Ruijie Reyee Series Access Point

Implementation Cookbook

Document Version: V1.2

Date: 2023-02-20

Copyright

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

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

Preface I

1 Product Introduction 1

1.1 Product List 1

1.2 LED Indicator 3

1.2.1 Reyee Indoor AP 3

1.2.2 Reyee Wall AP 4

1.2.3 Reyee Outdoor AP 5

1.3 Button 8

2 Getting Started 9

2.1 Network Planning 9

2.2 Installation 10

2.2.1 Safety Suggestions 10

2.2.2 Installation Site Requirement 11

2.2.3 Installing the AP 12

2.3 Quick Provisioning 13

2.3.1 Quick Provisioning Through Ruijie Cloud App 13

2.3.2 Quick Provisioning Through Reyee Eweb 26

3 Device Management 30

3.1 Login 30

3.1.1 Case Demonstration 30

3.2 Setting the Login Password 31

3.3 Performing Upgrade and Checking the System Version 32

3.3.1 Online Upgrade 32

3.3.2 Local Upgrade 32

3.4 Configuring Backup and Import 33

3.5 Restoring Factory Settings 33

4 Configuration 35

4.1 Wireless Configuration 35

4.1.1 Wireless Basic Configuration 35

4.1.2 Guest Wi-Fi Configuration 36

4.1.3 Multiple SSID Configuration 38

4.1.4 Healthy Mode 39

4.1.5 Wireless Client List 40

4.1.6 Radio Frequency Configuration 40

4.1.7 Wireless Blacklist/Whitelist Configuration 44

4.1.8 AP Group Configuration 46

4.2 Basic Configuration 48

4.2.1 WAN Port Configuration 48

4.2.2 LAN Port Configuration 50

4.3 Advanced Configuration 54

4.3.1 ARP List 54

4.3.2 Local DNS 55

4.3.3 PoE Configuration 55

4.3.4 Port Flow Control Configuration 56

4.4 Operation and Maintenance ... 56
4.4.1 Network Check ... 56
4.4.2 Alarms ... 58
4.4.3 Network Tools ... 59
4.4.4 Fault Collection ... 60
4.4.5 System ... 61
5 Advanced Solution Guide ... 67
5.1 Reyee Flow Control Solution ... 67
5.1.1 Application Scenario ... 67
5.1.2 Configuration Case ... 67
5.2 Reyee Cloud Authentication Solution ... 74
5.2.1 Working Principle ... 74
5.2.2 Application Scenario ... 74
5.2.3 Configuration Case ... 74
5.3 Reyee Guest Wi-Fi Solution ... 82
5.3.1 Working Principle ... 82
5.3.2 Application Scenario ... 82
5.3.3 Configuration Case ... 82
5.4 Reyee SON ... 96
5.4.1 Working Mechanism of Reyee SON ... 96
5.4.2 Reyee SON Configuration ... 99
5.4.3 SON Troubleshooting ... 100
5.5 Reyee Economic Hotel Network Solution ... 101
5.5.1 Application Scenario ... 101
5.5.2 Configuration Case ... 101
6 Reyee FAQ ... 110
6.1 Reyee Password FAQ (Collection) ... 110
6.2 Reyee Guest WiFi FAQ (Collection) ... 110
6.3 Reyee Wireless Configuration FAQ (Collection) ... 110
6.4 Reyee Self-Organizing Network (SON) FAQ (Collection) ... 110
6.5 Reyee series Devices Parameters Tables ... 110
6.6 Reyee Parameter Consultation FAQ (Collection) ... 110
7 Appendix: Monitoring ... 111
7.1 Memory Usage ... 111
7.2 Device Status ... 111
7.3 AP Working Mode ... 111
7.4 Checking the SON Status ... 113
7.5 Online Clients ... 113
7.6 Device Information ... 114
7.7 Wireless Information ... 114
7.8 Ethernet Status ... 114

1 Product Introduction

Reyee cloud-managed access points (APs) have high performance for indoor, outdoor, and wall scenarios. In conformance with 802.11ac Wave 2, Reyee cloud-managed series APs support Multi-user Multiple Input, Multiple Output (MU-MIMO) dual-stream technology.

Reyee APs are easy to install and maintain with the industrial design.

Good Performance Based on Dual-band Wi-Fi

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

Seamless Layer 3 Roaming

The AP supports Layer 3 roaming on a complex Layer 3 network. When users move across Layer 3 networks, seamless roaming can be achieved without service interruption.

SON Support

Self-Organizing Networking (SON) eliminates 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. The mobile app allows you to quickly complete device deployment and configuration, remote management, operation and maintenance (O&M) of the entire network, which greatly reduces the investment of device, labor, and time cost during wireless network construction.

1.1 Product List

Model	Coverage	Recommend Number of Clients	WLAN ID	SON Number	Spatial Streams
RG-RAP1200(F)	20 meters	40 = 8 (2.4 GHz) + 32 (5 GHz)	8	150	2.4 GHz 2x2 MIMO 5 GHz 2x2 MIMO
RG-RAP1200(P)	20 meters	80 = 16 (2.4 GHz) + 64 (5 GHz)	8	150	2.4 GHz 2x2 MIMO 5 GHz 2x2 MIMO
RG-RAP2200(F)	30 meters	48 = 16 (2.4 GHz) + 32 (5 GHz)	8	150	2.4 GHz 2x2 MIMO 5 GHz 2x2 MIMO
RG-RAP2200(E)	30 meters	80 = 16 (2.4 GHz) + 64 (5 GHz)	8	300	2.4 GHz 2x2 MIMO 5 GHz 2x2 MIMO
RG-RAP2260(G)	30 meters	100 = 16 (2.4 GHz) + 84 (5 GHz)	8	300	2.4 GHz 2x2 MIMO 5 GHz 2x2 MIMO

Model	Coverage	Recommend Number of Clients	WLAN ID	SON Number	Spatial Streams
RG-RAP2260(E)	30 meters	120 = 16 (2.4 GHz) + 104 (5 GHz)	8	300	2.4 GHz 4x4 MIMO 5 GHz 4x4 MIMO
RG-EAP602	2.4 GHz 100 meters 5 GHz 300 meters	96 = 32 (2.4 GHz) + 64 (5 GHz)	8	150	2.4 GHz 2x2 MIMO 5 GHz 2x2 MIMO
RG-RAP6260(G)	100 meters	100 = 16 (2.4 GHz) + 84 (5 GHz)	8	300	2.4 GHz 2x2 MIMO 5G GHz 2x2 MIMO
RG-RAP6262G	2.4 GHz 100 meters 5 GHz 300 meters	100 = 16 (2.4 GHz) + 84 (5 GHz)	8	300	2.4 GHz 2x2 MIMO 5 GHz 2x2 MIMO
RG-RAP6202G	2.4 GHz 100 meters 5 GHz 300 meters	96 = 32 (2.4 GHz) + 64 (5 GHz)	8	300	2.4 GHz 2x2 MIMO 5 GHz 2x2 MIMO
RG-RAP2260	150meters	110 = 16 (2.4 GHz) + 94 (5 GHz)	8	300	2.4 GHz 2x2MIMO 5 GHz 2x2MIMO
RG-RAP6262	2.4 GHz 100 meters 5 GHz 300 meters	80 = 16 (2.4 GHz) + 64 (5 GHz)	8	300	2.4 GHz 2x2MIMO 5 GHz 2x2MIMO
RG-RAP2260(H)	150 meters	130 = 16 (2.4 GHz) + 114 (5 GHz)	8	300	2.4 GHz 4x4 MIMO 5 GHz 4x4 MIMO
RG-	2.4 GHz	120 = 16 (2.4 GHz) + 104 (5	8	300	2.4 GHz 4x4 MIMO

Model	Coverage	Recommend Number of Clients	WLAN ID	SON Number	Spatial Streams
RAP6260(H)	100 meters 5 GHz 300 meters	GHz)			5 GHz 4x4 MIMO

⚠ Note

The above coverage data is based on ideal conditions with straight distance and no obstacles. The real coverage distance is subject to the real environment.

1.2 LED Indicator

1.2.1 Reyee Indoor AP

Reyee indoor APs include RG-RAP2200(E), RG-RAP2200(F), RG-RAP2260(E), RG-RAP2260(G), RG-RAP2260, and RG-RAP2260(H).

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	0.5 Hz	The AP is functioning properly but an alarm is generated.
	Fast blinking	10 Hz	Possible cases: ● Restoring factory settings ● Upgrading the firmware ● Restoring the image file ● Initializing the device
	Solid green	N/A	The AP is functioning properly with no alarms.

RG-RAP2260

LED Indicator	Status	Description
LED Indicator	Solid blue	The AP is functioning properly with no alarms.
	Off	The AP is not receiving power.
	Fast flashing	The AP is starting up.
	Slow flashing (at 0.5 Hz)	The network is unreachable.
	Flashing twice in succession	Possible cases: ● The AP is restoring the factory settings. ● The AP is upgrading the software. ⚠ Caution Do not power off the device in this case.
	One long flash followed by three short flashes.	Other faults occur.

RG-RAP2260(H)

LED Indicator	Status	Description
LED Indicator	Off	The AP is not receiving power.
	Slow Blinking	The AP is functioning properly but an alarm is generated.
	Fast blinking	Possible cases: ● Restoring the access point to factory settings. ● Upgrading the firmware. ● Handling alarms automatically. ● Starting up the access point.
	Solid blue	The AP is functioning properly with no alarms.

1.2.2 Reyee Wall AP

Reyee wall APs include RG-RAP1200(F) and RG-RAP1200(P).

LED Indicator	State	Frequency	Meaning
LED indicator	Off	N/A	The AP is powered off.
	Slow blinking	0.5 Hz	The AP is functioning properly but an alarm is generated.
	Fast blinking	10 Hz	Possible cases: ● Restoring factory settings ● Upgrading the firmware ● Self-repairing ● Initializing the AP ● The PoE OUT port is overloaded.
	Solid green	NA	The AP is functioning properly with no alarms.

1.2.3 Reyee Outdoor AP

Reyee outdoor APs include RG-EAP602, RG-RAP6260(G), RG-RAP6262(G), RG-RAP6202(G), RG-RAP6262, and RG-RAP6260(H).

RG-EAP602/RG-RAP6260(G)

LED Indicator	State	Frequency	Meaning
LED indicator	Off	N/A	The AP is not receiving power.
	Slow blinking	0.5 Hz	The AP is normal but is not connected to Ruijie Cloud.
	Fast blinking	10 Hz	Possible cases: ● Restoring factory settings ● Upgrading the firmware Restoring the image file ● Initializing the device
	Solid Blue	On	The AP is functioning properly with no alarms.

RG-RAP6262(G)/RG-RAP6202(G)

LED Indicator	State	Meaning
Wi-Fi (green)	Blinking	Data is transmitted by Wi-Fi.

LED Indicator	State	Meaning
	Solid on	Wi-Fi is enabled and no data is transmitted.
	Off	Wi-Fi is disabled.
SYS (blue)	Fast blinking	The AP is being initialized.
	Slow blinking (0.5 Hz)	The Internet is unreachable.
	Blinking twice	1. Restore factory settings. 2. Upgrade the firmware and restore the image file. **Caution** Do not power off the device in this case.
	A long blink and three short blinks	Other faults occur.
	Solid on	The AP is working properly with no alarm.
	Off	The AP is powered off.
LAN 1 (green)	Blinking	The port is Up and data is transmitted.
	Solid on	The port is Up and no data is transmitted.
	Off	The port is Down.
LAN 2 (green)	Blinking	The port is Up and data is transmitted.
	Solid on	The port is Up and no data is transmitted.
	Off	The port is Down.

RG-RAP6262

LED Indicator	State	Meaning
Wi-Fi LED (Green)	Flashing	Data is transmitted by Wi-Fi.
	Solid on	Wi-Fi is enabled and no data is transmitted.
	Off	Wi-Fi is disabled.
System Status LED (Blue)	Fast flashing	The access point is starting up.
	Slow flashing (at 0.5 Hz)	The network is unreachable.
	Flashing twice in succession	Possible cases: ● Restoring the access point to factory settings. ● Upgrading the firmware. ● Handling alarms automatically. Note: Do not power off the access point in this case.
	Solid on	The access point is functioning properly.
	Off	The access point is not receiving power.
LAN Port Status LED (Green)	Flashing	The port has made a successful link and is sending/receiving traffic.
	Solid on	The port has made a successful link and is not sending/receiving traffic.
	Off	No link is detected for the port.
SFP Port Status LED (Green)	Flashing	The port has made a successful link and is sending/receiving traffic.
	Solid on	The port has made a successful link and is not sending/receiving traffic.
	Off	No link is detected for the port.

RG-RAP6260(H)

LED Indicator	State	Meaning
LED Indicator	Off	The access point is not receiving power.
	Slow Blinking	The access point is operating normally but there is an alarm generated.

LED Indicator	State	Meaning
	Fast Blinking	Possible cases: ● Restoring the access point to factory settings. ● Upgrading the firmware. ● Handling alarms automatically. ● Starting up the access point.
	Solid Blue	The access point is operating normally with no alarms.

1.3 Button

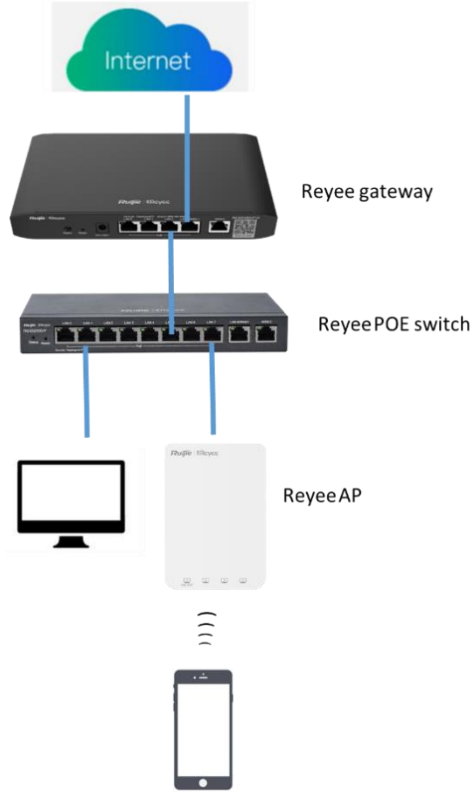
Model	Button		Meaning
All AP	Reset	Pressing this button for less than 2 seconds	Restart the AP.
		Pressing this button for more than 5 seconds	Restore factory defaults.

2 Getting Started

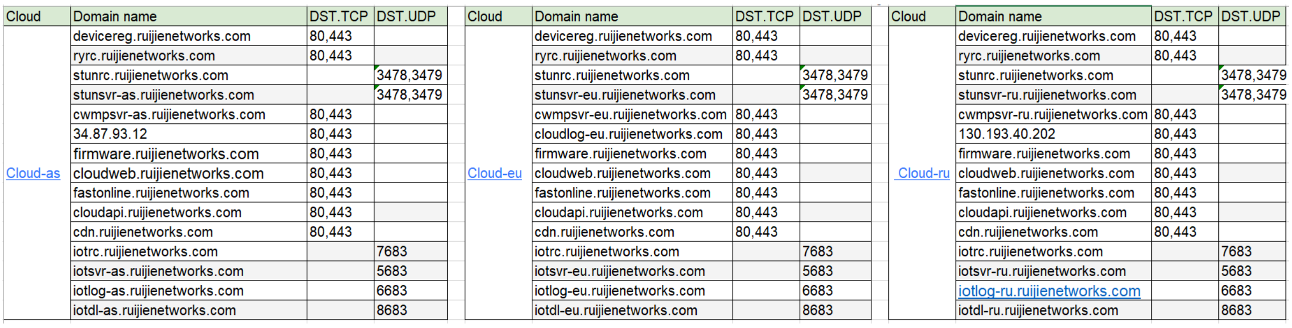
2.1 Network Planning

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

- 192.168.110.0/24 in VLAN 1 for devices on this network
- 192.168.10.0/24 in VLAN 10 for clients on this network



The following ports are used for Ruijie Cloud management. To connect devices on Ruijie Cloud, ensure that these ports are available and data streams are permitted on the 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

2.2 Installation

2.2.1 Safety Suggestions

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

Installation

- Keep the chassis clean and free from any dust.
- Do not place devices in a walking area.
- Do not wear loose clothes or accessories that may be hooked or caught by devices during installation and maintenance.

Movement

- Do not frequently move devices.
- When moving devices, keep the balance and avoid hurting legs and feet or straining the back.
- Before moving devices, turn off all power supplies and dismantle all power modules.

Electricity

- Observe local regulations and specifications when performing electric operations. The operators must be qualified.
- Before installing the device, carefully check any potential danger in the surroundings, such as ungrounded power supply, and damp or wet ground or floor.
- 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.
- Try to avoid maintaining the switch that is powered on alone.
- Make a careful check before you cut off the power supply.
- Do not place the equipment in a damp location. Do not let any liquid enter the chassis.

Static Discharge Damage Prevention

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

- Properly ground grounding screws on the back panel of the device; use a three-wire single-phase socket with the protective earth wire (PE) as the AC power socket.
- Prevent indoor dusts.
- Ensure proper humidity conditions.

Laser

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

- When a fiber transceiver is working, ensure that the port has been connected to an optical fiber or is covered with a dust cap, to keep out dust and avoid burns.
- When the optical module is working, do not pull out the fiber cable or look directly into a transceiver. The transceiver emit laser light that can damage your eyes.

2.2.2 Installation Site Requirement

The installation site must meet the following requirement to ensure normal working and a prolonged durable life of Reyee APs.

Ventilation

When installing devices, reserve at least 10 cm distances from both sides and the back plane of the cabinet at ventilation openings to ensure good ventilation. After cables have been connected, bundle or place the cables on the cabling rack to prevent them from blocking the air inlets. It is recommended that the device be cleaned at regular intervals. In particular, avoid dust from blocking the screen mesh on the back of the cabinet.

Temperature and Humidity

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

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

- In an environment with a high humidity, insulating materials may have bad insulation or even leaking electricity. Sometimes the materials may suffer from mechanical performance change and metallic parts may get rusted.
- In an environment with a low humidity, insulating strips may dry and shrink. Static electricity may occur easily and endanger circuits on the device.
- In an environment with a high temperature, the AP is subject to more serious harm. Its performance may degrade drastically and various hardware faults may occur.

Cleanness

Dust poses a severe threat to the running of the AP. The indoor dust falling on the AP may be adsorbed by the static electricity, causing bad contact of the metallic joint. Such electrostatic adsorption may occur more easily when the relative humidity is low. This affects the lifecycle of the AP and causes communication faults.

Grounding

A good grounding system is the basis for stable and reliable operation of the device, preventing lightning strokes and resisting interference. Carefully check the grounding conditions at the installation site according to the grounding requirements, and perform grounding operations properly as required.

Lightning Grounding

The lightning protection system of a facility is an independent system that consists of the lightning rod, down conductor, and connector to the grounding system, which usually shares the power reference ground and ground cable. The lightning discharge ground is targeted for the facility.

EMC Grounding

The grounding required for EMC design includes the 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 1 Ω.

EMI

Electro-Magnetic Interference (EMI), from either outside or inside the device 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 through 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 an 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 device, but can be controlled by a filter. Radiated interference may affect any signal path in the device and is difficult to shield.

- For the TN AC power supply system, the single-phase three-core power socket with protective earthing conductors (PE) should be adopted to effectively filter out interference from the power grid through filtering circuits.
- Do not use the grounding device of the device cannot be used for an electrical device or anti-lightning grounding device. In addition, the grounding device of the device must be deployed far away from the grounding device of the electrical device and anti-lightning grounding device.
- Keep the device away from the high-power radio transmitter, radar transmitting station, and high-frequency large-current device.
- Take measures to shield static electricity.
- Lay interface cables inside the equipment room. Outdoor cabling is prohibited, avoiding damages to device signal interfaces caused by over-voltage or over-current of lightning.

2.2.3 Installing the AP

For how to install the AP, refer to the hardware installation manual of each AP.

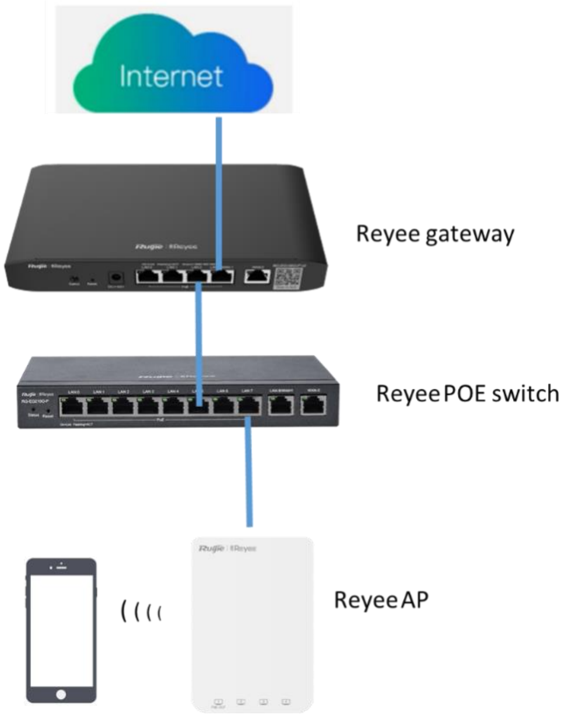
Model	**Link of Hardware Installation Manual**
RG-RAP1200(F)	https://www.ruijienetworks.com/resources/preview/76609
RG-RAP1200(P)	https://www.ruijienetworks.com/resources/preview/76610
RG-RAP2200(F)	https://www.ruijienetworks.com/resources/preview/76612
RG-RAP2200(E)	https://www.ruijienetworks.com/resources/preview/76611
RG-RAP2260(G)	https://www.ruijienetworks.com/resources/preview/76769
RG-RAP2260(E)	https://www.ruijienetworks.com/resources/preview/76806
RG-EAP602	https://www.ruijienetworks.com/resources/preview/76616
RG-RAP6260(G)	https://www.ruijienetworks.com/resources/preview/76770
RG-RAP6262G	https://www.ruijienetworks.com/resources/preview/77058
RG-RAP6202G	https://www.ruijienetworks.com/resources/preview/77243

Model	Link of Hardware Installation Manual
RG-RAP2260	https://www.ruijienetworks.com/resources/preview/77449
RG-RAP6262	https://www.ruijienetworks.com/resources/preview/77494
RG-RAP2260(H)	https://www.ruijienetworks.com/resources/preview/77409
RG-RAP6260(H)	https://www.ruijienetworks.com/resources/preview/77410

2.3 Quick Provisioning

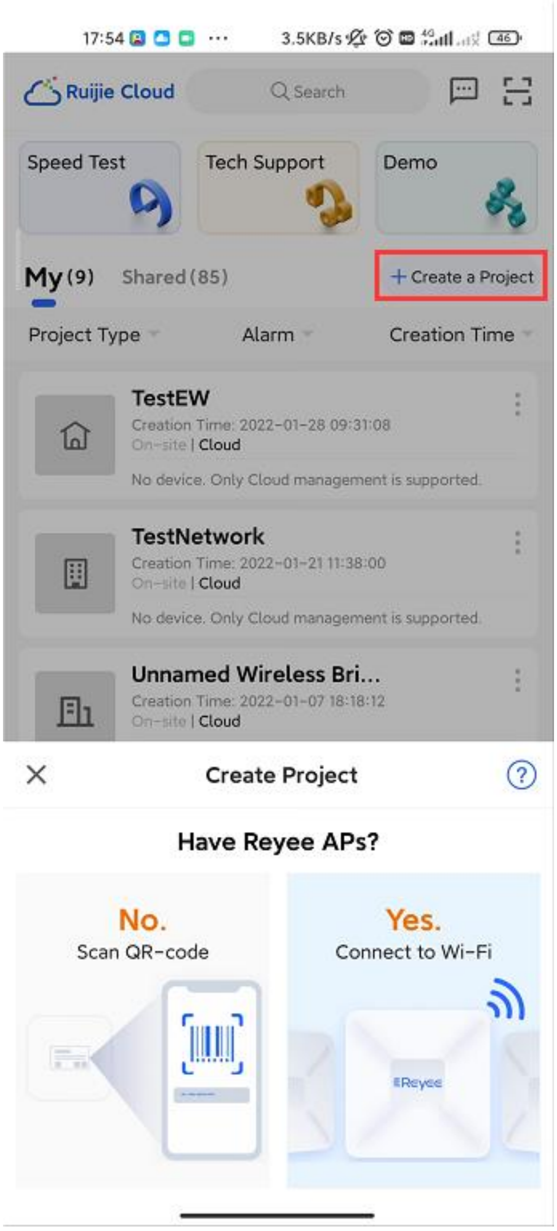
2.3.1 Quick Provisioning Through Ruijie Cloud App

The network topology shown below includes the Reyee gateway, Reyee PoE switch, and Reyee AP.



Creating a Project

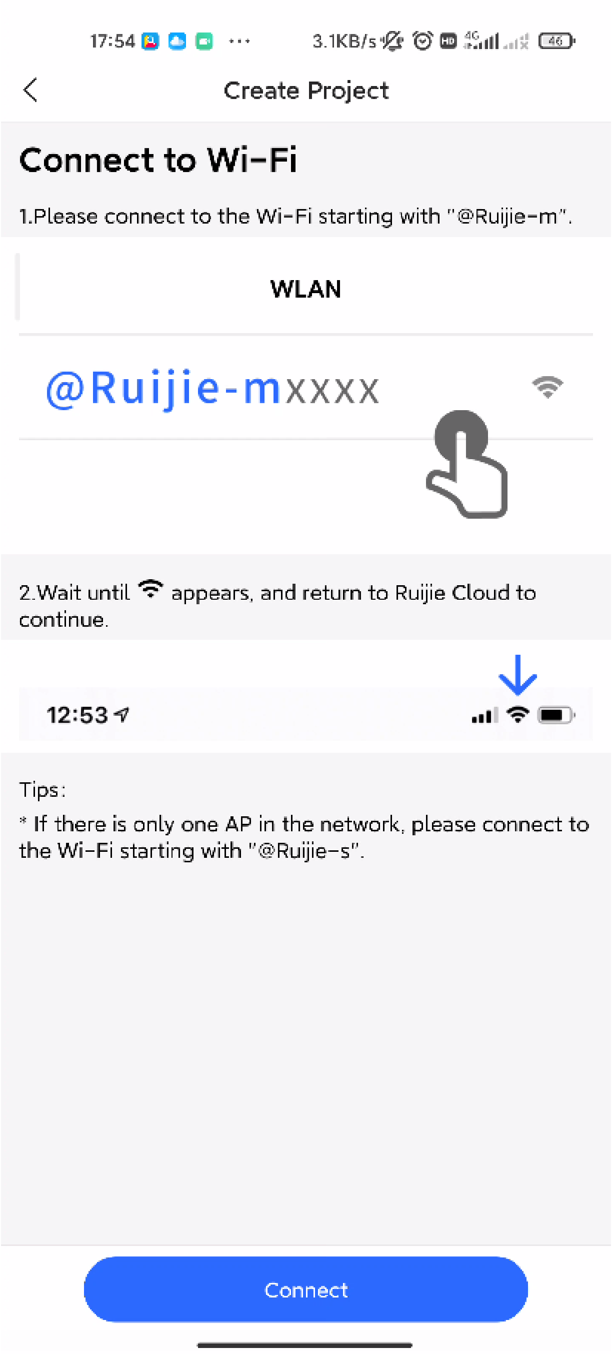
(1) Open Ruijie Cloud App, tap **Create a Project**, and select **Connect to Wi-Fi**.



Tap **Yes**. Ruijie Cloud App asks you to connect **@Ruijie-m***xxxx* SSID.

Instruction

@Ruijie-m*xxxx* is generated after the SON is established successfully. **@Ruijie-s***xxxx* is generated on a standalone device, where *xxxx* is the last four digits of MAC address of the AP.



Connect to Wi-Fi

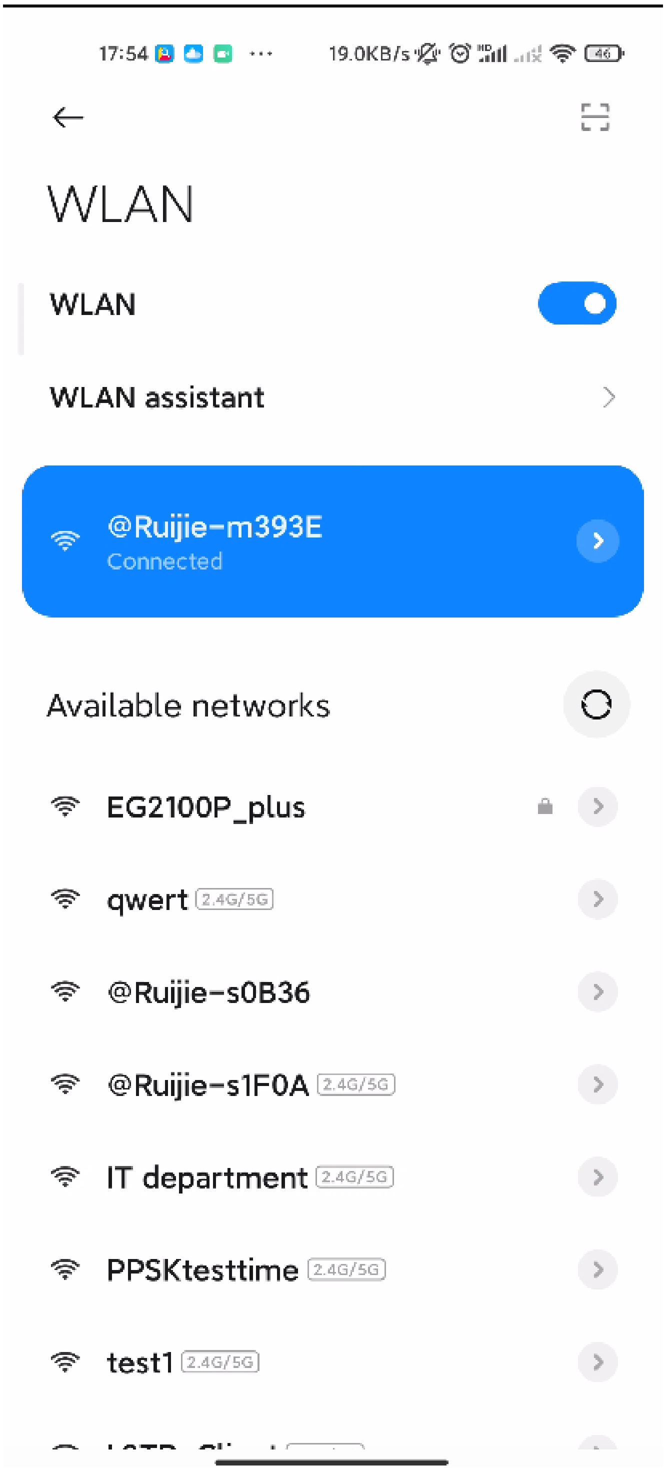
1.Please connect to the Wi-Fi starting with "@Ruijie-m".

2.Wait until ᯤ appears, and return to Ruijie Cloud to continue.

Tips:

* If there is only one AP in the network, please connect to the Wi-Fi starting with "@Ruijie-s".

(2) Connect the SSID **@Ruijie-m***xxxx* on your phone.



17:54 19.0KB/s

WLAN

WLAN

WLAN assistant

@Ruijie-m393E
Connected

Available networks

EG2100P_plus

qwert 2.4G/5G

@Ruijie-s0B36

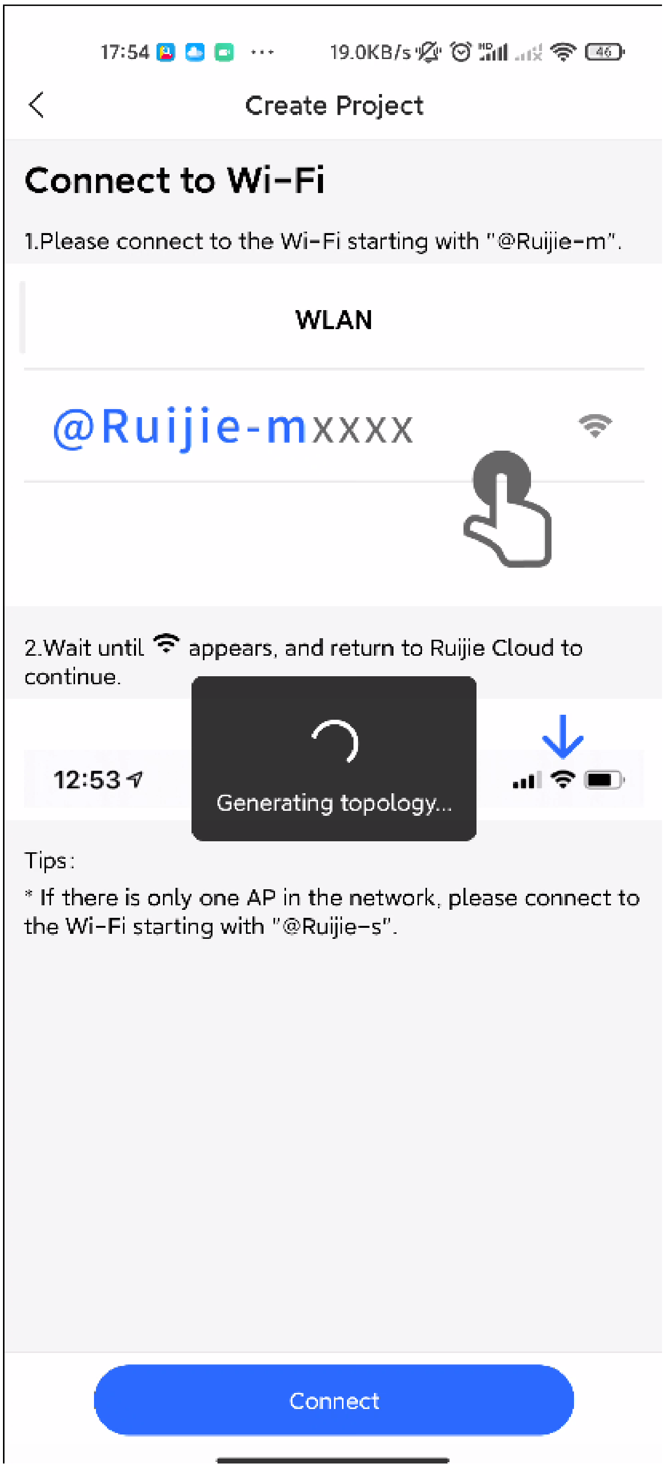
@Ruijie-s1F0A 2.4G/5G

IT department 2.4G/5G

PPSKtesttime 2.4G/5G

test1 2.4G/5G

After the phone is connected to the SSID **@Ruijie-m***xxxx*, return to Ruijie Cloud App. The Cloud App will generate the topology and detect all devices on this SON.



Create Project

Connect to Wi-Fi

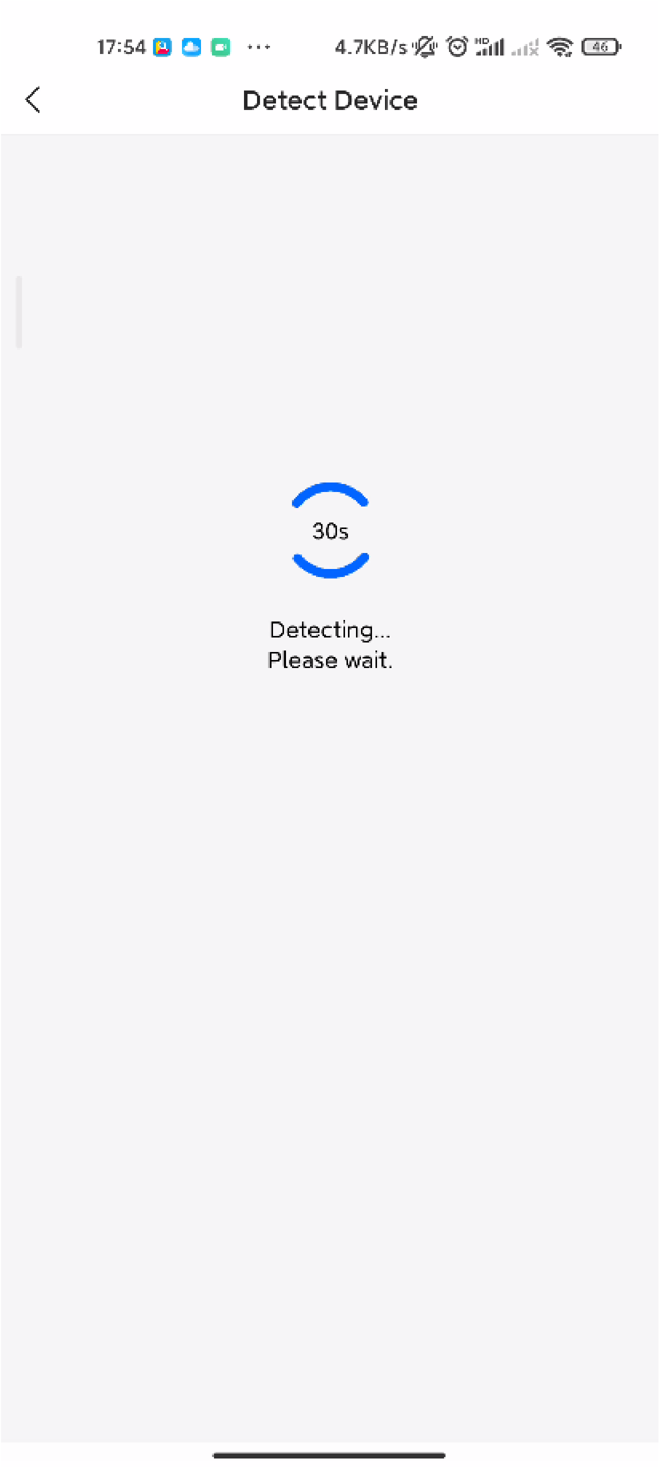
1.Please connect to the Wi-Fi starting with "@Ruijie-m".

2.Wait until ᯤ appears, and return to Ruijie Cloud to continue.

Generating topology...

Tips:

* If there is only one AP in the network, please connect to the Wi-Fi starting with "@Ruijie-s".



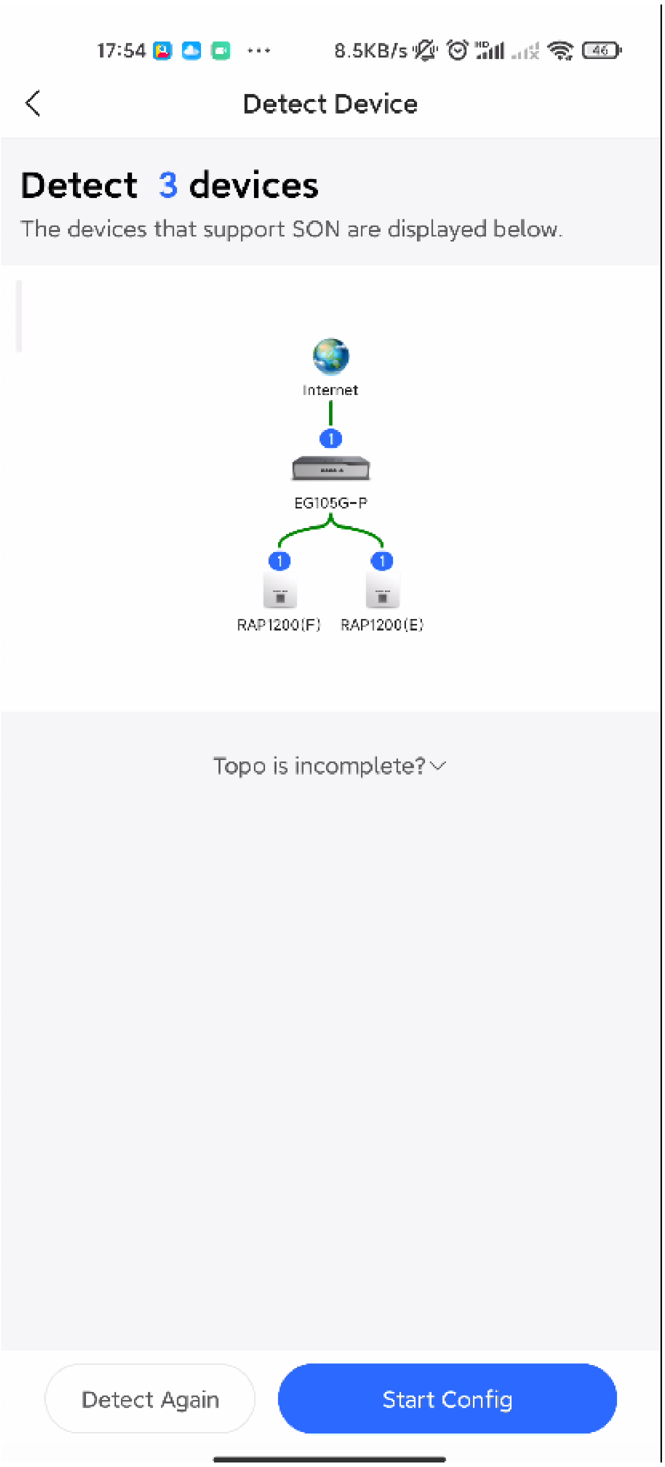
17:54 ··· 4.7KB/s

Detect Device

30s

Detecting...
Please wait.

After all devices are detected, Ruijie Cloud App will display them and show the topology.



Detect Device

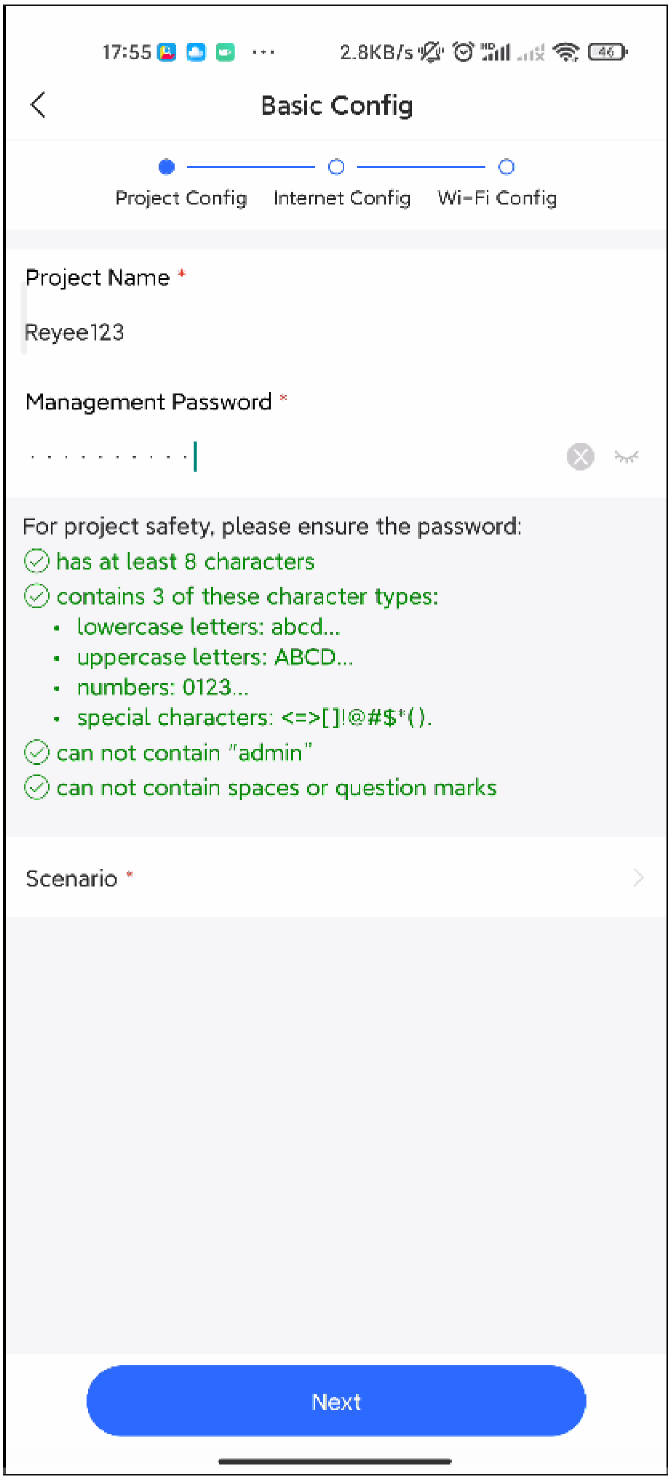
Detect 3 devices

The devices that support SON are displayed below.

(3) Click **Start Config** to perform basic configuration of this project.

Configuring the Project

(1) Enter **Project Name** and **Management Password**.



Project Name *

Reyee123

Management Password *

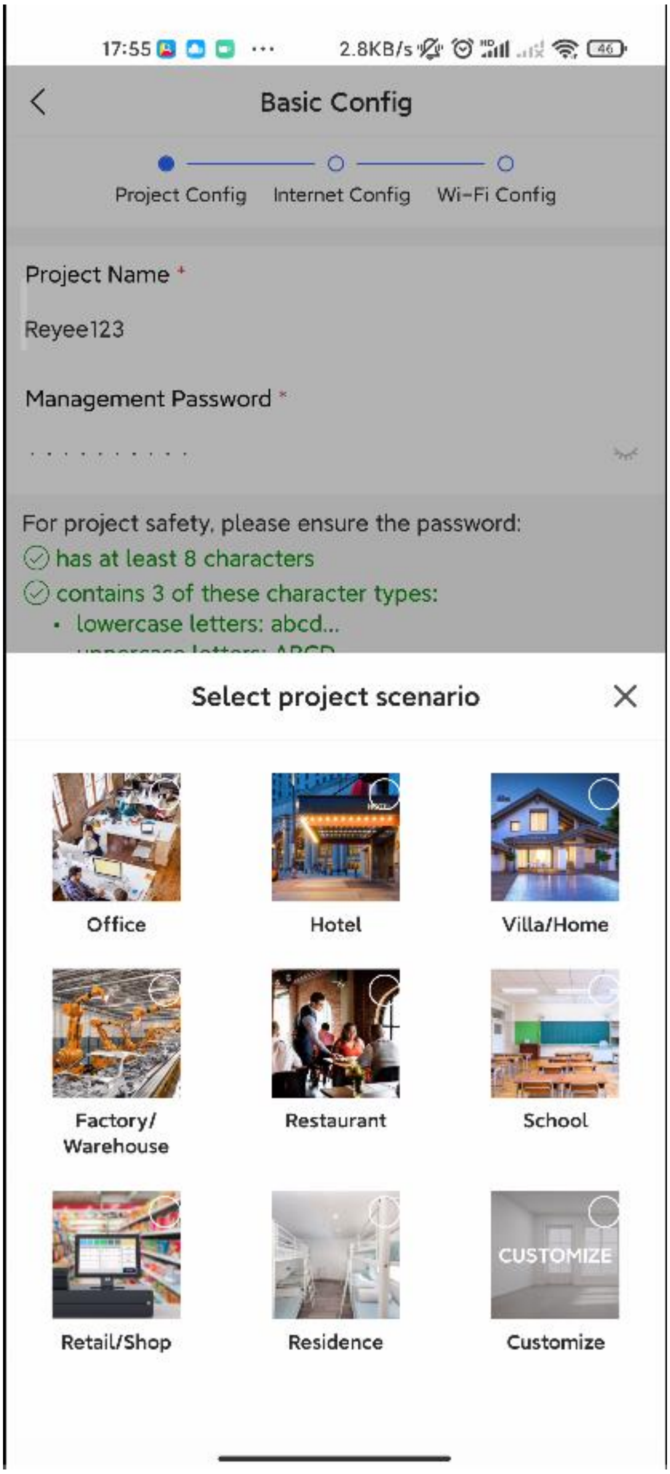
··········

For project safety, please ensure the password:

- ✓ has at least 8 characters
- ✓ contains 3 of these character types:
  - lowercase letters: abcd...
  - uppercase letters: ABCD...
  - numbers: 0123...
  - special characters: <=>[]!@#$*().
- ✓ can not contain "admin"
- ✓ can not contain spaces or question marks

Scenario *

(2) Select the scenario of this project based on your requirement.



17:55 2.8KB/s

Basic Config

● Project Config ○ Internet Config ○ Wi-Fi Config

Project Name *

Reyee123

Management Password *

. . . .

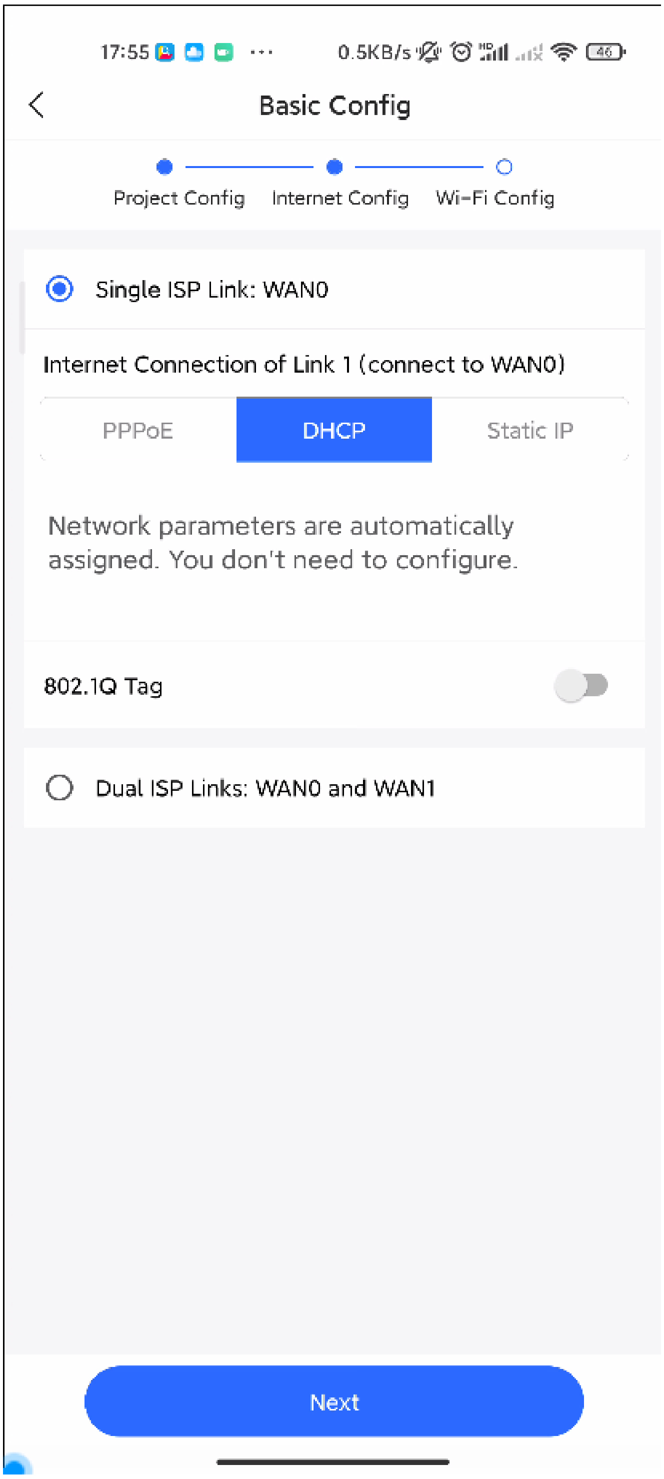
For project safety, please ensure the password:

- has at least 8 characters
- contains 3 of these character types:
  - lowercase letters: abcd...

Select project scenario ✕

Configuring the Internet

For WAN configuration, you can select **PPPoE**, **DHCP**, or **Static IP**.



◉ Single ISP Link: WAN0

Internet Connection of Link 1 (connect to WAN0)

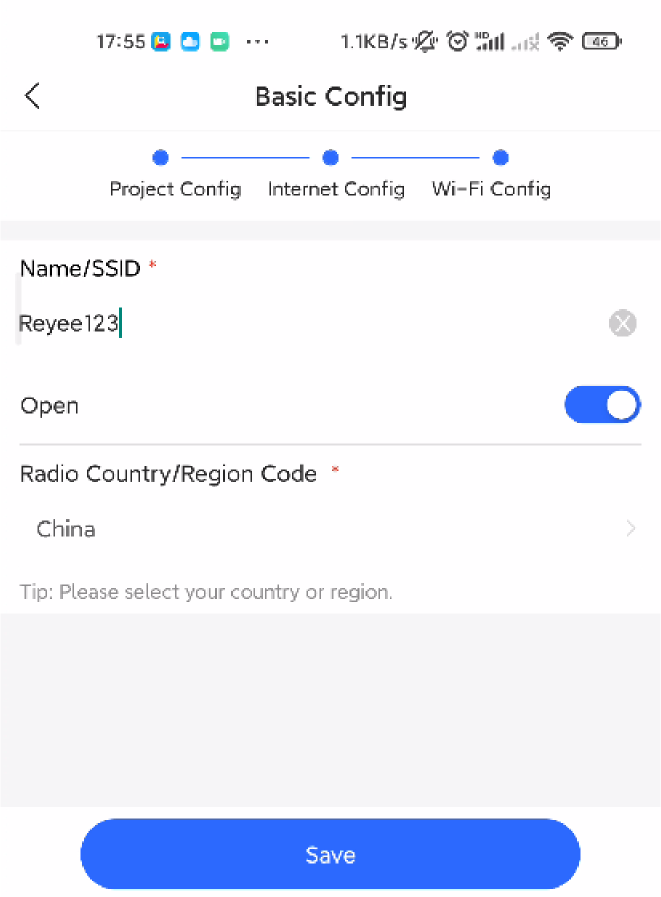
Network parameters are automatically assigned. You don't need to configure.

802.1Q Tag

○ Dual ISP Links: WAN0 and WAN1

Configuring the SSID

For SSID settings, enter the name of the SSID and enable **Open** or configure the password for this SSID. Then select the region code and click **Save**.



Name/SSID *

Reyee123

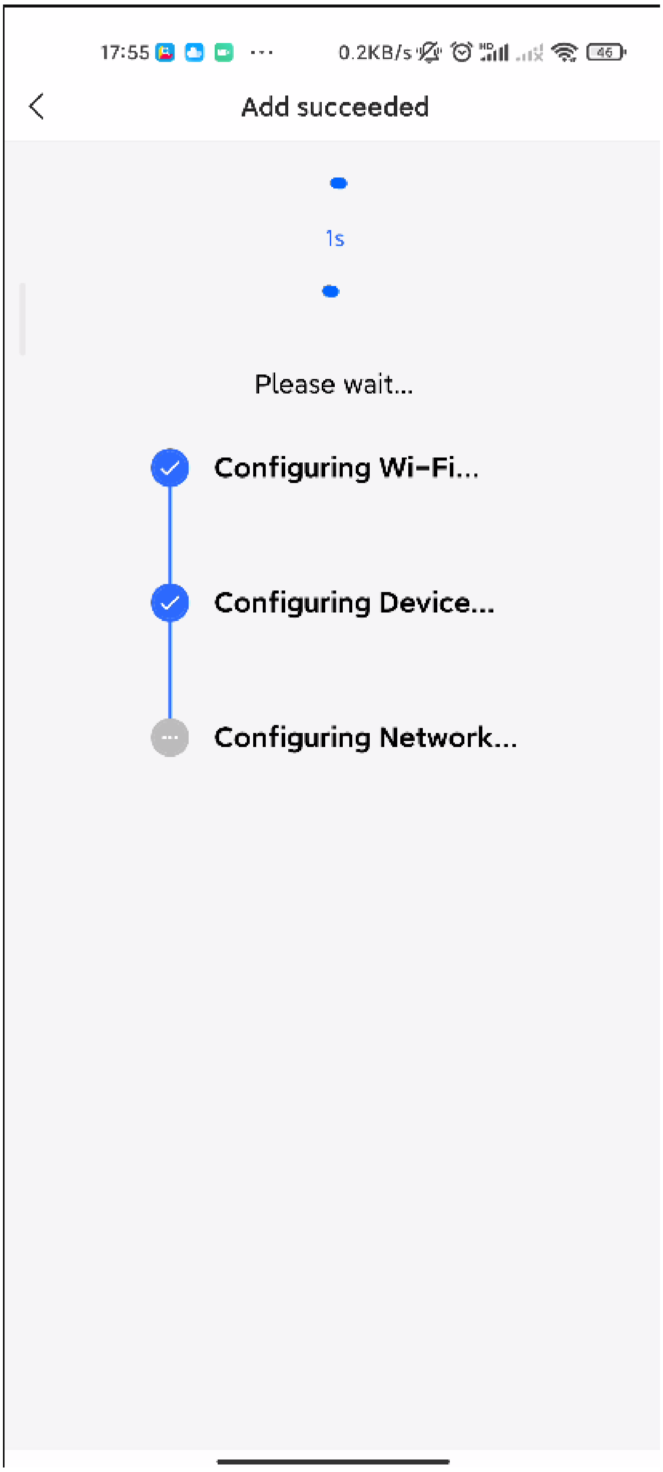
Open

Radio Country/Region Code *

China

Tip: Please select your country or region.

The configuration will be synchronized to the network.



17:55 0.2KB/s

Add succeeded

1s

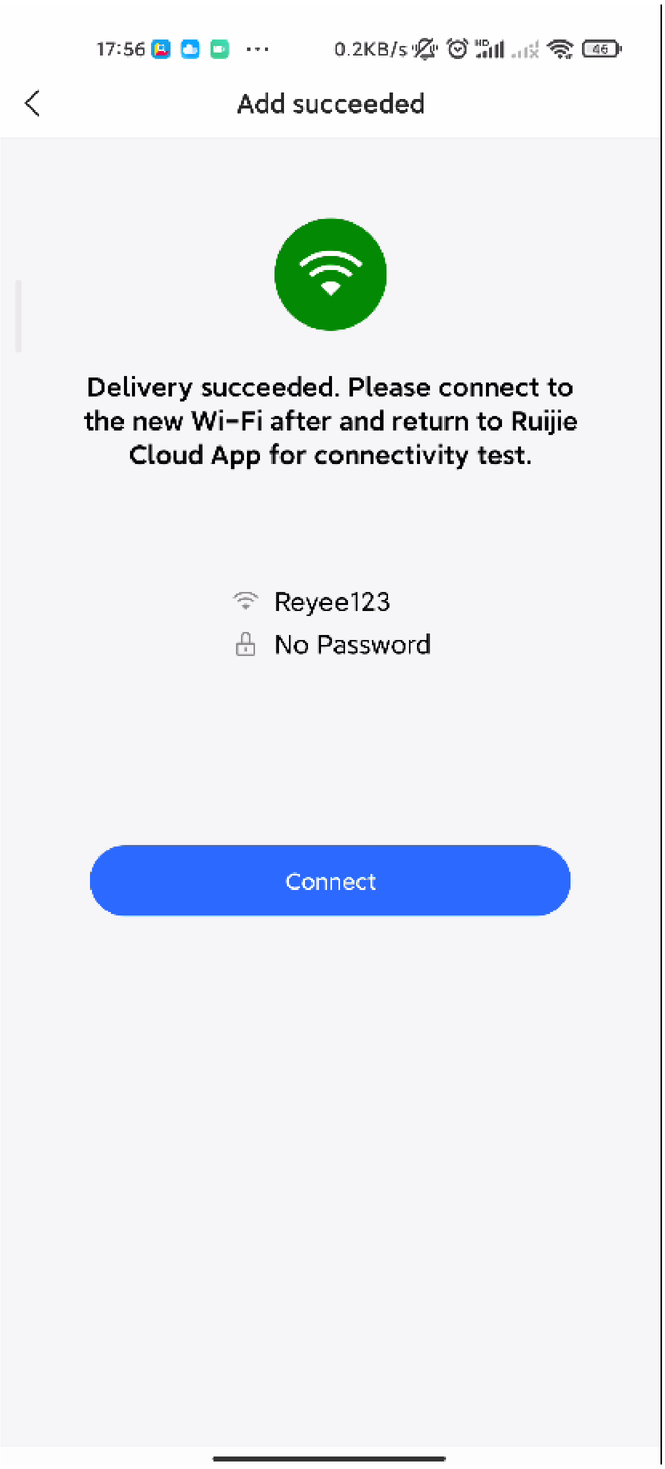
Please wait...

✓ Configuring Wi-Fi...

✓ Configuring Device...

Configuring Network...

Ruijie Cloud App displays that the configuration is delivered successfully about 3s later.



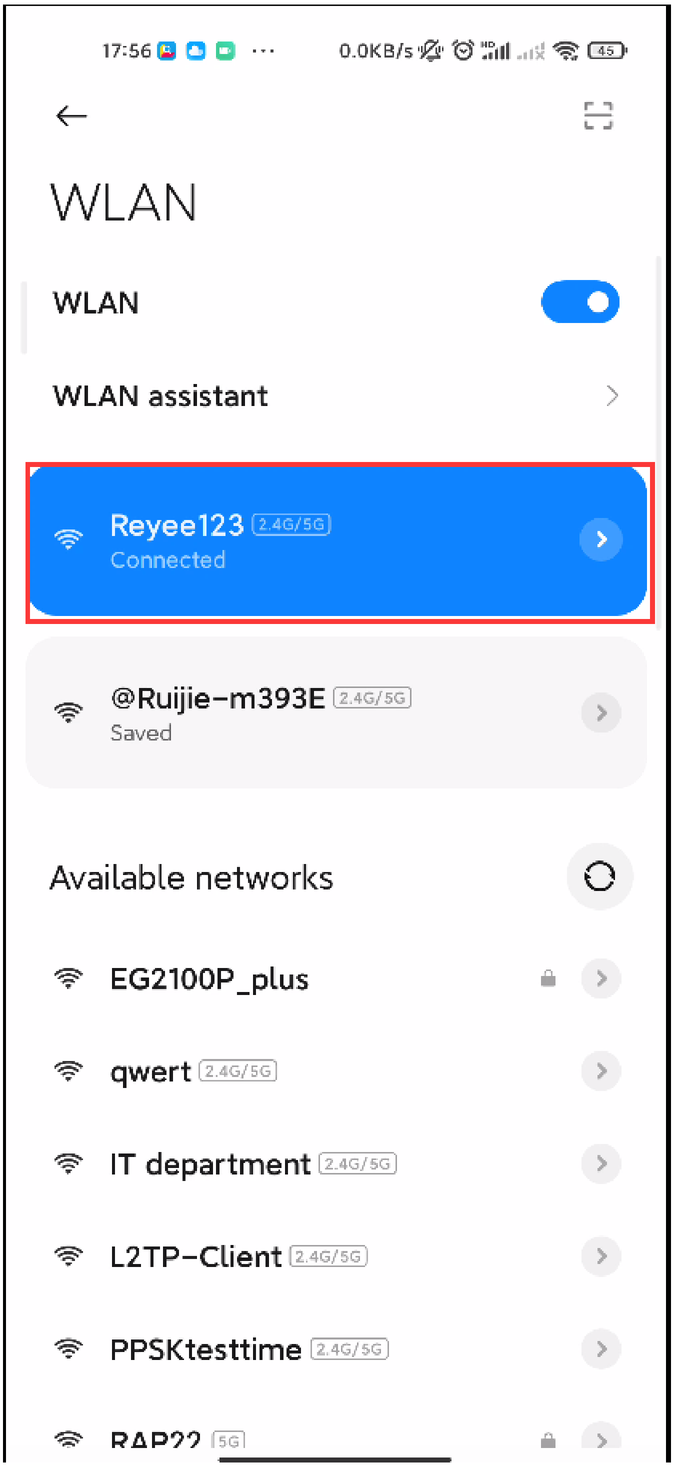
Add succeeded

Delivery succeeded. Please connect to the new Wi-Fi after and return to Ruijie Cloud App for connectivity test.

Reyee123

No Password

Connect to the SSID created to manage the entire 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

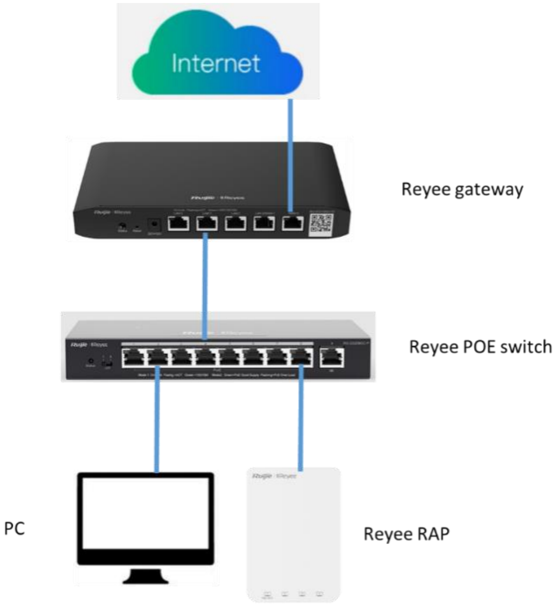
L2TP-Client 2.4G/5G

PPSKtesttime 2.4G/5G

RAP22 5G

2.3.2 Quick Provisioning Through Reyee Eweb

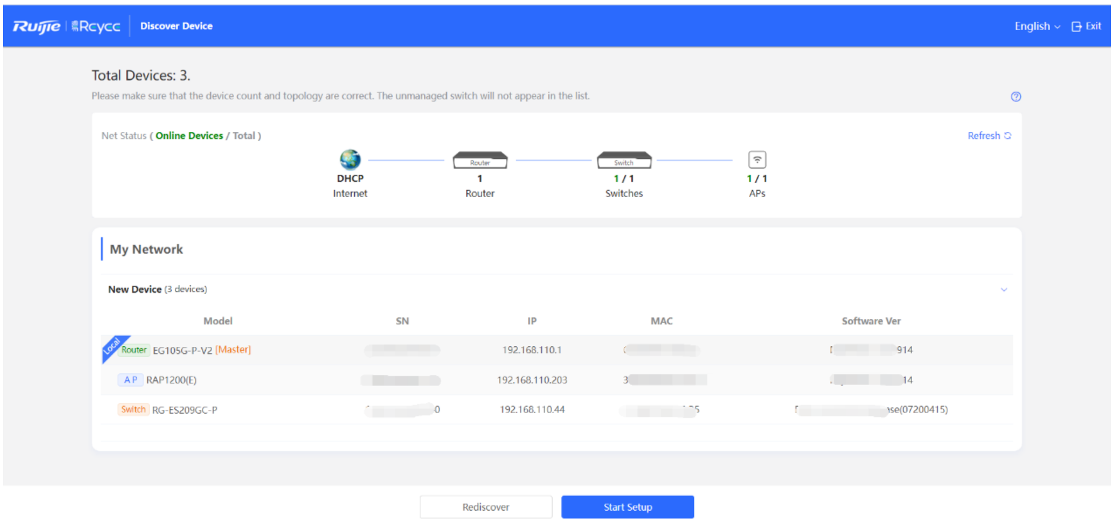
The network topology shown below includes the Reyee gateway, Reyee POE switch, and Reyee RAP.



(1) Connect a PC to the POE switch, set the IP address of the PC to the static IP address 192.168.110.*x* (*x* is an integer between 2 and 254) and the subnet mask to 255.255.255.0, and enter 192.168.110.1 in the browser address bar to log in to the Eweb of the EG.

All devices on this network will be displayed in the Eweb.

(2) Click **Start Setup** to perform quick start of the network.



Total Devices: 3.

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

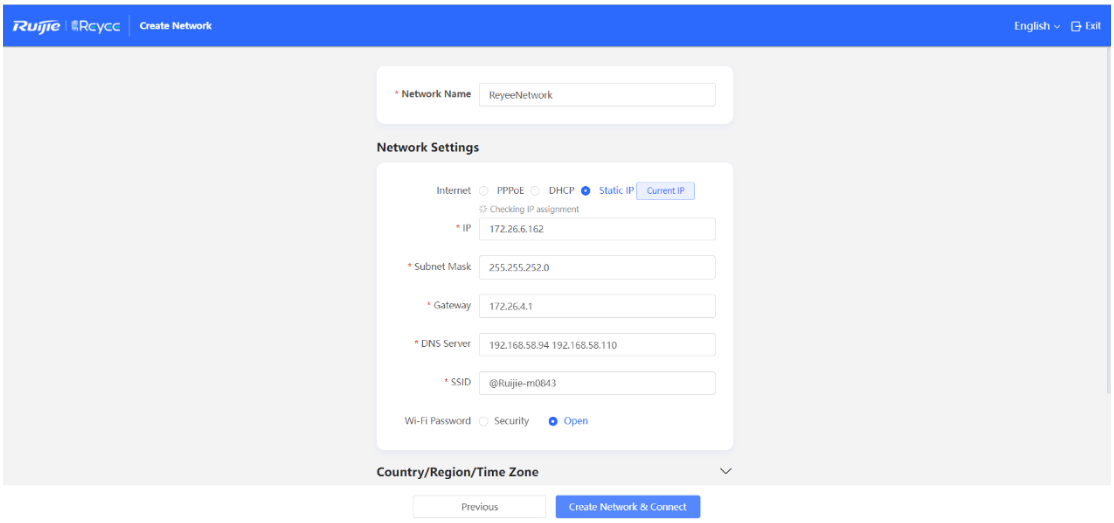
Net Status (Online Devices / Total)

My Network

New Device (3 devices)

Model	SN	IP	MAC	Software Ver
Local Router EG105G-P-V2 [Master]	[redacted]	192.168.110.1	[redacted]	[redacted]
AP RAP1200(E)	[redacted]	192.168.110.203	[redacted]	[redacted]
Switch RG-ES209GC-P	[redacted]	192.168.110.44	[redacted]	[redacted]

(3) To finish quick start of the network, enter the network name, configure the Internet access mode of the network and enter the password of the SSID or enable **Open**. Then select **Country/Region/Time Zone**.



* Network Name: ReyeeNetwork

Network Settings

Internet: ○ PPPoE ○ DHCP ● Static IP Current IP

Checking IP assignment

* IP: 172.26.6.162

* Subnet Mask: 255.255.252.0

* Gateway: 172.26.4.1

* DNS Server: 192.168.58.94 192.168.58.110

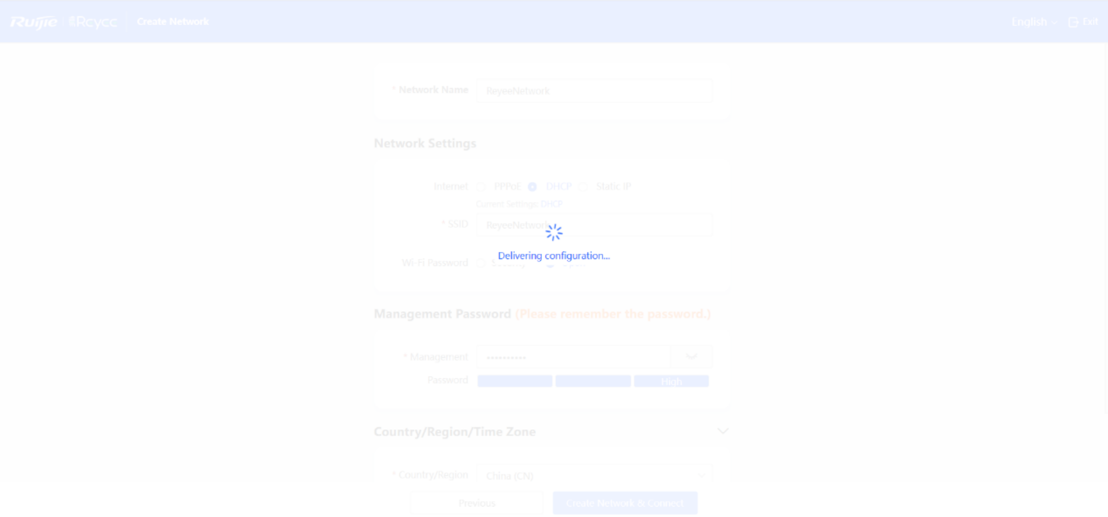
* SSID: @Ruijie-m0843

Wi-Fi Password: ○ Security ● Open

Country/Region/Time Zone

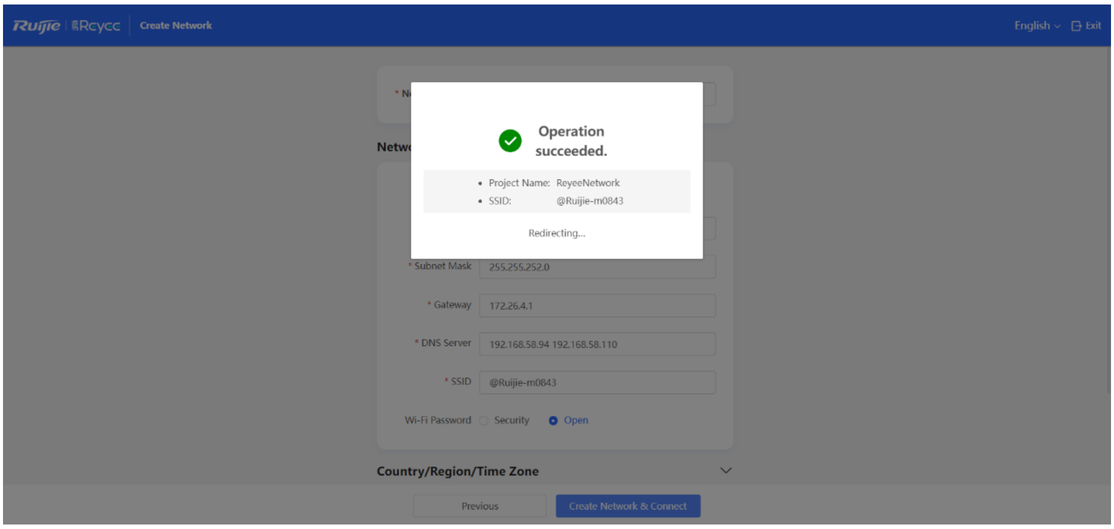
(4) Click **Create Network & Connect**.

The configuration will be delivered and activated.



Delivering configuration...

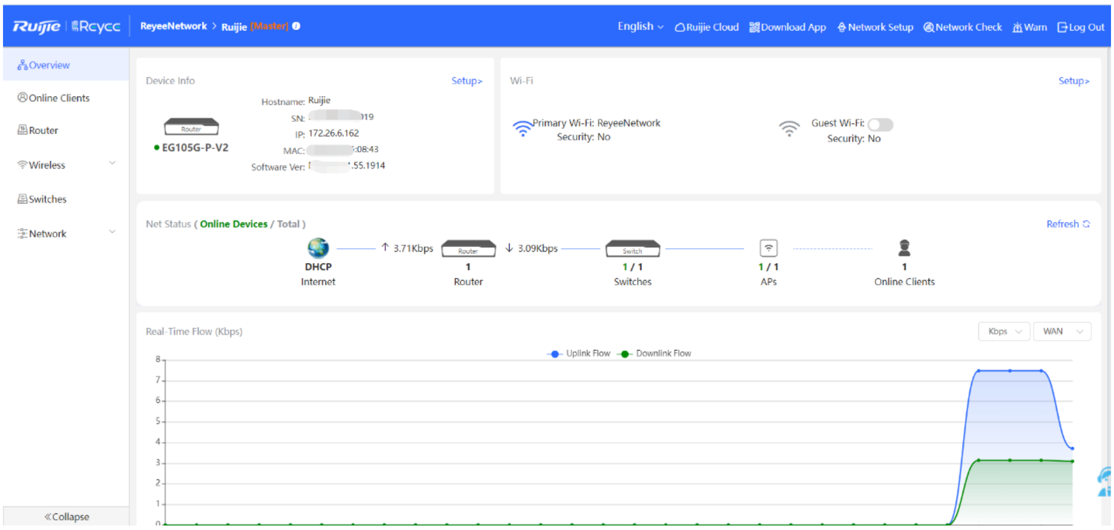
After the configuration has been delivered and activated, you can access the overview interface to manage the SON of Reyee devices.



Operation succeeded.

- Project Name: ReyeeNetwork
- SSID: @Ruijie-m0843

Redirecting...



Device Info

EG105G-P-V2

Hostname: Ruijie

SN: [redacted]19

IP: 172.26.6.162

MAC: [redacted]:08:43

Software Ver: [redacted].55.1914

Wi-Fi

Primary Wi-Fi: ReyeeNetwork
Security: No

Guest Wi-Fi:
Security: No

Net Status (Online Devices / Total)

↑ 3.71Kbps ↓ 3.09Kbps

DHCP
Internet

1
Router

1 / 1
Switches

1 / 1
APs

1
Online Clients

Real-Time Flow (Kbps)

3 Device Management

3.1 Login

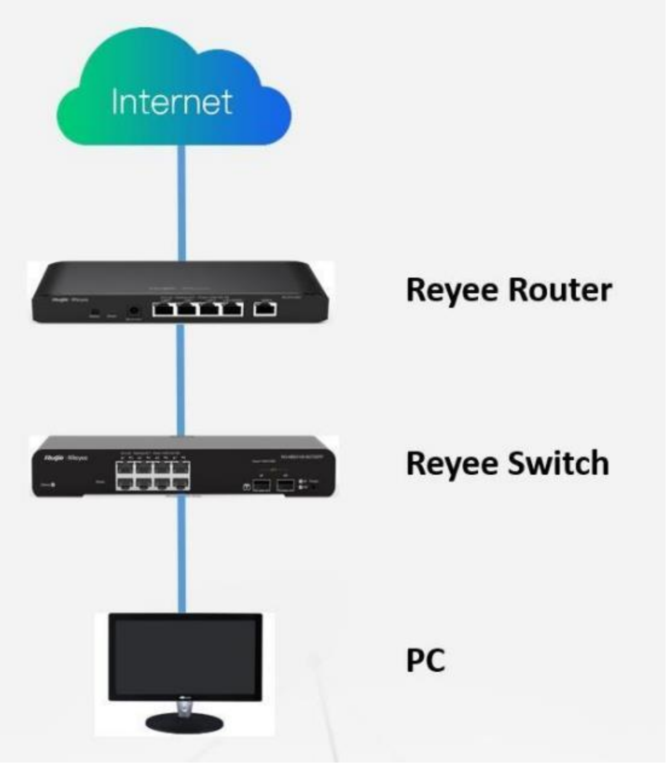
Eweb is a web-based network management system used to manage or configure devices. You can access Eweb through a browser such as Google Chrome. Web-based management involves a web server and a web client. The web server, which is integrated in a device, is used to receive and process requests from the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

The Reyee managed switches support both web interface management and remote management through life-time-free Ruijie Cloud App and Ruijie Cloud platform. You can view the network status, modify the configuration, and troubleshoot faults easily.

3.1.1 Case Demonstration

Network Topology

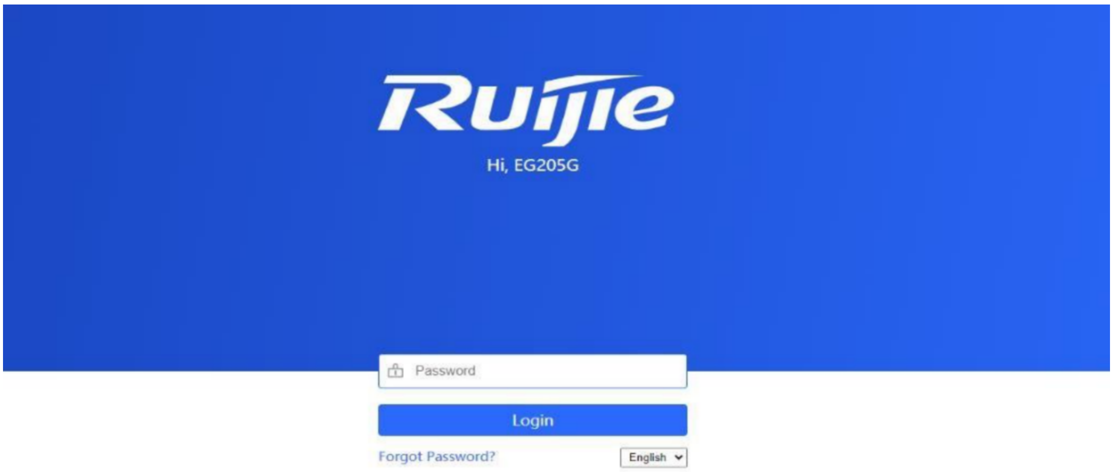
In the following figure, you can access the Eweb management system of an access or aggregation switch through a PC browser to manage and configure the device.



(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**.



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

For the Reyee switch, you may use 10.44.77.200 to access it.

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

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

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

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

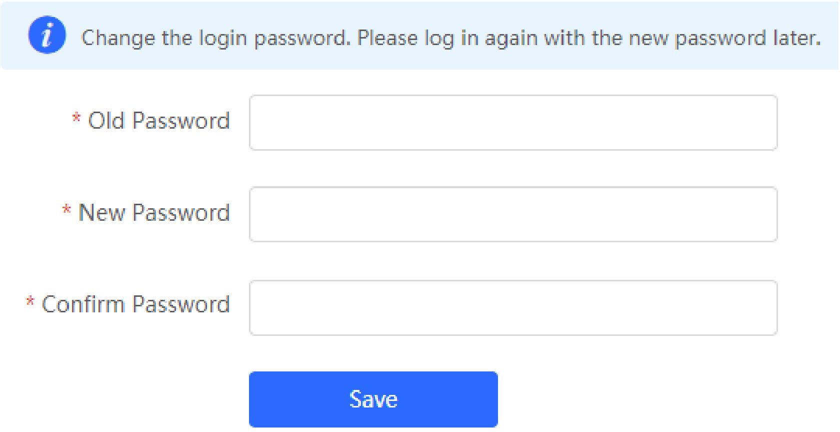
3.2 Setting the Login Password

Choose **System** > **Login** > **Login Password**.

Enter the old password and new password. After saving the configuration, use the new password to log in.

Note

In SON mode, the login password of all devices on the network will be changed synchronously.


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

3.3 Performing Upgrade and Checking the System Version

Note

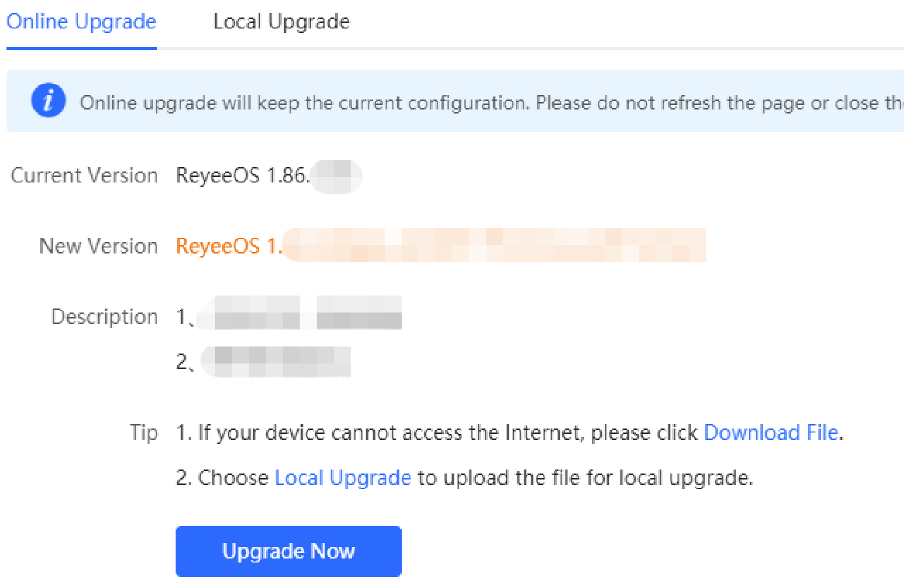
- You are advised to back up the configuration before upgrading the AP.
- After being upgraded, the AP will restart. Therefore, exercise caution when performing this operation.

3.3.1 Online Upgrade

- In SON mode, select **Local Device** and choose **System** > **Upgrade** > **Online Upgrade**.
- In standalone mode, choose **System** > **Upgrade** > **Online Upgrade**.

You can view the current system version.

- If a new version is available, you can click **Upgrade Now** for an upgrade. The upgrade operation does not affect the current configuration, but the AP will restart after being upgraded successfully. Do not refresh the page or close the browser during the upgrade. You will be redirected to the login page automatically after the upgrade.



Online upgrade will keep the current configuration. Please do not refresh the page or close th

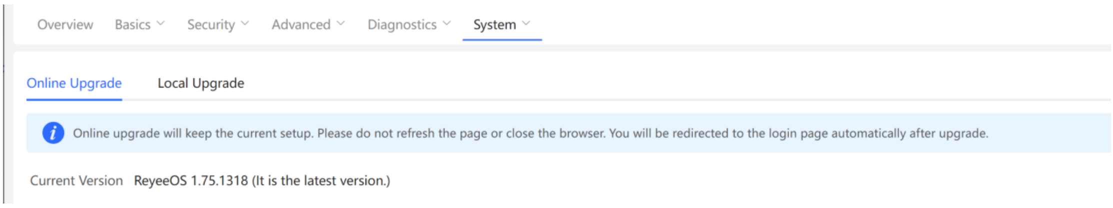
Current Version ReyeeOS 1.86.[redacted]

New Version ReyeeOS 1.[redacted]

Description 1、[redacted]
2、[redacted]

Tip 1. If your device cannot access the Internet, please click Download File.
2. Choose Local Upgrade to upload the file for local upgrade.

- If there is no new version, a massage is displayed, indicating that the current version is the latest.



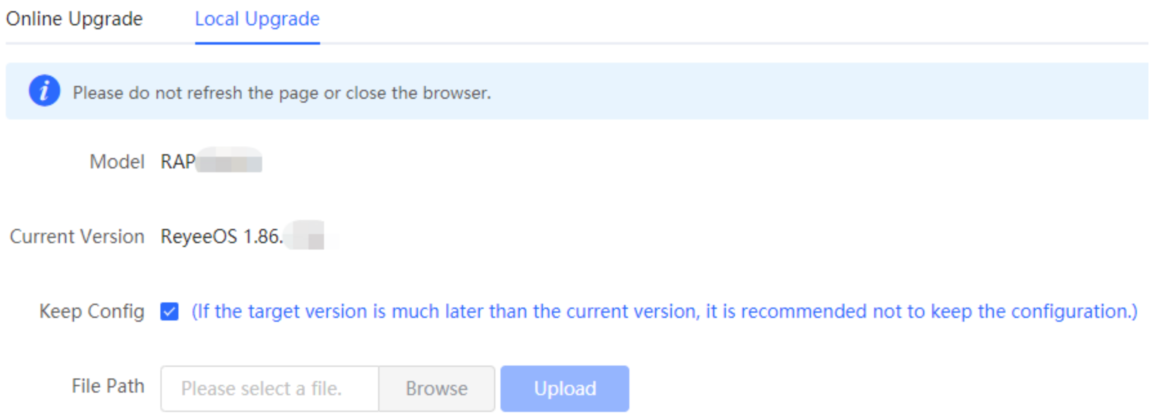
Online upgrade will keep the current setup. Please do not refresh the page or close the browser. You will be redirected to the login page automatically after upgrade.

Current Version ReyeeOS 1.75.1318 (It is the latest version.)

3.3.2 Local Upgrade

- In SON mode, select **Local Device** mode and choose **System** > **Upgrade** > **Local Upgrade**.
- In standalone mode, choose **System** > **Upgrade** > **Local Upgrade**.

You can view the current software version, hardware version, and device model. To upgrade the device with the configuration retained, check **Keep Config**. Click **Browse**, select an upgrade package on the local PC, and click **Upload** to upload the file. After the AP is uploaded successfully, the system will display upgrade package information and asks you to upgrade the AP. Click **OK** to start the upgrade.



Online Upgrade | Local Upgrade

Please do not refresh the page or close the browser.

Model RAP[redacted]

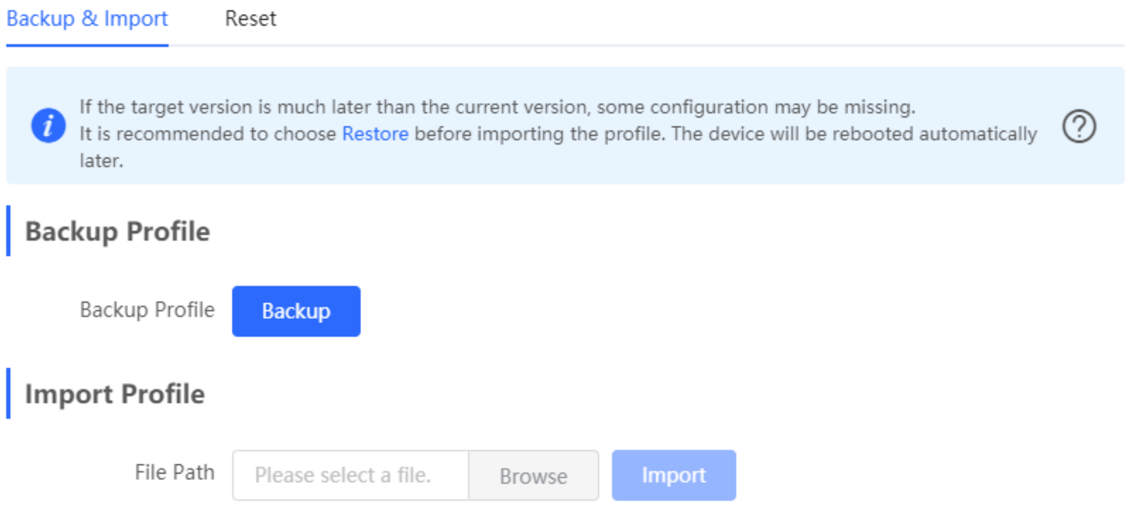
Current Version ReyeeOS 1.86.[redacted]

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

File Path Please select a file. Browse Upload

3.4 Configuring Backup and Import

Choose **System** > **Management** > **Backup & Import**.



Backup & Import | Reset

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

Backup Profile

Backup Profile Backup

Import Profile

File Path Please select a file. Browse Import

You can import a configuration file to the AP or export the current configuration of the AP.

- Configuration backup: Click **Backup** to download a configuration file locally.
- Configuration import: Click **Browse**, select a backup file on the local PC, and click **Import** to import the configuration file. The AP will restart.

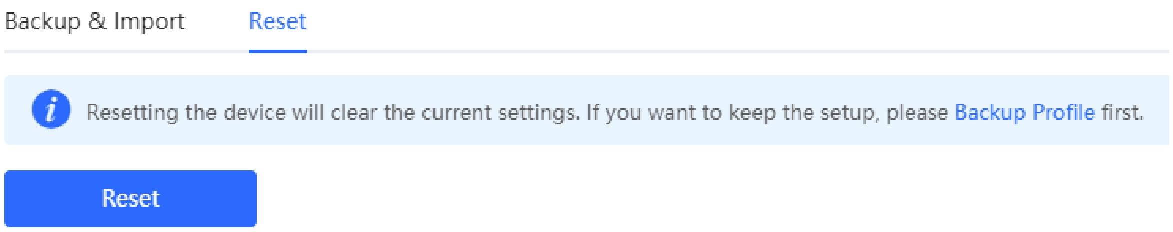
  If the target version is much later than the current version, some configuration may be missing.

  You are advised to restore the settings before importing the configuration. The AP will restart automatically if you restore it.

3.5 Restoring Factory Settings

- In SON mode, select **Local Device** mode and choose **System** > **Management** > **Reset**.
- In standalone mode, choose **System** > **Management** > **Reset**.

Click **Reset** to restore the AP to factory defaults.



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

⚠ **Note**

The operation will clear all configuration of the AP. To retain the current configuration, back up the configuration first (see 3.4Configuring Backup and Import). Therefore, exercise caution when performing this operation.

4 Configuration

4.1 Wireless Configuration

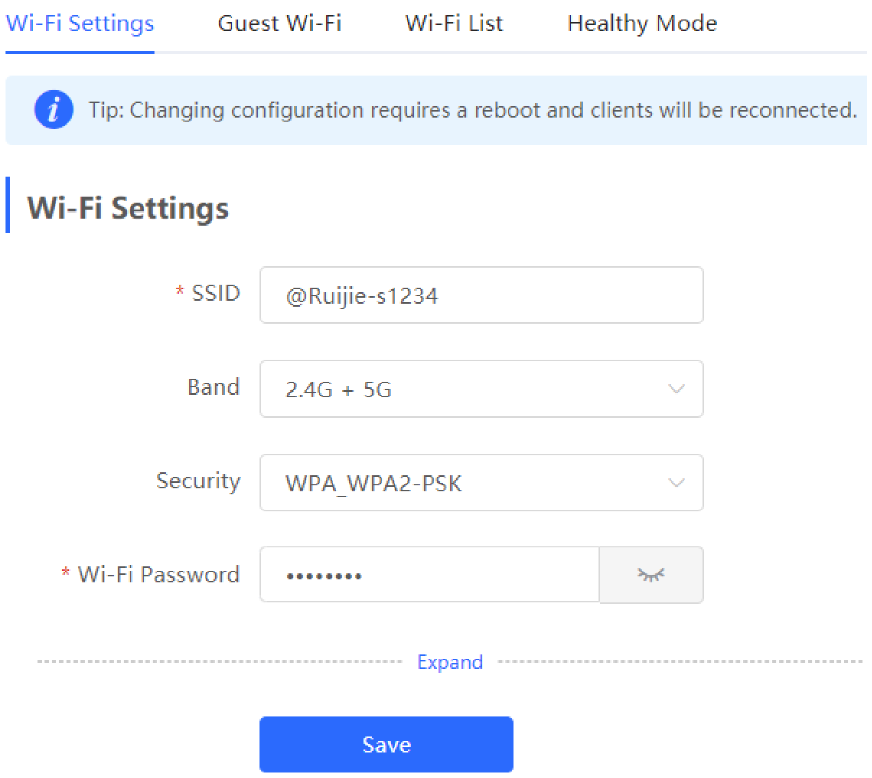
4.1.1 Wireless Basic Configuration

- SON mode
    - To configure the master Wi-Fi, select **Network** and choose **Network** > **Wi-Fi** > **Wi-Fi Settings**.
    - To configure other Wi-Fi, select **Network** and choose **Network** > **Wi-Fi** > **Wi-Fi List**. Then select the target Wi-Fi in the list and click **Edit** in the action bar.
- Standalone mode
    - To configure the master Wi-Fi, choose **WLAN > Wi-Fi > Wi-Fi Settings**.
    - To configure other Wi-Fi, choose **WLAN** > **Wi-Fi** > **Wi-Fi List**. Then select the target Wi-Fi in the list and click **Edit** in the action bar.

Set parameters of the Wi-Fi network and click **Save**.

Note

After the configuration is saved, all online clients will be disconnected from the Wi-Fi network. You have to enter the new password to connect to the Wi-Fi network.



Tip: Changing configuration requires a reboot and clients will be reconnected.

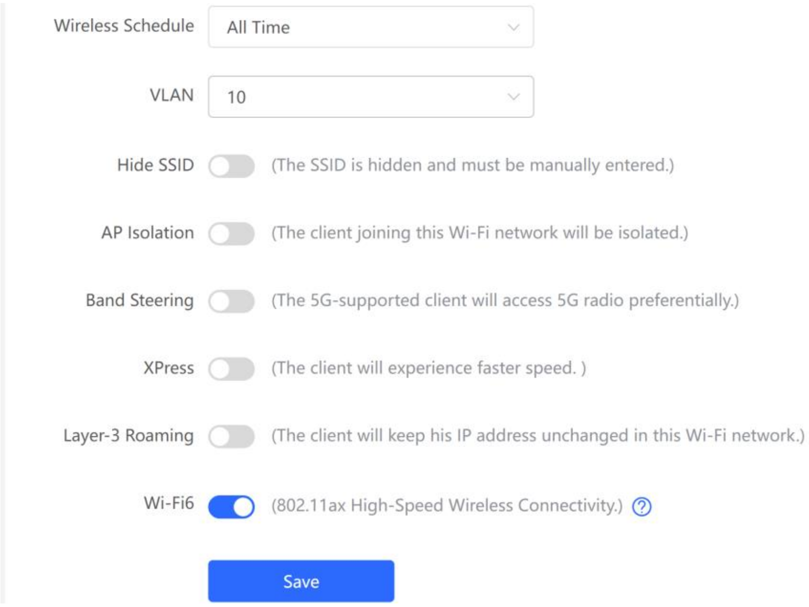
Wi-Fi Settings

* SSID: @Ruijie-s1234

Band: 2.4G + 5G

Security: WPA_WPA2-PSK

* Wi-Fi Password: ••••••••



Wireless Schedule: All Time

VLAN: 10

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-Fi6: ● (802.11ax High-Speed Wireless Connectivity.) ?

SSID: indicates the Wi-Fi name.

Band: indicates the band, which is **2.4G**, **5G**, or **2.4G + 5G**.

Security: indicates the security authentication mode, which is **Open**, **WPA-PSK**, **WPA2-PSK**, or **WPA_WPA2-PSK**.

Wireless Schedule: indicates the time when Wi-Fi takes effect.

Hide SSID: disables or enables SSID broadcasting.

AP Isolation: indicates that the SSID-based client will be isolated.

Band Steering: detects clients capable of 5 GHz and steers them to that frequency. 2.4 GHz is available for legacy clients. Enabling this function is not recommended if most clients only support 2.4 GHZ.

XPress: enables faster speed for clients.

Layer-3 Roaming: A client will keep the IP address unchanged on the Wi-Fi network. Layer 3 roaming can be enabled on Reyee APs here, and Ruijie Cloud only supports Ruijie APs.

Wi-Fi 6: Some wireless adapters of old versions may be incompatible. The end points accessing the Wi-Fi 6 network must support 802.11ax.

4.1.2 Guest Wi-Fi Configuration

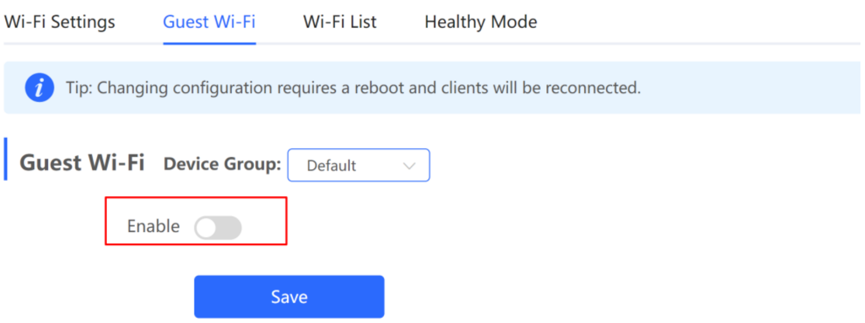
This Wi-Fi network is provided for guests and is disabled by default. It supports client isolation, that is, clients are isolated from each other. The clients can only access the Internet by Wi-Fi, but cannot access each other, improving security. The guest Wi-Fi network can be disabled as scheduled. When the time expires, the guest network is disconnected.

Procedure

(1) Access the **Guest Wi-Fi** page.

- In SON mode, select **Network** mode and choose **Network** > **Wi-Fi** > **Guest Wi-Fi**.
- In standalone mode, choose **WLAN** > **Wi-Fi** > **Guest Wi-Fi**.

The guest Wi-Fi is disabled by default.



Wi-Fi Settings | Guest Wi-Fi | Wi-Fi List | Healthy Mode

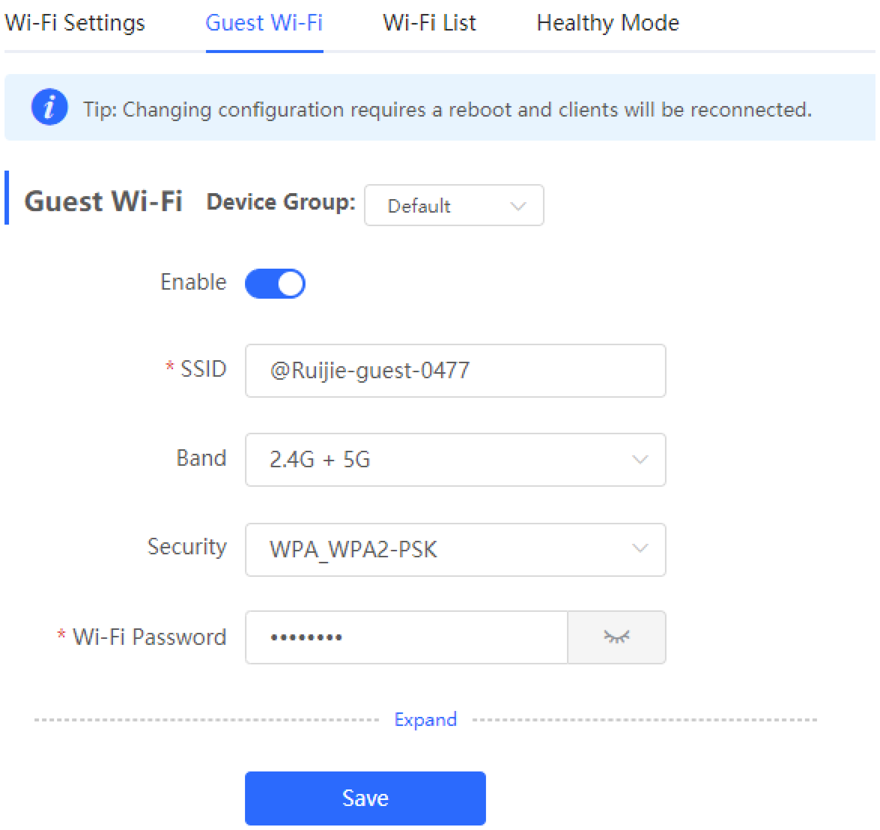
Tip: Changing configuration requires a reboot and clients will be reconnected.

Guest Wi-Fi Device Group: Default

Enable ○

Save

(2) Enable **Guest Wi-Fi** and enter the SSID and Wi-Fi password.



Wi-Fi Settings | Guest Wi-Fi | Wi-Fi List | Healthy Mode

Tip: Changing configuration requires a reboot and clients will be reconnected.

Guest Wi-Fi Device Group: Default

Enable ●

* SSID: @Ruijie-guest-0477

Band: 2.4G + 5G

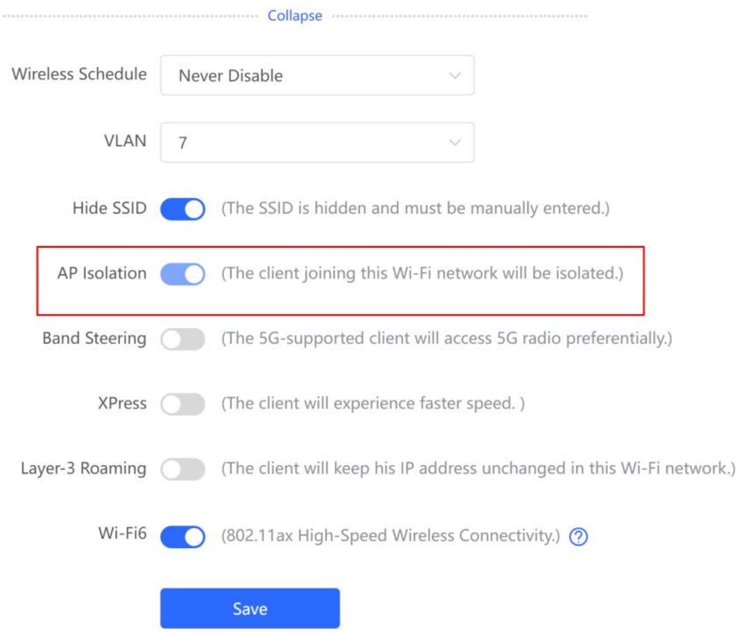
Security: WPA_WPA2-PSK

* Wi-Fi Password: ••••••••

Expand

Save

(3) Click **Expand** to configure the validity time and other Wi-Fi features in the expanded settings. Click **Save**. The guest Wi-Fi network will be created. Guests can access the guest Wi-Fi network by entering the SSID and Wi-Fi password.



Wireless Schedule: Never Disable

VLAN: 7

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-Fi6: ● (802.11ax High-Speed Wireless Connectivity.)

Instruction

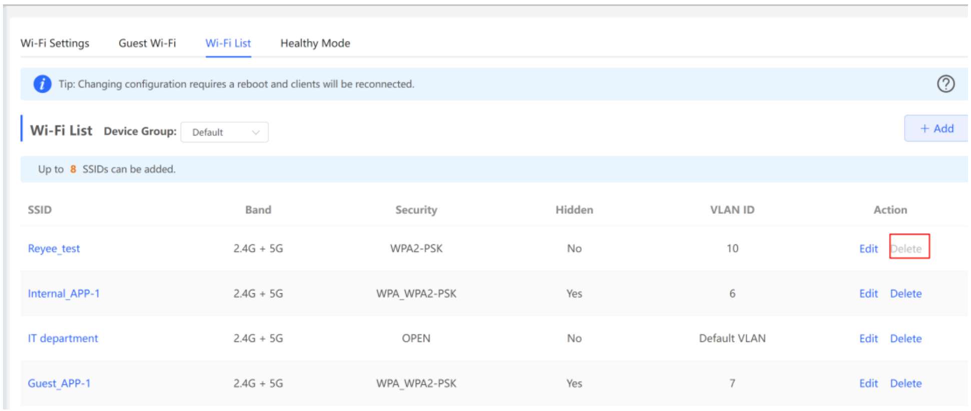
AP isolation is enabled by default and cannot be modified.

Set the wireless schedule. The guest Wi-Fi will be enabled only at this schedule. When the time expires, the guest Wi-Fi will be disabled.

4.1.3 Multiple SSID Configuration

- In SON mode, select **Network** mode and choose **Network** > **Wi-Fi** > **Wi-Fi List**.
- In standalone mode, choose **WLAN** > **Wi-Fi** > **Wi-Fi List**.

Wi-Fi List displays all Wi-Fi networks. The primary Wi-Fi is also listed here and cannot be deleted.



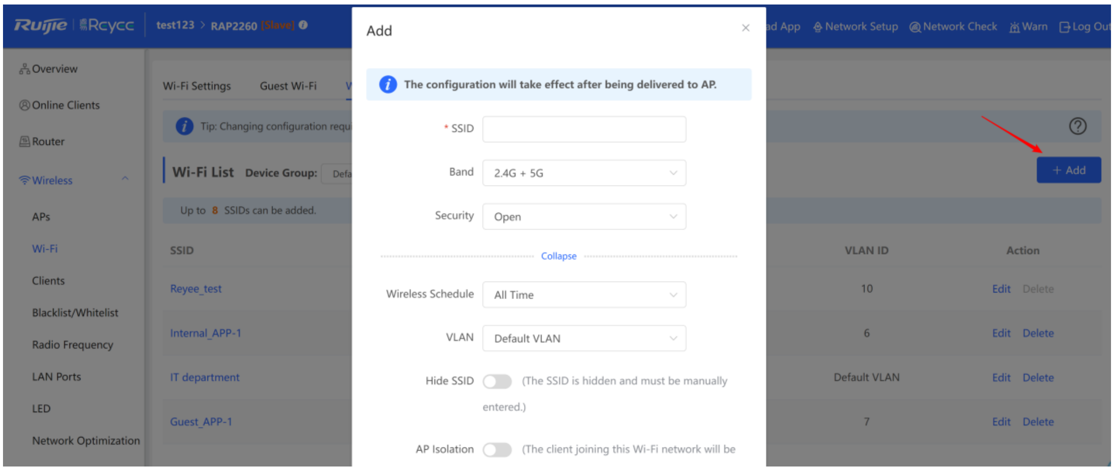
Tip: Changing configuration requires a reboot and clients will be reconnected.

Wi-Fi List Device Group: Default

Up to 8 SSIDs can be added.

SSID	Band	Security	Hidden	VLAN ID	Action
Reyee_test	2.4G + 5G	WPA2-PSK	No	10	Edit Delete
Internal_APP-1	2.4G + 5G	WPA_WPA2-PSK	Yes	6	Edit Delete
IT department	2.4G + 5G	OPEN	No	Default VLAN	Edit Delete
Guest_APP-1	2.4G + 5G	WPA_WPA2-PSK	Yes	7	Edit Delete

- To reconfigure an existing Wi-Fi network, click **Edit**, set parameters in the displayed dialog box, and click **OK**. After changing the configuration, restart the device. Then your network will be reconnected.
- To add a Wi-Fi network, click **Add**, configure parameters in the displayed dialog box, and click **OK** to save the configuration.



Tip: Changing configuration requ

Wi-Fi List Device Group: Defa

Up to 8 SSIDs can be added.

Add

The configuration will take effect after being delivered to AP.

* SSID

Band: 2.4G + 5G

Security: Open

Wireless Schedule: All Time

VLAN: Default VLAN

Hide SSID (The SSID is hidden and must be manually entered.)

AP Isolation (The client joining this Wi-Fi network will be

4.1.4 Healthy Mode

Healthy Mode allows you to enable the healthy mode and set a schedule.

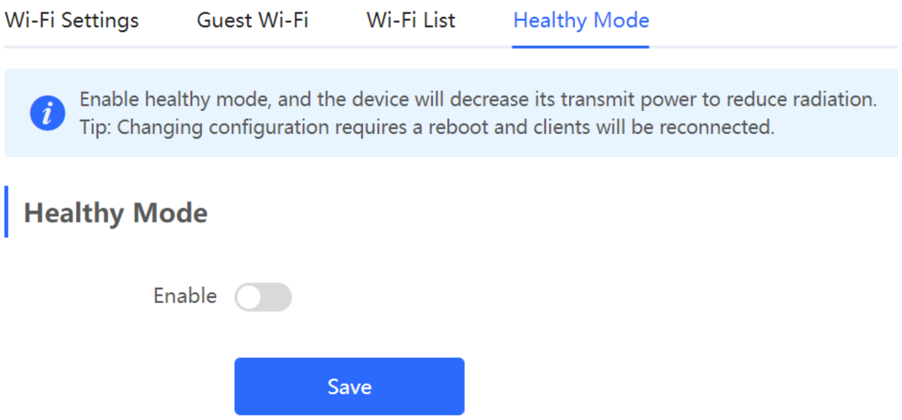
- The healthy mode may reduce signal strength and cause network suspension. You are advised to disable it or enable it when the network is idle.
- After the healthy mode is enabled, the AP will decrease its transmit power to reduce radiation.
- After changing the configuration, restart the device. Then your network will be reconnected.
- Router radiation is much lower than common radiation, which does not cause damage to the human body.

Procedure

(1) Access the **Healthy Mode** page.

- In SON mode, select **Network** and choose **Network** > **Wi-Fi** > **Healthy Mode**.
- In standalone mode, choose **WLAN** > **Wi-Fi** > **Healthy Mode**.

(2) Click **Enable** to enable the healthy mode.

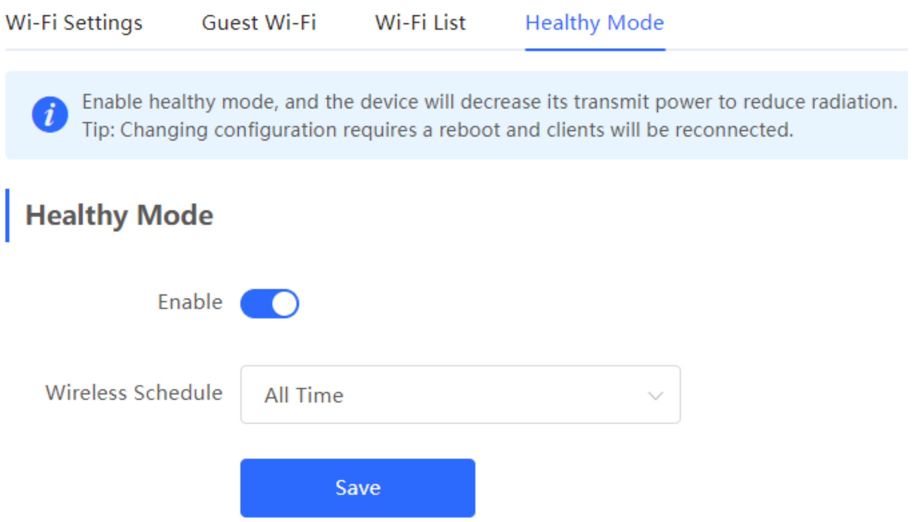


Enable healthy mode, and the device will decrease its transmit power to reduce radiation.
Tip: Changing configuration requires a reboot and clients will be reconnected.

Healthy Mode

Enable

(3) Set the validity time for the healthy mode, and click **Save**.



Enable healthy mode, and the device will decrease its transmit power to reduce radiation.
Tip: Changing configuration requires a reboot and clients will be reconnected.

Healthy Mode

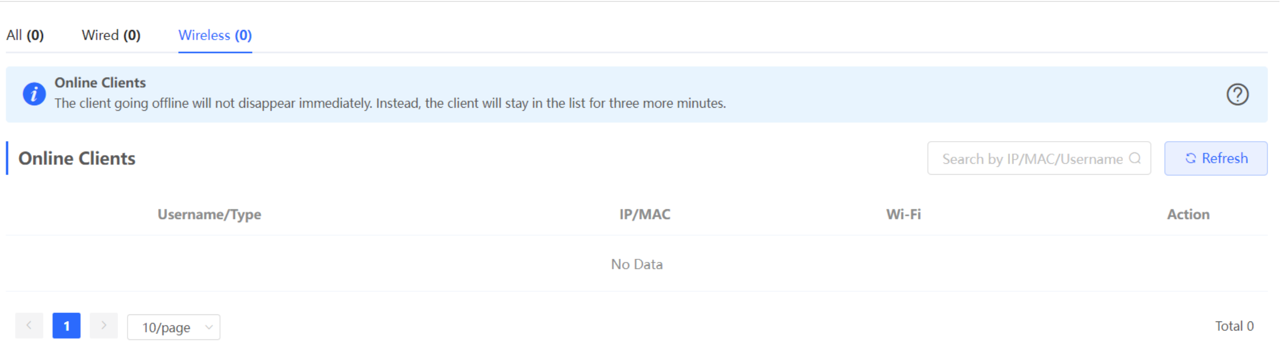
Enable: on

Wireless Schedule: All Time

4.1.5 Wireless Client List

Choose **Clients** > **Online Clients** > **Wireless**.

Check information about all wireless clients connected to the Wi-Fi network. You can click **Advanced Search** to search clients by SN and MAC address.



Online Clients
The client going offline will not disappear immediately. Instead, the client will stay in the list for three more minutes.

Online Clients

Username/Type	IP/MAC	Wi-Fi	Action
	No Data		

Total 0

Table 1-1 Description of Wireless Client Information

Item	Description
Username/Type	Name and type of the client.
IP/MAC	IPv4 address and MAC address of the client.
Wi-Fi	Name of the Wi-Fi network associated with the client.
Action	Click **Add to Blacklist** to disconnect a client and prevent the client from accessing the Wi-Fi network.

4.1.6 Radio Frequency Configuration

- SON mode:

- ○ To configure the master device, select **Network** and choose **Network > Radio Frequency**.
- ○ To configure the slave device, select **Devices**, select the target device in the device list, and choose **SN** > **Radio Frequency**.

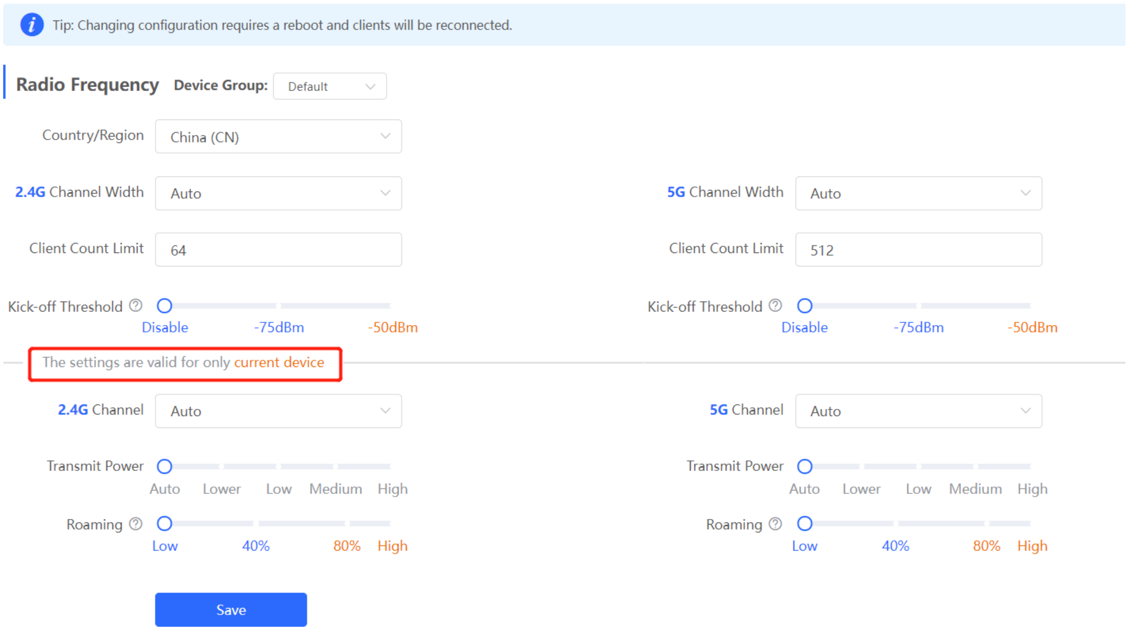
- In standalone mode, choose **WLAN > Radio Frequency**.

Select the best channel identified by Wi-Fi Moho or other Wi-Fi scanning App. Click **Save** to make the configuration take effect immediately. More devices in a channel indicate more severe interference.

Instruction

The available channel is related to the country or region code. Select the local country or region.

Configure radio frequency parameters on the **Radio Frequency** page and click **Save**.



Tip: Changing configuration requires a reboot and clients will be reconnected.

Radio Frequency Device Group: Default

Country/Region: China (CN)

2.4G Channel Width: Auto

5G Channel Width: Auto

Client Count Limit: 64

Client Count Limit: 512

Kick-off Threshold: Disable -75dBm -50dBm

Kick-off Threshold: Disable -75dBm -50dBm

The settings are valid for only current device

2.4G Channel: Auto

5G Channel: Auto

Transmit Power: Auto Lower Low Medium High

Transmit Power: Auto Lower Low Medium High

Roaming: Low 40% 80% High

Roaming: Low 40% 80% High

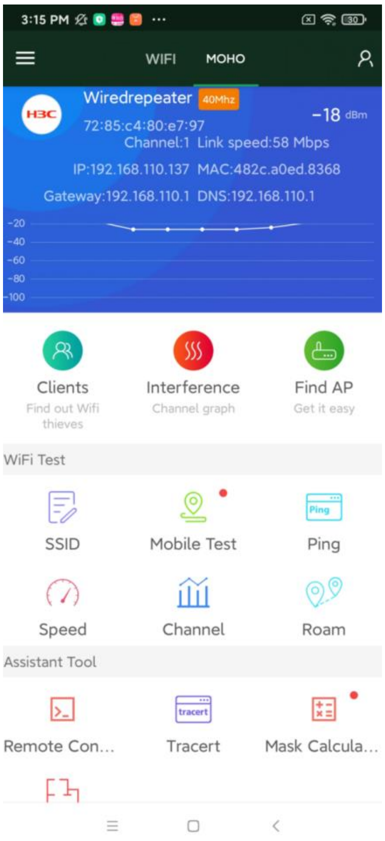
Table 1-2 Description of Radio Frequency Information

Item	Description
Country/Region	Set this parameter according to your location.
2.4G Channel Width/5G Channel Width	Different products and different regions may have different channel width. If the interference is severe, select a lower channel width to avoid network suspension. The AP supports the channel width of 20 MHz and 40 MHz. You are advised to select 20 MHz 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. The AP that is associated with a large number of clients has lower performance, affecting user experience. After the threshold is configured, new clients over the threshold are not allowed to access the Wi-Fi network. You can

Item	Description
	reduce the threshold if bandwidth is required per client. You are advised to keep the default settings unless there are special cases.
Kick-off Threshold	A farther distance where the client is away from the AP indicates a lower signal strength. When the signal strength is lower than the threshold, the client will be disconnected. In this case, select a nearer Wi-Fi signal.
2.4G Channel/5G Channel	In **Auto** mode, the AP will automatically select the best channel according to the environmental interference. You can also select the best channel identified by Wi-Fi Moho or other Wi-Fi scanning App. Click **Save** to make the configuration take effect immediately. More devices in a channel indicate more severe interference.
Transmit Power:	**Lower** means 25%, **Low** means 50%, **Medium** means 75%, and **High** means 100%. A larger value indicates a wider coverage. A greater transmit power indicates a larger coverage and brings more severe interference to surrounding wireless routers. In a high-density scenario, you are advised to set a small transmit power. The **Auto** mode is recommended, indicating automatic adjustment of the transmit power.
Roaming Sensitivity	Roaming sensitivity is the rate at which a device selects and switches to the nearest available AP, offering a better signal. A higher roaming sensitivity level indicates a poorer Wi-Fi coverage. If the device does not roam, select a low roaming sensitivity level. If the device roams, increase the roaming sensitivity level to obtain a better signal. A lower level indicates a greater coverage and less frequent roaming. Advantage: The connection is retained. 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 ended when roaming occurs.

Wireless Optimization Example

Enable Wi-Fi Moho when the SSID is connected and click **Channel** to check the current environmental channel utilization.



Wiredrepeater 40Mhz

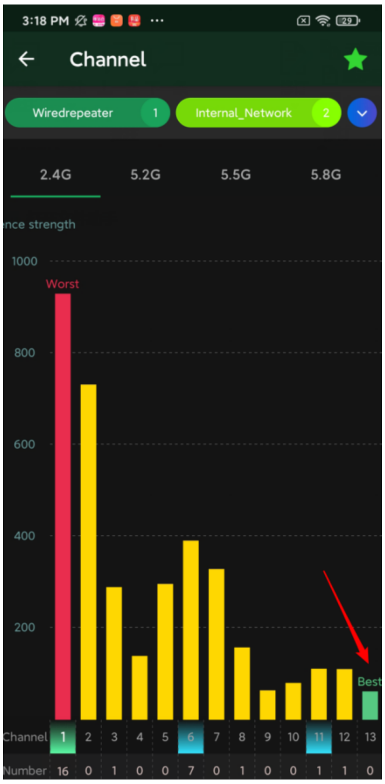
72:85:c4:80:e7:97 −18 dBm

Channel:1 Link speed:58 Mbps

IP:192.168.110.137 MAC:482c.a0ed.8368

Gateway:192.168.110.1 DNS:192.168.110.1

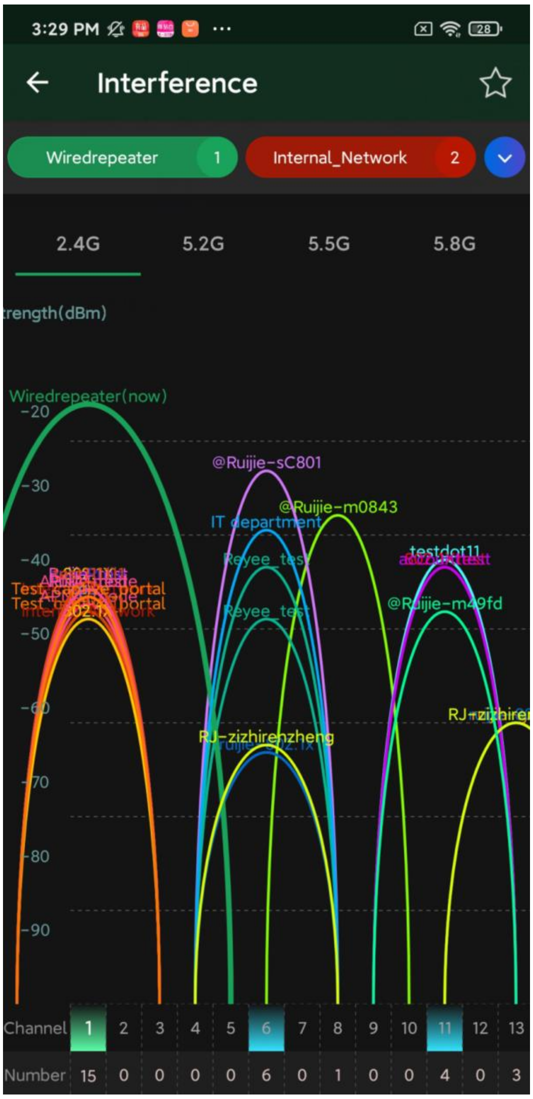
In the following figure, devices are centralized in channel 1 under 2.4 GHz, and channel 13 is the best.



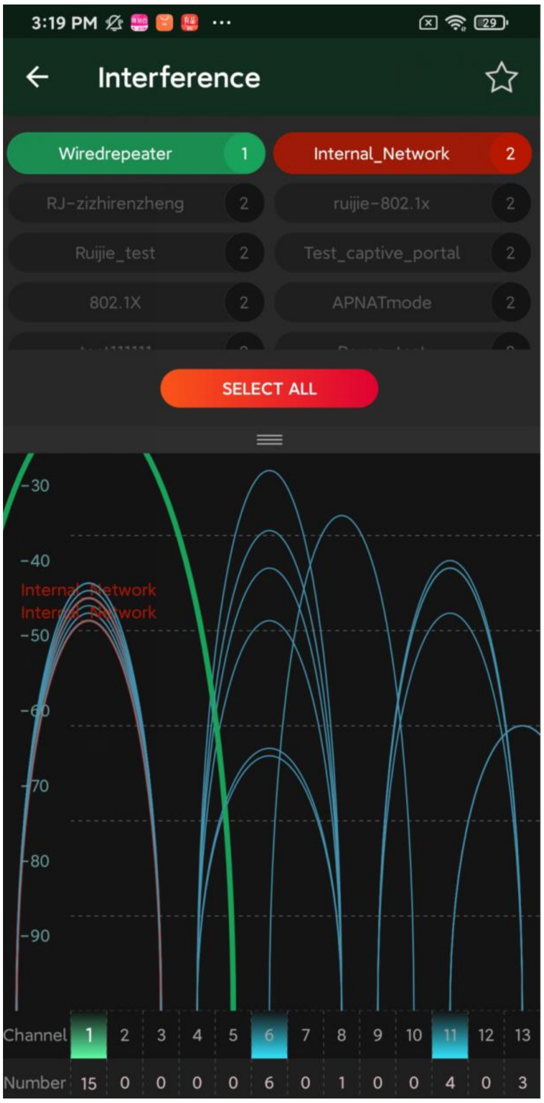
To learn the SSID that belongs to a channel, click **Interference**.

The green color represents the currently connected SSID. You can select the remaining SSIDs on the top to view the channel.

When your wireless speed is slow or during deployment, you can use Wi-Fi Moho to check the configuration. Then select the channel with the least interference.



Channel	1	2	3	4	5	6	7	8	9	10	11	12	13
Number	15	0	0	0	0	6	0	1	0	0	4	0	3



Channel	1	2	3	4	5	6	7	8	9	10	11	12	13
Number	15	0	0	0	0	6	0	1	0	0	4	0	3

4.1.7 Wireless Blacklist/Whitelist Configuration

You can configure the global or SSID-based blacklist and whitelist. The MAC address can be matched exactly or based on the OUI.

- 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 allowed 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.

Configuring a Global Blacklist or Whitelist

(1) Access the **Global Blacklist/Whitelist** page.

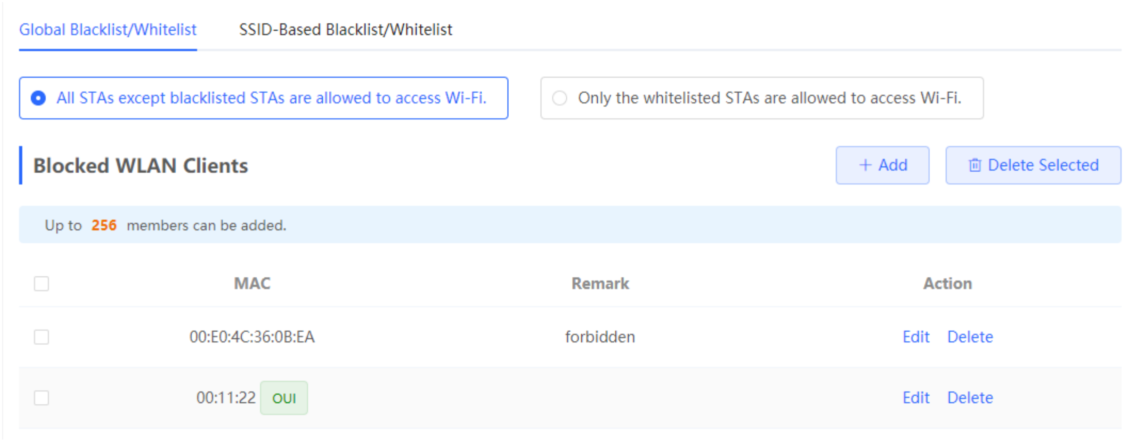
- In SON mode, select **Network** and choose **Clients** > **Blacklist/Whitelist** > **Global Blacklist/Whitelist**.

- In standalone mode, choose **WLAN** > **Blacklist/Whitelist** > **Global Blacklist/Whitelist**.

(2) Select the blacklist or whitelist mode and click **Add** to add a client to a blacklist or whitelist.

⚠ **Note**

An empty whitelist does not take effect. In this case, all clients are allowed to access the Internet.



Global Blacklist/Whitelist SSID-Based Blacklist/Whitelist

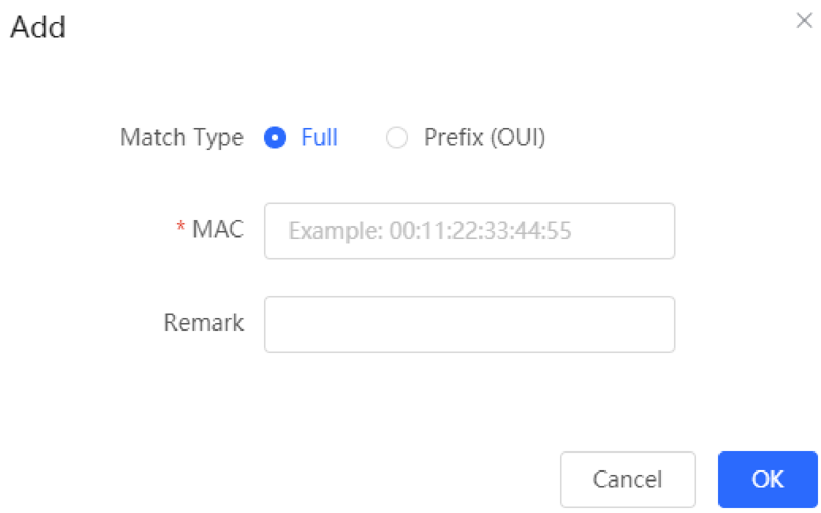
● All STAs except blacklisted STAs are allowed to access Wi-Fi. ○ Only the whitelisted STAs are allowed to access Wi-Fi.

Blocked WLAN Clients

Up to 256 members can be added.

□	MAC	Remark	Action
□	00:E0:4C:36:0B:EA	forbidden	Edit Delete
□	00:11:22 OUI		Edit Delete

(3) In the **Add** window, enter the MAC address and remarks of the target client and click **OK**. If a client is already associated with the AP, its MAC address is displayed automatically. Click the MAC address. All clients in the blacklist are disconnected and prevented from accessing the Wi-Fi network. The global blacklist and whitelist settings take effect on all Wi-Fi networks of the AP.



Add

Match Type ● Full ○ Prefix (OUI)

* MAC Example: 00:11:22:33:44:55

Remark

Configuring an SSID-based Blacklist or Whitelist

⚠ **Note**

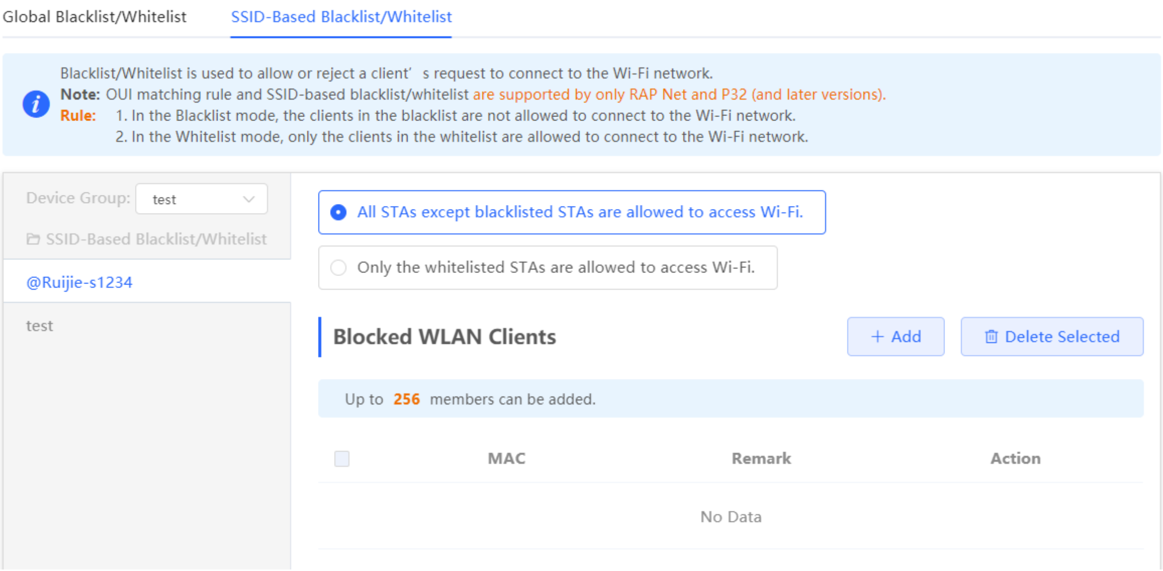
Only RAP Net and P32 (and later versions) support OUI matching and SSID-based blacklist or whitelist.

(1) Access the **SSID-Based Blacklist/Whitelist** page.

- In SON mode, select **Network** and choose **Clients** > **Blacklist/Whitelist** > **SSID-Based Blacklist/Whitelist**.

- ○ In standalone mode, choose **WLAN** > **Blacklist/Whitelist** > **SSID-Based Blacklist/Whitelist**.

(2) Select a target Wi-Fi network from the left column and select the blacklist or whitelist mode

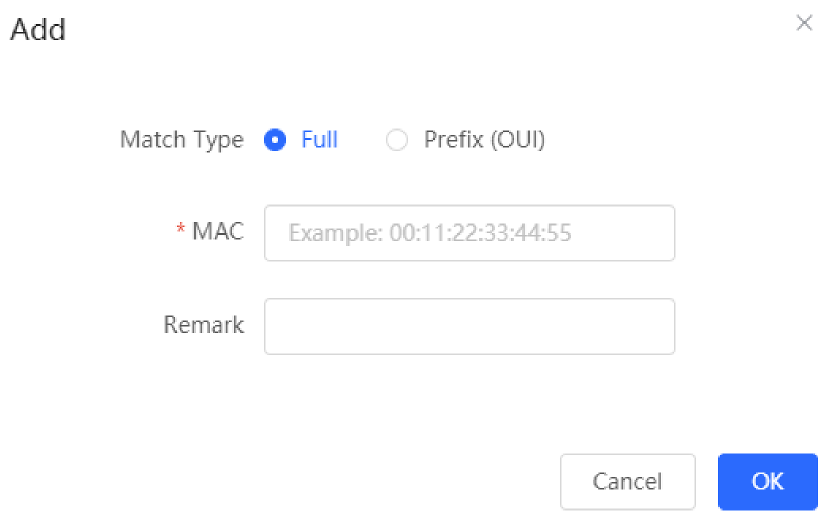


Blacklist/Whitelist is used to allow or reject a client' s request to connect to the Wi-Fi network.
Note: OUI matching rule and SSID-based blacklist/whitelist are supported by only RAP Net and P32 (and later versions).
Rule: 1. In the Blacklist mode, the clients in the blacklist are not allowed to connect 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.

● All STAs except blacklisted STAs are allowed to access Wi-Fi.
○ Only the whitelisted STAs are allowed to access Wi-Fi.

Up to 256 members can be added.

(3) Click **Add** to add a client to a blacklist or whitelist. The SSID-based blacklist or whitelist will restrict or allow the client's access to the specified Wi-Fi network.



Match Type ● Full ○ Prefix (OUI)

* MAC Example: 00:11:22:33:44:55

Remark

4.1.8 AP Group Configuration

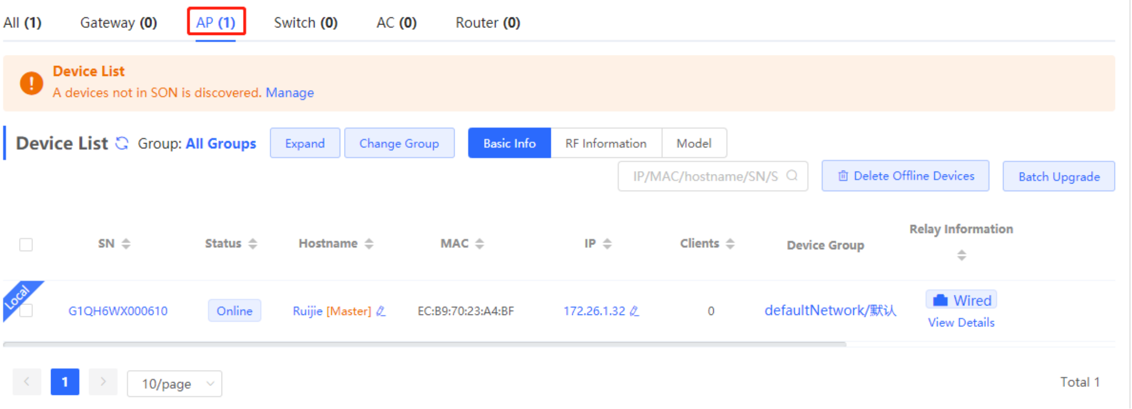
After the SON is enabled, the device can act as the master AP or AC to perform batch configuration and management on the downlink APs in a group. Aps need to be grouped before the configuration is delivered.

⚠ **Note**

If you specify a group when setting up a wireless network, the corresponding configuration will take effect on the wireless devices in the specified group.

In **Network** mode, choose **Devices** > **AP**.

Check information about all APs on the live network, including basic information, RF information, and models. You can click **SN** to configure the device.



All (1) Gateway (0) AP (1) Switch (0) AC (0) Router (0)

Device List
A devices not in SON is discovered. Manage

Device List Group: **All Groups** Expand Change Group Basic Info RF Information Model

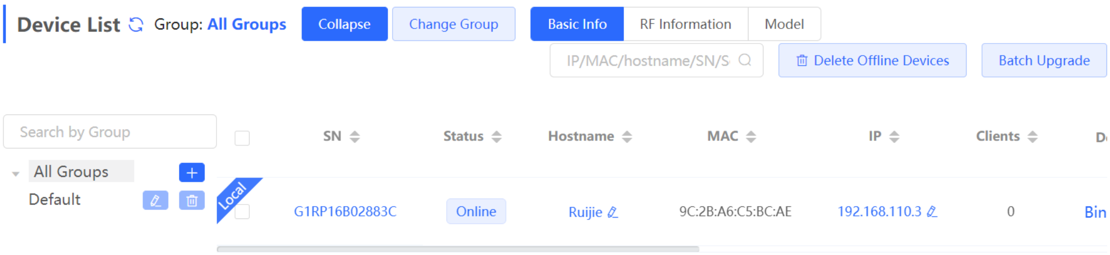
IP/MAC/hostname/SN/S Delete Offline Devices Batch Upgrade

	SN	Status	Hostname	MAC	IP	Clients	Device Group	Relay Information
Local □	G1QH6WX000610	Online	Ruijie [Master]	EC:B9:70:23:A4:BF	172.26.1.32	0	defaultNetwork/默认	Wired View Details

1 10/page Total 1

You can configure AP groups, and APs can be upgraded, deleted, or moved to other groups.

- Click **Expand** to view all groups on the left part of the **AP List** page. A device can only belong to a group. By default, all devices belong to the default group. The default group cannot be deleted and its name cannot be edited.



Device List Group: **All Groups** Collapse Change Group Basic Info RF Information Model

IP/MAC/hostname/SN/S Delete Offline Devices Batch Upgrade

Search by Group

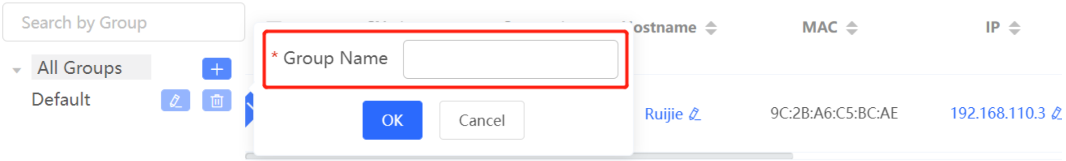
All Groups +
Default

	SN	Status	Hostname	MAC	IP	Clients	D
Local □	G1RP16B02883C	Online	Ruijie	9C:2B:A6:C5:BC:AE	192.168.110.3	0	Bin

After clicking **Expand**, you can add or delete a group, edit the group name, or click the group name.

- Add a group. Up to eight groups can be added.

  Click +, enter the group name, and click **OK** to create a group.



Search by Group

All Groups +
Default

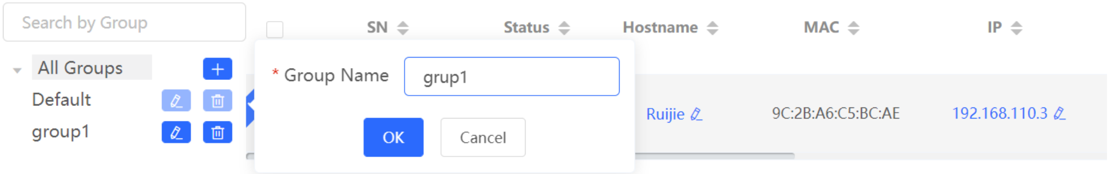
* Group Name

OK Cancel

Hostname	MAC	IP
Ruijie	9C:2B:A6:C5:BC:AE	192.168.110.3

- Edit the group name.

  Click ✎, change the group name, and click **OK**.



Search by Group

All Groups +
Default
group1

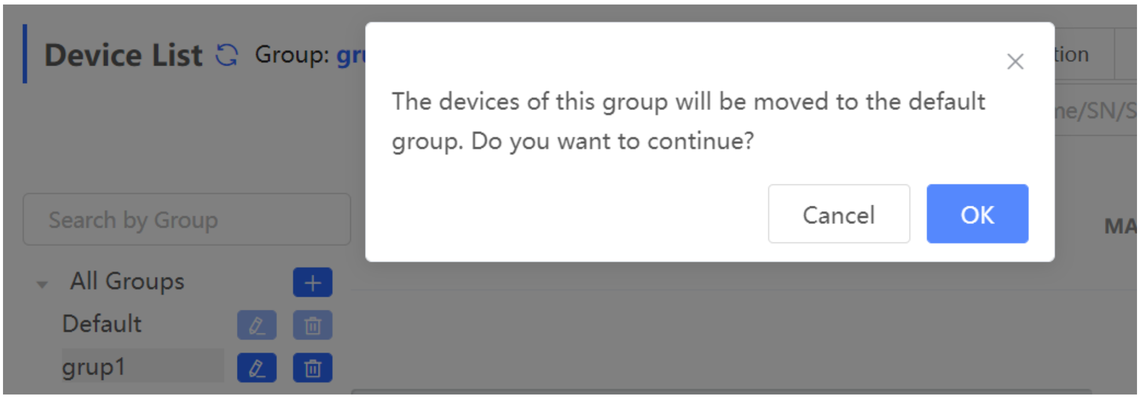
* Group Name grup1

OK Cancel

SN	Status	Hostname	MAC	IP
		Ruijie	9C:2B:A6:C5:BC:AE	192.168.110.3

- Delete a group.

  Click 🗑. Then click **OK** in the displayed window.

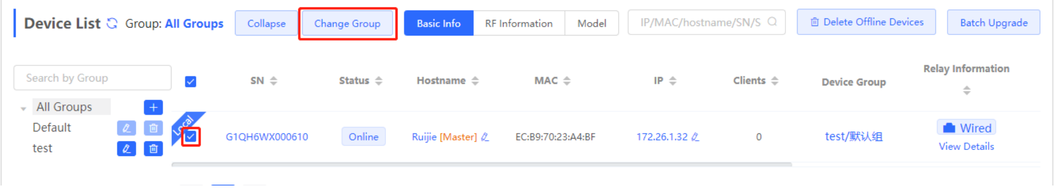


The devices of this group will be moved to the default group. Do you want to continue?

- Click the group name on the left part to view all devices in this group.

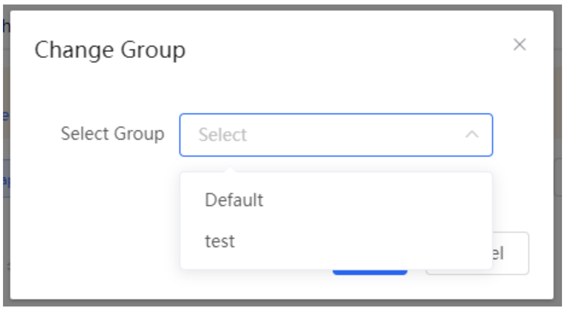
- Change the group that the device belongs to.

a Select one or more offline devices in **Device list** and click **Change Group**.



☑	SN	Status	Hostname	MAC	IP	Clients	Device Group	Relay Information
☑	G1QH6WX000610	Online	Ruijie [Master]	EC:B9:70:23:A4:BF	172.26.1.32	0	test/默认组	Wired View Details

b Select a new group for the target device and click **OK**. Then the device will apply the configuration of this group.



Change Group

Select Group: Select

- Delete offline devices.

  Select one or more offline devices in **Device list** and click **Delete Offline Devices** to remove devices from the list.

- Upgrade devices.

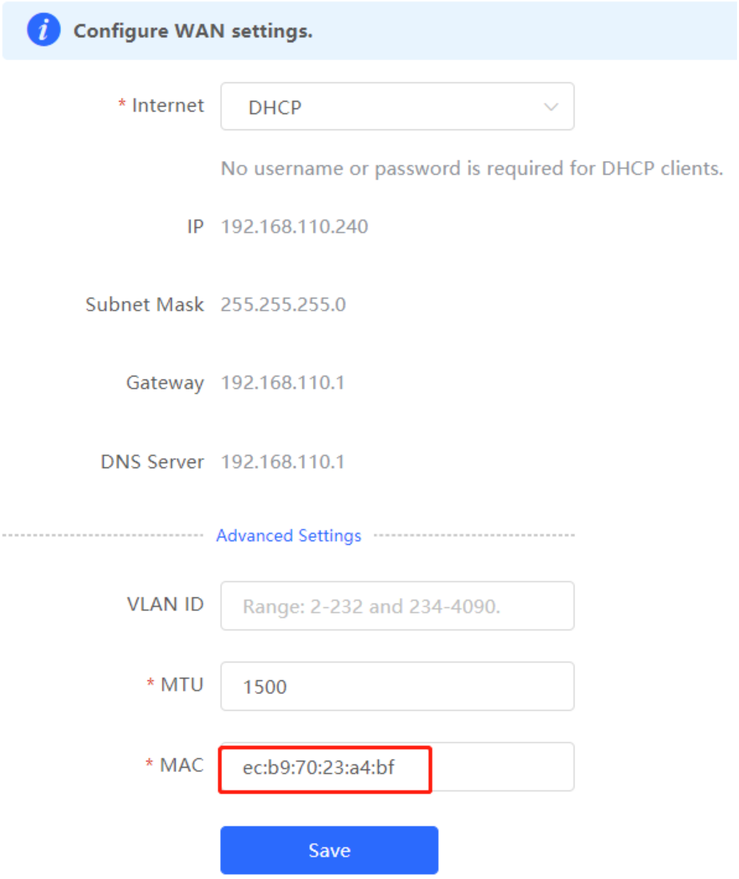
  Select one or more devices in **Device list** and click **Batch Upgrade** to upgrade devices in batches.

4.2 Basic Configuration

4.2.1 WAN Port Configuration

- In SON mode, select **Local Device** and choose **Network** > **WAN**.
- In standalone mode, choose **Network** > **WAN**.

Set parameters of WAN port configuration and click **Save**.



Configure WAN settings.

* Internet: DHCP

No username or password is required for DHCP clients.

IP: 192.168.110.240

Subnet Mask: 255.255.255.0

Gateway: 192.168.110.1

DNS Server: 192.168.110.1

Advanced Settings

VLAN ID: Range: 2-232 and 234-4090.

* MTU: 1500

* MAC: ec:b9:70:23:a4:bf

Internet: Select the Internet access mode after confirming with the ISP. You can select **PPPoE**, **DHCP**, or **Static IP**.

- **PPPoE**: Access the Internet by using the broadband account provided by the ISP.
- **DHCP**: Access the Internet by using the dynamic IP address provided by the ISP.
- **Static IP**: Access the Internet by using a static IP address provided by the ISP.

  When **Internet** is set to **Static IP**, **IP Address**, **Subnet Mask**, **Gateway**, and **DNS Server** are mandatory.

VLAN ID: The value ranges from 2 to 232 and 234 to 4090.

MTU: Maximum transmission unit (MTU) allowed by a WAN port. The default value is 1500 bytes. In some scenarios, large data packets need to be rate-limited or prevented. As a result, the network speed is low or even the network is disconnected. In this case, you can configure a small MTU.

MAC: ISPs may restrict Internet access from devices with unknown MAC addresses to ensure security. In this case, you can change the MAC address of the WAN port.

Note

Changing the MAC address will disconnect the device from the network. You need to reconnect the device to the network or restart the device. Therefore, exercise caution when performing this operation. You do not need to change the default MAC address unless in special cases.

4.2.2 LAN Port Configuration

VLAN Settings of a Port

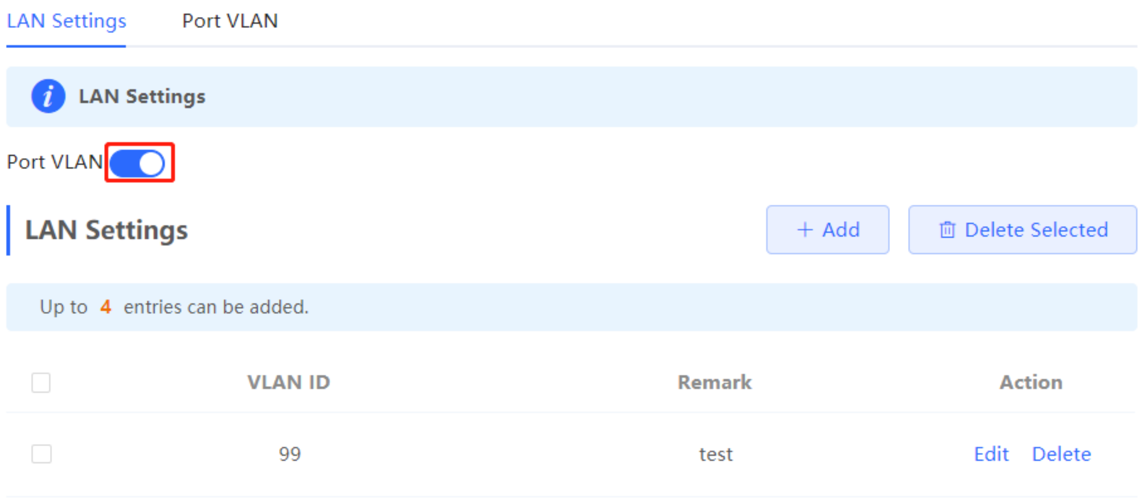
Note

The VLAN of a port can be configured only when the device works in AP mode.

(1) Access the **LAN** page.

- In SON mode, select **Local Device** mode and choose **Network** > **LAN**.
- In standalone mode, choose **Network** > **LAN**.

(2) On the **LAN Settings** tab page, enable **Port VLAN**, and click **OK** in the displayed dialog box.



LAN Settings | Port VLAN

LAN Settings

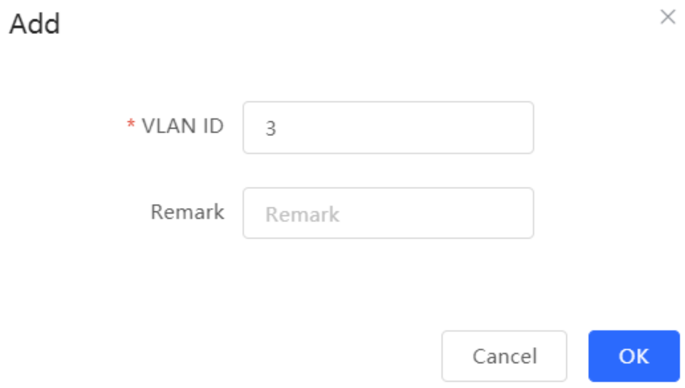
Port VLAN ●

LAN Settings   + Add   Delete Selected

Up to 4 entries can be added.

□	VLAN ID	Remark	Action
□	99	test	Edit Delete

(3) Click **Add**. Enter the VLAN ID and description, and click **OK** to create a VLAN. The added VLAN is used to set the VLAN to which a port belongs.



Add ×

* VLAN ID: 3

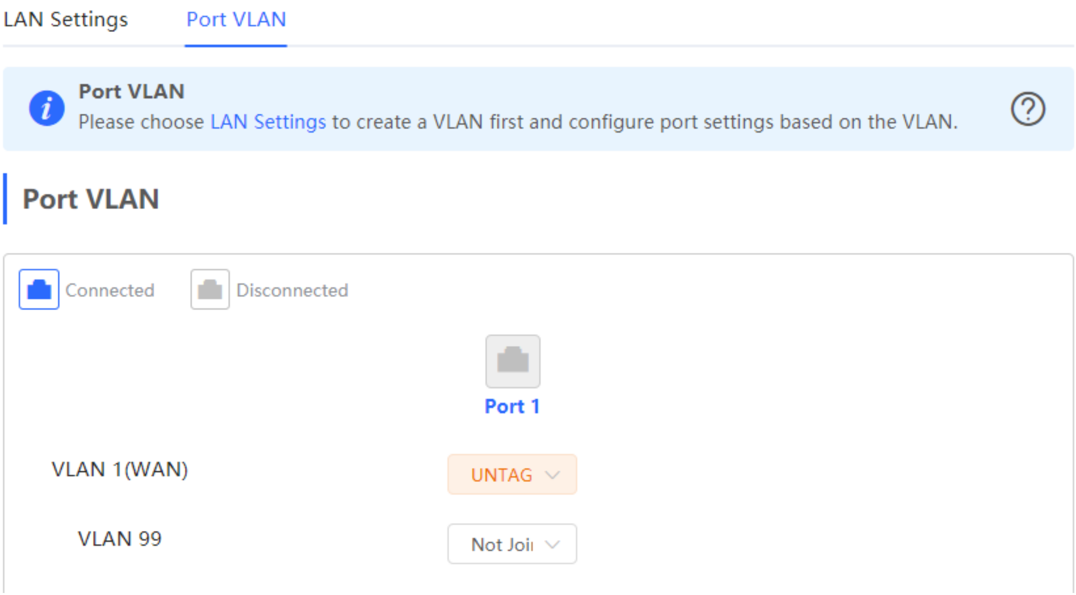
Remark: Remark

Cancel   OK

(4) Switch to the **Port VLAN** tab page and configure VLANs for the port. Select the mapping between a VLAN and the port from the drop-down list box, and click **Save**.

- **UNTAG**: Configure the VLAN as the native VLAN of the port. That is, when receiving a packet from this VLAN, the port removes the VLAN tag from the packet and forwards the packet. When receiving an untagged packet, the port adds the VLAN tag to the packet and forwards the packet through the VLAN. Only one VLAN can be configured as an untagged VLAN on each port.

- **TAG**: Configure the VLAN as an allowed VLAN of the port. The VLAN cannot be the native VLAN. That is, VLAN packets carry the original VLAN tag when being forwarded by the port.
- **Not Join**: Configure the port not to allow packets from this VLAN to pass through. For example, if port 2 is not added to VLAN 10 and VLAN 20, port 2 does not receive or send packets from or to VLAN 10 and VLAN 20.



Port VLAN
Please choose LAN Settings to create a VLAN first and configure port settings based on the VLAN.

Port VLAN

VLAN 1(WAN) UNTAG

VLAN 99 Not Joi

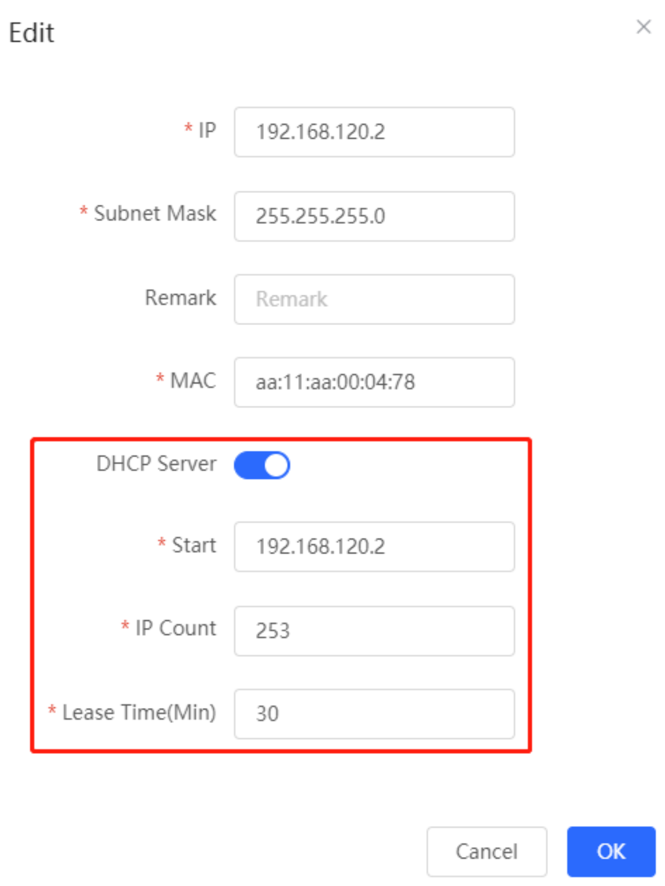
DHCP Server Configuration

Note

- This function is only available in router mode.
- If the DHCP server function is disabled on all devices of a network, clients cannot automatically obtain IP addresses. You need to enable the DHCP server function on one device or manually configure a static IP address for each client for Internet access.

- In SON mode, select **Local Device** and choose **Network** > **LAN**.
- In standalone mode, choose **Network** > **LAN**.

On the **LAN Settings** tab page, click **ADD**, set parameters of the DHCP server, and click **OK**.



Edit

* IP: 192.168.120.2

* Subnet Mask: 255.255.255.0

Remark: Remark

* MAC: aa:11:aa:00:04:78

DHCP Server: ●

* Start: 192.168.120.2

* IP Count: 253

* Lease Time(Min): 30

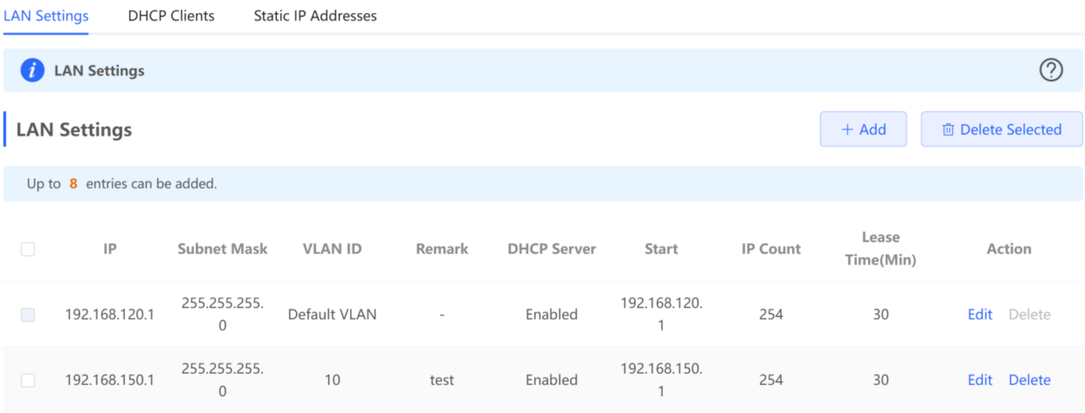
DHCP server: The DHCP server function is enabled by default in router mode. You are advised to enable the function if the device is used as the sole router on a network. When multiple routers are connected to the upper-layer device through LAN ports, disable this function.

Start: Enter the start IP address of the DHCP address pool. A client obtains an IP address from the address pool. If all the addresses in the address pool are used up, no IP address can be obtained from the address pool.

IP Count: Enter the number IP addresses in the address pool.

Lease Time(Min): Enter the address lease time. When a client is connected, the leased IP address is automatically renewed. If a leased IP address is not renewed due to client disconnection or network instability, the IP address will be reclaimed after the lease time expires. After the client connection is restored, the client can request an IP address again. The default lease time is 30 minutes.

After the DHCP server is configured, you can check the configuration on the LAN Settings tab page. You can click **Edit** to change the DHCP server configuration.

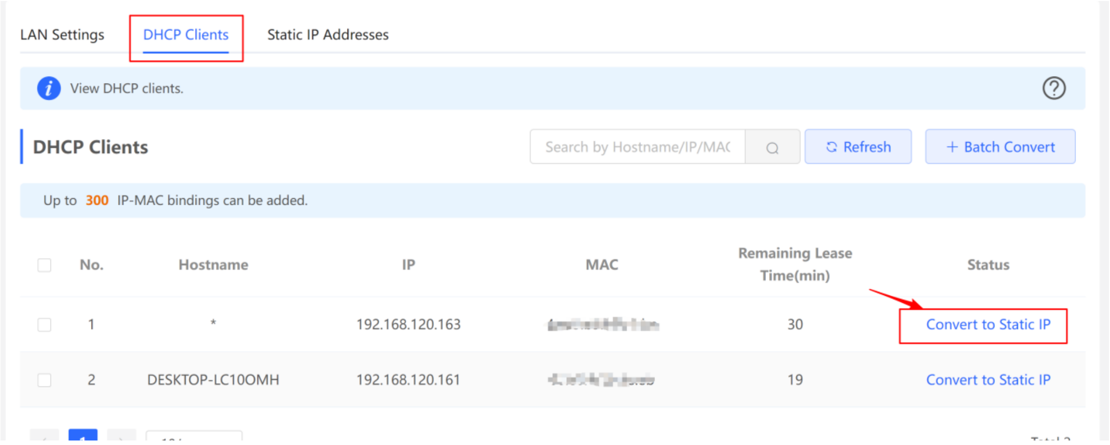


LAN Settings

Up to 8 entries can be added.

□	IP	Subnet Mask	VLAN ID	Remark	DHCP Server	Start	IP Count	Lease Time(Min)	Action
□	192.168.120.1	255.255.255.0	Default VLAN	-	Enabled	192.168.120.1	254	30	Edit Delete
□	192.168.150.1	255.255.255.0	10	test	Enabled	192.168.150.1	254	30	Edit Delete

Switch to the **DHCP Clients** tab page to check information about an online client. Click **Convert to Static IP**. Then, the static IP address will be obtained each time the client connects to the network.



View DHCP clients.

Up to 300 IP-MAC bindings can be added.

□	No.	Hostname	IP	MAC	Remaining Lease Time(min)	Status
□	1	*	192.168.120.163	[redacted]	30	Convert to Static IP
□	2	DESKTOP-LC10OMH	192.168.120.161	[redacted]	19	Convert to Static IP

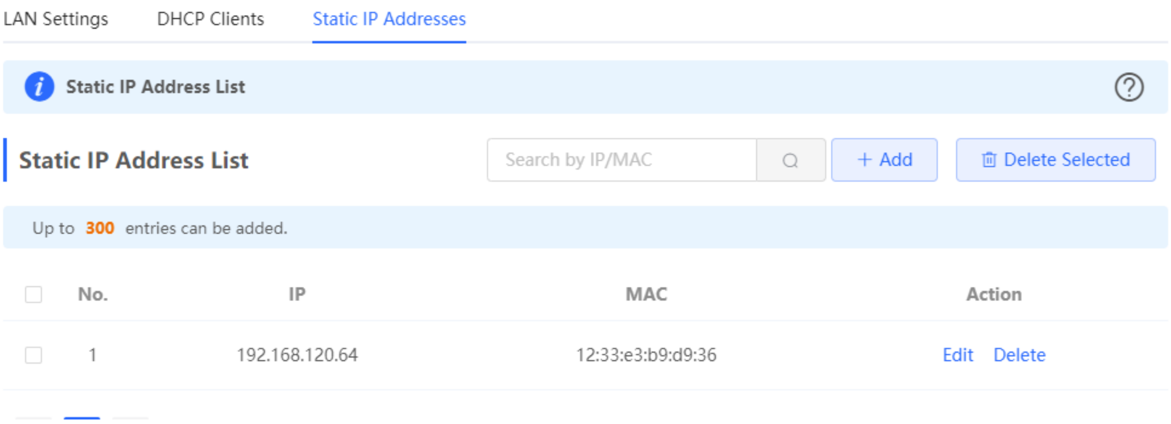
Binding Static IP Addresses

⚠ **Note**

This function is only available in router mode.

- In SON mode, select **Local Device** and choose **Network** > **LAN** > **Static IP Addresses**.
- In standalone mode, choose **Network** > **LAN** > **Static IP Addresses**.

Click **Add**. In the displayed dialog box of static IP address bindings, enter the MAC address and IP address of the client to be bound, and click **OK**. After a static IP address is bound, the bound IP address will be obtained each time the client connects to the network. You can click **Edit** to modify IP address and MAC address.



Static IP Address List

Up to 300 entries can be added.

□	No.	IP	MAC	Action
□	1	192.168.120.64	12:33:e3:b9:d9:36	Edit Delete

4.3 Advanced Configuration

4.3.1 ARP List

Note

This function is not supported when the device works in AP mode.

ARP List displays the mapping relationship between IP addresses and MAC addresses.

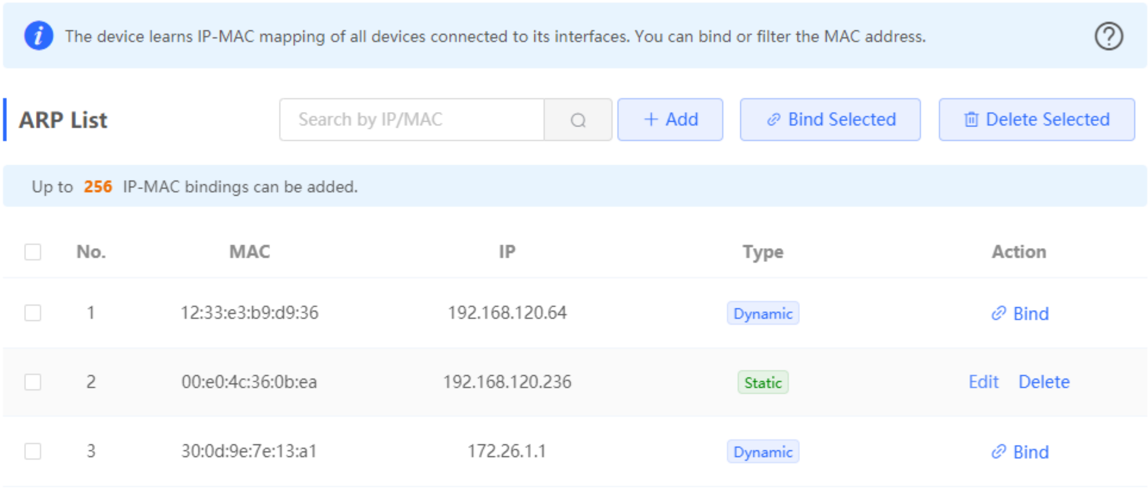
The device learns the IP and MAC addresses of network devices connected to ports of the device and generates ARP entries. You can bind ARP mappings to improve network security.

- In SON mode, select **Local Device** and choose **Advanced** > **Local DNS**.
- In standalone mode, choose **Advanced** > **Local DNS**.

In **Local Device** mode, choose **Security** > **ARP List**.

ARP mappings can be bound in two ways:

- Select a dynamic ARP entry in the ARP list and click **Bind**. You can select multiple entries to be bound at one time and click **Bind Selected** to bind them. To remove the binding between a static IP address and a MAC address, click **Delete** in the **Action** column.

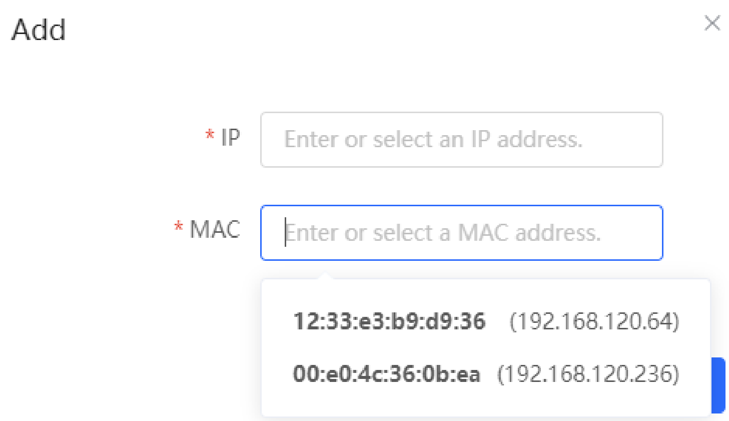


The device learns IP-MAC mapping of all devices connected to its interfaces. You can bind or filter the MAC address.

Up to 256 IP-MAC bindings can be added.

□	No.	MAC	IP	Type	Action
□	1	12:33:e3:b9:d9:36	192.168.120.64	Dynamic	Bind
□	2	00:e0:4c:36:0b:ea	192.168.120.236	Static	Edit Delete
□	3	30:0d:9e:7e:13:a1	172.26.1.1	Dynamic	Bind

- Click **Add**, enter the IP address and MAC address to be bound, and click **OK**. The input box can display existing address mappings in the ARP list. You can click a mapping to automatically enter the address mapping.



Add

* IP Enter or select an IP address.

* MAC Enter or select a MAC address.

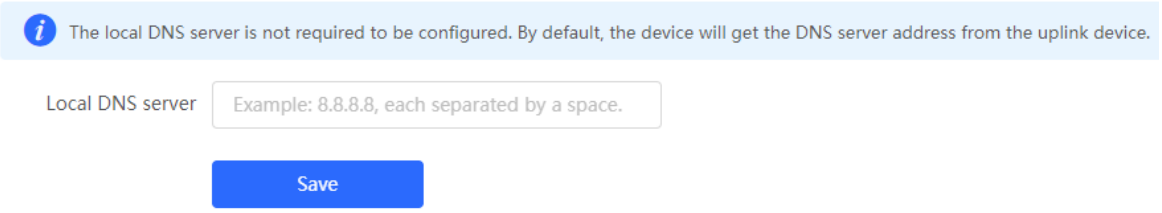
12:33:e3:b9:d9:36 (192.168.120.64)

00:e0:4c:36:0b:ea (192.168.120.236)

4.3.2 Local DNS

- In SON mode, select **Local Device** and choose **Advanced** > **Local DNS**.
- In standalone mode, choose **Advanced** > **Local DNS**.

Enter the IP address of the DNS server and click **Save**. The local DNS server is optional. The device obtains the DNS server address from the connected uplink device by default. The default configuration is recommended. The available DNS service varies by region. You can consult the local ISP.



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

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

4.3.3 PoE Configuration

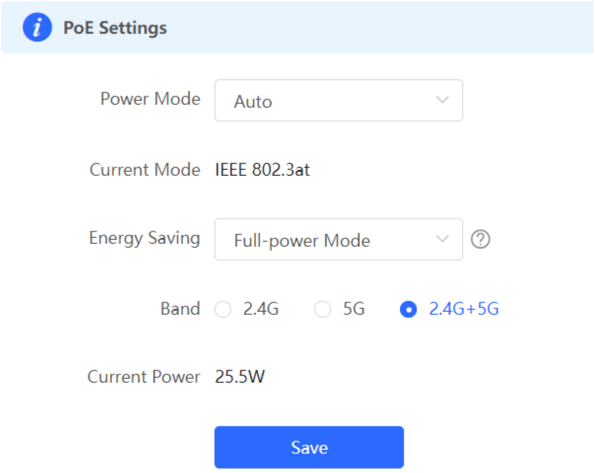
Note

Only some devices support this function.

The **PoE Settings** page allows you to configure the PoE mode.

- In SON mode, select **Local Device** mode and choose **Advanced** > **PoE Settings**.
- In standalone mode, choose **Advanced** > **PoE Settings**.

Set parameters on the **PoE Settings** page and click **Save**.



PoE Settings

Power Mode: Auto

Current Mode: IEEE 802.3at

Energy Saving: Full-power Mode

Band: ○ 2.4G ○ 5G ● 2.4G+5G

Current Power: 25.5W

Power Mode: indicates the power mode for the AP to accept power over PoE. In AF mode, the maximum power supported by the device is 15.4 W. In AT mode, the maximum power is 30 W according to the IEEE 802.3at standard. By default, the device automatically negotiates with the power sourcing equipment (PSE) about the power mode. The default configuration is recommended.

Current Mode: indicates the current PoE mode.

Energy Saving: indicates the energy saving mode. In rate-limiting mode, the device is rate-limited. In flow-limiting mode, the spatial stream in each band is halved.

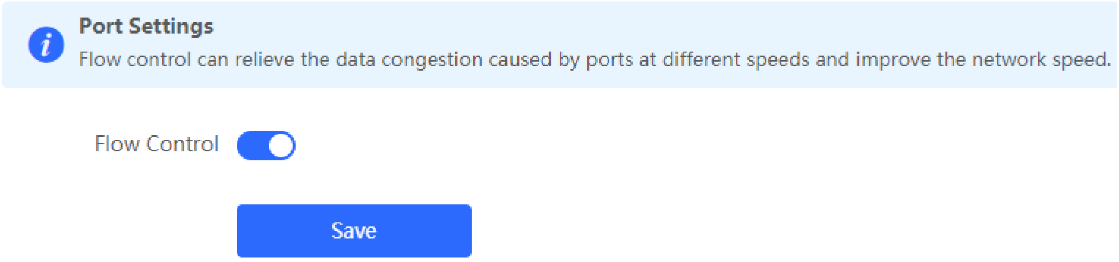
Band: indicates the band type.

Current Power: indicates the current power.

4.3.4 Port Flow Control Configuration

- In SON mode, select **Local Device** mode and choose **Advanced** > **Port Settings**.
- In standalone mode, choose **Advanced** > **Port Settings**.

When the LAN ports work at different rates, data congestion may occur. This slows down the network speed and affects the Internet access experience. Enabling port flow control can help mitigate this problem.



Port Settings

Flow control can relieve the data congestion caused by ports at different speeds and improve the network speed.

Flow Control: On

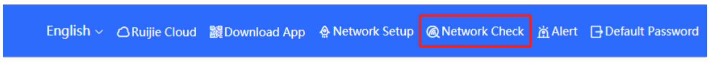
4.4 Operation and Maintenance

4.4.1 Network Check

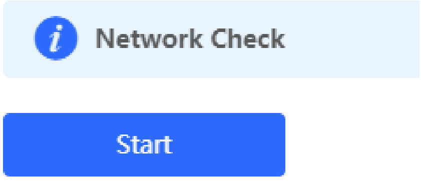
When a network error occurs, perform **Network Check** to identify the fault and take the suggested action.

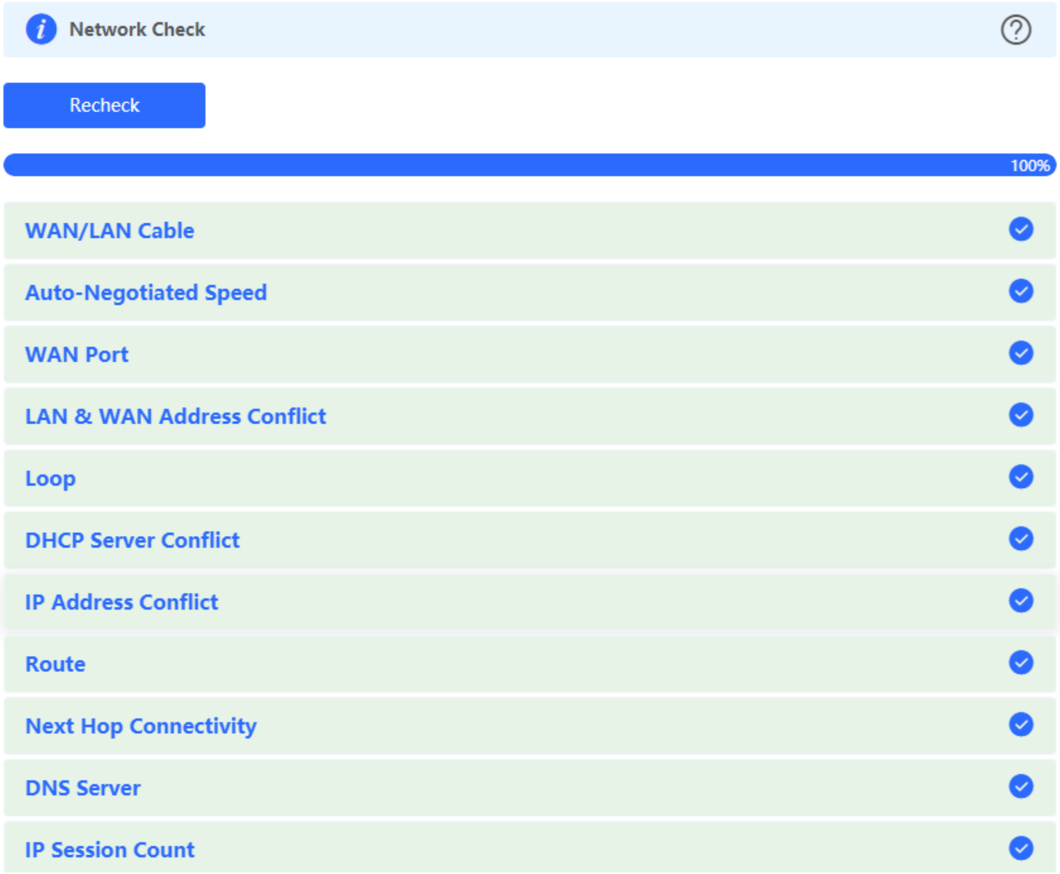
(1) Go to the **Network Check** page.

- In SON mode, select **Local Device**. Then click in the navigation bar or choose **Diagnostics** > **Network Check**.
- In standalone mode, click in the navigation bar or choose **Diagnostics** > **Network Check**.



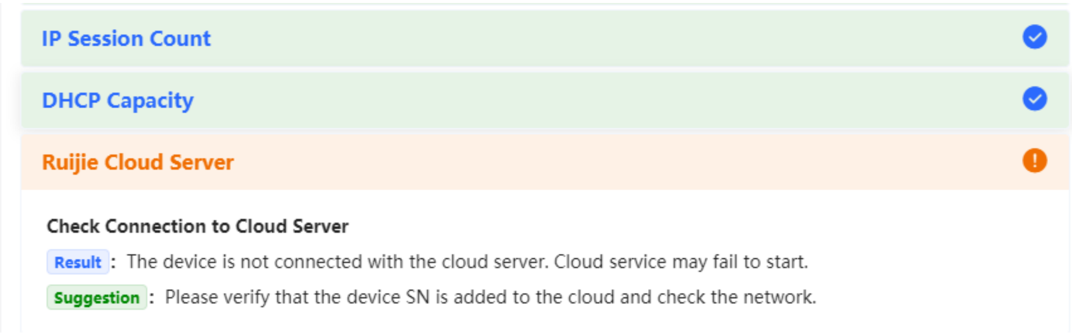
(2) Click **Start** to perform the network check and check the result.





- WAN/LAN Cable ✓
- Auto-Negotiated Speed ✓
- WAN Port ✓
- LAN & WAN Address Conflict ✓
- Loop ✓
- DHCP Server Conflict ✓
- IP Address Conflict ✓
- Route ✓
- Next Hop Connectivity ✓
- DNS Server ✓
- IP Session Count ✓

After performing network check, you will find the check result and suggested action.



IP Session Count ✓

DHCP Capacity ✓

Ruijie Cloud Server !

Check Connection to Cloud Server

Result: The device is not connected with the cloud server. Cloud service may fail to start.

Suggestion: Please verify that the device SN is added to the cloud and check the network.

4.4.2 Alarms

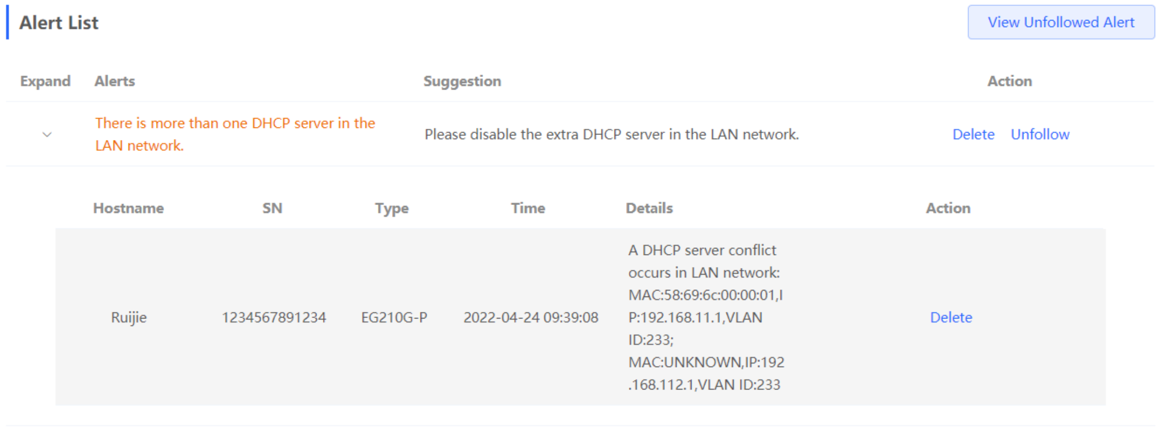
Choose **Network** (**Diagnostics**) > **Alerts**.

The **Alerts** page displays possible problems in the network environment and on the device. You can delete or unfollow alarms.

Note

- After you click **Delete**, the alarm will reappear if the warning occurs. After clicking **Unfollow**, the alarm will never appear.
- When a type of alarms is unfollowed, the device will not discover and process all alarms of this type in a timely manner. Therefore, exercise caution when performing this operation.

All types of alarms are followed by default.



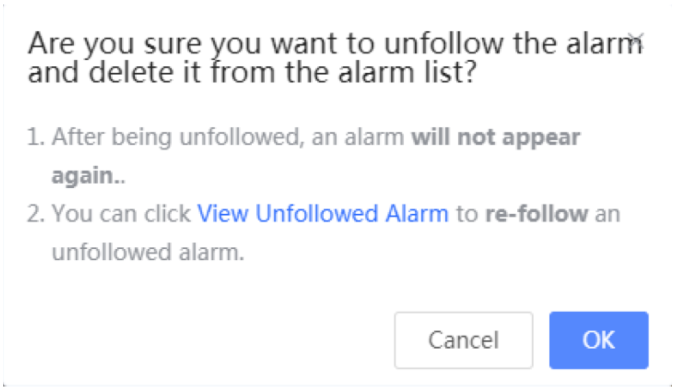
Alert List

Expand	Alerts	Suggestion	Action
⌄	There is more than one DHCP server in the LAN network.	Please disable the extra DHCP server in the LAN network.	Delete Unfollow

Hostname	SN	Type	Time	Details	Action
Ruijie	1234567891234	EG210G-P	2022-04-24 09:39:08	A DHCP server conflict occurs in LAN network: MAC:58:69:6c:00:00:01,IP:192.168.11.1,VLAN ID:233; MAC:UNKNOWN,IP:192.168.112.1,VLAN ID:233	Delete

- Unfollow an alarm.

  Click **Unfollow** in the **Action** column. Then click **OK** in the displayed window to unfollow this type of alarms.

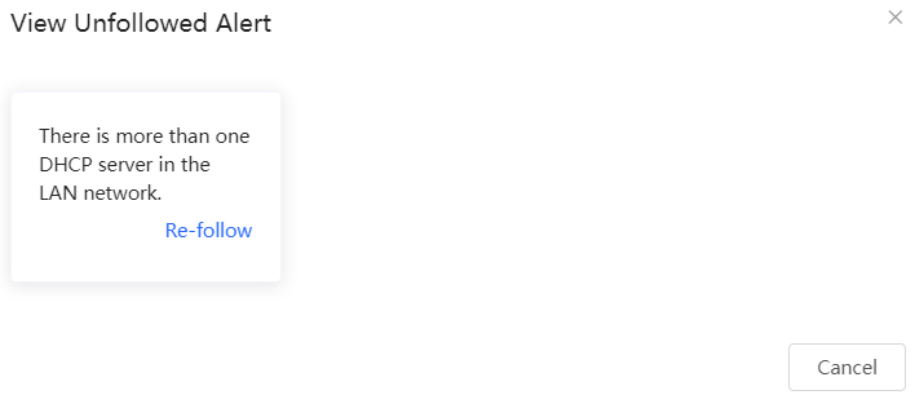


Are you sure you want to unfollow the alarm and delete it from the alarm list?

1. After being unfollowed, an alarm **will not appear again..**
2. You can click View Unfollowed Alarm to **re-follow** an unfollowed alarm.

- Re-follow the alarm.

  Click **View Unfollowed Alert** to view the unfollowed alarm. Then click **Re-follow** to follow the alarm again in the displayed window.



View Unfollowed Alert

There is more than one DHCP server in the LAN network.

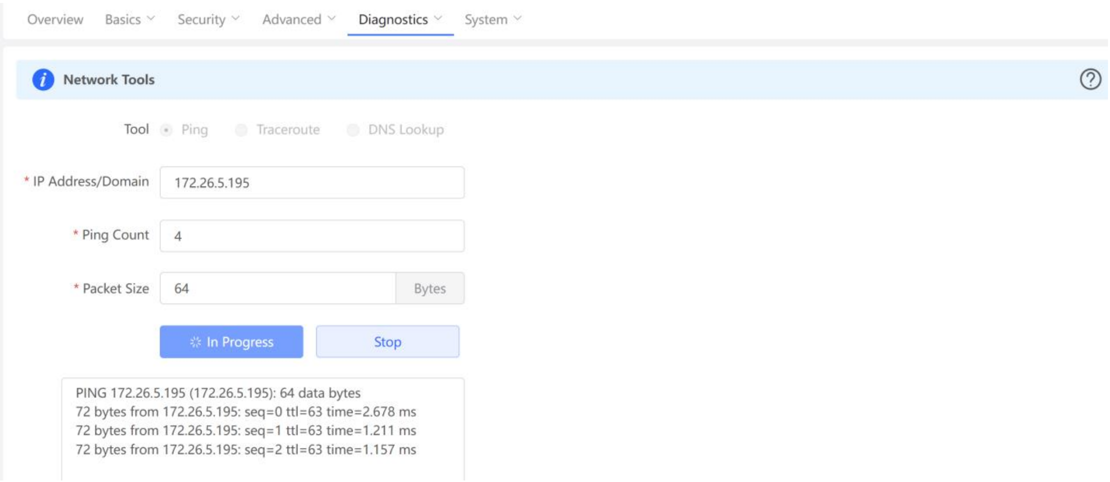
4.4.3 Network Tools

- In SON mode, select **Local Device** and choose **Diagnostics** > **Network Tools**.
- In standalone mode, choose **Diagnostics** > **Network Tools**.

Network tools includes **Ping**, **Traceroute**, and **DNS Lookup**.

- **Ping**: Test whether the IP address or domain name is reachable.

  Enter the IP address or URL and click **Start** to test the connectivity between the AP and the IP address or URL. The message "Ping failed" indicates that the IP address or URL is inaccessible.



Tool ● Ping ○ Traceroute ○ DNS Lookup

* IP Address/Domain: 172.26.5.195

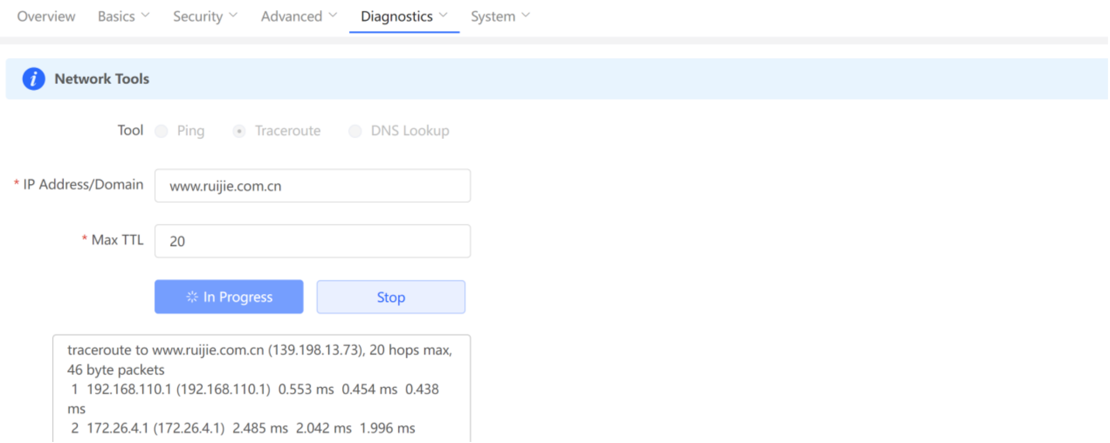
* Ping Count: 4

* Packet Size: 64 Bytes

```
PING 172.26.5.195 (172.26.5.195): 64 data bytes
72 bytes from 172.26.5.195: seq=0 ttl=63 time=2.678 ms
72 bytes from 172.26.5.195: seq=1 ttl=63 time=1.211 ms
72 bytes from 172.26.5.195: seq=2 ttl=63 time=1.157 ms
```

- **Traceroute**: Count the number of hops, displaying communication links from one point to another point and the time taken for each hop.

  Enter the IP address or URL, fill in **MAX TTL**, and click **Start** to display the network path to a specific IP address or URL.



Tool ○ Ping ● Traceroute ○ DNS Lookup

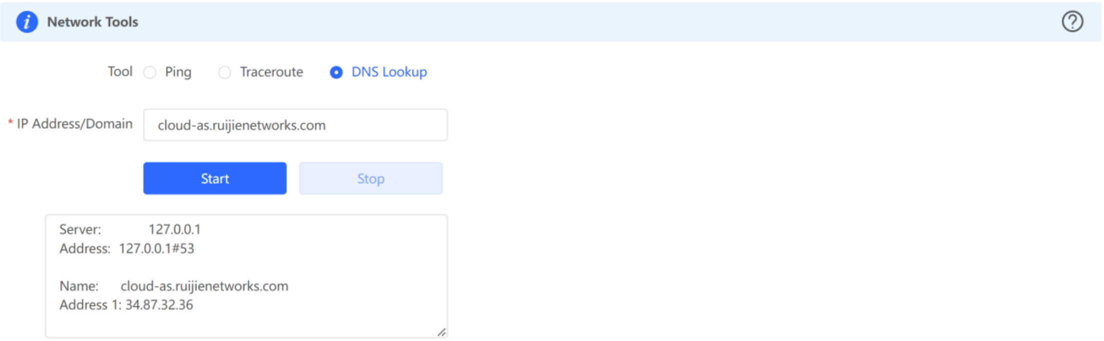
* IP Address/Domain: www.ruijie.com.cn

* Max TTL: 20

```
traceroute to www.ruijie.com.cn (139.198.13.73), 20 hops max,
46 byte packets
 1  192.168.110.1 (192.168.110.1)  0.553 ms  0.454 ms  0.438
ms
 2  172.26.4.1 (172.26.4.1)  2.485 ms  2.042 ms  1.996 ms
```

- **DNS Lookup**: Display the DNS server address used to resolve a URL.

  Enter the IP address or URL and click **Start**.



Tool ○ Ping ○ Traceroute ● DNS Lookup

* IP Address/Domain: cloud-as.ruijienetworks.com

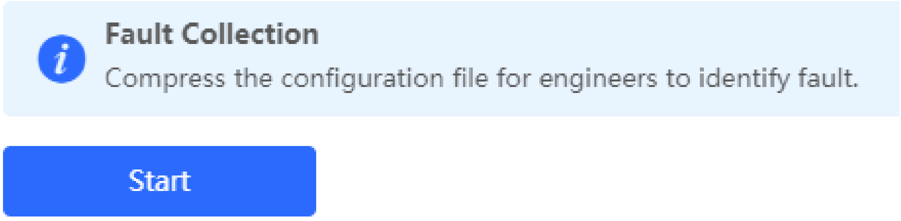
```
Server:        127.0.0.1
Address:  127.0.0.1#53

Name:     cloud-as.ruijienetworks.com
Address 1: 34.87.32.36
```

4.4.4 Fault Collection

- In SON mode, select **Local Device** and choose **Diagnostics** > **Fault Collection**.
- In standalone mode, choose **Diagnostics** > **Fault Collection**.

When an unknown fault occurs on the device, you can collect fault information on this page. Click **Start** to collect fault information and compress it into a file for engineers to identify the fault.



Fault Collection

Compress the configuration file for engineers to identify fault.

4.4.5 System

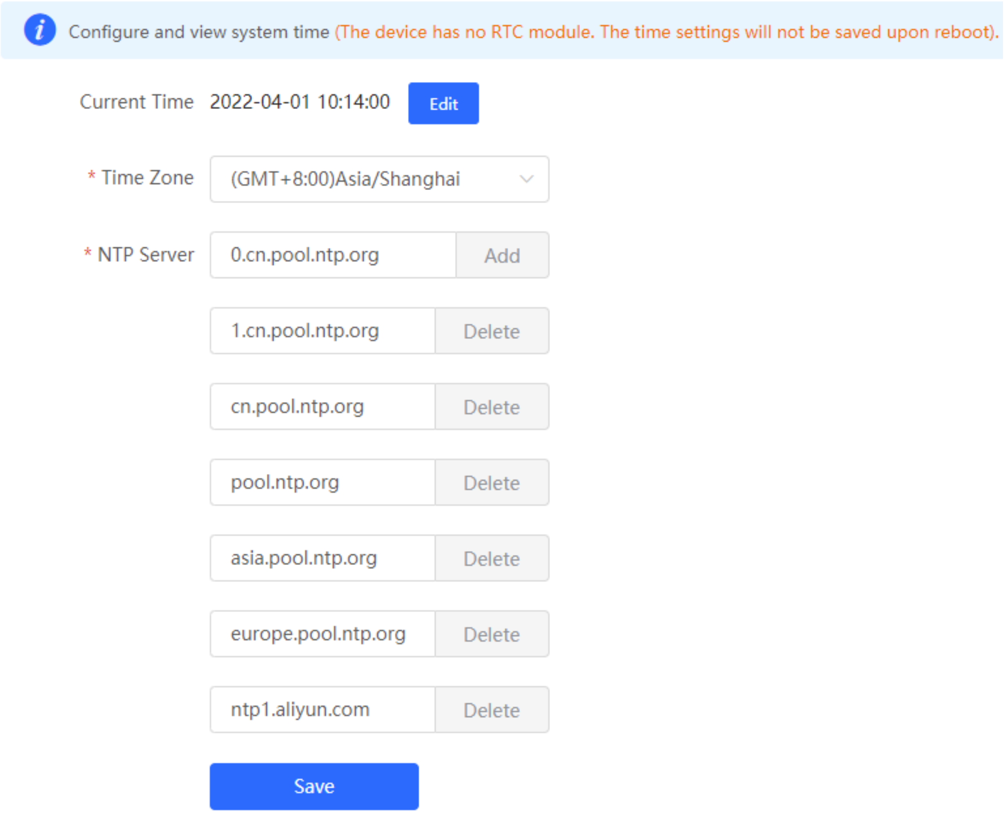
Setting the System Time

Note

In SON mode, the system time of all devices on the network will be changed synchronously.

Choose **System** > **System Time**.

Set parameters of the system time and click **Save**.



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

Current Time 2022-04-01 10:14:00

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

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

1.cn.pool.ntp.org

cn.pool.ntp.org

pool.ntp.org

asia.pool.ntp.org

europe.pool.ntp.org

ntp1.aliyun.com

Current 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 the time is still incorrect, click **Edit** to manually set the time.
- If the time is not set or synchronized with a time server, the device will start with the manufacturing time.

Time Zone: Select the time zone based on your address.

NTP Server: The device supports Network Time Protocol (NTP) servers. By default, multiple servers serve as the backup of each other. You can add or delete the local server as required.

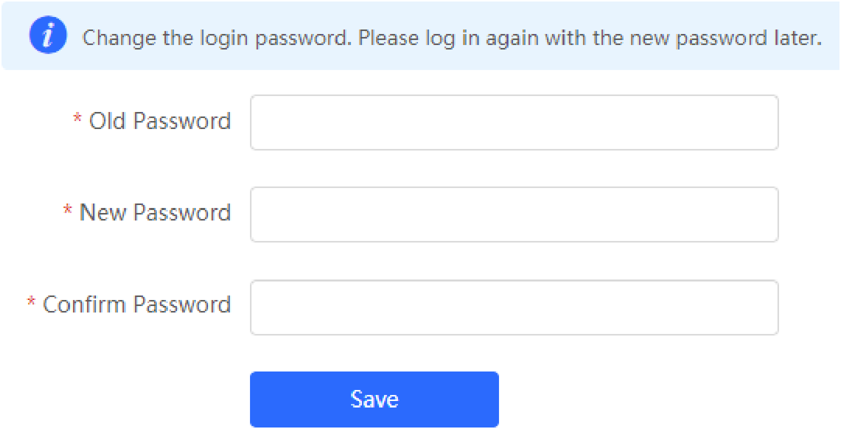
Setting the Login Password

Choose **System** > **Login** > **Login Password**.

Enter the old password and new password. After saving the configuration, use the new password to log in.

⚠ **Note**

In SON mode, the login password of all devices on the network will be changed synchronously.



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

* Old Password

* New Password

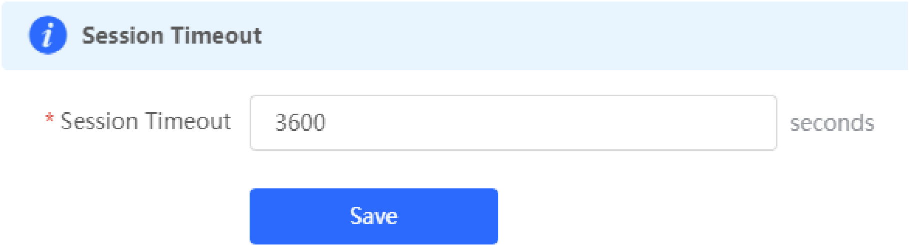
* Confirm Password

Setting the Timeout of the Login Page

If no operation is performed on the web page within a period of time, a session is automatically disconnected. To perform operations again, enter the password to log in. The default timeout is 3600 seconds, that is, 1 hour.

- In SON mode, select **Local Device** mode and choose **System** > **Login** > **Session Timeout**.
- In standalone mode, choose **System** > **Login** > **Session Timeout**.

Set the timeout of the login page and click **Save**. The value ranges from 600 to 7200 seconds.

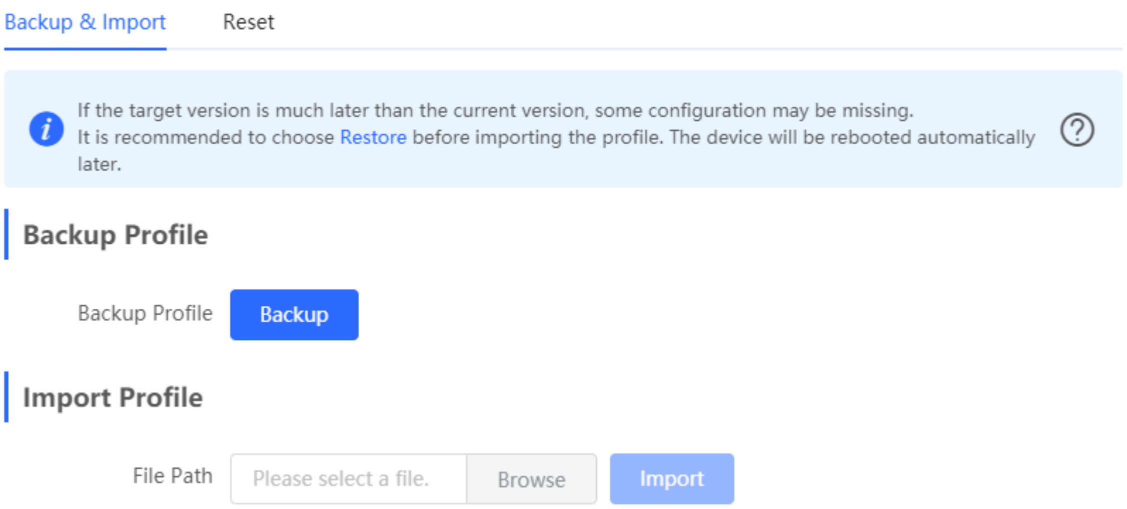


Session Timeout

* Session Timeout 3600 seconds

Backup/Import Configuration

Choose **System** > **Management** > **Backup & Import**.



Backup & Import   Reset

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

Backup Profile

Backup Profile: Backup

Import Profile

File Path: Please select a file. Browse Import

You can import a configuration file to AP or export the current configuration of the AP.

- Configuration backup: Click **Backup** to download a configuration file locally.
- Configuration import: Click **Browse**, select a backup file on the local PC, and click **Import** to import the configuration file. The AP will restart.

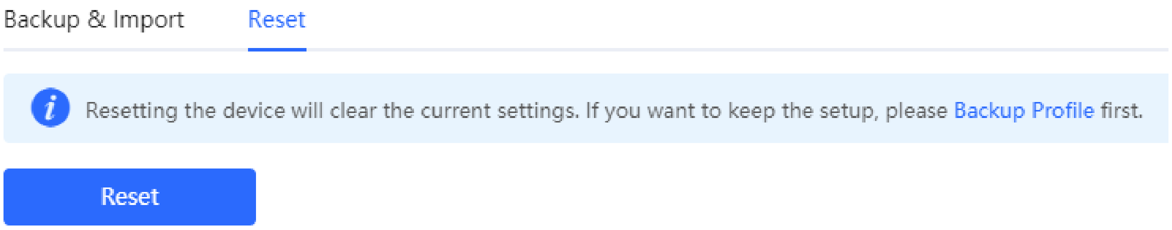
  If the target version is much later than the current version, some configuration may be missing.

  You are advised to restore the settings before importing the configuration. The AP will restart automatically if you restore it.

Reset

Choose **System** > **Management** > **Reset**.

Click **Reset** to restore the device to the factory settings.



Backup & Import   Reset

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

Reset

Note

The operation will clear all configuration of the current device. To retain the current configuration, first back up the configuration (see 0Backup/Import Configuration). Therefore, exercise caution when performing this operation.

Upgrade

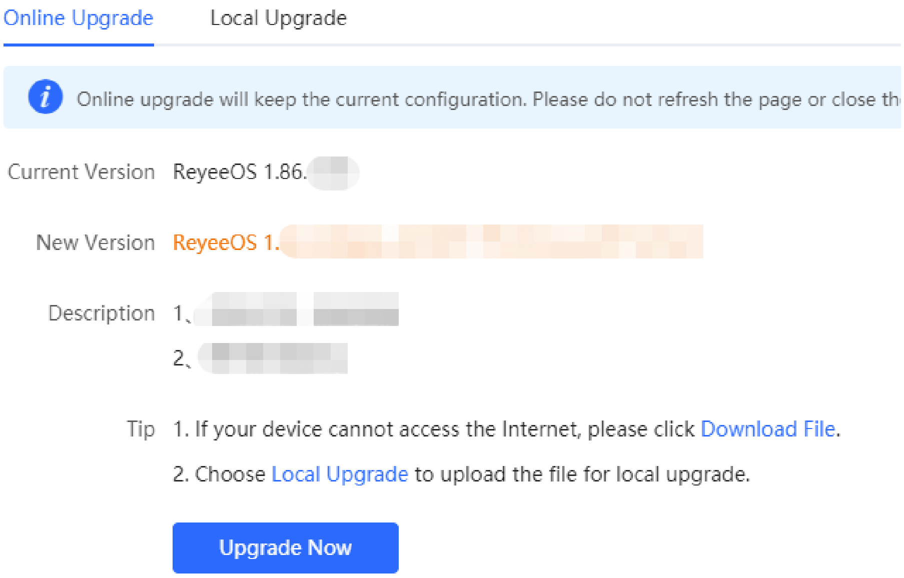
There are two modes: **Online Upgrade** and **Local Upgrade**.

Online Upgrade

- In SON mode, select **Local Device** mode and choose **System** > **Upgrade** > **Online Upgrade**.
- In standalone mode, choose **System** > **Upgrade** > **Online Upgrade**.

You can view the current system version.

- If a new version is available, you can click **Upgrade Now** for an upgrade. The upgrade operation does not affect the current configuration, but the AP will restart after being upgraded successfully. Do not refresh the page or close the browser during the upgrade. You are redirected to the login page automatically after the upgrade.



Online upgrade will keep the current configuration. Please do not refresh the page or close th

Current Version ReyeeOS 1.86.[redacted]

New Version ReyeeOS 1.[redacted]

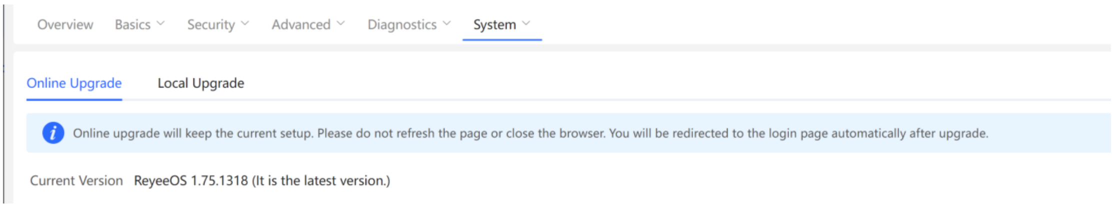
Description 1、[redacted]

2、[redacted]

Tip 1. If your device cannot access the Internet, please click Download File.

2. Choose Local Upgrade to upload the file for local upgrade.

- If there is no new version, the system displays a message indicating that the current version is the latest.



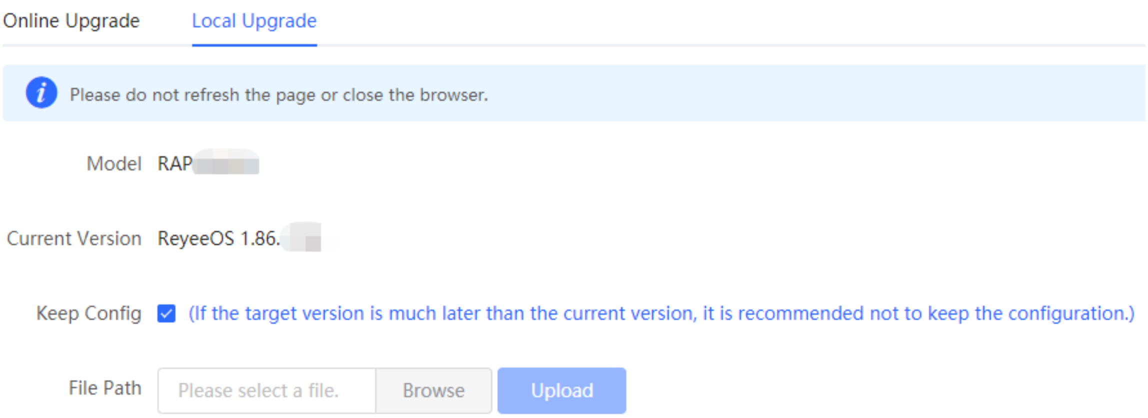
Online upgrade will keep the current setup. Please do not refresh the page or close the browser. You will be redirected to the login page automatically after upgrade.

Current Version ReyeeOS 1.75.1318 (It is the latest version.)

Local Upgrade

- In SON mode, select **Local Device** mode and choose **System** > **Upgrade** > **Local Upgrade**.
- In standalone mode, choose **System** > **Upgrade** > **Local Upgrade**.

You can view the current software version, hardware version, and device model. To upgrade the device with the configuration retained, check **Keep Config**. Click **Browse**, select an upgrade package on the local PC, and click **Upload** to upload the file. After the file is uploaded successfully, the system displays upgrade package information and asks for the upgrade. Click **OK** to start the upgrade.



Please do not refresh the page or close the browser.

Model RAP[redacted]

Current Version ReyeeOS 1.86.[redacted]

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

File Path Please select a file.

Restarting the Device

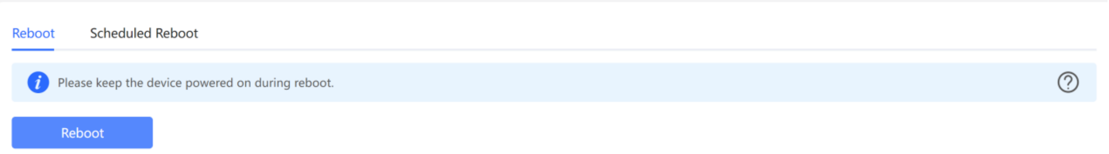
- In SON mode, select **Local Device** mode and choose **System** > **Reboot**.
- In standalone mode, choose **System** > **Reboot**.

You can restart the device immediately or set a scheduled restart.

- Restart the device immediately.

  On the **Reboot** tab page, click **Reboot** and click **OK** in the confirmation box. **Reboot** allows you to restart the device immediately.

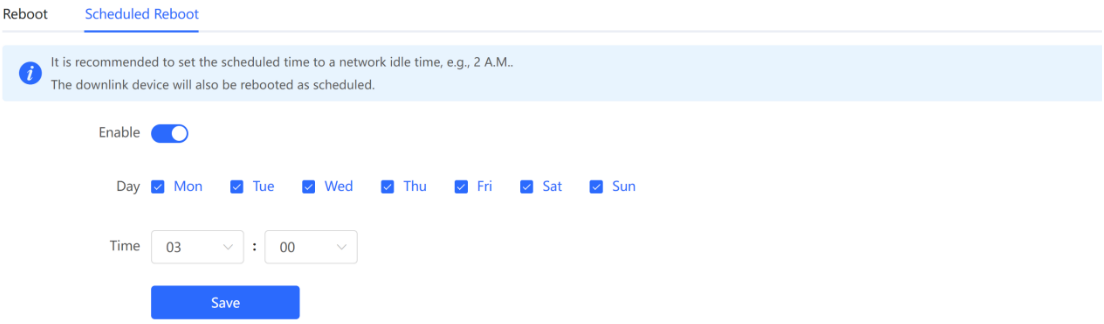
  The device is restarted, and you need to log into the Eweb management system again after the restart. Do not refresh the page or close the browser during the restart. After the device is successfully restarted, you will be redirected to the login page of the Eweb management system.



Please keep the device powered on during reboot.

- Set a scheduled reboot.

  Switch to the **Scheduled Reboot** tab page, enable scheduled reboot, set the scheduled day and time, and click **Save**.



It is recommended to set the scheduled time to a network idle time, e.g., 2 A.M..
The downlink device will also be rebooted as scheduled.

Enable: on

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

Time 03 : 00

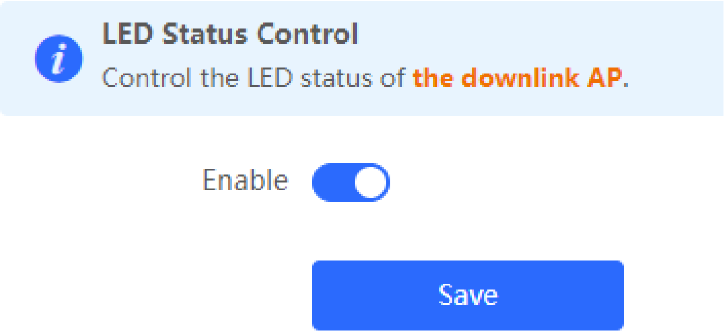
AP LED

Note

The **LED Status Control** function is not supported in the standalone mode (the SON is not enabled).

In **Network** mode, choose **Network** > **LED**.

Enable or disable the LED of all downlink APs on the network and click **Save**.



LED Status Control

Control the LED status of **the downlink AP**.

Enable ●

5 Advanced Solution Guide

5.1 Reyee Flow Control Solution

5.1.1 Application Scenario

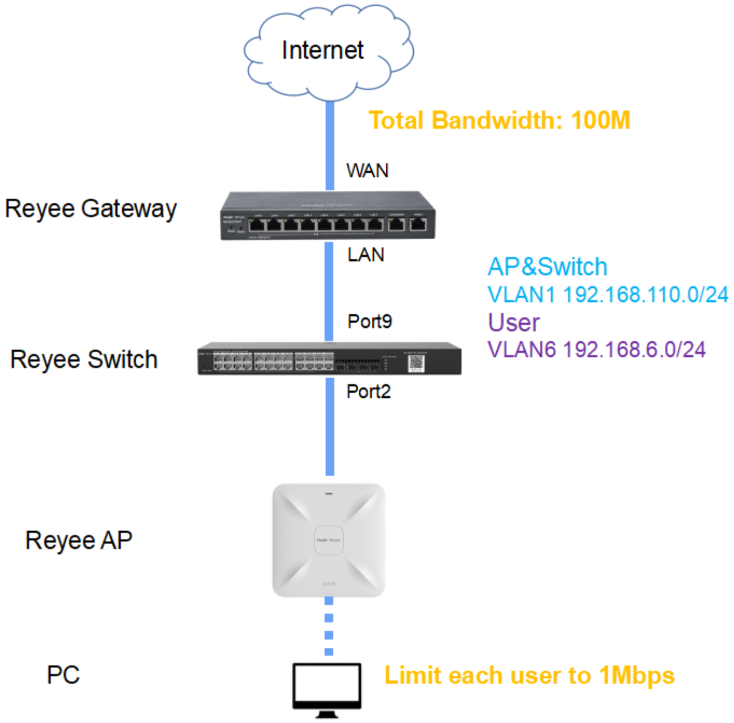
Flow control is used for setting the rate limit of download and upload for the clients, and protects the network bandwidth from being occupied by some clients.

5.1.2 Configuration Case

Requirement

The total bandwidth of the EG egress needs to be limited to 100 Mbit/s and the rate of each user in VLAN 6 to 1 Mbit/s.

Network Topology



Network Description:

The EG works as a DHCP server to assign IP addresses to users, Reyee AP, and Reyee switch.

The AP and switch obtain IP addresses on network segment 192.168.110.0/24 in VLAN 1 for Internet access.

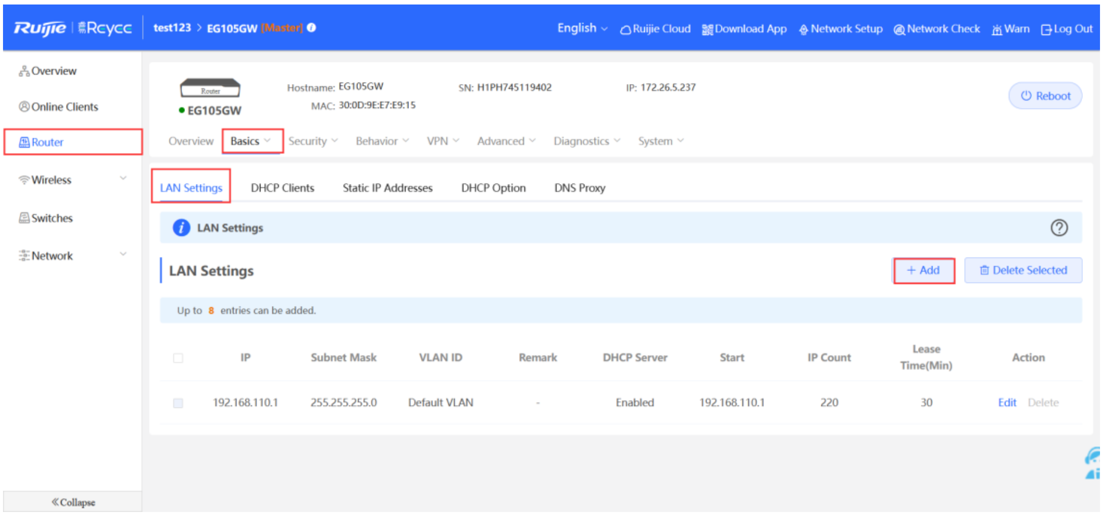
Users obtain IP addresses on network segment 192.168.6.0/24 in VLAN 6 for Internet access.

Configuration Steps

The configuration steps include configuring the basic network, enabling smart flow control, and configuring a customized policy.

(1) Configure the basic network.

a Choose **Router** > **Basics** > **LAN** > **LAN Settings** > **Add**. Configure LAN settings and a DHCP pool for VLAN 1 and VLAN 6 on the EG.



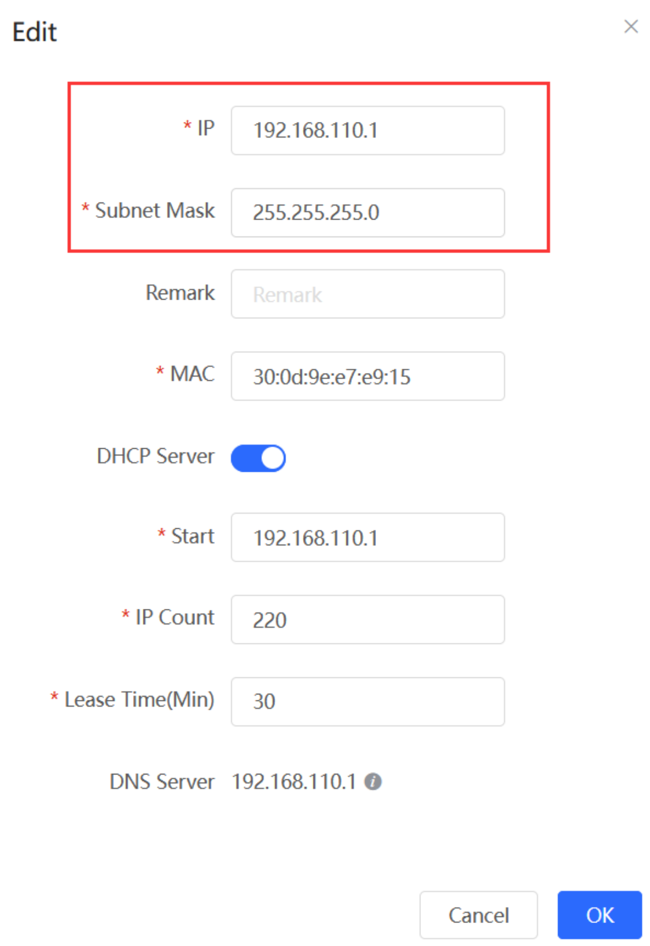
Hostname: EG105GW
MAC: 30:0D:9E:E7:E9:15
SN: H1PH745119402
IP: 172.26.5.237

LAN Settings

LAN Settings

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

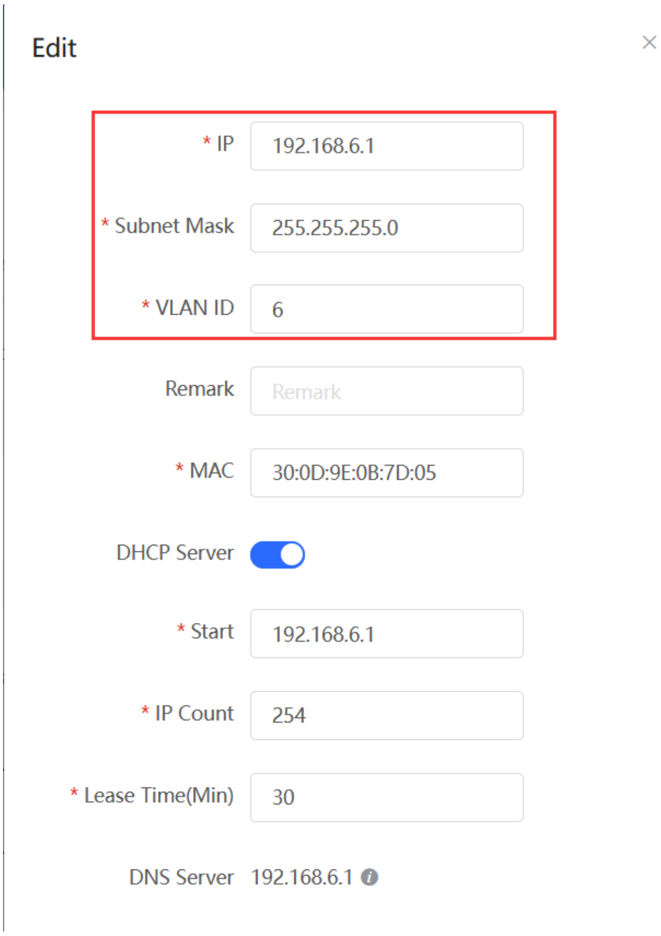
DHCP Server: ●

* Start: 192.168.110.1

* IP Count: 220

* Lease Time(Min): 30

DNS Server: 192.168.110.1



Edit

* IP: 192.168.6.1

* Subnet Mask: 255.255.255.0

* VLAN ID: 6

Remark: Remark

* MAC: 30:0D:9E:0B:7D:05

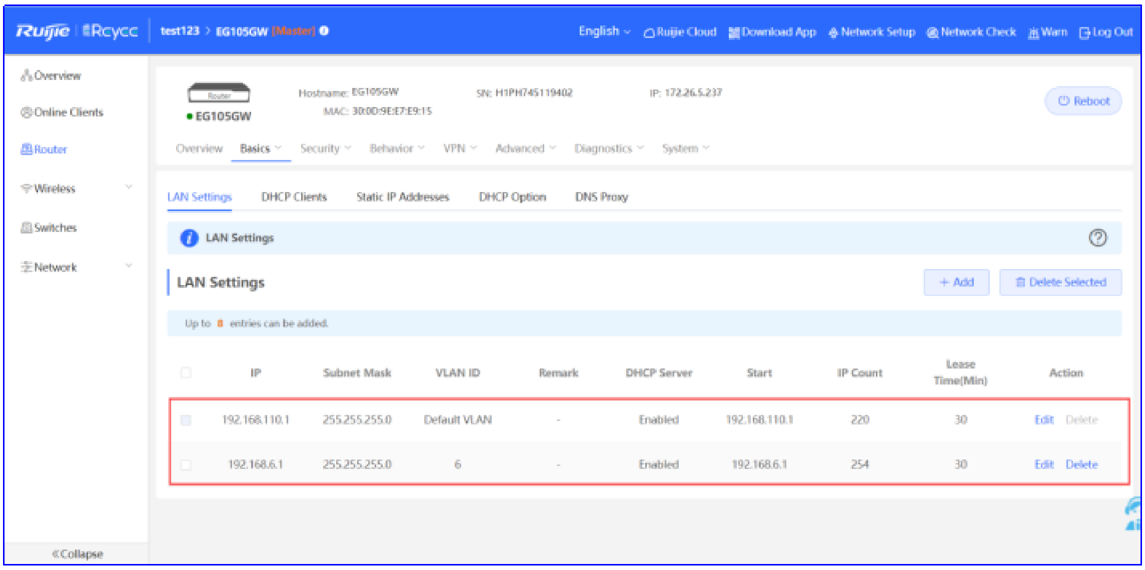
DHCP Server: ●

* Start: 192.168.6.1

* IP Count: 254

* Lease Time(Min): 30

DNS Server: 192.168.6.1



EG105GW Hostname: EG105GW MAC: 30:0D:9E:E7:E9:15 SN: H1PH745119402 IP: 172.26.5.237

LAN Settings

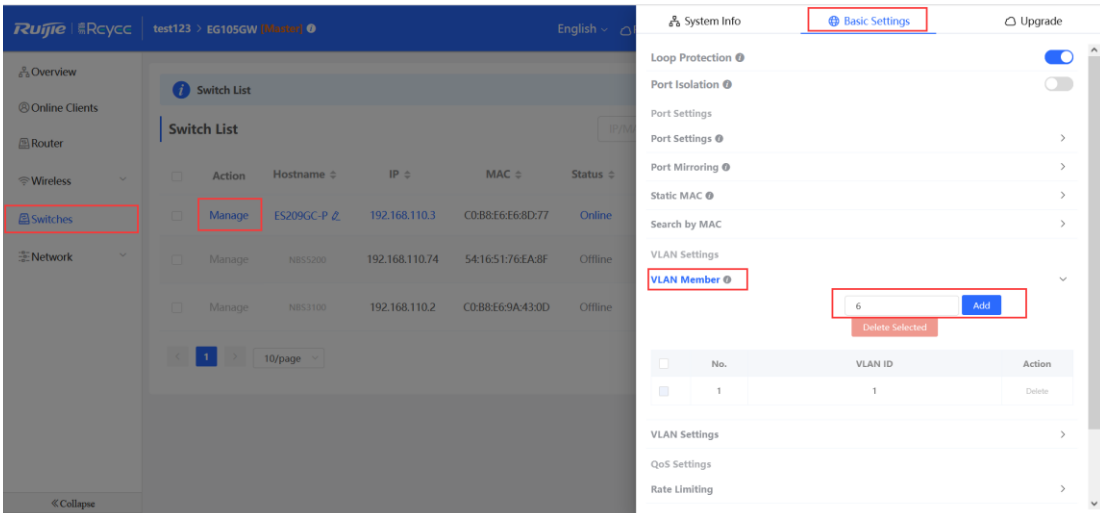
Up to 8 entries can be added.

□	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
□	192.168.6.1	255.255.255.0	6	-	Enabled	192.168.6.1	254	30	Edit Delete

Note

The network segment 192.168.110.0/24 is configured for VLAN 1.

b Choose **Switches** > **Manage** > **Basic Settings** > **VLAN Member** to create VLAN 6 on the switch, and click **VLAN Settings** to configure port 2 and port 9 connected to the AP and EG as trunk ports and allow packets from VLAN 1 and VLAN 6 to pass through. Then check port settings on the switch.



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

Loop Protection: on

Port Isolation: off

Port Settings: Port Settings, Port Mirroring, Static MAC, Search by MAC

VLAN Settings

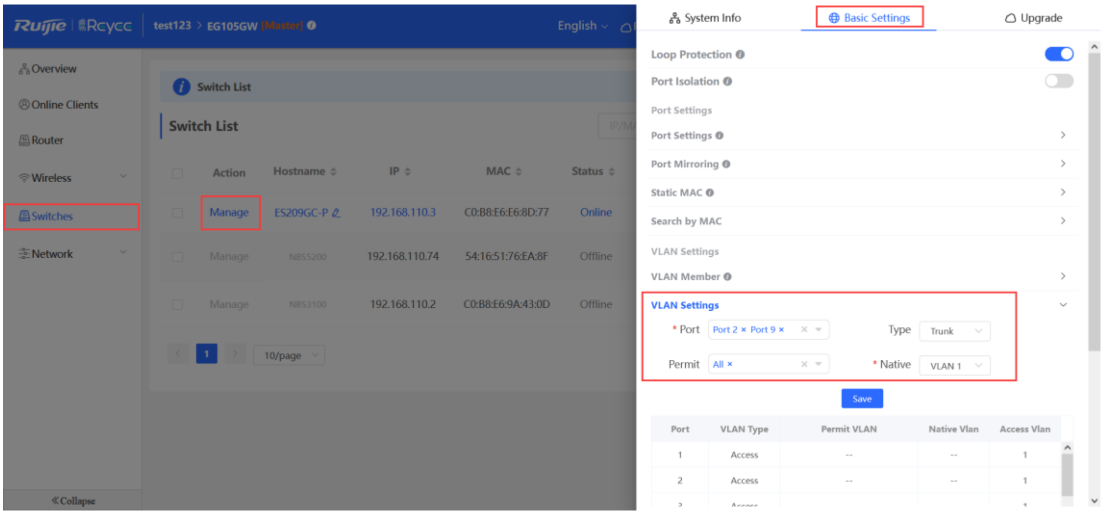
VLAN Member: 6 Add

Delete Selected

No.	VLAN ID	Action
1	1	Delete

VLAN Settings

QoS Settings: Rate Limiting



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

Loop Protection: on

Port Isolation: off

Port Settings: Port Settings, Port Mirroring, Static MAC, Search by MAC

VLAN Settings: VLAN Member

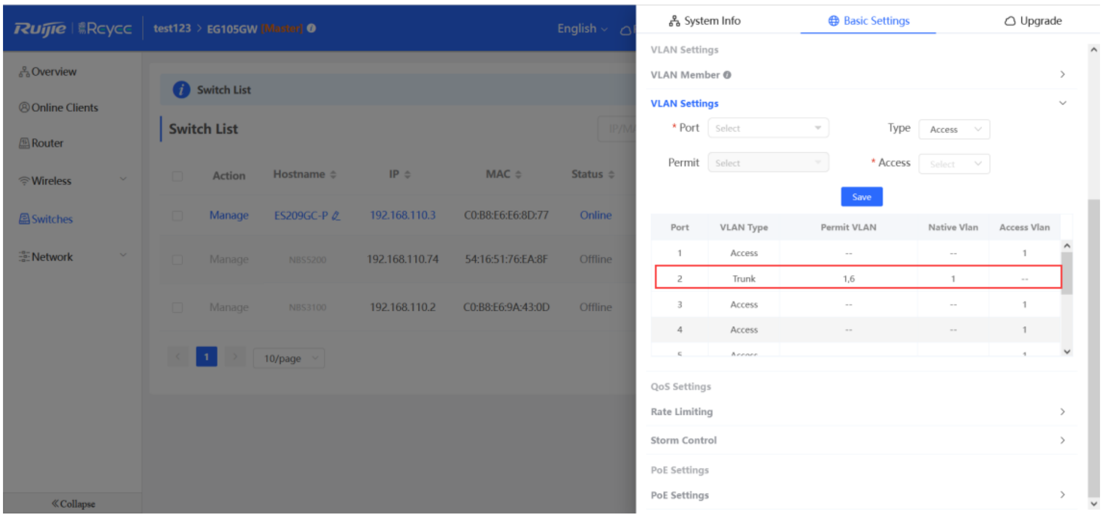
VLAN Settings

* 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
3	Access			1



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

VLAN Settings: VLAN Member

VLAN Settings

* Port: Select Type: Access

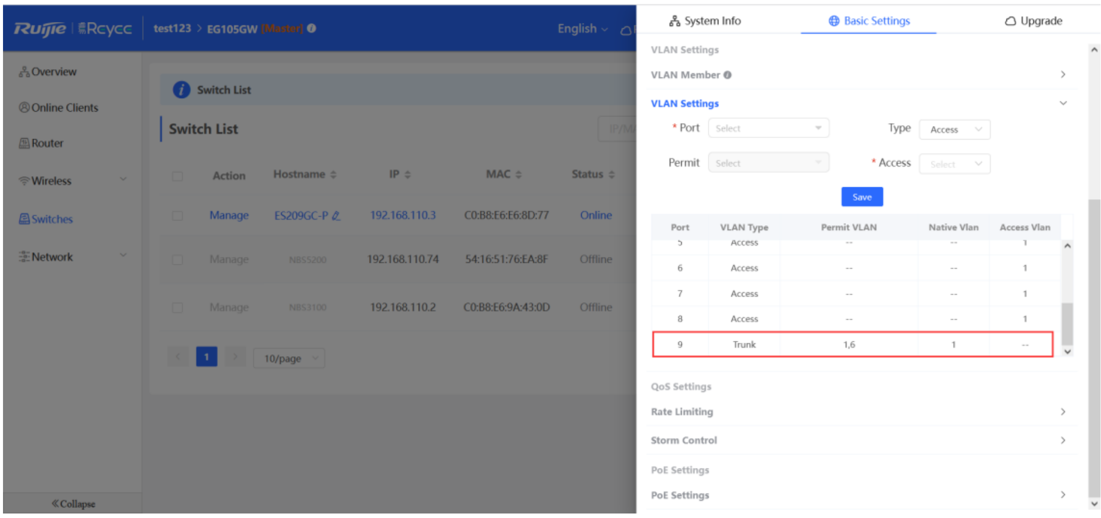
Permit: Select * Access: Select

Save

Port	VLAN Type	Permit VLAN	Native Vlan	Access Vlan
1	Access	--	--	1
2	Trunk	1,6	1	--
3	Access	--	--	1
4	Access	--	--	1
5	Access			1

QoS Settings: Rate Limiting, Storm Control

PoE Settings: PoE Settings



Ruijie | Reyee 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

1 10/page

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
5	Access	--	--	1
6	Access	--	--	1
7	Access	--	--	1
8	Access	--	--	1
9	Trunk	1,6	1	--

QoS Settings

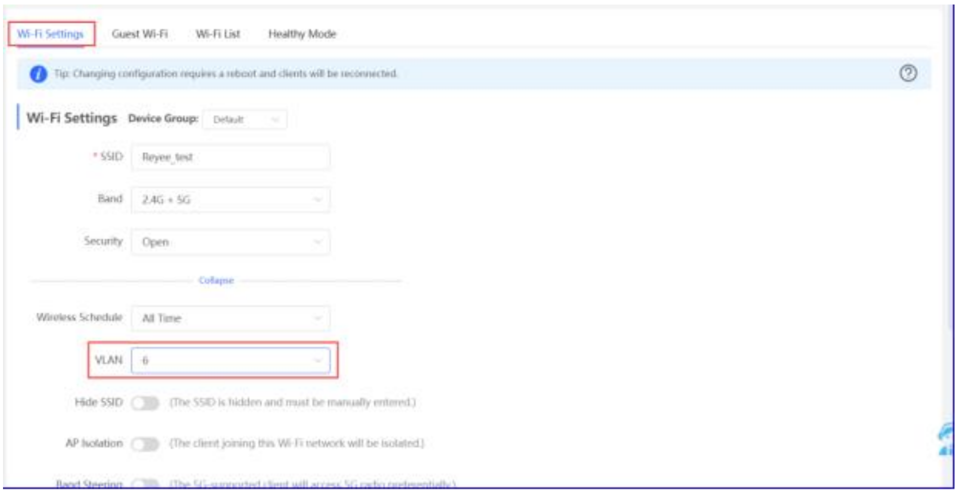
Rate Limiting

Storm Control

PoE Settings

PoE Settings

c Choose **WLAN** > **Wi-Fi** > **Wi-Fi Settings**. Configure the SSID named **Reyee_test** and associate VLAN 6 with the SSID.



Wi-Fi Settings | Guest Wi-Fi | Wi-Fi List | Healthy Mode

Tip: Changing configuration requires a reboot and clients will be reconnected.

Wi-Fi Settings Device Group: Default

* SSID: Reyee_test

Band: 2.4G + 5G

Security: Open

Collapse

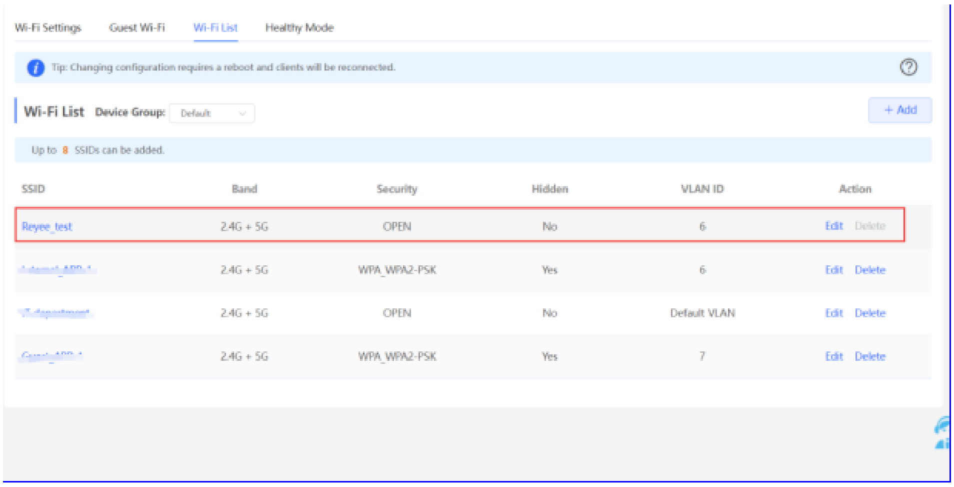
Wireless Schedule: All Time

VLAN: 6

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.)



Wi-Fi Settings | Guest Wi-Fi | Wi-Fi List | Healthy Mode

Tip: Changing configuration requires a reboot and clients will be reconnected.

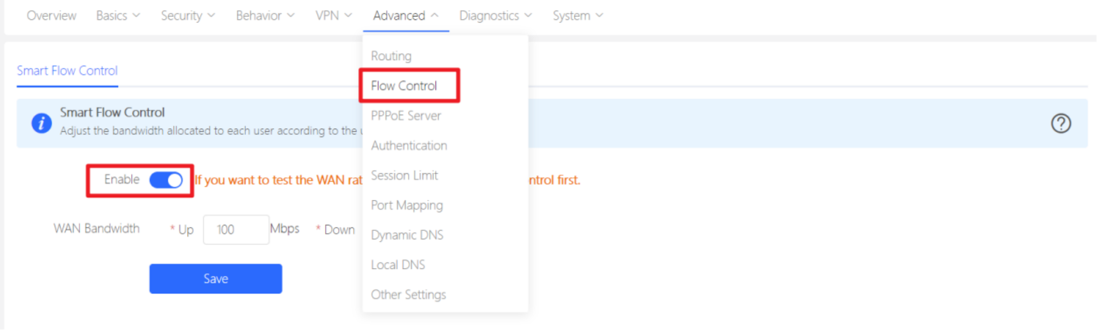
Wi-Fi List Device Group: Default + Add

Up to 8 SSIDs can be added.

SSID	Band	Security	Hidden	VLAN ID	Action
Reyee_test	2.4G + 5G	OPEN	No	6	Edit Delete
[redacted]	2.4G + 5G	WPA_WPA2-PSK	Yes	6	Edit Delete
[redacted]	2.4G + 5G	OPEN	No	Default VLAN	Edit Delete
[redacted]	2.4G + 5G	WPA_WPA2-PSK	Yes	7	Edit Delete

(2) Configure **Smart Flow Control** and a customized policy.

a Choose **Router** > **Advanced** > **Flow Control** and enable **Smart Flow Control**.

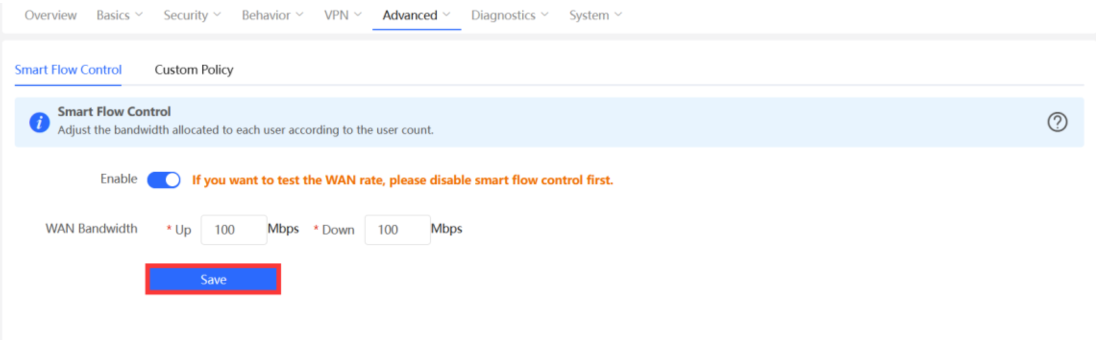


Smart Flow Control
Adjust the bandwidth allocated to each user according to the u

Enable
If you want to test the WAN rat ntrol first.

WAN Bandwidth * Up 100 Mbps * Down

b Set uplink and downlink WAN bandwidth to 100 Mbit/s and click **Save** to save the configuration.

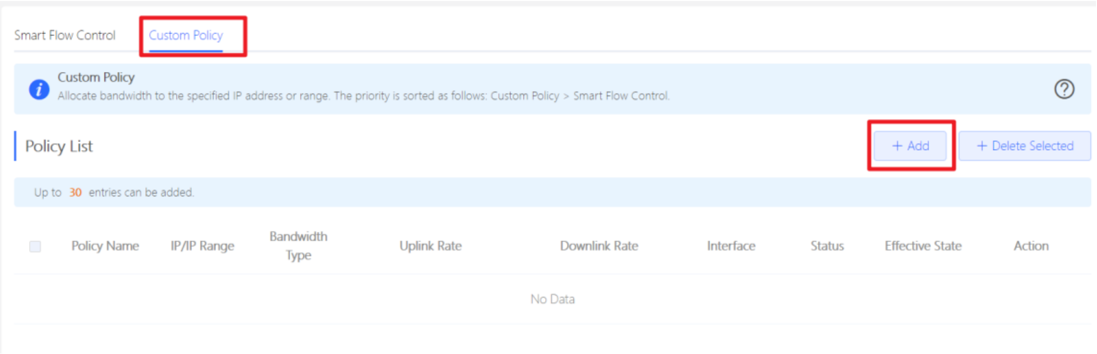


Smart Flow Control
Adjust the bandwidth allocated to each user according to the user count.

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

WAN Bandwidth * Up 100 **Mbps** * Down 100 **Mbps**

c After the previous step is complete, **Custom Policy** will be displayed. Click **Add** to add a policy.



Custom Policy
Allocate bandwidth to the specified IP address or range. The priority is sorted as follows: Custom Policy > Smart Flow Control.

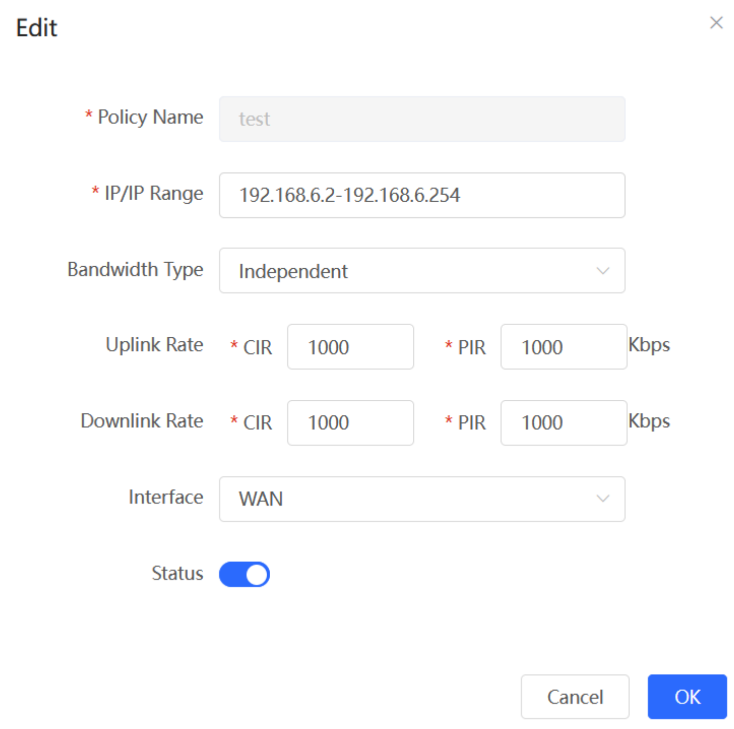
Policy List

Up to 30 entries can be added.

□	Policy Name	IP/IP Range	Bandwidth Type	Uplink Rate	Downlink Rate	Interface	Status	Effective State	Action

No Data

d Set **Policy Name**, **IP range**, **Bandwidth Type**, **Rate**, and other parameters.



Edit

* Policy Name: test

* IP/IP Range: 192.168.6.2-192.168.6.254

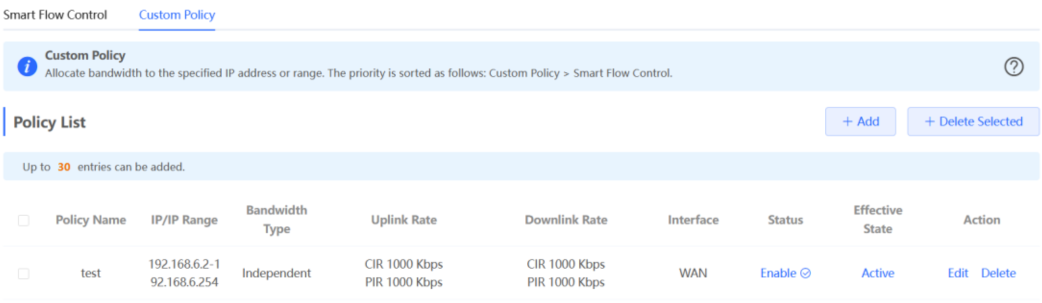
Bandwidth Type: Independent

Uplink Rate: * CIR 1000 * PIR 1000 Kbps

Downlink Rate: * CIR 1000 * PIR 1000 Kbps

Interface: WAN

Status: ●



Custom Policy

Allocate bandwidth to the specified IP address or range. The priority is sorted as follows: Custom Policy > Smart Flow Control.

Policy List

Up to 30 entries can be added.

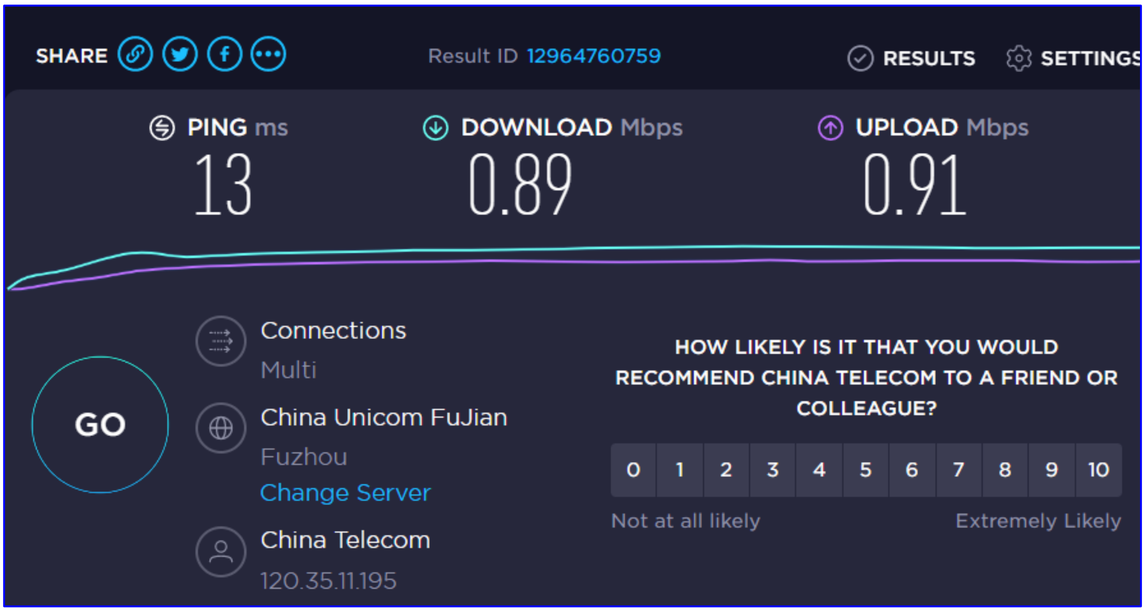
□	Policy Name	IP/IP Range	Bandwidth Type	Uplink Rate	Downlink Rate	Interface	Status	Effective State	Action
□	test	192.168.6.2-192.168.6.254	Independent	CIR 1000 Kbps PIR 1000 Kbps	CIR 1000 Kbps PIR 1000 Kbps	WAN	Enable ✓	Active	Edit Delete

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

Uplink Rate/**Downlink Rate**: **CIR** means the committed information rate. **PIR** means the peak information rate.

Configuration Verification

Use the speed test tool to check that each user is limited to 1 Mbit/s.



Result ID 12964760759

PING ms 13

DOWNLOAD Mbps 0.89

UPLOAD Mbps 0.91

Connections
Multi

China Unicom FuJian
Fuzhou

China Telecom
120.35.11.195

HOW LIKELY IS IT THAT YOU WOULD RECOMMEND CHINA TELECOM TO A FRIEND OR COLLEAGUE?

0 1 2 3 4 5 6 7 8 9 10

Not at all likely Extremely Likely

5.2 Reyee Cloud Authentication Solution

5.2.1 Working Principle

Cloud authentication allows you to control users' access to the wireless network. The configuration will be synchronized from the cloud to the local EG. In portal authentication, all the clients' HTTP requests will be redirected to an authentication page first. The clients are required for authentication, payment, acceptance of the end-user license agreement, acceptable use policy, survey completion, or other valid credentials. Then they can visit the Internet after successful authentication.

5.2.2 Application Scenario

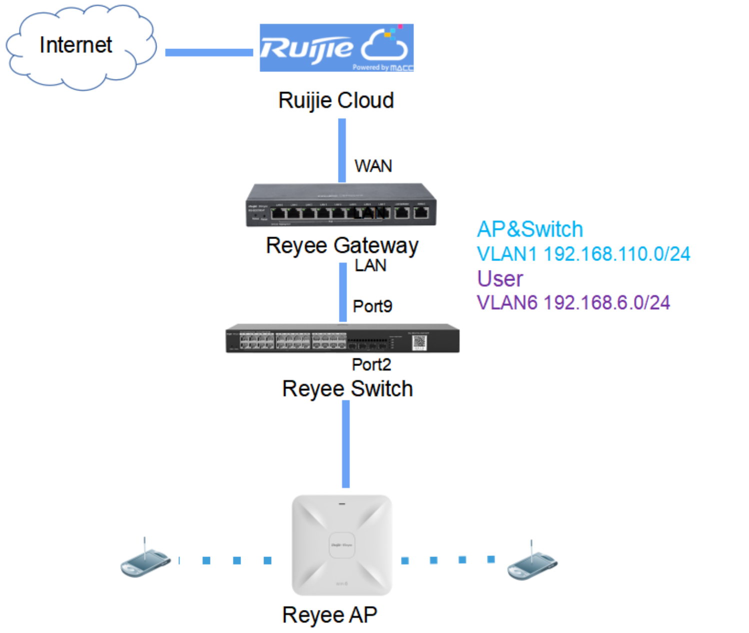
Portal authentication, also known as web authentication, is usually deployed on a guest-access network (such as a hotel or a coffee shop) to control the clients' Internet access.

5.2.3 Configuration Case

Requirement

Users need to be authenticated first before being allowed to access the Internet. A Reyee AP does not support cloud authentication, so a Reyee EG is required.

Network Topology



Network Description:

The EG works as a DHCP server to assign IP addresses to users, Reyee AP, and Reyee switch.

The AP and switch obtain IP addresses on network segment 192.168.110.0/24 in VLAN 1 for Internet access

Users obtain IP addresses on network segment 192.168.6.0/24 in VLAN 6 for Internet access.

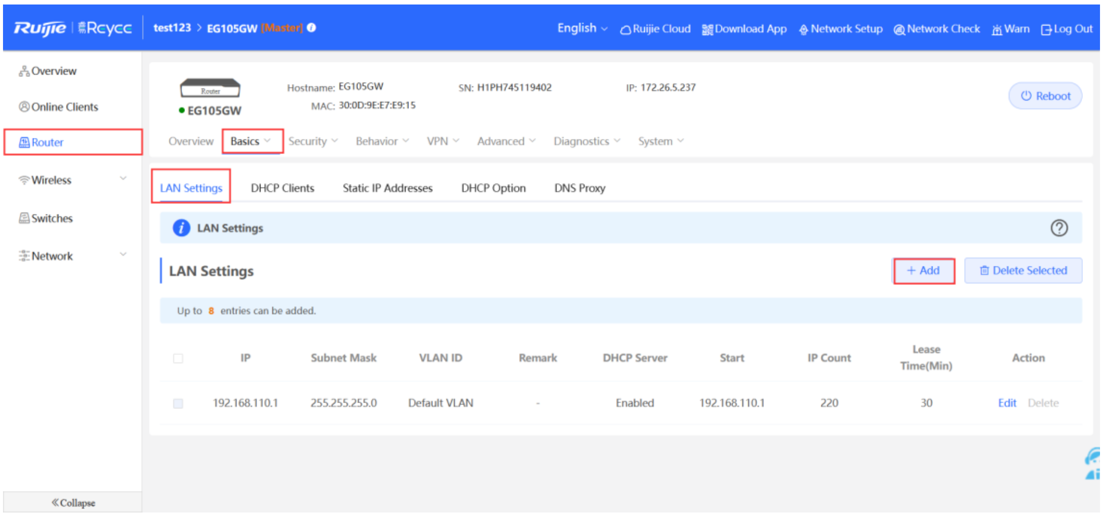
Ruijie Cloud manages and monitors devices and clients and provides captive authentication for clients.

Configuration Steps

The configuration steps include configuring the basic network and cloud authentication.

(1) Configure the basic network.

a Choose **Router** > **Basics** > **LAN** > **LAN Settings** > **Add**. Configure LAN settings and a DHCP pool for VLAN 1 and VLAN 6 on the EG.

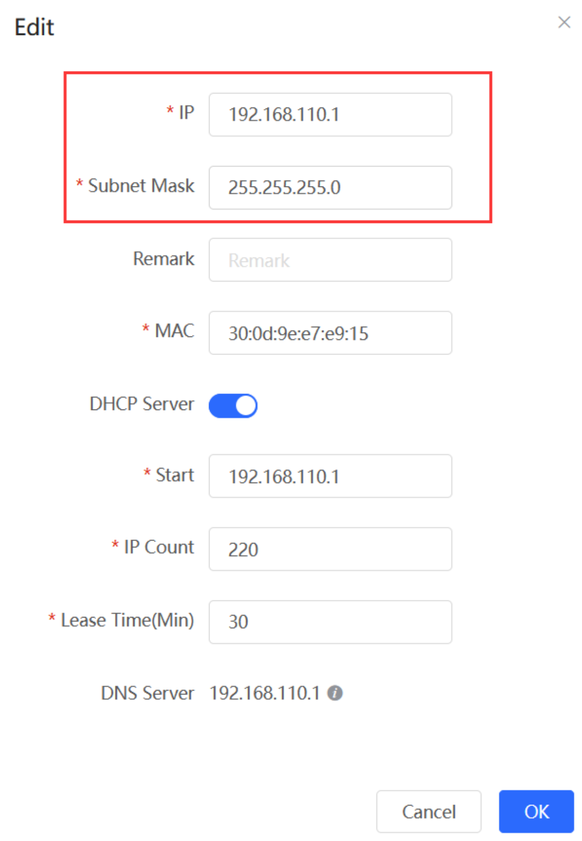


Hostname: EG105GW
MAC: 30:0D:9E:E7:E9:15
SN: H1PH745119402
IP: 172.26.5.237

LAN Settings

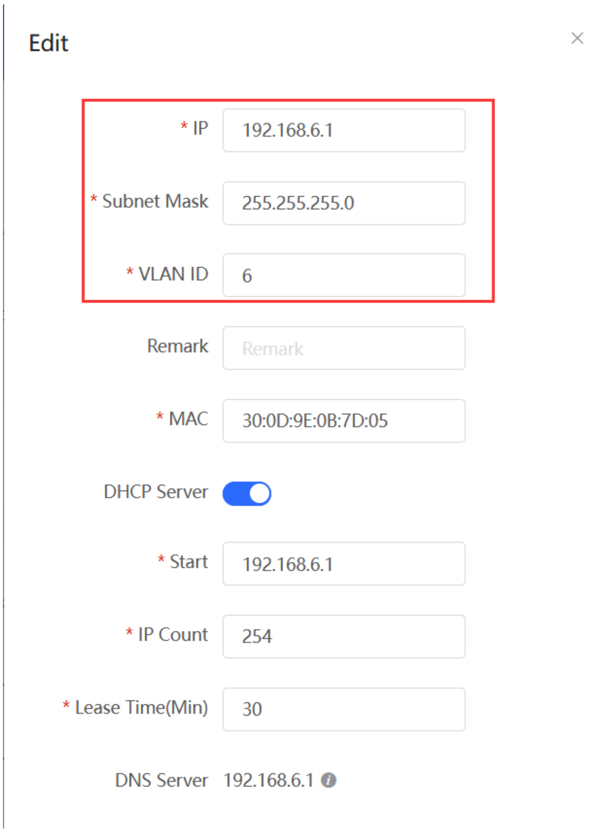
Up to 8 entries can be added.

□	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



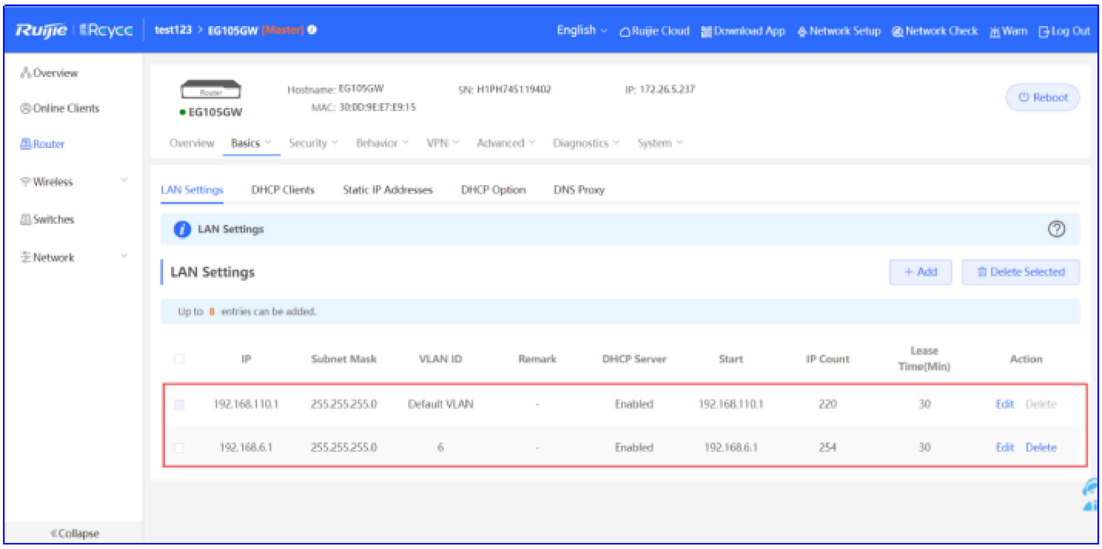
Edit

* 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



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



LAN Settings

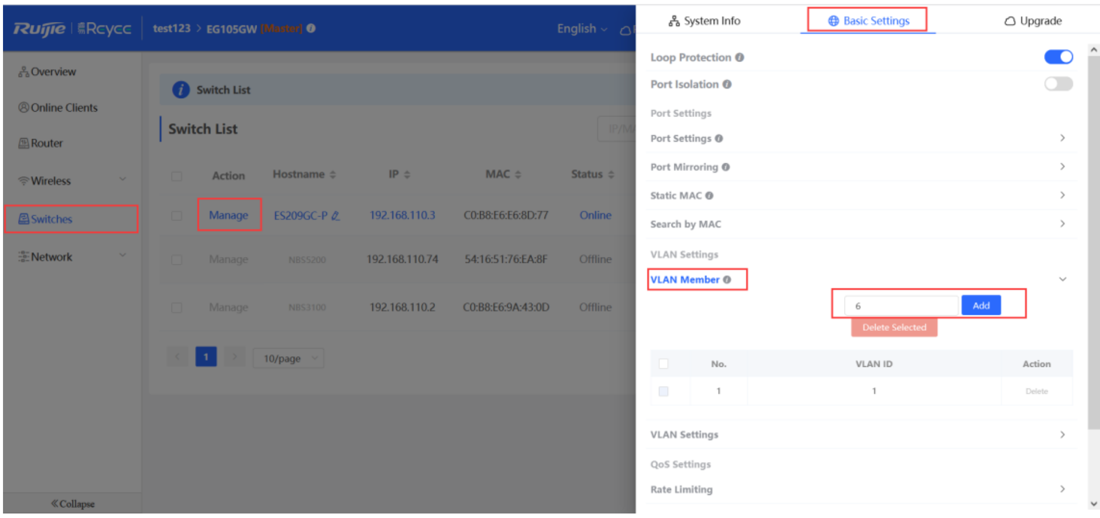
Up to 8 entries can be added.

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
192.168.6.1	255.255.255.0	6	-	Enabled	192.168.6.1	254	30	Edit Delete

Instruction

The network segment 192.168.110.0/24 is configured for VLAN 1.

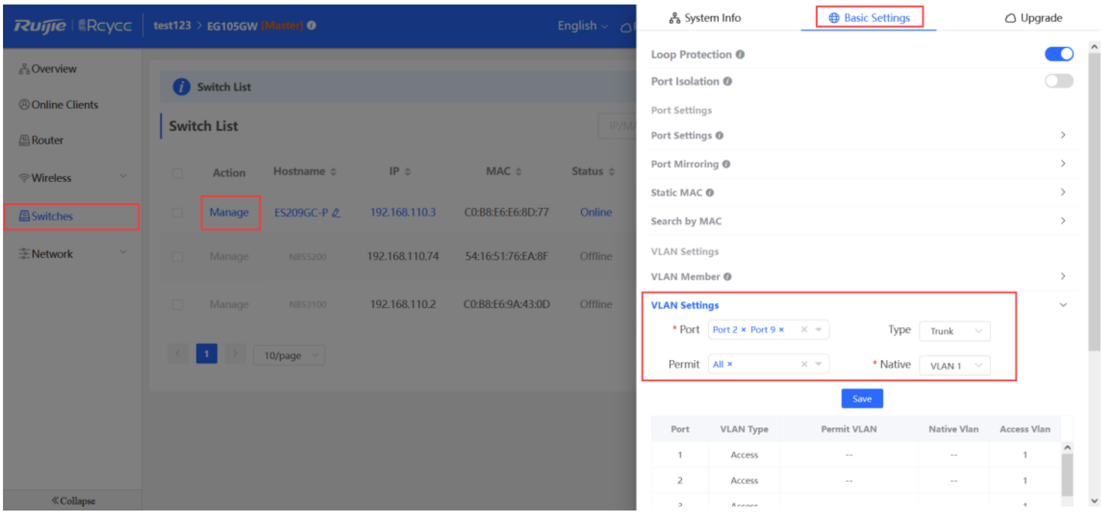
b Choose **Switches** > **Manage** > **Basic Settings** > **VLAN Member** to create VLAN 6 on the switch, and click **VLAN Settings** to configure port 2 and port 9 connected to the AP and EG as trunk ports and allow packets from VLAN 1 and VLAN 6 to pass through. Then check port settings on the switch.



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

No.	VLAN ID	Action
1	1	Delete



Switch List

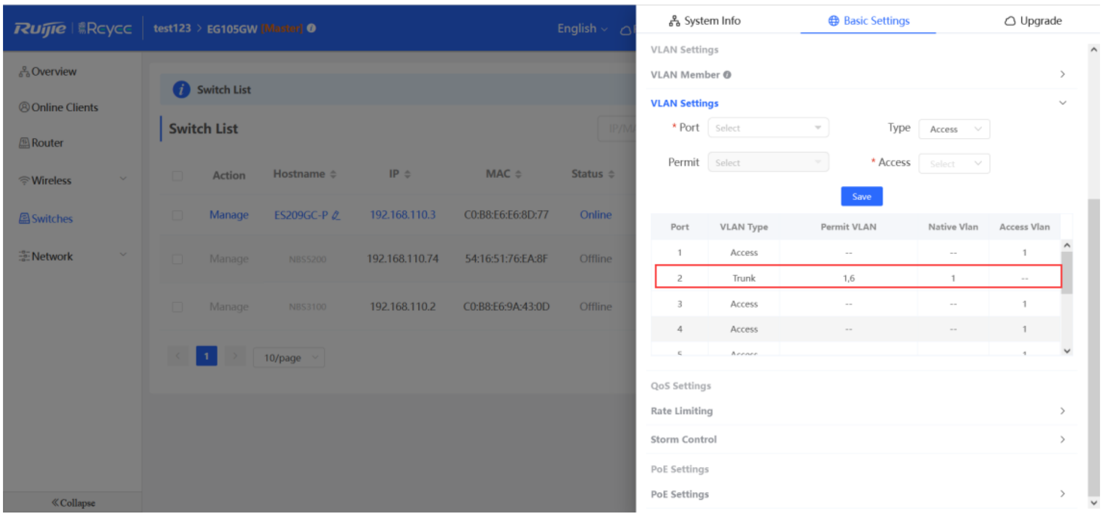
Action	Hostname	IP	MAC	Status
Manage	ES209GC-P	192.168.110.3	C0:B8:E6:E6:8D:77	Online
Manage	NBS5200	192.168.110.74	54:16:51:76:EA:8F	Offline
Manage	NBS3100	192.168.110.2	C0:B8:E6:9A:43:0D	Offline

VLAN Settings

* Port: Port 2 × Port 9 × Type: Trunk

Permit: All × * Native: VLAN 1

Port	VLAN Type	Permit VLAN	Native Vlan	Access Vlan
1	Access	--	--	1
2	Access	--	--	1

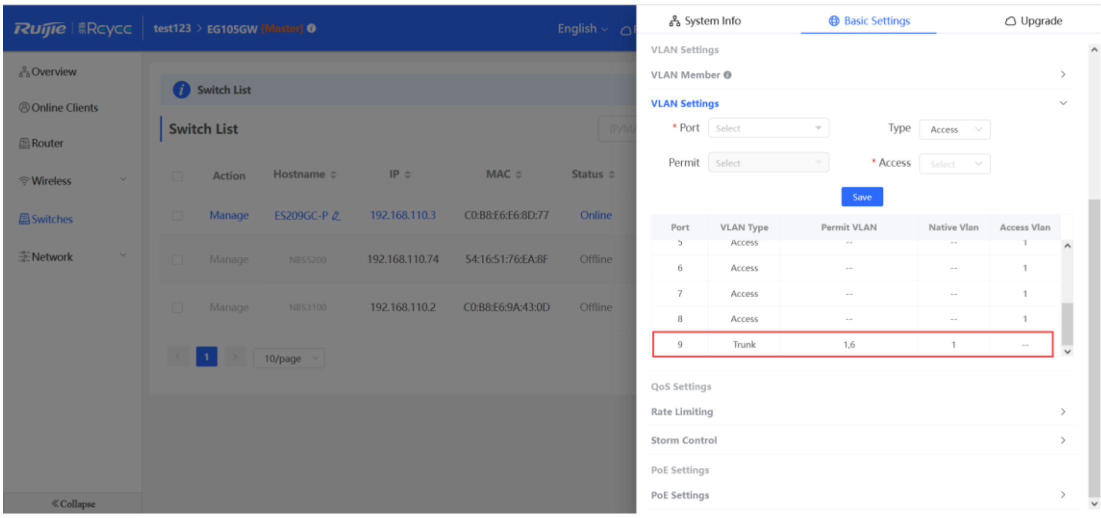


VLAN Settings

* Port: Select Type: Access

Permit: Select * Access: Select

Port	VLAN Type	Permit VLAN	Native Vlan	Access Vlan
1	Access	--	--	1
2	Trunk	1,6	1	--
3	Access	--	--	1
4	Access	--	--	1



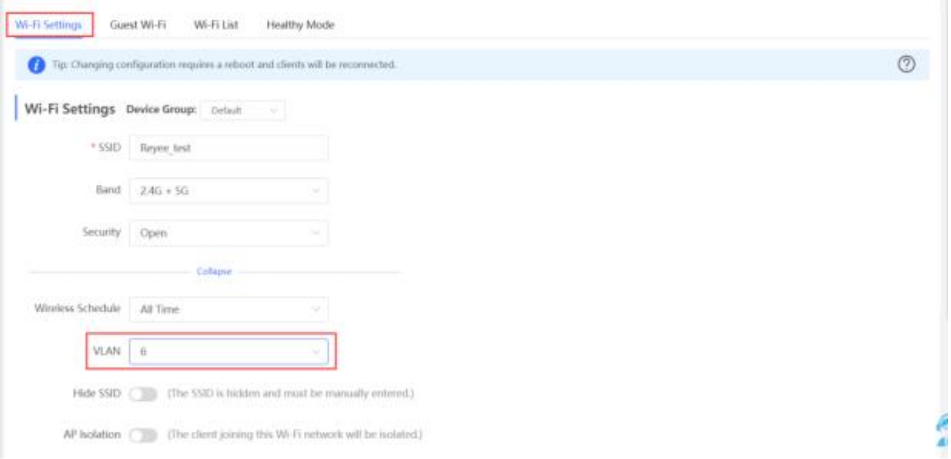
VLAN Settings

* Port: Select Type: Access

Permit: Select * Access: Select

Port	VLAN Type	Permit VLAN	Native Vlan	Access Vlan
5	Access	--	--	1
6	Access	--	--	1
7	Access	--	--	1
8	Access	--	--	1
9	Trunk	1,6	1	--

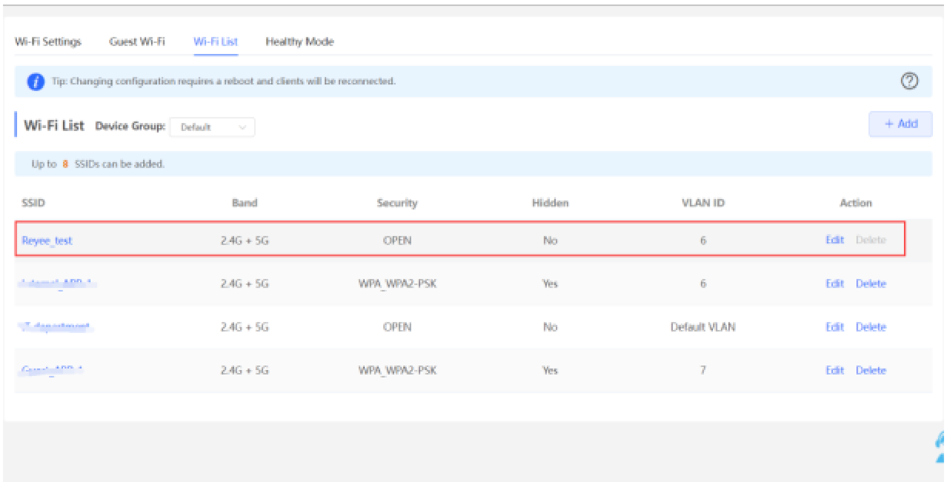
c Choose **WLAN** > **Wi-Fi** > **Wi-Fi Settings**, configure a SSID named **Reyee test** and associate VLAN 6 with the SSID.



Tip: Changing configuration requires a reboot and clients will be reconnected.

Wi-Fi Settings Device Group: Default

- * SSID: Reyee_test
- Band: 2.4G + 5G
- Security: Open
- Collapse
- Wireless Schedule: All Time
- VLAN: 6
- Hide SSID: (The SSID is hidden and must be manually entered.)
- AP Isolation: (The client joining this Wi-Fi network will be isolated.)



Tip: Changing configuration requires a reboot and clients will be reconnected.

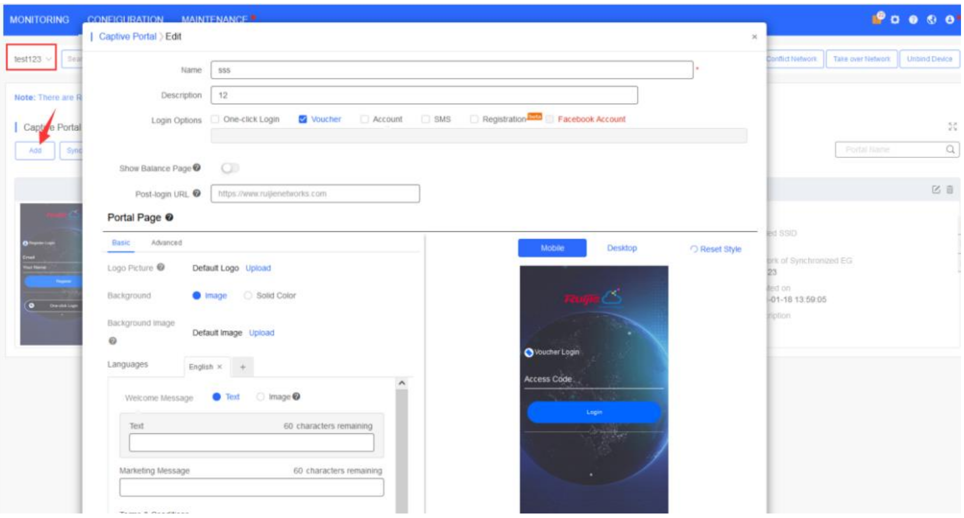
Wi-Fi List Device Group: Default

Up to 8 SSIDs can be added.

SSID	Band	Security	Hidden	VLAN ID	Action
Reyee_test	2.4G + 5G	OPEN	No	6	Edit Delete
[redacted]	2.4G + 5G	WPA_WPA2-PSK	Yes	6	Edit Delete
[redacted]	2.4G + 5G	OPEN	No	Default VLAN	Edit Delete
[redacted]	2.4G + 5G	WPA_WPA2-PSK	Yes	7	Edit Delete

(2) Configure cloud authentication.

a Choose **CONFIGURATION** > **AUTHENTICATION** > **Captive Portal** to access the **Captive Portal** page, select a network in this account, and click **Add** to create a new portal template and edit the captive portal template.



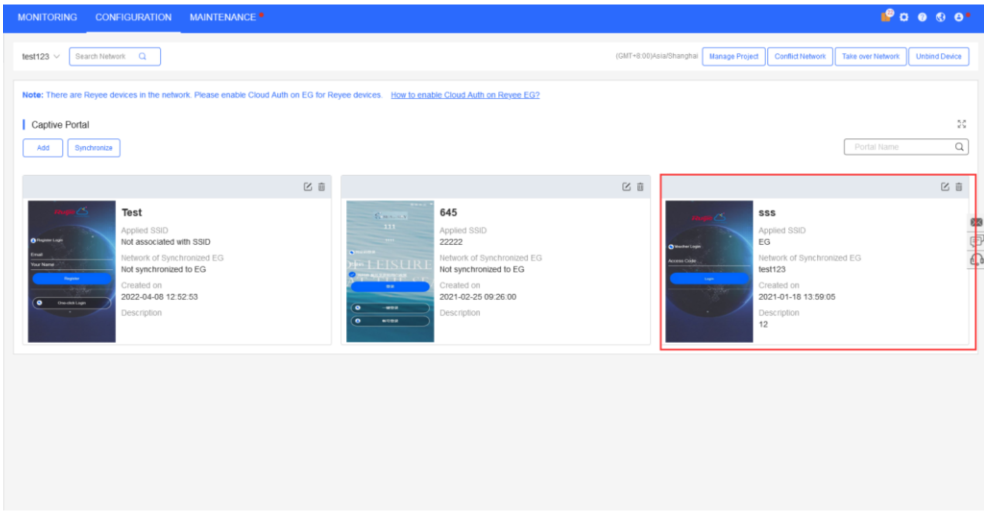
Captive Portal > Edit

- Name: sss *
- Description: 12
- Login Options: □ One-click Login ☑ Voucher □ Account □ SMS □ Registration □ Facebook Account
- Show Balance Page
- Post-login URL: https://www.ruijienetworks.com

Portal Page

Basic | Advanced

- Logo Picture: Default Logo Upload
- Background: ● Image ○ Solid Color
- Background Image: Default Image Upload
- Languages: English × +
- Welcome Message: ● Text ○ Image
- Text: 60 characters remaining
- Marketing Message: 60 characters remaining



Note: There are Reyee devices in the network. Please enable Cloud Auth on EG for Reyee devices. How to enable Cloud Auth on Reyee EG?

Captive Portal

Test
Applied SSID
Not associated with SSID
Network of Synchronized EG
Not synchronized to EG
Created on
2022-04-08 12:52:53
Description

645
Applied SSID
22222
Network of Synchronized EG
Not synchronized to EG
Created on
2021-02-25 09:26:00
Description

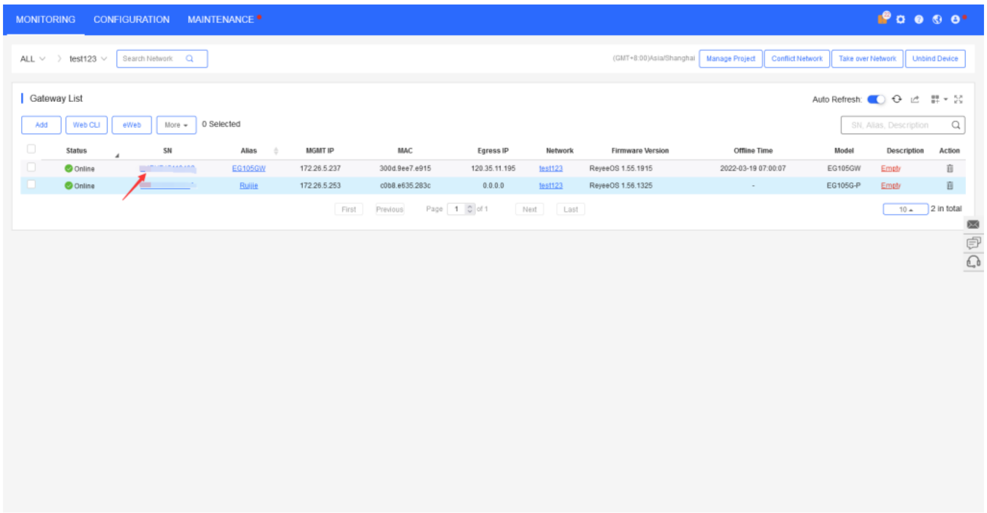
sss
Applied SSID
EG
Network of Synchronized EG
test123
Created on
2021-01-18 13:59:05
Description
12

One-click Login: Log in without the username and password. **Access Duration** and **Access Times per day** can be configured.

Voucher: Log in with a random eight-digit password.

Account: Log in with the account and password.

b Choose **MONITORING > DEVICE** > **Gateway**. Ensure that the Reyee EG is online on Ruijie Cloud and click its SN in the list to access the configuration page.

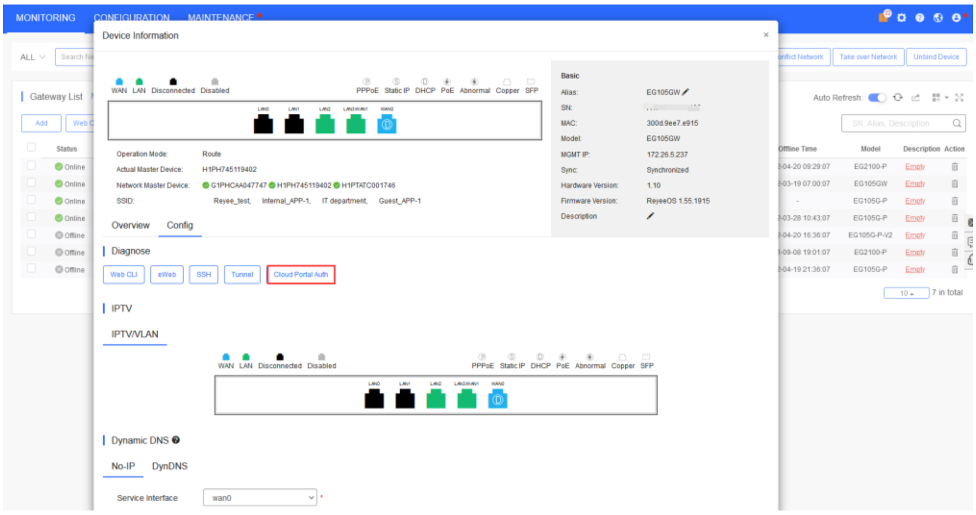


Gateway List

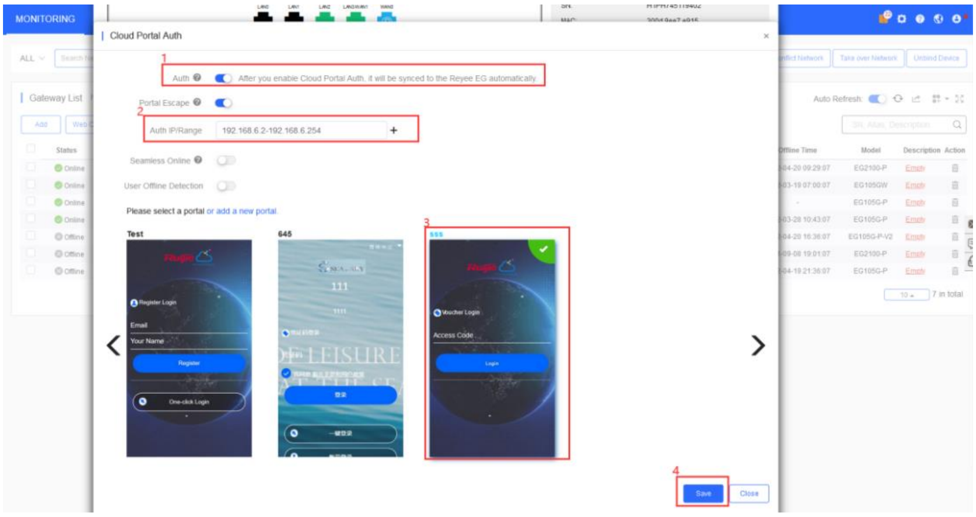
0 Selected

Status	SN	Alias	MGMT IP	MAC	Egress IP	Network	Firmware Version	Offline Time	Model	Description	Action
Online	[redacted]	EG105GW	172.26.5.237	300d.9ee7.e915	120.35.11.195	test123	ReyeeOS 1.55.1915	2022-03-19 07:00:07	EG105GW	Empty	
Online	[redacted]	Ruijie	172.26.5.253	c0b8.e635.283c	0.0.0.0	test123	ReyeeOS 1.56.1325	-	EG105G-P	Empty	

c Click **Cloud portal Auth** to configure authentication on Ruijie Cloud.



d Enable **Auth**, set **Auth IP Range 192.168.6.2-192.168.6.254** for authentication, and select a portal template to be used. Then click **Save** to save all configurations.


Cloud Portal Auth

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

Portal Escape: ●

2 Auth IP/Range: 192.168.6.2-192.168.6.254 +

Seamless Online: ○

User Offline Detection: ○

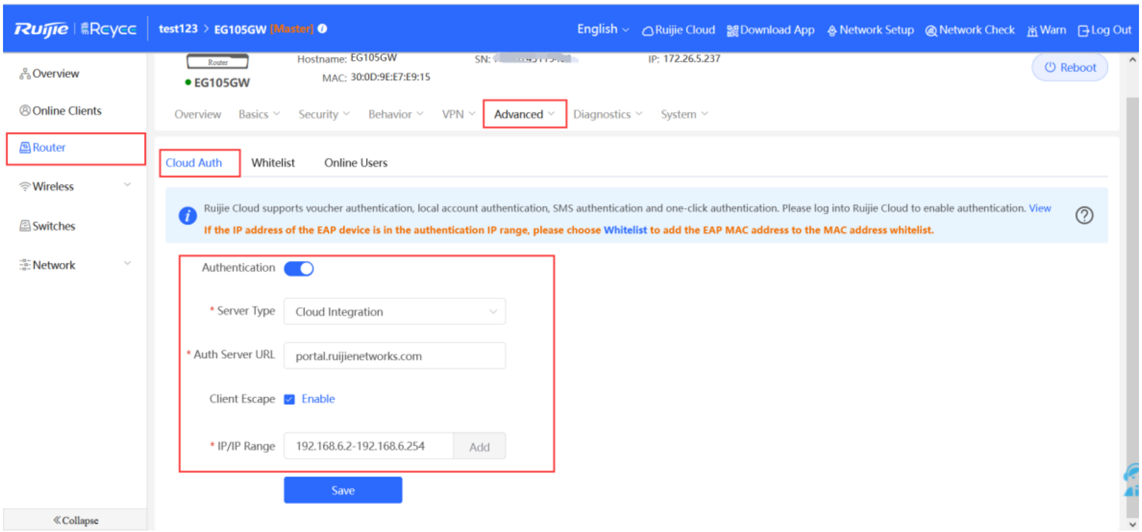
Please select a portal or add a new portal

⚠ Note

The IP addresses of the EG, switch, and AP need to be excluded; otherwise, the EG, switch, and AP cannot access the Internet.

Configuration Verification

Choose **Router** > **Advanced** > **LAN** > **Authentication** > **Cloud Auth**. Check whether the configuration is synchronized to the EG.



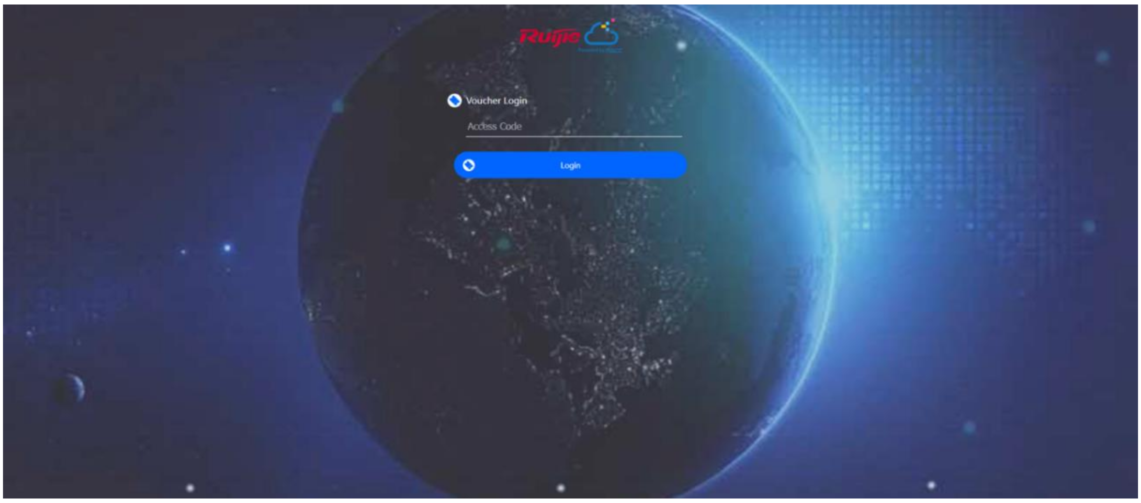
Hostname: EG105GW
MAC: 30:0D:9E:E7:E9:15
SN: [redacted]
IP: 172.26.5.237

Ruijie Cloud supports voucher authentication, local account authentication, SMS authentication and one-click authentication. Please log into Ruijie Cloud to enable authentication. View

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

Authentication: On
* Server Type: Cloud Integration
* Auth Server URL: portal.ruijienetworks.com
Client Escape: ☑ Enable
* IP/IP Range: 192.168.6.2-192.168.6.254 Add

Users whose IP addresses are in the range from 192.168.6.2 to 192.168.6.254 IP need to be authenticated before accessing the Internet.



5.3 Reyee Guest Wi-Fi Solution

5.3.1 Working Principle

A single Internet entrance can be created by using guest Wi-Fi. The devices that are allowed to access guest Wi-Fi can access the Internet but cannot access the home Wi-Fi.

5.3.2 Application Scenario

Guest Wi-Fi provides secure Wi-Fi access for guests to share your home or office network. When someone visits your house, apartment, or workplace, you can enable guest Wi-Fi for them. You can set different access options for guest users, ensuring security and privacy of the main network.

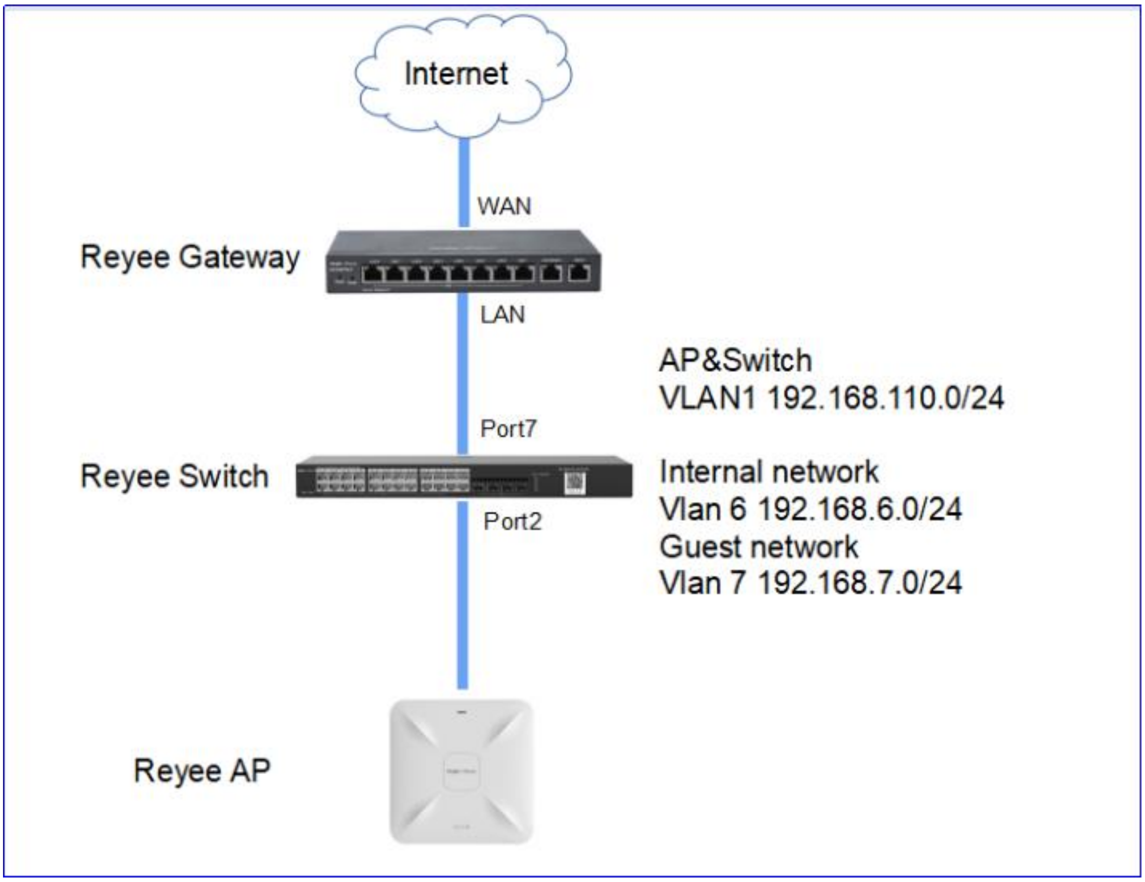
5.3.3 Configuration Case

Configuration Through EG's Eweb

Requirement

Guest Wi-Fi needs to be configured for guests in VLAN 7, so the guests are not allowed to access the internal network in VLAN 6.

Network Topology



Network Description:

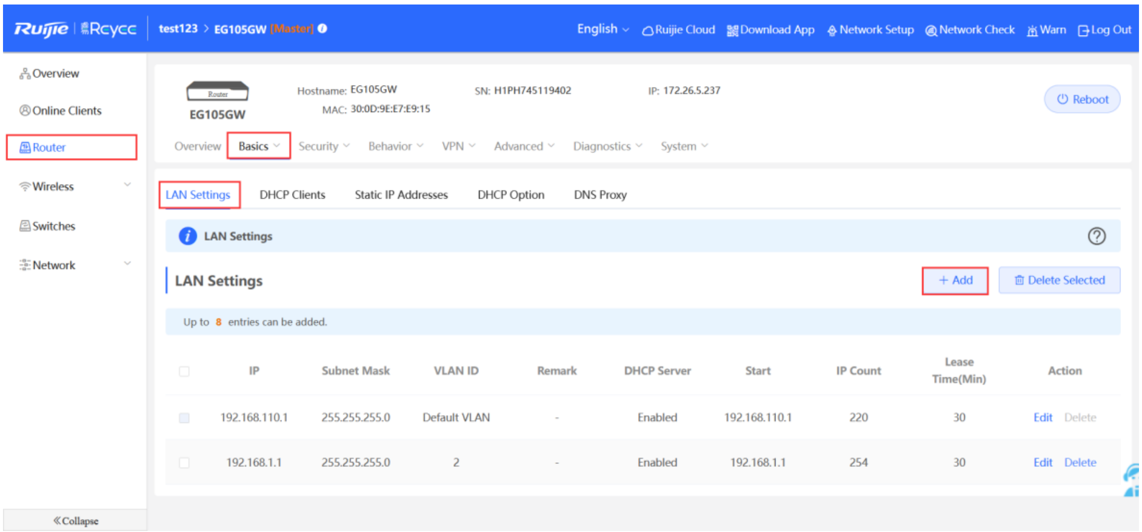
The EG works as a DHCP server to assign IP addresses to users, Reyee AP, and Reyee switch.

The AP and switch obtain IP addresses in VLAN 1 for Internet access.

Internal users obtain IP addresses on the network segment in VLAN 6 for Internet access, and guests obtain IP addresses on the network segment in VLAN 7 for Internet access.

Configuration Steps

(1) Choose **Router** > **Basics** > **LAN** > **LAN Settings** > **Add**. Configure LAN settings and a DHCP pool for VLAN 6 and VLAN 7 on the EG.



EG105GW

Hostname: EG105GW

MAC: 30:0D:9E:E7:E9:15

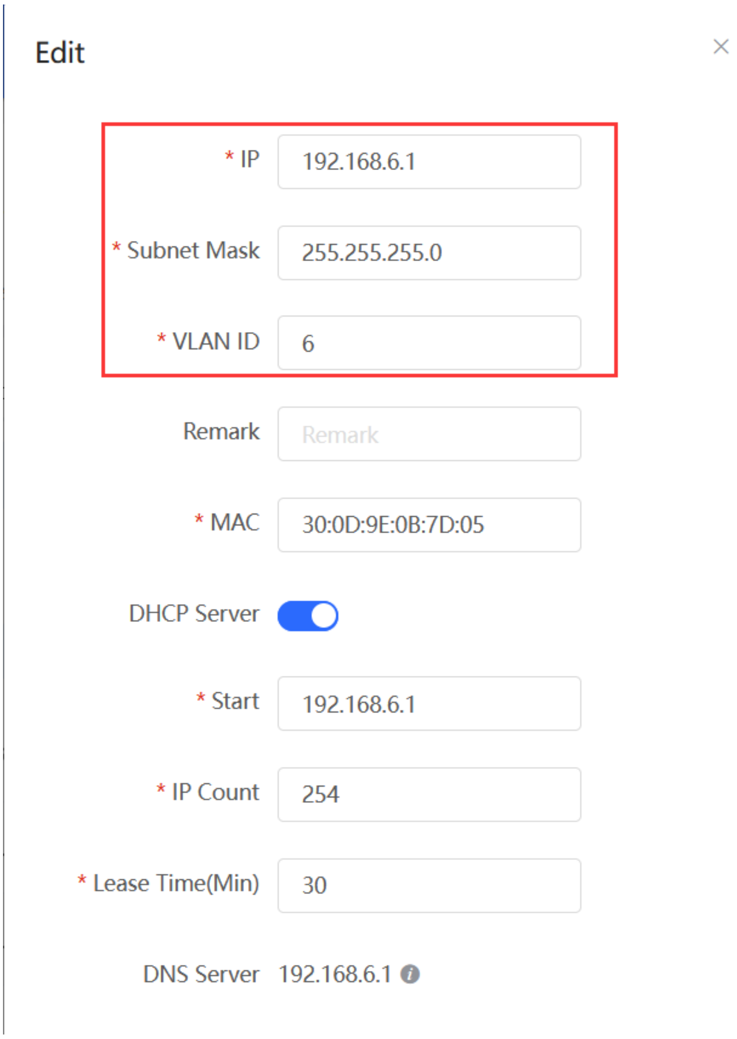
SN: H1PH745119402

IP: 172.26.5.237

LAN Settings

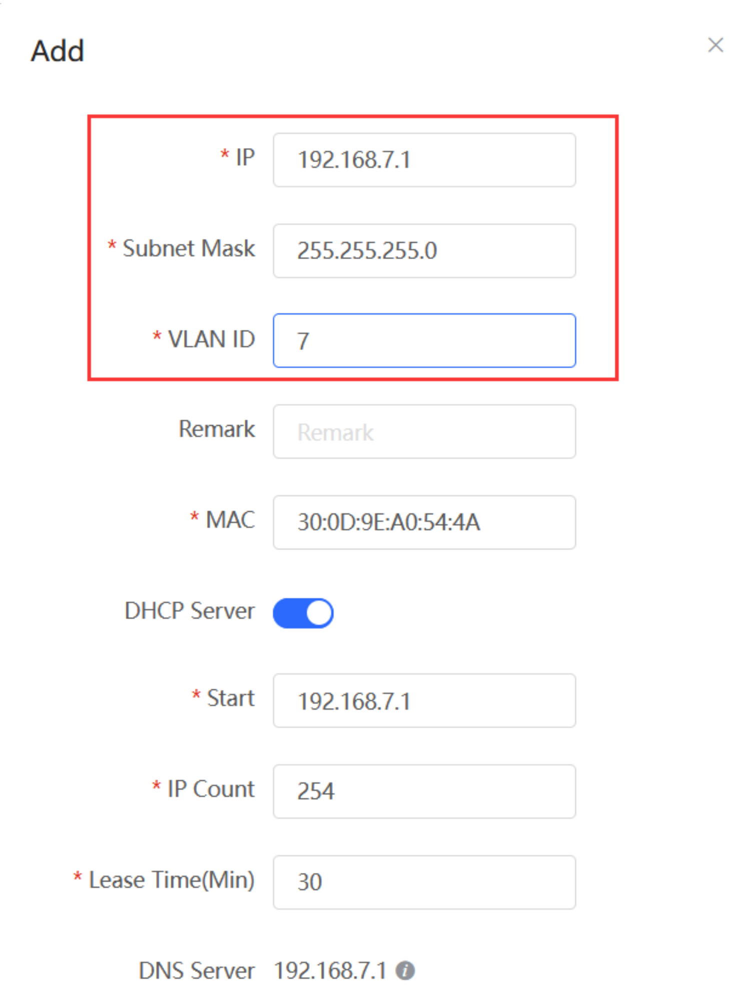
Up to 8 entries can be added.

□	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



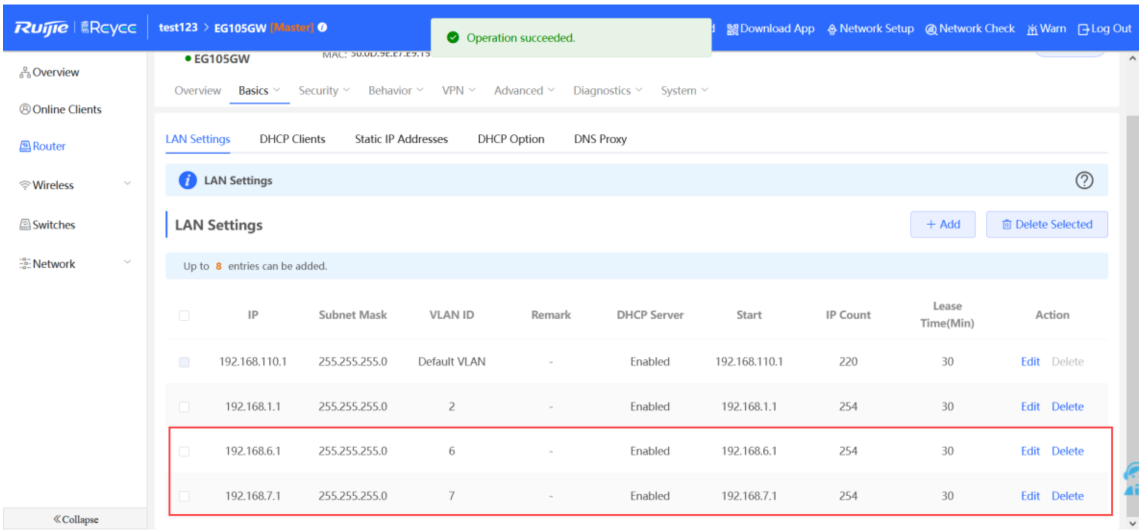
Edit

* 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



Add

* IP	192.168.7.1
* Subnet Mask	255.255.255.0
* VLAN ID	7
Remark	Remark
* MAC	30:0D:9E:A0:54:4A
DHCP Server	●
* Start	192.168.7.1
* IP Count	254
* Lease Time(Min)	30
DNS Server	192.168.7.1



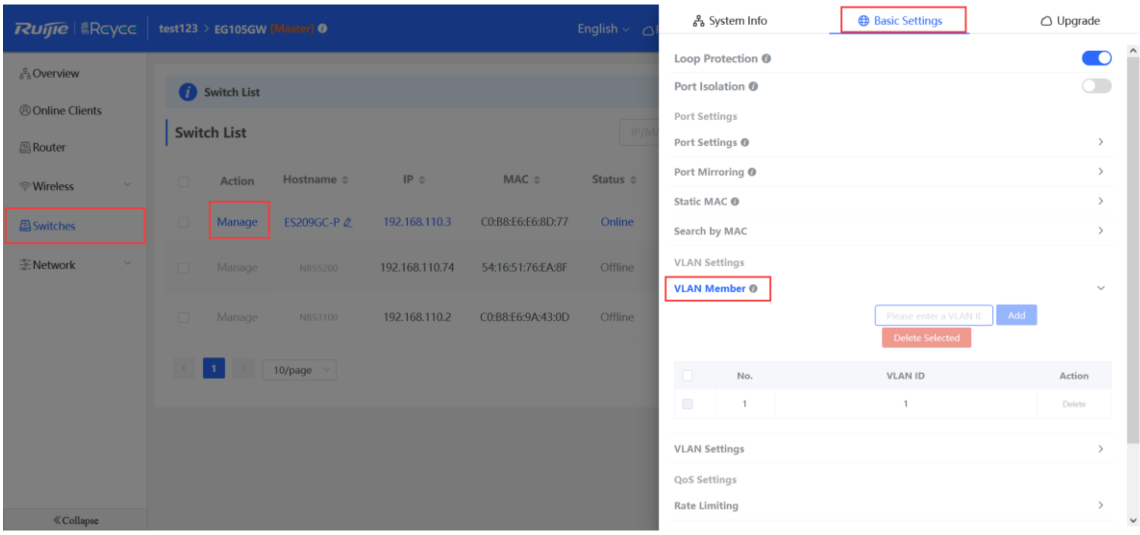
Operation succeeded.

LAN Settings

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
□	192.168.6.1	255.255.255.0	6	-	Enabled	192.168.6.1	254	30	Edit Delete
□	192.168.7.1	255.255.255.0	7	-	Enabled	192.168.7.1	254	30	Edit Delete

(2) Choose **Switches** > **Manage** > **Basic Settings** > **VLAN Member** to create VLAN 6 and VLAN 7 on the switch, and click **VLAN Settings** to configure port 2 and port 7 connected to the AP and EG as trunk ports and allow packets from VLAN 1, VLAN 6, and VLAN 7 to pass through. Then check port settings on the switch.



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

1 10/page

Loop Protection

Port Isolation

Port Settings

Port Settings

Port Mirroring

Static MAC

Search by MAC

VLAN Settings

VLAN Member

Please enter a VLAN ID Add

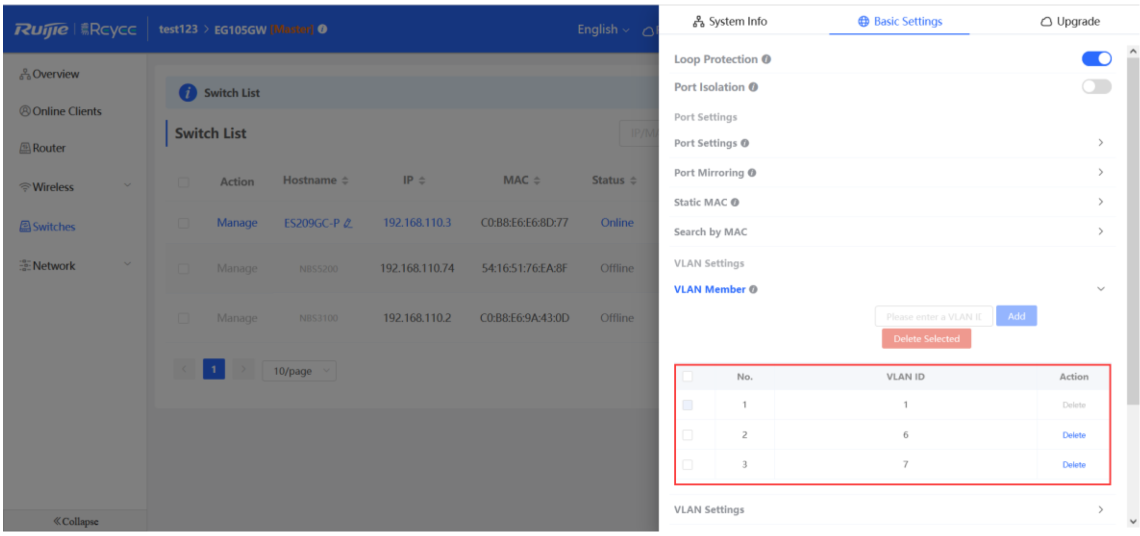
Delete Selected

No.	VLAN ID	Action
1	1	Delete

VLAN Settings

QoS Settings

Rate Limiting



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

1 10/page

Loop Protection

Port Isolation

Port Settings

Port Settings

Port Mirroring

Static MAC

Search by MAC

VLAN Settings

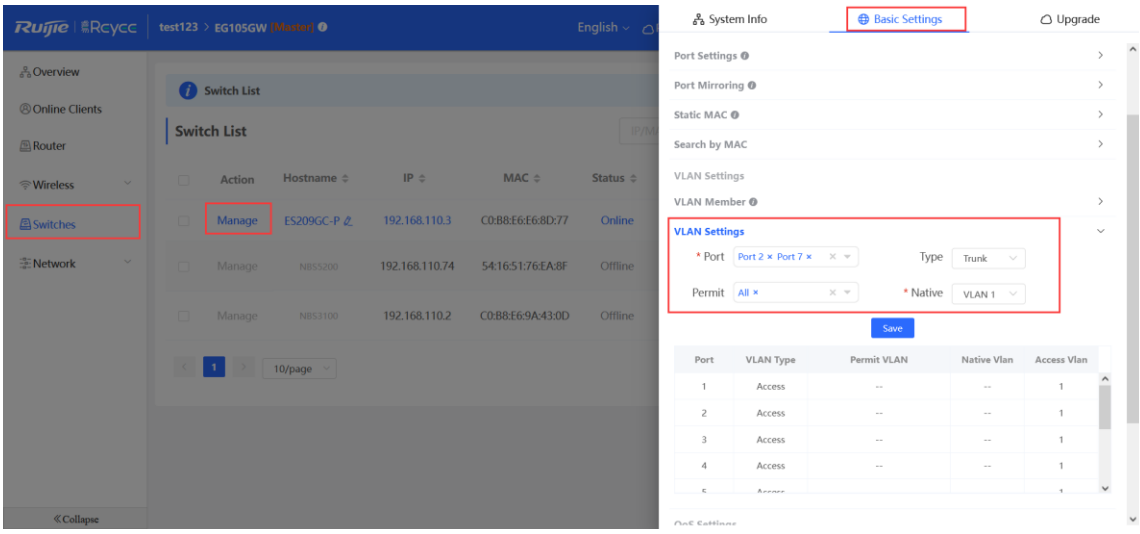
VLAN Member

Please enter a VLAN ID Add

Delete Selected

No.	VLAN ID	Action
1	1	Delete
2	6	Delete
3	7	Delete

VLAN Settings



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

1 10/page

Port Settings

Port Mirroring

Static MAC

Search by MAC

VLAN Settings

VLAN Member

VLAN Settings

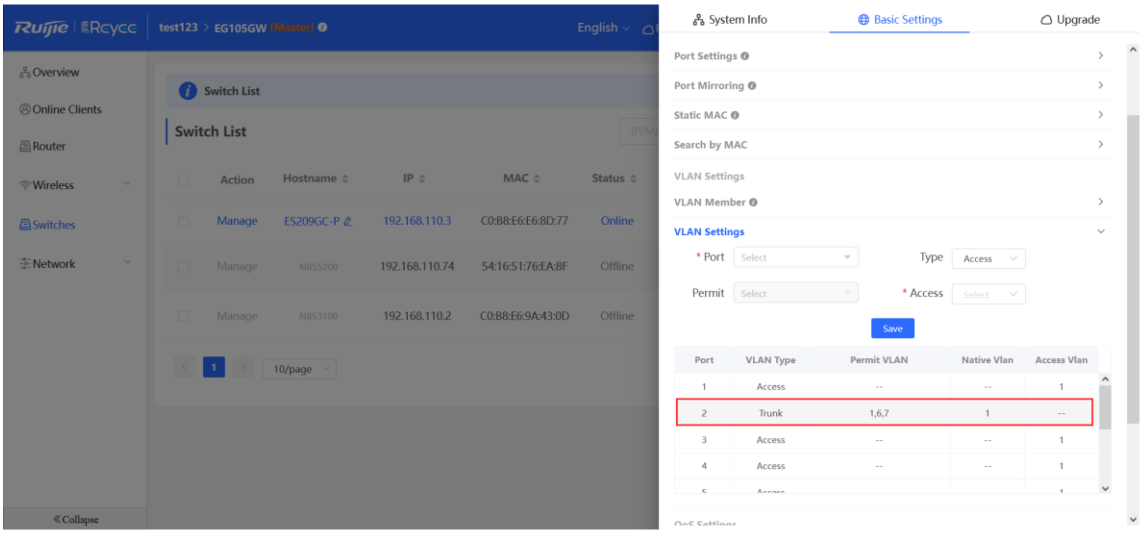
* Port: Port 2 × Port 7 × Type: Trunk

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
5	Access			1

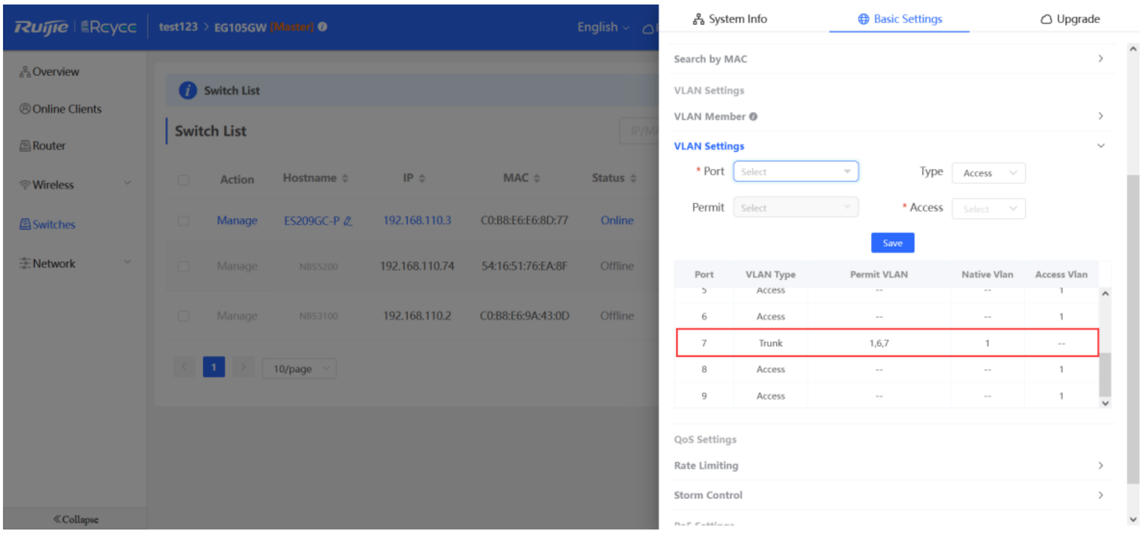
QoS Settings



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

* Port: Select
Type: Access
Permit: Select
* Access: Select

Port	VLAN Type	Permit VLAN	Native Vlan	Access Vlan
1	Access	--	--	1
2	Trunk	1,6,7	1	--
3	Access	--	--	1
4	Access	--	--	1

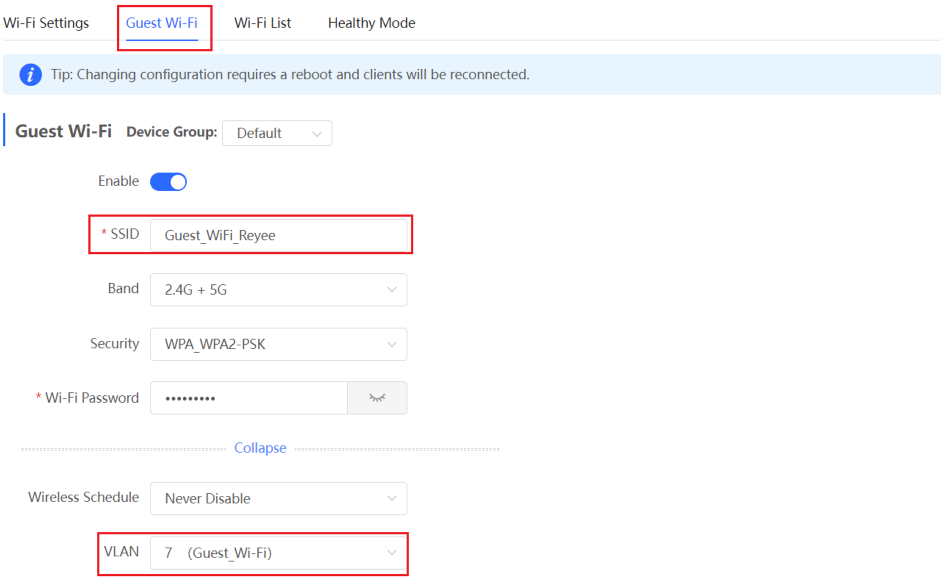


Action	Hostname	IP	MAC	Status
Manage	ES209GC-P	192.168.110.3	C0:B8:E6:E6:8D:77	Online
Manage	NBS5200	192.168.110.74	54:16:51:76:EA:8F	Offline
Manage	NBS3100	192.168.110.2	C0:B8:E6:9A:43:0D	Offline

* Port: Select
Type: Access
Permit: Select
* Access: Select

Port	VLAN Type	Permit VLAN	Native Vlan	Access Vlan
5	Access	--	--	1
6	Access	--	--	1
7	Trunk	1,6,7	1	--
8	Access	--	--	1
9	Access	--	--	1

(3) Choose **WLAN > Wi-Fi > Guest Wi-Fi**, configure a guest Wi-Fi SSID named **Guest_WiFi_Reyee** and associate VLAN 7 with the SSID.



Tip: Changing configuration requires a reboot and clients will be reconnected.

Guest Wi-Fi Device Group: Default

Enable: ●

* SSID: Guest_WiFi_Reyee

Band: 2.4G + 5G

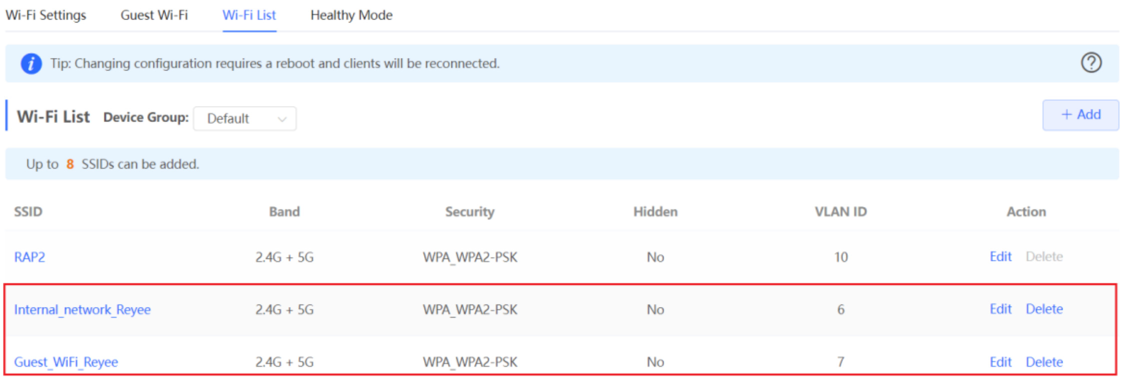
Security: WPA_WPA2-PSK

* Wi-Fi Password: •••••••••

Wireless Schedule: Never Disable

VLAN: 7 (Guest_Wi-Fi)

(4) Choose **WLAN** > **Wi-Fi** > **Wi-Fi List** > **Add**, configure the SSID named **Internal_network_Reyee** for internal users, configure VLAN6 for this SSID, and check Wi-Fi settings in **Wi-Fi List**.



Tip: Changing configuration requires a reboot and clients will be reconnected.

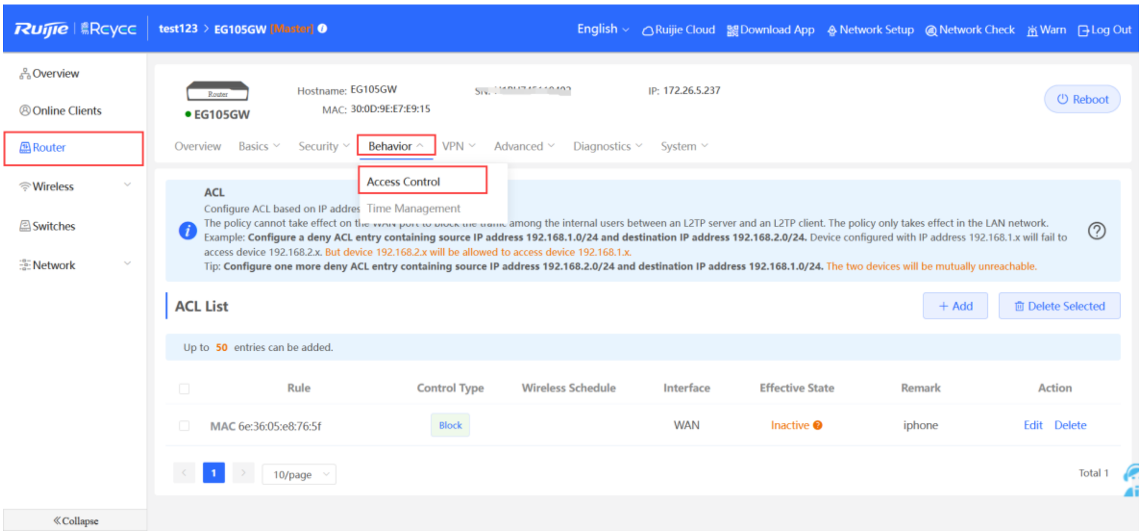
Wi-Fi List Device Group: Default

+ Add

Up to 8 SSIDs can be added.

SSID	Band	Security	Hidden	VLAN ID	Action
RAP2	2.4G + 5G	WPA_WPA2-PSK	No	10	Edit Delete
Internal_network_Reyee	2.4G + 5G	WPA_WPA2-PSK	No	6	Edit Delete
Guest_WiFi_Reyee	2.4G + 5G	WPA_WPA2-PSK	No	7	Edit Delete

(5) Choose **Router** > **Behavior** > **Access Control**, configure an ACL to block traffic from guests on network segment 192.168.7.0/24 in VLAN 7 to internal users on network segment 192.168.6.0/24 in VLAN 6, and apply the ACL to a LAN interface on the EG.



● EG105GW Hostname: EG105GW MAC: 30:0D:9E:E7:E9:15 SN: [redacted] IP: 172.26.5.237

ACL

Configure ACL based on IP addres

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 in 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.

Tip: **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.

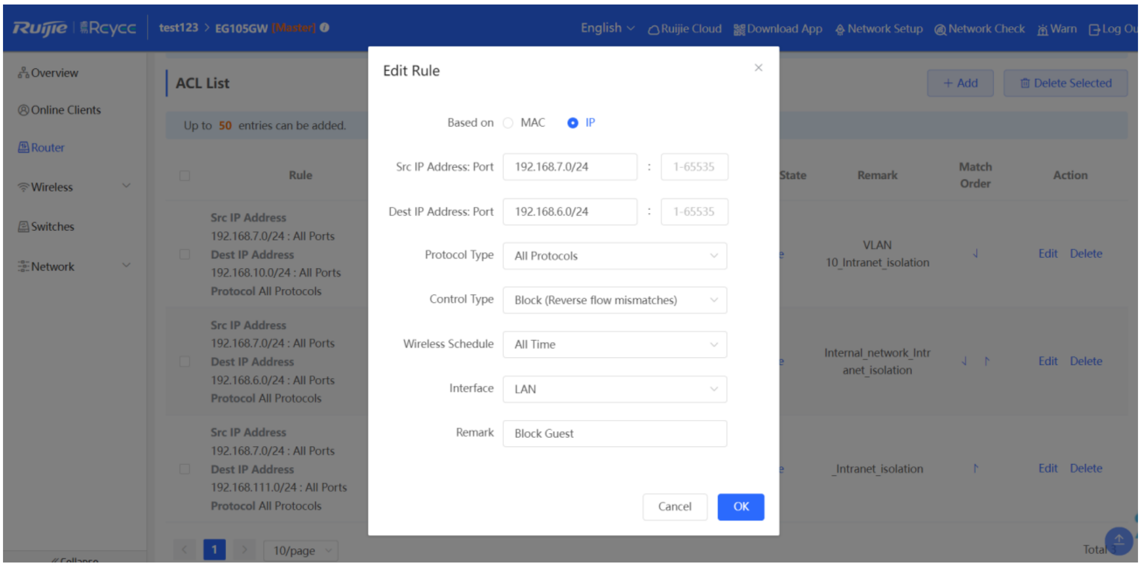
ACL List

+ Add Delete Selected

Up to 50 entries can be added.

□	Rule	Control Type	Wireless Schedule	Interface	Effective State	Remark	Action
□	MAC 6e:36:05:e8:76:5f	Block		WAN	Inactive	iphone	Edit Delete

1 10/page Total 1



Ruijie | Reyee
test123 > EG105GW [Master]
English
Ruijie Cloud
Download App
Network Setup
Network Check
Warn
Log Ou
Overview
Online Clients
Router
Wireless
Switches
Network
Collapse
ACL List
+ Add
Delete Selected
Up to 50 entries can be added.
Rule
State
Remark
Match Order
Action
Src IP Address 192.168.7.0/24 : All Ports Dest IP Address 192.168.10.0/24 : All Ports Protocol All Protocols
VLAN 10_Intranet_isolation
Edit Delete
Src IP Address 192.168.7.0/24 : All Ports Dest IP Address 192.168.6.0/24 : All Ports Protocol All Protocols
Internal_network_Intranet_isolation
Edit Delete
Src IP Address 192.168.7.0/24 : All Ports Dest IP Address 192.168.111.0/24 : All Ports Protocol All Protocols
_Intranet_isolation
Edit Delete
10/page
Total

Edit Rule

Based on ○ MAC ● IP

Src IP Address: Port 192.168.7.0/24 : 1-65535

Dest IP Address: Port 192.168.6.0/24 : 1-65535

Protocol Type All Protocols

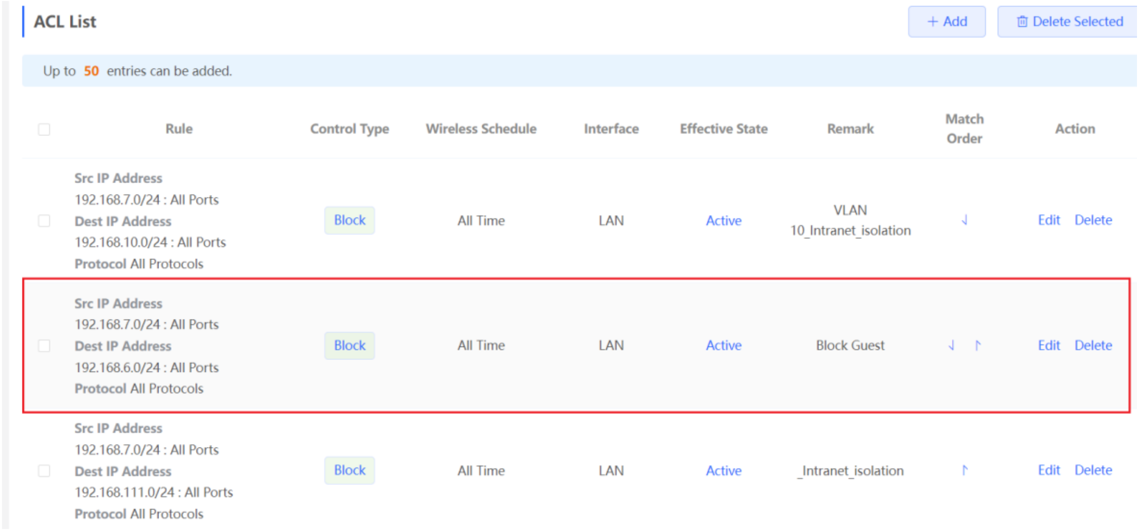
Control Type Block (Reverse flow mismatches)

Wireless Schedule All Time

Interface LAN

Remark Block Guest

Cancel OK



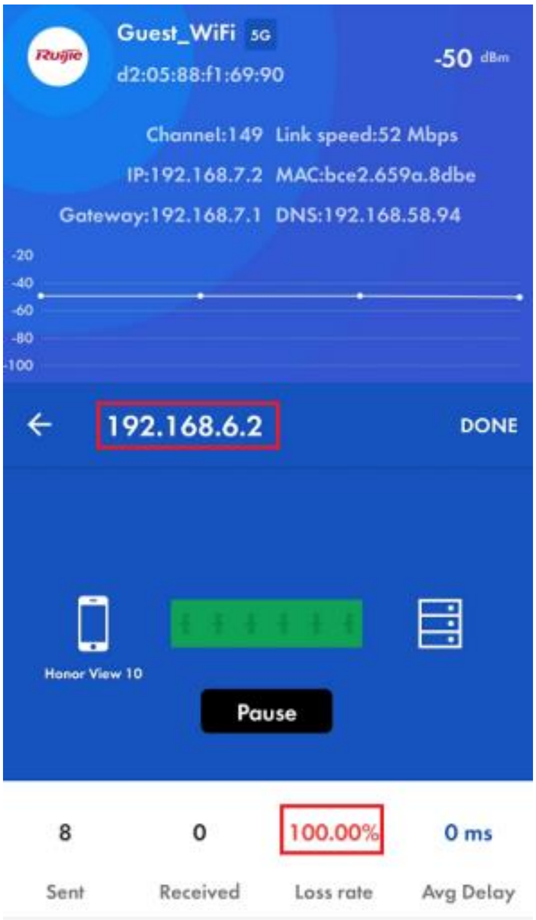
ACL List

Up to 50 entries can be added.

□	Rule	Control Type	Wireless Schedule	Interface	Effective State	Remark	Match Order	Action
□	Src IP Address 192.168.7.0/24 : All Ports Dest IP Address 192.168.10.0/24 : All Ports Protocol All Protocols	Block	All Time	LAN	Active	VLAN 10_Intranet_isolation	↓	Edit Delete
□	Src IP Address 192.168.7.0/24 : All Ports Dest IP Address 192.168.6.0/24 : All Ports Protocol All Protocols	Block	All Time	LAN	Active	Block Guest	↓ ↑	Edit Delete
□	Src IP Address 192.168.7.0/24 : All Ports Dest IP Address 192.168.111.0/24 : All Ports Protocol All Protocols	Block	All Time	LAN	Active	_Intranet_isolation	↑	Edit Delete

Configuration Verification

Guests at 192.1687.2 cannot access the internal users at 192.168.6.2.



Guest_WiFi 5G
d2:05:88:f1:69:90
-50 dBm

Channel:149 Link speed:52 Mbps
IP:192.168.7.2 MAC:bce2.659a.8dbe
Gateway:192.168.7.1 DNS:192.168.58.94

192.168.6.2

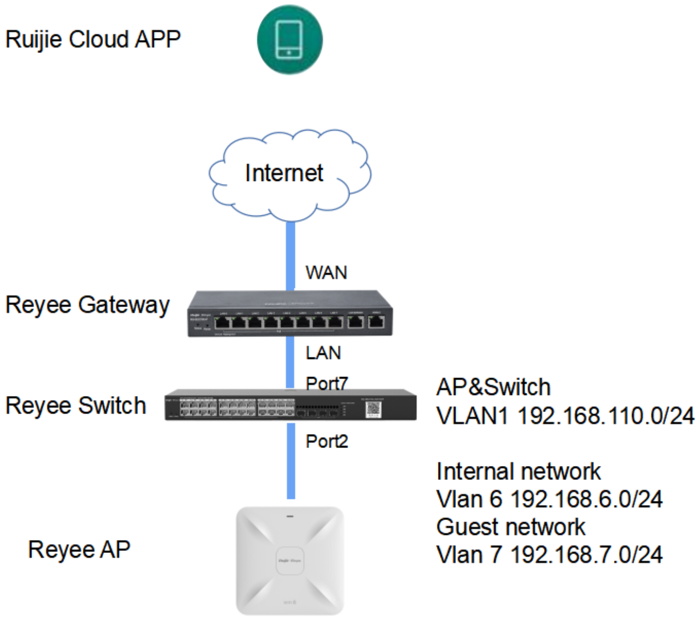
8	0	100.00%	0 ms
Sent	Received	Loss rate	Avg Delay

Configuration Through Ruijie Cloud App

Requirement

Guest Wi-Fi needs to be configured through Ruijie Cloud App for guests in VLAN 7, so guests are not allowed to access the internal network in VLAN 6. Ruijie Cloud App will deliver the corresponding configuration to the gateway, switch, and AP automatically.

Network Topology



Network Description:

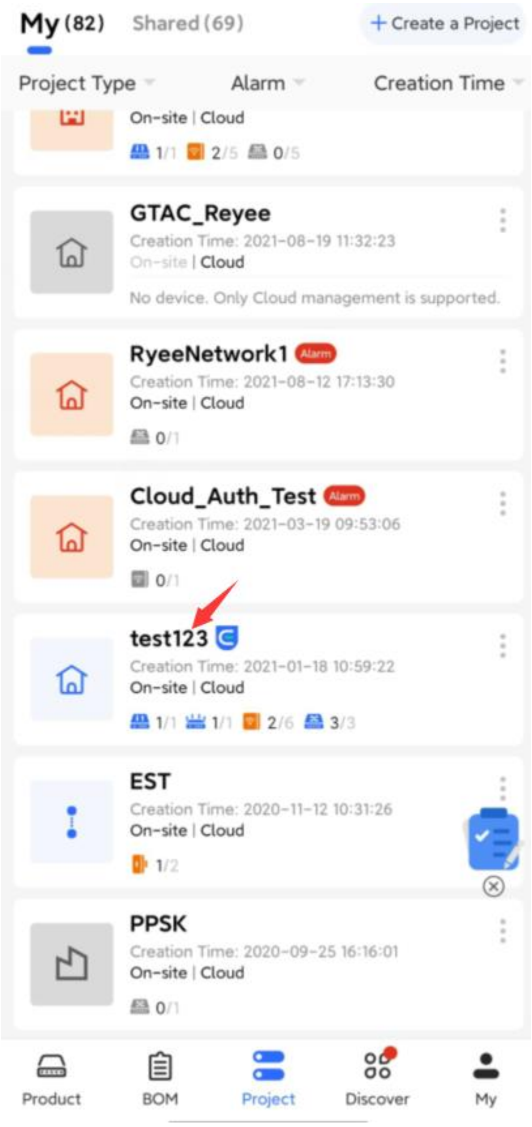
The EG works as a DHCP server to assign IP addresses to users, Reyee AP, and Reyee switch.

The AP and switch obtain IP addresses in VLAN 1 for Internet access.

Internal users obtain IP addresses in VLAN 6 for Internet access, and guests obtain IP addresses in VLAN 7 for Internet access.

Configuration Steps

(1) Log in to your Ruijie Cloud App on your smartphone, and then access the project through Reyee gateway and RAP.



My (82) Shared (69) + Create a Project

Project Type Alarm Creation Time

On-site | Cloud
1/1 2/5 0/5

GTAC_Reyee
Creation Time: 2021-08-19 11:32:23
On-site | Cloud
No device. Only Cloud management is supported.

RyeeNetwork1 Alarm
Creation Time: 2021-08-12 17:13:30
On-site | Cloud
0/1

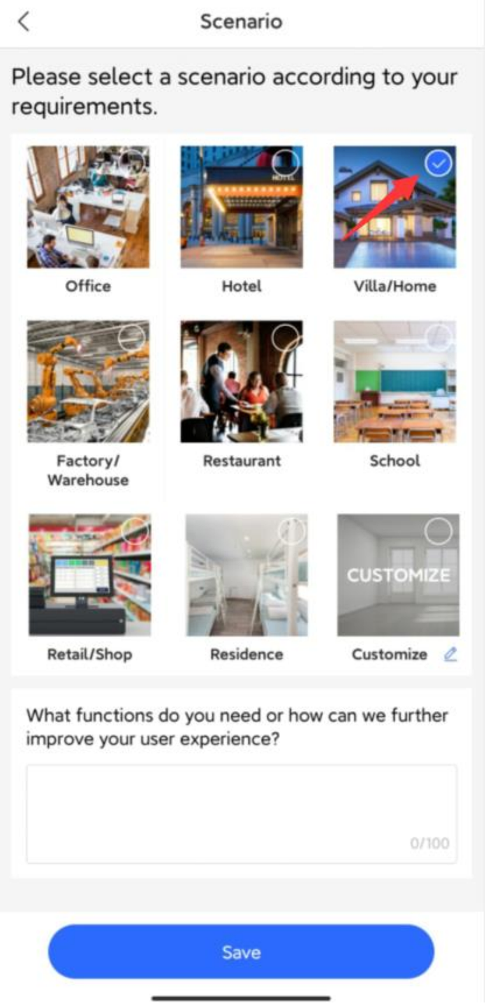
Cloud_Auth_Test Alarm
Creation Time: 2021-03-19 09:53:06
On-site | Cloud
0/1

test123
Creation Time: 2021-01-18 10:59:22
On-site | Cloud
1/1 1/1 2/6 3/3

EST
Creation Time: 2020-11-12 10:31:26
On-site | Cloud
1/2

PPSK
Creation Time: 2020-09-25 16:16:01
On-site | Cloud
0/1

(2) Choose **Villa/Home**. Then you can check the **Guest Wi-Fi** button.



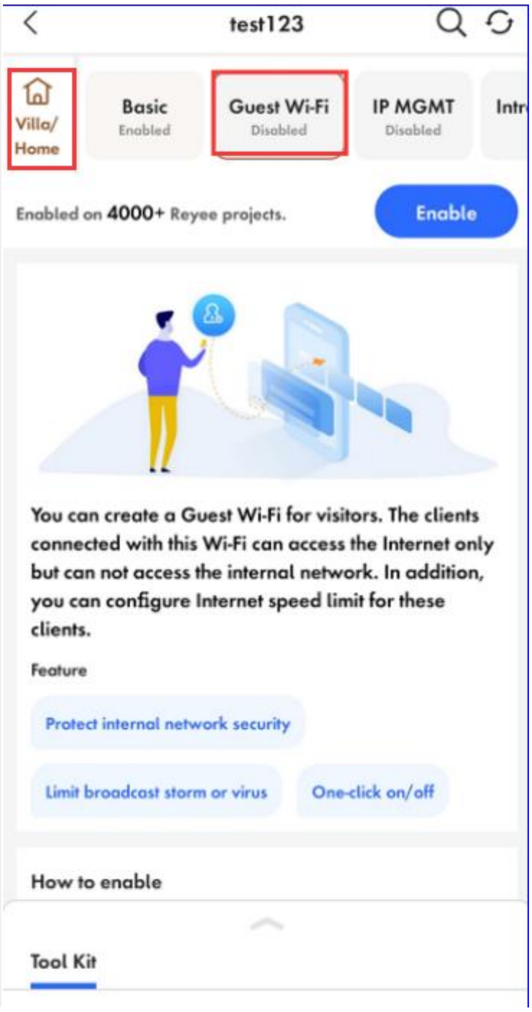
Scenario

Please select a scenario according to your requirements.

What functions do you need or how can we further improve your user experience?

0/100

Save



test123

Enabled on 4000+ Reyee projects.

Enable

You can create a Guest Wi-Fi for visitors. The clients connected with this Wi-Fi can access the Internet only but can not access the internal network. In addition, you can configure Internet speed limit for these clients.

Feature

Protect internal network security

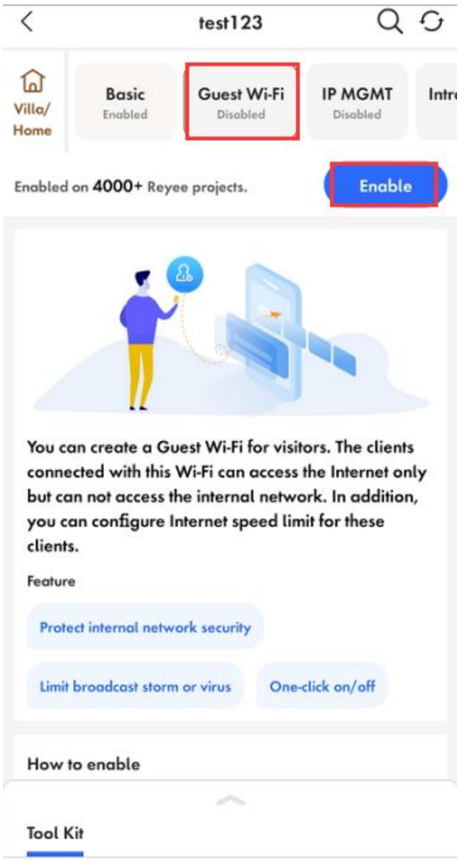
Limit broadcast storm or virus

One-click on/off

How to enable

Tool Kit

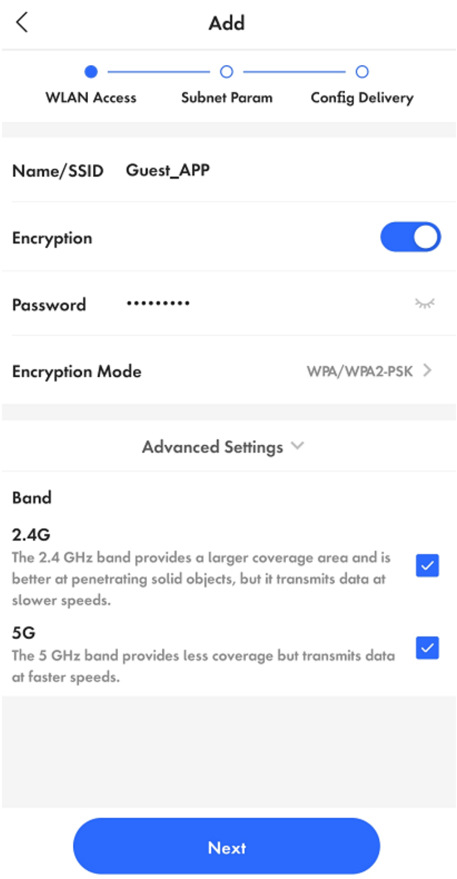
(3) Select **Guest Wi-Fi** and click **Enable**.



Enabled on 4000+ Reyee projects.

You can create a Guest Wi-Fi for visitors. The clients connected with this Wi-Fi can access the Internet only but can not access the internal network. In addition, you can configure Internet speed limit for these clients.

(4) Modify guest Wi-Fi information, configure an internal user SSID named **Guest_APP** and associate VLAN 6 with this SSID, configure a guest Wi-Fi SSID named **Guest_WiFi** and associate VLAN 7 with this SSID, and Click **Save** to save your configuration.



Name/SSID Guest_APP

Encryption ●

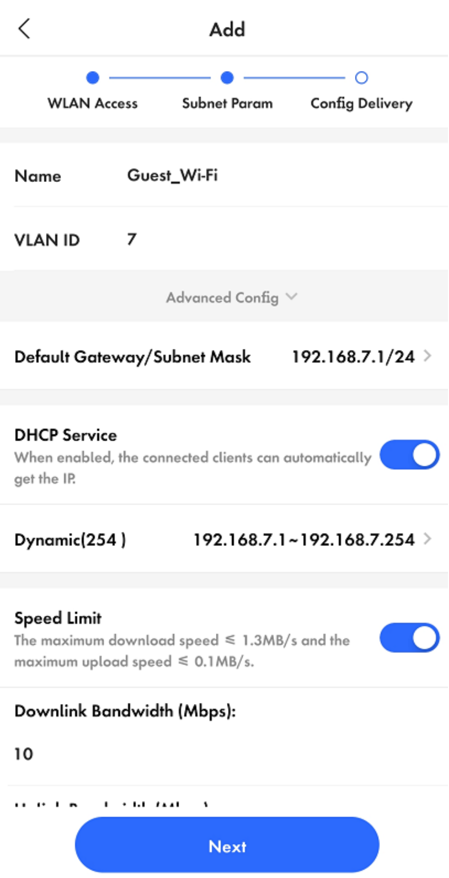
Password •••••••••

Encryption Mode WPA/WPA2-PSK >

Band

2.4G
The 2.4 GHz band provides a larger coverage area and is better at penetrating solid objects, but it transmits data at slower speeds. ☑

5G
The 5 GHz band provides less coverage but transmits data at faster speeds. ☑



Name Guest_Wi-Fi

VLAN ID 7

Default Gateway/Subnet Mask 192.168.7.1/24 >

DHCP Service
When enabled, the connected clients can automatically get the IP. ●

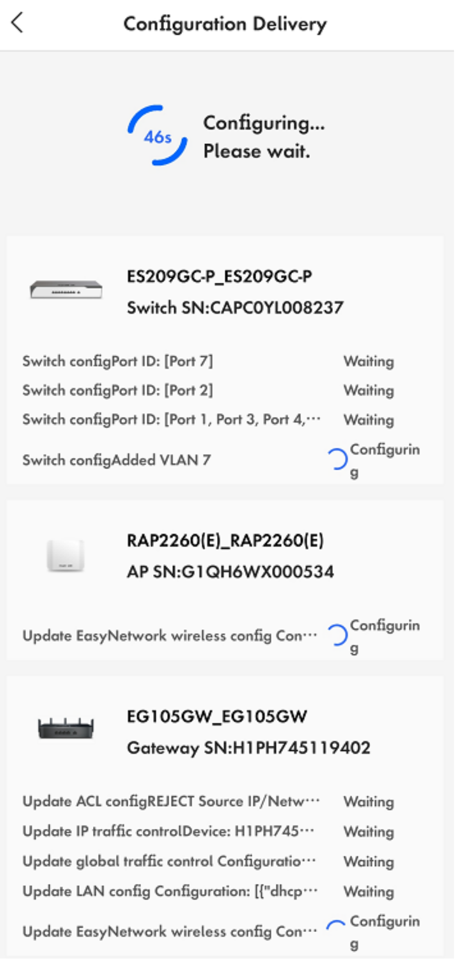
Dynamic(254) 192.168.7.1~192.168.7.254 >

Speed Limit
The maximum download speed ≤ 1.3MB/s and the maximum upload speed ≤ 0.1MB/s. ●

Downlink Bandwidth (Mbps):

10

(5) Wait for about 1 minute for the system to deliver the configuration to the device.


Configuration Delivery

46s Configuring... Please wait.

ES209GC-P_ES209GC-P
Switch SN:CAPC0YL008237

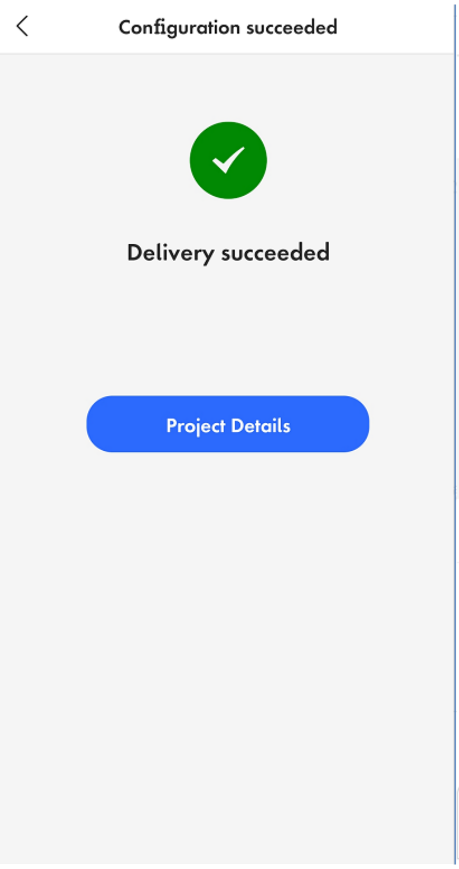
Switch configPort ID: [Port 7] Waiting
Switch configPort ID: [Port 2] Waiting
Switch configPort ID: [Port 1, Port 3, Port 4,⋯ Waiting
Switch configAdded VLAN 7 Configurin g

RAP2260(E)_RAP2260(E)
AP SN:G1QH6WX000534

Update EasyNetwork wireless config Con⋯ Configurin g

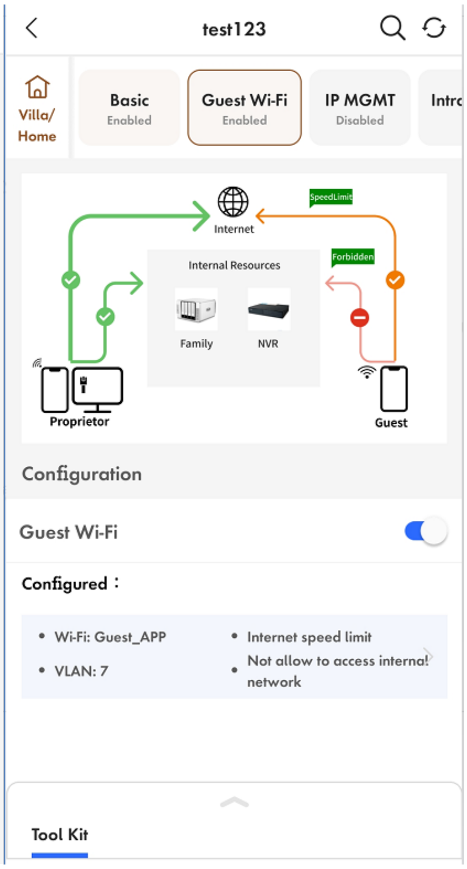
EG105GW_EG105GW
Gateway SN:H1PH745119402

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⋯ Configurin g


Configuration succeeded

Delivery succeeded

Project Details


test123

Villa/ Home | Basic Enabled | Guest Wi-Fi Enabled | IP MGMT Disabled | Intr

Configuration

Guest Wi-Fi

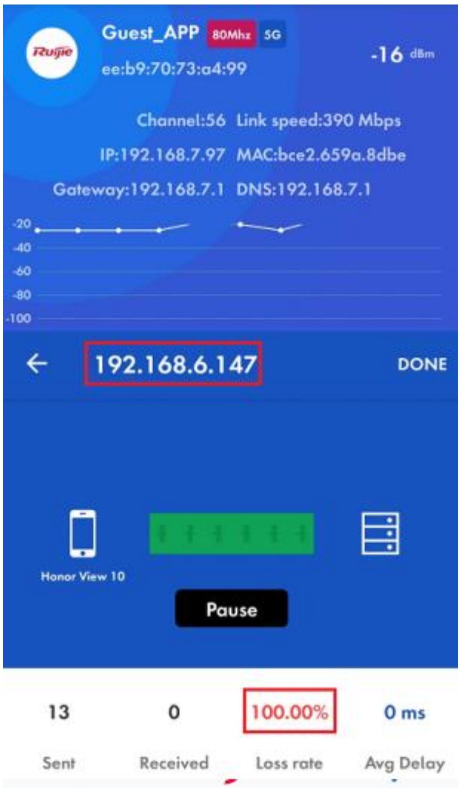
Configured：

- Wi-Fi: Guest_APP
- VLAN: 7
- Internet speed limit
- Not allow to access internal network

Tool Kit

Configuration Verification

The guest at 192.168.7.97 cannot access the internal user at 192.168.6.147.



Guest_APP

ee:b9:70:73:a4:99

-16 dBm

Channel:56 Link speed:390 Mbps

IP:192.168.7.97 MAC:bce2.659a.8dbe

Gateway:192.168.7.1 DNS:192.168.7.1

192.168.6.147

Sent	Received	Loss rate	Avg Delay
13	0	100.00%	0 ms

5.4 Reyee SON

SON eliminates 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 mobile APP, you can quickly complete device deployment and configuration, remote management, O&M of the entire network, which greatly reduces the investment of the device, labor, and time cost during wireless network construction.

5.4.1 Working Mechanism of Reyee SON

Network ID

Every device has its own network ID.

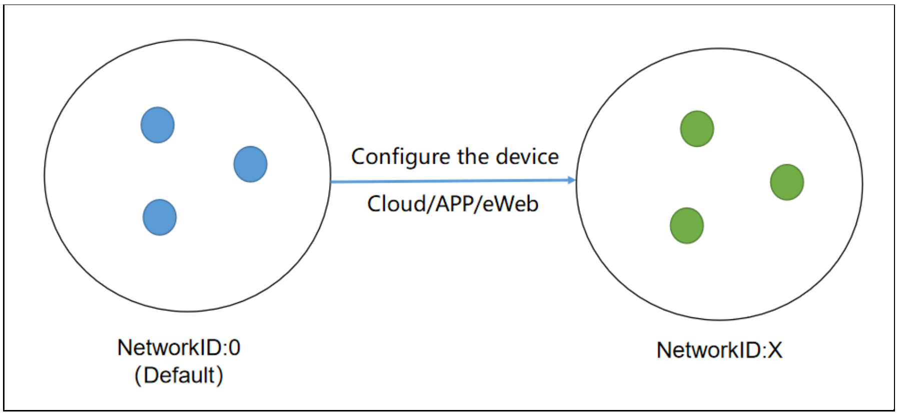
Only devices with the same network ID can be added to a network.

Different network IDs of devices are required to be merged before the devices are added to the same network.

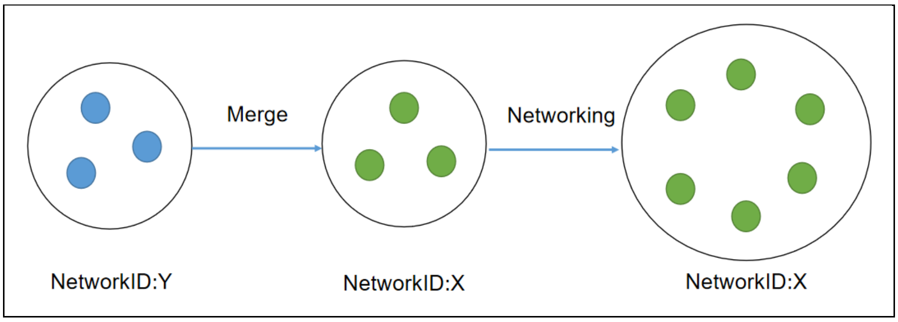
The network ID is 0 by default.

After the device is configured, it will have a new network ID (non-zero value).

After configuration:



Merge:



Protocol

Easydisc

Easydisc provides neighbor discovery, master election, and notification of master changes.

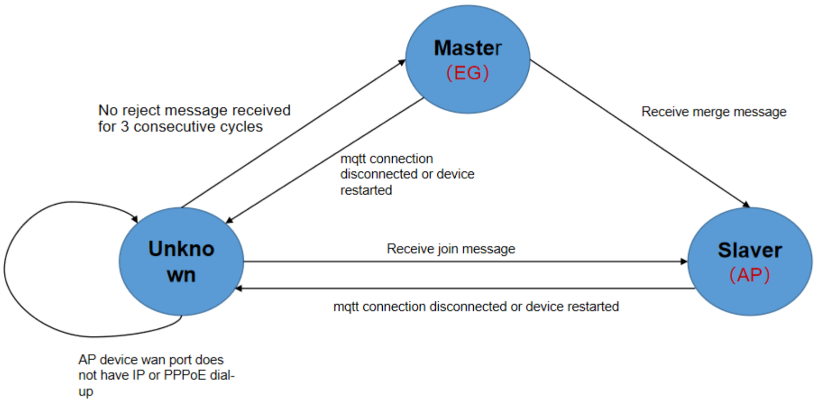
Easydisc is a proprietary protocol and uses UDP port numbers 43561 and 43562 for communication.

MQTT

MQTT collects information about network devices and STAs, and synchronizes the configuration.

MQTT is a standard protocol and uses TCP port number 1883 for communication.

Easydisc - Role


Master
(EG)
No reject message received for 3 consecutive cycles
Receive merge message
mqtt connection disconnected or device restarted
Unkno wn
Slaver
(AP)
Receive join message
mqtt connection disconnected or device restarted
AP device wan port does not have IP or PPPoE dial-up

Easydisc - Packets

Packet types:

Declare: In Initial state, the device broadcasts Declare packets and sends its own priority and other related information.

Reject: When receiving a decade packet in unicast mode, the device with a higher priority sends a Reject packet according to the election priority.

Join: The Join packet is broadcast by the master. When other devices in initial state receive the packet, they will connect to the master according to master information in it.

Conflict: The master sends a Conflict packet in unicast mode when receiving a Join packet from another master. As a result, the slave cannot resolve the packet according to the conflict handling algorithm.

Merge: The master sends a Merge packet in unicast mode when receiving a Join packet from other master devices. In this case, the master combines Join packets from other masters according to the conflict handling algorithm.

Hello: All devices start broadcasting Hello packets after the role status is confirmed for neighbor discovery.

Master Election

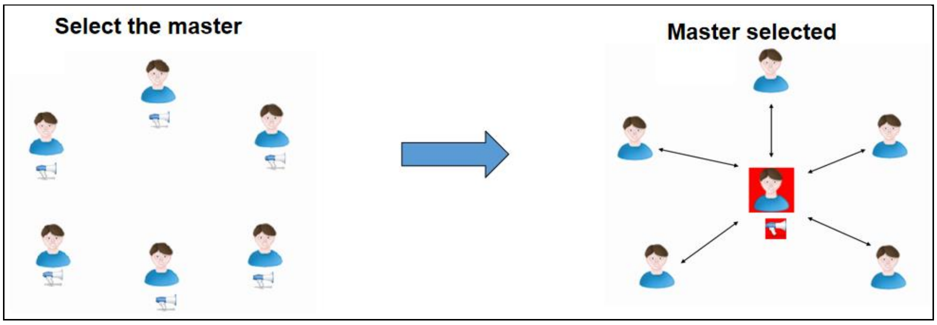
Priority:

(1) EG > AP > switch

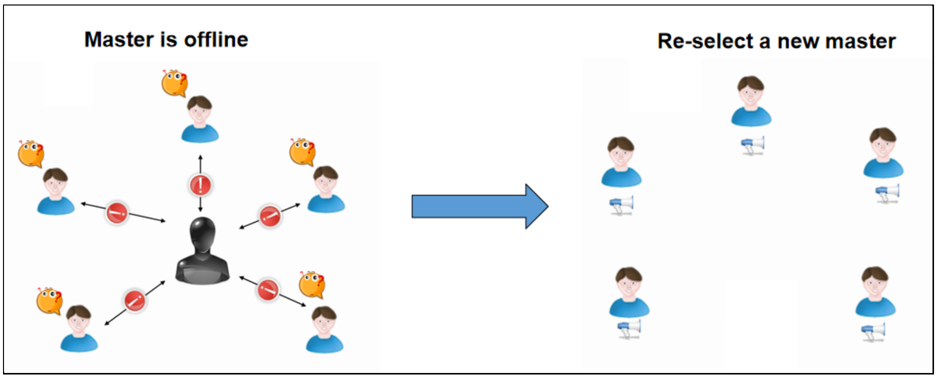
(2) Device model: device CPU/memory/other information (AP radio number)

(3) When the priorities are the same, the device with a larger MAC address will be the master.

Select the master.



Re-select the master.



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.

- For AP networking, after the master is selected, if a new EG is added, the EG will become the master. Preemption time: 7-8s
- For AP networking, after the master is selected, if a new AP with a higher priority is added, the preemption is delayed.

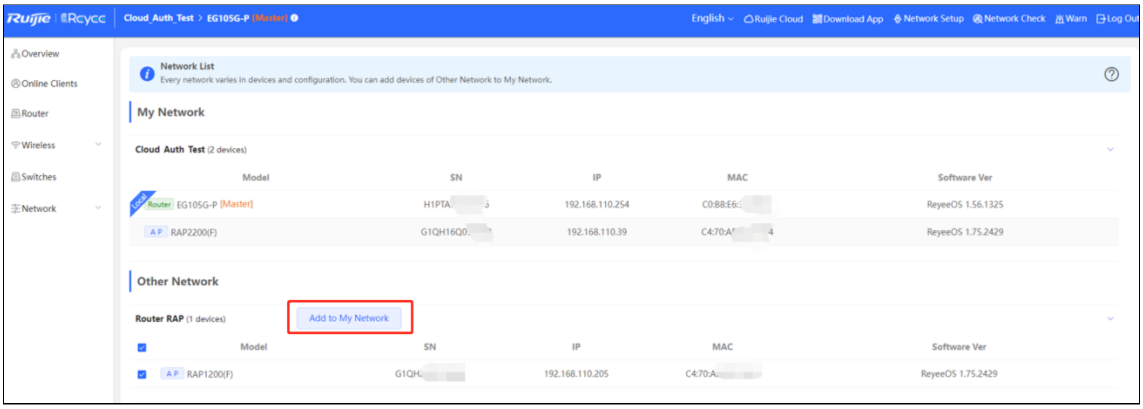
Preemption time: Preemption starts after the master is powered on for 36 hours and the new device is powered on for 5 minutes. Otherwise, preemption starts after the new device is powered on for 30 minutes.

- For networking with the AP and switch, after the master is selected, if a new EG is added, the EG will become the master.

5.4.2 Reyee SON Configuration

Neighbor Discovery

Add devices of other networks to **My Network**.



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

My Network

Cloud Auth Test (2 devices)

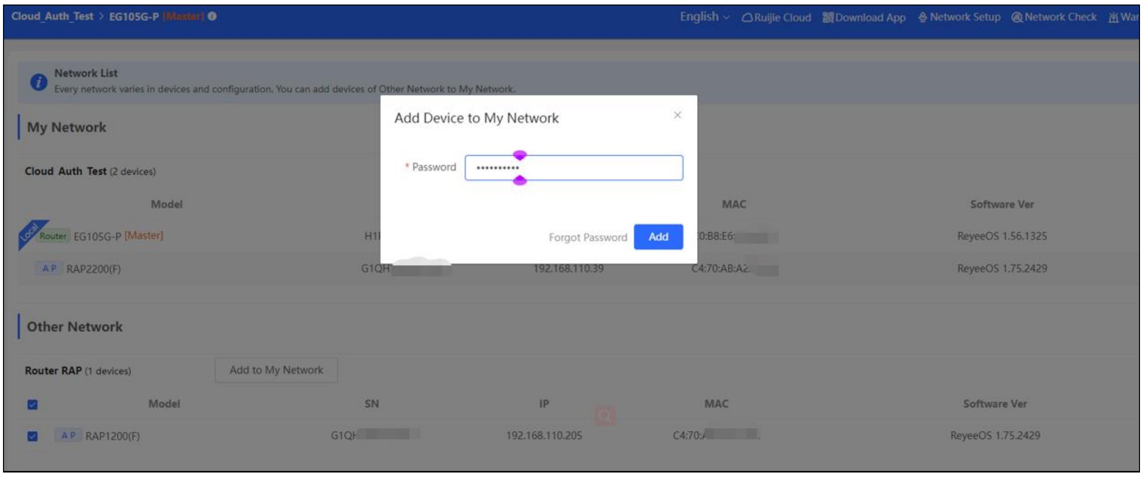
Model	SN	IP	MAC	Software Ver
Router EG105G-P [Master]	H1PTA[redacted]5	192.168.110.254	C0:B8:E6:[redacted]	ReyeeOS 1.56.1325
AP RAP2200(F)	G1QH16Q0[redacted]	192.168.110.39	C4:70:A[redacted]4	ReyeeOS 1.75.2429

Other Network

Router RAP (1 devices)

☑	Model	SN	IP	MAC	Software Ver
☑	AP RAP1200(F)	G1QH[redacted]	192.168.110.205	C4:70:A[redacted]	ReyeeOS 1.75.2429

Enter the device password.



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

Add Device to My Network

* Password ••••••••••••

My Network

Cloud Auth Test (2 devices)

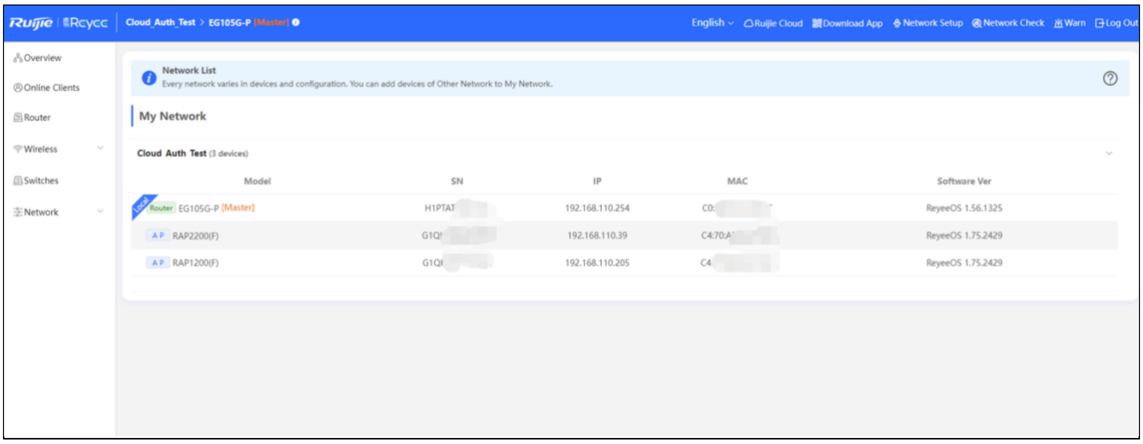
Model	SN	IP	MAC	Software Ver
Router EG105G-P [Master]	H1		0:B8:E6:[redacted]	ReyeeOS 1.56.1325
AP RAP2200(F)	G1QH[redacted]	192.168.110.39	C4:70:AB:A2[redacted]	ReyeeOS 1.75.2429

Other Network

Router RAP (1 devices)

☑	Model	SN	IP	MAC	Software Ver
☑	AP RAP1200(F)	G1QH[redacted]	192.168.110.205	C4:70:A[redacted]	ReyeeOS 1.75.2429

The device is added to the network.



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

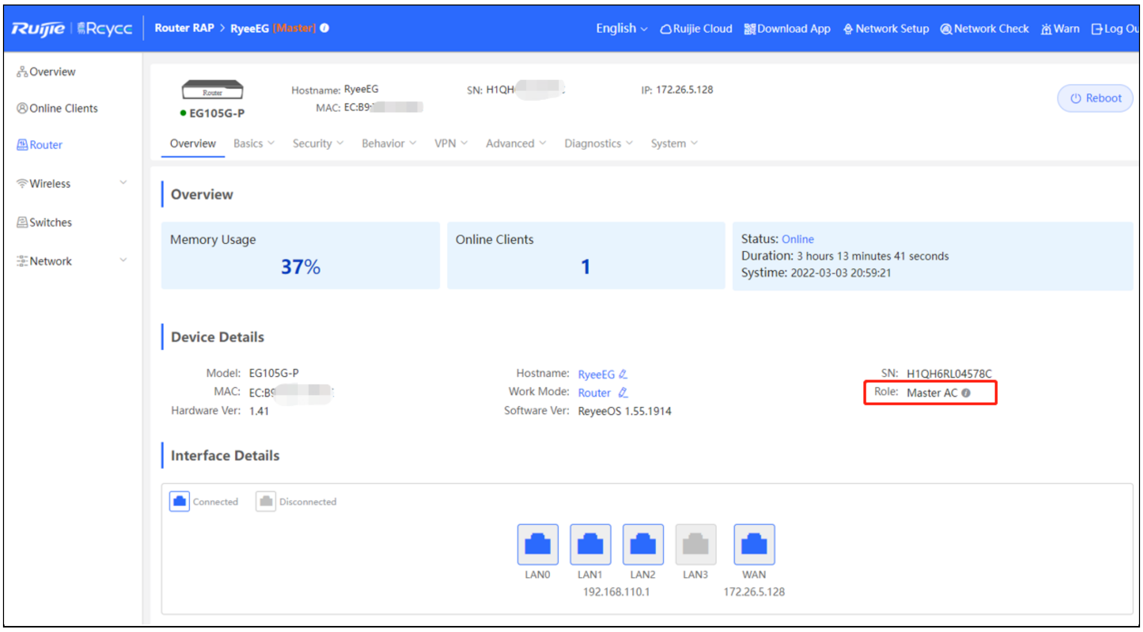
My Network

Cloud Auth Test (3 devices)

Model	SN	IP	MAC	Software Ver
Router EG105G-P [Master]	H1PTAT[redacted]	192.168.110.254	C0:[redacted]	ReyeeOS 1.56.1325
AP RAP2200(F)	G1Q[redacted]	192.168.110.39	C4:70:A[redacted]	ReyeeOS 1.75.2429
AP RAP1200(F)	G1Q[redacted]	192.168.110.205	C4[redacted]	ReyeeOS 1.75.2429

Device Networking Role

Master:



EG105G-P

Hostname: RyeeEG

MAC: EC:B9:[redacted]

SN: H1QH[redacted]

IP: 172.26.5.128

Overview

Memory Usage 37%

Online Clients 1

Status: Online
Duration: 3 hours 13 minutes 41 seconds
Systime: 2022-03-03 20:59:21

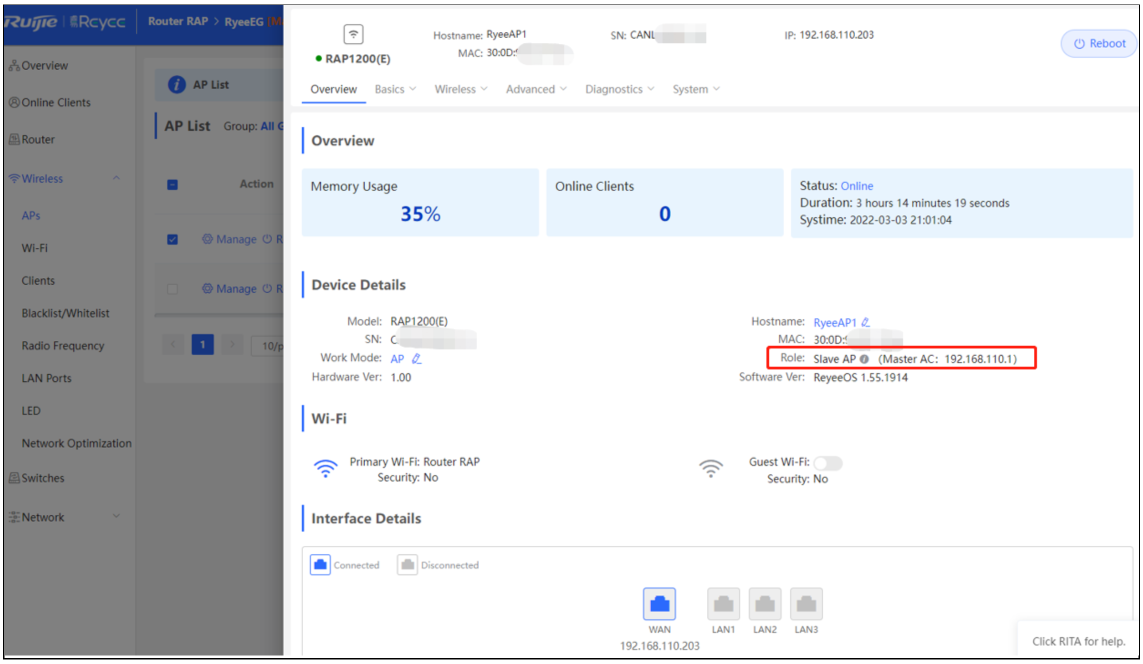
Device Details

Model: EG105G-P
MAC: EC:B9[redacted]
Hardware Ver: 1.41
Hostname: RyeeEG
Work Mode: Router
Software Ver: ReyeeOS 1.55.1914
SN: H1QH6RL04578C
Role: Master AC

Interface Details

LAN0 LAN1 LAN2 LAN3 WAN
192.168.110.1 172.26.5.128

Slave:



RAP1200(E)

Hostname: RyeeAP1

MAC: 30:0D:[redacted]

SN: CANL[redacted]

IP: 192.168.110.203

Overview

Memory Usage 35%

Online Clients 0

Status: Online
Duration: 3 hours 14 minutes 19 seconds
Systime: 2022-03-03 21:01:04

Device Details

Model: RAP1200(E)
SN: C[redacted]
Work Mode: AP
Hardware Ver: 1.00
Hostname: RyeeAP1
MAC: 30:0D:[redacted]
Role: Slave AP (Master AC: 192.168.110.1)
Software Ver: ReyeeOS 1.55.1914

Wi-Fi

Primary Wi-Fi: Router RAP
Security: No

Guest Wi-Fi:
Security: No

Interface Details

WAN LAN1 LAN2 LAN3
192.168.110.203

5.4.3 SON Troubleshooting

Fault Symptom

The SON fails.

Cause

There are multiple masters, and more than one @Ruijie-mxxx SSID can be viewed.

Layer 2 broadcast becomes ineffective.

Solution

Check whether the devices are connected to and join the same network.

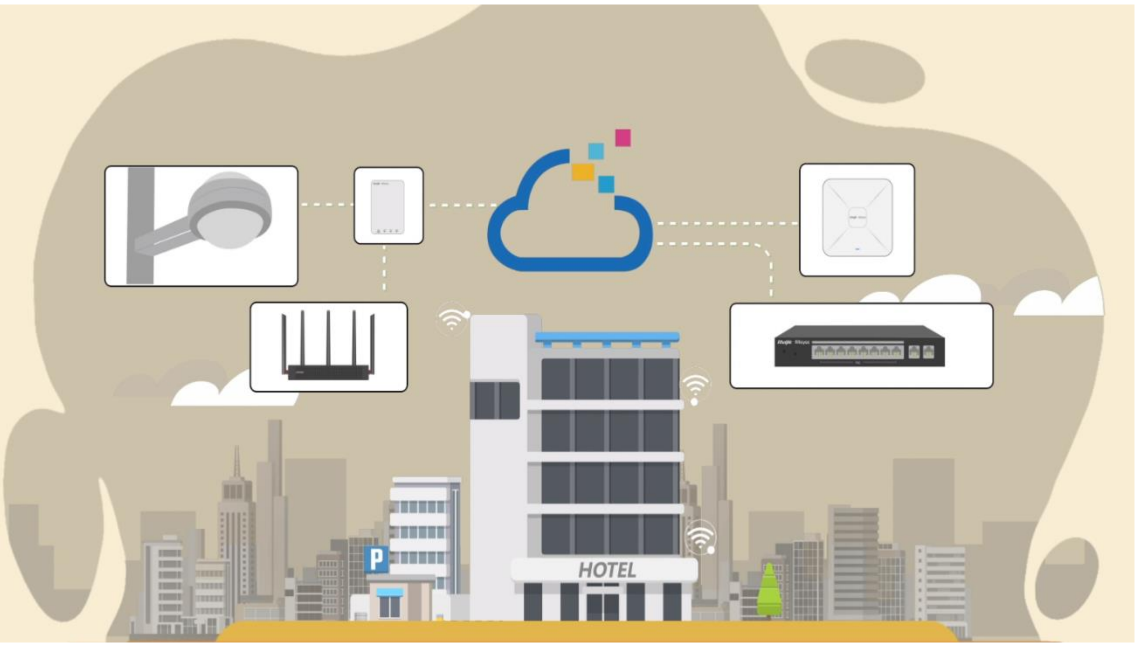
Check whether there are some configurations such as VLAN and port isolation.

Check whether the SON is disabled.

5.5 Reyee Economic Hotel Network Solution

5.5.1 Application Scenario

Reyee economic hotel network solution provides an affordable 5-star Wi-Fi for clients. The AP can operate concurrently at 2.4 GHz and 5 GHz, providing high-speed wireless access of 574 Mbit/s at 2.4 GHz, 1201 Mbit/s at 5 GHz, and up to 1775 Mbit/s. The wall AP provides a LAN port at the front to facilitate expansion of IPTV devices, IP phones, and other terminals.



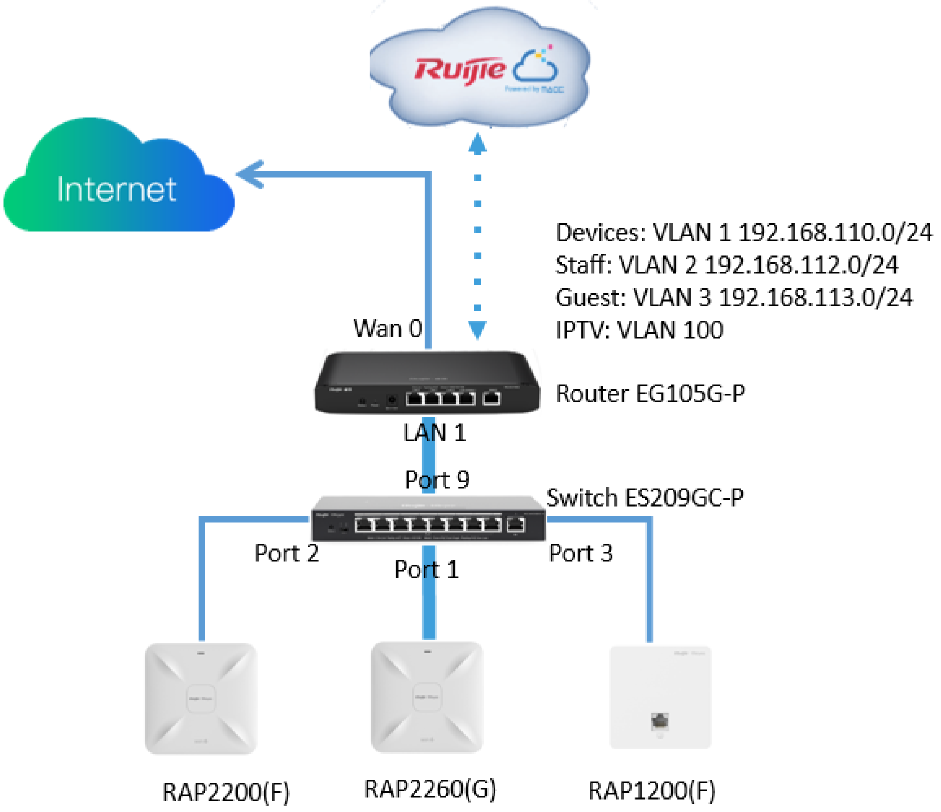
5.5.2 Configuration Case

Requirement

(1) On the wireless network for the hotel scenario, guests need to pass voucher authentication before accessing the Internet and are not allowed to access the internal network of the hotel.

(2) Wired connections are provided for IPTV.

Network Topology



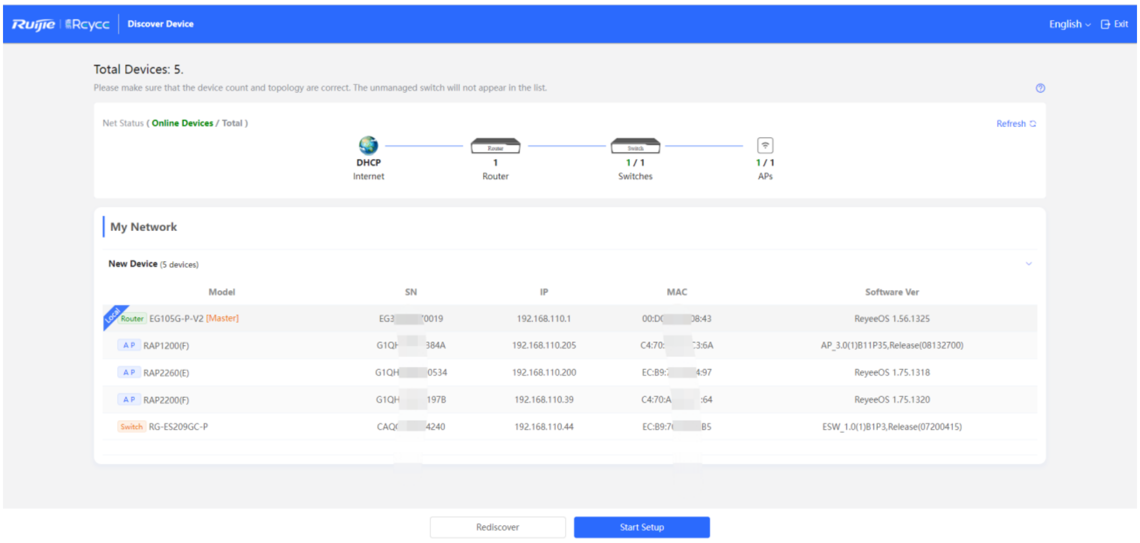
Devices List

Type	Model	Function
Gateway	EG105G-P	Connects to the Internet and works as the DHCP server for downlink devices and clients. Manages APs and switches locally. Supports voucher authentication with Ruijie Cloud.
Switch	ES209GC-P	Provides wired and PoE connections.
Wall AP	RAP1200(F)	Provides wireless connections for rooms. Provides wired connections for IPTV.
Indoor AP	RAP2200(F)&RAP2260(G)	Provides wireless connections for the hall and corridor.

Configuration Steps

(1) Power on and connect to the device according to the topology.

(2) The IP address of the access gateway is 192.168.110.1. Configure basic network settings according to **Start Setup**.



Total Devices: 5.

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

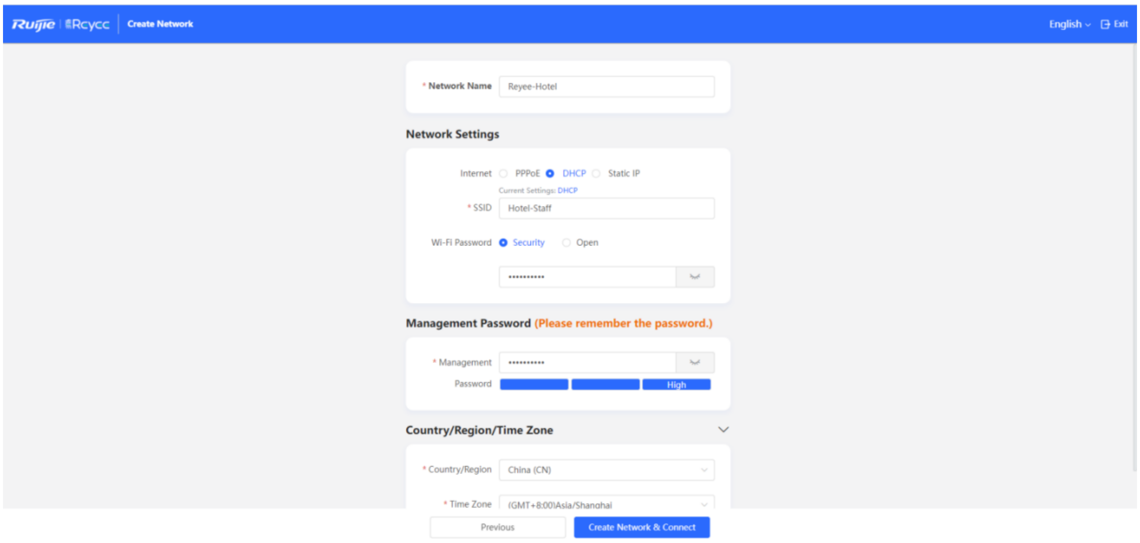
Net Status (Online Devices / Total)

My Network

New Device (5 devices)

Model	SN	IP	MAC	Software Ver
Router EG105G-P-V2 [Master]	EG3[redacted]0019	192.168.110.1	00:D[redacted]08:43	ReyeeOS 1.56.1325
AP RAP1200(F)	G1Q[redacted]384A	192.168.110.205	C4:70:[redacted]3:6A	AP_3.0(1)B11P35,Release(08132700)
AP RAP2260(E)	G1QH[redacted]0534	192.168.110.200	EC:B9:[redacted]4:97	ReyeeOS 1.75.1318
AP RAP2200(F)	G1QH[redacted]197B	192.168.110.39	C4:70:A[redacted]:64	ReyeeOS 1.75.1320
Switch RG-ES209GC-P	CAQ[redacted]4240	192.168.110.44	EC:B9:7[redacted]B5	ESW_1.0(1)B1P3,Release(07200415)

Set **Network Name**, **Network Settings**, and **SSID** for staffs and set **Management Password**.



* Network Name: Reyee-Hotel

Network Settings

Internet: ○ PPPoE ● DHCP ○ Static IP

Current Settings: DHCP

* SSID: Hotel-Staff

Wi-Fi Password: ● Security ○ Open

••••••••••

Management Password (Please remember the password.)

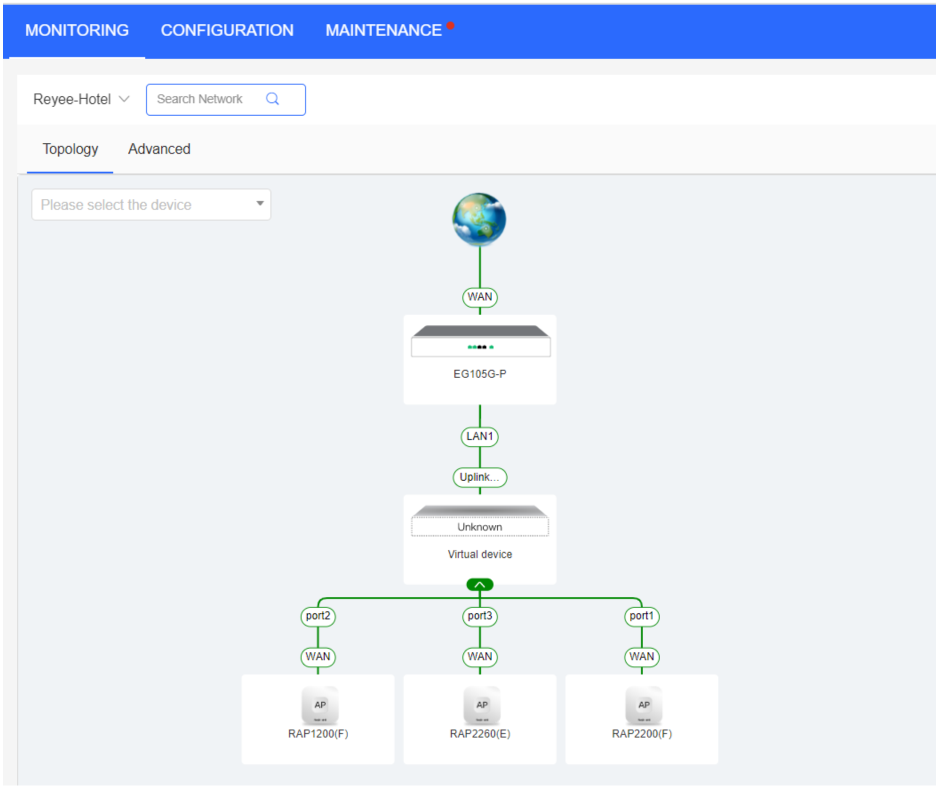
* Management Password: ••••••••••

Country/Region/Time Zone

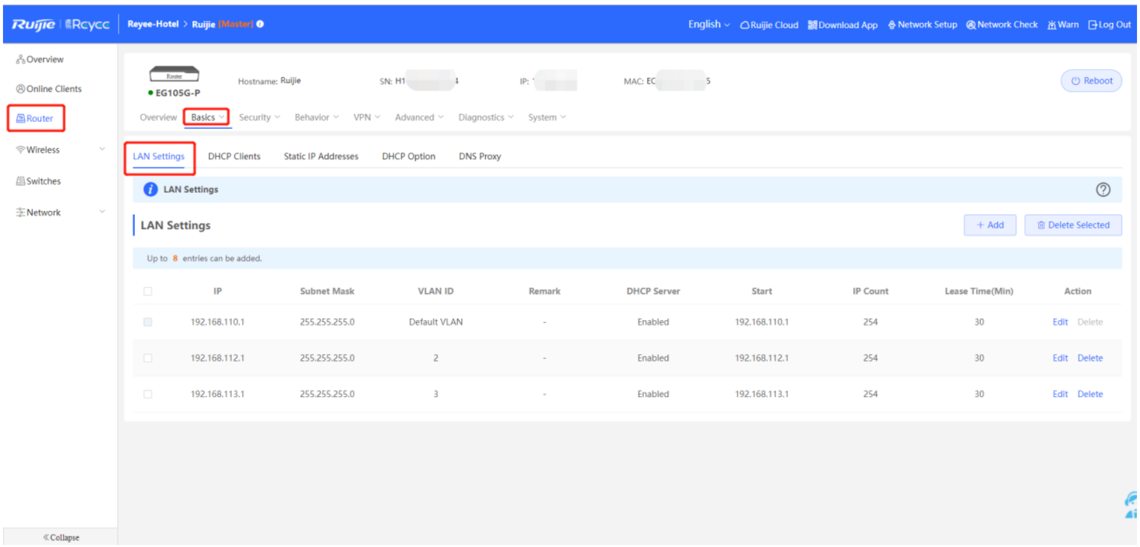
* Country/Region: China (CN)

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

Click **Create Network & Connect** to activate the configuration and add devices to Ruijie Cloud.



(3) Choose **Router > Basic > LAN** to create VLAN 2 and VLAN 3 for staffs and guests.



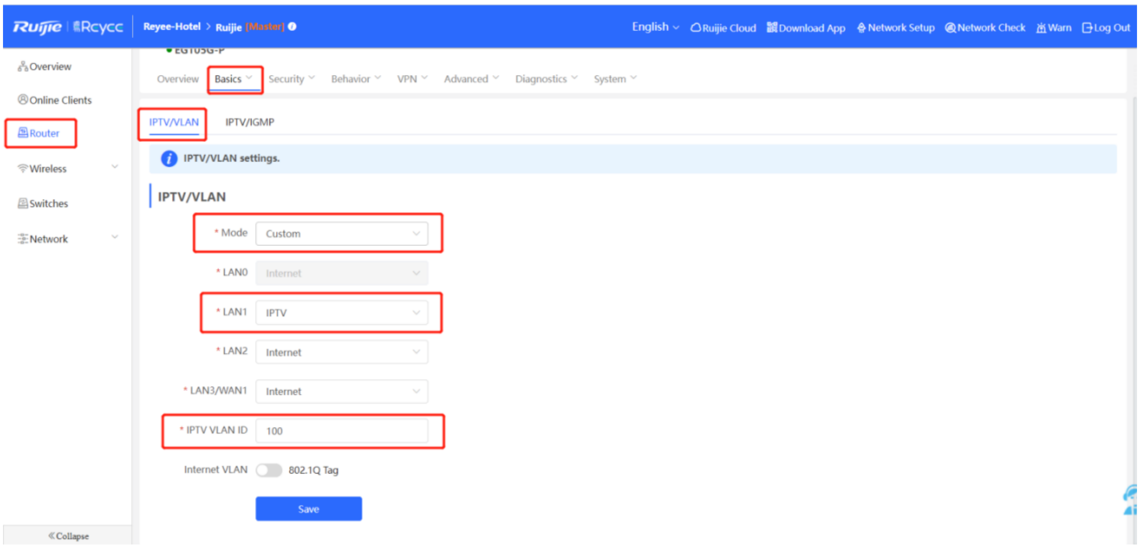
Hostname: Ruijie SN: [redacted] IP: [redacted] MAC: [redacted]

LAN Settings

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	254	30	Edit Delete
□	192.168.112.1	255.255.255.0	2	-	Enabled	192.168.112.1	254	30	Edit Delete
□	192.168.113.1	255.255.255.0	3	-	Enabled	192.168.113.1	254	30	Edit Delete

(4) Choose **Router > Basic > IPTV** to configure IPTV settings obtained from the ISP. For example, the IPTV VLAN ID is 100. Perform the operation as follows.



IPTV/VLAN settings.

IPTV/VLAN

* Mode: Custom

* LAN0: Internet

* LAN1: IPTV

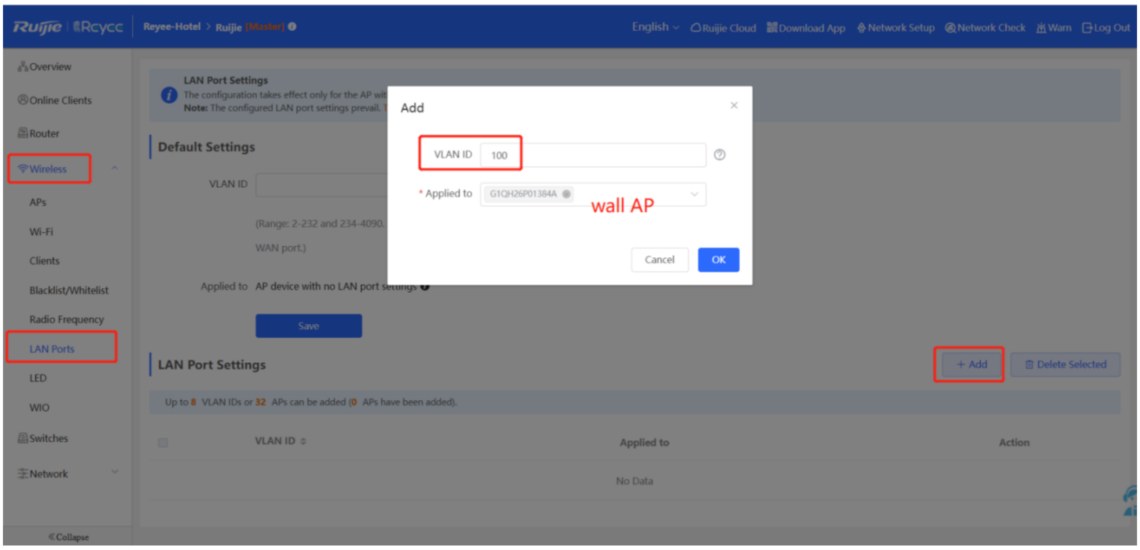
* LAN2: Internet

* LAN3/WAN1: Internet

* IPTV VLAN ID: 100

Internet VLAN: 802.1Q Tag

(5) Choose **WLAN > LAN Ports > Add** to configure VLAN 100 for IPTV. If default VLAN 1 is used, ignore this step.



LAN Port Settings
The configuration takes effect only for the AP wit
Note: The configured LAN port settings prevail.

Default Settings

VLAN ID
(Range: 2-232 and 234-4090. WAN port.)

Applied to: AP device with no LAN port settings

LAN Port Settings

Up to 8 VLAN IDs or 32 APs can be added (0 APs have been added).

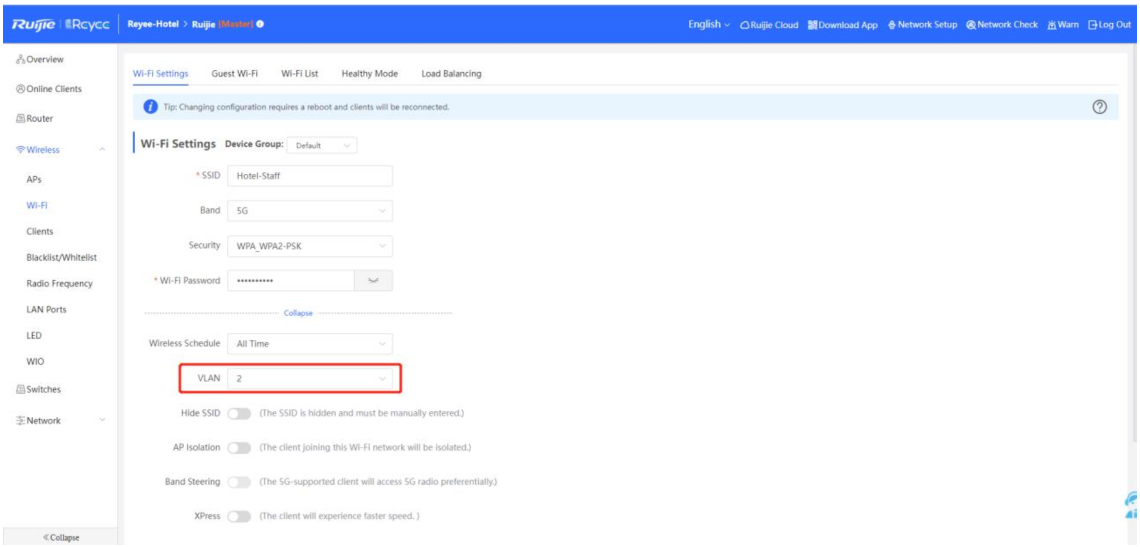
VLAN ID	Applied to	Action
No Data		

Add

VLAN ID: 100

* Applied to: G1QH26P01384A

(6) Choose **WLAN > Wi-Fi** to configure Wi-Fi for staffs and guests. Select VLAN 2 for staffs.



Tip: Changing configuration requires a reboot and clients will be reconnected.

Wi-Fi Settings Device Group: Default

* SSID: Hotel-Staff

Band: 5G

Security: WPA_WPA2-PSK

* Wi-Fi Password: ••••••••••

Wireless Schedule: All Time

VLAN: 2

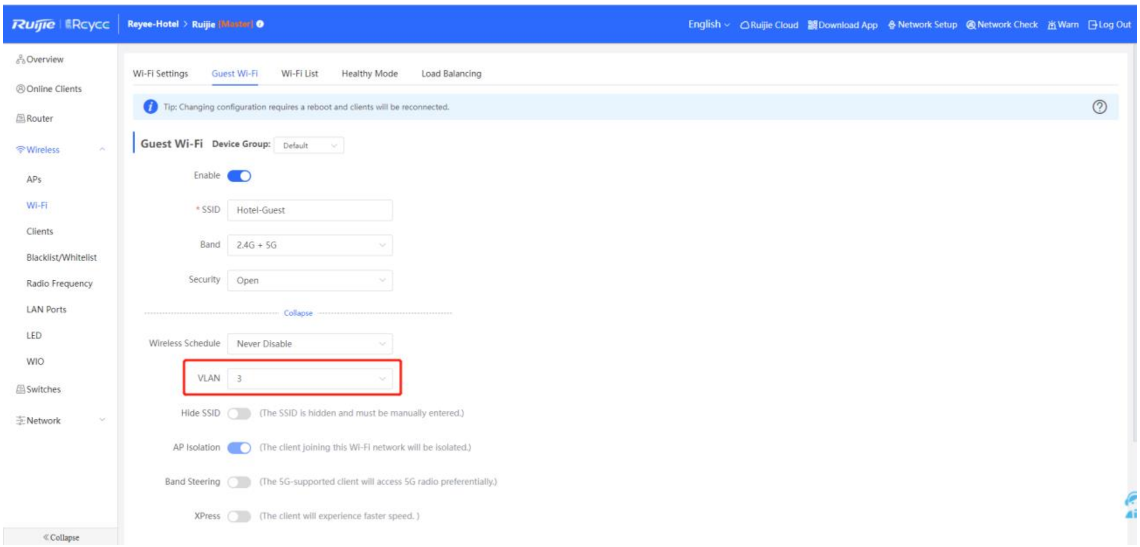
Hide SSID (The SSID is hidden and must be manually entered.)

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.)

(7) Enable guest Wi-Fi, and select VLAN 3 for it.



Tip: Changing configuration requires a reboot and clients will be reconnected.

Guest Wi-Fi Device Group: Default

Enable: on

SSID: Hotel-Guest

Band: 2.4G + 5G

Security: Open

Wireless Schedule: Never Disable

VLAN: 3

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

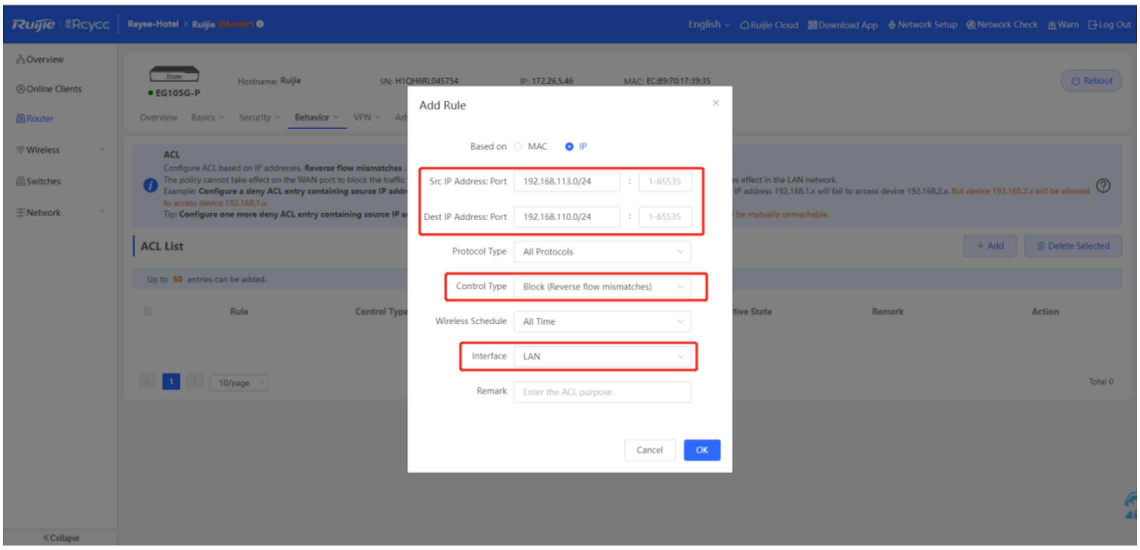
AP Isolation: on (The client joining this Wi-Fi network will be isolated.)

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

XPress: off (The client will experience faster speed.)

(8) Choose **Router > Behavior > Access Control**. Configure ACLs to block guests from accessing the internal network.

Add two ACLs and apply them to a LAN port to block devise in VLAN 3 from accessing users in VLAN 1 and VLAN 2.



Add Rule

Based on ○ MAC ● IP

Src IP Address: Port 192.168.113.0/24 : 1-65535

Dest IP Address: Port 192.168.110.0/24 : 1-65535

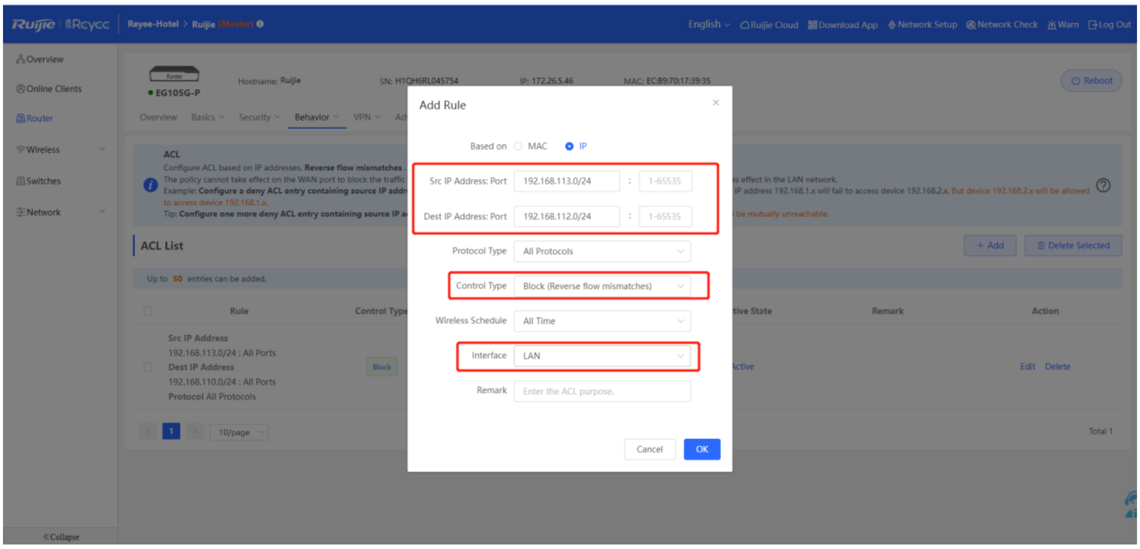
Protocol Type: All Protocols

Control Type: Block (Reverse flow mismatches)

Wireless Schedule: All Time

Interface: LAN

Remark: Enter the ACL purpose.



Add Rule

Based on ○ MAC ● IP

Src IP Address: Port 192.168.113.0/24 : 1-65535

Dest IP Address: Port 192.168.112.0/24 : 1-65535

Protocol Type: All Protocols

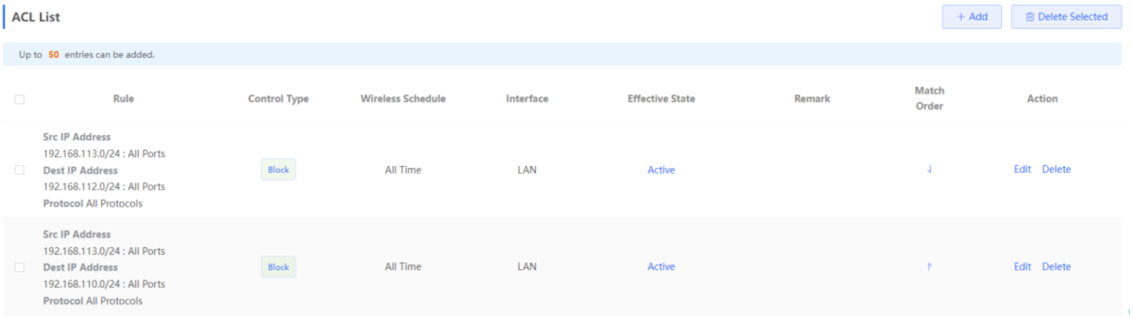
Control Type: Block (Reverse flow mismatches)

Wireless Schedule: All Time

Interface: LAN

Remark: Enter the ACL purpose.

Src IP Address 192.168.113.0/24 : All Ports Dest IP Address 192.168.110.0/24 : All Ports Protocol All Protocols | Block | Active | Edit Delete



ACL List

+ Add | Delete Selected

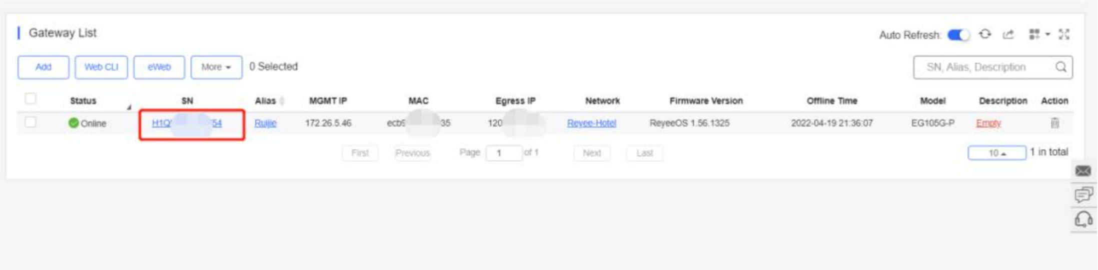
Up to 50 entries can be added.

□	Rule	Control Type	Wireless Schedule	Interface	Effective State	Remark	Match Order	Action
□	Src IP Address 192.168.113.0/24 : All Ports Dest IP Address 192.168.112.0/24 : All Ports Protocol All Protocols	Block	All Time	LAN	Active		↓	Edit Delete
□	Src IP Address 192.168.113.0/24 : All Ports Dest IP Address 192.168.110.0/24 : All Ports Protocol All Protocols	Block	All Time	LAN	Active		↑	Edit Delete

(9) Log in to Cloud web to configure Cloud voucher authentication for guests.

a Choose **MONITORING** > **DEVICE** > **Gateway**.

b Click the SN of the EG to access the page of device details.



Gateway List

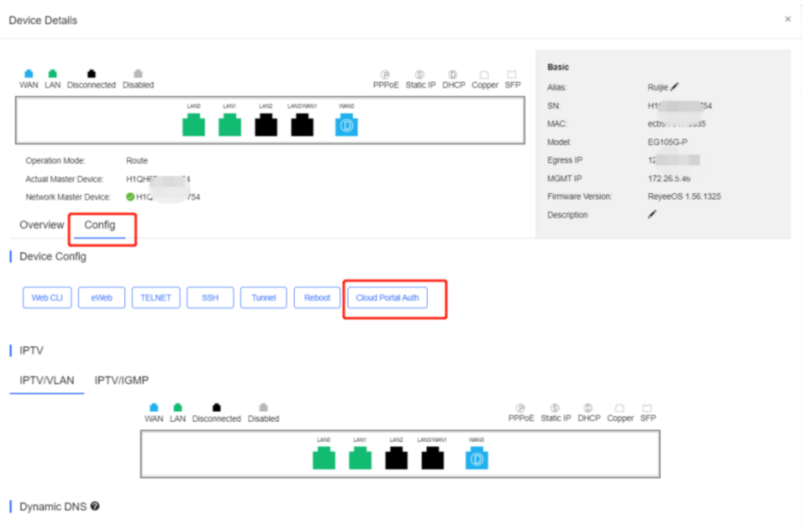
Auto Refresh:

Add | Web CLI | eWeb | More ▾ | 0 Selected | SN, Alias, Description

□	Status	SN	Alias	MGMT IP	MAC	Egress IP	Network	Firmware Version	Offline Time	Model	Description	Action
□	● Online	H1Q[redacted]54	Ruijie	172.26.5.46	ecb[redacted]35	120[redacted]	Reyee-Hotel	ReyeeOS 1.56.1325	2022-04-19 21:36:07	EG105G-P	Empty	🗑

First | Previous | Page 1 of 1 | Next | Last | 10 ▴ 1 in total

c Choose **Config** > **Cloud Portal Auth**.



Device Details

Operation Mode: Route

Actual Master Device: H1QH[redacted]4

Network Master Device: ● H1Q[redacted]754

Basic

Alias: Ruijie

SN: H1[redacted]54

MAC: ecb[redacted]35

Model: EG105G-P

Egress IP: 12[redacted]

MGMT IP: 172.26.5.46

Firmware Version: ReyeeOS 1.56.1325

Description:

Overview | Config

Device Config

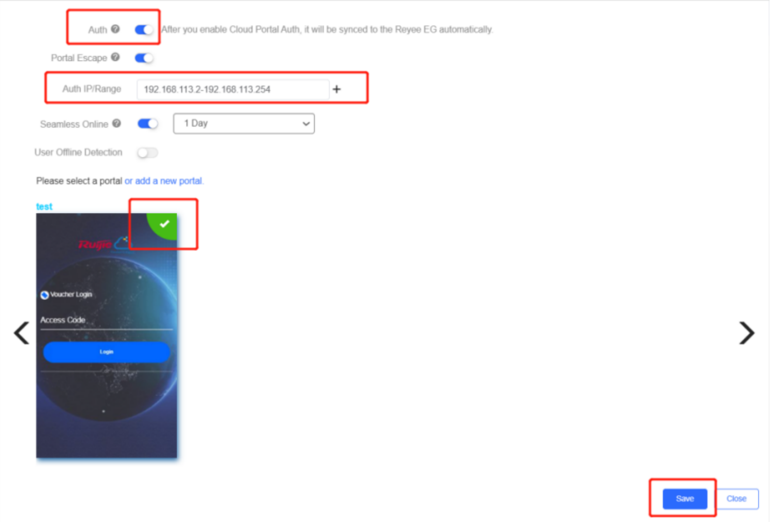
Web CLI | eWeb | TELNET | SSH | Tunnel | Reboot | Cloud Portal Auth

IPTV

IPTV/VLAN | IPTV/IGMP

Dynamic DNS

d Enable **Auth** and configure guests' IP address range from 192.168.113.2 to 192.168.113.254.



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

Portal Escape ❓ ●

Auth IP/Range: 192.168.113.2-192.168.113.254 +

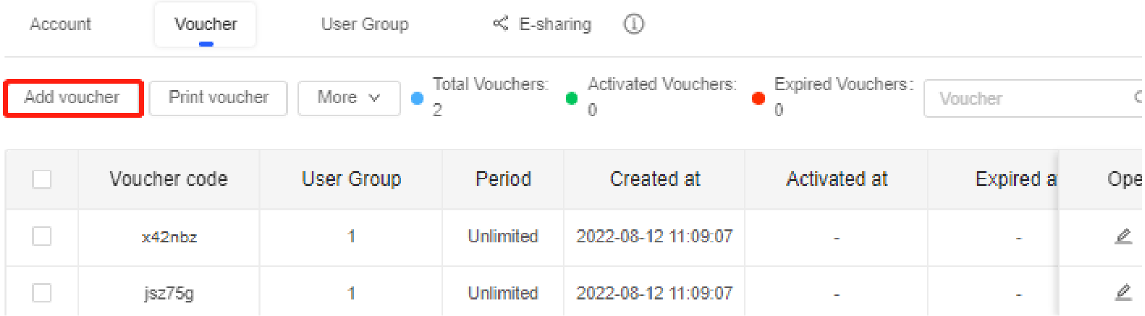
Seamless Online ❓ ● 1 Day

User Offline Detection ○

Please select a portal or add a new portal.

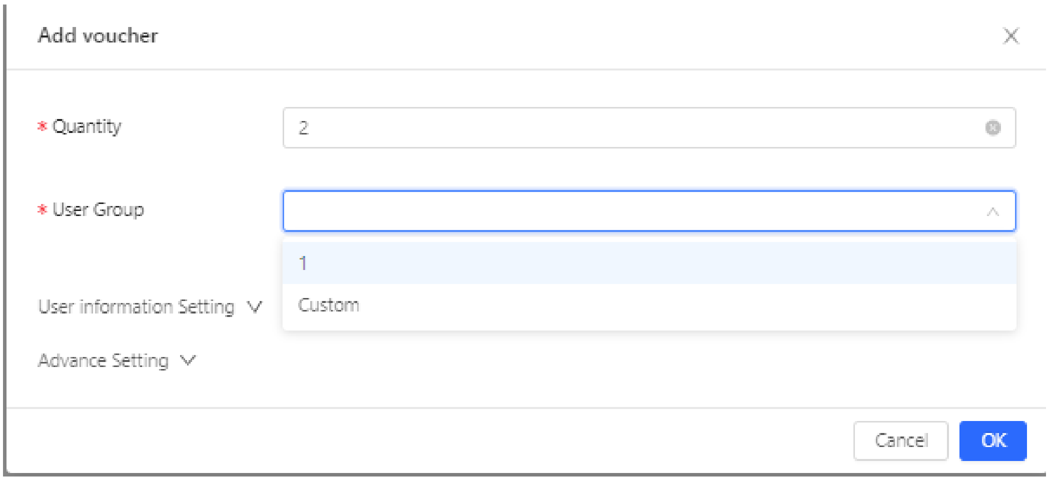
e Add the voucher for guests.

Choose **CONFIGURATION** > **AUTHENTICATION** > **User Management**, switch to the **Voucher** tab page, click **Add voucher** to configure **Quantity** and **User Group** of the voucher for guests. After the voucher is added, obtain the voucher code for guests from the **Voucher code** column in the voucher list.



Total Vouchers: 2
Activated Vouchers: 0
Expired Vouchers: 0

□	Voucher code	User Group	Period	Created at	Activated at	Expired a	Ope
□	x42nbz	1	Unlimited	2022-08-12 11:09:07	-	-	✎
□	jsz75g	1	Unlimited	2022-08-12 11:09:07	-	-	✎



Add voucher

* Quantity: 2

* User Group:

Quantity: Enter the quantity of vouchers.

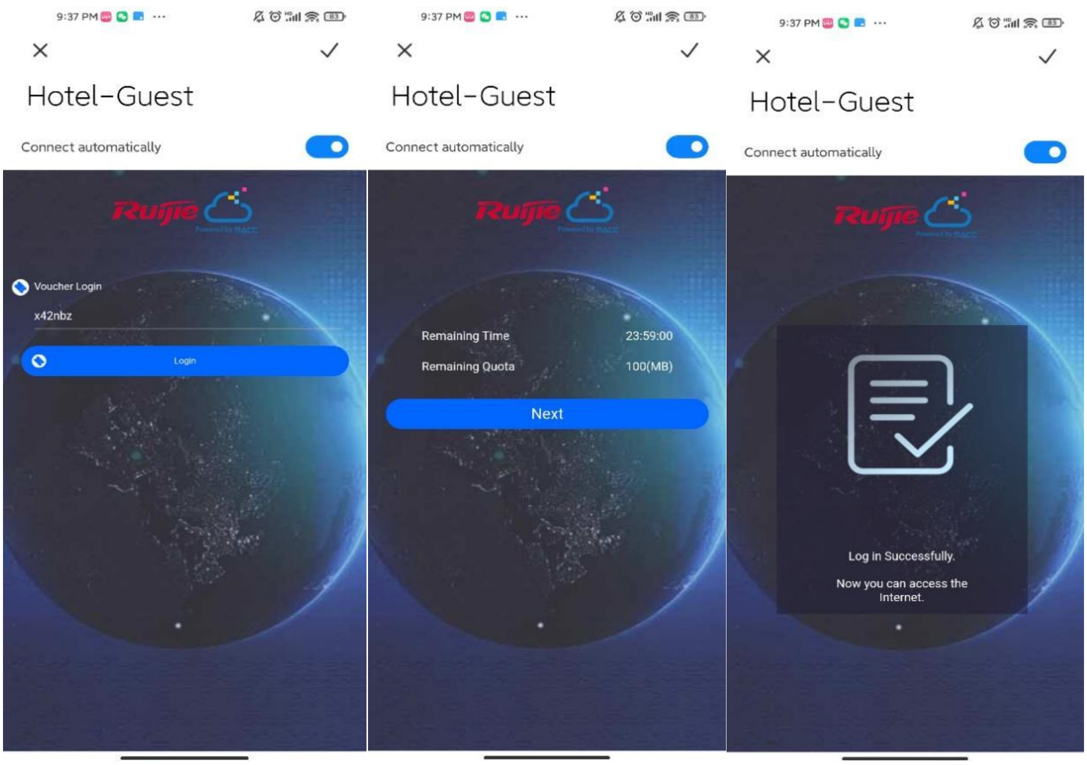
User Group: Select an existing user group or click **Custom** to customize a new user group.

User information Setting: Set user information.

Advance Setting: Set **Voucher code type** and **Voucher length**. **Voucher code type** can be set to **Alphanumeric 0-9, a-z**, **Alphabetic a-z**, or **Numeric 0-9**. **Voucher length** can be set to 6 to 9.

Configuration Verification

Connect guest Wi-Fi. Then you can view that the internal IP address 192.168.110.1 cannot be accessed.



9:37 PM

Hotel-Guest

Connect automatically

Voucher Login

x42nbz

Login

9:37 PM

Hotel-Guest

Connect automatically

Remaining Time 23:59:00

Remaining Quota 100(MB)

Next

9:37 PM

Hotel-Guest

Connect automatically

Log in Successfully.

Now you can access the Internet.

6 Reyee FAQ

6.1 Reyee Password FAQ (Collection)

6.2 Reyee Guest WiFi FAQ (Collection)

6.3 Reyee Wireless Configuration FAQ (Collection)

6.4 Reyee Self-Organizing Network (SON) FAQ (Collection)

6.5 Reyee series Devices Parameters Tables

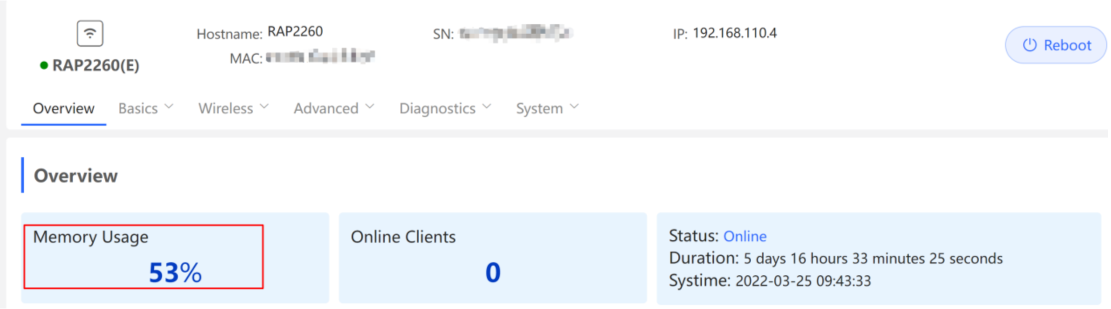
6.6 Reyee Parameter Consultation FAQ (Collection)

7 Appendix: Monitoring

7.1 Memory Usage

- In SON mode, select **Local Device** and select **Overview**.
- In standalone mode, select **Overview**.

Check the memory usage in the **Overview** area.



Hostname: RAP2260
MAC: [redacted]
SN: [redacted]
IP: 192.168.110.4

Memory Usage 53%

Online Clients 0

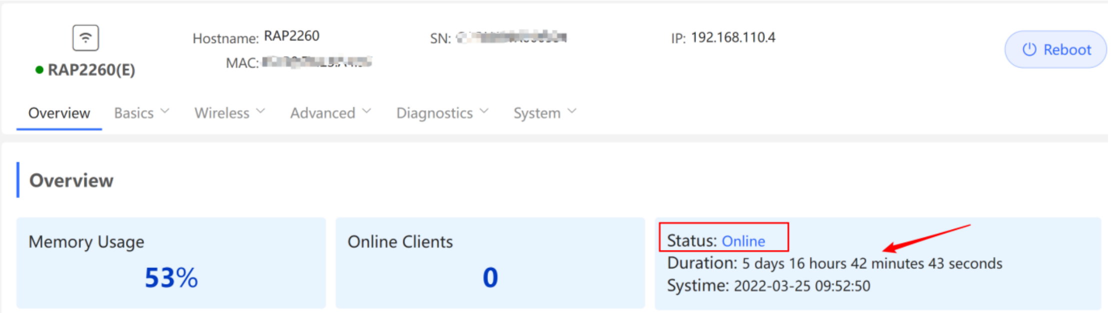
Status: Online
Duration: 5 days 16 hours 33 minutes 25 seconds
Systime: 2022-03-25 09:43:33

The valid memory usage is between 40% and 70%. When there are no clients, the reason for a high usage is that the memory usage is pre-allocated.

7.2 Device Status

- In SON mode, select **Local Device** and select **Overview**.
- In standalone mode, select **Overview**.

Check the device status in the **Overview** area.



Hostname: RAP2260
MAC: [redacted]
SN: [redacted]
IP: 192.168.110.4

Memory Usage 53%

Online Clients 0

Status: Online
Duration: 5 days 16 hours 42 minutes 43 seconds
Systime: 2022-03-25 09:52:50

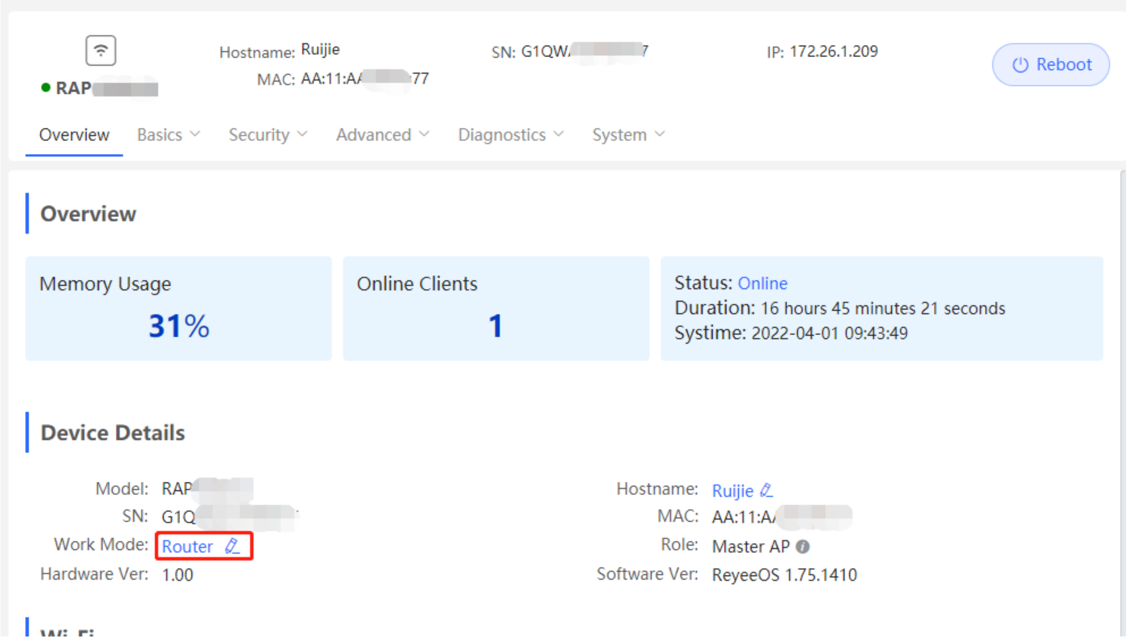
Status: indicates the device status. Check whether the device is online. **Online** means the SON feature of the Reyee device and is irrelevant to Ruijie Cloud.

Duration: indicates the online duration.

7.3 AP Working Mode

- In SON mode, select **Local Device** and choose **Overview** > **Device Details**.
- In standalone mode, choose **Overview** > **Device Details**.

Click the current working mode to access the working mode configuration page.



RAP[redacted]

Hostname: Ruijie

MAC: AA:11:A[redacted]77

SN: G1QW[redacted]7

IP: 172.26.1.209

Overview

Memory Usage 31%

Online Clients 1

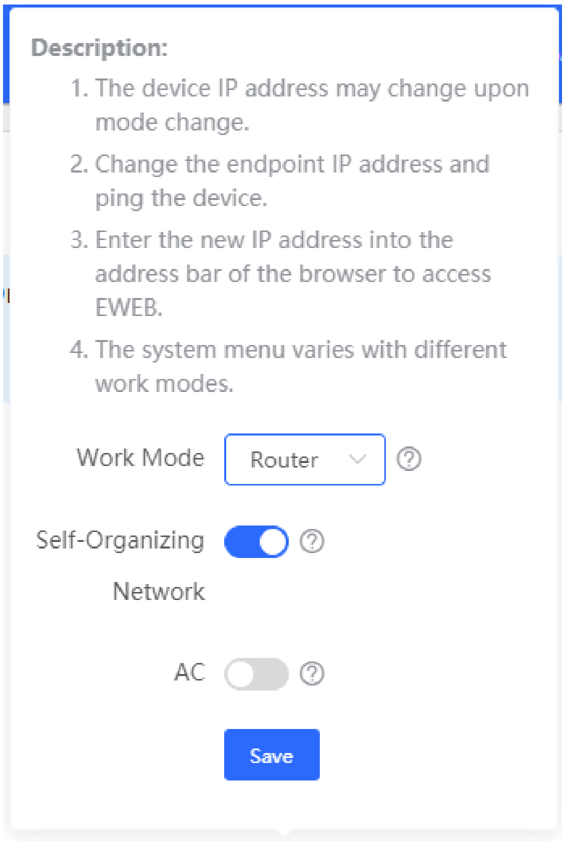
Status: Online
Duration: 16 hours 45 minutes 21 seconds
Systime: 2022-04-01 09:43:49

Device Details

Model: RAP[redacted]
SN: G1Q[redacted]
Work Mode: Router
Hardware Ver: 1.00

Hostname: Ruijie
MAC: AA:11:A[redacted]
Role: Master AP
Software Ver: ReyeeOS 1.75.1410

Set parameters of the working mode and click **Save**.



Description:

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

Work Mode: Router

Self-Organizing Network: on

AC: off

Working Mode: An AP can work in **AP** mode or **Router** mode.

- **Router**: indicates NAT forwarding. The AP in **Router** mode supports networking, network-wide configuration, and AP-specific radio functions.
- **AP**: indicates bridge forwarding.

Self-Organizing Network: If this function is enabled, the device role will be displayed. If it is disabled, the device works in standalone mode.

AC: When **Working Mode** is set to **Router** and **Self-Organizing Network** is enabled, this parameter is available. You can enable or disable the AC function. After the AC function is enabled, the device in router mode supports the virtual AC function and can manage downlink devices. If this function is disabled, the device needs to be elected as an AC in SON mode and then manage downlink devices.

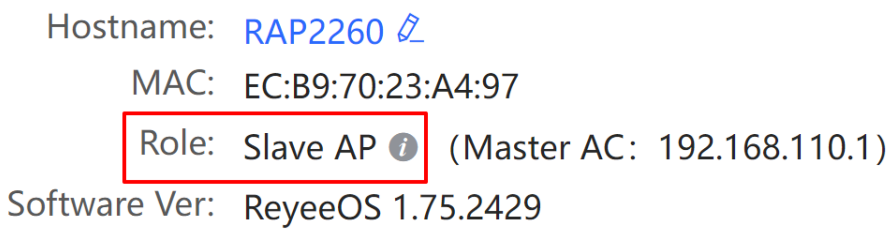
⚠ **Note**

After SON discovery is enabled, you can check the role of the device in SON mode.

7.4 Checking the SON Status

In SON mode, select **Local Device** and choose **Overview** > **Device Details**.

View the device role.



Hostname: RAP2260

MAC: EC:B9:70:23:A4:97

Role: Slave AP (Master AC: 192.168.110.1)

Software Ver: ReyeeOS 1.75.2429

There are four types of 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 an SON and works as a common AP.
- **Standalone**: The device has not joined an SON.

ⓘ **Instruction**

If the role is incorrect, press **F5** to refresh the page.

Ruijie EG3230/3250 and Reyee ES switches cannot act as the master.

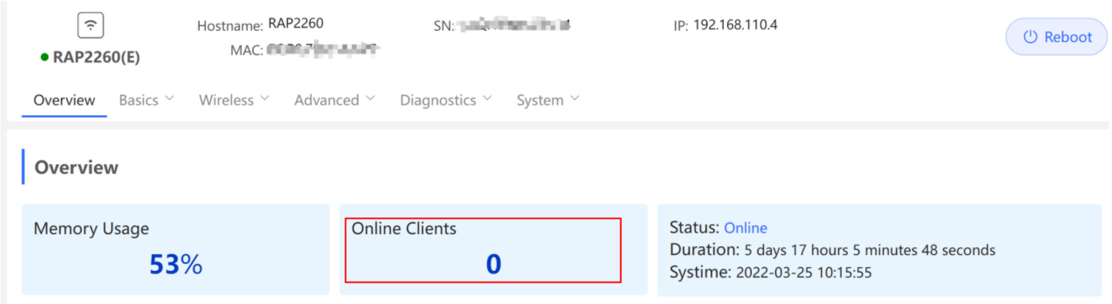
The priority of SON networking is as follows:

- Different models: EG (AC mode) > EG (router mode) > AP (router mode) > AP (AP mode) > switch
- Device CPU/Memory/other information (AP radio number): If devices have the same type but different models, a large parameter value indicates a higher priority of the device.
- Same model: If devices have the same type and models, a larger MAC address indicates a higher priority of the device.\

7.5 Online Clients

- In SON mode, select **Local Device** and select **Overview**.
- In standalone mode, select **Overview**.

View the number of online clients in the **Overview** area.



RAP2260(E)

Hostname: RAP2260

MAC: [redacted]

SN: [redacted]

IP: 192.168.110.4

Overview

Memory Usage 53%

Online Clients 0

Status: Online

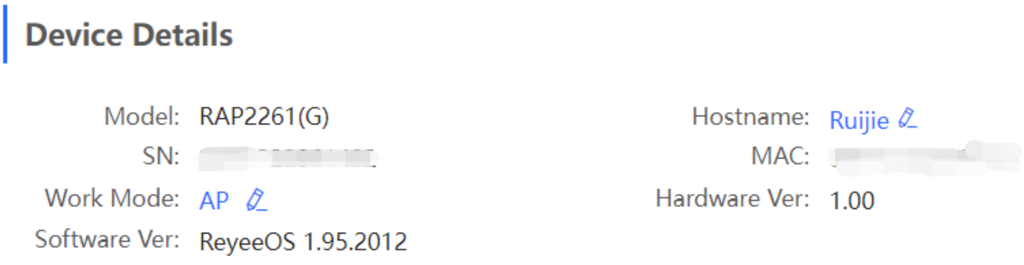
Duration: 5 days 17 hours 5 minutes 48 seconds

Systime: 2022-03-25 10:15:55

7.6 Device Information

- In SON mode, select **Local Device** and choose **Overview** > **Device Details**.
- In standalone mode, choose **Overview** > **Device Details**.

Check the device information.



Device Details

Model: RAP2261(G)

SN: [redacted]

Work Mode: AP

Software Ver: ReyeeOS 1.95.2012

Hostname: Ruijie

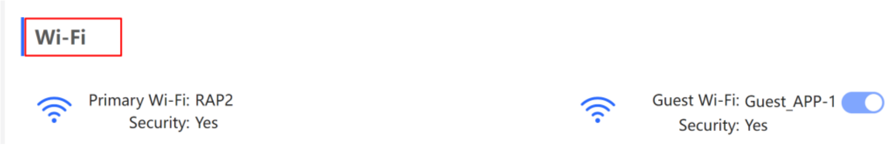
MAC: [redacted]

Hardware Ver: 1.00

7.7 Wireless Information

- In SON mode, select **Local Device** and choose **Overview** > **Wi-Fi**.
- In standalone mode, choose **Overview** > **Wi-Fi**.

Check wireless information.



Wi-Fi

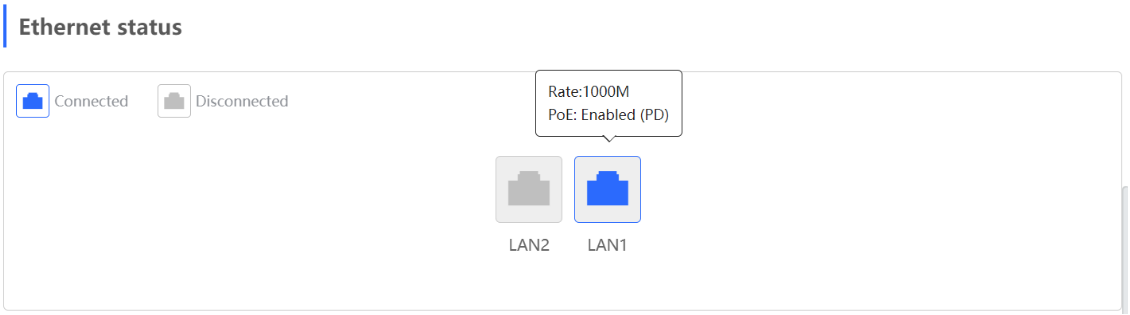
Primary Wi-Fi: RAP2
Security: Yes

Guest Wi-Fi: Guest_APP-1
Security: Yes

7.8 Ethernet Status

- In SON mode, select **Local Device** and choose **Overview** > **Ethernet status**.
- In standalone mode, choose **Overview** > **Ethernet status**.

Check the interface details.



Ethernet status

Connected Disconnected

Rate:1000M
PoE: Enabled (PD)