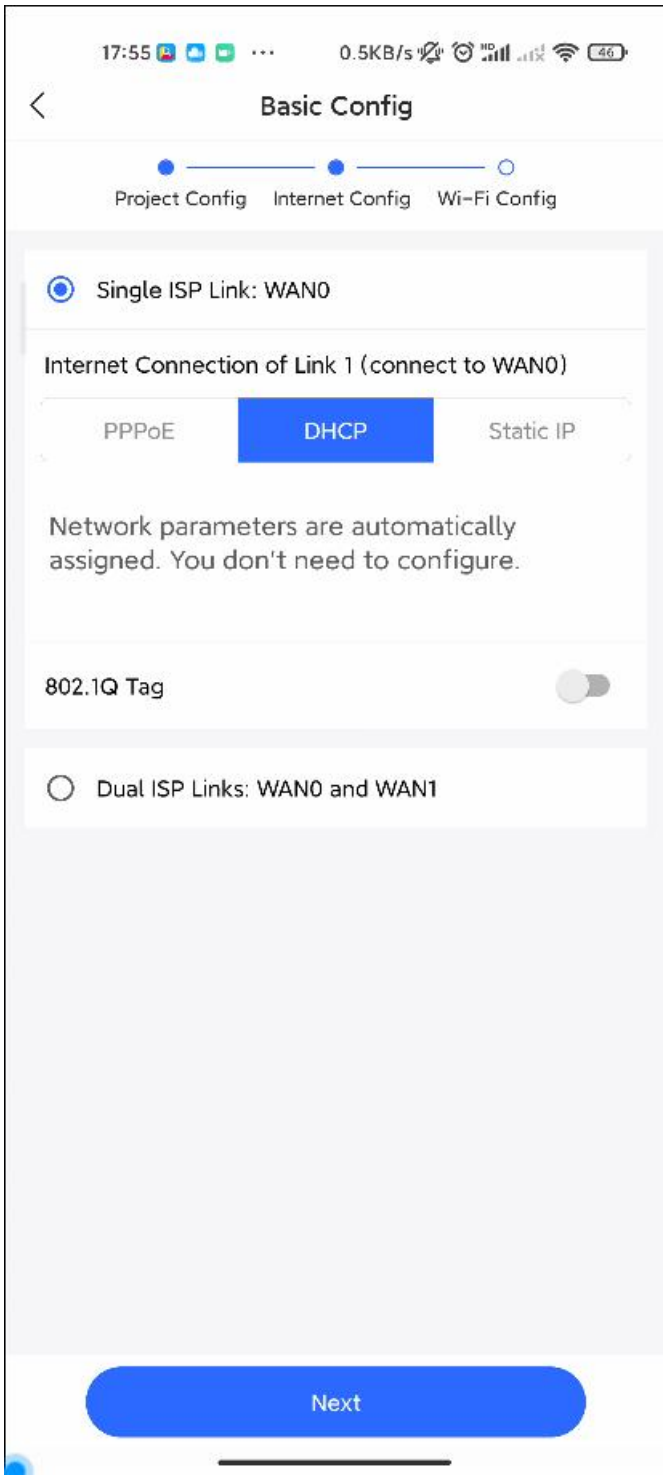


Then select the scenario of this project based on your requirement.



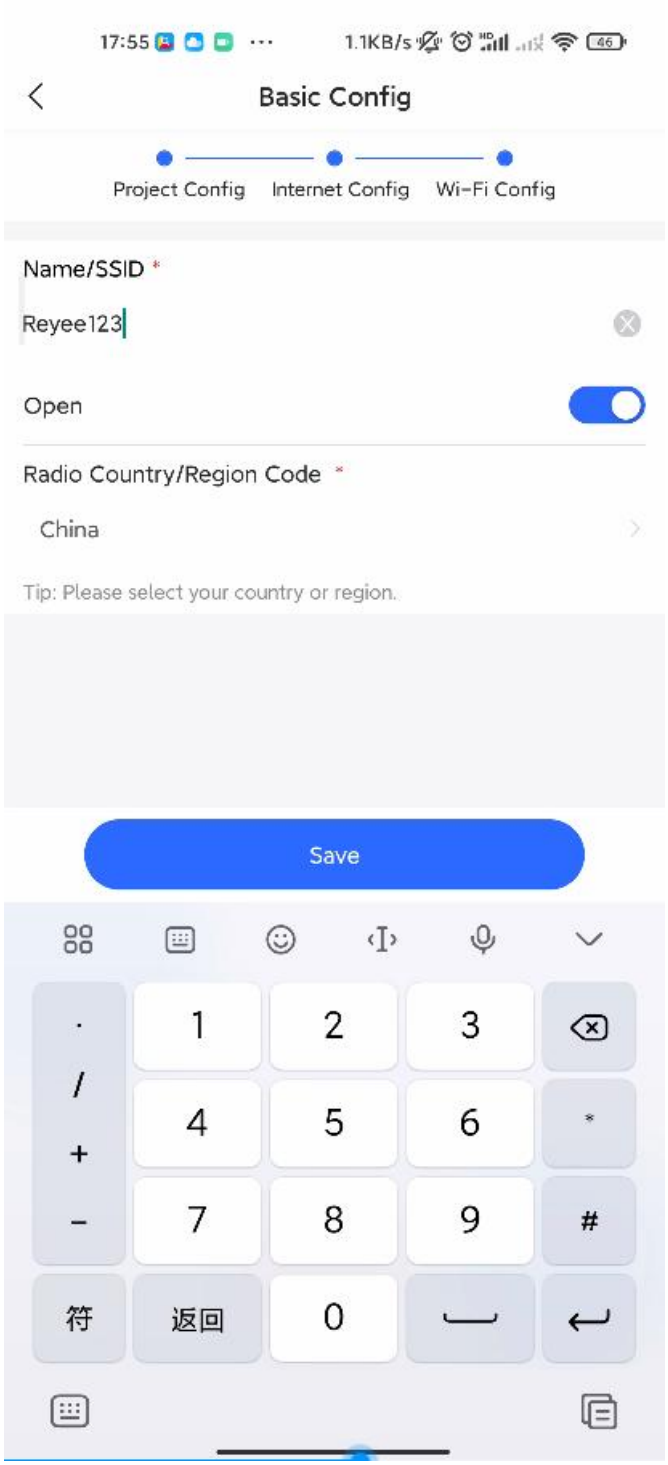
3.2.1.3 Configure the internet

For configuring WAN, you can chose PPPoE, DHCP and Static IP.

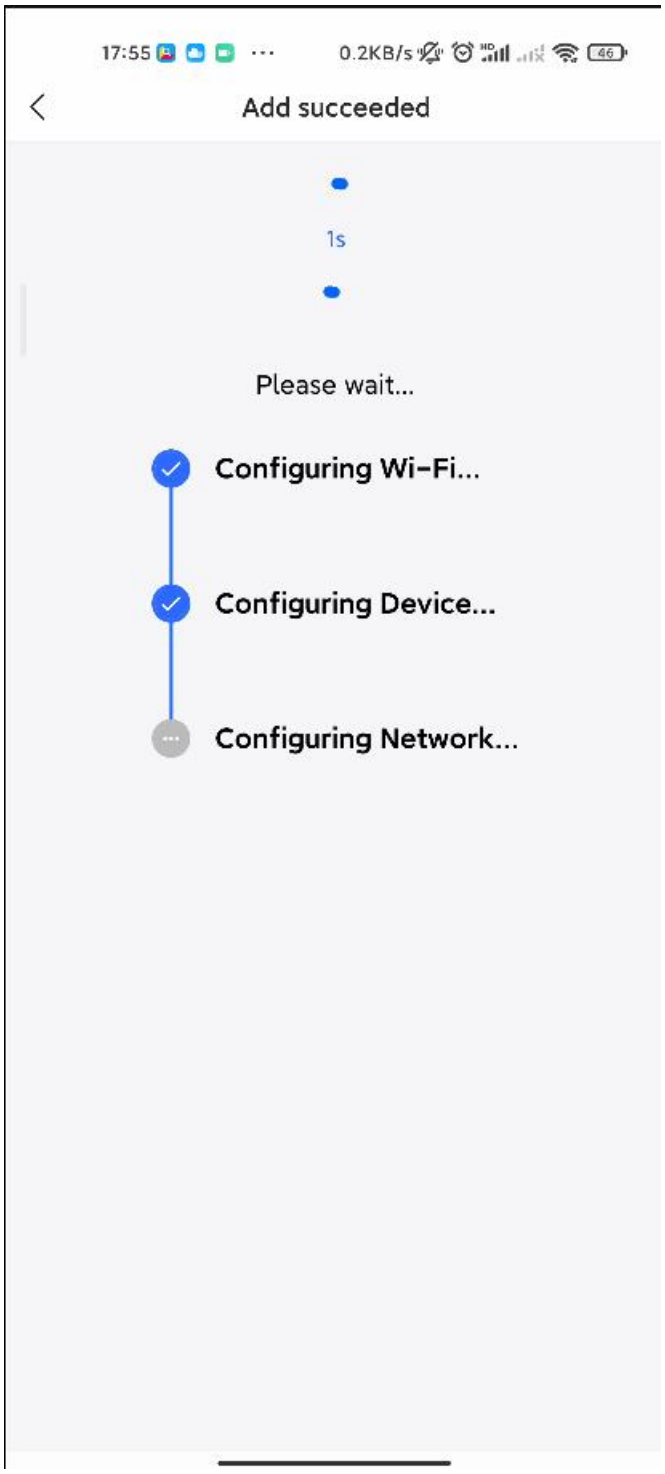


3.2.1.4 Configure the SSID

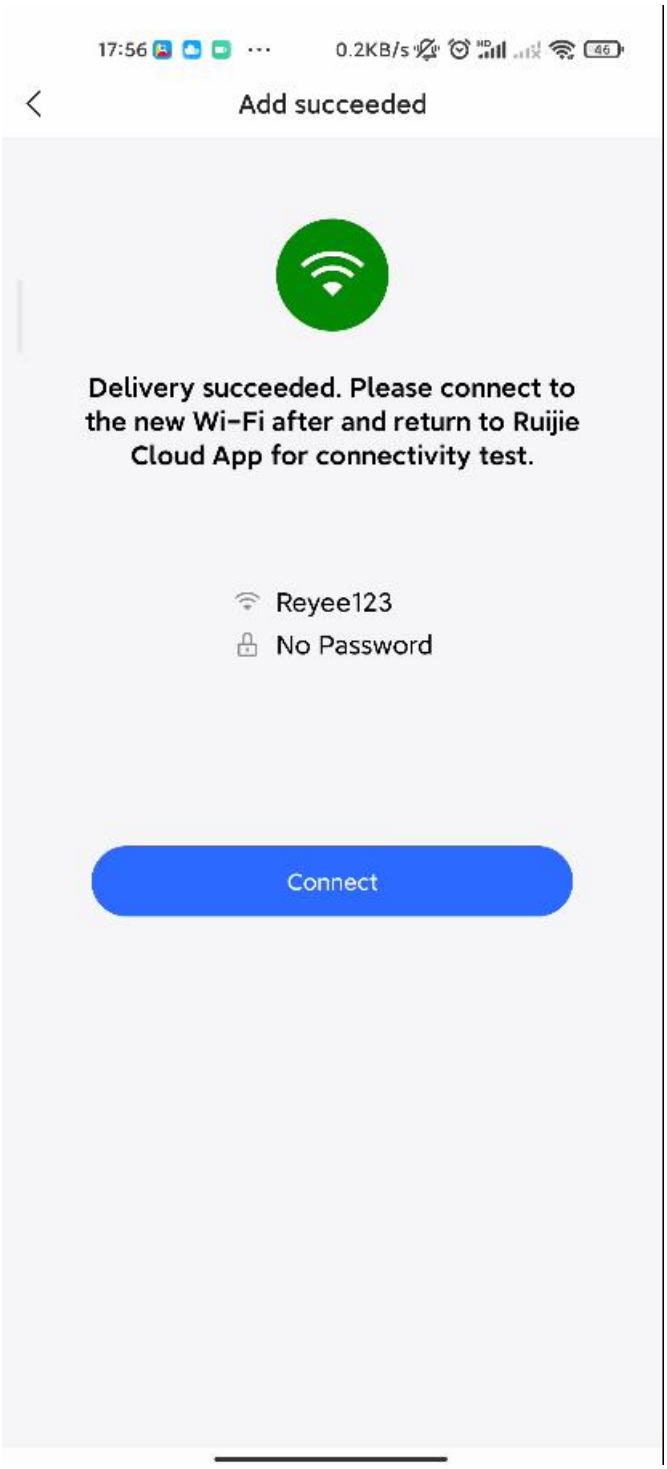
For SSID settings, input the name of SSID and configure it as open or configure password for this SSID. Select the region code.



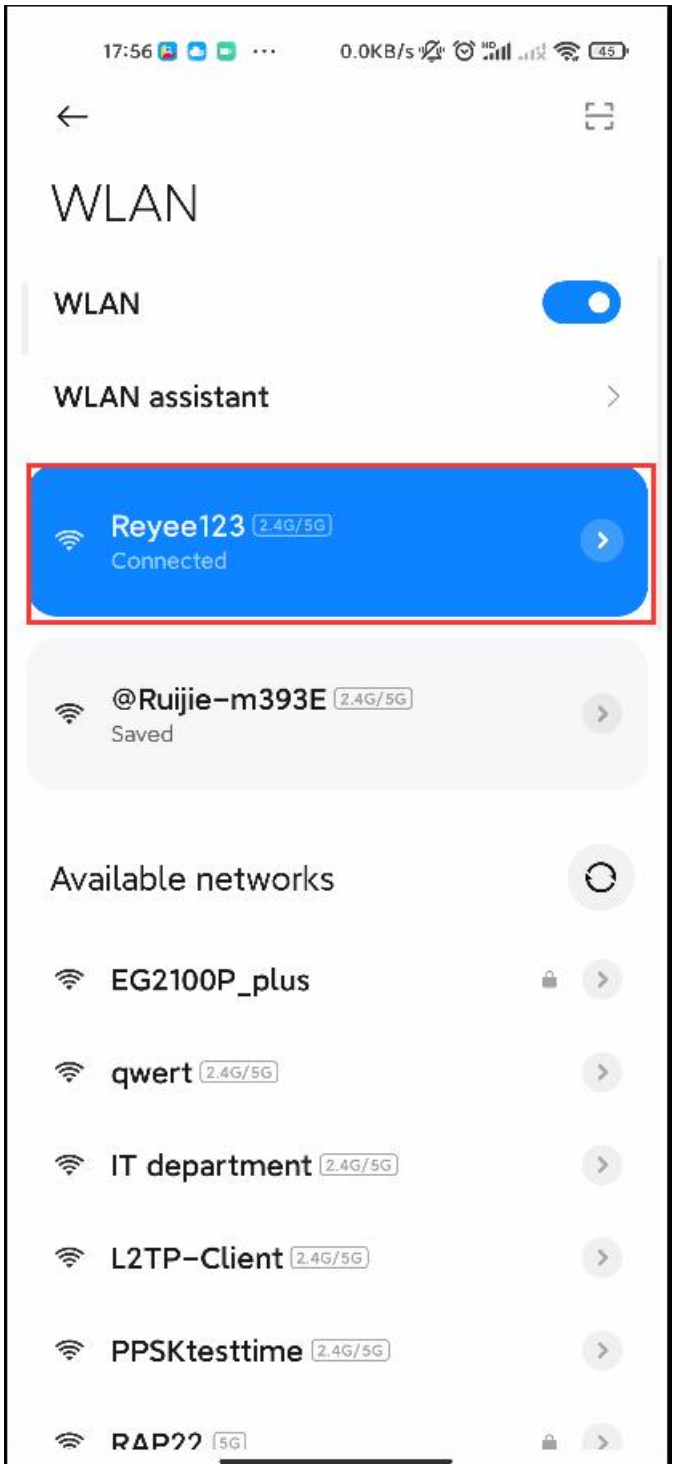
The configuration will be synchronized to the network



After about 3s, Ruijie Cloud App will prompt that the configuration is delivery succeed.

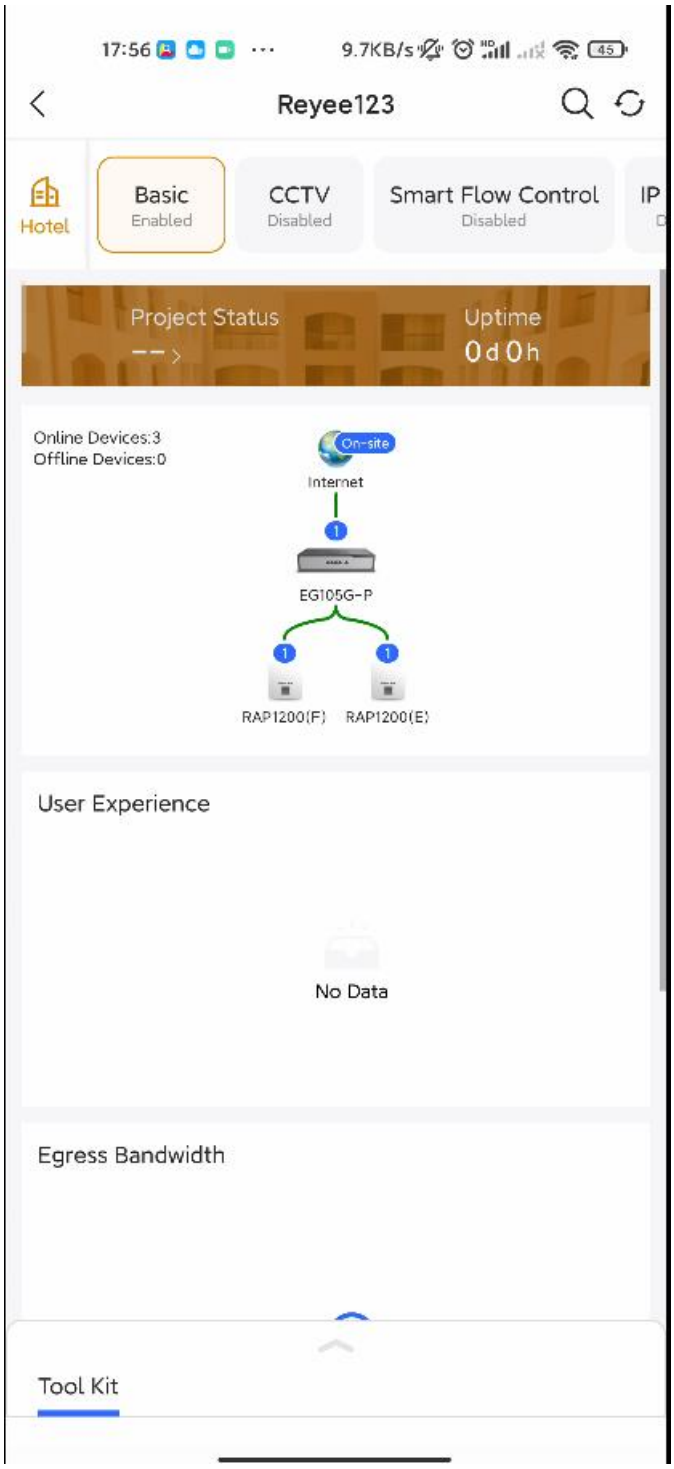


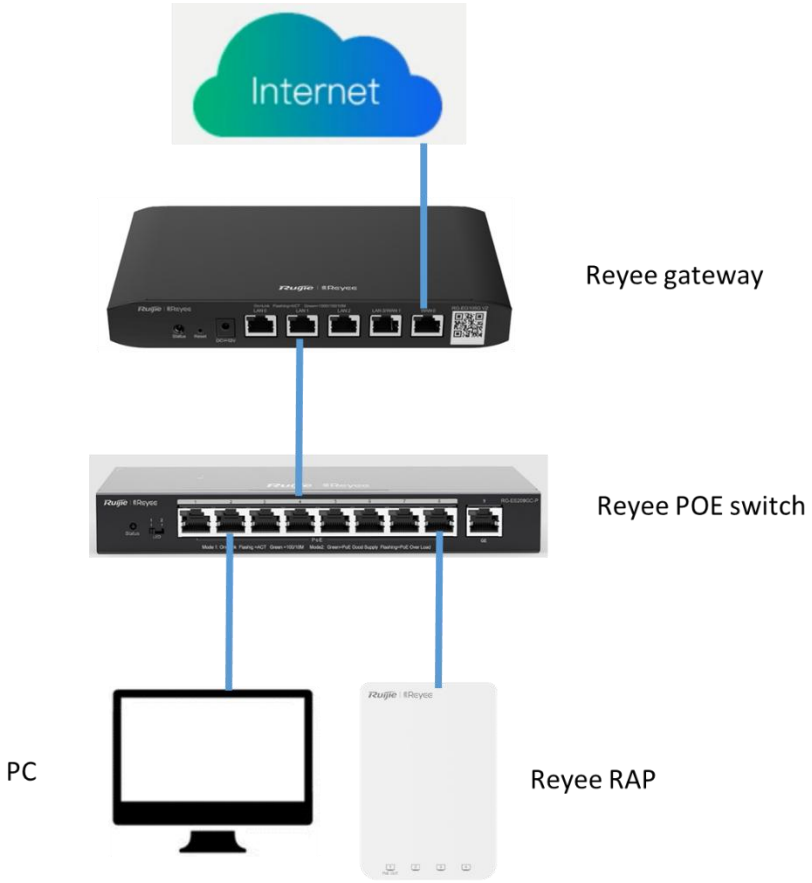
Connect to the SSID created just now to manage the whole network on Cloud App.


17:56
0.0KB/s
WLAN
WLAN
WLAN assistant
Reyee123 2.4G/5G
Connected
@Ruijie-m393E 2.4G/5G
Saved
Available networks
EG2100P_plus
qwert 2.4G/5G
IT department 2.4G/5G
L2TP-Client 2.4G/5G
PPSKtesttime 2.4G/5G

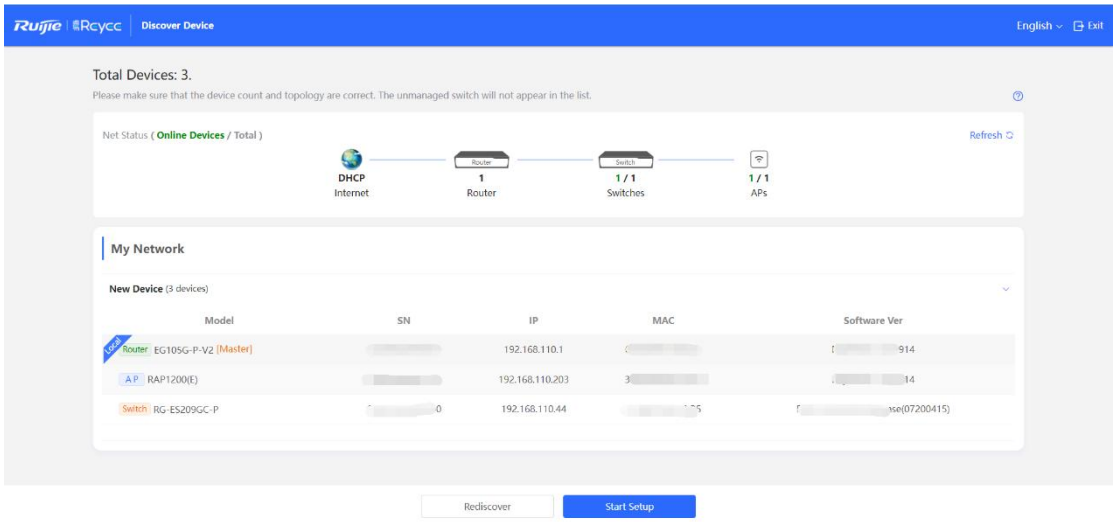
3.2.2 Quick provisioning via Reyee EWeb

The network topology shown in the below picture includes the Reyee gateway, Reyee POE switch and Reyee RAP.

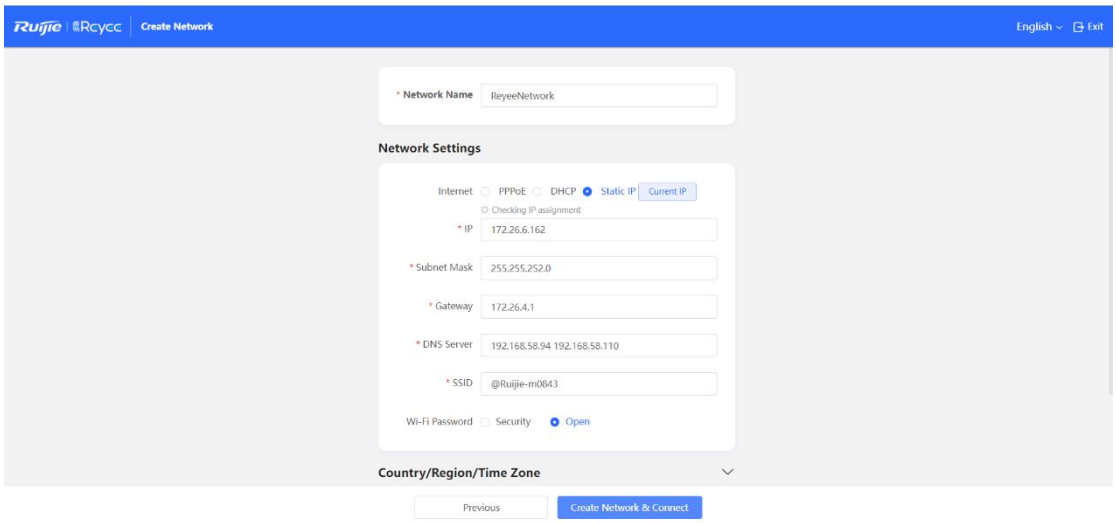


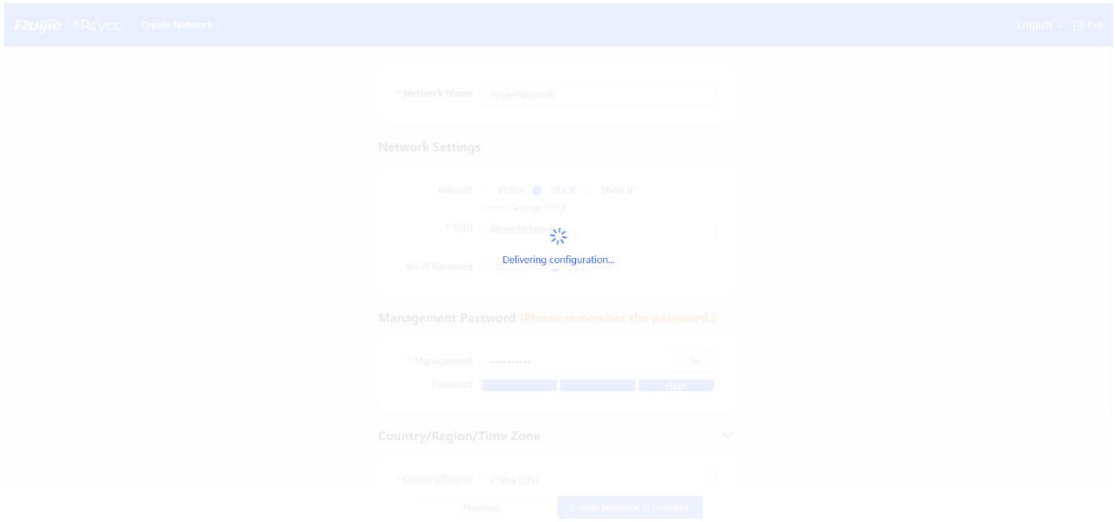


Connect PC to POE switch, set the ip address of PC as static ip address 192.168.110.x, then input 192.168.110.1 on the browser to login the EWEB of EG. All devices in this networks will display in EWEB. Click the Start Setup to perform the quick start of this network.

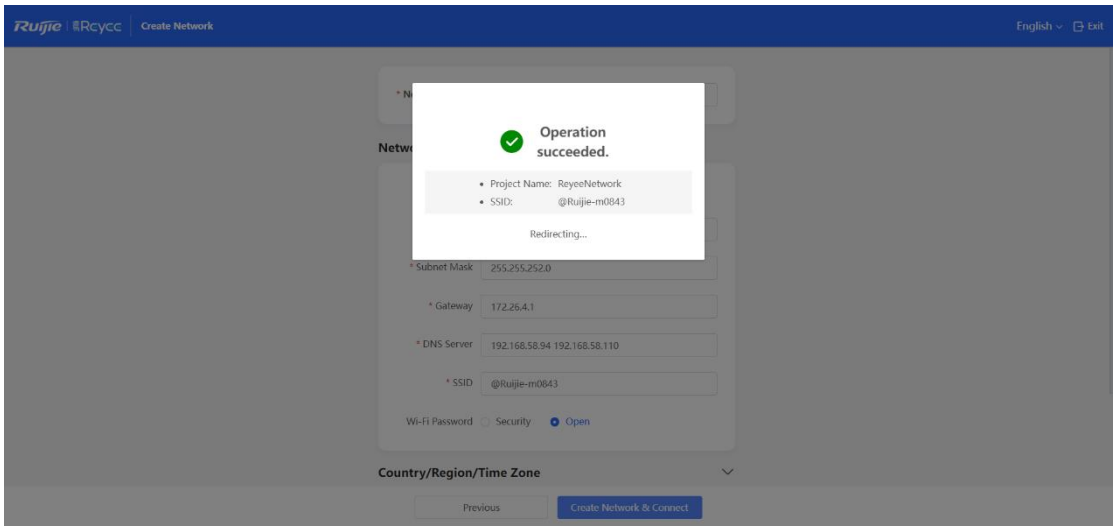


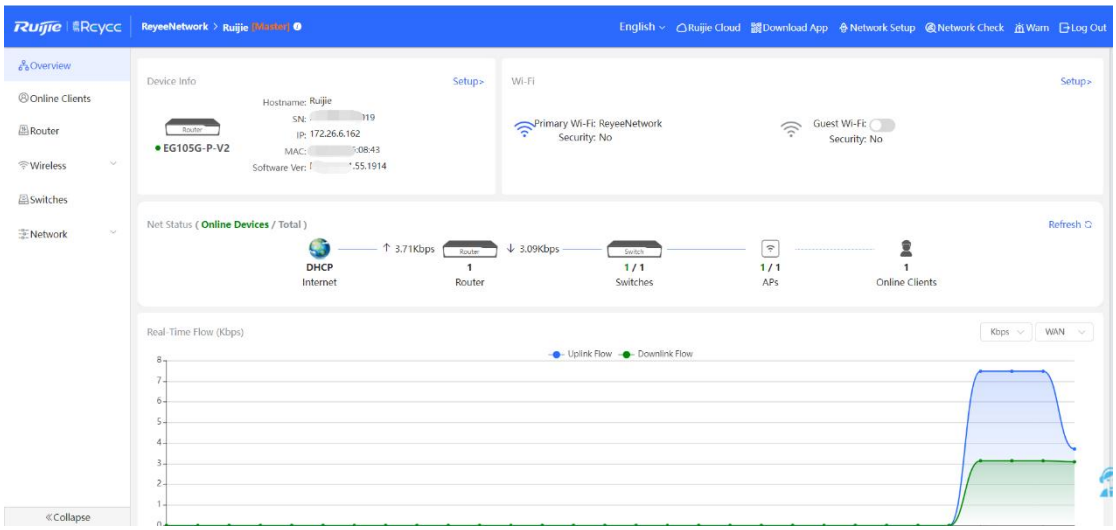
Show in the below picture, to finish the quick start of this network, you need to input the network name, configure the manner to access internet of this network and input the password of SSID or set the SSID as open. After select the Country/Region and click **Create Network & Connect,** the configuration will be delivery and activated, shown as the below two picture.





After the configuration has been delivery and activated, you can enter the overview interface to manage the SON of Reyee devices.




ReyeeNetwork > Ruijie [Master]
English
Ruijie Cloud
Download App
Network Setup
Network Check
Warn
Log Out
Overview
Online Clients
Router
Wireless
Switches
Network
Collapse
Device Info
Setup>
Hostname: Ruijie
IP: 172.26.6.162
EG105G-P-V2
Wi-Fi
Setup>
Primary Wi-Fi: ReyeeNetwork
Security: No
Guest Wi-Fi:
Security: No
Net Status (Online Devices / Total)
Refresh
3.71Kbps
3.09Kbps
DHCP
Internet
1
Router
1 / 1
Switches
1 / 1
APs
1
Online Clients
Real-Time Flow (Kbps)
Kbps
WAN
Uplink Flow
Downlink Flow

4 Configuration

4.1 Reyee EG Series Router Configuration

4.1.1 Network Access Setting

Application Scenario

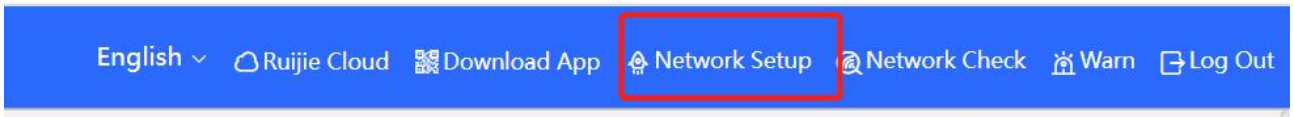
Preparation

Need provide an uplink cable which can access internet.

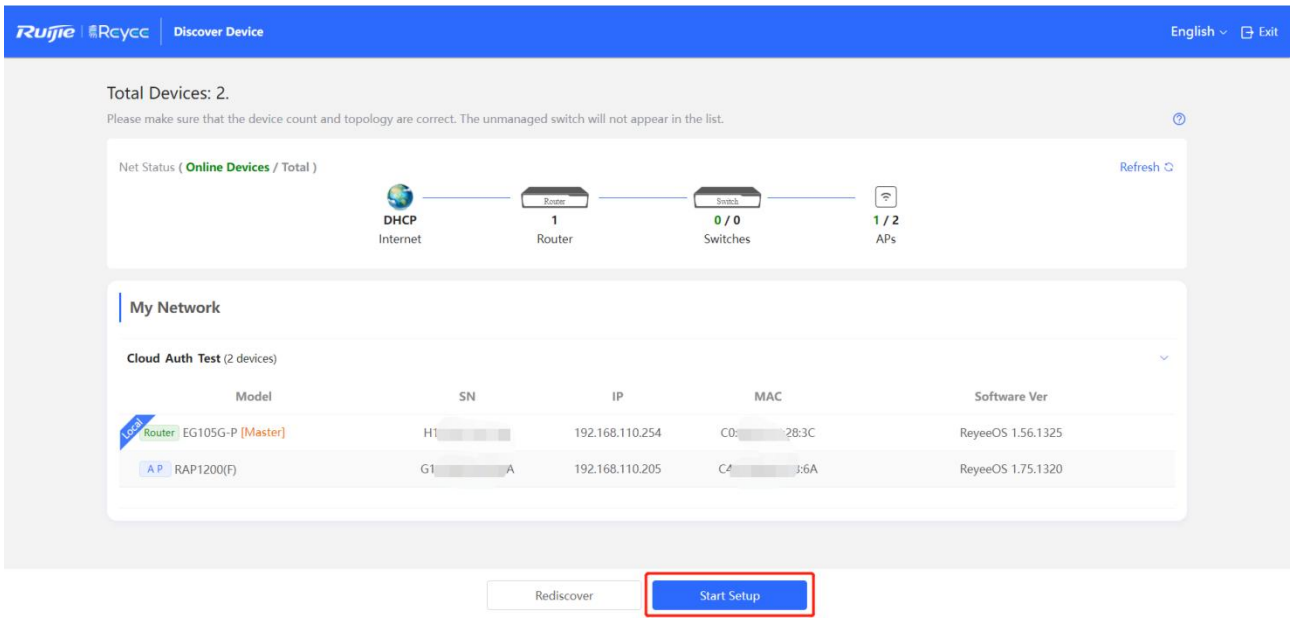
Procedure

4.1.1.1 PPPoE setting with WAN port

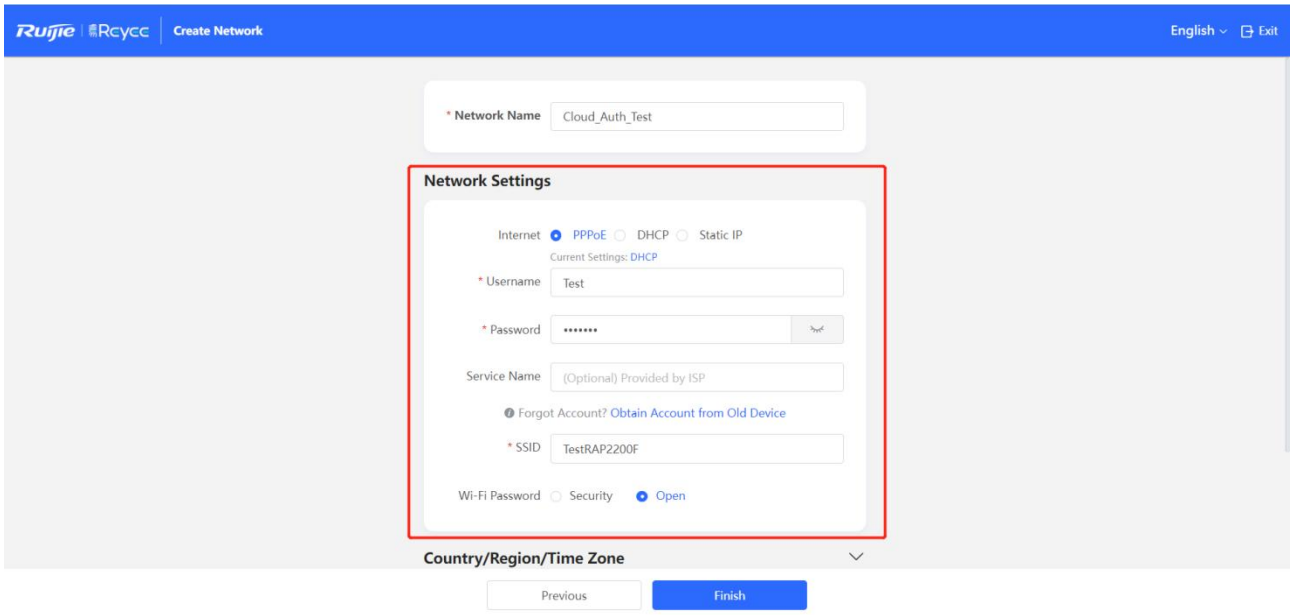
1.1 Click Network Setup to enter the network setting page.



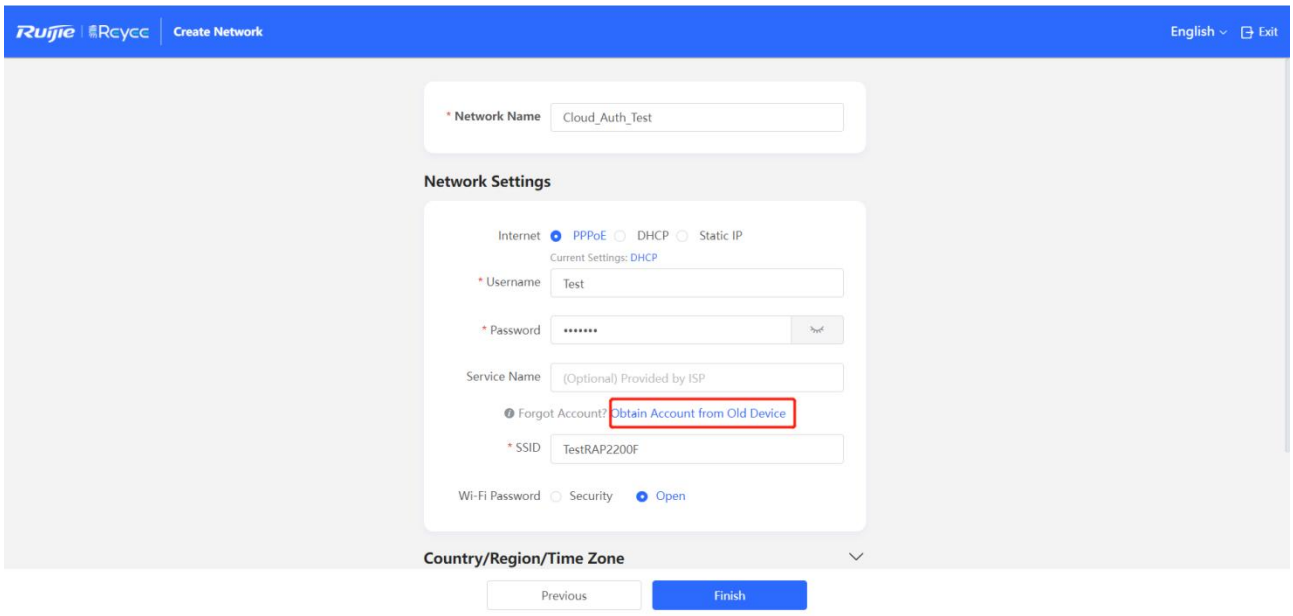
1.2 Click Start Setup

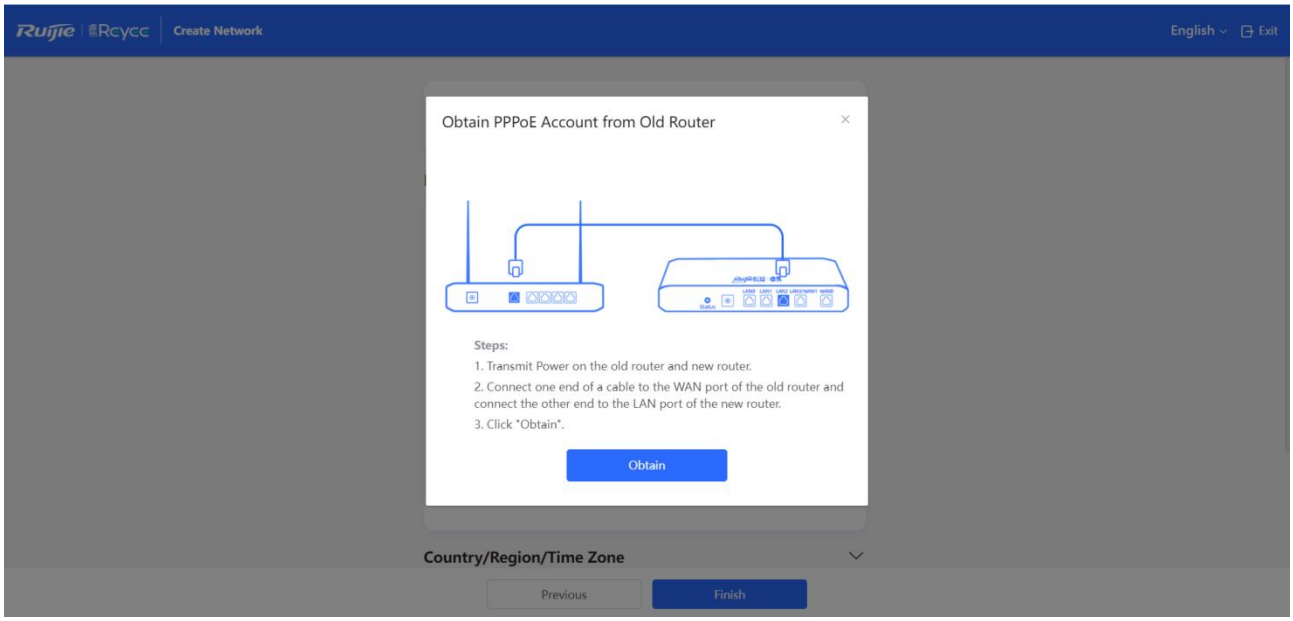


1.3 Choose **PPPoE**, enter your **Username** and **Password** which get from the ISP. The Service Name is optional



1.4 If you forgot the password from ISP, please click **Obtain Account from Old Device**





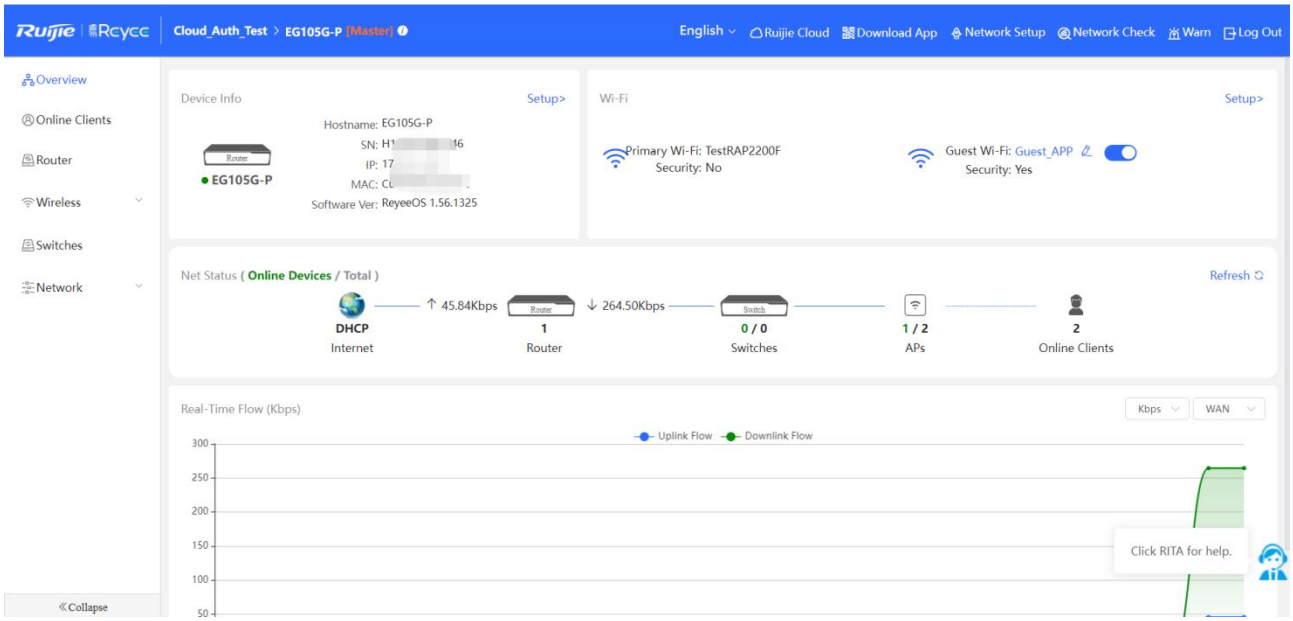
Steps:

1) Power on the old router and new router.

2) Connect one end of a cable to the WAN port of the old router and connect the other end to the LAN port of the new router.

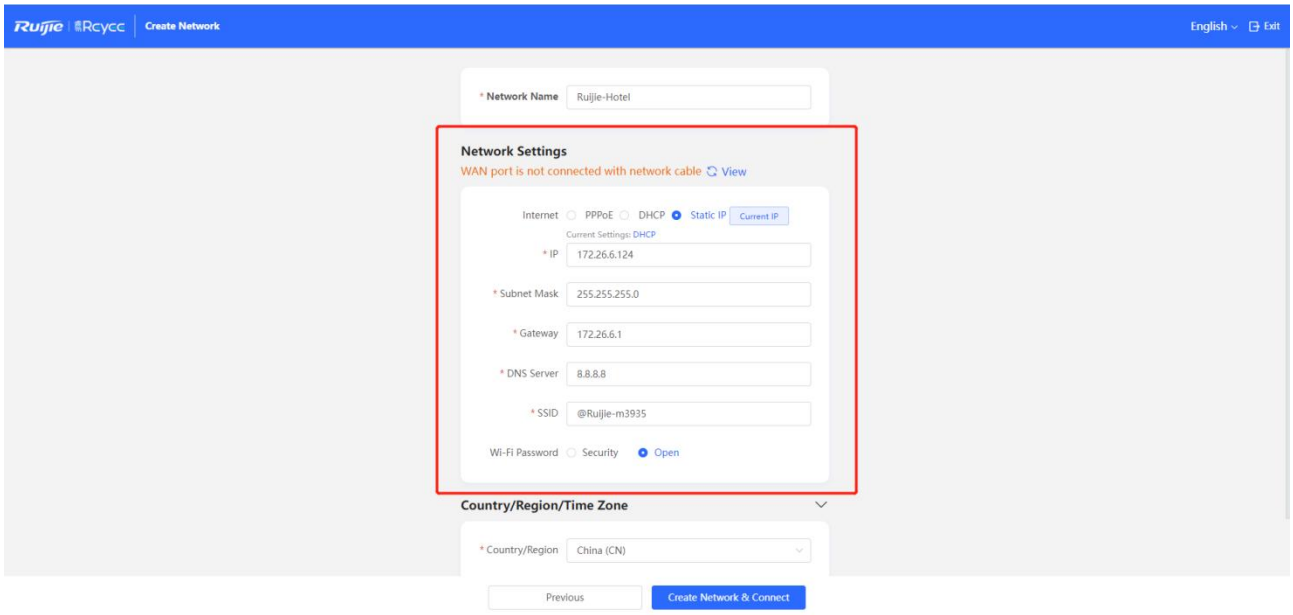
3) Click **"Obtain".**

After enter the PPPoE information, click **Finish** to enter the main eWeb page. The Router will get the internet from ISP.



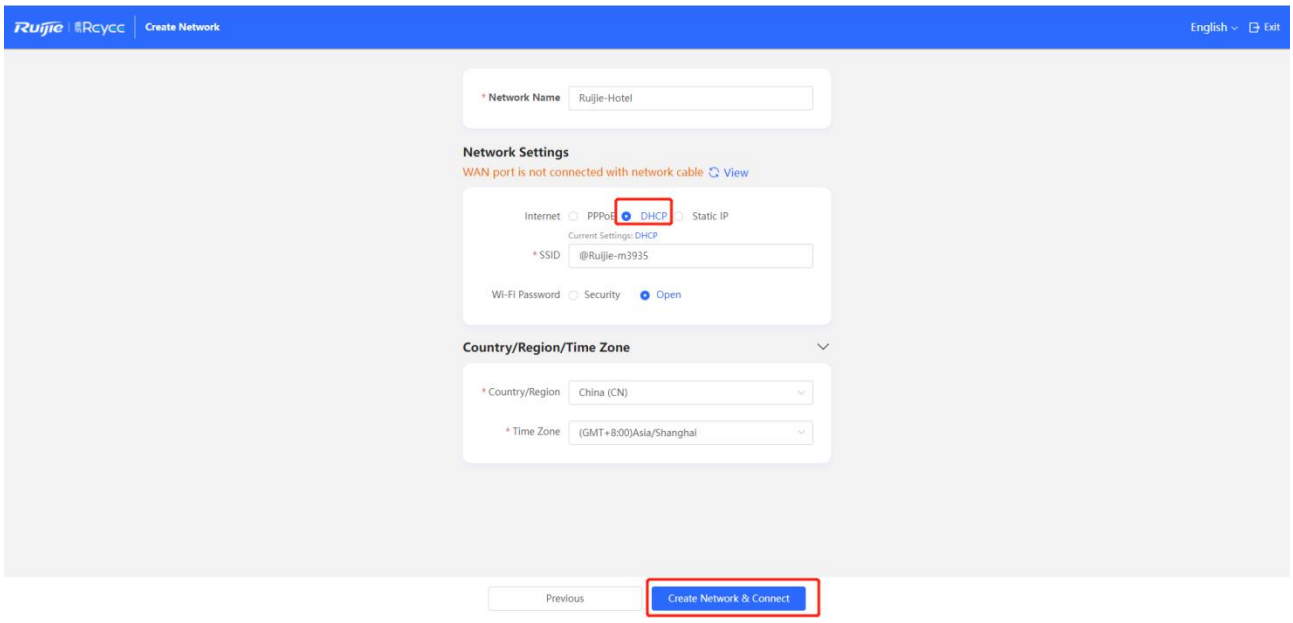
4.1.1.2 Static IP setting with WAN port

Choose **Static IP** on **Network Setup page**, and fill in IP, Subnet Mask, Gateway IP, DNS server information. Then click **Create Network & Connect.**



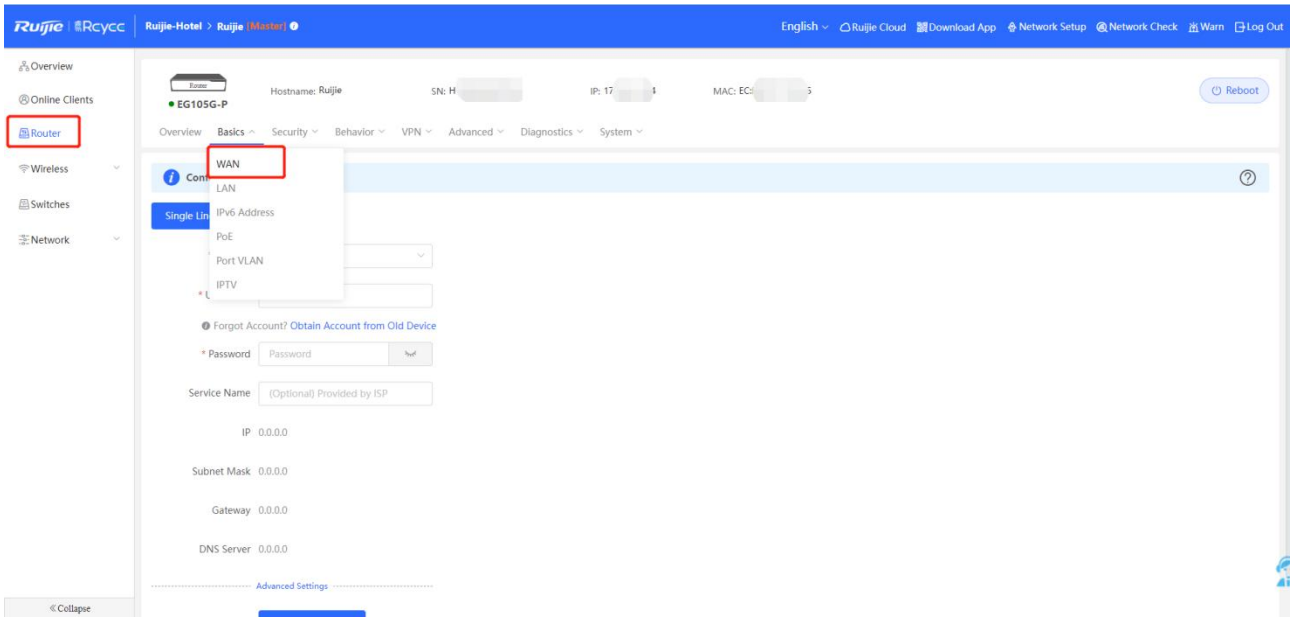
4.1.1.3 DHCP IP setting with WAN port

Choose **DHCP** on **Network Setup** page, then click **Create Network & Connect.**



> **Sign**
>
> You can configure the WAN setting through the following page too.

Click **Router->Basics->WAN.**



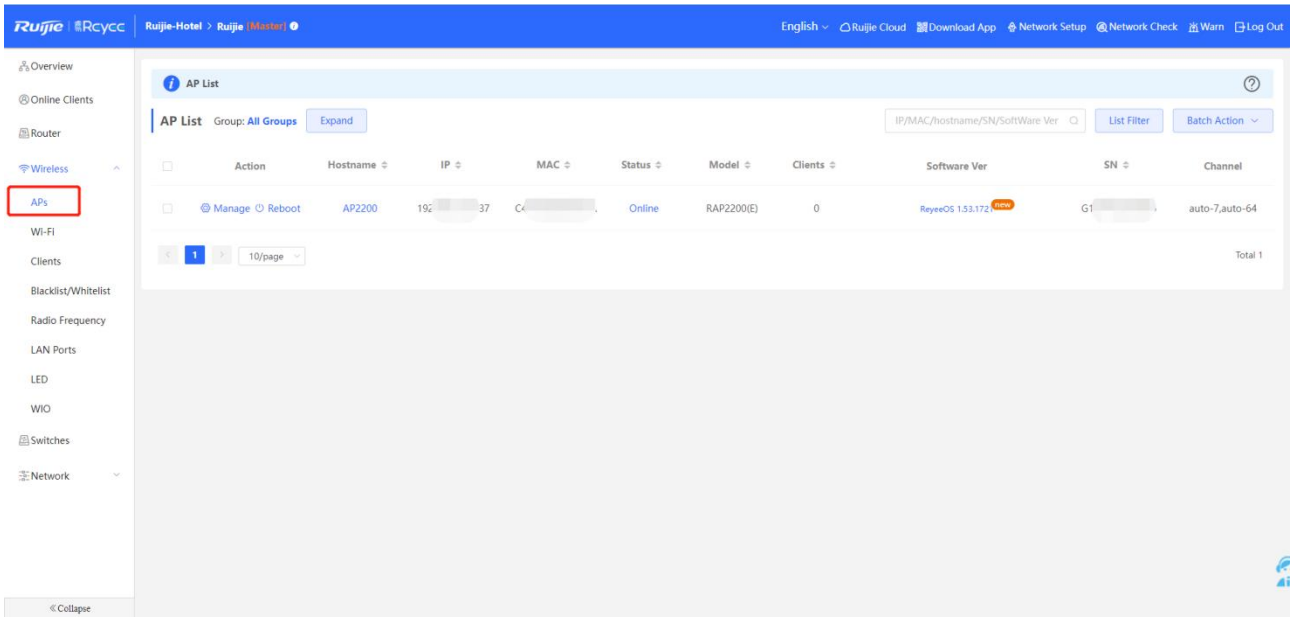
4.1.2 Wireless Setting

Application Scenario

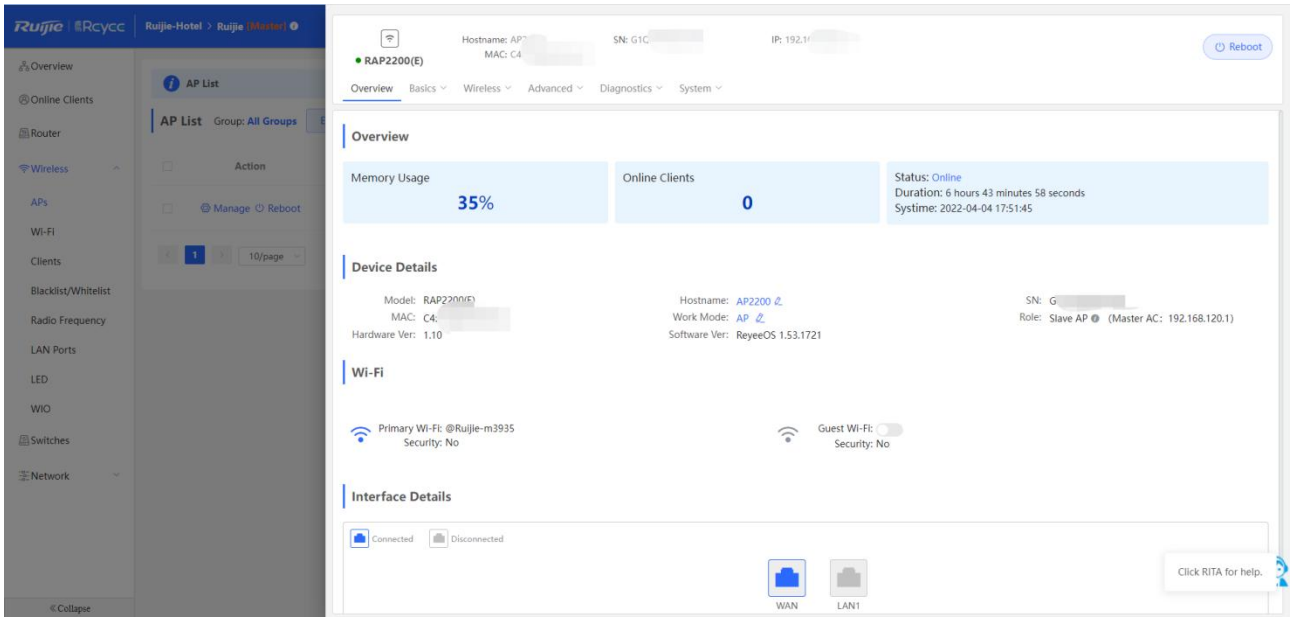
Procedure

4.1.2.1 Wireless->APs

The APs page displays all APs which are managed by Router. The information including AP's **Hostname, IP, MAC, Status, Model, Wireless Clients Number, Software Version, SN and Radio Channel** could be seen in this page.. you also can see categories of the APs by Clicking .



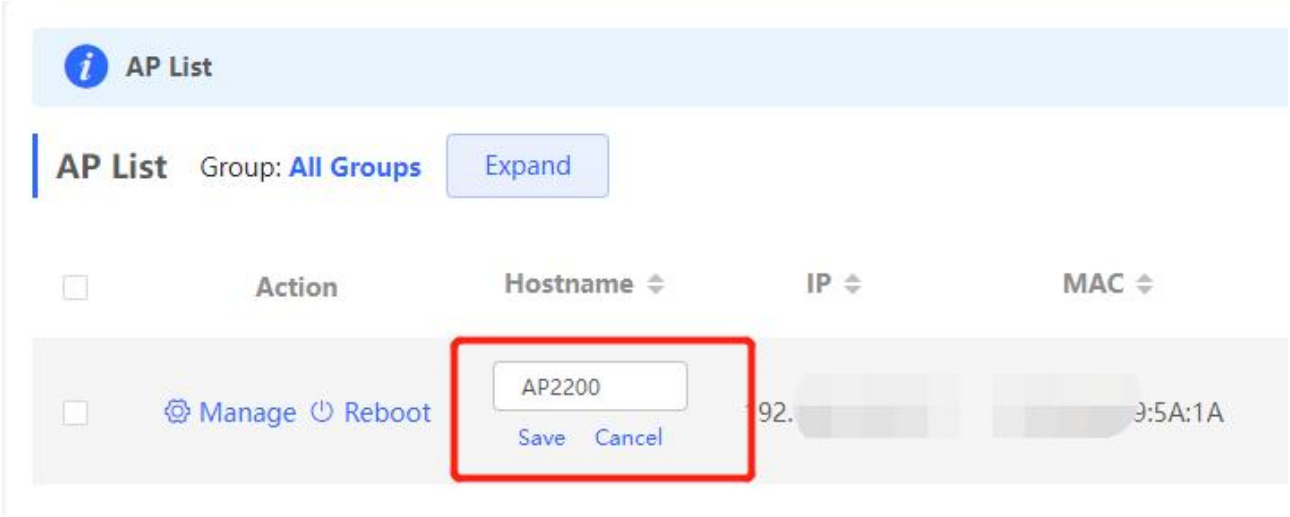
Manage: Go to the AP detail setting page



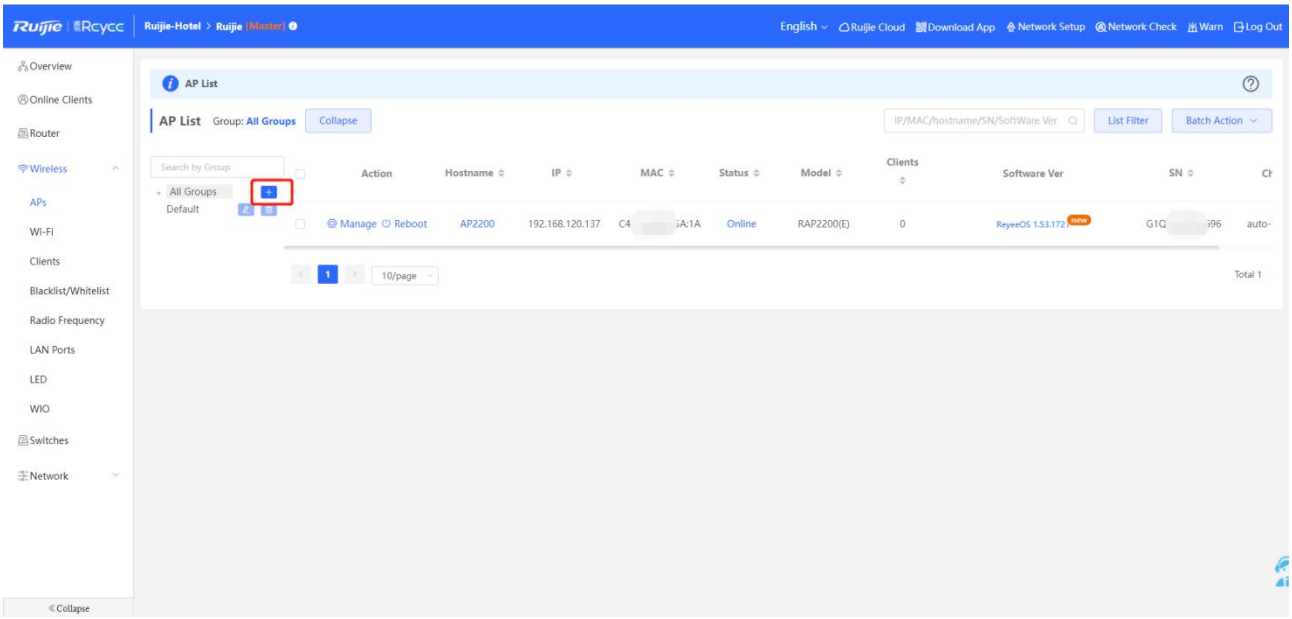
Reboot: Reboot the AP

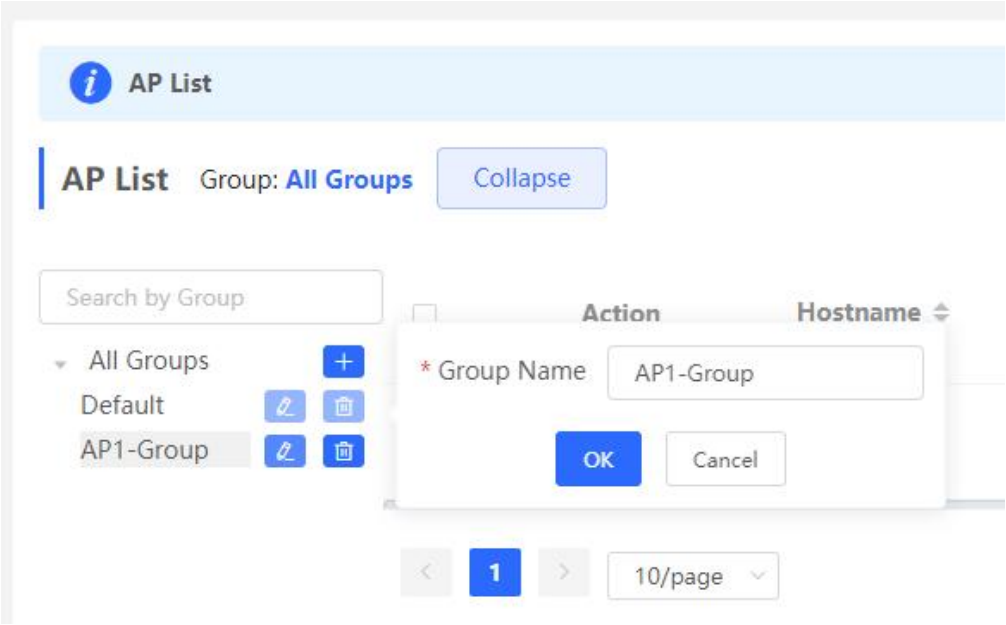
Online: Show the SON status of AP.

Hostname: Click to modify the hostname of AP



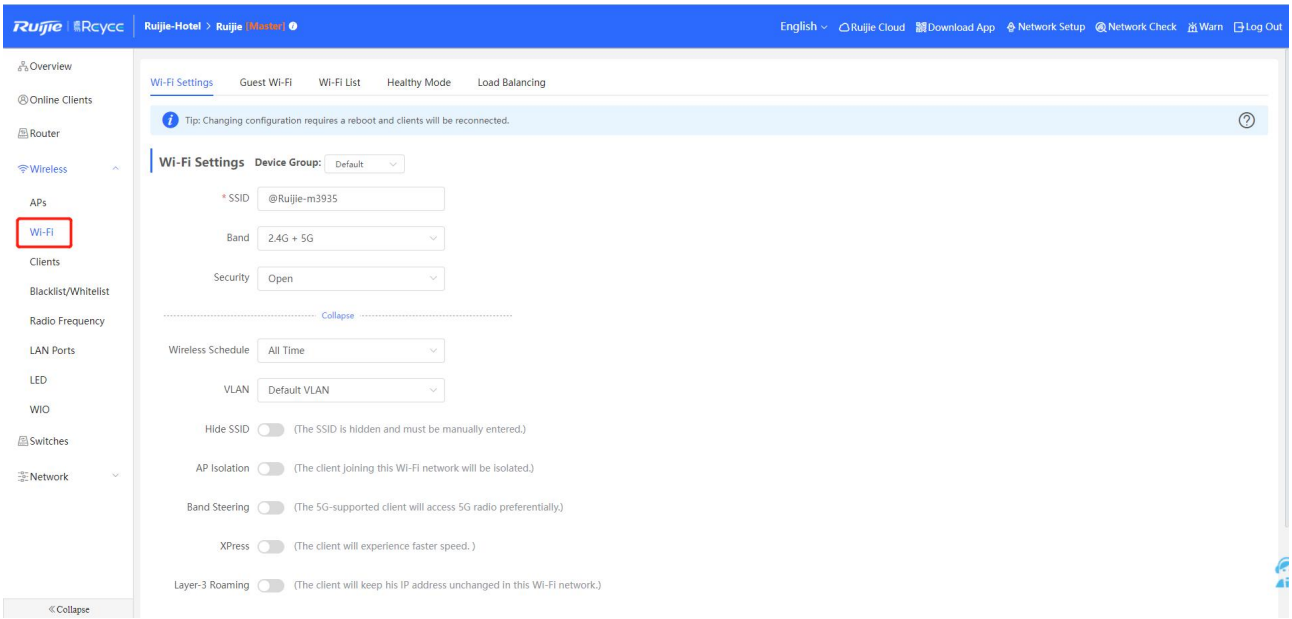
Expand: Go to **Device Group Page**, can add new device group.





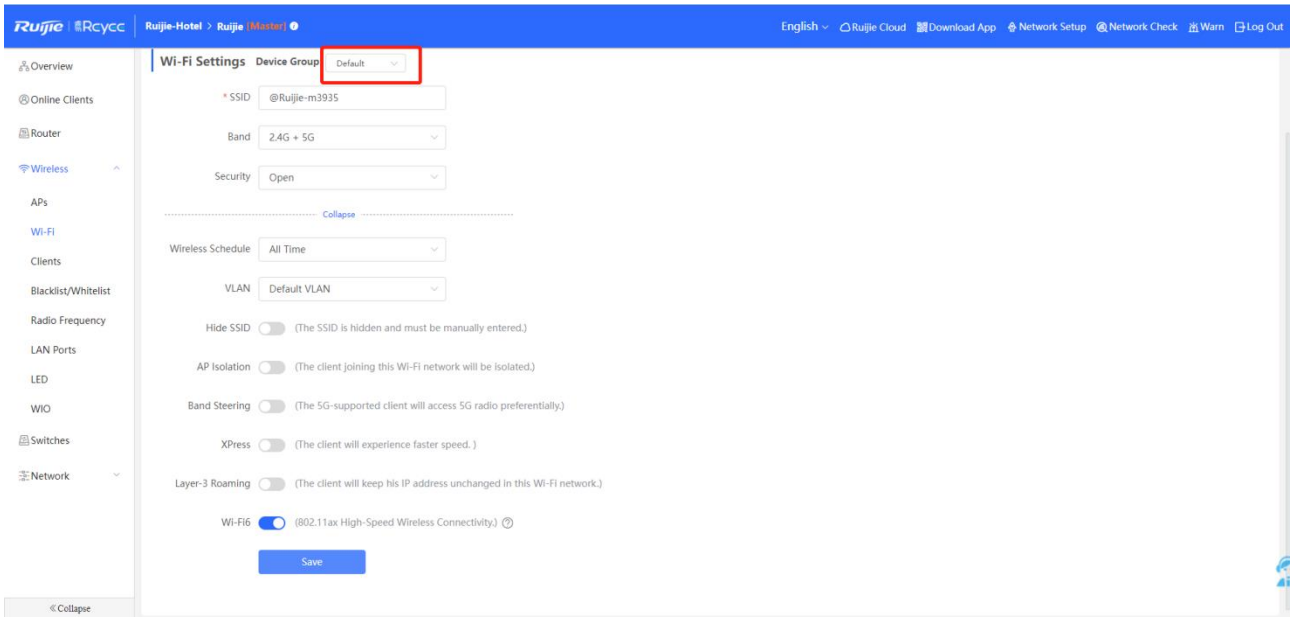
4.1.2.2 Wireless->Wi-Fi

This page has the Wi-Fi Setting, Guest Wi-Fi, Wi-Fi List, Healthy Mode, Load Balancing functions.



1. Wi-Fi Settings

Click the **Device Group** to choose the AP group, then can set the Wi-Fi settings for that AP group.



SSID: SSID name

Band: 2.4G+5G, 2.4G, 5G

Security: Open, WPA-PSK,WPA2-PSK, WPA_WPA2-PSK

Wireless Schedule: All Time, Weekdays, Weekends, Custom

VLAN: Choose the VLAN used by this Wi-Fi Clients.

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

AP Isolation: The client joining this Wi-Fi network will be isolated.

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

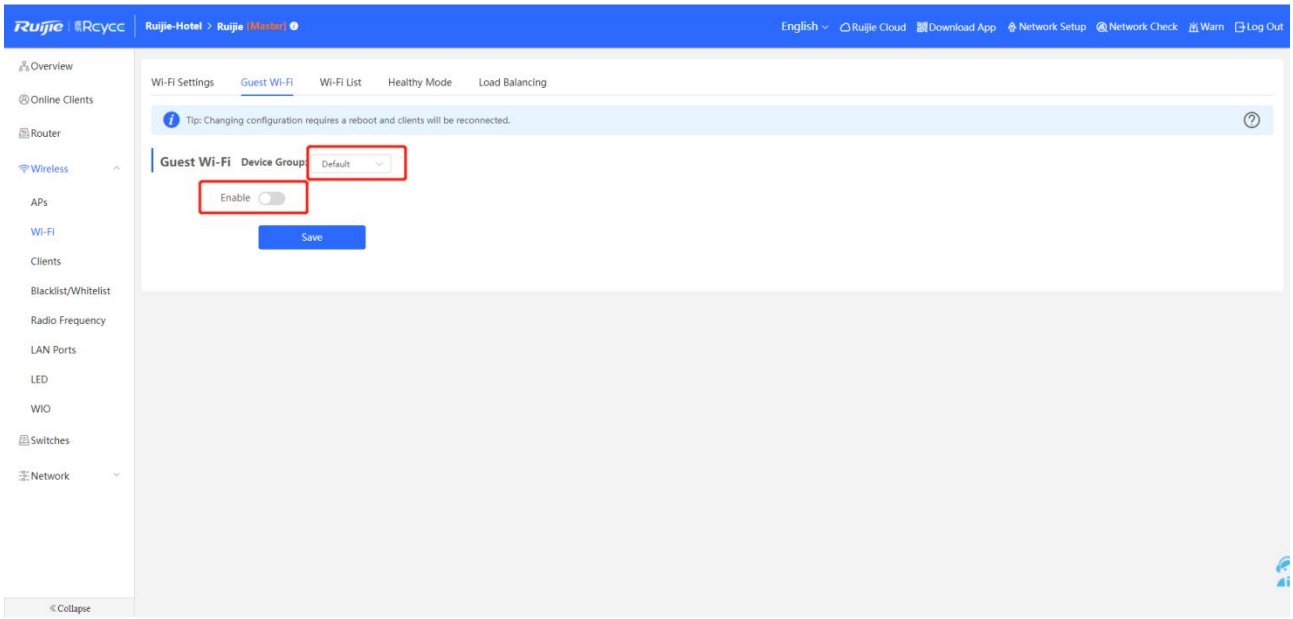
XPress: The client will experience faster speed.

Layer-3 Roaming: The client will keep his IP address unchanged in this Wi-Fi network.

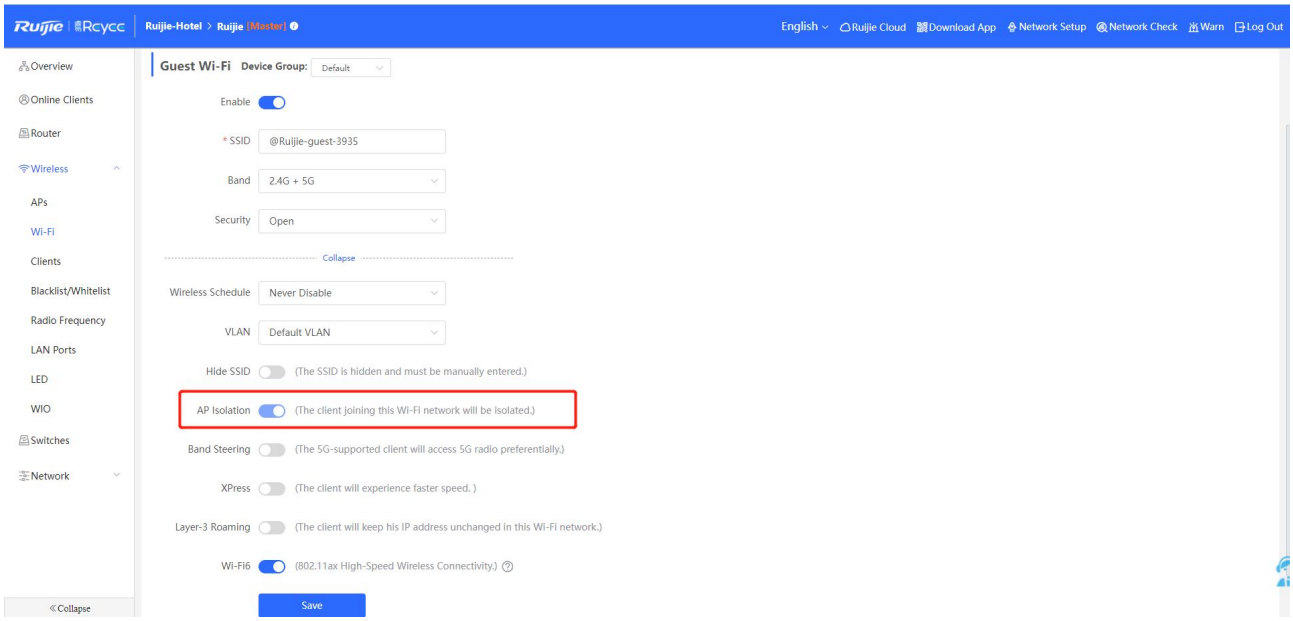
Wi-Fi 6: 802.11ax High-Speed Wireless Connectivity.

2. Guest Wi-Fi

Click **Device Group** to choose the AP group, then can set the Guest Wi-Fi settings for that AP group. Click **Enable** to enable Guest Wi-Fi.

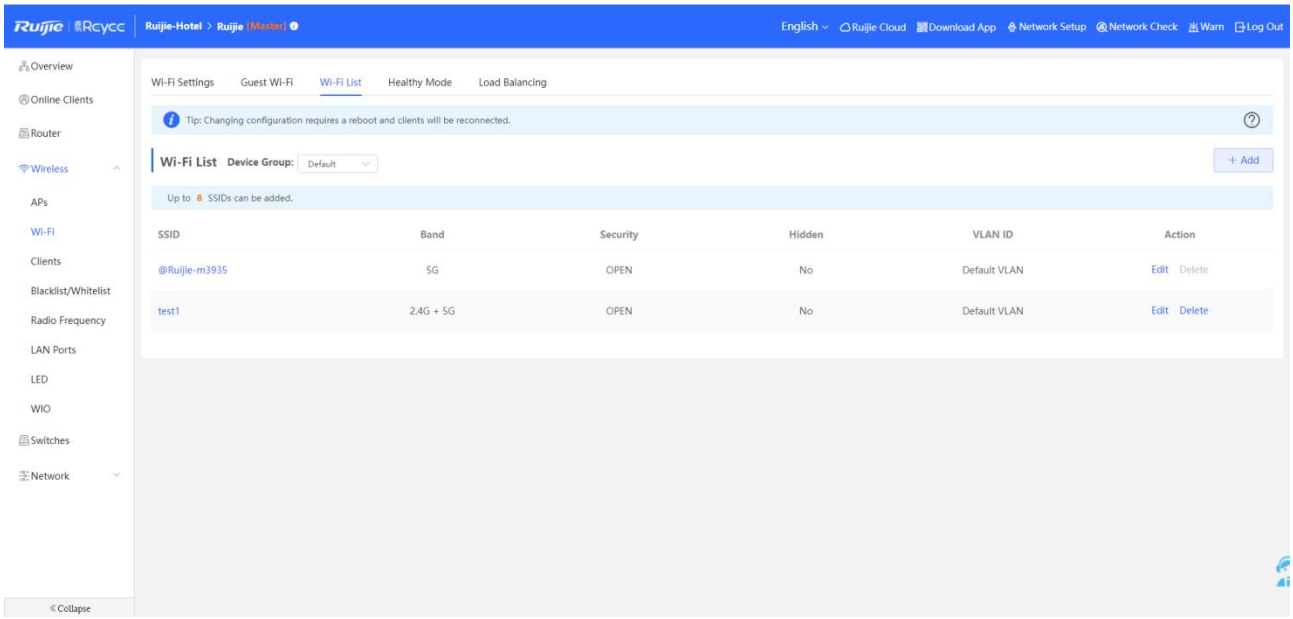


The Guest Wi-Fi will enable **AP Isolation** default and can't be disabled, others are same with normal Wi-Fi.



3. Wi-Fi List

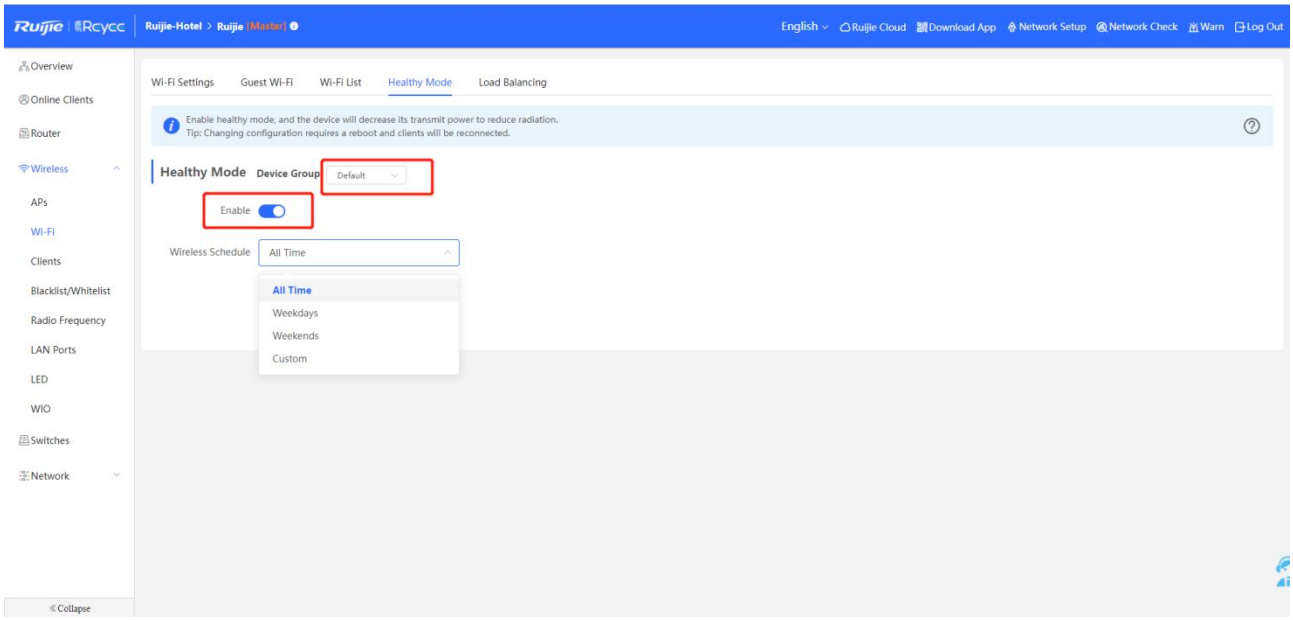
There are up to 8 SSIDs can be added for per AP group. But the default SSID can't been removed.



4. Healthy Mode

Enable **Healthy Mode**, and the device will decrease it's transmit power to reduce radiation.

You can enable the **Healthy Mode** base on **Device Group** and Choose the Working schedule.

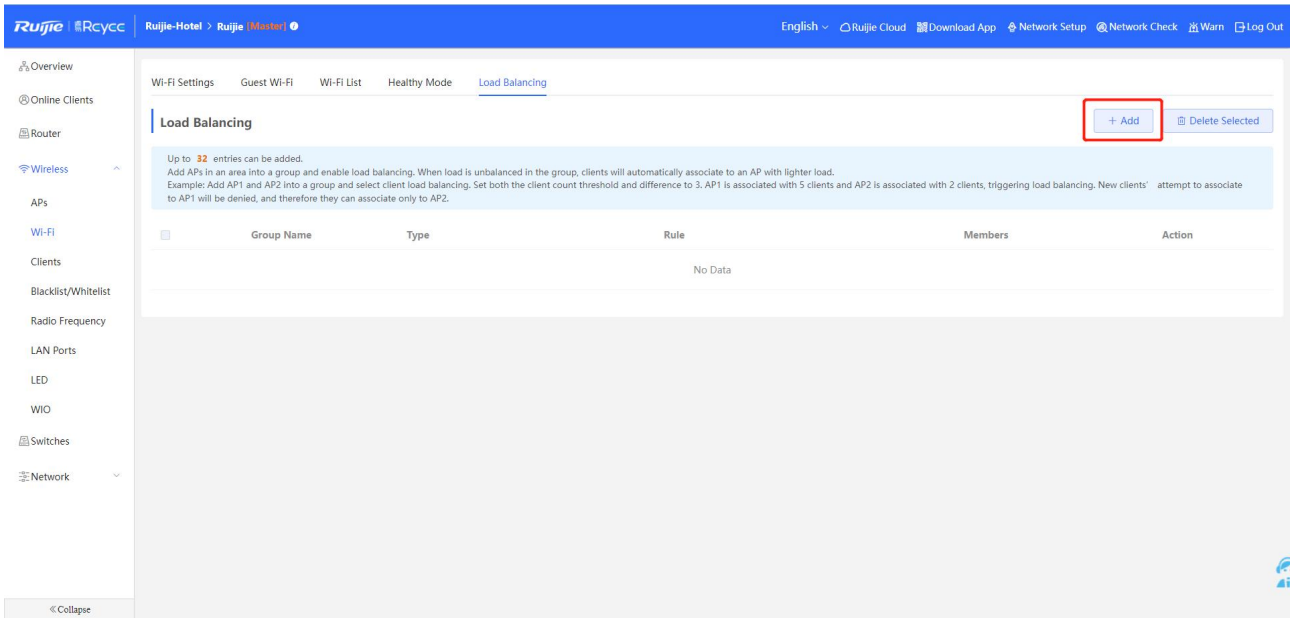


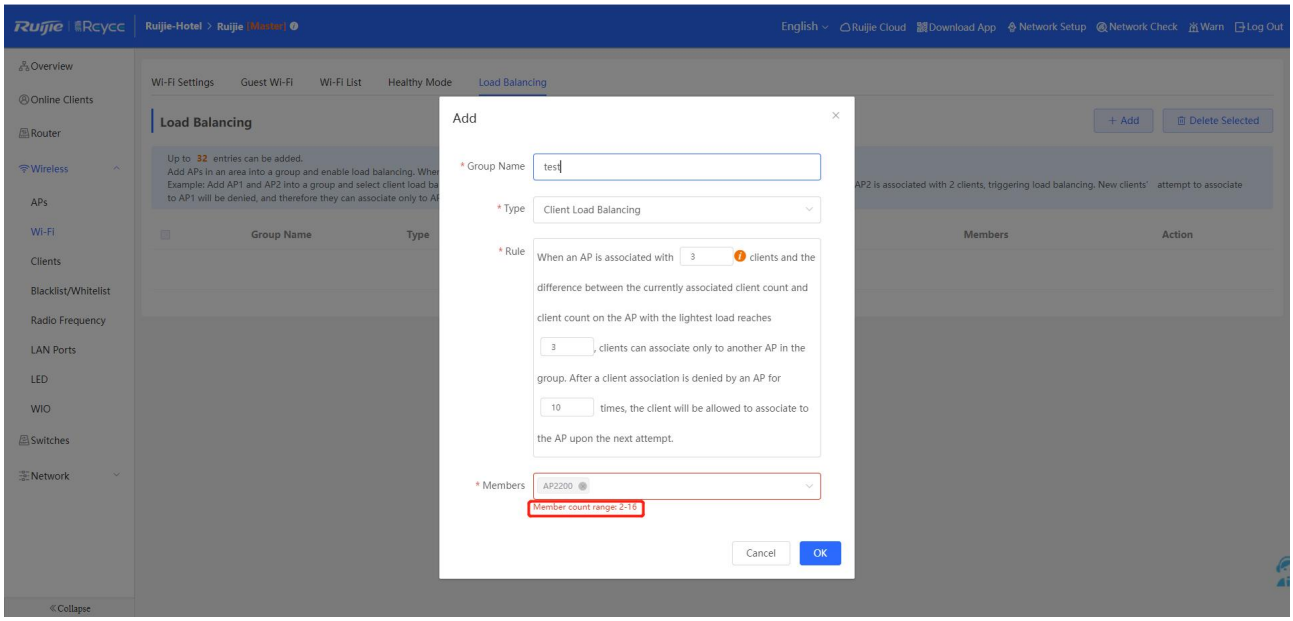
> ⚠ Note:
>
> Changing configuration requires to reboot your devices and clients will be reconnected.

5. Load Balancing

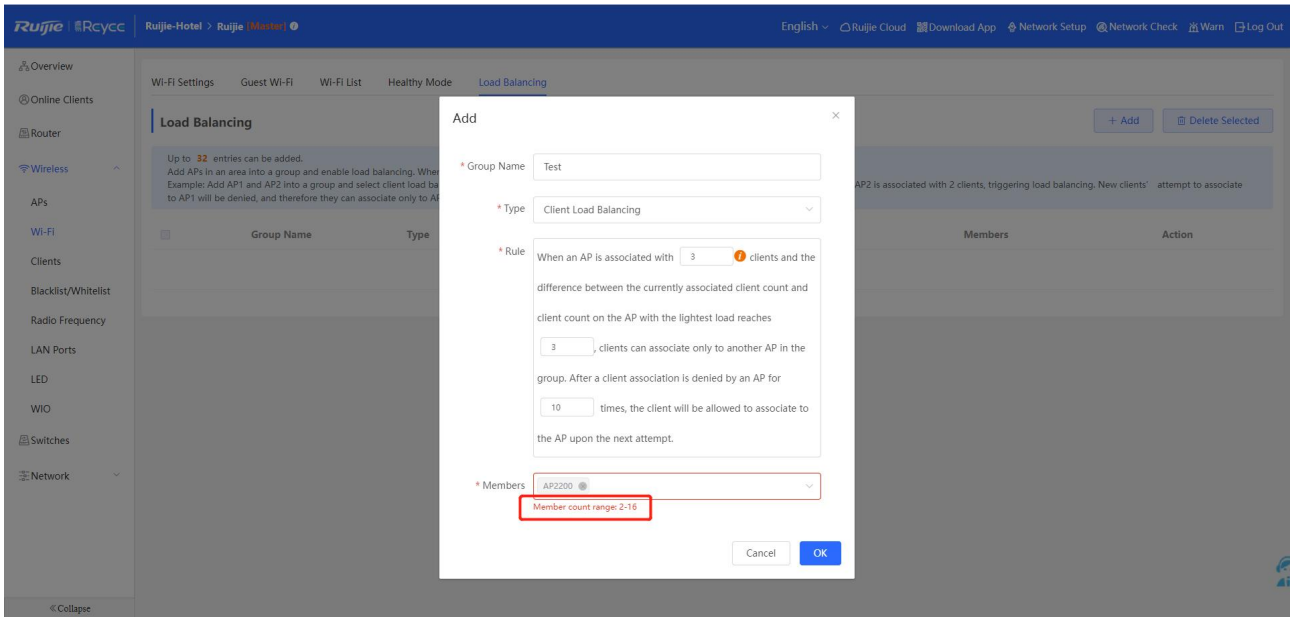
Add APs in the area into a group and enable load balancing. When load is unbalanced in the group, clients will automatically associate to an AP with lighter load.

Example: Add AP1 and AP2 into a group and select client load balancing. Set both the clients count threshold and difference value to 3. when AP1 is associated with 5 clients and AP2 is associated with 2 clients, the load balancing will be triggered. The association request of new clients to AP1 will be denied, and therefore they can only associate to AP2.



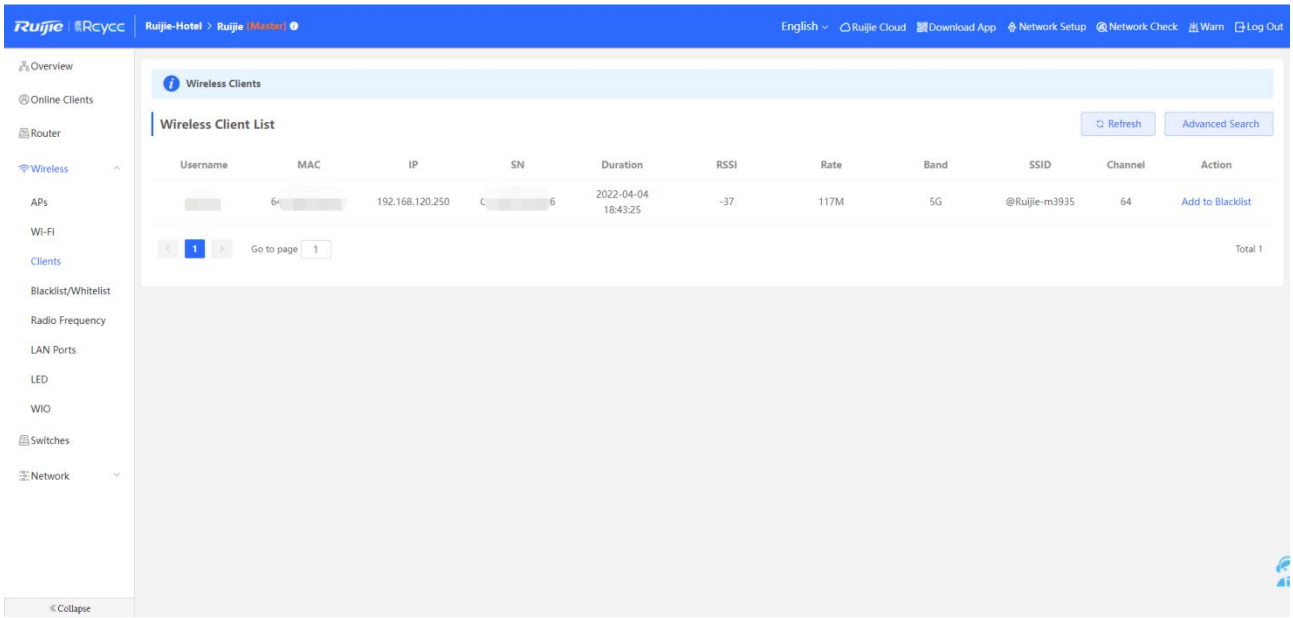


> **Note**
>
> Up to 32 entries can be added.
>
> Member count range: 2-16.

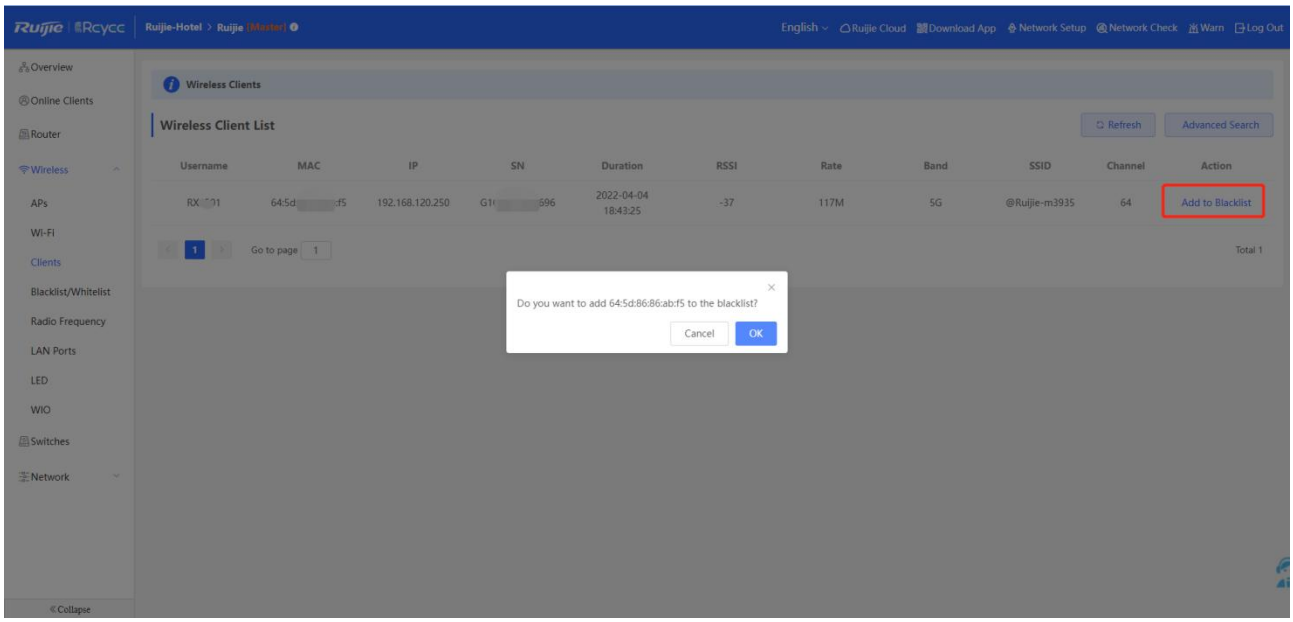


4.1.2.3 Wireless->Clients

The Wireless Client List displays **Username, MAC, IP, SN, Duration, RSSI, Rate, Band, SSID, Channel, Action.**



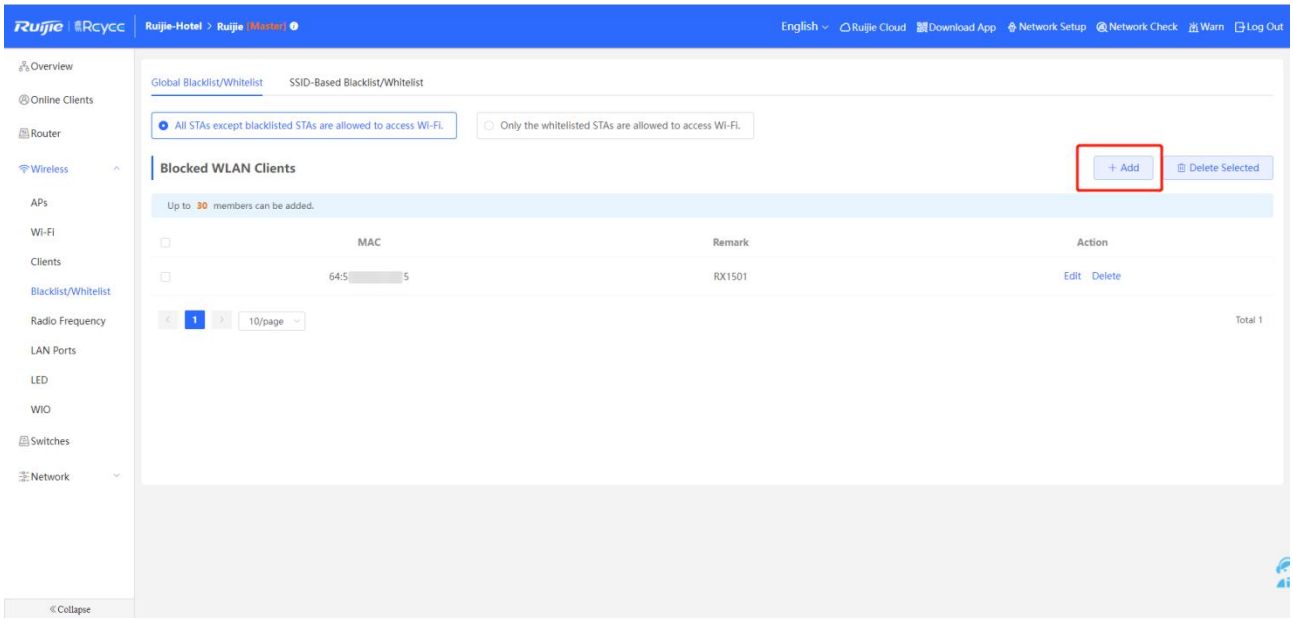
Click Add to **Blacklist** can add the client to blacklist.

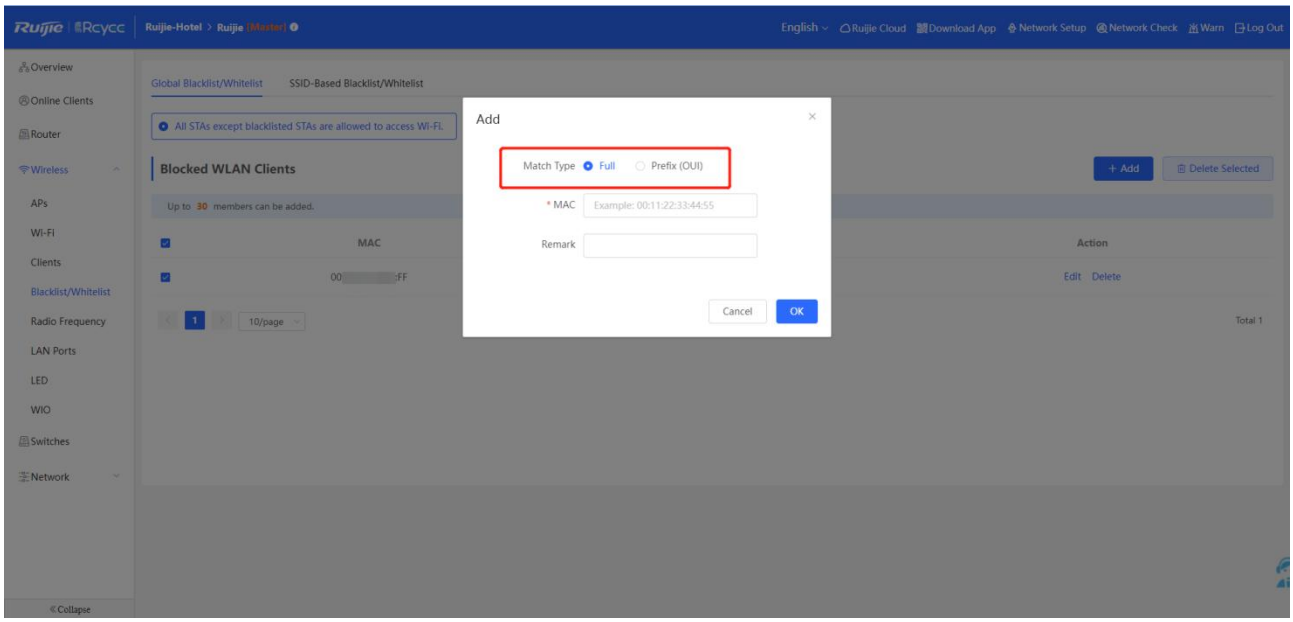


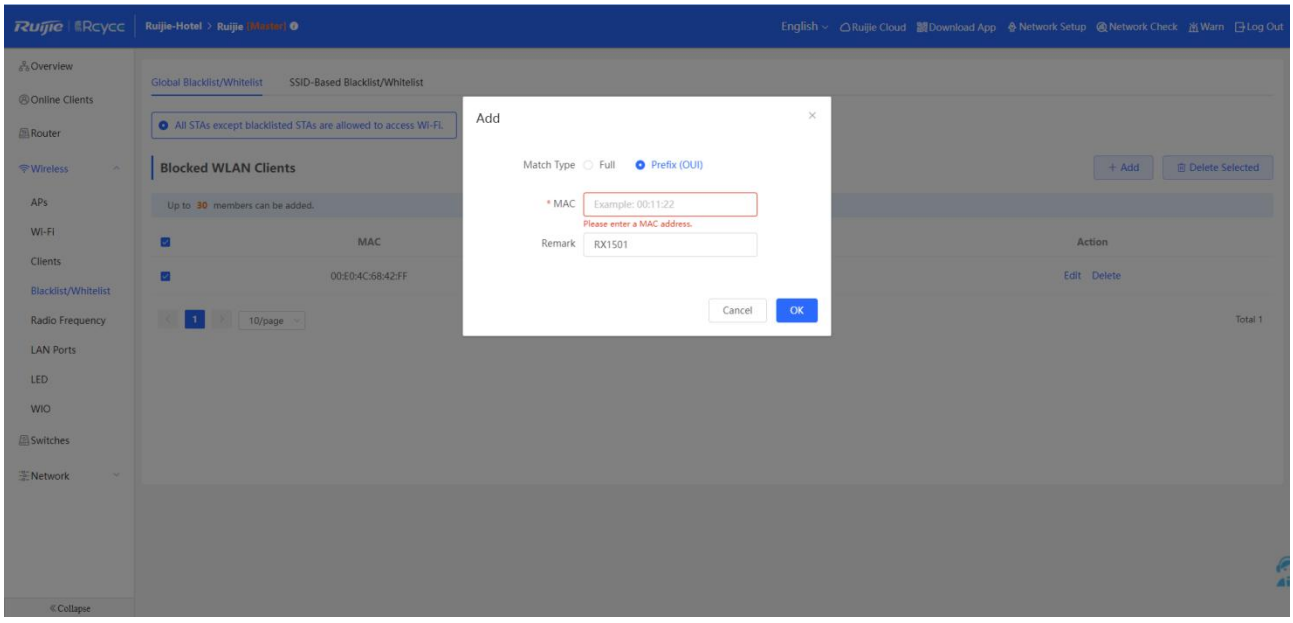
4.1.2.4 Wireless->Blacklist/Whitelist

1. Global Blacklist/Whitelist

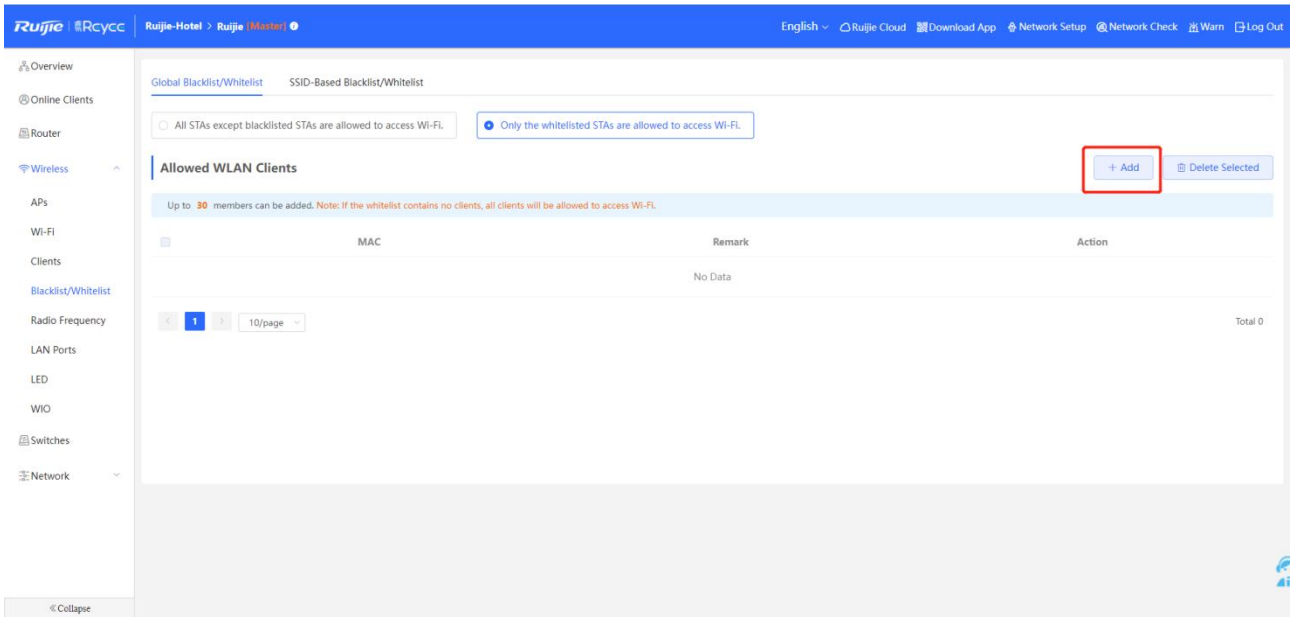
Choose All STAs except blacklisted STAs are allowed to access Wi-Fi, then you can click Add to add the blacklist WLAN clients. With the Client, you can add with full MAC address or prefix of mac address.




Ruijie-Hotel > Ruijie
English
Ruijie Cloud
Download App
Network Setup
Network Check
Warn
Log Out
Overview
Online Clients
Router
Wireless
APs
WI-FI
Clients
Blacklist/Whitelist
Radio Frequency
LAN Ports
LED
WIO
Switches
Network
Collapse
Global Blacklist/Whitelist
SSID-Based Blacklist/Whitelist
All STAs except blacklisted STAs are allowed to access Wi-Fi.
Blocked WLAN Clients
+ Add
Delete Selected
Up to 30 members can be added.
MAC
Action
Edit Delete
10/page
Total 1
Add
Match Type Full Prefix (OUI)
* MAC
Example: 00:11:22:33:44:55
Remark
Cancel
OK

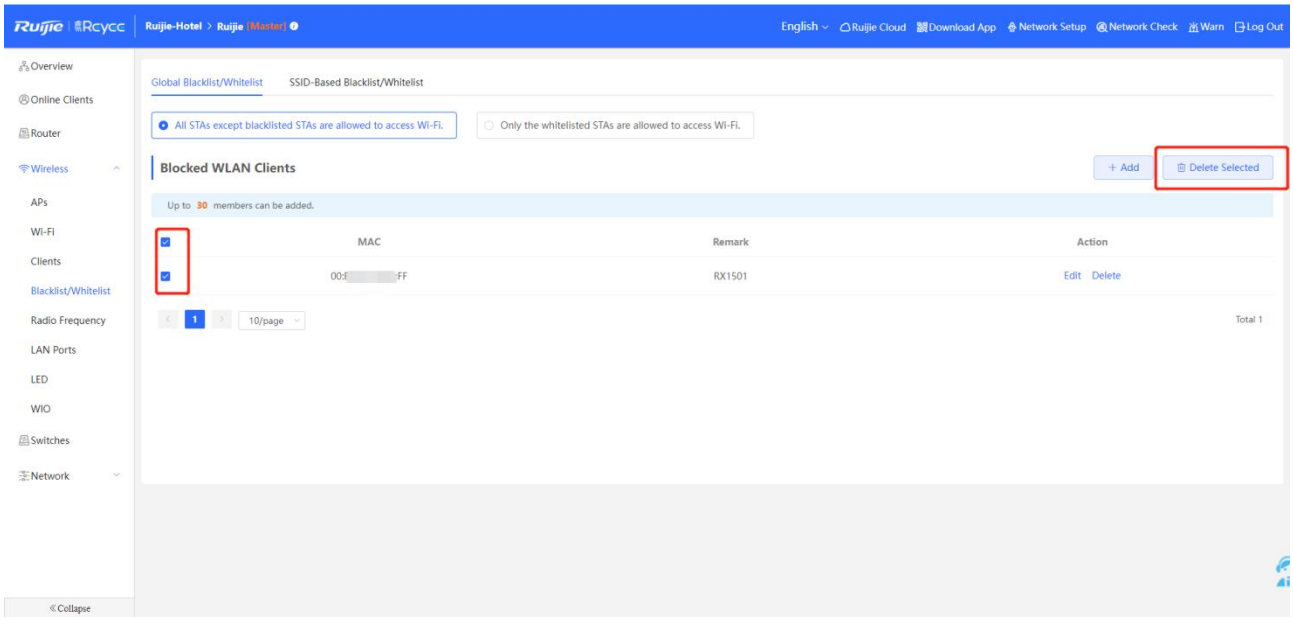

Ruijie-Hotel > Ruijie
English
Ruijie Cloud
Download App
Network Setup
Network Check
Warn
Log Out
Overview
Online Clients
Router
Wireless
APs
WI-FI
Clients
Blacklist/Whitelist
Radio Frequency
LAN Ports
LED
WIO
Switches
Network
Collapse
Global Blacklist/Whitelist
SSID-Based Blacklist/Whitelist
All STAs except blacklisted STAs are allowed to access Wi-Fi.
Blocked WLAN Clients
+ Add
Delete Selected
Up to 30 members can be added.
MAC
Action
00:E0:4C:68:42:FF
Edit Delete
10/page
Total 1
Add
Match Type Full Prefix (OUI)
* MAC
Example: 00:11:22
Please enter a MAC address.
Remark
RX1501
Cancel
OK

Choose **Only the whitelisted STAs** are allowed to access Wi-Fi, then you can click Add to add the whitelist WLAN clients.

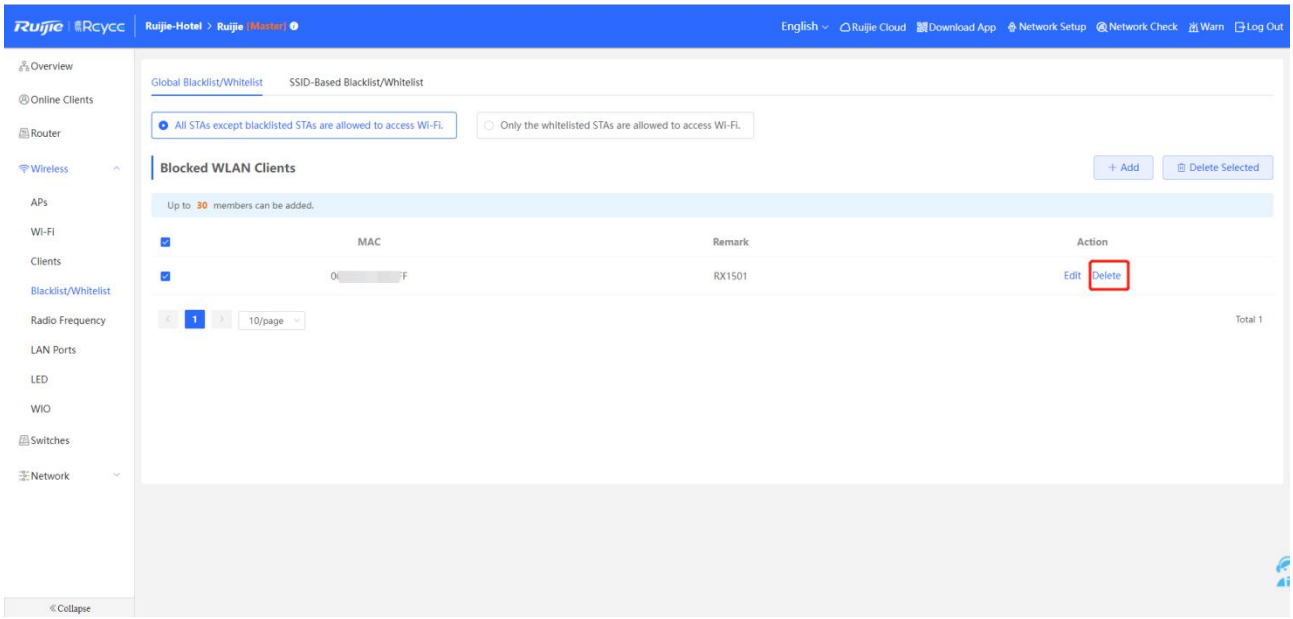


> **Note**
>
> Up to 30 members can be added.

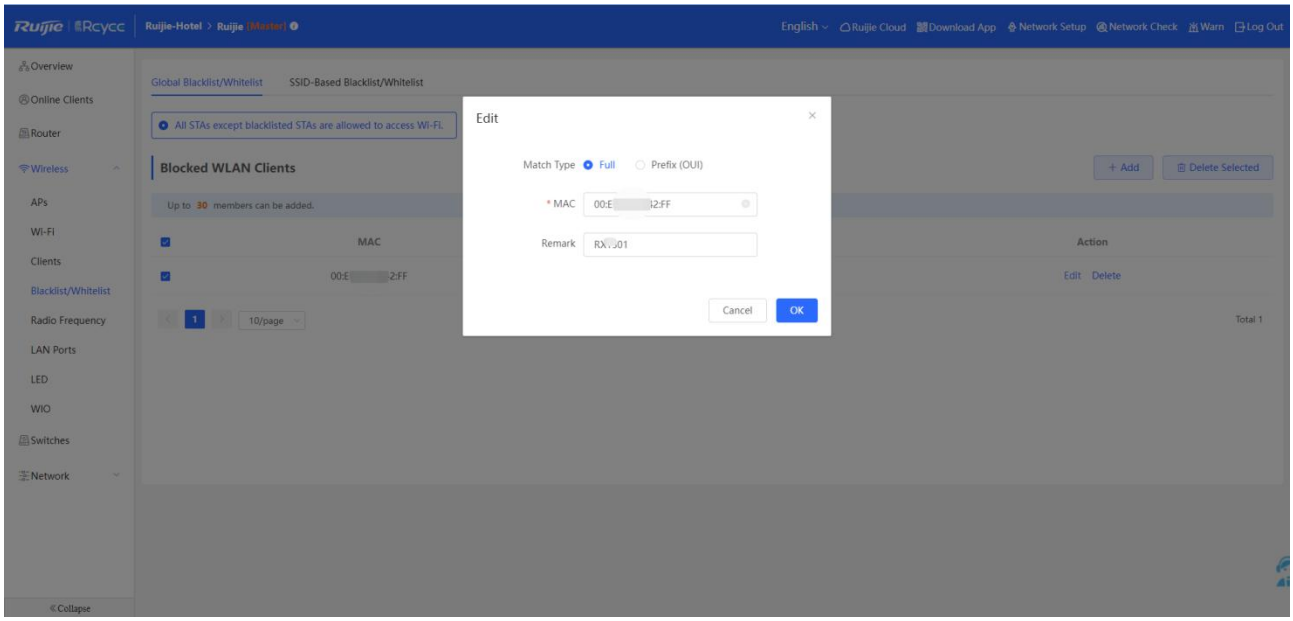
If you want to remove the client, you can select the clients then click Delete Selected



Or click **delete** it here

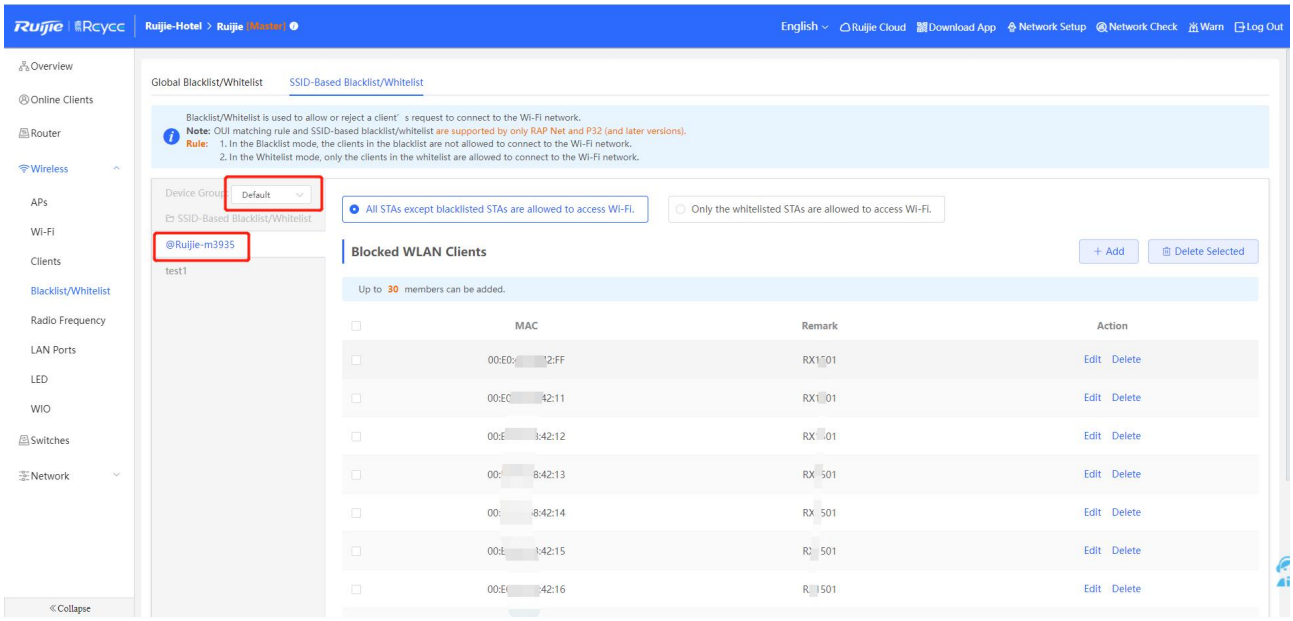


Click **Edit** can modify the client information



2. SSID-Based Blacklist/Whitelist

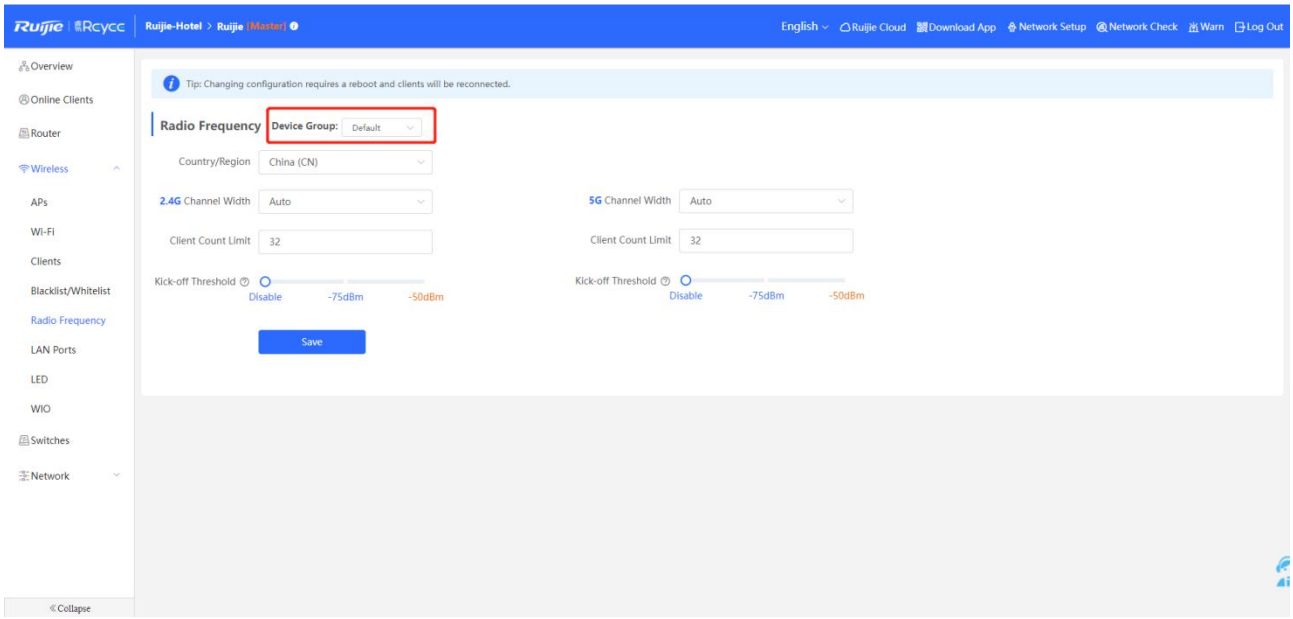
Choose **Device Group** and **SSID** and then base on **Blacklist/Whitelist to add WLAN clients.**



> **Note**
>
> Up to 30 members based on SSID can be added.
>
> OUI matching rule and SSID-based Blacklist/Whitelist are supported by only RAP Net and P32 (and later versions).

4.1.2.5 Wireless->Radio Frequency

Radio Frequency page can modify the **Country Code, 2.4G Channel Width, 5G Channel Width, Client Count Limit, Kick-off Threshold** based on the device group.



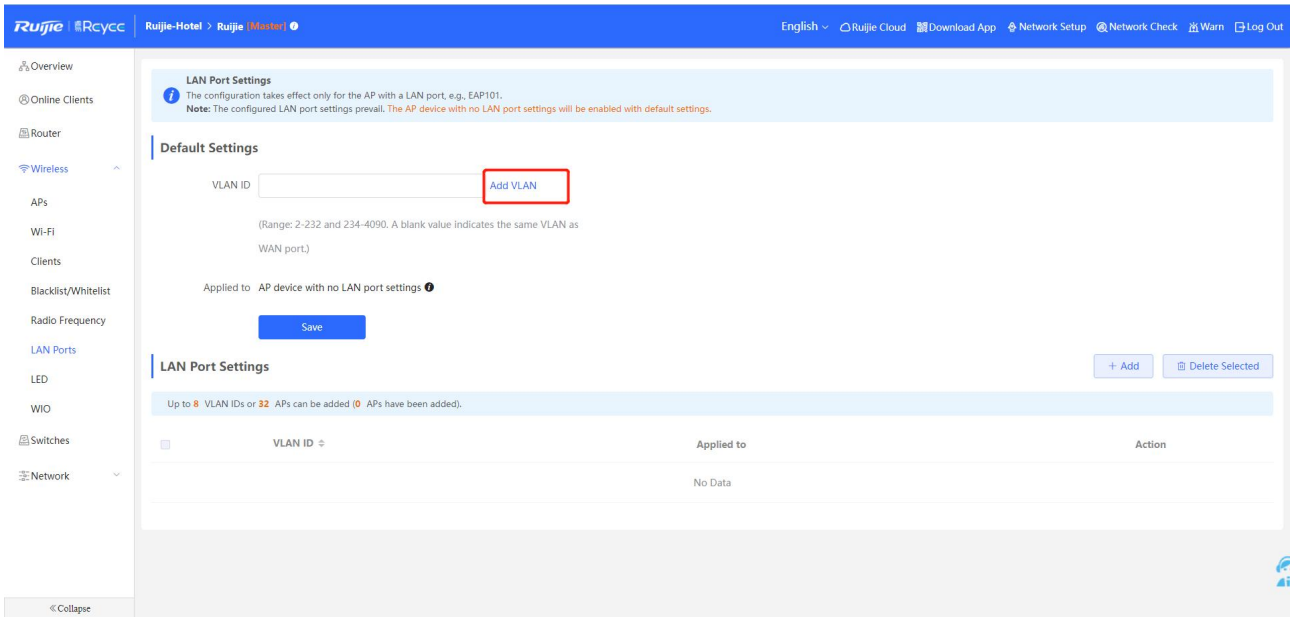
Kick-off Threshold: When the client's RSSI is lower than the threshold, it will be kicked off.

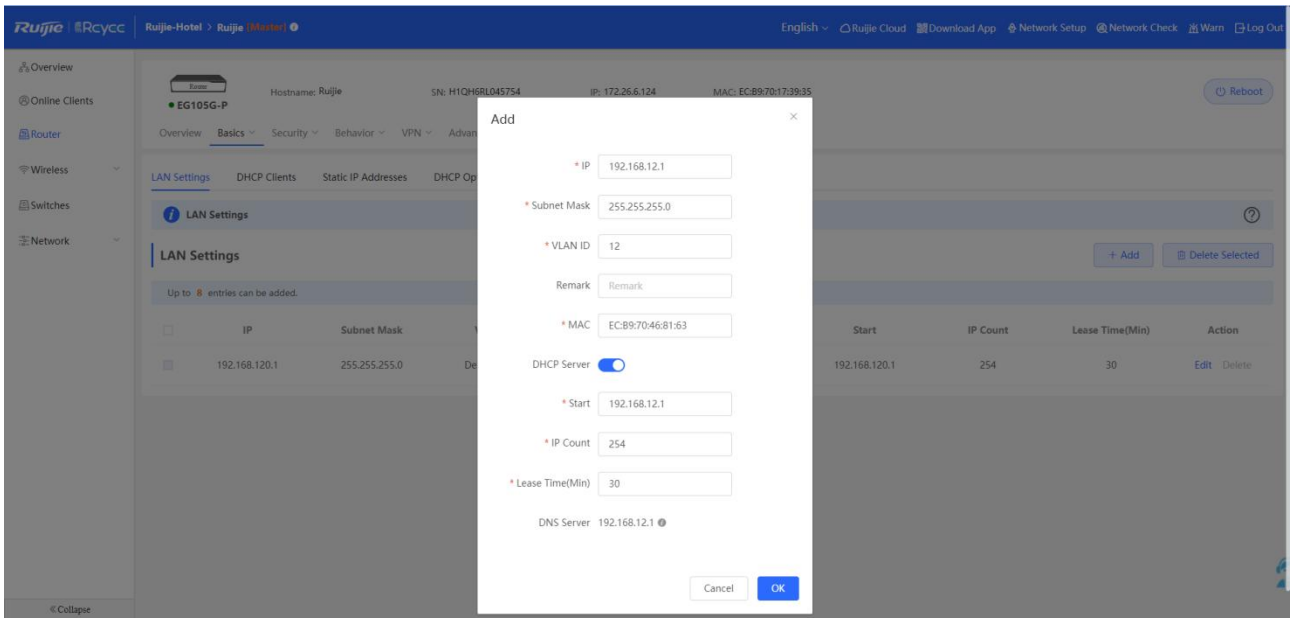
4.1.2.6 Wireless->LAN Ports

You can configure the Default LAN Port Settings or configure LAN Port Settings base on APs.

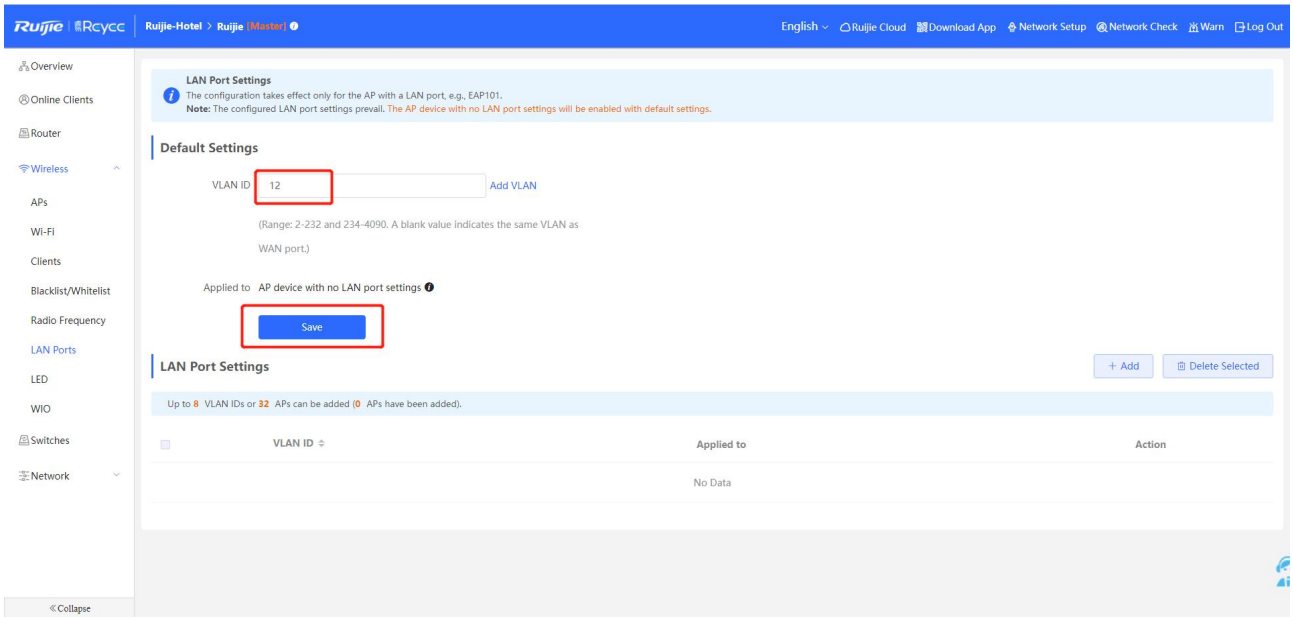
1. Default Settings

Click **Add VLAN** to add the needed VLAN on Gateway first, if you have set the needed VLAN, this step can be ignored.



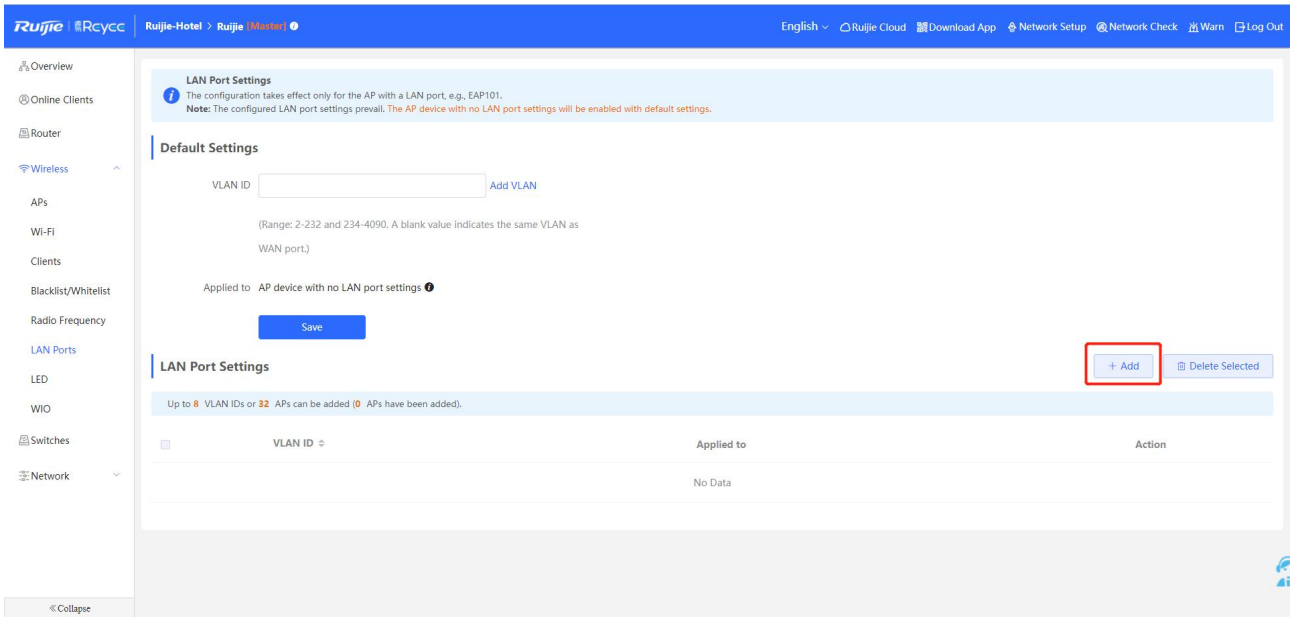


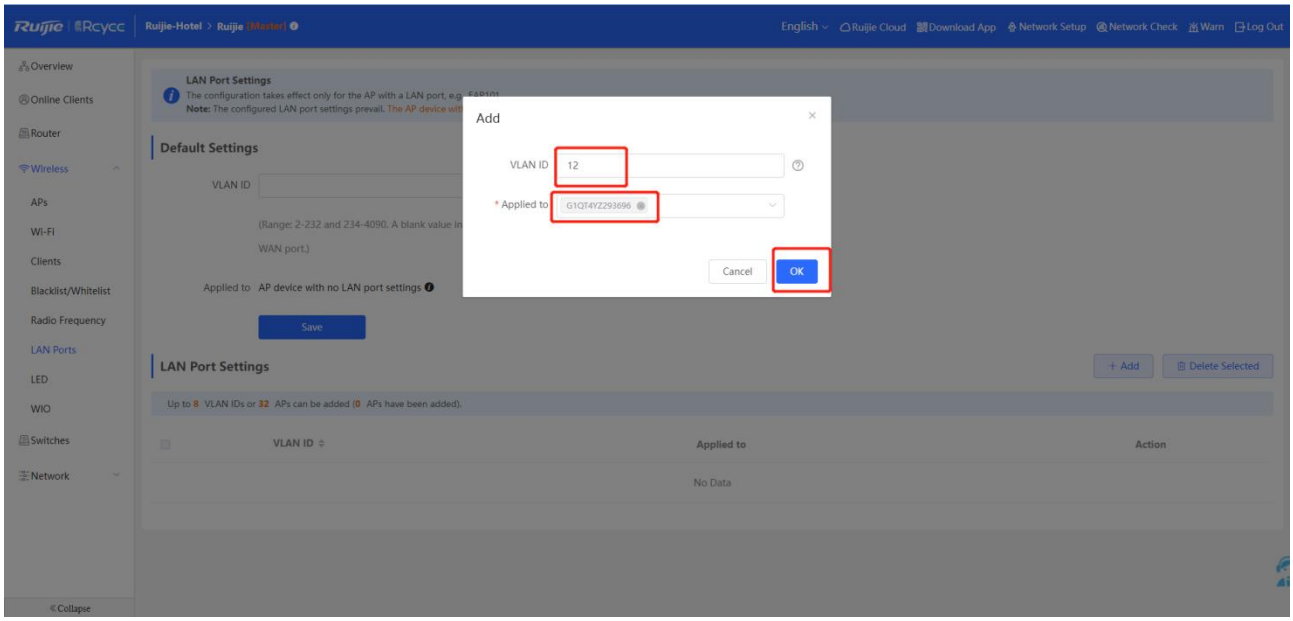
Then fill the needed VLAN, it will apply to AP devices without LAN port settings



2. LAN Port Settings

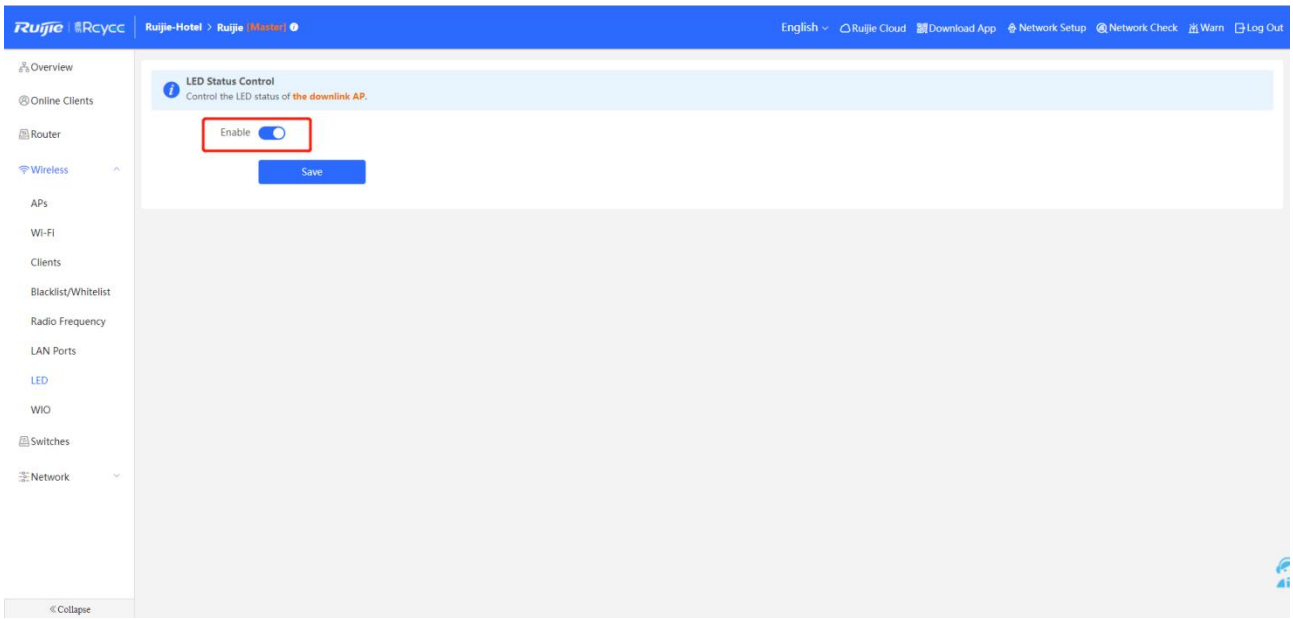
Click **Add** to set the VLAN of AP LAN port





4.1.2.7 Wireless->LED

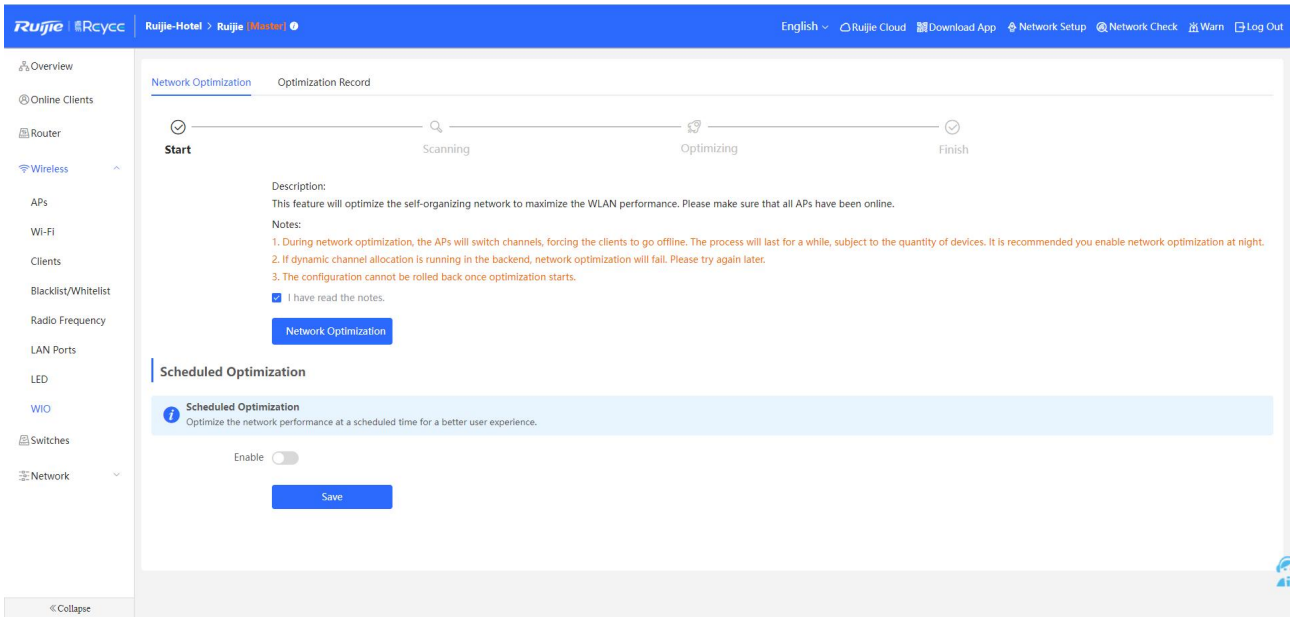
Control the LED status of the downlink AP.



4.1.2.8 Wireless->WIO

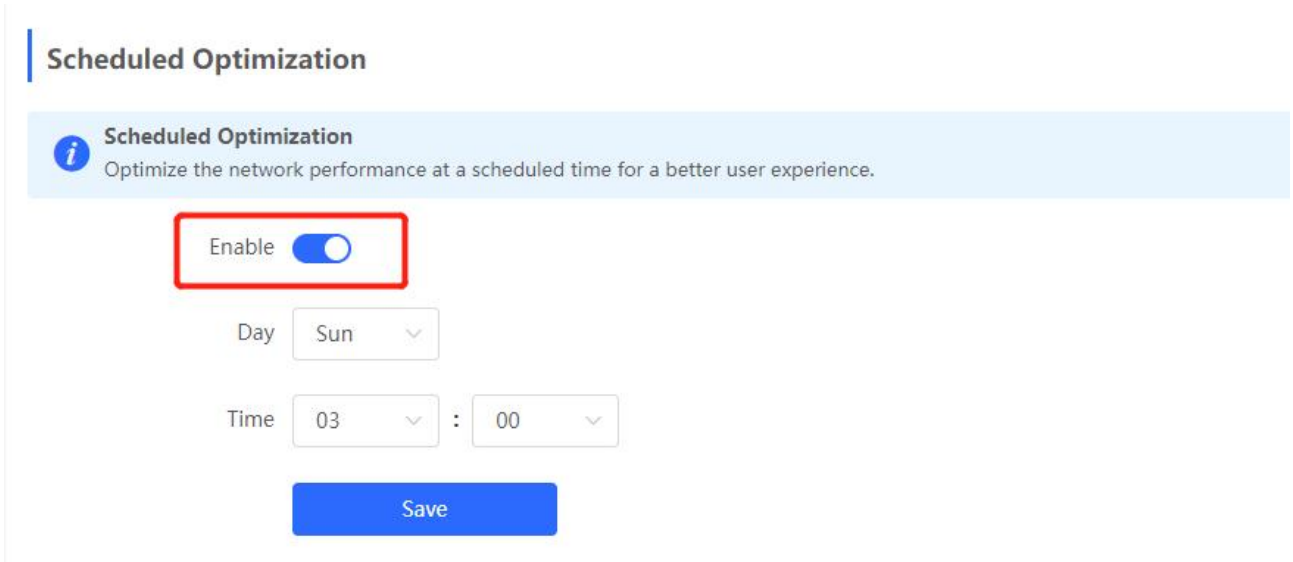
This feature will optimize the self-organizing network to maximize the WLAN performance. Please make sure that all APs have been online.

Choose **I have read the notes**, then you can start Network Optimization.



> **Note**
>
> 1) During network optimization, the APs will switch channels, forcing the clients to go offline. The process will last for a while which depends on the quantity of devices. It is recommended to enable your network optimization at night.
>
> 2) If the dynamic channel allocation is running in the backend, network optimization will fail. Please try it again later.
>
> 3) The configuration cannot be rolled back once the optimization starts.

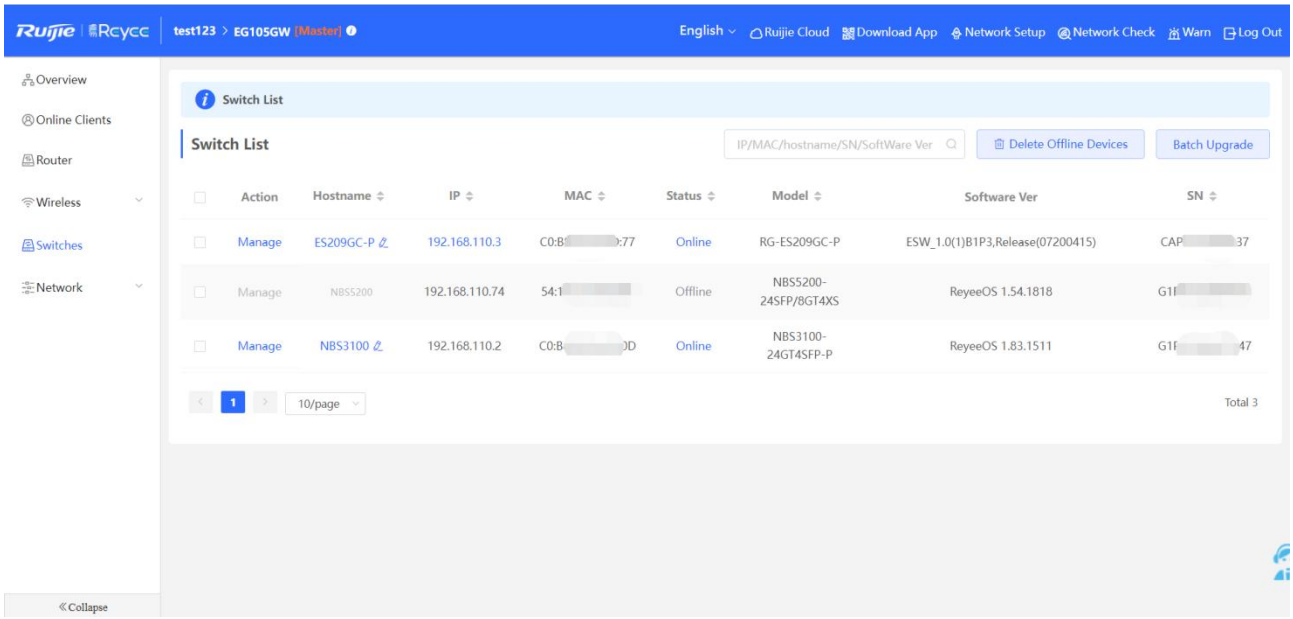
Scheduled Optimization: Optimize the network performance at a scheduled time for a better user experience.



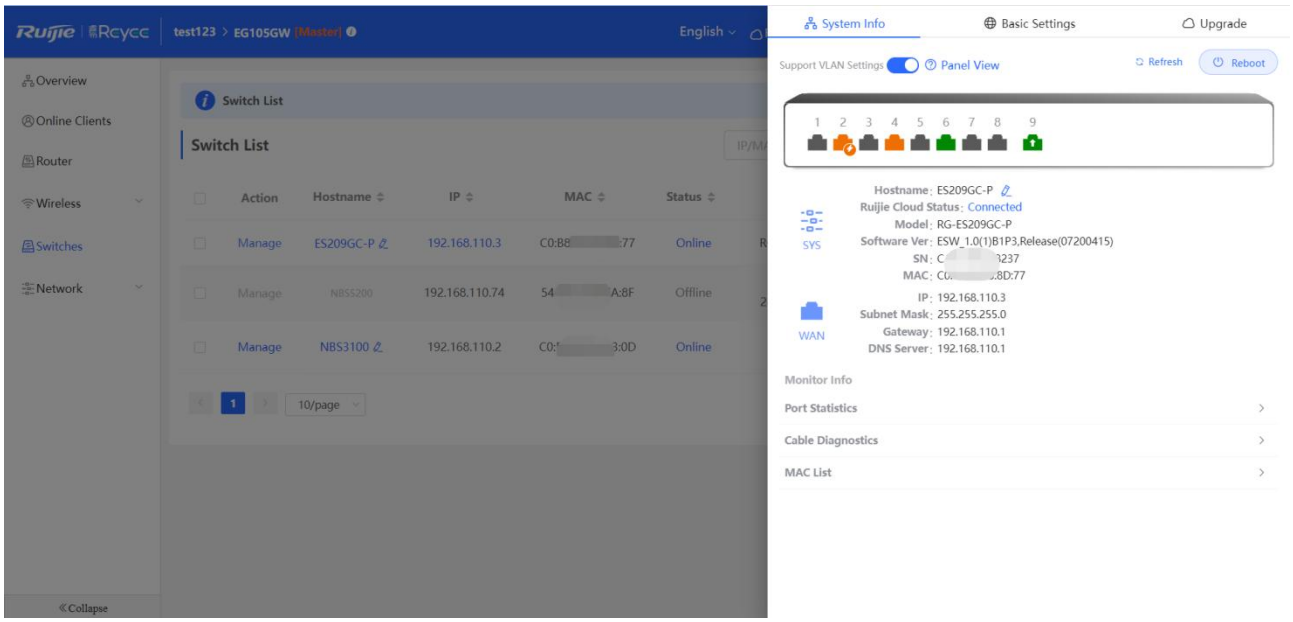
4.1.3 Switches Setting

Switch List displays all switches which are managed by Router. The information including Switch's Hostname, IP, MAC, Status, Model, Software Version, SN can be in this page. AP categories could be seen by clicking

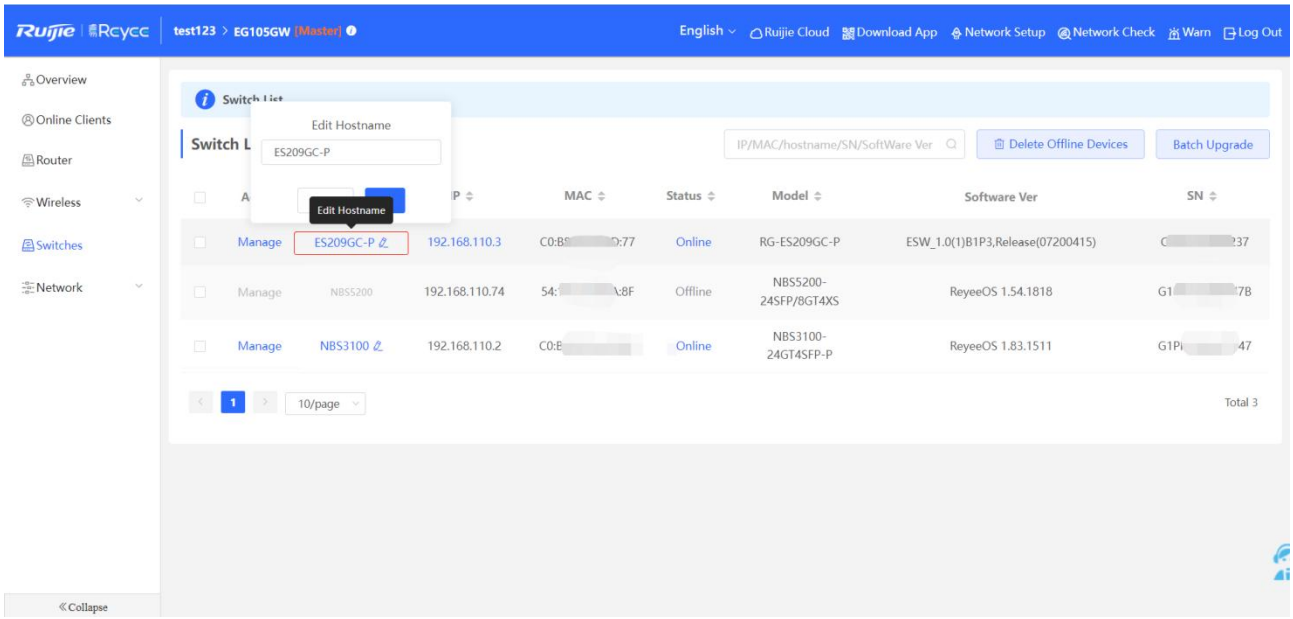
.



Manage: Go to the Switch detail setting page



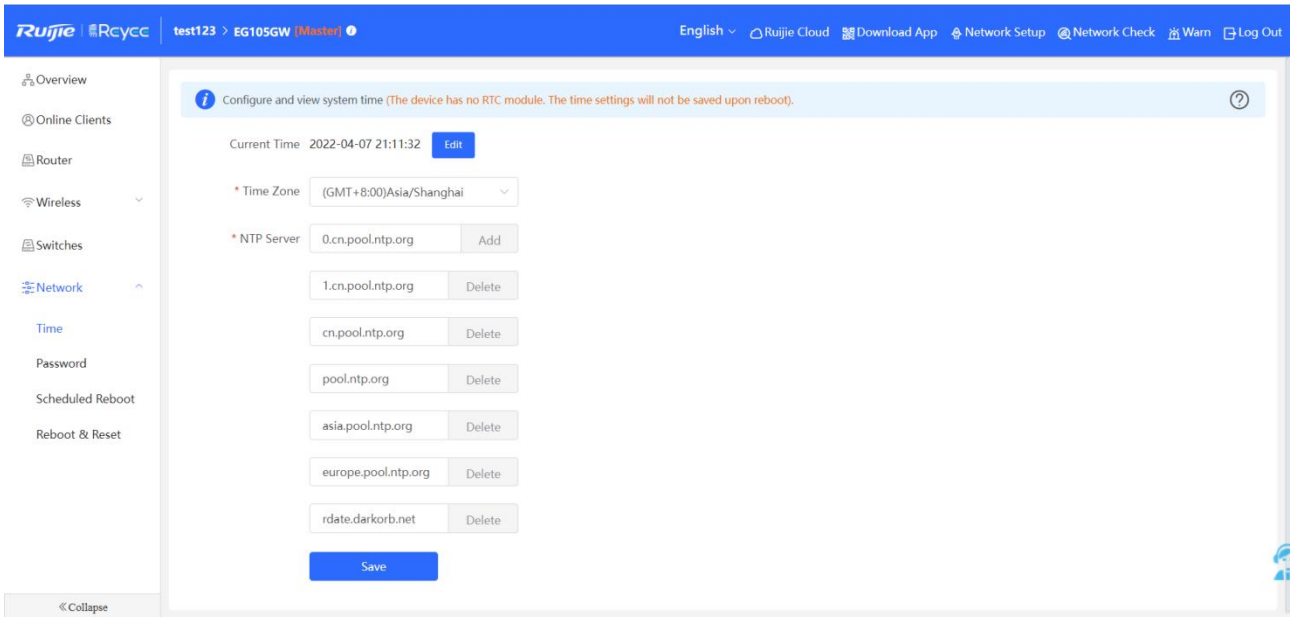
Edit Hostname: Modify the hostname of switch



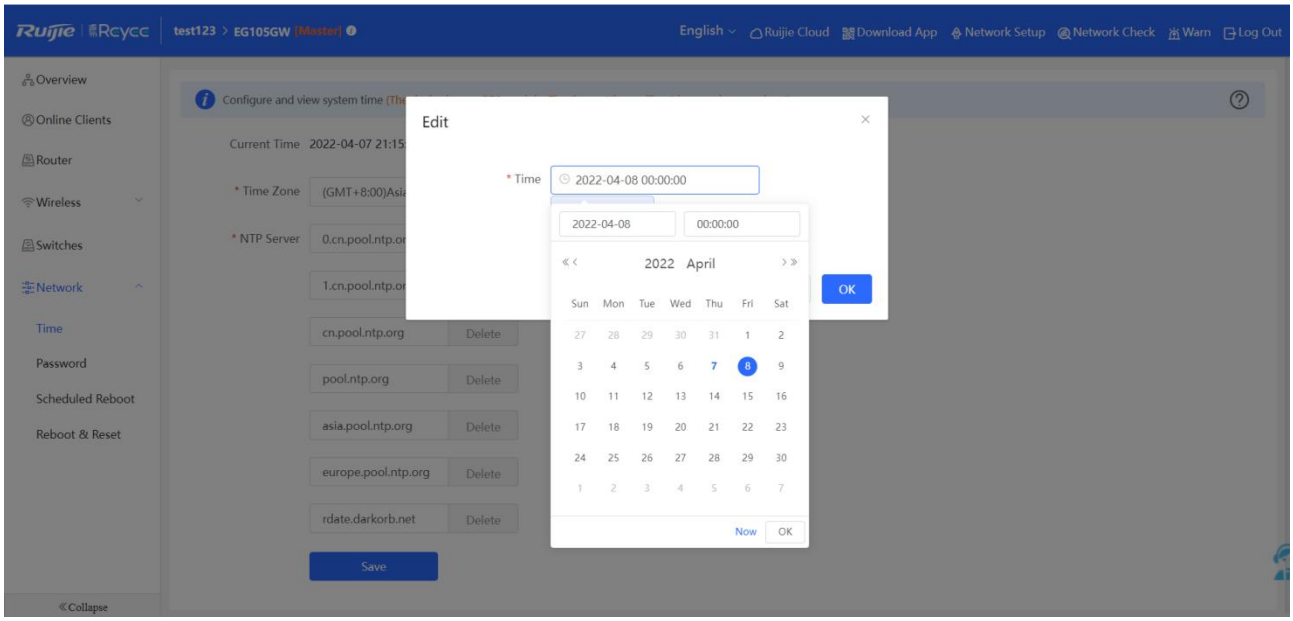
4.1.4 System Setting

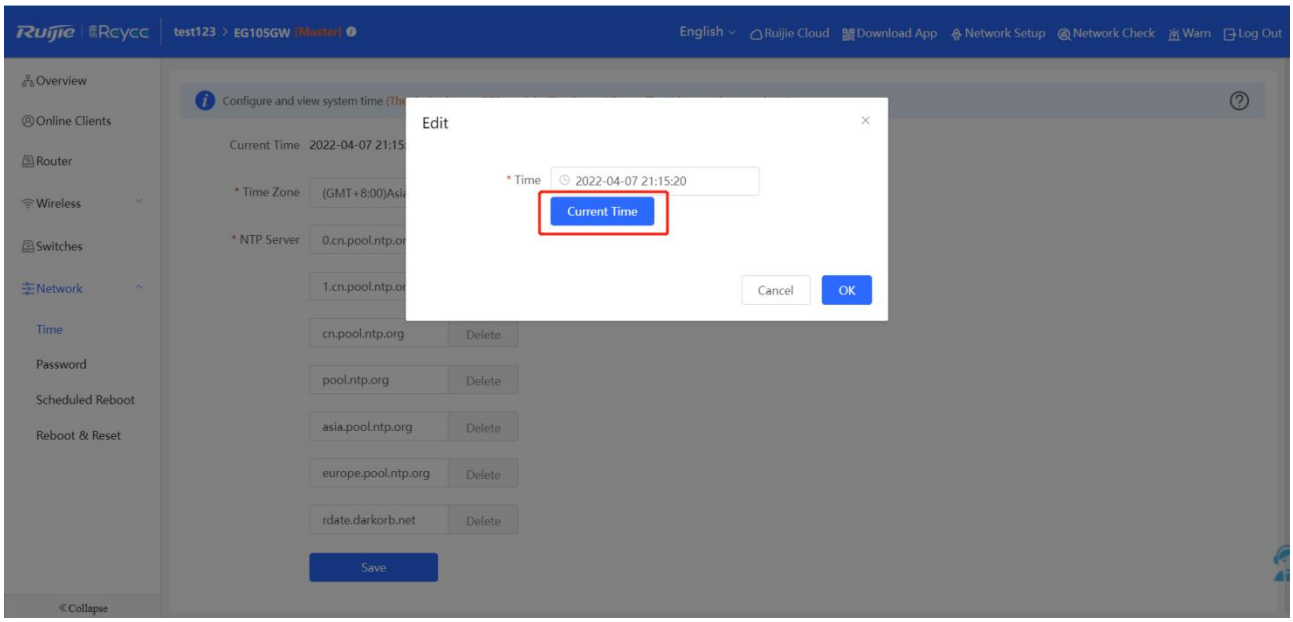
4.1.4.1 Time

This page displays **Current Time, Time Zone and NTP Server**. It will synchronize the correct time automatically,

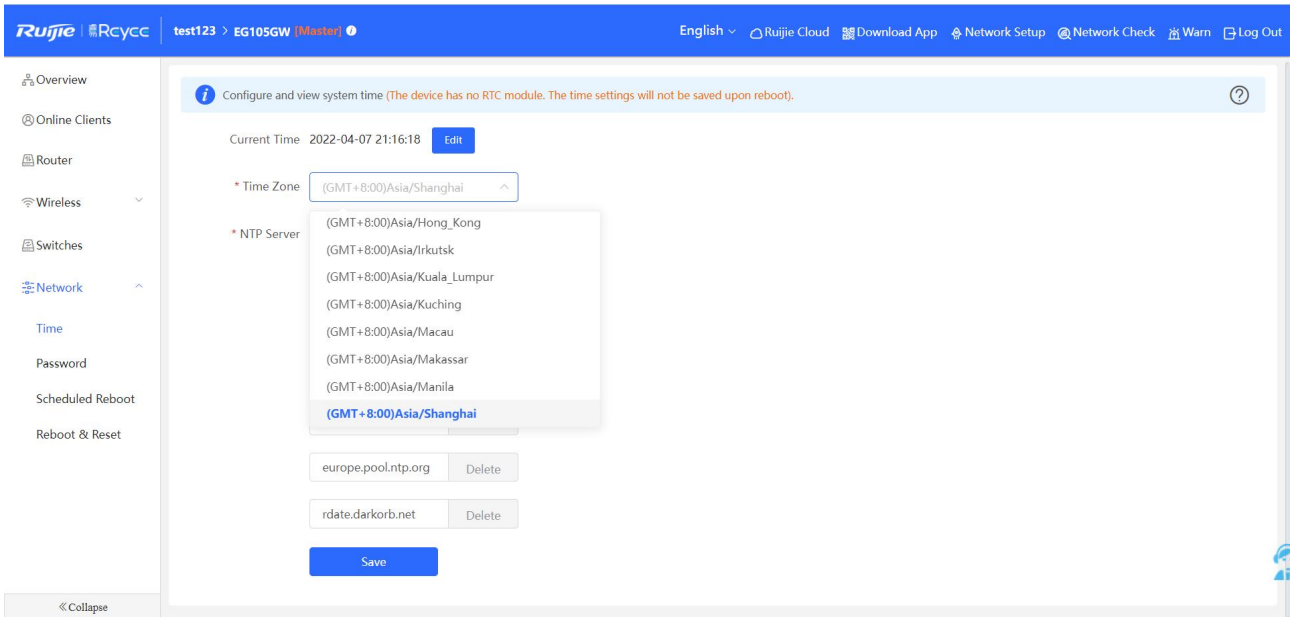


1. Manually edit the current time or click **current time** to let it synchronize current time automatically.

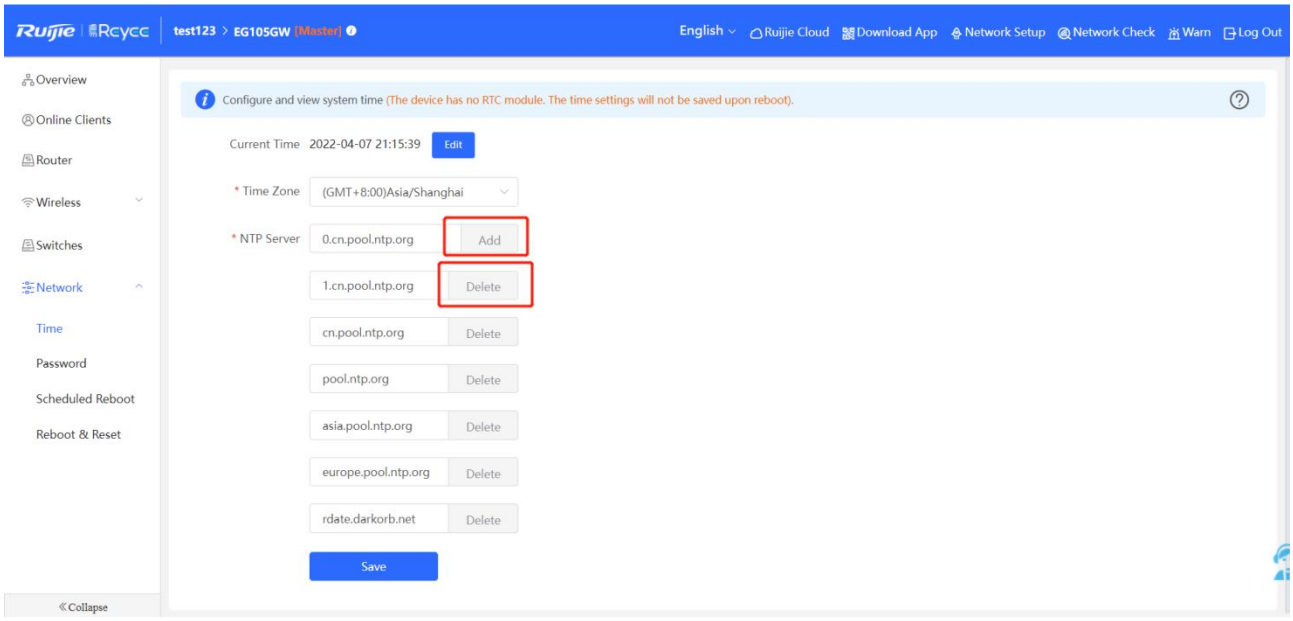




2. Manually choose the Time Zone

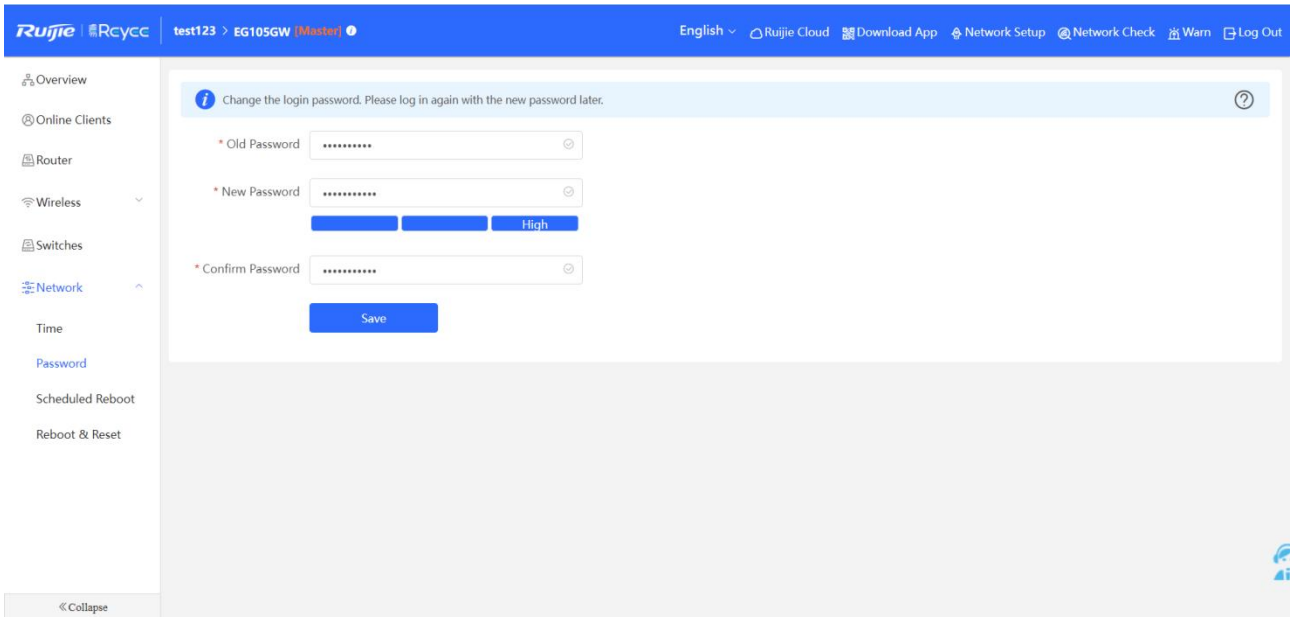


3. Add or delete the NTP server.



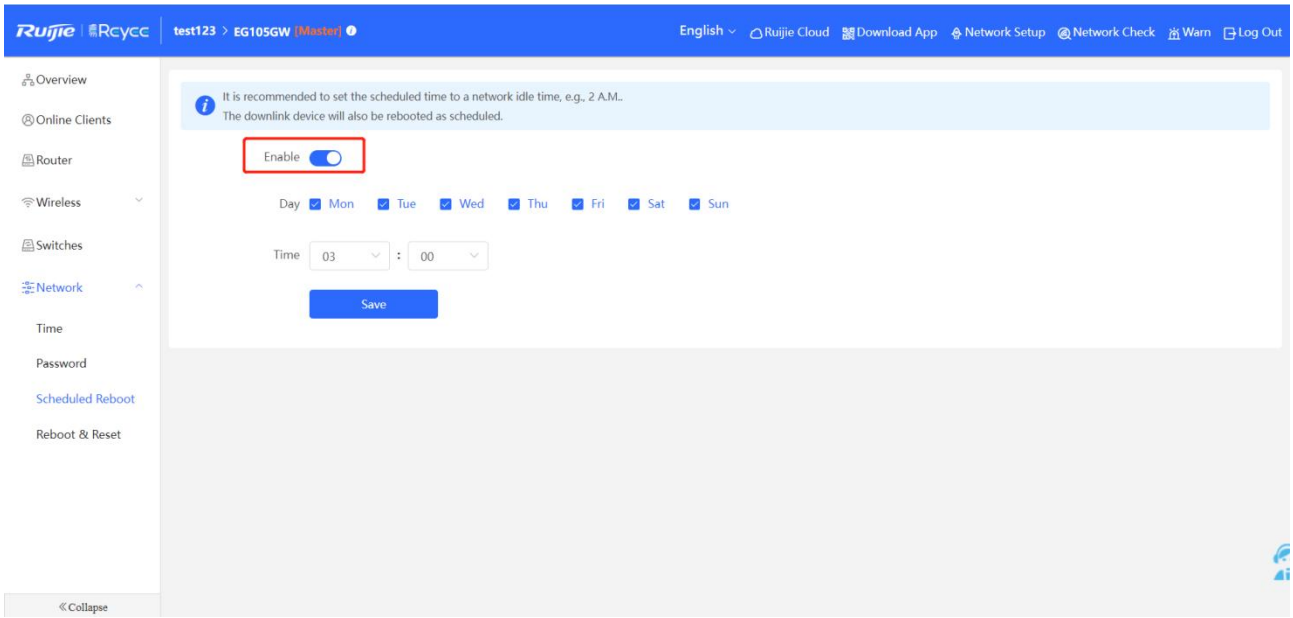
4.1.4.2 Password

Modify the password by enter your old password and new password.

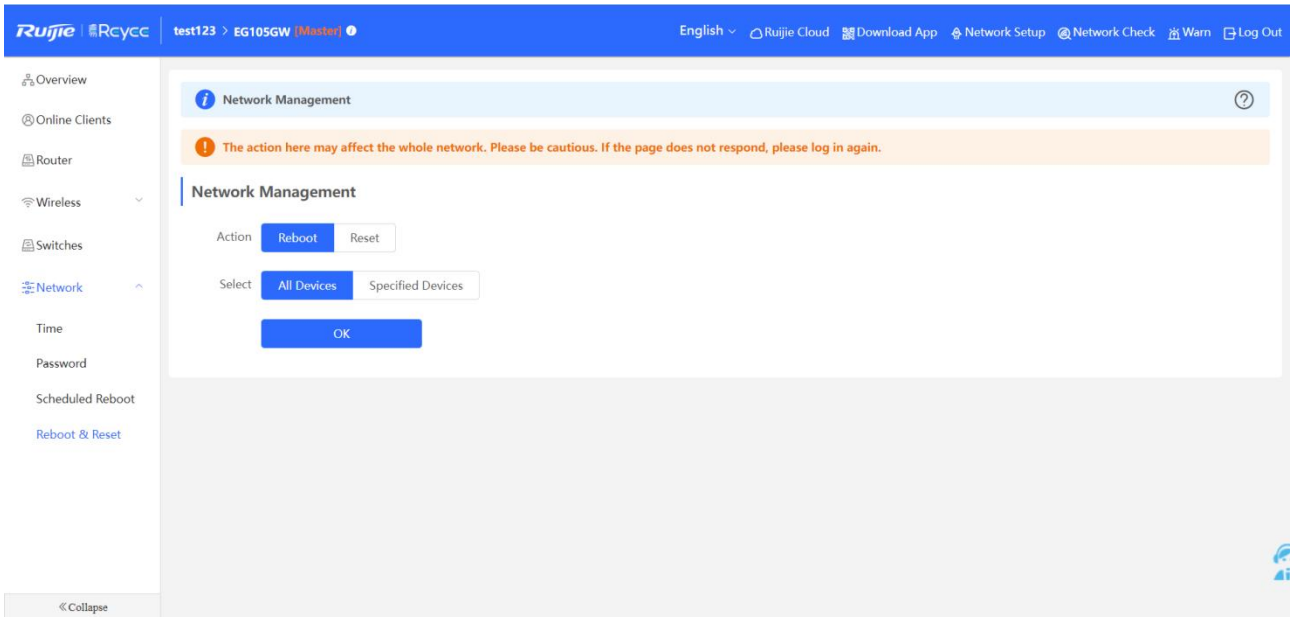


4.1.4.3 Reboot

1. Schedule Reboot for All Devices on the same SON network.

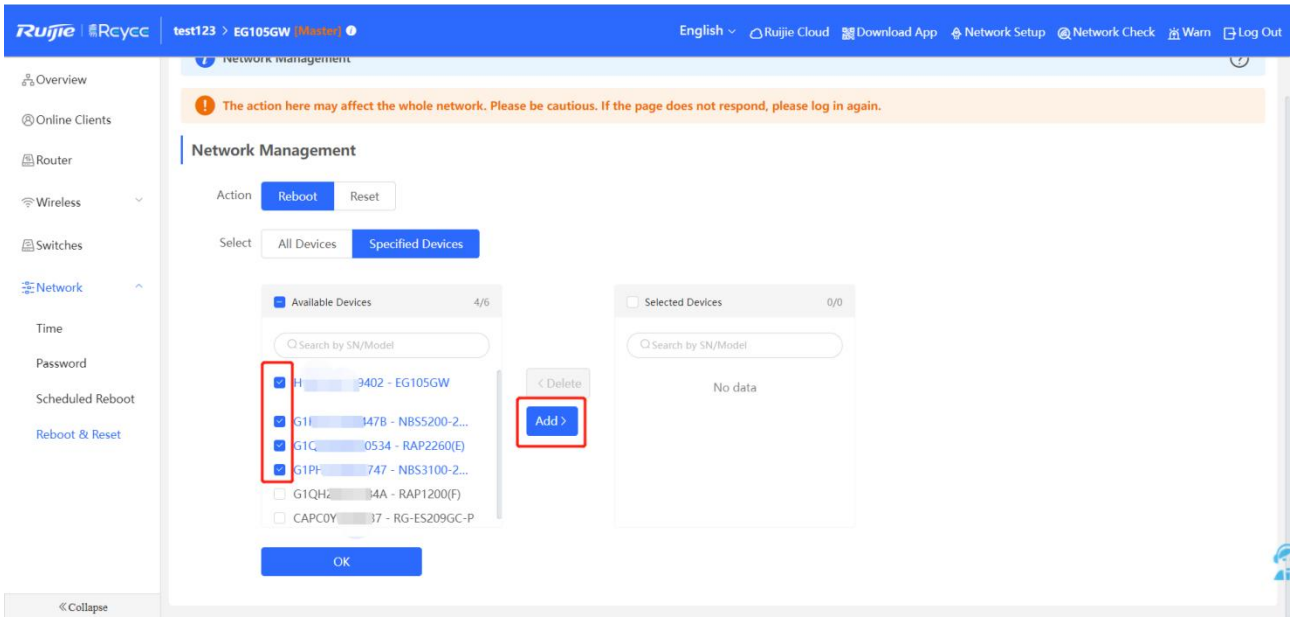


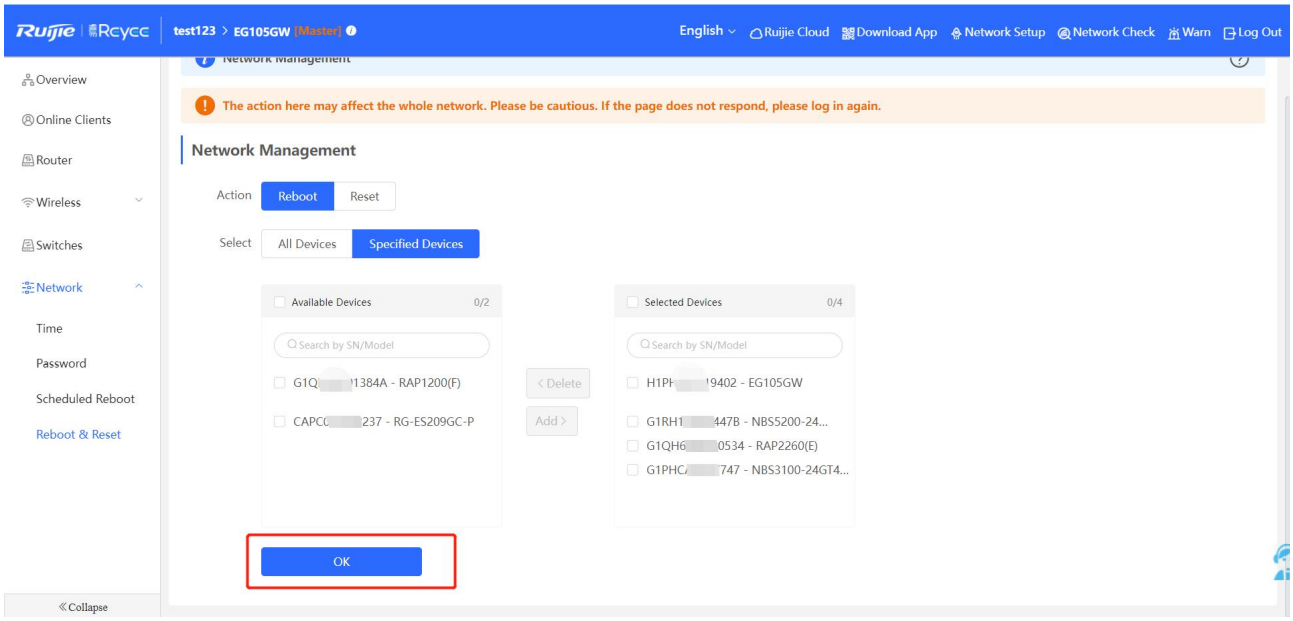
2. Reboot for All Devices or Specified Devices on the same SON network immediately.



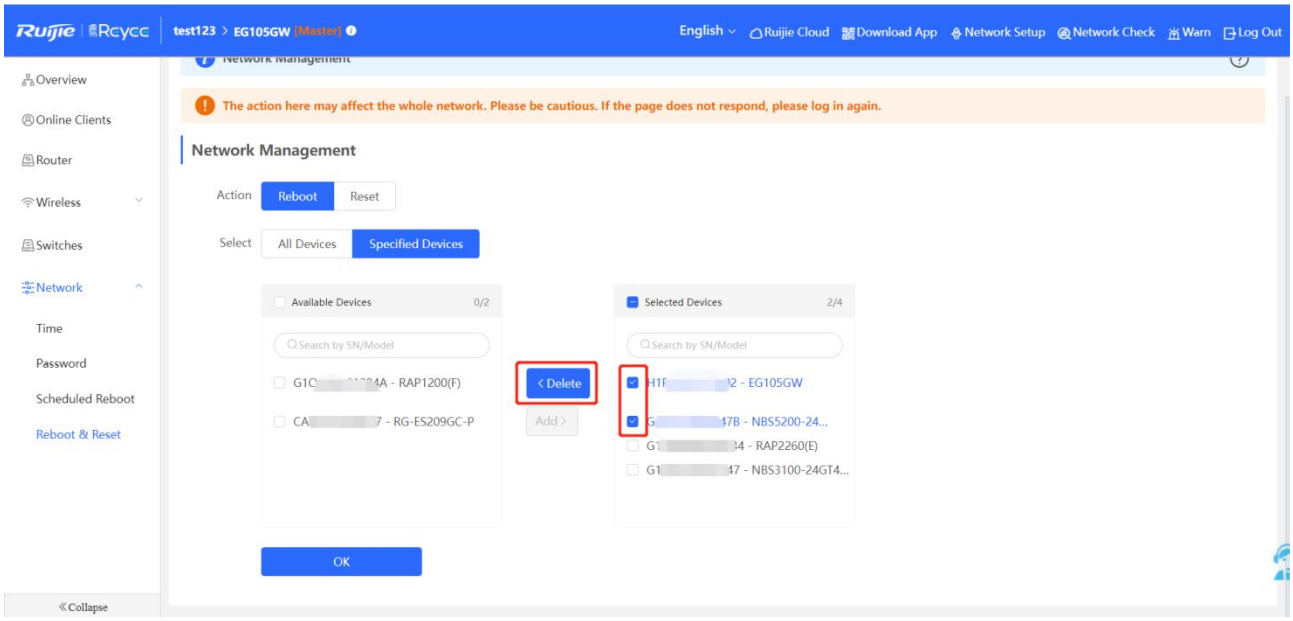
3. Reboot for **Specified Devices** on the same SON network immediately.

Choose the devices which need to be reboot, then click **Add** and **OK**, then the devices will reboot.



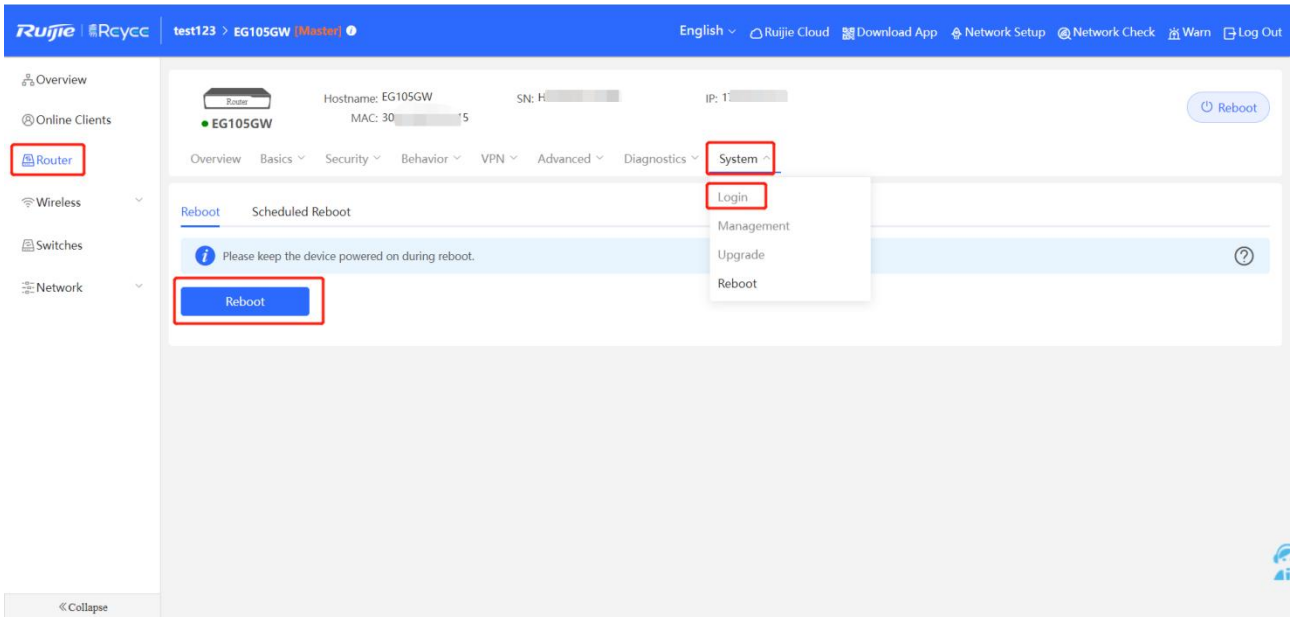


If you don’t want to reboot some selected devices, you can select then delete.



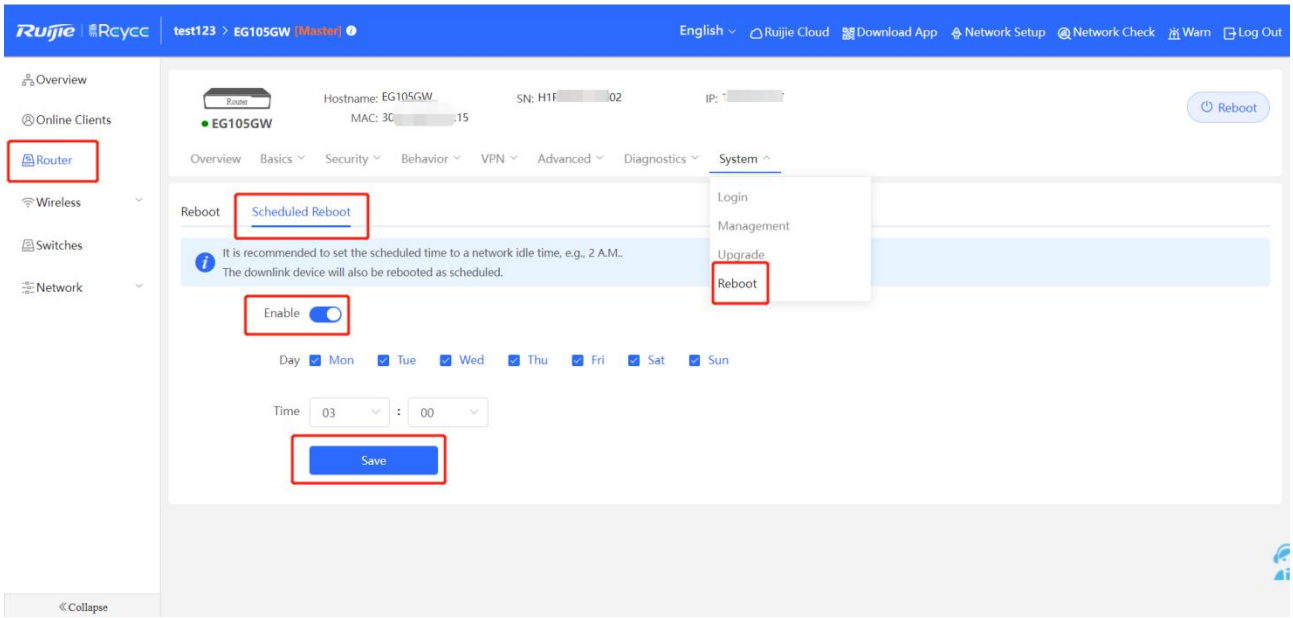
4. Reboot Router

Click **Router->System->Reboot**, then click Reboot to reboot Router itself.



5. Schedule Reboot Router

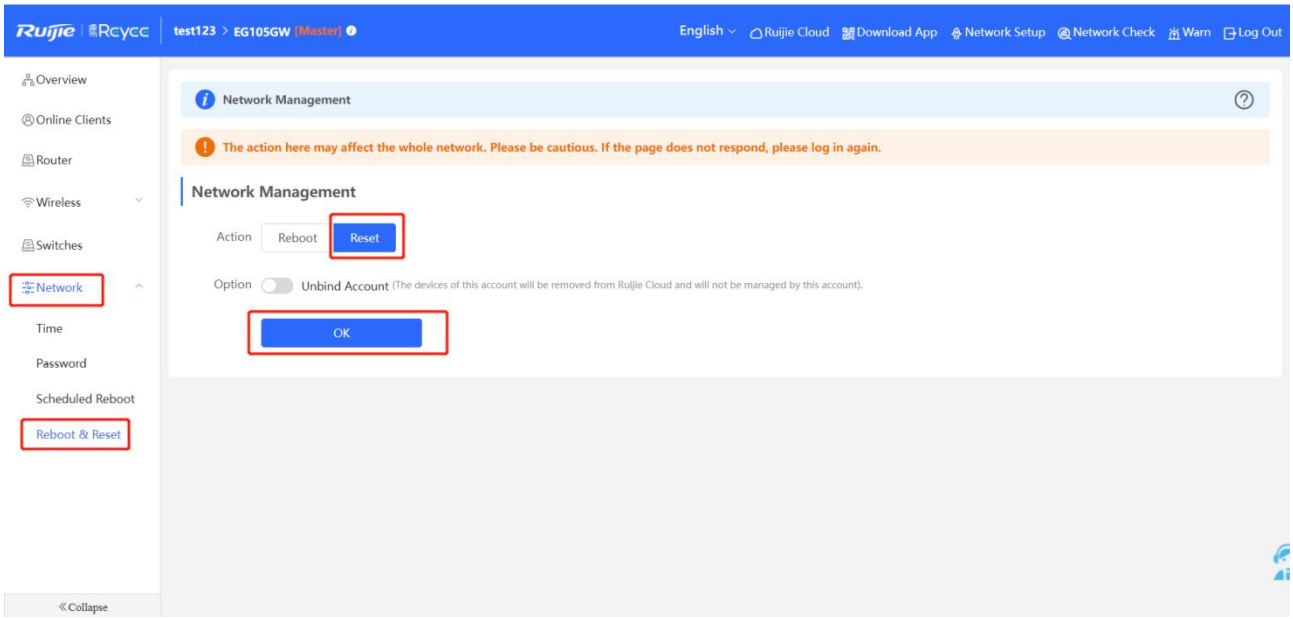
Click **Router->System->Reboot**, then choose Schedule Reboot and click **Enable** to set the reboot day and time. Finally **Save** the setting



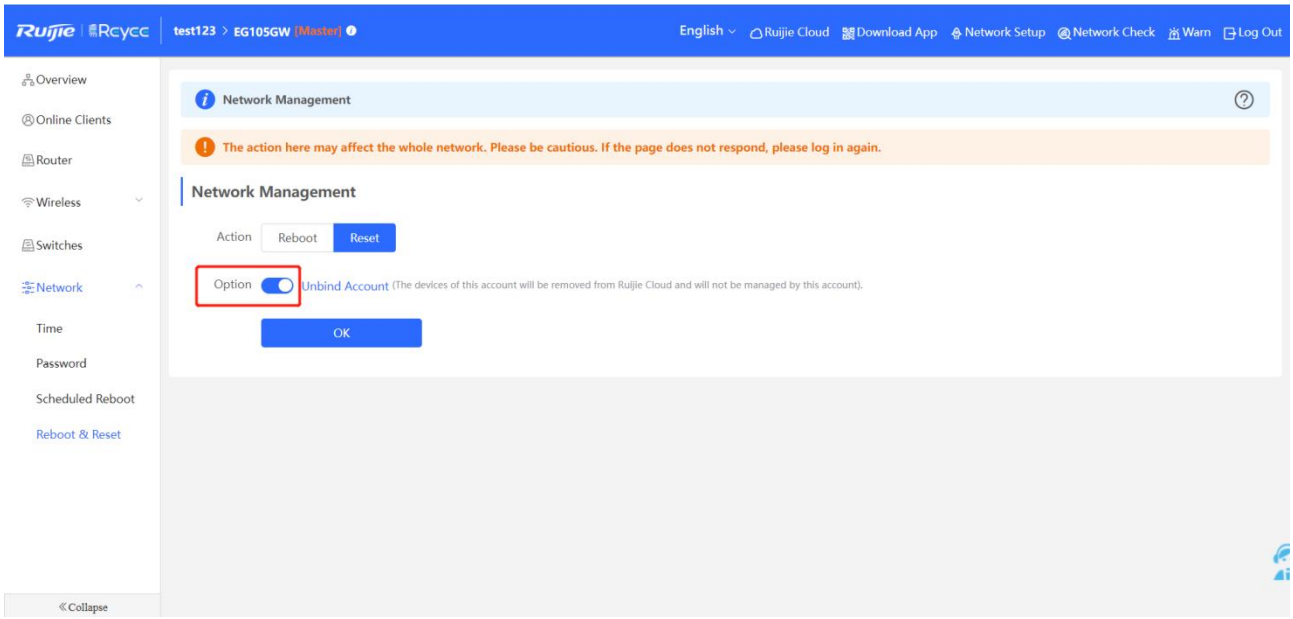
4.1.4.4 Reset

1. Reset all devices on the same SON network

Click **Network->Reboot&Reset->Reset,** then click **OK** to reset all devices.

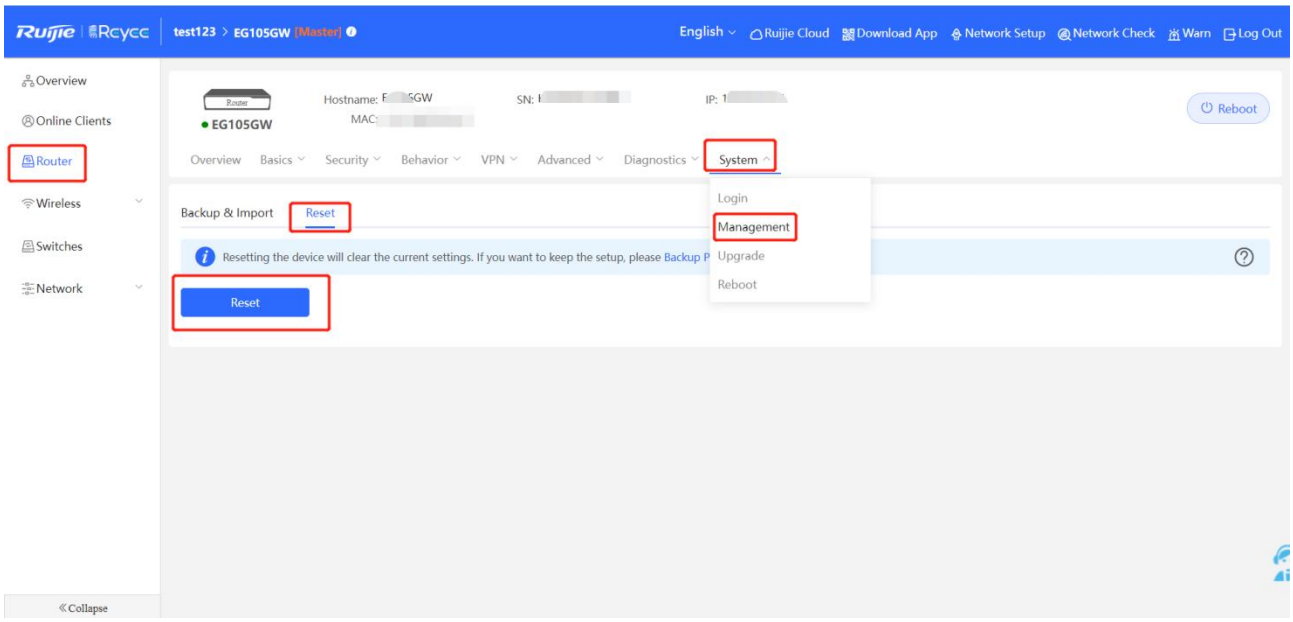


If you want to remove devices from Ruijie Cloud, can enable the option Unbind Account, then click OK.



2. Reset Router

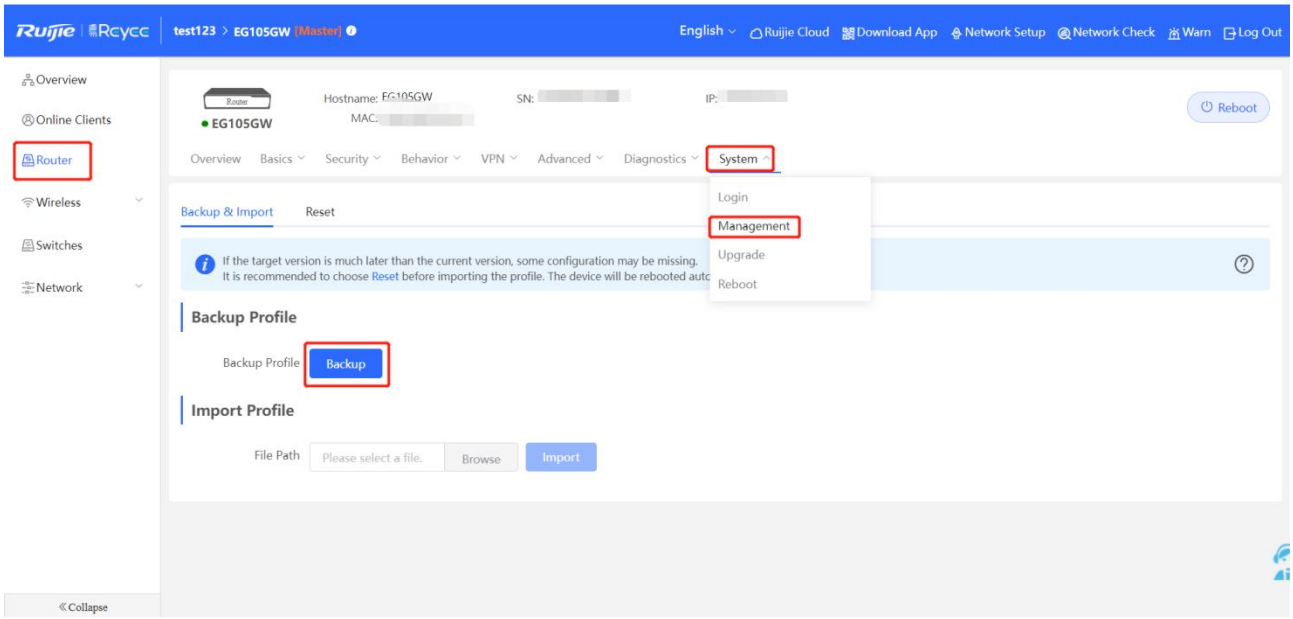
Click **Router->System->Management->Reset.**



> **Note**
>
> Resetting the device will clear the current settings. If you want to keep the setup, please Backup Profile first.

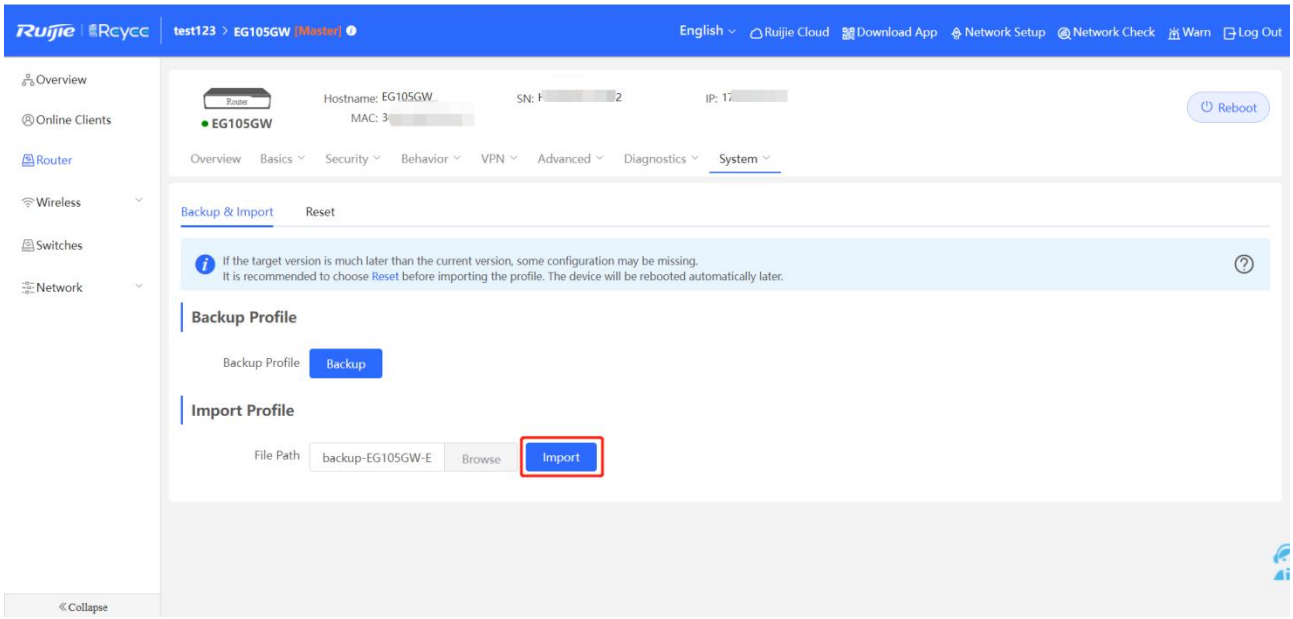
4.1.4.5 Backup &Import the configuration of Router

Click **Router->System->Management->Backup & Import->Backup** to backup configuration.



Click **Router->System->Management->Backup & Import->Browse** to choose the configuration, then click Import to import it.

4.1.4.6 Upgrade the firmware of Router

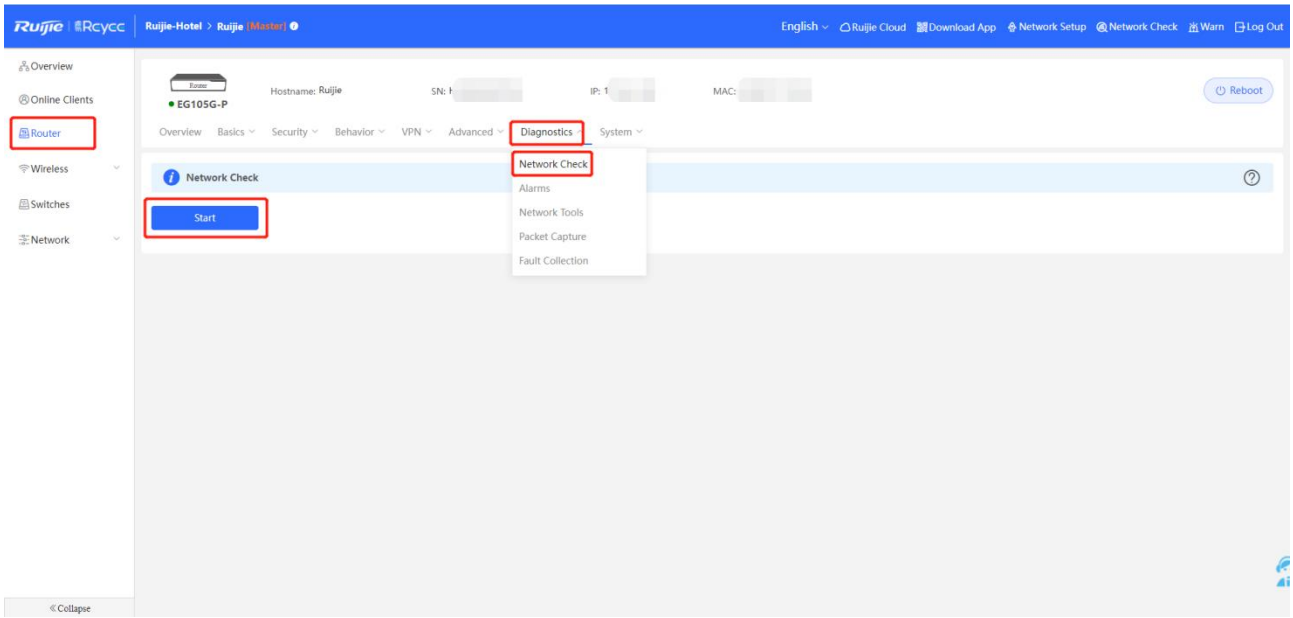


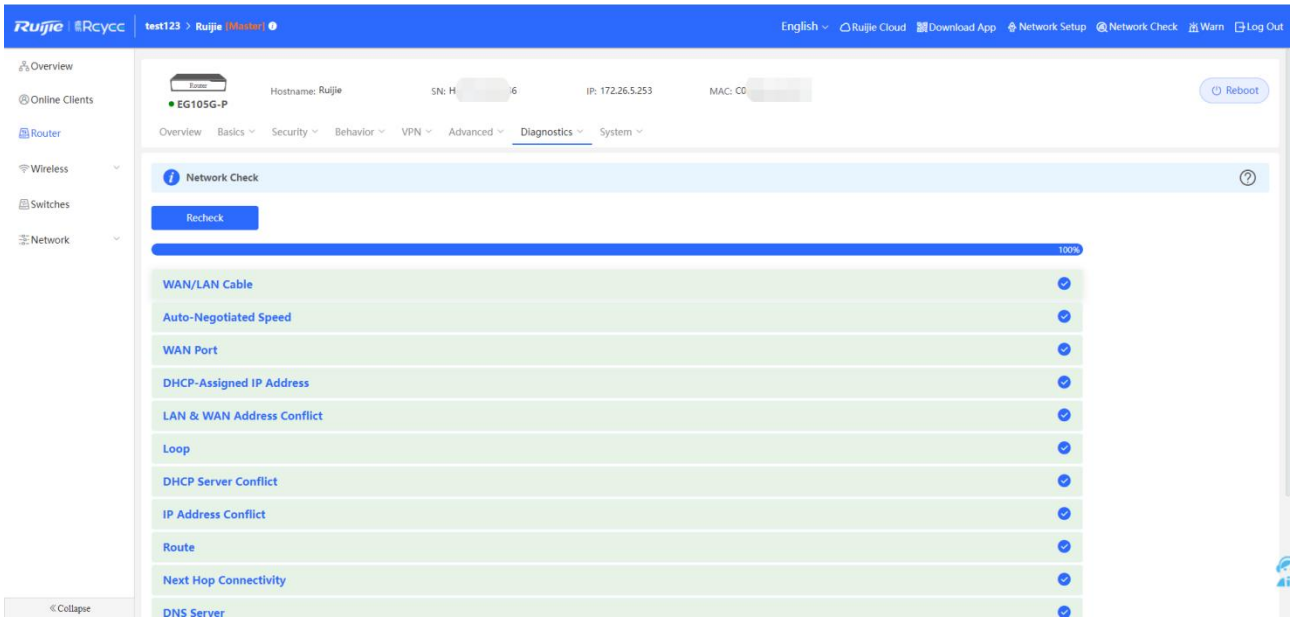
4.1.5 Diagnostics

4.1.5.1 Network Check

You can check your network and fix the problem on this page.

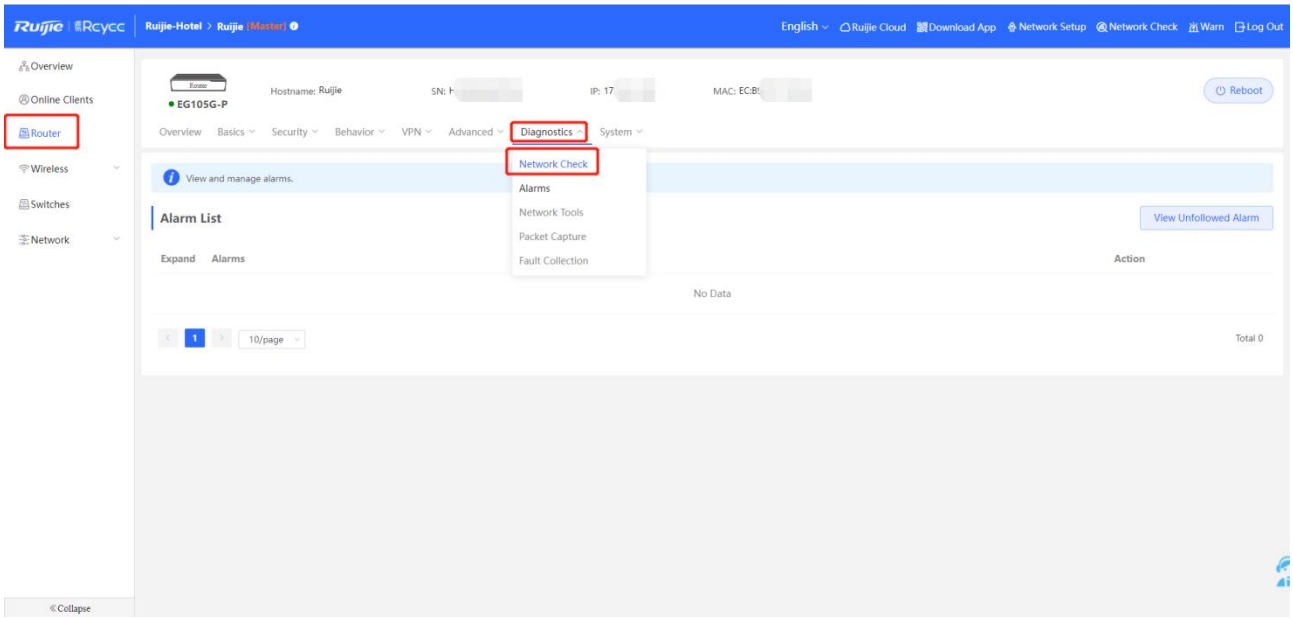
Click **Router->Diagnostics->Network Check->Start**





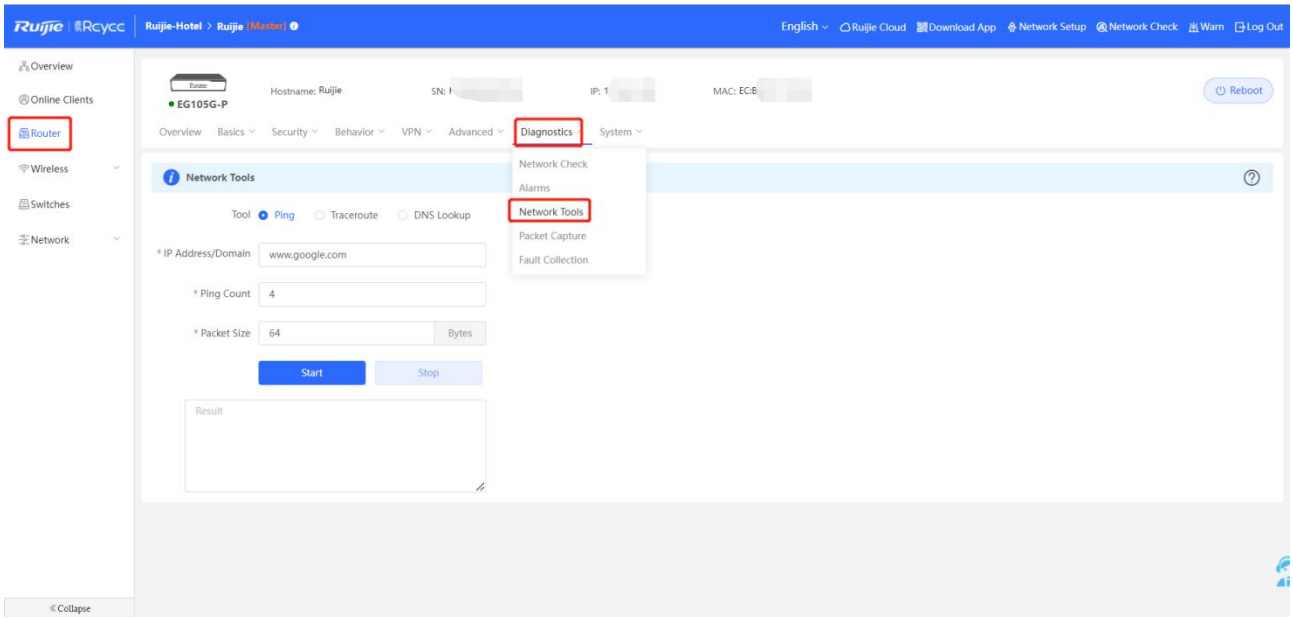
4.1.5.2 Alarms

Alarms page can view and manage alarms.



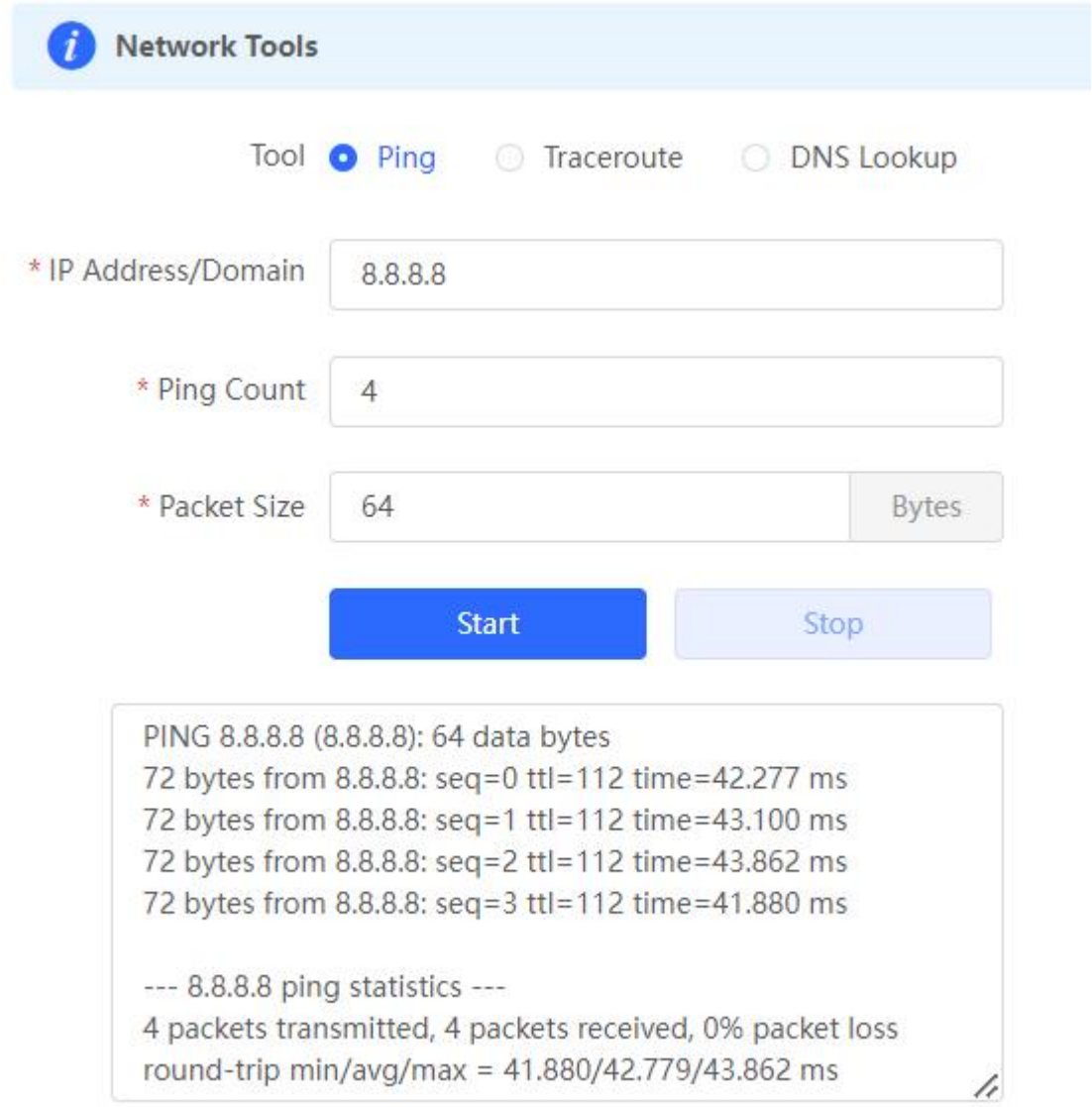
4.1.5.3 Network Tool

You can check the network status by some tools on this page, such as Ping, Traceroute, DNS Lookup Tools



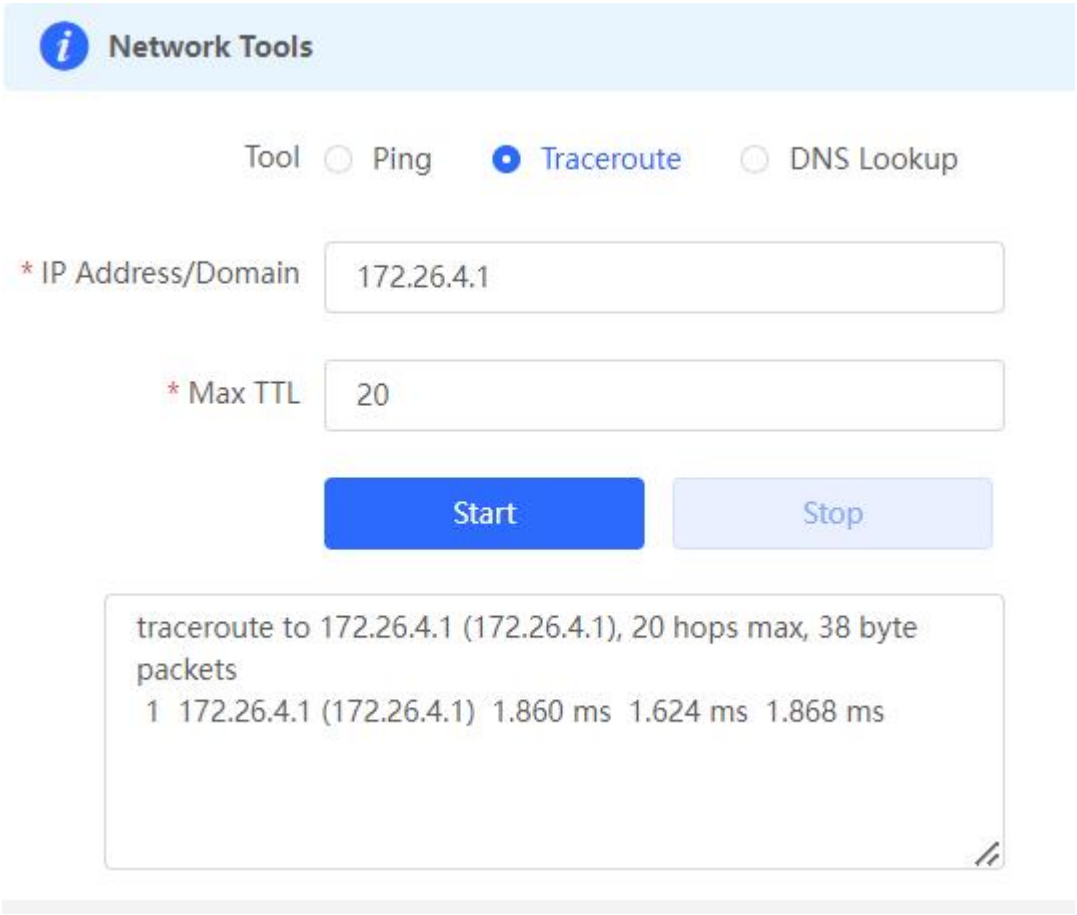
1. Ping Tool

Key in **IP Address/Domain, Ping Count, Packet Size** on this page, then Click Start will show the ping result on the following windows.



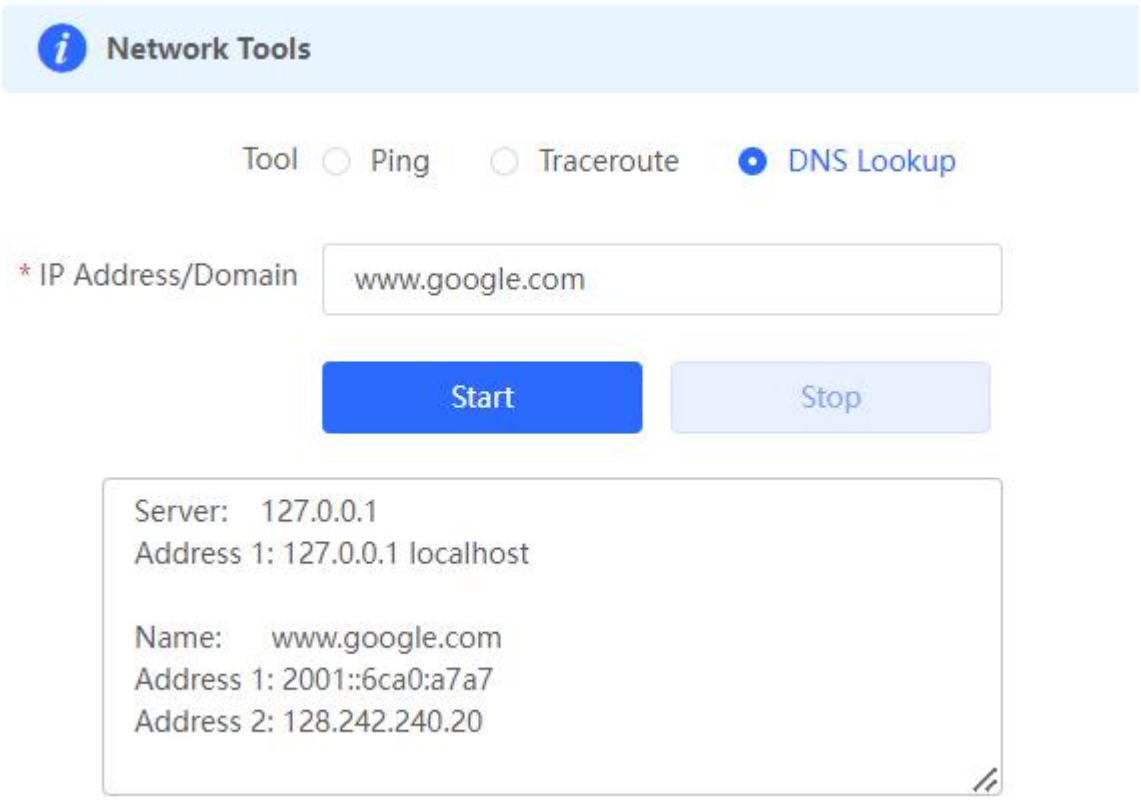
2. Traceroute Tool

Key in **IP Address/Domain, Max TTL** on this page, then Click **Start** will show the ping result on the following windows.



3. DNS Lookup Tool

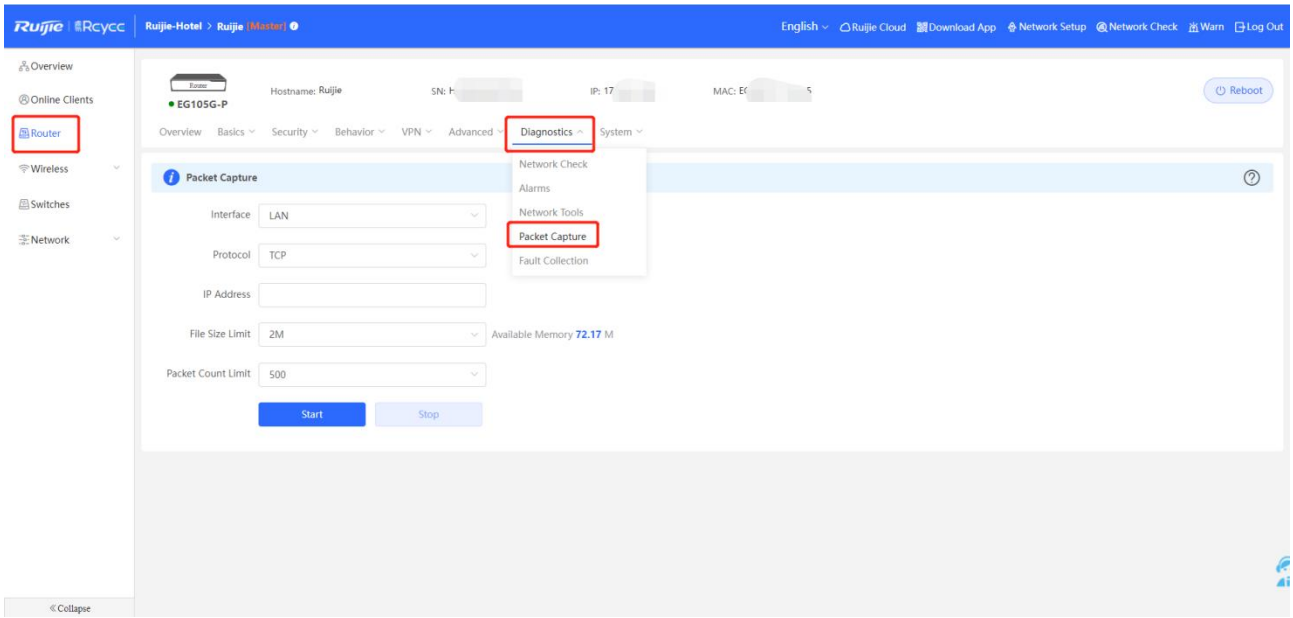
Resolve the domain to an IP address.



4. Packet Capture

You can capture packet to generate a diagnosis file on this page.

Click **Router->Diagnostics->Packet Capture**, fill the **Interface, Protocol, IP Address, File Size Limit, Packet Count Limit** then click **Start.**



Interface: Capture packets passing through this interface.

Protocol: Capture packets of this protocol.

IP Address: Capture packets of this IP address

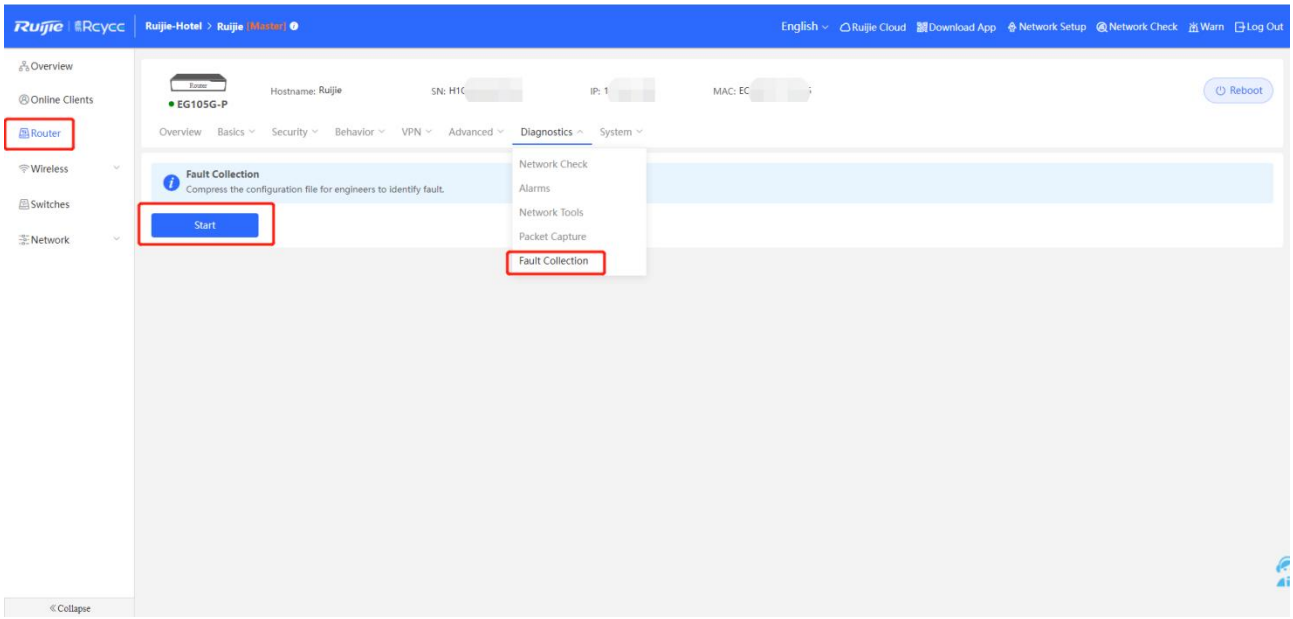
File Size Limit: Limit the size of packet file

Packet Count Limit: Limit the packet count. When the packet count reaches the limit, packet capture will stop and a download link will be generated.

5. Fault Collection

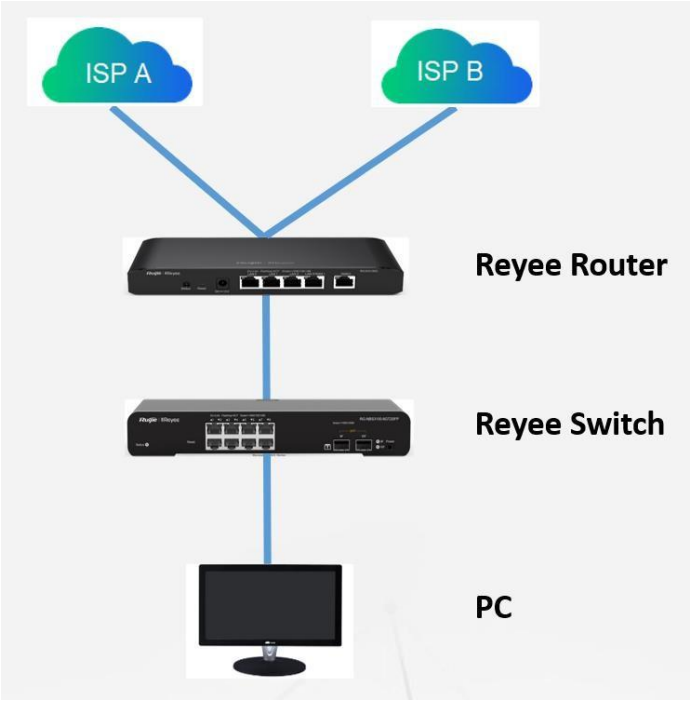
Compress the configuration file for engineers to identify fault.

Click **Router->Diagnostics->Fault Collection->Start**. Then will auto download a fault collection file for this.



4.1.6 WAN Load Balance

Application Scenario

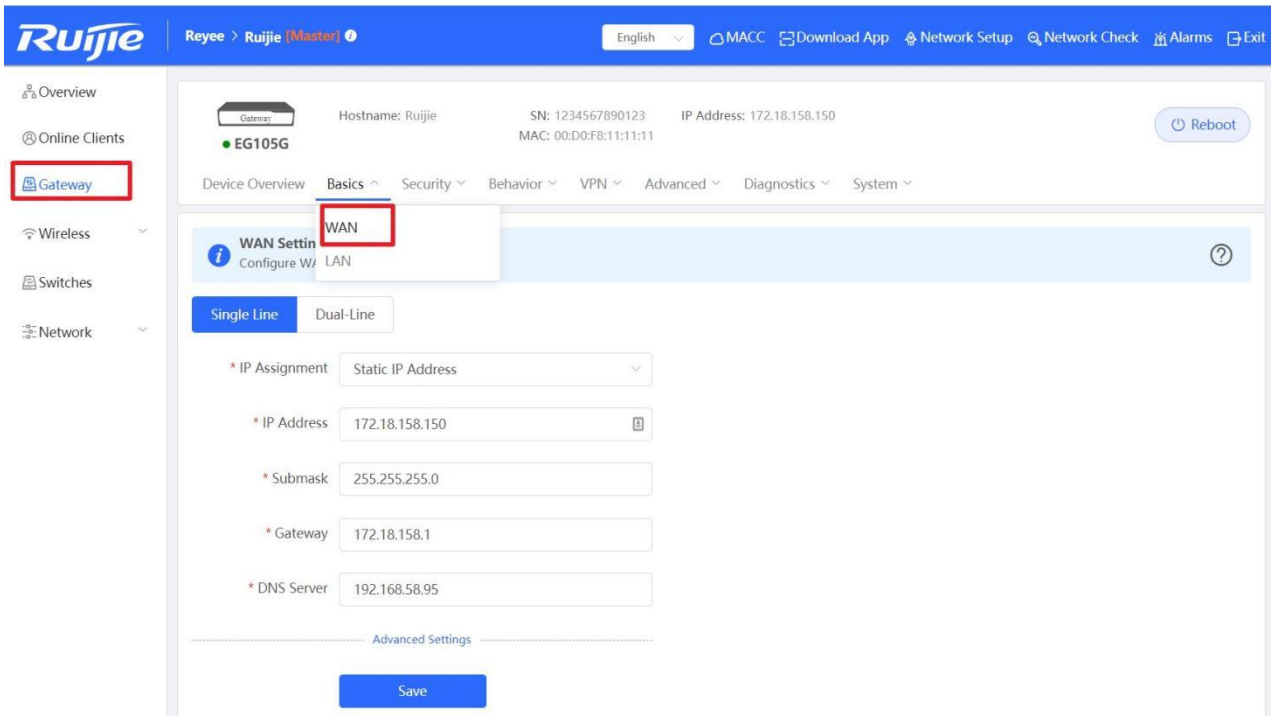


Prerequisite

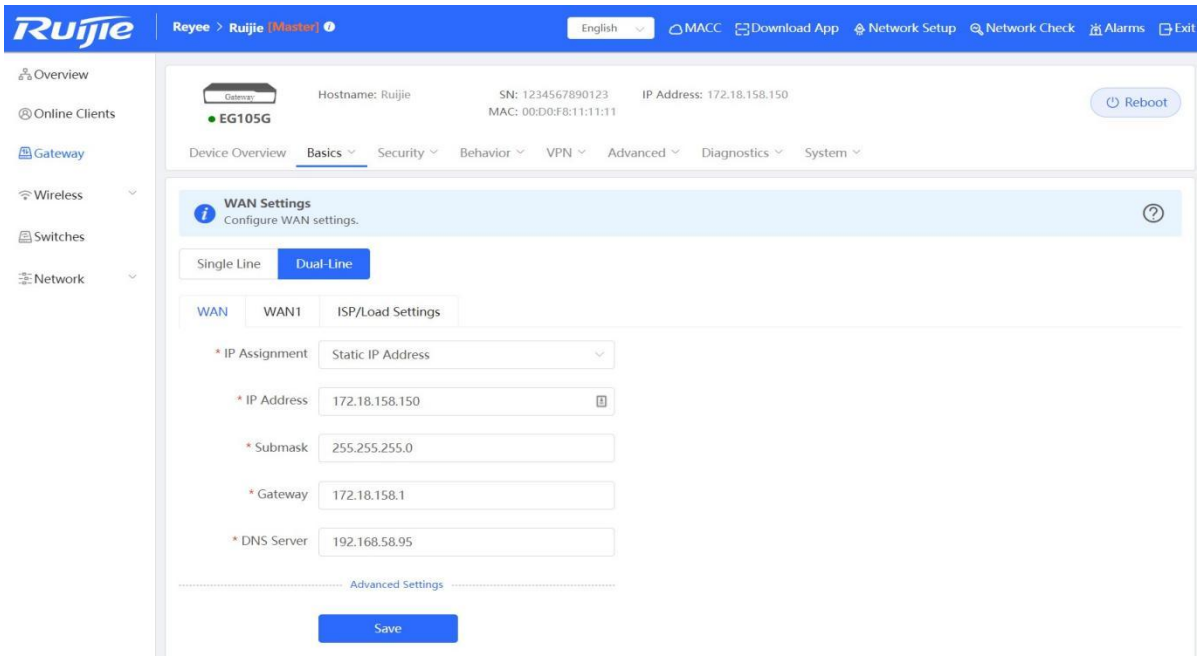
Two uplink cables which can access internet should be prepared.

Procedure

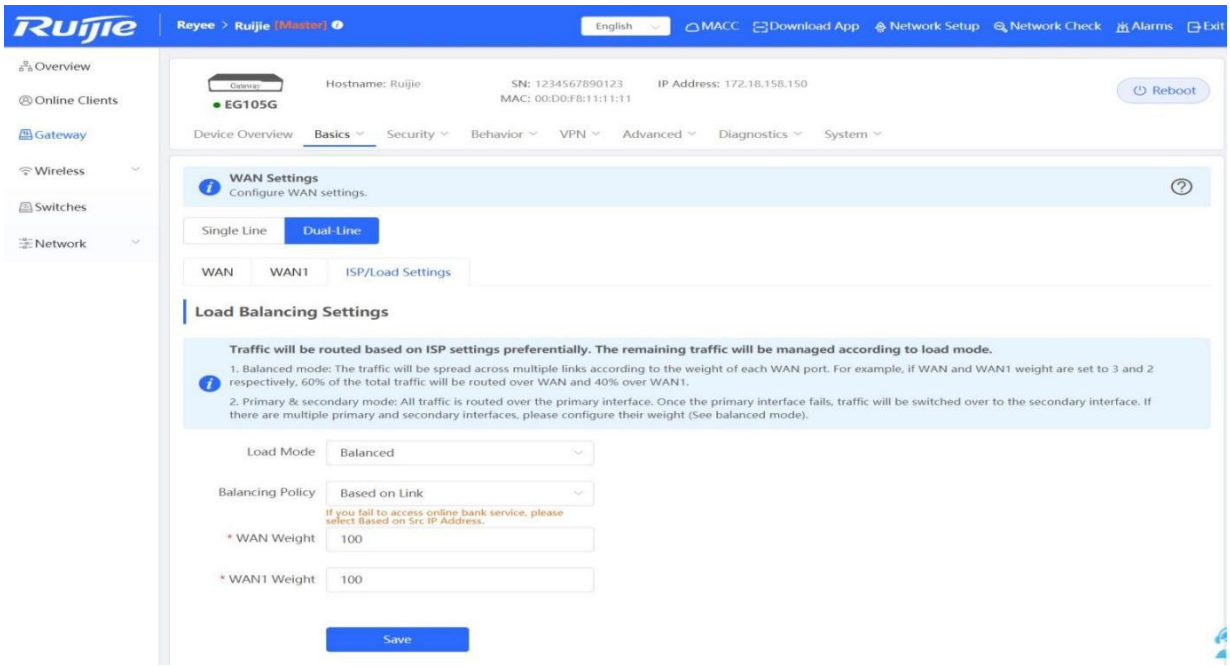
Step 1: Choose **Gateway → Basics → WAN**



Step 2: Configure the **WAN interface** accordingly



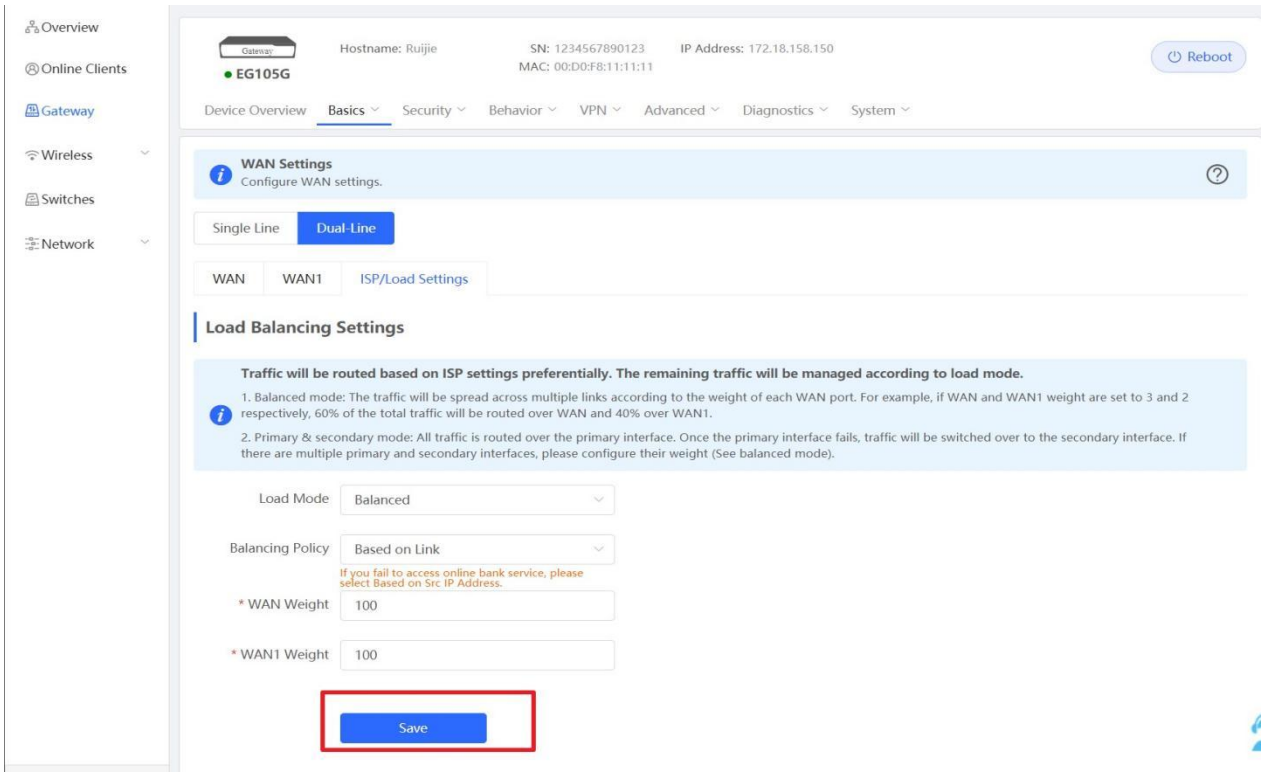
Step 3: Choose **ISP/Load Settings**, and configure the load mode and interface weight



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.

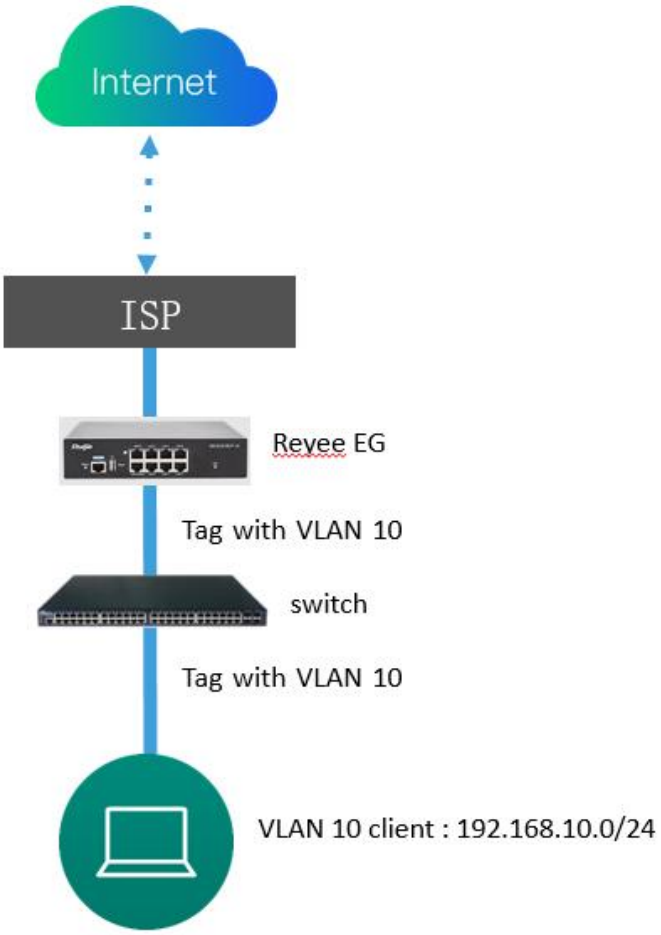
Primary & secondary mode: All traffic is routed over the primary interface. Once the primary interface fails, traffic will be switched over to the secondary interface. If there are multiple primary and secondary interfaces, please configure their weight (See balanced mode).

Step 4: Save the configuration



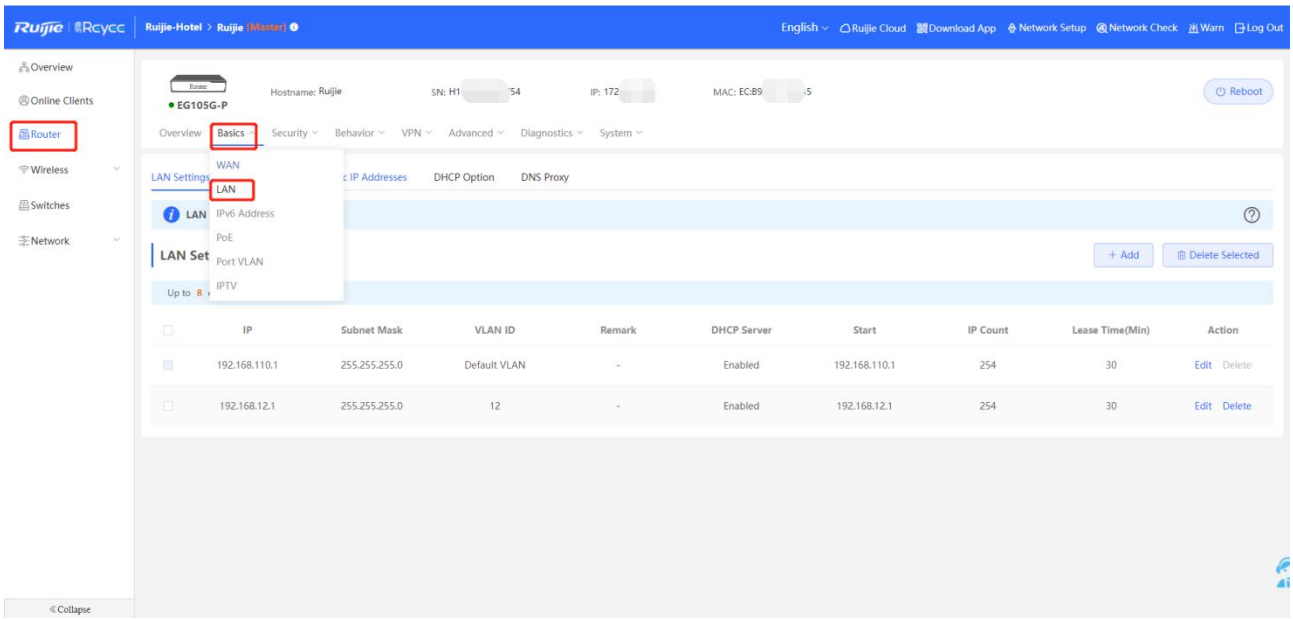
4.1.7 Port VLAN

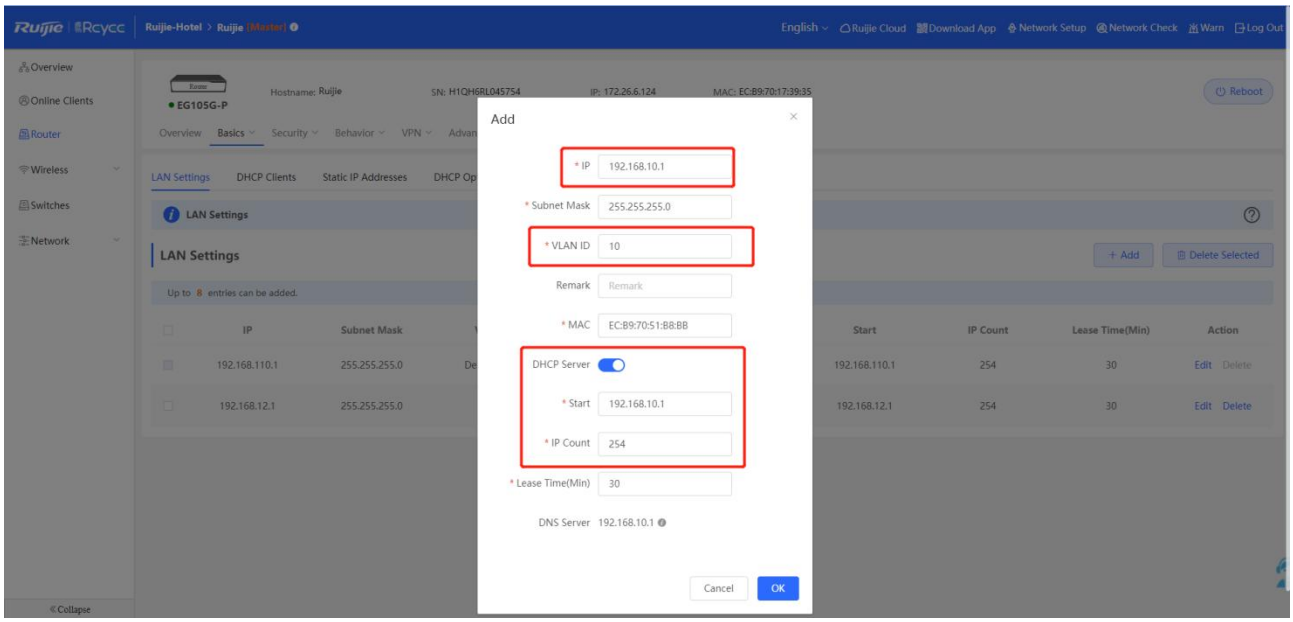
Application Scenario



Procedure

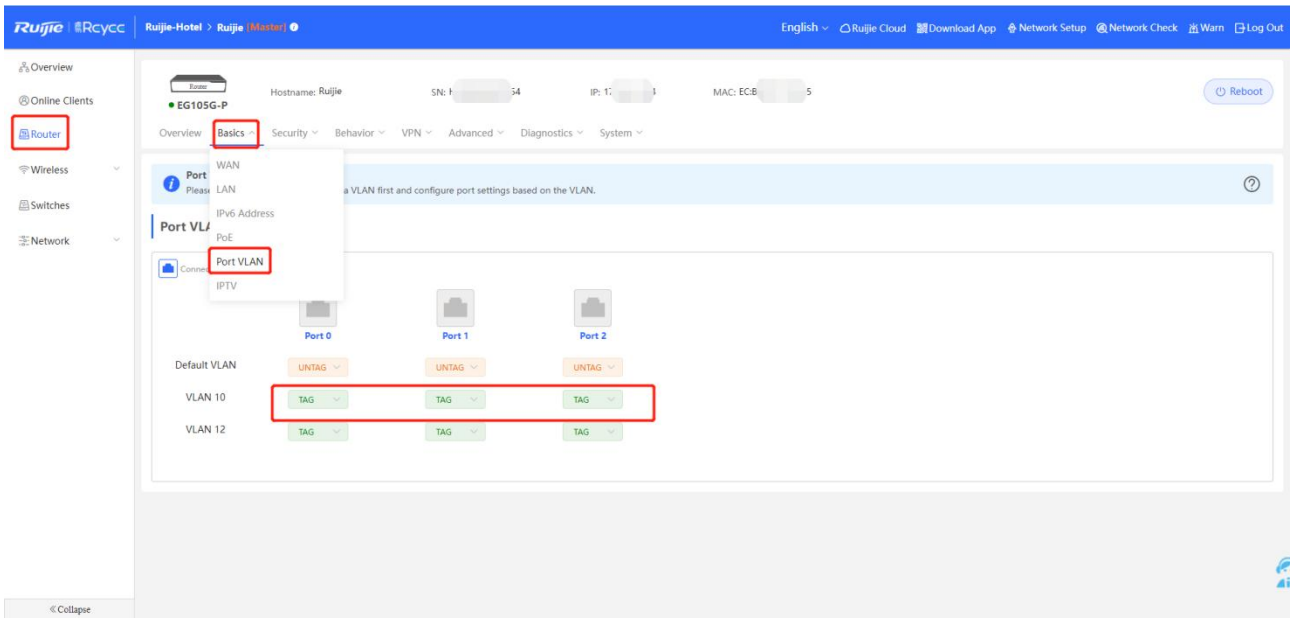
1. Click **Router->Basics->LAN** to create VLAN first.





	192.168.10.1	255.255.255.0	10	-	Enabled	192.168.10.1	254	30	Edit Delete

2. Click **Port VLAN** to tag VLAN, normally the VLAN will be tagged default.



UNTAG: If VLAN 10 is set to untag VLAN of port 2, VLAN 10 will be the native VLAN of port 2. The packets from VLAN 10 will be forwarded over port 2 without tag VLAN 10 and all untagged packets over port 2 will be taken as the packets from VLAN 10.

Each port can be configured with only one untag VLAN.

The native VLAN of port 1 is the default VLAN and cannot be edited.

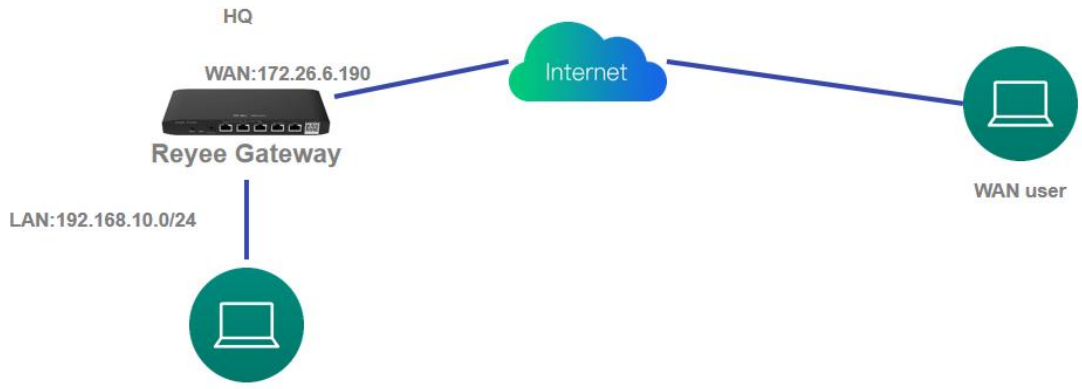
TAG: If both VLAN 10 and VLAN 20 are set to tag VLAN of port 2, the packets from VLAN 10 and VLAN 20 will be forwarded over port 2 with the corresponding VLAN tag.

Not Join: If both VLAN 10 and VLAN 20 are set to **Not Join port 2**, port 2 will not receive or transmit packets from VLAN 10 or VLAN 20.

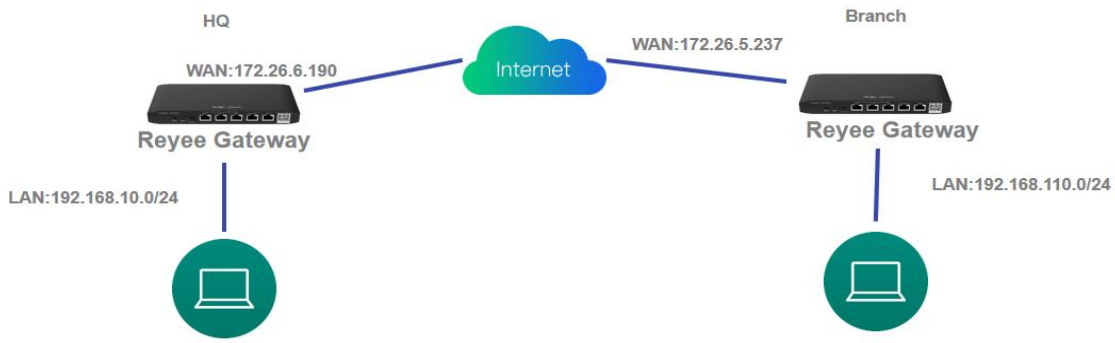
4.1.8 VPN

Application Scenario

Clients to Site Scenario



Site to Site Scenario



Procedure

4.1.8.1 PPTP VPN

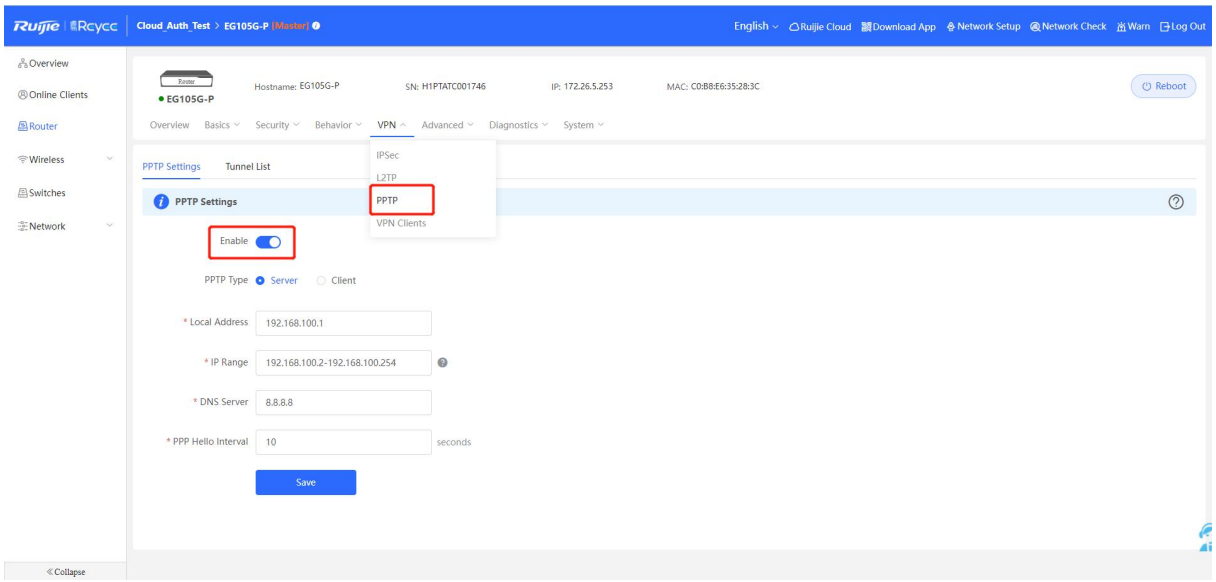
PPTP VPN usually is used for the clients to site scenario and site to site scenario. For example, clients work from home, but he need to access company server through PPTP VPN tunnel. Another example is that a company has three branches which are distributed in three different places of the Internet, and every place need to establish a tunnel with each other by a gateway.

1) Clients to Site Scenario Configuration

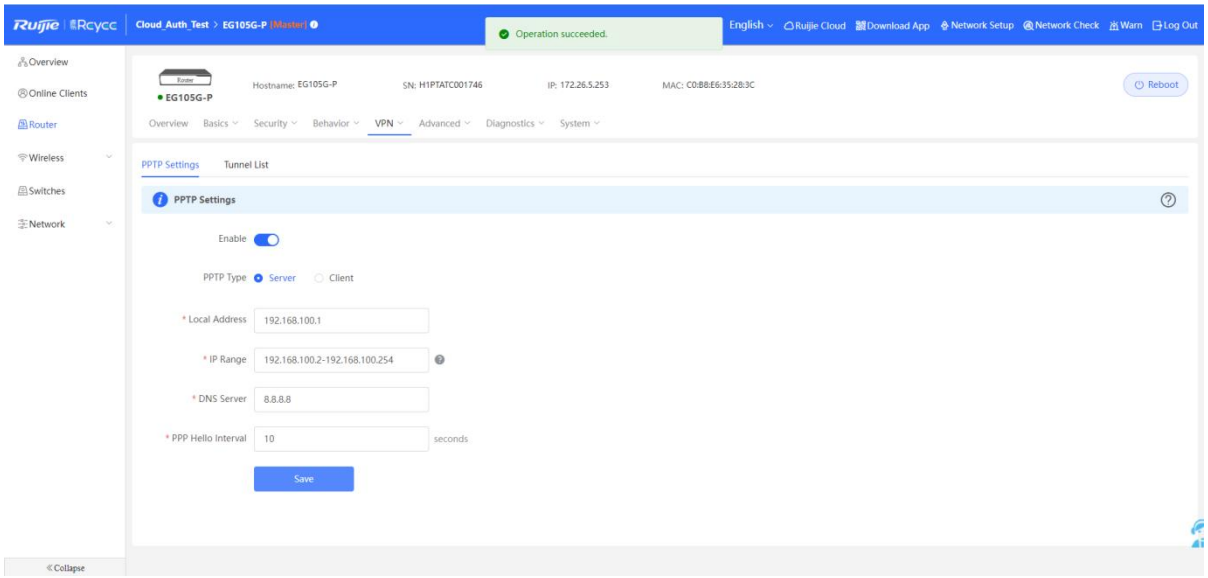
(1) On the HQ side:

Log in to Reyee EG by the default IP 192.168.110.1.

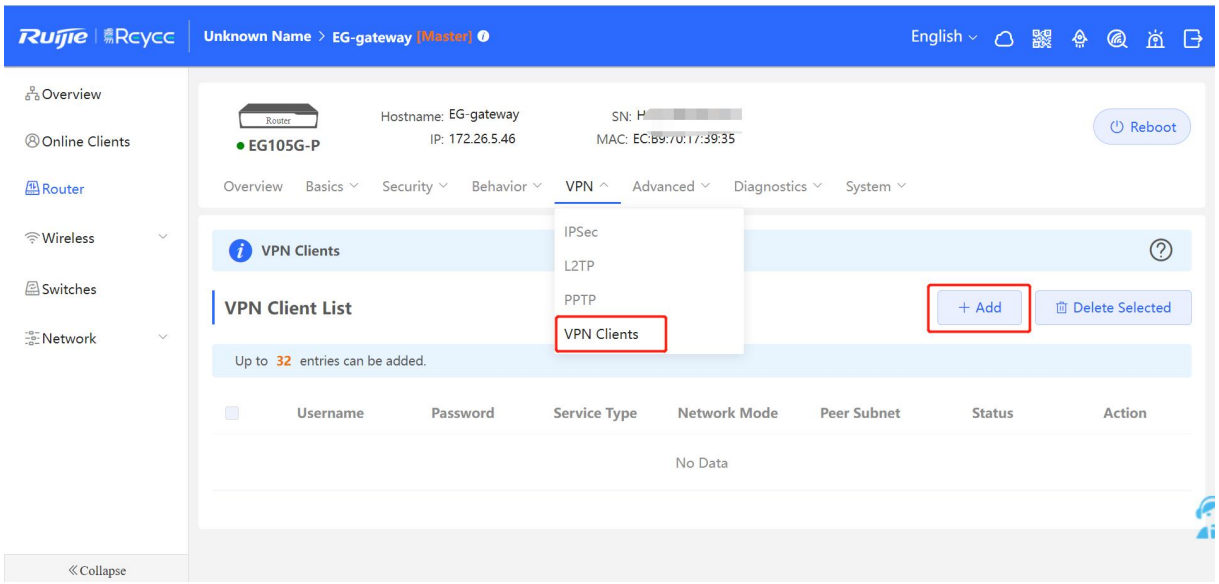
Click **Setup->VPN->PPTP** and enable **PPTP.**

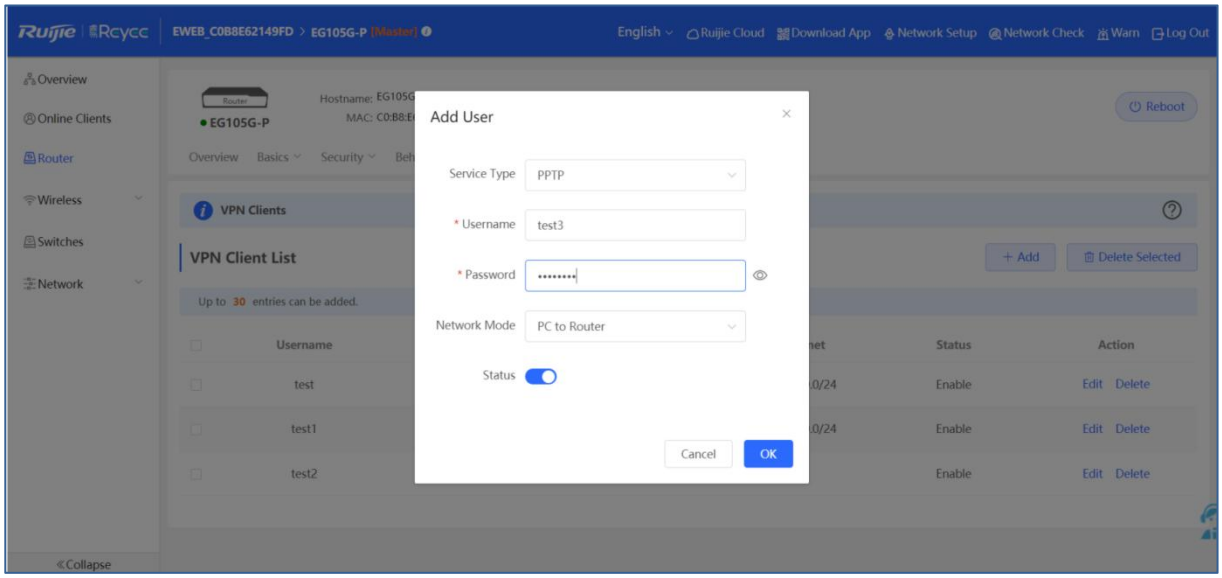


c Configure the PPTP setting and click Save.



d Configure VPN clients



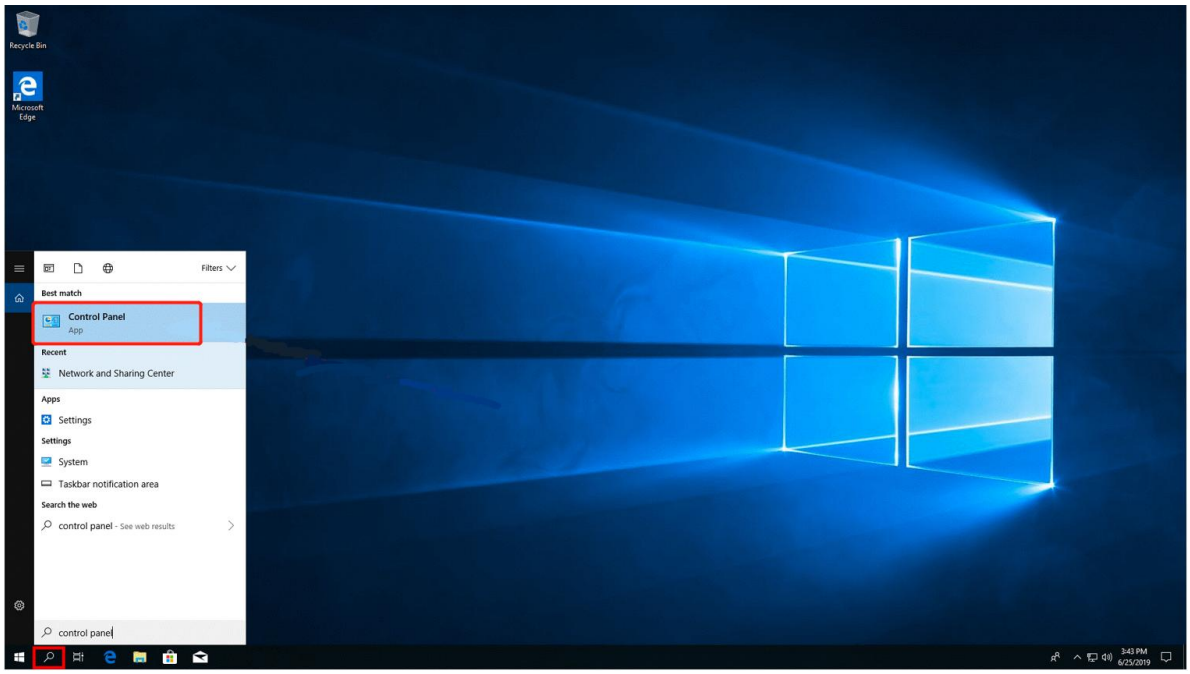


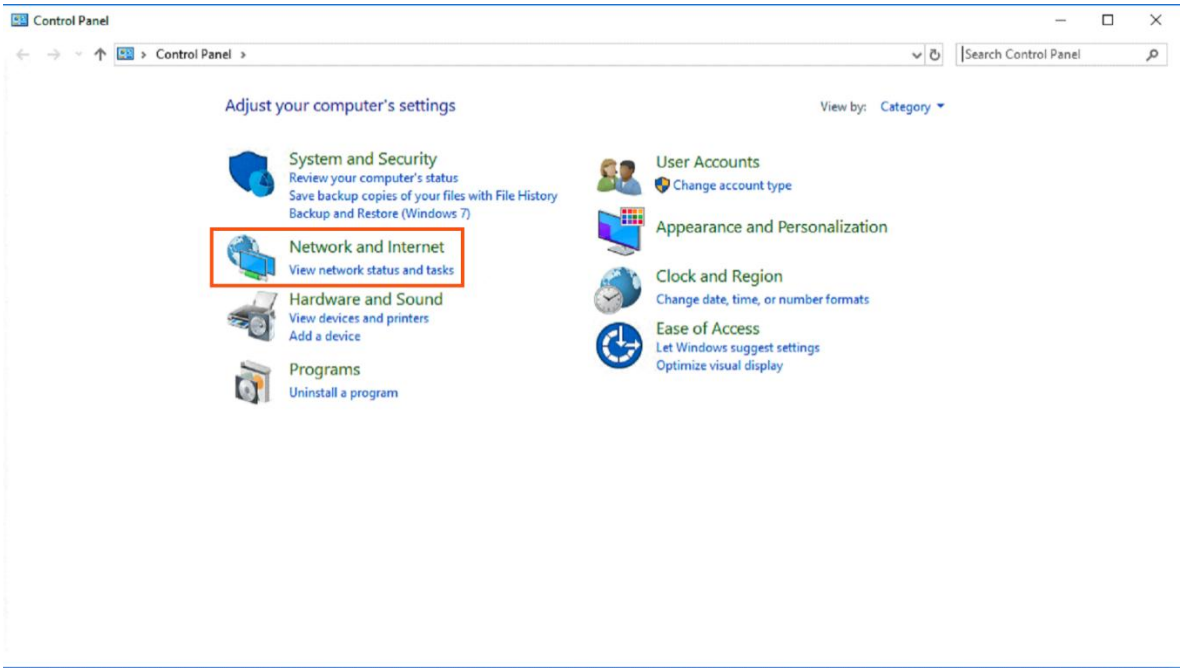
Note

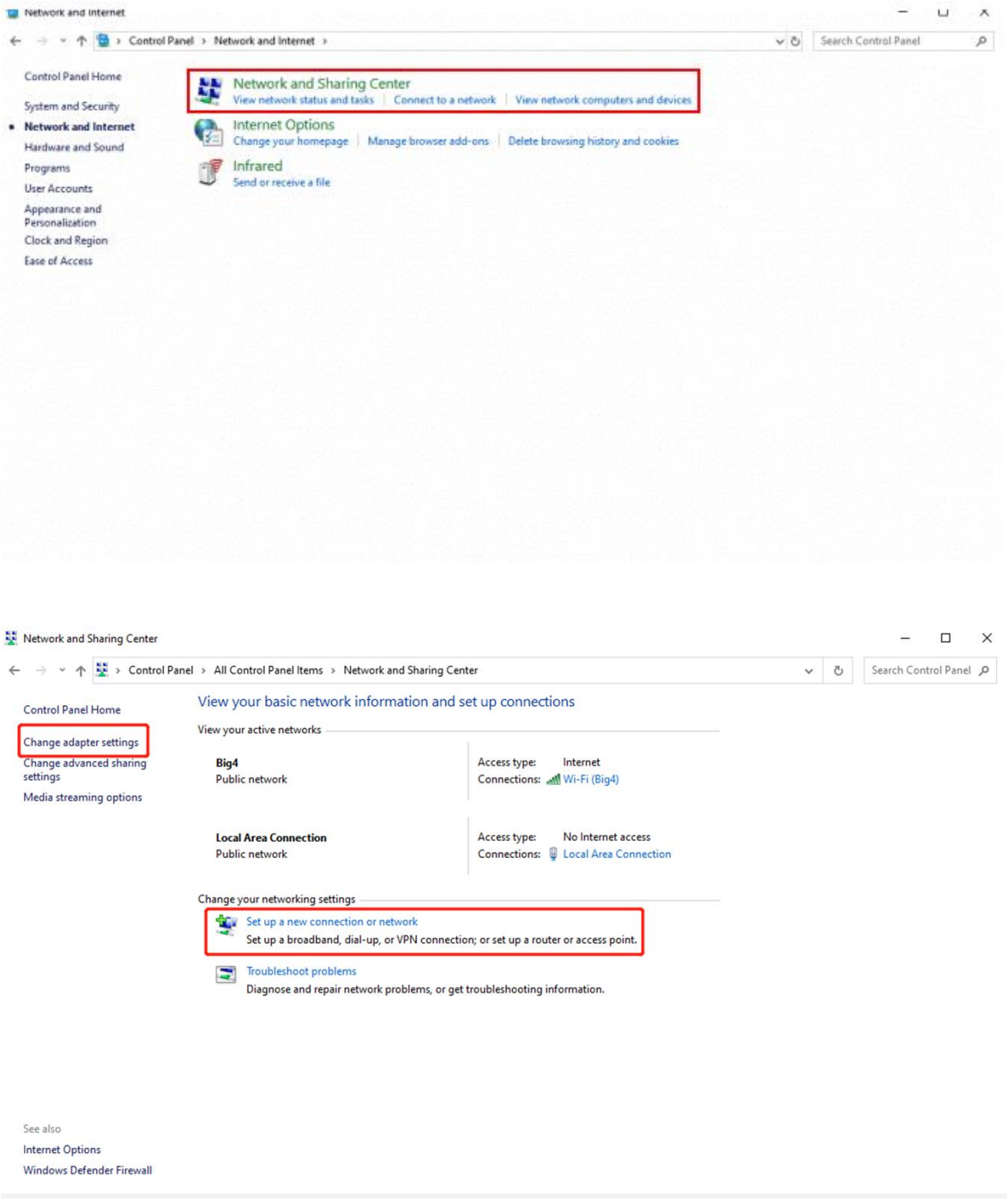
- Service type: select PPTP.
- Network mode: select router to router.
- Peer Subnet: fill in the internal network segment of the branch. Please do(not to overlap with the internal network segment of the headquarters).

(2) On the Clients side (take Windows 10 as example):

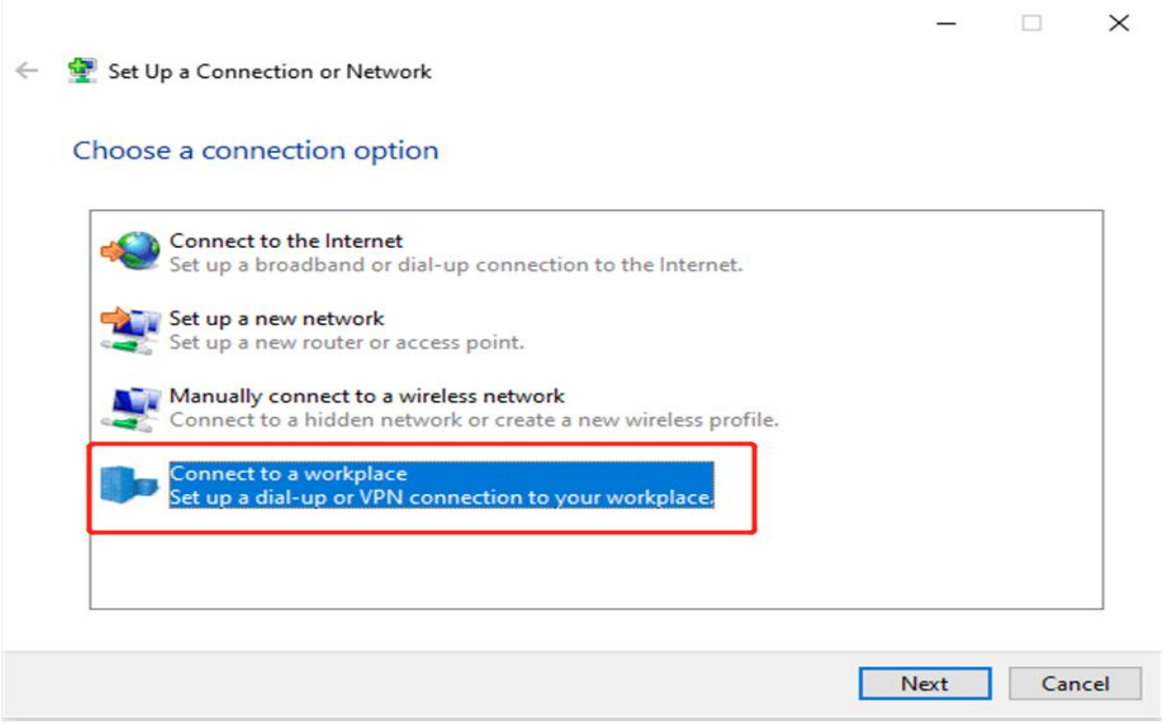
Enter **Control Panel→Network and Internet→Network and Sharing Center**

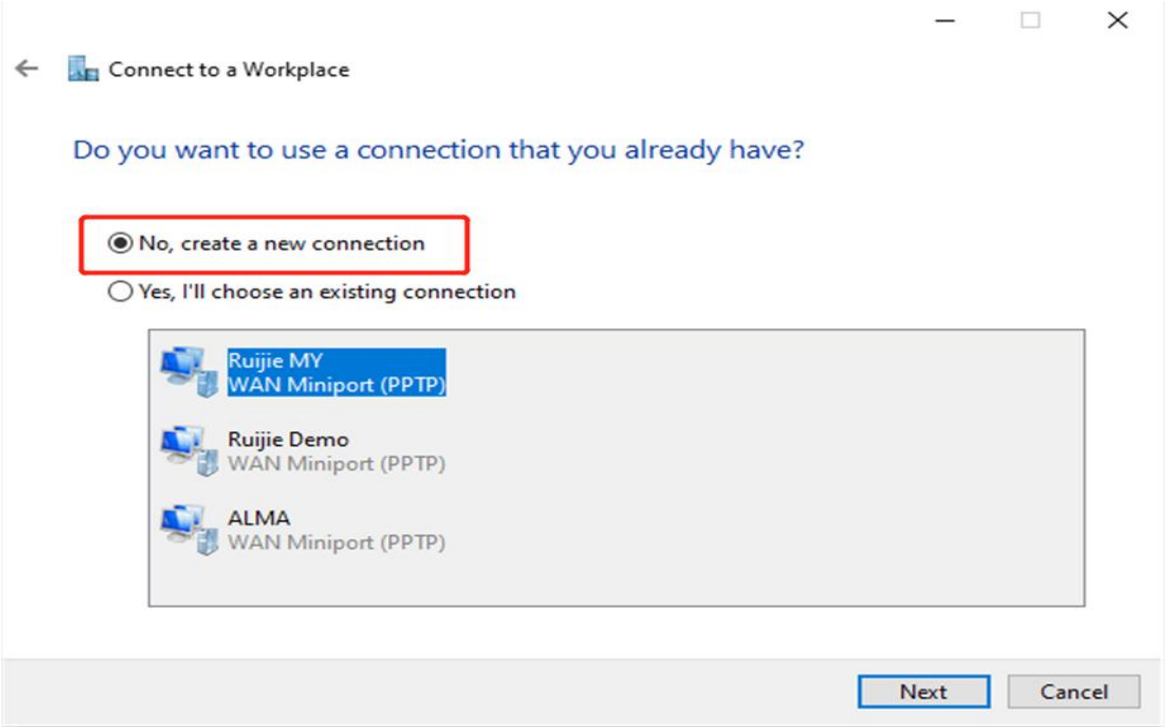

Recycle Bin
Microsoft Edge
Filters
Best match
Control Panel
App
Recent
Network and Sharing Center
Apps
Settings
Settings
System
Taskbar notification area
Search the web
control panel - See web results
control panel
3:43 PM
6/25/2019

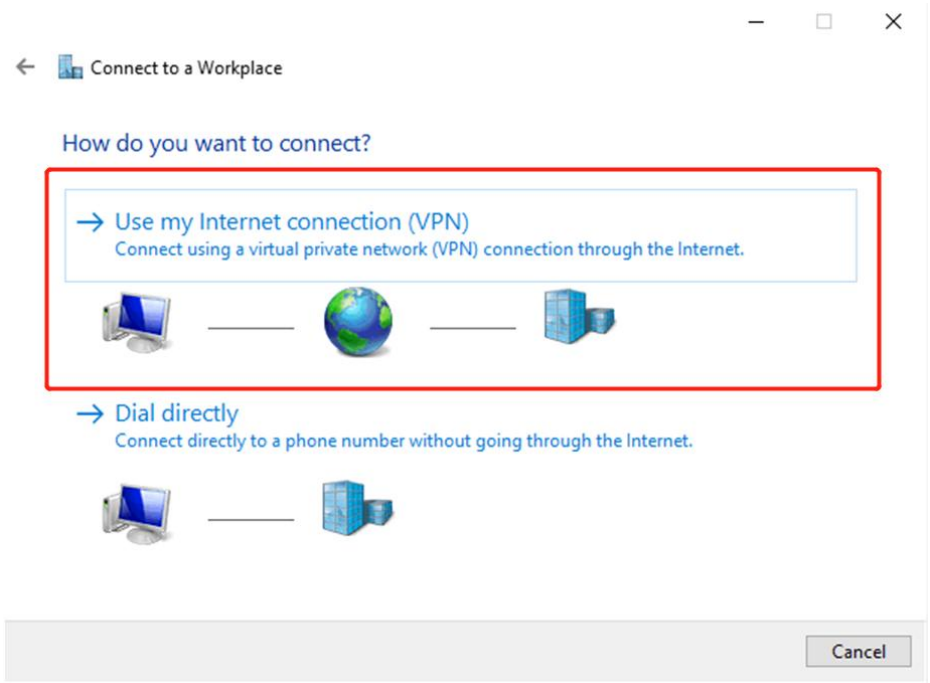

Control Panel
Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
Network and Internet
View network status and tasks
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalization
Clock and Region
Change date, time, or number formats
Ease of Access
Let Windows suggest settings
Optimize visual display

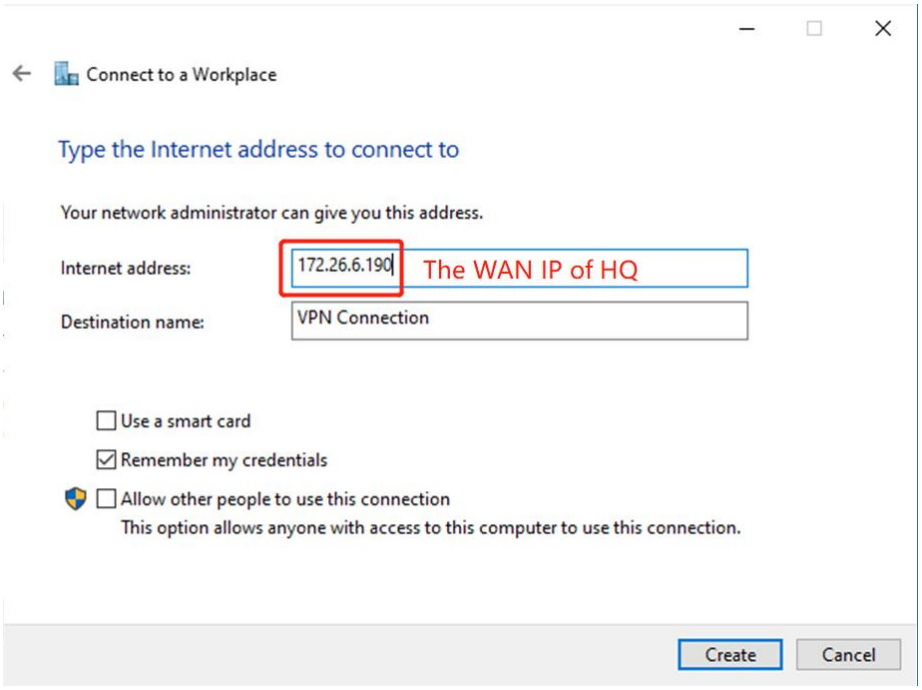


b Configure VPN connection

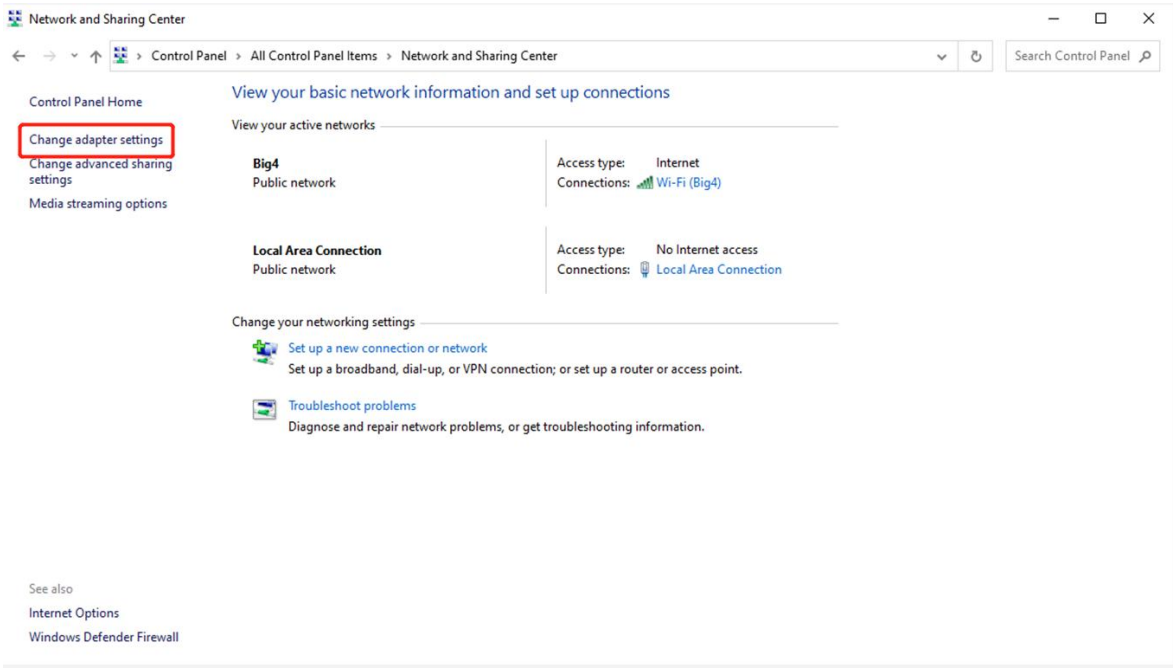

Set Up a Connection or Network
Choose a connection option
Connect to the Internet
Set up a broadband or dial-up connection to the Internet.
Set up a new network
Set up a new router or access point.
Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.
Connect to a workplace
Set up a dial-up or VPN connection to your workplace.
Next
Cancel

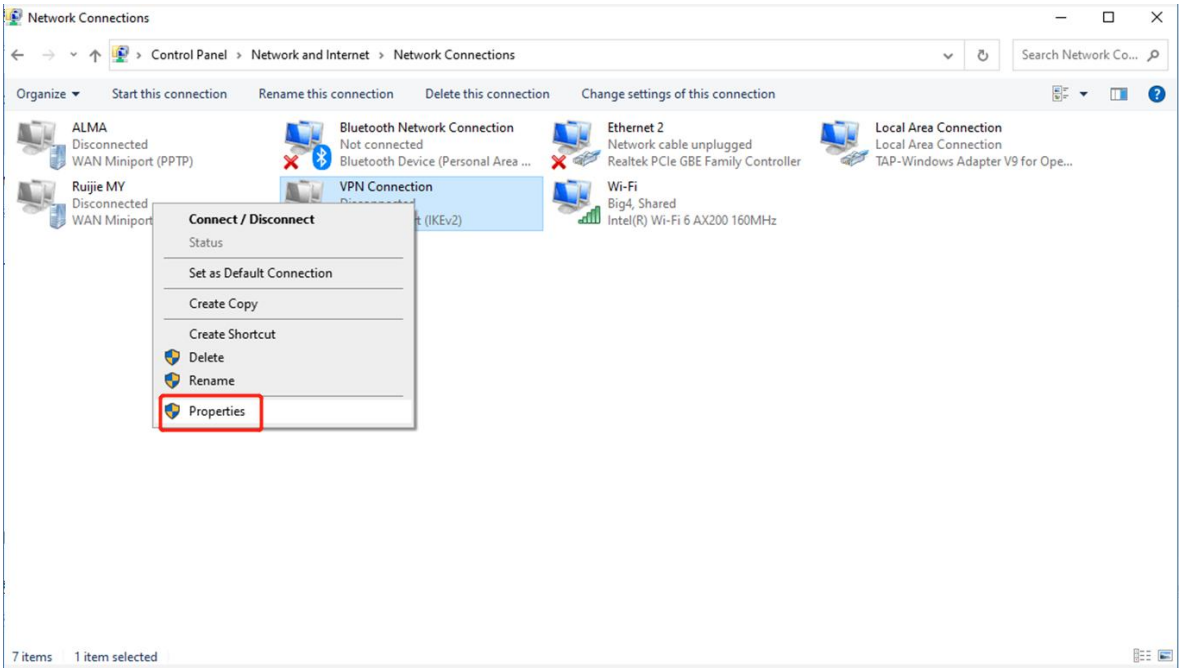

Connect to a Workplace
Do you want to use a connection that you already have?
No, create a new connection
Yes, I'll choose an existing connection
Ruijie MY
WAN Miniport (PPTP)
Ruijie Demo
WAN Miniport (PPTP)
ALMA
WAN Miniport (PPTP)
Next
Cancel

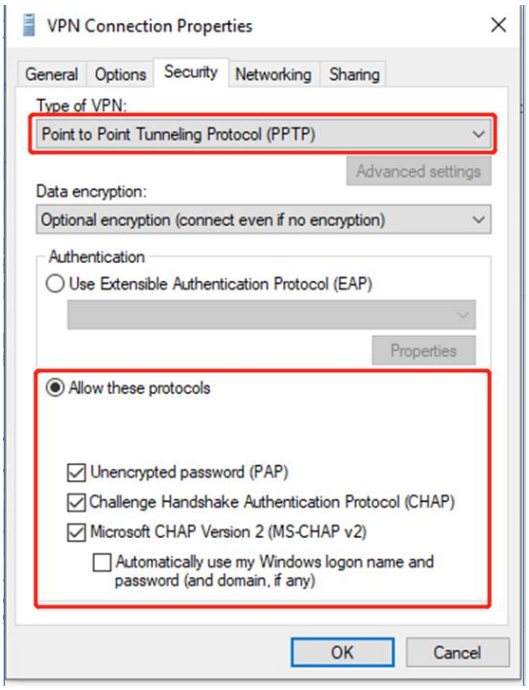




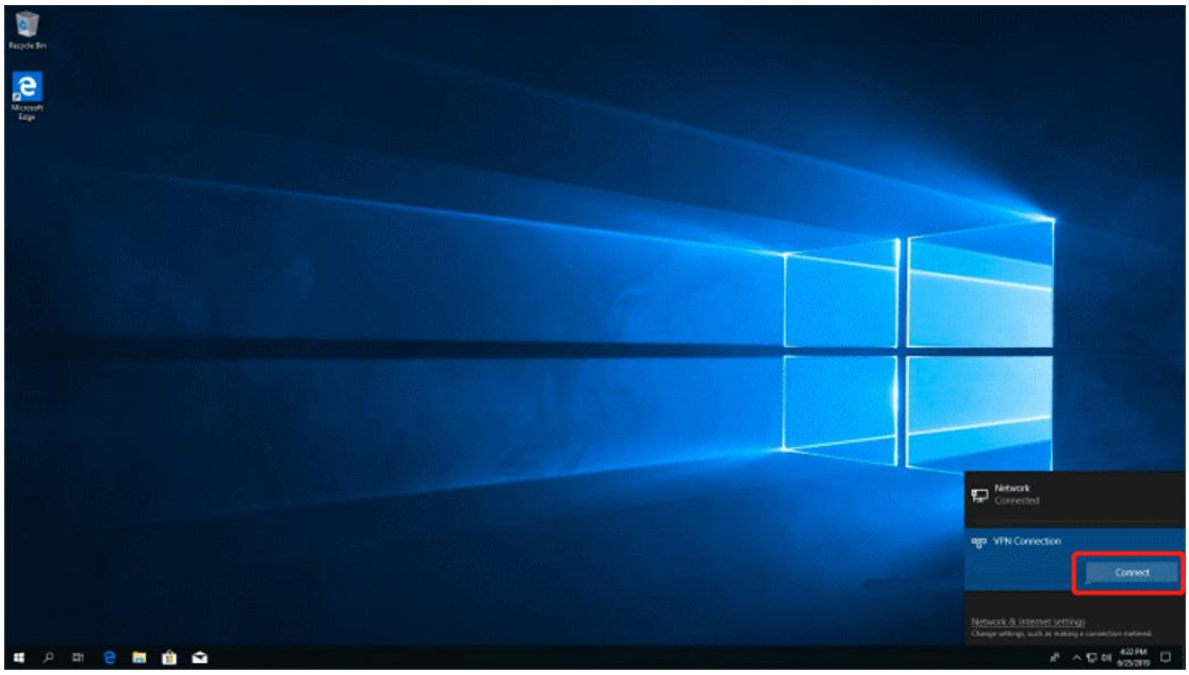
c Change adapter's setting.

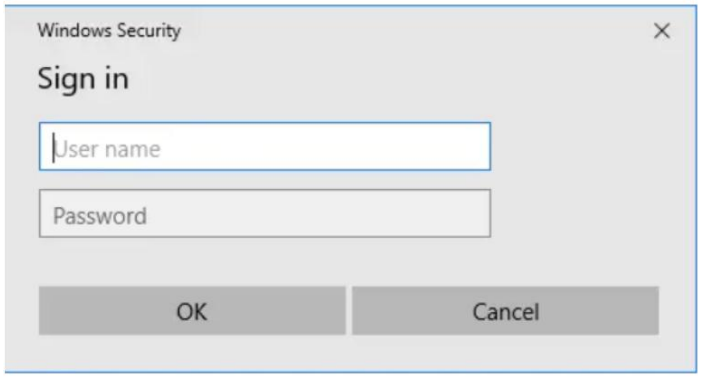

Network and Sharing Center
Control Panel › All Control Panel Items › Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
Media streaming options
View your basic network information and set up connections
View your active networks
Big4
Public network
Access type: Internet
Connections: Wi-Fi (Big4)
Local Area Connection
Public network
Access type: No Internet access
Connections: Local Area Connection
Change your networking settings
Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.
See also
Internet Options
Windows Defender Firewall

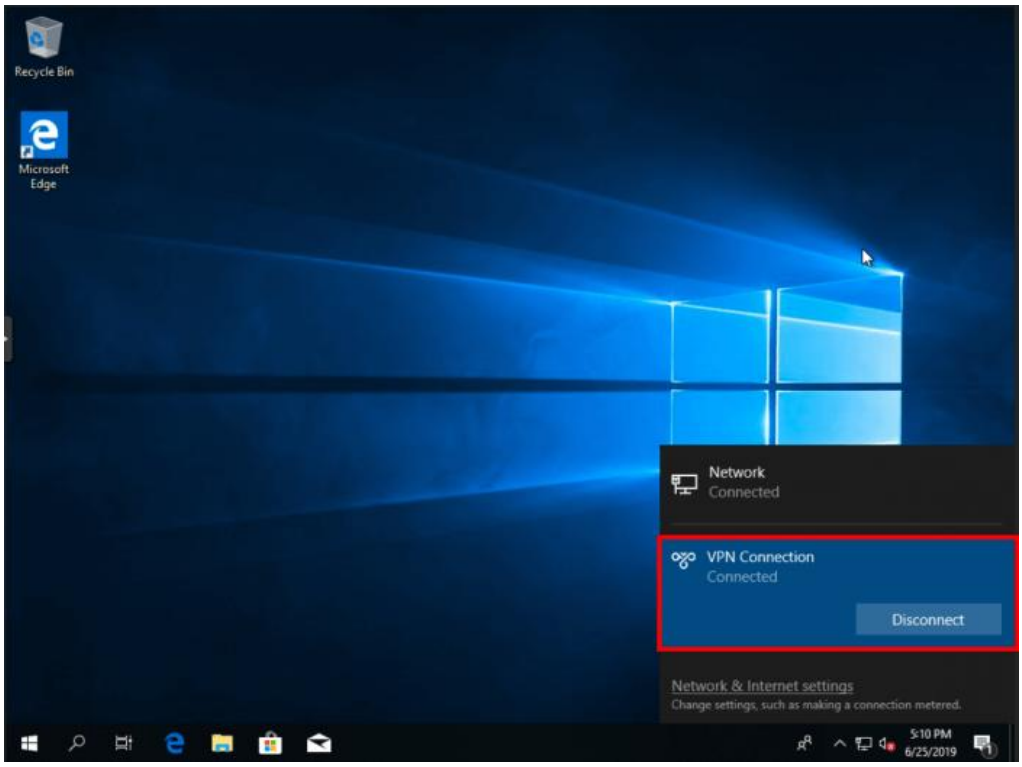

Network Connections
Control Panel › Network and Internet › Network Connections
Search Network Co...
Organize
Start this connection
Rename this connection
Delete this connection
Change settings of this connection
ALMA
Disconnected
WAN Miniport (PPTP)
Bluetooth Network Connection
Not connected
Bluetooth Device (Personal Area ...
Ethernet 2
Network cable unplugged
Realtek PCIe GBE Family Controller
Local Area Connection
Local Area Connection
TAP-Windows Adapter V9 for Ope...
Ruijie MY
Disconnected
WAN Miniport
VPN Connection
Wi-Fi
Big4, Shared
Intel(R) Wi-Fi 6 AX200 160MHz
Connect / Disconnect
Status
Set as Default Connection
Create Copy
Create Shortcut
Delete
Rename
Properties
7 items
1 item selected



d Check the Status of Connect VPN Connection Status.







e If your PC can't reach HQ internal devices(192.168.10.0/24) after VPN connected. Add the following static route on your PC. The 192.168.100.2 is the PC's IP get from HQ. Then PC can reach HQ internal devices normally.

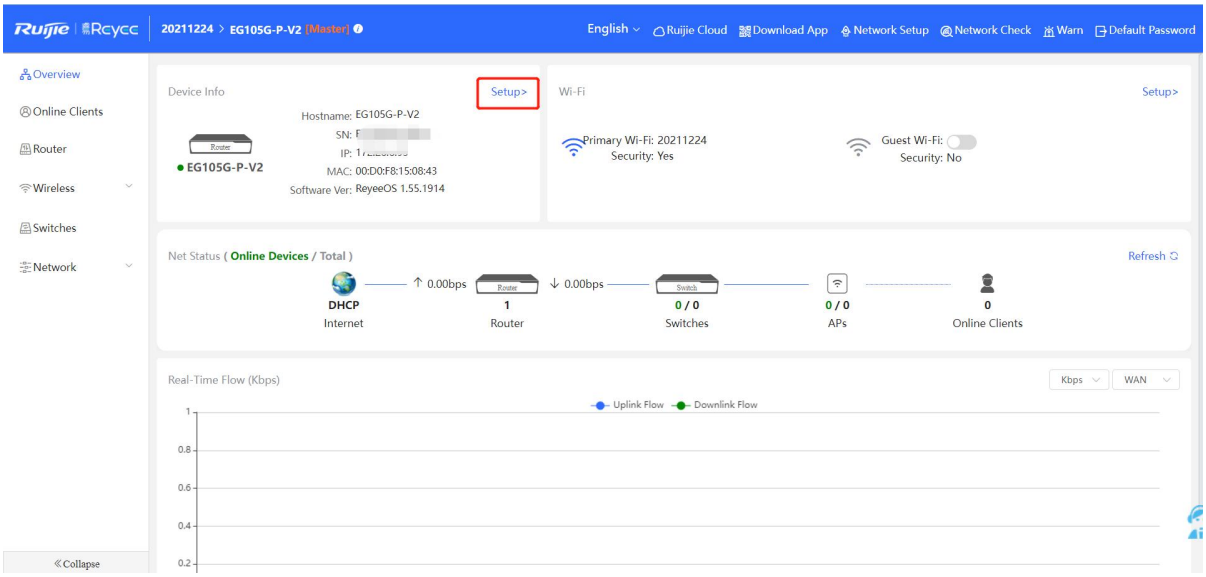
```
C:\Users\Daisy>route add 192.168.168.10.0 mask 255.255.255.0 192.168.100.2
```

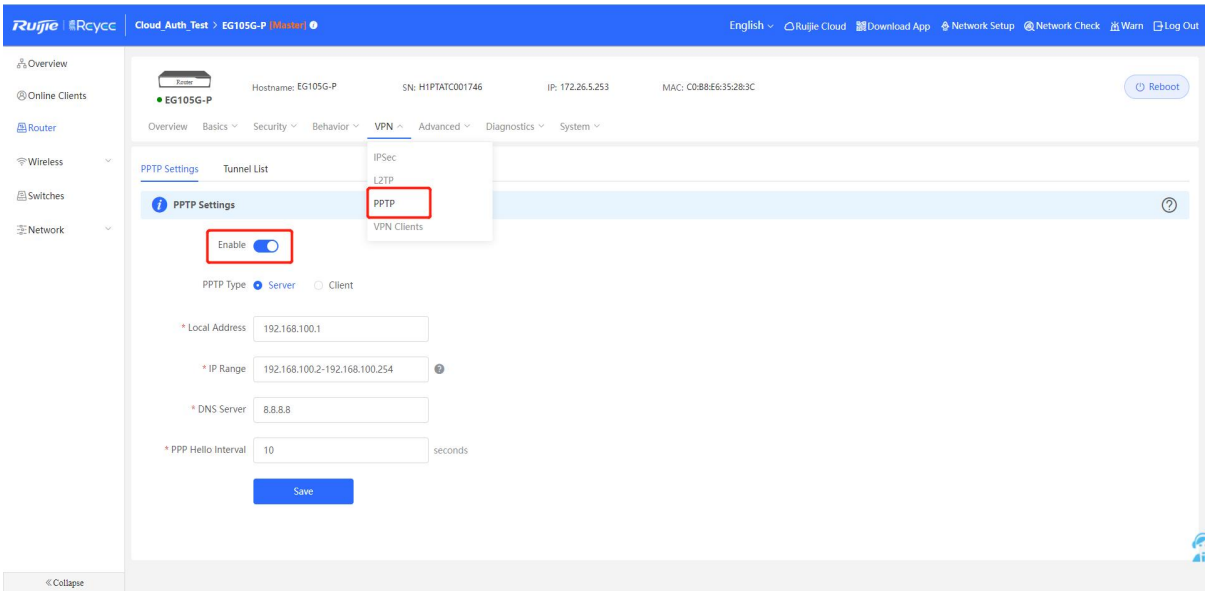
Site to Site Scenario Configuration

(1) On the HQ side:

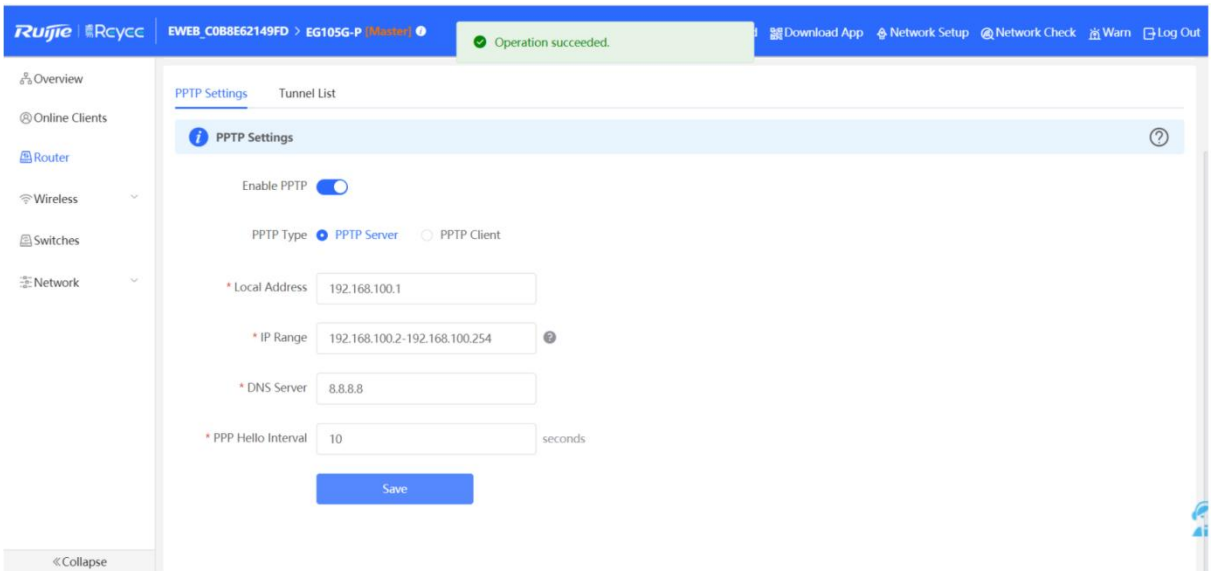
a Log in to Reyee EG by the default IP 192.168.110.1.

b Click Setup->VPN->PPTP and then enable PPTP, choose PPTP type as Server.

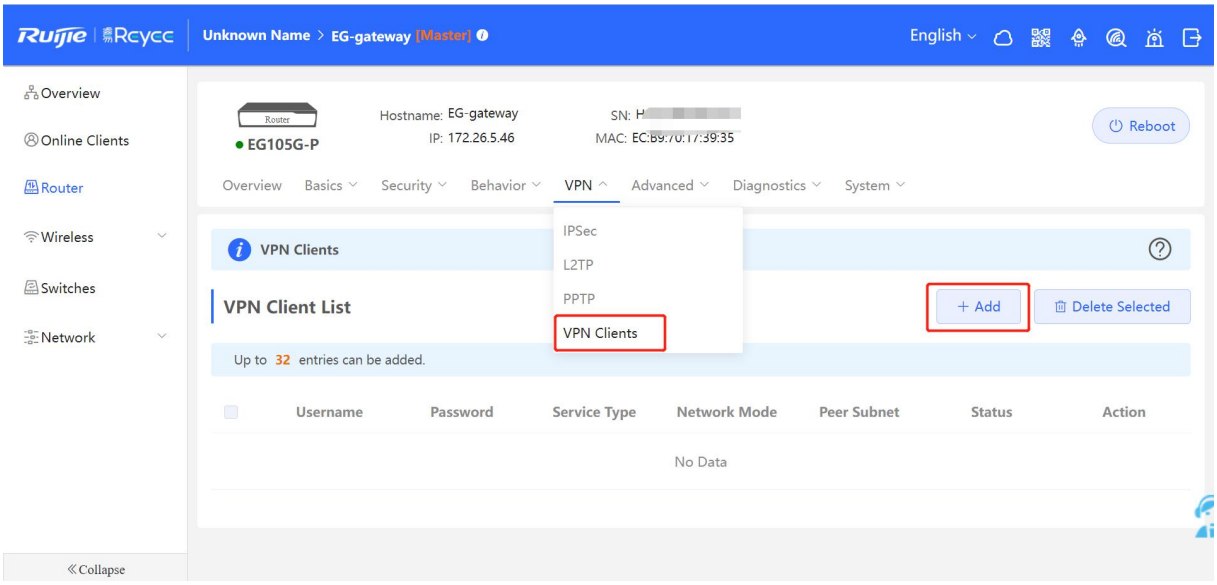


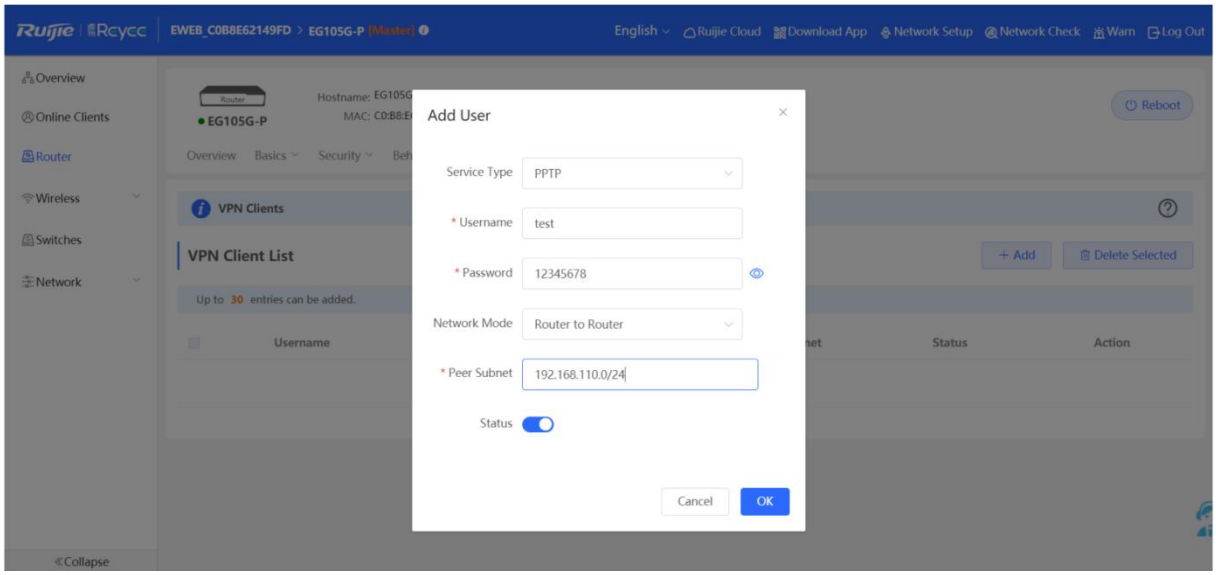


c Configure the PPTP settings and click Save.



d Configure VPN client.





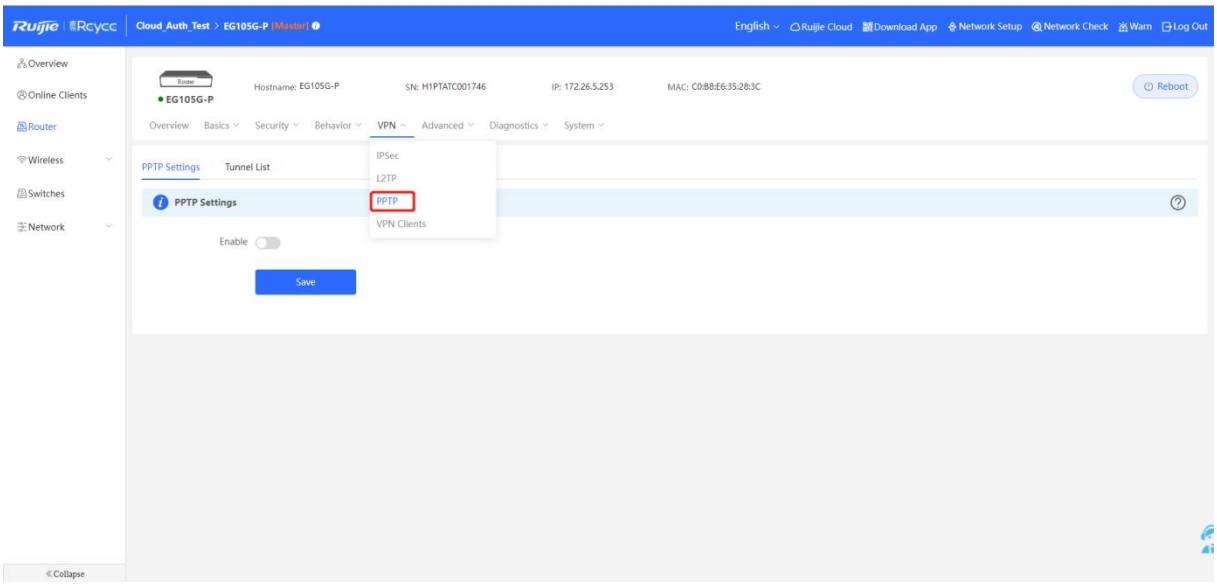
Note

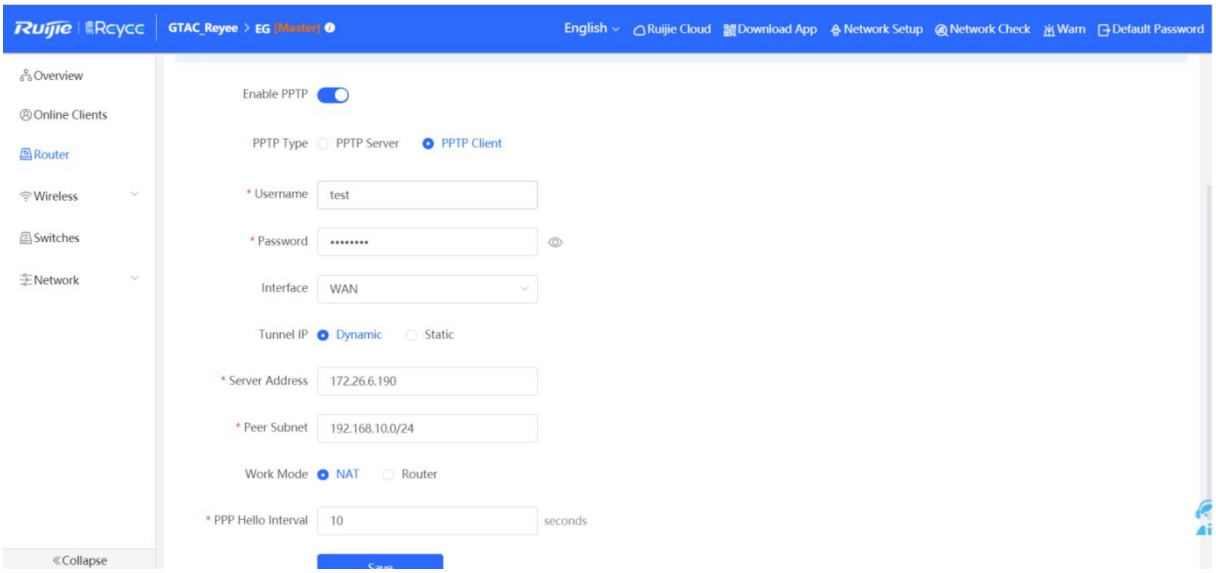
- The Peer Subnet is the local IP range of its branch.

On the Branch side:

a Log in to the Reyee EG by the default IP 192.168.110.1.

b Click **Setup->VPN->PPTP** and then enable **PPTP**, choose **PPTP type** as **Client**.

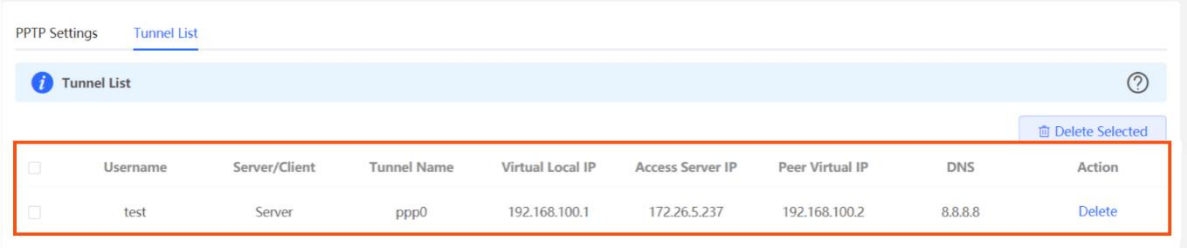




Note

- PPTP type: select PPTP Client
- Username and password: Fill in the username and password Which have been added in the headquarters
- Tunnel IP: Tunnel IP address is the address in the IP range of the address pool filled in by the headquarters. Selecting dynamic means assigning the IP address of the address pool randomly. Selecting static means that, any addresses in the address pool can be entered by yourself without conflict.
- Server address: Fill in the WAN port address of the headquarters (public network IP is required. This is a test, so it is a private network address).
- Peer Subnet: the internal network segment of the headquarters (do not overlap with the internal network segment of the branch).
- Work mode: The work mode here refers to whether the headquarters is allowed to access the branch intranet, if it is allowed, select [Router], if not, select [NAT].

c Check the VPN connection status.



4.1.8.2 L2TP VPN

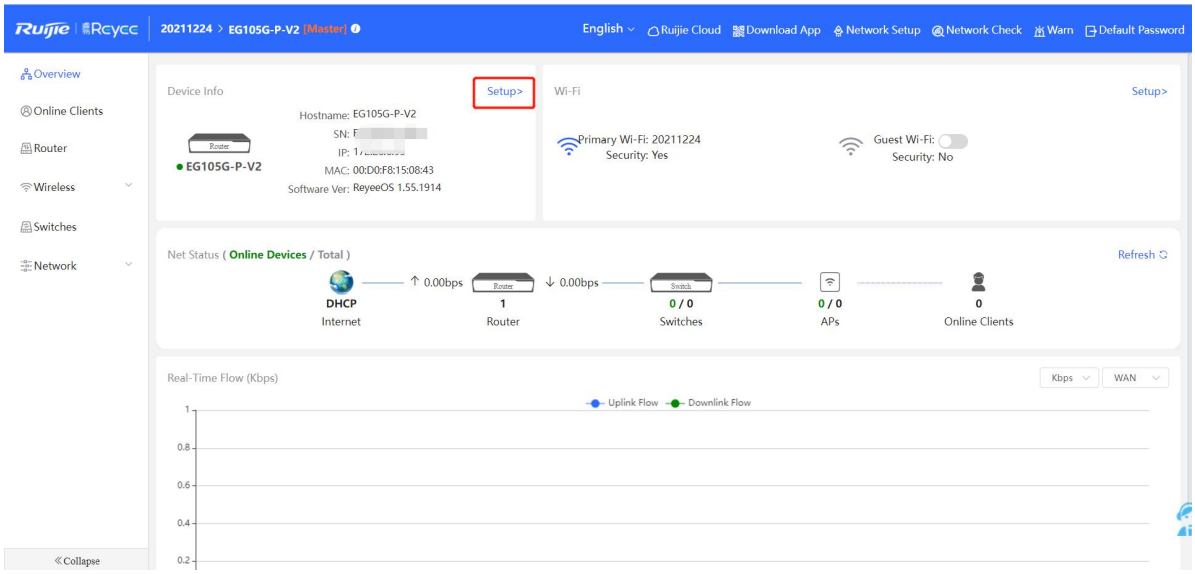
L2TP VPN usually is used for the clients to site scenario and site to site scenario. For example, clients work from home but he need to access company server through L2TP VPN tunnel. Another example is that a company has three branches which are distributed in three different places of the Internet, and everyone need to establish a tunnel with each other by a gateway.

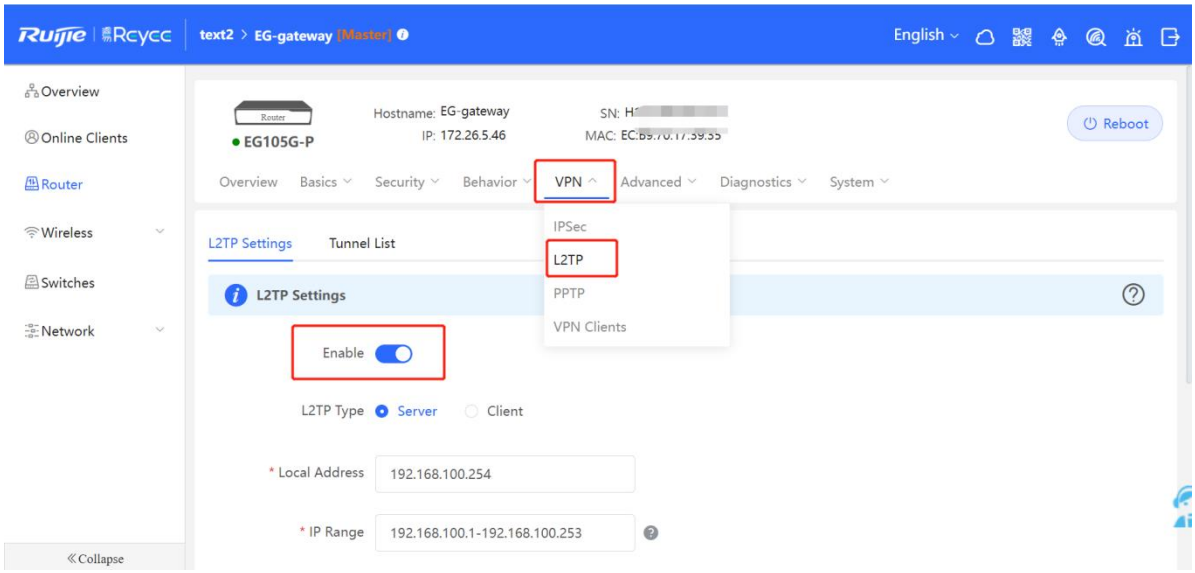
Clients to Site Scenario Configuration

On the HQ side:

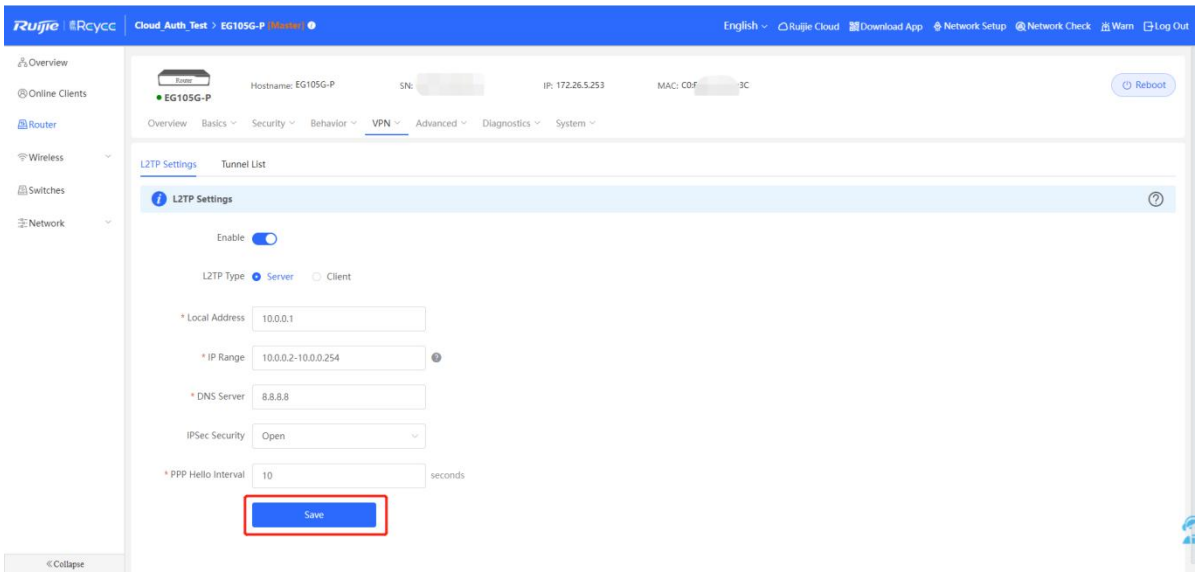
a Log in to Reyee EG by the default IP 192.168.110.1.

b Click Setup->VPN->L2TP and enable L2TP.

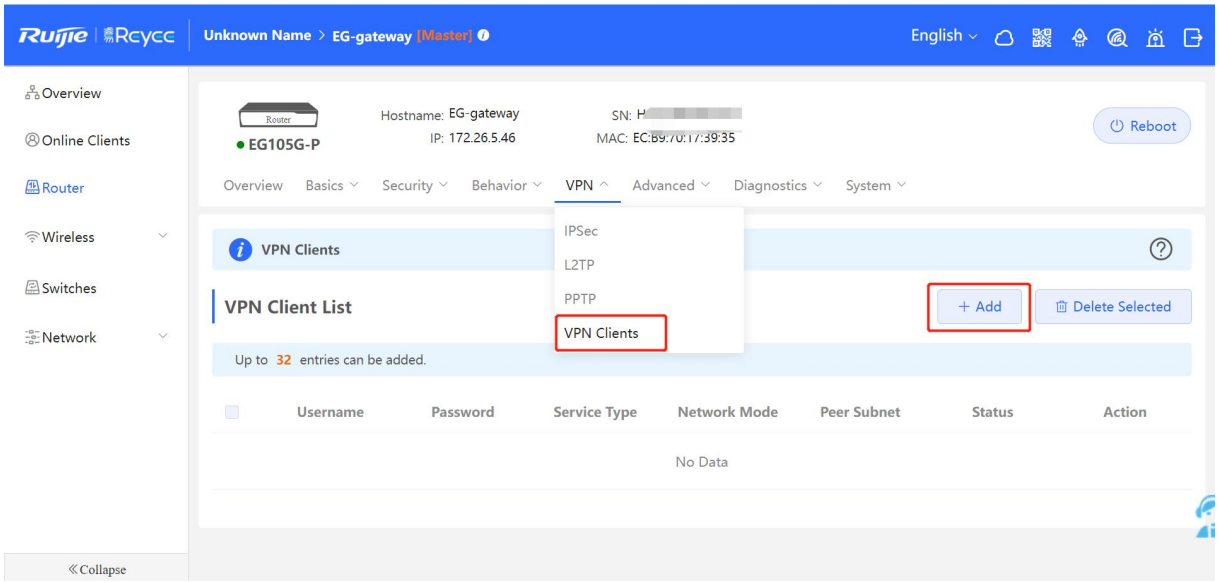


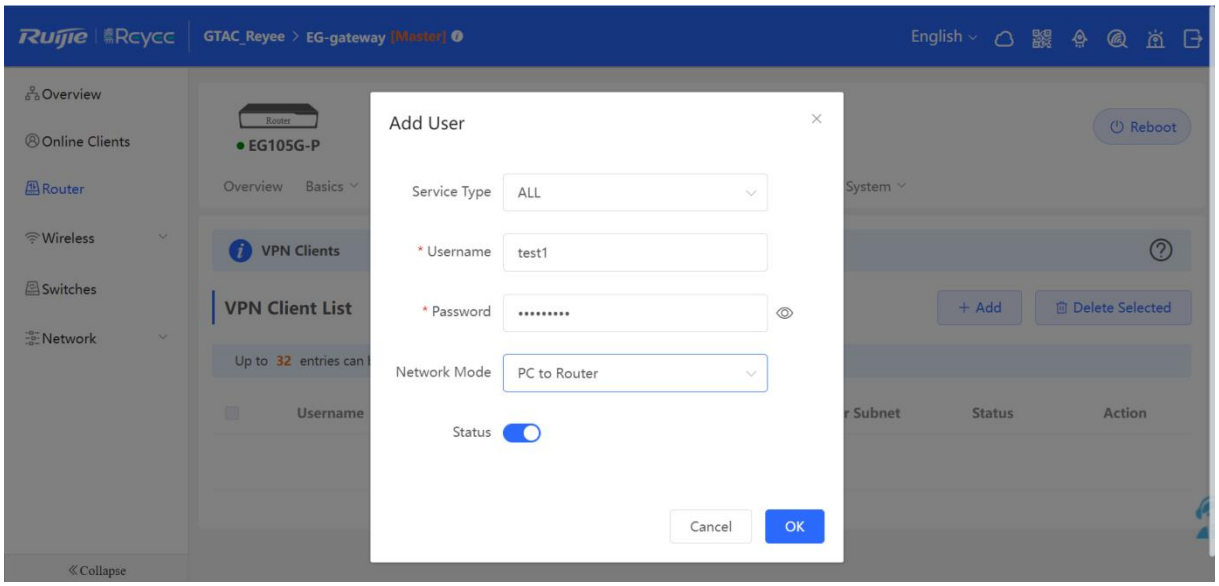


c Configure the L2TP setting and click **Save**.



d Configure VPN clients



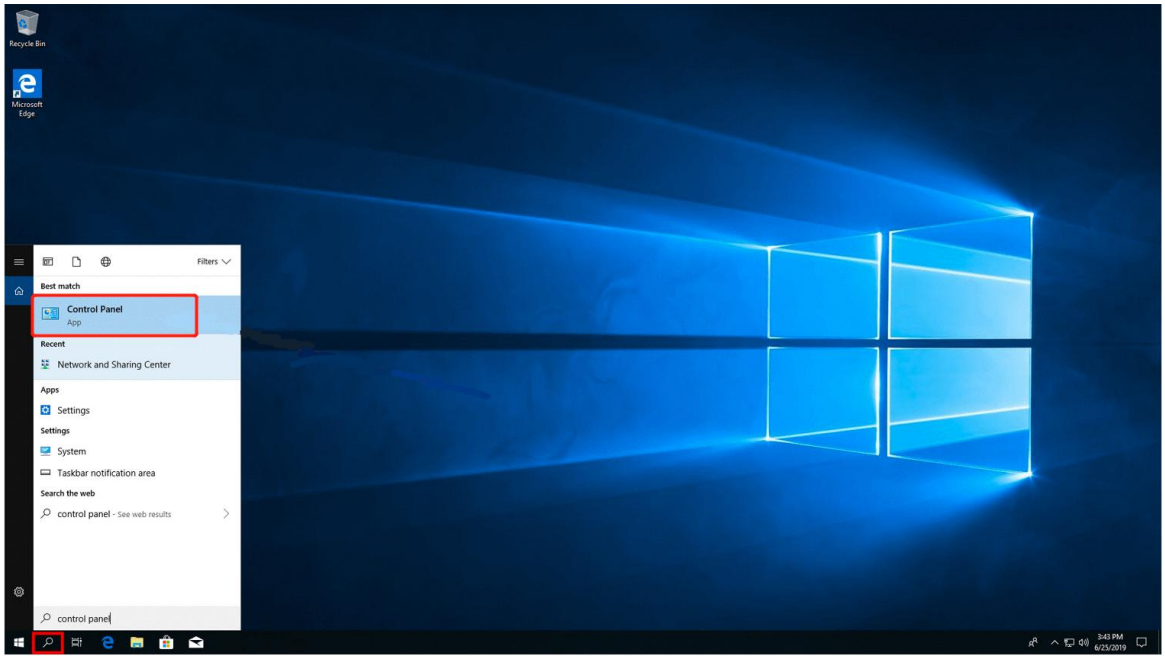


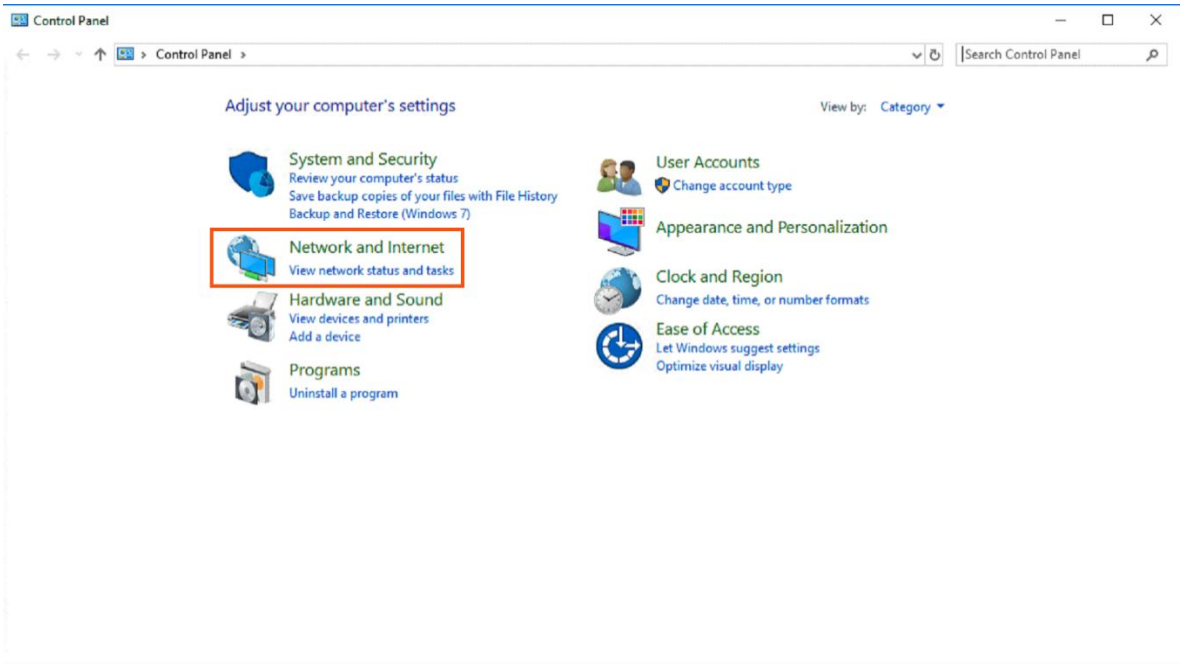
Note

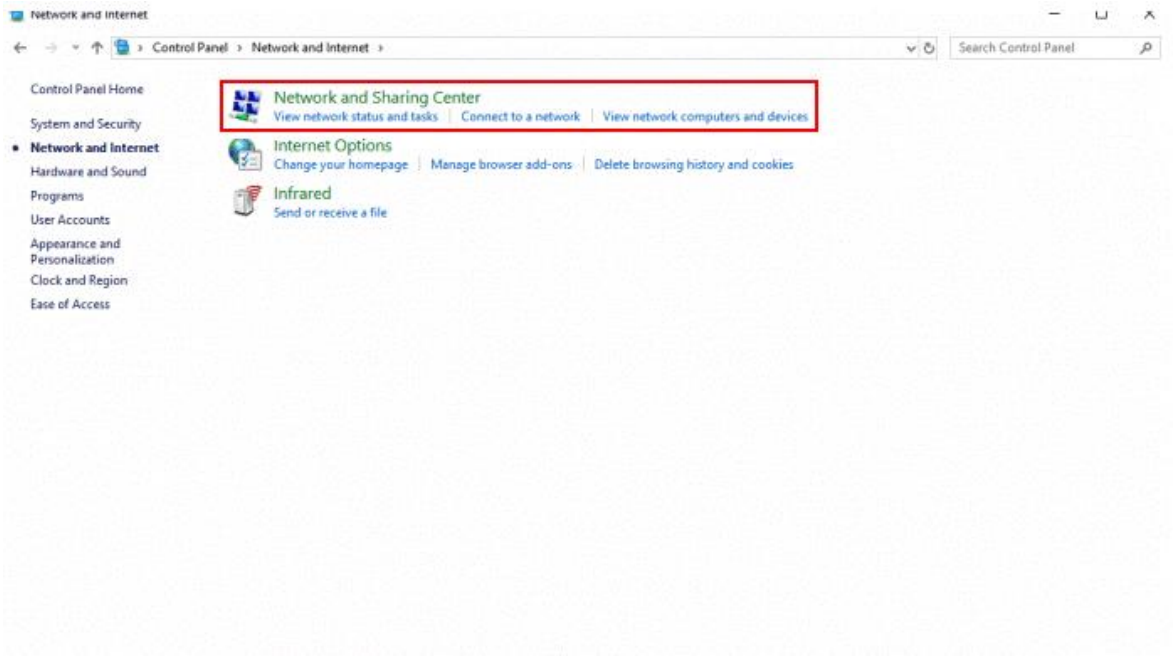
- The local address and the IP range of address pool cannot conflict with the internal network address of the device.
- Local address: Local address is the local virtual IP of the VPN tunnel. The PC can access the server through this address after dialing in.
- Address pool IP range: The IP address pool assigned by the L2TP servers to the clients.
- The PPP link maintenance interval is the default, which refers to the interval at which PPP link maintenance detection messages are sent after PPTP is connected.

On the Clients side (take Windows 10 as example):

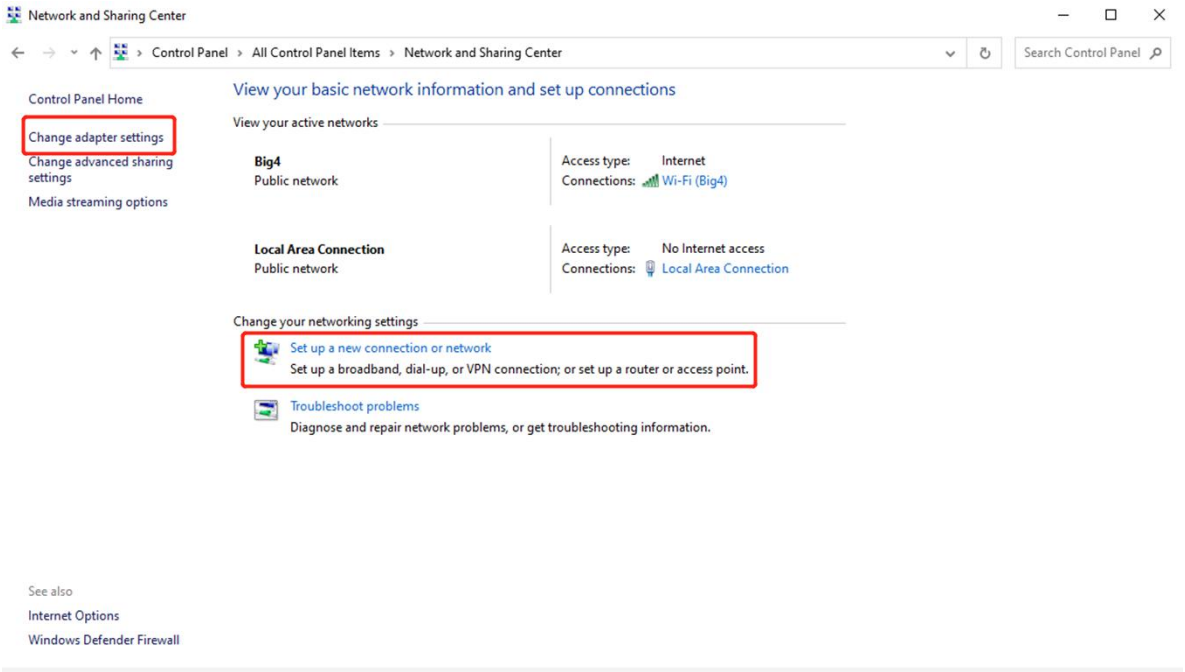
a Enter Control Panel→Network and Internet→Network and Sharing Center

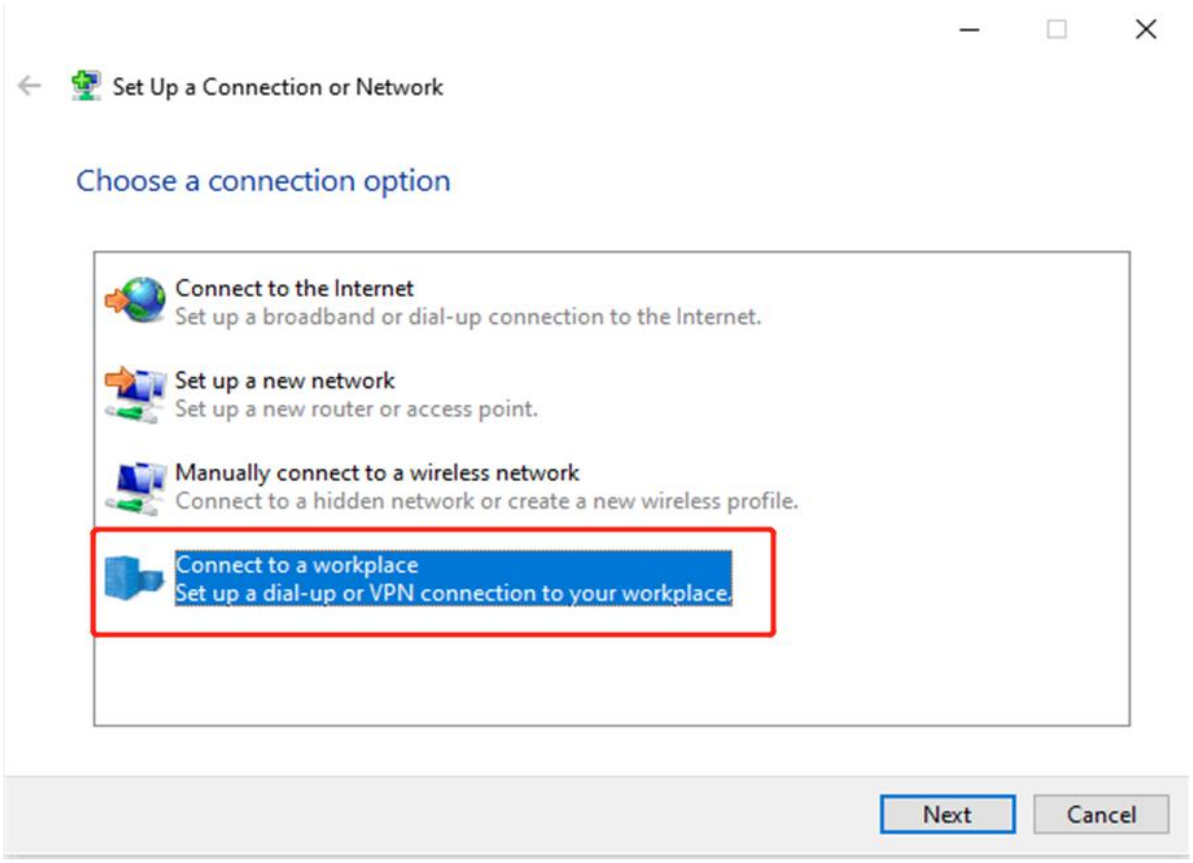


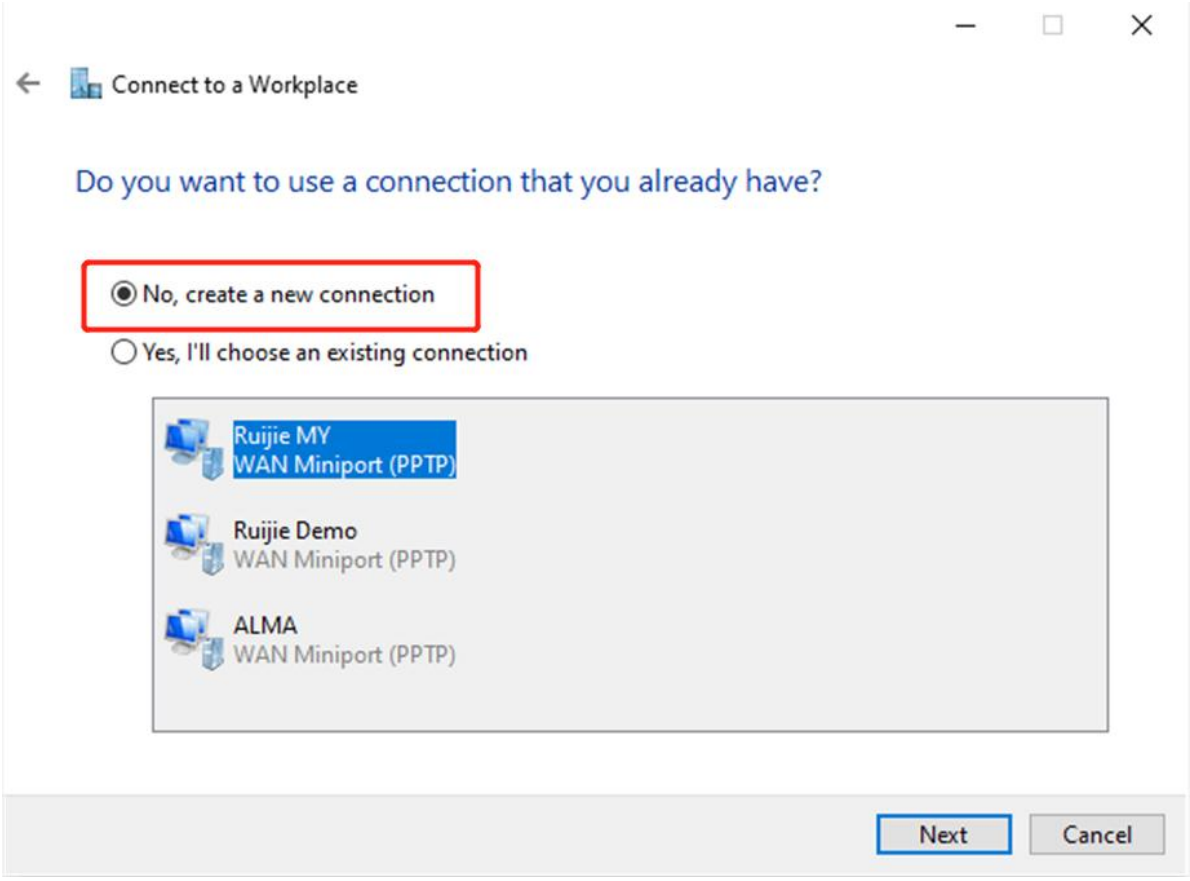


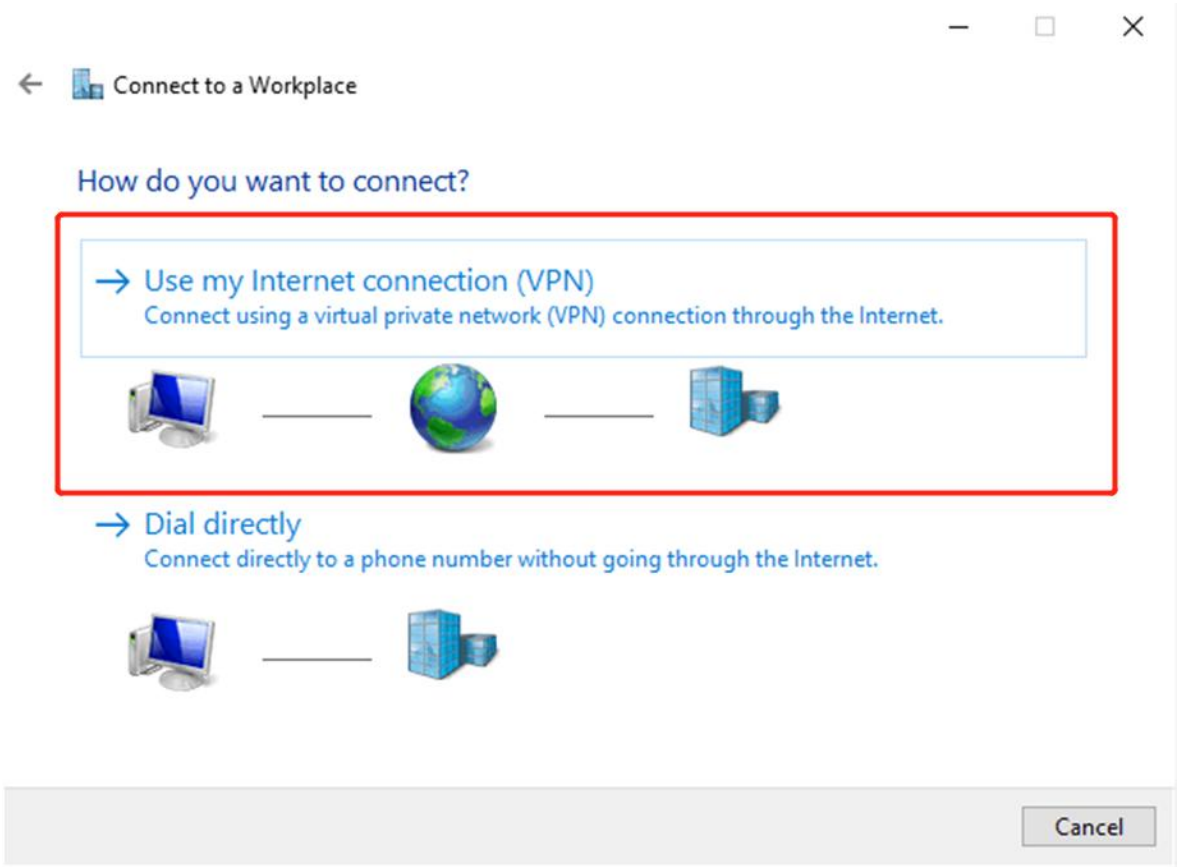


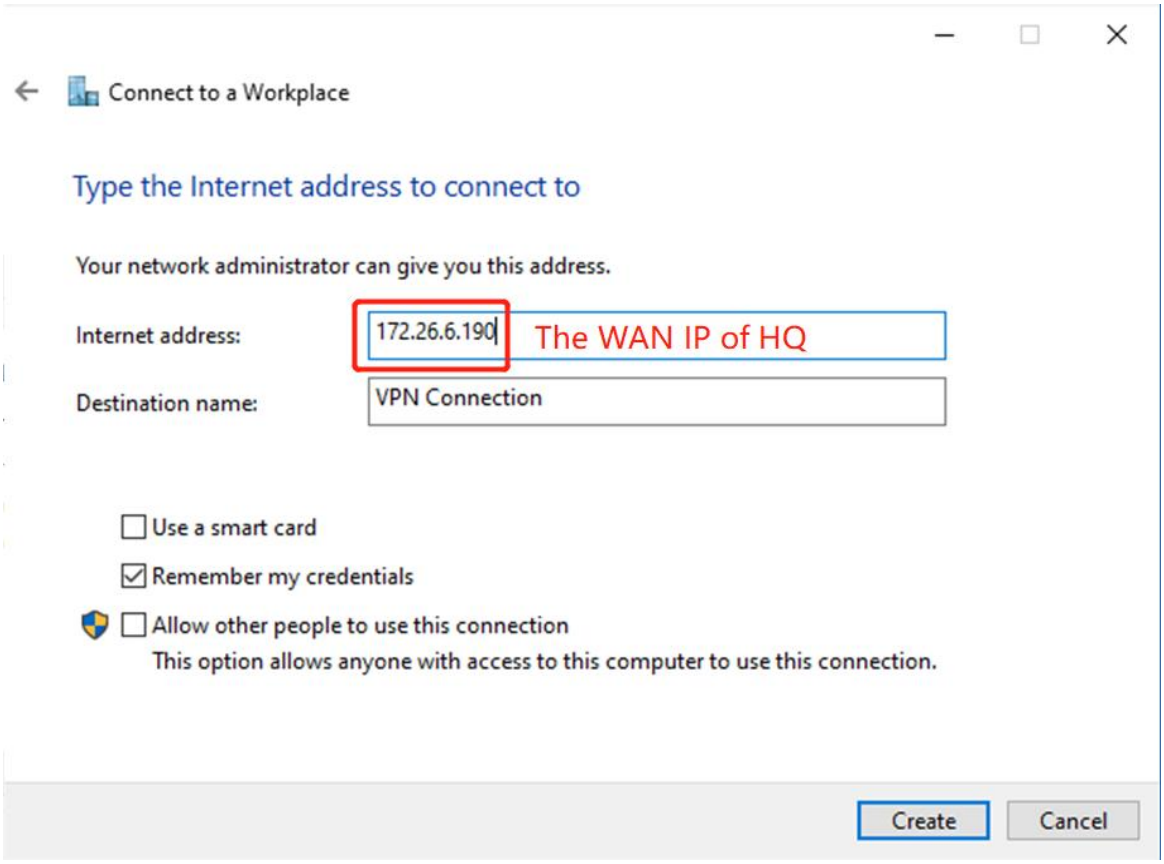
b Configure VPN connection



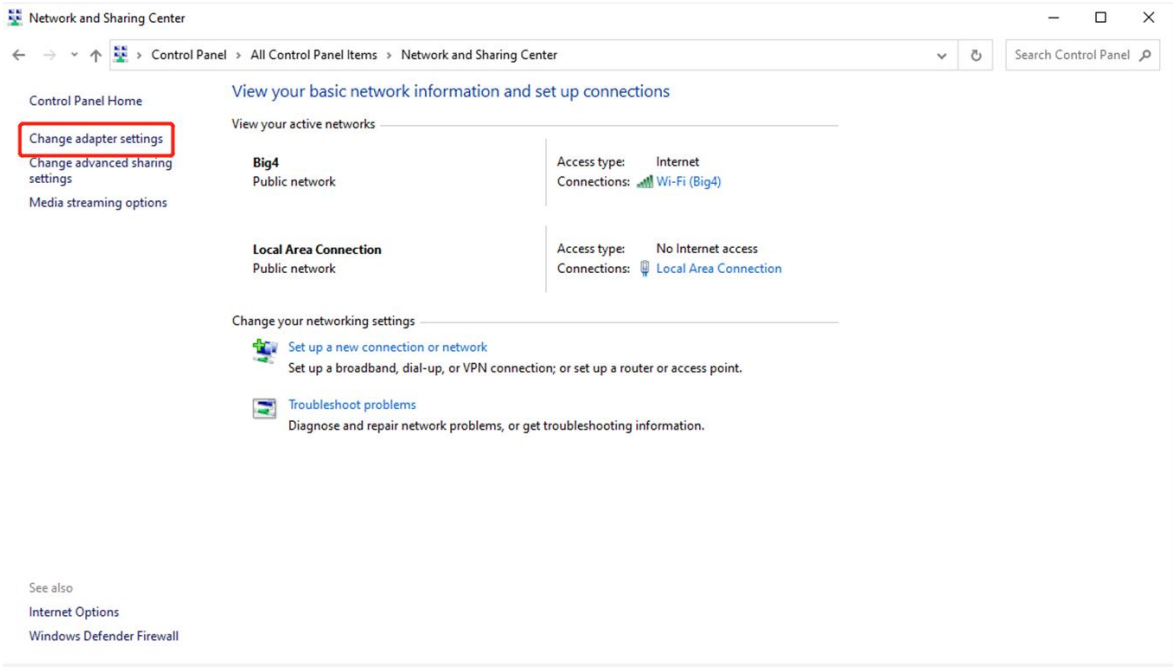

Set Up a Connection or Network
Choose a connection option
Connect to the Internet
Set up a broadband or dial-up connection to the Internet.
Set up a new network
Set up a new router or access point.
Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.
Connect to a workplace
Set up a dial-up or VPN connection to your workplace.
Next
Cancel

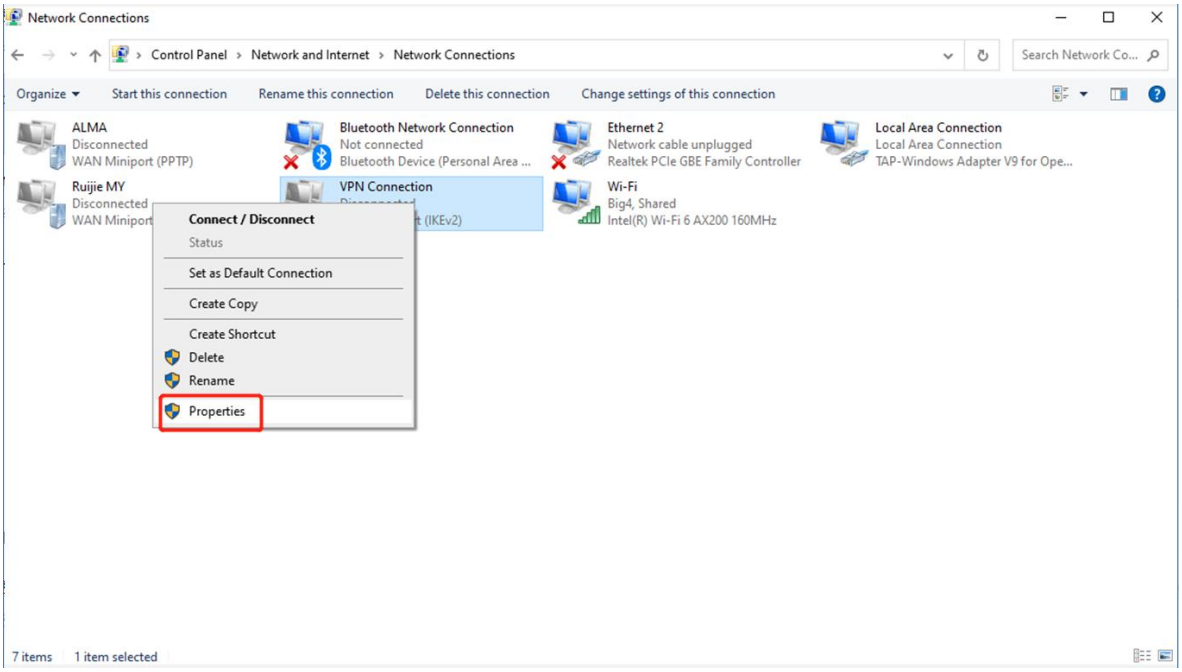

Connect to a Workplace
Do you want to use a connection that you already have?
No, create a new connection
Yes, I'll choose an existing connection
Ruijie MY
WAN Miniport (PPTP)
Ruijie Demo
WAN Miniport (PPTP)
ALMA
WAN Miniport (PPTP)
Next
Cancel

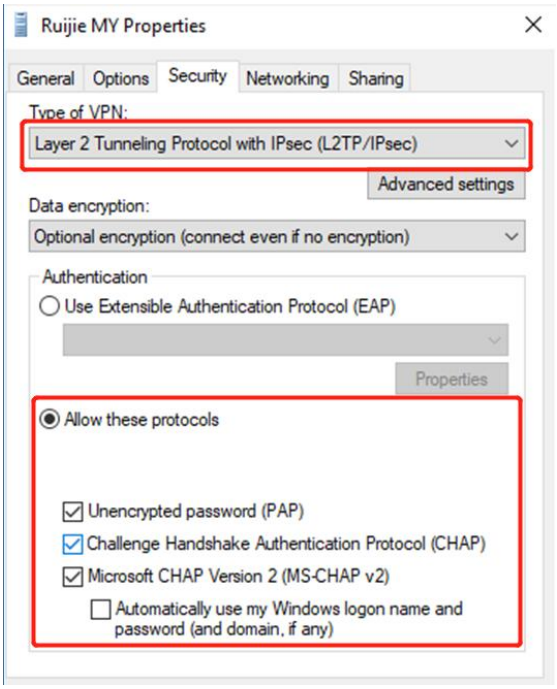

Connect to a Workplace
How do you want to connect?
Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.
Dial directly
Connect directly to a phone number without going through the Internet.
Cancel


Connect to a Workplace
Type the Internet address to connect to
Your network administrator can give you this address.
Internet address:
172.26.6.190
The WAN IP of HQ
Destination name:
VPN Connection
Use a smart card
Remember my credentials
Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.
Create
Cancel

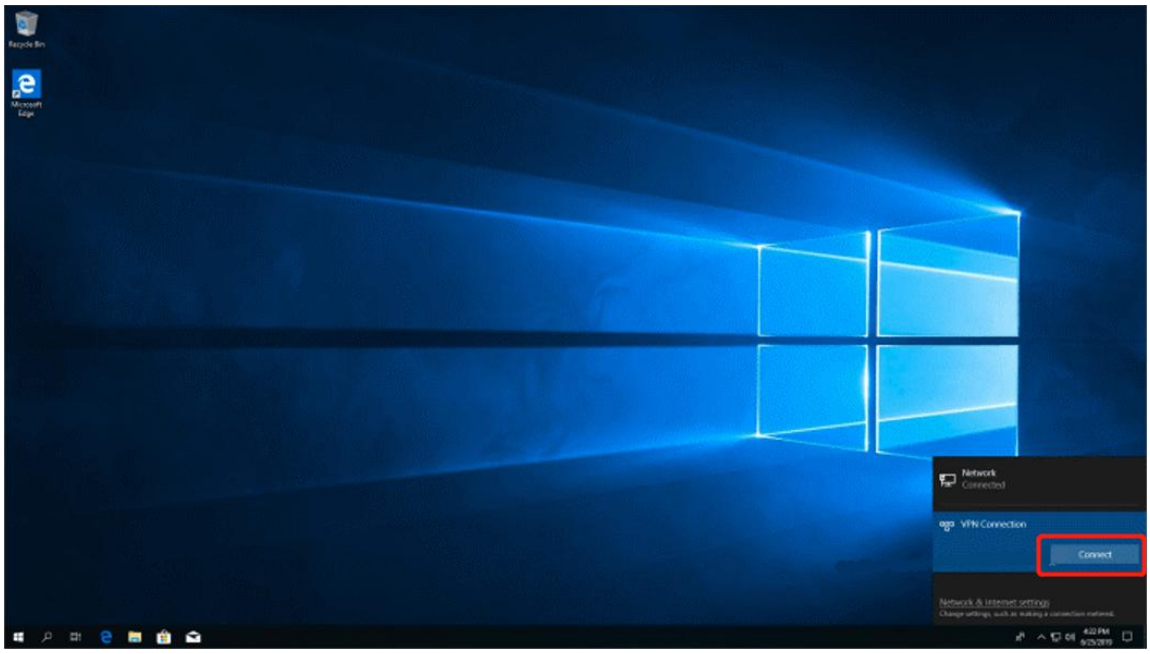
c Change adapter's setting.

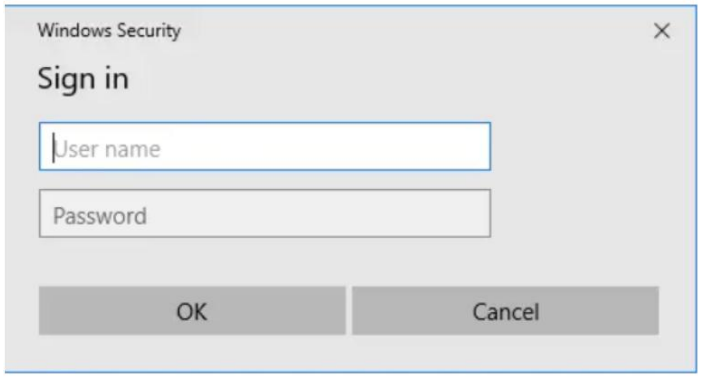


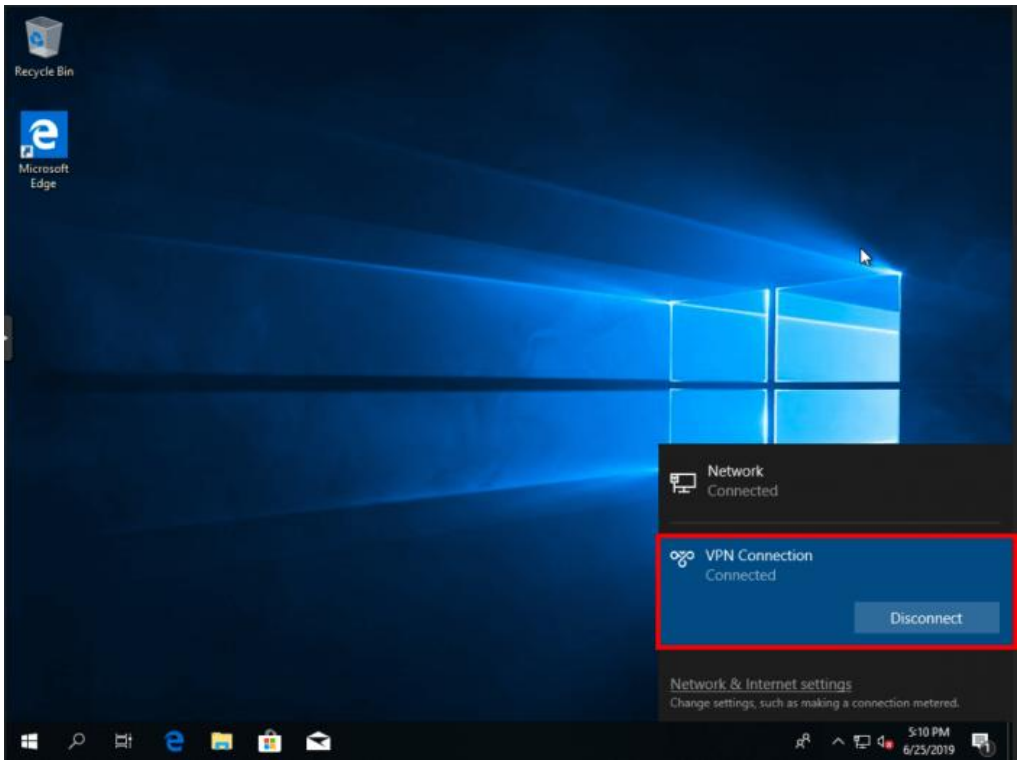




d Check the Status of Connect VPN Connection Status.







e If your PC can't reach HQ internal devices(192.168.10.0/24) after VPN connected. Add the following static route on your PC. The 192.168.100.2 is the PC's IP get from HQ. Then PC can reach HQ internal devices normally.

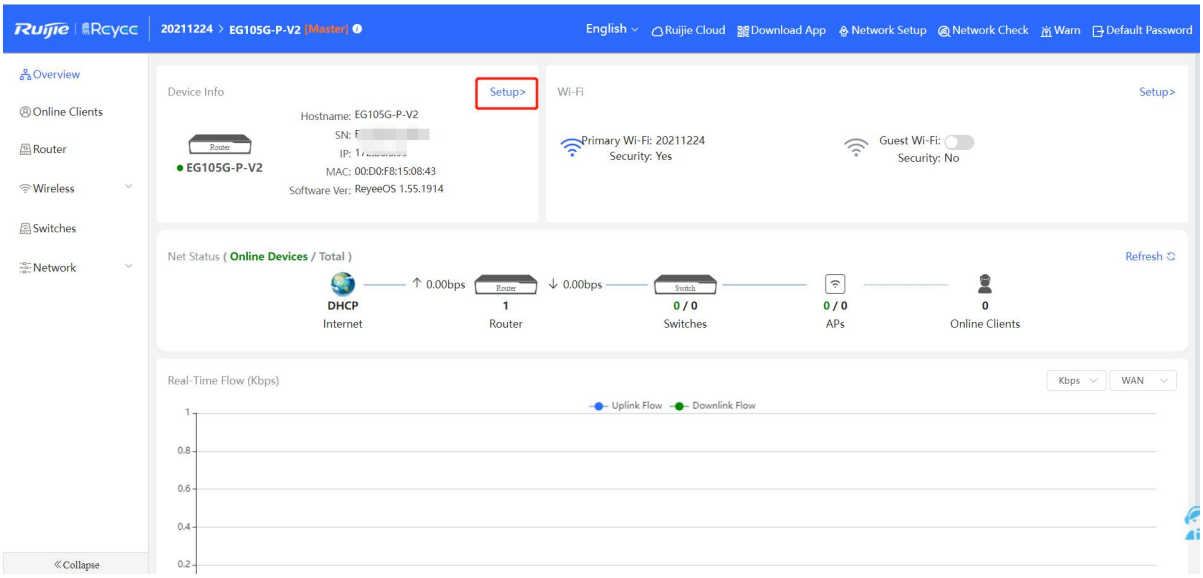
```
C:\Users\Daisy>route add 192.168.168.10.0 mask 255.255.255.0 192.168.100.2
```

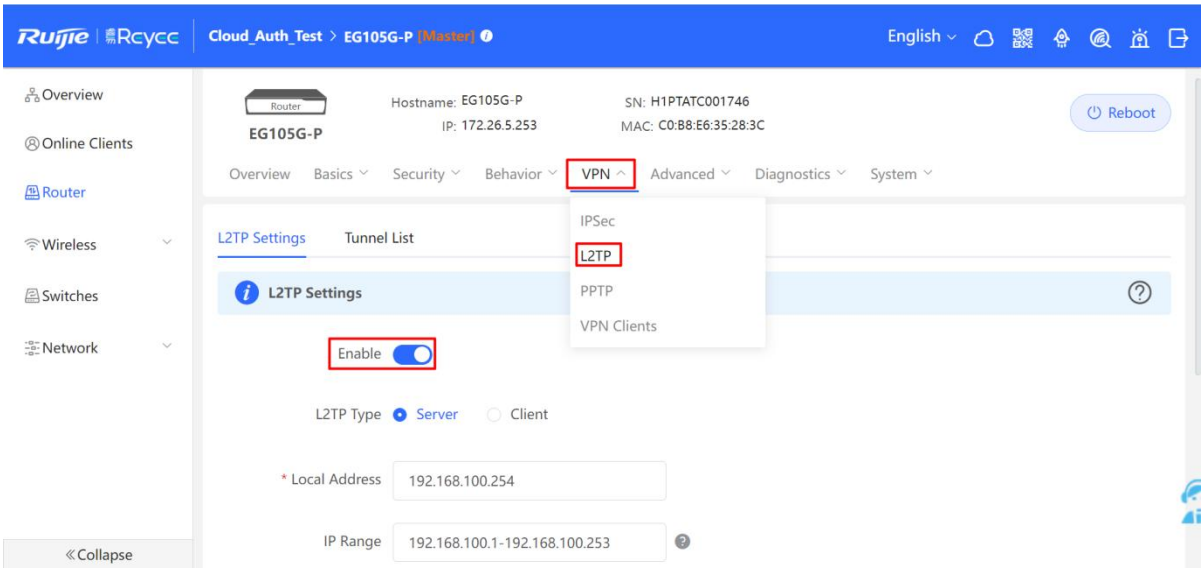
Site to Site Scenario Configuration

On the HQ side:

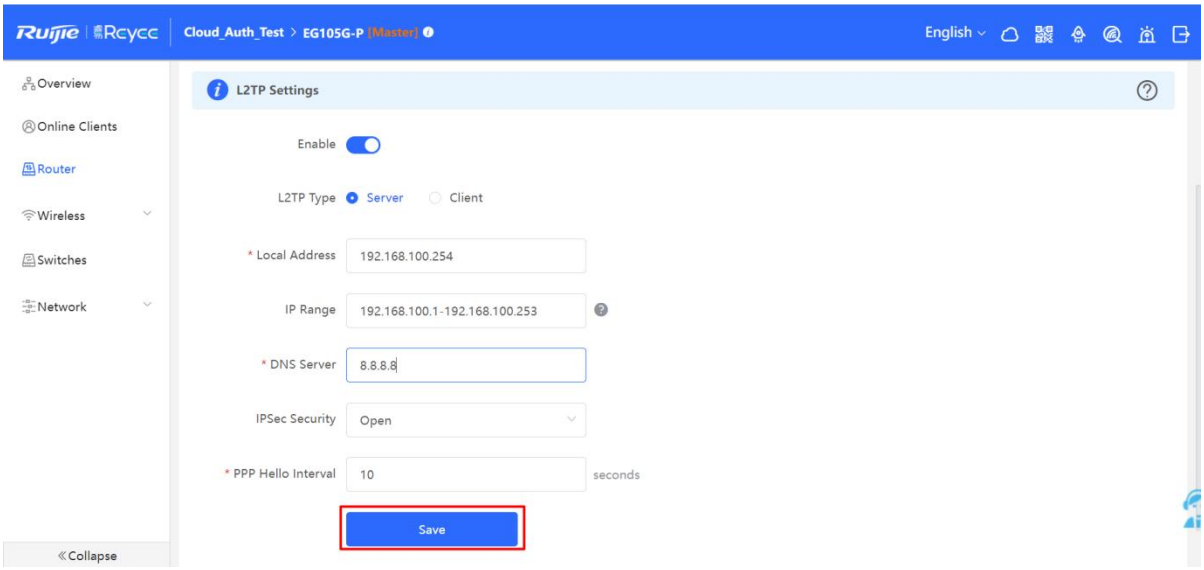
a Log in to Reyee EG by the default IP 192.168.110.1

b Click Setup->VPN->L2TP and then enable L2TP, choose L2TP type as Server.

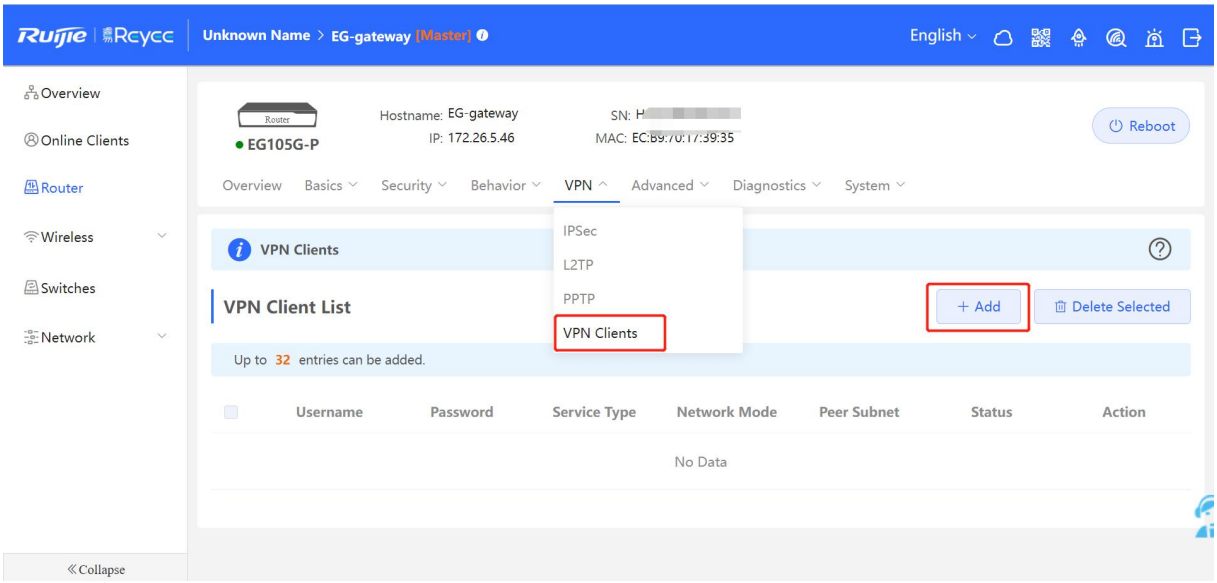


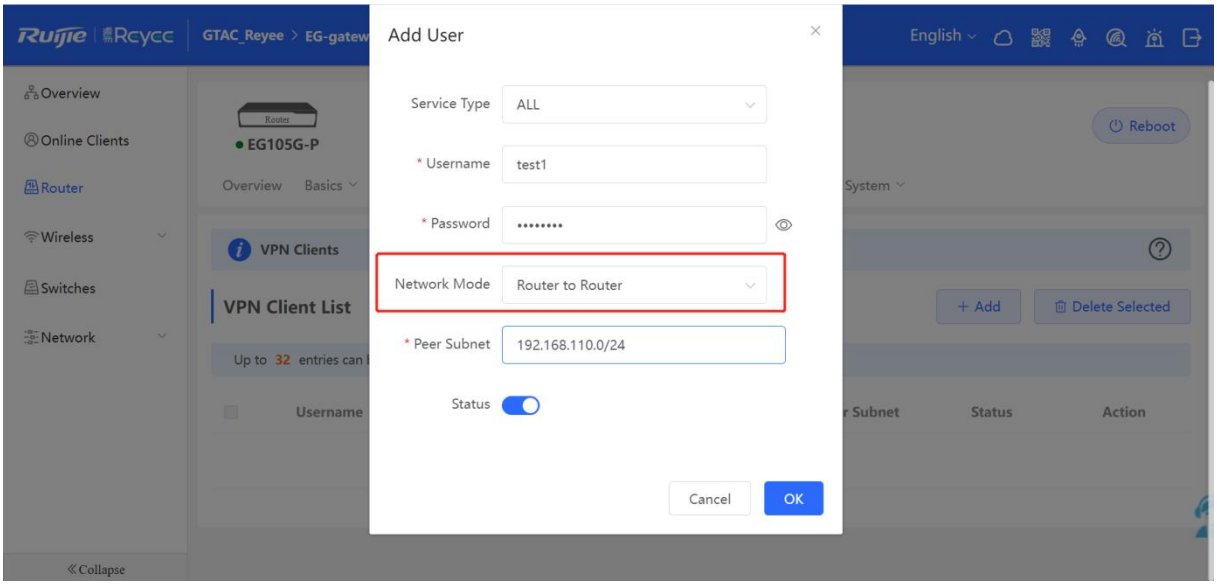


c Configure the L2TP settings and click **Save**.



d Configure VPN client.





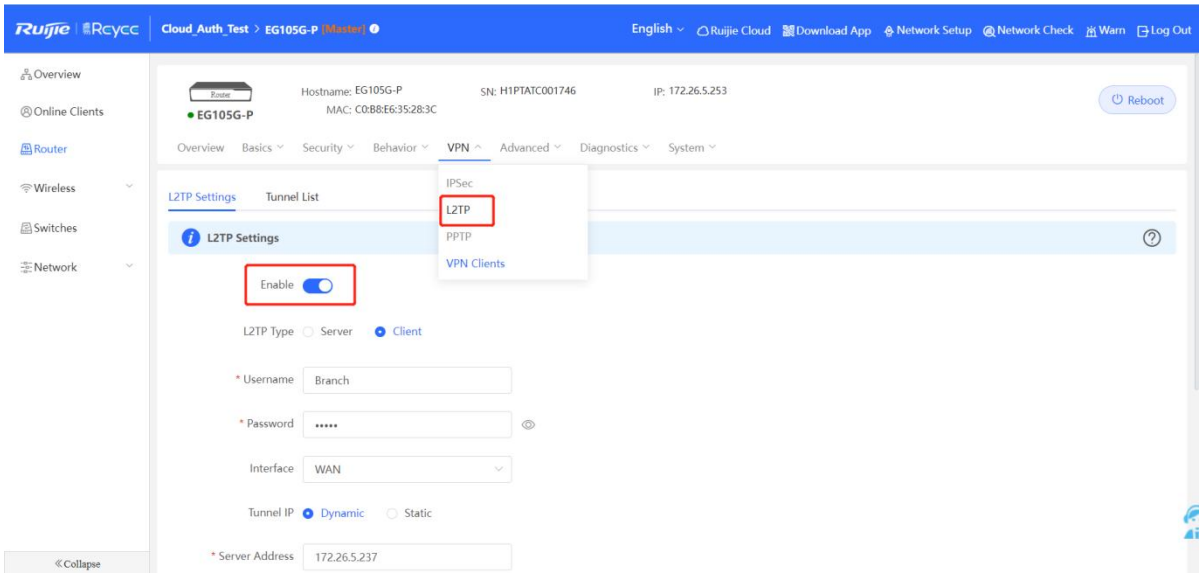
Note

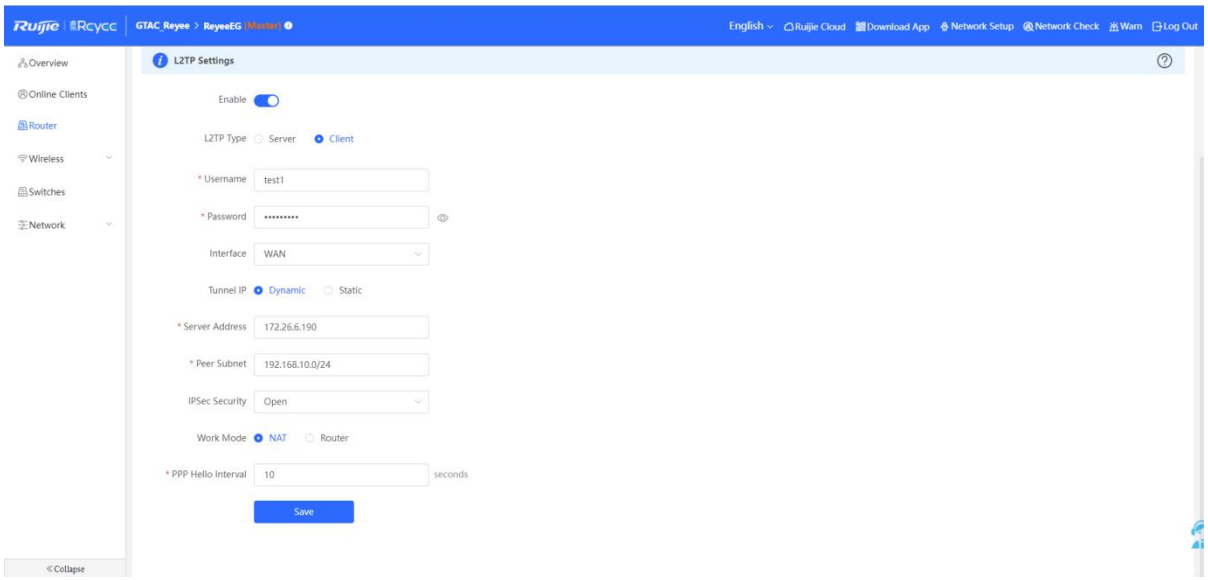
The Peer Subnet is the local IP range of its branch.

On the Branch side:

a Log in to the Reyee EG by the default IP 192.168.110.1

b Click Setup->VPN->L2TP and then enable L2TP, choose L2TP type as Client.

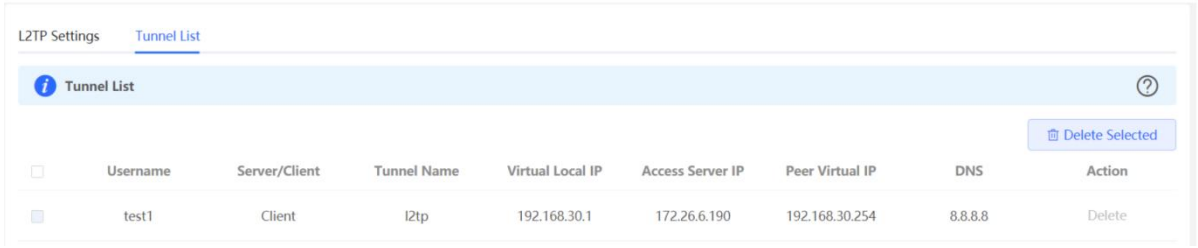




Note

- Work Mode description：
- NAT: NAT the incoming L2TP packets (Replace the source IP address with the local virtual IP address).
- Router: Only route the incoming L2TP packets.

c Check the VPN connection status



4.1.8.3 IPsec VPN

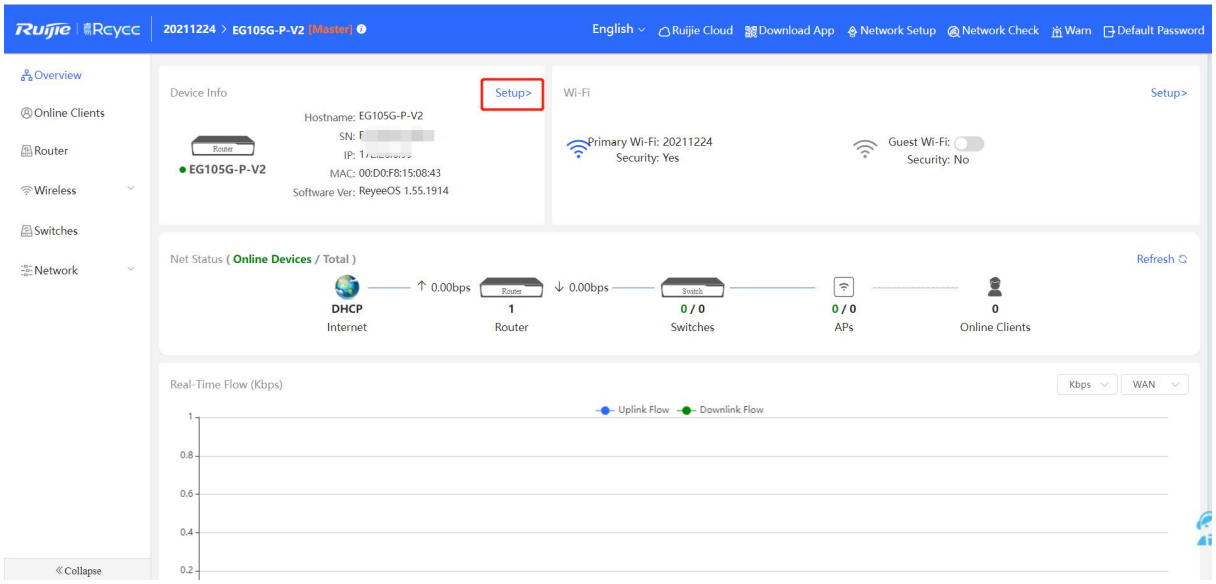
IPsec VPN is used for Site to Site scenario. For example, three branches of a company are distributed in three different places of the internet. And every branch uses a gateway to establish tunnels with everyone, and the data between the corporate intranets (several PCs) is securely interconnected through the IPSec VPN tunnel established by these gateways.

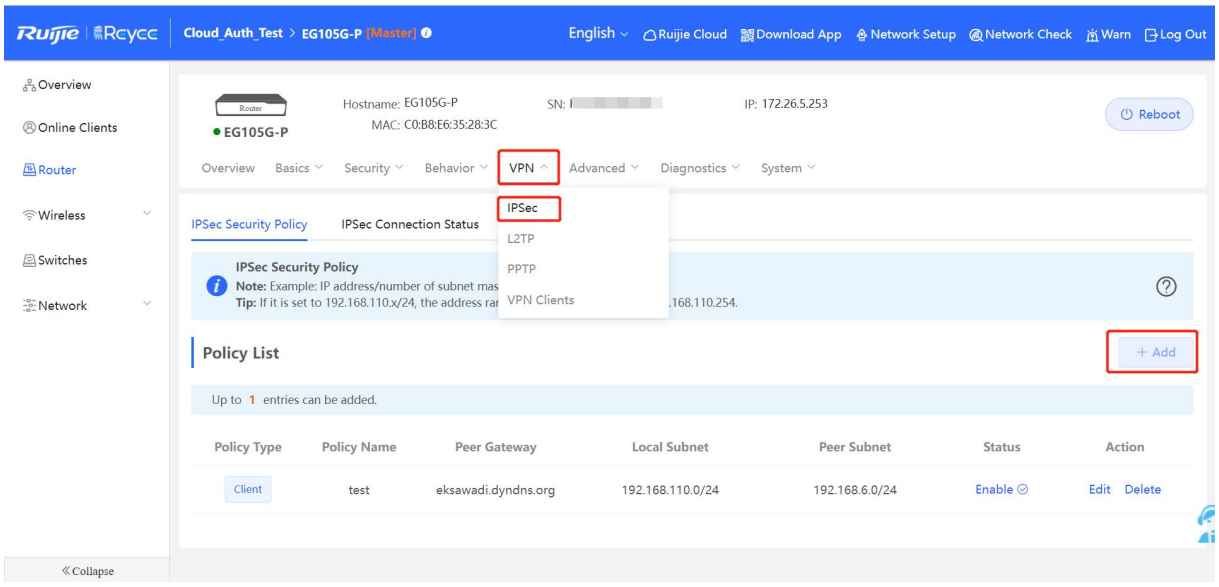
Site to Site Scenario Configuration

On the HQ side:

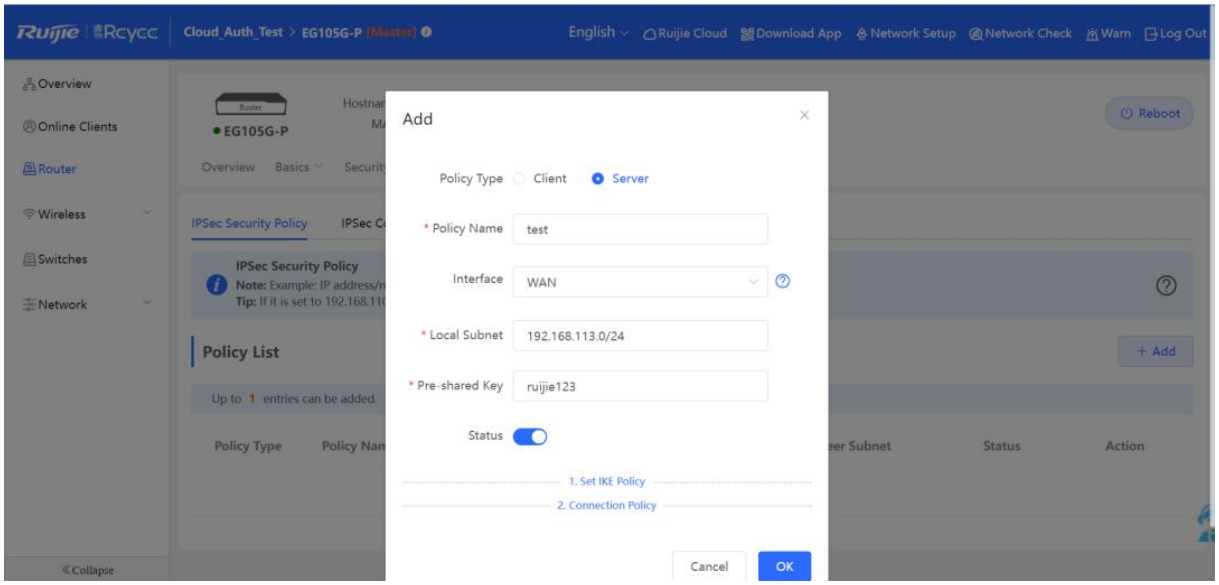
a Log in to Reyee EG by the default IP 192.168.110.1.

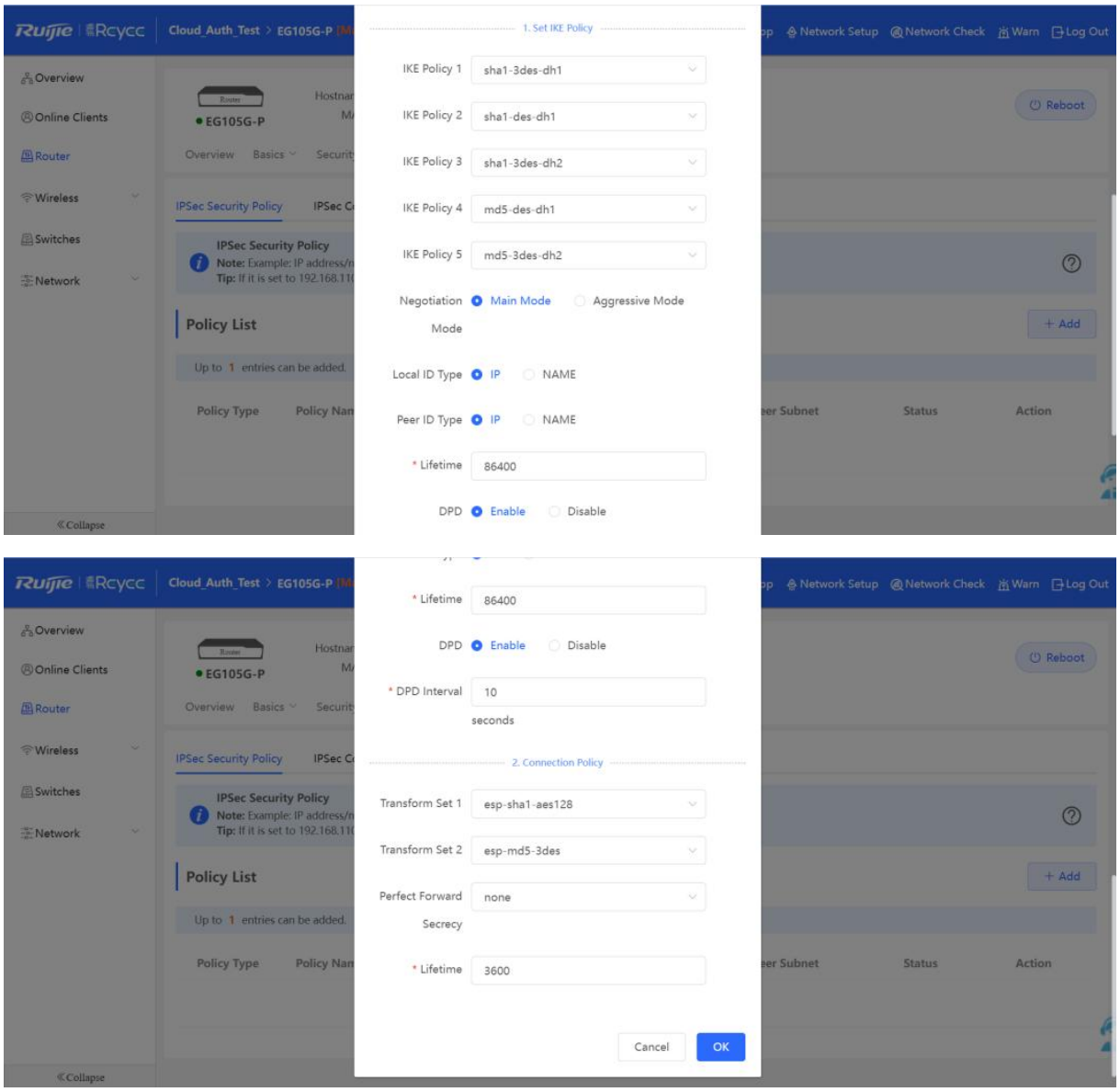
b Click Setup > VPN > IPSec > Add the policy.





c Configure the IPsec VPN Security Policy.

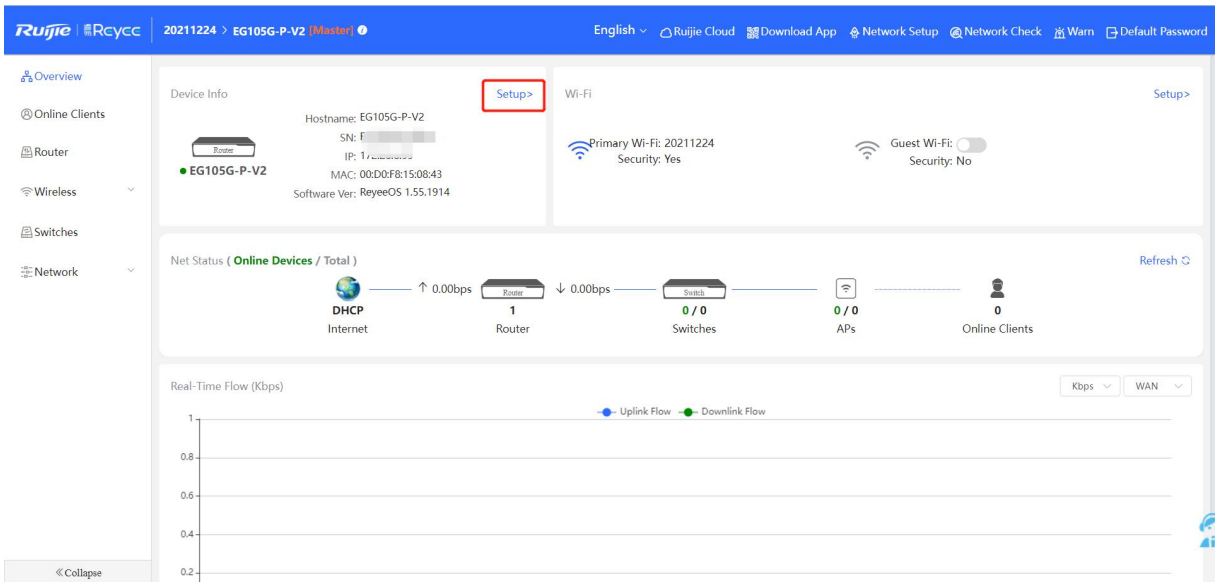


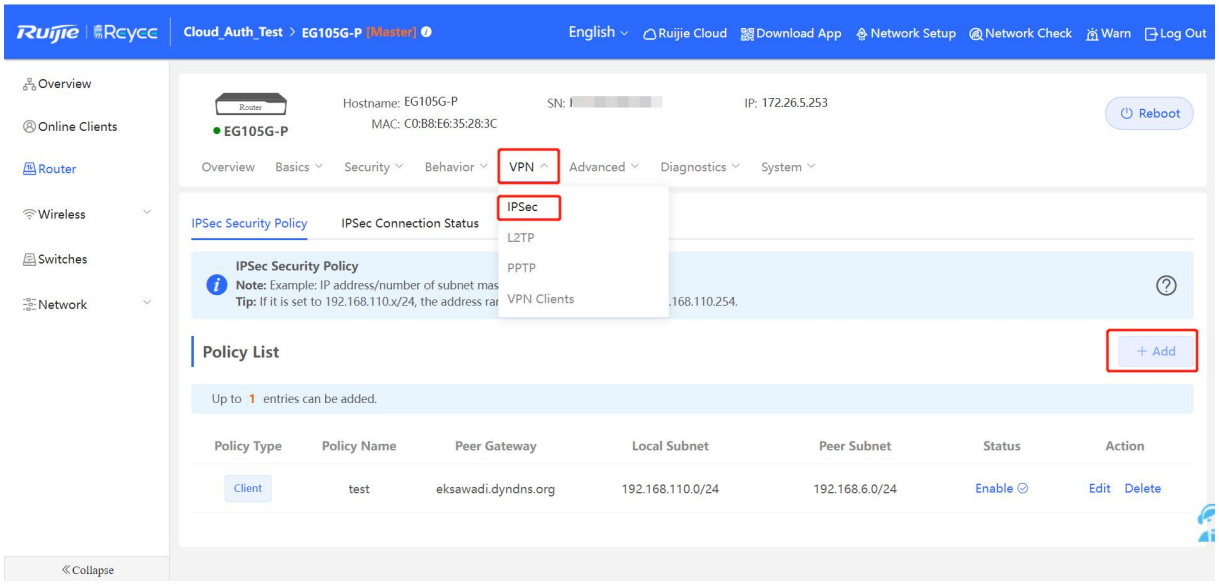


On the Branch side:

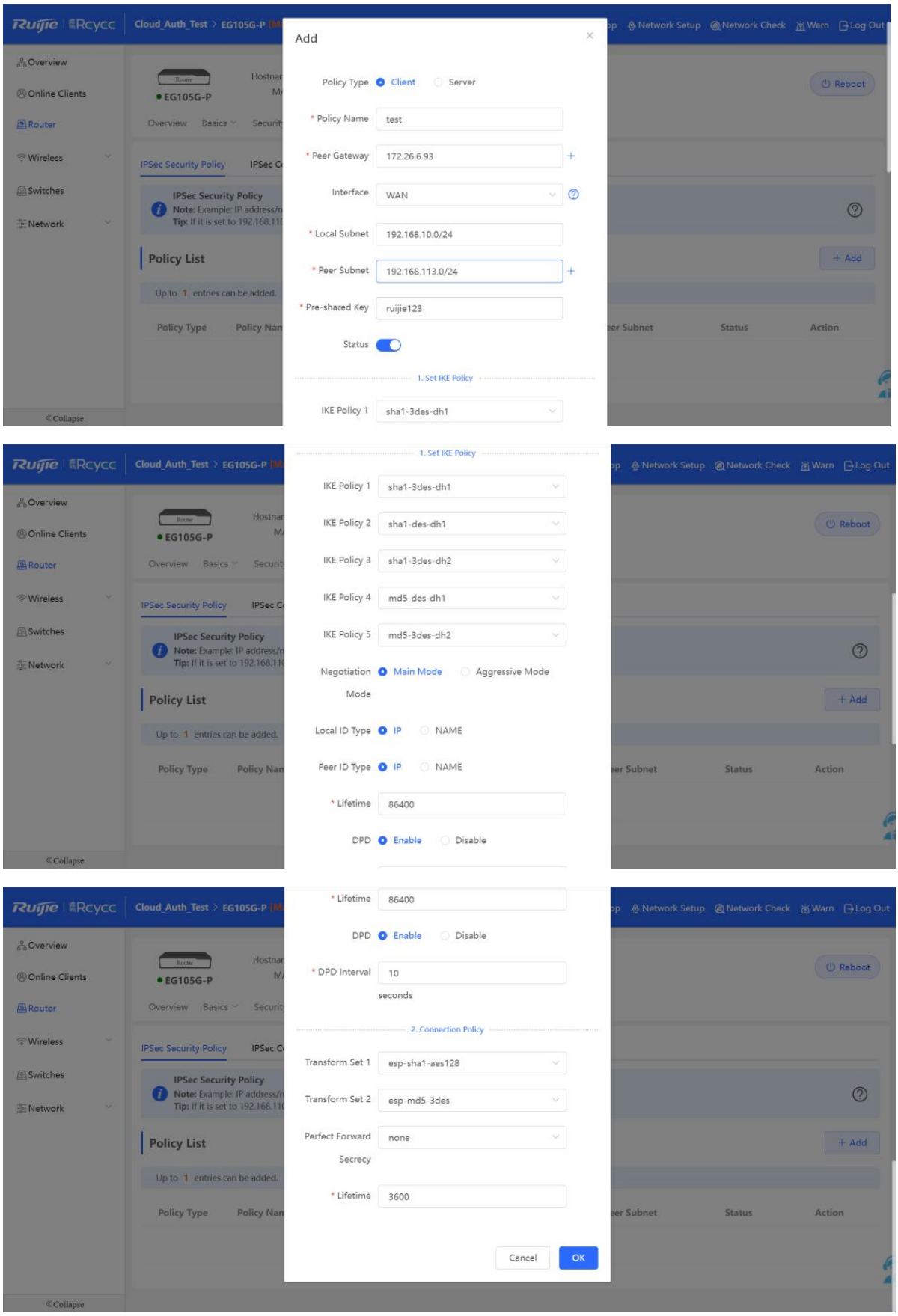
a Log in to the Reyee EG by the default IP 192.168.110.1.

b Click Setup > VPN > IPSec and then Add the policy.

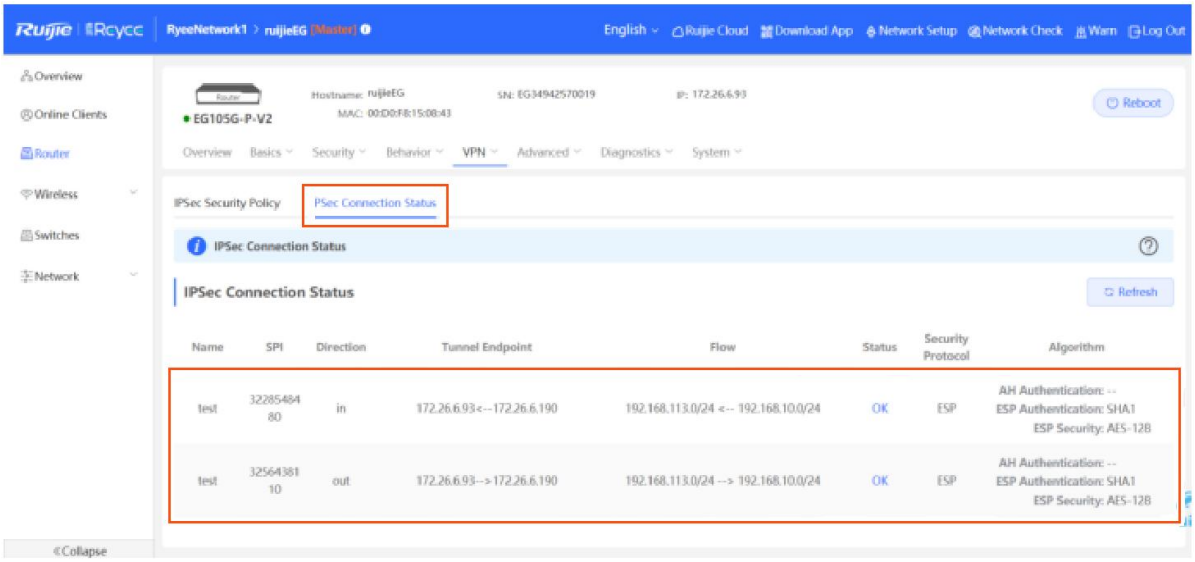




c Configure the IPSec Security Policy, make sure the IKE Policy and Connection Policy are same on both side.



d Check IPSec Connection Status.



Note

- If you HQ EG has no public IP configured under other external devices, you need to configure port mapping on external devices and configure **Local ID Type** as **NAME** on HQ and Branches.

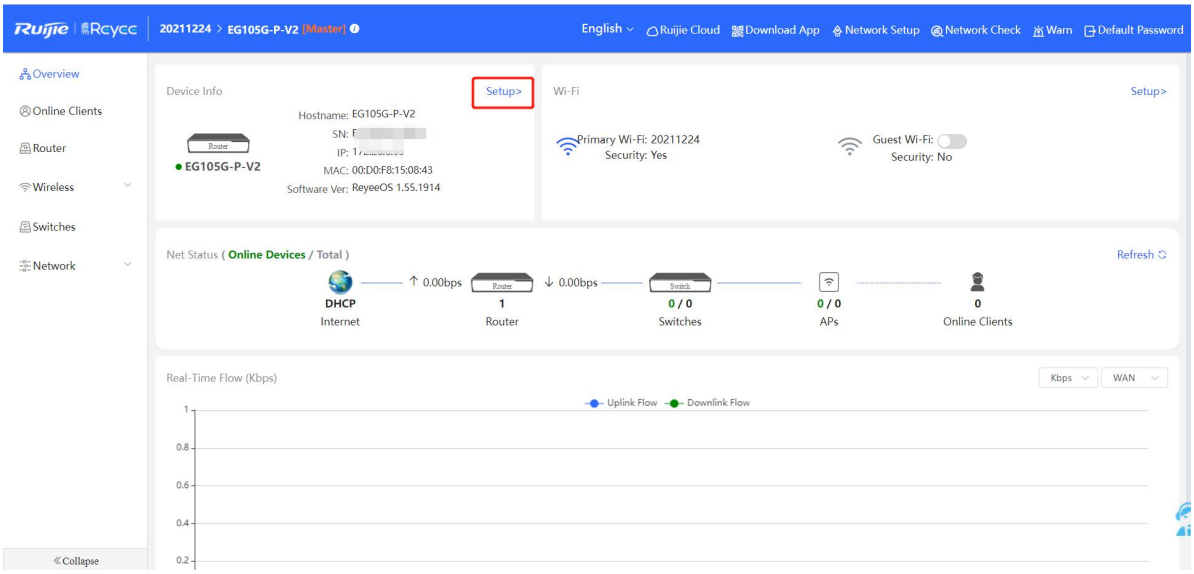
4.1.8.4 L2TP Over IPsec VPN

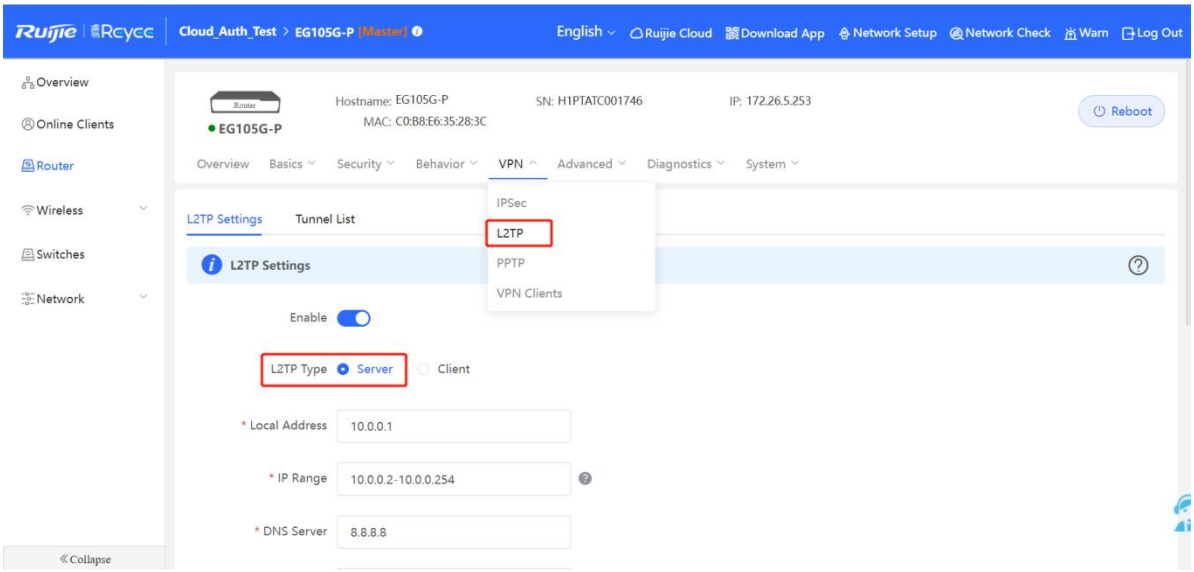
L2TP over IPsec VPN usually is used for the Site to Site scenario and Client to Site scenario. For example, three branches of a company are distributed in three different places of the Internet, and everyone uses a gateway to establish tunnels with each other, and the data between the corporate intranets (several PCs) is securely interconnected through the L2TP over IPSec VPN tunnel established by these gateways, the staff who work at home can access company data through L2TP over IPSec VPN tunnel too.

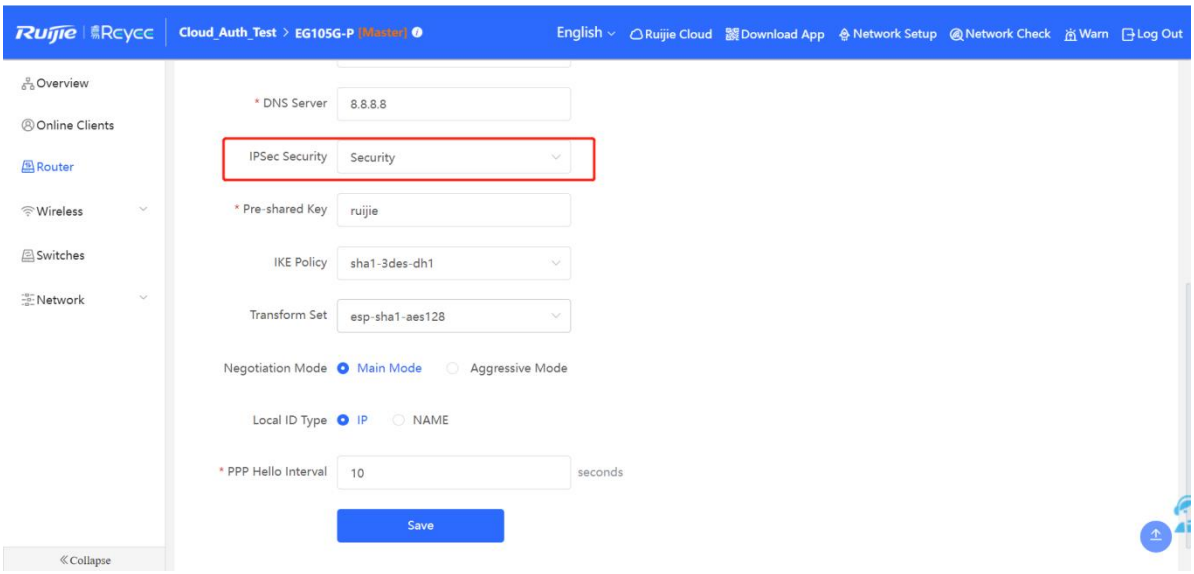
On the HQ side:

a Log in to Reyee EG by the default IP 192.168.110.1.

b Click **Setup->VPN->L2TP** and choose **IPsec Security.**



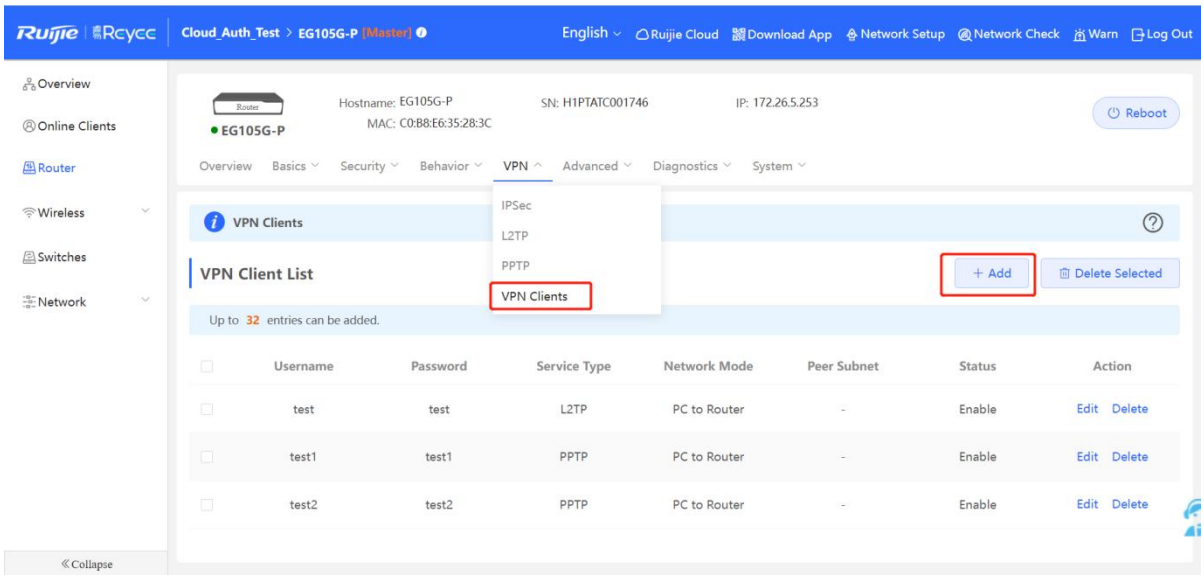


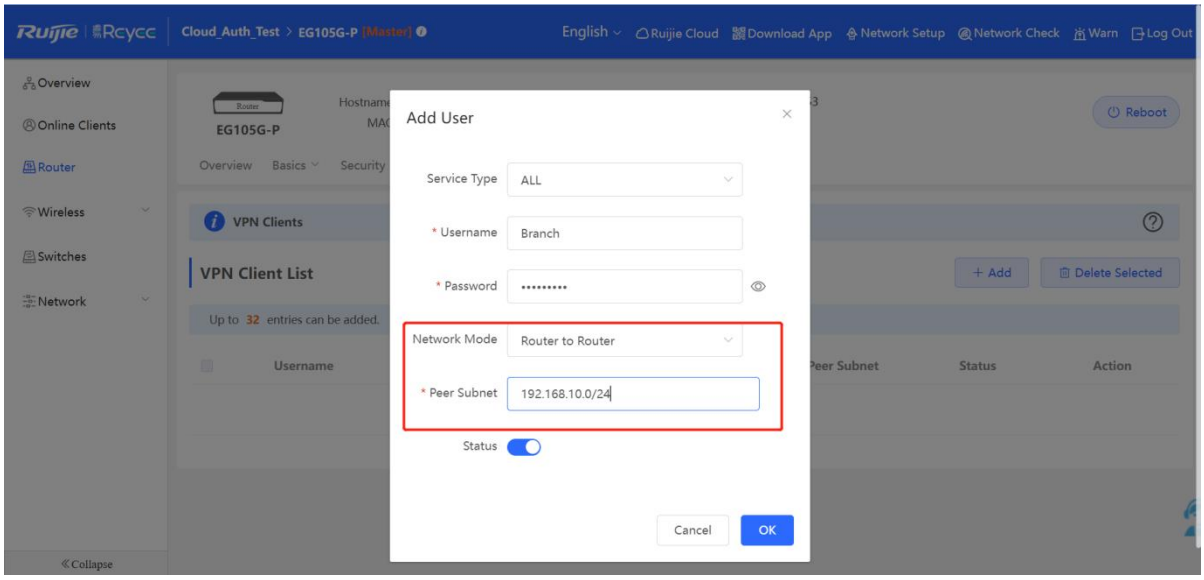


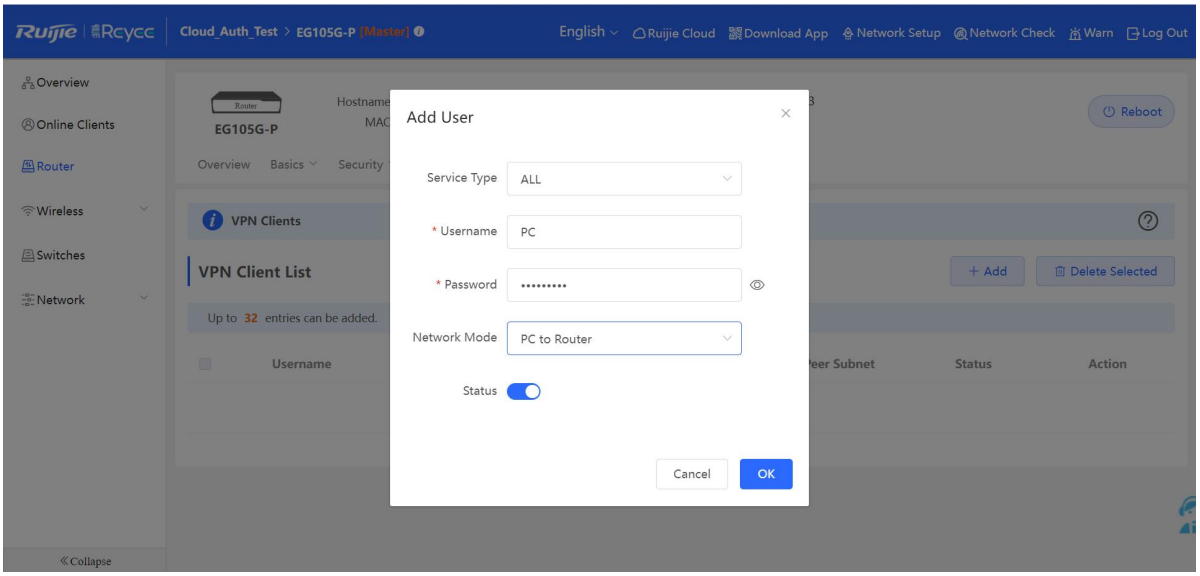
Note

- PPP Hello Interval：The interval between hello messages on PPP over IPsec connection
- IPsec Auth: Whether to encrypt the tunnel or not.
- Pre-shared Key：A pre-shared key is required for IPsec encryption.
- Local ID Type：When your HQ WAN port set with public IP, you can choose IP, when your HQ WAN port set with private IP, you need to choose name and set DMZ on external device.

c Configure VPN clients and set clients, one is for branch EG, another is for PC.


Cloud_Auth_Test > EG105G-P [Master]
English
Ruijie Cloud
Download App
Network Setup
Network Check
Warn
Log Out
Overview
Online Clients
Router
Wireless
Switches
Network
EG105G-P
Hostname: EG105G-P
MAC: C0:B8:E6:35:28:3C
SN: H1PTATC001746
IP: 172.26.5.253
Reboot
Overview
Basics
Security
Behavior
VPN
Advanced
Diagnostics
System
IPSec
L2TP
PPTP
VPN Clients
VPN Clients
VPN Client List
+ Add
Delete Selected
Up to 32 entries can be added.
Username
Password
Service Type
Network Mode
Peer Subnet
Status
Action
test
test
L2TP
PC to Router
Enable
Edit
Delete
test1
test1
PPTP
PC to Router
Enable
Edit
Delete
test2
test2
PPTP
PC to Router
Enable
Edit
Delete
Collapse


Add User
Service Type
ALL
* Username
Branch
* Password
Network Mode
Router to Router
* Peer Subnet
192.168.10.0/24
Status
Cancel
OK


Add User
Service Type
ALL
* Username
PC
* Password
Network Mode
PC to Router
Status
Cancel
OK

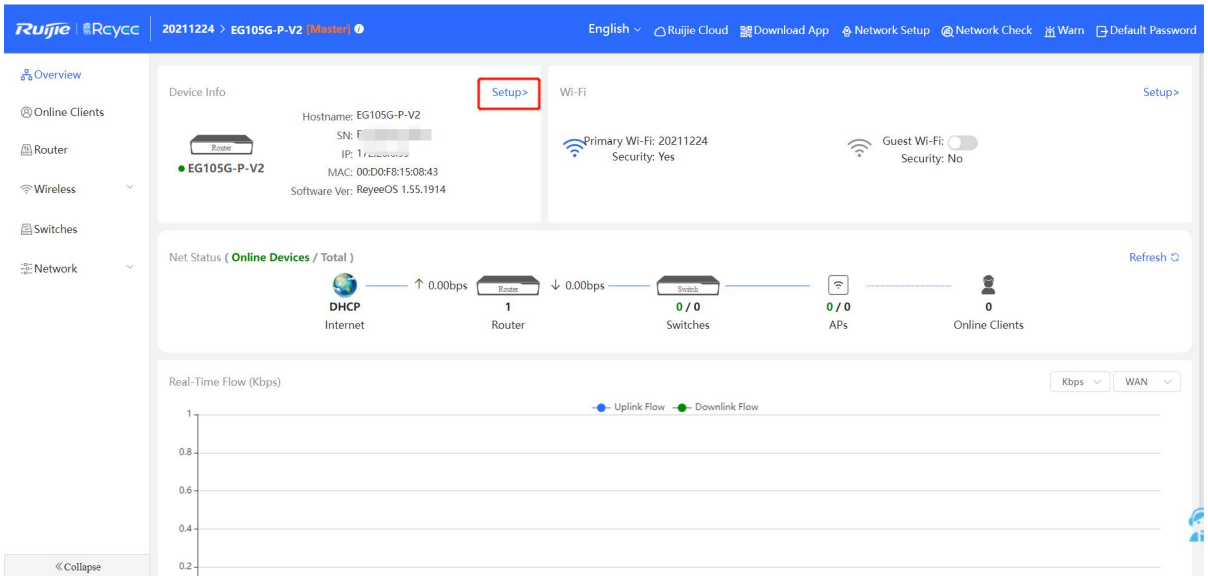
Note

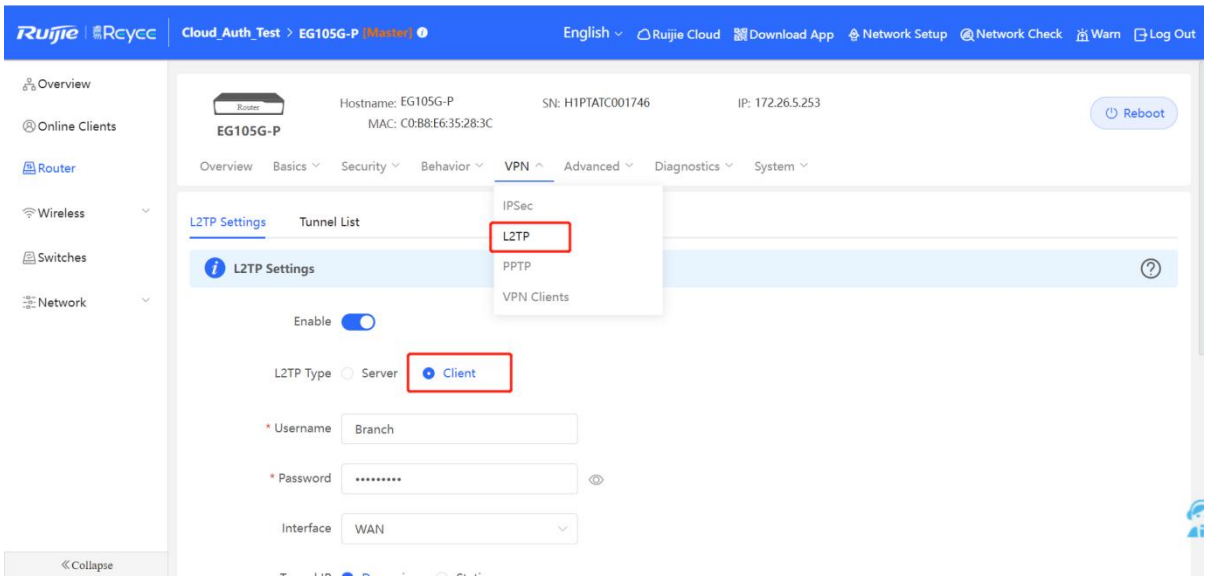
- PC-to-Router: PC-to-router connection is established between a PC and an terminal
- Router-to-Router: Router-to-router VPN typically creates a direct, unshared and secure connection between two terminals.

On the Branch side:

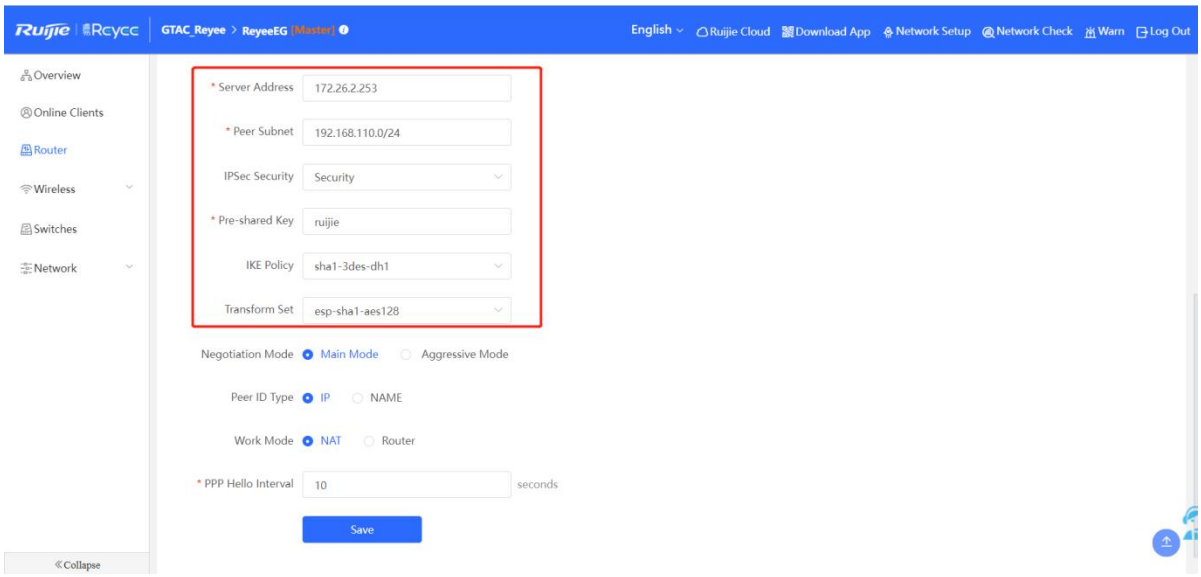
a Log in to the Reyee EG by the default IP 192.168.110.1.

b Click **Setup->VPN->L2TP** and then enable **IPsec Auth**.

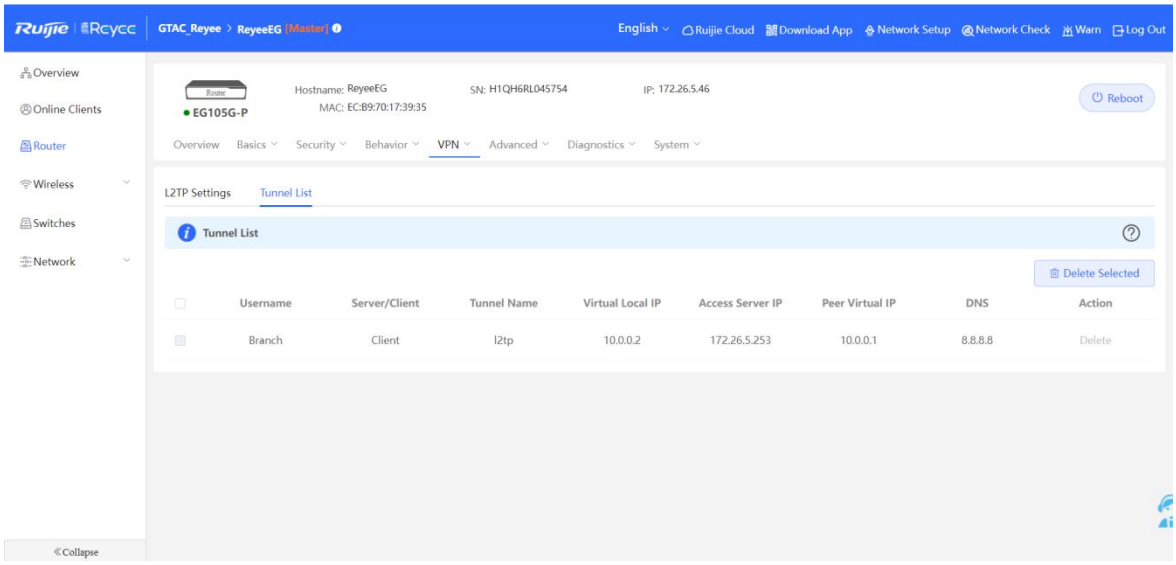




c Configure the IPsec Security, make sure the pre-share password, IKE Policy and Transform Set is the same on both side.

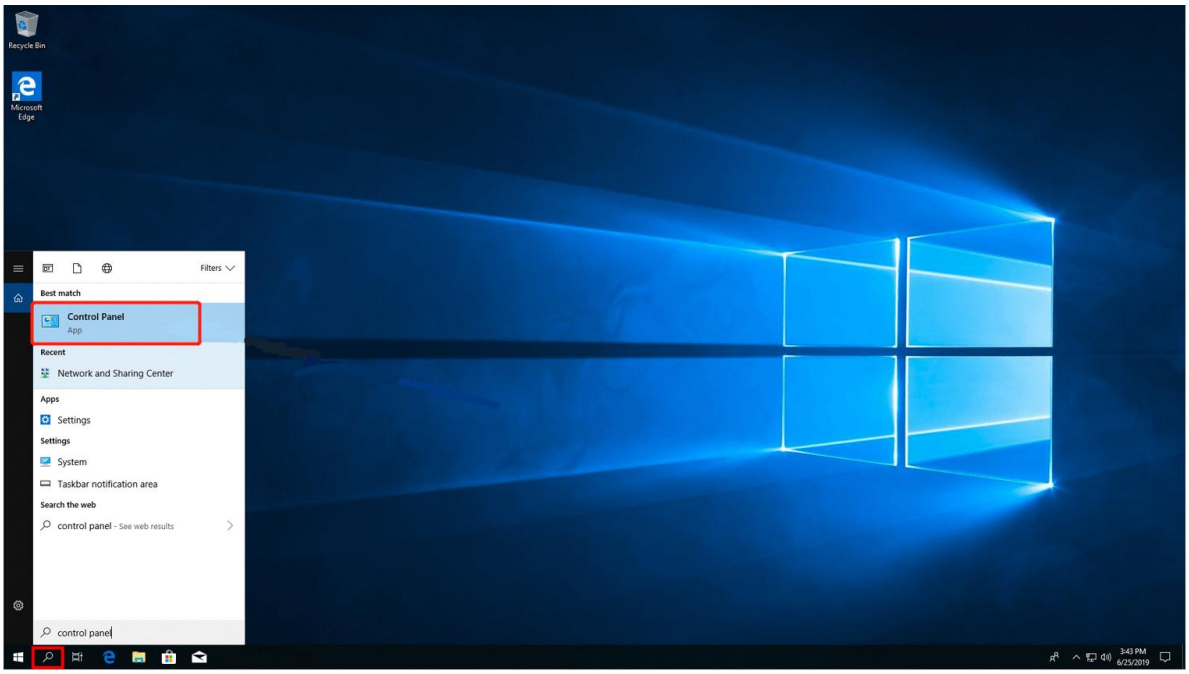


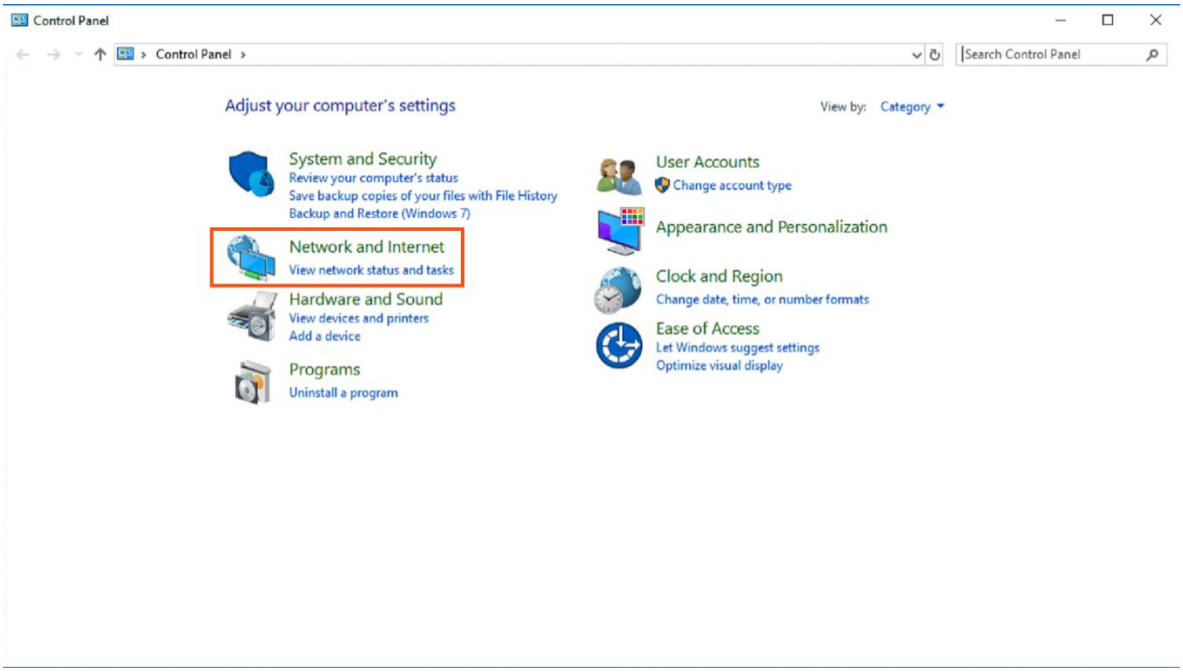
d Check the status of L2TP over IPsec Connection.

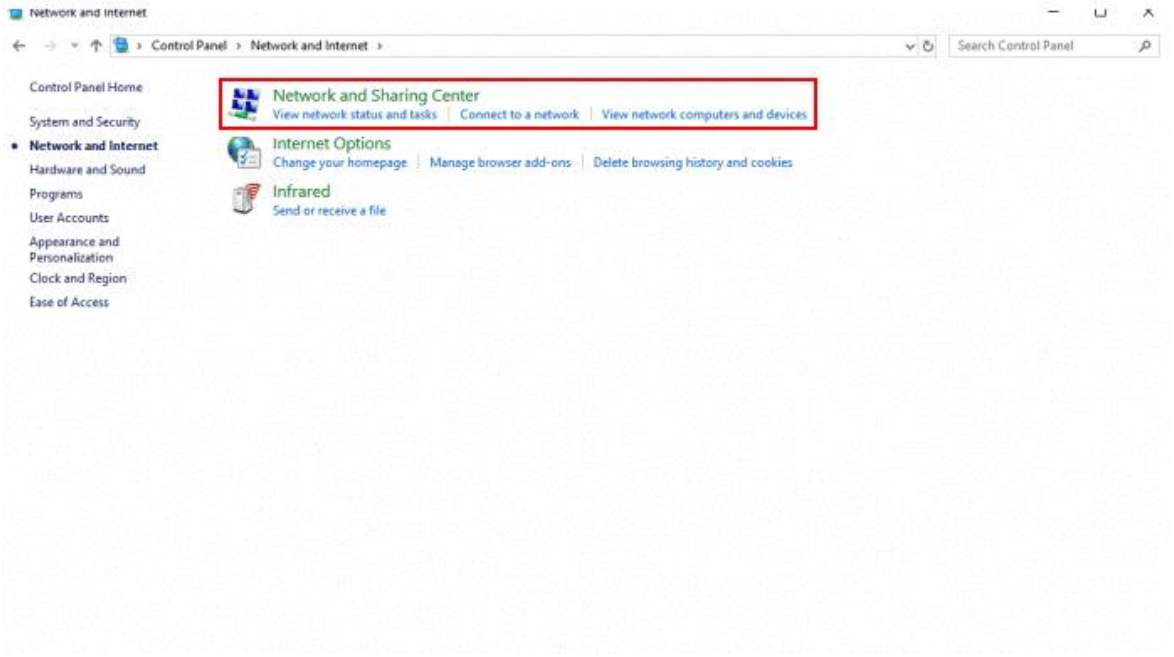


On the Clients side (take Windows 10 as example):

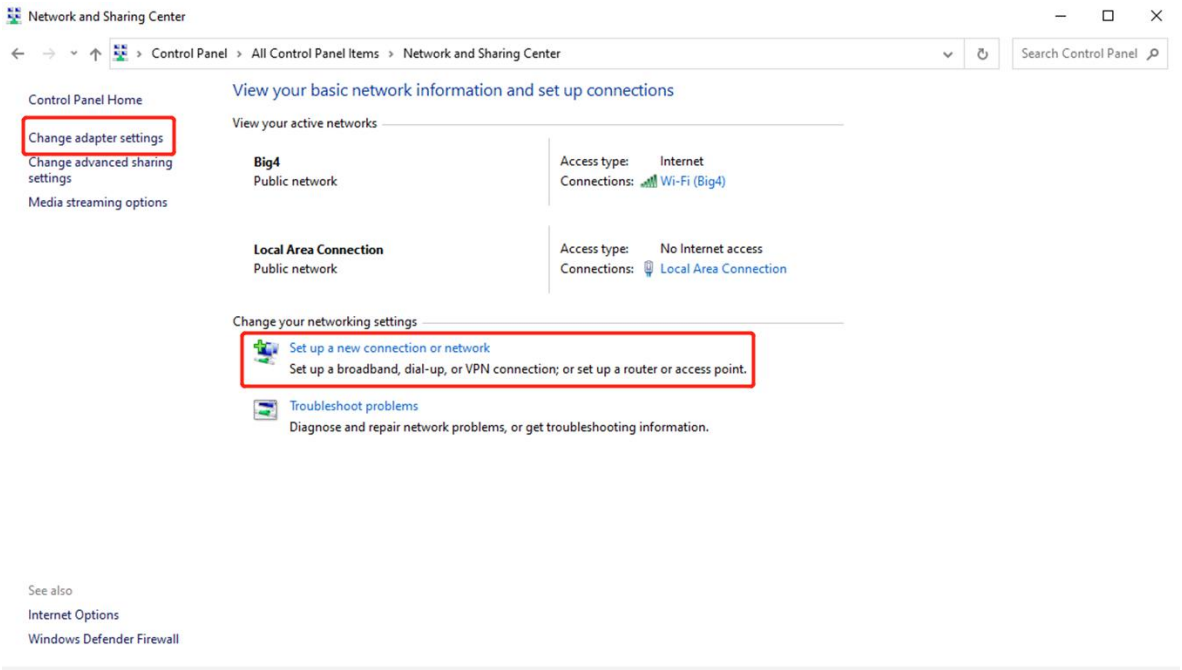
a Enter Control Panel→Network and Internet→Network and Sharing Center

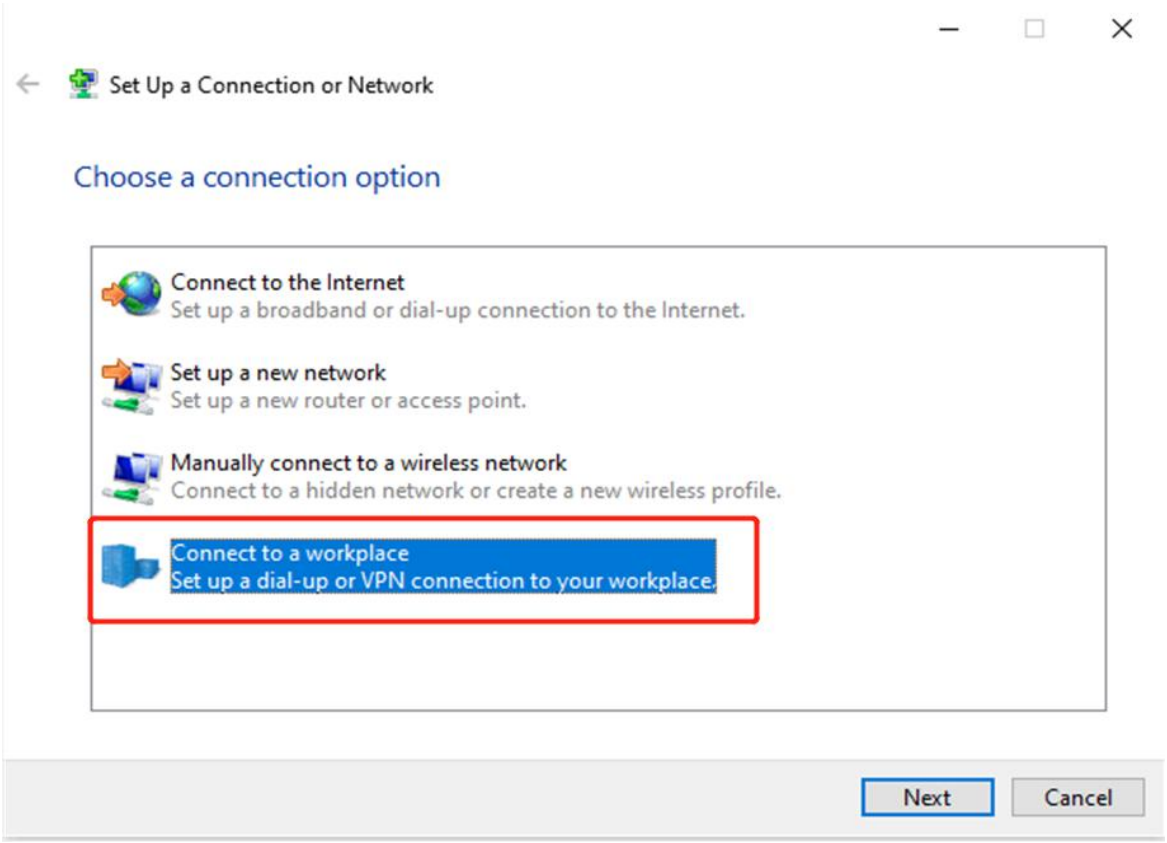

Recycle Bin
Microsoft Edge
Filters
Best match
Control Panel
App
Recent
Network and Sharing Center
Apps
Settings
Settings
System
Taskbar notification area
Search the web
control panel - See web results
control panel
3:43 PM
6/25/2019

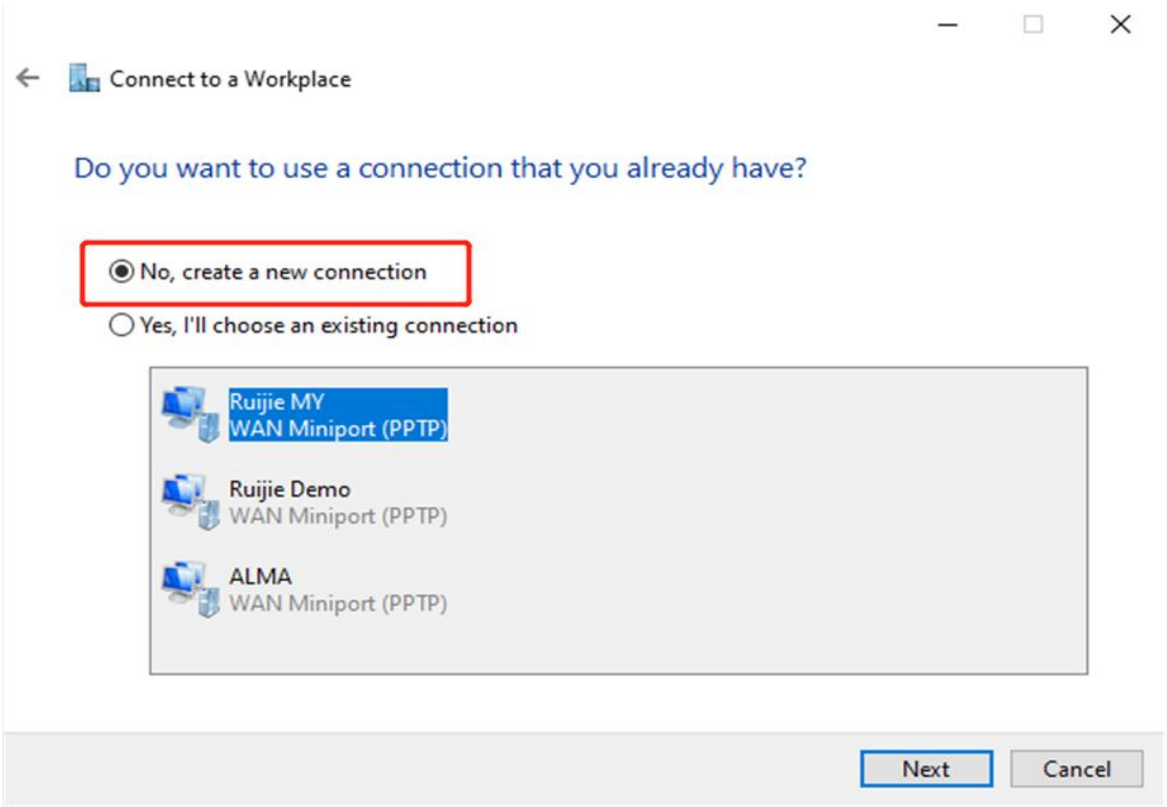

Control Panel
Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
Network and Internet
View network status and tasks
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalization
Clock and Region
Change date, time, or number formats
Ease of Access
Let Windows suggest settings
Optimize visual display

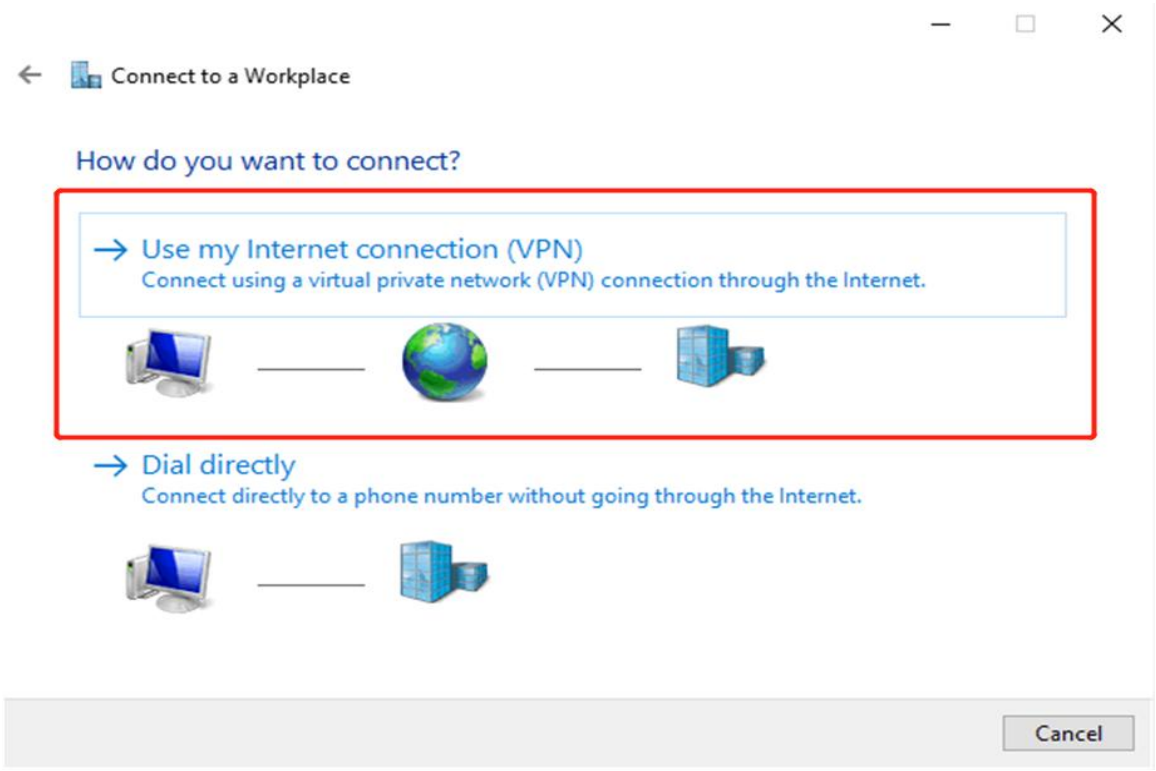


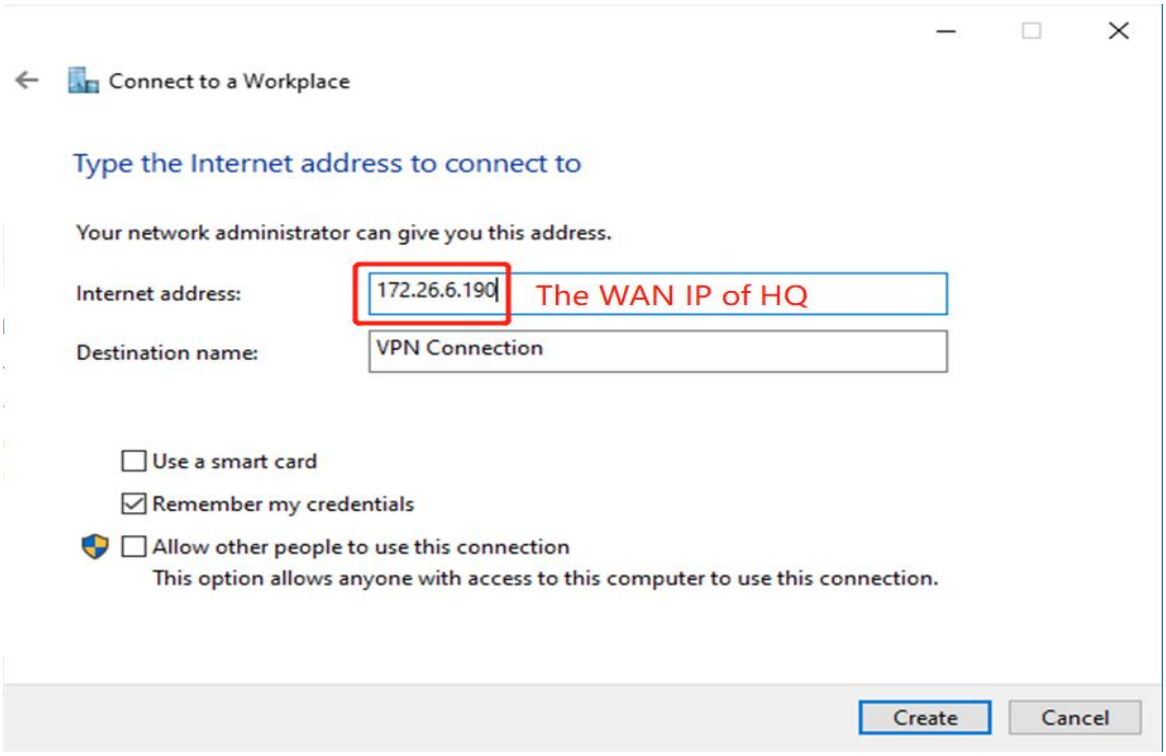
b Configure VPN connection



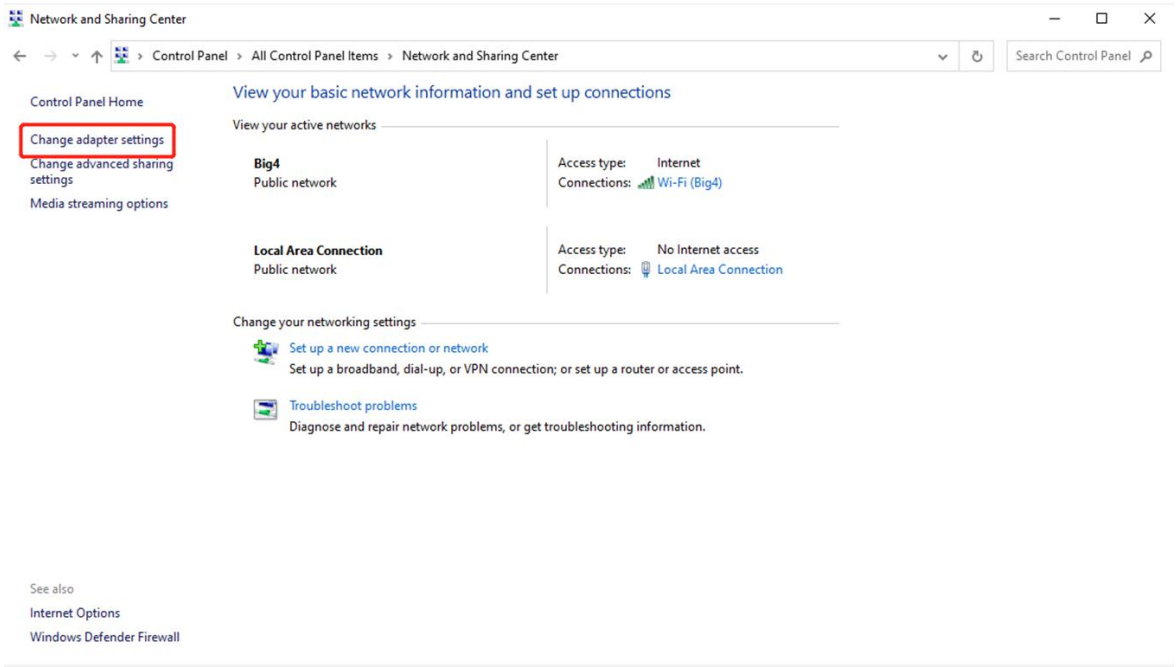

Set Up a Connection or Network
Choose a connection option
Connect to the Internet
Set up a broadband or dial-up connection to the Internet.
Set up a new network
Set up a new router or access point.
Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.
Connect to a workplace
Set up a dial-up or VPN connection to your workplace.
Next
Cancel

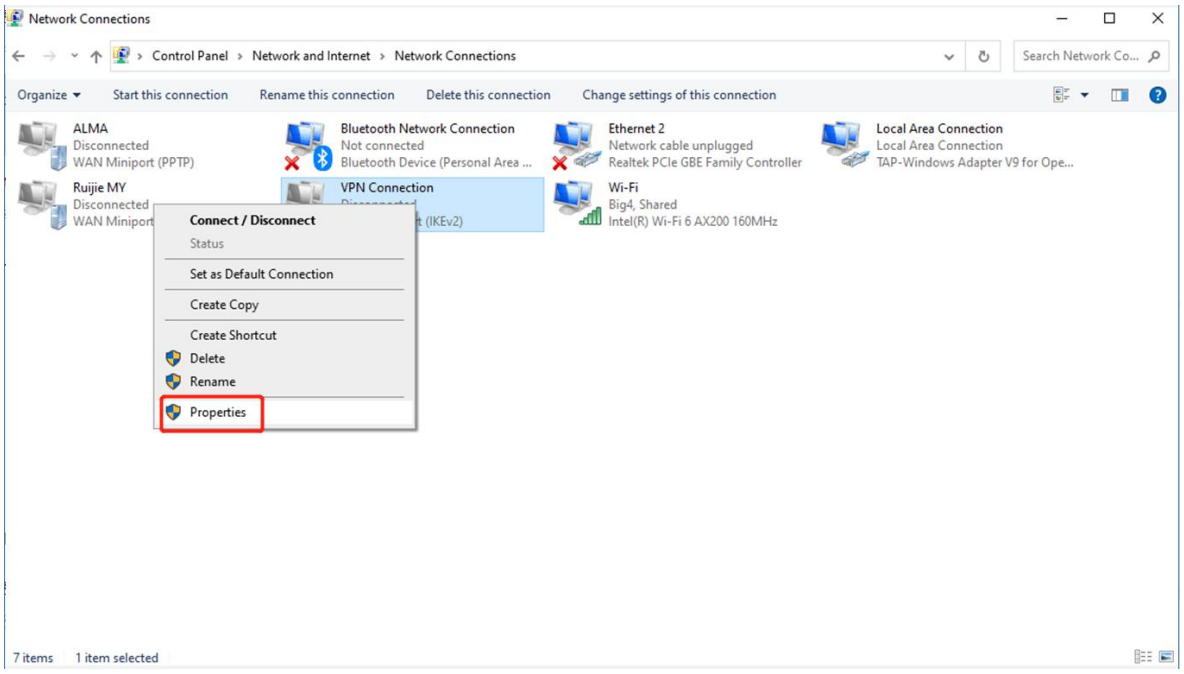

Connect to a Workplace
Do you want to use a connection that you already have?
No, create a new connection
Yes, I'll choose an existing connection
Ruijie MY
WAN Miniport (PPTP)
Ruijie Demo
WAN Miniport (PPTP)
ALMA
WAN Miniport (PPTP)
Next
Cancel

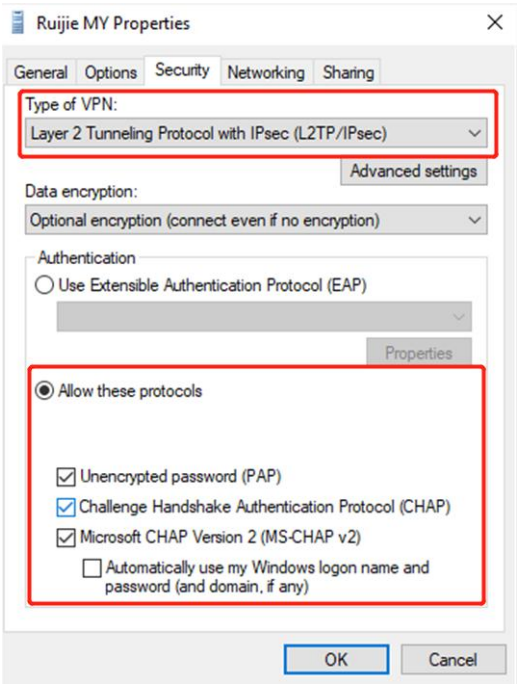




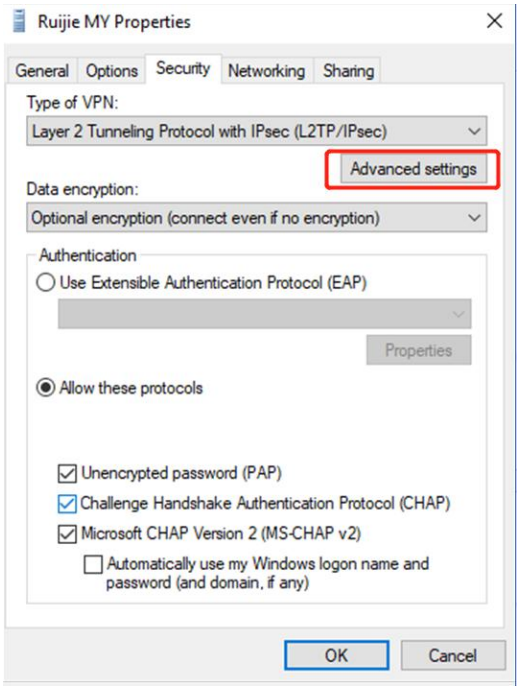
c Change adapter's setting.

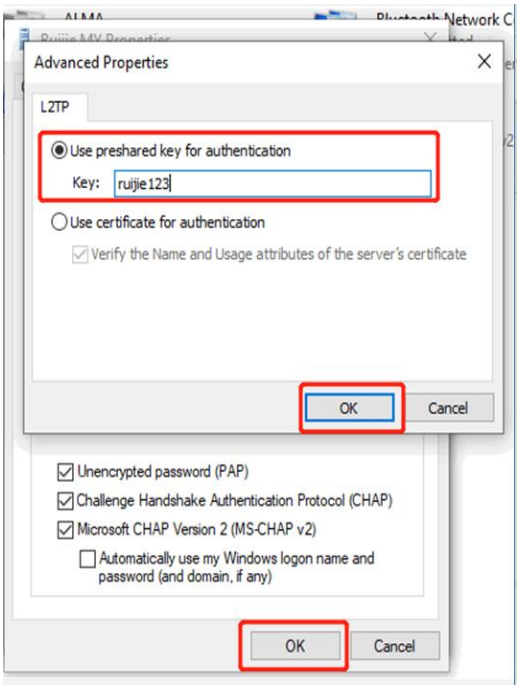

Network and Sharing Center
Control Panel › All Control Panel Items › Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
Media streaming options
View your basic network information and set up connections
View your active networks
Big4
Public network
Access type: Internet
Connections: Wi-Fi (Big4)
Local Area Connection
Public network
Access type: No Internet access
Connections: Local Area Connection
Change your networking settings
Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.
See also
Internet Options
Windows Defender Firewall


Network Connections
Control Panel › Network and Internet › Network Connections
Search Network Co...
Organize
Start this connection
Rename this connection
Delete this connection
Change settings of this connection
ALMA
Disconnected
WAN Miniport (PPTP)
Bluetooth Network Connection
Not connected
Bluetooth Device (Personal Area ...
Ethernet 2
Network cable unplugged
Realtek PCIe GBE Family Controller
Local Area Connection
Local Area Connection
TAP-Windows Adapter V9 for Ope...
Ruijie MY
Disconnected
VPN Connection
Wi-Fi
Big4, Shared
Intel(R) Wi-Fi 6 AX200 160MHz
Connect / Disconnect
Status
Set as Default Connection
Create Copy
Create Shortcut
Delete
Rename
Properties
7 items
1 item selected

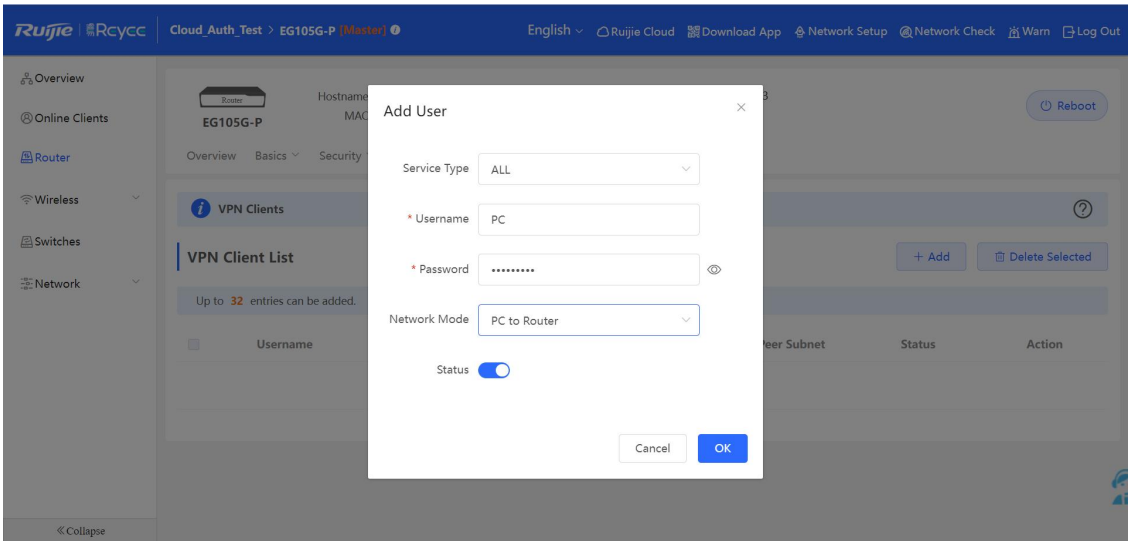


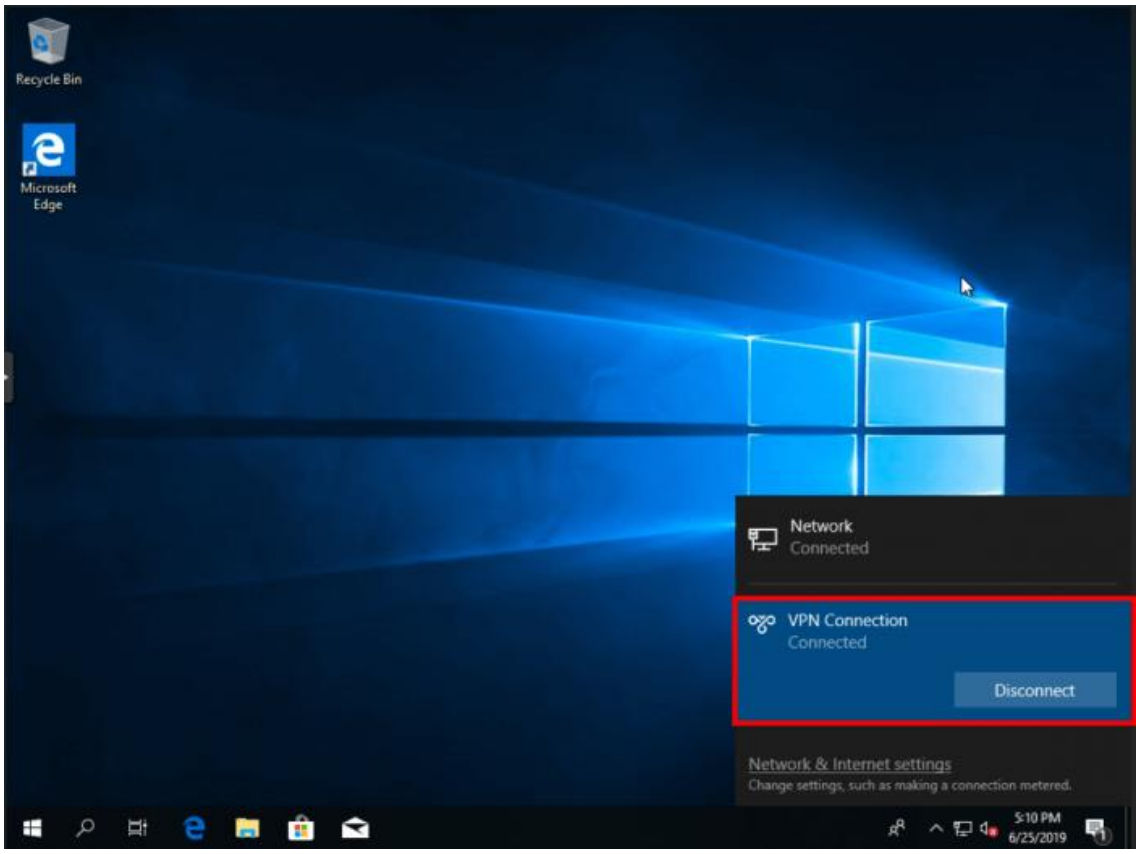
d Click Advanced Settings to configure the pre-shared password.





e Using the account of PC-to-Router to connect PC.



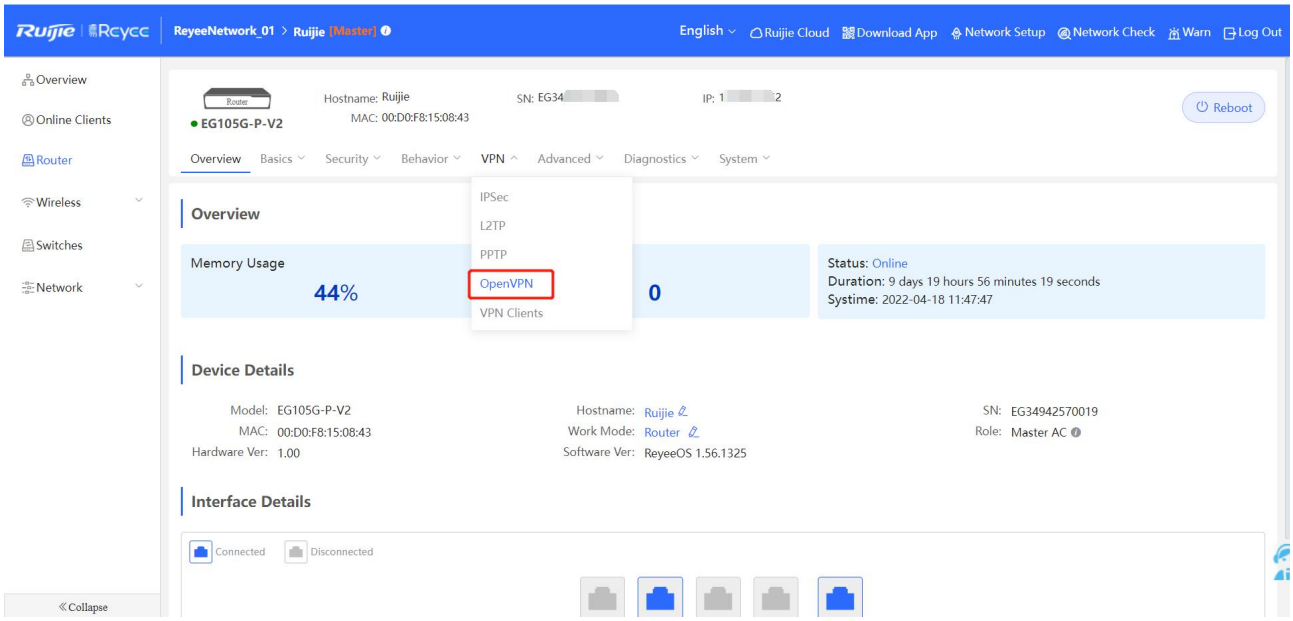


4.1.8.5 Open VPN

Open VPN usually is used for the Site to Site scenario and Client to Site scenario. OpenVPN is an application-layer VPN implementation based on the OpenSSL library. Compared with traditional VPN, its advantages is simple to use. The literal translation of VPN is a virtual private channel, which is a tunnel that provides secure data transmission between enterprises or between companies. Open VPN is a full-featured SSL VPN that uses Layer 2 or Layer 3 secure network technology using industrial Standard SSL/TLS protocol. SSL (Secure Sockets Layer), and its successor Transport Layer Security (TransportLayer Security, TLS) is a security protocol that provides security and data integrity for network communications. OpenVPN supports flexible client authorization methods, supports certificates, usernames and passwords, allowing users to A virtual interface that connects to the VPN, OpenVPN is not a web proxy-based application, nor is it a browser-based access.

(1) On the HQ side:

1. Login in to **EG -> VPN -> OpenVPN.**



2. Enable **Open VPN** and select/ input VPN information to below fields.

+ VPN type (Server/Client) based on your needed

+ Server Mode - 3 authentications method supported: Account, Certificate, Account & Certificate

- Account mode: you have to create account at VPN => VPN Clients

- Certificate: VPN connection will use certificate to auth.

- Account & Certificate: use both methods

+ Protocol: TCP or UDP

+ Server Address: IP/domain (your WAN ip address) or your domain name.

+ Port ID: 1194 by default.

+ IP Range: the IP will assign to client device.

+ Deliver Route: based on your network, you can add more than one route.

Advanced configuration:

- TLS authentication: to secure your VPN connection with TLS key

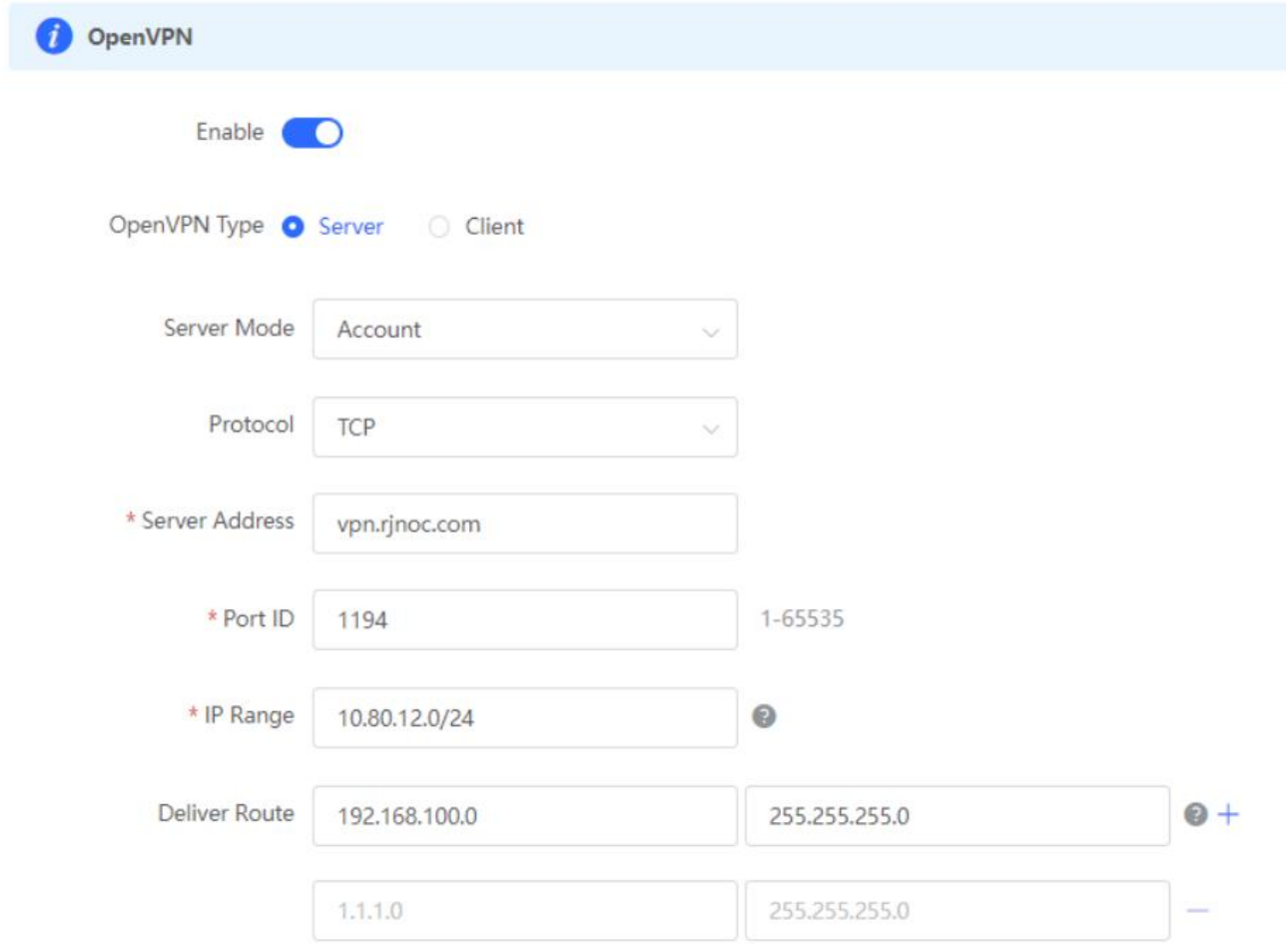
- Allow Data Compression: Yes by default.

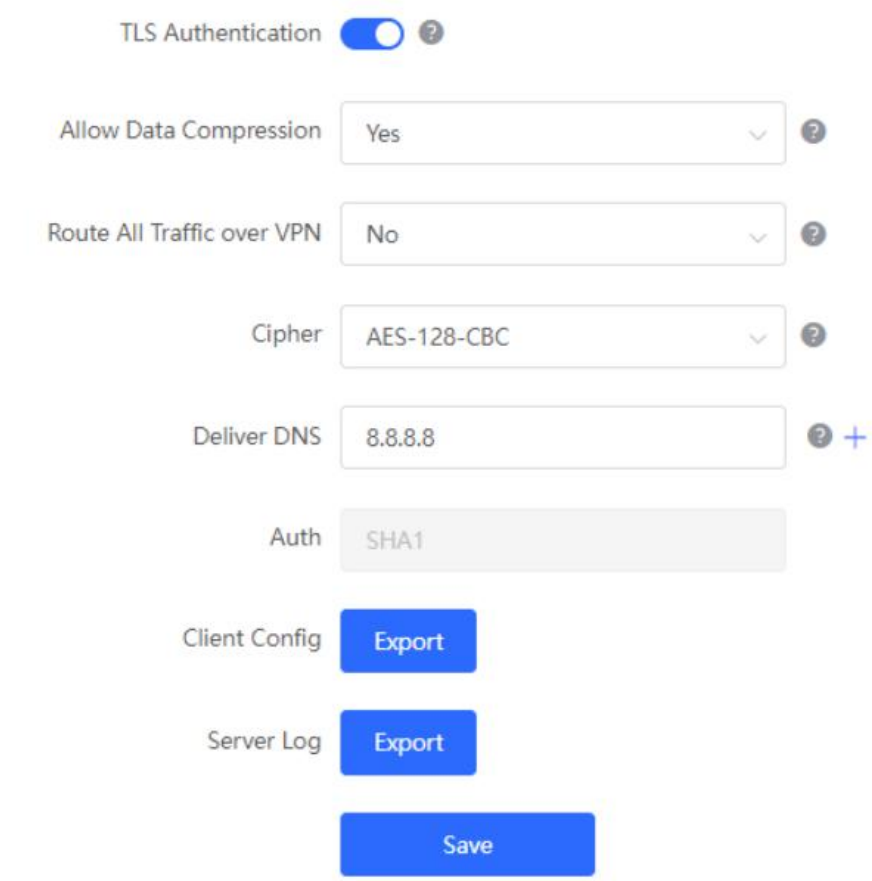
- Route All Traffic over VPN: No by default.

- Ciper: Allow you to chose data encryption algorithms, by default will be AES-128-CBC

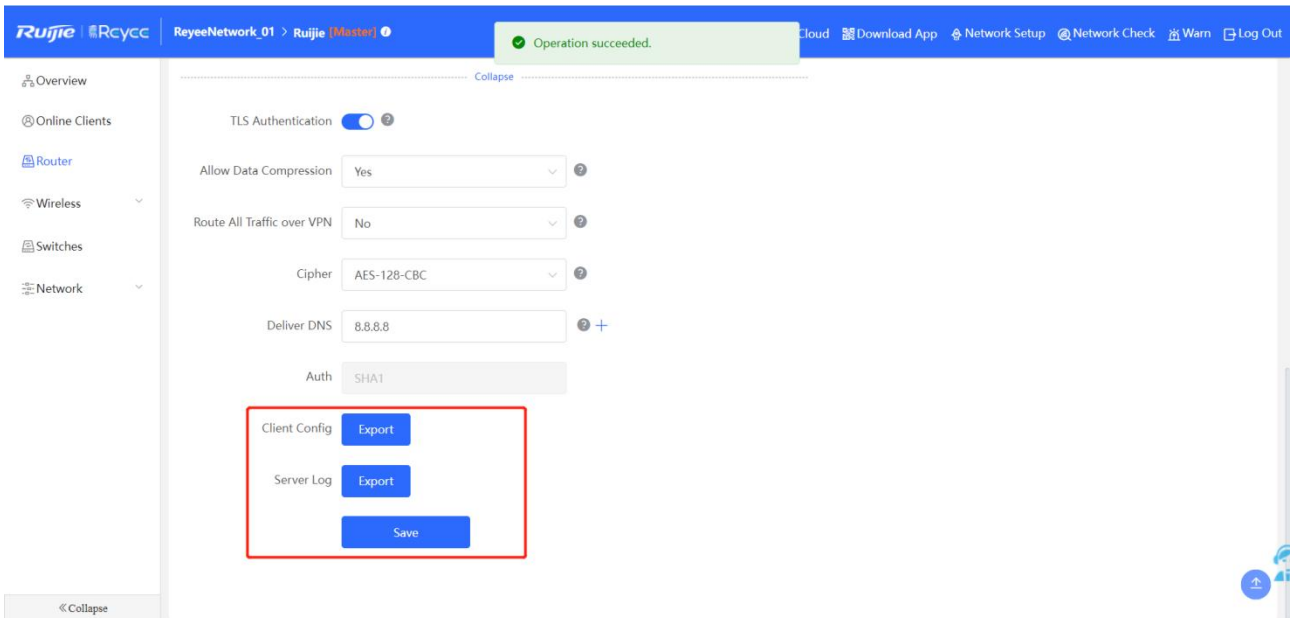
- Deliver DNS: will assign DNS address to client device.

- Auth: SHA1 by default.


OpenVPN
Enable
OpenVPN Type
Server
Client
Server Mode
Account
Protocol
TCP
* Server Address
vpn.rjnoc.com
* Port ID
1194
1-65535
* IP Range
10.80.12.0/24
Deliver Route
192.168.100.0
255.255.255.0
1.1.1.0
255.255.255.0



3. Save configuration by click to Save button and Export Client Config/ Server log



On the Clients side (take Windows 10 as example):

1. Download and install OpenVPN application to your PC

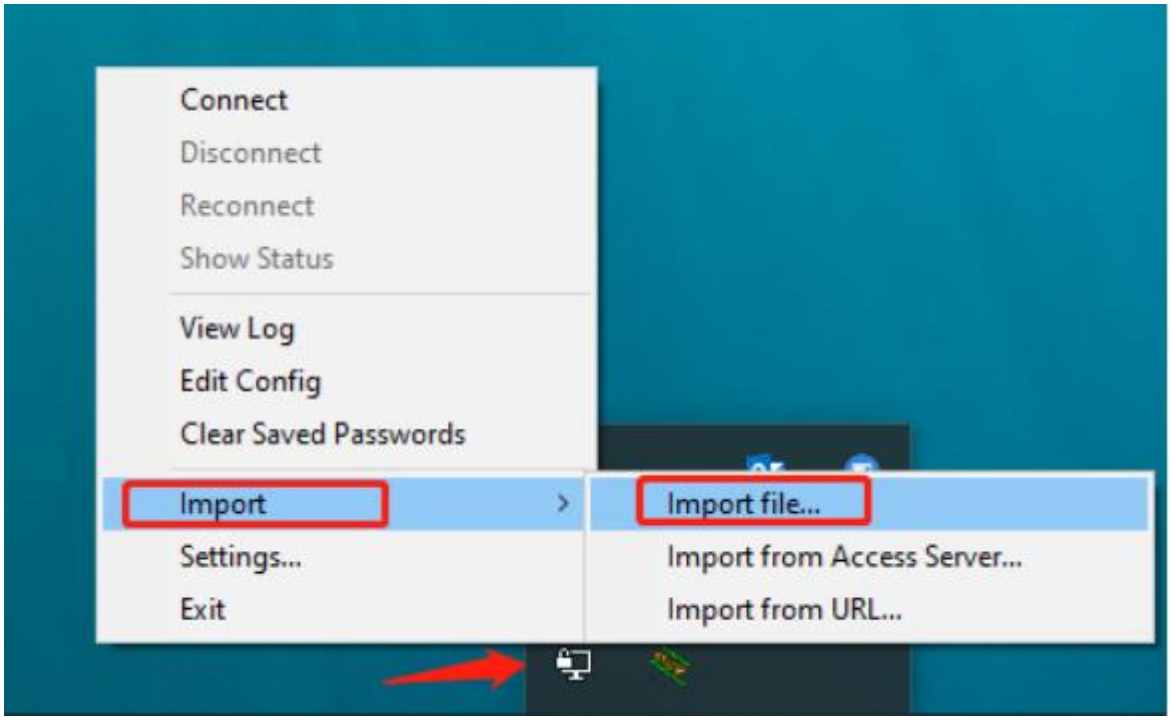
- You can download OpenVPN client in this link (select suitable version for your PC):

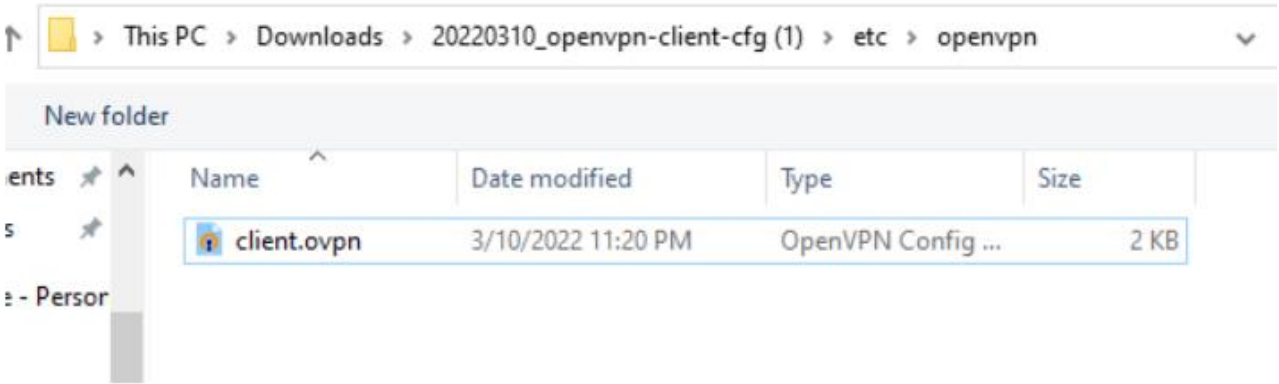
https://openvpn.net/community-downloads/

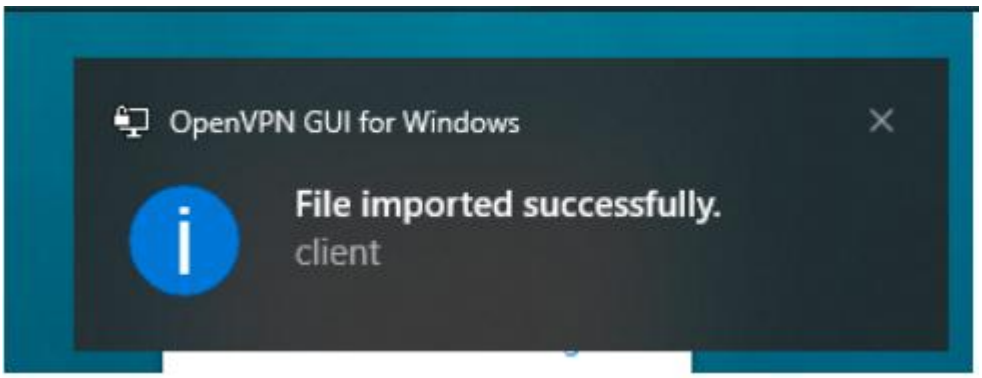
2. Import Client config to OpenVPN client after installed on your PC.

- Extract Client that you downloaded before then you will get etc folder with client.ovpn file

- Right click to OpenVPN icon on try system and chose Import => Import file... => browse to the location client.ovpn extracted.

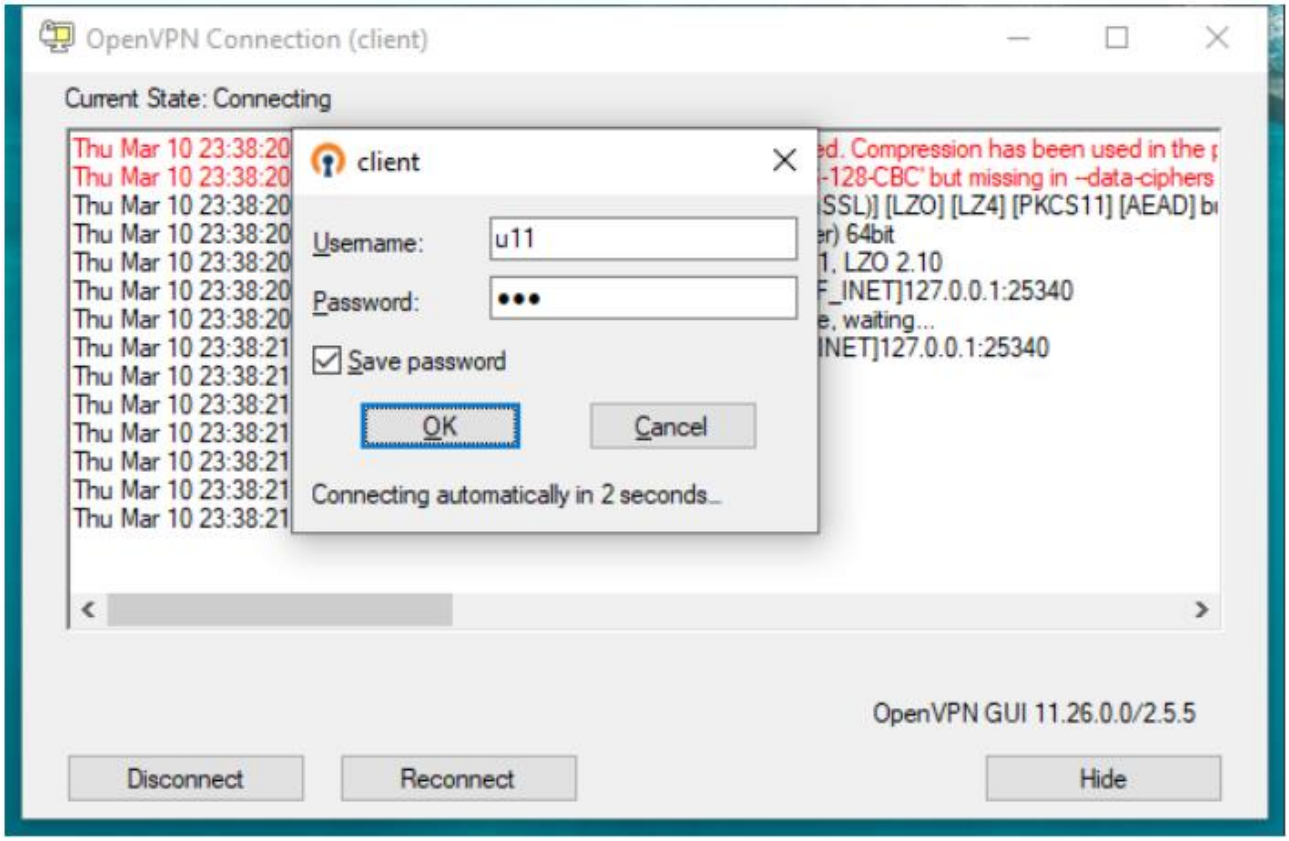




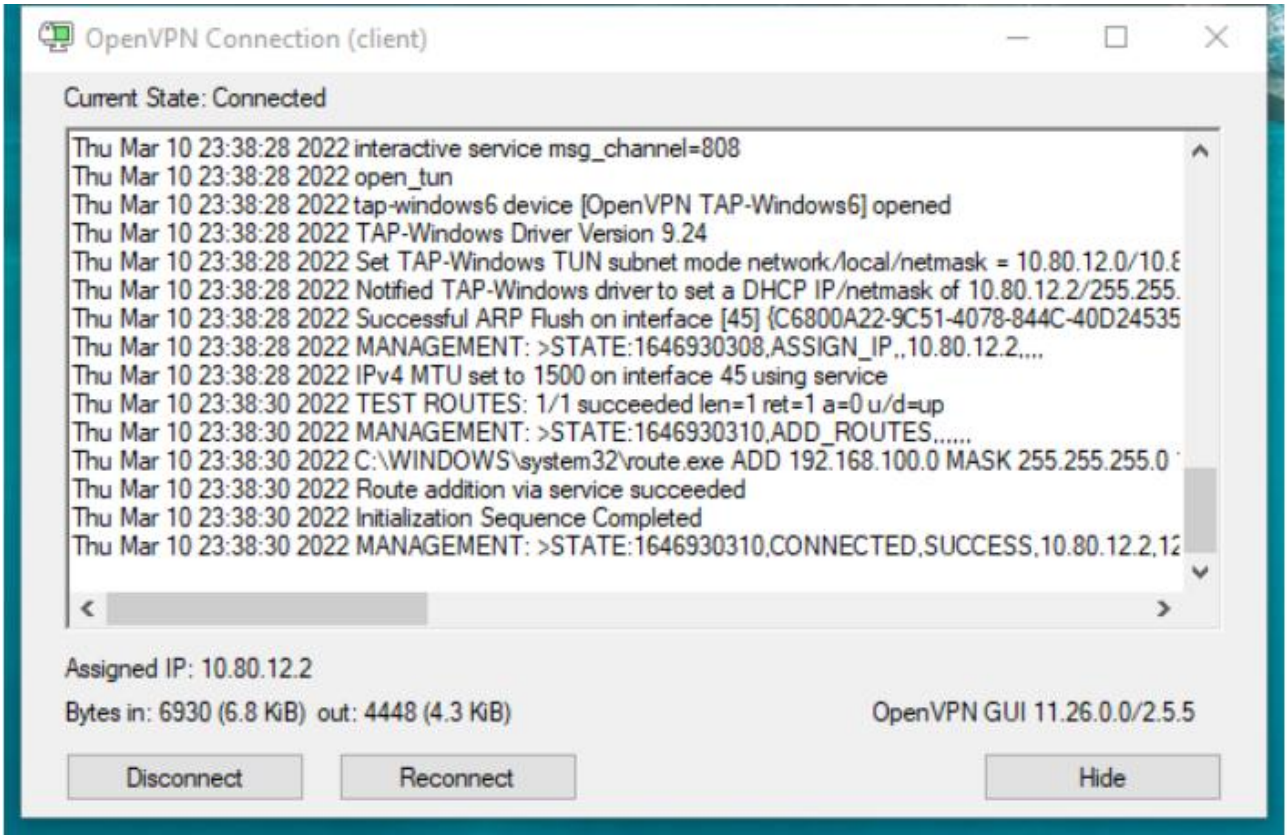


File Imported successfully, then you can connect to VPN

3. Click to OpenVPN icon on try system then select connect, if you using Account authentication method then you have to input your vpn account at this step.



Connection success and able to access to HQ resource.

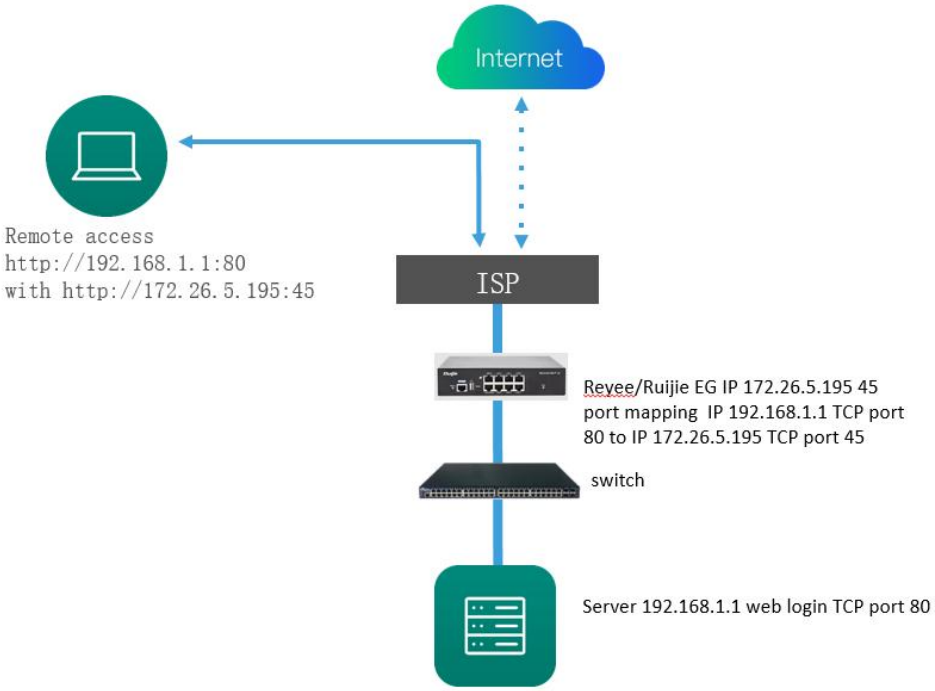


4.1.9. Port Mapping

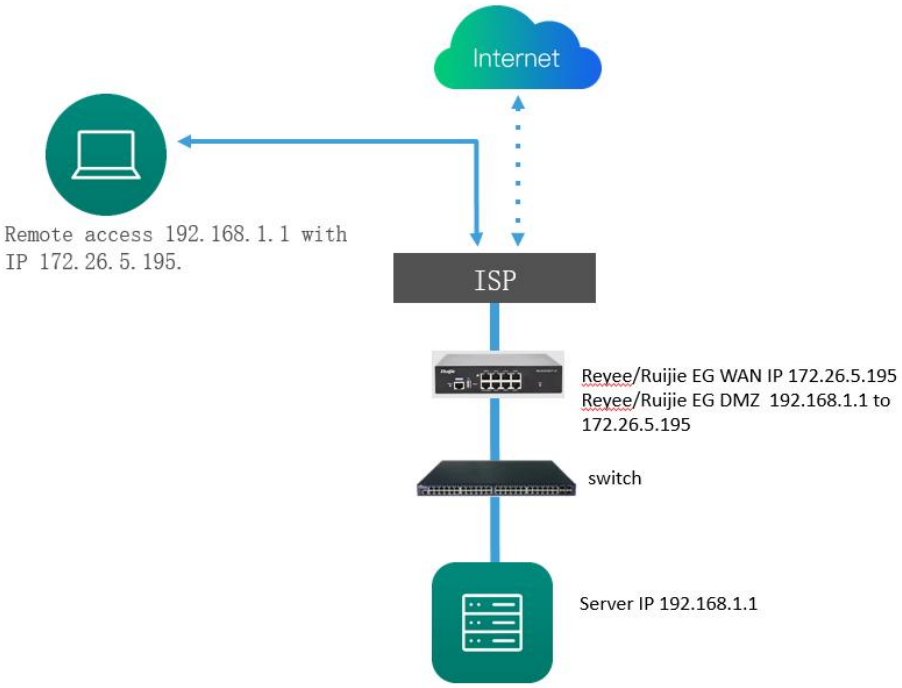
Port Mapping is used to map the internal server IP and the port to external IP, so that the outside staffs can access internal server. The difference between port mapping and DMZ is that port mapping only map one/several ports, but DMZ will map all ports.

Application Scenario

Typical Port Mapping Scenario

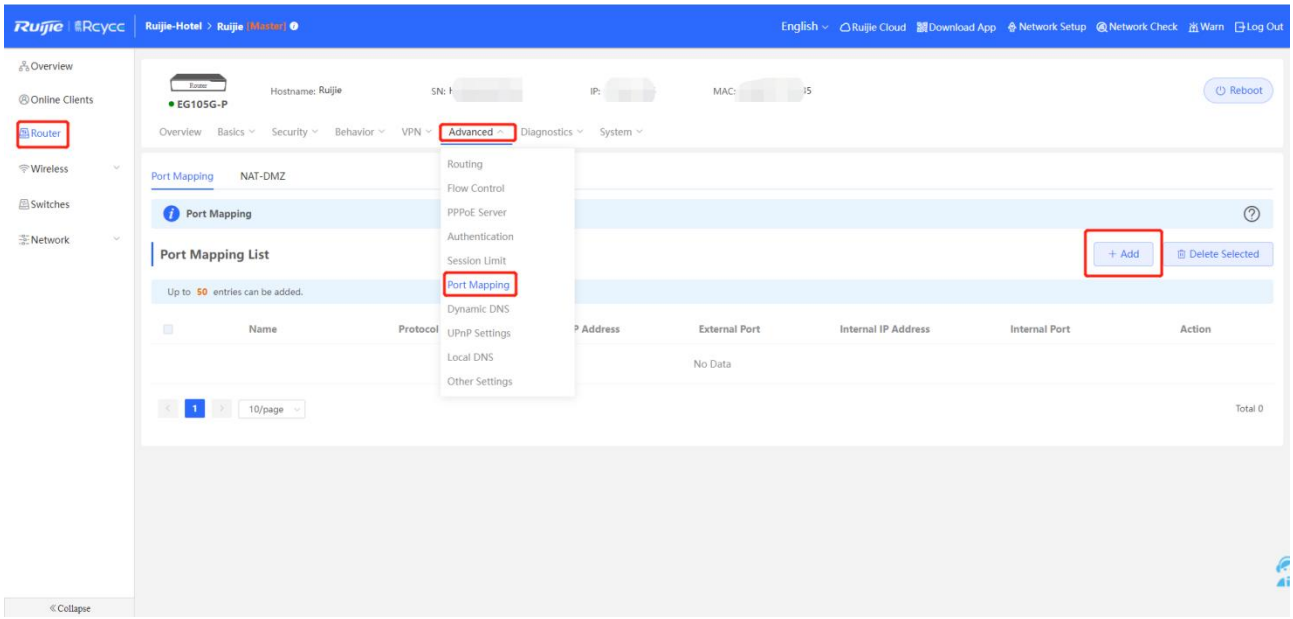


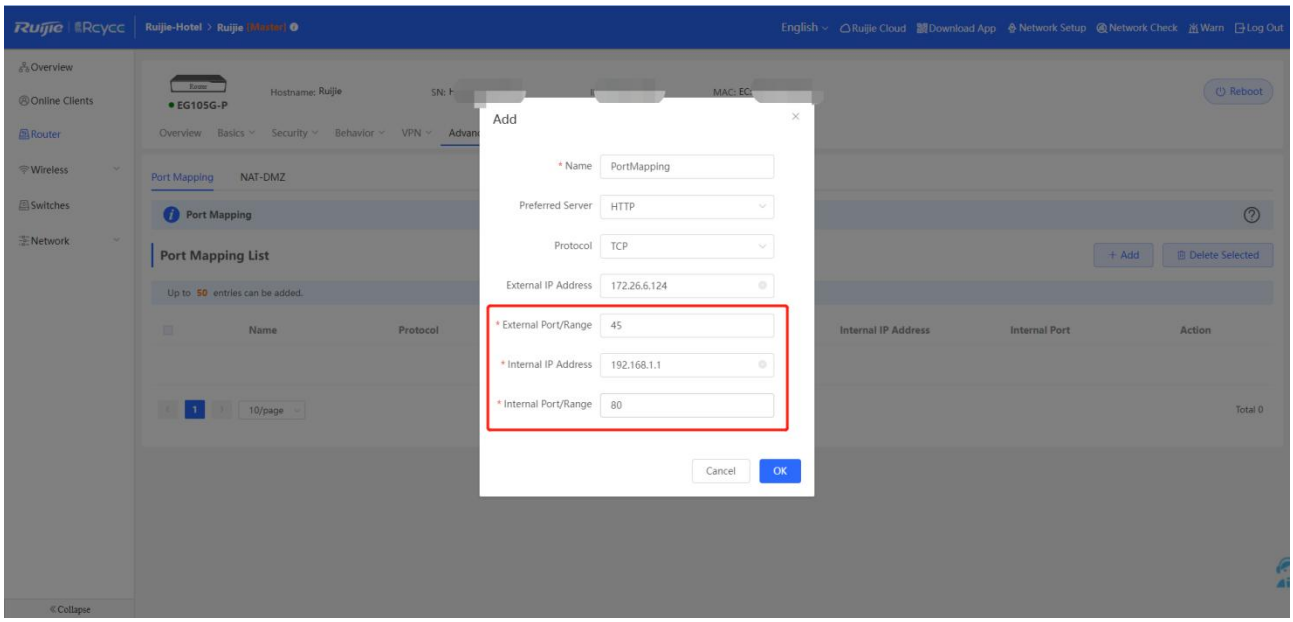
Typical DMZ scenario

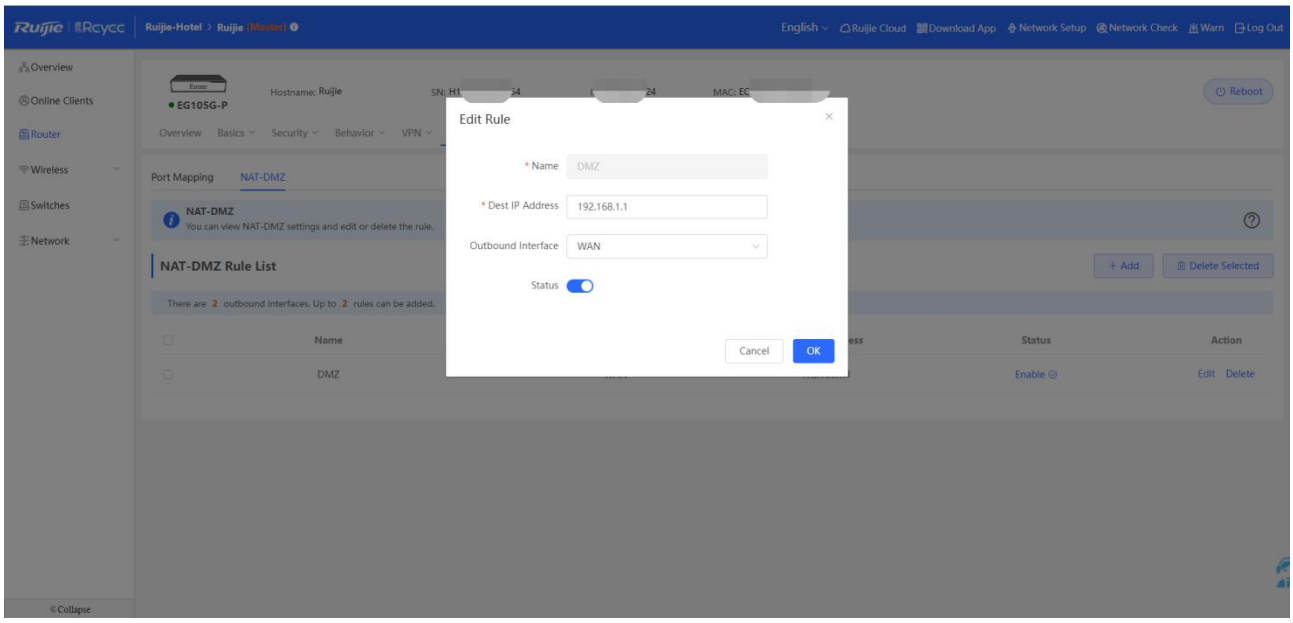


Procedure

Click **Router->Advanced->Port Mapping->Add** to add the port mapping or DMZ policy.







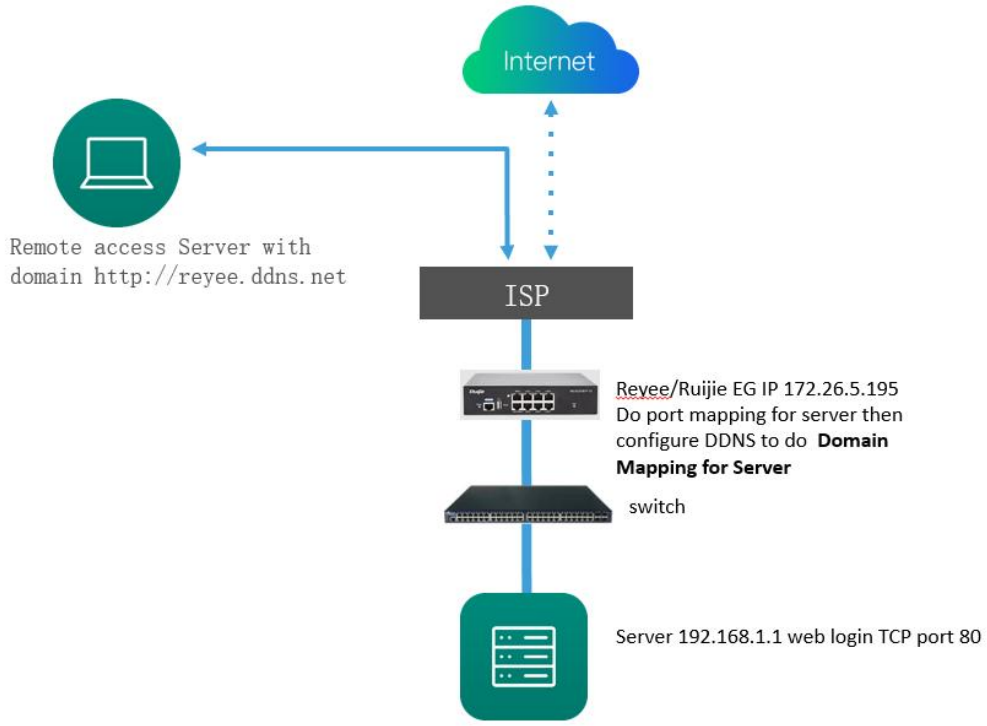
> **Note**
>
> When the DMZ and Port Mapping enable at the same time, the Port Mapping will work priority.

4.1.10. Dynamic DNS

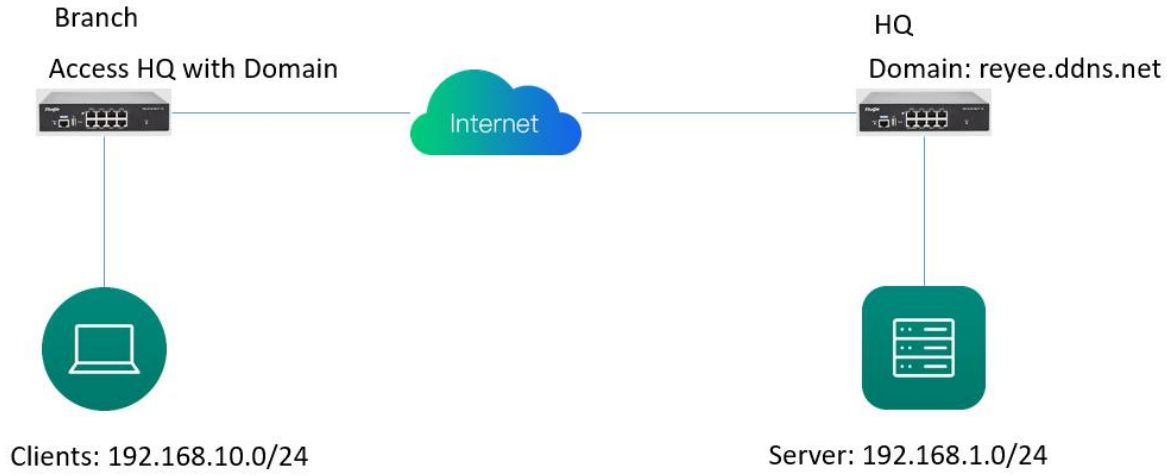
DDNS (Dynamic Domain Name Server) is to map the user's dynamic IP address to a fixed domain name resolution service. Every time the user connects to the network, the client program will transfer the dynamic IP address of the host through information transmission. It is transmitted to the server program located on the host of the service provider, and the server program is responsible for providing DNS services and implementing dynamic domain name resolution.

Application Scenario

Access Server with Domain Scenario



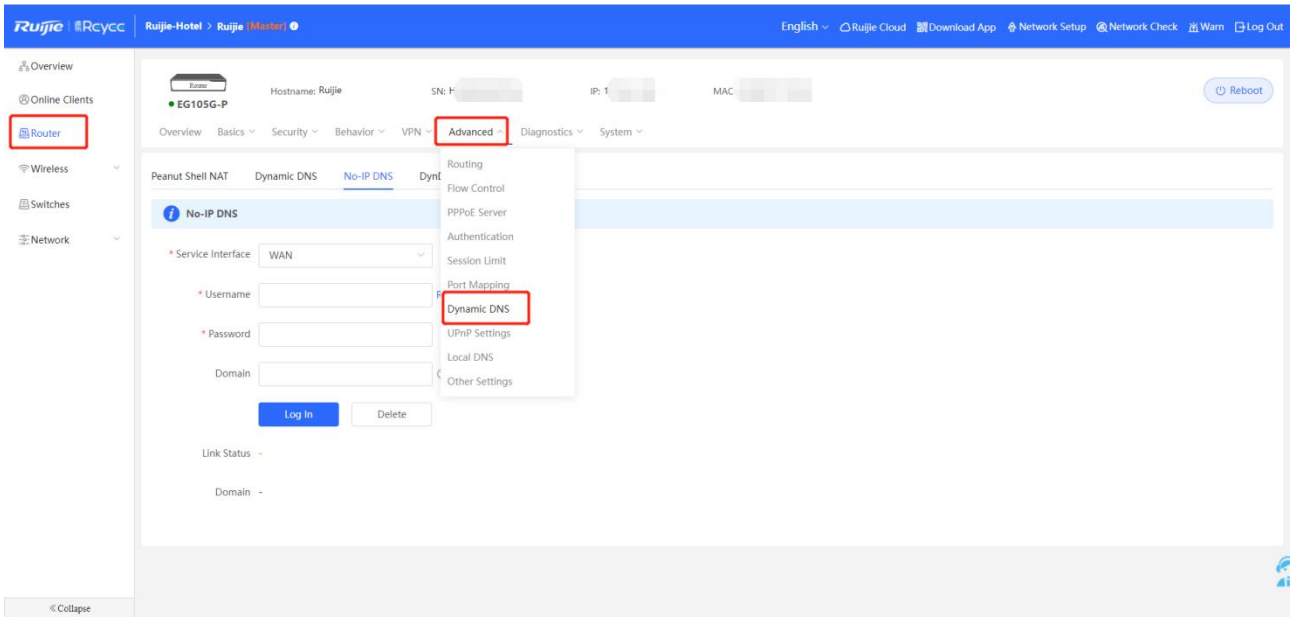
Connect VPN with Domain Scenario



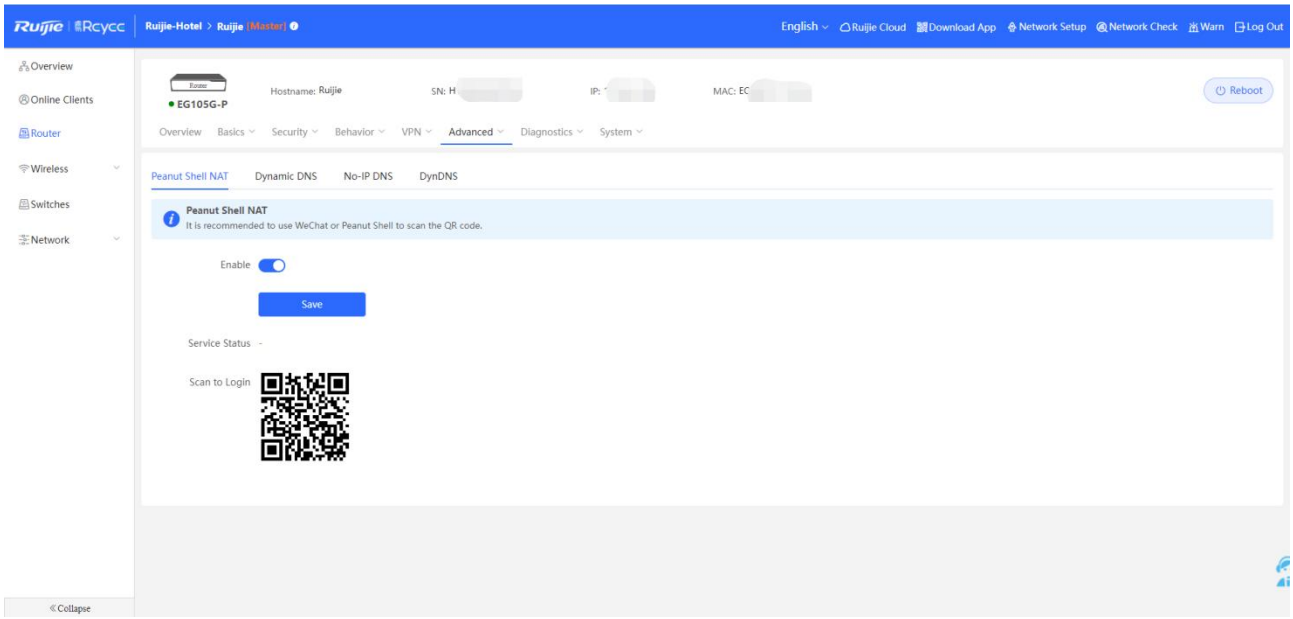
Procedure

Click **Router->Advanced->Dynamic DNS**, there are three DDNS servers you can choose to connect.

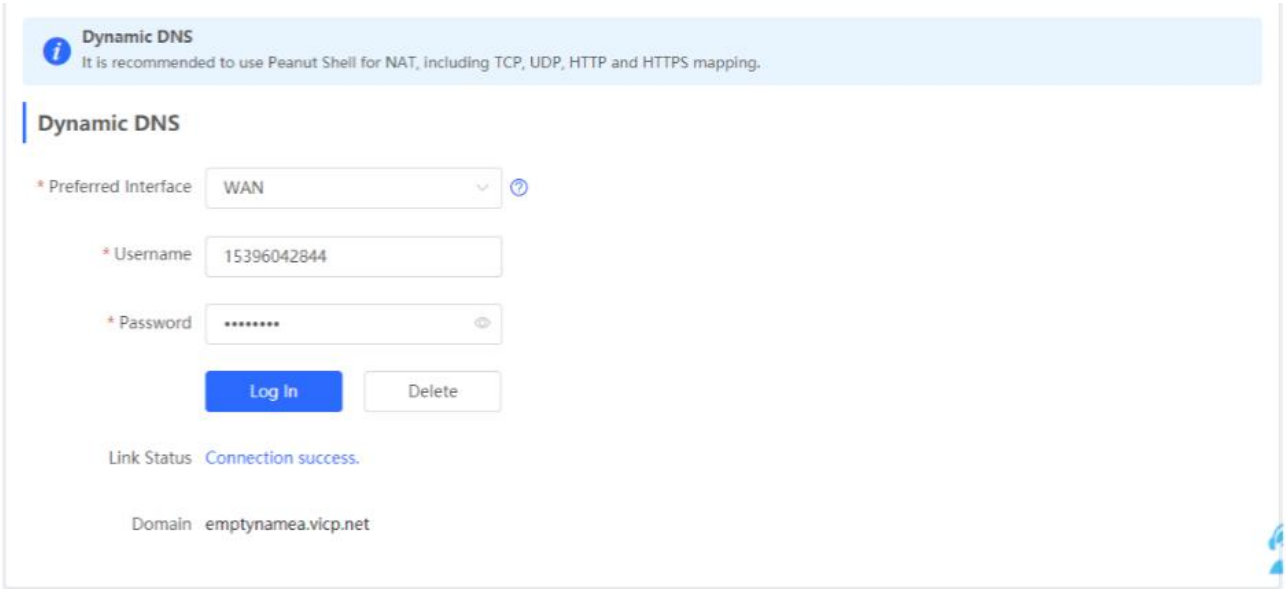
Peanut Shell DDNS, NO-IP DNS and DynDNS.



If using Peanut Shell DDNS, It is recommended to use WeChat or Peanut Shell to scan the QR code to register account.



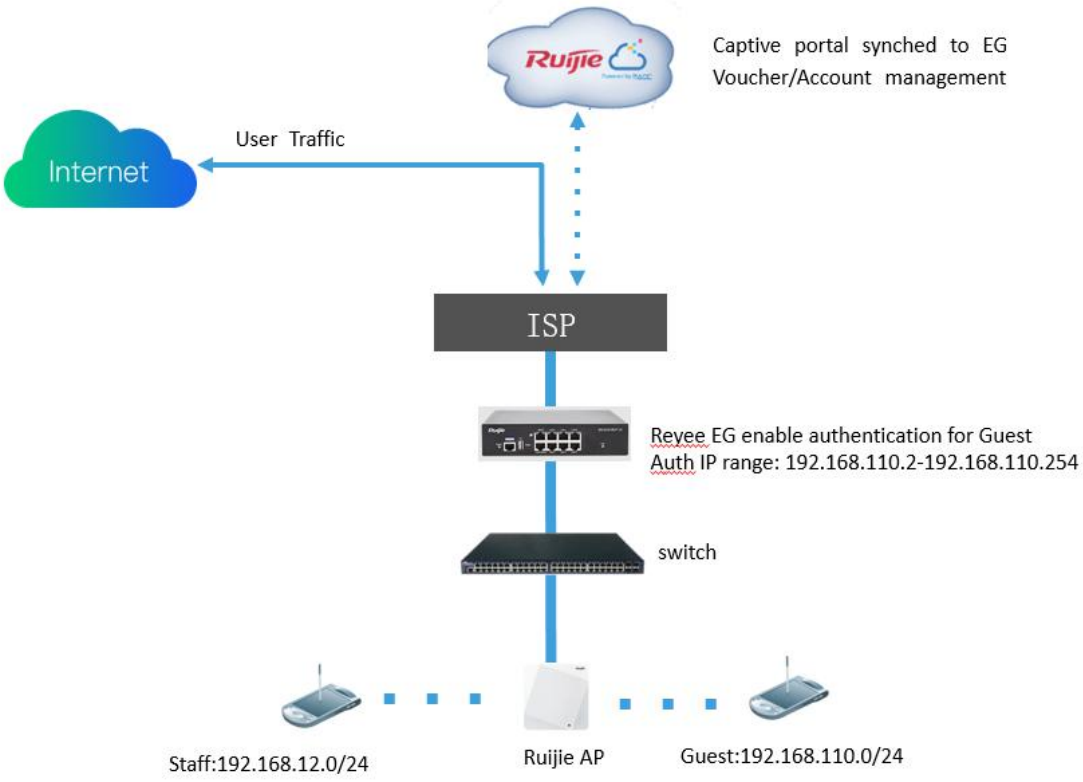
Click **Dynamic DNS** to fill in the username and password, then click Log In to connect the DDNS server. Finally you can use the Domain to access the intranet server or HQ device.



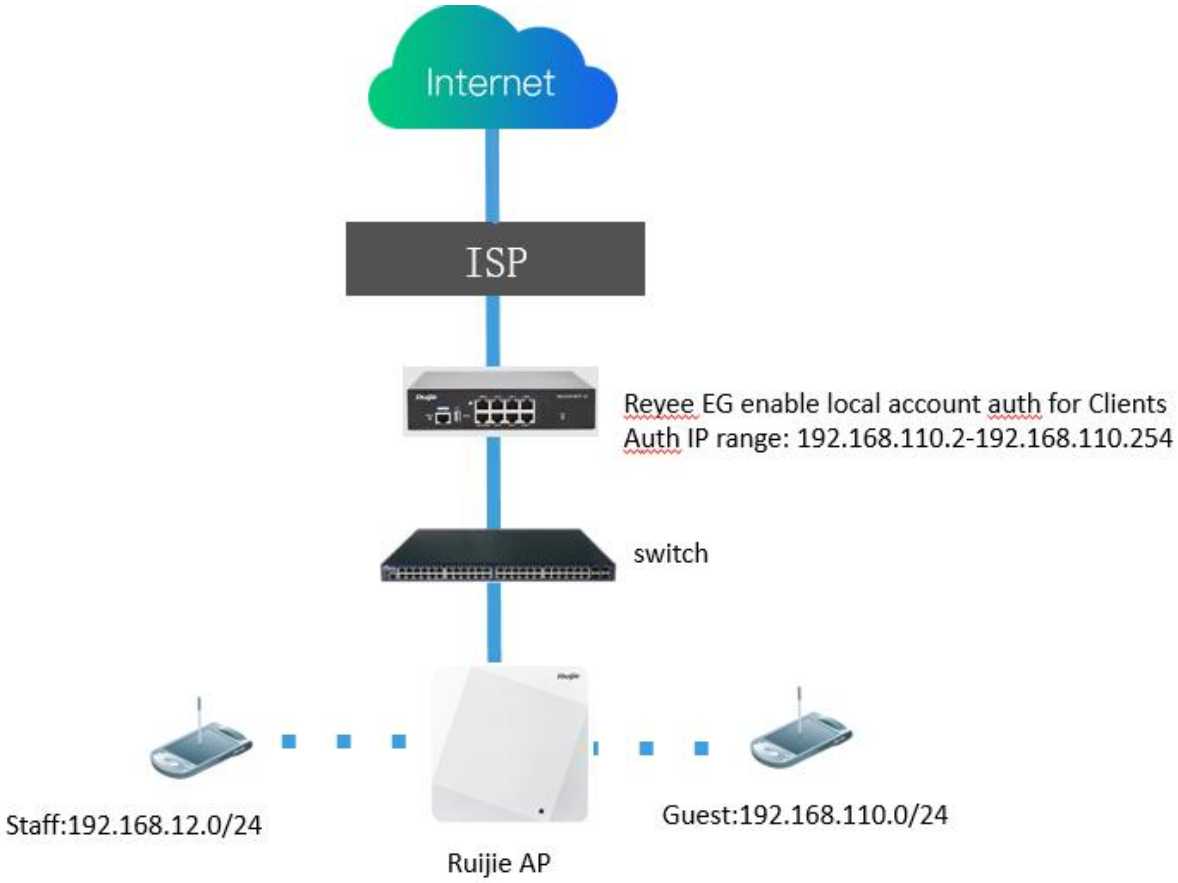
4.1.11. Authentication

Application Scenario

Cloud Auth Scenario



Local Account Auth Scenario



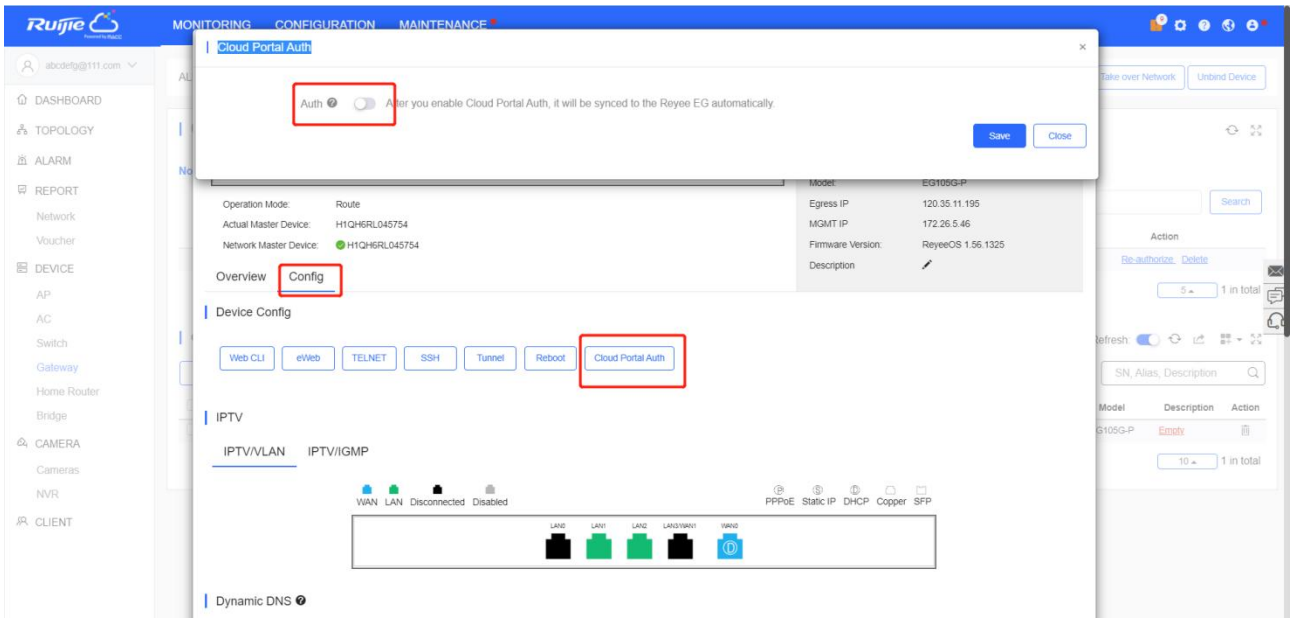
Procedure

4.1.11.1 Cloud Auth

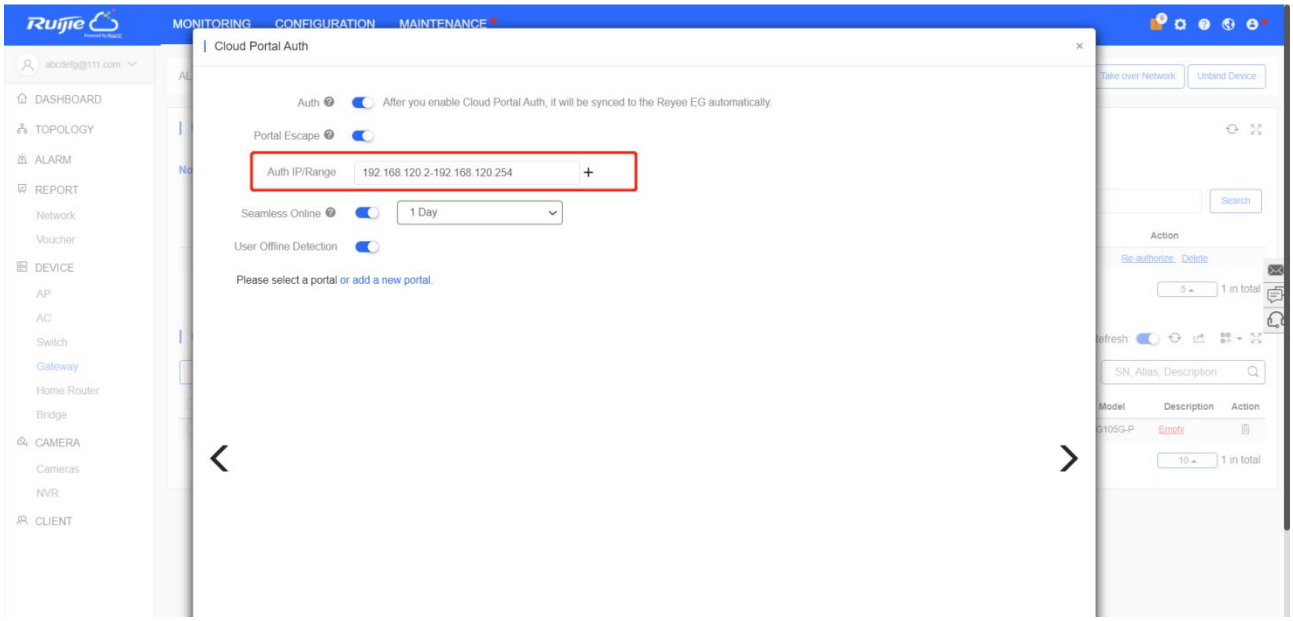
Reyee EG devices support Cloud portal authentication, including one-click, voucher, account, SMS (integrated with Twilio) authentications.

1. Configuring the Cloud authentication on cloud, click the SN of the EG to enter the the EG detail page

2. Click **Config-> Cloud Portal Auth**,



3. Fill the **Auth IP/Range** who need to do authentication then can access internet.

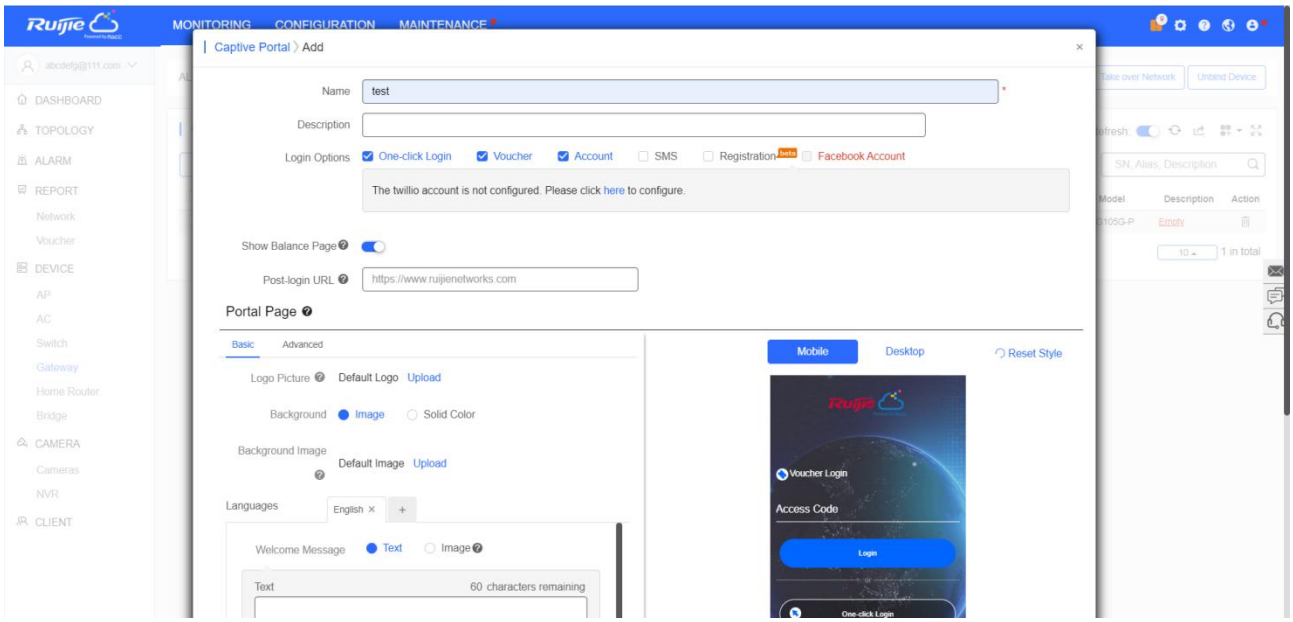


Portal Escape: When the cloud server was down, if you enable this function, the clients can access internet directly without authentication.

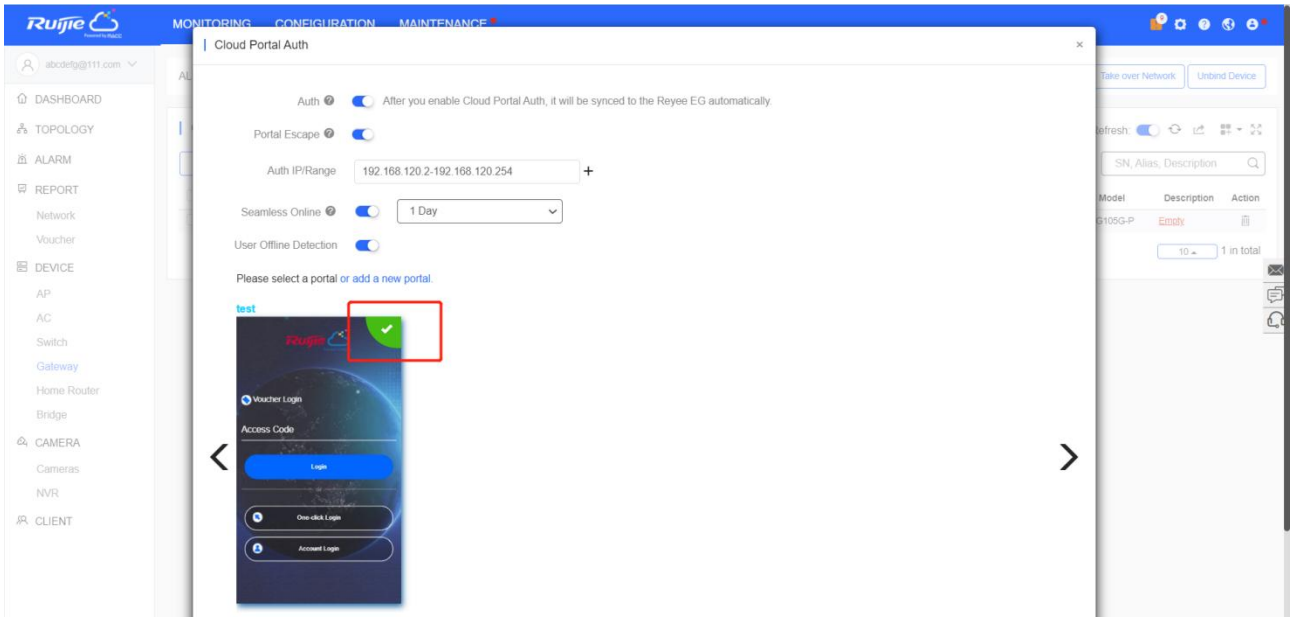
Seamless Online: User only need to pass the authentication once. If they want to go online again，authentication is not required. After users go online, they do not need to log in again in the specified period. You can choose 1 Day, 1 week，1 Month or Always.

User Offline Detection: User won't access internet after the valid period

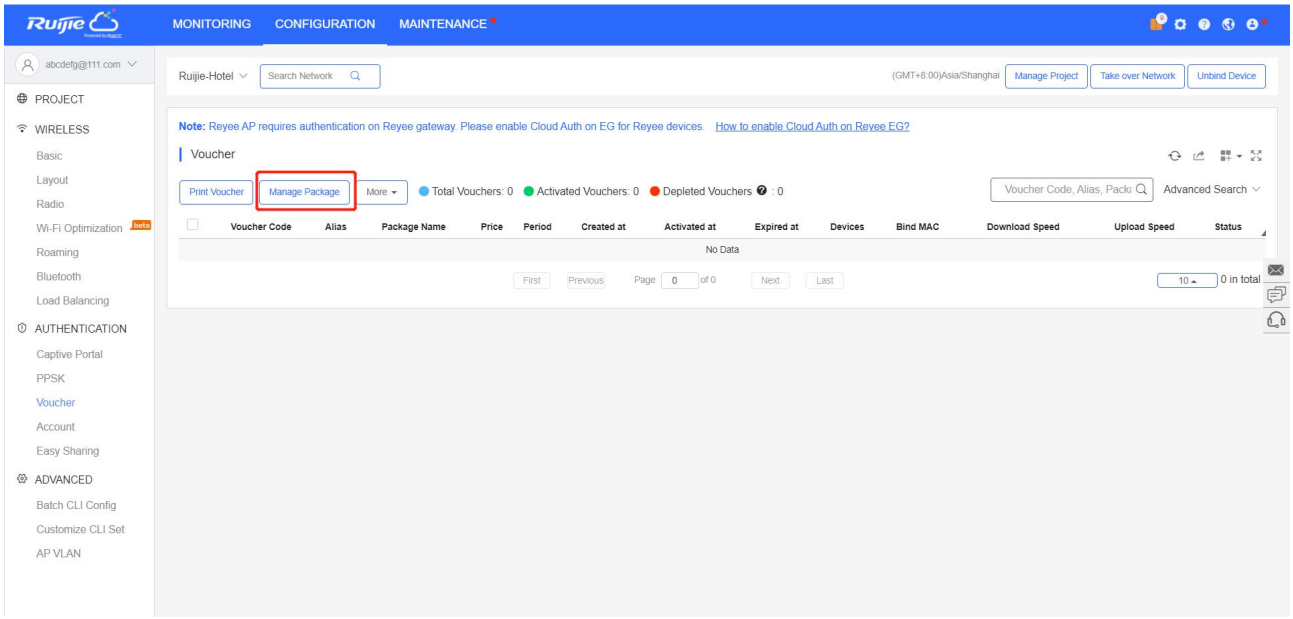
4. Click add a new portal to add a portal page.



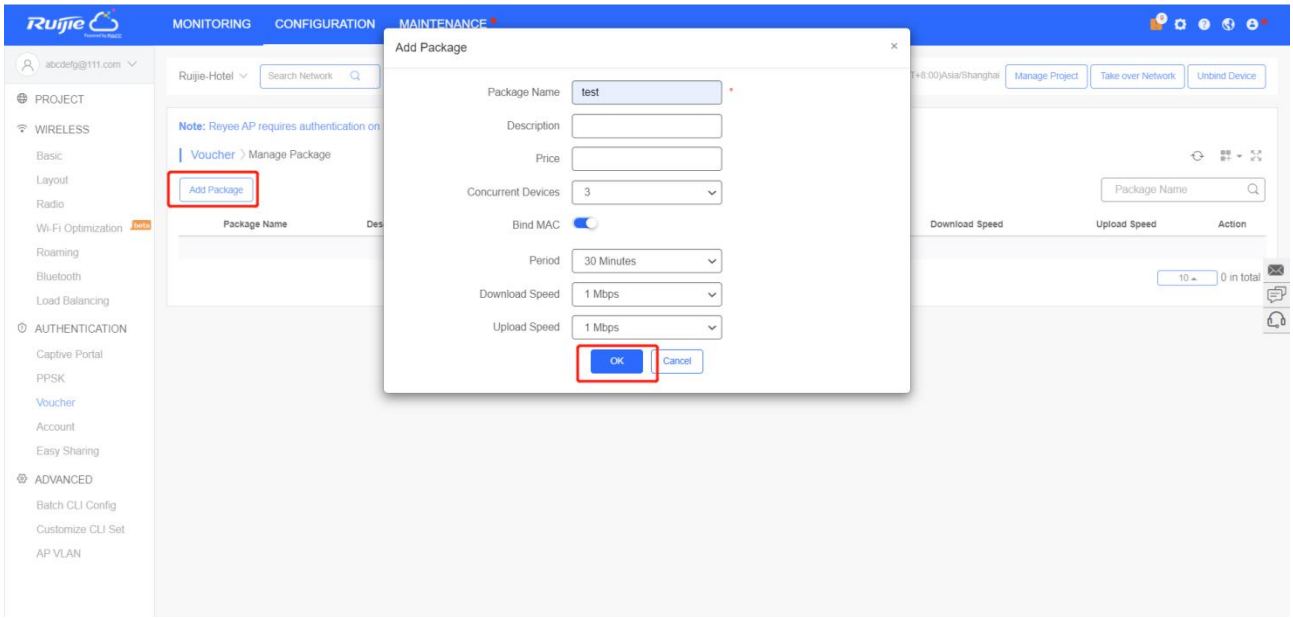
5. Click the portal page to apply it, then click **Save.**



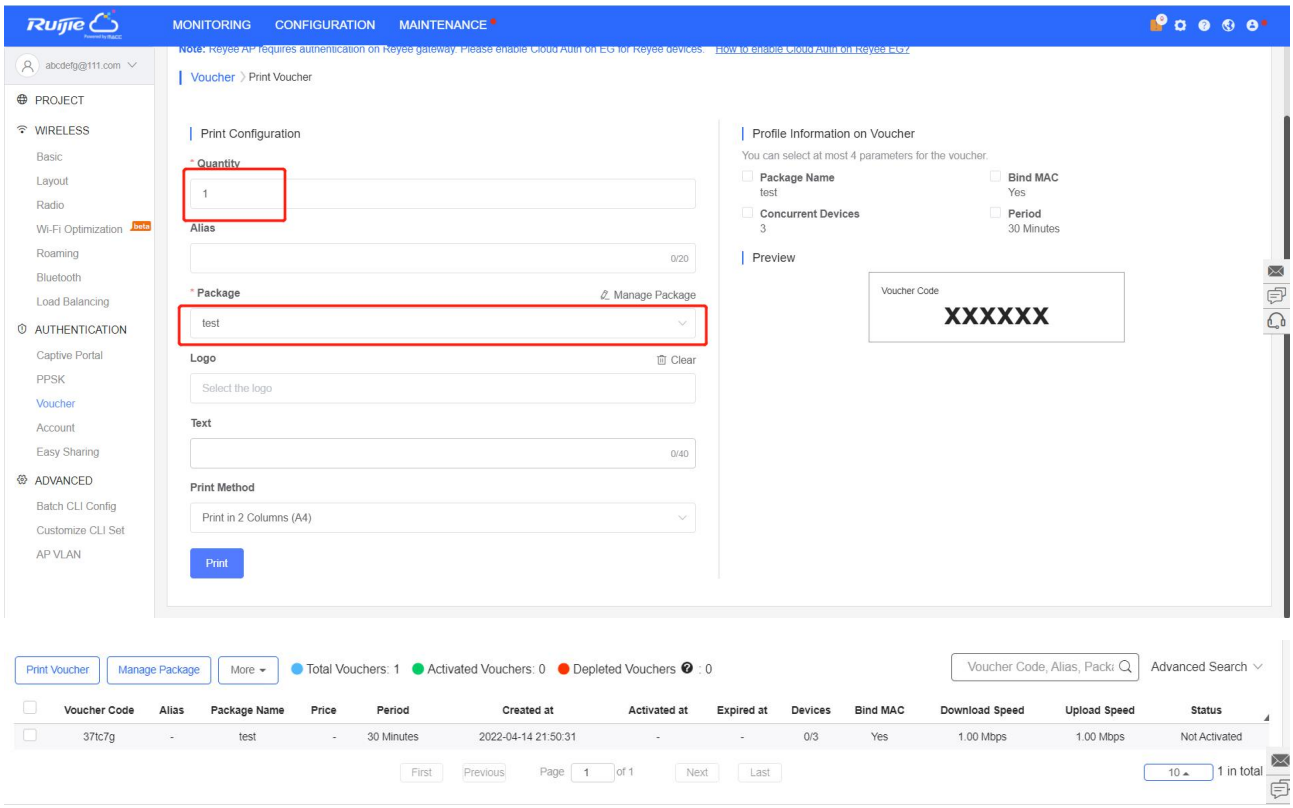
6. If you use voucher or account authentication, click **Configuration->Voucher/Account** to add voucher or account used for clients. Click **Manage Package** to add package



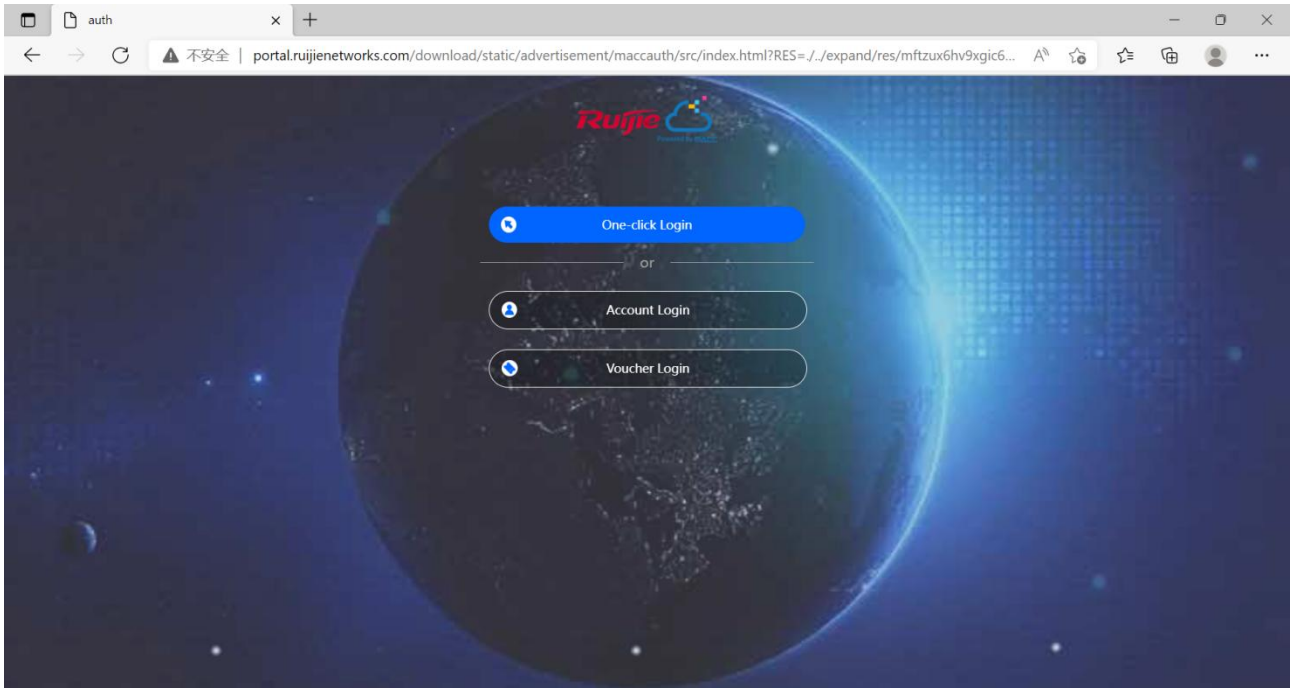
7. Click **Add Package**, fill the **Price, Concurrent Devices, Bind MAC, Period, Download Speed, Upload Speed.**



8. Click **Print Voucher** to add voucher. Fill the **Quantity** and choose the Package you add just now. Then click **Print.**



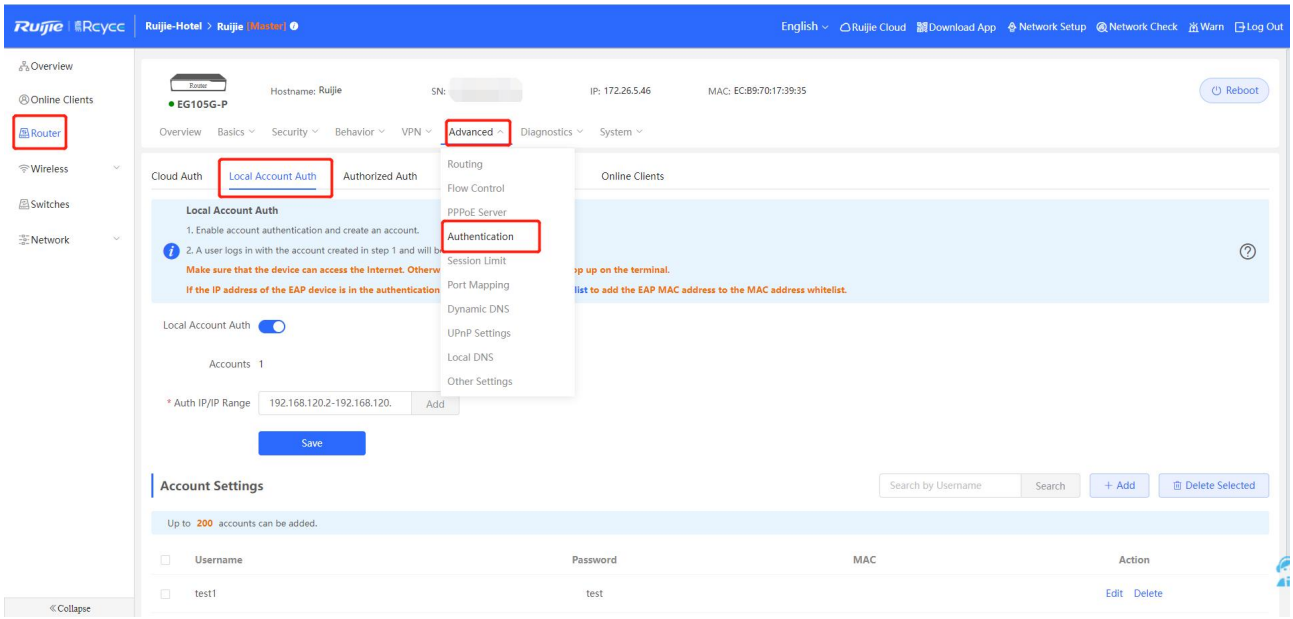
9. Click **One-Click** to Login to do authentication on PC



4.1.11.2 Local Account Auth

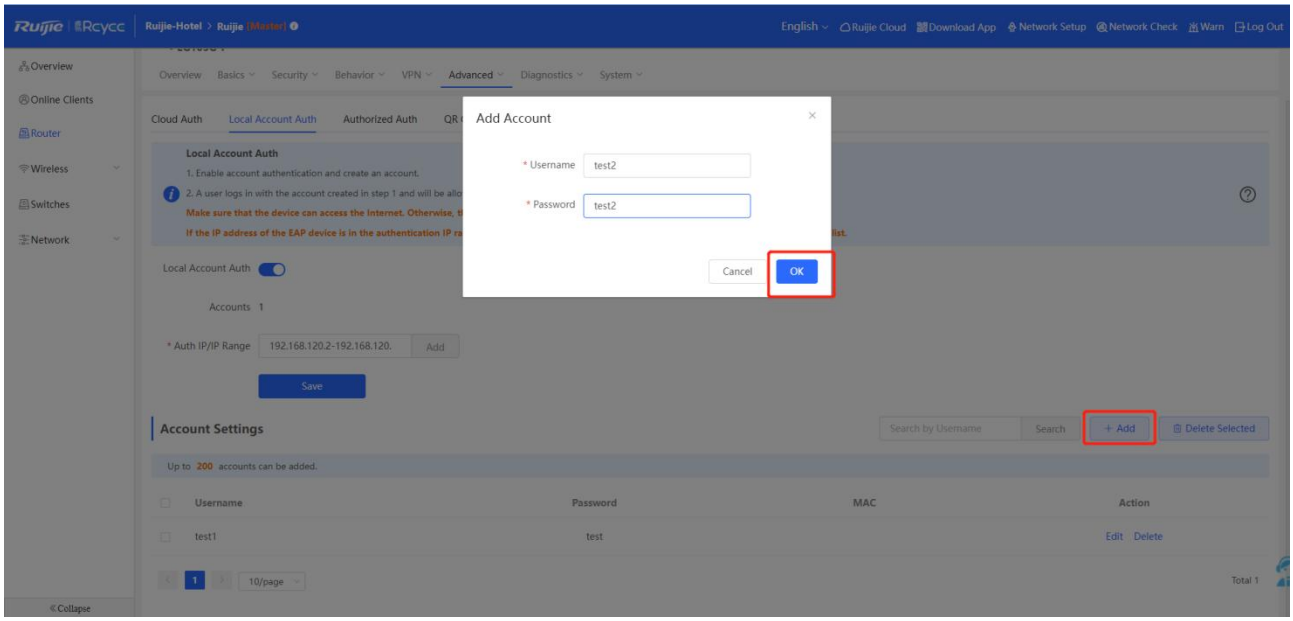
Reyee EG devices provide local account authentication, the portal page and account are all created locally.

1. Click **Router->Advanced->Local Account Auth**, enable local account auth, fill the Auth IP/IP Range, then click **Save.**



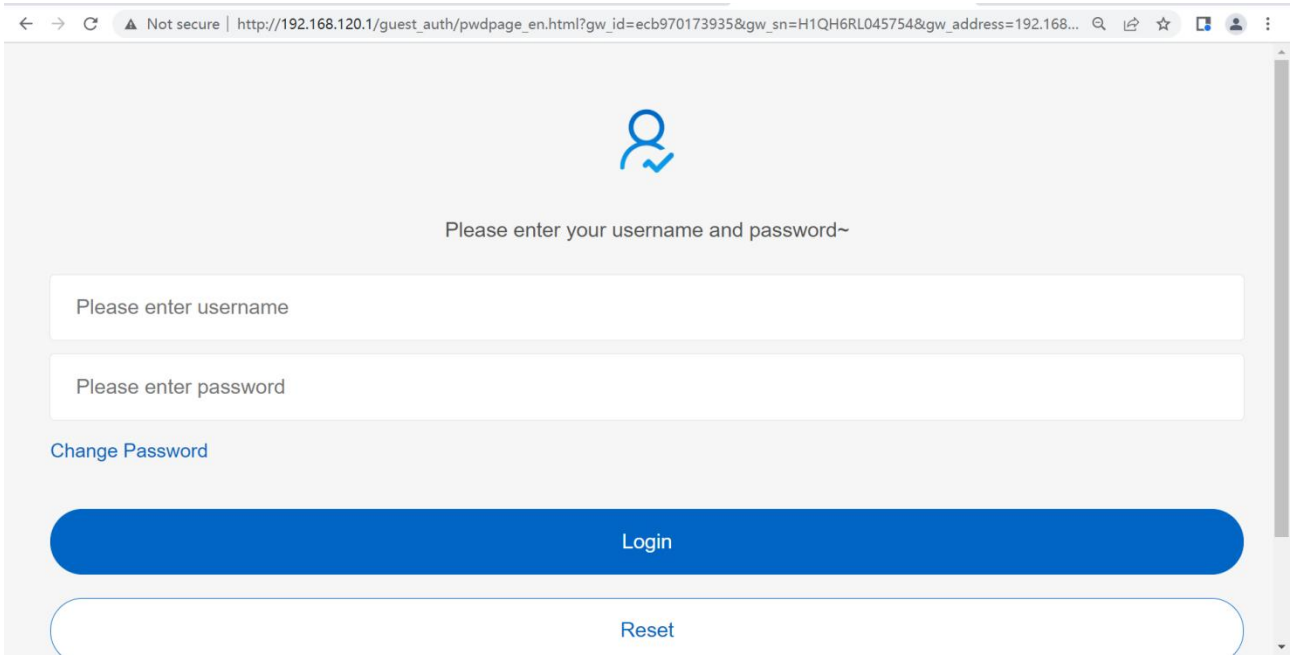
Auth IP/IP Range: The IP of the client who needs to do authentication. The IP can't overlap with other auth IP.

2. Add the account used by clients, up to 200 accounts can be added.

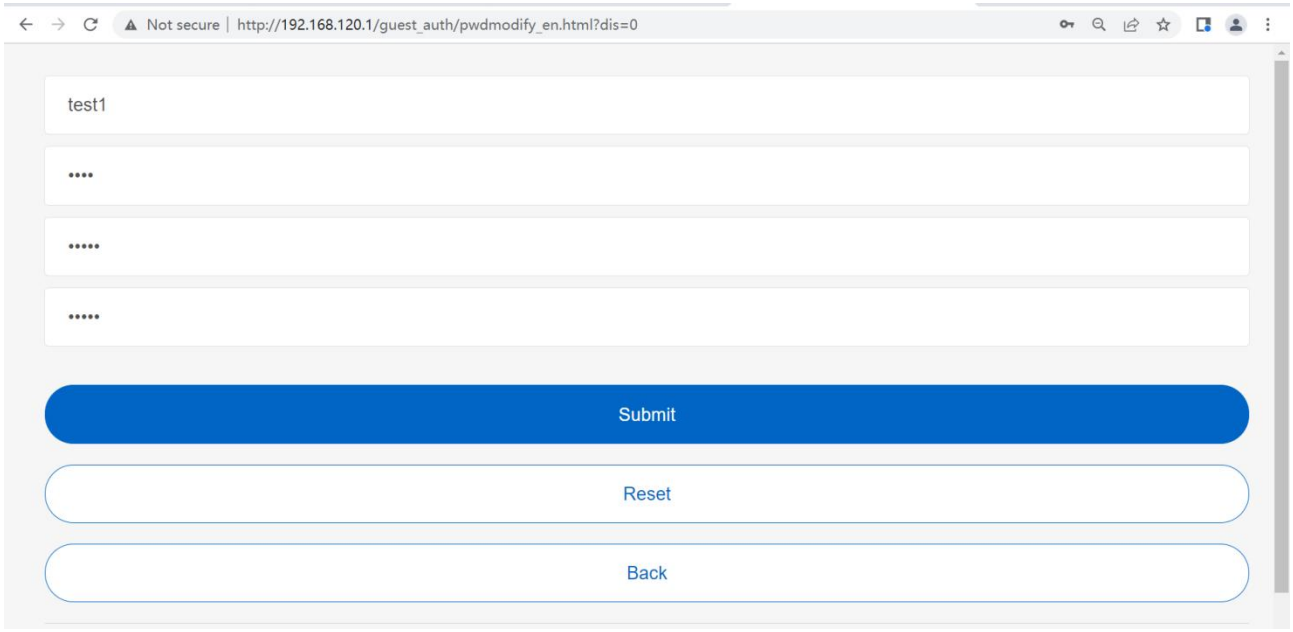


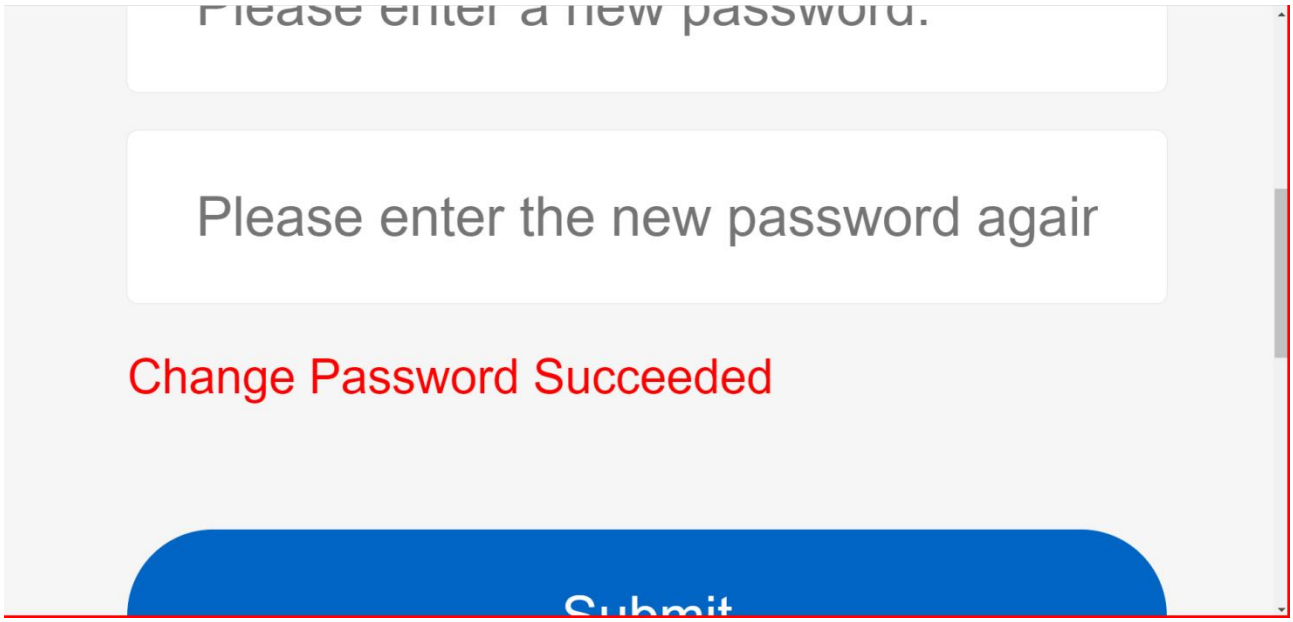
> **Note**
>
> The account can be used by multi clients.

3. Do authentication on PC, normally the portal page will pop-up automatically. If it can't pop-up auto, please try to key in 1.1.1.1 to redirect to portal page (The page will auto showing with English or Chinese based on your browser language setting).

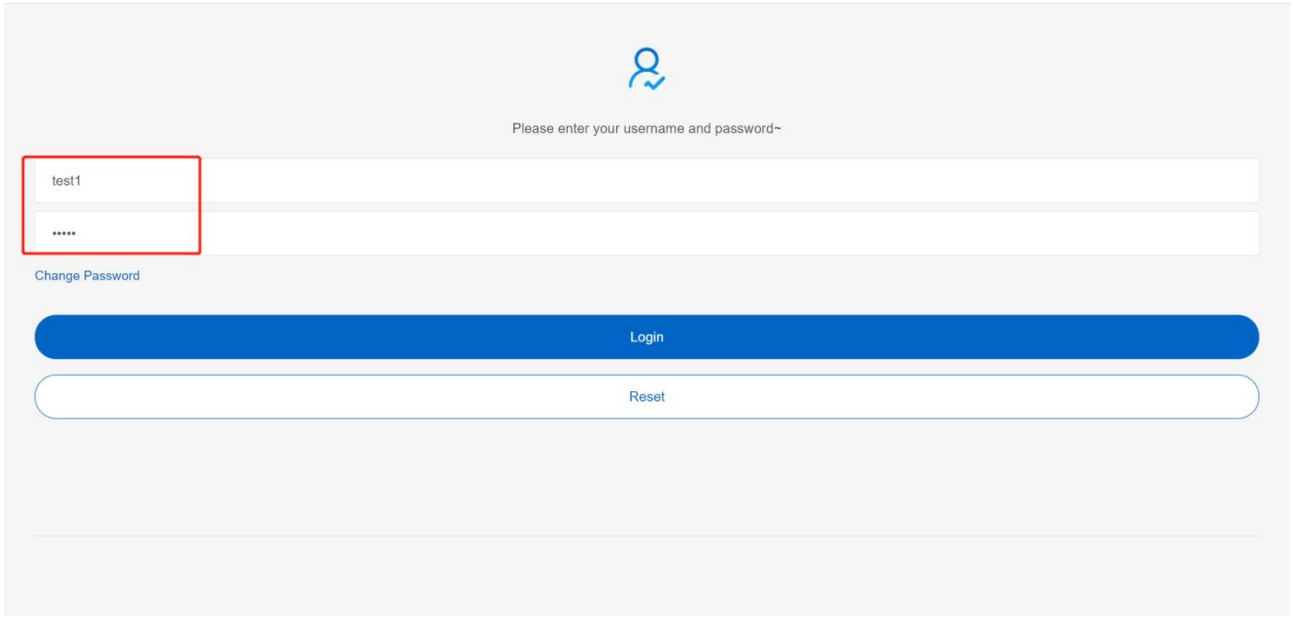


4. Fill the **username** and **password** got from manager, or if you want to change the password, you can click **Change Password.**

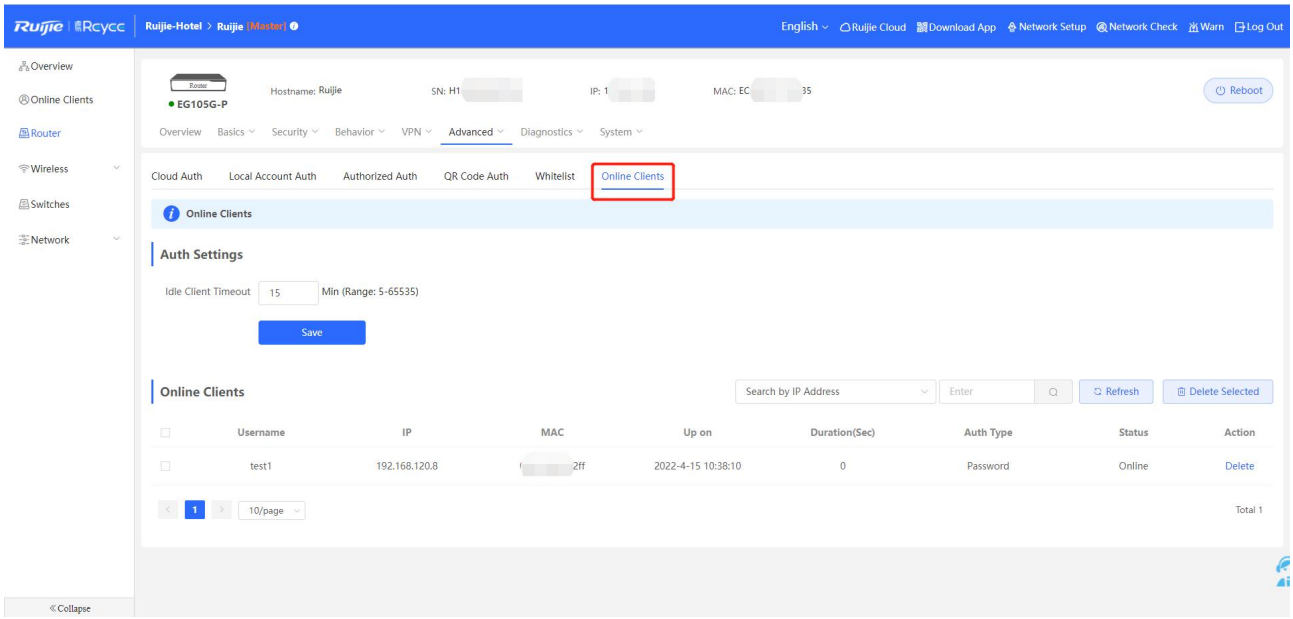




5. Fill the new username and password to login. The page will appear automatically after you login in, then you can access the internet.



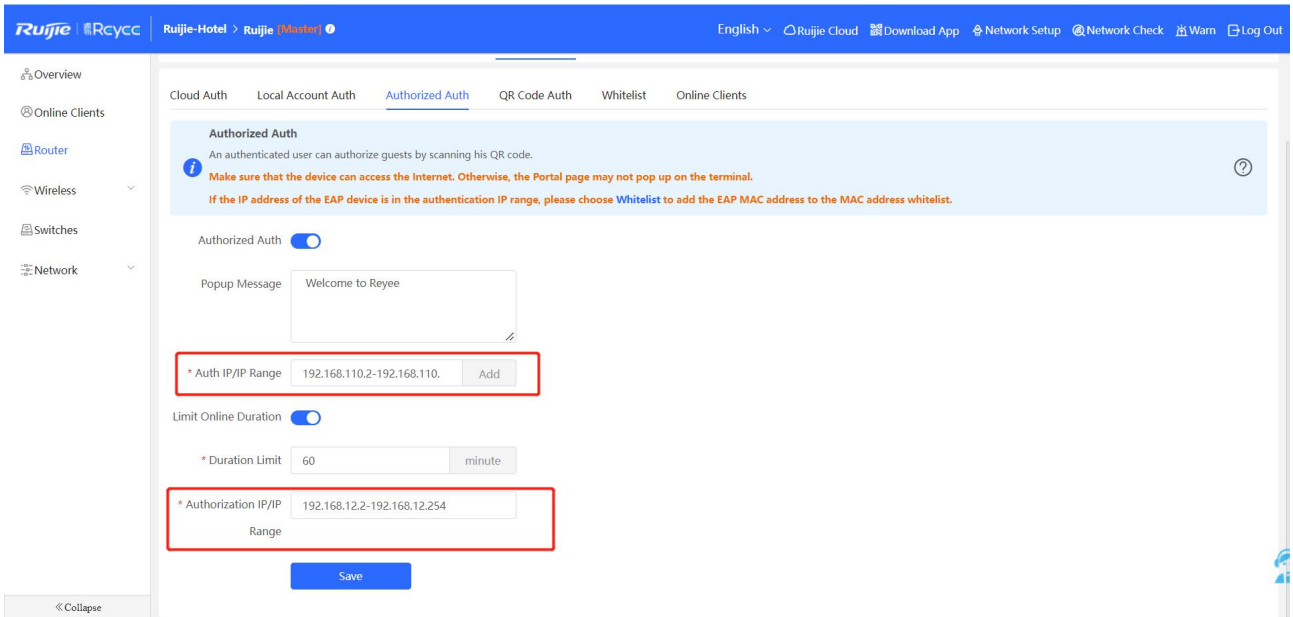
6. Check the online information on EG



4.1.11.3 Authorized Auth

Reyee EG supports **Authorized Auth.** Once this function is enabled the authenticated user can authorize guests by scanning his/her QR code.

1. Click **Router->Advanced->Authentication->Authorized Auth**, then enable it.

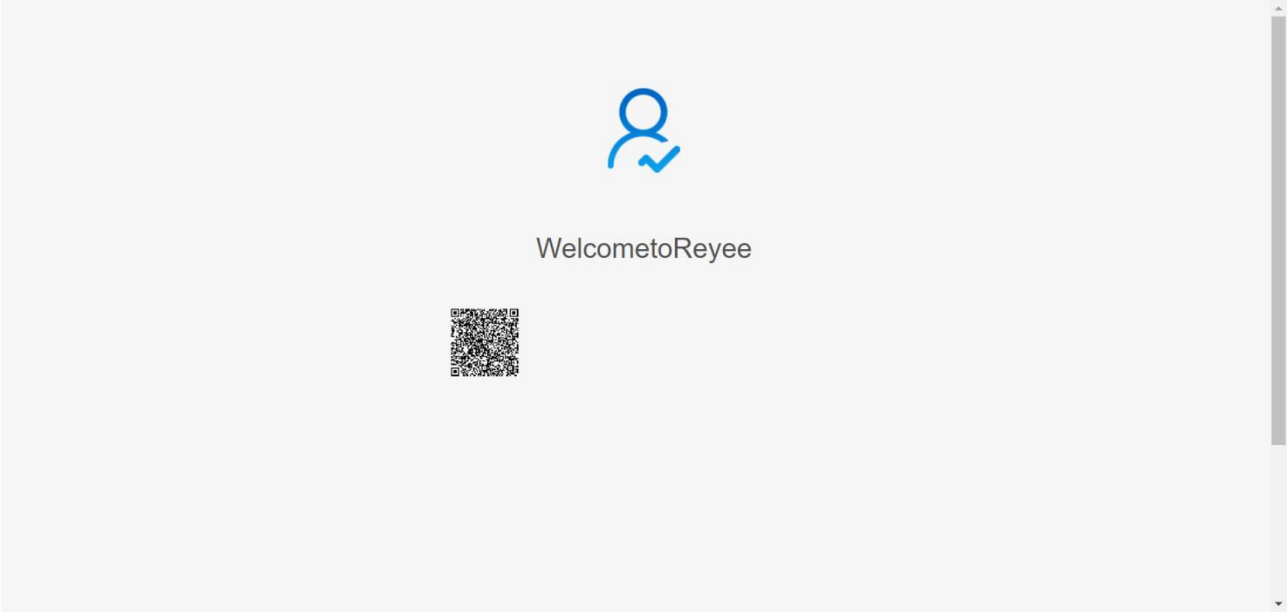


Auth IP/IP Range: The IP of the guest.

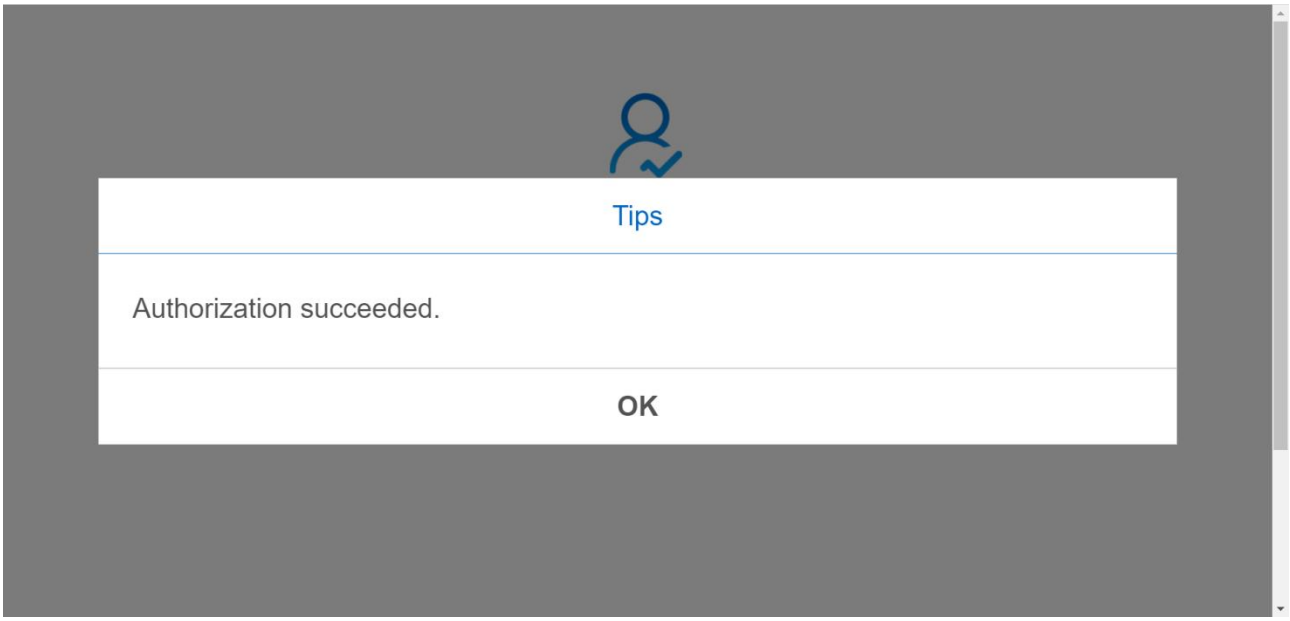
Limit Online Duration: The online duration of guest.

Authorization IP/IP: The IP of the authenticated user.

2. The guest will pop-up the following authentication portal page automatically after he/she connected to the internet.



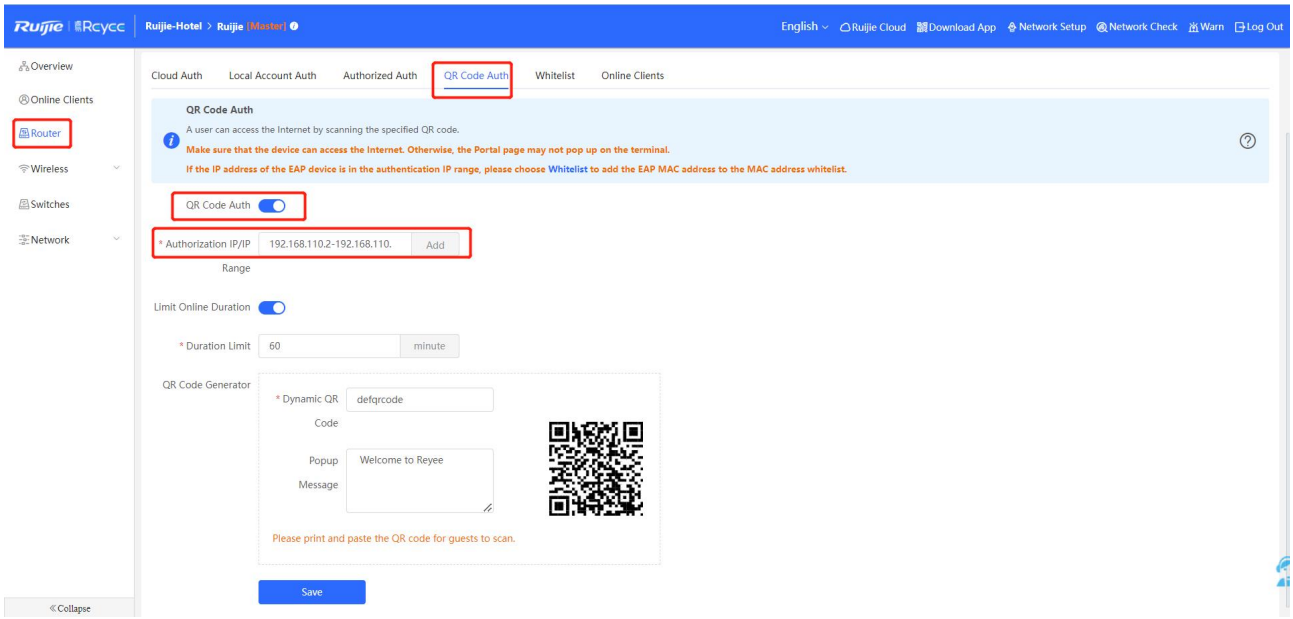
3. After the Authorization clients scan the QR code, the guest authorized succeed, then can access internet.



4.1.11.4 QR Code Auth

Reyee EG supports QR Code Auth. Once this function is enabled, the user can access the Internet by scanning the specified QR code.

1. Click Router->Advanced->Authentication->QR Code Auth, then enable it.

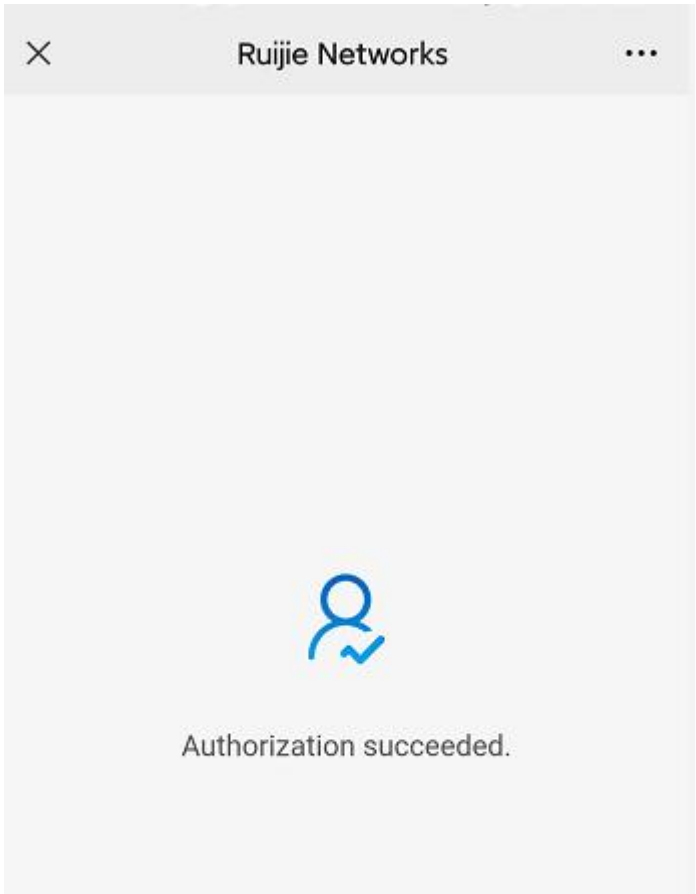


Authorization IP/IP Range: The IP of guest.

Limit Online Duration: The online duration of guest.

QR Code Generator: Please print and paste the QR code for guests to scan.

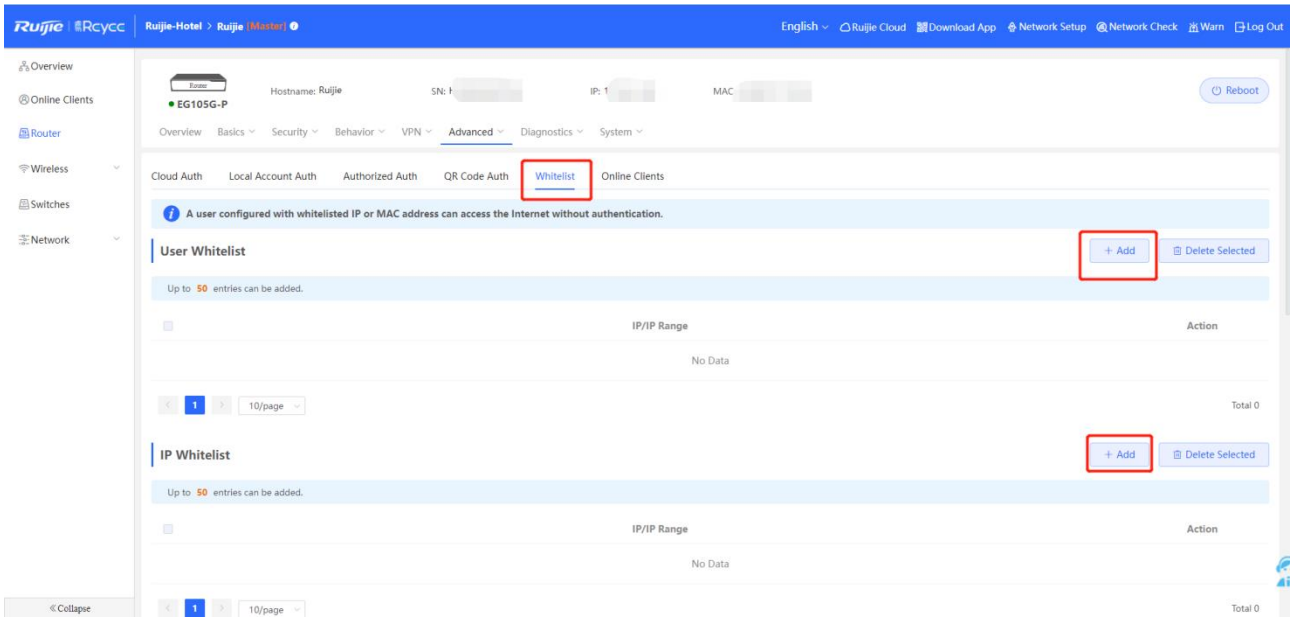
2. The guest scan the QR Code then can access internet.

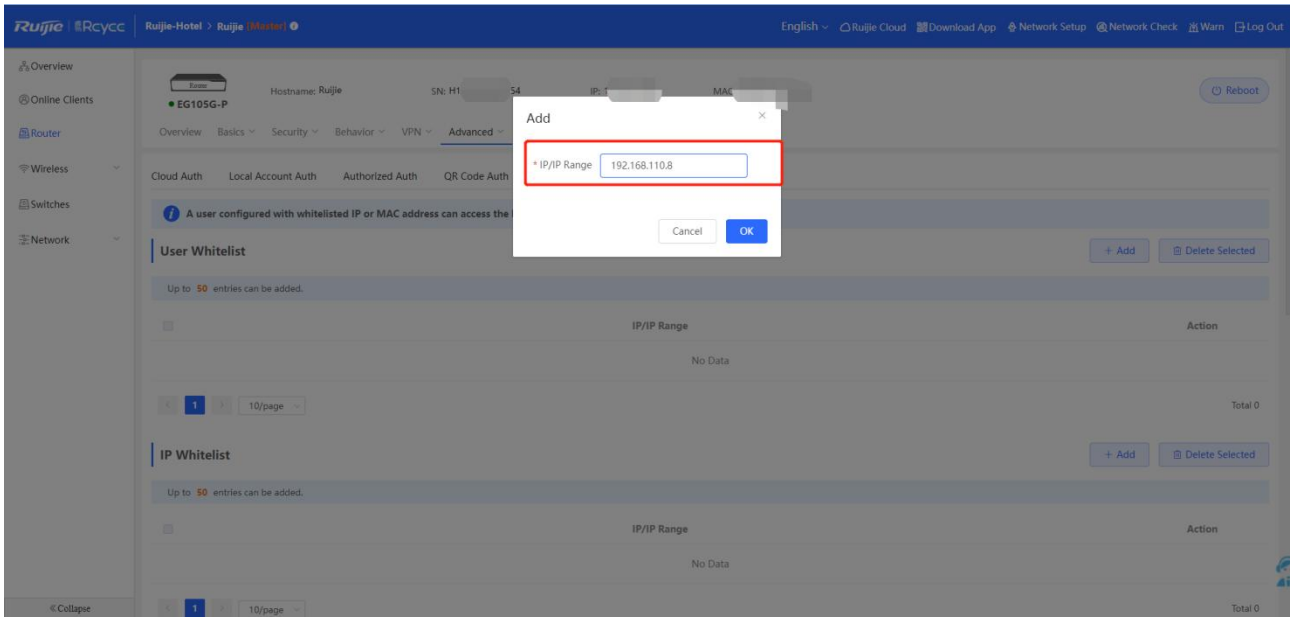


4.1.11.5 Whitelist

A user configured with whitelisted IP or MAC address can access the Internet without authentication.

1. Click **Router->Advanced->Authentication->Whitelist**, add User Whitelist, IP Whitelist, URL Whitelist, MAC Whitelist, MAC Blacklist.



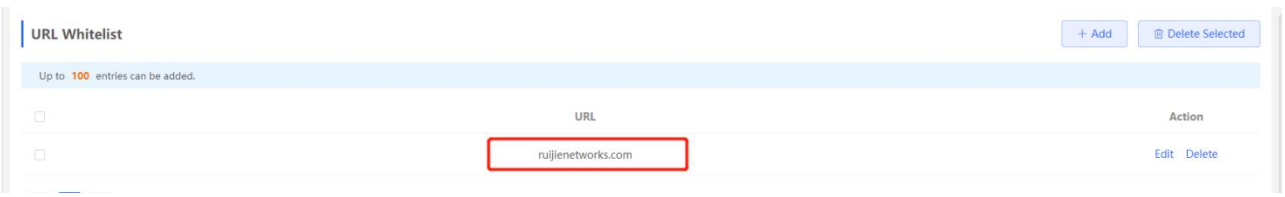


User Whitelist: The user can access internet without authentication. Up to 50 entries can be added.

IP Whitelist: Users can access this external IP without authentication. Up to 50 entries can be added.

URL Whitelist: Users can access this URL without authentication. Up to 100 entries can be added.

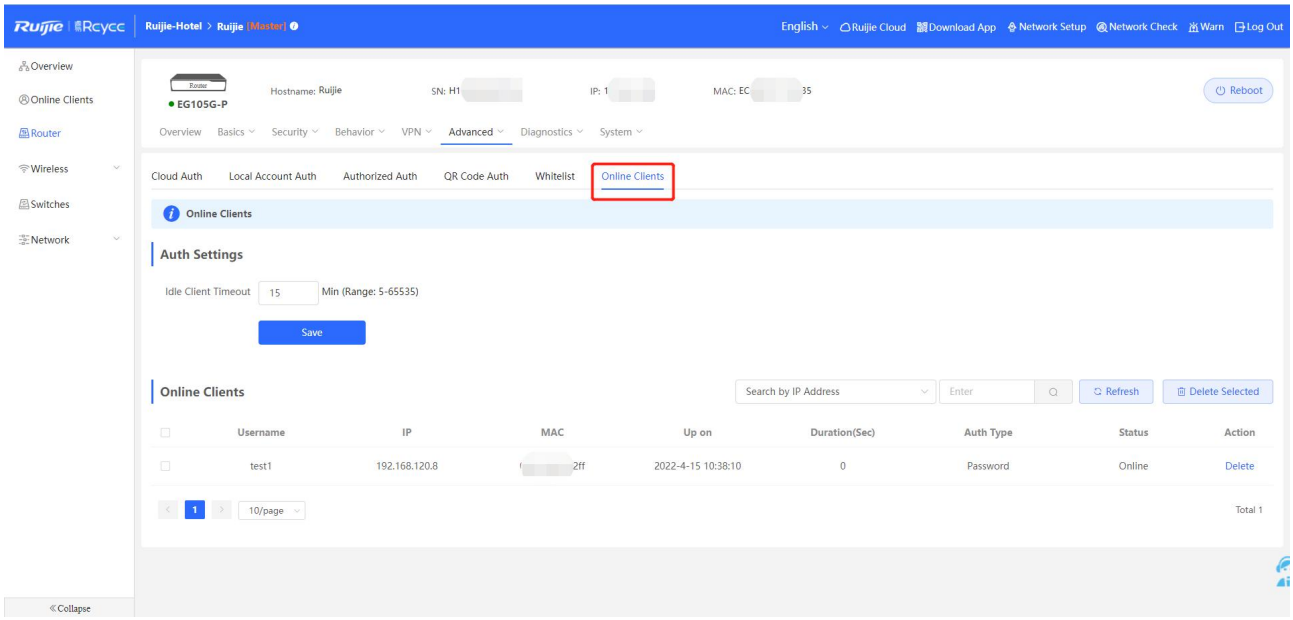
The following URL is the default URL added for the Cloud Auth.



MAC Whitelist: The MAC can access internet without authentication. Up to 250 accounts can be added.

MAC Blacklist: The MAC can't do authentication.

4.1.11.6 Online Clients



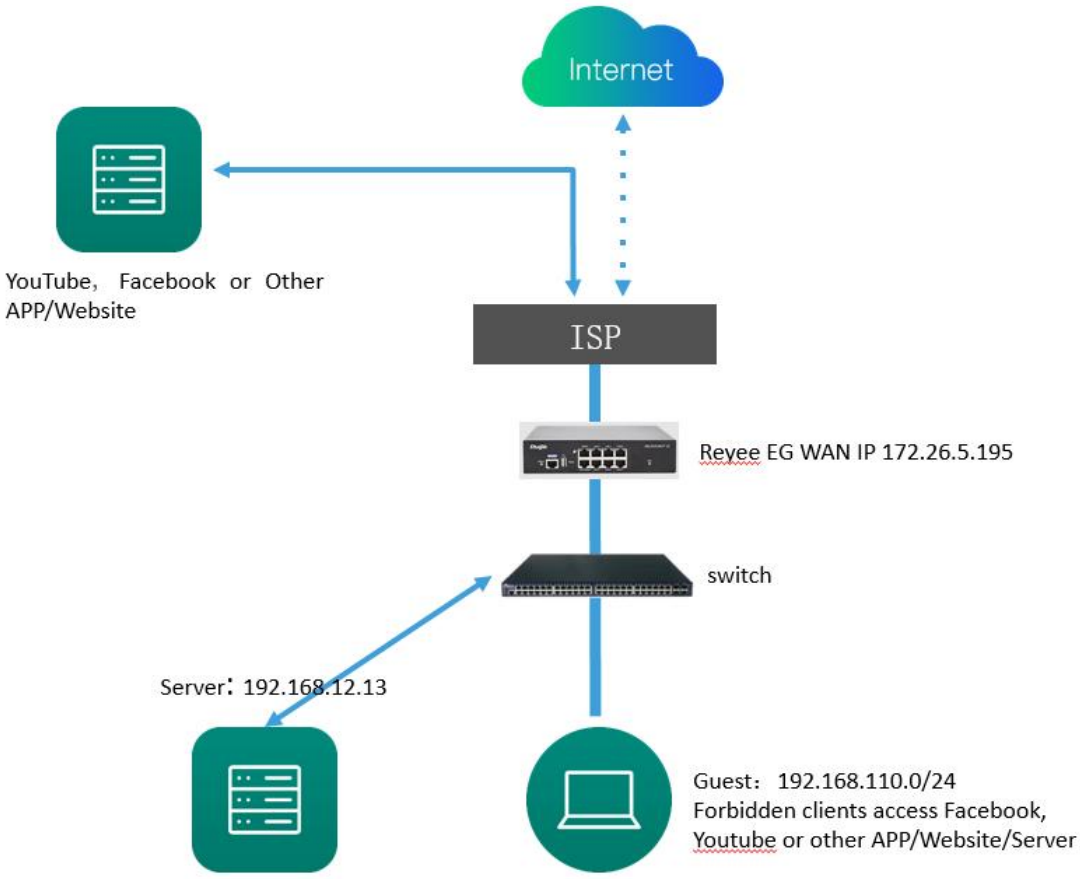
Idle Client Timeout: The idle client will be kicked offline after 15 minutes. (Range: 5-65535 Min)

Search Function: Search by IP Address, Search by MAC, Search by Username.

Delete: The clients will be kicked offline, need to do re-auth then can access internet again.

4.1.12. Behavior

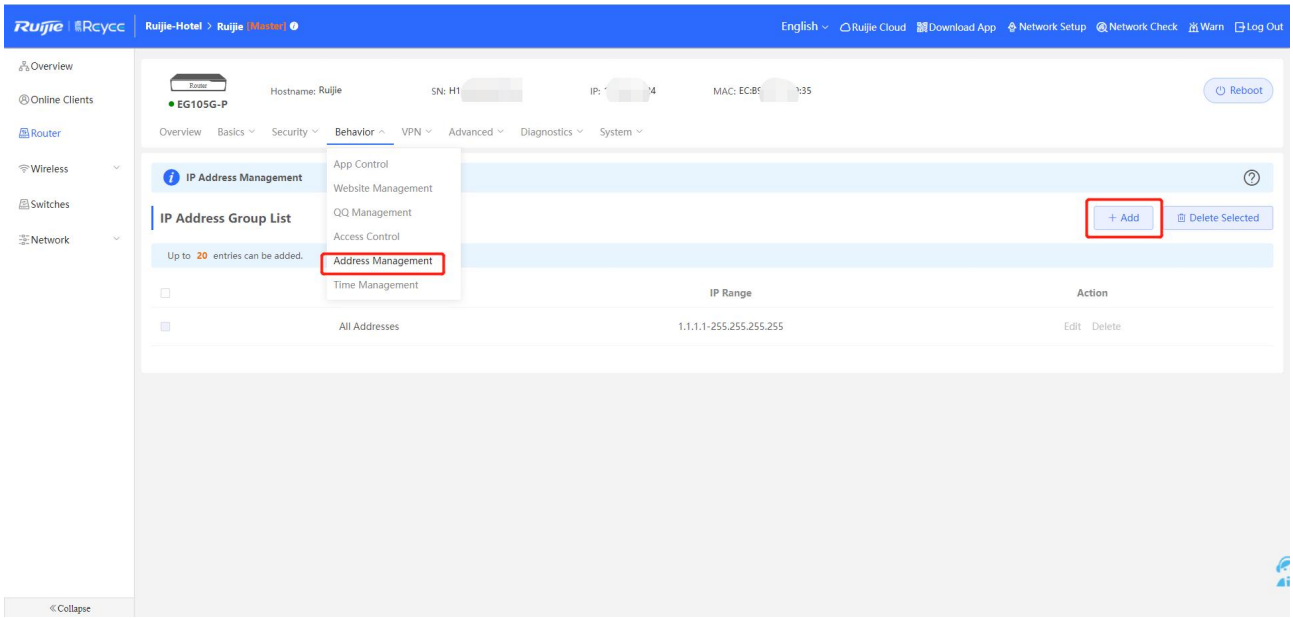
Application Scenario

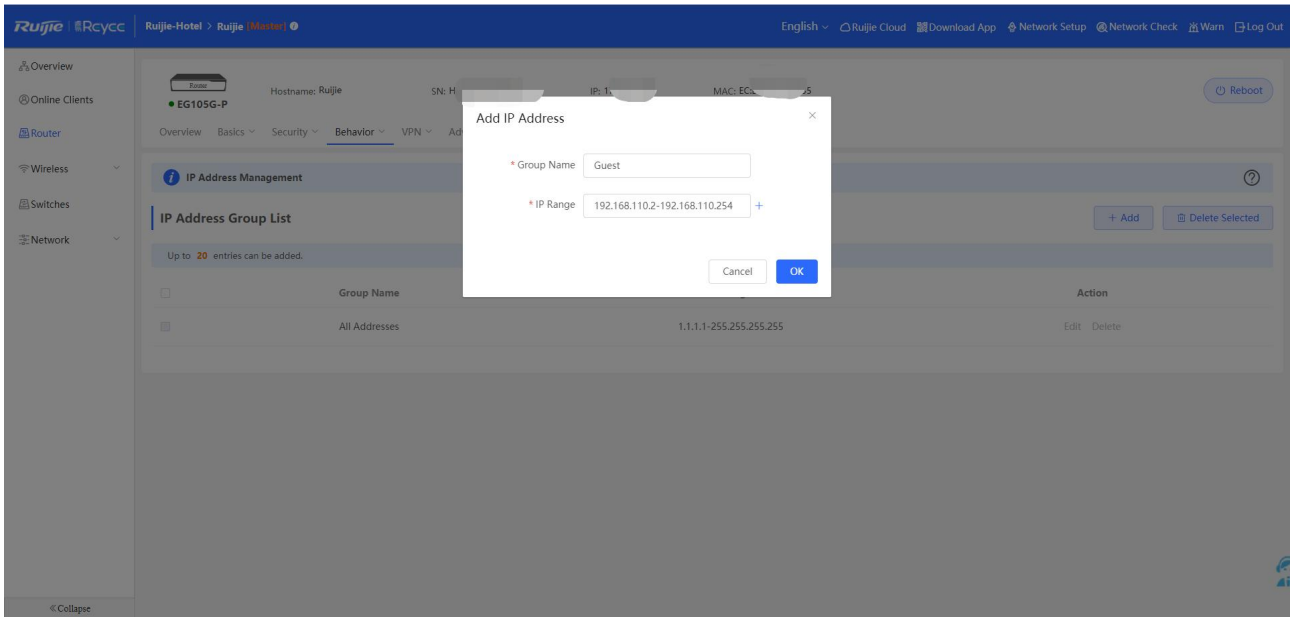


Procedure

4.1.12.1 App Control

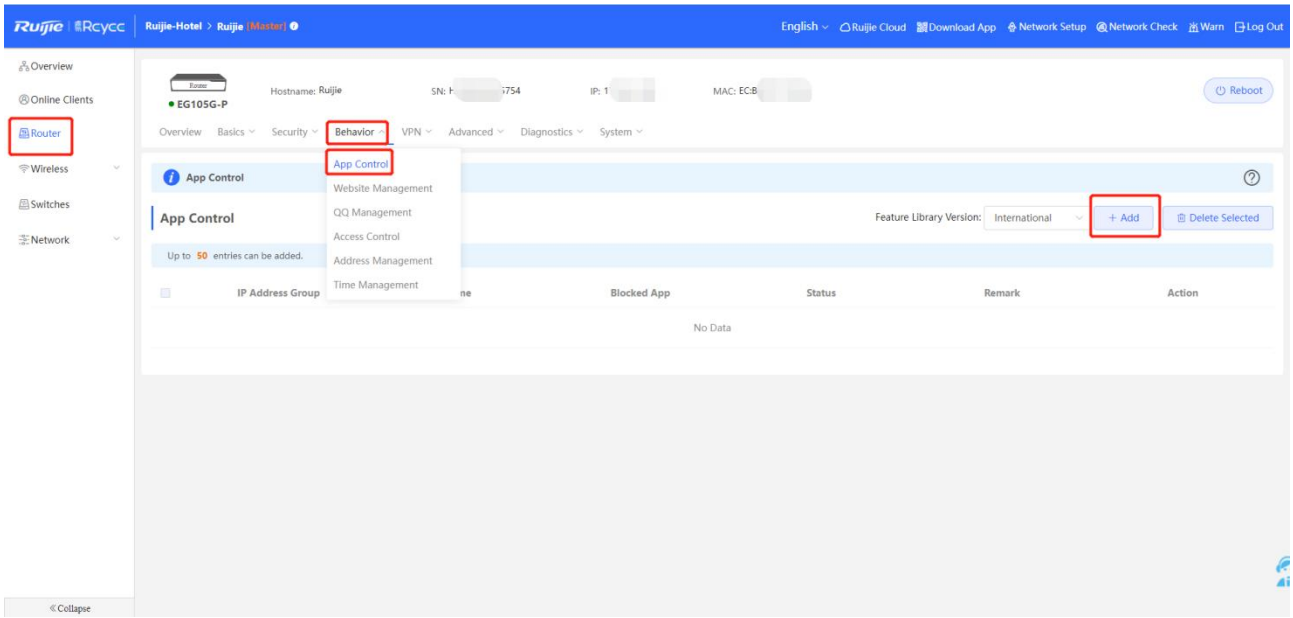
1. Click **Router->Behavior->Address Management** to add the IP address group for clients.

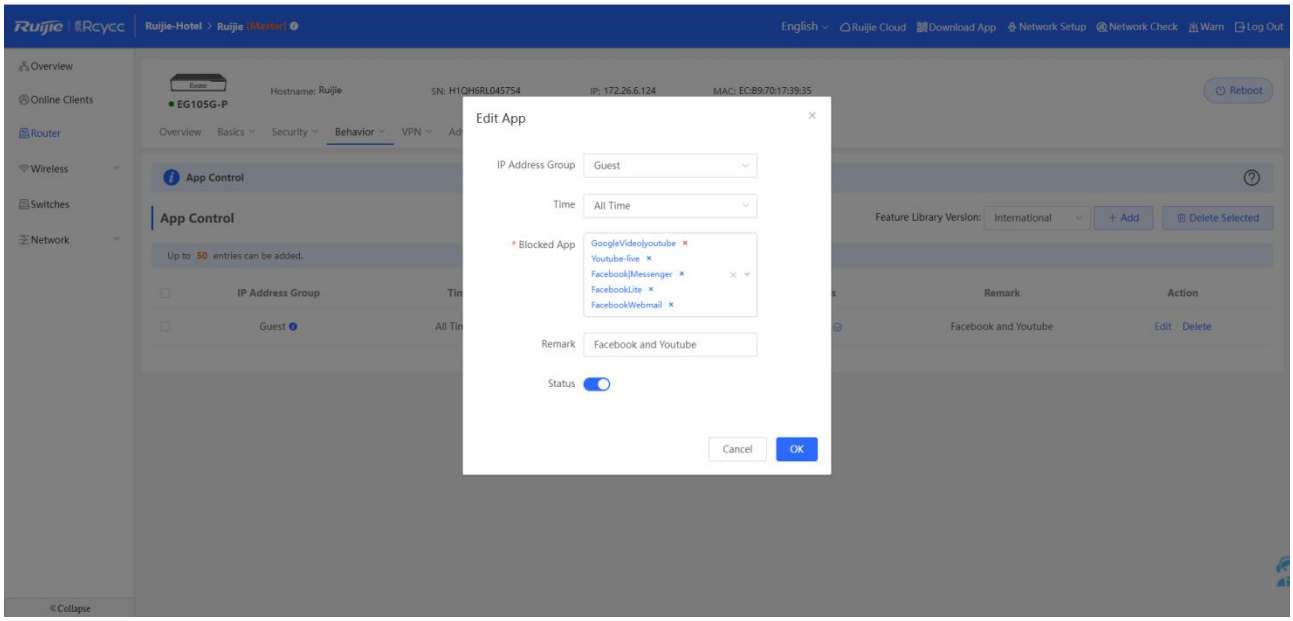




Guest	192.168.110.2-192.168.110.254	Edit	Delete
Server	192.168.12.13	Edit	Delete

2. Click **Router->Behavior->APP Control** to add policy for rejecting the guest to access Facebook and YouTube





IP Address Group： Set a managed IP address group.

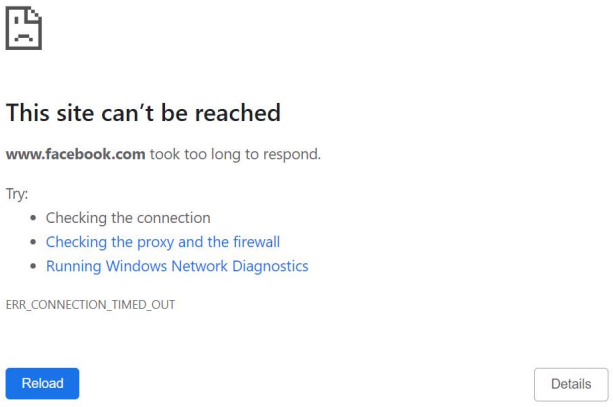
Time： Set a managed time span when managed clients cannot access the blocked application.

Blocked List: Select applications to be blocked.

Remark: Set a remark up with 64 characters long.

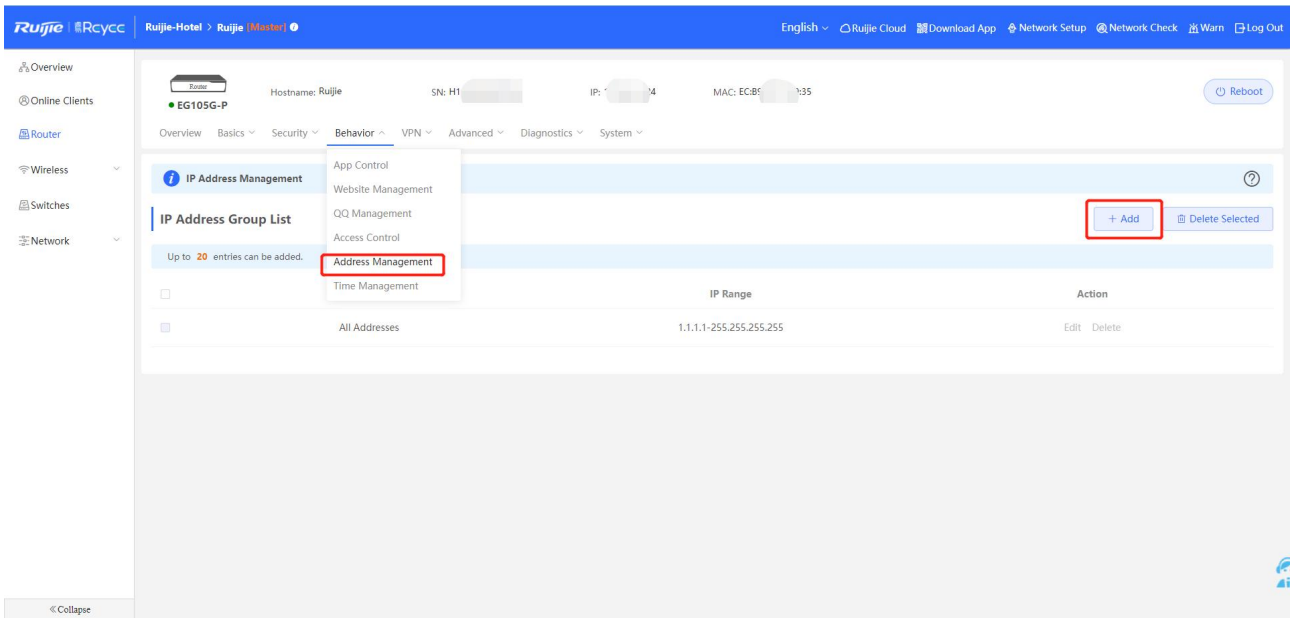
Status: Enable or disable a rule.

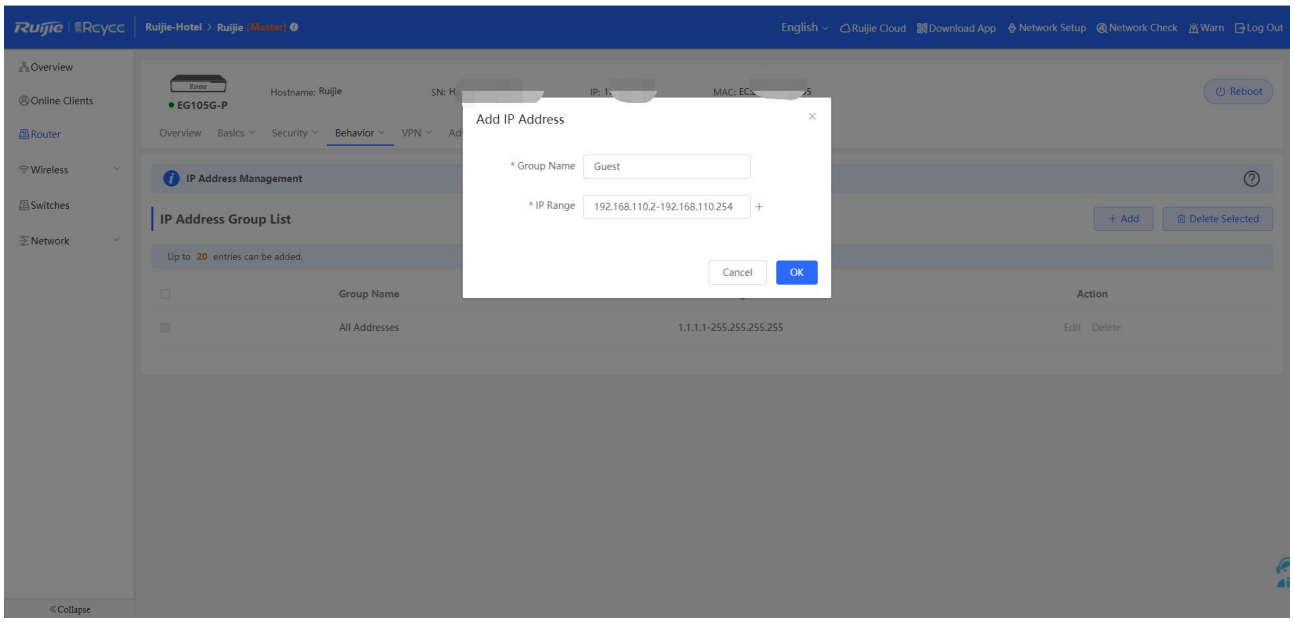
3. Try to access Facebook on Guest PC, failed.



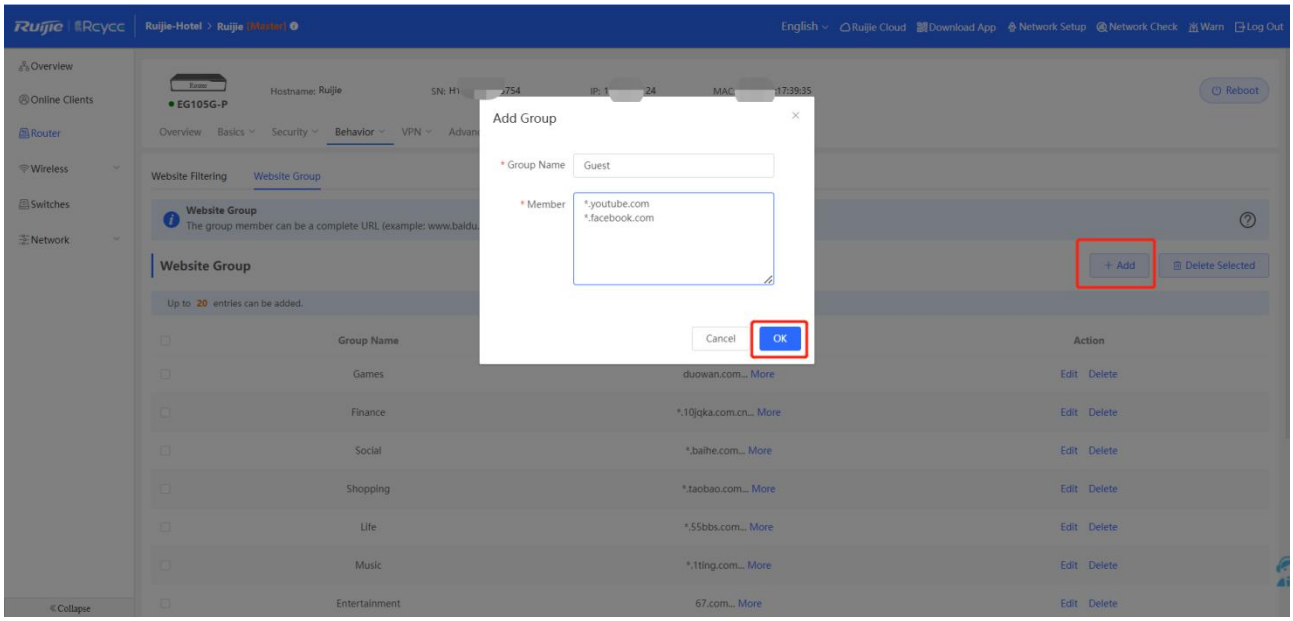
4.1.12.2 Website Management

1. Click **Router->Behavior->Address Management** to add the IP address group for clients.

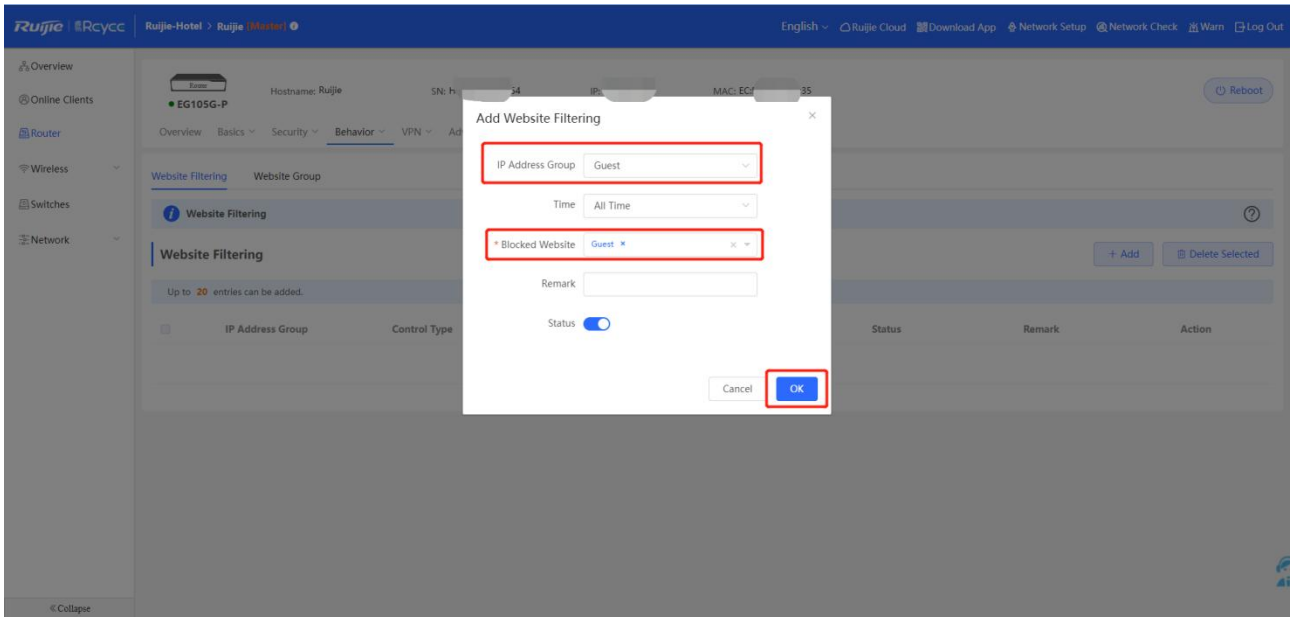




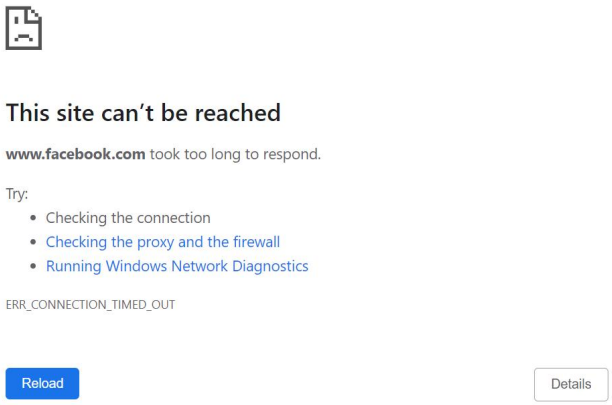
2. Click **Router->Behavior->Website Management** to add policy for rejecting the Guest to access Facebook and YouTube website. Click **Website Group->Add**, fill the group information like following



3. Click **Website Filtering->Add**, choose the IP Address Group and Blocked Website to guest.



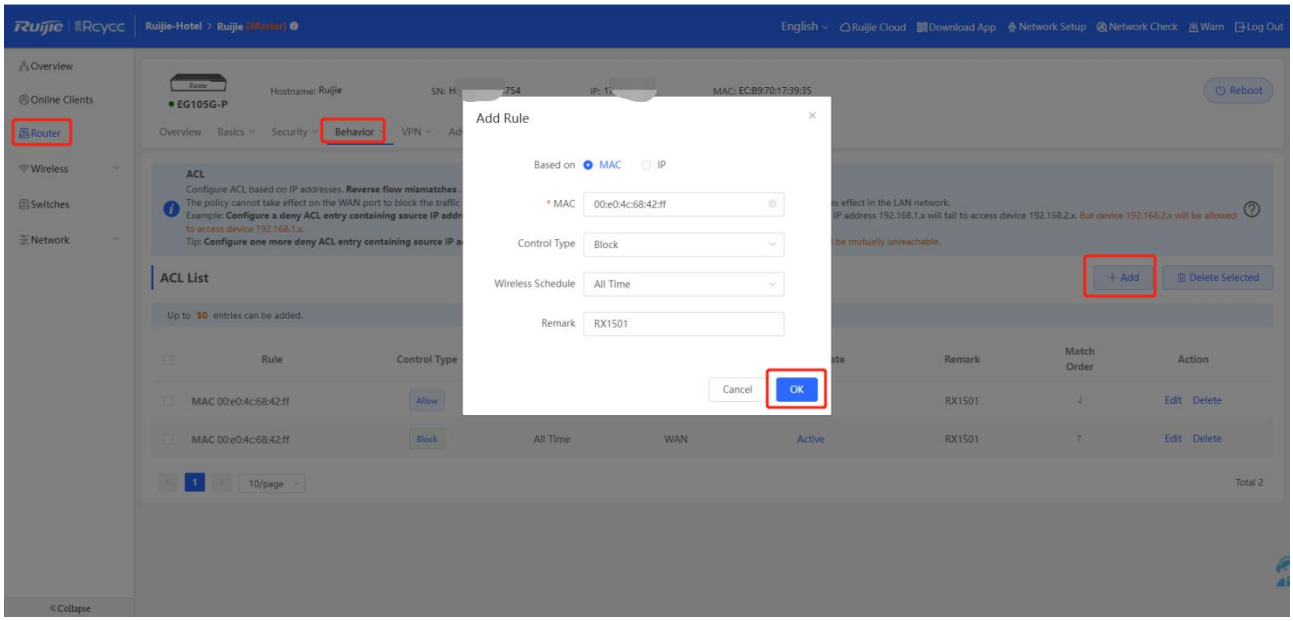
4. Try to access Facebook on Guest PC, then you can see the Facebook page failed.



4.1.12.3 Access Control

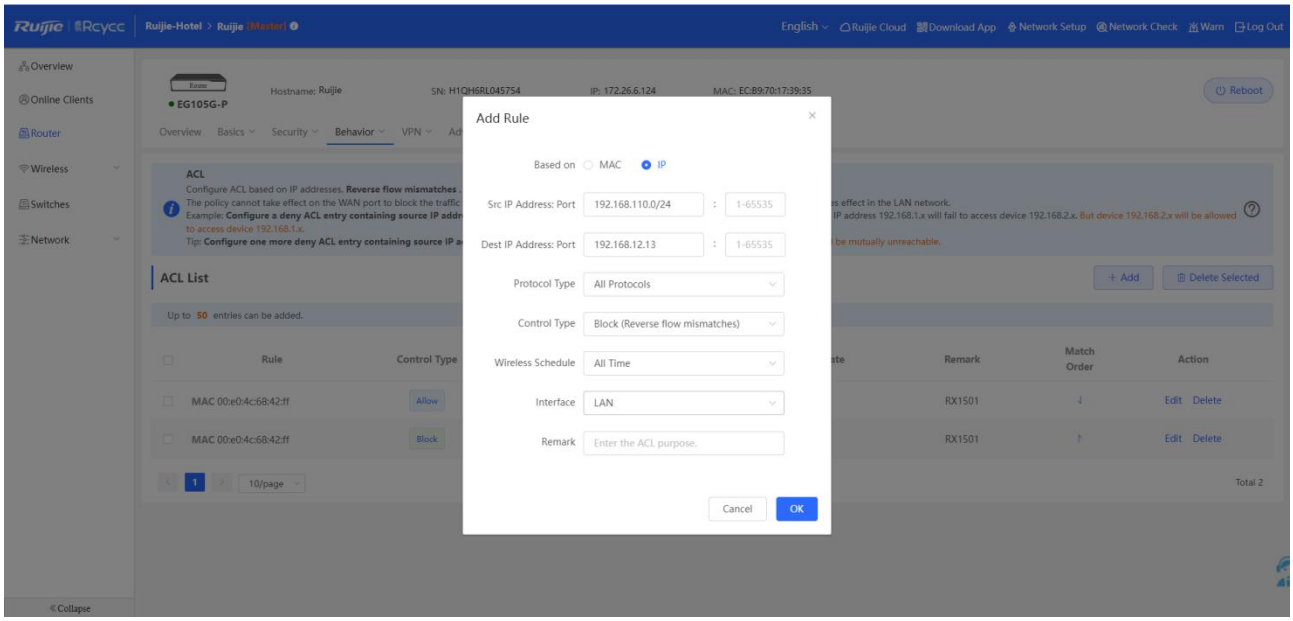
Configure Access Control to block/allow client A to access internet, or block/allow Clients A to Clients B.

1. Click **Router->Behavior->Access Control-> Add**, choose MAC to block or allow the clients based on MAC. The policy will take effect from top to button.



2. Choose IP to block/allow Clients A to Clients B based on IP.

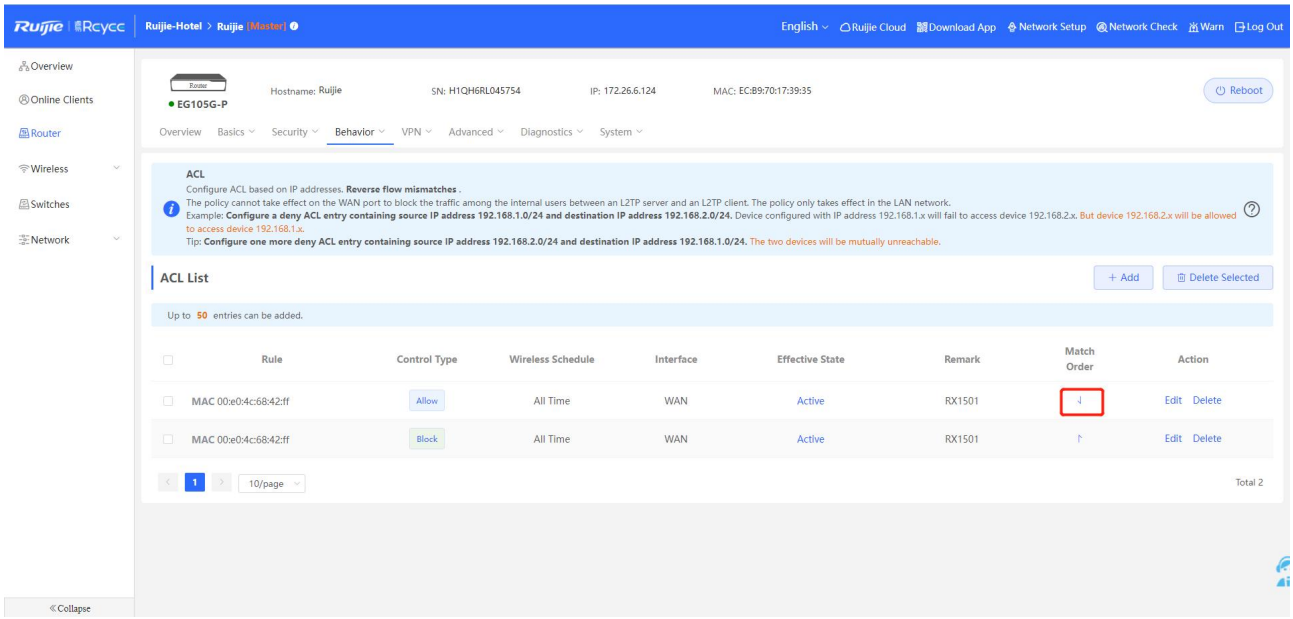
Example: Block Guest (192.168.110.0/24) to access Server(192.168.12.13)



Wireless schedule: Effective schedule.

Interface: Since Guest and Server both are in LAN network, it is recommended to choose LAN port.

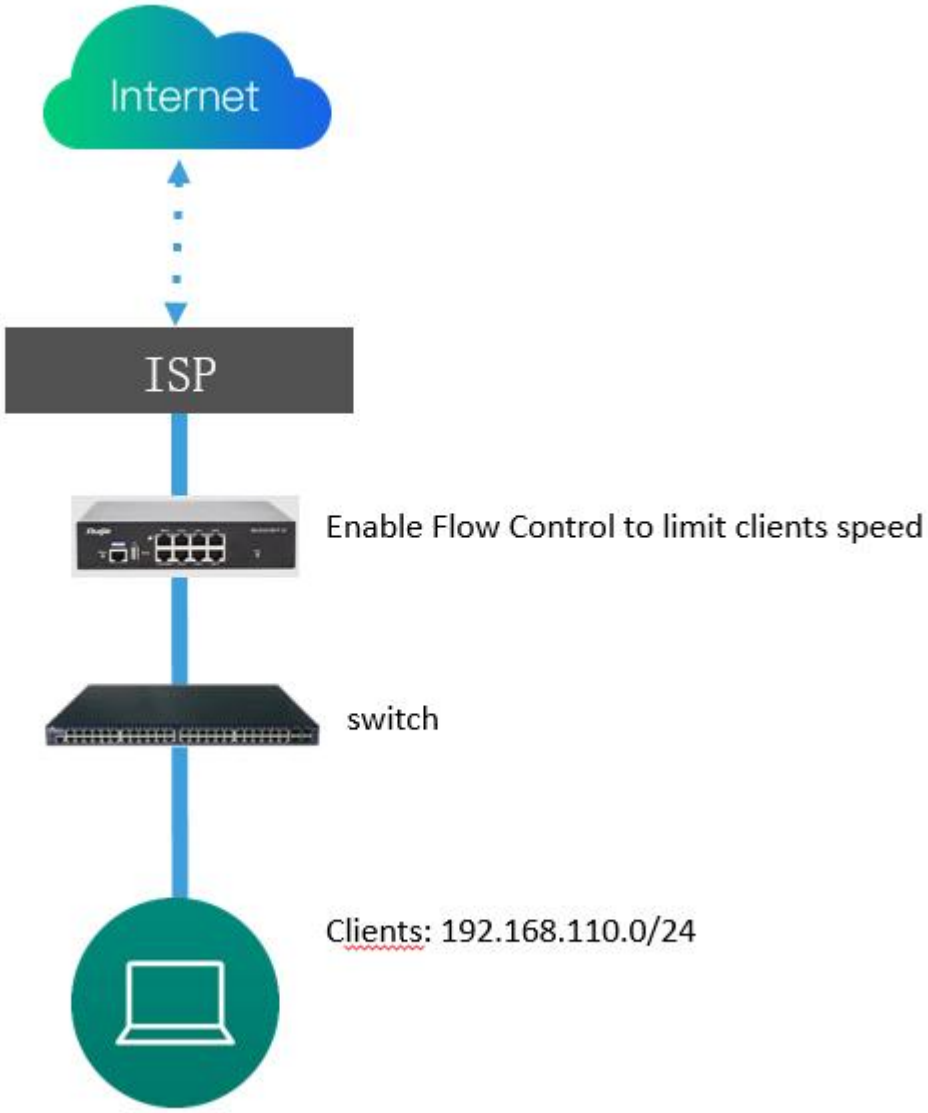
3. Click **Match Order** to move up or down the policy.



> **Note**
>
> The policy cannot take effect on the WAN port to block the traffic among the internal users between an L2TP server and an L2TP client. The policy only takes effect when the traffic go from the LAN network.
>
> Example: Configure a deny ACL entry containing source IP address 192.168.1.0/24 and destination IP address 192.168.2.0/24. Device configured with IP address 192.168.1.x will fail to access device 192.168.2.x. But device 192.168.2.x will be allowed to access device 192.168.1.x. Configure one more deny ACL entry containing source IP address 192.168.2.0/24 and destination IP address 192.168.1.0/24. The two devices will be mutually unreachable.

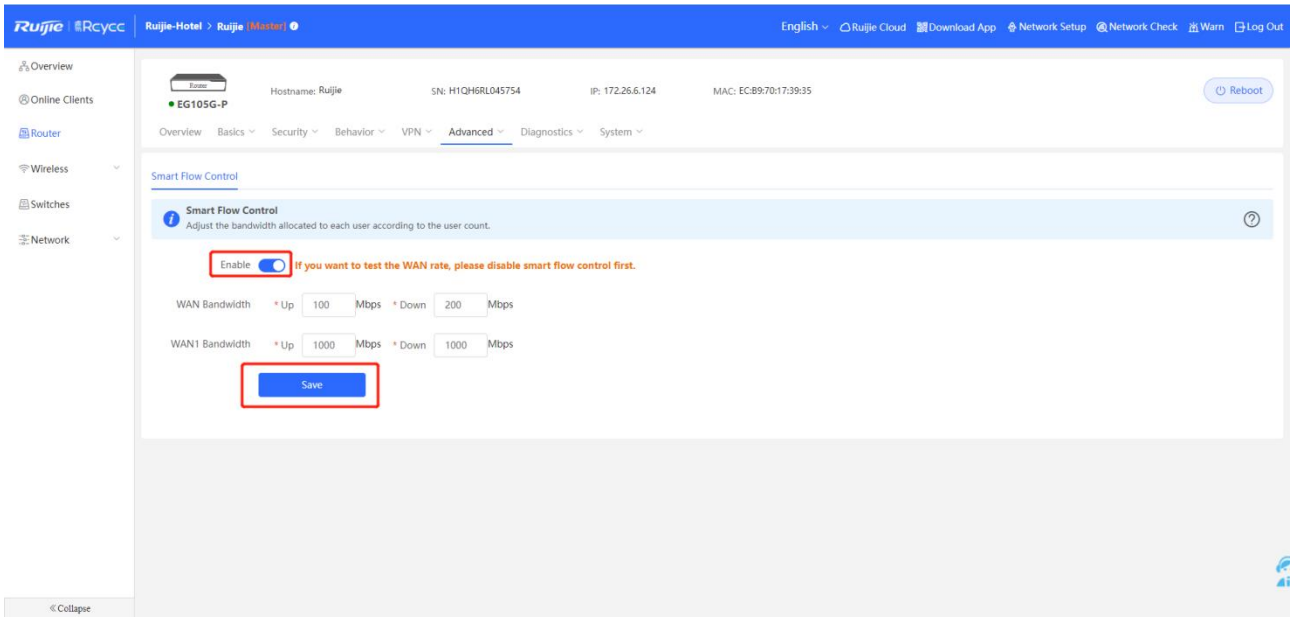
4.1.13. Flow Control

Application Scenario



Procedure

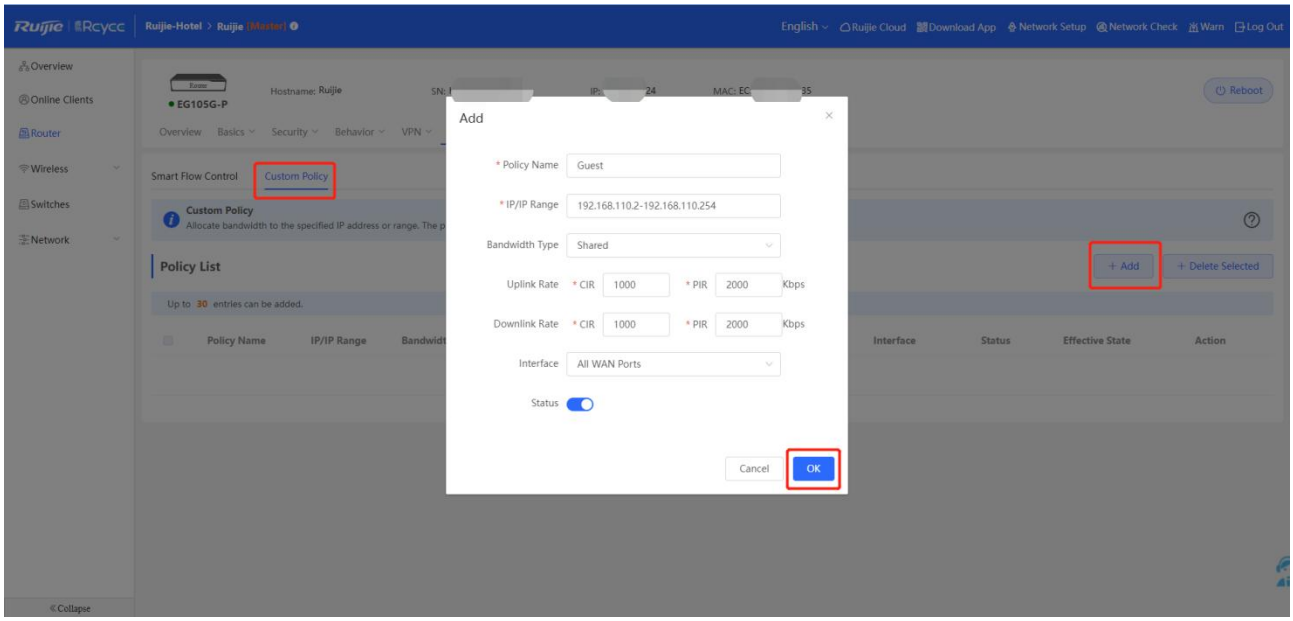
1. Click **Router->Advanced->Flow Control->Enable,** configure the WAN Bandwidth based on reality. For example, ISP give you a cable with uplink 100Mbps and downlink 200Mbps, you can fill up 100 Mbps and down 200 Mbps here, then click Save.



Note

If you want to test the WAN rate, please disable smart flow control first.

2. After enable flow control, you can see a new button Custom Policy. Click it to allocate bandwidth to the specified IP address or range. The priority is sorted as follows: **Custom Policy > Smart Flow Control.**



IP/IP Range: Set an IP address or IP address range.

Bandwidth Type: Shared indicates that all IP addresses share the total bandwidth. Independent indicates that the rate limit is set per IP address.

Uplink Rate:

CIR: CIR indicates the committed information rate.

PIR: PIR indicates the peak information rate.

Downlink Rate:

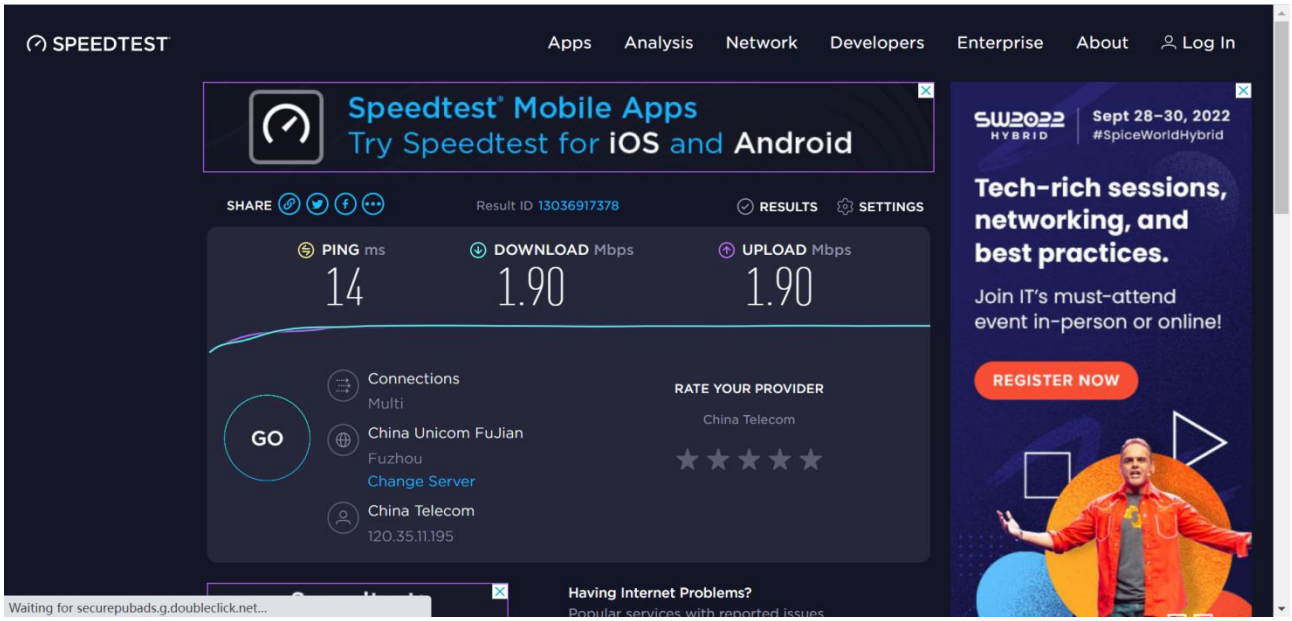
CIR: CIR indicates the committed information rate.

PIR: PIR indicates the peak information rate.

Interface: Select a WAN port which the policy is applied to. If choose All WAN Ports: The policy is applied to all WAN ports.

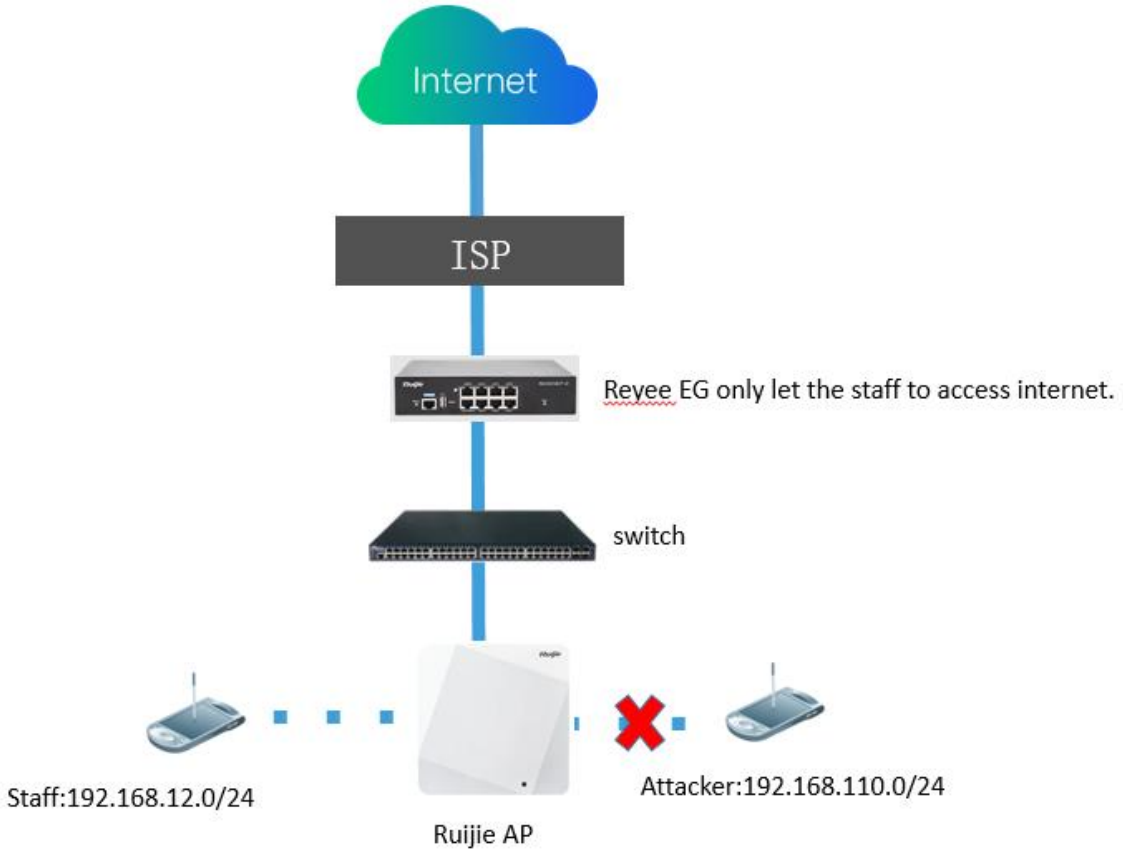
Status: Enable or disable a policy.

3. Do speed test, showing the guest only can reach under 2Mbps



4.1.14. Security

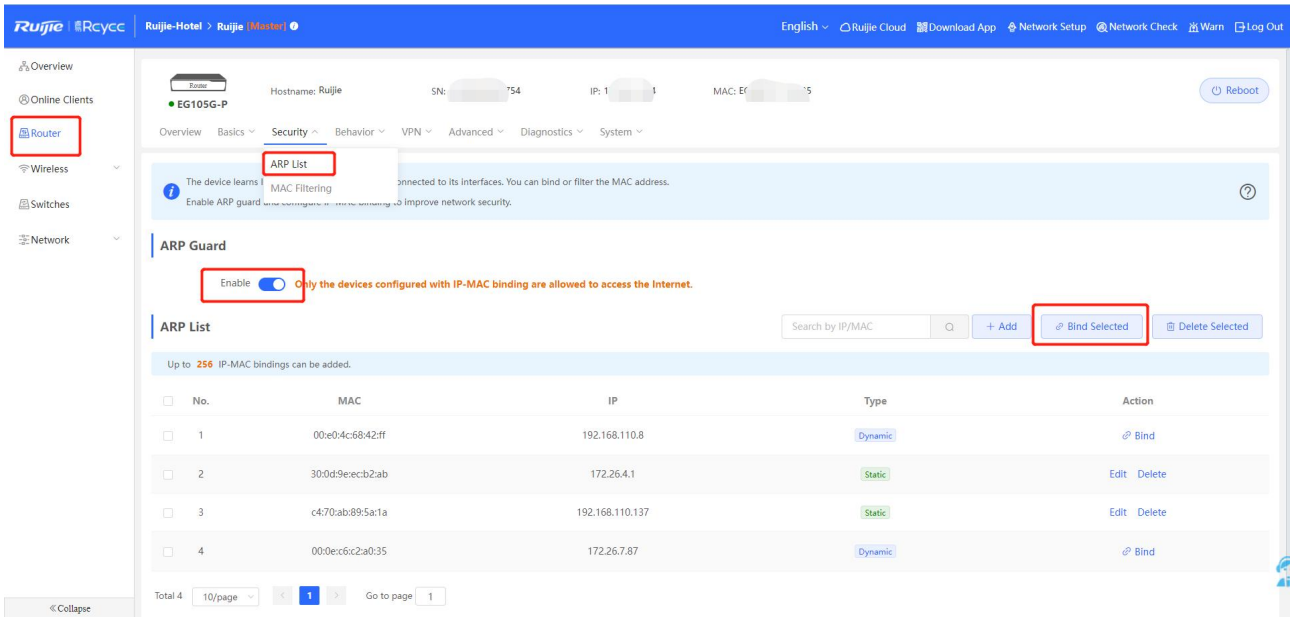
Application Scenario



Procedure

4.1.14.1 ARP List

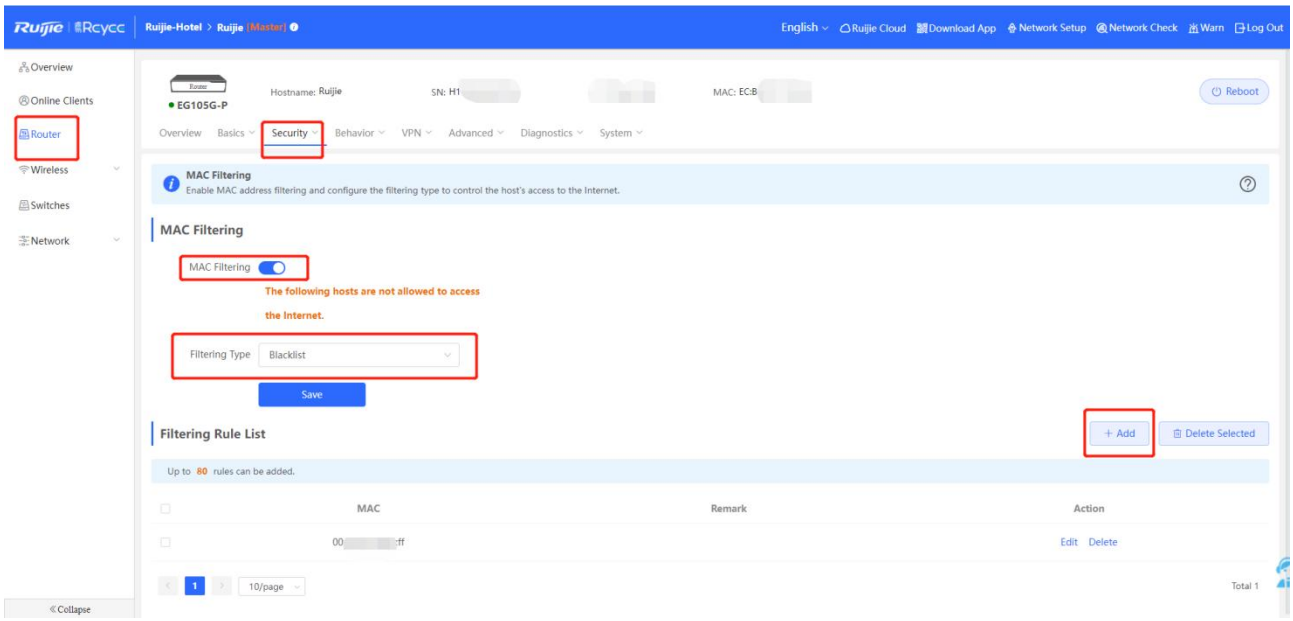
1. Click **Router->Security->ARP List->Enable,** select the clients to bind IP-MAC then only the devices configured with IP-MAC binding are allowed to access the Internet which could avoid the attacker used bandwidth.

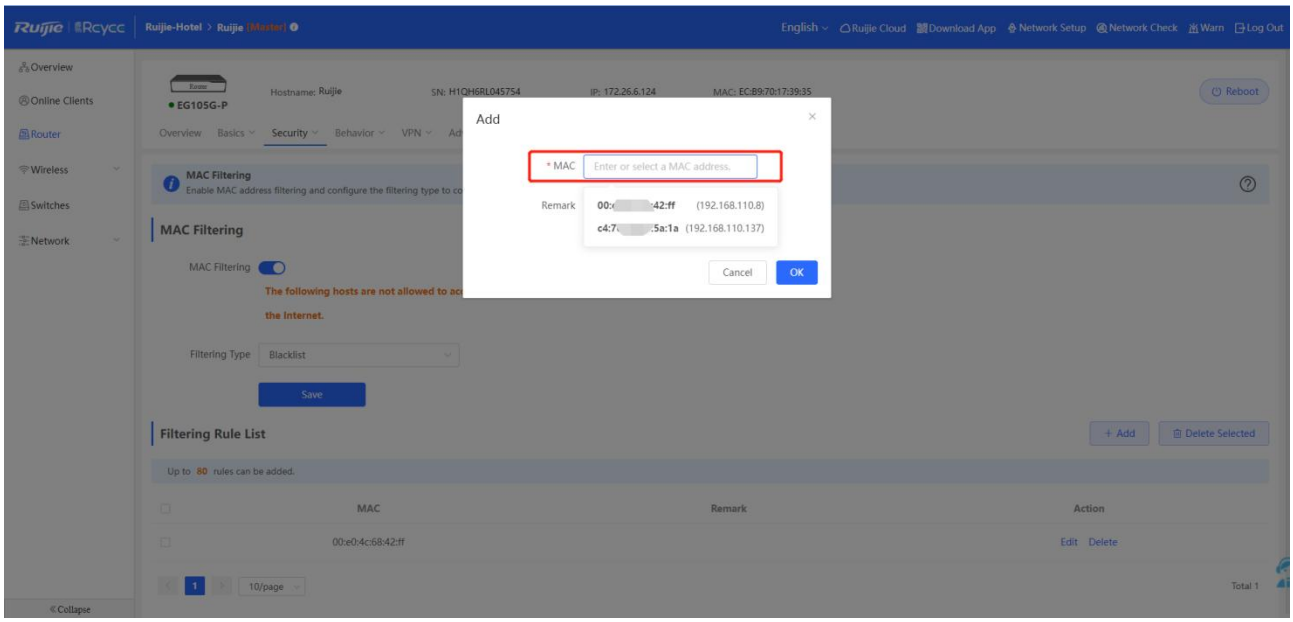


4.1.14.2 MAC Filtering

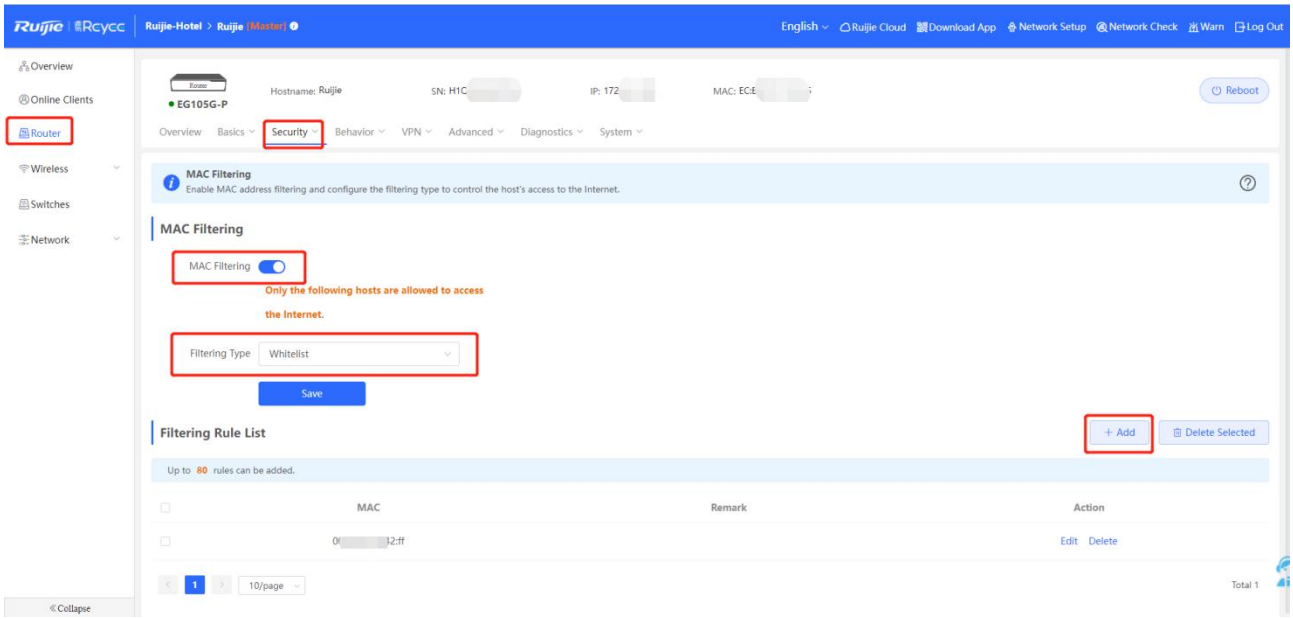
Enable MAC address filtering and configure the filtering type to control the host's access to the Internet.

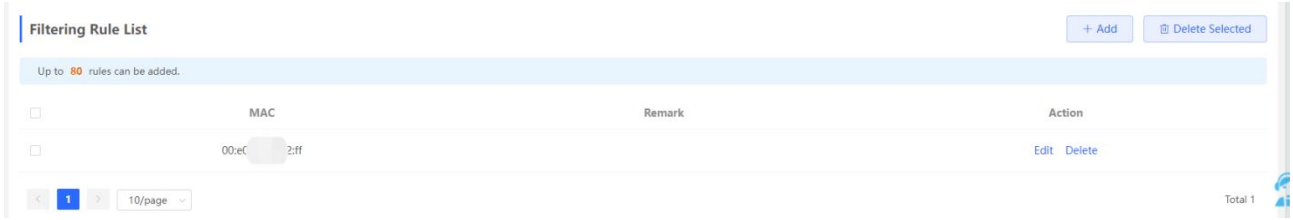
Blacklist Type: The following hosts are not allowed to access the Internet.





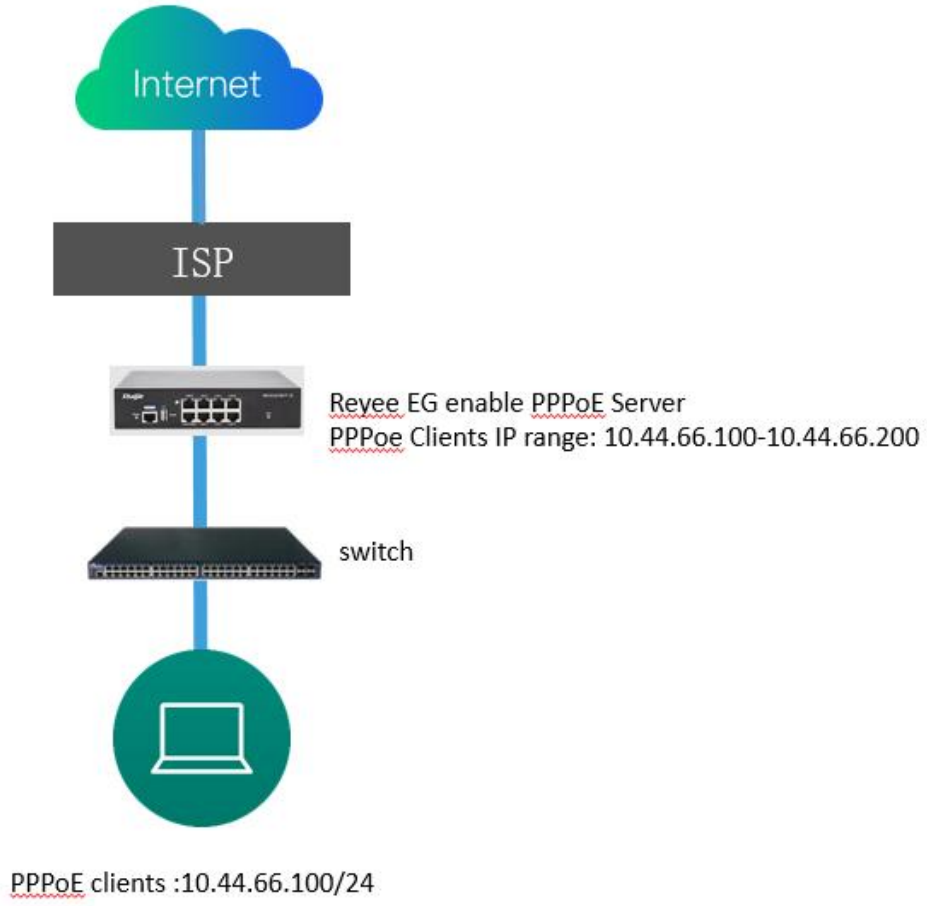
Whitelist Type: Only the following hosts are allowed to access the Internet.





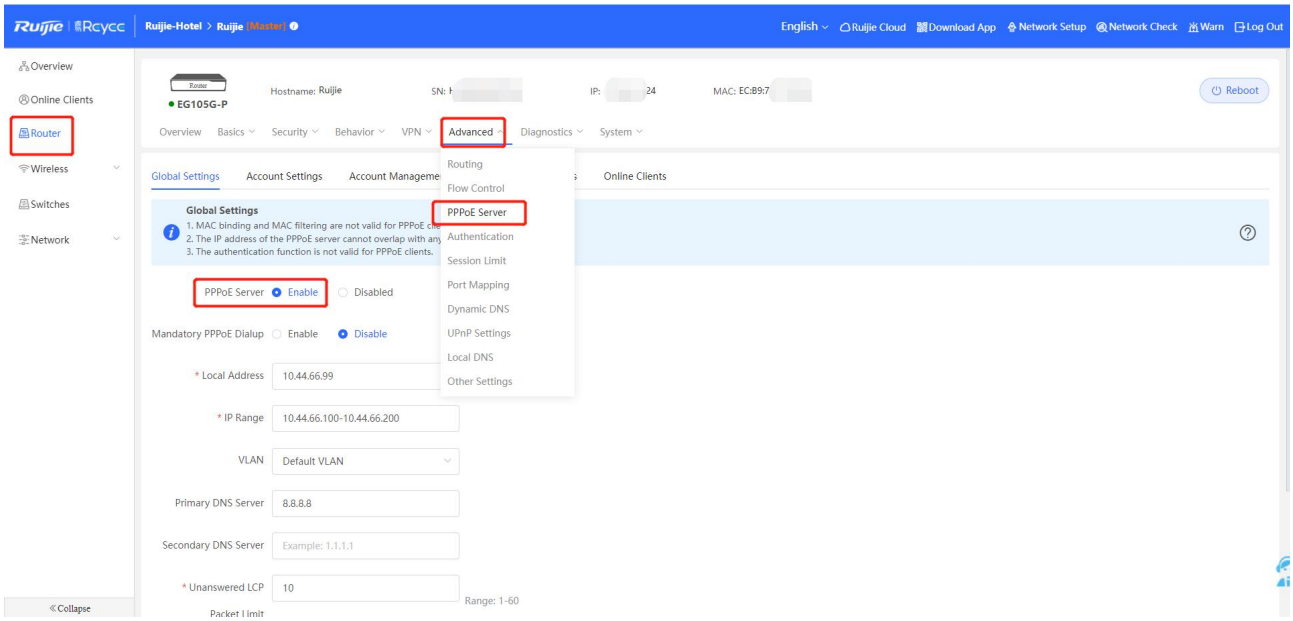
4.1.15. PPPoE Server

Application Scenario



Procedure

1. Click **Router->Advanced->PPPoE Server->Global Settings**, enable **PPPoE Server.**



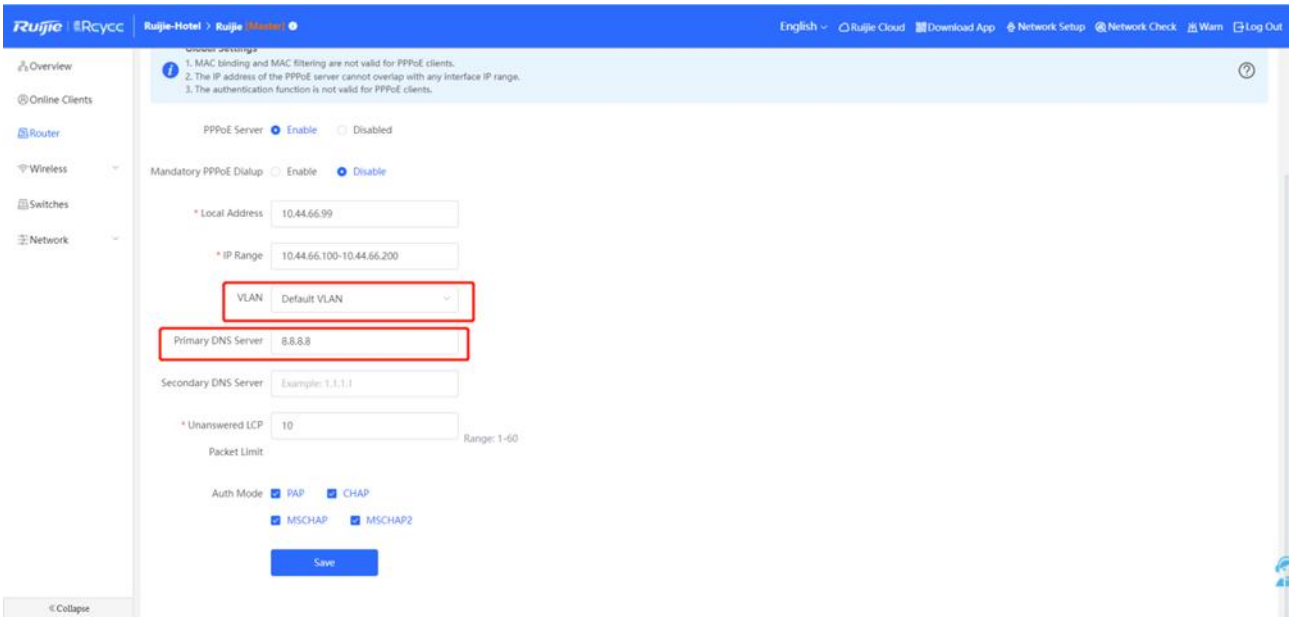
Note

1) MAC binding and MAC filtering are not valid for PPPoE clients.

2) The IP address of the PPPoE server cannot overlap with any interfaces' IP range.

3) The authentication function is not valid for PPPoE clients.

2. Fill PPPoE clients IP range, you can modify it or keep it on default. Choose the VLAN who need to do PPPoE dial up.

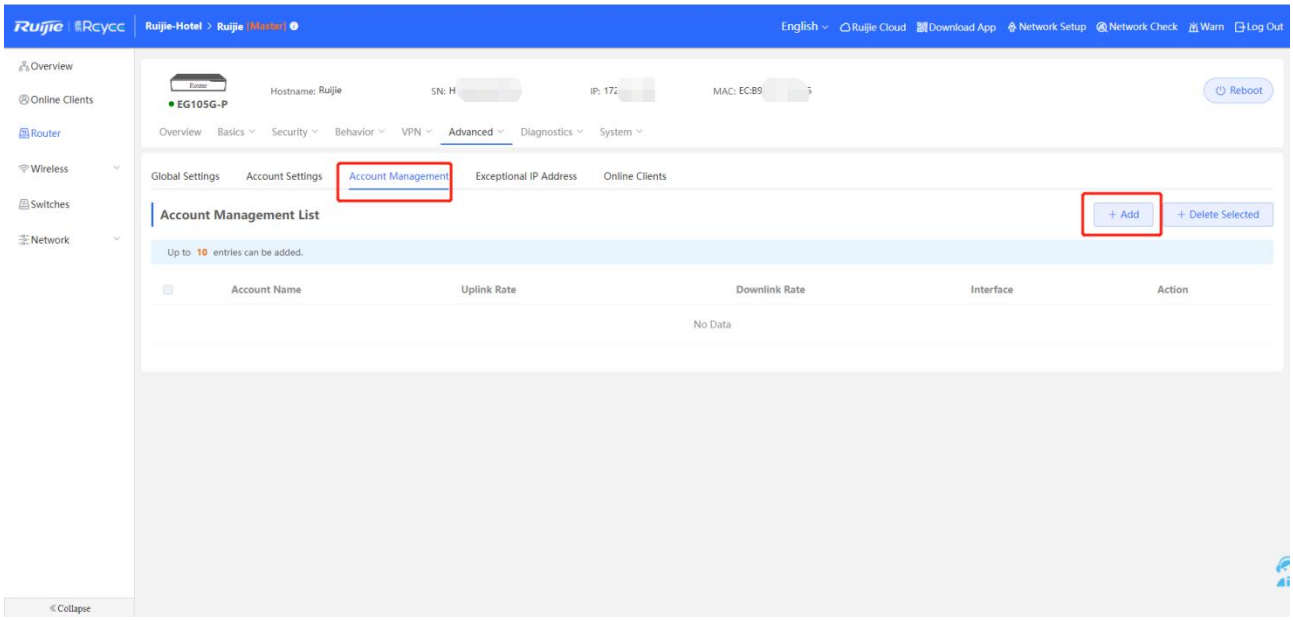


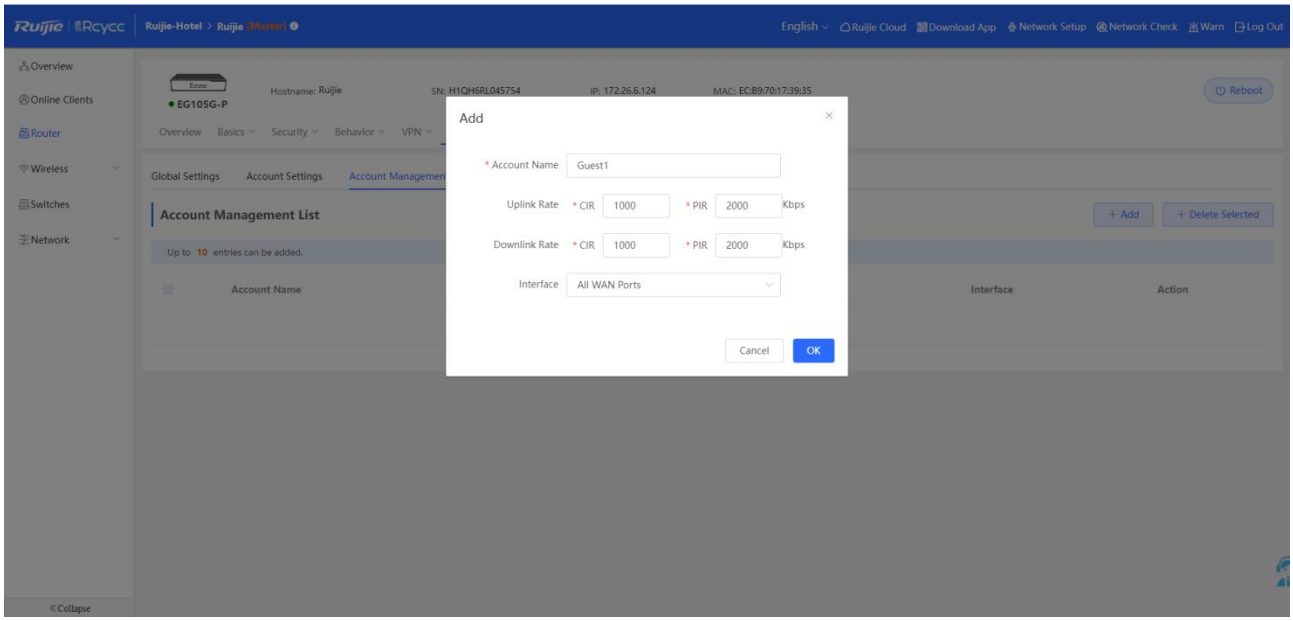
Mandatory PPPoE Dial up: Enable or disable mandatory PPPoE dial up.

After you enable this function, only dial up users and exceptional clients can access the Internet. If you want to configure exceptional IP addresses, please choose Exceptional IP Address. If you only need the choosed VLAN to do PPPoE authentication, please disable this function.

Unanswered LCP Packet Limit: When the number of unanswered LCP packets exceeds the limit, the session will be disconnected automatically. Default: 10.

3. Click **Account Management** to add speed limit policy for clients.





Uplink Rate:

CIR: CIR indicates the committed information rate.

PIR: PIR indicates the peak information rate.

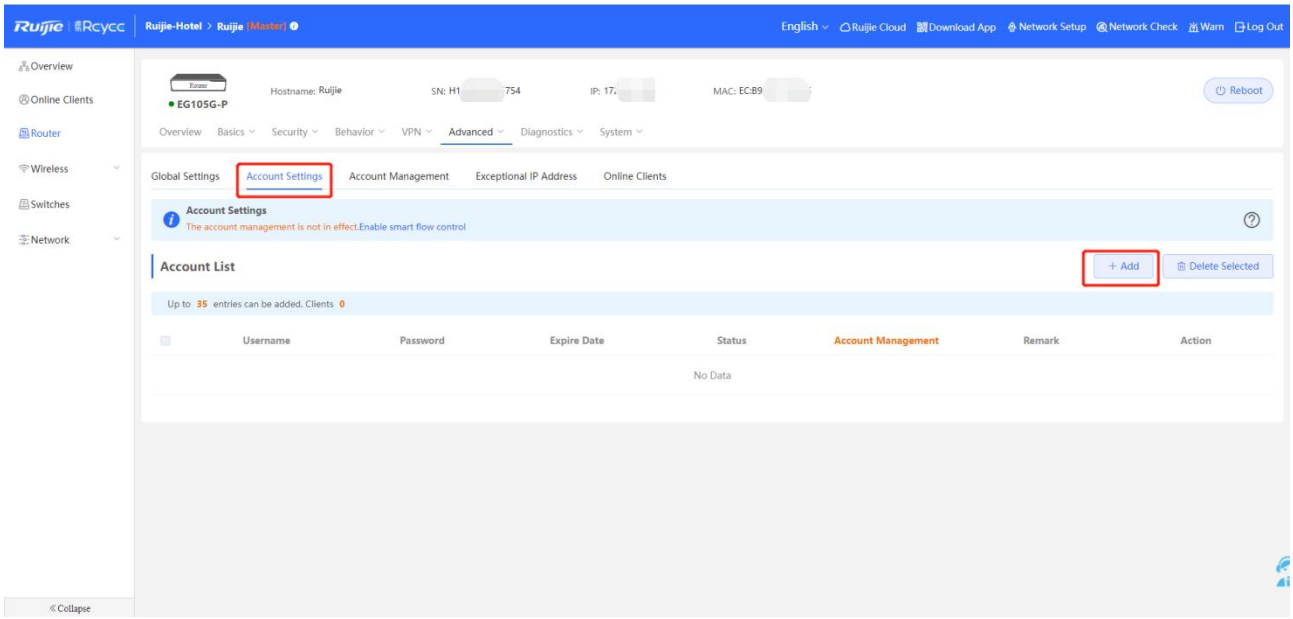
Downlink Rate:

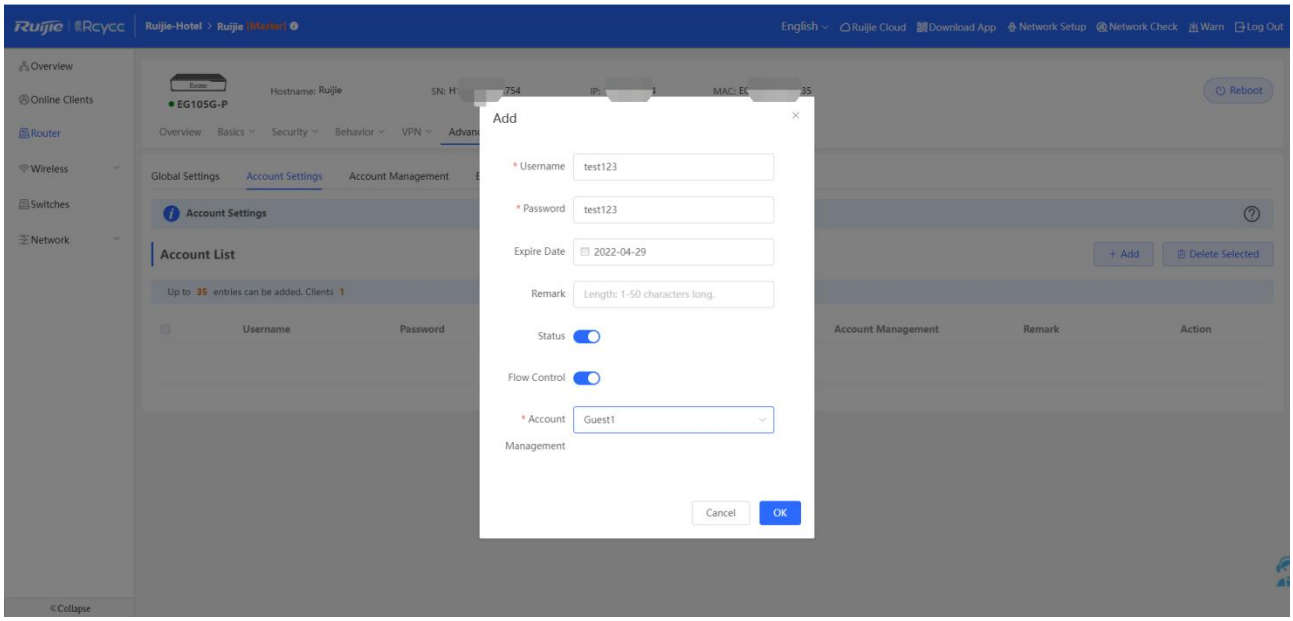
CIR: CIR indicates the committed information rate.

PIR: PIR indicates the peak information rate.

Interface: Select a WAN port which the policy is applied to. If choose All WAN Ports: The policy is applied to all WAN ports.

4. Click **Account Settings** to add account.

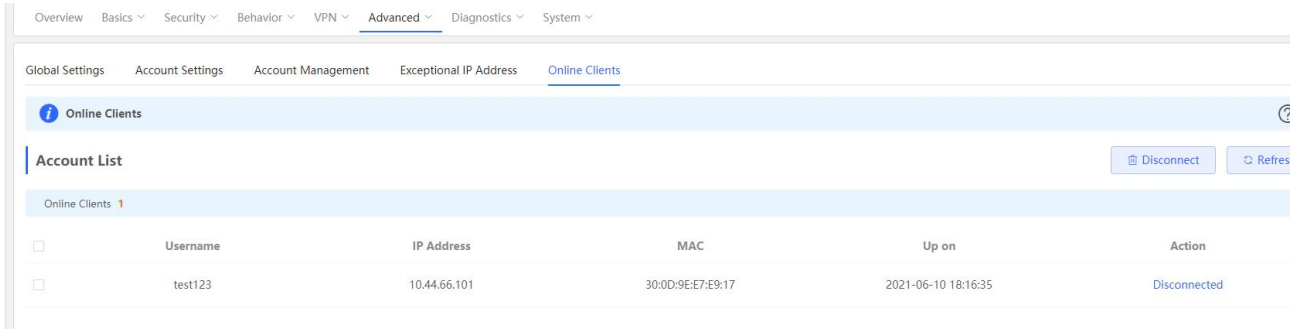




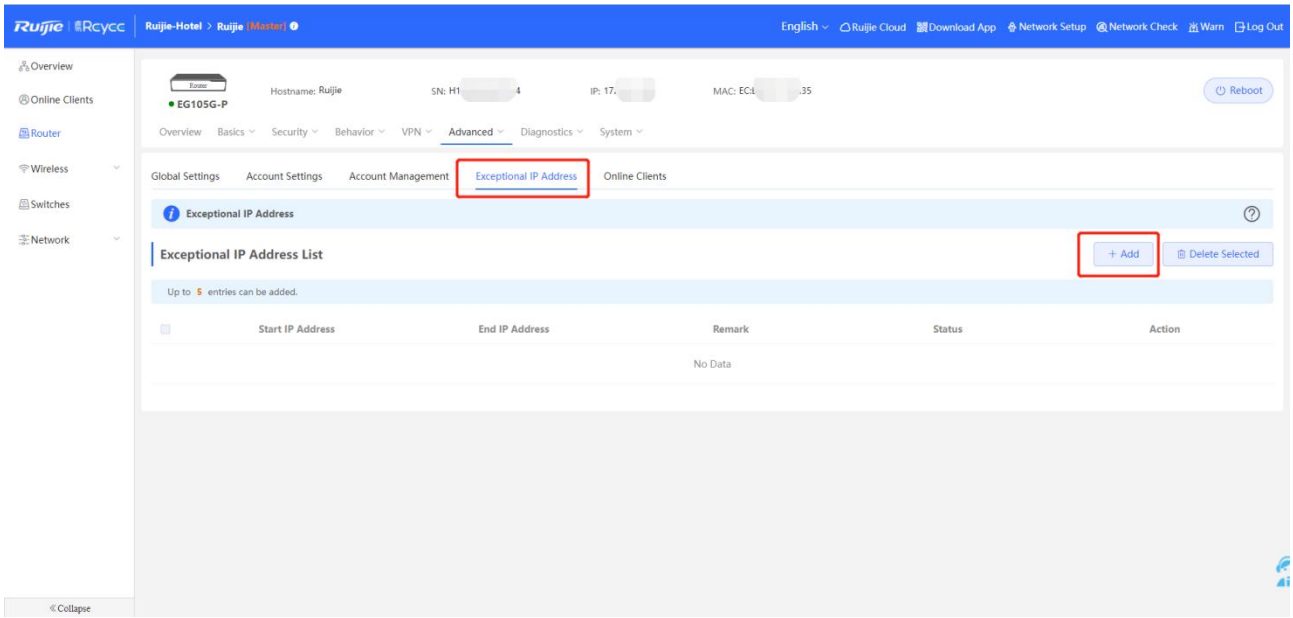
Expire Date: Set expire date for the account. Max date: 2099-01-01.

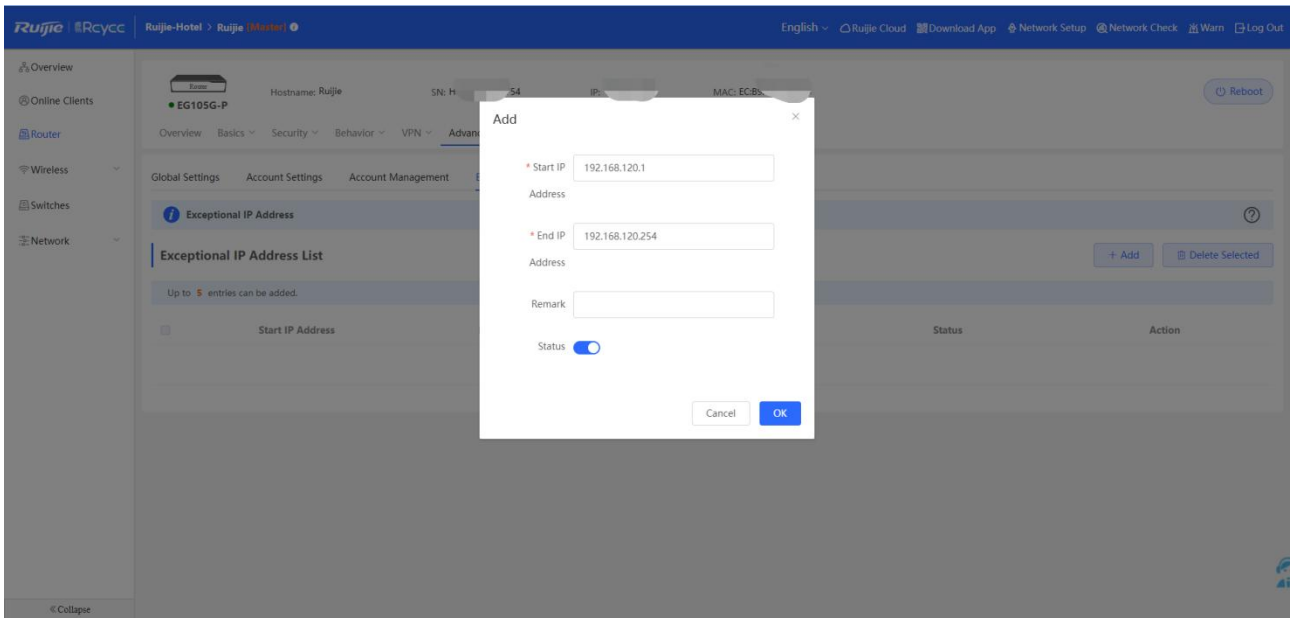
Flow Control: Select the account management policy to limit speed for the account.

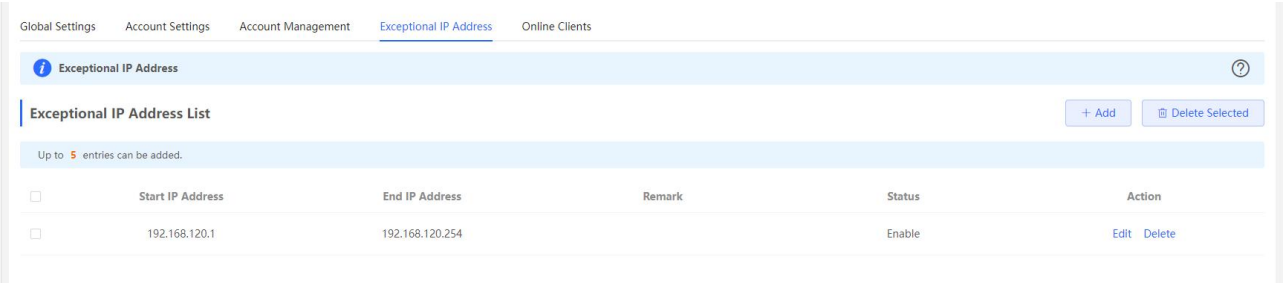
5. Dial up on PC, check the online status on EG.



6. Click **Exceptional IP Address** to configure whitelist user who can access internet without authentication.



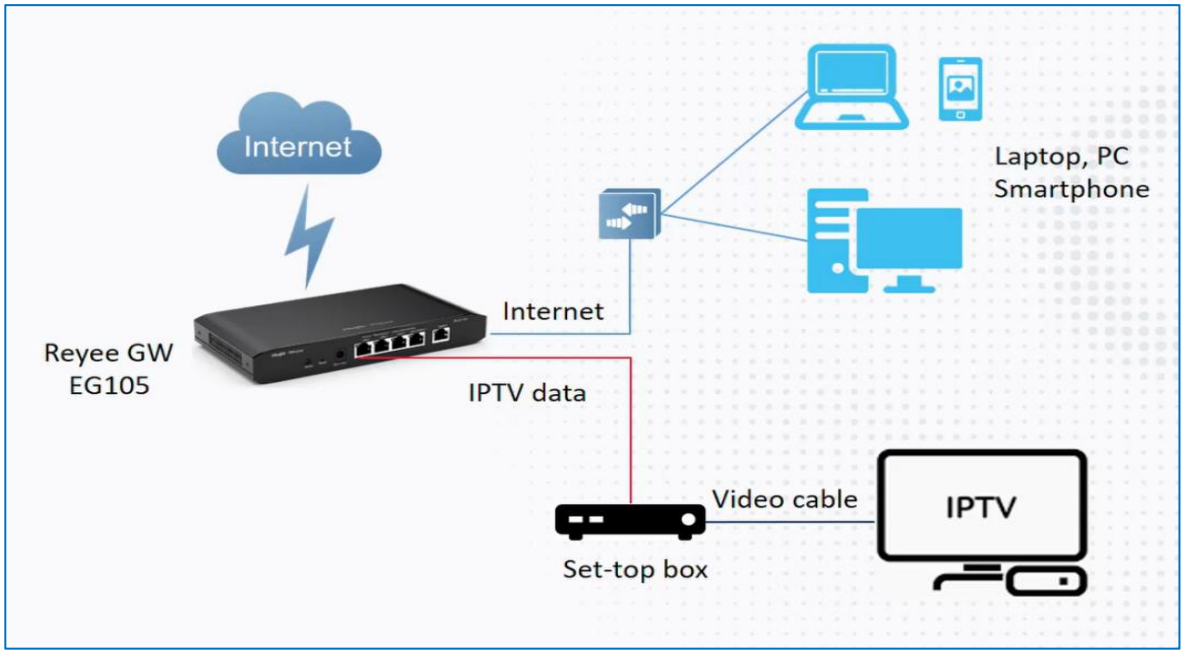




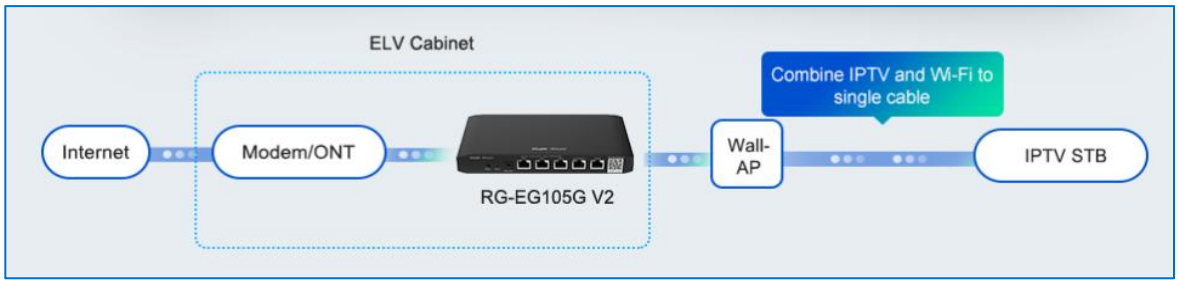
4.1.16. IPTV

Application Scenario

Scenario 1:



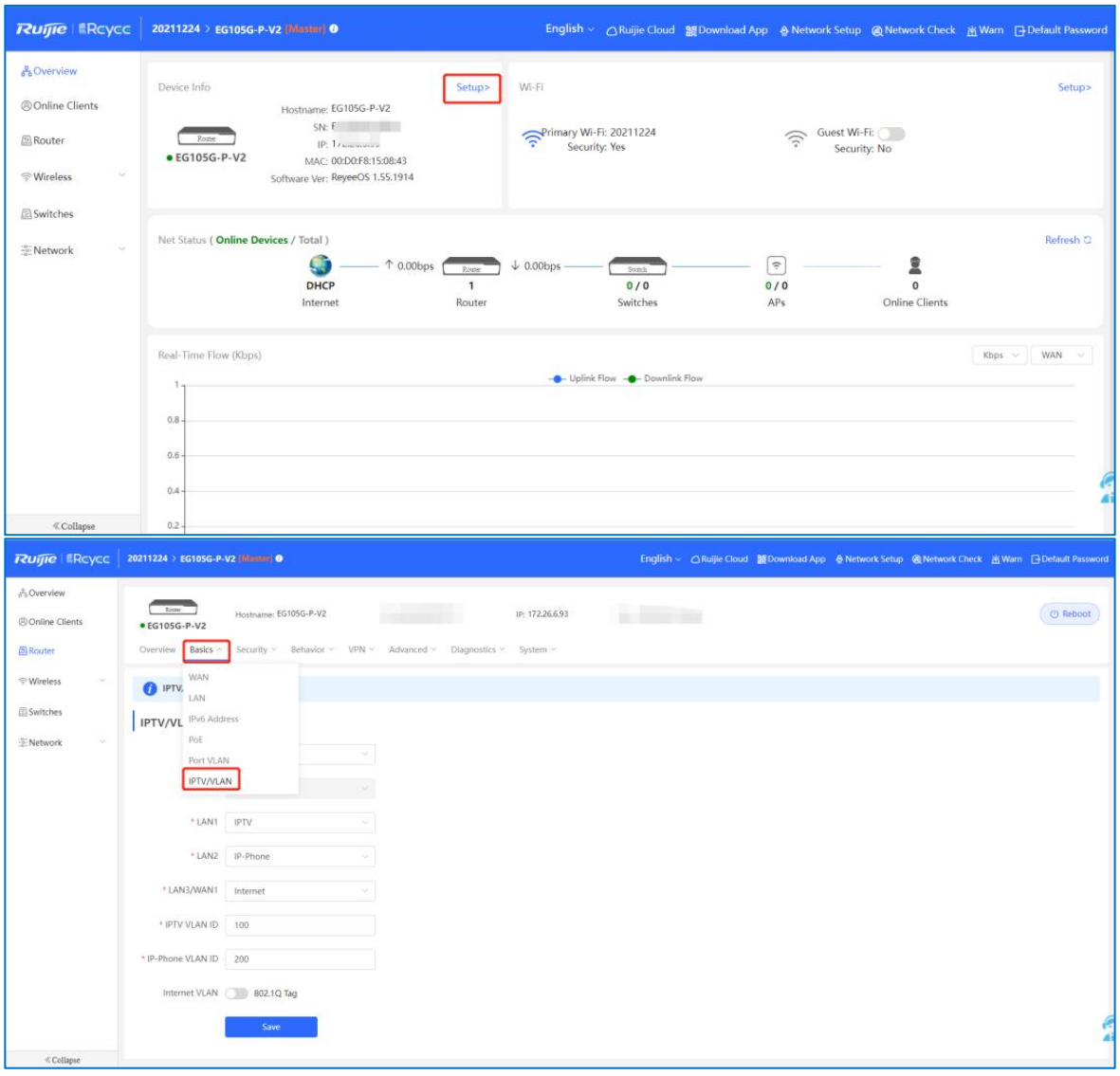
Scenario 2:



Procedure

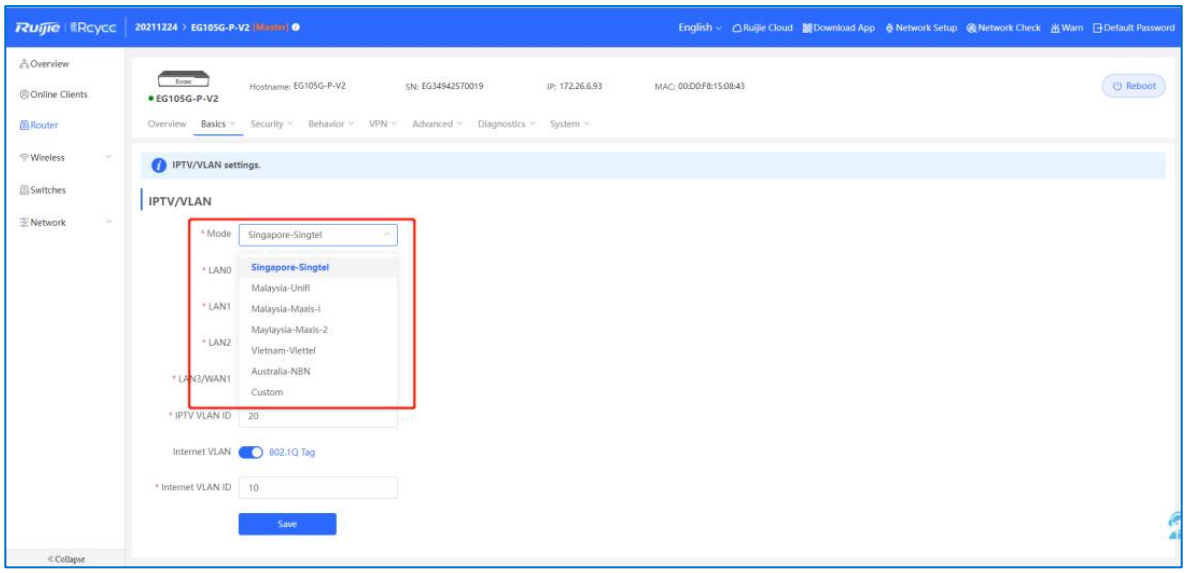
a 1 Connect the ISP cable with WAN port, and connect your PC with LAN port. Using the default IP 192.168.110.1 to login Reyee EG and then refer to the wizard to let your EG can access Internet successfully.

b 2. Click **Setup->Basics->IPTV/VLAN**

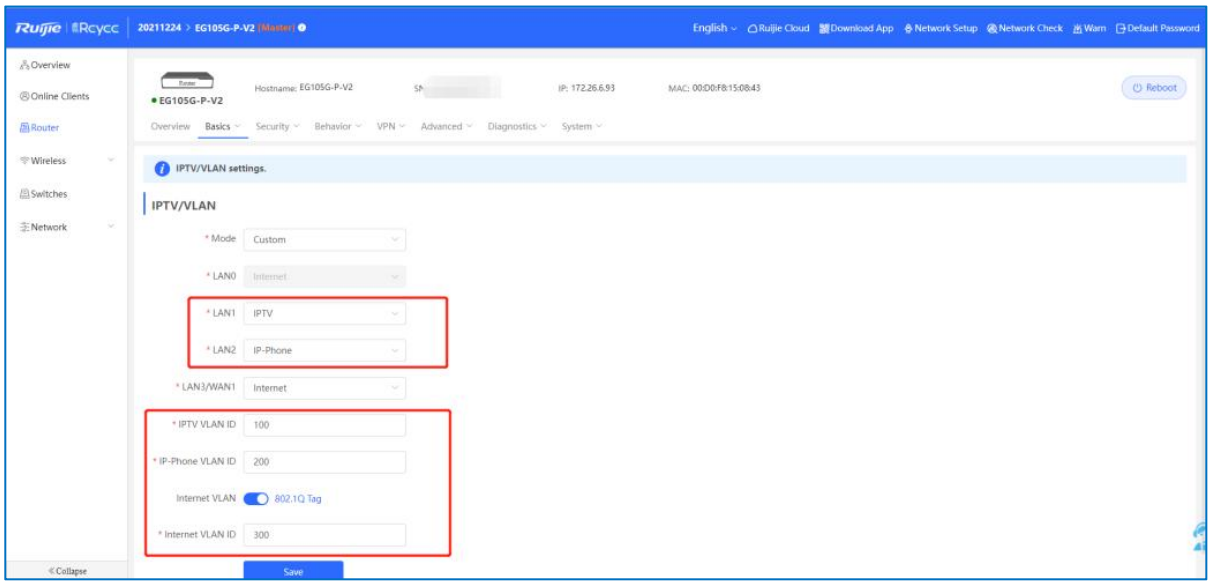


3. Configure the IPTV VLAN ID or IP-Phone VLAN ID:

1) If you are in following regions, you can choose the mode directly.

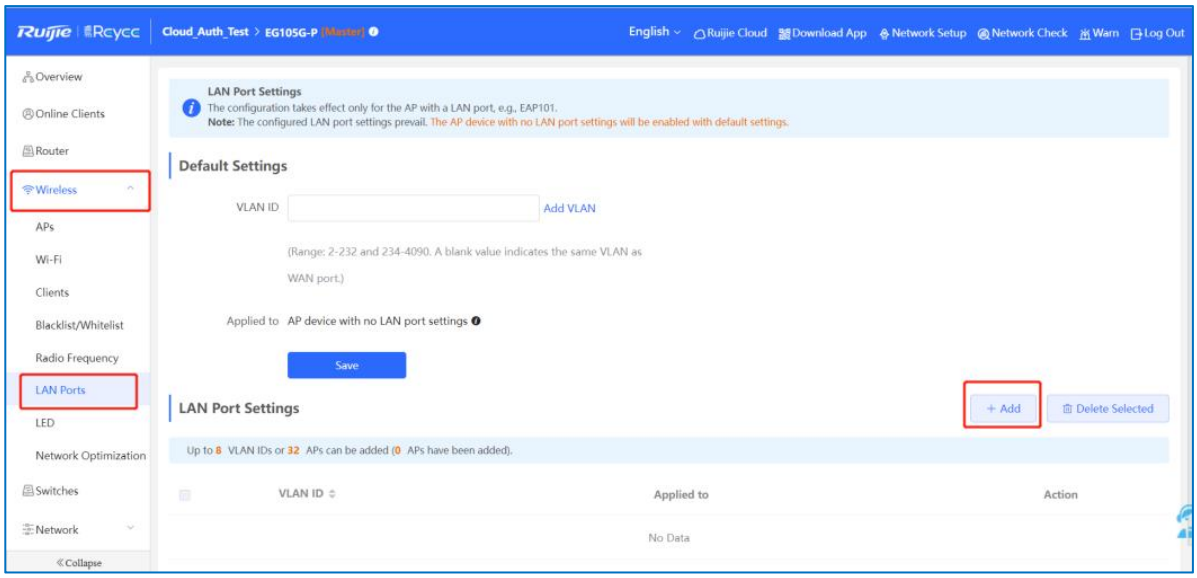


2) If you are not in these regions, you can choose custom, and contact with ISP for the IPTV setting, then connect the IPTV and IP-Phone with related LAN ports. For example, the IPTV VLAN is 100, IP-Phone VLAN is 200 and the .Internet VLAN ID is 300.

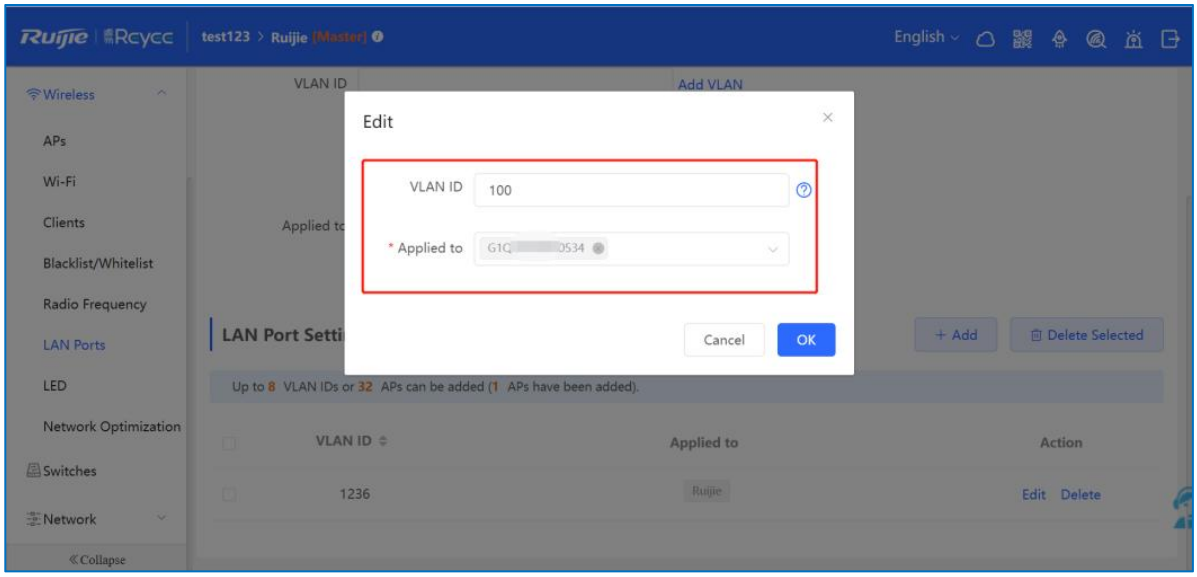


3) If you are scenario 2, after configuring IPTV setting on Reyee EG, you need to configure the IPTV VLAN 100 on WALL AP LAN port. If you are scenario 1, please ignore this step.

Click **Wireless->LAN Ports->Add**



Configure VLAN ID to be 100, Applied to WALL AP.



Note

- Reyee OS 1.55 or later version can support IPTV.

4.1.17. UPnP

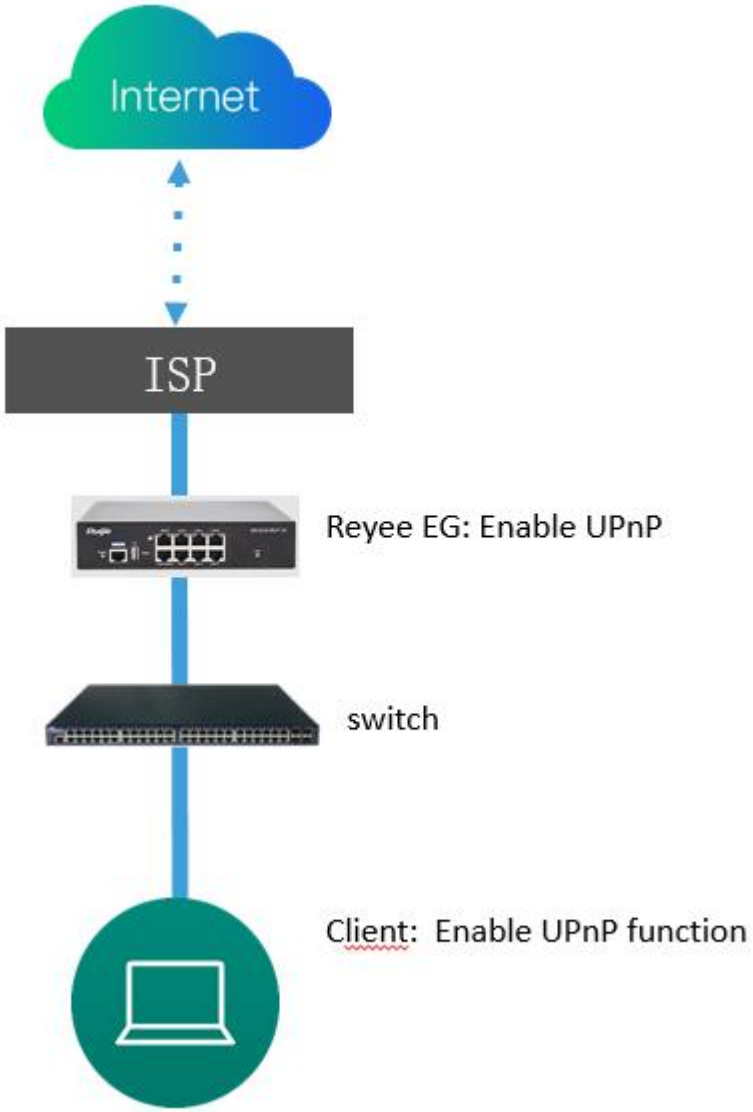
Application Scenario

UPnP （Universal Plug and Play) is a protocol that enables application running on a host to automatically configure port mapping on the NAT-Router. On the other hand, enabling UPnP may pose potential danger to network security. There are three requirements for applying UPnP:

1) The device must be enabled with UPnP.

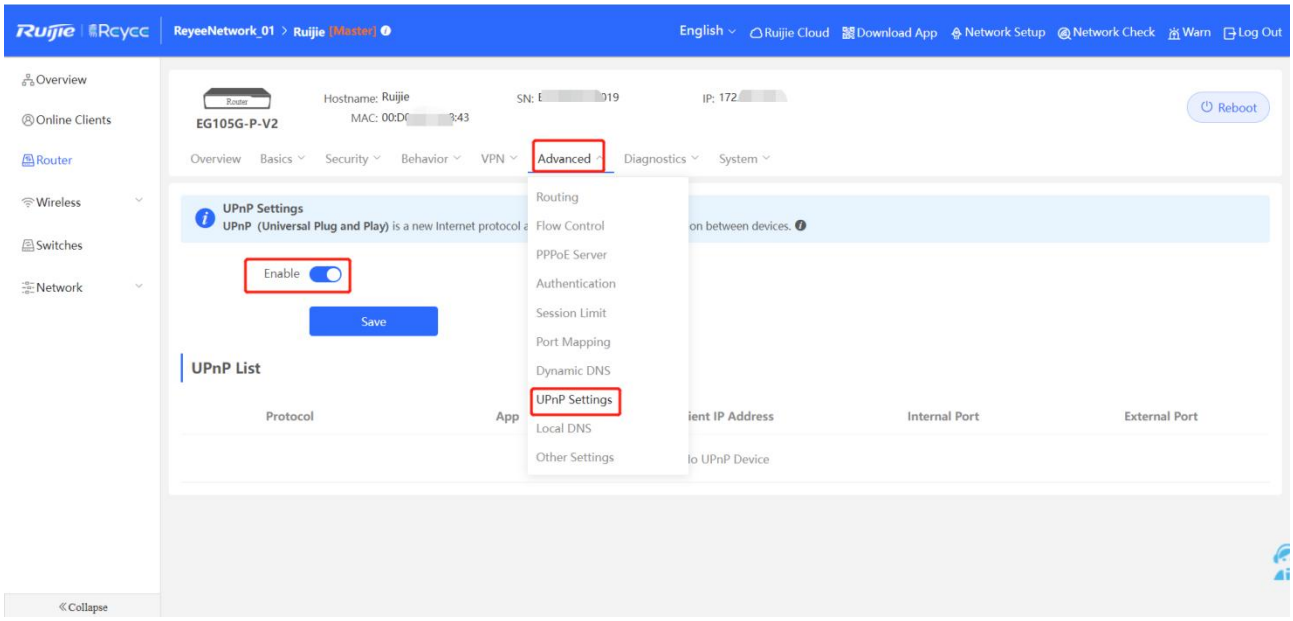
2) The operating system of the internal host must support UPnP.

3) The application must support UPnP.



Procedure

1. Click **Router->Advanced->UPnP Settings->Enable**. then enable UPnP function on your Phone or PC. The Router will auto detect your device and set port mapping for it. Finally you can use external IP and port to access your Phone or PC service.



4.2 Reyee ES Series Switches Configuration

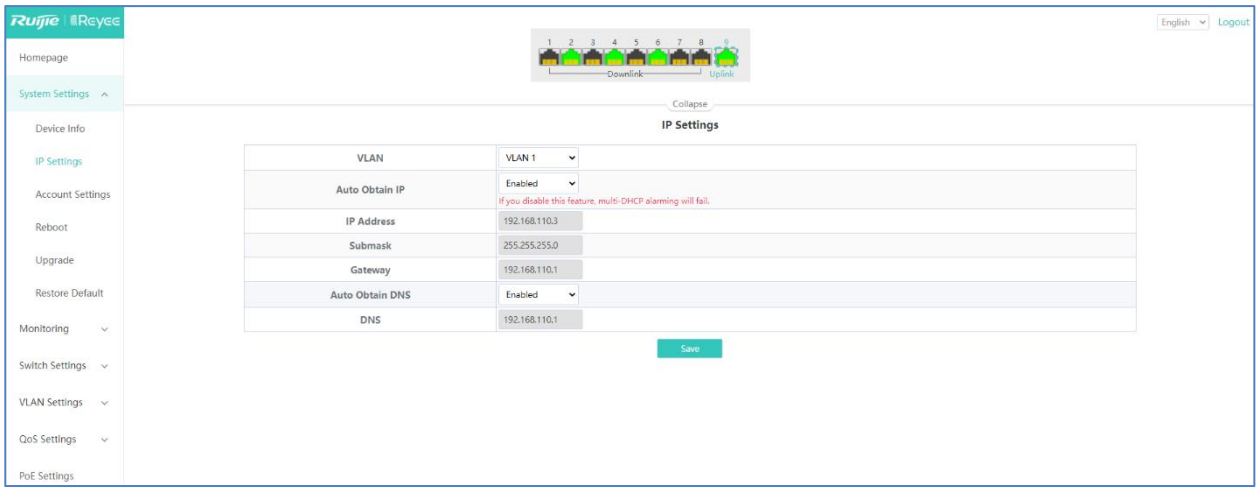
4.2.1 System Settings

4.2.1.1 Device Info

Device Info displays device details, including Hostname, Model, MAC Address, IP Address, Submask, Gateway, DNS, SN, Firmware Version, Firmware Date and Hardware Version.

4.2.1.2 IP Settings

IP Settings could configure the management IP address and management VLAN for the device. A**uto Obtain IP** is set to **Enabled** by default. When **VLAN Settings** is set to **off**, the management VLAN is 1.



When **VLAN Settings** is set to **on**, the following figure will be displayed.

When VLAN Settings is set to on, select the management VLAN from the configured VLANs (you can choose **VLAN Settings > VLAN Members** to add a VLAN).

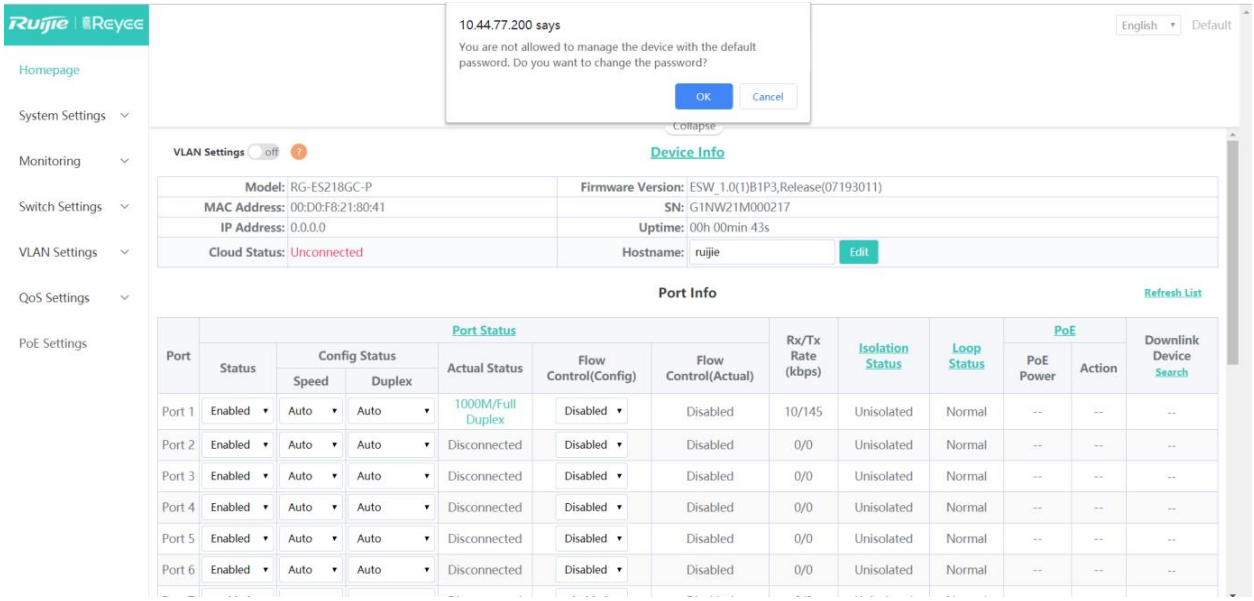
You can change the status of Auto Obtion IP to Disabled to manually configure Static IP Address that belong to the management VLAN and DNS server for the device.

The device will be disconnected for a short time during the period of IP address configuration. If Auto Obtain IP is set to Enabled, the device needs to obtain an IP address from the uplink device, or you can enter the management IP address (10.44.77.200) for Web management.

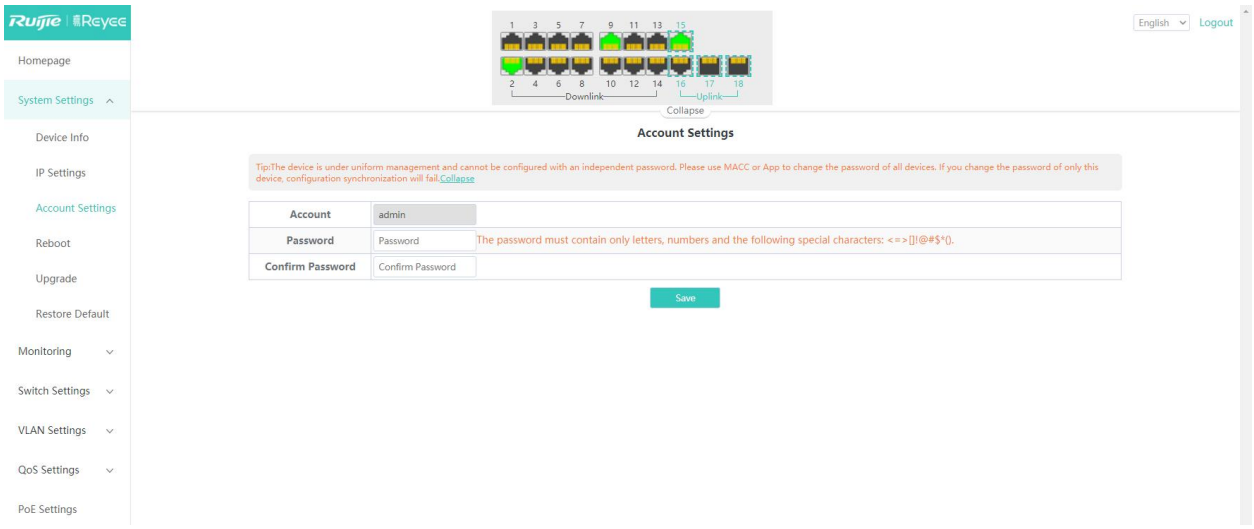
After **VLAN Settings** is set to **on**, change the management VLAN and check whether the port VLAN contains the management VLAN to avoid IP address inaccessibility.

4.2.1.3 Account Settings

Under factory default settings, the eWeb management system displays a prompt, asking you whether to change the password. (You can configure switch functions only after changing the password.)



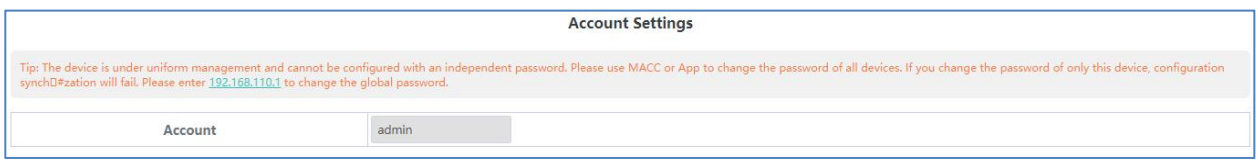
Click **OK.** The Web management system automatically redirects to the Account Settings page (or you can choose **System Settings > Account Settings** to configure the login password).



Enter a new password according to password rules and then click **Save**. In the displayed dialog box, click **OK**.

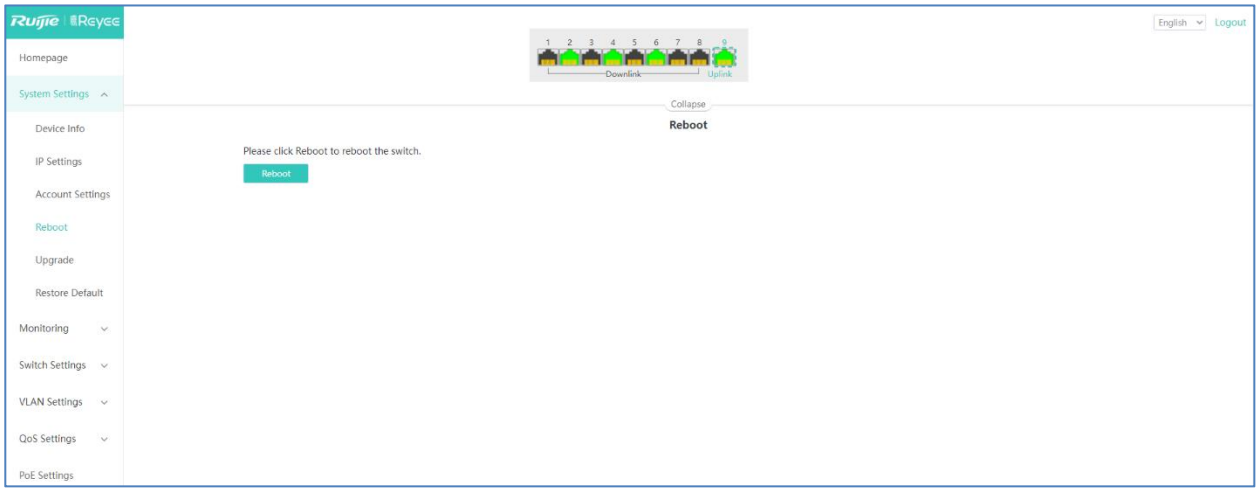
Keep the configured device management password in mind. After the password is being changed, the eWeb management system may need re-authentication and login.

When switches are managed via a Self-Organizing Network (SON), no management password can be separately configured for the device and the global password needs to be configured on the master device.



4.2.1.4 Reboot

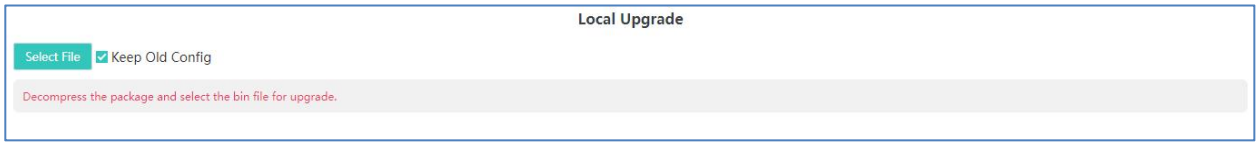
Click **Reboot** to reboot the switch.



4.2.1.5 Upgrade

Local Upgrade

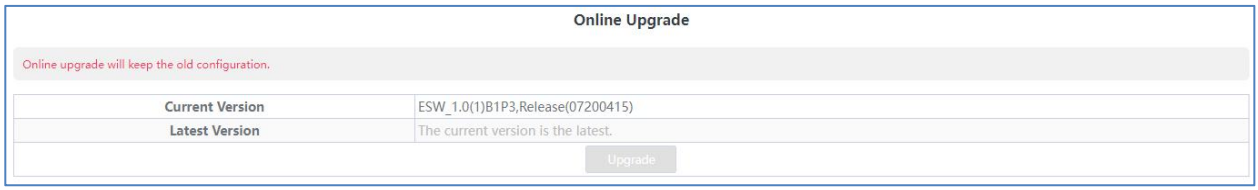
Click **Select File**. In the displayed dialog box, select a target upgrade package. (The software upgrade package is an xxx.bin file while the system upgrade package is an xxxx.tar.gz file. You need to manually decompress the package and select the xxx.bin file for upgrade.)



Keep Old Config is selected by default. If the target version is much later than the current version, it is recommended not to choose **Keep Old Config.**

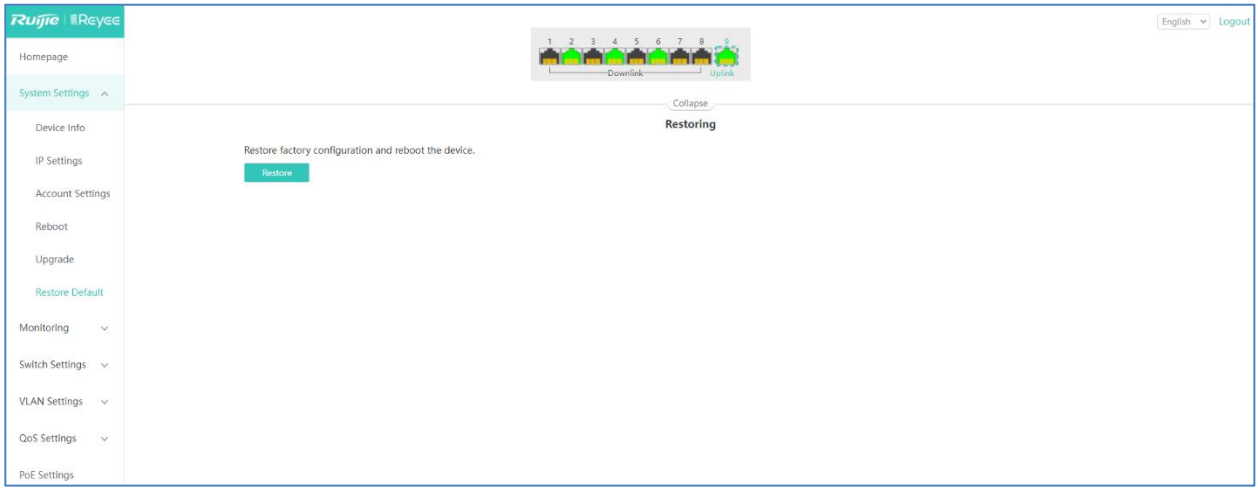
Online Upgrade

Online upgrade will keep your current configuration. If there is a new version available, the Upgrade button can be clicked. Click **Upgrade** button and then confirm upgrade. The device will download the new version from the Cloud and upgrade to the target version. The time it takes depends on network performance.



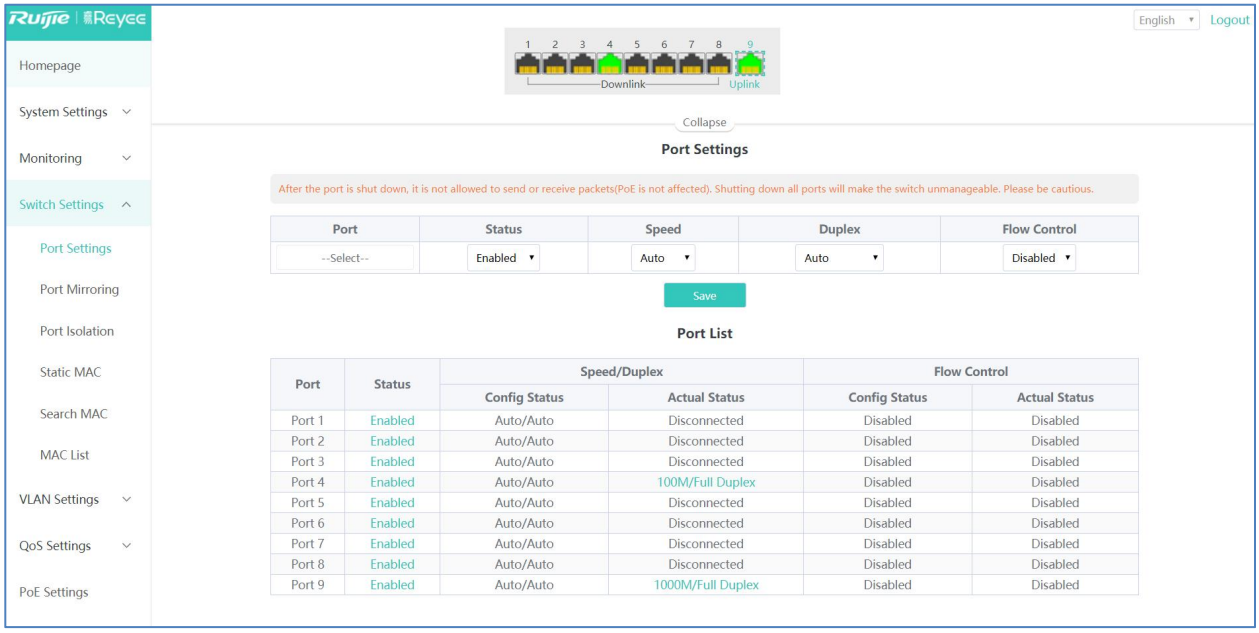
4.2.1.6 Restore Default

Click **Restore** to restore factory settings and reboot the device.

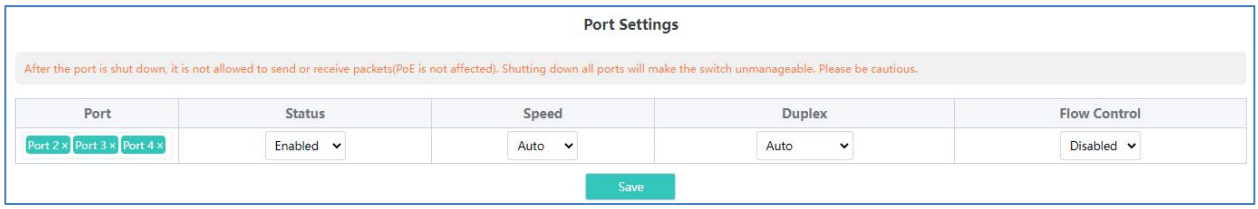


4.2.2 Switch Settings

4.2.2.1 Port Settings



In the **Port Settings** page, you can configure the port status, speed, duplex mode, and flow control status of the ports.



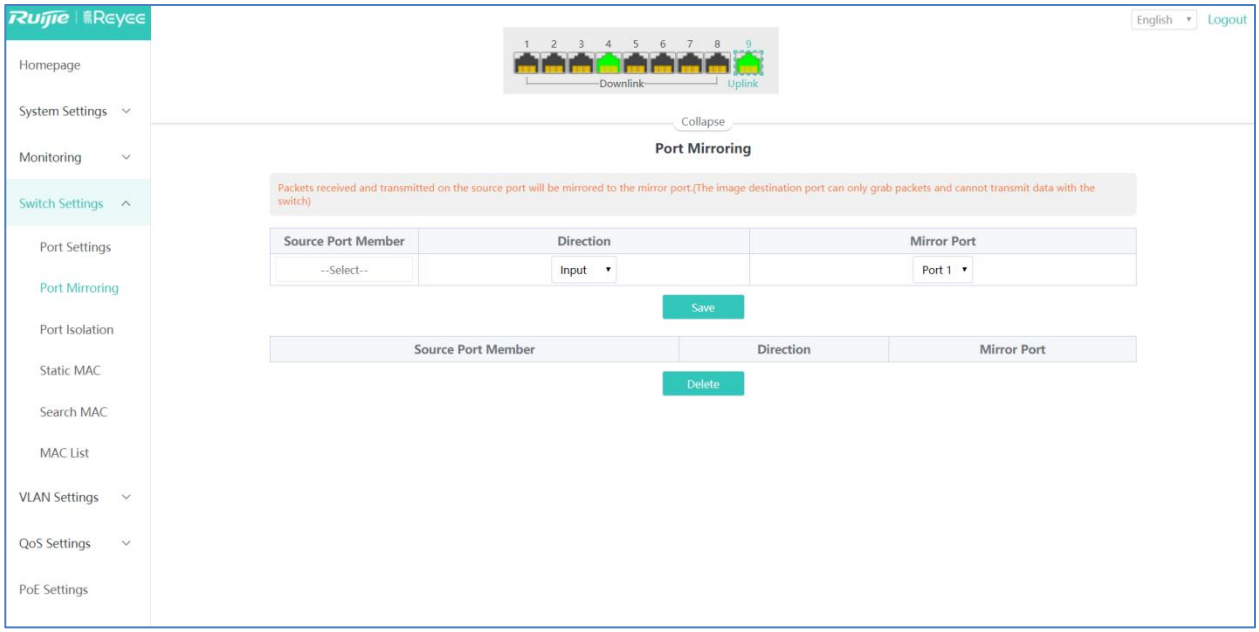
A disabled port cannot transmit or receive packets (the PoE function is not affected). Disabling all ports of a switch will make the switch unmanageable. Therefore, exercise caution when disabling ports.

In the **Port List**, it displays the configuration properties and the actual properties in effect for each port of the device.

Port List

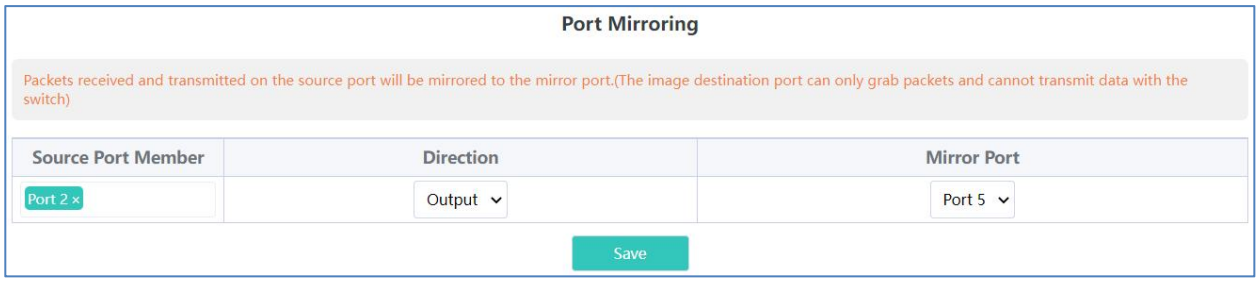
Port	Status	Speed/Duplex		Flow Control	
		Config Status	Actual Status	Config Status	Actual Status
Port 1	Enabled	Auto/Auto	1000M/Full Duplex	Disabled	Disabled
Port 2	Enabled	Auto/Auto	1000M/Full Duplex	Disabled	Disabled
Port 3	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 4	Enabled	Auto/Auto	100M/Full Duplex	Disabled	Disabled
Port 5	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 6	Enabled	Auto/Auto	1000M/Full Duplex	Disabled	Disabled
Port 7	Enabled	Auto/Auto	1000M/Full Duplex	Disabled	Disabled
Port 8	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 9	Enabled	Auto/Auto	Disconnected	Disabled	Disabled

4.2.2.2 Port Mirroring

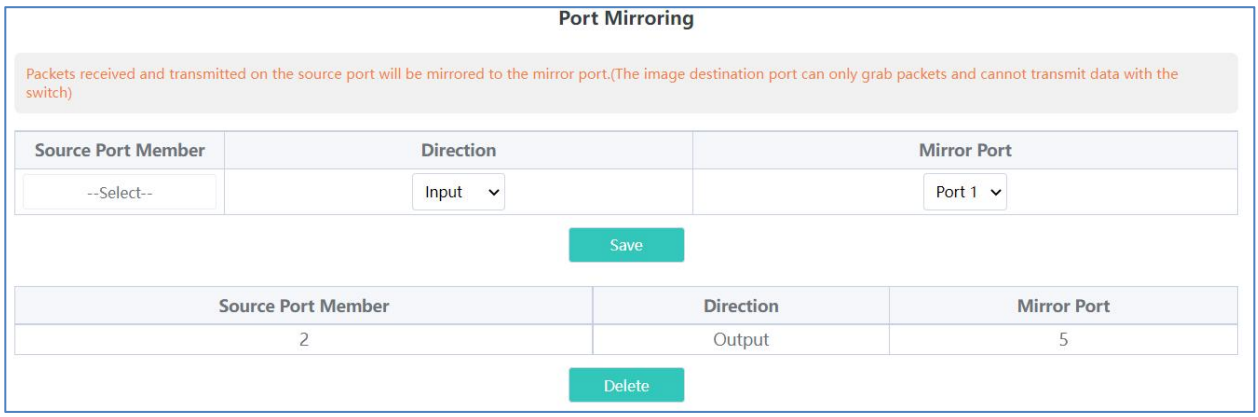


Port Mirroring forwards input/output packets of one or more source port to the destination port to monitor the network.

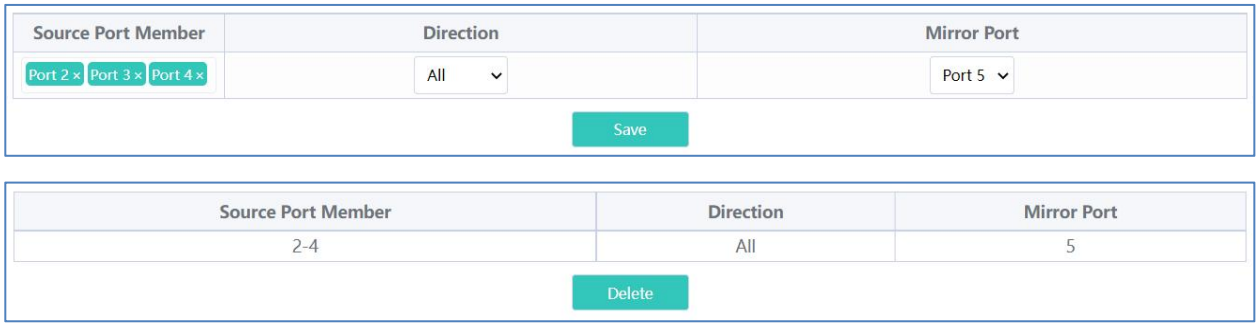
Select the source port, direction (Input/Output/All), mirror port for port mirroring configuration and click **Save.**



The following list shows the port mirroring configurations that currently exist:



Only one port mirroring entry can be set, but multiple source ports are supported:



Destination mirroring ports on RG-ES205C-P, RG-ES205GC-P, RG-ES209C-P, and RG-ES209GC-P can only capture packets. They cannot transmit data to the switch.

4.2.2.3 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.

PC1: connect to Port 1, IP: 192.168.1.10 PC2: connect to Port 2, IP: 192.168.1.12

Ping the test results when the port Isolation turned off:

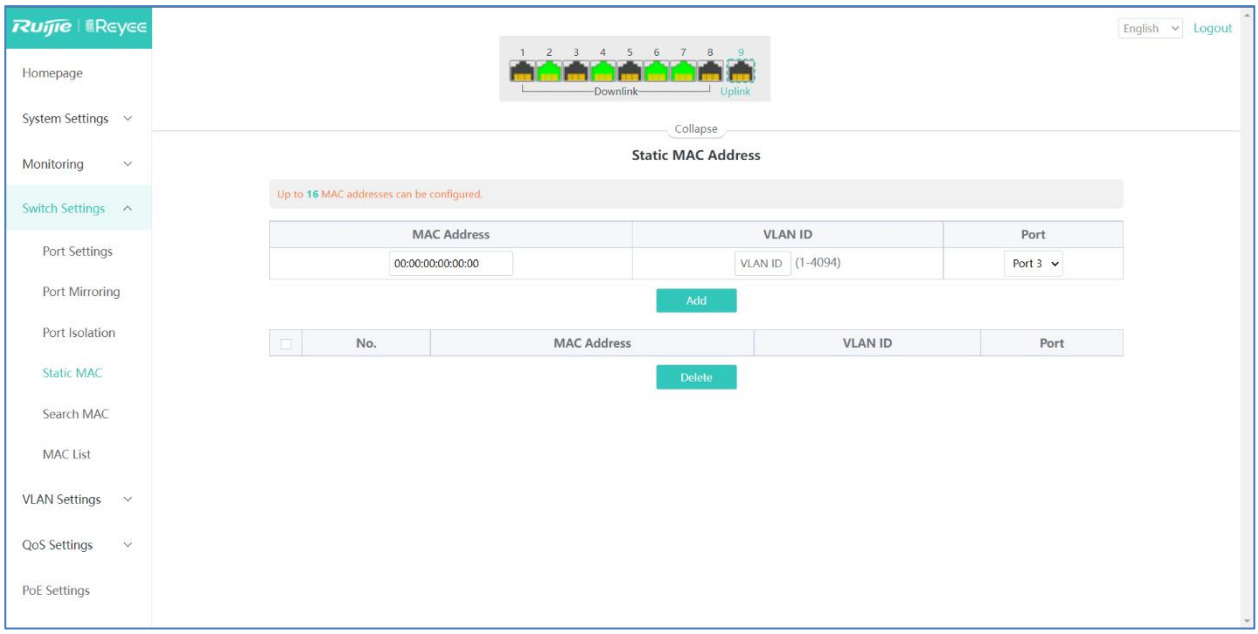
```
C:\Users\Administrator>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:
Reply from 192.168.1.10: bytes=32 time=2ms TTL=128
Reply from 192.168.1.10: bytes=32 time=2ms TTL=128
Reply from 192.168.1.10: bytes=32 time=2ms TTL=128
Reply from 192.168.1.10: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

Ping test results when the port Isolation turned on:

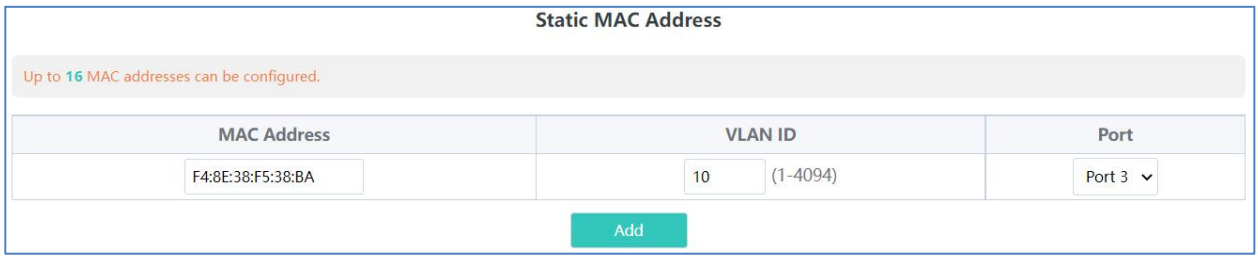
```
C:\Users\Administrator>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

4.2.2.4 Static MAC

The **Static MAC** page is divided into two parts:

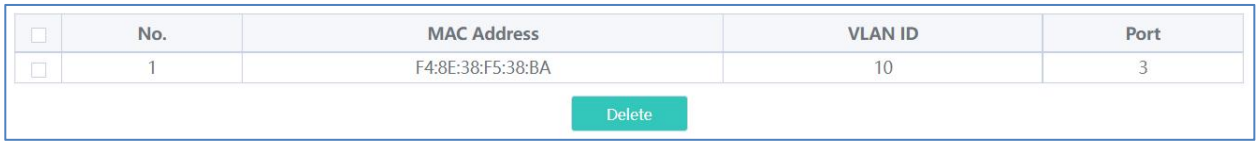


Adding a static MAC address: Enter a valid MAC address and VLAN ID, select a port, and then click Add to add a static MAC address. Up to 16 static MAC addresses can be added.



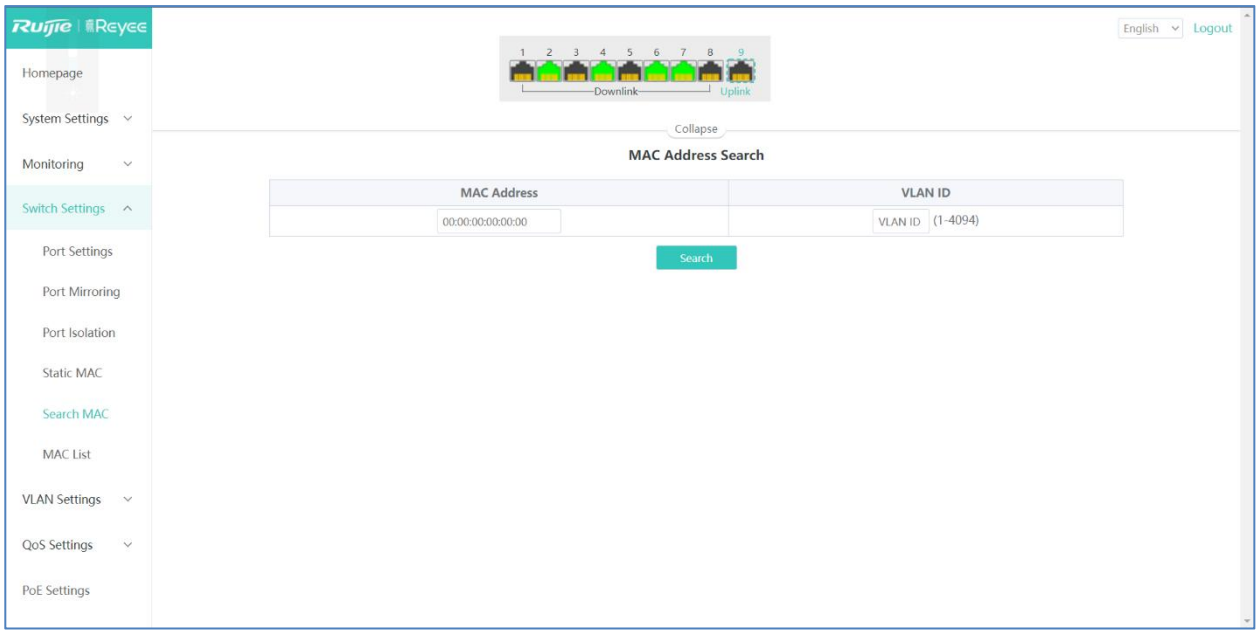
After VLAN Settings is set to off, no VLAN ID needs to be entered to add a static MAC address.

Displaying and deleting a static MAC address: After a valid static MAC address is added, the information will be displayed in the list below. Select a static MAC address and click Delete to delete the static MAC address.

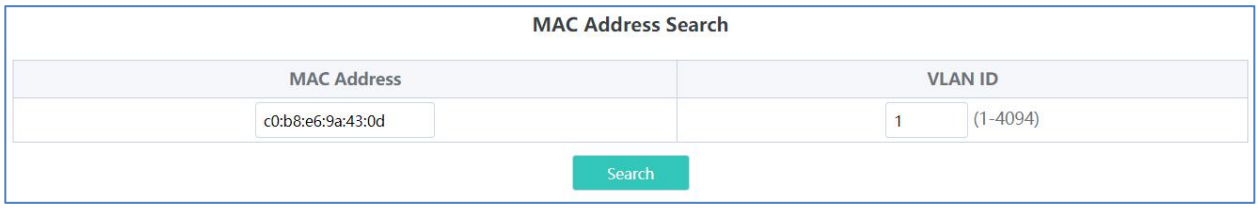


4.2.2.5 Search MAC

With the **Search MAC** function, you can search for the MAC addresses learned by the device. MAC addresses can be fuzzily searched.



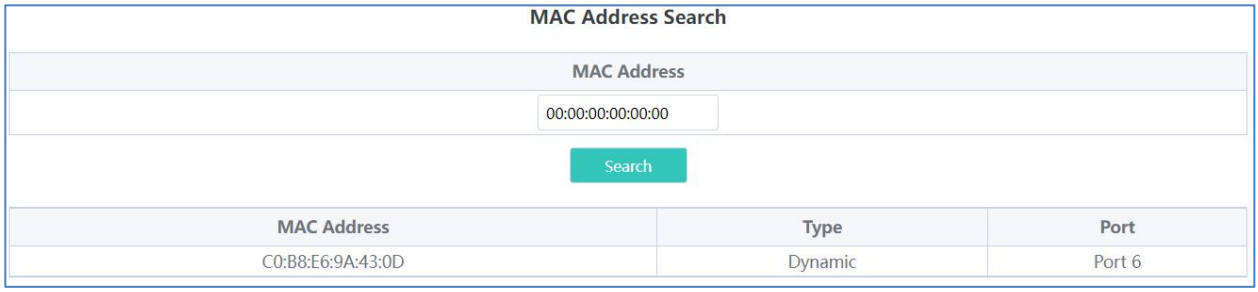
You can enter a part of a complete MAC address (such as c0:b8:e6:9a:43:0d) for searching.



The search results will show the information of **VLAN ID, Type, Port** corresponding to the MAC address:

MAC Address	VLAN ID	Type	Port
C0:B8:E6:9A:43:0D	1	Dynamic	Port 6

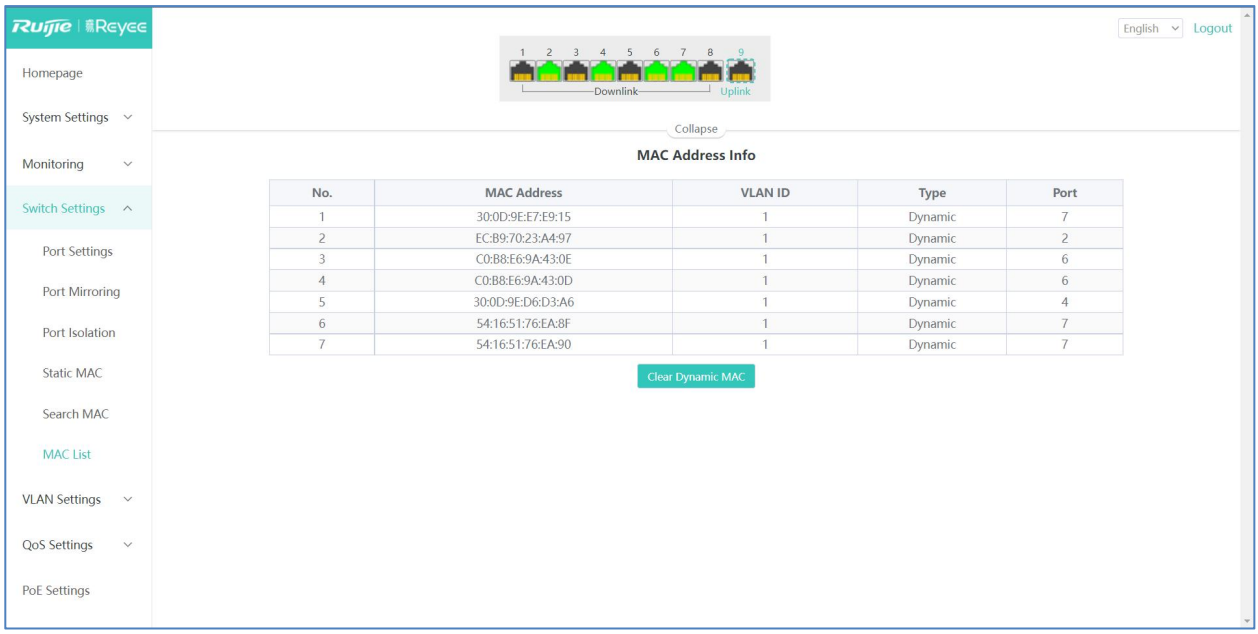
After **VLAN Settings** is set to **off**, the **VLAN ID** column will not be displayed.



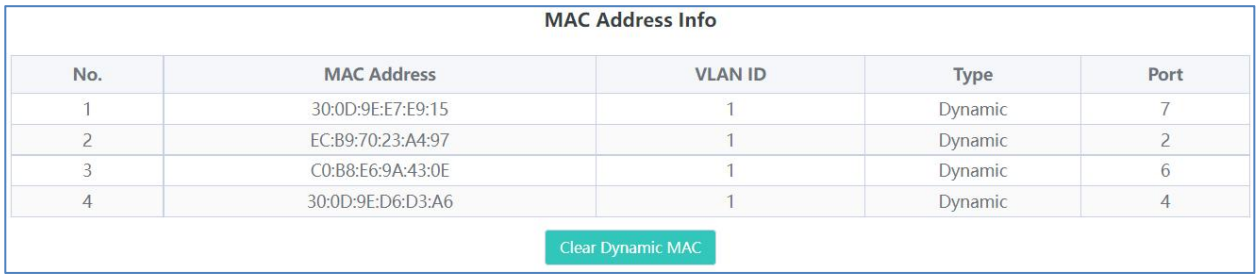
MAC Address	Type	Port
C0:B8:E6:9A:43:0D	Dynamic	Port 6

4.2.2.6 MAC List

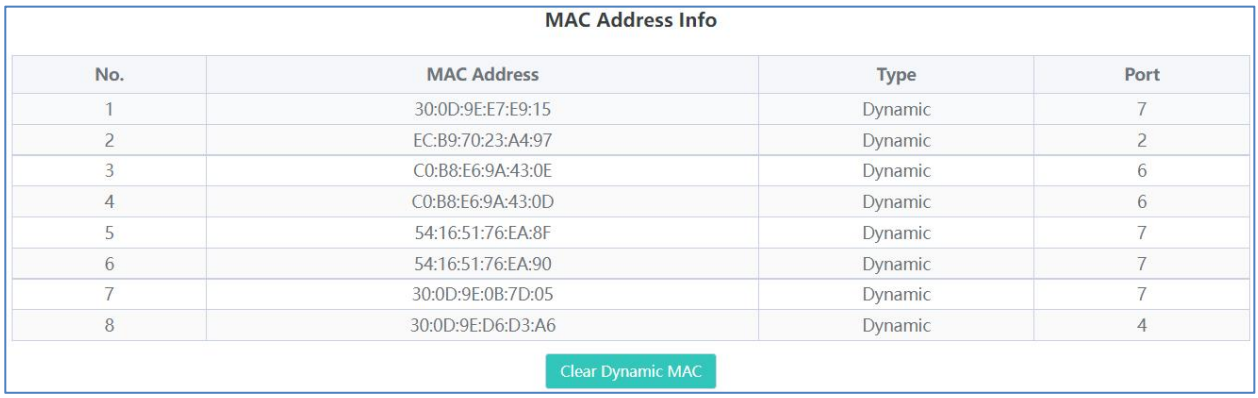
The **MAC List** page lists MAC addresses learned by the device.



Click **Clear Dynamic MAC,** the device will re-obtain the list of learned MAC addresses.

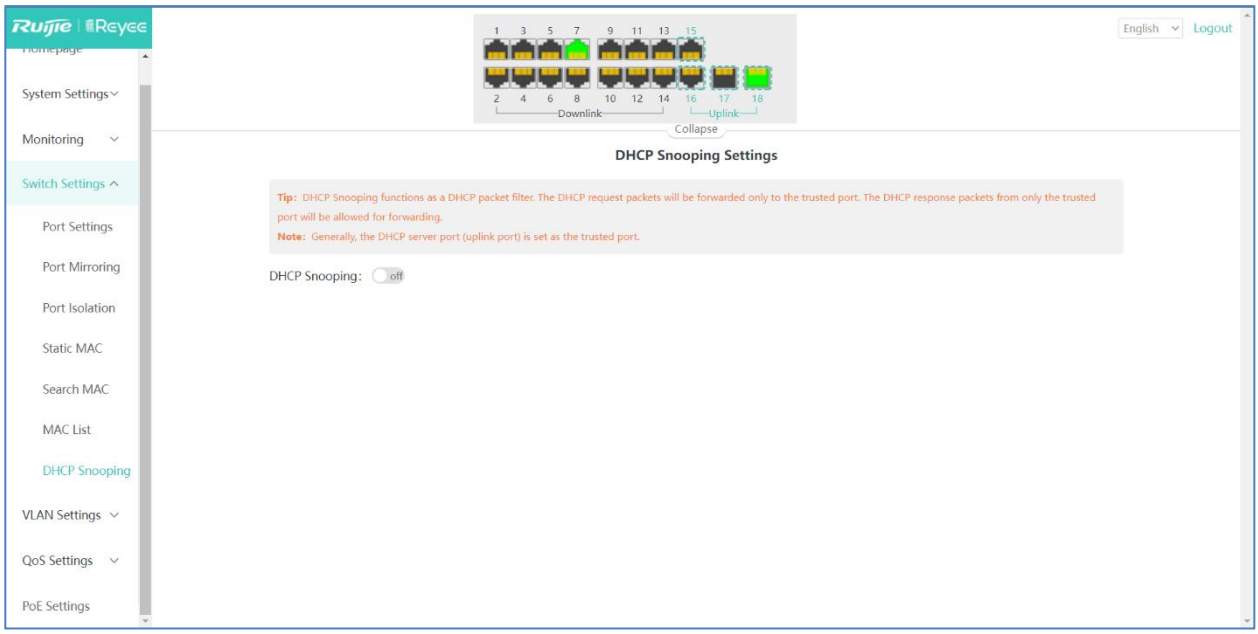


After **VLAN Settings** is set to off, the **VLAN ID** column will not be displayed.

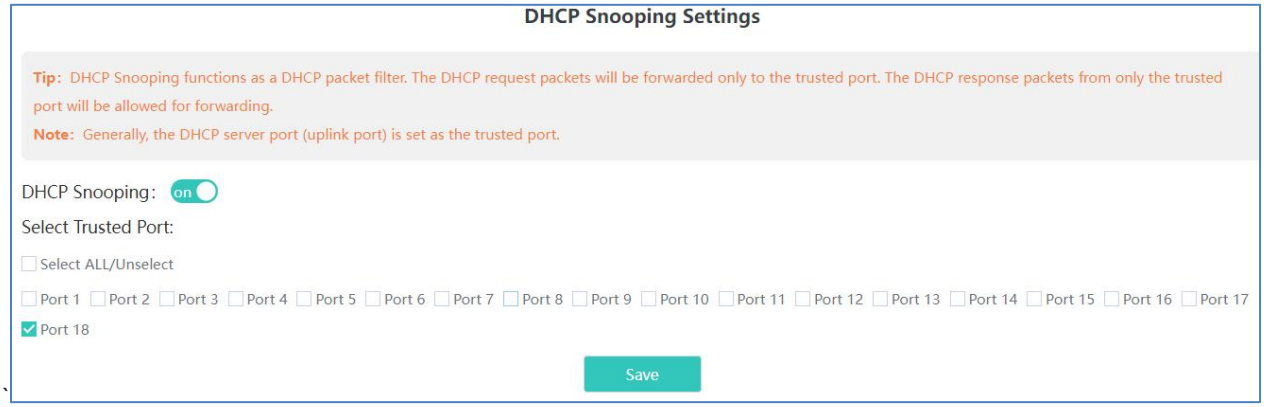


4.2.2.7 DHCP Snooping

DHCP Snooping is used as a DHCP packet filter. The DHCP request packets will be forwarded only to the trusted port. Only the DHCP response packets from the trusted port will be allowed to forward.



After **DHCP Snooping** is set to **on,** as shown in the figure below, the device sets the uplink port as a trusted port by default. You can select a port and click **Save** to set the port as the trusted port.



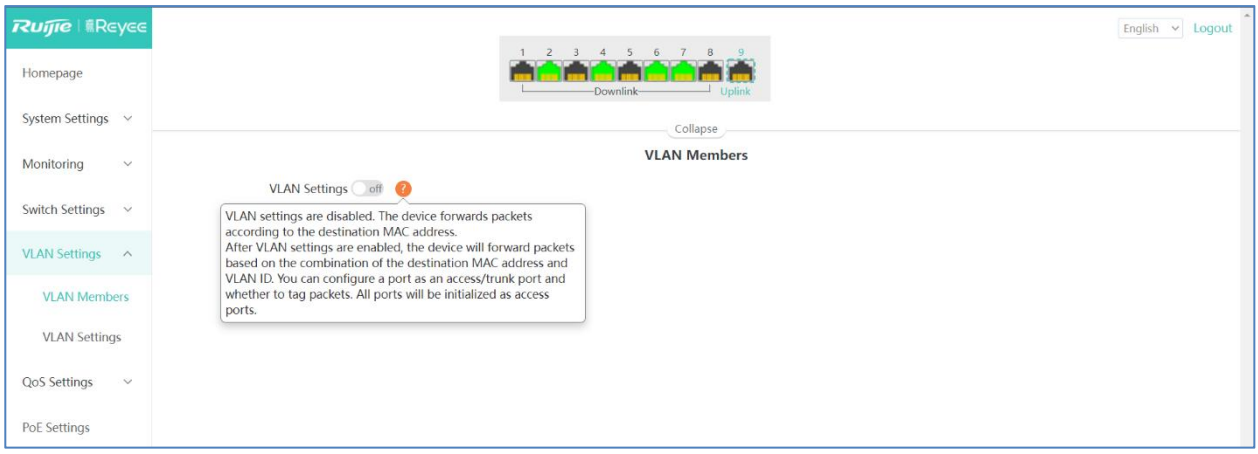
The port connected to the DHCP server (uplink port) is configured as the trusted port generally.

The ES205GC-P and ES209GC-P do not support this feature.

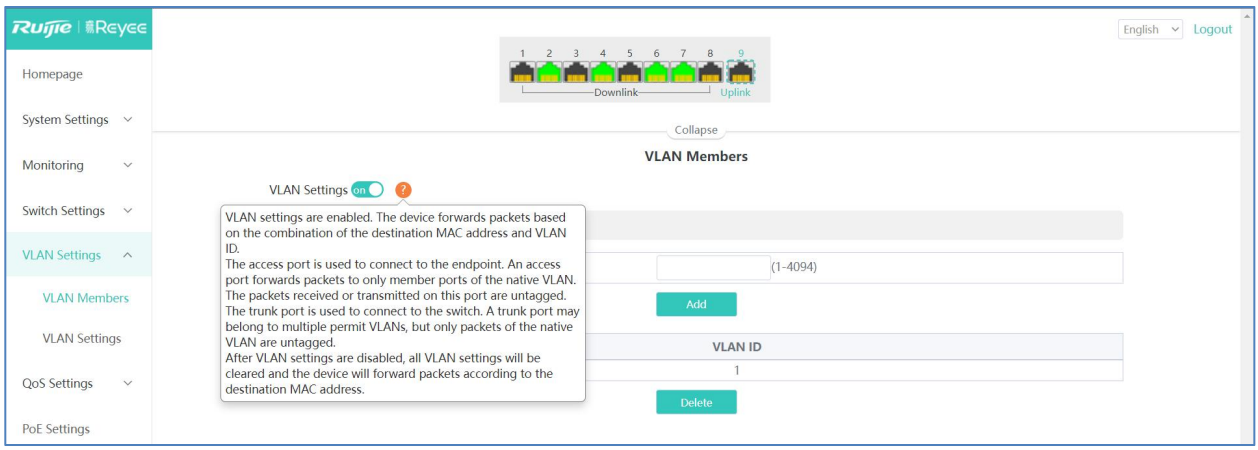
4.2.3 VLAN Settings

4.2.3.1 VLAN Members

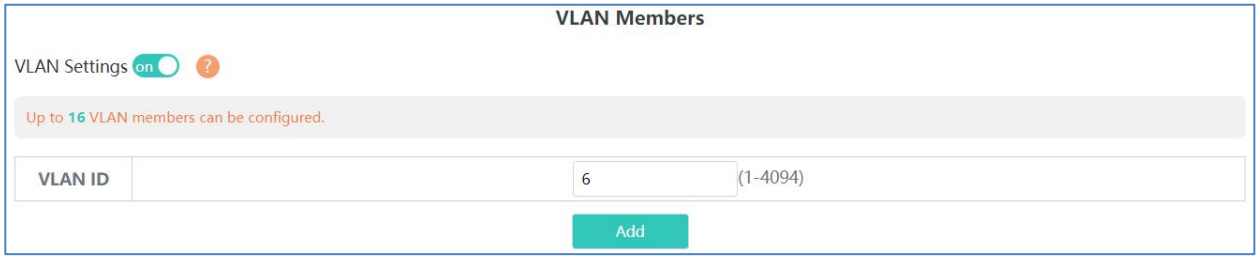
When **VLAN Settings** is set to **off,** the page is shown in the figure below:



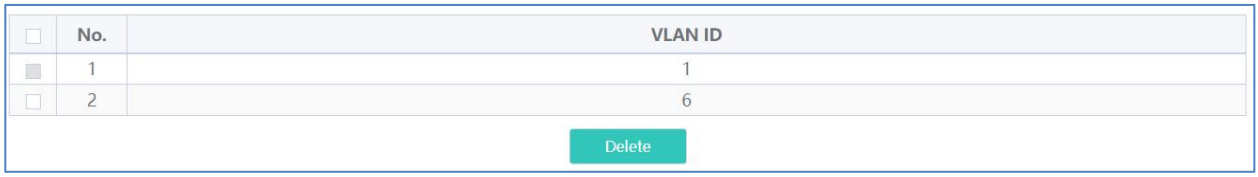
When **VLAN Settings** is set to on, the page is shown in the figure below:



After VLAN Settings is set to on, enter a valid VLAN ID and click **Add** to configure a new VLAN. Up to 16 VLANs can be configured.



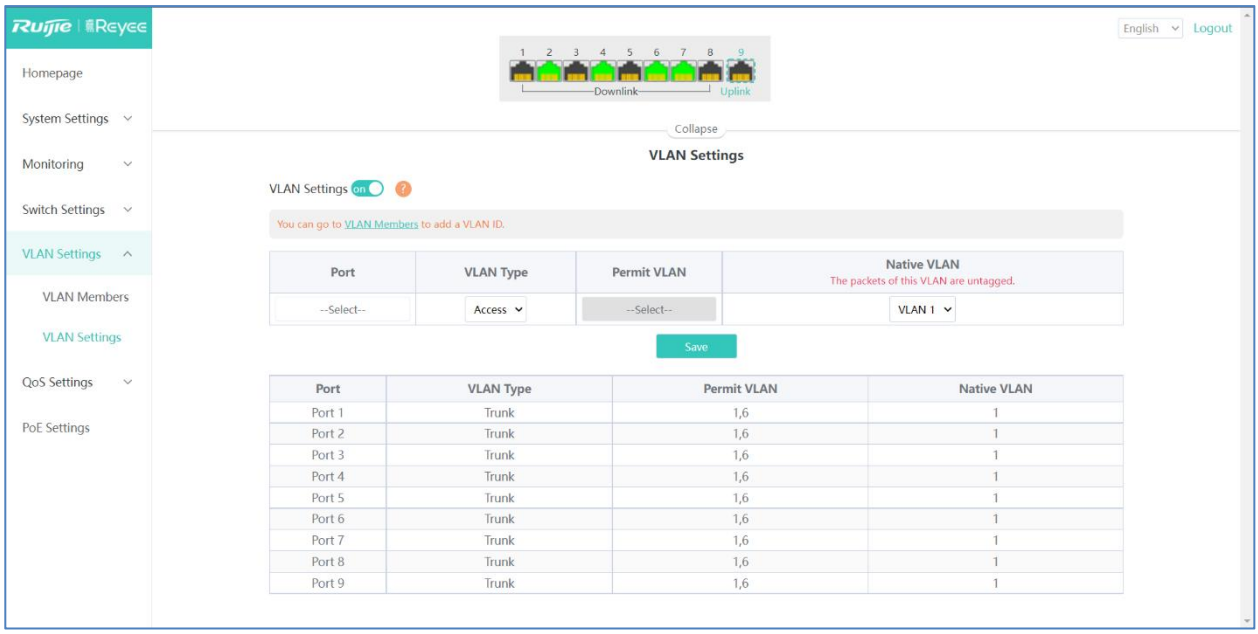
In the **VLAN list**, you can select VLANs and click Delete to delete them in batches.



A VLAN ID bound to the port cannot be deleted.

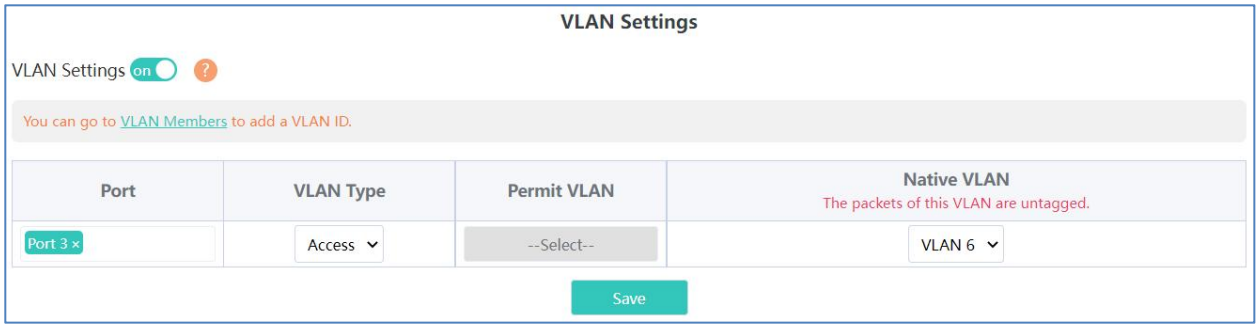
4.2.3.2 VLAN Settings

When **VLAN Settings** is set to **on**, the page is shown in the figure below:



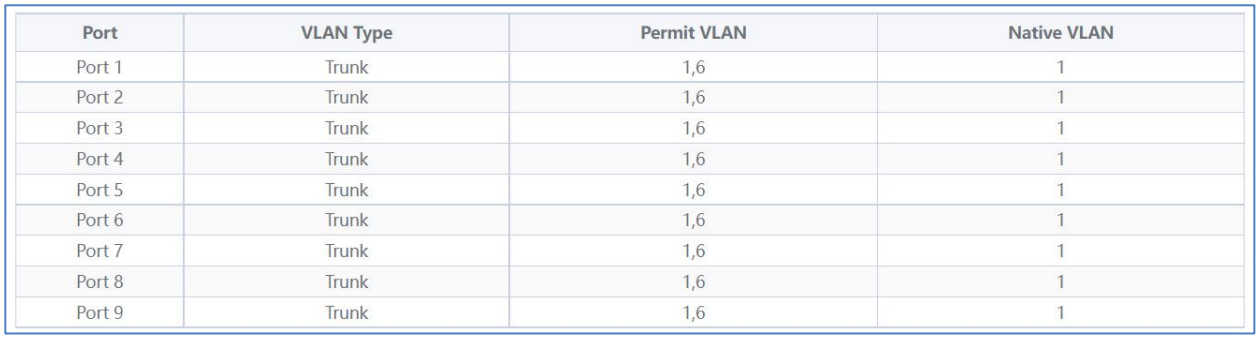
The VLAN Settings page is divided into two parts:

The upper part enables port VLAN configuration. You can select a port, set the VLAN type as (Access or Trunk; when Trunk is selected, Permit VLAN can be configured), Permit VLAN, and Native VLAN, and click **Save** to save the port VLAN configuration:



Native VLAN: The packets of this VLAN are untagged.

The lower part lists the port and VLAN settings:

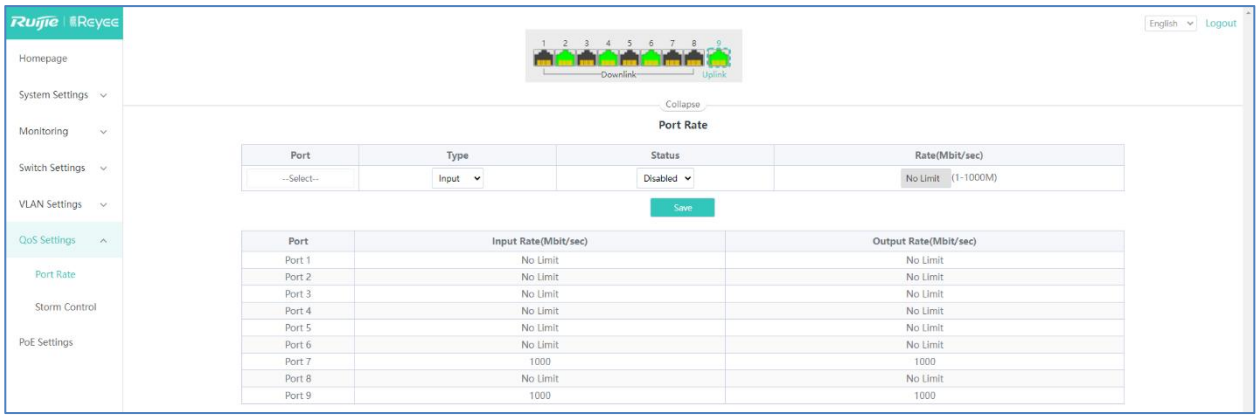


Port	VLAN Type	Permit VLAN	Native VLAN
Port 1	Trunk	1,6	1
Port 2	Trunk	1,6	1
Port 3	Trunk	1,6	1
Port 4	Trunk	1,6	1
Port 5	Trunk	1,6	1
Port 6	Trunk	1,6	1
Port 7	Trunk	1,6	1
Port 8	Trunk	1,6	1
Port 9	Trunk	1,6	1

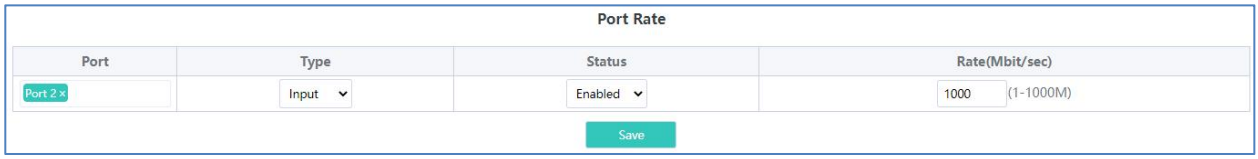
4.2.4 QoS Settings

4.2.4.1 Port Rate

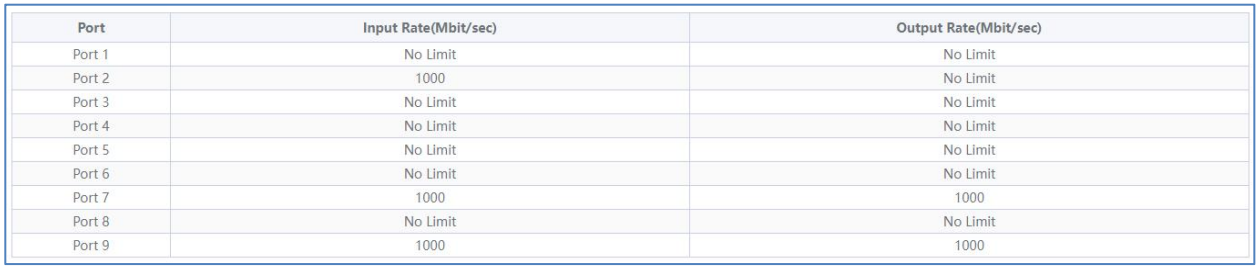
You can configure the input and output rates for a port. The **Port Rate** page is divided into two parts:



Configuration part: Select one or more ports, set the port type and whether to enable rate limiting (if yes, enter the rate limit value of the port), and click Save.



Display part: The input and output rates configured for device ports are displayed.



Port	Input Rate(Mbit/sec)	Output Rate(Mbit/sec)
Port 1	No Limit	No Limit
Port 2	1000	No Limit
Port 3	No Limit	No Limit
Port 4	No Limit	No Limit
Port 5	No Limit	No Limit
Port 6	No Limit	No Limit
Port 7	1000	1000
Port 8	No Limit	No Limit
Port 9	1000	1000

For RG-ES205C-P, the range of the port rate limit is from 1 Mbit/s to 100 Mbit/s.

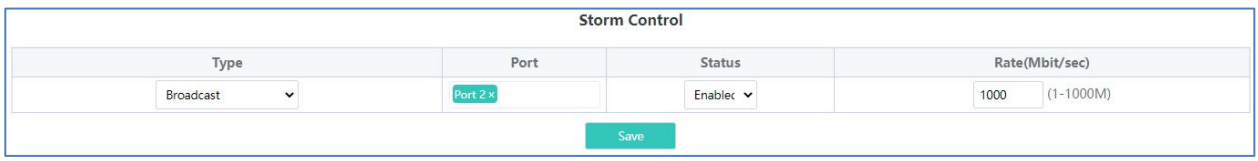
For RG-ES209C-P, the maximum rate is 100 Mbit/s for ports 1–8, and the actual rate is 100 Mbit/s if a greater rate is configured. The range of the port rate limit is from 1 Mbit/s to 1000 Mbit/s for port 9.

For RG-ES226GC-P, RG-ES218GC-P, RG-ES205GC-P, and RG-ES209GC-P, the range of the port rate limit is from 1 Mbit/s to 1000 Mbit/s.

4.2.4.2 Storm Control

The **Storm Control** page is divided into two parts:

Configuration part: Specify the storm control type (Broadcast/Unknown Unicast/Unknown Broadcast), select ports, enable storm control, and enter the storm control rate. Click **Save** to configure storm control.



Display part: The storm control types and rates configured for device ports are displayed (when storm control is enabled, the storm control rates are displayed).

Type	Broadcast(Mbit/sec)	Unknown Unicast(Mbit/sec)	Unknown Broadcast(Mbit/sec)
Port 1	Disabled	Disabled	Disabled
Port 2	1000	Disabled	Disabled
Port 3	Disabled	Disabled	Disabled
Port 4	Disabled	Disabled	Disabled
Port 5	Disabled	Disabled	Disabled
Port 6	Disabled	Disabled	Disabled
Port 7	Disabled	Disabled	Disabled
Port 8	Disabled	Disabled	Disabled
Port 9	Disabled	Disabled	Disabled

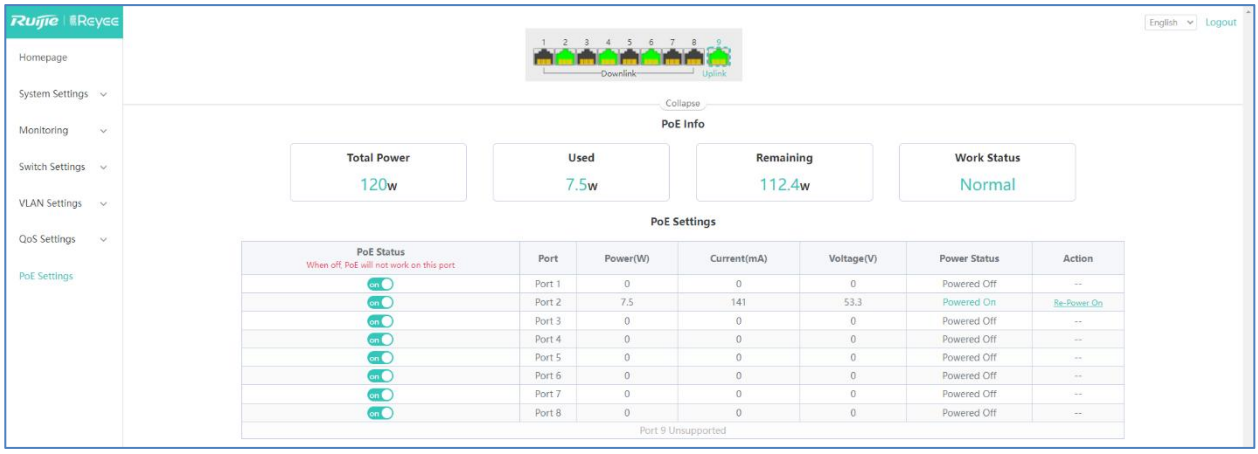
For RG-ES205C-P, the range of the port rate limit is from 1 Mbit/s to 100 Mbit/s.

For RG-ES209C-P, the maximum rate is 100 Mbit/s for ports 1–8, and the actual rate is 100 Mbit/s if a greater rate is configured. The range of the port rate limit is from 1 Mbit/s to 1000 Mbit/s for port 9.

For RG-ES226GC-P, RG-ES218GC-P, RG-ES205GC-P, and RG-ES209GC-P, the range of the port rate limit is from 1 Mbit/s to 1000 Mbit/s.

4.2.5 PoE Settings

The PoE system status and PoE port status of the device are displayed.



System status: The total power, used power, remaining power, and work status of the PoE function of the device are displayed.

Port status: The PoE voltage, current, power, and current power status of ports are displayed. You can choose whether to enable PoE function on a port and restart PDs.

PoE Status When off, PoE will not work on this port	Port	Power(W)	Current(mA)	Voltage(V)	Power Status	Action
on	Port 1	0	0	0	Powered Off	--
on	Port 2	7.5	141	53.3	Powered On	Re-Power On
on	Port 3	0	0	0	Powered Off	--
on	Port 4	0	0	0	Powered Off	--
on	Port 5	0	0	0	Powered Off	--
on	Port 6	0	0	0	Powered Off	--
on	Port 7	0	0	0	Powered Off	--
on	Port 8	0	0	0	Powered Off	--
Port 9 Unsupported						

Fiber ports (last two ports) of RG-ES226GC-P and RG-ES218GC-P do not support the PoE function.

Disabling PoE on a port will stop powering downlink devices connected to the port.

4.3 Reyee NBS Series Switches Configuration

4.3.1 VLAN

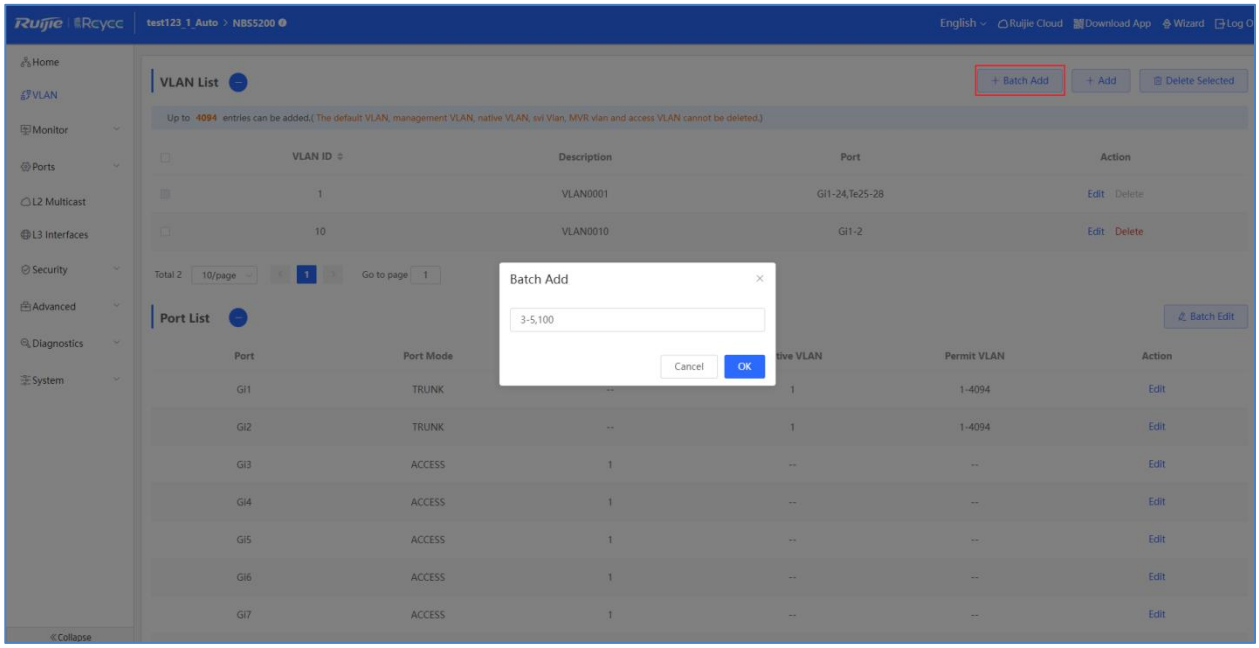
4.3.1.1 VLAN List

In the **VLAN List** screen, you can add and delete VLANs and edit the VLAN description. The time for loading the VLAN page increases when there are many VLAN entries.

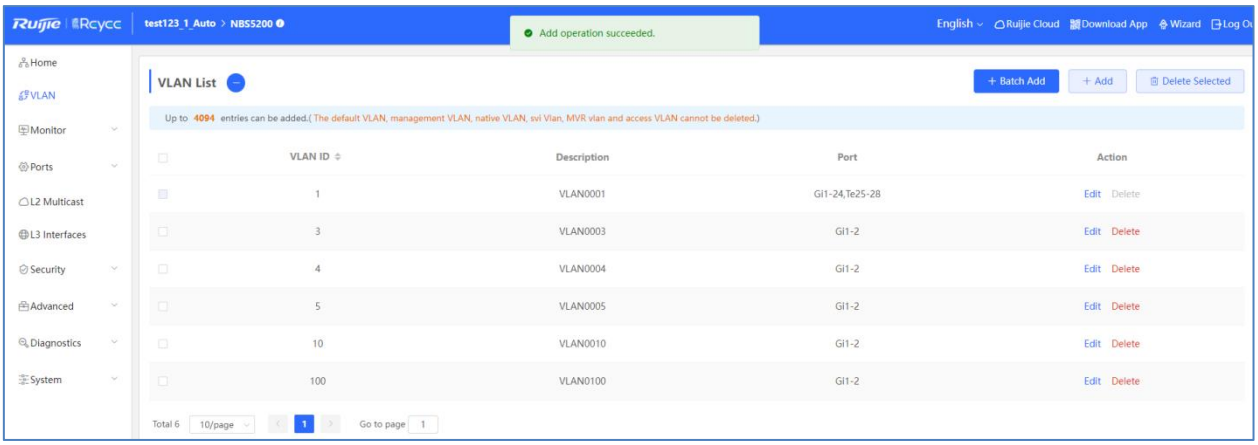
Batch adding VLANs/Adding a single VLAN

The VLAN range is 1–4094.

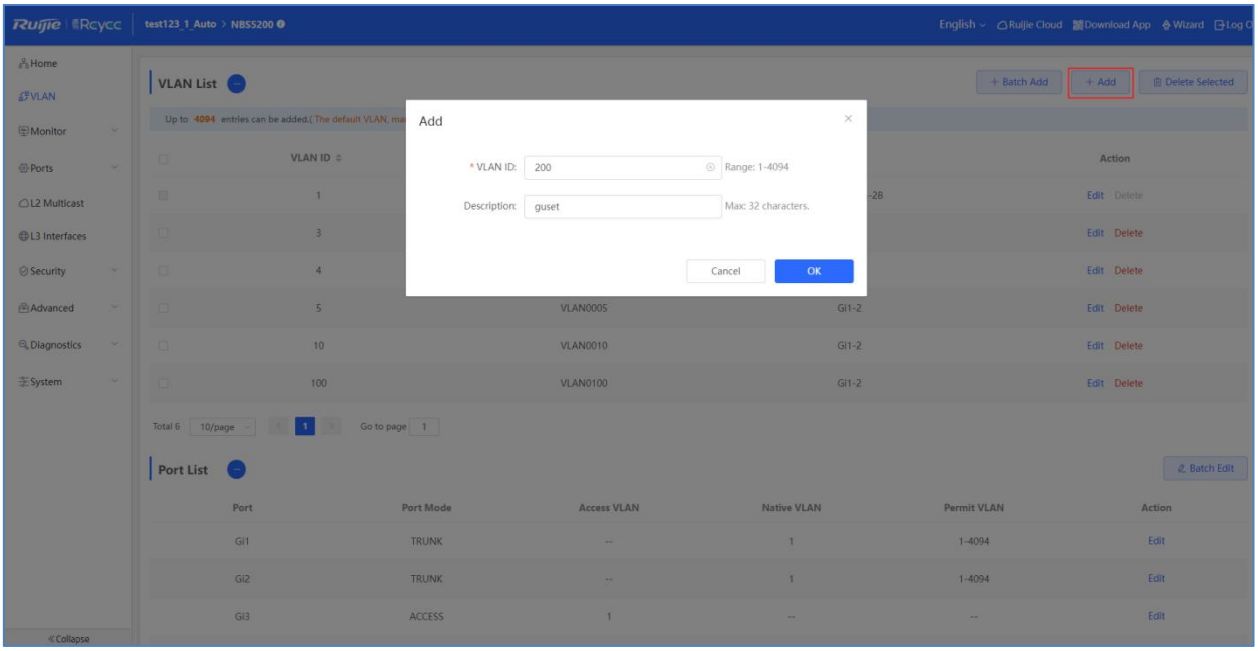
Click **Batch Add**. In the displayed dialog box, enter VLANs or a VLAN range (separate multiple VLANs by using commas (",")), and click **OK.**



The added VLANs are displayed in **VLAN List.**

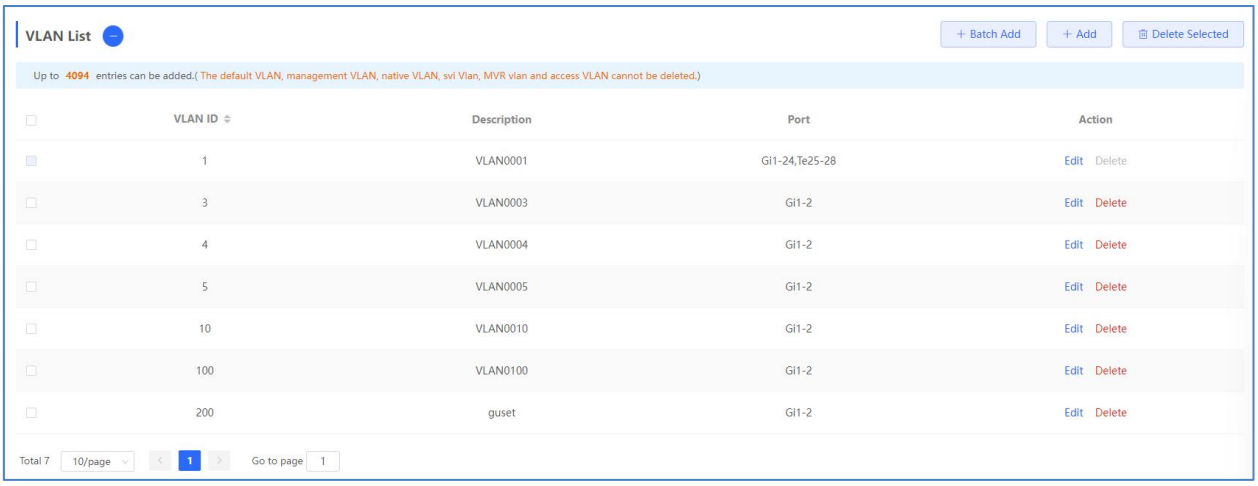


Click **Add**. In the displayed dialog box, enter the VLAN (mandatory) and VLAN description, and click **OK.**



If no **VLAN descriptions** are configured when VLANs are added, the system creates VLAN descriptions in corresponding formats, for example, VLAN000XX. VLAN descriptions **cannot be repeated.**

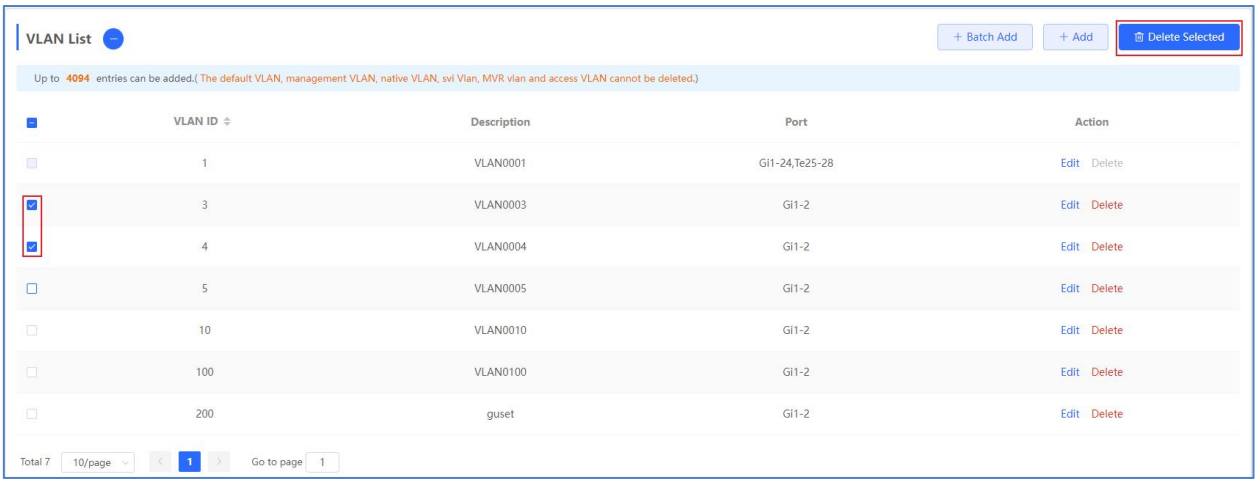
The added VLAN is displayed in **VLAN List.**



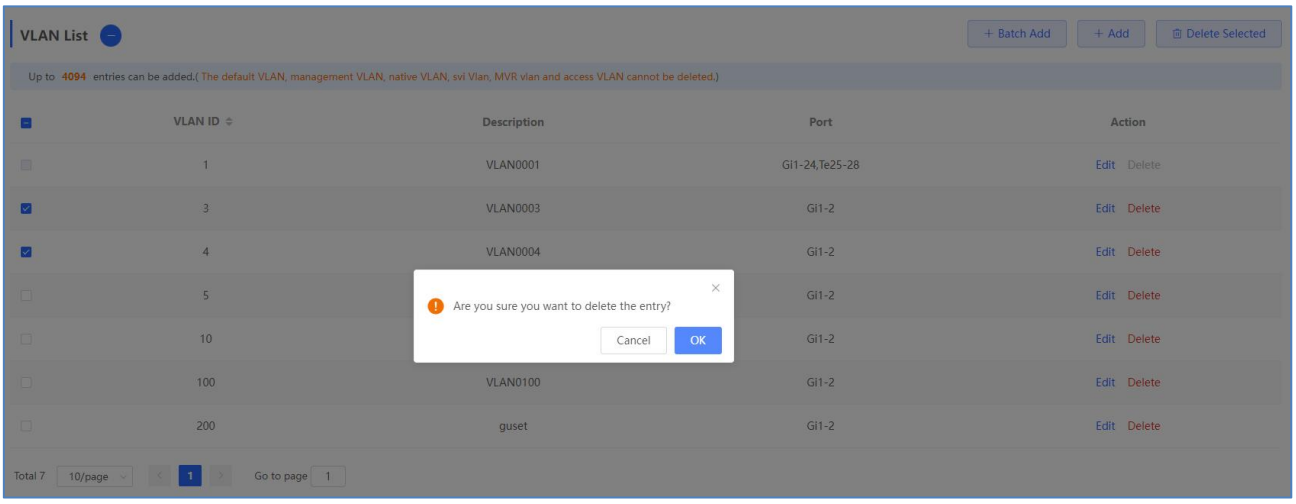
Batch adding VLANs/Adding a single VLAN

The default VLAN (VLAN 1), management VLAN, native VLAN, and access VLAN **cannot be deleted.**

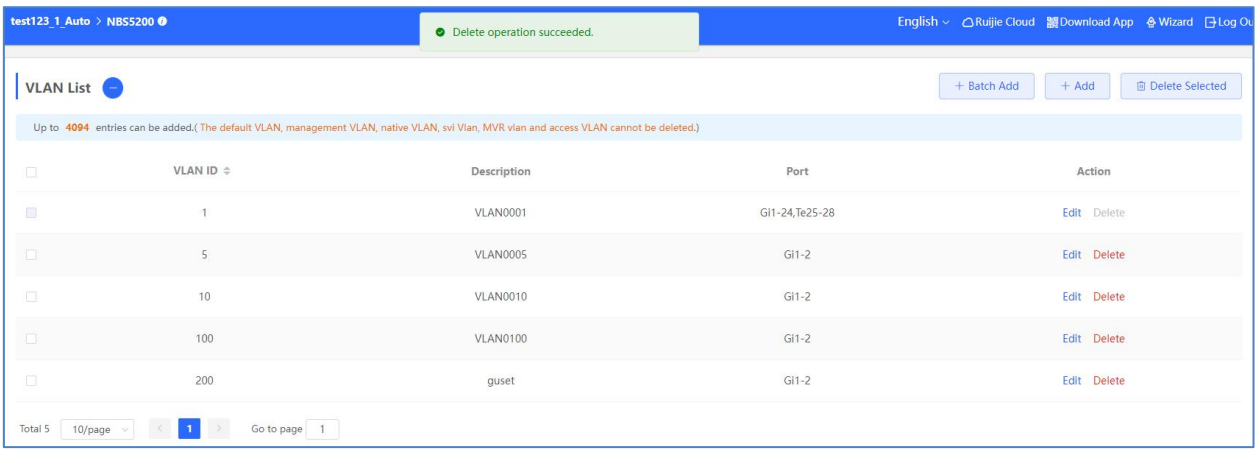
Select multiple entries in **VLAN List** and click **Delete Selected.**



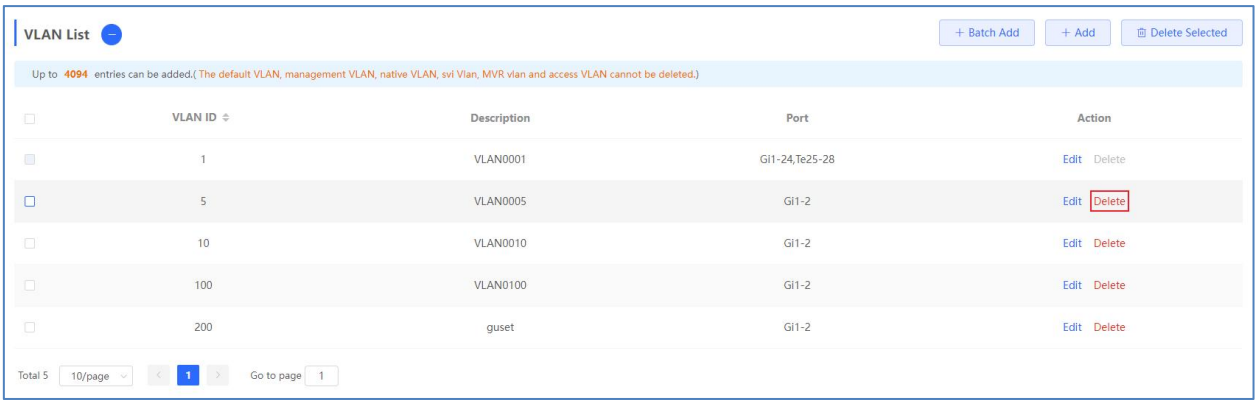
The message "Are you sure you want to delete the VLAN?" is displayed. In the displayed dialog box, click **OK**.



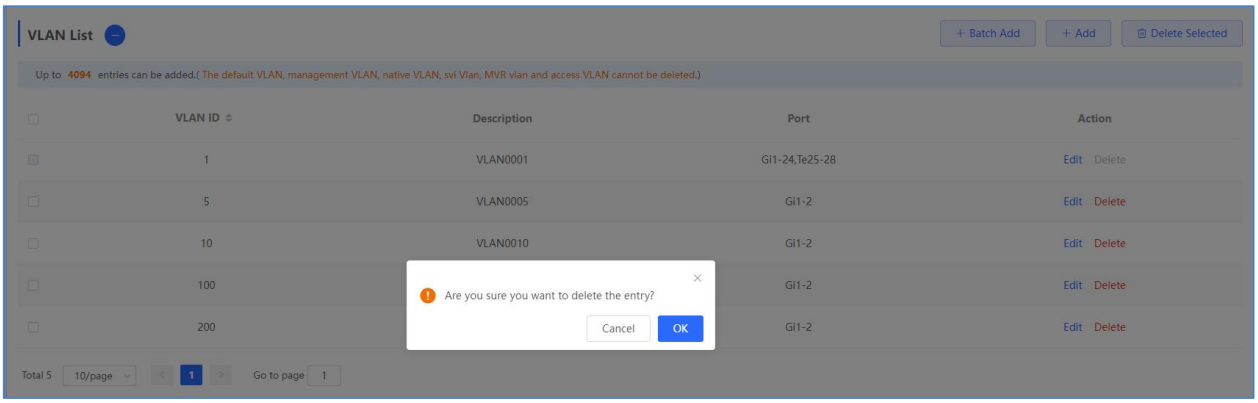
The message "Delete operation succeeded." is displayed, the selected VLANs will be deleted in **VLAN List.**



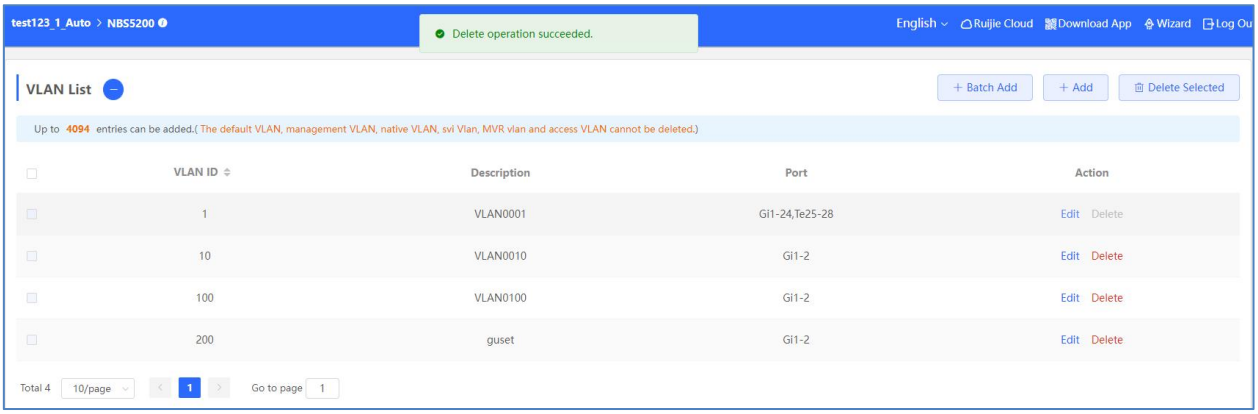
Click **Delete** in the **Action** column.



The message "Delete operation succeeded." is displayed, the selected VLANs will be deleted in **VLAN List.**

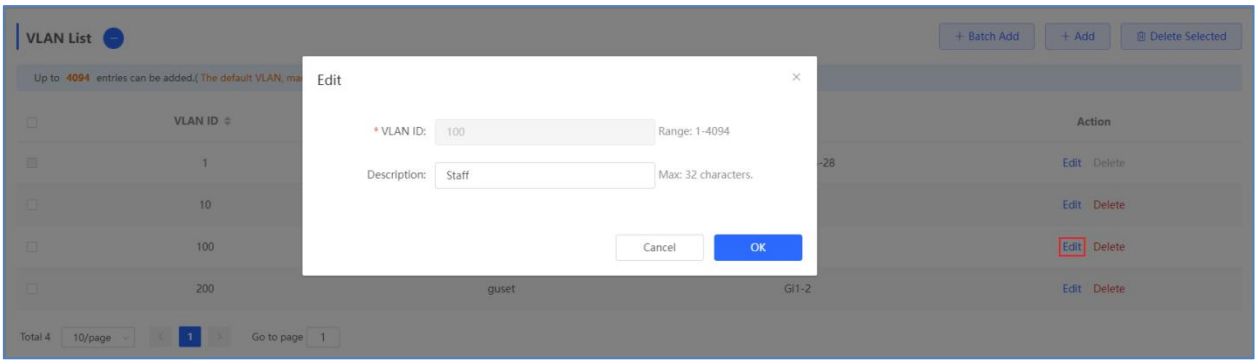


The message "Delete operation succeeded." is displayed, the selected VLAN will be deleted in **VLAN List.**

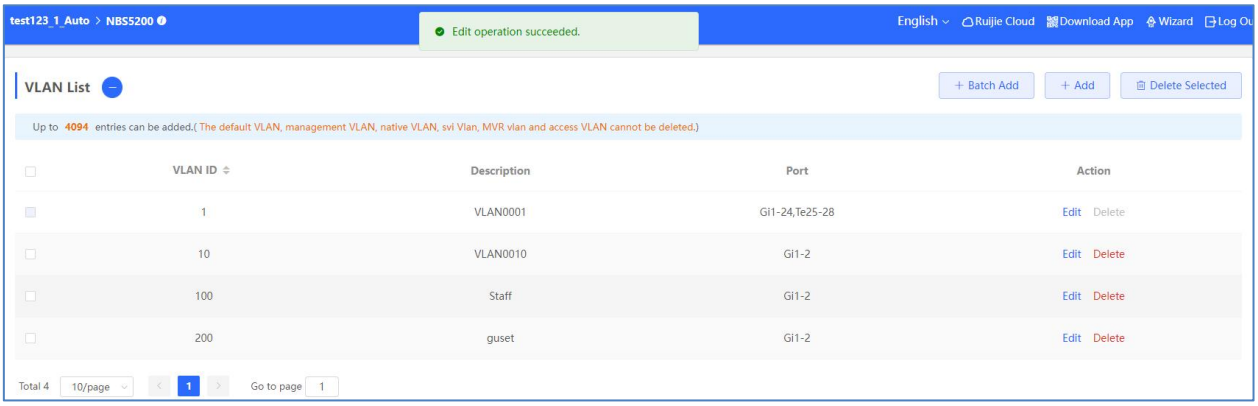


Editing a VLAN

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



The message "Edit operation succeeded." is displayed



4.3.1.2 Port List

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

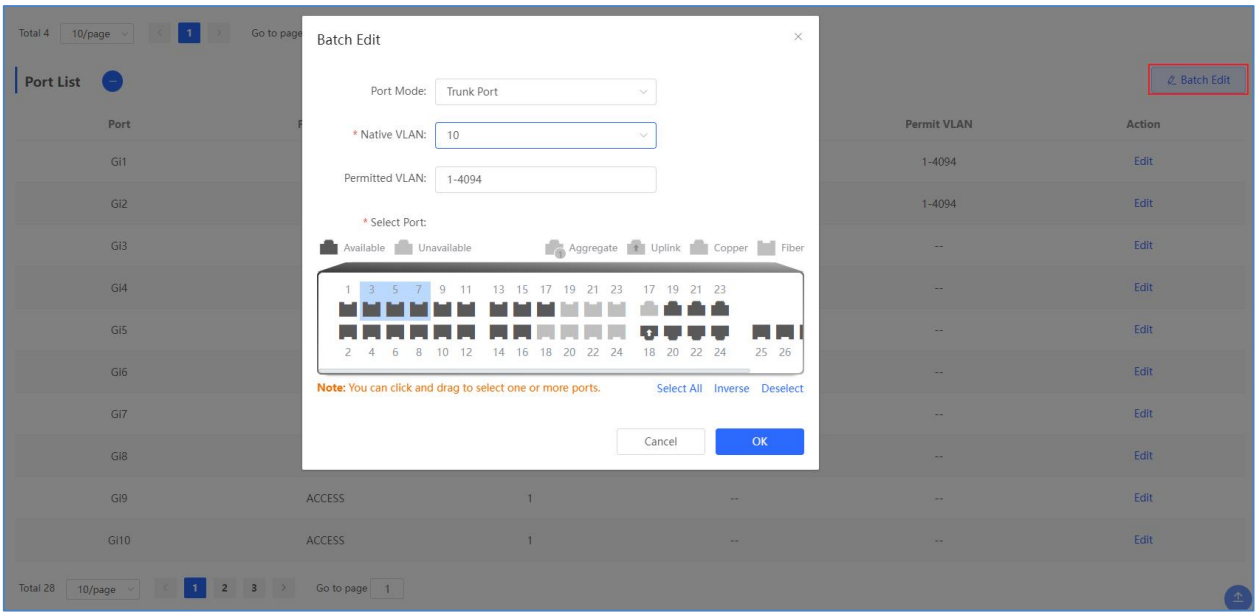
Improper configuration of port VLANs may lead to failure in accessing the eWeb management system. Exercise caution during the configuration.

In **Access Port** mode, if an access VLAN is configured, only packets tagged with the corresponding access VLAN ID are permitted. Untagged packets are automatically tagged with this VLAN ID.

In **Trunk Port** mode, if a native VLAN is configured, untagged packets are automatically tagged with the corresponding native VLAN ID. Generally, the native VLAN is included in a permitted VLAN range. Otherwise, data may be blocked.

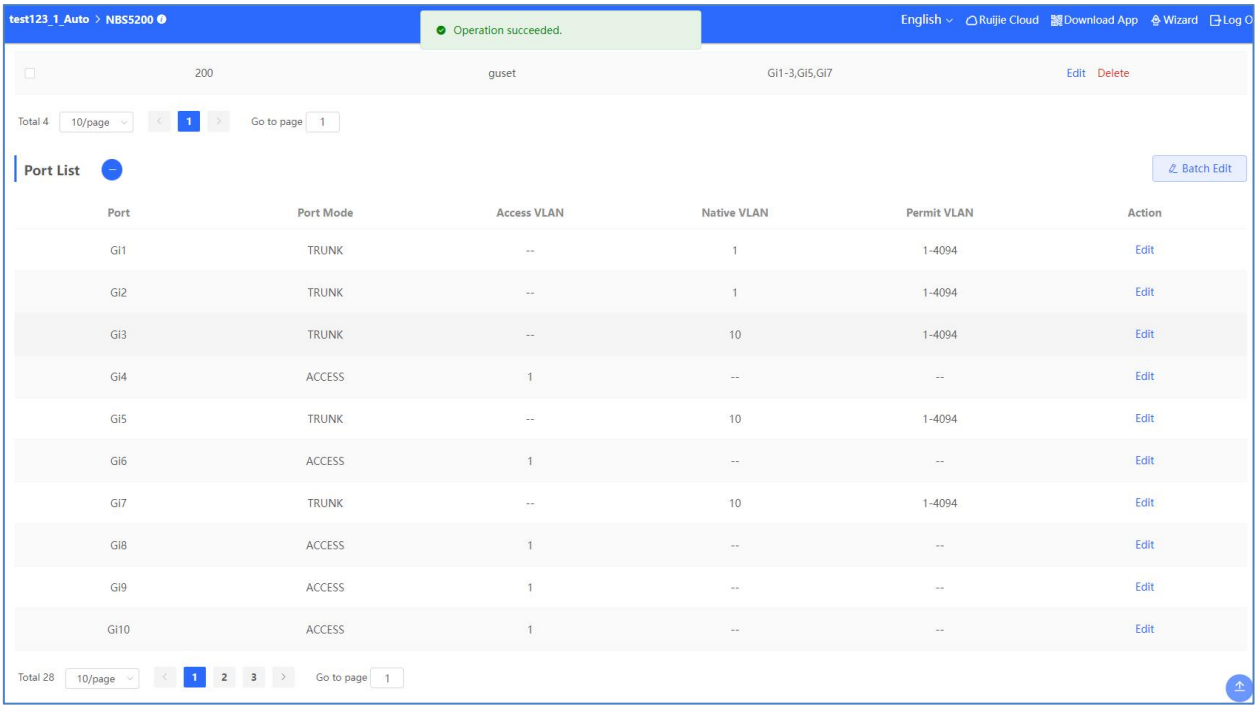
Batch editing ports

Click **Batch Edit**. In the displayed dialog box, select a port mode, select the required port, set the native VLAN or access VLAN, and click **OK**.



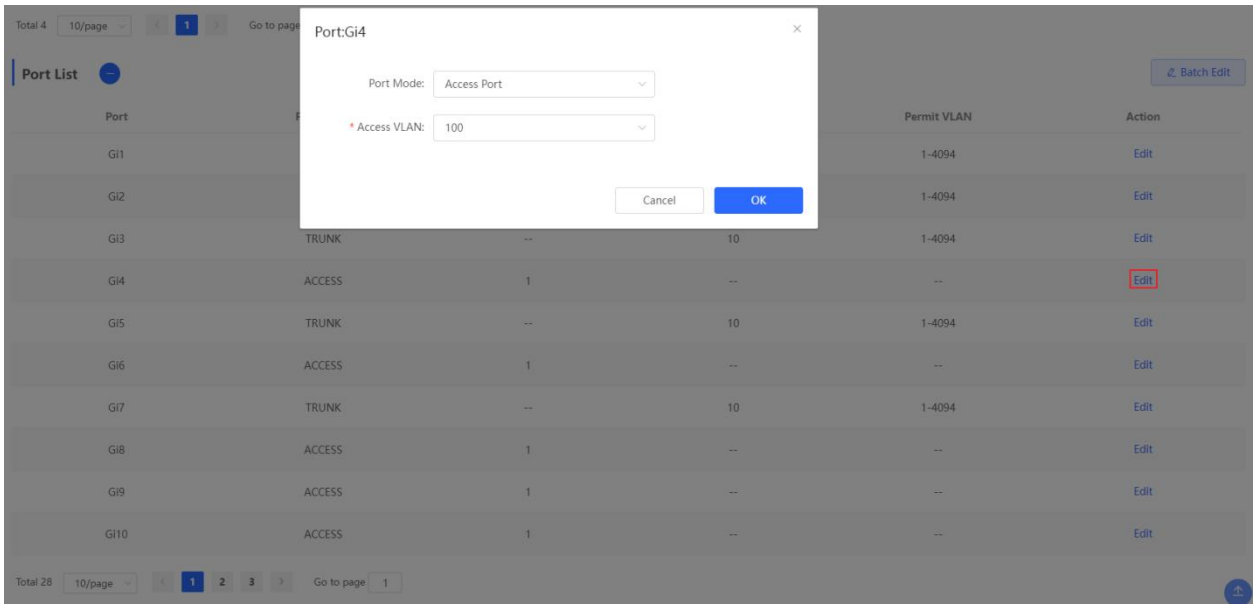
Select ports on the port panel and set the port mode to Access Port or Trunk Port. In Trunk Port mode, configure permitted VLAN ranges (separated by commas ","), set VLAN IDs for the ports, and click OK. The port list and VLAN list will be updated correspondingly.

The message "Operation succeeded." is displayed.

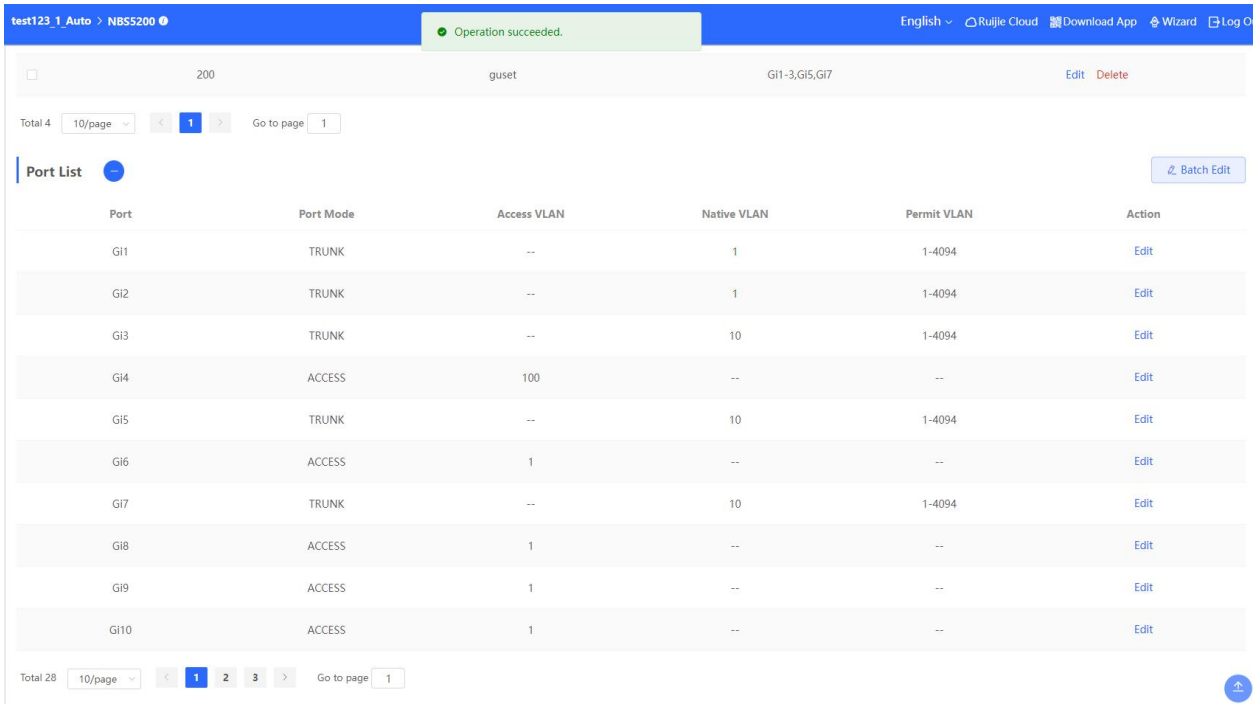


Editing a single port

Click **Edit** in the **Action** column, configure the port mode and VLAN, and click **OK**.



The message "Operation succeeded." is displayed.

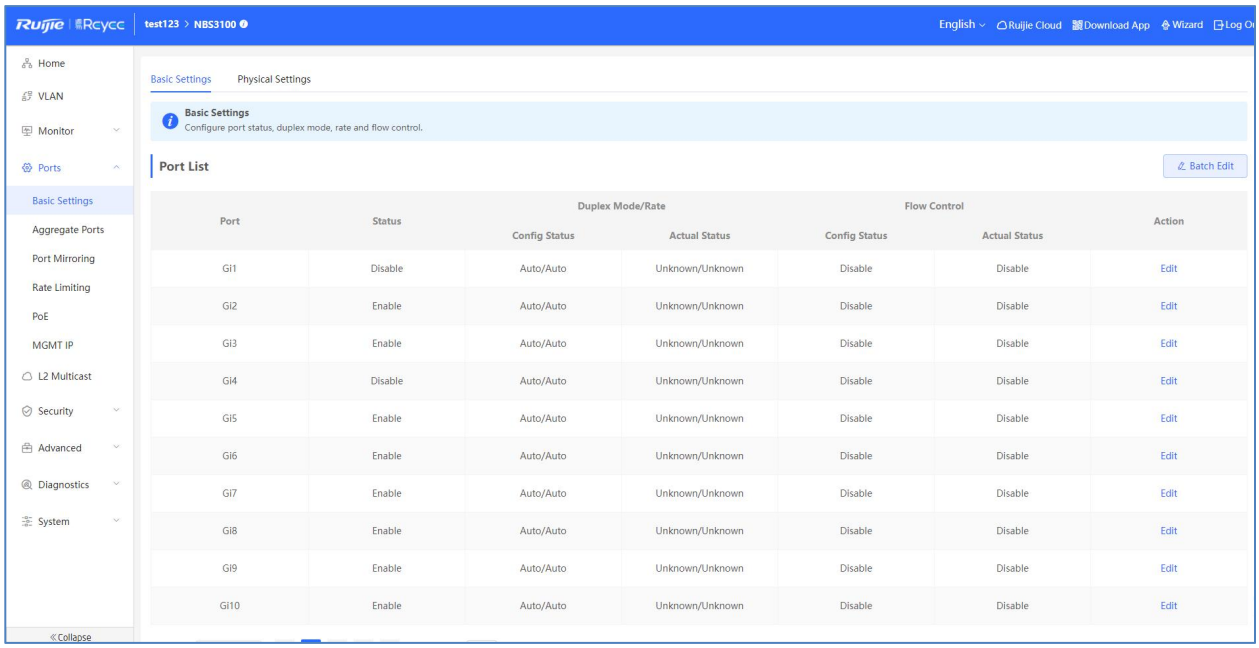


4.3.2 Ports

4.3.2.1 Basic Settings

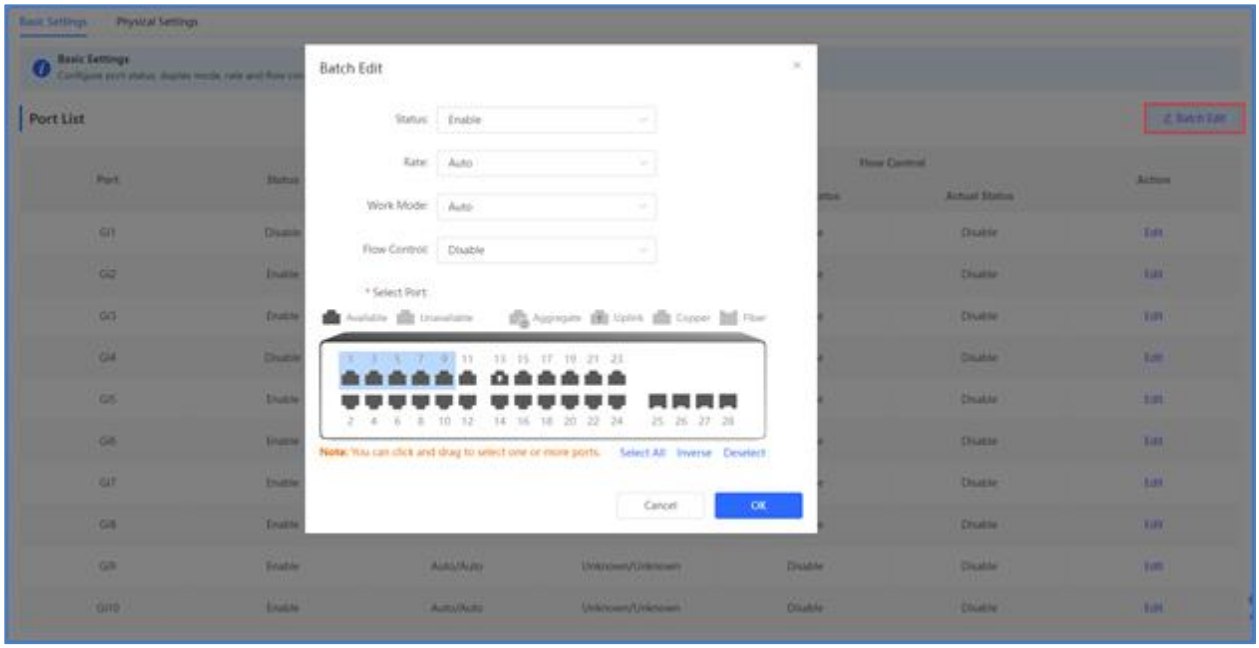
1.1 Basic Settings

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

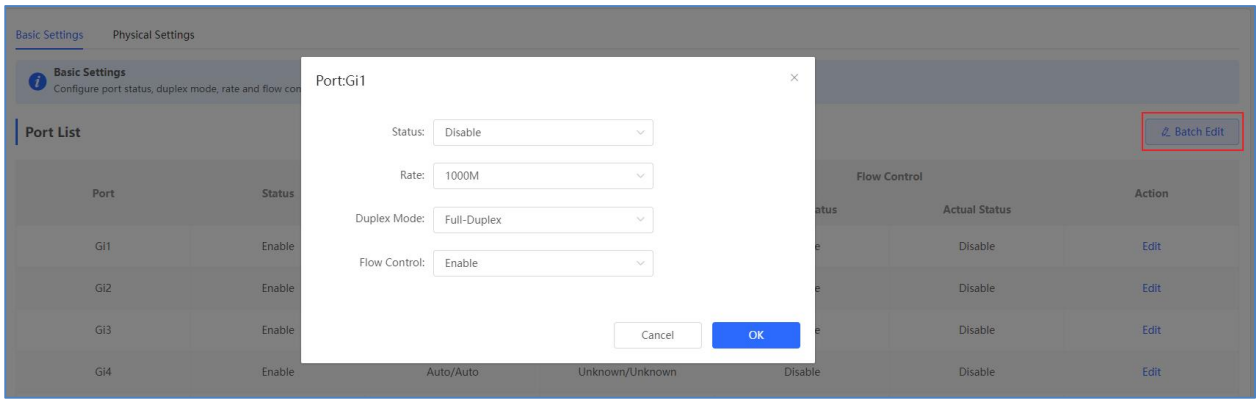


Configuration items for ports with different attributes (1000M port, 10G port, and fiber port) vary. During batch configuration, only the common configuration items are configurable.

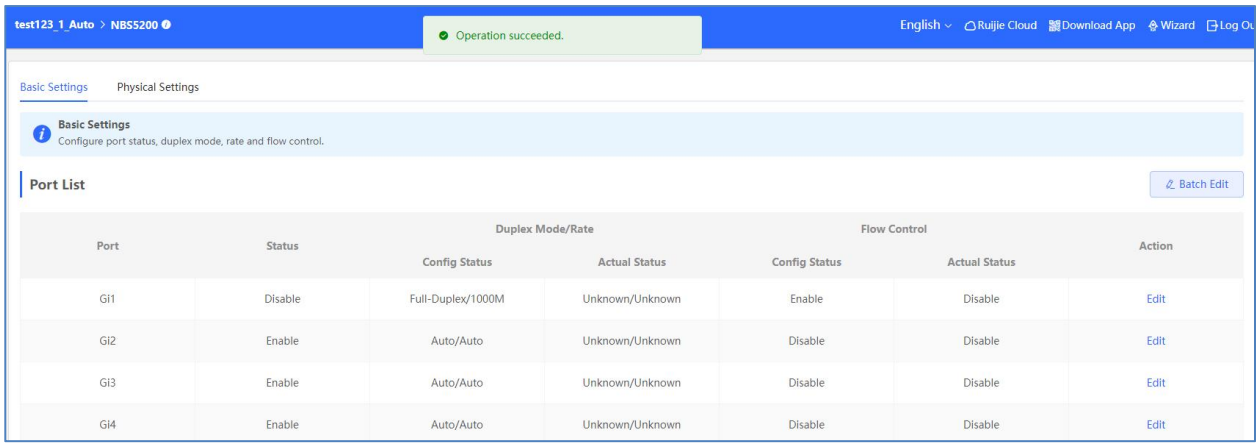
Click **Batch Edit.** In the displayed dialog box, select the target port, set the port status, speed, and mode, and click **OK.**



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



The message "Delete operation succeeded." is displayed.

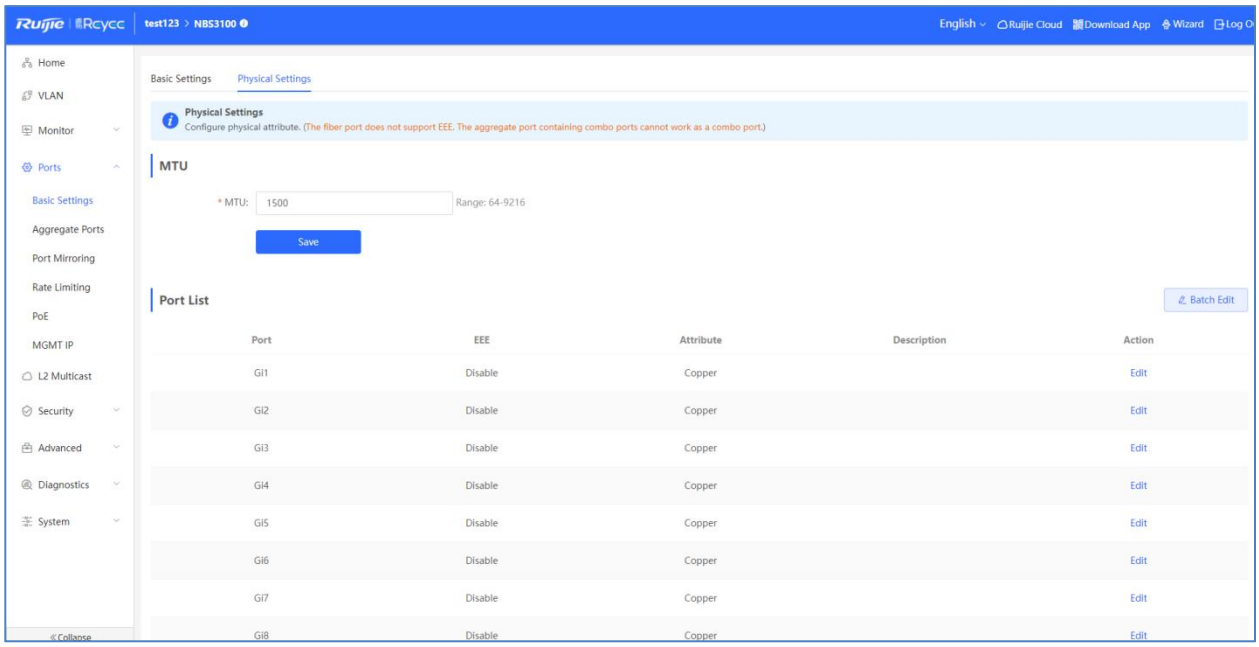


1.2 Physical Settings

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

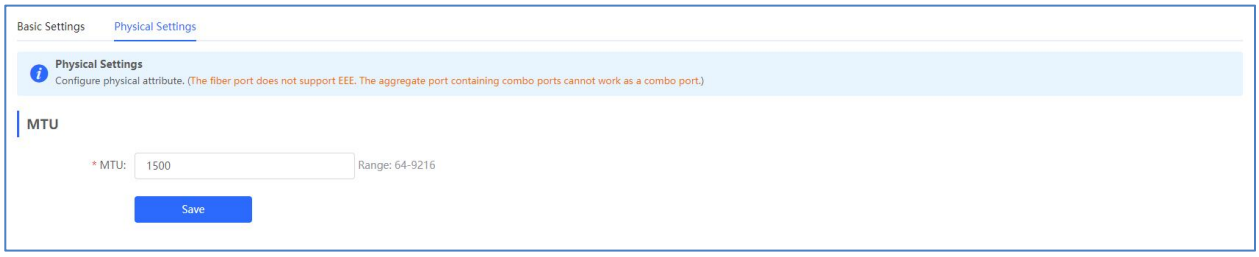
MTU Configuration

The page of NBS3100/3200 series switches is as below:



The series of NBS3100/3200 supports MTU global configuration, but cannot configure it based on specified port.

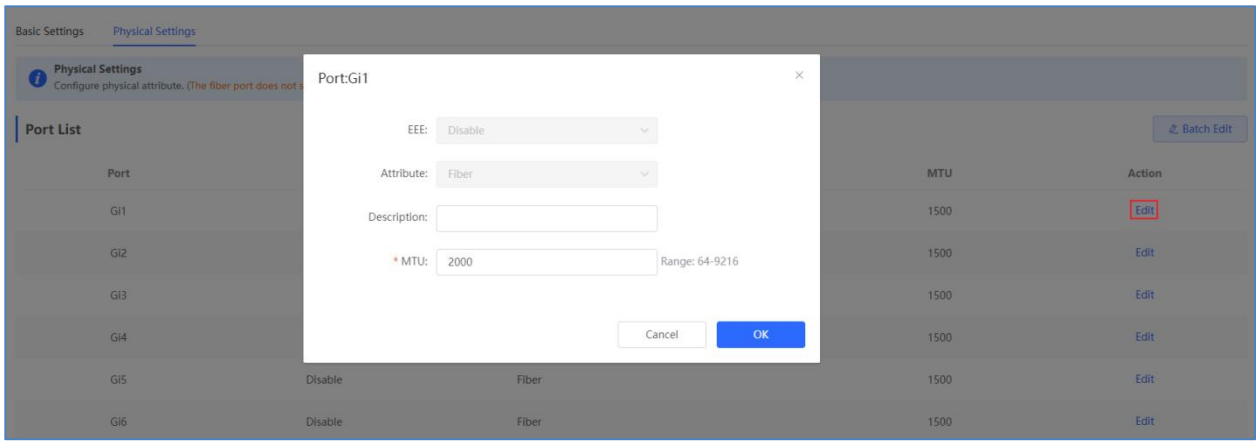
Enter the MTU value and then click “Save” the value range of MTU is within 64-9216.



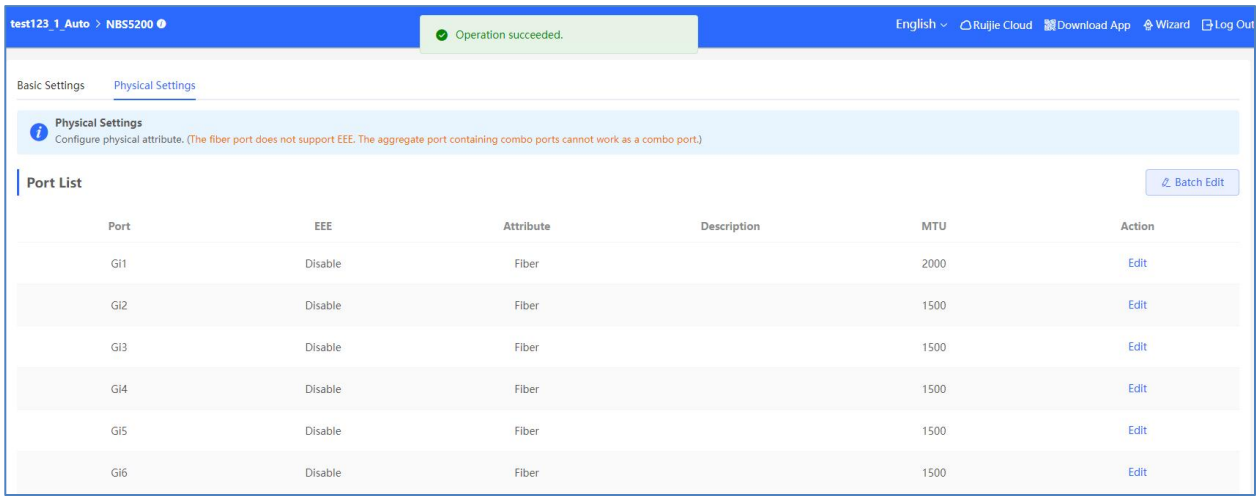
NBS5100/5200 supports MTU configuration based on single or multiple ports

Configure MTU value for a single port:

Click **Edit** in the **Action** column,and enter the MTU value in the dialog box, then save theconfigure by clicking **OK**.

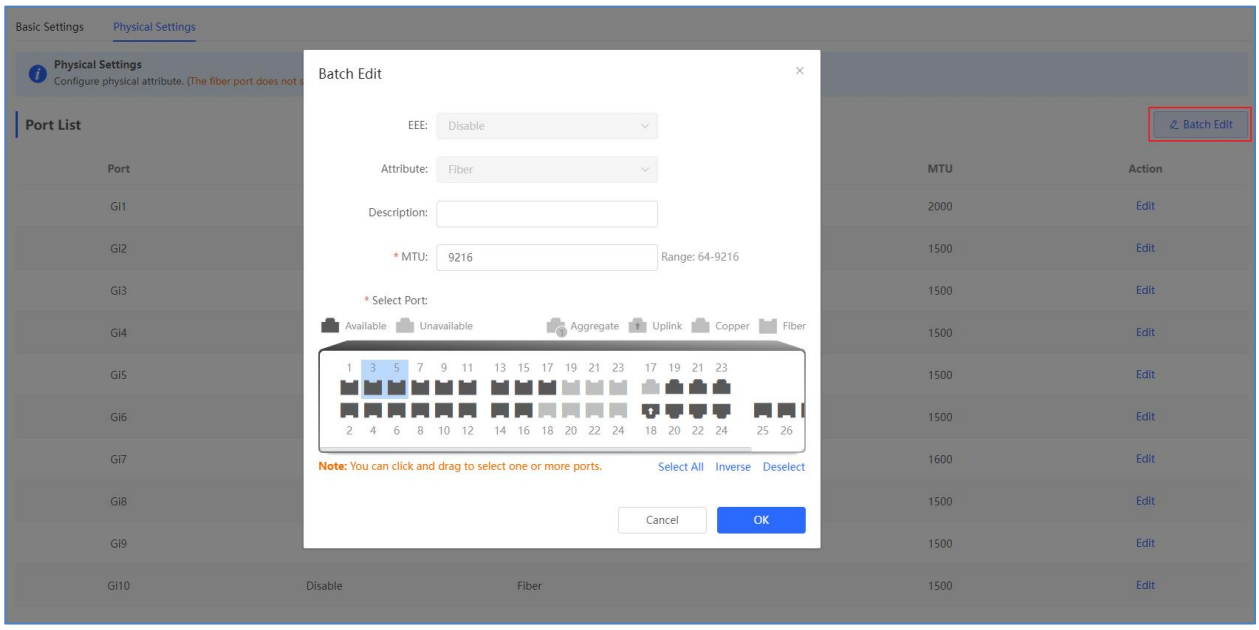


The displaying of “Operation Succeeded” indicate the action of modifying MTU value for the port have been succeed

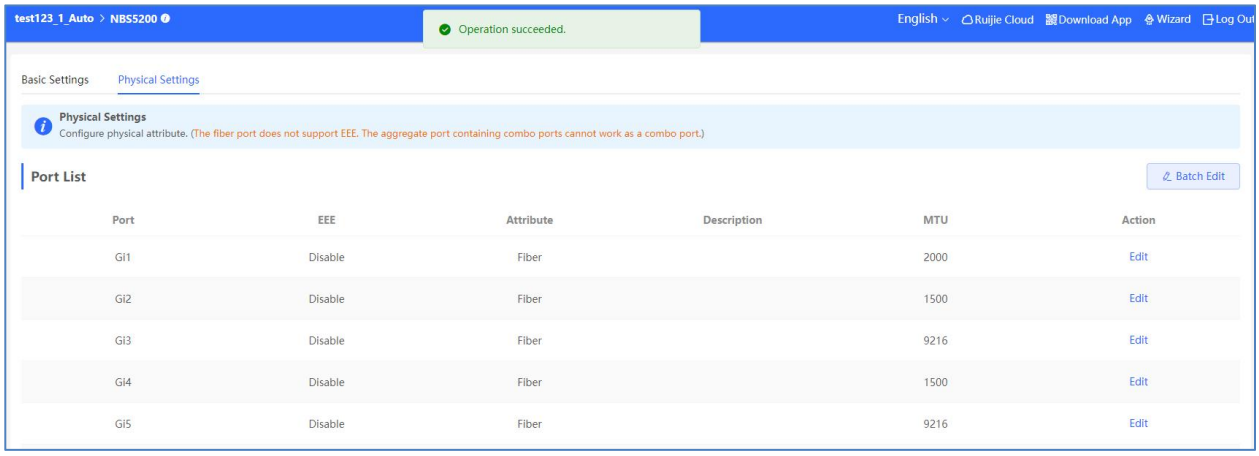


Configure NTU value for multiple ports:

Click Batch Edit to choose the port, and then enter the MTU value and click **OK** to save the configuration.

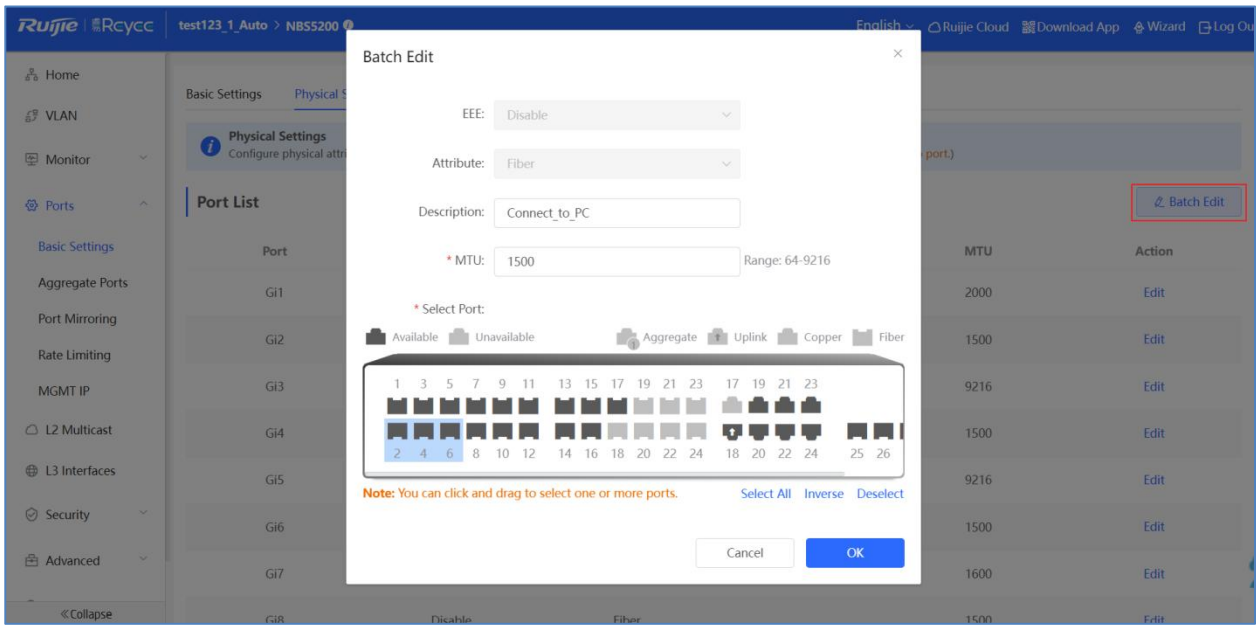


When displaying “Operation Succeeded” means the action of modifying the MTU value to the port have been succeed.

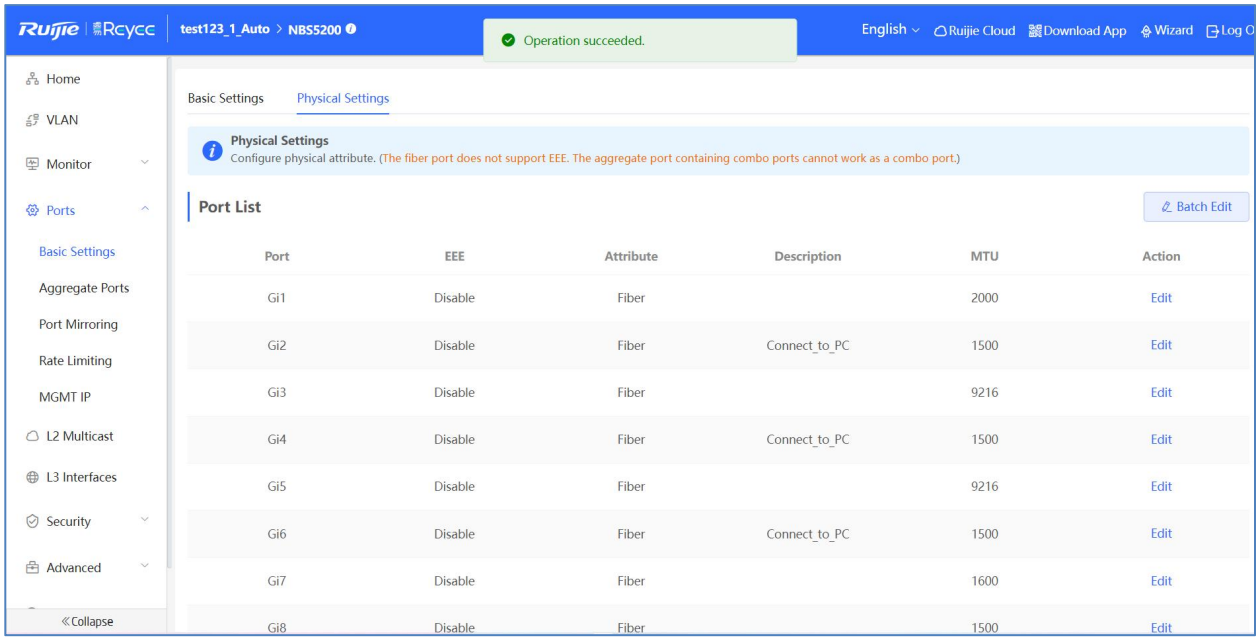


Batch editing ports

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



The message "Operation succeeded." is displayed.

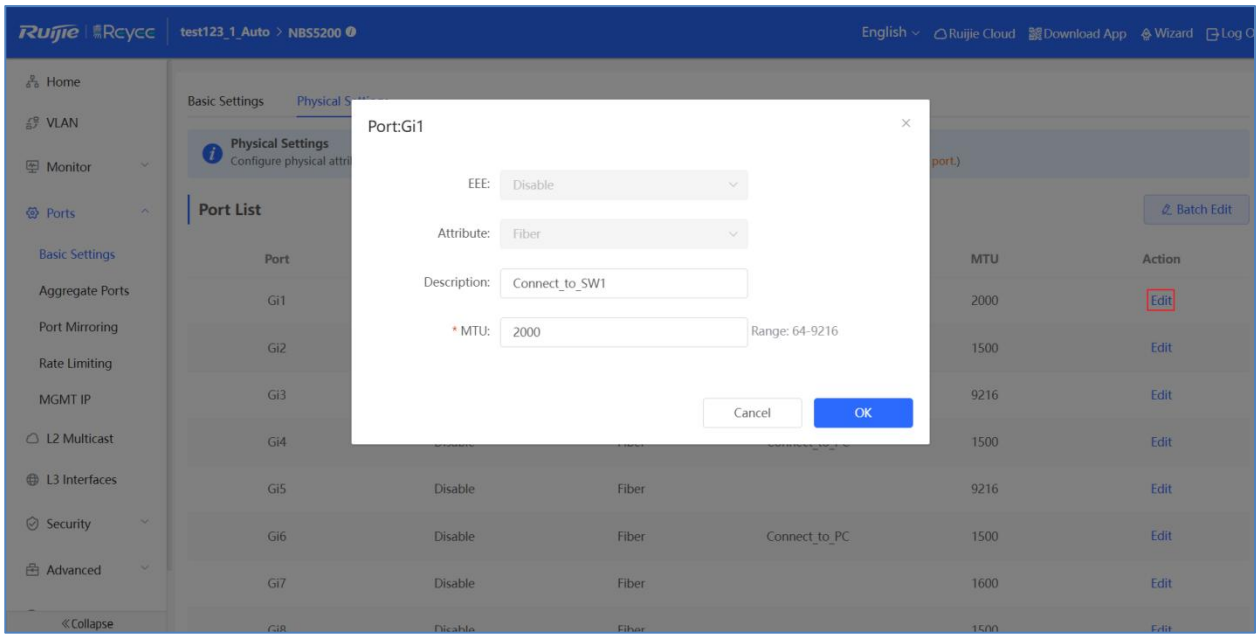


Copper ports and fiber ports cannot be simultaneously configured during batch configuration.

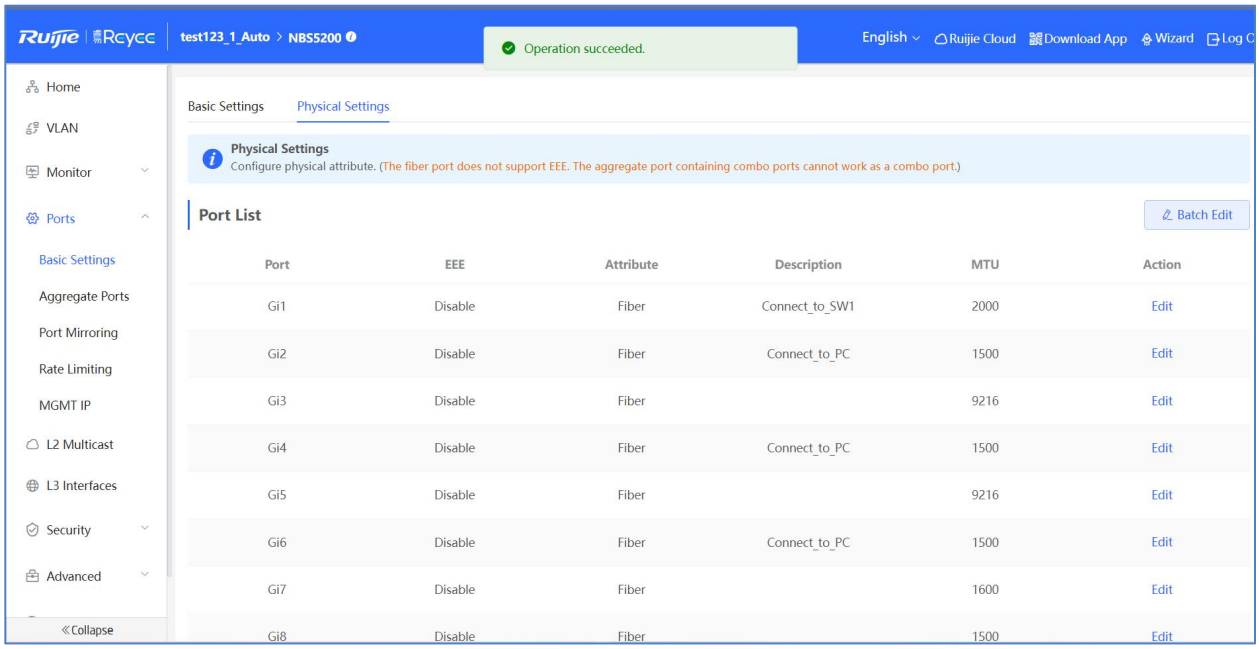
Fiber ports do not support EEE configuration.

Editing a single port

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



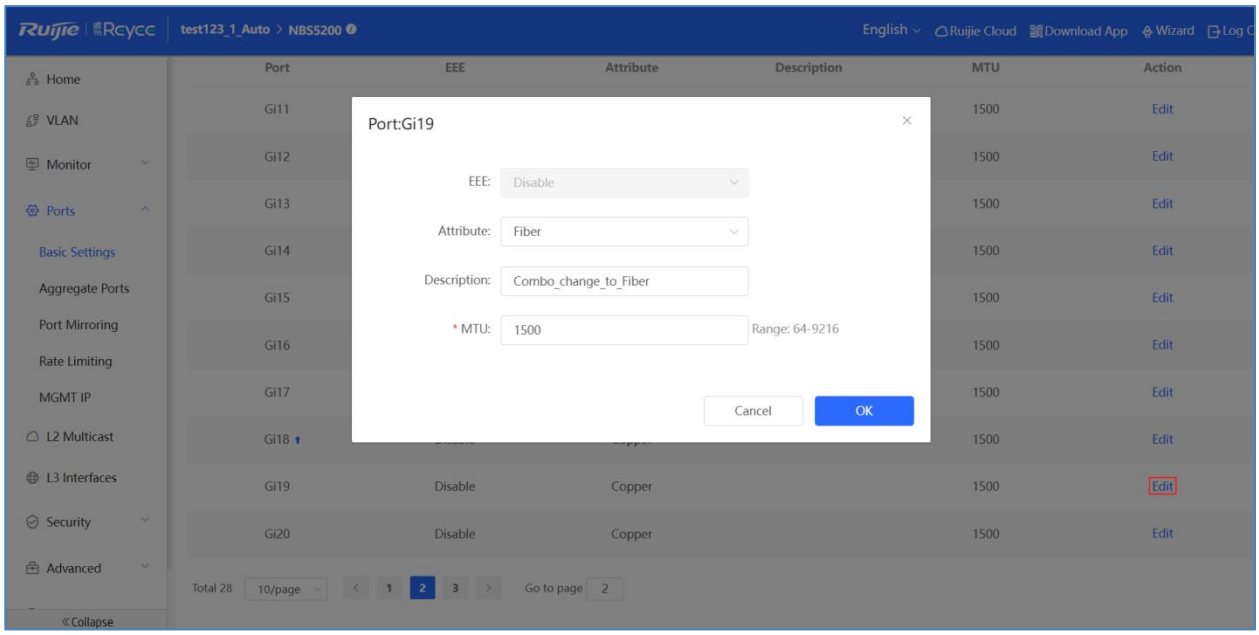
The message "Operation succeeded." is displayed.



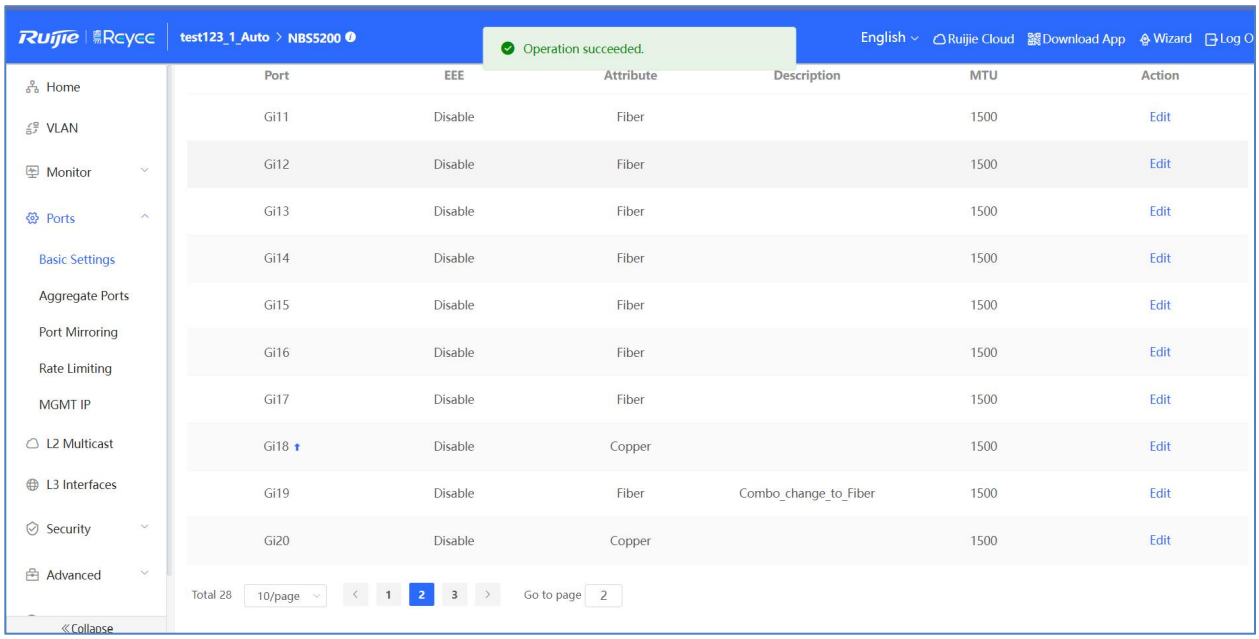
Port mode switchover

Only the SFP combo ports support port mode switchover.

Click **Edit** in the **Action** column. In the displayed dialog box, set the port mode to **Fiber** or **Copper** (by default), and click **OK.**

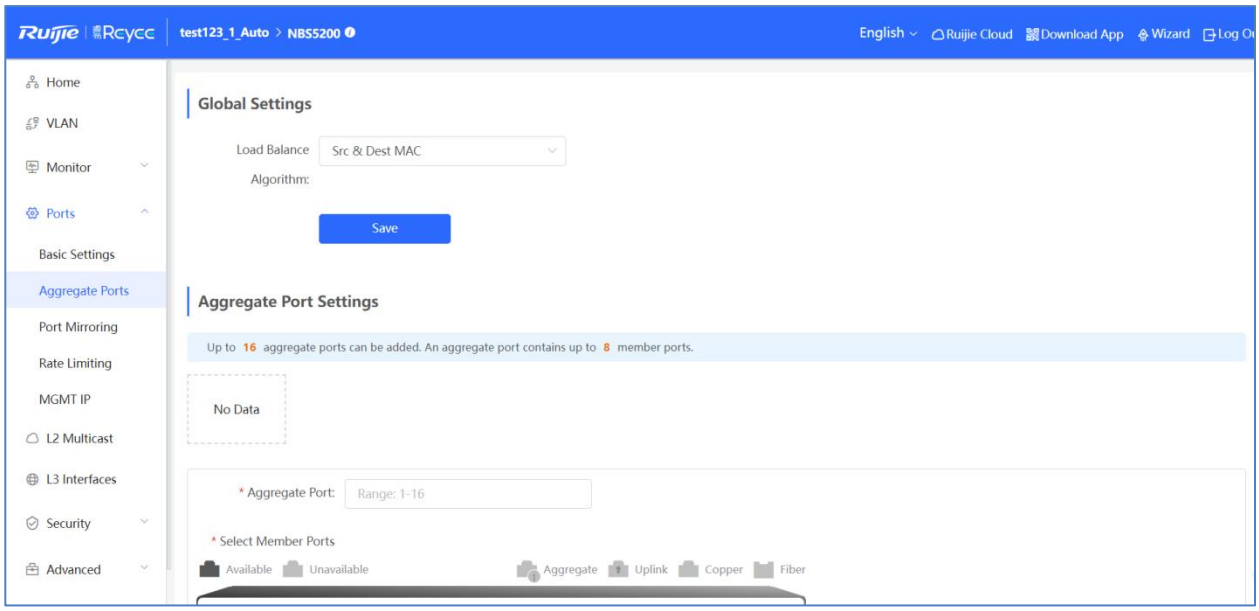


The message "Operation succeeded." is displayed.



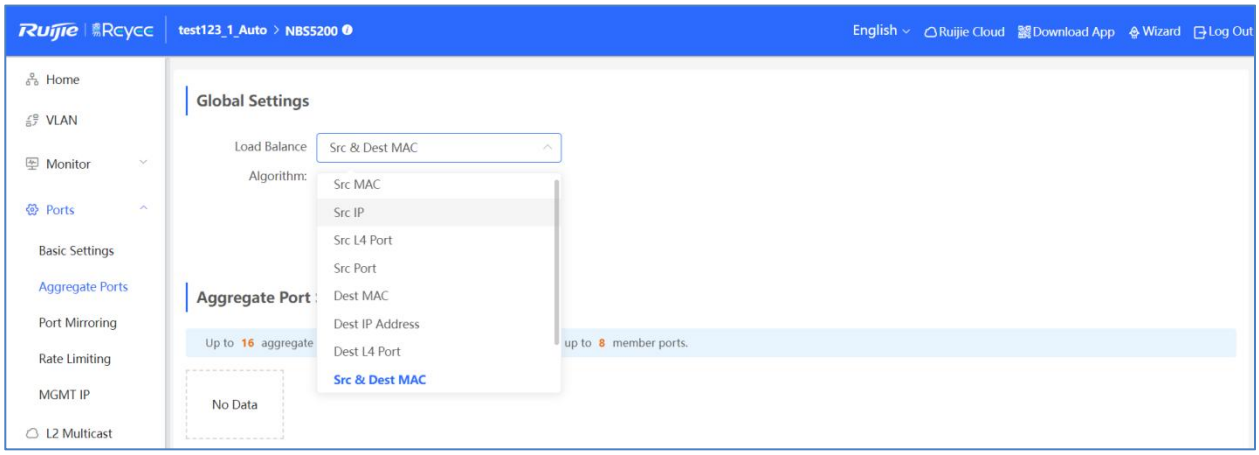
4.3.2.2 Aggregate Ports

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



1.1 Global Settings

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

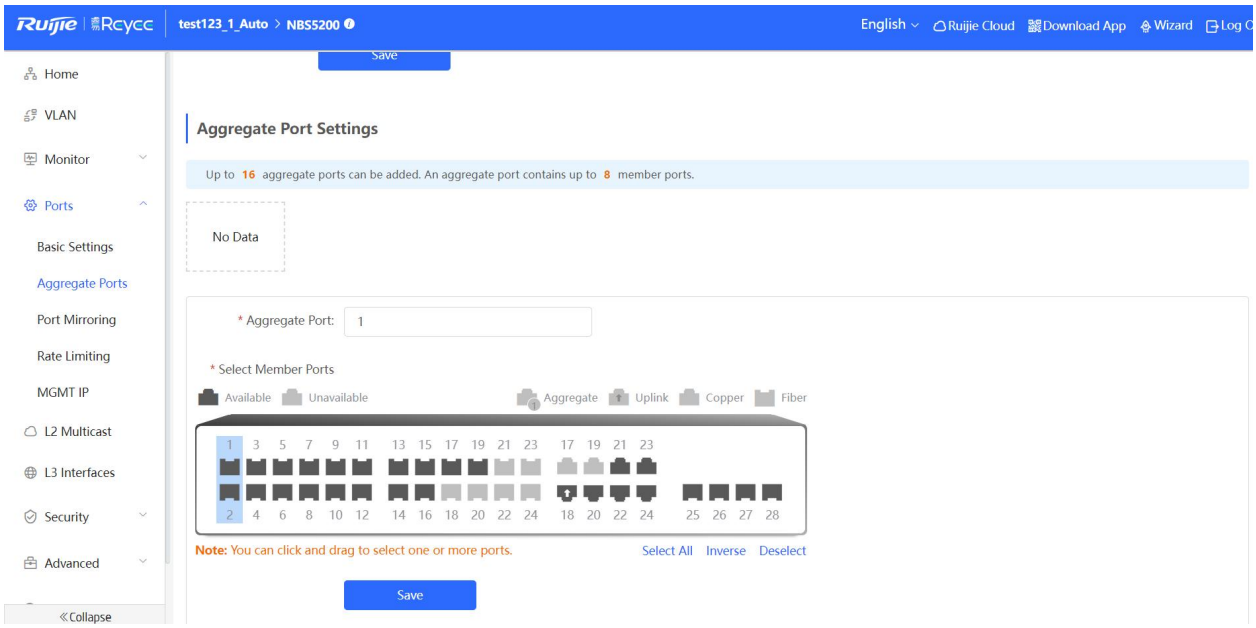


The ports supported load balance algorithms are Src MAC, Src IP, Src L4 Port, Src Port, Dest MAC, Dest IP Address, Dest L4 Port, Src & Dest MAC, Src & Dest IP Address, Src & Dest L4 Port.

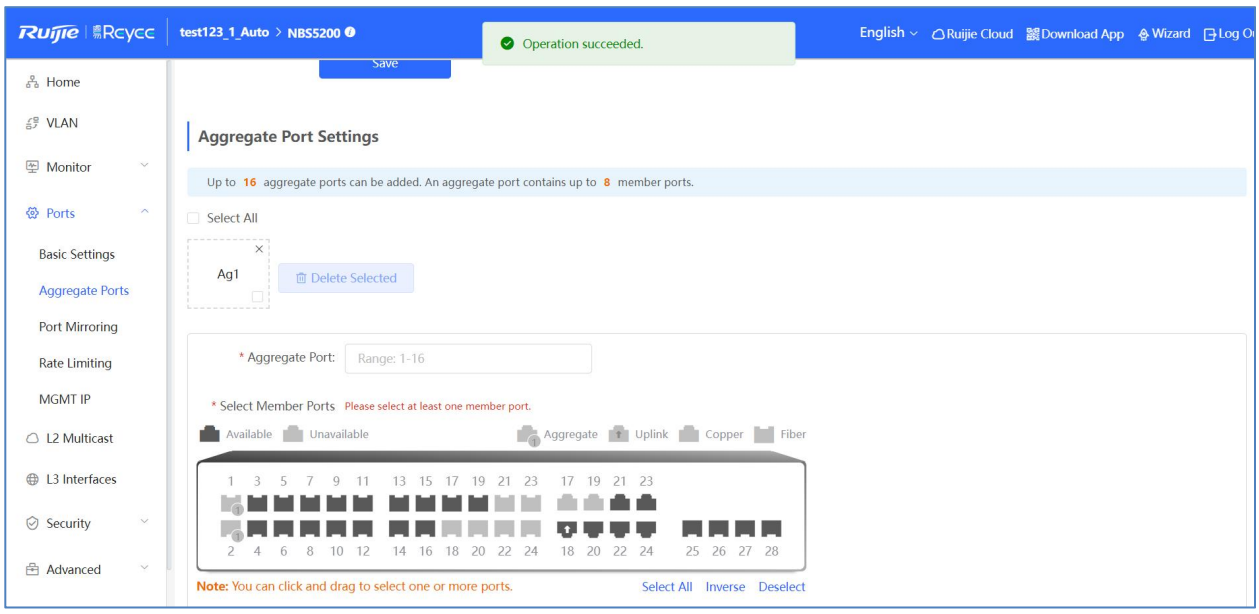
1.2 Aggregate Ports Settings

Adding an aggregate port

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



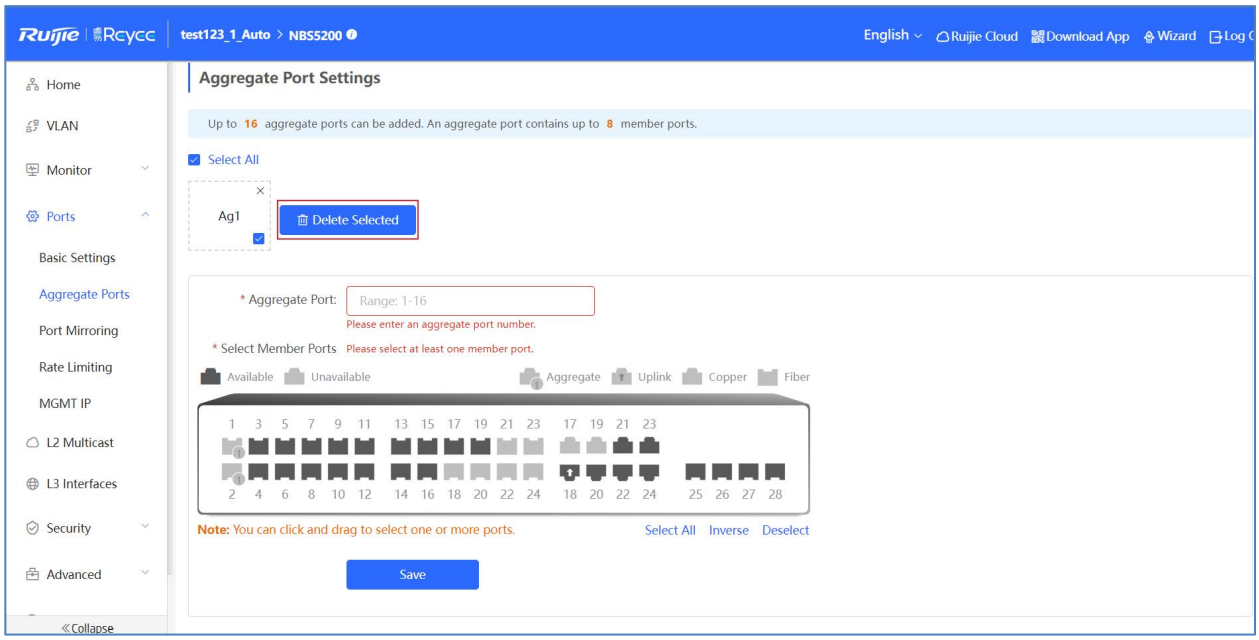
The message "Operation succeeded." is displayed. The port panel displays the added aggregate port.



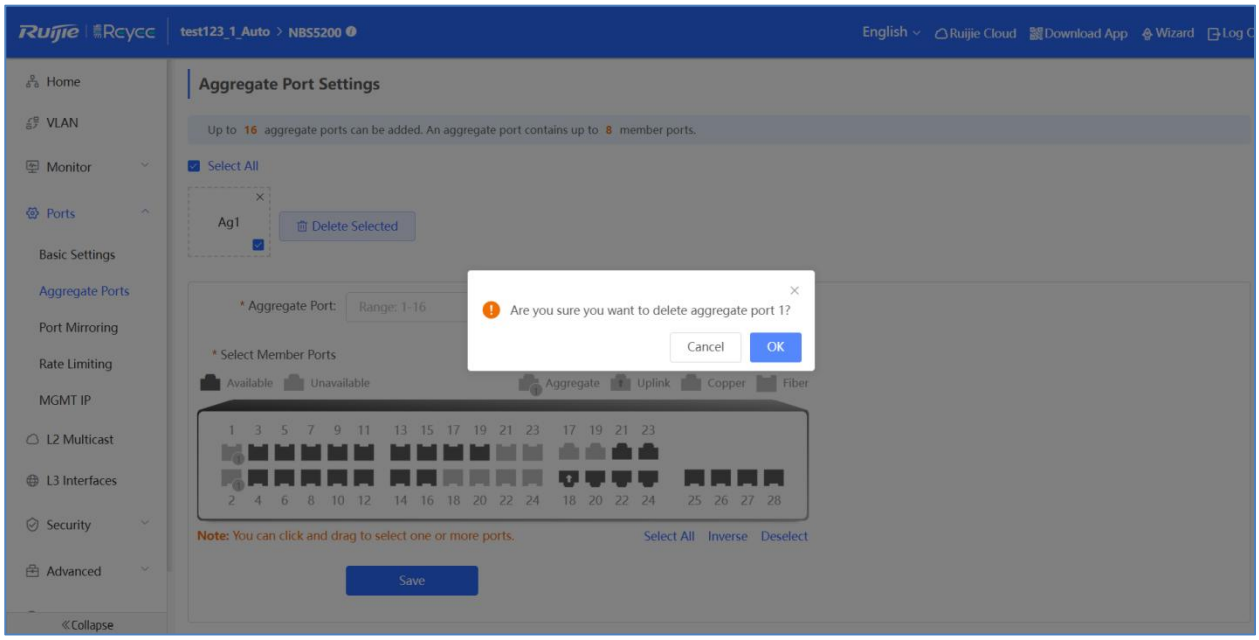
An aggregate port contains a maximum of eight member ports.

Batch deleting aggregate ports/Deleting a single aggregate port

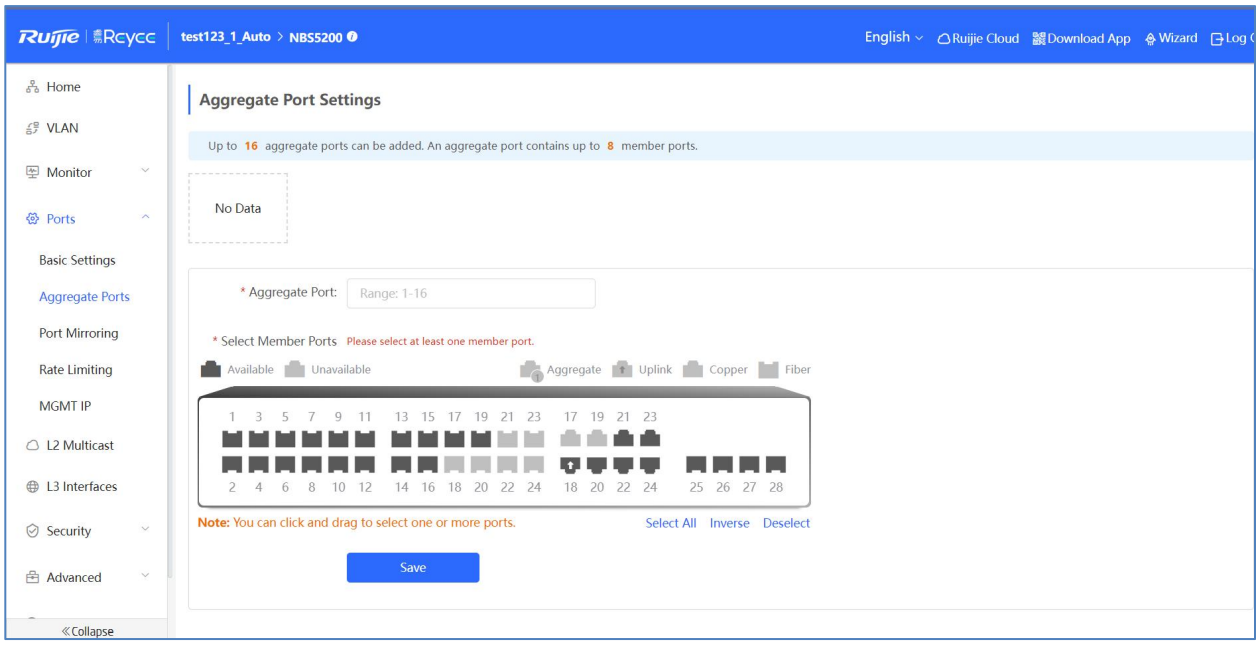
In the aggregate port list, click to select aggregate ports, and click **Delete Selected**.



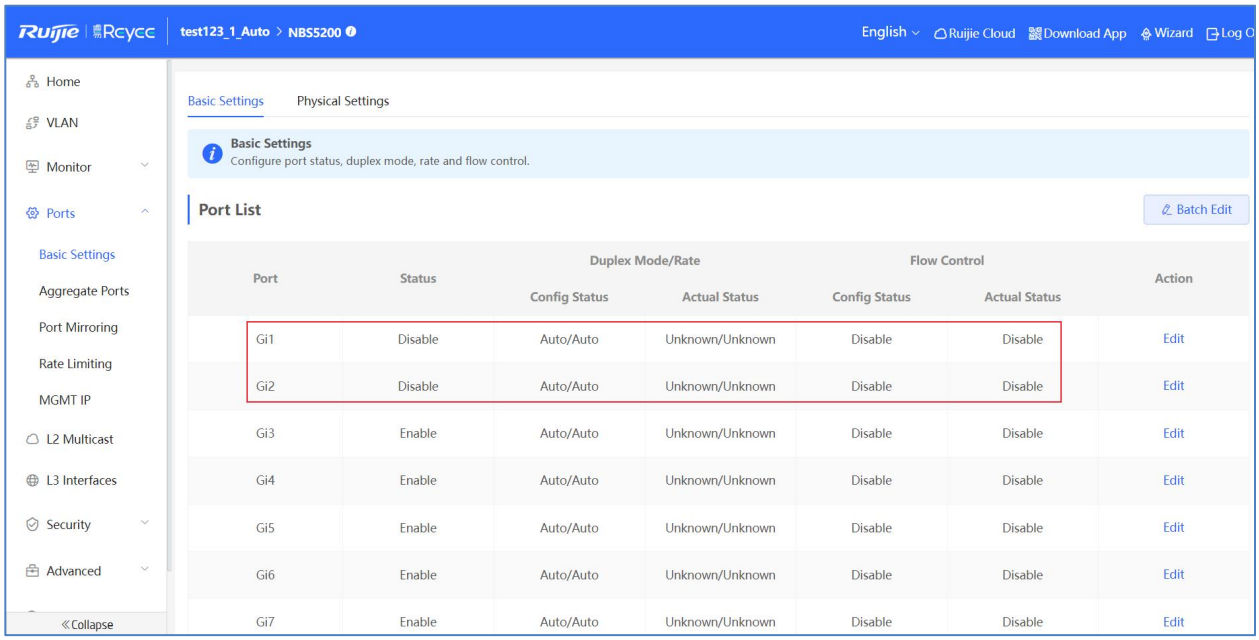
In the displayed confirmation box, click **OK**.



A deleted aggregate port becomes available on the port panel.

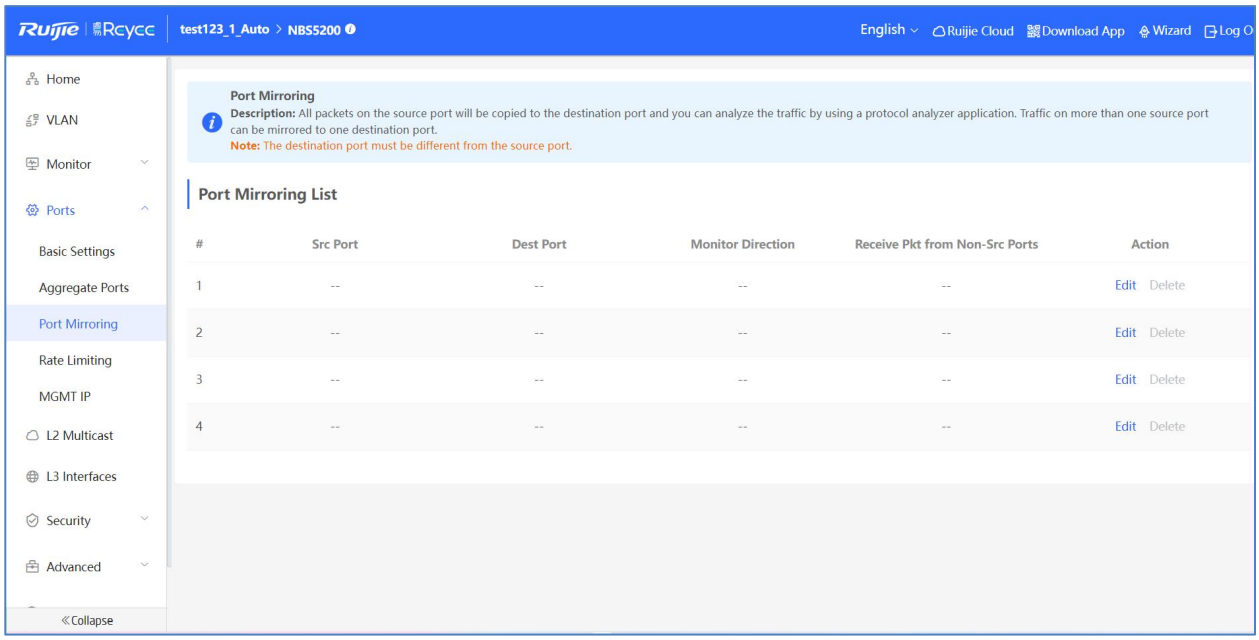


After the aggregate port is **deleted**, its member ports are restored to the **default settings** and are **disabled.**



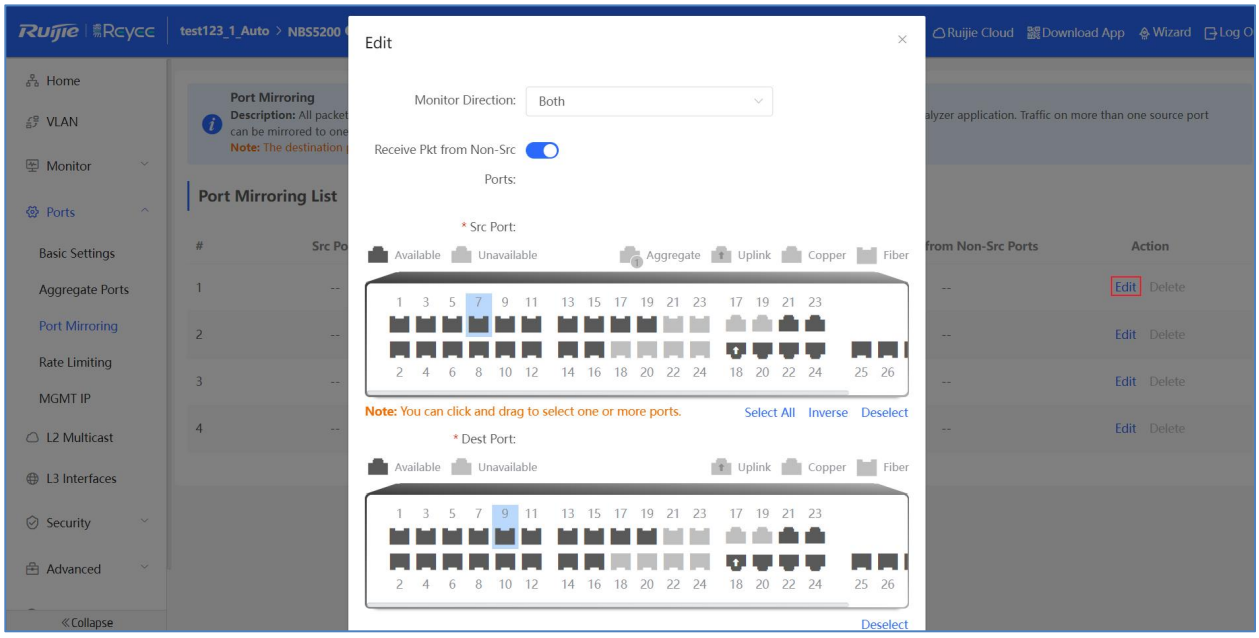
4.3.2.3 Port Mirroring

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

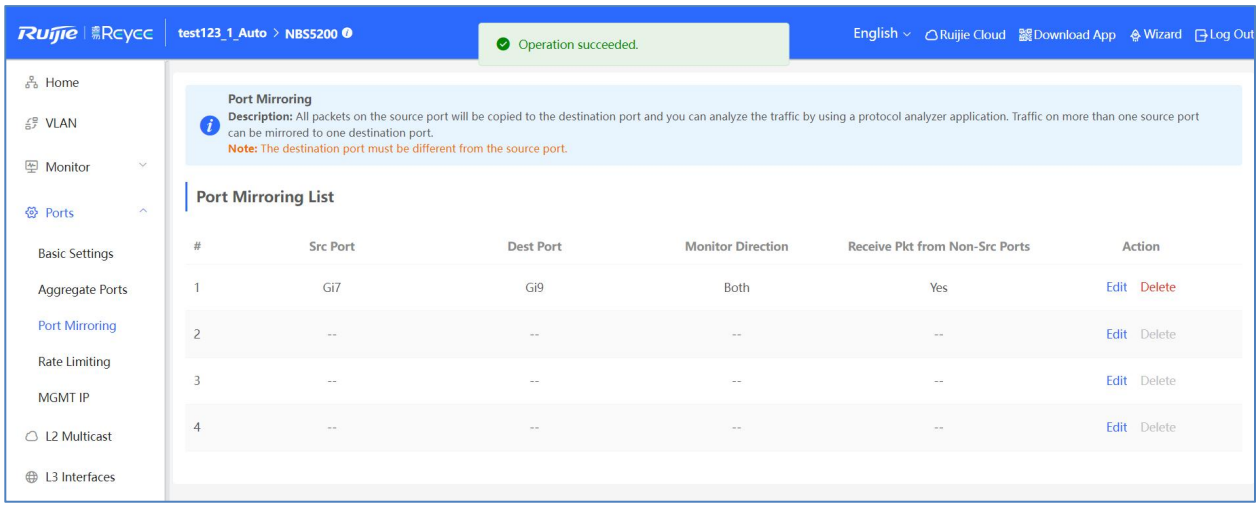


Editing a port mirroring entry

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



The message "Operation succeeded." is displayed.

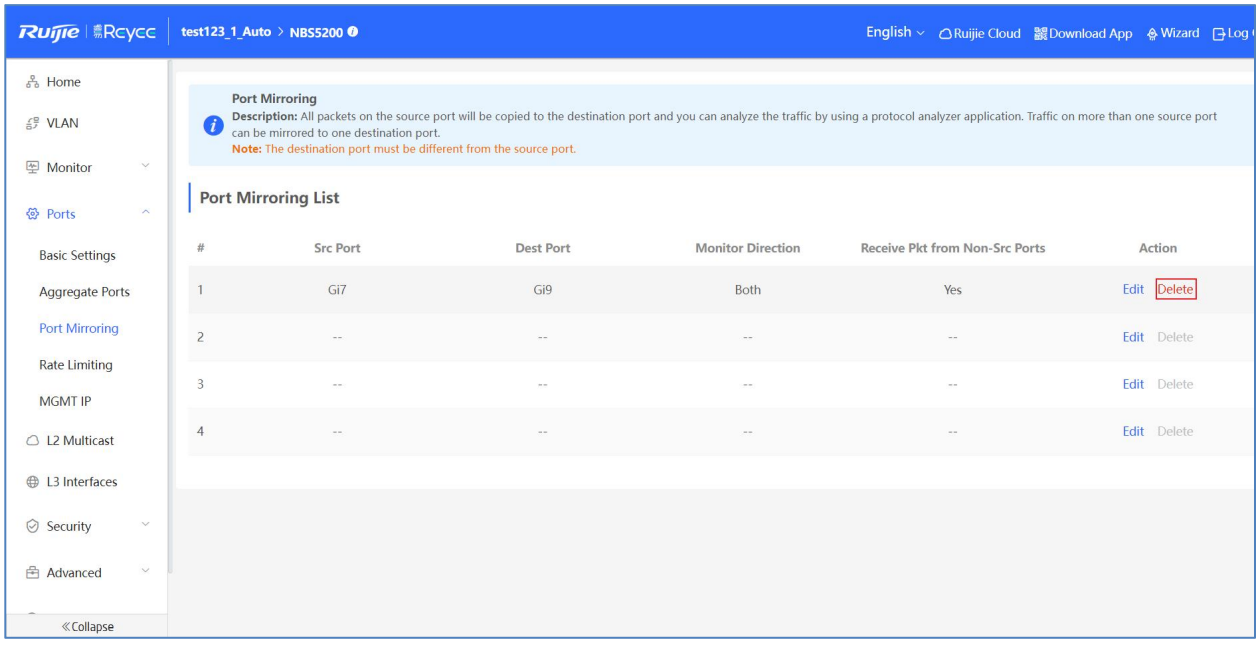


You can select **multiple source ports** but only **one destination port** for port mirroring. Moreover, the source ports cannot contain the destination port and an **aggregate port** cannot be used as the destination port.

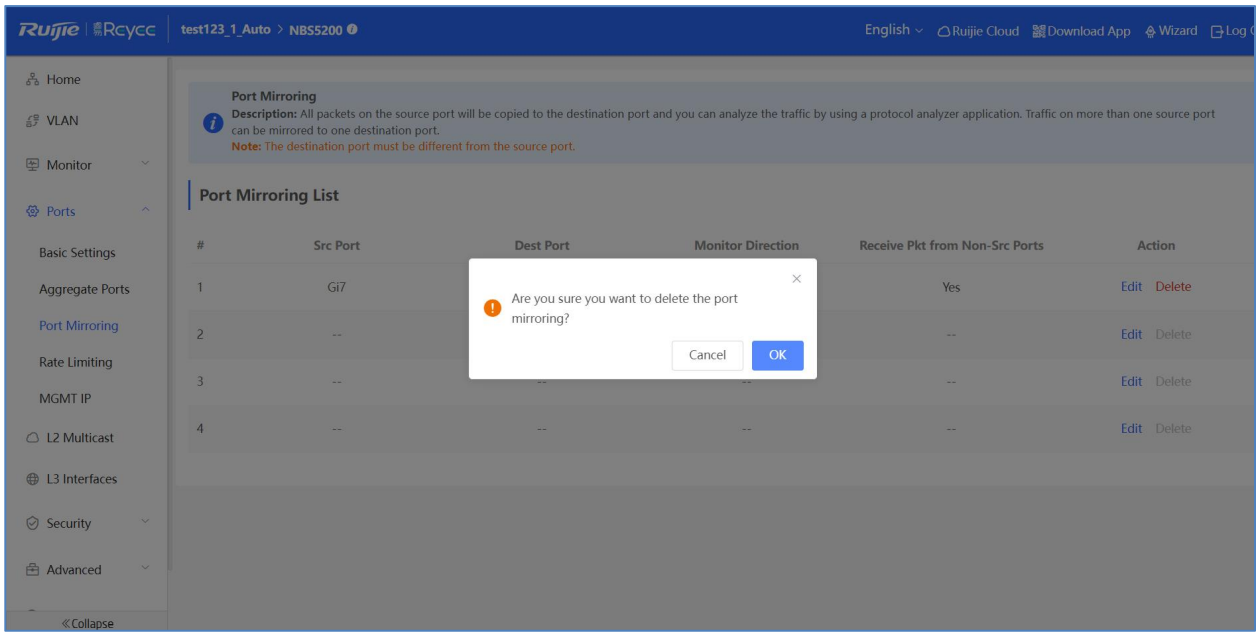
A maximum of four port mirroring entries can be configured. Port mirroring cannot be configured for ports that are already mirrored.

Deleting a port mirroring entry

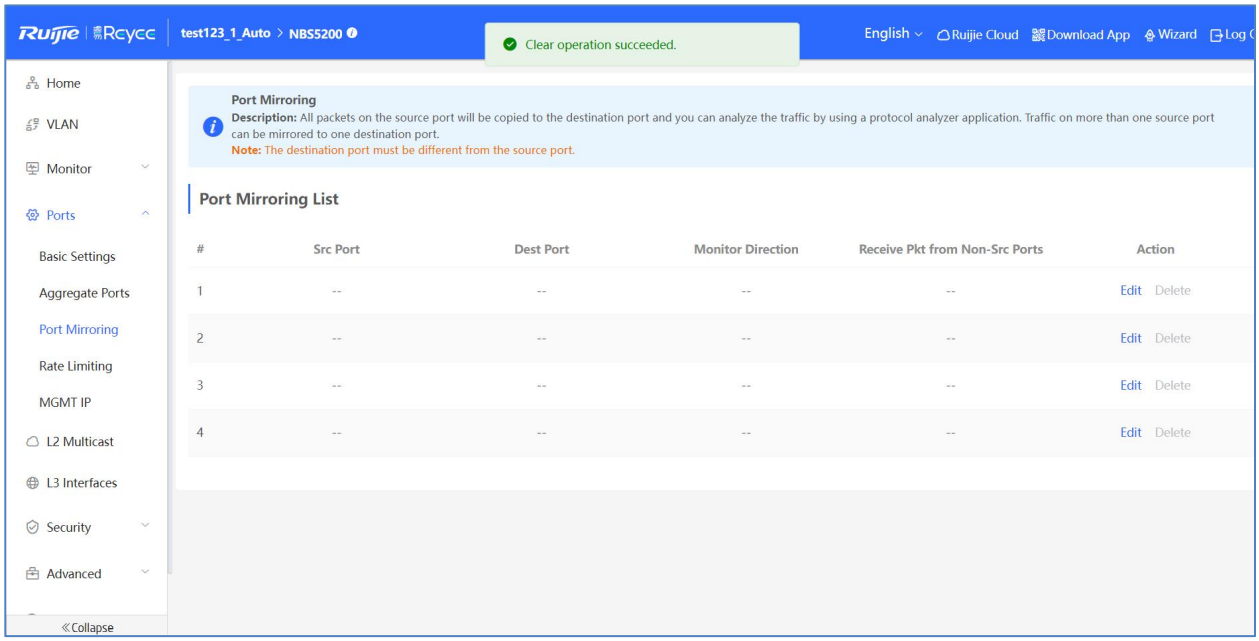
Click **Delete** in the **Action** column. In the displayed confirmation box, click **OK.**



In the displayed confirmation box, click **OK.**

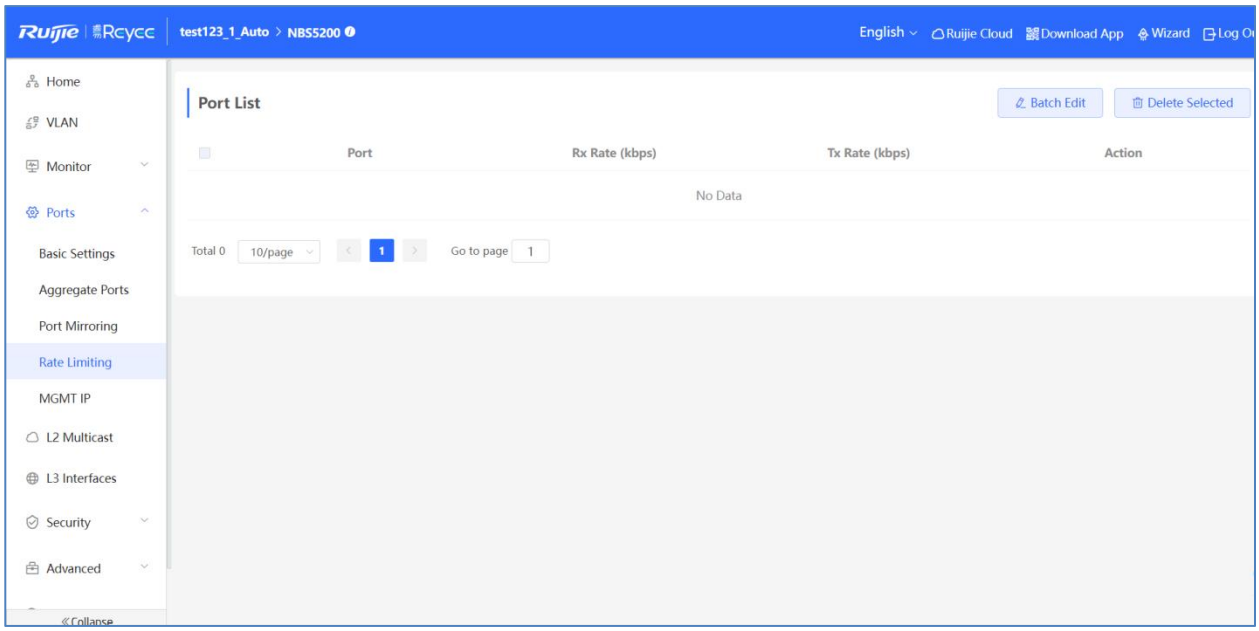


The message "Clear operation succeeded." is displayed.



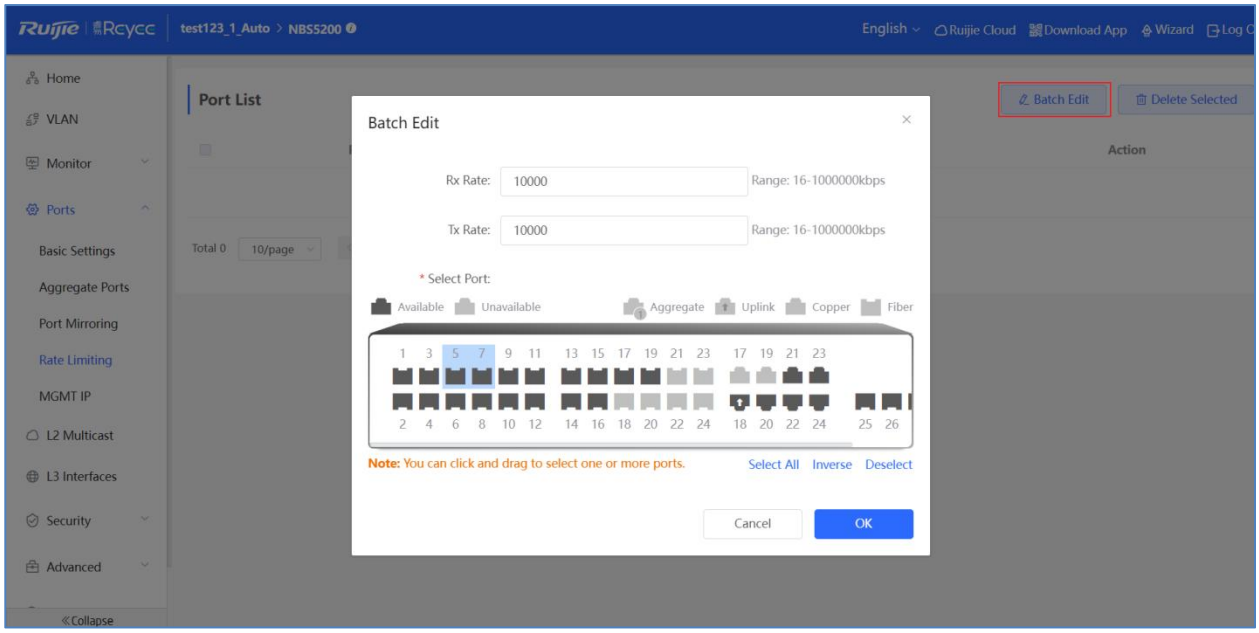
4.3.2.4 Rate Limiting

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

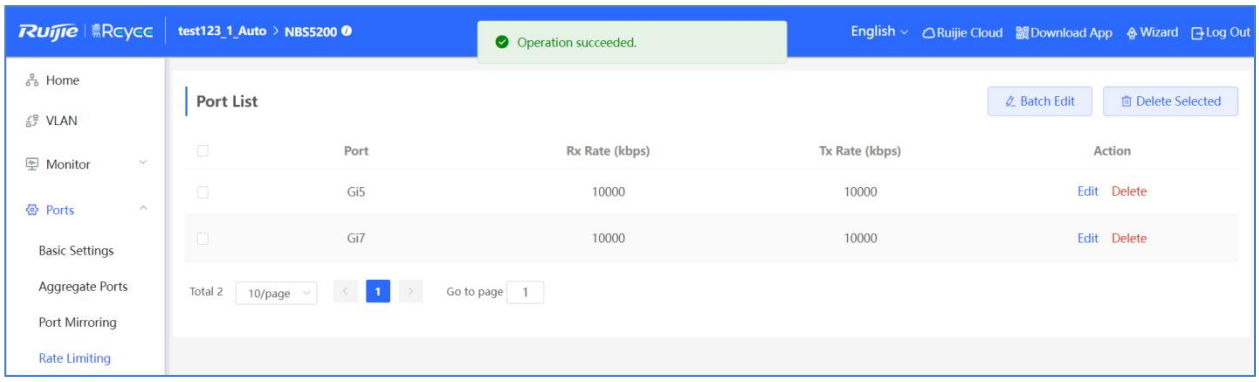


Batch editing the rate limit of ports/Editing the rate limit of a single port

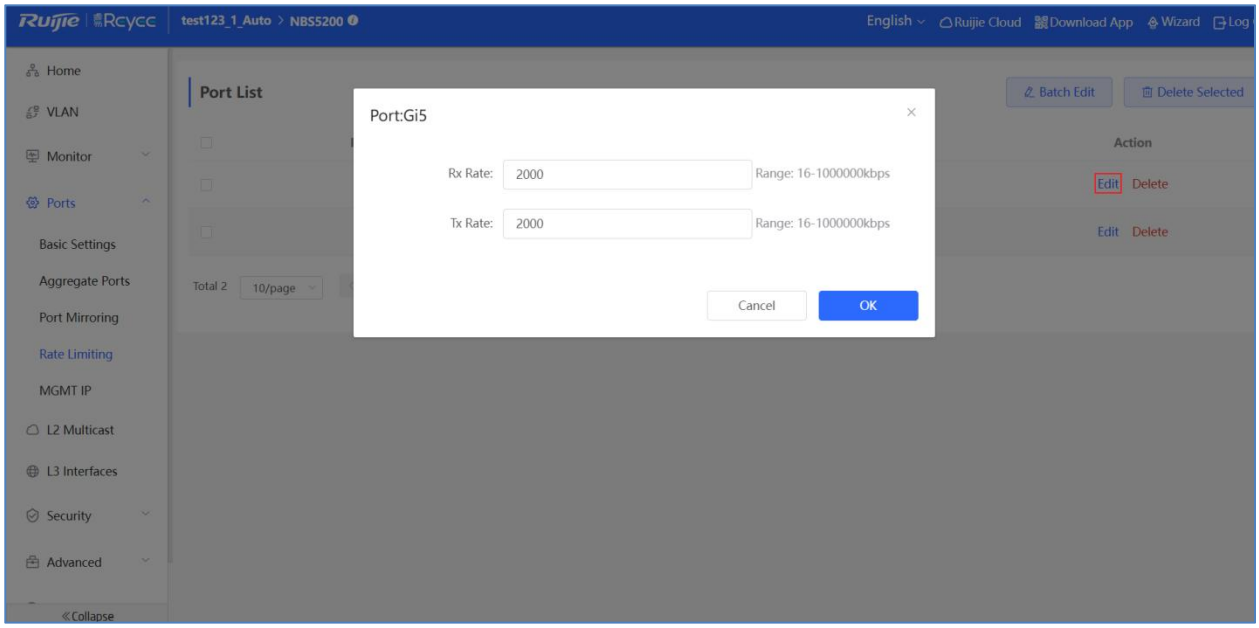
Click **Batch Edit.** In the displayed dialog box, select ports, set the Rx speed or the Tx speed, and click **OK.**



The message "Operation succeeded." is displayed, and the port list is updated.

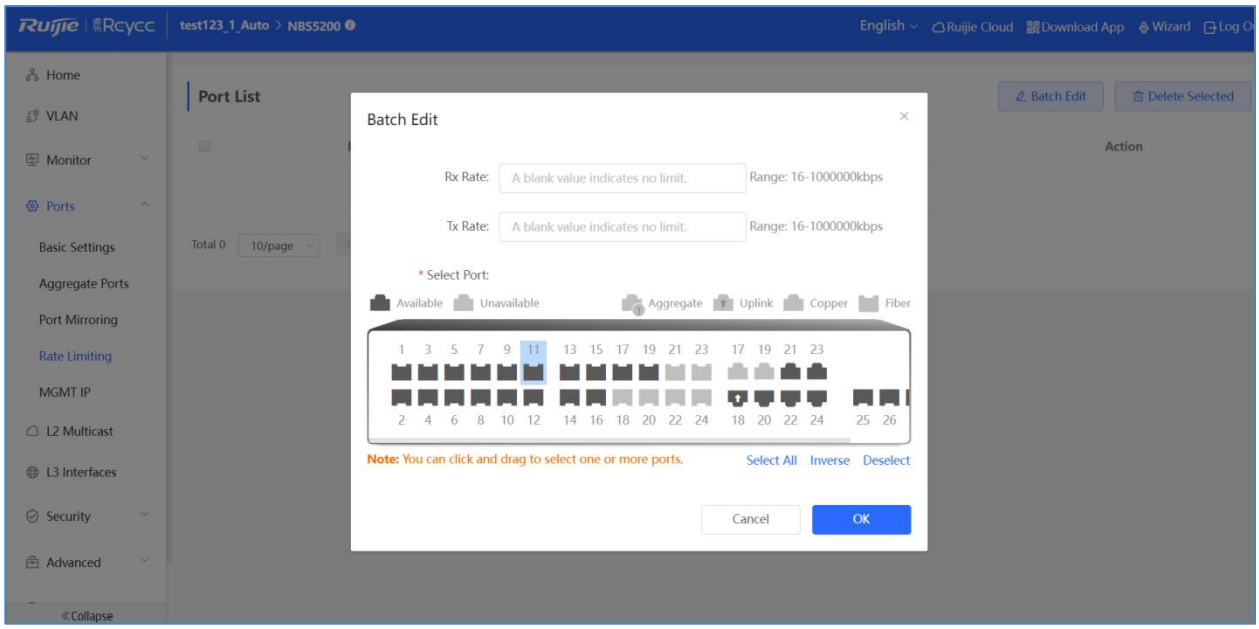


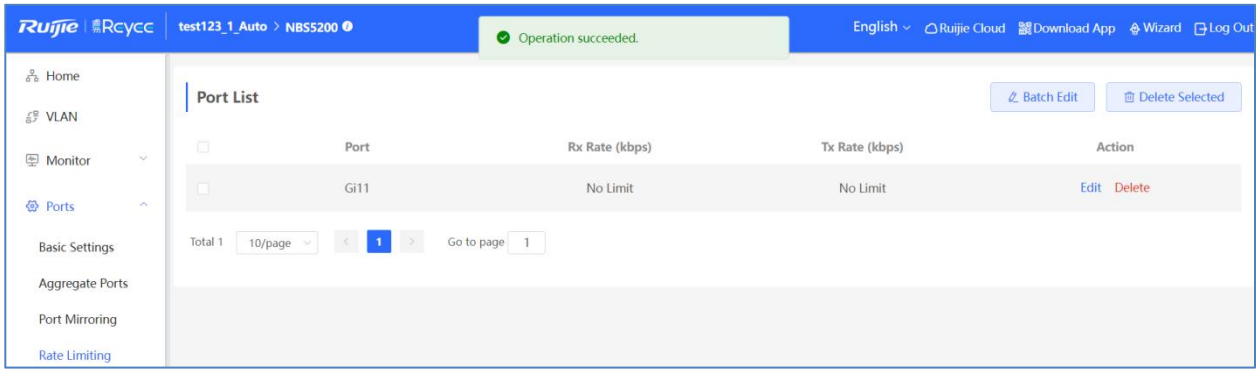
Click **Edit** in the **Action** column. In the displayed dialog box, set the Rx speed or the Tx speed, and click **OK.**



The message "Operation succeeded." is displayed, and the port list is updated.

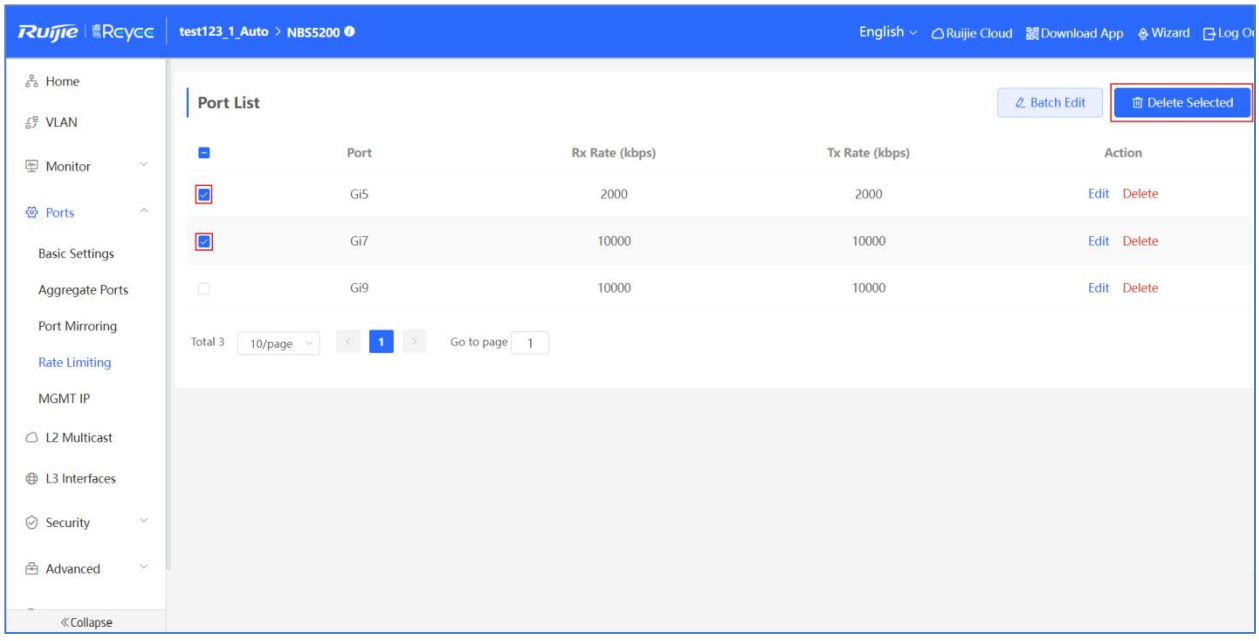
You must set the Rx speed or the Tx speed. If the Rx speed and the Tx speed are not set, the port rate is not limited.



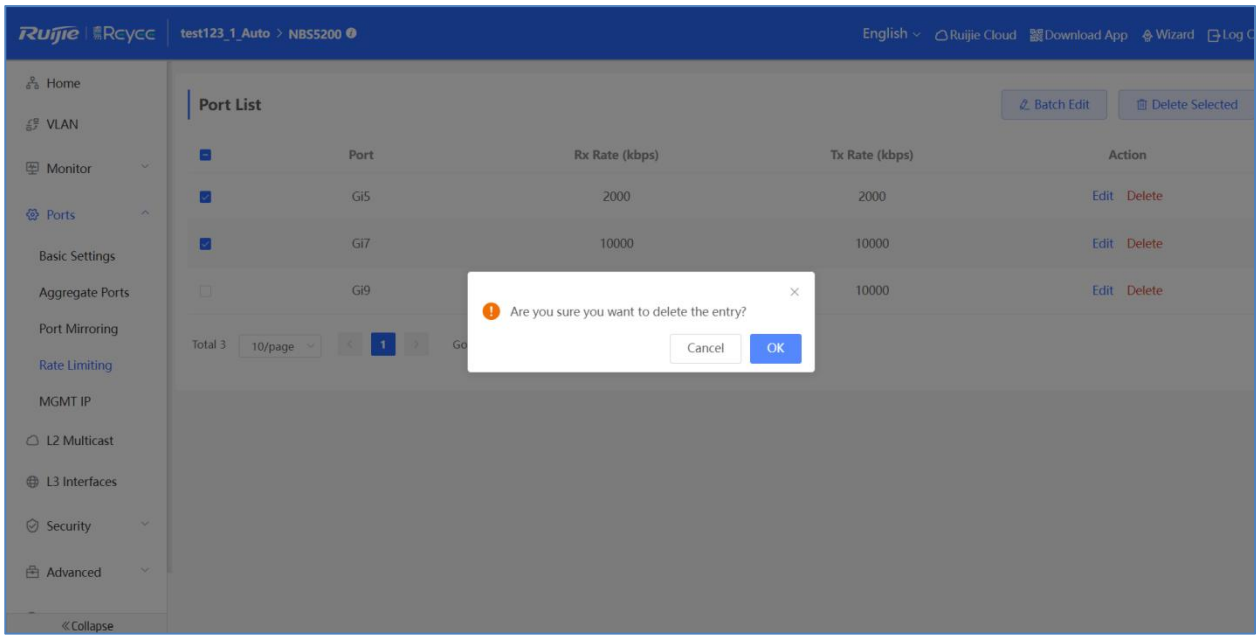


Batch deleting the rate limit of ports/Deleting the rate limit of a single port

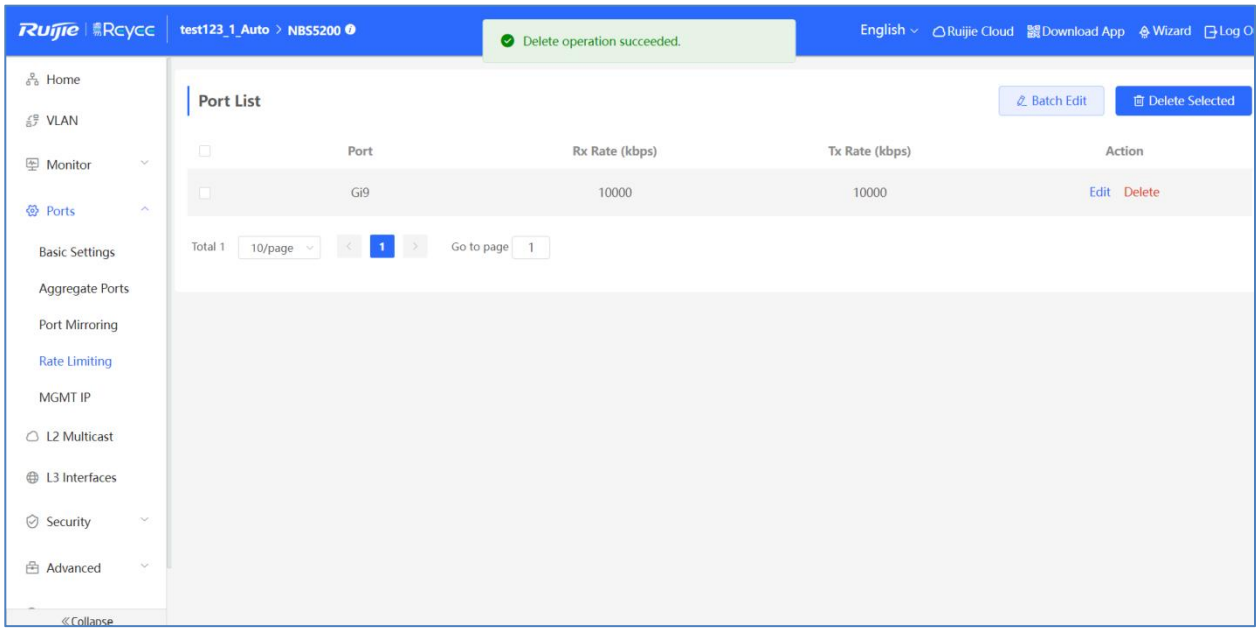
Select multiple entries in **Port List** and click **Delete Selected.**



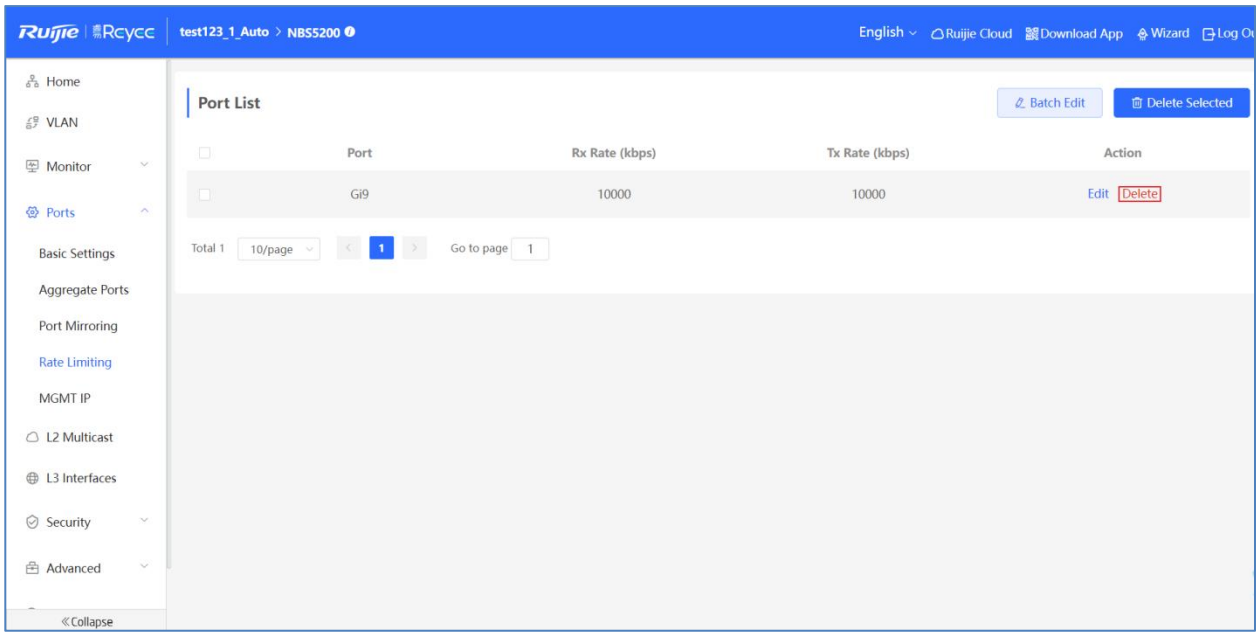
In the displayed confirmation box, click **OK.**



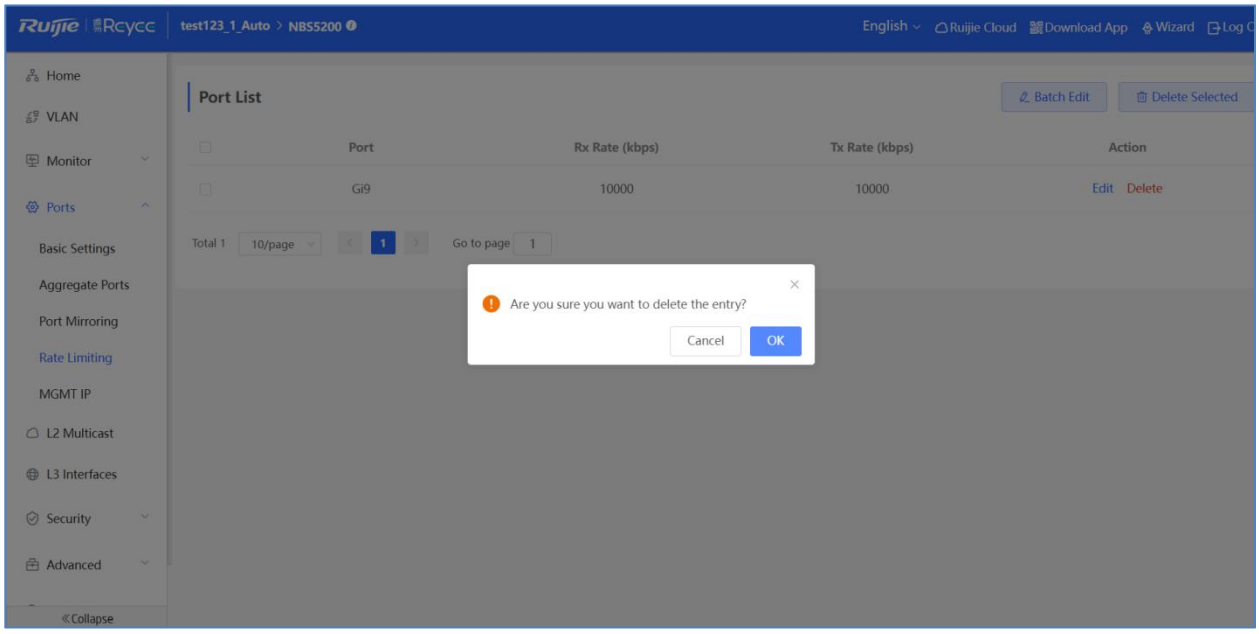
The message "Delete operation succeeded." is displayed, and the port list is updated.



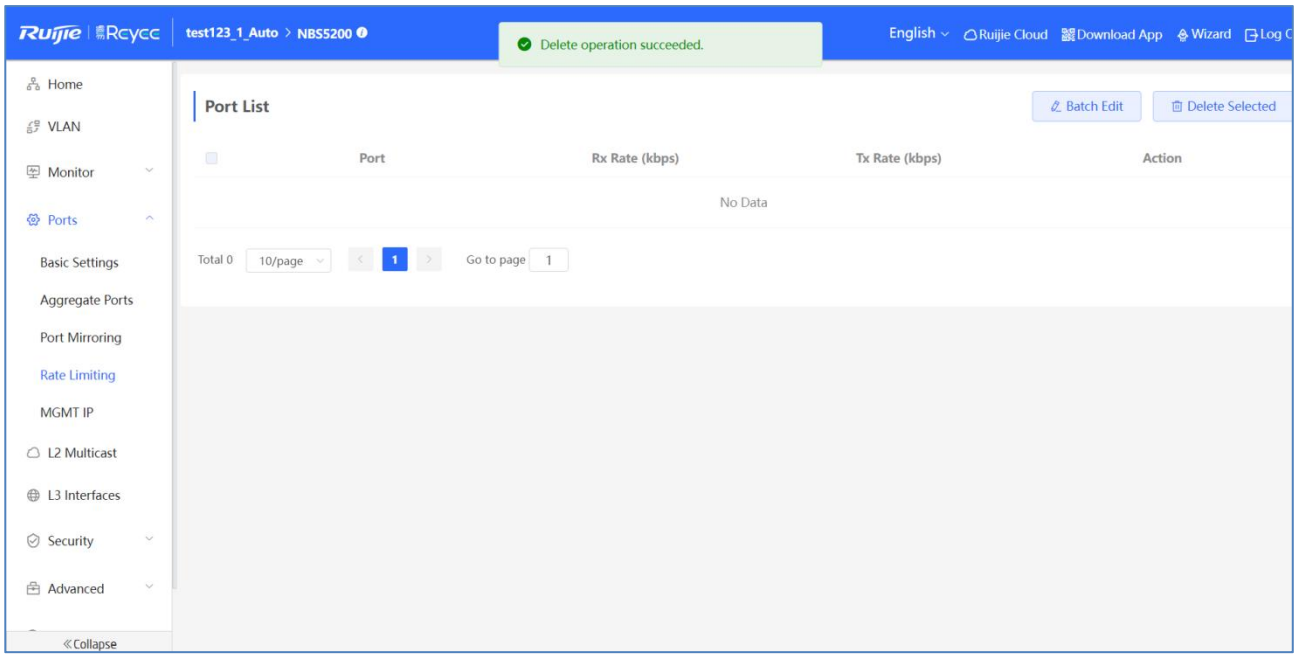
Click **Delete** in the **Action** column.



In the displayed confirmation box, click **OK.**

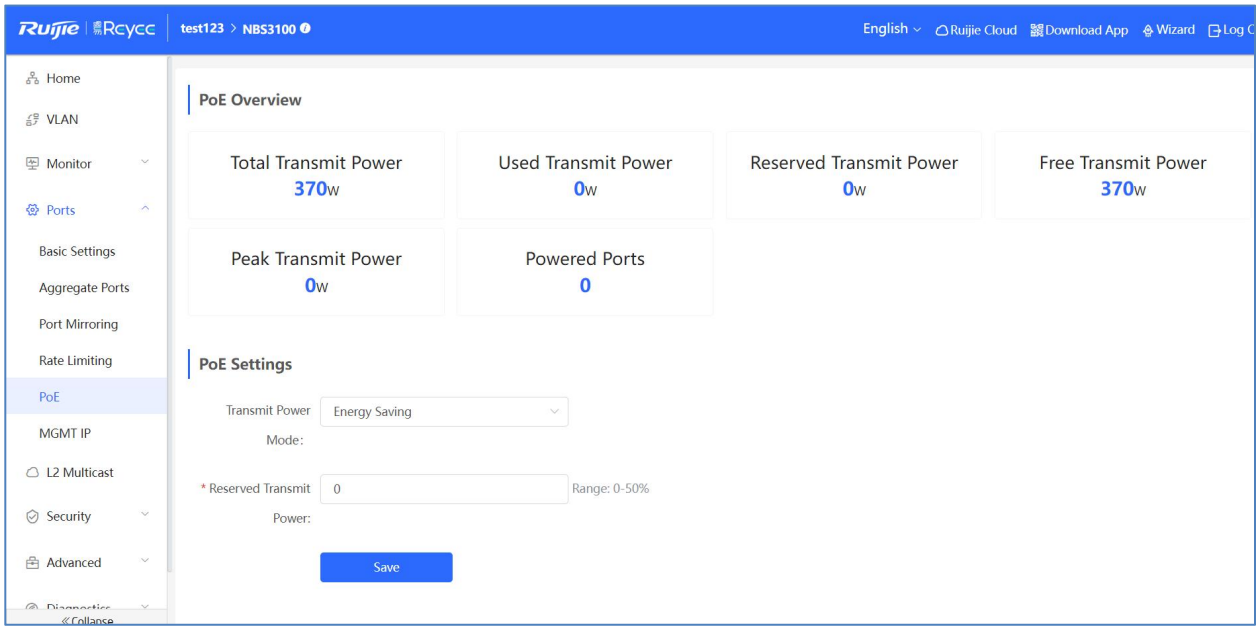


The message "Delete operation succeeded." is displayed, and the port list is updated.



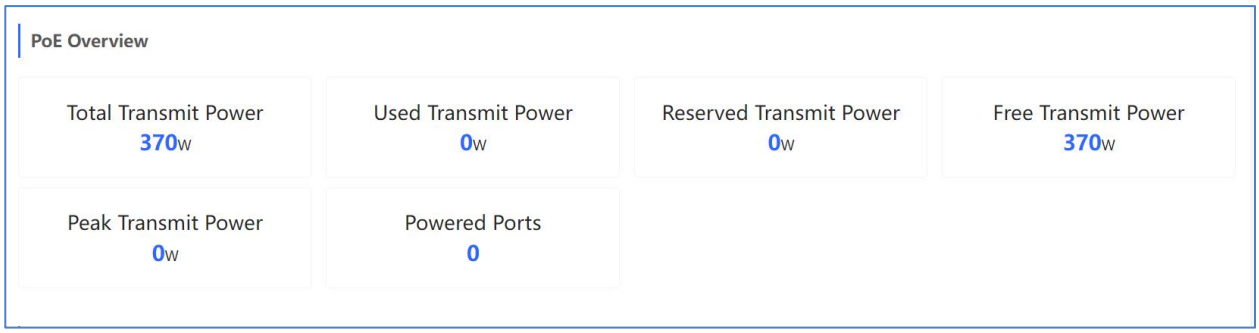
4.3.2.5 PoE

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



1. 1 PoE Overview

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

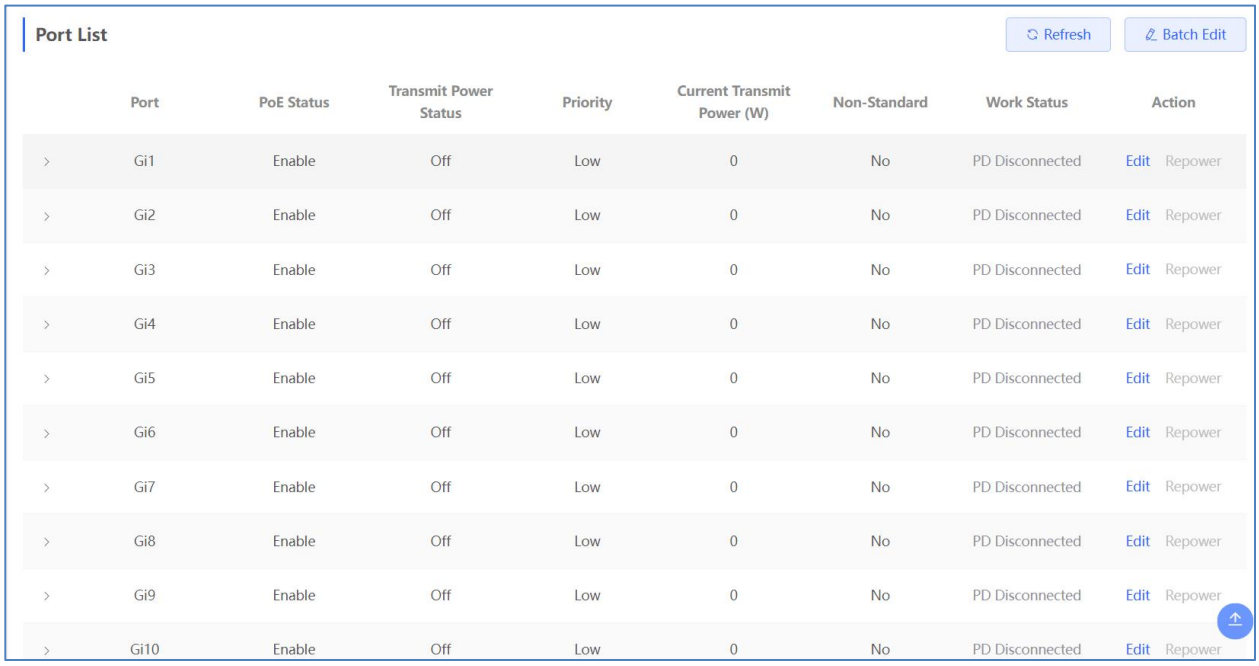


1.2 PoE settings

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

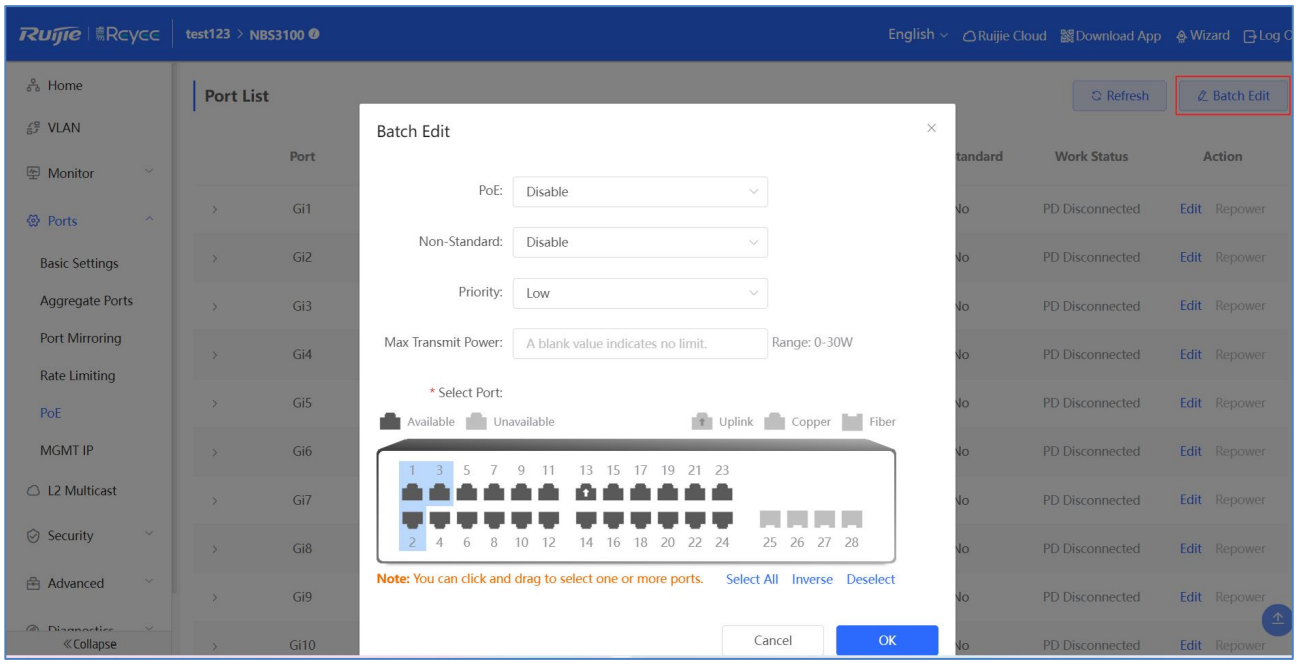
1.3 Port List

Port List displays the details of the POE ports.

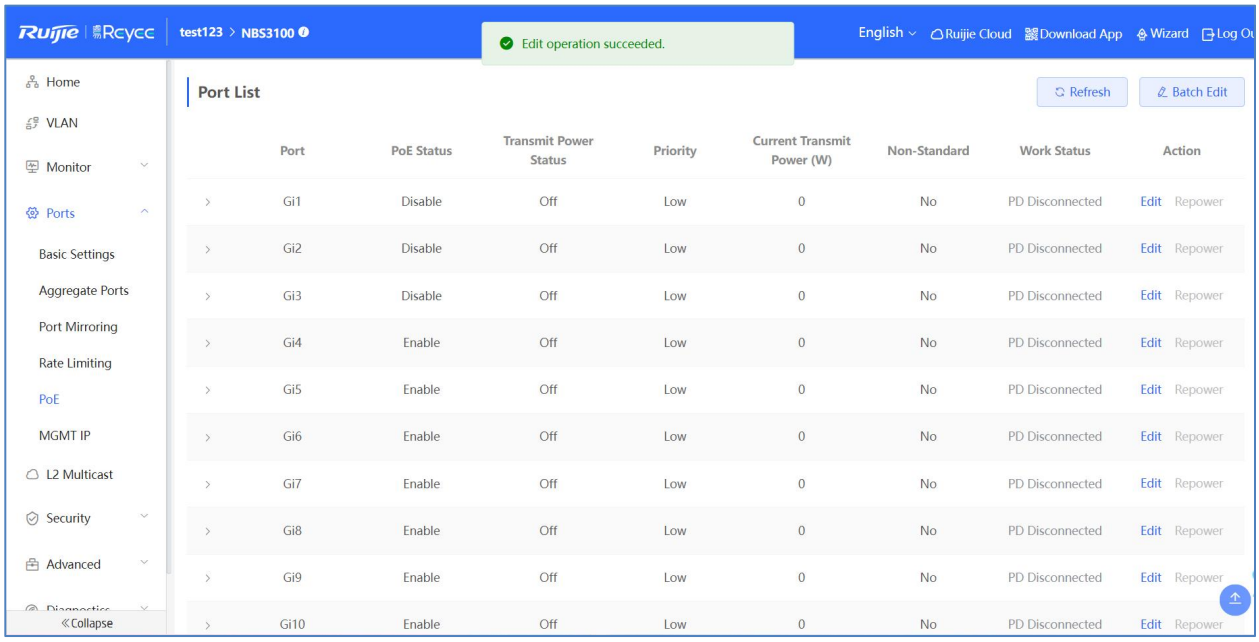


Batch editing PoE ports/Editing a single PoE port

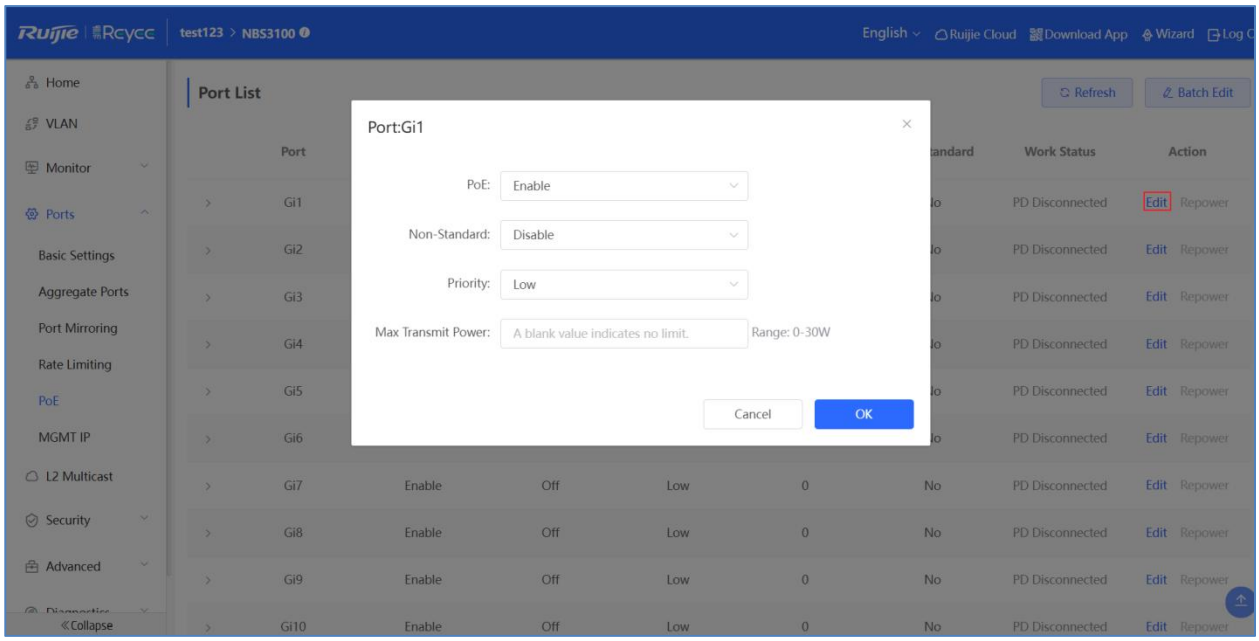
Click **Batch Edit** in **Port List.** In the displayed dialog box, set the PoE port attributes, and click **OK.**



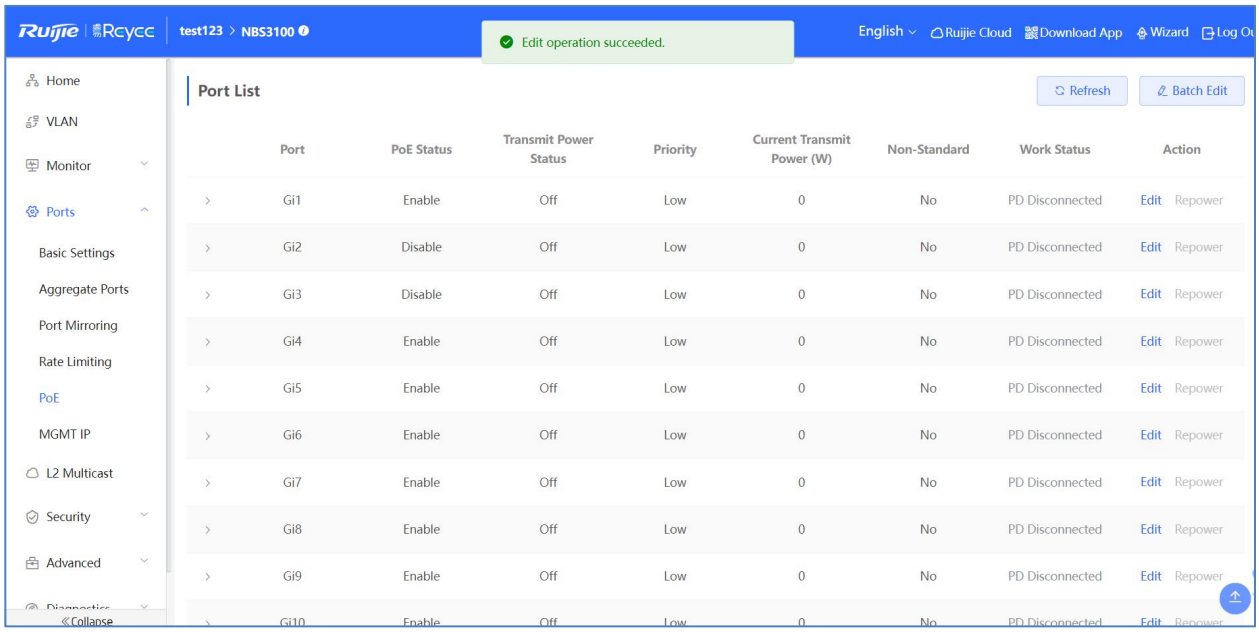
The message "Edit operation succeeded." is displayed, and the port list is updated.



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

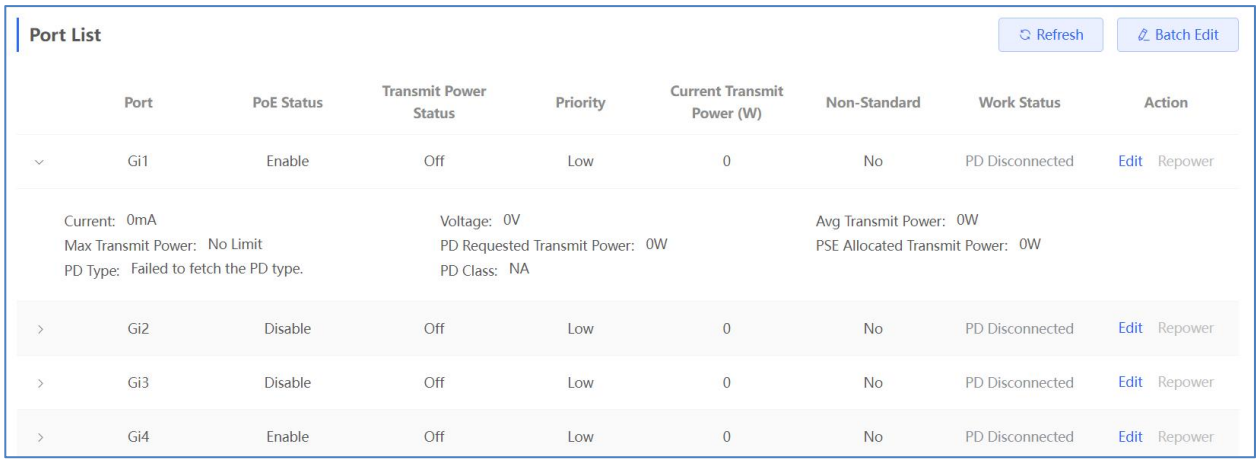


The message "Edit operation succeeded." is displayed, and the port list is updated.



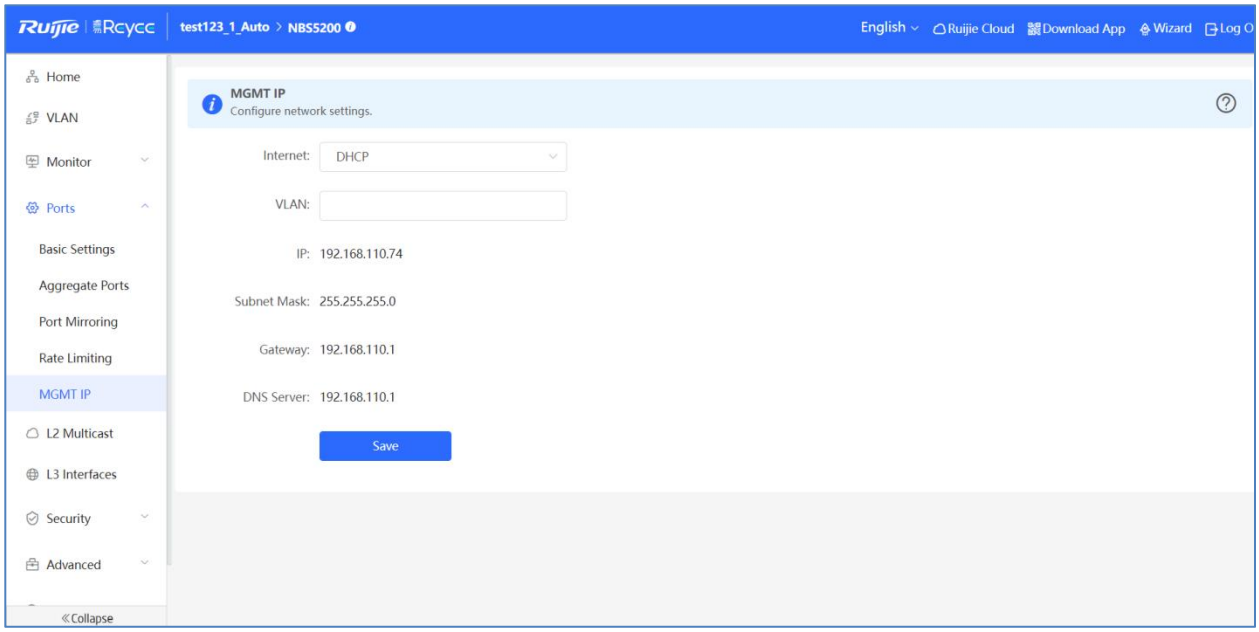
Displaying PoE port details

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



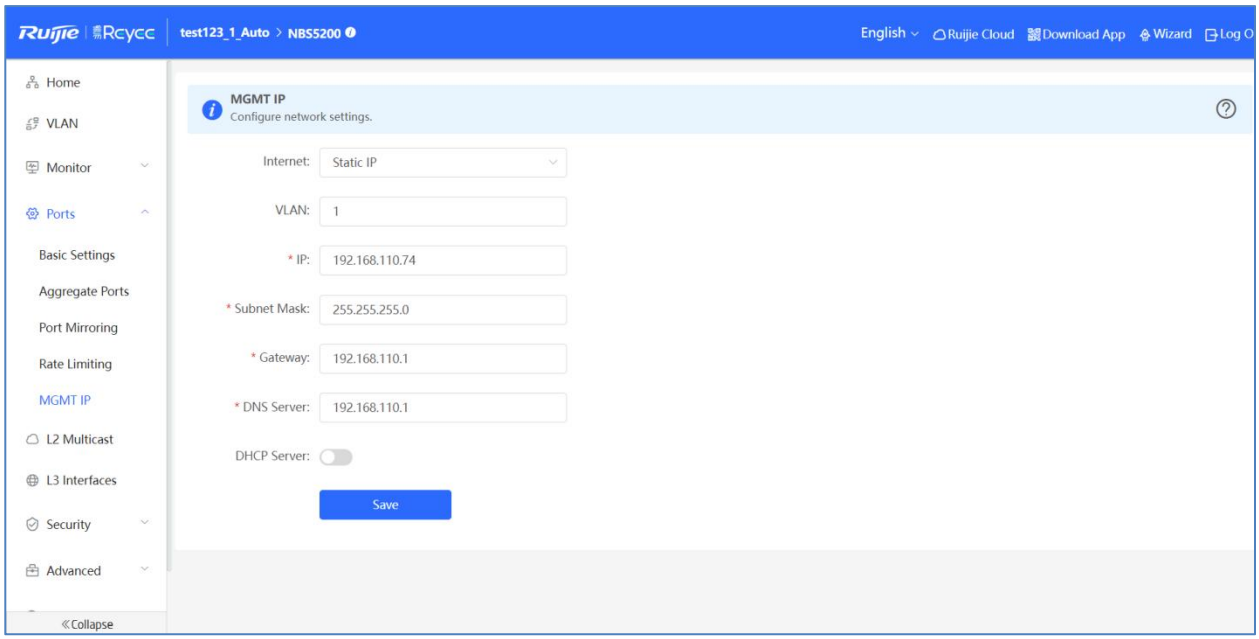
4.3.2.6 MGMT IP

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



Configuring a Static IP address

Configure the management VLAN, IP address, subnet mask, default gateway, and DNS server, and click **Save.**



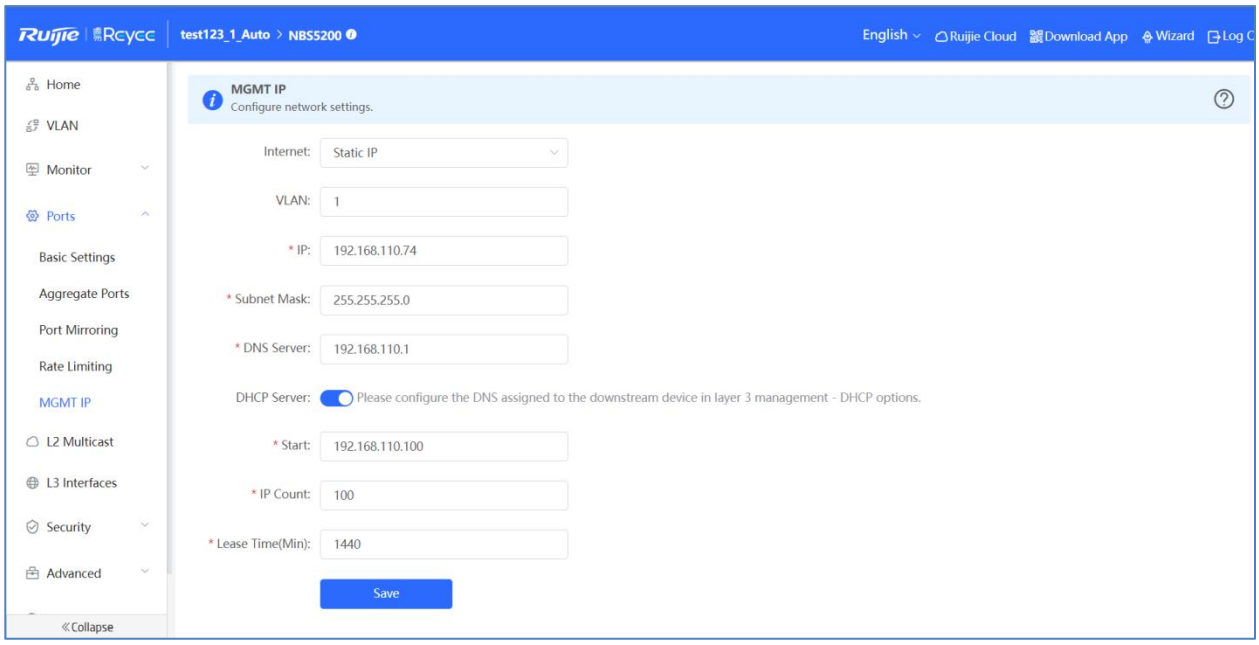
VLAN 1 takes effect when the management VLAN is set to **null or empty**.

The **management VLAN** must be created before the configuration. To create a management VLAN, follow the instructions in VLAN List.

You are advised to bind a configured management VLAN to an uplink port. Otherwise, you may fail to access the eWeb management system.

Management IP Address Supporting DHCP Server

Please select static IP from the Internet dropdown list before enabling DHCP Server. Configure the start IP address, IP count and lease time, and click **Save.**

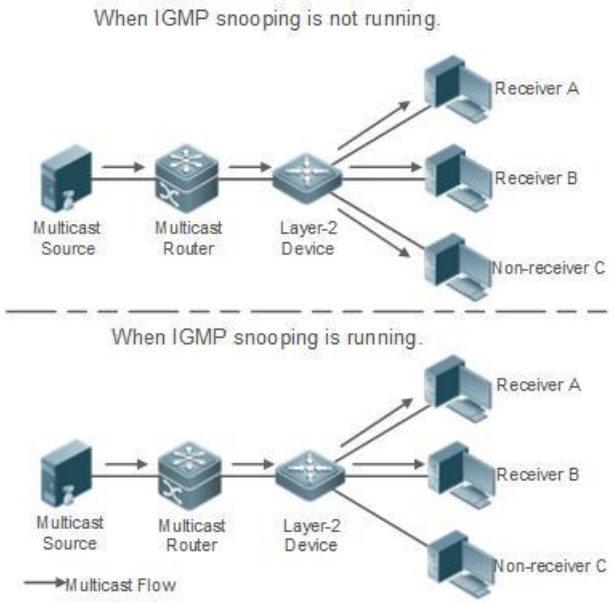


4.3.3 L2 Multicast

The NBS series switches support two types of multicast features, IGMP Snooping and Multicast VLAN Registration (MVR).

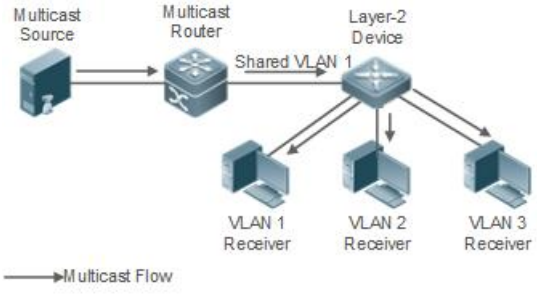
IGMP Snooping

Multicast packets are transmitted to users through a Layer-2 switch. When Layer-2 multicast control is not performed, namely, when IGMP snooping is not implemented, multicast packets are flooded to all the users including those who are not expected to receive these packets. After IGMP snooping is implemented, the multicast packets from an IP multicast profile will no longer be broadcasted within the VLAN but transmitted to designated receivers.

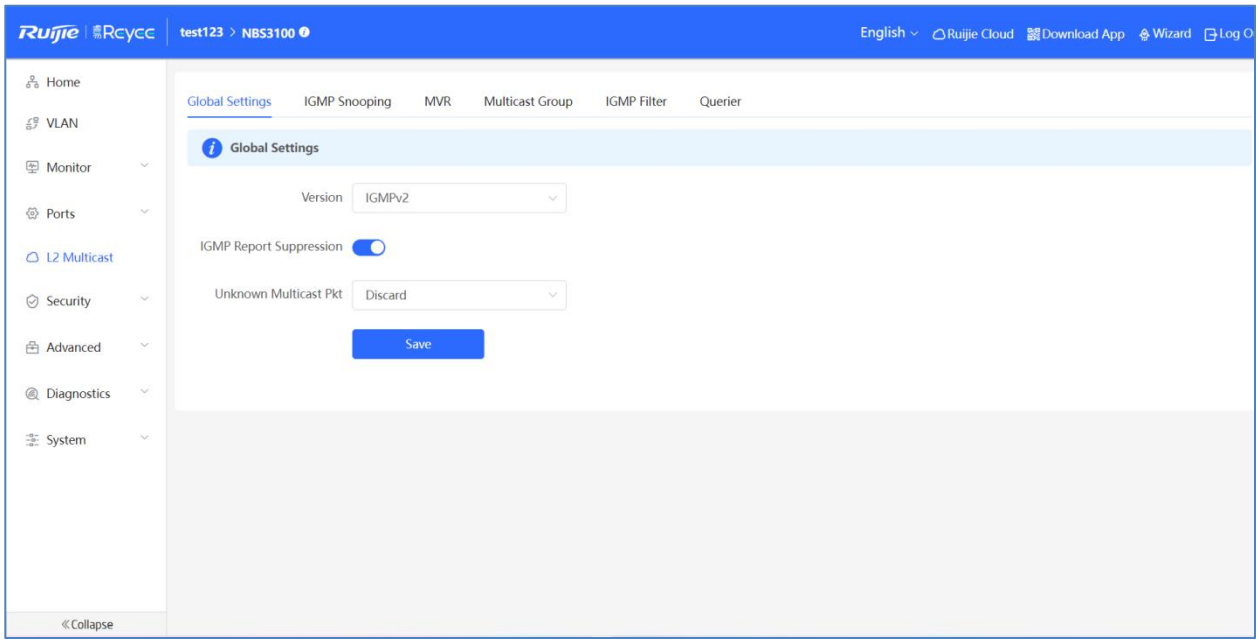


MVR

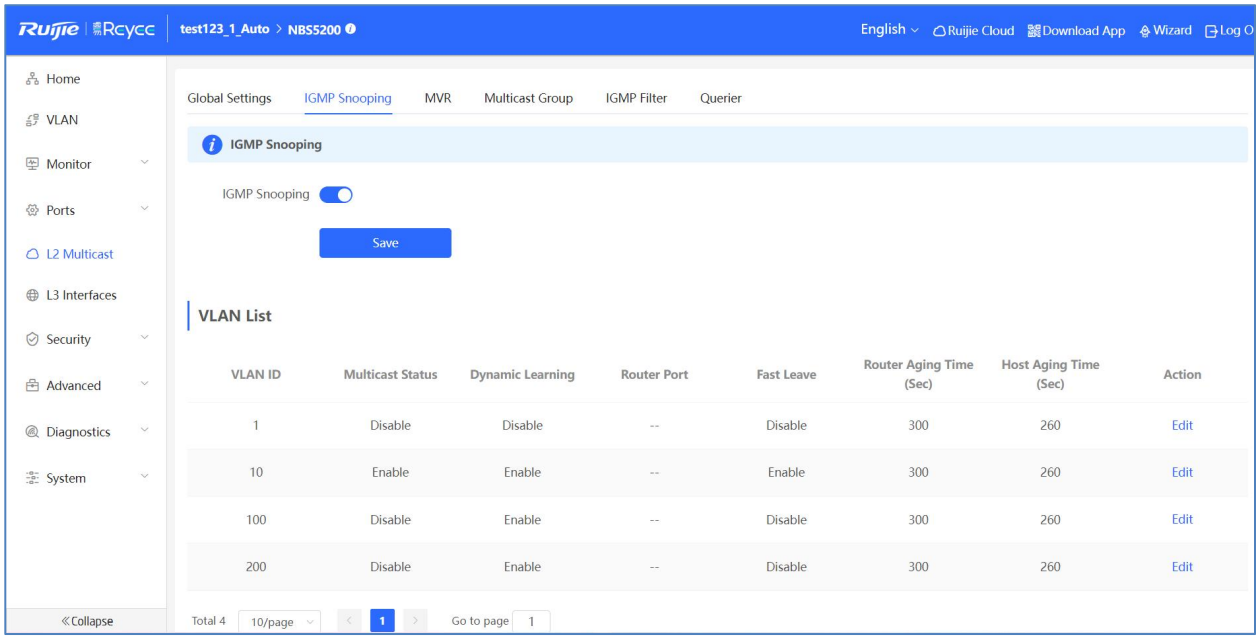
The multicast router sends a multicast packet to VLAN 1, and the Layer-2 multicast device automatically transfers the packet to VLAN 1, VLAN 2, and VLAN 3. In this way, the multicast services of VLAN 1 are shared by VLAN 2 and VLAN 3.



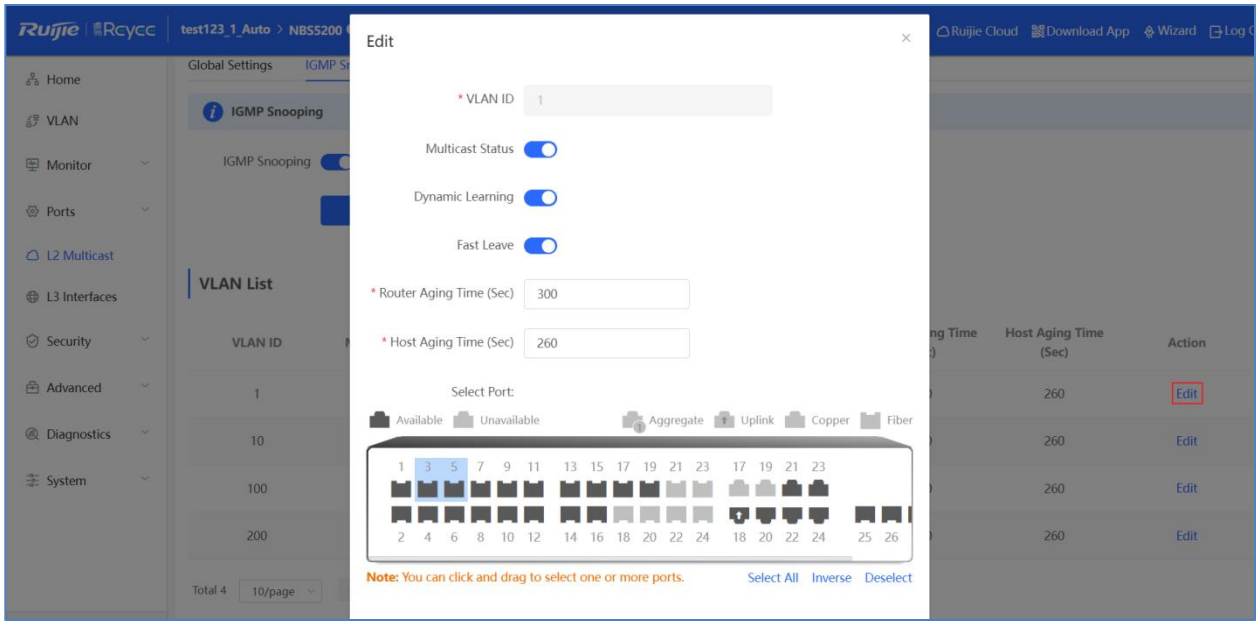
4.3.3.1 Global Settings



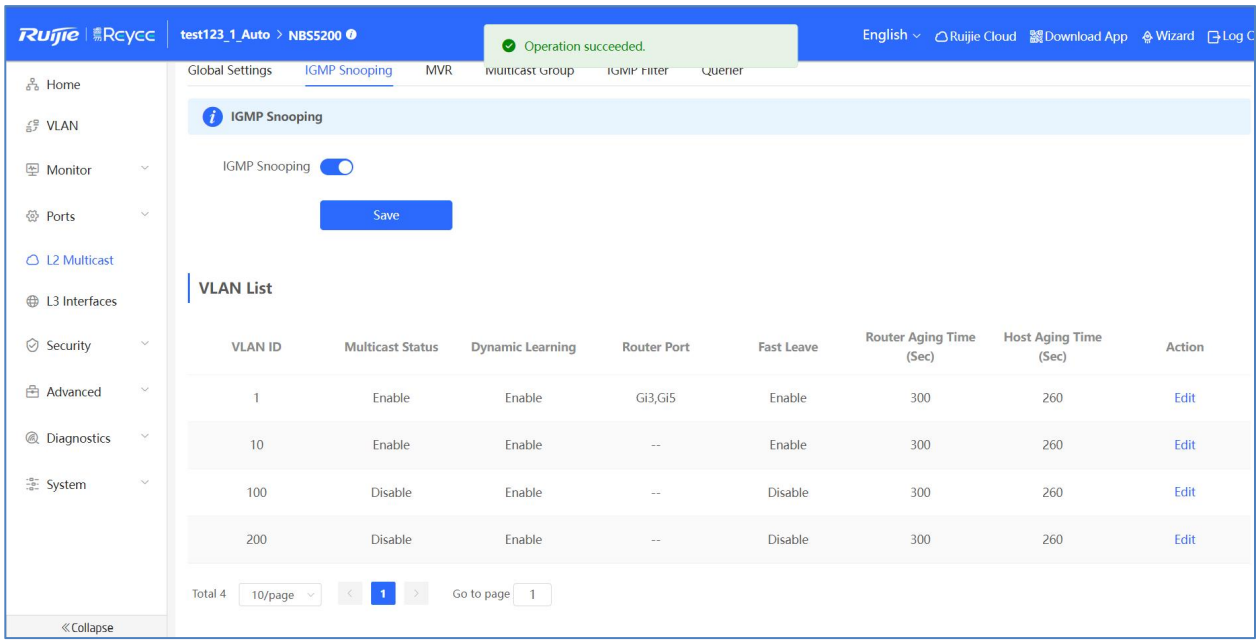
4.3.3.2 IGMP Snooping



Click **Edit** in the **Action** column. In the displayed dialog box, you can set multicast, dynamic learning, fast leave, router aging time, host aging time and select ports.



The message "Operation succeeded." is displayed, and the VLAN list is updated.



4.3.3.3 MVR

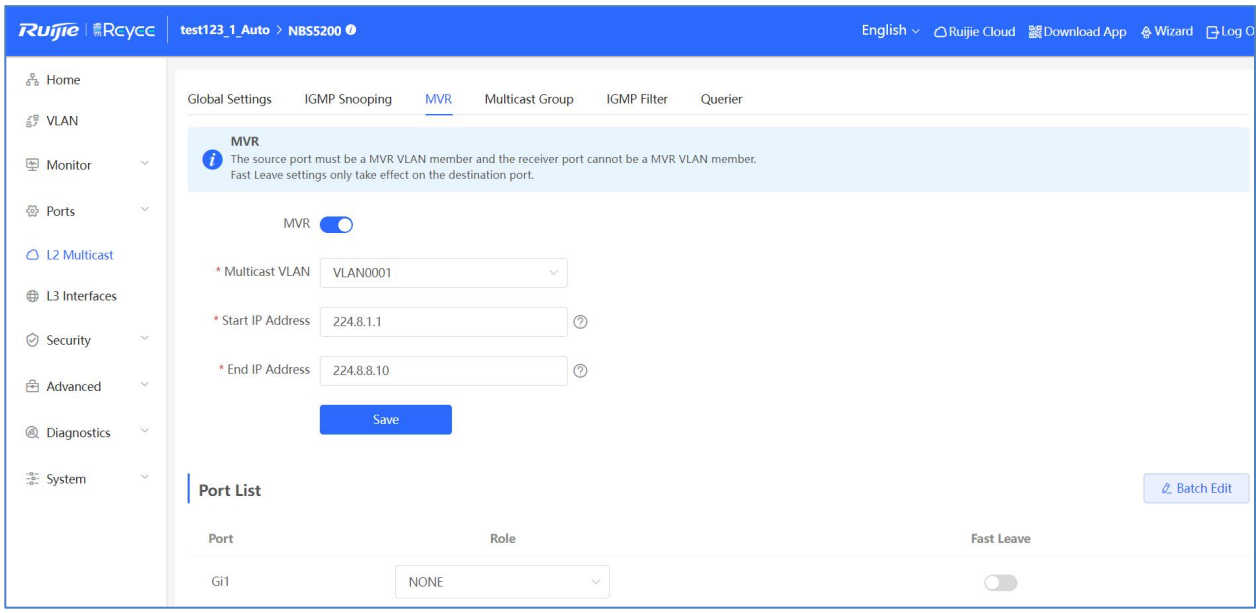
There are two types of MVR ports: source port and receiver port.

Source Port: The source port is the port to which the multicast traffic flows using the multicast VLAN.

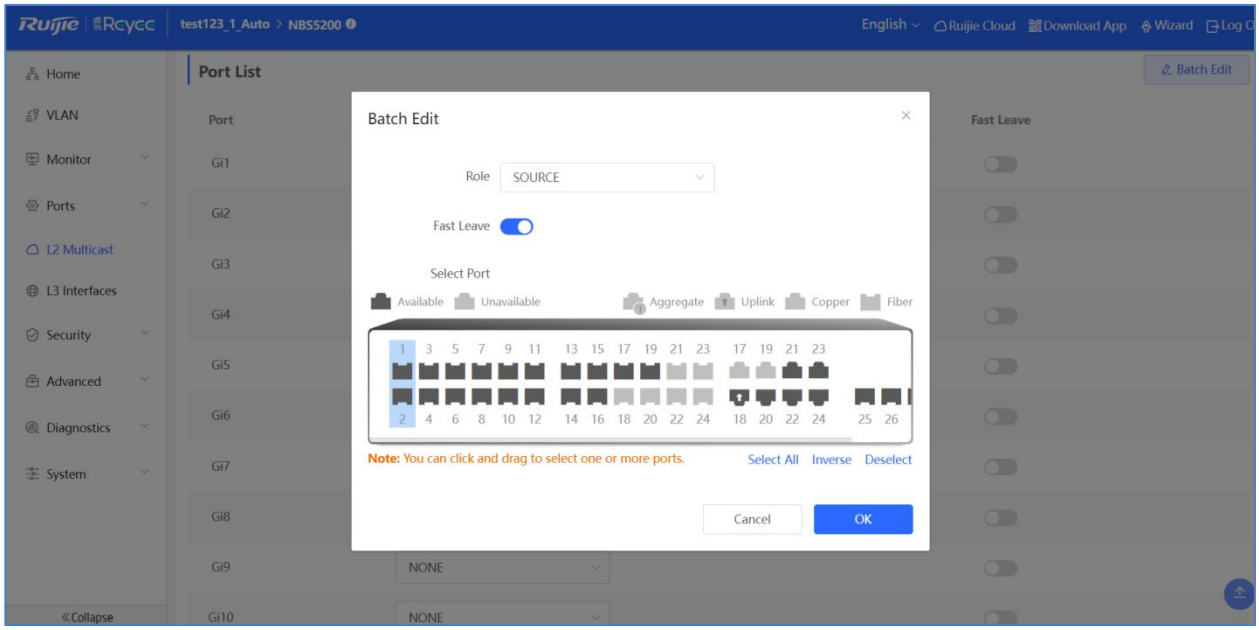
Receiver Port: The receiver port is the port where a listening host is connected to the switch. It utilizes any (or no) VLAN, except the multicast VLAN. This implies that the MVR switch performs VLAN tag substitution from the multicast VLAN source port to the VLAN tag used by the receiver port.

The Multicast VLAN is the VLAN that is configured in the specific network for MVR purposes. It has to be manually specified by the operator for all source ports in the network. It is a VLAN that is used to transfer multicast traffic over the network to avoid duplication of multicast streams for clients in different VLANs.

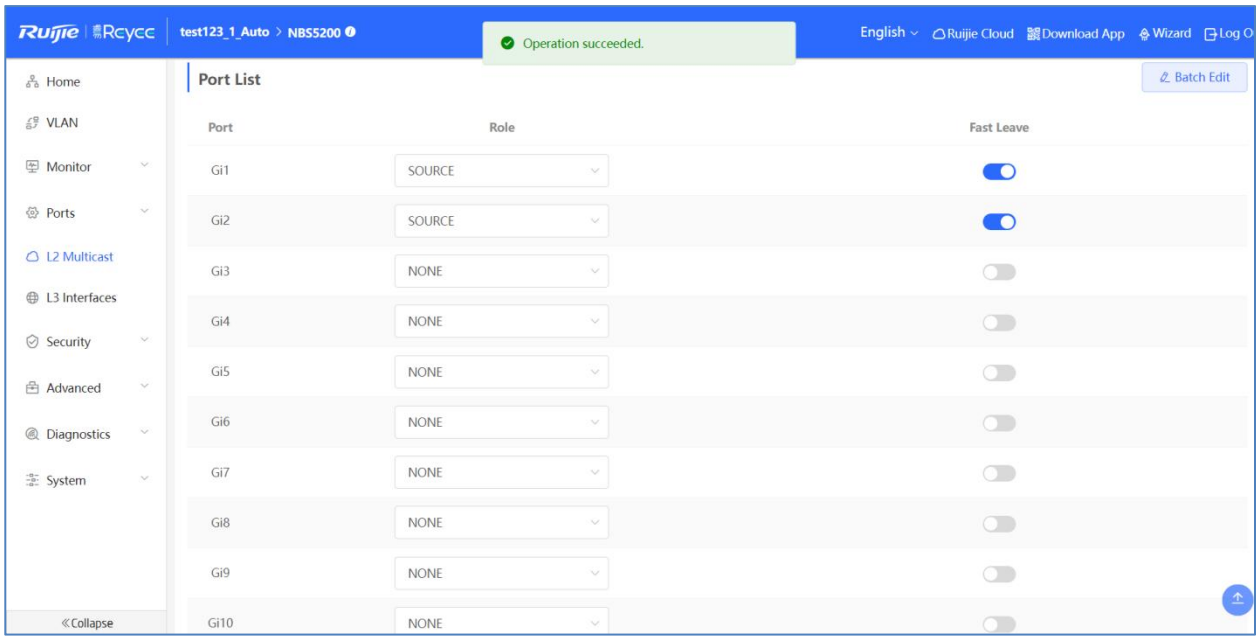
Enable the MVR and enter the Multicast VLAN, Start IP Address, End IP Addres, at last, click **Save**.



Click **Batch Edit** in the **Action** column. In the displayed dialog box, you can set port role, fast leave and select ports.



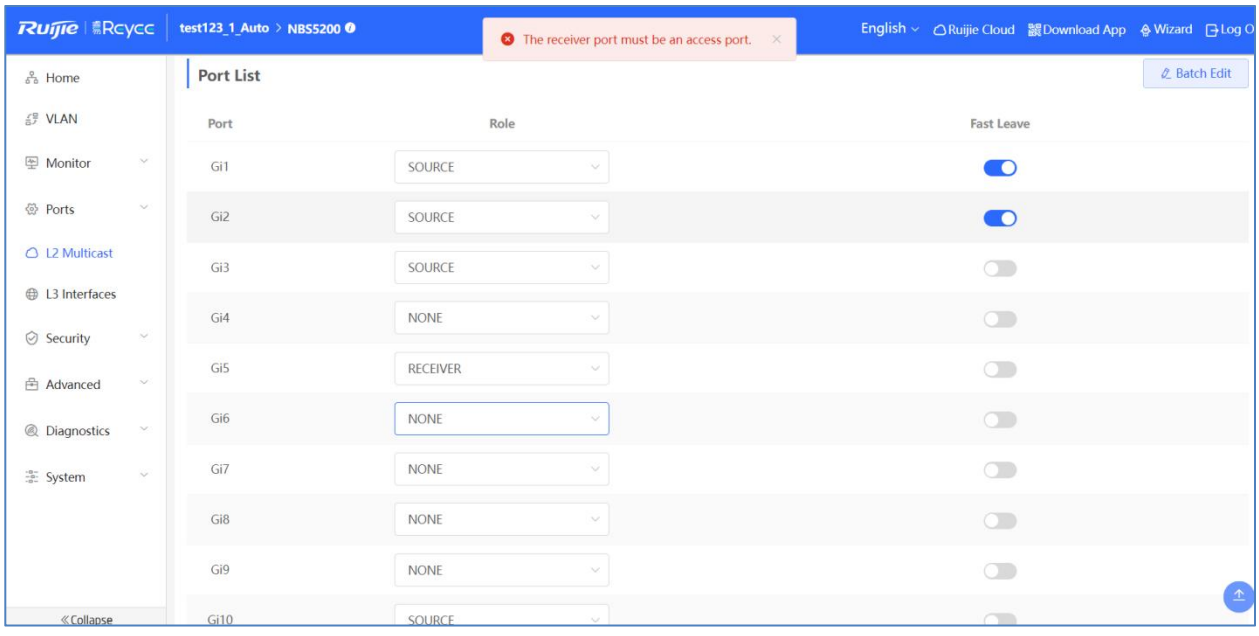
The message "Operation succeeded." is displayed, and the port list is updated.



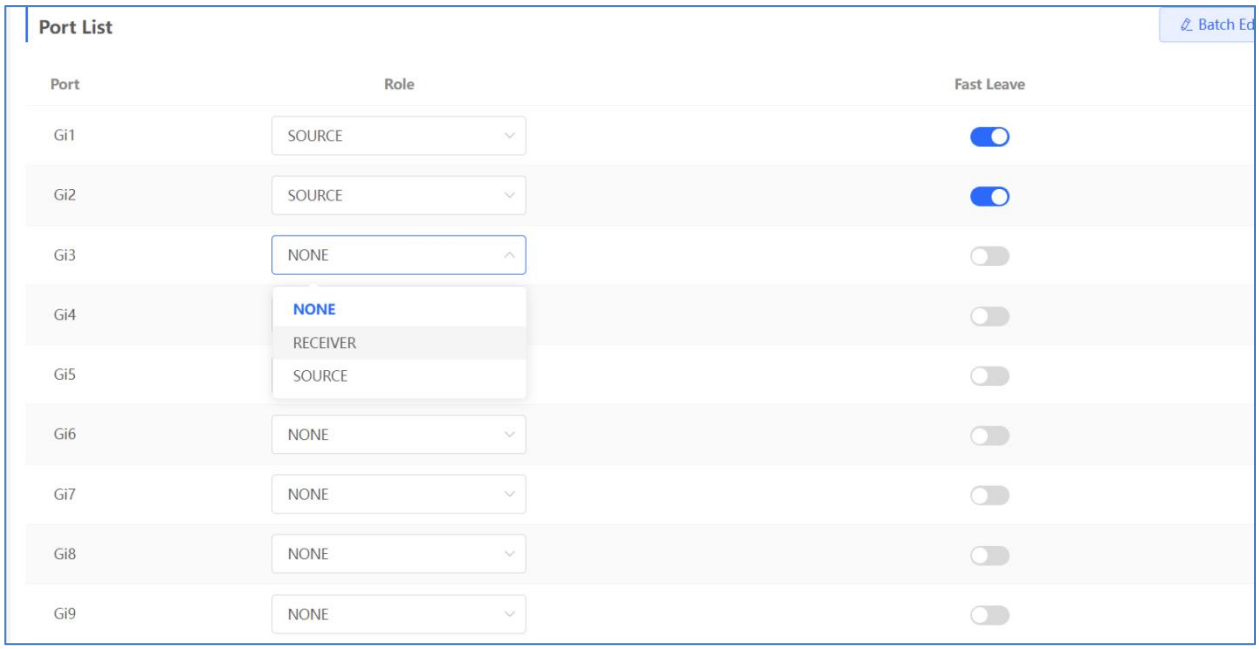
The source port must be a MVR VLAN member and the receiver port cannot be a MVR VLAN member.

Fast Leave settings only take effect on the destination port.

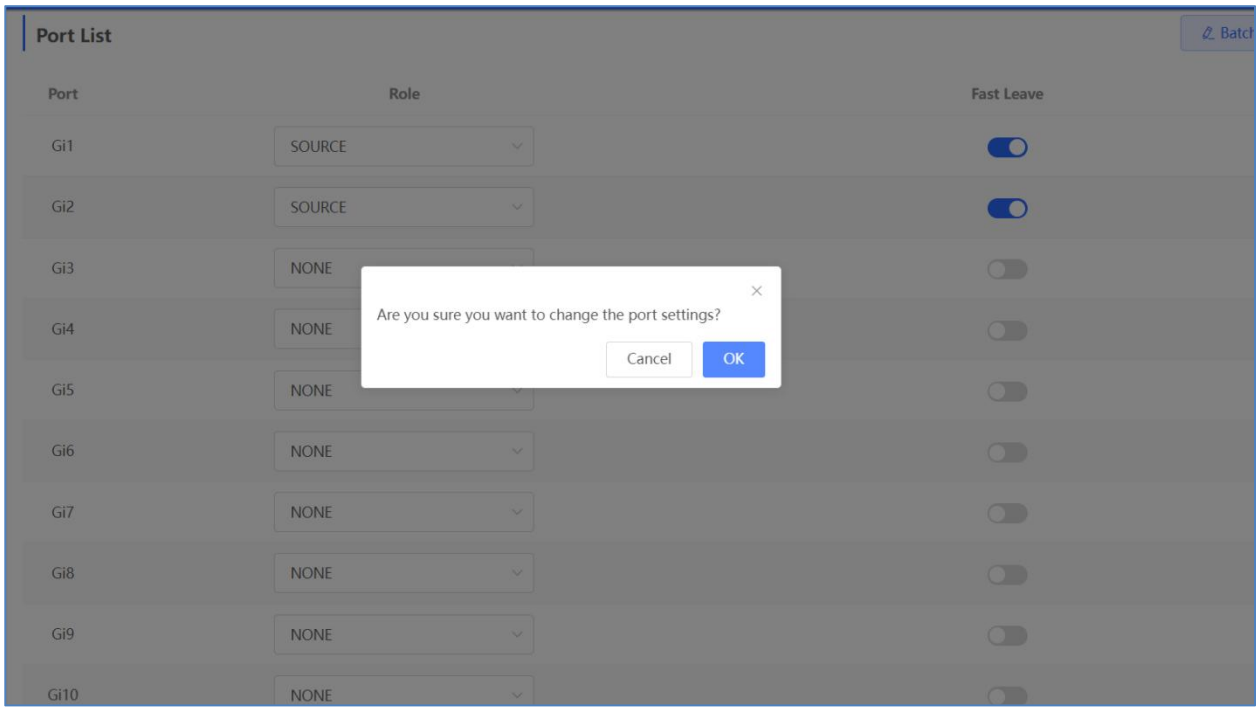
The receiver port must be an access port.



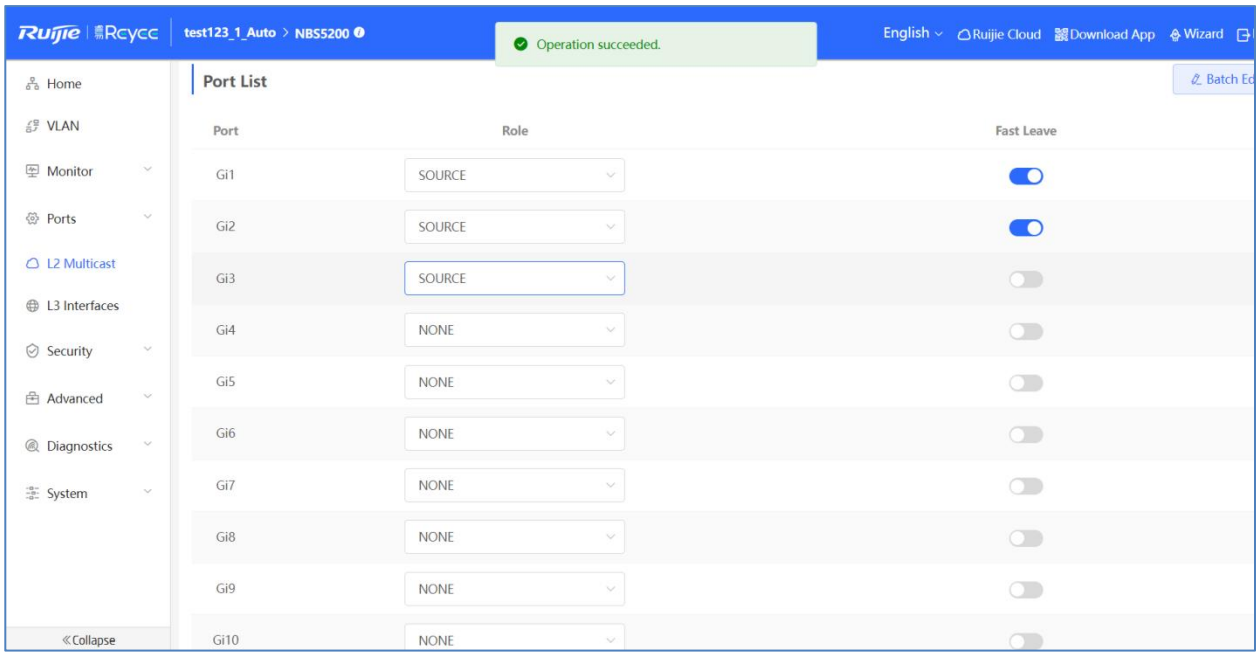
You can configure the **Role** of a single in its role column.



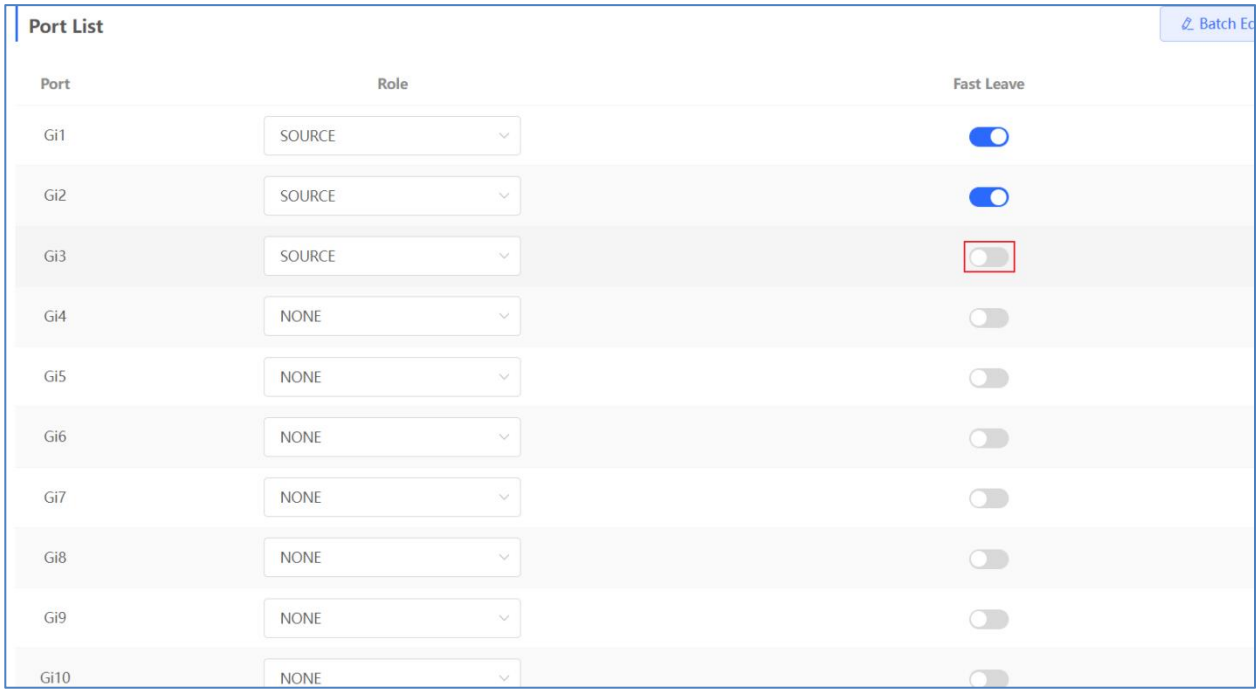
Click **OK** in the pop-up window.



The message "Operation succeeded." is displayed, and the port list is updated.

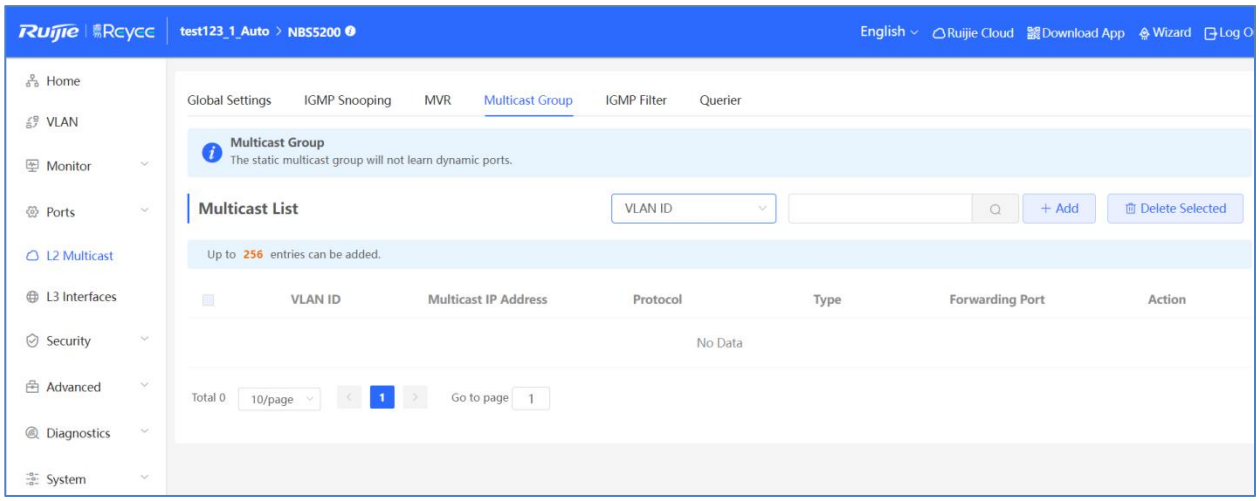


You can configure **Fast Leave** to a single port in its Fast Leave column.

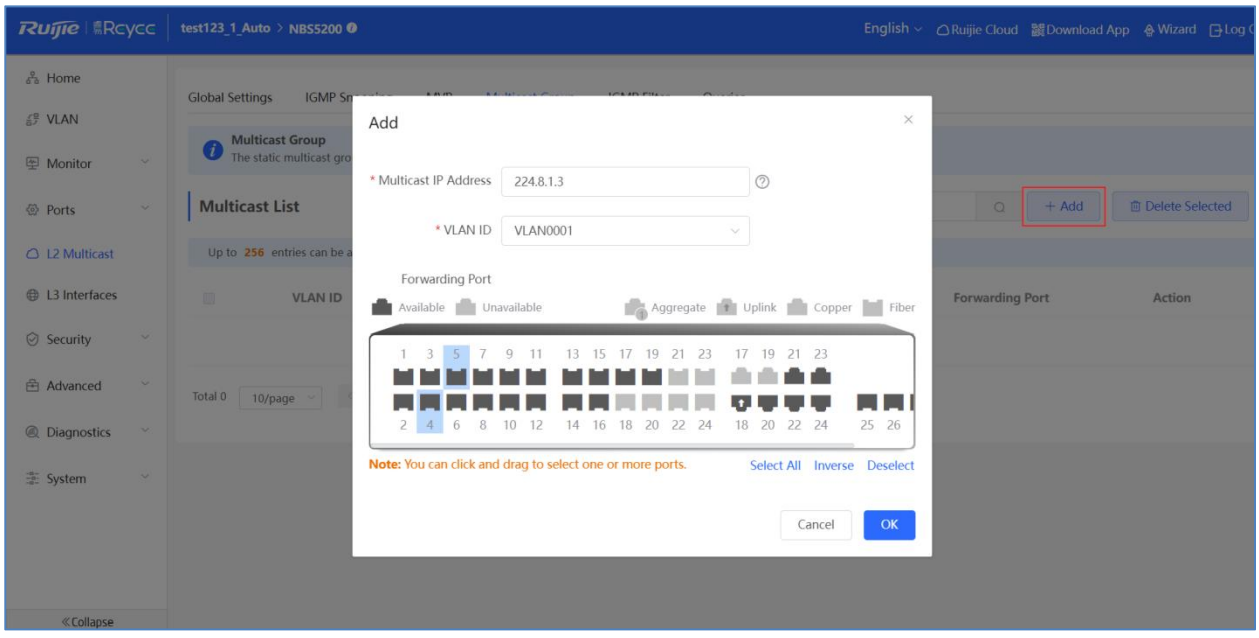


4.3.3.4 Multicast Group

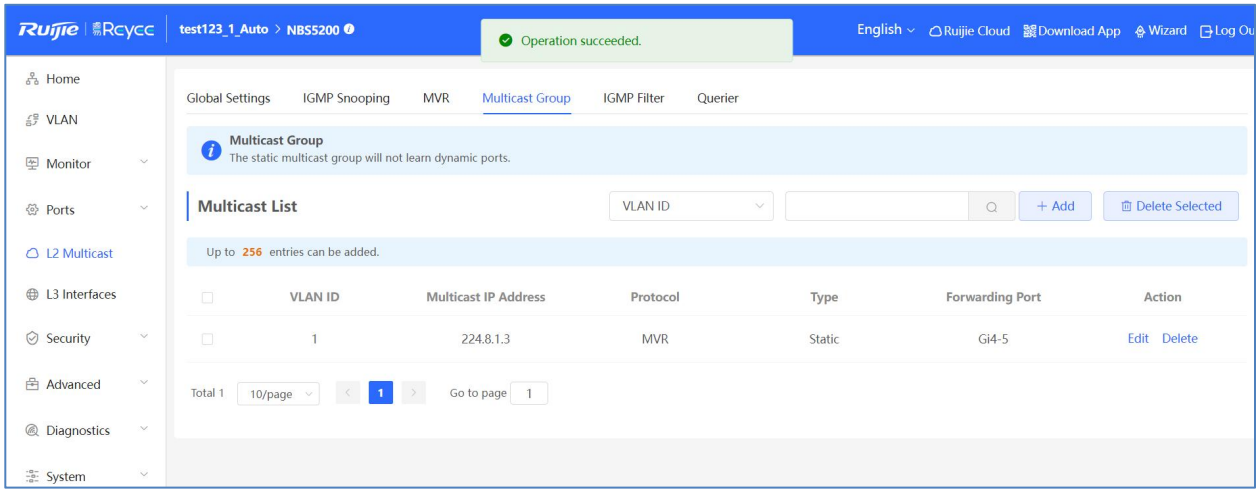
The static multicast group will not learn dynamic ports.



Click **Add**. In the displayed dialog box, you can set the multicast IP address, VLAN ID and select ports.

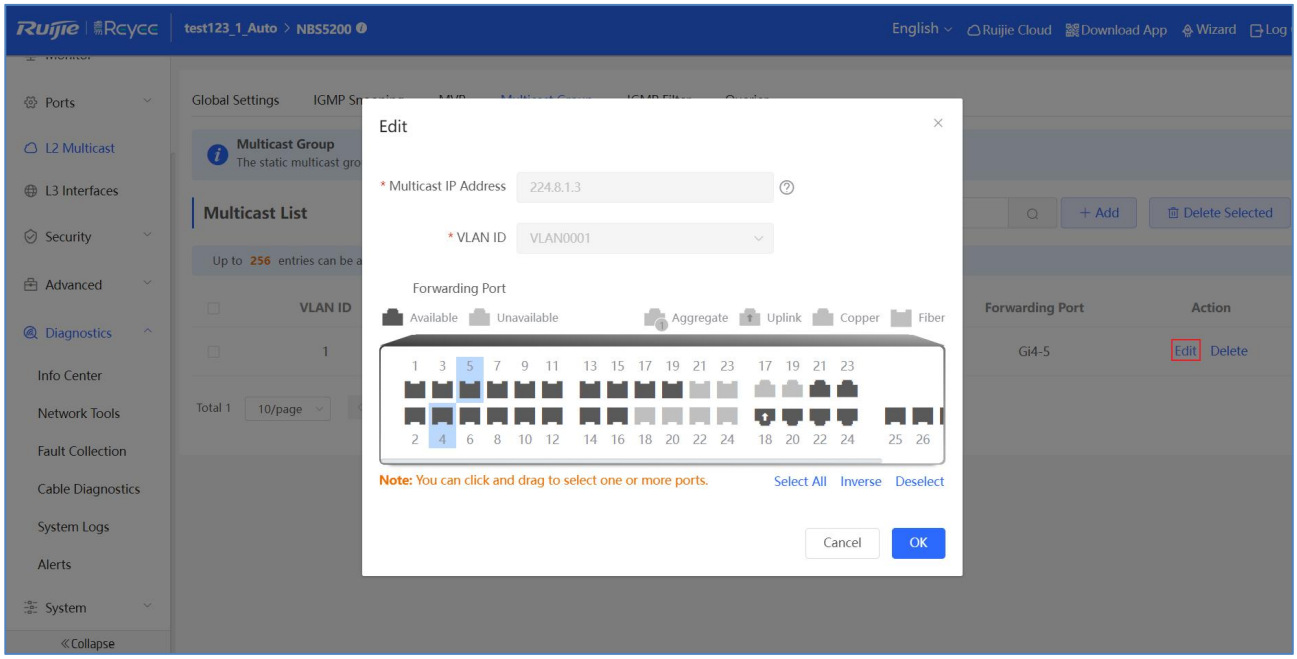


The message "Operation succeeded." is displayed, and the Multicast list is updated.

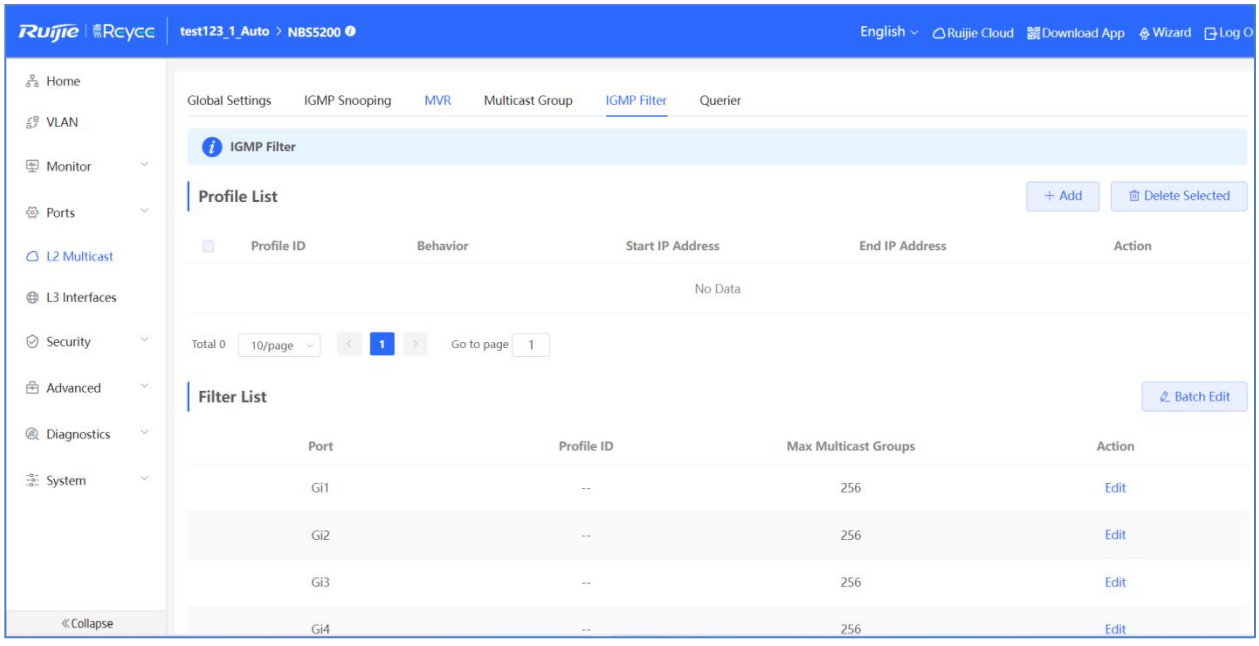


The MVR outgoing port must be a receiver port.

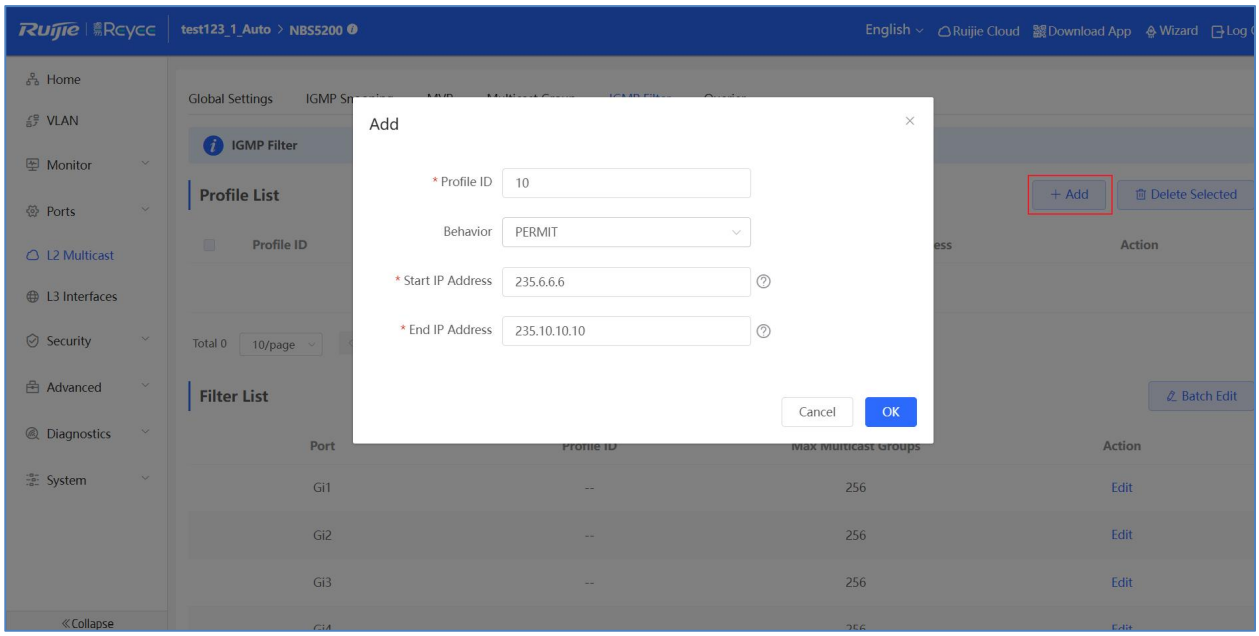
Click **Edit**. In the displayed dialog box, you can select or deselect the ports.



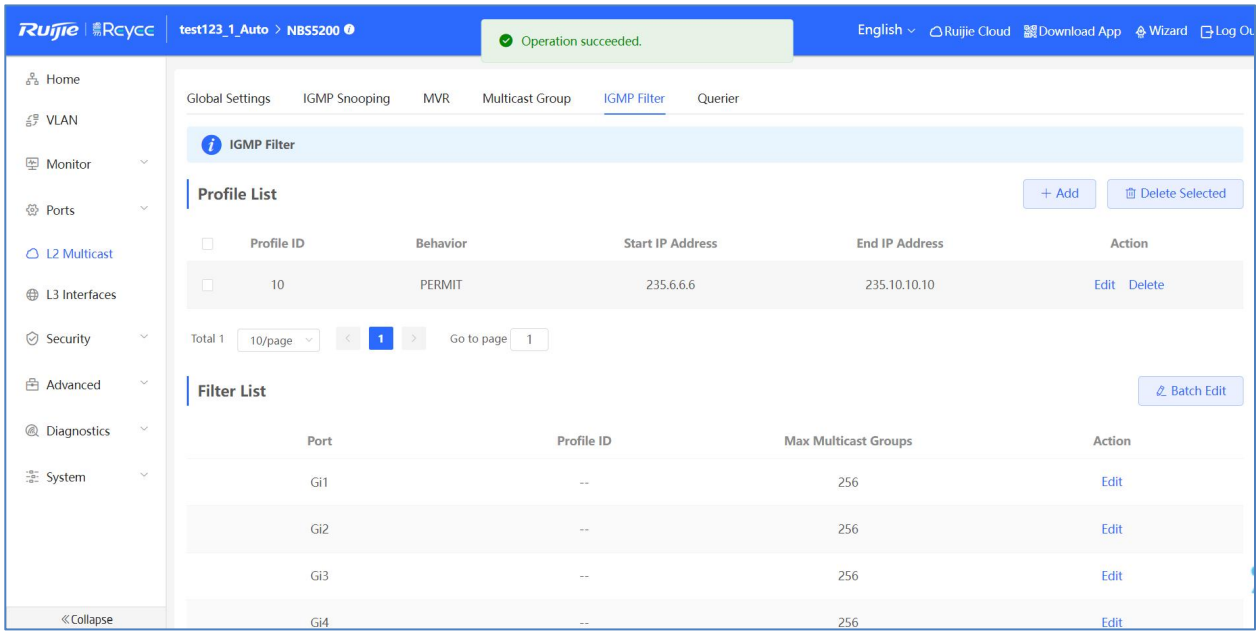
4.3.3.5 IGMP Filter



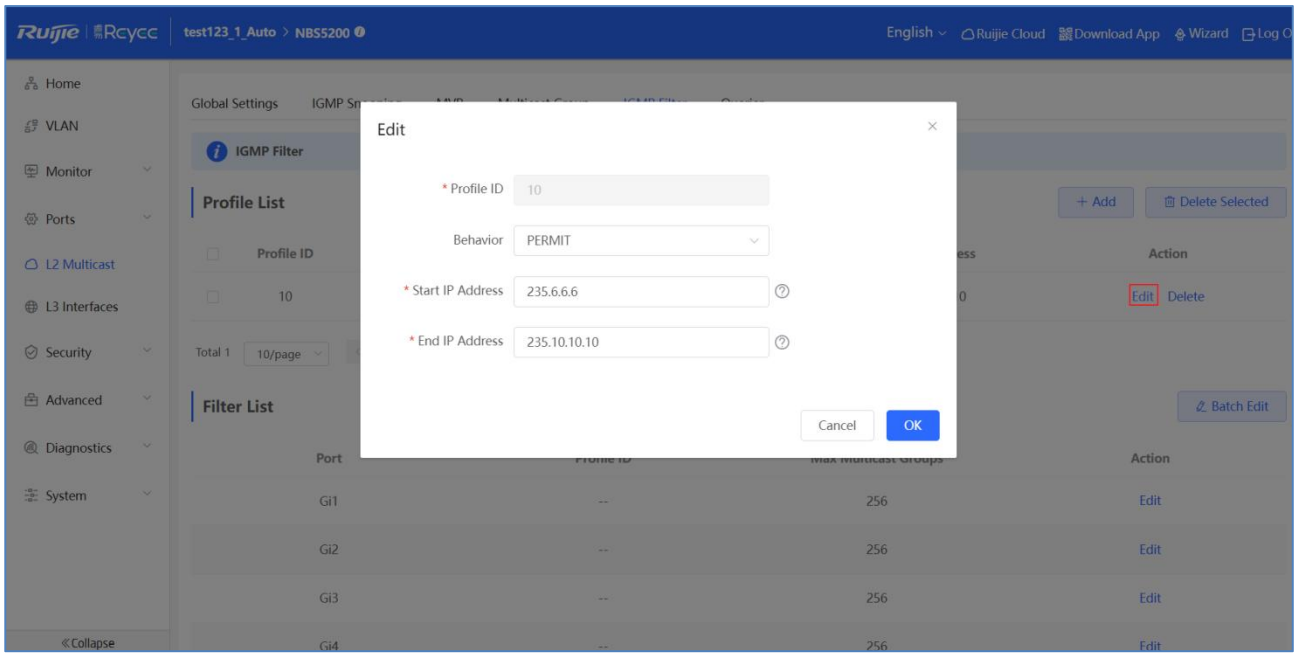
Click **Add**. In the displayed dialog box, you can set the profile ID, behavior, start IP address and end IP address.



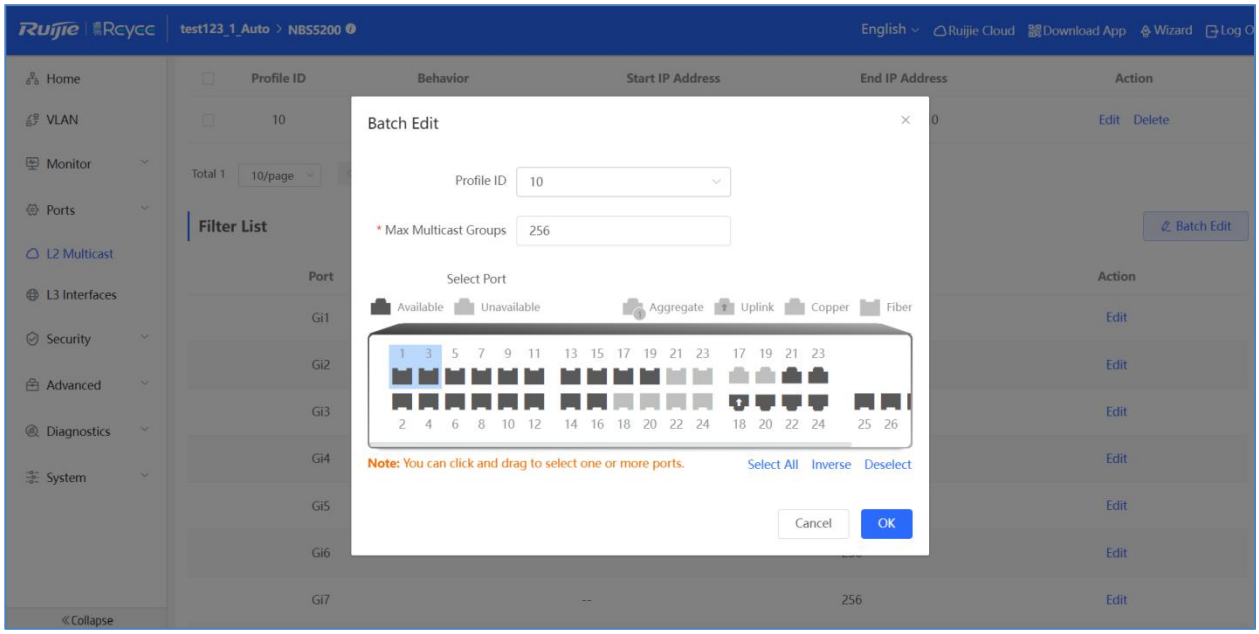
The message "Operation succeeded." is displayed, and the profile list is updated.



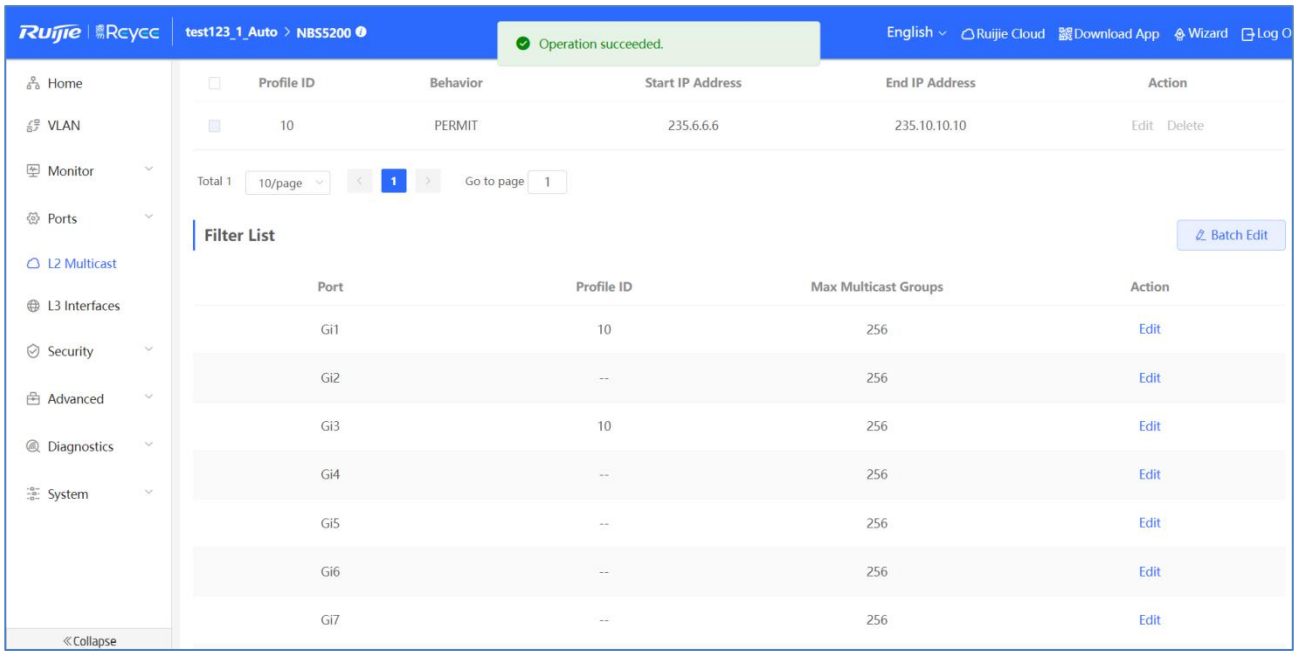
Click **Edit**. In the displayed dialog box, you can set the behavior, start IP address and end IP address.



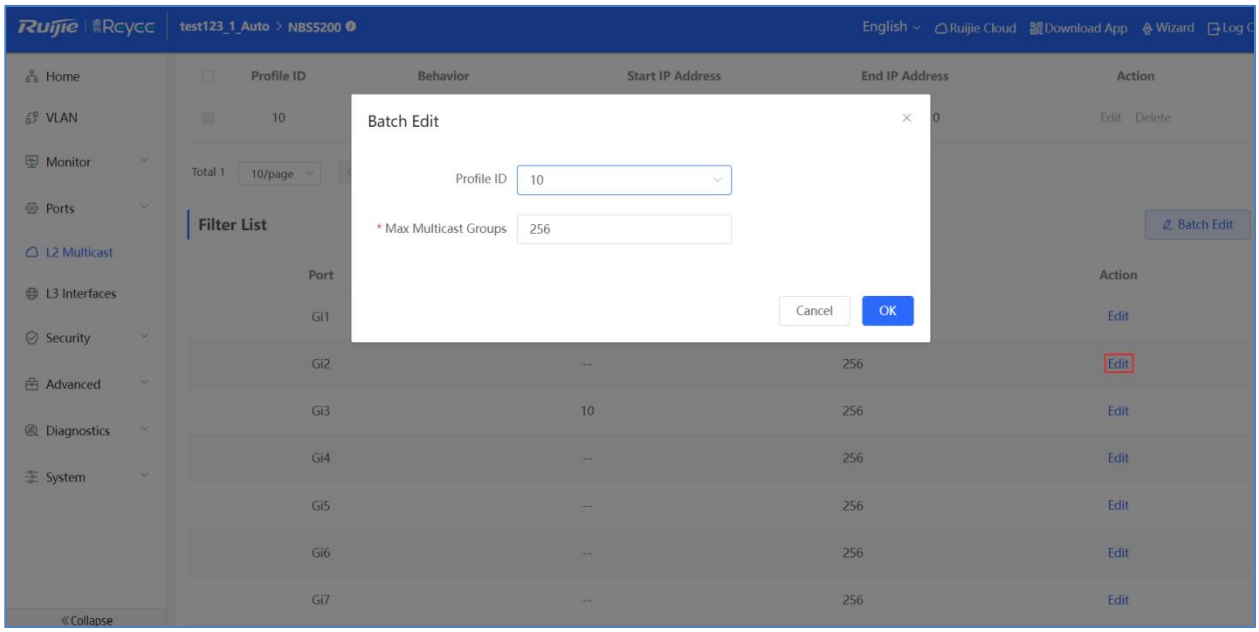
Click **Batch Edit.** In the displayed dialog box, you can set the profile ID, max multicast groups and select ports.



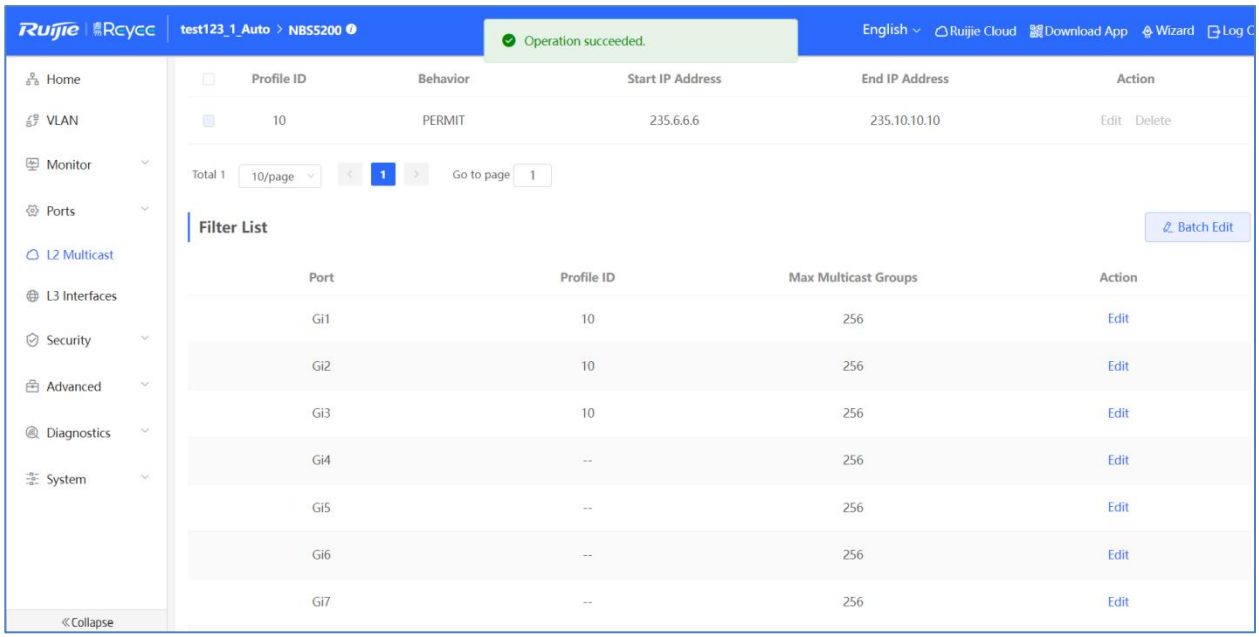
The message "Operation succeeded." is displayed, and the filter list is updated.



Click **Edit.** In the displayed dialog box, you can set the profile ID, max multicast groups and select ports.

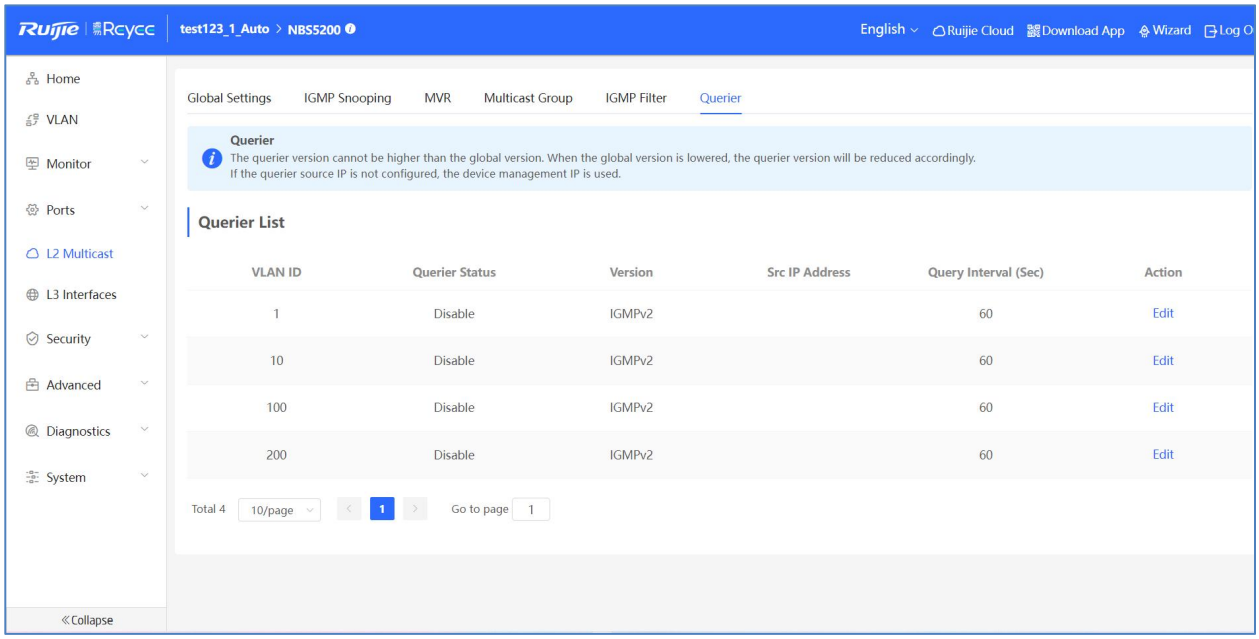


The message "Operation succeeded" is displayed, and the filter list is updated.

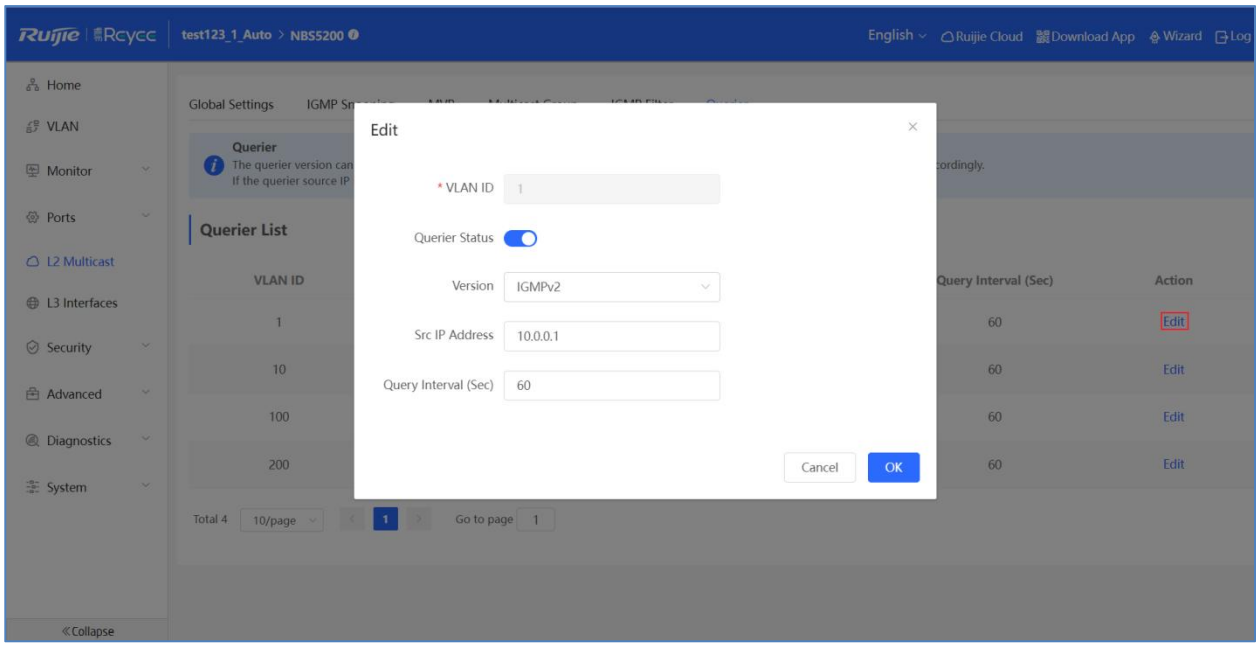


4.3.3.6 Querier

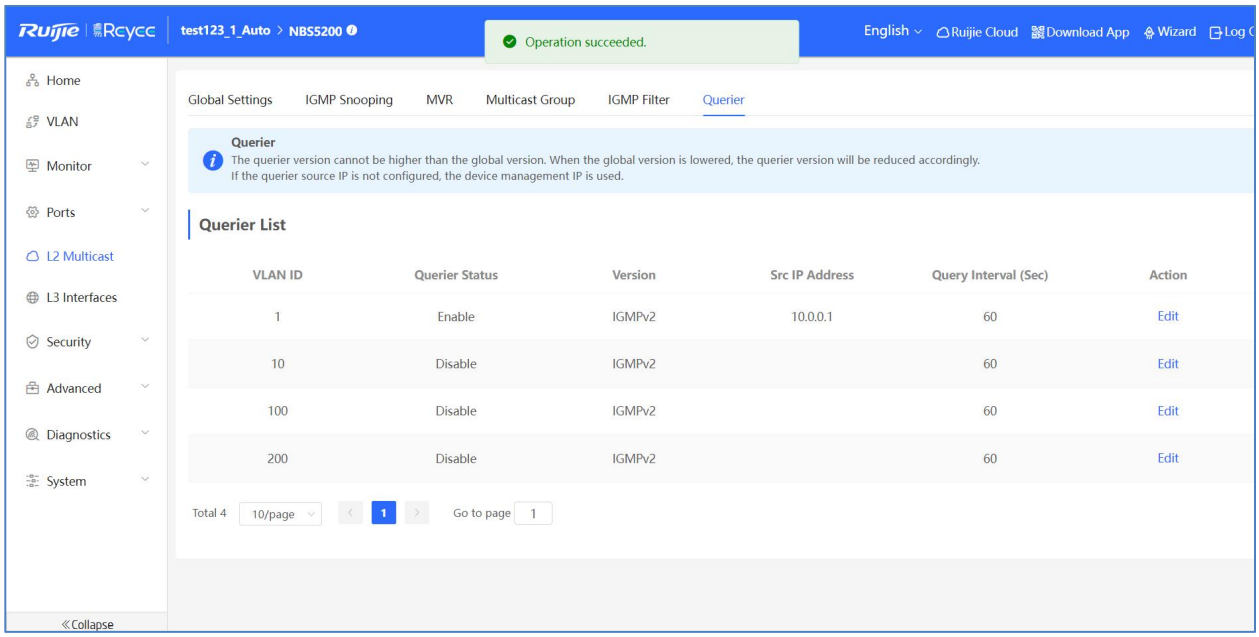
The querier version cannot be higher than the global version. When the global version is lowered, the querier version will be reduced accordingly. If the querier source IP is not configured, the device management IP is used.



Click **Edit.** In the displayed dialog box, you can set VLAN ID, querier status, version, source IP address and query interval.



The message "Operation succeeded" is displayed, and the querier list is updated.



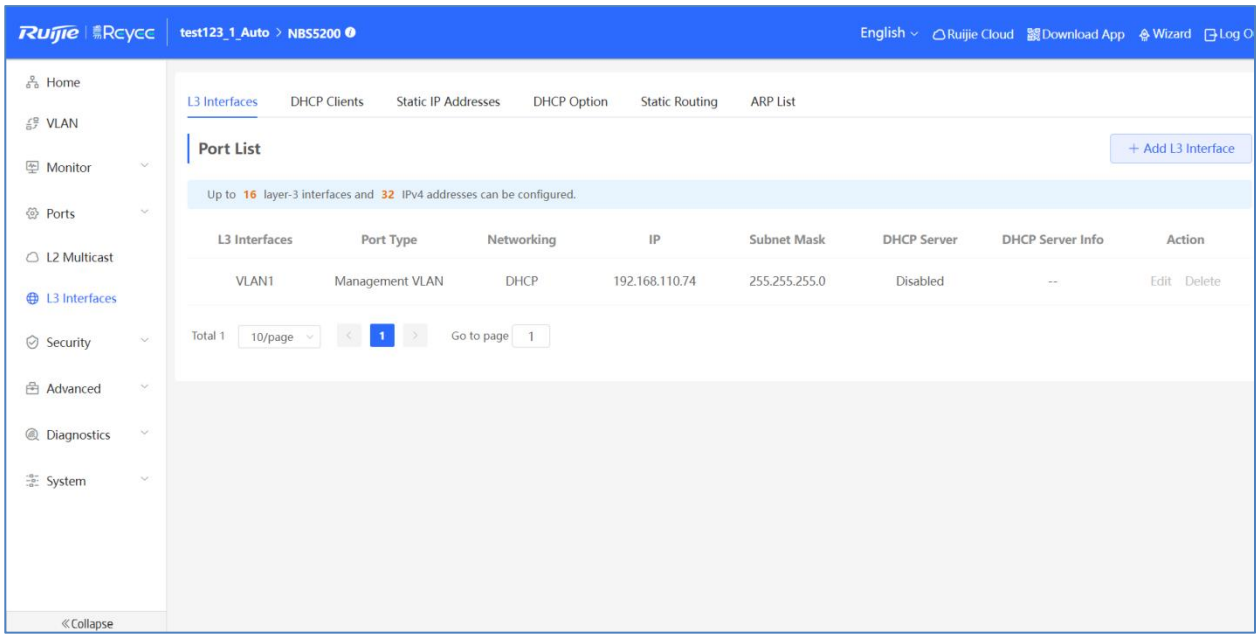
4.3.4 L3 Interfaces

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

Routed Port: A physical port of a layer-3 device can be configured as a routed port. A routed port works as an access port and does not support layer-2 switching.

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

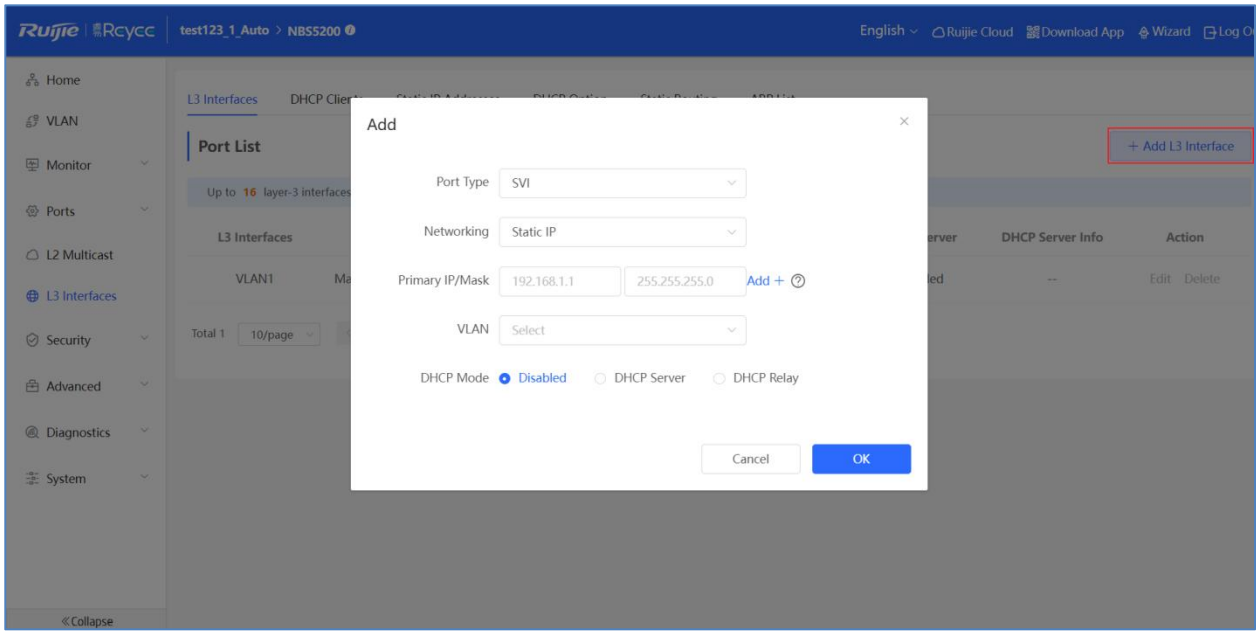
SVI: An SVI can be used as a management interface. You can also create an SVI for inter VLAN routing.



4.3.4.1 L3 Interfaces

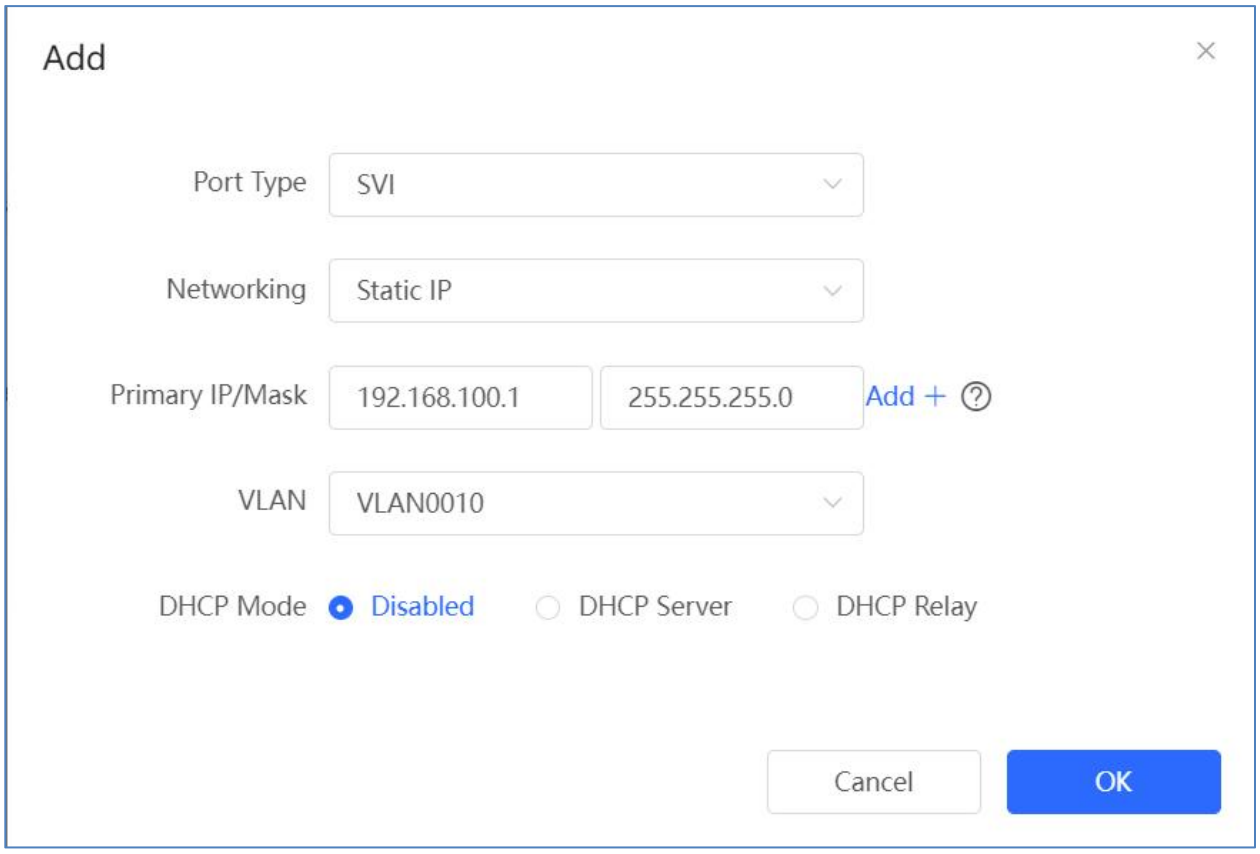
1.1 Add an SVI

Click **Add L3 Interface**. In the displayed dialog box, select **SVI** from the **Port Type** dropdown list.

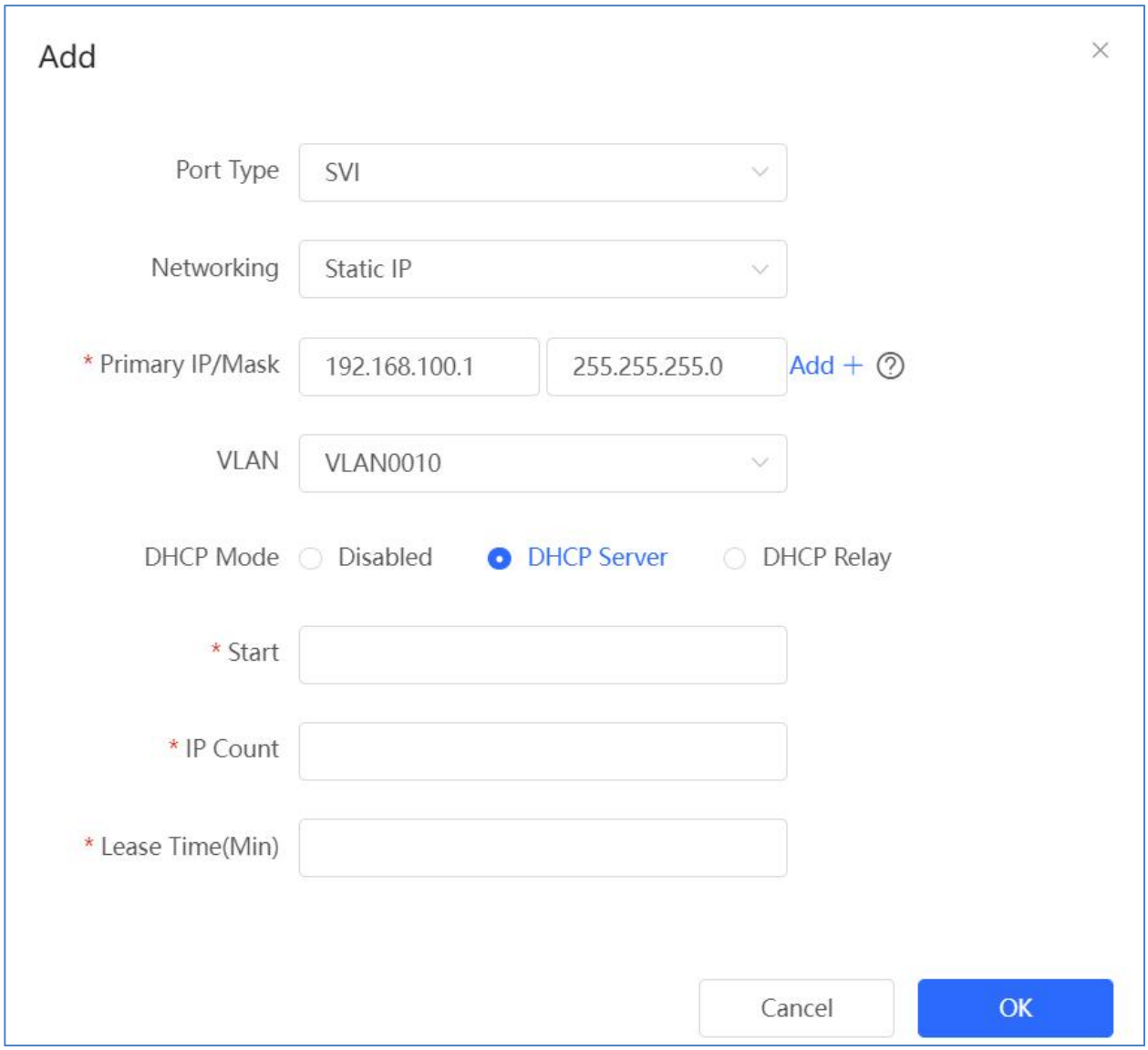


Select the **networking.** If you select the **Static IP** Address, you can set the IP address, subnet mask manually (You can configure one primary IP address and multiple secondary IP addresses, if the primary IP address is not configured, the secondary IP address does not take effect.), VLAN and DHCP Mode.

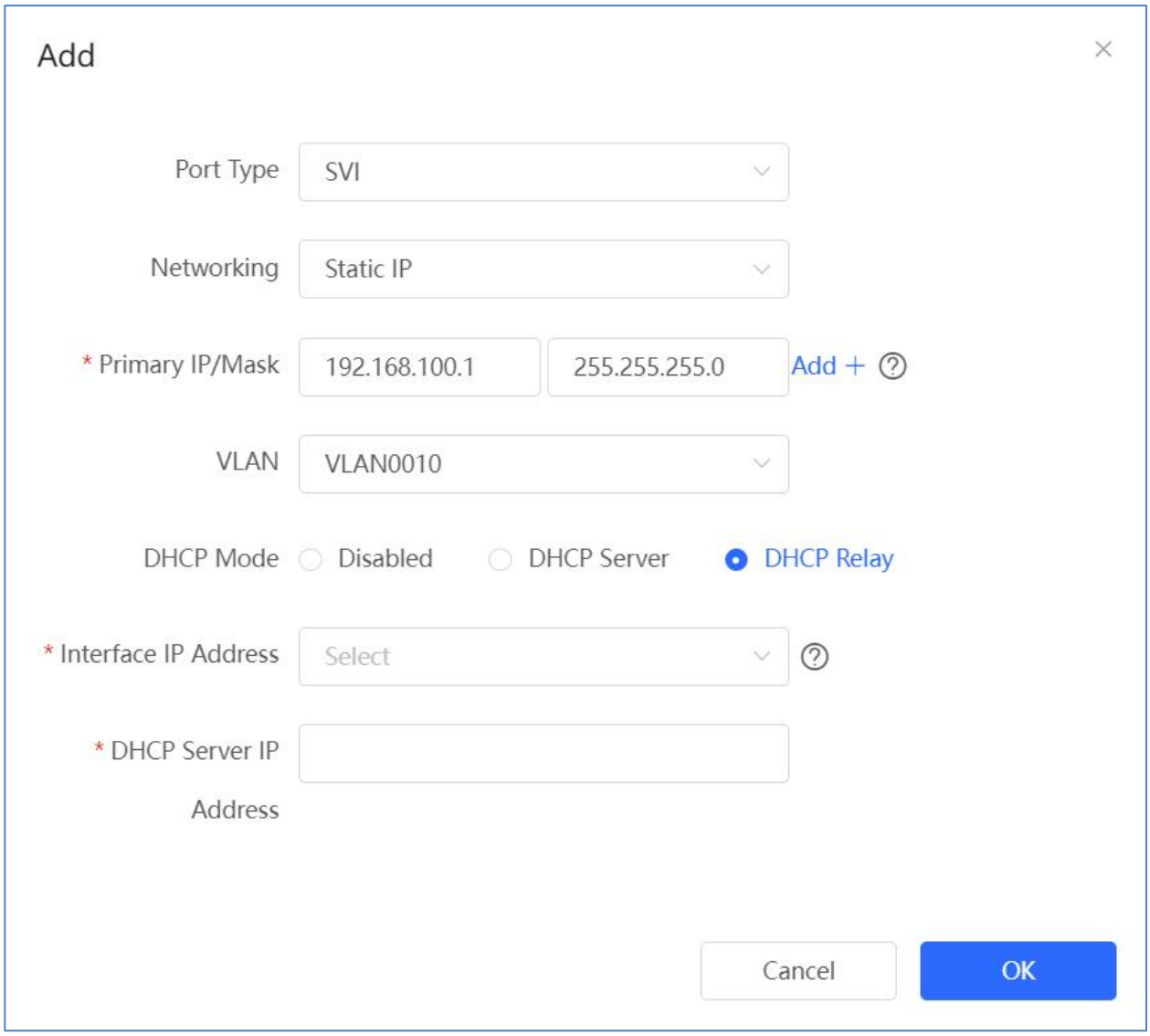
DHCP Mode: Disable



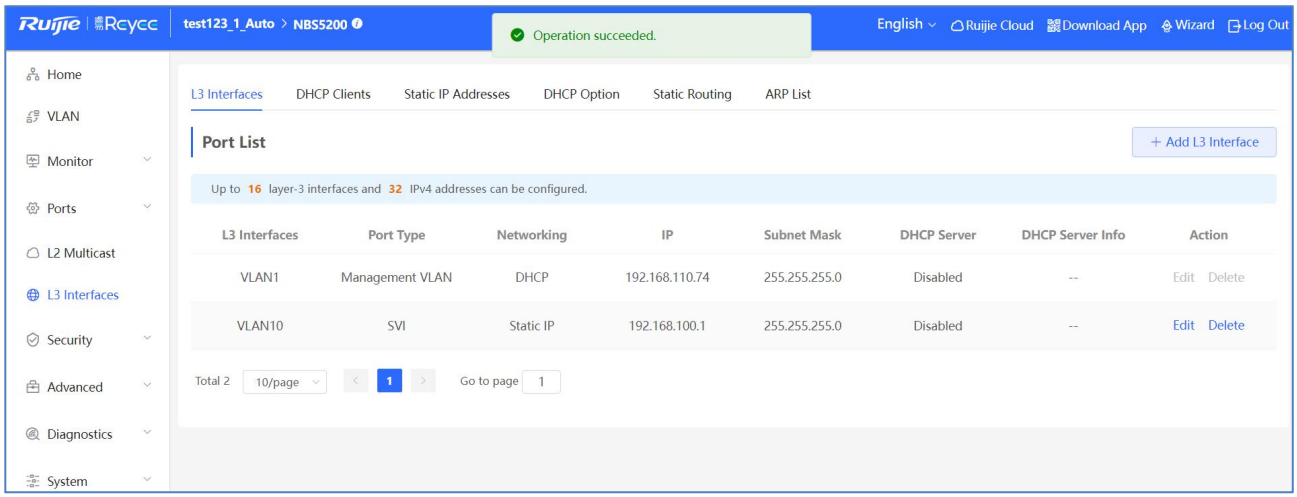
DHCP Mode: DHCP Server



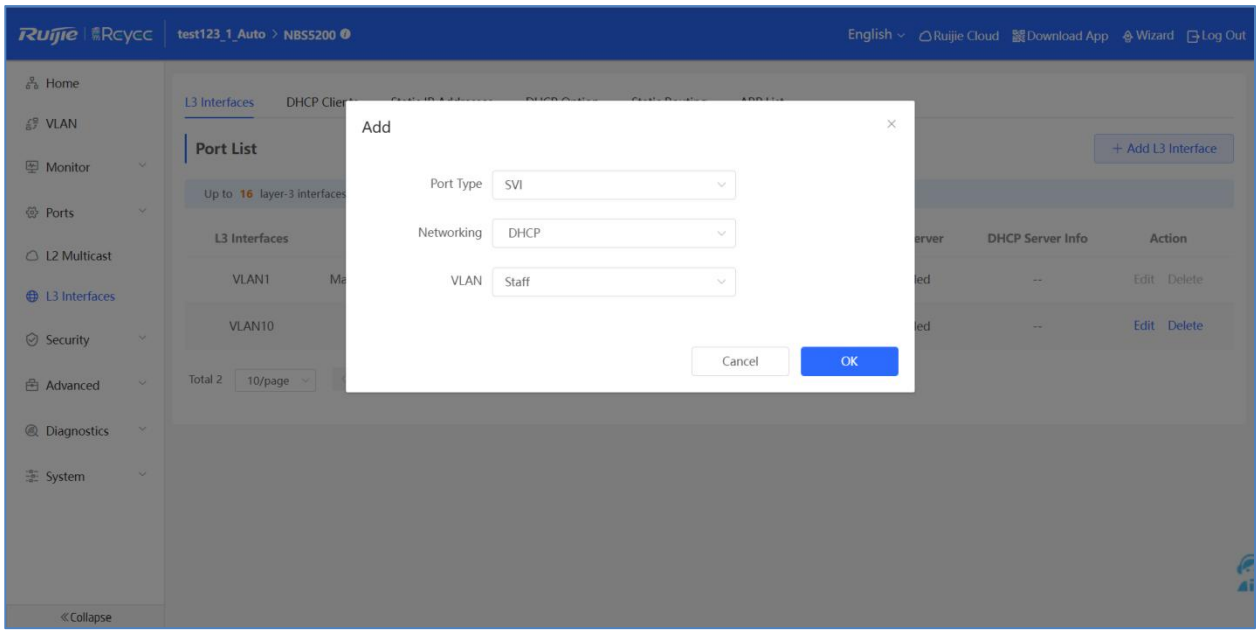
DHCP Mode: DHCP Relay



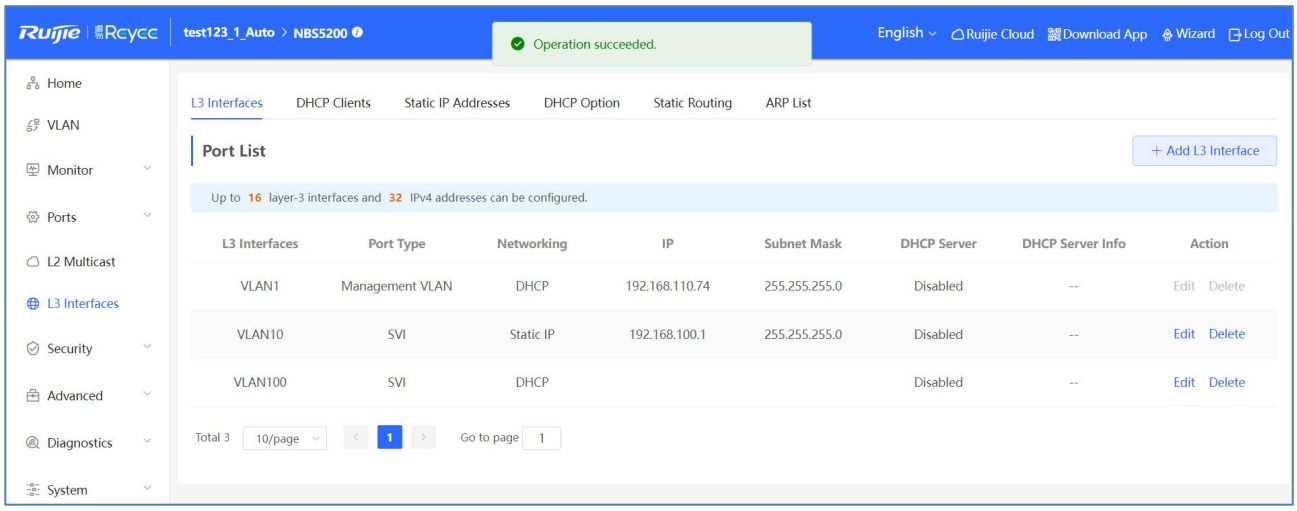
The message "Operation succeeded." is displayed, and the port list is updated.



If you select **DHCP**, the SVI will obtain the DHCP-assigned IP address.



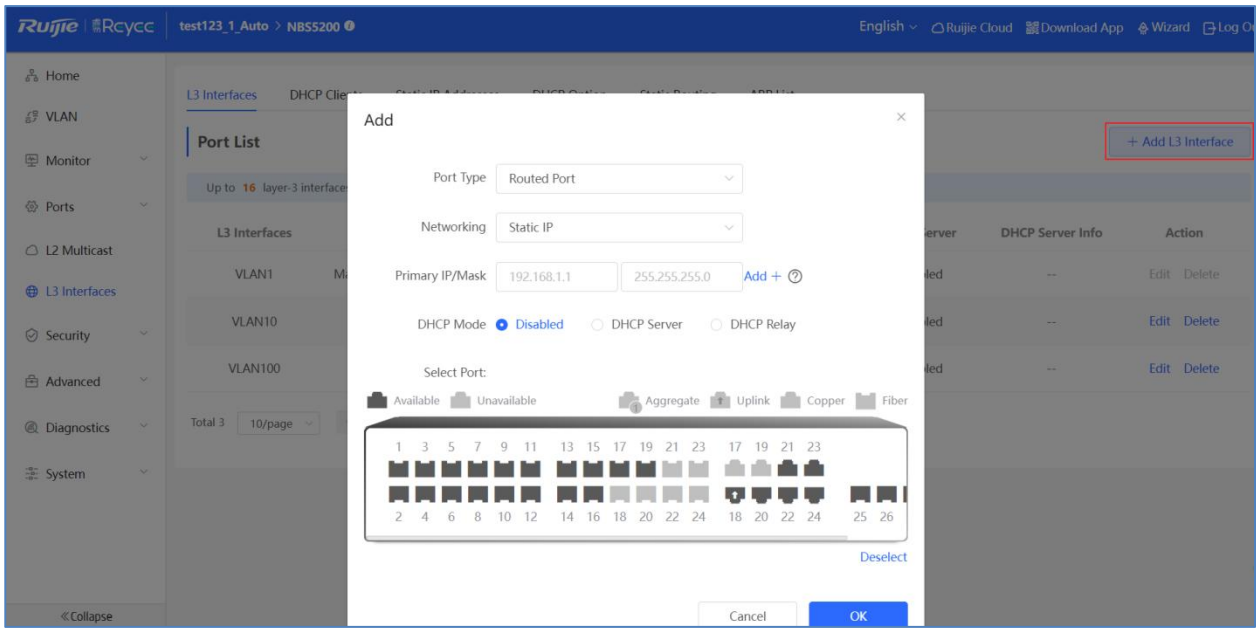
The message "Operation succeeded." is displayed, and the port list is updated.



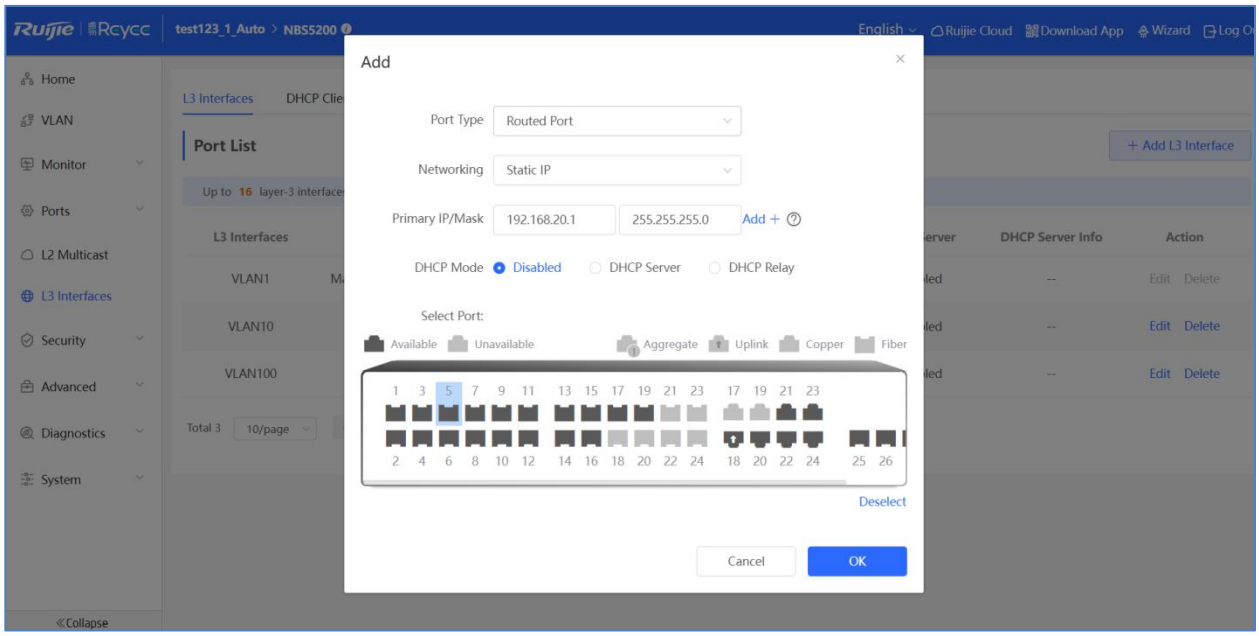
If you want to configure an **SVI** for a **VLAN**, please make sure that the VLAN is already created.

1.2 Add a Routed Port

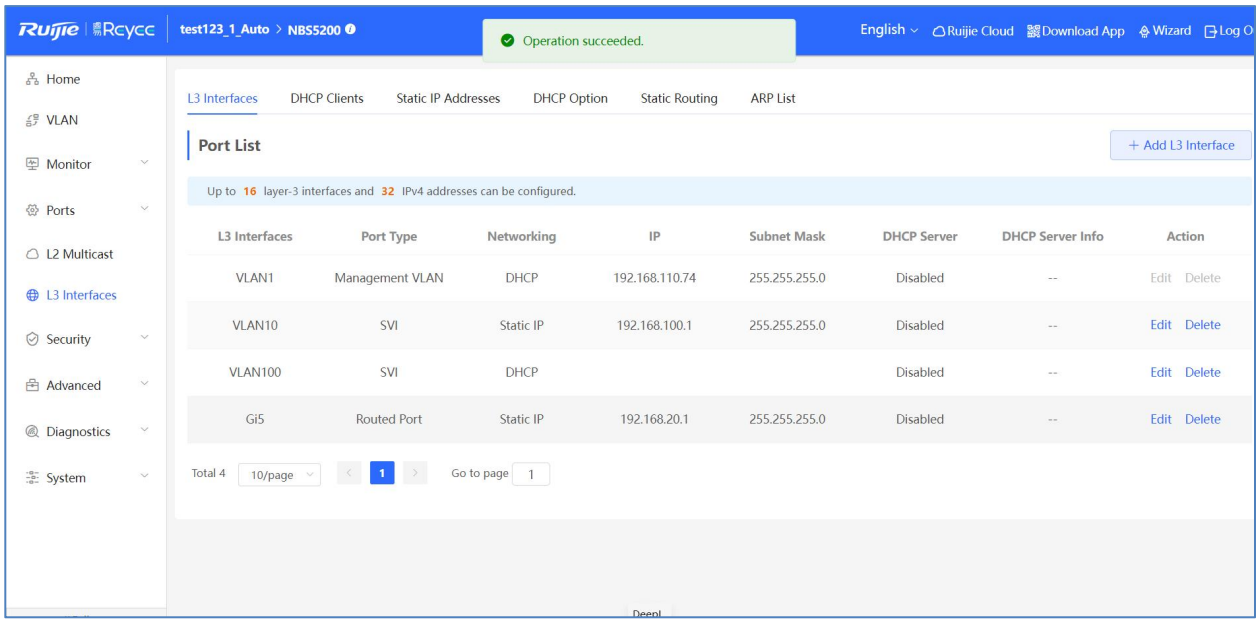
Click **Add L3 Interface**. In the displayed dialog box, select **Routed Port** from the Port Type dropdown list.



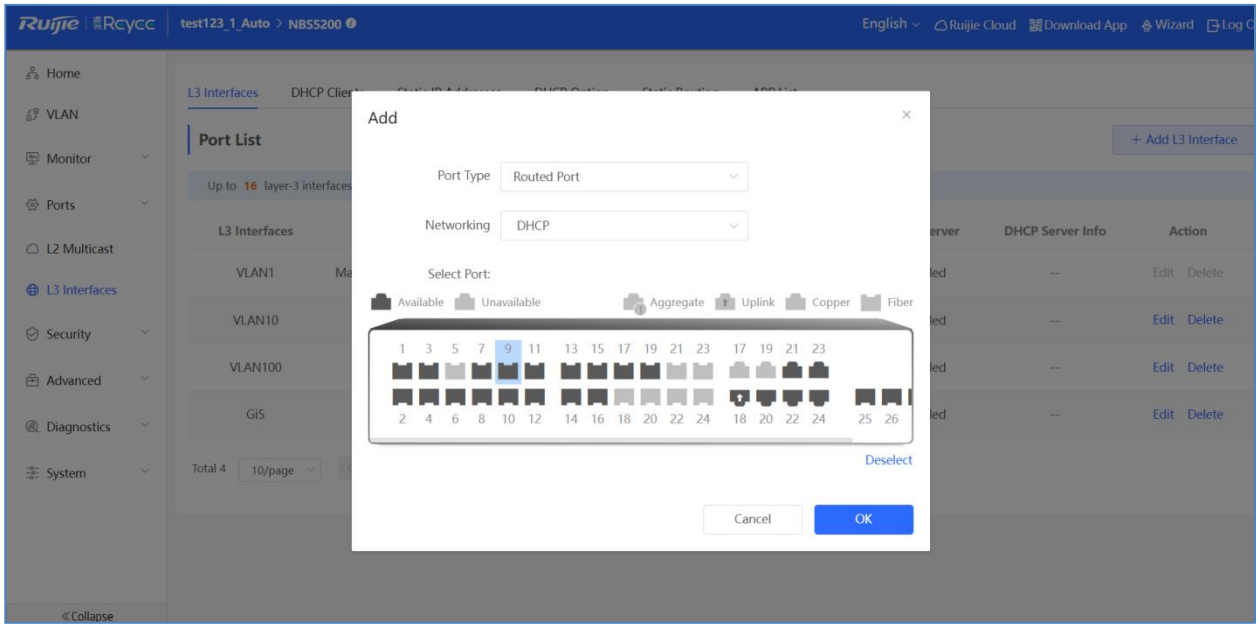
Select the **networking**. If you select **Static IP** Address, you can set the IP address, subnet mask manually (You can configure one primary IP address and multiple secondary IP addresses. If the primary IP address is not configured, the secondary IP address does not take effect.), DHCP Mode and select a physical port from the panel.



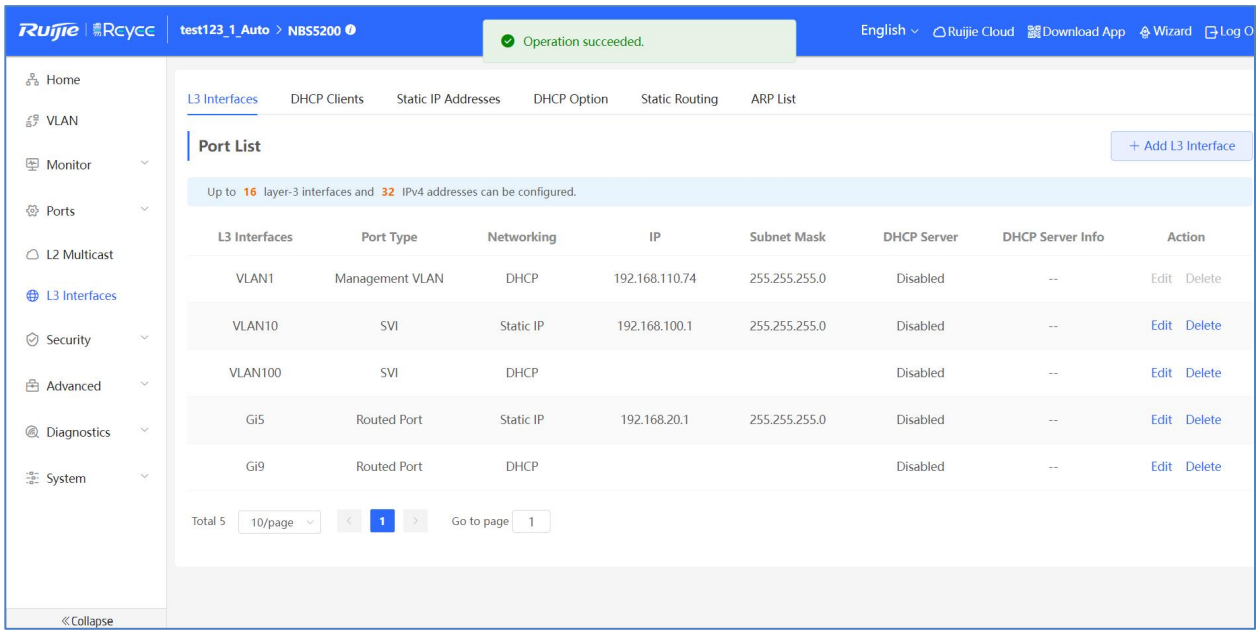
The message "Operation succeeded." is displayed, and the port list is updated.



If you select **DHCP**, the routed port will obtain the DHCP-assigned IP address.

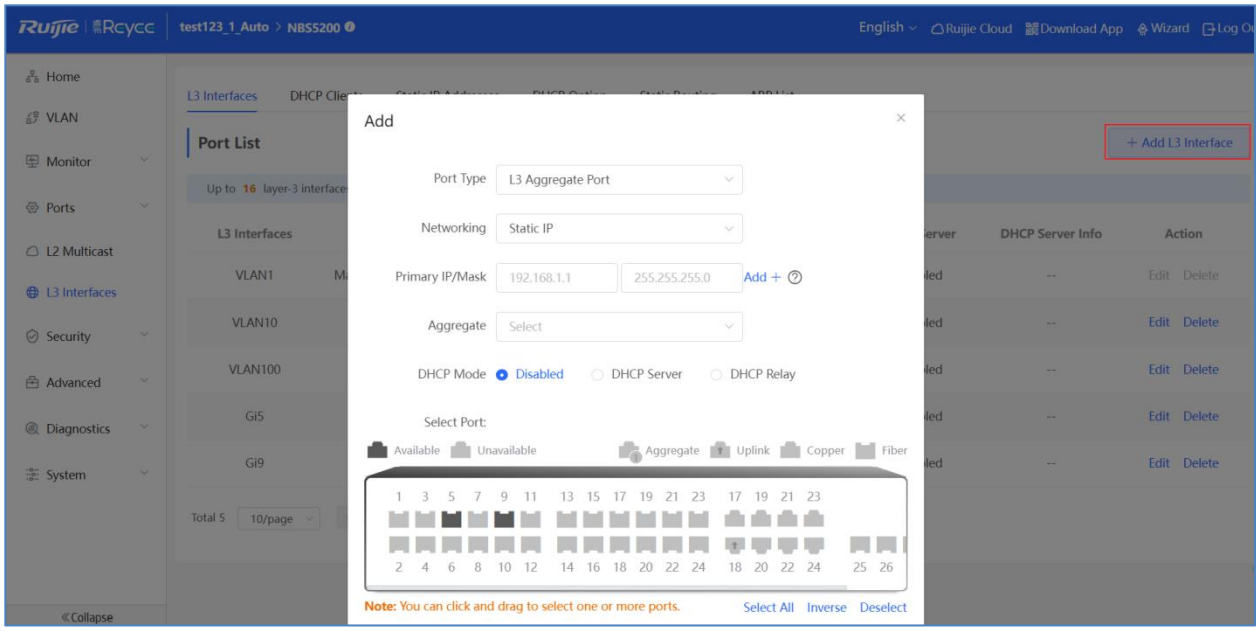


The message "Operation succeeded." is displayed, and the port list is updated.



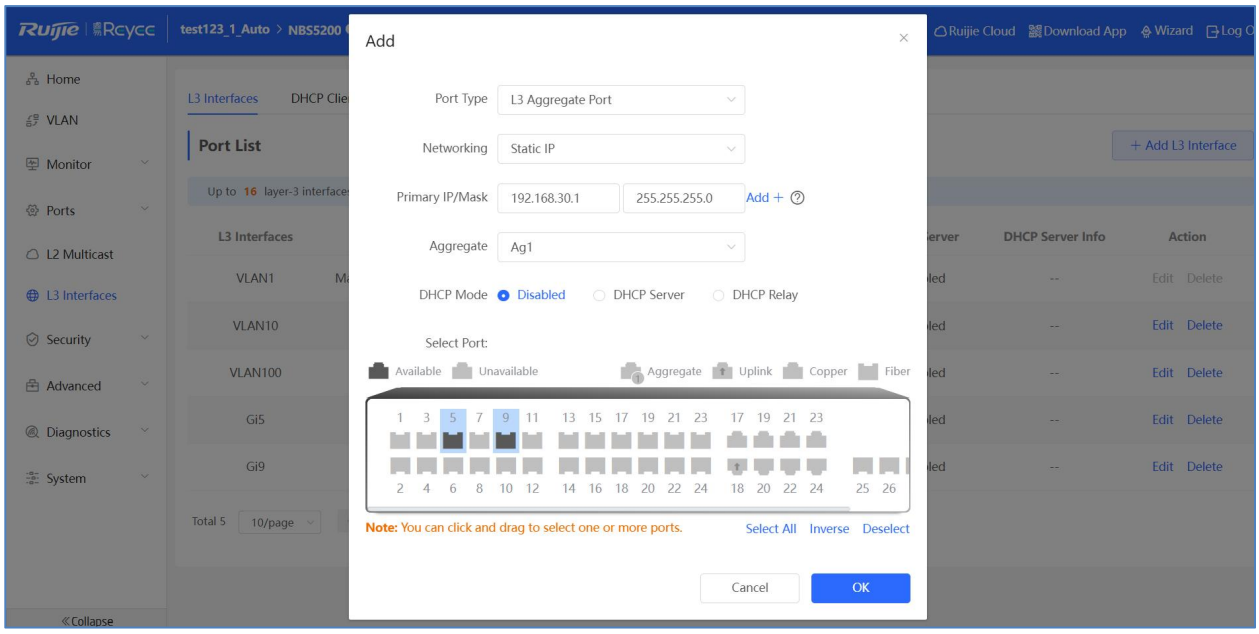
1.3 Add a L3 Aggregate Port

Click **Add L3 Interface**. In the displayed dialog box, select **L3 Aggregate Port** from the Port Type dropdown list.

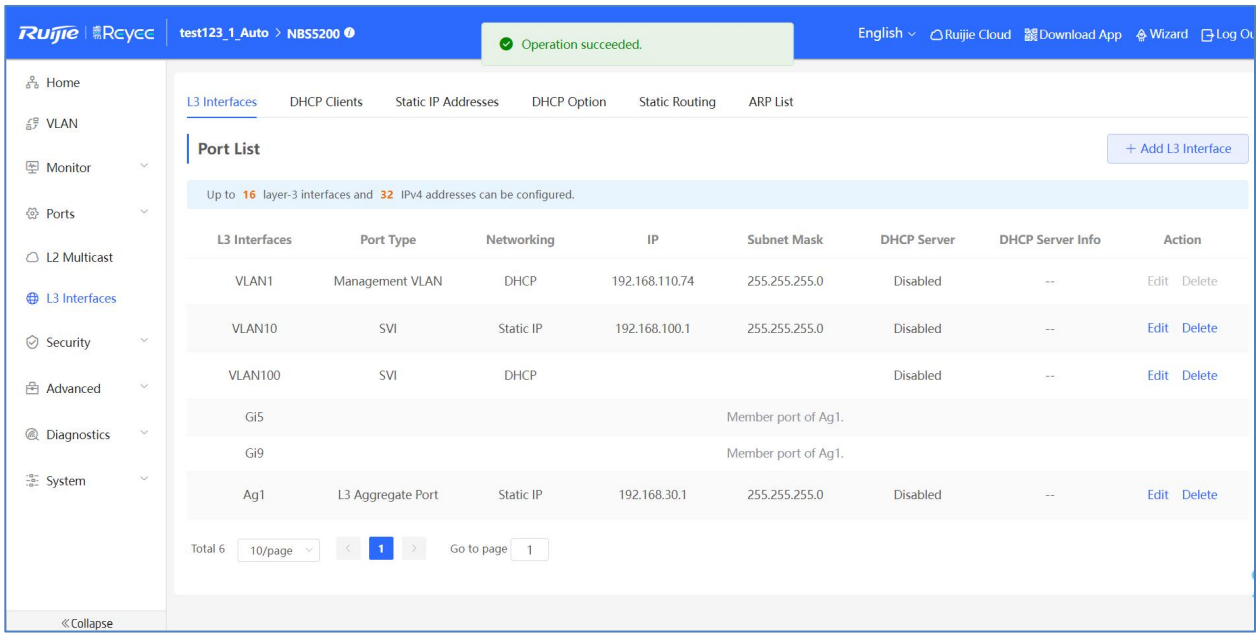


Select the **networking**. If you select **Static IP** Address, you can set the IP address, subnet mask manually (You can configure one primary IP address and multiple secondary IP addresses. If the primary IP address is not configured, the secondary IP address does not take effect.), Aggregate, DHCP Mode and select physical **routed** ports from the panel.

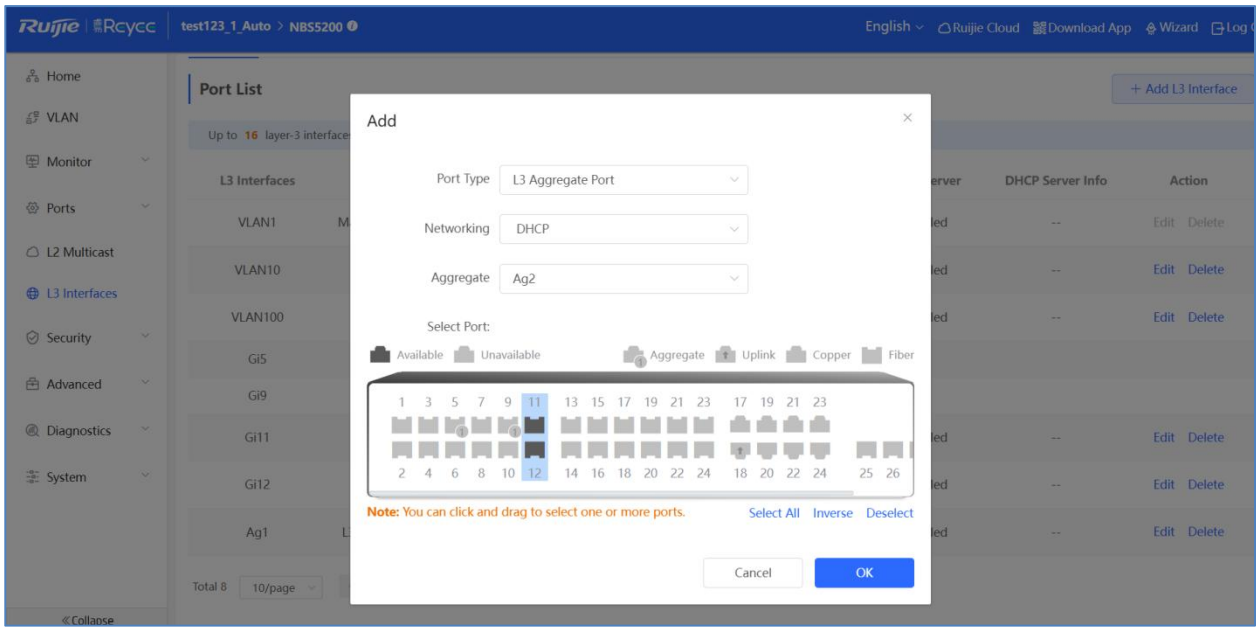
Set an aggregate port and select its member ports from the panel. Please configure its member ports as routed ports first.



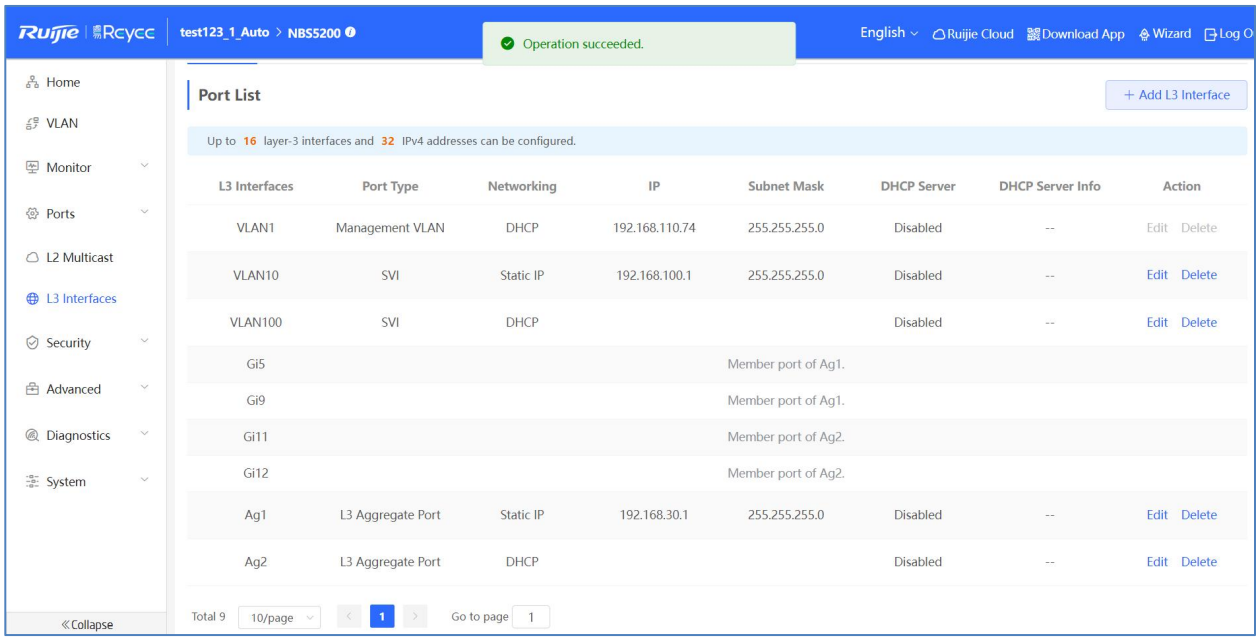
The message "Operation succeeded." is displayed, and the port list is updated.



If you select **DHCP**, the routed port will obtain the DHCP-assigned IP address.

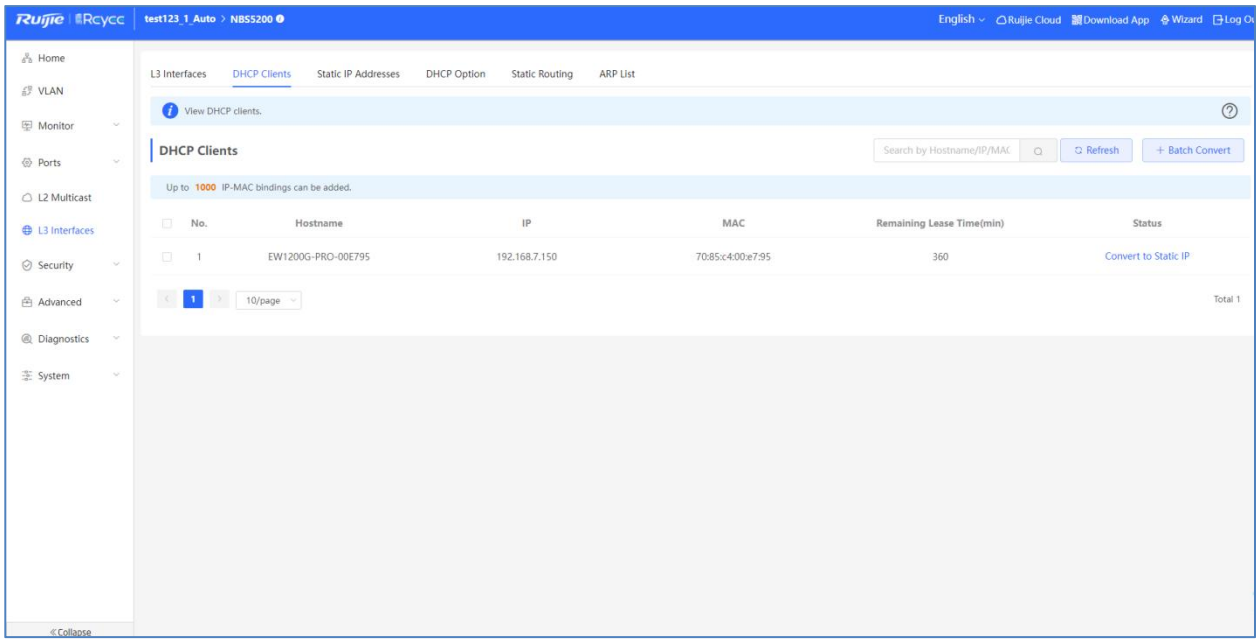


The message "Operation succeeded." is displayed, and the port list is updated.



4.3.4.2 DHCP Clients

You can view the dynamic IP addresses allocated by the DHCP server to the clients and convert dynamic IP addresses to static IP addresses on this page.



Hostname: The client hostname.

MAC: The client MAC address.

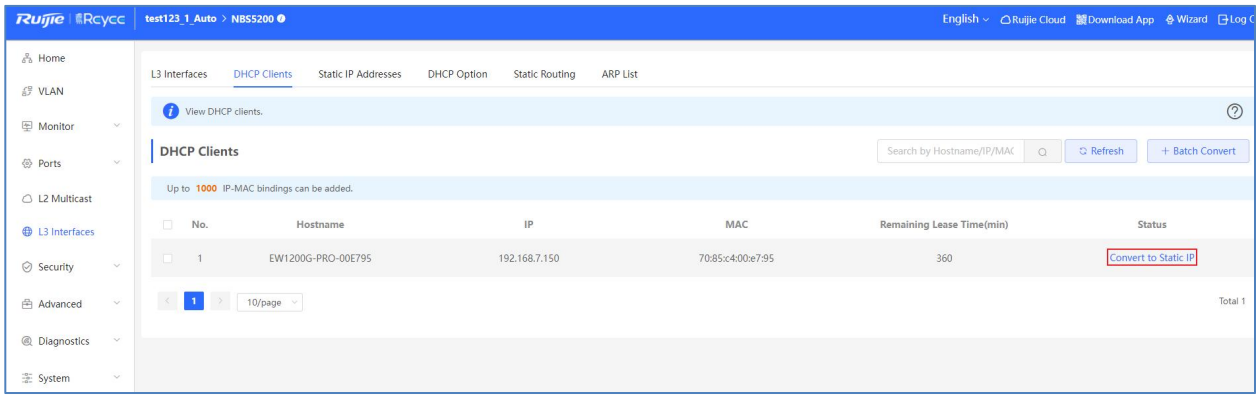
IP Address: The dynamic IP address allocated by the DHCP server to the client.

Remaining Lease Time: The remaining DHCP lease time. After the time expires, the client will obtain an IP address again.

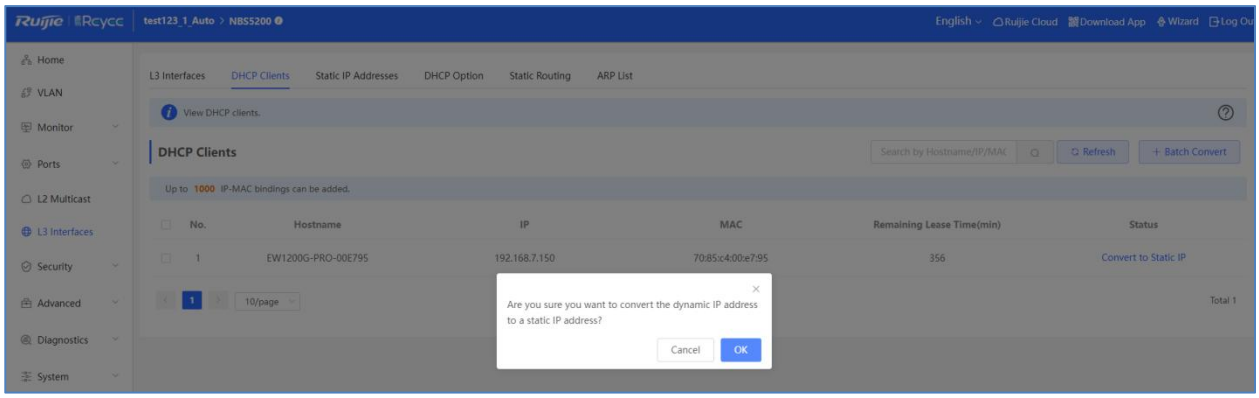
Refresh: Click **Refresh** to refresh the DHCP client list.

Convert to Static IP: Click **Convert to Static IP** to convert a dynamic IP address to a static IP address.

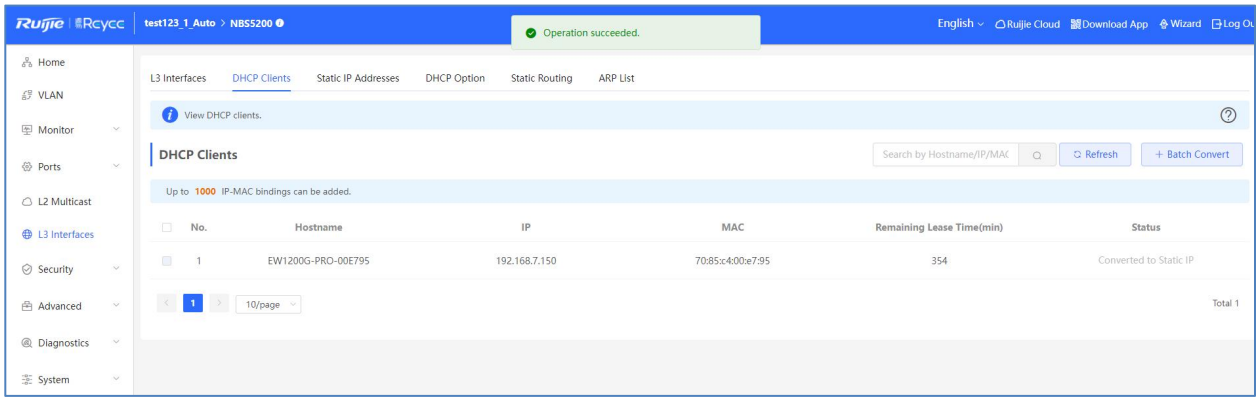
Click **Convert** or **Batch Convert** to convert a dynamic IP address to a **static IP** address.

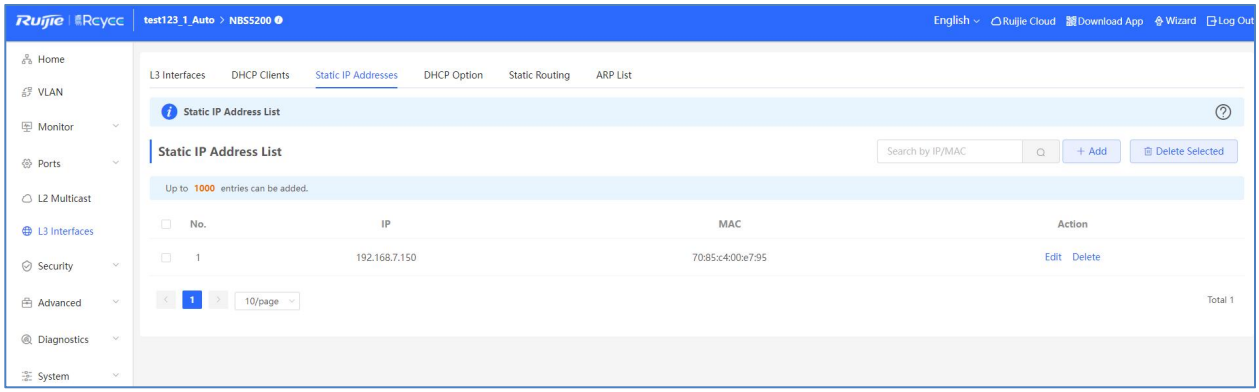


Click **OK** in the confirmation box.

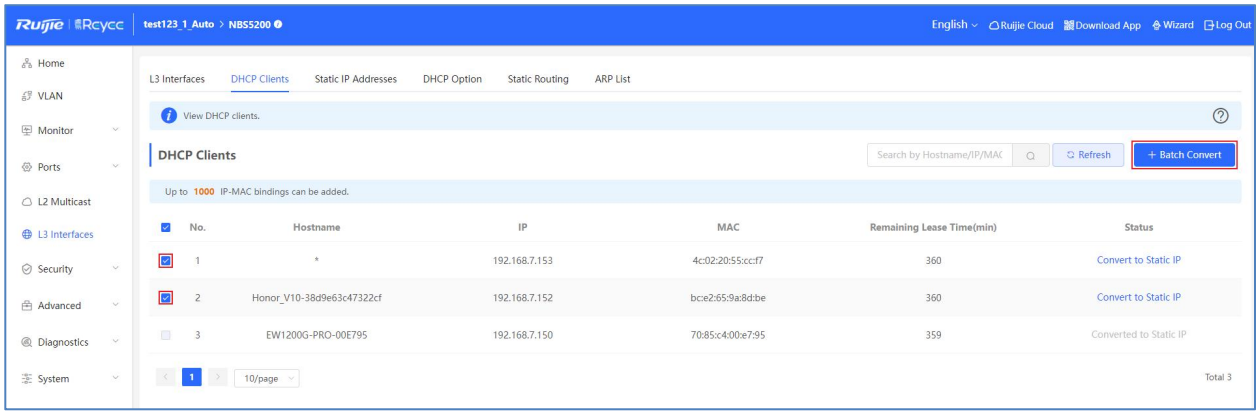


The message "Operation succeeded." is displayed, and the DHCP Clients list and Static IP Address List are updated.

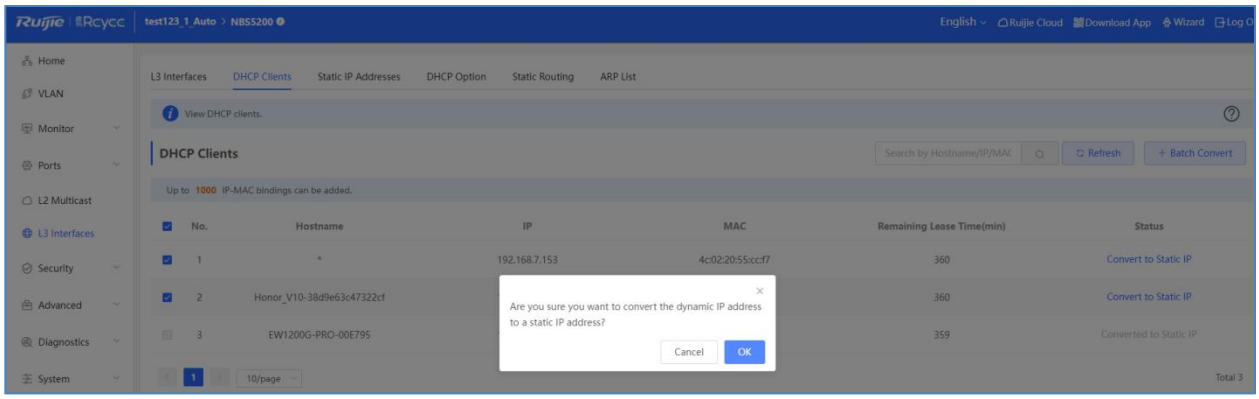




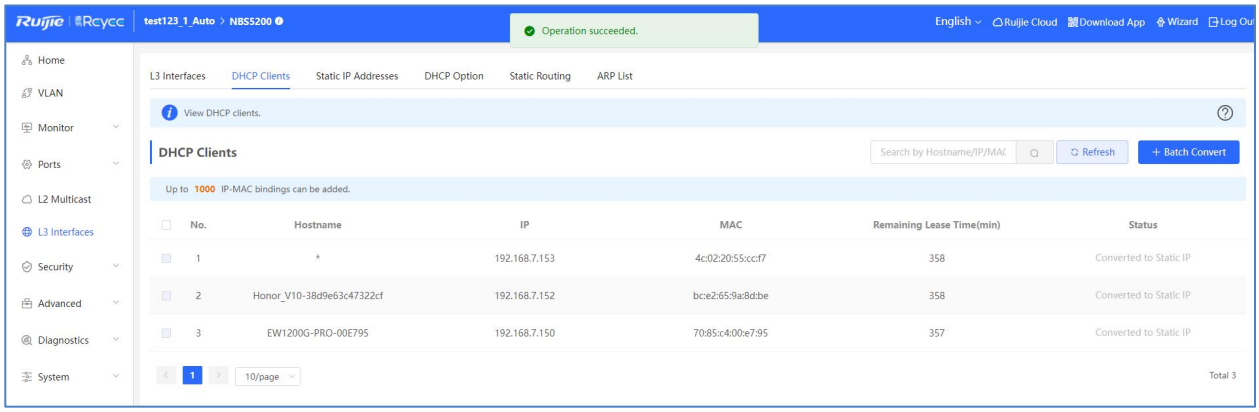
Click **Batch Convert** to convert **dynamic IP** addresses to **static IP** addresses.

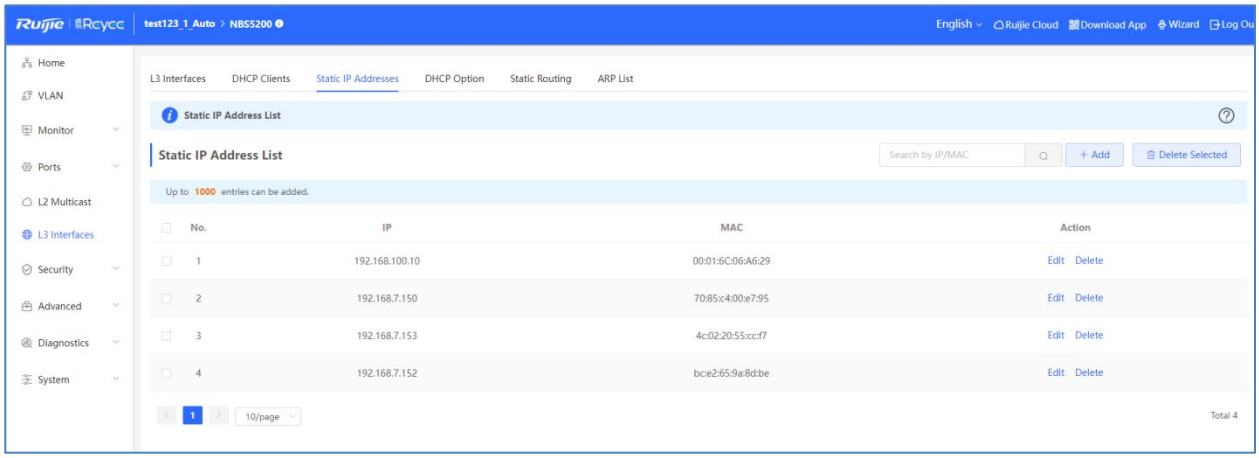


Click **OK** in the confirmation box.



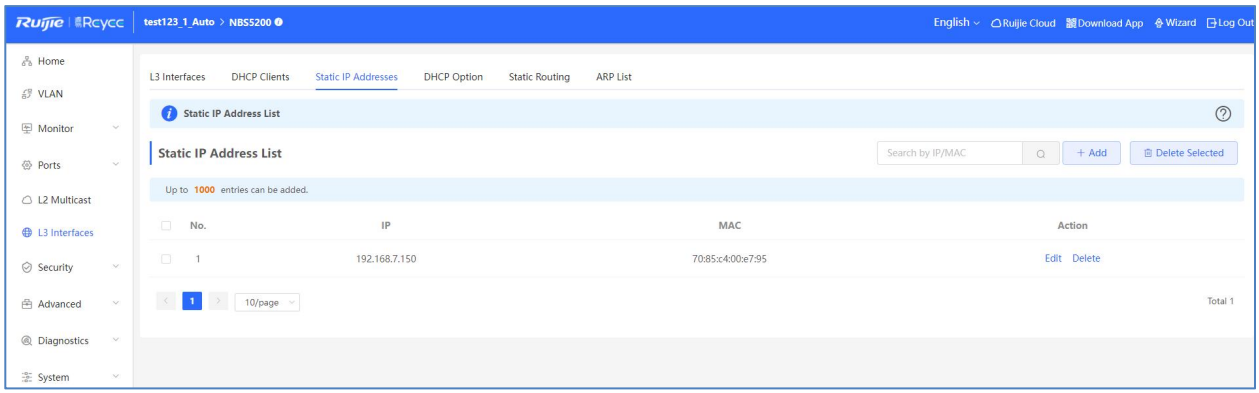
The message "Operation succeeded" is displayed, and the DHCP Clients list and Static IP Address List are updated.



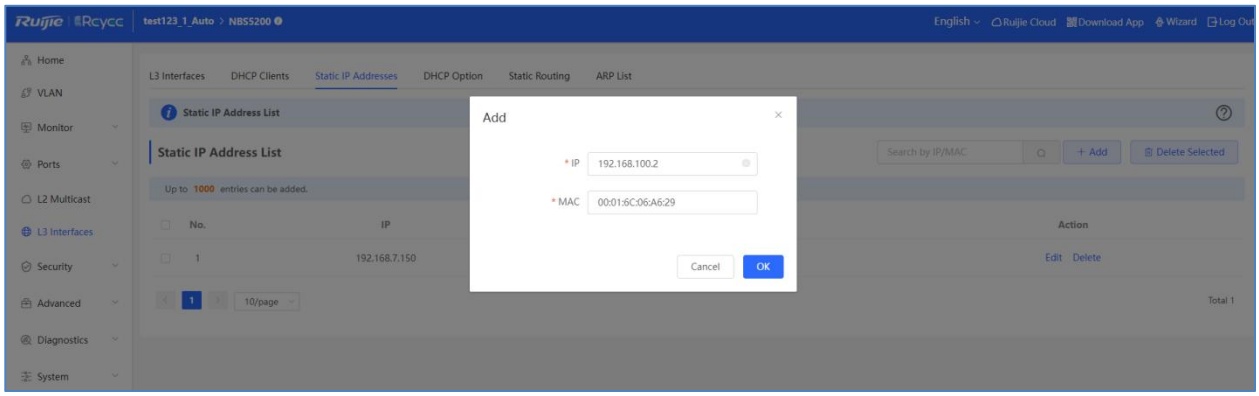


4.2.4.3 Static IP Addresses

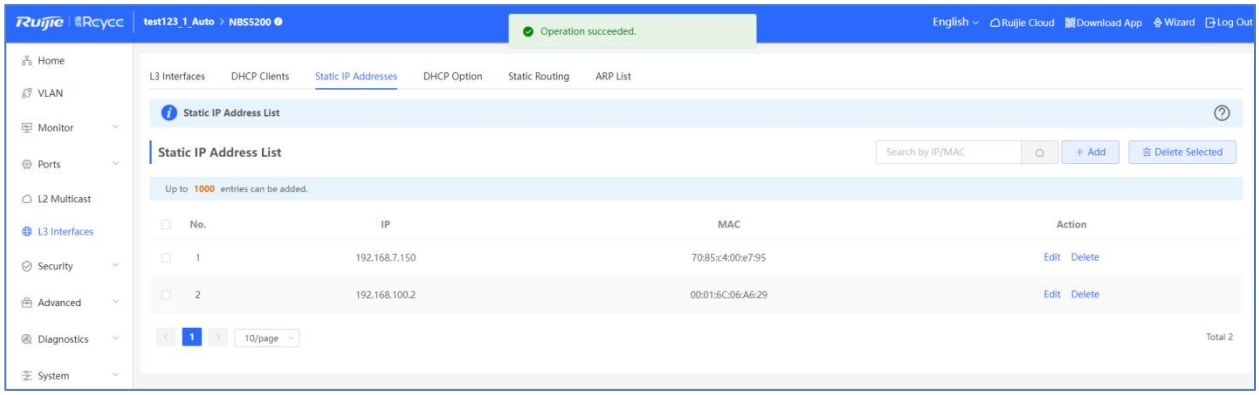
You can view and manage static IP addresses on this page.



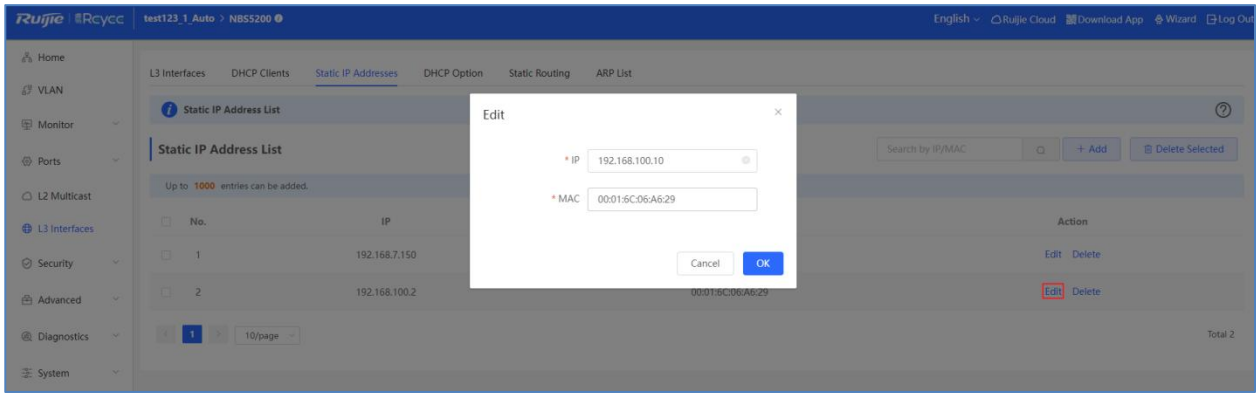
Click **Add.** In the displayed dialog box, you can set a static IP address.



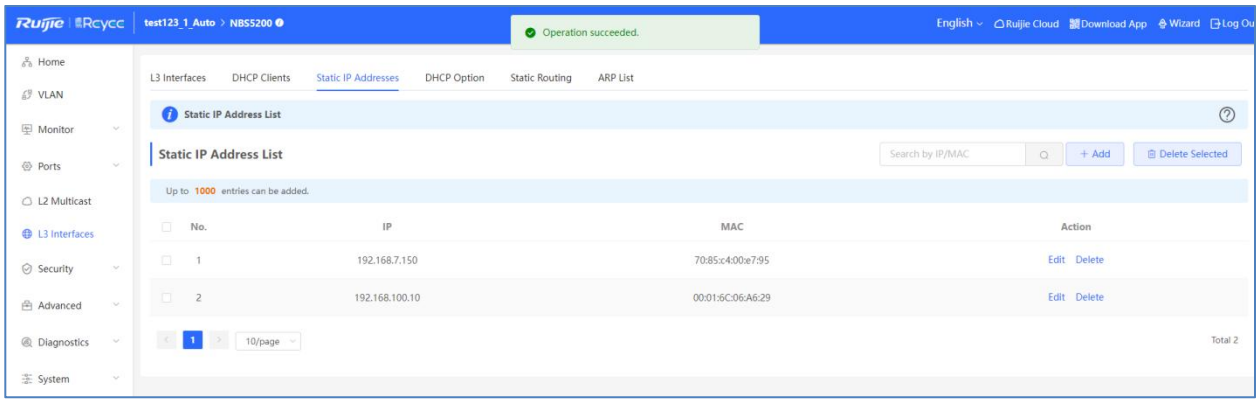
The message "Operation succeeded." is displayed, and the static IP address list is updated.



Click **Edit.** In the displayed dialog box, you can modify a static IP address.

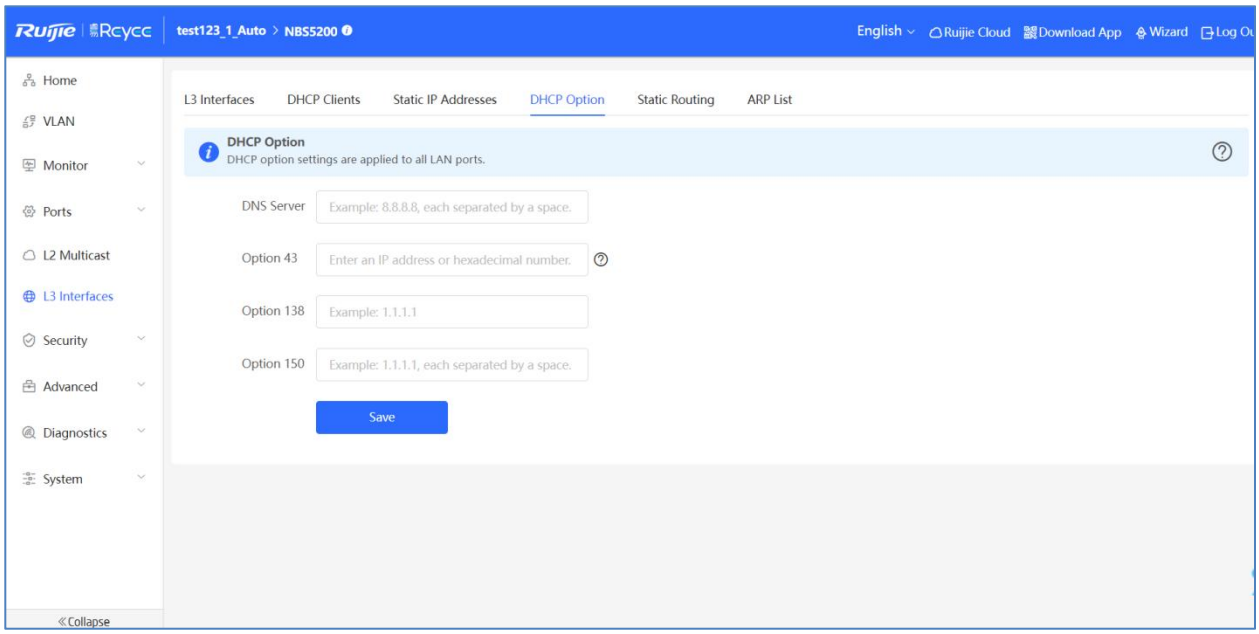


The message "Operation succeeded." is displayed, and the port list is updated.



4.2.4.4 DHCP Option

DHCP option settings are applied to all LAN ports.



DNS Server: (Optional) Set a DNS server address provided by the ISP.

Option 43: (Optional) There are two formats available:

IP addresses, each separated by a space.

A hexadecimal string. Example: 01:C0:A8:01:01.

Option 138: (Optional) Enter the IP address of the wireless controller.

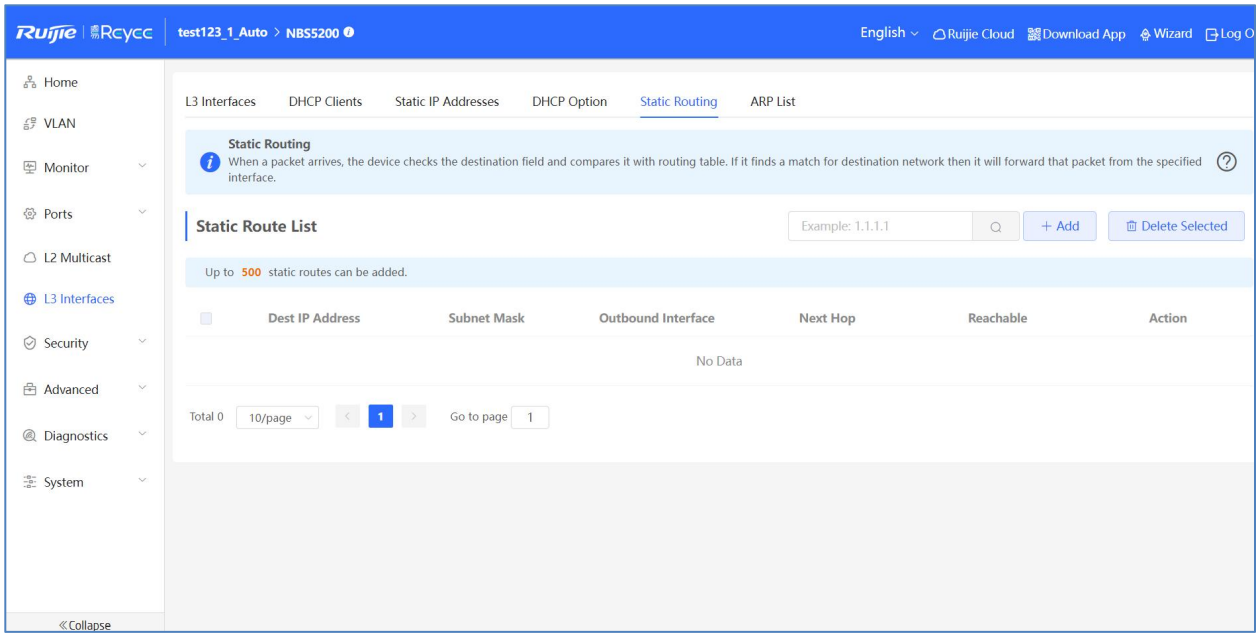
Option 150: (Optional) Enter the IP address of the TFTP server.

4.3.4.5 Static Routing

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

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

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



Dest IP Address/Subnet Mask: Set a destination IP address and a subnet mask.

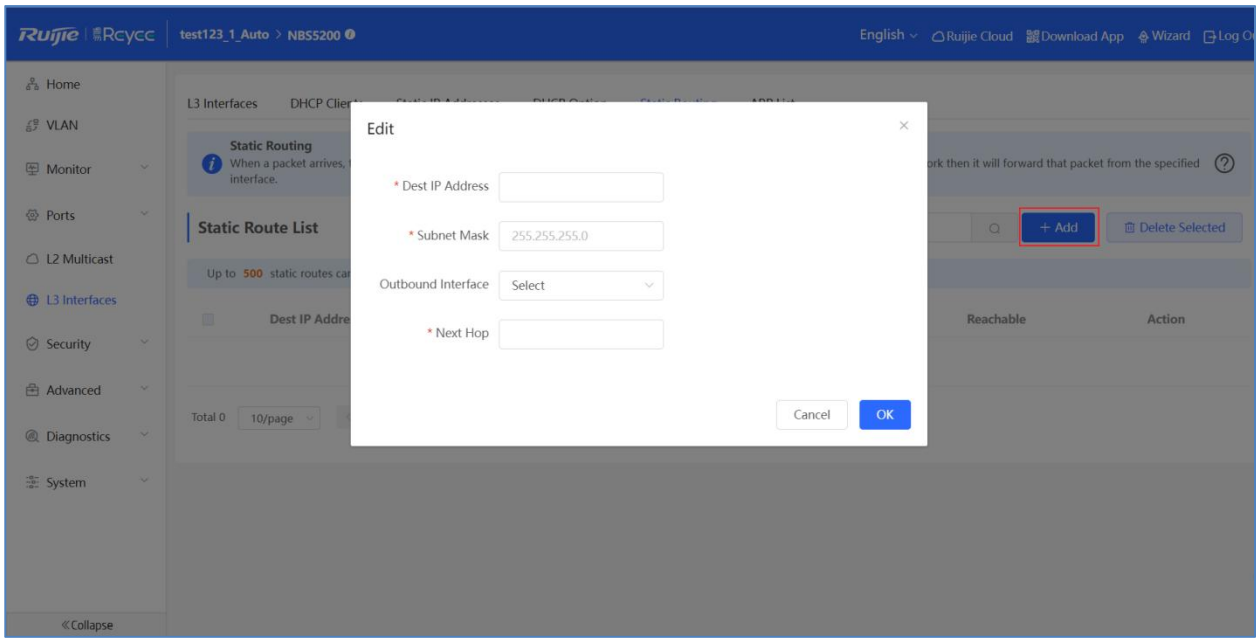
Outbound Interface: Select an interface which packets are routed over.

Next Hop: Set a next hop. If the outbound interface is PPPoE, the next hop is not required.

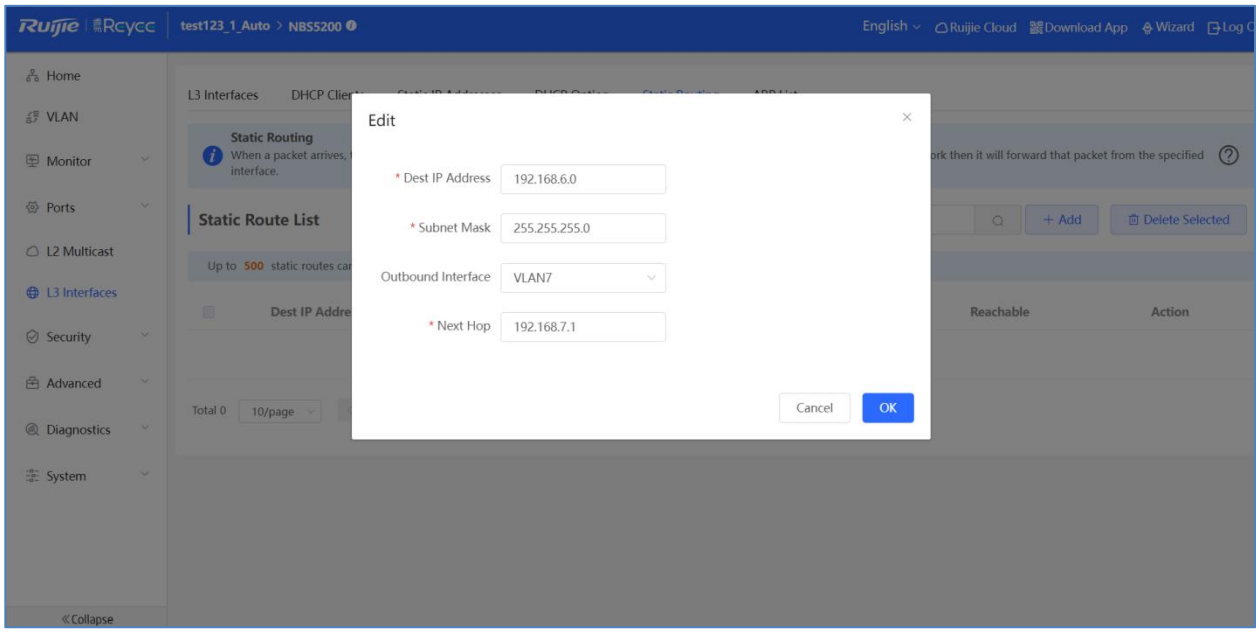
Reachable: Whether the next hop is reachable.

1.1 Add a Generic Static Route

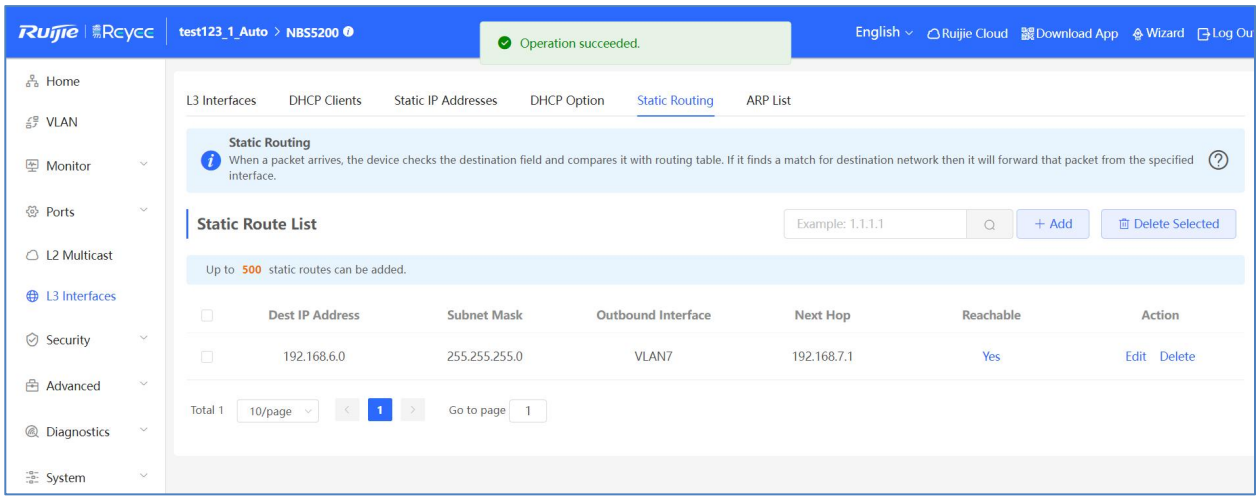
Click **Add.** In the displayed dialog box, you can set a Generic Static Route.



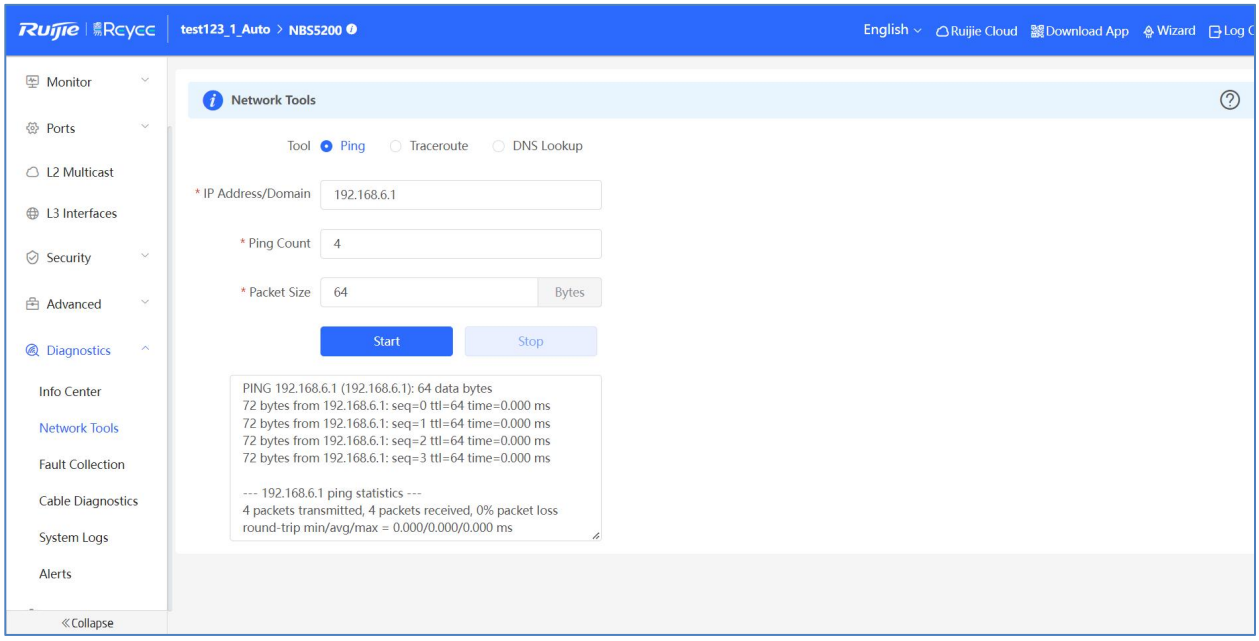
Specify the destination IP address and subnet mask, select an outbound interface from the Outbound Interface dropdown list, set a next hop address. If the outbound interface is enabled with PPPoE, the next hop address is not required.



Click **OK**. The message "Operation succeeded" is displayed, and the static route list is updated.



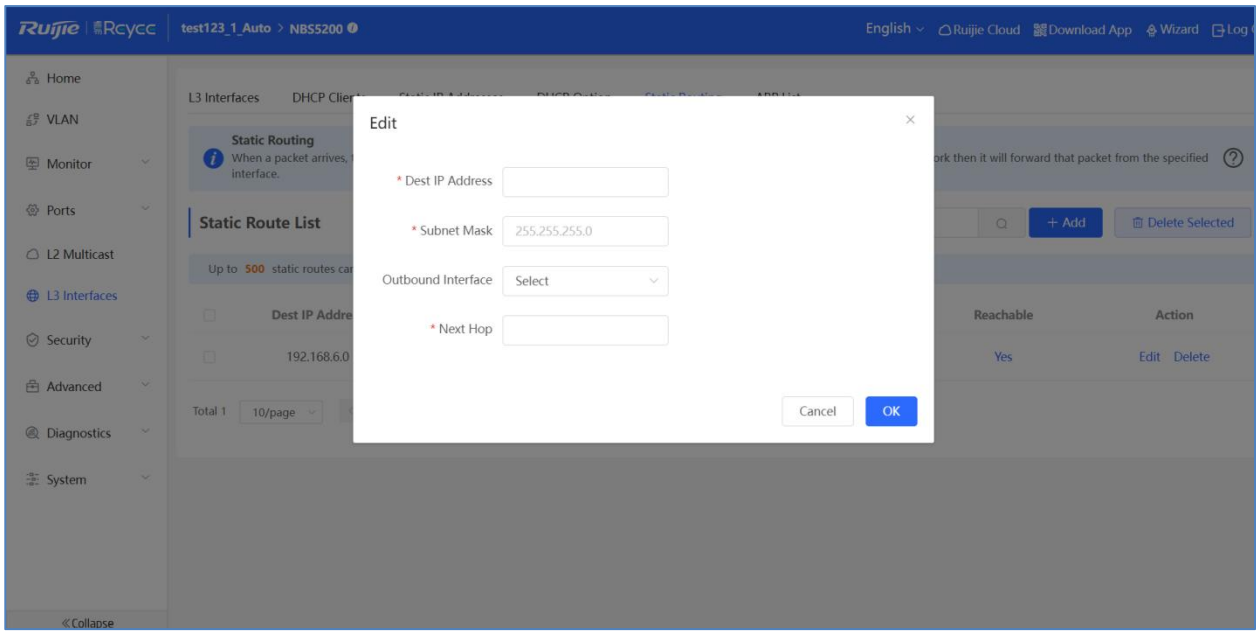
Ping test:



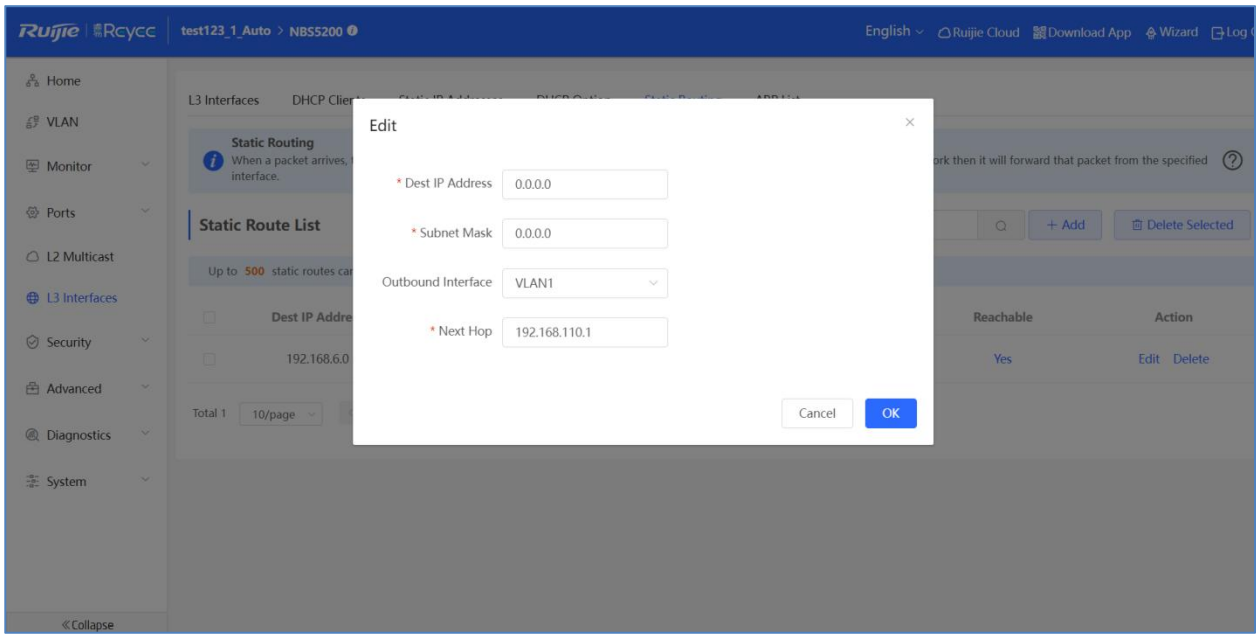
1.2 Add a Default Static Route

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

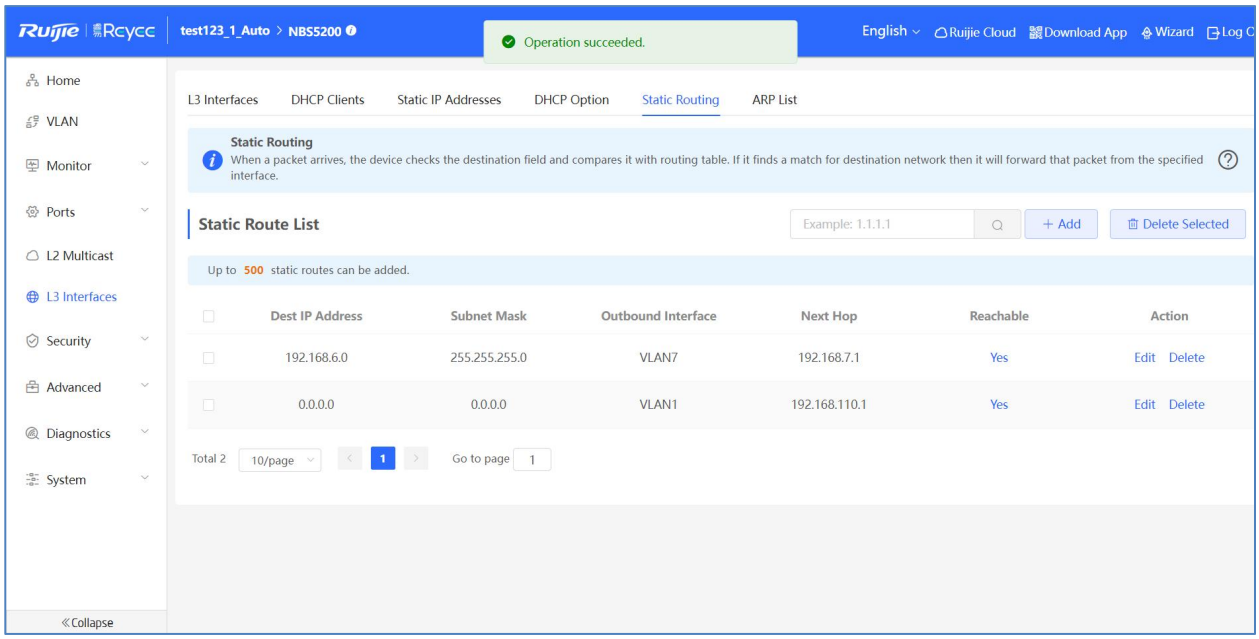
Click **Add.** In the displayed dialog box, you can set the Default Static Route.



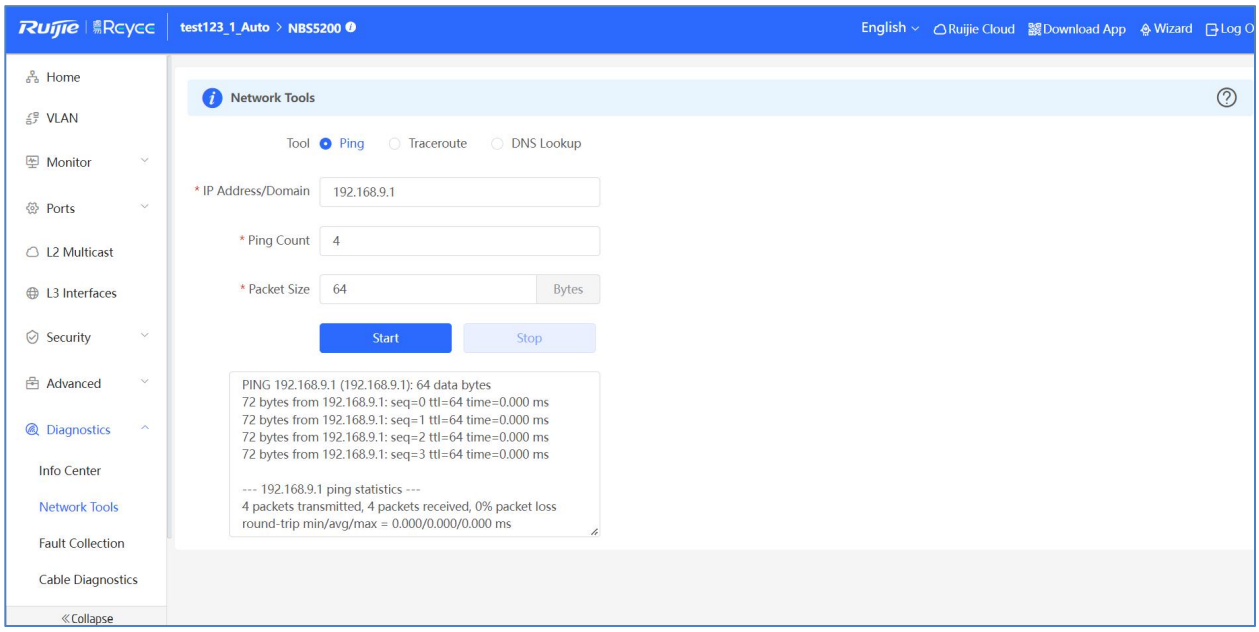
Set both the destination IP address and the subnet mask to all 0s, then set a next hop address.



Click **OK**. The message "Operation succeeded." is displayed, and the static route list is updated.



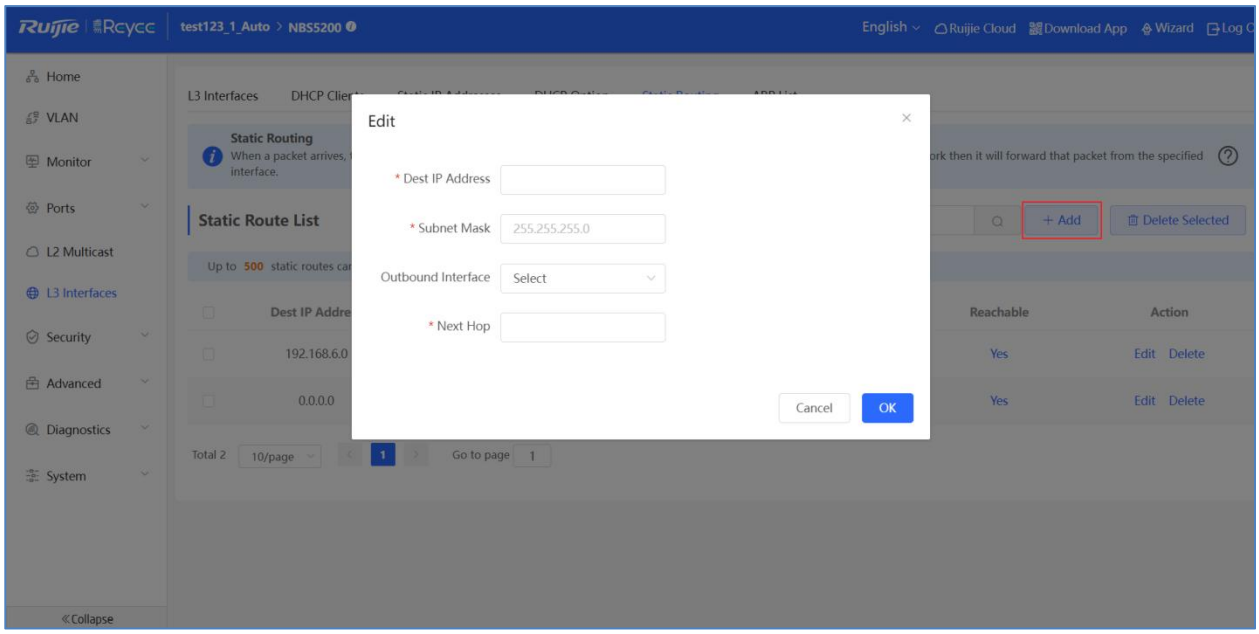
Ping test:



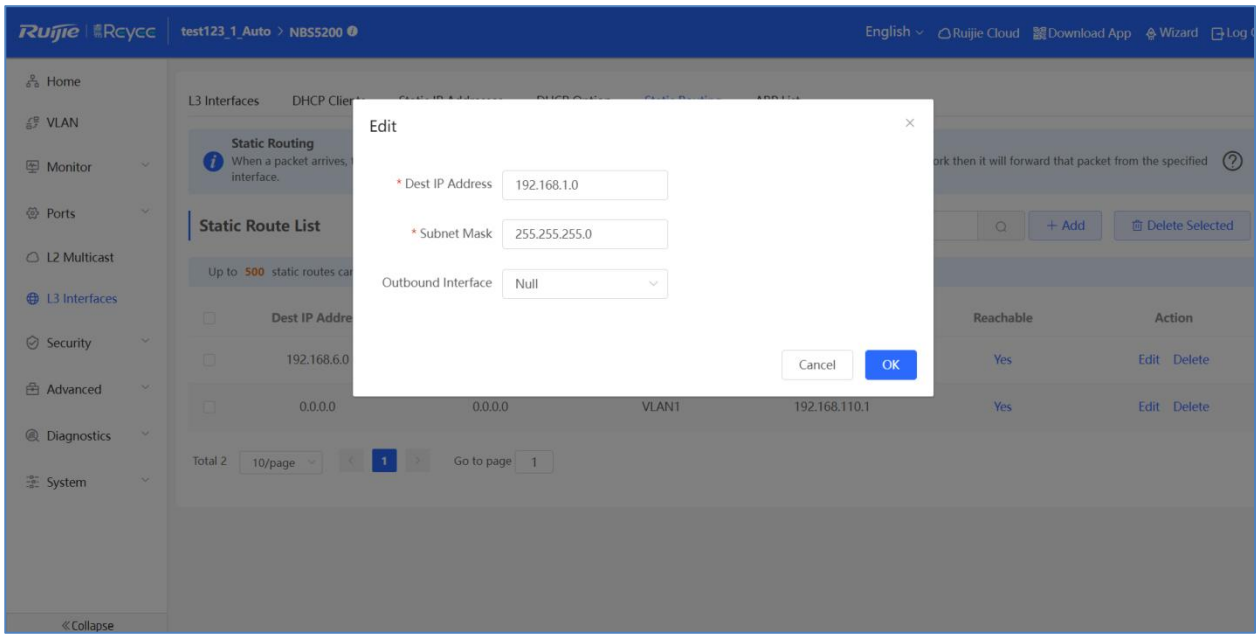
1.3 Add a Static Blackhole Route

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

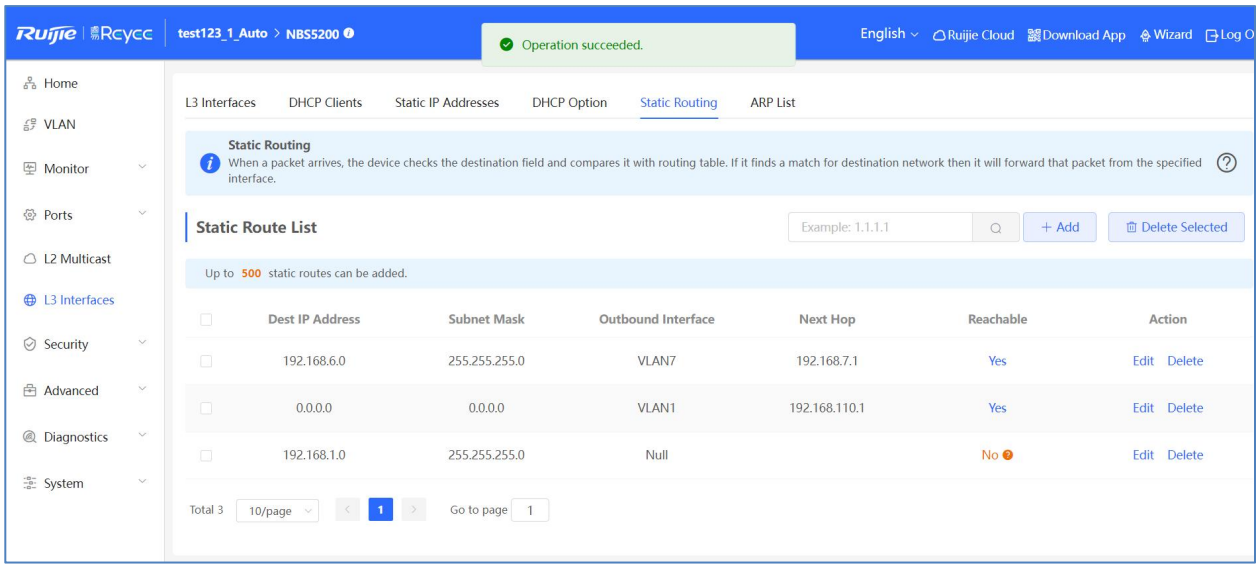
Click **Add.** In the displayed dialog box, you can set a Static Blackhole Route.



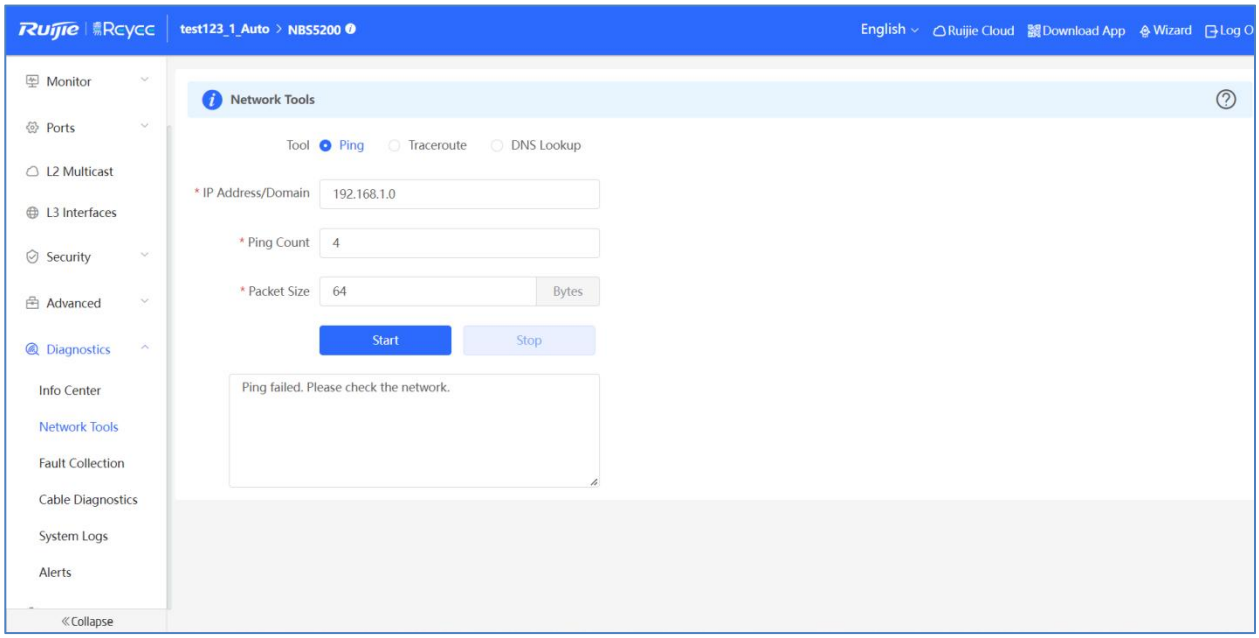
Specify the destination IP address and a subnet mask, select **Null** from the **Outbound Interface** dropdown list.



Click **OK**. The message "Operation succeeded." is displayed, and the static route list is updated.

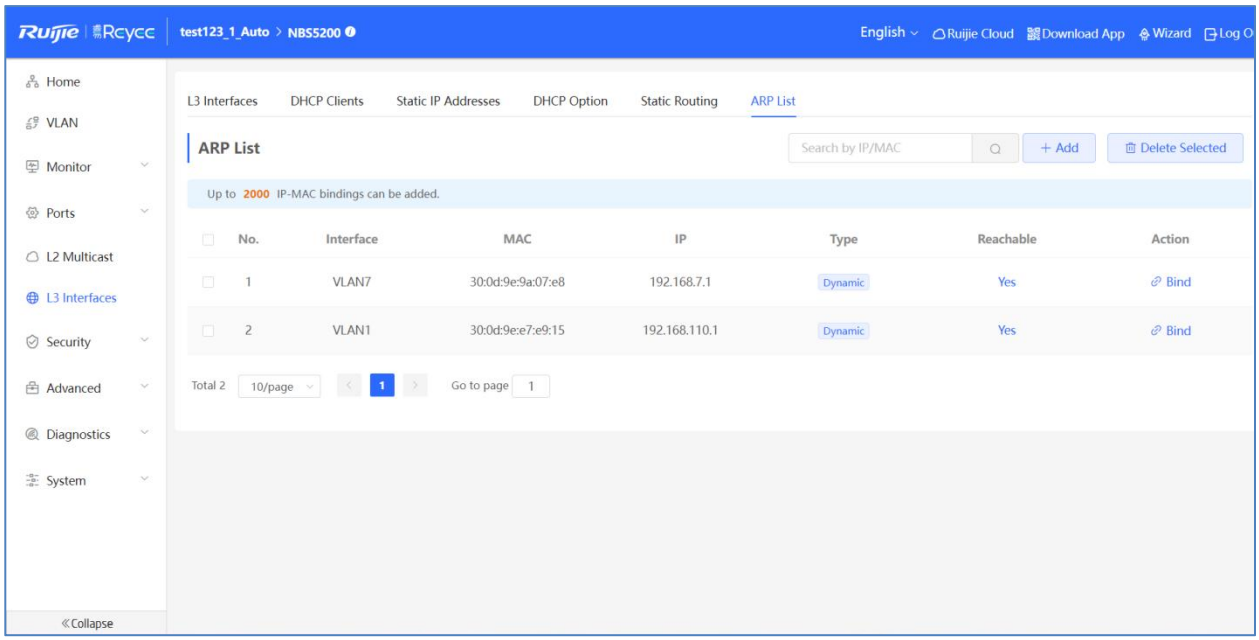


Ping test:

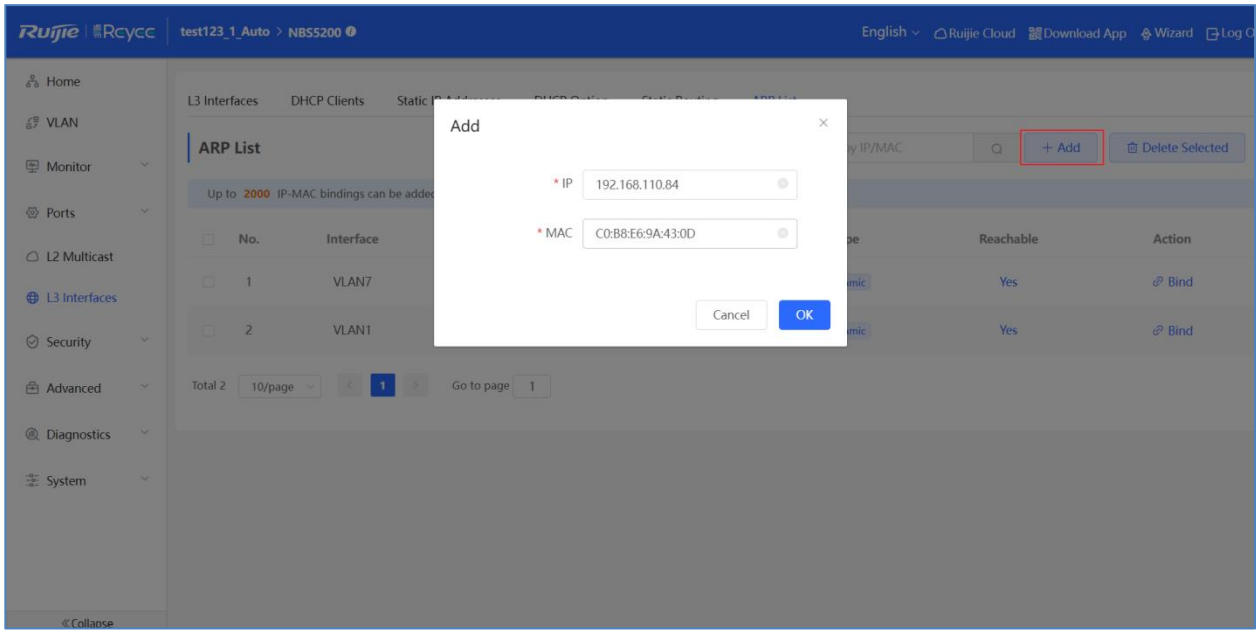


4.3.4.6 ARP List

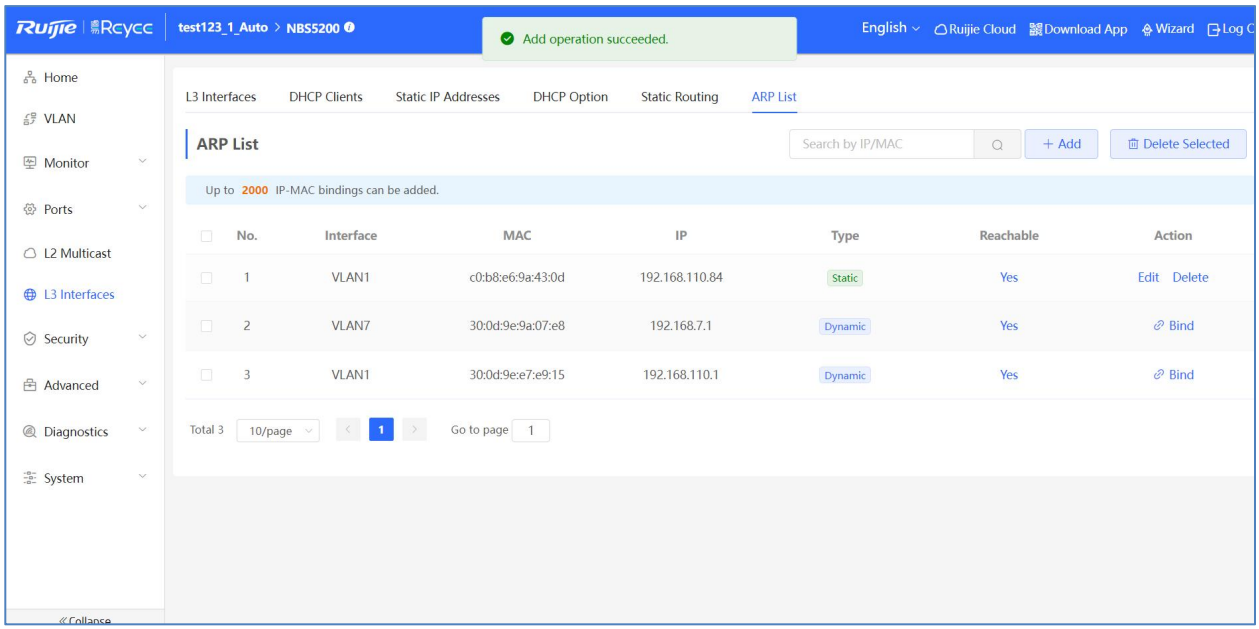
The **ARP List** module displays all static and dynamic ARP entries.



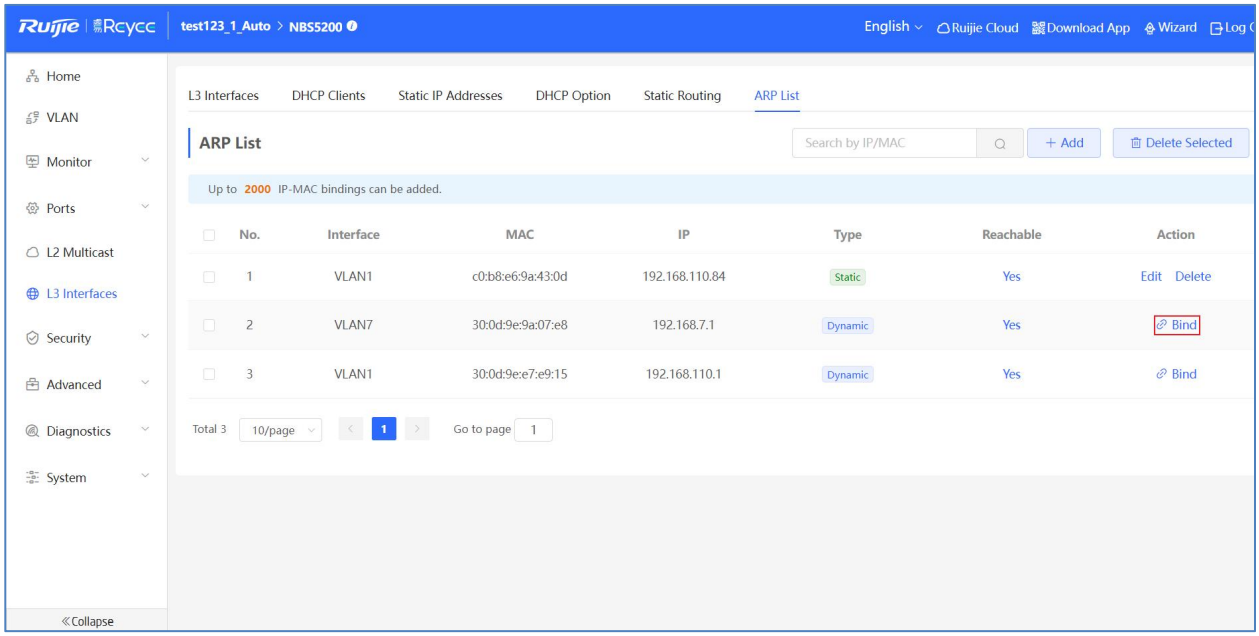
Click **Add,** you can add a static ARP entry.



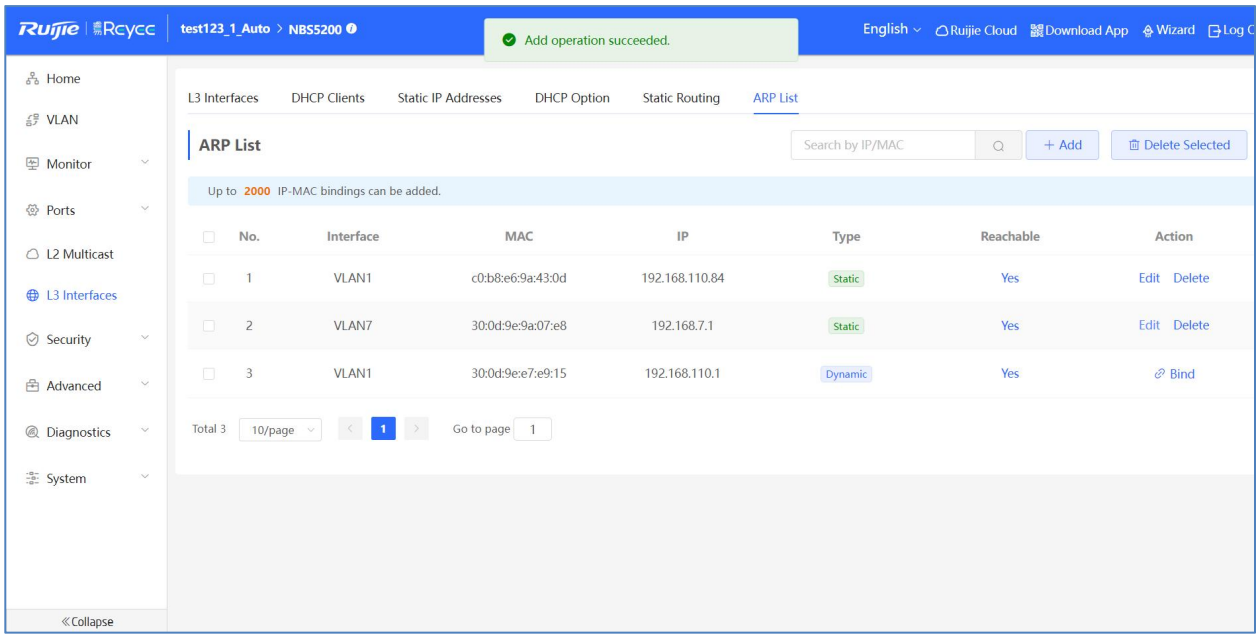
Click **OK.** The message "Operation succeeded." is displayed, and the ARP list is updated.



Click **Bind,** you can bind a **dynamic** ARP entry to a **static** ARP entry.



The message "Operation succeeded." is displayed, and the ARP list is updated.

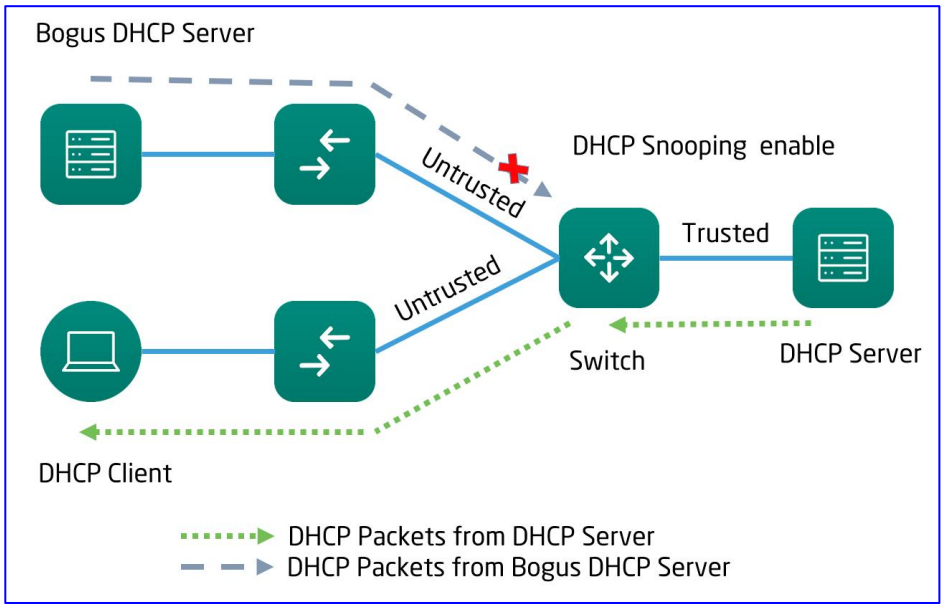


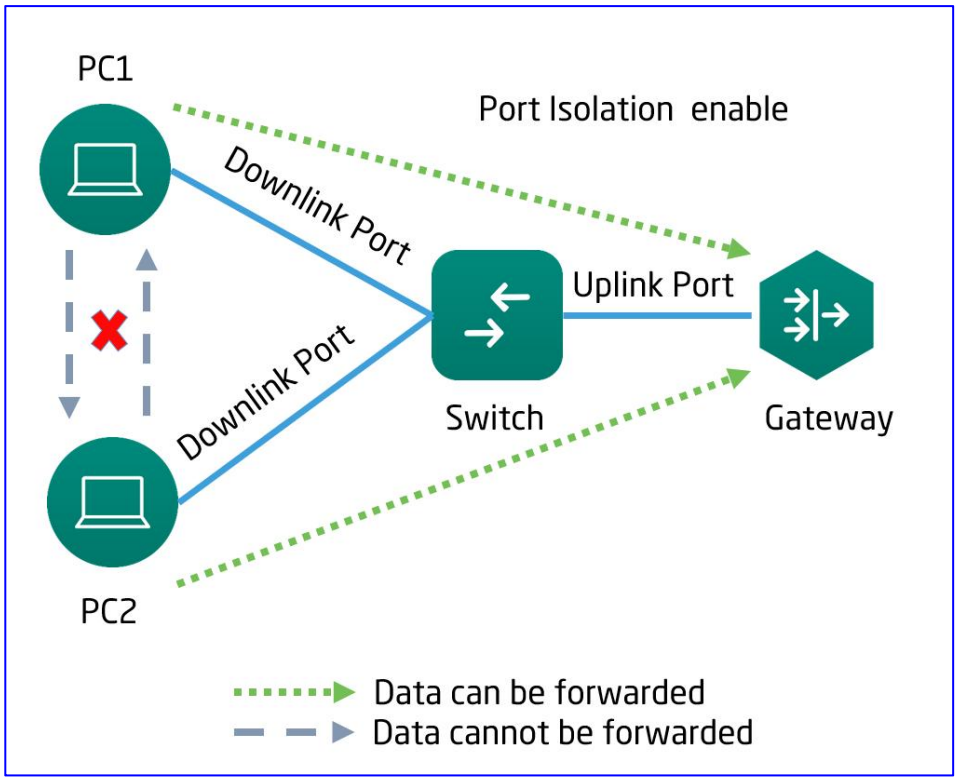
4.3.5 Security

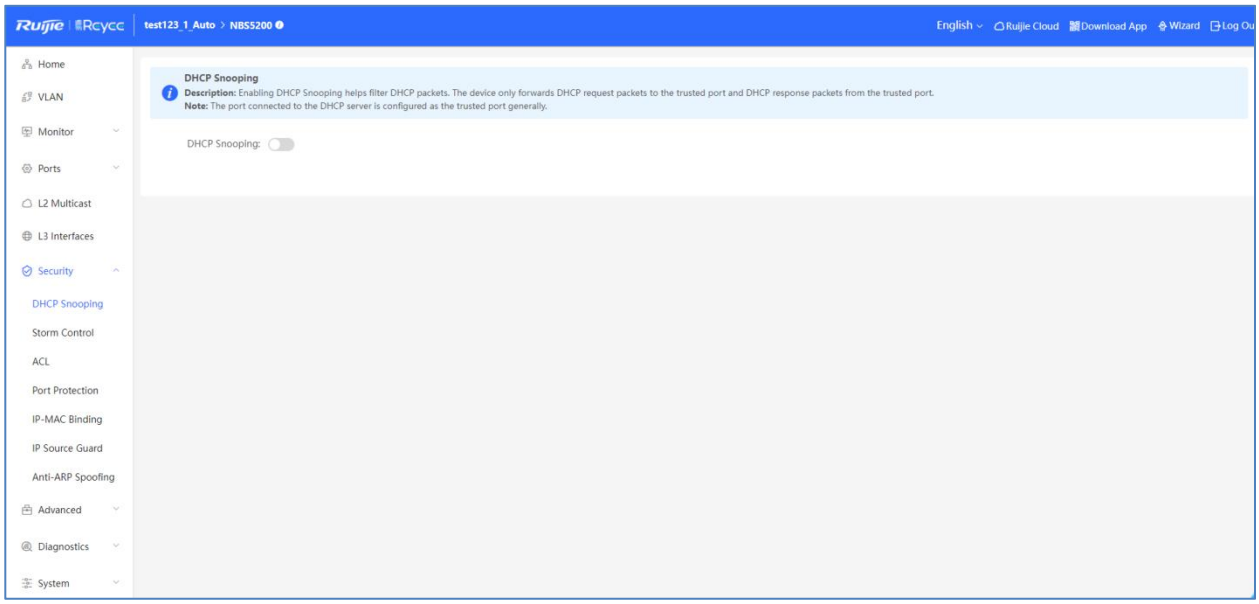
The **Security** module includes **DHCP Snooping**, **Storm Control**, **ACL**, **Port Protection**, **IP-MAC Binding**, **IP Source Guard** and **Anti-ARP Spoofing**.

4.3.5.1 DHCP Snooping

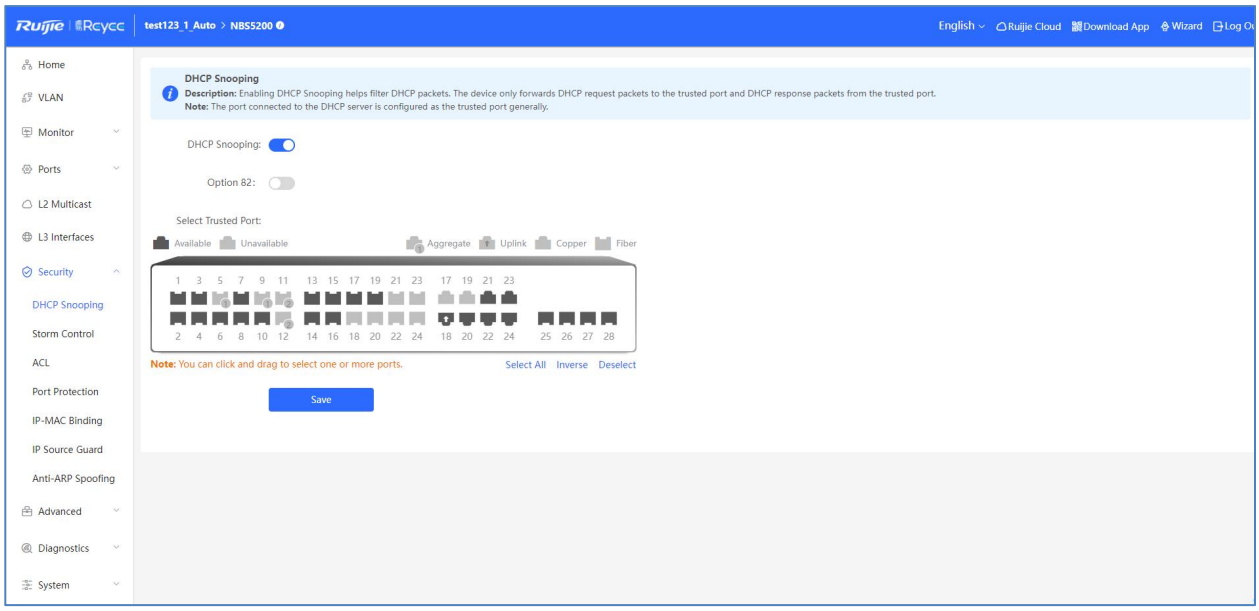
The DHCP Snooping module allows snooping the DHCP packets exchanged between clients and servers to record and monitor IP addresses of users. It also allows filtering invalid DHCP packets, including request packets from clients and response packets from servers. User data based on DHCP Snooping serves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







Click the **DHCP Snooping** toggle to enable or disable DHCP snooping.



After DHCP snooping is enabled, set trusted ports, and click **Save.**

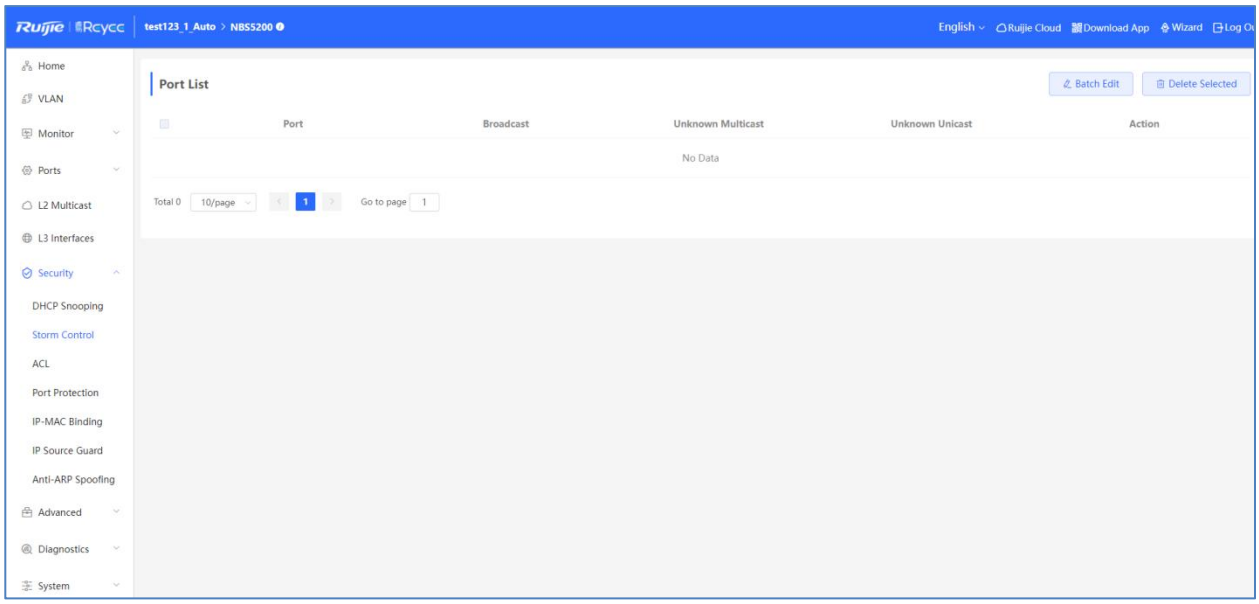
Enabling DHCP Snooping helps filter DHCP packets. The device only forwards DHCP request packets to the trusted port and DHCP response packets from the trusted port.

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

4.3.5.2 Storm Control

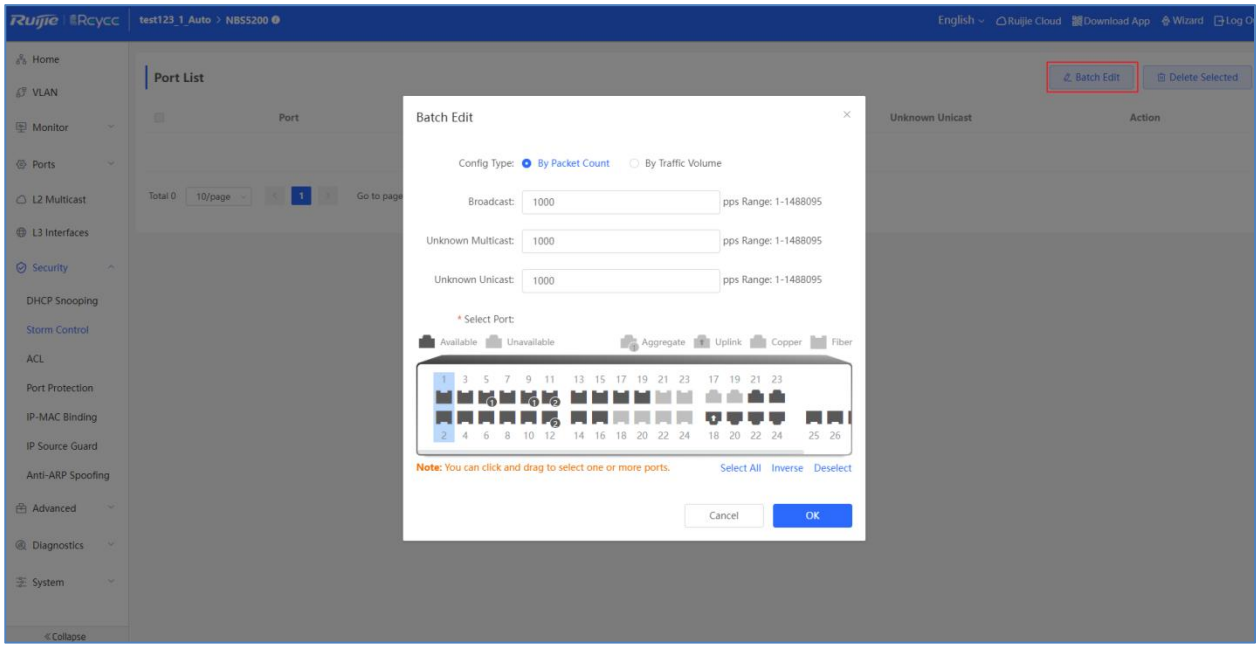
When there are excessive broadcast, multicast or unknown unicast data flows in the LANs, the network speed decreases and packet transmission timeout greatly increases. This is called LAN storm, which may be caused by topology protocol execution errors or incorrect network configuration.

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



Batch adding ports/Adding a single port

Click **Batch Edit.** In the displayed dialog box, select ports, enter the broadcast, unknown multicast, and unknown unicast rate limits, and click **OK.**

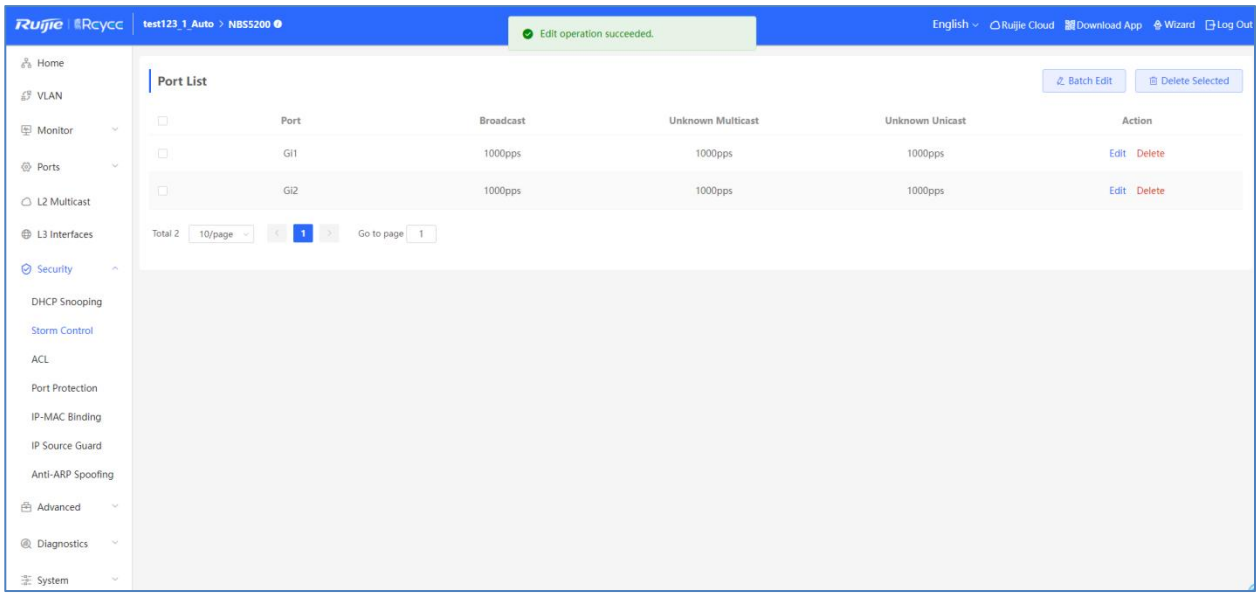


Broadcast: the package consisting of Fbased on MAC address.

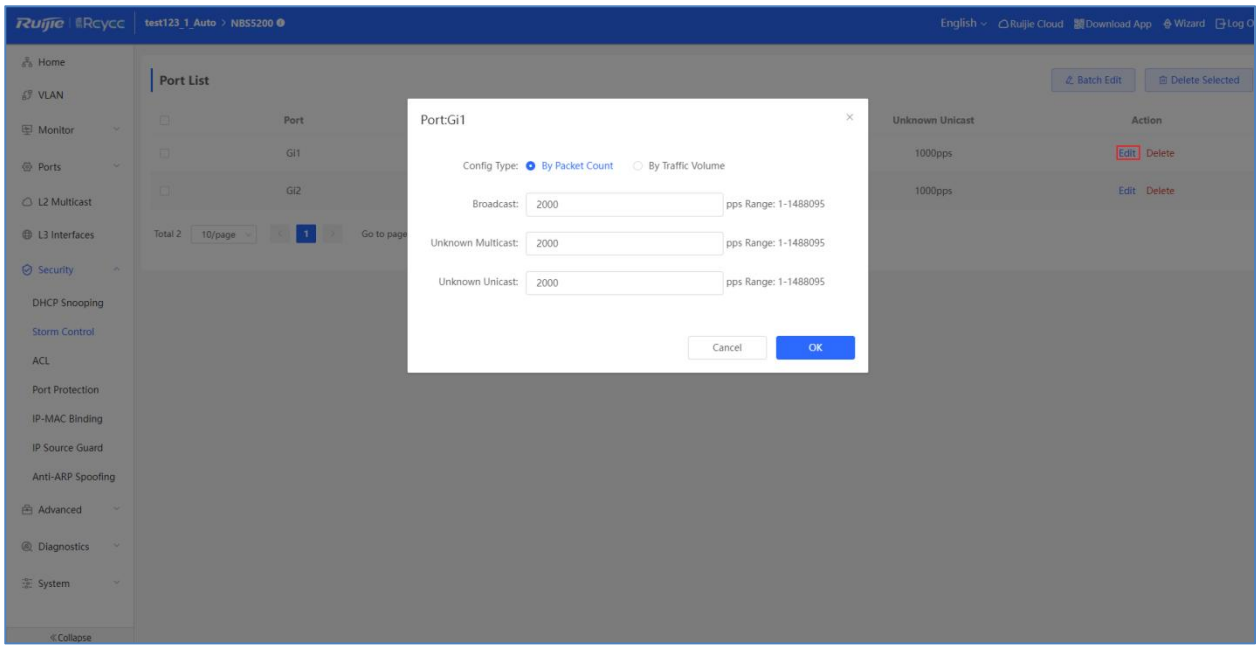
Unknown multicast: Unconventional multicast

Unknown unicast: The unicast packetof its source MAC not being in MAC address table.

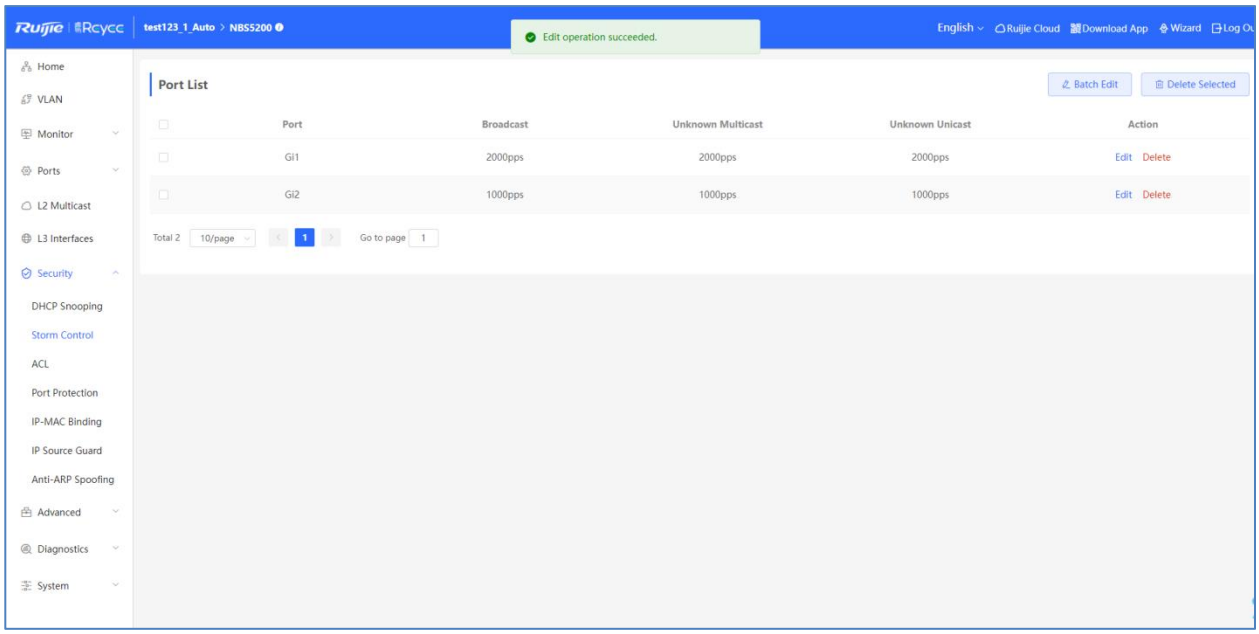
A message "Operation succeeded." is displayed, and the port list is updated.



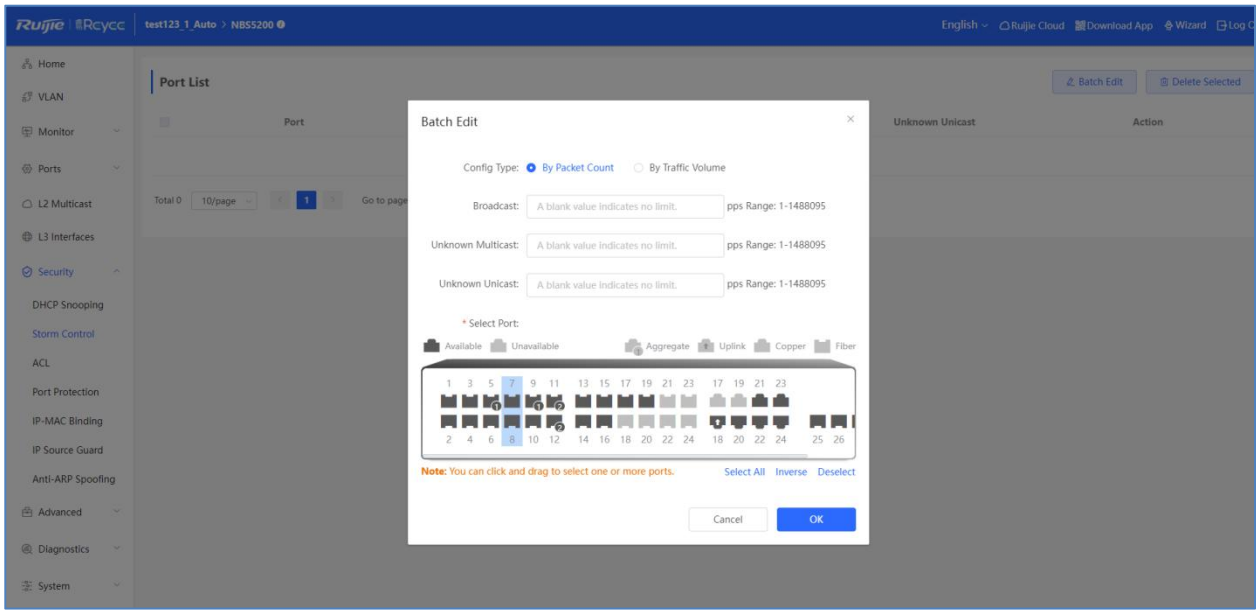
Click **Edit** in the **Action** column of Port List. In the displayed dialog box, enter the broadcast, unknown unicast, and unknown multicast rate limits, and click **OK.**



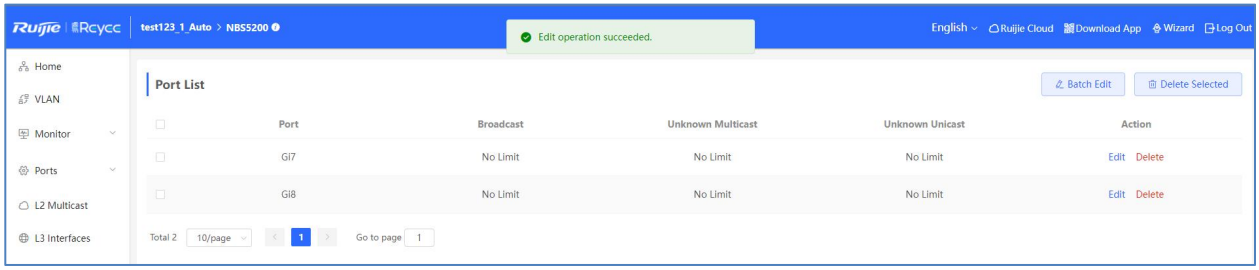
A message "Operation succeeded." is displayed, and the port list is updated.



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

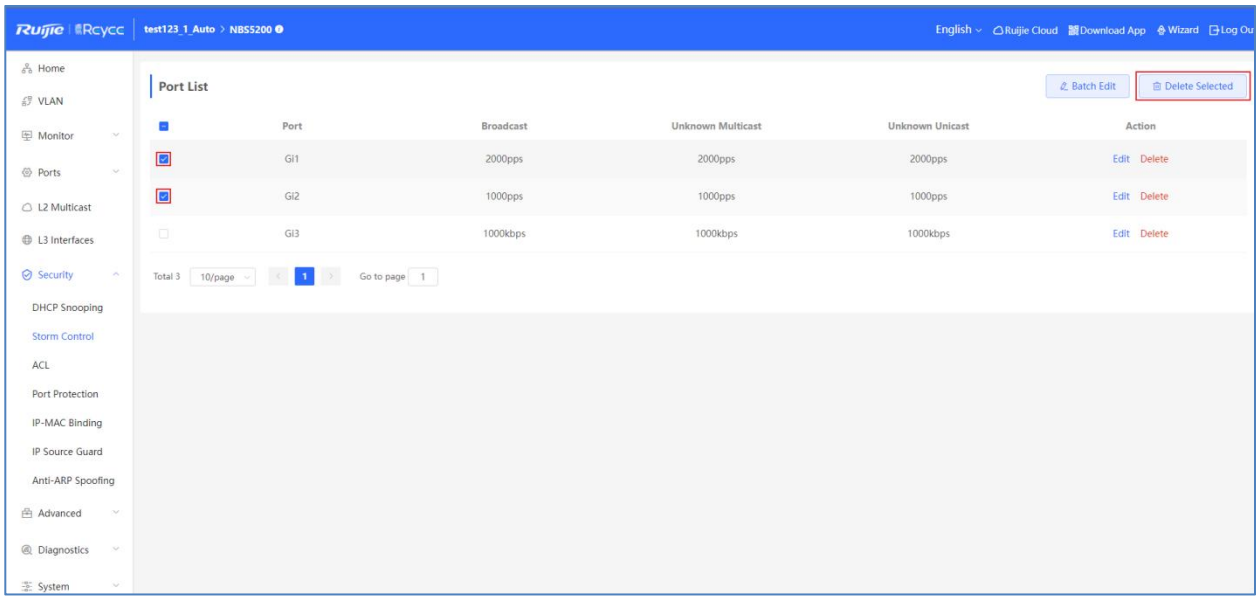


A message "Edit operation succeeded." is displayed, and the port list is updated.

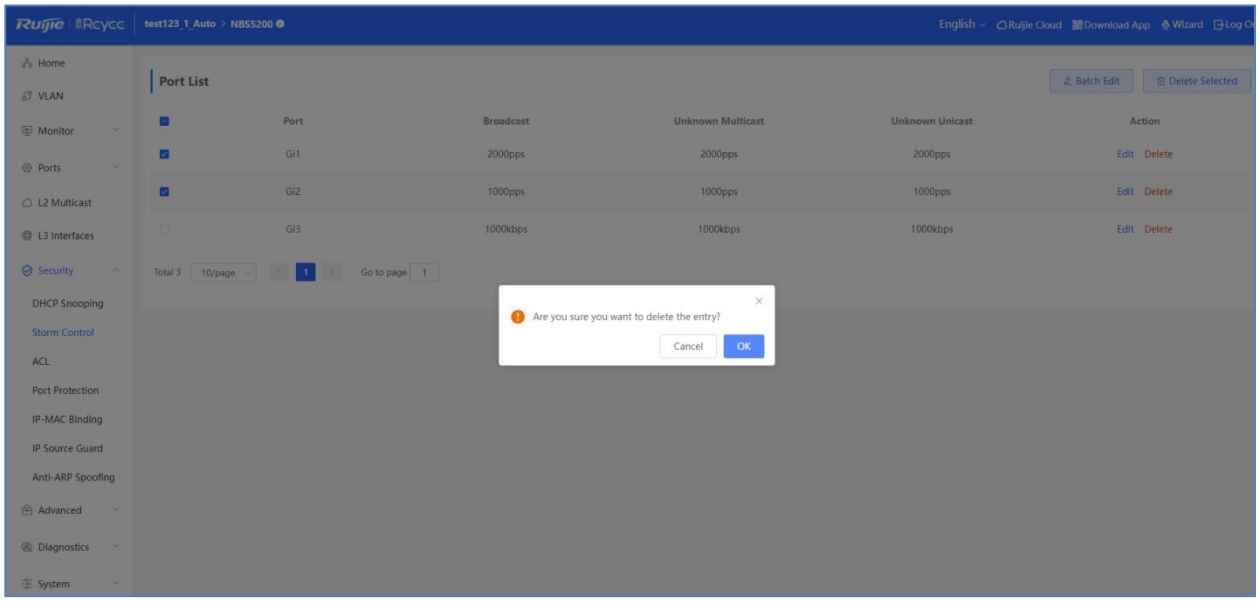


Batch deleting ports/Deleting a single port for storm control

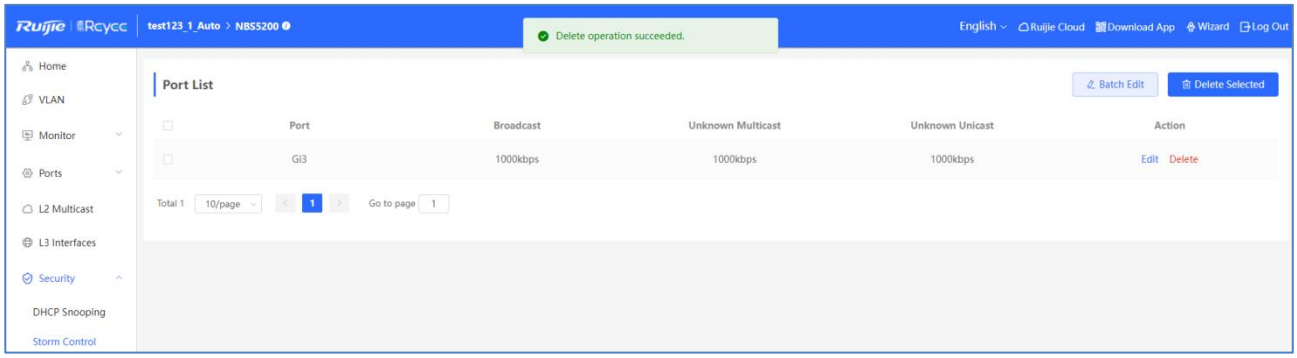
Select multiple entries in **Port List** and click **Delete Selected.**



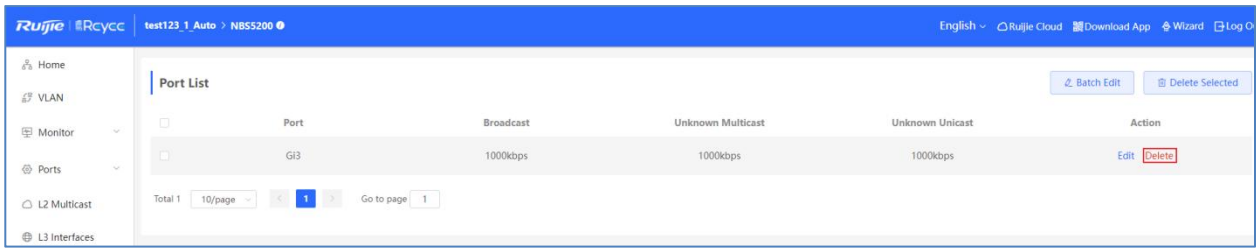
In the displayed confirmation box, click **OK.**



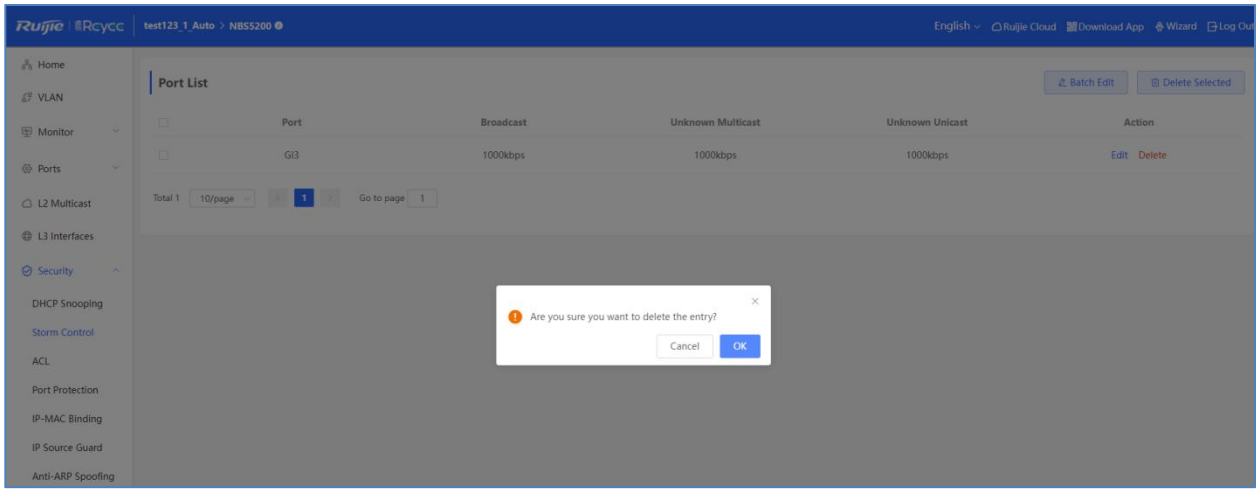
A message "Delete operation succeeded." is displayed, and the port list is updated.



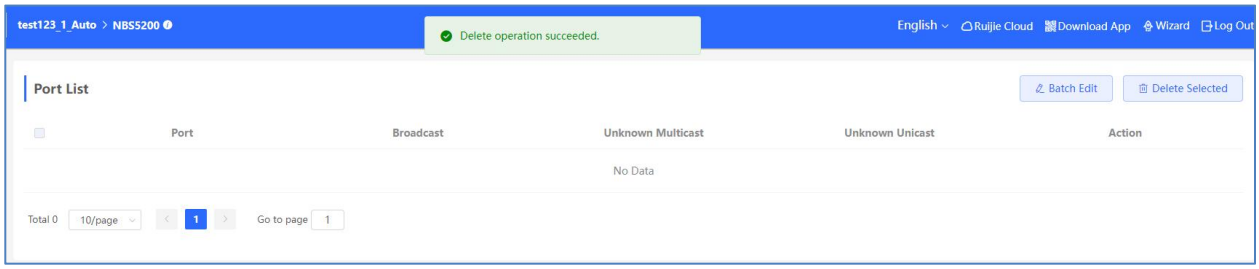
Click **Delete** in the **Action** column.



In the displayed confirmation box, click **OK**.



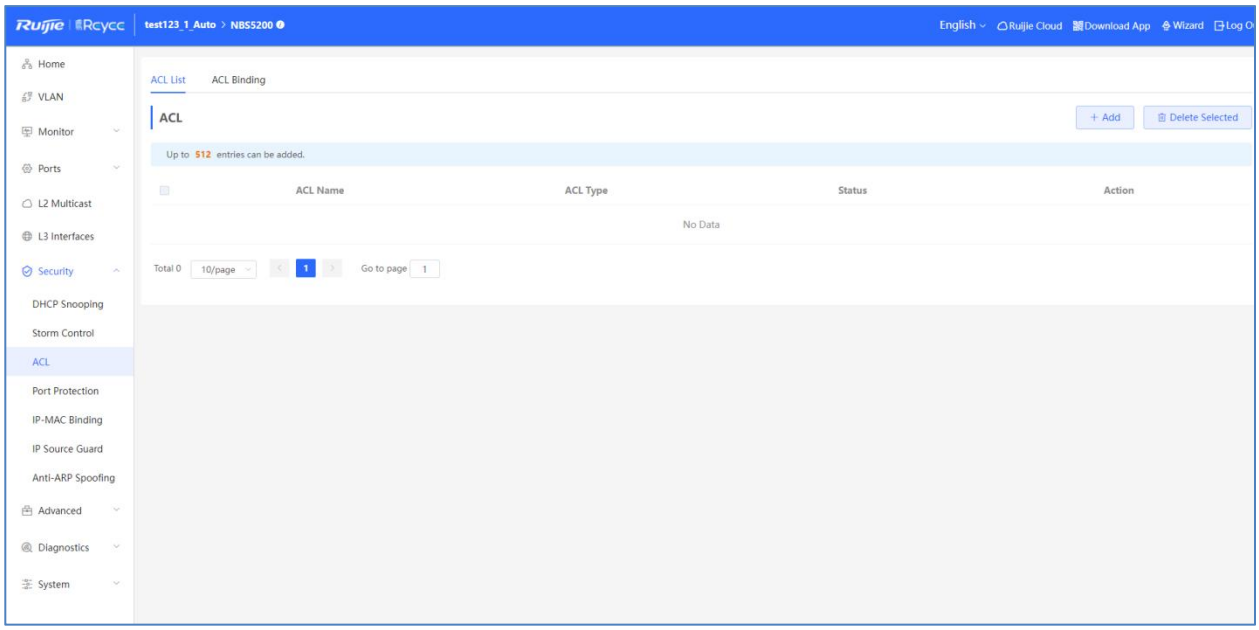
A message "Delete operation succeeded." is displayed, and the port list is updated.



4.3.5.3 ACL

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

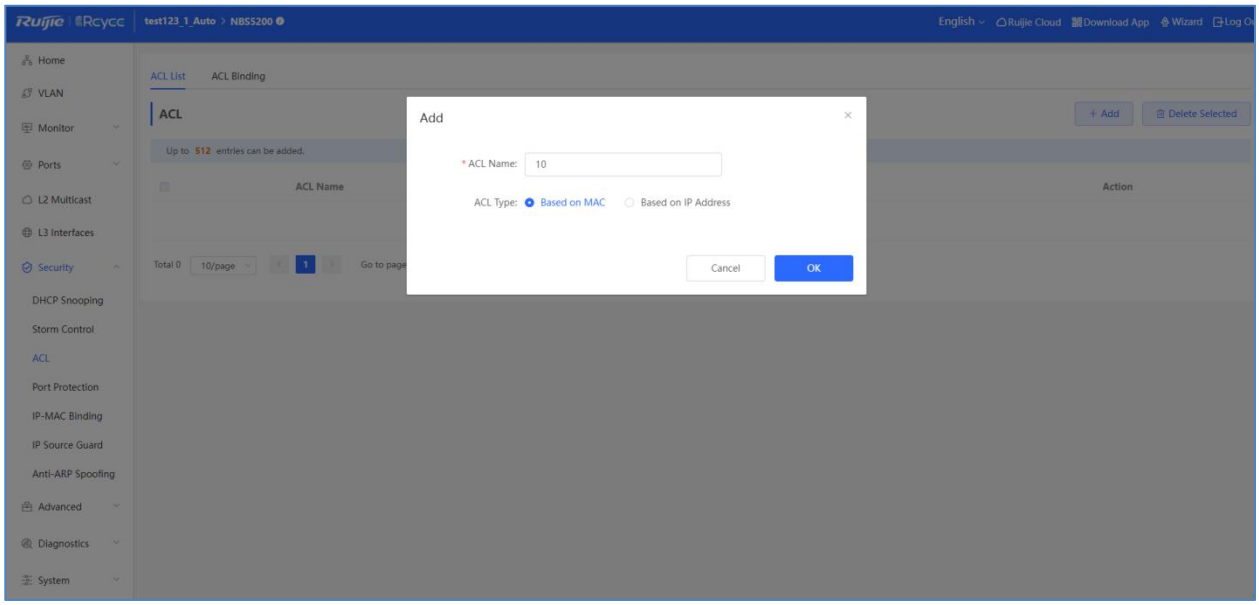
The **ACL** module includes **ACL List** (two types: **Based on MAC** and **Based on IP**) and **ACL Binding**.

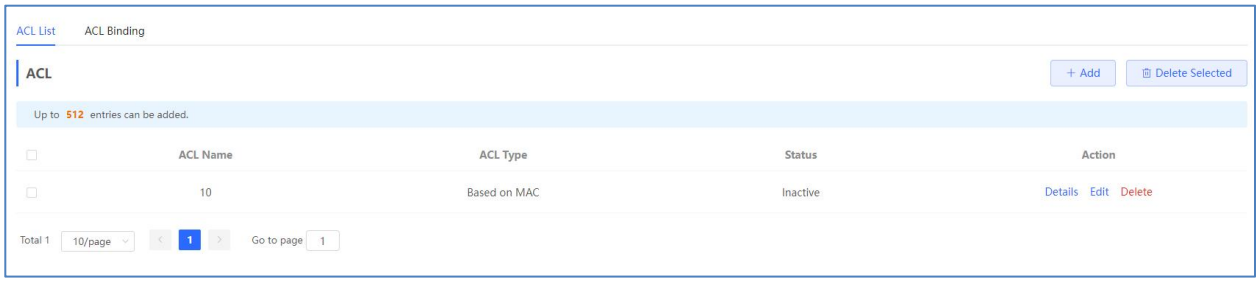


1.1 Base on MAC

Adding an ACL

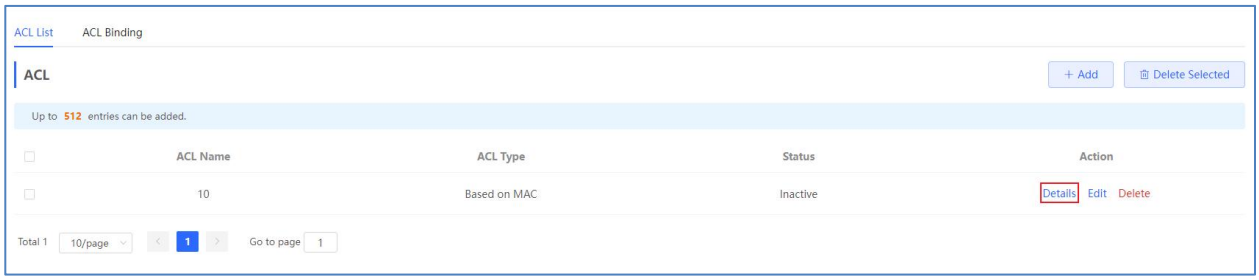
Click **Add**. In the displayed dialog box, select the ACL type, enter the ACL name, and click **OK.**



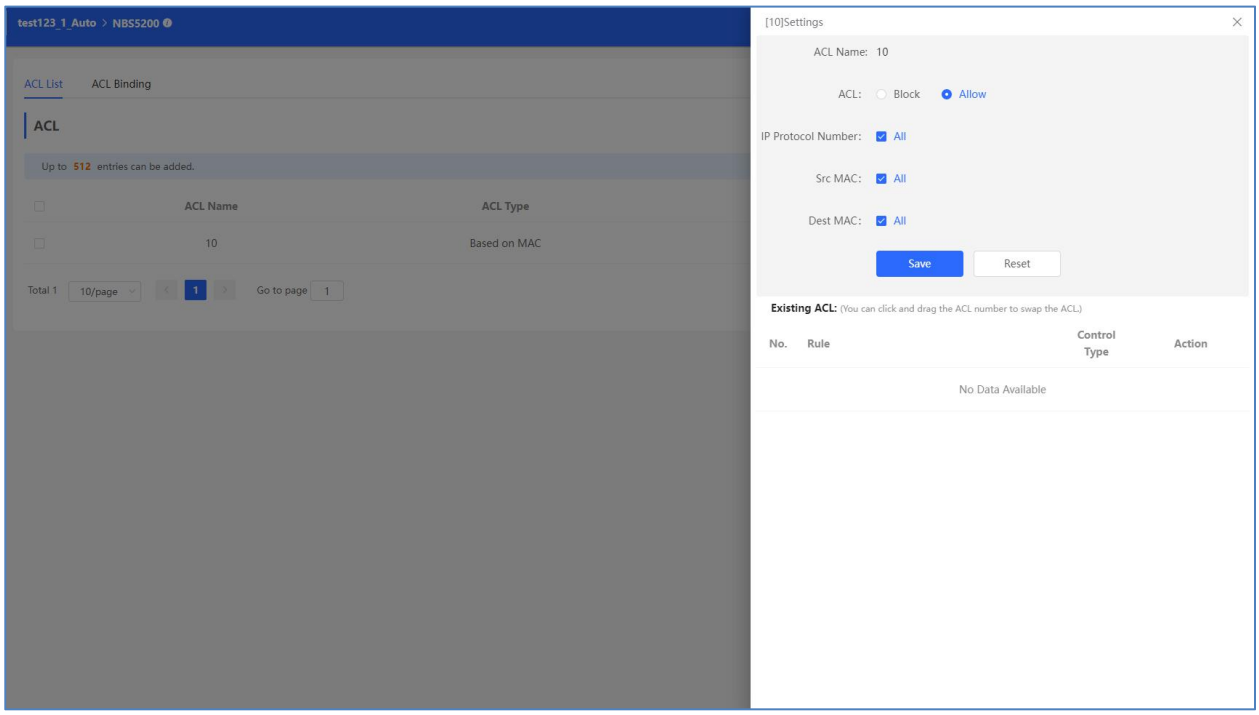


Editing ACEs

Click **Details** in the **Action** column.



In the displayed side pane, query, add, edit, or delete ACEs.

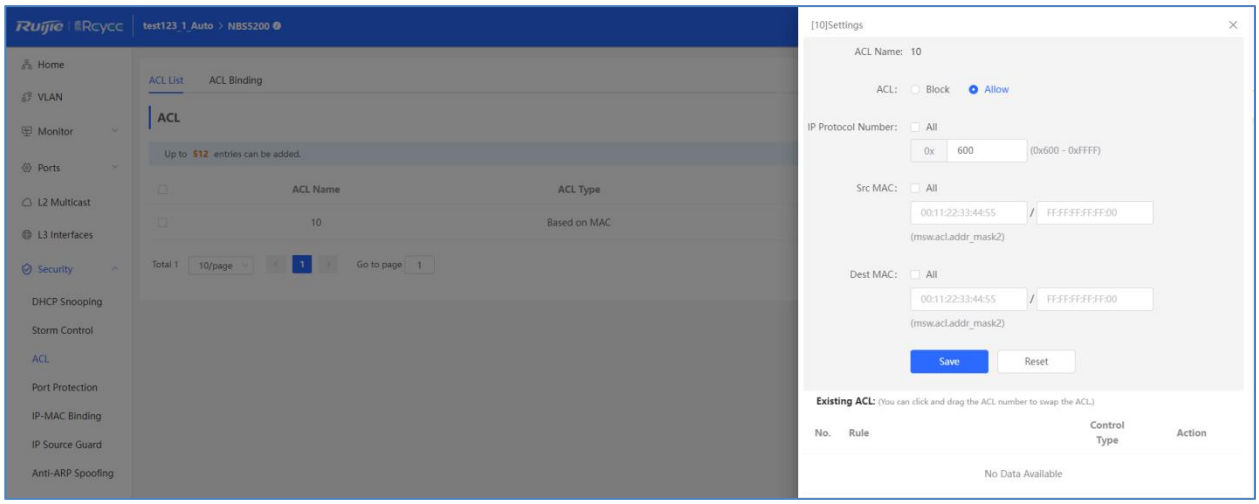


ACL: Block or Allow

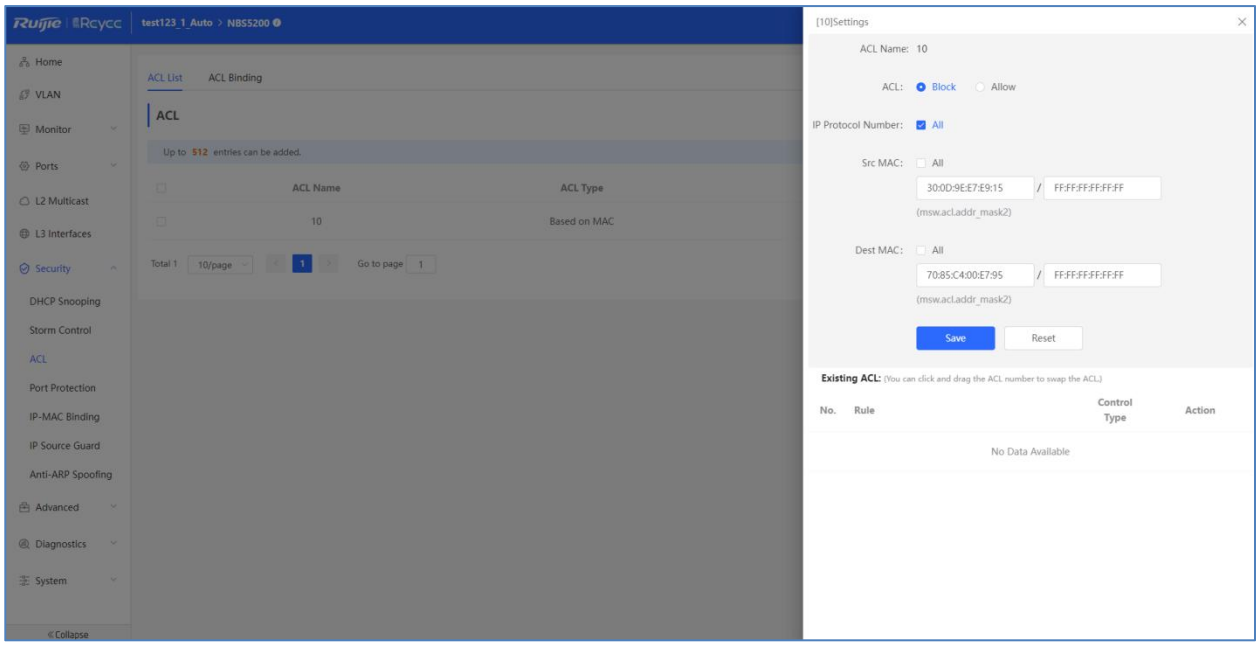
IP Protocol Number: Protocol number in the frame header

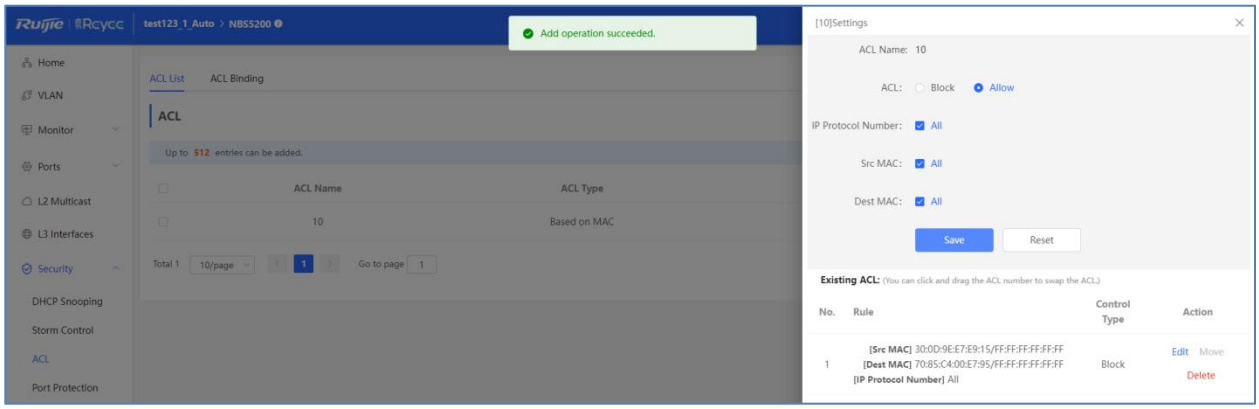
Src MAC: Source MAC address

Dest MAC: Destination MAC address



Enter the source MAC address/mask and click Save.

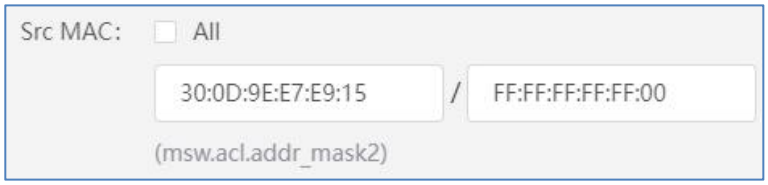




Subnet mask: supports FF:FF:FF:FF:FF:FF, FF:FF:FF:FF:FF:00, FF:FF:FF:FF:00:00, FF:FF:FF:00:00:00.

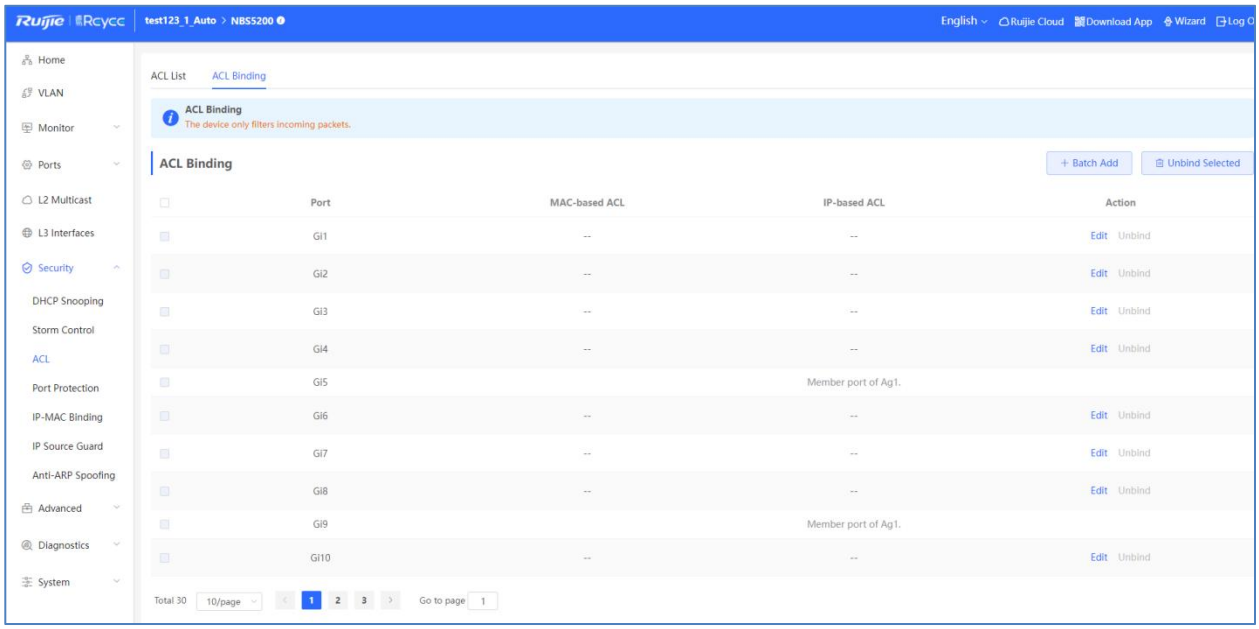
FFindicates exact match while 00 indicates random

For example：

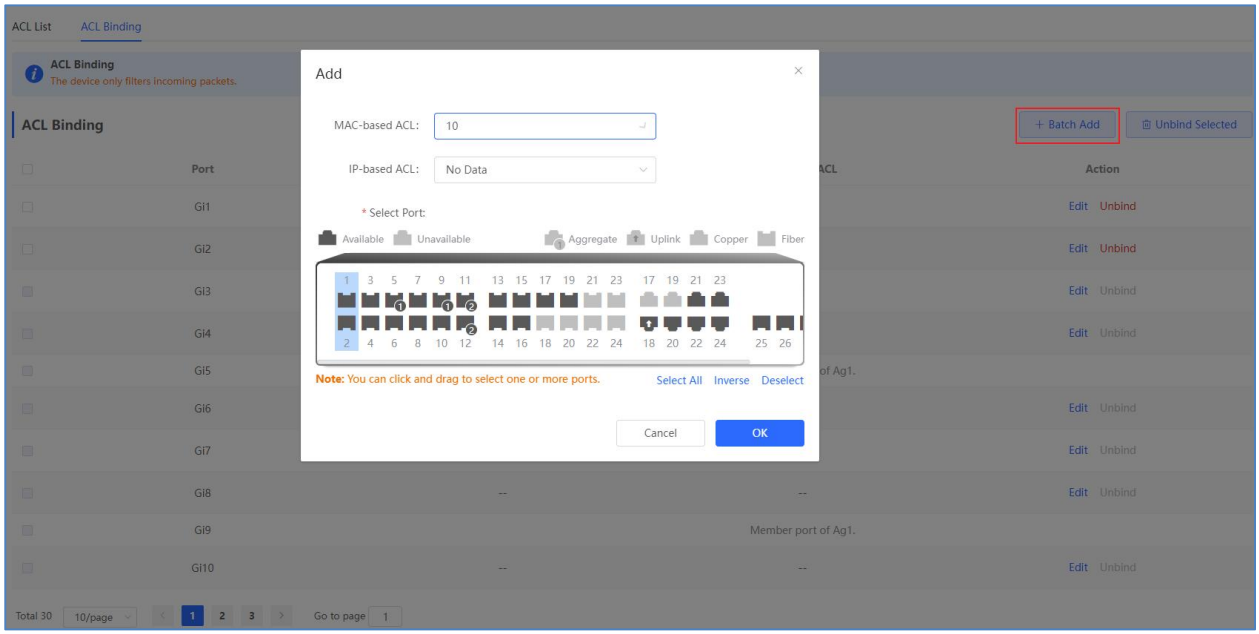


Indicate 30:0D:9E:E7:E9:xx is being matched --xx could be any letters

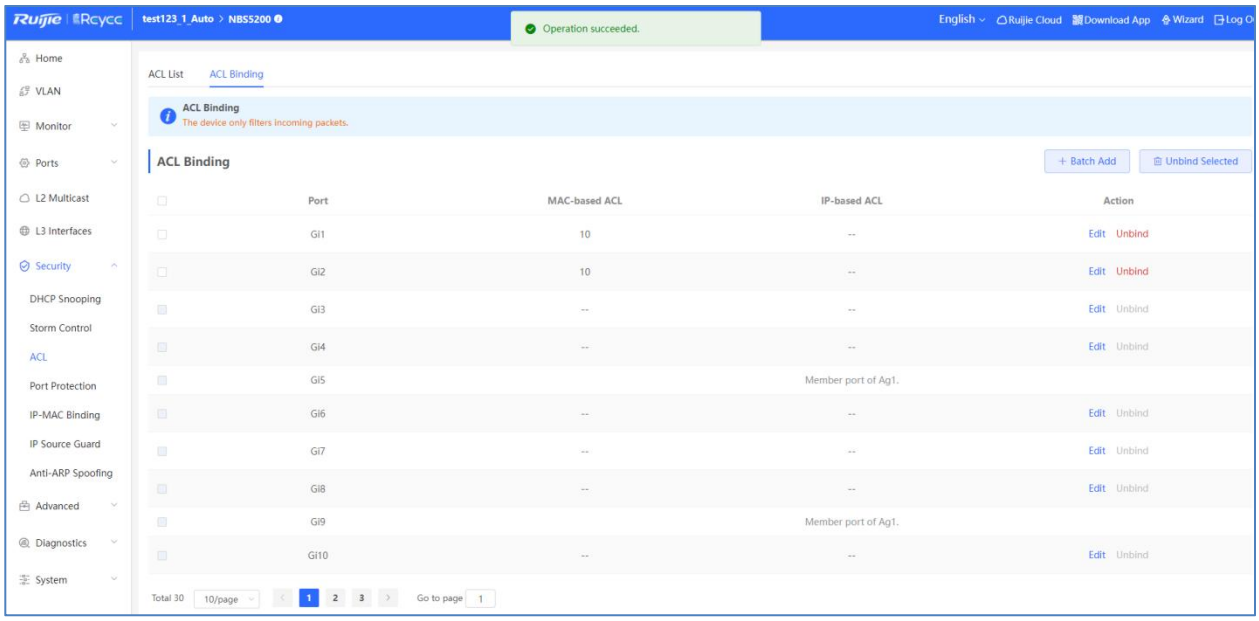
Binding to interfaces



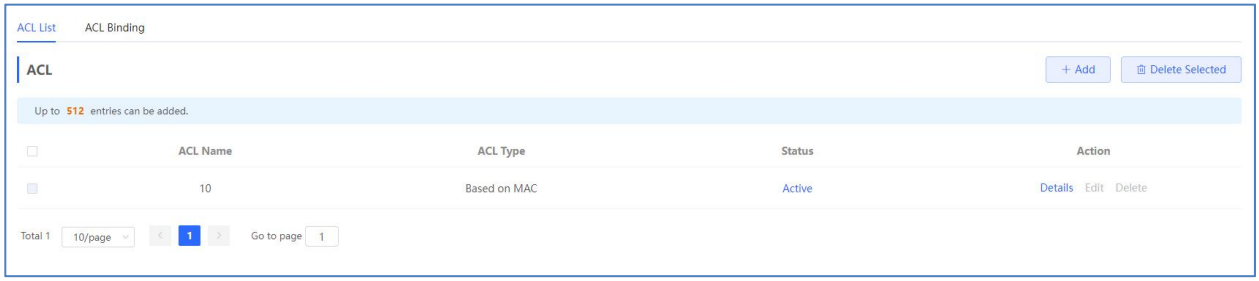
Click **Batch Add**. In the displayed dialog box, select the target MAC-based ACL and ports, and click **OK.**



The message "Operation succeeded" is displayed, and the ACL Binding list is updated.



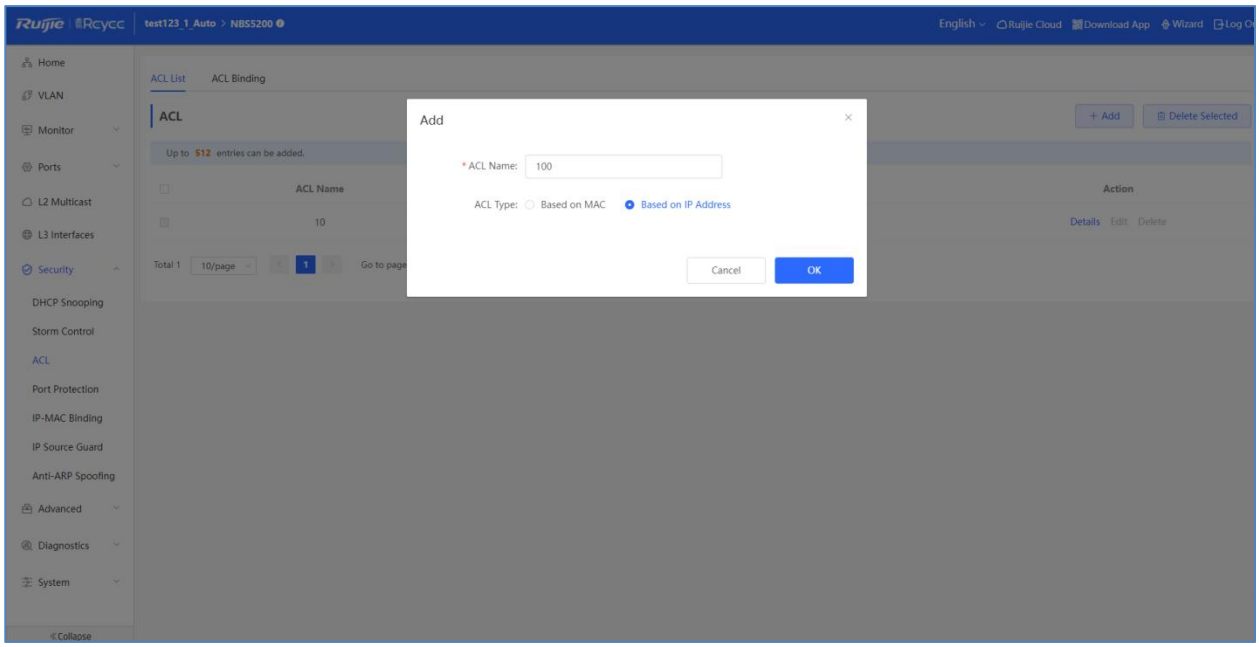
In the ACL list page, the status of ACL will show as **Active.**

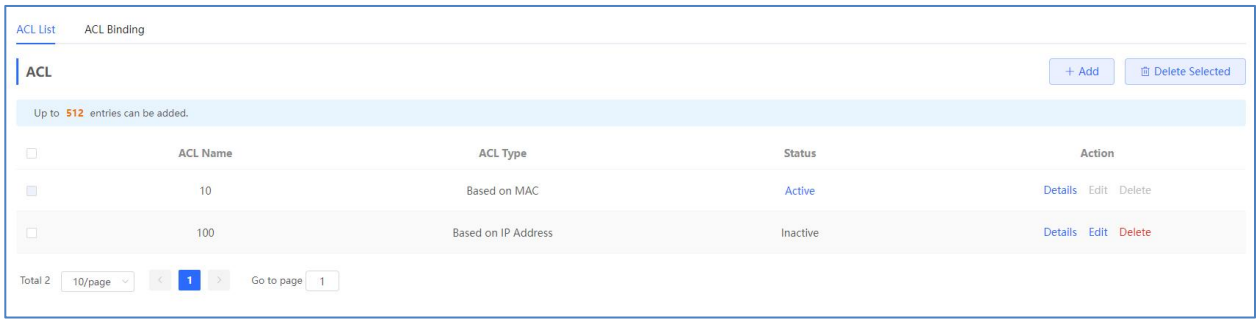


1.2 Base on IP Address

Adding an ACL

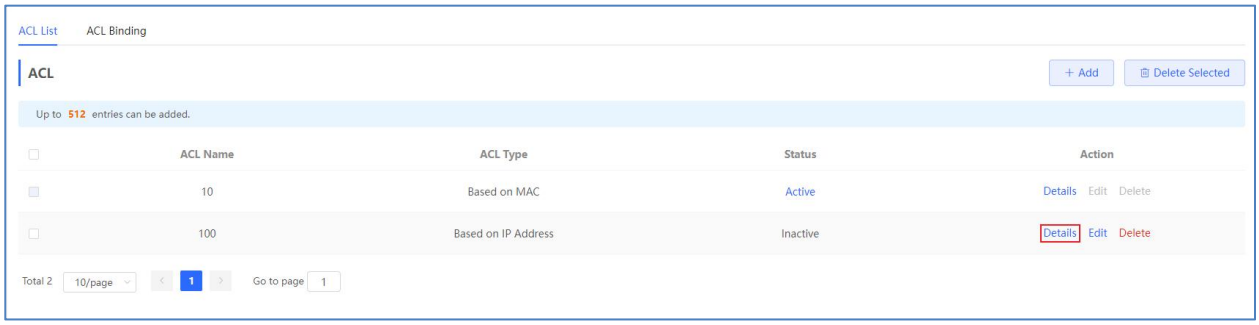
Click **Add.** In the displayed dialog box, select the ACL type, enter the ACL name, and click **OK.**



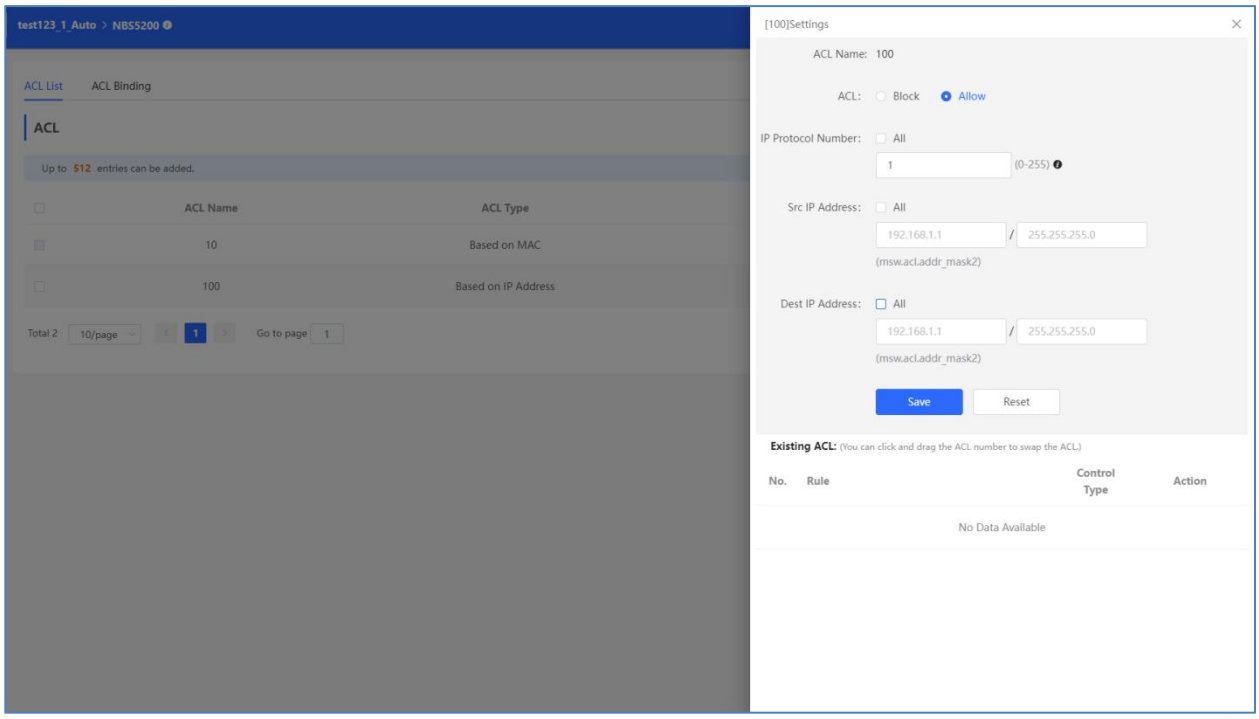


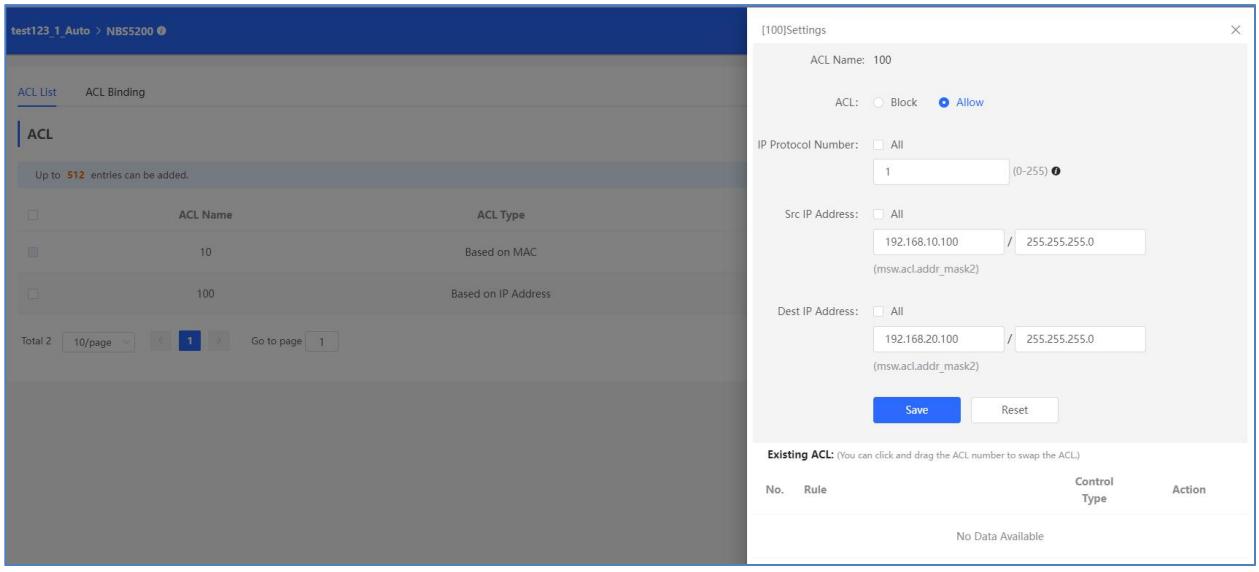
Editing ACEs

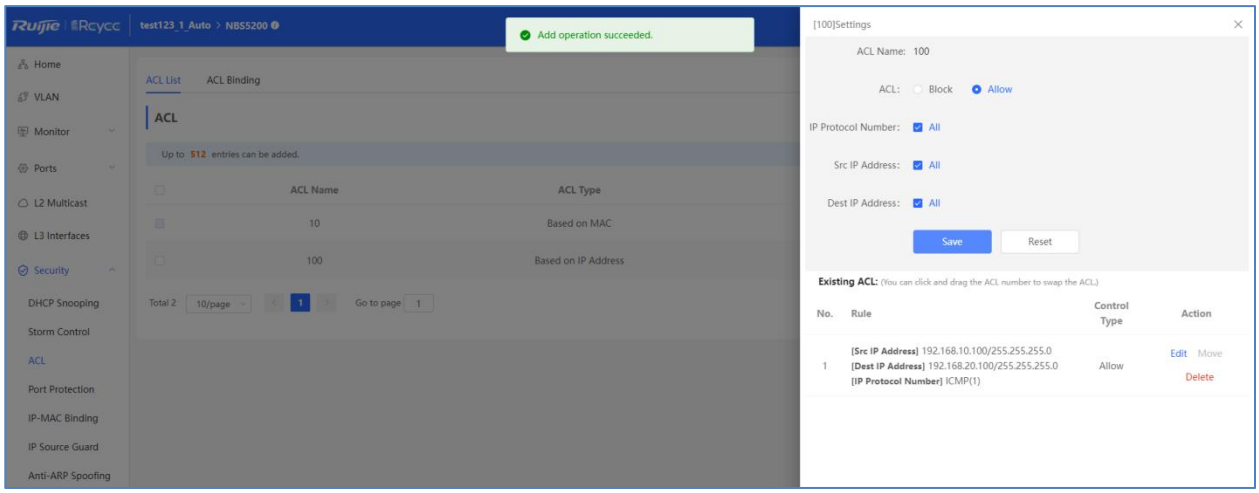
Click **Details** in the **Action** column.



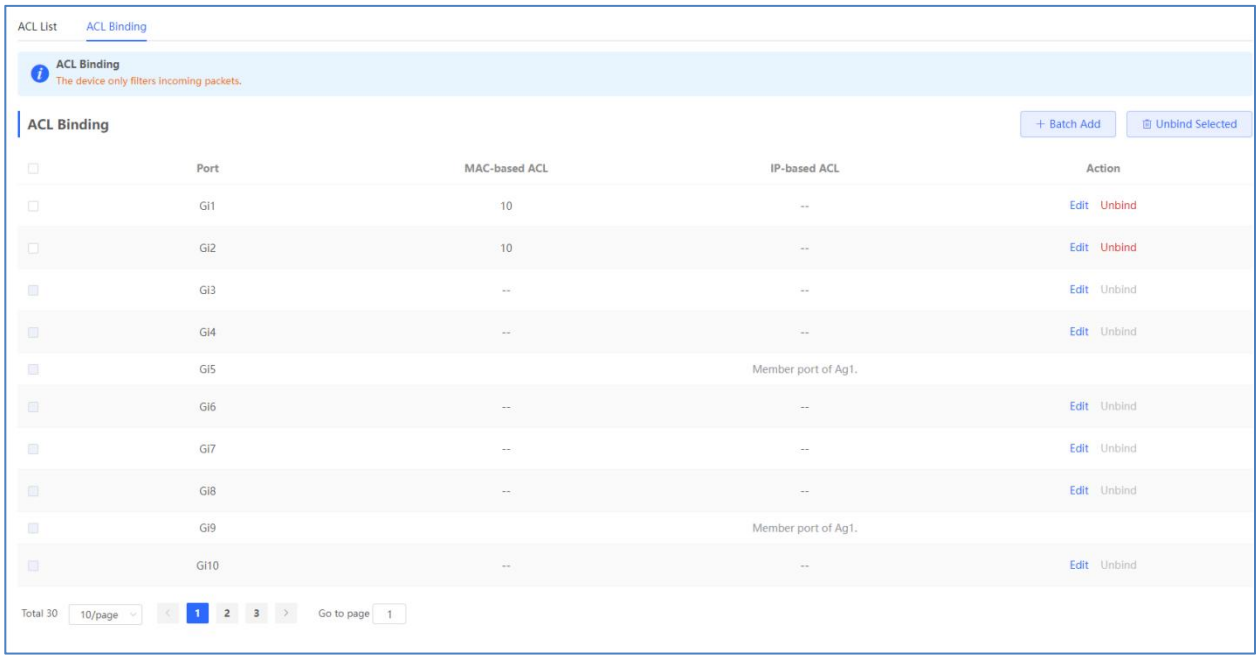
In the displayed side, you can pane, query, add, edit, or delete ACEs.


test123_1_Auto > NBS5200
ACL List
ACL Binding
ACL
Up to 512 entries can be added.
ACL Name
ACL Type
10
Based on MAC
100
Based on IP Address
Total 2
10/page
Go to page
[100]Settings
ACL Name: 100
ACL: Block Allow
IP Protocol Number: All
1
(0-255)
Src IP Address: All
192.168.1.1
255.255.255.0
(msw.acl.addr_mask2)
Dest IP Address: All
192.168.1.1
255.255.255.0
(msw.acl.addr_mask2)
Save
Reset
Existing ACL: (You can click and drag the ACL number to swap the ACL.)
No.
Rule
Control Type
Action
No Data Available

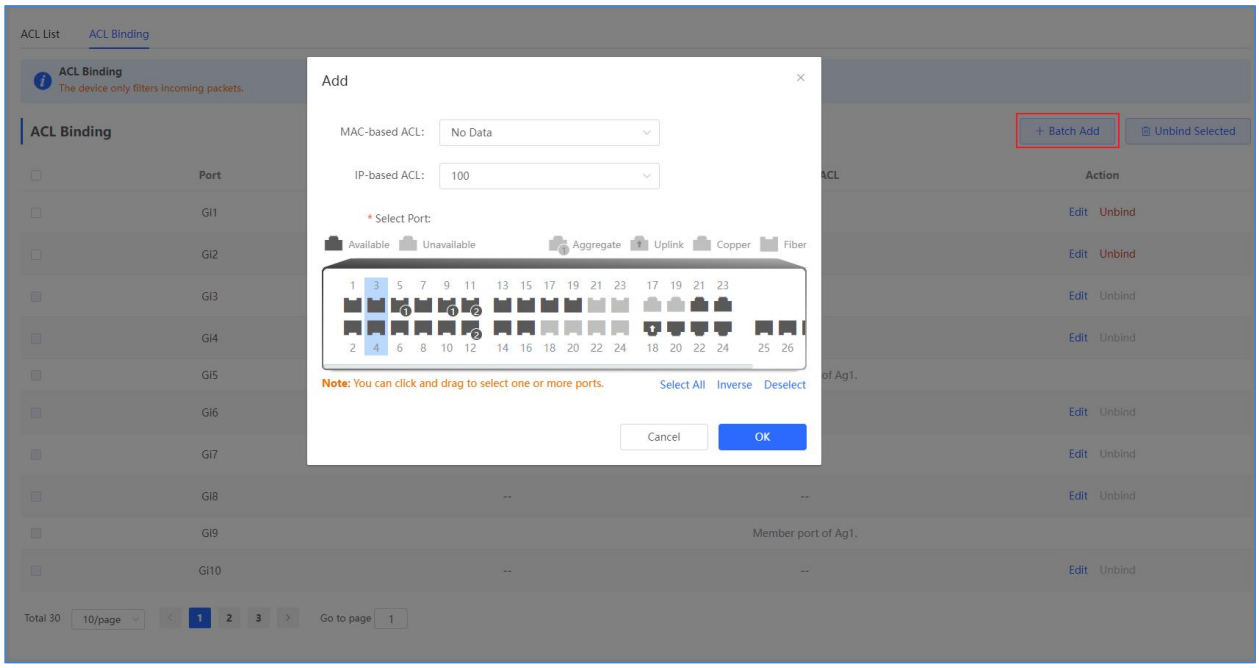

test123_1_Auto > NBS5200
ACL List
ACL Binding
ACL
Up to 512 entries can be added.
ACL Name
ACL Type
10
Based on MAC
100
Based on IP Address
Total 2
10/page
Go to page
[100]Settings
ACL Name: 100
ACL: Block Allow
IP Protocol Number: All
1
(0-255)
Src IP Address: All
192.168.10.100
255.255.255.0
(msw.acl.addr_mask2)
Dest IP Address: All
192.168.20.100
255.255.255.0
(msw.acl.addr_mask2)
Save
Reset
Existing ACL: (You can click and drag the ACL number to swap the ACL.)
No.
Rule
Control Type
Action
No Data Available



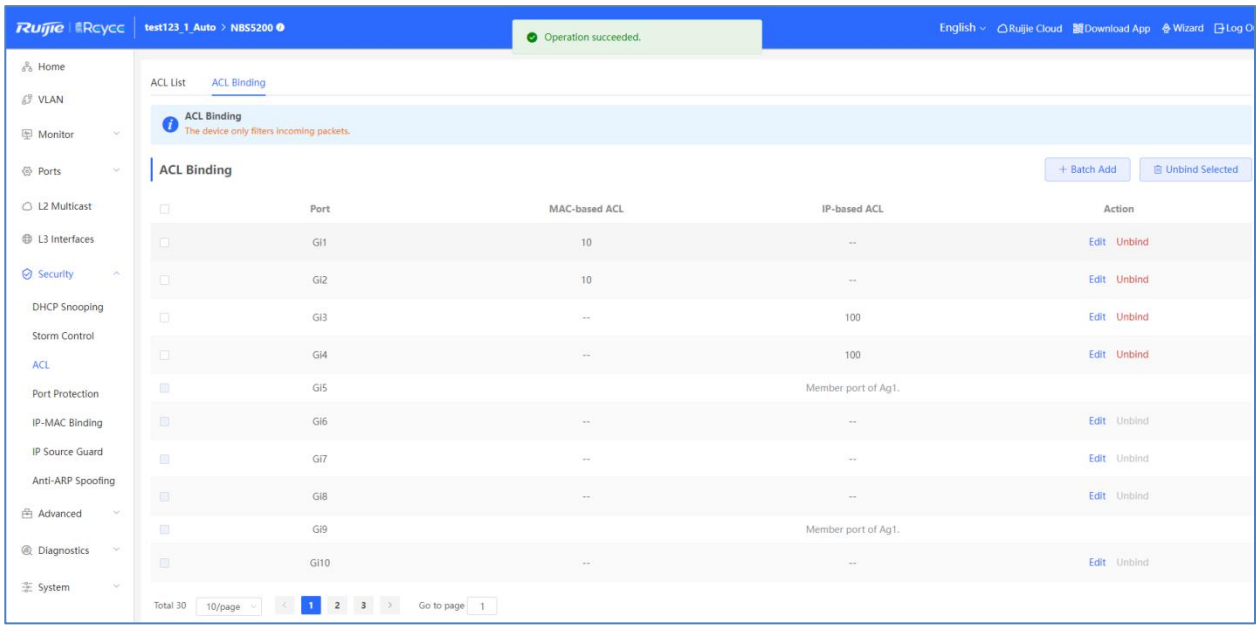
Binding to interfaces



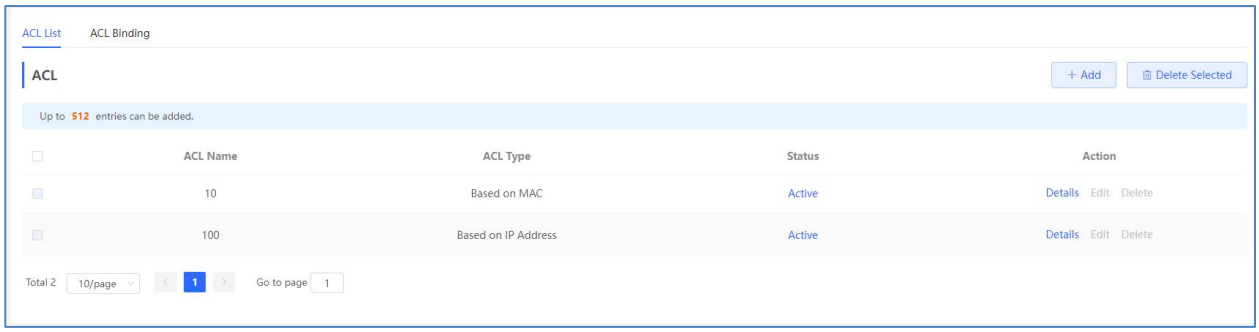
Click **Batch Add**. In the displayed dialog box, select the target MAC-based ACL and ports, and click **OK.**



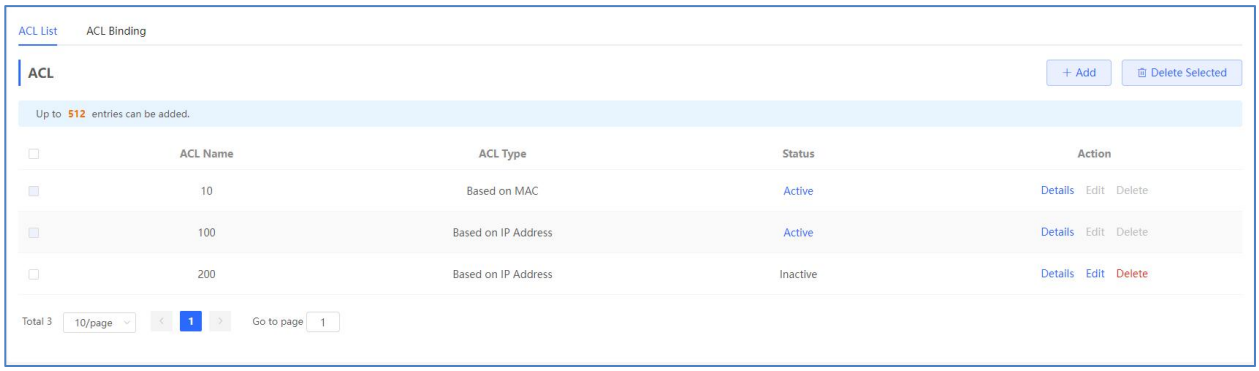
The message "Operation succeeded." is displayed, and the ACL Binding list is updated.



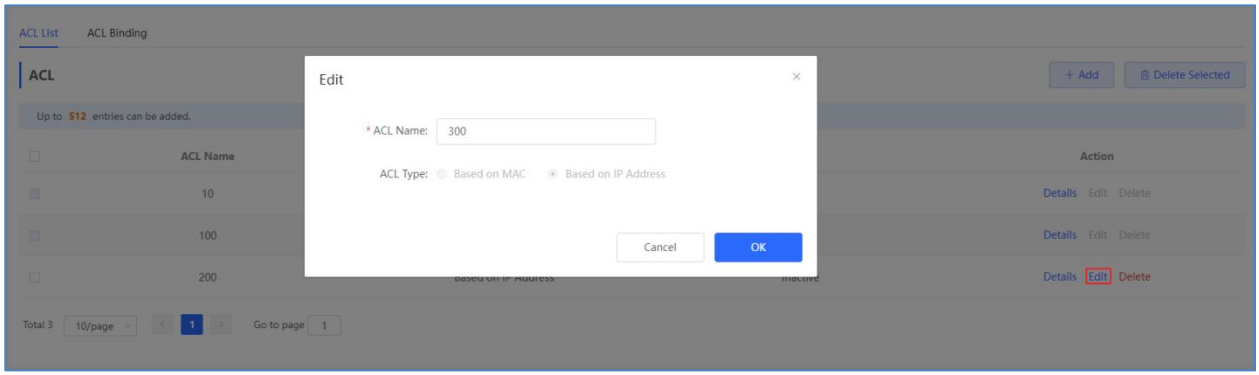
In the ACL list page, the status of ACL will show as **Active.**



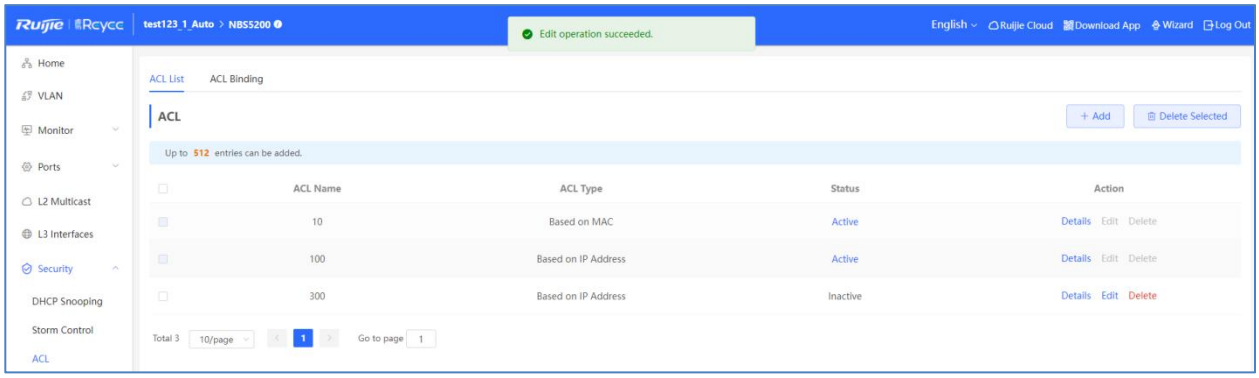
1.3 Editing an ACL



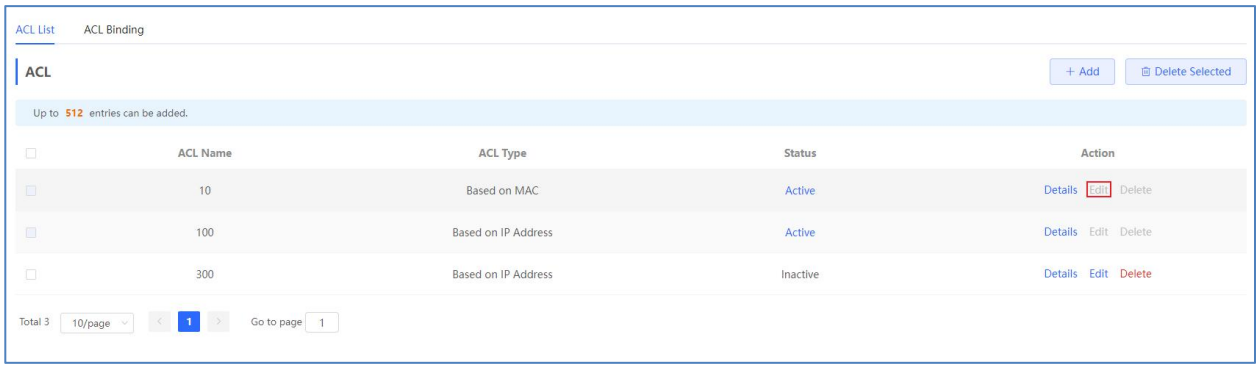
Click **Edit** in the **Action** column. In the displayed dialog box, edit the ACL name and click **OK.**



A message "Edit operation succeeded." is displayed, and the ACL list is updated.

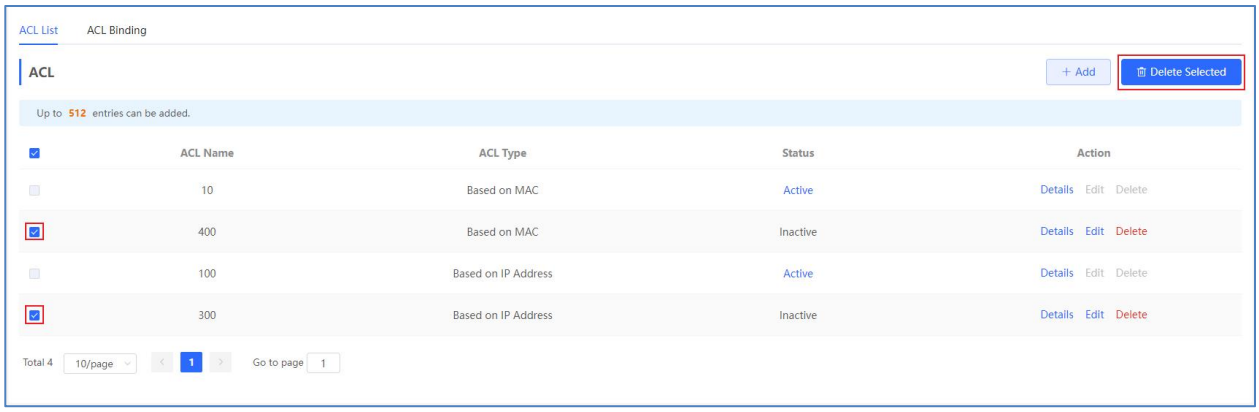


The ACL which has been bound to interface cannot be edited. You need to remove the bind before editing.

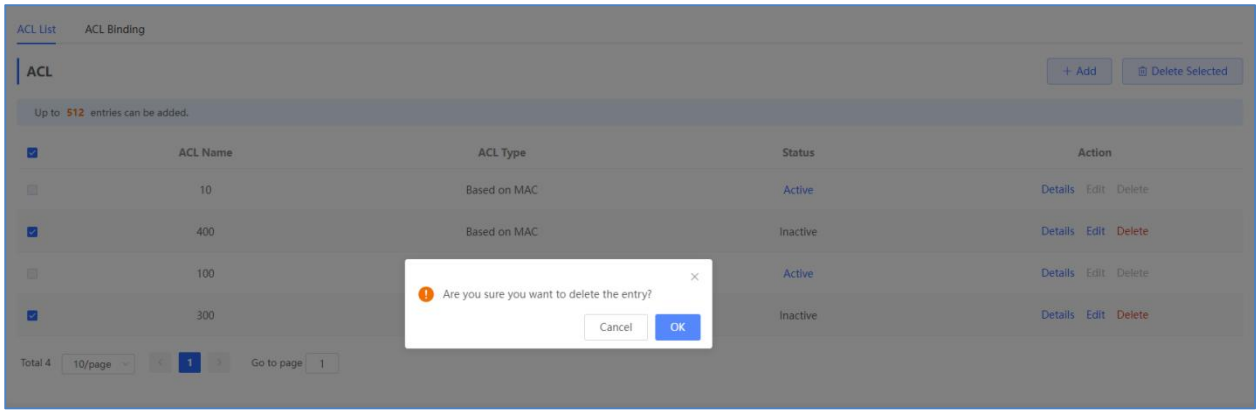


1.4 Batching deleting ACLs/Deleting a single ACL

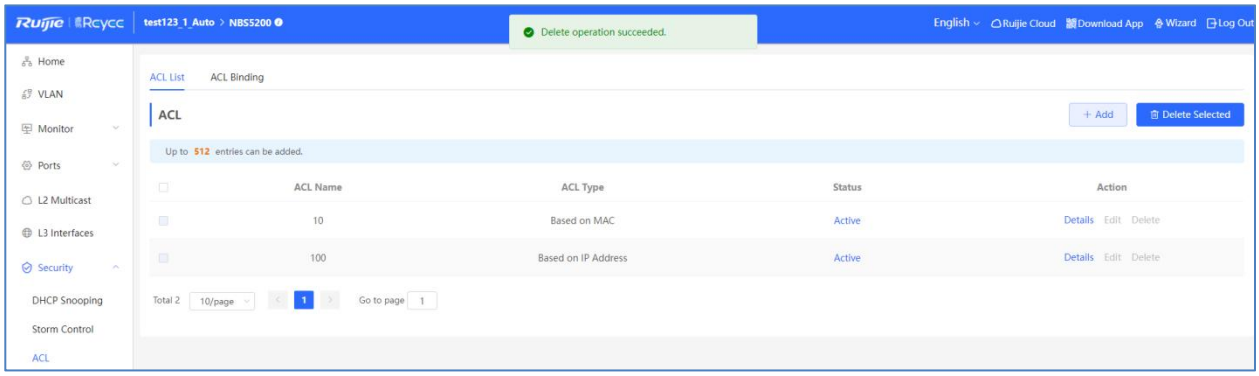
Select ACLs in the ACL list, and click **Delete Selected.**



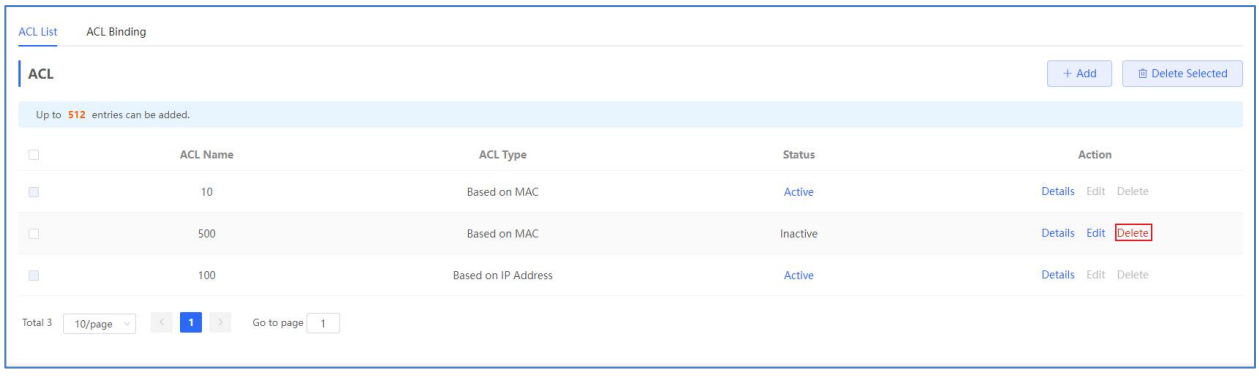
Click **OK** in the confirmation box.



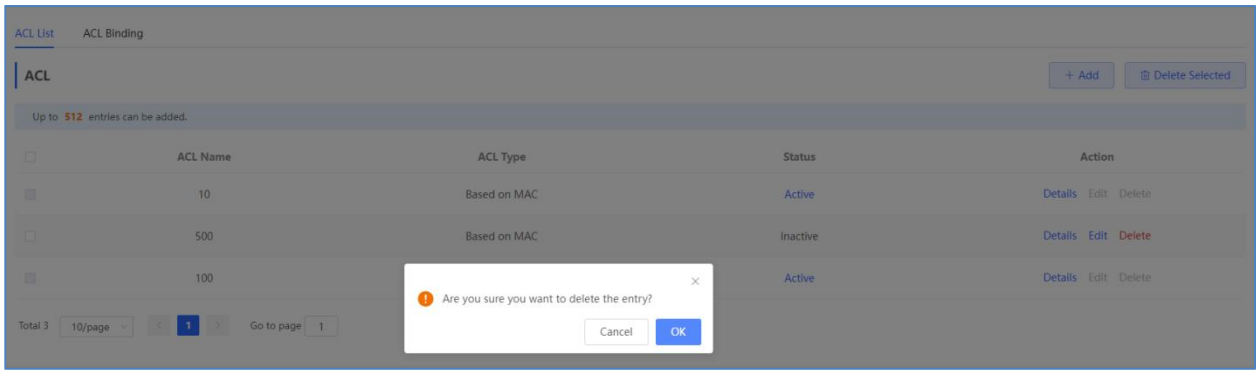
A message "Delete operation succeeded." is displayed, and the ACL list is updated.



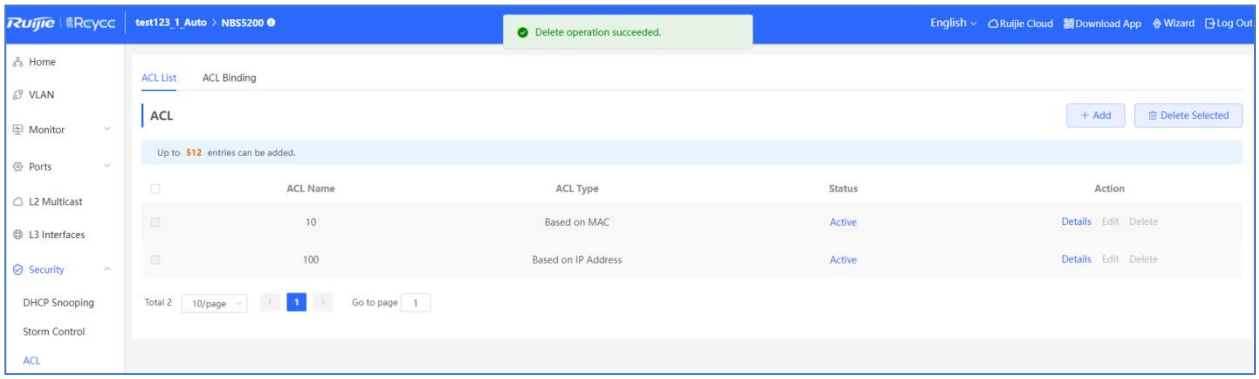
Alternatively, click **Delete** in the Action column.



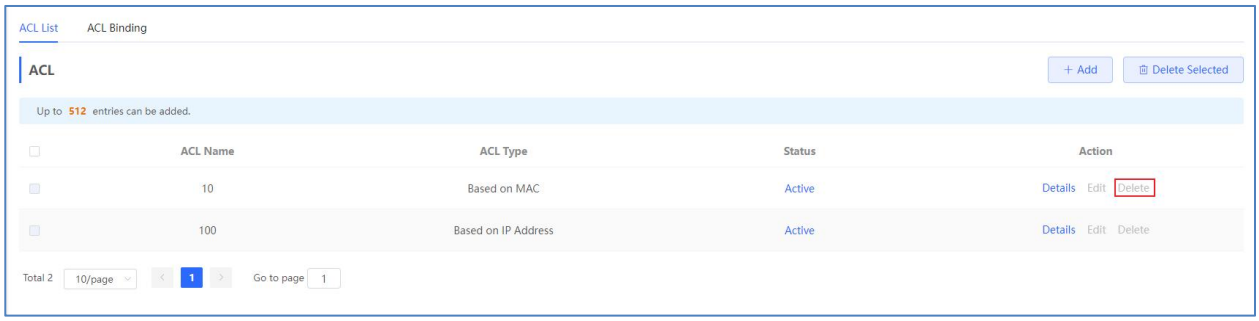
In the displayed confirmation box, click OK.



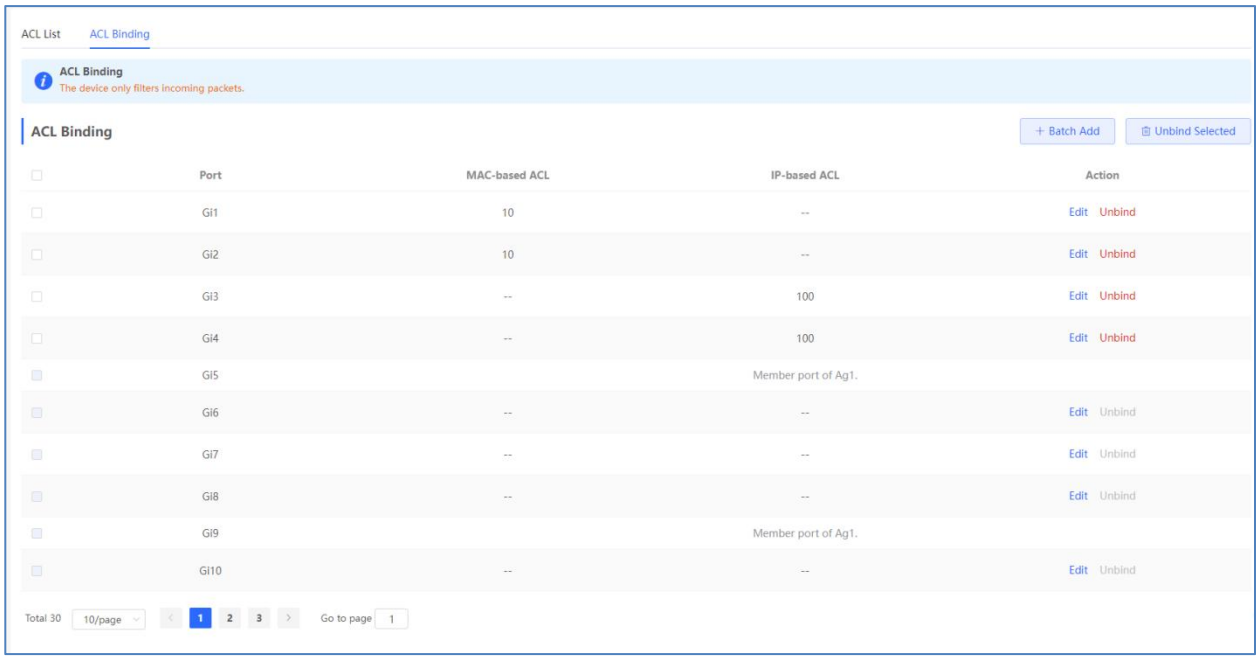
A message "Delete operation succeeded." is displayed, and the ACL list is updated.



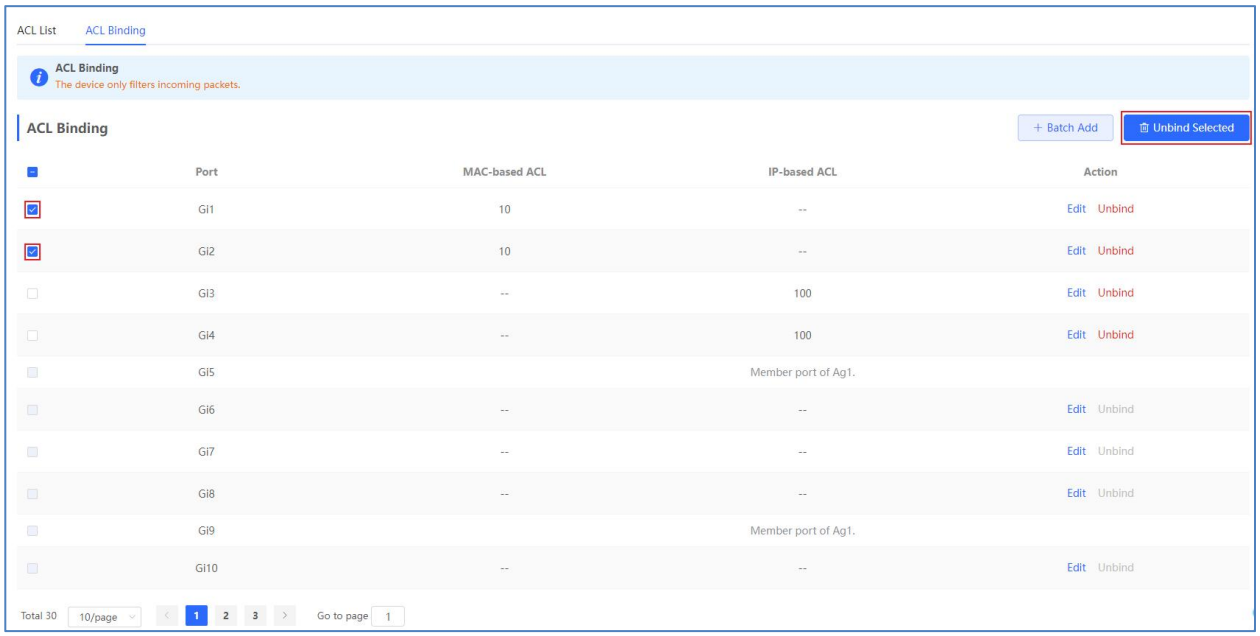
The ACL which has been bound to interface cannot be edited. You need to remove the bind before editing.



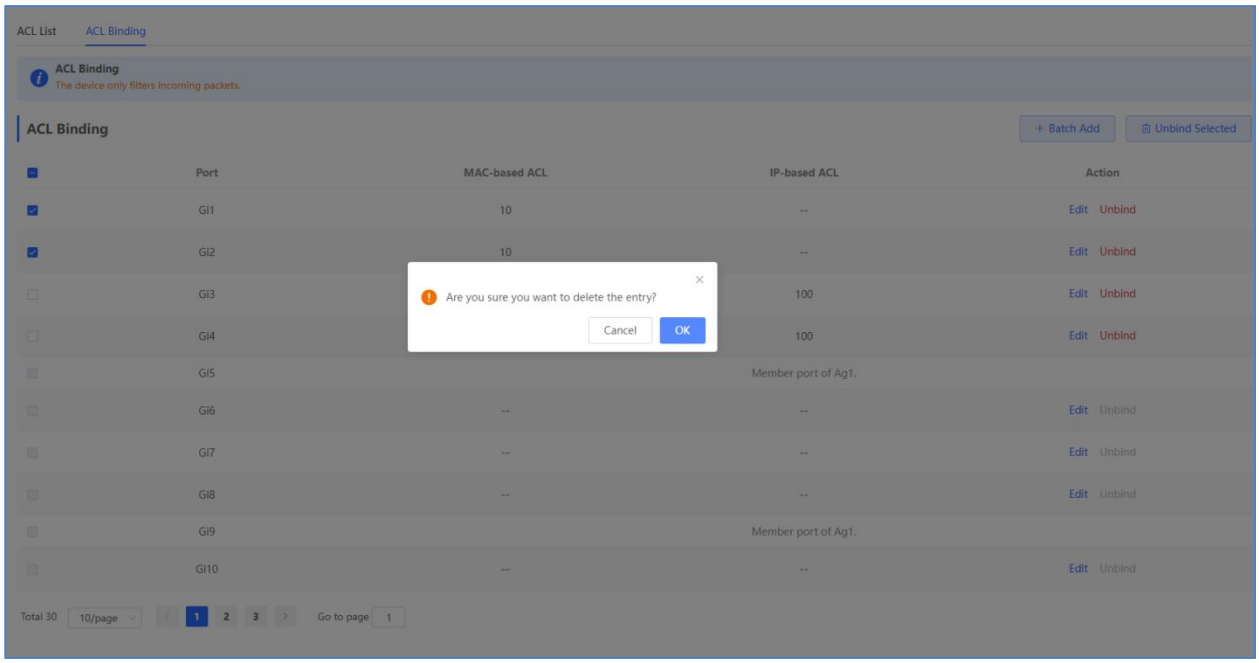
1.5 Batch unbinding ACLs/Unbinding a single ACL



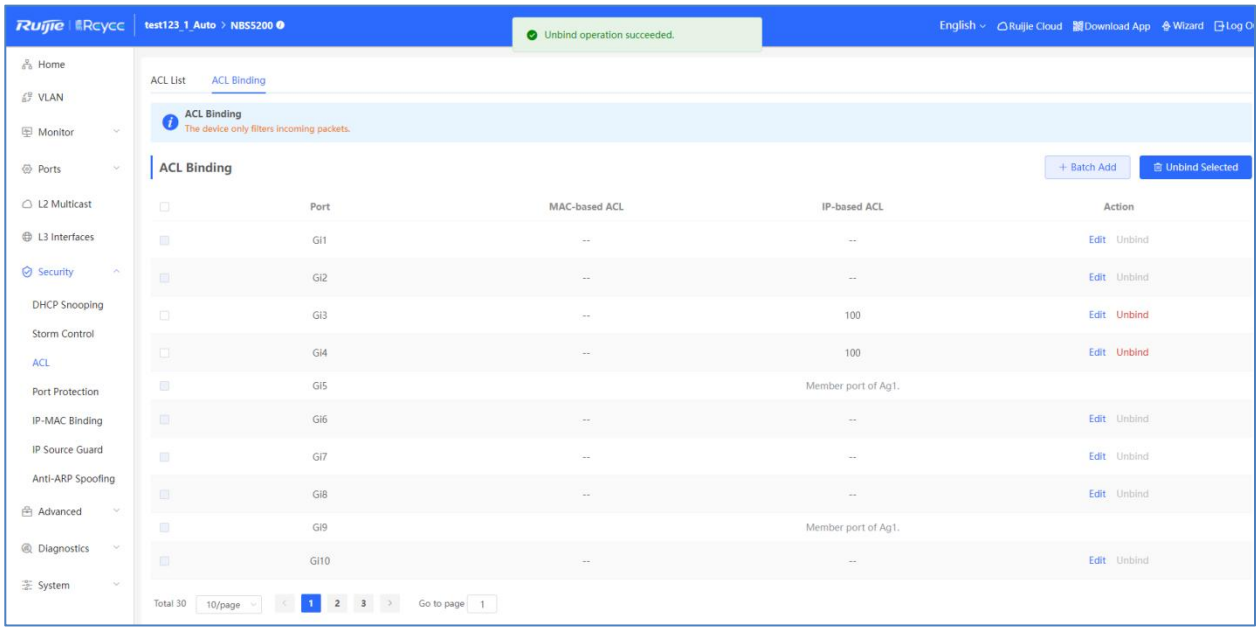
Select multiple entries in **ACL Binding,** and click **Unbind Selected.**



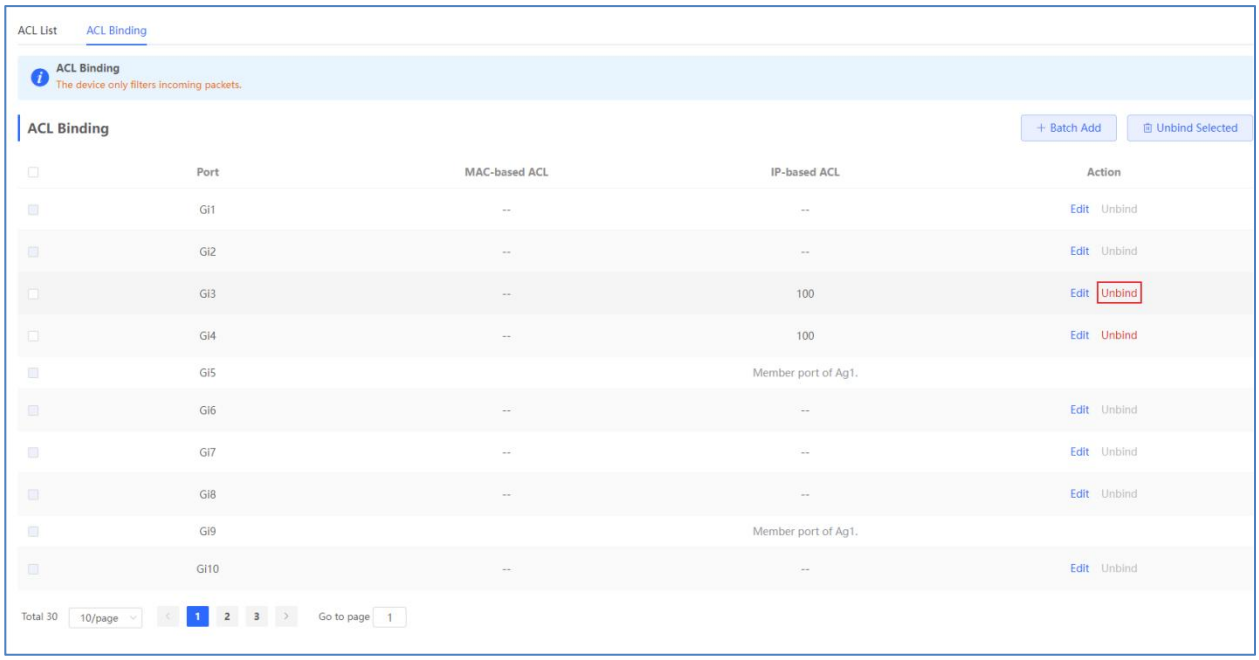
Click **OK** in the confirmation box.



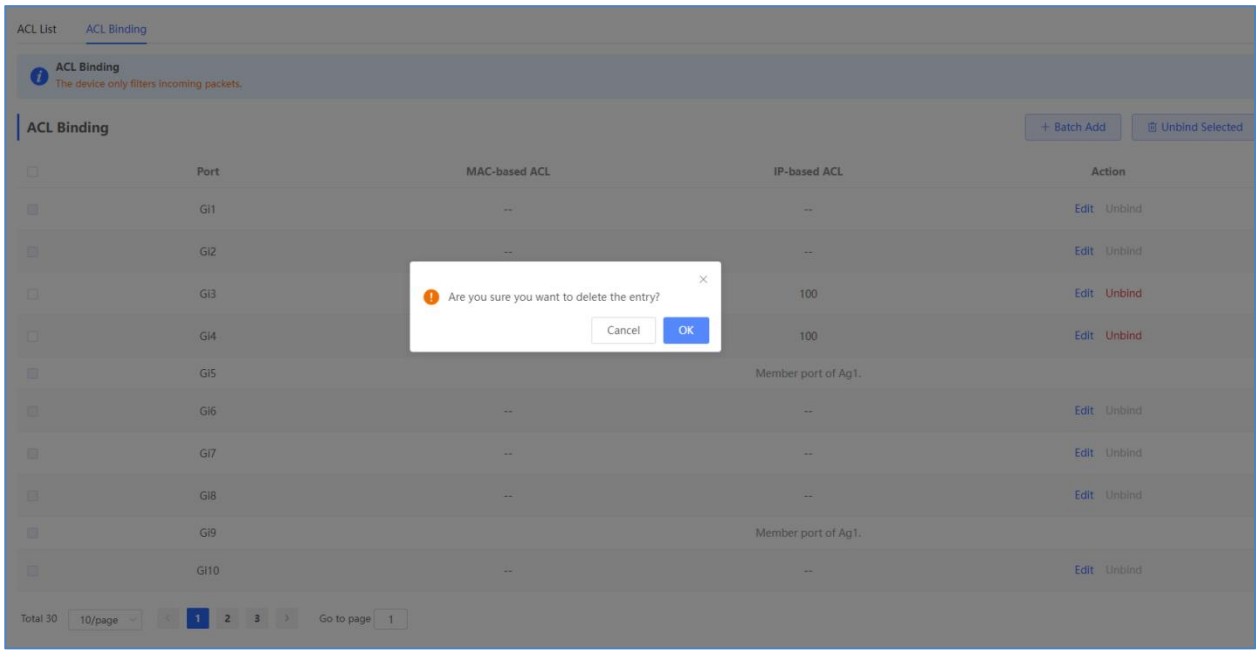
A message "Unbind operation succeeded." is displayed, and the ACL Binding list is updated.



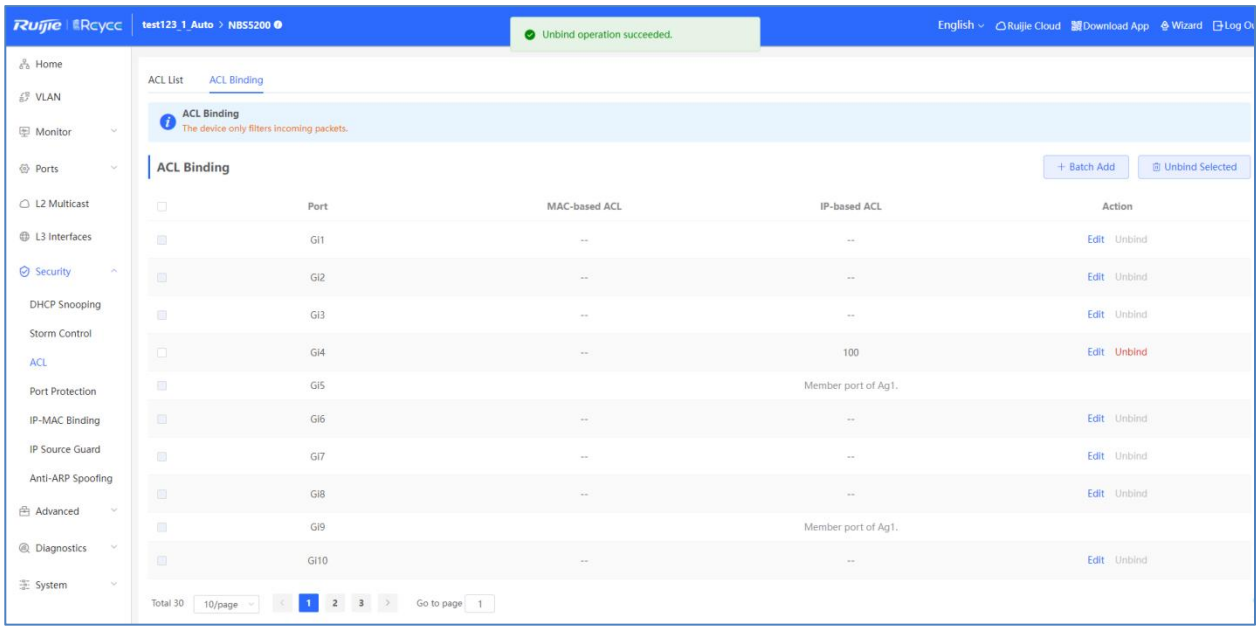
Alternatively, click **Unbind** in the **Action** column.



In the displayed confirmation box, click **OK.**

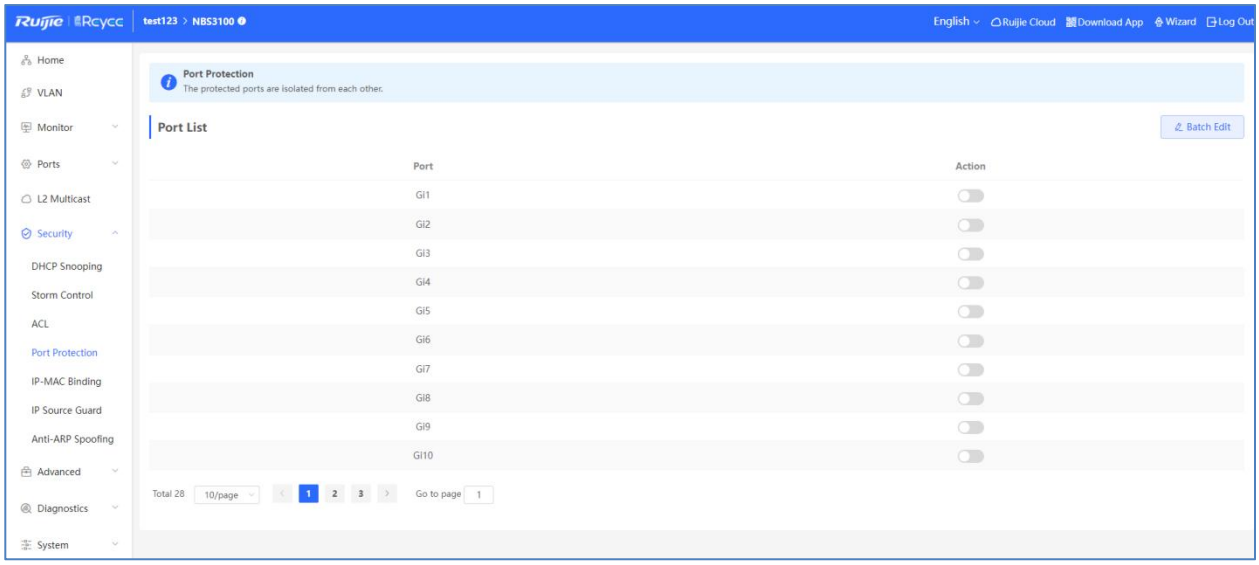


A message "Unbind operation succeeded." is displayed, and the ACL Binding list is updated.

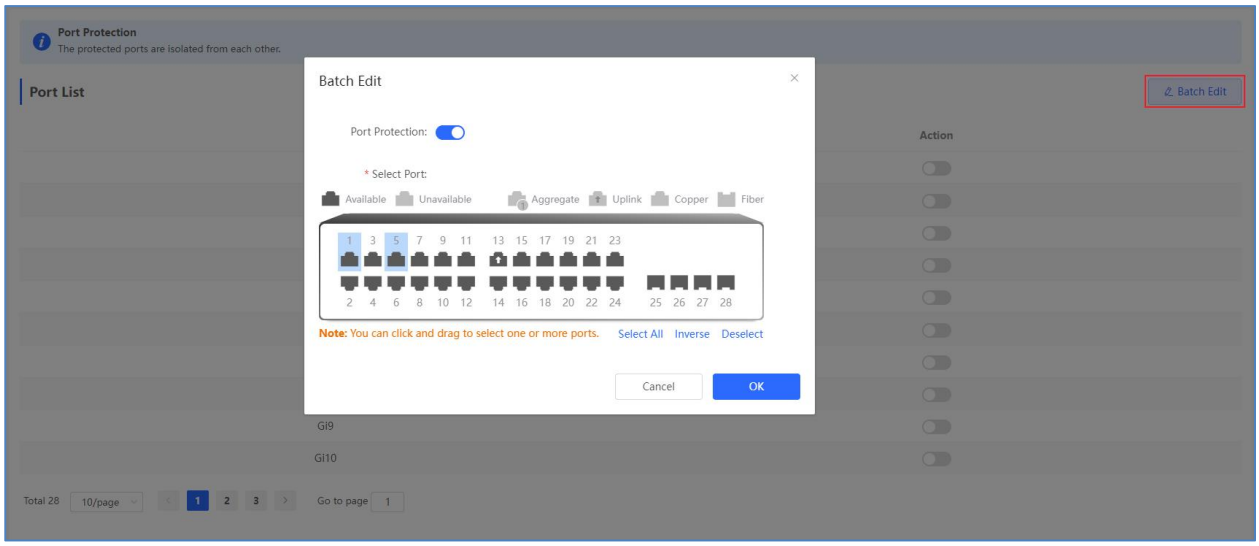


4.3.5.4 Port Protection

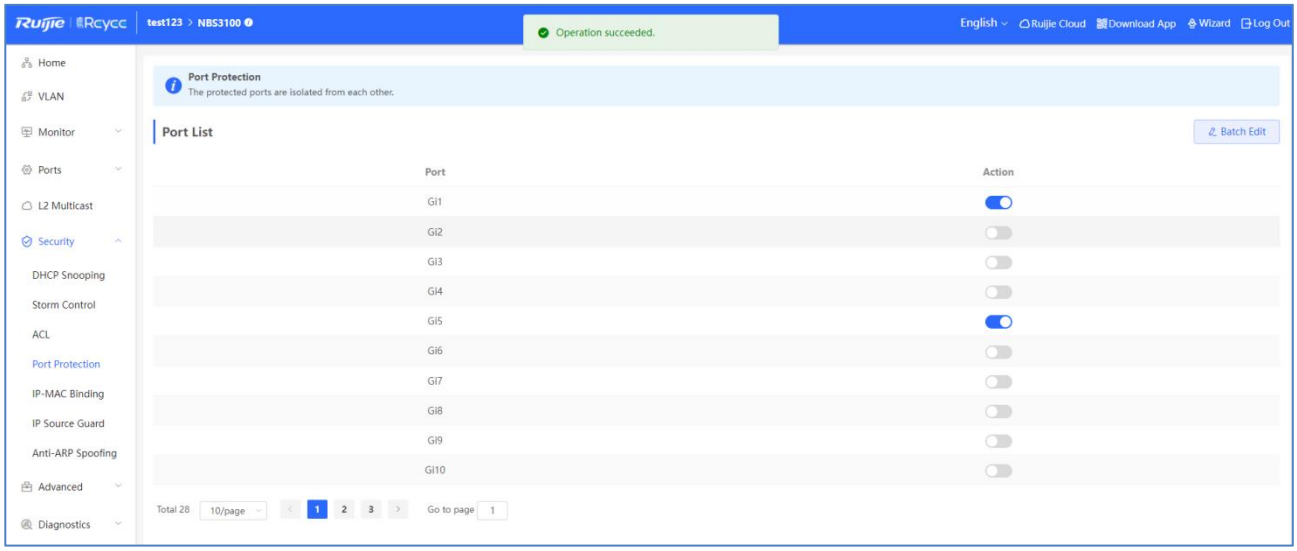
Users on different ports are isolated at layer 2 when port protection is enabled.



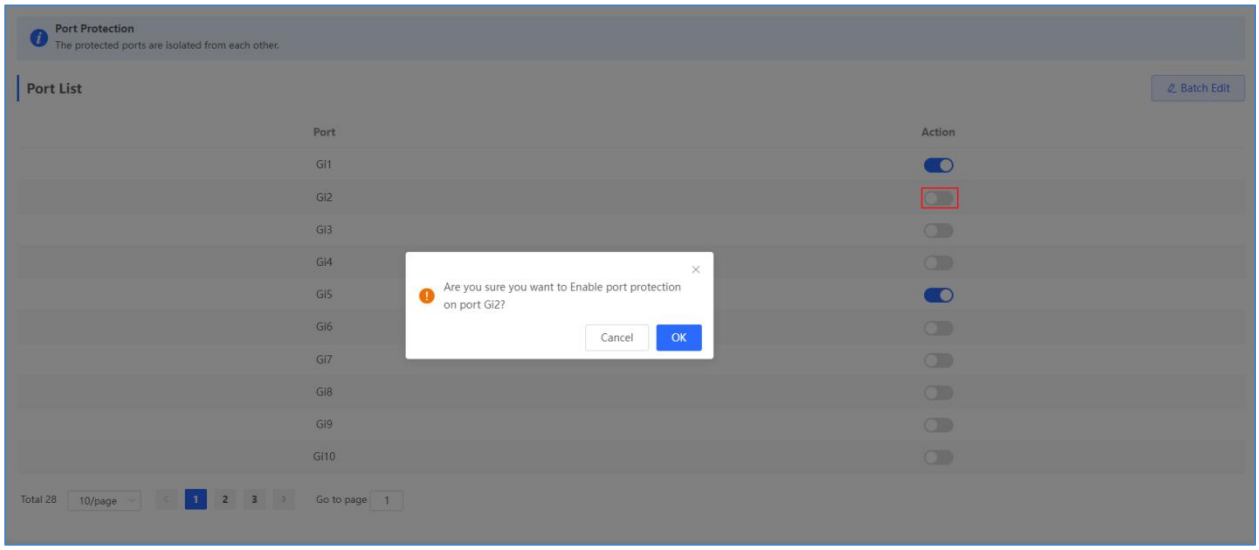
Click **Batch Edit.** In the displayed dialog box, enable or disable port protection and select ports.



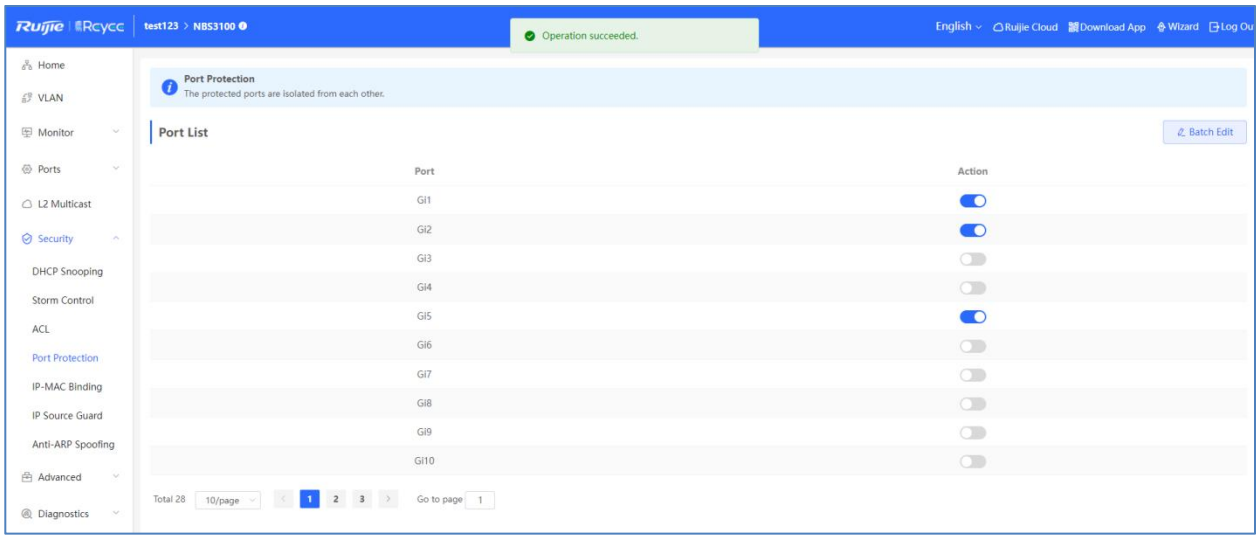
The message "Operation succeeded." is displayed, and the port list is updated.



Alternatively, click the toggle button in the **Action** column. In the displayed confirmation box, click **OK.**



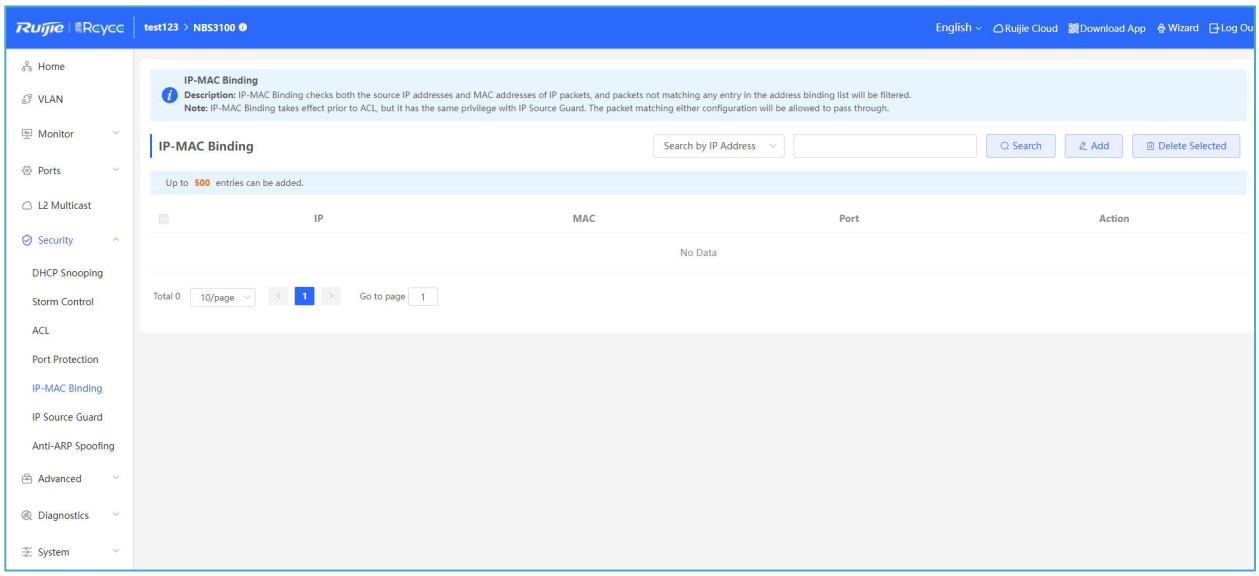
The message "Operation succeeded." is displayed, and the port list is updated.



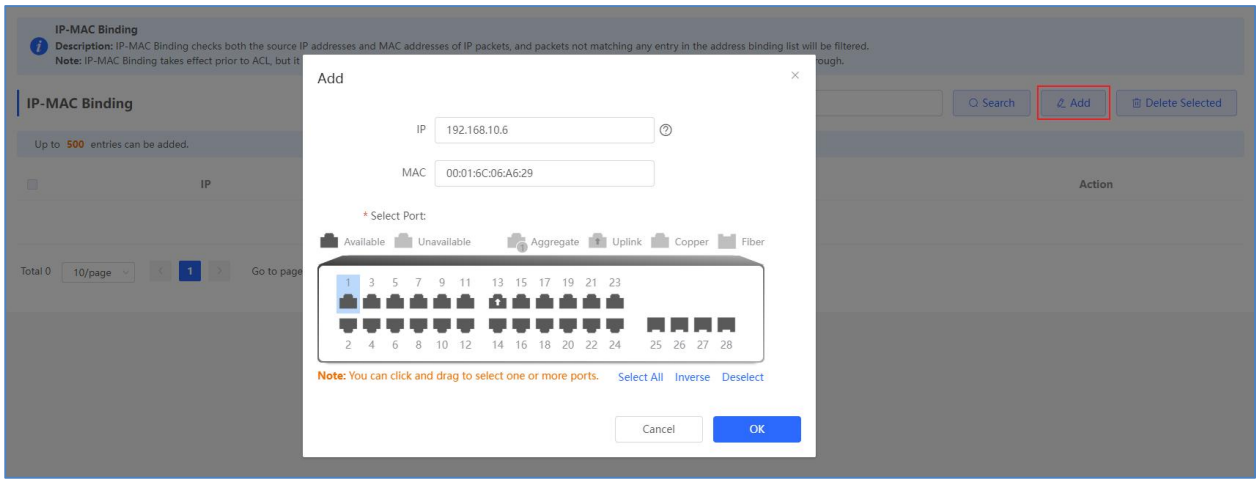
4.3.5.5 IP-MAC Binding

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

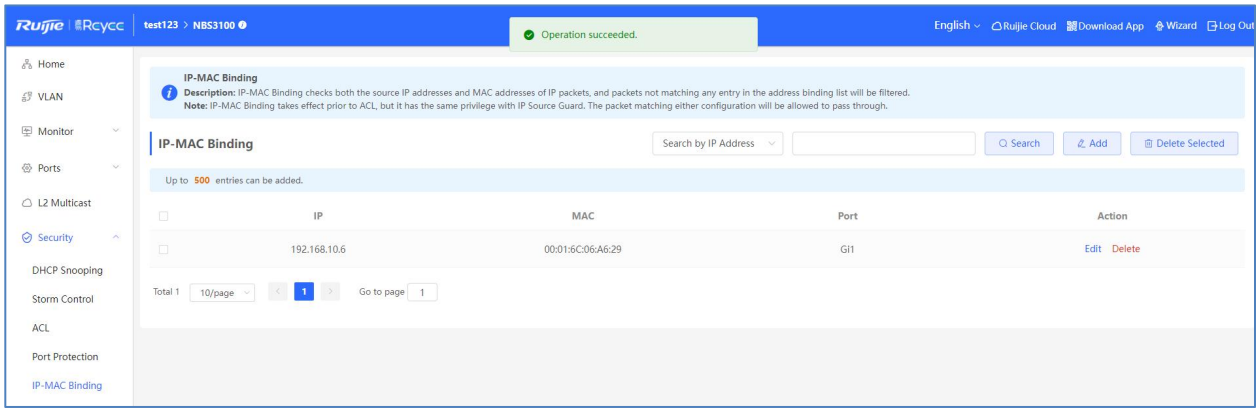
IP-MAC Binding takes effect prior to ACL, but it has the same privilege with IP Source Guard. The packets matching either configuration will be allowed to pass through.



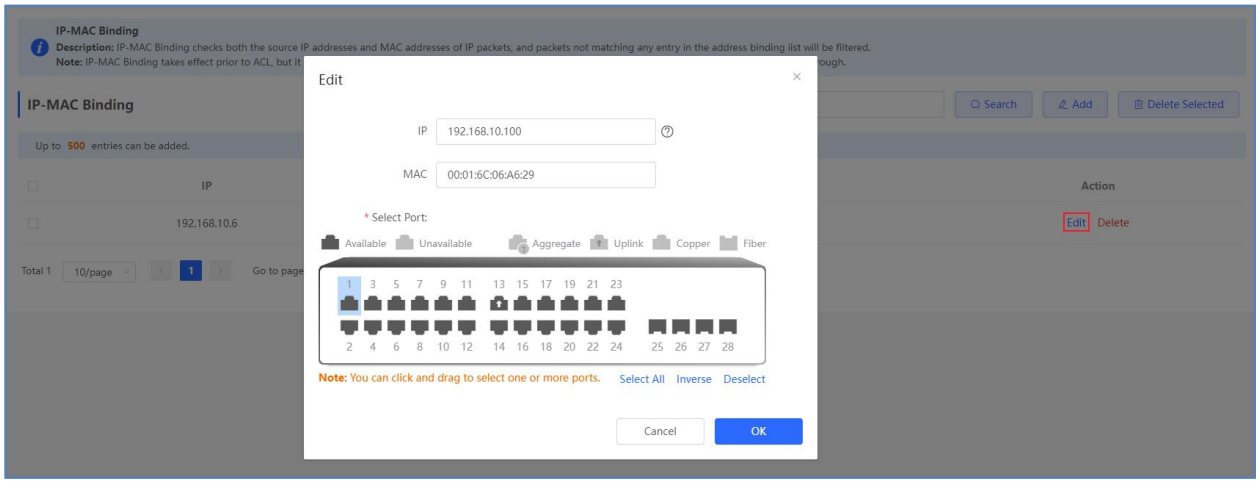
Click **Add**, select ports and configure parameters, and click **OK.**



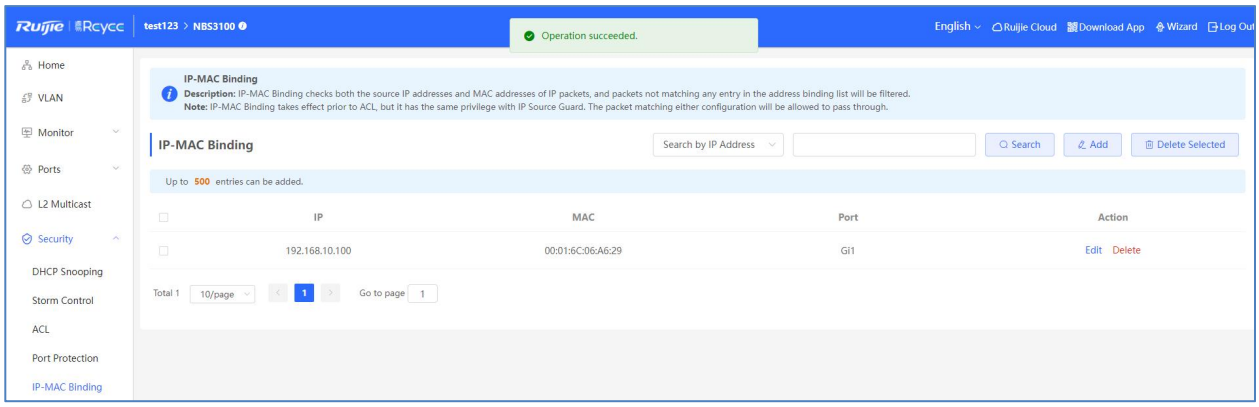
The message "Operation succeeded." is displayed, and the IP-MAC Binding list is updated.



Alternatively, click **Edit** in the **Action** column, configure parameters, and click **OK.**

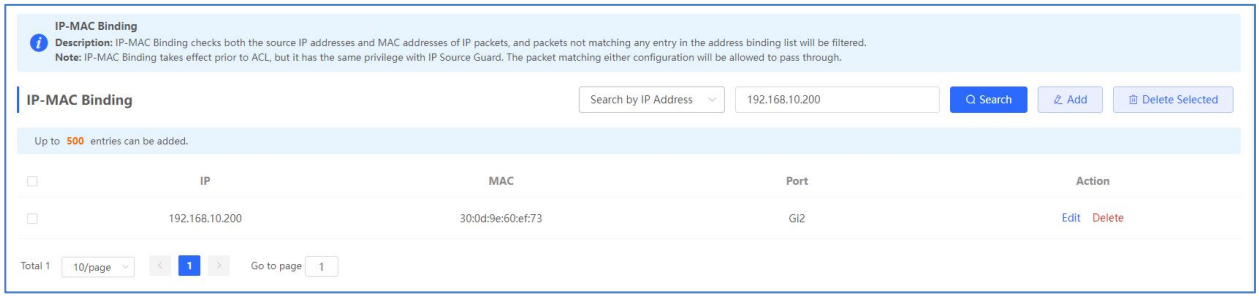


The message "Operation succeeded." is displayed, and the IP-MAC Binding list is updated.

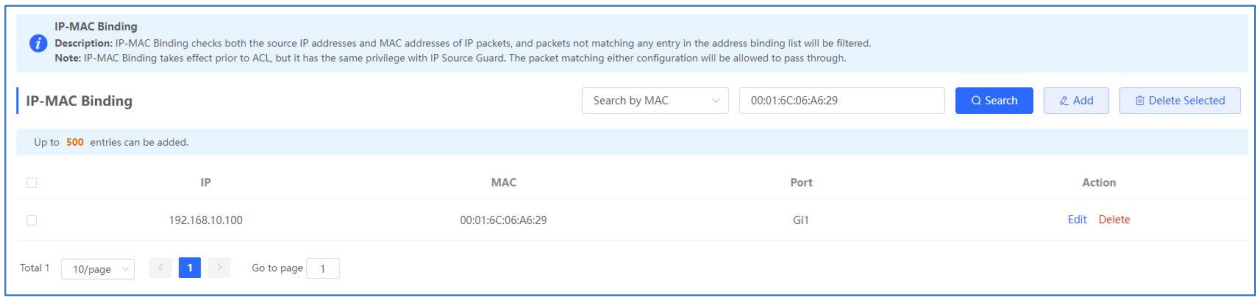


Select a search type (**Search by IP Address**, **Search by MAC**, or **Search by Port**) from the dropdown list, enter the term to be searched for, and click **Search**.

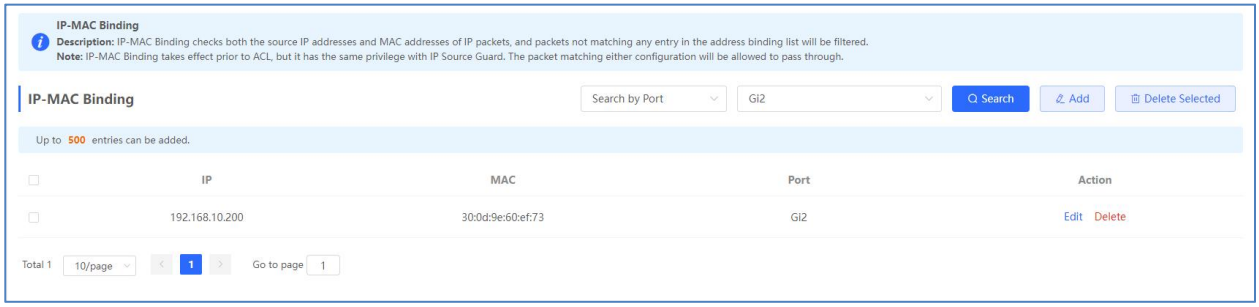
Search by IP Address



Search by MAC



Search by Port

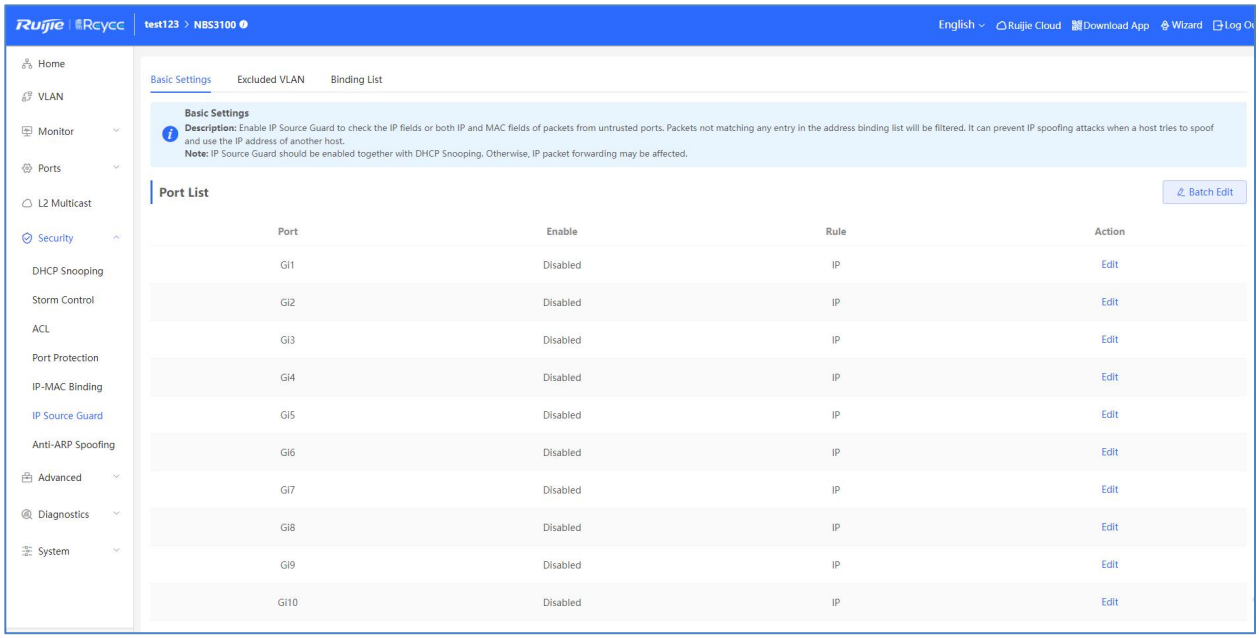


4.3.5.6 IP Source Guard

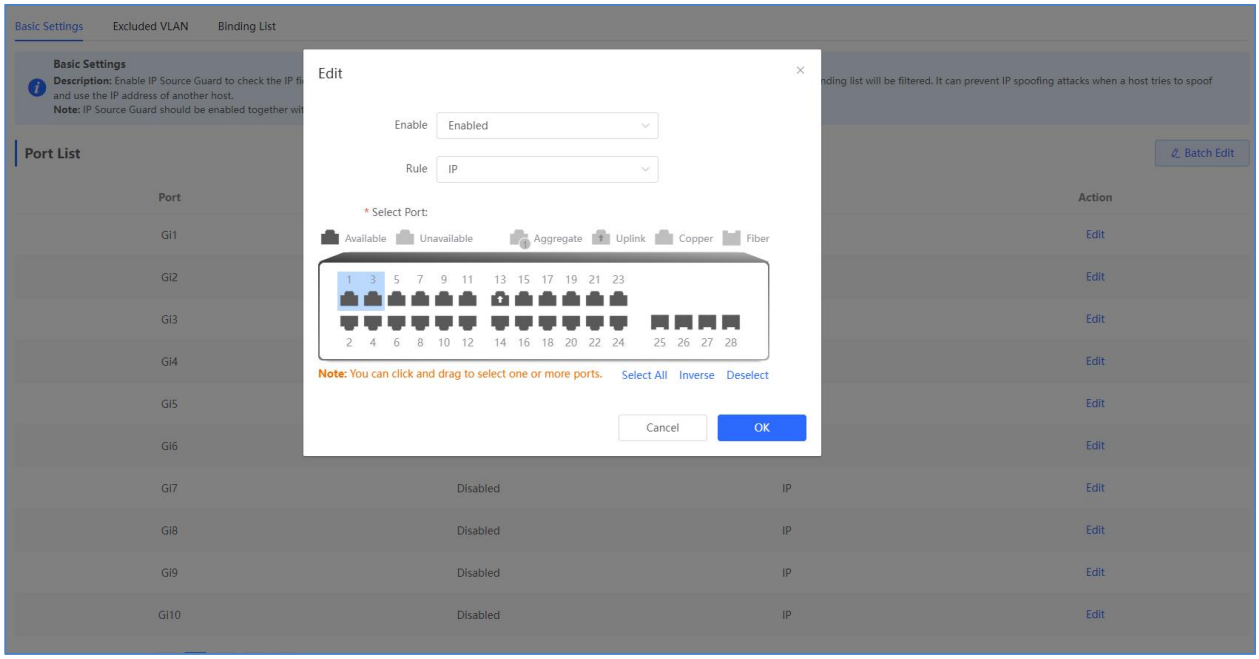
Enable IP Source Guard to check the IP fields or both IP and MAC fields of packets from the untrusted ports. Packets not matching any entry in the address binding list will be filtered. It can prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

1.1 Basic Settings

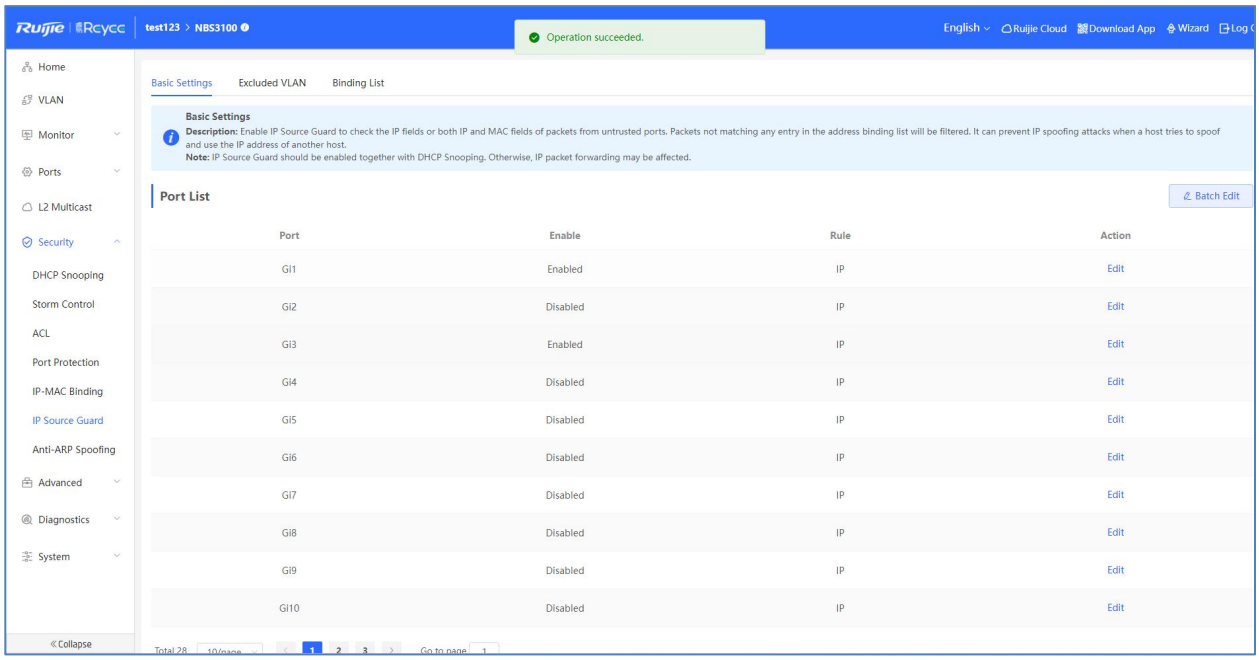
IP Source Guard should be enabled together with DHCP Snooping. Otherwise, IP packet forwarding may be affected.



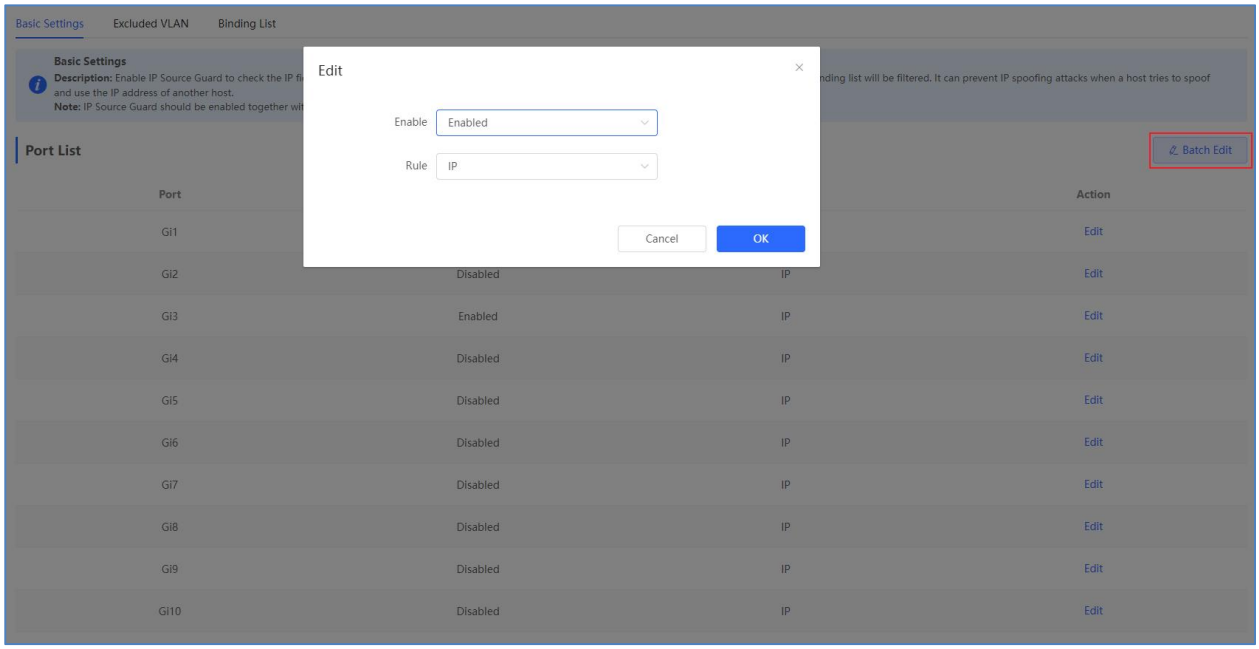
Click **Batch Edit**, select ports, and configure parameters, and click **OK.**



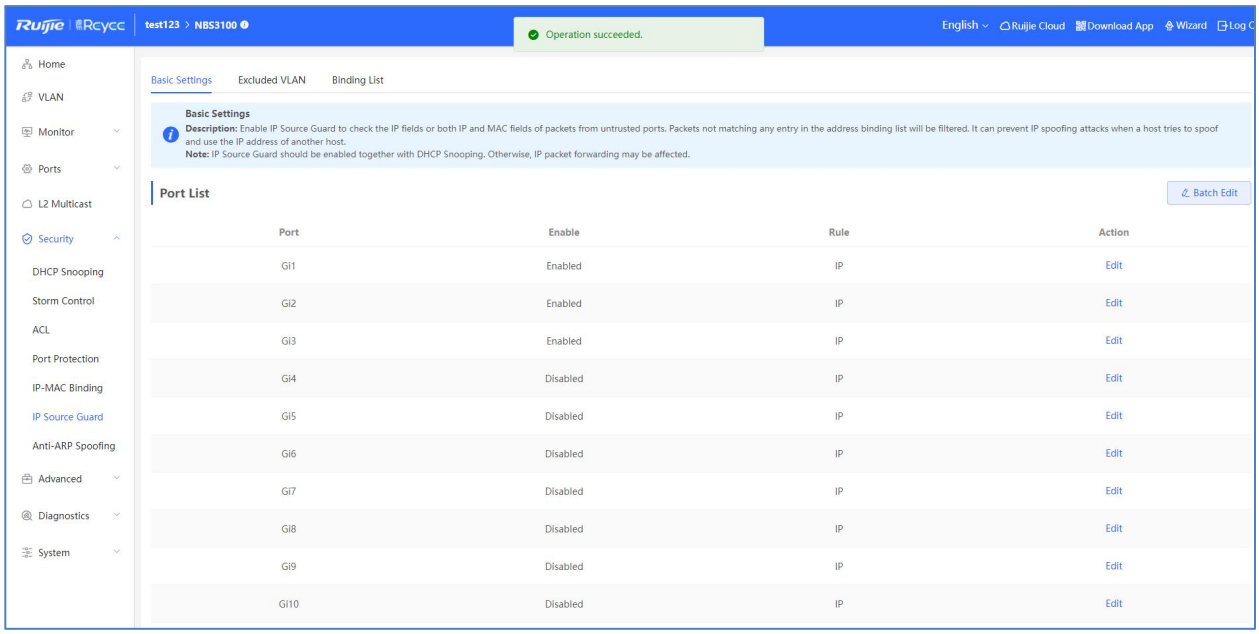
The message "Operation succeeded." is displayed, and the port list is updated.



Alternatively, click **Edit** in the **Action** column, configure parameters, and click **OK.**



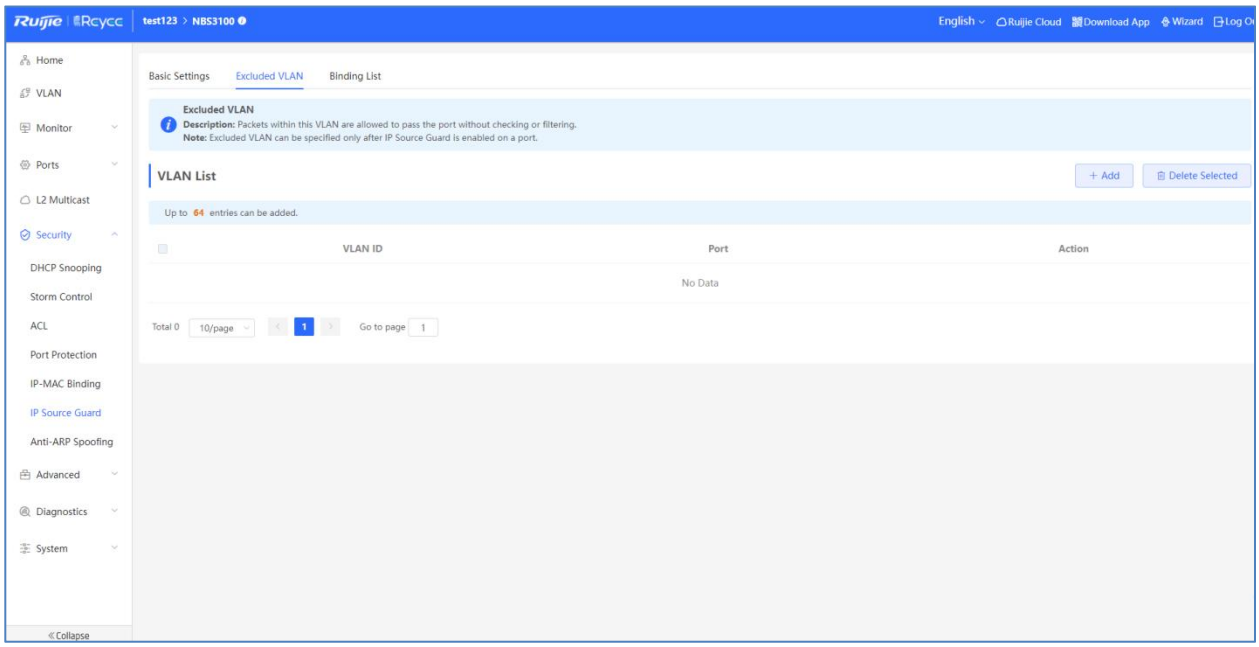
The message "Operation succeeded." is displayed, and the port list is updated.



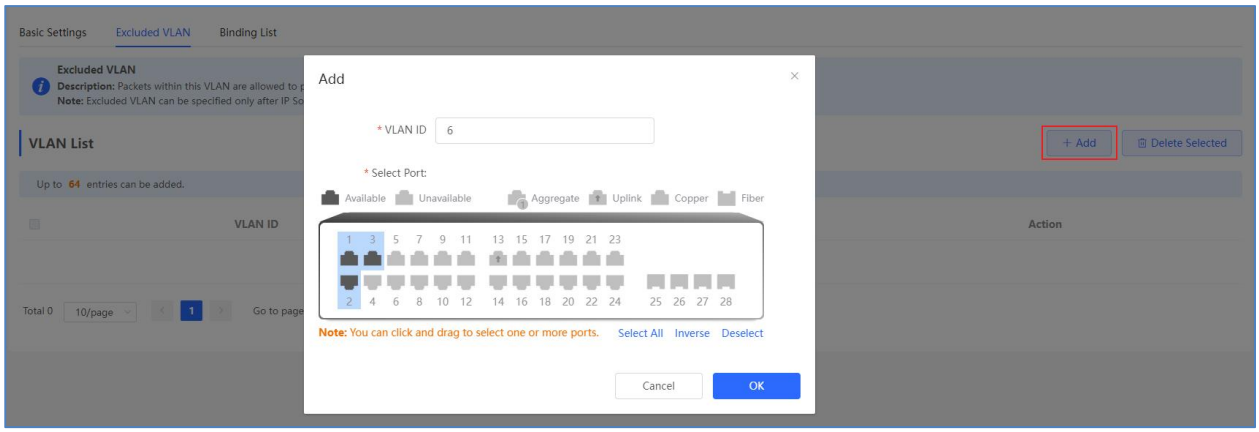
1.2 Excluded VLAN

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

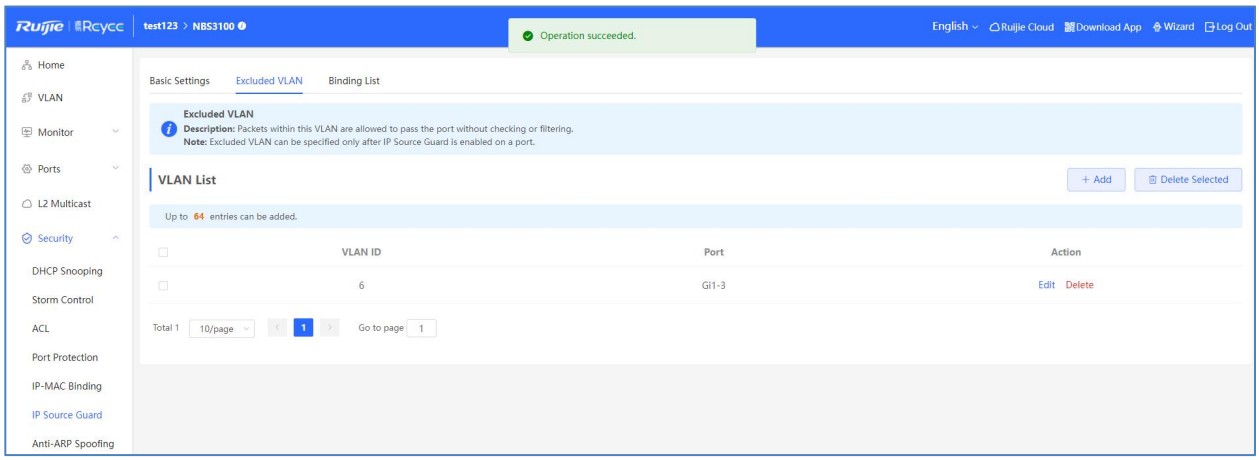
Excluded VLAN can be specified only after IP Source Guard is enabled on the port.



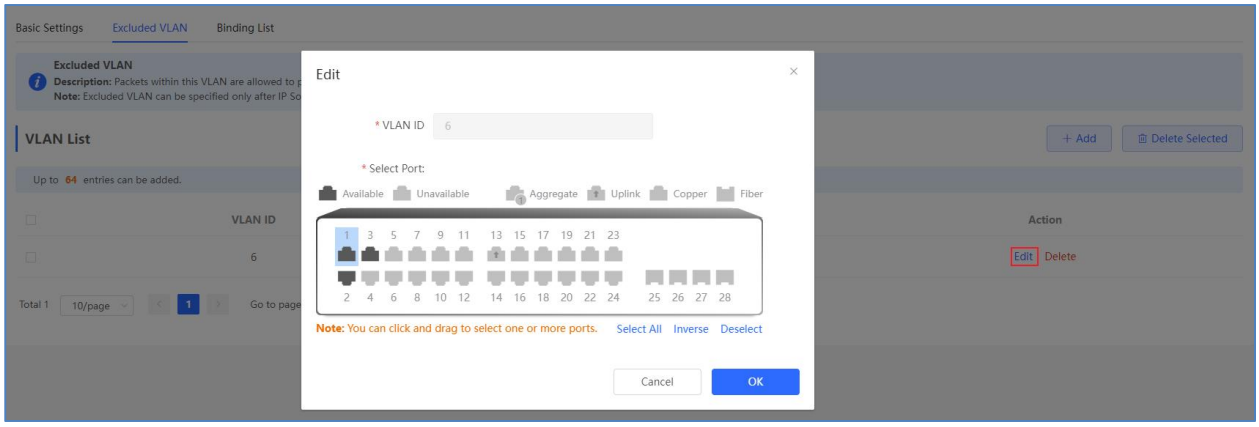
Click **Add,** select ports and configure parameters, and click **OK.**



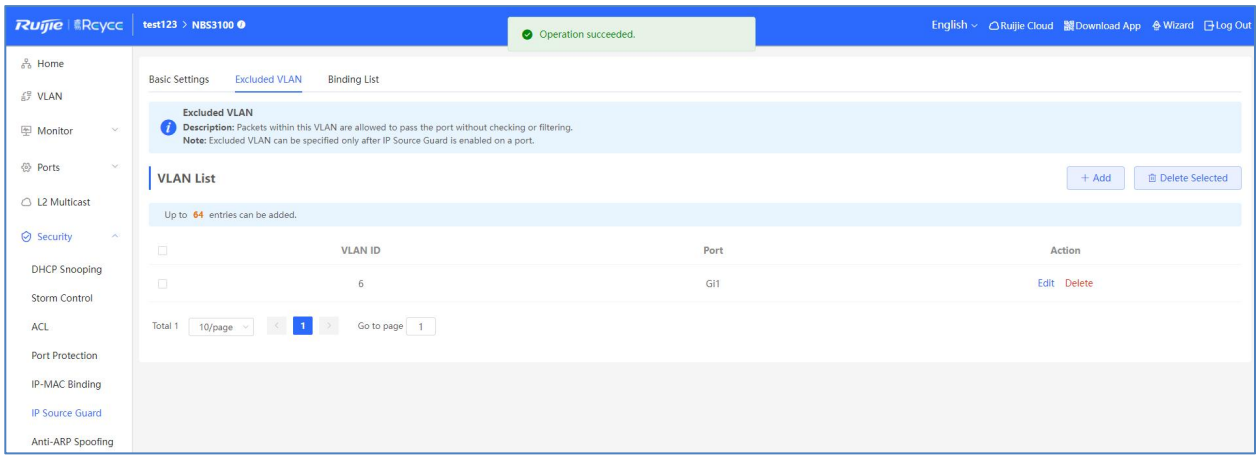
The message "Operation succeeded." is displayed, and the VLAN list is updated.



Alternatively, click **Edit** in the **Action** column, configure parameters, and click **OK.**

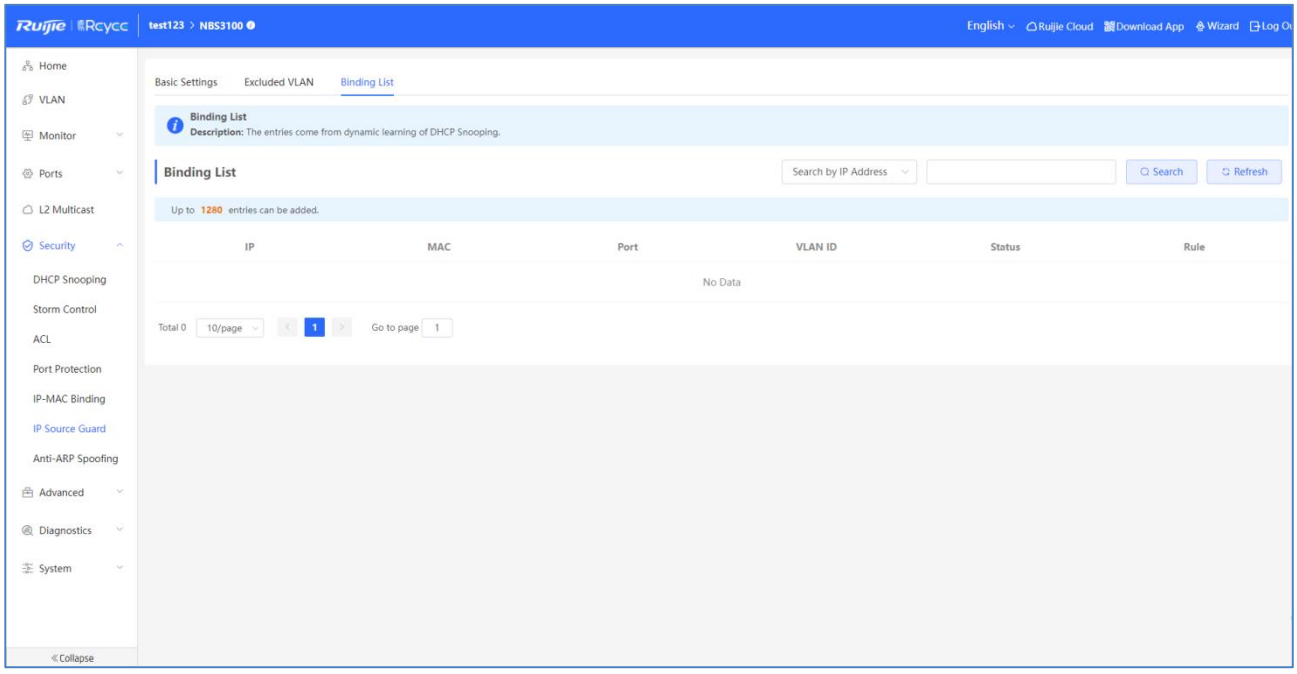


The message "Operation succeeded." is displayed, and the VLAN list is updated.

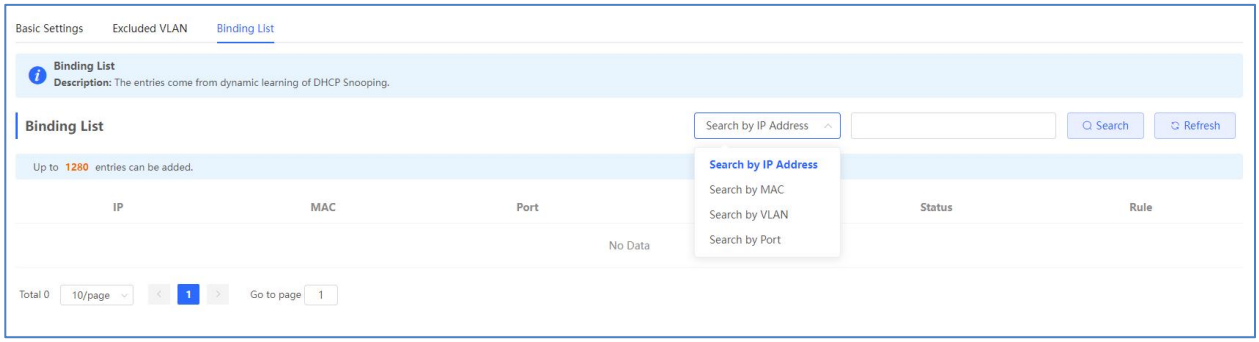


1.3 Binding List

The entries come from dynamic learning of DHCP Snooping.



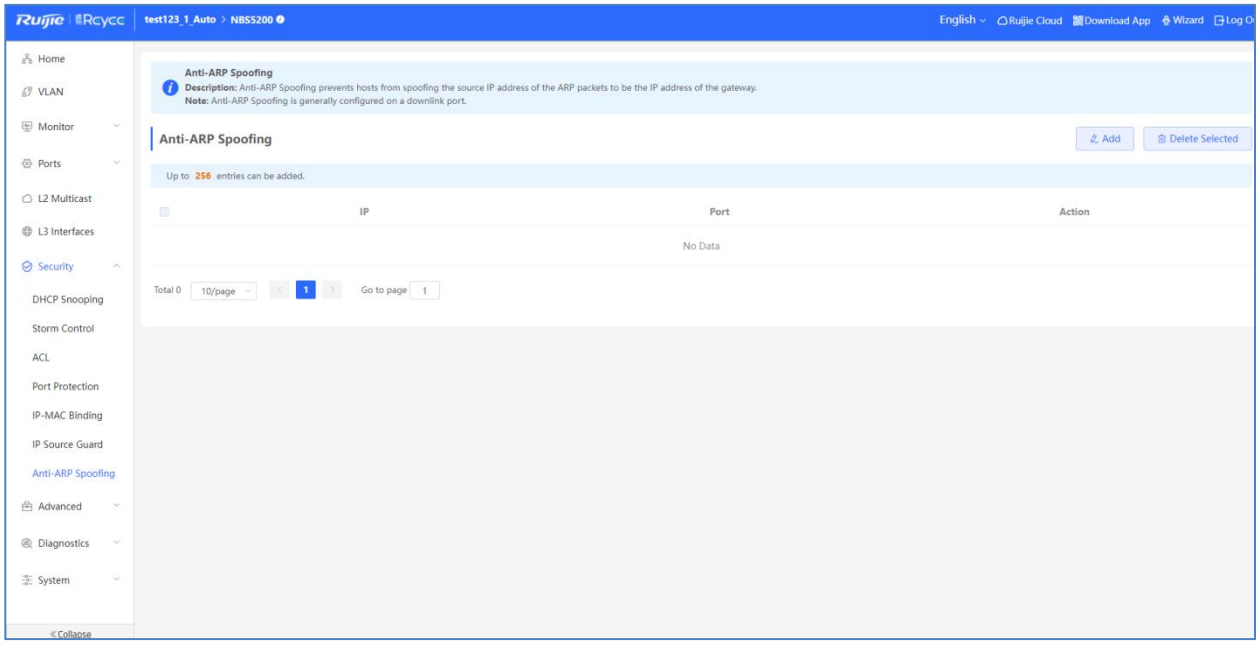
Select a search type (**Search by IP Address**, **Search by MAC**, **Search by VLAN** or **Search by Port**) from the dropdown list, enter the term to be searched for, and click **Search.**



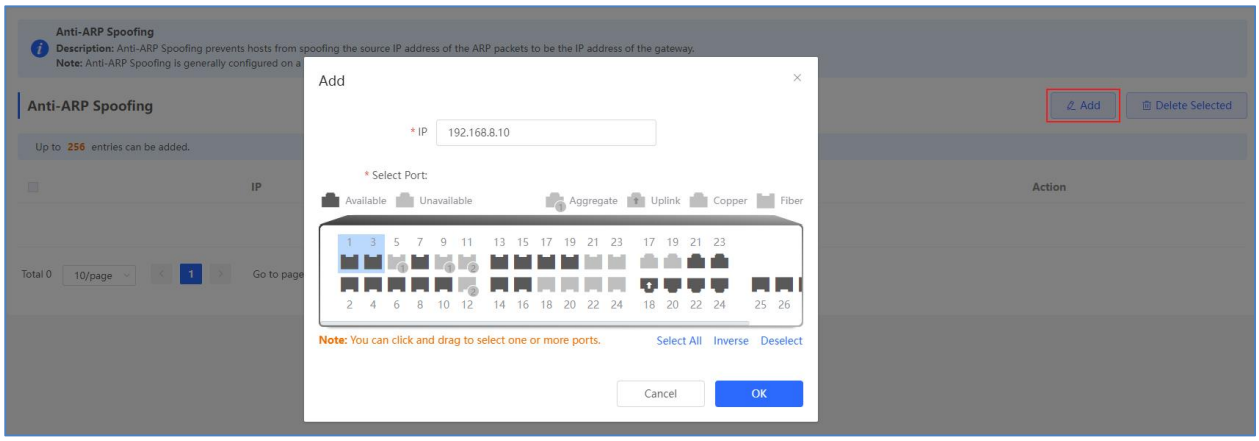
4.3.5.7 Anti-ARP Spoofing

Anti-ARP spoofing prevents hosts from spoofing the source IP address of the ARP packets to be the IP address of the gateway.

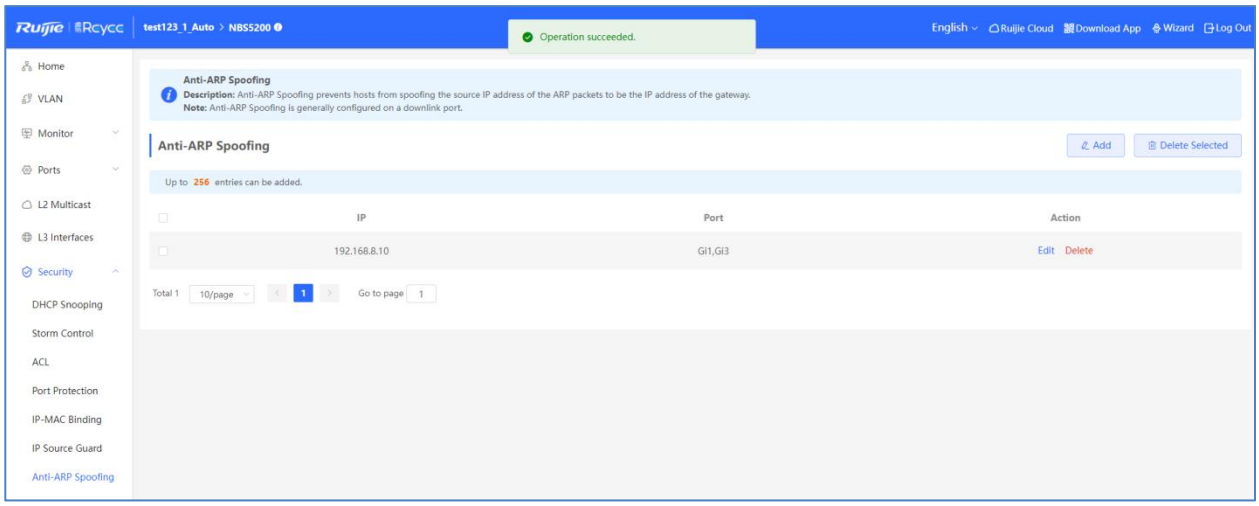
Anti-ARP Spoofing is generally configured on a downlink port.



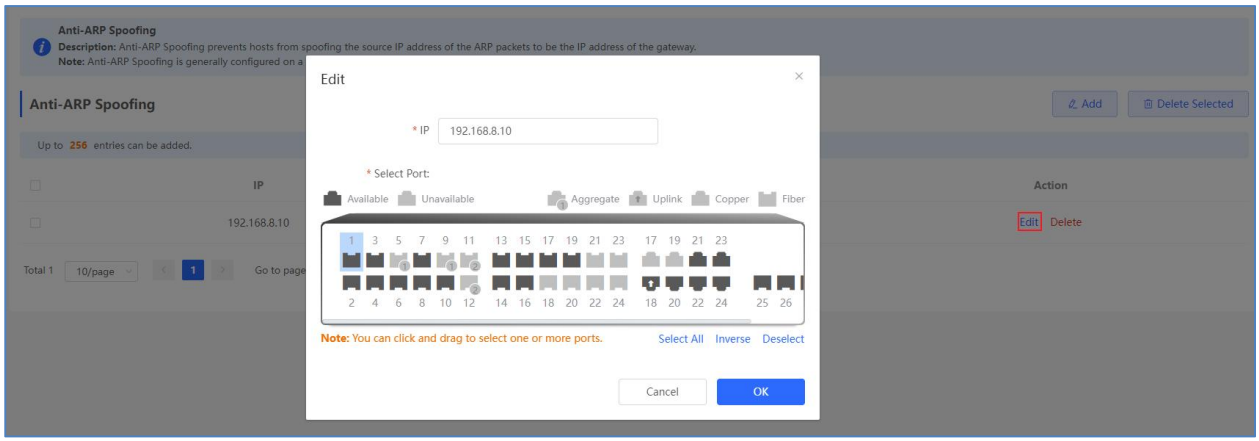
Click **Add,** select ports and configure parameters, and click OK.



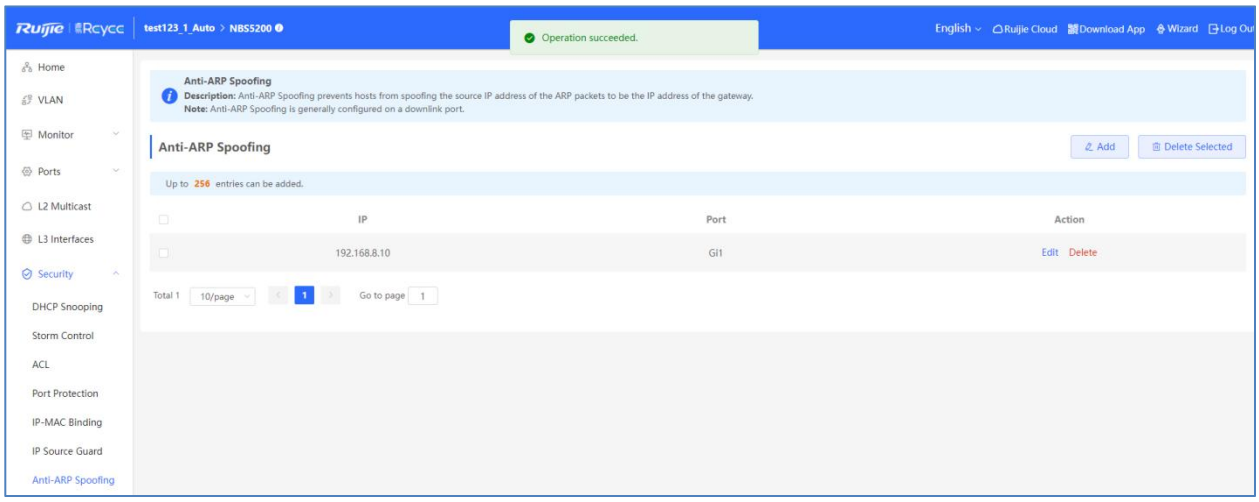
The message "Operation succeeded." is displayed, and the Anti-ARP Spoofing list is updated.



Alternatively, click Edit in the Action column, configure parameters, and click OK.



The message "Operation succeeded." is displayed, and the Anti-ARP Spoofing list is updated.

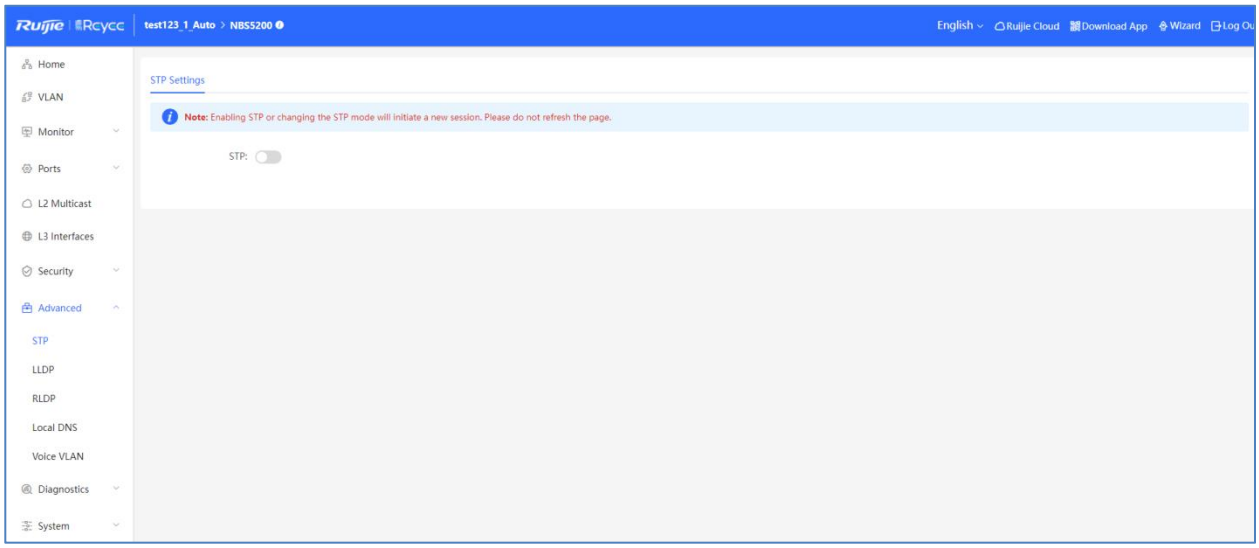


4.3.6 Advanced

The **Advanced** module includes **STP**, **LLDP**, **RLDP**, **Local DNS** and **Voice VLAN**.

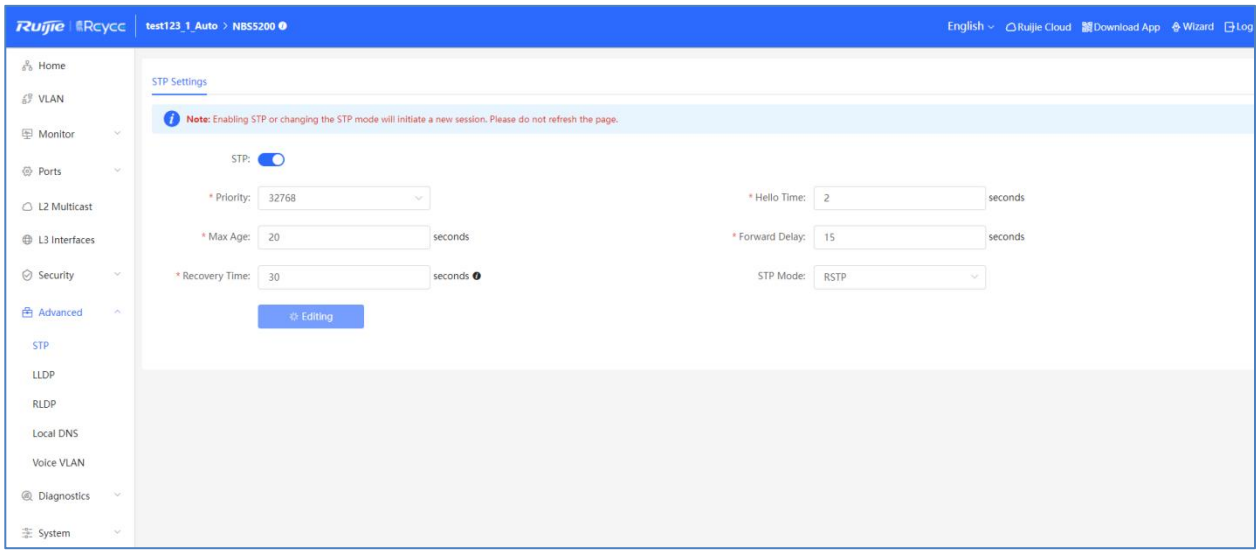
4.3.6.1 STP

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

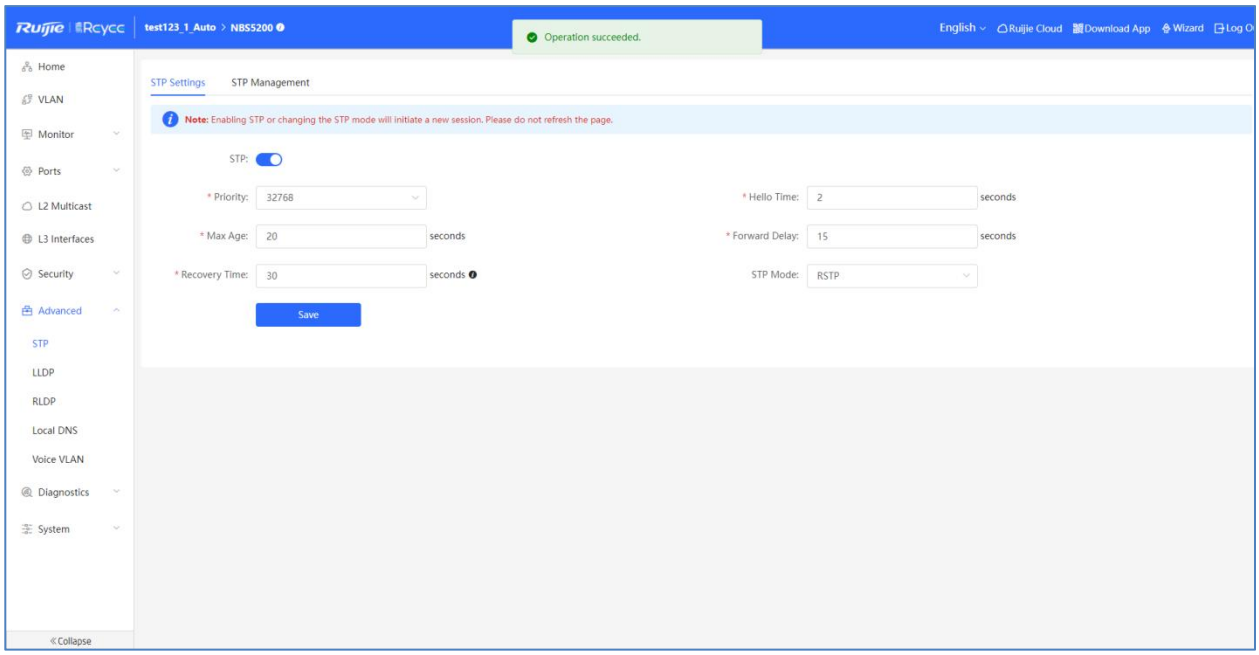


1.1 STP Settings

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

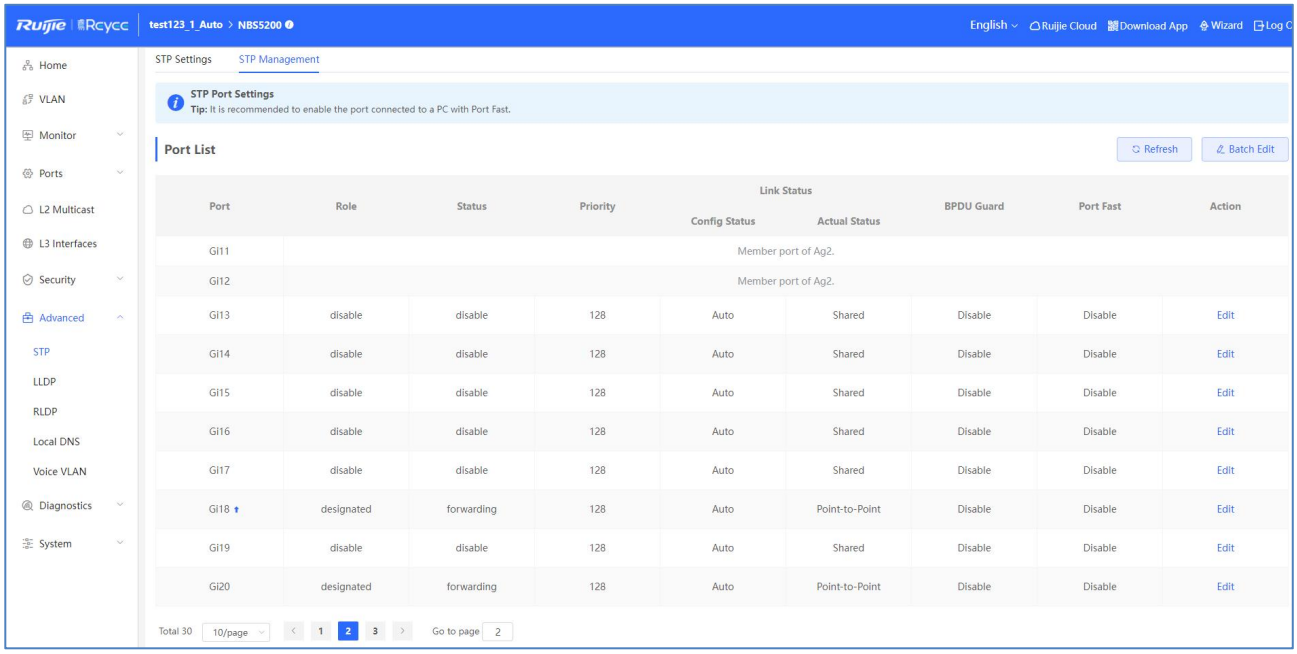


The message "Operation succeeded." is displayed which means that the parameters of STP have been dilivered successfully, and then, the page of STP management will appear..



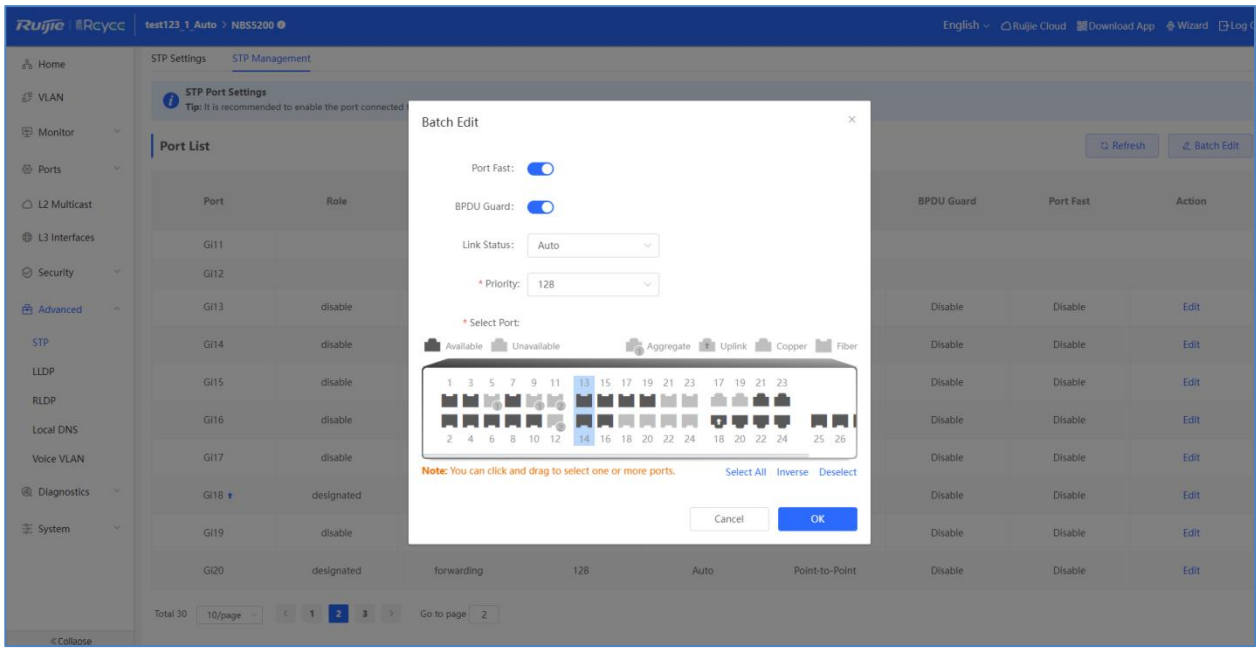
Enabling STP or changing the STP mode will initiate a new session. Please do not refresh the page.

1.2 STP Management

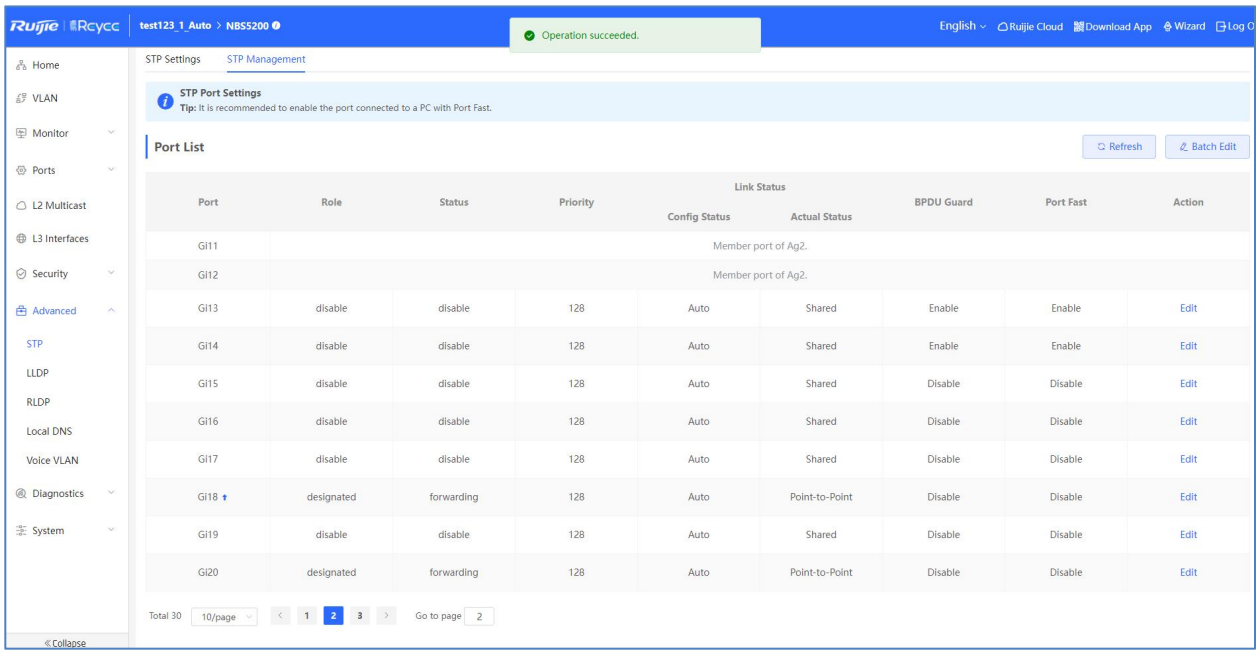


Port	Role	Status	Priority	Link Status		BPDU Guard	Port Fast	Action
				Config Status	Actual Status			
Gi11	Member port of Ag2.							
Gi12	Member port of Ag2.							
Gi13	disable	disable	128	Auto	Shared	Disable	Disable	Edit
Gi14	disable	disable	128	Auto	Shared	Disable	Disable	Edit
Gi15	disable	disable	128	Auto	Shared	Disable	Disable	Edit
Gi16	disable	disable	128	Auto	Shared	Disable	Disable	Edit
Gi17	disable	disable	128	Auto	Shared	Disable	Disable	Edit
Gi18	designated	forwarding	128	Auto	Point-to-Point	Disable	Disable	Edit
Gi19	disable	disable	128	Auto	Shared	Disable	Disable	Edit
Gi20	designated	forwarding	128	Auto	Point-to-Point	Disable	Disable	Edit

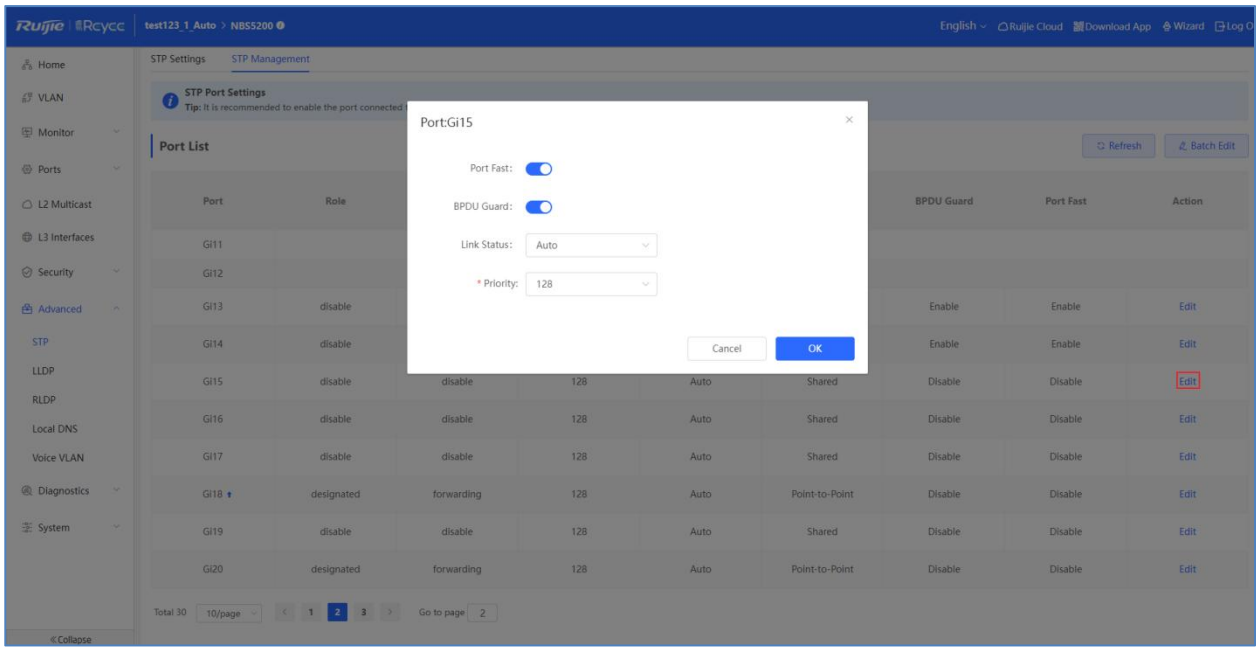
Click **Batch Edit,** select ports, and configure parameters.



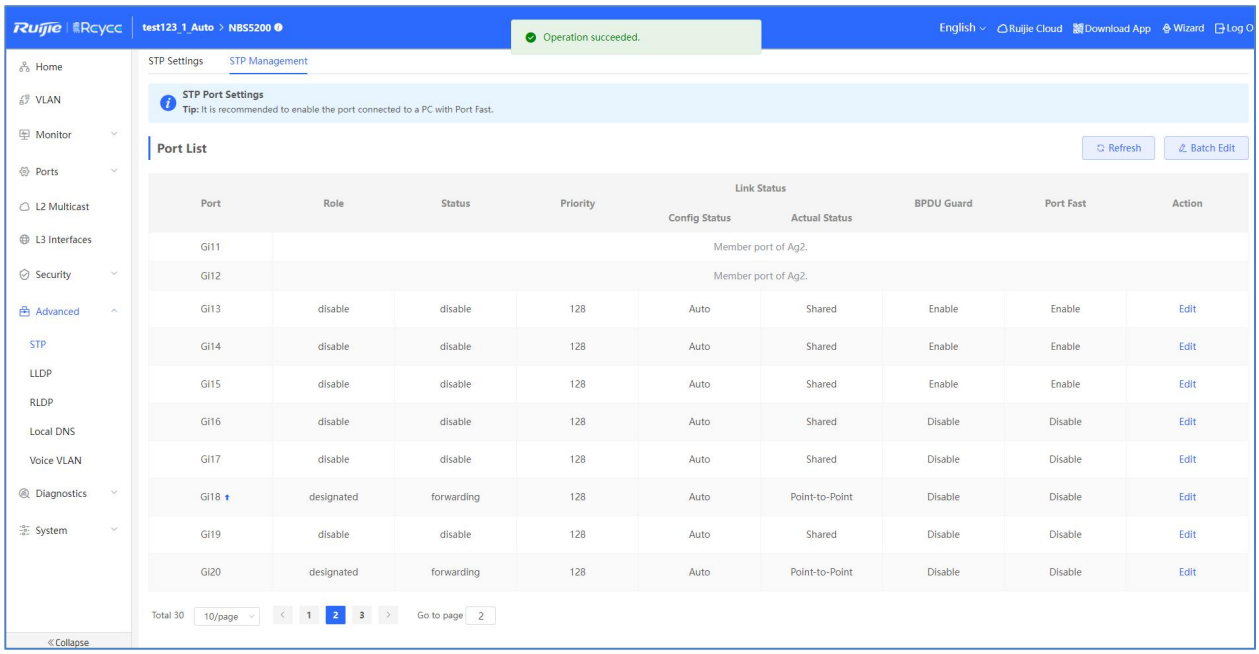
The message "Operation succeeded." is displayed, and the port list is updated.



Alternatively, click **Edit** in the Action column, configure parameters, and click **OK**.



The message "Operation succeeded." is displayed, and the port list is updated.



It is recommended to enable Port Fast on the port connected to a PC.

When there is a loop occur, the port having a loop will be blocked, which could be seen in the STP Management page.

Port List

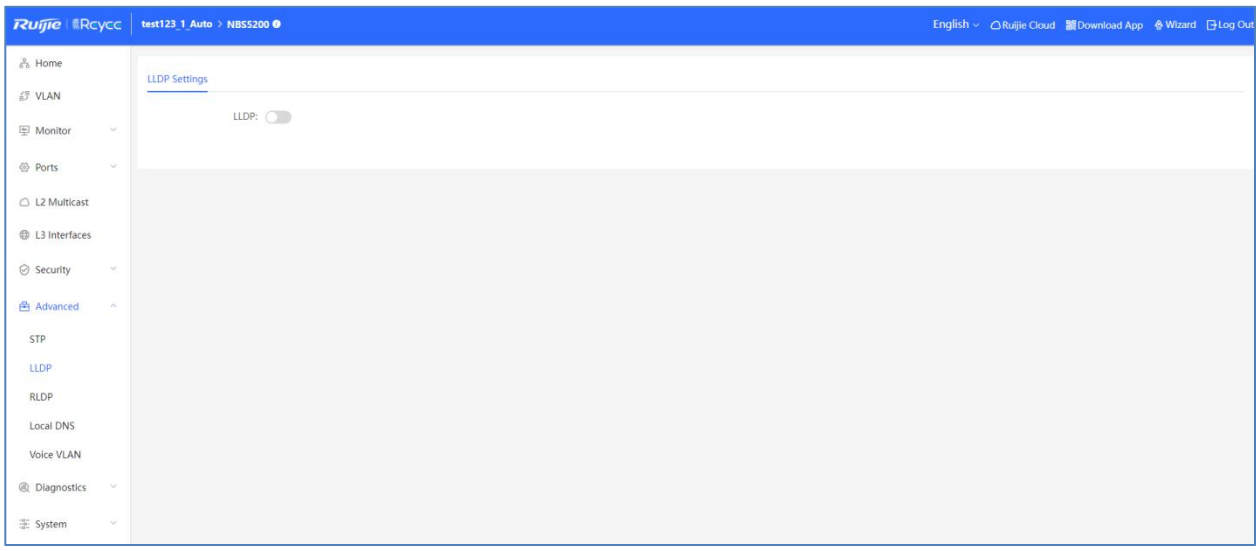
Refresh Batch Edit

Port	Role	Status	Priority	Link Status		BPDU Guard	Port Fast	Action
				Config Status	Actual Status			
Gi11	Member port of Ag2.							
Gi12	Member port of Ag2.							
Gi13	disable	disable	128	Auto	Shared	Enable	Enable	Edit
Gi14	disable	disable	128	Auto	Shared	Enable	Enable	Edit
Gi15	disable	disable	128	Auto	Shared	Enable	Enable	Edit
Gi16	disable	disable	128	Auto	Shared	Disable	Disable	Edit
Gi17	disable	disable	128	Auto	Shared	Disable	Disable	Edit
Gi18	designated	blocking	128	Auto	Point-to-Point	Disable	Disable	Edit
Gi19	disable	disable	128	Auto	Shared	Disable	Disable	Edit
Gi20	designated	blocking	128	Auto	Point-to-Point	Disable	Disable	Edit

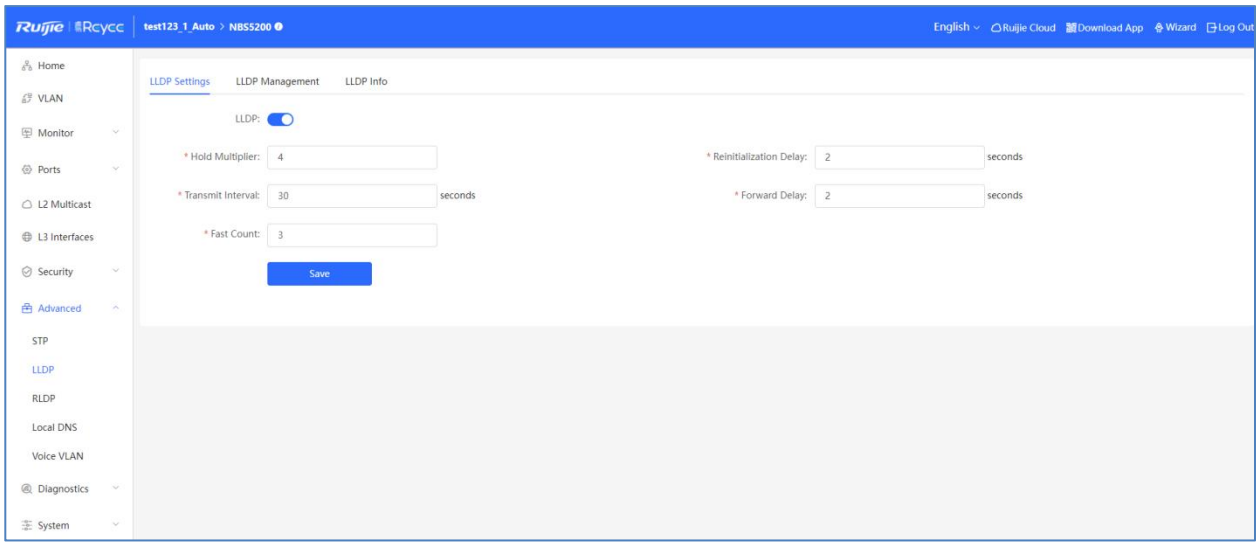
4.3.6.2 LLDP

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

1.1 LLDP Settings

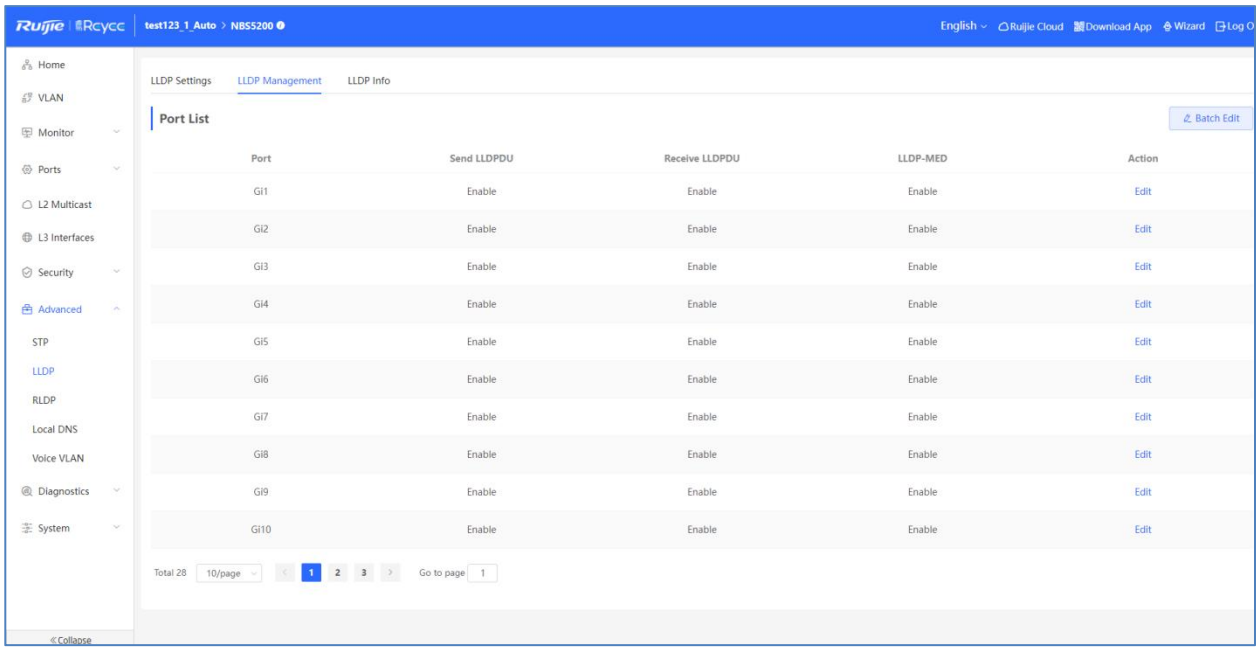


Enable **LLDP**, configure related parameters, and click **Save.**

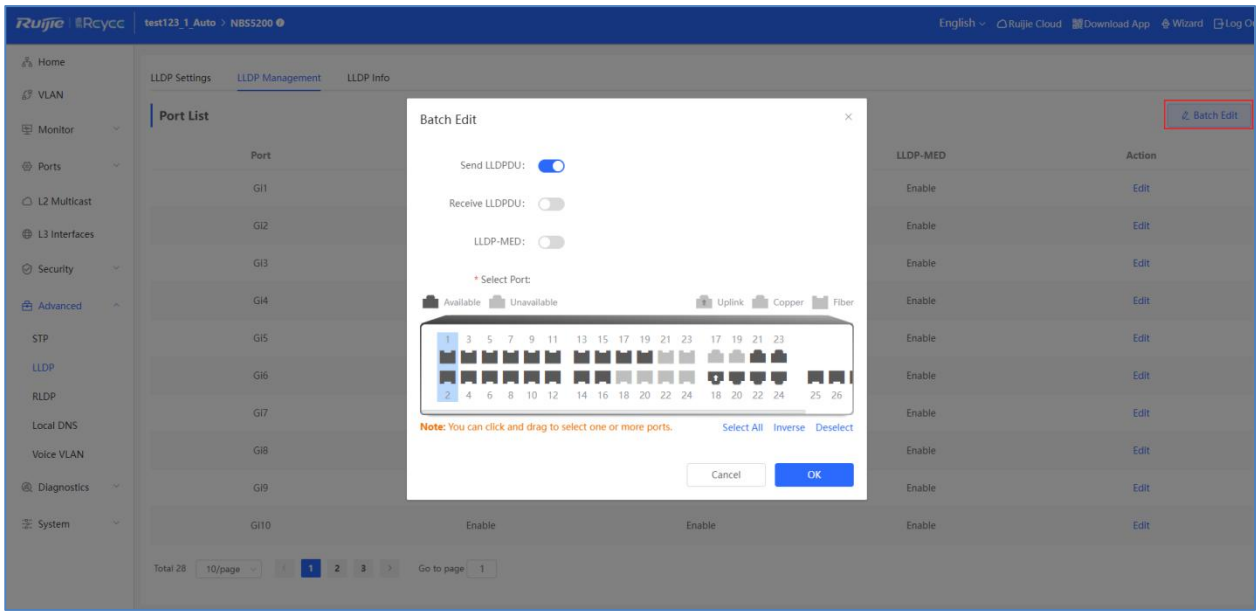


When LLDP is enabled， the pages of LLDP Management and LLDP Info will be displayed.

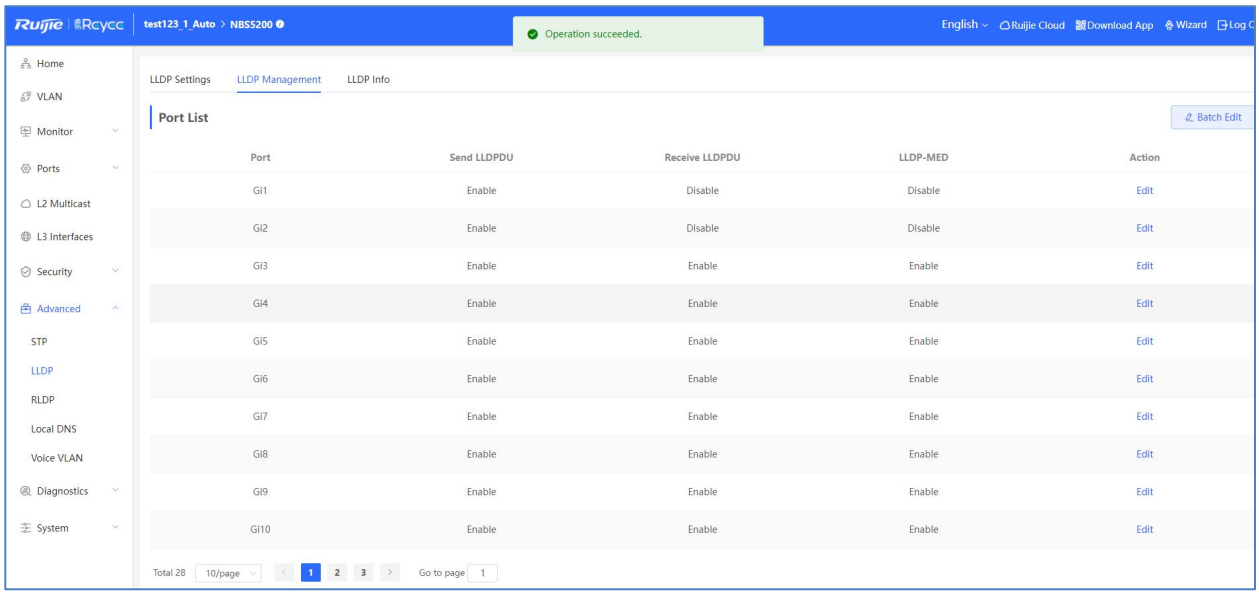
1.2 LLDP Management



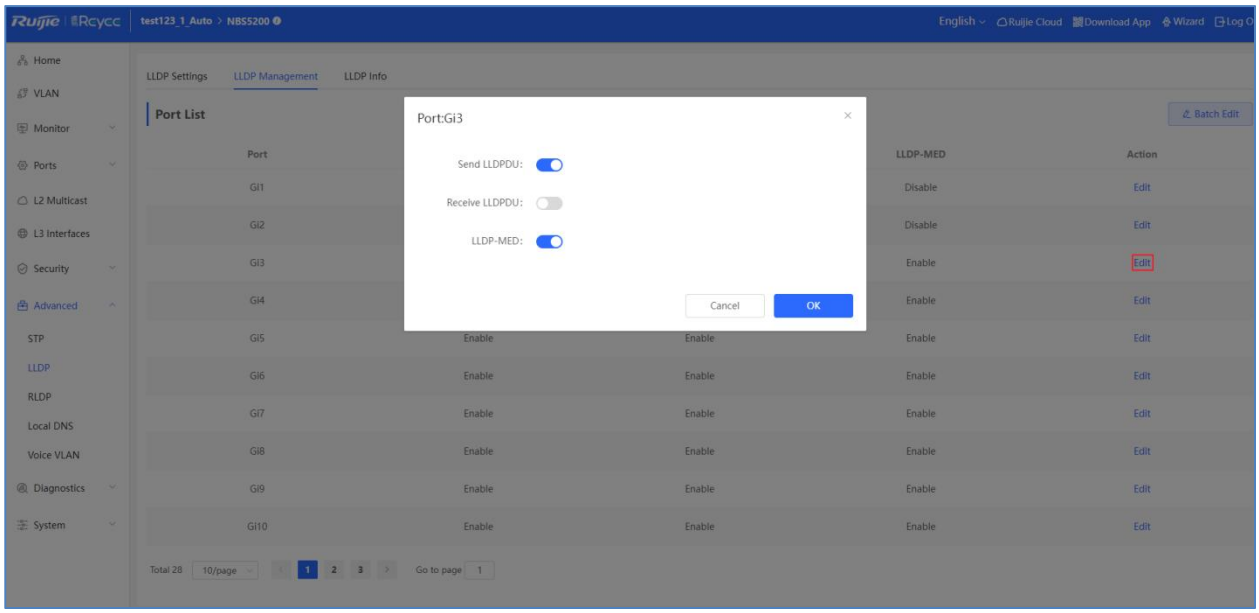
Click **Batch Edit**, select ports, and configure parameters.



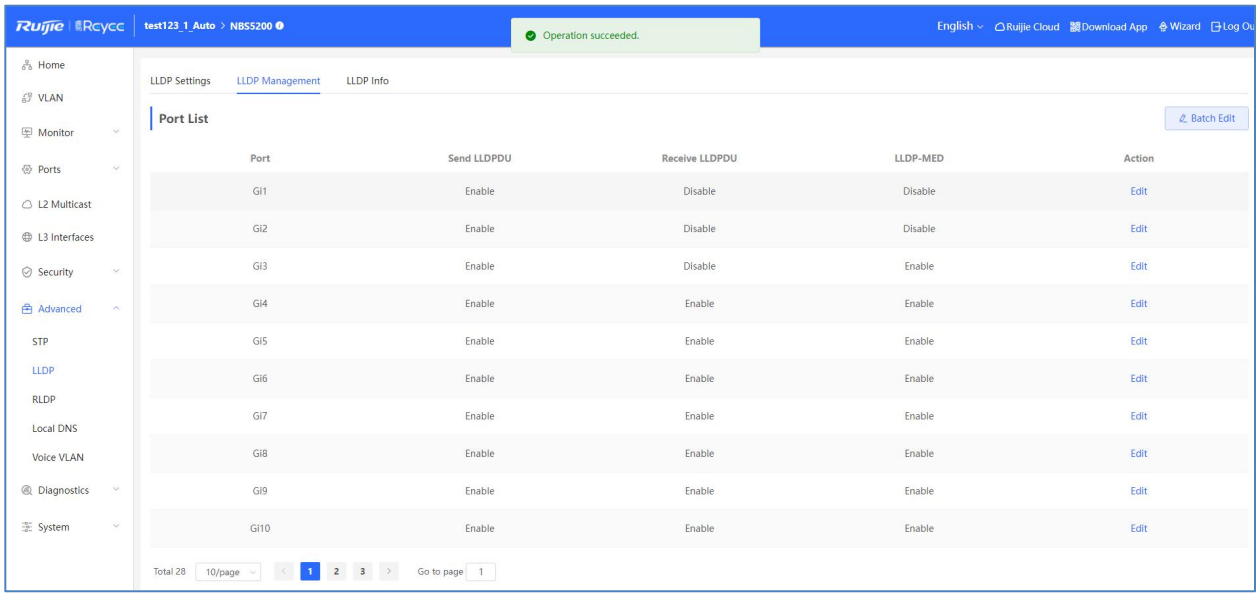
The message "Operation succeeded." is displayed, and the port list is updated.



Alternatively, click **Edit** in the Action column, configure parameters, and click **OK**.

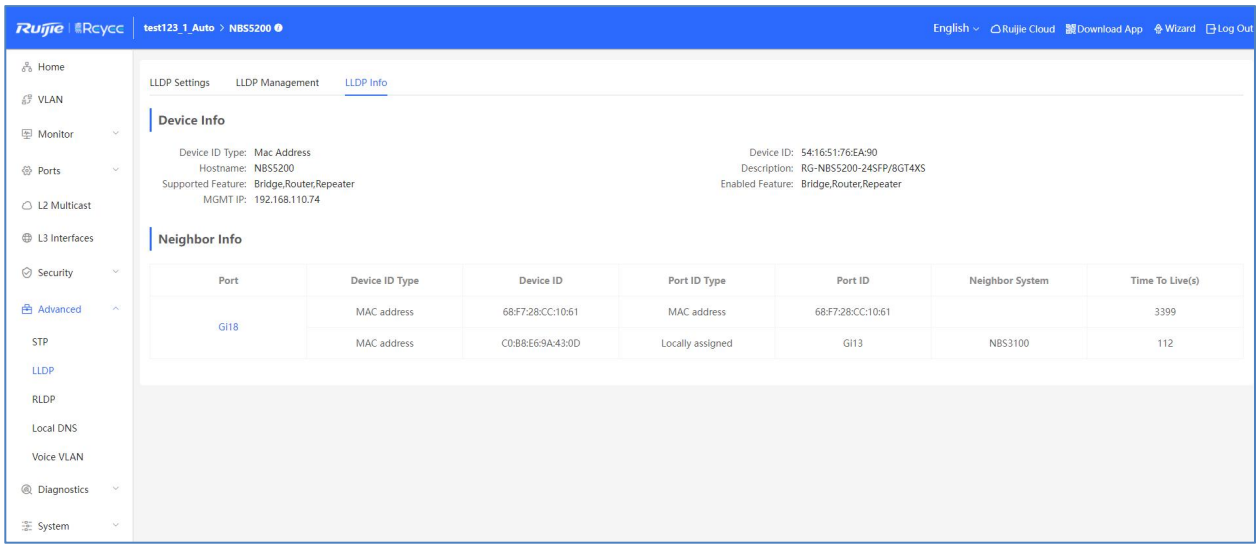


The message "Operation succeeded." is displayed, and the port list is updated.



1.3 LLDP Info

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

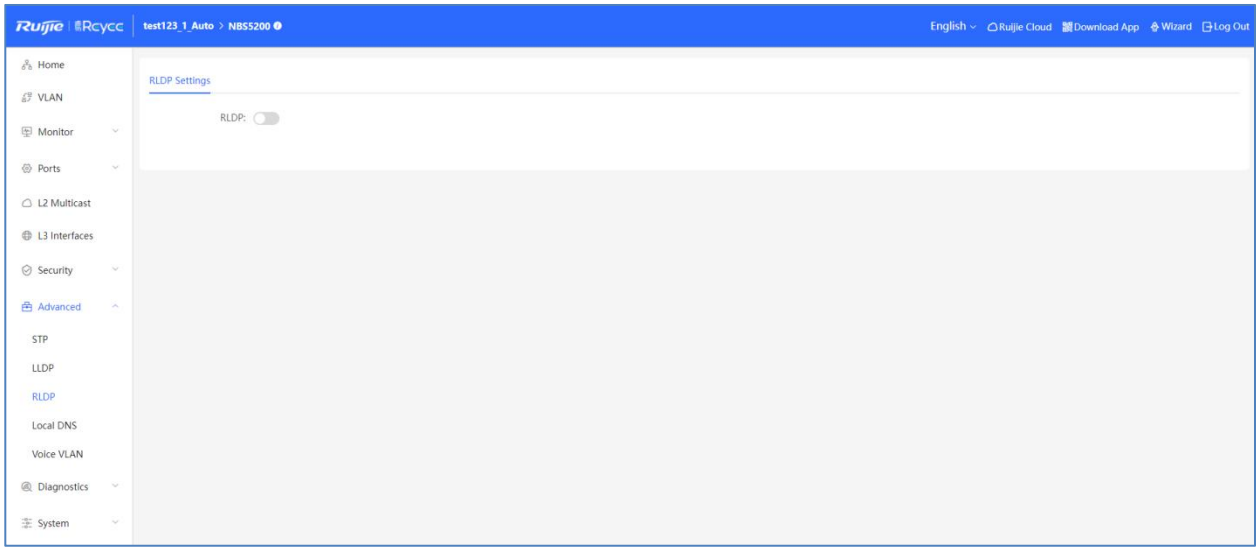


LLDP can be used to display the topological connection status, such as the numbers of switches, MED devices, and NMS devices in the network topology.

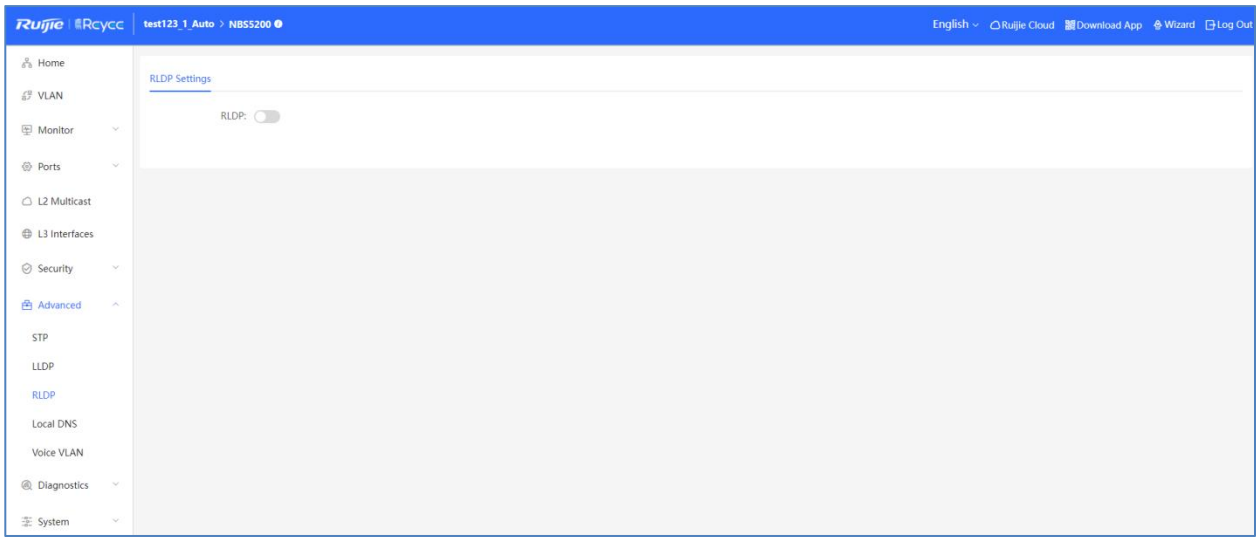
LLDP can be used to detect errors, for example, display incorrect configuration information if two switches are directly connected in the network topology.

4.3.6.3 RLDP

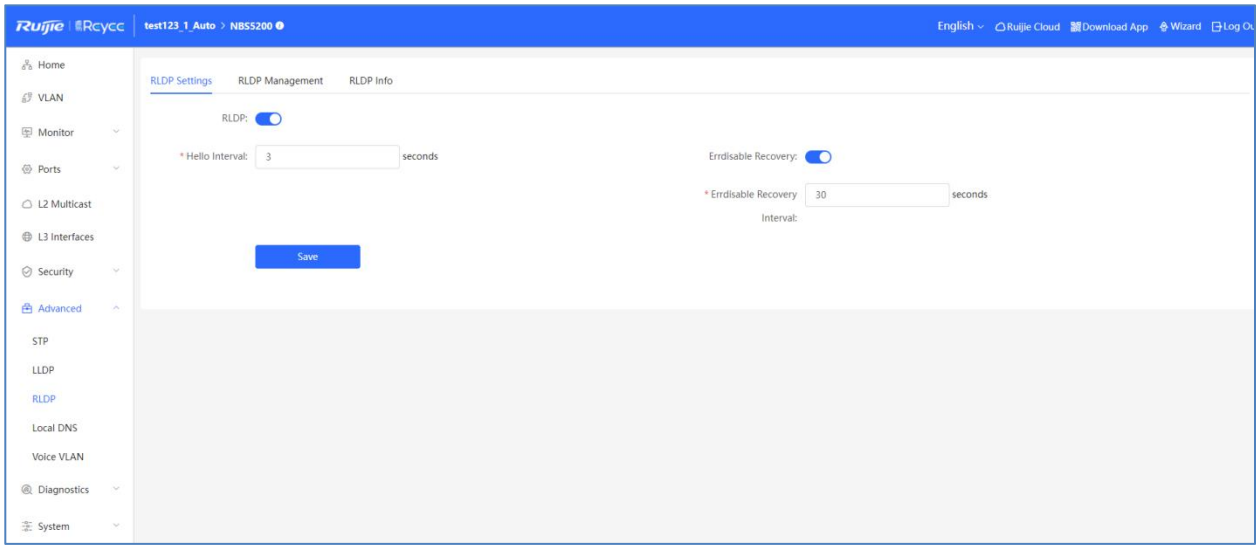
RLDP is used to detect downlink loops. You can select an action among warning, block and shutdown to prevent forwarding loops on a layer-2 network.



1.1 RLDP Settings



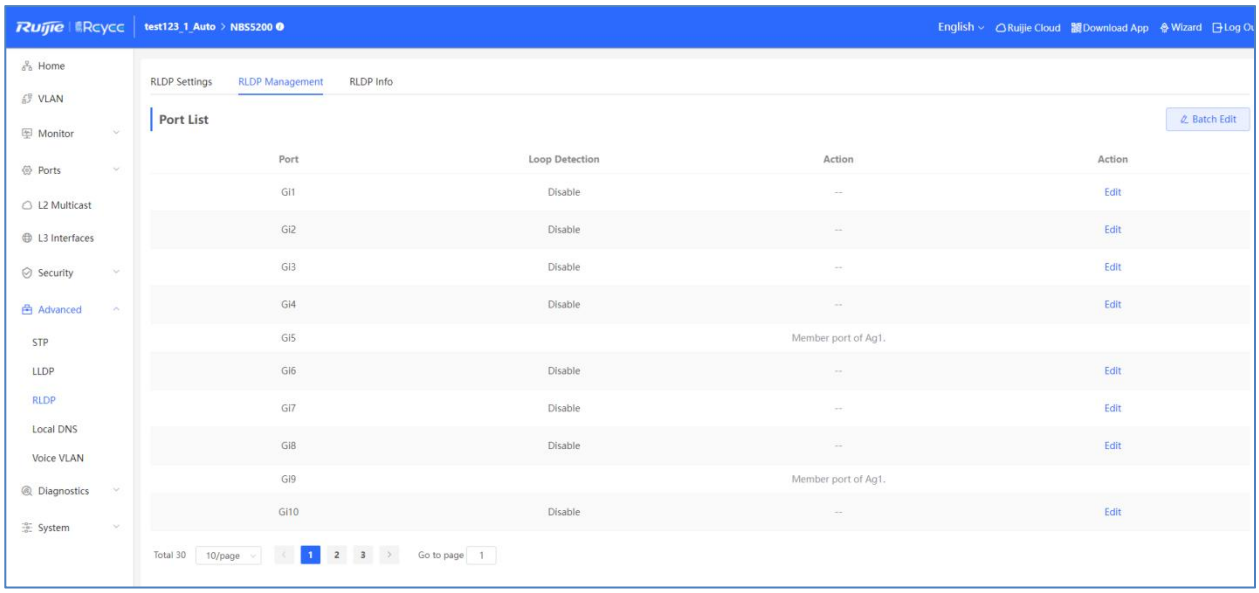
Enable **RLDP**, set global RLDP parameters, and click **Save.**



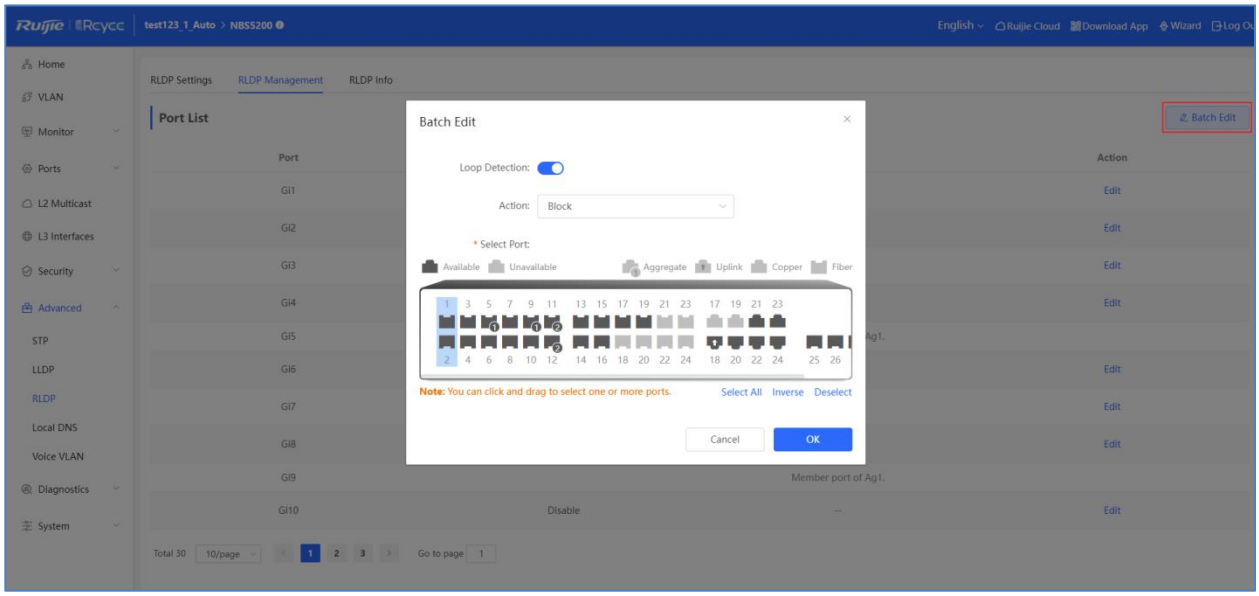
Errdisable Recovery: after the errdisable recovery interval, the port will be restored to its origional status.

When RLDP is enabled, the page of RLDP Management and RLDP Info will ne displayed

1.2 RLDP Management



Click **Batch Edit**, select ports, and configure parameters.



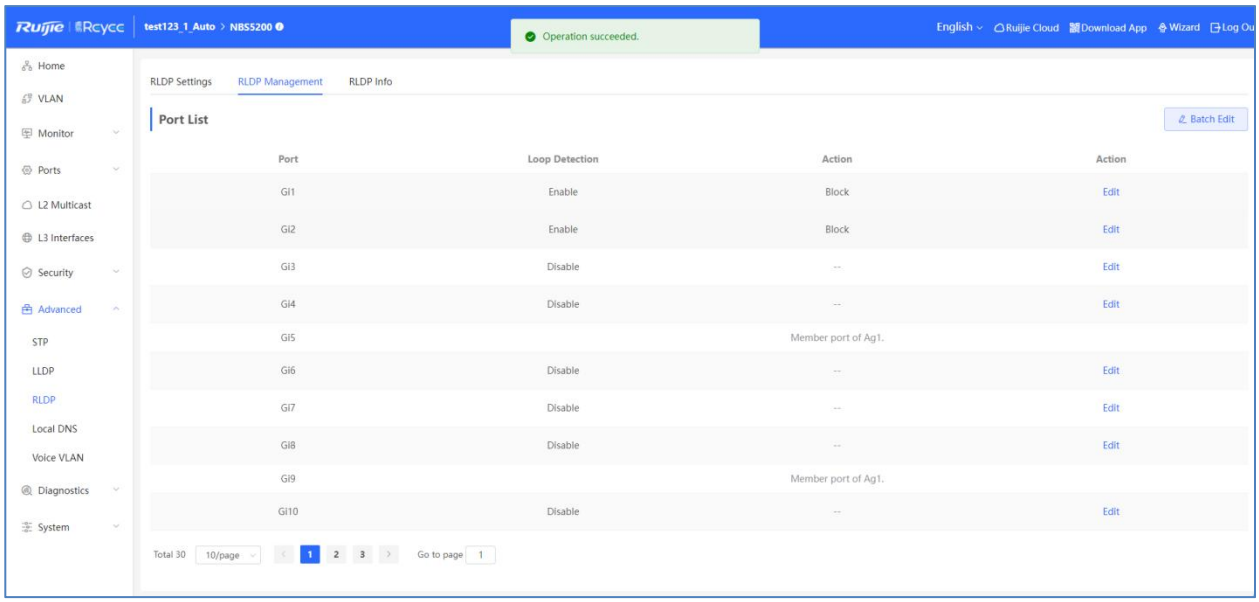
Action

Block: Packets block

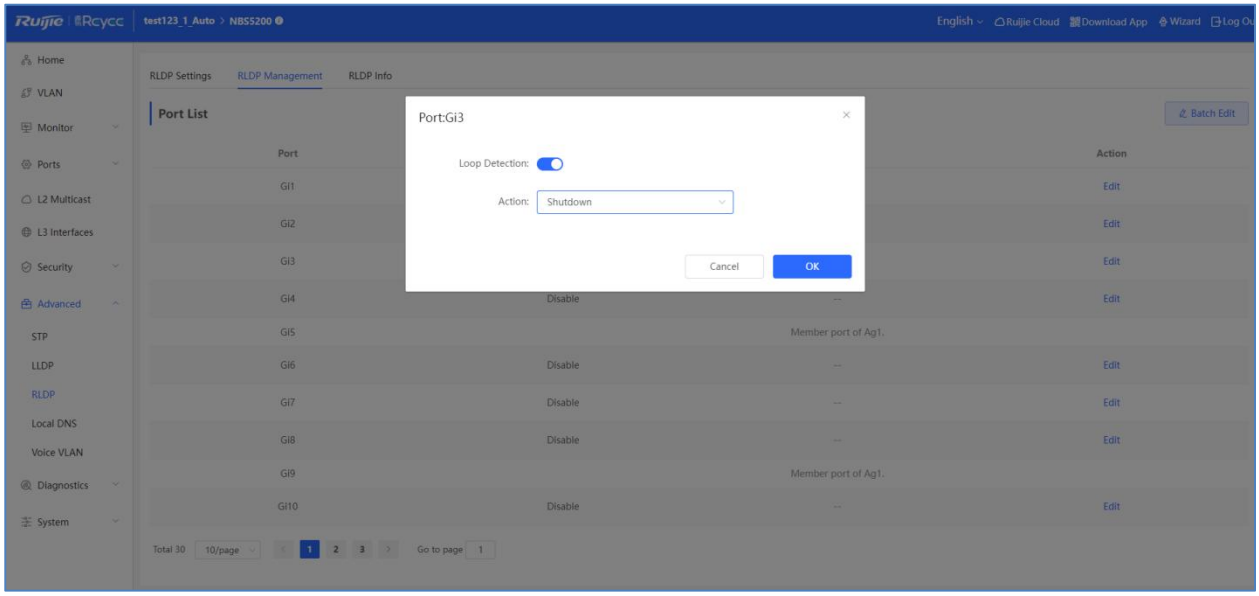
Warning: Only a warning, but packets will not be blocked.

Shutdown: Shut down the looping interface.

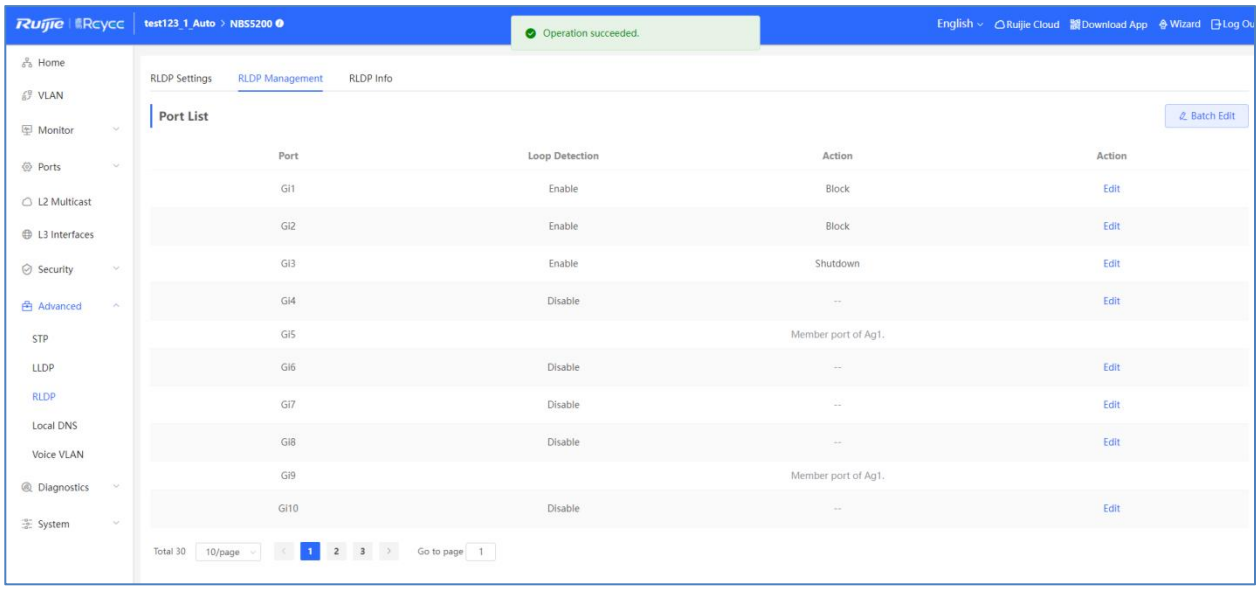
The message "Operation succeeded." is displayed, and the port list is updated.



Alternatively, click **Edit** in the **Action** column, configure parameters, and click **OK.**

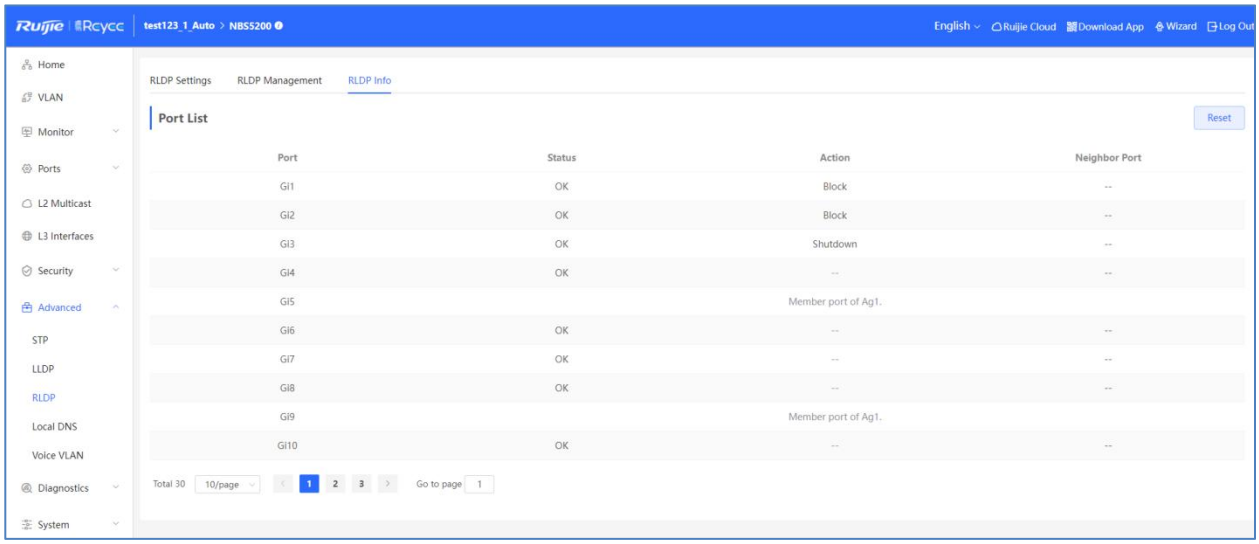


The message "Operation succeeded." is displayed, and the port list is updated.

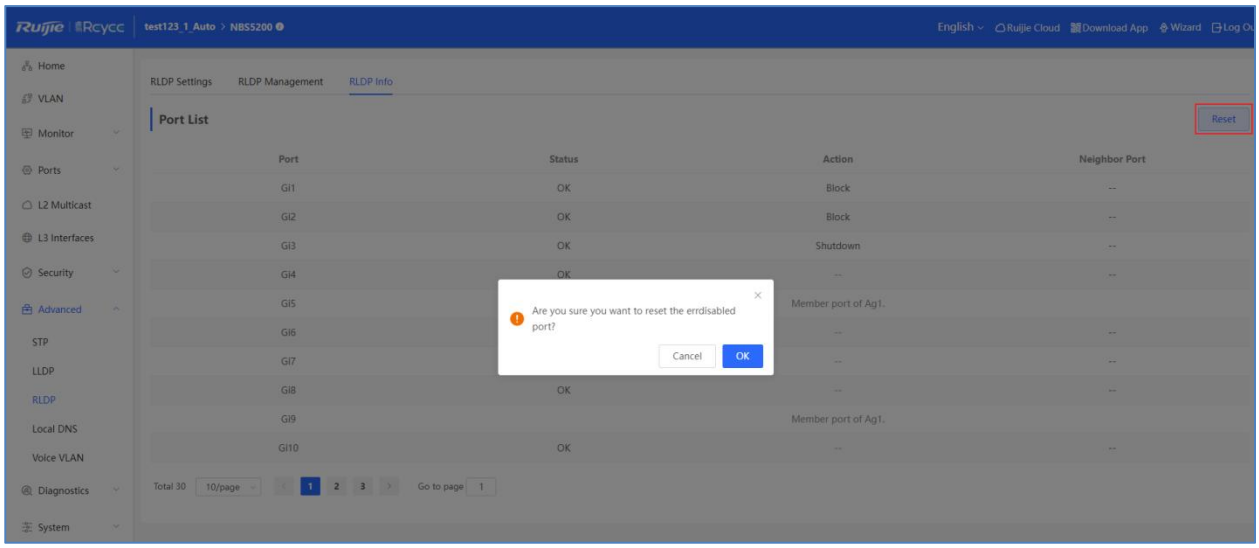


1.3 RLDP Info

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



Click **Reset** to reset the errdisabled port.



When the looping occurs, the RIDP Info will the display the wrong message.

RLDP Settings RLDP Management RLDP Info

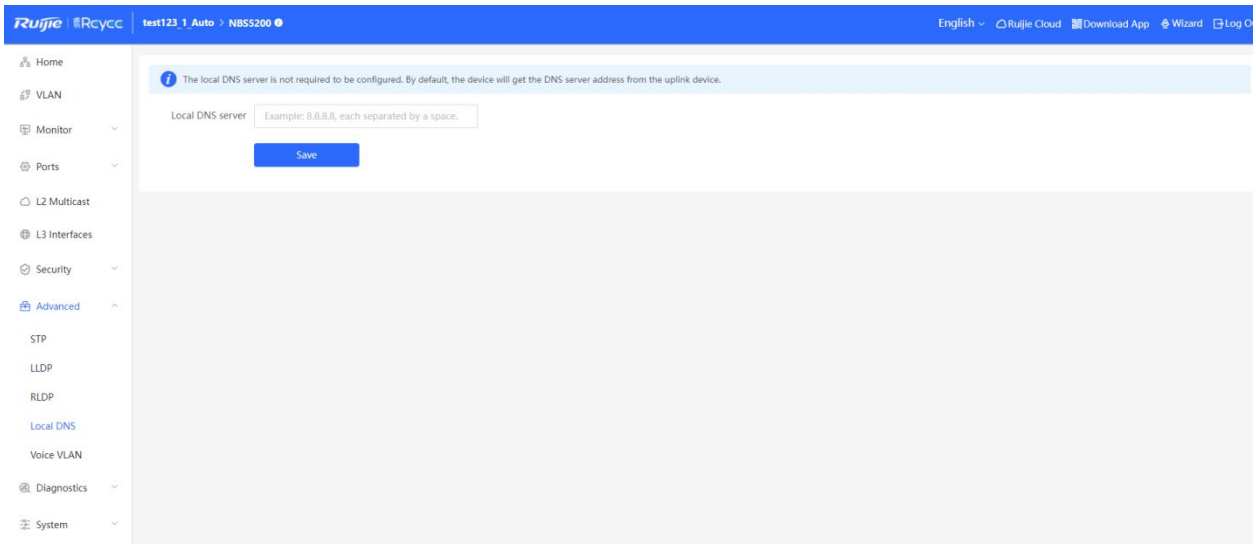
Port List Reset

Port	Status	Action	Neighbor Port
Gi11		Member port of Ag2.	
Gi12		Member port of Ag2.	
Gi13	OK	--	--
Gi14	OK	--	--
Gi15	OK	--	--
Gi16	OK	--	--
Gi17	OK	--	--
Gi18	Exception	Warning	Gi20
Gi19	OK	--	--
Gi20	Exception	Warning	Gi18

Total 30 10/page 1 2 3 Go to page 2

4.3.6.4 Local DNS

The **Local DNS** module allows you to set a DNS Server for this device.



Fill in a DNS Server address and click **Save.**

The local DNS server is not required to be configured. By default, the device will get the DNS server address from the uplink device.

4.3.6.5 Voice VLAN

1.1 Overview

IP phones are widely used thanks to rapid development of technologies. The voice virtual local area network (VLAN) is a VLAN dedicated to voice data streams of users.

The device with the Voice VLAN function matches the source MAC address field in the packets entering the port by the MAC address. The source MAC address in the packets which matches the OUI address of systems settings will be regarded as voice data streams. Such packet will be allocated to voice VLAN for transmission. Priority rules are automatically delivered to improve the priority of Voice streams and ensure call quality.

The OUI is the first 24 bits of the MAC address. It is a globally unique identifier allocated by the Institute of Electrical and Electronics Engineers (IEEE) to an equipment supplier. You can determine the supplier of a product based on the OUI.

1.2 Features

Automatic and Manual Modes of the Voice VLAN

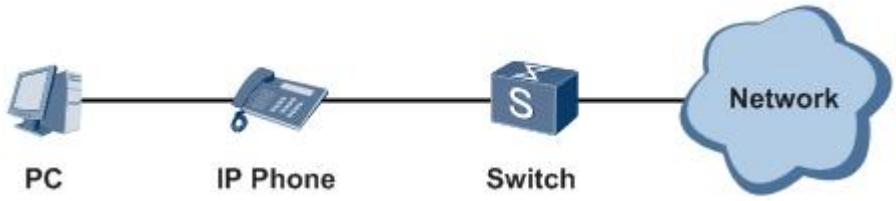
Ports in the voice VLAN can work either in automatic or manual mode. The way that ports are added to the voice VLAN varies according to the working mode.

Automatic mode

The automatic mode is applicable to the scenario where the PC and IP phone are serially connected to the port and transmit both voice and data streams.

When the port is configured as automatic mode, the switch and voice devices will communicte through LLDP. When the switch received the LLDP packets from the voice device, the device will automatically add the input port of the voice packet to the voice VLAN, and issue a policy to change the priority of the voice packet to the priority of the voice stream in the voice VLAN configured on the device, and uses the aging mechanism to maintain ports in the voice VLAN. If the system does not receive any voice packet from an input port before the aging timer expires, the system will delete this port from the voice VLAN.

The automatic mode must be configured when IP phones support LLDP., such as the topology below:

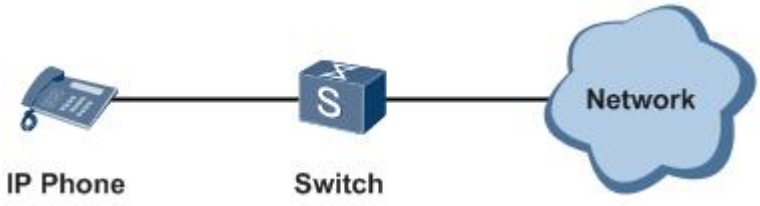


After the automatic Voice VLAN mode is enabled on a port, the Voice VLAN is removed from the Permit VLAN of the port until the port receives Voice data that belongs to the Voice VLAN (data tag=Voice VLAN). In automatic mode, the Voice VLAN is automatically added to the Permit VLAN so that Voice data can pass through the Voice VLAN. At the same time, a timer is started. If no Voice data is received within the aging time, the Voice VLAN is removed from the Permit VLAN.

Manual Mode

The manual mode is applicable to the scenario where the IP phone is directly connected to a switch and the port transmits only voice packets. In this networking mode, the port is dedicated to transmission of voice streams, which prevents data streams from affecting transmission of voice streams.

In manual port, the administrator manually adds a port to or deletes a port from the voice VLAN. The device identifies the source MAC address of the voice packet sent by the IP phone and compares this address with the OUI configured on the device. If the source MAC address matches the OUI, the device issues a policy to change the priority of the voice packet to the priority of the voice stream in the voice VLAN configured on the device,such as the topology below:



When the manual mode is enabled, If the voice streams from the IP Phone are untagged, the voice VLAN should equal to the Native VLAN, If the voice streams from the IP Phone are tagged, the voice VLAN is unequal to the Natice VLAN.

The following table describes the relationship between the working mode of the voice VLAN, IP phone type, and port type.

Working Mode of the Voice VLAN	Voice Stream Type	Port Type	Supported Or Not
Automatic mode	Untagged voice stream	Access port	Not supported.
		Trunk port	Not supported.
	Tagged voice stream	Access Port	Not supported.
		Trunk port	Supported. The native VLAN connected to the port must exist and cannot be a voice VLAN. In addition, the port allows packets of the native VLAN to pass through
Manual mode	Untagged voice stream	Access port	Supported. The voice VLAN must one of the VLANs to which the connected port is added.
		Trunk port	Supported. The native VLAN connected to the port must be a voice VLAN, and the port allows packets of this VLAN to pass through.
	Tagged voice stream	Access port	Not supported.
		Trunk port	Supported. The native VLAN connected to the port must exist and cannot be a voice VLAN. In addition, the port allows packets of the native VLAN and the voice VLAN to pass through.

Security Mode of the Voice VLAN

In order to better isolate voice streams from data streams during transmission, the voice VLAN provides the security mode.

When the security mode is enabled, the voice VLAN only allows the transmission of voice streams. In this case, the device checks the source MAC address of each packet. When the source MAC address of a packet is a voice VLAN OUI that can be identified, the packet can be transmitted in the voice VLAN; otherwise, the packet is dropped.

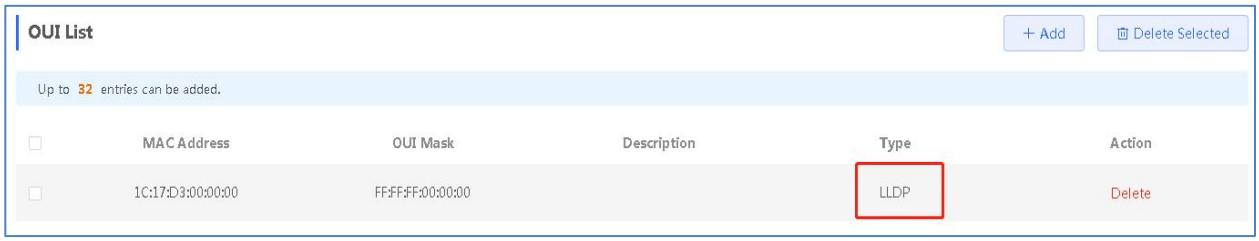
When the security mode is disabled, the device does not check the source MAC address of each packet, and all packets can be transmitted in the voice VLAN.

In security mode, the device checks the source MAC address of only the untagged packets or the packet containing the voice VLAN tag. For other packets that do not contain the voice VLAN tag, the device forwards or drops these packets according to the VLAN rules.

You are advised not to transmit voice and data streams concurrently in a voice VLAN. If it is necessary to concurrent transmission of voice and data streams, confirm that the security mode of the voice VLAN has been disabled.

LLDP function

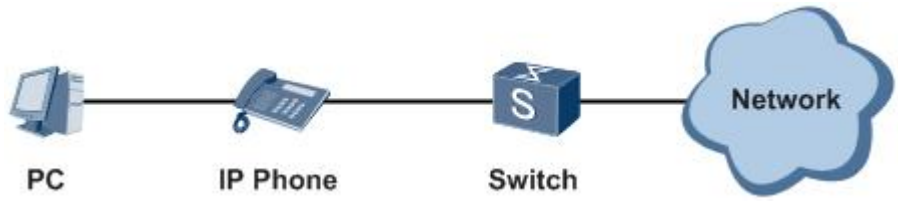
If the IP phone supports THE LLDP protocol, users do not need to configure OUI. The device can capture the LLDP protocol sent by the IP phone to identify the device capability fields in the protocol packets. The device whose function is identified as “telephone” is the voice device. The source MAC addresses of protocol packets are extracted and automatically added to the OUI list for automatic voice identification, as shown in below picture:



Some advanced IP phones proactively send LLDP packets to obtain the Voice VLAN information configured on the switch. If the Voice VLAN is enabled on the switch port connected to the IP phone, the Voice VLAN information is filled in the related fields and sent to the IP phone. After receiving the LLDP packet with Voice VLAN information, the IP phone sends Voice packets with tags.

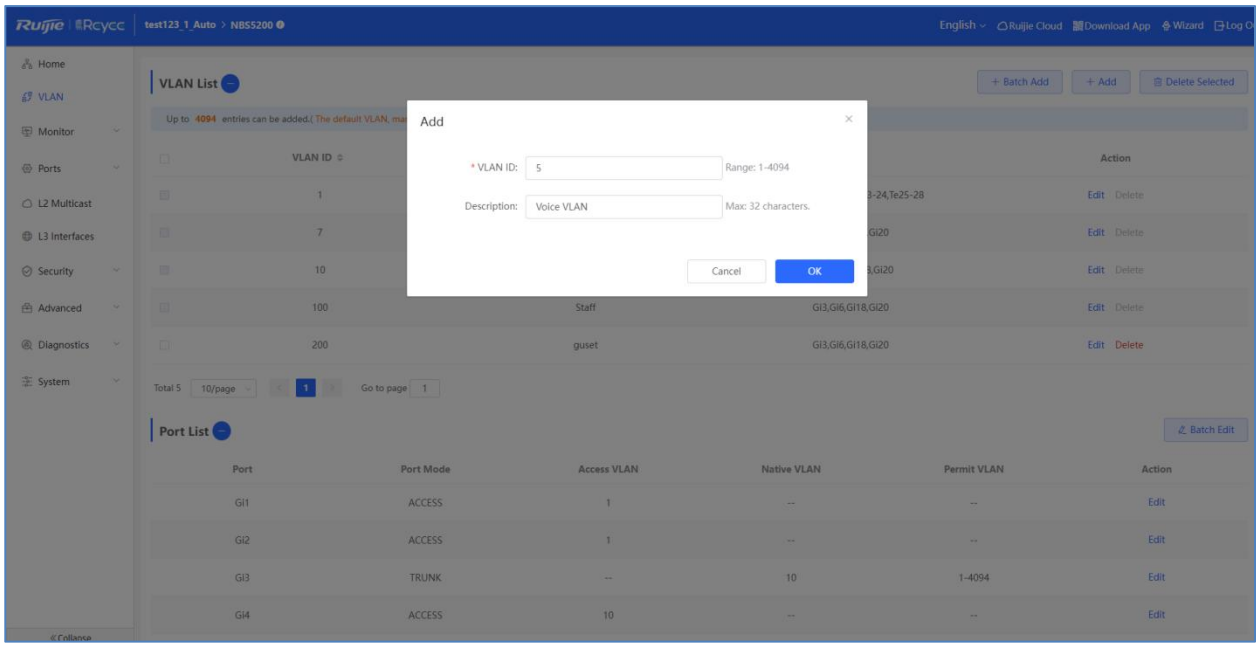
1.3 Automatic Mode Configuration

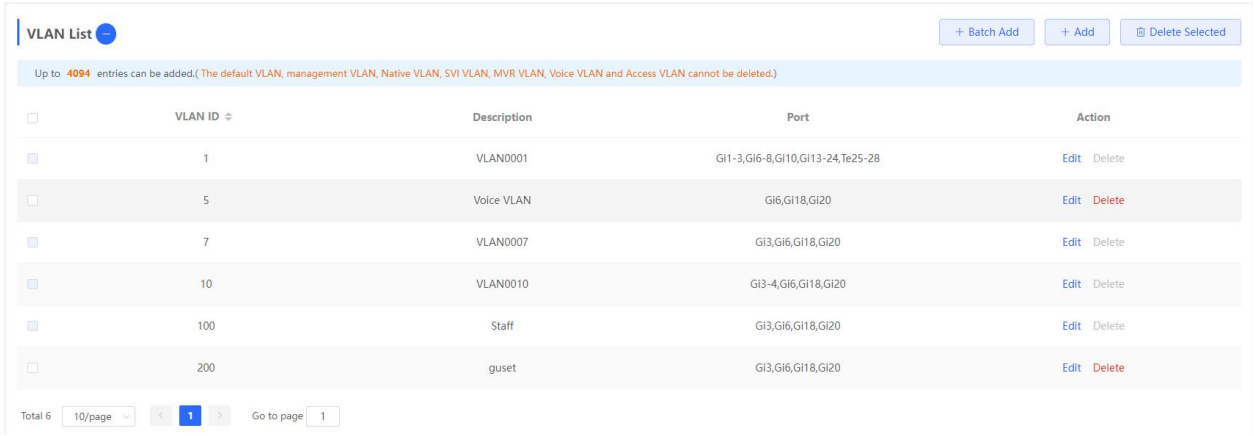
Configuring the port as automatic, the voice date will pass through Voice VLAN, and the PC data will pass through the default VLAN.



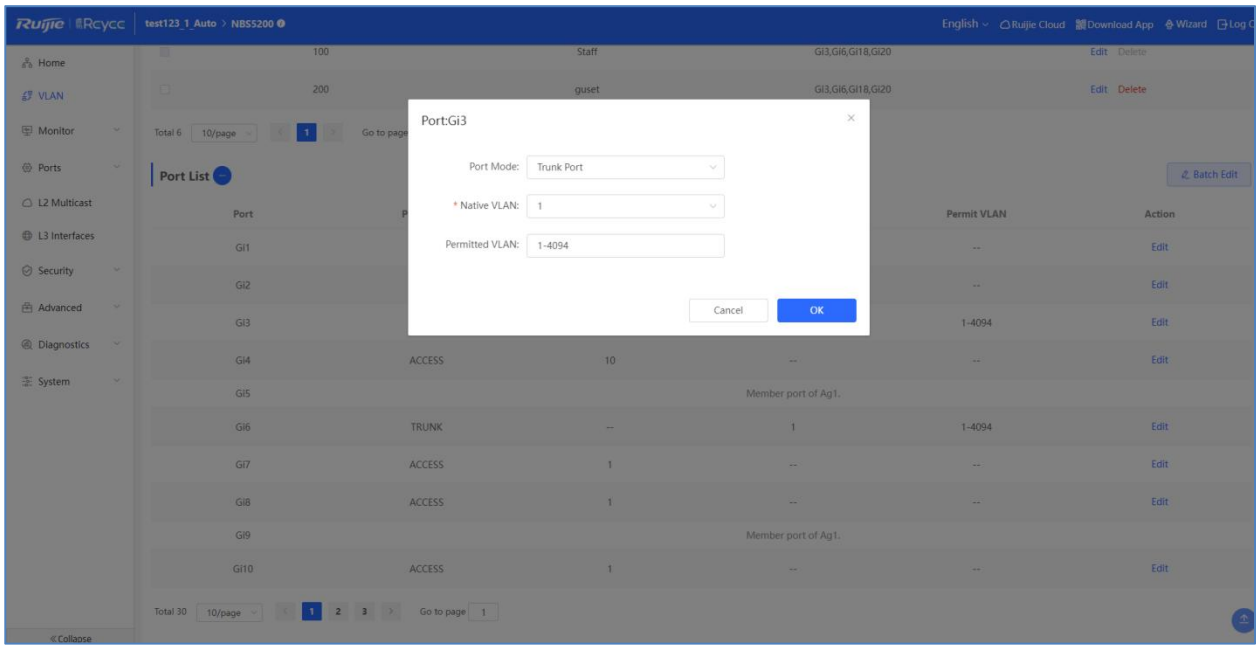
If IP Phone is connected to the 3 ports of switch:

Step 1：Enter VLAN page by eWeb and Create VLAN 5 as Voice VLAN.


Add
* VLAN ID: 5
Range: 1-4094
Description: Voice VLAN
Max: 32 characters.
Cancel
OK
VLAN List
Port List


VLAN List
+ Batch Add
+ Add
Delete Selected
Up to 4094 entries can be added.(The default VLAN, management VLAN, Native VLAN, SVI VLAN, MVR VLAN, Voice VLAN and Access VLAN cannot be deleted.)
VLAN ID
Description
Port
Action
1 VLAN0001 Gi1-3,Gi6-8,Gi10,Gi13-24,Te25-28 Edit Delete
5 Voice VLAN Gi6,Gi18,Gi20 Edit Delete
7 VLAN0007 Gi3,Gi6,Gi18,Gi20 Edit Delete
10 VLAN0010 Gi3-4,Gi6,Gi18,Gi20 Edit Delete
100 Staff Gi3,Gi6,Gi18,Gi20 Edit Delete
200 guset Gi3,Gi6,Gi18,Gi20 Edit Delete
Total 6 10/page 1 Go to page 1

Step 2：Configure port 3 as trunk mode in the Port List of VLAN page.



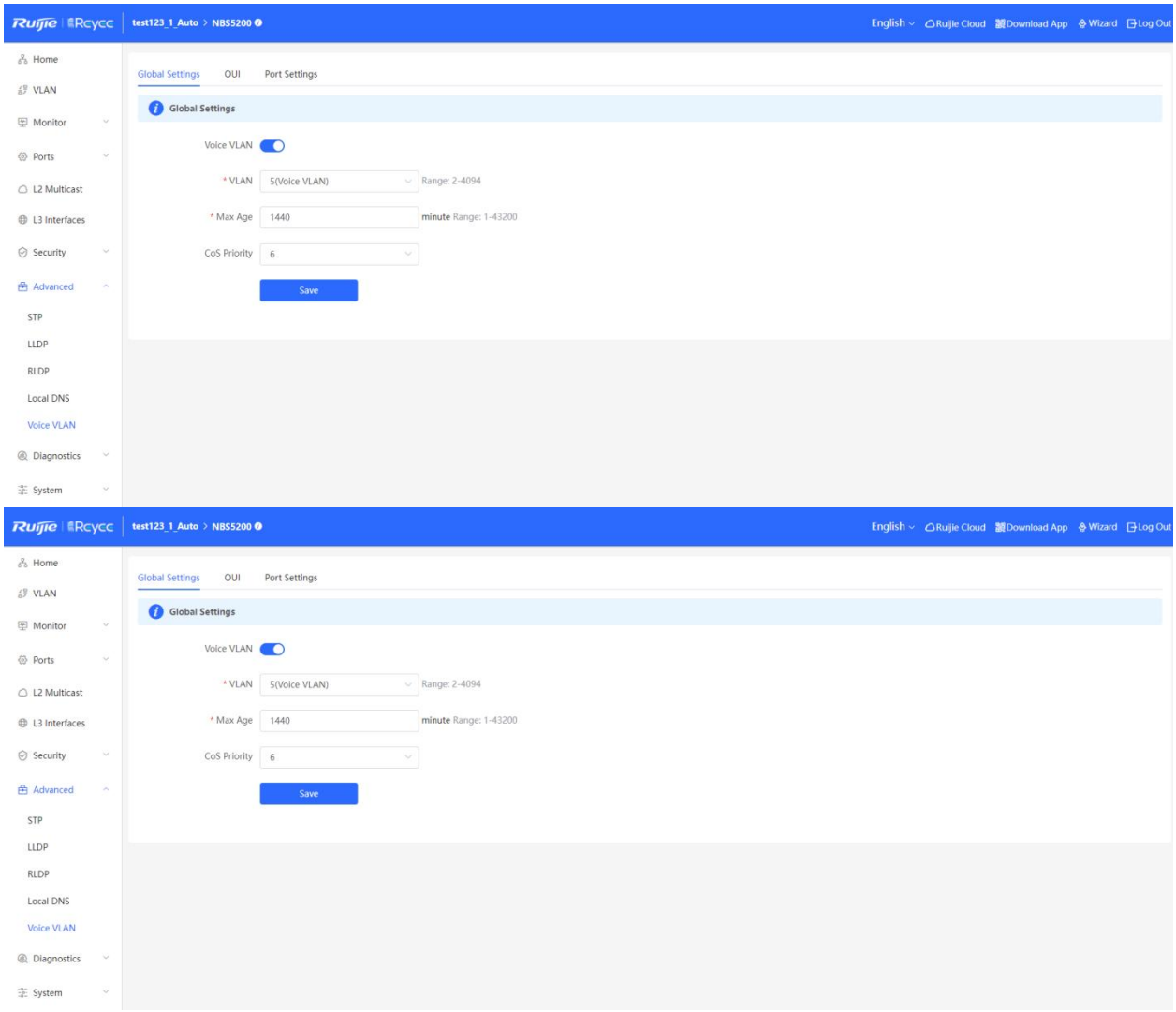
Port List

Batch Edit

Port	Port Mode	Access VLAN	Native VLAN	Permit VLAN	Action
Gi1	ACCESS	1	--	--	Edit
Gi2	ACCESS	1	--	--	Edit
Gi3	TRUNK	--	1	1-4,6-4094	Edit
Gi4	ACCESS	10	--	--	Edit
Gi5			Member port of Ag1.		
Gi6	TRUNK	--	1	1-4094	Edit
Gi7	ACCESS	1	--	--	Edit
Gi8	ACCESS	1	--	--	Edit
Gi9			Member port of Ag1.		
Gi10	ACCESS	1	--	--	Edit

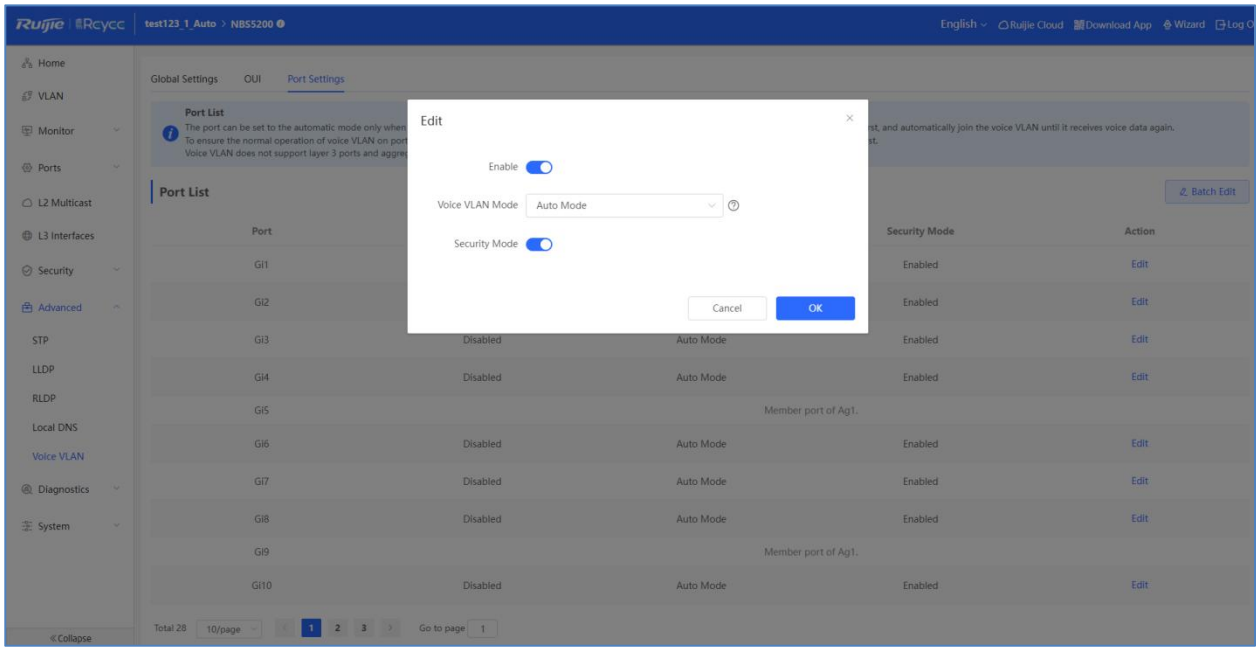
Total 30 10/page 1 2 3 Go to page 1

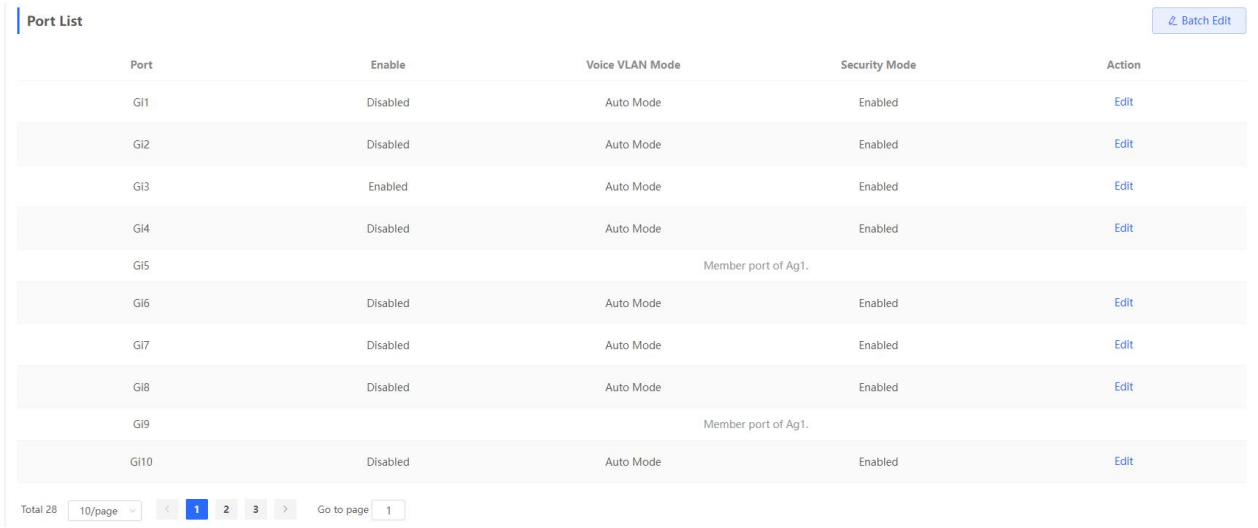
Step 3： In Voice Vlan page, click **Advanced->Voice VLAN->Global Settings** to configure VLAN 5 as Voice VLAN



Other parameters can be selected based on site requirements. Otherwise, default values will be used.

Step 3: Click **Advanced->Voice VLAN->Port Settings** to enable the Voice VLAN of port 3.





Port List

Batch Edit

Port	Enable	Voice VLAN Mode	Security Mode	Action
Gi1	Disabled	Auto Mode	Enabled	Edit
Gi2	Disabled	Auto Mode	Enabled	Edit
Gi3	Enabled	Auto Mode	Enabled	Edit
Gi4	Disabled	Auto Mode	Enabled	Edit
Gi5		Member port of Ag1.		
Gi6	Disabled	Auto Mode	Enabled	Edit
Gi7	Disabled	Auto Mode	Enabled	Edit
Gi8	Disabled	Auto Mode	Enabled	Edit
Gi9		Member port of Ag1.		
Gi10	Disabled	Auto Mode	Enabled	Edit

Total 28 10/page 1 2 3 Go to page 1

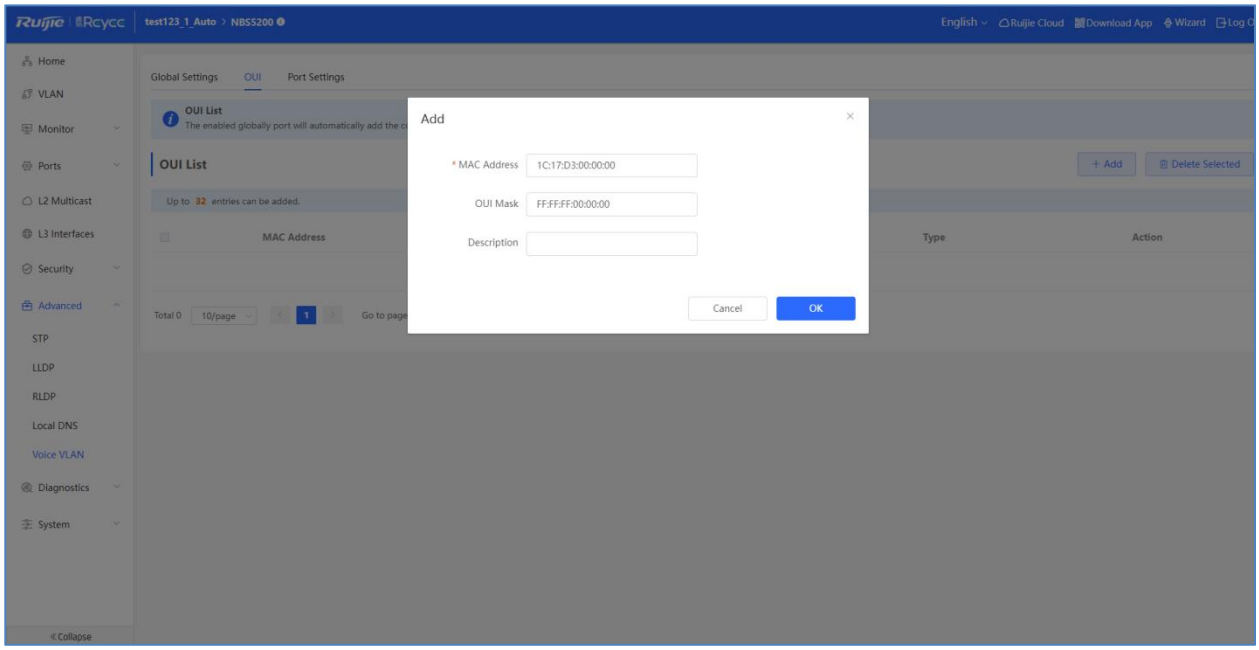
When security mode is enabled, Voice VLAN only allows passing through the voice date. If disable, all data could pass through Voice VLAN.

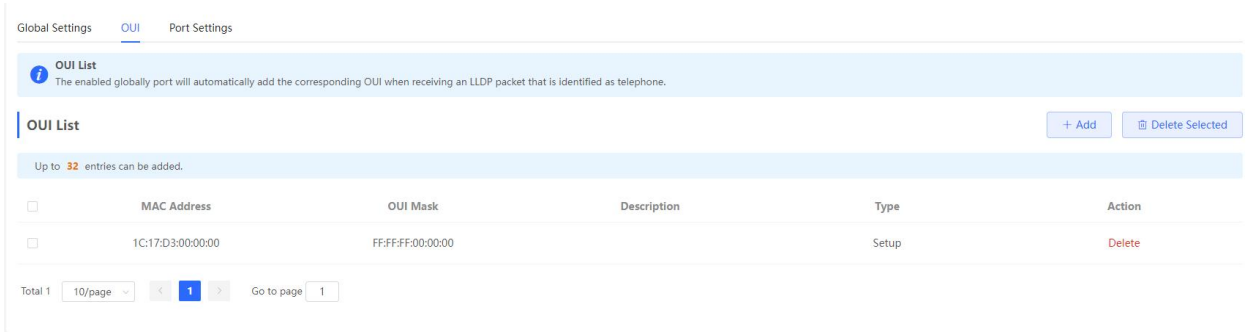
The port can be set to the automatic mode only when the port VLAN is in the trunk mode. When the port is in the automatic mode, the port will exit the voice VLAN first, and automatically join the voice VLAN until it receives voice data again.

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

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

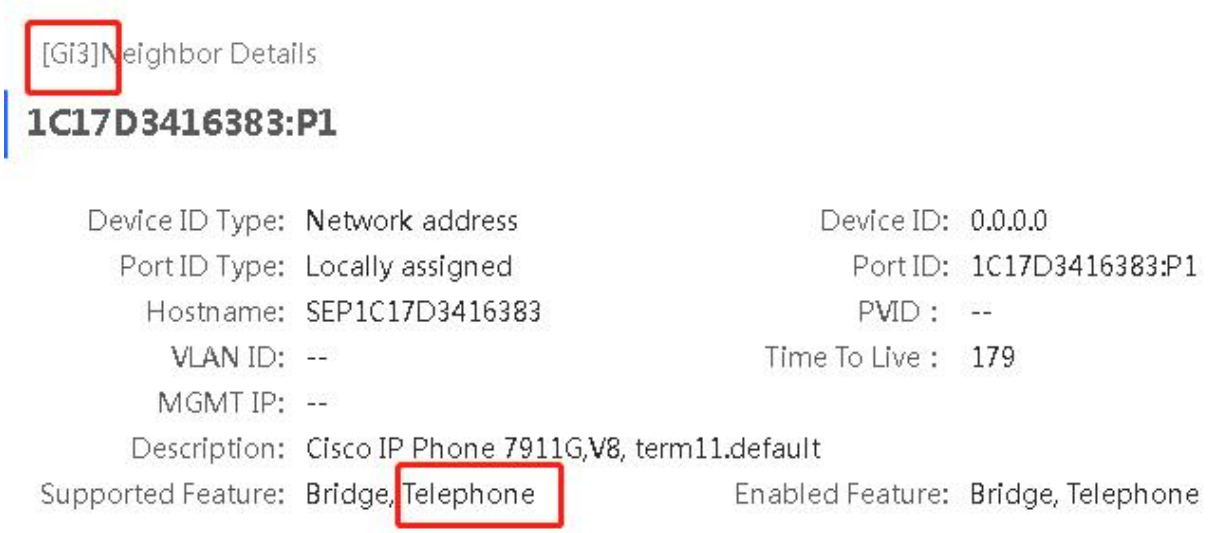
Step 5: Click **Advance->Voice VLAN->OUI** to add the OUI of voice devices.





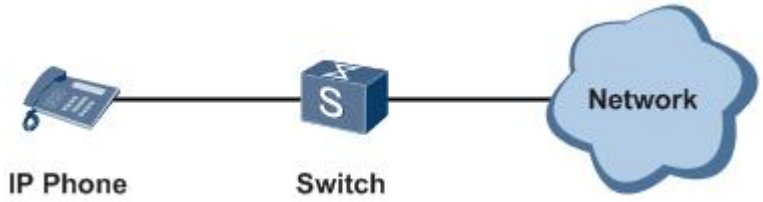
If the IP phone supports LLDP, the device automatically adds the OUI of the IP phone to the OUI list after the Voice VLAN function is enabled on the port. In this case, you can skip Step 5. If the port 3 does not have LLDP Neihbor Info, the device does not support LLDP.

Check the LLDP information of IP Phone by clicking **Advance->LLDP->LLDP Info**



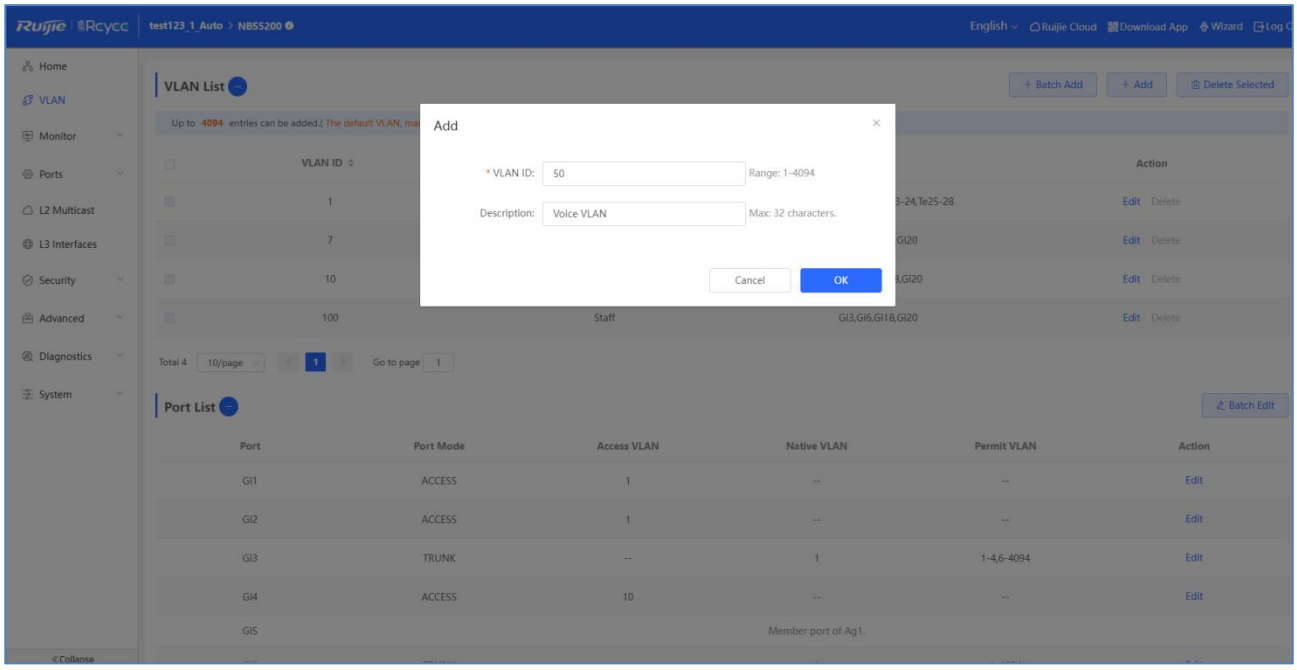
1.4 Manual Mode Configuration

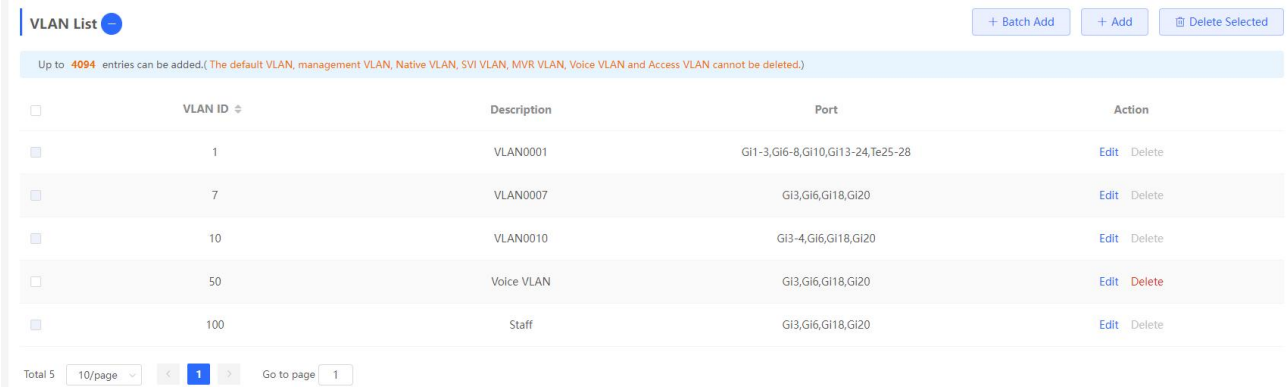
Set the port to manual mode and let Voice data pass through the Voice VLAN.



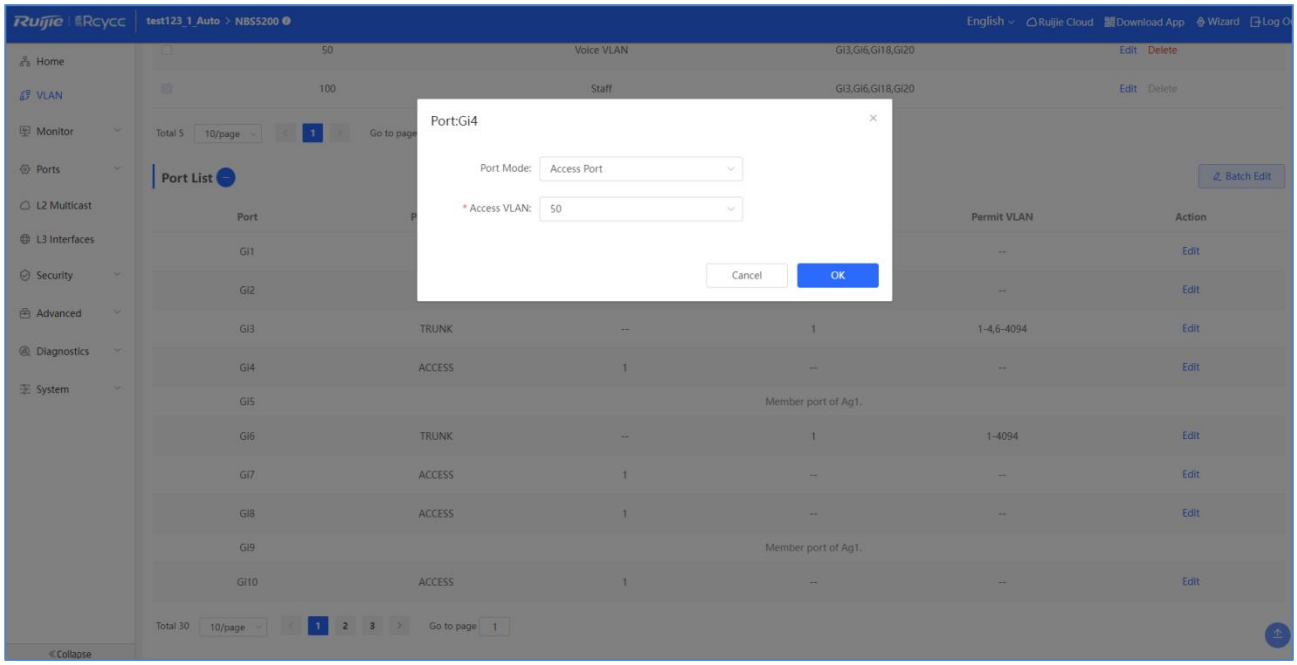
For example: if the port 4 of switch connects to IP Phone,

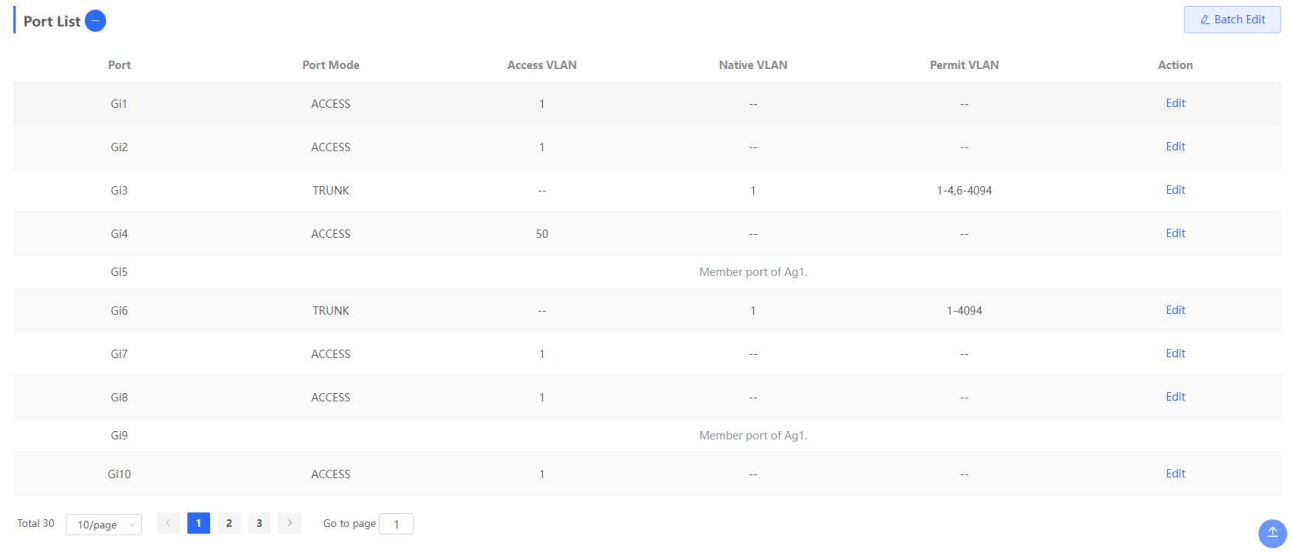
Step 1：Enter VLAN page by eWeb, and create VLAN 50 as Voice VLAN.



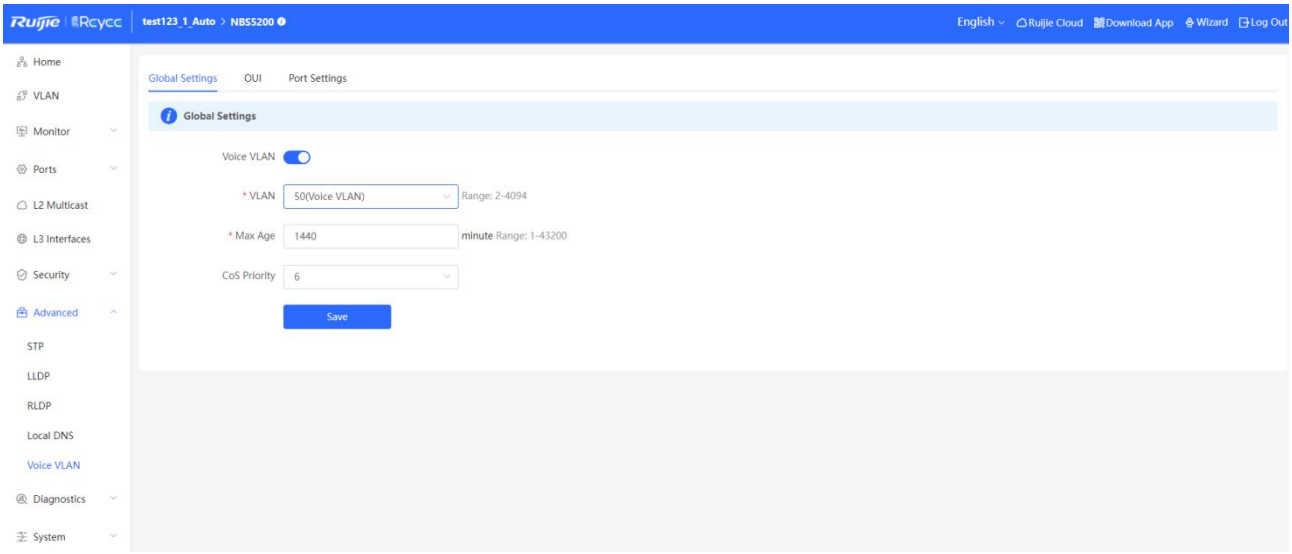


Step3: Configure port 4 as access mode and Access VLAN as VLAN 50 in the Port List of VLAN page.



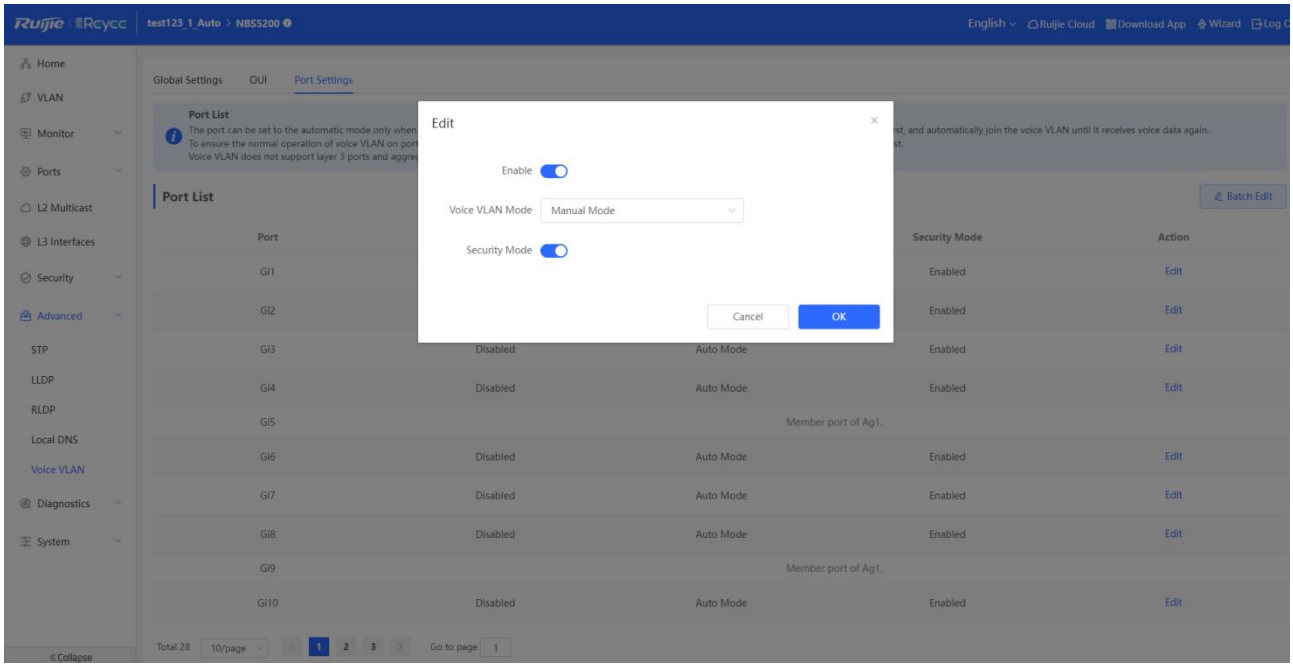


Step3: In the Voice VLAN page, Click **Advanced->Voice VLAN->Global Settings** to choose VLAN 5 as Voice VLAN.



Other parameters can be selected based on site requirements. Otherwise, use the default values

Step 4: Click Advanced->Voice VLAN->Port Settings to enable port 4 as Voice VLAN and enable it as maunal mode.



After security mode is enabled, only Voice data can pass through the Voice VLAN. If security mode is disabled, other data can also pass through the Voice VLAN. So it is recommended to the security mode

Port List

Batch Edit

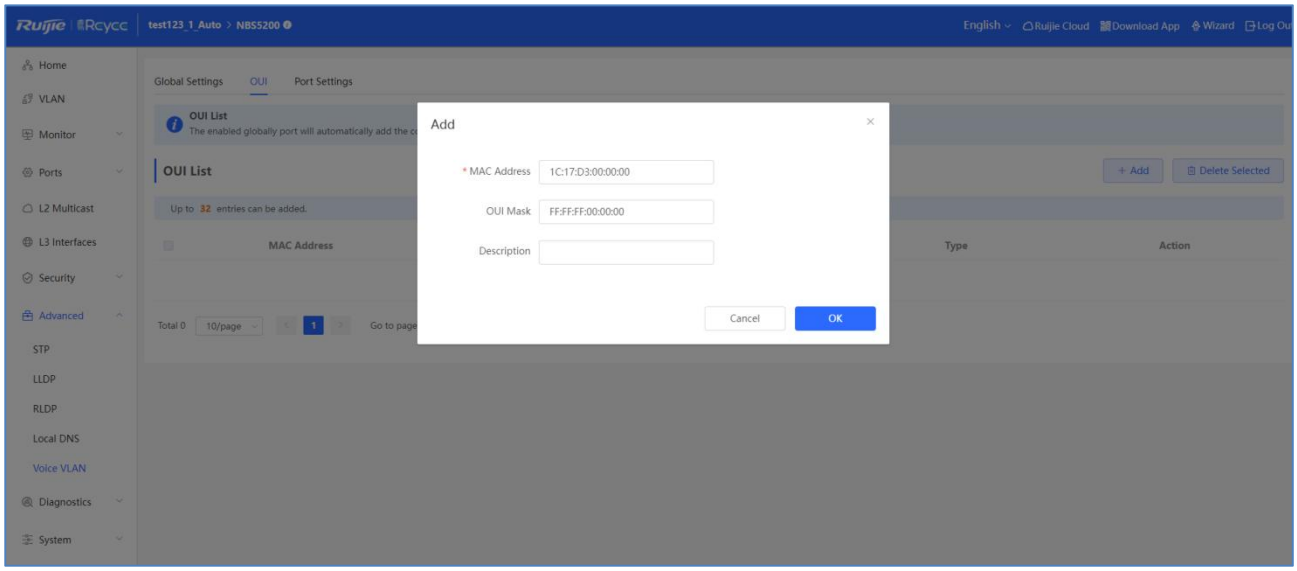
Port	Enable	Voice VLAN Mode	Security Mode	Action
Gi1	Disabled	Auto Mode	Enabled	Edit
Gi2	Disabled	Auto Mode	Enabled	Edit
Gi3	Disabled	Auto Mode	Enabled	Edit
Gi4	Enabled	Manual Mode	Enabled	Edit
Gi5		Member port of Ag1.		
Gi6	Disabled	Auto Mode	Enabled	Edit
Gi7	Disabled	Auto Mode	Enabled	Edit
Gi8	Disabled	Auto Mode	Enabled	Edit
Gi9		Member port of Ag1.		
Gi10	Disabled	Auto Mode	Enabled	Edit

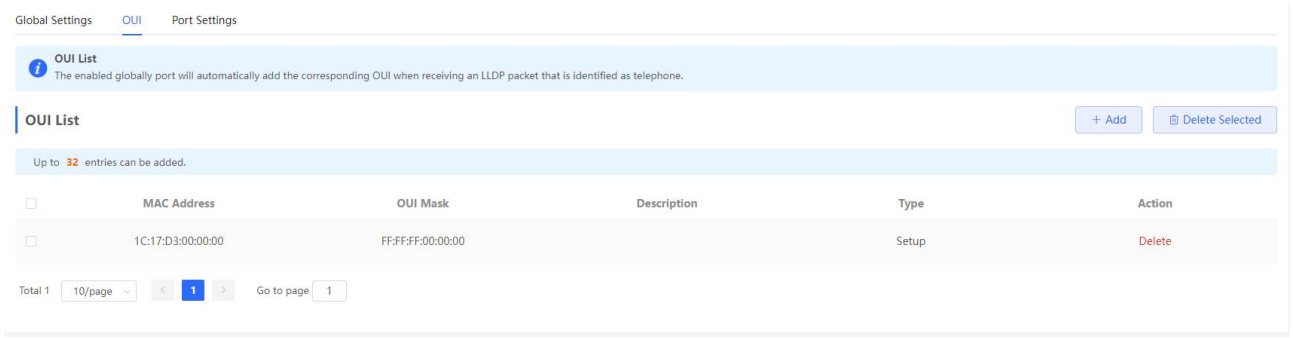
The port can be set to the automatic mode only when the port VLAN is in the trunk mode. When the port is in the automatic mode, the port will exit the voice VLAN first, and automatically join the voice VLAN until it receives voice data again.

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

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

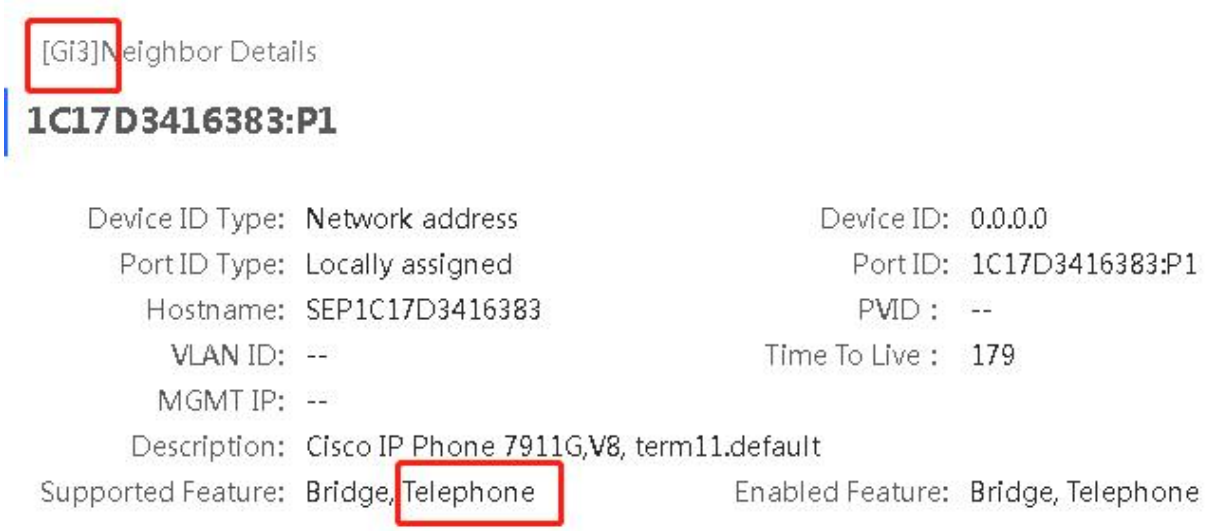
Step 5: Click **Advanced settings ->Voice VLAN->OUI** to add the OUIs of voice devices





If the IP phone supports LLDP, after the Voice VLAN is enabled on the port, the DEVICE automatically adds the OUI of the IP phone to the OUI list. In this case, you can skip Step 5. If port 3 does not have LLDP Neihbor Info, the device does not support LLDP.

Click Advanced->LLDP->LLDP Info to check the LLDP information of IP Phone.



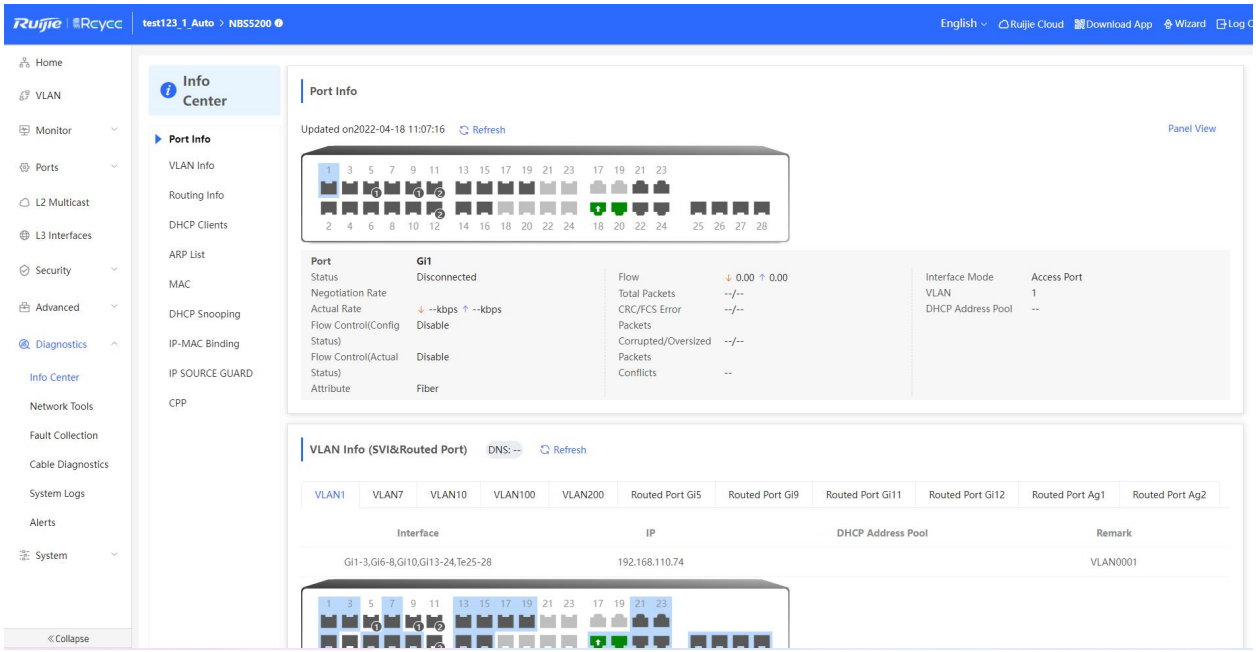
4.3.7 Diagnostics

4.3.7.1 Info Center

The **Info Center** module displays the running status and configuration. The information displayed here provides reference for troubleshooting.

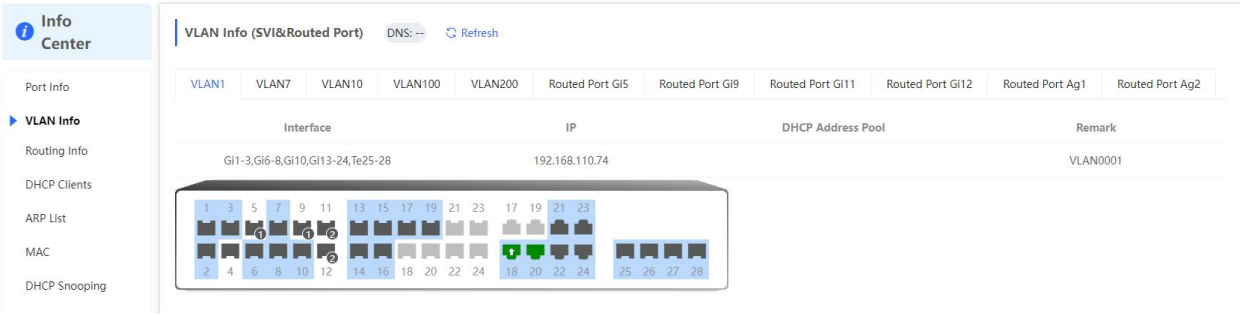
Port Info

Display the **Port Information** of devices.



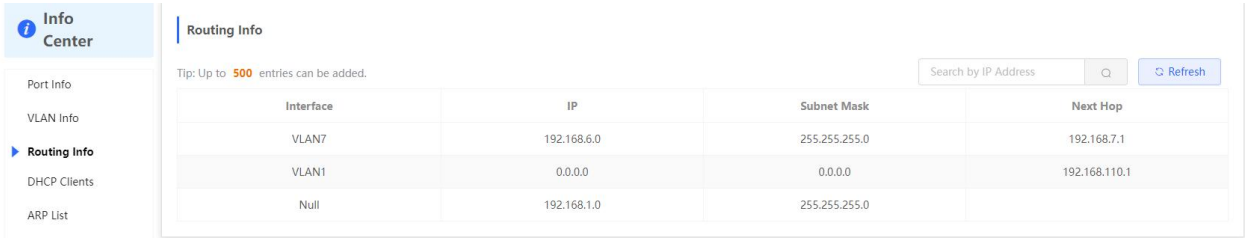
VLAN Info

Display the information of **VLAN, SVI, Routed Port**



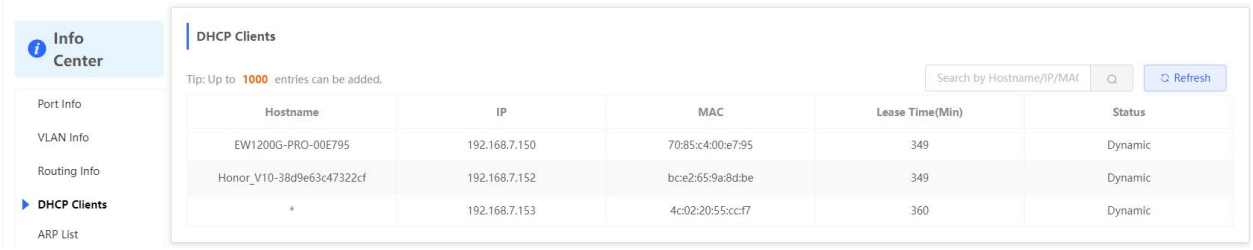
Routing Info

Display device's Routing information



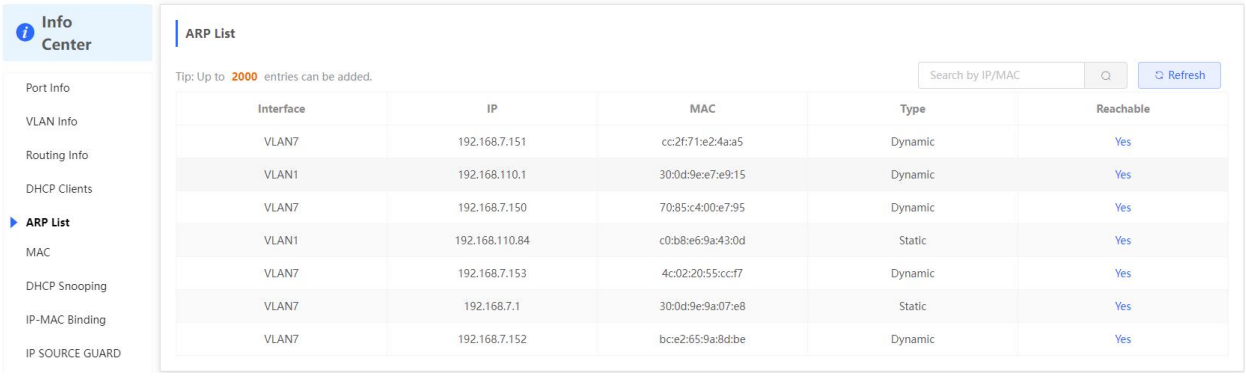
DHCP Clients

Display device's DHCP Clients information



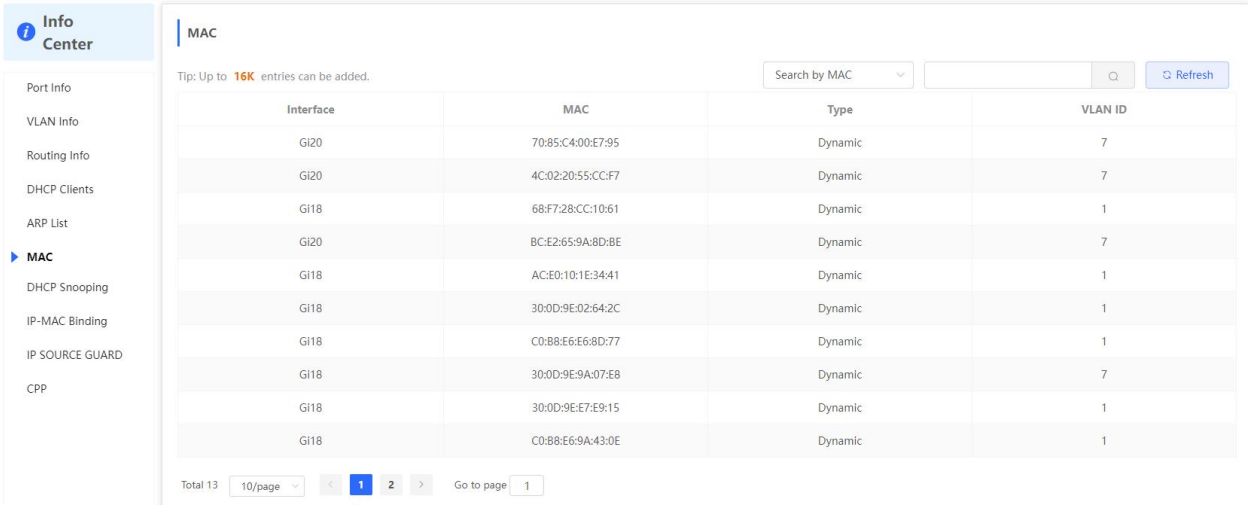
DHCP Clients

Display DHCP Clients information of devices



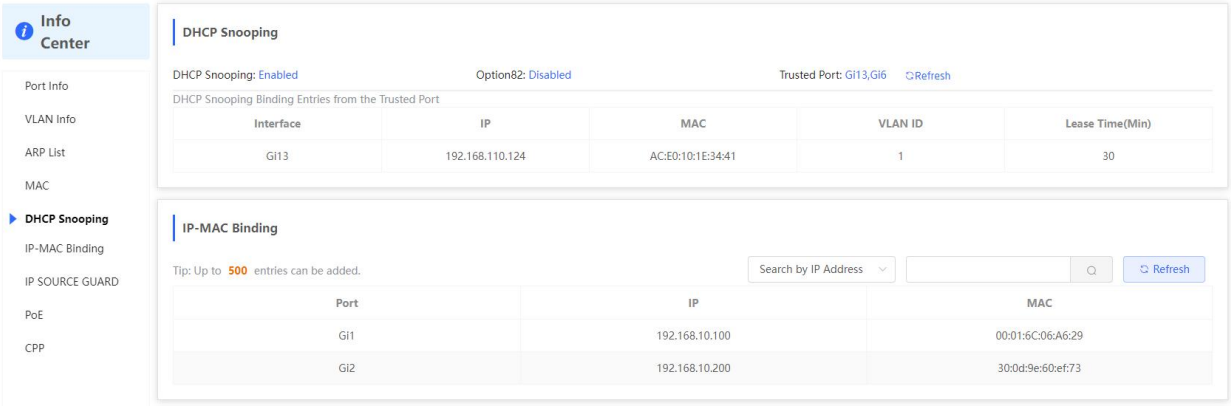
MAC

Display the MAC address table of device.



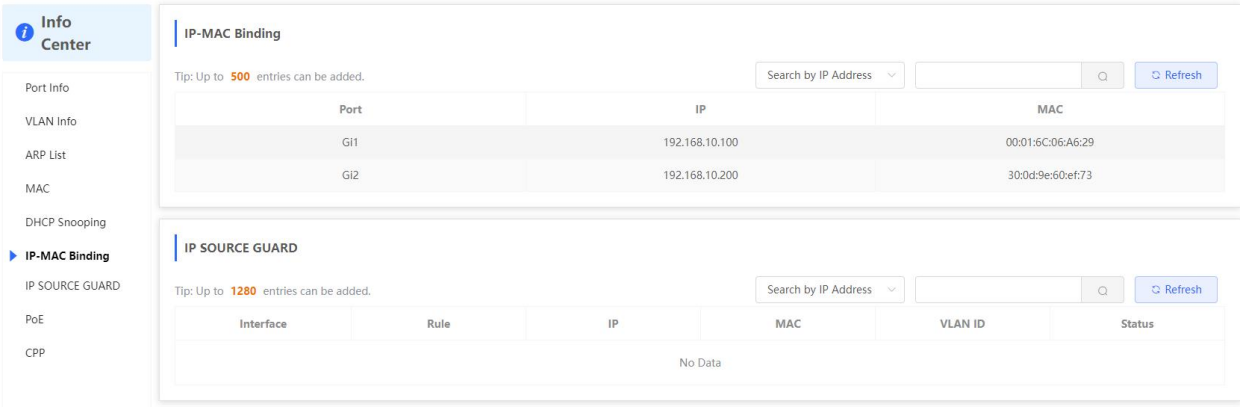
DHCP Snooping

Display the DHCP Snooping of devices



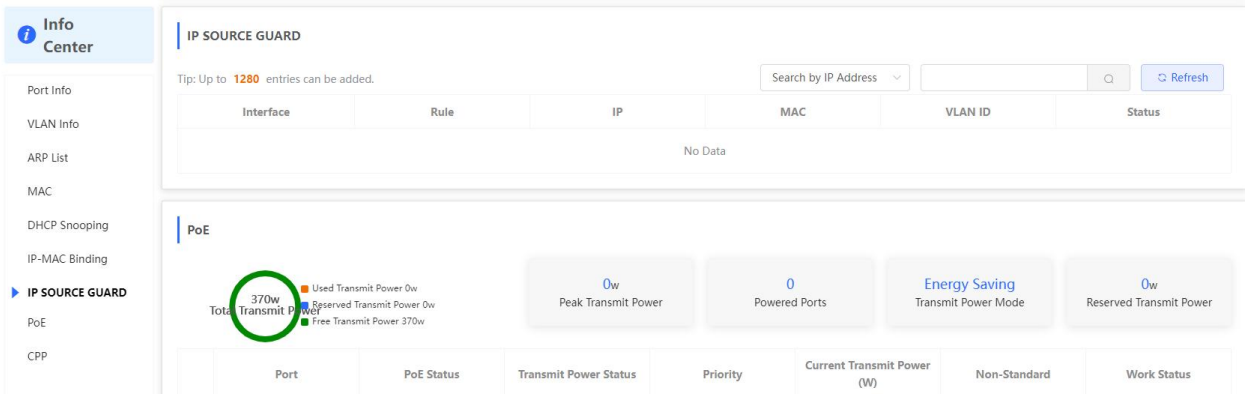
IP-MAC Binding

Display IP-MAC Binding information of device



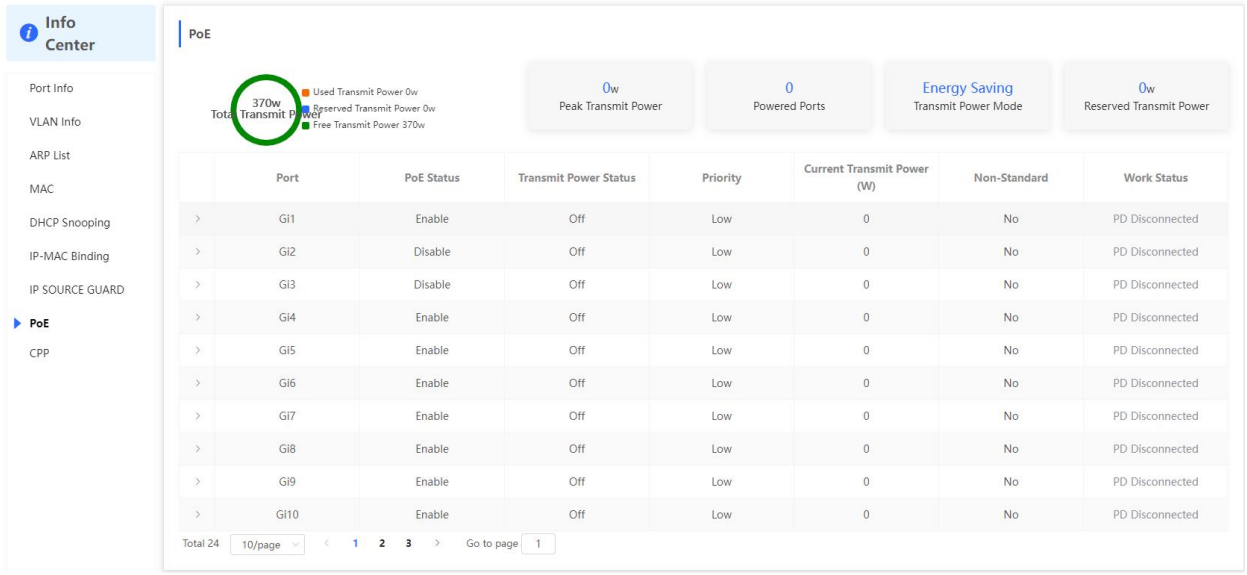
IP SOURCE GUARD

Display IP SOURCE GUARD information of device



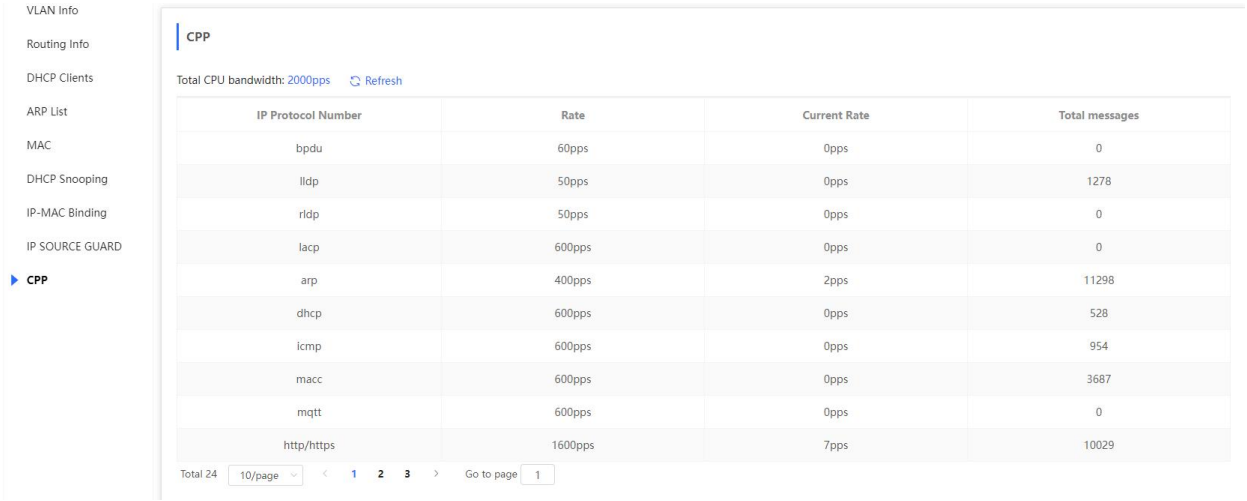
POE

Display the POE information of device.



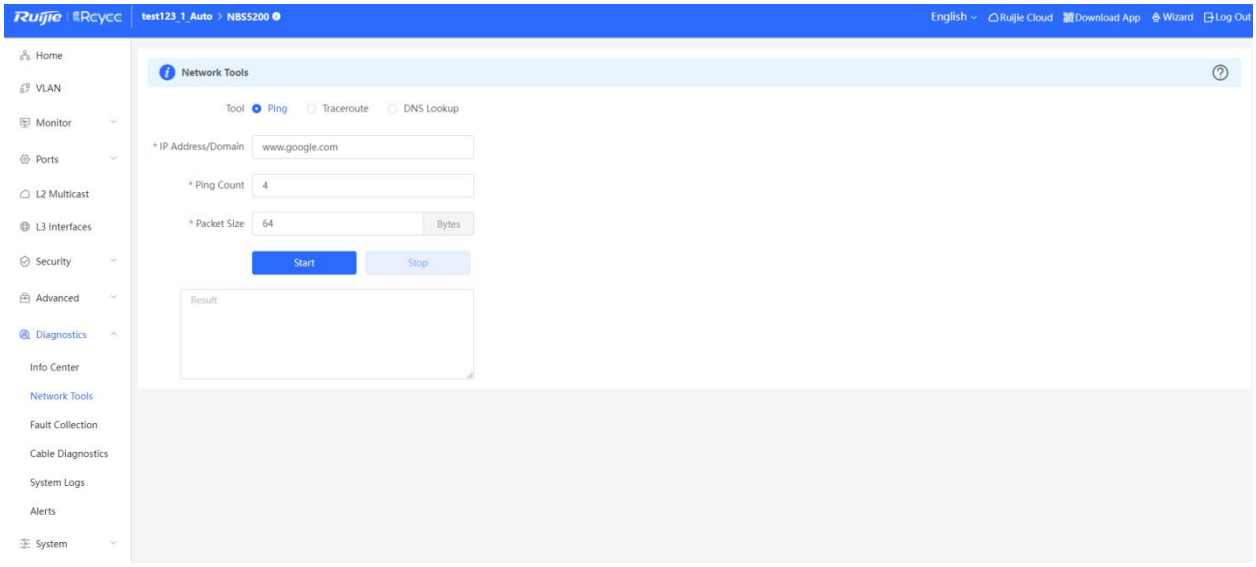
CPP

Display CPP information of devices.



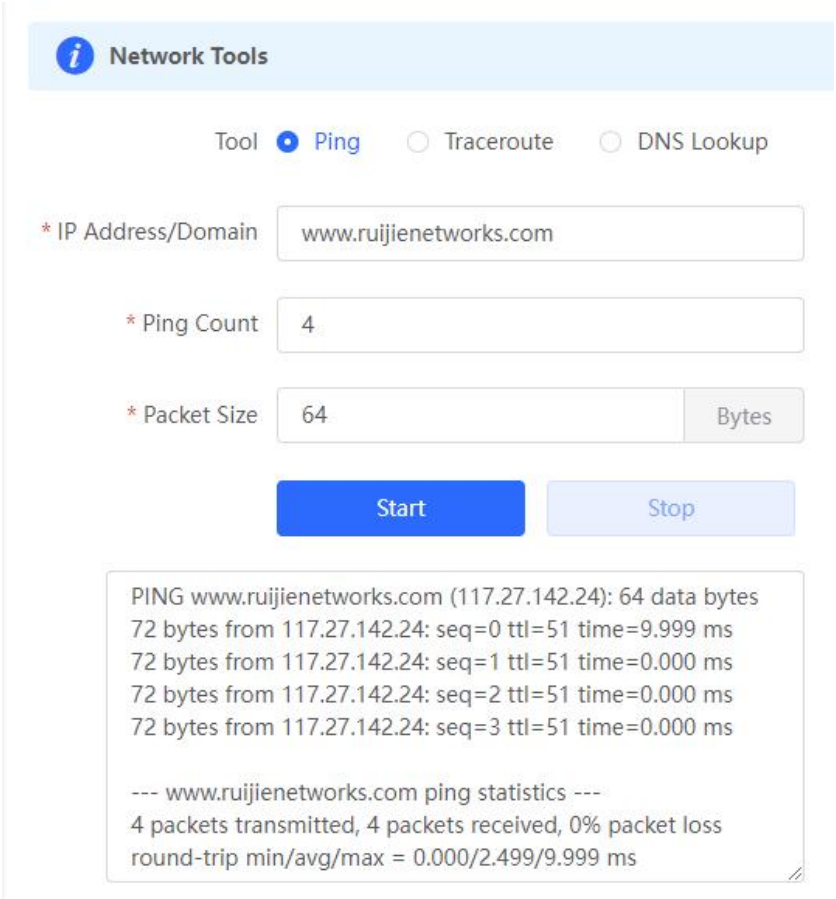
4.3.7.2 Network Tools

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



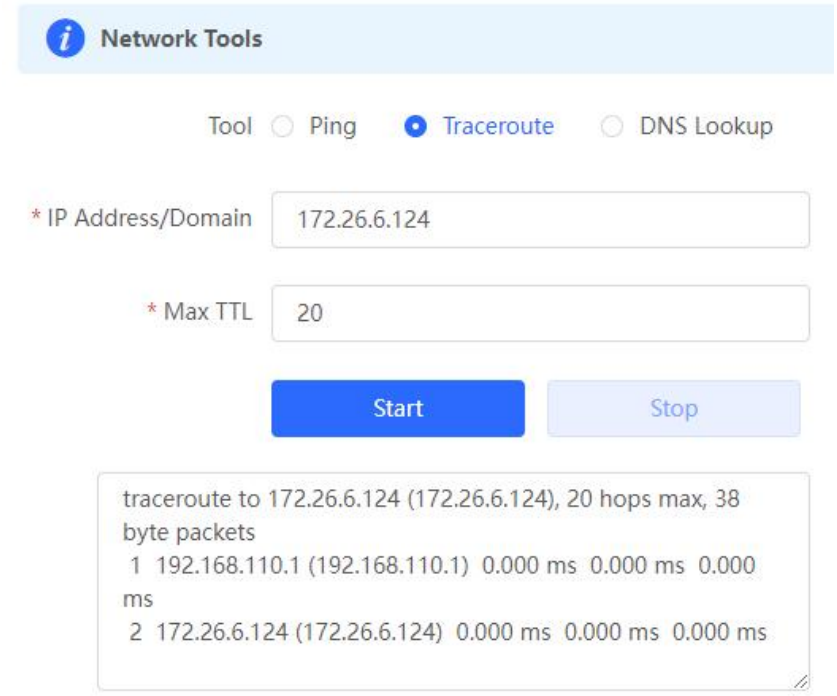
Ping

Test whether the node is reachable.



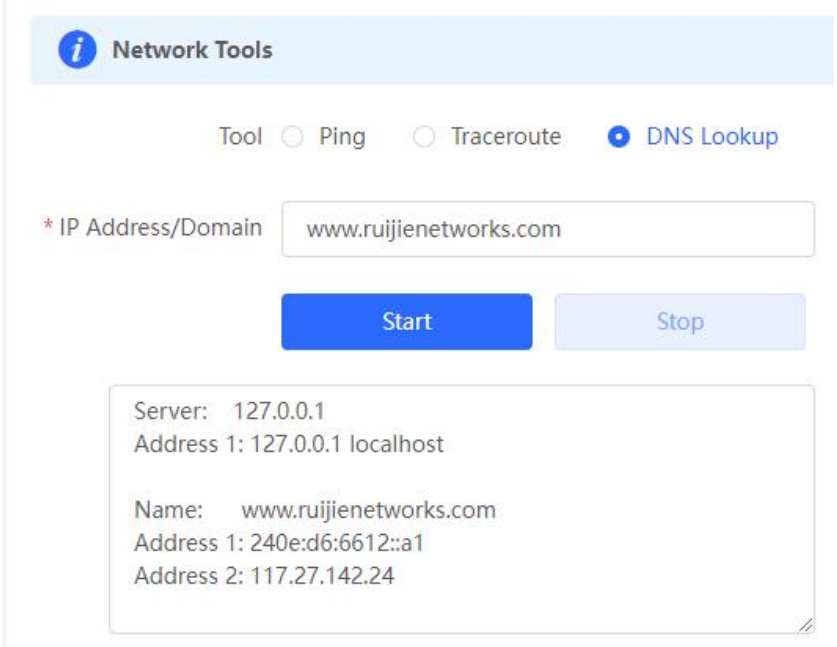
Traceroute

Count the number of hops or communication links from one point to another and the time it takes for each hop.



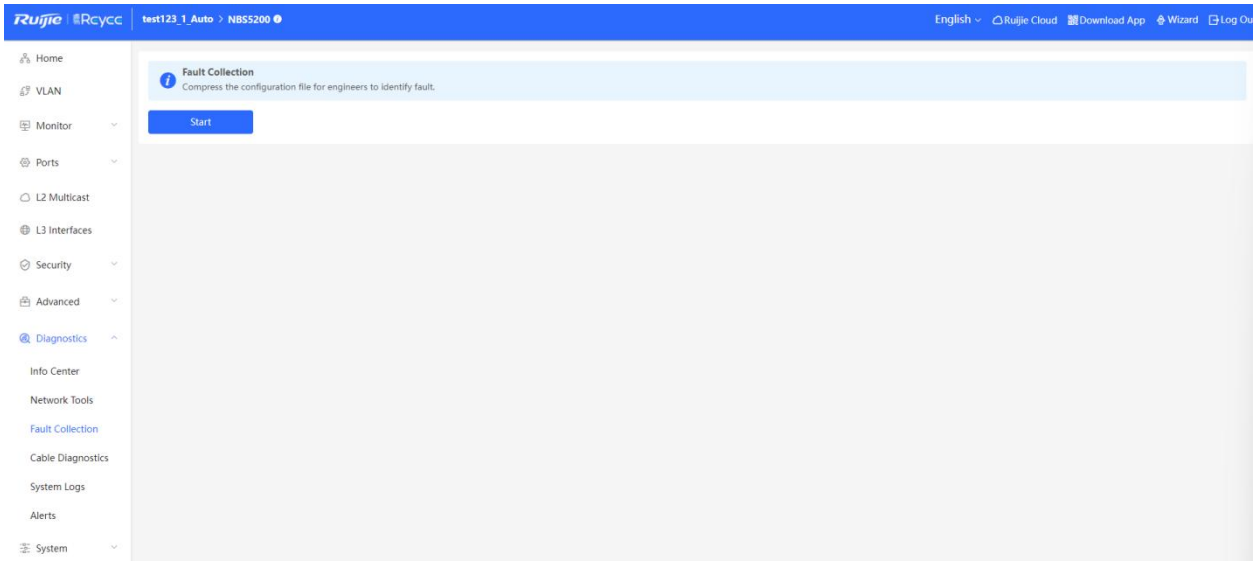
DNS Lookup

Resolve the domain to the IP address.

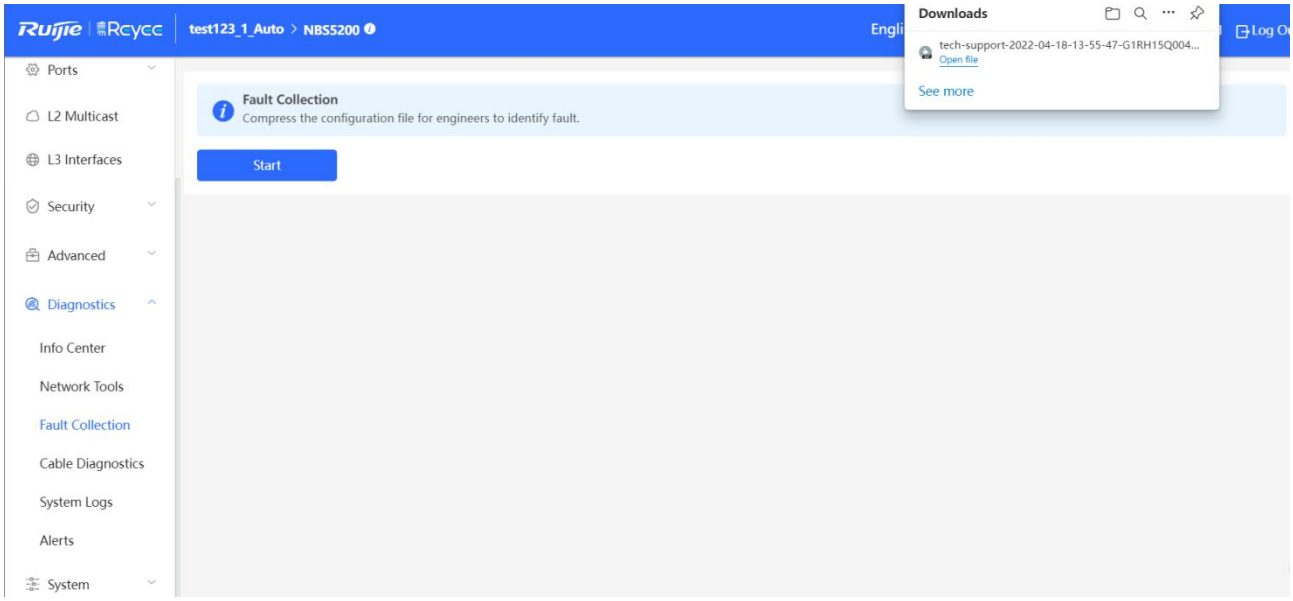


4.3.7.3 Fault Collection

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

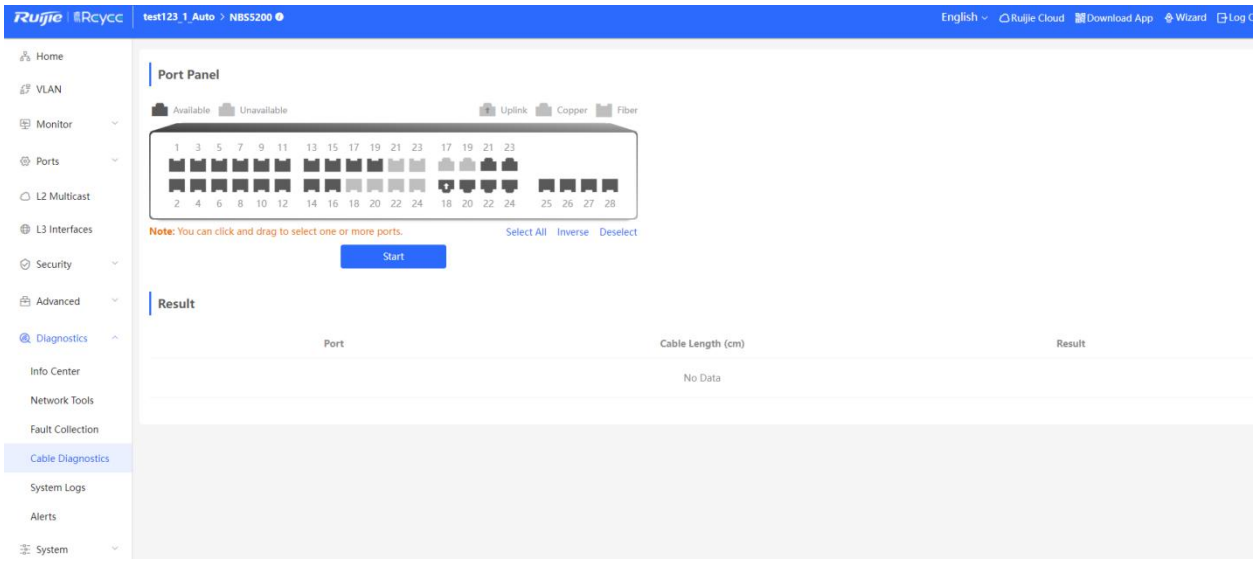


Click **Start** to download the fault information.

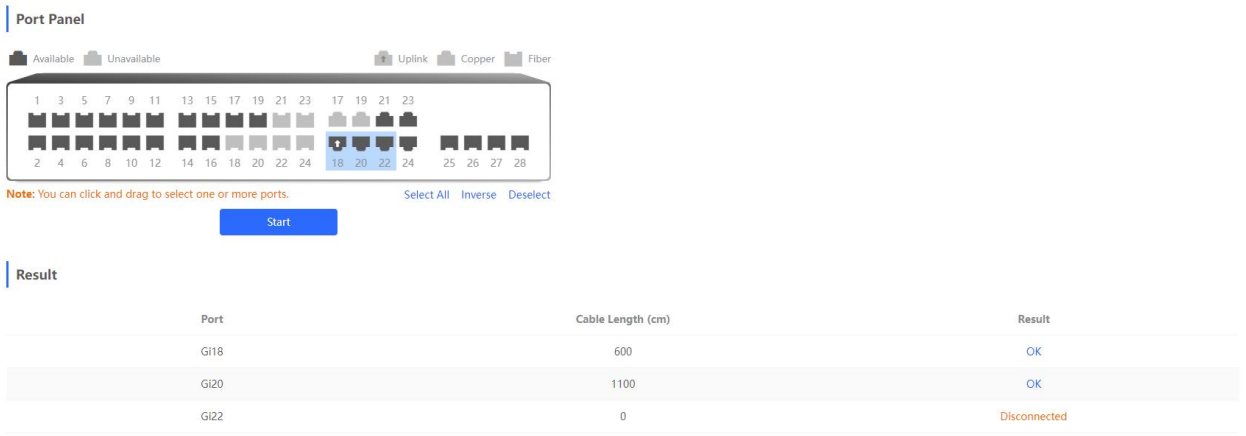


4.3.7.4 Cable Diagnostics

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



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

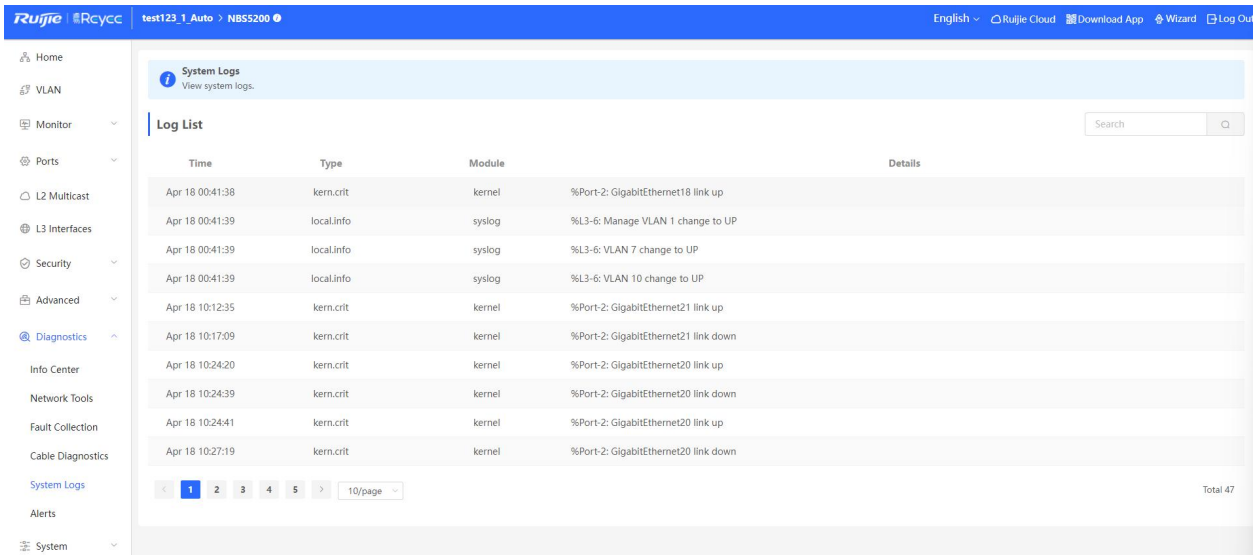


Only copper ports support cable diagnostics while fiber ports and aggregate ports do not.

If cable diagnostics is executed on a normally connected interface, the connection is temporarily down and will be reestablished.

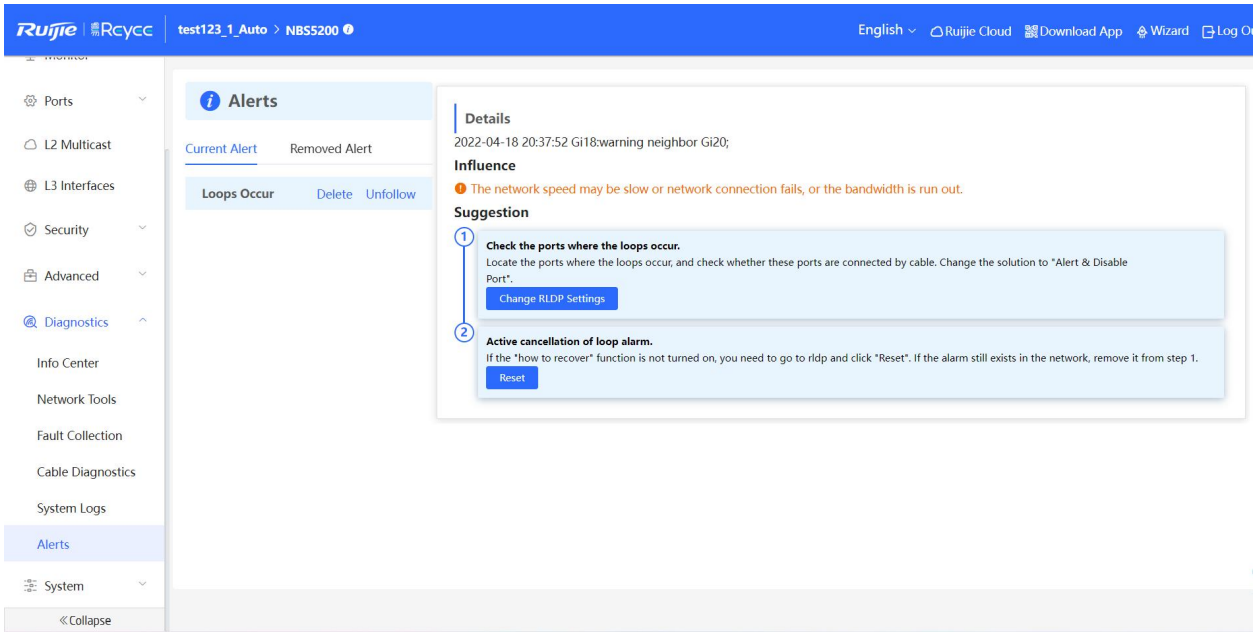
4.3.7.5 System Logs

The System Logs module provides logs recording the device's running status and configuration change, which provides a reference for troubleshooting.

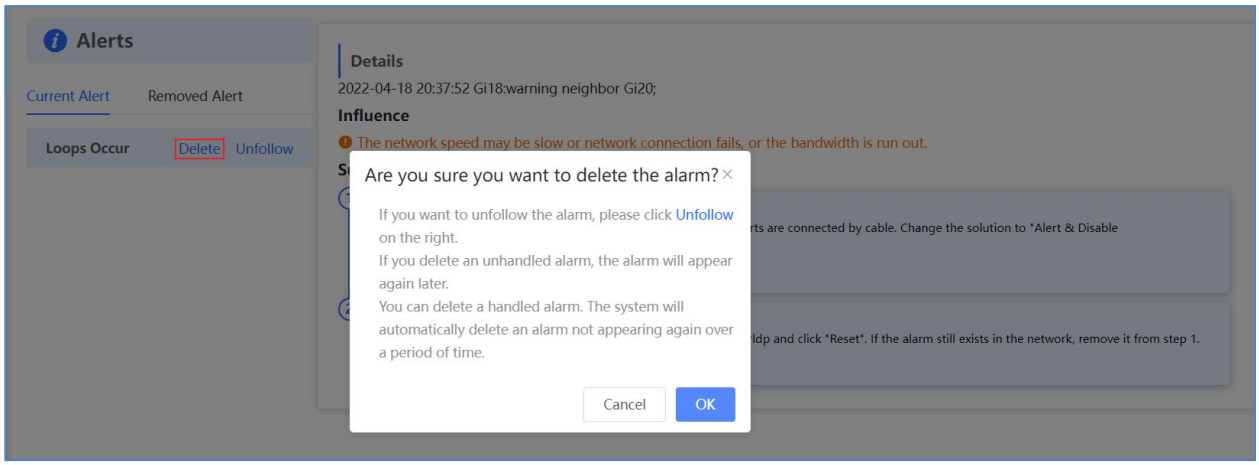


4.3.7.6 Alerts

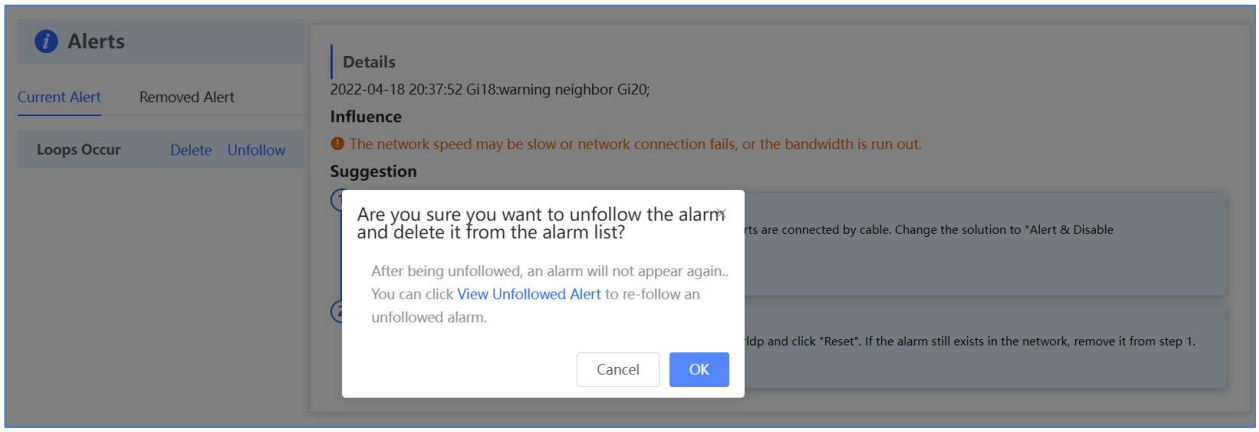
The **Alarms** module contains alarm events that may cause network errors or affect device performance. It also provides guidance to help users clear the alarms.



Delete



Unfollow



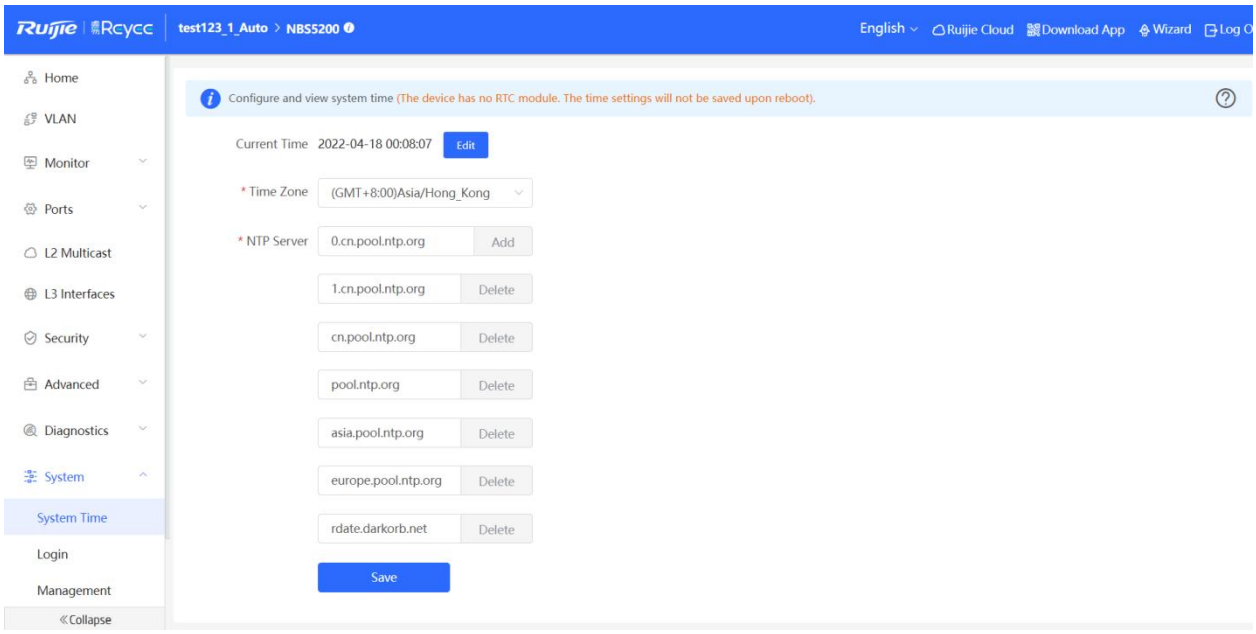
4.3.8 System

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

4.3.8.1 System Time

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

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



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

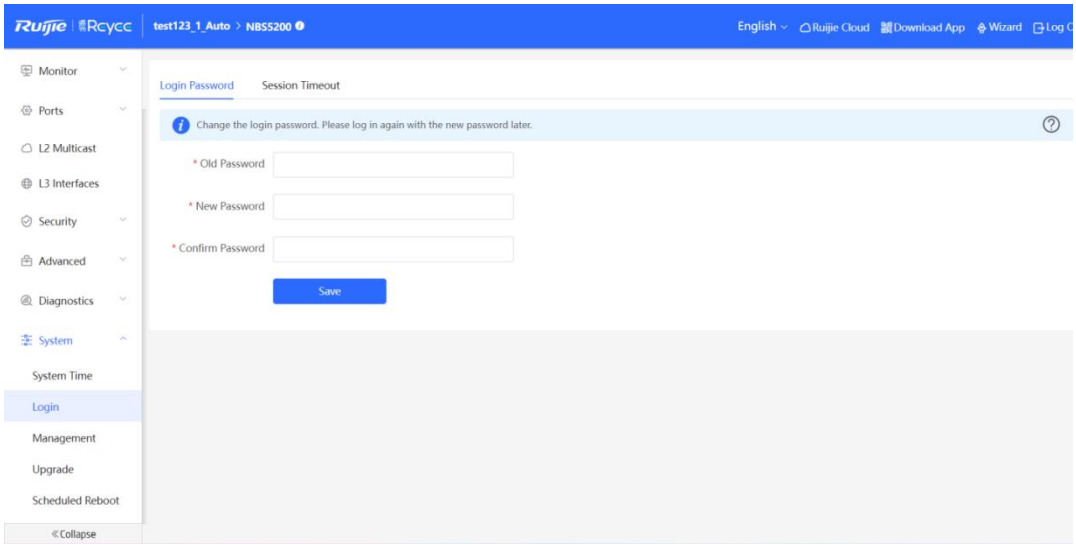
4.3.8.2 Login

The **Login** module allows you to perform a series of settings, including the **Login Password** and **Session Timeout**.

1.1 Login Password

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

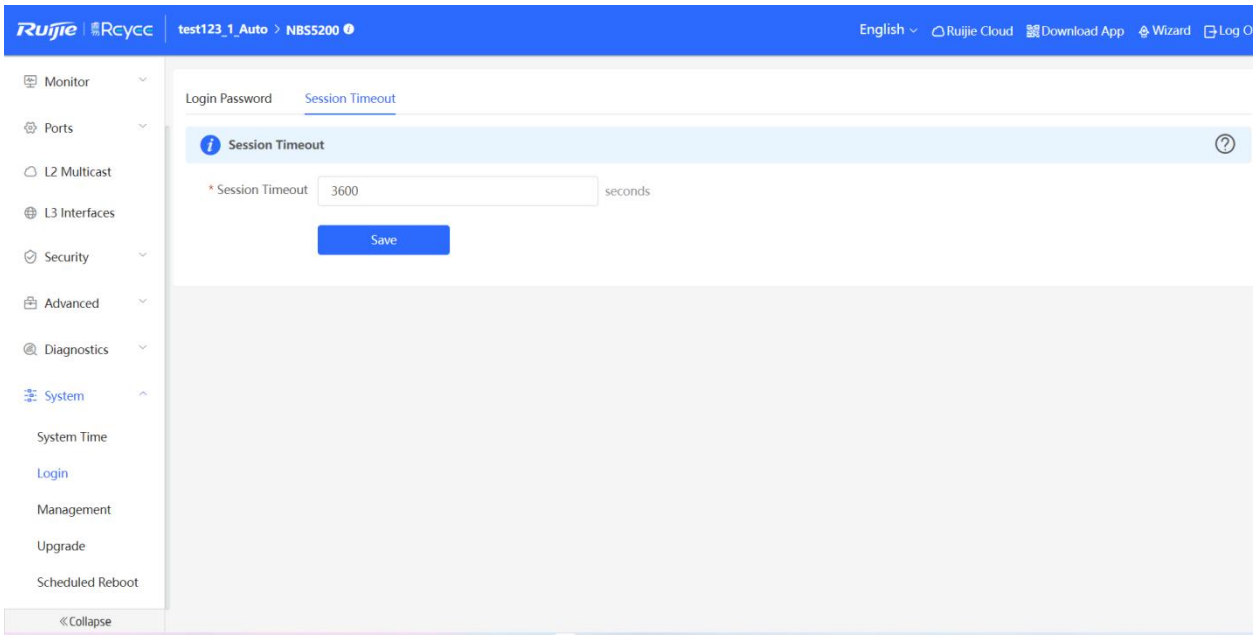
Enter the **old** and **new** passwords (at least 6 characters long), and click **Save.** (Please keep the login password in mind.)



1.2 Session Timeout

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

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



4.3.8.3 Management

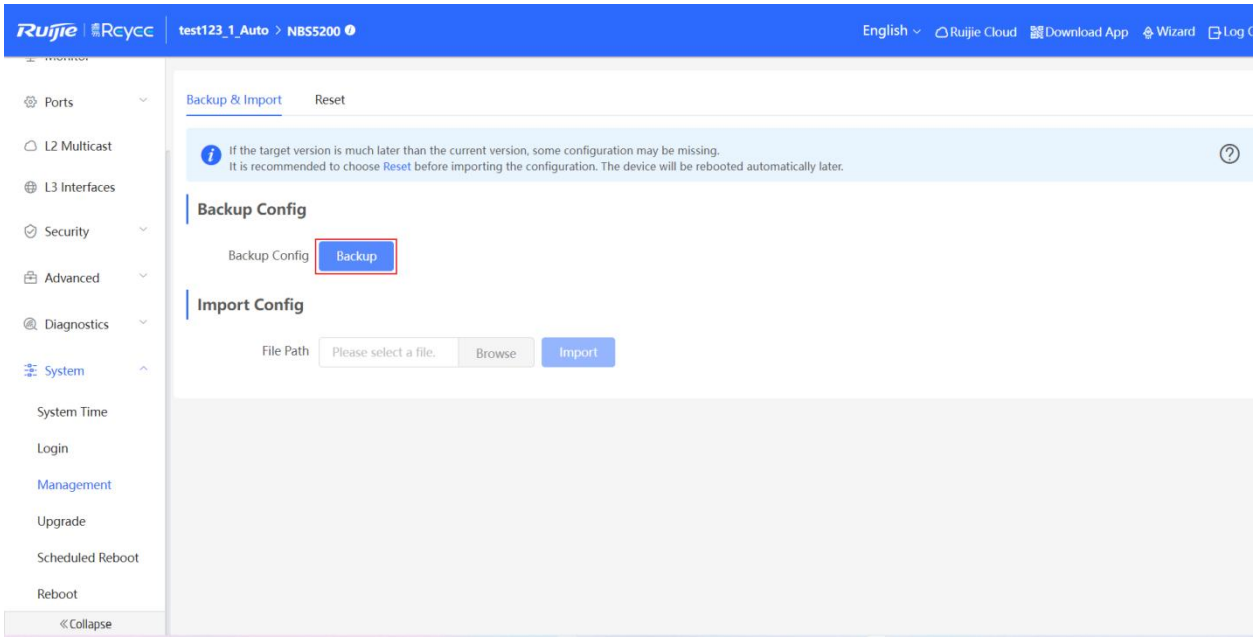
The **Management** module includes **Back & Import** and **Reset.**

1.1 Backup & Import

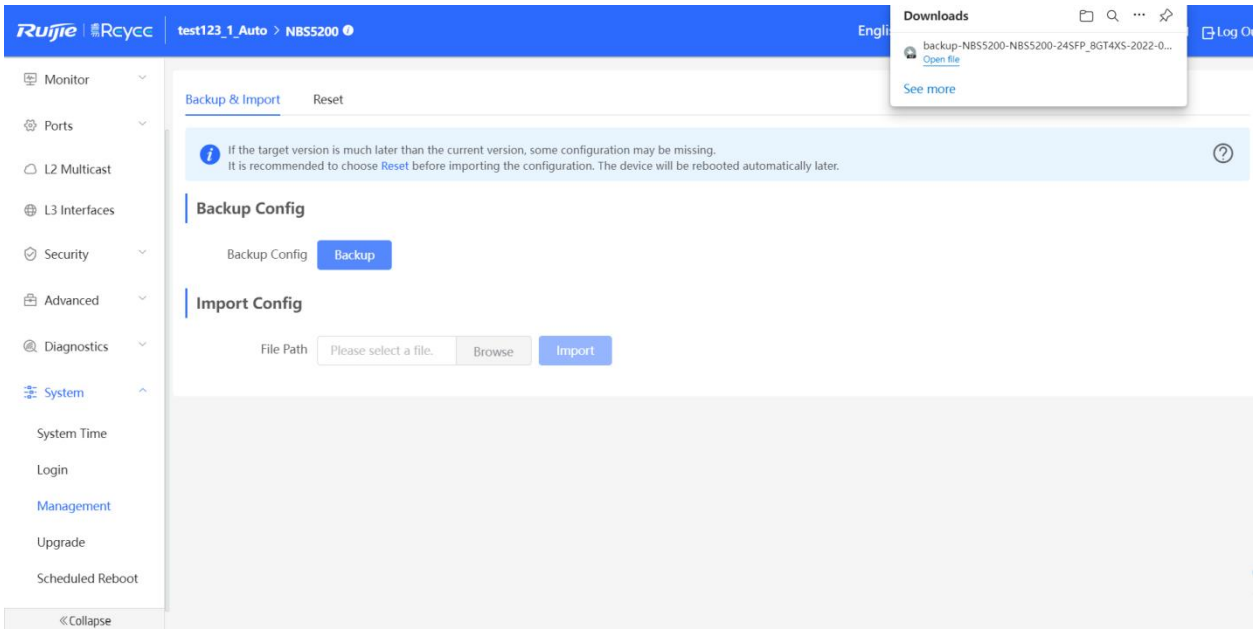
The **Backup & Import** page allows you to import a configuration file and apply the imported settings. It also allows exporting the configuration file to generate a backup.

Backup

Click **Backup** to export your current configuration in a file. It is recommended to do a backup before upgrading.

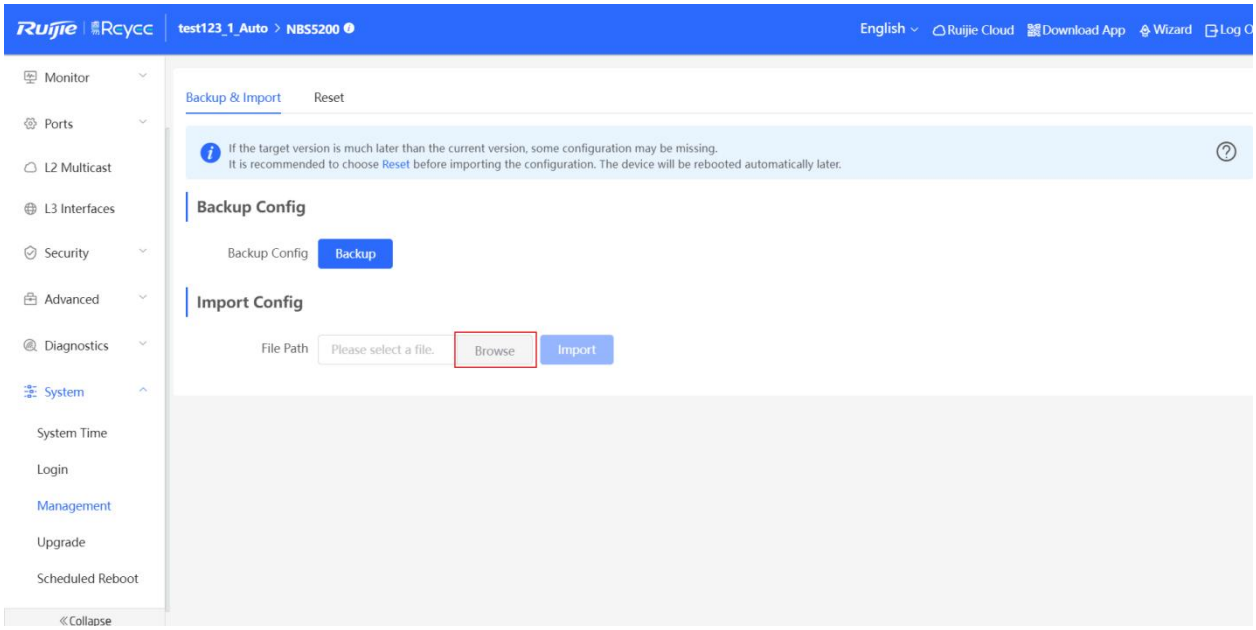


A configuration file with the suffix tar.gz will be downloaded

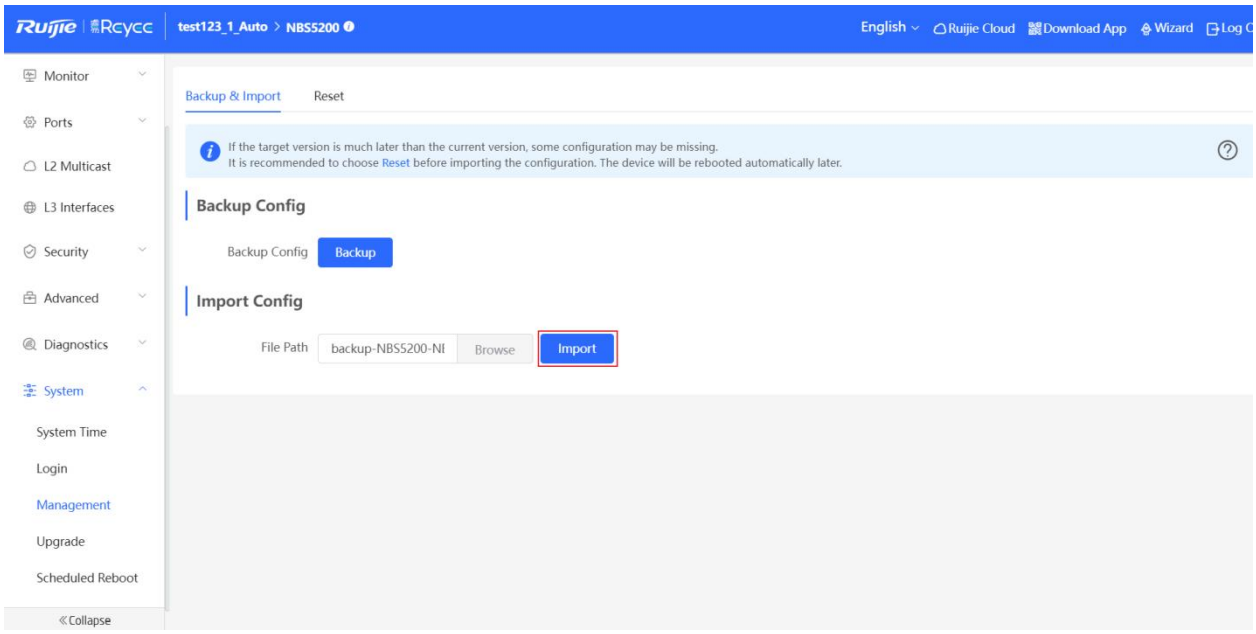


Import Config

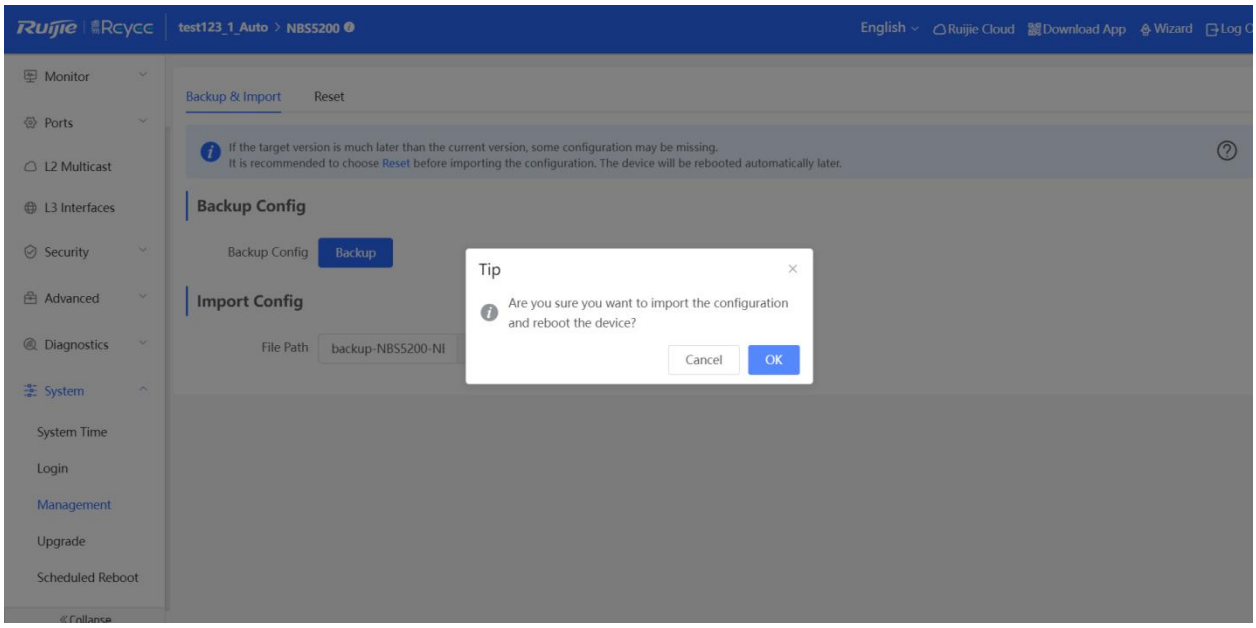
Click **Browse** to select the configuration file to import.



Click **Import** to import a configuration file to restore your configuration.



Click **OK** in the dialog box.



f The target version is much later than the current version, some configurations may be missed.

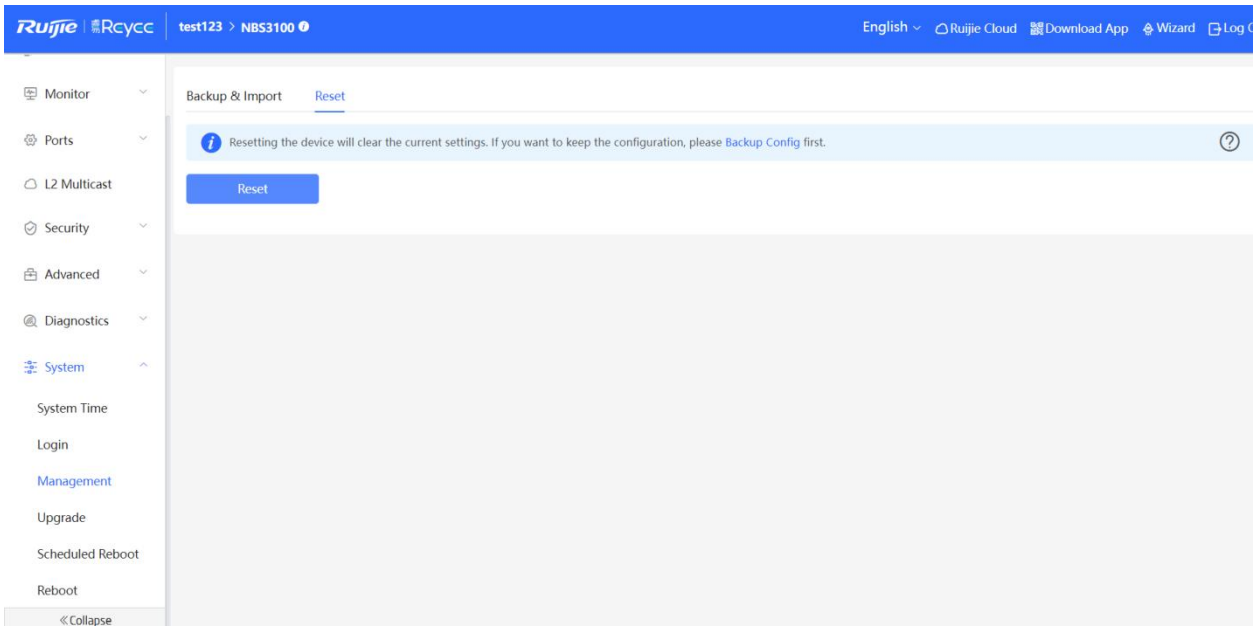
It is recommended to choose **Reset** before importing the configuration. The device will be rebooted automatically later.

1.2 Reset

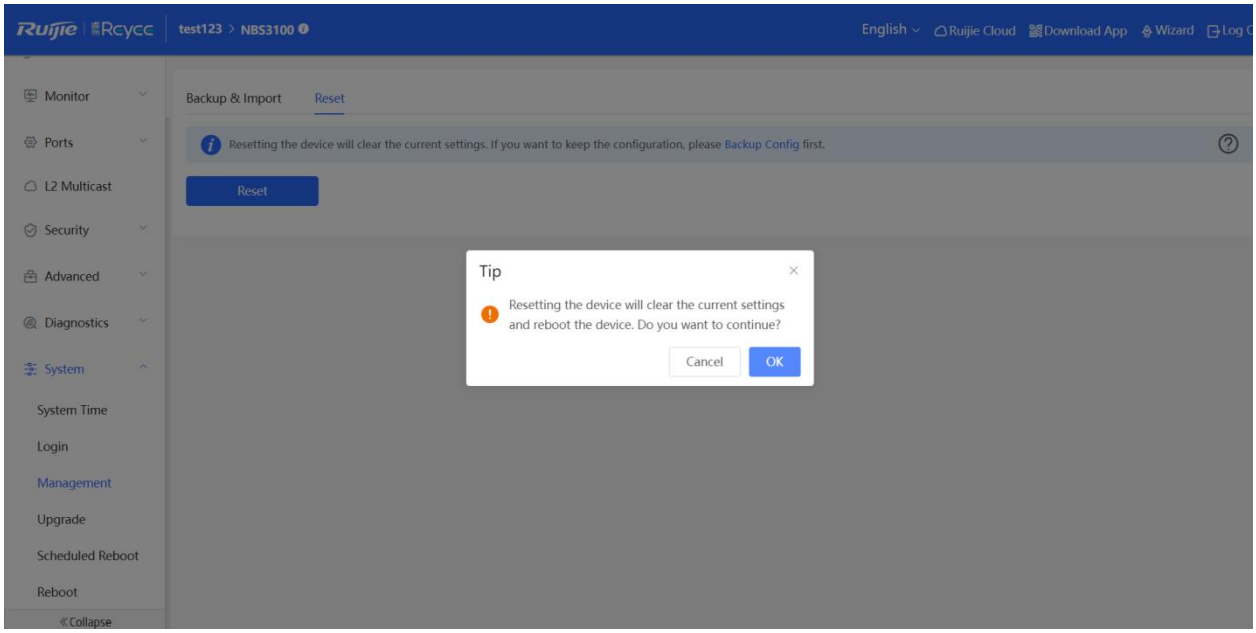
The **Reset** page allows you to restore the device to factory settings.

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

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



Click **OK** to restore all default values. This function is recommended when the network configuration is incorrect or the network environment is changed.

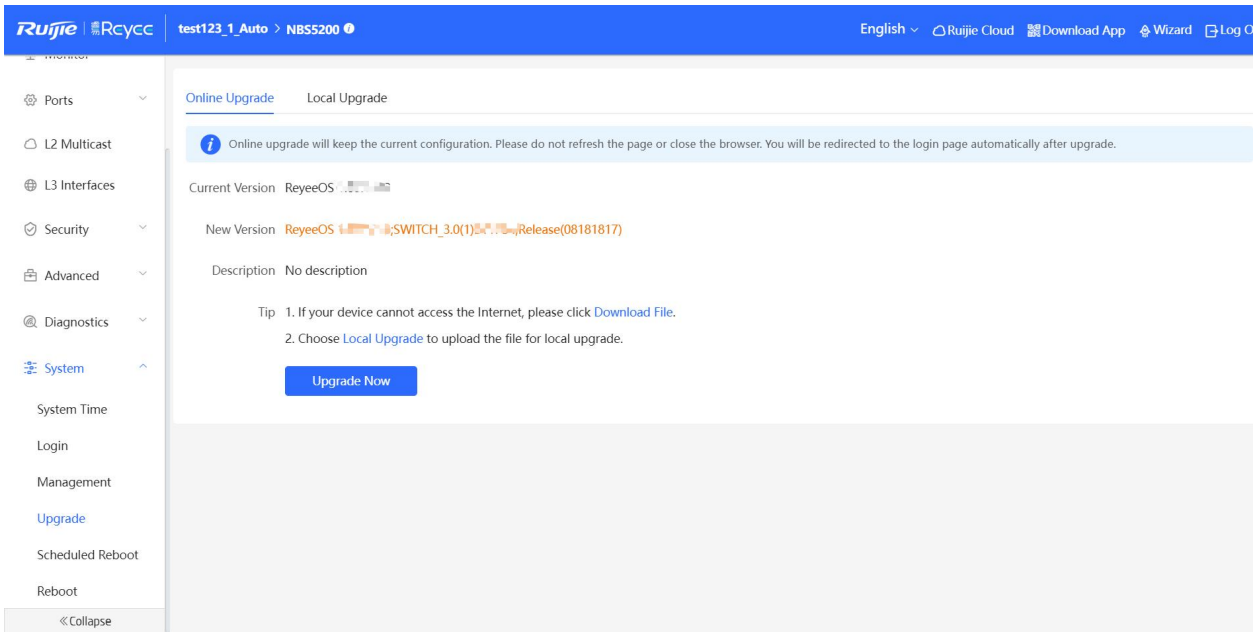


4.3.8.4 Upgrade

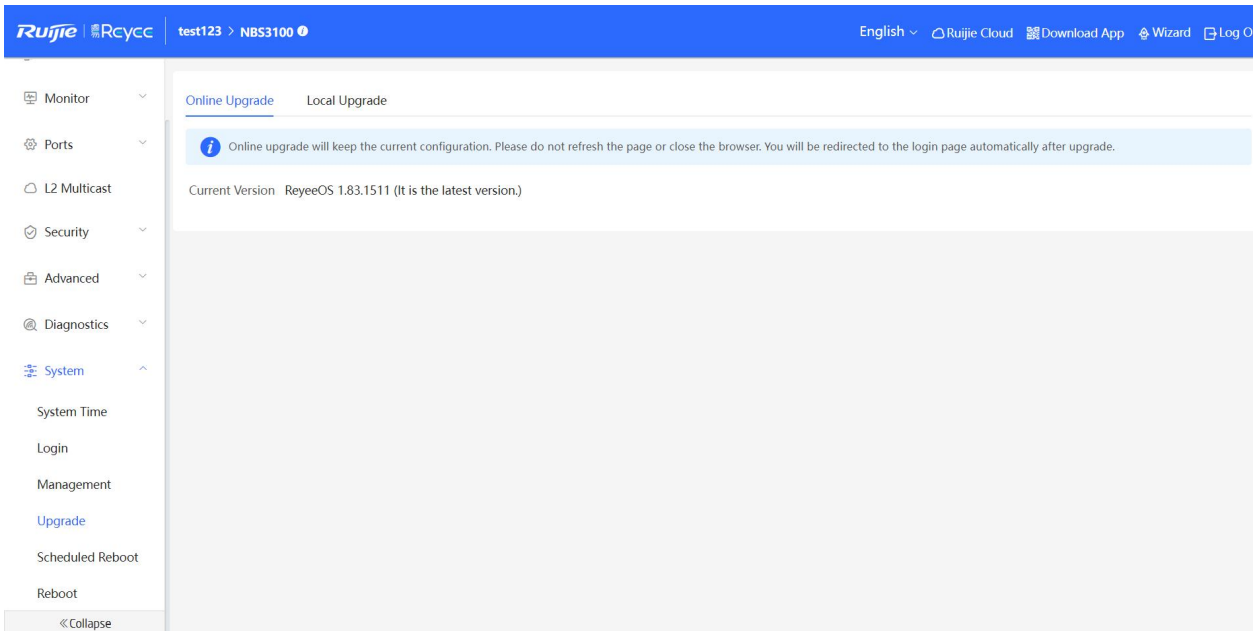
The **Upgrade** module includes **Online Upgrade** and **Local Upgrade.**

1.1 Online Upgrade

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



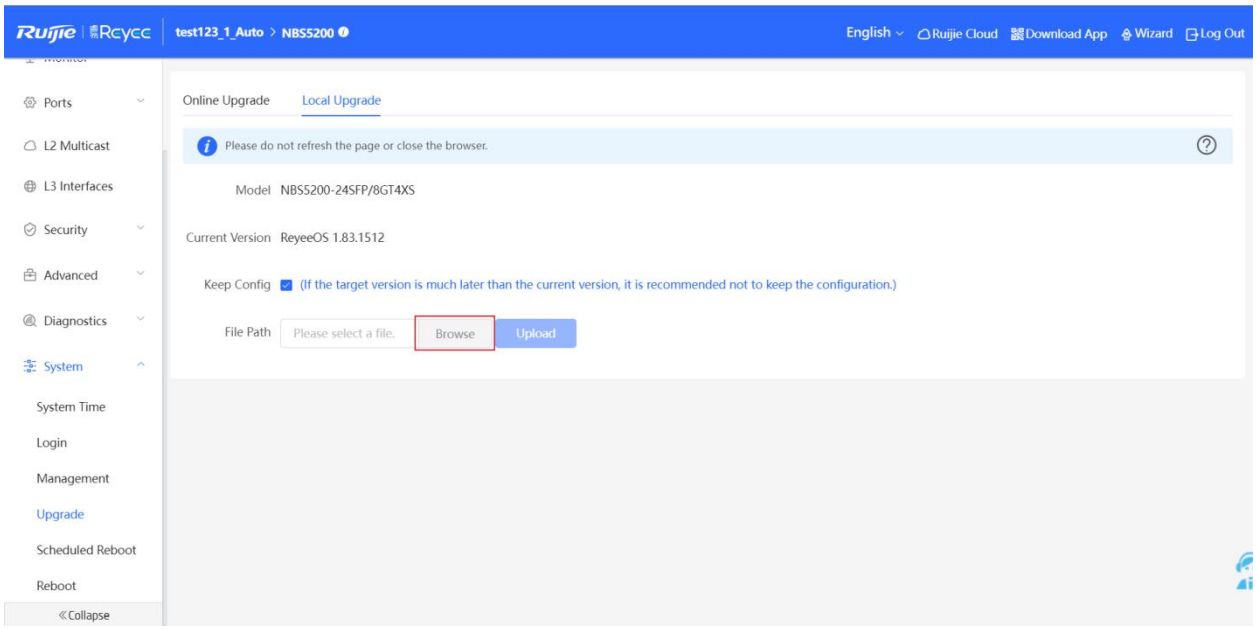
Click **Upgrade Now.** The device downloads the upgrade package from the network, and upgrades the current version. The upgrade operation retains configuration of the current device. Alternatively, you can select Download File to the local device and import the upgrade package on the Local Upgrade page.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



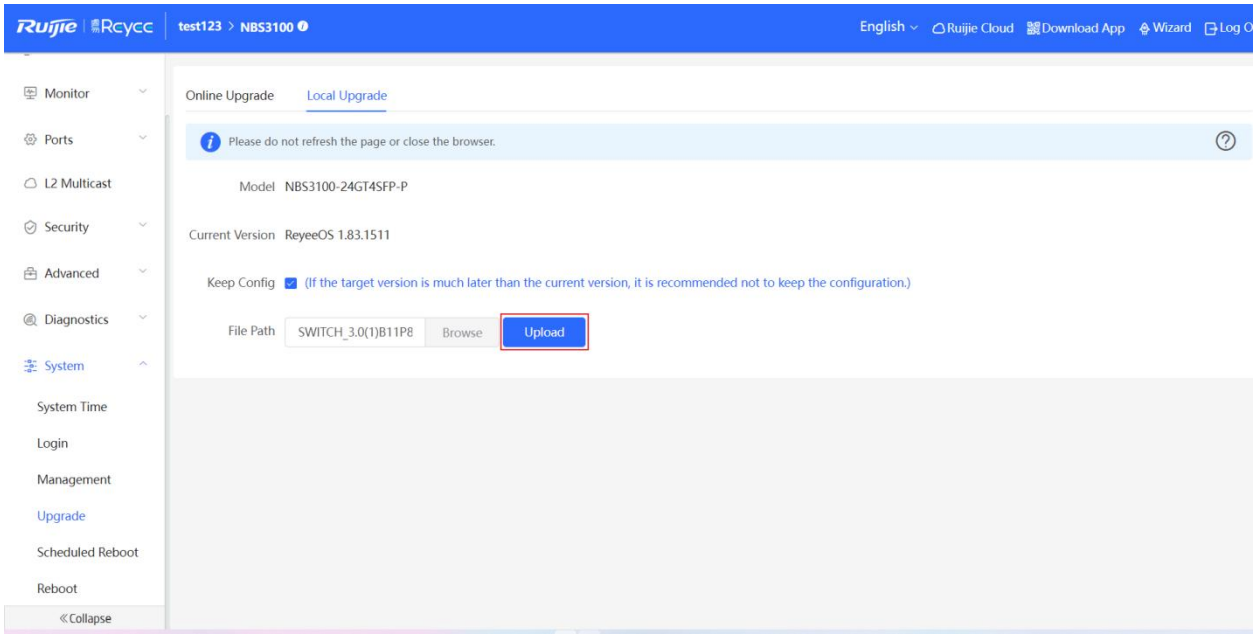
Online upgrade will maintain the current configuration. Please do not refresh the page or close the browser. You will be redirected to the login page automatically after upgrading.

1.2 Local Upgrade

Click **Browse** to select an upgrade package.



Click **Upload.**



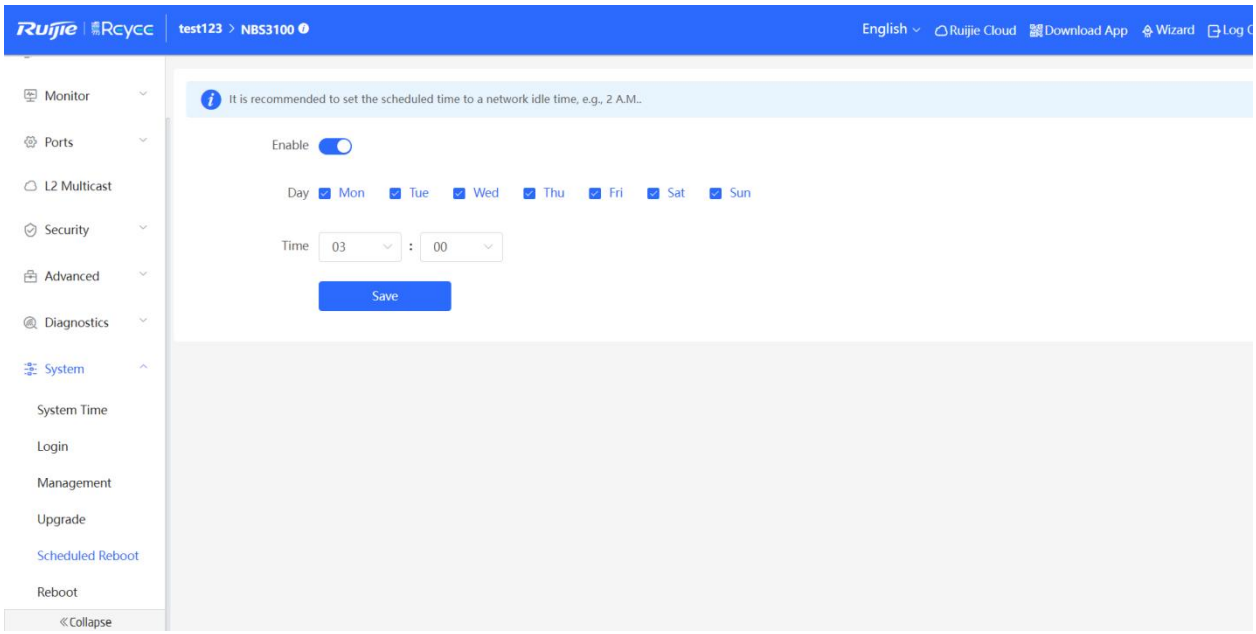
After uploading and checking the package, the device displays the upgrade package information and a prompt asking for upgrade confirmation, click **OK** to start the upgrade.

If the target version is much later than the current version, it is recommended not to retain the settings (uncheck **Keep Setup**).

The upgrade takes a period of time. **Do not refresh** the page or **close** the browser during the upgrade.

4.3.8.5 Scheduled Reboot

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

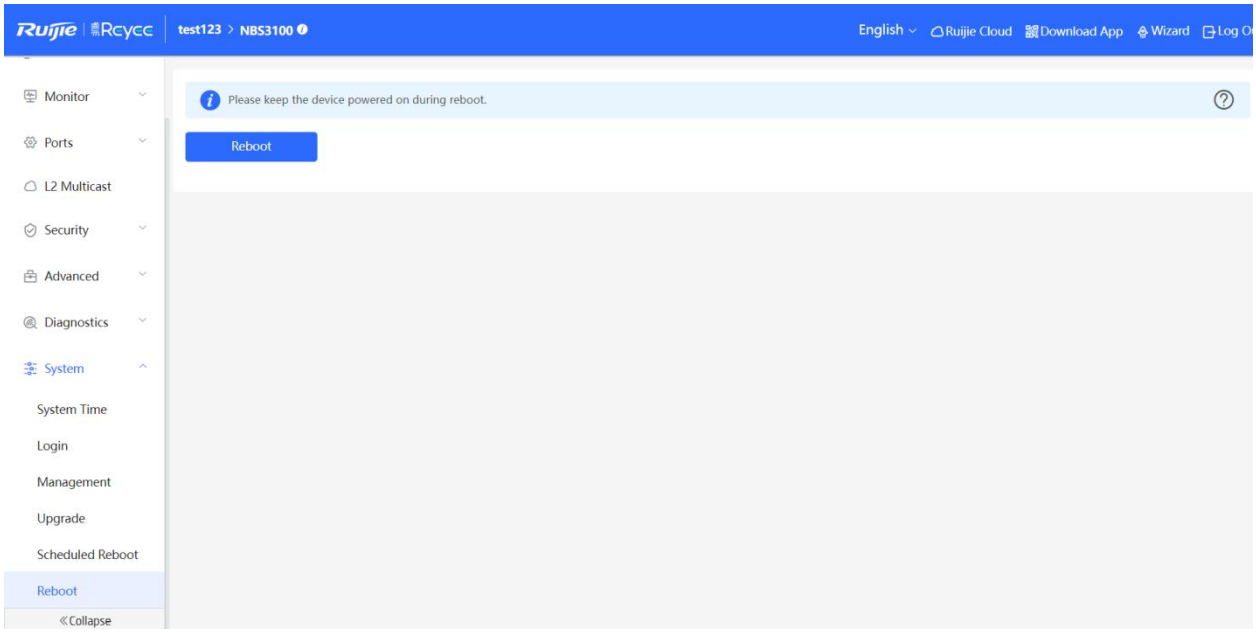


When this function is enabled, the system will be rebooted at scheduled time.. Off-peak hours are recommended for the reboot.

4.3.8.6 Reboot

The **Reboot** module provides a **Reboot** button.

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

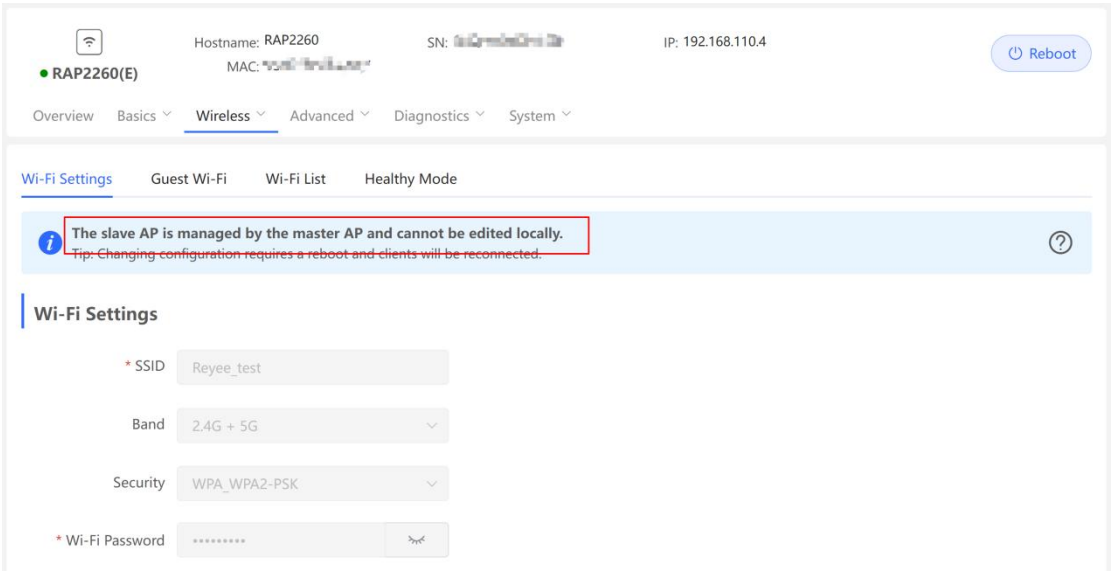


4.4 Reyee Access Point Configuration

4.4.1 Wireless Configuration

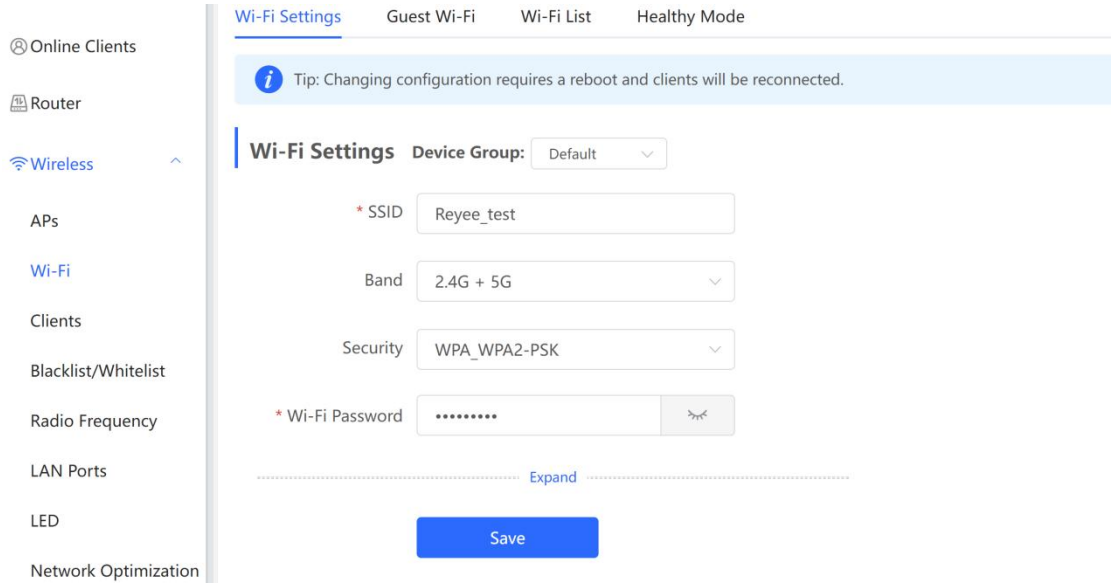
4.4.1.1 Wireless Basic Configuration

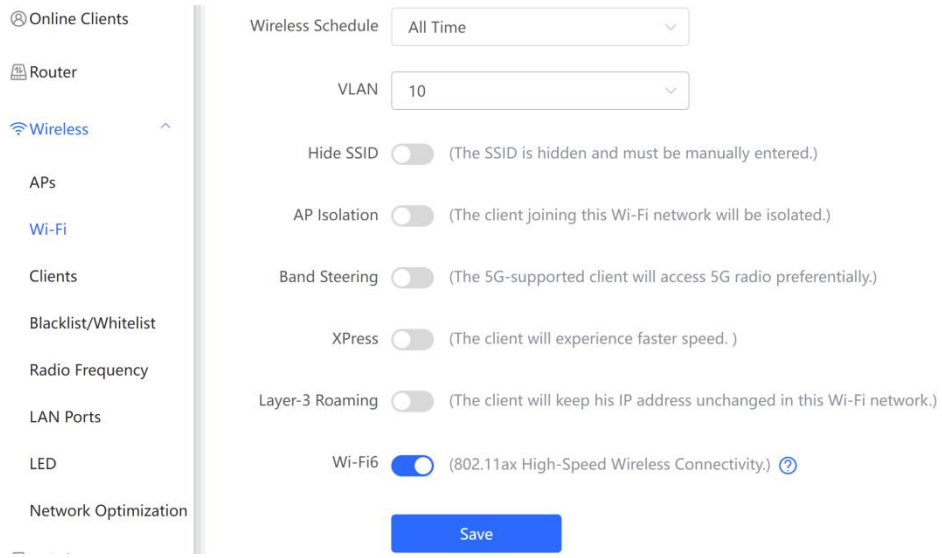
Configure the Wireless by Clicking **Wireless ->APs->Manage->Wireless->Wi-Fi.**



4 It will be found that it cannot be configured at this time, because the SON role of the AP is slave AP, so the SSID can only be configured in the following ways:

Click **Wireless—Wi-Fi—Wi-Fi settings** to Configure Wireless

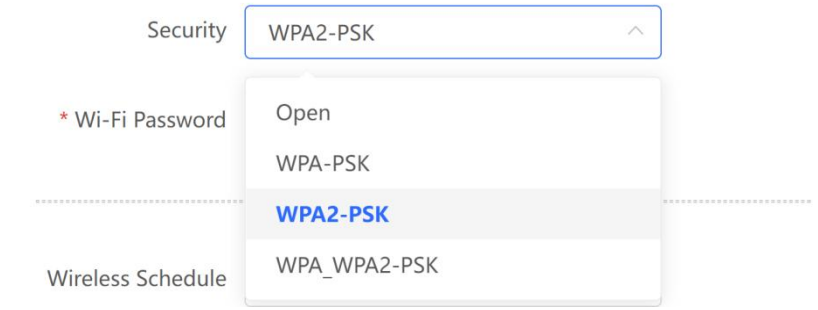




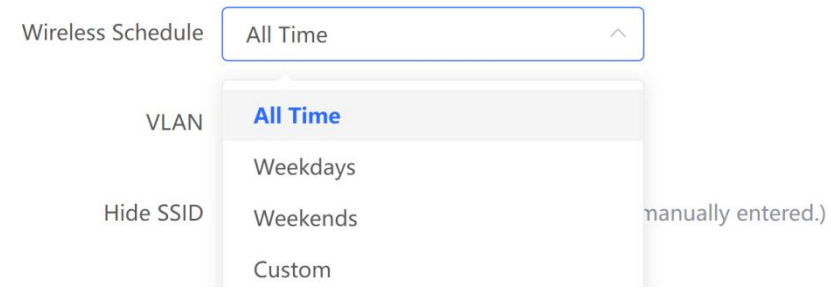
SSID: Wi-Fi Name

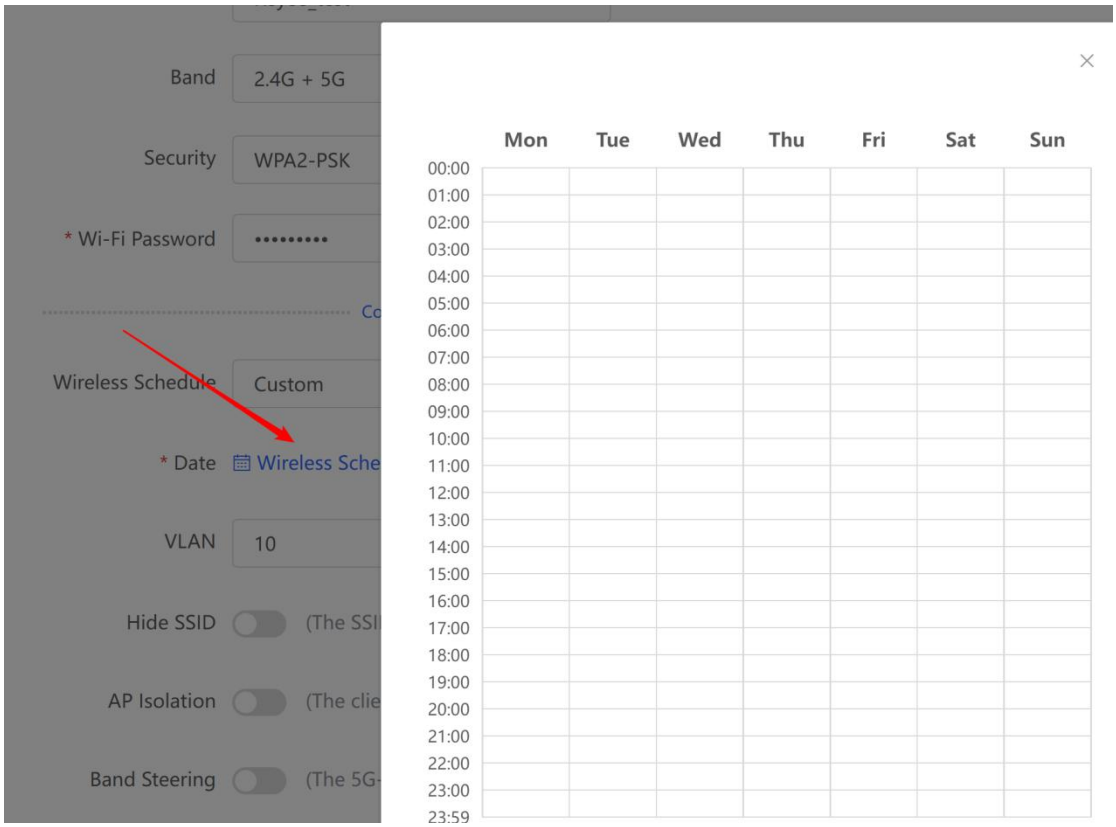
Band: Three modes, 2.4G, 5G or both on

Security: Open, WPA-PSK, WPA2-PSK,WPA_WPA2-PSK



Wireless Schedule: it is used to choose the time when Wi-Fi takes effect.





Hide SSID: disable/enable broadcasting SSID

AP isolation: SSID-based client isolation

Band Steering： 5G-Prior Access detects clients capable of 5 GHz operation and steers them to that frequency, while leaving 2.4 GHz available for legacy clients. It is not recommended to enable this function if most of clients only support 2.4GHZ

XPress: enable faster speed

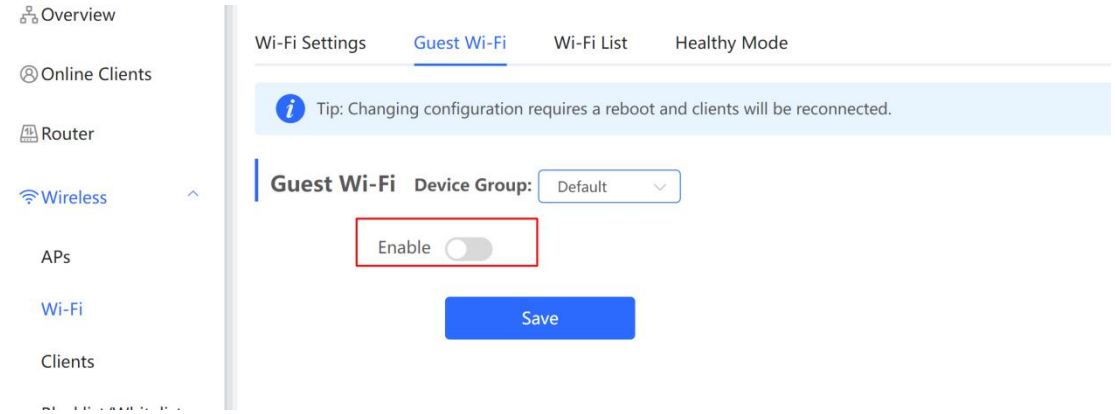
Layer-3 Roaming: The client will keep his IP address unchanged in this Wi-Fi network, Layer 3 roaming of Reyee AP can only be enabled here, and Ruijie Cloud only supports Ruijie AP.

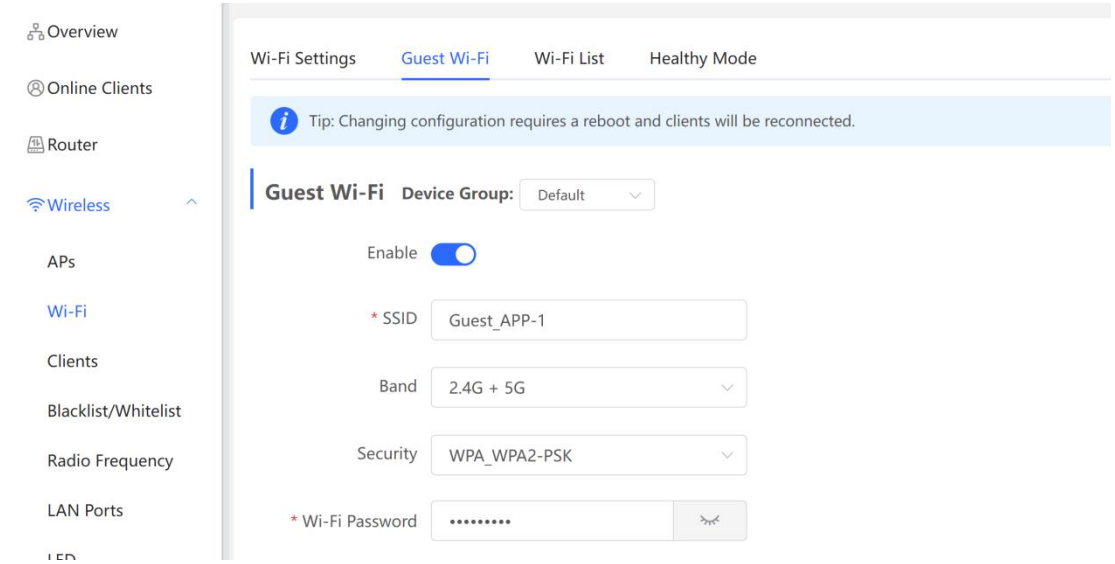
Wi-Fi 6: Some wireless adapters of old versions may not be compatible. The end points accessing the Wi-Fi6 network must support 802.11ax.

4.4.1.2 Guest Wi-Fi Configuration

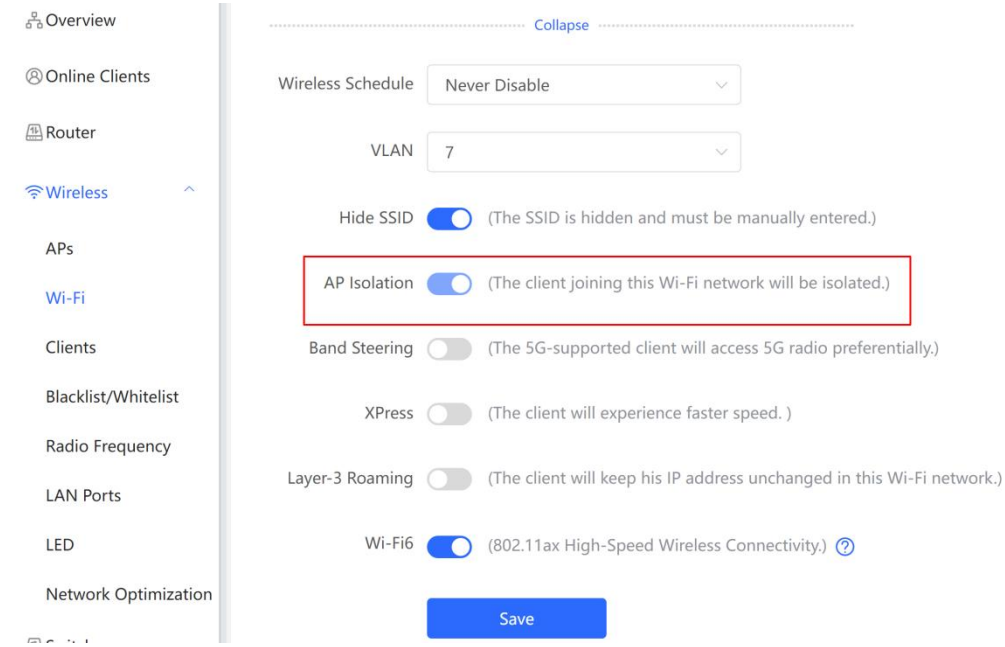
Click **Wireless—>Wi-Fi—>Guest Wi-Fi** to Configure Wireless

The guest Wi-Fi is disabled by default. You can enable the guest Wi-Fi on below page or **Homepage.**

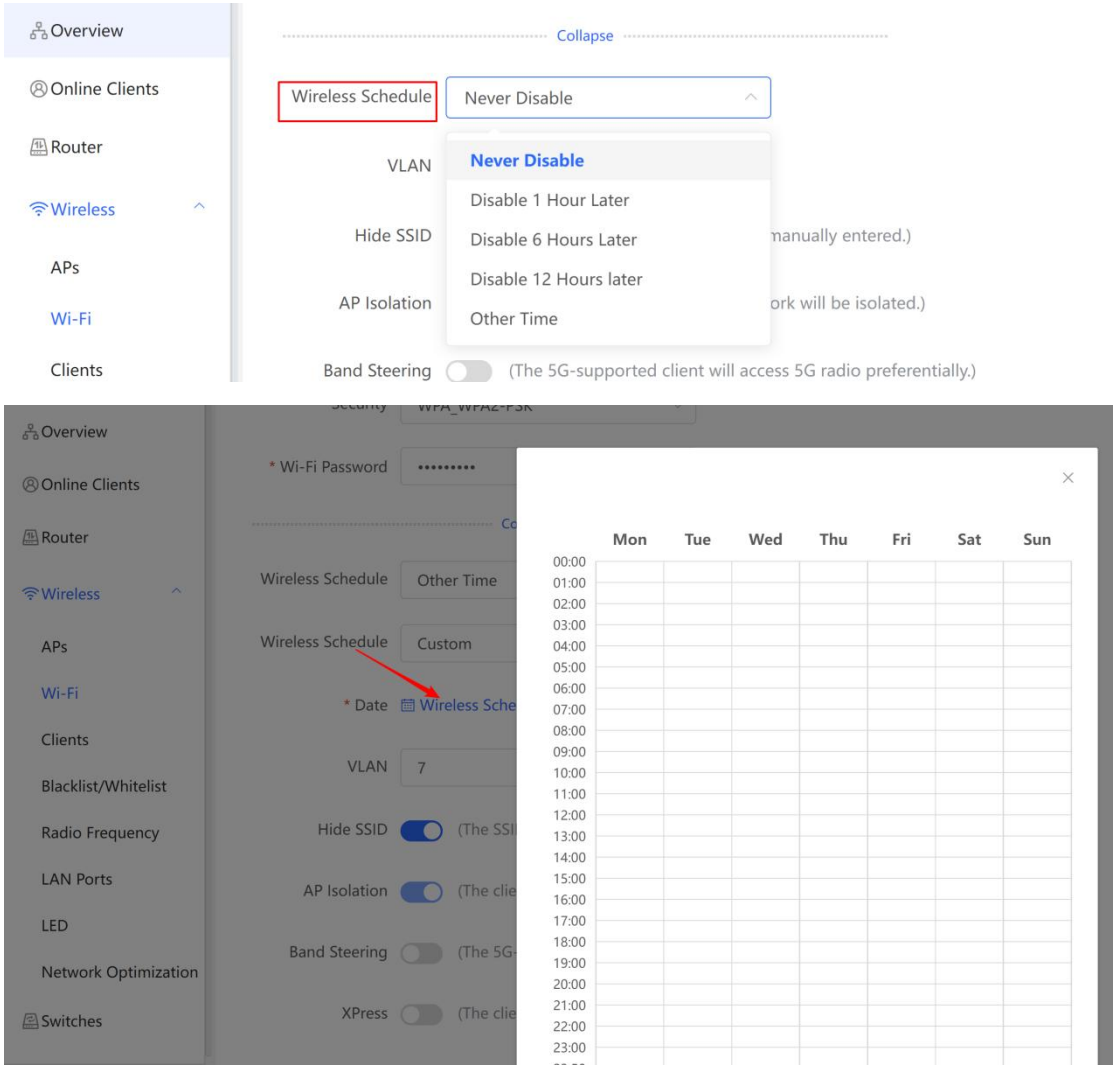




- **AP isolation is enabled by default and cannot be edited.**

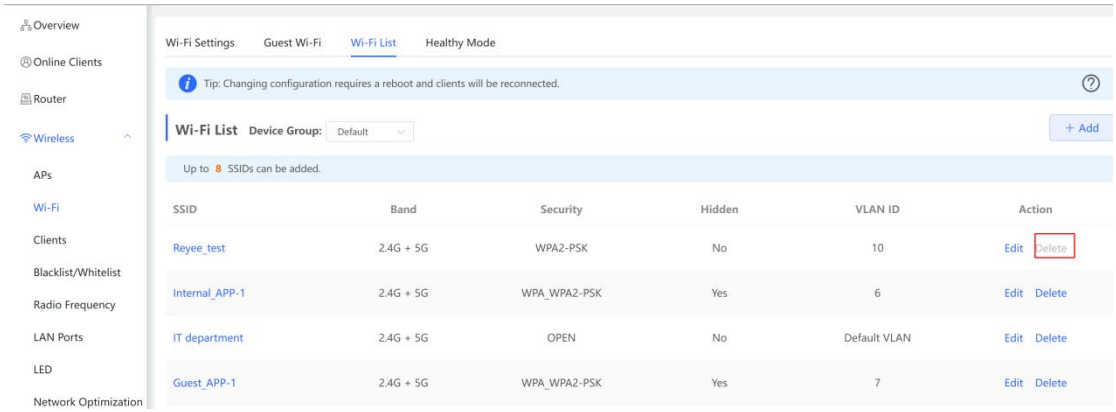


Set a schedule, and the guest Wi-Fi will be enabled only during this period time. When the time expires, the guest Wi-Fi will be disabled.

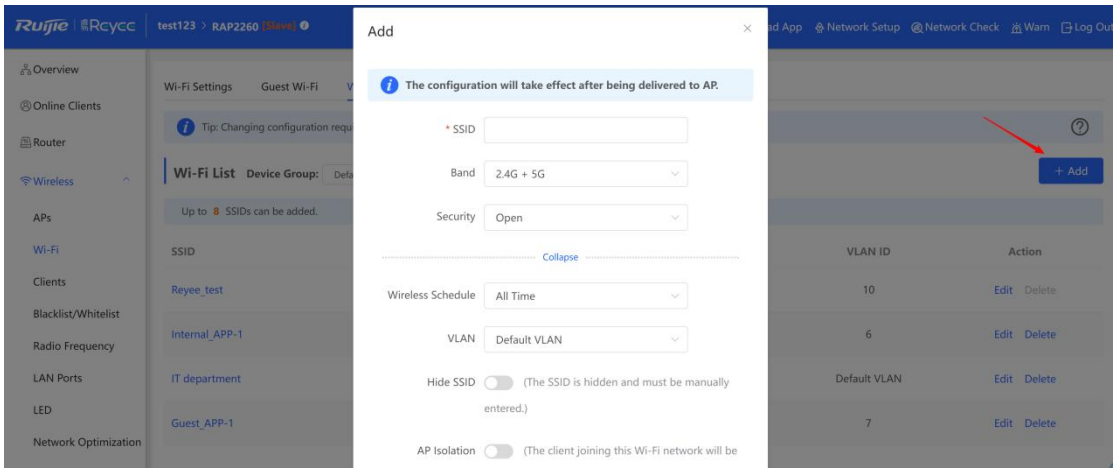


4.4.1.3 Multiple SSID Configuration

- The **Wi-Fi List** displays all Wi-Fi networks. The primary Wi-Fi is also listed here and cannot be deleted.
- It is necessary to reboot your device if you want to change your configuration and your network will be reconnected.

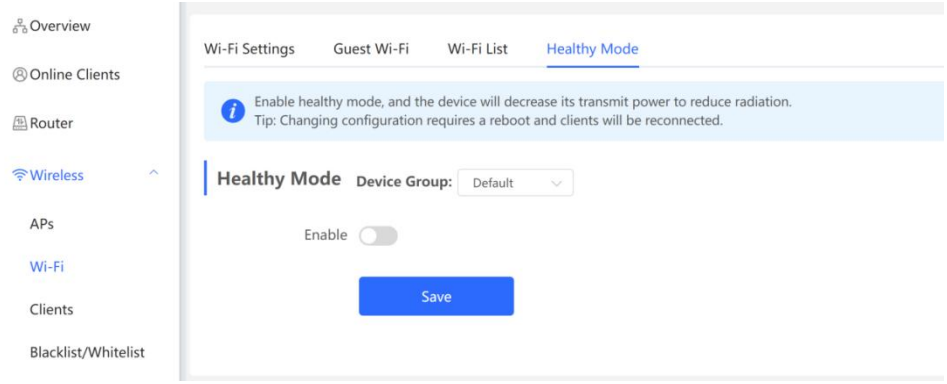


- Click **Add** to add a Wi-Fi network. In the displayed dialog box, configure your settings and click **OK** to save your configuration.



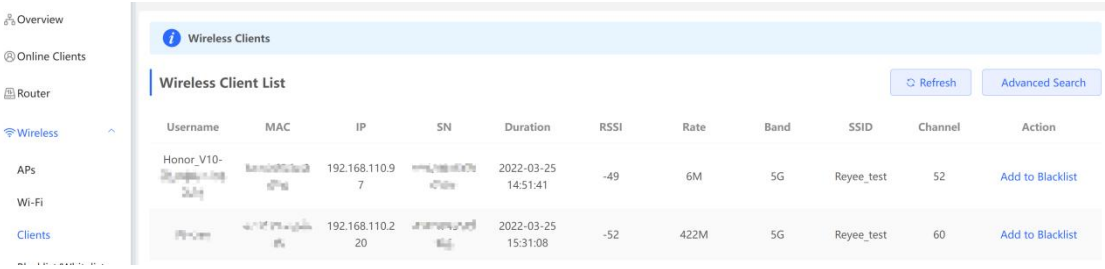
4.4.1.4 Healthy Mode

- The **Healthy Mode** module allows you to enable health mode and set a schedule.
- Enable **Healthy Mode**, and the device will decrease its transmit power to reduce radiation.
- It is necessary to reboot your device if you want to change your configuration and your network will be reconnected.
- Router radiation is much lower than common radiation which doesn't harm to the human body.



4.4.1.5 Wireless Client List

- The Clients module displays the wireless clients

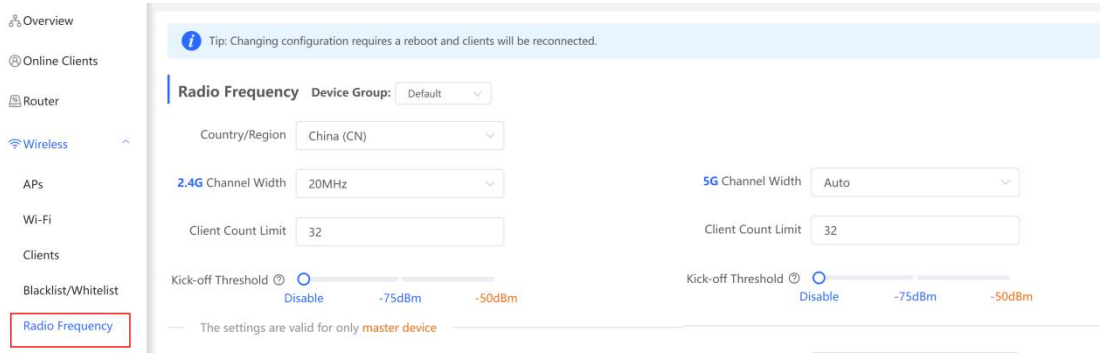


Click **Advanced Search**, and you can search clients by SN and MAC address.

4.4.1.6 Radio Frequency Configuration

Click **Wireless—>Radio Frequency** to Configure Radio Frequency

The **Radio Frequency** allows you to configure the Radio Frequency parameters.

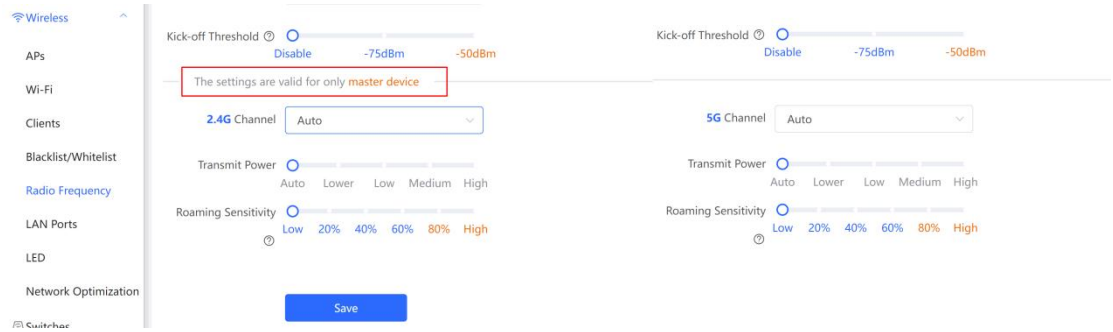


Country/Region: Choose the Country/Region according to your location.

2.4G/5GChannel Width: Different products, different regions may be have different channel width.. If the interference is severe, choose a lower channel width to avoid network stalling. The access point supports the channel width of 20 MHz and 40 MHz. You are advised to select 20MHz channel width. After changing the channel width, click Save to make the configuration take effect immediately.

Client Count Limit: Limit the number of connected clients. If the access point is associated with too many clients, it will have a lower performance, affecting user experience. After you configure the threshold, new clients over the threshold will not be allowed to access the Wi-Fi network. You can lower the threshold if there is requirement for bandwidth per client. You are advised to keep the default settings unless there are special cases.

Kick-off Threshold: Farther the client is from the access point, lower the signal strength is. When the signal strength is lower than the threshold, the client will be forced offline and select a nearer Wi-Fi signal.



2.4G/5G Channel: When set to Auto, the device will automatically select the best channel according to the environmental interference. Can also choose the best channel identified by Wi-Fi Moho or other Wi-Fi scanning App. Click **Save** to make the configuration take effect immediately. The more devices in a channel, the greater the interference.

Transmit Power: Lower means 25%, Low means 50%, Medium means 75%, High means 100%, the larger the value, the wider the coverage.

A greater transmit power indicates a larger coverage and brings stronger interference to surrounding wireless routers. In a high-density scenario, you are advised to set the transmit power to a small value. The Auto mode is recommended, indicating automatic adjustment of the transmit power.

Roaming Sensitivity:

a) Roaming sensitivity is the rate at which your device selects and switches to the nearest available access point, offering a better signal.

b) A higher roaming sensitivity level indicates a poorer Wi-Fi coverage.

c) If your device will not roam, select a low roaming sensitivity level.

d) If your device will roam, increase the roaming sensitivity level to get a better signal.

A lower level indicates a greater coverage and less frequent roaming.

Advantage: The connection will stay up.

Disadvantage: The signal may be poor.

A higher level indicates a poorer coverage and more frequent roaming

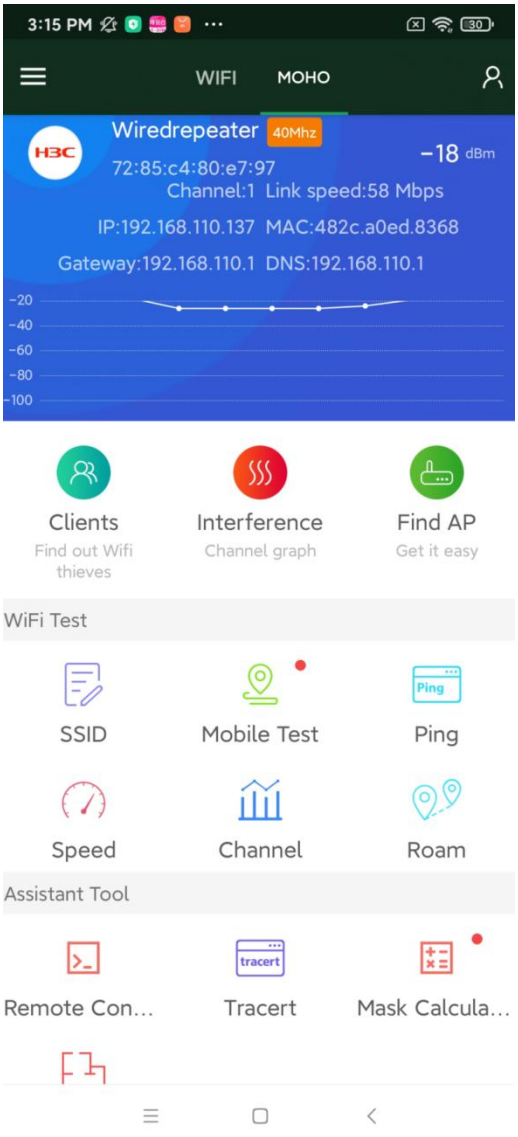
Advantage: The device will send a strong signal.

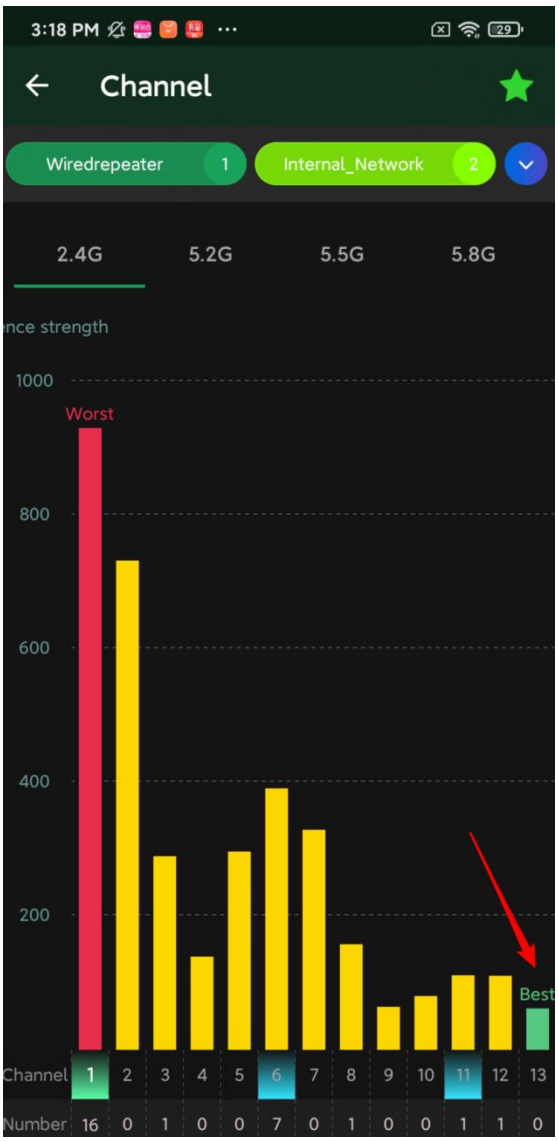
Disadvantage: The connection will be down briefly when roaming occurs.

Wireless Optimization Example:

Turn on Wi-Fi Moho when SSID is connected, can click channel to view the current environmental channel utilization.

In the figure below, can see that channel 1 is crowded under 2.4G, and channel 13 is the best.

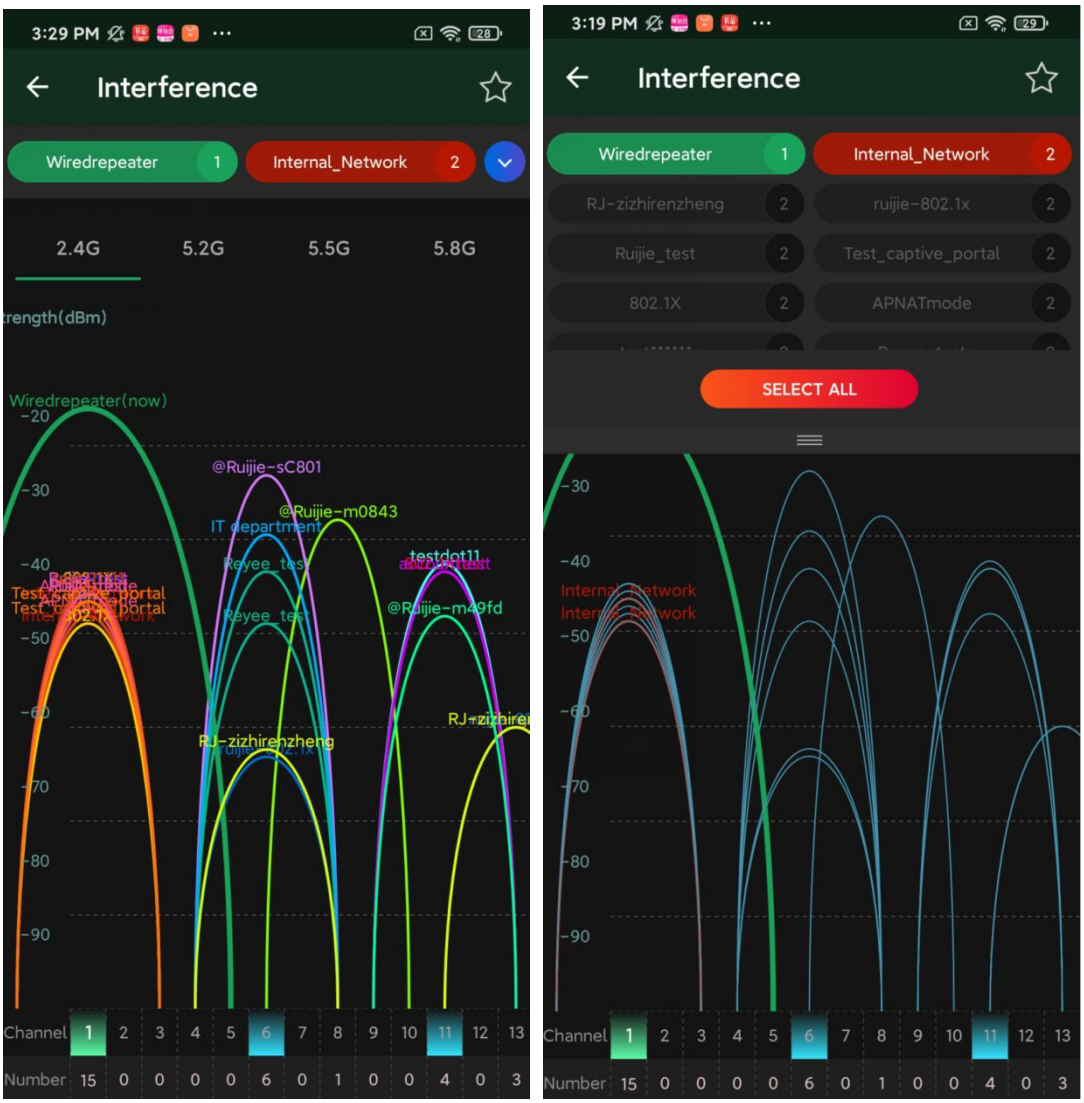




When you want to know which SSID belongs to which channel, can click interface:

The green color represents the currently connected SSID, can select the remaining SSIDs on the top to view which channel belongs to.

When your wireless speed is slow or in the stage of deployment, you can use WI-FI Moho to check, choose the channel with the least interference.



4.4.1.7 Wireless black/whitelist Configuration

The Blacklist / Whitelist module allows you to configure wireless global or SSID-based client blacklist and whitelist. Blacklist and whitelist can achieve full match or prefix match (OUI).

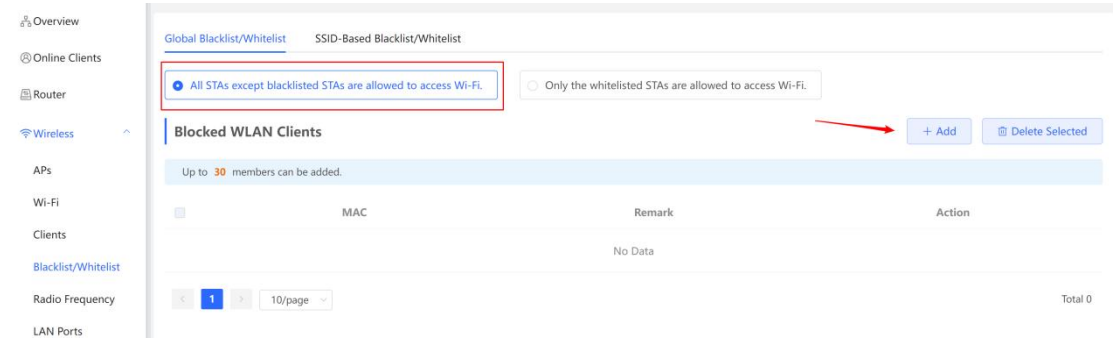
Click **Wireless—Blacklist/Whitelist** to Configure

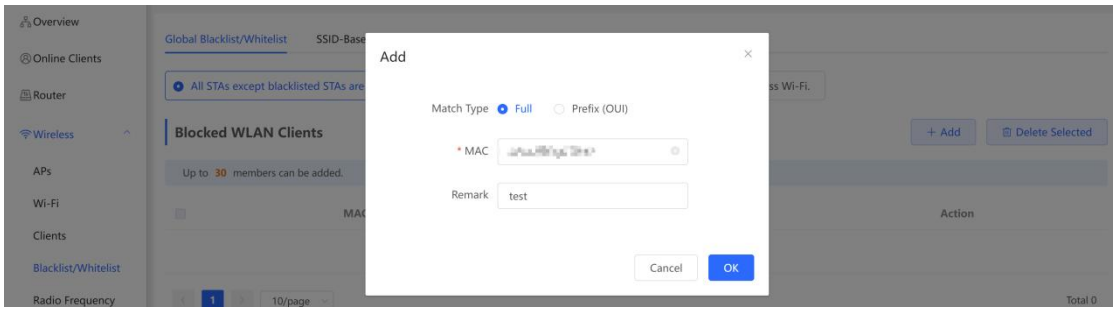
Global Blacklist/Whitelist

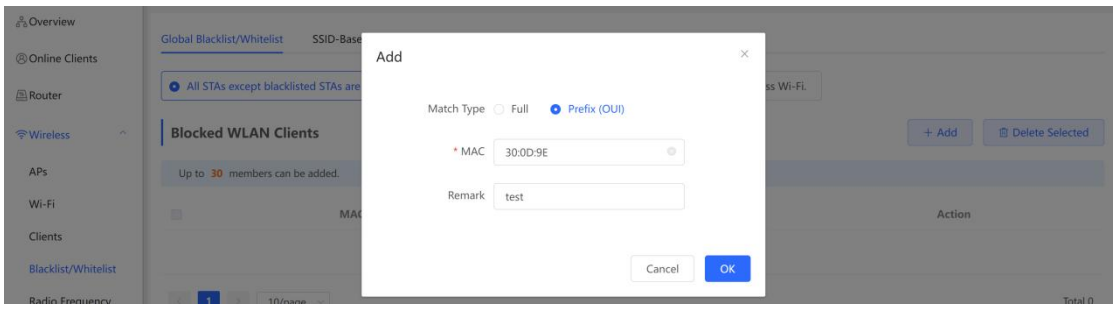
Click Add to add a blacklisted or whitelisted client. In the displayed dialog box, configure settings and click OK.

Blacklist configuration:

The blacklist is empty by default and all clients will be allowed to access the Internet. You can choose Clients to blacklist manually.



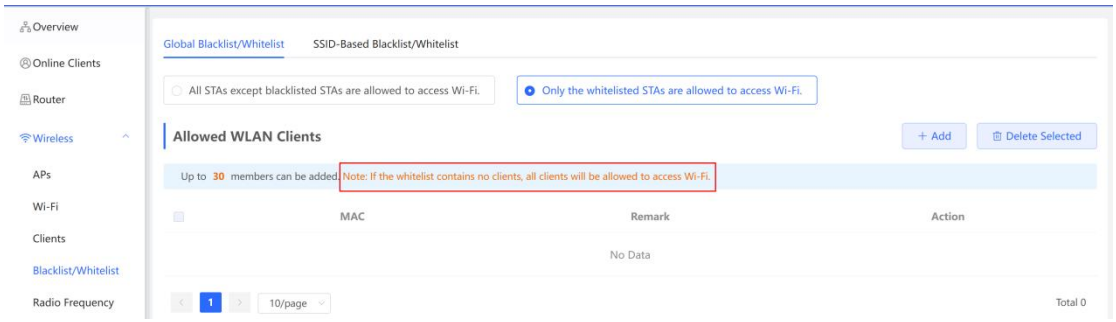




Whitelist configuration:

All online clients will be included into the whitelist by default. You can add or delete whitelist members to allow or forbid clients' accessing to the Internet.

Note: No clients in the whitelist means all clients will be allowed to access Wi-Fi.



a) SSID-Based Blacklist/Whitelist

Blacklist/Whitelist is used to allow or reject a client's request to connect to the Wi-Fi network.

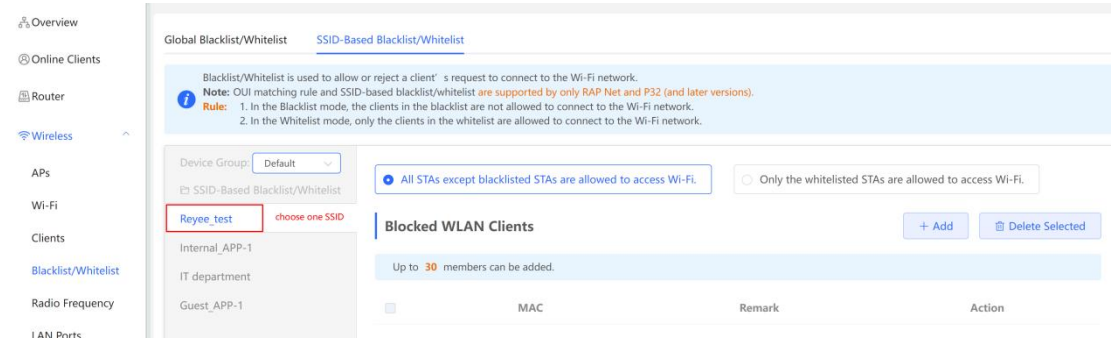
Note:

OUI matching rule and SSID-based blacklist/whitelist are supported by only RAP Net and P32 (and later versions).

Rules:

1. In the Blacklist mode, the clients in the blacklist are not allowed to connect to the Wi-Fi network.

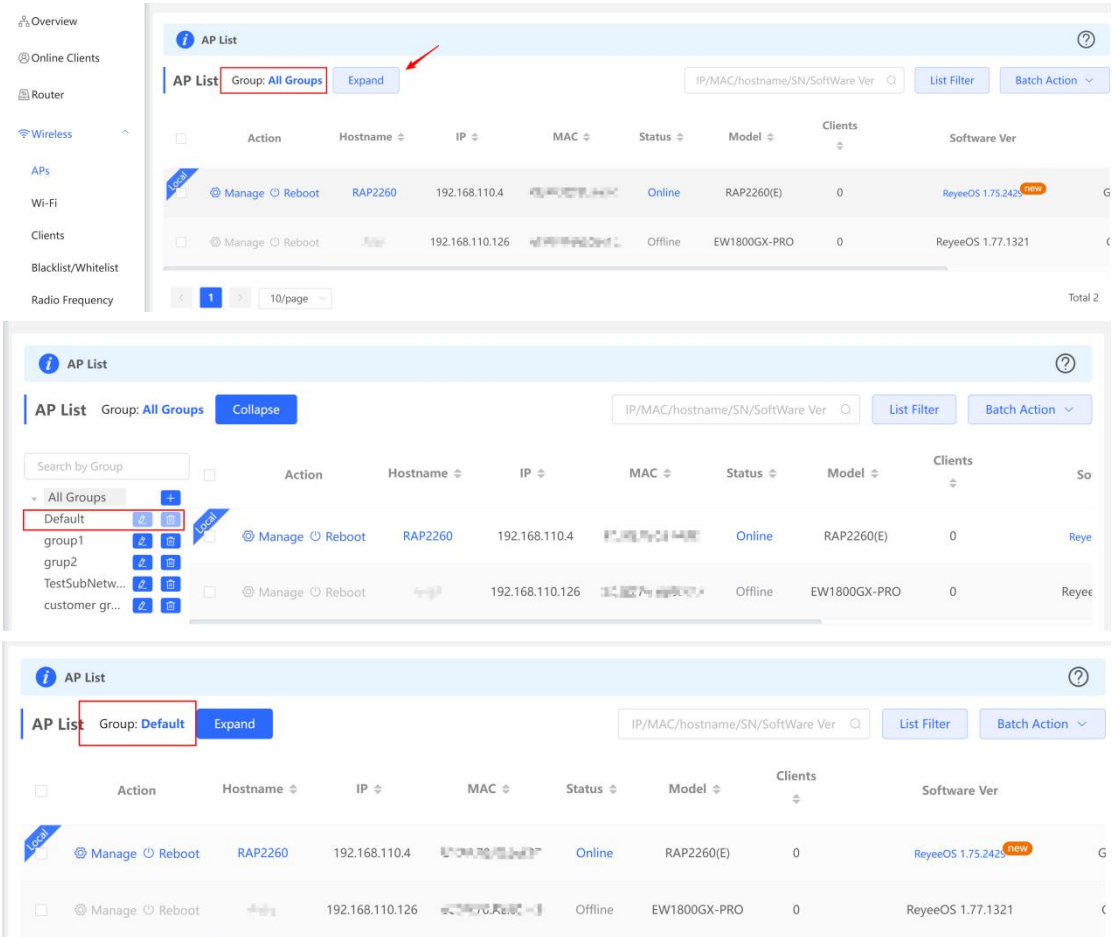
2. In the Whitelist mode, only the clients in the whitelist are allowed to connect to the Wi-Fi network.



4.4.1.8 AP Group Configuration

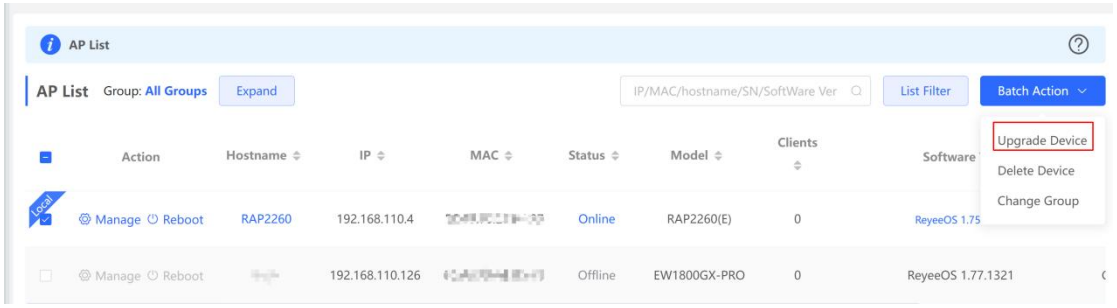
a) AP group, batch upgrade, delete

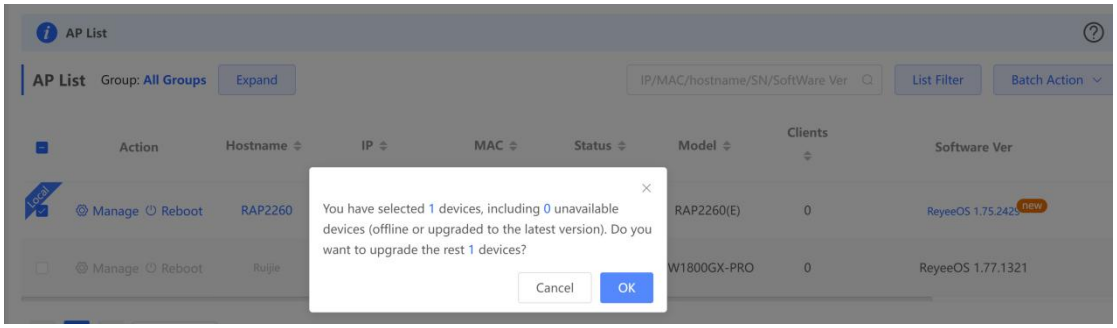
All devices are added on default group which cannot be renamed or deleted.

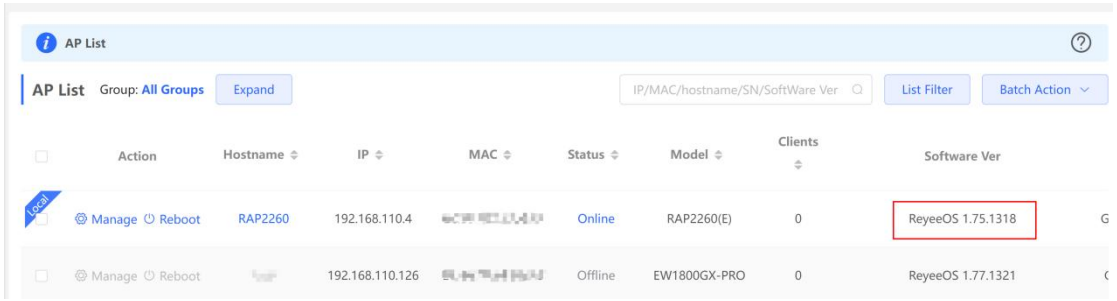


The APs in the default group can be upgraded, deleted in batches or moved to other groups.

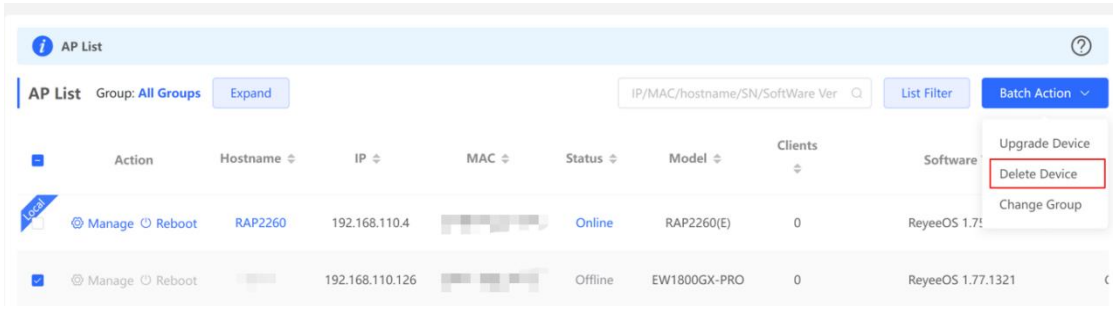
Upgrade device

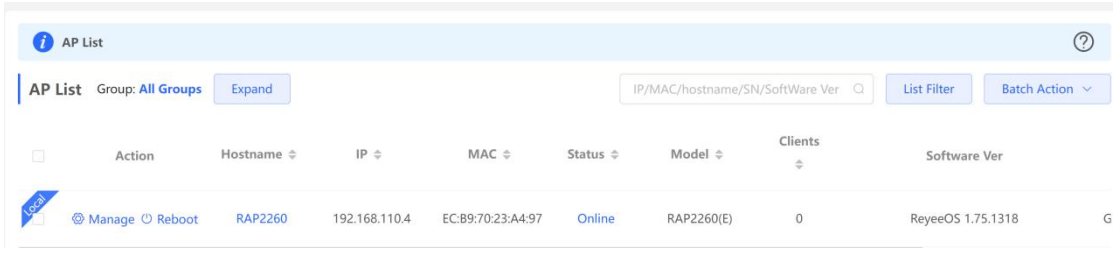






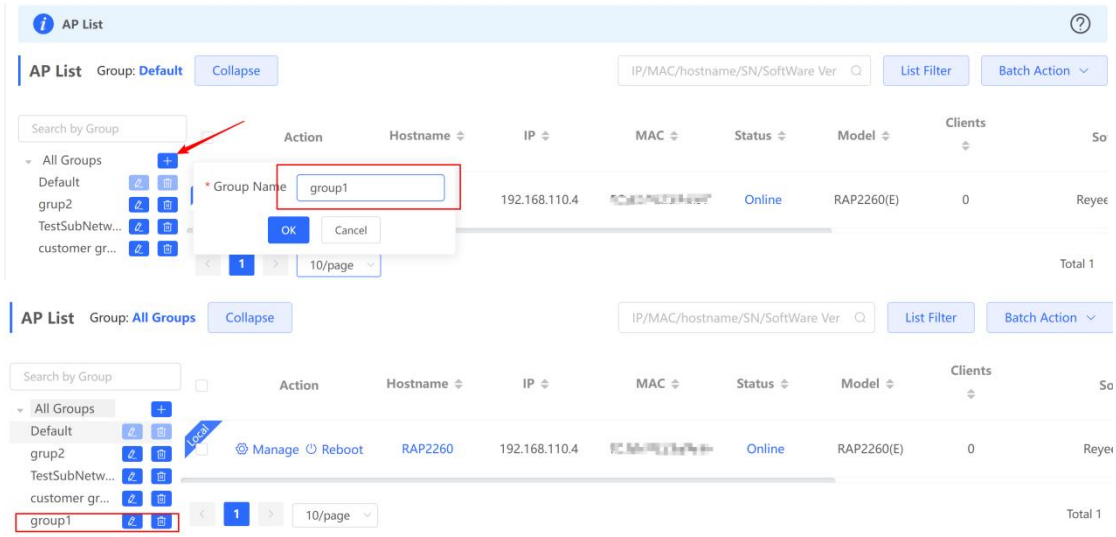
Delete device



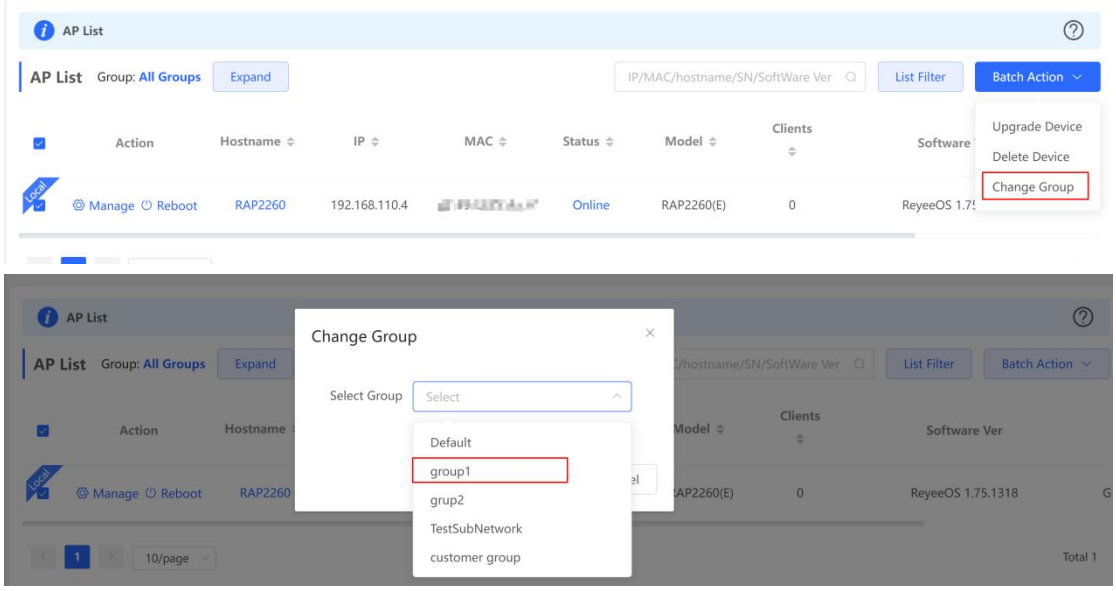


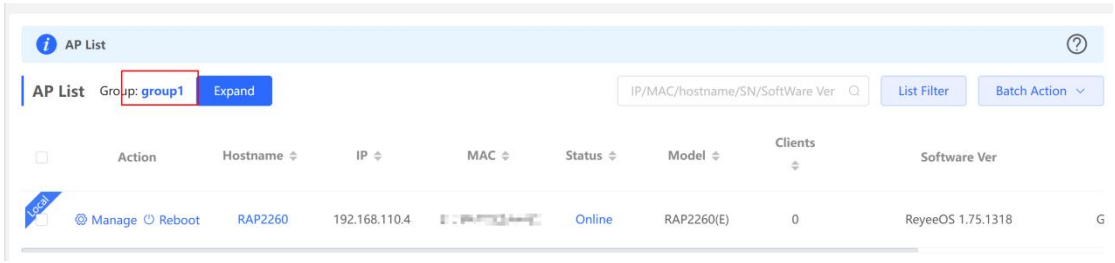
b) Add, Change, Delete AP group

Add group

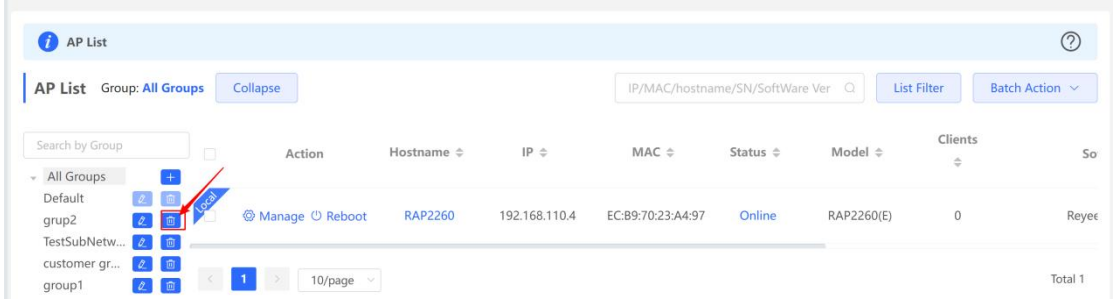


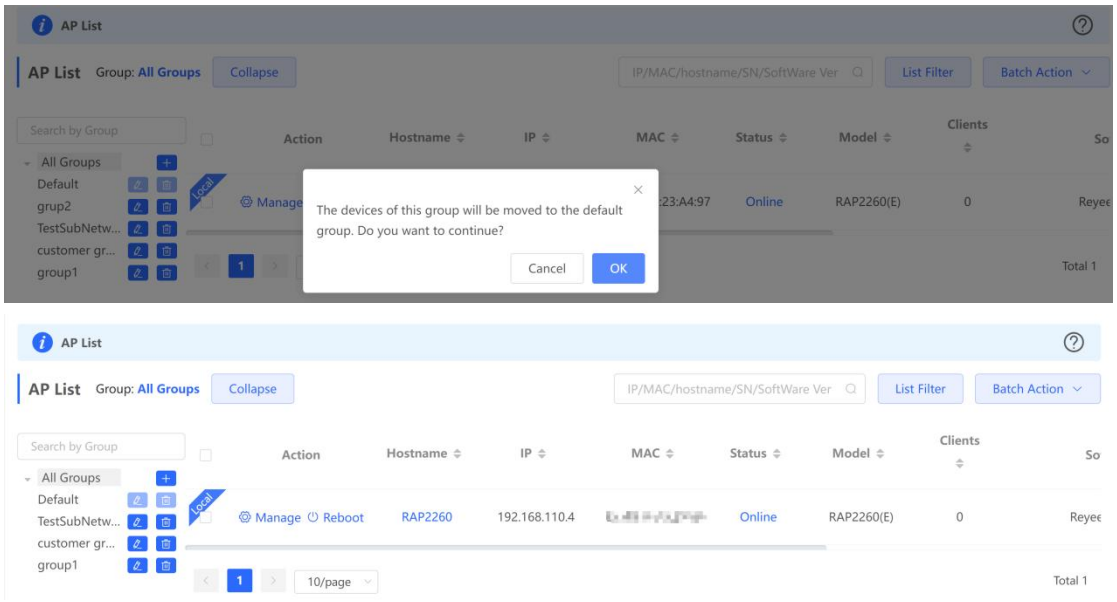
Change group





Delete group





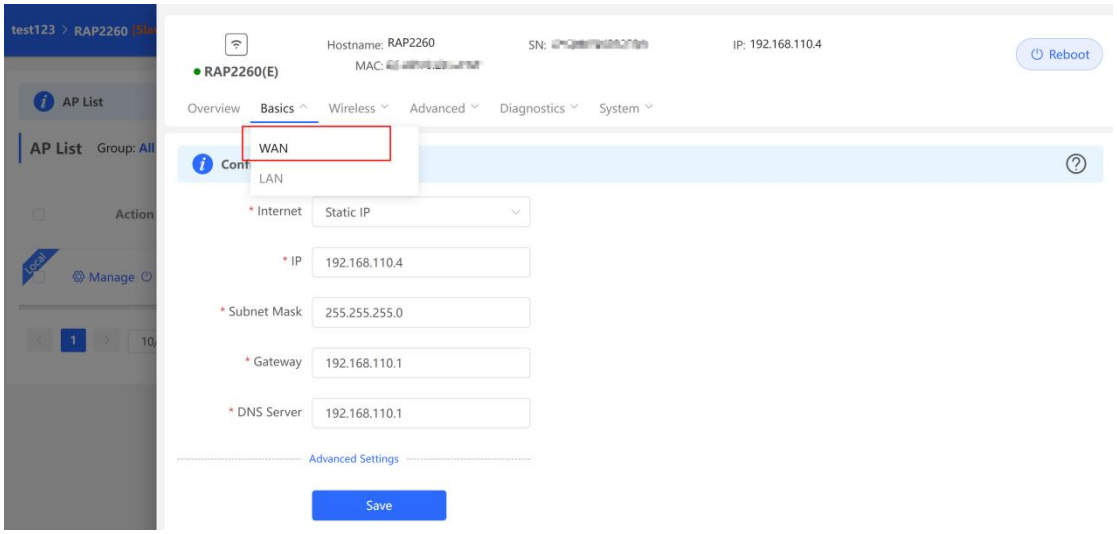
b) The local AP group configuration will synchronize to Ruijie Cloud.

When AP group was changed locally, it will be automatically synchronize the sub-group in the cloud:

4.4.2 Basic Configuration

4.4.2.1 WAN Port Configuration

Click **Basics—WAN** to configure WAN port setting.

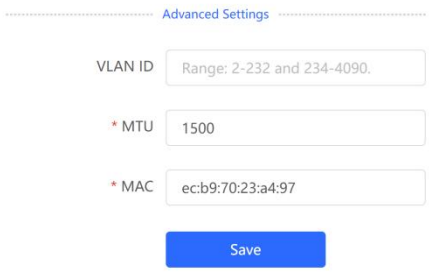


PPPoE: Access the internet by using the broadband account provided by ISP.

DHCP: Access the internet by using the dynamic IP address provided by ISP.

Static IP Address: Access the internet by using a static IP address provided by ISP.

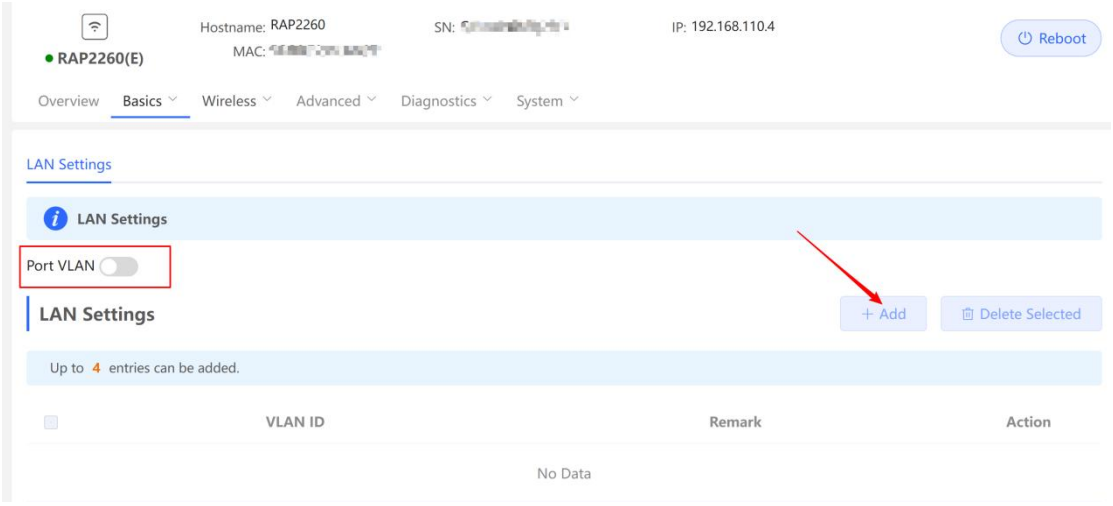
IP Address/Subnet Mask/Gateway/DNS Server: Those settings are required for static IP address.

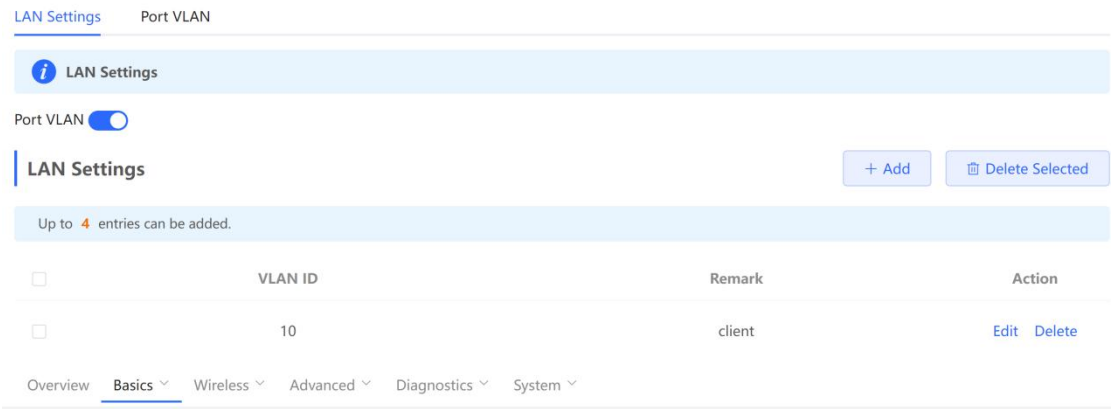


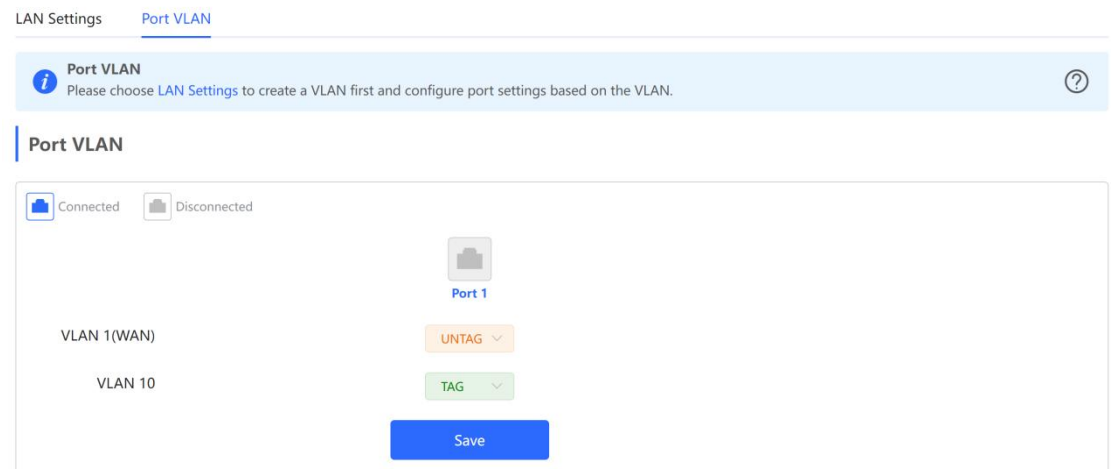
VLAN ID, MTU, MAC: you can customize those configurations as needed

4.4.2.2 LAN Port Configuration

a) Port VLAN Settings

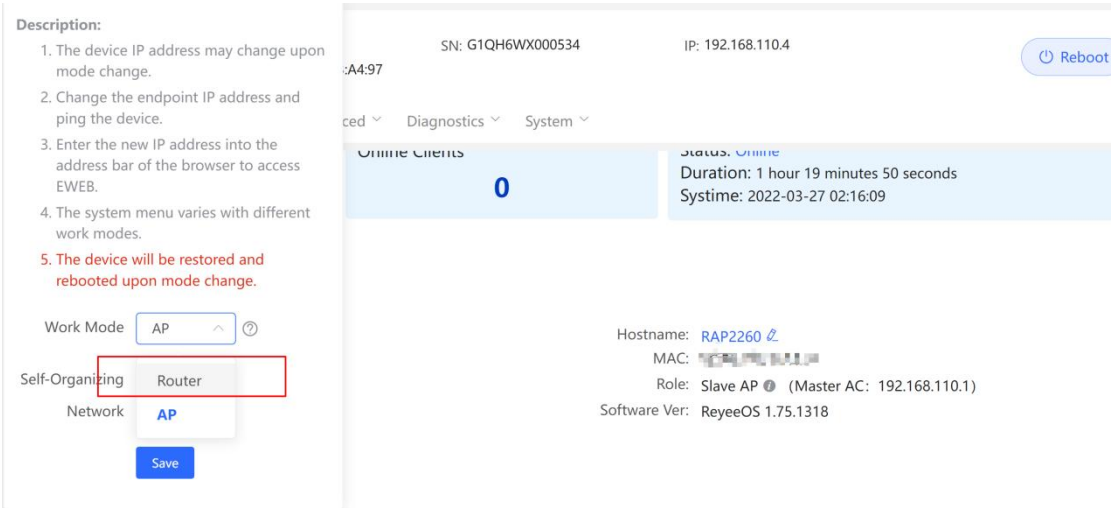






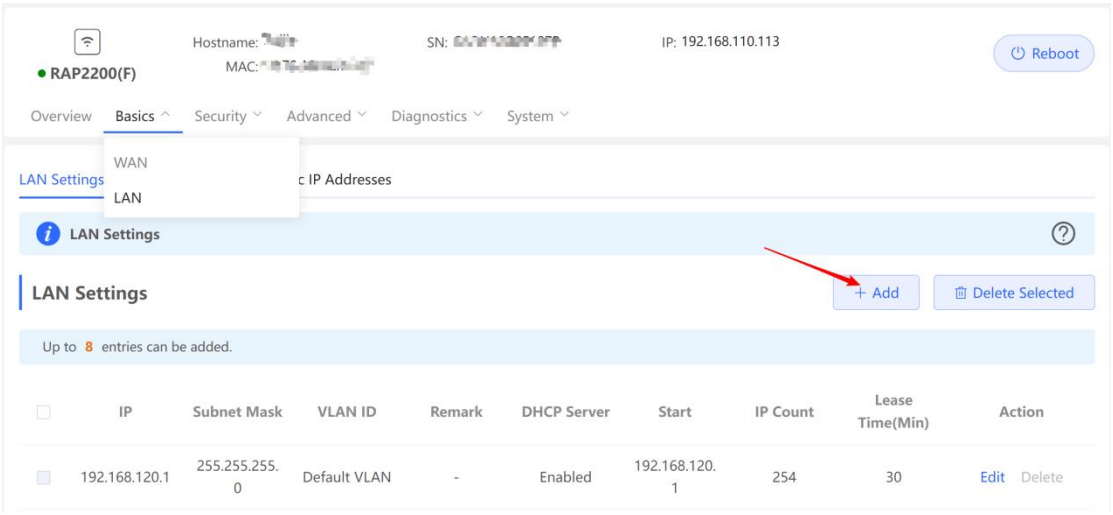
b) DHCP Configuration (only be visible in router mode)

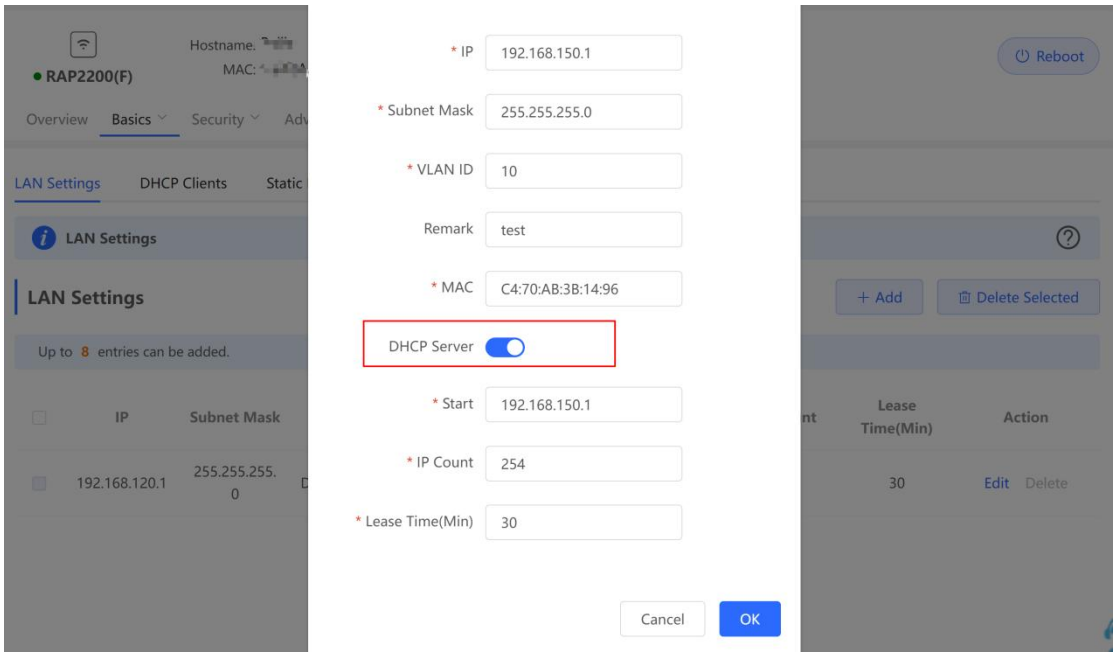
Change the AP's mode to Router mode



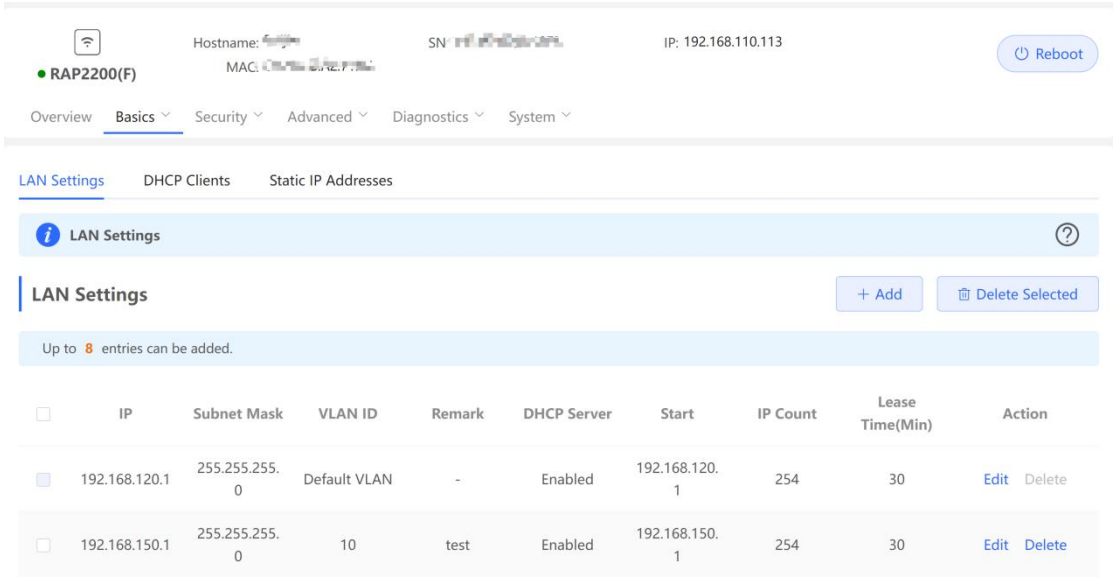
Click **basics—LAN** to config DHCP Pool

The default VLAN 1 can't be removed and its default IP address is 192.168.120.0/24.

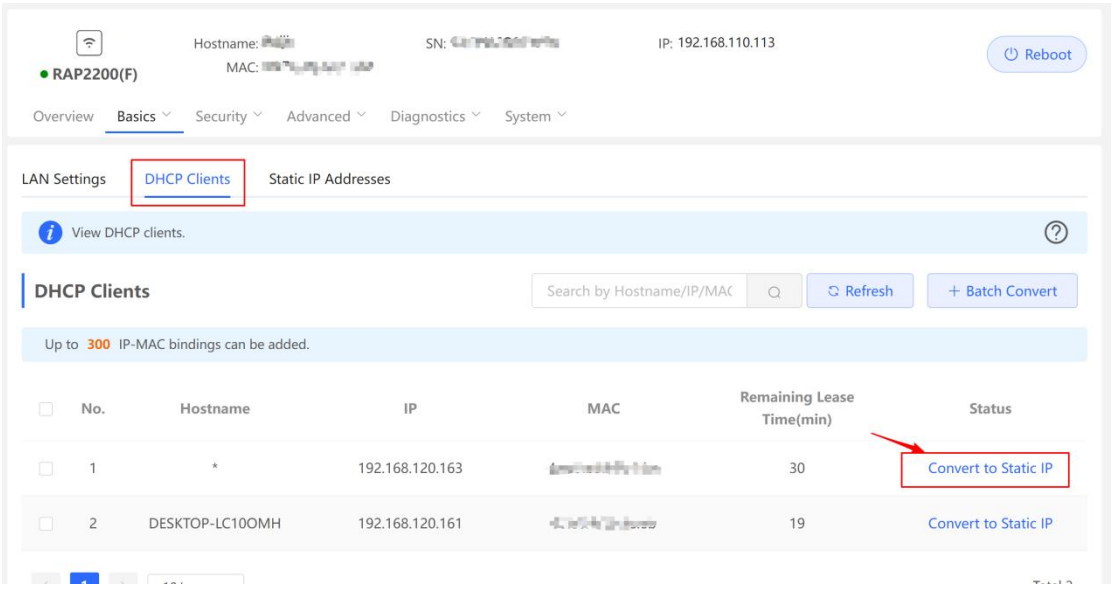




View configuration

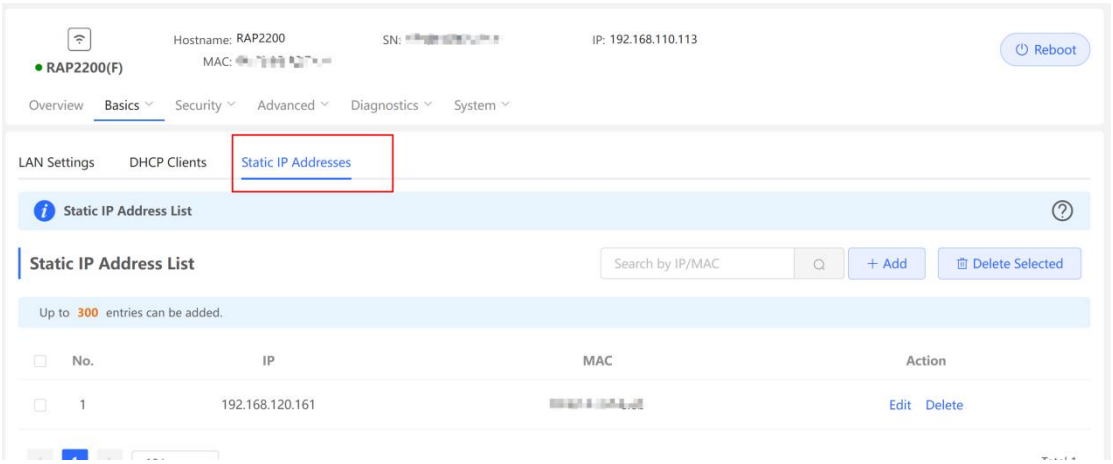


View DHCP Clients



c) Binding Static IP

Click **Convert to static IP**



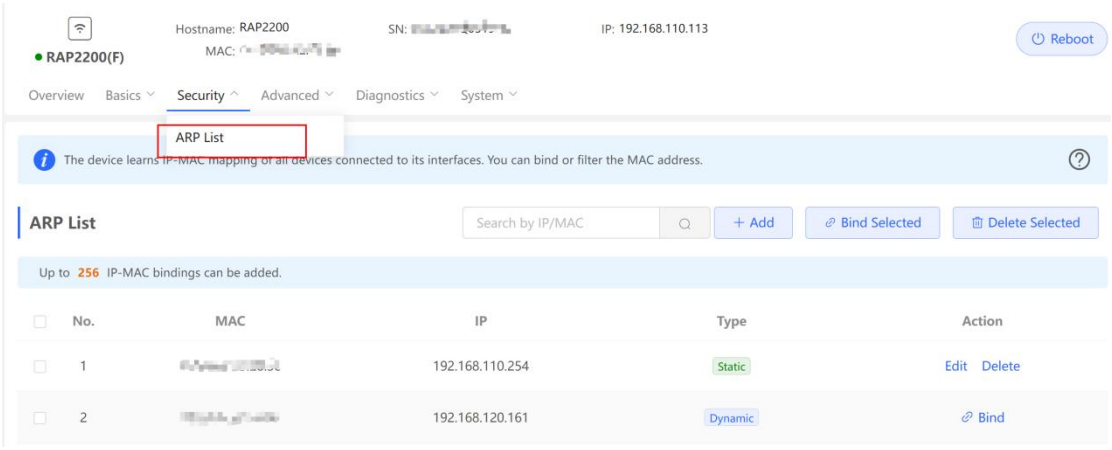
Click **Edit** to modify IP address and MAC address

4.4.3 Advanced Configuration

4.4.3.1 ARP List

Click **Security—ARP** List to view ARP list which is the mapping relationship between IP address and MAC address.

The AP can learn all connected devices' ARP. You can bind the MAC address and IP address by clicking **Bind**.



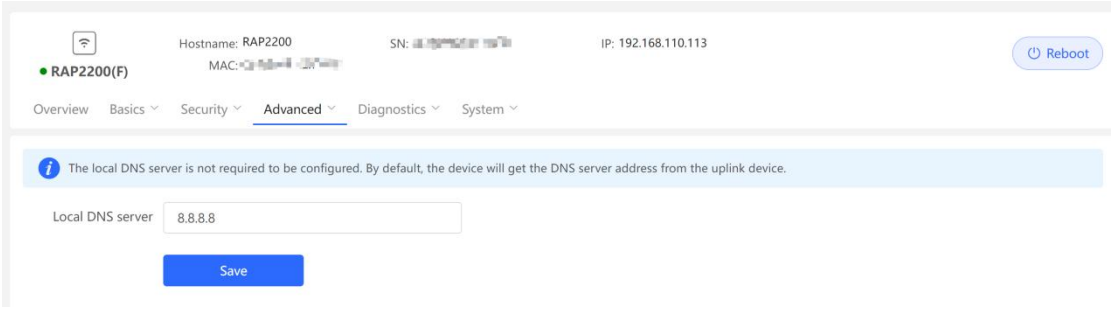
Bind Selected: Batch to bind the selected ARPs to convert them from dynamic to static.

Delete Selected: delete the selected ARP entry

Click **Add** can add static ARP.

4.4.3.2 Local DNS

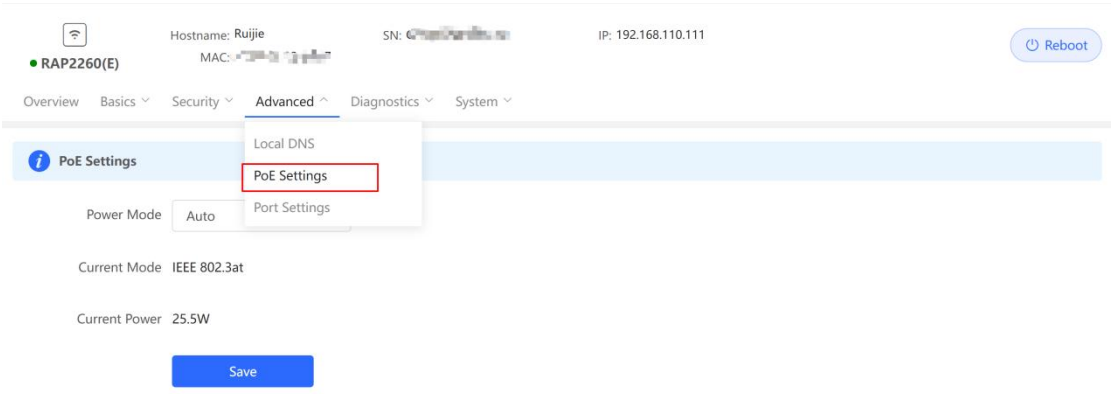
You can click **Advanced->Local DNS** to configure local DNS server, but the local DNS server normally no need to be configured. Since it will get the DNS address from the uplink DHCP Sever.

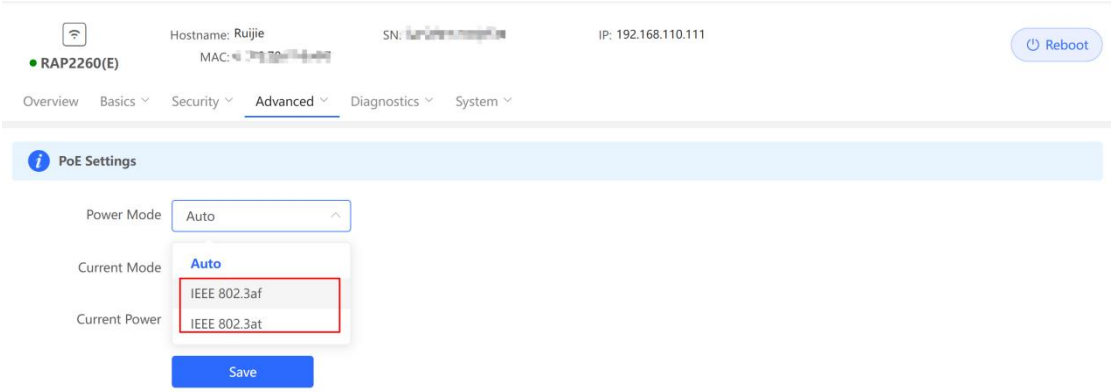


4.4.3.3 POE Configuration (Only support with RAP2260(E))

The PoE Settings module allows you to configure the PoE mode.

Click **advanced—PoE Settings**





Power Mode: IEEE 802.3at, IEEE 802.3af or Auto

Current Mode: Display current PoE mode

Current Power: Display current Power consumption.

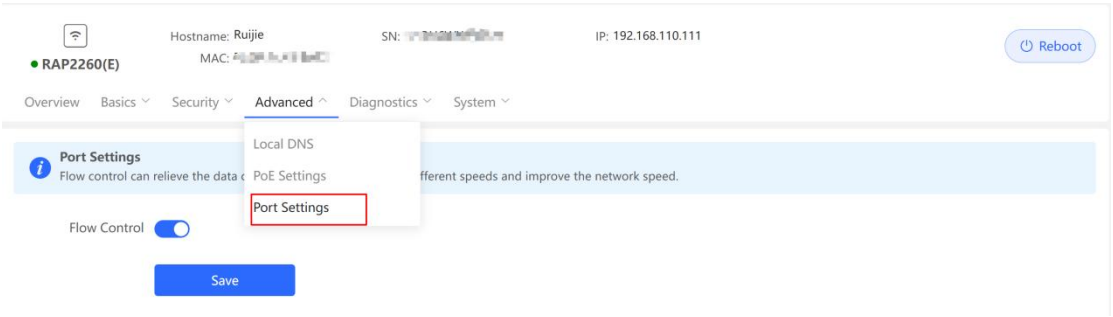
Note:

Only Wi-Fi6 products support POE In function **(**RG-RAP2260(G), RG-RAP2260(E), RG-RAP6260(G) **)**

4.4.3.4 Port Flow Control Configuration

Click **advanced—Port settings**

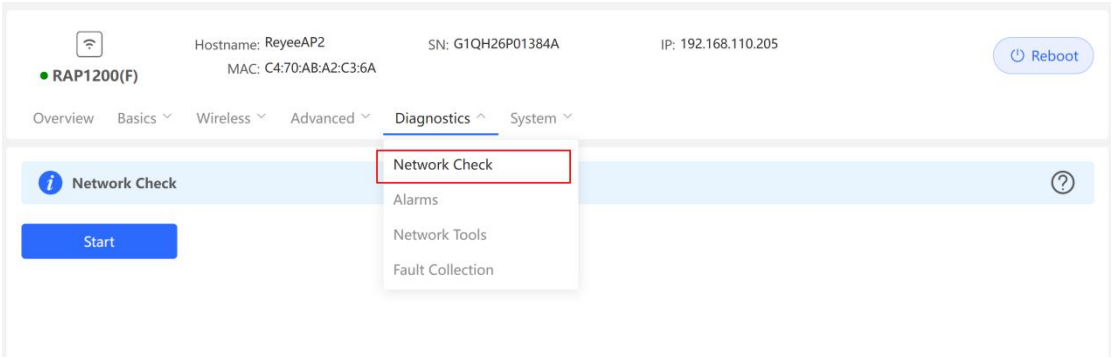
Flow control can relieve the data congestion caused by ports at different speeds and improve the network speed.

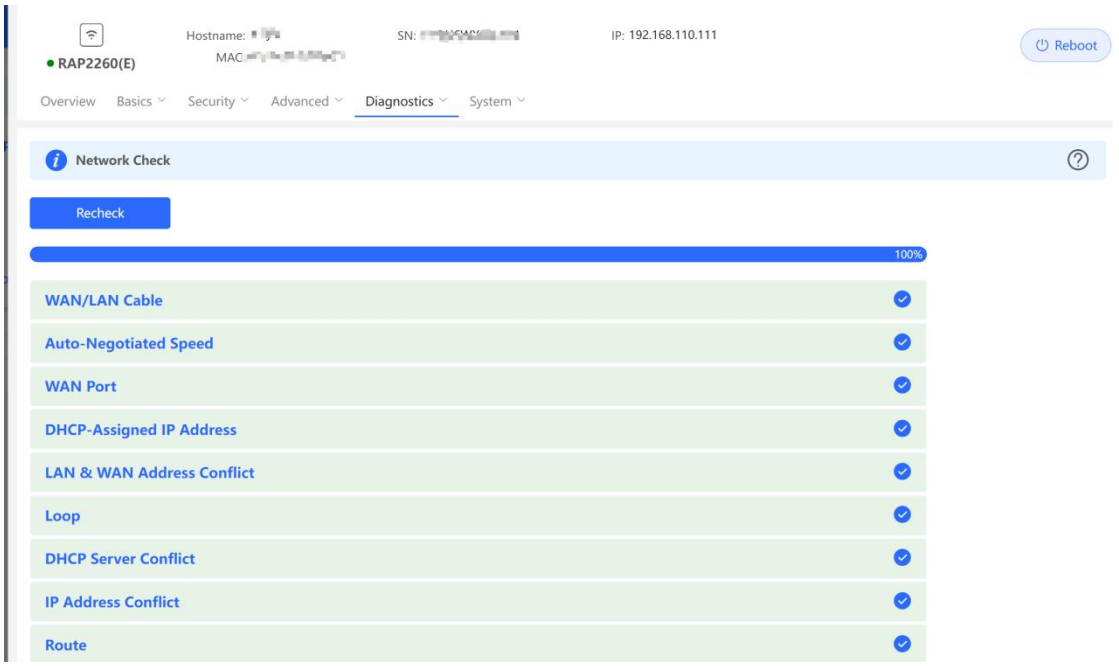


4.4.4 Operation and Maintenance

4.4.4.1 Network Check

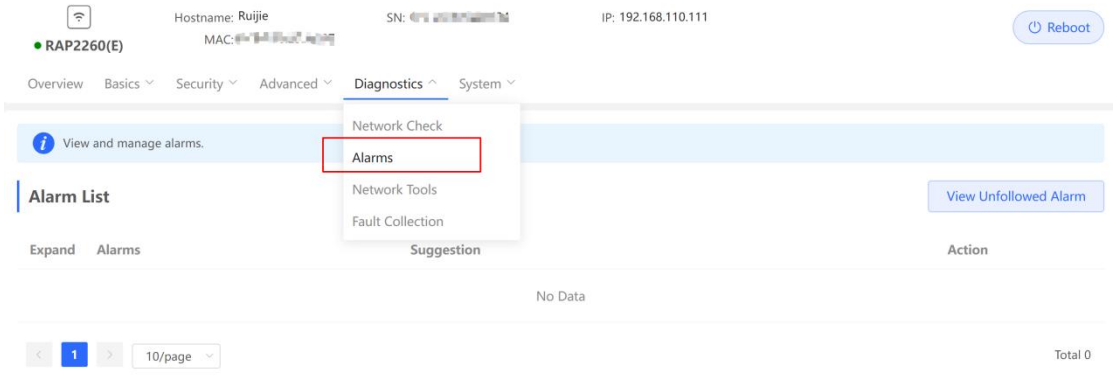
Click **Start->OK**, it will start the network check, then show the result in one minute.



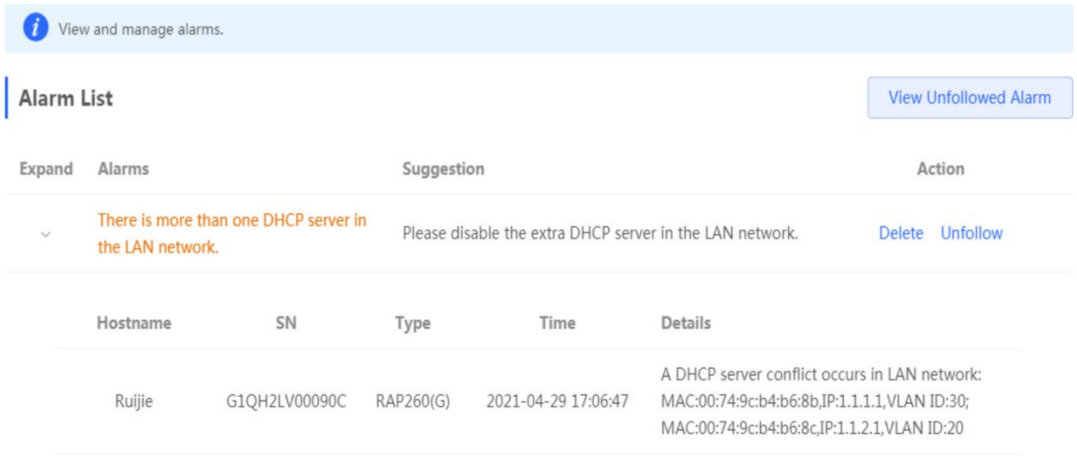


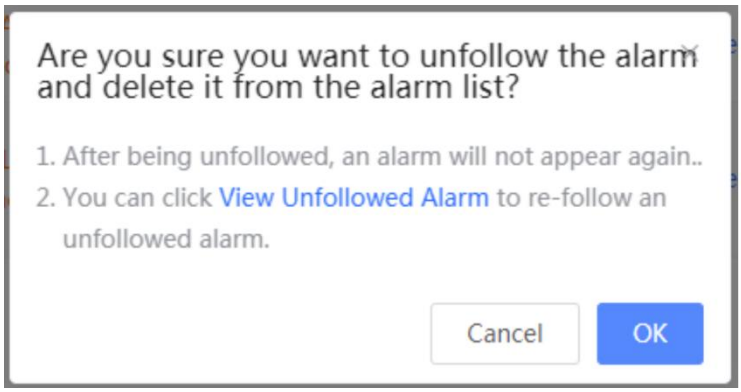
4.4.4.2 Alarms

You can view and manage the Alarms here.



Click **Unfollow** to un-follow an alarm.





Click View Unfollowed Alarm, then you can view and follow the alarm again.

Note:

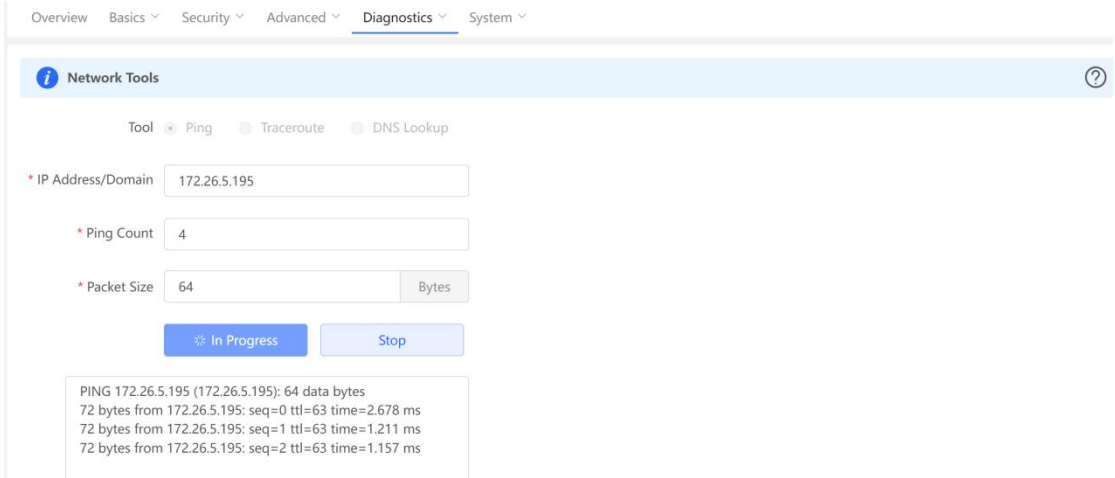
After clicking **delete,** the alarm will reappear when the warning occurs. And after clicking Unfollow, the alarm will never appear

4.4.4.3 Network Tools

The Network Tools including: Ping, Traceroute, and DNS Lookup.

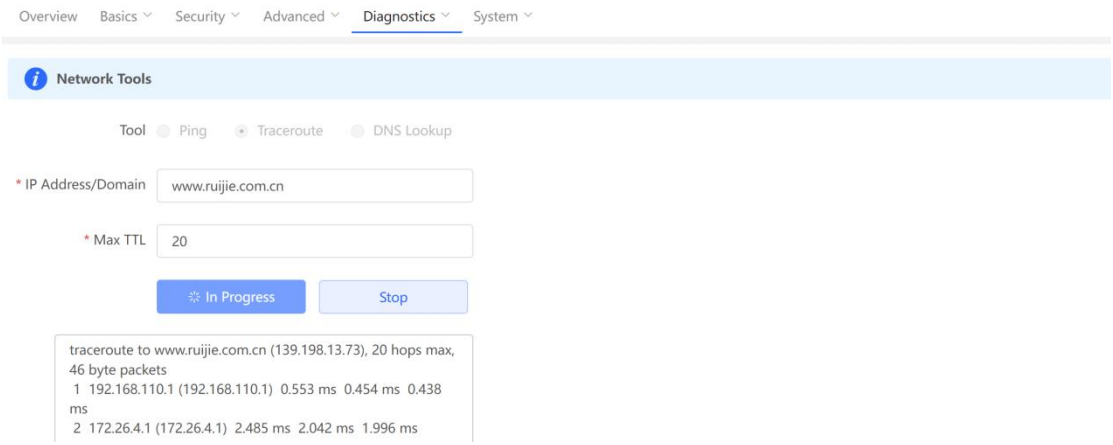
a) Ping tool

Test whether the IP/Domain is reachable.



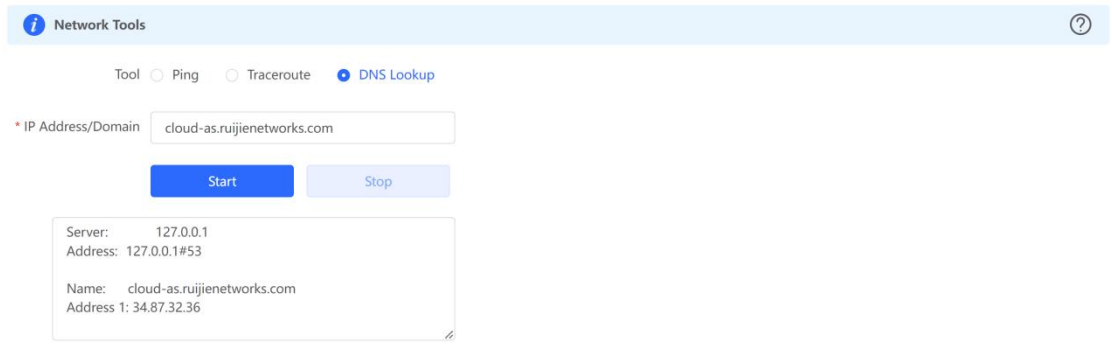
b) Traceroute

Traceroute tool can count the number of hops, showing communication links from one point to another point and the time it takes for each hops.



c) DNS Lookup

Resolve a domain to an IP address.



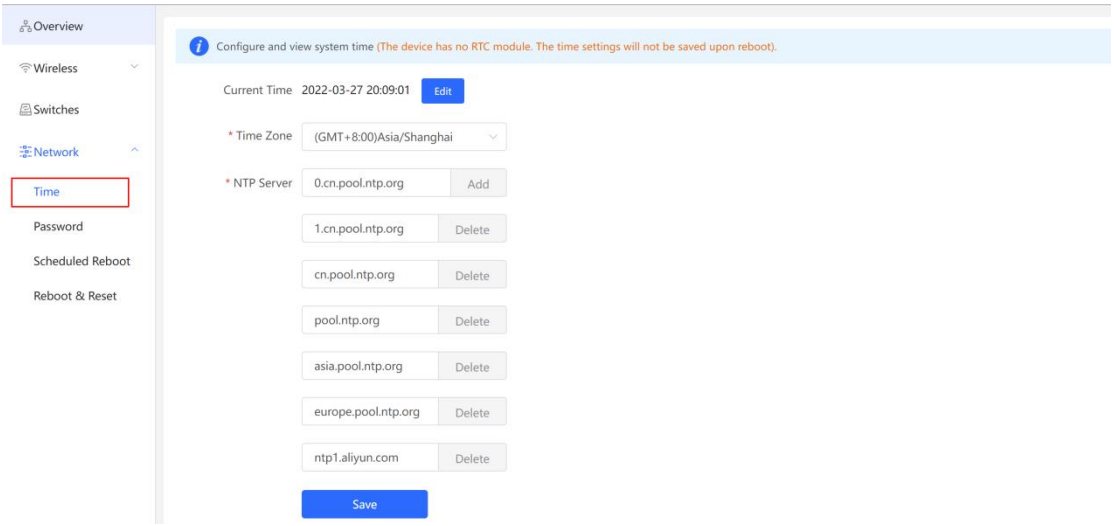
4.4.4.4 Fault Collection

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

4.4.4.5 System

1 Setting system time

Click **Network—Time** to set system time



Current Time: If not set or synchronized with a time server, it will be start with the manufacture time.

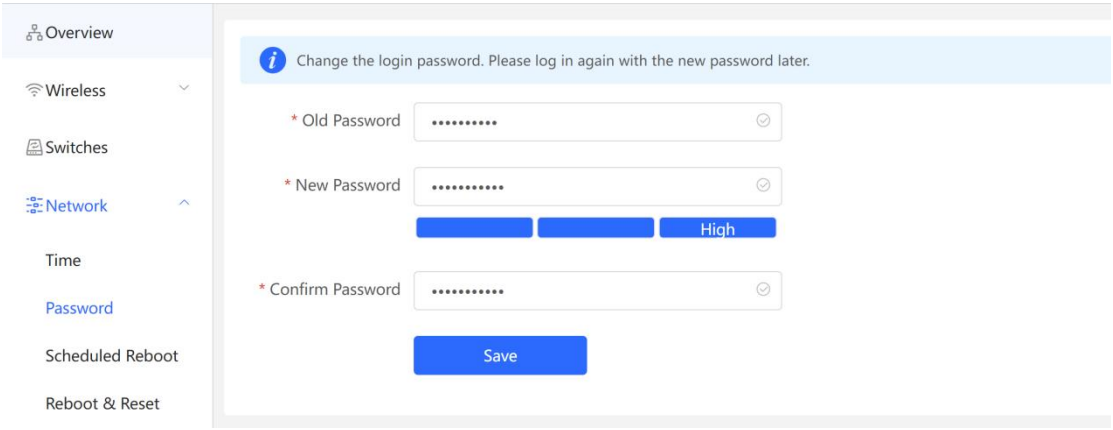
Time Zone: Choose the time zone based on your address.

NTP Server: You can click Add to add an NTP server.

2 Setting login Password

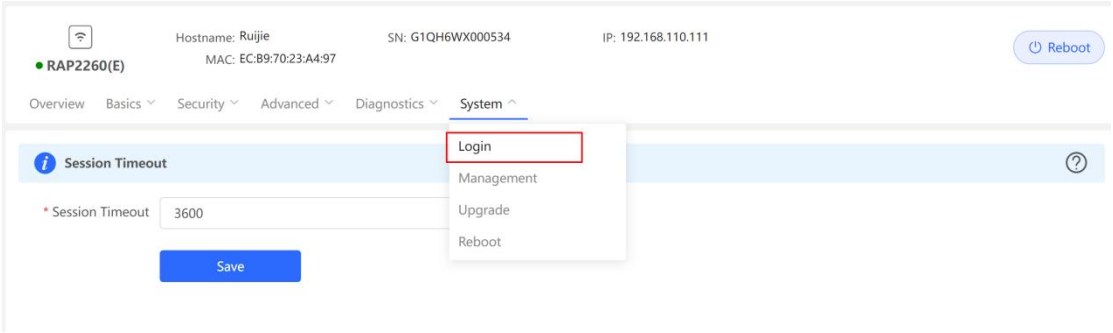
Click **Network—Password** to set login password.

Set a new password with at least 6 characters.



3 Setting Login Page Timeout

Click **System—Login** to set the login page timeout time. This can be set from 600 to 7200 seconds.



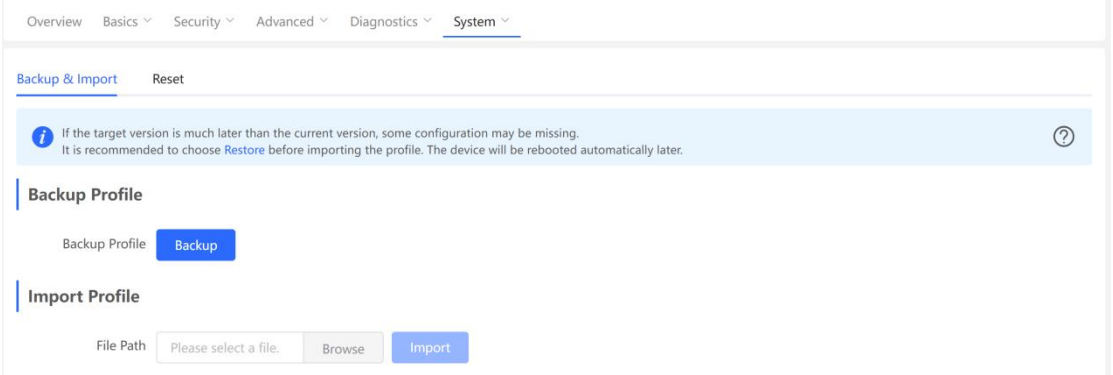
4 Backup/Import Configuration

Click **System—management**

You can import a configuration file to AP or export the current configuration of AP here.

If the target version is much later than the current version, some configuration may be missing.

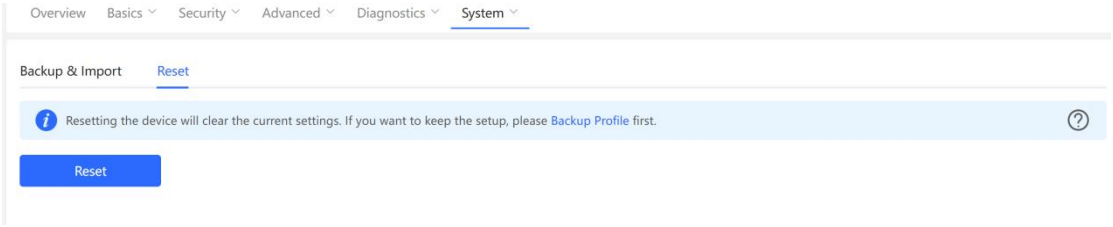
It is recommended to restore the settings first then importing the configuration. The device will reboot automatically if you restore it.



5 Reset

You can restore the device to factory settings on this page.

Click **Reset** to restore the device.

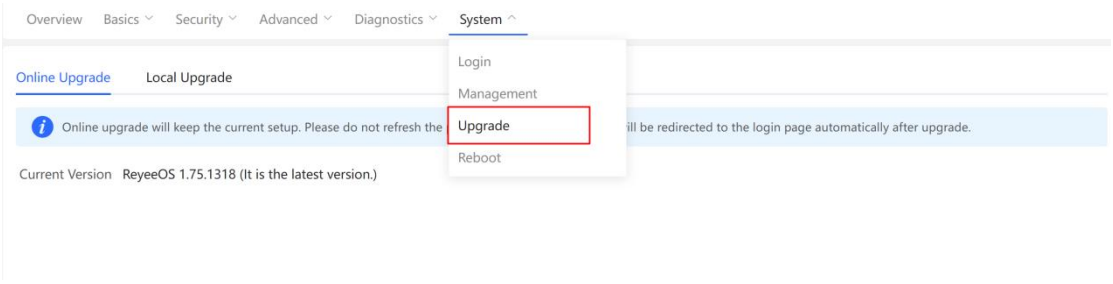


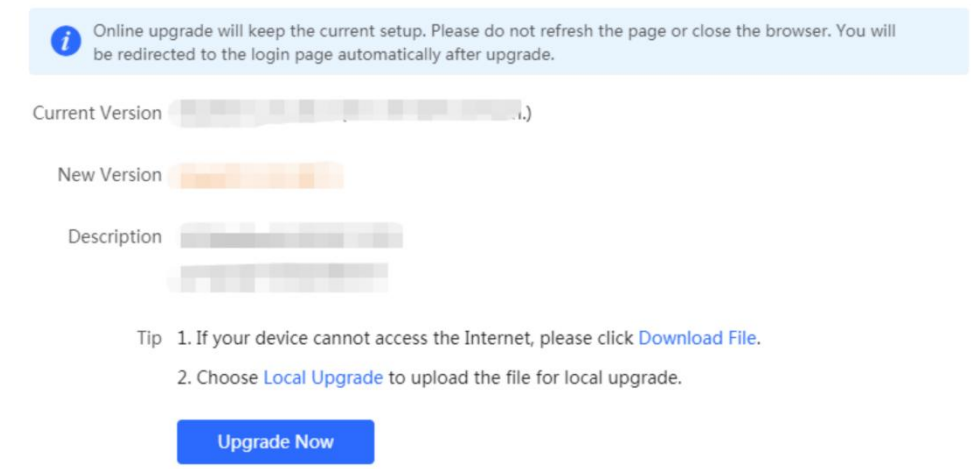
6 Upgrade

There are two modes to choose：Online Upgrade and Local Upgrade.

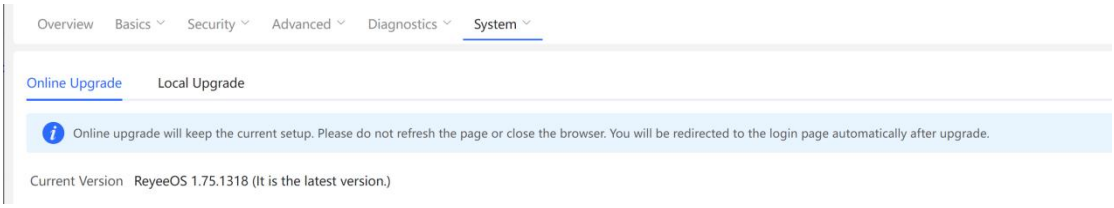
Online Upgrade

Click **Upgrade->Online Upgrade->Upgrade Now**, will download and upgrade to latest version. The upgrade operation won't affect the current configuration, but the AP will reboot after upgrading successfully. Please do not refresh the page or close the browser when do upgrading. It will be redirected to the login page automatically after upgrading.



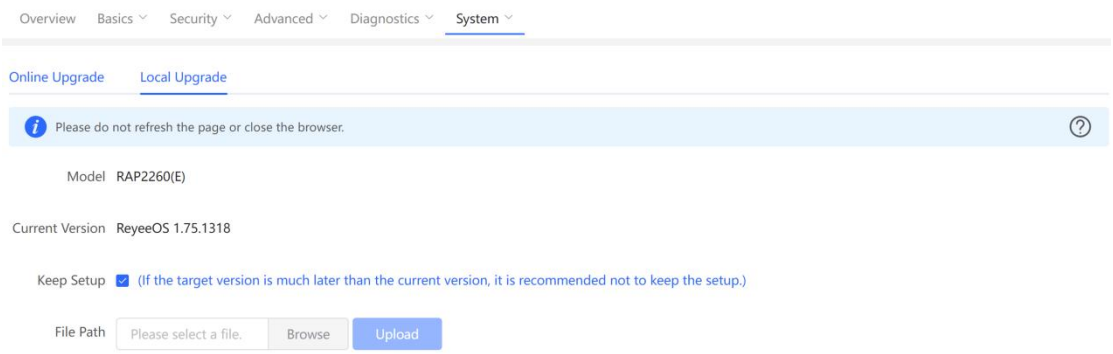


If there isn't new version, the device will pop-up a massage that the current version is the latest.



Local Upgrade

Click **Browse** to select an upgrade package, click **Upload**. After uploading successfully, it will display the upgrade package information and pop-up a prompt asking for upgrading. Click OK to start the upgrade.



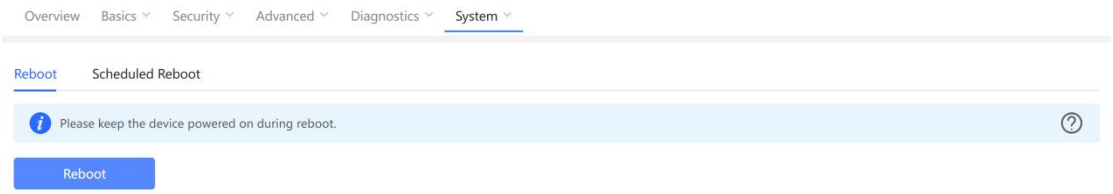
Keep Setup: If the target version is much later than the current version, it is recommended not to keep the configuration.

7 Reboot the device/Schedule Reboot

click **System—.>Reboot**

a) Reboot

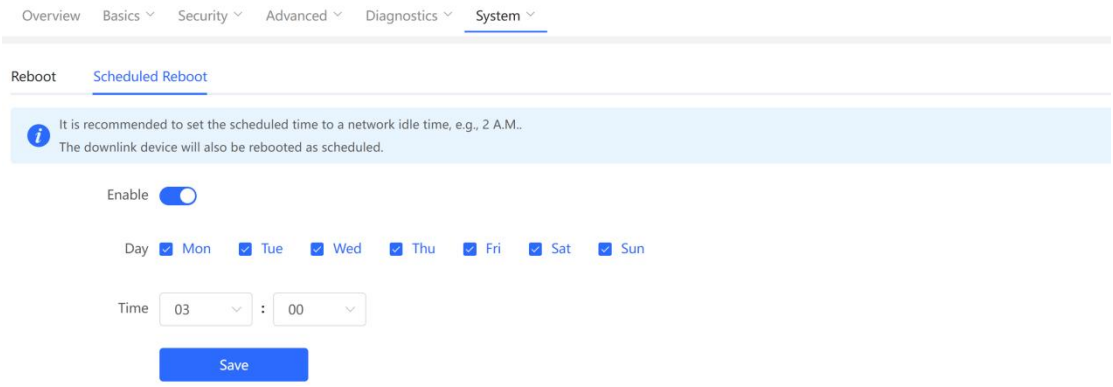
The Reboot module allows you to reboot the device immediately.



Click **Reboot**, and click **OK** in the confirmation box. The device is rebooted and you need to log into the Eweb management system again after the reboot. Do not refresh the page or close the browser during the reboot.

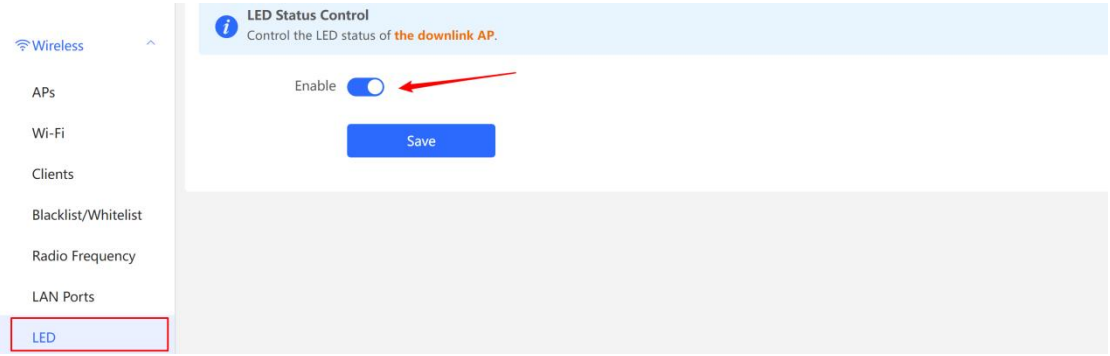
After the device is successfully rebooting, you will be redirected to the login page of the eWEB management system.

b) Schedule Reboot



8 AP LED

You can turn on/off the AP's LED indicator here.



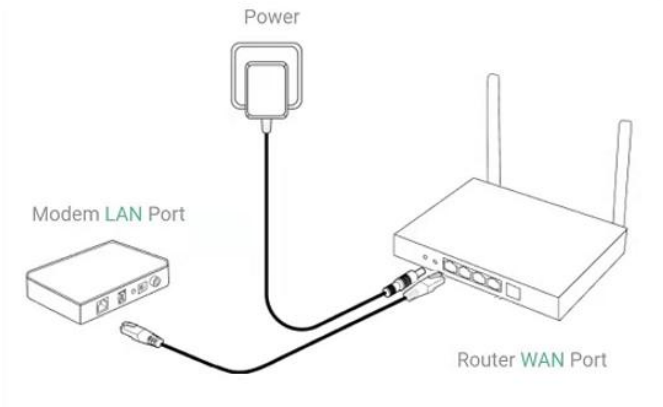
4.5 Reyee Mesh Wi-Fi Configuration

4.5.1 Network Setting

4.5.1.1 Quick start

Wired connect

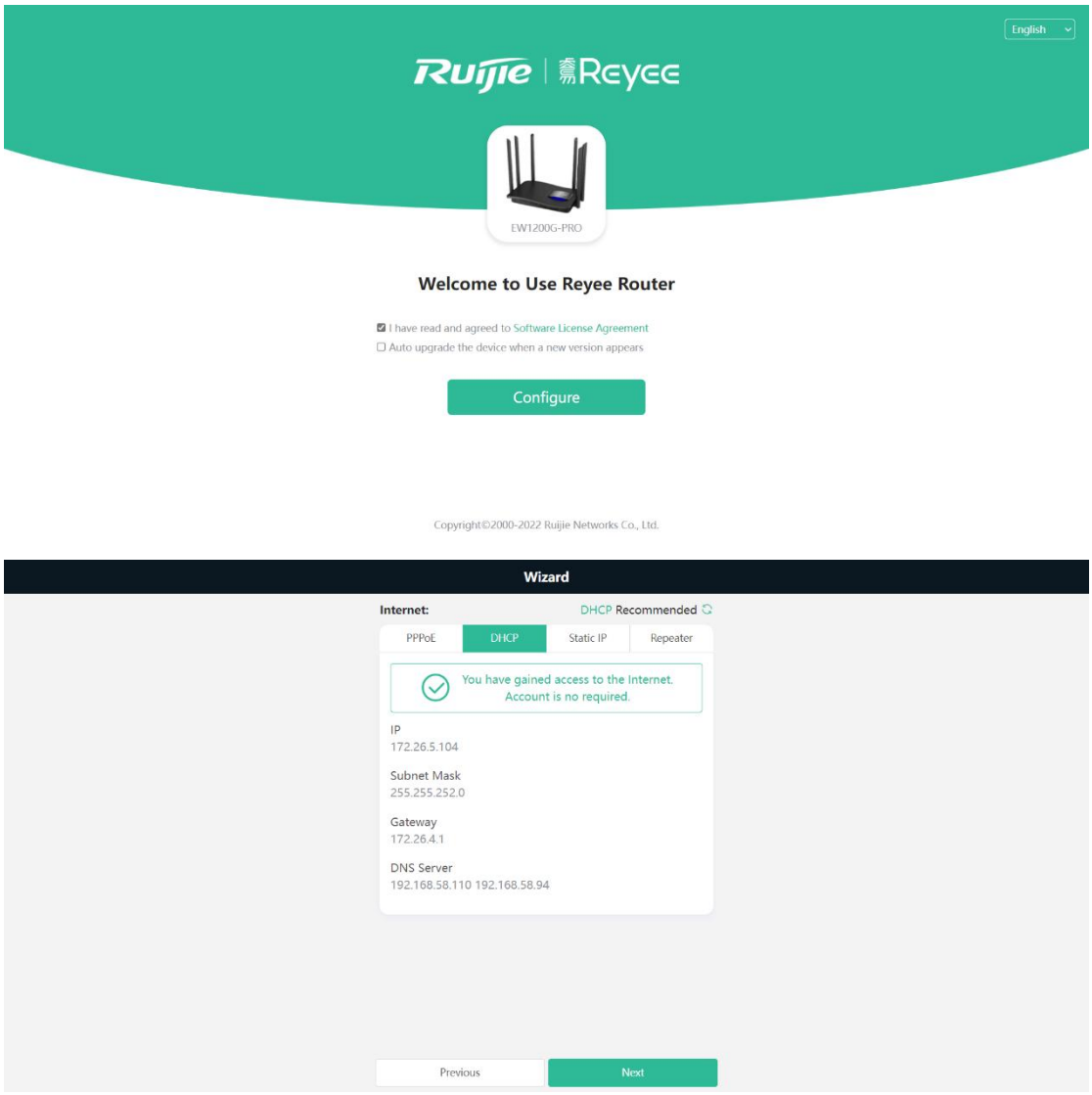
You need to connect the router to a power supply and connect the LAN port of a modem to the WAN port of the router. The port nearest to the Reset button on the router is the WAN port, and other network ports are LAN ports.



1. Configuring the Internet Connection Type

Configure the Internet connection type according to requirements of the local Internet Service Provider (ISP). Otherwise, the Internet access may fail due to the improper configuration. You are advised to contact your local ISP to confirm the Internet connection type:

- Figure out whether the Internet connection type is PPPoE, DHCP mode, or static IP address mode.
- In the PPPoE mode, username, password, and the service name are needed.
- In the static IP address mode, IP address, subnet mask, gateway, and DNS server are needed to configure.



2. Configuring a Wi-Fi Network

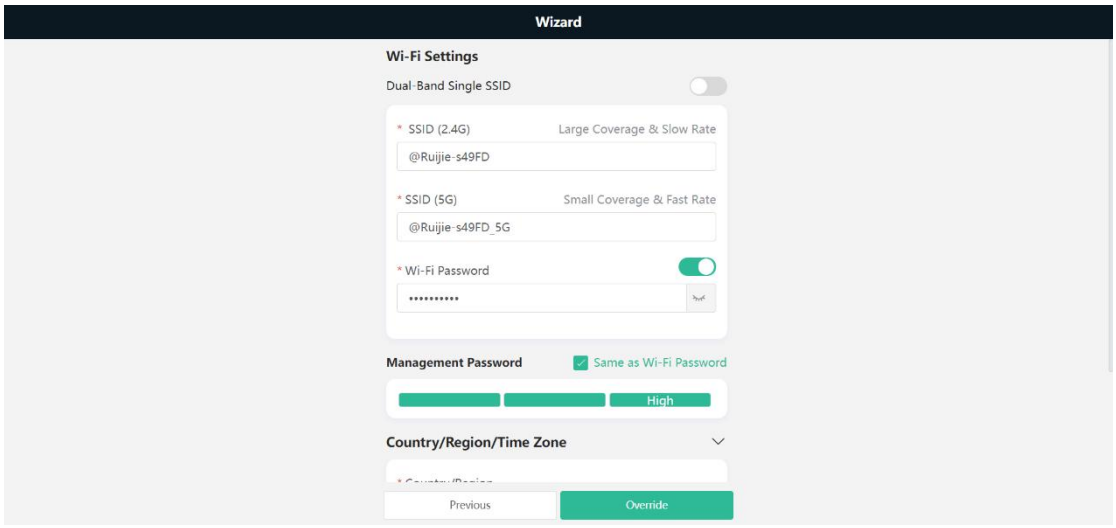
(1) Setting the SSID and Wi-Fi password: The device has no Wi-Fi password by default, indicating that the Wi-Fi network is an open network. You are advised to configure a complex password to enhance the network security. The password must be a string of 8 to 31 characters, which can contain uppercase and lowercase letters, digits, and English characters but cannot contain special characters such as single quotation marks ('), double quotation marks ('), or spaces.

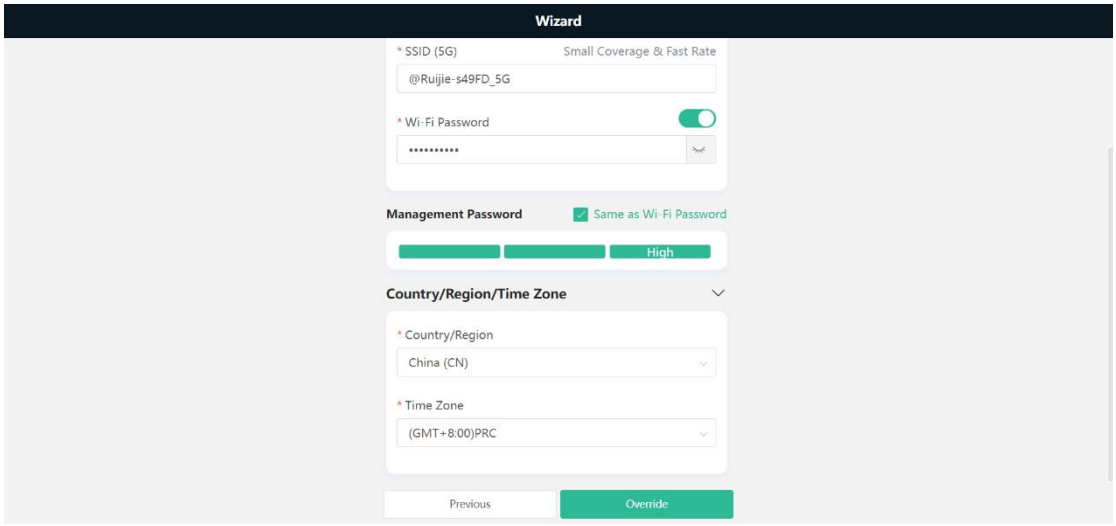
(2) Setting the management password: The password is used for logging in to the management page. The management password must be a string of 8 to 31 characters that contain at least three types among uppercase letters, lowercase letters, digits, and English characters but cannot contain **admin**, Chinese characters, spaces, or question marks (?). You can set the password s**ame as the Wi-Fi one**.

(3) Setting the country or region: The Wi-Fi channel may vary from country to country. To ensure that a client searches for a Wi-Fi network successfully, you are advised to select the actual country or region.

(4) Setting time: Set the system time. The network time server is enabled by default to provide the time service. You are advised to select the actual time zone.

(5) Overriding the configuration: Click **Override**. The Wi-Fi network will be restarted. You need to enter the new Wi-Fi password to connect to the new Wi-Fi network.





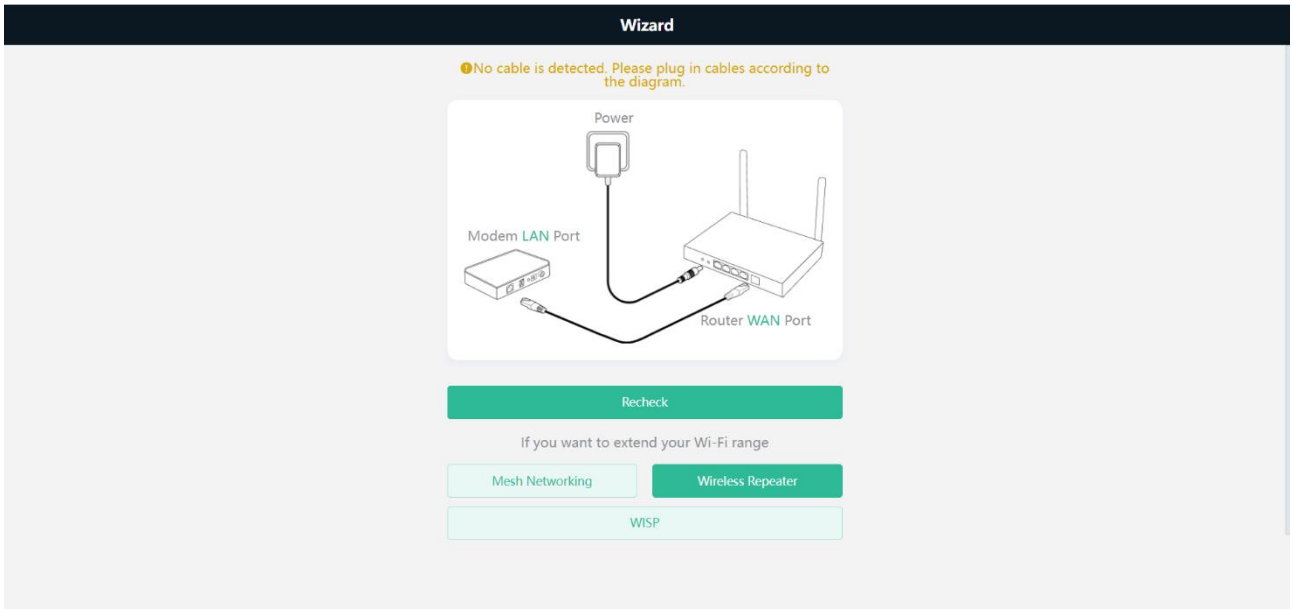
3. Verification and Testing

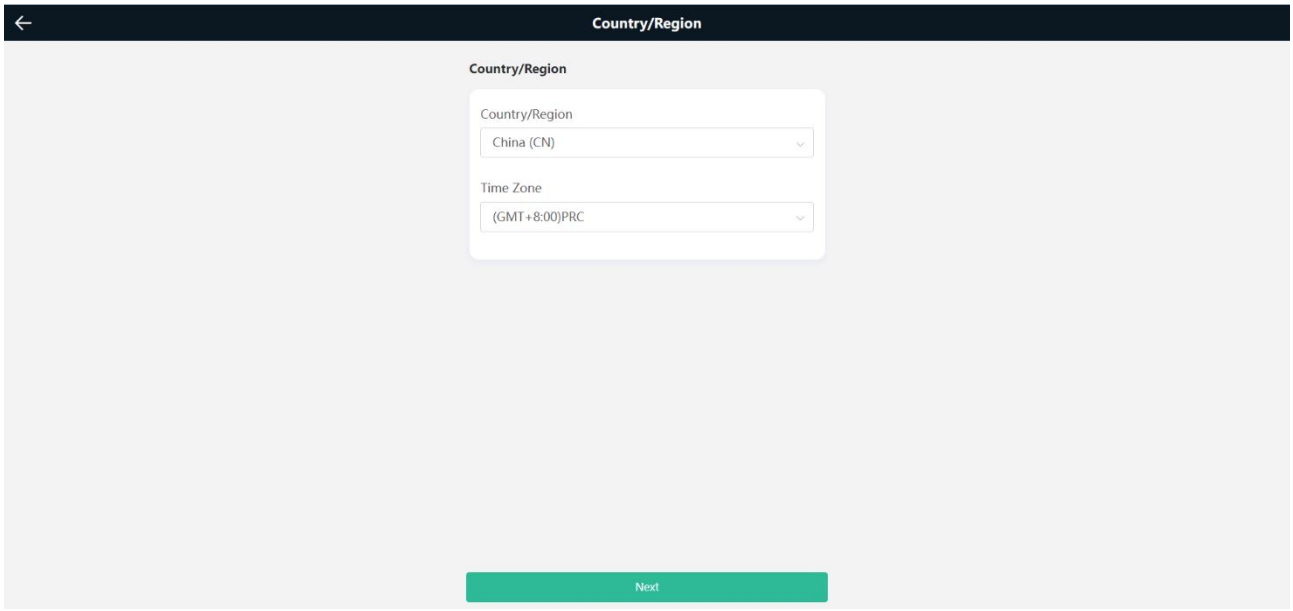
You can access the Internet after connecting to the Wi-Fi network. Log in the management page (the default address is 192.168.110.1) and, Internet connection status, real-time upstream and downstream traffic data will be displayed on the page.

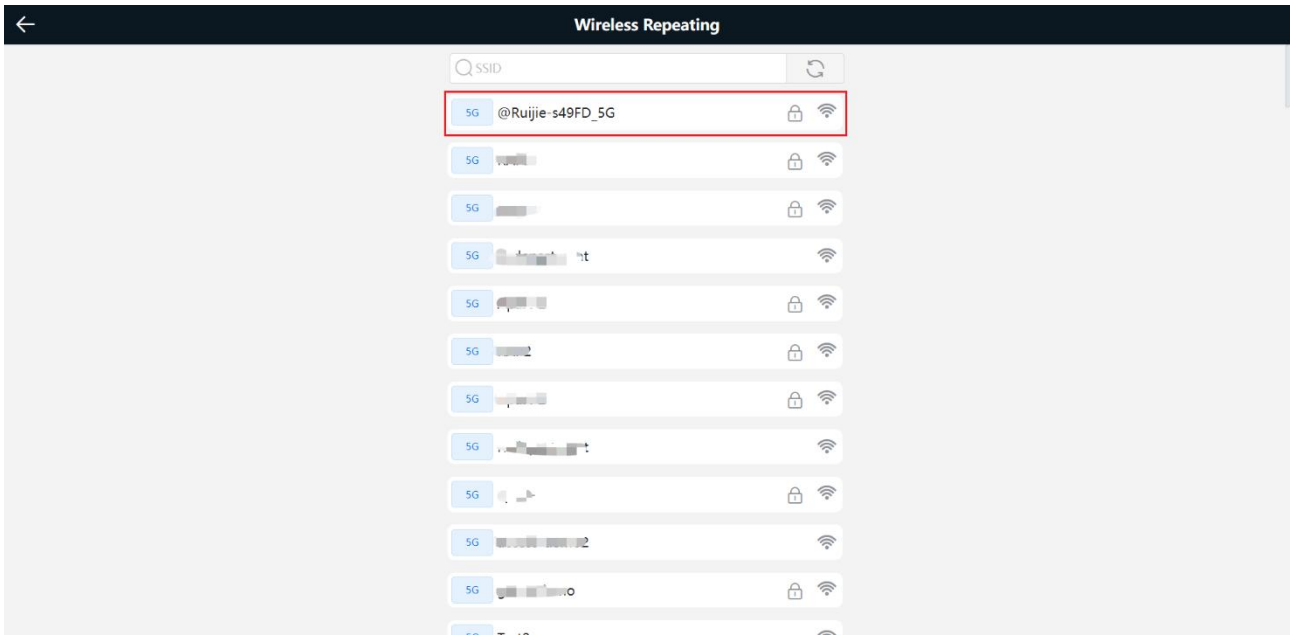
Wireless connect

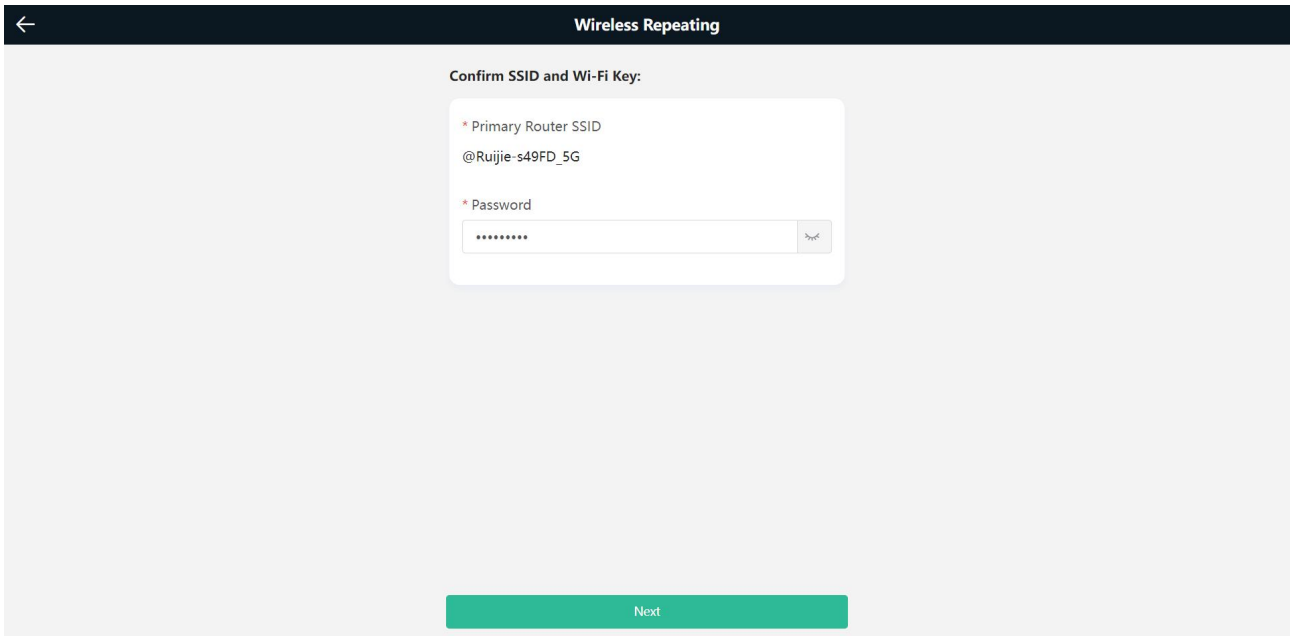
1. Wireless repeater mode

(1) Click Wireless **Repeater**, select the **Country/Region** and the **SSID** of the primary router, and enter the Wi-Fi password to connect to the primary router.

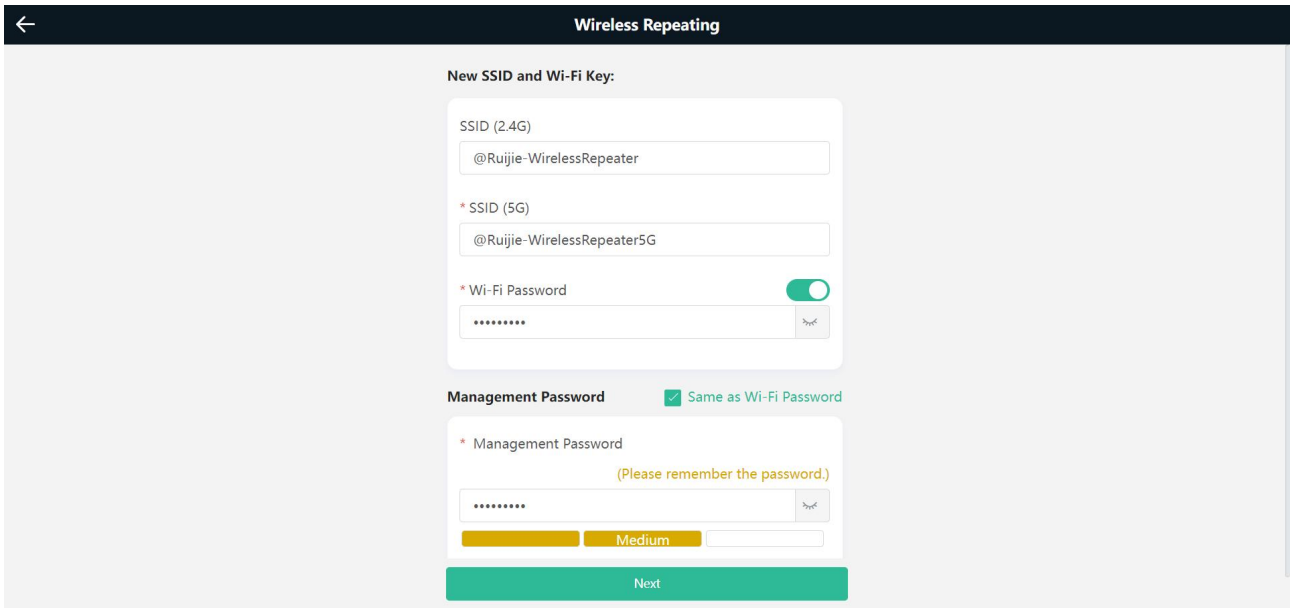

Wizard
No cable is detected. Please plug in cables according to the diagram.
Power
Modem LAN Port
Router WAN Port
Recheck
If you want to extend your Wi-Fi range
Mesh Networking
Wireless Repeater
WISP

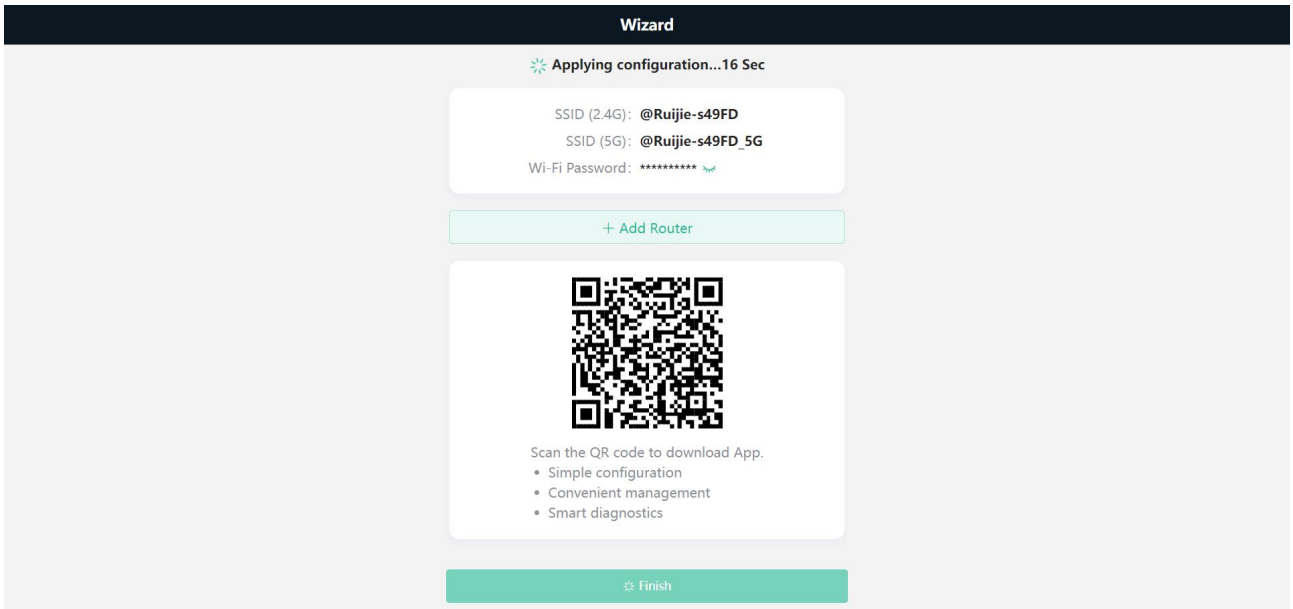

Country/Region
Country/Region
Country/Region
China (CN)
Time Zone
(GMT+8:00)PRC
Next

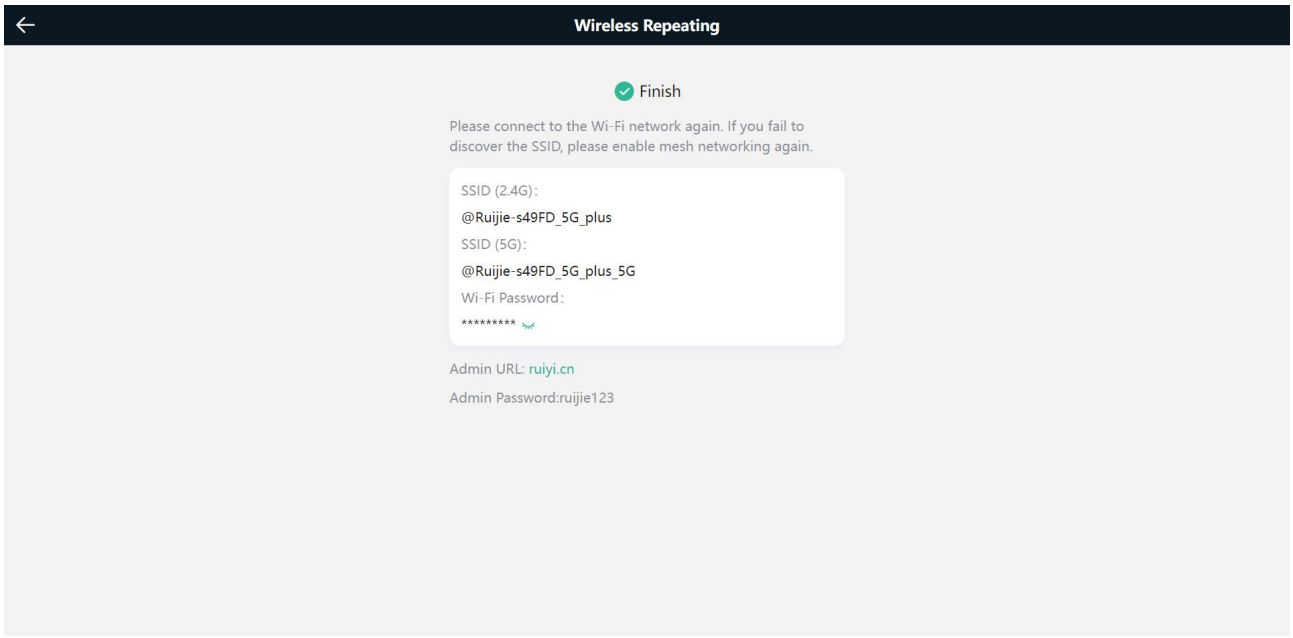




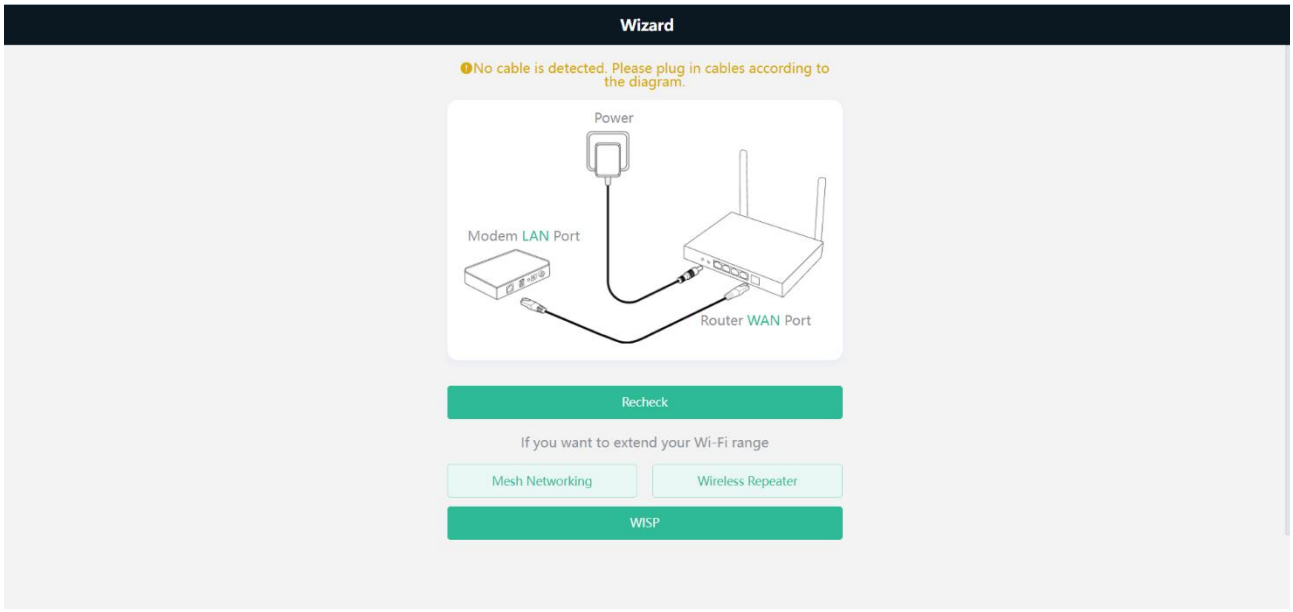
(2) Set the SSID and password and save the settings. Then, the Wi-Fi network will be restarted.


Wireless Repeating
New SSID and Wi-Fi Key:
SSID (2.4G)
@Ruijie-WirelessRepeater
* SSID (5G)
@Ruijie-WirelessRepeater5G
* Wi-Fi Password
Management Password
Same as Wi-Fi Password
* Management Password
(Please remember the password.)
Medium
Next


Wizard
Applying configuration...16 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



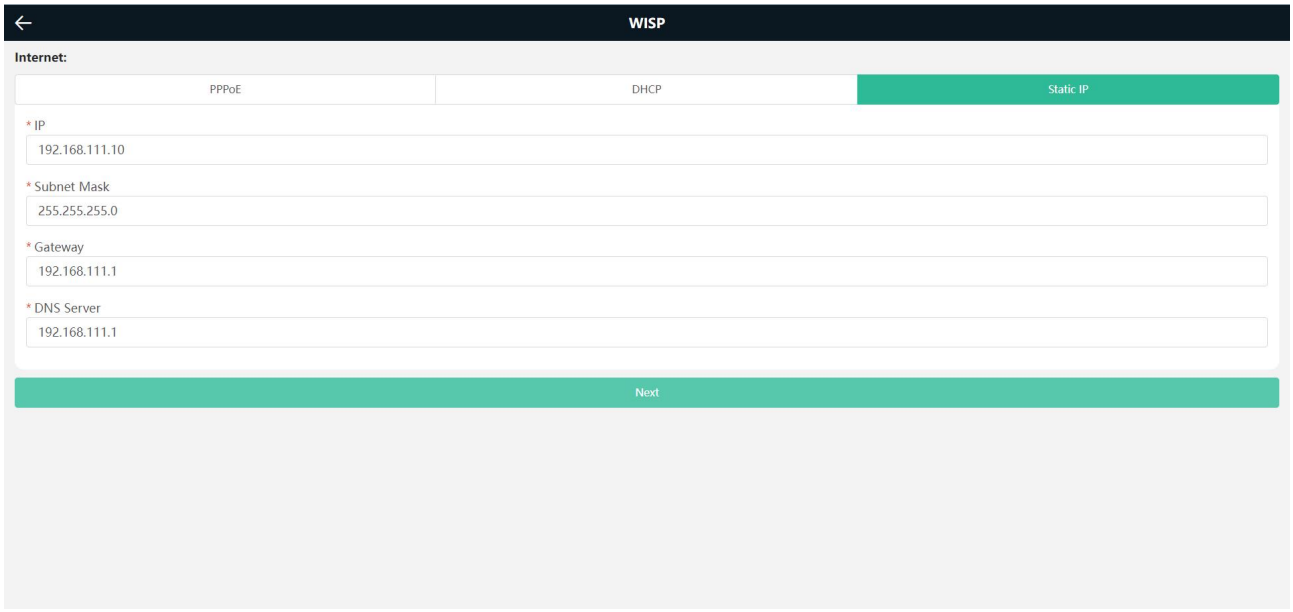
In the wireless repeater mode, only Wi-Fi signals are extended and the DHCP function is disabled. The IP addresses of all clients connected to the primary and secondary routers are assigned by the primary router. If the device connects to the primary router in wireless repeater mode, the WAN port of the device keeps unchanged. If WAN cable is plugged in, the device automatically switches to the wired repeater mode.

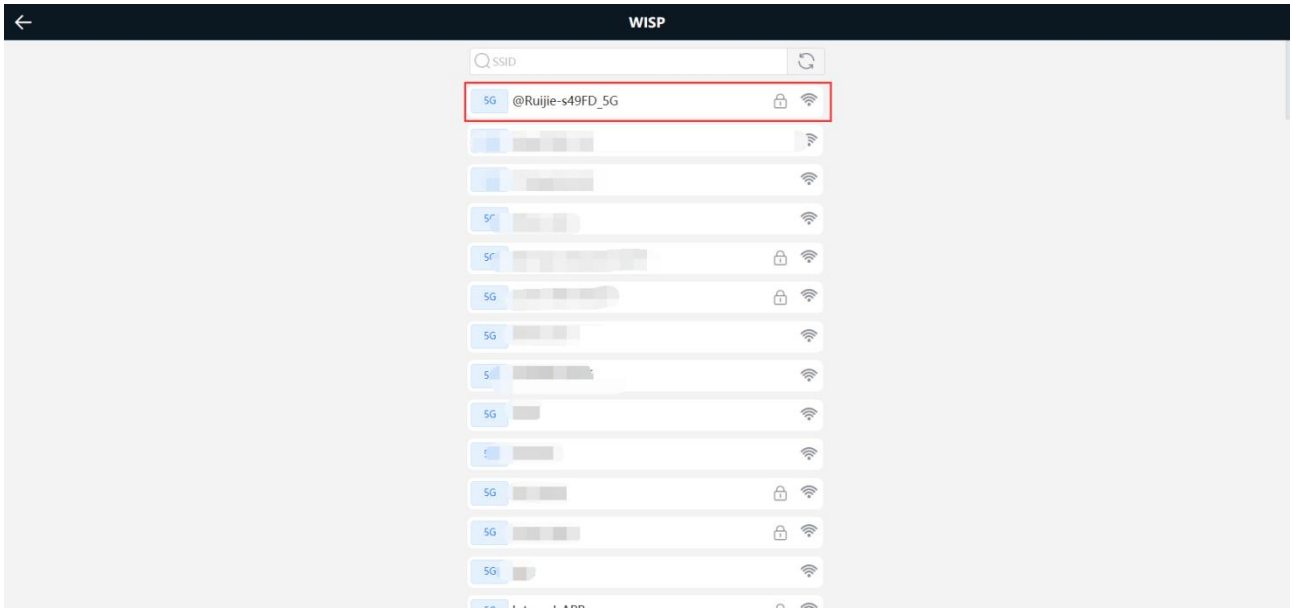


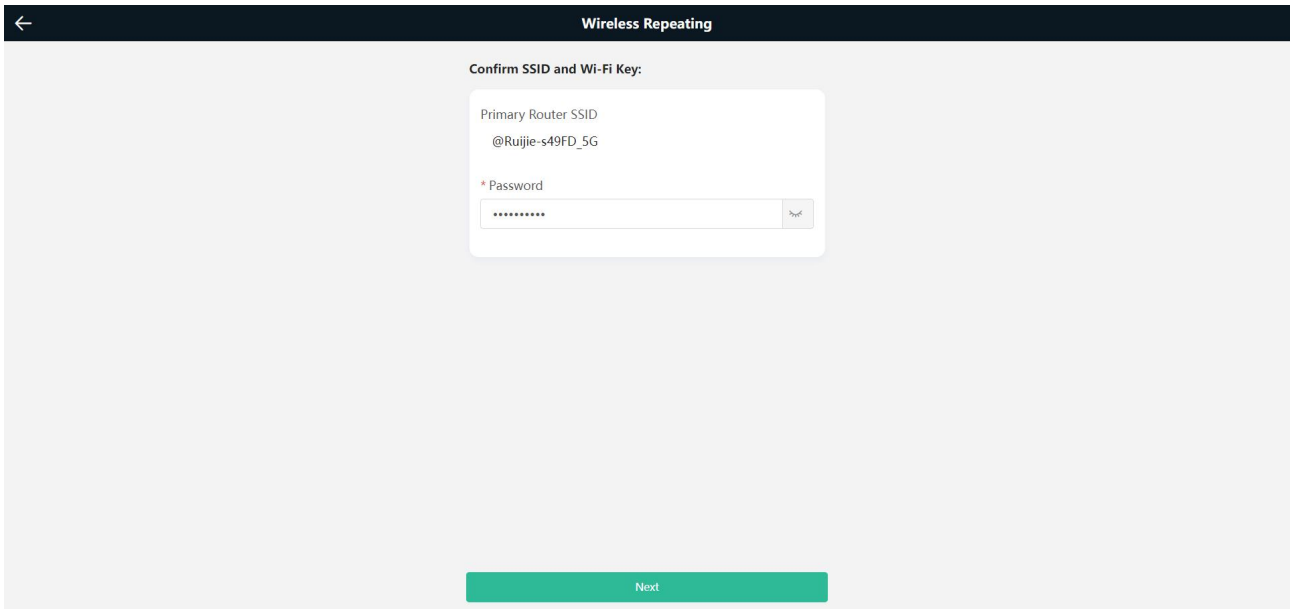
2. Wireless ISP mode

(1) Click **WISP**. On the displayed network setup page, click **Next** to automatically obtain an IP address. If the primary router cannot deliver an IP address, select Static IP. Select the SSID of the primary router and enter the Wi-Fi password

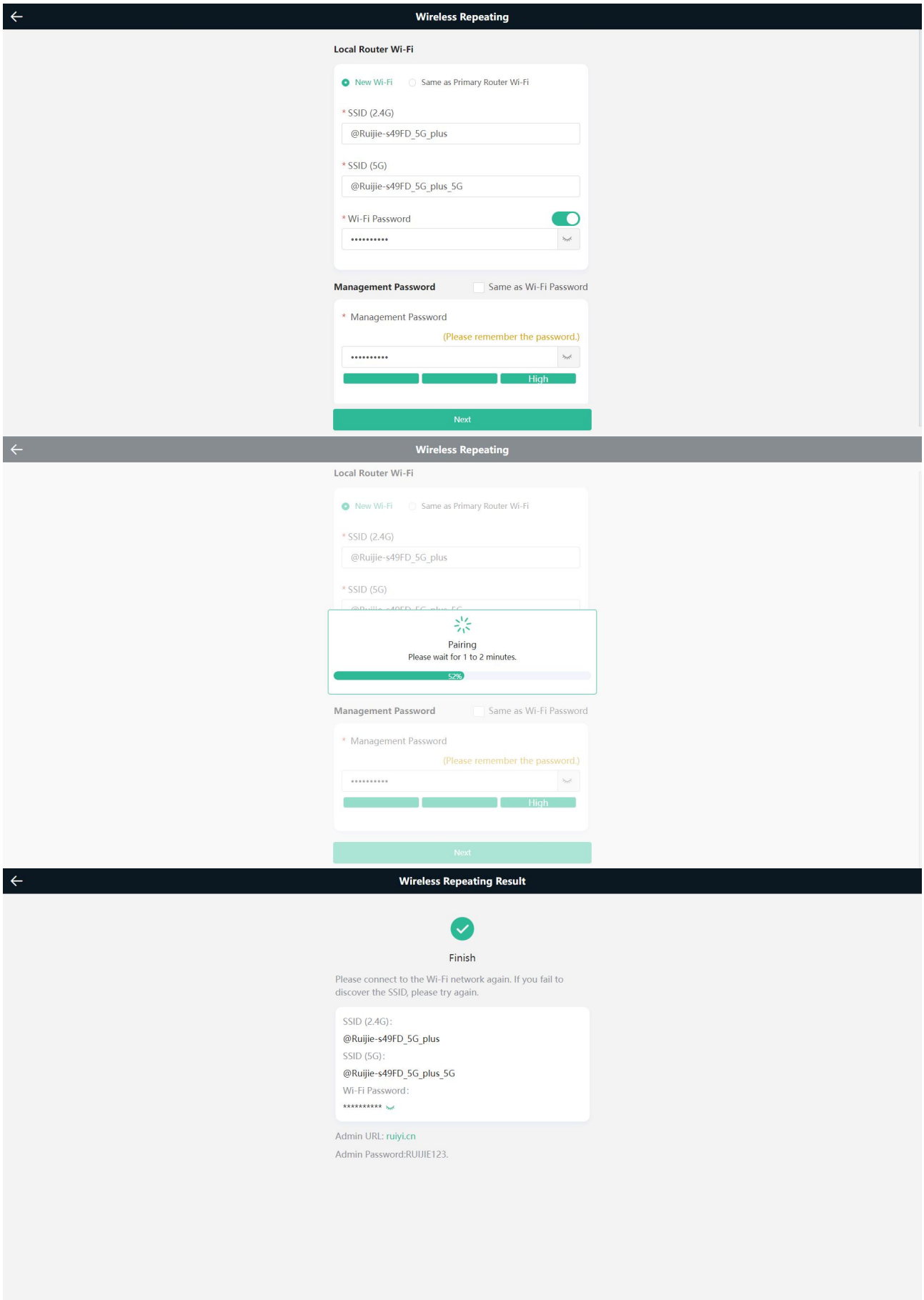
to connect to the primary router.







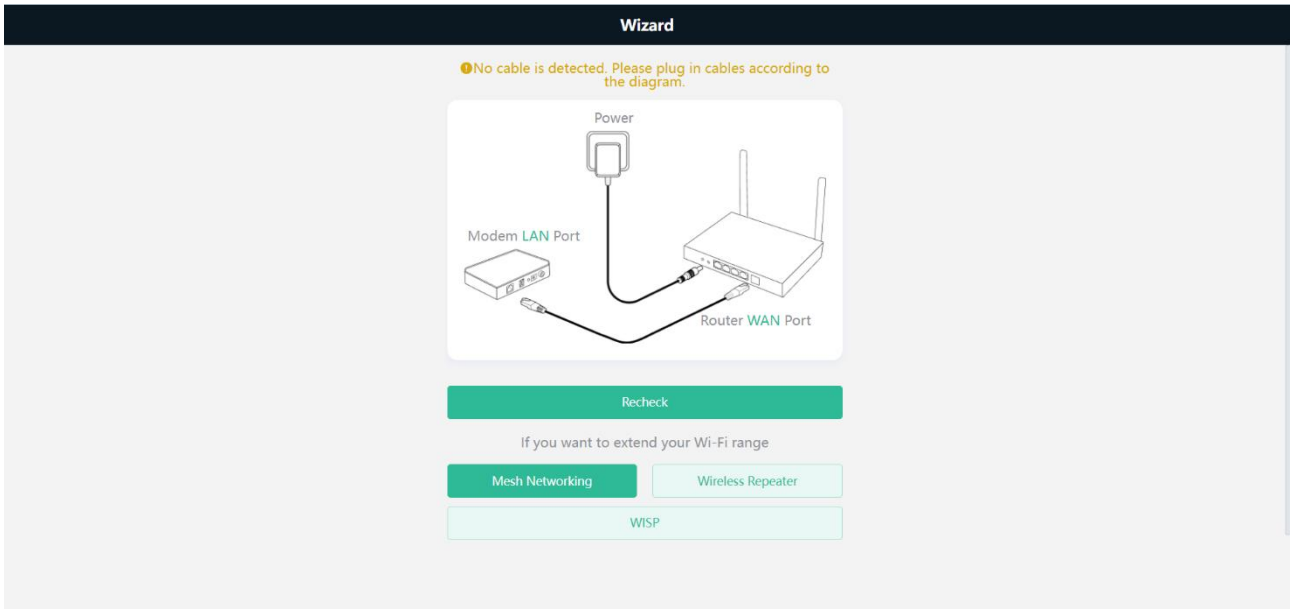
(2) Set the SSID and password and save the settings. Then, the Wi-Fi network will be restarted.

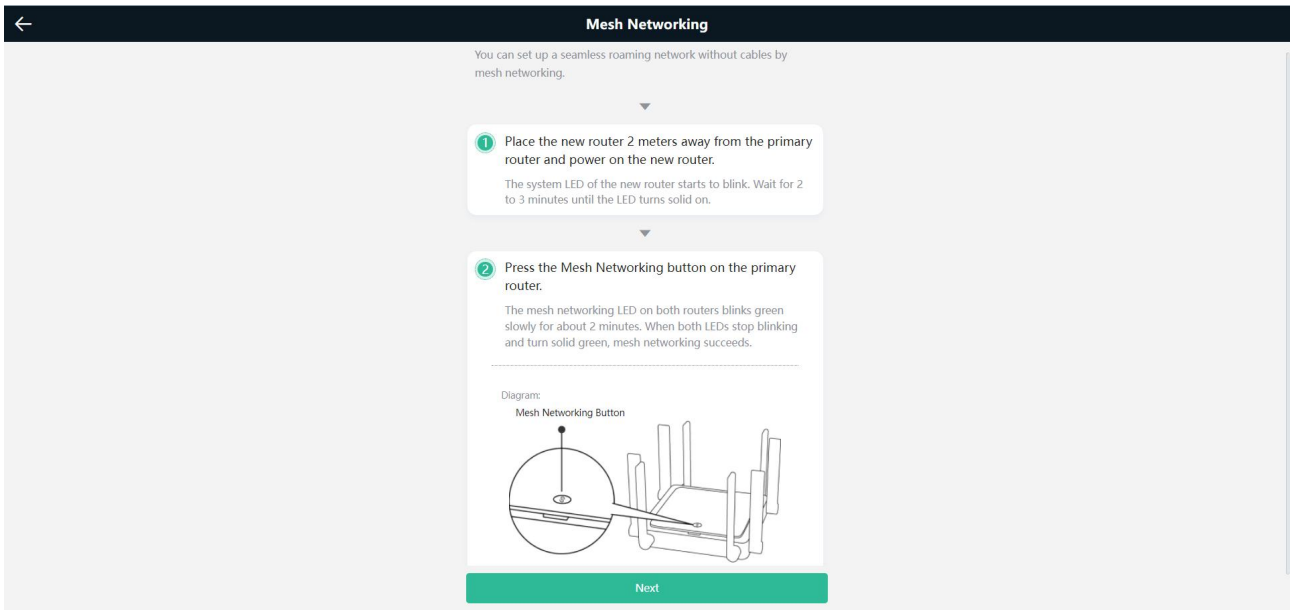

Wireless Repeating
Local Router Wi-Fi
New Wi-Fi
Same as Primary Router Wi-Fi
* SSID (2.4G)
@Ruijie-s49FD_5G_plus
* SSID (5G)
@Ruijie-s49FD_5G_plus_5G
* Wi-Fi Password
Management Password
Same as Wi-Fi Password
* Management Password
(Please remember the password.)
High
Next
Wireless Repeating
Local Router Wi-Fi
New Wi-Fi
Same as Primary Router Wi-Fi
* SSID (2.4G)
@Ruijie-s49FD_5G_plus
* SSID (5G)
Pairing
Please wait for 1 to 2 minutes.
52%
Management Password
Same as Wi-Fi Password
* Management Password
(Please remember the password.)
High
Next
Wireless Repeating Result
Finish
Please connect to the Wi-Fi network again. If you fail to discover the SSID, please try again.
SSID (2.4G):
@Ruijie-s49FD_5G_plus
SSID (5G):
@Ruijie-s49FD_5G_plus_5G
Wi-Fi Password:
Admin URL: ruiyi.cn
Admin Password:RUIJIE123.

In the wireless ISP mode, the device still supports routing and DHCP functions, the IP addresses of clients connected to the primary router are assigned by the primary router and the IP addresses of clients connected to the secondary router are assigned by the secondary router. When the device connects to the Internet through wireless connection, the wired WAN port becomes the LAN port for use by clients.

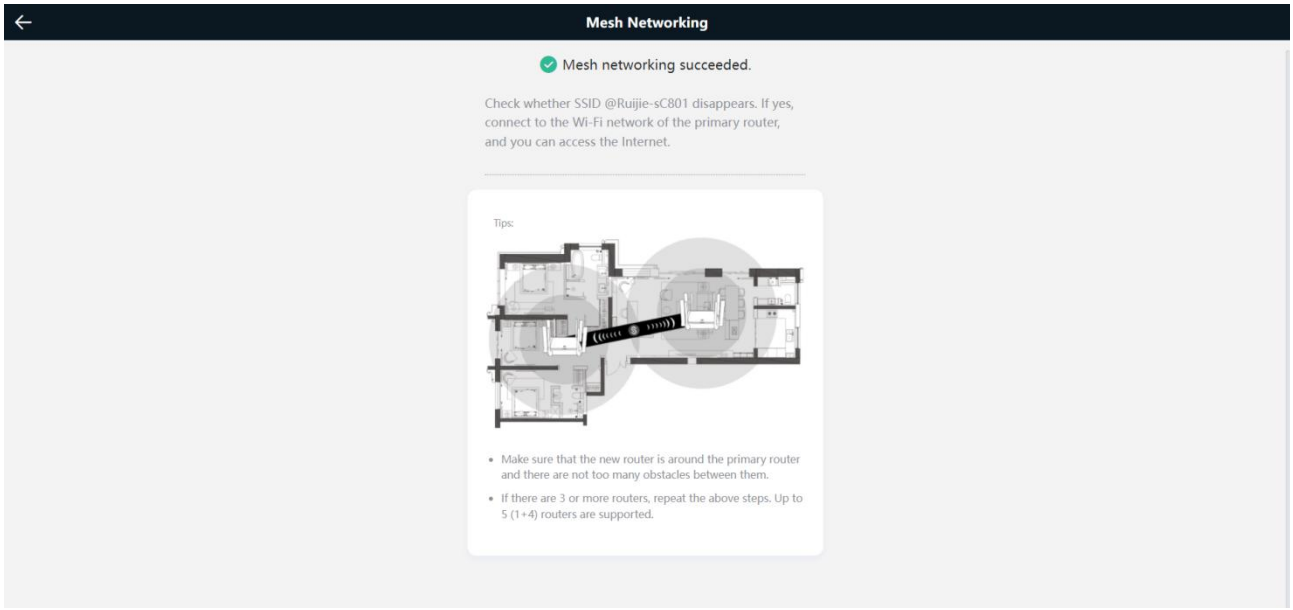
Mesh

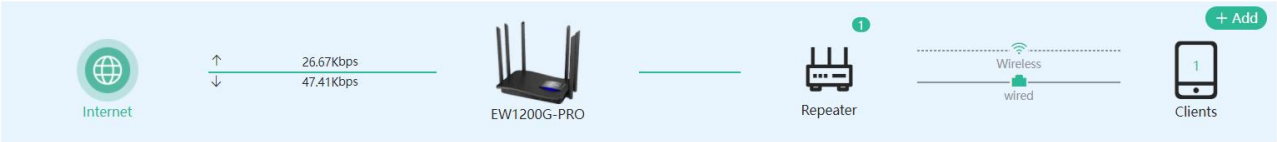
(1) Click **Mesh Networking**, then click the Next button after enter the mesh page. According to the mesh steps in this page, press the mesh networking button on the primary and second router.





(2) After the page prompts that the mesh networking is succeeded, you can see one new repeater is connecting to primary router.

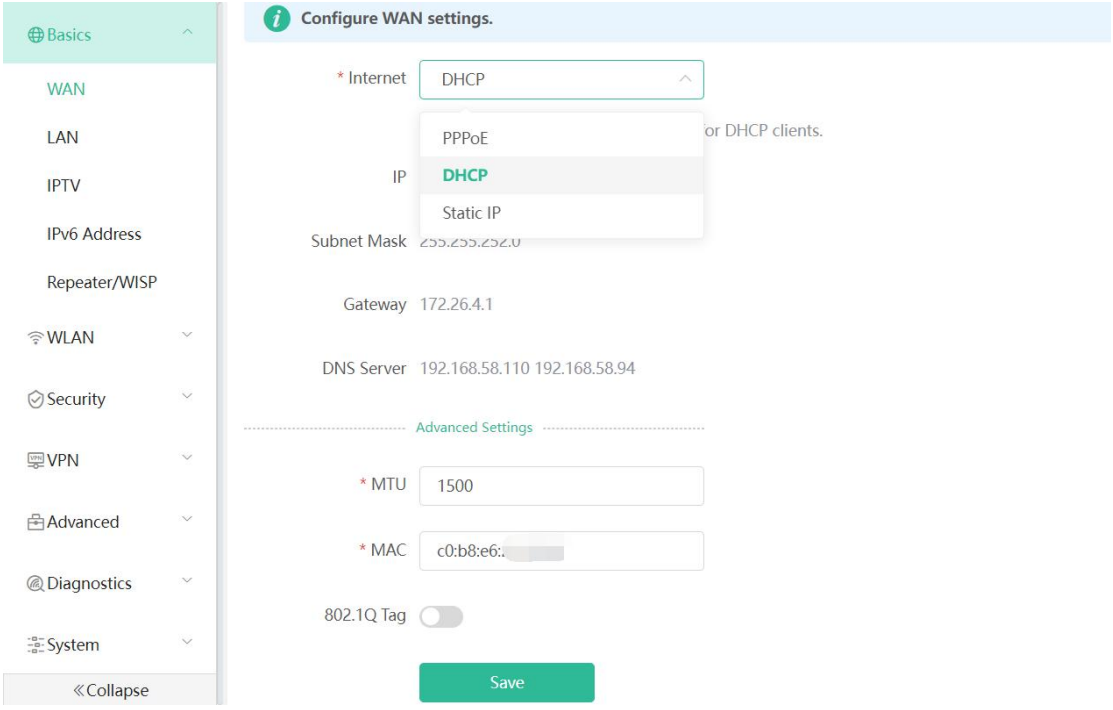




4.5.1.2 Basic

1.1 WAN

The router supports three Internet connection types: PPPoE, DHCP, and static IP.



MTU: Sometimes, the ISP restrict the speed of large data packets or prevent large data packets from passing through. As a result, the network speed is low or even the network is disconnected. In this case, you are required to set the maximum transmission unit (MTU) to a smaller value.

The default MTU value is 1500, which is the maximum MTU size. You are advised to gradually adjust the value to 1492, 1400, or even smaller if necessary.

MAC: The ISP may restrict the access of devices with unknown Mac addresses to the Internet for the sake of security. In this case, you can change the MAC address of the WAN port to another address. You are advised to use the MAC address of an old router that is allowed to access the Internet (the MAC address can be found on the bottom label of the device). Enter the Mac address in the format of 00:11:22:33:44:55.

> ⚠ Note:
>
> Changing the MAC address of the LAN or WAN port will disconnect the network. You need to reconnect to the router or restart the router, please handle with care.

1.2 LAN

a) Overview

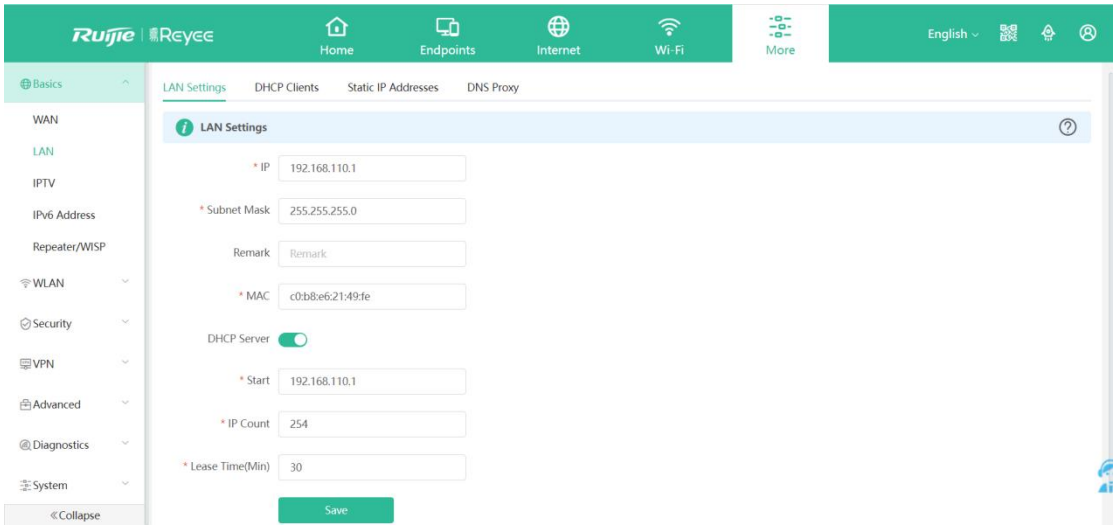
The DHCP server function enables a router to automatically assign IP addresses to clients so that clients connected to the LAN ports or Wi-Fi network of the router could obtain IP addresses for Internet access. When multiple routers are connected through LAN ports, the DHCP server conflict will occur. In this case, you need to disable the DHCP server function and keep the DHCP service only on one router available. Otherwise, some devices may be disconnected to the network from time to time.

b) Configuration Steps

Choose **More > Basics > LAN.**

DHCP Server: The DHCP server function is enabled by default. You are advised to enable it when only a single router is used. When multiple routers are connected to the primary router through LAN ports, you need to disable this function.

If the DHCP server function is disabled on all routers on the network, clients cannot automatically obtain IP addresses. You need to enable the DHCP server on a router or manually configure a static IP address for every clients for Internet access.



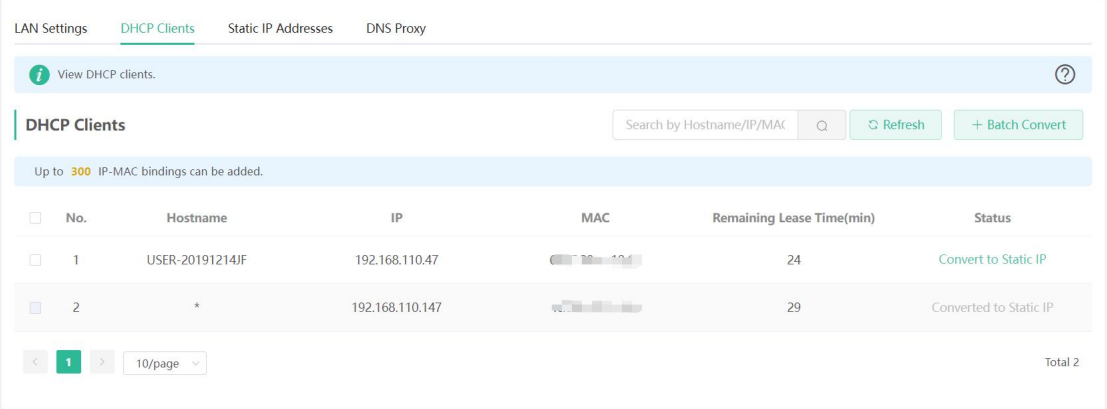
Configure the IP address and subnet mask, and click Save. After the IP address of a LAN port is changed, you need to log in to eWeb by using the new IP address of the LAN port.

Start: Enter the initial IP address of the DHCP address pool. Client obtains an IP address from the address pool. If all the addresses in the address pool are used up, the client will fail to obtain the IP address.

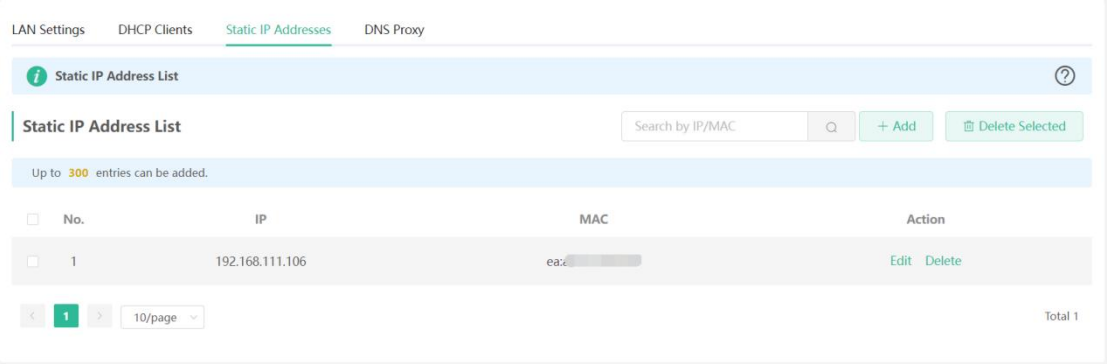
IP Count: Enter the number of IP addresses in the address pool. The default value is 254.

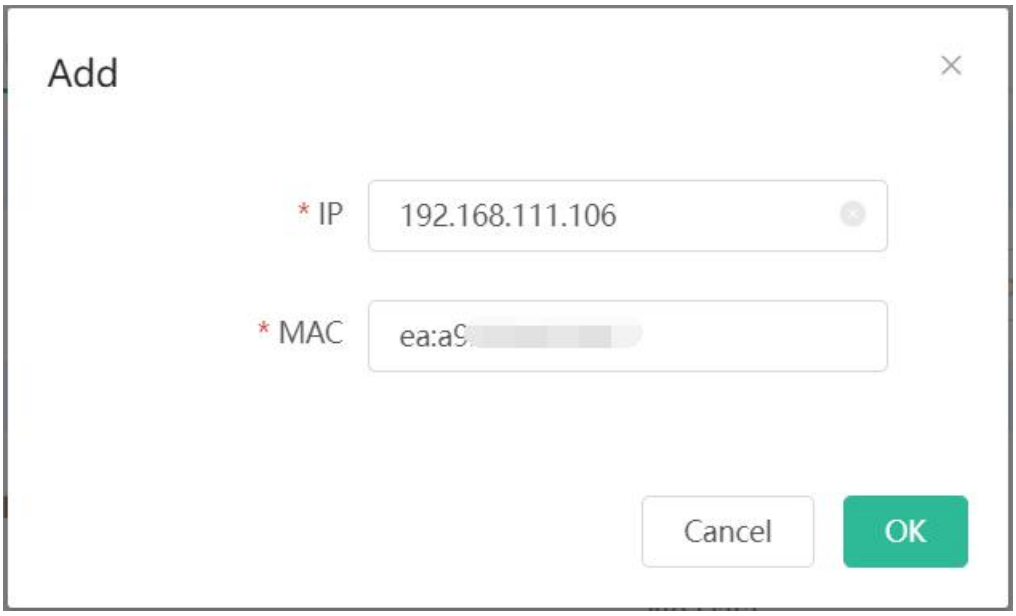
Lease Time (Min): Enter the address lease time period. When a client keeps connecting, the lease is automatically renewed. If the lease time is not renewed due to the client disconnection or network instability, the IP address will be reclaimed after the lease period expires. After the client connection is restored, the client could request an IP address once again. The default lease period is 30 minutes.

DHCP Clients: this page displays all clients got IP address from this device. Click Convert to Static IP to bind specify static IP address, you can see all users with static IP address in the Static

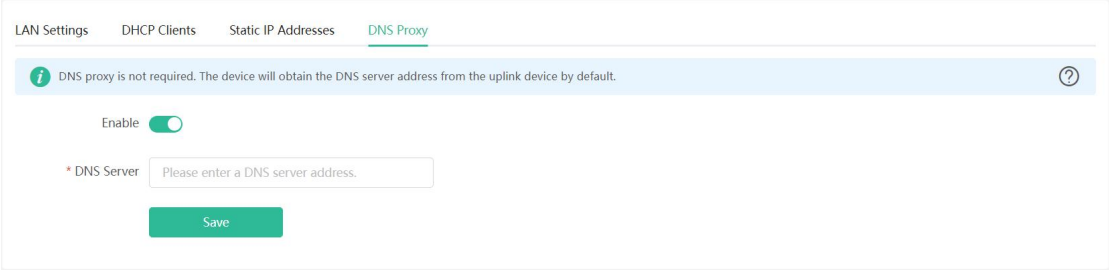


Static IP Address List: Click **Add.** In the displayed static IP address dialog box, enter the Mac address and the IP address of the target client, and click **OK.** After the static IP address is bound, the client will obtain the IP address when they connect to the router.





DNS Proxy: It is disabled by default and the DNS delivered by a carrier is used. If the DNS is incorrectly configured, the network is accessible and the mobile app can access the Internet properly, but the Web page cannot be opened. You are advised to disable the function.



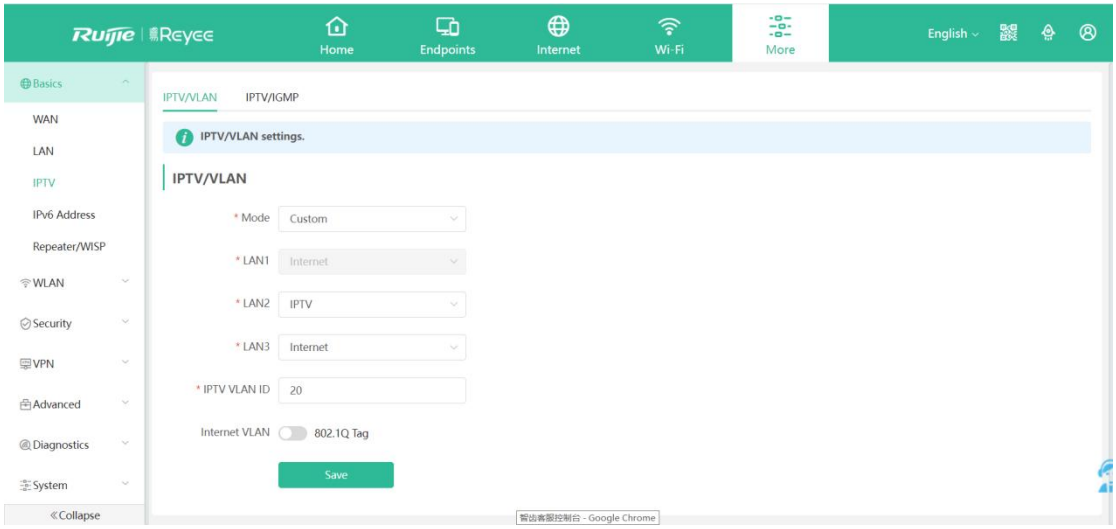
DNS Server: Clients automatically use the DNS service provided by the primary router by default. The default configuration is recommended. After the DNS proxy function is enabled, you can enter the IP address of the DNS server. The available DNS service varies from region to region. You can consult the local ISP.

1.3 IPTV

a) **IPTV/VLAN**

Choose **More > Basics > IPTV.** IPTV is an Internet television service provided by ISP. At the beginning, you need to check whether the IPTV service has been provisioned and the local IPTV service is of the VLAN or Internet Group Management Protocol (IGMP) type. If the local IPTV is of the VLAN type, confirm the VLAN ID. If you are not sure of the IPTV type, contact your local ISP.

Select a local ISP mode, click the drop-down list of the target port, select IPTV from the drop-down list, and enter the VLAN ID provided by the ISP. For example, connect an IPTV set top box (STB) to LAN3 and set the VLAN ID to The configuration is shown in the figure below.

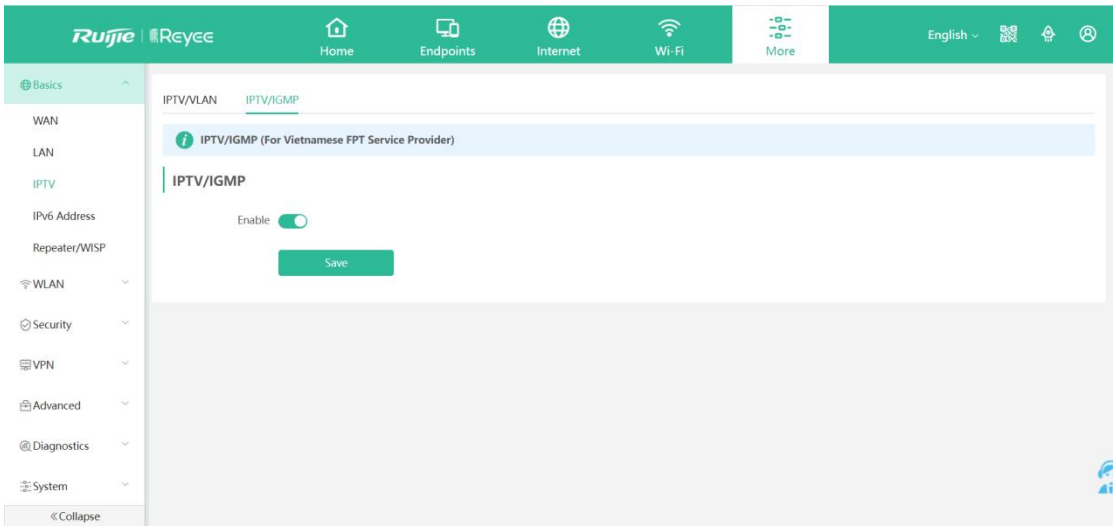


Internet **VLAN**: If a VLAN ID needs to be set for the Internet access service, enable the Internet VLAN function and enter a VLAN ID. The VLAN tag function is disabled by default. You are advised to disable the function unless in special cases.

After the configuration, confirm that the IPTV STB is connected to the specified port properly. Take the following figure as an example, connect the IPTV STB to LAN3.

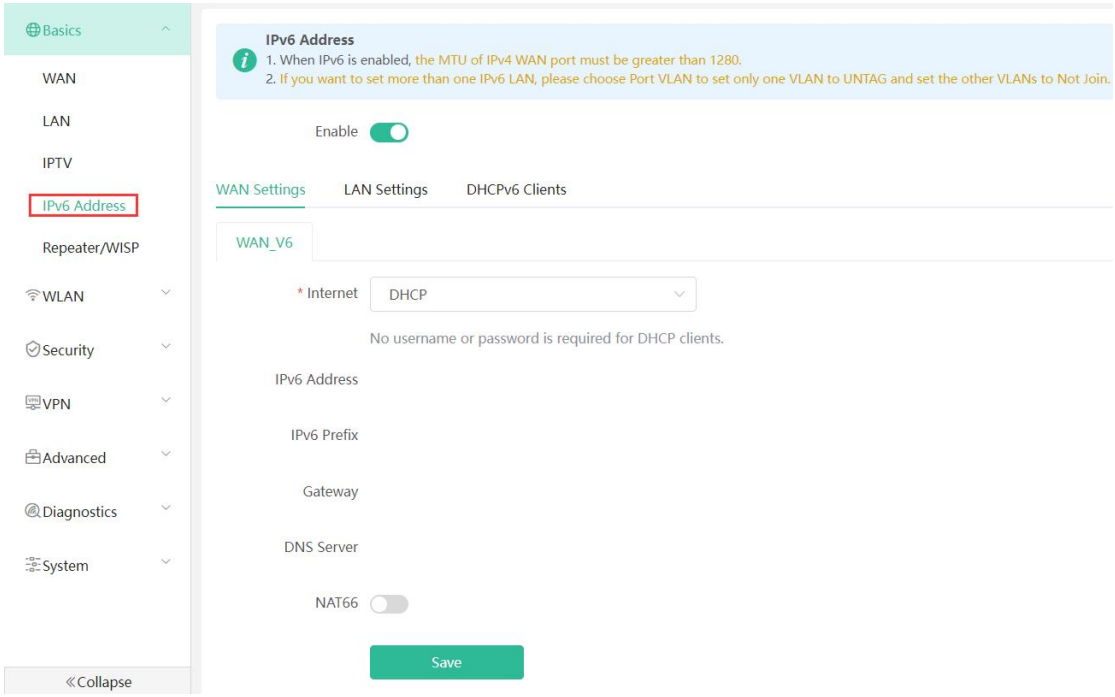
b) IPTV/IGMP

The configuration applies to Vietnam FPT ISP. After it is enabled, connect the IPTV STB to any LAN port of the router.

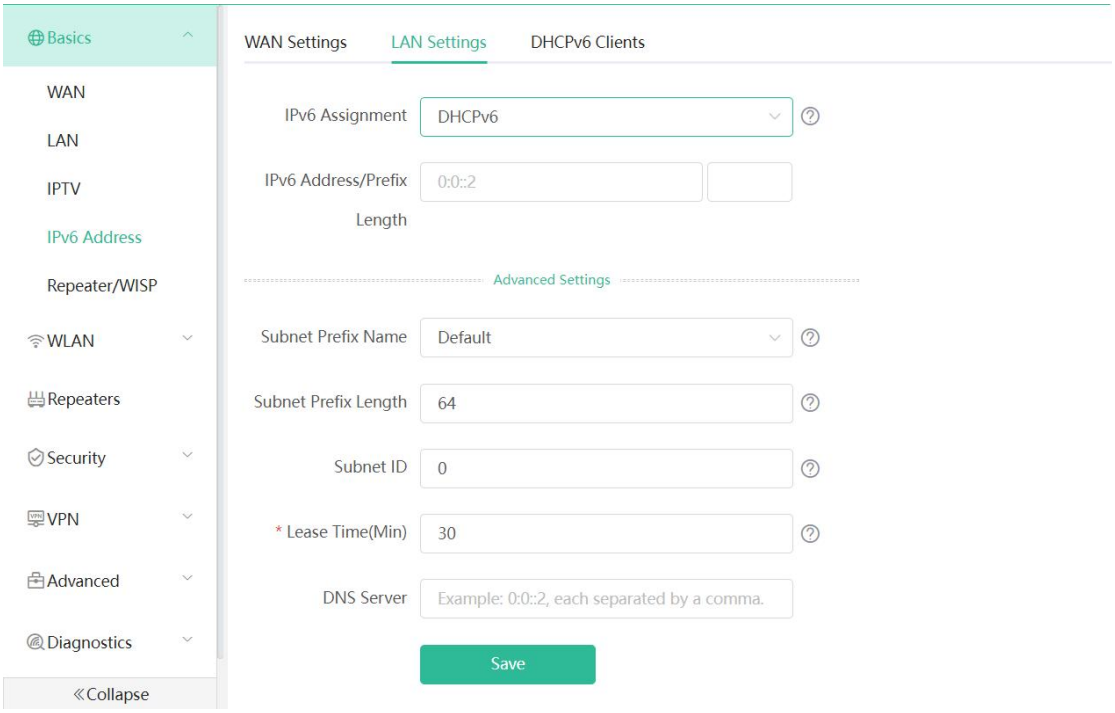


1.4 IPv6 Address

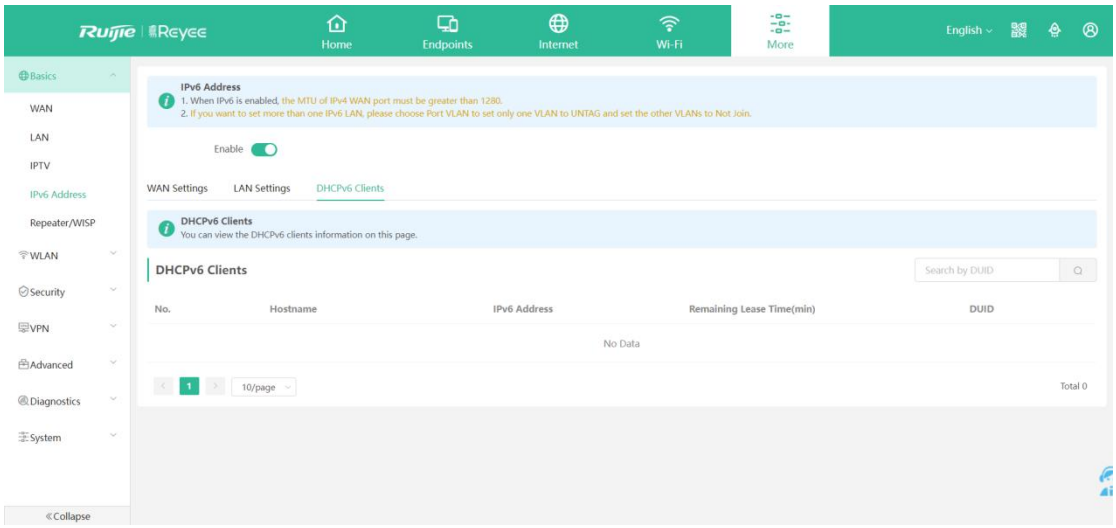
The WAN Settings module allows you to configure WANv6 settings, including DHCP, static



The LAN Settings module allows you to configure LANv6 settings. For IPv6 Assignment, you can chose Auto, DHCPv6 and SLAAC. For IPv6, you need to input one IPv6 Prefix.

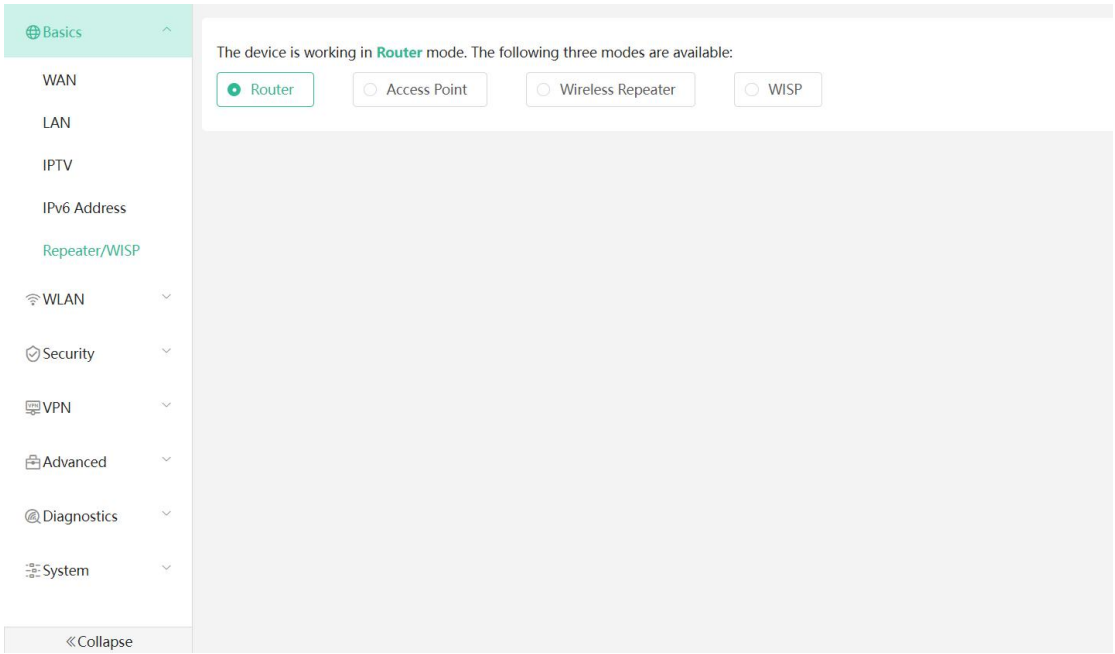


The DHCPv6 Clients module allows you to configure DHCPv6 clients.



1.5 Repeater/WISP

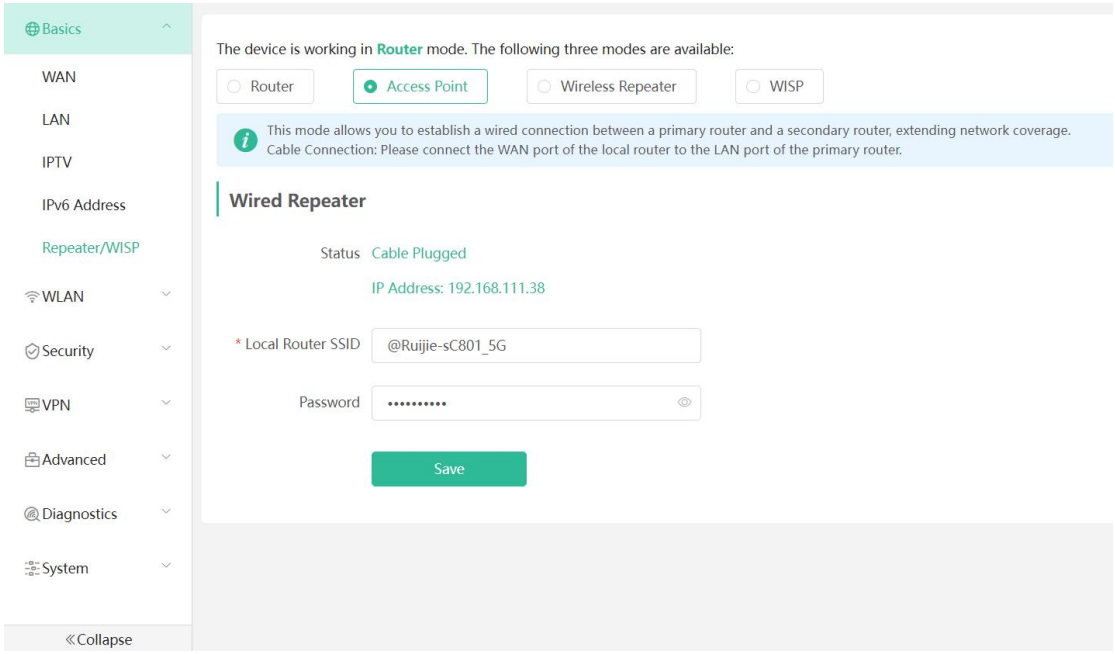
Router: the Repeater/WISP module displays the current mode and the other available modes. When device works as Router mode, it means this device acts as the DHCP server and connected users will obtain the ip address from this device.



Access Point

The Access Point mode relies on a network cable to provide reliable transmission over a more stable Wi-Fi network with less interference. You are advised to use the wired repeater mode. Ensure that the primary router can access the Internet with DHCP server enabled. Otherwise, the configuration will fail.

Click **Access Point**, click **Check**, and then click **Save**. The device will run in the AP mode, namely, network address translation (NAT) and DHCP-related routing functions will be disabled.

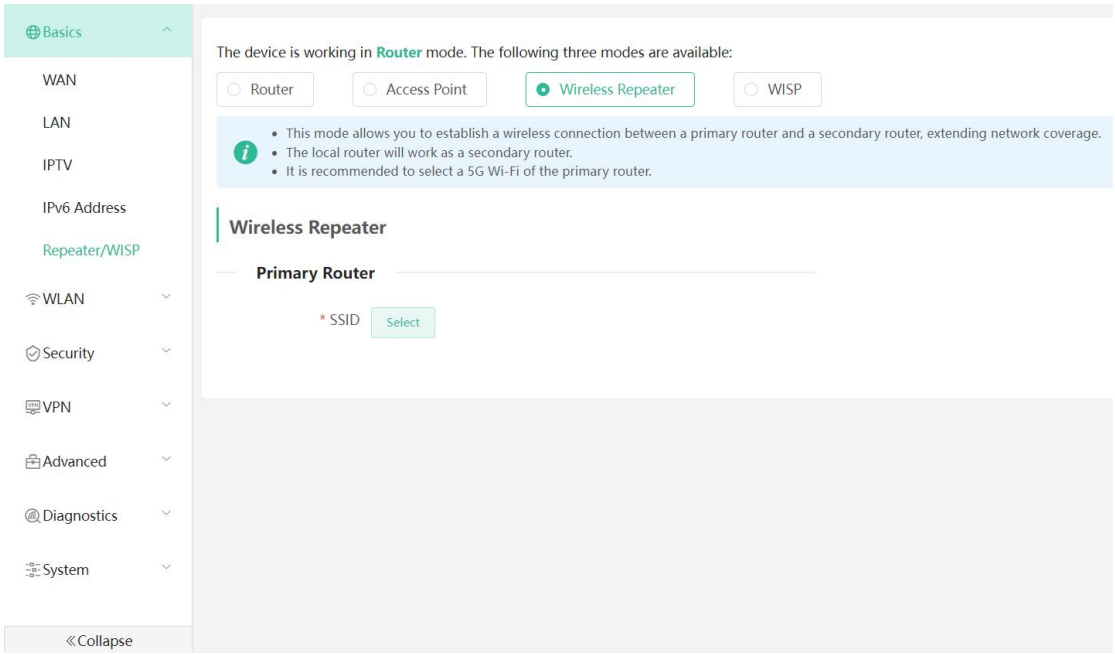


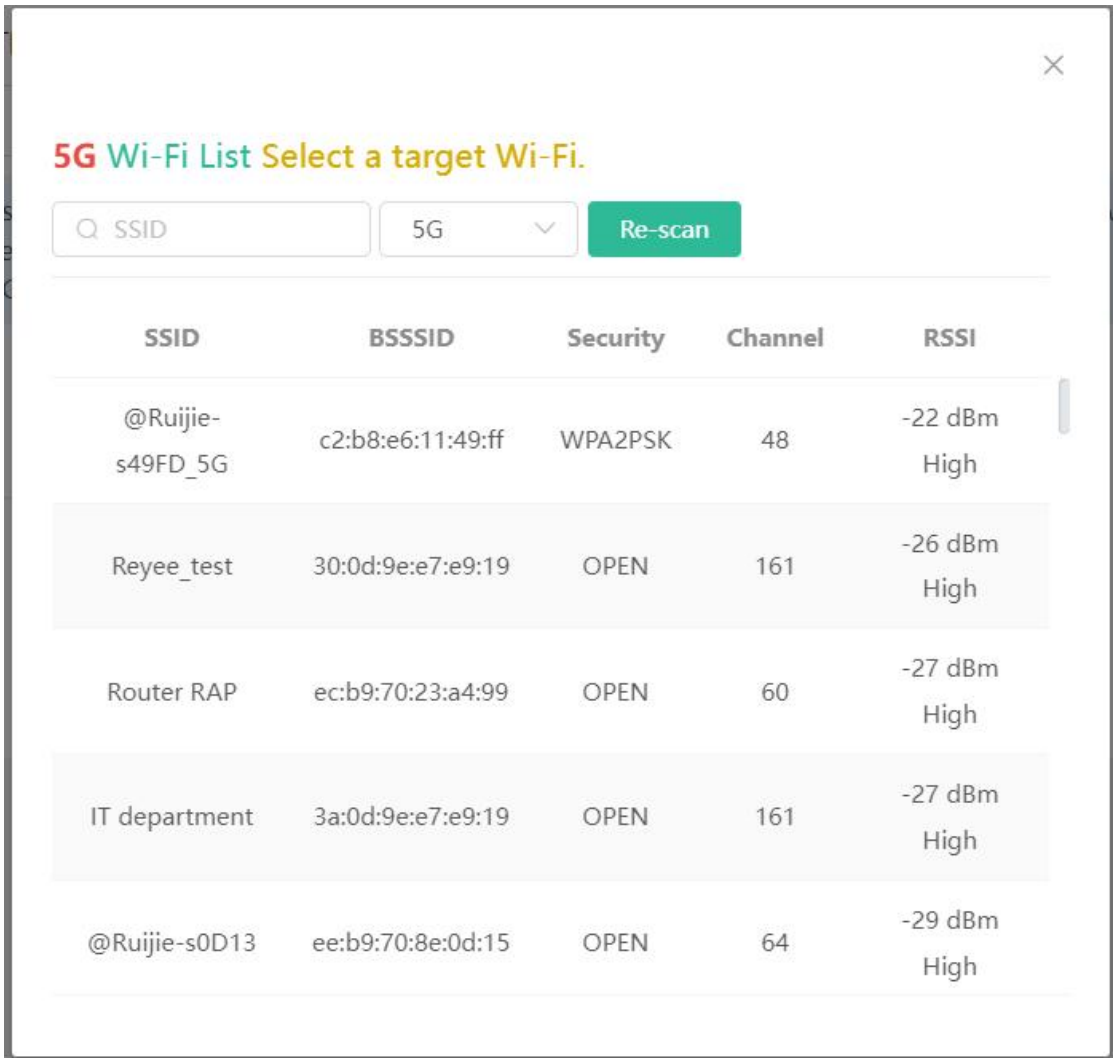
> **Note:**
>
> Ensure that the primary router can access the Internet with DHCP server enabled. After the configuration is saved, the Wi-Fi network will be restarted, and clients need to reconnect the Wi-Fi network.

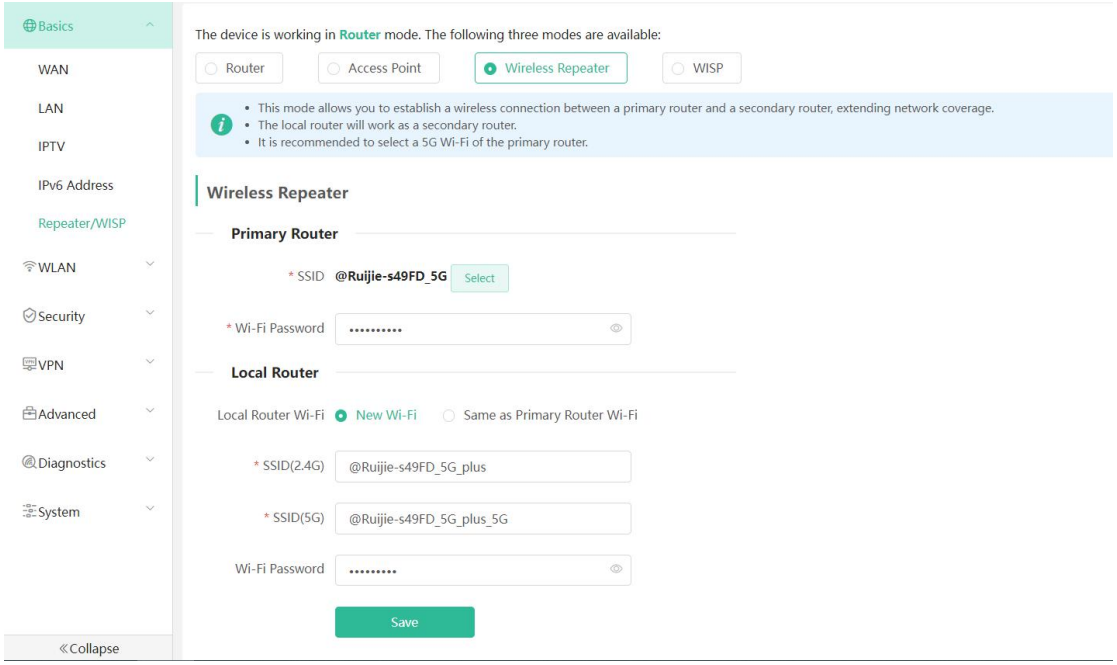
Wireless Repeater

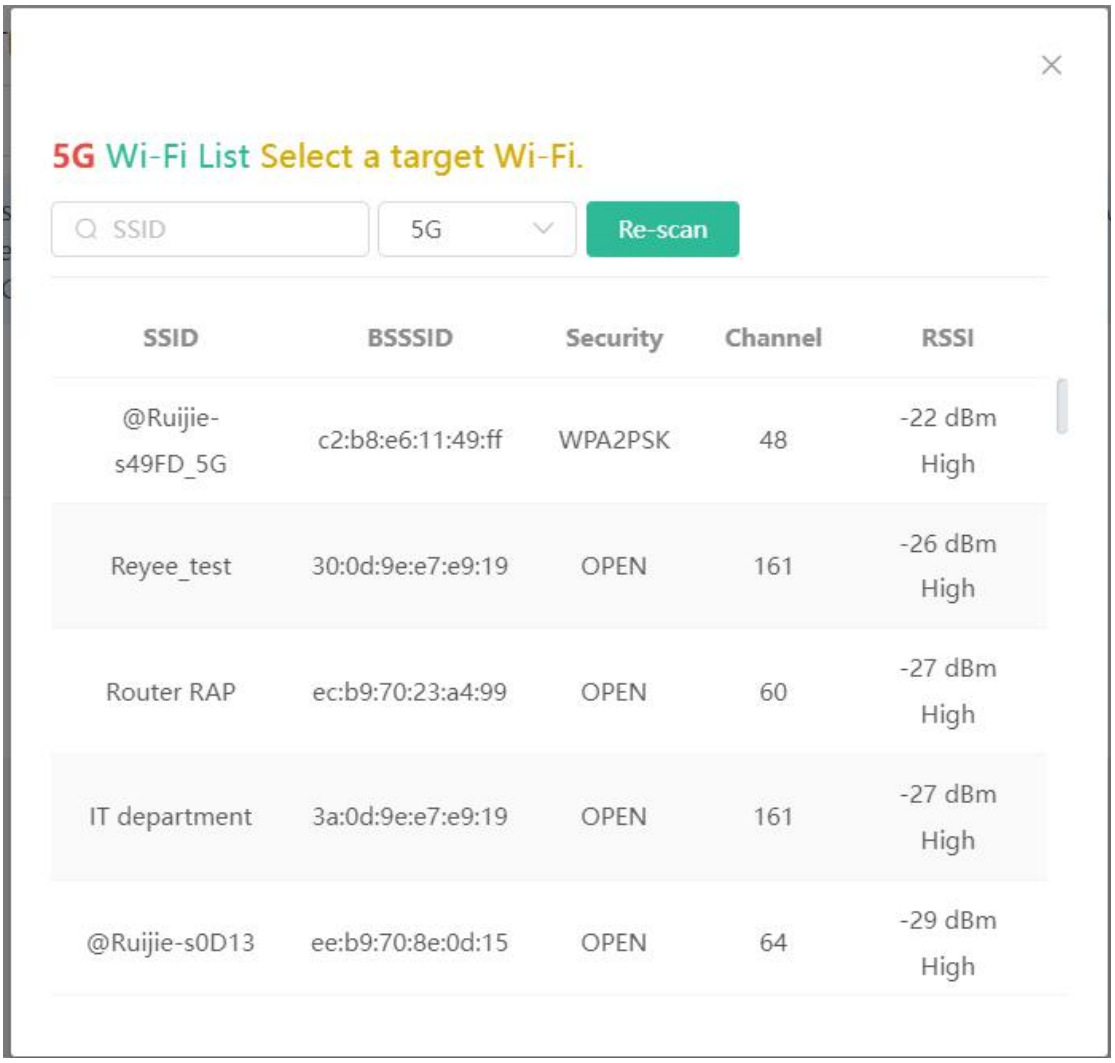
The wireless repeater mode extends the Wi-Fi coverage of the primary router. Switch this device over to the wireless repeater mode, it needs slave device connect the SSID of master device. After enable this feature, the connected users will obtain the IP address from the uplink device.

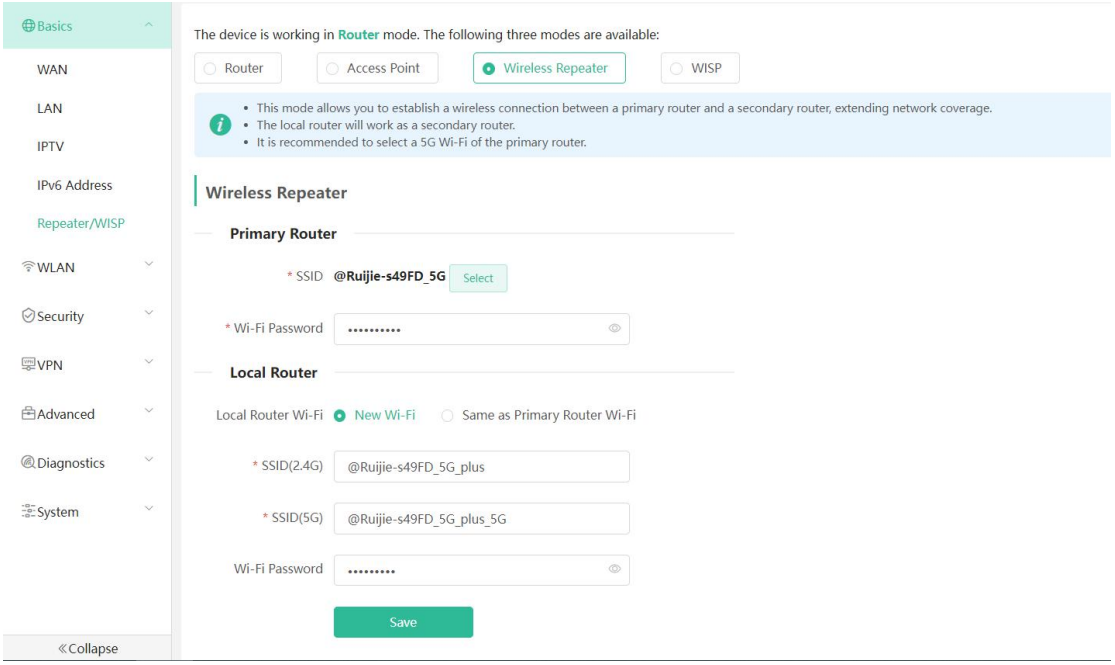
Click **Wireless Repeater** and then click **Select**. A list of surrounding Wi-Fi signals pops up.




5G Wi-Fi List Select a target Wi-Fi.
SSID
5G
Re-scan
SSID BSSSID Security Channel RSSI
@Ruijie-s49FD_5G c2:b8:e6:11:49:ff WPA2PSK 48 -22 dBm High
Reyee_test 30:0d:9e:e7:e9:19 OPEN 161 -26 dBm High
Router RAP ec:b9:70:23:a4:99 OPEN 60 -27 dBm High
IT department 3a:0d:9e:e7:e9:19 OPEN 161 -27 dBm High
@Ruijie-s0D13 ee:b9:70:8e:0d:15 OPEN 64 -29 dBm High


Basics
WAN
LAN
IPTV
IPv6 Address
Repeater/WISP
WLAN
Security
VPN
Advanced
Diagnostics
System
Collapse
The device is working in Router mode. The following three modes are available:
Router
Access Point
Wireless Repeater
WISP
This mode allows you to establish a wireless connection between a primary router and a secondary router, extending network coverage.
The local router will work as a secondary router.
It is recommended to select a 5G Wi-Fi of the primary router.
Wireless Repeater
Primary Router
* SSID @Ruijie-s49FD_5G Select
* Wi-Fi Password
Local Router
Local Router Wi-Fi New Wi-Fi Same as Primary Router Wi-Fi
* SSID(2.4G) @Ruijie-s49FD_5G_plus
* SSID(5G) @Ruijie-s49FD_5G_plus_5G
Wi-Fi Password
Save





In this mode, you can create new WiFi for users to connect or chose the WiFi same as primary router WiFi.

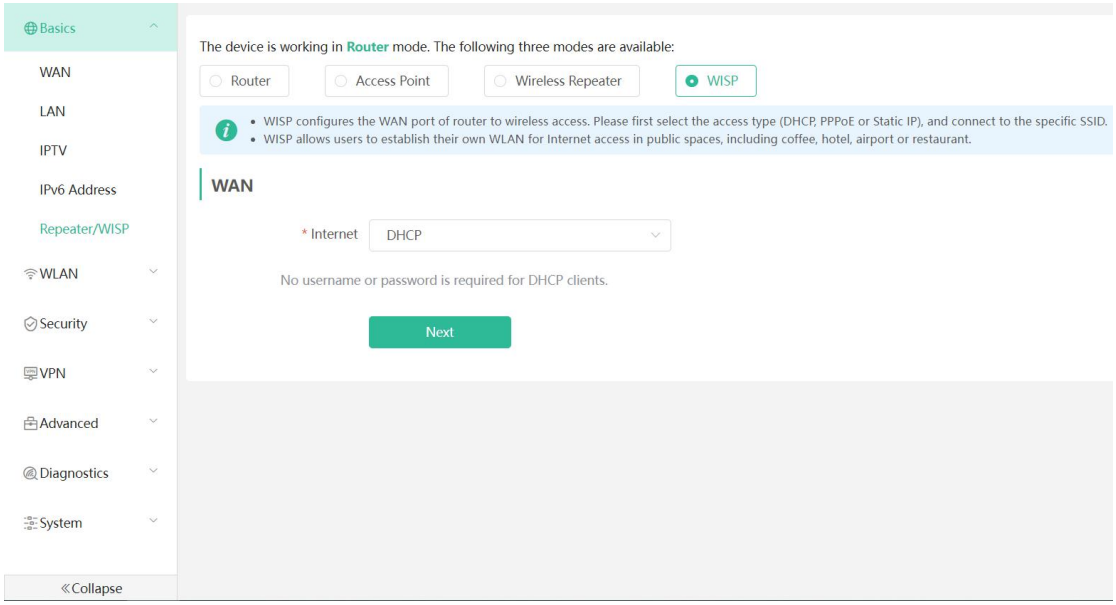
Note:

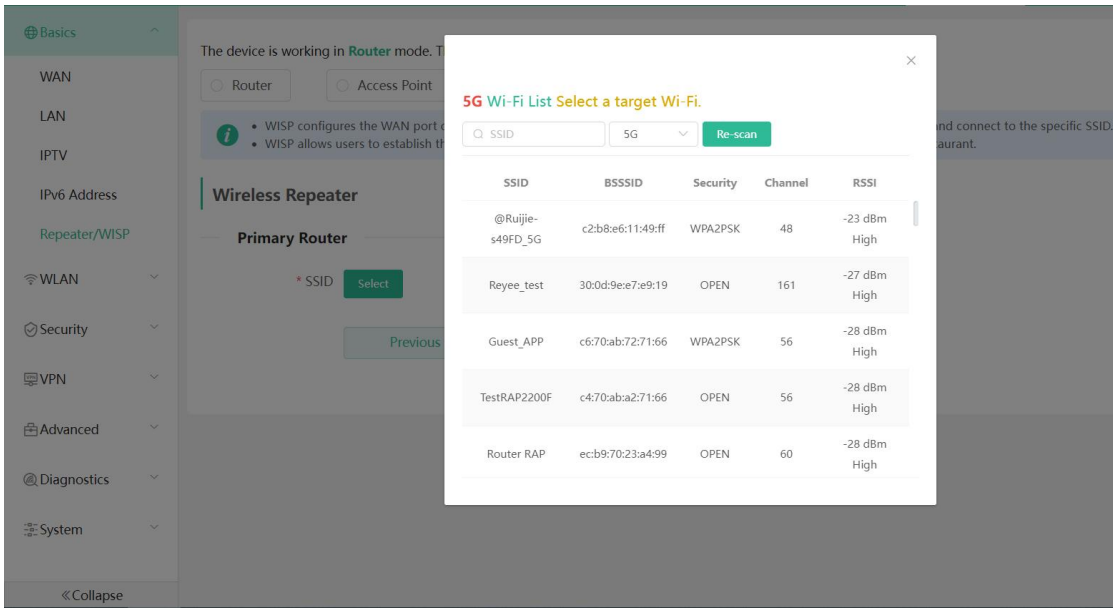
1) The wireless repeater mode will affect the network speed and stability. You are advised to plug in a network cable and select the wired repeater mode if the network cable is available.

2) In the wireless repeater mode, unpluging the WAN cable to prevent loops, which may cause network interruption.

WISP

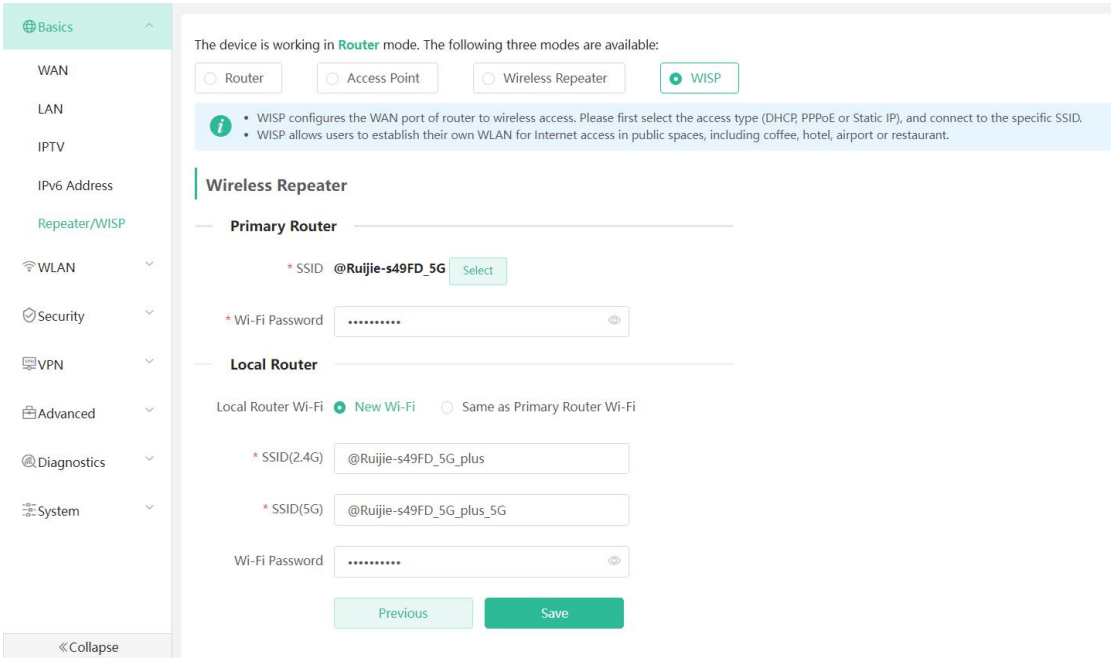
Switching the device to the WISP mode allows users to establish their own WLAN for Internet access in public spaces, such as coffee shop, hotel, airport or restaurant. WISP configures the WAN port of router to wireless access. Please first select the access type (DHCP, PPPoE or Static IP), and connect to the specific SSID.



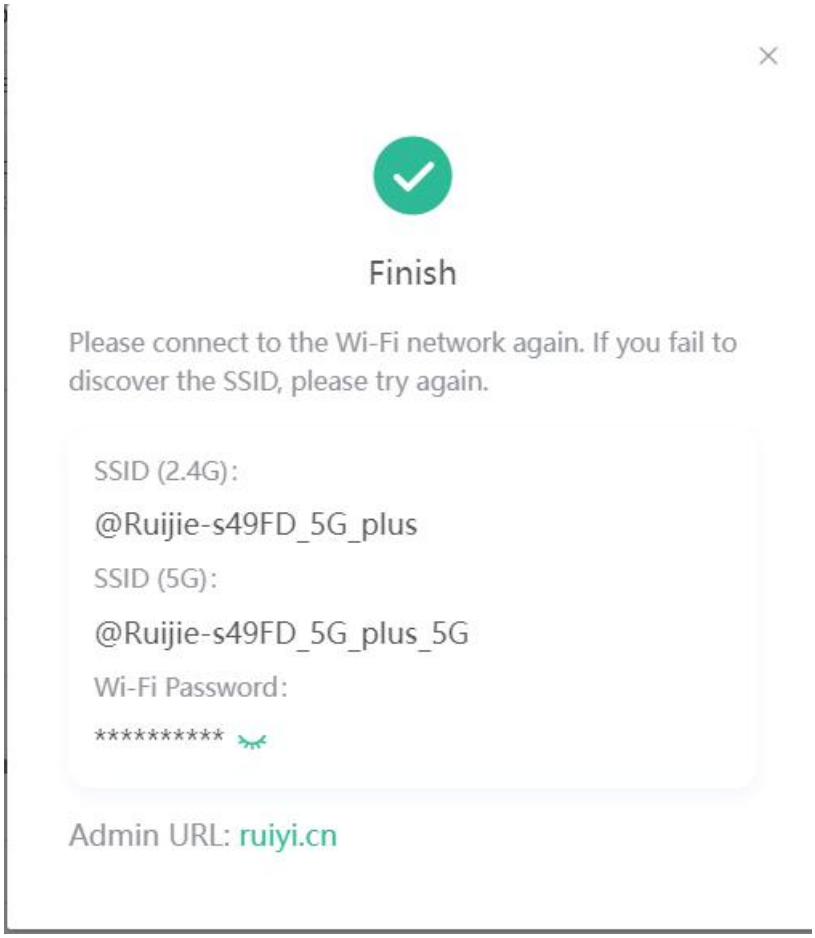


Note:

After you click **Save**, the Wi-Fi network will restart. You need to connect the new Wi-Fi network. Exercise caution when performing this operation. Remember the SSID and password.



In this mode, you can create a new WiFi for the user to connect or choose the WiFi same as primary router WiFi.

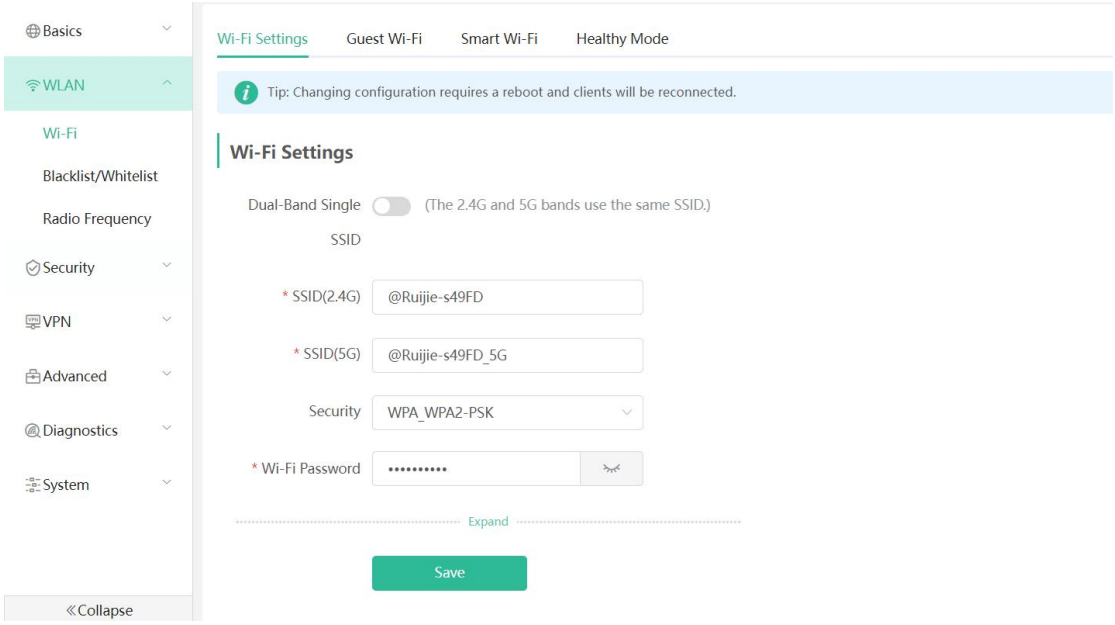


4.5.1.3 WLAN

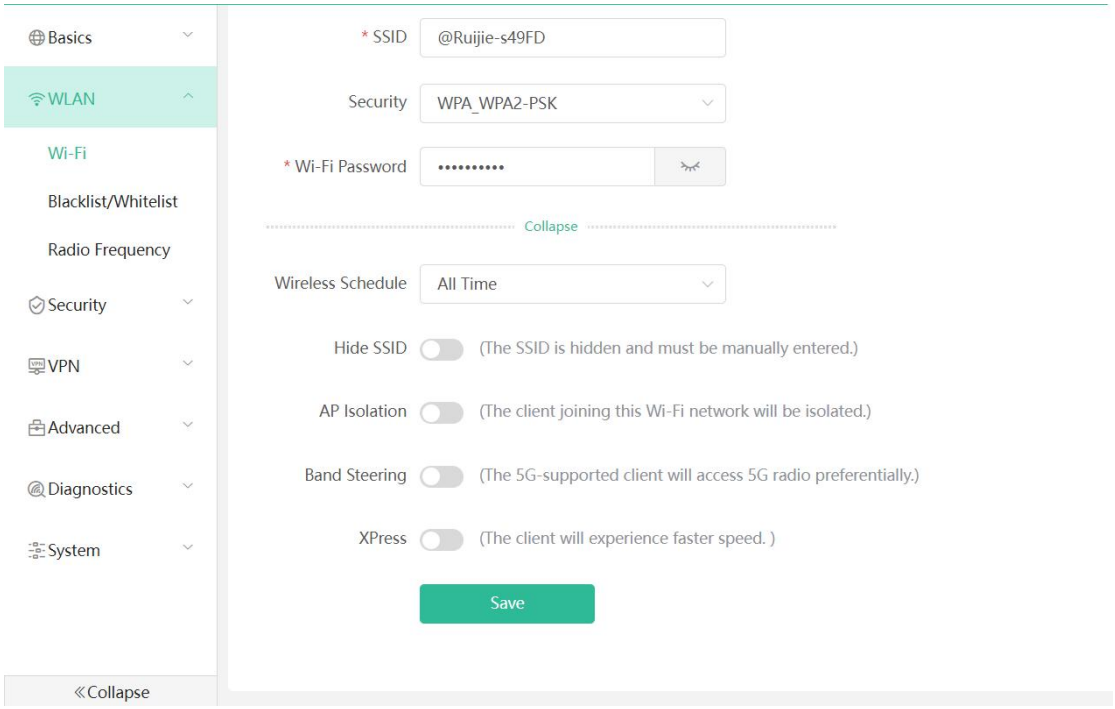
1.1 Wi-Fi

a) Wi-Fi settings

The WiFi Settings module allows you to configure the primary WiFi. If the **Dual-Band Single** function is enabled, the 2.4G and 5G bands will use the same SSID.



Click the **Expand** button to make some advanced settings for this SSID, including Wireless Schedule, Hide SSID, AP isolation, Band Steering and Xpress. For **Wireless Schedule, you can choose All Time, Weekdays, Weekends and Custom.**



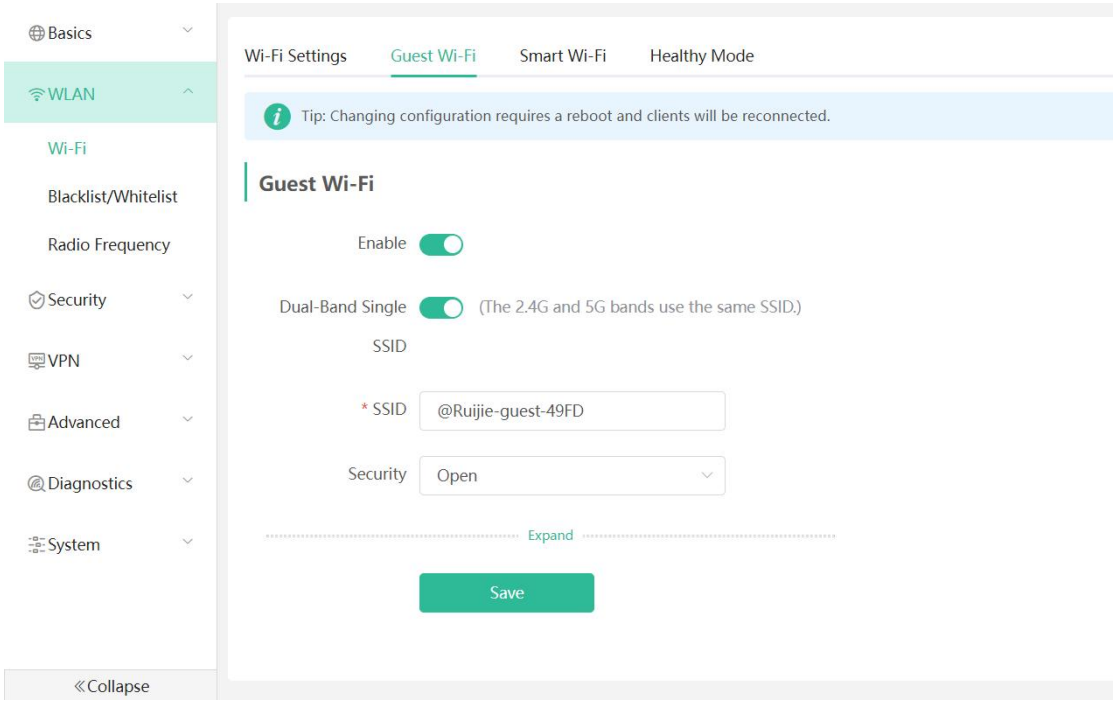
Hide SSID: Hiding the SSID can prevent unauthorized users from accessing the Wi-Fi network and enhance network security. After this function is enabled, the mobile phone or PC cannot search out the SSID. Instead, you have to manually enter the correct SSID and password.

Xpress: if this feature is enabled, you will have a more stable gaming experience.

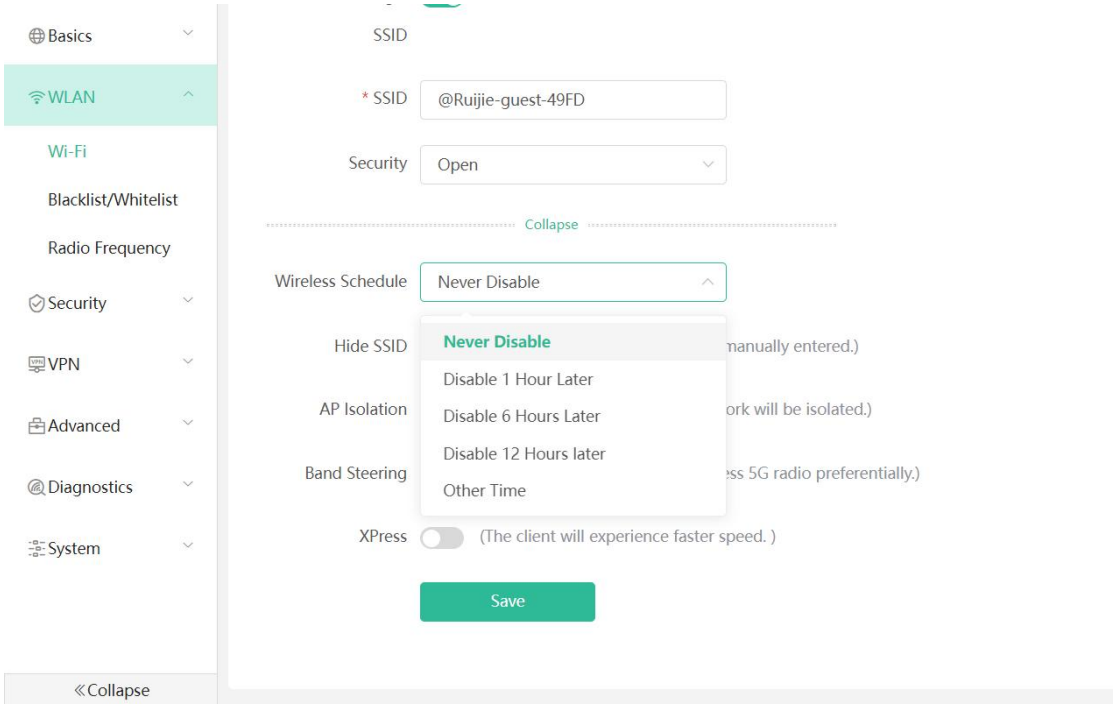
b) Guest Wi-Fi

This Wi-Fi network is provided for guests and is disabled by default. It supports user isolation, that is, accessed users are isolated from each other. They can only access the Internet via Wi-Fi, so as to ensure safety.

The guest Wi-Fi network can be turned off as scheduled. You can configure to turn off the guest Wi-Fi network one hour later. When the time expires, the guest network is off.

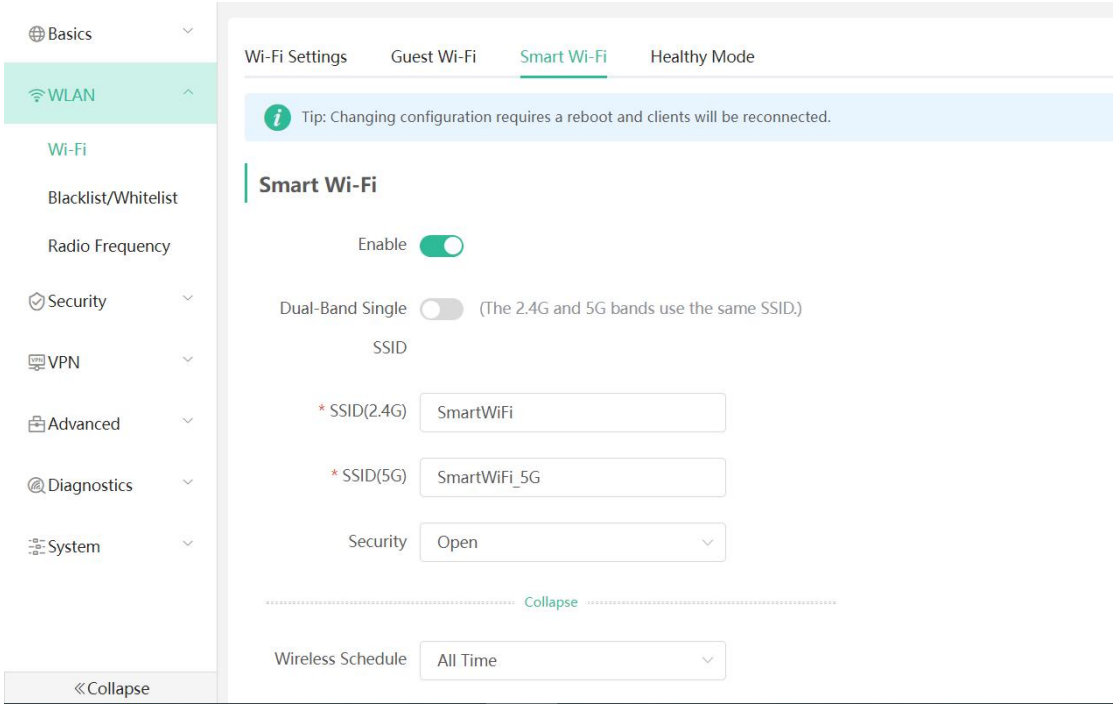


Click the **Expand** button to make some advanced settings for guest WiFi, including Wireless Schedule, Hide SSID, AP isolation, Band Steering and Xpress. For Wireless Schedule, you can chose Never Disable, Disable 1 Hour Later, Disable 6 Hour Later, Disable 12 Hour Later and other Time. The AP isolation is enabled by default and cannot be edited.

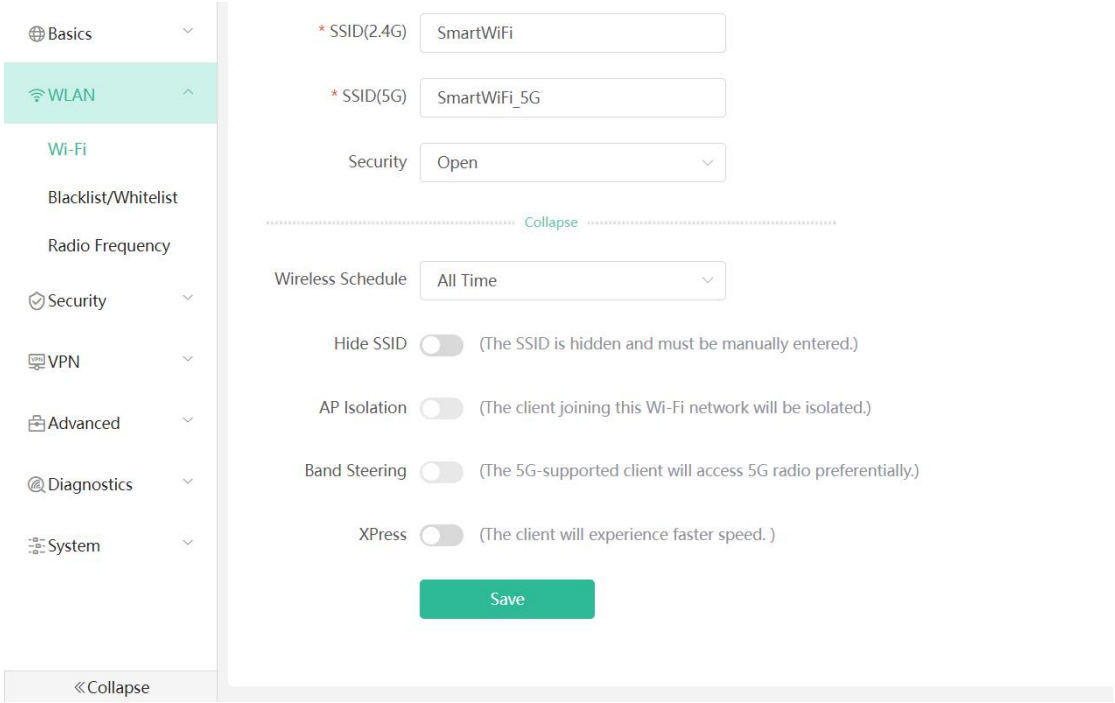


c) Smart Wi-Fi

The smart Wi-Fi network is disabled by default. Smart terminal devices can connect to the smart Wi-Fi network for long. The smart Wi-Fi network cannot be turned off as scheduled.



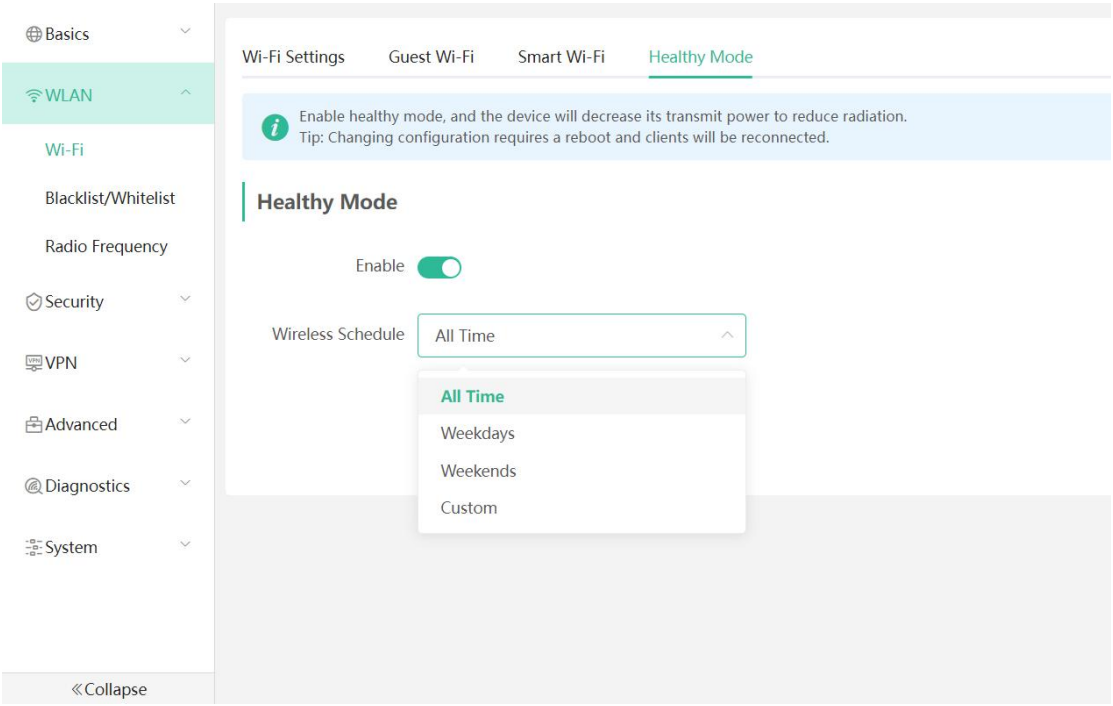
Click **Expand** button to make some advanced settings for smart WiFi, including Wireless Schedule, Hide SSID, AP isolation, Band Steering and Xpress. For Wireless Schedule, you can chose All Time, Weekdays, Weekends and Custom.



d) Healthy Mode

Click **Enable** to enable the healthy mode. You are allowed to set the effective time period for the healthy mode.

After the healthy mode is enabled, the transmit power and the Wi-Fi coverage area will decrease. It is recommended to enable the healthy mode because which can reduce signal strength and cause network stalling.

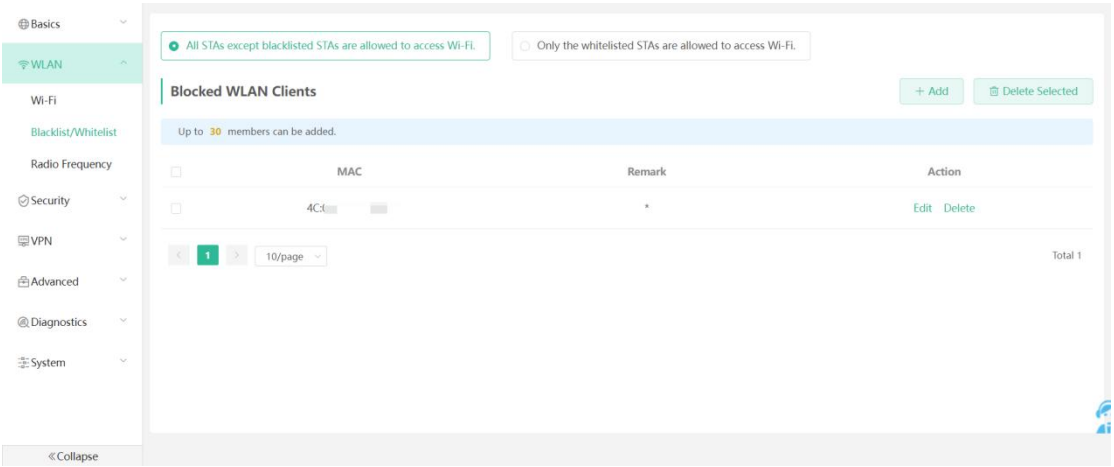


1.2 Blacklist/Whitelist

Wi-Fi blacklist: Clients in the Wi-Fi blacklist are prevented from accessing the Internet. Clients that are not added to the Wi-Fi blacklist are free to access the Internet.

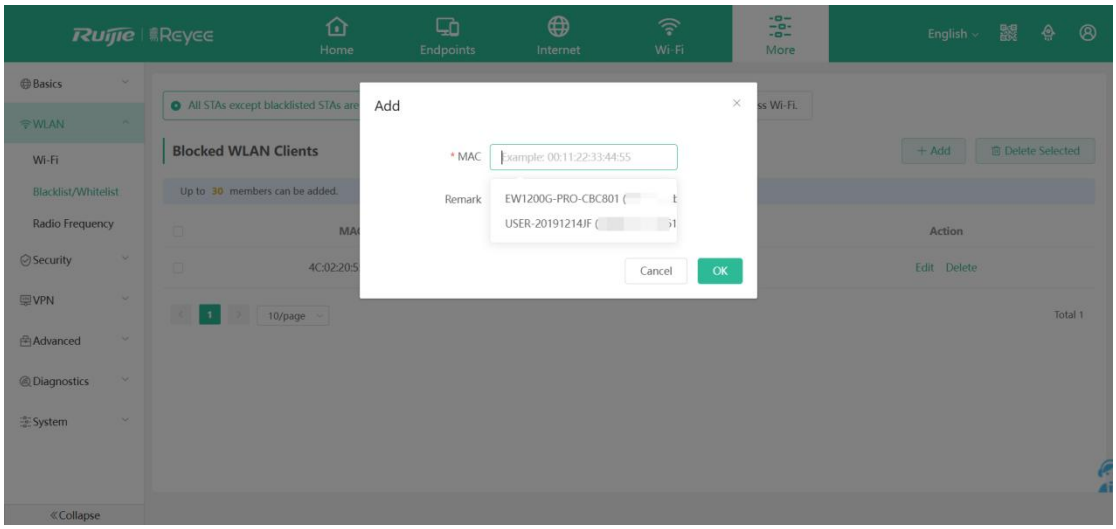
Wi-Fi whitelist: Only clients in the Wi-Fi whitelist can access the Internet. Clients that are not added to the Wi-Fi whitelist are prevented from accessing the Internet.

Choose **More > WLAN > Blacklist/Whitelist.**

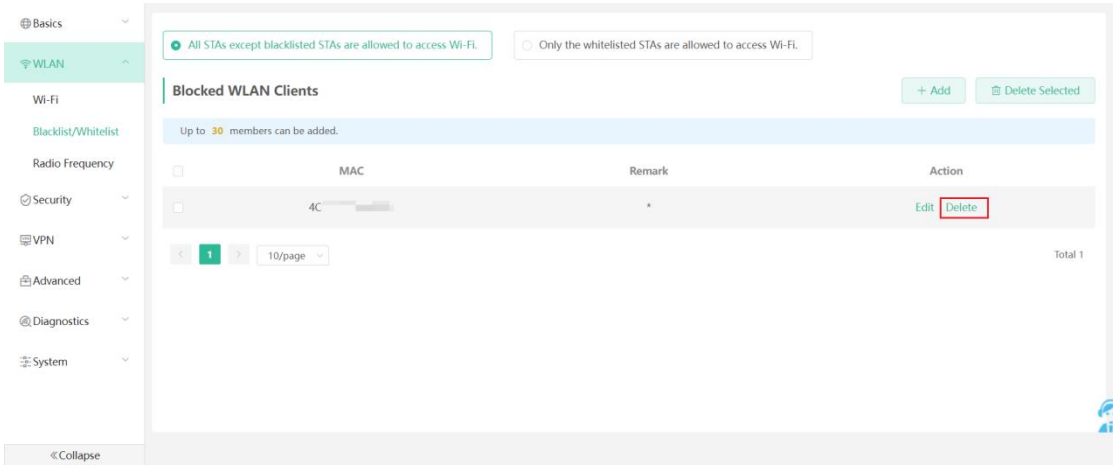


Select the blacklist mode and click **Add**. The default mode is blacklist mode.

In the pop-up dialog box, enter the MAC address and remarks of the client to be blacklisted. The device displays information about the connected clients. Select a client, and it will be added to the blacklist automatically. Click OK to save the configuration. The client will be disconnected and prevented from connecting to the Wi-Fi network.



Click **Delete**. The client can connect to the Wi-Fi network again.

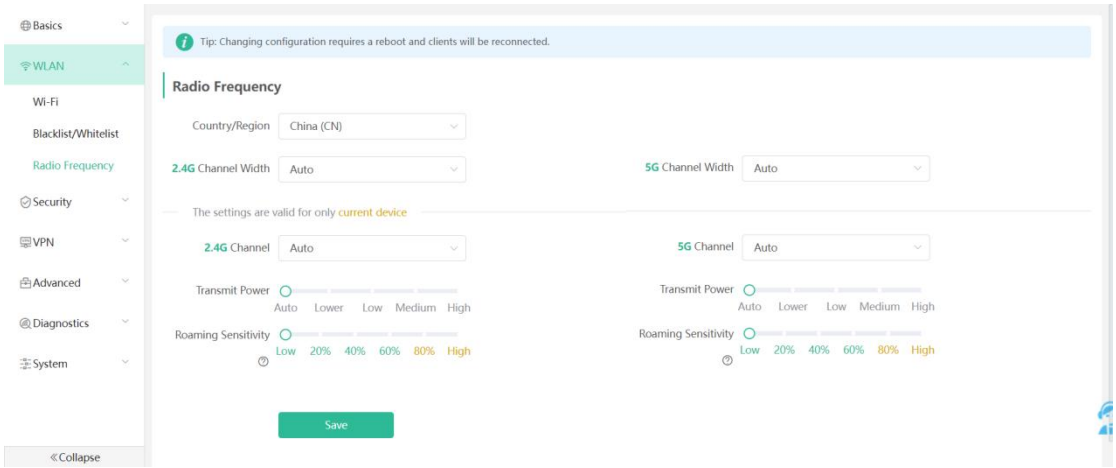


Note:

The steps of adding users into whitelist are same with adding users into blacklist and only clients in whitelist can connect to the Wi-Fi network.

1.3 Radio Frequency

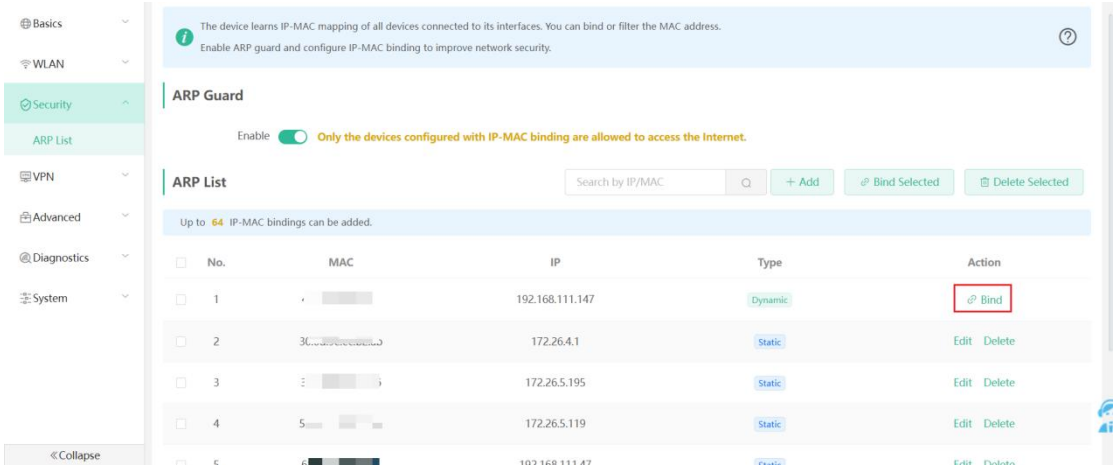
The **Radio Frequency** module allows you to configure Country/Region, channel, channel width, transmit power and roaming sensitivity.



4.5.1.4 Security

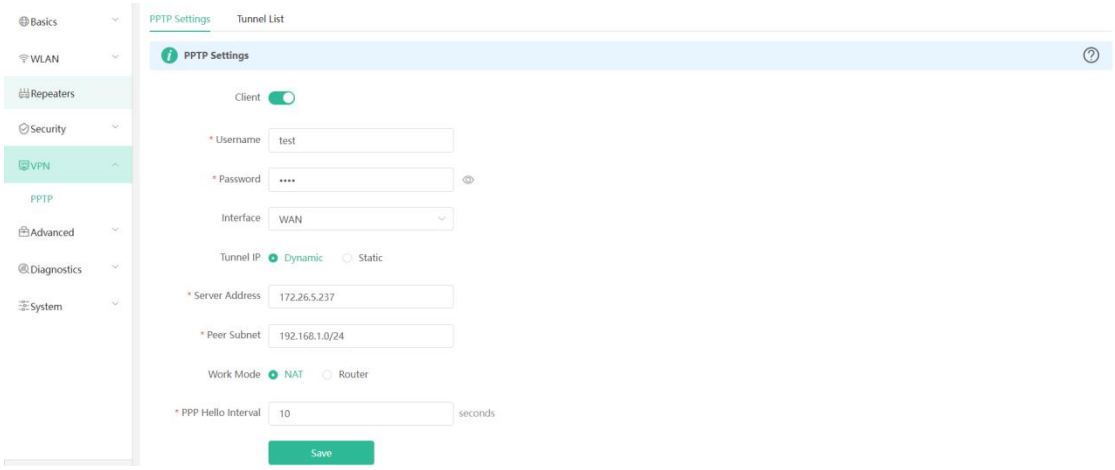
1.1 ARP List

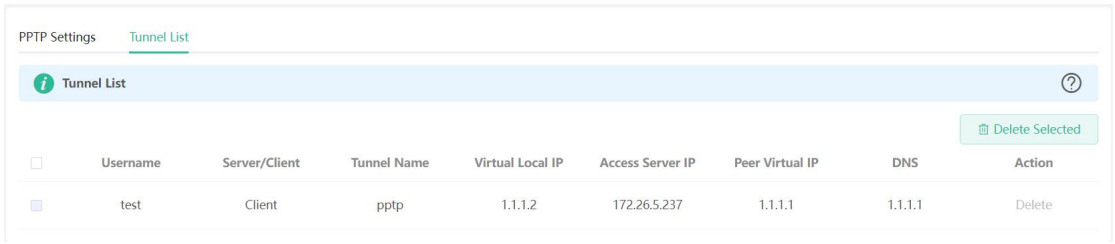
The ARP List page displays ARP entries and supports ARP binding. Click **Bind** to change one user's MAC address and IP address as static-bind, then enable the ARP Guard function, only users with static-bind can access the internet.



4.5.1.5 VPN

The PPTP settings allow you to configure this device as the PPTP clients. After input the correct information including **Username**, **Password**, **Server address** and **peer subnet**, the VPN tunnel will be created and you can see it in the **Tunnel List**.





4.5.1.6 Advanced

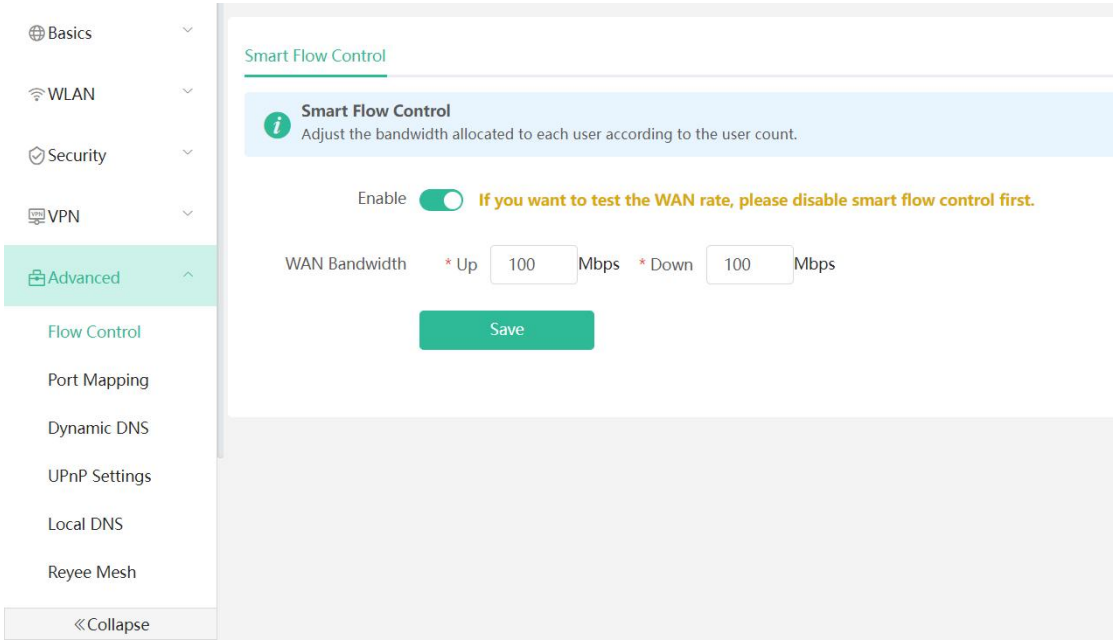
1.1 Flow Control

Choose More > Advanced > Flow Control > Smart Flow Control.

Click Enable and set the network bandwidth provided by the ISP. After the configuration is saved, the router adjusts the bandwidth of each client based on the total bandwidth to prevent any one client from occupying too much bandwidth.

Note:

After flow control is enabled, speed measurement will be affected. Disable flow control if you want to do speed measurement.



1.2 Port Mapping

a) Overview

Port mapping maps the IP address of a device on the LAN to an external network in the form of a combination of a WAN IP address and a port number, so as to provide the external network access service.

1) Scenario 1: When you need to access IP cameras or PCs at home while you are away from home, port mapping needs to be configured.

2) Scenario 2: When a server needs to be set up on the home network for Internet access, port mapping or demilitarized zone (DMZ) needs to be configured.

Port mapping maps the WAN port IP address of a router to an internal network host and port so that Internet users can proactively access hosts on the LAN.

DMZ forwards all packets from the Internet to DMZ hosts to provide the Internet access service.

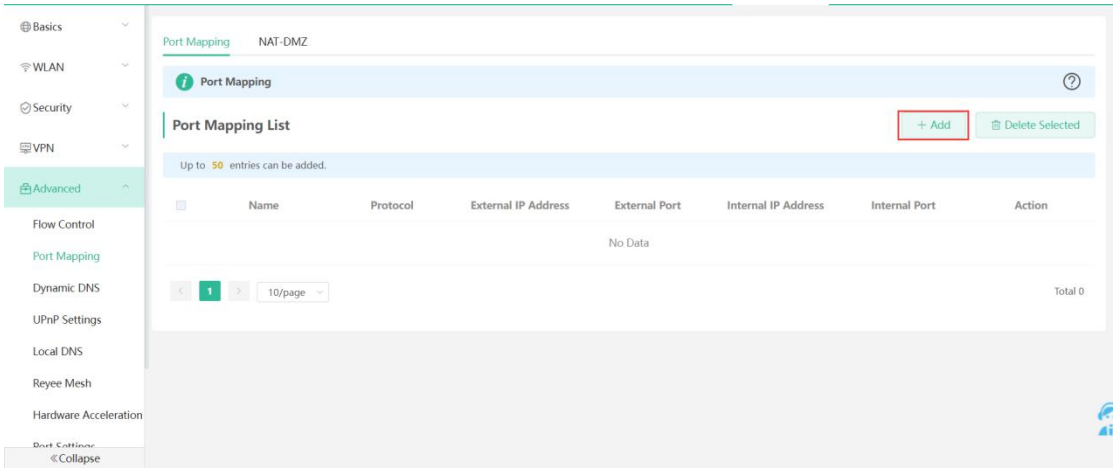
b) Getting Started

1) Confirm the IP address of the target device in the internal network and service port ID.

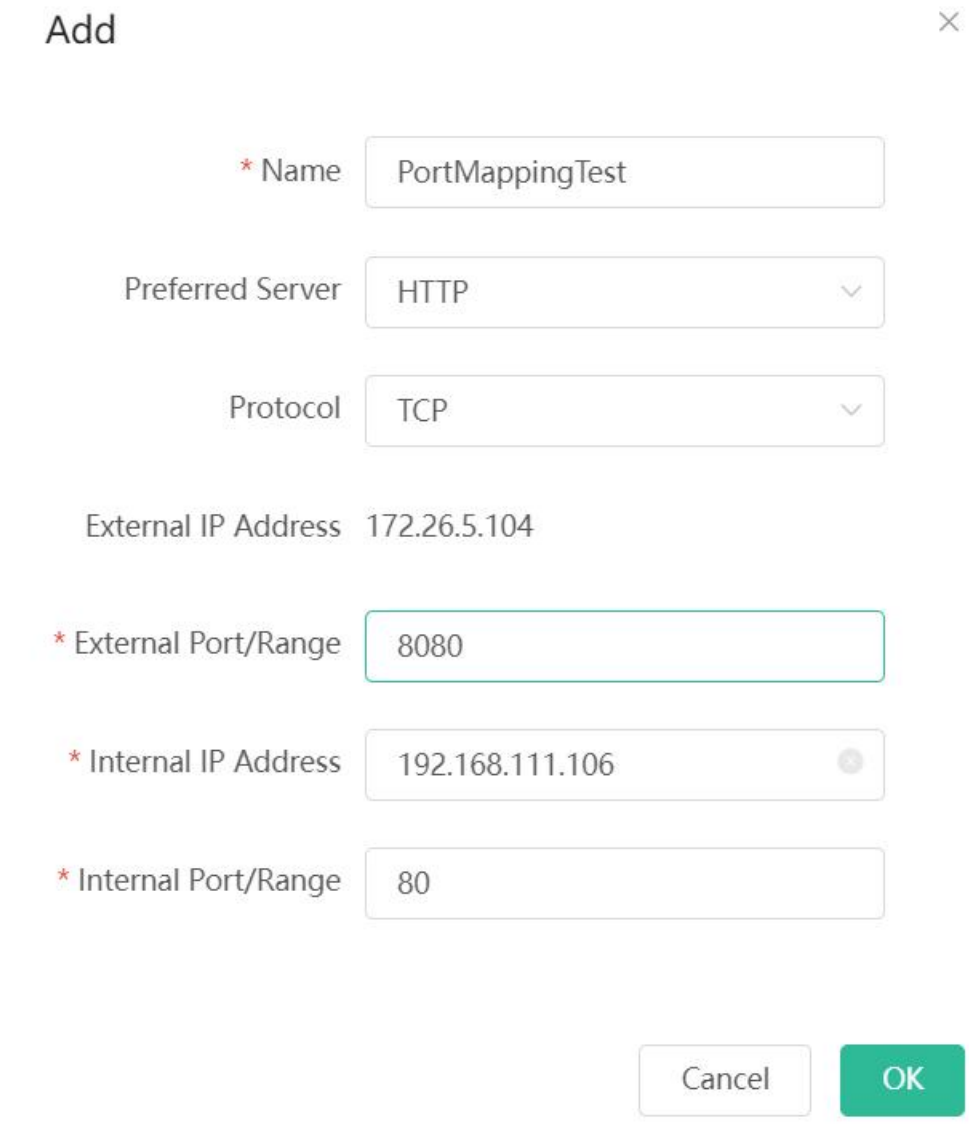
2) Ensure that port mapping is available in the internal network.

c) Configuration Steps

Choose **More > Advanced > Port Mapping.**



Click **Add**. In the pop-up dialog box, enter the name, service type, protocol type, external port/range, internal IP address, and internal port/range. A maximum of 50 port mapping rules can be configured.



Name: Enter a name for easy maintenance.

Preferred Server: Select a service to be mapped, such as HTTP or FTP. The device will automatically fill in the internal port number of the service. If you are not sure of the service, you can select Custom.

Protocol: Select the transport-layer protocol used by the selected service, such as ALL, TCP, or UDP. The configuration on the server end must be consistent with that on the client end.

External Port/Range: Enter the port number used for external network access. You need to check the port number in software, such as camera monitoring software.

Internal IP Address: Enter the LAN IP address used by external networks to access the device, such as the IP address of an IP camera.

Internal Port/Range: Enter the port number used by an application accessed by external networks, such as port 8080 used by the Web service.

d) Verification and Testing

Use an external device to test whether the destination service is accessible based on the external IP address and port number.

e) Solution to a Test Failure

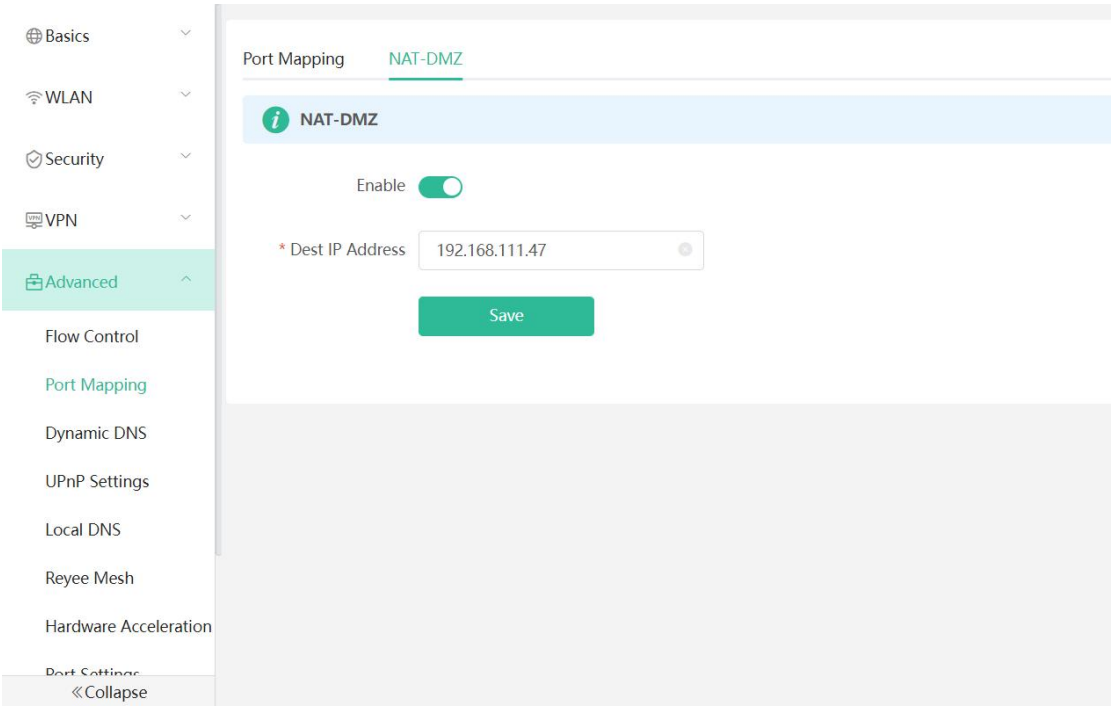
1) Use a new external port number and perform the test again. The test often fails on the ports blocked by firewalls of some ISPs.

2) Enable the remote access permission on the server. The common cause is that remote access is disabled on the server by default. As a result, the internal network access is successful but the access across different network segments is failed.

f) DMZ Configuration Steps

Choose **More > Advanced > Port Mapping > NAT-DMZ**.

Click **Enable**, enter the IP address of the internal server, and click **Save**.



1.3 Dynamic DNS

a) Overview

After the dynamic domain name service (DDNS) is enabled, you can use the fixed domain name on the Internet to access service resources of the router without checking the IP address of the WAN port. To make the service available, you need to register an account and domain name with a third-party DNS service provider. The router supports PeanutHull, Dyn DNS, and No-IP DNS.

b) Getting Started

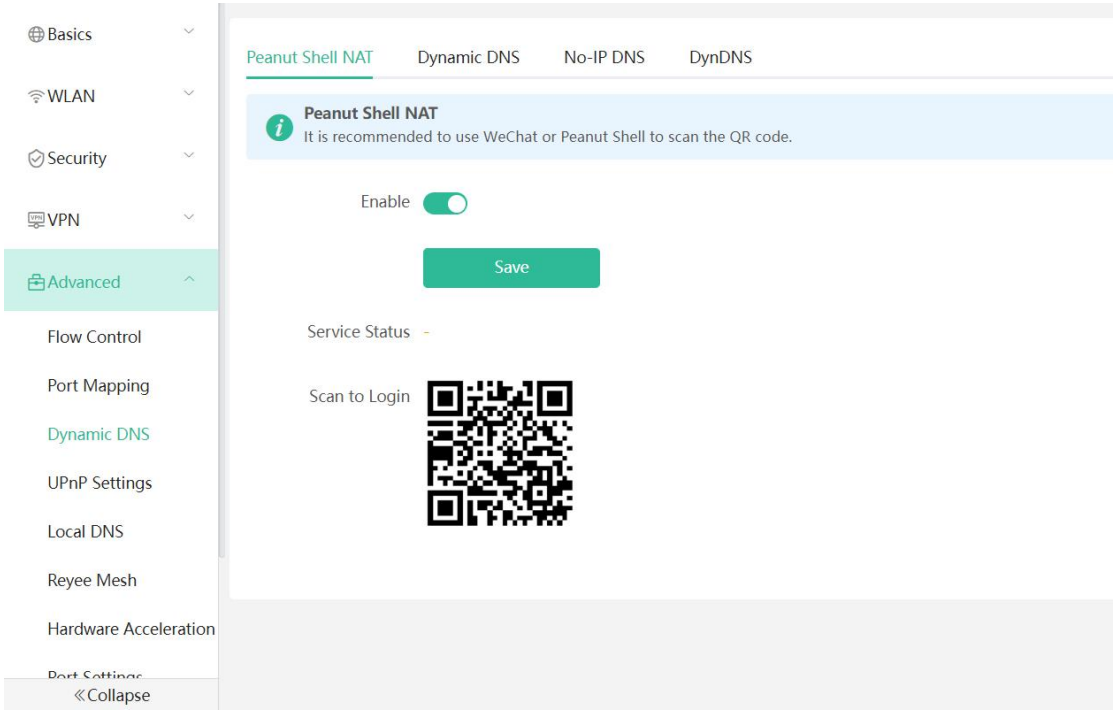
Register an account and domain name at PeanutHull or No-IP official website.

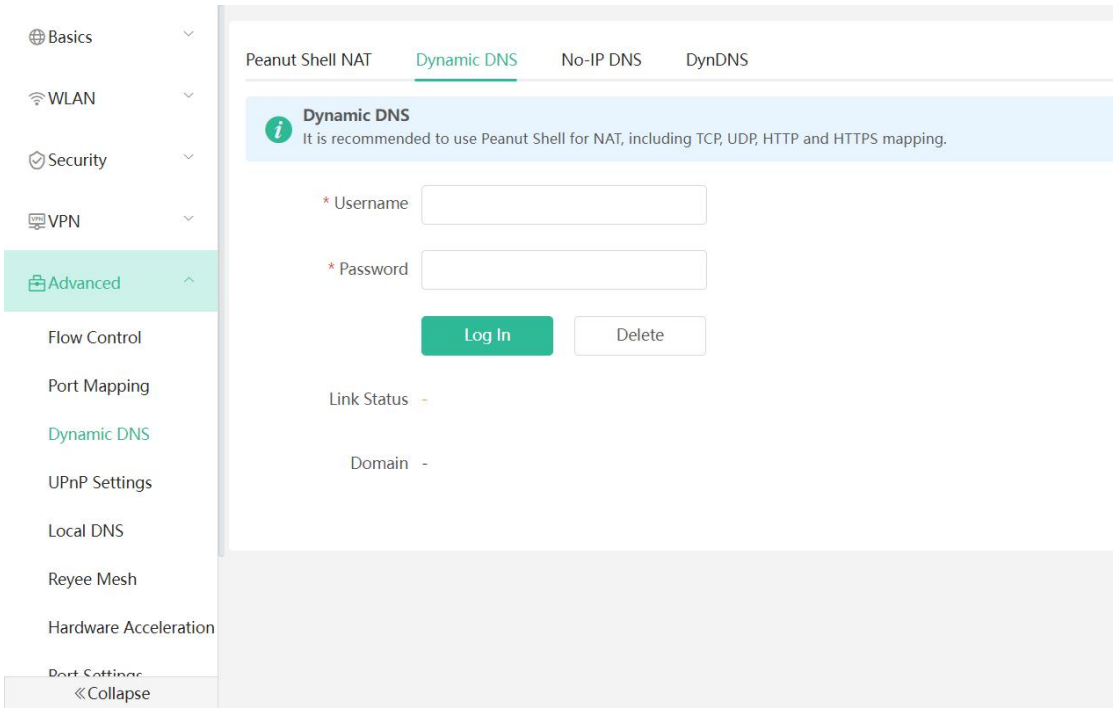
c) Configuration Steps

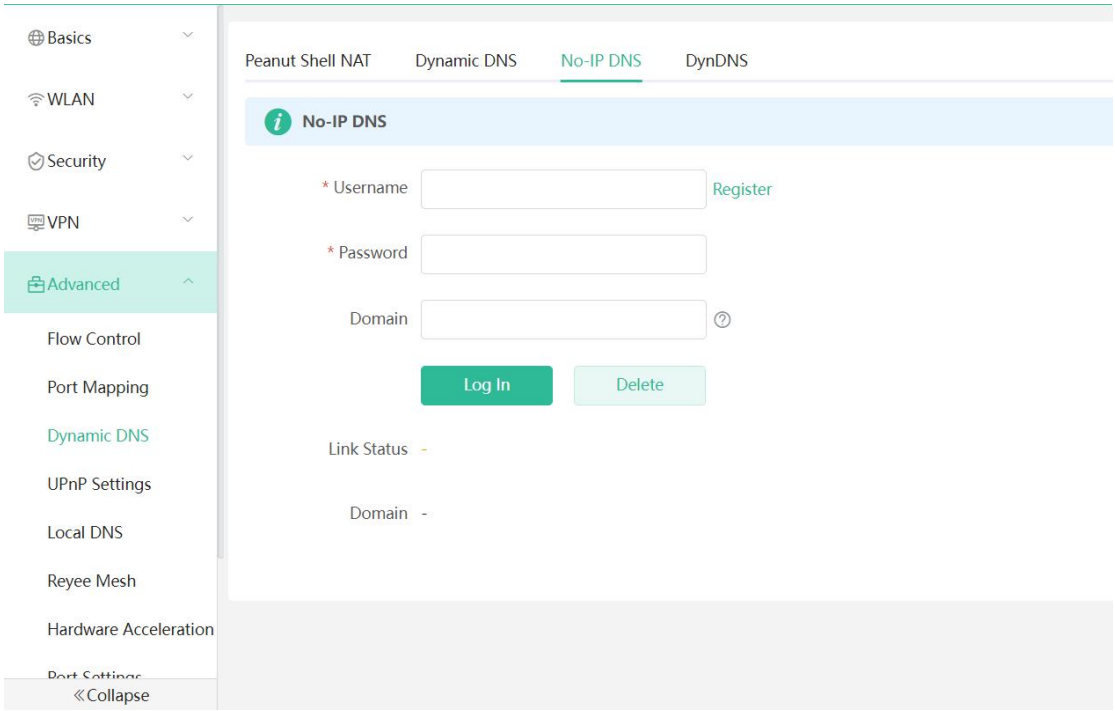
Choose **More > Advanced > Dynamic DNS > Dynamic DNS.**

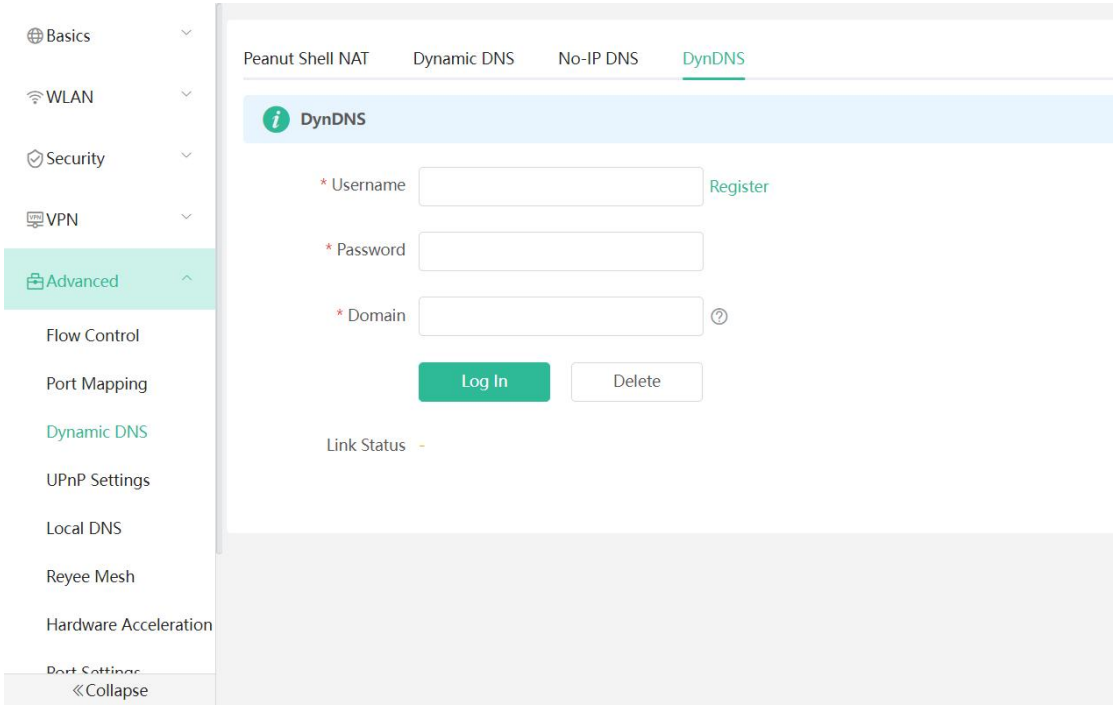
Peanut Shell NAT is a more advanced version of DDNS, which can be used when an internal network IP address is configured for the WAN port. Peanut Shell NAT is recommended. Click Enable and then click Save. The service status and QR code for login appear in the lower part of the page. Scan the QR code to log in by using WeChat or PeanutHull app (the QR code shown in the figure below is not available. Scan the QR code displayed on your device).

If you select Peanut Shell NAT, Dynamic DNS, No-IP DNS, or DynDNS, enter the registered account and password, and click Log In. The connection status and domain name will be displayed in the lower part of the page.




Basics
WLAN
Security
VPN
Advanced
Flow Control
Port Mapping
Dynamic DNS
UPnP Settings
Local DNS
Reyee Mesh
Hardware Acceleration
Collapse
Peanut Shell NAT
Dynamic DNS
No-IP DNS
DynDNS
Dynamic DNS
It is recommended to use Peanut Shell for NAT, including TCP, UDP, HTTP and HTTPS mapping.
* Username
* Password
Log In
Delete
Link Status -
Domain -

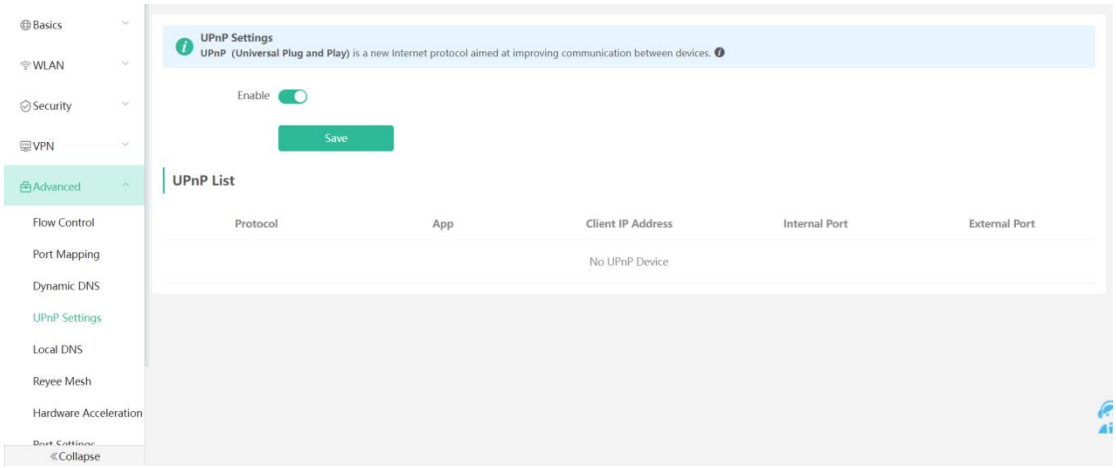

Basics
WLAN
Security
VPN
Advanced
Flow Control
Port Mapping
Dynamic DNS
UPnP Settings
Local DNS
Reyee Mesh
Hardware Acceleration
Collapse
Peanut Shell NAT
Dynamic DNS
No-IP DNS
DynDNS
No-IP DNS
* Username
Register
* Password
Domain
Log In
Delete
Link Status -
Domain -



1.4 UPnP Settings

a) Overview

The universal plug and play (UPnP) function can map the port used by the client for Internet accessing according to the client's request so that related applications run faster or more stably. Common applications that support UPnP include MSN Messenger, Xunlei, BT and PPLive.



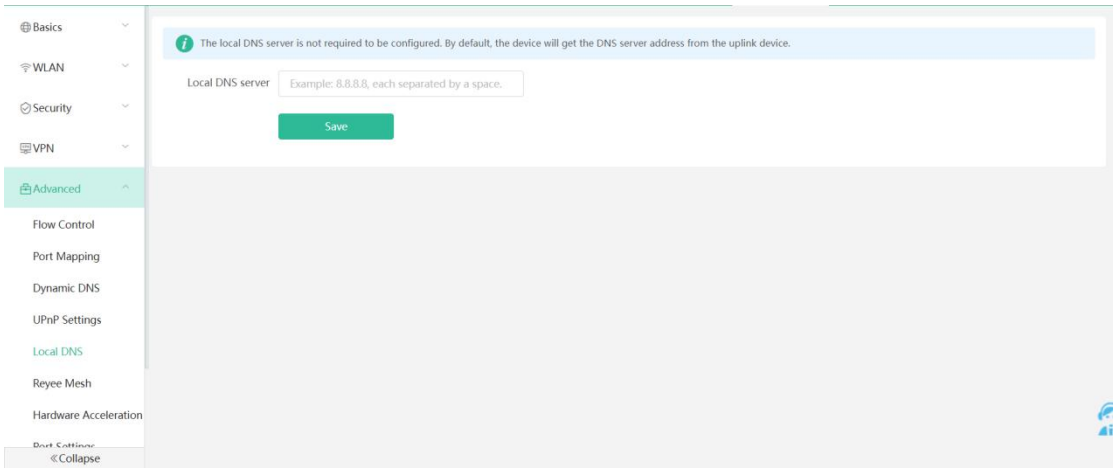
b) Configuration Steps

Choose **More** > **Advanced** > **UPnP Settings.**

Click **Enable**. You are advised to disable the function. Any applications that use UPnP to map ports will be listed below.

1.5 Local DNS

The **Local DNS** module allows you to configure a local DNS server.

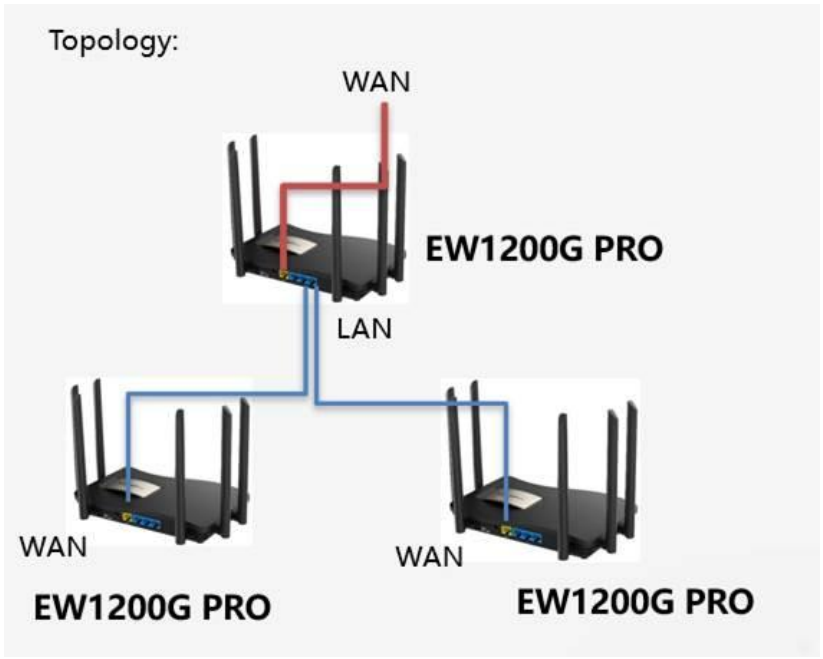


1.5 Reyee Mesh

The Reyee Mesh module allows you to enable the mesh function on this device. After Reyee Mesh is enabled, the new router will join the network automatically when being connected to the LAN port of the device. And then you can press the key for Reyee Mesh pairing. After Reyee Mesh is disabled, the bridged slave router will still be connected.

a) Wired MESH

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).



b) Wireless MESH

1) Master must meet two conditions:

①Finish the quick setup

②The WAN port is connected and the interface indicator is on.

2）Slave must meet two conditions：

①Slave is the factory state;

②Slave 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

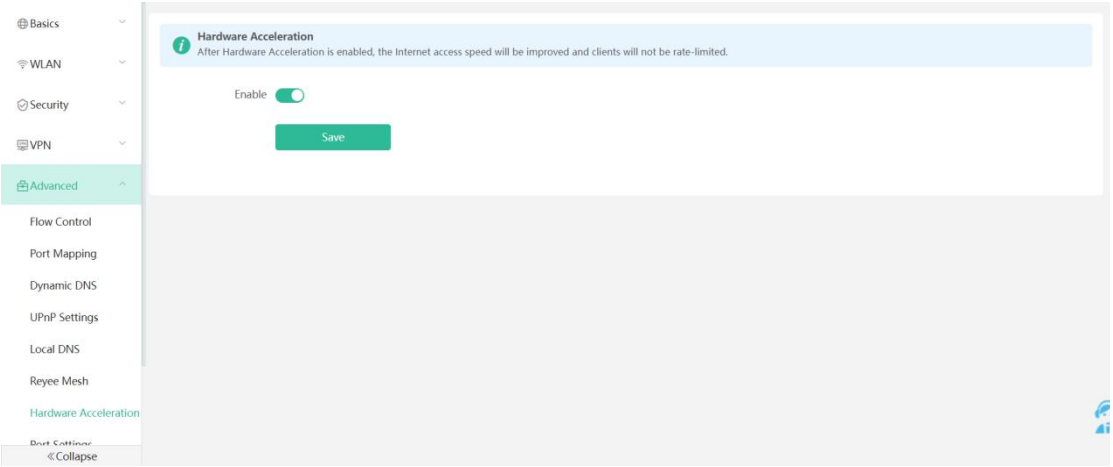
Press the reset button of the master, and the indicator light will flash quickly

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

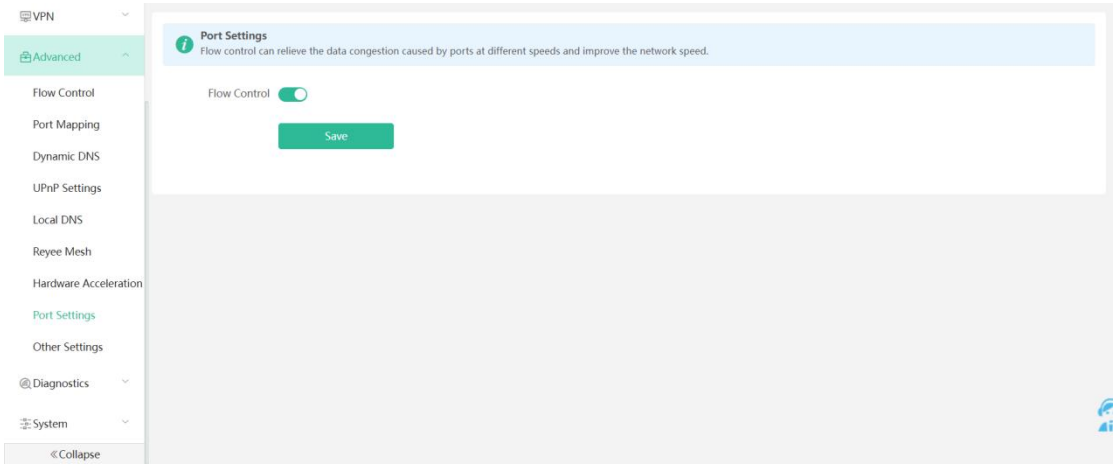
1.6 Hardware Acceleration

The **Hardware Acceleration** module allows you to enable hardware acceleration to improve network speed.



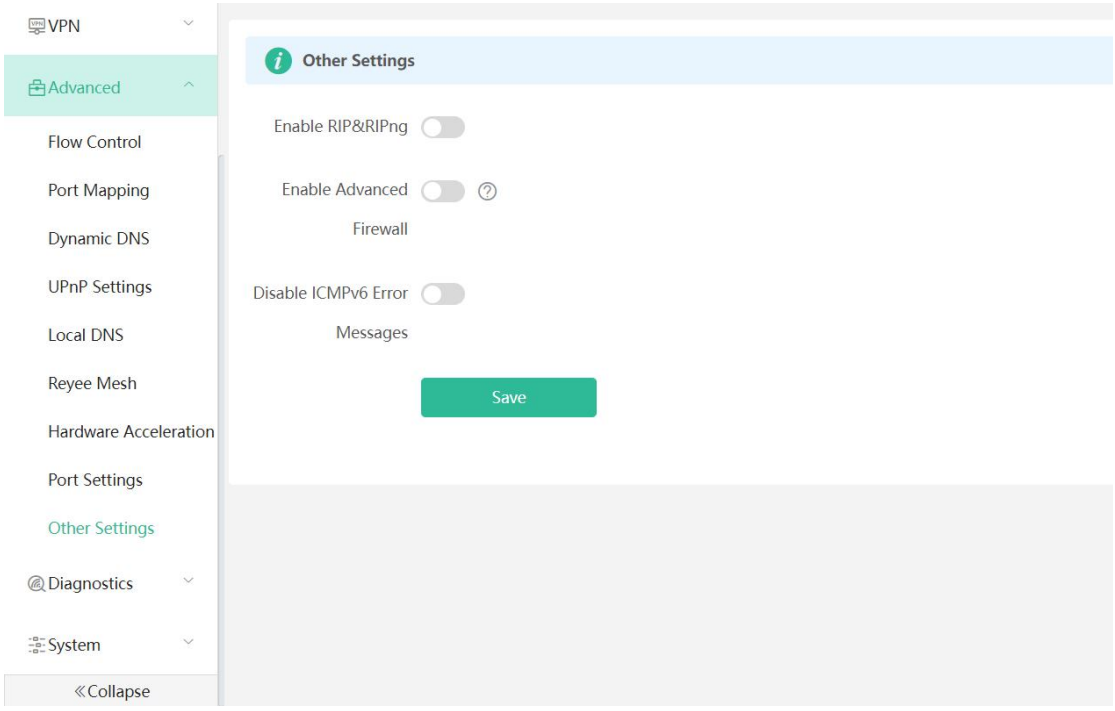
1.7 Port Settings

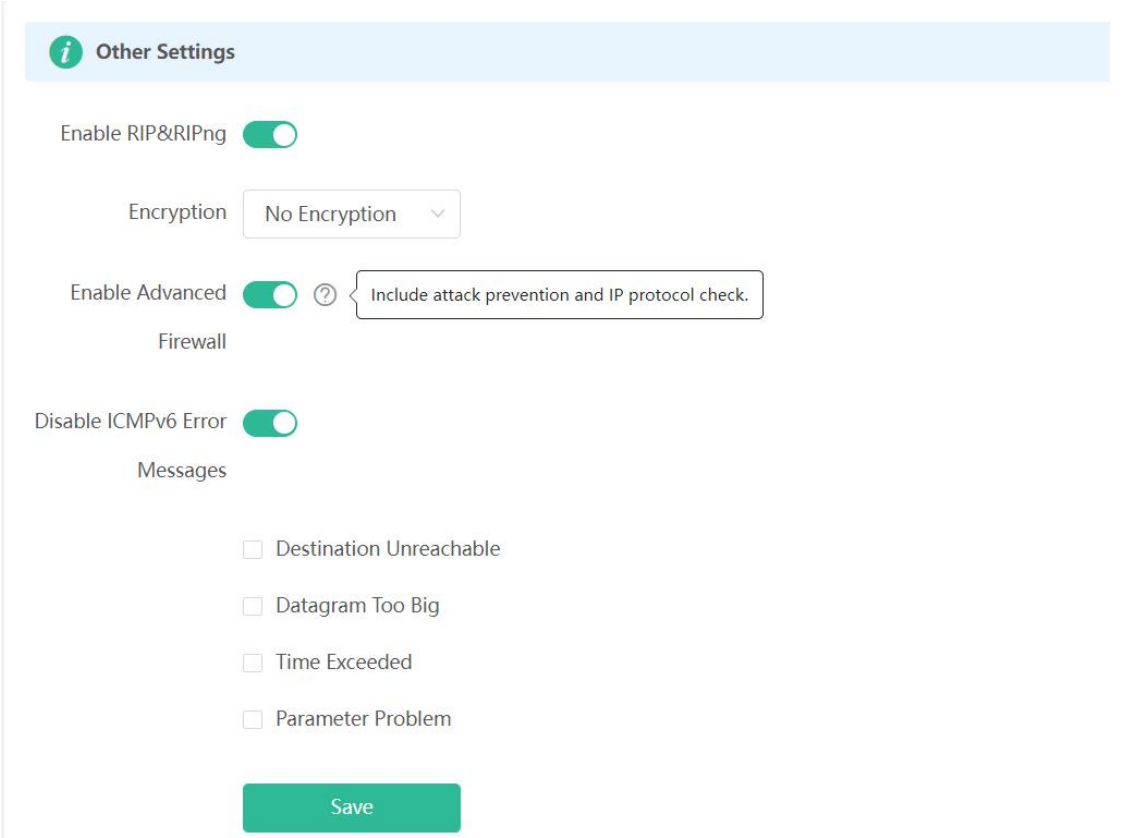
The **Port Settings** module allows you to enable flow control to improve network speed by relieving the data congestion caused by ports at different speeds.



1.8 Other Settings

The **Other Settings** module allows you to enable RIP&RIPng, Advanced Firewall and disable ICMPv6 error message.





RIP&RIPng: including **No Encryption, Plain Text and MD5** three manners.

Enable Advanced Firewall: including attack prevention and IP protocol check.

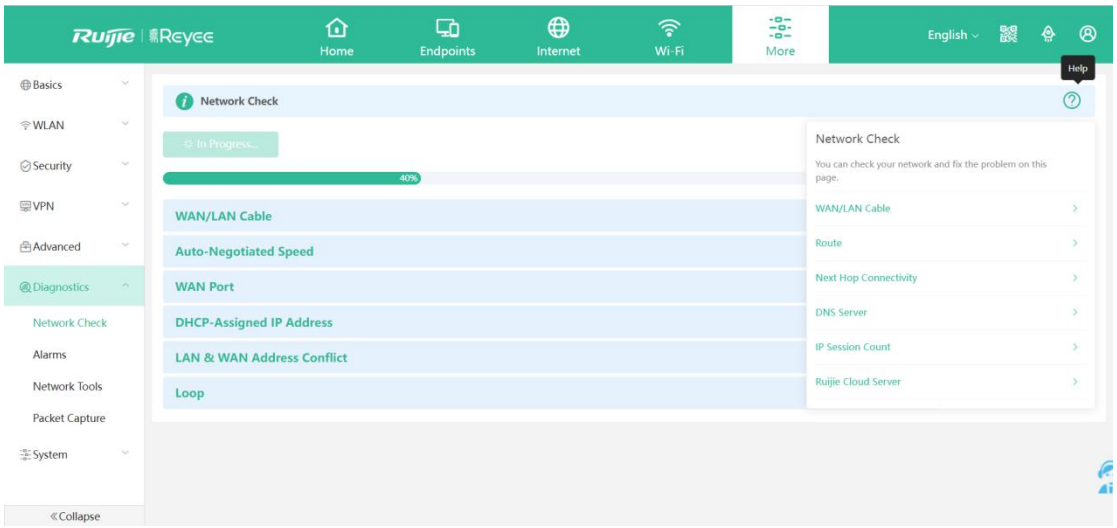
Disable ICMPv6 Error Messages: including **Destination Unreachable, Datagram Too Big, Time Exceeded and Parameter Problem.**

4.5.2 Maintenance

4.5.2.1 Diagnostics

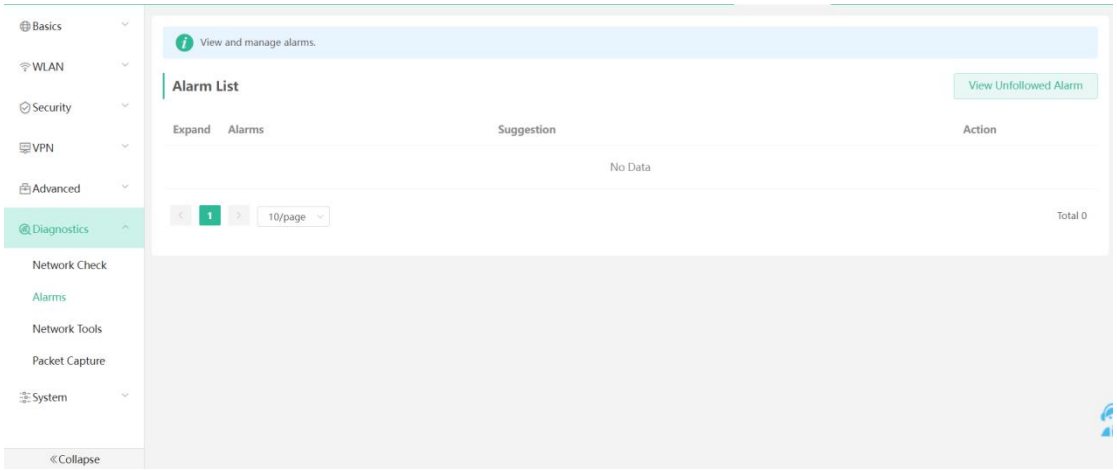
1.1 Network Check

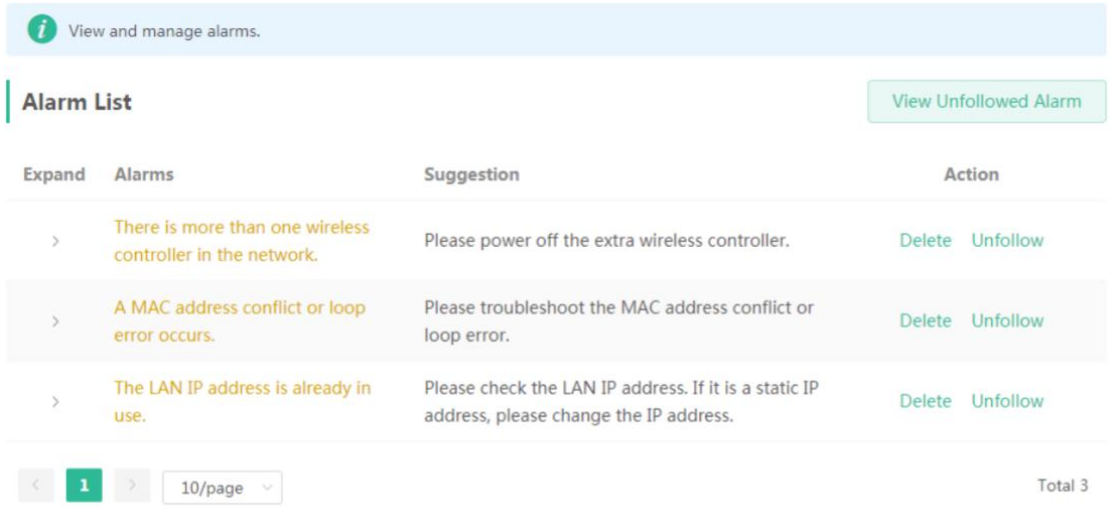
This page allow you to check your network and fix the problem on this page. The checked items include **WAN/LAN Cable, Route, Next Hop Connectivity, DNS Server, IP Session Count** and **Ruijie Cloud Server.**



1.2 Alarms

The **Alarms** module allows you to view and manage alarms in the network.





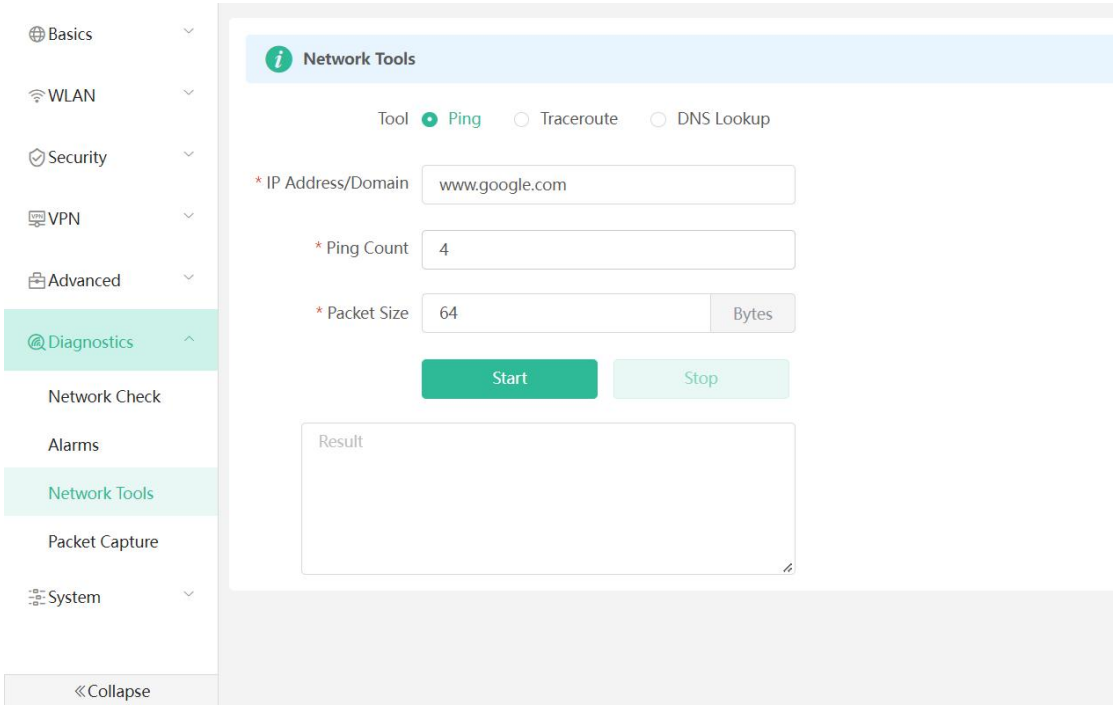
Click **Unfollow** in the **Action** column to unfollow an alarm. In the confirmation box, click **OK**.

1.3 Network Tools

When you select the ping tool, you can enter the IP address or URL and click Start to test the connectivity between the router and the IP address or URL. The message "Ping failed" indicates that the router cannot reach the IP address or URL.

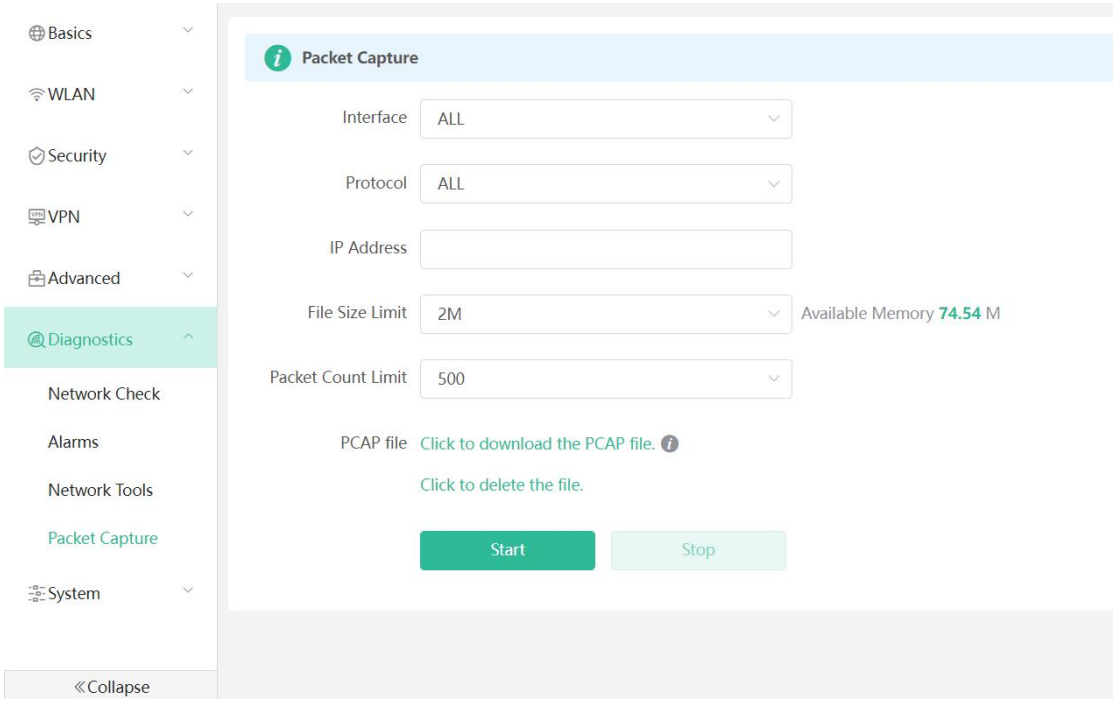
The Traceroute tool displays the network path to a specific IP address or URL.

The DNS Lookup tool displays the DNS server address used to resolve a URL.



1.4 Packet Capture

Set the interface, protocol, and IP address whose packets need to be captured, file size limit, and packet count limit to limit the volume of packets captured. Click **Start**. Packet capture can be stopped at any time and the link to the generated file is generated. You can download this PCAP file and use Wireshark or another analysis software to open the file.



Note:

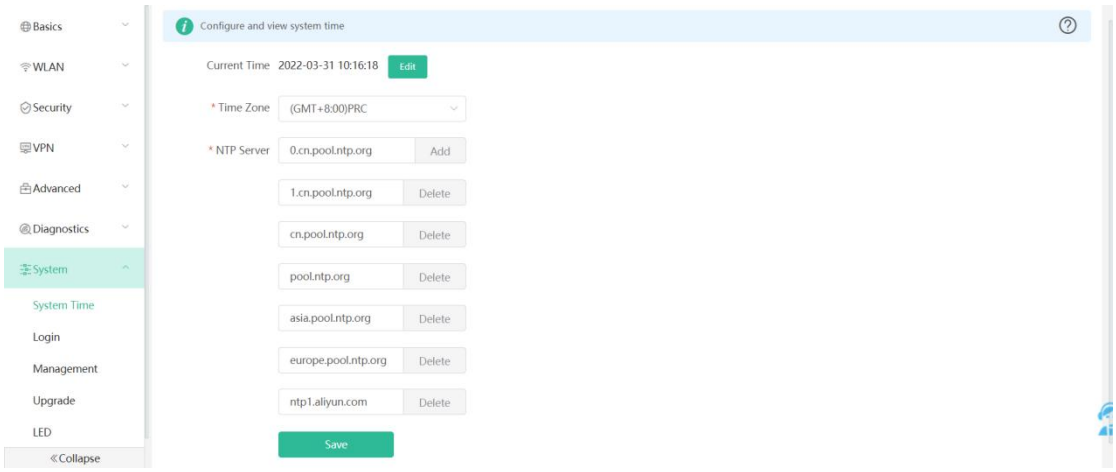
> Note
>
> Packet capture may occupy many system resources and cause network stalling. Exercise caution when performing this operation

.

4.5.2.2 System

1.1 System Time

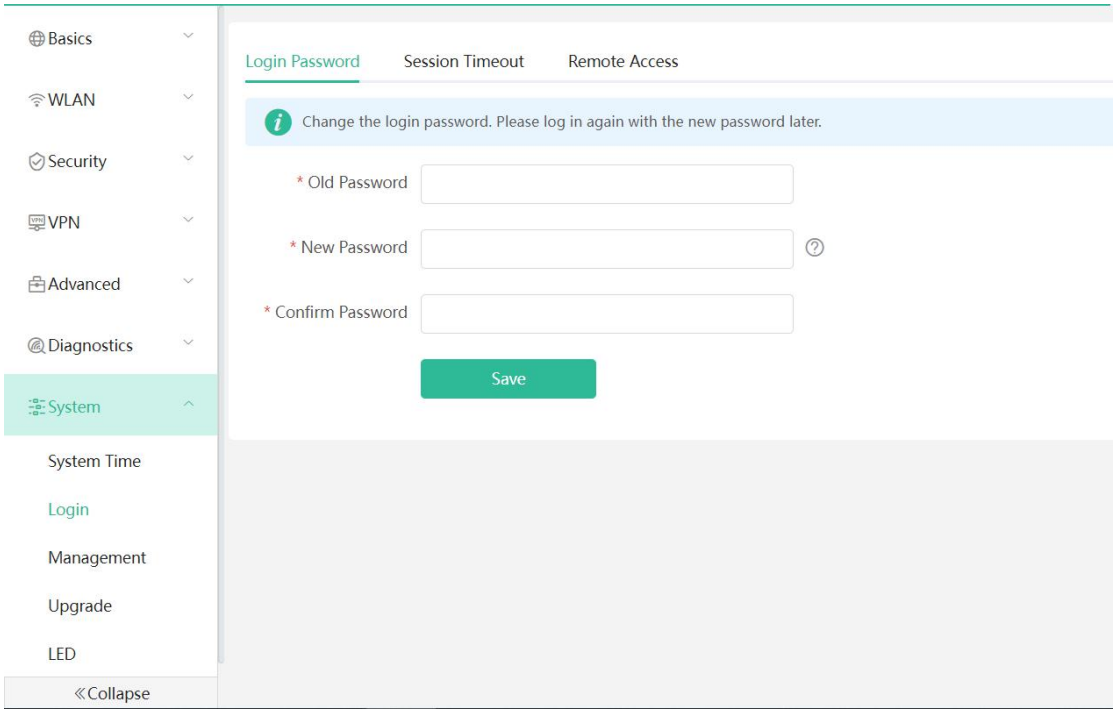
You can view the current system time. If the time is incorrect, check and select the local time zone. If the time zone is correct but time is still incorrect, click **Edit** to manually set the time. In addition, the router supports Network Time Protocol (NTP) servers. By default, multiple servers serve as the backup of each other. You can add or delete local servers as required.



1.2 Login

a) Login Password

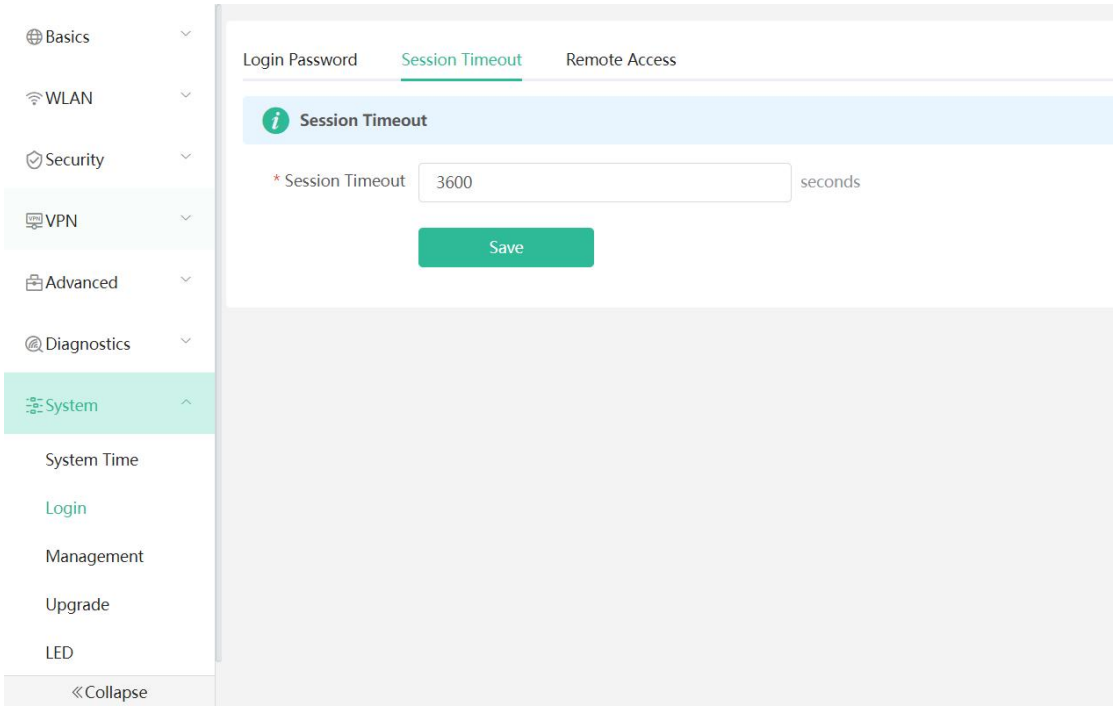
The Login Password module allows you to set the device's login password. You need to log in the system again after changing the password.



b) Session Timeout

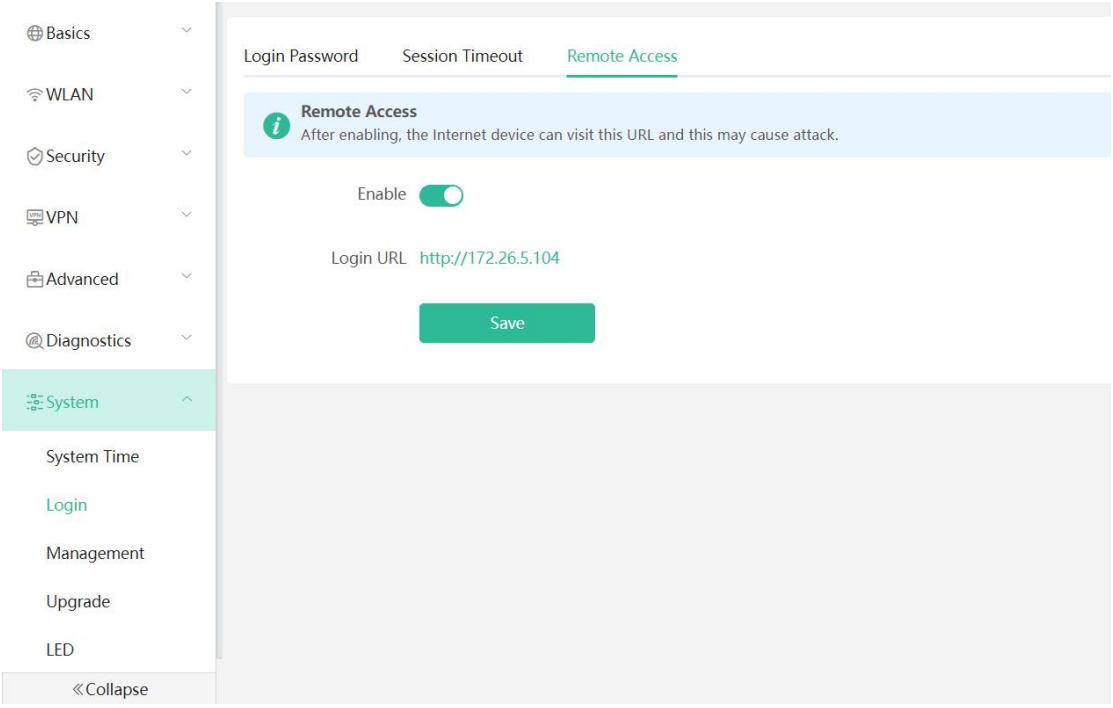
The Session Timeout module allows you to set the session timeout period for loging in the eWeb management system.

If no operation is performed on the page within a period of time, the session will be down. When you need to perform operations again, enter the password to open the configuration page. The default timeout duration is 3600 seconds, that is, 1 hour.



b) Remote Access

After enable the **Remote Access,** the internet device can visit this URL and this may cause attack.



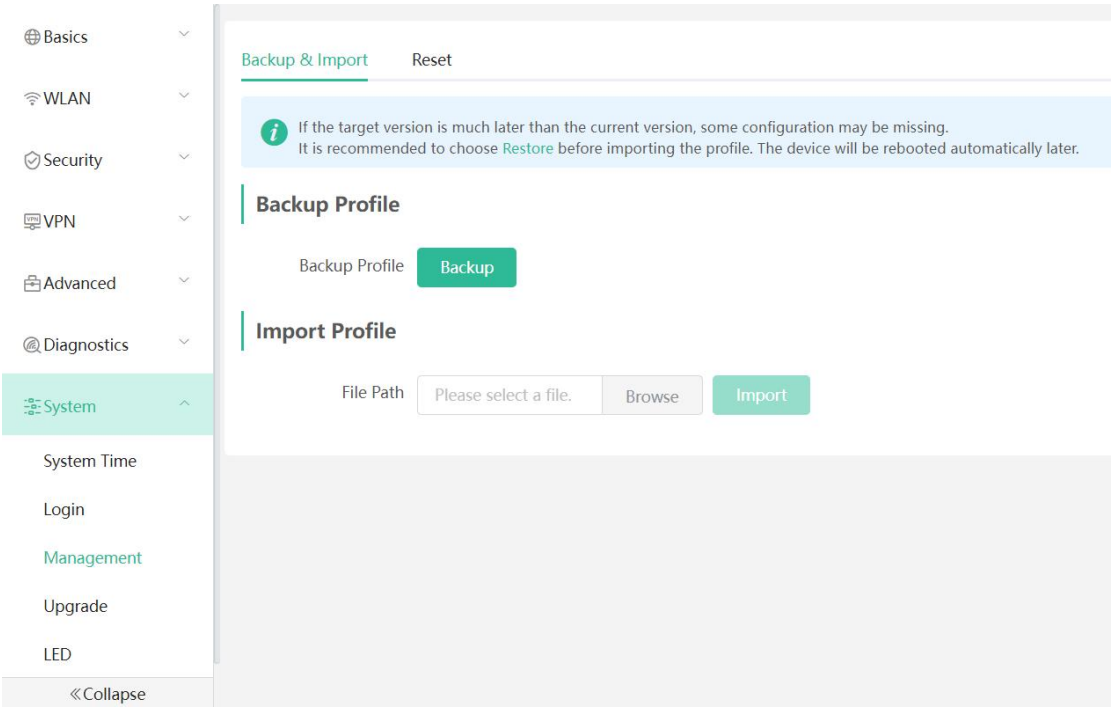
1.3 Management

a) Backup & Import

The Backup & Import module allows you to import a configuration file and apply the imported settings. It can also import the configuration file, and restore the import configuration.

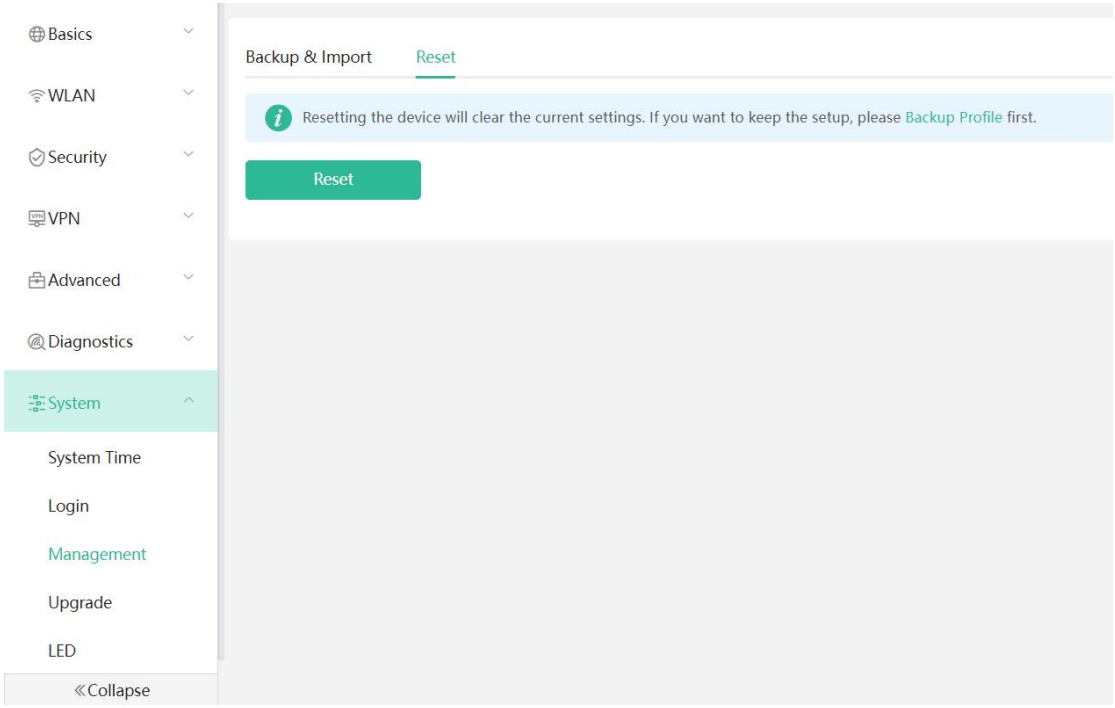
Configure backup: Click **Backup** to download a configuration file locally.

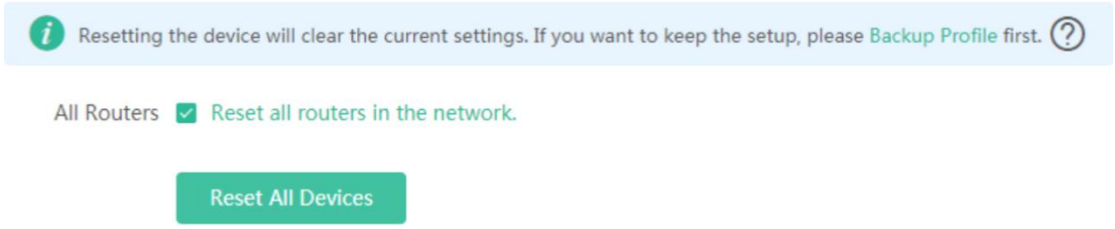
Configure import: Click **Browse**, select a configuration file backup on the local PC, and click Import to import the configuration file. The device will restart.

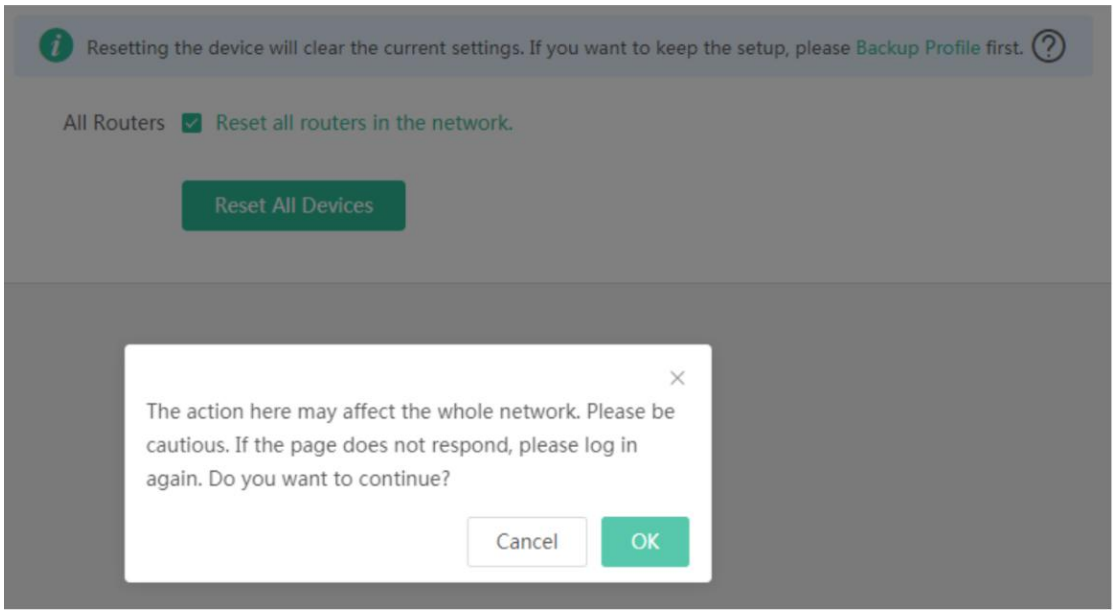


b) Reset

The Reset module allows you to reset the device to factory settings. The module could provides Reset all routers option only when there is a repeater.







Click **OK** to restore all default values. This function is recommended when the network configuration is incorrect or the network environment is changed.

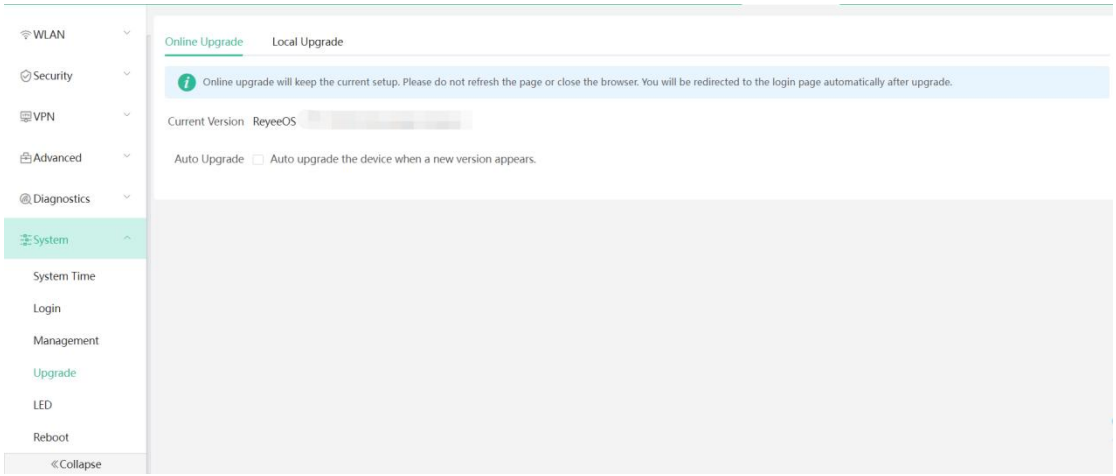
Note

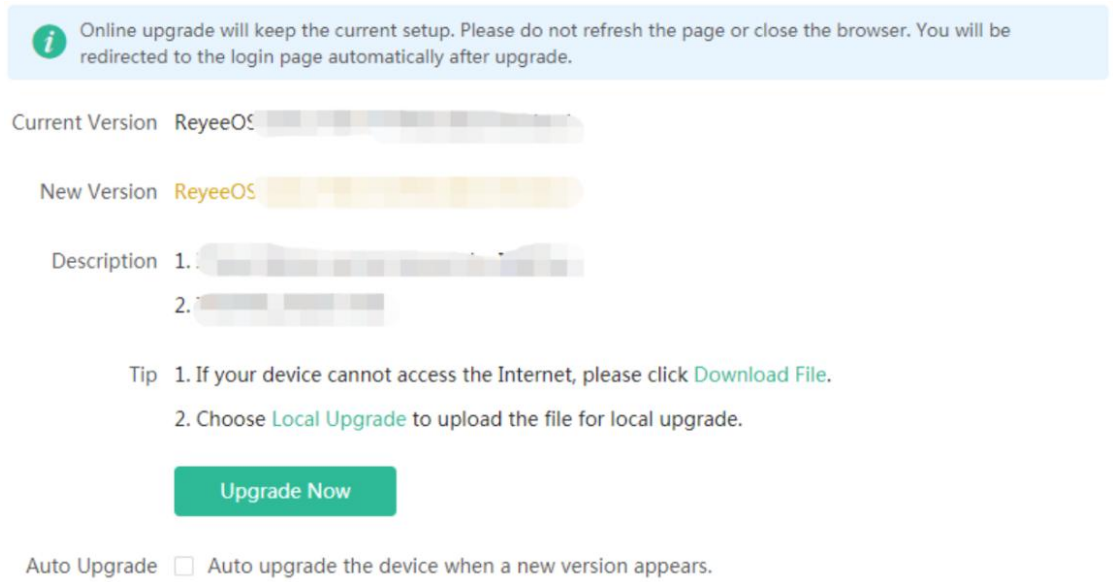
Please exercise caution if you want to restore the factory settings.

1.4 Upgrade

a) Online Upgrade

This page allows you to perform online upgrade. If any upgradeable “online version” is available in the network, information of the upradable version will be displayed in this page.





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

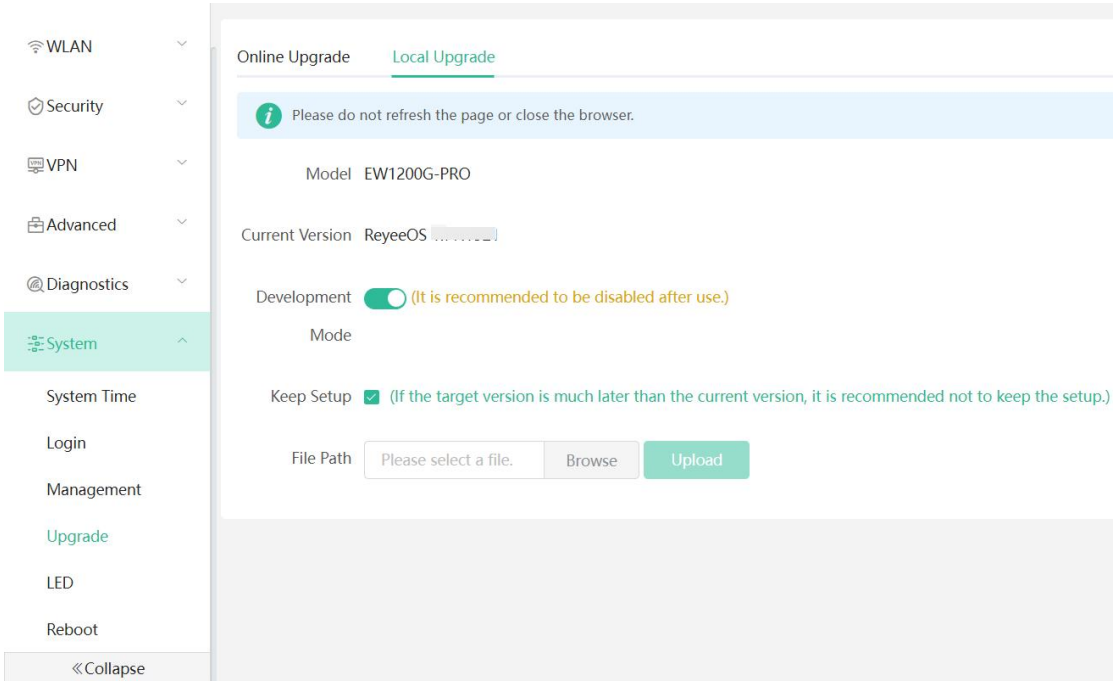
Note:

After being updated, the device will restart. Therefore, exercise caution when performing this operation. You are advised to set the scheduled update time to an early morning time to avoid affecting Internet access.

If no version update is detected and online upgrade cannot be performed, check whether the DNS is correctly obtained or go to **More > Advanced > Local DNS** to set the DNS server for the router.

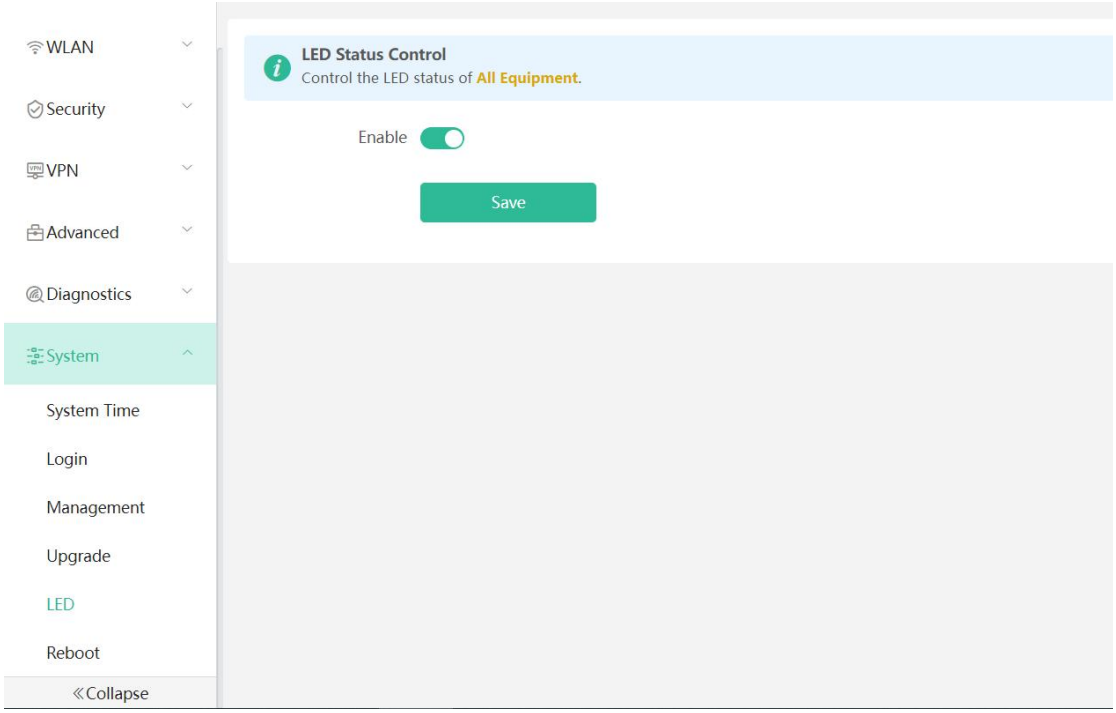
b) Local Upgrade

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



1.5 LED

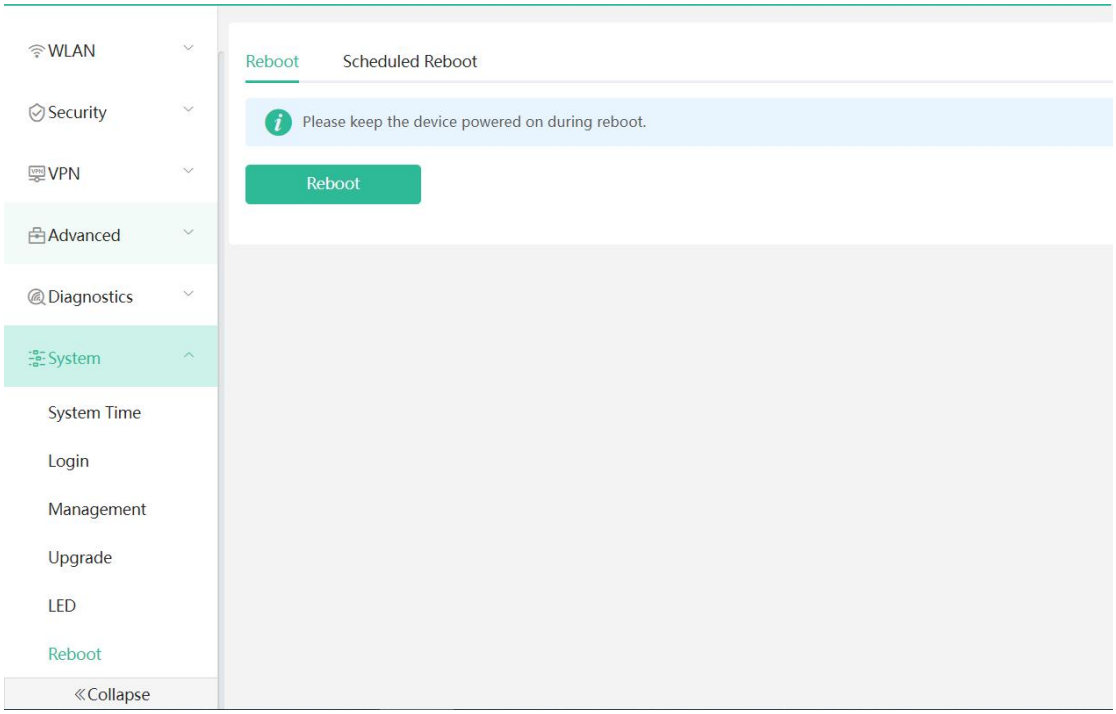
The **LED** module allows you to enable LED.

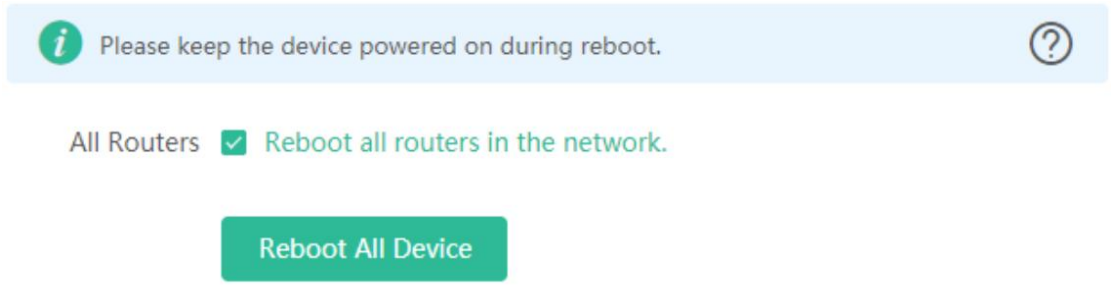


1.6 Reboot

a) Reboot

The Reboot module allows you to reboot the device immediately. The module provides the Reset all routers option only when there is any repeater.

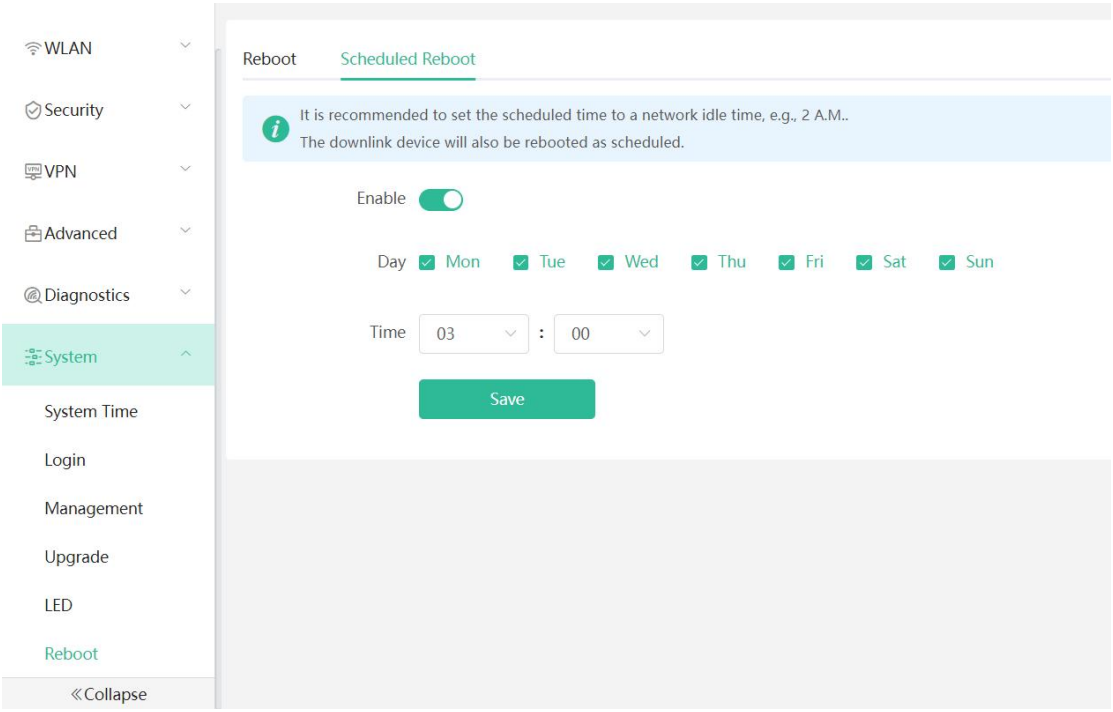




Click **Reboot,** and click **OK** in the confirmation box. The device is rebooted and you need to log in the eWeb management system again after reboot. Do not refresh the page or close the browser during the reboot. After the device is successfully rebooted and the eWeb service becomes available, you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

b) Scheduled Reboot

The **Scheduled Reboot** module allows you to reboot the device at a scheduled time.



Enable the scheduled reboot, select the time and click **Save.**

4.6 Reyee Wireless Bridge Configuration

4.6.1 Installing the Device

4.6.1.1 Installation Tools

Tools	Marker, Phillips (crosshead) screwdriver, slotted screwdriver, drill, paper knife, crimping pliers, diagonal pliers, wire stripper, network cable tester, related power and fiber cables, wrench, hammer, hose clamp, ESD tools, multimeter.

4.6.1.2 Before installation

Before you install the device, verify that all the parts in the parts list are there and make sure that:

The installation site meets temperature and humidity requirements.

The installation site is equipped with a proper power supply.

Network cables are in place.

4.6.1.3 Precautions

The device can be mounted on a wall and a pole (diameter: 35 mm to 89 mm). If the diameter of the pole is out of the range, the hose clamp should be prepared by customers themselves. In this case, we recommend you to use a hose clamp with thickness of 2.5mm at least. Otherwise, the device could fall down to cause injuries. When multiple bridges are installed at a close range, in order to avoid interference between bridges, the horizontal distance between two bridges should be 2m and the vertical distance be 0.5m, or the horizontal angle of the two bridges should be greater than 120 degrees. The installation site can vary due to on-the-spot surveys conducted by technical personnel.

1) Before connecting the power supply, please use the PoE adapter shipped with the device or use a PoE adapter with the same specification.

2) Before connecting the power cord, make sure the power switch is in the OFF position.

3) Make sure the power supply is properly connected

4.6.1.4 Installing Device

1.1 Wall Mounting (connected to cable in advance)

1) Secure the mounting bracket on the wall.

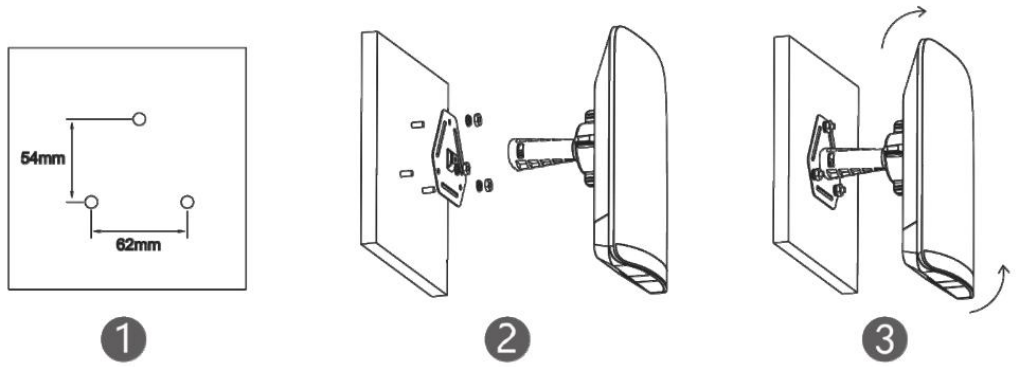
2) Install the device to the mounting bracket.

Here are the detailed steps:

a) Drill holes into the marked positions and insert wall anchors. The head of the wall anchor should be at least 10 mm above the wall surface.

b) Assemble the mounting kit.

c) Adjust the orientation.



1.2 Pole Mounting

1) Secure the mounting bracket to the pole by threading a clamp through the mounting bracket.

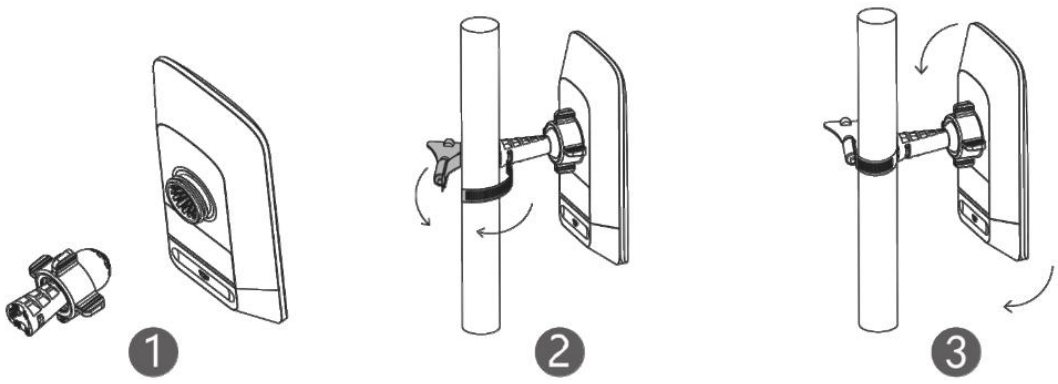
2) Install the device to the mounting bracket.

Here are the detailed steps:

a) Assemble the mounting kit.

b) Secure the device on a pole by using a hose clamp.

c) Adjust the orientation.



4.6.2 Login device

4.6.2.1 Power the device

Plug one end of the cable into the PoE port of the PoE injector and plug the other end into the LAN port of the device. Connect the LAN port of the PoE injector to the server or camera. Connect the PoE adapter to the DC port of the PoE injector. Or you can connect the PoE adapter to the DC port of the device. Plug one end of the cable to the LAN port of the device and plug the other end to the server or camera

4.6.2.2 Choose the EST's SSID

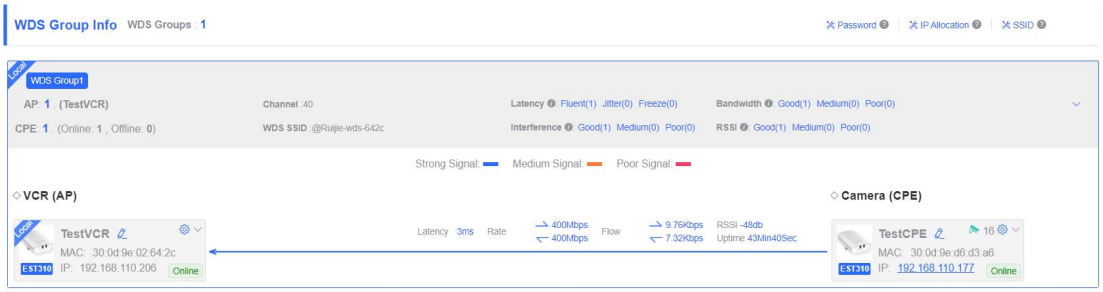
The default device management service set identifier (SSID) is @Ruijie-bXXXX. (XXXX is the last four digits of the MAC address of each device, and the default management SSID varies with devices.

4.6.2.3 Login

Input 10.44.77.154 on the browser to login the web page.

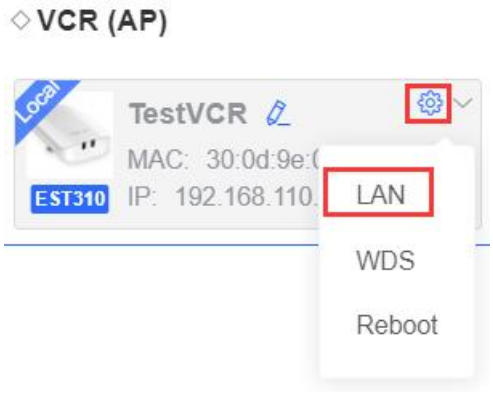
4.6.3 Overview

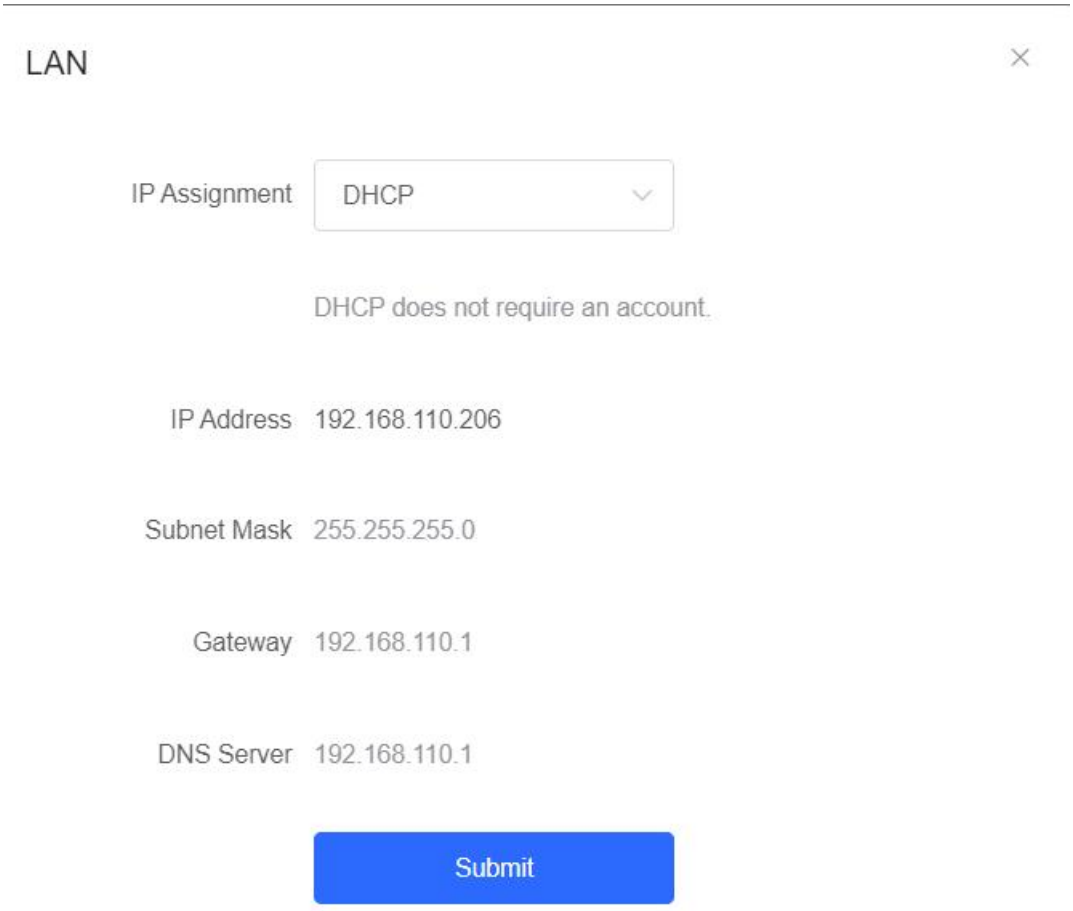
4.6.3.1 Setting the Address of a LAN Port for a Single Online Bridge

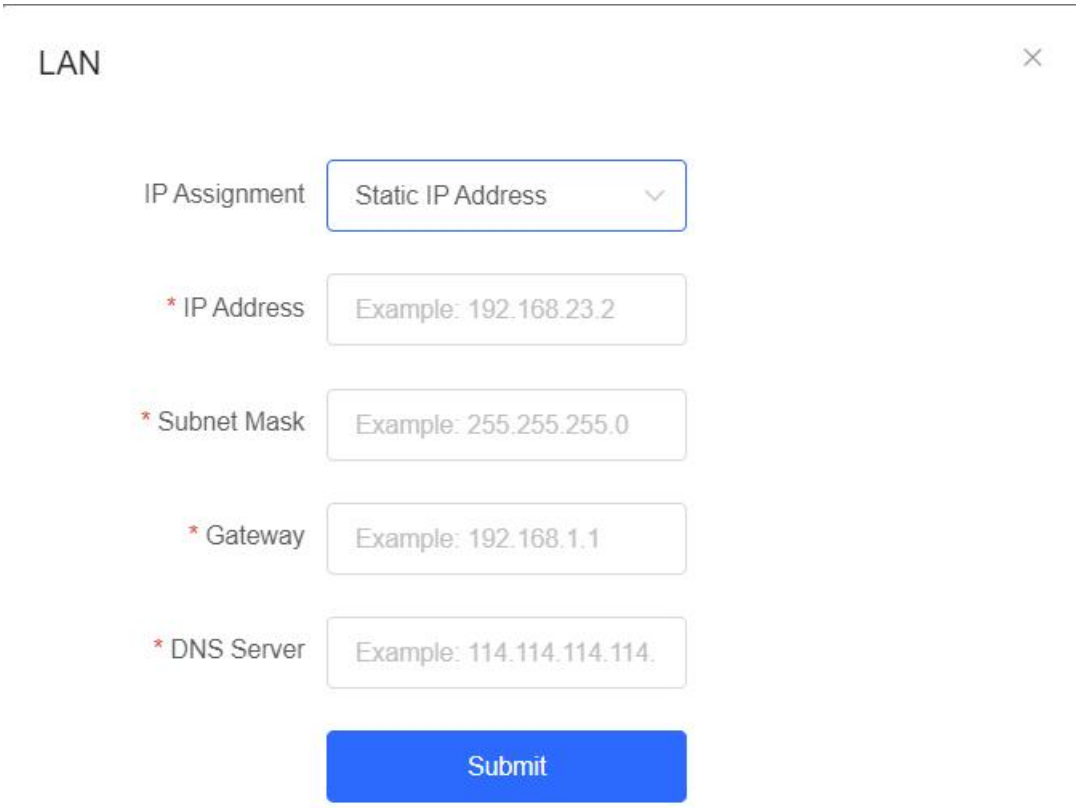


Choose **Overview > WDS Group Info > NVR (AP)/Camera (CPE).**

To set the IP address for a single device, click, and select LAN from the drop-down list. The type of IP assignment includes DHCP and static IP address




LAN
IP Assignment
DHCP
DHCP does not require an account.
IP Address
192.168.110.206
Subnet Mask
255.255.255.0
Gateway
192.168.110.1
DNS Server
192.168.110.1
Submit



Note:

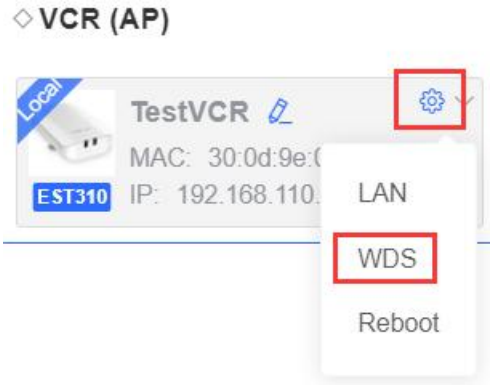
After the IP address and subnet mask are changed, the device web page may not be accessed. You need to enter a new IP address in the browser address bar and ensure that the IP addresses of the management computer and the device are in the same network segment. If they are not in the same network segment, reconfigure the IP address of the management computer.

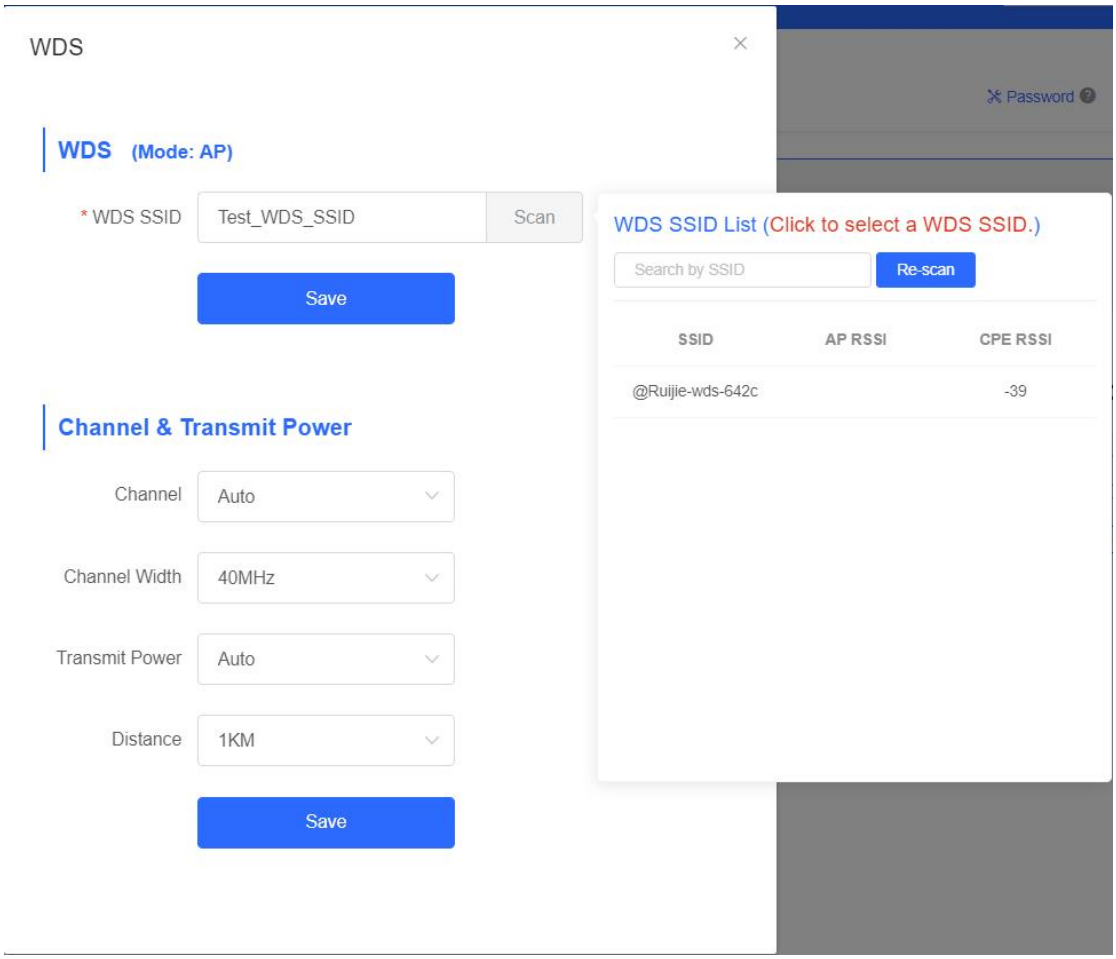
4.6.3.2 Setting the WDS SSID

Choose **Overview > WDS Group Info > NVR (AP)/Camera (CPE).**

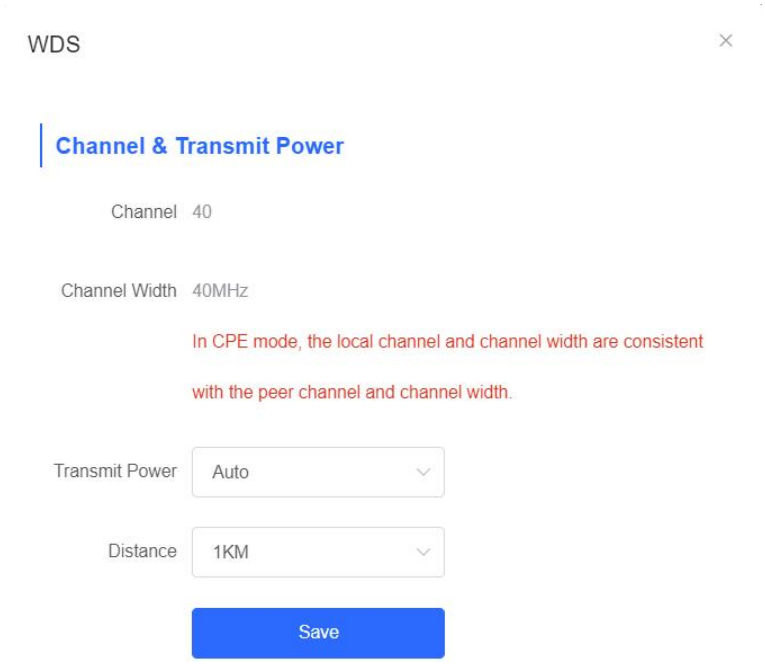
To set the WDS SSID for one bridge, click, and select WDS from the drop-down list.

In AP mode, it supports customize the WDS SSID and chose the SSID from ESTs in the scan list as the WDS SSID. You are allowed to configure the 5G channel, channel width, transmit power and distance for this WDS SSID.





In CPE mode, the local channel and channel width are consistent with the peer channel and channel width. You are only allowed to configure the transmit power and distance.



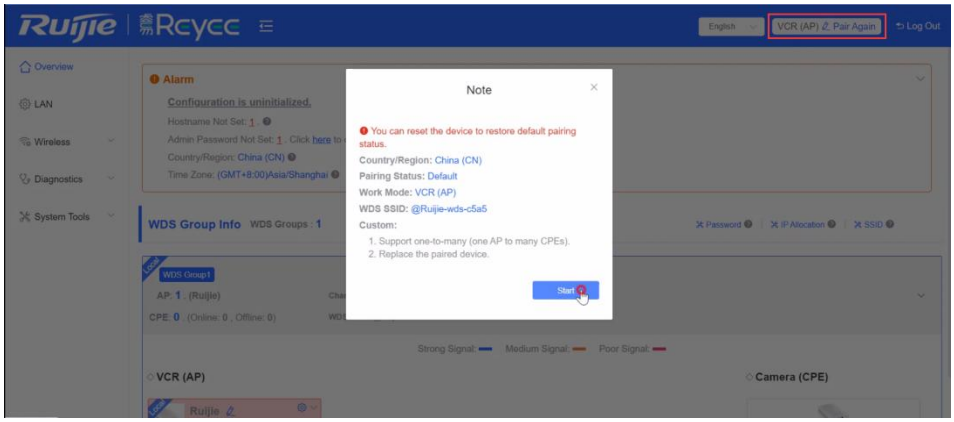
4.6.3.3 Point To Multiple Point (PTMP)

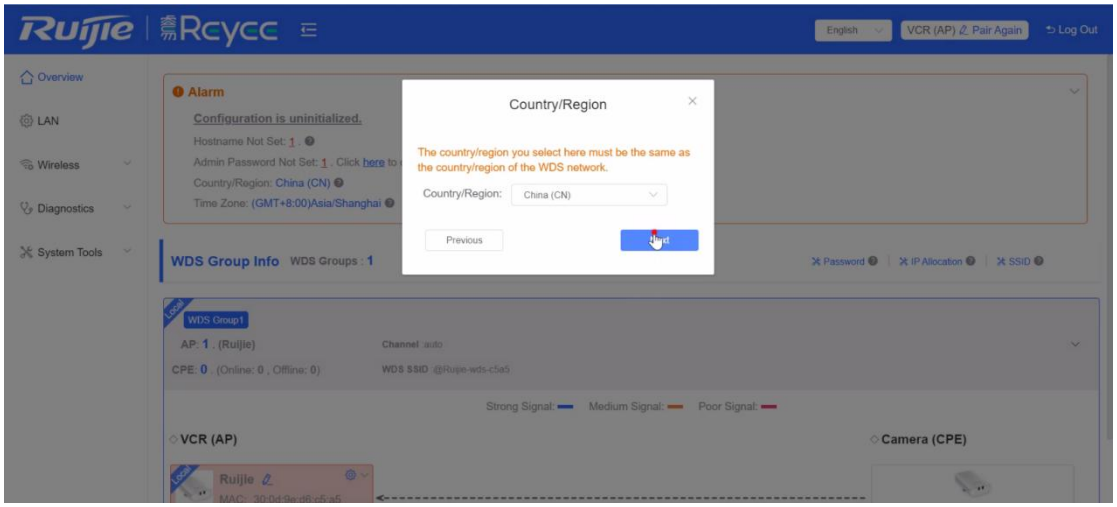
EST310 and EST350 both support PTMP feature. For EST310, one AP(VCR) supports bridging with up to 5 CPEs, For EST350, one AP(VCR) supports bridging with up to 3 CPEs.

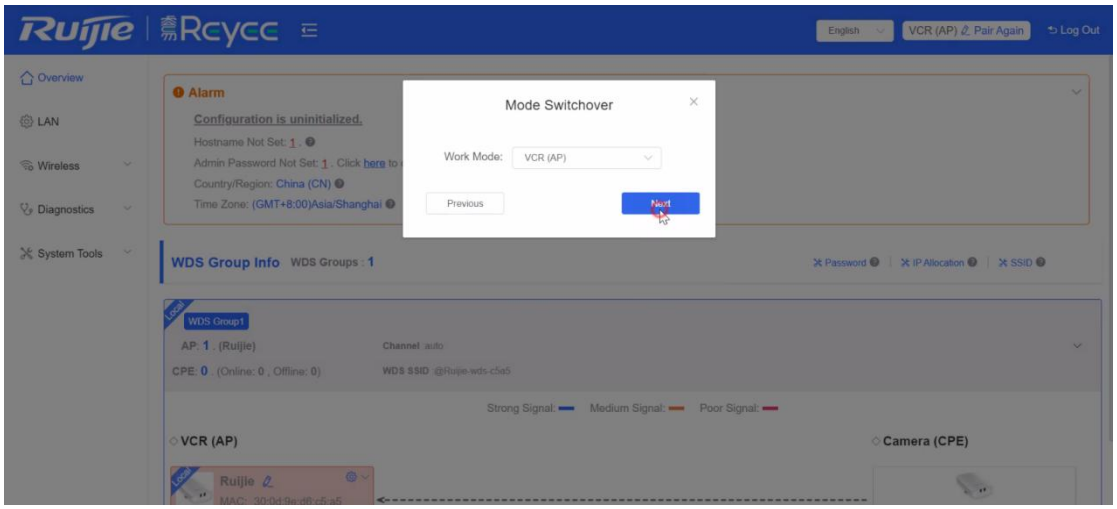
The following is the guidance for configuring PTMP.

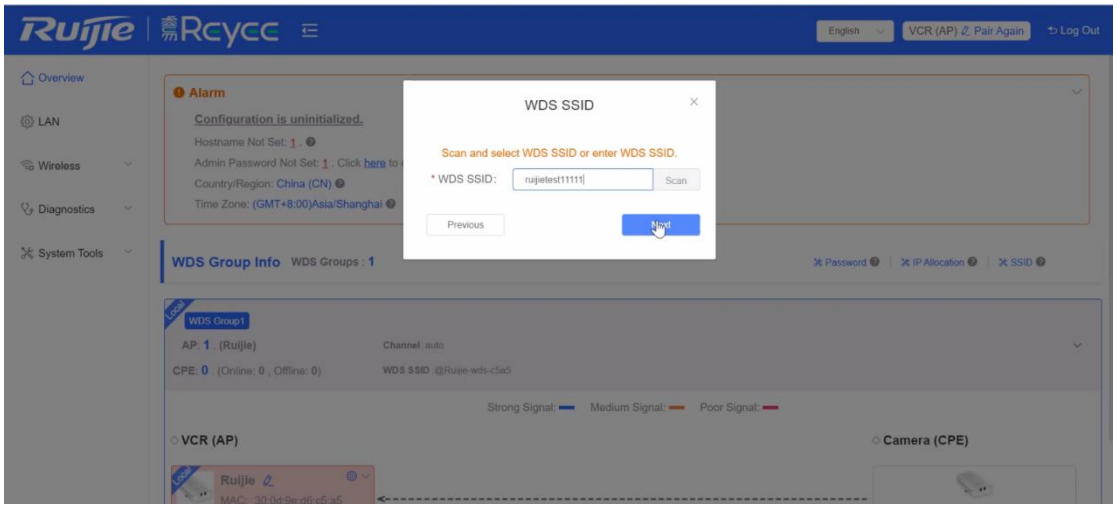
a) AP(VCR)

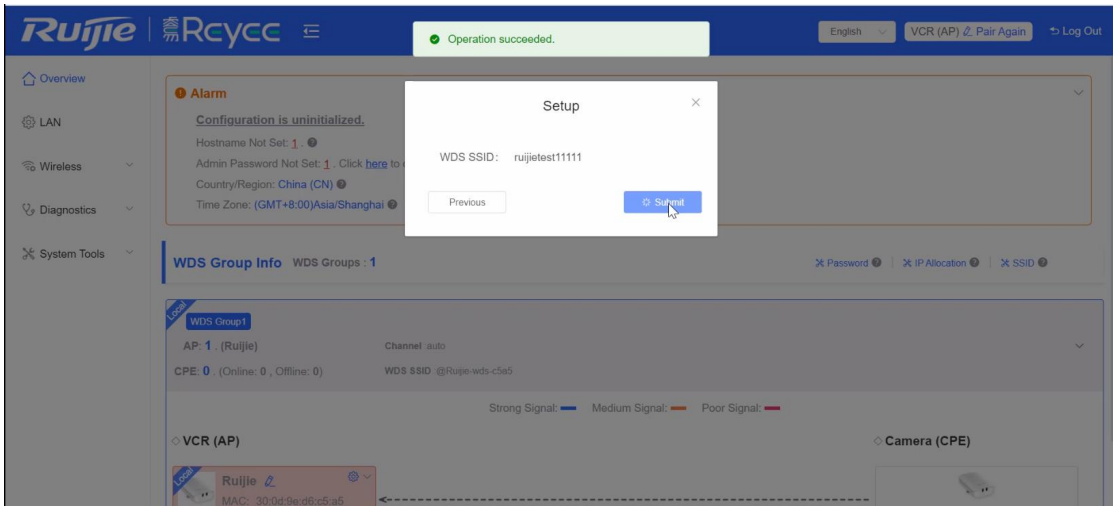
For AP(VCR) side, it needs to confirm the Country/Region and device mode, then create the WDS SSID and customize the name of it, as shown in the following pictures:





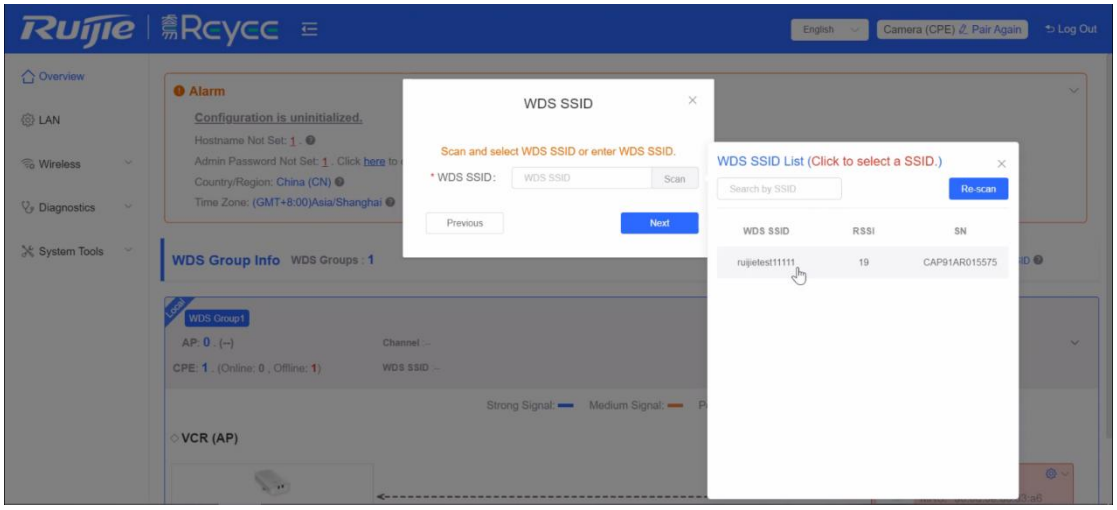


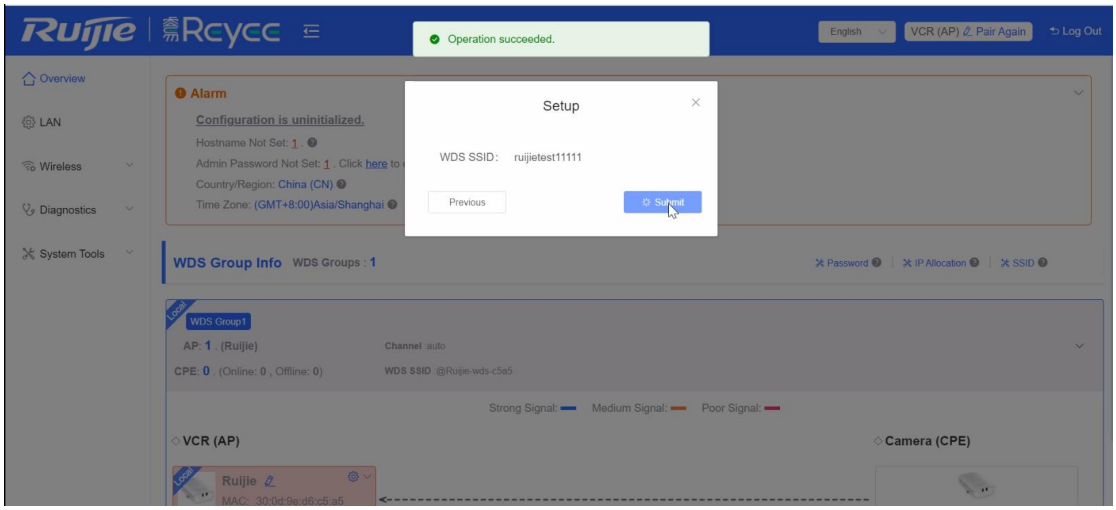




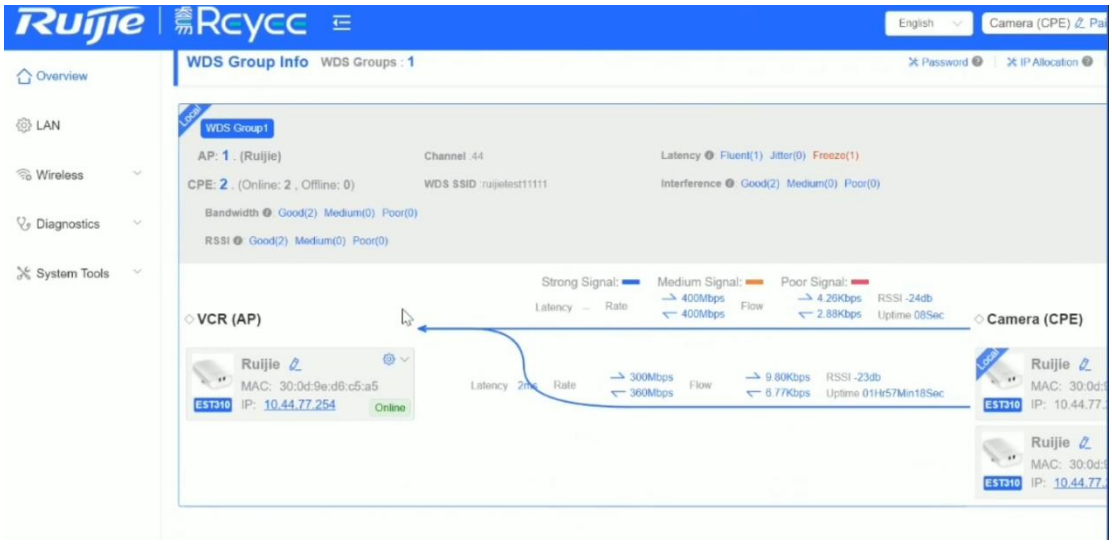
b) CPE

For CPE side, apart from confirming the Country/Region and device mode, it needs to scan the WDS SSID and chose it. The configuration steps of another CPEs in the same WDS group are the same.



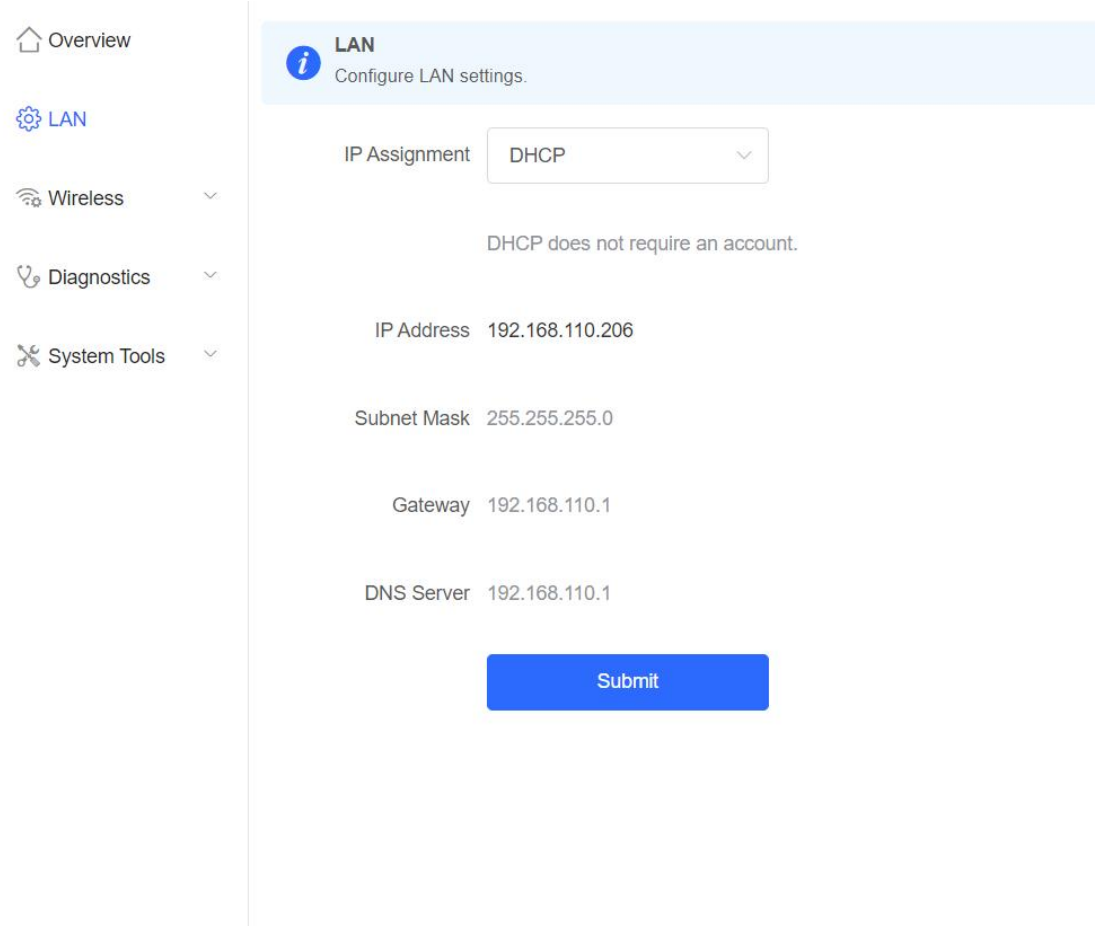


After all CPEs have connected to the WDS SSID, you can see the topology of bridge in the eWeb.



4.6.4 LAN

If a DHCP server is deployed in the network, you are advised to set Internet to DHCP. If no DHCP server is deployed, set Internet to Static IP Address, set IP Address, Subnet Mask, Gateway, and DNS Server, and click **Save.**



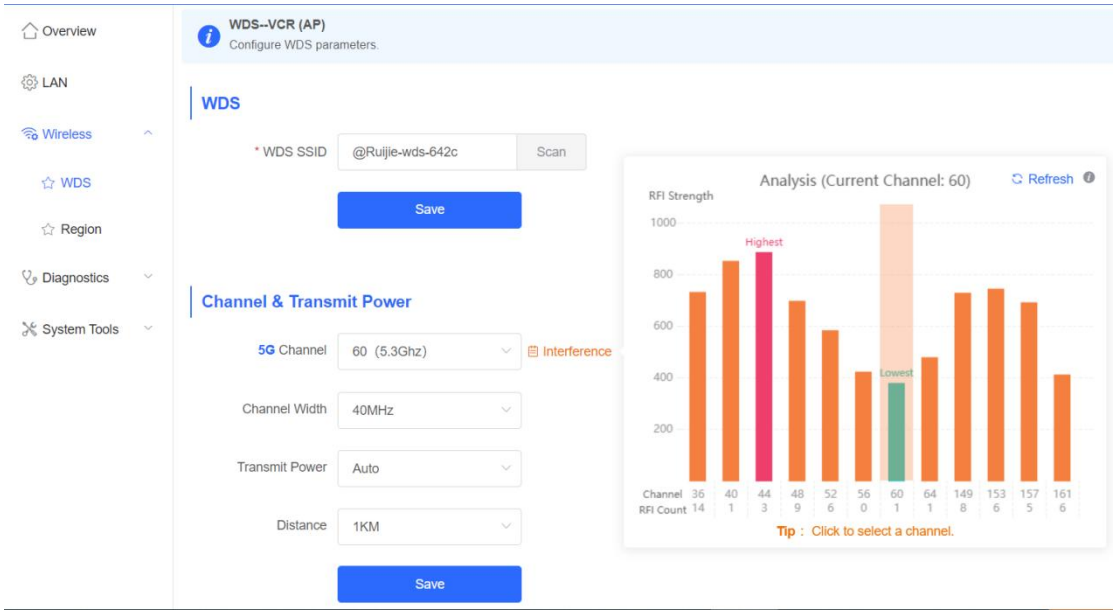
4.6.5 Wireless

4.6.5.1 WDS

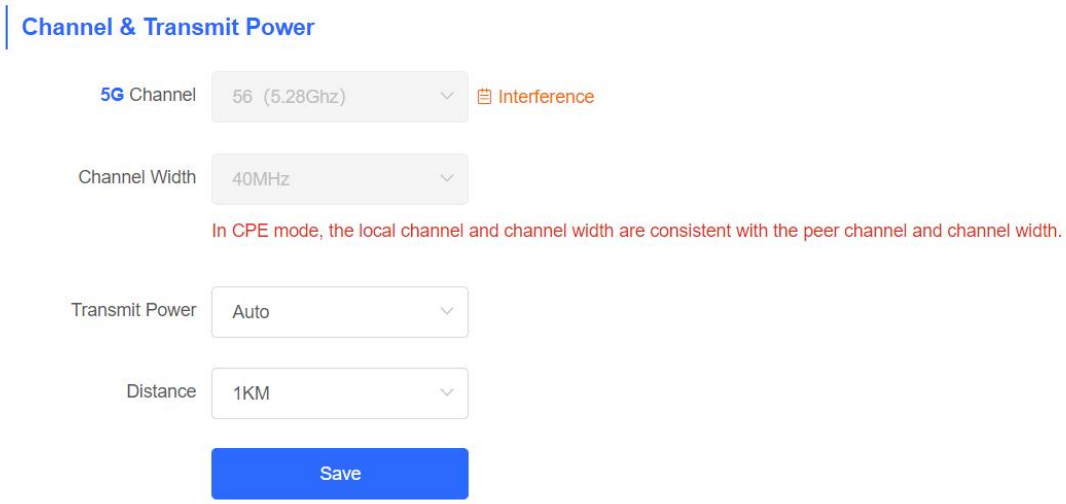
This page allows you to configure the WDS SSID in the local device. The device detects the surrounding wireless environment and selects the appropriate configuration upon power-on. However, network stalling caused by wireless environment changes cannot be avoided. You can also analyze the wireless environment around the bridge and manually select appropriate parameters.

Before configuration, you can check the interference in the current environment in the following way to find the optimal channel.

Choose **Wireless> WDS> Channel &Transmit Power**. Click Interference to check the interference of current channels. The channel with the smallest interference is the optimum.



The camera mode does not support independent channel settings. After the channel at the NVR end is adjusted, the camera end automatically changes its channel to be the same as the NVR end.



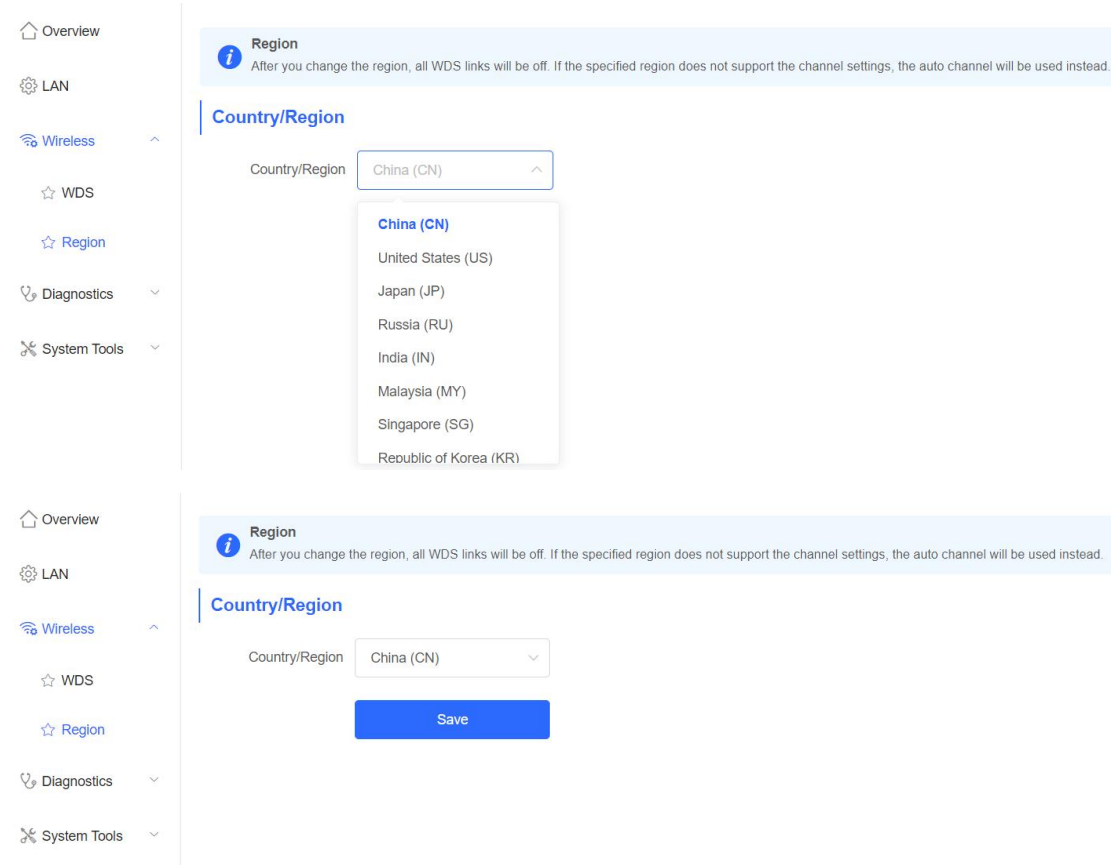
Note:

The available channel is related to the country/region code. Select the local country or region.

4.6.5.2 Region

The change of Country/region code takes effect on all devices in the entire network, that is, all bridges on the Overview page. Therefore, before changing the country/region code, confirm that the target device is in the current network and the WDS link works well.

Choose the target country/region from the drop-down list, and click **Save.**



Note:

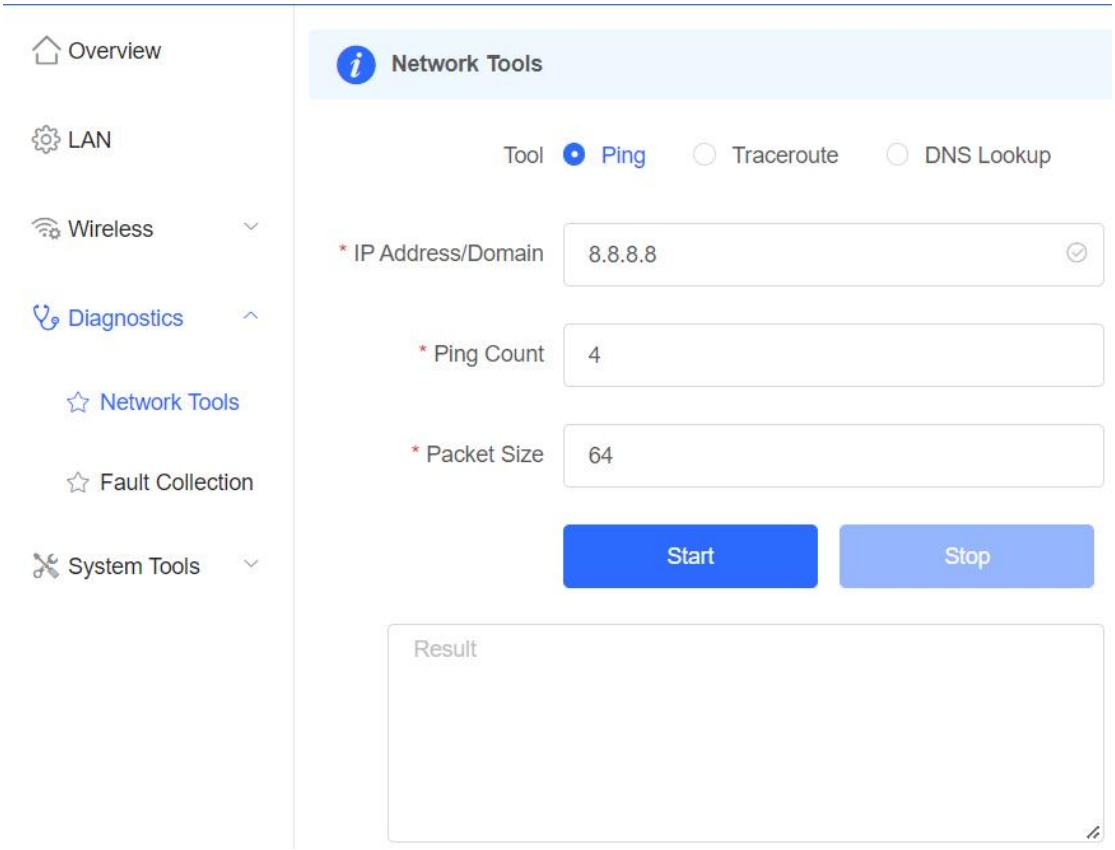
After the country/region code is changed, the Wi-Fi network will restart, and the NVR and camera will be reconnected after the Wi-Fi network is restarted. The current channel may be switched to Auto because it is not supported by the country/region. Therefore, exercise caution when performing this operation.

4.6.6 Diagnostics

When you select the ping tool, you can enter the IP address or URL and click Start to test the connectivity between the router and the IP address or URL. The message "Ping failed" indicates that the router cannot reach the IP address or URL.

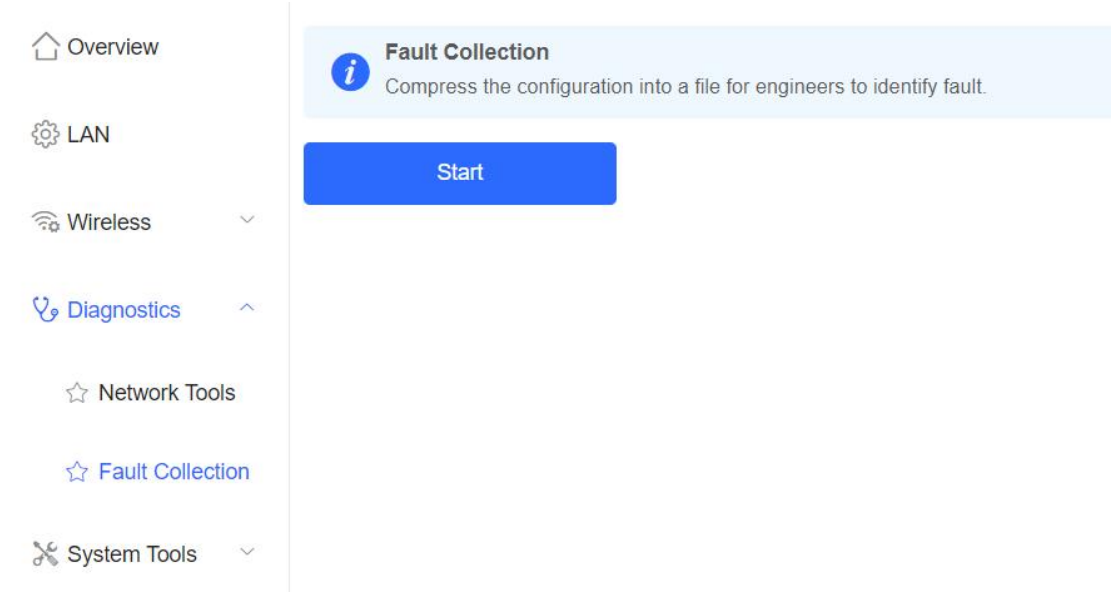
The Traceroute tool displays the network path to a specific IP address or URL.

The DNS Lookup tool displays the DNS server address used to resolve a URL.



Choose **Diagnostics> Fault Collection.**

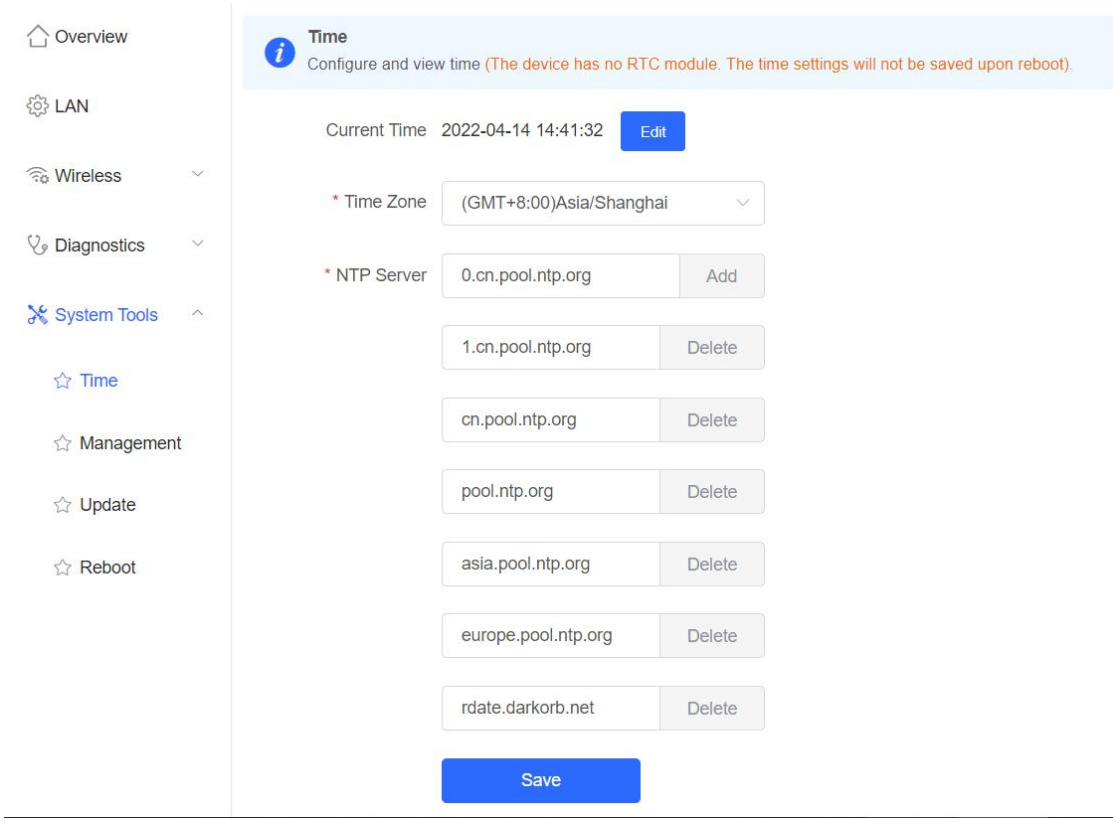
Click **Start** to collect fault information and compress it into a file for engineers to identify fault.



4.6.7 System tools

4.6.7.1 Time

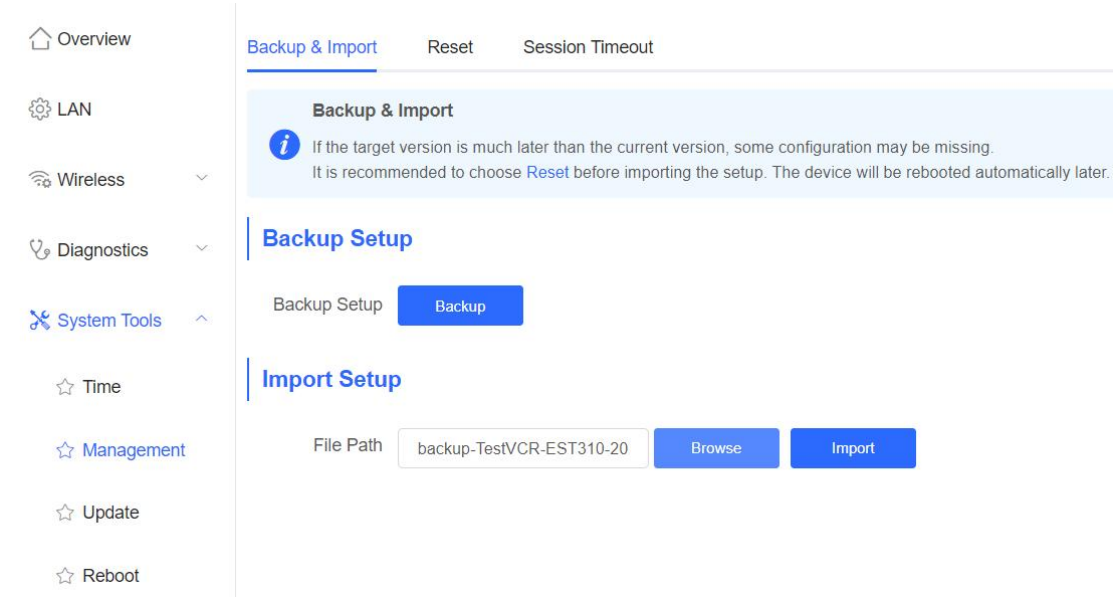
Choose **System Tools> Time**. You can view the current system time. If the time is incorrect, check and select the local time zone. If the time zone is correct but time is still incorrect, click Edit to manually set the time. In addition, the bridge supports Network Time Protocol (NTP) servers. By default, multiple servers serve as the backup of each other. You can add or delete local servers as required.



4.6.7.2 Management

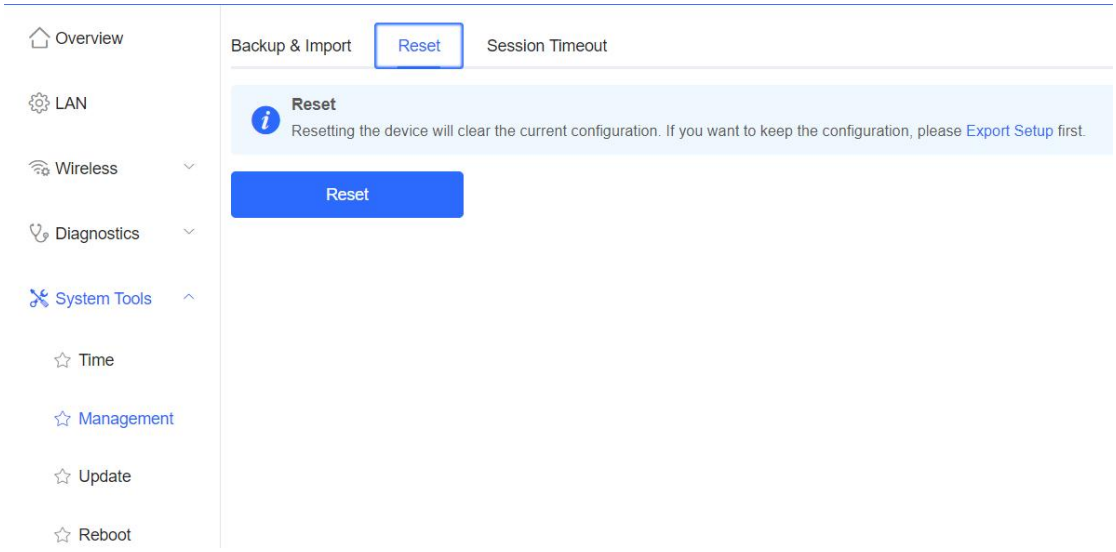
Choose **System Tools> Management> Backup & Import.**

Configure backup: Click **Backup** to download a configuration file locally. Configure import: Click **Browse**, select a configuration file backup on the local PC, and click Import to import the configuration file. The device will restart.

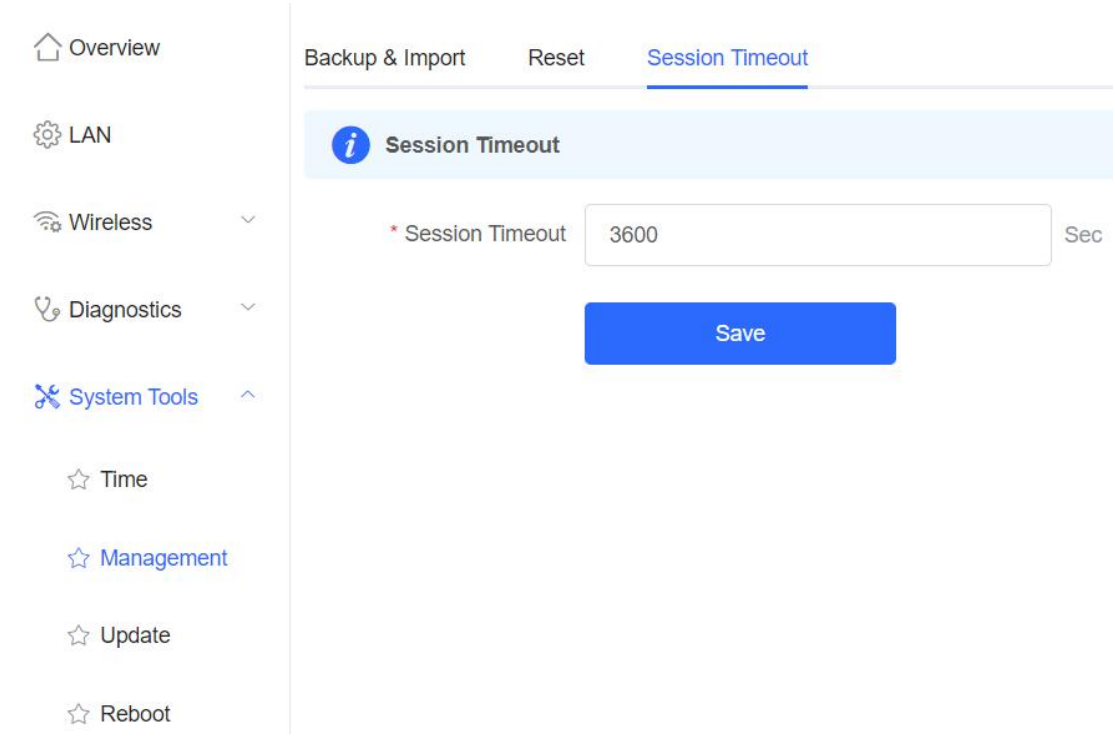


Choose S**ystem Tools> Management> Reset.**

Click **Reset** to restore factory settings.



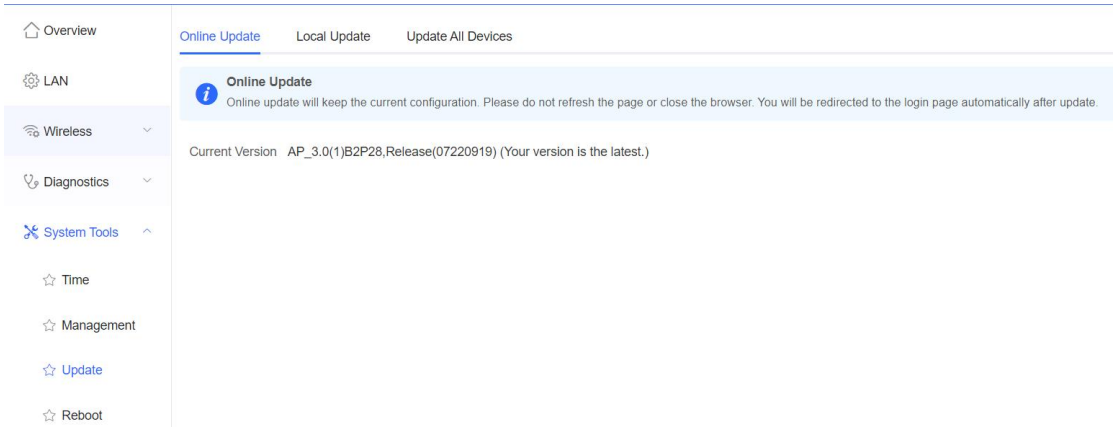
Choose **System Tools> Management> Session Timeout**. If no operation is performed on the page within a period of time, the session will be down. When you need to perform operations again, enter the password to open the configuration page. The default timeout duration is 3600 seconds, that is, 1 hour.



4.5.6.3 Update

Choose **System Tools> Update> Online Update.**

If there a new version available, you can click it for updating

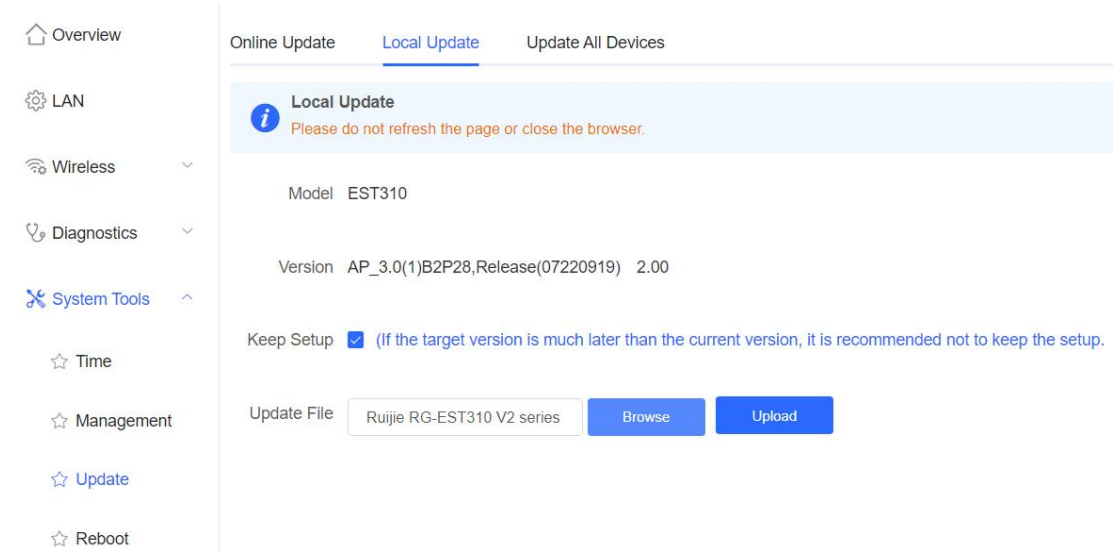


Note:

After being updated, the device will reboot. Therefore, exercise caution when performing this operation. If no version updating is detected or online update cannot be performed, check whether the bridge is connected to the Internet.

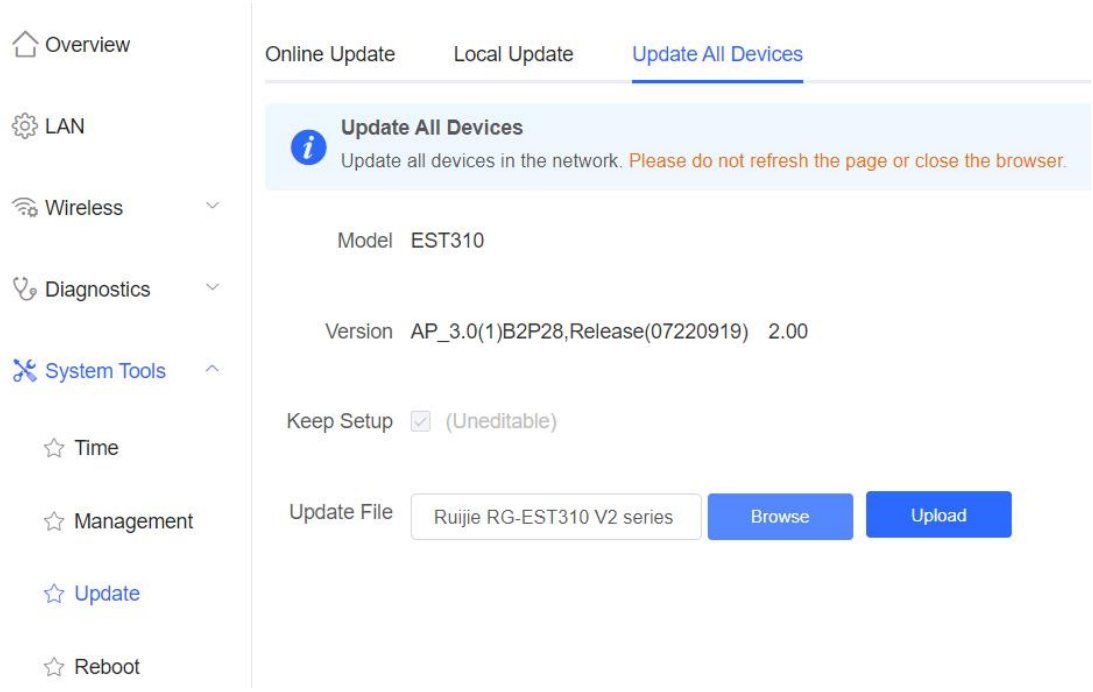
Choose **System Tools> Update> Local Update.**

You can view the current software version, hardware version and device model. If you want to update the device with the configuration retained, check **Keep Setup.** Click **Browse**, select an update package on the local PC, and click Upload to upload the file. The device will be updated.



Choose **System Tools> Update> Update All Devices.**

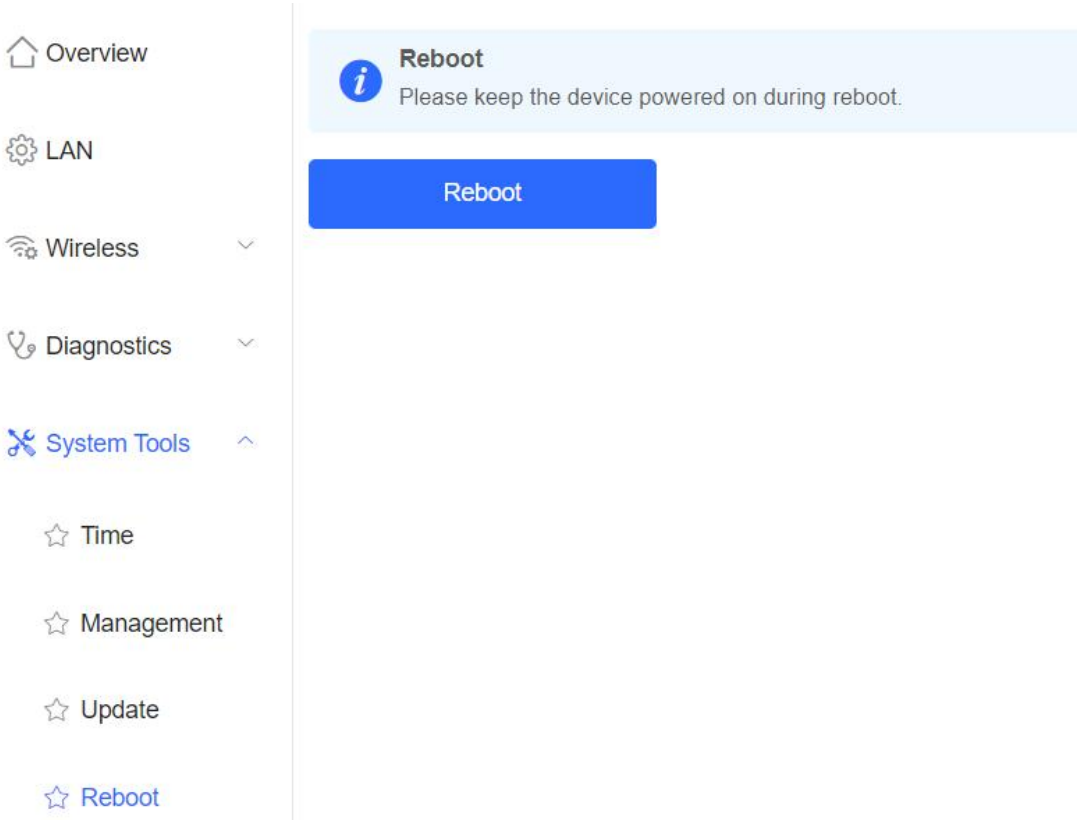
You can view the current software version, hardware version and device model. You are advised to update all devices with configuration data retained. Click **Browse,** select an update package on the local PC, and click **Upload** to upload the file. In the pop-up page, click **Details** to check the target update package and devices. Click Update to start updating all devices.



4.5.6.4 Reboot

Choose **System Tools> Reboot.**

You are allowed to restart the local device, please keep the device powering on.



5 Advanced Solution Guide

5.1 Reyee Flow Control Solution

5.1.1 Application Scenario

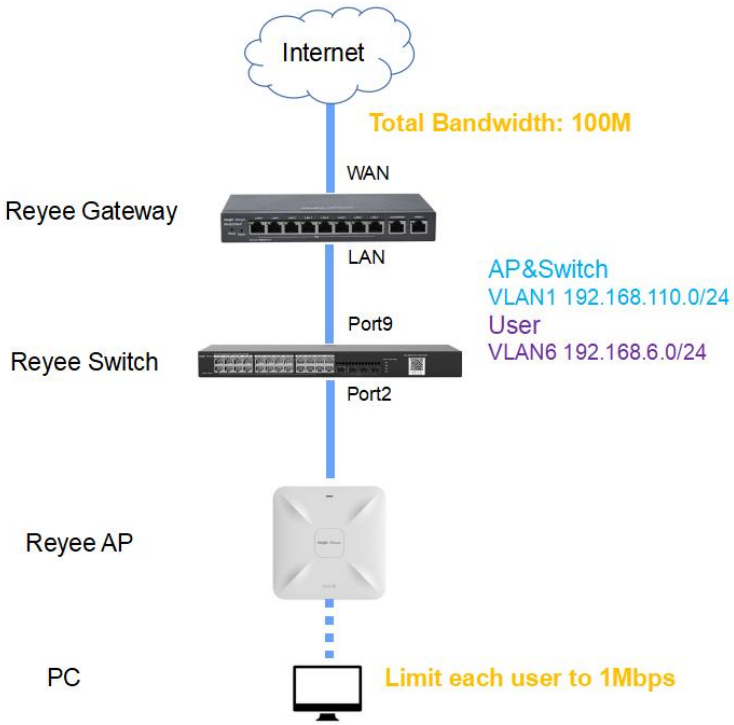
Flow Control is used for setting the rate limitations of download and upload for the clients. With the Flow Control configured, we can protect the network bandwidth from being occupied too much by some of the clients.

5.1.2 Configuration Case

Requirement

Limiting EG egress total bandwidth to 100Mbps and each user rate of VLAN 6 network segment to 1Mbps.

Network Topology



Network Description:

- EG works as a DHCP server to assign IP addresses to users and AP & switch devices.
- The AP & switch devices obtain the IP address 192.168.110.0/24 in the VLAN1 network segment for Internet access.
- The users obtain the IP address 192.168.6.0/24 in the VLAN6 network segment for Internet access.

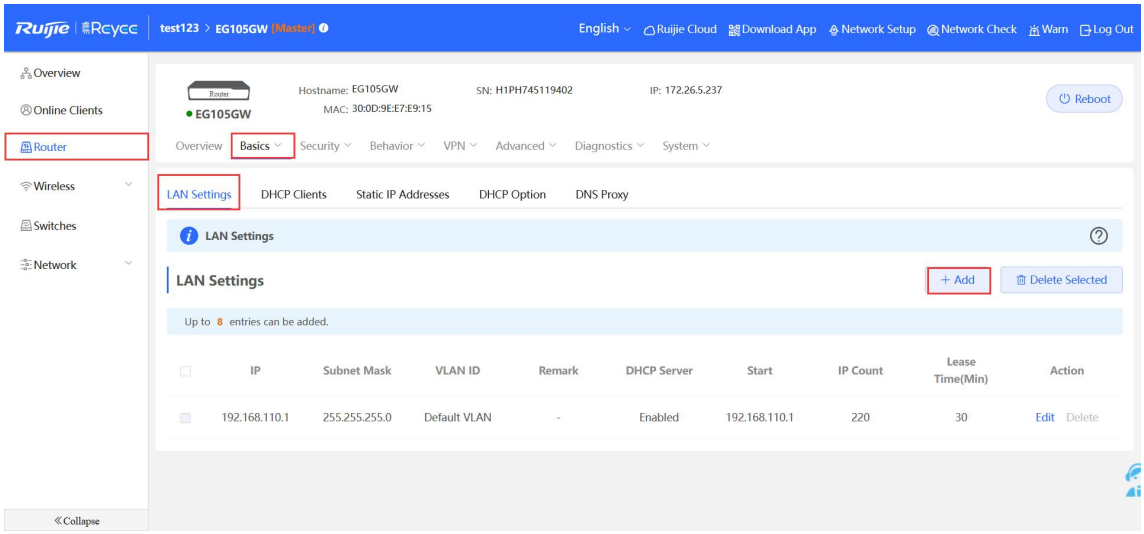
Configuration Steps

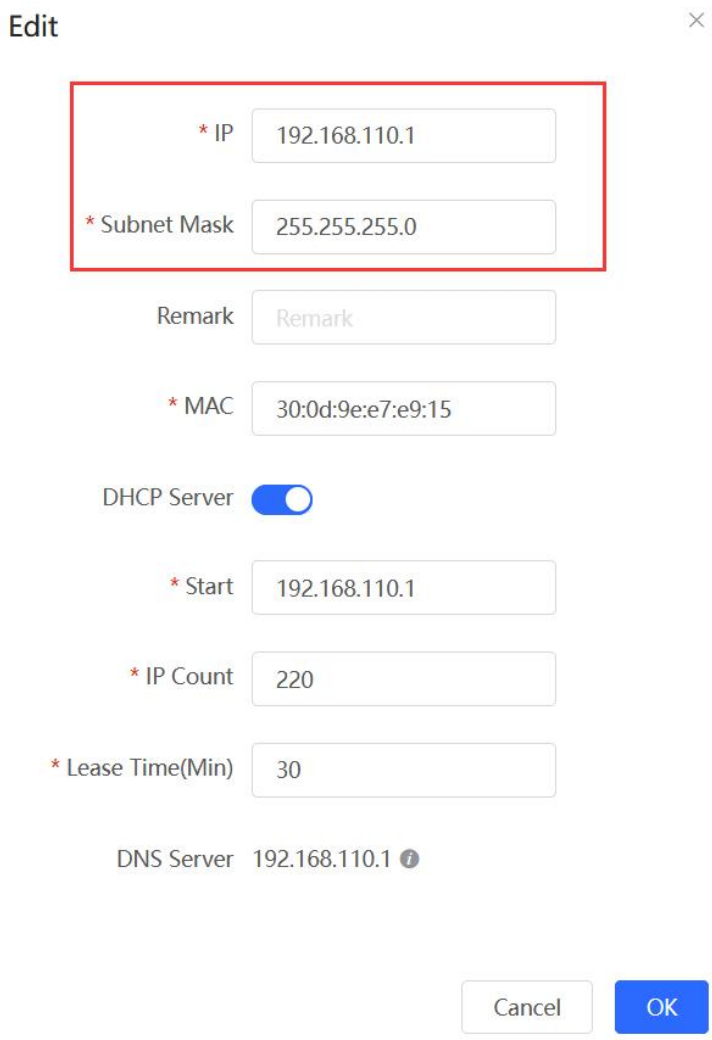
- basic network configuration

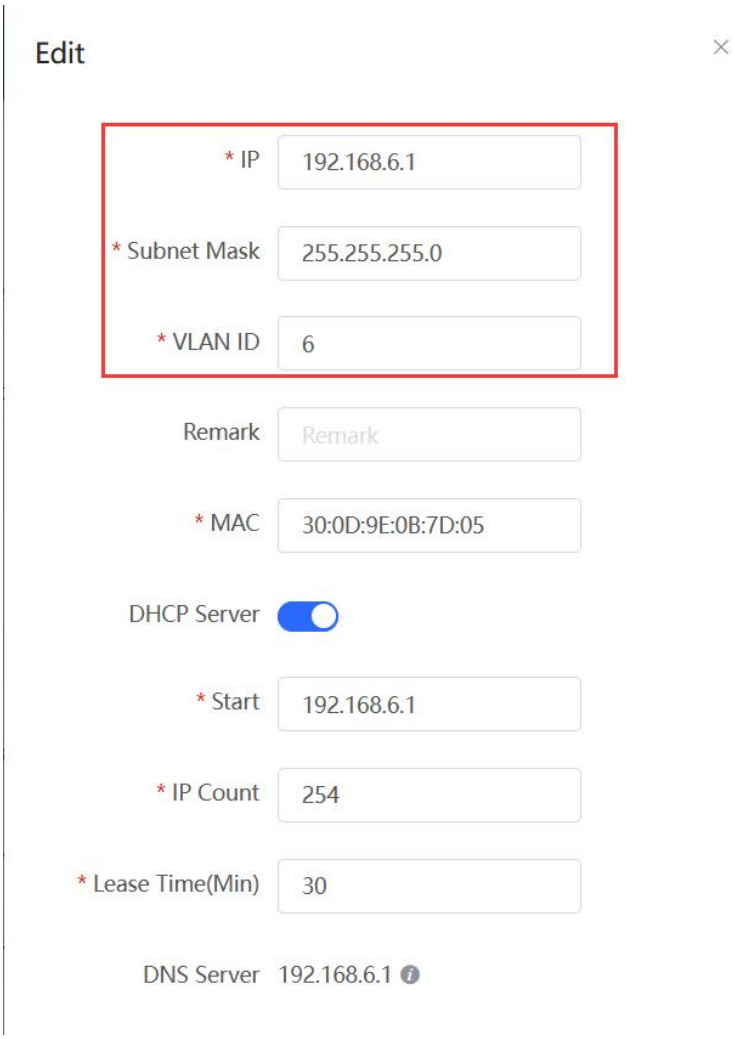
- Enable Smart Flow Control function and configure the custom policy

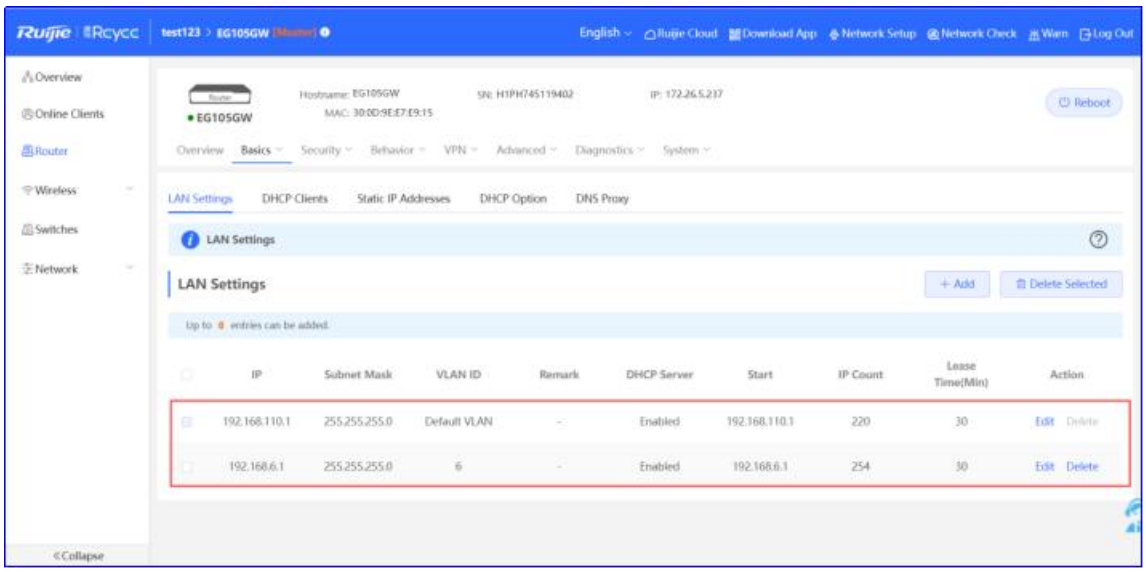
1. Configure basic network configuration

Step 1: Click **Router** -> **Basics** -> **LAN** -> **LAN Settings** -> **Add,** Configure LAN Settings and DHCP pool of VLAN1 and VLAN6 network segment on the EG.




Edit
* IP
192.168.110.1
* Subnet Mask
255.255.255.0
Remark
Remark
* MAC
30:0d:9e:e7:e9:15
DHCP Server
* Start
192.168.110.1
* IP Count
220
* Lease Time(Min)
30
DNS Server
192.168.110.1
Cancel
OK

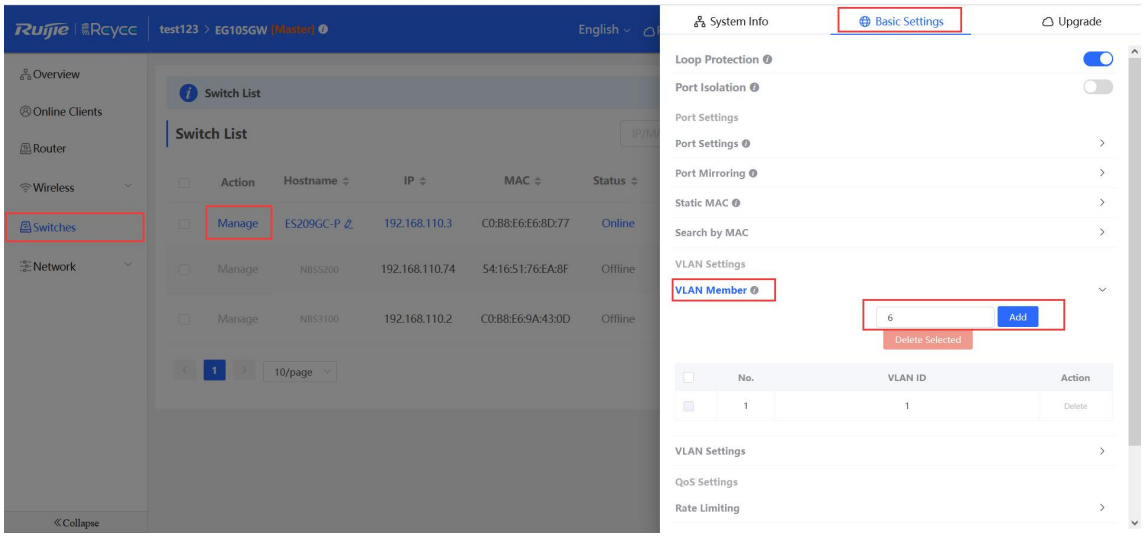


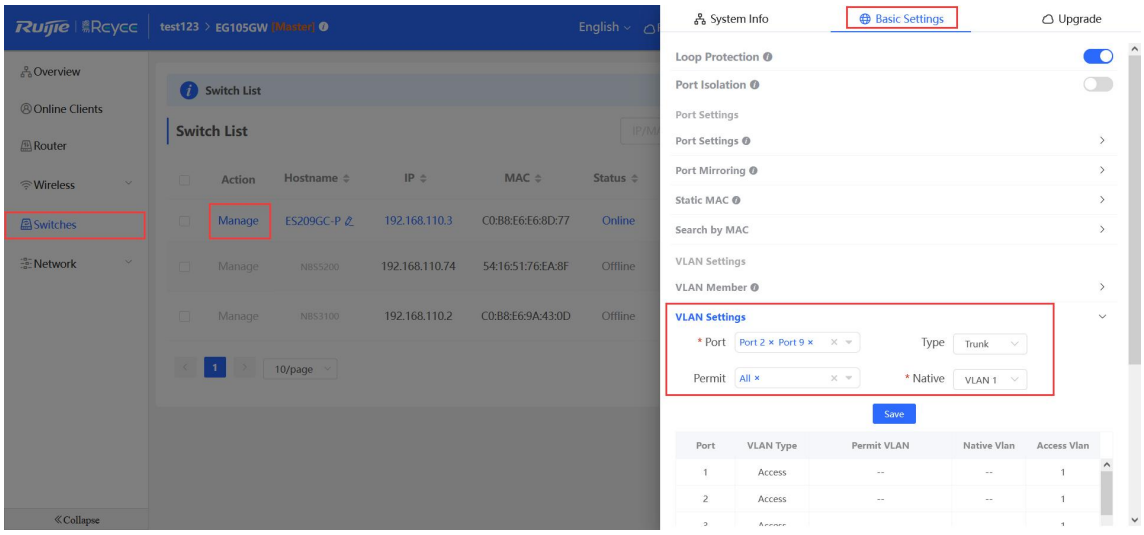


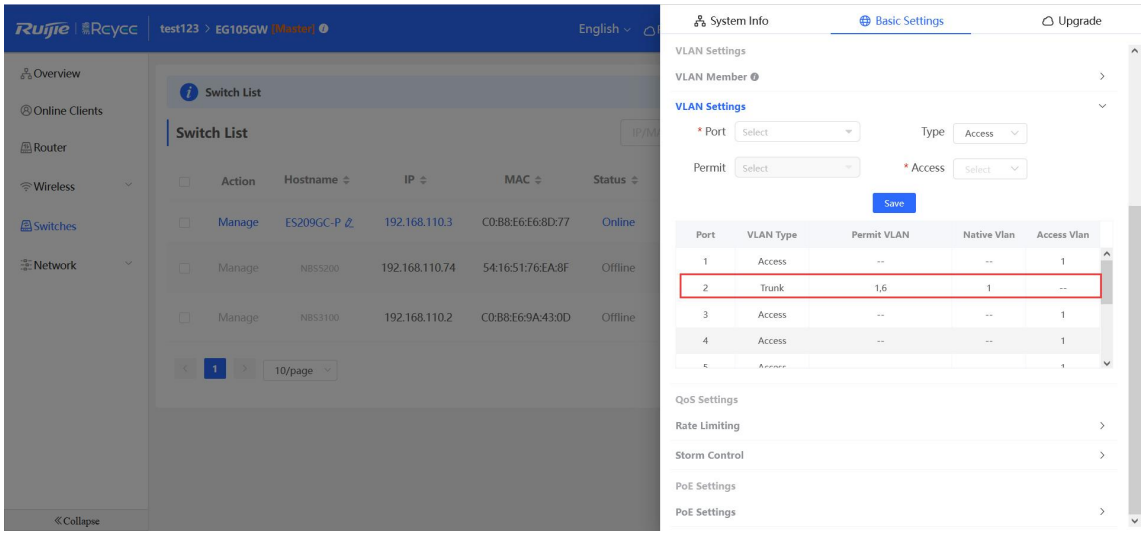
Note:

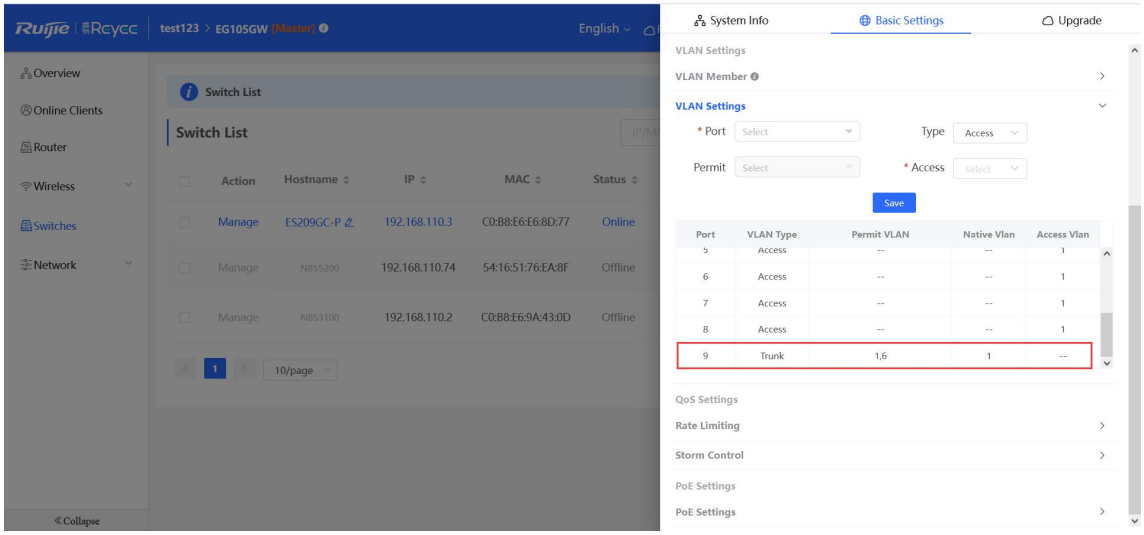
Default VLAN 1 network is set to 192.168.110.0/24 network segment.

Step 2: Click **Switches** -> **Manage** -> **Basic Settings** -> **VLAN Member** to create VLAN6 on the switch, and click **VLAN Settings** to set port2 and port9 which connect to AP and EG to trunk port and allow the VLAN1 and VLAN6 to pass through, then check the port settings on the device.

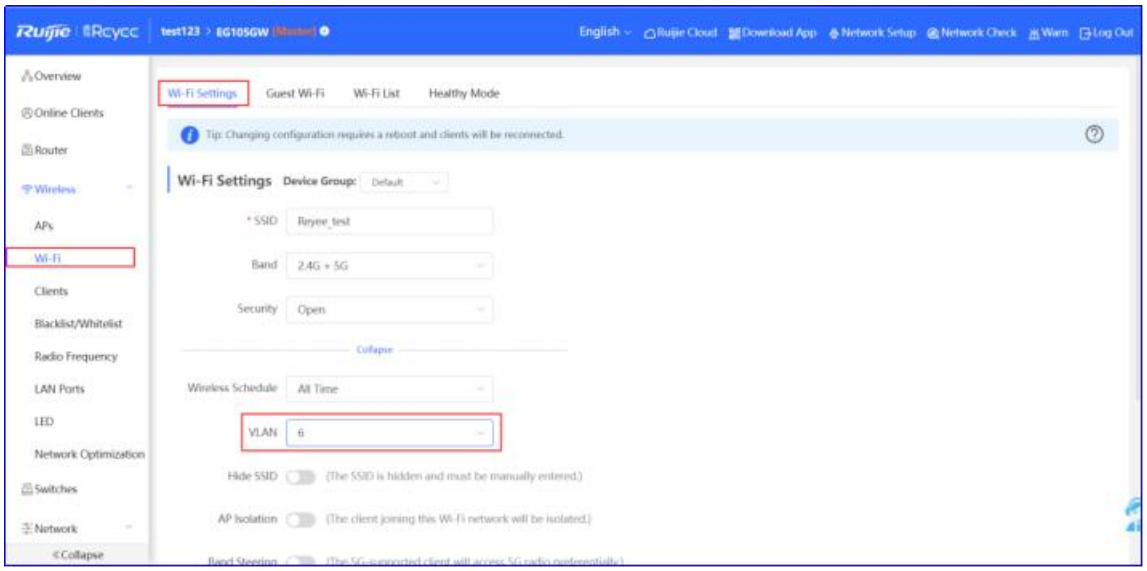


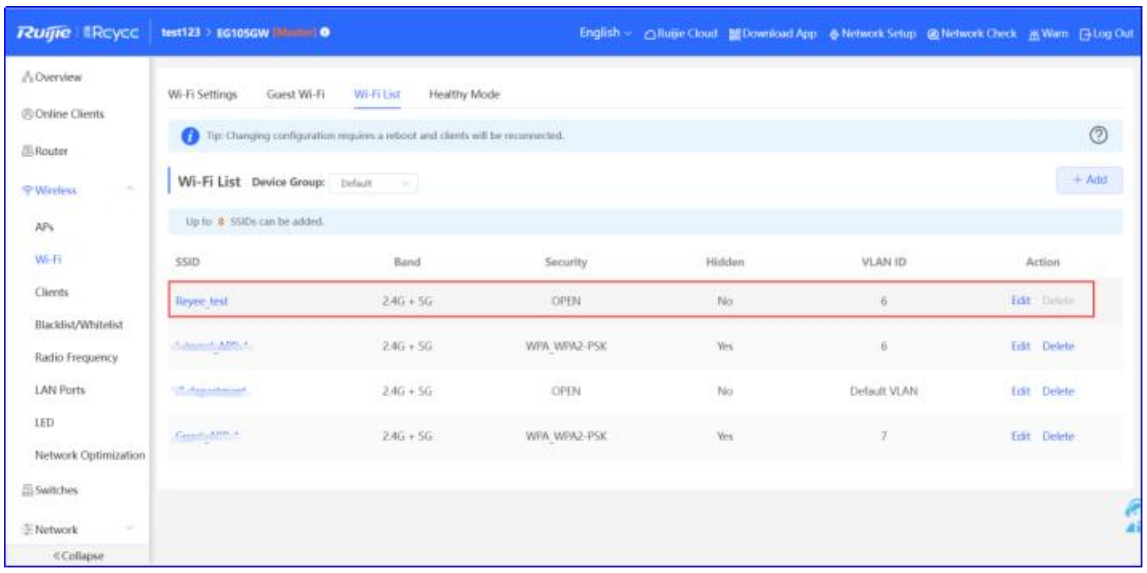






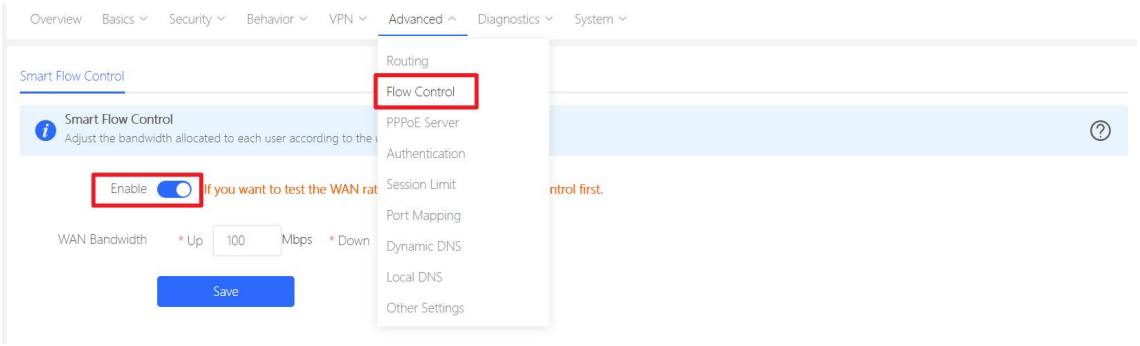
Step 3: Click **Wireless-> Wi-Fi -> Wi-Fi Settings,** Configure SSID named Reyee_test and set VLAN6 to this ssid.



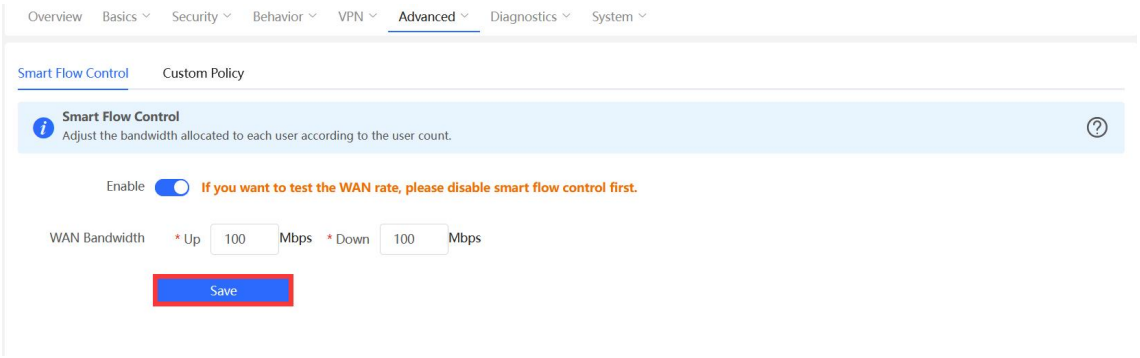


2. Configure Smart Flow Control

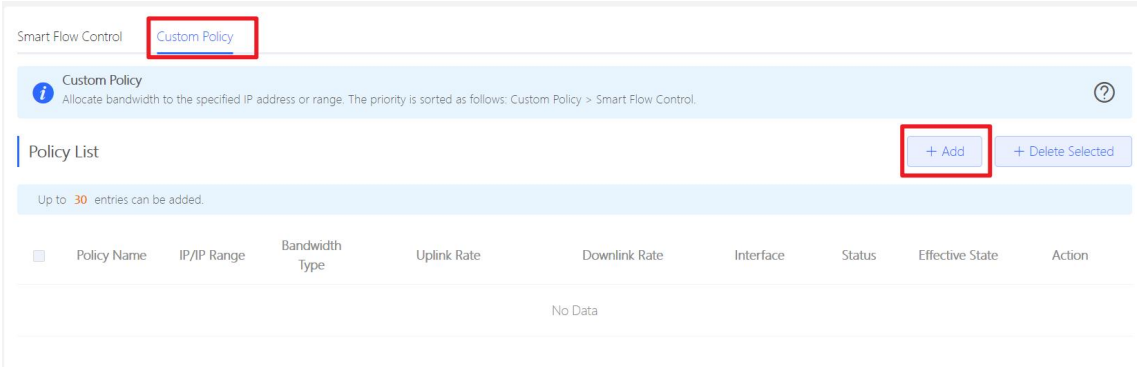
Step 1: Choose **Router** → **Advanced** → **Flow Control** and enable **Smart flow control** feature.



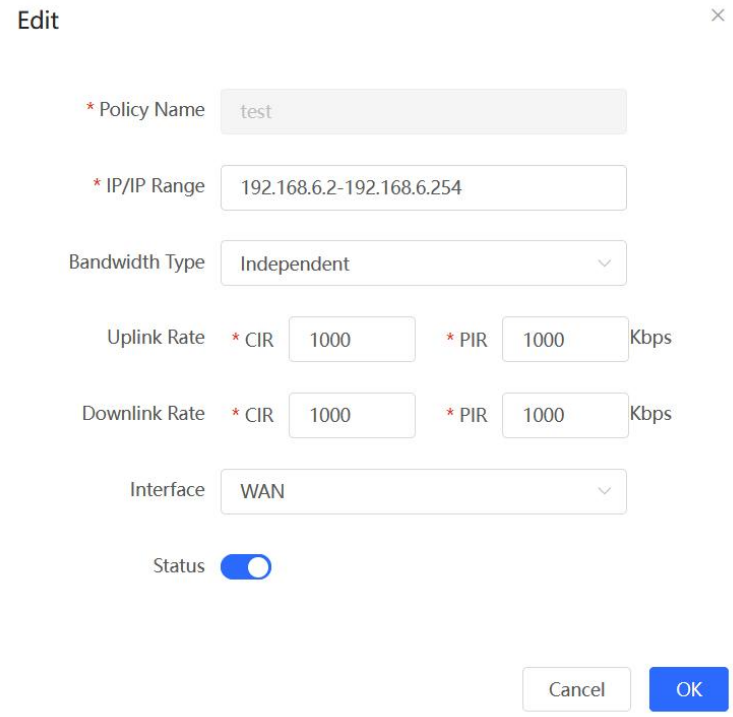
Step 2: Fill in the uplink and downlink WAN bandwidth as 100Mbps and **Save** the configuration.

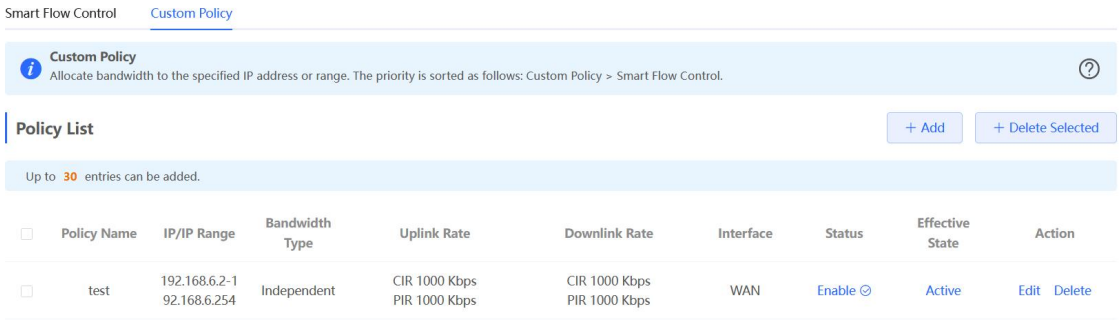


Step 3: After step2 is being done, **Custom Policy** will be displayed. Click **Add** to add policy.



Step 4: Set **Policy Name**, **IP range**, **Bandwidth Type**, **Rate**, etc.





Note:

Bandwidth Type:

1) Shared: Shared indicates that all IP addresses share with the total bandwidth.

2) Indenpended: Independent indicates that the rate limit is setted for per IP address.

CIR: CIR means committed information rate.

PIR: PIR means peak information rate.

Configuration Verification

Use Speed test tool to check that each user is limited up to 1Mbps.

5.2 Reyee Cloud Authentication Solution

5.2.1 Working Principle

Cloud authentication allows you to control users accessing to the wireless network. The configuration will be synchronized from Cloud to local EG device. In portal authentication, all the client's HTTP requests will be redirected to an authentication page first. The clients are required to authenticate, payment, accept the end-user license agreement, acceptable use policy, survey completion, or other valid credentials, then they can visit the internet after the authentication succeeded.

5.2.2 Application Scenario

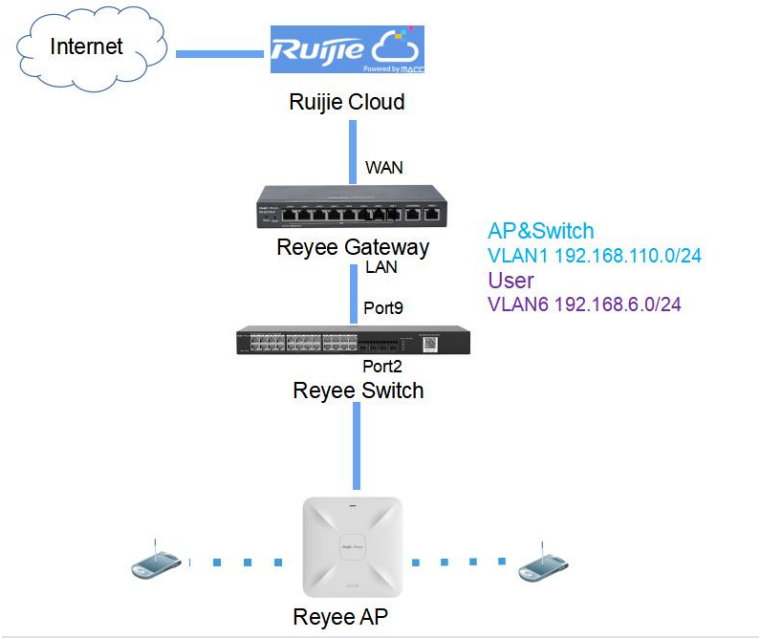
Portal authentication, also known as Web authentication, is usually deployed in a guest-access network (like a hotel or a coffee shop) to control the client's internet access.

5.2.3 Configuration Case

Requirement

Users are required to authenticate first before allowed to access the Internet. Reyee AP can't support cloud authentication, need Reyee EG to do that.

Network Topology



Network Description:

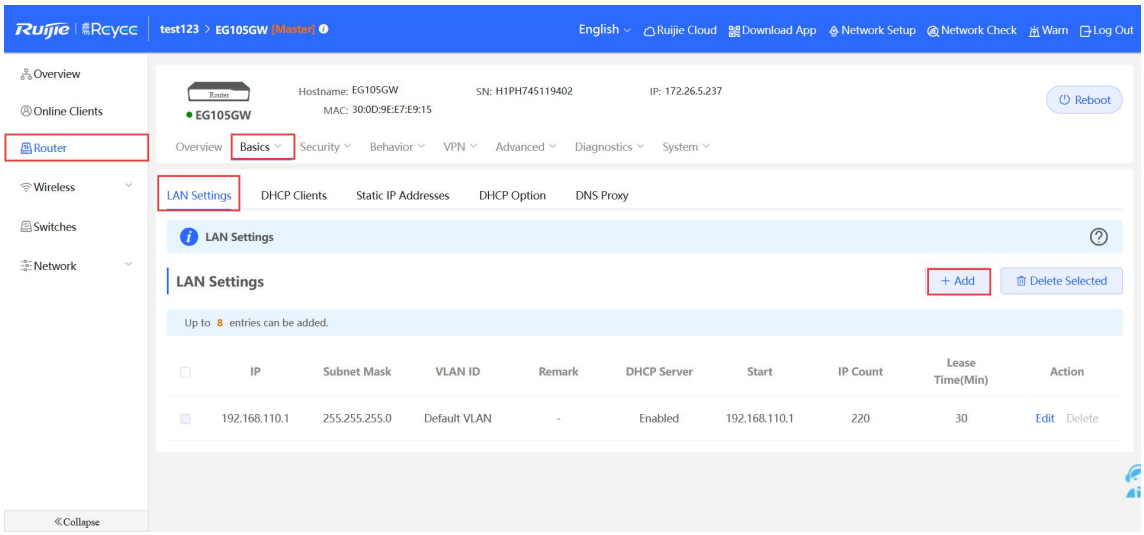
- EG works as a DHCP server to assign IP addresses to users and AP& switch devices
- The AP& switch devices obtain the IP address 192.168.110.0/24 in the VLAN1 network segment for Internet access
- The users obtain the IP address 192.168.6.0/24 in the VLAN6 network segment for Internet access
- The Ruijie Cloud work as platform to manage and monitor devices and clients status and provide captive authentication for clients.

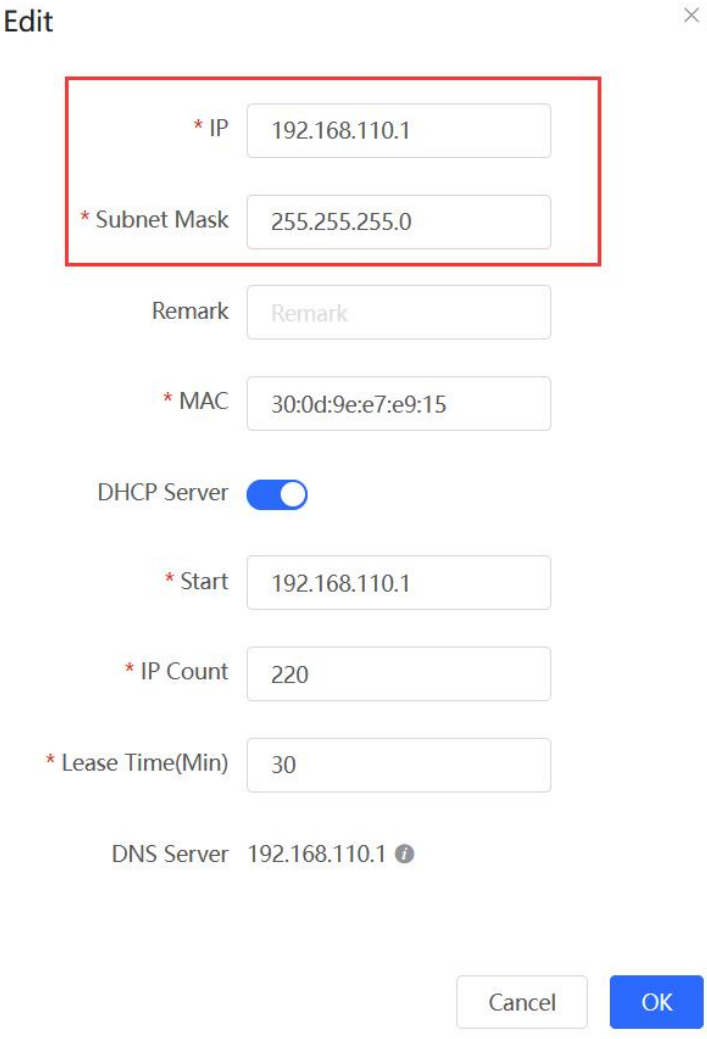
Configuration Steps

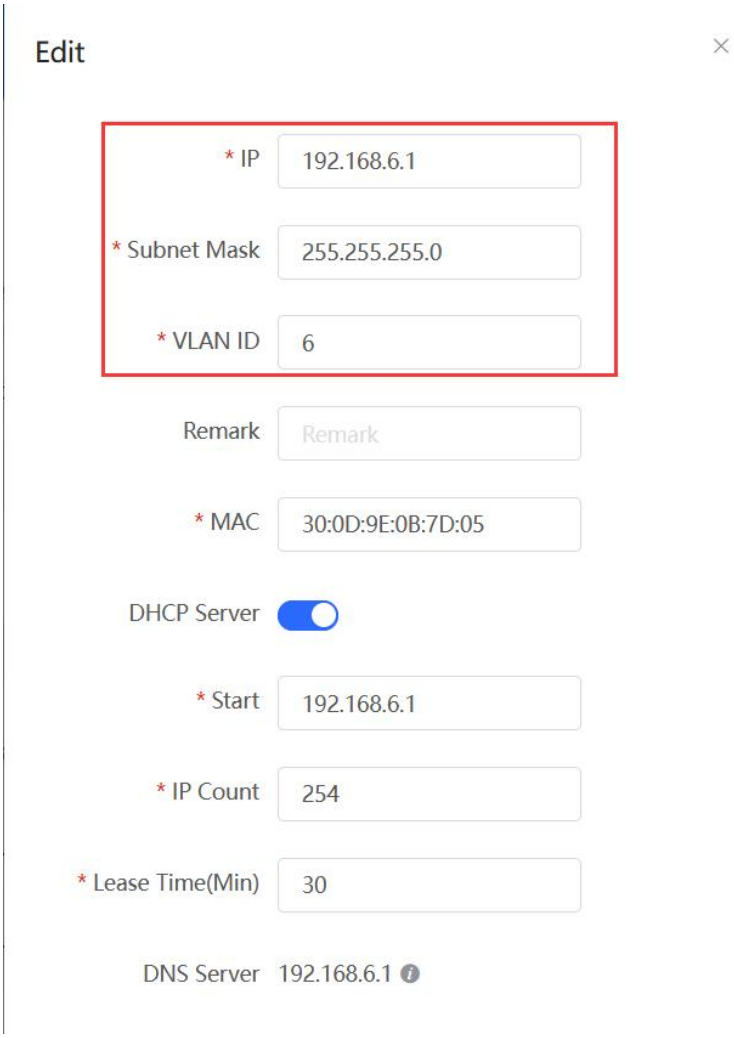
- Configure basic network
- Configure cloud authentication

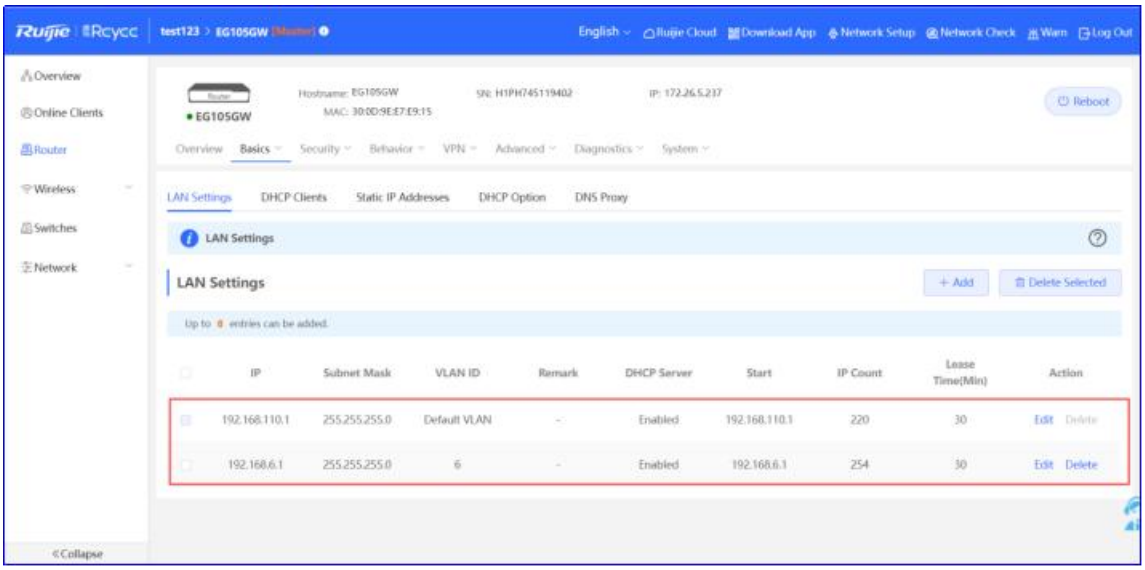
1. Configure basic network

Step 1: Click **Router** -> **Basics** -> **LAN** -> **LAN Settings** -> **Add,** Configure LAN Settings and DHCP pool of VLAN1 and VLAN6 network segment on the EG.


test123 > EG105GW (Master)
English
Ruijie Cloud
Download App
Network Setup
Network Check
Warn
Log Out
Overview
Online Clients
Router
Wireless
Switches
Network
Collapse
Hostname: EG105GW
MAC: 30:0D:9E:E7:E9:15
SN: H1PH745119402
IP: 172.26.5.237
EG105GW
Reboot
Overview
Basics
Security
Behavior
VPN
Advanced
Diagnostics
System
LAN Settings
DHCP Clients
Static IP Addresses
DHCP Option
DNS Proxy
LAN Settings
LAN Settings
+ Add
Delete Selected
Up to 8 entries can be added.
IP
Subnet Mask
VLAN ID
Remark
DHCP Server
Start
IP Count
Lease Time(Min)
Action
192.168.110.1
255.255.255.0
Default VLAN
-
Enabled
192.168.110.1
220
30
Edit
Delete


Edit
* IP
192.168.110.1
* Subnet Mask
255.255.255.0
Remark
Remark
* MAC
30:0d:9e:e7:e9:15
DHCP Server
* Start
192.168.110.1
* IP Count
220
* Lease Time(Min)
30
DNS Server
192.168.110.1
Cancel
OK

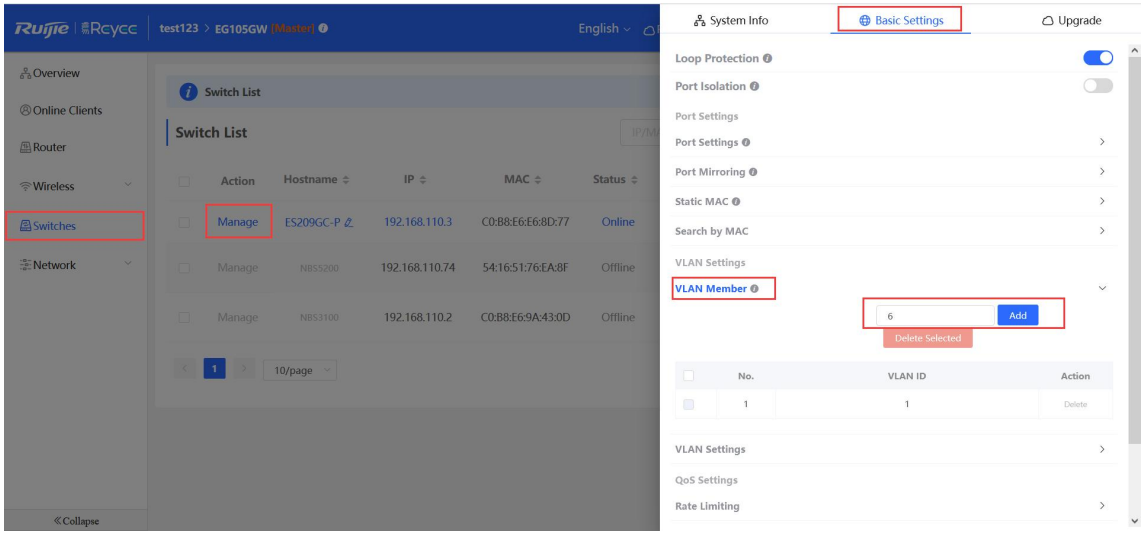


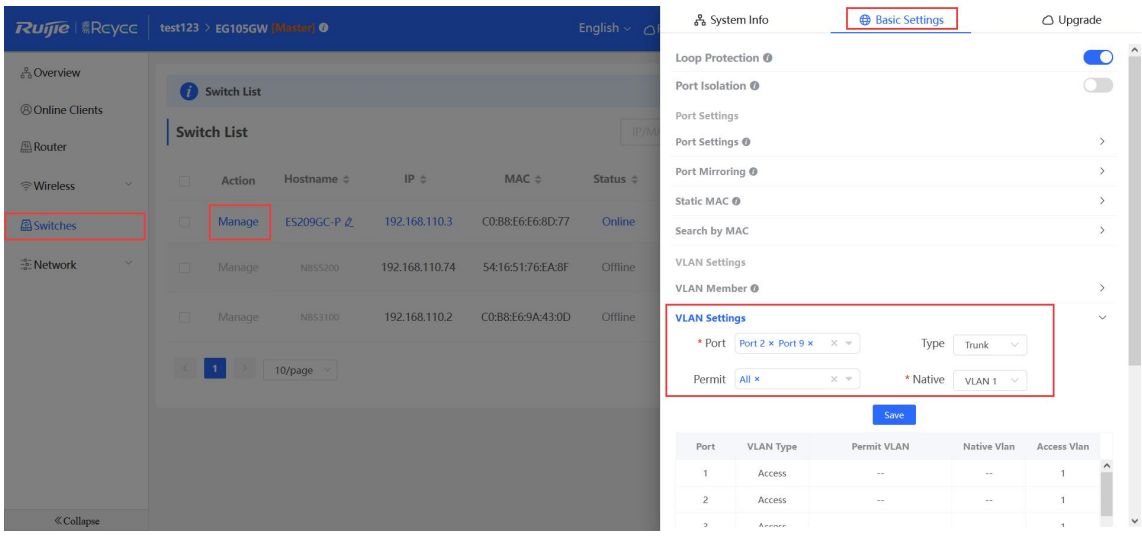


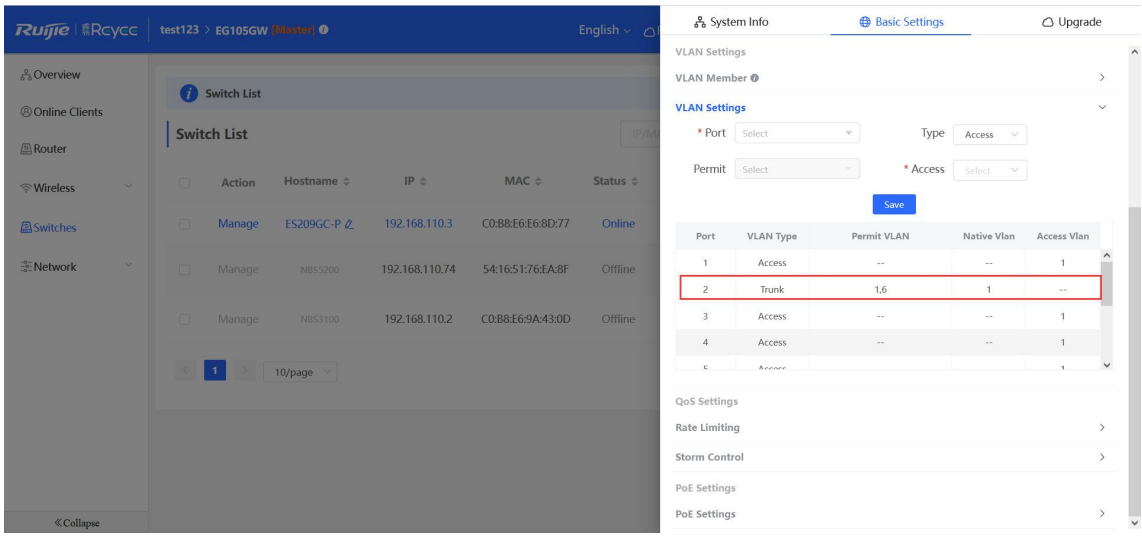
Note:

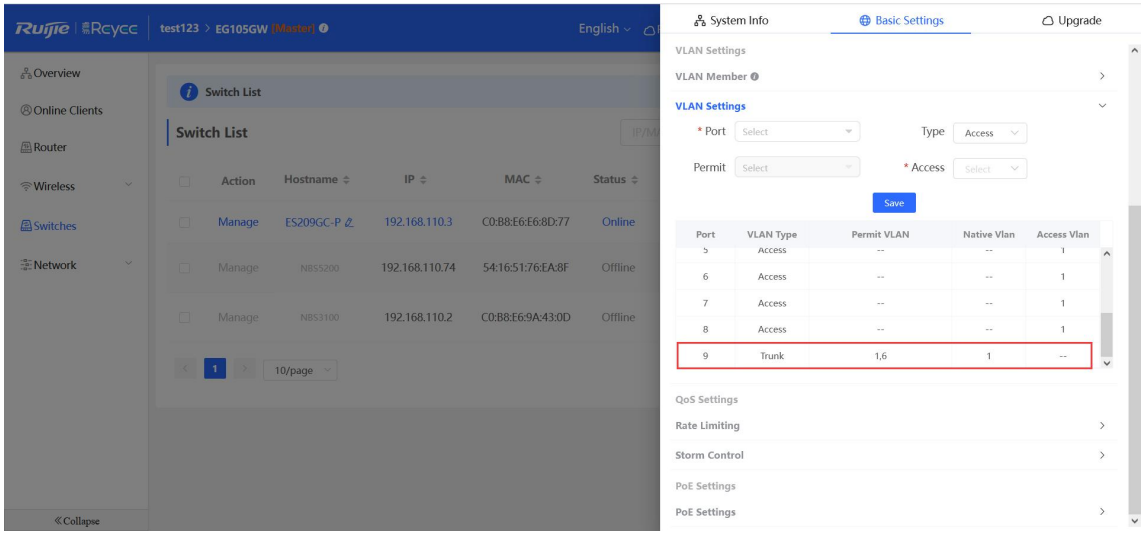
Default VLAN network is set to 192.168.110.0/24 network segment.

Step 2: Click **Switches** -> **Manage** -> **Basic Settings** -> **VLAN Member** to create VLAN6 on the switch, and click **VLAN Settings** to set port 2 and port 9 to trunk port which connect to AP and EG and allow VLAN 1 and VLAN 6 to pass through, then check the port settings on the device.

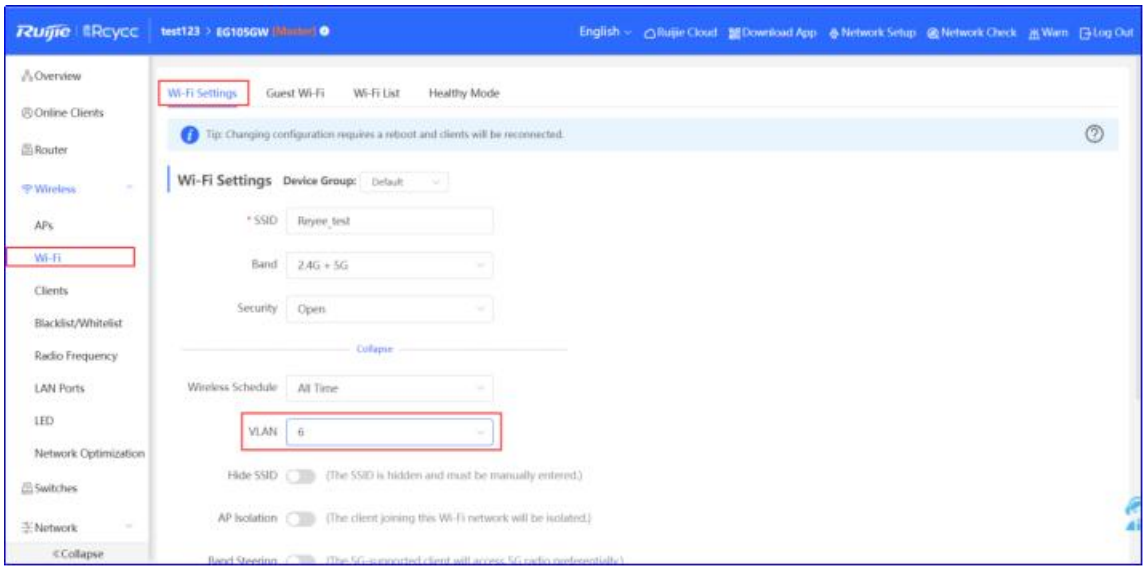

test123 > EG105GW (Master)
English
Overview
Online Clients
Router
Wireless
Switches
Network
Switch List
Action
Hostname
IP
MAC
Status
Manage
ES209GC-P
192.168.110.3
C0:B8:E6:E6:8D:77
Online
NBS5200
192.168.110.74
54:16:51:76:EA:8F
Offline
NBS3100
192.168.110.2
C0:B8:E6:9A:43:0D
10/page
Collapse
System Info
Basic Settings
Upgrade
Loop Protection
Port Isolation
Port Settings
Port Settings
Port Mirroring
Static MAC
Search by MAC
VLAN Settings
VLAN Member
6
Add
Delete Selected
No.
VLAN ID
Action
1
1
Delete
VLAN Settings
QoS Settings
Rate Limiting

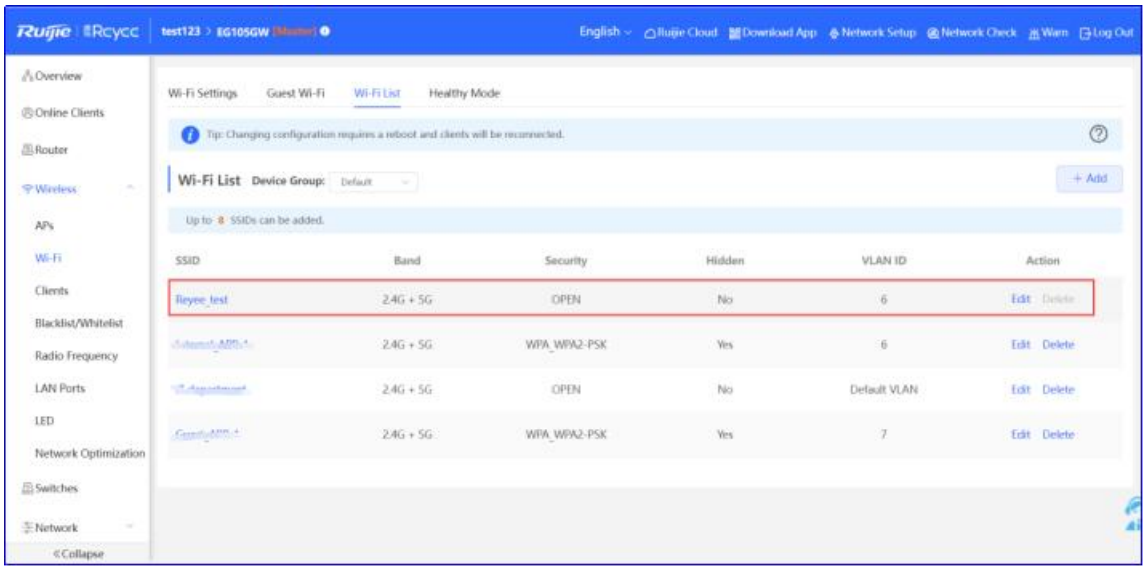

test123 > EG105GW (Master)
English
Overview
Online Clients
Router
Wireless
Switches
Network
Switch List
Action
Hostname
IP
MAC
Status
Manage
ES209GC-P
192.168.110.3
C0:B8:E6:E6:8D:77
Online
NBS5200
192.168.110.74
54:16:51:76:EA:8F
Offline
NBS3100
192.168.110.2
C0:B8:E6:9A:43:0D
10/page
Collapse
System Info
Basic Settings
Upgrade
Loop Protection
Port Isolation
Port Settings
Port Settings
Port Mirroring
Static MAC
Search by MAC
VLAN Settings
VLAN Member
VLAN Settings
* Port
Port 2 × Port 9 ×
Type
Trunk
Permit
All ×
* Native
VLAN 1
Save
Port
VLAN Type
Permit VLAN
Native Vlan
Access Vlan
1
Access
--
--
1
2
Access
--
--
1


test123 > EG105GW (Master)
English
Overview
Online Clients
Router
Wireless
Switches
Network
Switch List
Action
Hostname
IP
MAC
Status
Manage
ES209GC-P
192.168.110.3
C0:B8:E6:E6:8D:77
Online
NBS5200
192.168.110.74
54:16:51:76:EA:8F
Offline
NBS3100
192.168.110.2
C0:B8:E6:9A:43:0D
10/page
Collapse
System Info
Basic Settings
Upgrade
VLAN Settings
VLAN Member
VLAN Settings
* Port
Select
Type
Access
Permit
Select
* Access
Select
Save
Port
VLAN Type
Permit VLAN
Native Vlan
Access Vlan
1
Access
--
--
1
2
Trunk
1,6
1
--
3
Access
--
--
1
4
Access
--
--
1
QoS Settings
Rate Limiting
Storm Control
PoE Settings
PoE Settings



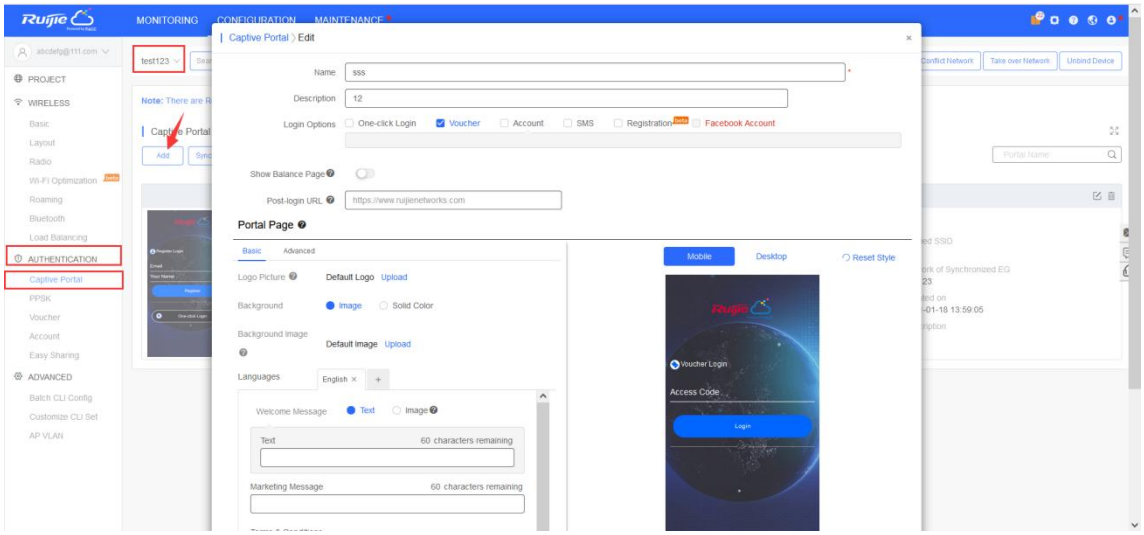
Step 3: Click **Wireless** -> **Wi-Fi** -> **Wi-Fi Settings, c**onfigure a SSID named as Reyee test and set VLAN6 to this SSID.

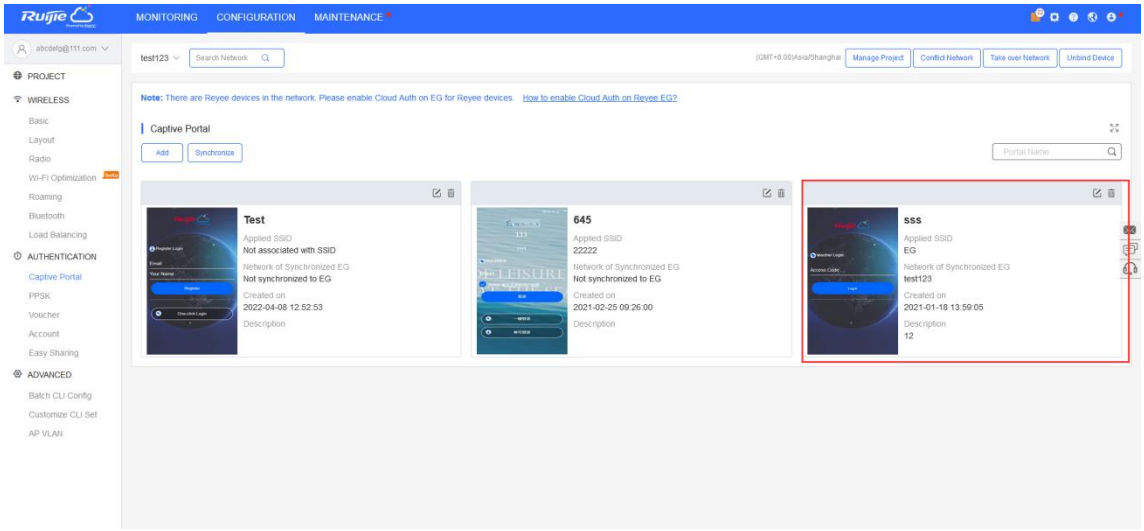




2. Configure cloud authentication

Step 1: Select **CONFIGURATION** -> **AUTHENTICATION** -> **Captive Portal** to open the Captive Portal page, and click **Add** to create a new portal template and edit the captive portal template.





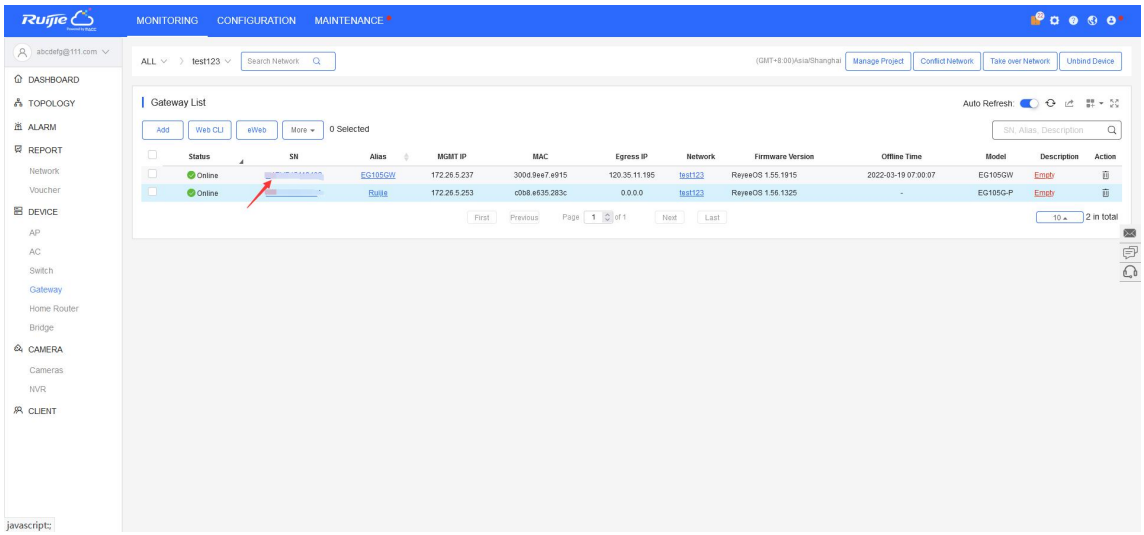
Note:

One-click Login: Login without username and password. Support to set the Access Duration and Access Times per day.

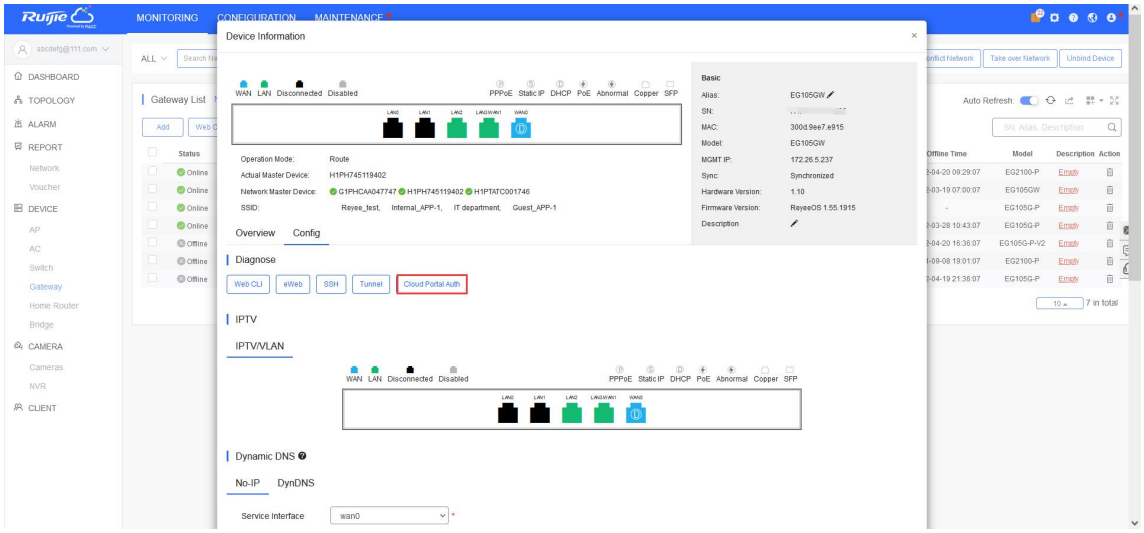
Voucher: Login with a random eight-digit password.

Account: Login with the account and password.

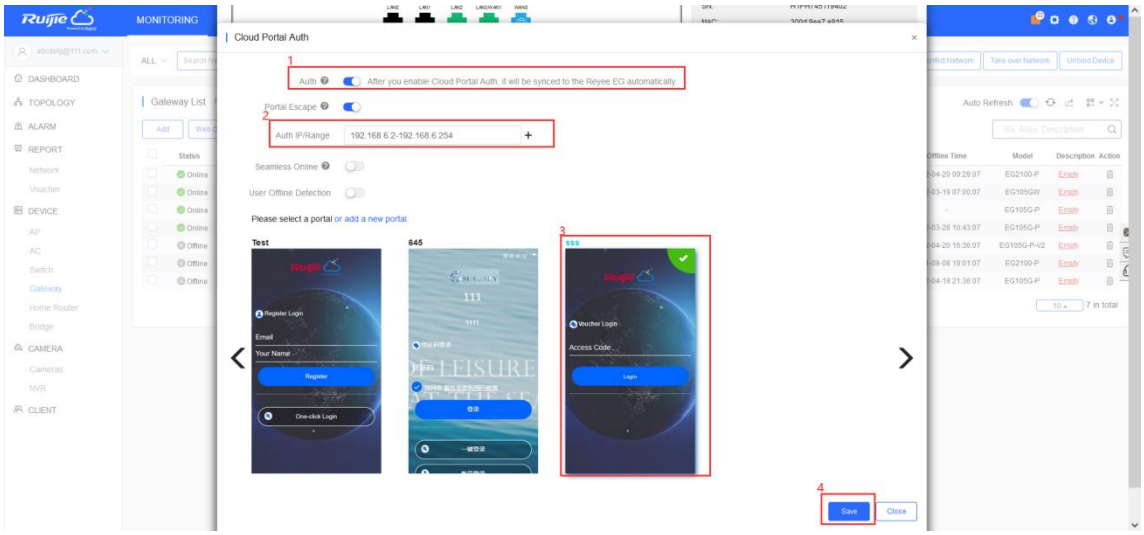
Step 2: Make sure the Reyee EG is online on Ruijie Cloud and click its SN in the list to enter the configure page



Step 3: Click **Cloud portal Auth** to configure the authentication on Cloud



Step 4: Enable **Auth** firstly, then set **Auth IP Range 192.168.6.2-192.168.6.254** which need to authenticate and choose the portal template to be used. In the end, click **Save** to save all configurations.

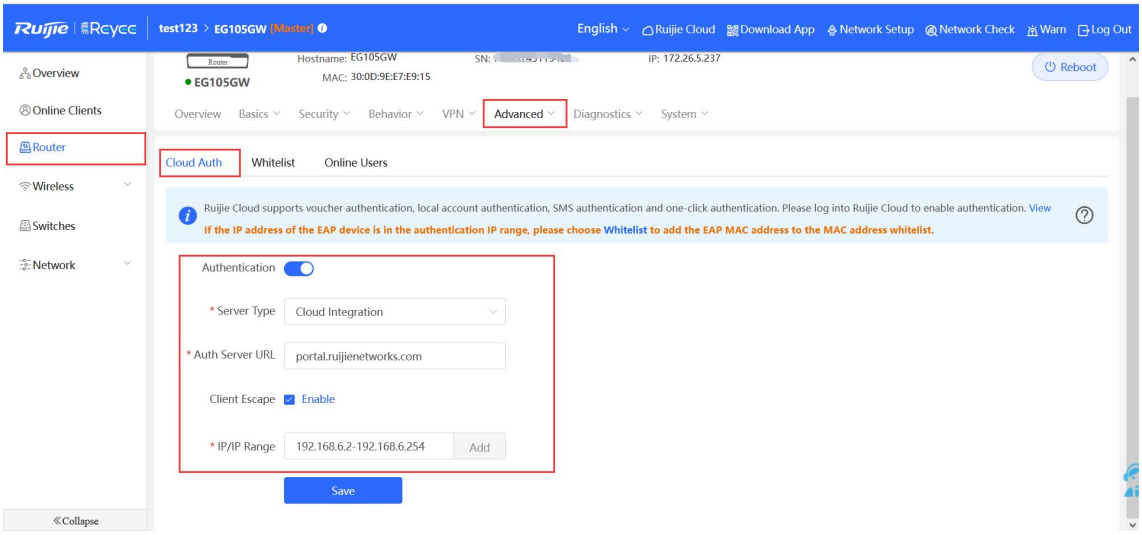


Note:

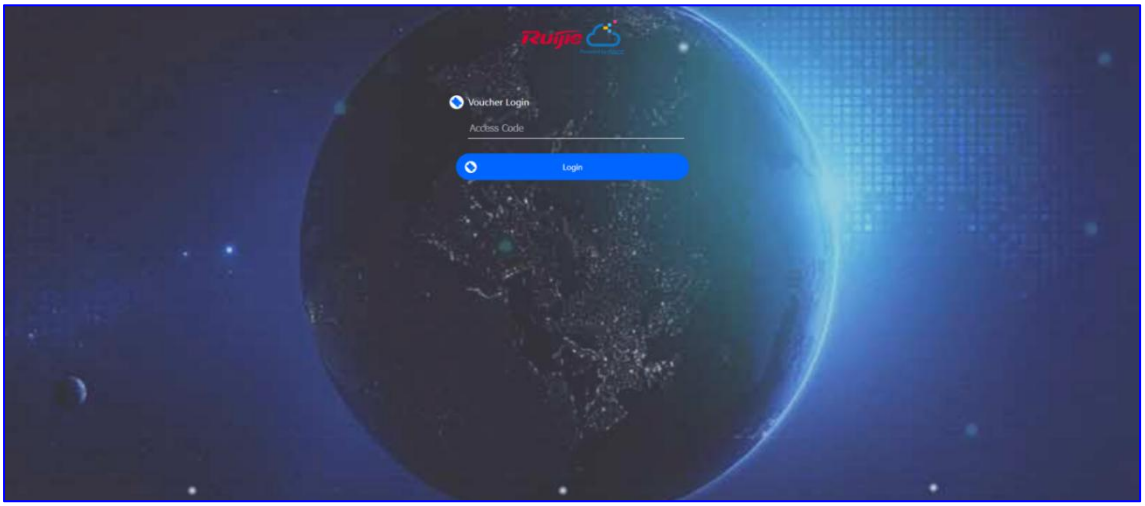
The EG, Switch and AP IP address needs to be excluded, otherwise the device will not be able to access the Internet.

Configuration Verification

1. Click **Router** -> **Advanced** -> **LAN** -> **Authentication** -> **Cloud Auth,** Check whether the configuration has been synchronized to EG.



2. Users which in 192.168.6.2-192.168.6.254 IP range are required to authenticate before accessing the Internet.



5.3 Reyee Guest WiFi Solution

5.3.1 Working Principle

Create a single internet entrance by using guest WiFi. The devices you allowed to access guest WiFi can access the internet but can’t access the home WiFi.

5.3.2 Application Scenario

Guest WiFi provides a secured Wi-Fi access for guests to share your home or office network. When someone visits your house, apartment, or workplace, you can enable the guest WiFi for them. You can set different access options for guest users, which is very effective to ensure the security and privacy of your main network.

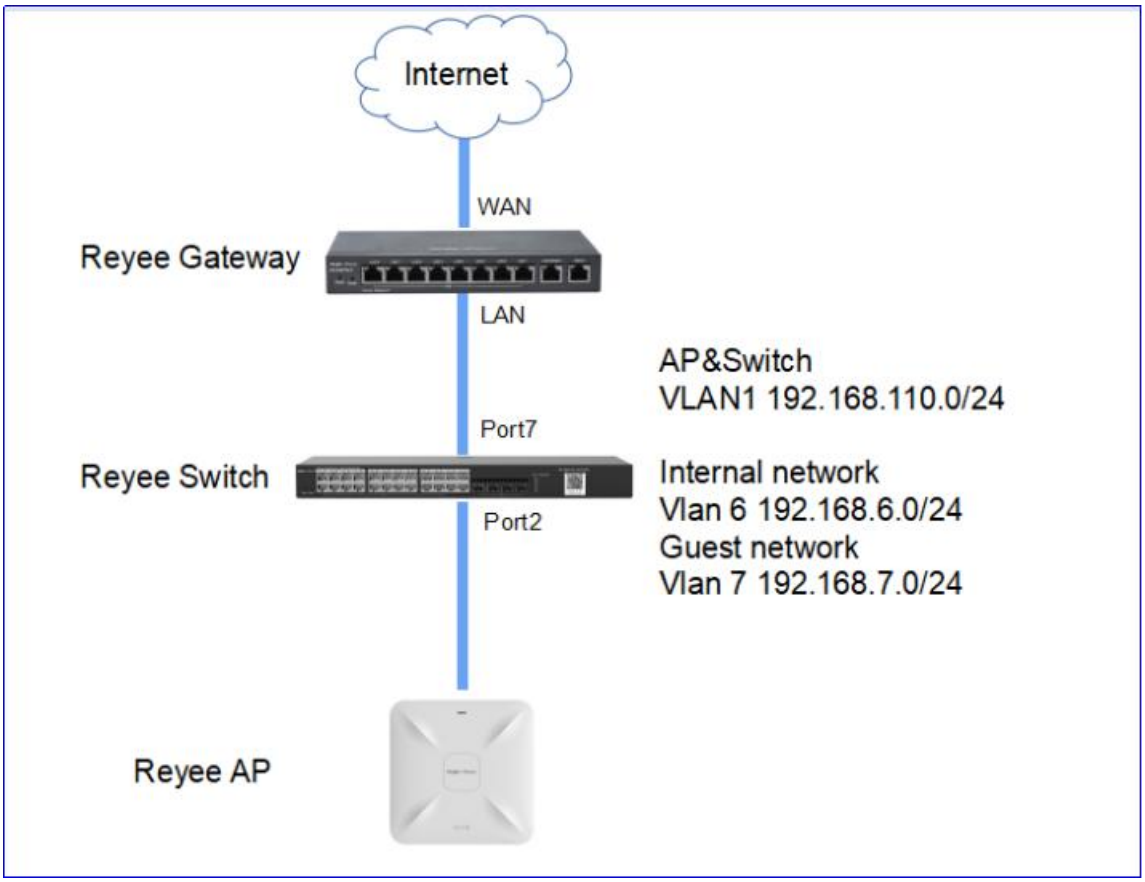
5.3.3 Configuration Case

5.3.3.1 Configuration via EG's eWeb

Requirement

Configure Guest WiFi for the Guest users in the VLAN7 network segment and the users will cannot access the internal network in the VLAN6 network segment.

Network Topology

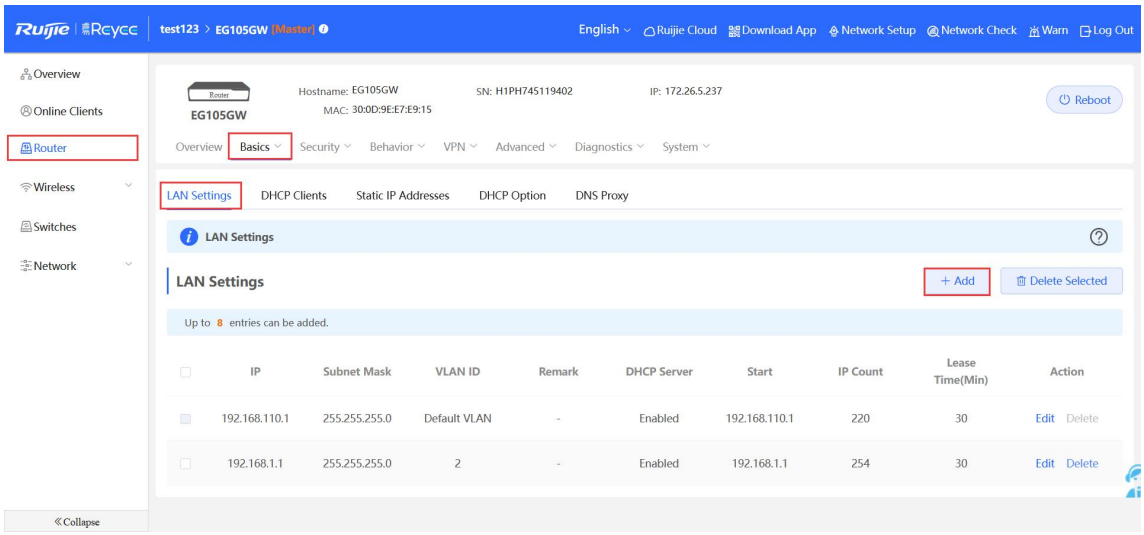


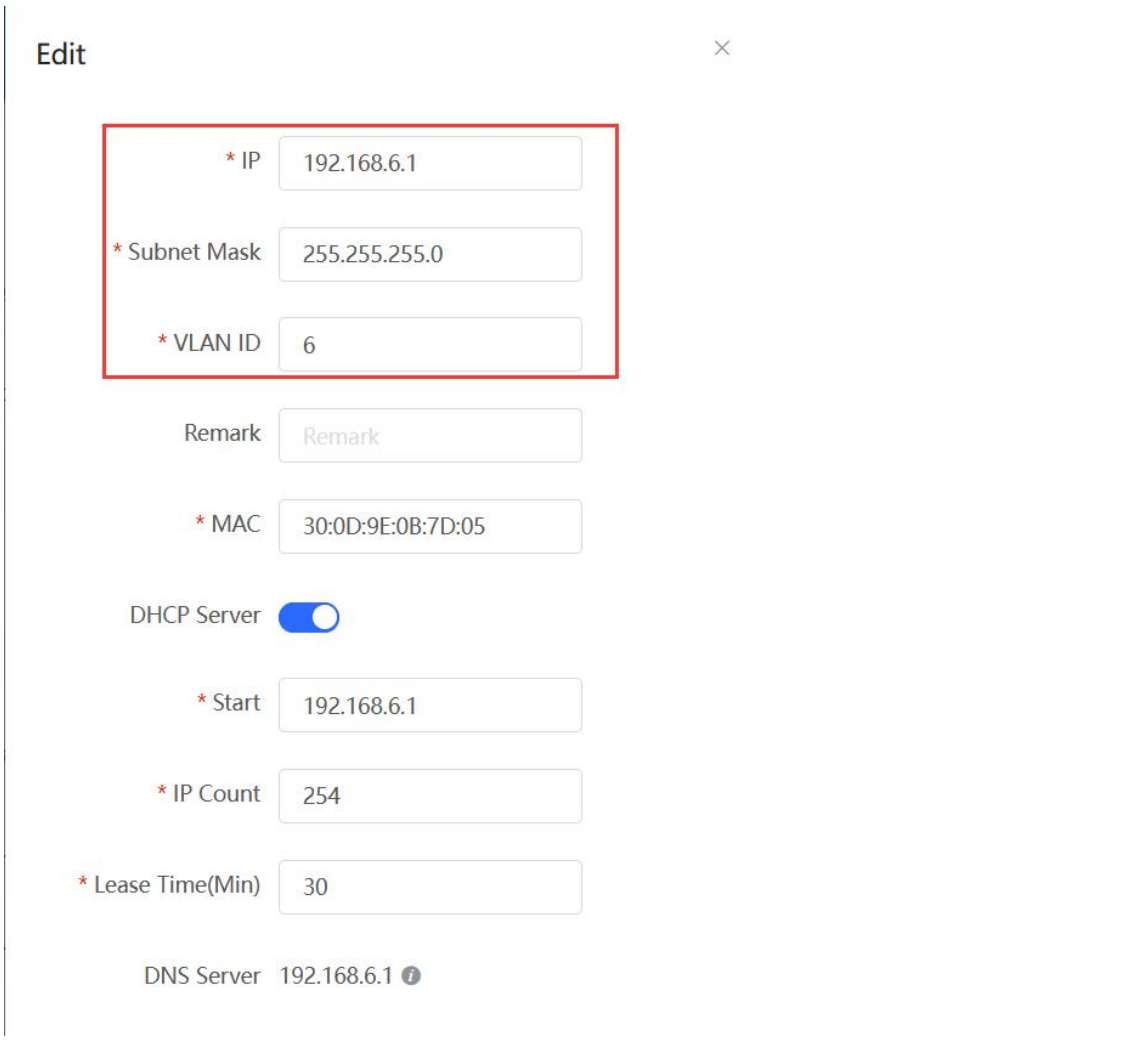
Network Description:

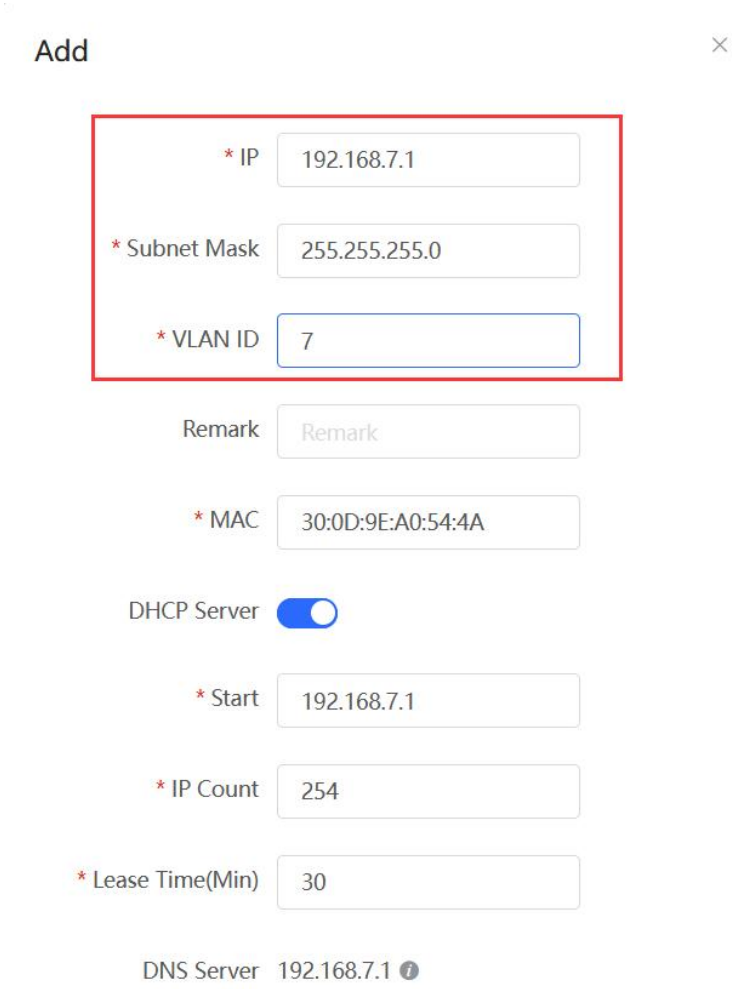
- EG works as a DHCP server to assign IP addresses to users and AP & switch devices
- The AP & switch devices obtain the IP address in the VLAN1 network segment for Internet access
- The internal users obtain the IP address in the VLAN6 network segment for Internet access and the guest user obtain the IP address in the VLAN7 network segment for Internet access

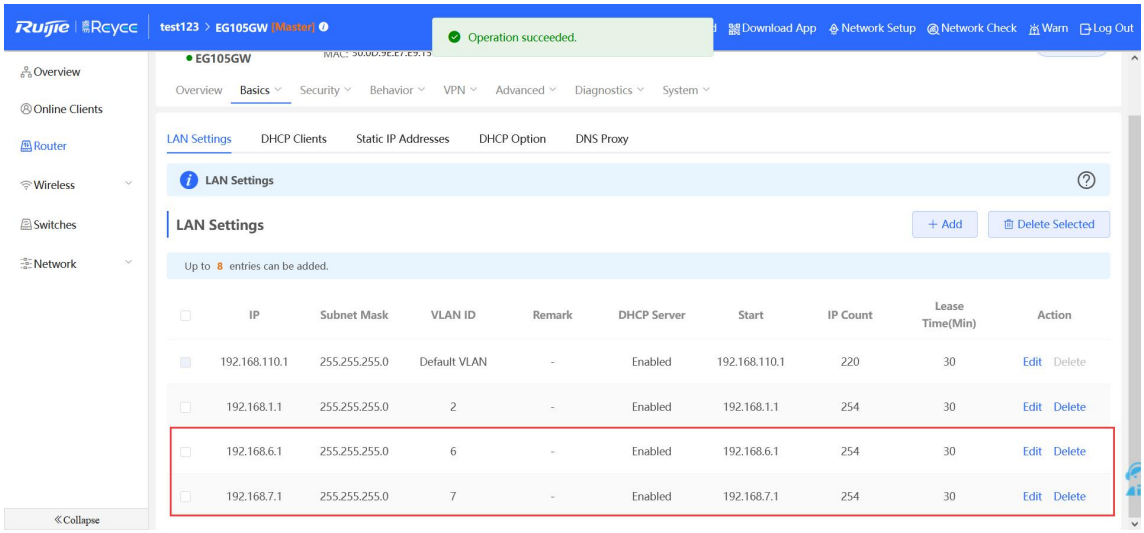
Configuration Steps

Step 1: Click **Router** -> **Basics** -> **LAN** -> **LAN Settings** -> **Add,** Configure LAN Settings and DHCP pool of VLAN 6 and VLAN 7 network segment on the EG

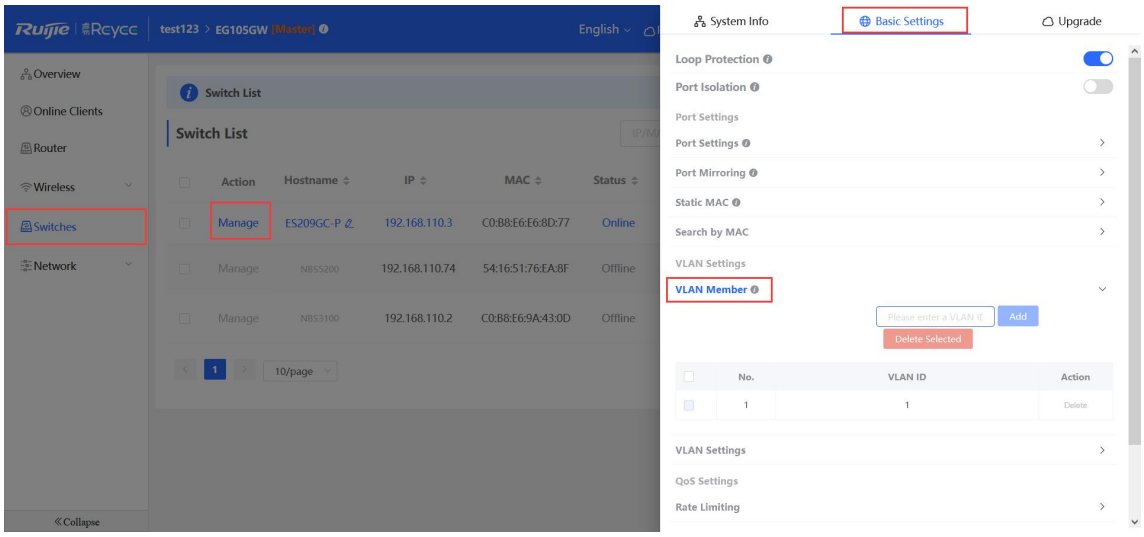

test123 > EG105GW (Master)
English
Ruijie Cloud
Download App
Network Setup
Network Check
Warn
Log Out
Overview
Online Clients
Router
Wireless
Switches
Network
Collapse
EG105GW
Hostname: EG105GW
MAC: 30:0D:9E:E7:E9:15
SN: H1PH745119402
IP: 172.26.5.237
Reboot
Overview
Basics
Security
Behavior
VPN
Advanced
Diagnostics
System
LAN Settings
DHCP Clients
Static IP Addresses
DHCP Option
DNS Proxy
LAN Settings
LAN Settings
+ Add
Delete Selected
Up to 8 entries can be added.
IP
Subnet Mask
VLAN ID
Remark
DHCP Server
Start
IP Count
Lease Time(Min)
Action
192.168.110.1
255.255.255.0
Default VLAN
Enabled
192.168.110.1
220
30
Edit
Delete
192.168.1.1
255.255.255.0
2
Enabled
192.168.1.1
254
30
Edit
Delete

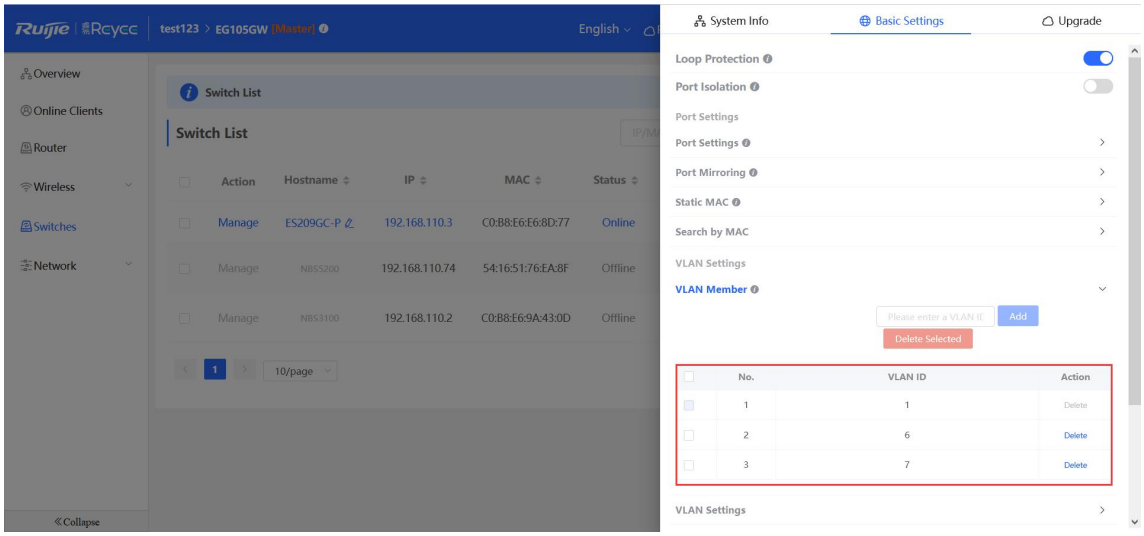

Edit
* IP
192.168.6.1
* Subnet Mask
255.255.255.0
* VLAN ID
6
Remark
Remark
* MAC
30:0D:9E:0B:7D:05
DHCP Server
* Start
192.168.6.1
* IP Count
254
* Lease Time(Min)
30
DNS Server
192.168.6.1

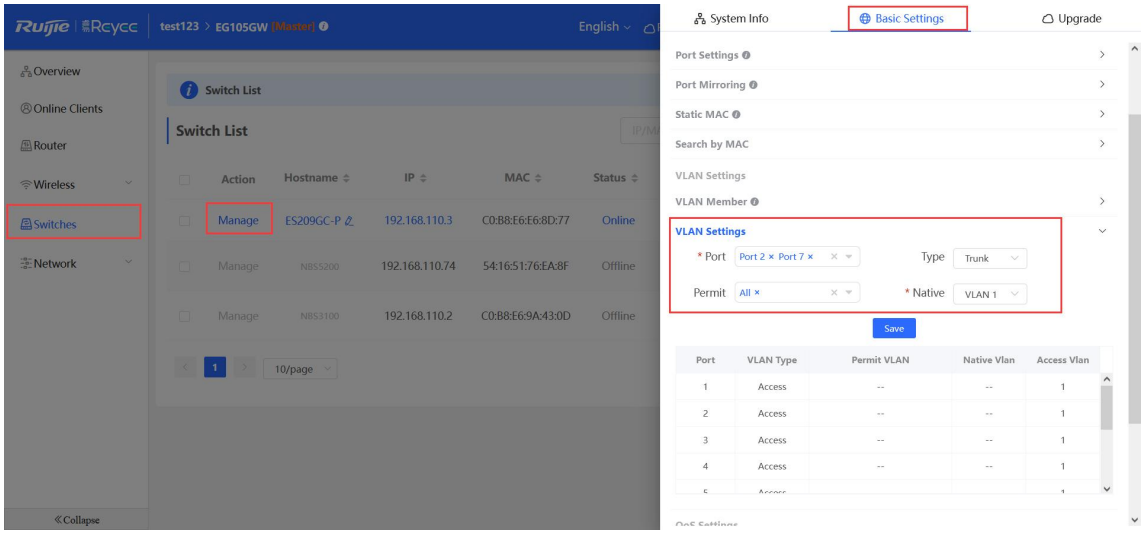


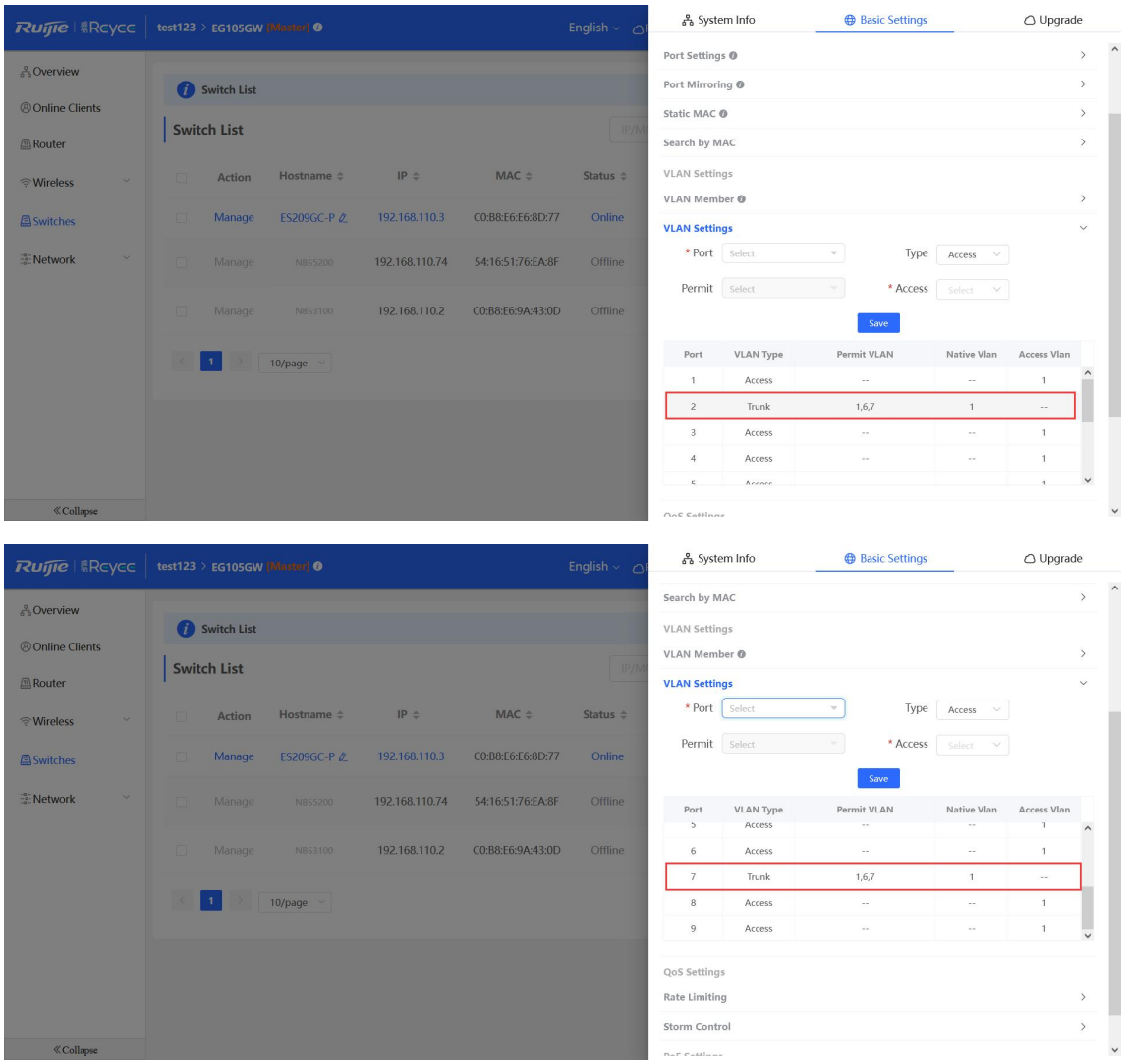


Step 2: Click **Switches** -> **Manage** -> **Basic Settings** -> **VLAN Member** to create VLAN 6 and VLAN 7 on the switch, and click **VLAN Settings** to set port 2 and port 7 to trunk port which connect to AP and EG and allow VLAN 1、VLAN 6 and VLAN 7 to pass through, then check the port settings on the device.

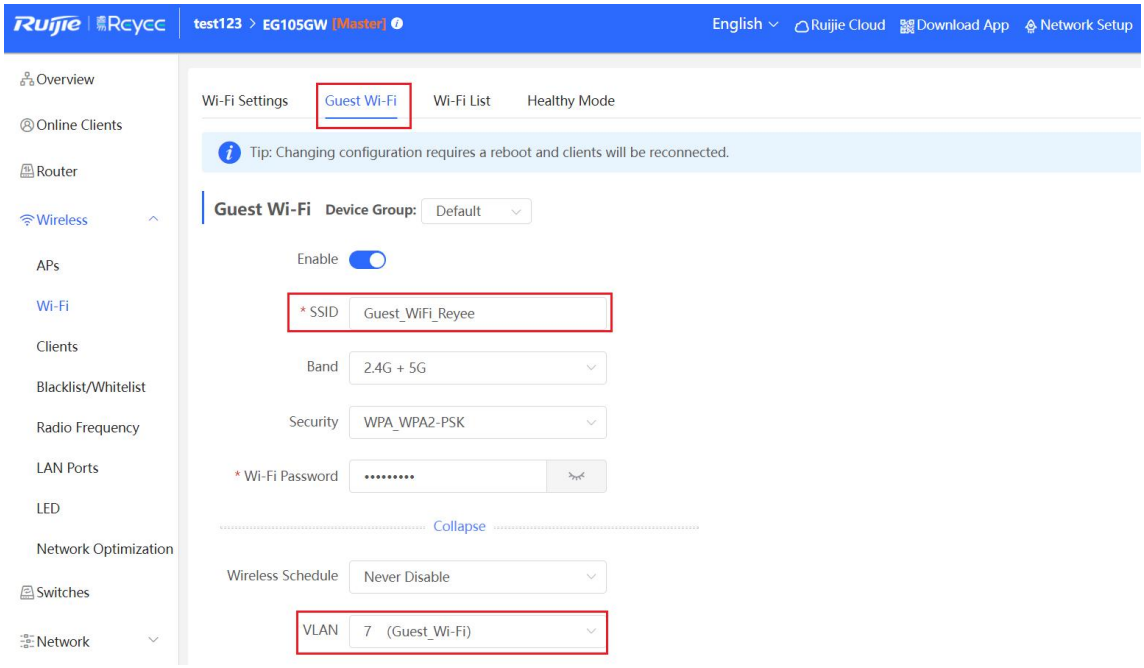

test123 > EG105GW (Master)
English
Overview
Online Clients
Router
Wireless
Switches
Network
Collapse
Switch List
Switch List
Action
Hostname
IP
MAC
Status
Manage
ES209GC-P
192.168.110.3
C0:B8:E6:E6:8D:77
Online
Manage
NBS5200
192.168.110.74
54:16:51:76:EA:8F
Offline
Manage
NBS3100
192.168.110.2
C0:B8:E6:9A:43:0D
Offline
10/page
System Info
Basic Settings
Upgrade
Loop Protection
Port Isolation
Port Settings
Port Settings
Port Mirroring
Static MAC
Search by MAC
VLAN Settings
VLAN Member
Add
Delete Selected
No.
VLAN ID
Action
1
1
Delete
VLAN Settings
QoS Settings
Rate Limiting


test123 > EG105GW (Master)
English
Overview
Online Clients
Router
Wireless
Switches
Network
Collapse
Switch List
Switch List
Action
Hostname
IP
MAC
Status
Manage
ES209GC-P
192.168.110.3
C0:B8:E6:E6:8D:77
Online
Manage
NBS5200
192.168.110.74
54:16:51:76:EA:8F
Offline
Manage
NBS3100
192.168.110.2
C0:B8:E6:9A:43:0D
Offline
10/page
System Info
Basic Settings
Upgrade
Loop Protection
Port Isolation
Port Settings
Port Settings
Port Mirroring
Static MAC
Search by MAC
VLAN Settings
VLAN Member
Add
Delete Selected
No.
VLAN ID
Action
1
1
Delete
2
6
Delete
3
7
Delete
VLAN Settings

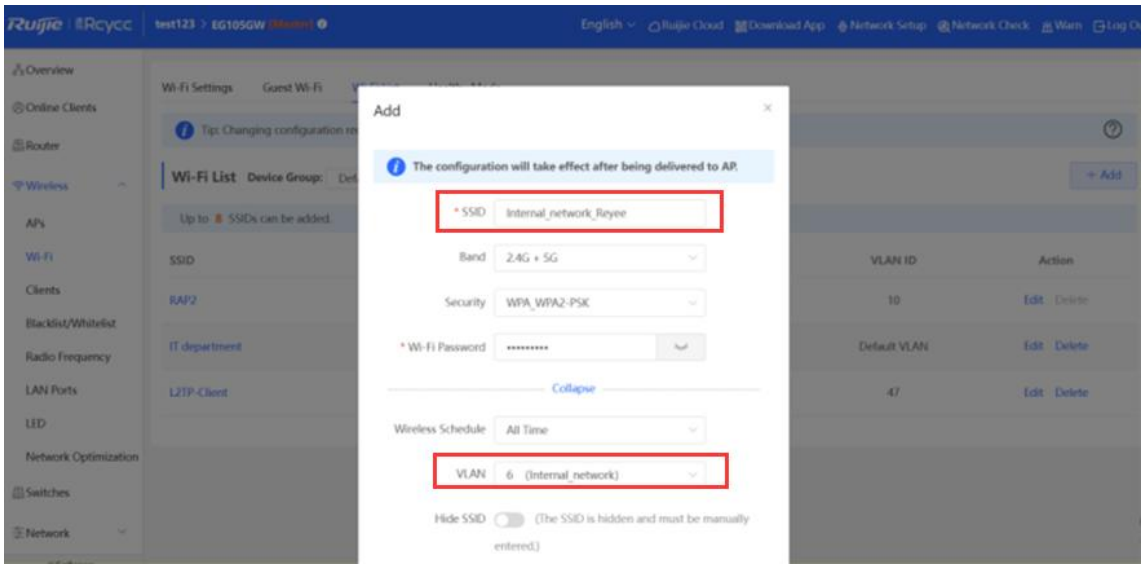

test123 > EG105GW (Master)
English
Overview
Online Clients
Router
Wireless
Switches
Network
Collapse
Switch List
Switch List
Action
Hostname
IP
MAC
Status
Manage
ES209GC-P
192.168.110.3
C0:B8:E6:E6:8D:77
Online
Manage
NBS5200
192.168.110.74
54:16:51:76:EA:8F
Offline
Manage
NBS3100
192.168.110.2
C0:B8:E6:9A:43:0D
Offline
10/page
System Info
Basic Settings
Upgrade
Port Settings
Port Mirroring
Static MAC
Search by MAC
VLAN Settings
VLAN Member
VLAN Settings
* Port
Port 2 × Port 7 ×
Type
Trunk
Permit
All ×
* Native
VLAN 1
Save
Port
VLAN Type
Permit VLAN
Native Vlan
Access Vlan
1
Access
--
--
1
2
Access
--
--
1
3
Access
--
--
1
4
Access
--
--
1

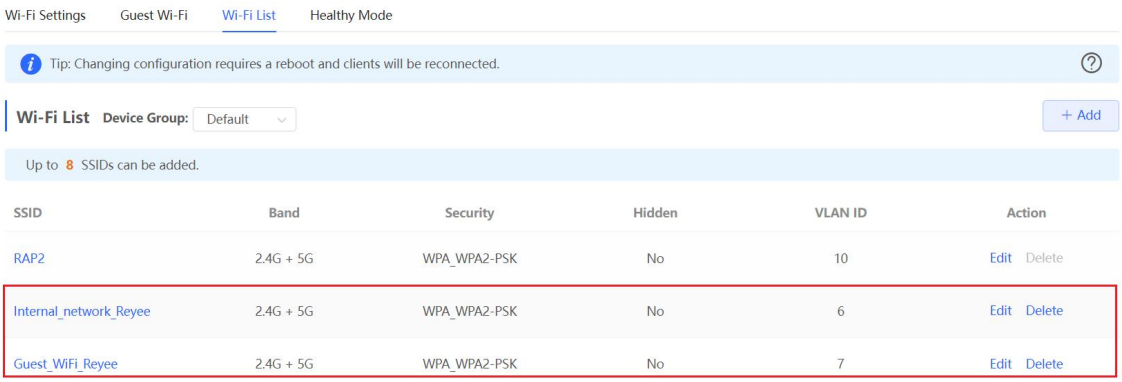


Step 3: Click **Wireless-> Wi-Fi -> Guest WiFi,** configure a Guest WiFi SSID named as Guest_WiFi_Reyee and set VLAN 7 to this SSID.

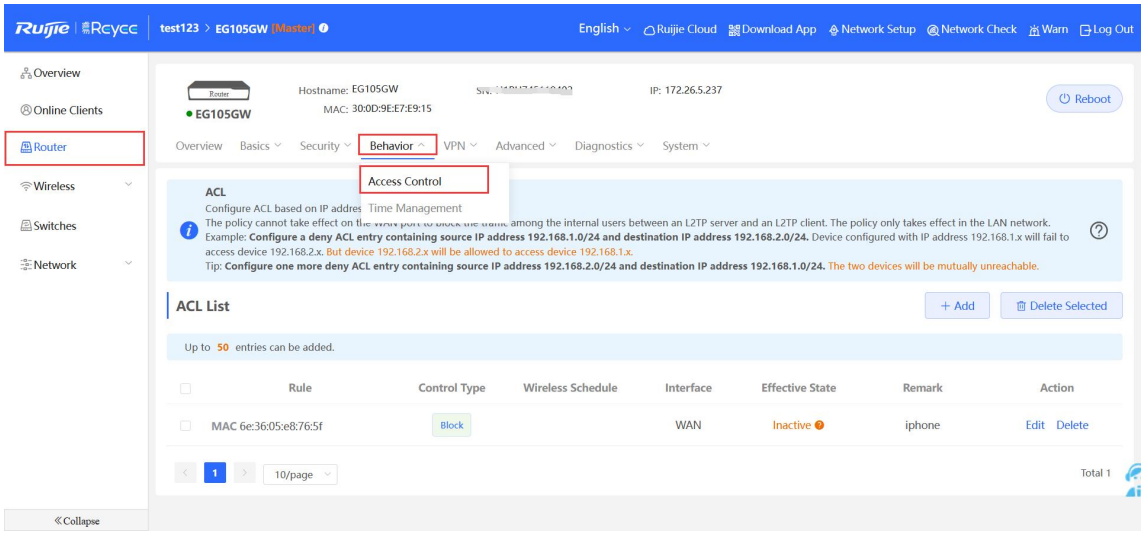


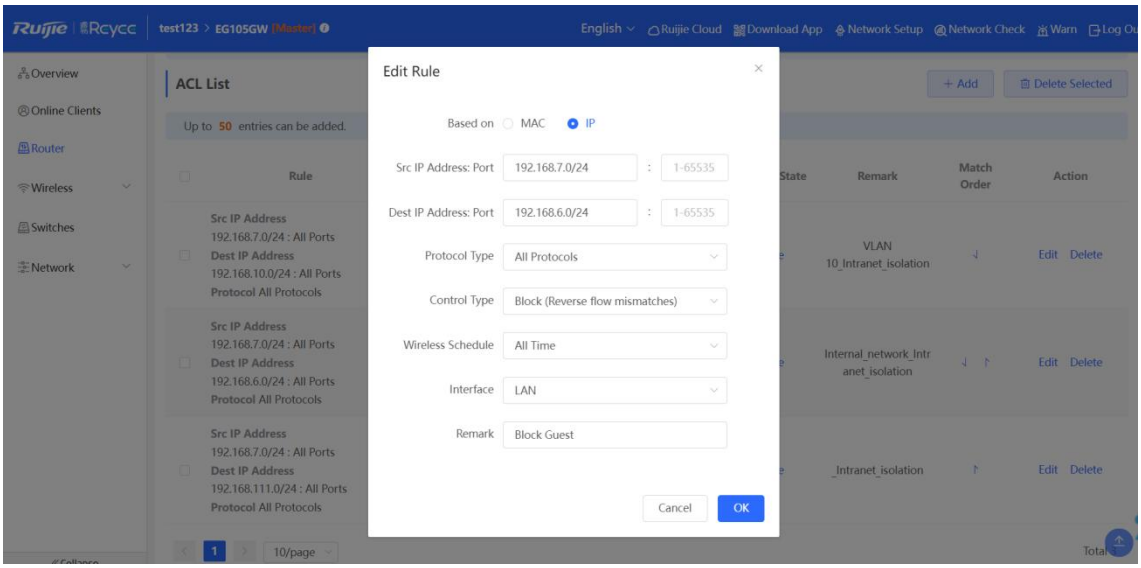
Step 4: Click **Wireless** ->**Wi-Fi** ->**Wi-Fi List** ->**Add c**onfigure the internal user SSID named as Internal_network_Reyee and set VLAN6 to this SSID and check the WiFi settings on the WiFi list.

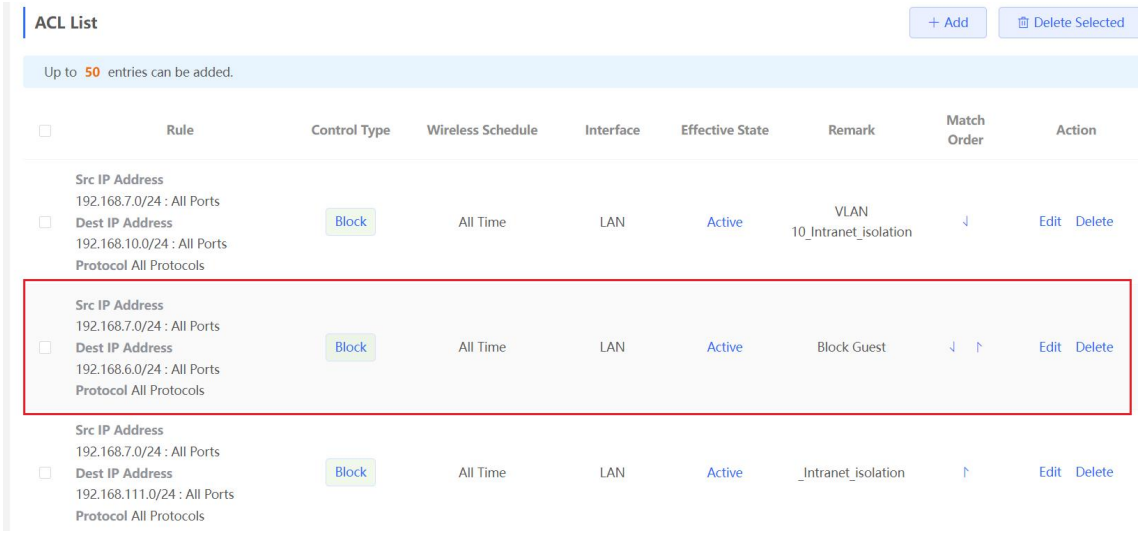




Step 5: Click **Router** -> **Behavior** -> **Access Control**, configure ACL to block the traffic from guest user of vlan7 network 192.168.7.0/24 to internal user of VLAN 6 192.168.6.0/24 and apply to LAN interface on EG.







Configuration Verification

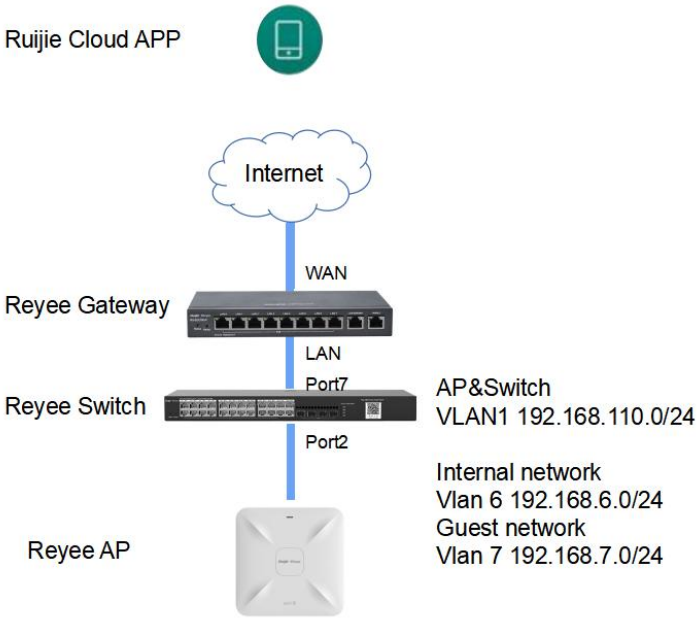
Guest network users 192.1687.2 can’t access the internal network users 192.168.6.2.

5.3.3.2 Configure via Ruijie Cloud APP

Requirement

Configure Guest WiFi via Ruijie Cloud APP for Guest users in the VLAN7 network segment which cannot access the internal network in the VLAN6 network segment. Ruijie Cloud APP will deliver the corresponding configuration to device automatically..

Network Topology

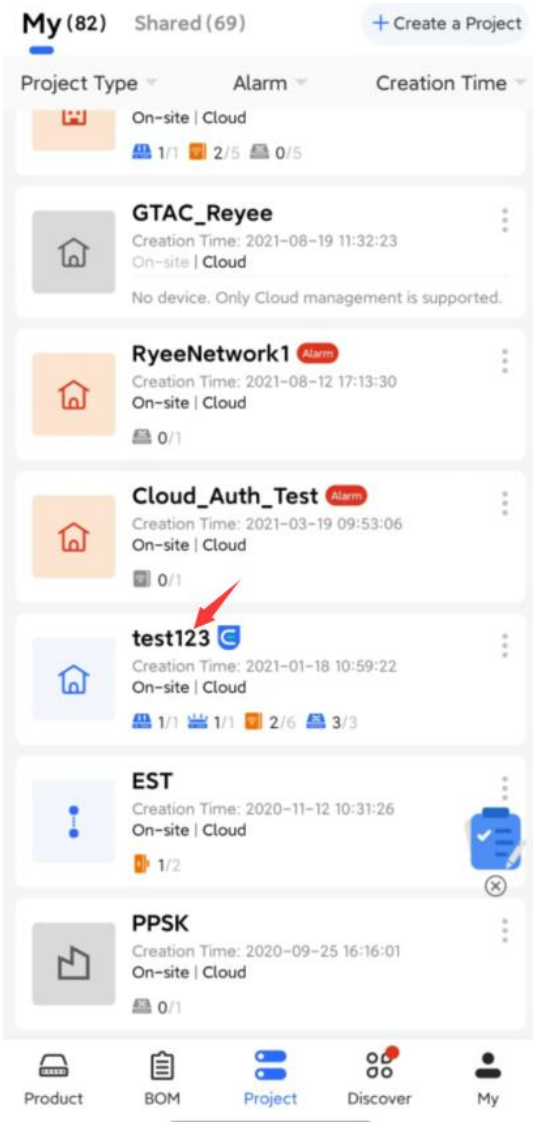


Network Description:

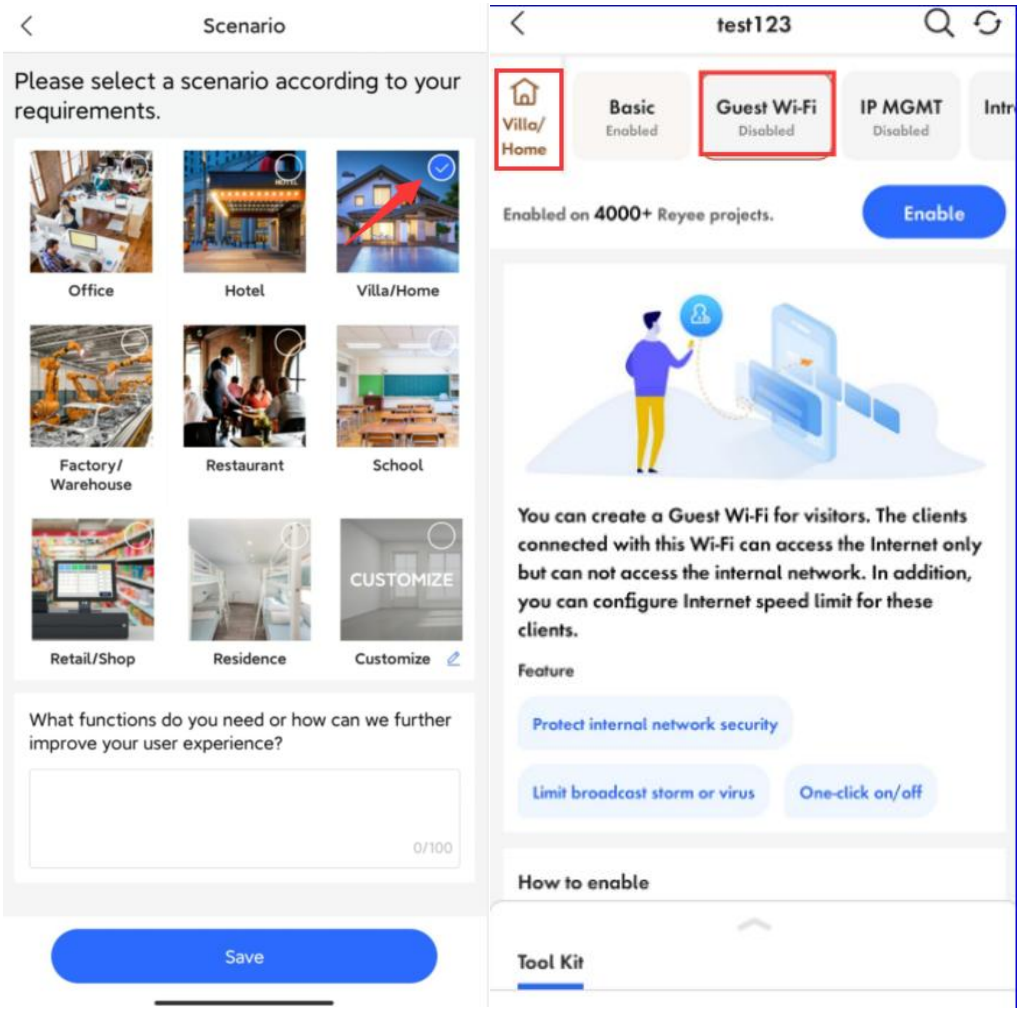
- EG works as a DHCP server to assign IP addresses to users and AP & switch devices
- The AP & switch devices obtain the IP address in the VLAN1 network segment for Internet access
- The internal users obtain the IP address in the VLAN6 network segment for Internet access and the guest user obtain the IP address in the VLAN7 network segment for Internet access

Configuration Steps

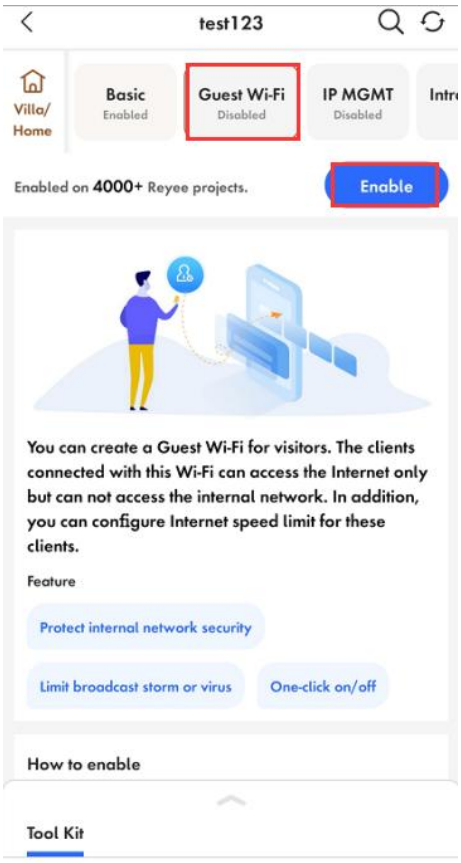
Step1: Login to your Ruijie Cloud APP on smartphone then enter the project with Reyee gateway + RAP



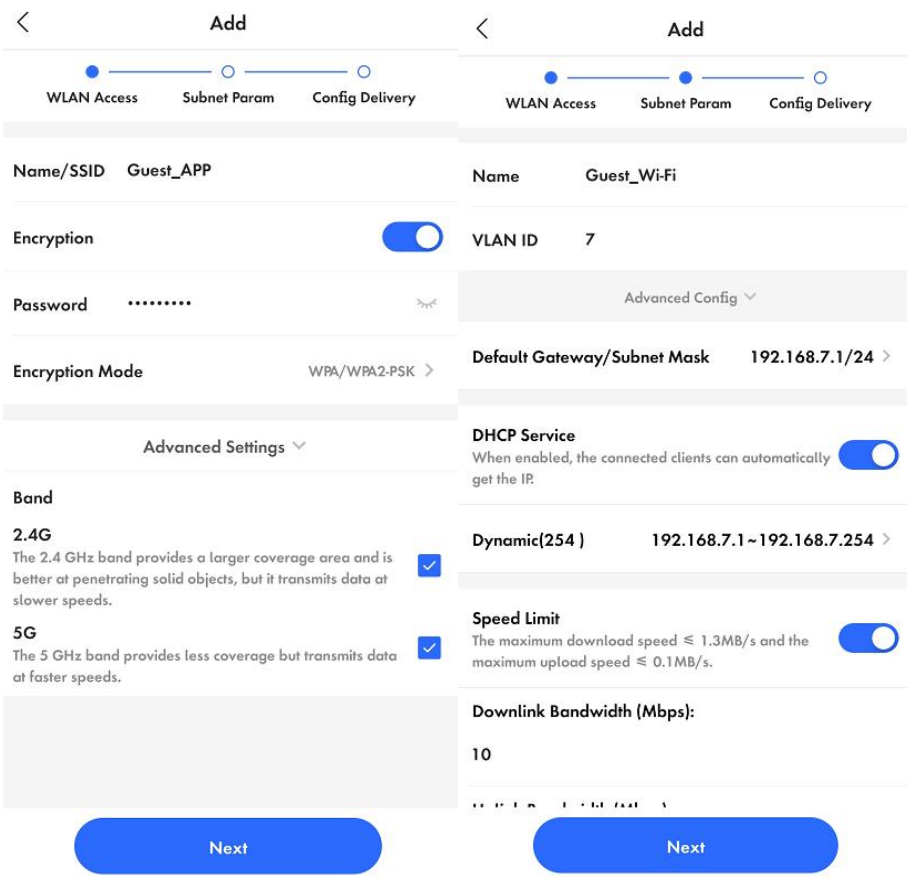
Step2: Choose Villa/Home scenario then you can see Guest Wi-Fi button.



Step3: Select Guest Wi-Fi function and click **Enable** button.

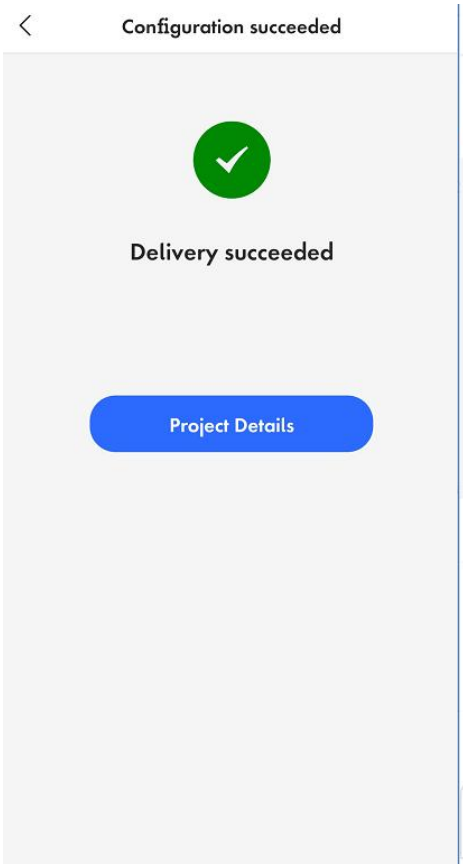


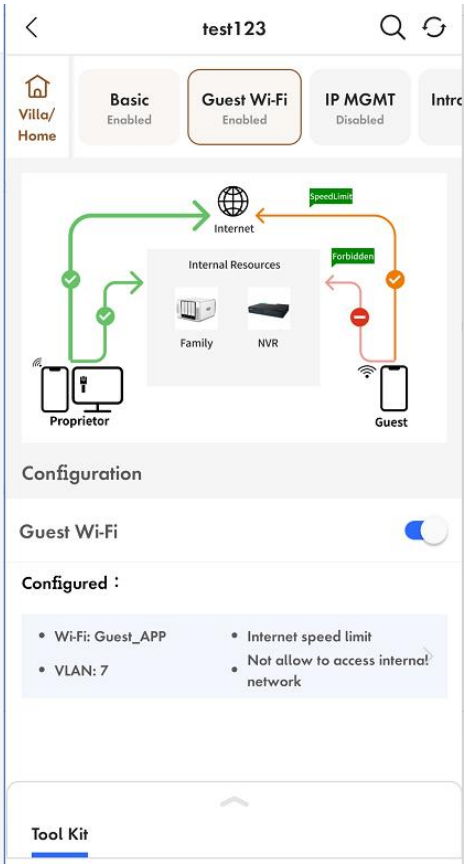
Step4: Modify Guest Wi-Fi information, configure a Internal user SSID named as Guest_APP and set VLAN6 to this SSID and configure a Guest WiFi SSID named as Guest_WiFi and set VLAN7 to this SSID, then Click Save to save your configuration.



Step4: Waiting around 1 minute for system delivering the configuration to device.


Configuration Delivery
46s
Configuring...
Please wait.
ES209GC-P_ES209GC-P
Switch SN:CAPC0YL008237
Switch configPort ID: [Port 7] Waiting
Switch configPort ID: [Port 2] Waiting
Switch configPort ID: [Port 1, Port 3, Port 4,··· Waiting
Switch configAdded VLAN 7 Configuring
RAP2260(E)_RAP2260(E)
AP SN:G1QH6WX000534
Update EasyNetwork wireless config Con··· Configuring
EG105GW_EG105GW
Gateway SN:H1PH745119402
Update ACL configREJECT Source IP/Netw··· Waiting
Update IP traffic controlDevice: H1PH745··· Waiting
Update global traffic control Configuratio··· Waiting
Update LAN config Configuration: [{"dhcp··· Waiting
Update EasyNetwork wireless config Con··· Configuring


Configuration succeeded
Delivery succeeded
Project Details


test123
Villa/ Home
Basic
Enabled
Guest Wi-Fi
Enabled
IP MGMT
Disabled
Internet
SpeedLimit
Internal Resources
Forbidden
Family
NVR
Proprietor
Guest
Configuration
Guest Wi-Fi
Configured :
Wi-Fi: Guest_APP
VLAN: 7
Internet speed limit
Not allow to access internal network
Tool Kit

Configuration Verification

The guest user 192.168.7.97 can't be able to access the internal user 192.168.6.147.

5.4 Reyee SON—Self-Organizing Network

Self-organizing network 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 networks, which greatly reduces the investment of equipment cost, labor cost and time cost in the process of wireless network construction.

5.4.1 The principle of Reyee SON

5.4.1.1 Network ID

Every device has its own network ID.

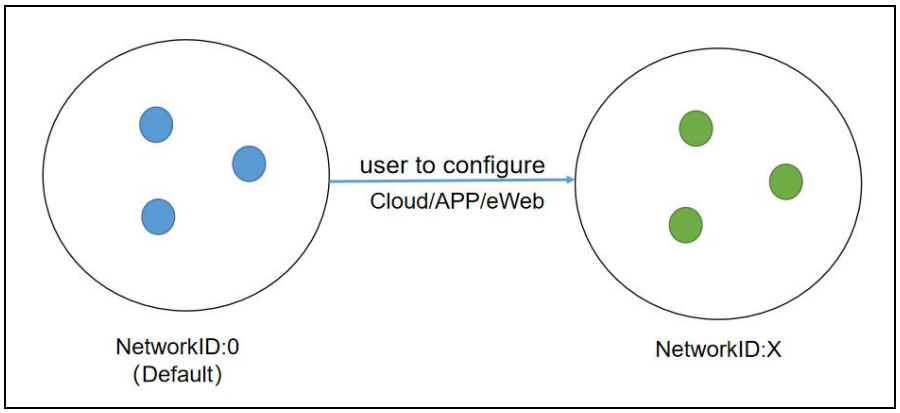
Only devices with the same networkID can be added to a network.

Devices with different networkID should be merged before added to the same network.

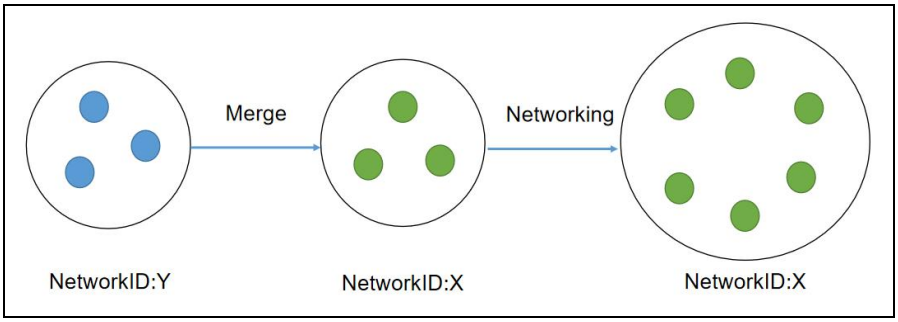
The network ID is 0 by default.

After the device is configured, it will have a new network ID(networkid is non-zero).

After configure:



Merge:



5.4.1.2 Protocol

Easydisc

Responsible for neighbor discovery, master election, and notification of master changes.

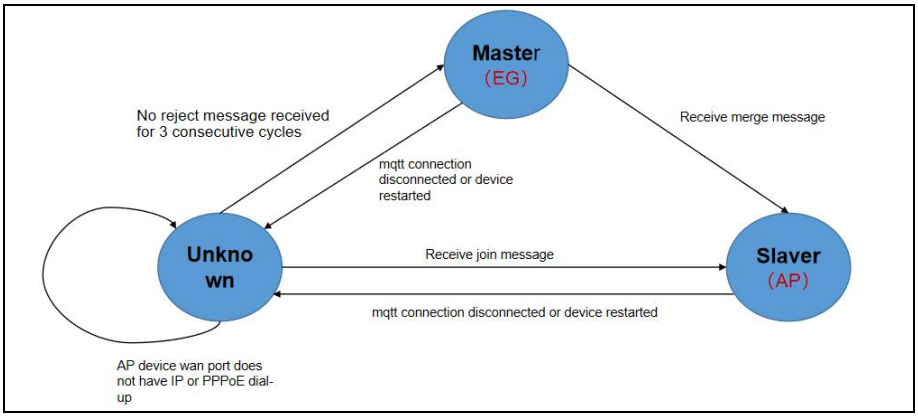
Easydisc is a proprietary protocol and uses UDP port numbers 43561 and 43562 for communication.

MQTT

Responsible for the collection of networking equipment information, the collection of STA information, and the synchronization of configuration information.

MQTT is a standard protocol and uses TCP port number 1883 for communication.

5.4.1.3 Easydisc – Role



5.4.1.4 Easydisc- packet

Packet type:

Declare: broadcast; in the Initial state, broadcast declares message; send its own priority and other related information.

Reject: unicast; when receiving the decade message, according to the election priority, if its own priority is higher, it will reply reject.

Join: broadcast; sent by the master, when other initial states receive the message, they will connect to the master according to the master information in it.

Conflict: unicast; the master sends a conflict message when it receives a join message from another master and cannot be resolved according to the conflict handling algorithm.

Merge: unicast; the master sends a merge message when it receives a join message from other masters and can merge the other party's network according to the conflict handling algorithm.

Hello: broadcast; all devices start broadcasting hello packets after the role status is confirmed for neighbor discovery.

5.4.1.5 Master election roles

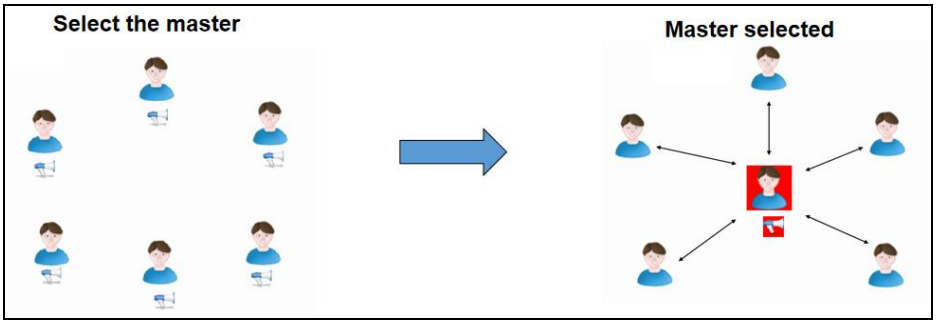
Priority:

(1) EG > AP > SW

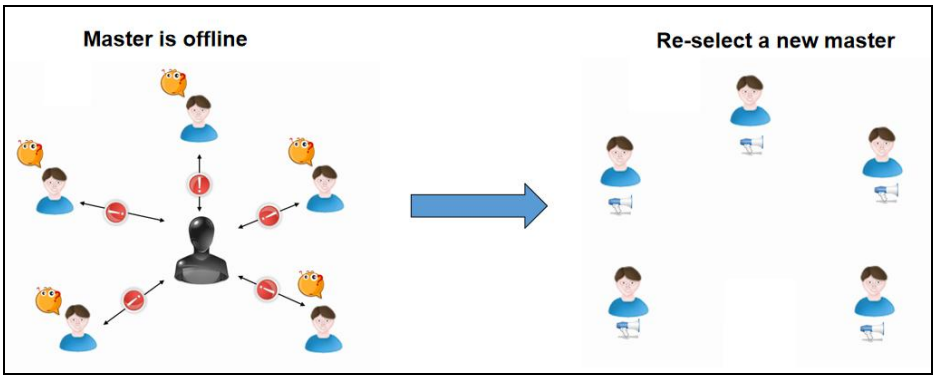
(2) Device model: device CPU/Memory/other(AP radio number)

(3) When the priorities are the same, the larger MAC address will be the master.

Select the Master:



Re-select the Master:



5.4.1.6 Master preemption mechanism

If a device with a higher priority joins a network, the master device will change. The new device will send a merge packet to the master device.

1.For AP networking, after the master is selected, if a new EG is added, EG will become the master.

Delay time: 7-8s

2.For AP networking, after the master is selected, if a new AP with a higher priority is added, the preempt is delayed.

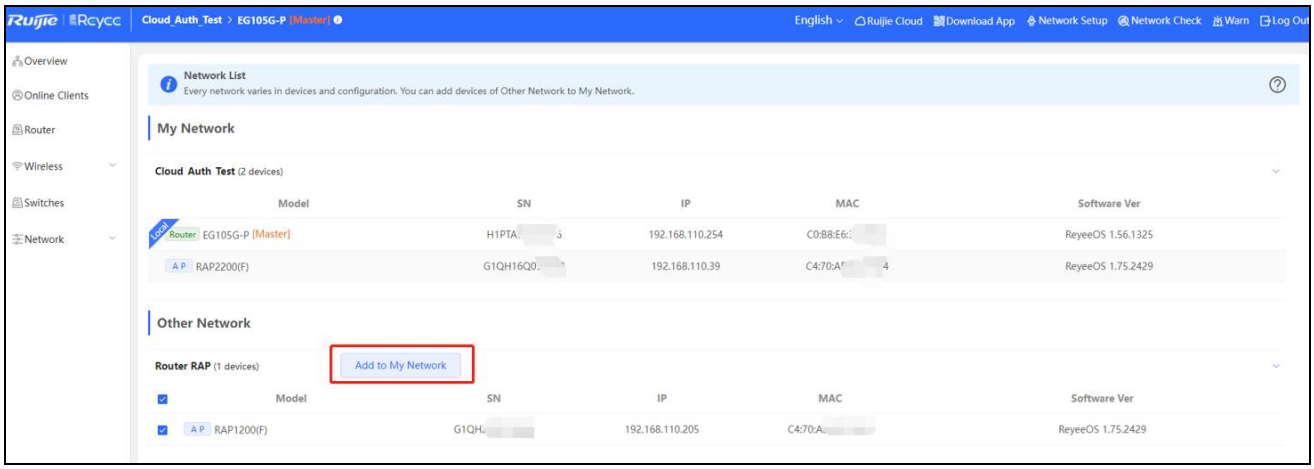
Delay time: preemption starts after the master is powered on for 36 hours and the new device is powered on for 5 minutes; otherwise, preemption starts after the new device is powered on for 30 minutes.

3. For AP+SW networking, after the master is selected, if a new EG is added, EG will become the master.

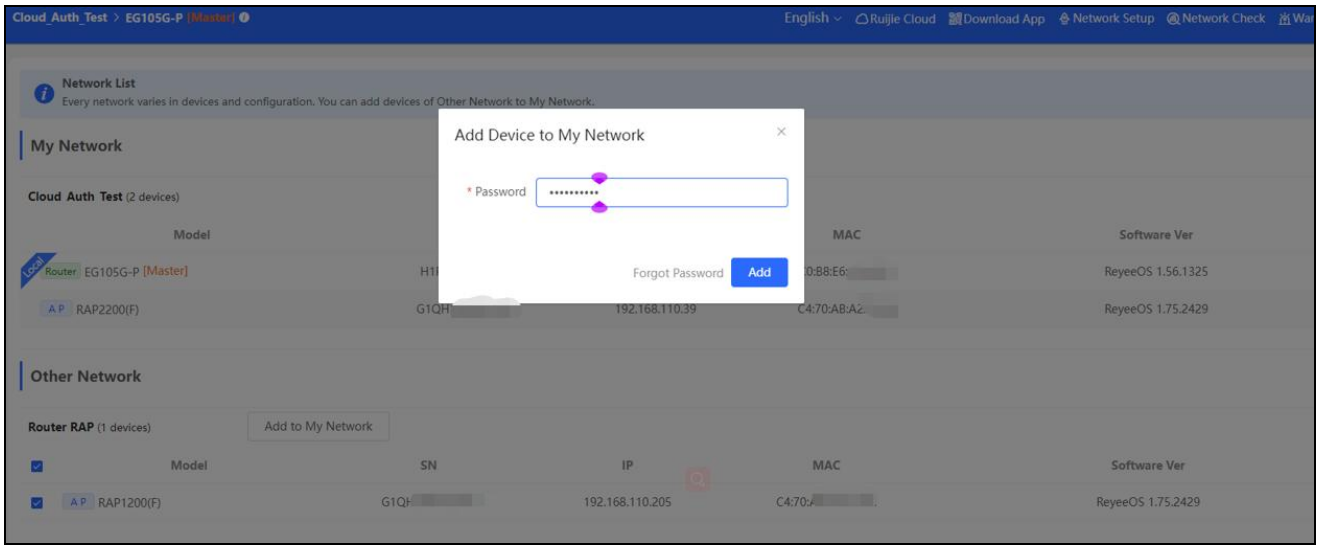
5.4.2 The configuration of Reyee SON

5.4.1.1 Neighbor Discovery

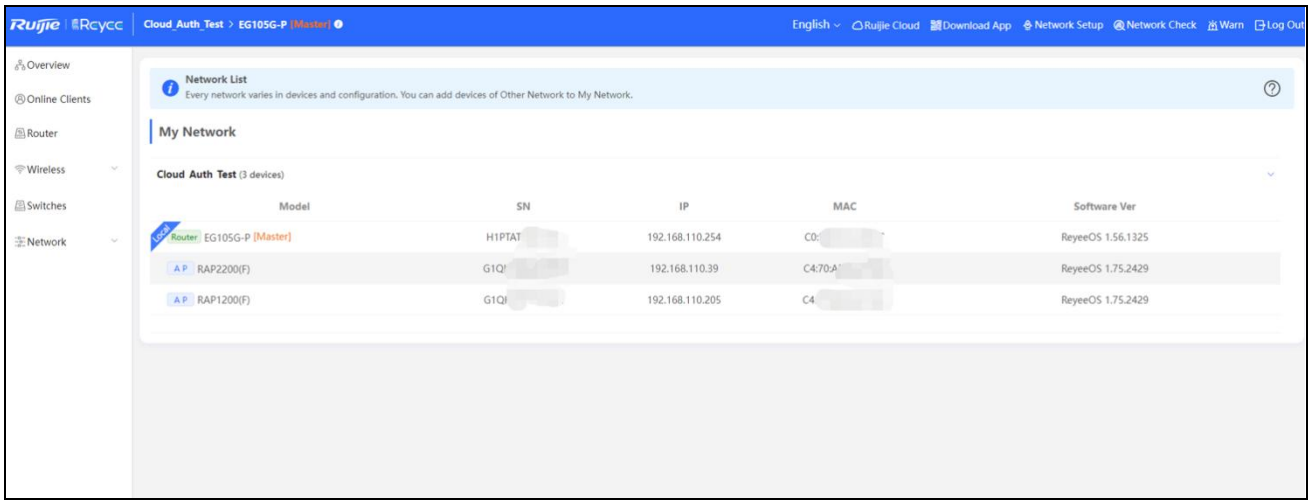
Add devices of other networks to **My Network**.



Enter the password of device.

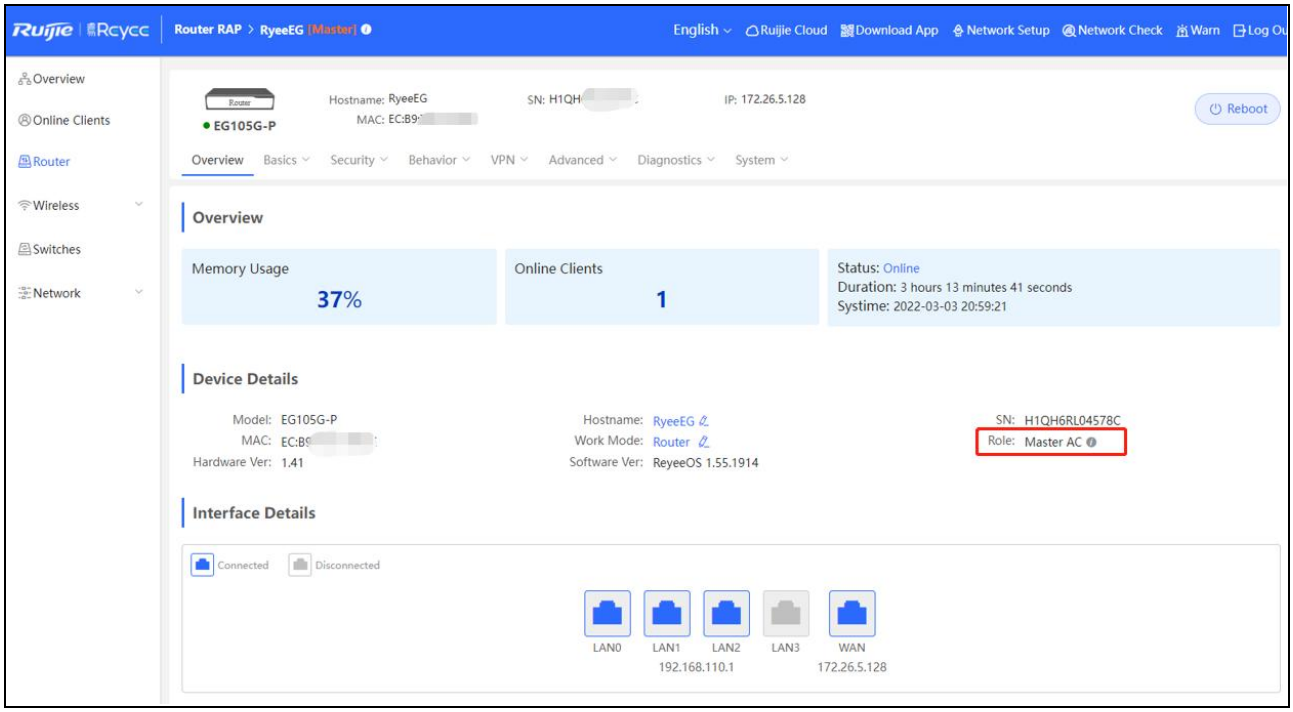


Device is added to the network.

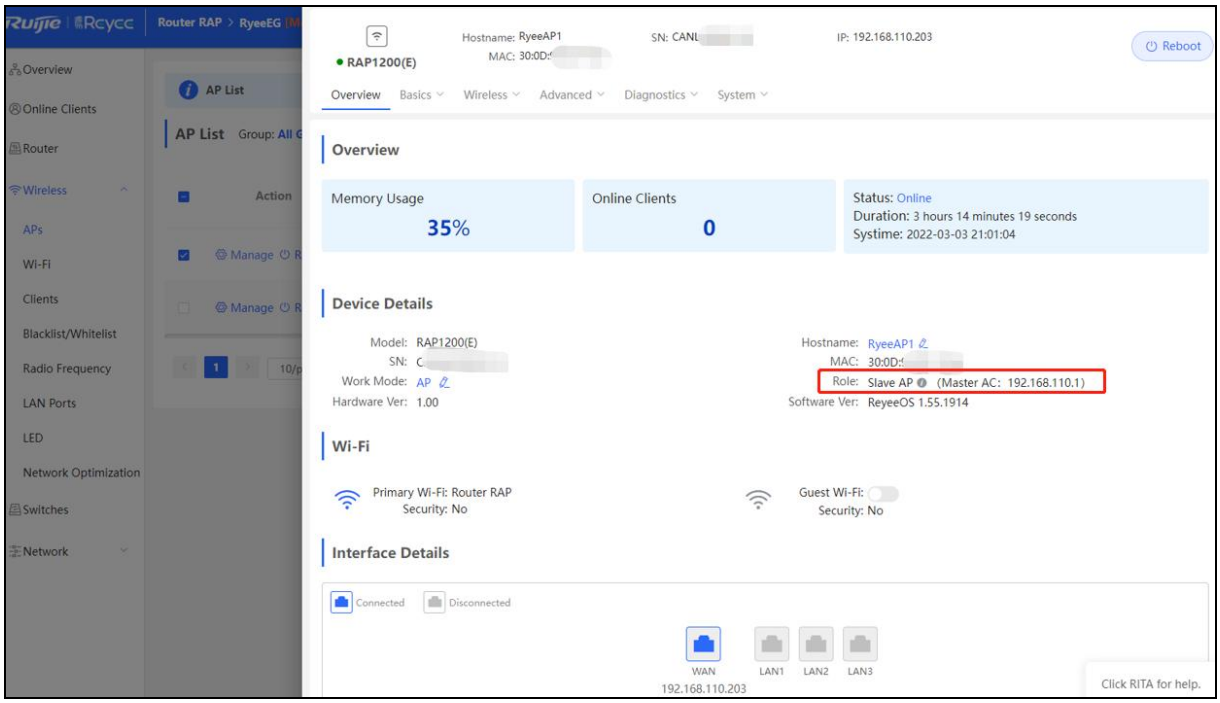


5.4.1.2 Device networking role

Master:



Slave:



5.4.3 The troubleshooting of SON

Fault symptom

Network self-organization Fail

Cause

There are multiple masters, and more than 1 @Ruijie-mxxx SSID could be seen.

Layer fails to broadcast.

Solution

Check whether the devices are connected with same network and merge all the devices to the same network.

Check whether there are have some configurations like VLAN and port isolation.

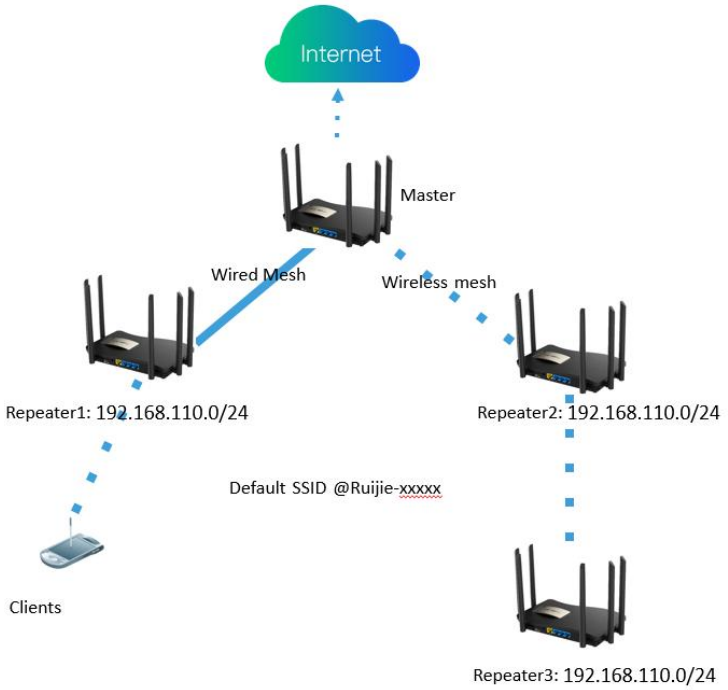
Check whether the SON is disabled.

5.5 Reyee Mesh Solution

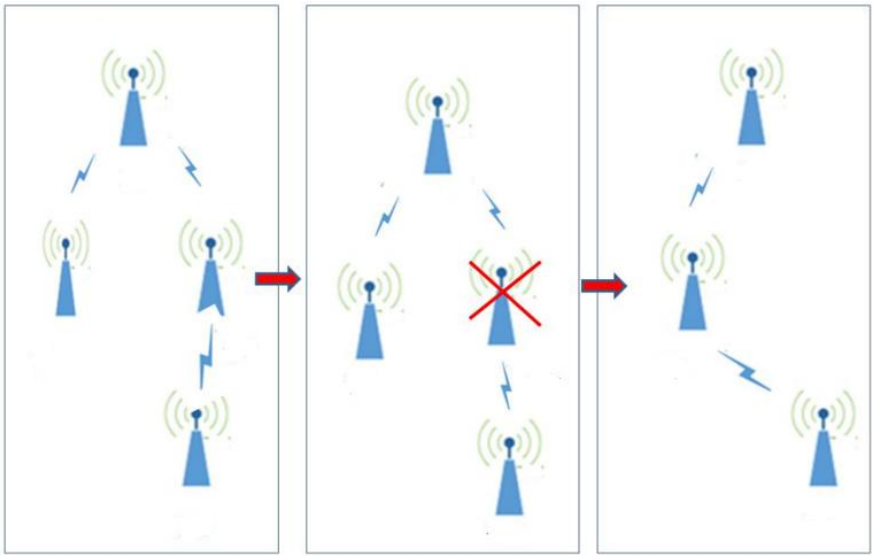
The Mesh function of Reyee EW series routers support zero-configuration networking for multiple devices, and can self-recover when there are some single point issues. The wireless coverage requirements of home scenarios could be satisfied by the Mesh function of Reyee EW series completely..

5.5.1 Application Scenario

Zero-Configuration Network



Self-Recover Network



Tips:

The Mesh function can automatically switch between wired and wireless links. It will automatically switch to wired mesh after wired access and automatically switch to wireless mesh after the network cable is unplugged

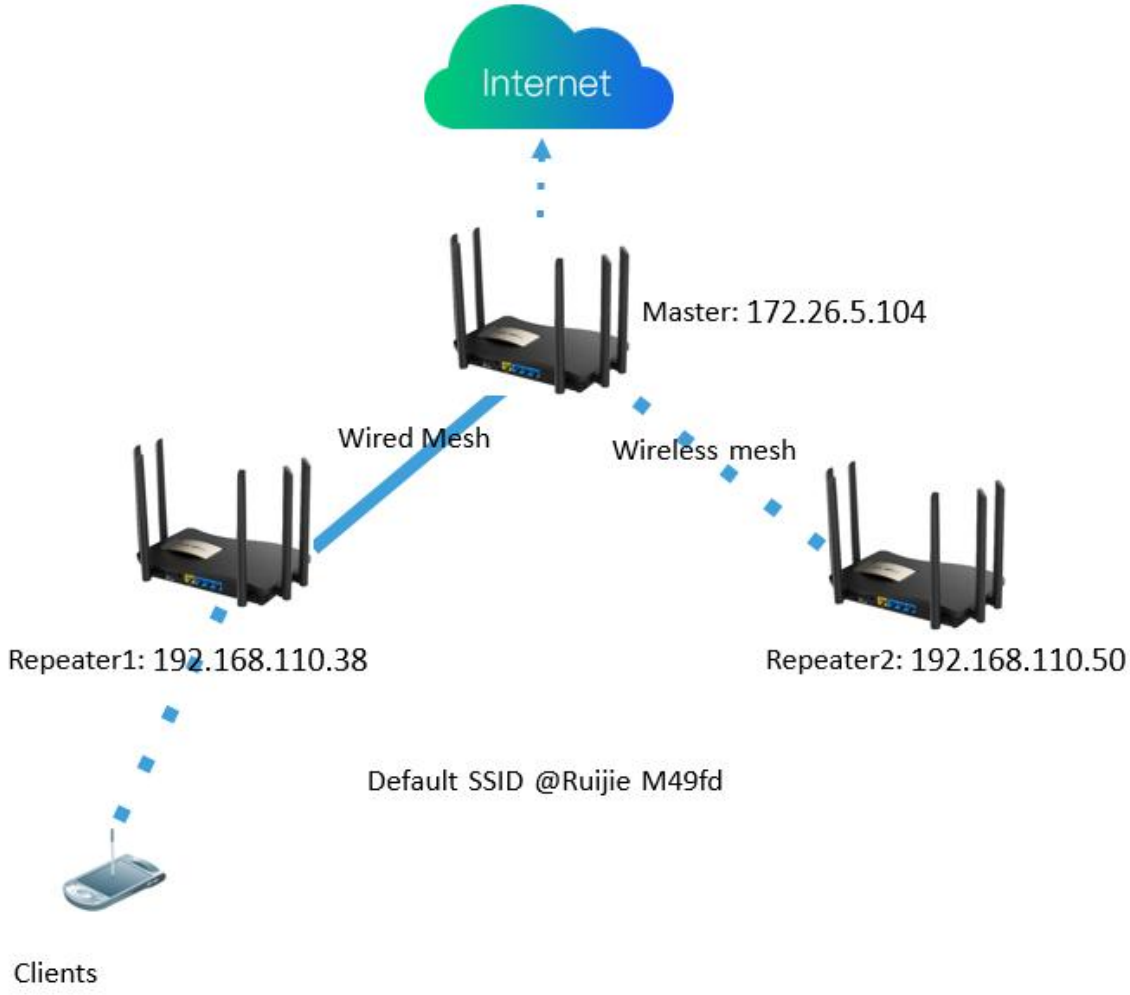
5.5.2 Configuration Case

Requirement

Provide wireless network for clients' home (Two rooms and one hall).

One of room requires to connect the wireless internet and the other one connect to wire internet.

Network Topology



Network Description:

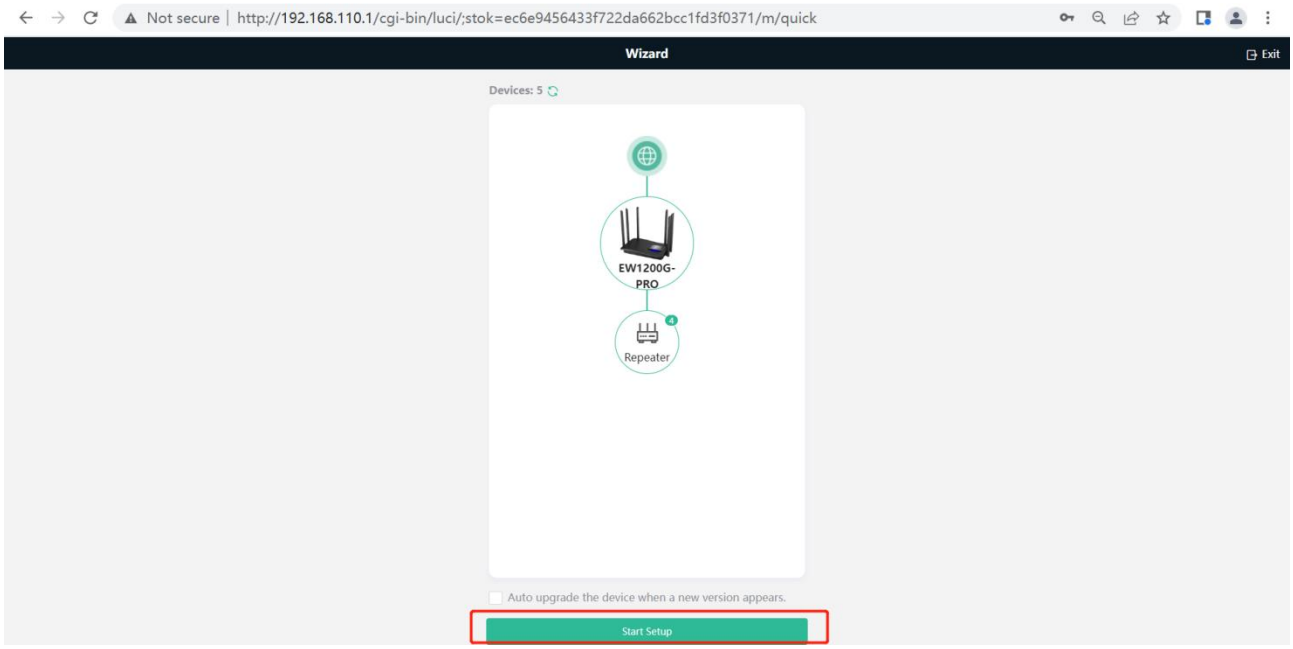
1. Master gets the DHCP IP address from ISP to access internet, broadcasting default SSID @Ruijie-m49fd which is used by clients and broadcast a default hidden mesh Wi-Fi to let repeater to connect.

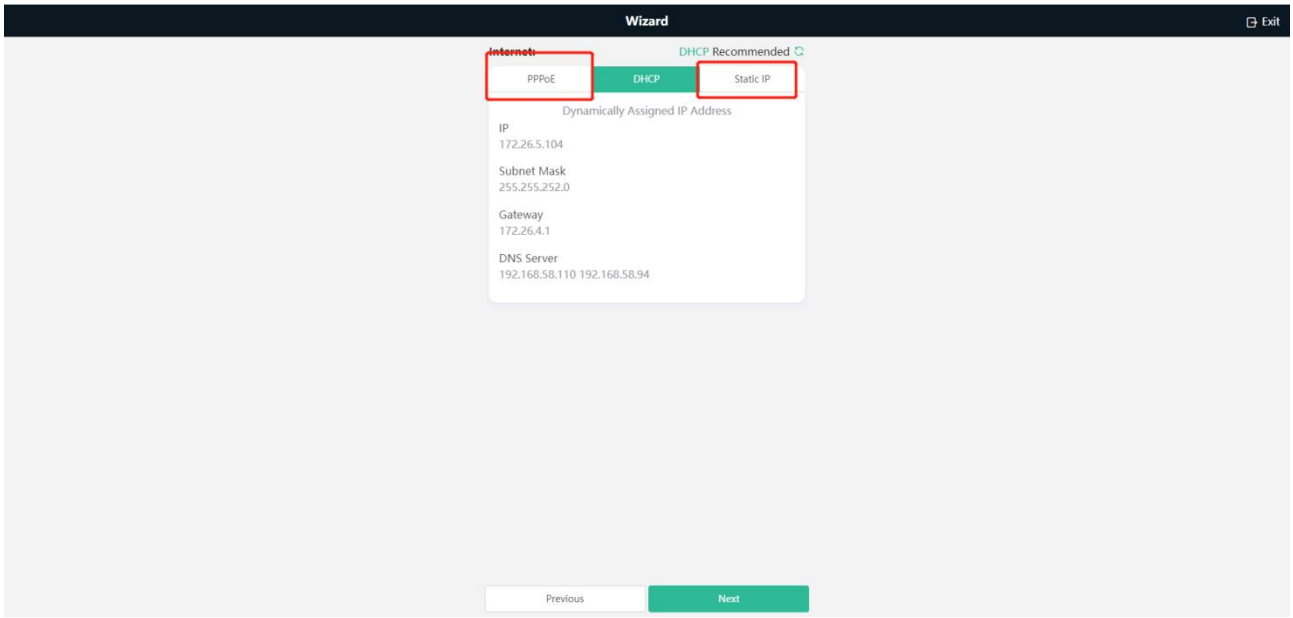
2. Repeater connected with Master using wired or wireless will broadcast the default SSID @Ruijie-m49fd after mesh succeed.

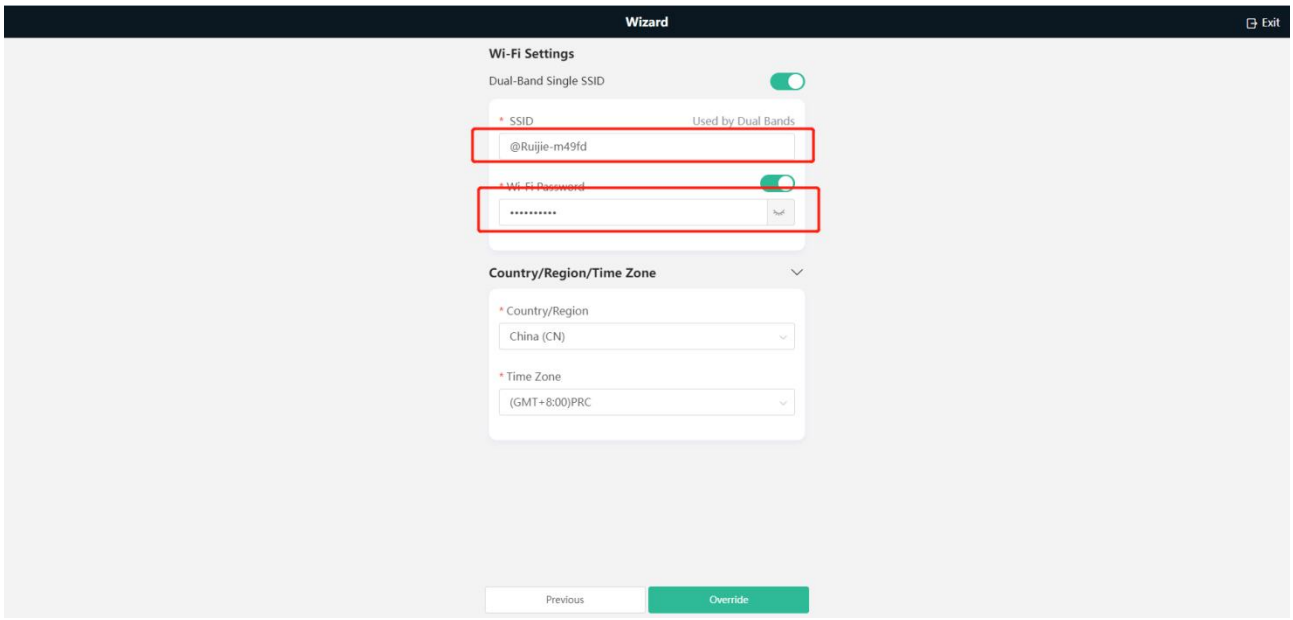
Configuration Steps:

Step 1: Connect the ISP cable to the WAN port of Master. The master will get the DHCP IP address from ISP which can access internet.

If you need to configure PPPoE account or static IP, you can connect your PC to the LAN port of the master, using default IP 192.168.110.1 to access it. Then refer to the Wizard to configure the internet. Click Start-Setup, fill the PPPoE information or Static IP information, click Next to configure the SSID information.


Not secure | http://192.168.110.1/cgi-bin/luci/;stok=ec6e9456433f722da662bcc1fd3f0371/m/quick
Wizard
Exit
Devices: 5
EW1200G-PRO
Repeater
Auto upgrade the device when a new version appears.
Start Setup


Wizard
Exit
Internet:
DHCP Recommended
PPPoE
DHCP
Static IP
Dynamically Assigned IP Address
IP
172.26.5.104
Subnet Mask
255.255.252.0
Gateway
172.26.4.1
DNS Server
192.168.58.110 192.168.58.94
Previous
Next

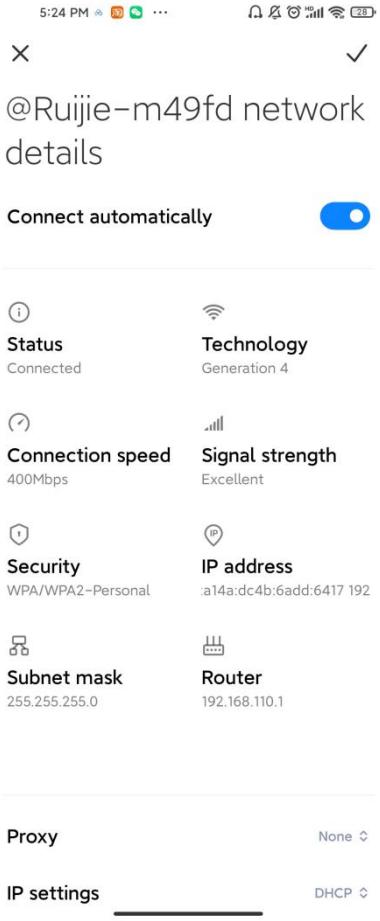


Step 2: Connect the WAN port of Repeater1 to the LAN port of Master.

Step 3: Press the **Pairing** button <1s on Master and Repeater 2

Configuration Verification

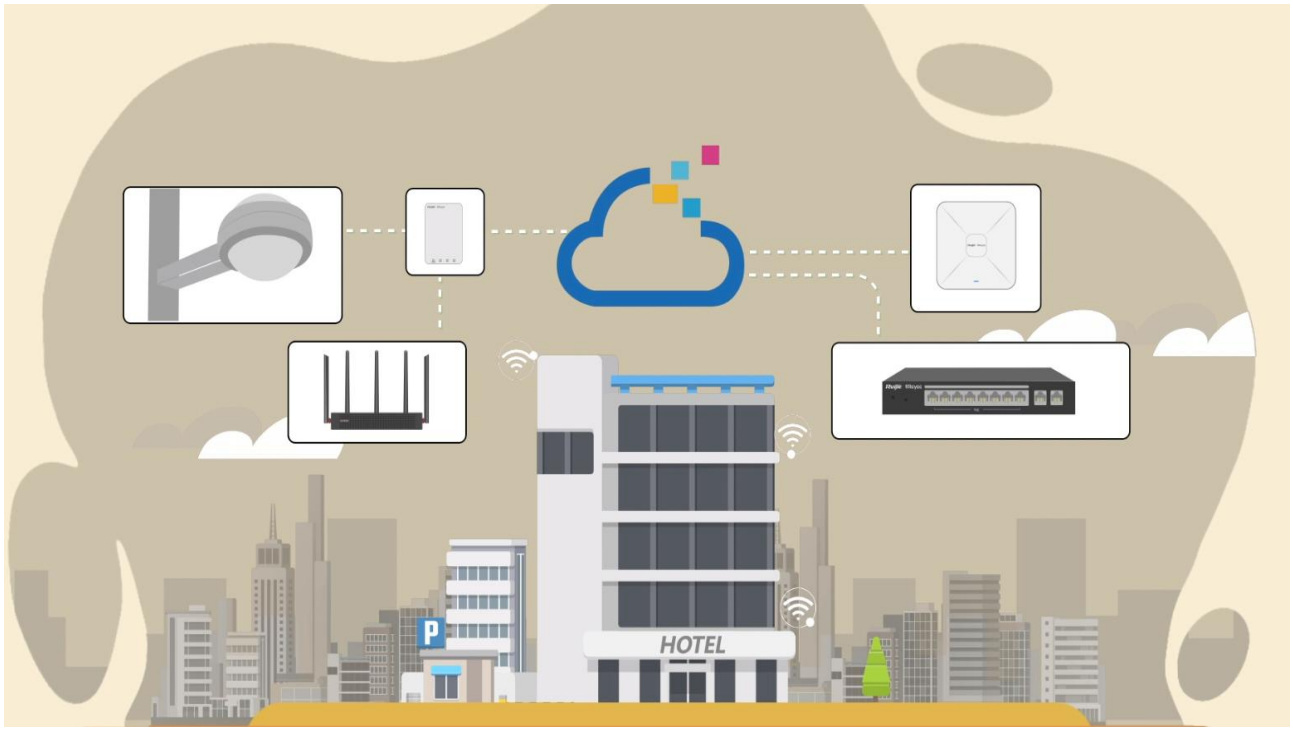
Clients can connect the Wi-Fi @Ruijie-m49fd and access internet successfully.



5.6 Reyee Economic Hotel Network Solution

5.6.1 Application Scenario

Reyee economic hotel network solution provides an affordable 5-star Wi-Fi for clients. It can operate concurrently at 2.4GHz and 5GHz, providing high-speed wireless access of 574Mbps at 2.4GHz, 1201Mbps at 5GHz and up to 1775Mbps per AP. The wall AP provides a LAN port at the front to facilitate the expansion of IPTV, IP phone, etc.

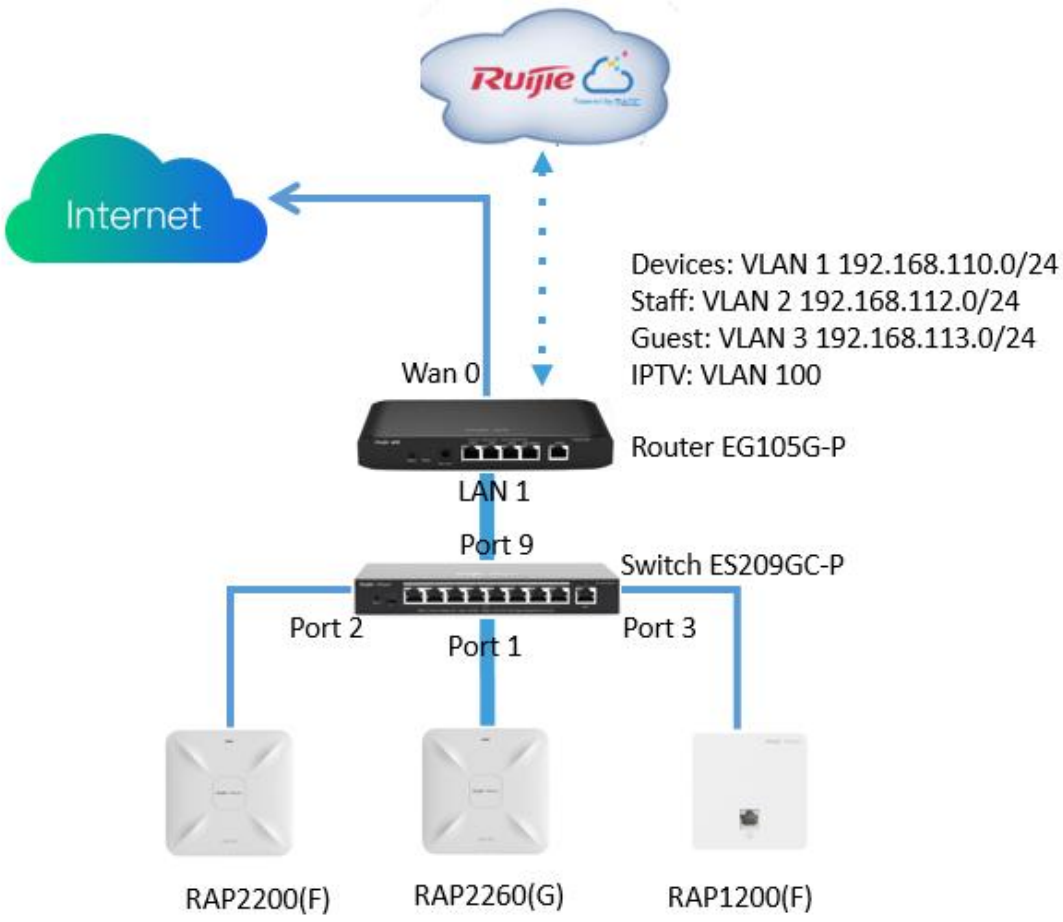


5.6.2 Configuration Case

Requirement

1. Wireless network for Hotel, guests need to do voucher authentication before accessing internet and can't access internal network of hotel.
2. Providing wired connection for IPTV.

Network Topology



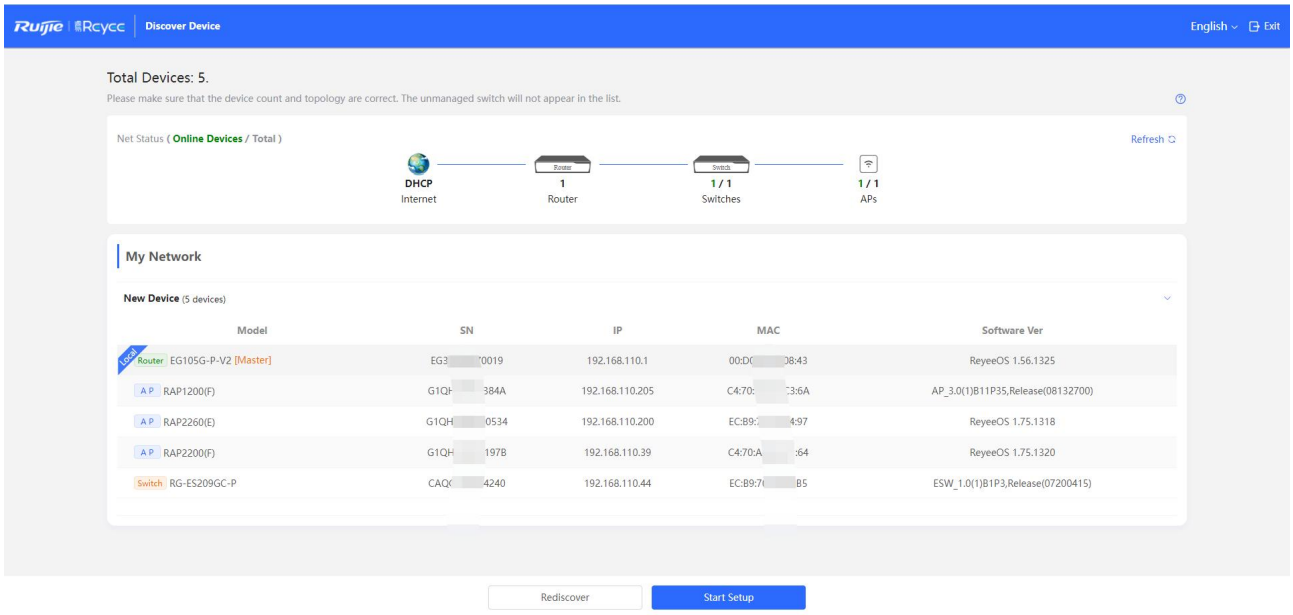
Devices List

Type	Model	Function
Gateway	EG105G-P	1.Connect Internet and work as DHCP server for downlink devices and clients; 2.Manage AP and Switch Devices locally; 3.Support Cloud voucher authentication with Ruijie Cloud;
Switch	ES209GC-P	Provide wired and POE connection.
Wall AP	RAP1200(F)	1.Provide wireless connection for room. 2.Provide wired connection for IPTV.
Indoor AP	RAP2200(F)&RAP2260(G)	Provide wireless connection for hall and corridor.

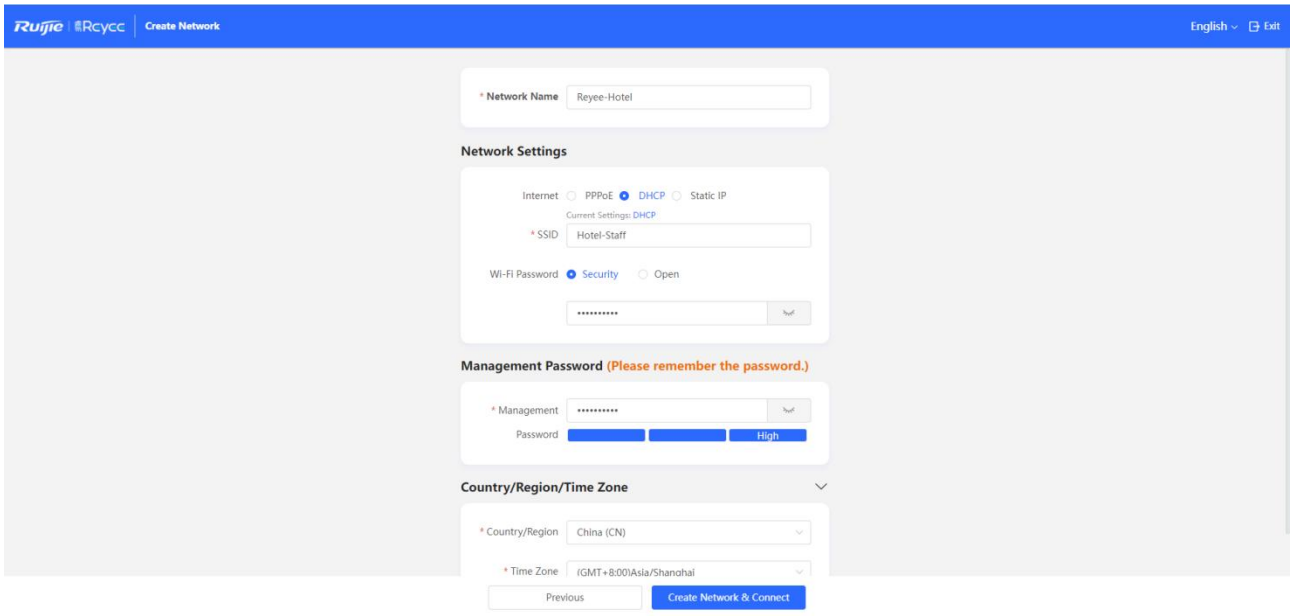
Configuration Steps

Step1: Power on and connect the device refer to the topology.

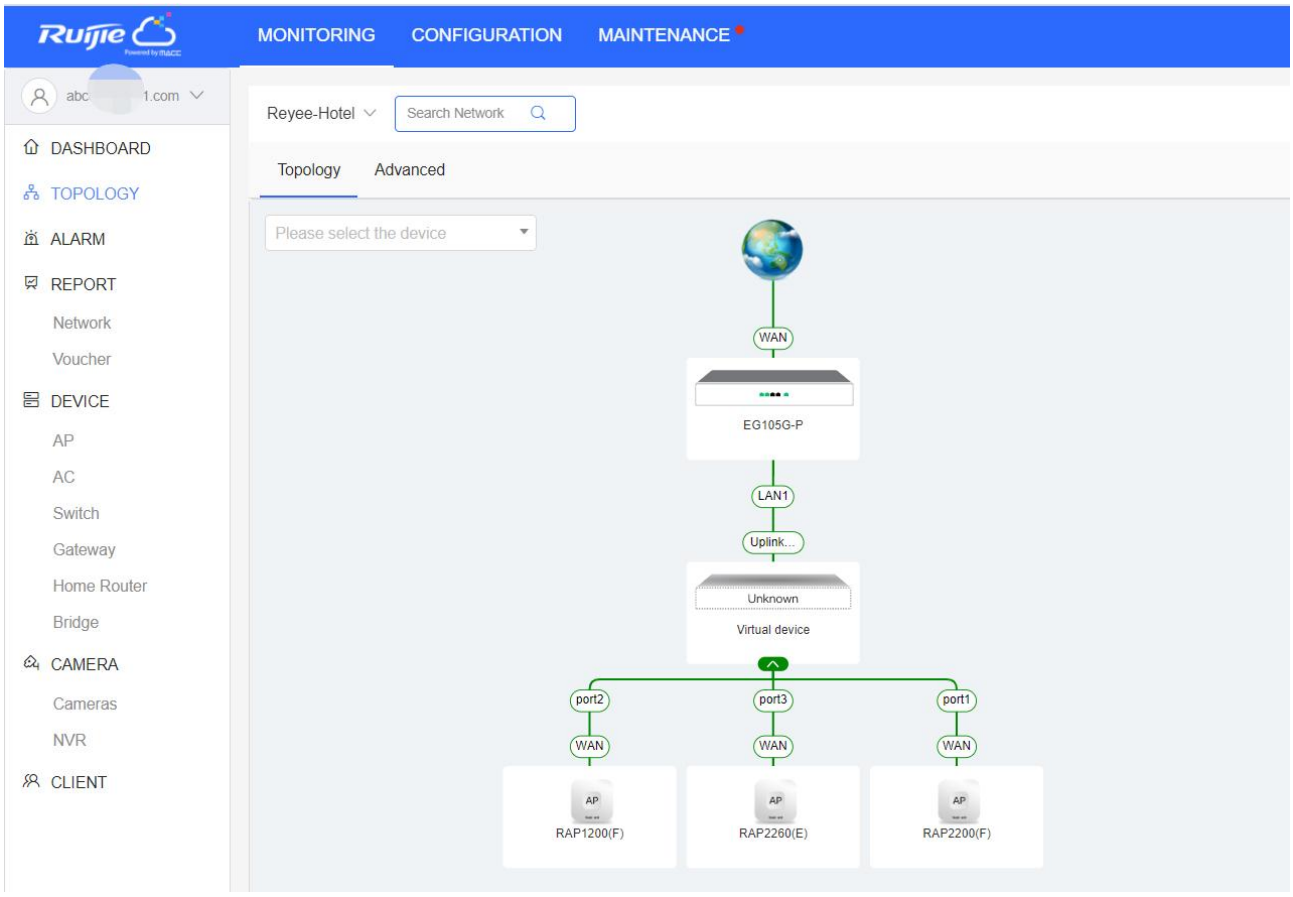
Step2: Access Gateway by default IP 192.168.110.1, refer the **Start Setup** step to configure the basic network settings.



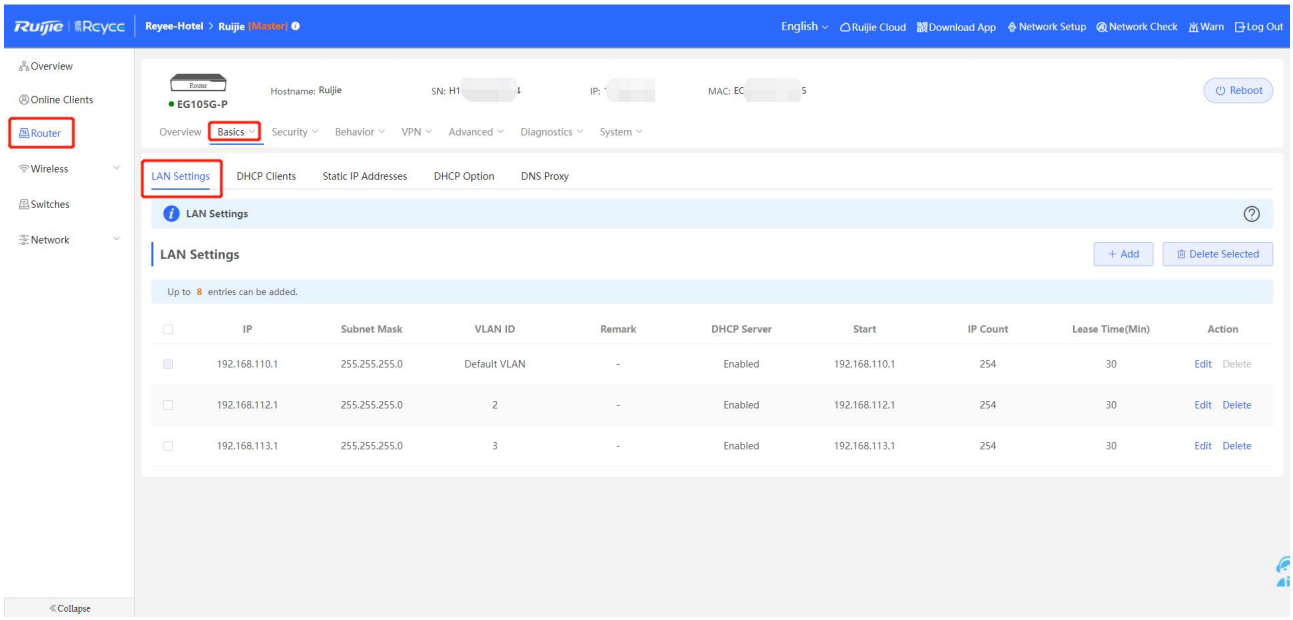
Set the **Network Name**, **Network Settings, SSID** for Staffs and the set the **Management Password.**



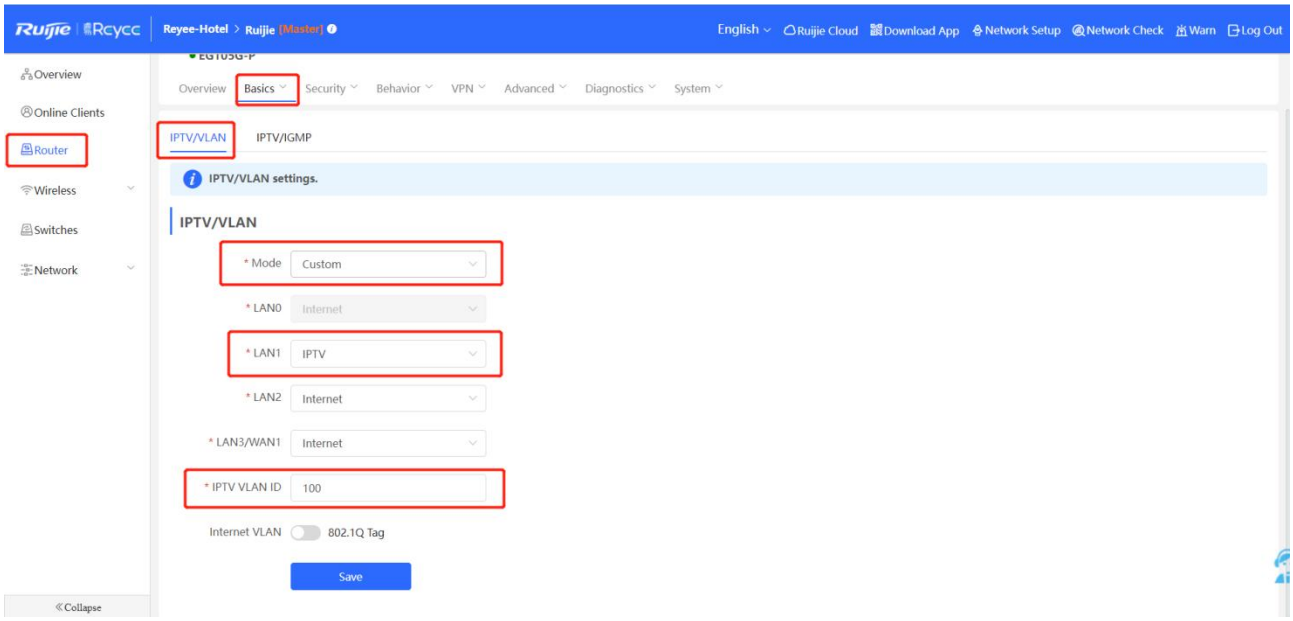
Click **Create Network & Connect** to active configuration and add the devices to Cloud.



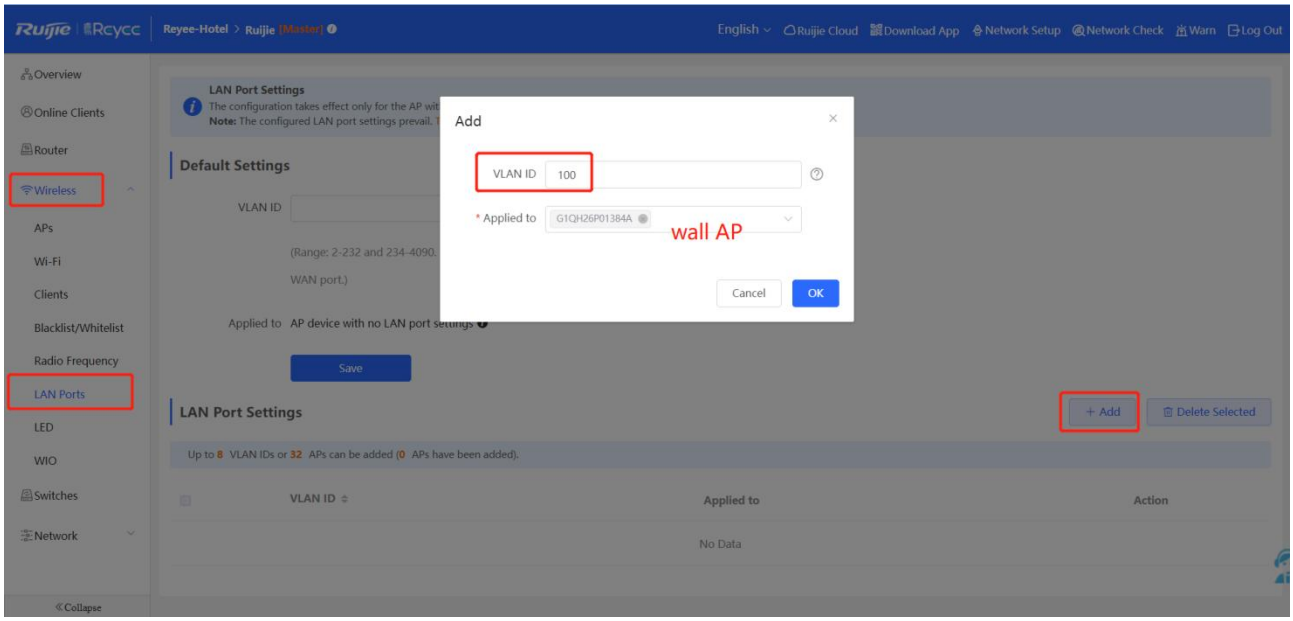
Step2: Click **Router->Basic->LAN** to create VLAN 2 and VLAN 3 for Staff and Guest.



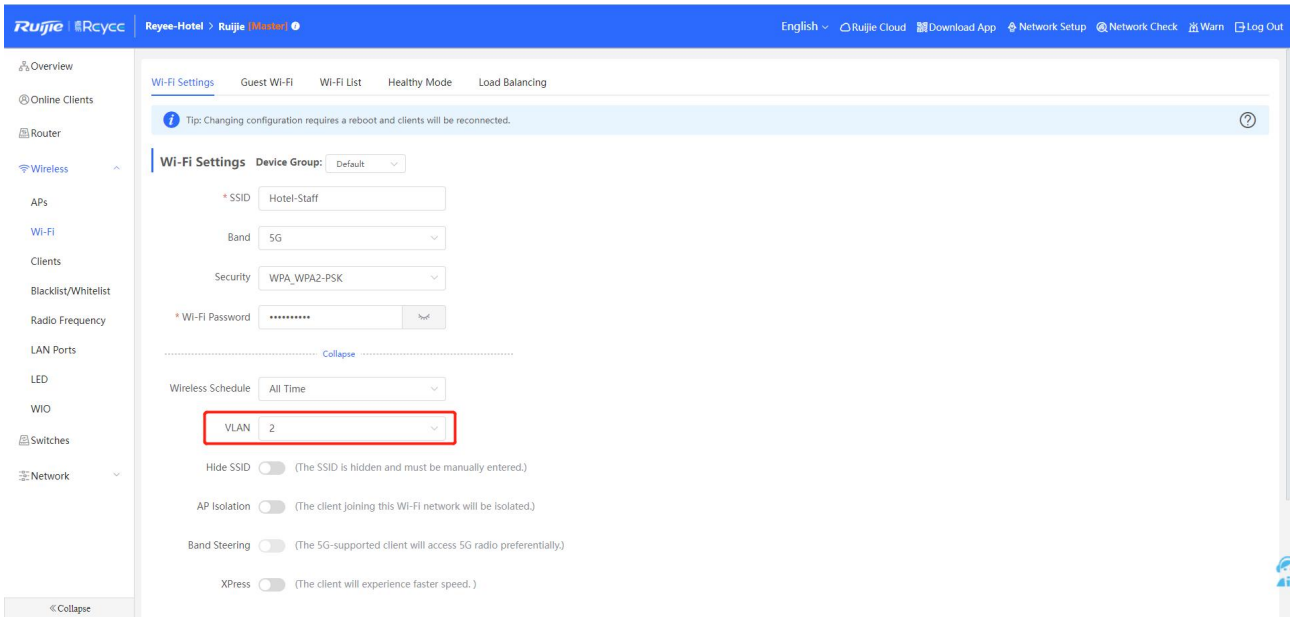
Step3: Click **Router->Basic->IPTV** to set IPTV settings get from ISP. For example, the IPTV VLAN is 100, you can do as below:.



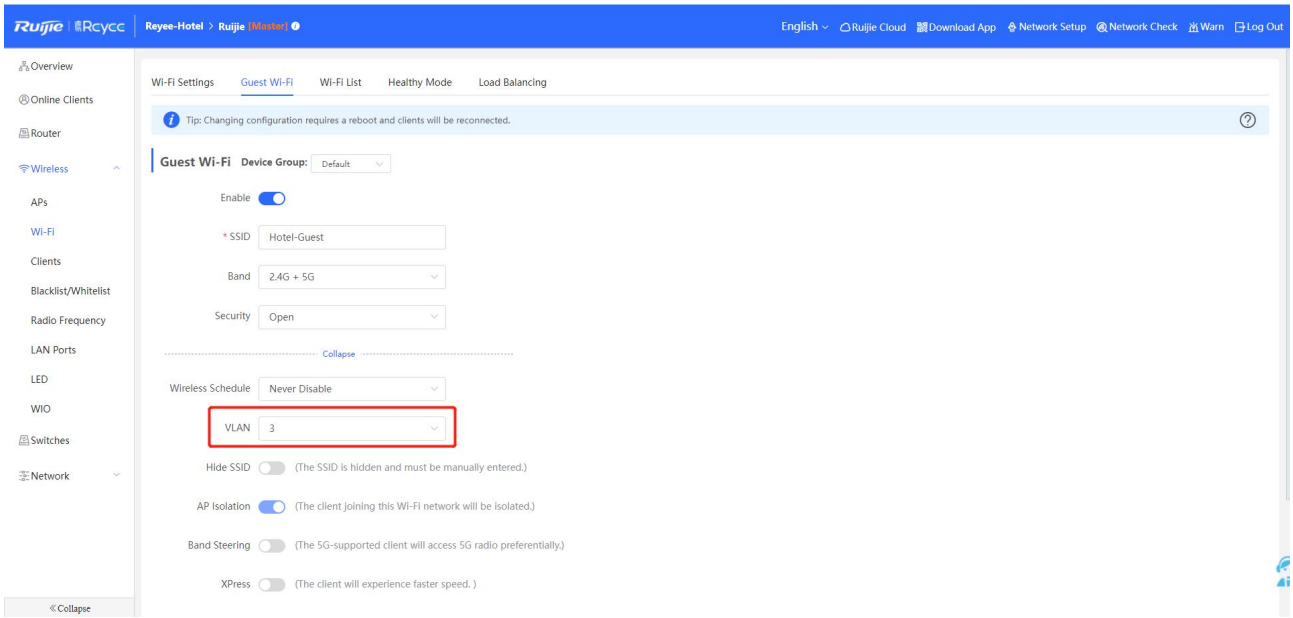
Step4: Click **Wireless->LAN Ports->Add** to configure VLAN 100 for IPTV, if it use the default VLAN 1, this step could be ignored.



Step5: Click **Wireless->Wi-Fi** to configure the WiFi for staff and guest. Choose VLAN 2 for Staff.

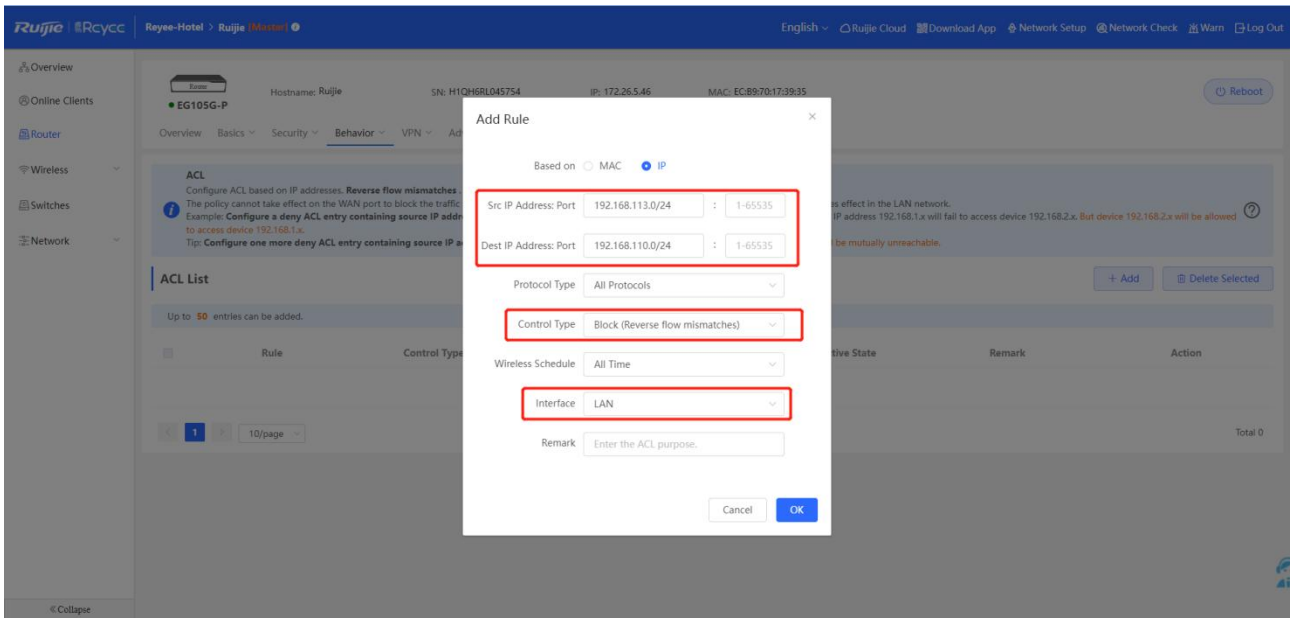


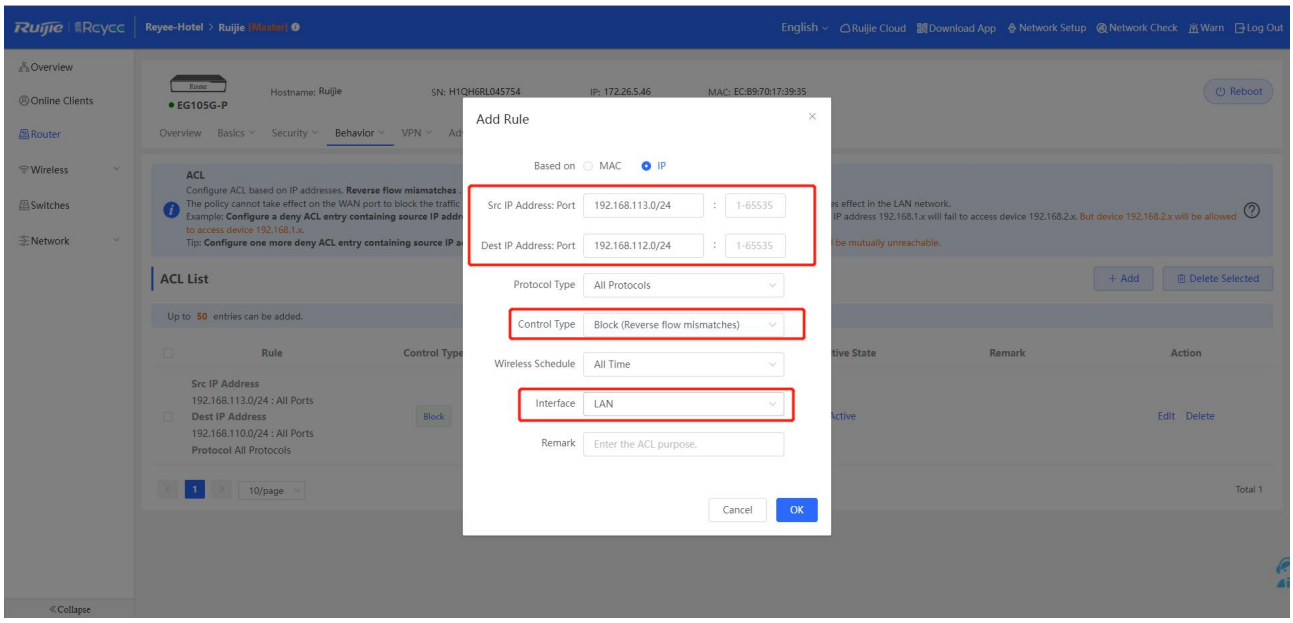
Step6: Enable Guest WiFi, choose VLAN 3 for it.

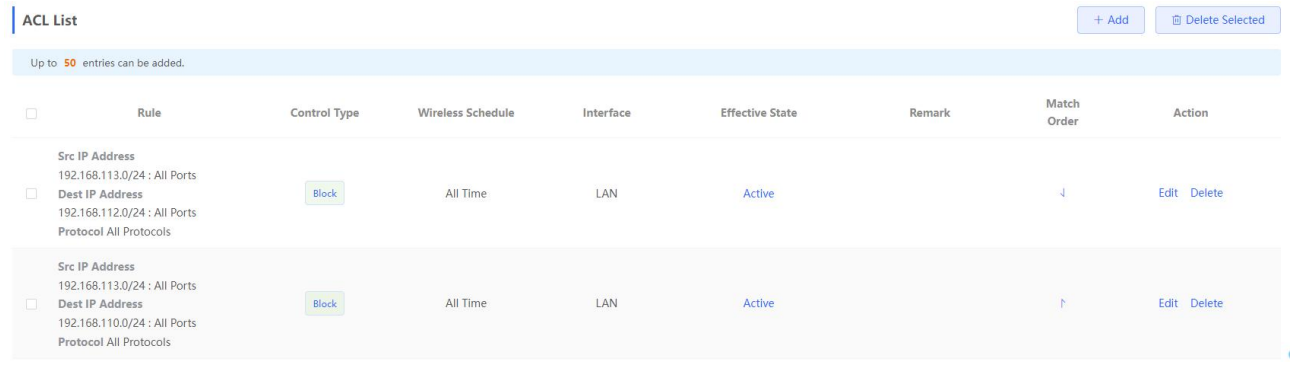


Step7: Click **Router->Behavior->Access Control, Configure ACL** to add ACL to block guest accessing to the internal network.

Add two ACLs to block VLAN 3 accessing to VLAN 1 & VLAN 2, this function is applied in LAN port.

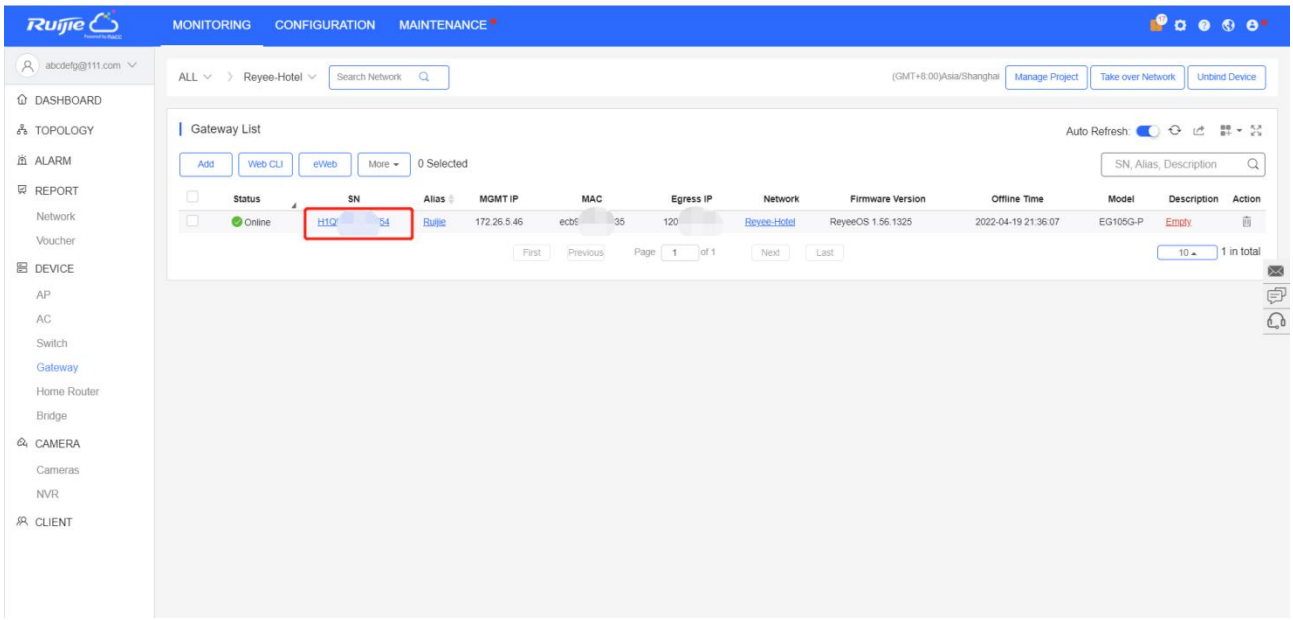




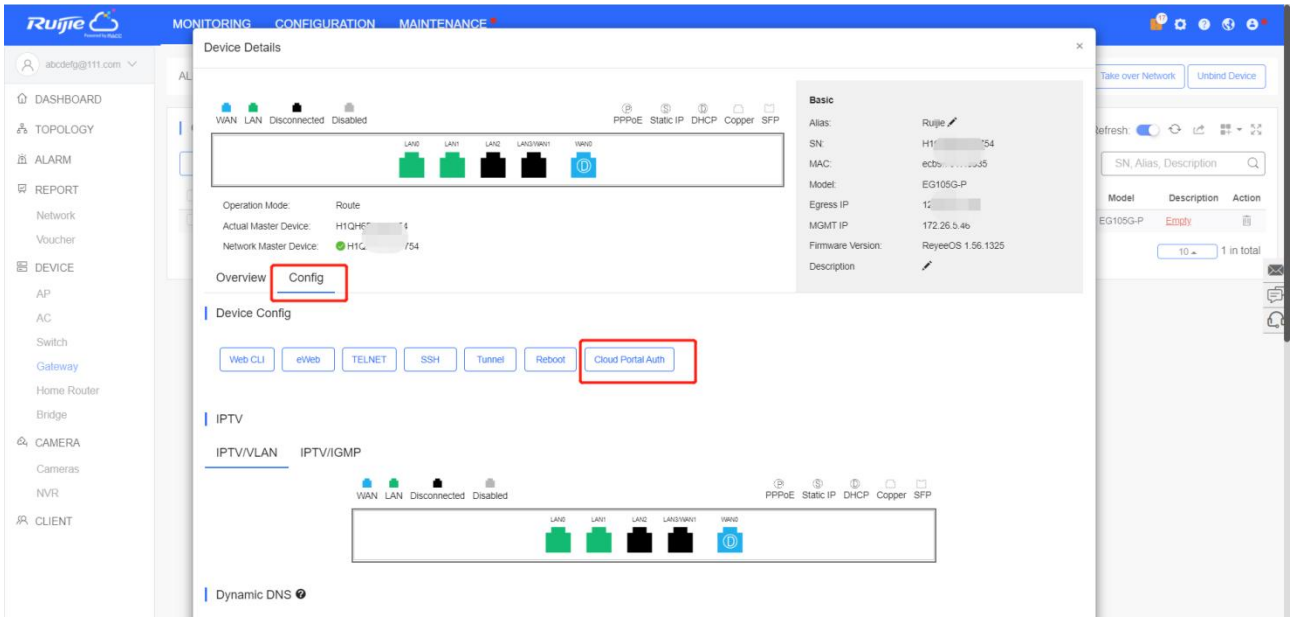


Step 8: Login to Cloud web to configure Cloud voucher authentication for guest.

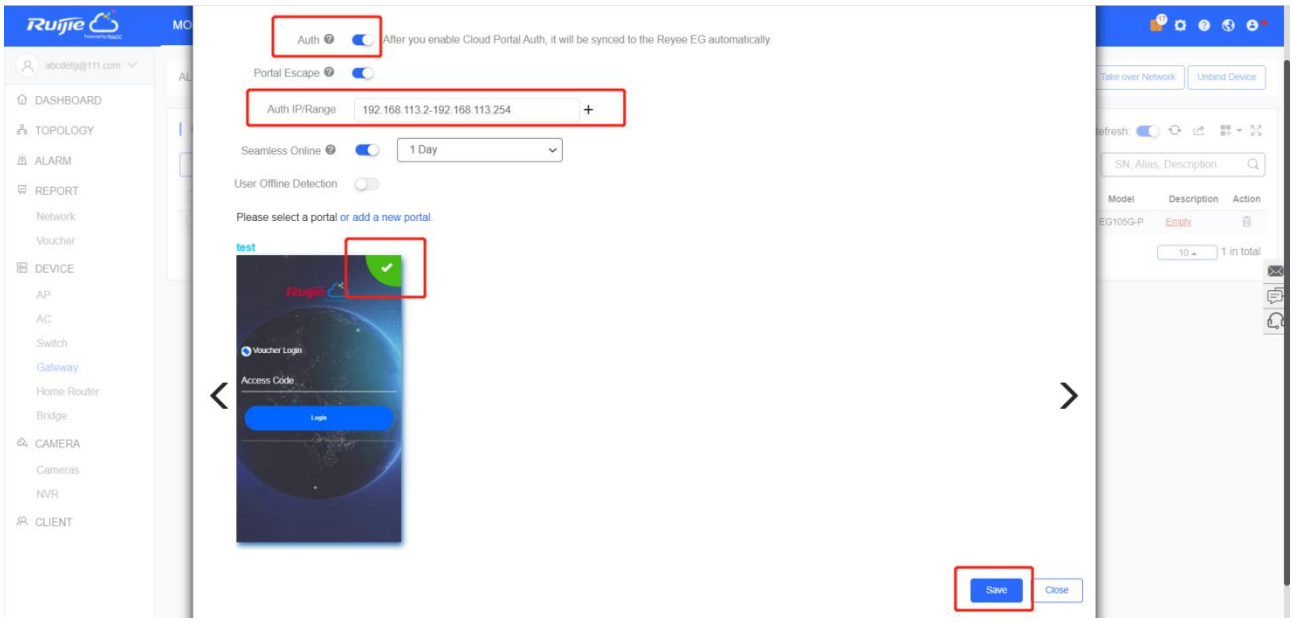
Click the SN of the EG to enter its device detail page.



Click Config->Cloud Portal Auth

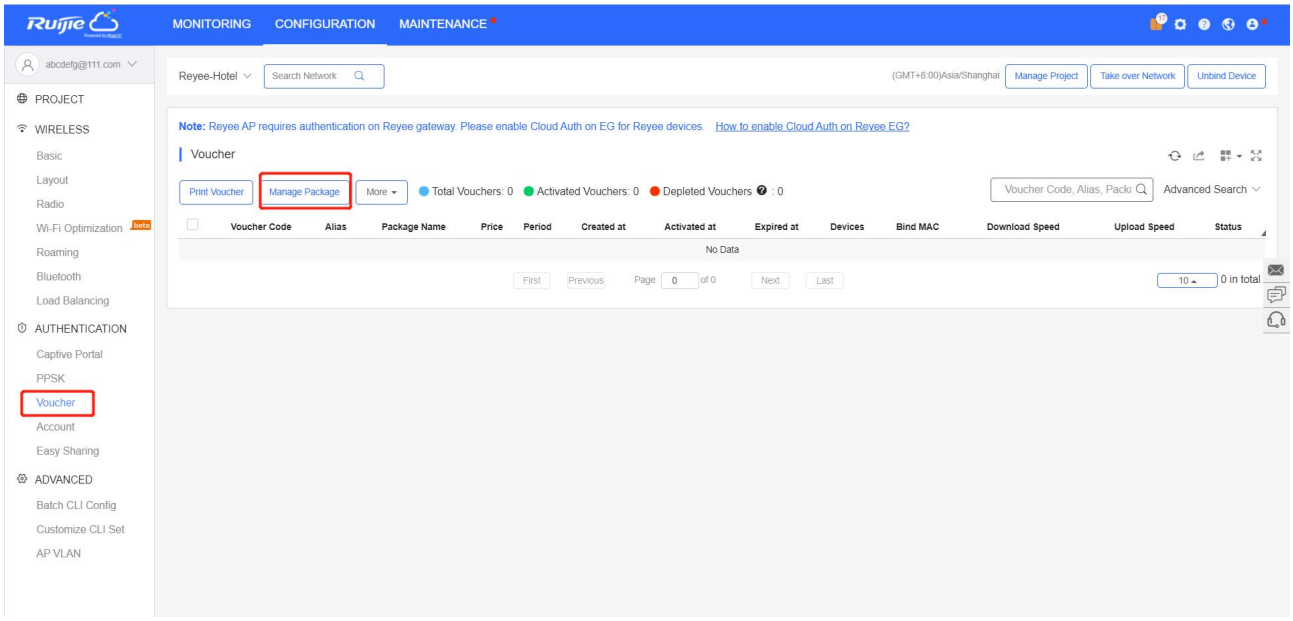


Enable auth and configure the Guest clients IP range from 192.168.113.2 to 192.168.113.254.

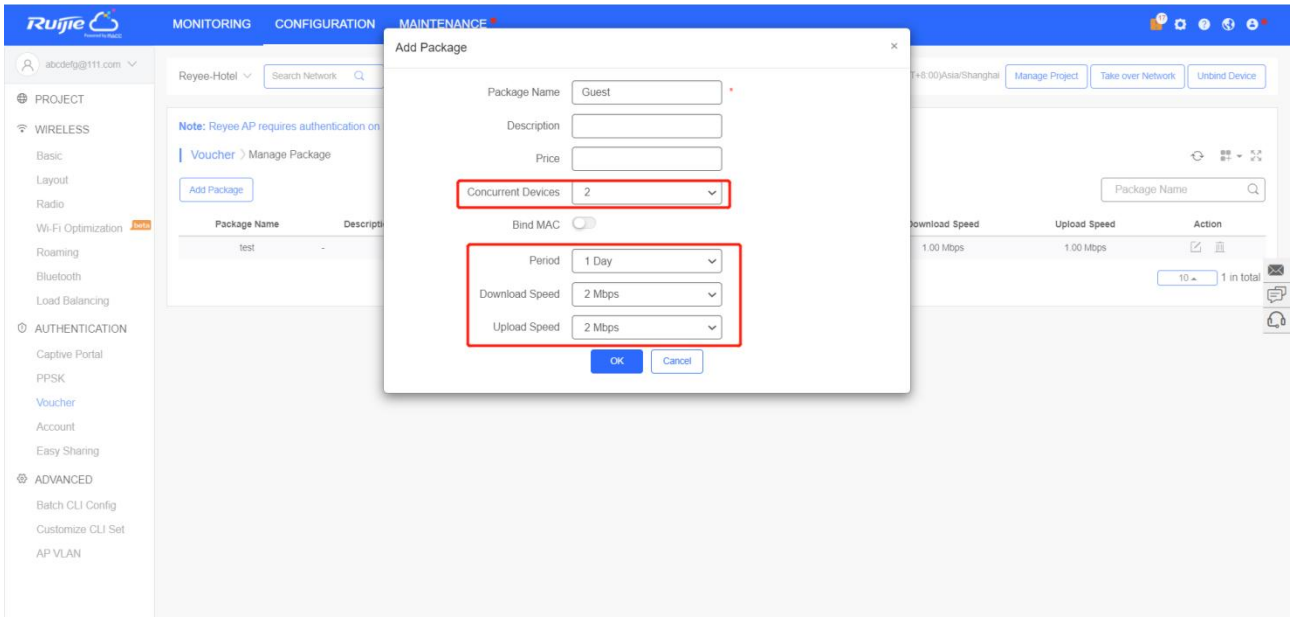


Add the voucher package for Guest

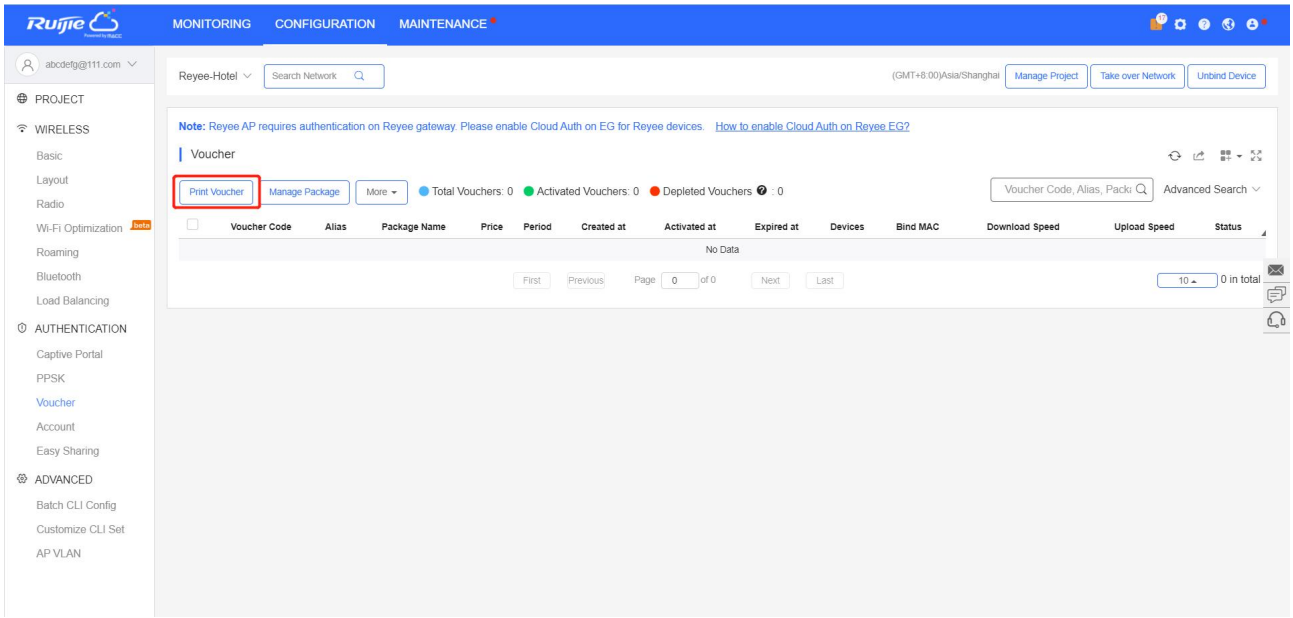
Click **Voucher->Manage Package->Add Package** to add voucher package for Guest.

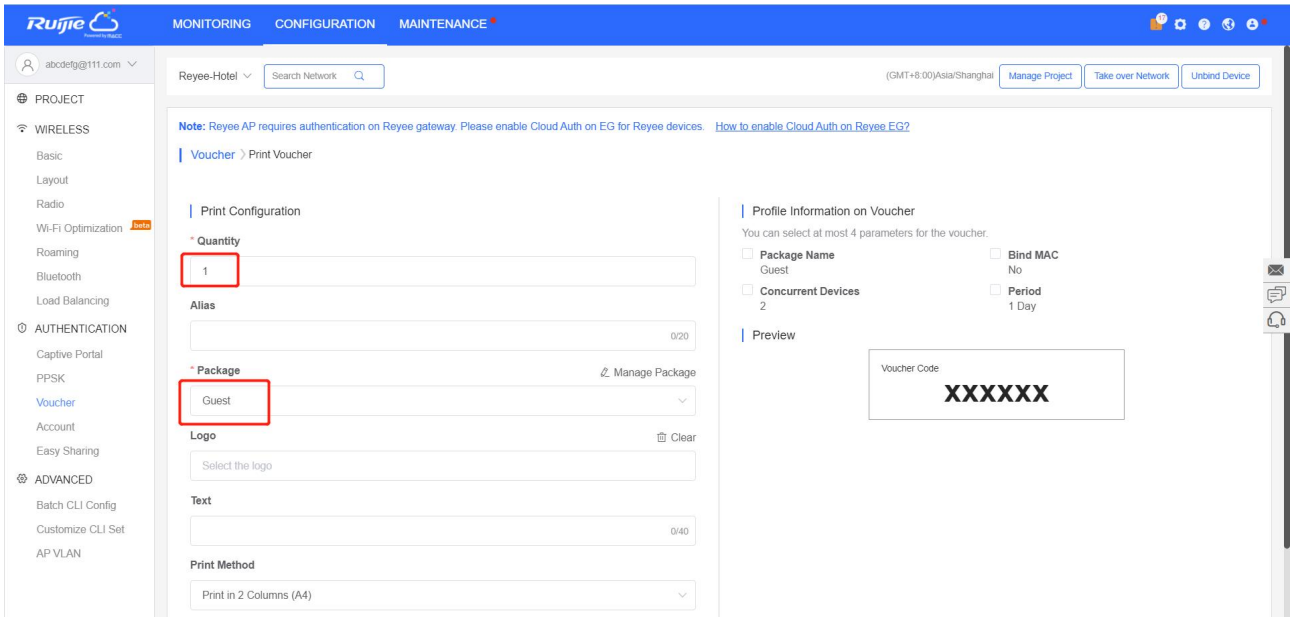


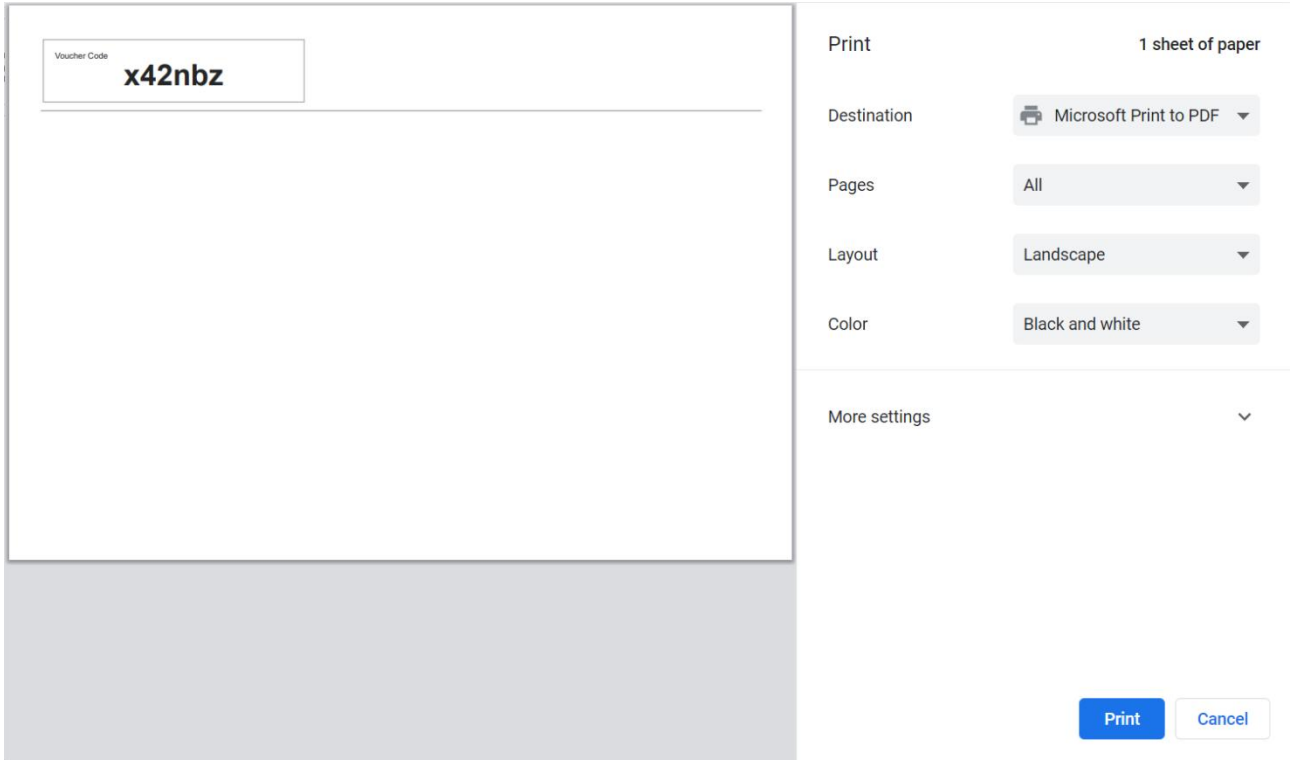
Example: the **Concurrent Devices** to be 2, **Period** to be 1 day and the upload and download speed limitation to be 2Mbps.



Click **Print Voucher** to get one code for Guest.

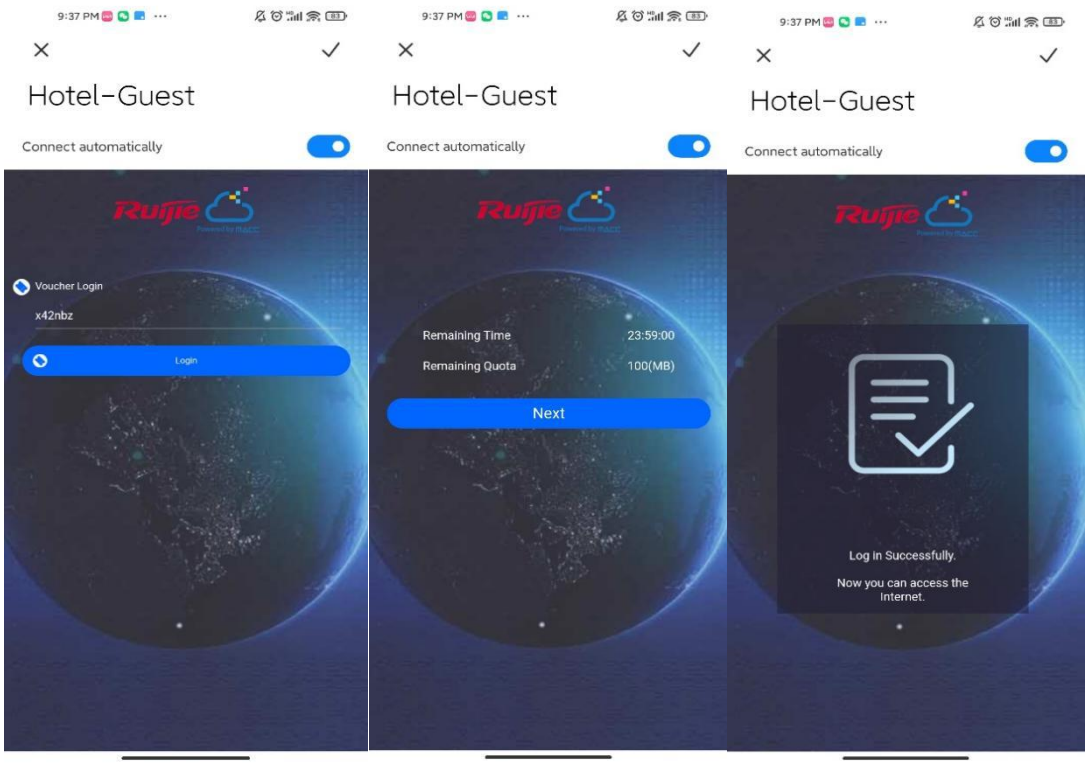






Configuration Verification

Connect Guest WiFi, then you can see the internal IP 192.168.110.1 can not be accessed.

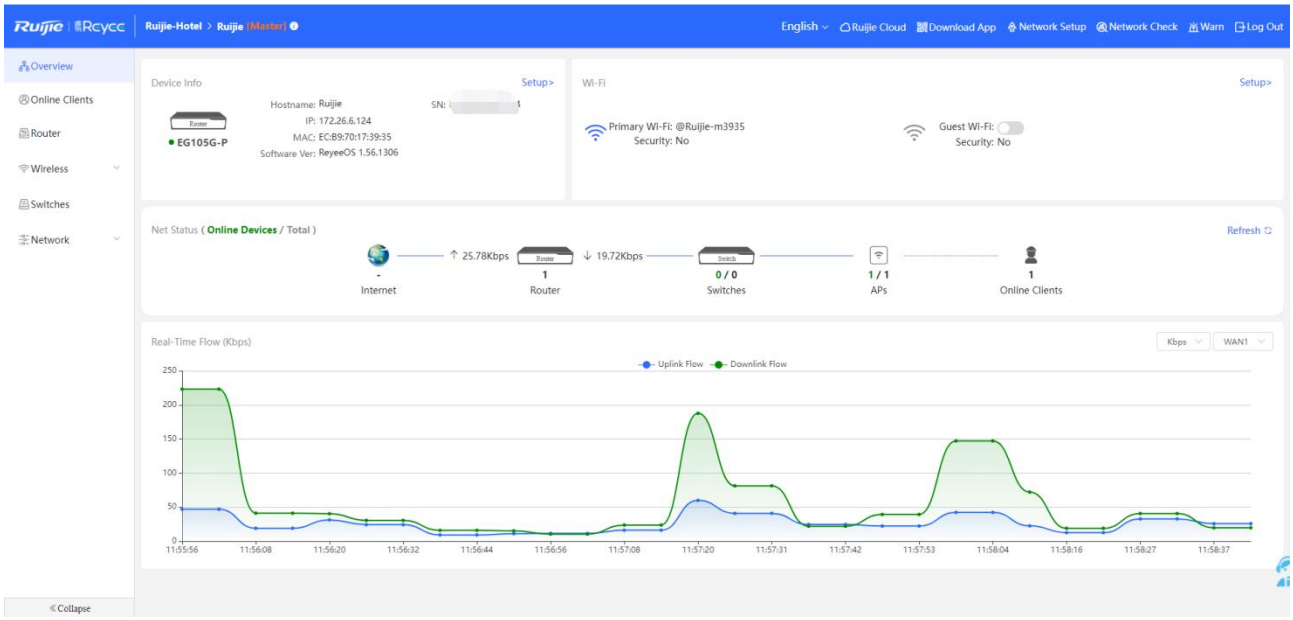

Hotel-Guest
Connect automatically
Voucher Login
x42nbz
Login
Hotel-Guest
Connect automatically
Remaining Time 23:59:00
Remaining Quota 100(MB)
Next
Hotel-Guest
Connect automatically
Log in Successfully.
Now you can access the Internet.

6 Reyee FAQ

7 Appendix：Monitor

7.1 Reyee Gate Series Router Monitor

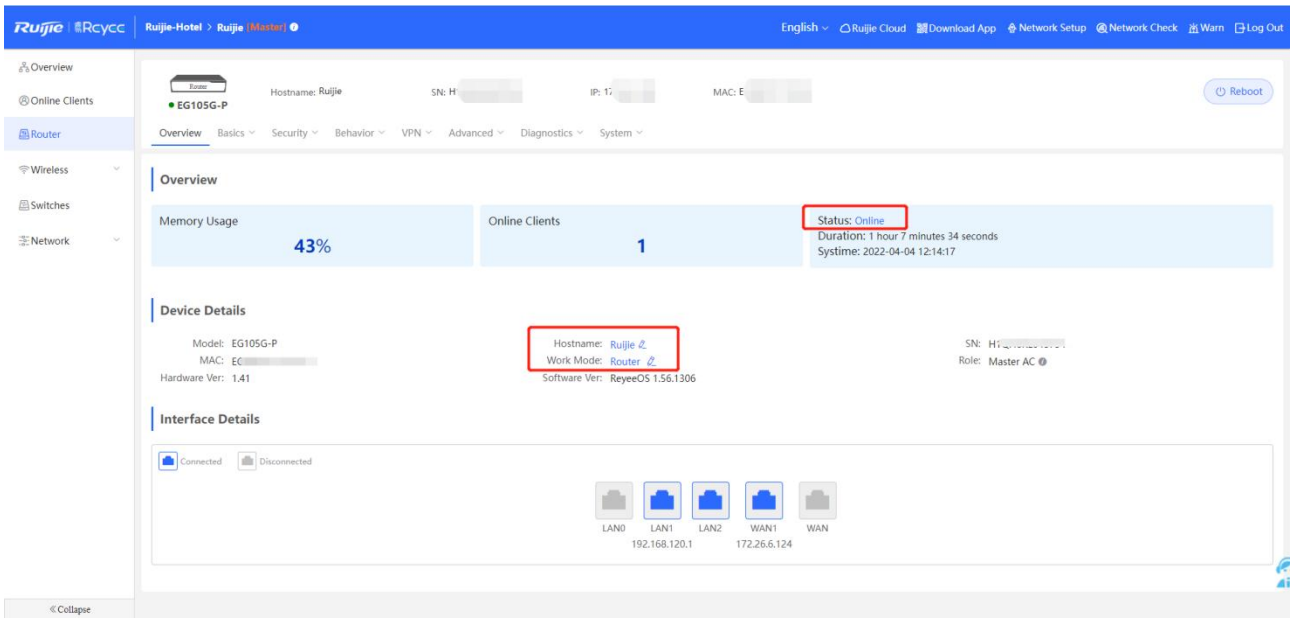
The overview page displays **Device Info**, **Wi-Fi information**, **Network Status** and **Real-Time Flow**.



7.1.1 Device Info

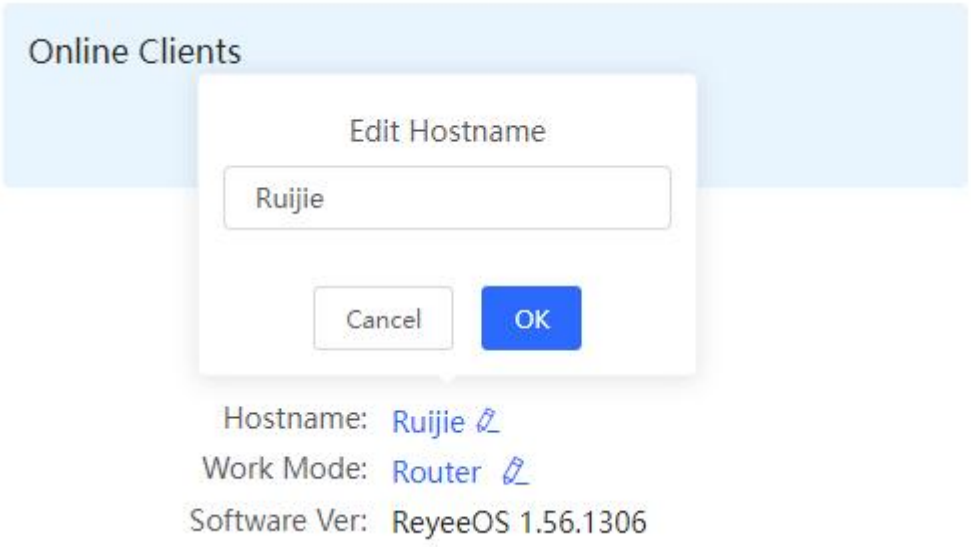
The **Device Info** page show the model, hostname, IP, MAC, software version, SN of the Router.

Router->Overview page will appear by clicking Setup which displays **Memory Usage, Online Clients, Status, Device Details,** and **Interface Details.**

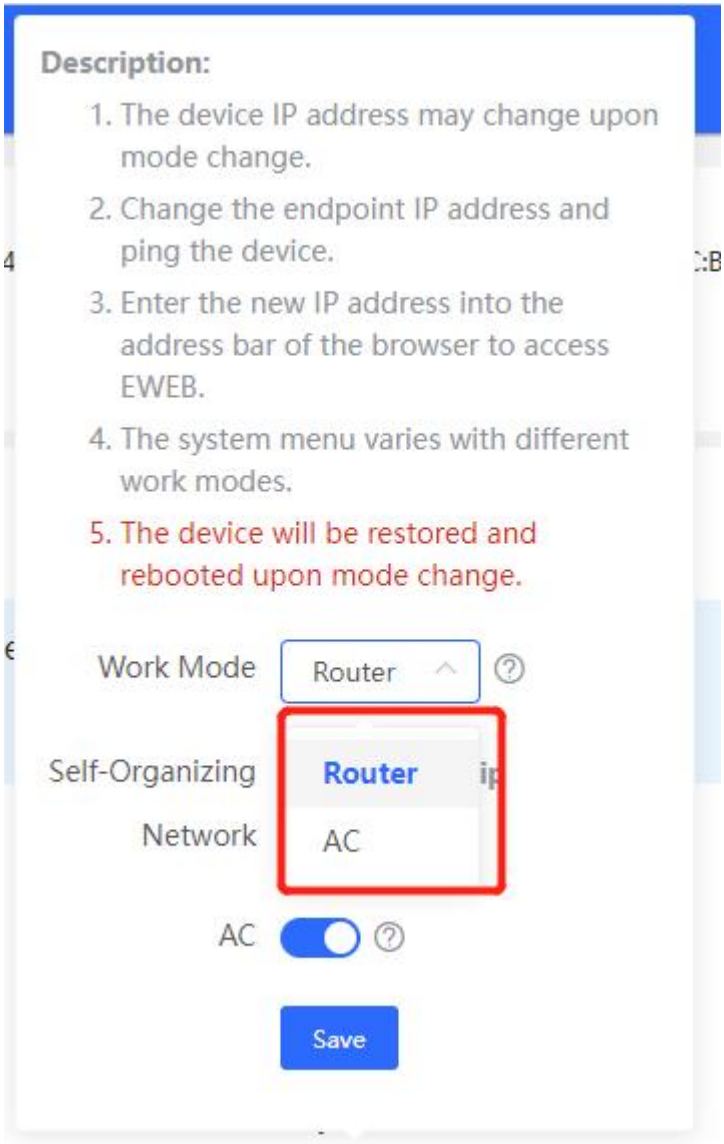


The **Online** status indicates the SON status of the Reyee devices but not the online status of Ruijie Cloud.

You can Click **Hostname** to modify it.



Choose the work mode you need by clicking **Work Mode**. Router mode and AC mode are two available modes for Reyee Gate series Router. But the default mode is Router mode.



Router Mode: Nat forwarding

AC Mode: Bridge forwarding

Self-Organizing Network:

1. If it is enabled, the device role will be displayed.

2. If it is disabled, the device works in standalone mode.

3. It is enabled by default in AC mode.

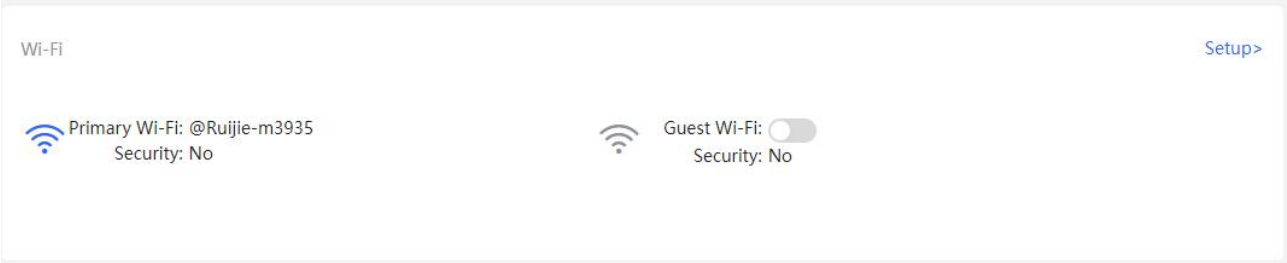
AC:

1. It is enabled by default. The device works as a virtual AC to manage downlink devices.

2. When it is disabled, the device must be elected as the AC before managing downlink devices

7.1.2 Wi-Fi information

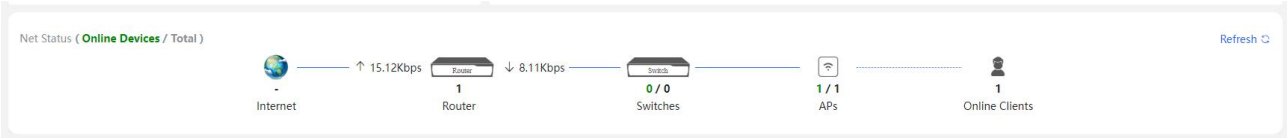
You can name the Wi-Fi of the network and enable Guest Wi-Fi.



Setup: Go to the Wi-Fi setting page.

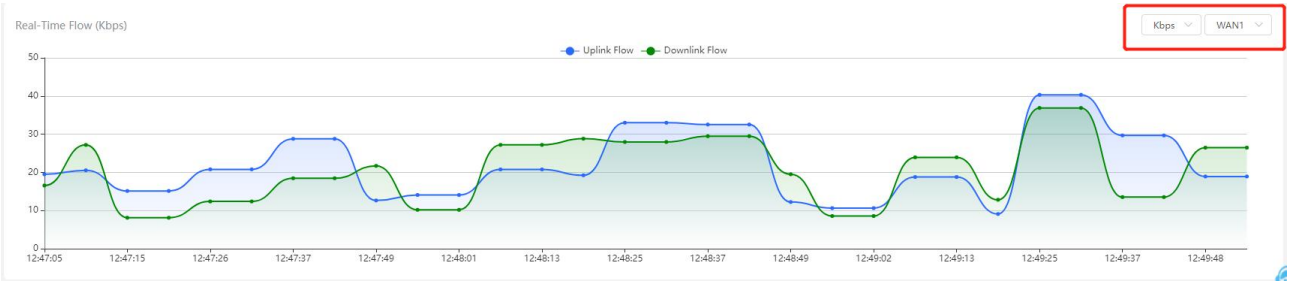
7.1.3 Net Status

The **Network Status** page displays the topology and connected status of the network.



7.1.4 Real-Time Flow (Kbps)

The Real-Time Flow page displays the uplink and downlink flow of the Router. The default unit is Kbps, you can change it to be bps and Mbps. The default showing interface is WAN port, if there are several WAN ports, you can choose to show other WAN ports flow information.

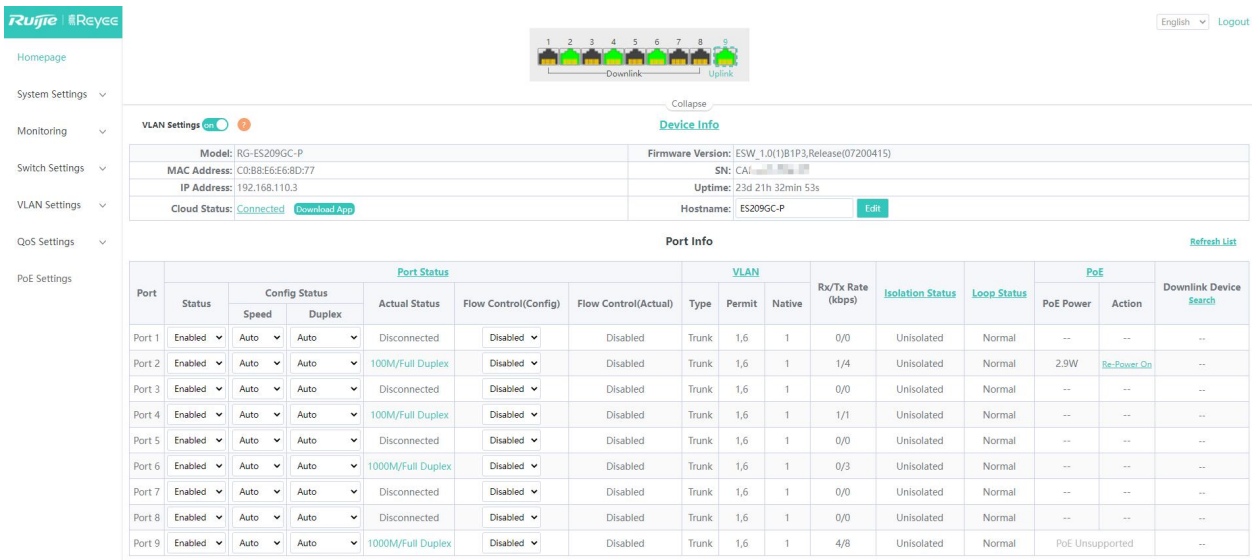


7.1.5 Online Clients

The Online Clients page displays the username, Type (Wired/Wireless), IP and MAC, Current Rate, connected Wi-Fi name, Access Control.

7.2 Reyee ES Switch Monitor

7.2.1 Homepage



Device Info displays the model, firmware version, MAC address, SN, IP address, Uptime, Cloud status and Hostname of the device.

Model: Display the model of the device.

Firmware Version: Display the firmware version of the device.

MAC Address: Display the MAC address of the device.

SN: Display the SN of the device.

IP Address: Display the IP address of the device.

Uptime: Display the running time of the device.

VLAN Setting: Display the VLAN Setting status of the device, click to enable or disable the VLAN Setting function of the device.

Cloud Status: Display the connection status of the device with Ruijie Cloud.

Hostname: Display the hostname of the device, click **Edit** to modify the Hostname of the device

Port Info shows ports status, VLAN configuration, isolation status, loop status, POE status and downlink device.

Port Info Refresh List

Port	Port Status						VLAN			Rx/Tx Rate (kbps)	Isolation Status	Loop Status	PoE		Downlink Device Search
	Status	Config Status		Actual Status	Flow Control(Config)	Flow Control(Actual)	Type	Permit	Native				PoE Power	Action	
		Speed	Duplex												
Port 1	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	Trunk	1,6	1	0/0	Unisolated	Normal	--	--	--
Port 2	Enabled	Auto	Auto	100M/Full Duplex	Disabled	Disabled	Trunk	1,6	1	1/4	Unisolated	Normal	2.9W	Re-Power On	--
Port 3	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	Trunk	1,6	1	0/0	Unisolated	Normal	--	--	--
Port 4	Enabled	Auto	Auto	100M/Full Duplex	Disabled	Disabled	Trunk	1,6	1	1/1	Unisolated	Normal	--	--	--
Port 5	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	Trunk	1,6	1	0/0	Unisolated	Normal	--	--	--
Port 6	Enabled	Auto	Auto	1000M/Full Duplex	Disabled	Disabled	Trunk	1,6	1	0/3	Unisolated	Normal	--	--	--
Port 7	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	Trunk	1,6	1	0/0	Unisolated	Normal	--	--	--
Port 8	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	Trunk	1,6	1	0/0	Unisolated	Normal	--	--	--
Port 9	Enabled	Auto	Auto	1000M/Full Duplex	Disabled	Disabled	Trunk	1,6	1	4/8	Unisolated	Normal	PoE Unsupported		--

Click **Search** below **Downlink Device to** search its downlink devices.

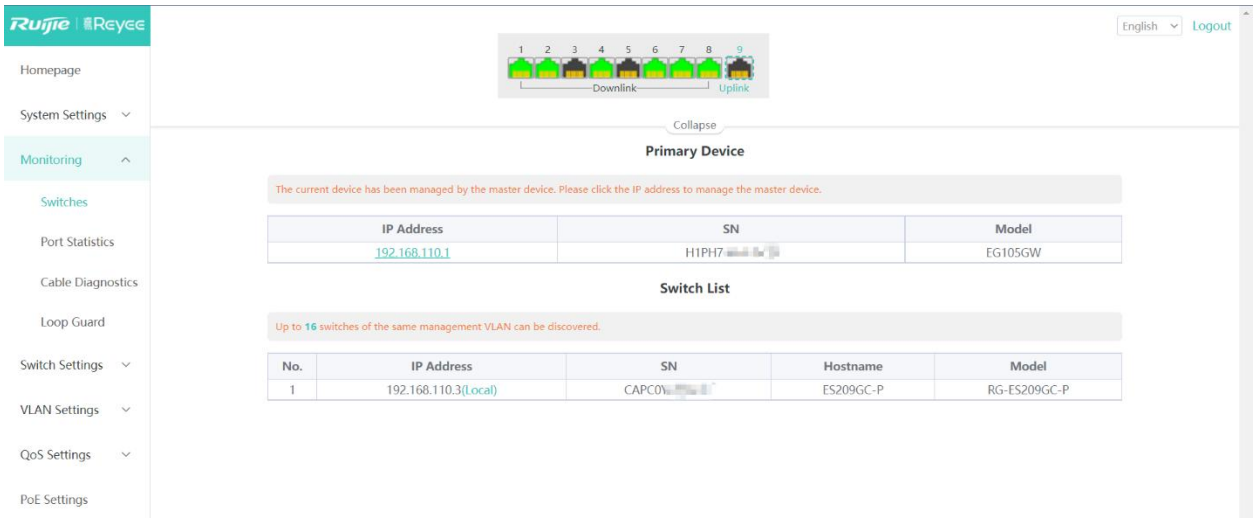
Port	Port Status						VLAN			Rx/Tx Rate (kbps)	Isolation Status	Loop Status	PoE		Downlink Device Search
	Status	Config Status		Actual Status	Flow Control(Config)	Flow Control(Actual)	Type	Permit	Native				PoE Power	Action	
		Speed	Duplex												
Port 1	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	Trunk	1,6	1	0/0	Unisolated	Normal	--	--	--
Port 2	Enabled	Auto	Auto	100M/Full Duplex	Disabled	Disabled	Trunk	1,6	1	1/2	Unisolated	Normal	2.9W	Re-Power On	--
Port 3	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	Trunk	1,6	1	0/0	Unisolated	Normal	--	--	--
Port 4	Enabled	Auto	Auto	100M/Full Duplex	Disabled	Disabled	Trunk	1,6	1	1/0	Unisolated	Normal	--	--	--
Port 5	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	Trunk	1,6	1	0/0	Unisolated	Normal	--	--	--
Port 6	Enabled	Auto	Auto	1000M/Full Duplex	Disabled	Disabled	Trunk	1,6	1	9/1	Unisolated	Normal	--	--	--
Port 7	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	Trunk	1,6	1	0/0	Unisolated	Normal	--	--	--
Port 8	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	Trunk	1,6	1	0/0	Unisolated	Normal	--	--	--
Port 9	Enabled	Auto	Auto	1000M/Full Duplex	Disabled	Disabled	Trunk	1,6	1	4/16	Unisolated	Normal	PoE Unsupported		--

To view the MAC and VLAN information of the downlink devices by clicking **View:**

Port	Port Status						VLAN			Rx/Tx Rate (kbps)	Isolation Status	Loop Status	PoE		Downlink Device Search
	Status	Config Status		Actual Status	Flow Control(Config)	Flow Control(Actual)	Type	Permit	Native				PoE Power	Action	
		Speed	Duplex												
Port 1	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	Trunk	1,6	1	0/0	Unisolated	Normal	--	--	View
Port 2	Enabled	Auto	Auto	100M/Full Duplex	Disabled	Disabled	Trunk	1,6	1	1/2	Unisolated	Normal	MAC:C4:70:AB:A2:C3:6A-->VLAN ID:1		View
Port 3	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	Trunk	1,6	1	0/0	Unisolated	Normal	--	--	View
Port 4	Enabled	Auto	Auto	100M/Full Duplex	Disabled	Disabled	Trunk	1,6	1	1/0	Unisolated	Normal	--	--	View
Port 5	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	Trunk	1,6	1	0/0	Unisolated	Normal	--	--	View
Port 6	Enabled	Auto	Auto	1000M/Full Duplex	Disabled	Disabled	Trunk	1,6	1	9/1	Unisolated	Normal	--	--	View
Port 7	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	Trunk	1,6	1	0/0	Unisolated	Normal	--	--	View
Port 8	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	Trunk	1,6	1	0/0	Unisolated	Normal	--	--	View
Port 9	Enabled	Auto	Auto	1000M/Full Duplex	Disabled	Disabled	Trunk	1,6	1	4/16	Unisolated	Normal	PoE Unsupported		View

7.2.2 Monitoring

1.1 Switches



Primary Device

When this switch is managed by master device in SON (some functions are not available, such as setting the device management password).

The list displays the IP, SN and Model information of the master device in SON, click on the IP address can redirect to the web interface of the Master device.

Switch List

The device can discover other ES switches that belong to the same management VLAN and display the IP, SN, Hostname and model information of other switches in the list. The number of discovered switches in a management VLAN varies with the switch models:

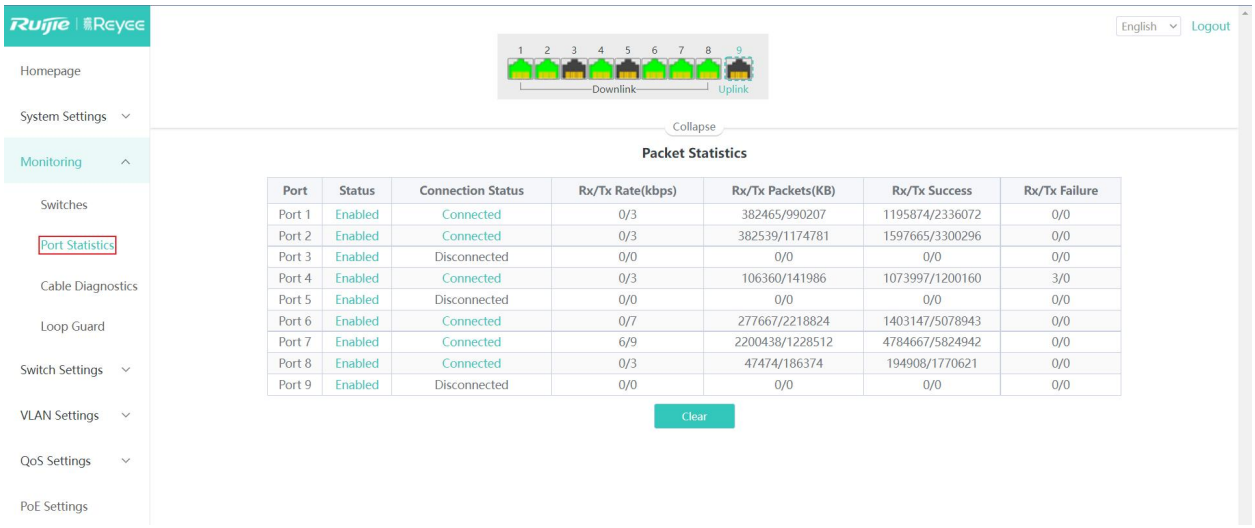
The following models can discover up to 32 switches in the management VLAN: RG-ES226GC-P, RG-ES218GC-P, RG-ES224GC, and RG-ES216GC.

The following models can discover up to 16 switches in the management VLAN: RG-ES205C-P, RG-ES205GC-P, RG-ES209C-P, and RG-ES209GC-P.

The first entry shows the information about the current device and other entries show information about the discovered devices. You can click the IP address to redirect to the eWeb management of a specific device (login is required).

1.2 Port Statistics

The Port Statistics page displays the statistics and status of device ports, such as port Rx/Tx rate and Rx/Tx packets.



Port: Displays the port number of the switch.

Status: Displays the status of the port.

Connection Status: Displays the connection status of the port.

Rx/Tx Rate (kbps): Displays the received and transmitted rates of the port.

Rx/Tx Packets (KB): Displays the traffic of receive and transmit packets of the port.

Rx/Tx Success: Displays the amount of traffic for packets successfully received and transmitted of the port.

Rx/Tx Failure: Displays the amount of traffic for packets that failed to be received and transmitted of this port.

1.3 Cable Diagnostics

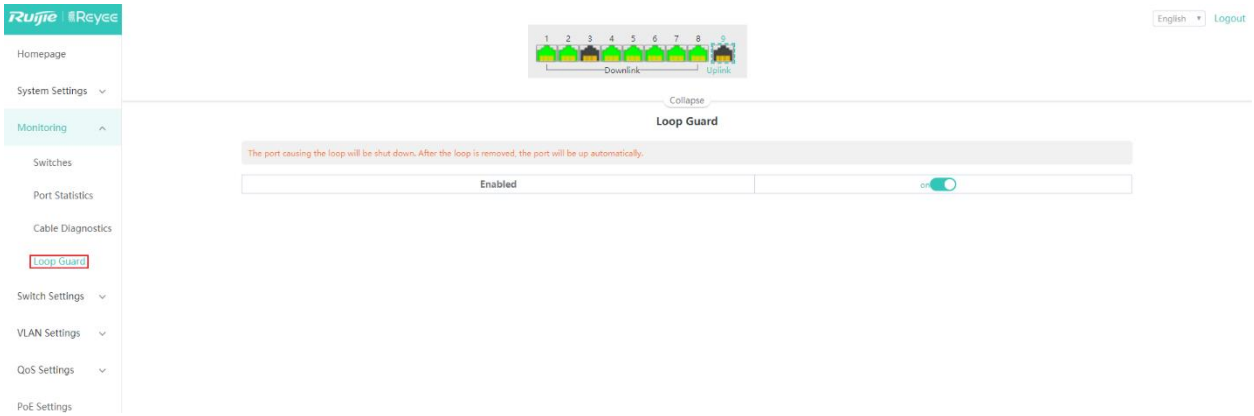
Cable Diagnostics displays the cable condition of the corresponding port (e.g., whether the cable is short-circuited, disconnected, etc.), click the Start button to start cable diagnostics:

Cable Diagnostics

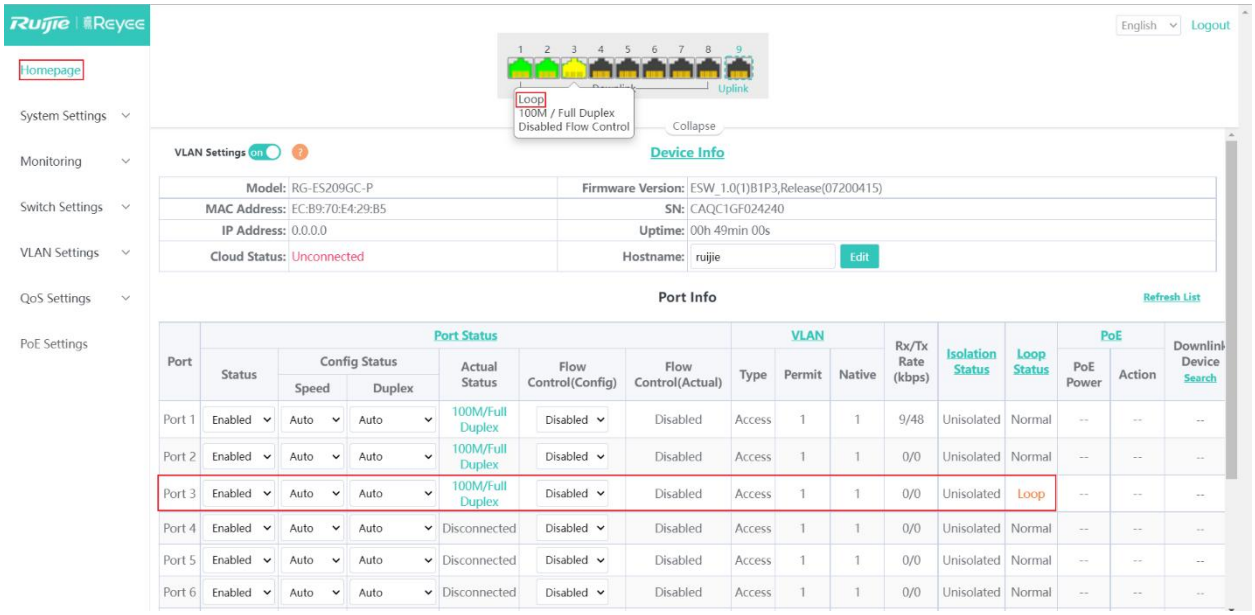
	Port	Test Result	Details
☐	Port 1	-	-
☑	Port 2	Normal	The cable works well.
☑	Port 3	Disconnected	Please check cable connection or replace the cable.
☐	Port 4	-	-
☐	Port 5	-	-
☐	Port 6	-	-
☐	Port 7	-	-
☐	Port 8	-	-
☐	Port 9	-	-

Start Start All

1.4 Loop Guard



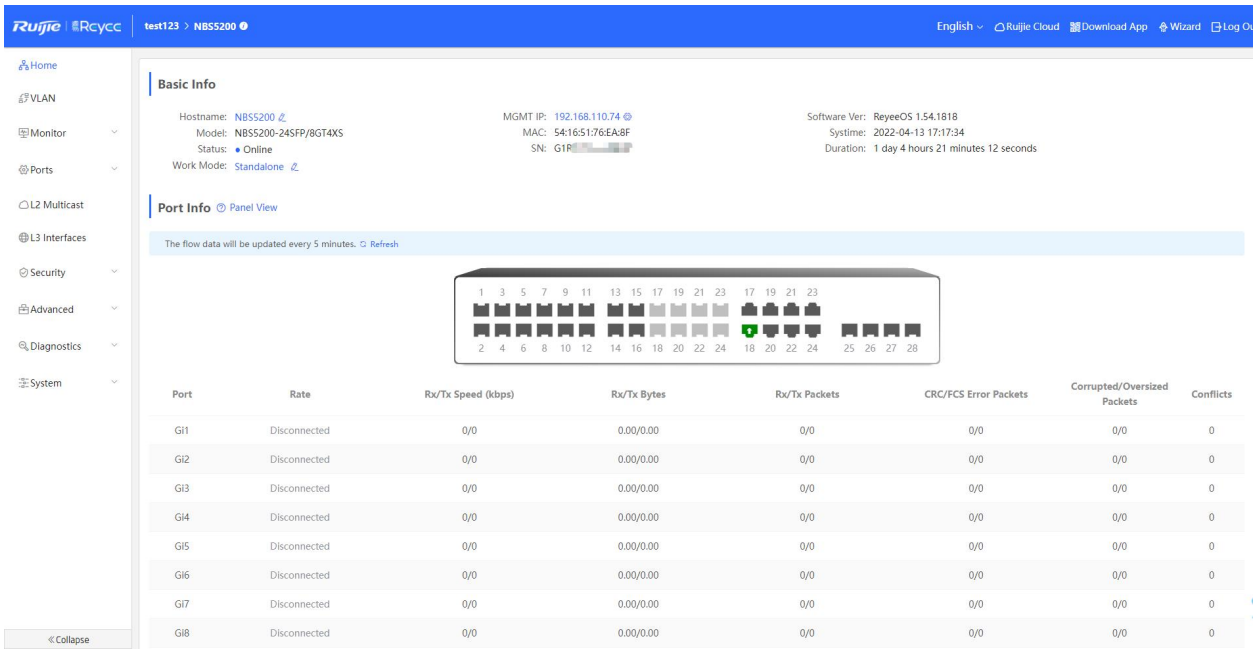
After loop guard is enabled (which is disabled by default), the port causing a loop on the current device will be automatically disabled. After the loop is removed, the port is restored automatically.



7.3 Reyee NBS Switch Monitor

7.3.1 Home

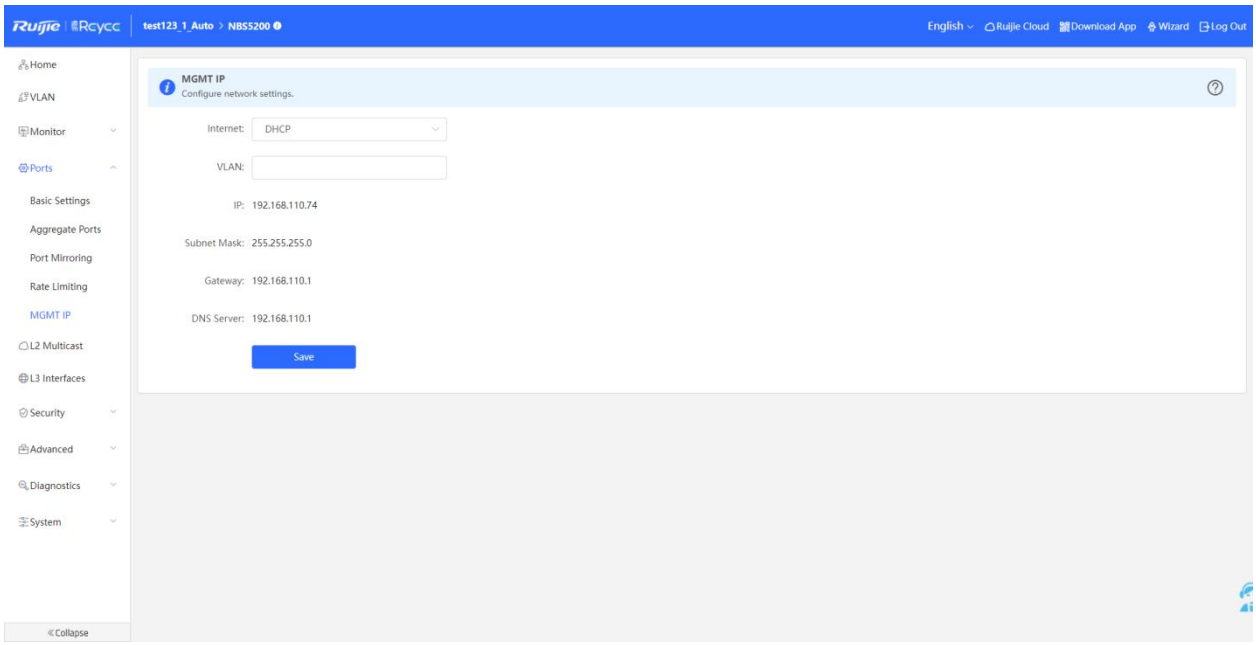
The **Home** module displays the basic information about the device and the switch ports.



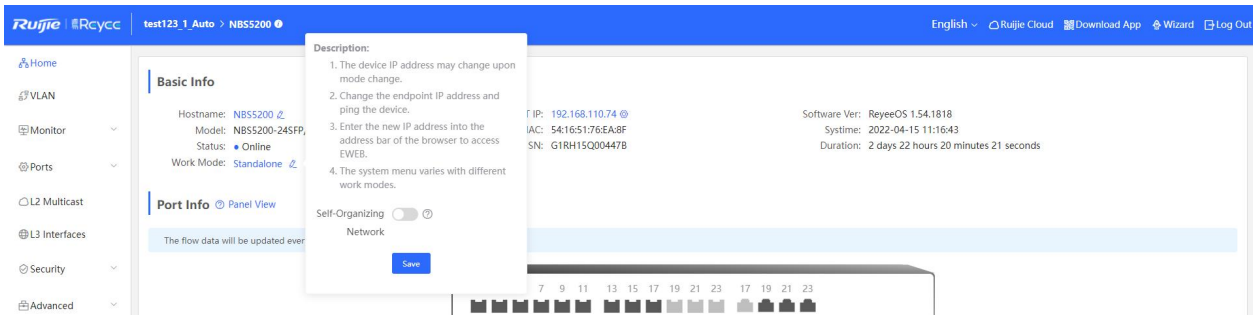
The **Basic Info** area allows you to configure the device name and the management IP address, and modify the work mode of devices.

Click on the button to the right of the Hostname to change the switch's Hostname.

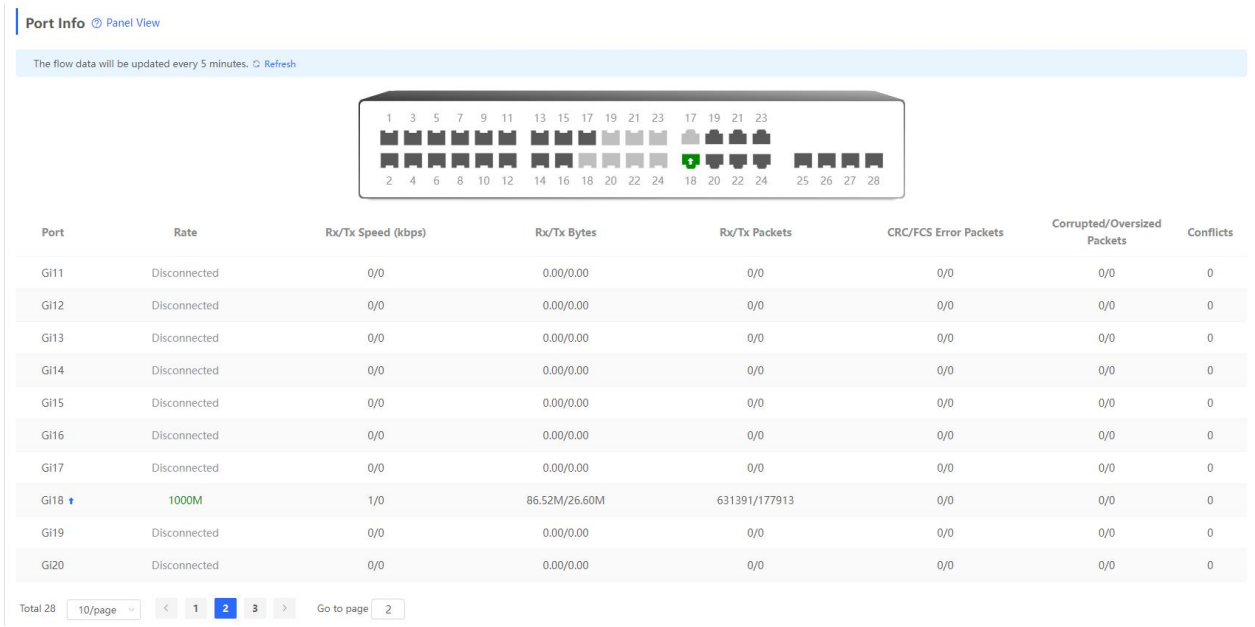
Click on the button to the right of the MGMT IP will redirect you to the device's management IP configuration screen.



Click the button to the right of Work Mode to switch the switch's work mode.



The **Port Info** area displays the details of all ports.



Port: Display the port number of the device.

Rate: Display the negotiation rate of the port when the port is Up.

Rx/Tx Speed (kbps): Display the received and transmit rates of the port.

Rx/Tx Bytes: Display the received and transmit traffic of the port.

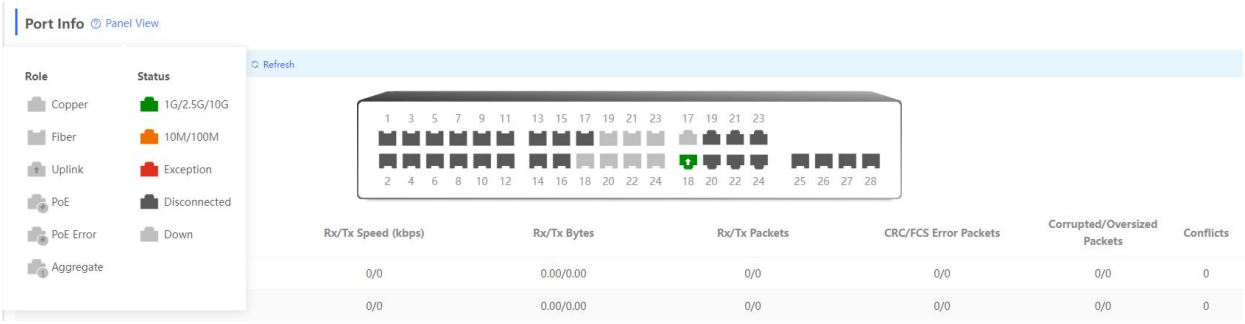
Rx/Tx Packets: Display the number of packets received and transmitted by the port.

CRC/FCS Error Packets: Display the number of packets with CRC/FCS errors on the port.

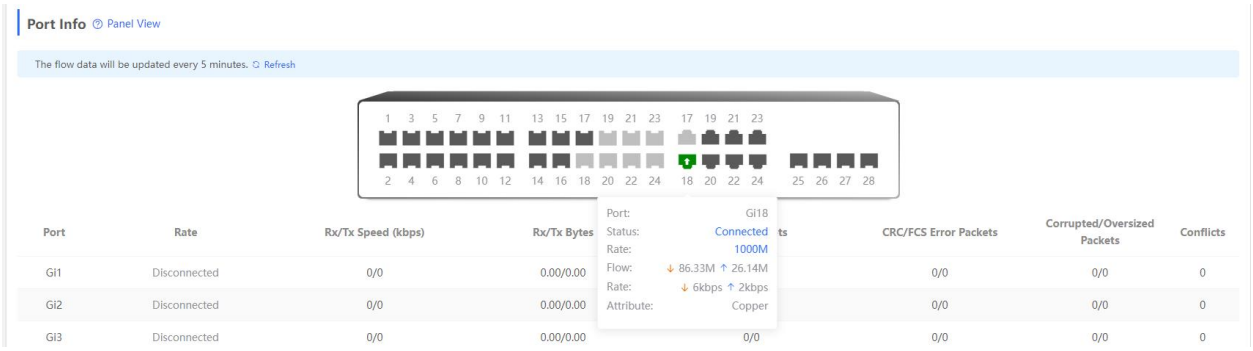
Corrupted/Oversized Packets: Display the number of Corrupted/Oversized packets of the port.

Conflicts: Display the number of conflicts on the port, when the interface is negotiated in half-duplex mode, there may have packet receive and transmit conflicts.

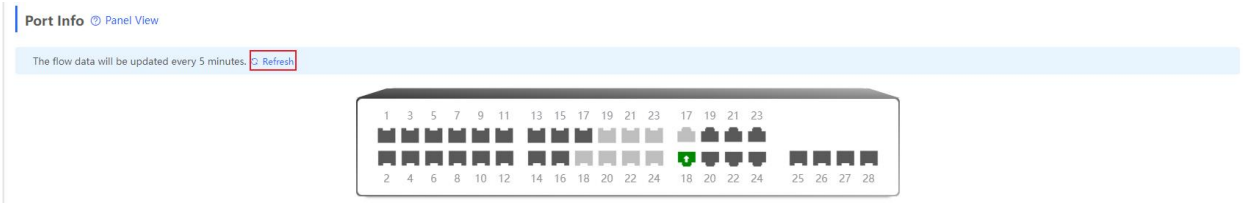
Click **Panel View** to display the icon color and type of each port.



Move the cursor to the port icon on the port panel to display more information of the port.



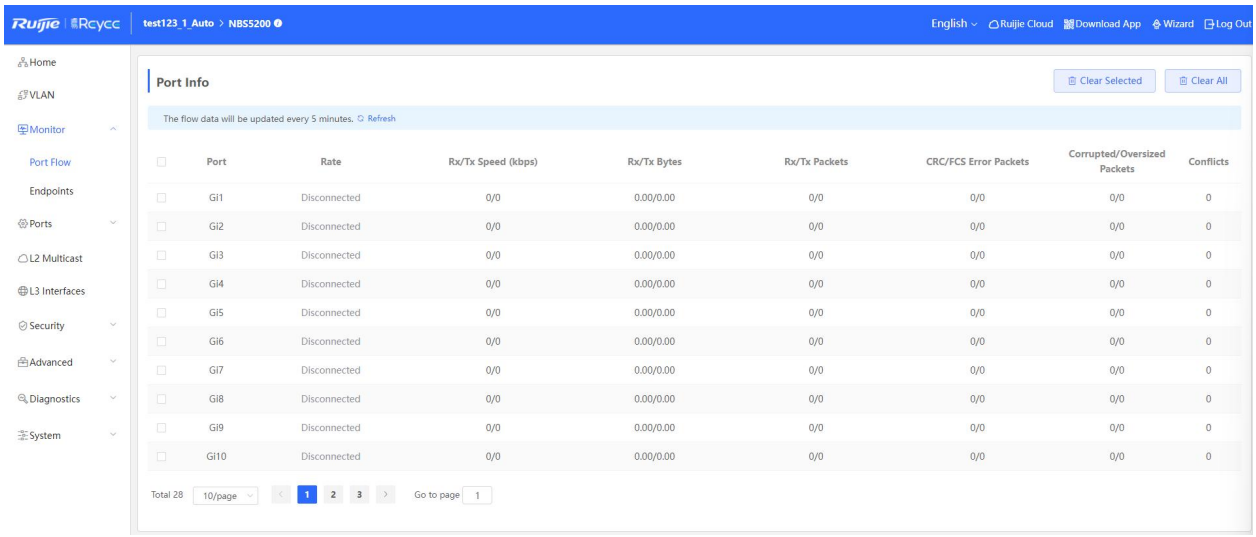
The flow data will be updated every 5 minutes, you can click **Refresh** above the port panel to obtain the latest port traffic and status information.



7.3.2 Monitor

1.1 Port Flow

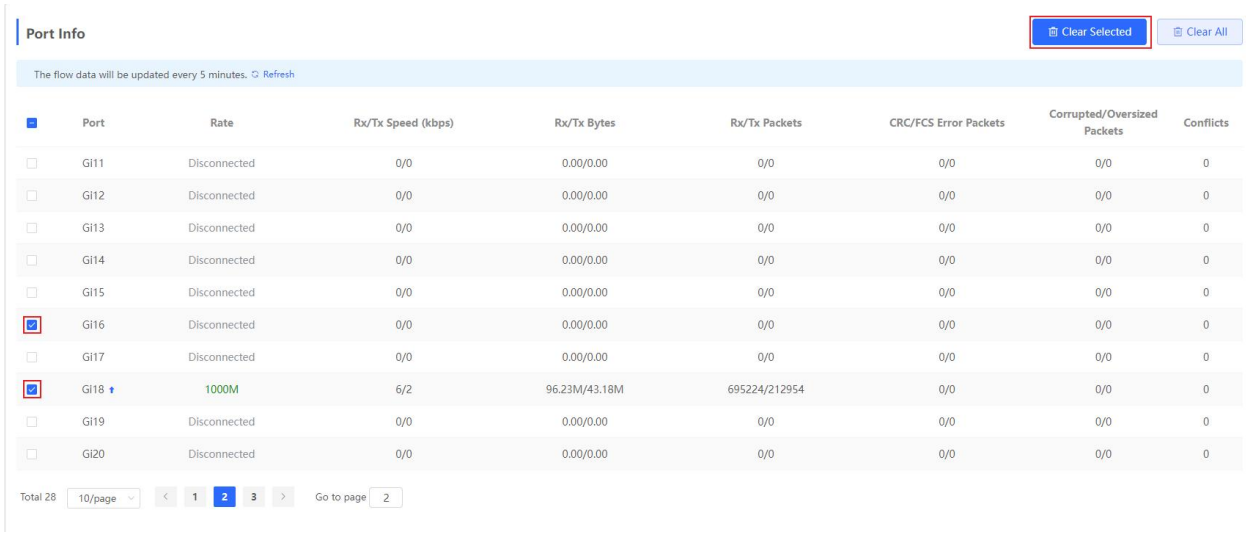
The **Port Flow** module displays port flow data.



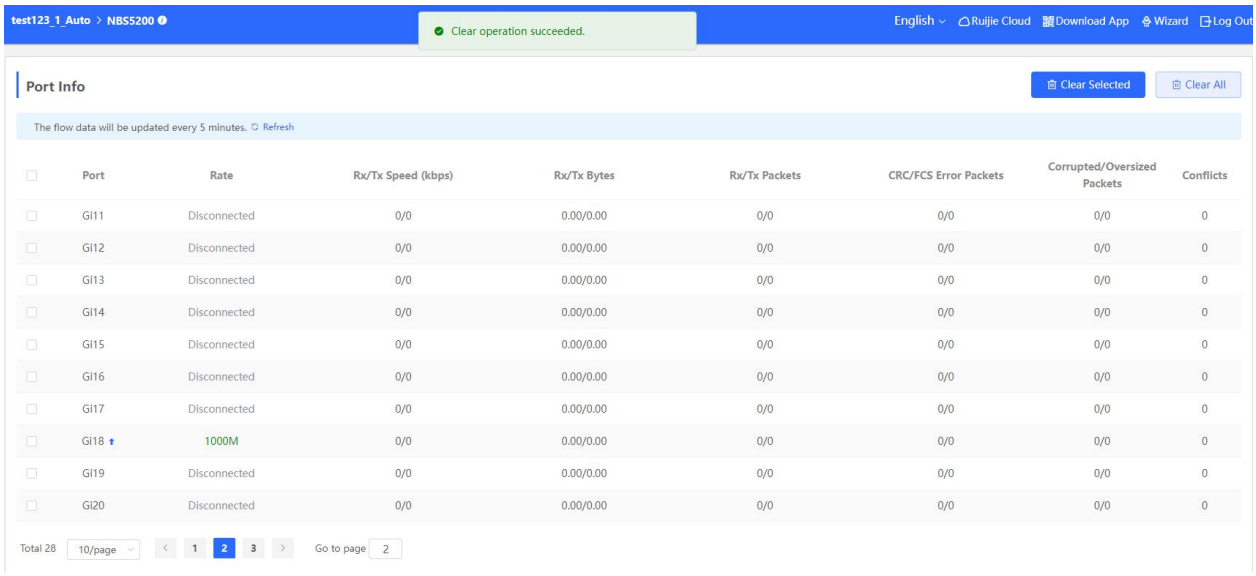
Aggregate port flow will also be displayed. Traffic of an aggregate port is the sum of traffic of all member ports.

Batch Clearing Data

Select multiple entries in **Port Info** and click **Clear Selected**.

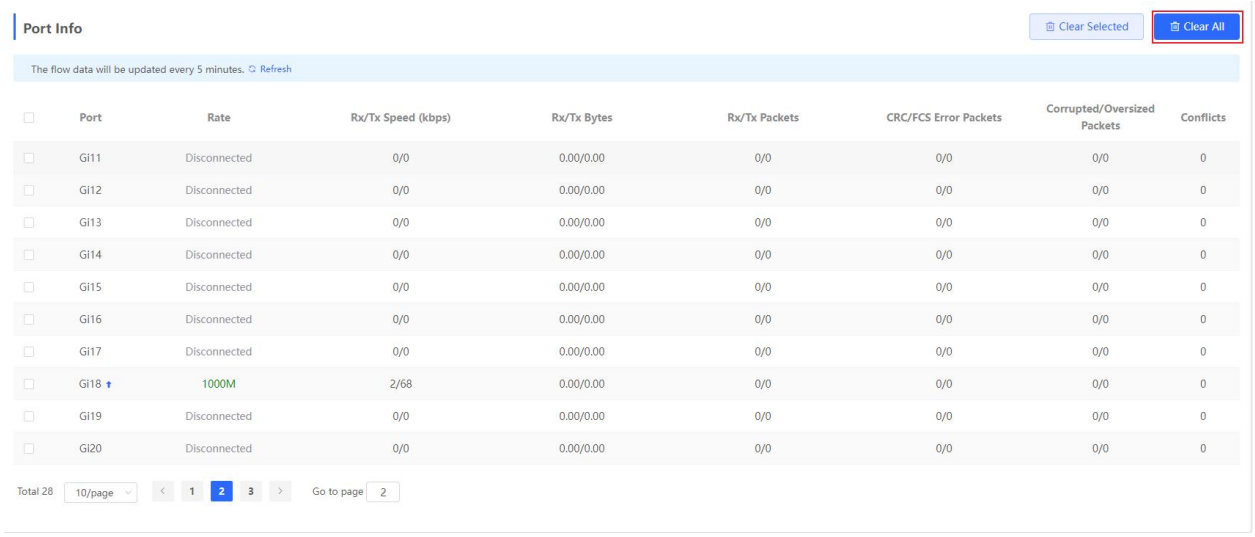


The message "Clear operation succeeded." is displayed.



Clear All

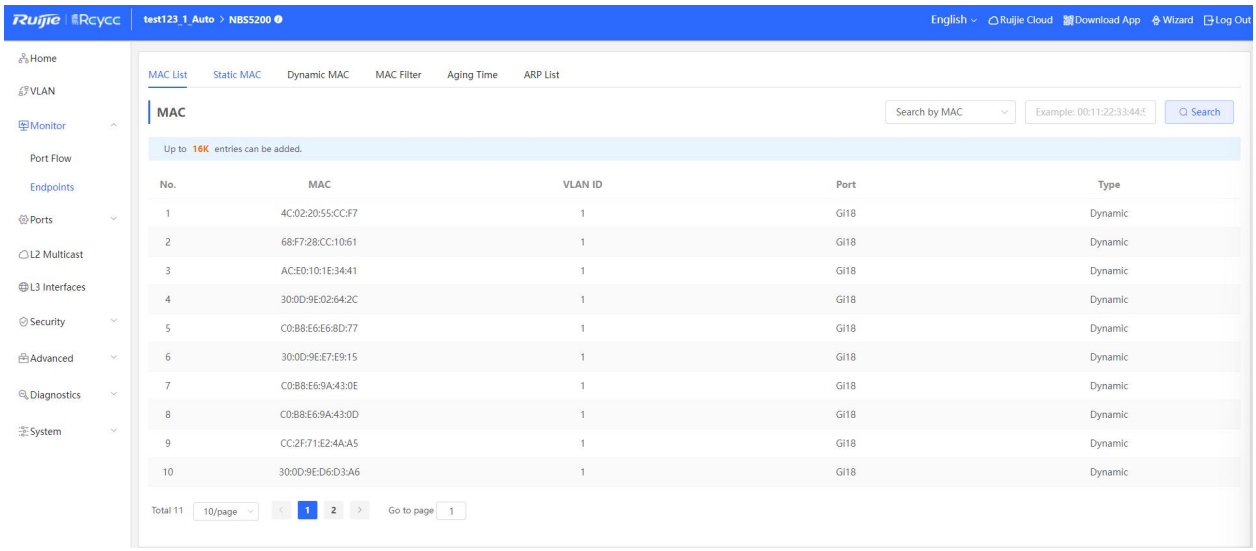
Click **Clear All** to clear statistics of port traffic and other data.



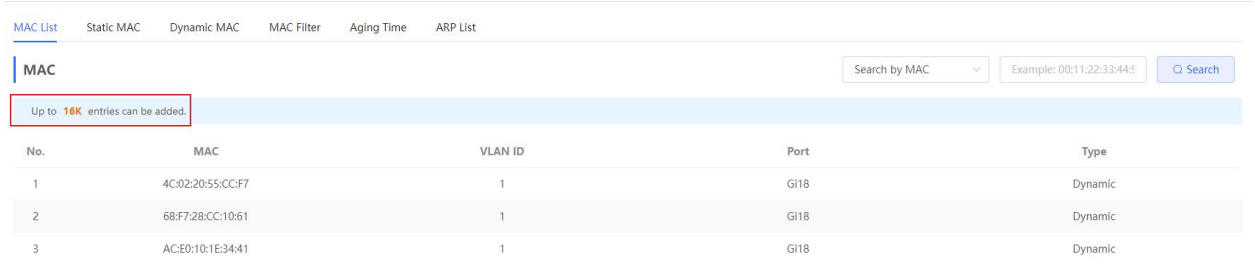
1.2 End points /Clients

a) MAC List

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



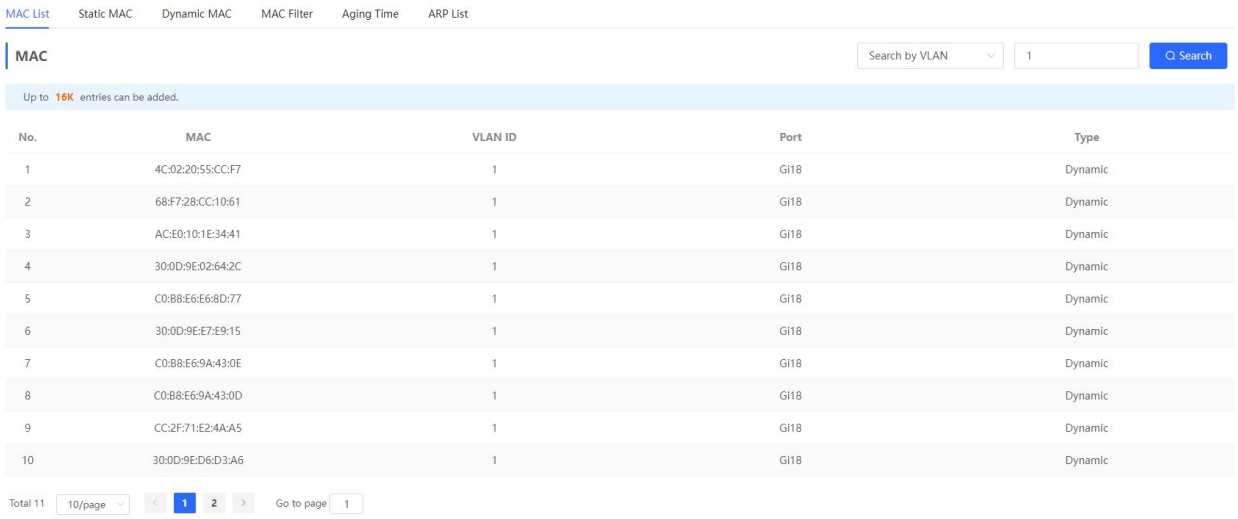
The MAC address capacity varies with the device, you can see above the list.



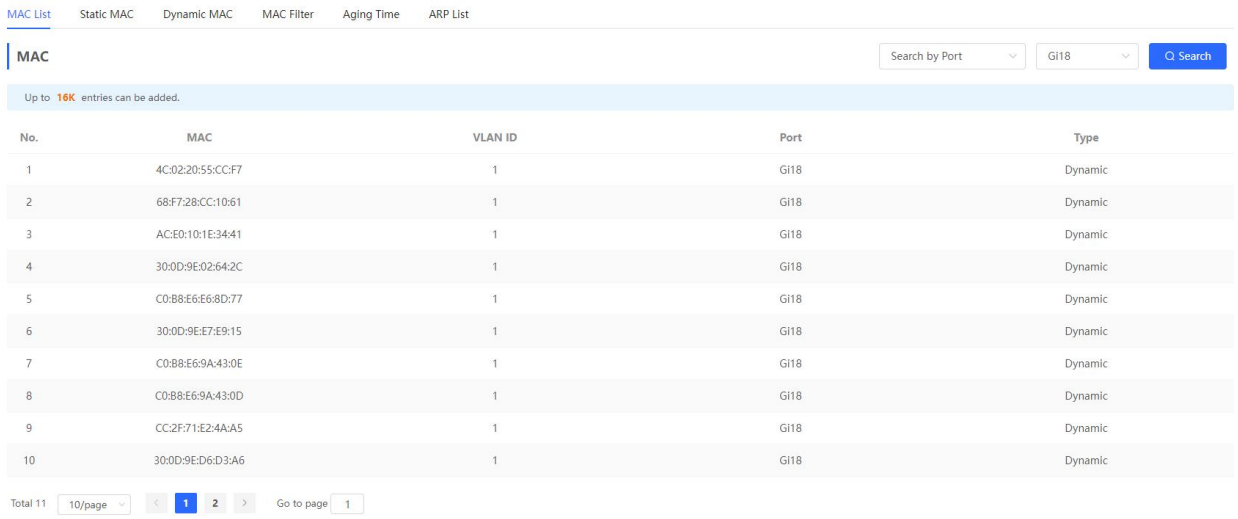
Select the search types (**Search by MAC, Search by VLAN,** or **Search by Port**), enter the term to be searched for, and click **Search** to filter MAC addresses that meet the search conditions.

Search by MAC

Search by VLAN

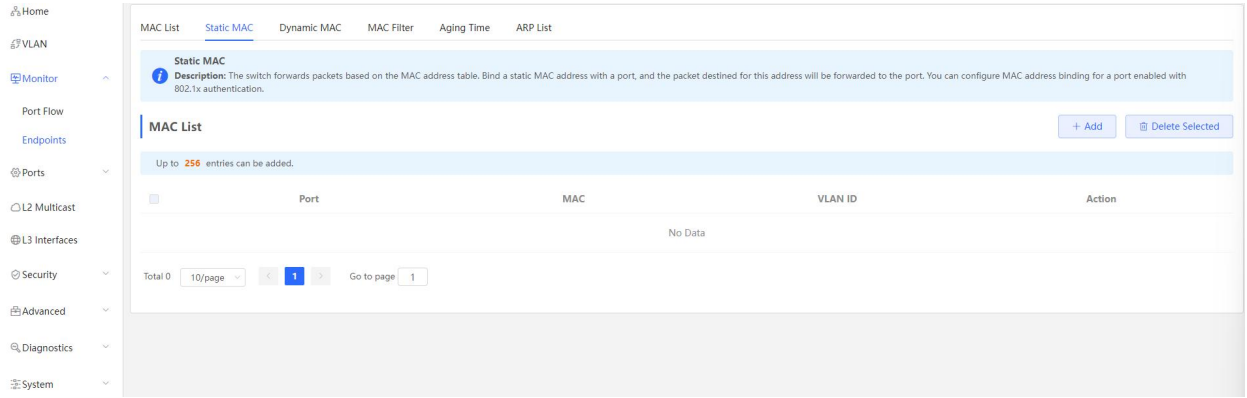


Search by Port



b) Static MAC

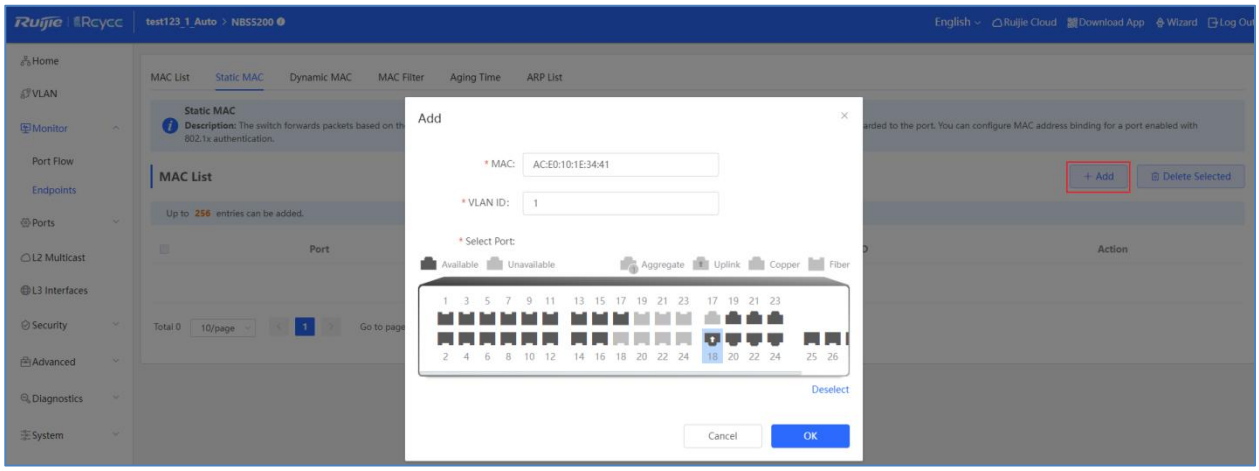
The **Static MAC** page displays the MAC-port binding relationship.



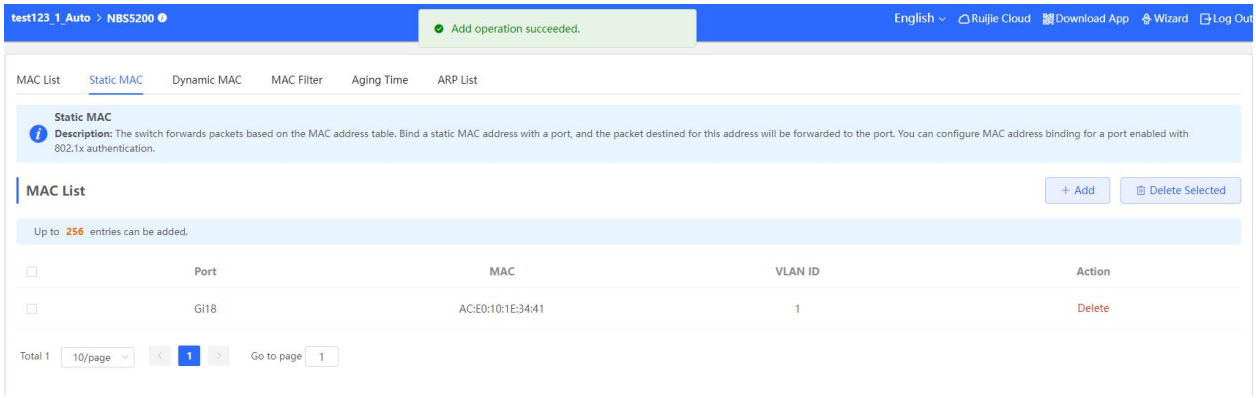
The switch forwards packets based on the MAC address table. Binding the static MAC address with a port, and the packet destined for this address will be forwarded to the port. You can configure the MAC address binding for a port enabled with 802.1x authentication.

Adding a static address

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

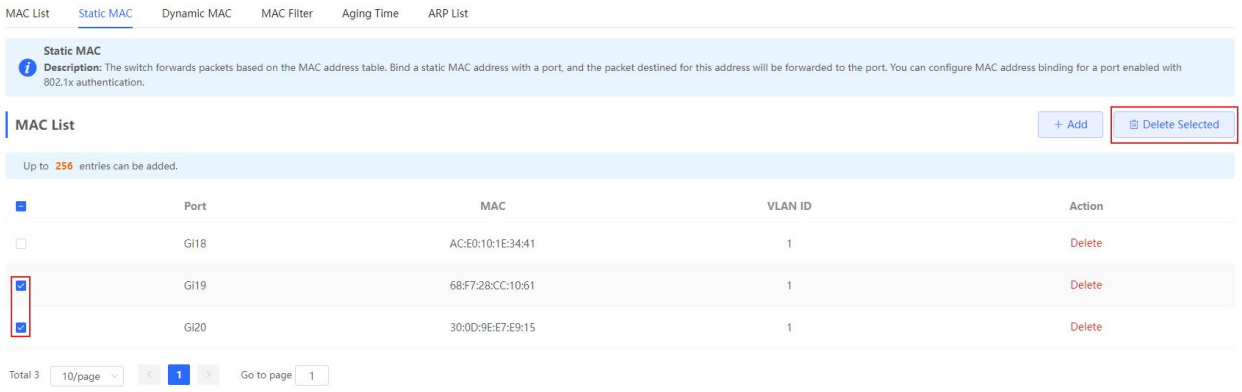


When the message "Add operation succeeded." is displayed, the MAC list is updated.

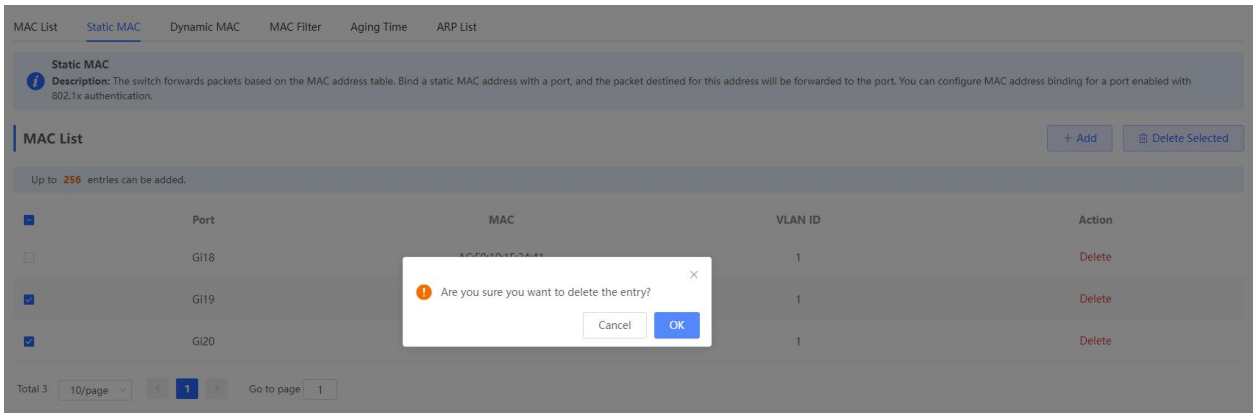


Batch deleting static MAC addresses/Deleting a single static MAC address

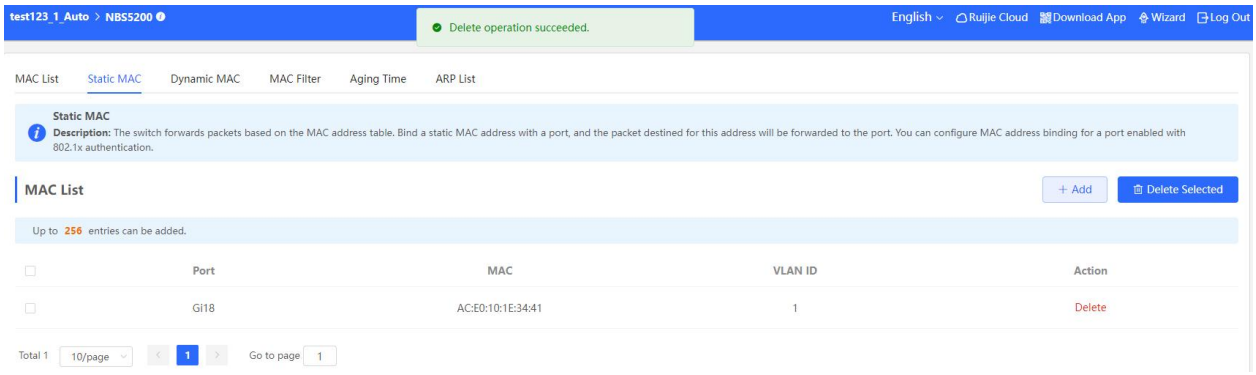
Select the target MAC address in MAC List, and click **Delete** Selected. In the displayed confirmation box, click **OK**.



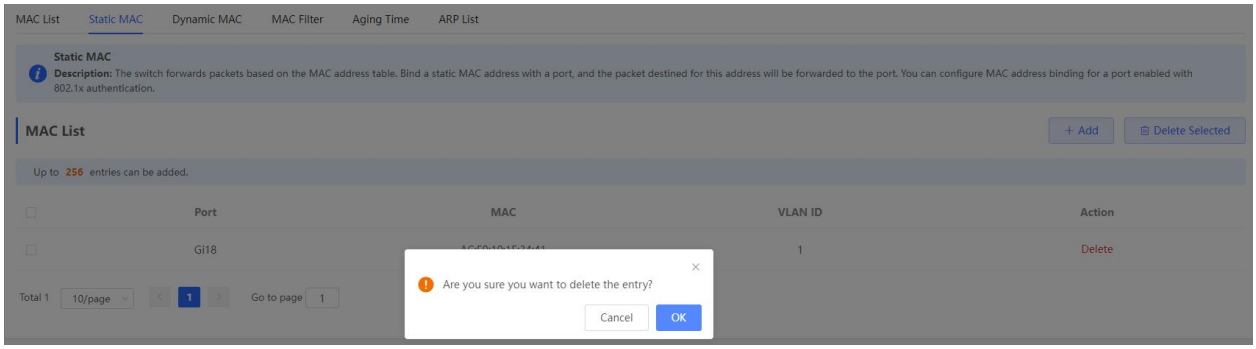
The message "Are you sure you want to delete the entry?" is displayed. In the displayed confirmation box, click **OK** in the displayed dialog box.



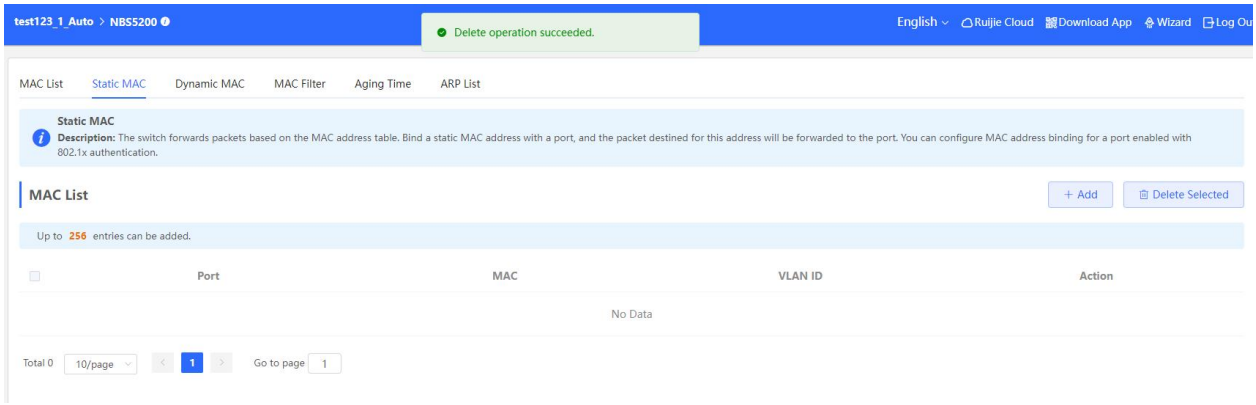
The message indicating successful deletion is displayed, and the MAC list is updated.



Click **Delete** in the **Action** column. The message "Are you sure you want to delete the entry?" is displayed. In the displayed confirmation box, click **OK** in the displayed dialog box.

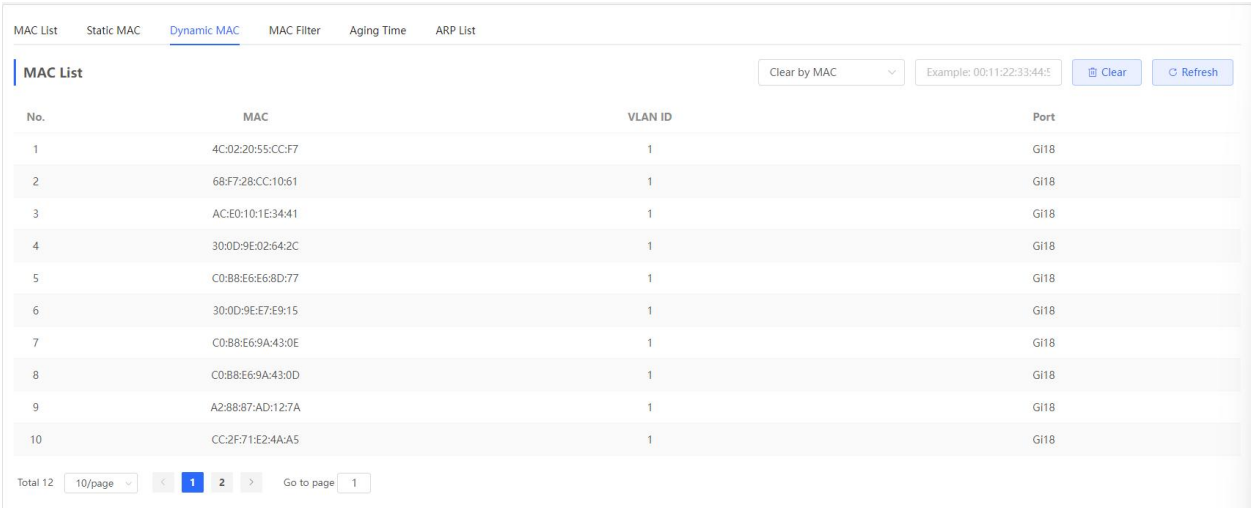


The message "Delete operation succeeded." is displayed.



c) Dynamic MAC

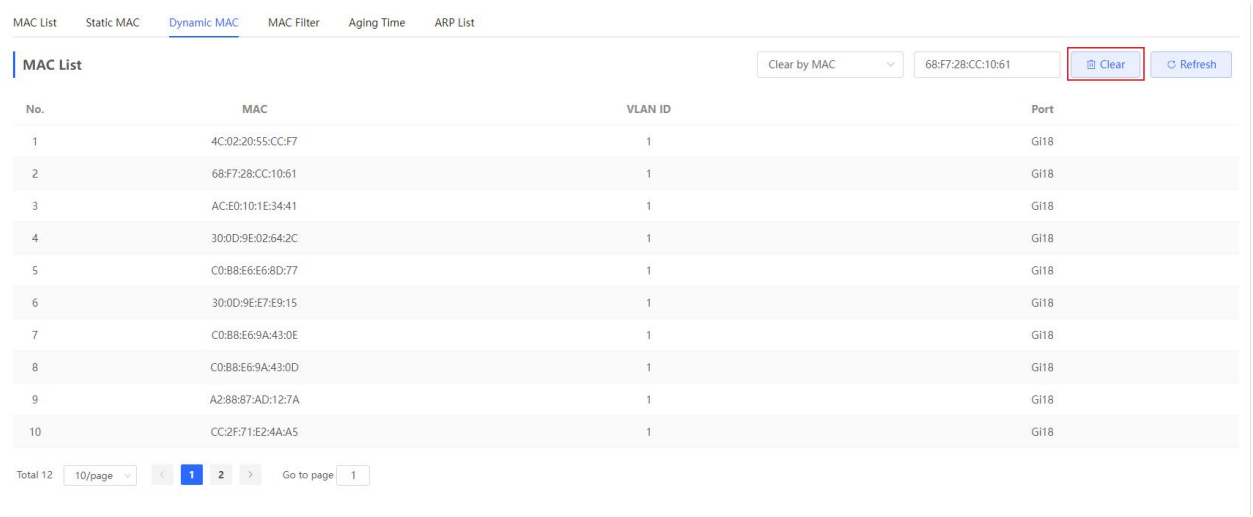
The **Dynamic MAC** page displays dynamic MAC addresses learned by the device.



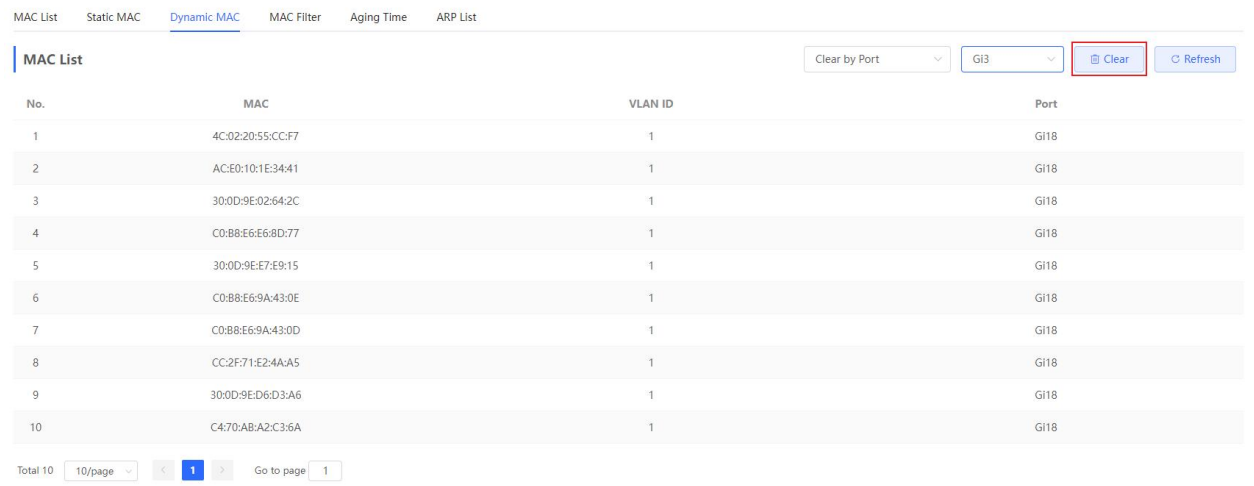
Clear

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

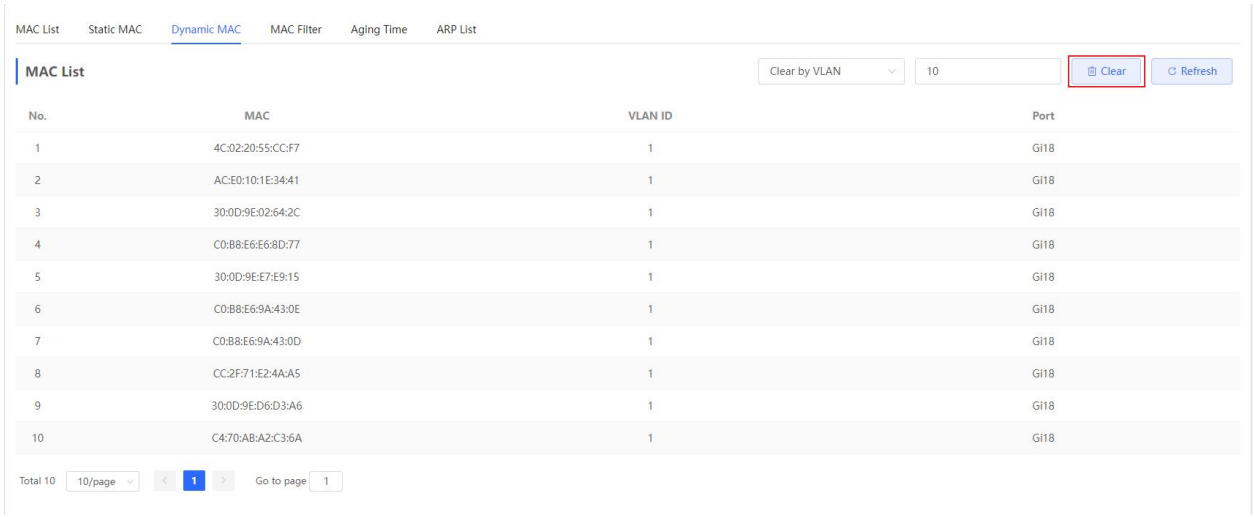
Clear by MAC



Clear by Port

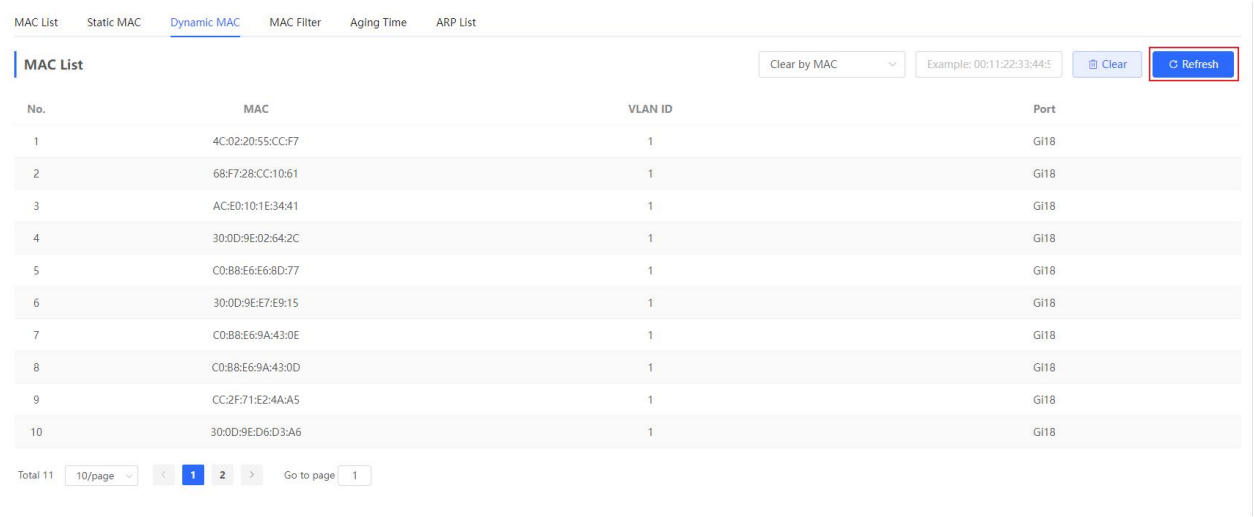


Clear by VLAN



Refresh

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



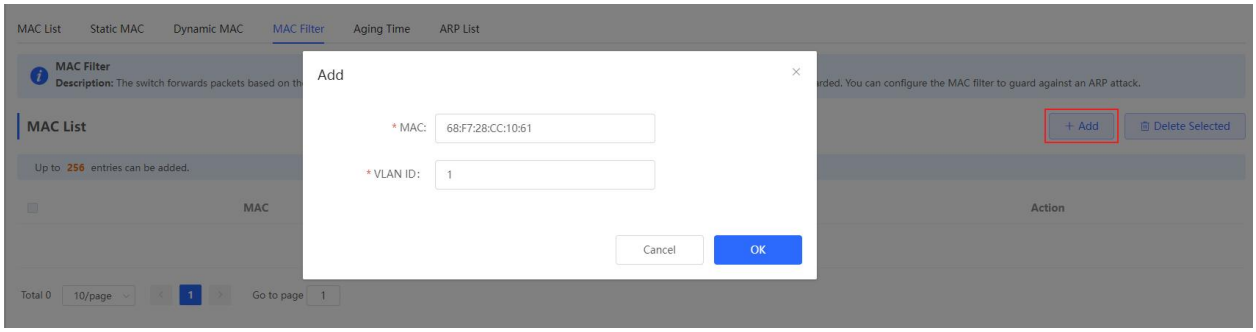
d) MAC Filter

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

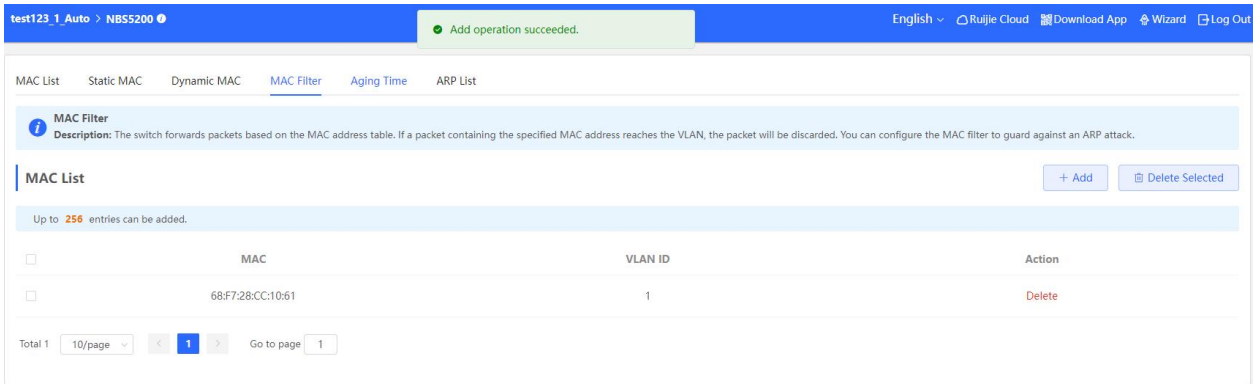
The switch forwards packets based on the MAC address table. If the packet containing the specified MAC address reaching to the VLAN, the packets will be discarded. You can configure MAC address filter to guard against an ARP attack.

Adding a MAC address to be filtered

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

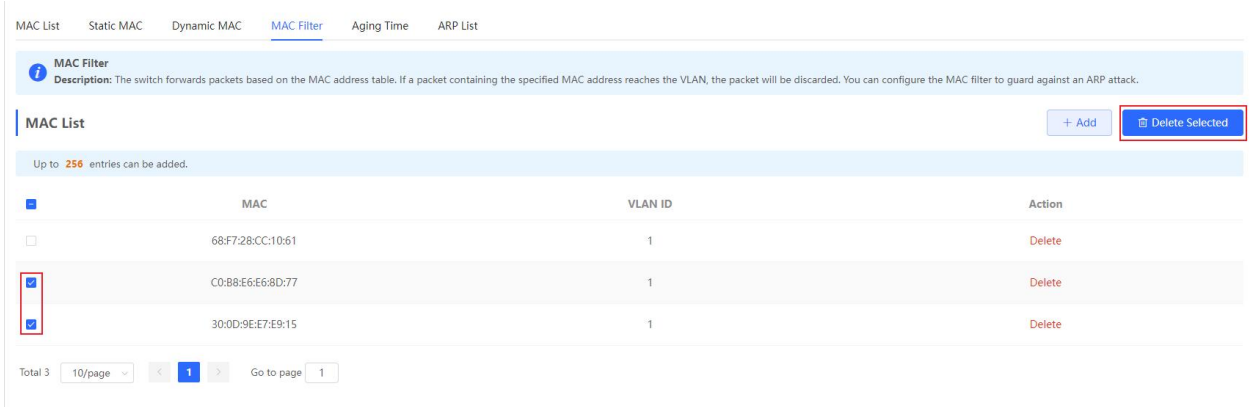


The message "Add operation succeeded." is displayed and the MAC list is updated.

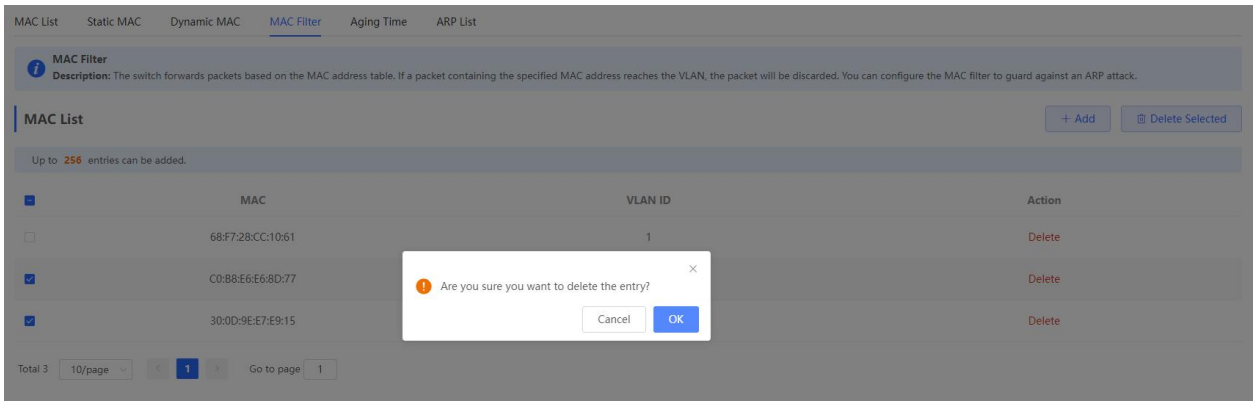


Batch deleting MAC addresses/Deleting a single MAC address

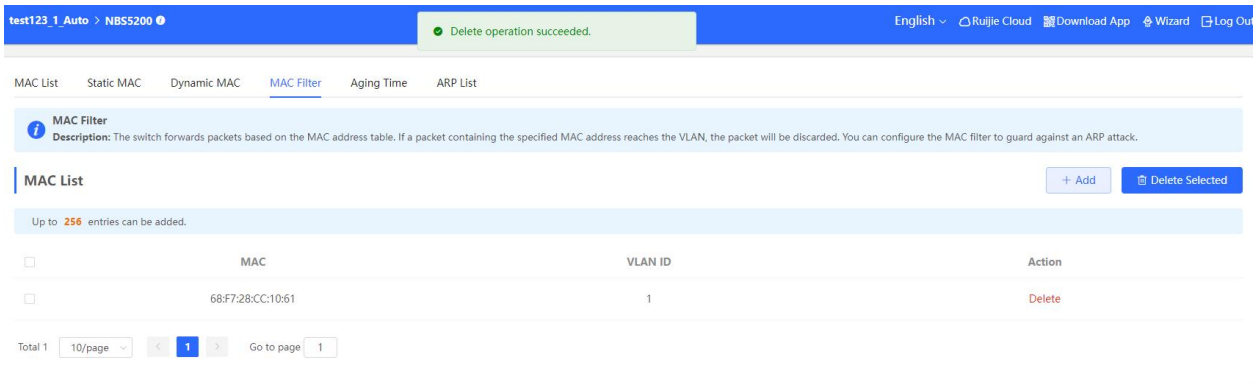
Select the target MAC address, and click **Delete** Selected. In the displayed confirmation box, click **OK**.



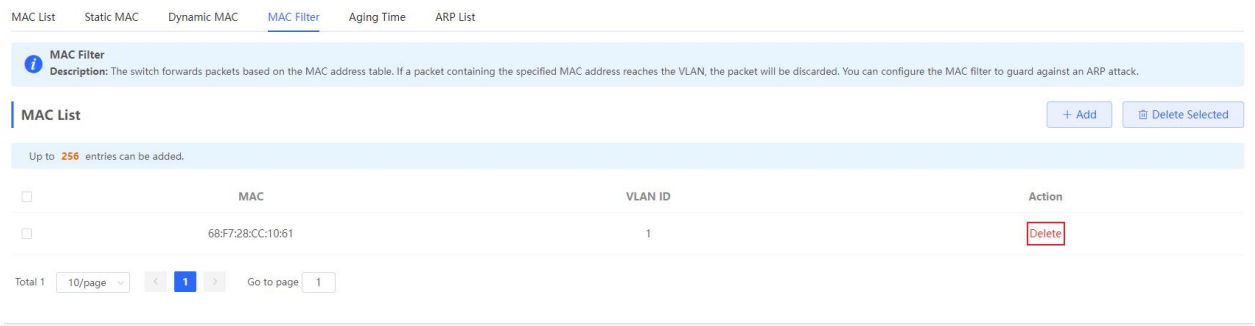
The message "Are you sure you want to delete the entry?" is displayed. In the displayed confirmation box, click **OK** in the displayed dialog box.



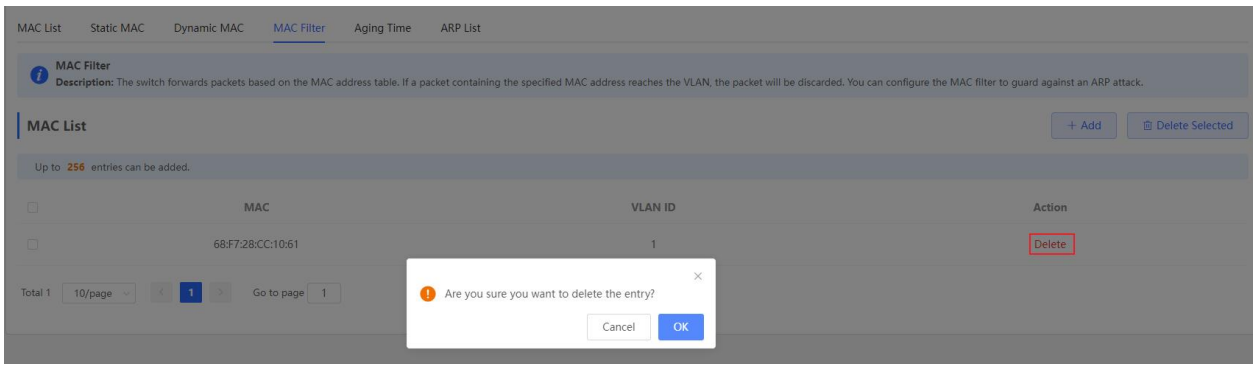
The message "Delete operation succeeded.” is displayed and the MAC list is updated.



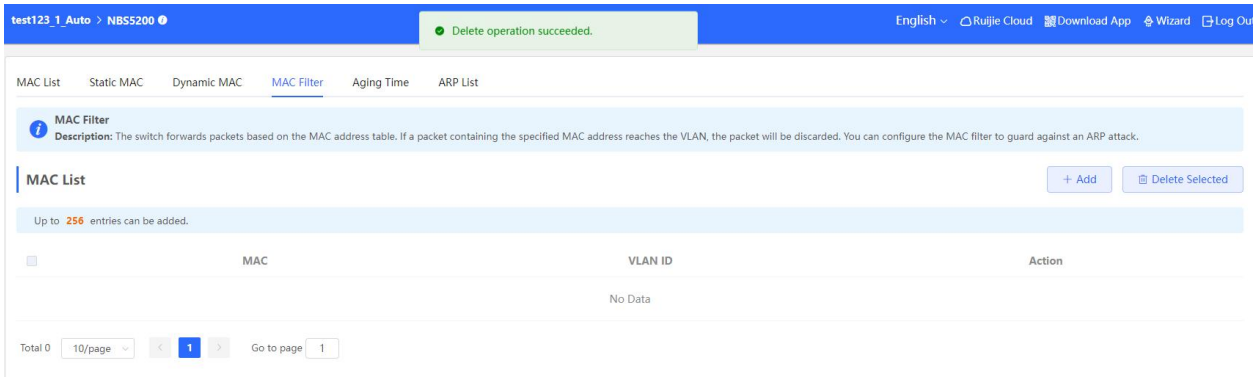
Click **Delete** in the **Action** column.



The message "Are you sure you want to delete the entry?” is displayed. In the displayed confirmation box, click **OK** in the displayed dialog box.

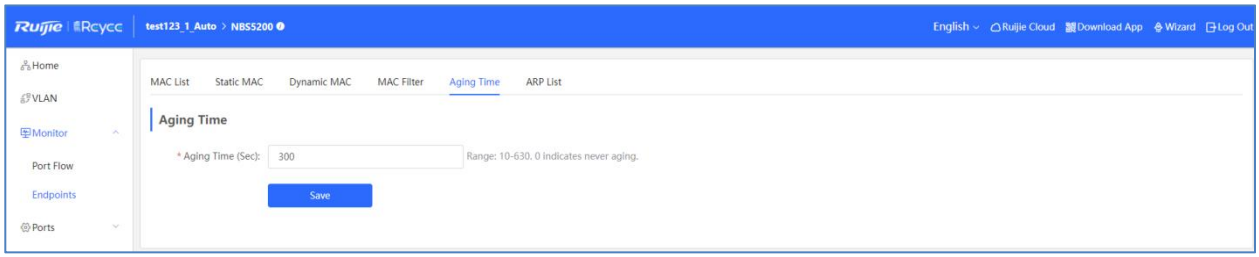


The message "Delete operation succeeded." is displayed.



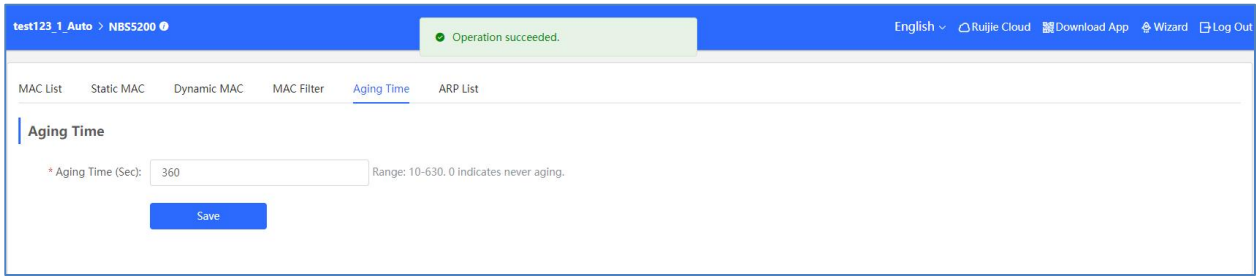
e) Aging Time

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



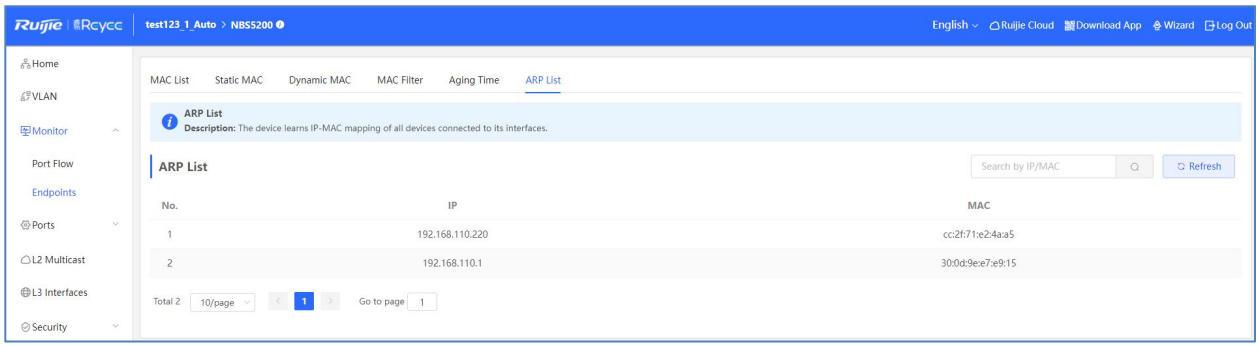
The aging time of the device ranges from 10 to 630 seconds. The value 0 indicates that the MAC addresses do not age.

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



f) ARP List

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

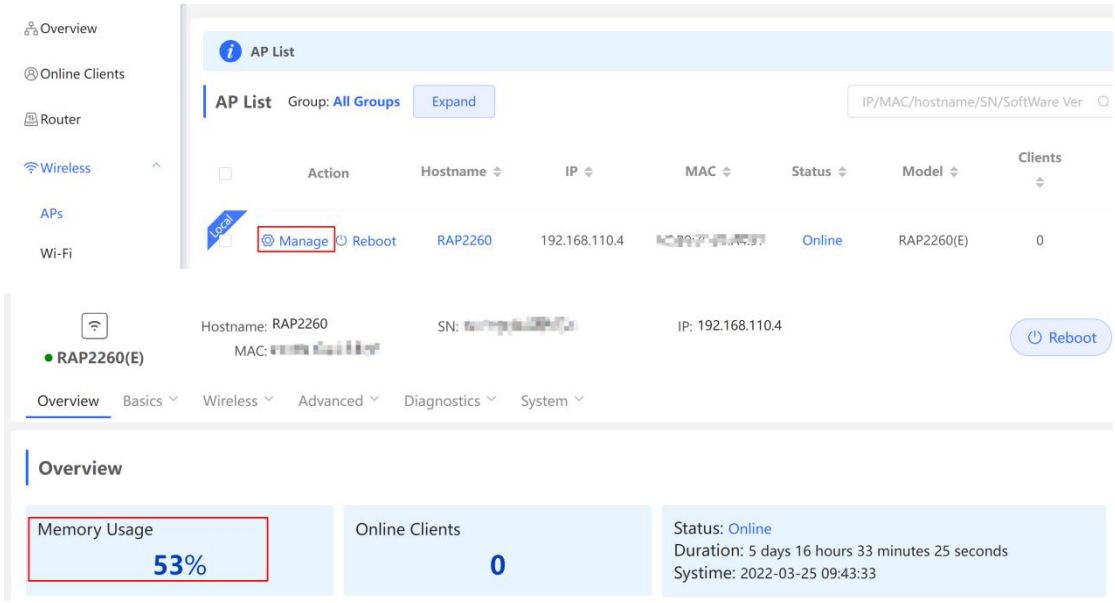


7.4 Reyee Access Point Monitor

The overview page displays **Memory Usage**, **Wireless Information**, **Device Information**, and **More** will be displayed in the Overview Page.

7.4.1 Memory Usage

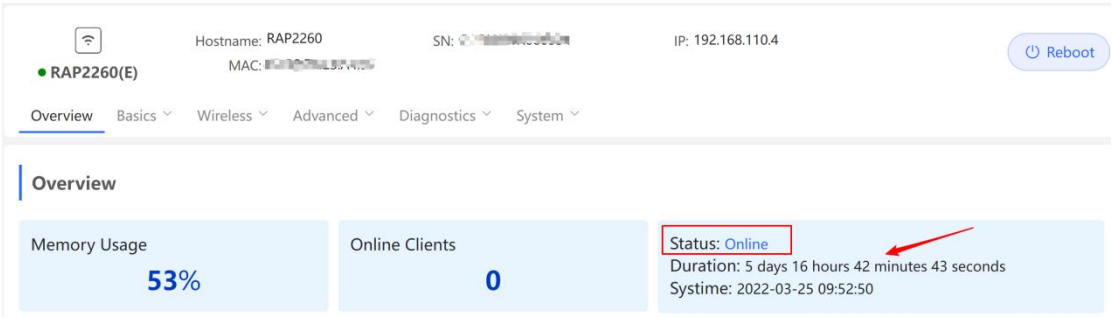
Click **Wireless->APs->Manage** to manage the device after loging in the Eweb interface of Reyee AP.



The normal Memory Usage is between 40%-70%. The reason why it so high when there isn't clients is that memory usage is pre-allocated.

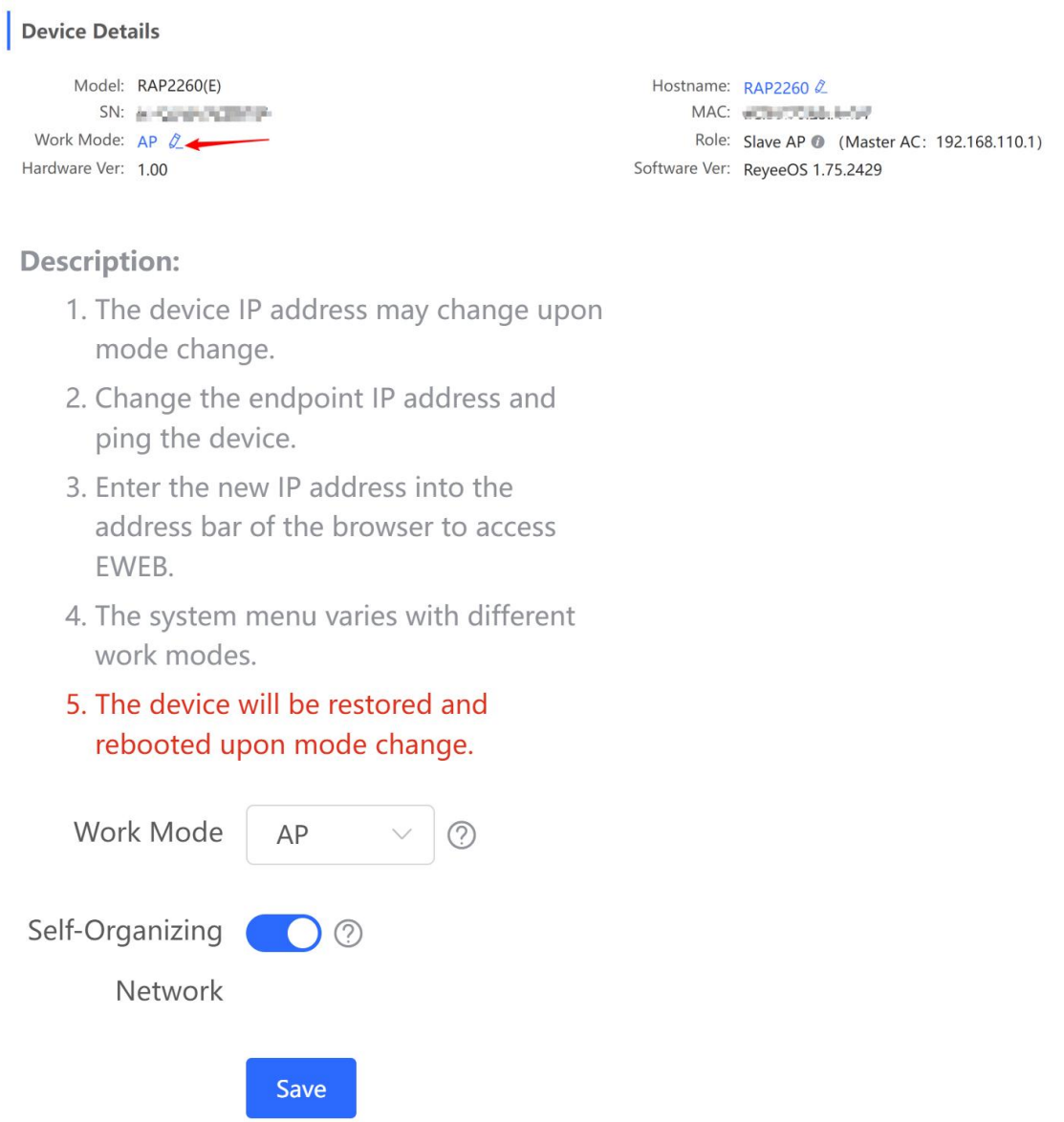
7.4.2 Device Status

The **Device Status** shows whether the device is online and how long it has been online. The "online" here is the SON feature of the Reyee device and has nothing to do with Ruijie Cloud.



7.4.3 AP Working Mode

You can click **Work Mode** to switch the working mode of the device：



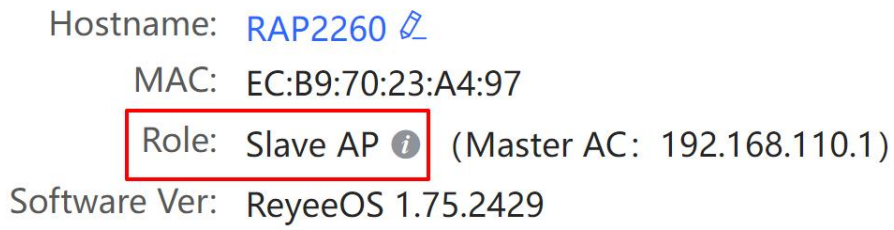
There are three types of working modes：

Router mode：NAT forwarding. **The AP in the Router mode contains networking, network setup and some radio features.**

AP mode：Bridge forwarding.

Self-Organizing：**If it is enabled, the device role will be displayed. If it is disabled, the device works in standalone mode.**

7.4.4 View SON Status



Role

Master AP/AC: The device can manage downlink devices.

Slave AP/Device: The device has been managed by an AC.

Unknown: The device failed to join a Self-Organizing Network and works as a generic AP.

Standalone: The device has not joined a Self-Organizing Network.

> Note
>
> If the role is incorrect, please press F5 to refresh the page.

What is the priority of SON networking?

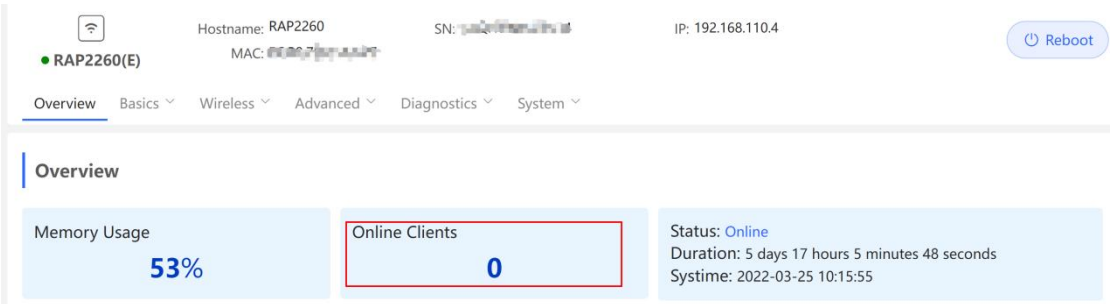
a) EG（AC mode）＞EG（router mode）＞AP（router mode）＞AP（AP mode）＞SW.

b) Device CPU / Memory / others (AP radio number). Priority: The larger the parameter, the higher the priority.

c) Same model：Priority: The larger the parameter of MAC address, the higher the priority.

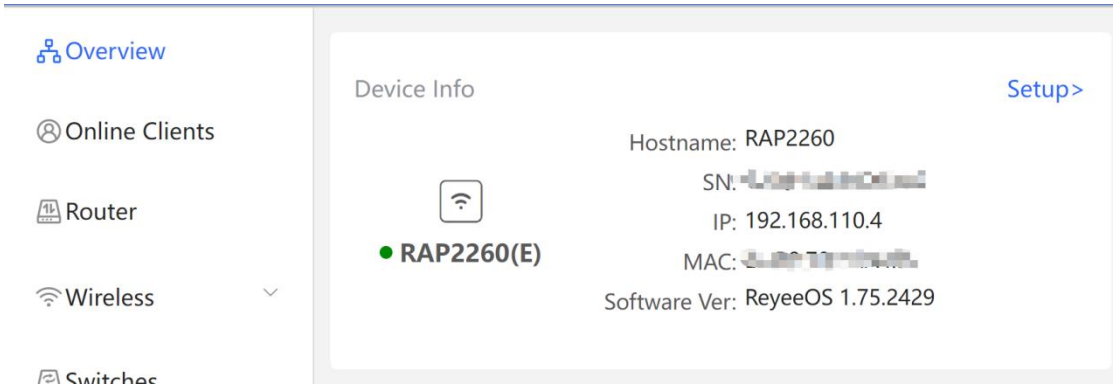
> Note
>
> Ruijie EG3230/3250 and Reyee ES switches cannot act as Masters.

7.4.5 Online Clients



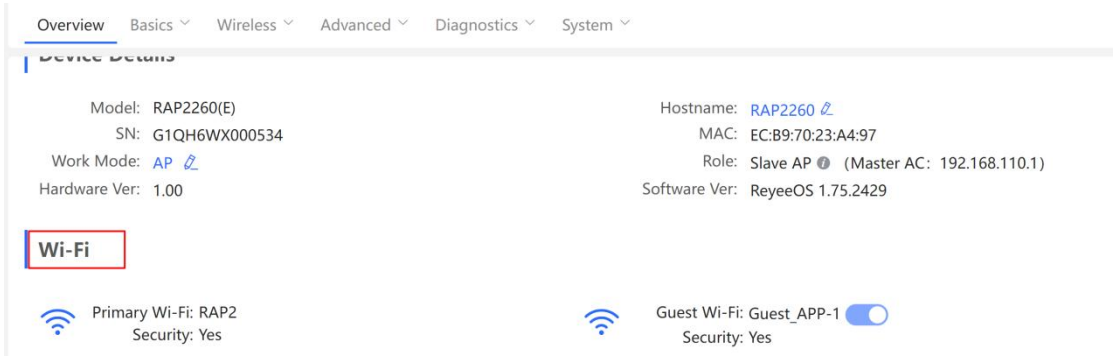
7.4.6 Device Info

Log in to the Eweb interface of the device and click **Overview** to check the device information.



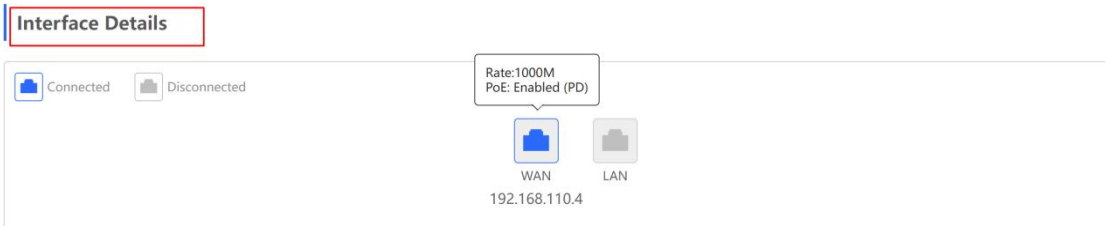
7.4.7 Wireless Info

Log in to the Eweb interface of the device and click **Wireless —> Aps —> Manage** to check the wireless information.



7.4.8 Interface Details

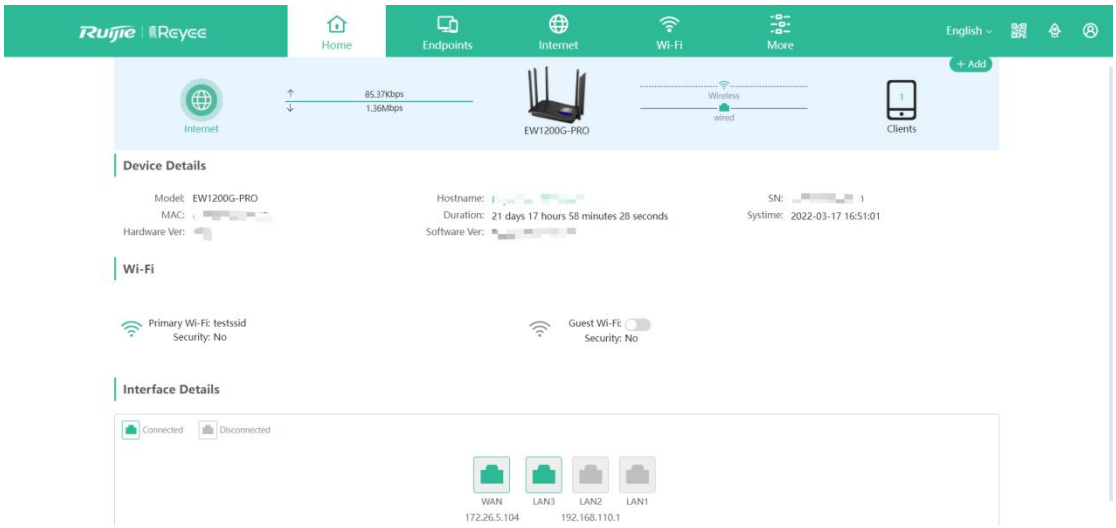
Log in to the Eweb interface of the device and click **Wireless—>Aps—>Manage** to check the interface details.



7.5 Reyee Mesh Wi-Fi Router Monitor

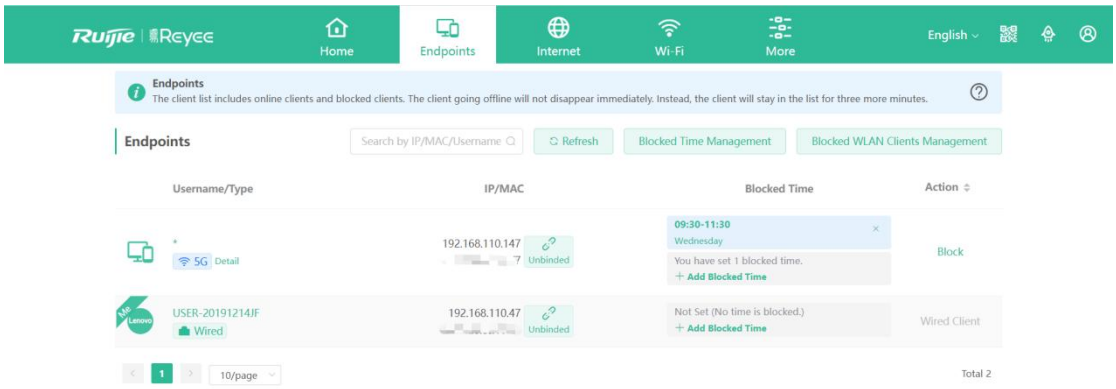
7.5.1 Overview

The overview page displays the local connection situation and information of **Device Details**, **Wi-Fi** and **Interface Details**. The information of download speed, upload speed, local device and connected clients is displayed on the top of this page. The **Device Details** includes the model, Host name, SN, MAC, etc. The **Interface Details** displays the connection of WAN and LAN.

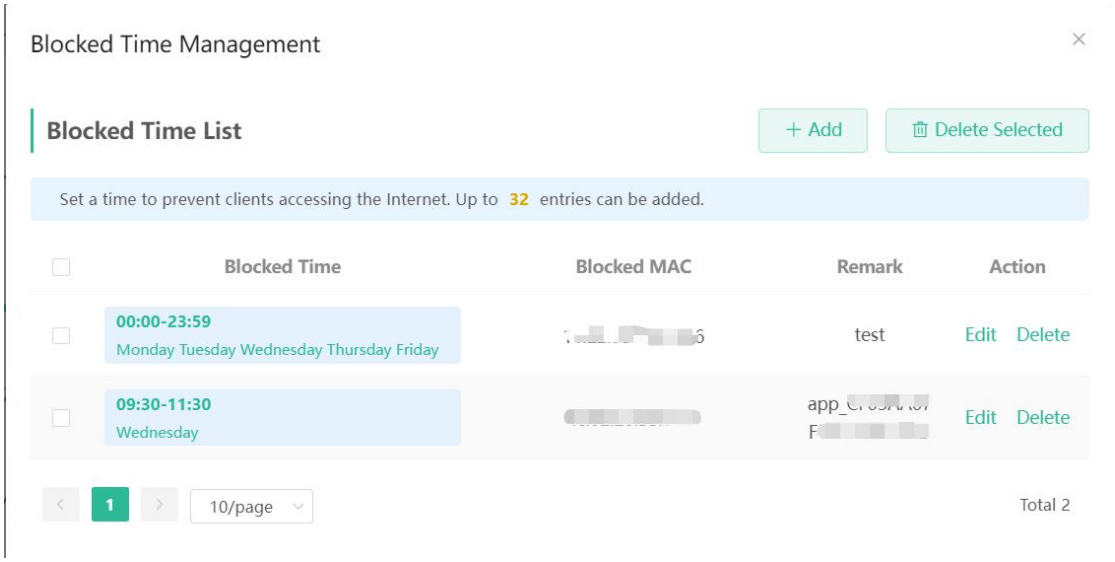


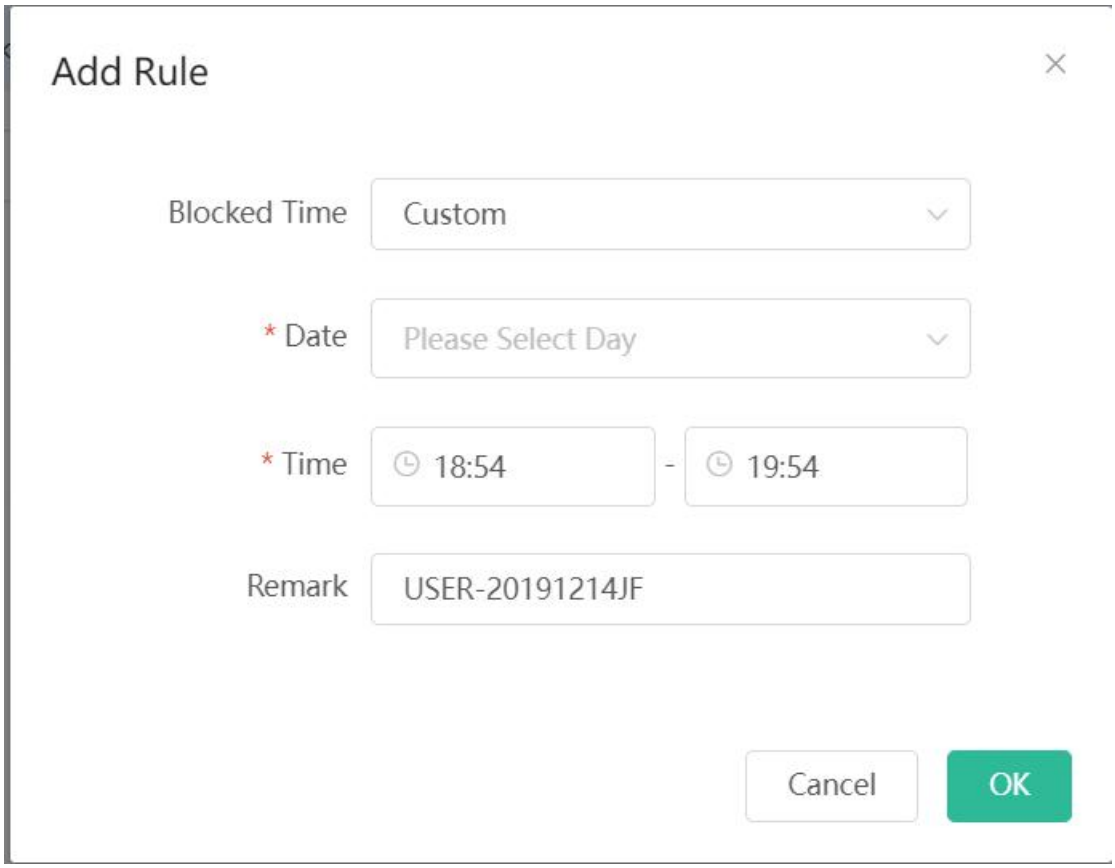
7.5.2 Endpoints

This page displays all connected endpoints in this network, including wired users and wireless users. The Clients module allows you to bind the static IP, manage blocked time and block WLAN clients.

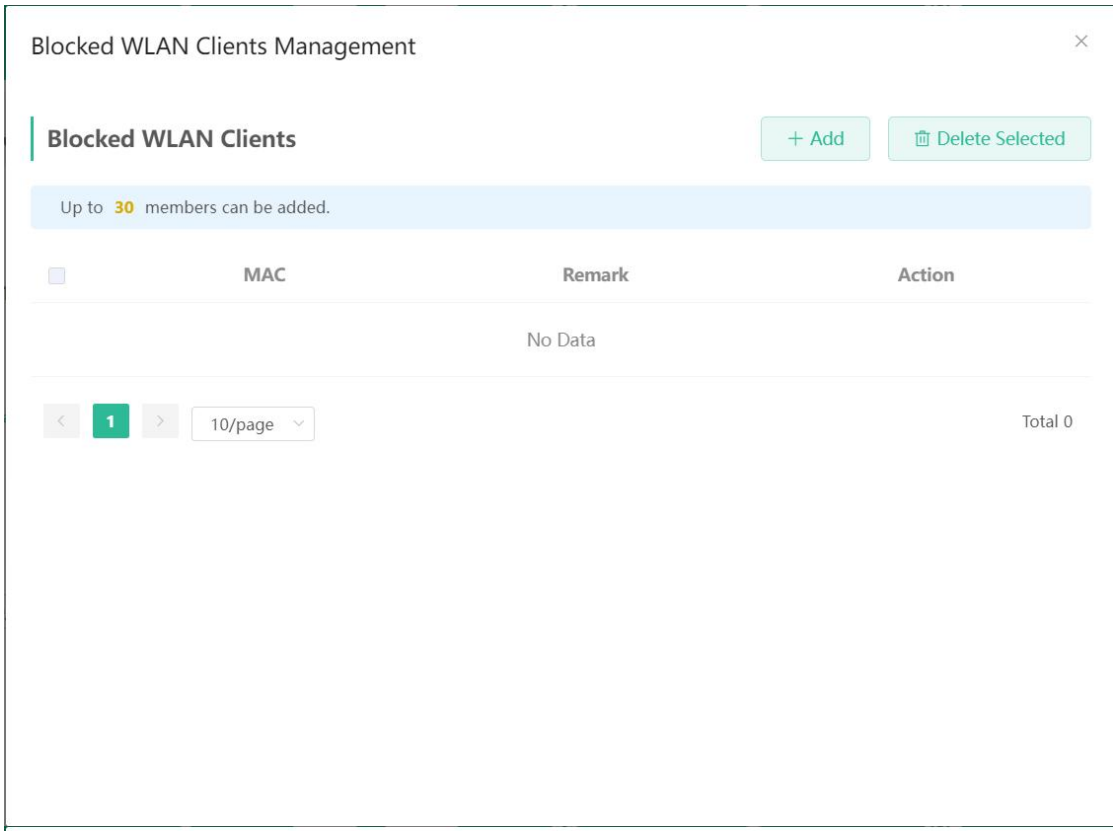


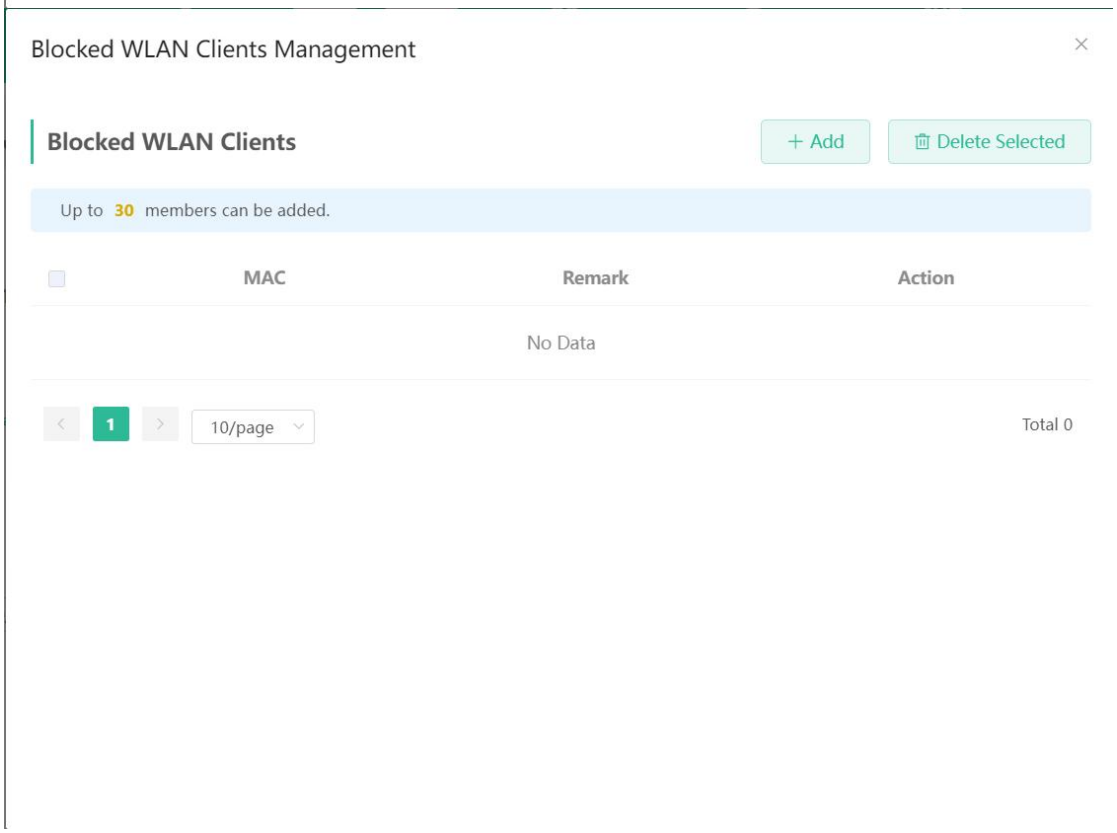
Click **Blocked Time Management** to customize the time to block users





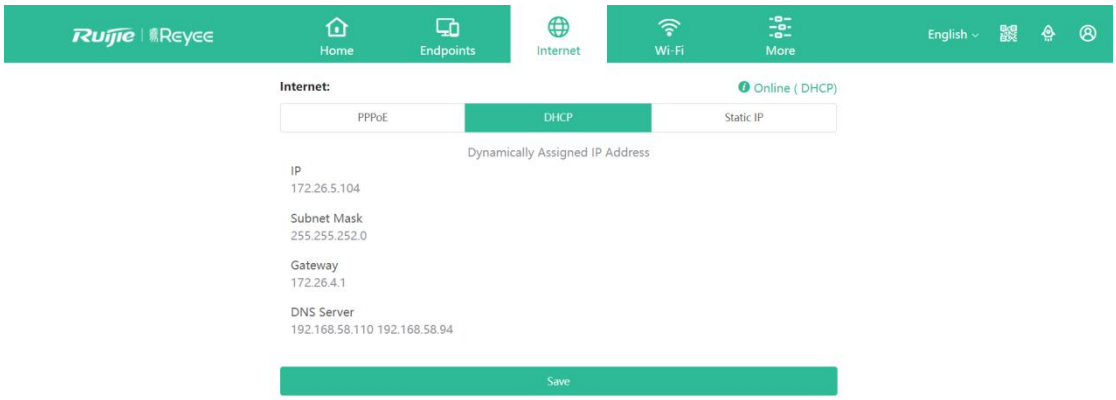
Click **Blocked WLAN Clients Management** and add the Mac address to prevent WLAN users from connecting the SSID.





7.5.3 Internet

This page displays the ways which device access the internet, including PPPoE, DHCP and Static IP.



DHCP: The router detects whether the IP address can be abtained via DHCP by default. If the router connects to the Internet successfully, you can click **Next** without entering an account.

PPPoE: Click **PPPoE**, and enter the username, password, and service name. Click **Next**.

Static IP: Enter the IP address, subnet mask, gateway, and DNS server, and click **Next**.

7.6 Reyee Wireless Bridge Monitor

7.6.1 Overview

VCR and Camera

There are a pair of devices of EST bridges which can be paired automatically with each other after power-on. You can also manually pair the devices by setting up a WDS network.

In a paired WDS group, bridges can work in access point (AP) or Customer Premises Equipment (CPE) mode

VCR end (AP): A bridge sending bridging signals is generally connected to the VCR end in the surveillance room. A WDS group can contain at most one AP can be contained at most in a WDS Group.

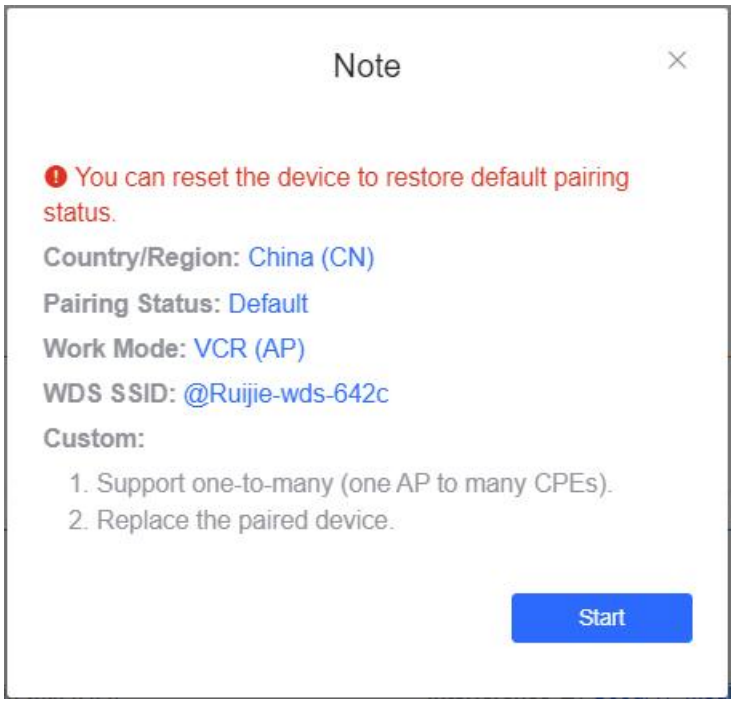
Camera end (CPE): A bridge that enables customers to access ISP's communication services is generally connected to the camera end. A WDS group can contain multiple CPEs.

a) Switching VCR and Camera Mode

If a VCR fails, you replace it and switch the new device to NVR (AP). If multiple cameras (CPE) are required, a device newly joining the WDS group needs switch it to the Camera (CPE).

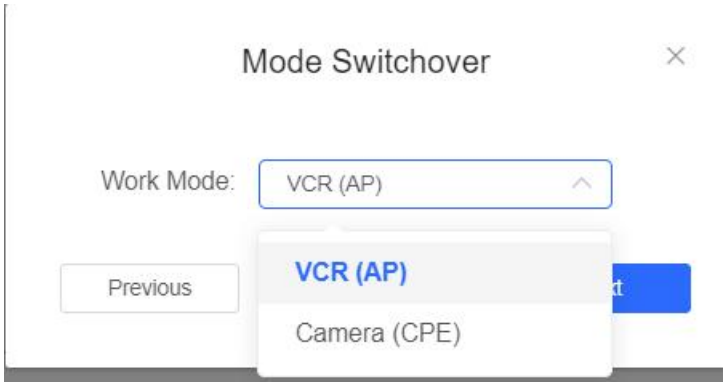
(1) You can check the current mode in the upper right corner of the Web page and click Pair Again to switch the mode.

(2) In the displayed dialog box, it shows the current pairing information, including Country/Region, Pairing Status, **Work Mode** and **WDS SSID**, click **Start** to enter the next step.



(3) Select your Country/Region and click **Next.**

(4) Change the work mode to **VCR(AP)** or **Camera(CPE).**



After you changed the work mode, the device will reboot, then you can see its mode has been changed after device reboot. Therefore, exercise caution when performing this operation.

Alarm

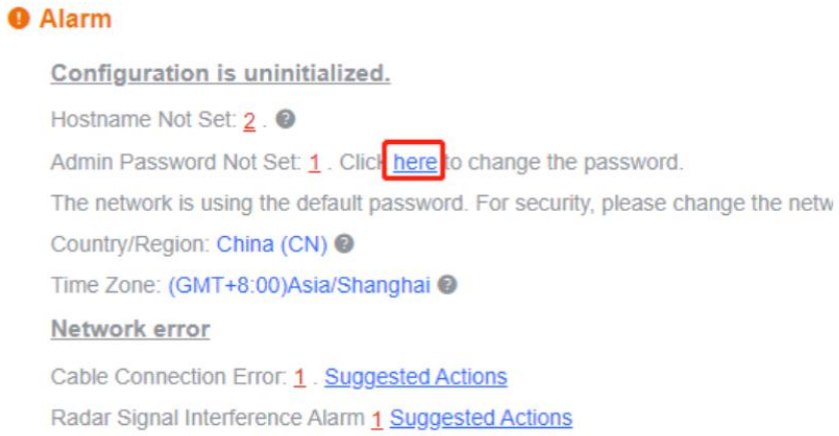
When bridges fail or lack some necessary security configuration, the system prompts key alarms about the bridges on the homepage, so that users can handle the exceptions promptly.

a) Device Name Is Not Modified

Modifying device names can help you better distinguish each bridge. It is recommended to modify the default device name under the normal situation.

b) Default Admin Password Is Still Used

For the device and network security, you are advised to configure the admin password for the network to prevent the login of unauthorized users. Click here to configure the admin password for the network.



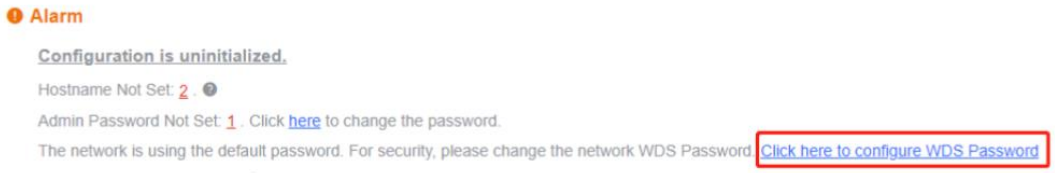
Note

The admin password is used to log in to the web page of any device in the network. Therefore, please keep your admin password in mind. If you forget the admin password, you also can restore factory settings.

If there is an unbridged device in the network, the function of configuring the admin password will be disabled.

c) Default WDS Password Is Still Used by All Devices

The default WDS passwords of devices of the same model is the same. Changing the WDS password can prevent others from illegally accessing the network by using a device of the same model. Click Click here to configure WDS Password, enter the new password, and click Save to change the WDS password for the entire network.

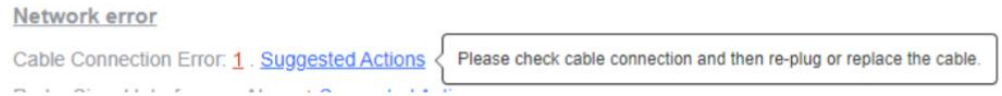


Note:

> Note
>
> When configuring the WDS password for the entire network, ensure that all devices are online. Otherwise, WDS passwords of the devices will be inconsistent.
>
> Configuring the WDS password for the entire network will reconnect all devices in the network. Therefore, exercise caution when performing this operation.
>
> If there is an unbridged device in the network, the function of configuring the WDS password for the entire network will be disabled.

d) Network Cable Is Disconnected or Incorrectly Connected

Hover the cursor over the orange number of the prompt to display the alarm details. Click the suggested action to check the solution.



e) Latency Is High or Bandwidth Is Insufficient

First, check whether the device latency is too high. If yes, the interference in the environment may be severe. Then, you are advised to change the channel with a smaller interference. If not, increase the channel width.

To check whether the latency is too high, perform as follows: Hover the cursor over the orange number of the prompt to display all WDS groups, and click a group to display the details. On the **Overview** page, check whether **Latency** is **Freeze**. If so, the latency is too high. Otherwise, the latency is normal.

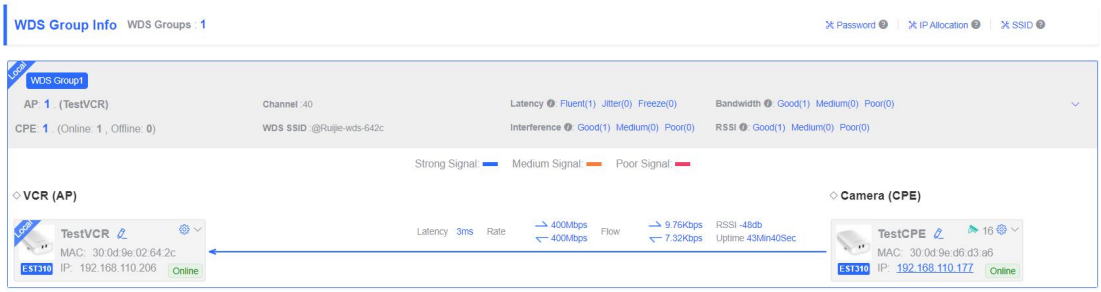
In CPE mode, the local channel and channel width are consistent with the peer channel and channel width. You are only allowed to configure the transmit power and distance.

7.6.2 WDS Group Info

Choose **Overview >WDS Group Info**. Displayed WDS group information includes the number of APs and CPEs in the group, current working channel, SSID, latency, interference, wireless bandwidth and quality, RSSI and quality, data rate, real-time traffic, and uptime. Hover the cursor over to view the detailed information of every item.

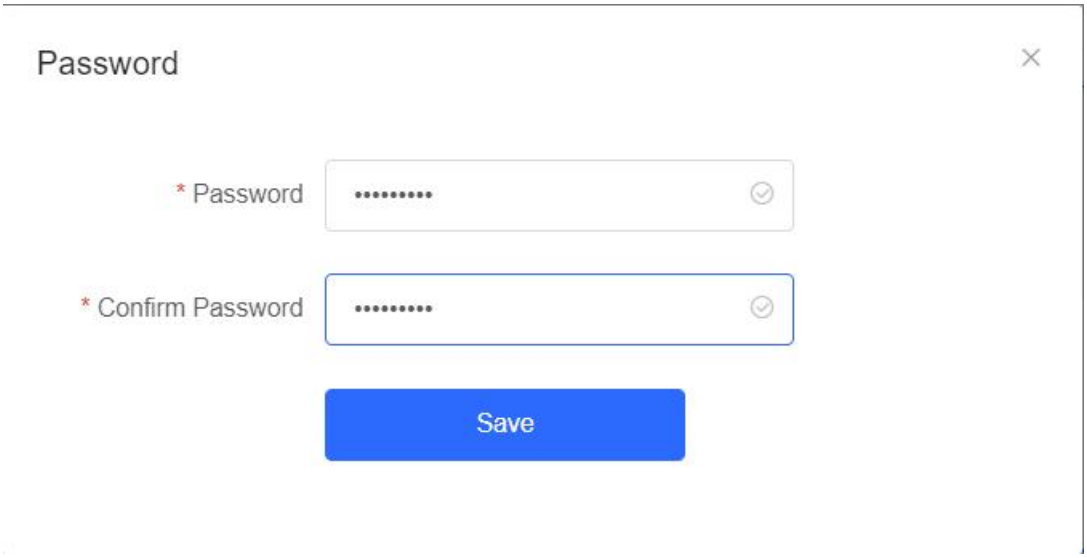
Note:

AP is at the NVR end, while CPE is at the camera end.



1.1 Password

The login password configured here applied to all EST devices in the network.

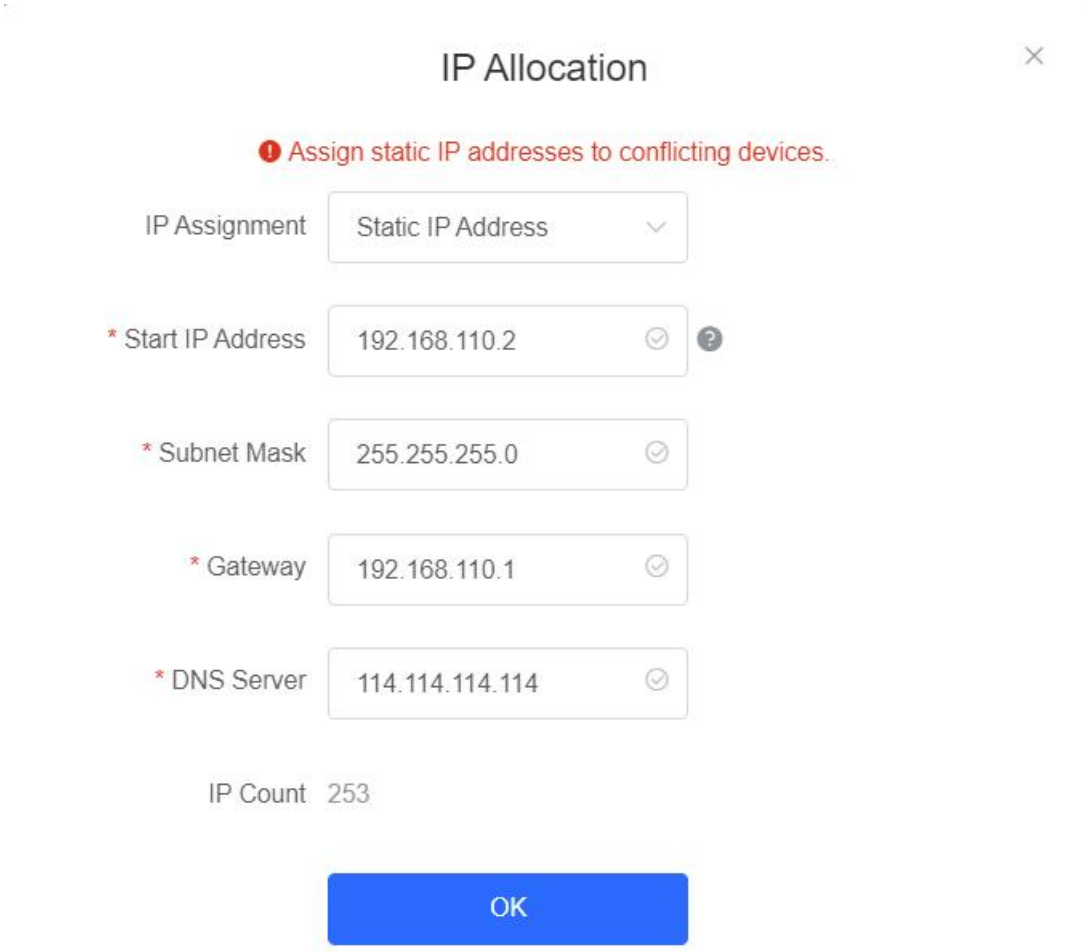


Note

When configuring the WDS password for the entire network, ensure that all devices in the network are online. Otherwise, the WDS passwords of the devices will be inconsistent. Configuring the WDS password for the entire network will reconnect all devices in the network. Therefore, exercise caution when performing this operation. If there is an unbridged device in the network, the WDS password cannot be configured.

1.2 IP Allocation

When a large number of devices in the network require static IP addresses, you can use **IP Allocation** to automatically allocate a static IP address for each device. Click **IP Allocation**, set **Internet** to **Static IP Address**, set **Start IP Address**, **Subnet Mask**, **Gateway**, and **DNS Server**, and click **OK.**



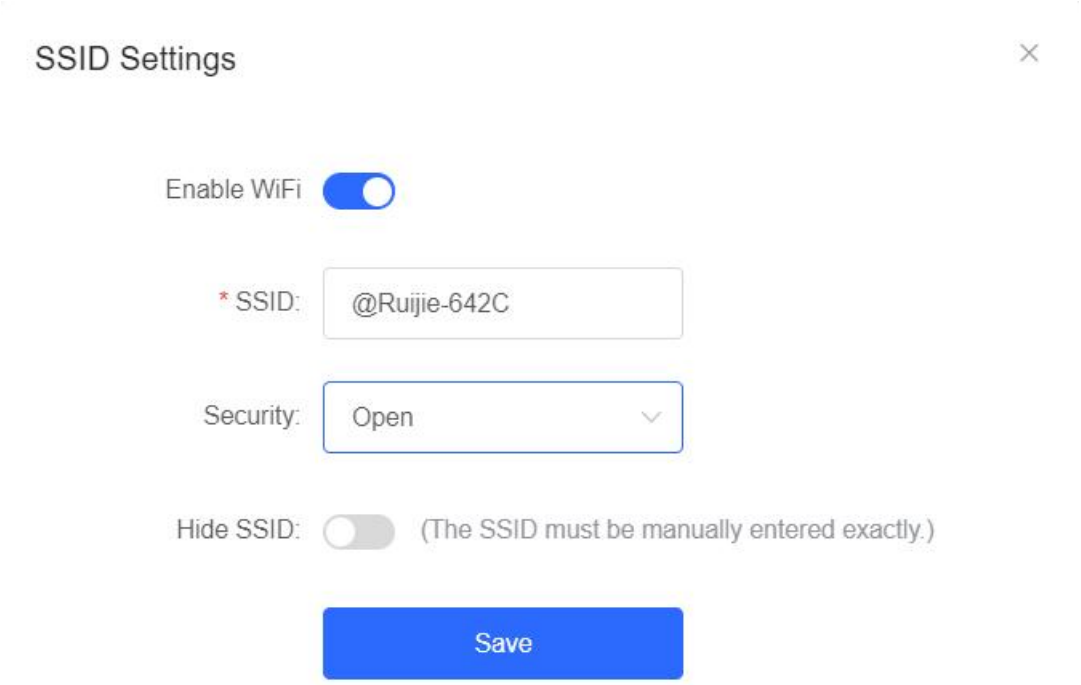
Note

The Start IP Address cannot be in the same network segment as the current IP address. Otherwise, the configuration will fail. After the configuration, the device IP address will change, and the device web page cannot be accessed. You need to enter the new IP address in the browser address bar and ensure that the IP addresses of the management computer and the device are in the same network segment. If they are not in the same network segment, reconfigure the IP address of the management computer.

When a large number of devices in the network require dynamic IP addresses, you can configure dynamic IP addresses (DHCP) for the entire network so that each device can dynamically obtain an IP address. Set Internet to DHCP, and click OK.

1.3 SSID

It indicates configure an SSID for all EST devices in the network. The SSID is disabled by default and users cannot manage devices by accessing WiFi.



The default device management service set identifier (SSID) is @Ruijie-bXXXX. (XXXX is the last four digits of the MAC address of each device, and the default management SSID varies with devices.) Click SSID on the page to set the same management SSID and password for all bridges in the LAN.

Enable WiFi: Choose whether to enable the management Wi-Fi for all devices in the network.

SSID: The SSID is the name of the management Wi-Fi network.

Security: The following encryption types are available: Open, WPA-PSK, WPA2-PSK, and WPA_WPA2-PSK. You are advised to choose WPA_WPA2-PSK and set the password to strengthen the security.

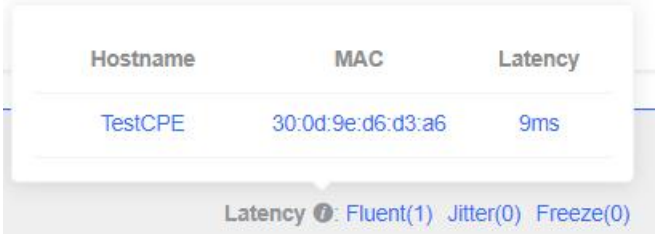
Hide SSID: When this function is enabled, mobile phones or computers cannot find the Wi-Fi name, and users need to manually enter the correct name and password. This can prevent Wi-Fi from being accessed by unauthorized users and can strengthen the security.

AP: it indicates the number of EST with VCR mode in this group, there can only be one EST as AP in group.

CPE: it indicates the number of ESTs with CPE mode in this group. EST310 supports one to five bridging. EST350 supports to one to three bridging.

Channel: it displays the channel for WDS SSID which only supports 5G channel.

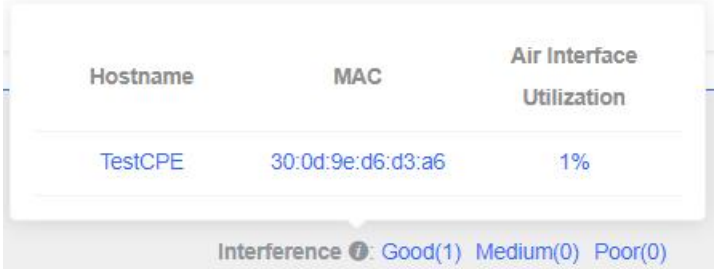
Latency: it displays the stability of bridges in this group, including Fluent, Jitter and Freeze. You can click the icon to see the exact latency number of all CPEs.



Bandwidth: it displays the transmission rate of all bridges in this group, including Good, Medium and Poor. You can click the icon to see the exact bandwidth number of all CPEs.

WDS SSID: it displays the name of WDS SSID.

Interference: it indicates the interference status of all bridges in this group, including Good, Medium and Poor. You can click the icon to see the exact air interface utilization of all CPEs.



RSSI: it displays the connected signal of all bridges in this group, including Good, Medium and Poor. You can click the button to see the exact RSSI of all CPEs.

1.4 Displaying the Information about a Single Device

Choose **Overview> WDS Group Info> NVR (AP)/Camera (CPE)**

Click the icon of a device to display the basic information about the device in the right panel of the page, including the hostname, uptime, online status, model, SN, MAC address, software and hardware versions, IP address, subnet mask, LAN port status, noise floor/utilization, distance, channel, transmit power, channel width, RSSI, and band.