

Ruijie Reyee RG-RAP62 Access Point

Implementation Cookbook



Document Version: V1.0 Date: February 27, 2025 Copyright © 2025 Ruijie Networks

Copyright

Copyright © 2025 Ruijie Networks

All rights are reserved in this document and this statement.

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



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

Disclaimer

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

The names, links, descriptions, screenshots, and any other information regarding third-party software mentioned in this document are provided for your reference only. Ruijie Networks does not explicitly or implicitly endorse or recommend the use of any third-party software and does not make any assurances or guarantees concerning the applicability, security, or legality of such software. You should choose and use third-party software based on your business requirements and obtain proper authorization. Ruijie Networks assumes no liability for any risks or damages arising from your use of third-party software.

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: <u>https://reyee.ruijie.com</u>
- Technical Support Website: <u>https://reyee.ruijie.com/en-global/support</u>
- Case Portal: https://www.ruijienetworks.com/support/caseportal
- Community: <u>https://community.ruijienetworks.com</u>
- Technical Support Email: service_rj@ruijienetworks.com
- Online Robot/Live Chat: <u>https://reyee.ruijie.com/en-global/rita</u>

Conventions

1. GUI Symbols

Interface symbol	Description	Example
Boldface	 Button names Window names, tab name, field name and menu items Link 	 Click OK. Select Config Wizard. 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:

U 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.

1 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.



Overview

This cookbook consists of multiple independent volumes, introducing the installation, deployment, and webbased configuration of the RG-RAP62 access point, including:

01- Installation Guide

02- ReyeeOS 2.289 Configuration Guide

Contents

1 Overview
1.1 About the RG-RAP621
1.2 Package Contents1
1.3 Product Appearance2
1.3.2 Front Panel2
1.3.3 Rear Panel
1.4 Technical Specifications4
1.5 Power Supply Technical Specifications6
1.6 Cooling7
2 Preparing for Installation8
2.1 Safety Guidelines8
2.1.1 General Safety Guidelines8
2.1.2 Chassis-Lifting Guidelines8
2.1.3 Electrical Safety Guidelines8
2.2 Site Requirements9
2.2.1 Bearing Requirements9
2.2.2 Space Requirements9
2.2.3 Ventilation Requirements9
2.2.4 Temperature/Humidity Requirements9
2.2.5 Cleanliness Requirements10
2.2.6 Prevention of Electrostatic Discharge Damage10
2.2.7 EMI Requirements11

2.3 Tools11
3 Installing the AP12
3.1 Before You Begin12
3.2 Safety Precautions During Installation12
3.3 Installing the AP13
3.4 Removing the AP16
3.5 Connecting Cables16
3.6 Bundling Cables17
3.7 Verifying the Installation17
4 Commissioning
4.1 Setting Up the Configuration Environment18
4.2 Powering on the AP18
4.2.1 Checklist Before Power-On18
4.2.2 Checklist After Power-on18
4.3 Troubleshooting Power Supply Failures18
4.4 Logging In to the Web GUI18
5 Monitoring and Maintenance
5.1 Monitoring20
5.2 Hardware Maintenance20
6 Common Troubleshooting21
6.1 Troubleshooting Flowchart21
6.2 Common Faults21
6.2.1 Why Is the LED Off After the AP Is Powered On?21
6.2.2 Ethernet Port Is Not Working After the Ethernet Cable Is Plugged In21

6.2.3 A Client Cannot Discover the AP	21
7 Appendix	23
7.1 Connectors and Media	23
7.1.1 10/100/1000BASE-T Port	23
7.2 Cabling Recommendations	25
7.2.1 Requirements for the Minimum Bend Radius of Ethernet Cables	25
7.2.2 Precautions for Cable Bundling	25

1 Overview

1.1 About the RG-RAP62

The RG-RAP62 is a cost-effective Wi-Fi 6 dual-band ceiling access point (AP) launched by Ruijie Reyee for indoor Wi-Fi coverage scenarios. It supports IEEE 802.3af and IEEE 802.3at standards as well as local 12 V DC power supply. Compliant with IEEE 802.11a/b/g/n/ac Wave 1/Wave 2/ax Wi-Fi standards, the RG-RAP62 features dual-stream MU-MIMO technology and built-in omni-directional antennas. It operates in both 2.4 GHz and 5 GHz bands, providing data rates of 573 Mbps in the 2.4 GHz band and 1201 Mbps in the 5 GHz band, with a combined data rate of up to 1774 Mbps. With a coverage capability of over 40 meters (131.23 ft.), the RG-RAP62 is ideal for a range of wireless applications, especially in offices, businesses, villas, hotels, and small- and medium-sized government services.

1.2 Package Contents

No. Item Quantity 1 RG-RAP62 access point 1 2 Mounting bracket 1 3 4 Phillips pan head screws (M4 x 20 mm) 4 Wall anchors 4 5 **User Manual** 1 6 1 Key to securing latch 7 Mounting template 1 8 1 Warranty Card

Table 1-1 Package Contents

i) Note

The package contents are subject to the purchase contract, and actual delivery may vary. Please check the items carefully against the package contents or purchase contract. If you have any questions, please contact the distributor.

Overview

1.3 Product Appearance





1.3.2 Front Panel





Table 1-2 LEDs

No.	ltem	Status	Description
1	System	Solid blue	The AP is operating normally without any alarms.

No.	Item	Status	Description
	status LED	Off	The AP is not receiving power.
		Fast blinking blue (eight blinks per second)	The AP is starting up.
		Slow blinking blue (one blink per 2 seconds)	The AP is not connected to the Internet.
		Two blue flashes	 Possible cases are as follows: The AP is resetting. The AP is upgrading. The AP is recovering. AP is recovering. Caution Do not power off the AP when its LED is in this state.
		Blinking blue (three quick flashes followed by one slow flash)	Other faults have occurred.

1.3.3 Rear Panel





No.	ltem	Description
1	RESET button	Press and hold for less than 2 seconds: Restart the AP.
		Press and hold for more than 5 seconds: Restore the AP to factory settings.
2	LAN/PoE port	1 x 10/100/1000BASE-T Ethernet port, supporting PoE input
3	DC=12 V connector	Connects to a DC power adapter for power supply. The DC power voltage is 12 V and the current is 1.5 A.
4	Label	The label is located at the bottom.

Table 1-3 Components on the Rear Panel

1.4 Technical Specifications

Table 1-4 Specification

RF Design	2.4 GHz and 5 GHz dual-band dual-stream	
Transmission Standards	IEEE 802.11ax, IEEE 802.11ac Wave 2/Wave 1, and IEEE 802.11a/b/g/n	
Operating Frequency Bands	IEEE 802.11b/g/n/ax: 2.4 GHz to 2.4835 GHz IEEE 802.11a/n/ac/ax: 5.150 GHz to 5.350 GHz, 5.470 GHz to 5.725 GHz,, 5.725 GHz to 5.850GHz A Caution Country-specific restrictions apply.	
Antenna	2.4 GHz, two built-in omni-directional antennas (Antenna gain: 3.13 dBi)5 GHz, three built-in omni-directional antennas (Antenna gain: 4.58 dBi)	
Number of Spatial Streams	2.4 GHz, two spatial streams, 2x2 MIMO 5 GHz, two spatial streams, 2x2 MIMO	
Data Rate	2.4 GHz: 573 Mbps 5 GHz: 1201 Mbps Combined: 1774 Mbps	
Modulation	OFDM: BPSK @ 6/9 Mbps, QPSK @ 12/18 Mbps, 16QAM @ 24 Mbps, and 64QAM @ 48/54 Mbps DSSS: DBPSK @ 1 Mbps, DQPSK @ 2 Mbps, and CCK @ 5.5/11 Mbps MIMO-OFDM: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, and 1024-QAM OFDMA	
Receiver Sensitivity	11b: –91 dBm (1 Mbps), –88 dBm (5.5 Mbps), –85 dBm (11 Mbps)	

	11a/g: -89 dBm (6 Mbps), -80 dBm (24 Mbps), -76 dBm (36 Mbps), -71 dBm (54		
	Mbps)		
	11n: -83 dBm (MCS0), -65 dBm (MCS7), -83 dBm (MCS8), -65 dBm (MCS15)		
	11ac: 20 MHz: -83 dBm (MCS0), -57 dBm (MCS9)		
	11ac: 40 MHz: –79 dBm (MCS0), –57 dBm (MCS9)		
	11ac: 80 MHz:76 dBm (MCS0),51 dBm (MCS9)		
	11ax: 20 MHz: –85 dBm (MCS0), –58 dBm (MCS11)		
	11ax: 40 MHz: –82 dBm (MCS0), –54 dBm (MCS11)		
	11ax: 80 MHz: –79 dBm (MCS0), –52 dBm (MCS11)		
	Frequency bands and the maximum Effective Isotropic Radiated Power (EIRP):		
	i Note		
	The actual transmit power may vary in different countries and regions		
	according to the rules and regulations.		
	 European Union & United Kingdom 		
	o 2400–2483.5 MHz, EIRP ≤ 20 dBm		
	o 5150–5350 MHz, EIRP ≤ 23 dBm		
	o 5470–5725 MHz, EIRP ≤ 30 dBm		
Max Transmit	 Myanmar: 2400–2483.5 MHz, EIRP ≤ 23 dBm 5725–5825 MHz, EIRP ≤ 30 dBm Theiland: 		
Nax. Transmit			
Power			
	• Thailand. 0.2400-2483.5 MHz EIRP < 20 dBm		
	o 5150-5350 MHz EIRP < 23 dBm		
	$0.5470-5725 \text{ MHz}$, EIRP $\leq 30 \text{ dBm}$		
	\circ 5725–5825 MHz, EIRP \leq 30 dBm		
	Indonesia:		
	o 2400–2483.5 MHz, EIRP ≤ 27 dBm		
	o 5150–5350 MHz, EIRP ≤ 23 dBm		
	o 5725–5825 MHz, EIRP ≤ 23 dBm		
	• Egypt:		
	o 2400–2483.5 MHz, EIRP ≤ 20 dBm		
	0 5150-5350 MHZ, EIRP ≤ 23 dBm		
Power Step	1 dBm		
Dimensions (Ø x H)	175 mm x 39 mm (6.89 in. x 1.54 in., excluding the mounting bracket)		
Woight	Weight of the access point: ≤ 0.4 kg (0.88 lbs.)		
weight	Weight of the mounting bracket: ≤ 0.06 kg (0.13 lbs.)		
Service Ports	1 x 10/100/1000BASE-T Ethernet port, supporting PoE input		
Management Port	N/A		

Status LED	1 x system status LED		
Power Supply	 DC power supply using a power adapter (input voltage and current: 12 V/1.5 A) A Caution The power adapter is optional. DC connector dimensions: inner diameter: 2.1 mm (0.08 in.); outer diameter: 5.5 mm (0.22 in.); length: 10 mm (0.39 in.). PoE: Compliant with the IEEE 802.3af (PoE) or IEEE 802.3at (PoE+) standards. PoE injector: Compliant with the IEEE 802.3af (PoE) or IEEE 802.3at (PoE+) standards. 		
Power Consumption	≤ 12.95 W		
	Operating temperature: 0°C to 40°C (32°F to 104°F)		
Environmental	Storage temperature: -40°C to 70°C (-40°F to +158°F)		
	Operating humidity: 5% to 95% RH (non-condensing)		
	Storage humidity: 5% to 95% RH (non-condensing)		
Mounting	Ceiling mount using screws		
Certification	CE, RoHS		
Mean Time Between Failures (MTBF)	> 400,000 hours		

1.5 Power Supply Technical Specifications

The RG-RAP62 supports DC and PoE power supply.

- When the AP is powered by a DC power adapter, the power adapter should have a voltage of 12 V and a current of 1.5 A or higher. If you require a DC power adapter, it can be purchased separately from us. Dimensions of the DC power connector (outer diameter x inner diameter x length): 5.5 mm x 2.1 mm x 10 mm (0.22 in. x 0.08 in. x 0.39 in.).
- When the AP is powered by standard PoE, connect one end of the Ethernet cable to the LAN/PoE port on the AP, and the other end to a PoE-capable switch port or PSE. Ensure that the PoE-capable switch port or PSE is IEEE 802.3af-compliant or IEEE 802.3at-compliant.
- When the AP is powered by a PoE injector, ensure that the PoE injector complies with the IEEE 802.3af or IEEE 802.3at standards.

A Caution

- The DC input power of the DC power adapter must be greater than the actual power consumption of the AP.
- When the AP is powered by a DC power adapter, you are advised to use the power adapter that comes with the Ruijie device.
- Ruijie-certified PoE adapters are recommended.

1.6 Cooling

The AP adopts a fanless design.

🛕 Caution

Ensure that there is sufficient space around the AP for heat dissipation.

2 Preparing for Installation

2.1 Safety Guidelines

🚺 Note

- To avoid personal injury or equipment damage, review the safety guidelines in this chapter before you begin the installation.
- The following safety guidelines may not include all the potentially hazardous situations.

2.1.1 General Safety Guidelines

- Do not expose the equipment to high temperature, dusts, or harmful gases. Do not install the equipment in an inflammable or explosive environment. Keep the equipment away from EMI sources such as large radar stations, radio stations, and substations. Do not subject the equipment to unstable voltage, vibration, and noises.
- The installation site should be dry. Do not install the equipment in a place near the sea. Keep the equipment at least 500 meters away from the ocean and do not face it towards the sea breeze.
- The installation site should be free from water flooding, seepage, dripping, or condensation. The installation site should be selected according to network planning, communications equipment features, and considerations such as climate, hydrology, geology, earthquake, electrical power, and transportation.

🛕 Caution

Always install and remove the equipment according to the installation procedures outlined in this document.

2.1.2 Chassis-Lifting Guidelines

- After the equipment is installed, avoid handling it frequently.
- Cut off all power supplies and unplug all power cords before moving or handling the equipment.

2.1.3 Electrical Safety Guidelines

🕕 Warning

- Improper or incorrect electric operations may cause a fire, electric shock, and other accidents, and lead to severe and fatal personal injury and device damage.
- Direct or indirect contact with high voltage or mains power supply through wet objects may cause fatal dangers.
- Observe local regulations and specifications during electric operations. Only personnel with relevant qualifications can perform such operations.
- Check whether there are potential risks in the work area. For example, check whether the ground is wet.
- Find out the position of the indoor emergency power switch before installation. Cut off the power switch in case of accidents.

- Make sure that the equipment is powered off when you cut off the power supply.
- Do not place the equipment in a damp/wet location. Do not let any liquid enter the chassis.
- Keep the equipment far away from grounding or lightning protection devices for power equipment.
- Keep the equipment away from radio stations, radar stations, high-frequency high-current devices, and microwave ovens.

2.2 Site Requirements

Install the equipment indoors to ensure its normal operation and prolonged service life. The installation site must meet the following requirements.

2.2.1 Bearing Requirements

Ensure that the installation position is sturdy enough to support the weight of the RG-RAP62 and its accessories.

2.2.2 Space Requirements

- The equipment should be installed in an open environment if possible. If the environment is enclosed, confirm that a good ventilation and heat dissipation system is available.
- Ensure that the installation location is suitable for the RG-RAP62, leaving sufficient space on the front, back, left, and right sides for heat dissipation.

2.2.3 Ventilation Requirements

The RG-RAP62 dissipates heat naturally. Therefore, certain space needs to be reserved around the equipment for heat dissipation.

2.2.4 Temperature/Humidity Requirements

To ensure that the RG-RAP62 works properly and has a long service life, maintain a proper temperature and humidity in the operating environment. The operating environment with too high or too low temperature and humidity for a long period of time may damage the equipment.

- In an environment with high relative humidity, the insulating material may have poor insulation or even leak electricity. Sometimes high humidity may causes changes in the mechanical properties and causes rusting of metal parts.
- In an environment with low relative humidity, static electricity is prone to occur and damage the internal circuits of the equipment.
- Too high temperatures can accelerate the aging of insulation materials, greatly reducing the reliability of the equipment and severely affecting its service life.

The following table lists the temperature and humidity requirements.

Table 2-1 Temperature/Humidity Requirements

Operating Temperature	Operating Humidity	
0°C to 40°C (32°F to 104°F)	5% to 95% RH (non-condensing)	

2.2.5 Cleanliness Requirements

Dust poses a major threat to the equipment. The indoor dust takes on a positive or negative static electric charge when falling on the switch, causing poor contact of the metallic joint. Such electrostatic adhesion may occur more easily when the relative humidity is low, not only affecting the service life of the equipment, but also causing communication faults. The following table describes the requirements for the dust content and granularity in the machine room.

Table 2-2 Requirements for Dust

Dust	Unit	Content
Dust particles (diameter ≥ 0.5 μm)	Particles/m ³	≤ 3.5 x 10 ⁶
Dust particles (diameter ≥ 5 µm)	Particles/m ³	≤ 3.5 x 10 ⁴

Apart from dust, the salt, acid, and sulfide in the air in the machine room must meet strict requirements. These harmful substances will accelerate metal corrosion and component aging. Therefore, the machine room should be properly protected against the intrusion of harmful gases, such as sulfur dioxide, hydrogen sulfide, nitrogen dioxide, and chlorine gas. The following table lists limit values for harmful gases.

Table 2-3Requirements for Gases

Gas	Average (mg/m ³)	Maximum (mg/m³)
Sulfur dioxide (SO ₂)	0.2	1.5
Hydrogen sulfide (H ₂ S)	0.006	0.03
Nitrogen dioxide (NO ₂)	0.04	0.15
Ammonia gas (NH ₃)	0.05	0.15
Chlorine gas (Cl ₂)	0.01	0.3

🚺 Note

Average refers to the average value of harmful gases measured in one week. Maximum refers to the upper limit of harmful gases measured in one week, and the maximum value cannot last for more than 30 minutes every day.

2.2.6 Prevention of Electrostatic Discharge Damage

This equipment is engineered with stringent anti-static measures during circuit design. However, excessive static electricity can still potentially damage the printed circuit board. Static electricity in the communication network connected to the equipment primarily comes from two sources:

- Outdoor high-voltage power lines, lightning, and other external electric fields; and
- Internal systems such as flooring materials and the internal structure of the equipment

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

- Keep the indoor installation environment clean and free of dust; and
- Maintain appropriate temperature and humidity conditions.

2.2.7 EMI Requirements

- Keep the equipment far away from grounding or lightning protection devices for power equipment.
- Keep the equipment away from radio stations, radar stations, high-frequency high-current devices, and microwave ovens.

2.3 Tools

Common Tools	Phillips screwdriver, cables, fastening bolts, diagonal plier, cable ties
Special Tools	Anti-ESD gloves, wire stripper, crimper, RJ45 crimping plier, wire cutter, and waterproof tape
Meters	Multimeter and bit error rate tester (BERT)

1 Note

The equipment is delivered without a toolkit. Prepare the preceding tools by yourself.

3 Installing the AP

The AP is required to be fixed indoors.

🛕 Caution

Before installing the equipment, ensure that guidelines and requirements in Chapter 2 have been met.

3.1 Before You Begin

Carefully plan and arrange the installation position, networking mode, power supply, and cabling before installation. Confirm the following requirements before installation:

- The installation site provides sufficient space for proper ventilation.
- The installation site meets the temperature and humidity requirements of the AP.
- The power supply and required current are available in the installation site.
- The selected power supply modules meet the system power requirements.
- The installation site meets the cabling requirements of the AP.
- The installation site meets the site requirements of the AP.
- The customized AP meets the client-specific requirements.

3.2 Safety Precautions During Installation

To ensure the normal operation and prolonged service life of the AP, observe the following safety precautions:

- Do not power on the AP during installation.
- Place the AP in a well-ventilated environment.
- Do not subject the AP to high temperatures.
- Keep the AP away from high-voltage power cables.
- Install the AP indoors.
- Do not expose the AP in a thunderstorm or strong electric field.
- Keep the AP clean and dust-free.
- Cut off the power switch before cleaning the AP.
- Do not wipe the AP with a damp cloth.
- Do not wash the AP with liquid.
- Do not open the enclosure when the AP is working.
- Fasten the AP tightly.

3.3 Installing the AP

1 Note

- For indoor environments, ceiling mounting is preferred because it offers a broader coverage area than wall mounting.
- This installation guide is for reference only. The actual installation procedure may differ depending on the specific physical product.
- (1) Drill holes in the ceiling or wall using the mounting template.



(2) Secure the mounting bracket to the ceiling or wall using wall anchors and Phillips pan head screws (M4 x 20 mm).



A Caution

The plane deviation of the wall in a specific area should be within 2 mm (0.08 in.), and the recommended torque for installation is 4kgf.cm. In case of uneven installation site, mount the AP on a protruding wall.

- (3) Connect cables according to the actual topology. The following describes how to connect cables on the AP side.
- Ethernet cable: Connect one end of the Ethernet cable to the LAN/PoE port (supporting PoE input) on the rear of the AP.
- DC power cord: When DC power supply is used, connect one end of the power cord to the 12 V DC power connector on the rear of the AP.



(4) Align the slots on the rear of the AP with the square feet on the mounting bracket, and slide the AP into the mounting bracket slowly to ensure that the AP is secured.



A Caution

- Before securing the AP to the mounting bracket, connect the cables first.
- The slots on the rear of the AP must be aligned with and slid into the square feet on the mounting bracket. Do not press the slots into the square feet by force.
- After the installation is complete, check whether the AP is secured.

3.4 Removing the AP

(1) Insert the key to security latch into the reserved slot.



(2) Slide down the AP as indicated by the arrow.



3.5 Connecting Cables

Connect twisted pairs with the LAN/PoE port on the AP. See <u>7.1</u> Connectors and Media for supported wiring of twisted pairs.

A Caution

- Avoid a small bend radius at the connector.
- You are advised not to use Ethernet cables with protective caps for the RG-RAP62, as they complicate the assembly of the Ethernet cables.

3.6 Bundling Cables

Precautions

- Bundle the cable in a visually pleasing way.
- Bend twisted pairs naturally or to a large radius close to the connector.
- Do not over-tighten the twisted pair bundle as it may reduce the cable life and performance.

Bundling Steps

- (1) Bundle the hanging part of the twisted pairs using cable ties and lead them to the LAN/PoE port of the AP by convenience.
- (2) Fasten the twisted pair cables to the cable trough of the mounting bracket.
- (3) Extend the twisted pair cables under the AP and route them in a straight line.

3.7 Verifying the Installation

- Verify that the AP is securely fastened.
- Verify that the twisted pair cable matches the port type.
- Verify that the cables are properly bundled.
- Verify that the PSE is IEEE 802.3af-compliant or IEEE 802.3at-compliant.

4 Commissioning

4.1 Setting Up the Configuration Environment

After powering on the AP through a DC power adapter or a PSE, ensure that the power cord is properly connected and meets safety requirements.

4.2 Powering on the AP

4.2.1 Checklist Before Power-On

- The power cord is properly connected.
- The power voltage meets the requirement.

4.2.2 Checklist After Power-on

- Verify the LED status.
- After the AP is powered on, verify that the SSID can be searched by a mobile phone or other wireless devices.

4.3 Troubleshooting Power Supply Failures

You can determine whether there is a power system failure by checking the LED status on the front panel of the RG-RAP62. For the LED status description, see <u>Table 1-2 LEDs</u>. Perform the following checks in the case of any abnormality:

- Verify that the AP is properly powered.
- Verify that the Ethernet port is correctly connected.

🚺 Note

If the AP cannot be powered on after all the preceding items are verified, contact your local distributor or technical support.

4.4 Logging In to the Web GUI

 Power on the PC and configure the local connection attribute on the PC. Set the IP address of the PC to 10.44.77.XXX (1 to 255, excluding 254).

🎚 Network	Properties		×
Networking			
C Interne	t Protocol Version 4 (TCP/IPv4)	Properties	×
Gener	al		
T this of for the formation of the forma	can get IP settings assigned autor capability. Otherwise, you need to ne appropriate IP settings.	atically if your netwo ask your network ad	ork supports Iministrator
	Use the following IP address:	Ŷ	
IP	address:	10 . 44 . 77 .	111
SU	bnet mask:	255.255.255.	٥
De	efault gateway:		
	044-1- 04/2	-411.	

(2) Open a browser on the PC and enter 10.44.77.254 to log in to the web interface. The default password is admin for the first login. For security purposes, change the default password after login.

5 Monitoring and Maintenance

5.1 Monitoring

When the RG-RAP62 is operating, you can monitor the device running status by observing the LED. For LED status description, see <u>Table 1-2 LEDs</u>.

5.2 Hardware Maintenance

If the hardware is faulty, contact your local distributor.

6 Common Troubleshooting

6.1 Troubleshooting Flowchart



6.2 Common Faults

6.2.1 Why Is the LED Off After the AP Is Powered On?

- If you use a PoE power supply, verify that the PSE is IEEE 802.11at-compliant, and then verify that the cable is connected properly.
- If you use a power adapter, verify that the power adapter is connected with an active power outlet, and then verify that the power adapter works properly.

6.2.2 Ethernet Port Is Not Working After the Ethernet Cable Is Plugged In

Verify that the device at the other end of the Ethernet cable is working properly, and then verify that the Ethernet cable is capable of providing the required data rate and is properly connected.

6.2.3 A Client Cannot Discover the AP

- (1) Verify that the AP is properly powered.
- (2) Verify that the Ethernet port is correctly connected.

- (3) Verify that the AP is correctly configured.
- (4) Move the client closer to the AP.

Appendix

7 Appendix

7.1 Connectors and Media

7.1.1 10/100/1000BASE-T Port

A 10/100/1000BASE-T port supports three rates with auto-negotiation, and supports the automatic MDI/MDIX crossover function at these three rates.

Compliant with IEEE 802.3ab, the 1000BASE-T port requires Cat5/5e or higher 100-ohm unshielded twisted pair (UTP) or shielded twisted pair (STP) cables with a maximum distance of 100 m (328.08 ft.).

The 1000BASE-T port requires all four pairs of wires to be connected for data transmission. The following figure shows the four pairs of wires for the 1000BASE-T port.

Figure 7-1 1000BASE-T Twisted Pair Connections

Straight-Through		Crossover	
Device	Device	Device	Device
1 TP0+ 🗲		1 TP0+ 🗲	→1 TP0+
2 TP0- 🗲		2 TP0-	✓ →2 TP0-
3 TP1+ 🗲		3 TP1+ 🔶	→3 TP1+
6 TP1- 🗲		6 TP1- ←	→6 TP1-
4 TP2+ 🗲	→ 4 TP2+	4 TP2+ 🗲	→4 TP2+
5 TP2- 🗲		5 TP2- 🗲	✓ →5 TP2-
7 TP3+ 🗲		7 TP3+	✓→7 TP3+
8 TP3- 🗲	→ 8 TP3-	8 TP3- 🗲	→8 TP3-

In addition to cables with the above-mentioned specifications, the 10BASE-T/100BASE-TX port can be connected using 100-ohm Cat3, Cat4, and Cat5 cables at 10 Mbps data speed or using 100-ohm Cat5 cables at 100 Mbps data speed with a maximum distance of 100 m (328.08 ft.). The following table shows 10BASE-T/100BASE-TX pin assignments.

Pin	Socket	Plug
1	Input Receive Data+	Output Transmit Data+
2	Input Receive Data-	Output Transmit Data-
3	Output Transmit Data+	Input Receive Data+
6	Output Transmit Data-	Input Receive Data-
4, 5, 7, 8	Not Used	Not Used

Table 7-1 10BASE-T/100BASE-TX Pin Assignments

The following figure shows feasible connections of the straight-through and crossover twisted pairs for a 10BASE-T/100BASE-TX port.

Straight-Through		Crossover		
Device	Device	Device	Device	
1 IRD+ ←	→ 1 OTD+	1 IRD+ ←	→ 1 IRD+	
2 IRD- ←	→ 2 OTD-	2 IRD- ←	→ 2 IRD-	
3 OTD+ ←		3 OTD+	3 OTD+	
6 OTD- 🗲	← 6 IRD-	6 OTD- ←	→ 6 OTD-	

Figure 7-2 10BASE-T/100BASE-TX Twisted Pair Connections

7.2 Cabling Recommendations

During installation, route cable bundles upward or downward along the sides of the rack depending on the actual situation in the equipment room. All adapted connectors should be placed at the bottom of the rack in an orderly manner, and cannot be exposed outside the rack. Power cords are routed upward or downward beside the rack close to the location of the DC power distribution box, AC socket, or surge protection box in the equipment room.

7.2.1 Requirements for the Minimum Bend Radius of Ethernet Cables

- The bend radius of a fixed power cord, Ethernet cable, or flat cable should be over five times greater than their respective diameters. The bend radius of these cables that are often bent or plugged should be over seven times greater than their respective diameters.
- The bend radius of a fixed common coaxial cable should be over seven times greater than its diameter. The bend radius of these cables that are often bent or plugged should be over 10 times greater than their respective diameters.
- The minimum bend radius of a high-speed cable, such as an SFP+ cable, should be over five times greater than its diameter. The bend radius of these cables that are often bent or plugged should be over 10 times greater than their respective diameters.

7.2.2 Precautions for Cable Bundling

- Before cables are bound, mark labels and stick them to cables wherever appropriate.
- Cables should be neatly and properly bound in the cabinet without twisting or bending, as shown in Figure 7-3.



Figure 7-3 Bundling Cables

- Route and bundle power, signal, ground cables separately. Mixed bundling is not allowed. When the cables are close to each other, crossover cabling is recommended. In the case of parallel cabling, maintain a minimum distance of 30 mm (1.18 in.) between power cords and signal cables.
- The cable management brackets and cabling troughs inside and outside the rack should be smooth without sharp corners.

- The metal holes traversed by cables should have a smooth and fully rounded surface or an insulated lining.
- Use cable ties to bundle up cables properly. Do not connect two or more cable ties to bundle up cables.
- After bundling up cables with cable ties, cut off the remaining part. The cut should be smooth and trim without sharp corners, as shown in Figure 7-4.

Figure 7-4 Cutting off an Excess Cable Tie



• When cables need to be bent, bind them first, but do not tie cable ties within the bend. Otherwise, stress may be generated on the cables and causes the wires inside to break, as shown in Figure 7-5.





- Cables not to be assembled or the remaining parts of cables should be folded and placed in a proper position of the rack or cable trough. The proper position refers to a position that does not affect the device running or damage the equipment or cables.
- Do not bind power cords to the guide rails of moving parts.
- The power cords connecting moving parts such as door grounding cables should be reserved with some excess after being assembled. This can avoid tension or stress on power cords. After the moving part arrives

at the position of the power cords, the remaining cable part should not touch heat sources, sharp corners, or sharp edges. If heat sources cannot be avoided, high-temperature cables should be used.

• When using screw threads to secure a cable lug, ensure that the bolt or screw is properly tightened and take measures to prevent it from loosening, as shown in Figure 7-6.

Figure 7-6 Fastening Cable Lugs



1. Flat washer	3. Spring washer
2. Nut	4. Flat washer

- Hard power cords should be fastened in the terminal connection area to prevent stress on terminal connection and cable.
- Do not use self-tapping screws to fasten terminals.
- Power cords of the same type and in the same cabling direction should be bundled up into cable bunches, with cables in cable bunches clean and straight.
- Bundle up cables by using cable ties.

Cable Bunch Diameter	Distance between Every Binding Point
10 mm (0.39 in.)	80 mm to 150 mm (3.15 in. to 5.91 in.)
10 mm to 30 mm (0.39 in. to 1.18 in.)	150 mm to 200 mm (5.91 in. to 7.87 in.)
30 mm (1.18 in.)	200 mm to 300 mm (7.87 in. to 11.81 in.)

- No knot is allowed in cabling or bundling.
- For wiring terminal blocks (such as air switches) of the cord end terminal type, the metal part of the cord end terminal should not be exposed outside the terminal block when assembled.

Contents

	1 Change Description	1
	1.1 ReyeeOS 2.289	1
	1.1.1 Hardware Changes	1
	1.1.2 Software Feature Changes	1
4	2 Fast Internet Access	2
	2.1 Configuration Environment Requirements	2
	2.1.1 PC	2
	2.2 Default Configuration	2
	2.3 Login to Web Interface	2
	2.3.1 Connecting to the Access Point	2
	2.3.2 Configuring the IP Address of the Management Client	2
	2.3.3 Logging in to the Web Page	3
	2.4 Work Mode	4
	2.4.1 AP Mode	4
	2.4.2 Router Mode	4
	2.4.3 Wireless Repeater Mode	5
	2.5 Configuration Wizard (Router Mode)	5
	2.5.1 Getting Started	5
	2.5.2 Configuration Steps	6
	2.6 Configuration Wizard (AP Mode)	9
	2.6.1 Getting Started	9
	2.6.2 Configuration Steps	9
2.7 Configuration Wizard (Wireless Repeater Mode)	9	
---	----	
2.7.1 Getting Started	9	
2.7.2 Configuration Steps	10	
2.8 Introduction to the Web Interface	12	
2.8.1 Management Page for Wi-Fi 6 Products	12	
3 Network Monitoring	1	
3.1 Viewing the Network Information	1	
3.2 Adding Network Devices	3	
3.2.1 Wired Connection	3	
3.2.2 AP Mesh	5	
3.3 Managing Network Devices	13	
3.4 Configuring Network Planning	15	
3.4.1 Configuring Wired VLAN	16	
3.4.2 Configuring Wi-Fi VLAN	19	
4 Wi-Fi Network Settings	22	
4.1 Configuring AP Groups	22	
4.1.1 Overview	22	
4.1.2 Configuration Steps	22	
4.2 Adding a Wi-Fi Network	24	
4.3 Configuring SSID and Wi-Fi Password	27	
4.4 Managing Wi-Fi Networks	28	
4.5 Hiding the SSID		
4.5.1 Overview		
4.5.2 Configuration Steps		

4.6 Configuring Wi-Fi Band	31
4.7 Configuring Band Steering	32
4.8 Configuring Wi-Fi 6	32
4.9 Configuring Layer-3 Roaming	33
4.10 Configuring Client Isolation	33
4.11 Configuring 802.11r	34
4.12 Configuring a Guest Wi-Fi	35
4.12.1 Overview	35
4.12.2 Configuration Steps	35
4.13 Configuring Wireless Rate Limiting	35
4.13.1 Overview	35
4.13.2 Configuration Steps	36
4.14 Configuring Wi-Fi Blocklist or Allowlist	40
4.14.1 Overview	40
4.14.2 Configuration Steps	40
4.15 Optimizing Wi-Fi Network	41
4.15.1 Overview	41
4.15.2 Getting Started	42
4.15.3 Configuring Global Radio Settings	42
4.15.4 Configuring Standalone Radio Settings	45
4.15.5 Configuring WIO	48
4.15.6 Configuring Wi-Fi Roaming Optimization (802.11k/v)	52
4.16 Configuring IGMP Snooping	54
4.16.1 Overview	54

4.16.2 Configuration Steps	54
4.17 Configuring Healthy Mode	54
4.18 Configuring XPress	55
4.19 Configuring Wireless Schedule	55
4.20 Enabling Reyee Mesh	56
4.21 Domain Proxy	56
4.22 Client Association	57
4.22.1 Configuring Intelligent Association	57
4.22.2 Configuring Client Association	58
4.23 Configuring AP Load Balancing	59
4.23.1 Overview	59
4.23.2 Configuring Client Load Balancing	60
4.23.3 Configuring Traffic Load Balancing	61
4.24 Wireless Authentication	63
4.24.1 Overview	63
4.24.2 Configuring One-click Login on Ruijie Cloud	63
4.24.3 Configuring Voucher Authentication on Ruijie Cloud	68
4.24.4 Configuring Account Authentication on Ruijie Cloud	76
4.24.5 Configuring SMS Authentication on Ruijie Cloud	84
4.24.6 Configuring Registration on Ruijie Cloud	91
4.24.7 Configuring an Authentication-Free User List on Web Interface	96
4.24.8 Displaying Authenticated Users on web interface	
4.24.9 Displaying Authenticated Users on Ruijie Cloud	99
4.25 Configuring 802.1X Authentication	

4.25.1 Overview	100
4.25.2 Configuring 802.1X Authentication	100
4.25.3 Viewing Wireless User List	104
4.25.4 Viewing Wired User List	105
5 Network Settings	106
5.1 Switching Work Mode	106
5.1.1 Work Mode	106
5.1.2 Self-Organizing Network Discovery	106
5.1.3 Configuration Steps	106
5.2 Configuring Internet Connection Type (IPv4)	108
5.3 Configuring Internet Connection Type (IPv6)	109
5.4 Configuring LAN Port	109
5.5 Configuring Repeater Mode	111
5.5.1 Wired Repeater	111
5.5.2 Wireless Repeater	111
5.6 Creating a VLAN	113
5.7 Changing MAC Address	115
5.8 Changing MTU	115
5.9 Configuring DHCP Server	116
5.9.1 DHCP Server	116
5.9.2 Configuring the DHCP Server Function	116
5.9.3 Displaying Online DHCP Clients	117
5.9.4 Displaying the DHCP Static IP Address List	118
5.10 Configuring DNS	118

5.11 Configuring Self-Healing Mesh	119
5.12 Hardware Acceleration	119
5.13 Configuring Port Flow Control	119
5.14 Configuring ARP Binding	120
5.15 Configuring LAN Ports	121
5.16 IPv6 Settings	122
5.16.1 Overview	
5.16.2 IPv6 Basic	122
5.16.3 IPv6 Address Assignment Methods	123
5.16.4 Enabling IPv6	123
5.16.5 Configuring the IPv6 Address for the WAN Port	124
5.16.6 Configuring the IPv6 Address for the LAN Port	126
5.16.7 Viewing DHCPv6 Clients	128
5.16.8 Configuring the Static DHCPv6 Address	
5.16.9 Configuring the IPv6 Neighbor List	129
6 Online Client Management	131
6.1 Configuring Client IP Binding	
6.2 Configuring Client Access Control	135
6.3 Configuring Client Association	135
6.4 Blocking Clients	136
6.5 Configuring Client Rate Limiting	138
7 System Settings	140
7.1 PoE Settings	140
7.2 Setting the Login Password	140

7.3 Setting the Session Timeout Duration	141
7.4 Setting and Displaying System Time	141
7.5 Configuring SNMP	142
7.5.1 Overview	142
7.5.2 Global Configuration	142
7.5.3 View/Group/Community/User Access Control	144
7.5.4 SNMP Service Typical Configuration Examples	152
7.5.5 Configuring Trap Service	157
7.5.6 Trap Service Typical Configuration Examples	161
7.6 Configuring Reboot	164
7.6.1 Rebooting the Master Device	164
7.6.2 Rebooting Local Device	165
7.6.3 Rebooting All Devices on the Network	165
7.6.4 Rebooting the Specified Devices	166
7.7 Configuring Scheduled Reboot	167
7.8 Configuring Backup and Import	168
7.9 Restoring Factory Settings	168
7.9.1 Restoring the Current Device to Factory Settings	168
7.9.2 Restoring All Devices to Factory Settings	169
7.9.3 Restoring Master Device to Factory Settings	169
7.10 Performing Upgrade and Checking System Version	170
7.10.1 Online Upgrade	170
7.10.2 Local Upgrade	170
7.11 Switching System Language	171

	7.12 Configuring LED Status Control	171
	7.12.1 Configuring Standalone LED Status	172
	7.12.2 Configuring Network-wide LED Status	173
	7.13 Configuring Cloud Service	173
	7.13.1 Overview	173
	7.13.2 Configuration Steps	173
	7.13.3 Unbinding Cloud Service	175
8 N	Network Diagnosis Tools	176
	8.1 Network Check	176
	8.2 Network Tools	177
	8.3 Alerts	178
	8.4 Fault Collection	179
	8.5 Packet Capturing	180
9 F	FAQs	183
	9.1 Login Failure	183
	9.2 Factory Setting Restoration	183
	9.3 Password Loss	183

1 Change Description

This section outlines the key changes in software, hardware, and documentation across versions. For detailed hardware changes between different versions, please refer to the release notes provided with the software release.

1.1 ReyeeOS 2.289

1.1.1 Hardware Changes

This is the baseline version, with no hardware changes. The following table lists the supported hardware models.

Туре	Model	Version Number
Wi-Fi 6	RG-RAP62	1.xx

1.1.2 Software Feature Changes

This is the baseline version, with no changes to software features.

2 Fast Internet Access

2.1 Configuration Environment Requirements

2.1.1 PC

- Browser: Google Chrome, Internet Explorer 9.0, 10.0, and 11.0, and some Chromium/Internet Explorer kernel-based browsers (such as 360 Extreme Explorer) are supported. Exceptions such as garble or format error may occur if an unsupported browser is used.
- Resolution: 1024 x 768 or a higher resolution is recommended. If other resolutions are used, the page fonts and formats may not be aligned, the GUI is less artistic, or other exceptions may occur.

2.2 Default Configuration

Table 2-1 Default Web Configuration

Item	Default
IP address	10.44.77.254
Username/Password	A username is not required when you log in for the first time. The default password is admin .

2.3 Login to Web Interface

2.3.1 Connecting to the Access Point

You can open the management page and complete Internet access configuration only after connecting a client to the access point in either of the following ways:

Wired Connection

Connect a local area network (LAN) port of the access point to the network port of the PC, and set the IP address of the PC. See <u>2.3.2</u> Configuring the IP Address of the Management Client.

Wireless Connection

On a mobile phone or laptop, search for wireless network **@Ruijie-S***XXX* (XXXX is the last four digits of the MAC address of each device). In this mode, you do not need to set the IP address of the management Client, and you can skip the operation in <u>2.3.2</u> Configuring the IP Address of the Management Client.

2.3.2 Configuring the IP Address of the Management Client

Configure an IP address for the management client in the same network segment as the default IP address of the device (The default device IP address is 10.44.77.254, and the subnet mask is 255.255.255.0.) so that the

management client can access the device. For example, set the IP address of the management client to 10.44.77.100.

🛕 Caution

- Make sure that the client can access the web interface as long as it can ping the access point.
- The IP address of the management client cannot be set to 10.44.77.253, because this IP address is reserved by the device. If the management client uses this IP address, it cannot access the device.

2.3.3 Logging in to the Web Page

(1) Enter the IP address (10.44.77.254 by default) of the access point in the address bar of the browser to open the login page.

Note

If the static IP address of the device is changed, or the device obtains a new dynamic IP address, the new IP address can be used to access the web management system of the device as long as the management client and the device are in the same network segment of a LAN.

	🛛 English 👻
Rujje	
\ \ \ \ \	
Password have read and agreed User Agreement and	
Reyee Data Processing Agreement.	
Forgot Password ③ Google Chrome and Internet Explorer browser 9, 10 or 11 are	
supported. Copyright©2000-2023 Ruijie Networks Co., Ltd.	

(2) On the web page, enter the password and click Log in to enter the web management system.

You can use the default password **admin** to log in to the device for the first time. For security purposes, you are advised to change the default password as soon as possible after logging in, and to regularly update your password thereafter.

If you forget the IP address or password, hold down the **Reset** button on the device panel for more than 5 seconds when the device is connected to the power supply to restore factory settings. After restoration, you can use the default IP address and password to log in.

A Caution

Restoring factory settings will delete the existing configuration and you are required to configure the device again at your next login. Therefore, exercise caution when performing this operation.

2.4 Work Mode

The device can work in the router mode, AP mode or wireless repeater mode. The displayed system menu page and function ranges vary with the work mode. The RAP works in the AP mode by default.

When setting the work mode, you can also set whether to enable the self-organizing network discovery function. This function is enabled by default.

Self-organizing network mode: After the self-organizing network discovery function is enabled, the new device and other unconnected devices can be discovered. Devices connect with each other to form a network based on their status and synchronize their configurations globally. You can log in to the web interface of the device to view management information of all devices on the network. After the self-organizing network discovery function is enabled, you can efficiently maintain and manage the network. You are advised to keep this function enabled.

When the device connect with each other to form a network, two configuration modes are displayed: networkwide mode and local device mode. See <u>2.8</u> Introduction to the Web I.

Local device mode: After the self-organizing network discovery function is disabled, the device will not be discovered. After logging in to the web interface, you can configure and manage only the new device. If only one device is configured or global configuration does not need to be synchronized to the device, you can disable the self-organizing network discovery function.

To switch the work mode, see <u>5.1 Switching Work Mode</u>.

2.4.1 AP Mode

The device performs L2 forwarding and does not support the DHCP address pool function. In AP mode, the device often networks with devices supporting the routing function. IP addresses of downlink wireless clients are assigned and managed by the uplink device (supporting the DHCP address pool) of the AP in a unified manner, and the AP only transparently transmits data.

2.4.2 Router Mode

The device supports N/AT routing and forwarding. The addresses of wireless clients can be assigned by the AP and wireless network data is routed and forwarded by the AP. N/AT is supported in this mode. When an AP works in the router mode, it supports device networking, network-wide configuration, and AP-specific radio functions.

There are three Internet types available: PPPoE, DHCP mode and static IP address mode. You can connect the device to an Ethernet cable or an upstream device.

A Caution

After switching to the router mode, the device's LAN IP address will change to 192.168.120.1. Please obtain an IP address automatically for your management client and enter 10.44.77.254 into the address bar of the browser to log in to web interface again.

2.4.3 Wireless Repeater Mode

The device does not support the routing and DHCP server functions in the wireless repeater mode. IP addresses of the clients are assigned and managed by the primary router. On an available network, the device can be connected to the primary router through wireless connection to expand the Wi-Fi coverage and increase the number of LAN ports and wireless access devices.

2.5 Configuration Wizard (Router Mode)

Upon first login, you can perform quick setup to configure the Internet type, Wi-Fi network and management password.

2.5.1 Getting Started

- Connect the device to a power supply and connect the port of the device to an upstream device with an Ethernet cable. Or you can connect an Ethernet cable to the device.
- (2) Configure the Internet connection type according to requirements of the local Internet Service Provider (ISP). Otherwise, the Internet access may fail due to improper configuration. You are advised to contact your local ISP to confirm the Internet connection type:
 - o Figure out whether the Internet connection type is PPPoE, DHCP mode, or static IP address mode.
 - o In the PPPoE mode, a username, a password, and possibly a service name are needed.
 - o In the static IP address mode, an IP address, a subnet mask, a gateway, and a DNS server need to be configured.
- (3) The device works in the AP mode by default. If you want to switch the work mode to the router mode, perform the configuration on the work mode setting page. See <u>5.1</u> <u>Switching Work Mode</u> for more details.

	P ∉ GMT IP:15 4 ∉ &G1 379	MAC Addr Reyee OS: Monitor	ess: 80x 45 Config	Working Mode AP Hardware Version:1.	
		Normal LED: AP	Location: LED blinking		
Clients 56 Connected: 0 Capacity: 110 Total Connected: 0 Capacity: 110	3 >	SSID 중 @@@###111 2.4G	> 5G	Band 2.4G 5G Channel Auto Char Transmit Power Auto Transmit	> Inel 40 Imit Power Auto
Username	SSID and Band	Signal Quality 🗘	IP/MAC	Negotiation Rate	Online Duration 🗘
				Total 0 <	1 > 10/page >

Working Mode

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.

Working Mode ⑦	Router	r	\sim
Self-Organizing Network ⑦			
AC ⑦			
		Cancel	Save

2.5.2 Configuration Steps

1. Add a Device to Network

You can manage and configure all devices in the network in batches by default. Please verify the device count and network status before configuration.

 \times

(i) Note

New devices will join in a network automatically after being powered on. You only need to verify the device count.

If a new device is detected not in the network, click **Add to My Network** and enter its management password to add the device manually.

ycc Discover Device					🕝 English 🗸		
Total Devices: 2. Other Device Please make sure that the device count an	Total Devices: 2. Other Devices (to be added manually): 1. Please make sure that the device count and topology are correct. The unmanaged switch will not appear in the list.						
Net Status 🔉	R ++++	SW we can see a set of the set of		•			
DHCP	Gateway	Switches	APs	Other Devices			
My Network							
未32 (1 devices)					~		
Model	SN	IP Address	MAC Address	Software Version			
A P [Master]	G1 79	19; 4	80:0	ReyeeOS :			
Other Devices 🕖							
dasui (1 devices)	+ Add to My Network				~		
Model	SN	IP Address	MAC Address	Software Version			
	Re	discover	Start Setup				

2. Creating a Network Project

- (1) Click Start Setup to configure the Internet connection type and Wi-Fi network.
- Internet: Configure the Internet connection type according to requirements of the local Internet Service Provider (ISP).
 - o DHCP: The access point detects whether it can obtain an IP address via DHCP by default. If the access point connects to the Internet successfully, you can click Next without entering an account.
 - o PPPoE: Click PPPoE, and enter the username, password, and service name. Click Next.
 - o Static IP: Enter the IP address, subnet mask, gateway, and DNS server, and click Next.
- Wi-Fi Settings: Select the Wi-Fi configuration mode. This configuration option is unavailable for a new project.
 - o Use Old Settings: Use the Wi-Fi settings of an existing project.
 - o Use New Settings: Configure the Wi-Fi network using new settings.
- **SSID and Wi-Fi Password**: The device has no Wi-Fi password by default, indicating that the Wi-Fi network is an open network. You are advised to configure a complex password to enhance the network security.
- **Country/Region**: The Wi-Fi channel may vary from country to country. To ensure that a client searches for a Wi-Fi network successfully, you are advised to select the actual country or region.
- **Time Zone**: Set the system time. The network time server is enabled by default to provide the time service. You are advised to select the actual time zone.

Ruijie I Rcycc	Network Settings		🕲 English 🗸	⊖ Homepage
	Internet	C PPPoE O DHCP Static IP		
	Wi-Fi Settings	Use old settings O Use new settings		
	Dual-Band Single SSID			
	2.4G+5G			
	* SSID	@Ruijie-s0477		
	Encryption O	Open Osecurity		
	Security	OPEN(Open)		
	No available frequency band? Log in to Ruiji	e Cloud to add or re-identify the target frequency band. Re-identify View Causes		
		Country/Region/Time Zone		
	* Country/Region	China (CN)		
	* Time Zone	(GMT+8:00)Asia/Shanghai		
	P	revious Next		

- (2) Click Next. On the page that is displayed, set the project name and management password.
- **Project Name**: Identify the network project where the device is located.
- Management Password: The password is used for logging in to the management page.

RuffielRcycc	Project Settings			⊘ English ∨	- E→ Homepage
	1 Network Settings			② Project Settings	
		* Project Name	test		
		Management Password	The management passwords of the network-wide dr There are four requirements for setting the password - The password must contain 8 to 31 characters. - The password must contain uppercase and lowercase letters, numbers and three types of speci- characters. - The password cannot contain admin.	al	
		Confirm Password Password Hint	The password cannot contain question marks, spaces, and Chinese characters. Enter new management password again. Enter a hint that can help you remember the manage		
			Previous Finish		

Click Finish. The device will deliver the initialization and check the network connectivity.



Redirecting...

The device can access the Internet now. Bind the device with a Ruijie Cloud account for remote management. Follow the instruction to log in to Ruijie Cloud for further configuration.

🚺 Note

- If your device is not connected to the Internet, click **Exit** to exit the configuration wizard.
- Please log in again with the new password if you change the management password.

2.6 Configuration Wizard (AP Mode)

2.6.1 Getting Started

- Power on the device and connect the device to an upstream device.
- Make sure that the device can access the Internet.

2.6.2 Configuration Steps

The device obtains the IP address through the DHCP by default. Configure the SSID, Wi-Fi password and management password. The default Internet connection type is DHCP mode. You are advised to use the default value.

Ruijie I Rcycc	Network Settings		🕝 English 🗸	← [→ Homepage
	Internet	t O DHCP O Static IP		
	Wi-Fi Setting:	s 🔿 Use old settings 🔹 O Use new settings		
	Dual-Band Single SSID			
	2.46+56			
	* SSID	@Ruijie-s0477		
	Encryption	Open Oceanity		
	Security	OPEN(Open)		
	No available frequency band? Log in to Ruij	ie Cloud to add or re-identify the target frequency band. Re-identify. View Causes		
		Country/Region/Time Zone		
	* Country/Region	n China (CN) 🗸		
	* Time Zone	GMT+8:00)Asia/Shanghai		
	р	Yrevious Next		

2.7 Configuration Wizard (Wireless Repeater Mode)

2.7.1 Getting Started

- Before configuring the wireless repeater mode, configure the primary router and test that the primary router can access the Internet.
- Place the device where it can discover at least two-bar Wi-Fi signal of the primary router.

A Caution

No Ethernet cable is required in the wireless repeater mode. The wireless network stability can be affected by many factors. Therefore, the wired connection is recommended.

2.7.2 Configuration Steps

(1) Connect the device to a power supply without connecting an Ethernet cable to the uplink port, and click **Start Setup**.

Ruíjie Rcy	CC Discover Device					
	Total Devices: 2. Other Device Please make sure that the device count an	s (to be added manually d topology are correct. The unmar	/): 1. naged switch will not appe	ar in the list.		0
	Net Status 🕄	R •••••	or an area well with		•	
	DHCP	Gateway	Switches	APs	Other Devices	
	My Network					
	未32 (1 devices)					~
	Model	SN	IP Address	MAC Address	Software Version	
	A P [Master]	G1 . 79	19; 14	80:0	ReyeeOS ;	
	Other Devices 0					
	dasui (1 devices)	+ Add to My Network				~
	🗹 Model	SN	IP Address	MAC Address	Software Version	
		Re	ediscover	Start Setup		

(2) If you see a dialogue box indicating that the Ethernet cable is not connected to the WAN port, click **Wireless Repeater**.



(3) Select the primary router SSID that requires expanding the Wi-Fi coverage, enter the Wi-Fi password of the primary router, and click **Next**.

IRCycc Wireless Repeater				🗘 Alert Center
	Qssid		G	
	5G 132		(;	
	5G abc_plus_5G	÷	(î;	
	5G @Ruijie-sD2CE_plus_5G		((r	
	5G down		(î;	
	5G 213dsa		(î;	
	5G @@@	⇔	(î;	
	5G 222	÷	(î;	
	5G 333	£	((r	
	5G ruijie-guest		(î)	
	5G rj-network	£	•	
	5G ruijie-office	£	÷	
	2.4G @Ruijie-sD2CE_plus		(î)	

Rபராச Rcycc Wireless Repeater			\bigcirc English $\sim \models$ Exit
	Please enter the Wi-Fi password		
	Primary Router SSID abc_plus_5G		
	* Password		
	Please enter a password.	۲	
	Previous Next		

(4) Set the SSID and password and click Save. Then, the Wi-Fi network will be restarted.

Ruijie RCYCC Wireless Repeater		ậ Alert Center → @ English ~[-
	Local Router Wi-Fi	
	Same as Primary Router Wi-Fi New Wi-Fi SSID(2.4G) abc.plus_5G SSID(5G) abc.plus_5G	
	Wi-Fi Password	٢
	Management Password Same as V	Wi-Fi Password
	* Management Password(Please remember the password Length: 8-31 characters.	word.)
	Previous Save	

(5) Set the country/region code and time zone, and click ${\bf Save}.$

e IRcycc Wireless Repeater		ධූ Alert Center	⊗ English ~
	Country/Region/Time Zone		
	* Country/Region China (CN)		
	Previous Save		

2.8 Introduction to the Web Interface

To facilitate flexible device management, the Web page displays different system configuration menus in different work modes. For details about the work mode, see <u>5.1</u> Switching Work Mode.

As to the RG-RAP62 model, please refer to 2.8.1 Management Page for Wi-Fi 6 Products.

The self-organizing network discovery function is enabled by default, but can be disabled manually. After this function is disabled, the web interface displays the local device mode.

When the self-organizing network discovery function is enabled, you can switch between the network-wide mode and the local device mode. The displayed function menus vary with the mode.

Note

After the self-organizing network discovery function is enabled, the system configuration menus on the web interface depends on the primary device on the network. If the primary device supports Wi-Fi 6 or later, the web interface of the other devices on the network is the same as that of the primary device.

2.8.1 Management Page for Wi-Fi 6 Products

1. Enabling Self-Organizing Network Discovery

- Network-Wide Mode: Displays the management information of all devices on the network. You can configure all devices on the network from a network-wide perspective.
- Local Device Mode: You can only configure the current logged in device.

Network-Wide Mode.

Ruijie IRcycc		C Search	⊖ Alert Centen ⊘ English ~ Exit
One-Device	radio ℓ. ᢙ → → Workspace :=	Physical Topology	⊘ 7 m 1 + Discover Devices
Network-Wide	n 🕫 🗞 Network WLAN O Quick Se		
Devices	Wireless ^	Harmen	
ù.] Clients	😤 🚆 🛱	UNIXOUWN	
 System 	& ¤	SNE UNIXADAM	
	Blocklist AP Mesh LAN Ports		
	× • •		
	LED Client As DNS Proxy	Net in SON SW	
	Wired ^	SN: G1	
	۵ H W	port 10 port 12 port 6 port 3	port 9 Rotate
	WAN DHCP Sn RLDP	(WAN) (WAN) (WAN)	WAN O Restore
	SW Confin	Net in SON	Refresh
	Sw coming	SN: G1, 697 SN: G10, 100, 000, 288 SN: MJ 000, 000, 000, 000, 000, 000, 000, 0	SN: G1^// 233
	Network-Wide		
	SNMP Diannosa Raboot	Last Updated: 2023-12-05 04:00:12	
L .			

Local Device Mode.

- To access the local device mode for the configuration and management of a single device, perform the following steps:
 - o Method 1: Click the device name in the One Device menu and then click Config.

Ruíjie I Rcycc			⊥ Alert Center ⊗ English ~ Exit
One-Device		AP 2 MGMT IP:191	MAC Address: 48:01:01:02:02:E3 Working Mode:AP Reyee OS: Hardware Version:1.01
Network-Wide		Monito	Config
Clients System	Q	Clients 3 > SSID 56 Connected: 0 Capacity: 512	Band Acc
System		Total Connected: 0 Capacity: 512	2.4G 5G Channel Auto 2.4G 5G Transmit Power Auto
	ට Restore	Signal Qu Username SSID and Band ‡	ality Negotiation Onlin IP/MAC Rate ‡
	ର Refrest		No Data
			Total 0 < 1 > 10/page >
L			

• Method 2: Choose Network-Wide > Devices and click Manage next to a device in the AP list.

Ruíjie I Reyce					Q Search				Alert Center	⊘ English ~ Exit
One-Device		All (8) Gatewa Devices outsi Group: All Groups	ay (0) AP (7) S de your network hav Expand ⑦ Che	witch (1) AC	(0) Router (0) 💽 I. Handle Basic Info RF II	Select Reboo	t Batch Upgrade	0	Delete Offline	IAC/hostname/SN/Sr Q
Network-Wide			Username ⑦	Model 🗘	SN ‡	IP Address 🗘	MAC Address 🗘	Clients ‡	Device Group	Action
Devices		• 🔀	AP 2	In a close	G15	192.1 ***** 65 Ø.	48:8 :E3	0	Default	Manage Reboot
 Clients System 	•	• *	AP 2	L	G1C2122203350C	192.1	C4:7 DC	0	Default	Manage Reboot
<i>u</i> ,		•)*(AP &	I (5)	G1CH2LC000038	192	C4:7 \:16	0	Default	Manage Reboot
		• 🔀	AP Ø	·····;)	G1Q520	192	C4:7 C:E4	0	Default	Manage Reboot
		• 🔀	AP [Moster] Z	;-)	G1C, 597	192. 18 🖉	C4:70 D:28	0	Default	Manage Reboot
		• .	AP 2		G15!****** 1233	192.1 5 🖉	10:82 E8	0	Default	Manage Reboot
		• 🔀	AP 2		MA(************************************	192.1 13 <i>Q</i>	00:D0 8:91	0	Default	Manage Reboot

Ruijie	Rcycc			△ Alert Center 🛛 🔗 English ~ 🛛 Exit
P	← Devices			
©	•	AP & MGMT IP:19 65 & SN:GTS 4	MAC Address: 48 E3 Reyee OS2	O Reboot Hardware Version:1.01
ណ			Monitor Config	
\odot	Q search	WAN WAN_v6 Settings		
	Bevice Overview	* Internet ⑦ DHCP		
Þ	Clients	Username and passw	ord are not required.	
	Network ^	IP Address 192.168.110.65		
	WAN	Subnet Mask 255.255.255.0		
	LAN	Gateway 192.168.110.1		
	Work Mode	DNS Server 192.168.110.1		
	🗢 WLAN	Dedicated DNS Optional		
	🖻 Advanced 🗸 🗸	Server (2) Advanced Settings		

2. Disabling Self-Organizing Network Discovery

If a device is in standalone mode, you can configure and manage only the currently logged in device. The web interface displays the configuration menu of a single device on the left side.

Fast Internet Access

Configuration Guide

Ruíjie I Rcycc			ර Cloud Service රා Alert Center 🚯 W	fizard 🛛 🕹 English 🗸	Exit
Q search	Device Info				
Clients	Memory Usage 37%	Online Clients	Connection Status: Online Uptime: 22 hours 53 minutes 15 seconds System Time: 2		
Metwork			-,		
⇔ wlan v	Device Details Model: 1	Device Name: 62 🖉	SN: r		
🖻 Advanced 🗸 🗸	MAC Address: Coloradorea	Working Mode: AP 🖉	Hardware Version: 1.00		
Diagnostics	Ethernet status 🕐				
System	•	LAN			
		B			
				Click RITA for help). 👩
					Ail

3 Network Monitoring

Choose Network-Wide > Workspace > Topology.

The **Overview** webpage displays the current network topology, real-time uplink and downlink flow, networking status, and the number of users. The quick access to network and device settings is also provided on the **Overview** webpage. Users can monitor, configure and manage the network status on the current page.

Ruíjie I Rcycc		Q Search	û Alert Center	
One-Device	د جو ک	Physical Topology	🔀 1	+ Discover Devices
Network-Wide	Workspace i≡			
Workspace				
Devices	Network WLAN O Quick Se			
[] Clients	Wireless ^	+		
 System 	📚 🛬 📚 Wi-Fi Radio Se Rate Limi			
	& Ø Ø	Unknown		
	Blocklist Wireless AP Mesh	UNINOWN SNE UNKNOWN		
	M X	UNKNOWN		J↑ Rotate
	Load Bal LAN Ports LED	WAN		0 Restore
				C
	Chent As Domain	• 62 SN: 111111		Reinesti
	Wired			
	WAN	Last Updated: 2024-11-07 10:20:23		2

3.1 Viewing the Network Information

You can view the online device, port ID, device SN as well as the real-time uplink and downlink flow in the network topology.



• Click the egress gateway to view real-time traffic information of the device.



Click the device in the topology to view the operating status and configuration of the device and configure the device functions. The hostname is set to the product model by default. You can click to modify the hostname.

Ruíjie	Rcycc			Q Search			유 Alert Center	⊗ English ∨ Exit
P	← Workspace							
				AP 4				(D) Reboot
©			· / ? \	MGMT IP:192).65 L	MAC Address: 4	Working Mode	e:AP
<u></u>				314.0131 334		Reyee OS.	Haluwale veis	101.101
<u>.</u> .					Mor	itor Config		
\odot				WHE	Normal			
		*			LED:	AP Location: LED blinking		
ŀ		SNE GTQHEL	Clients	3 >	SSID	>	Band	>
		4	5G Connected: 0 Capacity: 512		? @@@@5(3	2.4G	5G
		Rotate	Total Connected: 0 Capacity: 51	2	奈 @@@123123	2.4G 5G	Transmit Power Auto	Transmit Power Auto
		Restore			Signal Quality			Online Duration
		C Refresh	Username	SSID and Band	÷	IP/MAC	Negotiation Rate	¢
						No Data		
							Total 0 < 1	> 10/page ~

• The update time of the topology is displayed at the bottom left corner. Click **Refresh** to update the topology to the latest status. Please wait for a few minutes for the update.



3.2 Adding Network Devices

3.2.1 Wired Connection

(1) If a new device is connected to the device in the network through wired connection, a prompt message will pop up, indicating that a device not in SON (Self-Organizing Network) is discovered. The number (in orange)

of devices that are not in SON is displayed under the **Devices** at the top left corner of the page. Click **Handle** to add the device to the current network.



(2) Go to the Network List page, click Other Network to select the target device and click Add to My Network.

Ruijie IRcycc					🗘 Alert Center 🛛 🔗 English ~	Exit						
One-Device	 Every network varies in devices an 	nd configuration. You can add devi	ces of Other Network to	My Network.		?						
	My Network											
Network-Wide	: (1 devices)					~						
© Workspace	Model	SN	IP Address	MAC Address	Software Version							
Devices	A P (Master)	G .)	192. 4	80:0 2:45	ReyeeOS							
Clients	New Device List											
 System 	New Device (1 devices)	+ Add to My Network				~						
	Model	SN	IP Address	MAC Address	Software Version							
	APF.,)	CAI 734	19. 93	30:0E 94:BF	AP_"							
	Other Network											
	Unnamed Network (1 devices)	+ Add to My Network				~						
	💆 Model	SN	IP Address	MAC Address	Software Version							
	Switch po seesson.p	G1Q 1047	192 59	00:D)1:11	ESW	6						

If the target device is not configured yet, you can add the device directly without a password. If the device is configured with a password, please enter the management password of the device. If the password is incorrect, the device cannot be added to the network.



3.2.2 AP Mesh

1. Overview

After being powered on and enabled with Mesh (see <u>4.20</u> Enabling Reyee Mesh for details), a Mesh-capable new AP can be paired with other Mesh-capable wireless devices on the target network through multiple ways. Then the AP will be synchronized its Wi-Fi configuration with other devices automatically. Mesh networking addresses pain points such as complex wireless networking and cabling. A new AP can be connected to any uplink wireless device among AP, EG router, and EGW router in the following ways:

- Button-based pairing: Short press the Mesh button on the EGW router on the target network to implement fast pairing of the AP with the EGW router.
- Search-based pairing: Log in to the web interface of a device on the target network. Search and add APs to be paired.
- Wired pairing: Connect the new AP to a wireless device on the target network using an Ethernet cable. The new AP will go online on the target network.

After pairing finishes, the new AP obtains the wireless backhaul information from network-wide neighboring APs. Install the new AP as planned, and it will connect to the optimal neighboring AP.

2. Configuration Steps



3. Configuration Steps for Button-based Pairing

A Caution

- The uplink device is an EGW router.
- Only EG105GW-X and EG105GW(T) support button-based pairing, and each router can be paired with up to 15 new APs.

- The primary device must be properly configured. Otherwise, AP mesh failure may occur due to constant channel scanning.
- The new AP must be in factory status.
- It can be scanned only when the live network is enabled with Mesh (see 4.20 <u>Enabling Reyee Mesh</u> for details).
- Place the new AP no more than 2 meters away from the uplink device to ensure that the new AP can receive the Wi-Fi signal from the uplink device. The new AP may fail to be scanned due to the long distance or obstacles between it and the uplink device.
- (1) Power on the new AP and place it near the EGW router on the target network.
- (2) Press and hold the Mesh button on the EGW router for no more than two seconds to start pairing. The pairing process takes about one minute.
- (3) Check the topology on the Physical Topology page to make sure that the new AP has connected to the uplink device in wireless mode.



- (4) Power off the new AP and install it as planned.
- (5) Log in to the web interface of a device on the target network. In Network-Wide mode, choose Devices > AP.

Make sure that the new AP is online and the corresponding entry contains icon in the **Relay** in the **Relay** Information column. The icon indicates that wireless backhaul is performed through the 5 GHz radio.

Configuration Guide

All (54)	Gateway (1) AP (50)	Switch (2)	AC (1)	Router (0)	0)					
							Select	Batch Upgr	rade 🕐	Delete Offline	IP/MAC/hostname/	SN/SEQ
🕛 Devic	es outside y	our network hav	/e been discove	red. Hand	dle							
Group: All C	Groups Exp	pand ⑦ Ch	ange Group 🕐	• • B	asic Info 🛛 🔾	RF	Information 🔿 M	lodel				
		Username ?	Model 🗘		¢ ¢		Device Group	Relay Information ≑	Softwa	re Version ⑦	Acti	on
• >	?	AP 🖉		:	0 0		Default	Wired View Details	ReyeeOS		Manage	Reboot
• >	?	AP 🖉			0		Default	Wired View Details	ReyeeOS	{	Manage	Reboot
• >	* *	AP 🖉		i	7 0		Default	Wired View Details	ReyeeOS	1	Manage	Reboot
•)	\$ \	AP 🖉		i	i 0		Default	Wired View Details	ReyeeOS	2	Manage	Reboot
• >	*	AP 🖉			6 O		Default	중 5G View Details	ReyeeOS		Manage	Reboot

(6) Click View Details following the

🛜 5G

icon to obtain information about the uplink device and RSSI.

•	AP 🖉	 0	Default	View Details	Noise Floor: -82	dBm	ot
•	AP 🖉	7 0	Default	Wired View Details	Utilization: 16 % RSSI: -26 dBm Good		
•	AP 🖉	i O	Default	Wired U View Details	legotiation Rate: 173 lptime: 13 minutes 18	Mbps seconds	ot
•	AP 🖉	i O	Default	중 5G View Details		5G	ot
•	AP 🖉	· 0	Default	View Details	AP odel: I	AP Model:	ot
•	AP 🖉	i 0	Default	Wired SN View Details	: ZASI 923 192 155	SN: G1NC 79 IP: 192 .31	ot

4. Configuration Steps for Search-based Pairing

A Caution

- Uplink device is an AP or EGW router.
- The primary device must be properly configured. Otherwise, AP mesh failure may occur due to constant channel scanning.
- The new AP must be in factory status.
- It can be scanned only when the live network is enabled with Mesh (see <u>4.20 Enabling Reyee Mesh</u> for details).
- Place the new AP no more than 2 meters away from the uplink device to ensure that the new AP can receive the Wi-Fi signal from the uplink device. The new AP may fail to be scanned due to the long distance or obstacles between it and the uplink device.
- You can scan to discover new APs on the AP Mesh page only when there are APs supporting the AP Mesh function on the network.
- (1) Power on the new AP and place it near the AP or EGW router on the target network.
- (2) Log in to the web interface of a device on the target network. In Network-Wide mode, click +Discover Devices in the upper right corner of the Physical Topology page to scan the APs in other networks not plugged in with Ethernet cables.

Rujje IRcycc		c) Search			⊥ Alert Center	🕝 English 🗸 📃	Exit
One-Device	radio 4.	Physical Topology			⇔ 1 ⊠ 50	@2 @1 ₽6	+ Discover Device	es
Controller	Workspace i≡							
🖴 Gateway	EM 🔅 🗞							
Network-Wide	Network WLAN O Quick Se							
Workspace	Wireless ^			(WN) † 0.00bps → 0.00bps				
Devices	() () () () () () () () () () () () () (R				
Clients	Wi-Fi Radio Se Rate Limi		(LAND) (LAND	SIN CAPIT B68	(100)	(14)(2)(8)(4)(2)	7	
⊘ System	Blocklist Wireless 802.1x A	WAY WAY WAY Group	AC • • • • • • • • • • • • • • • • • •	Б 	Likemen • UNIXXOWN Site UNIXXOWN Site UNIXXOWN	(port)) Second Second	Carets Rot	J∖ tate
	8 9		Ļ		www	Rest	D atore	
	AP Mesh Load Bal LAN Ports			19/19	(14/14)	16/16	C Refi	ධ fresh
	× •							
	LED Client As DNS Proxy							
	Wired ^	Last Updated: 2023-12-15 16:58:23						

(3) On the **AP Mesh** page, click **Scan** to scan devices that are not connected to the network via an Ethernet cable.

Device Networking	AP Mesh	
<i>i</i> Every network	rk varies in devices and configuration. You can add devices of Other Network to My	Network.
My Network		
radio (53 devices)		
Other Device		
		No data
		Scan

(4) Select the APs to be added and click Add to My Network. No more than eight APs are allowed at a time. Wait until network merging finishes.

Version

(5) Check the topology on the **Physical Topology** page to make sure that the new AP has connected to the uplink device in wireless mode.



- (6) Power off the new AP and install it as planned.
- (7) Log in to the web interface of a device on the target network. In Network-Wide mode, choose Devices > AP.

Make sure that the new AP is online and the corresponding entry contains icon in the **Relay** in the **Relay** Information column. The icon indicates that wireless backhaul is performed through the 5 GHz radio.

All (54) Gatew	vay (1) AP (50)	Switch (2) AC	C (1) Rou	ıter (0)	0			
					Select Rebo	Batch Upgra	ade (?) Delete Offline	IP/MAC/hostname/SN/S⊢Q
Devices outsi	de your network h	ave been discovered.	Handle					
Group: All Groups	Expand ⑦	Change Group 🕐	Basic Inf	fo OR	F Information	Model		
	Username (¢	?) Model 🌲	*	Clients \$	Device Group	Relay Information ≑	Software Version ⑦	Action
•	AP 🖉	. ,)	0	Default	Wired View Details	ReyeeOS	Manage Reboot
•	AP 🖉			0	Default	View Details	ReyeeOS ;	Manage Reboot
•	AP 🖉		7	0	Default	Wired View Details	ReyeeOS ;	Manage Reboot
•	AP 🖉		i	0	Default	Wired View Details	ReyeeOS 2	Manage Reboot
•	AP 🖉		à	0	Default	중 5G View Details	ReyeeOS	Manage Reboot

奈 5G

icon to obtain information about the uplink device and RSSI.

•	AP 🖉		0	Default	View Details	Noise Floor: -82	dBm	ot
•	AP 🖉	7	0	Default	View Details	Utilization: 16 % RSSI: -26 dBm Good		
•	AP 🖉	i	0	Default	View Details	Uptime: 13 minutes 18	Mbps seconds	ot
•	AP 🖉	i	0	Default	중 5G View Details		5G	ot
•	AP 🖉		0	Default	View Details	AP Model: 1	AP Model:	ot
•	AP 🖉	i	0	Default	Wired View Details	SN: ZASL _ 923 IP: 192 155	SN: G1NC 79 IP: 192 .31	ot

5. Configuration Steps for Wired Pairing

🛕 Caution

- Uplink device is an AP, EG router, or EGW router.
- The new AP must be in factory status.
- It can be scanned only when the live network is enabled with Mesh (see <u>4.20 Enabling Reyee Mesh</u> for details).
- (1) Plug one end of the Ethernet cable to the uplink port of the new AP, and the other end to the downlink port of an AP, EG router, or EGW router on the target network. Mesh networking takes one to three minutes. When the system status LED is steady on, it indicates that Mesh networking finishes.
- (2) Log in to the web interface of a device on the target network. In **Network-Wide** mode, choose **Devices** and make sure that the new AP is online.

All (54)	Gateway (1)	AP (50)	Switch (2)	AC (1)	Router (0)	0							
						Select	Reboot	Batch Upgrade	() De	lete Offline	MAC/hostname/SN/Sr Q		
🕛 Devi	Devices outside your network have been discovered. Handle												
Group: All	Groups Expa	and ⑦ Cha	inge Group 🕐	O Ba	isic Info 🛛 🔿 R	RF Informat	ion 🔿 Mo	del					
		Username ⑦ ¢	Model 🗘		SN \$	IP A	ddress ≑	MAC Address 🗘	Clients \$	Device Group	Action		
Local .	÷.	AP 🖉			G1)4233	19.	15 L	10:8 I:E8	0	Default	Manage Reboot		
•	*	AP			ZAS 0170	No IF Availa	Address	E0:1 9:12:F1	0	-	Manage Reboot		
·	\$ \$	AP 🖉			G1N 00379	19	0.31 🖉	80:():45	0	Default	Manage Reboot		

- (3) Self-Healing Mesh is disabled by default. You need to enable it first (for details, see<u>5.11 Configuring Self-Healing Mesh</u>) to complete the wired-to-wireless handoff process.
- (4) Unplug the Ethernet cable, power off the new AP, and install it as planned.
- (5) Log in to the web interface of a device on the target network. In Network-Wide mode, choose Devices > AP.

Make sure that the new AP is online and the corresponding entry contains icon in the **Relay** in the **Relay Information** column. The icon indicates that wireless backhaul is performed through the 5 GHz radio.

Configuration Guide

All (54)	Gateway (1) AP (50)	Switch (2)	AC (1)	Router (0)	0)					
							Select	Batch Upgr	rade 🕐	Delete Offline	IP/MAC/hostname/	SN/SEQ
🕛 Devid	es outside y	our network ha	ve been discove	red. Hand	dle							
Group: All C	Groups Ex	pand ⑦ Cł	ange Group 🕐	O Ba	asic Info	RF	Information 🛛 🔿 N	lodel				
		Username ?) Model 🌐		¢ ¢		Device Group	Relay Information \$	Softwa	re Version ⑦	Acti	on
• >	\$ \	AP 🖉			0 0		Default	Wired View Details	ReyeeOS		Manage	Reboot
•)	ج (AP 🖉			0		Default	Wired View Details	ReyeeOS		Manage	Reboot
• >	* *	AP 🖉			7 0		Default	Wired View Details	ReyeeOS	1	Manage	Reboot
•)	*	AP 🖉		i	i 0		Default	Wired View Details	ReyeeOS	î	Manage	Reboot
•)	*	AP 🖉			i 0		Default	중 5G View Details	ReyeeOS		Manage	Reboot

(6) Click View Details following the

奈 5G

icon to obtain information about the uplink device and RSSI.

•	AP 🖉	 0	Default	Wired View Details	Noise Floor: -82 dBm	ot
•	AP 🖉	7 0	Default	View Details	Utilization: 16 % RSSI: -26 dBm Good	ot
•	AP 🖉	i 0	Default	View Details	Vegotiation Kate: 1/3 Mbps Uptime: 13 minutes 18 seconds	ot
•	AP 🖉	i 0	Default	중 5G View Details	5G	ot
•	AP 🖉	· 0	Default	View Details	AP AP Model:	ot
•	AP 🖉	÷ 0	Default	Wired View Details	SN: ZASL 923 SN: G1NC 79 IP: 192 155 IP: 192 .31	ot

6. Enabling WAN Port

The WAN port works as the wired uplink port of the AP by default. For the AP added to the target network through Mesh pairing, the WAN port is disabled by default. If you want to connect the Mesh AP to other downlink device in wired mode to expand the network, enable this port.

 Log in to the web interface of the network project. Choose Network-Wide > Devices > AP, and click Manage next to a device in the AP list.

All (54)	Gateway	y (1) AP (50)	Switch (2) AC (1) Router (0) 🜔					
					Select	Batch Upgrade	?	Delete Offline	IP/MAC/hostname/SN/Sr Q
🕛 Devi	ces outside	your network hav	e been discovered. H	andle					
Group: All	Groups	Expand ⑦ Cha	ange Group ⑦	Basic Info ORF In	nformation O Mo	odel			
		Username ⑦	Model ≑	SN 🌩	IP Address ≑	MAC Address ≑	Clients \$	Device Grou	p Action
Loca ·	÷	AP 🖉		G1SK3 04233	192. 0.45 🖉	10:82 :E8	0	Default	Manage Reboot
•	¢	AP		ZASLA: 170	No IP Address Available	E0:5D 2:F1	0	-	Manage Reboot
•	?	AP 🖉		G1NQCA 79	192.1(10.31 Ø	80:(2:45	0	Default	Manage Reboot

(2) Choose **Config > Advanced > Enable WAN**, toggle on **Enable**, and click **Save**.



7. Querying Mesh APs and Mesh Details

- (1) Log in to the web interface of a device on the target network.
- (2) Query Mesh APs.
- Method 1: In **Network-Wide** mode, check the topology on the **Physical Topology** page. The AP that connects to the uplink device in wireless mode is a Mesh AP.



 Method 2: In Network-Wide mode, choose Devices > AP. If an entry contains icon Relay Information column, the corresponding AP is a Mesh AP.



All (54)	Gateway (1)	AP (50)	Switch (2)	AC (1)	Router (0)	0			
						Select	Reboot Batch Upgr	rade ⑦ Delete Offline	IP/MAC/hostname/SN/Sr Q
🕛 Devic	es outside yo	ur network hav	e been discove	red. Handl	е				
Group: All G	iroups Expa	and ⑦ Cha	ange Group 🕐	O Bas	ic Info	RF Information	O Model		
		Username ⑦ ¢	Model ≑	45	Clients ‡	Device Group	Relay Information ≑	Software Version ⑦	Action
• >	R. X	AP 🖉)	0	Default	View Details	ReyeeOS	Manage Reboot
•	R. X	AP 🖉			0	Default	View Details	ReyeeOS ;	Manage Reboot
•	R. L	AP &		7	0	Default	View Details	ReyeeOS 2	Manage Reboot
•	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	AP 🖉		i	0	Default	View Details	ReyeeOS 2	Manage Reboot
• >	P	AP 🖉		ŝ	0	Default	중 5G View Details	ReyeeOS	Manage Reboot

(3) Query Mesh networking details.

In Network-Wide mode, choose Devices > AP. Select the target AP, and click View Details in the Relay Information column to obtain the Mesh networking details.

•	AP 🖉		0	Default	Wired View Details	Noise Floor: -82 dBm	ot		
•	AP 🖉	7	0	Default	Wired View Details	Utilization: 16 % RSSI: -26 dBm Good			
•	AP 🖉	i	0	Default	View Details	Uptime: 13 minutes 18 seconds	ot		
•	AP 🖉	i	0	Default	중 5G View Details	5G	ot		
•	AP 🖉		0	Default	Wired View Details	AP AP Model: I Model:	ot		
•	AP 🖉	i	0	Default	View Details	SN: ZASL 923 SN: G1NC 77 IP: 192 155 IP: 192 .31	9 ot		

3.3 Managing Network Devices

You can view information of all devices on the network. You can configure and manage all devices on the network by simply logging in to only one device on the network. Follow the following steps to access the device's management page:

• Method 1: Click the device icon in the upper right corner of the topology to switch to the device list view.



Method 2: Choose Network-Wide > Devices.
Configuration Guide

RuffelRcycc					Q Search			⊉ Alert Center	🕝 English ~ 🛛 Exit
One-Device		All (7) Gateway	(0) AP (6) Si	witch (1) AC (0)	Router (0) 📀		Select Re	boot Delete Offline IP/M/	AC/hostname/SN/Sr Q
□ 1 .) Network-Wide			Username ⑦	Model 🗘	SN ¢	IP Address 🗘	MAC Address 🗘	Software Version ⑦	Action
(i) Workspace		• 🔀	AP 2	F	G15k _ 1654	192.1 .65 Ø	48:8 ::E3	ReyeeOS I	Manage Reboot
Devices		• 🔀	AP Z	۱	G15 4233	192.101 15 Ø	10:81:E8	ReyeeOS .	Manage Reboot
Clients		• 🔀	AP [Master] &		G1C 0520	192.1 d	C4:70 4C:E4	ReyeeOS :	Manage Reboot
⊘ System	•	• 💌	AP Z	1	MA ZX01	192.1: 1 &	00:DC ::91	ReyeeOS 1 7	Manage Reboot
		• 🔀	AP &	.)	G1C, 50C	192.1 L	C4:7()C	ReyeeOS 2 1	Manage Reboot
		• >	AP &		G1(238	19262 <i>Q</i>	C4:70)A:16	ReyeeOS	Manage Reboot
		• SW see mar.	Switch 4	F	G1P _ A	192 .54	30:0D: E3:E1	ESW_1 . ,	Manage Reboot
								Total 7 🦿 🕇	> 10/page ~

(7) Gateway ((0) AP (6) S	witch (1) AC (0)	Router (0) 🖸		Select Re	boot Delete Offline IP/M	AC/hostname/SN/Sr C
Devices outside	your network have	e been discovered.	Handle				
	Username ⑦	Model 🌲	SN \$	IP Address 🌲	MAC Address 🌲	Software Version ⑦	Action
•	AP 🖉		G1Sk 654	192.1 🖉	48:8 :E3	ReyeeOS .	Manage Reboo
•	AP 🖉		G1S 004233	192. <u></u>	10:8 1:E8	ReyeeOS 🤅	Manage Reboo
•	AP [Master] 🖉		G1C0520	192. ⁻ 🖉	C4:7 :4C:E4	ReyeeOS	Manage Reboot
•	AP 🖉		MAC 2ZX01	192 <i>&</i>	00:D 38:91	ReyeeOS	Manage Reboot
•	AP 🖉		G1Q)50C	192. 🦳 🖉	C4:70:/ ':4C:DC	ReyeeOS	Manage Reboot
•	AP 🖉	-	G1QI)238	192. i 💦 c 🖉	C4:70 A:16	ReyeeOS ELEVINEUE	Manage Reboot
• SW 10001 (000	Switch 🖉	-	G1PQ 0A	192.	30:0D 3:E1	ESW	Manage Reboot

• Click **Select** to select an offline device, and click **Delete Offline** to remove the selected device from the list and the topology.

All (7) Gat	eway (0) AP (6) S	witch (1) AC (0)	Router (0) 🜔		Select Rel	Delete Offline	IP/MAC/hostname/SN/Sr Q
Devices of	utside your network have	e been discovered. <mark>Ha</mark> r	dle				
	Username ⑦ ¢	Model ≑	SN \$	IP Address ≑	MAC Address 🗘	Software Version ⑦	Action
1968) · 沃	AP 🖉		G15 4	19; 🖉	48:	ReyeeOS	Manage Reboot

Network Monitoring

All (7) Gateway (0)	AP (6) Switch (1	I) AC (0) F	Router (0) 🖸	De	Reboot	Delete Offline IP/M/	AC/hostname/SN/S+ Q
Devices outside your	network have been o	discovered. Handl	e				
•	Username ⑦ ¢	Model ≑	SN ≑	IP Address ≑	MAC Address ≑	Software Version ⑦	Action
	AP 🖉		G15 654	192.1(5 Ø	48:81:	ReyeeOS	Manage Reboot

3.4 Configuring Network Planning

Choose Network-Wide > Workspace > Network Planning.

Ruíjie IRcycc		Q Search			🕝 English 🗸	Exit
One-Device	radio & ⊘ →	Physical Topology		⊠6 📾 1	+ Discover D	evices
a .)	Workspace i≡					
Network-Wide © Workspace	Network WLAN O Quick Se		€			
Devices	Wireless ^					
Clients	((c.		Unkinown Unkinown SN-1 Incontration			
 System 	Wi-Fi Radio Se Rate Limi					
	2. 🖾 🚥		(WAN) (pert)			1
	Blocklist AP Mesh LAN Ports		Nut in SDN DW Image: Comparison of the state of the			Rotate
	× 🕫 🔺		÷			O Restore
	LED Client As DNS Proxy		wm *			C Refresh
	Wired ^		AP Group			
	ē 4 e					
	WAN DHCP Sn RLDP	Last Updated: 2023-12-06 04:00:12				

Click the SSID to edit the Wi-Fi configuration. For details, see Chapter 3 Wi-Fi Network Settings.

Network Planning(2)	All ~	Æ	Ð	<
			S	
VLAN1 Wired VLAN Wi-Fi VLAN VLAN1	N	•		
VLAN2 Wired VLAN Wi-Fi VLAN VLAN2	4 >	Unkno	wn	
		• UNKN	IOWN	
			NOWN	
		UNKNOWN	UNKNOWN (port 1)	
		Not in SON	SW	
		• SN: 6 75	SN: (A	Rotate
			L. C.	් Restore
			wan	C
			8/8	Refresh
			• AP Group	
		@@@@ 11111111		
Edit Wi-Fi VLAN			×	
* SSID	@@@@			
Purpose 🕐 🖸	General [IoT [Gues	it		
Band 🕐 🔽	2.4G SG			
No	o available frequency bar	nd? Log in to Ruijie Cloud	to add or re-identify	
the	e target frequency band.	Re-identify View Causes	2	
Encryption 🧿	Open O Security	802.1x (Enterprise)	0	
* Security 🕐	OPEN(Open)	\sim		
	Advanced Settings			
	o and a second			
			Cancel	

3.4.1 Configuring Wired VLAN

Choose Network-Wide > Workspace > Network Planning. On the Network Planning page, click Add Wired VLAN.



Alternatively, you can select an existing wired VLAN and click Setup to edit the VLAN.



(1) Configure the VLAN ID, address pool server, and DHCP pool. The gateway is configured as the address pool server by default to assign IP addresses to clients. If an access switch exists in the network, you can select the access switch as the address pool server. Click **Next** after VLAN parameters are configured.

Configuration Guide

Configure Network Planning/Add Wired VLAN		×
1 Configure VLAN Parameters	2 Configure Wired Access 3 Confirm Config Delivery	
Des	cription:	
* VL	AN ID: 33	
Addr	ess Pool 🧿 Gateway Server	
Gatewa	ay/Mask: 192.168.33.1 / 255.255.255.0	
DH	CP Pool:	
16	P Range: 192.168.33.1 - 192.168.33.254	
		e
	Next	

(2) Select the target switch in the topology and all member ports in the VLAN, and click Next.

Configure Network Planning/Add Wired VLAN		\times
1 Configure VLAN Parameters	2 Configure Wired Access 3 Confirm Config Delivery	
() () () () () () () () () () () () () (VLAN20 (1) 192.168.20.1–192.168.20.254 You have selected 0 device(s) with 0 port(s). (2) Panel View No Device and Port Selected Step 1: Click to select the device in the topology. Step 2: Click or drag to select the port.	(La la

(3) Please confirm the delivered configurations and click **Save**. The configurations will take effect after a few minutes.

Configuration Guide

Configure Netwo	rk Planning/Add Wired VLAN		×
	1 Configure VLAN Parameters	2 Configure Wired Access	elivery
		To configure (test VLAN10 192.168.10.1-192.168.10.254) , configuration will be delivered following configuration will be delivered: Image: Configure (test VLAN10 192.168.10.1 Subnet Mask: 255.255.05) Model (Configure 1) Model (Configure	to 1 device(s).The ;4
		Previous Save	

3.4.2 Configuring Wi-Fi VLAN

Choose Network-Wide > Workspace > Network Planning.

On the Network Planning page, click Add Wi-Fi LAN.



Alternatively, you can select an existing wireless VLAN and click **Setup** to edit the VLAN.

(1) Configure the SSID, Wi-Fi password and band. Click **Expand** to expand the advanced settings and set the parameters. Then, click **Next**.

Configure Network Planning/Add Wi-Fi VLAN		×
1 Configure Wireless Access	2 Configure VLAN Parameters	3 Confirm Config Delivery
* SSID ⑦		
Purpose 🤅	General IoT Guest	
Band 🤅	2.46 Z 5G	
	No available frequency band? Log in to Ru target frequency band. <u>Re-identify</u> . <u>View C</u>	ijie Cloud to add or re-identify the auses
Encryption	Open Oceanity 802.1x (E	nterprise) 🕐
* Security (?	WPA2-PSK ~	
* Wi-Fi Password	9 ₇₇ 4	1
	Advanced Settings	
SSID Encoding	UTF-8 🗸	
Wi-Fi Standard 🤅	Auto 🗸	
Schedule 🤅	All Time ~	
Hide SSIC	(The SSID is hidden and must be r	nanually entered.)
	Next	

(2) Configure the VLAN ID, address pool server and DHCP pool. The gateway is configured as the address pool server by default to assign IP addresses to clients. If an access switch exists in the network, you can select the access switch as the address pool server. Click **Next** after VLAN parameters are configured.

Configure Network Planning/Add Wi-Fi VLAN		\times
1 Configure Wireless Access	2 Configure VLAN Parameters 3 Confirm Config Delivery	
* Descriptio	n	
VLAN	Add VLAN \vee	
* VLAN ID		
Address Poo Server (D Gateway	
Gateway/Mas	k: 192.168.110.1 / 255.255.255.0	
DHCP Poo	ok 💽	
IP Rang	e: 192.168.110.1 - 192.168.110.254	
	Previous Next	(? Ai

(3) Please confirm the delivered configurations and click **Save**. The configurations will take effect after a few minutes.

Configuration Guide

Configure Network Planning/Add Wi-Fi VLAN		×
1 Configure Wireless Access	2 Configure VLAN Parameters 3 Confirm Config Delivery	
()	To configure (test1 VLAN30 192.168.30.1-192.168.30.254) , configuration will be delivered to 2 device(s).The following configuration will be delivered: SSID: Password:Open	
	Add VLAN 30.IP Address: 192.168.30.1 Subnet Mask: 255.255.255.0 DHCP Pool. Start IP Address: 192.168.30.1 End IP Address: 192.168.30.254 DNS: 192.168.30.1 Lease Time (Min)480	
(Margani) (Margani)	Previous Save	(). Ai

4 Wi-Fi Network Settings

🚺 Note

Wi-Fi network settings covers the Wi-Fi settings of the currently logged in devices and the management of all wireless devices in the network. In **Network** mode, the Wi-Fi network settings are synchronized to all wireless devices in the network. You can configure device groups to limit the synchronization range. For details, see <u>4.1</u> <u>Configuring AP Groups</u>.

4.1 Configuring AP Groups

4.1.1 Overview

After the self-organizing network is enabled, the device can act as the primary AP/AC to perform batch configuration and management on the downlink APs in groups. Group the APs before the configurations are 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.

4.1.2 Configuration Steps

Choose Network-Wide > Devices > AP.

(1) The AP page displays all APs on the network. Click Manage to configure the selected device.

Rujje IRcycc					C	Q Search				🗘 Alert Center	⊘ English ~ Exit
One-Device		All (7) Gatewa	y (0) AP (6) S de your network hav Expand ⑦ Cha	witch (1) AC (0) e been discovered. ange Group ⑦	Router (0) Handle Basic Info	C RF	Select Reboo	bt Batch Upgrad	e 🕐	Delete Offline	IAC/hostname/SN/S- Q
Network-Wide			Username ⑦	Model 🗘	SN ‡		IP Address 🗘	MAC Address \doteqdot	Clients ‡	Device Group	Action
Devices		• 🔀	AP Z		G15 .	654	1925 L	48:8	0	Default	Manage Reboot
 Clients System 	4	•	AP Z		G1QF	0C	192. 90 &	C4: :DC	0	Default	Manage Reboot
		•)*(AP Z		MACC	:01	192.1 &	00:50	0	Default	Manage Reboot
		•	AP Z		G1QI	0238	192.1 2 Q	C4:7 :16	0	Default	Manage Reboot
		•)~(AP 2		G1SK:	233	192.1 45 🖉	10:^^^ ^^ := :E8	0	Default	Manage Reboot
		• 🔀	AP [Master] 신		G1Q	20	192.1 i4 &	C4:7 :E4	0	Default	Manage Reboot
										Total 6 🔹 🚺	> 10/page ~

(2) Click Expand to view all device groups on the left section of the Devices page.

All (7) Gateway (0) AP (6) Switch (1) AC	(0) Router (0) 🜔 Selec	t Reboot E	Batch Upgrade ⑦	Delete Off	line IP/MAC	/hostname/SN/Sr Q
Devices outside your networ	rk have been discovere	ed. Handle						
roup: All Group: Expand ③	Change Group ⑦	• Basic Info	RF Information	tion O Model				
Usernan ‡	ne ⑦ Model 章	SN \$	IP A	ddress 🗘 MAC	C Address 🖨	lients ≑ Devi	ce Group	Action
s ^{da} •)★ AP &		G1		48:81:	0	Defau	lt	Manage Reboot
) Click + to cre	ate a new gro	oup. Up to	o 8 groups	can be addeo	d. You can	click 🙎	to edit t	he group na
All (7) Gateway (0) AP (6	Switch (1)	group. The	e default gr	oup cannot b	e deleted	and its nar		t be edited
	rk have been discover	ed Handle			baten opginae i			
roup: All Groups Collapse ?	Change Group ?	Basic Inf	fo RE Inform	nation O Model				
Search by Group		Username ⑦	Model ≑	SN \$	IP Address	🗧 MAC Ad	Cli Idress ‡ ‡	e Action
Default 2 1	•	AP 🖉	F)	G1SI 654	192	5 🖉 48:81:	iC:E3 0	Manage Rebo
	•	AP 🖉	E	G1C ;0C	192.) 🖉 C4:70	-C:DC 0	Manage Rebo
	•	AP 🖉		MA(2X01	192 <mark>.</mark> 1	3 🖉 00:D0:	38:91 0	Manage Rebo
	•	AP 🖉		G1QI 3	192.	2 🖉 C4:7(0A:16 0	Manage Rebo
		AP Ø		C16 222	192.	j 🖉 10:82	1.69 0	
				015 255			1.20 0	Manage Reb
	•	AP [Master] 🖉	E	G1Q 520	19;	4 🖉 C4:70:,	4C:E4 0	Manage Rebo

(4) Click the group name on the left part to view all devices in this group. A device can only belong to a group. By default, all devices belong to the default group. Select an entry in the list and click **Change Group** to move the target device to a specified group, and then the device will apply the configurations of this group. Click **Delete Offline Devices** to remove the offline device from the list.

All (7)	Gateway (0)	AP (6)	Switch (1)	AC (0)	Router (0)	Θ				
						Deselect	Reboot	Batch Upgrade 🕐	Delete Offline	IP/MAC/hostname/SN/Sr Q
🕛 Devi	ices outside yo	our network	have been disc	overed. Ha	ndle					
Group: All	Groups Col	lapse 🕐	Change Grou	ıp 🕐 💿	Basic Info	O RF Information	 Model 			
Search by	y Group	-	•		Username (?) Model 🗘	SN ≑	IP Addres	s 🗘 MAC Add	dress 🗢 Action
Default 2	l L		, 		AP 🖉		G1S	654 192. 0	0.65 ℓ 48:81:	C:E3 Manage Reboot

Change Group)	×	
Select Group	Select	^	
	Default		
	2	el	

4.2 Adding a Wi-Fi Network

- (1) Go to the page for configuration.
- Method 1: Choose Network-Wide > Workspace > Wireless > Wi-Fi > Wi-Fi List.
- Method 2: Choose One-Device > Config > WLAN > Wi-Fi > Wi-Fi List.
- (2) Click Add Wi-Fi.

Wi-Fi List	Healthy Mode					
Wi-Fi List	Device Group:	Default \lor			manag	ge + Add Wi-Fi
	SSID ?	Band ⑦	Security ?	Hidden	VLAN ID	Action
((r;	LJW_55	2.4G	WPA2-PSK	No	The same VLAN as AP	Edit Delete
(r	1	2.4G 5G	OPEN(Open)	No	The same VLAN as AP	Edit Delete
(ír.	TEST	2.4G 5G	OPEN(Open)	No	The same VLAN as AP	Edit Delete

Up to 8 SSIDs can be added.

(3) Configure the SSID, password, and other information.

Add	×
* SSID ⑦	
Purpose ③	General IoT Guest
Band 🕐	2.4G SG
	No available frequency band? Log in to Ruijie Cloud to add or re-identify
	the target frequency band. <u>Re-identify</u> <u>View Causes</u>
Encryption	 Open Oscurity 802.1x (Enterprise)
* Security ⑦	OPEN(Open)
	advanced Setting
	Cancel OK

(4) Click **advanced Settings** to configure more Wi-Fi parameters. After configuration, click **OK**. After the Wi-Fi is added, a client can detect the SSID, and the Wi-Fi information is displayed in the Wi-Fi list.

	Advanced Settings
SSID Encoding	UTF-8 \lor
Wi-Fi Standard ၇	Auto
Schedule 🕐	All Time \checkmark
VLAN	The same VLAN as AP \sim
Hide SSID	(The SSID is hidden and must be manually entered.)
Client Isolation (?)	(Prevent wireless clients of this Wi-Fi from communicating with one another.)
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 the IP address unchanged on the Wi-Fi network.)
802.11r 🕐	(After this feature is enabled, roaming time is reduced to achieve fast transition.)
LimitSpeed	
	Do you want to edit RF parameters? Navigate to Radio Frequency for configuration.

Table 4-1 V	Vi-Fi Configuration	Parameters
-------------	---------------------	------------

Parameter	Description
SSID	Enter the name displayed when a wireless client searches for a wireless network.
Purpose	Set the Wi-Fi usage scenario. The options include General , IoT , and Guest . The system will recommend different Wi-Fi parameter combinations based on the selected purpose.

Cancel

Parameter	Description
Band	Set the band used by the Wi-Fi signal. The options are 2.4 GHz and 5 GHz. The 5 GHz band provides faster network transmission rate and less interference than the 2.4 GHz band, but is inferior to the 2.4 GHz band in terms of signal coverage range and wall penetration performance. Select a proper band based on actual needs. The default value is 2.4G + 5G , indicating that the device provides signals at both 2.4 GHz and 5 GHz bands.
	Note In networks with APs supporting the 6 GHz frequency band, you'll see an additional '6G' option in the frequency settings. The 6 GHz-band provides faster data transmission rates, but it's worth noting that-not all access devices may fully support this band.
Encryption	The encryption options for a Wi-Fi network include Open , Security , and 802.1x (Enterprise).
Security	Indicates encryption technologies used to ensure the security of data transmission.
Wi-Fi Password	When the Security is set to WEP, you need to set the password for connecting to the wireless network. The password is a string of 8 to 63 characters.
Select server group	When the Encryption is set to 802. 1x (Enterprise) , you need to configure a remote server set for authentication and authorization.
SSID Encoding	The SSID encoding standard is set to "UTF-8" by default when Chinese characters are included in the SSID. If the Chinese characters are garbled, you can choose "GB2312" as the SSID encoding standard.
Wi-Fi Standard	The Wi-Fi standards include 802.11ax (Wi-Fi 6) , Compatibility Mode , or Auto . The final effective Wi-Fi standard depends on the support of Wi-Fi standards on each device. The latest standard is recommended. If there is a compatibility issue, try use an older standard. However, an old standard setting will affect the bandwidth.
Schedule	Specify the time periods during which Wi-Fi is enabled. After you set this parameter, users cannot connect to Wi-Fi in other periods.
VLAN	Set the VLAN to which the Wi-Fi signal belongs. You can choose from the available VLANs or click Add New VLAN , and go to the LAN Settings page to add a VLAN.

Parameter	Description
Hide SSID	Enabling the hide SSID function can prevent unauthorized user access to Wi-Fi, improving security. However, mobile phones or computers cannot find the SSID after this function is enabled. You must manually enter the correct name and password to connect to Wi-Fi. Record the current SSID before you enable this function.
Client Isolation	After you enable this parameter, clients associated with the Wi-Fi are isolated from one other, and end users connected to the same AP (in the same network segment) cannot access each other. This improves security.
Band Steering	After this function is enabled, 5G-capable clients select 5G Wi-Fi preferentially. You can enable this function only when Band is set to 2.4G + 5G .
XPress	After this function is enabled, the device sends game packets preferentially, providing more stable wireless network for games.
Layer-3 Roaming	After this function is enabled, clients keep their IP addresses unchanged when associating with the same Wi-Fi. This function improves the roaming experience of users in the cross-VLAN scenario.
802.11r	Enabling the 802. 11r function can shorten the roaming handover time. The 802. 11r function is supported only when Encryption is set to Security or 802. 1x (Enterprise) . Once 802. 11r is enabled, the encryption type can only be WPA2-PSK or WPA2-802. 1X.
LimitSpeed	 After enabling Wi-Fi rate limiting, you can set the uplink and downlink rate limits for users. Rate Limit Per User: The rate limit applies to all clients connected to the SSID. Rate Limit All Users: All clients connected to the SSID share the configured rate limit equally. The rate limit of each client changes dynamically with the number of clients connected to the SSID.

4.3 Configuring SSID and Wi-Fi Password

(1) Go to the page for configuration.

- Method 1: Choose Network-Wide > Workspace > Wireless > Wi-Fi > Wi-Fi List. Select the Wi-Fi network, and click Edit.
- Method 2: Choose One-Device > Config > WLAN > Wi-Fi > Wi-Fi List. Select the Wi-Fi network, and click Edit.

Wi-Fi List	Healthy Mode						
Wi-Fi List	Device Group:	Default \lor				manag	ge + Add Wi-Fi
	SSID ⑦	Band ⑦		Security ?	Hidden	VLAN ID	Action
(ír.	LJW_55	2.4G		WPA2-PSK	No	The same VLAN as AP	Edit Delete
(ſŗ	1	2.4G	5G	OPEN(Open)	No	The same VLAN as AP	Edit Delete
(r	TEST	2.4G	5G	OPEN(Open)	No	The same VLAN as AP	Edit Delete

Up to 8 SSIDs can be added.

(2) Click the target Wi-Fi network, change the SSID and Wi-Fi password of the Wi-Fi network, and click OK.

🛕 Caution

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.

Edit	×
* SSID ⑦	@@@123123
Purpose ⑦	General IoT Guest
Band ③	2.4G SG
	No available frequency band? Log in to Ruijie Cloud to add or re-identify the target frequency band. <u>Re-identify</u> <u>View Causes</u>
Encryption	Open Security 802.1x (Enterprise)
* Security	WPA/WPA2-PSK V
* Wi-Fi Password	<u>بر ج</u> ر
	advanced Setting
	Cancel

4.4 Managing Wi-Fi Networks

- (1) Go to the configuration page.
- Method 1: Choose Network-Wide > Workspace > Wireless > Wi-Fi > Wi-Fi List.
- Method 2: Choose One-Device > Config > WLAN > Wi-Fi > Wi-Fi List.
- (2) Click manage to batch manage Wi-Fi networks.

Wi-Fi List	Healthy Mode					
Wi-Fi List	Device Group:	Default \lor			manag	e + Add Wi-Fi
	SSID ?	Band ?	Security ?	Hidden	VLAN ID	Action
(ſŗ	LJW_55	2.4G	WPA2-PSK	No	The same VLAN as AP	Edit Delete
((r	1	2.4G 5G	OPEN(Open)	No	The same VLAN as AP	Edit Delete
(ir.	TEST	2.4G 5G	OPEN(Open)	No	The same VLAN as AP	Edit Delete

Up to 8 SSIDs can be added.

(3) Batch manage Wi-Fi networks.

o Batch enable Wi-Fi networks: Select the desired Wi-Fi networks, and click **Enable**.

Wi-Fi Lis	t Healt	thy Mode				
Wi-Fi L	ist Devic	e Group: Default	\sim	Enable	Disable Delete	Exit + Add Wi-Fi
		SSID ?	Band 🕐	Security ?	Hidden	VLAN ID
	(ķ.	LJW_55	2.4G	WPA2-PSK	No	The same VLAN as AP
	\$? }	1	2.4G 5G	OPEN(Open)	No	The same VLAN as AP
	*	TEST	2.4G 5G	OPEN(Open)	No	The same VLAN as AP

Up to 8 SSIDs can be added.

o Batch disable Wi-Fi networks: Select the desired Wi-Fi networks, and click Disable.

Wi-Fi List	Health	iy Mode				
Wi-Fi List	Device	Group: Default V		Enable	Disable	Exit + Add Wi-Fi
•		SSID ⑦	Band 🕐	Security 🕐	Hidden	VLAN ID
	1	LJW_55	2.4G	WPA2-PSK	No	The same VLAN as AP
•	1	1	2.4G 5G	OPEN(Open)	No	The same VLAN as AP
	3	TEST	2.4G 5G	OPEN(Open)	No	The same VLAN as AP

Up to 8 SSIDs can be added.

o Batch delete Wi-Fi networks: Select the desired Wi-Fi networks, and click Delete.

Wi-Fi Lis	t Healt	thy Mode				
Wi-Fi l	List Devic	e Group: Default	~	Enable	e Disable Dele	Exit + Add Wi-Fi
		SSID (?)	Band ⑦	Security ⑦	Hidden	VLAN ID
	((î;	LJW_55	2.4G	WPA2-PSK	No	The same VLAN as AP
	(<u>(</u>	1	2.4G 5G	OPEN(Open)	No	The same VLAN as AP
	((r.	TEST	2.4G 5G	OPEN(Open)	No	The same VLAN as AP

Up to 8 SSIDs can be added.

(4) Click Exit to exit Wi-Fi network batch management.

Wi-Fi List	Healt	hy Mode				
Wi-Fi Li	st Device	e Group: Default V		Enable	Disable	Exit + Add Wi-Fi
		SSID ⑦	Band ⑦	Security 🕐	Hidden	VLAN ID
	((iç.	LJW_55	2.4G	WPA2-PSK	No	The same VLAN as AP
	((iç.	1	2.4G 5G	OPEN(Open)	No	The same VLAN as AP
	((î;	TEST	2.4G 5G	OPEN(Open)	No	The same VLAN as AP

Up to 8 SSIDs can be added.

4.5 Hiding the SSID

4.5.1 Overview

Hiding the SSID can prevent unauthorized clients from accessing the Wi-Fi network and enhance network security. After this function is enabled, the mobile phone or PC cannot search out the SSID. Instead, you have to manually enter the correct SSID and Wi-Fi password. Remember the SSID so that you can enter the correct SSID after the function is enabled.

4.5.2 Configuration Steps

- (1) Go to the page for configuration.
- Method 1: Choose Network-Wide > Workspace > Wireless > Wi-Fi > Wi-Fi List. Select the Wi-Fi network, and click Edit.
- Method 2: Choose One-Device > Config > WLAN > Wi-Fi > Wi-Fi List. Select the Wi-Fi network, and click Edit.

Wi-Fi List Device Group: Default VLAN ID SSID ⑦ Band ⑦ Security ⑦ Hidden VLAN ID	manage + Add Wi-Fi
SSID ⑦ Band ⑦ Security ⑦ Hidden VLAN ID	
	Action
LJW_55 2.4G WPA2-PSK No The same VLAN	as AP Edit Delete
Image: 1 2.4G 5G OPEN(Open) No The same VLAN	as AP Edit Delete
TEST 2.4G 5G OPEN(Open) No The same VLAN	as AP Edit Delete

Up to 8 SSIDs can be added.

(2) Click to expand advanced settings, turn on Hide SSID in the expanded settings and click OK.

🛕 Caution

After the configuration is saved, you have to manually enter the SSID and Wi-Fi password before connecting any device to the Wi-Fi network. Therefore, exercise caution when performing this operation.

Edit

Wi-Fi Standard ၇	Auto	~	
Schedule 🕐	All Time	~	
VLAN	The same VLAN as AP	~	
Hide SSID	(The SSID is hidden and	d must be i	manually entered.

4.6 Configuring Wi-Fi Band

- (1) Go to the page for configuration.
- Method 1: Choose Network-Wide > Workspace > Wireless > Wi-Fi > Wi-Fi List. Select the Wi-Fi network, and click Edit.
- Method 2: Choose One-Device > Config > WLAN > Wi-Fi > Wi-Fi List. Select the Wi-Fi network, and click Edit.
- (2) Set the band of Wi-Fi signals. The device supports the 2.4 GHz and 5 GHz bands. Compared with the 2.4 GHz band, the 5 GHz band supports a higher network transmission rate and is less susceptible to interference, but is inferior in signal coverage and through-wall penetration. You can select an appropriate signal band based on actual requirements. The default Wi-Fi band is **2.4G+5G**, indicating that Wi-Fi signals are emitted in both 2.4 GHz and 5 GHz bands.

 \times

* SSID 🕐	@@@###111
Purpose 🕐	General IoT Guest
Band 🕐	✓ 2.4G ✓ 5G
	No available frequency band? Log in to Ruijie Cloud to add or re-identify
	the target frequency band. <u>Re-identify</u> <u>View Causes</u>
Encryption	Open Osecurity 802.1x (Enterprise)
* Security 🕐	OPEN(Open) V
	advanced Setting
	Cancel

4.7 Configuring Band Steering

A Caution

This function can be enabled only after the dual-band integration (**Band** is set to **2.4G+5G**) is enabled on the Wi-Fi network. A client automatically selects a band only when the SSIDs of the 2.4 GHz and 5 GHz bands are the same.

- (1) Go to the page for configuration.
- Method 1: Choose Network-Wide > Workspace > Wireless > Wi-Fi > Wi-Fi List. Select the Wi-Fi network, and click Edit.
- Method 2: Choose One-Device > Config > WLAN > Wi-Fi > Wi-Fi List. Select the Wi-Fi network, and click Edit.
- (2) Click to expand advanced settings, turn on **Band Steering** in the expanded settings, and click **OK**. After the function is enabled, the client supporting 5 GHz selects the 5G Wi-Fi network preferentially.

Band 📀	✓ 2.4G ✓ 5G
	No available frequency band? Log in to Ruijie Cloud to add or re-identify
	the target frequency band. Re-identify View Causes
Encryption	• Open Security 802.1x (Enterprise) ()
* Security (?)	OPEN(Open)
	Advanced Settings
SSID Encoding	UTF-8 \lor
Wi-Fi Standard (?)	Auto 🗸
Schedule (?)	All Time
VLAN	The same VLAN as AP \sim
Hide SSID	(The SSID is hidden and must be manually entered.)
Client Isolation (?)	(Prevent wireless clients of this Wi-Fi from communicating with
	one another.)
Band Steering	(The 5G-supported client will access 5G radio preferentially.)

4.8 Configuring Wi-Fi 6

A Caution

The function takes effect only on APs supporting the IEEE 802.11ax protocol. In addition, access clients must support IEEE 802.11ax so that clients can enjoy high-speed Internet access experience brought by Wi-Fi 6. If clients do not support Wi-Fi 6, you can disable this function.

- (1) Go to the page for configuration.
- Method 1: Choose Network-Wide > Workspace > Wireless > Wi-Fi > Wi-Fi List. Select the Wi-Fi network, and click Edit.
- Method 2: Choose One-Device > Config > WLAN > Wi-Fi > Wi-Fi List. Select the Wi-Fi network, and click Edit.
- (2) Click advanced Settings to set the Wi-Fi Standard to 802.11ax(Wi-Fi6). Click OK. After this function is enabled, wireless clients can have faster network speed and optimized network experience.

	Advanced Settings	
SSID Encoding	UTF-8 ~	·]
Wi-Fi Standard (?)	Auto	
Schedule 🕐	Auto	
VLAN	Compatibility Mode 802.11ax(Wi-Fi6)	

4.9 Configuring Layer-3 Roaming

- (1) Go to the page for configuration.
- Method 1: Choose Network-Wide > Workspace > Wireless > Wi-Fi > Wi-Fi List. Select the Wi-Fi network, and click Edit.
- Method 2: Choose One-Device > Config > WLAN > Wi-Fi > Wi-Fi List. Select the Wi-Fi network, and click Edit.
- (2) Click to expand advanced settings, turn on Layer 3 Roaming in the expanded settings and click OK. The client will keep the IP address unchanged in this Wi-Fi network, improving roaming experience across VLANs.

XPress		(The client will experience faster speed.)
Layer 3 Roaming 🕐		(The client will keep the IP address unchanged on the Wi-Fi
	networ	k.)

4.10 Configuring Client Isolation

- (1) Go to the page for configuration.
- Method 1: Choose Network-Wide > Workspace > Wireless > Wi-Fi > Wi-Fi List. Select the Wi-Fi network,

and click Edit.

- Method 2: Choose One-Device > Config > WLAN > Wi-Fi > Wi-Fi List. Select the Wi-Fi network, and click Edit.
- (2) Click to expand advanced settings, turn on AP Isolation in the expanded settings and click Save. The clients joining in this Wi-Fi network will be isolated. The clients associated with the same access point cannot access each other.

VLAN	The same VLAN as AP $$
Hide SSID	(The SSID is hidden and must be manually entered.)
Client Isolation ⑦	(Prevent wireless clients of this Wi-Fi from communicating with
	one another.)

4.11 Configuring 802.11r

The **802.11r** function is available only when the Encryption is set to **Security** or **802.1x(Enterprise)**. Once **802.11r** is enabled, **Security** can only be set to WPA2-PSK or WPA2-802.1X.

- (1) Go to the page for configuration.
- Method 1: Choose Network-Wide > Workspace > Wireless > Wi-Fi > Wi-Fi List. Select the Wi-Fi network, and click Edit.
- Method 2: Choose One-Device > Config > WLAN > Wi-Fi > Wi-Fi List. Select the Wi-Fi network, and click Edit.
- (2) Click advanced Settings. Enable 802.11r, and click OK.

	XPress	(The client will experience faster speed.)
Layer 3 Roaming 🕥		(The client will keep the IP address unchanged on the Wi-Fi network.)
	802.11r ን	(After this feature is enabled, roaming time is reduced to achieve
		tast transition.)
LimitSpeed		
		Do you want to edit RF parameters? Navigate to Radio Frequency for configuration.
		Cancel OK

4.12 Configuring a Guest Wi-Fi

4.12.1 Overview

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

4.12.2 Configuration Steps

- Method 1: Choose Network-Wide > Workspace > Wireless > Wi-Fi > Wi-Fi List.
- Method 2: Choose One-Device > Config > WLAN > Wi-Fi > Wi-Fi List.

Click **Add Wi-Fi**. Set the purpose to **Guest** and configure the SSID and password. Click **advanced Settings** to configure the effective time of the guest Wi-Fi and other Wi-Fi parameters. After the settings are saved, guests can connect to the Internet through the set SSID and password.

Add	×
* SSID ③	@Ruijie-guest-60A9
Purpose ?	General IoT Guest
Band ⑦	✓ 2.4G ✓ 5G
	No available frequency band? Log in to Ruijie Cloud to add or re-identify
	the target frequency band. Re-identify View Causes
Encryption	Open Security 802.1x (Enterprise)
* Security ⑦	WPA/WPA2-PSK V
* Wi-Fi Password	2md
	advanced Setting
	Cancel OK

4.13 Configuring Wireless Rate Limiting

4.13.1 Overview

The device supports four rate limiting modes: client-based rate limiting, SSID-based rate limiting, AP-based rate limiting, and packet-based rate limiting. For the same client, if multiple rate limiting modes are configured, the priority order is as follows: client-based rate limiting > SSID-based rate limiting > AP-based rate limiting > packet-based rate limiting.

- Client-based rate limiting: This function allows you to limit the rate based on the MAC address of the client, so as to limit or guarantee the bandwidth required by specific clients.
- SSID-based rate limiting: This function provides two rate limiting modes for a specified SSID: Rate Limit Per

User and Rate Limit All Users. Rate Limit Per User means that all clients connected to the SSID use the same rate limit. Rate Limit All Users means that the configured rate limit value is evenly allocated to all clients connected to the SSID. The rate limit value of each client dynamically changes with the number of clients connected to the SSID.

- AP-based rate limiting: This function limits the client rates based on the whole network. All clients connected to the network will work according to the configured rate limit value.
- Packet-based rate limiting: This function limits the client rates based on the downlink broadcast and multicast packets. The device supports rate limiting for specific broadcast packets (such as ARP and DHCP), multicast packets (such as MDNS and SSDP), or all types of broadcast and multicast packets. If network stalling remains during network access and there is no client with large traffic, you are advised to adjust the rate between 1 kbps and 512 kbps.

4.13.2 Configuration Steps

1. Configuring Client-based Rate Limiting

Choose Network-Wide > Workspace > Wireless > Rate Limiting > Client-based Rate Limiting.

(1) Enable Wireless Rate Limiting.

Wireless Rate Limiting				
Client-based Rate Limiting	SSID-based Rate Limiting	AP-based Rate Limiting	Packet-based Rate Limiting	
i The rate limiting m	ode based on wireless clients can li	mit or provide the bandwidth f	or specific clients.	
Client-based Rate Li	miting		+ Ad	d 🗇 Delete Selected
Client MAC	Uplink Rate Limit	Downlink Rate Limit	Remarks	Action
		No Data		
Up to 512 entries can be	added.		Total 0 <	1 > 10/page >

(2) Click Add. In the dialog box that appears, set the MAC address and uplink and downlink rate limit values of the client, and click OK.

Wireless Rate Limiting								
Client-b	based Rate Limiting	SSID-based Rate Limiting	AP-based Rate Limiting	Packet-based Rate Limiting				
1	he rate limiting mode	based on wireless clients can lin	nit or provide the bandwidth 1	or specific clients.				
Client	-based Rate Limiti	ng		+ Add	Delete Selected			
	Client MAC	Uplink Rate Limit	Downlink Rate Limit	Remarks	Action			
			No Data					
Up to	512 entries can be adde	ed.		Total 0 < 1	> 10/page >			

Add

* Client MAC	Exampl	le: 00:11:22:33:44	:55	
Uplink Rate	No Lim	it by Default. R	Kbps	~
Limit	Current:	Kbps. Range: 1	-170000	0 Kbp
Downlink Rate	No Lim	it by Default. R	Kbps	~
Limit	Current:	Kbps. Range: 1	-170000	0 Kbp
Remarks				
			Ca	ancel

2. Configuring SSID-based Rate Limiting

Method 1: Choose Network-Wide > Workspace > Wireless > Rate Limiting > SSID-based Rate Limiting.

 \times

- (1) Enable Wireless Rate Limiting.
- (2) Click **Edit** in the **Action** column of the target SSID. In the dialog box that appears, set the uplink and downlink rate limit modes and values, and click **OK**.

Wireless Rate Limiting						
Clien	t-based Rate Limiting	SSID-based Rate Limiting	AP-based Rate Limiting	Packet-based	Rate Limiting	
This function provides rate limit per ufser and dynamic rate limiting for a specified SSID. Rate Limit per User indicates that all clients connected to the SSID use the same rate limit. Rate Limit All Users indicates that all clients connected to the SSID share the rate limit in average. The priority of this function is lower than that of client-based rate limiting.						
SSI	D-based Rate Limiting	J Device Group: Default	\sim	Are you	sure you want to add a Wi-Fi? Click to go.	
	SSID	Uplink Rate L	imit Dow	nlink Rate Limit	Action	
	0000	No Limit		No Limit	Edit Disable	

 \times

Edit		
Uplink Rate Limit 🕐	• Rate Limit Per User	O Rate Limit All Users
Rate Limit	No Limit by Default. R	Kbps 🗸
	Current: Kbps. Range: 1-	-1700000 Kbps
Downlink Rate Limit ⑦	• Rate Limit Per User	Rate Limit All Users
Rate Limit	No Limit by Default. R	Kbps 🗸
	Current: Kbps. Range: 1-	-1700000 Kbps

Method 2:

- (1) Go to the configuration page:
- Method 1: Choose Network-Wide > Workspace > Wireless > Wi-Fi > Wi-Fi List. Select the Wi-Fi network, and click Edit.

Cancel

- Method 2: Choose One-Device > Config > WLAN > Wi-Fi > Wi-Fi List. Select the Wi-Fi network, and click Edit.
- (2) Click to expand advanced settings. Enable LimitSpeed, set the uplink and downlink rate limit modes and rate limits, and click OK.

	LimitSpeed							
Uplink	Rate Limit 🕐	O Rate	Limit Per User	Rate Li	mit A	II Users		
	Rate Limit	No Lim	it by Default. R	Kbps 🗸				
		Current:	Kbps. Range: 1	-1700000 Kb	ps			
Downlink	Rate Limit ⑦	O Rate I	Limit Per User	Rate Li	mit A	II Users		
	Rate Limit	No Lim	it by Default. R	Kbps 🗸 🗸				
		Current:	Kbps. Range: 1	-1700000 Kb	ps			
		Do you w configura	vant to edit RF p ation.	arameters? N	Vavig	ate to Ra	adio Frequen	cy for
							Cancel	ОК

3. Configuring AP-based Rate Limiting

Choose Network-Wide > Workspace > Wireless > Rate Limiting > AP-based Rate Limiting.

(1) Enable Wireless Rate Limiting.

(2) Set the uplink and downlink rate limit modes to **Rate Limit Per User**, configure the rate limit values, and click **OK**.

Wireless Rate Limiting			
Client-based Rate Limiting	SSID-based Rate Limiting	AP-based Rate Limiting	Packet-based Rate Limiting
This function provid value. The priority of this	les client rate limiting based on the v iunction is lower than that of client-b	whole network. All devices co pased rate limiting and SSID-t	nnected to the network use the preset rate limiting pased rate limit per user.
AP-based Rate Limit	ing		
Uplink Rate Limit ⑦	No Limit Rate Limit Per U	Jser	
	Kbps V	//	
Downlink Rate Limit	No Limit Rbps. Range: 1-1700000 No Limit Rbps. V	Jser	
	Current: Kbps. Range: 1-1700000	Kbps	

4. Configuring Packet-based Rate Limiting

Choose Network-Wide > Workspace > Wireless > Rate Limiting > Packet-based Rate Limiting.

- (1) Enable Wireless Rate Limiting.
- (2) Select the specific type of packets for rate limiting, configure the rate limit value, and click **Save**.

Wireless Rate Limiting	\bigcirc		
Client-based Rate Limiting	SSID-based Rate Limitin	AP-based Rate Limiting	Packet-based Rate Limiting
This function allows when no client need better network imp Tip: A lower rate lin improvement.	s users to limit the downlink ra ds large amounts of traffic, you rovement. hit brings better network impro	ate for broadcast and multicast pack u are advised to set the rate rangin ovement but may affect client servi	kets. If the internet access is still slow and unstable g from 1 Kbps to 512 Kbps. Smaller rate brings ices.A higher rate limit indicates poorer network
Packet-based Rate L	imiting		
Broadcast Rate Limiting	O Disable O Limit All	• Limit Part	
	ARP Packet DHCP	Packet	
Multicast Rate Limiting	O Disable O Limit All	• Limit Part	
	MDNS Packet SSD	PP Packet	
* Rate Limit		Kbps \vee	
	Current: 0 Kbps. Range: 1-1	700000 Kbps	
	Save		

4.14 Configuring Wi-Fi Blocklist or Allowlist

4.14.1 Overview

You can configure the global or SSID-based blocklist and allowlist. The MAC address supports full match and OUI match.

Wi-Fi blocklist: Clients in the Wi-Fi blocklist are prevented from accessing the Internet. Clients that are not added to the Wi-Fi blocklist are free to access the Internet.

Wi-Fi allowlist: Only clients in the Wi-Fi allowlist can access the Internet. Clients that are not added to the Wi-Fi allowlist are prevented from accessing the Internet.

A Caution

If the allowlist is empty, the allowlist does not take effect. In this case, all clients are allowed to access the Internet.

4.14.2 Configuration Steps

1. Configuring a Global Blocklist/Allowlist

Choose Network-Wide > Workspace > Wireless > Blocklist and Allowlist > Global Blocklist/Allowlist.

Select the blocklist or allowlist mode and click **Add** to configure a blocklist or allowlist client. Enter the device name, match type, and MAC address of the client to be added to the blacklist or whitelist in the displayed dialog box, and click **OK**. If a client is already associated with the access point, its MAC address will pop up automatically. Click the MAC address directly for automatic input. All clients in the blocklist will be forced offline and not allowed to access the Wi-Fi network. The global blocklist and allowlist settings take effect on all Wi-Fi networks of the access point.

Global Blocklist/Allowlist	SSID-Based Blocklist/Allowlist		
• All STAs except blocklisted	STAs are allowed to access Wi-Fi.	Only the allowlisted STAs are allow	ed to access Wi-Fi.
Blocked WLAN Client	s		+ Add Delete Selected
De	vice Name	MAC Address	Action
		No Data	
Up to 512 members can be	added.		Total 0 < 1 > 10/page >

Add			×
Device Name ⑦ Op	tional		
Match Type 💿 Fu	III O Prefix (OUI)		
* MAC Address Exa	mple: 00:11:22:33:44:55		
		Cance	el OK

2. Configuring an SSID-based Blocklist/Allowlist

Choose Network-Wide > Workspace > Wireless > Blocklist and Allowlist > SSID-Based Blocklist/Allowlist.

Select a target Wi-Fi network from the left column, select the blocklist or allowlist mode and click **Add** to configure a blocklist or allowlist client. The SSID-based blocklist and allowlist will restrict the client access to the specified Wi-Fi.

Global Blocklist/Allowlist SSID-Ba	sed Blocklist/Allowlist		
Blocklist/Allowlist is used to allo Note: OUI matching rule and SS Rule: 1. In the Blocklist mode, 2. In the Allowlist mode,	w or reject a client's request to connect iD-based blocklist/allowlist are supported the clients in the blocklist are not allowed only the clients in the allowlist are allowe	to the Wi-Fi network. J by only RAP Net and P32 (and later to connect to the Wi-Fi network. d to connect to the Wi-Fi network.	versions).
Device Group: Default ✓ ➡ SSID-Based Blocklist/Allowlist @@@@	All STAs except blocklisted STAs are all Only the allowlisted STAs are allowed a Blocked WLAN Clients	lowed to access Wi-Fi. to access Wi-Fi.	d 🗇 Delete Selected
	Device Name	MAC Address	Action
		No Data	
	Up to 512 members can be added.	Total 0 <	1 > 10/page >

4.15 Optimizing Wi-Fi Network

4.15.1 Overview

The device detects the surrounding wireless environment and selects the appropriate configuration upon poweron. However, network stalling caused by wireless environment changes cannot be avoided. You can optimize the network with one single click, analyze the wireless environment around the access point and select appropriate parameters.

A Caution

After being optimized, the Wi-Fi network will restart, and clients need to reconnect to the W-Fi network. Therefore, exercise caution when performing this operation.

4.15.2 Getting Started

Install Wi-Fi Moho or other Wi-Fi scanning app on the mobile phone and check interference analysis results to find out the best channel.



4.15.3 Configuring Global Radio Settings

1. Optimizing the Channel Width

Choose Network-Wide > Workspace > Wireless > Radio Setting.

A network with a lower channel width is more stable, while a network with a higher channel width is susceptible to interference. If the interference is severe, choose a lower channel width to avoid network stalling to a certain extent. The access point supports the channel width of 20 MHz and 40 MHz in the 2.4 GHz channel, and the channel width of 20 MHz, 40 MHz and 80 MHz in the 5 GHz channel.

The default value is **Auto**, indicating that the channel width is automatically selected based on the environment. After changing the channel width, click **Save** to make the configuration take effect immediately.

A Caution

In the self-organizing network mode, the channel width settings will be synchronized to all devices in the network.

Radio Setting	Device Group: Default \checkmark Not solved yet? Click here to access the Network Optimization page for automatic optimization.
Common Paramete	r No available frequency band? Log in to Ruijie Cloud to add or re-identify the target frequency band. Re-identify View Causes
Country/Regi	China (CN) \lor
Radio Parameters	
2.4G	Global Radio Settings
	Channel Width ⑦ Auto \checkmark
5G	Multicast Rate (Mbps) ⑦ Auto ~
	Client Count Limit [®]
	Disconnection Threshold O ^{(Disable} -85dBm -65dBm
	Save

2. Configuring the Multicast Rate

Choose Network-Wide > Workspace > Wireless > Radio Setting.

If the multicast rate is too high, the packet loss rate of multicast packets may increase. If the multicast rate is too low, the radio interface may become busy. When network stalling is serious, you are advised to configure a high multicast rate. When network stalling is minor, configure a medium multicast rate. After adjusting the configuration, click **Save**.

Radio Setting	Device Group: Default V	Not solved yet? Click here to access the Network Optimization page for automatic optimization.
Common Paramete	er No available frequency band? Log in to Ruijie Cloud to add	or re-identify the target frequency band. <u>Re-identify</u> <u>View Causes</u>
Country/Regi	ion China (CN) \lor	
Radio Parameters		
3.46	Global Radio Settings	
2.40	Channel Width ⑦ Auto	~
5G	Multicast Rate (Mbps) ⑦ Auto	~]
5G	Client Count Limit ⑦	
	Disconnection Threshold O O ^{Disable} -85dBm	-65dBm
	Save	

3. Configuring the Client Limit

Choose Network-Wide > Workspace > Wireless > Radio Setting.

If the access point is associated with too many clients, it will have a lower performance, affecting user experience. After you configure the threshold, new clients over the threshold will not be allowed to access the Wi-Fi network. You can lower the threshold if there is requirement for bandwidth per client. The **Client Count Limit** toggle switch is disabled by default. If there is no need to set a client limit, please keep the default setting.

You can toggle on the Client Count Limit toggle switch to set a client limit, and then click Save.

Radio Setting	Device Group: Default	Not solved	ret? Click here to access the Network Optimization page for automatic optimization.
Common Parameter	r No available frequency	band? Log in to Ruijie Cloud to add or re-identi	iy the target frequency band. <u>Re-identify</u> <u>View Causes</u>
Country/Regio	China (CN)	~	
Radio Parameters			
2.46		Global Radio Settings	
2.46	Channel Width ⑦	Auto 🗸	
5G	Multicast Rate (Mbps) 🕐	Auto	
	Client Count Limit ⑦	64	
	Disconnection Threshold ⑦ ^{Di}	O sable -85dBm -65dBm	
	Save		

Note

The **Client Count Limit** refers to the maximum number of clients that can be connected to a single access point.

4. Configuring the Kick-off Threshold

Choose Network-Wide > Workspace > Wireless > Radio Setting.

In the case of multiple Wi-Fi signals, setting the kick-off threshold can improve the wireless signal quality to a certain extent. The farther the client is away from the access point, the lower the signal strength is. If the signal is lower than the kick-off threshold, the Wi-Fi will be disconnected, and the client will be forced offline and select a nearer Wi-Fi signal.

However, the higher the kick-off threshold is, the easier it is for the client to be kicked offline. To ensure normal Internet access, you are advised to disable the kick-off threshold or set the value to less than -75dBm. After adjusting the configuration, click **Save**.

Configurat	ion Guide					Wi-Fi Network Settings
R Co Rai	Radio Setting mmon Paramete Country/Regio dio Parameters	Device Group: Default r No available frequency on China (CN)	band? Log in to Ruijie Cloud to ad	Not solved yet? Id or re-identify t	Click here to access the Network Opt he target frequency band. <u>Re-identi</u>	imization page for automatic optimization. fy <u>View Causes</u>
	2.46		Global Radio Settings			
	2.40	Channel Width ⑦	Auto	~		
	5G	Multicast Rate (Mbps) 🕐	Auto	~		
		Client Count Limit ⑦	64			
		Disconnection Threshold ⑦ ^D	O sable -85dBm	-65dBm		
		Save				

🛕 Caution

In the self-organizing network mode, the kick-off threshold settings will be synchronized to all devices in the network.

4.15.4 Configuring Standalone Radio Settings

Go to the configuration page.

- Method 1: Choose One-Device > Config > WLAN > Radio Setting.
- Method 2: Choose Network-Wide > Devices> Manage > Config > WLAN > Radio Setting.

In high-density client environments, you can fine-tune radio settings to alleviate radio frequency interference resulting from too many access points in close proximity. This include disabling the radio of neighboring APs that are causing significant interference, aiming to minimize signal conflicts and enhance the overall quality and stability of wireless communication.

In environments like conference rooms, offices, and smart homes, disabling the 2.4GHz radio of specific APs can enhance the performance of wireless devices such as mice, keyboards, Bluetooth and Zigbee devices when they experience signal interference or operational lag.

The **Radio Switch** is enabled by default, and can be disabled as required.

Radio Setting				Not so	olved yet? C	lick here to acc	ess the Netwo	rk Optimizatio	n page for au	tomatic optin	ization.
Radio Parameters											
2.4G	Standalon Radio Switch 🔵	e Radio Settings									
5G	Channel Auto			~							
	Auto Roaming ③ O Low	Lower Low	Medium 80%	High High							
	Access Threshold ⑦ O Disable	-85dBm		-65dBm							
	Response Threshold ⑦ O Disable	-85dBm		-65dBm							
	Save										

1. Optimizing the Radio Channel

- Method 1: Choose One-Device > Config > WLAN > Radio Setting.
- Method 2: Choose Network-Wide > Devices > Manage > Config > WLAN > Radio Setting.

Choose the best channel identified by Wi-Fi Moho or other Wi-Fi scanning App. Click **Save** to make the configuration take effect immediately. The more devices in a channel, the greater the interference.

Note

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

2.4G	Standalo	one Radio Settings		
	Radio Switch			
5G	Channel Auto			~
56	Tx Power O Auto	Lower Low	Medium	High
	Roaming ⑦ O	40%	80%	High
	Access Threshold ⑦ O Disable	-85dBm		-65dBm
	Response Threshold ⑦ O Disable	-85dBm		-65dBm

2. Optimizing the Transmit Power

- Method 1: Choose One-Device > Config > WLAN > Radio Setting.
- Method 2: Choose Network-Wide > Devices > Manage > Config > WLAN > Radio Setting.

A greater transmit power indicates a larger coverage and brings stronger interference to surrounding wireless routers. In a high-density scenario, you are advised to set the transmit power to a small value. The **Auto** mode is recommended, indicating automatic adjustment of the transmit power. After adjusting the configuration, click **Save**.

Radio Setting		Not solved yet? Click here to access the Network Optimization page for automatic opt
Radio Parameters		
2.4G	Standalone Radio Settings	
	Radio Switch	
5G	Channel Auto ~	<u>]</u>
	Tx Power O Auto Lower Low Medium Hi	igh
	Roaming ⑦ O Low 40% 80% Hir	igh
	Access Threshold ⑦ O Disable -85dBm -65c	dBm
	Response Threshold ⑦ O Disable -85dBm -65c	dBm
	Save	

3. Configuring the Roaming Sensitivity

- Method 1: Choose One-Device > Config > WLAN > Radio Setting.
- Method 2: Choose Network-Wide > Devices > Manage > Config > WLAN > Radio Setting.

The roaming sensitivity enables the device to actively disconnect a client from the Wi-Fi network when the client is far away, forcing the client to re-select the nearest signal and thus improving the sensitivity of wireless roaming. Higher the roaming sensitivity level, smaller the wireless signal coverage. To improve the signal quality for a client moving within more than one Wi-Fi coverage, improve the roaming sensitivity level. You are advised to keep the default settings. After adjusting the configuration, click **Save**.

Radio Setting				Not s	solved	l yet? Click h	ere to access tl	he Network (ptimization	page for auto	matic optimi:	zatio
Radio Parameters												
2.4G	Standalon	e Radio Settings										
	Radio Switch 🔵											
5G	Channel Auto			~								
50	Tx Power O Auto	Lower Low	Medium	High								
	Roaming ⑦ O Low	40%	80%	High								
	Access Threshold ⑦ O Disable	-85dBm		-65dBm								
	Response Threshold ⑦ O Disable	-85dBm		-65dBm								
	Save											

- 4. Configuring Access Threshold
- Method 1: Choose One-Device > Config > WLAN > Radio Setting.

• Method 2: Choose Network-Wide > Devices > Manage > Config > WLAN > Radio Setting.

When the wireless signal of the end user is lower than the access threshold set on the device, the client cannot detect the wireless signal of the device. After adjusting the configuration, click **Save**.

Radio Setting		Not solved yet? Click here to access the Network Optimization page for automatic optimization.
Radio Parameters		
	Standalone Radio Settings	

240		-		
2.46	Radio Switch 🔵			
56	Channel Auto			~
30	Tx Power O Auto	Lower Low	Medium	High
	Roaming ⑦ O	40%	80%	High
	Access Threshold ⑦ O Disable	-85dBm		-65dBm
	Response Threshold ⑦ O Disable	-85dBm		-65dBm
	Save			

5. Configuring Response RSSI Threshold

- Method 1: Choose One-Device > Config > WLAN > Radio Setting.
- Method 2: Choose Network-Wide > Devices > Manage > Config > WLAN > Radio Setting.

When the wireless signal of the end user is lower than the response RSSI threshold configured on the device, the client cannot detect the wireless signal of the device. The smaller the response RSSI threshold is configured, the less the environmental factors interfere with the AP. However, the connection of the client may be affected. After adjusting the configuration, click **Save**.

Radio Setting					Not s	olved y	yet? Click her	re to access	the Netwo	rk Optimiz	ation pag	e for auto	matic opti	imization.
Radio Parameters														
2.4G	Standalone Radio Settings													
	Radio Switch													
5G	Channel	Auto			~									
	Tx Power	O Auto	Lower Low	Medium	High									
	Roaming ⑦	O Low	40%	80%	High									
	Access Threshold ③	O Disable	-85dBm		-65dBm									
	Response Threshold ⑦	O Disable	-85dBm		-65dBm									
	Save													

4.15.5 Configuring WIO

Choose Network-Wide > Workspace > WLAN Optimization.

Select the optimization mode. Then, click OK to optimize the wireless network.

A Caution

- WIO is supported only in the self-organizing network mode.
- The client may be offline during the optimization process. The configuration cannot be rolled back once optimization starts. Therefore, exercise caution when performing this operation.

Table 4-2	Tuning Mode	Configuration	Parameters
	ranning moao	ooningaration	i urumotoro

Parameter	Description				
Quick tuning	In this mode, external interference and bandwidth are not considered. A quick optimization is performed to optimize channel, power, and management frame power.				
Deep tuning	 In this mode, external interference and bandwidth are considered. A deep optimization is performed to optimize channel, power, and management frame power. Click to expand Advanced Settings to configure the scanning time, channel bandwidth and channels. Scanning time: Indicates the time for scanning channels during the optimization. Roaming Sensitivity: The roam sensitivity can be optimized based on the actual environment to ensure fast roaming of wireless devices. Transmit power: Increasing the transmit power enhances both the strength and coverage of the wireless signal, but it may also introduce interference to surrounding wireless networks. With this feature enabled, the AP will automatically adjust the transmit power based on the environment. 2.4G Channel bandwidth: Indicates the channel bandwidth. The channel bandwidth will be calculated by the system if Default is selected. Selected channels: Indicates the channel bandwidth. The channel bandwidth will be calculated by the system if Default is selected. Selected channels: Indicates the channel bandwidth. The channel bandwidth will be calculated by the system if Default is selected. Selected channels: Indicates the channel bandwidth. The channel bandwidth will be calculated by the system if Default is selected. 				

• Choose Quick optimization, and click OK.


• Choose **Deep optimization**. Click to expand **Advanced Settings** to set the scanning time, channel bandwidth and selected channels. Then, click **OK**.

Network Optimization	Scheduled Optimization	Optimization Record	802.11k/v Roaming Optimization	Advanced
		Wir	reless Intelligent Optimizatior	1
		In a i	networking environment, WIO can help	maximize wireless performance by optimizing your network.
		Opt	imization	
			Optimization 🔘 Quick optimization	• Deep optimization
			mode	
			Advanced Settings	
			Scan time 10s	~
			Roaming 🔵	
			Sensitivity	
		т	Fransmit Power 🗾	



After the optimization starts, please be patient and wait for the optimization to complete. After optimization is completed, you can click Cancel Optimization to restore the optimized RF parameters to their default values. Click Back to Home to perform wireless optimization again.

Network Optimization	Scheduled Optimization Optimization Record 802.11k/v Roaming Optimization Advanced		
\bigcirc	Finish Completion time: 2024-11-07 13:46:55 Optimization mode Deep optimization Time consumed: 3 minutes 39 seconds. Optimized 1 APs, resolved severe interference of 1 APs, reduced channel interference by 56:77%, and improved user experience by 35:78%.	Cancel Optimization	Back to Home
AP Interference Trer	d (In general, a lower interference value indicates a better network experience.)	Enter AP name/SN Q	2.4G 5G
Interfere	ne (%)		Top10 v
100			
80 -			
50			
60-			
40 -		62	
20 -		Before: 1 After: 1	
	1	View More	
0+	62		Hostname
Ontimization Dotail			
optimization Details	, Interformers Referen Interformers After Interformers		

Network Optimization	Scheduled Optimization	Optimization Record	802.11k/v Roaming Opti	mization A	dvanced			
 Last Optimized:202 Time consumed: 3 	24-11-07 13:46:55 minutes 39 seconds. Optimize	ed 1 APs, resolved severe inter	rference of 1 APs, reduced	d channel interf	erence by 56.77%, and in	nproved user experi	ience by 35.78%.	
AP Interference Trer	nd (In general, a lower inter	ference value indicates a be	tter network experience	a.)		Enter AP nar	me/SN Q	2.4G 5G
Interference	(%)		Before	After				Top10 \vee
100 -								
80 -								
60 -								
40								
20								
0		1			1			- Hostname
			62					
Optimization Detail	s							
Hostname 🚖	Band ≜ SN ∉	Interference	Interference	Interference	Channel Width	Channel	Transmit Power	Sensitivity

Click Optimization Record to view the details of the latest optimization.

You are advised to set a scheduled task to optimize the wireless network in the early hours of the morning or when the network is idle.

Network Optimization	on	Scheduled Optimization	Optimization Record	802.11k/v Roaming Optimization	Advanced
<i>i</i> Optimize the	networl	k performance at a scheduled	l time for a better user expe	erience.	
Enable					
Day	Wed				
Time	05	\[
Schedule	• We	eekly One time			
Optimization mode	O Qu	ick optimization O Deep	o optimization		
		Save			

4.15.6 Configuring Wi-Fi Roaming Optimization (802.11k/v)

Choose Network-Wide > Workspace > WLAN Optimization > 802.11k/v Roaming Optimization.

Choose the optimization mode. Click **Enable** and the Wi-Fi roaming is further optimized through the 802.11k/v protocol. Smart clients compliant with 802.11k/v can switch to the APs with better signal and faster speed during the roaming process, ensuring high-speed wireless connectivity. To ensure smart roaming effect, the WLAN environment will be auto scanned when Wi-Fi roaming optimization is first enabled.

A Caution

- WIO is supported only in the self-organizing network mode.
- During the WLAN environment scanning, the APs will switch channels, forcing the clients to go offline. The process will last for 2 minutes.

Network Optimization	Scheduled Optimization	Optimization Record	802.11k/v Roaming Optimization	Advanced		
⊘		_ ⊘			🛇	
Start		Scanning	Optin	nizing	Finish	
	Description: The Wi-Fi roaming is further optimized through the 802.11k/v protocol. Smart clients compliant with 802.11k/v can switch to the APs with better signal and faster speed during the roaming process, ensuring high-speed wireless connectivity. To ensure smart roaming effect, the WLAN environment will be auto scanned when Wi-Fi roaming optimization is first enabled.					
	During the WLAN environm	ent scanning, the APs will s	witch channels, forcing the clients to g	go offline. The process will last for 2	2 minutes.	
	Optimization Mode 🕐 💿	Performance-prior	Roaming-prior			
	Enable					

Table 4-3 Optimization Mode

Parameter	Description
Performance-prior	Maximum negotiation speed is preferentially guaranteed but connection stability may be affected.
Roaming-prior	Connection stability is preferentially guaranteed but maximum negotiation speed may be reduced.

Network Optimization	Scheduled Optimization	Optimization Record	802.11k/v Roaming Optimization Advanced	
⊘		- *	•	
Start		Scanning	Optimizing	Finish
\frown	802.11k/v Roam	ing Optimizatio	nScanning	
20%	Start: 2023-12-11 17:33:34 Expected Time: 2 minute			
Network Optimization	Scheduled Optimization	Optimization Record	802.11k/v Roaming Optimization Advanced	
\otimes ——		$- \odot$ —		$ \odot$
Start		Scanning	Ontimizing	
			Optimizing	Finish
	Optimization is e	enabled.	Optimizing	Finish

4.16 Configuring IGMP Snooping

4.16.1 Overview

1. IGMP Snooping

IGMP Snooping technology listens to IGMP packets exchanged between devices and clients to establish a relationship between multicast traffic and clients, creating corresponding multicast group table entries. This technology can convert multicast packets sent by the AP into unicast packets, thereby improving transmission speed and reducing wireless channel utilization.

Air interface: The pathway through which wireless devices transmit data.

2. Unknown Multicast Packet

An unknown multicast packet refers to a multicast data packet transmitted across the network with a destination address that has not yet been mapped to a corresponding IGMP table entry in the AP.

4.16.2 Configuration Steps

Choose Network-Wide > Workspace > WLAN Optimization > Advanced Settings.

Enable IGMP Snooping, select the action for unknown multicast packets, and click Save.

Network Optimization	Scheduled Optimization	Optimization Record	802.11k/v Roaming Optimization	Advanced
IGMP Snooping D	evice Group: Default V			
When this feature To enhance user e Setting the unkno action to "Flood"	is enabled, the AP converts mul- xperience, you are advised to en wn multicast action to "Discard ' for those specific clients.	ticast packets to unicast pa able this feature in scenar " may lead to dropping c	ackets for a higher data rate and reduc ios with high multicast traffic on air int of multicast packets sent by specific clie	ed airtime usage. erfaces or slow network connections. nts. In such cases, set the unknown multicast
IGMP Snooping				
Unknown Multicast Action	Flood ~			
I	Save			

🛕 Caution

- You are advised to enable this function when a large number of multicast packets are transmitted and the network is congested to improve the user experience.
- If you set the action for unknown multicast packets to **Discard**, multicast packets sent by certain clients may be discarded. Therefore, exercise caution when performing this configuration.

4.17 Configuring Healthy Mode

Go to the configuration page:

- Method 1: Choose Network-Wide > Workspace > Wireless > Wi-Fi > Healthy Mode.
- Method 2: Choose One-Device > Config > WLAN > Wi-Fi > Healthy Mode.

Select **Device Group** from the drop-down list box. Click **Enable** to enable the healthy mode. You are allowed to set the effective time period for the healthy mode.

After the healthy mode is enabled, the transmit power and the Wi-Fi coverage area will decrease. The healthy mode may reduce signal strength and cause network stalling. You are advised to disable it or enable it when the network is idle.

Wi-Fi List Healthy	Mode	
Healthy Mode Dev	vice Group: Default	\checkmark
Enable ⑦		
Effective Time ?	All Time	~
	Save	

4.18 Configuring XPress

- (1) Go to the page for configuration.
- Method 1: Choose Network-Wide > Workspace > Wireless > Wi-Fi > Wi-Fi List. Select the Wi-Fi network, and click Edit.
- Method 2: Choose One-Device > Config > WLAN > Wi-Fi > Wi-Fi List. Select the Wi-Fi network, and click Edit.
- Click to expand advanced settings, turn on XPress in the expanded settings and click OK. After XPress is enabled, the gaming traffic will be prioritized, ensuring a more stable gaming experience.

Band	Steering		(The 5G-supported client will access 5G radio preferentially.)
	XPress		(The client will experience faster speed.)
Layer 3 Roa	ming ?	networ	(The client will keep the IP address unchanged on the Wi-Fi k.)
80	2.11r 🕐	fast tra	(After this feature is enabled, roaming time is reduced to achieve nsition.)

4.19 Configuring Wireless Schedule

- (1) Go to the page for configuration.
- Method 1: Choose Network-Wide > Workspace > Wireless > Wi-Fi > Wi-Fi List. Select the Wi-Fi network, and click Edit.
- Method 2: Choose One-Device > Config > WLAN > Wi-Fi > Wi-Fi List. Select the Wi-Fi network, and click Edit.

(2) Click to expand advanced settings, select a scheduled time span to turn on Wi-Fi and click OK. Clients will be allowed to access the Internet only in the specified time span.

Wi-Fi Standard 🕐	Auto	~	
Schedule 🕐	All Time	^]
VLAN	All Time		
Hida SSID	Weekdays		~
Fille 351D	Weekends		1
Client Isolation 🕐	Custom		-

4.20 Enabling Reyee Mesh

Choose Network-Wide > Workspace > Wireless > AP Mesh.

After Reyee Mesh is enabled, you can set up a Mesh network through Mesh pairing between the devices that support Reyee Mesh. You can press the **Mesh** button on the device to automatically discover a new device for Mesh pairing or log in to the management page to select a new device for Mesh pairing. Reyee Mesh is enabled on the device by default.



4.21 Domain Proxy

Go to the configuration page:

- Method 1: Choose Network-Wide > Workspace > Wireless > Domain Proxy.
- Method 2: Choose One-Device > Config > WLAN > Domain Proxy.

🚺 Note

The method 2 is supported only when the AP is the primary device.

When a client accesses a Wi-Fi network, the message "No Internet connection" or "The Wi-Fi is not connected to the Internet" may be displayed. The possible cause is that the client's operating system introduces an Internet detection mechanism. Generally, the detection mechanism sends a probe packet to a specified domain name and evaluates whether the wireless network can access the Internet based on the detection result. If the DNS

server takes a long time to parse a domain name or returns a probe node with a long delay, the probe may be deemed unreachable, causing a false network unavailability.

After the **Domain Proxy** function is enabled, the device returns the preset domain name node to the client, reducing the misjudgment of network unavailability of the client.

Domain Proxy					
Enable 🔵					
User Configuration List				+ Add	Delete Selected
Domain	Name	IP		Action	
		No Data			
Up to 32 entries can be added.				Total 0 < 1	> 10/page >
Click +Add , enter the p	preset domain name and	IP address, and	click OK .		
Add			\times		
* Domain Name					
* IP	Example: 1.1.1.1				
		Cancel	ОК		

4.22 Client Association

4.22.1 Configuring Intelligent Association

Go to the configuration page by choosing **Network-Wide > Workspace > Wireless > Client Association > Intelligent Association**.

After certain smart home devices are associated with a remote AP, they are unable to re-associate with a nearby AP, resulting in poor user experience and significant delays.

With the Intelligent Association feature enabled, clients can dynamically select the access point for association, eliminating issues related to poor user experience caused by remote associations.

Toggle on the Intelligent Association switch, select the association mode, and click Save.

Signal First

Associate with the AP with the best signal.

Experience First

Associate with the AP with the best wireless experience.

Intelligent Association ⁽²⁾					
Intelligent Associat	ion 🔵				
Association Mode	• Signal First RSSI Threshold Associate with the AP with the best signal	O Experience First Associate with the AP with the best wireless experience			
Save					

4.22.2 Configuring Client Association

Choose Network-Wide > Workspace > Wireless > Client Association > Client Association.

Click **Add Association**. Select the client and the associated device. You can associate the client with a specified AP on the network to reduce remote association and improve the wireless experience.

Client Association 📀		Enter MAC Q	Delete Selected	+ Add Association
Client	IP/MAC	Associated Device ⑦	Signal Strength ≑	Action
		No Data		
Up to 128 entries can	be added.		Total 0 < 1	> 10/page >
Add Association		×		
* Client	Enter the MAC address	~		
* Associated Device ⑦	Select	~		
	Advanced Settings			
		Cancel		

Click Advanced Settings to configure the SSID for client association and to enable Forced Association.

Add Association	×
* Client	Enter the MAC address \checkmark
* Associated Device ⑦	Select ~
	Advanced Settings
SSID	Select
Forced Association	Enabling this feature will forcefully associate the client with a specific AP. However, since the client cannot initiate automatic association, this may cause disconnection and unsuccessful association attempts.
L	Cancel OK

🛕 Caution

The **Forced Association** feature may cause the client to go offline or fail to associate with the AP. Therefore, exercise caution when performing this configuration.

4.23 Configuring AP Load Balancing

4.23.1 Overview

The AP load balancing function is used to balance the load of APs in the wireless network. When APs are added to a load balancing group, clients will automatically associate with the APs with light load when the APs in the group are not load balanced. AP load balancing supports two modes:

- Client Load Balancing: The load is balanced according to the number of associated clients. When a large
 number of clients have been associated with an AP and the count difference to the AP with the lightest load
 has reached the specified value, the client can only associate with another AP in the group.
- Traffic Load Balancing: The load is balanced according to the traffic on the APs. When the traffic on an AP is large and the traffic difference to the AP with the lightest load has reached the specified value, the client can only associate with another AP in the group.

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

After a client request is denied by an AP and it fails to associate with another AP in the group, the client will keep trying to associate with this AP. If the client attempts reach the specified value, the AP will permit connection of this client, ensuring that the user can normally access the Internet.

4.23.2 Configuring Client Load Balancing

Choose Network-Wide > Workspace > Wireless > Load Balancing.

Click Add. In the dialog box that appears, set Type to Client Load Balancing, and configure Group Name, Members, and Rule.

Load Balancing	I			-	+ Add	1 Delete Selected
By grouping AP optimal traffic of For example, wi and a strategy to 2 clients, any ne APs.	Ps in the same a distribution. hen AP1 and A to trigger load ew client trying	area into a load balancing P2 are added to the same balancing when one AP h I to connect to AP1 will be	group, they can collaborate to o load balancing group, with the as 3 clients and the load-balanci e denied access and redirected to	control the access of wir load balancing type set ng threshold is 3, if AP1 o AP2, achieving load ba	eless clients a to Client Loa has 5 clients alancing betw	and to achieve d Balancing and AP2 has veen the two
Group	Name	Туре	Rule	Mem	bers	Action
			No Data			
Up to 32 entries ca	n be added.					
Add				×		
* Group Name						
* Туре	Client Load	l Balancing	~			
* Rule	Load baland	cing is triggered when t to an AP in a group read	he number of clients ches 3 , and			
	the client co	ount difference between exceeds 3.0	n the AP and other APs in nce a client has been			
	denied acce	ess to an AP in the grou owed to connect to tha	p for a total of 10 attempts, t AP again upon the next			
	attempt.					
* Members	Enter an Al	P name or SN.	~			

Cancel

Parameter	Description	
Group Name	Enter the name of the AP load balancing group.	
Туре	Select Client Load Balancing.	
Rule	Configure a detailed load balancing rule, including the maximum number of clients allowed to associate with an AP, the difference between the currently associated client count and client count on the AP with the lightest load, and the number of attempts to the AP with full load. By default, when an AP is associated with 3 clients and the difference between the currently associated client count and client count on the AP with the lightest load the currently associated client count and client count on the AP with the lightest load reaches 3, clients can associate only to another AP in the group. After a client associate to the AP upon the next attempt.	
Members	Specify the APs to be added to the AP load balancing group.	

Table 4-4 Client Load Balancing Configuration Parameters

4.23.3 Configuring Traffic Load Balancing

Choose Network-Wide > Workspace > Wireless > Load Balancing.

Click Add. In the dialog box that appears, set Type to Traffic Load Balancing, and configure Group Name, Members, and Rule.

Load Balancing			+ Add	Delete Selected	
By grouping APs in the same area into a load balancing group, they can collaborate to control the access of wireless clients and to achieve optimal traffic distribution. For example, when AP1 and AP2 are added to the same load balancing group, with the load balancing type set to Client Load Balancing and a strategy to trigger load balancing when one AP has 3 clients and the load-balancing threshold is 3, if AP1 has 5 clients and AP2 has 2 clients, any new client trying to connect to AP1 will be denied access and redirected to AP2, achieving load balancing between the two APs.					
Group Name Type Rule Members Action					
		No Data			

Up to 32 entries can be added.

Add	
* Group Name	
* Туре	Traffic Load Balancing \checkmark
* Rule	Load balancing is triggered when the traffic on an AP in a
	group reaches 5 *100Kbps, and the traffic
	difference between the AP and other APs in the group
	exceeds 5 x 100Kbps. Once a client has been
	denied access to an AP in the group for a total of 10 attempts,
	it will be allowed to connect to that AP again upon the next
	attempt.
* Members	Enter an AP name or SN.

Parameter	Description	
Group Name	Enter the name of the AP load balancing group.	
Туре	Select Traffic Load Balancing.	
Rule	Configure a detailed load balancing rule, including the maximum traffic allowed on an AP, the difference between the current traffic and the traffic on the AP with the lightest load, and the number of attempts to the AP with full load. By default, when the traffic load on an AP reaches 500 Kbit/s and the difference between the current traffic and the traffic on the AP with the lightest load reaches 500 Kbit/s, clients can associate only to another AP in the group. After a client association is denied by an AP for 10 times, the client will be allowed to associate to the AP upon the next attempt.	
Members	Specify the APs to be added to the AP load balancing group.	

Cancel

Table 4-5 Traffic Load Balancing Configuration Parameters

 \times

4.24 Wireless Authentication

4.24.1 Overview

Wireless authentication verifies the identity of users on a wireless network. Only authenticated users can access the network, ensuring wireless network security. You can configure authentication-free for wireless STAs (IP address/MAC address), public IP addresses, and domain names. Users can directly use network services or access specific websites without entering the username, password, or other information.

To use the wireless authentication function, ensure that the AP is added to Ruijie Cloud and is online. Then, configure a portal template on Ruijie Cloud and apply it to a specific SSID. When STAs connect to this SSID and access the network, the AP allows STAs added to the authentication-free lists configured on the web interface (excluding those added to the MAC address blocklist) to access the network without authentication. The AP forbids STAs whose MAC addresses are added to the MAC address blocklist configured on the web interface from accessing the network. For other users or domain names, the AP redirects them to the portal authentication page. Users need to complete identity verification on the portal page.

The following four authentication modes are supported:

- One-click Login: indicates login without the username and password.
- Voucher: indicates login with a random eight-digit password.
- Account: indicates login with the account and password.
- SMS: indicates login with the phone number and code.

Two or more authentication modes can be configured in a portal template. When multiple authentication modes are configured, users can select an authentication mode on the portal page.

4.24.2 Configuring One-click Login on Ruijie Cloud

1. Configuring a Portal Template with the Authentication Mode Set to One-click Login

- Log in to Ruijie Cloud, choose Project > Configuration > Auth & Accounts > Authentication > Captive Portal, and select a network that needs to configure wireless authentication.
- (2) Click Add Captive Portal to open the portal template configuration page.

Captive Portal ⑦



New Authentication Function

• New version upgrade, support AP/Gatgeway unified configuration

- o Support multiple login methods, one-click login, Voucher, Account, SMS verification, registered account
- Support multi-language and flexible customization of Portal pages.



(3) Click Add Page to customize a portal page.

Portal Page ᠀

Current Proje	ct	Shared Portals
Add Page		

(4) Configure basic information of the portal template.

Portal Basic Settings	
Portal Name:	
Login Options:	✓ One-click Login
	Access Duration (Min): Unlimited 15 30 60 Custom
	Voucher
	Account
	SMS
	Registration
	Facebook Account ①
Show Balance Page:	
Post-login URL:	https://www.ruijienetworks.com

Table 4-6 Portal Template Configuration Parameters

Parameter	Description			
Portal Name	Indicates the name of a captive portal template.			
Login Options	Select One-click Login, which indicates login without the username and password. You can set Access Duration and Access Times Per Day. One-click Login Access Duration (Min): Unlimited 15 30 60 Custom Customed Duration (Min): 60 Access Times Per Day: Unlimited V			
Show Balance Page	Indicates the available duration, time, or data after portal authentication.			
Post-login URL	Indicates the URL that is displayed after portal authentication.			

(5) Configure visual settings of the portal template.

Portal Visual Settings			
Logo:		Mobile Desktop	Reset style
Logo Image:	Upload		
Logo Position:	0 0 0 0 0 0		
Background :	Picture Solid Color	1 1 1 1	
Background Image:	Upload	One-click Login	
Background Mask Color:	#999999 0%		
Welcome Message ③:	• Text O Picture	the general second	
English	+	Contraction of the second	
Default Language:		Carl And Ma	and the second sec
Welcome Text:	Enter less than 60 characters.	1997年1月	Les les
		and the second	
Marketing Message:	Enter less than 60 characters.	Carlo Sala	
Terms & Conditions:			
Copyright'	Enter less than 50 characters		
Opp click Login	Litter ress than oo characters.		
Login Button:	One-click Login		
Advertisement :			
Welcome Text Color:	#ffffff		
Welcome Text Size:			
Button Color:	#0066ff		
Button Text Color:	#ffffff		
Link Color:	#ffffff		
Text Color in Box:	#ffffff		

Cancel OK

Table 4-7 Portal Page Configuration Parameters

Parameter	Description
Logo	Select whether to display the logo image.
Logo Image	When Logo is set to Image , upload the logo picture or select the default logo.
Logo Position	Select the logo position (Upper, Middle, or Lower).
Background	Select the background with the image or the solid color.

Parameter	Description	
Background Image	When Background is set to Image , upload the background image or select the default image.	
Background Mask Color	When Background is set to Solid Color , configure the background color. The default value is #ffffff .	
Welcome Message	Select the welcome message with the image or text.	
Language	 Select the language of the portal page and configure the content displayed on the portal page as required. You can click to add portal pages in other languages. Welcome Message: Select the welcome message with the image or text. Marketing message: Enter the marketing message. Terms & Conditions: Enter terms and conditions. Copyright: Enter the copyright. One-click Login: After One-click Login is enabled, you can customize the button name displayed on the portal page, which is set to One-click Login by default. One-click Login Login Button: One-click Login 	
Advertisement	Select whether to display the advertisement.	
Welcome Text Color	Select the welcome message text color. The default value is #ffffff.	
Welcome Text Size	Select the welcome text size.	
Button Color	Select the button color. The default value is #0066ff.	
Button Text Color	Select the button text color. The default value is #ffffff.	
Link Color	Select the link color. The default value is #ffffff.	
Text Color in Box	Select the text color in the box. The default value is #ffffff.	

(6) After the configuration, click **OK** to save the portal template configurations.

2. Configuring Policy Info

Configure basic information of the policy info to add captive portal. After the configuration, click **OK** for the configurations to take effect.

1 Note

When **Encryption Mode** is set to a value other than **WPA2-Enterprise(802.1x)**, the **Captive Portal** page is available. You can select whether to perform wireless authentication.

Policy Info		
* Policy Name:		
Policy Mode 10:	● Inner ◯ Local ◯ External	
Authentication Device ③:	O Router 💿 AP	
* SSID:		
Seamless Online:		
Seamless Online Period :	1 Day	\sim
Portal Escape:		

 Table 4-8
 Captive Portal Configuration Parameters

Parameter	Description	
Policy Name	Indicates the name of a captive portal template.	
Policy Mode	Indicates the authentication mode to which the captive portal applies: Inner: Cloud-based authentication. The built-in authentication server in the public cloud is used for authentication. Local: Device-based local authentication and acceleration. Portal pages and accounts in the cloud are synchronized with the device for local authentication and acceleration. External: Third-party authentication, facilitating integration between the device and a third-party authentication server for authentication.	
Authentication Device	Indicates the device that performs the authentication. When there is a router on the network, you are advised to enable authentication on the router. You can perform authentication on either an access point (AP) or a router. AP: An AP acts as the N/AS. Router: A router or gateway acts as the N/AS responsible for performing authentication at the gateway exit. Reyee AP Authentication: RAP, ReyeeOS 1.219 or later version. This parameter is not required if the policy mode is Local.	

Parameter	Description
	Indicates the wired network that requires authentication. Enter the network segment in this field.
Network	Users connecting to the wired network corresponding to this network segment must be authenticated.
	This parameter is required if the Authentication Device is Router.
	Indicates the network name of the Wi-Fi network that requires authentication.
SSID	Users connecting to this wireless network must be authenticated.
	This parameter is required if the Authentication Device is AP.
Seamless Online	After this function is enabled, if the first authentication is successful,
	subsequent connections to this Wi-Fi network will automatically be
	authenticated within a certain period of time.
	Indicates the time period for seamless online. If the first authentication is
Seamless Online Period	successful, subsequent connections to this Wi-Fi network will automatically be authenticated within this period of time.
	Indicates the portal page that is displayed after portal authentication.
Portal Page	Click Current Project to select the portal page for an existing project.
	Click Shared Portals to select an existing portal page.
	Click Add Page to customize a portal page.

4.24.3 Configuring Voucher Authentication on Ruijie Cloud

1. Configuring a Portal Template with the Authentication Mode Set to Voucher

- Log in to Ruijie Cloud, choose Project > Configuration > Auth & Accounts > Authentication > Captive Portal, and select a network that needs to configure wireless authentication.
- (2) Click Add Captive Portal to open the portal template configuration page.

Captive Portal 💿



New Authentication Function

• New version upgrade, support AP/Gatgeway unified configuration

o Support multiple login methods, one-click login, Voucher, Account, SMS verification, registered account

• Support multi-language and flexible customization of Portal pages.

Add Captive Portal

(3) Click Add Page to customize a portal page.

Portal Page ⑦ Current Project Shared Portals Add Page

(4) Configure basic information of the portal template.

Portal Basic Settings	
Portal Name:	
Login Options:	One-click Login
	Voucher
	Account
	SMS
	Registration
	Facebook Account ①
Show Balance Page:	
Post-login URL:	https://www.ruijienetworks.com

Table 4-9 Portal Template Configuration Parameters

Parameter	Description
Portal Name	Indicates the name of a captive portal template.
Login Options	Select Voucher , which indicates login with a random eight-digit password.
Show Balance Page	Indicates the available duration, time, or data after portal authentication.
Post-login URL	Indicates the URL that is displayed after portal authentication.

(5) Configure visual settings of the portal template.

Portal Page)	X
Portal Visual Settings			I
Logo:		Mobile Desktop Reset style	
Logo Image:	Upload		
Logo Position:	° ° ° ° ° ° ° ° ° ° ° ° ° ° ° ° ° ° °		
Background @:	Picture Solid Color		
Background Image:			
	Upload	Voucher Login	
Background Mask Color:	#999999 0%		
Welcome Message ③:	• Text O Picture	Access Code	
English	+	Login	
Default Language:		and the second	
Welcome Text:	Enter less than 60 characters.		
Marketing Message:	Enter less than 60 characters.	Contraction of the second s	
Terms & Conditions :			
<i>c</i>			
Copyright:	Enter less than 60 characters.		
Voucher	Voucher Login		
Code Placeholder:	Access Code		
Login Button:	Login		Í
Switching Button:	Voucher Login		
Advertisement @:			
Welcome Text Color:	#ffffff		
Welcome Text Size:	0		
Button Color:	#0066ff		
Button Text Color:	#ffffff		
Link Color:	#ffffff		
Text Color in Box:	#fffff		

Cancel OK

Table 4-10 Portal Page Configuration Parameters

Parameter	Description
Logo	Select whether to display the logo image.

Parameter	Description		
Logo Image	When Logo is set to Image , upload the logo picture or select the default logo.		
Logo Position	Select the logo position (Upper, Middle, or Lower).		
Background	Select the background with the i	mage or the solid color.	
Background Image	When Background is set to Ima the default image.	age, upload the background image or select	
Background Mask Color	When Background is set to So l default value is #ffffff .	lid Color, configure the background color. The	
Welcome Message	Select the welcome message wi	ith the image or text.	
Language	Select the language of the portal the portal page as required. You languages. Welcome Message: Select Marketing message: Enter Terms & Conditions: Enter Copyright: Enter the copyri Voucher Login: After Vouc names of controls related t Voucher Title: Code Placeholder: Login Button: Switching Button:	I page and configure the content displayed on can click to add portal pages in other the welcome message with the image or text. the marketing message. terms and conditions. terms and conditions. terms and conditions. terms and conditions. Ther Login is enabled, you can customize the o voucher authentication.	
Advertisement	Select whether to display the ad	lvertisement.	
Welcome Text Color	Select the welcome message te	xt color. The default value is #ffffff.	
Welcome Text Size	Select the welcome text size.	Select the welcome text size.	
Button Color	Select the button color. The defa	ault value is #0066ff.	
Button Text Color	Select the button text color. The default value is #ffffff.		
Link Color	Select the link color. The default value is #ffffff.		
Text Color in Box	Select the text color in the box.	Select the text color in the box. The default value is #ffffff.	

(6) After the configuration, click \mathbf{OK} to save the portal template configurations.

2. Configuring Policy Info

Configure basic information of the policy info to add captive portal. After the configuration, click **OK** for the configurations to take effect.

1 Note

When **Encryption Mode** is set to a value other than **WPA2-Enterprise(802.1x)**, the **Captive Portal** page is available. You can select whether to perform wireless authentication.

Policy Info		
* Policy Name:		
Policy Mode ⑦:	● Inner ◯ Local ◯ External	
Authentication Device ③:	ORouter AP	
* SSID:		
Seamless Online:		
Seamless Online Period :	1 Day	\sim
Portal Escape:		

 Table 4-11
 Captive Portal Configuration Parameters

Parameter	Description	
Policy Name	Indicates the name of a captive portal template.	
Policy Mode	Indicates the authentication mode to which the captive portal applies: Inner: Cloud-based authentication. The built-in authentication server in the public cloud is used for authentication. Local: Device-based local authentication and acceleration. Portal pages and accounts in the cloud are synchronized with the device for local authentication	
	and acceleration. External: Third-party authentication, facilitating integration between the device and a third-party authentication server for authentication.	

Parameter	Description
	Indicates the device that performs the authentication.
	When there is a router on the network, you are advised to enable authentication on the router. You can perform authentication on either an access point (AP) or a router.
Authentication Device	AP: An AP acts as the N/AS.
	Router: A router or gateway acts as the N/AS responsible for performing authentication at the gateway exit.
	Reyee AP Authentication: RAP, ReyeeOS 1.219 or later version.
	This parameter is not required if the policy mode is Local.
	Indicates the wired network that requires authentication. Enter the network segment in this field.
Network	Users connecting to the wired network corresponding to this network segment must be authenticated.
	This parameter is required if the Authentication Device is Router.
	Indicates the network name of the Wi-Fi network that requires authentication.
SSID	Users connecting to this wireless network must be authenticated.
	This parameter is required if the Authentication Device is AP.
	After this function is enabled, if the first authentication is successful,
Seamless Online	subsequent connections to this Wi-Fi network will automatically be
	authenticated within a certain period of time.
	Indicates the time period for seamless online. If the first authentication is
Seamless Online Period	successful, subsequent connections to this Wi-Fi network will automatically be
	authenticated within this period of time.
	Indicates the portal page that is displayed after portal authentication.
Portal Page	Click Current Project to select the portal page for an existing project.
	Click Shared Portals to select an existing portal page.
	Click Add Page to customize a portal page.

3. Adding a Voucher

- Log in to Ruijie Cloud, choose Project > Auth & Accounts > Accounts > User Management, and select a network in this account.
- (2) Configure a user group.
 - a On the **User Group** tab, click **Add**.

Cancel

Configuration Guide

Account	Voucher	User Group	≪ E-sharing	i
+ Add				
			No Data	

b Configure user group parameters. After the configuration, click **OK**.

Add user group		×
* User group name	test	
	User Group Policy	
Price		
Concurrent devices	3	~
Period	30Minutes	~
Quota (i)	100 MB	~
Maximum upload rate	Unlimited	~
Maximum download rate	Unlimited	~
Bind MAC on first use		

User Group Name: indicates the user group name.

Price: indicates the price of the user group. Mark user groups by numeral. The current version has no impact on network usage.

Concurrent Devices: indicates the number of concurrent devices for one account.

Period: indicates the maximum validity time of an account. The maximum value is counted after the client passes authentication and successfully accesses the Internet.

Quota: indicates the maximum amount of data transfer.

Maximum upload rate: indicates the maximum upload rate.

Maximum download rate: indicates the maximum download rate.

Bind MAC on first use: indicates that the MAC address of the first device used will be bound and other devices used by the same user will be prohibited from accessing the Internet.

- (3) Configure a voucher.
 - a On the Voucher tab, click Add voucher.

Account	Voucher	User Group	≪ E-sharing	1
Add voucher	Print voucher	More v	• Total Vouchers: 222 •	Activated Vouchers: 0 • Expired Vouchers: 0

b Configure voucher parameters. After the configuration, click **OK**.

Add voucher		X
* Quantity	2	
* User group	^]
	test	
User information setting $leftarrow$	Custom	
Advance setting \checkmark		
	Cance	ОК

Quantity: Enter the quantity of the voucher to print. When the value is set to 1, you can add a voucher and configure the name and the email address. When the value is greater than 1, you can add vouchers in batches. In this case, you can only configure the name and email address separately after the vouchers are added.

User group: Select a created user group from the drop-down list. If the created user group does not meet the requirements, click **Custom** to create a user group.

User information setting: Configure user information, which is optional.

Advance setting:

o Voucher code type: Set the value to Alphanumeric 0-9, a-z, Alphabetic a-z, or Numeric 0-9.

Advance Setting 🔨			
Voucher code type	Alphanumeric 0-9, a-z		^
Voucher length	Alphanumeric 0-9, a-z		
	Alphabetic a-z		
	Numeric 0-9		
		Cancel	ОК

• Voucher length: Select the voucher length. The value ranges from 6 to 9.

Voucher length	6	
	6	
	7	
	8	
	9	

(4) Obtain the voucher code from the voucher list.

٩	Voucher	Expired Vouchers:	Activated Vouchers: 0	Total Vouchers: 4	r More 🗸 🔵	Print vouche	dd vou
Operation	Expired a	Activated at	Created at	Period	User Group	Voucher code	
LCO	•		2022-08-12 18:34:31	Unlimited	1	fqyhwg	
LCO			2022-08-12 18:34:31	Unlimited	1	dxwgkh	
LCO			2022-08-12 11:09:07	Unlimited	1	t5nq76	
LCO		-	2022-08-12 11:09:07	Unlimited	1	jsz75g	

4.24.4 Configuring Account Authentication on Ruijie Cloud

1. Configuring a Portal Template with the Authentication Mode Set to Account

- Log in to Ruijie Cloud, choose Project > Configuration > Auth & Accounts > Authentication > Captive Portal, and select a network that needs to configure wireless authentication.
- (2) Click Add Captive Portal to open the portal template configuration page.

Captive Portal ⑦



New Authentication Function

• New version upgrade, support AP/Gatgeway unified configuration

- o Support multiple login methods, one-click login, Voucher, Account, SMS verification, registered account
- Support multi-language and flexible customization of Portal pages.



(3) Click Add Page to customize a portal page.

Portal Page ⑦

Current Project	Shared Portals
Add Page	

(4) Configure basic information of the portal template.

One-click Login
Voucher
Account
SMS
Registration
Facebook Account ①
https://www.ruijienetworks.com

Table 4-12 Portal Template Configuration Parameters

Parameter	Description
Portal Name	Indicates the name of a captive portal template.
Login Options	Select Account, which indicates login with the account and password.
Show Balance Page	Indicates the available duration, time, or data after portal authentication.
Post-login URL	Indicates the URL that is displayed after portal authentication.

(5) Configure visual settings of the portal template.

Portal Page				>
Portal Visual Settings				
Logo:		Mobile Desktop	Reset style	
Logo Image:	Upload			
Logo Position:	° ° ° ° ° ° ° ° ° ° ° ° ° ° ° ° ° ° °			
Reduced Or	Distant O Calid Calar	1		
Background Image:				
background image.				
		Account Login	all good	
Background Mask Color:	#999999 0%	Account Login		
Welcome Message @:	Text Picture	Account		
English	+	Password		
Default Language			and the second	
Welcome Text:	Enter less than 60 characters	Login		
welcome lext.	Litter less than of characters.	Lie Deg	to the	
Marketing Message:	Enter less than 60 characters.			
Terms & Conditions		and the set of		
ternis & conditions.				
Copyright:	Enter less than 60 characters.			
Account				
Title:	Account Login			
Account Placeholder:	Account			
Password Placeholder:	Password			
Login Button:	Login			
Advertisement @:				
Welcome Text Color:	#ffffff			
Welcome Text Size:	0			
Button Color:	#0066ff			
Button Text Color:	#ffffff			
Link Color:	#ffffff			
Text Color in Box:	#ffffff			
				_

Cancel OK

Parameter	Description
Logo	Select whether to display the logo image.

Table 4-13 Portal Page Configuration Parameters

Parameter	Description				
Logo Image	When Logo is set to Image , upload the logo picture or select the default logo.				
Logo Position	Select the logo position (Upper, Middle, or Lower).				
Background	Select the background with the image or the solid color.				
Background Image	When Background is set to Image , upload the background image or select the default image.				
Background Mask Color	When Background is set to Solid Color , configure the background color. The default value is #ffffff .				
Welcome Message	Select the welcome message with the image or text.				
Language	Select the language of the portal page and configure the content displayed on the portal page as required. You can click to add portal pages in other languages. • Welcome Message: Select the welcome message with the image or text. • Marketing message: Enter the marketing message. • Terms & Conditions: Enter terms and conditions. • Copyright: Enter the copyright. • Account Login: After Account Login is enabled, you can customize the names of the controls related to account authentication. • Account Title: Account • Account • Password Placeholder: Password Login Button: Login • Switching Button: Account Login				
Advertisement	Select whether to display the advertisement.				
Welcome Text Color	Select the welcome message text color. The default value is #ffffff.				
Welcome Text Size	Select the welcome text size.				
Button Color	Select the button color. The default value is #0066ff.				
Button Text Color	Select the button text color. The default value is #ffffff.				
Link Color	Select the link color. The default value is #ffffff.				
Text Color in Box	Select the text color in the box. The default value is #ffffff.				

(6) After the configuration, click **OK** to save the portal template configurations.

2. Configuring Policy Info

Configure basic information of the policy info to add captive portal. After the configuration, click **OK** for the configurations to take effect.

1 Note

When **Encryption Mode** is set to a value other than **WPA2-Enterprise(802.1x)**, the **Captive Portal** page is available. You can select whether to perform wireless authentication.

Policy Info		
* Policy Name:		
Policy Mode ⑦:	● Inner ◯ Local ◯ External	
Authentication Device ③:	O Router O AP	
* SSID:		
Seamless Online:		
Seamless Online Period :	1 Day	~
Portal Escape:		

Table 4-14 Captive Portal Configuration Parameters

Parameter	Description
Policy Name	Indicates the name of a captive portal template.
Policy Mode	Indicates the authentication mode to which the captive portal applies: Inner: Cloud-based authentication. The built-in authentication server in the public cloud is used for authentication. Local: Device-based local authentication and acceleration. Portal pages and accounts in the cloud are synchronized with the device for local authentication and acceleration. External: Third-party authentication, facilitating integration between the device and a third-party authentication server for authentication.

Parameter	Description
	Indicates the device that performs the authentication.
	When there is a router on the network, you are advised to enable authentication on the router. You can perform authentication on either an access point (AP) or a router.
Authentication Device	AP: An AP acts as the N/AS.
	Router: A router or gateway acts as the N/AS responsible for performing authentication at the gateway exit.
	Reyee AP Authentication: RAP, ReyeeOS 1.219 or later version.
	This parameter is not required if the policy mode is Local.
	Indicates the wired network that requires authentication. Enter the network segment in this field.
Network	Users connecting to the wired network corresponding to this network segment must be authenticated.
	This parameter is required if the Authentication Device is Router.
	Indicates the network name of the Wi-Fi network that requires authentication.
SSID	Users connecting to this wireless network must be authenticated.
	This parameter is required if the Authentication Device is AP.
	After this function is enabled, if the first authentication is successful,
Seamless Online	subsequent connections to this Wi-Fi network will automatically be
	authenticated within a certain period of time.
	Indicates the time period for seamless online. If the first authentication is
Seamless Online Period	successful, subsequent connections to this Wi-Fi network will automatically be authenticated within this period of time.
	Indicates the portal page that is displayed after portal authentication.
Portal Page	Click Current Project to select the portal page for an existing project.
i ulai raye	Click Shared Portals to select an existing portal page.
	Click Add Page to customize a portal page.

3. Adding an Account

- Log in to Ruijie Cloud, choose Project > Auth & Accounts > Accounts > User Management, and select a network in this account.
- (2) Configure a user group.
 - a On the **User Group** tab, click **Add**.

Cancel

Configuration Guide

Account	Voucher	User Group	≪ E-sharing	i
+ Add				
			No Data	

b Configure user group parameters. After the configuration, click **OK**.

Add user group		×
* User group name	test	
	User Group Policy	
Price		
Concurrent devices	3	~
Period	30Minutes	~
Quota (i)	100 MB	~
Maximum upload rate	Unlimited	~
Maximum download rate	Unlimited	~
Bind MAC on first use		

User Group Name: indicates the user group name.

Price: indicates the price of the user group. Mark user groups by numeral. The current version has no impact on network usage.

Concurrent Devices: indicates the number of concurrent devices for one account.

Period: indicates the maximum validity time of an account. The maximum value is counted after the client passes authentication and successfully accesses the Internet.

Quota: indicates the maximum amount of data transfer.

Cancel

Maximum upload rate: indicates the maximum upload rate.

Maximum download rate: indicates the maximum download rate.

Bind MAC on first use: indicates that the MAC address of the first device used will be bound and other devices used by the same user will be prohibited from accessing the Internet.

- (3) On the Account tab, add an account. Accounts can be added manually or through batch import.
- Adding an account manually

Click Add an Account, set parameters about the account, and click OK.

Add account		Х
* User name		
* Password		
* User group		~
Allow VPN connection		
Tips: By enabling this option, t	he user can use this account to log in remotely using a VPN.	
User information setting $ \lor $		

User name: The value is a string of less than 32 characters, consisting of letters, numerals, and underscores.

Password: The value is a string of less than 32 characters, consisting of letters, numerals, and underscores.

User group: Select a created user group from the drop-down list. If the created user group does not meet the requirements, click **Custom** to create a user group.

Allow VPN connection: By enabling this option, the user can use this account to log in remotely using a VPN.

User information setting: You can expand it to have more user information displayed, including the first name, last name, email, phone number, and alias.

- Adding accounts through batch import
 - a Click Bulk import.

Bulk import accounts

Х

Step1: Download and fill in the device information in the template. Up to 500 records can be imported each time.

Account and Password fields are required. Please enter less than 32 characters, consisting of letters, numbers or underscores.



- b Click Download Template to download the template.
- c Edit the template and save it.

A Caution

- Account, Password, and User Group are mandatory.
- Check that the user group already exists and the added accounts are not duplicate with existing accounts.

11	<u>ь</u>	~ ~				0
Account	Password	First name	Last name	Alias	User group	Email
test2	test2				test	
test3	test3				test	
test4	test4				test	

d Click **Please select an .xls or .xlsx file** to upload the file. After uploading, users are automatically created.

Account	Voucher	User Group	Contraction Contractic Con	(j)							
Add accou	unt Bulk import	One-click send	More v • T	otal Accounts: 3 🏼 A	ctivated Accounts: (• Expired Accounts: 0				Accou	nt Q
	Account	Password	User group	Status 🛈 🐨	Period	First name	Alias	Created at	Activated at	Ex	Operation
	test3	test3	test	Not used	30Minutes	Empty	Empty.	2023-02-13 16:42:21	-		∠Cē
	test4	test4	test	Not used	30Minutes	Empty	Empty.	2023-02-13 16:42:21	-		∠Cē
	test2	test2	test	Not used	30Minutes	Empty	Empty	2023-02-13 16:42:21	-		∠Cō

3 in total \langle **1** \rangle **10 / page** \vee

4.24.5 Configuring SMS Authentication on Ruijie Cloud

1. Adding a Twilio Account

Prerequisites

A Twilio account has been applied for from the Twilio official website (https://www.twilio.com/login).

Note

A Twilio account is used to send the SMS verification code.

Configuration Steps

(1) Log in to Ruijie	Cloud and choose 🥝	> A	ccol	int.					
		Ð	Q	Û.	Ģ	۲	0	8	
					Acco	unt			
					Sub	Accour	nt		
					SAM	l SSO			
					Help	Cente	r		
					Supp	orted	Model	s	
					Swite	ch to C	ld Des	ign	
					Logo	ut			
							:=	1×1	

(2) Add Twilio account information and click Save.

Modify Twilio Account How to apply twilio account?

Twilio Account SID:	Account SID of Twilio	
Auth Token:	Auth Token of Twilio	
Auth Phone:	Active Number (Country Code + Phone Number) of Twilio	
	Save	

2. Configuring a Portal Template with the Authentication Mode Set to SMS

- Log in to Ruijie Cloud, choose Project > Configuration > Auth & Accounts > Authentication > Captive Portal, and select a network that needs to configure wireless authentication.
- (2) Click Add Captive Portal to open the portal template configuration page.

Captive Portal ⑦



New Authentication Function

o New version upgrade, support AP/Gatgeway unified configuration
 o Support multiple login methods, one-click login, Voucher, Account, SMS verification, registered account

o Support multi-language and flexible customization of Portal pages.

Add Captive Portal
(3) Click Add Page to customize a portal page.

Portal Page 곗	
Current Project	Shared Portals
Add Page	

(4) Configure basic information of the portal template.

Portal Basic Settings	
Portal Name:	
Login Options:	One-click Login
	Voucher
	Account
	SW2
	Twilio Account SID:
	Auth Token:
	Auth Phone:
	Registration
	Facebook Account ① The SMS configuration cannot be empty
Show Balance Page:	
Post-login URL:	https://www.ruijienetworks.com

Table 4-15 Portal Template Configuration Parameters

Parameter	Description
Portal Name	Indicates the name of a captive portal template.
Login Options	Select SMS , which indicates login with the phone number and code.
Show Balance Page	Indicates the available duration, time, or data after portal authentication.
Post-login URL	Indicates the URL that is displayed after portal authentication.

(5) Configure visual settings of the portal template.

Portal Page			Х
Portal Visual Settings			1
Logo:		Mobile Desktop Reset style	
Logo Image:	Upload		
Logo Position:	• • • • • • •		
Background @:			
Background Image:			- 1
		CMC	
Background Mask Color:	Upioad 0%	SMS Login	
Welcome Message @:	Text Dicture	+86 Phone	
English	+	(Verification Code) Get Code	
Ligisi	_ 1		
Default Language:		Login	
Welcome Text:	Enter less than 60 characters.	and the second	
Marketing Message:	Enter less than 60 characters.		
		a the second sec	
Terms & Conditions:			
Copyright:	Enter less than 60 characters.		
SMS			
Title:	SMS Login		
Phone Placeholder:	Phone		
Code Placeholder:	Verification Code		
Code Button:	Get Code		- 1
Advertisement @:			
Welcome Text Color:	#fffff		
Welcome Text Size:	0		
Button Color:	#0066ff		
Button Text Color:	#ffffff		
Link Color:	#ffffff		
Text Color in Box:	#fffff		

Cancel OK

Parameter	Description	Description		
Logo	Select whether to display the logo image.			
Logo Image	When Logo is set to Image , upload the logo picture or select the default logo.			
Logo Position	Select the logo position (Upper, Middle, or Lower).		
Background	Select the background wi	th the image or the solid color.		
Background Image	When Background is set to Image , upload the background image or select the default image.			
Background Mask Color	When Background is set to Solid Color , configure the background color. The default value is #ffffff .			
Welcome Message	Select the welcome mess	Select the welcome message with the image or text.		
Language	Select the welcome message with the image or text. Select the language of the portal page and configure the content displayed on the portal page as required. You can click + to add portal pages in other languages. • Welcome Message: Select the welcome message with the image or text. • Marketing message: Enter the marketing message. • Terms & Conditions: Enter terms and conditions. • Copyright: Enter the copyright. • SMS Login: After SMS Login is enabled, you can customize the names of the controls related to SMS authentication. SMS SMS Title: SMS Login Phone Code Placeholder: Code Button: Get Code Login Button: Login Switching Button: SMS Login			
Advertisement	Select whether to display the advertisement.			
Welcome Text Color	Select the welcome message text color. The default value is #ffffff.			
Welcome Text Size	Select the welcome text size.			
Button Color	Select the button color. The default value is #0066ff.			

Table 4-16 Portal Page Configuration Parameters

Parameter	Description
Button Text Color	Select the button text color. The default value is #ffffff.
Link Color	Select the link color. The default value is #ffffff.
Text Color in Box	Select the text color in the box. The default value is #ffffff.

(6) After the configuration, click **OK** to save the portal template configurations.

3. Configuring Policy Info

Configure basic information of the policy info to add captive portal. After the configuration, click **OK** for the configurations to take effect.

1 Note

When Encryption Mode is set to a value other than WPA2-Enterprise(802.1x), Go to the "Captive Portal" page is available and you can select whether to perform wireless authentication.

Policy Info		
* Policy Name:		
Policy Mode ③:	● Inner ◯ Local ◯ External	
Authentication Device ③:	ORouter	
* SSID:		
Seamless Online:		
Seamless Online Period :	1 Day	\vee
Portal Escape:		

Table 4-17 Captive Portal Configuration Parameters

Parameter	Description
Policy Name	Indicates the name of a captive portal template.

Parameter	Description
	Indicates the authentication mode to which the captive portal applies:
	Inner: Cloud-based authentication. The built-in authentication server in the
	public cloud is used for authentication.
Policy Mode	Local: Device-based local authentication and acceleration. Portal pages and accounts in the cloud are synchronized with the device for local authentication and acceleration.
	External: Third-party authentication, facilitating integration between the device and a third-party authentication server for authentication.
	Indicates the device that performs the authentication.
	When there is a router on the network, you are advised to enable authentication on the router. You can perform authentication on either an access point (AP) or a router.
Authentication Device	AP: An AP acts as the N/AS.
	Router: A router or gateway acts as the N/AS responsible for performing authentication at the gateway exit.
	Reyee AP Authentication: RAP, ReyeeOS 1.219 or later version.
	This parameter is not required if the policy mode is Local.
	Indicates the wired network that requires authentication. Enter the network segment in this field.
Network	Users connecting to the wired network corresponding to this network segment must be authenticated.
	This parameter is required if the Authentication Device is Router.
	Indicates the network name of the Wi-Fi network that requires authentication.
SSID	Users connecting to this wireless network must be authenticated.
	This parameter is required if the Authentication Device is AP.
Seamless Online	After this function is enabled, if the first authentication is successful, subsequent connections to this Wi-Fi network will automatically be authenticated within a certain period of time.
Seamless Online Period	Indicates the time period for seamless online. If the first authentication is successful, subsequent connections to this Wi-Fi network will automatically be authenticated within this period of time.
	Indicates the portal page that is displayed after portal authentication.
Portal Page	Click Current Project to select the portal page for an existing project.
	Click Shared Portals to select an existing portal page.
	Click Add Page to customize a portal page.

4.24.6 Configuring Registration on Ruijie Cloud

- 1. Configuring a Portal Template with the Authentication Mode Set to One-click Login
- Log in to Ruijie Cloud, choose Project > Configuration > Auth & Accounts > Authentication > Captive Portal, and select a network that needs to configure wireless authentication.
- (2) Click Add Captive Portal to open the portal template configuration page.

Captive Portal ⑦



New Authentication Function

New version upgrade, support AP/Gatgeway unified configuration
 Support multiple login methods, one-click login, Voucher, Account, SMS verification, registered account

• Support multi-language and flexible customization of Portal pages.



(3) Click Add Page to customize a portal page.

Portal Page ⑦



(4) Configure basic information of the portal template.

Portal Basic Settings	
Portal Name:	
Login Options:	✓ One-click Login
	Access Duration (Min): Unlimited 15 030 60 Custom
	Voucher
	Account
	SMS
	Registration
	Facebook Account ①
Show Balance Page:	
Post-login URL:	https://www.ruijienetworks.com

Table 4-18 Portal Template Configuration Parameters

Parameter	Description		
Portal Name	Indicates the name of a captive portal template.		
Login Options	Select One-click Login, which indicates login without the username and password. You can set Access Duration and Access Times Per Day. One-click Login Access Duration (Min): Unlimited 15 30 60 Custom Customed Duration (Min): 60 Access Times Per Day: Unlimited V		
Show Balance Page	Indicates the available duration, time, or data after portal authentication.		
Post-login URL	Indicates the URL that is displayed after portal authentication.		

(5) Configure visual settings of the portal template.

Portal Visual Settings			
Logo:		Mobile Desktop Reset style	
Logo Image:	Upload	a sulla su s	
Logo Position:	° ° ° ° ° ° ° ° ° ° ° ° ° ° ° ° ° ° °		
Background :	Picture Solid Color		
Background Image:	Upload	One-click Login	
Background Mask Color:	#999999 0%	and the second second	
Welcome Message ③:	• Text O Picture	the parts .	
English	+	- 🖌 🖈 👘 📩	
Default Language:		a share proved	
Welcome Text:	Enter less than 60 characters.		
Marketing Message:	Enter less than 60 characters.	and the second	
Terms & Conditions:			
Copyright:	Enter less than 60 characters.		
One-click Login			
Login Button:	One-click Login		
Advertisement ③:			
Welcome Text Color:	#ffffff		
Welcome Text Size:	-0		
Button Color:	#0066ff		
Button Text Color:	#ffffff		
Link Color:	#ffffff		
Text Color in Box:	#ffffff		

Cancel OK

Table 4-19 Portal Page Configuration Parameters

Parameter	Description
Logo	Select whether to display the logo image.
Logo Image	When Logo is set to Image , upload the logo picture or select the default logo.
Logo Position	Select the logo position (Upper, Middle, or Lower).
Background	Select the background with the image or the solid color.

Parameter	Description				
Background Image	When Background is set to Image , upload the background image or select the default image.				
Background Mask Color	When Background is set to Solid Color , configure the background color. The default value is #ffffff .				
Welcome Message	Select the welcome message with the image or text.				
Language	 Select the language of the portal page and configure the content displayed on the portal page as required. You can click to add portal pages in other languages. Welcome Message: Select the welcome message with the image or text. Marketing message: Enter the marketing message. Terms & Conditions: Enter terms and conditions. Copyright: Enter the copyright. One-click Login: After One-click Login is enabled, you can customize the button name displayed on the portal page, which is set to One-click Login by default. One-click Login Login Button: One-click Login 				
Advertisement	Select whether to display the advertisement.				
Welcome Text Color	Select the welcome message text color. The default value is #ffffff.				
Welcome Text Size	Select the welcome text size.				
Button Color	Select the button color. The default value is #0066ff.				
Button Text Color	Select the button text color. The default value is #ffffff.				
Link Color	Select the link color. The default value is #ffffff.				
Text Color in Box	Select the text color in the box. The default value is #ffffff.				

(6) After the configuration, click **OK** to save the portal template configurations.

2. Configuring Policy Info

Configure basic information of the policy info to add captive portal. After the configuration, click **OK** for the configurations to take effect.

1 Note

When **Encryption Mode** is set to a value other than **WPA2-Enterprise(802.1x)**, the **Captive Portal** page is available. You can select whether to perform wireless authentication.

Policy Info		
* Policy Name:		
Policy Mode 10:	● Inner ◯ Local ◯ External	
Authentication Device ③:	O Router () AP	
* SSID:		
Seamless Online:		
Seamless Online Period :	1 Day	\sim
Portal Escape:		

Parameter	Description
Policy Name	Indicates the name of a captive portal template.
Policy Mode	Indicates the authentication mode to which the captive portal applies: Inner: Cloud-based authentication. The built-in authentication server in the public cloud is used for authentication. Local: Device-based local authentication and acceleration. Portal pages and accounts in the cloud are synchronized with the device for local authentication and acceleration. External: Third-party authentication, facilitating integration between the device and a third-party authentication server for authentication.
Authentication Device	 Indicates the device that performs the authentication. When there is a router on the network, you are advised to enable authentication on the router. You can perform authentication on either an access point (AP) or a router. AP: An AP acts as the N/AS. Router: A router or gateway acts as the N/AS responsible for performing authentication at the gateway exit. Reyee AP Authentication: RAP, ReyeeOS 1.219 or later version. This parameter is not required if the policy mode is Local.

Parameter	Description				
	Indicates the wired network that requires authentication. Enter the network segment in this field.				
Network	Users connecting to the wired network corresponding to this network segment must be authenticated.				
	This parameter is required if the Authentication Device is Router.				
	Indicates the network name of the Wi-Fi network that requires authentication.				
SSID	Users connecting to this wireless network must be authenticated.				
	This parameter is required if the Authentication Device is AP.				
	After this function is enabled, if the first authentication is successful,				
Seamless Online	subsequent connections to this Wi-Fi network will automatically be				
	authenticated within a certain period of time.				
	Indicates the time period for seamless online. If the first authentication is				
Seamless Online Period	successful, subsequent connections to this Wi-Fi network will automatically be authenticated within this period of time.				
	Indicates the portal page that is displayed after portal authentication.				
	Click Current Project to select the portal page for an existing project.				
Portal Page	Click Shared Portals to select an existing portal page.				
	Click Add Page to customize a portal page.				

4.24.7 Configuring an Authentication-Free User List on Web Interface

You can configure authentication-free for wireless STAs (IP address/MAC address), public IP addresses, and domain names. Users can directly use network services or access specific websites without entering the username, password, or other information.

1. Configuring an Authentication-Free User

- (1) Choose Network-Wide > Workspace > Wireless > Wireless Auth > Allowlist > User Allowlist.
- (2) Click Add to open the configuration page.

Cloud Integration	Allowlist	Client List	
i A user configu	ured with whitelis	ed IP or MAC address can access the Internet without authentication.	
User Allowlist	IP Allowlist	Domain Allowlist MAC Blocklist/Allowlist	
User Allowlist			+ Add Delete Selected
Up to 50 entries	can be added.		
		IP / IP Range	Action
		No Data	
< 1 >	10/page 🗸		Total 0

(3) Configure an STA IP address or IP address range. After the configuration, click **OK** to save the configurations.

Add				×
	* IP / IP Range	Example: 1.1.1.1-1.1.1.100		
			Cancel	ОК

2. Configuring an Authentication-Free Public IP Address

- (1) Choose Network-Wide > Workspace > Wireless > Wireless Auth > Allowlist > IP Allowlist.
- (2) Click Add to open the configuration page.

Cloud Integration	Allowlist	Client List	
i A user config	ured with whitelis	ted IP or MAC address can access the Internet without authentication.	
User Allowlist	IP Allowlist	Domain Allowlist MAC Blocklist/Allowlist	
IP Allowlist			+ Add Delete Selected
Up to 50 entries	can be added.		
		IP / IP Range	Action
		No Data	
< 1 >	10/page V		Total 0

(3) Configure a public IP address or public IP address range. After the configuration, click **OK** to save the configurations.

			×
Example: 1.1.1.1-1.1.1.100			
		Cancel	ОК
	Example: 1.1.1.1-1.1.1.100	Example: 1.1.1.1.1.100	Example: 1.1.1.1.1.100

3. Configuring a Domain Name Allowlist

- (1) Choose Network-Wide > Workspace > Wireless > Wireless Auth > Allowlist > Domain Allowlist.
- (2) Click **Add** to open the configuration page.

Cloud Integration	Allowlist	Client List					
<i>i</i> A user configu	ured with whiteli	isted IP or MAC address ca	n access the Internet without a	uthentication.			
User Allowlist	IP Allowlist	Domain Allowlist	MAC Blocklist/Allowlist				
Domain Allow	/list					+ Add	Delete Selected
Up to 100 entrie	s can be added.						
				URL			Action
				No Data			
< 1 >	10/page v						Total 0

(3) Configure authentication-free websites. After the configuration, click **OK**.

Add			\times
* (RL		
		Cancel	ОК

4. Configuring a MAC Address Allowlist and Blocklist

STAs whose MAC addresses are added to the MAC address allowlist can access the network without authentication, and STAs whose MAC addresses are added to the MAC address blocklist are forbidden to access the network.

- (1) Choose Network-Wide > Workspace > Wireless > Wireless Auth > Allowlist > MAC Blocklist/Allowlist.
- (2) Click Add to open the MAC address allowlist or blocklist configuration page.

Cloud Integration Allowlist	Client List		
() A user configured with whitelis	ted IP or MAC address can access the Internet without authentication.		
User Allowlist IP Allowlist	Domain Allowlist MAC Blocklist/Allowlist		
MAC Allowlist		+ Add	Delete Selected
Up to 250 entries can be added.			
	MAC Address		Action
	No Data		
< 1 > 10/page >			Total 0
MAC Blocklist		+ Add	Delete Selected
Up to 250 entries can be added.			
	MAC Address		Action
	No Data		
< 1 > 10/page >			Total 0

(3) Configure the MAC address of a wireless STA. After the configuration, click **OK**.

Add			×
* MAC Address	Example: 00:11:22:33:44:55		
		Cancel	ОК

4.24.8 Displaying Authenticated Users on web interface

Choose Network-Wide > Workspace > Wireless > Wireless Auth > Client List to display authenticated users.

Note							
client going offl	ine will not	t disappear im	mediately. In	stead, the c	lient will stay c	on the list for	three more
utes.							
Integration Allowlist	Client List						
ent List						P/MAC	Q ψ Batch Logout
The client going offline will	not disappear imm	nediately. Instead, the clien	t will stay in the list for t	three more minutes.			
Username	IP	MAC Address	Online Time	Auth Type	Connect the SSID	Access Name	Action
			No E	Data			
1 > 10/page >							Total 0
	Note client going offlutes.	Note client going offline will not utes. Integration Allowlist Client List ent List The client going offline will not disappear imm Username IP	Note client going offline will not disappear imutes. Integration Allowlist Client List Inte client going offline will not disappear immediately. Instead, the client Username IP MAC Address	Note client going offline will not disappear immediately. In utes. Integration Allowlist Client List ent List The client going offline will not disappear immediately. Instead, the client will stay in the list for Username IP MAC Address Online Time No t 1 > 10/page	Note client going offline will not disappear immediately. Instead, the client states. Integration Allowlist Client List Inte client going offline will not disappear immediately. Instead, the client will stay in the list for three more minutes. Username IP MAC Address Online Time No Data Image: Table State	Note client going offline will not disappear immediately. Instead, the client will stay of utes. Integration Allowlist Client List ent List Immediately. Instead, the client will stay in the list for three more minutes. Username IP MAC Address Online Time Auth Type Connect the SSID No Data I Improve Improve Improve	Note client going offline will not disappear immediately. Instead, the client will stay on the list for ites. Integration Allowlist Client List ent List IP/MAC Inte client going offline will not disappear immediately. Instead, the client will stay in the list for three more minutes. IP/MAC Inte client going offline will not disappear immediately. Instead, the client will stay in the list for three more minutes. IP/MAC Inte client going offline will not disappear immediately. Instead, the client will stay in the list for three more minutes. INO Data Image: Image

4.24.9 Displaying Authenticated Users on Ruijie Cloud

Log in to Ruijie Cloud, choose **Project** > **Network** > **Clients** > **Auth Clients**, and select a network that needs to display authenticated users.



4.25 Configuring 802.1X Authentication

4.25.1 Overview

IEEE 802.1X is a port-based network access control standard that provides secure access services for LANs.

On an IEEE 802 LAN, a user can directly access network resources without authentication and authorization as long as it can connect to a network device. This uncontrolled behavior can bring security risks to the network. The IEEE 802.1X protocol was proposed to address the security issues on an IEEE 802 LAN.

The IEEE 802.1X protocol supports three security applications: Authentication, Authorization, and Accounting, abbreviated as AAA.

- Authentication: Determines whether a user can obtain access, and restricts unauthorized users.
- Authorization: Authorizes services available for authorized users, and controls the permissions of unauthorized users.
- Accounting: Records the usage of network resources by users, and provides a basis for traffic billing.

The 802.1X feature can be deployed on networks to control user authentication, authorization, and more.

An 802.1X network uses a typical client/server architecture, consisting of three entities: client, access device, and authentication server. A typical architecture is shown here.

Figure 4-1 Typical Architecture of 802.1X Network



- The client is usually an endpoint device which can initiate 802.1X authentication through the client software. The client must support the Extensible Authentication Protocol over LANs (EAPoL) on the local area network.
- The access device is usually a network device (AP or switching device) that supports the IEEE 802.1X protocol. It provides an interface for clients to access the local area network, which can be a physical or a logical interface.
- The authentication server can realize user authentication, authorization, and accounting. Usually a RADIUS server is used as the authentication server.

1 Note

The RG-RAP APs only support the authentication.

4.25.2 Configuring 802.1X Authentication

- (1) Choose Network-Wide > Workspace > Wireless > 802.1x Authentication.
- (2) Click Global 802.1x. A pop-up window is displayed. Click OK.

Configuration Guide

802.1x Authentication	RADIUS	Server Management	Wireless User List	Wired User List
802.1x Authen	tication De	evice Group: Default		
Global 802.1x				
Authentication				~
		Are you sure you want to	o Enable global 802.1x	^
	Go to	authentication?		
	Set the		Cancel	ок
	_			
Escape SSID	•			
Re-authentication	•			
Client Packet * Timeout Duration	30			
	Override			

Enable the **Escape SSID** and configure parameters such as Escape SSID. Users can temporarily connect to the Escape SSID without a password when the authentication server is unavailable.

Escape SSID	• 0	
* Escape SSID	802.1x_escape	
* Security	WPA-PSK	~
* Wi-Fi Password	•••••	***

Toggle on **Re-authentication** and set the re-authentication interval. The re-authentication function performs periodic user authentication, and users who do not pass the periodic authentication will be disconnected.

A Caution							
The re-authenticati	The re-authentication interval must be set to 10800 seconds or above.						
Re-authentication							
* Re-auth Interval	s						

Client Packet Timeout Duration: The time limit for a client to wait for a response from the server. An authentication failure occurs after this time limit expires. The value range is 10 to 60 seconds.

802.1x Authen	tication	Device Group:	Default	~
Global 802.1x				
Authentication				
	Go to Wi Set the sec	- Fi curity mode of the	e SSID to 802	.1X (Enterprise
Escape SSID	0			
Re-authentication	0			
Client Packet * Timeout Duration	30			s
	Overrid	e		

(3) Add a server.

Before proceeding, make sure that the following conditions are met:

- The RADIUS server is ready and the following configurations have been completed.
 - o A username and a password have been added for client login.
 - The firewall has been disabled. Otherwise, authentication messages may be blocked, leading to authentication failure.
 - The IP address of the device to be authenticated has been added as a trusted IP address on the RADIUS server.
- The network between the device and the RADIUS server is reachable.
- The IP addresses of the RADIUS server and the device to be authenticated have been obtained.

Click **Add Server group** to configure server group parameters. You can click **Edit** to edit the server group, and click **Delete** to delete the server group.

🚺 Note

- You need to add at least one server for each server group, and a maximum of five servers can be added.
- Up to 20 server groups can be added under **RADIUS Server Management**.

802.1x Authentication	RADIUS Server Management	Wireless User List	Wired User List		
RADIUS Server M	anagement				Add Server group
Up to 20 entries can b	be added.				
Server group name	Server IP	Auth Port	Accounting Port	Shared Password	Action
group1	1.1.1.2 1.1.1.1	1812 1812	1813 1813	ruijie ruijie	Edit Delete
group2	1.1.1.3	1812	1813	ruijie	Edit Delete

You can click \bigcirc Add Server to add multiple servers to a server group, and click 1 Server to delete a selected server.

Add				\times
* Server group name				
* Server IP	🔟 Server 1			
* Server name				
* Auth Port	1812			
* Accounting Port	1813	0		
* Shared Password				
* Match Order		0		
	••••••••••••••••••••••••••••••••••••••	 		
		Cancel	ОК	

Table 4-21 Server Group Configuratio

Parameter	Description
Server group name	Name of RADIUS server group
Server IP	IP address of the RADIUS server.
Server name	Name of RADIUS server
Auth Port	The port number for the RADIUS server to perform user authentication.
Accounting Port	The port number for the RADIUS server to perform user accounting.
Shared Password	Shared key of the RADIUS server.
Match Order	The system supports up to five RADIUS servers. A larger value indicates a higher priority.

(4) Configure the server and click **Save**.

RADIUS Server Management					Add Server
Up to 5 entries can be added.					
Server IP	Auth Port	Accounting Port	Shared Password	Match Order	Action
			No Data		
Server global configuration					
		* Packet Retransmission Interval	3 5		
		Packet Retransmission Count	3 time		
		Server Detection			
		Detection Interval	1 min		
		* Detection Count	5 time	0	
		Detection Username	ruijie123		
		MAC Address Format	x0000000000 ~	0	
			Save		

 Table 4-22
 Server Global Configuration Parameters

Parameter	Description
Packet Retransmission Interval	Configure the interval during which the device sends a request to a RADIUS server before confirming that the RADIUS server is unreachable.
Packet Retransmission Count	Configure the number of times that the device sends requests to a RADIUS server before confirming that the RADIUS server is unreachable.
Server Detection	If this function is enabled, it is necessary to set the server detection cycle, server detection times, and server detection username. Determines the server status and whether to enable functions such as the escape function.
MAC Address Format	 Configure the format of the MAC address used in attribute 31 (Calling-Station-ID) of a RADIUS message. The following formats are supported: Dotted hexadecimal format. For example, 00d0.f8aa.bbcc. IETF format. For example: 00-D0-F8-AA-BB-CC. Unformatted (default). For example: 00d0f8aabbcc

4.25.3 Viewing Wireless User List

When the 802.1X feature is configured globally, and a client is authenticated and connected to the network in a wireless manner, you can view the client in the **Wireless User List**.

Choose Network-Wide > Workspace > Wireless > 802.1x Authentication > Wireless User List.

802.1x Authentication	RADIUS Server N	anagement Wir	eless User Lis	t	Wired User List				
<i>Description</i> The client going c	offline will not disappea	ar immediately. Instead	, the client will	l stay ir	n the list for a more	minutes.			
Wireless User Lis	it			Q	Search by ip/ma	c/Usernar	Refresh	↓ Batc	h Logout
Name	IP	MAC Address	Online Tin	ne	Online Duration	Connect S	SSID Acces	ss Name	Action
			No Da	ita					
	/page \vee								Total 0

Click Refresh to view the latest user list.

If you want to disconnect a user from the network, select the user and click **Logout** under the **Action** column. You can also select multiple users and click **Batch Logout** to disconnect selected users.

4.25.4 Viewing Wired User List

When the 802.1X feature is configured globally, and a client is authenticated and connected to the network in a wired manner, you can view the client in the **Wired User List**.

Choose Network-Wide > Workspace > Wireless > 802.1x Authentication > Wired User List.

802.1x Authen	tication	RADIUS Serve	er Management	Wireless L	Jser List	Wired	User List			
Wired Us	er List				Q	Search b	y mac	Refresh	↓ Batch Logout	
Use	ername	Status	Interface	MAC Address	Onli	ine Time	Online Duration	Access Name	Action	
					No Data	a				
< 1	> 10/pa	age \vee							Total 0	

Click Refresh to view the latest user list.

If you want to disconnect a user from the network, select the user and click **Logout** under the **Action** column. You can also select multiple users and click **Batch Logout** to disconnect selected users.

5 Network Settings

🚺 Note

This chapter takes the currently logged in device as an example to describe the entry of each function setting page. If you need to configure other devices in the network, please refer to the following path to enter the configuration page of the corresponding device, and then configure the function. For RG-RAP62: Click <u>3.3</u> <u>Managing Network Devices</u>.

5.1 Switching Work Mode

5.1.1 Work Mode

See 2.4 Work Mode for details.

5.1.2 Self-Organizing Network Discovery

When setting the work mode, you can set whether to enable the self-organizing network discovery function. This function is enabled by default.

After the self-organizing network discovery function is enabled, the device can be discovered in the network and discover other devices in the network. Devices network with each other based on the device status and synchronize global configuration. You can log in to the Web management page of any device in the network to check information about all devices in the network. After this function is enabled, clients can maintain and manage the current network more efficiently. You are advised to keep this function enabled.

If the self-organizing network discovery function is disabled, the device will not be discovered in the network and it runs in local device mode. After logging in to the Web page, you can configure and manage only the currently logged in device. If only one device is configured or global configuration does not need to be synchronized to the device, you can disable the self-organizing network discovery function.

5.1.3 Configuration Steps

🚺 Note

If you need to switch the work mode to wireless bridging mode, please see <u>5.5.2 Wireless Repeater</u> for details.

Go to the configuration page:

- Method 1: Choose One-Device. Click the device model.
- Method 2: Choose Network-Wide > Devices > AP. Select the target device in the list and click Manage.

Click the current work mode to change the work mode.

Configuration Guide

Ruíjie IRcycc				۵ Aler	rt Center 🛛 🛛 English 🗸 🛛 Exit
One-Device	•	AP 2 MGMT IP:192	MAC Address: 80:0	:45 Working Mode: AP	() Reboot
Network-Wide)	SN:G1N4 J0379	Reyee OS	Hardware Version:1.	00
Devices			• Normal		
 Clients System 			LED: AP Location:	LED blinking	
٠	Clients 5G Connected: 0 Capacity: 110 Total Connected: 0 Capacity: 1	10	SSID ≈ @Ruijiewada 2,4G 5G	Band 2.4G 5G Channel Auto Cha Transmit Power Auto Transmit Power Auto	nnel Auto Ismit Power Auto
	Username	SSID and Band	Signal Quality IP/MAC	Negotiation Rate	Online Duration \Rightarrow
			No Data		
				Total 0 <	1 > 10/page >

AC function switch: If a device works in the router mode and the self-organizing network discovery function is enabled, you can enable or disable the AC function. After the AC function is enabled, the device in the 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 self-organizing network mode and then manage downlink devices.

Working Mode		×
Description:		
1. The device IP address may	y change upon mode change	2.
2. Change the endpoint IP a	ddress and ping the device.	
 Enter the new IP address in browser to access Eweb. 	into the address bar of the	
4. The system menu varies v	vith different work modes.	
Working Mode ⑦	Router ~	
Self-Organizing Network ⑦		
AC (?)		
	Cancel	e

🛕 Caution

After the self-organizing network discovery is enabled, you can check the role of the device in self-organizing network mode.

5.2 Configuring Internet Connection Type (IPv4)

Go to the configuration page:

- Method 1: Choose One-Device > Config > Network > WLAN > WAN.
- Method 2: Choose Network-Wide > Workspace > Wired > WAN > WAN.

Select the Internet connection type after confirming with the ISP. For detailed configuration, see <u>2.5</u> <u>Configuration Wizard (Router Mode)</u>. After completing the configuration, click **Save**.

WAN	WAN_v6 Set	ttings
	* Internet 🕐	DHCP
		Username and password are not required.
	IP Address	192.168.110.65
	Subnet Mask	255.255.255.0
	Gateway	192.168.110.1
	DNS Server	192.168.110.1
I	Dedicated DNS	Optional
	Server 🕐	
		Advanced Settings
	VLAN ID	Enter a VLAN ID in the range of 2-23
	* MTU (?)	1500
* N	1AC Address 💮	48:81:d4:eb:6c:e3
		Save

The device supports the following Internet connection types:

- **PPPoE**: This Internet connection type is supported only when the device works in routing mode. You need to manually configure the PPPoE username and password.
- **DHCP**: The current device will act as a DHCP client and apply for the IPv4 address/prefix from the upstream network device.
- Static IP: If this Internet connection type is selected, you need to manually configure a static IPv4 address, subnet mask, gateway address, and DNS server.

5.3 Configuring Internet Connection Type (IPv6)

A Caution

- This function is supported when the device works in AP mode.
- Before configuring this feature, ensure that Hardware Acceleration is disabled.

Go to the configuration page:

- Method 1: Choose One-Device > Config > Network > WLAN > WAN_V6 Settings.
- Method 2: Choose Network-Wide > Workspace > Wired > WAN > WAN_V6 Settings.

Select the Internet connection type after confirming with the ISP. After completing the configuration, click Save.

tings	
Null	^
DHCP	
Static IP	
Null	
Save	
	Null DHCP Static IP Null Save

The device supports the following Internet connection types:

- **DHCP**: The current device will act as a DHCPv6 client and apply for the IPv6 address/prefix from the upstream network device.
- Static IP: If this Internet connection type is selected, you need to manually configure a static IPv6 address, gateway address, and DNS server.
- **Null**: The IPv6 function is disabled on the current WAN port.

5.4 Configuring LAN Port

A Caution

This function is supported when the device works in router mode.

Go to the configuration page:

- Method 1: Choose One-Device > Config > Network > LAN > LAN Settings.
- Method 2: Choose Network-Wide > Workspace > Wired > LAN > LAN Settings.

Click **Edit**. In the displayed dialog box, enter the IP address and subnet mask, and click **OK**. Change the IP address of the LAN port. Enter the new IP address in the browser and log in to the device again to configure and manage the device.

LAN S	ettings							+ Add	Delete Selected
	IP Address 🕐	Subnet Mask	VLAN ID 🕐	Remarks	DHCP Server ?	Start IP Address ⑦	IP Count ③	Lease Time (Min) ⑦	Action
	192.168.110.1	255.255.255.0	Default VLAN	-	Enabled	192.168.110.1	254	30	Edit Delete
	192.168.2.1	255.255.255.0	2	-	Enabled	192.168.2.1	254	30	Edit Delete
Up to 8	entries can be add	ed.							
Edit					×				
				_					
	* IP Addre	ss 192.168.1	10.1						
	* Subnet Ma	sk 255.255.2	255.0						
	Remar	cs Remarks							
	MAC Addres	30:0d:9e:0	d0:de:01						
	DHCP Serv	er							
				Cancel	ОК				

Table 5-1 LAN Settings

Parameter	Description
IP Address	Default gateway for devices connected to the Internet through this LAN.
Subnet Mask	Subnet mask of devices on the LAN.
VLAN ID	VLAN ID.
Remarks	VLAN description.
DHCP Server	After this function is enabled, devices on the LAN can automatically obtain the IP address. You need to configure the start IP address, IP count and lease time, as well as DHCP server options. For details, see <u>5.9 Configuring DHCP Server</u>
Start IP Address	Start IP address that a DHCP server automatically assigns to clients. The start IP address must be within the network segment calculated based on the IP address and subnet mask.
IP Count	The number of assignable IP addresses depends on the LAN segment and the start IP address.

Parameter	Description
Lease Time (Min)	Lease time of the automatically assigned IP addresses. When the lease time expires, devices on the LAN will obtain IP addresses again.

5.5 Configuring Repeater Mode

5.5.1 Wired Repeater

Choose One-Device. Click the device mode, and then choose Config > Network > Work Mode.

Connect a network cable from the WAN port (uplink LAN port) of the device to the upper-layer device.

Select **Access Point**, click **Check**, confirm the Wi-Fi settings of the AP, and then click **Save** to expand the network coverage.

A Caution

After the configuration is saved, connected clients will be disconnected from the network for a short period of time. You can reconnect the clients to the Wi-Fi network for restoration.

The device is working i	n Access Point mode.
O Router	Access Point OWireless Repeater
This mode allow Cable Connection Tip: The local ro	rs you to establish a wired connection between a primary router and a secondary router, extending network coverage. on: Please connect the WAN port of the local router to the LAN port of the primary router. uter is a secondary router. The local router Wi-Fi is managed by the primary router.
Access Point	
Status	Enabled
IP Address	192.168.110.45
Subnet Mask	255.255.255.0
DNS Server	192.168.110.1
	Edit

5.5.2 Wireless Repeater

The wireless repeater mode extends the Wi-Fi coverage range of the primary device. The device supports the dual-link wireless repeater mode and can extend both 2.4 GHz and 5 GHz signals of the primary device.

🚺 Note

- To avoid loops in wireless repeater mode, remove the network cable from the WAN port.
- Obtain the Wi-Fi name and Wi-Fi password of the upper-layer router.

Choose One-Device. Click the device mode, and then choose Config > Network > Work Mode.

Click **Wireless Repeater** and then click **Select**. A list of surrounding Wi-Fi signals pops up. A list of nearby 5 GHz Wi-Fi networks is displayed by default. You can switch from 5 GHz to 2.4 GHz band by selecting **2.4G** from the drop-down list box. You are advised to select a strong 5 GHz Wi-Fi network signal.

uter Acce	ess Point • Wireless	Repeater				
 This mode allows You are advised to You dia a dia di	you to establish a wireless o o select a 5G Wi-Fi of the pri ess repeater is not allowed t	connection betwee imary device for b to be configured.	en the primary de etter Internet exp	vice and the local devi perience.	ce that works as the se	condary device, extending netwo
ess Repeater						
rimary Device						
* SSID S	Select					
					×	
Wi-Fi List S	elect a target W	i-Fi.				
SSID	5G	~ R	e-scan			
SSID	BSSID	Security	Channe I	RSSI	MLO	
SSID @Ruijie-	BSSID	Security	Channe I	RSSI -17 dBm	MLO Not	
SSID @Ruijie- D2CE_plus_5G	BSSID 4a:81:d4:9b:6c:e5	Security	Channe I 36	RSSI -17 dBm High	MLO Not supported	
SSID @Ruijie- D2CE_plus_5G @Ruijie-	BSSID 4a:81:d4:9b:6c:e5	Security OPEN	Channe I 36	RSSI -17 dBm High -27 dBm	MLO Not supported	
SSID @Ruijie- D2CE_plus_5G @Ruijie- D2CE_plus_5G	BSSID 4a:81:d4:9b:6c:e5 c6:70:ab:18:71:39	Security OPEN OPEN	Channe I 36 36	RSSI -17 dBm High -27 dBm High	MLO Not supported Not supported	
SSID @Ruijie- D2CE_plus_5G @Ruijie- D2CE_plus_5G	BSSID 4a:81:d4:9b:6c:e5 c6:70:ab:18:71:39	Security OPEN OPEN	Channe I 36 36	RSSI -17 dBm High -27 dBm High	MLO Not supported Not supported	
SSID @Ruijie- D2CE_plus_5G @Ruijie- D2CE_plus_5G rj-network	BSSID 4a:81:d4:9b:6c:e5 c6:70:ab:18:71:39 f2:82:3d:b9:3b:01	Security OPEN OPEN WPA2PSK	Channe I 36 36	RSSI -17 dBm High -27 dBm High	MLO Not supported Not supported	
SSID @Ruijie- D2CE_plus_5G @Ruijie- D2CE_plus_5G rj-network	BSSID 4a:81:d4:9b:6c:e5 c6:70:ab:18:71:39 f2:82:3d:b9:3b:01	Security OPEN OPEN WPA2PSK	Channe I 36 36 36 36	RSSI -17 dBm High -27 dBm High -78 dBm Low	MLO Not supported Not supported	
SSID @Ruijie- D2CE_plus_5G @Ruijie- D2CE_plus_5G rj-network ruijie-guest	BSSID 4a:81:d4:9b:6c:e5 c6:70:ab:18:71:39 f2:82:3d:b9:3b:01 f2:82:3d:b9:3b:02	Security OPEN OPEN WPA2PSK OPEN	Channe I 36 36 36	RSSI -17 dBm High -27 dBm High -78 dBm Low	Not supported Not supported Not supported Not supported Not Supported	
SSID @Ruijie- D2CE_plus_5G @Ruijie- D2CE_plus_5G rj-network ruijie-guest	BSSID 4a:81:d4:9b:6c:e5 c6:70:ab:18:71:39 f2:82:3d:b9:3b:01 f2:82:3d:b9:3b:02	Security OPEN OPEN WPA2PSK OPEN	Channe I 36 36 36	-17 dBm -17 dBm -27 dBm -27 dBm -27 dBm -28 dBm Low	Not Supported Not supported Not supported Not supported	

- (1) Select the Wi-Fi signal of the upper-layer device that you want to extend. The configuration items of the local device are displayed. If the signal of the upper-layer device is encrypted, enter the Wi-Fi password of the upper-layer device.
- (2) Configure Local Router Wi-Fi. You can select New Wi-Fi or Same as Primary Router Wi-Fi.
 - If you select Same as Primary Router Wi-Fi, the Wi-Fi settings of the router are automatically synchronized with those on the primary router. Generally, clients merge Wi-Fi signals with the same name into one Wi-Fi signal, and they can search out only the Wi-Fi signal of the primary router.

The device is working in Access Point mode.
Router Access Point Wireless Repeater
 This mode allows you to establish a wireless connection between the primary device and the local device that works as the secondary device, extending network coverage. You are advised to select a 5G Wi-Fi of the primary device for better Internet experience. To avoid loops, wireless repeater is not allowed to be configured.
Wireless Repeater
Primary Device
* SSID rj-network Select
* Wi-Fi Password
Local Device
Local Router Wi-Fi 💫 New Wi-Fi 💿 Same as Primary Router Wi-Fi
Save
o If New Wi-Fi is selected, you can set a local Wi-Fi name and password. Clients will search out differen
Wi-Fi signals.
The device is working in Access Point mode.
Router Access Point Image: Construction of the second secon
 This mode allows you to establish a wireless connection between the primary device and the local device that works as the secondary device, extending network coverage. You are advised to select a 5G Wi-Fi of the primary device for better Internet experience. To avoid loops, wireless repeater is not allowed to be configured.
Wireless Repeater
Primary Device
* SSID rj-network Select
* Wi-Fi Password
Local Device
Local Router Wi-Fi 🔹 New Wi-Fi 💦 Same as Primary Router Wi-Fi
* SSID(2.4G) rj-network_plus
* SSID(5G) rj-network_plus_5G
Wi-Fi Password A blank value indicates no annuntion

🛕 Caution

- After the configuration is saved, the AP will be disconnected from the Wi-Fi network and needs to connect to the new Wi-Fi network. Exercise caution when performing this operation. Record the new Wi-Fi name and password.
- You are advised to install the AP in a position where the RSSI is greater than two bars of signal to prevent signal loss. If the signal at the installation position is too weak, the Wi-Fi extension may fail or the quality of extended signal may be poor.

5.6 Creating a VLAN

A Caution

This function is supported when the device works in router mode.

Go to the configuration page:

- Method 1: Choose One-Device > Config > Network > LAN > LAN Settings.
- Method 2: Choose Network-Wide > Workspace > Wired > LAN > LAN Settings.

A LAN can be classified into multiple VLANs. Click Add to create a VLAN.

AN Settings							+ Add	🗇 Delete Selecte
IP Address ⑦ Subn	et Mask ⑦	VLAN ID 🕐	Remarks	DHCP Server ⑦	Start IP Address ⑦	IP Count ⑦	Lease Time (Min) ⑦	Action
192.168.120.1 255.2	255.255.0	Default VLAN	-	Enabled	192.168.120.1	254	30	Edit Delete
o to 8 entries can be added.								
Add				×				
* IP Address								
* Subnet Mask	255.25	55.255.0						
* VLAN ID								
Remarks	Rema	rks						
MAC Address	E0:5D	:54:1A:C7:95						
DHCP Server								

Table 5-2 VLAN Configuration Parameters

Parameter	Description
IP Address	IP address of the VLAN interface. The default gateway of devices that access the Internet through the current LAN should be set to this IP address.
Subnet Mask	Subnet mask of the IP address of the VLAN interface.
VLAN ID	VLAN ID.
Remark	VLAN description.
MAC Address	MAC address of the VLAN interface.

Parameter	Description
	Enable the DHCP server function. After it is enabled, devices on the LAN can automatically
	obtain IP addresses. After the DHCP service is enabled, you need to configure the start IP
DHCP Server	address to be assigned, number of IP addresses to be assigned, and address lease term
	for the DHCP server, and other DHCP server options. For details, see <u>5.9 Configuring</u>
	DHCP Server.

🛕 Caution

VLAN configuration is associated with the configuration of the uplink device. Therefore, refer to the configuration of the uplink device when configuring a VLAN.

5.7 Changing MAC Address

Go to the configuration page:

- Method 1: Choose One-Device > Config > Network > WAN > WAN.
- Method 2: Choose Network-Wide > Workspace > Wired > WAN > WAN.

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

Click to expand **Advanced Settings**, enter the MAC address, and click **Save**. You do not need to change the default MAC address unless in special cases.

In the router mode, change the MAC address of the LAN port on LAN > LAN Settings.

🛕 Caution

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.

/	Advanced Settings
VLAN ID	Enter a VLAN ID in the range of 2-23
* MTU (?)	1500
* MAC Address (?)	10:82:3d:58:11:e8
	Save

5.8 Changing MTU

Go to the configuration page:

• Method 1: Choose One-Device > Config > Network > WAN > WAN.

Method 2: Choose Network-Wide > Workspace > Wired > WAN > WAN.

WAN interface MTU indicates the maximum transmission unit (MTU) allowed by the WAN interface. The default value is 1500 bytes, indicating the maximum data forwarding efficiency. Sometimes, ISP networks restrict the speed of large data packets or forbid large data packets from passing through. As a result, the network speed is unsatisfactory or even the network is disconnected. In this case, you can set the MTU value to a smaller value.

····· /	Advanced Settings
VLAN ID	Enter a VLAN ID in the range of 2-23
* MTU	1500
* MAC Address (?)	10:82:3d:58:11:e8
	Save

5.9 Configuring DHCP Server

A Caution

This function is supported when the device works in router mode.

5.9.1 DHCP Server

In the router mode, the DHCP server function can be enabled on the device to automatically assign IP addresses to clients so that clients connected to the LAN ports or Wi-Fi network of the device obtain IP addresses for Internet access.

5.9.2 Configuring the DHCP Server Function

Go to the configuration page:

- Method 1: Choose One-Device > Config > Network > LAN > LAN Settings.
- Method 2: Choose Network-Wide > Workspace > Wired > LAN > LAN Settings.

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

🛕 Caution

If the DHCP server function is disabled on all devices in the 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.

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 term. 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 term expires. After the client connection is restored, the client can request an IP address again. The default lease term is 30 minutes.

 \times

Add

* IP Address		
* Subnet Mask	255.255.255.0	
* VLAN ID		
Remarks	Remarks	
MAC Address	E0:5D:54:DB:09:D1	
DHCP Server		
* Start IP Address		
* IP Count	254	
* Lease Time (Min)	30	
* Lease Time (Min)	30	

5.9.3 Displaying Online DHCP Clients

Go to the configuration page:

- Method 1: Choose One-Device > Config > Network > LAN > DHCP Clients.
- Method 2: Choose Network-Wide > Workspace > Wired > LAN > DHCP Clients.

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.

Configuration Guide

LAN Se	ttings	DHCP Clients Static IP A	Addresses				
DHCP	Clients			Search	by Hostname/IP Address/	Q C Refree	sh + Batch Add
	No.	Device Name	IP Address	MAC Address	Remaining Lease Tir	me(min)	Status
	1	nova G- f5a 97	192.168.120.172	42:11:26:	23	Co	nvert to Static IP
Up to 3	300 static	binding entries are supported.			Тс	otal 0 < 1	> 10/page >

5.9.4 Displaying the DHCP Static IP Address List

Go to the configuration page:

- Method 1: Choose One-Device > Config > Network > LAN > Static IP Addresses.
- Method 2: Choose Network-Wide > Workspace > Wired > LAN > Static IP Addresses.

Click **Add**. In the displayed static IP address binding dialog box, 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.

No. Device Name IP Address MAC Address Action	atic IP Address List		Batch Import Batch Expor	t + Add 🗇 Delete Selected	Search by IP Address/MAC Addre
In Data Total 0 < 1 > 10/page Id × Device Name ③ Optional * IP Address Example: 1.1.1.1 * MAC Address Example: 00:11:22:33:44:55	No.	Device Name	IP Address	MAC Address	Action
p to 300 entries can be added. Total 0 < 1 > 10/page d × Device Name ③ Optional * IP Address Example: 1.1.1.1 * MAC Address Example: 00:11:22:33:44:55			No Data		
d × Device Name ③ Optional * IP Address Example: 1.1.1.1 * MAC Address Example: 00:11:22:33:44:55	p to 300 entries can be ac	lded.			Total 0 < 1 > 10/page
Device Name ③ Optional * IP Address Example: 1.1.1.1 * MAC Address Example: 00:11:22:33:44:55					
Id × Device Name ③ Optional * IP Address Example: 1.1.1.1 * MAC Address Example: 00:11:22:33:44:55					
Device Name ⑦ Optional * IP Address Example: 1.1.1.1 * MAC Addresss Example: 00:11:22:33:44:55	ld		×		
* IP Address Example: 1.1.1.1 * MAC Address Example: 00:11:22:33:44:55	Davica Nama @	Ontional			
* IP Address Example: 1.1.1.1 * MAC Address Example: 00:11:22:33:44:55		Optional			
* MAC Address Example: 00:11:22:33:44:55	* IP Address	Example: 1.1.1.1			
	* MAC Address	Example: 00:11:22:3	3:44:55		
			Cancel		

5.10 Configuring DNS

Choose One-Device > Config > 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 from region to region. You can consult the local ISP.

i The local DNS ser	rver 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.	
	Save	

5.11 Configuring Self-Healing Mesh

Choose One-Device > Config > Advanced > Self-Healing Mesh.

After Reyee Mesh is enabled, Self-Healing Mesh is automatically switched to Wireless Repeater mode to ensure normal service operation if a fault occurs on the wired link.

After Reyee Mesh is enabled, Self-Healing Mesh is automatically switched to Wireless Repeater mode to ensure normal service operation if a fault occurs on the wired link.
Enable
Save

5.12 Hardware Acceleration

Choose One-Device > Config > Advanced > Hardware Acceleration.

After Hardware acceleration is enabled, the Internet access speed will be improved. Hardware Acceleration is enabled on the device by default.

i After Hardware A	cceleration is enabled, th	he Internet access speed will be improved and clients will not be rate-limited.
Enable		
	Save	

🛕 Caution

Hardware Acceleration and IPv6 are mutually exclusive.

- When the device is in router mode: Ensure that IPv6 is disabled. (For IPv6 settings, see <u>5.16 IPv6</u> <u>Settings</u>).
- When the device is in AP mode: Ensure that the internet connection type in WAN_V6 settings is "Null" (for WAN_V6 settings, see <u>5.3</u> Configuring Internet Connection Type (IPv6)).

5.13 Configuring Port Flow Control

Choose One-Device > Config > Advanced > Port Settings.

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

<i>i</i> Port flow control can relieve the data congestion caused by ports at different speeds and improve the network speed.						
Enable						
Save						

5.14 Configuring ARP Binding

🛕 Caution

This function is supported when the device works in router mode.

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.

Choose One-Device > Config > Security > ARP List.

ARP mappings can be bound in two ways:

(1) 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.

ARP List 🖯			Search by IP Address/MAC Addr	Q + Add Ø Bind Selected	Delete Selected
No.	Device Name	MAC Address	IP Address	Туре	Action
1	Click to edit 🖉	30:0d:9e:d0:de:01	192.168.110.1	Dynamic	
Up to 256 entries can be added.				Total 1 < 1	> 10/page >

(2) 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			×
Device Name 🕐	Optional		
* IP Address	Enter or select an IP address.		
* MAC Address	Enter or select a MAC address.		
	Can	cel	ОК

5.15 Configuring LAN Ports

🛕 Caution

The configuration takes effect only on APs having wired LAN ports.

Choose Network-Wide > Workspace > Wireless > LAN Ports.

Enter the VLAN ID and click **Save** to configure the VLAN, to which the AP wired ports belong. If the VLAN ID is null, the wired ports and WAN port belong to the same VLAN.

 This profile takes effect only on APs with wired LAN ports, and is subject to the actual device. For example, the AP wired port profile takes effect on the RG-EAP101 AP. Note: This profile takes effect on APs on the AP Wired Port Profile List. The AP Wired Profile Default Profile takes effect on other APs on the network. 								
Default Settings								
	VLAN ID		Add VLAN					
		(Range: 2-232, 234-4090. If this fie VLAN corresponding to the WAN	eld is left blank, it indicates that the port is used.)					
	Apply to	APs not on the AP Wired Port Prof	file List 🕖					
LAN Port	Settings			+ Add	Delete Selected			
	VLAN	D \$	Apply to		Action			
			No Data					

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

In self-organizing network mode, the AP wired port configuration applies to all APs having wired LAN ports on the current network. The configuration applied to APs in **LAN Port Settings** takes effect preferentially. Click **Add** to add the AP wired port configuration. For APs, to which no configuration is applied in **LAN Port Settings**, the default configuration of the AP wired ports will take effect on them.
Configuration Guide

This profile takes effect takes effect on the RG-E Note: This profile takes the network.	only on APs with wired LAN ports, and is subject to the actual device. For example, the A EAP101 AP. effect on APs on the AP Wired Port Profile List. The AP Wired Profile Default Profile takes	P wired port profile effect on other APs on
Default Settings		
VLAN ID	Add VLAN	
(Range VLAN	e: 2-232, 234-4090. If this field is left blank, it indicates that the corresponding to the WAN port is used.)	
Apply to APs no	ot on the AP Wired Port Profile List 🕖	
LAN Port Settings	+ Ac	Id 🗇 Delete Selected
VLAN ID ≑	Apply to	Action
	No Data	
Up to 8 VLAN IDs or 32 APs ca	an be added (0 APs have been added).	

5.16 IPv6 Settings

🛕 Caution

- This function is supported when the device works in router mode.
- Before configuring this feature, ensure that Hardware Acceleration is disabled.

5.16.1 Overview

Internet Protocol Version 6 (IPv6) is the next generation IP protocol designed by the Internet Engineering Task Force (IETF) to replace IPv4 and solve the IPv4 problems such as address depletion.

5.16.2 IPv6 Basic

1. IPv6 Address Format

IPv6 increases the length of the address from 32 bits in IPv4 to 128 bits, and therefore has a larger address space than IPv4.

The basic format of an IPv6 address is **X:X:X:X:X:X:X**. The 128-bit IPv6 address is divided into eight 16-bit sections that are separated by colons (:), and 16 bits in each section are represented by four hexadecimal characters (0–9 and A–F). Each **X** represents a 4-character hexadecimal number.

For example: 2001:ABCD:1234:5678:AAAA:BBBB:1200:2100, 800:0:0:0:0:0:0:1, 1080:0:0:0:8:800:200C:417A

The number **0** in the IPv6 address can be abbreviated as follows:

- The starting 0s can be omitted. For example, 2001:00CD:0034:0078:000A:000B:1200:2100 can be written as 2001:CD:34:78:A:B:1200:2100.
- Consecutive 0s can be replaced by two colons (::). For example, **800:0:0:0:0:0:0:1** can be written as **800::1**. Consecutive 0s can be replaced by two colons only when the 16-bit section contains all 0s, and the two

colons can only appear once in the address.

2. IPv6 Prefix

An IPv6 address consists of two parts:

- Network prefix: It contains n bits, and is equivalent to the network ID in an IPv4 address.
- Interface identifier: It contains (128 n) bits, and is equivalent to the host ID in an IPv4 address.

The length of the network prefix is separated from the IPv6 address by a slash (/). For example, **12AB::CD30:0:0:0/60** indicates that the length of the prefix used for routing in the address is 60 bits.

3. Special IPv6 Address

There are also some special IPv6 addresses, for example:

fe80::/8 is a link local address, and equivalent to 169.254.0.0/16 in IPv4.

fc00::/7 is a local address, and similar to 10.0.0.0/8, 172.16.0.0/16, or 192.168.0.0/16 in IPv4.

ff00::/12 is a multicast address, and similar to 224.0.0.0/8 in IPv4.

4. N/AT66

IPv6-to-IPv6 Network Address Translation (N/AT66) is the process of converting the IPv6 address in an IPv6 packet header to another IPv6 address. N/AT66 prefix translation is an implementation of N/AT66. It replaces the IPv6 address prefix in the packet header with another IPv6 address prefix to achieve IPv6 address translation. N/AT66 can realize mutual access between an intranet and Internet.

5.16.3 IPv6 Address Assignment Methods

- Manual configuration: The IPv6 address/prefix and other network configuration parameters are manually configured.
- Stateless Address Autoconfiguration (SLAAC): The link local address is generated based on the interface ID, and then the local address is automatically configured based on the prefix information contained in the route advertisement packet.
- Stateful address autoconfiguration, that is, DHCPv6: DHCPv6 is divided into the following two types:
 - DHCPv6 autoconfiguration: The DHCPv6 server automatically configures the IPv6 address/prefix and other network configuration parameters.
 - DHCPv6 Prefix Delegation (PD): The lower-layer network device sends a prefix allocation application to the upper-layer network device. The upper-layer network device assigns an appropriate address prefix to the lower-layer device. The lower-layer device automatically subdivides the obtained prefix (generally less than 64 bits in length) into subnet segments with 64-bit prefix length, and then advertises the subdivided address prefixes to the user link directly connected to the IPv6 host through the route to realize automatic address configuration of the host.

5.16.4 Enabling IPv6

Choose One-Device > Config > Network > IPv6 Address.

Click Enable, and then click OK in the dialog box that appears to enable IPv6.

Enable ⑦		
	Tinc	٦
	Are you sure you want to enable IPv6 address?	
	Cancel	
		<u>'</u>

After IPv6 is enabled, you can configure the IPv6 addresses of WAN and LAN ports, view the DHCPv6 client, and configure a static DHCPv6 address for the client.

Enabl	e 🕐 💽		
WAN Settings	LAN Settings	DHCPv6 Clients	Static DHCPv6
* Inte	ernet DHCP/PPI	PoE	~
IPv6 Add	lress		
IPv6 P	refix		
Gate	eway		
DNS Se	erver		
NAT6	6 @		
	Sa	ave	

5.16.5 Configuring the IPv6 Address for the WAN Port

Choose One-Device > Config > Network > IPv6 Address > WAN Settings.

Configure the IPv6 address for the WAN port, and click Save.

WAN Settings LAN	N Settings DHCPv	6 Clients	Static DHCPv6
* Internet	DHCP/PPPoE		^
IPv6 Address	DHCP/PPPoE		
IPv6 Prefix	Static IP Null		
Gateway			
DNS Server			
NAT66 ⑦			
	Save		

Parameter	Description
Internet	 Specify the method for obtaining an IPv6 address for the WAN port. DHCP/PPPoE: The current device will act as a DHCPv6 client and apply for the IPv6 address/prefix from the upstream network device. Static IP: If this Internet connection type is selected, you need to manually configure a static IPv6 address, gateway address, and DNS server. Null: The IPv6 function is disabled on the current WAN port.
IPv6 Address	If Internet is set to DHCP/PPPoE , the automatically obtained IPv6 address is displayed. If Internet is set to Static IP , you need to manually configure this parameter.
IPv6 Prefix	If Internet is set to DHCP/PPPoE and the current device obtains the IPv6 address prefix from the upstream device. The obtained IPv6 address prefix is displayed.
Gateway	If Internet is set to DHCP/PPPoE , the automatically obtained gateway address is displayed. If Internet is set to Static IP , you need to manually configure this parameter.
DNS Server	If Internet is set to DHCP/PPPoE , the automatically obtained DNS server address is displayed. If Internet is set to Static IP , you need to manually configure this parameter.

Description
If the current device cannot access the Internet in DHCP mode or
cannot obtain the IPv6 address prefix, you must enable N/AT66 to
assign the IPv6 address to an intranet client.

5.16.6 Configuring the IPv6 Address for the LAN Port

Choose One-Device > Config > Network > IPv6 Address > LAN Settings.

When the device accesses the network in DHCP mode, the upstream device can assign an IPv6 address to the LAN port, and assign IPv6 addresses to the clients in the LAN based on the IPv6 address prefix. If the upstream device cannot assign an IPv6 address prefix to the current device, you need to manually configure an IPv6 address prefix for the LAN port, and assign IPv6 addresses to the clients in the LAN by enabling the N/AT66 function (see <u>5.16.5</u> <u>Configuring the IPv6 Address for the WAN Port</u>).

	Enable 🕐 👥						
WAN Settin	gs LAN Settings	DHCPv6 Clients S	tatic DHCPv6				
LAN Sett	ings 🕐					+ Add 🗇 De	lete Selected
	VLAN ID	IPv6 Assignment	Subnet Prefix Name	Subnet ID	Subnet Prefix Length	IPv6 Address/Prefix Length	Action
	Default	Auto		0	64		Edit Delete
Up to 8 enti	ries can be added.						

Click Edit corresponding to the default VLAN, and fill in a local address of no more than 64 bits in the IPv6 Address/Prefix Length column. This address will also be used as the IPv6 address prefix.

IPv6 Assignment specifies the method for assigning IPv6 addresses for clients. The following options are available:

- Auto: Both DHCPv6 and SLAAC are used to assign IPv6 addresses to clients.
- DHCPv6: DHCPv6 is used to assign IPv6 addresses to clients.
- SLAAC: SLAAC is used to assign IPv6 addresses to clients.
- Null: No IPv6 addresses are assigned to clients.

The setting of **IPv6 Assignment** is determined by the protocol supported by intranet clients. If you are not sure about the protocol supported by intranet clients, select **Auto**.

Edit			×
IPv6 Assignment ⑦	Auto	^	
IPv6 Address/Prefix	Auto		
Length 🕐	DHCPv6		
	SLAAC		
	Null		
		Cancel	ОК

You can click Advanced Settings to configure more address attributes.

Add		
* VLAN ID	Select ~	
IPv6 Assignment ⑦	Auto ~	
IPv6 Address/Prefix	Example: 2000::1	
Length 🕐		
	Advanced Settings	
Subnet Prefix Name	Default \lor	
(?)		l
Subnet Prefix Length	64	
?		
Subnet ID 🕐	0	
* Lease Time (Min) ⑦	30	
DNS Server	Example: 2000::1, each separated by a comma.	

0

Cancel

 \times

Parameter	Description
Subnet Prefix Name	Configure the interface from which the prefix is obtained, for example, WAN_V6 . The default value is all interfaces.
Subnet Prefix Length	Configure the length of the subnet prefix. The value ranges from 48 to 64.
Subnet ID	Configure the subnet ID in hexadecimal notation. 0 indicates that the subnet ID automatically increments.
Lease Time (Min)	Configure the lease term of the IPv6 address. The unit is minutes.
DNS Server	Configure the address of the IPv6 DNS server.

Table 5-4 LAN Port IPv6 Address Configuration Parameters

5.16.7 Viewing DHCPv6 Clients

Choose One-Device > Config > Network > IPv6 Address > DHCPv6 Clients.

When the device acts as a DHCPv6 server to assign IPv6 addresses to clients, you can view information about the clients that obtain IPv6 addresses from the device on the current page. The information includes the host name, IPv6 address, remaining lease term, and DHCPv6 Unique Identifier (DUID) of each client.

Enter an IPv6 address or DUID in the search bar, and click to quickly find the information of the specified DHCPv6 client.

Enab	ole 🕐 👥					
WAN Settings	LAN Settings	DHCPv6 Clients	Static DHCPv6			
i You can vi	ew the DHCPv6 clie	nts information on th	iis page.			
DHCPv6 Clier	nts				Search by IPv6 Address/DUID	Q + Bind Selected
No.	Hostnam	e	IPv6 Address	Remaining Lease Time(min)	DUID	Status
				No Data		
					Total 0 <	1 > 10/page v

5.16.8 Configuring the Static DHCPv6 Address

Configure the IPv6 address statically bound to the DUID of a client so that the client can obtain the specified address each time.

Choose One-Device > Config > Network > IPv6 Address > Static DHCPv6.

Enable 🕐 💽							
WAN Settings LAN Settings	DHCPv6 Clients S	tatic DHCPv6					
Static IP Address List				Search by IPv6 Address/DUID	Q	+ Add	Delete Selected
No.	IPv6 Address		DUID			Action	
		No E	Data				
Up to 200 entries can be added.					Total () < 1	> 10/page >
(1) Click Add							
Add			2	<			
* IPv6 Addres	Example: 200	D::1					
* DUI	D Example: 0003	3000100d0f819685f					
		Cancel	OK				

- (2) Enter the IPv6 address and DUID of the client.
- (3) Click **OK**.

5.16.9 Configuring the IPv6 Neighbor List

In IPv6, Neighbor Discovery Protocol (NDP) is an important basic protocol. NDP replaces the ARP and ICMP route discovery protocols of IPv4, and supports the following functions: address resolution, neighbor status tracking, duplicate address detection, router discovery, and redirection.

Choose One-Device >	> Config >	Security >	IPv6 Neighbor	List.

IPv6 I	Veighbo	or List 🕒		Search by IP Address/MAC Addre	Q + Add Ø Bind Select	ed 🗇 Delete Selected
	No.	IPv6 Address	MAC Address	Туре	Ethernet status	Action
	1	fe80::84ee:eff:fe1c:9ca6	86:ee:0e:1c:9c:a6	Dynamic	LAN	@ Bind
	2	fe80::e25d:54ff:fe29:12f1	e0:5d:54:29:12:f1	Dynamic	WAN	∂ Bind
	3	fe80::9e8d:50ae:fd73:ac70	7c:a1:77:d0:5c:65	Dynamic	LAN	
Up to a	256 entrie	s can be added.			Total 3 <	1 > 10/page >

(1) Click Add and add the interface, IPv6 address and MAC address of the neighbor.

* Int	erface	Select	~
* IPv6 Ad	ddress	Please enter an IPv6 address.	
* MAC Ad	ddress	Please enter a MAC address.	

(2) Select the IPv6 neighbor list to be bound, and click **Bind** in the **Action** column to bind the IPv6 address and MAC address.

IPv6	Neighbo	or List		Search by IP Address/MAC Addre	Q + Add Ø Bind Selec	ted 🗇 Delete Selected
	No.	IPv6 Address	MAC Address	Туре	Ethernet status	Action
	1	fe80::84ee:eff:fe1c:9ca6	86:ee:0e:1c:9c:a6	Dynamic	LAN	
	2	fe80::e25d:54ff:fe29:12f1	e0:5d:54:29:12:f1	Dynamic	WAN	@ Bind
	3	fe80::9e8d:50ae:fd73:ac70	7c:a1:77:d0:5c:65	Dynamic	LAN	
Up to	256 entrie	es can be added.			Total 3 <	1 → 10/page ~

6 Online Client Management

🛕 Caution

- When the AP is used as the primary device, clients on the network are only displayed when the AP works in router mode.
- When the AP is used as a secondary device, the functions presented in the web interface are based on the primary device on the network.

Go to the configuration page:

- Choose Network-Wide > Clients.
- AP as a secondary device: Choose **One-Device** > **Config** > **Clients**.

The client list displays wired, wireless, and users not connected on the current network, including the username, connection mode, associated device, IP/MAC address, IP address binding status, rate, and related operations.

• AP as a secondary device.

Username	SSID and Band	Connected To	IP/MAC	Rate	Action
Click to edit $\&$	5G @@@@@zzzzzzzzzz	AP W 9	192.168.110.6 6? 1 a Not bound	↑ 0.00bps ↓ 0.00bps	Access Control Associate Block
M2102J2SC 🖉	56 @@@@@zzzzzzzzzz	AP V9	192.168.110.7 ε δ Not bound	↑ 571.00bps ↓ 1.35Kbps	Access Control Associate Block
DESKTOP-DTTUM8V 🖉	Wired LAN3/WAN1	eg205g	192.168.110.9 7 5 Not bound	↑ 0.00bps ↓ 475.00bps	Access Control
DESKTOP-IPV6G6R 🖉	Wired LAN1/WAN3	eg205g	192.168.110.14 c(4 Not bound	↑ 295.54Kbps ↓ 79.64Kbps	Access Control
zhuyihan 🖉	2.4G @@@@@zzzzzzzzzz	AP V 9	192.168.110.16	↑ 132.00bps↓ 43.00bps	Access Control Associate Block
				То	tal 5 < 1 > 10/page

Air (3) Writed (2)	vileless (1) User hot						Select 26 DIOCK	O BING IP	search by IP/MAC/Osemanie
The client going offlin	e will not disappear imn	nediately. Instead, the c	lient will stay in the list f	for 3 more minutes.					
Username	SSID and Band	Signal Quality 🗘	Connected To	IP/MAC	Rate	Negot Rate	iation Online Duration	LimitSpeed	Action
* 2	⇔ 5G ruiji e	-45db Channel:52	AP	192.168.110.9 6 ⁹ () Not bound	↑ 0.00bps ↓ 0.00bps	1080M	42 minutes 25 second	s No Limit	Access Control Associate Block
								Total 1	< 1 > 10/page >
AP as a primary device.									
 The client going of 	fline will not disappea	ar immediately. Instea	d, the client will stay i	in the list for 3 more minute	95.				
Username	SSID and Band	Signal Quality	Connected To	o IP/MAC		Negotiation Rate	Online Duration 🗘 🛛 L	imitSpeed	Action
*	⇔ 5G	-64db Channel:56	АР	0 0 0 0000 0	්? Not bound	288M	7 minutes 34 seconds	lo Limit	Associate Block
DESKTOP- O3SVIQ2	🗅 Wired -) ;	්? Not bound	-			-

Click Not Bound in the IP/MAC column to bind the client to a static IP address.

Click a button in the Action column to perform the corresponding operation on the online client.

- Wired: Only access control can be configured.
- Wireless: Access control, associate, and block can be configured.
- User not connected: Only the delete action is supported.

Note

- Client IP binding is only supported when the AP works in router mode.
- Access Control is not supported on AP devices . However, when there are devices on the network that support the Access Control function, you can configure this feature globally.

Parameter	Description						
Username	Name of the connected client.						
SSID and Band	Indicates the access mode of the client, which can be wireless or wired. The SSID and frequency band is displayed when a client is connected wirelessly.						
	The Wi-Fi signal strength of the client and the associated channel.						
Signal Quality	1 Note						
	This information is displayed only in the wireless online client list.						
Connected To	Indicates wired or wireless connection, the associated device and SN.						
IP/MAC	Indicates the IP address and MAC address of the client.						
Rate	Indicates the uplink and downlink rates of the client.						
	Negotiation rate between the client and the AP.						
Negotiated Rate	1 Note						
	This information is displayed only in the wireless online client list.						
	Client access duration.						
Online Duration	1 Note						
	This information is displayed only in the wireless online client list.						
	Implement wireless speed limiting for clients to prevent certain clients from						
	consuming large amounts of bandwidth resources. For details, see <u>6.5</u>						
LimitSpeed							
	This information is displayed only in the wireless online client list.						

Table 6-1 Online Client Management Configuration Parameters

Parameter	Description
Action	You can click the corresponding button to perform access control, association, and block operations on online clients.

Wired Clients

Click the Wired tab to see details about wired clients.

All (24) Wired (23) Wi	ireless (1) User not connecte	d (6) 🖸		Select & Block	⇒ Bind IP Search by IP/MAC/Username Q
The client going offline wi	ill not disappear immediately. Ins	tead, the client will stay in the list i	for 3 more minutes.		
Username	SSID and Band	Connected To	IP/MAC	Rate	Action
Click to edit 🌊	🗅 Wired Gi1/18	NBS6000	192.168.120.1 6 ^{.9} Not bound	 ↑ 0.00bps ↓ 0.00bps 	Access Control
PC-4277ac 🖉	🗅 Wired Gi1/21	NBS60001	192.168.110.3 30 ac Bound	 ↑ 40.18Kbps ↓ 21.28Kbps 	Access Control

Wireless Clients

Click the Wireless tab to see details about wireless clients.

All (4) Wired (1)	Wireless (3) User no	t connected (0) O					Select & Block	Bind IP	Search by IP/MAC/Username Q
The client going offlir	ne will not disappear im	mediately. Instead, the	client will stay in the lis	t for 3 more minutes.					
Username	SSID and Band	Signal Quality ≑	Connected To	IP/MAC	Rate	Negotiation Rate	Online Duration 🗘	LimitSpeed	Action
* 0_	5G @@@@@#222222222	-42db Channel:149	AP 89	192.168.110.6 6 ⁻⁹ 1. 3 Not bound	† 0.00bps ↓ 0.00bps	866M	44 minutes 47 seconds	No Limit	Access Control Associate Block
M2102J2SC 🖉	56 @@@@@################################	-33db Channel:149	AP W ^{eree}	192.168.110.7 6 ⁹ Not bound	↑ 1.20Kbps ↓ 5.90Kbps	585M	8 seconds	No Limit	Access Control Associate Block

User not connected

Click the **User not connected tab** to see details about clients waiting to connect. This list includes clients tagged manually or recognized as devices previously connected to the network but not currently listed in device management or online client lists. To remove a client device, click **Delete**.

All (24) Wired (23) Wireless (1) User not connect	ed (6)	Bind IP Search by IP/MAC/Username Q
() The client going offline will not disappear immediately. Ir	stead, the client will stay in the list for 3 more minutes.	
Username	MAC Address	Action
00:11:22:33:44:55 🏼	00:11:22:33:44:55	Delete
00:11:22:33:44:66 🖉	00:11:22:33:44:66	Delete

6.1 Configuring Client IP Binding

A Caution

This function is supported when the device works in router mode.

Choose Network-Wide > Clients.

IP address binding is a security and access control policy that associates a specific IP address with a specific device or user to achieve identity authentication, access control, monitoring, and accounting.

• Single client IP address binding

Select the client to be bound with an IP address in the list, click **Not bound**, and click **OK** in the pop-up box to bind the client to a static IP address.

All (5) Wired (2) Wirele	ss (3) User not connecte	ed (0)		Select	& Block ⇔ Bind IP	
The client going offline will	not disappear immediately.	Instead, the client will	stay in the list for 3 more m	inutes.		
Username	SSID and Band	Connected To	IP/MAC		Rate	Action
Click to edit \mathscr{Z}_{-}	56 @@@@@#######	AP v)	192.168.110.6 1a N	67 ot bound	↑ 0.00bps ↓ 0.00bps	Access Control Associate Block
M2102J25C &	56 @@@@@.	sure you want to conve	× rt the dynamic IP address	69 t bound	† 571.00bps ↓ 1.35Kbps	Access Control Associate Block
DESKTOP-DTTUM8V 🖉	Wired LAN3/W. to a stati	ic IP address?	Cancel	C? t bound	† 0.00bps ↓ 475.00bps	Access Control
DESKTOP-IPV6G6R 🖉	Wired LAN1/Wmw	М		of bound	† 295.54Kbps ↓ 79.64Kbps	Access Control

 Batch IP binding Click Select.

Block ⇔ E	Bind IP	Search by IP/MAC/Username	Q
	Block ⇔	Block ⇔ Bind IP	Block Gearch by IP/MAC/Username

Select the clients to be bound, click **Bind IP**, and click **OK** in the pop-up box to bind the selected clients to a static IP address.

All (5) V	Vired (2) Wireless (3)	User not connected (0)) 0	Deselect 🕹 B	lock Sind IP	earch by IP/MAC/Username Q
i The clie	ent going offline will not die	sappear immediately. Inste	ead, the client will stay in the	list for 3 more minutes.		
	Username	SSID and Band	Connected To	IP/MAC	Rate	Action
	Click to edit 🖉	5G @@@@@2222222222	AP V 9	192.168.110.6 6 ⁹ Not bound	↑ 0.00bps ↓ 0.00bps	Access Control Associate Block
	M2102J2SC 🖉	5G @@@@@2222222222	AP \9	192.168.110.7 ن ې 8 Not bound	↑ 571.00bps ↓ 1.35Kbps	Access Control Associate Block
	DESKTOP-DTTUM8V 企	Wired LAN3/WAN1	eg205g M 15	192.168.110.9 6 7(5 Not bound	 ↑ 0.00bps ↓ 475.00bps 	Access Control

• Unbind an IP address

Select the client to be unbound from the list, click **Bound**, and click **OK** in the pop-up box.

All (5)	Wired (2) Wireless	(3) User not connected (0	0 0	1	Deselect	& Block	⇔ Bind IP	Search by IP/MAC/U	sername	
🕜 The c	lient going offline will n	ot disappear immediately. Inst	ead, the client will stay	in the list for 3 more mil	nutes.					
	Username	SSID and Band	Connected To	IP/MAC		Rate		Action		
	Click to edit 🖉	5G @@@@@2222222222	AP	192.168.110.6 1a:	© Bound	↑ 0.00 ↓ 0.00)bps)bps	Access Control Block	Associat	e

6.2 Configuring Client Access Control

A Caution

Access Control is not supported on AP devices . However, when there are devices on the network that support the **Access Control** function, you can configure this feature globally.

Choose Network-Wide > Clients.

Select a client in the list and click **Access Control** in the **Action** column. You will be redirected to the **Edit Rule** page, where a MAC-based access control rule is automatically generated. The name and MAC address are automatically generated based on the selected client. After selecting the control type and effective time, click **OK** to create an access control rule for the client.

Edit Rule)
Status				
Name	iPhone			
Based on	MAC Address	IP Address		
* MAC Address	1a			
Control Type 🕐	Allow	~		
Effective Time ⑦	All Time	~		
			Cancel	OK

6.3 Configuring Client Association

Choose Network-Wide > Clients.

A Caution

This function applies only to wireless clients.

Select a client in the list and click **Associate** in the **Action** column. You will be redirected to the **Edit Association** page.

) Wired (1) W	fireless (3) User not connecte	ed (0) 🖸		Select	& Block ⇔ Bind I	P Search by IP/MAC/Username
he client going offline	e will not disappear immediately.	Instead, the client will s	stay in the list for 3 more	e minutes.		
Username	SSID and Band	Connected To	IP/MAC		Rate	Action
* 0_	5G @@@@@2222222222	AP W 9	192.168.110.6 14 a	ේ? Not bound	↑ 0.00bps ↓ 0.00bps	Access Control Associate Block
M2102J2SC 🖉	5G @@@@@zzzzzzzzz	AP V	192.168.110.7 8 4	ي Not bound	 ↑ 2.95Kbps ↓ 5.79Kbps 	Access Control Associate Block

The **Client** field is populated with the MAC address of the selected client and cannot be modified. The **Associated Device** field is populated with the associated device of the client by default. Set the SSID and the Forced Association feature as required, and click **OK**. For details, see<u>4.22</u> <u>Client Association</u>.

 \times

* Client	86:ee:0e:1c:9c:a6 \lor
* Associated Device ⑦	Select ~
	Advanced Settings
	Audiced Settings
SSID	Select ~
Forced Association	
	Enabling this feature will forcefully associate the client with a specific AP. However,
	since the client cannot initiate automatic association, this may cause disconnection
	and unsuccessful association attempts.
	Cancel OK

6.4 Blocking Clients

Edit Association

Choose Network-Wide > Clients.

An unauthorized client may occupy network bandwidth and pose security risks. You can block specified clients to solve the unauthorized access problem.

🛕 Caution

Client block is available only for wireless clients.

Block a single client

Select a client to block in the list, click **Block** in the **Action** column, and click **OK** in the pop-up box to block the selected client.

The client going offlin	e will not disannear immediately	Instead, the client will	stay in the list for 3 mor	e minutes		
Username	SSID and Band	Connected To	IP/MAC	e minutes.	Rate	Action
* 2	5G @@@@@@########	АР W 9	192.168.110.6 1. a	6 ⁹ Not bound	↑ 0.00bps ↓ 0.00bps	Access Control Asso Block
M2102J2SC @_	5G @@@@@ <i>zzzzzzzzz</i>	AP v v	192.168.110.7 8 4	් [?] Not bound	† 2.95Kbps ↓ 5.79Kbps	Access Control Asso Block
D		6 · · · · · · · · · · · · · · · · · · ·	×			
Do you want to	add 86:	Cio the blo Cancel	× ocklist? OK			
Do you want to Batch block clie a Click Selec	add 86:	Cancel	× ocklist? OK			

b Select the target clients, click **Block**, and click **OK** in the pop-up box to block the selected clients.

All (4) Wired (1) Wireless	(3) User not connected (0) 🖸	Deselect	& Block ⊖ Bind	P Search by IP/MAC/Username Q
7 The client going offline will not see the client going offline will not see the client going of the c	ot disappear immediately. Ins	tead, the client will sta	y in the list for 3 more minutes.		
Username	SSID and Band	Connected To	IP/MAC	Rate	Action
*2	5G @@@@@ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ	AP WE	192.168.110.6	↑ 0.00bps ↓ 0.00bps	Access Control Associate Block
✓ M2102J2SC &	5G @@@@@ZZZZZZZZZZZ	AP WI	192.168.110.7 6 ⁹ 8	↑ 2.95Kbps ↓ 5.79Kbps	Access Control Associate Block

Cancel block

Choose Network-Wide > Workspace > Wireless > Blocklist/Allowlist > Global Blocklist/Allowlist.

Select the client to be removed from the blocklist in the wireless blocklist and click Delete.

Global Blocklist/Allow	ist SSID-Based Blocklist/Allowlist			
• All STAs except bloc	klisted STAs are allowed to access Wi-Fi.	Only the allowlisted STAs are allowed to access Wi-Fi.		
Blocked WLAN Cl	ients		+ Add	Delete Selected
	Device Name	MAC Address	Actio	on
	M2102J2SC 🖉	81 1	Edit D	elete
Up to 512 members c	an be added.	Total 1	۲ ا	> 10/page >

6.5 Configuring Client Rate Limiting

Choose Network-Wide > Clients > Wireless.

To ensure fair resource allocation, the network administrator can implement wireless rate limiting to prevent some users or devices from occupying a large amount of bandwidth and affecting the network experience of other users.

A Caution

Rate limiting applies only to wireless clients.

• Configure rate limits for clients

Click the **Wireless** tab, click the **LimitSpeed** column in the table, set the uplink rate limit and downlink rate limit, and click **OK**.

All (4) Wired (1)	Wireless (3) User no	t connected (0) O					Select & Block	🗢 Bind IP	Search by IP/MAC/Username Q
The client going offlin	ie will not disappear imi	nediately. Instead, the	client will stay in the list	for 3 more minutes.					
Username	SSID and Band	Signal Quality 🗘	Connected To	IP/MAC	Rate	Negotiation Rate	Online Duration 🗘	LimitSpeed	Action
* 0_	5G @@@@@#######	-42db Channel:149	AP 89	192.168.110.6 1. 3 Not bound	† 0.00bps ↓ 0.00bps	866M	44 minutes 47 seconds	No Limit	Access Control Associate Block
M2102J25C &	5G @@@@@######	-33db Channel:149	AP W	192.168.110.7 6 ⁹ 8 Not bound	† 1.20Kbps ↓ 5.90Kbps	585M	8 seconds	No Limit	Access Control Associate Block

 \times

LimitSpeed

Uplink Rate	No Limit	t by Default. R	Kbps	\sim	
Limit	Current:	Kbps. Range: 1	-1700000) Kbps	
Downlink Rate	No Limit	t by Default. R	Kbps	\sim	
Limit	Current:	Kbps. Range: 1	-1700000) Kbps	
		Disable	Ca	ncel	OI

Cancel rate limits

Click the Wireless tab, click the LimitSpeed column in the table, and click Disable.

All	(4) Wired (1) W	ireless (3) User not	connected (0) 📀				S	elect & Block	⇔ Bind IP	Search by IP/MAC/Username
0	1 The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.									
	Username	SSID and Band	Signal Quality 🗘	Connected To	IP/MAC	Rate	Negotiation Rate	Online Duration ≑	LimitSpeed	Action
	* 0_	5G @@@@@########	-42db Channel:149	AP	192.168.110.6 0 ^(?) Not bound	† 0.00bps ∔ 0.00bps	866M	44 minutes 47 seconds	† 100Mbps ↓ 100Mbps	Access Control Associate Block
	M2102J2SC &	56 @@@@@ uuuuuu	-33db Channel:149	AP W39	192.168.110.7 ε ι Not bound	† 1.20Kbps ↓ 5.90Kbps	585M	8 seconds	No Limit	Access Control Associate Block

LimitSpeed							\times
Uplink Rate	10000			Kbps	~		
Limit	Current:	10000	Kbps. Ra	ange: 1-1	70000	0 Kbps	
Downlink Rate	10000			Kbps	\sim		
Limit	Current:	10000	Kbps. Ra	ange: 1-1	70000	0 Kbps	
			Disable	Car	ncel	OK	

7 System Settings

7.1 PoE Settings

Choose One-Device > Config > Advanced > PoE Settings.

Set 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. In BT mode, the maximum power is 51 W according to the IEEE 802.3bt standard. By default, the device automatically negotiates with the power sourcing equipment (PSE) about the power mode. The default configuration is recommended.

Power Mode	IEEE 802.3at	~
Energy Saving 🕐	Full-Power Mode	~
Radio Switch ⑦	✓ 2.4G ✓ 5G	
Current Power	25.5W	
	Save	

7.2 Setting the Login Password

Go to the configuration page:

- In self-organizing network mode: Choose Network-Wide > Workspace > Network-Wide > Password.
- In standalone mode: Choose **System** > **Login** > **Password**.

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

A Caution

In self-organizing network mode, the login password of all devices in the network will be changed synchronously.

🥖 Change the login pa	assword. Please log in again with the new password later
Old Management	Enter old management password of the project.
Password	
New Management	The management passwords of the network-wide de
Password	There are four requirements for setting the password:
	\cdot The password must contain 8 to 31 characters.
	\cdot The password must contain uppercase and
	lowercase letters, numbers and three types of special
	characters.
	\cdot The password cannot contain admin.
	\cdot The password cannot contain question marks,
	spaces, and Chinese characters.
* Confirm Password	Enter new management password again.
Password Hint	Enter a hint that can help you remember the manag
	Save

7.3 Setting the Session Timeout Duration

Go to the configuration page:

- In self-organizing network mode: Choose One-Device > Config > System > Login.
- In standalone mode: Choose System > Login > Session Timeout.

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

* Session Timeout ⑦	3600	seconds	
	Save		

7.4 Setting and Displaying System Time

Go to the configuration page:

- In self-organizing network mode: Choose Network-Wide > System > System Time.
- In standalone mode: Choose **System > System Time**.

You can view the current system time. If the time is incorrect, check and select the local time zone. If the time zone is correct but time is still incorrect, click **Edit** to manually set the time. In addition, the 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.

A Caution

In self-organizing network mode, the system time of all devices in the network will be changed synchronously.

<i>i</i> Configure and vi	ew system time (the device h	as no RTC	² module, and time settings are not saved upon restart).
Current Time ⑦	2023-12-13 10:22:54 Edi	t	
* Time Zone	(GMT+8:00)Asia/Shanghai	\sim	
* NTP Server 🕐	0.cn.pool.ntp.org	Add	
	1.cn.pool.ntp.org	Delete	
	cn.pool.ntp.org	Delete	
	pool.ntp.org	Delete	
	asia.pool.ntp.org	Delete	
	europe.pool.ntp.org	Delete	
	ntp1.aliyun.com	Delete	
	Save		

7.5 Configuring SNMP

7.5.1 Overview

The Simple Network Management Protocol (SNMP) is a protocol for managing network devices. Based on the client/server model, it can achieve remote monitoring and control of network devices.

SNMP uses a manager and agent architecture. The manager communicates with agents through the SNMP protocol to retrieve information such as device status, configuration details, and performance data. It can also be used to configure and manage devices.

SNMP can be used to manage various network devices, including routers, switches, servers, firewalls, etc. You can achieve user management through the SNMP configuration interface and monitor and control devices through the third-party software.

7.5.2 Global Configuration

1. Overview

The purpose of global configuration is to enable the SNMP service and make the SNMP protocol version (v1/v2c/v3) take effect, so as to achieve basic configuration of local port, device location, and contact information.

SNMP v1: As the earliest version of SNMP, SNMP v1 has poor security, and only supports simple community string authentication. SNMP v1 has certain flaws, such as plaintext transmission of community strings and vulnerability to attacks. Therefore, SNMP v1 is not recommended for modern networks.

SNMP v2c: As an improved version of SNMP v1, SNMP v2c supports richer functions and more complex data types, with enhanced security. SNMP v2c performs better than SNMP v1 in terms of security and functionality, and is more flexible. It can be configured according to different needs.

SNMP v3: As the newest version, SNMP v3 supports security mechanisms such as message authentication and encryption compared to SNMP v1 and SNMP v2c. SNMP v3 has achieved significant improvements in security and access control.

2. Configuration Steps

Choose Network-Wide > Workspace > Network-Wide > SNMP > Global Config.

(1) Enable the SNMP service.

Global Config		
SNMP Service	C	
* SNMP Version	/1	imes Are you sure you want to Enable SNMP?SNMP
* Local Port 16	51	v1/v2c is considered unsafe. Therefore, only SNMP v3 is enabled by default. To proceed, please add SNMP v3 users by selecting
* Device Location Co	om	View/Group/Community/User Access Control before using the SNMP service.
* Contact Info	ıijie	Cancel OK
	Save	ve

When it is enabled for the first time, SNMP v3 is enabled by default. Click OK.

(2) Set SNMP service global configuration parameters.

Global Config V	iew/Group/Community/Client Access Control	Trap Settings
SNMP Service	•	
* SNMP Version	n 🗌 v1 🗌 v2c 🗹 v3	
* Local Por	t 161	
* Device Location	Company	
* Contact Info	Ruijie@Ruijie.com	
	Save	

Parameter	Description			
SNMP Service	Indicates whether SNMP service is enabled.			
SNMP Version	Indicates the SNMP protocol version, including v1, v2c, and v3 versions.			
Local Port	The port range is 1 to 65535.			
Device Location	1-64 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed.			
Contact Info	1-64 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed.			

Table 7-1 Global Configuration Parameters

(3) Click Save.

After the SNMP service is enabled, click **Save** to make basic configurations such as the SNMP protocol version number take effect.

7.5.3 View/Group/Community/User Access Control

1. Configuring Views

• Overview

Management Information Base (MIB) can be regarded as a database storing the status information and performance data of network devices. It contains a large number of object identifiers (OIDs) to identify the status information and performance data of these network devices.

Views in SNMP can limit the range of MIB nodes that the management system can access, thereby improving the security and reliability of network management. Views are an indispensable part of SNMP and need to be configured or customized according to specific management requirements.

A view can have multiple subtrees. The management system can only access MIB nodes in these subtrees, and cannot access other unauthorized MIB nodes. This can prevent unauthorized system administrators from accessing sensitive MIB nodes, thereby protecting the security of network devices. Moreover, views can also improve the efficiency of network management and speed up the response from the management system.

Configuration Steps

Choose Network-Wide > Workspace > Network-Wide > SNMP > View/Group/Community/Client Access Control > View List.

(1) Click Add under the View List to add a view.

System Settings

View List				+ Add	🗓 Delete Selected
Up to 20 entries are allo	owed.				
	View Name			Action	
		No Data			
Total 0 10/page V	< 1 Go to page	1			
(2) Configure basic	information of a view.				
Add			>	×	
* View Name					
OID	Example: .1.3				
	Add Included Rule	Add Excluded Rule			
Rule/OID List			Delete Selected		
Up to 100 entries a	re allowed.				
Ru	le d	DID	Action		
	No Da	ta			
Total 0 10/page ~	\langle 1 \rangle Go t	o page 1			
			Cancel		

 Table 7-2
 View Configuration Parameters

Parameter	Description			
View Name	Indicates the name of the view. 1-32 characters. Chinese or full width characters are not allowed.			
OID	Indicates the range of OIDs included in the view, which can be a single OID or a subtree of OIDs.			
Туре	 There are two types of rules: included and excluded rules. The included rule only allows access to OIDs within the OID range. Click Add Included Rule to set this type of view. Excluded rules allow access to all OIDs except those in the OID range. Click Add Excluded Rule to configure this type of view. 			

1 Note

A least one OID rule must be configured for a view. Otherwise, an alarm message will appear.

(3) Click OK.

2. Configuring v1/v2c Users

Overview

When the SNMP version is set to v1/v2c, user configuration is required.

Global Config	
SNMP Service	
* SNMP Version	✓ v1 ✓ v2c 🗌 v3
* Local Port	161
* Device Location	company
* Contact Info	test@123
	Save

i Note

Select the SNMP protocol version, and click **Save**. The corresponding configuration options will appear on the **View/Group/Community/User Access Control** page.

• Configuration Steps

Choose Network-Wide > Workspace > Network-Wide > SNMP > View/Group/Community/Client Access Control > SNMP v1/v2c Community Name List.

(1) Click Add in the SNMP v1/v2c Community Name List pane.

Global Config View/Group/Comm	nunity/Client Access Control Trap S	Settings		
SNMP v1/v2c Community I	Name List			+ Add 🗈 Delete Selected
Up to 20 entries are allowed.				
Community Nam	e Access I	Node	MIB View	Action
		No Data		
Total 0 10/page > 1	So to page 1			
(2) Add a v1/v2c user.				
Add				×
* Community Name				
* Access Mode	Read-Only	~		
* MIB View	all	~	Add View +	
			Cancel	ОК

Table 7-3 v1/v2c User Configuration Parameters

Parameter	Description		
	At least 8 characters.		
	It must contain at least three character categories, including uppercase		
Community Name	and lowercase letters, digits, and special characters.		
	Admin, public or private community names are not allowed.		
	Question marks, spaces, and Chinese characters are not allowed.		
Access Mode	Indicates the access permission (read-only or read & write) for the community name.		
MIB View	The options under the drop-down box are configured views (default: all, none).		

A Caution

- Community names cannot be the same among v1/v2c users.
- Click Add View to add a view.

(3) Click OK.

3. Configuring v3 Groups

Overview

SNMP v3 introduces the concept of grouping to achieve better security and access control. A group is a group of SNMP users with the same security policies and access control settings. With SNMP v3, multiple groups can be configured, each with its own security policies and access control settings. Each group can have one or more users.

• Prerequisites

When the SNMP version is set to v3, the v3 group configuration is required.

Global Config	View/Group/Community/Client Access Control	Trap Settings
SNMP Ser	vice 🗾	
* SNMP Vers	sion 🗌 v1 🗌 v2c 🔽 v3	
* Local I	Port 161	
* Device Loca	tion Company	
* Contact	Info Ruijie@Ruijie.com	
	Save	

(i) Note

Select the SNMP protocol version, and click **Save**. The corresponding configuration options will appear on the **View/Group/Community/User Access Control** page.

• Configuration Steps

Choose Network-Wide > Workspace > Network-Wide > SNMP > View/Group/Community/Client Access Control > SNMP v3 Group List.

(1) Click Add in the SNMP v3 Group List pane to create a group.

Global Config	View/Group/Community/	Client Access Control Trap Se	ttings			
SNMP v3 Group List + Add						
Up to 20 ent	tries are allowed.					
	Group Name	Security Level	Read-Only View	Read & Write View	Notification View	Action
	default_group	Auth & Security	all	none	none	Edit Delete
Total 1 10/pa	age v (1)	Go to page 1				

(2) Configure v3 group parameters.

Add		×
* Group Name		
* Security Level	Allowlist & Security \sim	
* Read-Only View	all \vee	Add View +
* Read & Write View	all ~	Add View +
* Notification View	none \vee	Add View +
		Cancel OK

Table 7-4 v3 Group Configuration Parameters

Parameter	Description
	Indicates the name of the group.
Group Name	1-32 characters.
	Chinese characters, full-width characters, question marks, and spaces are not allowed.
Security Level	Indicates the minimum security level (authentication and encryption, authentication but no encryption, no authentication and encryption) of the group.
Read-Only View	The options under the drop-down box are configured views (default: all, none).
Read & Write View	The options under the drop-down box are configured views (default: all, none).
Notification View	The options under the drop-down box are configured views (default: all, none).

🛕 Caution

- A group defines the minimum security level, read and write permissions, and scope for users within the group.
- The group name must be unique. To add a view, click Add View.

(3) Click OK.

4. Configuring v3 Users

• Prerequisites

When the SNMP version is set to v3, the v3 group configuration is required.

Global Config	View/Group/Community/Client Access Control	Trap Settings
SNMP Serv	ice 🔵	
* SNMP Versi	ion 🗌 v1 🗌 v2c 🔽 v3	
* Local P	ort 161	
* Device Locati	ion Company	
* Contact Ir	nfo Ruijie@Ruijie.com	
	Save	

Note

Select the SNMP protocol version, and click **Save**. The corresponding configuration options will appear on the **View/Group/Community/User Access Control** page.

• Configuration Steps

Choose Network-Wide > Workspace > Network-Wide > SNMP > View/Group/Community/Client Access Control > SNMP v3 Client List.

(1) Click Add in the SNMP v3 Client List pane to add a v3 user.



(2) Configure v3 user parameters.

ОК

Cancel

Add				×
* Usernam	e Username			
* Group Nam	e Select	~		
* Security Leve	Auth & Security	~		
* Auth Protoco	MD5	~	* Auth Password	
* Encryption Protoco	AES	~	* Encrypted Password	

Parameter	Description		
	Username		
	At least 8 characters.		
Username	It must contain at least three character categories, including uppercase		
	and lowercase letters, digits, and special characters.		
	Admin, public or private community names are not allowed.		
	Question marks, spaces, and Chinese characters are not allowed.		
Group Name	Indicates the group to which the user belongs.		
Security Level	Indicates the security level (authentication and encryption, authentication		
	but no encryption, and no authentication and encryption) of the user.		
	Authentication protocols supported:		
	MD5/SHA/SHA224/SHA256/SHA384/SHA512.		
	Authentication password: 8-31 characters. Chinese characters, full-width		
Auth Protocol Auth Password	characters, question marks, and spaces are not allowed. It must contain		
	at least three character categories, including uppercase and lowercase		
	letters, digits, and special characters.		
	Note: This parameter is mandatory when the security level is		
	authentication and encryption, or authentication but no encryption.		

Parameter	Description
	Encryption protocols supported: DES/AES/AES192/AES256.
	Encryption password: 8-31 characters. Chinese characters, full-width
Encryption Protocol Encrypted	characters, question marks, and spaces are not allowed.
Password	It must contain at least three character categories, including uppercase
	and lowercase letters, digits, and special characters.
	Note: This parameter is mandatory when the security level is
	authentication and encryption.
Password	It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Note: This parameter is mandatory when the security level is authentication and encryption.

🛕 Caution

- The security level of v3 users must be greater than or equal to that of the group.
- There are three security levels, among which authentication and encryption requires the configuration of authentication protocol, authentication password, encryption protocol, and encryption password. Authentication but no encryption only requires the configuration of authentication protocol and encryption protocol, while no authentication and encryption does not require any configuration.

5. Viewing v3 Device Identifier

Choose Network-Wide > Workspace > Network-Wide > SNMP > View/Group/Community/Client Access Control > SNMP v3 Device Identifier List.

View the v3 device identifier in the SNMP v3 Device Identifier List pane.

SNMP v3	Device Identifier List			~
No.	Device Model	IP	engineID	Action
1			80	Сору
Total 1 10/	′page ∨ < <mark>1</mark> > Go	to page 1		

7.5.4 SNMP Service Typical Configuration Examples

1. Configuring SNMP v2c

• Application Scenario

You only need to monitor the device information, but do not need to set and deliver it. A third-party software can be used to monitor the data of nodes like 1.3.6.1.2.1.1 if v2c version is configured.

Configuration Specification

According to the user's application scenario, the requirements are shown in the following table:

Item	Description
View range	Included rule: the OID is .1.3.6.1.2.1.1, and the custom view name is "system".
Version	For SNMP v2c, the custom community name is "Ruijie_com", and the default port number is 161.
Read & write permission	Read-only permission.

Table 7-6 User Requirement Specification

- Configuration Steps
- (1) In the global configuration interface, select v2c and set other settings as default. Then, click Save.

Global Config	View/Group/Community/Client Access Control	Trap Settings
SNMP	Service	
* SNMP \	/ersion □ v1 🔽 v2c □ v3	
* Loc	al Port 161	
* Device Lo	Company	
* Conta	act Info Ruijie@Ruijie.com	
	Save	

- (2) Add a view on the View/Group/Community/Client Access Control interface.
 - a Click Add in the View List pane to add a view.
 - b Enter the view name and OID in the pop-up window, and click Add Included Rule.
 - c Click OK.

Add			×
* View Name	system		
OID	.1.3.6.1.2.1.1		
	Add Included Rule	Add Excluded Rule	
Rule/OID List			Delete Selected
Up to 100 entries a	re allowed.		
R	ule	OID	Action
		No Data	
Total 0 10/page v		Go to page 1	
			Cancel

- (3) On the View/Group/Community/Client Access Control interface, enter the SNMP v1/v2c community name.
 - a Click Add in the SNMP v1/v2c Community Name List pane.
 - b Enter the group name, access mode, and view in the pop-up window.
 - c Click OK.

Add			×
* Community Name	Ruijie_com		
* Access Mode	Read-Only ~		
* MIB View	system \lor	Add View +	
		Cancel O	К

2. Configuring SNMP v3

Application Scenario

You need to monitor and control devices, and use the third-party software to monitor and deliver device information to public nodes (1.3.6.1.2.1). The security level of v3 is authentication and encryption.

Configuration Specification

According to the user's application scenario, the requirements are shown in the following table:

ltem	Description	
View range	Included rule: the OID is .1.3.6.1.2.1, and the custom view name is "public_view".	
	Group name: group	
	Security level: authentication and encryption	
Group configuration	Select public_view for a read-only view.	
	Select public_view for a read & write view.	
	Select none for a notify view.	
	User name: v3_user	
	Group name: group	
Configuring v3 Users	Security level: authentication and encryption	
	Authentication protocol/password: MD5/Ruijie123	
	Encryption protocol/password: AES/Ruijie123	
Version	For SNMP v3, the default port number is 161.	

Table 7-7 User Requirement Specification

- Configuration Steps
- (1) On the global configuration interface, select v3, and change the port number to 161. Set other settings to defaults. Then, click **Save**.

Global Config	/iew/Group/Community/Client Access Control	Trap Settings
SNMP Servio	e 🚺	
* SNMP Versic	on □ v1 □ v2c 🔽 v3	
* Local Po	rt 161	
* Device Locatio	Company	
* Contact Inf	o Ruijie@Ruijie.com	
	Save	

- (2) Add a view on the View/Group/Community/Client Access Control interface.
 - a Click Add in the View List pane.
 - b Enter the view name and OID in the pop-up window, and click Add Included Rule.
 - c Click OK.

Configuration Guide

Add				×
* View Name	public_view			
OID	.1.2.6.1.2.1			
	Add Included Rule	Add Excluded Rule		
Rule/OID List			Delete Selected	
Up to 100 entries ar	e allowed.			
R	ıle	OID	Action	
		No Data		
Total 0 10/page v		Go to page 1		
			Cancel	

- (3) On the View/Group/Community/Client Access Control interface, add an SNMP v3 group.
 - a Click Add in the SNMP v3 Group List pane.
 - b Enter the group name and security level on the pop-up window. As this user has read and write permissions, select public_view for read-only and read & write views, and select none for notify views.
 - c Click OK.

Add		×
* Group Name	group	
* Security Level	Allowlist & Security \sim	
* Read-Only View	public_view \lor	Add View +
* Read & Write View	public_view \lor	Add View +
* Notification View	none \lor	Add View +
		Cancer

- (4) On the View/Group/Community/Client Access Control interface, add an SNMP v3 user.
 - a Click Add in the SNMP v3 Client List pane.
 - b Enter the user name and group name in the pop-up window. As the user's security level is authentication and encryption, enter the authentication protocol, authentication password, encryption protocol, and encryption password.
 - c Click OK.

Add			×
* Username	v3_userRuijie		
* Group Name	group		
* Security Level	Auth & Security		
* Auth Protocol	MD5 ~	* Auth Password	Ruijie123
* Encryption Protocol	AES	* Encrypted Password	Ruijie123
			Cancel

7.5.5 Configuring Trap Service

Trap is a notification mechanism of the Simple Network Management Protocol (SNMP) protocol. It is used to report the status and events of network devices to administrators, including device status, faults, performance, configuration, and security management. Trap provides real-time network monitoring and fault diagnosis services, helping administrators discover and solve network problems in a timely manner.

1. Enabling Trap Service

Enable the trap service and select the effective trap version, including v1, v2c, and v3 versions.

Choose Network-Wide > Workspace > Network-Wide > SNMP > Trap Settings.

Global Config	View/Group/Community/Client Access Control	Trap Settings		
Trap Ser	vice 💽			
* Trap Ver	sion 🗹 v1 🗌 v2c 🗌 v3			
	Save			
Trap v1/v2c	Client List	×		+ Add 📋 Delete Selected
Up to 20 entri	es are allowed.	Are you sure you want to Enable trap?		
	Dest Host IP Ve	Сапсеі ОК	Community Name	Action
		No Data		
Total 0 10/pag	e 🗸 🤇 🚺 > Go to page 👔			

(1) Enable the trap service.

When the trap service is enabled for the first time, the system will pop up a prompt message. Click OK.

(2) Set the trap version.

The trap versions include v1, v2c, and v3.

(3) Click Save.

After the trap service is enabled, click **Save** for the configuration to take effect.
Global Config	View/Group/Community/Client Access Control	Trap Settings
Trap Se	ervice	
* Trap Ve	rsion 🗹 v1 🗌 v2c 🗌 v3	
	Save	

2. Configuring Trap v1/v2c Users

• Overview

Trap is a notification mechanism that is used to send alerts to administrators when important events or failures occur on devices or services. Trap v1/v2c are two versions in the SNMP protocol for network management and monitoring.

Trap v1 is the first version that supports basic alert notification functionality. Trap v2c is the second version, which supports more alert notification options and advanced security features.

By using trap v1/v2c, administrators can promptly understand problems on the network and take corresponding measures.

Prerequisites

Once trap v1 and v2c versions are selected, it is necessary to add trap v1v2c users.

• Configuration Steps

Choose Network-Wide > Workspace > Network-Wide > SNMP > Trap Settings.

(1) Click Add in the Trap v1/v2c Client List pane to add a trap v1/v2c user.

Global Config	J View/Group/Co	mmunity/Client Access Control	Trap Settings		
Traj	p Service 🔵				
* Trap	p Version 🗹 v1 🔽	v2c v3			
	Sa	ve			
Trap v1/	v2c Client List			+ Add	Delete Selected
Up to 20	entries are allowed.				
	Dest Host IP	Version Number	Port ID	Community Name	Action
			No Data		
Total 0 10	0/page 🗸 🔇 1	Go to page 1			

(2) Configure trap v1/v2c user parameters.

* Dest Host IP	Support IPv4/IPv6		
* Version Number	v1	~	
* Port ID			
* Community	Community Name/Username		
Name/Username			

Parameter	Description
Dest Host IP	IP address of the trap peer device. An IPv4 or IPv6 address is supported.
Version Number	Trap version, including v1 and v2c.
Port ID	The port range of the trap peer device is 1 to 65535.
	Community name of the trap user.
	At least 8 characters.
Community Name/Lisername	It must contain at least three character categories, including uppercase
	and lowercase letters, digits, and special characters.
	Admin, public or private community names are not allowed.
	Question marks, spaces, and Chinese characters are not allowed.

Cancel

OK

Table 7-8 Trap v1/v2c User Configuration Parameters

🛕 Caution

- The destination host IP address of trap v1/ v1/v2c users cannot be the same.
- Community names of trap v1/v1/v2c users cannot be the same.

(3) Click OK.

3. Configuring Trap v3 Users

Overview

Trap v3 is a network management mechanism based on the SNMP protocol. It is used to send alert notifications to administrators. Unlike previous versions, trap v3 provides more secure and flexible configuration options, including authentication and encryption features.

Trap v3 offers custom conditions and methods for sending alerts, as well as the recipients and notification methods for receiving alerts. This enables administrators to have a more accurate understanding of the status of network devices and to take timely measures to ensure the security and reliability of the network.

• Prerequisites

When the v3 version is selected for the trap service, it is necessary to add a trap v3 user.

Configuration Steps

Choose Network-Wide > Workspace > Network-Wide > SNMP > Trap Settings.

(1) Click Add in the Trap v3 Client List pane to add a trap v3 user.

Global Config	View/Group/Commu	inity/Client Access Control	Trap Settings				
Trap Se	ervice 🚺						
* Trap Ve	ersion v1 v2	c 🗹 v3					
	Save						
Trap v3 Cli	ent List					+ Add	Delete Selected
Up to 20 ent	tries are allowed.						
De	est Host IP	Port ID	Username	Security Level	Auth Password	Encrypted Password	Action
				No Data			
Total 0 10/pa	nge 🗸 🤇 1	So to page 1					

(2) Configure trap v3 user parameters.

Add							×
* Dest Host IP	Support IPv4/IPv6		* Port ID				
* Username			* Security Level	Auth & S	Security	~	
* Auth Protocol	MD5	\sim	* Auth Password				
* Encryption Protocol	AES	\sim	* Encrypted Password				
					Cancel	0	ĸ

Table 7-9 Trap v3 User Configuration Parameters

Parameter	Description
Dest Host IP	IP address of the trap peer device. An IPv4 or IPv6 address is supported.
Port ID	The port range of the trap peer device is 1 to 65535.

Parameter	Description
	Name of the trap v3 user.
	At least 8 characters.
Username	It must contain at least three character categories, including uppercase
	and lowercase letters, digits, and special characters.
	Admin, public or private community names are not allowed.
	Question marks, spaces, and Chinese characters are not allowed.
Security Level	There are three security levels for a trap user, which are "Auth &
Cecurity Level	Security", "Auth & Open", and "Allowlist & Security".
	Authentication protocols supported:
	MD5/SHA/SHA224/SHA256/SHA384/SHA512.
	Authentication password: 8-31 characters. Chinese characters, full-width
Auth Protocol, Auth Password	characters, question marks, and spaces are not allowed. It must contain
	at least three character categories, including uppercase and lowercase letters, digits, and special characters.
	Note: This parameter must be set when the Security Level is Auth &
	Security or Auth & Open.
	Encryption protocols supported: DES/AES/AES192/AES256.
	Encryption password: 8-31 characters. Chinese characters, full-width
Encryption Protocol Encrypted	characters, question marks, and spaces are not allowed.
Password	It must contain at least three character categories, including uppercase
	and lowercase letters, digits, and special characters.
	Note: This parameter must be set when the Security Level is Auth &
	Security.

A Caution

The destination host IP address of trap v1/v2c/v3 users cannot be the same.

(3) Click OK.

7.5.6 Trap Service Typical Configuration Examples

1. Configuring Trap v2c

• Application Scenarios

During device monitoring, if the device is suddenly disconnected or encounters an abnormality, and the thirdparty monitoring software cannot detect and handle the abnormal situation in a timely manner, you can configure the device with a destination IP address of 192.168.110.85 and a port number of 166 to enable the device to send a v2c trap in case of an abnormality.

Configuration Specification

According to the user's application scenario, the requirements are shown in the following table:

Table 7-10 User Requirement Specific

Item	Description
IP address and port number	The destination host IP is 192.168.110.85, and the port number is 166.
Version	Select the v2c version.
Community name/User name	Trap_ruijie

Configuration Steps

(1) Select the v2c version in the Trap Setting interface and click Save.

Global Config	View/Group/Co	ommunity/Client Access Control	Trap Settings		
Trap	Service 🚺				
* Trap	Version 🗌 v1	✓ v2c □ v3			
	S	ave			
Trap v1/v	/2c Client List			+ Add	Delete Selected
Up to 20	entries are allowed.				
	Dest Host IP	Version Number	Port ID	Community Name	Action
			No Data		
Total 0 10,	/page 🗸 🤇	1 > Go to page 1			

- (2) Click Add in the Trap v1/v2c Client List to add a trap v2c user.
- (3) Enter the destination host IP address, version, port number, user name, and other information. Then, click **OK**.

* Dest Host IP	102 169 110 95	
	192.100.110.05	
* Version Number	v2c ~	
* Port ID	166	
* Community	Trap_ruijie	

2. Configuring Trap v3

• Application Scenarios

During device monitoring, if the device is suddenly disconnected or encounters an abnormality, and the thirdparty monitoring software cannot detect and handle the abnormal situation in a timely manner, you can configure the device with a destination IP address of 192.168.110.87 and a port number of 167 to enable the device to send a v3 trap, which is a safer trap compared with v1/v2c traps.

Cancel

Configuration Specification

According to the user's application scenario, the requirements are shown in the following table:

Table 7-11 User Requirement Specification

Item	Description
IP address and port number	The destination host IP is 192.168.110.87, and the port number is 167.
Version and user name	Select the v3 version and trapv3_ ruijie for the user name.
Authentication	
protocol/authentication password	Authentication protocol/password: MD5/Ruijie123
Encryption protocol/encryption	Encryption protocol/password: AES/Ruijie123
password	

- Configuration Steps
- (1) Select the v3 version in the Trap Setting interface and click Save.

Global Config	View/Group/Comr	munity/Client Access Co	ntrol Trap Settings				
Trap	Service 🚺						
* Trap \	/ersion v1	v2c 🗹 v3					
	Save	•					
Trap v3 Cl	ient List					+ Add	Delete Selected
Up to 20 er	ntries are allowed.						
	est Host IP	Port ID	Username	Security Level	Auth Password	Encrypted Password	Action
				No Data			
Total 0 10/p	age 🗸 🤇 1	> Go to page	1				

- (2) Click Add in the Trap v3 Client List to add a trap v3 user.
- (3) Enter the destination host IP address, port number, user name, and other information. Then, click OK.

Add			×
* Dest Host IP	192.168.110.87	* Port ID	167
* Username	trapv3_ruijie	* Security Level	Auth & Security \vee
* Auth Protocol	MD5	* Auth Password	Ruijie123
* Encryption Protocol	AES	* Encrypted Password	Ruijie123
			Cancel OK

7.6 Configuring Reboot

A Caution

- Do not cut off power during system reboot to avoid device damage.
- Do not refresh the page or close the browser during the reboot. After the device is successfully rebooted and the Web service becomes available, the device automatically jumps to the login page.
- Rebooting the device affects the network. Therefore, exercise caution when performing this operation.

7.6.1 Rebooting the Master Device

In self-organizing network mode:

- Choose Network-Wide > System > Reboot. Click the Reboot tab and select master device.
- Choose Network-Wide > Workspace > Network-Wide > Reboot. Click the Reboot tab and select master

device.

Click the **Reboot** button. The **master device** will restart.

Reboot	Sche	duled Re	boot			
i Do r	not pov	ver off the	e device during	j reboot.		
S	Select	• mast	er device	O All Devices	O Specified Devices	
		F	Reboot			

7.6.2 Rebooting Local Device

• In self-organizing network mode, choose One-Device > Config > System > Reboot.

Click the **Reboot** button. The device will restart.

	<i>i</i> Do not power off the device during reboot.	
	Reboot	
• C	In standalone mode: choose System > Reboot > Rebo Click the Reboot button. The device will restart.	oot.
	Reboot Scheduled Reboot	
	<i>i</i> Do not power off the device during reboot.	
	Reboot	

7.6.3 Rebooting All Devices on the Network

In self-organizing network mode, you can batch reboot all devices on the network.

Go to the configuration page:

- Choose Network-Wide > System > Reboot. Click the Reboot tab and select All Devices.
- Choose Network-Wide > Workspace > Network-Wide > Reboot. Click the Reboot tab and select All Devices.

Click the **Reboot** button to batch reboot all devices on the network.

Reboot	Scheduled Reboot		
i Do not	power off the device during	reboot.	
Sel	ect O master device	• All Devices	O Specified Devices
	Reboot		

🛕 Caution

It takes time to reboot all devices in the current network. The action may affect the whole network. Please be cautious.

7.6.4 Rebooting the Specified Devices

In self-organizing network mode, you can reboot specified devices in the network in batches. Go to the configuration page:

- Choose Network-Wide > System > Reboot. Click the Reboot tab and select Specified Devices.
- Choose Network-Wide > Workspace > Network-Wide > Reboot. Click the Reboot tab and select Specified Devices.

Select required devices from the **Available Devices** list, and click **Add** to add devices to the **Selected Devices** on the right.

Reboot Sch	eduled Reboot				
🚺 Do not por	wer off the device during reboot.				
Select	O master device All Devices	• Specified Devices			
	Available Devices	1/1		Selected Devices	0/0
	Q Search by SN/Model			Q Search by SN/Model	
			< Delete Add >	No data	
	Reboot				

Click the **Reboot** button. Specified devices in the **Selected Devices** list will be rebooted.

Configuration Guide

Reboot Sch	eduled Reboot				
i Do not por Select	wer off the device during reboot.	• Specified Devices			
	Available Devices Search by SN/Model No data	0/0	< Delete Add >	Selected Devices Search by SN/Model N	1/1
	Reboot				

7.7 Configuring Scheduled Reboot

Confirm that the system time is accurate to avoid network interruption caused by device reboot at wrong time. For details about how to configure the system time, see <u>7.4</u> Setting and Displaying System Time.

Go to the configuration page:

- Choose Network-Wide > System > Reboot > Scheduled Reboot.
- Choose Network-Wide > Workspace > Network-Wide > Reboot > Scheduled Reboot.
- AP as primary device: One-Device > Config > System > Reboot > Scheduled Reboot.

A Caution

If you configure scheduled reboot on the management webpage, all devices will restart when the system time matches with the scheduled reboot time. Please be cautious.

Click **Scheduled Reboot**, and select the date and time of scheduled reboot every week. Click **Save**. When the system time matches with the scheduled reboot time, the device will restart. You are recommended to set scheduled reboot time to off-peak hours.

Reboot	Scheduled Reboot
1. Aft i 2. You Note:	ter this feature is enabled, the device will reboot at the scheduled time. u are advised to set the scheduled reboot time in the early morning or other service idle time. : When the upstream device is rebooted at the scheduled time, all downstream devices connected to it will also be rebooted.
Schedul	ed Reboot
F	Repeats on 🗌 Mon 🗹 Tue 🔽 Wed 🗌 Thu 🗌 Fri 🗌 Sat 🗌 Sun
Re	boot Time $00 \lor$: $00 \lor$
	Save

7.8 Configuring Backup and Import

Go to the configuration page:

- Choose Network-Wide > System > Backup & Import. •
- Choose One-Device > Config > System > Backup > Backup & Import.

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 device will restart.

If the target version is much later than the current version, some configuration may be missing. 1. Before importing the configuration file, you are advised to Reset the device.

2. After the configuration file is imported, the device will reboot automa	tical	ll	y.
--	-------	----	----

Backup Config ⑦

Backup Config	Backup			
mport Config ?				
File Path	Choose a fil	е	Browse	Import

7.9 Restoring Factory Settings

7.9.1 Restoring the Current Device to Factory Settings

Choose One-Device > Config > System > Backup > Reset.

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

Backup & Import	Reset	
Vou can reset th performing a fa	he device to factory settings by clicking the Factory Reset button below. If you want to retain the current configuration while ctory reset, then back up the profile the configuration file prior to the reset.	?
Reset		
Backup & Import	Reset	
You can reset th performing a fa	e device to factory settings by clicking the Factory Reset button below. If you want to retain the current configuration while ctory reset, then back up the profile the configuration file prior to the reset.	?
Reset		
	Tips ×	
	Resetting the device will clear the current settings and reboot the device. Do you want to continue?	
	Cancel	

A Caution

The operation will clear all configuration of the current device. If you want to retain the current configuration, back up the configuration first (See <u>7.8</u> Configuring Backup and Import). Therefore, exercise caution when performing this operation.

7.9.2 Restoring All Devices to Factory Settings

In the self-organizing network mode, all devices in the network will be restored to factory settings.

Go to the configuration page:

- Choose Network-Wide > System > Reset.
- Choose Network-Wide > Workspace > Network-Wide > Reset.

Click **All Devices**, select whether to enable **Retain bound account** and Click **Reset All Devices**. All devices in the network will be restored to factory settings.

 You can reset while perform 	the device to factory settings by clicking the Factory Reset button below. If you want to retain the current configuration ing a factory reset, then back up the profile the configuration file prior to the reset.	?
Select	master device All Devices	
Retain bound account	Selecting this checkbox will allow the cloud account to maintain its project management privileges without requiring rebind your account.	you to
	Reset All Devices	

A Caution

The operation will clear all configuration of all devices in the network. If you want to retain the current configuration, back up the configuration first (See <u>7.8</u> <u>Configuring Backup and Import</u>). Therefore, exercise caution when performing this operation.

7.9.3 Restoring Master Device to Factory Settings

Go to the configuration page:

- Choose Network-Wide > System > Reset.
- Choose Network-Wide > Workspace > Network-Wide > Reset.

Select **master device**, and check or uncheck the box next to **Retain bound account**. Then, click **Reset**. The primary device will be restored to factory settings.

You can reset while perform	the device to factory sett ing a factory reset, then	ings by clicking the Factory Reset button below. If you want to retain the current configura back up the profile the configuration file prior to the reset.	tion ?
Select	• master device	All Devices	
Retain bound account	Selecting this checkt rebind your account.	ox will allow the cloud account to maintain its project management privileges without requ	uiring you to
	Reset		

A Caution

This operation will clear the current settings of the primary device on the network and reboot the device. If you want to retain the current configuration, back up the configuration first (See <u>7.8</u> <u>Configuring Backup and</u> <u>Import</u>). Therefore, exercise caution when performing this operation.

7.10 Performing Upgrade and Checking System Version

A Caution

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

7.10.1 Online Upgrade

Go to the configuration page:

- Upgrade primary device on the network: Choose Network-Wide > Workspace > Network-Wide > Upgrade > Online Upgrade.
- Upgrade local device: Choose One-Device > Config > System > Upgrade > Online Upgrade.

You can view the current system version. If there is a new version available, you can click it for an update.



7.10.2 Local Upgrade

Go to the configuration page:

- Upgrade primary device on the network: Choose Network-Wide > Workspace > Network-Wide > Upgrade > Local Upgrade.
- Upgrade local device: Choose One-Device > Config > System > Upgrade > Local Upgrade.

You can view the current software version, hardware version and device model. If you want to upgrade the device with the configuration retained, check **Retain Configuration**. Click **Browse**, select an upgrade package on the local PC, and click **Upload** to upload the file. The device will be upgraded.

Online Upgrade	Local Upgrade	e			
_					
i systool.upgrad	leWarningTip				
M	odel				
Current Version	n 🕐 ReyeeOS				
Retain Configuration	n 🕐 🔽 (lf the	e target version is	s much later tl	han the current	version, you are advised not to retain the configuration.)
File Path	n ? Please	select a file.	Browse	Upload	

7.11 Switching System Language



7.12 Configuring LED Status Control

🛕 Caution

- When the primary device supports the individual AP LED switch function, all the secondary devices will
 also support individual AP LED configuration.
- When the primary device does not support the individual AP LED switch function, none of the secondary
 devices will support individual AP LED configuration either. Only a one-click toggle for the LEDs of all APs
 in the network is available.

7.12.1 Configuring Standalone LED Status

You can enable or disable the system LED status for individual wireless devices on the network.

Go to the configuration page:

• Method 1: Choose Network-Wide > Workspace > Wireless > LED.

LED ⑦			Batch Operation	✓ Open All Close all	IP/MAC/hostname/SN/Sr Q
	Username 🌲	Model 🌲	SN ≑	IP Address ≑	Action ≑
•			G1 2	15 4	
•)*(M. 11	19;	
				Total 2 <	1 > 10/page >

- Method 2: Choose One-Device > Config > Network > LED.
 - o When the AP is the primary device:

LED 💿			Batch Operation	Open All Close all	IP/MAC/hostname/SN/Sr Q
	Username 🍦	Model ≑	SN ≑	IP Address ≑	Action ≑
•			r.	1 3	
				Total 1	1 > 10/page ~

o When the AP is a secondary device.



• Method 3: Choose **One-Device** > **Monitor** > **LED**.

•	MGMT IP:19; SN:N	3 Ø	MAC Address: ۵۵: میں MAC Address: ۵۵ Reyee OS:	0.45 Working Mode: AP ≓ Uptime: 18 minutes 13 se	(U Reboot
	WIFI6	• Normal	or Config	g	
Clients 5G Connected: 0 Capacity: 512 Total Connected: 0 Capacity: 57	3 >	SSID	> 2.4G 5G	Band 2.4G ● 5G ● Channel Auto Channel Auto Tx Power Auto Tx Power Auto	>

7.12.2 Configuring Network-wide LED Status

Choose Network-Wide > Workspace > Wireless > LED.

Turn on the LED of all downlink access points in the network.

LED ⑦			Batch Operation	✓ Open All Close all	IP/MAC/hostname/SN/Sr Q
	Username ≑	Model ≑	SN ≑	IP Address ≑	Action \Rightarrow
•				1	
				Total 1 <	1 > 10/page >

7.13 Configuring Cloud Service

7.13.1 Overview

The Cloud Service feature provides powerful remote network management and operation capabilities, making it convenient and efficient to manage geographically dispersed networks with diverse device types. This feature supports wireless devices, switches, and gateways, enabling unified network management and visualized monitoring and operation. Additionally, it also offers various components such as real-name authentication, dedicated Wi-Fi, and passenger flow analysis, allowing for flexible expansion of network services.

By configuring Cloud Service, you can conveniently mange networks through Ruijie Cloud or the Ruijie Reyee app.

7.13.2 Configuration Steps

Choose One-Device > Config > System > Cloud Service.

If the device is not currently associated with a cloud account, simply follow the on-screen instructions to add it to the network. Open up the Ruijie Reyee app, click the scan icon at the upper left corner on the **Project** page, and enter the device's management password.



Once the device is associated with a cloud account, it will automatically be bound to a cloud server based on its geographic location.

🛕 Caution

Exercise caution when modifying cloud service configurations as improper modifications may lead to connectivity issues between the device and the cloud service.

Cloud Server

\oslash	On-Premises	Private	Cloud	Connected	Cancel
-----------	-------------	---------	-------	-----------	--------

This device is connected to Ruijie Cloud. The IP is 47.104.1.209, Exercise caution when modifying the cloud service configuration to ensure uninterrupted device connectivity.

	Save		
Upload Certificate	.pem .crt .txt	Browse	
	The field is required.		0
* Domain Name			Configure IP
Cloud Server	On-Premises Private Clo	Reset	

To change the Cloud Service configurations, select the cloud server from the **Cloud Server** drop-down list, enter the domain name and IP address, and click **Save**.

(i) Note

If the server selected is not **Other Cloud**, the system automatically fills in the domain name and IP address of the cloud server. When **Other Cloud** is selected, you need to manually configure the domain name and IP address and upload the cloud server certificate.

Table 7-12 Cloud Server Description

Parameter	Description
Cloud Server	Geographic location of the cloud server, including Asian Cloud, European Cloud, Latin American Cloud, American Cloud, Middle Eastern Cloud, Middle Asian Cloud, and On-Premises Private Cloud (Current).
Domain Name	Domain name of the cloud server.
IP Address	IP address of the cloud server.

7.13.3 Unbinding Cloud Service

Choose One-Device > Config > System > Cloud Service

You can click Unbind to unbind the account if you no longer wish to manage this project remotely.

Project Name:radio

Account:

Unbind the account if you no longer wish to manage this project remotely.

It is used to unbind all devices throughout the network. To unbind a single device, remove the device from the network and restore its default settings.



8 Network Diagnosis Tools

🛕 Caution

If the issue persists despite following the troubleshooting methods provided in this section, you may require remote support from a technician who will enable developer mode to resolve the issue. We will ensure your data is protected during this process.

8.1 Network Check

When a network problem occurs on the device, perform a network check and configure the device based on the detection result.

Go to the configuration page: Choose **One-Device** > **Config** > **Diagnostics** > **Diagnose**.

(1) Click Start to perform the network check and show the result.

Start	
	×
	Are you sure you want to perform the network check now?
	Cancel

Recheck

WAN/LAN Cable Connection	0
Negotiation Speed	0
WAN Port Configuration	0
DHCP IP Address Allocation	0
Loop Detection	0
IP Conflicts	0
Routing Configuration	0
Next-Hop Connectivity	0
DNS Configuration	0
IP Session Count	0
Cloud Service Configuration	I

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

IP Session Count	0
DHCP Capacity	0
Ruijie Cloud Server	0
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.	

8.2 Network Tools

Choose One-Device > Config > Diagnostics > Network Tools.

- The Ping tool tests the connectivity between the access point and the IP address or URL. The message "Ping failed" indicates that the access point cannot reach the IP address or URL.
- The Traceroute tool displays the network path to a specific IP address or URL.
- The DNS Lookup tool displays the DNS server address used to resolve a URL.

Enter an IP address or a URL, and click **Start**. If you need to perform the ping or Traceroute operation, configure other parameters as required.

Tool	• Ping	O DNS Lookup	Tool	Ping O Traceroute	DNS Lookup
Туре	● IPv4 ○ IPv6		Туре	 IPv4 IPv6 	
* IP Address/Domain	www.baidu.com		* IP Address/Domain	www.baidu.com	
* Ping Count	4		* Max TTL	20	
* Packet Size	64	Bytes		Start	Stop
PING www.ba 72 bytes from ms 72 bytes from ms 72 bytes from ms 72 bytes from ms 72 bytes from ms	Start idu.com (163.177.151.109): 64 163.177.151.109: seq=0 ttl=5 163.177.151.109: seq=1 ttl=5 163.177.151.109: seq=2 ttl=5 163.177.151.109: seq=3 ttl=5 163.177.151.109: seq=3 ttl=5 163.177.151.109: seq=3 ttl=5 163.177.151.109: seq=3 ttl=5	Stop 4 data bytes 51 time=18.896 51 time=18.686 51 time=18.284 51 time=20.310 ONS Lookup	traceroute to max, 46 byte 1 192.168.11 ms 2 172.20.74. 3 172.20.255 10.932 ms 4 * * * 5 172.22.0.2 6 112.111.60 ms 7 218.104.22	www.baidu.com (163.177.1 packets 11.1 (192.168.111.1) 0.621 r 1 (172.20.74.1) 2.271 ms 9 5.109 (172.20.255.109) 2.97 49 (172.22.0.249) 1.902 ms 0.97 (112.111.60.97) 3.215 r 29.69 (218.104.229.69) 2.89	51.109), 20 hops ms 0.536 ms 0.548 .091 ms 8.565 ms 4 ms 6.424 ms .1.453 ms 1.081 ms ms 3.290 ms 2.794 0 ms 2.639 ms
* IP Address/Domain	www.google.com				
DNS	8.8.8.8				
	Start	Stop			
Result					

8.3 Alerts

When a network exception occurs, the network overview page will display an alert and provide a suggestion. Click an alert in the **Alert Center** to view the faulty device, problem details, and description. You can troubleshoot the fault based on the suggestion.

Ruíjie | Rcycc

The **Alert List** page displays possible problems on the network environment and device. All types of alarms are followed by default. You can click **Unfollow** in the **Action** column to unfollow this type of alarm.

🛕 Caution

After unfollowing a specified alert type, you will not discover and process all alerts of this type promptly. Therefore, exercise caution when performing this operation.

rch

Alert Center ⊗ English ~ Exit

🪺 Vie	ew and manage aları	ms.						
Alert Li	st						View Unfollowed Alert	
Expand	d Alerts		Sug	gestion		A	ction	
~	Power supply is in	sufficient.	Unde the p	er voltage may affect device p power supply of device.	erformance or cause device reboot. Please check	Delete	Unfollow	
	Device Name	SN	Туре	Time	Details		Action	
	Ruijie	G15K34H004233	RAP6260(H)-D	2023-12-06 15:33:10	Currently, 802.3at POE power supply is used. A POE switch or pow supply module compliant with IEEE 802.3bt standard is needed to provide power for the device.	er 9	Delete	
					Total 1	< 1	> 10/page >	
Are y and o	ou sure you delete it fror	ı want to unfo n the alarm li	llow the alar st?	mi				
 After being unfollowed, an alarm will not appear again. You can click View Unfollowed Alert to re-follow an unfollowed alarm. 								
		C	Cancel OF	< l				

Click View Unfollowed Alert to view the unfollowed alert. You can follow the alert again in the pop-up window.

() View and manage alarms.		
Alert List		View Unfollowed Alert
Expand Alerts	Suggestion	Action
	No Data	
		Total 0 < 1 > 10/page >
View Unfollowed Alert		×
Power supply is insufficient. Re-follow		
		Cancel

8.4 Fault Collection

Choose One-Device > Config > 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 fault.

i Compress the configuration file for engineers to identify fault.

Start

8.5 Packet Capturing

Choose One-Device > Config > Diagnostics > Packet Collection.

If the device fails and troubleshooting is required, the packet capture result can be analyzed to locate and rectify the fault.

Select an interface and a protocol and specify the host IP address to capture the content in data packets. Select the file size limit and packet count limit to determine the conditions for automatically stopping packet capture. (If the file size or number of packets reaches the specified threshold, packet capture stops and a diagnostic package download link is generated.)

A Caution

The packet capture operation may occupy excessive system resources, causing network freezing. Therefore, exercise caution when performing this operation.

If you have not installed the packet capture component, you need to download it from the cloud by clicking **Download Component Package**.

Tips: Feature to b	e initialized. Download th	ne component package fro	om Ruijie Cloud! Download Component Package
Interface	ALL	~	
Protocol	ALL	~	
IP			
MAC			
File Size Limit	10		MB
Packet Count Limit			
	Start	Stop	

The downloaded component package takes effect automatically. Click **Start** to execute the packet capture command.

i Packet Capture		
Interface	ALL ~	
Protocol	ALL	
IP		
MAC		
File Size Limit	10	МВ
Packet Count Limit		
Wireless Sniffing		
	Delete Component Package	
	Start Stop	

Table 8-1 Packet Collection Configuration Parameters

Parameter	Description
Interface	Physical or logical interface on the network
Protocol	Protocol used by the packet
IP	IP address of the device
MAC	MAC address of the device
File Size Limit	The maximum amount of data allowed to be stored within a certain time period. If this limit is reached during packet capture, new packet capture will be stopped, or excess packets will be discarded. The maximum limit is 10 MB.
Packet Count Limit	The number of packets stored and analyzed during packet capture. The maximum limit is 1500. A Caution You can configure either the packet count limit or the file size limit, as they are mutually exclusive parameters.
Wireless Sniffing	You can select a wireless interface for packet capture only after enabling this function. After this function is enabled, the interface will be marked as Down, and the Wi-Fi network will be unavailable. To prevent users from forgetting to disable this function and causing the Wi-Fi network to be unusable, the system will automatically disable this function 10 minutes later after it is enabled.

Packet capture can be stopped at any time. After that, a download link is generated. Click this link to save the packet capture result in the PCAP format locally. Use analysis software such as Wireshark to view and analyze the result.

🥡 Packet Capture		
Interface	ALL ~	
Protocol	ALL	
IP		
MAC		
File Size Limit	10	MB
Packet Count Limit		
Wireless Sniffing		
PCAP file	Click to download the PCAP file.	the file.
	Delete Component Package	
	Start Stop	

9 FAQs

9.1 Login Failure

> What can I do when I failed to log in to the web interface?

Perform the following steps:

- (1) Check that the Ethernet cable is properly connected to the LAN port of the device.
- (1) Before accessing the setup page, you are advised to choose Auto for the device enabled with DHCP service to assign an IP address to the PC. If you want to configure a static IP address for the PC, please make sure the IP address of the PC and the LAN port are in the same IP range. The default IP address of the LAN port is 10.44.77.254, and the subnet mask is 255.255.255.0. The IP address of the PC should be set to 10.44.77.X (X is an integer between 2 and 254), and the subnet mask is 255.255.255.0.
- (2) Run the **Ping** command to check the connectivity between the PC and the device. If the ping fails, please check the network settings.
- (3) If the login failure persists, restore the device to factory settings.

9.2 Factory Setting Restoration

> How can I restore the device to factory settings?

Power on the device and press the **Reset** button for more than 5 seconds. The device is restored to factory settings after it is restarted. Then, you can log in to the web interface using the default IP address (10.44.77.254).

9.3 Password Loss

What can I do when I forget the password?

- Webpage management password loss: Please enter the Wi-Fi password. If it is still incorrect, please restore the device to factory settings.
- Wi-Fi password loss: When the access point expands the Wi-Fi coverage, its Wi-Fi password is consistent with that of the primary router. Please check the configuration of the primary router and enter its Wi-Fi password. If the password is still incorrect, please restore the device to factory settings and reconfigure the Wi-Fi password.